kaspersky

Kaspersky Secure Mobility Management

© 2024 АО "Лаборатория Касперского"

Содержание

Справка Kaspersky Secure Mobility Management

Что нового

Работа с Консолью администрирования на базе MMC

- Основные сценарии использования
- О Kaspersky Secure Mobility Management
  - Комплект поставки
  - 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
  - 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
    - Работа с сертификатами мобильных устройств
      - Перевыпуск мобильного сертификата Сервера администрирования
      - Настройка правил выпуска сертификатов
      - Создание сертификата мобильных устройств
      - Интеграция с инфраструктурой открытых ключей
  - Развертывание систем управления мобильными устройствами
    - Сценарий: развертывание Управления мобильными устройствами
    - Включение Управления мобильными устройствами
    - Развертывание системы управления по протоколу iOS MDM
      - Сценарии развертывания Сервера iOS MDM
      - Упрощенная схема развертывания
      - Схема развертывания с использованием принудительного делегирования Kerberos Constrained Delegation (KCD)
      - Включение поддержки Kerberos Constrained Delegation
      - Установка Сервера iOS MDM
      - Получение APNs-сертификата
      - Обновление APNs-сертификата
      - Настройка резервного сертификата Сервера iOS MDM
      - Установка APNs-сертификата на Сервер iOS MDM
      - Настройка доступа к сервису Apple Push Notification
    - Подключение KES-устройств к Серверу администрирования
      - Прямое подключение устройств к Серверу администрирования
      - Схема подключения KES-устройств к Серверу с использованием принудительного делегирования Kerberos Constrained Delegation (KCD)

Использование Firebase Cloud Messaging
Выключение Управления мобильными устройствами
Установка Kaspersky Endpoint Security для Android
Разрешения
Установка Kaspersky Endpoint Security для Android на персональные устройства
Установка Kaspersky Endpoint Security для Android в режиме device owner
Установка Kaspersky Endpoint Security для Android в режиме device owner в закрытой сети
Другие способы установки Kaspersky Endpoint Security для Android
Установка Kaspersky Endpoint Security для Android 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
Контроль
Настройка ограничений
Особые рекомендации для устройств под управлением Android 10 или 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
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
Статусы мобильных устройств
Инвентаризация программного обеспечения на Android-устройствах
Настройка отображения Android-устройств в Kaspersky Security Center
Защита
Настройка защиты от вредоносного ПО на Android-устройствах
Защита Android-устройств в интернете
Защита данных при потере или краже устройств
Отправка команд на утерянное или украденное 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 Per App VPN на устройствах iOS MDM
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
Настройка ограничений на использование SD-карт (только для устройств Samsung)
Управление мобильными устройствами
Управление KES-устройствами
Режим device owner
Ограничение функций Android на устройствах
Настройка режима киоска для Android-устройств
Подключение к NDES/SCEP-серверу
Включение проверки подлинности на основе сертификатов KES-устройств
Создание пакета мобильных приложений для KES-устройств
Просмотр информации о KES-устройстве
Отключение KES-устройства от управления
Управление iOS MDM-устройствами
Подписание iOS MDM-профиля сертификатом
Добавление конфигурационного профиля
Установка конфигурационного профиля на устройство
Удаление конфигурационного профиля с устройства
Добавление provisioning-профиля
Установка provisioning-профиля на устройство
Удаление provisioning-профиля с устройства
Настройка управляемых приложений
Установка приложения на мобильное устройство
Удаление приложения с устройства
Установка и удаление приложений для группы iOS MDM-устройств

Настройка роуминга на iOS MDM-устройстве
Просмотр информации о iOS MDM-устройстве
Отключение устройства iOS MDM от управления
Настройка режима киоска для iOS MDM-устройств
Управление параметрами мобильных устройств
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)
Настройка статуса устройства в Kaspersky Security Center
Управление настройками приложения
Управление настройками Google Chrome
Управление Exchange ActiveSync для Gmail
Настройка прочих приложений
Управление разрешениями приложений
Создание отчета об установленных мобильных приложениях
Установка корневых сертификатов на Android-устройствах
Настройка уведомлений Kaspersky Endpoint Security для Android
Основные функции управления мобильными устройствами в Консоли администрирования на базе MMC
Подключение iOS MDM-устройств к AirPlay
Подключение iOS MDM-устройств к AirPrint
Отключение блокировки активации на контролируемых iOS-устройствах
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
Разблокирование рабочего профиля
Добавление учетной записи LDAP
Добавление учетной записи календаря
Добавление учетной записи контактов
Настройка подписки на календарь
Управление веб-клипами
Установка обоев
Добавление шрифтов
Работа с командами для мобильных устройств
Команды для мобильных устройств
Отправка команд
Просмотр статусов команд в журнале команд
Управление приложением с помощью сторонних EMM-систем (только Android)
Начало работы
Как установить приложение
Защита устройств в интернете
Как активировать приложение

Как подключить устройство к Kaspersky Security Center
Тихий режим работы приложения
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, 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 баз вредоносного ПО
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
Настройка приложения в режиме device owner на устройствах с Android версии 7 и выше
Настройка приложения в режиме device owner на устройствах с Android версий 5–6
Установка корневых сертификатов на устройстве
Установка и использование почтовых и VPN-сертификатов на устройстве
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
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
Комплект поставки
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 защиты от вредоносного ПО
Настройка постоянной защиты
Настройка автоматического запуска поиска вредоносного ПО на мобильном устройстве
Настройка обновления баз вредоносного ПО
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, 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
Лицензирование программы
О Лицензионном соглашении
О лицензии
О подписке
О лицензионном ключе
О коде активации
О файле ключа
Предоставление данных в Kaspersky Endpoint Security для Android
Предоставление данных в Kaspersky Security для iOS
Сравнение функций решения в зависимости от средств управления
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)
KES-устройство
Manifest-файл
POP3
Provisioning-профиль
SSL
Автономный пакет установки
Агент администрирования
Администратор Kaspersky Security Center
Администратор устройства
Активация программы
Базы вредоносного ПО
Веб-сервер Kaspersky Security Center
Виртуальный Сервер администрирования
Вредоносное ПО
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 Kaspersky Secure Mobility Management

Что нового

Узнайте, что нового в последней версии решения.

Настройка защиты устройств

Управляйте защитой мобильных устройств удаленно. Вам доступны Защита от вредоносного ПО, Веб-Фильтр, Анти-Вор и другие функции.

Комплект поставки

Узнайте о компонентах, доступных в вашей версии решения.

Изменение параметров устройства

Управляйте мобильными устройствами удаленно: настраивайте Wi-Fi, VPN, электронную почту, корневые сертификаты на Android-устройствах, веб-клипы и прочее.

Развертывание

Узнайте, как развернуть решение в корпоративной инфраструктуре – настроить Консоль администрирования, установить Kaspersky Endpoint Security для Android и пользоваться MDM-профилями для iOS-устройств.

Настройка контроля устройств

Отслеживайте мобильные устройства удаленно, в том числе настраивайте ограничения, пользовательский доступ к веб-сайтам, Контроль соответствия, Контроль приложений и прочее.

Команды

Управляйте мобильными устройствами удаленно с помощью команд для мобильных устройств: Заблокировать, Удалить корпоративные данные, Определить местоположение, Сфотографировать, Воспроизвести звуковой сигнал и других.

Настройка режима device owner

Управляйте ограничениями ОС Android, настройками Google Chrome, режимом киоска и прочими функциями.

Рабочий профиль Android

Настройте рабочий профиль Android на своем устройстве и пользуйтесь его преимуществами.

Другое

Управляйте безопасностью Android-устройств с помощью стороннего EMM-решения или установите наше решение через KNOX для расширения возможностей защиты устройств Samsung.

Корпоративный каталог приложений

Создайте собственный корпоративный каталог приложений и загружайте приложения из каталога на устройства пользователей через браузер.

Что нового

Версия 4.1

- Мы перешли на новый API Firebase Cloud Messaging (FCM) для принудительной отправки команд и настроек политики на Android-устройства. Мы рекомендуем обновить параметры Firebase Cloud Messaging в Консоли администрирования Kaspersky Security Center, Kaspersky Security Center Web Console и Cloud Console, так как старые API больше не поддерживаются.

- Исправлен ряд ошибок и сделаны некоторые улучшения.

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.

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

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?

О Kaspersky Secure Mobility Management

Kaspersky Secure Mobility Management – это комплексное решение для защиты корпоративных и личных мобильных устройств, используемых сотрудниками компании в корпоративных целях, а также для управления ими.

Kaspersky Secure Mobility Management 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 *справке Kaspersky Endpoint Security Cloud*.

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

Комплект поставки

В комплект поставки Kaspersky Secure Mobility Management могут входить различные компоненты в зависимости от выбранной версии программы.

Kaspersky Security Center

- `ksc_14_<version>_full_<language>.exe`

  Программа установки Kaspersky Security Center. Эта версия создана специально для работы с Kaspersky Secure Mobility Management.

- `ksc_14_<version>_Console_<language>.exe`

  Программа установки Консоли администрирования на базе MMC. Эта версия создана специально для работы с Kaspersky Secure Mobility Management.

  Можно установить Консоль администрирования на другое устройство и управлять Сервером администрирования Kaspersky Security Center удаленно.

Управление мобильными устройствами в Консоли администрирования на базе MMC

- `klcfginst.exe`

  Программа установки Плагина управления Kaspersky Endpoint Security для Android.

- `klmdminst.exe`

  Программа установки Плагина управления Kaspersky Device Management для iOS.

Управление мобильными устройствами в Kaspersky Security Center Web Console

- `on_prem_ksm_devices_<version>.zip`

  Архив, содержащий файлы 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_<version>.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*.

Файл приложения Kaspersky Endpoint Security для Android

`kesandroid10<version><languages>.apk` – пакетный файл Android для приложения Kaspersky Endpoint Security для Android.

Файл Корпоративного каталога приложений

`Install_<version>.exe` – дистрибутив Корпоративного каталога приложений. Дистрибутив содержит следующие компоненты:

- Корпоративный каталог приложений
- Консоль управления корпоративным каталогом приложений
- Сервер Apache

Дополнительная информация об установке Корпоративного каталога приложений приведена в *справке по Корпоративному каталогу приложений*.

Дополнительные файлы

- `sc_package_<languages>.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.

- `kesandroid10<version><languages>.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.

Если вы создадите инсталляционный пакет с архивом `sc_package.exe` в Kaspersky Security Center версии ниже 14.2, Kaspersky Endpoint Security для Android не удастся установить на устройствах под управлением Android 10 и выше. Чтобы избежать этой проблемы, обновитесь до Kaspersky Security Center 14.2 или обратитесь в Службу технической поддержки для получения соответствующей версии архива.

Комплект документации

- Справка Kaspersky Secure Mobility Management.

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:

- **Защита от вредоносного ПО**. Позволяет обнаруживать и устранять угрозы на мобильном устройстве, используя базы вредоносного ПО приложения и дополнительно облачную службу Kaspersky Security Network. В состав Защиты от вредоносного ПО 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 базы вредоносного ПО 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.

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 приложений.** 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).

О плагине управления Kaspersky Endpoint Security для Android

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

- создавать групповые политики безопасности мобильных устройств;

- удаленно настраивать параметры работы приложения Kaspersky Endpoint Security для Android на мобильных устройствах пользователей;

- получать отчеты и статистику о работе мобильного приложения Kaspersky Endpoint Security для Android на устройствах пользователей.

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

О плагине управления Kaspersky Device Management для iOS

Плагин управления Kaspersky Device Management для iOS обеспечивает интерфейс управления мобильными устройствами, подключенными по 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").

Подробная информация о подключении мобильных устройств к Kaspersky Security Center по протоколу iOS MDM приведена в разделе Управление iOS MDM-устройствами.

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

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 Secure Mobility Management.

Аппаратные и программные требования к компьютеру администратора

Для развертывания комплексного решения Kaspersky Secure Mobility Management 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 14.2 и выше.

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

- Консоль администрирования Kaspersky Security Center 14.2 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 14.2 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 или выше (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 10–17 или iPadOS 13–17;
- подключение к интернету.

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 Защита от вредоносного ПО и Веб-Фильтр. Администратор может настраивать параметры Защиты от вредоносного ПО 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 при удалении приложения

- Перед удалением Kaspersky Endpoint Security для Android с устройства снимите флажок **Блокировать системные приложения** в параметрах политики **Контроль приложений** или выключите Контроль приложений.

Известные проблемы в работе Защиты от вредоносного ПО

- 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 базы вредоносного ПО, 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 баз вредоносного ПО с Сервера администрирования может завершиться ошибкой на мобильных устройствах. В этом случае запустите задачу обновления баз вредоносного ПО на Сервере администрирования.

- На некоторых устройствах Kaspersky Endpoint Security для Android не обнаруживает устройства, подключенные по USB OTG. Выполнить поиск вредоносного ПО на таких устройствах невозможно.

- На устройствах с операционной системой Android 11 или 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 и выше может некорректно отображаться окно настройки расписания запуска поиска вредоносного ПО (не отображаются элементы управления). Проблема связана с известным дефектом в Android 7.

- На устройствах под управлением Android 7 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 Kaspersky Endpoint Security для Android не обнаруживает загрузку вредоносного файла в память устройства. Вредоносный файл может быть обнаружен Защитой от вредоносного ПО при запуске файла или во время поиска вредоносного ПО на устройстве. Проблема связана с известным дефектом в Android 6. Для обеспечения безопасности устройства рекомендуется настроить запуск поиска вредоносного ПО по расписанию.

Известные проблемы в работе Веб-Фильтра

- Веб-Фильтр на Android-устройствах поддерживается только браузерами Google Chrome, HUAWEI Browser, Samsung Internet и Яндекс Браузер.

- Функция Custom Tabs поддерживается браузерами Google Chrome, HUAWEI Browser и Samsung Internet.

- В браузерах HUAWEI Browser, Samsung Internet и Яндекс Браузер Веб-Фильтр не блокирует сайты на мобильном устройстве, если используется рабочий профиль и установлен флажок Включить Веб-Фильтр только в рабочем профиле.

- 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 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.

- Чтобы гарантировать, что приложение Kaspersky Endpoint Security для Android разрешает или ограничивает доступ к веб-сайту во всех поддерживаемых версиях Google Chrome, HUAWEI Browser, Samsung Internet Browser и Yandex Browser, добавьте один и тот же URL дважды: один раз – с указанием протокола HTTP (например, https://example.com), а другой раз – с указанием протокола HTTPS (например, https://example.com). В качестве альтернативы вы можете использовать регулярные выражения.

- В Яндекс Браузере и Samsung Internet Browser вредоносные и фишинговые сайты могут оставаться незаблокированными. Это связано с тем, что проверяется только домен веб-сайта, и, если он является доверенным, Веб-Фильтр может пропустить угрозу.

- Если Kaspersky Endpoint Security для Android не установлен в качестве службы Специальных возможностей, то Веб-Фильтр может блокировать разрешенный сайт при подгрузке на него элементов с сайта, домен которого не добавлен в список разрешенных.

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 и выше, необходимо предоставить разрешение "Всегда" для доступа к местоположению устройства. Выдать это разрешение на устройствах с операционной системой Android 10 в режиме device owner невозможно.

- Чтобы выполнить снимок с помощью устройства с операционной системой Android 11 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.

- На некоторых личных устройствах HUAWEI и Honor приложения из разрешенных категорий могут быть заблокированы, а приложения из запрещенных категорий могут оставаться разблокированными. Это связано с тем, что категория для некоторых приложений из AppGallery не может быть определена правильно.

- На некоторых устройствах Samsung и Oppo после снятия флажка **Блокировать системные приложения** значки приложений могут остаться скрытыми на рабочем столе. Это связано с особенностями операционной системы Android.

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 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 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 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.

- На некоторых устройствах HUAWEI появляется уведомление о слишком простом методе разблокировки устройства. В этом случае пользователь должен установить PIN-код, соответствующий требованиям политики. Дополнительные сведения о настройке правильного PIN-кода на устройствах HUAWEI смотрите в разделе Настройка надежного пароля разблокировки для устройства Android.

- На некоторых iOS MDM-устройствах, если задано значение параметра **Минимальное количество специальных символов** и установлен флажок **Разрешить простой пароль**, устройство отображает информацию об установке пароля из 6 или более символов, хотя можно установить пароль из 4 и более символов.

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.

- На управляемых устройствах iOS MDM при установке флажка **Принудительно подключаться только к разрешенным сетям Wi-Fi (только для supervised, iOS 14.5+)** в процессе настройки ограничений функций текущее подключение к Wi-Fi будет прервано, даже если оно добавлено в список разрешенных сетей Wi-Fi. Это связано с особенностями операционной системы Android. Пользователь должен вручную заново подключиться к сети Wi-Fi.

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, 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 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 и выше запрет на использование сетей Wi-Fi не поддерживается.
- 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.
- На Android-устройствах, когда запрещено использование камеры, некоторые приложения могут автоматически закрываться. Эта проблема связана с особенностями работы таких сервисов и функций, как Android System Intelligence и Адаптивный спящий режим, которые используют камеру, чтобы экран не выключался, пока пользователь смотрит на него.

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.
- Если на устройстве Android отключена служба Google "Точность местоположения", команда **Определить местоположение устройства** работать не будет. Обращаем внимание, что не на всех устройствах Android есть эта служба.
- Если вы отправите команду **Включить режим пропажи** на контролируемое устройство iOS MDM без SIM-карты и это устройство будет перезапущено, оно не сможет подключиться к сети Wi-Fi и получить команду **Отключить режим пропажи**. Эта проблема связана с особенностями iOS-устройств. Чтобы этого избежать, можно отправлять эту команду только на устройства с SIM-картой или вставить SIM-карту в заблокированное устройство – в этом случае оно сможет получить команду **Отключить режим пропажи** по мобильной сети.

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.

- На некоторых устройствах Xiaomi рабочий профиль Android можно разблокировать с помощью отпечатка пальца только в том случае, если значение параметра **Период неактивности без блокировки экрана устройства** будет установлено после установки отпечатка пальца в качестве метода разблокировки экрана.

- При выборе действия **Отклонять разрешения автоматически** в параметре **Выдача дополнительных разрешений для работы приложений**, если после синхронизации устройства с Kaspersky Security Center пользователь настроил для приложения необходимые разрешения до того, как это приложение их запросило, то эти разрешения нельзя будет изменить без переустановки приложения или удаления его данных.

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 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 устройствах HUAWEI под управлением Android 5.X или 6 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 устройствах HUAWEI с прошивкой EMUI под управлением Android 7 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 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 или ниже сразу после запуска приложения Kaspersky Endpoint Security для Android происходит его сбой. Это связано с проблемой в Android.

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

- На некоторых устройствах (например, Xiaomi, TECNO и Realme) под управлением Android 9 или выше после установки флажка **Запретить изменение языка** в режиме device owner пользователь по-прежнему может изменить язык, при этом предупреждающее сообщение не отобразится.

- На некоторых устройствах Xiaomi, если для развертывания приложения Kaspersky Endpoint Security для Android используется инсталляционный пакет из Kaspersky Security Center, встроенный антивирус может предложить загрузку из проверенного источника, например, из Xiaomi GetApps. Это связано с тем, что сертификат подписи инсталляционного пакета отличается от указанного в магазине приложений. Если установить приложение из магазина приложений, его дальнейшее обновление может завершиться с ошибкой. Чтобы предотвратить это, пользователю следует нажать на кнопку **Игнорировать** в появившемся окне **Обнаружены угрозы безопасности**, чтобы продолжить установку.

- На некоторых устройствах HUAWEI разрешения службы Специальных возможностей могут быть сброшены после запуска встроенного приложения Digital Balance.

- 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

- Некоторые опции режима device owner и функции управления могут работать некорректно на устройствах Xiaomi (включая Redmi и POCO) из-за особенностей устройств этих производителей.
  - На устройствах Xiaomi, Redmi и POCO могут не работать следующие ограничения функций Android:
    - **Запретить изменение приложений через Настройки**
    - **Запретить удаление приложений**
  - Прочие проблемы:
    - При установке приложения Kaspersky Endpoint Security для Android в режиме device owner на устройствах Xiaomi под управлением Android 12 приложение не запускается автоматически после завершения настройки устройства. Пожалуйста, запустите приложение вручную.

- При настройке разрешений для приложения Kaspersky Endpoint Security для Android на устройствах Xiaomi MI A3 под управлением стандартной операционной системы Android 11 может потребоваться дважды выдать разрешение "Специальные возможности", чтобы настройки применились. После выбора опции **Разрешить** разрешение "Специальные возможности" может быть запрошено повторно. Переведите переключатель в положение **Выключено**, а затем снова в положение **Включено**, чтобы применить изменения и завершить настройку.

- Защита приложения Kaspersky Endpoint Security для Android от удаления может не работать на некоторых устройствах Xiaomi. Проблема вызвана особенностями прошивки MIUI 7 и 8 на устройствах Xiaomi.

- На некоторых устройствах под управлением Android 10 или ниже после установки флажка **Запретить изменение приложений через Настройки** при настройке ограничений для приложений и после применения политики 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 невозможно установить в режиме device owner на следующие устройства: Honor 30i (Android 10), HUAWEI Y8p, HUAWEI Y5 (Android 8.0), 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.

- На некоторых устройствах Samsung и Xiaomi ограничение **Запретить передачу файлов через USB** не блокирует передачу файлов через Android Debug Bridge (ADB).

- На некоторых устройствах (например, Samsung, Oppo или Google Pixel), если после обнаружения несоответствия **Установлены запрещенные приложения** истекло время, выделенное пользователю устройства для устранения этого несоответствия, то выбранное действие может выполниться с задержкой или может потребовать синхронизации устройства с Kaspersky Security Center.

Известные проблемы в режиме киоска

- На iOS MDM-устройствах под управлением iOS 17 и iPadOS 17 после снятия флажка **Автоповорот экрана** в **Настройках режима киоска** ориентация экрана по-прежнему автоматически меняется при повороте устройства.

Известные проблемы, связанные с конфигурациями приложений

- Настройки **Настроить Безопасный режим для YouTube**, **Включить обязательное использование хотя бы Умеренного безопасного режима** и **Отключить обязательное использование Безопасного режима** не работают для Google Chrome. Проблема связана с известным дефектом в Google Chrome.

Развертывание

Этот раздел справки адресован специалистам, которые осуществляют установку Kaspersky Secure Mobility Management, и специалистам технической поддержки организаций, использующих Kaspersky Secure Mobility Management.

Архитектура решения

Kaspersky Secure Mobility Management 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.

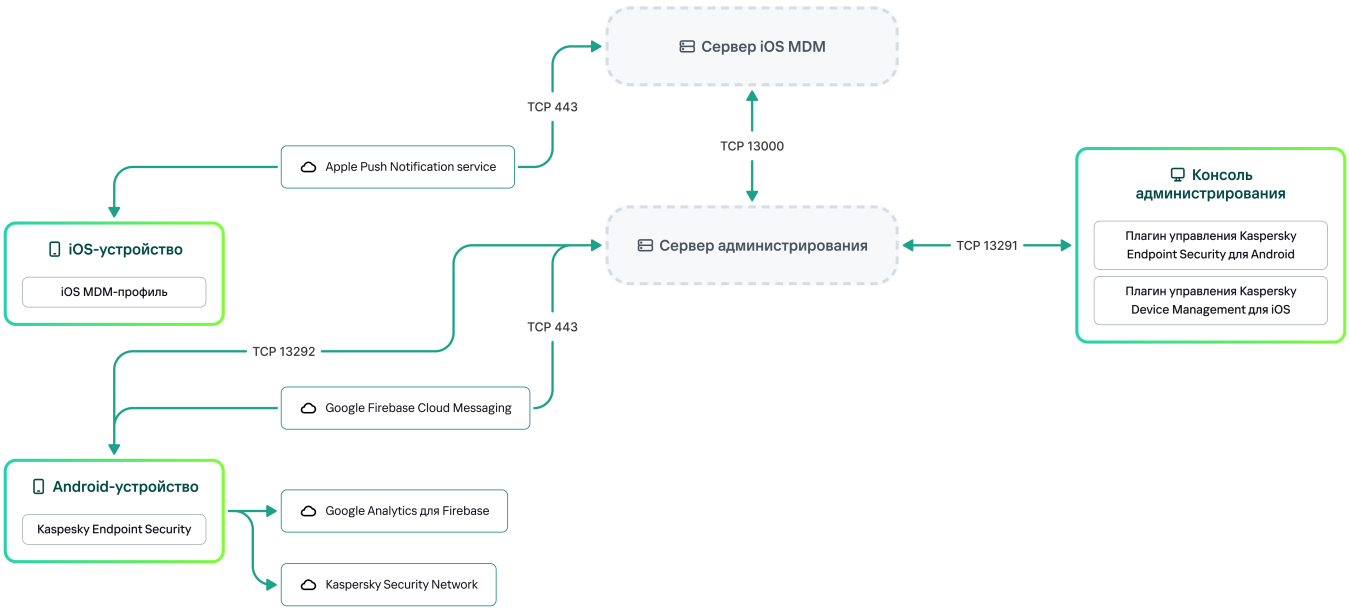
- Плагин управления Kaspersky Endpoint Security для Android

  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 Secure Mobility Management представлена на рисунке ниже.



Архитектура Kaspersky Secure Mobility Management

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

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 *личных устройствах* вы можете развернуть Kaspersky Endpoint Security для Android через Kaspersky Security Center, отправив сообщения со ссылкой на загрузку инсталляционного пакета приложения из Kaspersky Security Center.

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 пакета установки. Доступна массовая рассылка.

Пользователь устанавливает Kaspersky Endpoint Security для Android на мобильное устройство после получения сообщения со ссылкой. Дополнительной подготовки приложения к работе не требуется.

Если для развертывания приложения используется пакет установки, загруженный из Kaspersky Security Center, на экране устройства может появиться сообщение "Заблокировано Play Защитой". Это связано с тем, что сертификат подписи пакета установки отличается от указанного в Google Play. Для продолжения установки необходимо нажать кнопку **Все равно установить**. При нажатии кнопки **ОК** процесс установки будет прерван, а настройки устройства будут сброшены до заводских.

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 следующими способами:

- С помощью отправки QR-кода со ссылкой на загрузку приложения с веб-сайта "Лаборатории Касперского".
- С помощью отправки QR-кода со ссылкой на загрузку пакета установки из Kaspersky Security Center.

Для развертывания Kaspersky Endpoint Security для Android в режиме device owner через приложение, загруженное с веб-сайта "Лаборатории Касперского", 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 пакета установки 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.

> Если для развертывания приложения используется пакет установки, загруженный из Kaspersky Security Center, после сброса настроек устройства до заводских и сканирования QR-кода на экране устройства может появиться сообщение **Заблокировано Play Защитой**. Это связано с тем, что сертификат подписи пакета установки отличается от указанного в Google Play. Для продолжения установки необходимо нажать кнопку **Все равно установить**. При нажатии **ОК** процесс установки будет прерван, а настройки устройства будут сброшены до заводских.

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.

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 сервиса Apple Push Notification service (APNs).

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.

Прежде чем приступить к развертыванию профиля iOS MDM, необходимо развернуть систему управления мобильными устройствами.

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 профиля iOS MDM через Kaspersky Security Center может быть выполнено через отправку сообщений со ссылкой на загрузку профиля iOS MDM. 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.

Подготовка Консоли администрирования к развертыванию комплексного решения

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

Настройка параметров Сервера администрирования для подключения мобильных устройств

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

Чтобы настроить параметры Сервера администрирования для подключения мобильных устройств:

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

   Откроется окно свойств Сервера администрирования.

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

   a. Выберите раздел **Параметры подключения к Серверу администрирования → Дополнительные порты**.

   b. Установите флажок **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 флажок **Открывать порт для мобильных устройств** снят 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 приложения Kaspersky Endpoint Security для Android.

По умолчанию указан порт 17100.

e. Нажмите **OK**.

3. При необходимости замените сертификат, используемый устройствами для подключения к Серверу администрирования:

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

   a. Выберите раздел **Сертификаты**.

   b. Задайте необходимые параметры.

4. Укажите резервный сертификат Сервера администрирования.

   Вам необходимо указать резервный сертификат Сервера администрирования, чтобы обеспечить соответствие требованиям безопасности вашей организации и поддержать постоянное соединение управляемых устройств с Сервером. Резервный сертификат не выпускается по умолчанию.

5. Нажмите **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.

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 **OK**.

   f. В разделе **Точки распространения** нажмите **OK**, 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.

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.

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*.

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** → **Обнаружение устройств** → **Домены** → **KES10** (папка **KES10** используется по умолчанию). 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 разделе **Применение правила** выберите вариант **Выполняется один раз для каждого устройства**.
7. Установите флажок **Перемещать только устройства, которые не входят ни в одну группу 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 **Приложения** 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*.

Работа с сертификатами для мобильных устройств

Этот раздел содержит информацию о работе с сертификатами мобильных устройств. В разделе приведены инструкции по установке сертификатов на мобильные устройства пользователей и по настройке правил выписки сертификатов. Раздел также содержит инструкции по интеграции программы с инфраструктурой открытых ключей и по настройке поддержки Kerberos.

Перевыпуск мобильного сертификата Сервера администрирования

Вам необходимо указать резервный сертификат Сервера администрирования в параметрах перевыпуска сертификата, чтобы обеспечить соответствие требованиям безопасности вашей организации и поддержать постоянное соединение управляемых устройств с Сервером. Резервный сертификат не выпускается по умолчанию.

Мы рекомендуем указывать резервный сертификат при установке Сервера администрирования или не позднее, чем за 30 дней до истечения срока действия основного сертификата. Точное время истечения сертификата доступно в параметрах сертификата в поле **Действителен до** (контекстное меню Сервера администрирования: **Свойства** → **Параметры подключения к Серверу администрирования** → **Сертификаты**).

Максимальный срок действия любого сертификата Сервера администрирования не превышает 397 дней.

Резервный сертификат доставляется на устройство при синхронизации и становится основным сразу после истечения срока действия основного сертификата. Если срок действия сертификата истек, а резервный сертификат не указан, связь между Сервером администрирования и Kaspersky Endpoint Security на управляемых устройствах будет потеряна. В этом случае для повторного подключения устройств необходимо указать новый сертификат и переустановить Kaspersky Endpoint Security на каждом из управляемых устройств.

Чтобы перевыпустить сертификат Сервера администрирования с отложенной заменой (указать сертификат как резервный):

1. В дереве консоли в контекстном меню Сервера администрирования выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования выберите **Параметры подключения к Серверу администрирования** → **Сертификаты**.
3. Если вы планируете и дальше использовать сертификат, выпущенный Kaspersky Security Center:
   a. В группе параметров **Аутентификация Сервера администрирования мобильными устройствами** выберите параметр **Сертификат выпущен средствами Сервера администрирования** и нажмите **Перевыпустить**.
   b. В открывшемся окне **Перевыпуск сертификата**:

a. В группе параметров **Адрес подключения** выберите пункт **Оставить адрес подключения прежним** или пункт **Изменить адрес подключения на**, если будет использован новый адрес подключения.

b. В группе параметров **Срок активации** выберите пункт **Через указанный срок (сут)**, чтобы указать сертификат в качестве резервного.

> Рекомендуется указать срок активации сертификата не менее 30 дней, чтобы все устройства успели получить сертификат. Обратите внимание, что указанный период должен быть больше периода синхронизации устройств с Сервером администрирования. Подробная информация о настройке параметров синхронизации устройств с Сервером администрирования приведена в разделе Настройка параметров синхронизации.

c. Нажмите **ОК**.

d. В появившемся окне нажмите **Да**.

Если вы планируете использовать собственный сертификат:

a. Проверьте, соответствует ли ваш сертификат требованиям Kaspersky Security Center и требованиям к доверенным сертификатам Apple. При необходимости измените сертификат.

b. Выберите параметр **Другой сертификат** и нажмите **Обзор**.

c. В открывшемся окне **Сертификат** в поле **Тип сертификата** выберите тип вашего сертификата и укажите расположение сертификата и параметры:

- Если вы выбрали **Контейнер PKCS#12**, нажмите на кнопку **Обзор** рядом с полем **Файл сертификата** и укажите файл сертификата на жестком диске. Если файл сертификата защищен паролем, введите пароль в поле **Пароль (если есть)**.
- Если вы выбрали **X.509-сертификат**, нажмите на кнопку **Обзор** рядом с полем **Закрытый ключ (.prk, .pem)** и укажите закрытый ключ на жестком диске. Если закрытый ключ защищен паролем, введите пароль в поле **Пароль (если есть)**. Нажмите на кнопку **Обзор** рядом с полем **Открытый ключ (.cer)** и укажите закрытый ключ на жестком диске.

d. В группе параметров **Срок активации** выберите пункт **Через указанный срок (сут)**, чтобы указать сертификат в качестве резервного.

e. В окне Сертификат нажмите **ОК**.

f. В появившемся окне нажмите **Да**.

Сертификат перевыпущен для использования в качестве сертификата Сервера администрирования или указан как резервный.

Чтобы немедленно перевыпустить сертификат Сервера администрирования (не рекомендуется, если есть управляемые мобильные устройства):

> Не рекомендуется выбирать **Немедленно** в случае, если у вас есть управляемые мобильные устройства. При выборе опции будет потеряна связь со всеми управляемыми устройствами, так как новый сертификат не будет доставлен на устройства, а ранее действующий сертификат потеряет силу.

1. В дереве консоли в контекстном меню Сервера администрирования выберите пункт **Свойства**.

2. В окне свойств Сервера администрирования выберите **Параметры подключения к Серверу администрирования → Сертификаты**.

3. Если вы планируете и дальше использовать сертификат, выпущенный Kaspersky Security Center:

   a. В группе параметров **Аутентификация Сервера администрирования мобильными устройствами** выберите параметр **Сертификат выпущен средствами Сервера администрирования** и нажмите **Перевыпустить**.

   b. В открывшемся окне **Перевыпуск сертификата**:

      a. В группе параметров **Адрес подключения** выберите пункт **Оставить адрес подключения прежним** или пункт **Изменить адрес подключения на**, если будет использован новый адрес подключения.

      b. В группе параметров **Срок активации** выберите пункт **Немедленно**.

   c. Нажмите **ОК**.

   d. В появившемся окне нажмите **Да**.

   Если вы планируете использовать собственный сертификат:

   a. Проверьте, соответствует ли ваш сертификат требованиям Kaspersky Security Center и требованиям к доверенным сертификатам Apple. При необходимости измените сертификат.

   b. Выберите параметр **Другой сертификат** и нажмите **Обзор**.

   c. В открывшемся окне **Сертификат** в поле **Тип сертификата** выберите тип вашего сертификата и укажите расположение сертификата и параметры:

      - Если вы выбрали **Контейнер PKCS#12**, нажмите на кнопку **Обзор** рядом с полем **Файл сертификата** и укажите файл сертификата на жестком диске. Если файл сертификата защищен паролем, введите пароль в поле **Пароль (если есть)**.

      - Если вы выбрали **X.509-сертификат**, нажмите на кнопку **Обзор** рядом с полем **Закрытый ключ (.prk, .pem)** и укажите закрытый ключ на жестком диске. Если закрытый ключ защищен паролем, введите пароль в поле **Пароль (если есть)**. Нажмите на кнопку **Обзор** рядом с полем **Открытый ключ (.cer)** и укажите закрытый ключ на жестком диске.

   d. В группе параметров **Срок активации** выберите пункт **Немедленно**.

   e. В окне Сертификат нажмите **ОК**.

   f. В появившемся окне нажмите **Да**.

   Сертификат перевыпущен для использования в качестве сертификата Сервера администрирования или указан как резервный.

Дополнительная информация о сертификатах представлена в справке Kaspersky Security Center.

Настройка правил выпуска сертификатов

Сертификаты используются для аутентификации устройств на Сервере администрирования. Все управляемые мобильные устройства должны иметь сертификаты. Можно настроить способ выпуска сертификатов.

Чтобы настроить правила выпуска сертификатов:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите подпапку **Сертификаты**.
2. В рабочей области папки **Сертификаты** по кнопке **Добавить сертификат** откройте окно **Правила выпуска сертификатов**.
3. Перейдите в раздел с названием типа сертификата:

   Выпуск мобильных сертификатов — для настройки выпуска сертификатов для мобильных устройств.

   Выпуск почтовых сертификатов — для настройки выпуска почтовых сертификатов.

   Выпуск VPN-сертификатов — для настройки выпуска VPN-сертификатов.
4. В блоке **Параметры выпуска** настройте выпуск сертификата:

   - Укажите срок действия сертификата в днях.
   - Выберите источник сертификатов (**Сервер администрирования** или **Сертификаты задаются вручную**).

     По умолчанию источником сертификатов выбран Сервер администрирования.
   - Задайте шаблон сертификатов (**Шаблон по умолчанию**, **Другой шаблон**).

     Настройка шаблонов доступна, если в разделе **Интеграция с PKI** настроена интеграция с инфраструктурой открытых ключей.
5. Для VPN-сертификатов и почтовых сертификатов, если настроена интеграция с PKI, включите и настройте автоматический выпуск сертификата при подключении устройства к Kaspersky Security Center.

   Для этого в разделе **Автоматическая выписка сертификата <тип сертификата> при подключении устройства** установите флажки **Выписывать для KES-устройств под управлением Kaspersky Secure Mobility Management** и/или **Выписывать для iOS MDM-устройств**.

   Если вы установили флажок **Выписывать для iOS MDM-устройств**, выберите тег выпуска сертификата в раскрывающемся списке. Доступны следующие теги: *Шаблон сертификата 1*, *Шаблон сертификата 2* или *Шаблон сертификата 3*.

   Вы можете настроить дальнейшее использование выбранного тега для выпуска сертификата в следующих разделах:

   - Если в окне **Правила выпуска сертификатов** выбран раздел **Выпуск почтовых сертификатов**:
     - В свойствах учетной записи электронной почты для iOS MDM-устройств.
     - В свойствах учетной записи Exchange ActiveSync для iOS MDM-устройств.
   - Если в окне **Правила выпуска сертификатов** выбран раздел **Выпуск VPN-сертификатов**:
     - В свойствах сети VPN для iOS MDM-устройств.
     - В свойствах сети Wi-Fi для iOS MDM-устройств.
6. В блоке **Параметры автоматического обновления** настройте автоматическое обновление сертификата:

   - В поле **Обновлять, когда до истечения срока действия осталось (сут)** укажите, за какое количество дней до истечения срока действия нужно обновлять сертификат.
   - Чтобы включить автоматическое обновление сертификатов, установите флажок **Автоматически перевыпускать сертификат, если это возможно**.

Мобильный сертификат можно перевыпускать только вручную.

7. В блоке **Защита паролем** включите и настройте использование пароля при расшифровке сертификатов.

   Защита паролем доступна только для мобильных сертификатов.

   a. Установите флажок **Запрашивать пароль при установке сертификата**.

   b. С помощью ползунка настройте максимальное количество символов в пароле для шифрования.

8. Нажмите на кнопку **OK**.

Создание сертификата мобильных устройств

На мобильном устройстве пользователя можно создавать сертификаты следующих типов:

- Мобильные сертификаты для идентификации мобильного устройства.
- Почтовые сертификаты для настройки корпоративной почты на мобильном устройстве.
- VPN-сертификат для настройки на мобильном устройстве доступа к виртуальной частной сети.

Чтобы создать сертификат мобильного устройства:

1. В дереве консоли выберите папку **Управление мобильными устройствами → Сертификаты**.
2. В рабочей области папки **Сертификаты** нажмите на кнопку **Добавить сертификат**, чтобы запустить мастер установки сертификатов.
3. На странице **Тип сертификата** укажите тип сертификата, который необходимо установить на мобильное устройство пользователя:

   - **Мобильный сертификат**

     Этот сертификат нужен для идентификации мобильного устройства.

   - **Почтовый сертификат**

     Этот сертификат нужен для настройки корпоративной почты на мобильном устройстве.

   - **VPN-сертификат**

     Этот сертификат нужен для настройки доступа к виртуальной частной сети на мобильном устройстве.

4. На странице **Выбор типа устройства** укажите тип операционной системы на устройстве:

   - **iOS MDM-устройство**

     Выберите этот вариант, если вы хотите установить сертификат на мобильное устройство, подключенное к серверу iOS MDM по протоколу iOS MDM.

   - **KES-устройство под управлением Kaspersky Security для мобильных устройств**

     Выберите этот вариант, если хотите установить сертификат на KES-устройство. В этом случае сертификат будет использоваться при подключении к Серверу администрирования для идентификации пользователя.

- **KES-устройство, которое подключается к Серверу администрирования без аутентификации по пользовательскому сертификату**

  Выберите этот вариант, если вы хотите установить сертификат на устройство KES без аутентификации по сертификату. В этом случае на последнем шаге работы мастера в окне **Способ уведомления пользователей** необходимо выбрать тип авторизации пользователя при каждом подключении к Серверу администрирования.

Это окно отображается, только если ранее был выбран тип сертификата **Почтовый сертификат** или **VPN-сертификат**.

5. На странице **Выбор пользователя** выберите пользователей, группы пользователей или группы пользователей Active Directory, для которых вы хотите создать сертификат.

6. На странице **Источник сертификата** укажите способ создания сертификата.

   - Чтобы создать 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 **Обзор** откройте окно **Сертификат** и укажите в нем файл сертификата.

7. На странице **Параметры публикации сертификатов** установите флажок **Не уведомлять пользователя о новом сертификате**, если вы не хотите уведомлять пользователя о создании сертификата. В этом случае страница **Способ уведомления пользователей** отображаться не будет.

8. На странице **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте.

Эта страница не отображается, если вы выбрали **iOS MDM-устройство** в качестве типа устройства или если вы выбрали параметр **Не уведомлять пользователя о новом сертификате**.

a. В поле **Тип авторизации** укажите тип аутентификации пользователя:

   - Учетные данные (доменные или псевдонима)

     В этом случае пользователь использует доменный пароль или пароль внутреннего пользователя Kaspersky Security Center, для того чтобы получить новый сертификат.

   - Одноразовый пароль

     В этом случае пользователь получит одноразовый пароль, который будет выслан на электронную почту или с помощью SMS. Этот пароль необходимо будет указать для получения нового сертификата.

     Этот параметр изменится на **Пароль**, если вы включили параметр **Разрешить устройству получать один и тот же сертификат несколько раз (только для устройств с установленными приложениями безопасности "Лаборатории Касперского")** в окне **Параметры публикации сертификатов**.

   Это поле отображается, если вы выбрали **Мобильный сертификат** в окне **Тип сертификата** или если в качестве типа устройства вы выбрали **KES-устройство, которое подключается к Серверу администрирования без аутентификации по пользовательскому сертификату**.

b. Выберите вариант уведомления пользователя:

- **Показать пароль после завершения работы мастера**

  Если вы выберете этот параметр, имя пользователя, SAM-имя пользователя (Security Account Manager) и пароль для получения сертификата для каждого из выбранных пользователей будут отображаться на последнем шаге мастера установки сертификата. Настройка параметров уведомления пользователя об установленном сертификате будет недоступна.

  Если вы добавляете сертификаты для нескольких пользователей, вы можете сохранить предоставленные учетные данные в файл, нажав на кнопку **Экспорт** на последнем шаге мастера установки сертификата.

  Этот параметр недоступен, если вы выбрали **Учетные данные (доменные или псевдонима)** на шаге **Способ уведомления пользователя** мастера установки сертификата.

- **Сообщить пользователю о новом сертификате**

  При выборе этого варианта вы можете настроить параметры уведомления пользователя о новом сертификате.

  - **По электронной почте**

    В блоке параметров По электронной почте вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью сообщений электронной почты. Этот способ уведомления доступен, только если настроен SMTP-сервер.

    Перейдите по ссылке **Изменить сообщение**, чтобы просмотреть и изменить сообщение, если это необходимо.

  - **С помощью SMS**

    В этом блоке параметров вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью SMS-сообщений. Этот способ оповещения доступен, только если настроено SMS-оповещение.

    Перейдите по ссылке **Изменить сообщение**, чтобы просмотреть и изменить сообщение, если это необходимо.

9. На странице **Генерация сертификата** нажмите на кнопку **Готово** для завершения работы мастера установки сертификатов.

После завершения работы мастера сертификат будет создан и добавлен в список сертификатов пользователя; кроме того, пользователю будет отправлено уведомление со ссылкой для загрузки и установки сертификата на мобильное устройство. Можно удалять и перевыпускать сертификаты, а также просматривать их свойства.

Интеграция с инфраструктурой открытых ключей

Интеграция с инфраструктурой открытых ключей (Public Key Infrastructure, далее – PKI) в первую очередь предназначена для упрощения выпуска доменных пользовательских сертификатов Сервером администрирования. В результате интеграции выписка сертификатов происходит автоматически.

Минимально поддерживаемая версия сервера PKI – Windows Server 2008.

Администратор может назначить для пользователя доменный сертификат в Консоли администрирования. Это можно сделать одним из следующих способов:

- назначить пользователю особый (персонализированный) сертификат из файла в мастере установки сертификатов;
- выполнить интеграцию с PKI и назначить PKI источником сертификатов для конкретного типа сертификатов либо для всех типов.

Общий принцип интеграции с PKI для выпуска доменных сертификатов пользователей

Обратите внимание:

- В параметрах интеграции с PKI можно указать шаблон по умолчанию для всех типов сертификатов. При этом в правилах выпуска сертификатов (правила доступны в рабочей области папки **Управление мобильными устройствами** / **Сертификаты** по нажатии кнопки **Настроить правила выпуска сертификатов**) можно задать отдельный шаблон для каждого типа сертификатов.
- На устройстве с Сервером администрирования в хранилище сертификатов учетной записи, под которой выполняется интеграция с PKI, должен быть установлен особый сертификат Enrollment Agent (EA). Его предоставляет администратор доменного ЦС (Центра сертификации).

Учетная запись, под которой выполняется интеграция с PKI, должна:

- принадлежать доменному пользователю;
- принадлежать локальному администратору устройства с Сервером администрирования, с которого выполняется интеграция с PKI;
- обладать разрешением *Вход в качестве службы*;
- под этой учетной записью необходимо хотя бы один раз запустить устройство с установленным Сервером администрирования, чтобы создать постоянный профиль пользователя.

Под настроенной учетной записью нужно хотя бы один раз выполнить вход на устройстве с установленным Сервером администрирования для того, чтобы создать постоянный профиль пользователя. В хранилище сертификатов этого пользователя, на устройстве с Сервером администрирования, необходимо установить сертификат агента регистрации, предоставленный администраторами домена.

Настройка интеграции с PKI

Чтобы настроить интеграцию с инфраструктурой открытых ключей:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Сертификаты**.

2. В рабочей области нажмите на кнопку **Тип сертификата**, чтобы открыть раздел **Интеграция с PKI** окна **Правила выпуска сертификатов**.

   Откроется раздел **Интеграция с PKI** окна **Правила выпуска сертификатов**.

3. Установите флажок **Интегрировать выписку сертификатов с PKI**.

4. В поле **Учетная запись** укажите имя учетной записи, которая будет использоваться для интеграции с инфраструктурой открытых ключей.

5. В поле **Пароль** укажите доменный пароль учетной записи.

6. В списке **Имя шаблона сертификата в системе PKI** выберите шаблон сертификата, который будет использоваться для выпуска сертификатов пользователям домена.

   Под указанной учетной записью в Kaspersky Endpoint Security запускается специализированная служба. Эта служба отвечает за выпуск доменных сертификатов пользователей. Служба запускается, когда происходит загрузка списка шаблонов сертификатов по кнопке **Обновить список**, или при выпуске сертификата.

   При подключении к Kaspersky Security Center любого мобильного устройства (под управлением Android или iOS), владельцем которого является недоменный пользователь, попытка выписки сертификата может завершиться ошибкой.

7. Нажмите на кнопку **OK**, чтобы сохранить параметры.

В результате интеграции выписка сертификатов происходит автоматически.

Развертывание систем управления мобильными устройствами

В этом разделе описано развертывание систем управления мобильными устройствами по протоколам iOS MDM и Kaspersky Endpoint Security.

Сценарий: развертывание Управления мобильными устройствами

В этом разделе приведен сценарий для настройки возможностей Управления мобильными устройствами в Kaspersky Security Center.

Предварительные требования

Убедитесь, что ваша лицензия предоставляет доступ к возможностям Управления мобильными устройствами.

Этапы

Развертывание возможностей Управления мобильными устройствами состоит из следующих этапов:

1. **Подготовка портов**

Убедитесь, что порт 13292 доступен на Сервере администрирования. Этот порт требуется для подключения мобильных устройств. Также вы можете сделать доступным порт 17100. Этот порт требуется только для активации прокси-сервера для управляемых мобильных устройств; если управляемые мобильные устройства имеют доступ в интернет, этот порт доступным делать не требуется.

2. **Включение Управления мобильными устройствами**

   Вы можете включить Управление мобильными устройствами во время запуска мастера первоначальной настройки Сервера администрирования или позже.

3. **Указание внешнего адреса Сервера администрирования**

   Вы можете указать внешний адрес во время запуска мастера первоначальной настройки Сервера администрирования или позже. Если вы не выбрали Управление мобильными устройствами для установки и не указали адрес в мастере установки программы, укажите внешний адрес в свойствах инсталляционного пакета.

4. **Добавление мобильных устройств в группу управляемых устройств**

   Добавьте мобильные устройства в группу Управляемые устройства, чтобы управлять этими устройствами с помощью политик. Вы можете создать правило перемещения на одном из шагов мастера первоначальной настройки Сервера администрирования. Также вы можете создать правило перемещения позже. Если вы не создадите такое правило, вы можете добавить мобильные устройства в группу Управляемые устройства вручную.

   Вы можете добавить мобильные устройства в группу Управляемые устройства напрямую или создать для них подгруппу (или несколько подгрупп).

   Позже, в любое время вы можете подключить новое мобильное устройство к Серверу администрирования с помощью мастера подключения мобильного устройства.

5. **Создание политики для мобильных устройств**

   Чтобы управлять мобильными устройствами, создайте политику (или несколько политик) для этих устройств в группе, к которой они принадлежат. Вы можете изменить параметры политики в любое время.

Результаты

После завершения сценария вы сможете управлять устройствами Android и iOS, используя Kaspersky Security Center. Вы можете работать с сертификатами мобильных устройств и отправлять команды на мобильные устройства.

Включение Управления мобильными устройствами

Чтобы управлять мобильными устройствами, вам нужно включить Управление мобильными устройствами. Если вы не включили эту функцию в мастере первоначальной настройки Kaspersky Security Center, вы можете включить ее позже. Для работы функции Управление мобильными устройствами требуется лицензия.

Включение Управления мобильными устройствами доступно только на основном Сервере администрирования.

Чтобы включить Управление мобильными устройствами, выполните следующие действия:

1. В дереве консоли выберите папку **Управление мобильными устройствами**.
2. В рабочей области папки нажмите на кнопку **Включить Управление мобильными устройствами**. Эта кнопка доступна, только если вы ранее не включали **Управление мобильными устройствами**.

Откроется окно **Дополнительные компоненты** мастера первоначальной настройки Сервера администрирования.

3. Для управления мобильными устройствами выберите **Включить Управление мобильными устройствами**.

4. В окне **Выбор способа активации программы** произведите активацию программы с помощью файла ключа или кода активации

   Управление мобильными устройствами будет недоступно, пока вы не активируете возможность Управления мобильными устройствами.

5. На странице **Параметры прокси-сервера для получения доступа в интернет** установите флажок **Использовать прокси-сервер**, если вы хотите использовать прокси-сервер при подключении к интернету. Если флажок установлен, становятся доступны поля ввода параметров. Настройте параметры подключения к прокси-серверу.

6. На странице **Проверка обновлений для плагинов и инсталляционных пакетов** выберите один из следующих вариантов:

   - **Проверить актуальность плагинов и инсталляционных пакетов**

     Запуск проверки на актуальность. Если проверка выявит устаревшие версии некоторых плагинов или инсталляционных пакетов, мастер предложит загрузить актуальные версии для замены устаревших.

   - **Пропустить проверку**

     Продолжение работы без проверки плагинов и инсталляционных пакетов на актуальность. Вы можете выбрать этот вариант, например, если у вас нет доступа в интернет или вы по какой-то причине хотите продолжить работу с устаревшей версией приложения.

     Пропуск проверки актуальности плагинов может привести к некорректной работе программы.

7. В окне **Доступные последние версии плагинов** загрузите и установите последние версии плагинов на необходимом вам языке. Обновление плагинов не требует лицензии.

   После установки плагинов и пакетов приложение проверяет, установлены ли все плагины, необходимые для правильной работы мобильных устройств. Если обнаружатся устаревшие версии некоторых плагинов или инсталляционных пакетов, мастер предложит загрузить актуальные версии вместо устаревших.

8. На странице **Параметры подключения мобильных устройств** настройте порты Сервера администрирования.

После завершения работы мастера будут выполнены следующие изменения:

- создана политика Kaspersky Endpoint Security для Android.
- создана политика Kaspersky Device Management для iOS.
- открыты порты Сервера администрирования для мобильных устройств.

Развертывание системы управления по протоколу iOS MDM

Kaspersky Endpoint Security позволяет управлять мобильными устройствами на платформе iOS. Устройствами iOS MDM называются мобильные устройства под управлением iOS, подключенные к Серверу iOS MDM и находящиеся под управлением Сервера администрирования.

Подключение мобильных устройств к Серверу iOS MDM выполняется в следующей последовательности:

1. Администратор устанавливает Сервер iOS MDM.
2. Администратор получает сертификат Apple Push Notification Service (APNs-сертификат).

   APNs-сертификат позволяет Серверу администрирования подключаться к серверу APNs для отправки push-уведомлений на устройства iOS MDM.
3. Администратор устанавливает на Сервере iOS MDM APNs-сертификат.
4. Администратор создает профиль iOS MDM для пользователя мобильного устройства iOS.

   Профиль iOS MDM содержит набор параметров для подключения мобильных устройств iOS к Серверу администрирования.

После установки профиля и синхронизации мобильного устройства iOS MDM с Сервером администрирования устройство отображается в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Сценарии развертывания Сервера iOS MDM

Количество устанавливаемых копий Сервера iOS MDM зависит от доступного аппаратного обеспечения и от общего числа обслуживаемых мобильных устройств.

Следует учесть, что на одну установку Kaspersky Device Management для iOS рекомендуется не более 50 000 мобильных устройств. С целью уменьшения нагрузки устройства можно распределить между несколькими серверами с установленным Сервером iOS MDM.

Аутентификация устройств iOS MDM осуществляется с помощью пользовательских сертификатов (профиль, устанавливаемый на устройство, содержит сертификат владельца этого устройства). Поэтому возможны две схемы развертывания Сервера iOS MDM:

- Упрощенная схема
- Схема развертывания с использованием принудительного делегирования Kerberos Constrained Delegation (KCD)

Упрощенная схема развертывания

При развертывании Сервера iOS MDM по упрощенной схеме мобильные устройства напрямую подключаются к веб-службе iOS MDM. При этом для аутентификации устройств могут быть использованы только пользовательские сертификаты, выпущенные Сервером администрирования. Интеграция с инфраструктурой открытых ключей для пользовательских сертификатов невозможна.

Схема развертывания с использованием принудительного делегирования Kerberos Constrained Delegation (KCD)

Для использования схемы развертывания с принудительным делегированием Kerberos Constrained Delegation (KCD) Сервер администрирования и Сервер iOS MDM должны располагаться во внутренней сети организации.

Эта схема развертывания предполагает:

- интеграцию с Microsoft Forefront Threat Management Gateway (TMG);
- использование схемы принудительного делегирования Kerberos Constrained Delegation для аутентификации мобильных устройств;
- интеграцию с инфраструктурой открытых ключей для применения пользовательских сертификатов.

При использовании этой схемы развертывания следует учесть, что:

- в Консоли администрирования в параметрах веб-службы iOS MDM необходимо установить флажок **Обеспечить совместимость с Kerberos Constrained Delegation**;
- в качестве сертификата веб-службы iOS MDM следует указать персонализированный сертификат, заданный при публикации веб-службы iOS MDM на TMG;
- пользовательские сертификаты для iOS-устройств должны выпускаться доменным Центром сертификации (ЦС). Если в домене несколько корневых ЦС, то пользовательские сертификаты должны быть выпущены Центром сертификации, указанным при публикации веб-службы iOS MDM на TMG.

  Соответствие пользовательского сертификата указанному требованию обеспечивается несколькими способами:

  - Указать пользовательский сертификат в мастере создания профилей iOS MDM и в мастере установки сертификатов.
  - Интегрировать Сервер администрирования с доменной инфраструктурой открытых ключей и настроить соответствующий параметр в правилах выпуска сертификатов:

    1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Сертификаты**.
    2. В рабочей области папки **Сертификаты** нажмите на кнопку **Настроить правила выпуска сертификатов**, чтобы открыть окно **Правила выпуска сертификатов**.
    3. В разделе **Интеграция с инфраструктурой открытых ключей** настройте интеграцию с инфраструктурой открытых ключей.
    4. В разделе **Выдача мобильных сертификатов** укажите источник сертификатов.

Рассмотрим пример настройки принудительного делегирования KCD со следующими допущениями:

- веб-служба iOS MDM запущена на порте 443;
- имя устройства с TMG – tmg.mydom.local;
- имя устройства с веб-службой iOS MDM – iosmdm.mydom.local;
- имя внешней публикации веб-службы iOS MDM – iosmdm.mydom.global.

Имя субъекта-службы (SPN) для http/iosmdm.mydom.local

В домене требуется зарегистрировать имя субъекта-службы (SPN) для устройства с веб-службой iOS MDM (iosmdm.mydom.local):

```
setspn -a http/iosmdm.mydom.local iosmdm
```

Настройка доменных свойств устройства с TMG (tmg.mydom.local)

Для делегирования трафика необходимо доверить устройство с TMG (tmg.mydom.local) службе, определенной по SPN (http/iosmdm.mydom.local).

Чтобы доверить устройство с TMG службе, определенной по SPN (http/iosmdm.mydom.local), администратор должен выполнить следующие действия:

1. В оснастке Microsoft Management Console под названием Active Directory Users and Computers (Консоль управления пользователями и компьютерами Active Directory) выбрать устройство с установленным TMG (tmg.mydom.local).

2. В свойствах устройства на закладке **Делегирование** для переключателя **Доверять компьютеру делегирование только указанным службам** выбрать вариант **Использовать любой протокол аутентификации**.

3. В список **Службы, с которыми эта учетная запись может использовать делегированные учетные данные** добавить SPN (http/iosmdm.mydom.local).

Особый (персонализированный) сертификат для публикуемой веб-службы (iosmdm.mydom.global)

Требуется выписать особый (персонализированный) сертификат для веб-службы iOS MDM на FQDN iosmdm.mydom.global и указать его взамен сертификата по умолчанию в параметрах веб-службы iOS MDM в Консоли администрирования.

Следует учесть, что в контейнере с сертификатом (файл с расширением p12 или pfx) также должна присутствовать цепочка корневых сертификатов (открытые ключи).

Публикация веб-службы iOS MDM на TMG

На TMG для трафика, идущего со стороны мобильного устройства на порт 443 iosmdm.mydom.global, необходимо настроить KCD на SPN (http/iosmdm.mydom.local) с использованием сертификата, выпущенного для FQDN (iosmdm.mydom.global). При этом следует учесть, что к публикации и публикуемой веб-службе должен быть применен один и тот же сертификат сервера.

Включение поддержки Kerberos Constrained Delegation

Программа поддерживает использование Kerberos Constrained Delegation.

Чтобы включить поддержку Kerberos Constrained Delegation:

1. В дереве консоли выберите папку **Управление мобильными устройствами**.

2. В дереве консоли в папке **Управление мобильными устройствами** выберите подпапку **Серверы мобильных устройств**.

3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
4. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.
5. В окне свойств Сервера iOS MDM выберите раздел **Параметры**.
6. В разделе **Параметры** установите флажок **Обеспечить совместимость с Kerberos constrained delegation**.
7. Нажмите на кнопку **ОК**.

Установка Сервера iOS MDM

Чтобы установить Сервер iOS MDM на клиентское устройство, выполните следующие действия:

1. В дереве консоли, в папке **Управление мобильными устройствами** выберите подпапку **Серверы мобильных устройств**.
2. Нажмите на кнопку **Установить Сервер iOS MDM**.

   Запустится мастер развертывания Сервера iOS MDM. Пройдите все шаги мастера, нажимая на кнопку **Далее**.
3. На странице **Выбор пакета установки** выберите пакет установки Сервера iOS MDM, который требуется установить.

   Если в списке нет нужного пакета, нажмите на кнопку **Новый**, чтобы создать нужный пакет.
4. При необходимости на странице **Выбор пакета установки Агента администрирования для комбинированной установки** оставьте флажок **Установить Агент администрирования вместе с этим приложением** и выберите версию Агента администрирования, которую необходимо установить.

   Агент администрирования требуется для подключения Сервера iOS MDM к Kaspersky Security Center. Если Агент администрирования уже установлен на устройстве, на котором необходимо установить Сервер iOS MDM, этот шаг можно пропустить.
5. На странице **Параметры подключения** в поле **Внешний порт подключения к iOS MDM** укажите внешний порт для подключения мобильных устройств к службе iOS MDM.

   Внешний порт 5223 используется мобильными устройствами для связи с APNs-сервером. Убедитесь, что в сетевом экране открыт порт 5223 для подключения к диапазону адресов 17.0.0.0/8.

   Для подключения устройства к Серверу iOS MDM по умолчанию используется порт 443. Если порт 443 уже используется другим сервисом или приложением, вместо него можно использовать, например, порт 9443.

   Сервер iOS MDM использует внешний порт 2197 для отправки уведомлений на APNs-сервер.

   APNs-серверы работают в режиме сбалансированной нагрузки. Мобильные устройства не всегда подключаются к одним и тем же IP-адресам для получения уведомлений. Диапазон адресов 17.0.0.0/8 зарезервирован за компанией Apple, поэтому рекомендуется указать его в качестве разрешенного диапазона в параметрах сетевого экрана.
6. Если вы хотите вручную настроить порты взаимодействия для компонентов программы, выберите параметр **Настроить локальные порты вручную**, а затем укажите значения следующих параметров:

   - **Порт подключения к Агенту администрирования**

     Укажите в поле порт подключения службы iOS MDM к Агенту администрирования. Порт по умолчанию: 9799.

- **Локальный порт подключения к службе iOS MDM**

  Укажите в поле локальный порт подключения Агента администрирования к службе iOS MDM. Порт по умолчанию: 9899.

Рекомендуется использовать значения по умолчанию.

7. В поле **Адрес Сервера iOS MDM** укажите адрес клиентского устройства, на котором будет установлен Сервер iOS MDM.

   Этот адрес будет использоваться для подключения управляемых мобильных устройств к службе iOS MDM. Клиентское устройство должно быть доступно для подключения устройств iOS MDM.

   Можно указать адрес клиентского устройства в одном из следующих форматов:

   - **Использовать FQDN устройства**

     Будет использоваться полное доменное имя (FQDN).

   - **Использовать этот адрес**

     Введите адрес устройства вручную.

   Не следует включать в строку с адресом URL-схему и номер порта: эти значения будут добавлены автоматически.

8. На странице **Выбор устройств для установки** выберите устройства, на которые нужно установить Сервер iOS MDM.

9. На странице **Переместить в список управляемых устройств** укажите, нужно ли перемещать устройства в какую-либо группу администрирования после установки Агента администрирования.

   Этот вариант применим, если на предыдущей странице выбрано одно или несколько нераспределенных устройств. Если были выбраны только управляемые устройства, пропустите этот шаг.

10. Задайте другие параметры в мастере. Подробная информация об удаленной установке приложений приведена в справке Kaspersky Security Center.

По окончании работы мастера Сервер iOS MDM будет установлен на выбранные устройства. Сервер iOS MDM отображается в папке **Управление мобильными устройствами** дерева консоли.

Мастер установки перейдет к шагу **Установка APNs-сертификата**. Если вы не хотите сразу переходить к управлению сертификатами, можно создать сертификат или установить уже существующий сертификат позже.

Получение APNs-сертификата

Если у вас уже есть APNs-сертификат, обновите его, а не создавайте новый. При замене существующего APNs-сертификата на новый Сервер администрирования теряет управление подключенными в данный момент мобильными устройствами iOS.

После создания запроса Certificate Signing Request (CSR-запрос) на первом шаге мастера получения APNs-сертификата его закрытый ключ сохраняется в оперативной памяти устройства. Поэтому все шаги мастера должны быть завершены в рамках одной сессии работы с программой.

Чтобы получить APNs-сертификат, выполните следующие действия:

1. В дереве консоли, в папке **Управление мобильными устройствами** выберите подпапку **Серверы мобильных устройств**.

2. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.

3. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера iOS MDM.

4. В окне свойств Сервера iOS MDM выберите раздел **Сертификаты**.

5. В разделе **Сертификаты** в блоке параметров **Сертификат Apple Push Notification** нажмите на кнопку **Запросить новый**.

   Запустится мастер запроса нового APNs-сертификата.

6. Создайте запрос Certificate Signing Request (далее – CSR-запрос). Для этого:

   a. Нажмите на кнопку **Создать CSR-запрос**.

   b. В открывшемся окне **Создание CSR-запроса** укажите название запроса, название компании и отдела, город, регион и страну.

   c. Нажмите на кнопку **Сохранить** и укажите имя файла, в котором будет сохранен CSR-запрос.

   Закрытый ключ сертификата будет сохранен в памяти устройства.

7. Отправьте созданный файл с CSR-запросом на заверение в "Лабораторию Касперского" через ваш CompanyAccount.

   > Заверение CSR-запроса доступно только после загрузки на портал CompanyAccount ключа, позволяющего использовать Управление мобильными устройствами.

   После обработки вашего электронного запроса вы получите файл CSR-запроса, заверенный "Лабораторией Касперского".

8. Отправьте заверенный файл CSR-запроса на веб-сайт Apple Inc. через произвольный Apple ID.

   > Но мы не рекомендуем использовать персональный Apple ID. Создайте отдельный Apple ID для корпоративных целей. Созданный Apple ID привяжите к почтовому ящику организации, а не отдельного сотрудника.

   После обработки CSR-запроса в Apple Inc. вы получите открытый ключ APNs-сертификата. Сохраните полученный файл на диск.

9. Экспортируйте APNs-сертификат вместе с закрытым ключом, созданным при формировании CSR-запроса, в файл формата PFX. Для этого:

   a. В открывшемся окне мастера запроса нового APNs-сертификата нажмите на кнопку **Закрыть CSR-запрос**.

   b. В окне **Открытие файла** выберите файл с открытым ключом сертификата, полученный после обработки CSR-запроса от Apple Inc., и нажмите на кнопку **Открыть**.

Начнется экспорт сертификата.

c. В открывшемся окне введите пароль для закрытого ключа и нажмите на кнопку **OK**.

Заданный пароль будет использоваться для установки APNs-сертификата на Сервер iOS MDM.

d. В открывшемся окне **Сохранение APNs-сертификата** укажите имя файла для сохранения APNs-сертификата, выберите папку и нажмите на кнопку **Сохранить**.

Закрытый и открытый ключи сертификата будут объединены, APNs-сертификат будет сохранен в файл формата PFX. После этого можно установить APNs-сертификат на Сервер iOS MDM.

Обновление APNs-сертификата

Чтобы обновить APNs-сертификат, выполните следующие действия:

1. В дереве консоли, в папке **Управление мобильными устройствами** выберите подпапку **Серверы мобильных устройств**.
2. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
3. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера iOS MDM.
4. В окне свойств Сервера iOS MDM выберите раздел **Сертификаты**.
5. В разделе **Сертификаты** в блоке параметров **Сертификат Apple Push Notification** нажмите на кнопку **Обновить**.

   Откроется мастер обновления APNs-сертификатов.
6. Создайте запрос Certificate Signing Request (далее – CSR-запрос). Для этого:

   a. Нажмите на кнопку **Создать CSR-запрос**.

   b. В открывшемся окне **Создание CSR-запроса** укажите название запроса, название компании и отдела, город, регион и страну.

   c. Нажмите на кнопку **Сохранить** и укажите имя файла, в котором будет сохранен CSR-запрос.

   Закрытый ключ сертификата будет сохранен в памяти устройства.
7. Отправьте созданный файл с CSR-запросом на заверение в "Лабораторию Касперского" через ваш CompanyAccount.

   > Заверение CSR-запроса доступно только после загрузки на портал CompanyAccount ключа, позволяющего использовать Управление мобильными устройствами.

   После обработки вашего электронного запроса вы получите файл CSR-запроса, заверенный "Лабораторией Касперского".
8. Отправьте заверенный файл CSR-запроса на веб-сайт Apple Inc. через произвольный Apple ID.

Но мы не рекомендуем использовать персональный Apple ID. Создайте отдельный Apple ID для корпоративных целей. Созданный Apple ID привяжите к почтовому ящику организации, а не отдельного сотрудника.

После обработки CSR-запроса в Apple Inc. вы получите открытый ключ APNs-сертификата. Сохраните полученный файл на диск.

9. Запросите открытый ключ сертификата. Для этого выполните следующие действия:

   a. Перейдите на портал Apple Push Certificates. Для авторизации на портале потребуется Apple ID, полученный при первичном запросе сертификата.

   b. В списке сертификатов выберите сертификат, APSP-имя которого (в формате "APSP: <номер>") совпадает с APSP-именем сертификата, используемого Сервером iOS MDM, и нажмите на кнопку **Обновить**.

      APNs-сертификат будет обновлен.

   c. Сохраните созданный на портале сертификат.

10. Экспортируйте APNs-сертификат вместе с закрытым ключом, созданным при формировании CSR-запроса, в файл формата PFX. Для этого:

    a. В окне мастера обновления APNs-сертификатов нажмите на кнопку **Закрыть CSR-запрос**.

    b. В окне **Открытие файла** выберите файл с открытым ключом сертификата, полученный после обработки CSR-запроса в Apple Inc., и нажмите на кнопку **Открыть**.

       Начнется экспорт сертификата.

    c. В открывшемся окне введите пароль для закрытого ключа и нажмите на кнопку **OK**.

       Заданный пароль будет использоваться для установки APNs-сертификата на Сервер iOS MDM.

    d. В открывшемся окне **Обновление APNs-сертификата** укажите имя файла для сохранения APNs-сертификата, выберите папку и нажмите на кнопку **Сохранить**.

Закрытый и открытый ключи сертификата будут объединены, APNs-сертификат будет сохранен в файл формата PFX.

Настройка резервного сертификата Сервера iOS MDM

Функциональность Сервера iOS MDM позволяет выпустить резервный сертификат. Этот сертификат предназначен для использования в профилях iOS MDM, чтобы обеспечить переключение управляемых iOS-устройств после истечения срока действия сертификата Сервера iOS MDM.

Если ваш Сервер iOS MDM по умолчанию использует сертификат, выпущенный "Лабораторией Касперского", вы можете выпустить резервный сертификат (или указать собственный сертификат в качестве резервного) до истечения срока действия сертификата Сервера iOS MDM. По умолчанию резервный сертификат будет выпущен автоматически за 60 дней до истечения срока действия сертификата Сервера iOS MDM. Резервный сертификат Сервера iOS MDM становится основным сразу после истечения срока действия сертификата Сервера iOS MDM. Открытый ключ распространяется на все управляемые устройства через конфигурационные профили, поэтому вам не нужно передавать его вручную.

Чтобы выпустить резервный сертификат Сервера iOS MDM или указать пользовательский резервный сертификат, выполните следующие действия:

1. В дереве консоли, в папке **Управление мобильными устройствами** выберите подпапку **Серверы мобильных устройств**.

2. В списке серверов мобильных устройств выберите соответствующий Сервер iOS MDM и на правой панели нажмите на кнопку **Настроить Сервер iOS MDM**.

3. В открывшемся окне параметров Сервера iOS MDM выберите раздел **Сертификаты**.

4. В блоке параметров **Резервный сертификат** выполните одно из следующих действий:

   - Если вы планируете и дальше использовать самозаверенный сертификат (то есть сертификат, выпущенный "Лабораторией Касперского"), выполните следующие действия:

     a. Нажмите на кнопку **Выпустить**.

     b. В открывшемся окне **Дата активации** выберите один из двух вариантов даты, когда необходимо применить резервный сертификат:

        - Если вы хотите применить резервный сертификат в момент истечения срока действия текущего сертификата, выберите параметр **По истечении срока действия текущего сертификата**.

        - Если вы хотите применить резервный сертификат до истечения срока действия текущего сертификата, выберите параметр **По истечении указанного периода (в днях)**. В поле ввода рядом с этим параметром укажите продолжительность периода, по истечении которого резервный сертификат должен заменить текущий сертификат.

        > Срок действия указанного вами резервного сертификата не может превышать срок действия текущего сертификата Сервера iOS MDM.

     c. Нажмите на кнопку **ОК**.

     Будет выписан резервный сертификат Сервера iOS MDM.

   - Если вы планируете применить пользовательский сертификат, выпущенный вашим центром сертификации, выполните следующие действия:

     a. Нажмите на кнопку **Добавить**.

     b. В открывшемся окне проводника укажите файл сертификата в формате PEM, PFX или P12, который хранится на вашем устройстве, и нажмите на кнопку **Открыть**.

     Пользовательский сертификат указан как резервный сертификат Сервера iOS MDM.

Резервный сертификат Сервера iOS MDM указан. Подробная информация о резервном сертификате отображается в блоке параметров **Резервный сертификат** (название сертификата, компания, выпустившая сертификат, срок действия и дата применения резервного сертификата, если указана).

Установка APNs-сертификата на Сервер iOS MDM

После получения APNs-сертификата необходимо установить его на Сервер iOS MDM.

Чтобы установить APNs-сертификат на Сервер iOS MDM, выполните следующие действия:

1. В дереве консоли, в папке **Управление мобильными устройствами** выберите подпапку **Серверы мобильных устройств**.

2. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.

3. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера iOS MDM.

4. В окне свойств Сервера iOS MDM выберите раздел **Сертификаты**.

5. В разделе **Сертификаты** в блоке параметров **Сертификат Apple Push Notification** нажмите на кнопку **Установить**.

6. Выберите файл формата PFX, содержащий APNs-сертификат.

7. Введите пароль закрытого ключа, указанный при экспорте APNs-сертификата.

APNs-сертификат будет установлен на Сервер iOS MDM. Информация о сертификате будет отображаться в окне свойств Сервера iOS MDM в разделе **Сертификаты**.

Настройка доступа к сервису Apple Push Notification

Чтобы обеспечить корректную работу веб-службы iOS MDM и своевременное реагирование мобильных устройств на команды администратора, в параметрах Сервера iOS MDM нужно указать сертификат Apple Push Notification Service (далее – APNs-сертификат).

Взаимодействуя со службой Apple Push Notification (далее – APNs), веб-служба iOS MDM подключается к внешнему адресу api.push.apple.com по исходящему порту 2197. Поэтому веб-службе iOS MDM необходимо предоставить доступ к порту TCP 2197 для диапазона адресов 17.0.0.0/8. Со стороны iOS-устройства – доступ к порту TCP 5223 для диапазона адресов 17.0.0.0/8.

Если доступ к APNs со стороны веб-службы iOS MDM будет предоставляться через прокси-сервер, то на устройстве с установленной веб-службой iOS MDM необходимо выполнить следующие действия.

1. Добавить в реестр следующие строки.

   - Для 32-разрядных операционных систем:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Имя прокси-узла>"
"ApnProxyPort"="<Порт прокси-сервера>"
"ApnProxyLogin"="<Логин для прокси-сервера>"
"ApnProxyPwd"="<Пароль для прокси-сервера>"
```

   - Для 64-разрядных операционных систем:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Имя прокси-узла>"
"ApnProxyPort"="<Порт прокси-сервера>"
"ApnProxyLogin"="<Логин для прокси-сервера>"
"ApnProxyPwd"="<Пароль для прокси-сервера>"
```

2. Перезапустить веб-службу iOS MDM.

Подключение KES-устройств к Серверу администрирования

В зависимости от способа подключения устройств к Серверу администрирования существуют две схемы развертывания:

- схема развертывания с прямым подключением устройств к Серверу администрирования;
- схема развертывания с использованием Forefront Threat Management Gateway (TMG).

Прямое подключение устройств к Серверу администрирования

KES-устройства могут напрямую подключаться к порту 13292 Сервера администрирования.

В зависимости от способа аутентификации существуют два варианта подключения KES-устройств к Серверу администрирования:

- с использованием пользовательского сертификата;
- без пользовательского сертификата.

Подключение устройства с использованием пользовательского сертификата

При подключении устройства с использованием пользовательского сертификата оно привязывается к учетной записи пользователя, для которой был назначен соответствующий сертификат через средства Сервера администрирования.

В этом случае будет использована двусторонняя (взаимная) аутентификация SSL. Сервер администрирования и устройство будут аутентифицированы с помощью сертификатов.

Подключение устройства без пользовательского сертификата

При подключении устройства без пользовательского сертификата оно не будет привязано ни к одной учетной записи пользователя на Сервере администрирования. Но при получении устройством любого сертификата оно будет привязано к пользователю, которому был назначен соответствующий сертификат через средства Сервера администрирования.

При подключении устройства к Серверу администрирования будет использована односторонняя SSL-аутентификация, при которой только Сервер администрирования аутентифицируется с помощью сертификата. После получения устройством пользовательского сертификата тип аутентификации будет изменен на двустороннюю (взаимную) SSL-аутентификацию.

Схема подключения KES-устройств к Серверу с использованием принудительного делегирования Kerberos Constrained Delegation (KCD)

Схема подключения KES-устройств к Серверу администрирования с использованием принудительного делегирования Kerberos Constrained Delegation (KCD) предполагает:

- интеграцию с Microsoft Forefront Threat Management Gateway (TMG);

- использование принудительного делегирования Kerberos Constrained Delegation (далее – KCD) для аутентификации мобильных устройств;

- интеграцию с инфраструктурой открытых ключей (Public Key Infrastructure, далее – PKI) для применения пользовательских сертификатов.

При использовании этой схемы подключения следует учесть следующее:

- В качестве типа подключения KES-устройств к TMG следует выбрать двустороннюю аутентификацию SSL, то есть устройство должно подключаться к TMG по своему пользовательскому сертификату. Для этого в установленный на устройстве пакет установки Kaspersky Endpoint Security для Android необходимо интегрировать пользовательский сертификат. Этот KES-пакет создается Сервером администрирования специально для данного устройства (пользователя).

- Вместо сертификата сервера, используемого по умолчанию, для мобильного протокола следует указать особый (персонализированный) сертификат:

  1. В окне свойств Сервера администрирования в разделе **Параметры** установите флажок **Открыть порт для мобильных устройств** и в раскрывающемся списке выберите **Добавить сертификат**.

  2. В открывшемся окне укажите тот же сертификат, что задан на TMG при публикации точки доступа к мобильному протоколу на Сервере администрирования.

- Пользовательские сертификаты для KES-устройств должны быть выпущены доменным Центром сертификации (ЦС). Следует учесть, что если в домене несколько корневых ЦС, то пользовательские сертификаты должны быть выписаны тем Центром сертификации, который указан в публикации на TMG.

  Обеспечить соответствие пользовательского сертификата заявленному выше требованию возможно несколькими способами:

  - Указать особый пользовательский сертификат в мастере создания пакета установки и в мастере установки сертификатов.

  - Интегрировать Сервер администрирования с доменной инфраструктурой открытых ключей и настроить соответствующий параметр в правилах выпуска сертификатов:

    1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Сертификаты**.

    2. В рабочей области папки **Сертификаты** нажмите на кнопку **Настроить правила выпуска сертификатов**, чтобы открыть окно **Правила выпуска сертификатов**.

    3. В разделе **Интеграция с инфраструктурой открытых ключей** настройте интеграцию с инфраструктурой открытых ключей.

    4. В разделе **Выдача мобильных сертификатов** укажите источник сертификатов.

Рассмотрим пример настройки принудительного делегирования KCD со следующими допущениями:

- точка доступа к мобильному протоколу на Сервере администрирования настроена на порте 13292;

- имя устройства с TMG – tmg.mydom.local;

- имя устройства с Сервером администрирования – ksc.mydom.local;

- имя внешней публикации точки доступа к мобильному протоколу – kes4mob.mydom.global.

Доменная учетная запись для Сервера администрирования

Необходимо создать доменную учетную запись (например, KSCMobileSrvcUsr), под которой будет работать служба Сервера администрирования. Указать учетную запись для службы Сервера администрирования можно при установке Сервера администрирования или с помощью утилиты klsrvswch. Утилита klsrvswch расположена в папке установки Сервера администрирования.

Указать доменную учетную запись необходимо по следующим причинам:

- Управление KES-устройствами – неотъемлемая функция Сервера администрирования.
- Для правильной работы принудительного делегирования Kerberos Constrained Delegation (KCD) принимающая сторона (то есть Сервер администрирования) должна работать под доменной учетной записью.

Имя субъекта-службы (SPN) для http/kes4mob.mydom.local

В домене под учетной записью KSCMobileSrvcUsr требуется прописать SPN для публикации службы мобильного протокола на порте 13292 устройства с Сервером администрирования. Для устройства kes4mob.mydom.local с Сервером администрирования требуется прописать следующее:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Настройка доменных свойств устройства с TMG (tmg.mydom.local)

Для делегирования трафика нужно доверить устройство с TMG (tmg.mydom.local) службе, определенной по SPN (http/kes4mob.mydom.local:13292).

Чтобы доверить устройство с TMG службе, определенной по SPN (http/kes4mob.mydom.local:13292), администратор должен выполнить следующие действия:

1. В оснастке Microsoft Management Console под названием Active Directory Users and Computers (Консоль управления пользователями и компьютерами Active Directory) выбрать устройство с установленным TMG (tmg.mydom.local).
2. В свойствах устройства на закладке **Делегирование** для переключателя **Доверять компьютеру делегирование только указанным службам** выбрать вариант **Использовать любой протокол аутентификации**.
3. В список **Службы, с которыми эта учетная запись может использовать делегированные учетные данные** добавить SPN http/kes4mob.mydom.local:13292.

Особый (персонализированный) сертификат для публикации (kes4mob.mydom.global)

Для публикации мобильного протокола Сервера администрирования требуется выписать особый (персонализированный) сертификат на FQDN kes4mob.mydom.global и указать его вместо сертификата сервера, используемого по умолчанию, в параметрах мобильного протокола Сервера администрирования в Консоли администрирования. Для этого в окне свойств Сервера администрирования в разделе **Параметры** необходимо установить флажок **Открыть порт для мобильных устройств** и в раскрывающемся списке выбрать **Добавить сертификат**.

Следует учесть, что в контейнере с сертификатом сервера (файл с расширением p12 или pfx) должна также присутствовать цепочка корневых сертификатов (открытые ключи).

Настройка публикации на TMG

На TMG для трафика, идущего со стороны мобильного устройства на порт 13292 kes4mob.mydom.global, необходимо настроить KCD на SPN (http/kes4mob.mydom.local:13292) с использованием сертификата сервера, выпущенного для FQND kes4mob.mydom.global. Следует учесть, что к публикации и публикуемой точке доступа (порт 13292 Сервера администрирования) должен быть применен один и тот же сертификат сервера.

Использование Firebase Cloud Messaging

Для своевременной доставки команд на KES-устройства под управлением операционной системы Android в Kaspersky Security Center используется механизм push-нотификаций. Push-нотификации между KES-устройствами и Сервером администрирования осуществляются с помощью сервиса Firebase Cloud Messaging (далее – FCM). В Консоли администрирования Kaspersky Security Center вы можете указать параметры сервиса Cloud Messaging, чтобы подключить KES-устройства к этому сервису.

Для получения параметров Firebase Cloud Messaging вам необходимо иметь учетную запись Google.

Чтобы включить использование FCM, выполните следующие действия:

1. В Консоли администрирования выберите узел **Управление мобильными устройствами** и папку **Мобильные устройства**.
2. В контекстном меню папки **Мобильные устройства** выберите пункт **Свойства**.
3. В окне свойств папки выберите раздел **Параметры Google Firebase Cloud Messaging**.
4. В поле **Идентификатор отправителя** укажите Sender ID FCM.
5. В поле **Файл приватного ключа (в формате JSON)** выберите файл приватного ключа.

   При следующей синхронизации с Сервером администрирования KES-устройства под управлением операционной системы Android будут подключены к службе Firebase Cloud Messaging.

Вы можете изменить параметры Firebase Cloud Messaging по кнопке **Сбросить параметры**.

При переключении на другой проект Firebase работа FCM возобновляется через 10 минут.

Сервис FCM работает на следующих диапазонах адресов:

- Со стороны KES-устройства необходим доступ к портам 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) и 5230 (HTTPS) следующих адресов:
  - google.com;
  - fcm.googleapis.com;
  - android.apis.google.com;
  - все IP-адреса из списка "ASN 15169 Google".

- Со стороны Сервера администрирования необходим доступ к порту 443 (HTTPS) следующих адресов:
  - fcm.googleapis.com;
  - все IP-адреса из списка "ASN 15169 Google".

В случае, если в Консоли администрирования в свойствах Сервера администрирования заданы параметры прокси-сервера (**Дополнительно** / **Параметры доступа к интернету**), они будут использованы для взаимодействия с FCM.

Настройка FCM: получение Sender ID и файла приватного ключа

Чтобы настроить FCM, выполните следующие действия:

1. Зарегистрируйтесь на портале Google.
2. Перейдите в консоль Firebase.
3. Выполните одно из следующих действий:
   - Чтобы создать новый проект, нажмите на кнопку **Create a project** и следуйте инструкциям на экране.
   - Откройте существующий проект.
4. Нажмите на значок шестеренки и выберите **Project settings**.

   Откроется окно **Project settings**.
5. Выберите вкладку **Cloud Messaging**.
6. Скопируйте Sender ID из поля **Sender ID** в разделе **Firebase Cloud Messaging API (V1)**.
7. Выберите вкладку **Service accounts** и нажмите на кнопку **Generate new private key**.
8. В открывшемся окне нажмите на кнопку **Generate key**, чтобы сгенерировать и загрузить файл приватного ключа.

Firebase Cloud Messaging настроен.

Выключение Управления мобильными устройствами

Выключение Управления мобильными устройствами доступно только на главном Сервере администрирования.

Чтобы выключить Управление мобильными устройствами:

1. В дереве консоли выберите папку **Управление мобильными устройствами**.
2. В рабочей области папки перейдите по ссылке **Добавить мобильное устройство iOS**.

   Отобразится окно **Дополнительные компоненты** мастера первоначальной настройки Сервера администрирования.

3. Выберите пункт **Не включать Управление мобильными устройствами**, если вы больше не хотите управлять мобильными устройствами.

4. Нажмите на кнопку **ОК**.

Ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования. Порт подключения мобильных устройств и порт активации мобильных устройств будут закрыты автоматически.

Созданные политики Kaspersky Endpoint Security для Android и Kaspersky Device Management для iOS не будут удалены. Правила выпуска сертификатов не изменяются. Установленные плагины не удаляются. Правило перемещения мобильных устройств не будет удалено.

После повторного включения Управления мобильными устройствами на управляемых мобильных устройствах может потребоваться переустановка мобильных приложений, которые необходимы для управления мобильными устройствами.

Установка Kaspersky Endpoint Security для Android

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

Разрешения

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

На некоторых устройствах (например, HUAWEI, Meizu, Xiaomi) требуется в настройках устройства вручную 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 или выше, либо Android 6-10 (при использовании сервисов Google Play) необходимо выключить системную настройку **Удалять 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 (получение данных о статусе телефона)	Идентификация устройства с помощью IMEI (для Android 5–9; для Android 10 или выше в режиме device owner; для Android 10–11 в рабочем профиле)
	Контроль соответствия – проверка, была ли заменена или извлечена SIM-карта устройства
Память (обязательно)	Защита от вредоносного ПО

Доступ на управление всеми файлами (для Android 11 или выше)	Защита от вредоносного ПО
Устройства Bluetooth поблизости (для Android 12 или выше)	Ограничение использования Bluetooth На некоторых устройствах Xiaomi и HUAWEI под управлением Android 12 Kaspersky Endpoint Security для Android не запрашивает у пользователя разрешение "**Устройства Bluetooth поблизости**". Проблема связана с особенностями прошивки MIUI на Xiaomi и прошивки EMUI на HUAWEI. Несмотря на отсутствие запроса на это разрешение, все функции, связанные с использованием Bluetooth, корректно работают на этих устройствах.
Игнорировать оптимизацию батареи (для Android 12 или выше)	Контроль приложений
	Веб-Фильтр
	Анти-Вор
Уведомления (для Android 13)	Уведомление пользователя о проблемах безопасности и событиях приложения
Разрешение на работу в фоновом режиме (для Android 12 или выше)	Обеспечение непрерывной работы приложения. Если разрешение не предоставлено, приложение может быть выгружено из памяти и не сможет перезапуститься.
Администратор устройства (обязательно)	Анти-Вор – блокировка устройства (только для Android 5.0–6)
	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 или выше необходимо при появлении запроса предоставить разрешение "При использовании приложения".
Местоположение	Анти-Вор – определение местоположения устройства На устройствах с операционной системой Android 10 или выше необходимо при появлении запроса предоставить разрешение "Всегда".
Специальные возможности	Анти-Вор – блокировка устройства (только для Android 7.0 или выше)
	Веб-Фильтр
	Контроль приложений
	Защита приложения от удаления (только для Android 7.0 или выше)

	Отображение предупреждений Kaspersky Endpoint Security для Android (только для Android 10 или выше)
	Ограничение использования камеры (только для Android 11 или выше)
Отображать всплывающее окно (на некоторых устройствах Xiaomi)	Веб-Фильтр
Отображать всплывающие окна при работе в фоновом режиме (на некоторых устройствах Xiaomi)	Веб-Фильтр
Работа в фоновом режиме (для устройств Xiaomi с прошивкой MIUI под управлением Android 11 или ниже)	Контроль приложений
	Веб-Фильтр
	Анти-Вор

Установка Kaspersky Endpoint Security для Android на персональные устройства

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.

Приложение Kaspersky Endpoint Security для Android в настоящее время недоступно в Google Play. Вы можете установить Kaspersky Endpoint Security для Android вручную из RuStore.

Установить Kaspersky Endpoint Security для Android через Kaspersky Security Center можно одним из следующих способов.

- **Загрузить приложение из Google Play**

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.

Приложение Kaspersky Endpoint Security для Android в настоящее время недоступно в Google Play.

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.

- **Загрузить пакет установки из Kaspersky Security Center**

Инсталляционный пакет приложения будет загружен с сервера Kaspersky Security Center. Приложение также будет обновляться через Kaspersky Security Center с помощью настроек политики. Этот способ можно также использовать, если мобильные устройства в вашей компании работают без подключения к интернету.

Чтобы использовать этот способ, выполните предварительную настройку, которая включает следующие шаги:

1. Создайте и настройте инсталляционный пакет приложения.
2. Создайте автономный инсталляционный пакет.

Если для развертывания приложения используется инсталляционный пакет из Kaspersky Security Center, после сброса настроек устройства до заводских и сканирования QR-кода на экране устройства может появиться сообщение **Заблокировано Play Защитой**. Это связано с тем, что сертификат подписи пакета установки отличается от указанного в Google Play. Для продолжения установки необходимо нажать кнопку **Все равно установить**. При нажатии кнопки **OK** процесс установки будет прерван, а настройки устройства будут сброшены до заводских.

Чтобы установить Kaspersky Endpoint Security для Android с помощью Kaspersky Security Center на персональные устройства, 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 один из двух вариантов:

   - **Загрузить приложение из Google Play**

   - **Загрузить пакет установки из Kaspersky Security Center**, если не удается загрузить приложение из Google Play или если вам нужна определенная версия приложения (например, для использования в режиме device owner)

6. На странице **Выбор пользователей, мобильными устройствами которых вы хотите управлять** 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 пользователя** выберите способ передачи QR-кода для установки приложения:

   - Выберите **Показать QR-код в мастере** и отсканируйте QR-код с помощью камеры мобильного устройства, на которое будет установлено приложение.

   - Выберите **Отправить QR-код пользователю** и отправьте QR-код с соответствующей ссылкой на электронные адреса выбранных пользователей из вашей организации. Чтобы установить приложение, пользователь должен отсканировать QR-код с помощью камеры мобильного устройства или открыть ссылку на инсталляционный пакет.

     Если вы выбрали этот способ, укажите следующие параметры в блоке **По электронной почте**:

     a. Установите флажок **Адреса электронной почты пользователя**. В раскрывающемся списке выберите один из следующих вариантов:

        - **Все адреса электронной почты**

- **Основная электронная почта**
- **Дополнительная электронная почта**

Эти электронные адреса должны быть указаны в параметрах учетных записей пользователей в Kaspersky Security Center.

b. Если вы хотите отправить QR-код на электронную почту, не указанную в параметрах учетной записи в Kaspersky Security Center, установите флажок **Другая электронная почта**, а затем укажите нужный адрес.

c. Нажмите на кнопку **Изменить сообщение**, чтобы изменить тему и текст письма.

Если вы установили флажок **Запрашивать пароль при установке сертификата** в разделе **Выпуск мобильных сертификатов**, добавьте макрос %PASS% в текст письма, чтобы отправить пароль пользователю. В противном случае появится предупреждение и письмо не отправится.

Нажмите на кнопку **Далее**, чтобы отправить сгенерированное письмо.

9. Страница **Результат** отображает указанную вами информацию. Отсканируйте QR-код, если вы выбрали способ **Показать QR-код в мастере** на предыдущей странице.

10. 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.

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.

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 следующими способами:

- **Загрузить приложение с веб-сайта "Лаборатории Касперского"**

Выберите этот способ для мобильных устройств, которые имеют доступ в интернет, чтобы загрузить установочный файл APK с сайта "Лаборатории Касперского". Затем приложение будет обновляться с помощью HUAWEI AppGallery, Samsung Galaxy Store, RuStore или Xiaomi GetApps.

- **Загрузить пакет установки из Kaspersky Security Center**

  Инсталляционный пакет приложения будет загружен с сервера Kaspersky Security Center. Приложение также будет обновляться через Kaspersky Security Center с помощью настроек политики. Этот способ можно также использовать, если мобильные устройства в вашей компании работают без подключения к интернету.

  Чтобы использовать этот способ, перед генерацией QR-кода выполните следующие шаги:

  1. Создайте и настройте инсталляционный пакет приложения.
  2. Создайте автономный инсталляционный пакет.

  Если для развертывания приложения используется инсталляционный пакет из Kaspersky Security Center, после сброса настроек устройства до заводских и сканирования QR-кода на экране устройства может появиться сообщение **Заблокировано Play Защитой**. Это связано с тем, что сертификат подписи пакета установки отличается от указанного в Google Play. Для продолжения установки необходимо нажать кнопку **Все равно установить**. При нажатии кнопки **OK** процесс установки будет прерван, а настройки устройства будут сброшены до заводских.

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 **Сеть для загрузки Kaspersky Endpoint Security** выберите один из следующих вариантов:

   - **Предложить пользователю выбрать сеть Wi-Fi на устройстве**

     В этом случае пользователю будет предложено подключиться к любой доступной сети Wi-Fi для загрузки приложения.

     Этот параметр выбран по умолчанию.

   - **Использовать только указанную сеть Wi-Fi (Android 9 или выше)**

     В этом случае устройство попытается автоматически подключиться к указанной вами сети. Эта возможность поддерживается на устройствах с Android версии 9 и выше.

     Необходимо правильно ввести все параметры сети. Если какой-либо параметр указан неверно или сеть недоступна, процесс установки будет прерван, а настройки устройства будут сброшены до заводских.

Для настройки подключения к нужной сети Wi-Fi нажмите на кнопку **Задать сеть**. В окне **Сеть Wi-Fi для загрузки Kaspersky Endpoint Security** укажите следующие параметры:

- **Идентификатор сети SSID**

  Определяет имя беспроводной сети, содержащей точку доступа (SSID). Имя беспроводной сети должно состоять не более чем из 32 символов.

- **Скрытая сеть**

  Определяет, будет ли выбранная сеть транслировать свой SSID.

  По умолчанию флажок снят.

- **Защита сети**

  Определяет тип защиты беспроводной сети. Возможные значения:

  - **Открытая** - При выборе сеть не будет защищена (по умолчанию).
  - **WEP (Android 9 или ниже)** - При выборе сеть защищается по протоколу WEP. Этот параметр требует ввода пароля для доступа к сети и применяется только для Android 9 или ниже.
  - **WPA2 PSK** - При выборе сеть защищается по протоколу безопасности WPA2 PSK. Этот параметр требует ввода пароля для доступа к сети.

- **Пароль (передается в незашифрованном виде)**

  Определяет пароль для доступа к беспроводной сети, защищенной по протоколу WEP или WPA2 PSK. Пароль передается с QR-кодом.

  Не используйте пароль от конфиденциальной сети Wi-Fi. Пароль передается пользователю в открытом виде вместе с другими данными, необходимыми для настройки устройства.

- **Не использовать прокси-сервер**

  Прокси-сервер не используется (по умолчанию).

- **Использовать прокси-сервер**

  Прокси-сервер используется. Если выбран этот параметр, необходимо указать адрес и порт прокси-сервера. Также можно указать список сайтов, для которых прокси будет игнорироваться.

- **Адрес прокси-сервера**

  Определяет IP-адрес или символьное имя (веб-адрес) прокси-сервера. Максимальное количество символов – 256.

- **Порт прокси-сервера**

  Номер порта прокси-сервера. Значение должно быть в диапазоне от 0 до 65 536.

- **Не использовать прокси-сервер для адресов**

  Определяет адреса веб-сайтов, для которых не нужно использовать прокси-сервер.

  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.

- **URL PAC-файла**

  URL-адрес PAC-файла (proxy auto-configuration) для сети Wi-Fi.

- **Использовать мобильную сеть (Android 8.0 или выше)**

  В этом случае устройство попытается подключиться к мобильной сети для загрузки программы. Если в устройстве не установлена SIM-карта или мобильная сеть недоступна, пользователю будет предложено выбрать доступную сеть Wi-Fi.

  Эта возможность поддерживается на устройствах с Android версии 7.0 и выше.

6. В разделе **Дополнительно** установите флажок **Включить все системные приложения**, если вы хотите, чтобы системные приложения на устройстве были включены. Если флажок снят, все системные приложения отключены.

7. 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.

8. На странице **Способ установки Kaspersky Endpoint Security для Android в режиме device owner** выберите способ установки:

   - **Загрузить приложение с веб-сайта "Лаборатории Касперского"**

   - **Загрузить пакет установки из 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**.

9. На странице **Выбор пользователей, мобильными устройствами которых вы хотите управлять** 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.

10. 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.

11. На странице **Способ уведомления пользователя** выберите способ передачи QR-кода для установки приложения:

    - Выберите **Показать QR-код в мастере** и отсканируйте QR-код с помощью камеры мобильного устройства, на которое будет установлено приложение.

    - Выберите **Отправить QR-код пользователю** и отправьте QR-код с соответствующей ссылкой на электронные адреса выбранных пользователей из вашей организации. Чтобы установить приложение, пользователь должен отсканировать QR-код с помощью камеры мобильного устройства или открыть ссылку на инсталляционный пакет.

      Если вы выбрали этот способ, укажите следующие параметры в блоке **По электронной почте**:

      a. Установите флажок **Адреса электронной почты пользователя**. В раскрывающемся списке выберите один из следующих вариантов:

         - **Все адреса электронной почты**

         - **Основная электронная почта**

         - **Дополнительная электронная почта**

         Эти электронные адреса должны быть указаны в параметрах учетных записей пользователей в Kaspersky Security Center.

      b. Если вы хотите отправить QR-код на электронную почту, не указанную в параметрах учетной записи в Kaspersky Security Center, установите флажок **Другая электронная почта**, а затем укажите нужный адрес.

      c. Нажмите на кнопку **Изменить сообщение**, чтобы изменить тему и текст письма.

         Если вы установили флажок **Запрашивать пароль при установке сертификата** в разделе **Выпуск мобильных сертификатов**, добавьте макрос %PASS% в текст письма, чтобы отправить пароль пользователю. В противном случае появится предупреждение и письмо не отправится.

      Нажмите на кнопку **Далее**, чтобы отправить сгенерированное письмо.

12. Страница **Результат** отображает указанную вами информацию. Отсканируйте QR-код, если вы выбрали способ **Показать QR-код в мастере** на предыдущей странице.

13. 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.

Установка Kaspersky Endpoint Security для Android в режиме device owner в закрытой сети

При развертывании Kaspersky Endpoint Security для Android в режиме device owner с помощью QR-кода на устройствах с предустановленными Google Mobile Services (GMS) проверяется их подключение к определенным конечным точкам Google через сети Wi-Fi. Если сеть Wi-Fi не имеет доступа к интернету, проверить подключение не удается и развертывание завершается с ошибкой.

Чтобы избежать проверки подключения, вы можете развернуть приложение Kaspersky Endpoint Security для Android в режиме device owner в закрытой сети с помощью файла PAC (Proxy Auto-Configuration).

Чтобы использовать PAC-файл для развертывания приложения Kaspersky Endpoint Security для Android:

1. Создайте PAC-файл (например, proxy.pac) со следующим содержанием:
   ```
   function FindProxyForURL (url, host) {
    return "DIRECT";
   }
   ```

2. Опубликуйте созданный PAC-файл на ресурсе, который будет доступен в закрытой сети (например, на веб-сервере IIS).

   Сохраните ссылку на PAC-файл (например, https://intranet.mycompany.com/files/proxy.pac).

3. Убедитесь, что APK-файл развертываемого приложения Kaspersky Endpoint Security для Android доступен в закрытой сети. Для этого воспользуйтесь одним из следующих способов:

   - Загрузите инсталляционный пакет приложения с сервера Kaspersky Security Center. Если сервер доступен, на нем будут доступны инсталляционные пакеты.

   - Скачайте инсталляционный APK-файл с сайта Kaspersky и загрузите его в закрытую сеть.

     Выберите в качестве источника общую версию приложения.

4. Сгенерируйте QR-код для установки приложения в режиме device owner и отправьте его пользователю, следуя инструкциям мастера подключения нового мобильного устройства.

   При подключении устройства к Kaspersky Security Center вам будет предложено указать сеть для загрузки приложения Kaspersky Endpoint Security для Android. На этом шаге настройте использование ранее созданного PAC-файла для сетевого подключения, связав его с настройками сети Wi-Fi на устройстве. Для этого воспользуйтесь одним из следующих способов:

   - В разделе **Сеть для загрузки Kaspersky Endpoint Security для Android** выберите **Предлагать пользователю выбрать сеть Wi-Fi на устройстве**. При развертывании приложения пользователю необходимо указать ссылку на PAC-файл (шаг 2) в настройках сети при выборе сети Wi-Fi на устройстве. После установки соединения пользователь сможет продолжить настройку устройства и активировать приложение, следуя инструкциям мастера первоначальной настройки приложения.

- В разделе **Сеть для загрузки Kaspersky Endpoint Security для Android** выберите **Использовать только заданную сеть Wi-Fi (Android 9 или выше)**, нажмите на кнопку **Задать сеть**, вставьте ссылку на ранее созданный PAC-файл (шаг 2) в поле **URL PAC-файла** и нажмите на кнопку **OK**.

Если инсталляционный APK-файл был загружен с сайта Kaspersky (шаг 3), вам необходимо изменить ссылку в QR-коде, указав адрес закрытой сети.

Дополнительная информация о настройке Kaspersky Endpoint Security для Android в режиме device owner приведена в разделе Установка приложения в режиме device owner.

Если для развертывания приложения используется инсталляционный пакет из Kaspersky Security Center, после сброса настроек устройства до заводских и сканирования QR-кода на экране устройства может появиться сообщение **Заблокировано Play Защитой**. Это связано с тем, что сертификат подписи пакета установки отличается от указанного в Google Play. Для продолжения установки необходимо нажать кнопку **Все равно установить**. При нажатии кнопки **OK** процесс установки будет прерван, а настройки устройства будут сброшены до заводских.

Приложение Kaspersky Endpoint Security для Android будет установлено на устройстве в режиме device owner в закрытой сети.

Другие способы установки Kaspersky Endpoint Security для Android

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

Установка Kaspersky Endpoint Security для Android вручную

Вы можете вручную установить Kaspersky Endpoint Security для Android с сайта "Лаборатории Касперского", HUAWEI AppGallery, Samsung Galaxy Store, RuStore или Xiaomi GetApps.

Установка приложения

Чтобы установить приложение из магазина приложений, выполните стандартную процедуру установки для платформы Android.

Чтобы установить Kaspersky Endpoint Security для Android с сайта "Лаборатории Касперского":

1. Перейдите на сайт "Лаборатории Касперского".
2. Найдите Kaspersky Security для мобильных устройств на сайте.
3. Нажмите **Показать версии для загрузки**.
4. Выберите версию приложения и нажмите **Скачать**.
5. Откройте загруженный файл APK и следуйте инструкциям на экране.

Вам может понадобиться разрешить браузеру установку приложений из сторонних источников, отличных от Google Play, в разделе настроек устройства **Приложения → Специальный доступ → Установка неизвестных приложений**. Расположение этих настроек может отличаться на устройствах разных производителей.

Приложение будет установлено на устройство.

Настройка приложения

После установки Kaspersky Endpoint Security для Android нужно вручную настроить приложение. Процедура настройки зависит от того, отправил ли вам администратор адрес сервера или ссылку для скачивания приложения.

Чтобы настроить Kaspersky Endpoint Security для Android с использованием ссылки для скачивания приложения:

1. Откройте Kaspersky Endpoint Security для Android.
2. Прочитайте Лицензионное соглашение. Если вы принимаете Лицензионное соглашение, установите соответствующий флажок и нажмите **Продолжить**.
3. Нажмите **Продолжить** и предоставьте приложению необходимые разрешения.
4. В поле **Сервер** укажите ссылку, которую вы получили от администратора.
5. Нажмите **Продолжить**.

Приложение Kaspersky Endpoint Security для Android настроено.

Чтобы настроить Kaspersky Endpoint Security для Android с использованием адреса сервера:

1. Откройте Kaspersky Endpoint Security для Android.
2. Прочитайте Лицензионное соглашение. Если вы принимаете Лицензионное соглашение, установите соответствующий флажок и нажмите **Продолжить**.
3. Нажмите **Продолжить** и предоставьте приложению необходимые разрешения.
4. В поле **Сервер** укажите адрес Сервера администрирования, предоставленный администратором.
5. Нажмите **Продолжить**.
6. Нажмите **Включить**, чтобы включить приложение в качестве администратора устройства.
7. Нажмите **Разрешить** и предоставьте приложению необходимые разрешения.

Приложение Kaspersky Endpoint Security для Android настроено.

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

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 далее указаниям мастера.
3. На странице **Выбор типа инсталляционного пакета** нажмите на кнопку **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.
4. На странице **Определение имени инсталляционного пакета** введите имя инсталляционного пакета для отображения в рабочей области папки **Инсталляционные пакеты**.
5. На странице **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.

   > Если вы создадите инсталляционный пакет с архивом `sc_package.exe` в Kaspersky Security Center версии ниже 14.2, Kaspersky Endpoint Security для Android не удастся установить на устройствах под управлением Android 10 и выше. Чтобы избежать этой проблемы, обновитесь до Kaspersky Security Center 14.2 или обратитесь в Службу технической поддержки для получения соответствующей версии архива.
6. На странице **Принять 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 → Обнаружение устройств → Домены**.
   - В блоке **Действия при установке** установите флажок **Запрашивать адрес электронной почты**, чтобы при первом запуске приложение запрашивало у пользователя его адрес корпоративной электронной почты.

     Адрес электронной почты пользователя используется для формирования имени мобильных устройств при добавлении их в группу администрирования.
4. Чтобы применить указанные параметры, нажмите на кнопку **Применить**.

Создание автономного пакета установки

Чтобы создать автономный пакет установки, выполните следующие действия:

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

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 **Мастер создания автономного инсталляционного пакета** установите флажок **Открыть список автономных пакетов**.

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

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

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

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

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

Настройка параметров синхронизации

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

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

- **Принудительно**. Принудительная синхронизация выполняется с помощью push-уведомлений сервиса FCM (Firebase Cloud Messaging). Принудительная синхронизация, в первую очередь, предназначена для своевременной доставки команд на мобильное устройство. Это может быть полезно, если устройство находится в режиме экономии заряда батареи, поскольку в этом случае приложение может выполнять задачи позже, чем указано. Если вы хотите использовать принудительную синхронизацию, убедитесь что параметры FCM в Kaspersky Security Center настроены.

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.

   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 **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. Чтобы получать историю местоположений устройства, установите флажок **Отправлять историю местоположений устройства при синхронизации** в блоке **История местоположений устройства**. История местоположений будет отправляться на Сервер администрирования при каждой синхронизации.

   Функциональность должна использоваться в соответствии с требованиями локального законодательства, с уведомлением или согласием (в зависимости от требований законодательства) лица, использующего устройство, о включении на устройстве функциональности отслеживания местоположения.

   Включение этой настройки и задание геозоны приведет к увеличению энергопотребления устройства.

   Этот параметр работает только в том случае, если тип информационного события **История местоположения устройства** хранится в базе данных Сервера администрирования. События настраиваются в разделе **События** свойств политики. Дополнительная информация приведена в справке Kaspersky Security Center.
9. В раскрывающемся списке **Частота определения местоположений устройства** укажите частоту получения местоположения устройства По умолчанию указано значение **Каждые 15 минут**.

Из-за технических ограничений Android-устройств фактическое определение местоположения устройства может происходить реже, чем указано.

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

Параметры на мобильном устройстве будут изменены 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 разделе Отправка команд.

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.

В течение 15 минут выполните следующие действия. По истечении этого времени при сохранении изменений политики может возникнуть ошибка.

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 ключа, размещенного в хранилище Kaspersky Security Center, Kaspersky Secure Mobility Management заменит его 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 изменены после очередной синхронизации устройства с Kaspersky Security Center.

Установка iOS MDM-профиля

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

Прежде чем приступить к развертыванию профиля iOS MDM, необходимо развернуть систему управления мобильными устройствами.

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

О режимах управления iOS-устройствами

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

Неконтролируемые устройства

Неконтролируемые iOS-устройства – 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.

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. На странице **Выбор Сервера iOS MDM** выберите из списка Сервер iOS MDM.
5. На странице **Выбор пользователей, мобильными устройствами которых вы хотите управлять** выберите одного или несколько пользователей для установки iOS MDM-профиля на их мобильные устройства.

   Если пользователя нет в списке, можно добавить новую учетную запись, не выходя из мастера подключения нового мобильного устройства.
6. На странице **Источник сертификата** выберите источник сертификата для защиты обмена данными между 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. На странице **Способ уведомления пользователя** выберите способ передачи QR-кода для установки iOS MDM-профиля:

   - Выберите **Показать QR-код в мастере** и отсканируйте QR-код с помощью камеры мобильного устройства, на которое будет установлен профиль.
   - Выберите **Отправить QR-код пользователю** и отправьте QR-код с соответствующей ссылкой на электронные адреса выбранных пользователей из вашей организации. Чтобы установить iOS MDM-

профиль, пользователь должен отсканировать QR-код с помощью камеры мобильного устройства или открыть ссылку на профиль.

Если вы выбрали этот способ, укажите следующие параметры в блоке **По электронной почте**:

a. Установите флажок **Адреса электронной почты пользователя**. В раскрывающемся списке выберите один из следующих вариантов:

- **Все адреса электронной почты**
- **Основная электронная почта**
- **Дополнительная электронная почта**

> Эти электронные адреса должны быть указаны в параметрах учетных записей пользователей в Kaspersky Security Center.

b. Если вы хотите отправить QR-код на электронную почту, не указанную в параметрах учетной записи в Kaspersky Security Center, установите флажок **Другая электронная почта**, а затем укажите нужный адрес.

c. Нажмите на кнопку **Изменить сообщение**, чтобы изменить тему и текст письма.

> Если вы установили флажок **Запрашивать пароль при установке сертификата** в разделе **Выпуск мобильных сертификатов**, добавьте макрос %PASS% в текст письма, чтобы отправить пароль пользователю. В противном случае появится предупреждение и письмо не отправится.

Нажмите на кнопку **Далее**, чтобы отправить сгенерированное письмо.

8. Страница **Результат** отображает указанную вами информацию. Отсканируйте QR-код, если вы выбрали способ **Показать QR-код в мастере** на предыдущей странице.

9. Завершите работу мастера подключения нового мобильного устройства.

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

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

Установка плагинов управления

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

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

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

Чтобы убедиться, что плагины управления установлены:

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

Откроется список установленных плагинов управления.

Обновление предыдущей версии программы

Обновление программы должно выполняться с учетом следующих требований:

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

  Номера сборок версий плагина управления и мобильного приложения можно посмотреть в заметках о выпуске Kaspersky Secure Mobility Management.

- Убедитесь, что Kaspersky Security Center соответствует программным требованиям Kaspersky Secure Mobility Management.

- Плагины управления Kaspersky Endpoint Security для Android 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 предоставления технической поддержки для различных версий Kaspersky Secure Mobility Management см. на *веб-сайте технической поддержки "Лаборатории 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 с сайта "Лаборатории Касперского", вы можете посмотреть номер сборки в настройках приложения (**Настройки** → **О приложении**).

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в решении на территории США.

Обновление предыдущей версии Kaspersky Endpoint Security для Android

Kaspersky Endpoint Security для Android можно обновить следующими способами:

- С помощью сайта "Лаборатории Касперского". Пользователь мобильного устройства загружает с сайта "Лаборатории Касперского" новую версию приложения и устанавливает ее на свое устройство.
- С помощью HUAWEI AppGallery, Samsung Galaxy Store, RuStore или Xiaomi GetApps. Пользователь мобильного устройства загружает новую версию приложения из магазина приложений и устанавливает ее на свое устройство, выполнив стандартную процедуру обновления для платформы Android.

  Чтобы обновить приложение в Samsung Galaxy Store, у пользователя устройства должна быть учетная запись Samsung Account.

- 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 приложения с сайта "Лаборатории Касперского"

Чтобы обновить приложение с сайта "Лаборатории Касперского":

1. Перейдите на сайт "Лаборатории Касперского".
2. Найдите Kaspersky Security для мобильных устройств на сайте.
3. Нажмите **Показать версии для загрузки**.
4. Выберите версию приложения и нажмите **Скачать**.
5. Откройте загруженный файл APK и следуйте инструкциям на экране.

Приложение Kaspersky Endpoint Security для Android будет обновлено.

После загрузки приложения, 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 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.

   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 **Дополнительно**.
5. В блоке **Обновление приложения Kaspersky Endpoint Security для Android** нажмите на кнопку **Выбрать**.

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

   Вы можете обновить Kaspersky Endpoint Security для Android только до более новой версии. Обновить Kaspersky Endpoint Security для Android до более старой версии невозможно.

7. Нажмите на 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 изменены после очередной синхронизации устройства с Kaspersky Security Center. Пользователю мобильного устройства будет предложено установить новую версию приложения. После получения согласия новая версия приложения будет установлена на мобильное устройство.

Установка более ранней версии Kaspersky Endpoint Security для Android

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".

Подробную информацию о более ранних версиях Kaspersky Endpoint Security для Android см. в *справке для соответствующей версии Kaspersky Secure Mobility Management*.

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.

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 приложения со страницы Kaspersky Secure Mobility Management и запустить мастер установки каждого из плагинов. Предыдущие версии плагинов будут автоматически удалены во время работы мастера установки.

Мы рекомендуем использовать одинаковую версию приложения и плагинов 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 Secure Mobility Management, появятся в существующих политиках и будут иметь значения по умолчанию.

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

Обновление из списка в Консоли администрирования

Чтобы обновить плагины управления, выполните следующие действия:

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

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

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

Обновление из дистрибутива

Чтобы обновить плагин управления Kaspersky Endpoint Security для Android,

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

Установка выполняется с помощью мастера и не требует настройки параметров.

Чтобы обновить плагин управления Kaspersky Device Management для iOS,

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

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

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

Удаление Kaspersky Endpoint Security для Android

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

1. Удаление приложения пользователем

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

2. Удаление приложения администратором.

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

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.

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.

   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 **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 **Программы → Kaspersky Endpoint Security для мобильных устройств**.
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.

Разрешение пользователям удалять приложение

На устройствах под управлением операционной системы Android версии 7 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.

   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 **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 **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.

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.

Настройка и управление

Этот раздел справки адресован специалистам, которые осуществляют администрирование Kaspersky Secure Mobility Management, и специалистам технической поддержки организаций, использующих Kaspersky Secure Mobility Management.

Начало работы

В этом разделе описаны действия, которые рекомендуется выполнить в начале работы с Kaspersky Secure Mobility Management.

Запуск и остановка программы

Kaspersky Security Center автоматически запускает и останавливает плагины управления Kaspersky Endpoint Security для Android 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, для запуска антивирусной проверки по расписанию или синхронизации устройства с Kaspersky Security Center. Проблема связана с особенностями встроенного программного обеспечения этих устройств.

Создание группы администрирования

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

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

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

Чтобы создать группу администрирования, выполните следующие действия:

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

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

Групповые политики для управления мобильными устройствами

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

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

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

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

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

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

- **Высокий уровень защиты** – защита устройств обеспечена на должном уровне. Все компоненты защиты работают в соответствии с параметрами, рекомендуемыми специалистами "Лаборатории Касперского".
- **Средний уровень защиты** – уровень защиты снижен. Некоторые важные компоненты защиты выключены (например, Веб-Фильтр). Важные проблемы отмечены знаком .

- **Низкий уровень защиты** – существуют проблемы, которые могут привести к заражению устройства и потере данных. Некоторые критические компоненты защиты выключены (например, выключена постоянная защита устройств). Критические проблемы отмечены знаком ●.

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

Создание групповой политики

В этом разделе описано создание групповых политик для устройств, на которых установлено мобильное приложение Kaspersky Endpoint Security для Android, а также 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 **Новая политика** 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.

Настройка параметров синхронизации

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

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

- **Принудительно**. Принудительная синхронизация выполняется с помощью push-уведомлений сервиса FCM (Firebase Cloud Messaging). Принудительная синхронизация, в первую очередь, предназначена для своевременной доставки команд на мобильное устройство. Это может быть полезно, если устройство находится в режиме экономии заряда батареи, поскольку в этом случае приложение может выполнять задачи позже, чем указано. Если вы хотите использовать принудительную синхронизацию, убедитесь что параметры FCM в Kaspersky Security Center настроены.

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.

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 **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. Чтобы получать историю местоположений устройства, установите флажок **Отправлять историю местоположений устройства при синхронизации** в блоке **История местоположений устройства**. История местоположений будет отправляться на Сервер администрирования при каждой синхронизации.

   Функциональность должна использоваться в соответствии с требованиями локального законодательства, с уведомлением или согласием (в зависимости от требований законодательства) лица, использующего устройство, о включении на устройстве функциональности отслеживания местоположения.

   Включение этой настройки и задание геозоны приведет к увеличению энергопотребления устройства.

   Этот параметр работает только в том случае, если тип информационного события **История местоположения устройства** хранится в базе данных Сервера администрирования. События настраиваются в разделе **События** свойств политики. Дополнительная информация приведена в справке Kaspersky Security Center.

9. В раскрывающемся списке **Частота определения местоположений устройства** укажите частоту получения местоположения устройства По умолчанию указано значение **Каждые 15 минут**.

   Из-за технических ограничений Android-устройств фактическое определение местоположения устройства может происходить реже, чем указано.

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

Параметры на мобильном устройстве будут изменены 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 разделе Отправка команд.

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.

   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 **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.

Удаление групповой политики

Чтобы удалить групповую политику, выполните следующие действия:

1. В дереве консоли выберите группу администрирования, для которой нужно удалить политику.

2. В рабочей области группы администрирования на закладке **Политики** выберите политику, которую вы хотите удалить.

3. В контекстном меню политики выберите пункт **Удалить**.

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

Ограничение прав на настройку групповых политик

Администраторы Kaspersky Security Center могут настраивать права доступа пользователей Консоли администрирования к различным функциям комплексного решения Kaspersky Secure Mobility Management 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*.

Контроль

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

Настройка ограничений

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

Особые рекомендации для устройств под управлением Android 10 или 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 или ниже до Android 10 или выше, или при обновлении приложения Kaspersky Endpoint Security, установленного на устройстве под управлением Android 10 или выше, нельзя изменить или удалить сети, которые были ранее добавлены в Kaspersky Security Center, с помощью политик Kaspersky Security Center. Однако пользователь может изменить или удалить такие сети вручную в настройках устройства.

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

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

- При удалении Kaspersky Endpoint Security с устройства, сети, ранее предлагаемые приложением, игнорируются.

- Не поддерживается запрет на использование сетей Wi-Fi.

Доступ к камере

- На устройствах под управлением Android 10 использование камеры нельзя запретить полностью. Запрет на использование камеры для рабочего профиля по-прежнему доступен.

- Если стороннее приложение пытается получить доступ к камере устройства, это приложение будет заблокировано, а пользователь получит уведомление о проблеме. Однако приложения, использующие камеру во время работы в фоновом режиме, не могут быть заблокированы.

- Когда внешняя камера отключена от устройства, в некоторых случаях может отображаться уведомление о недоступности камеры.

Управление методами разблокировки экрана

- Kaspersky Endpoint Security приводит требования надежности пароля к одному из системных значений: средний или высокий.

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

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

- Управлять использованием отпечатка пальца для разблокировки экрана можно только в рабочем профиле.

Настройка ограничений для Android-устройств

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

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

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

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

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

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

   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 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 личных устройствах и устройствах с созданным рабочим профилем под управлением Android 10 и выше запрет на использование сетей Wi-Fi не поддерживается.

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

  Когда использование камеры запрещено, приложение уведомляет об этом пользователя и сразу же закрывается. На устройствах Asus и OnePlus уведомление выводится на весь экран. Пользователь может нажать на кнопку **Закрыть**, чтобы завершить работу приложения.

  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 изменены после очередной синхронизации устройства с Kaspersky Security Center.

Настройка ограничений для iOS MDM-устройств

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

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

6. Настройте ограничения функций iOS MDM-устройства.

   Список ограничений функций

Отложить обновление операционной системы, в днях (только для supervised, iOS 11.3+)

Позволяет отложить обновления операционной системы на устройстве.

Если флажок установлен, пользователь не может получить доступ к обновлениям в течение указанного периода. По умолчанию установлен период 30 дней. Вы можете указать другой период в поле **Укажите количество дней от 1 до 90**

Если флажок снят, пользователь может устанавливать обновления, как только они становятся доступны.

Настройка доступна для мобильных устройств под управлением iOS версии 11 или более поздней, а также iPad OS версии 13.1 или более поздней.

По умолчанию флажок снят.

Укажите количество дней от 1 до 90

Определяет количество дней, на которое будут отложены обновления операционной системы. По умолчанию установлено значение 30 дней.

Это поле доступно, если установлен флажок **Отложить обновление операционной системы, в днях**.

Разрешить использование камеры

Использование камеры на мобильном устройстве пользователя.

Если флажок установлен, пользователь может использовать камеру устройства.

Если флажок снят, на мобильном устройстве пользователя выключена камера. Пользователь не может делать фотографии, снимать видео и использовать приложение FaceTime. На главном экране устройства значок камеры отсутствует.

По умолчанию флажок установлен.

Разрешить FaceTime (только для supervised)

Использование приложения FaceTime на мобильном устройстве пользователя. Флажок доступен, если на устройстве разрешено использование камеры. Параметр доступен, если установлен флажок **Разрешить использование камеры**.

Если флажок установлен, пользователь может делать и принимать видеозвонки с помощью FaceTime.

Если флажок снят, на мобильном устройстве пользователя выключено приложение FaceTime. Пользователь не может делать видеозвонки, а также получать их.

По умолчанию флажок установлен.

Разрешить снимки и видеозаписи с экрана

Возможность сделать снимок экрана или видеозапись с экрана на iOS MDM-устройстве.

Если флажок установлен, пользователь может делать и сохранять снимки экрана и видеозаписи с экрана на мобильном устройстве.

Если флажок снят, пользователь не может делать и сохранять снимки экрана и видеозаписи с экрана на мобильном устройстве.

По умолчанию флажок установлен.

Разрешить просматривать экраны в "Классе" (только для supervised)

Возможность для преподавателя просматривать экраны iPad студентов с помощью программы "Класс". Подробнее о программе "Класс" см. на *веб-сайте технической поддержки Apple*.

Если флажок установлен, преподаватель может просматривать экраны iPad студентов в программе "Класс".

Если флажок снят, преподаватель не может просматривать экраны iPad студентов в программе "Класс".

По умолчанию флажок установлен.

Разрешить изменять настройки Персональной точки доступа (только для supervised, iOS 12.2+)

Если флажок установлен, пользователь устройства может изменять настройки Персональной точки доступа.

Если флажок снят, пользователь устройства не может изменять настройки Персональной точки доступа.

Настройка доступна для мобильных устройств под управлением iOS версии 12.2 или более поздней, а также iPad OS версии 13.1 или более поздней.

По умолчанию флажок установлен.

Разрешить доступ к USB-устройствам в приложении "Файлы" (только для supervised, iOS 13.1+)

Если флажок установлен, пользователь может получать доступ к USB-устройствам в приложении Файлы.

Если флажок снят, доступ к подключенным USB-устройствам в приложении Файлы заблокирован.

Настройка доступна для мобильных устройств под управлением iOS версии 13.1 или более поздней, а также iPad OS версии 13.1 или более поздней.

По умолчанию флажок установлен.

Включать режим USB Restricted Mode, когда устройство заблокировано (только для supervised, iOS 11.4.1+)

Определяет, включен ли режим USB Restricted Mode, когда устройство заблокировано.

Если флажок установлен, подключение заблокированного устройства к USB-накопителям ограничено с помощью USB Restricted Mode.

Если флажок снят, устройству разрешено подключаться к USB-накопителям, когда оно заблокировано.

Настройка доступна для мобильных устройств под управлением iOS версии 11.4.1 или более поздней, а также iPad OS версии 13.1 или более поздней.

По умолчанию флажок установлен.

Принудительно включать Wi-Fi (только для supervised, iOS 13.0+)

Определяет, должен ли Wi-Fi на управляемом устройстве всегда быть включен. Устройство может подключаться к любой сети Wi-Fi.

Если флажок установлен, Wi-Fi на устройстве всегда включен, даже в авиарежиме. Пользователь не может выключить Wi-Fi в настройках устройства.

Если флажок снят, пользователь может выключить Wi-Fi в настройках устройства.

Настройка доступна для мобильных устройств под управлением iOS версии 13.0 или более поздней, а также iPad OS версии 13.1 или более поздней.

По умолчанию флажок снят.

Принудительно подключаться только к разрешенным сетям Wi-Fi (только для supervised, iOS 14.5+)

Определяет, может ли устройство подключаться только к разрешенным сетям Wi-Fi. Эта функция доступна, если хотя бы одна сеть Wi-Fi добавлена в список сетей Wi-Fi в разделе **Wi-Fi**.

Если флажок установлен, устройство подключается только к разрешенным сетям Wi-Fi. Пользователь не может выключить Wi-Fi в настройках устройства.

Если флажок снят, пользователь может подключиться к любой сети Wi-Fi.

Настройка доступна для мобильных устройств под управлением iOS версии 14.5 или более поздней, а также iPad OS версии 13.1 или более поздней.

По умолчанию флажок снят.

Разрешить создавать конфигурации VPN (только для supervised, iOS 11+)

Если флажок установлен, пользователь может создать конфигурацию VPN на управляемом устройстве.

Если флажок снят, пользователь не может создать конфигурацию VPN на управляемом устройстве.

Настройка доступна для мобильных устройств под управлением iOS версии 11 или более поздней, а также iPad OS версии 13.1 или более поздней.

По умолчанию флажок установлен.

Разрешить AirDrop (только для supervised)

Использование функции AirDrop для передачи данных пользователя с iOS MDM-устройства на другие устройства Apple.

Если флажок установлен, пользователь может использовать AirDrop для передачи данных на другие устройства Apple.

Если флажок снят, пользователю запрещено передавать данные на другие устройства Apple с помощью AirDrop.

По умолчанию флажок установлен.

Разрешить изменение настроек eSIM (только для supervised, iOS 11+)

Установка или снятие флажка определяет, может ли пользователь устройства изменять настройки, связанные с тарифным планом.

Ограничение поддерживается на устройствах с iOS версии 11 и выше.

По умолчанию флажок установлен.

Разрешить iMessage (только для supervised)

Использование службы iMessage на мобильном устройстве пользователя.

Если флажок установлен, пользователь может отправлять и принимать сообщения с помощью службы iMessage.

Если флажок снят, служба iMessage недоступна на мобильном устройстве. Пользователь не может отправлять и получать сообщения iMessage.

По умолчанию флажок установлен.

Разрешить Apple Music (только для supervised)

Прослушивание музыки на мобильном устройстве пользователя с помощью сервиса Apple Music.

Если флажок установлен, пользователь может прослушивать музыку на мобильном устройстве в приложении "Музыка".

Если флажок снят, сервис Apple Music недоступен для пользователя.

По умолчанию флажок установлен.

Разрешить радио в Apple Music (только для supervised)

Прослушивание радио с помощью сервиса Apple Music на мобильном устройстве пользователя.

Если флажок установлен, пользователь может прослушивать радио в приложении "Музыка" на мобильном устройстве.

Если флажок снят, прослушивание радио недоступно для пользователя.

По умолчанию флажок установлен.

Разрешить изменение настроек Bluetooth (только для supervised, iOS 11+)

Если флажок установлен, пользователь может изменять настройки Bluetooth на мобильном устройстве.

Если флажок снят, настройки Bluetooth нельзя изменять на мобильном устройстве.

Настройка доступна для мобильных устройств под управлением iOS версии 11 или более поздней, а также iPad OS версии 13.1 или более поздней.

По умолчанию флажок установлен.

Разрешить использование NFC (только для supervised, iOS 14.2+)

Если флажок установлен, использование NFC разрешено.

Если флажок снят, использование NFC запрещено.

Параметр доступен для мобильных устройств под управлением iOS версии 14.2 и выше.

По умолчанию флажок установлен.

Разрешить голосовой набор на заблокированном устройстве

Использование функции голосового набора на заблокированном мобильном устройстве пользователя.

Если флажок установлен, пользователь может использовать голосовые команды для набора телефонных номеров на заблокированном мобильном устройстве.

Если флажок снят, пользователь не может использовать голосовые команды для набора телефонных номеров на заблокированном мобильном устройстве.

По умолчанию флажок установлен.

Разрешить использование Siri

Использование приложения Siri на мобильном устройстве пользователя.

Если флажок установлен, пользователь может использовать на устройстве голосовые команды приложения Siri.

Если флажок снят, пользователь не может использовать на устройстве голосовые команды Siri.

По умолчанию флажок установлен.

Разрешить фильтр нецензурной лексики (только для supervised)

Фильтрация нецензурной лексики при использовании приложения Siri на мобильном устройстве пользователя.

Если флажок установлен, при использовании Siri фильтруется нецензурная лексика.

Если флажок снят, при использовании Siri нецензурная лексика не фильтруется.

По умолчанию флажок установлен.

Разрешить на заблокированном устройстве

Использование голосовых команд Siri, когда мобильное устройство пользователя заблокировано. На мобильном устройстве пользователя должен быть установлен пароль. Параметр доступен, если установлен флажок **Разрешить использование Siri**.

Если флажок установлен, пользователь может использовать голосовые команды Siri на заблокированном мобильном устройстве.

Если флажок снят, пользователю запрещено использовать голосовые команды Siri на заблокированном устройстве.

По умолчанию флажок установлен.

Показывать данные пользователя (только для supervised)

Добавление персональных данных пользователя в Siri, чтобы использовать их в голосовых командах Siri (например, "напомни позвонить жене, когда приду домой") на iOS MDM-устройстве. Параметр доступен, если установлен флажок **Разрешить использование Siri**.

Если флажок установлен, пользователь может заполнить личную карточку в параметрах Siri и использовать эти данные для голосовых команд Siri.

Если флажок снят, пользователю запрещено добавлять свои персональные данные в Siri.

По умолчанию флажок установлен.

Разрешить AirPrint (только для supervised, iOS 11+)

Установка или снятие флажка определяет, может ли пользователь устройства использовать AirPrint.

Ограничение поддерживается на устройствах с iOS версии 11 и выше.

По умолчанию флажок установлен.

Разрешить хранение учетных данных AirPrint (только для supervised, iOS 11+)

Установка или снятие флажка определяет, может ли пользователь устройства хранить связку ключей для имени пользователя и пароля для AirPrint.

Ограничение поддерживается на устройствах с iOS версии 11 и выше.

По умолчанию флажок установлен.

Разрешить обнаружение iBeacon для принтеров AirPrint (только для supervised, iOS 11+)

Установка или снятие флажка определяет, включено ли обнаружение iBeacon для принтеров AirPrint. Отключение обнаружения iBeacon для принтеров AirPrint предотвращает фишинг сетевого трафика ложными маяками AirPrint Bluetooth.

Ограничение поддерживается на устройствах с iOS версии 11 и выше.

По умолчанию флажок установлен.

Принудительно использовать доверенный TLS-сертификат для AirPrint (только для supervised, iOS 11+)

Установка или снятие флажка определяет необходимость использования доверенного сертификата для передачи данных для печати по протоколу TLS.

Ограничение поддерживается на устройствах с iOS версии 11 и выше.

По умолчанию флажок снят.

Разрешить iBooks Store (только для supervised)

Доступ в интернет-магазин iBooks Store из приложения iBooks на мобильном устройстве пользователя.

Если флажок установлен, пользователь может переходить в интернет-магазин iBooks Store из приложения iBooks, установленного на устройстве.

Если флажок снят, пользователь не может переходить в iBooks Store из приложения iBooks.

По умолчанию флажок установлен.

Разрешить устанавливать приложения из Apple Configurator и iTunes (только для supervised)

Возможность самостоятельно устанавливать приложения на iOS MDM-устройство.

Если флажок установлен, пользователь может самостоятельно устанавливать или обновлять приложения на мобильном устройстве из App Store с помощью iTunes, Apple Configurator или Kaspersky Device Management для iOS.

Если флажок снят, пользователь не может устанавливать или обновлять на мобильном устройстве приложения из App Store с помощью iTunes, Apple Configurator или Kaspersky Device Management для iOS. Установка и обновление доступны только для корпоративных приложений. Значок App Store удален с главного экрана iOS MDM-устройства.

По умолчанию флажок установлен.

Разрешить устанавливать приложения из App Store (только для supervised)

Возможность самостоятельно устанавливать приложения на мобильное устройство из App Store. Флажок доступен, если установлен флажок **Разрешить устанавливать приложения из Apple Configurator и iTunes**.

Если флажок установлен, пользователь может самостоятельно устанавливать или обновлять приложения из App Store.

Если флажок снят, пользователь не может устанавливать или обновлять приложения на мобильном устройстве из App Store. Значок App Store удален с главного экрана iOS MDM-устройства.

По умолчанию флажок установлен.

Разрешить автоматическую загрузку приложений (только для supervised)

Использование функции автоматической загрузки приложений на мобильное устройство пользователя. Флажок доступен, если установлены флажки **Разрешить устанавливать приложения из Apple Configurator и iTunes** и **Разрешить устанавливать приложения из App Store**.

Если флажок установлен, пользователю доступна функция автоматической загрузки приложений (**Настройки** > **iTunes и App Store** > **Программы**). После включения этой функции приложения, которые пользователь приобрел в App Store, автоматически загружаются на другие Apple-устройства пользователя.

Если флажок снят, функция автоматической загрузки приложений выключена и недоступна.

По умолчанию флажок установлен.

Разрешить удалять приложения (только для supervised)

Возможность удаления приложений с мобильного устройства.

Если флажок установлен, пользователь может удалять с устройства приложения, которые были установлены из App Store или с помощью iTunes.

Если флажок снят, пользователь не может удалять с мобильного устройства приложения, которые были установлены из App Store или с помощью iTunes.

По умолчанию флажок установлен.

Разрешить Встроенные покупки

Использование системы in-App Purchase на мобильном устройстве.

Если флажок установлен, пользователь может совершать покупки в приложениях, установленных на мобильном устройстве.

Если флажок снят, пользователь не может совершать покупки в приложениях, установленных на мобильном устройстве.

По умолчанию флажок установлен.

Требовать пароль для каждой покупки в iTunes Store

Использование пароля ограничений при покупке медиаконтента в iTunes Store.

Если флажок установлен, перед совершением первой покупки в iTunes Store пользователь должен задать пароль ограничений в параметрах ограничения покупок и в дальнейшем использовать его для предотвращения случайных и несанкционированных покупок. После проверки подлинности учетной записи при совершении покупок не требуется повторно вводить пароль ограничений в течение следующих 15 минут.

Если флажок снят, перед совершением покупок в iTunes Store пользователю не требуется вводить пароль ограничений.

По умолчанию флажок снят.

Разрешить резервное копирование в iCloud

Автоматическое резервное копирование данных с iOS MDM-устройства в iCloud. В ходе резервного копирования не создаются копии данных, которые уже хранятся в iCloud. Также не создаются копии медиаконтента, который был получен в результате синхронизации устройства с компьютером, а не приобретен в iTunes Store.

Если флажок установлен, пользователь может сохранять резервные копии данных мобильного устройства в iCloud. Резервные копии данных ежедневно сохраняются в iCloud, когда устройство включено, заблокировано и подключено к источнику питания.

Если флажок снят, пользователю запрещено сохранять резервные копии данных мобильного устройства в iCloud.

По умолчанию флажок установлен.

Разрешить хранение документов и данных в iCloud (только для supervised)

Автоматическое резервное копирование документов в iCloud. Документы iCloud можно открывать и редактировать на других устройствах, на которых настроена служба iCloud.

Если флажок установлен, пользователь может сохранять документы в iCloud, открывать и редактировать их на других устройствах в приложениях, поддерживающих работу с iCloud (например, в TextEdit).

Если флажок снят, пользователю запрещено сохранять документы в iCloud.

По умолчанию флажок установлен.

Разрешить Связку ключей iCloud

Автоматическая синхронизация учетных данных пользователя iOS MDM-устройства с другими Apple-устройствами пользователя. Данные для синхронизации хранятся в Связке ключей iCloud. Данные в Связке ключей iCloud шифруются. Связка ключей iCloud позволяет сохранить в iCloud следующие данные:

- учетные записи веб-сайтов;
- номера банковских карт и сроки их действия;
- пароли от беспроводных сетей.

Если флажок установлен, пользователь может синхронизировать данные своих учетных записей с другими своими устройствами Apple.

Если флажок снят, пользователю запрещено использовать Связку ключей iCloud на мобильном устройстве.

По умолчанию флажок установлен.

Разрешить управляемым приложениям хранить данные в iCloud

Создание резервной копии данных управляемых приложений в iCloud. *Управляемые приложения* – это корпоративные приложения, установленные, настроенные и управляемые с помощью Kaspersky Device Management для iOS

Если флажок установлен, пользователь может хранить данные управляемых приложений в iCloud.

Если флажок снят, пользователю недоступно хранение корпоративных данных в iCloud.

По умолчанию флажок установлен.

Разрешить резервное копирование корпоративных книг

Резервное копирование корпоративных книг с помощью iCloud или iTunes. Вы можете предоставить доступ к корпоративным книгам, разместив их на веб-сервере компании.

Если флажок установлен, пользователю доступно резервное копирование корпоративных книг с помощью iCloud или iTunes.

Если флажок снят, резервное копирование корпоративных книг невозможно.

По умолчанию флажок установлен.

Разрешить синхронизацию примечаний и выделение цветом в корпоративных книгах

Возможность синхронизировать заметки, закладки, а также выделенный цветом текст в корпоративных книгах с помощью iCloud.

Если флажок установлен, пользователю доступна функция синхронизации, заметок, закладок и выделений цветом в корпоративных книгах (**Настройки** > **iBooks** > **Синхр. закладок и заметок**). При этом изменения будут доступны на всех Apple-устройствах пользователя с помощью iCloud.

Если флажок снят, заметки, закладки и выделенный текст будут доступны только на этом мобильном устройстве.

По умолчанию флажок установлен.

Разрешить Общий доступ к фото в iCloud

Использование функции Общий доступ к фото в iCloud на iOS MDM-устройстве для предоставления другим пользователям доступа к фотографиям и видео на сервере iCloud. У других пользователей должна быть настроена функция Общий доступ к фото в iCloud.

Если флажок установлен, пользователю мобильного устройства доступна функция Общий доступ к фото в iCloud. Пользователи других устройств могут просматривать фотографии и видео пользователя, оставлять комментарии, а также добавлять свои фотографии и видео. Также пользователь может получить доступ к данным других пользователей на сервере iCloud.

Если флажок снят, пользователю недоступна функция Общий доступ к фото в iCloud. Пользователь не может предоставлять доступ к своим фотографиям и видео на сервере iCloud другим пользователям, а также получить доступ к данным других пользователей на сервере iCloud.

По умолчанию флажок установлен.

Разрешить Медиатеку iCloud

Использование функции Медиатеки iCloud для автоматической отправки сделанных фотографий и видео с iOS MDM-устройства на другие Apple-устройства пользователя.

Если флажок установлен, пользователю доступна функция Медиатеки iCloud при работе с приложением "Фото".

Если флажок снят, пользователю недоступна функция Медиатеки iCloud. Фотографии и видео пользователя, сохраненные в Медиатеке iCloud, удаляются с сервера iCloud.

По умолчанию флажок установлен.

Разрешить Мой фотопоток (запрет может привести к потере данных)

Использование функции Мой фотопоток для автоматической отправки сделанных фотографий и видео с iOS MDM-устройства на другие Apple-устройства пользователя. Сделанные фотографии и видео хранятся в папке "Мой фотопоток" на сервере iCloud в течение 30 дней.

Если флажок установлен, пользователю доступна функция Мой фотопоток при работе с приложениями iPhoto или Aperture.

Если флажок снят, пользователю недоступна функция Мой фотопоток. Фотографии и видео пользователя, сохраненные в папке "Мой фотопоток", удаляются с сервера iCloud.

По умолчанию флажок установлен.

Разрешить автоматическую синхронизацию в роуминге

Автоматическая синхронизация данных пользователя, когда iOS MDM-устройство находится в роуминге.

Если флажок установлен, пользователь может включить автоматическую синхронизацию данных в роуминге. Включение автоматической синхронизации в роуминге может привести к непредвиденным расходам на мобильную связь.

Если флажок снят, пользователю запрещено использовать автоматическую синхронизацию данных в роуминге.

По умолчанию флажок установлен.

Включить шифрование резервных копий

Шифрование резервных копий данных iOS MDM-устройства в программе iTunes на компьютере пользователя.

Шифрование данных конфигурационной политики Kaspersky Device Management для iOS не выполняется независимо от того, включено шифрование резервной копии данных или нет.

Если флажок установлен, то при создании резервной копии данных мобильного устройства в приложении iTunes данные шифруются и защищаются паролем. В данном случае пользователь не сможет зашифровать резервные копии данных устройства в приложении iTunes.

Если флажок снят, пользователь может выбрать использование шифрования резервных копий данных в программе iTunes.

По умолчанию флажок снят.

Ограничить трекинг рекламы

Использование технологии IFA (Identifier for advertisers) для отслеживания открываемых веб-сайтов и запускаемых приложений на iOS MDM-устройстве. IFA позволяет настроить трекинг рекламы на мобильном устройстве в соответствии с интересами пользователя.

Если флажок установлен, технология IFA выключена на мобильном устройстве пользователя.

Если флажок снят, технология IFA включена на мобильном устройстве и отслеживает открываемые веб-сайты и запускаемые приложения для показа целевой рекламы.

По умолчанию флажок снят.

Разрешить сброс настроек до заводских (только для supervised)

Возможность удаления всех данных с устройства и сброса настроек до заводских.

Если флажок установлен, пользователю доступна функция удаления всех данных с устройства и сброса настроек до заводских (**Настройки** > **Основные** > **Сброс** > **Стереть контент и настройки**).

Если флажок снят, функция сброса настроек до заводских недоступна.

По умолчанию флажок установлен.

Разрешить пользователям использовать недоверенные TLS-сертификаты

Использование недоверенных TLS-сертификатов для обеспечения зашифрованного канала связи между приложениями на iOS MDM-устройстве (Mail, Контакты, Календарь, Safari) и корпоративными ресурсами.

Если флажок установлен, пользователь после предупреждения может разрешить использование недоверенного TLS-сертификата.

Если флажок снят, Kaspersky Device Management для iOS автоматически запрещает использование недоверенных TLS-сертификатов.

По умолчанию флажок установлен.

Разрешить автоматическое обновление доверенных сертификатов

Автоматическое обновление доверенных сертификатов на iOS MDM-устройстве.

Если флажок установлен, Kaspersky Device Management для iOS автоматически принимает изменения в параметрах доверия сертификата.

Если флажок снят, изменения в параметрах доверия сертификата автоматически не принимаются. Пользователь после предупреждения может самостоятельно принять изменения в параметрах доверия сертификата.

По умолчанию флажок установлен.

Разрешить доверять новым корпоративным разработчикам

Возможность настроить доверие к корпоративным приложениям на мобильном устройстве. Вы можете разработать корпоративные приложения и распространить их среди сотрудников для внутреннего использования. Для работы с корпоративным приложением пользователь мобильного устройства должен сделать его доверенным. При установке приложений с помощью Kaspersky Device Management для iOS доверие к приложениям устанавливается автоматически.

Если флажок установлен, пользователь может настраивать доверие к корпоративным приложениям (**Настройки** > **Основные** > **Профили** или **Профили и управление устройством**).

Если флажок снят, пользователь не может установить доверие к корпоративным приложениям при установке приложения вручную. Вы можете установить приложения только с помощью Kaspersky Device Management для iOS. Доверие к приложениям будет установлено автоматически.

По умолчанию флажок установлен.

Разрешить установку конфигурационных профилей (только для supervised)

Применение дополнительных конфигурационных профилей кроме политик Kaspersky Security Center на iOS MDM-устройстве.

Если флажок установлен, пользователь может устанавливать дополнительные конфигурационные профили на мобильное устройство.

Если флажок снят, пользователь не может устанавливать дополнительные конфигурационные профили кроме политики Kaspersky Security Center на мобильном устройстве.

По умолчанию флажок установлен.

Разрешить изменение параметров учетной записи (только для supervised)

Возможность добавлять на iOS MDM-устройстве новые учетные записи (например, учетные записи электронной почты) и изменять параметры учетных записей.

Если флажок установлен, пользователь мобильного устройства может добавлять новые учетные записи, а также изменять параметры существующих учетных записей.

Если флажок снят, пользователю мобильного устройства запрещено добавлять новые учетные записи, а также изменять параметры существующих учетных записей.

По умолчанию флажок установлен.

Разрешить изменение параметров сотовой связи (только для supervised)

Возможность настройки передачи данных приложениями, установленными на мобильном устройстве, по сотовой сети.

Если флажок установлен, пользователь может настраивать параметры передачи данных по сотовой сети (**Настройки** > **Сотовая связь** > **Сотовые данные для приложений**).

Если флажок снят, изменение настроек передачи данных приложениями по сотовой сети недоступно.

По умолчанию флажок установлен.

Разрешить изменение имени устройства (только для supervised)

Возможность изменить имя мобильного устройства.

Если флажок установлен, пользователь может изменить имя мобильного устройства (**Настройки** > **Основные** > **Об этом устройстве** > **Имя**).

Если флажок снят, изменение имени устройства недоступно.

По умолчанию флажок установлен.

Разрешить использование функции "Найти устройство" в приложении "Локатор" (только для supervised, iOS 13+)

Установка или снятие флажка определяет, может ли пользователь устройства использовать функцию "Найти устройство" в приложении "Локатор".

Ограничение поддерживается на устройствах с iOS версии 13 и выше.

По умолчанию флажок установлен.

Разрешить использование функции "Найти друзей" в приложении "Локатор" (только для supervised, iOS 13+)

Установка или снятие флажка определяет, может ли пользователь устройства использовать функцию "Найти друзей" в приложении "Локатор".

Ограничение поддерживается на устройствах с iOS версии 13 и выше.

По умолчанию флажок установлен.

Разрешить изменение параметров функции "Найти друзей" (только для supervised)

Возможность изменения параметров приложения "Найти друзей" на iOS MDM-устройстве.

Если флажок установлен, пользователь может изменять параметры приложения "Найти друзей" на iOS MDM-устройстве.

Если флажок снят, пользователь не может изменять настроенные параметры приложения "Найти друзей" на iOS MDM-устройстве.

По умолчанию флажок установлен.

Разрешить изменение параметров уведомлений (только для supervised)

Возможность настройки отображения уведомлений на мобильном устройстве.

Если флажок установлен, пользователь может настроить параметры отображения уведомлений на мобильном устройстве (**Настройки** > **Основные** > **Уведомления**).

Если флажок снят, настройка параметров отображения уведомлений недоступна.

По умолчанию флажок установлен.

Разрешить изменение пароля (только для supervised)

Возможность установки, изменения или удаления пароля разблокировки мобильного устройства.

Если флажок установлен, пользователь может установить, изменить или удалить пароль для разблокировки мобильного устройства (**Настройки** > **Пароль**).

Если флажок снят, управление паролем разблокировки устройства недоступно.

По умолчанию флажок установлен.

Разрешить изменение Touch ID и Face ID (только для supervised)

Возможность добавления и удаления отпечатков Touch ID или данных Face ID. Параметр доступен, если установлен флажок **Разрешить изменение пароля**.

Управление Face ID доступно на устройствах под управлением операционной системы iOS версии 11.0 и выше.

Если флажок установлен, пользователь может добавлять и удалять отпечатки Touch ID или данные Face ID (**Настройки** > **Touch ID и код-пароль / Face ID и код-пароль** > **Отпечатки**).

Если флажок снят, управление отпечатками Touch ID и данными Face ID недоступно.

Ограничение невозможно применить на iPad-устройствах.

По умолчанию флажок установлен.

Разрешить изменение ограничений (только для supervised)

Возможность настройки параметров ограничений на мобильном устройстве. Ограничения на мобильном устройстве могут быть использованы пользователем для выполнения функций родительского контроля. Пользователь может ограничить функции устройства (например, запретить использование камеры), доступ к медиаконтенту (например, установить возрастные ограничения на просмотр фильмов), работу приложений (например, запретить использование iTunes Store) и настроить другие ограничения.

Если флажок установлен, пользователь может настроить параметры ограничений на мобильном устройстве (**Настройки** > **Основные** > **Ограничения**).

Если флажок снят, настройка параметров ограничения на мобильном устройстве недоступна.

По умолчанию флажок установлен.

Разрешить изменение обоев (только для supervised)

Возможность выбрать изображение, которое будет отображаться на экране блокировки, экране "Домой".

Если флажок установлен, пользователь может выбрать обои для мобильного устройства.

Если флажок снят, выбор обоев недоступен.

По умолчанию флажок установлен.

Разрешить сторонние соединения (только для supervised)

Защита iOS MDM-устройства от сторонних соединений. *Стороннее соединение* – это соединение с другими устройствами, а также синхронизация с сервисами Apple, например, с iTunes.

Если флажок установлен, пользователь может синхронизировать iOS MDM-устройство с другими устройствами, а также с сервисами Apple.

Если флажок снят, Kaspersky Device Management для iOS блокирует сторонние соединения на мобильном устройстве пользователя.

По умолчанию флажок установлен.

Разрешить передачу документов из управляемых в неуправляемые приложения

Возможность открывать в неуправляемых (личных) приложениях на iOS MDM-устройстве документы, созданные с использованием управляемых (корпоративных) приложений и учетных записей. *Управляемые приложения* – это корпоративные приложения, установленные, настроенные и управляемые с помощью Kaspersky Device Management для iOS *Неуправляемые приложения* – приложения, установленные, настроенные и управляемые пользователем мобильного устройства.

Если флажок установлен, пользователь может открывать в неуправляемых приложениях документы, созданные в управляемых приложениях.

Если флажок снят, пользователю запрещено открывать документы, созданные в управляемых приложениях, в неуправляемых приложениях. Например, параметр позволяет предотвратить открытие конфиденциального почтового вложения из управляемой учетной записи электронной почты в личных приложения пользователя.

По умолчанию флажок установлен.

Разрешить передачу документов из неуправляемых в управляемые приложения

Возможность открывать в управляемых (корпоративных) приложениях на iOS MDM-устройстве документы, созданные с использованием неуправляемых (личных) приложений и учетных записей пользователя. *Управляемые приложения* – это корпоративные приложения, установленные, настроенные и управляемые с помощью Kaspersky Device Management для iOS *Неуправляемые приложения* – приложения, установленные, настроенные и управляемые пользователем мобильного устройства.

Если флажок установлен, пользователь может открывать в управляемых приложениях документы, созданные в неуправляемых приложениях.

Если флажок снят, пользователю запрещено открывать в управляемых приложениях документы, созданные в неуправляемых приложениях. Например, параметр позволяет предотвратить открытие документа из личной учетной записи iCloud в корпоративном приложении.

По умолчанию флажок установлен.

Считать AirDrop неуправляемым приложением

Использование AirDrop в качестве неуправляемого приложения для передачи данных с мобильного устройства на другие устройства Apple. Для работы этого ограничения необходимо снять флажок **Разрешить передачу документов из управляемых в неуправляемые приложения**. *Неуправляемые приложения* – приложения, установленные, настроенные и управляемые пользователем мобильного устройства.

Если флажок установлен, AirDrop считается неуправляемым приложением.

Если флажок снят, AirDrop считается управляемым приложением.

По умолчанию флажок установлен.

Разрешить Handoff

Использование функции Handoff на мобильном устройстве пользователя. Handoff позволяет начать работу с данными на одном Apple-устройстве, а затем переключиться на другое Apple-устройство и продолжить работу.

Если флажок установлен, пользователю доступна функция Handoff.

Если флажок снят, функция Handoff недоступна.

По умолчанию флажок установлен.

Разрешить предложения Spotlight (только для supervised)

Использование предложений Spotlight для работы функции "Поиск" на мобильном устройстве пользователя. Spotlight позволяет показывать результаты поиска из интернета, iTunes Store, App Store и других источников при использовании функции "Поиск". При использовании предложений Spotlight поисковые запросы и связанные с ними данные пользователя отправляются в компанию Apple.

Если флажок установлен, пользователь может разрешить добавить предложения Spotlight в функцию "Поиск" (**Настройки** > **Основные** > **Поиск Spotlight** > **Предложения Spotlight**).

Если флажок снят, предложения Spotlight недоступны. Пользовательские данные не отправляются в компанию Apple.

Ограничение невозможно применить на iPadOS-устройствах.

По умолчанию флажок установлен.

Разрешить отправлять в Apple диагностические и персональные данные

Автоматическое получение диагностической информации и сведений об использовании iOS MDM-устройства и отправка отчета с этими данными в компанию Apple для анализа.

Если флажок установлен, пользователь после предупреждения может разрешить отправку отчетов с диагностической информацией и сведений об использовании мобильного устройства в компанию Apple.

Если флажок снят, Kaspersky Device Management для iOS блокирует отправку отчетов с диагностической информацией и сведениями об использовании мобильного устройства в компанию Apple.

По умолчанию флажок установлен.

Разрешить изменение параметров отправки диагностических данных (только для supervised)

Автоматическое получение диагностической информации и сведений об использовании iOS MDM-устройства и отправка отчета с этими данными в компанию Apple для анализа. Параметр доступен, если установлен флажок **Разрешить отправлять в Apple диагностические и персональные данные**.

Если флажок установлен, пользователь может настроить отправку отчетов с диагностической информацией и сведений об использовании мобильного устройства в компанию Apple (**Настройки** > **Конфиденциальность** > **Диагностика и использование**).

Если флажок снят, настройка параметров отправки отчетов с диагностической информацией недоступна.

По умолчанию флажок установлен.

Разрешить Touch ID и Face ID для разблокировки устройства

Технологии Touch ID и Face ID позволяют использовать отпечаток пальца или распознавание лица как пароль для разблокировки iOS MDM-устройства. Touch ID и Face ID также можно использовать для авторизации покупок с помощью Apple Pay, iTunes Store, App Store, iBooks Store и выполнения входа в приложения.

Управление Face ID доступно на устройствах под управлением операционной системы iOS версии 11.0 и выше.

Если флажок установлен, пользователь может использовать отпечаток пальца или распознавание лица вместо пароля для разблокировки мобильного устройства.

Если флажок снят, пользователь не может использовать технологии Touch ID и Face ID для разблокирования мобильного устройства.

По умолчанию флажок установлен.

Включить распознавание запястья для Apple Watch

Автоматическое блокирование Apple Watch, когда пользователь снимает часы с руки.

Если флажок установлен, Apple Watch блокируются, когда пользователь снимает часы с руки (**Apple Watch** > **Мои часы** > **Основные** > **Распознавание запястья**). Для разблокирования пользователь должен ввести пароль на своем мобильном устройстве.

Если флажок снят, блокировка Apple Watch после снятия с руки недоступно.

По умолчанию флажок установлен.

Разрешить создавать пару с Apple Watch (только для supervised)

Создание пары Apple Watch и контролируемого мобильного устройства.

Если флажок установлен, пользователь контролируемого мобильного устройства может создать пару с Apple Watch.

Если флажок снят, создание пары с Apple Watch недоступно.

По умолчанию флажок установлен.

Требовать пароль при первом подключении по AirPlay

Использование пароля при подключении iOS MDM-устройства к устройствам, совместимым с AirPlay. Пароль применяется для безопасной передачи медиаконтента.

Если флажок установлен, перед первым подключением мобильного устройства к устройствам, совместимым с AirPlay, пользователь должен задать пароль в параметрах безопасности AirPlay и в дальнейшем использовать его.

Если флажок снят, пользователь самостоятельно принимает решение об использовании пароля при подключении мобильного устройства к устройствам, совместимым с AirPlay.

По умолчанию флажок снят.

Разрешить предиктивную клавиатуру (только для supervised)

Использование функции предиктивного набора текста. Функция предиктивного набора текста показывает варианты окончания слов и предложений на основе имеющихся словарей.

Если флажок установлен, пользователь может включить и использовать функцию предиктивного набора текста (**Настройки** > **Основные** > **Клавиатура** > **Предиктивный набор**).

Если флажок снят, функция предиктивного набора текста недоступна. При наборе текста подсказки не отображаются.

По умолчанию флажок установлен.

Разрешить сочетания клавиш (только для supervised)

Использование сочетаний клавиш для быстрого доступа к функциям мобильного устройства.

Если флажок установлен, пользователь может включить функцию сочетания клавиш и использовать ее при работе с мобильным устройством (**Настройки** > **Основные** > **Универсальный доступ** > **Сочетание клавиш**).

Если флажок снят, функция сочетания клавиш недоступна.

По умолчанию флажок установлен.

Разрешить автокоррекцию (только для supervised)

Использование функции автокоррекции при наборе текста.

Если флажок установлен, пользователь может включить и использовать функцию автокоррекции (**Настройки** > **Основные** > **Клавиатура** > **Автокоррекция**).

Если флажок снят, при наборе текста автокоррекция недоступна.

По умолчанию флажок установлен.

Разрешить проверку правописания (только для supervised)

Использование функции правописания при наборе текста на мобильном устройстве. Проверка правописания подчеркивает неправильно введенные слова и предлагает варианты замены.

Если флажок установлен, пользователь может включить и использовать функцию правописания (**Настройки** > **Основные** > **Клавиатура** > **Правописание**).

Если флажок снят, при наборе текста проверка правописания недоступна.

По умолчанию флажок установлен.

Разрешить поиск слова в словаре (только для supervised)

Получение определения слова в словаре на мобильном устройстве. Словарь является функцией только программной клавиатуры.

Если флажок установлен, пользователь может выделить любое слово на экране мобильного устройства и получить его определение.

Если флажок снят, поиск слова в словаре недоступен.

По умолчанию флажок установлен.

Разрешить Wallet показывать уведомления на заблокированном экране

Использование уведомлений приложения Wallet на экране блокировки iOS MDM-устройства.

Если флажок установлен, на экране блокировки мобильного устройства отображаются уведомления Wallet.

Если флажок снят, на экране блокировки мобильного устройства не отображаются уведомления Wallet. Для работы с Wallet пользователь должен разблокировать устройство.

По умолчанию флажок установлен.

Показывать Пункт управления на заблокированном экране

Возможность перейти в Пункт управления iOS MDM-устройством, когда устройство заблокировано.

Если флажок установлен, пользователь может перейти в Пункт управления, смахнув экран блокировки вверх.

Если флажок снят, пользователь не может перейти в Пункт управления, когда мобильное устройство заблокировано.

По умолчанию флажок установлен.

Показывать Центр уведомлений на заблокированном экране

Возможность перейти в Центр уведомлений iOS MDM-устройства, когда устройство заблокировано.

Если флажок установлен, пользователь может перейти в Центр уведомлений, смахнув экран блокировки вниз.

Если флажок снят, пользователь не может перейти в Центр уведомлений, когда мобильное устройство заблокировано.

По умолчанию флажок установлен.

Показывать "Сегодня" на заблокированном экране

Отображение сведений из раздела "Сегодня" Центра уведомлений на заблокированном iOS MDM-устройстве. В разделе "Сегодня" Центра уведомлений отображаются следующие сведения:

- запланированные события в календаре;
- напоминания;
- акции;
- погода.

Если флажок установлен, пользователь может просматривать уведомления из раздела "Сегодня" в Центре уведомлений на заблокированном мобильном устройстве.

Если флажок снят, раздел "Сегодня" не отображается на заблокированном мобильном устройстве.

По умолчанию флажок установлен.

7. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.
8. Выберите раздел **Ограничения приложений**.
9. В блоке **Параметры ограничений приложений** установите флажок **Применить параметры на устройстве**.
10. Настройте ограничения для приложений на iOS MDM-устройстве.
11. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.
12. Выберите раздел **Ограничения медиаконтента**.
13. В блоке **Параметры ограничения медиаконтента** установите флажок **Применить параметры на устройстве**.
14. Настройте ограничения для медиаконтента на iOS MDM-устройстве.
15. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

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

Настройка доступа пользователей к веб-сайтам

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

Настройка доступа к веб-сайтам на Android-устройствах

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

Для работы Веб-Фильтра необходимо выполнение следующих условий:

- 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 поддерживается только браузерами Google Chrome, HUAWEI Browser, Samsung Internet и Яндекс Браузер.

Если приложение Kaspersky Endpoint Security для Android в режиме device owner не установлено в качестве службы Специальных возможностей, Веб-Фильтр поддерживается только браузером Google Chrome и проверяет только домен сайта. Чтобы Веб-Фильтр поддерживался другими браузерами (Samsung Internet Browser, Яндекс Браузер и HUAWEI Browser), приложение Kaspersky Endpoint Security должно быть включено в качестве службы Специальных возможностей. Это также позволит использовать функцию Custom Tabs.

Функция Custom Tabs поддерживается браузерами Google Chrome, HUAWEI Browser и Samsung Internet Browser.

В браузерах HUAWEI Browser, Samsung Internet Browser и Яндекс Браузер Веб-Фильтр не блокирует сайты на мобильном устройстве, если используется рабочий профиль и установлен флажок Включить Веб-Фильтр только в рабочем профиле.

По умолчанию Веб-Фильтр включен: ограничен доступ пользователя к веб-сайтам категорий **Фишинг** и **Вредоносное программное обеспечение**. На устройствах в режиме device owner, управляемых приложением Kaspersky Endpoint Security для Android, Веб-Фильтр поддерживается только браузером Google Chrome и проверяет только домен сайта. Чтобы Веб-Фильтр поддерживался другими браузерами (Samsung Internet Browser, Яндекс Браузер и HUAWEI Browser), приложение Kaspersky Endpoint Security должно быть включено в качестве службы Специальных возможностей.

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.

   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 **Веб-Фильтр**.

5. Для использования Веб-Фильтра вам или пользователю устройства необходимо прочитать Положение об обработке данных в целях использования Веб-Фильтра (Положение о Веб-Фильтре) и принять его условия. Для этого:

   a. Нажмите на ссылку **Положение о Веб-Фильтре** в верхней части раздела.

      Откроется окно **Положение об обработке данных в целях использования Веб-Фильтра**.

   b. Прочитайте Политику конфиденциальности и примите ее условия, установив соответствующий флажок. Для того чтобы ознакомиться с Политикой конфиденциальности, необходимо перейти по ссылке Политика конфиденциальности.

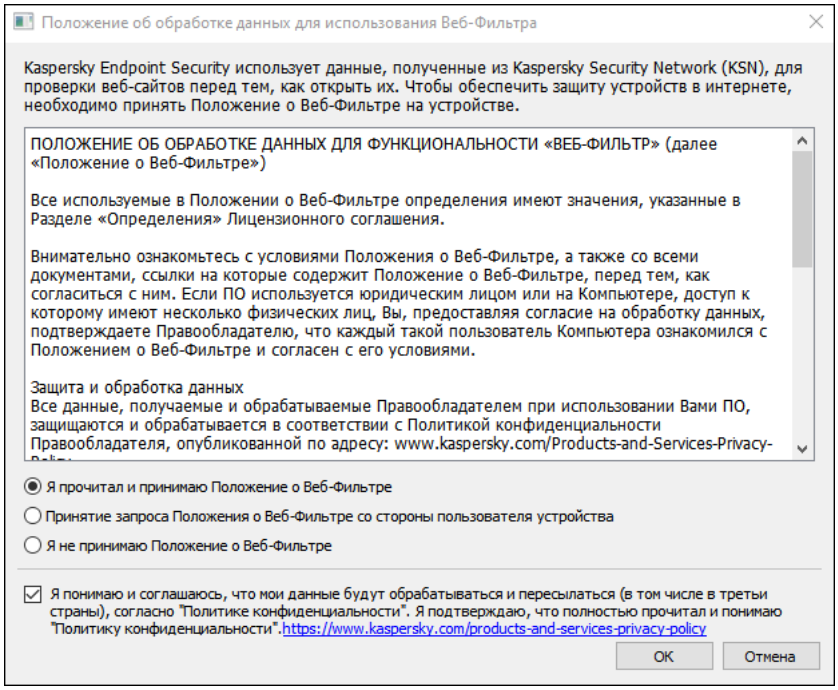
      Если вы не принимаете Политику конфиденциальности, пользователь мобильного устройства может принять Политику конфиденциальности в мастере первоначальной настройки или в приложении (→ **О приложении** → **Правовая информация** → **Политика конфиденциальности**).

   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.

   d. Нажмите на кнопку **OK**, чтобы закрыть окно.



Шаг 5. Примите условия Положения об обработке данных в целях использования Веб-Фильтра.

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

7. Если вы хотите, чтобы приложение проверяло полный веб-адрес при открытии сайта в Custom Tabs, установите флажок **Проверять полный веб-адрес при использовании Custom Tabs**.

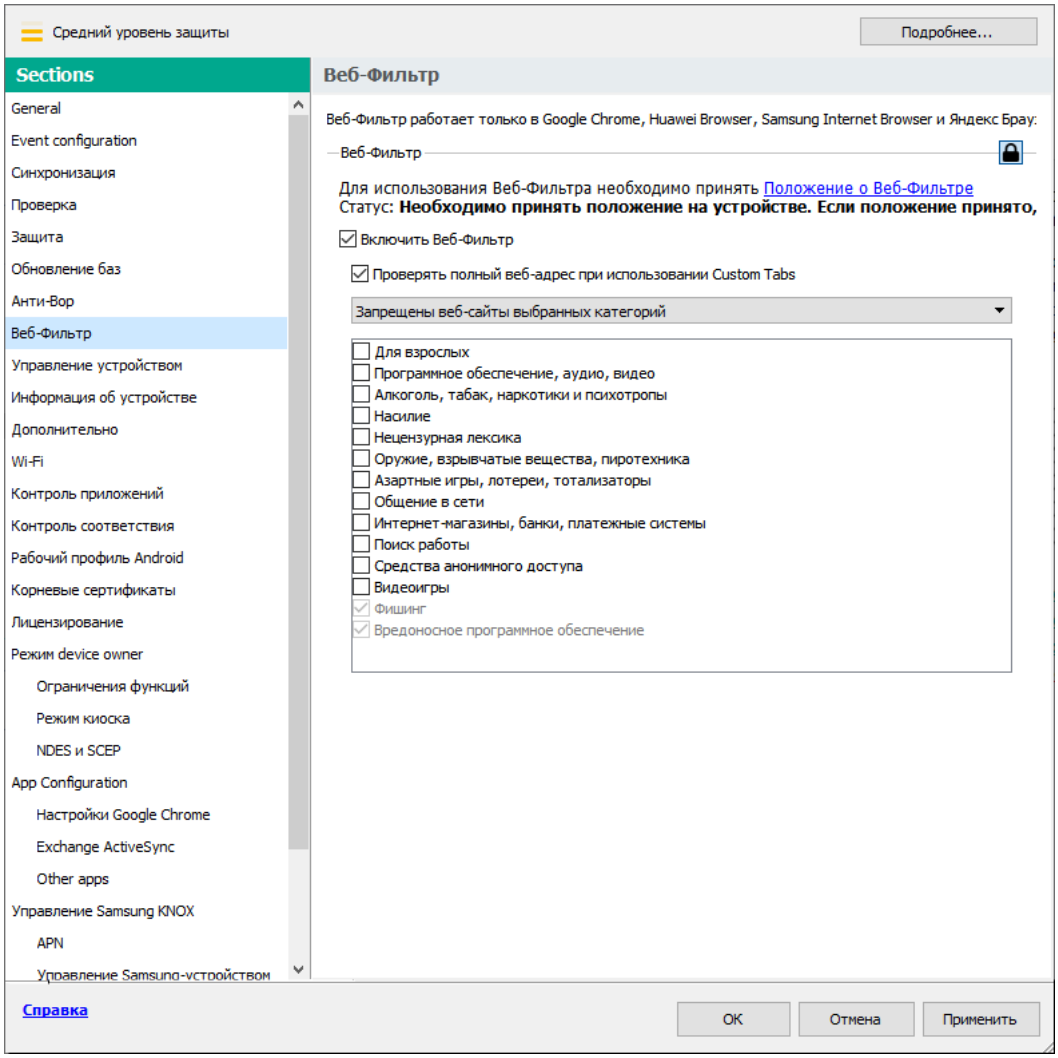
   Custom Tabs – это встроенный браузер, в котором можно просматривать веб-страницы, не покидая приложение и не переходя в полную версию браузера. Этот параметр повышает надежность обнаружения веб-адреса и его проверки по заданным правилам Веб-Фильтра. Если флажок установлен, Kaspersky Endpoint Security для Android открывает сайт в полной версии браузера и проверяет полный веб-адрес сайта. Если флажок снят, Kaspersky Endpoint Security для Android проверяет только домен сайта в Custom Tabs.

8. Выберите один из следующих вариантов:

   - 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.



Шаг 8. Раздел Веб-Фильтр. Выберите категории веб-сайтов, доступ к которым необходимо заблокировать.

   - Если вы хотите, чтобы приложение разрешало или ограничивало 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** или **Запрещены только перечисленные веб-сайты**.

Если Kaspersky Endpoint Security для Android не установлен в качестве службы Специальных возможностей, то Веб-Фильтр может блокировать разрешенный сайт при подгрузке на него элементов с сайта, домен которого не добавлен в список разрешенных.

b. Сформируйте список веб-сайтов, добавив адреса веб-сайтов, к которым приложение будет разрешать или ограничивать доступ (в зависимости от значения, выбранного в раскрывающемся списке). Вы можете добавить веб-сайты, используя ссылку (полный URL, включая протокол, например, `https://example.com`).

Чтобы гарантировать, что приложение разрешает или ограничивает доступ к веб-сайту во всех поддерживаемых версиях Google Chrome, HUAWEI Browser, Samsung Internet Browser и Yandex Browser, добавьте один и тот же URL дважды: один раз – с указанием протокола HTTP (например, `https://example.com`), а другой раз – с указанием протокола HTTPS (например, `https://example.com`).

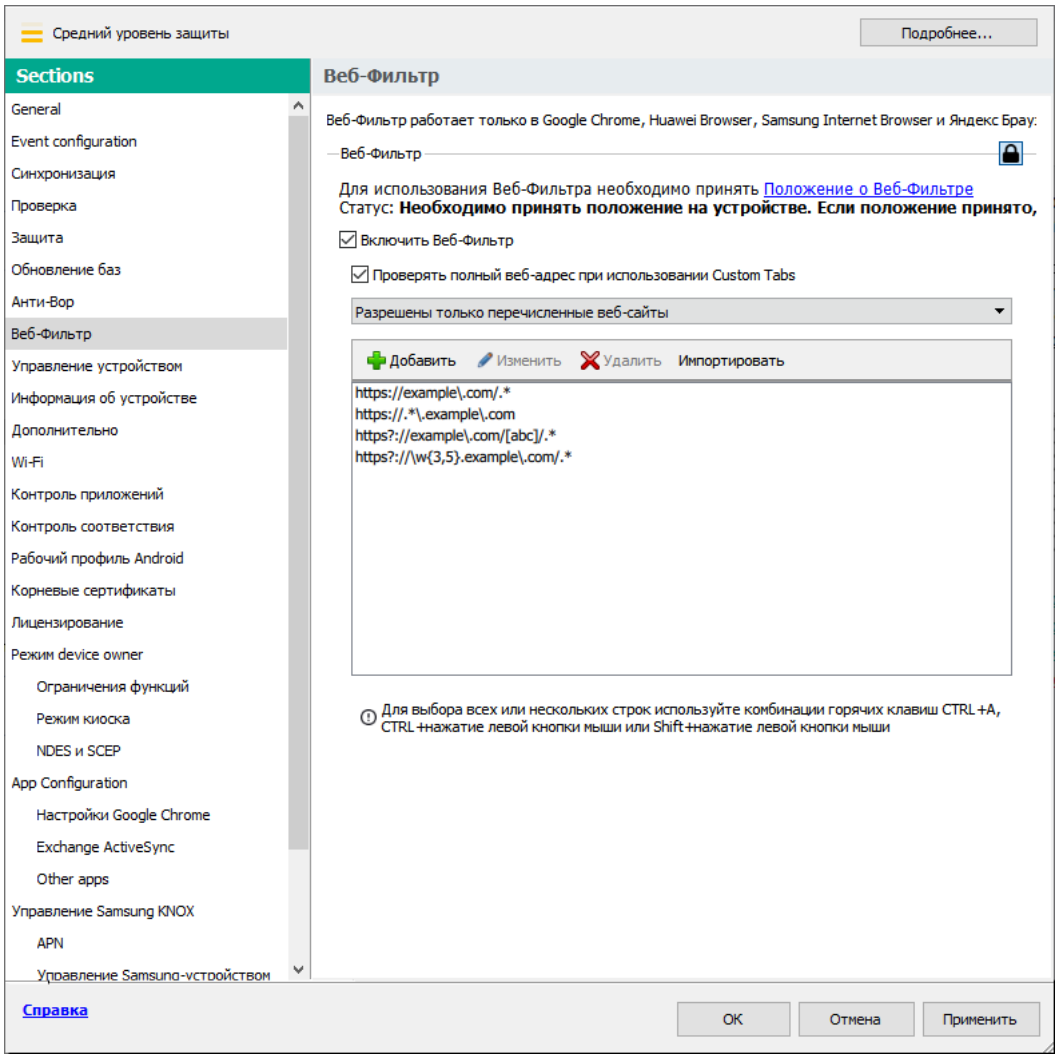
Например:

- `https://example.com` — Главная страница веб-сайта разрешена или заблокирована. Этот URL доступен только при использовании протокола HTTPS.
- `http://example.com`— Главная страница веб-сайта разрешена или заблокирована, но только при использовании протокола HTTP. Это не относится к протоколу HTTPS и другим.
- `https://example.com/page/index.html` — только страница `index.html` разрешена или заблокирована. Это не относится к остальным страницам веб-сайта.

Приложение также поддерживает регулярные выражения. При вводе адреса разрешенного или заблокированного веб-сайта используйте следующие шаблоны:

- `https://example\.com/.*` — этот шаблон блокирует или разрешает все дочерние страницы сайта, доступные при использовании протокола HTTPS (например, `https://example.com/about`).
- `https?://example\.com/.*`— этот шаблон блокирует или разрешает все дочерние страницы веб-сайта, доступные при использовании протоколов HTTP и HTTPS.
- `https?://.*\.example\.com`— этот шаблон блокирует или разрешает страницы всех субдоменов веб-сайта (например, `https://pictures.example.com`).
- `https?://example\.com/[abc]/.*`— этот шаблон блокирует или разрешает все дочерние страницы веб-сайта, URL-путь которых начинается с буквы "a", "b" или "c" в качестве первого каталога (например, `https://example.com/b/about`).
- `https?://\w{3,5}.example\.com/.*`— этот шаблон блокирует или разрешает все дочерние страницы веб-сайта, у которых субдомен содержит от 3 до 5 букв (например, `http://abde.example.com/about`).

Используйте выражение `https?`, чтобы выбрать оба протокола — HTTP и HTTPS. Подробнее о регулярных выражениях см. на сайте Службы технической поддержки Oracle.



Шаг 9. Раздел Веб-Фильтр. Укажите список веб-сайтов, к которым необходимо разрешить доступ.

- 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**.

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

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

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

Управление списком веб-сайтов

Для управления списком веб-сайтов используются следующие кнопки:

- **Добавить** – добавляет в список веб-сайт, заданный по URL-адресу или с помощью регулярного выражения.

- **Импортировать** – добавляет в список несколько веб-сайтов из файла TXT, который содержит необходимые URL-адреса или регулярные выражения. Файл должен быть закодирован в кодировке UTF-8. URL-адреса или регулярные выражения в файле должны быть разделены точкой с запятой или разрывом строки.

- **Редактировать** – позволяет изменить адрес веб-сайта.

- **Удалить** – удаляет веб-сайт из списка. Чтобы удалить несколько веб-сайтов из списка, выберите их с помощью горячих клавиш CTRL + A, CTRL + нажатие левой клавиши мыши или SHIFT + нажатие левой клавиши мыши и нажмите **Удалить**.

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.

Если веб-адрес переадресовывается на другую страницу, Веб-Фильтр проверяет только конечную страницу.

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 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 **Веб-Фильтр**.
5. В блоке **Параметры Веб-Фильтра** установите флажок **Применить параметры на устройстве**.
6. Чтобы блокировать доступ к запрещенным веб-сайтам и разрешить доступ к разрешенным веб-сайтам, выполните следующие действия:

   a. В раскрывающемся списке **Режим фильтрации веб-сайтов** выберите режим **Ограничить содержание "для взрослых"**.

   b. В блоке **Разрешенные веб-сайты** сформируйте список разрешенных веб-сайтов.

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

   c. В блоке **Запрещенные веб-сайты** сформируйте список запрещенных веб-сайтов.

      Адрес веб-сайта должен начинаться с `"http://"` или `"https://"`. Kaspersky Device Management для iOS запрещает доступ ко всем веб-сайтам домена.

7. Чтобы блокировать доступ ко всем веб-сайтам, кроме разрешенных веб-сайтов из списка закладок, выполните следующие действия:

   a. В раскрывающемся списке **Режим фильтрации веб-сайтов** выберите режим **Разрешить веб-сайты только из списка закладок**.

   b. В блоке **Закладки** сформируйте список закладок разрешенных веб-сайтов.

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

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

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

Контроль соответствия

В этом разделе приведены инструкции по контролю соблюдения корпоративных требований на устройствах и настройке правил контроля соответствия.

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, базы вредоносного ПО 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);
- действия, которые будут выполнены с устройством, если пользователь не устранит несоответствие в течение указанного времени (например, блокирование устройства).

> Если устройство находится в режиме энергосбережения, приложение может выполнить эту задачу позже, чем указано. Для своевременного реагирования KES-устройств под управлением Android на команды администратора, следует включить использование сервиса Firebase Cloud Messaging.

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.

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 **Контроль соответствия**.

5. Чтобы получать уведомления об устройствах, не соответствующих политике, в разделе **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 разделе **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 разделе **Правила контроля соответствия** сформируйте список правил проверки устройства на соответствие политике.

8. Чтобы добавить новое правило, нажмите на кнопку **Добавить**.

   Запустится мастер создания правила соответствия. Пройдите все шаги мастера, нажимая на кнопку **Далее**.

9. Выберите критерий несоответствия правилу.

   Доступны следующие критерии:

   - **Постоянная защита выключена.**

     Проверяет, было ли приложение установлено или запущено на устройстве.

   - **Базы вредоносного ПО устарели.**

     Проверяет, обновлялись ли базы вредоносного ПО 3 и более дней назад.

   - **Установлены запрещенные приложения.**

     Проверяет, содержит ли список приложений на устройстве приложения, запрещенные в Контроле приложений.

   - **Установлены приложения запрещенных категорий.**

     Проверяет, содержит ли список приложений на устройстве приложения из категорий, запрещенных в Контроле приложений.

   - **Не установлены все обязательные приложения.**

     Проверяет, содержит ли список приложений на устройстве приложение, установленное в качестве обязательного в Контроле приложений.

   - **Версия операционной системы устарела.**

     Проверяет соответствие версии Android на устройстве заданному диапазону разрешенных версий.

     Для этого критерия укажите минимальную и максимальную разрешенные версии Android. Если в качестве максимальной разрешенной версии выбрано значение **Любая**, это означает, что будущие версии Android, поддерживаемые Kaspersky Endpoint Security для Android, будут также разрешены.

   - **Устройство давно не синхронизировалось.**

Проверяет, как давно устройство синхронизировалось с Сервером администрирования последний раз.

Для этого критерия укажите максимальный период с момента последней синхронизации.

- **На устройстве получены root-права.**

  Проверяет, взломано ли устройство (получены ли на устройстве права суперпользователя).

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

  Проверяет, соответствует ли пароль разблокировки устройства параметрам, заданным в политике в разделе **Управление устройством**.

- **Установлена неактуальная версия Kaspersky Endpoint Security для Android.**

  Проверяет актуальность версии приложения на устройстве.

  Критерий применяется, только если приложение установлено с помощью инсталляционного пакета Kaspersky Endpoint Security для Android и если в блоке **Обновление Kaspersky Endpoint Security для Android** раздела **Дополнительно** свойств политики выбрана актуальная версия приложения.

  Для этого критерия также укажите минимальную разрешенную версию Kaspersky Endpoint Security для Android.

- **Использование SIM-карты не соответствует корпоративным требованиям.**

  Проверяет, была ли SIM-карта устройства заменена, вставлена или извлечена относительно предыдущего состояния проверки.

  Вы также можете включить проверку установки дополнительной SIM-карты.

  > В некоторых случаях проверяется также замена, установка и извлечение eSIM-карты.

- **Устройство находится в пределах или за пределами установленных геозон**

  > Указание геозоны приведет к увеличению энергопотребления устройства.

  Для этого критерия выберите требование, при нарушении которого нужно выполнить действие:

  - Устройство находится в пределах любой геозоны из списка (геозоны объединяются с помощью логического оператора "ИЛИ").
  - Устройство находится за пределами всех геозон из списка (геозоны объединяются с помощью логического оператора "И").

  В блоке **Список геозон** вы можете добавлять, редактировать или удалять геозоны.

  Чтобы добавить новую геозону:

  a. Нажмите на кнопку **Добавить**.

     Открывает окно **Добавить геозону**.

  b. Укажите **Название геозоны**.

  c. В разделе **Координаты периметра геозоны** укажите широту и долготу для каждой точки.

     Если вы хотите добавить более 3 точек, нажмите на кнопку **Добавить точку**. Чтобы удалить дополнительную точку, нажмите на кнопку **X**.

Для каждой геозоны можно вручную задать от 3 до 100 пар координат (широта, долгота) в формате десятичных чисел.

Периметр геозоны не должен содержать пересекающиеся прямые.

d. Вы можете просмотреть указанную геозону в программе "Яндекс Карты", нажав на кнопку **Посмотреть на карте**.

e. Нажмите на кнопку **Добавить**, чтобы добавить указанную геозону.

Новая геозона отобразится в списке.

Чтобы отредактировать геозону:

a. Выберите геозону, которую вы хотите отредактировать, и нажмите на кнопку **Изменить**.

b. Укажите новые параметры геозоны, как описано выше в этом разделе.

c. Нажмите на кнопку **Добавить**.

Отредактированная геозона отобразится в списке.

Чтобы удалить геозону:

a. Выберите геозону, которую вы хотите удалить, и нажмите на кнопку **Удалить**.

Геозона исчезнет из списка.

- **У Kaspersky Endpoint Security для Android нет доступа к точному или фоновому местоположению**

  Проверяет наличие у приложения Kaspersky Endpoint Security для Android разрешения определять точное местоположение устройства или использовать данные о местоположении в фоновом режиме.

10. Выберите действия, которые будут выполняться при обнаружении указанного критерия несоответствия. Вы можете добавить несколько критериев. Их можно объединить с помощью логического оператора "И".

    Некоторые действия Контроля соответствия являются длительными. Длительные действия применяются до выполнения одного из следующих условий:

    - Критерий несоответствия правилу перестал действовать.
    - Применена политика, в которой удалено соответствующее правило Контроля соответствия.

    Доступны следующие действия:

    - **Блокировка всех приложений, кроме системных**

      Запуск всех приложений, кроме системных, на мобильном устройстве пользователя заблокирован.

      Как только критерий несоответствия правилу перестанет обнаруживаться на устройстве, приложения автоматически разблокируются.

    - **Заблокировать устройство**

      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.

    - **Удалить корпоративные данные**

Корпоративные данные удалены с устройства. Перечень удаленных данных зависит от режима работы устройства.

- На личном устройстве удалены KNOX-контейнер и почтовый сертификат.
- Если устройство работает в режиме device owner, удалены KNOX-контейнер и сертификаты, установленные приложением Kaspersky Endpoint Security для Android (почтовые и VPN-сертификаты, сертификаты, полученные через профили SCEP, кроме мобильных сертификатов).
- Дополнительно, если установлен рабочий профиль Android, удален рабочий профиль (содержимое, настройки и ограничения) и сертификаты, установленные в рабочем профиле (почтовые и VPN-сертификаты, сертификаты, полученные через профили SCEP, кроме мобильных сертификатов).

- **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.

  На устройствах под управлением Android 14 или выше эта реакция применяется только в том случае, если устройство работает в режиме device owner.

- **Блокировка рабочего профиля**

  Рабочий профиль на устройстве заблокирован. Для получения доступа к рабочему профилю необходимо его разблокировать. Если после разблокирования рабочего профиля причина блокировки не устранена, рабочий профиль будет снова заблокирован через указанный период.

  > Это действие применяется только на устройствах под управлением Android 6 или выше.

  > После блокирования рабочего профиля история паролей рабочего профиля очищается. Это означает, что пользователь может повторно использовать один из недавних паролей, независимо от параметров пароля для рабочего профиля.

- **Удалить данные всех приложений**

  Это действие применяется только на устройствах под управлением Android 9 или выше в режиме device owner или с созданным рабочим профилем Android.

  Если устройство работает в режиме device owner, удаляются данные всех приложений. Если на устройстве создан рабочий профиль Android, удаляются данные всех приложений в рабочем профиле.

  В результате настройки приложений сброшены до установленных по умолчанию.

- **Удалить данные указанного приложения**

  Это действие применяется только на устройствах под управлением Android 9 или выше в режиме device owner или с созданным рабочим профилем Android.

  Для этого действия необходимо указать название пакета приложения, данные которого будут удалены. **Как получить имя пакета приложения**

Чтобы получить имя пакета приложения:

1. Откройте Google Play.
2. Найдите нужное приложение и откройте его страницу.

   URL приложения оканчивается именем пакета приложения (например, https://play.google.com/store/apps/details?id=**com.android.chrome**).

Чтобы получить имя пакета приложения, которое было добавлено в Kaspersky Security Center:

1. В дереве консоли Kaspersky Security Center выберите **Дополнительно** > **Удаленная установка** > **Инсталляционные пакеты**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Управление пакетами мобильных приложений**.

   В открывшемся окне **Управление пакетами мобильных приложений** в столбце **Название приложения** отображаются идентификаторы управляемых приложений.

   Если пакет приложения представлен файлом в формате APK, и необходимо узнать идентификатор приложения, можно добавить этот пакет приложения в окне **Управление пакетами мобильных приложений**, нажав на кнопку **Новый** и следуя инструкциям на экране.

В результате настройки приложения сброшены до установленных по умолчанию.

- **Запрет на запуск устройства в безопасном режиме**

  Пользователю запрещено запускать устройство в безопасном режиме.

  Это действие применяется только на устройствах под управлением Android 6 или выше в режиме device owner.

  Это длительное действие.

- **Запретить использование камеры**

  Пользователю запрещено использовать все имеющиеся на устройстве камеры.

  Это длительное действие.

- **Запретить использование Bluetooth**

  Пользователю устройства запрещено включать Bluetooth и изменять его параметры в Настройках.

  Это действие применяется только на устройствах под управлением Android 12 или ниже в режиме device owner или с созданным рабочим профилем Android.

  Это длительное действие.

- **Запретить использование Wi-Fi**

  Пользователю устройства запрещено использовать Wi-Fi и изменять его параметры в Настройках.

  Это действие применяется только на устройствах, работающих в режиме device owner (все версии Android), личных устройствах под управлением Android 9 или ниже.

  Это длительное действие.

- **Запрет на использование функций отладки по USB**

  Пользователю запрещено использовать функции отладки по USB и режим разработчика на устройстве.

Это действие применяется только на устройствах, работающих в режиме device owner, или устройствах с созданным рабочим профилем Android.

Это длительное действие.

- **Запрет режима полета**

  Пользователю запрещено включать режим полета на устройстве.

  Это действие применяется только на устройствах под управлением Android 9 или выше в режиме device owner.

  Это длительное действие.

  Новое правило появится в разделе **Правила контроля соответствия**.

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

12. В блоке **Действия при удалении пользователей из Active Directory** можно выбрать действия, которые будут выполняться на устройствах при удалении пользователей из Active Directory.

    Для этих настроек необходима интеграция с Microsoft Active Directory.

    Чтобы включить автоматическое удаление данных с устройств, связанных с неактивными учетными записями пользователей Active Directory, установите флажок **Удалять данные неактивных пользователей Active Directory** и выберите одно из следующих действий:

    - **Удалить корпоративные данные**

    - **Сбросить настройки до заводских**

      На устройствах под управлением Android 14 или выше это действие применяется только в том случае, если устройство работает в режиме device owner.

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

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

Контроль 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 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 **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 "И".

   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 идентификатор пакета приложения. **Как получить идентификатор пакета приложения**

Чтобы получить идентификатор пакета предустановленного приложения на iPhone или iPad,

Следуйте инструкциям в документации Apple.

Чтобы получить идентификатор пакета любого приложения для iPhone или iPad:

1. Откройте App Store.
2. Найдите нужное приложение и откройте его страницу.

   URL приложения оканчивается его числовым идентификатором (например, https://apps.apple.com/us/app/google-chrome/id**535886823**).
3. Скопируйте этот идентификатор (без букв "id").
4. Откройте страницу https://itunes.apple.com/lookup?id=<скопированный идентификатор>.

   Будет загружен текстовый файл.
5. Откройте загруженный файл и найдите в нем "bundleId".

Текст, следующий за "bundleId" – идентификатор пакета необходимого приложения.

Чтобы получить идентификатор пакета приложения, которое было добавлено в Kaspersky Security Center:

1. В дереве консоли Kaspersky Security Center выберите **Дополнительно** > **Удаленная установка** > **Инсталляционные пакеты**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Управление пакетами мобильных приложений**.

В открывшемся окне **Управление пакетами мобильных приложений** в столбце **Название приложения** отображаются идентификаторы управляемых приложений.

Если пакет приложения представлен файлом в формате .apk или .ipa, и необходимо узнать идентификатор приложения, можно добавить этот пакет приложения в окне **Управление пакетами мобильных приложений**, нажав на кнопку **Новый** и следуя инструкциям на экране.

- **Версия операционной системы**

  Проверяет версию операционной системы на устройстве.

  Для этого критерия необходимо выбрать оператор сравнения (**Равно**, **Не равно**, **Меньше**, **Меньше или равно**, **Больше** или **Больше или равно**) 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**).

- **Тип устройства**

Проверяет тип устройства.

Для этого критерия необходимо выбрать тип устройства (**iPhone** или **iPad**).

- **Модель устройства**

  Проверяет модель устройства.

  Для этого критерия необходимо выбрать оператор (**Входит в список** или **Не входит в список**) и перечислить модели, которые будут проверяться или исключаться из проверки соответственно.

  Чтобы указать модель, введите хотя бы один символ в поле **Идентификатор** и выберите нужную модель из появившегося списка. Список содержит коды мобильных устройств и соответствующие им публичные названия. Например, чтобы добавить все модели iPhone 14, введите "iPhone 14". В этом случае можно выбрать любую из доступных моделей: "iPhone 14", "iPhone 14 Plus", "iPhone 14 Pro", "iPhone 14 Pro Max".

  > В некоторых случаях одно публичное название может соответствовать нескольким кодам мобильных устройств (например, публичное название "iPhone 7" соответствует двум кодам мобильных устройств – "iPhone 9.1" и "iPhone 9.3"). Убедитесь, что выбрали все коды мобильных устройств, которые соответствуют нужным моделям.

  При вводе значения, отсутствующего в списке, ничего не будет найдено. Тем не менее, вы можете нажать на кнопку **OK** и добавить введенное значение к критерию.

- **Устройство находится в роуминге**

  Проверяет, находится устройство в роуминге (если выбрано **Да**) или нет (если выбрано **Нет**).

- **Пароль устройства установлен**

  Проверяет, установлен пароль (если выбрано **Да**) или нет (если выбрано **Нет**).

  При выборе **Да**, укажите, должен ли пароль устройства соответствовать (при выборе **Соответствует политике**) или не соответствовать (при выборе **Не соответствует политике**) параметрам, указанным в разделе **Параметры пароля**.

- **Свободное пространство**

  Проверяет, является ли объем свободного пространства на устройстве меньше указанного порога.

  Для этого критерия укажите пороговое значение свободного пространства и выберите единицу измерения (**ГБ** или **МБ**).

- **Устройство не зашифровано**

  Проверяет, зашифровано ли устройство.

  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**). Также для аппаратного шифрования на устройстве должно быть установлено значение **На уровне блоков и файлов** (этот параметр можно проверить в свойствах устройства: в дереве консоли выберите **Управление мобильными устройствами** > **Мобильные устройства** и дважды щелкните мышью по нужному устройству).

- **SIM-карта заменена**

  Проверяет, была ли SIM-карта устройства заменена, вставлена или извлечена относительно предыдущего состояния проверки.

  Вы также можете включить проверку установки дополнительной SIM-карты.

На устройствах, совместимых с eSIM, обнаруженное несоответствие невозможно удалить, вставив ранее удаленную eSIM. Это связано с тем, что операционная система устройства распознает каждую добавленную карту eSIM как новую. В этом случае вам необходимо удалить правило Контроля соответствия из политики.

- **Не синхронизировалось дольше, чем**

  Проверяет, как давно устройство синхронизировалось с Сервером администрирования последний раз.

  Для этого критерия укажите максимальное время с момента последней синхронизации и выберите единицы измерения (**часы** или **дни**).

  Мы не рекомендуем указывать значение меньше значения параметра **Частота обновления информации об устройстве** в настройках Сервера iOS MDM.

Если указаны противоречащие друг другу критерии (например, в поле **Тип устройства** указано значение **iPhone**, выбран оператор **Входит в список**, а в списке значений **Модель устройства** указана модель iPad), отобразится сообщение об ошибке. Такое правило сохранить невозможно.

8. На закладке **Действия** укажите действия, которые будут выполняться на устройстве при обнаружении всех указанных критериев несоответствия.

   Действия выполняются во время проверки соблюдения правил соответствия (1 раз в 40 минут) до следующей синхронизации с Сервером администрирования. Чтобы одно и то же несоответствие не обнаруживалось при каждом выполнении повторяющихся действий, в настройках Сервера iOS MDM для параметра **Частота обновления информации об устройстве** установите значение 30 минут.

   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. При необходимости можно отредактировать заданный по умолчанию текст сообщения электронной почты.

   - **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**.

   - **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.

Когда критерии несоответствия правилу перестанут обнаруживаться на устройстве, можно отменить действие, отправив устройству соответствующую команду.

- **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.

  Когда критерии несоответствия правилу перестанут обнаруживаться на устройстве, можно отменить действие, отправив устройству соответствующую команду.

- **Удалить все профили**

  Все ранее установленные конфигурационные профили будут удалены с устройства.

  Когда критерии несоответствия правилу перестанут обнаруживаться на устройстве, можно установить удаленные конфигурационные профили один за другим, отправив устройству соответствующую команду.

- **Обновить ОС**

  Операционная система устройства обновлена.

  Для этого действия необходимо выбрать конкретную операцию (**Загрузить и установить**, **Только загрузить** или **Только установить**, чтобы установить ранее загруженную версию) и версию iOS для загрузки и/или установки.

- **Изменить настройки Bluetooth (только для supervised)**

  Для этого действия необходимо выбрать, требуется ли включить или отключить Bluetooth на устройстве.

  Когда критерии несоответствия правилу перестанут обнаруживаться на устройстве, можно отменить действие, отправив устройству соответствующую команду.

- **Сбросить настройки до заводских**

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

- **Удалить управляемое приложение**

  Для этого действия необходимо указать идентификатор пакета управляемого приложения, которое требуется удалить с устройства. Приложение считается управляемым, если оно установлено на устройство с помощью Kaspersky Security Center. **Как получить идентификатор пакета приложения**

Чтобы получить идентификатор пакета предустановленного приложения на iPhone или iPad,

Следуйте инструкциям в документации Apple.

Чтобы получить идентификатор пакета любого приложения для iPhone или iPad:

1. Откройте App Store.
2. Найдите нужное приложение и откройте его страницу.

   URL приложения оканчивается его числовым идентификатором (например, https://apps.apple.com/us/app/google-chrome/id**535886823**).
3. Скопируйте этот идентификатор (без букв "id").
4. Откройте страницу https://itunes.apple.com/lookup?id=<скопированный идентификатор>.

   Будет загружен текстовый файл.
5. Откройте загруженный файл и найдите в нем "bundleId".

Текст, следующий за "bundleId" – идентификатор пакета необходимого приложения.

Чтобы получить идентификатор пакета приложения, которое было добавлено в Kaspersky Security Center:

1. В дереве консоли Kaspersky Security Center выберите **Дополнительно** > **Удаленная установка** > **Инсталляционные пакеты**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Управление пакетами мобильных приложений**.

   В открывшемся окне **Управление пакетами мобильных приложений** в столбце **Название приложения** отображаются идентификаторы управляемых приложений.

   Если пакет приложения представлен файлом в формате .apk или .ipa, и необходимо узнать идентификатор приложения, можно добавить этот пакет приложения в окне **Управление пакетами мобильных приложений**, нажав на кнопку **Новый** и следуя инструкциям на экране.

Когда критерии несоответствия правилу перестанут обнаруживаться на устройстве, можно отменить действие, отправив устройству соответствующую команду.

- **Удалить все управляемые приложения**

  Все управляемые приложения удаляются с устройства. Приложение считается управляемым, если оно установлено на устройство с помощью Kaspersky Security Center.

  Когда критерии несоответствия правилу перестанут обнаруживаться на устройстве, можно установить удаленные приложения одно за другим, отправив устройству соответствующую команду.

- **Удалить профиль(и) указанного типа**

  Для этого действия необходимо выбрать тип профиля, удаляемого с устройства (например, **Веб-клипы** или **Подписки на календари**).

  Как только критерии несоответствия правилу перестанут обнаруживаться на устройстве, удаленные профили автоматически восстановятся.

- **Изменить параметры роуминга**

  Для этого действия необходимо выбрать, требуется ли включить или отключить роуминг данных на устройстве.

  Когда критерии несоответствия правилу перестанут обнаруживаться на устройстве, можно отменить действие, отправив устройству соответствующую команду.

Если указаны противоречащие друг другу действия (например, **Включить Bluetooth** и **Отключить Bluetooth** одновременно), отобразится сообщение об ошибке. Такое правило сохранить невозможно.

9. Нажмите на кнопку **OK**, чтобы сохранить правило и закрыть мастер.

   Новое правило появится в списке в разделе **Правила Контроля соответствия**.

10. В блоке **Действия при удалении пользователей из Active Directory** можно выбрать действия, которые будут выполняться на устройствах при удалении пользователей из Active Directory.

    Для этих настроек необходима интеграция с Microsoft Active Directory.

    Чтобы включить автоматическое удаление данных с устройств, связанных с неактивными учетными записями пользователей Active Directory, установите флажок **Удалять данные неактивных пользователей Active Directory** и выберите одно из следующих действий:

    - **Удалить корпоративные данные**
    - **Сбросить настройки до заводских**

    Если вы используете профили политики, убедитесь, что вы выставили опцию удаления данных на всю политику. После удаления пользователя из Active Directory он в первую очередь удалится из группы пользователей Active Directory. Из-за того что профиль политики перестанет действовать на аккаунт пользователя, данные не удалятся с устройства.

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

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

Контроль приложений

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

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.

   В течение 15 минут выполните следующие действия. По истечении этого времени при сохранении изменений политики может возникнуть ошибка.

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.

   Перед удалением Kaspersky Endpoint Security для Android с устройства снимите этот флажок или выключите Контроль приложений.

9. Сформируйте список категорий и приложений для настройки запуска приложений.

   В список можно добавить пакеты мобильных приложений, ранее созданные в Kaspersky Security Center.
   Как получить имя пакета приложения

   Чтобы получить имя пакета приложения:

   1. Откройте Google Play.
   2. Найдите нужное приложение и откройте его страницу.

      URL приложения оканчивается именем пакета приложения (например, https://play.google.com/store/apps/details?id=**com.android.chrome**).

   Чтобы получить имя пакета приложения, которое было добавлено в Kaspersky Security Center:

   1. В дереве консоли Kaspersky Security Center выберите **Дополнительно** > **Удаленная установка** > **Инсталляционные пакеты**.
   2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Управление пакетами мобильных приложений**.

      В открывшемся окне **Управление пакетами мобильных приложений** в столбце **Название приложения** отображаются идентификаторы управляемых приложений.

      Если пакет приложения представлен файлом в формате APK, и необходимо узнать идентификатор приложения, можно добавить этот пакет приложения в окне **Управление пакетами мобильных приложений**, нажав на кнопку **Новый** и следуя инструкциям на экране.

   Подробную информацию о категориях приложений см. в Приложении.

   Список приложений, которые входят в каждую категорию, приведен на сайте "Лаборатории Касперского".

10. Если вы хотите, чтобы Kaspersky Endpoint Security для Android сформировал отчет об установленных приложениях, то в блоке **Отчет об установленных мобильных приложениях** установите флажок **Отправлять данные об установленных приложениях**, чтобы отправлять информацию о приложениях, установленных на мобильных устройствах, и при необходимости укажите следующие параметры:

    - Чтобы отправлять данные о системных приложениях, установленных на устройствах пользователей, на Сервер администрирования, установите флажок **Отправлять данные о системных приложениях**.
    - Чтобы отправлять данные о служебных приложениях, установленных на устройствах пользователей, на Сервер администрирования, установите флажок **Отправлять данные о служебных приложениях**.

    Если системное или служебное приложение настроено в параметрах **Контроля приложений**, данные отправляются независимо от состояния флажков **Отправлять данные о системных приложениях** или **Отправлять данные о служебных приложениях** соответственно.

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

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

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

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 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 **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. Укажите значение `com.apple.webapp`, чтобы разрешить все веб-клипы. **Как получить идентификатор пакета приложения**

   Чтобы получить идентификатор пакета предустановленного приложения на iPhone или iPad,

   Следуйте инструкциям в документации Apple.

   Чтобы получить идентификатор пакета любого приложения для iPhone или iPad:

   1. Откройте App Store.
   2. Найдите нужное приложение и откройте его страницу.

      URL приложения оканчивается его числовым идентификатором (например, https://apps.apple.com/us/app/google-chrome/id**535886823**).
   3. Скопируйте этот идентификатор (без букв "id").
   4. Откройте страницу https://itunes.apple.com/lookup?id=<скопированный идентификатор>.

      Будет загружен текстовый файл.
   5. Откройте загруженный файл и найдите в нем "bundleId".

   Текст, следующий за "bundleId" – идентификатор пакета необходимого приложения.

   Чтобы получить идентификатор пакета приложения, которое было добавлено в Kaspersky Security Center:

   1. В дереве консоли Kaspersky Security Center выберите **Дополнительно** > **Удаленная установка** > **Инсталляционные пакеты**.
   2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Управление пакетами мобильных приложений**.

   В открывшемся окне **Управление пакетами мобильных приложений** в столбце **Название приложения** отображаются идентификаторы управляемых приложений.

   Если пакет приложения представлен файлом в формате .apk или .ipa, и необходимо узнать идентификатор приложения, можно добавить этот пакет приложения в окне **Управление пакетами мобильных приложений**, нажав на кнопку **Новый** и следуя инструкциям на экране.
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. Укажите значение `com.apple.webapp`, чтобы запретить все веб-клипы. **Как получить идентификатор пакета приложения**

Чтобы получить идентификатор пакета предустановленного приложения на iPhone или iPad,

Следуйте инструкциям в документации Apple.

Чтобы получить идентификатор пакета любого приложения для iPhone или iPad:

1. Откройте App Store.
2. Найдите нужное приложение и откройте его страницу.

   URL приложения оканчивается его числовым идентификатором (например, https://apps.apple.com/us/app/google-chrome/id**535886823**).
3. Скопируйте этот идентификатор (без букв "id").
4. Откройте страницу https://itunes.apple.com/lookup?id=<скопированный идентификатор>.

   Будет загружен текстовый файл.
5. Откройте загруженный файл и найдите в нем "bundleId".

Текст, следующий за "bundleId" – идентификатор пакета необходимого приложения.

Чтобы получить идентификатор пакета приложения, которое было добавлено в Kaspersky Security Center:

1. В дереве консоли Kaspersky Security Center выберите **Дополнительно** > **Удаленная установка** > **Инсталляционные пакеты**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Управление пакетами мобильных приложений**.

   В открывшемся окне **Управление пакетами мобильных приложений** в столбце **Название приложения** отображаются идентификаторы управляемых приложений.

   Если пакет приложения представлен файлом в формате .apk или .ipa, и необходимо узнать идентификатор приложения, можно добавить этот пакет приложения в окне **Управление пакетами мобильных приложений**, нажав на кнопку **Новый** и следуя инструкциям на экране.

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.

Статусы мобильных устройств

Статусы мобильных устройств, определяемые Kaspersky Security Center

В Консоли администрирования можно быстро оценить текущее состояние Kaspersky Security Center и управляемых устройств с помощью цветовых индикаторов. Цветовые индикаторы расположены в рабочей области **Сервера администрирования** в папке **Управление мобильными устройствами** в подпапке **Мобильные устройства**. В рабочей области этой подпапки отображается таблица управляемых мобильных устройств.

Цветовой индикатор - это цветной значок в столбце **Управление** таблицы. Каждый индикатор может быть одного из этих цветов (см. таблицу *Цветовые кодировки индикаторов*). Цвет индикатора зависит от текущего состояния Kaspersky Security Center и от зарегистрированных событий.

Устройство может иметь один из следующих статусов: **OK**, **Критический** или **Предупреждение**.

Статусы присваиваются и отправляются в Kaspersky Security Center в соответствии со следующими требованиями:

- На устройстве обнаружена одна причина для присвоения статуса — устройству присваивается статус, отображающийся в списке управляемых устройств.
- На устройстве обнаружено несколько причин для присвоения статуса — Kaspersky Secure Mobility Management выбирает наиболее критический статус и присваивает его.
- На устройстве не обнаружено причин для присвоения статуса — Kaspersky Secure Mobility Management не отправляет структуру статусов в Kaspersky Security Center, присваивается статус *OK*.

Цветовые кодировки индикаторов

Значок	Состояние	Значение цвета индикатора
	Голубой Мобильное устройство, обнаруженное в сети и не входящее в состав какой-либо группы администрирования.	Зарегистрированы события, не связанные с угрозами для безопасности управляемых устройств.
	Зеленый Мобильное устройство, входящее в состав группы администрирования, со статусом **OK**.	Вмешательство администратора не требуется.
	Желтый Мобильное устройство, входящее в состав группы администрирования, со статусом **Предупреждение**.	Зарегистрированы события, не связанные с угрозами для безопасности управляемых устройств.
	Красный Мобильное устройство, входящее в состав группы администрирования, со статусом **Критический**.	Имеются серьезные проблемы. Требуется вмешательство администратора для их решения.
	Мобильное устройство, входящее в состав группы администрирования, соединение которого с Сервером администрирования потеряно.	Может быть любого цвета: голубой, зеленый, желтый, красный.

Задача администратора - сделать так, чтобы цветовые индикаторы оставались зелеными на всех устройствах.

Вы можете выбрать **Свойства** в контекстном меню мобильного устройства, а затем перейти в раздел **Защита**, чтобы просмотреть зарегистрированные события, влияющие на цветовые индикаторы и состояние Kaspersky Security Center (см. таблицу *Название, описание и цвет индикатора зарегистрированных событий*).

Название, описание и цвет индикатора зарегистрированных событий

Цвет индикатора	Отображаемое имя типа события	Описание
Красный	**Количество устройств, на которых срок действия лицензии истек: %1**	События этого типа возникают, если срок действия коммерческой лицензии окончен. Один раз в день Kaspersky Security Center проверяет, не истек ли срок действия лицензии. После окончания срока действия коммерческой лицензии, Kaspersky Security Center работает в режиме базовой функциональности.

		Чтобы продолжить использование Kaspersky Security Center, продлите срок действия коммерческой лицензии.
Красный	**Устройств с незапущенной программой безопасности: %1** Это не относится к iOS MDM-устройствам.	События этого типа возникают, когда программа безопасности, установленная на устройстве, не запущена. Убедитесь, что на устройстве запущена программа Kaspersky Endpoint Security.
Красный	**Устройств с выключенной защитой: %1**	События такого типа возникают, когда программа защиты на устройстве отключена больше указанного времени. Проверьте текущий статус постоянной защиты на устройстве и убедитесь, что все необходимые вам компоненты защиты включены.
Красный	**На Сервере администрирования зарегистрированы критические события**	События этого типа возникают при обнаружении критических событий Сервера администрирования. Проверьте список событий, хранящихся на Сервере администрирования, а затем последовательно исправьте критические события.
Красный	**На Сервере администрирования зарегистрированы ошибки в событиях**	События этого типа возникают при регистрации непредвиденных ошибок на стороне Сервера администрирования. Проверьте список событий, хранящихся на Сервере администрирования, а затем последовательно исправьте критические события.
Красный	**Потеряно соединение с устройствами: %1**	События этого типа возникают при потере соединения между Сервером администрирования и устройством. Просмотрите список отключенных устройств и попробуйте подключить их снова.
Красный	**Устройств, которые давно не соединялись с Сервером администрирования: %1**	События этого типа возникают, когда устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено. Убедитесь, что устройство включено и запущен Агент администрирования.
Красный	**Базы устарели: %1 устройств**	События этого типа возникают, когда базы вредоносного ПО на устройстве не обновлялись в течение заданного интервала времени. Следуйте инструкциям, чтобы обновить антивирусные базы "Лаборатории Касперского".
Красный	**Количество устройств, на которых обнаружены активные угрозы: %1**	События этого типа возникают при обнаружении активных угроз на управляемых устройствах. Просмотрите информацию об обнаруженных угрозах и следуйте рекомендациям.
Красный	**Устройств, на которых обнаружено много вирусов: %1**	События этого типа возникают при обнаружении вирусов на управляемых устройствах. Просмотрите информацию об обнаруженных вирусах и следуйте рекомендациям.
Красный	**Вирусная атака**	События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения. Просмотрите информацию об обнаруженных угрозах и следуйте рекомендациям.
Желтый	**Давно не выполнялся поиск вредоносного ПО на устройствах: %1**	События этого типа возникают, когда вам нужно выполнить поиск вредоносного ПО на управляемых устройствах. Запустите поиск вирусов.
Зеленый	**Управляемых устройств: %3. Обнаружено нераспределенных устройств: %1**	События этого типа возникают при обнаружении новых устройств в группах администрирования.
Зеленый	**Программа безопасности установлена на всех управляемых устройствах**	События этого типа возникают, когда программа Kaspersky Endpoint Security установлена на всех управляемых устройствах.
Зеленый	**Kaspersky Security Center функционирует нормально.**	События этого типа возникают при правильной работе Kaspersky Security Center.
Зеленый	**Защита включена**	События этого типа возникают, когда на управляемых устройствах включена постоянная защита.
Зеленый	**Не установлена программа безопасности**	События этого типа возникают, когда программа, защищающая от вредоносного ПО, не установлена на управляемых устройствах.
Зеленый	**Поиск вредоносного ПО проводится по расписанию**	События этого типа возникают, когда задача *Поиска вредоносного ПО* выполняется по расписанию.

Голубой	**Не принято Лицензионное соглашение мобильных приложений "Лаборатории Касперского"**	События этого типа возникают, когда администратор еще не принял Лицензионное соглашение мобильных приложений "Лаборатории Касперского".
Голубой	**Не принято Лицензионное соглашение для обновлений программ "Лаборатории Касперского"**	События этого типа возникают, когда администратор еще не принял Лицензионное соглашение обновлений программ "Лаборатории Касперского".
Голубой	**Положение о Kaspersky Security Network для обновлений программ "Лаборатории Касперского" не принято**	События этого типа возникают, когда администратор еще не принял Положение о Kaspersky Security Network для обновлений программ "Лаборатории Касперского".
Голубой	**Есть новые версии программ "Лаборатории Касперского"**	События этого типа возникают, когда новые версии программ "Лаборатории Касперского" доступны для установки на управляемые устройства.
Голубой	**Есть обновления для программ "Лаборатории Касперского"**	События этого типа возникают, когда доступны обновления для программ "Лаборатории Касперского".
Голубой	**Устройств, на которых полная проверка ни разу не проводилась: %1**	События этого типа возникают, когда полная проверка никогда не выполнялась на указанном количестве устройств.

Статусы мобильных устройств, определяемые Kaspersky Secure Mobility Management

Это дополнительные статусы, которые функционируют вместе со статусами, определенными Kaspersky Security Center (см. таблицу *Название, описание и цвет индикатора зарегистрированных событий*).

Kaspersky Secure Mobility Management определяет статус мобильных устройств на основе параметров политики, а затем отправляет структуру статусов в Kaspersky Security Center при синхронизации. Администратор может изменить статус устройства в политике в зависимости от уровня серьезности условия (см. таблицу *Значения по умолчанию, причины и условия для присвоения статуса*). В этом случае заданное администратором значение имеет приоритет над значением по умолчанию, заданным Kaspersky Secure Mobility Management.

Значения по умолчанию, причины и условия присвоения статуса

Условие	Причина присвоения статуса	Значение по умолчанию
Постоянная защита не работает.	Одна из следующих причин: • Доступ для управления всеми файлами не предоставлен. • Kaspersky Security Network выключен.	*Критический*
Веб-Фильтр не работает.	Одна из следующих причин: • Разрешение Специальные возможности не предоставлено. • Веб-Фильтр выключен пользователем в параметрах Kaspersky Endpoint Security. • Разрешение Игнорировать оптимизацию батареи не предоставлено. • Не принято соглашение для Веб-Контроля.	*Предупреждение*
Контроль приложений не работает.	Разрешение Специальные возможности не предоставлено.	*Предупреждение*
Блокирование устройства недоступно.	Одна из следующих причин: • Разрешение Администратор устройства не предоставлено. • Разрешение Специальные возможности не предоставлено.	*Предупреждение*
Определение местоположения устройства недоступно.	Одна из следующих причин: • Разрешение Местоположение не предоставлено. • Местоположение устройства не может быть определено (при наличии разрешения).	*Предупреждение*
Версии Положения о KSN не совпадают.	Версия Положения о Kaspersky Security Network, принятого пользователем в политике, и версия Положения о Kaspersky Security Network на устройстве не совпадают.	*Предупреждение*
Версии Маркетингового положения не совпадают.	Версия Положения об обработке данных в маркетинговых целях, принятого пользователем в политике, и версия Положения об обработке данных в маркетинговых целях на устройстве не совпадают.	*ОК*

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.

   В течение 15 минут выполните следующие действия. По истечении этого времени при сохранении изменений политики может возникнуть ошибка.

4. В окне **Свойства: <Название политики>** выберите раздел **Контроль приложений**.
5. В разделе **Отчет об установленных мобильных приложениях** установите флажок **Отправлять данные об установленных приложениях**.
6. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Kaspersky Security Center. Kaspersky Endpoint Security для Android отправляет данные в журнал событий каждый раз после установки или удаления приложения с устройства.

Настройка отображения Android-устройств в Kaspersky Security Center

Для удобства работы со списком мобильных устройств следует настроить параметры отображения устройства в Kaspersky Security Center. По умолчанию список мобильных устройств отображается в дереве консоли **Дополнительно → Управление мобильными устройствами → Мобильные устройства**. Информация об устройстве обновляется автоматически. Вы также можете обновить список мобильных устройств вручную по кнопке **Обновить** в правом верхнем углу.

После подключения устройства к Kaspersky Security Center оно автоматически добавляется в список мобильных устройств. В списке мобильных устройств может содержаться подробная информация об устройстве: модель, операционная система, IP-адрес и другие данные.

Вы можете настроить формат имени устройства, а также выбрать статус устройства. Статус устройства информирует 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.

   В течение 15 минут выполните следующие действия. По истечении этого времени при сохранении изменений политики может возникнуть ошибка.

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 формирует из данных, полученных от устройства, следующим образом:

   - На персональных устройствах с Android версии 9 и ниже приложение использует IMEI. Для более поздних версий Android приложение использует SSAID (идентификатор Android) или контрольную сумму других данных, полученных от устройства.
   - В режиме device owner приложение использует IMEI для всех версий Android.
   - При создании рабочего профиля на устройствах с Android версии 11 и ниже приложение использует IMEI. Для других версий Android приложение использует SSAID (идентификатор Android) или контрольную сумму других данных, полученных от устройства.

6. Установите атрибут "замок" в закрытое положение ( ).
7. В блоке **Статус устройства в Kaspersky Security Center** выберите статус устройства, если не работает компонент Kaspersky Endpoint Security для Android: (**Критический**), (**Предупреждение**) или (**ОК**).

   В списке мобильных устройств статус устройства будет изменен в соответствии с выбранным статусом.

8. Установите атрибут "замок" в закрытое положение.
9. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

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

Защита

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

Настройка защиты от вредоносного ПО на Android-устройствах

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

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.

Защита от вредоносного ПО имеет ряд ограничений:

- При работе Защиты от вредоносного ПО в рабочем профиле 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.
- На устройствах с операционной системой Android 11 или 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.

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.

   В течение 15 минут выполните следующие действия. По истечении этого времени при сохранении изменений политики может возникнуть ошибка.

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

5. В блоке **Защита** настройте параметры защиты файловой системы мобильного устройства:

- Чтобы включить постоянную защиту мобильного устройства пользователя от угроз, установите флажок **Включить защиту**.

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

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

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

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

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

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

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

- **Удалить**

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

- **Пропустить**

  > Если обнаруженные объекты были пропущены, Kaspersky Endpoint Security для Android предупреждает пользователя о проблемах в защите устройства. 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 изменены после очередной синхронизации устройства с Kaspersky Security Center.

Чтобы настроить автоматический запуск проверки на наличие вредоносного ПО 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.

   В течение 15 минут выполните следующие действия. По истечении этого времени при сохранении изменений политики может возникнуть ошибка.

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

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

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

   - **Удалить**

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

   - **Пропустить**

     Если обнаруженные объекты были пропущены, Kaspersky Endpoint Security для Android предупреждает пользователя о проблемах в защите устройства. 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 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.

Если во время проверки Kaspersky Endpoint Security для Android обнаруживает на устройствах пользователей вредоносные программы, действия различаются **в зависимости от режима управления устройством.**

В режиме device owner установленные вредоносные программы, обнаруженные Kaspersky Endpoint Security для Android, автоматически удаляются с устройства, если выбран параметр **Удалить**. Если Kaspersky Endpoint Security для Android обнаруживает вредоносные системные программы, их показ и запуск на устройствах пользователей запрещены.

В рабочем профиле Android установленные вредоносные программы, обнаруженные Kaspersky Endpoint Security для Android, не удаляются, их показ и запуск на устройствах пользователей запрещены без уведомления пользователей.

Однако, если выбран вариант **Запросить действие**, Kaspersky Endpoint Security для Android предлагает пользователям выбрать действие для каждого обнаруженного приложения как на устройствах в режиме device owner, так и на устройствах с созданным рабочим профилем Android.

Установленные вредоносные программы нельзя сохранить в карантине. Таким образом, если выбран параметр **Карантин**, обнаруженная вредоносная программа удаляется.

На личных устройствах обнаруженные вредоносные программы не могут быть удалены автоматически. В этом случае Kaspersky Endpoint Security для Android предлагает пользователю удалить или пропустить обнаруженную программу.

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.

   Если устройство находится в режиме экономии заряда батареи, приложение может выполнить эту задачу позже, чем указано. Для своевременного реагирования KES-устройств под управлением Android на команды администратора, следует включить использование сервиса Firebase Cloud Messaging.

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 баз вредоносного ПО.

По умолчанию обновление баз вредоносного ПО в зоне роуминга выключено. Обновление баз вредоносного ПО по расписанию не выполняется.

Чтобы настроить параметры обновления баз вредоносного ПО, 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 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 баз вредоносного ПО в роуминге вручную.

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

   - **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 баз вредоносного ПО на устройстве пользователя. Для этого нажмите на кнопку **Расписание** и в открывшемся окне **Расписание** задайте периодичность и время запуска обновления.

   Если устройство находится в режиме экономии заряда батареи, приложение может выполнить эту задачу позже, чем указано. Для своевременного реагирования KES-устройств под управлением Android на команды администратора, следует включить использование сервиса Firebase Cloud Messaging.

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

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

Защита Android-устройств в интернете

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

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

Веб-Фильтр на Android-устройствах поддерживается только браузерами Google Chrome, HUAWEI Browser, Samsung Internet и Яндекс Браузер.

Если приложение Kaspersky Endpoint Security для Android в режиме device owner не установлено в качестве службы Специальных возможностей, Веб-Фильтр поддерживается только браузером Google Chrome и проверяет только домен сайта. Чтобы Веб-Фильтр поддерживался другими браузерами (Samsung Internet Browser, Яндекс Браузер и HUAWEI Browser), приложение Kaspersky Endpoint Security должно быть включено в качестве службы Специальных возможностей. Это также позволит использовать функцию Custom Tabs.

Функция Custom Tabs поддерживается браузерами Google Chrome, HUAWEI Browser и Samsung Internet Browser.

В браузерах HUAWEI Browser, Samsung Internet Browser и Яндекс Браузер Веб-Фильтр не блокирует сайты на мобильном устройстве, если используется рабочий профиль и установлен флажок Включить Веб-Фильтр только в рабочем профиле.

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.

   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 **Веб-Фильтр**.
5. Для использования Веб-Фильтра вам или пользователю устройства необходимо прочитать Положение об обработке данных в целях использования Веб-Фильтра (Положение о Веб-Фильтре) и принять его условия. Для этого:

   a. Нажмите на ссылку **Положение о Веб-Фильтре** в верхней части раздела.

      Откроется окно **Положение об обработке данных в целях использования Веб-Фильтра**.

   b. Прочитайте Политику конфиденциальности и примите ее условия, установив соответствующий флажок. Для того чтобы ознакомиться с Политикой конфиденциальности, необходимо перейти по

ссылке Политика 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.

d. Нажмите на кнопку **OK**, чтобы закрыть окно.

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

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

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

Защита данных при потере или краже устройств

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

Отправка команд на утерянное или украденное мобильное устройство

Для защиты данных на мобильном устройстве в случае его потери или кражи вы можете отправить специальные команды.

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 (см. таблицу ниже).

Команды для Android-устройств

Команды для защиты данных при потере или краже Android-устройства

Команда	Результат выполнения команды
Заблокировать	Мобильное устройство заблокировано. Для получения доступа к данным необходимо разблокировать устройство.

Разблокировать	Мобильное устройство разблокировано. После разблокировки устройства под управлением операционной системы Android 5.0–6 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. Чтобы посмотреть местоположение устройства на карте, перейдите в папку **Управление мобильными устройствами → Мобильные устройства**. Затем в контекстном меню устройства выберите **Все команды → Определить местоположение → Посмотреть координаты 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. Если на устройстве Android отключена служба Google "Точность местоположения", команда **Определить местоположение устройства** работать не будет. Обращаем внимание, что не на всех устройствах Android есть эта служба.
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 данные приложения	Данные указанного приложения удалены с мобильного устройства. Действие применимо только к устройствам с Android 9 или выше в режиме device owner или с установленным рабочим профилем Android. Для выполнения действия необходимо указать имя пакета приложения, данные которого должны быть удалены. Как получить имя пакета приложения В результате выполнения команды приложение возвращается в состояние по умолчанию. Данные системных приложений и приложений-администраторов не удаляются.

	Чтобы получить имя пакета приложения: 1. Откройте Google Play. 2. Найдите нужное приложение и откройте его страницу. URL приложения оканчивается именем пакета приложения (например, https://play.google.com/store/apps/details?id=**com.android.chrome**). *Чтобы получить имя пакета приложения, которое было добавлено в Kaspersky Security Center:* 1. В дереве консоли Kaspersky Security Center выберите **Дополнительно** > **Удаленная установка** > **Инсталляционные пакеты**. 2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Управление пакетами мобильных приложений**. В открывшемся окне **Управление пакетами мобильных приложений** в столбце **Название приложения** отображаются идентификаторы управляемых приложений. Если пакет приложения представлен файлом в формате APK, и необходимо узнать идентификатор приложения, можно добавить этот пакет приложения в окне **Управление пакетами мобильных приложений**, нажав на кнопку **Новый** и следуя инструкциям на экране.
Удалить данные всех приложений	Данные всех приложений удалены с мобильного устройства. Действие применимо только к устройствам с Android 9 или выше в режиме device owner или с установленным рабочим профилем Android. Если устройство работает в режиме device owner, данные всех приложений на устройстве удалены. Если на устройстве создан рабочий профиль Android, данные всех приложений в рабочем профиле удалены. В результате выполнения команды приложения возвращаются в состояние по умолчанию. Данные системных приложений и приложений-администраторов не удаляются.
Удалить корпоративные данные	Корпоративные данные удалены с устройства. Перечень удаленных данных зависит от режима работы устройства. • На личном устройстве удалены KNOX-контейнер и почтовый сертификат. • Если устройство работает в режиме device owner, удалены KNOX-контейнер и сертификаты, установленные приложением Kaspersky Endpoint Security для Android (почтовые и VPN-сертификаты, сертификаты, полученные через профили SCEP, кроме мобильных сертификатов). • Дополнительно, если установлен рабочий профиль Android, удален рабочий профиль (содержимое, настройки и ограничения) и сертификаты, установленные в рабочем профиле (почтовые и VPN-сертификаты, сертификаты, полученные через профили SCEP, кроме мобильных сертификатов).
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. На устройствах под управлением Android 14 или выше эта реакция применяется только в том случае, если устройство работает в режиме device owner.
Получить историю местоположений	Отображается история местоположений мобильного устройства за последние 14 дней.

устройства	Чтобы посмотреть местоположение устройства на карте, перейдите в папку **Управление мобильными устройствами → Мобильные устройства**. Затем в контекстном меню устройства выберите **Все команды → Получить историю местоположений устройства → Посмотреть на карте**. Эта команда работает только в том случае, если в базе Сервера администрирования хранится тип информационного события **История местоположений устройства**. События настраиваются в разделе **События** свойств политики. Дополнительная информация о событиях приведена в справке Kaspersky Security Center. Из-за технических ограничений на устройствах Android фактическое получение местоположения устройства может происходить реже, чем указано в разделе **Синхронизация** свойств политики.

Команды для iOS MDM-устройств

Команды для защиты данных при потере или краже iOS MDM-устройства

Команда	Результат выполнения команды
Заблокировать	Мобильное устройство заблокировано. Для получения доступа к данным необходимо разблокировать устройство.
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.
Включить режим пропажи (только для контролируемых устройств)	На контролируемом мобильном устройстве включен режим пропажи, устройство заблокировано. На экране устройства появилось сообщение и номер телефона, которые вы можете редактировать. Если вы отправите команду **Включить режим пропажи** на контролируемое устройство iOS MDM без SIM-карты и это устройство будет перезапущено, оно не сможет подключиться к сети Wi-Fi и получить команду **Отключить режим пропажи**. Эта проблема связана с особенностями iOS-устройств. Чтобы этого избежать, можно отправлять эту команду только на устройства с SIM-картой или вставить SIM-карту в заблокированное устройство – в этом случае оно сможет получить команду **Отключить режим пропажи** по мобильной сети.
Определить местоположение (только для контролируемых устройств)	Получены данные о местоположении устройства. Перейдите по ссылке в журнале команд, чтобы получить координаты устройства и посмотреть его местоположение на карте. Чтобы посмотреть местоположение устройства на карте, перейдите в папку **Управление мобильными устройствами → Мобильные устройства**. Затем в контекстном меню устройства выберите **Все команды → Определить местоположение → Посмотреть координаты устройства**. Эта команда доступна только для контролируемых устройств в режиме пропажи.
Воспроизвести звук (только для контролируемых устройств)	На потерянном мобильном устройстве воспроизводится звуковой сигнал. Эта команда доступна только для контролируемых устройств в режиме пропажи.
Отключить режим пропажи (только для контролируемых устройств)	На мобильном устройстве отключен режим пропажи, устройство разблокировано. Эта команда поддерживается только на устройствах в режиме supervised.

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 и выше необходимо предоставить разрешение "Всегда" для доступа к местоположению устройства. На устройствах с операционной системой Android 11 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 разделе "Отправка команд".

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 разделе "Отправка команд".

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 **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 разблокировано.

После разблокировки устройства под управлением операционной системы Android 5.0–6 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.

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**). Также для аппаратного шифрования на устройстве должно быть установлено значение **На уровне блоков и файлов** (этот параметр можно проверить в свойствах устройства: в дереве консоли выберите **Управление мобильными устройствами** > **Мобильные устройства** и дважды щелкните мышью по нужному устройству).

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 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**).

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.

   В течение 15 минут выполните следующие действия. По истечении этого времени при сохранении изменений политики может возникнуть ошибка.

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.

Настройка надежности пароля разблокировки устройства

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

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

Настройка надежности пароля разблокировки Android-устройства

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

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

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

Чтобы настроить использование пароля разблокировки, выполните следующие действия:

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

   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 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.

Следующие правила применимы только к личным и рабочим профилям:

- В личном профиле Kaspersky Endpoint Security сводит требования к надежности пароля к одному из системных значений: средний или высокий уровень для устройств под управлением Android 10 или выше.
- В рабочем профиле Kaspersky Endpoint Security сводит требования к надежности пароля к одному из системных значений: средний или высокий уровень для устройств под управлением Android 12 или выше.

Значения уровня надежности 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 сложности пароля (Android 12 или ниже в режиме device owner)

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.

- **Требования не заданы**

  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 (например, !@#$%)**
  - **Минимальное количество заглавных букв**
  - **Минимальное количество строчных букв**
  - **Минимальное количество небуквенных символов (например, 1^&*9)**

- **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 12 или 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.

Эта настройка применима к устройствам с любыми поддерживаемыми версиями Android. Начиная с Android 10, эта настройка применима только для режима device owner.

- **Количество дней, за которое уведомлять о необходимости смены 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 последних паролей, которые нельзя использовать в качестве нового пароля (все версии Android; Android 10 или выше в режиме device owner)

- **Период неактивности без блокировки экрана 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 после разблокировки биометрическими методами до ввода пароля, в минутах (Android 8.0 или выше в режиме device owner)**

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 8.0 или выше в режиме device owner.

- **Разрешить биометрические методы разблокировки (Android 9 или выше; Android 10 или выше в режиме device owner)**

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 или выше. Начиная с Android 10, эта настройка применима только для режима device owner.

- Разрешить использование отпечатков пальцев (все версии Android; Android 10 или выше в режиме device owner)

Использование отпечатков пальцев для разблокировки экрана.

Флажок не ограничивает использование сканера отпечатков пальцев при входе в приложения или подтверждении покупок.

Если флажок установлен, использование отпечатков пальцев на мобильном устройстве разрешено.

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 или выше; Android 10 или выше в режиме device owner)**.

По умолчанию флажок установлен.

Эта настройка применима к устройствам с любыми поддерживаемыми версиями Android. Начиная с Android 10, эта настройка применима только для режима device owner.

На некоторых устройствах Xiaomi рабочий профиль Android можно разблокировать с помощью отпечатка пальца только в том случае, если значение параметра **Период неактивности без блокировки экрана устройства** будет установлено после установки отпечатка пальца в качестве метода разблокировки экрана.

- Разрешить распознавание лица (Android 9 или выше; Android 10 или выше в режиме device owner)
- Разрешить распознавание по радужной оболочке глаза (Android 9 или выше; Android 10 или выше в режиме device owner)

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 или выше; Android 10 или выше в режиме device owner)**.

По умолчанию флажок установлен.

Этот параметр применим только для устройств под управлением Android 9 или выше. Начиная с Android 10, эта настройка применима только для режима device owner.

- **Разрешить загрузку устройства до запроса пароля**

Если флажок установлен, устройство запускается и загружает системные процессы и фоновые приложения до запроса пароля разблокировки у пользователя.

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 версий с 7.0 по 10 включительно этот параметр применим только к личным устройствам, на которых не установлен пароль.

На устройствах под управлением операционной системы Android 11 или 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 10 или ниже, Kaspersky Endpoint Security для Android сразу устанавливает пароль.
- Если устройство работает под управлением операционной системы Android 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 изменены после очередной синхронизации устройства с Kaspersky Security Center.

На некоторых устройствах HUAWEI появляется сообщение о слишком простом способе разблокировки экрана.

Чтобы установить правильный PIN-код на устройстве HUAWEI, пользователь должен выполнить следующие действия:

1. В сообщении о проблеме нажмите на кнопку **Изменить**.
2. Введите текущий PIN-код.
3. В окне **Настройте новый пароль** нажмите на кнопку **Изменение способа разблокировки**.
4. Выберите способ разблокировки **Персональный PIN-код**.
5. Установите новый PIN-код.

   PIN-код должен соответствовать требованиям политики.

На устройстве установлен правильный PIN-код.

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 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 **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**.
- Чтобы сделать использование пароля обязательным, установите флажок **Принудительно использовать пароль**. Если флажок снят, мобильное устройство можно использовать без пароля.
- В списке **Минимальное количество символов** выберите минимальную длину пароля в символах.
- В списке **Минимальное количество специальных символов** выберите минимальное количество специальных символов в пароле (например, "$", "&", "!").
- В поле **Максимальный срок использования** укажите период времени в днях, в течение которого будет действовать пароль. По истечении установленного срока Kaspersky Device Management для iOS запрашивает у пользователя смену пароля.
- В списке **Включать автоблокировку через** выберите время включения автоблокировки iOS MDM-устройства.
- В поле **История паролей** укажите количество использованных паролей (включая текущий), которые Kaspersky Device Management для iOS при смене пароля сравнивает с новым паролем. Если пароли совпадут, новый пароль не будет принят.
- В списке **Максимальное время для разблокировки без пароля** выберите время, в течение которого пользователь может разблокировать iOS MDM-устройство без ввода пароля.
- В списке **Максимальное количество попыток ввода** выберите число доступных пользователю попыток ввести пароль для разблокировки iOS MDM-устройства.

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

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

Настройка виртуальной частной сети (VPN)

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

Настройка VPN на Android-устройствах (только Samsung)

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

Настройка VPN возможна только для Samsung-устройств под управлением операционной системы Android 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.

   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 → 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 изменены после очередной синхронизации устройства с Kaspersky Security Center.

Настройка VPN на iOS MDM-устройствах

Для подключения iOS MDM-устройства к виртуальной частной сети (VPN) и обеспечения безопасности данных при подключении к сети VPN следует настроить параметры подключения к сети VPN. VPN-протоколы IKEv2 и IPSec также позволяют 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 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 **VPN**.

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

   Откроется окно **Конфигурация 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 iOS MDM-устройства 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 iOS MDM-устройства с помощью паролей MS-CHAP v2 и двухфакторную аутентификацию.

     Соединение PPTP больше не поддерживается.

   - **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 iOS MDM-устройство 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 iOS MDM-устройство 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 iOS MDM-устройство 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 iOS MDM-устройство приложение SonicWALL Mobile Connect из App Store.

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

- **Custom SSL**. Соединение поддерживает аутентификацию пользователя iOS MDM-устройства 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. При необходимости для подключения по протоколам **IKEv2** и **IPsec** настройте Per App VPN для поддерживаемых системных приложений (**электронная почта**, **календарь**, **Safari** и **контакты**). Подробную информацию см. в разделе Настройка Per App VPN на устройствах iOS MDM или в контекстной справке плагина управления.

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.

Настройка Per App VPN на устройствах iOS MDM

Per App VPN позволяет подключать устройства к сети VPN при запуске поддерживаемых системных приложений (электронная почта, календарь, Safari и контакты). Эта функция доступна при подключении по протоколам IKEv2 и IPSec.

Чтобы включить Per App VPN, выполните следующие действия:

1. Выполните первоначальную настройку VPN-соединения. Порядок предварительной настройки описан в разделе Настройка VPN на устройствах iOS MDM.

2. Установите флажок **Включить Per App VPN**.

Настройте Per App VPN для поддерживаемых системных приложений (электронная почта, календарь, Safari и контакты) в соответствующих разделах политики.

При установке флажка **Включить Per App VPN** становится доступен и по умолчанию установлен флажок **Включать VPN автоматически для системных приложений**. Это означает, что устройство автоматически активирует VPN-соединение, когда ассоциированные системные приложения инициируют передачу данных по сети.

*Чтобы указать конфигурацию Per App VPN для приложений **Электронная почта**, **Календарь** и **Контакты**:*

1. Перейдите в соответствующий раздел политики.

2. Нажмите **Добавить**, чтобы создать новую учетную запись, или выберите существующую из списка и нажмите **Изменить**.

3. В разделе **Настройки Per App VPN** установите флажок **Включить Per App VPN (iOS 14+)**.

4. Выберите эту конфигурацию Per App VPN из раскрывающегося списка **Выбрать конфигурацию Per App VPN** и нажмите **OK**, чтобы сохранить изменения.

*Чтобы указать конфигурацию Per App VPN для **Safari**:*

1. Перейдите в раздел политики **Safari**.

2. Нажмите на кнопку **Добавить**.

   Откроется окно **Добавление домена для Safari**.

3. Выберите эту конфигурацию Per App VPN из раскрывающегося списка **Выберите конфигурацию Per App VPN**.

4. В поле **Домен, для которого будет включаться VPN-соединение** укажите домен веб-сайта, который активирует VPN-соединение в Safari. Домен необходимо указывать в формате `"www.example.com"`.

5. Нажмите **OK**, чтобы добавить домен в список.

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.

   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 → Управление Samsung-устройством**.
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 на кнопку **ОК**.
8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

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

Защита Kaspersky Endpoint Security для Android от удаления

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

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

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

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

   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 **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 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 изменены после очередной синхронизации устройства с Kaspersky Security Center. При попытке удаления приложения мобильное устройство будет заблокировано.

Обнаружение взлома устройства (получение root-прав)

Kaspersky Secure Mobility Management 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.

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).

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. Для этого в параметрах правила соответствия требуется выбрать критерий **На устройстве получены root-права**.

Настройка глобального HTTP-прокси на iOS MDM-устройствах

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

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

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

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

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 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 **Сертификаты**.
5. В блоке **Сертификаты** нажмите на кнопку **Добавить**.

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

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

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

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

Добавление профиля SCEP на iOS MDM-устройства

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

По умолчанию добавляется профиль SCEP со следующими параметрами:

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

Вы можете изменить указанные параметры при добавлении профиля SCEP.

Чтобы добавить профиль SCEP, выполните следующие действия:

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

   - **Не задан** – 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 iOS MDM-устройства.

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 iOS MDM-устройства 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 **OK**.

    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.

Настройка ограничений на использование SD-карт (только для устройств Samsung)

В параметрах SD-карты настройте возможности контроля за использованием SD-карты на мобильном устройстве пользователя.

Чтобы ограничить использование SD-карты 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.

    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** → **Управление Samsung-устройством**.

5. В разделе **Параметры SD-карты** укажите необходимые ограничения:

    - Разрешить доступ к SD-карте

Этот параметр применим для устройств с Android 5.0-12.

Установка или снятие этого флажка определяет, включен или отключен доступ к SD-карте на устройстве.

По умолчанию флажок установлен.

- **Разрешить запись на SD-карту**

  Установка или снятие этого флажка определяет, включена или отключена запись на SD-карту на устройстве.

  По умолчанию флажок установлен.

- **Разрешить перенос приложений на SD-карту**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства перемещать приложения на SD-карту.

  По умолчанию флажок установлен.

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

Параметры SD-карты настроены.

Управление мобильными устройствами

Этот раздел содержит информацию о том, как удаленно управлять мобильными устройствами в Консоли администрирования Kaspersky Security Center.

Управление KES-устройствами

В Kaspersky Security Center вы можете управлять KES-устройствами следующими способами:

- централизованно управлять KES-устройствами с помощью команд;
- просматривать информацию о параметрах управления KES-устройствами;
- устанавливать приложения с помощью пакетов мобильных приложений;
- отключать KES-устройства от управления.

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

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.

   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 **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 трансляцию, запись и снимки экрана**

Установка или снятие флажка определяет, разрешено ли пользователю устройства делать снимки экрана, а также записывать и демонстрировать экран устройства. Помимо этого установка или снятие флажка определяет, разрешен ли захват экрана в целях работы искусственного интеллекта.

По умолчанию флажок снят.

- Запретить изменение языка (Android 9 или выше)

  Установка или снятие флажка определяет, разрешено ли пользователю устройства изменять язык устройства.

  Ограничение поддерживается на устройствах с Android 9 или выше.

  По умолчанию флажок снят.

  На некоторых устройствах (например, Xiaomi, TECNO и Realme) под управлением Android 9 или выше после установки флажка **Запретить изменение языка** в режиме device owner пользователь по-прежнему может изменить язык, при этом предупреждающее сообщение не отобразится.

- Запретить изменение даты, времени и часового пояса (Android 9 или выше)

  Установка или снятие флажка определяет, разрешено ли пользователю устройства изменять дату, время и часовой пояс в Настройках.

  Ограничение поддерживается на устройствах с Android 9 или выше.

  По умолчанию флажок снят.

- Запретить добавление и удаление аккаунтов Google

  Установка или снятие флажка определяет, разрешено ли пользователю устройства добавлять и удалять аккаунты Google.

  По умолчанию флажок снят.

- Запретить изменение громкости и отключить звук на устройстве

  Ограничение регулировки громкости и отключение звука устройства.

  Если флажок установлен, пользователь не может регулировать громкость на устройстве, включен беззвучный режим.

  Если флажок снят, пользователь может регулировать громкость на устройстве, беззвучный режим отключен.

  Анти-Вор может воспроизводить звук на устройстве, независимо от этого ограничения. Ограничение отключается для воспроизведения звука, а затем включается повторно.

  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 камеру keyguard**

  Установка или снятие флажка определяет, запрещено ли пользователю устройства использовать камеру, когда устройство заблокировано.

  По умолчанию флажок снят.

- **Запретить уведомления keyguard**

  Установка или снятие флажка определяет, запрещены ли уведомления, когда экран устройства заблокирован.

  Этот флажок доступен, только если установлен флажок **Запретить функции keyguard**. В противном случае флажок **Запретить уведомления keyguard** снят и недоступен для изменения.

  По умолчанию флажок снят.

- **Запретить доверенных агентов keyguard**

  Установка или снятие флажка определяет, запрещены ли доверенные приложения, когда экран устройства заблокирован. Доверенные приложения – это приложения, позволяющие пользователю устройства разблокировать устройство без пароля, PIN-кода или отпечатка пальца.

  Этот флажок доступен, только если установлен флажок **Запретить функции keyguard**. В противном случае флажок **Запретить доверенных агентов keyguard** снят и недоступен для изменения.

  По умолчанию флажок снят.

- **Отключить разблокировку смахиванием keyguard**

  Установка или снятие флажка определяет, разрешено ли пользователю разблокировать устройство смахиванием.

  Данная настройка не действует, если в качестве текущего способа разблокировки устройства установлен пароль, PIN-код или графический пароль.

  По умолчанию флажок снят.

- **Запретить изменение яркости (Android 9 или выше)**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства регулировать яркость экрана мобильного устройства.

  Ограничение поддерживается на устройствах с Android версии 9 и выше.

  По умолчанию флажок снят.

- **Запретить автоматическое включение экрана (Android 9 или выше)**

  Если этот параметр включен, пользователь не может использовать функцию автоматического включения экрана на устройстве.

  По умолчанию этот параметр отключен.

- **Принудительно включать экран при подключении к сетевому зарядному устройству (Android 6 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 6 или выше.

  По умолчанию флажок снят.

- **Принудительно включать экран при подключении к зарядному устройству USB (Android 6 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 6 или выше.

  По умолчанию флажок снят.

- **Принудительно включать экран при подключении к беспроводному зарядному устройству (Android 6 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 6 или выше.

  По умолчанию флажок снят.

- **Запретить изменение обоев (Android 7.0 или выше)**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства изменять обои экрана мобильного устройства.

  Ограничение поддерживается на устройствах с Android 7.0 или выше.

  По умолчанию флажок снят.

- **Запретить строку состояния (Android 6 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 или выше.

По умолчанию флажок снят.

- **Запретить добавление пользователей**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства добавлять пользователей.

  По умолчанию флажок установлен. Если режим device owner был развернут на устройстве с помощью QR-кода, ограничение включено и не может быть отключено.

  Ограничение можно отключить только на устройствах, отвечающих следующим требованиям:

  - Режим device owner был развернут на устройстве с помощью инсталляционного пакета `adb.exe`.
  - Устройство должно поддерживать несколько пользователей.

- **Запретить смену пользователя (Android 9 или выше)**

  Если этот параметр включен, пользователь не может сменить текущего пользователя на устройстве.

  По умолчанию этот параметр отключен.

- **Запретить удаление пользователей**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства удалять пользователей.

  По умолчанию флажок установлен. Если режим device owner был развернут на устройстве с помощью QR-кода, ограничение не может быть отключено.

  Ограничение можно отключить только на устройствах, отвечающих следующим требованиям:

  - Режим device owner был развернут на устройстве с помощью инсталляционного пакета `adb.exe`.
  - Устройство должно поддерживать несколько пользователей.

- **Запретить безопасную загрузку (Android 6 или выше)**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства запускать устройство в безопасном режиме.

  Ограничение поддерживается на устройствах с Android версии 6 и выше.

  По умолчанию флажок снят.

- **Запретить использование микрофона**

Если этот параметр включен, микрофон на устройстве отключен.

Если этот параметр отключен, пользователь может включить микрофон и изменить его уровень громкости.

По умолчанию этот параметр отключен.

- **Запретить выключение микрофона (Android 12 или выше)**

  Если этот параметр отключен, пользователь не может отключить доступ к микрофону с помощью системного переключателя. Если доступ к микрофону на устройстве отключен при включении этого параметра, этот доступ автоматически включается.

  По умолчанию этот параметр отключен.

  На некоторых устройствах Xiaomi и HUAWEI это ограничение не работает. Проблема связана с особенностями прошивки MIUI на устройствах Xiaomi и прошивки EMUI на устройствах HUAWEI.

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.

  Если флажок установлен, программа обычно блокирует использование камеры. Однако на устройствах Asus и OnePlus значок приложения "Камера" полностью скрыт, если флажок установлен.

  По умолчанию флажок снят.

- **Запретить переключение камеры (Android 12 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 12 или выше.

  По умолчанию флажок снят.

  На некоторых устройствах Xiaomi и HUAWEI это ограничение не работает. Проблема связана с особенностями прошивки MIUI на устройствах Xiaomi и прошивки EMUI на устройствах HUAWEI.

- **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.

- **Выдача дополнительных разрешений для работы приложений**

Параметр **Выдача дополнительных разрешений для работы приложений** позволяет выбрать действие, которое будет выполняться, когда приложения, установленные на устройствах в режиме device owner, запрашивают дополнительные разрешения. Это неприменимо к разрешениям, выданным в Настройках устройства (например, Доступ ко всем файлам).

- **Запрашивать разрешения у пользователя**

  Пользователь решает, выдавать ли разрешение приложению.

  Этот параметр выбран по умолчанию.

- **Выдавать разрешения автоматически**

  Разрешения для всех приложений, установленных на устройствах в режиме device owner, выдаются без участия пользователя.

- **Отклонять разрешения автоматически**

  Запросы на разрешения для всех приложений, установленных на устройствах в режиме device owner, отклоняются без участия пользователя.

  Пользователи могут настраивать разрешения приложений в параметрах устройства, прежде чем эти разрешения будут автоматически запрещены.

На Android 12 или выше следующие разрешения не могут быть выданы автоматически, но могут быть автоматически отклонены. При выборе **Выдавать разрешения автоматически** следующие разрешения будут запрашиваться у пользователя:

- разрешения на использование местоположения;
- разрешения на доступ к камере;
- разрешения на запись звука;
- разрешение на распознавание физической активности;
- разрешение на отслеживание входящих SMS и MMS сообщений;
- разрешения на доступ к данным биометрических датчиков.

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 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 8.0 или 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 включение/выключение Wi-Fi (Android 13 или выше)**

  Если этот параметр включен, пользователь не может включать и отключать Wi-Fi на устройстве. Также Wi-Fi нельзя отключить при помощи режима полета.

  По умолчанию этот параметр отключен.

- **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 Wi-Fi Direct (Android 13 или выше)**

  Если этот параметр включен, пользователь не может использовать функцию Wi-Fi Direct на устройстве.

  По умолчанию этот параметр отключен.

- **Запретить передачу предварительно настроенных сетей Wi-Fi (Android 13 или выше)**

  Если этот параметр включен, пользователь не может передавать сети Wi-Fi, настроенные в политике. Ограничение не относится к другим сетям Wi-Fi на устройстве.

  По умолчанию этот параметр отключен.

- **Запретить добавление сетей Wi-Fi (Android 13 или выше)**

  Если параметр включен, пользователь не может вручную добавлять сети Wi-Fi на устройстве.

  По умолчанию этот параметр отключен.

- **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 режим полета (Android 9 или выше)**

  Установка или снятие флажка определяет, разрешено ли пользователю включать режим полета на устройстве.

  Ограничение поддерживается на устройствах с Android версии 9 и выше.

  По умолчанию флажок снят.

- **Запретить использование Bluetooth (Android 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 8.0 или выше. Для предыдущих версий Android установите флажок **Запретить использование Bluetooth** в разделе **Управление устройством**.

  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 обмен данными через Bluetooth (Android 8.0 или выше)**

Установка или снятие флажка определяет, разрешена ли на устройстве отправка данных через Bluetooth.

Ограничение поддерживается на устройствах с Android 8.0 или выше.

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 сброс настроек сетей (Android 6 или выше)**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства выполнять сброс настроек сетей в Настройках.

  Ограничение поддерживается на устройствах с Android 6 или выше.

  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 сотовых данных в роуминге (Android 7.0 или выше)**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства использовать сотовые данные в роуминге.

  Если флажок установлен, устройство не может обновлять базы вредоносного ПО и синхронизироваться с Сервером администрирования, находясь в роуминге.

  Чтобы разрешить обновление баз вредоносного ПО в роуминге, необходимо снять этот флажок и установить флажок **Разрешить обновление баз в роуминге** в разделе **Обновление баз**.

  Чтобы разрешить синхронизацию устройства с Сервером администрирования в роуминге, необходимо снять этот флажок, а также снять флажок **Выключить синхронизацию в роуминге** в разделе **Синхронизация**.

  Ограничение поддерживается на устройствах с Android 7.0 или выше.

  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.

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.

  Различные комбинации установки флажков **Запретить отслеживание местоположения** и **Запретить изменение настроек местоположения (Android 9 или выше)** позволяют получить разные варианты работы функции определения местоположения.

Запретить отслеживание местоположения	Запретить изменение настроек местоположения (Android 9 или выше)	Результат ограничения функций
Включено	Включено	Отслеживание местоположения отключено, и пользователь устройства не может включить его.
Включено	Выключено	Отслеживание местоположения отключено, но пользователь устройства может включить его. Отключение ограничения **Запретить изменение настроек местоположения (Android 9)** позволяет пользователю отключить отслеживание местоположения на устройстве, что может привести к недоступности некоторых функций.
Выключено	Включено	Отслеживание местоположения включено, и пользователь устройства не может отключить его.
Выключено	Выключено	Отслеживание местоположения включено, но пользователь устройства может отключить его. Отключение ограничения **Запретить изменение настроек местоположения (Android 9)** позволяет пользователю отключить отслеживание местоположения на устройстве, что может привести к недоступности некоторых функций.

- **Запретить передачу местоположения**

Если этот параметр включен, пользователь не может передавать местоположение устройства при помощи приложений, предоставляющих такую возможность.

По умолчанию этот параметр отключен.

- **Запретить изменение настроек местоположения (Android 9 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 9 или выше.

По умолчанию флажок снят.

Различные комбинации установки флажков **Запретить отслеживание местоположения** и **Запретить изменение настроек местоположения (Android 9 или выше)** позволяют получить разные варианты работы функции определения местоположения.

Запретить отслеживание местоположения	Запретить изменение настроек местоположения (Android 9 или выше)	Результат ограничения функций
Включено	Включено	Отслеживание местоположения отключено, и пользователь устройства не может включить его.
Включено	Выключено	Отслеживание местоположения отключено, но пользователь устройства может включить его. Отключение ограничения **Запретить изменение настроек местоположения (Android 9)** позволяет пользователю отключить отслеживание местоположения на устройстве, что может привести к недоступности некоторых функций.
Выключено	Включено	Отслеживание местоположения включено, и пользователь устройства не может отключить его.
Выключено	Выключено	Отслеживание местоположения включено, но пользователь устройства может отключить его. Отключение ограничения **Запретить изменение настроек местоположения (Android 9)** позволяет пользователю отключить отслеживание местоположения на устройстве, что может привести к недоступности некоторых функций.

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 или выше)

  В блоке **Периоды приостановки обновления системы (Android 9 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 9 или 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.

Настройка режима киоска для Android-устройств

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.

Режим киоска не влияет на работу приложения Kaspersky Endpoint Security для Android. Оно продолжает работать в фоновом режиме, выводит уведомления и может обновляться.

Типы режима киоска

В Kaspersky Endpoint Security доступны следующие типы режима киоска:

- Режим одного приложения

  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 приложение запускается непосредственно в режиме киоска.

  На устройствах с Android версии 8.0 и ниже для запуска приложение должно поддерживать функцию режима киоска и самостоятельно вызывать метод `startLockTask()`.

- Режим с несколькими приложениями

  Режим киоска с несколькими приложениями. В этом режиме пользователю устройства разрешено открывать на устройстве несколько приложений, которые указаны в настройках режима киоска.

Перед настройкой режима киоска

Перед настройкой режима киоска выполните следующие действия:

- 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.

- 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.

   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 **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 ниже в разделе "Ограничения режима киоска".
4. Установите флажок **Разрешить переход в дополнительные приложения**, если хотите разрешить пользователю устройства переход в другие приложения. Подробнее см. ниже в разделе **Добавление дополнительных приложений**.
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 **OK**.
3. Укажите любые необходимые ограничения. С доступными ограничениями можно ознакомиться ниже в разделе "Ограничения режима киоска".
4. Установите флажок **Разрешить переход в дополнительные приложения**, если хотите разрешить пользователю устройства переход в другие приложения. Подробнее см. ниже в разделе **Добавление дополнительных приложений**.
5. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Ограничения режима киоска

В режиме киоска вы можете установить следующие ограничения:

- Запретить строку состояния (Android 9 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 и выше.

По умолчанию флажок установлен.

- **Запретить кнопку Обзор (Android 9 или выше)**

  Установка или снятие флажка определяет, будет ли скрыта кнопка Обзор. Ограничение поддерживается на устройствах с Android версии 9 и выше.

  По умолчанию флажок установлен.

- **Запретить кнопку Главный экран (Android 9 или выше)**

  Установка или снятие флажка определяет, будет ли скрыта кнопка Главный экран. Ограничение поддерживается на устройствах с Android версии 9 и выше.

  По умолчанию флажок установлен.

- **Запретить показ системных уведомлений (Android 9 или выше)**

  Установка или снятие флажка определяет, будут ли скрыты системные уведомления. Ограничение поддерживается на устройствах с Android версии 9 или выше.

  По умолчанию флажок установлен.

Добавление дополнительных приложений

Помимо настройки устройства для работы с одним или несколькими приложениями, вы можете добавить дополнительные приложения, которые разрешено использовать основному приложению. Эти дополнительные приложения обеспечивают полную функциональность приложений, добавленных в режим киоска. Пользователь устройства не может запускать дополнительные приложения вручную.

*Для добавления дополнительных приложений в **Режим киоска** выполните следующие действия:*

1. Установите флажок **Разрешить переход в дополнительные приложения**.
2. Нажмите **Добавить**, укажите необходимое имя пакета приложения и нажмите **OK**. **Как получить имя пакета приложения**

Чтобы получить имя пакета приложения:

1. Откройте Google Play.
2. Найдите нужное приложение и откройте его страницу.

   URL приложения оканчивается именем пакета приложения (например, https://play.google.com/store/apps/details?id=**com.android.chrome**).

Чтобы получить имя пакета приложения, которое было добавлено в Kaspersky Security Center:

1. В дереве консоли Kaspersky Security Center выберите **Дополнительно** > **Удаленная установка** > **Инсталляционные пакеты**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Управление пакетами мобильных приложений**.

   В открывшемся окне **Управление пакетами мобильных приложений** в столбце **Название приложения** отображаются идентификаторы управляемых приложений.

   Если пакет приложения представлен файлом в формате APK, и необходимо узнать идентификатор приложения, можно добавить этот пакет приложения в окне **Управление пакетами мобильных приложений**, нажав на кнопку **Новый** и следуя инструкциям на экране.

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

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.

   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 **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

- **Обновлять сертификат автоматически**

  Если флажок установлен, сертификат будет автоматически перевыпущен на устройство до истечения срока действия текущего сертификата. Поле **Обновить, когда осталось (дней)** также становится доступным. В этом поле необходимо указать количество дней до истечения срока действия сертификата, когда сертификат будет перевыпущен.

  Если флажок снят, сертификат не будет автоматически обновлен.

  По умолчанию флажок снят.

- **Обновить, когда осталось (дней)**

  Количество дней до истечения срока действия сертификата, когда для устройства будет выпущен обновленный сертификат. Например, в этом поле можно указать 90 дней. Обновленный сертификат будет выпущен за 90 дней до истечения срока действия текущего сертификата.

  Это поле доступно и обязательно к заполнению, если установлен флажок **Обновлять сертификат автоматически**.

  Значение по умолчанию не задано.

- **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.

   После редактирования профиля сертификата в параметрах политики соответствующий сертификат автоматически удалится с устройства во время следующей синхронизации с Сервером администрирования, после чего будет установлен новый сертификат.

Чтобы удалить подключение или профиль сертификата:

1. Выберите необходимое подключение или профиль сертификата в соответствующем разделе.
2. Нажмите **Удалить**, а затем **ОК**.

   Если удалить соединение с центром сертификации, все профили сертификатов, которые используют это соединение, также будут удалены.

3. Нажмите **Применить**, чтобы сохранить внесенные изменения.

   После удаления профиля сертификата в параметрах политики соответствующий сертификат автоматически удалится с устройства во время следующей синхронизации с Сервером администрирования.

Включение проверки подлинности на основе сертификатов KES-устройств

Чтобы включить проверку подлинности на основе сертификатов KES-устройства:

1. Откройте системный реестр клиентского устройства, на котором установлен Сервер администрирования (например, локально с помощью команды regedit в меню **Пуск → Выполнить**).
2. Перейдите к кусту.
   - Для 32-разрядных систем:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - Для 64-разрядных систем:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. Создайте ключ с именем LP_MobileMustUseTwoWayAuthOnPort13292.
4. Укажите тип ключа REG_DWORD.

5. Установите значение ключа 1.

6. Перезапустите службу Сервера администрирования.

В результате обязательная проверка подлинности на основе сертификатов KES-устройства с использованием общего сертификата будет включена после запуска службы Сервера администрирования.

При первом подключении KES-устройства к Серверу администрирования наличие сертификата не обязательно.

По умолчанию проверка подлинности на основе сертификатов KES-устройств отключена.

Создание пакета мобильных приложений для KES-устройств

Для создания пакета мобильных приложений для KES-устройств необходима лицензия Kaspersky Endpoint Security для Android.

Чтобы создать пакет мобильных приложений, выполните следующие действия:

1. В дереве консоли в папке **Удаленная установка** выберите подпапку **Инсталляционные пакеты**.

   Папка **Удаленная установка** по умолчанию вложена в папку **Дополнительно**.

2. Нажмите на кнопку **Справка** и в раскрывающемся списке выберите **Пакеты мобильных приложений предназначены для установки на мобильные устройства не средствами Kaspersky Security Center. Например, такой пакет может быть отправлен пользователю по электронной почте или опубликован на Веб-сервере для дальнейшего скачивания и установки**.

3. В окне **Управление пакетами мобильных приложений** нажмите на кнопку **Новый**.

4. Запустится мастер создания инсталляционного пакета. Следуйте далее указаниям мастера.

Созданный пакет мобильных приложений отобразится в окне **Управление пакетами мобильных приложений**.

Просмотр информации о KES-устройстве

Чтобы просмотреть информацию о KES-устройстве:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте KES-устройства по протоколу управления *KES*.

3. Выберите мобильное устройство, информацию о котором нужно просмотреть.

4. В контекстном меню мобильного устройства выберите пункт **Свойства**.

В результате откроется окно свойств KES-устройства.

В окне свойств мобильного устройства отображается информация о подключенном KES-устройстве.

Отключение KES-устройства от управления

Чтобы отключить KES-устройство от управления, пользователь должен удалить Агент администрирования с мобильного устройства. После удаления пользователем Агента администрирования информация о мобильном устройстве удаляется из базы данных Сервера администрирования и администратор может удалить мобильное устройство из списка управляемых устройств.

Чтобы удалить KES-устройство из списка управляемых устройств:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте KES-устройства по протоколу управления *KES*.

3. Выберите мобильное устройство, которое необходимо отключить от управления.

4. В контекстном меню мобильного устройства выберите пункт **Удалить**.

   В результате мобильное устройство будет удалено из списка управляемых устройств.

   Если Kaspersky Endpoint Security для Android не удален с мобильного устройства, то после синхронизации с Сервером администрирования мобильное устройство снова появится в списке управляемых устройств.

Управление iOS MDM-устройствами

В этом разделе описаны дополнительные возможности управления iOS MDM-устройствами с помощью Kaspersky Security Center. Для управления iOS MDM-устройствами программа поддерживает следующие возможности:

- Централизованно настраивать параметры управляемых iOS MDM-устройств и ограничивать функции устройств с помощью конфигурационных профилей. Вы можете добавлять и изменять конфигурационные профили и устанавливать профили на мобильные устройства.

- Устанавливать приложения на мобильные устройства не через App Store с помощью provisioning-профилей. Например, вы можете использовать provisioning-профили для установки внутренних корпоративных приложений на мобильные устройства пользователей. Provisioning-профиль содержит информацию о приложении и мобильном устройстве.

- Устанавливать приложения на iOS MDM-устройство через App Store. Перед установкой приложения на iOS MDM-устройстве, необходимо добавить приложение на Сервер iOS MDM.

Каждые 24 часа всем подключенным iOS MDM-устройствам отправляется PUSH-нотификация для синхронизации данных с Сервером iOS MDM.

Информацию о конфигурационном профиле и provisioning–профиле, а также о приложениях, установленных на iOS MDM-устройстве, можно просмотреть в окне свойств устройства.

Подписание iOS MDM-профиля сертификатом

Вы можете подписать iOS MDM-профиль сертификатом. Вы можете использовать сертификат, который создали сами, или получить сертификат от доверенных центров сертификации.

Сертификат необязателен для корректной работы iOS MDM-профиля. Если iOS MDM-профиль не подписан сертификатом, то при установке iOS MDM-профиля отобразится предупреждение, и пользователям будет предложено подтвердить, что они доверяют организации, приславшей сертификат.

Чтобы подписать iOS MDM-профиль сертификатом, выполните следующие действия:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите подпапку **Мобильные устройства**.
2. В контекстном меню подпапки **Мобильные устройства** выберите пункт **Свойства**.
3. В окне свойств папки выберите секцию **Параметры подключения iOS-устройств**.
4. Нажмите на кнопку **Обзор** под полем **Выбрать файл сертификата**.

   Откроется окно **Сертификат**.
5. В поле **Тип сертификата** укажите тип открытого или личного сертификата:
   - Если выбрано значение **Контейнер PKCS#12**, укажите файл сертификата и пароль.
   - Если выбрано значение **X.509-сертификат**:
     a. Укажите файл личного ключа (с расширением *.prk или *.pem).
     b. Укажите пароль личного ключа.
     c. Укажите файл открытого ключа (с расширением *.cer).
6. Нажмите на кнопку **OK**.

iOS MDM-профиль подписан сертификатом.

Добавление конфигурационного профиля

Чтобы создать конфигурационный профиль, вы можете использовать приложение Apple Configurator 2, которое доступно на веб-сайте Apple Inc. Приложение Apple Configurator 2 работает только на устройствах под управлением macOS; если у вас нет таких устройств, вы можете использовать iPhone Configuration Utility на устройстве с установленной Консолью администрирования. Apple Inc. больше не поддерживает iPhone Configuration Utility.

Чтобы создать конфигурационный профиль с помощью iPhone Configuration Utility и добавить его на Сервер iOS MDM:

1. В дереве консоли выберите папку **Управление мобильными устройствами**.
2. В рабочей области папки **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
4. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера мобильных устройств.
5. В окне свойств Сервера iOS MDM выберите раздел **Конфигурационные профили**.
6. В разделе **Конфигурационные профили** нажмите на кнопку **Создать**.

   Откроется окно **Новый конфигурационный профиль**.
7. В окне **Новый конфигурационный профиль** укажите название профиля и идентификатор профиля.

   Идентификатор конфигурационного профиля должен быть уникальным, значение идентификатора следует задавать в формате Reverse-DNS, например, *com.companyname.identifier*.
8. Нажмите на кнопку **OK**.

   Запустится программа iPhone Configuration Utility, если она установлена.
9. Выполните настройку параметров профиля в программе iPhone Configuration Utility.

   Описание параметров профиля и инструкции по его настройке приведены в документации для программы iPhone Configuration Utility.

После настройки параметров профиля в программе iPhone Configuration Utility, новый конфигурационный профиль отображается в разделе **Конфигурационные профили** в окне свойств Сервера iOS MDM.

По кнопке **Изменить** конфигурационный профиль можно отредактировать.

По кнопке **Импортировать** можно загрузить конфигурационный профиль в программу.

По кнопке **Экспортировать** конфигурационный профиль можно сохранить в файле.

Созданный профиль требуется установить на iOS MDM-устройства.

Установка конфигурационного профиля на устройство

Чтобы установить конфигурационный профиль на мобильное устройство:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите подпапку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.
2. В рабочей области отфильтруйте устройства iOS MDM. Для этого:

   a. Перейдите по ссылке **Фильтр не указан, всего записей: <количество>**.

   b. В списке **Протокол управления** выберите **iOS MDM**.

3. Выберите мобильное устройство, на которое вы хотите установить профиль конфигурации.

   Вы можете выбрать несколько мобильных устройств, чтобы установить на них профиль одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Установить профиль** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав пункт **Все команды** в контекстном меню этого мобильного устройства, а затем **Установить профиль**.

   В результате откроется окно **Выбор профилей** со списком профилей. Выберите в списке профиль, который нужно установить на мобильное устройство. Вы можете выбрать и установить на мобильное устройство несколько профилей одновременно. Чтобы выбрать диапазон профилей, используйте клавишу **Shift**. Для объединения отдельных профилей в группу используйте клавишу **Ctrl**.

6. Нажмите на кнопку **OK**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранный конфигурационный профиль будет установлен на мобильное устройство пользователя. В случае успешного выполнения команды текущий статус команды в журнале команд примет значение *Выполнено*.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

   По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

   В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

7. Нажмите на кнопку **OK**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Вы можете просмотреть профиль, который вы установили, и удалить его, если необходимо.

Удаление конфигурационного профиля с устройства

Чтобы удалить конфигурационный профиль с мобильного устройства:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите подпапку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте устройства iOS MDM. Для этого:

   a. Перейдите по ссылке **Фильтр не указан, всего записей: <количество>**.

   b. В списке **Протокол управления** выберите **iOS MDM**.

3. Выберите мобильное устройство, с которого нужно удалить конфигурационный профиль.

   Вы можете выбрать несколько мобильных устройств, чтобы удалить с них профиль одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Удалить профиль** и нажмите на кнопку **Отправить команду**.

Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню устройства пункт **Все команды**, затем **Удалить профиль**.

В результате откроется окно **Удаление профилей** со списком профилей.

6. Выберите в списке профиль, который нужно удалить с мобильного устройства. Вы можете выбрать и удалить с мобильного устройства несколько профилей одновременно. Чтобы выбрать диапазон профилей, используйте клавишу **Shift**. Для объединения отдельных профилей в группу используйте клавишу **Ctrl**.

7. Нажмите на кнопку **OK**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранный конфигурационный профиль будет удален с мобильного устройства пользователя. В случае успешного выполнения команды текущий статус команды примет значение *Завершена*.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

   По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

   В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

8. Нажмите на кнопку **OK**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Добавление provisioning-профиля

Чтобы добавить provisioning-профиль на Сервер iOS MDM, выполните следующие действия:

1. В дереве консоли выберите папку **Управление мобильными устройствами**.

2. В дереве консоли в папке **Управление мобильными устройствами** выберите подпапку **Серверы мобильных устройств**.

3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.

4. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера мобильных устройств.

5. В окне свойств **Сервера iOS MDM** перейдите в раздел **Provisioning-профили**.

6. В разделе **Provisioning-профили** нажмите на кнопку **Импортировать** и укажите путь к файлу provisioning-профиля.

Профиль будет добавлен в параметры Сервера iOS MDM.

По кнопке **Экспортировать** provisioning-профиль можно сохранить в файле.

Вы можете установить provisioning-профиль, который вы импортировали, на iOS MDM-устройства.

Установка provisioning-профиля на устройство

Чтобы установить provisioning-профиль на мобильное устройство, выполните следующие действия:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите подпапку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте устройства iOS MDM. Для этого:

   a. Перейдите по ссылке **Фильтр не указан, всего записей: <количество>**.

   b. В списке **Протокол управления** выберите **iOS MDM**.

3. Выберите мобильное устройство пользователя, на которое нужно установить provisioning-профиль.

   Вы можете выбрать несколько мобильных устройств, чтобы установить на них provisioning-профиль одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Установить provisioning-профиль** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню мобильного устройства пункт **Все команды**, затем **Установить provisioning-профиль**.

   В результате откроется окно **Выбор provisioning-профилей** со списком provisioning-профилей. Выберите в списке provisioning-профиль, который нужно установить на мобильное устройство. Вы можете выбрать и установить на мобильное устройство несколько provisioning-профилей одновременно. Чтобы выбрать диапазон provisioning-профилей, используйте клавишу **SHIFT**. Для объединения отдельных provisioning-профилей в группу используйте клавишу **CTRL**.

6. Нажмите на кнопку **OK**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранный provisioning-профиль будет установлен на мобильное устройство пользователя. В случае успешного выполнения команды текущий статус команды в журнале команд принимает значение *Завершена*.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

   По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

   В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

7. Нажмите на кнопку **OK**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Вы можете просмотреть профиль, который вы установили, и удалить его, если необходимо.

Удаление provisioning-профиля с устройства

Чтобы удалить provisioning-профиль с мобильного устройства, выполните следующие действия:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите подпапку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте устройства iOS MDM. Для этого:

a. Перейдите по ссылке **Фильтр не указан, всего записей: <количество>**.

b. В списке **Протокол управления** выберите **iOS MDM**.

3. Выберите мобильное устройство, с которого нужно удалить provisioning-профиль.

   Вы можете выбрать несколько мобильных устройств, чтобы удалить с них provisioning-профиль одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Удалить provisioning-профиль** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню устройства пункт **Все команды**, затем **Удалить provisioning-профиль**.

   В результате откроется окно **Удаление provisioning-профилей** со списком профилей.

6. Выберите в списке provisioning-профиль, который нужно удалить с мобильного устройства. Вы можете выбрать и удалить с мобильного устройства несколько provisioning-профилей одновременно. Чтобы выбрать диапазон provisioning-профилей, используйте клавишу **SHIFT**. Для объединения отдельных provisioning-профилей в группу используйте клавишу **CTRL**.

7. Нажмите на кнопку **OK**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранный provisioning-профиль будет удален с мобильного устройства пользователя. Приложения, связанные с удаленным provisioning-профилем, не будут работать. В случае успешного выполнения команды текущий статус команды примет значение *Завершена*.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

   По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

   В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

8. Нажмите на кнопку **OK**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Настройка управляемых приложений

Перед установкой приложения на iOS MDM-устройстве, необходимо добавить приложение на Сервер iOS MDM. Приложение считается управляемым, если оно было установлено на устройство с помощью Kaspersky Security Center. Управляемым приложением можно дистанционно управлять средствами Kaspersky Endpoint Security.

Чтобы добавить управляемое приложение на Сервер iOS MDM, выполните следующие действия:

1. В дереве консоли откройте папку **Управление мобильными устройствами**.

2. В дереве консоли в папке **Управление мобильными устройствами** выберите подпапку **Серверы мобильных устройств**.

3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.

4. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера iOS MDM.

5. В окне свойств Сервера iOS MDM выберите раздел **Управляемые приложения**.

6. В блоке **Управляемые приложения** нажмите на кнопку Управляемые приложения.

   Откроется окно **Добавление приложения**.

7. В окне **Добавление приложения** в поле **Название приложения** укажите название добавляемого приложения.

8. В поле **Apple ID приложения или ссылка на манифест-файл** укажите Apple ID приложения, которое нужно добавить, или укажите ссылку на manifest-файл, который можно использовать для загрузки приложения.

9. Если вы хотите, чтобы при удалении iOS MDM-профиля одновременно с профилем с мобильного устройства пользователя было удалено и управляемое приложение, установите флажок **Удалять вместе с iOS MDM-профилем**.

10. Если вы хотите запретить резервное копирование данных приложения с помощью iTunes, установите флажок **Запретить создавать резервные копии данных**.

11. Если вы хотите настроить параметры управляемого приложения, нажмите на кнопку **Конфигурация приложений**.

    Откроется окно **Конфигурация приложений**.

12. В окне **Конфигурация приложений** нажмите на кнопку **Обзор**, чтобы выбрать и загрузить конфигурационный файл в формате PLIST.

    Чтобы сгенерировать конфигурационный файл, используйте генератор конфигурации (например, https://appconfig.jamfresearch.com/generator) или обратитесь к официальной документации по настраиваемому приложению.

    Пример настройки основных параметров для приложения Microsoft Outlook.

Ключ конфигурации	Описание	Тип	Значение	Зн ум
com.microsoft.outlook.EmailProfile.EmailAccountName	Имя пользователя	String	Имя пользователя, которое будет использоваться для получения имени пользователя из Microsoft Active Directory. Оно может отличаться от адреса электронной почты пользователя. Например, User.	
com.microsoft.outlook.EmailProfile.EmailAddress	Адрес электронной почты	String	Адрес электронной почты, который будет использоваться для получения адреса электронной почты пользователя из Microsoft Active Directory. Например, user@companyname.com.	
com.microsoft.outlook.EmailProfile.EmailUPN	Имя участника-пользователя или имя пользователя для профиля электронной почты, который используется для аутентификации учетной записи	String	Имя пользователя в формате адреса электронной почты. Например, userupn@companyname.com.	
com.microsoft.outlook.EmailProfile.ServerAuthentication	Метод аутентификации	String	Username and Password – запрашивает пароль у пользователя устройства. Certificates – проверка подлинности на основе сертификатов.	Us an Pa
com.microsoft.outlook.EmailProfile.ServerHostName	Полное доменное имя ActiveSync	String	URL почтового сервера Exchange ActiveSync. Перед URL не обязательно использовать HTTP:// или HTTPS://. Например, mail.companyname.com.	
com.microsoft.outlook.EmailProfile.AccountDomain	Домен электронной почты	String	Домен учетной записи пользователя. Например, companyname.	
com.microsoft.outlook.EmailProfile.AccountType	Тип аутентификации	String	ModernAuth – использует метод аутентификации на основе маркеров. Укажите ModernAuth в качестве типа учетной записи для Exchange Online. BasicAuth – запрашивает пароль у пользователя устройства. Укажите BasicAuth в качестве типа учетной записи для локальной версии Exchange.	Ba
IntuneMAMRequireAccounts	Требование входа	String	Указывает, требуется ли вход в учетную запись. Вы можете выбрать одно из следующих значений:	

			`Enabled` - приложение требует, чтобы пользователь вошел в управляемую учетную запись, заданную ключом `IntuneMAMUPN`, для получения данных организации. `Disabled` - вход в аккаунт не требуется.	
`IntuneMAMUPN`	UPN-адрес	String	Имя участника-пользователя учетной записи, которой разрешено входить в приложение. Например, `userupn@companyname.com`.	

[Пример файла конфигурации для приложения Microsoft Outlook.]

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>com.microsoft.outlook.EmailProfile.AccountType</key>
  <string>BasicAuth</string>
  <key>com.microsoft.outlook.EmailProfile.EmailAccountName</key>
  <string>My Work Email</string>
  <key>com.microsoft.outlook.EmailProfile.ServerHostName</key>
  <string>exchange.server.com</string>
  <key>com.microsoft.outlook.EmailProfile.EmailAddress</key>
  <string>%email%</string>
  <key>com.microsoft.outlook.EmailProfile.EmailUPN</key>
  <string>%full_name%</string>
  <key>com.microsoft.outlook.EmailProfile.AccountDomain</key>
  <string>my-domain</string>
  <key>com.microsoft.outlook.EmailProfile.ServerAuthentication</key>
  <string>Username and Password</string>
  <key>IntuneMAMAllowedAccountsOnly</key>
  <string>Enabled</string>
  <key>IntuneMAMUPN</key>
  <string>%full_name%</string>
</dict>
</plist>
```

13. После импорта файла PLIST конфигурация приложения отобразится в окне **Конфигурации приложений**.

    Вы можете изменить конфигурацию, отредактировав текст файла PLIST после его импорта.

14. Нажмите на кнопку **OK**, чтобы применить конфигурацию приложения.

15. Нажмите на кнопку **OK** повторно, чтобы закрыть окно **Добавление приложения**.

    Добавленное приложение отображается в разделе **Управляемые приложения** окна свойств Сервера iOS MDM.

Также можно изменить или удалить конфигурацию уже добавленного приложения.

Чтобы изменить конфигурацию управляемого приложения, выполните следующие действия:

1. В разделе **Управляемые приложения** выберите управляемое приложение из списка и нажмите на кнопку **Изменить**.

   Откроется окно **Изменение параметров мобильного приложения**.

2. В окне **Изменение параметров мобильного приложения** нажмите на кнопку **Конфигурация приложения**.

   Откроется окно **Конфигурация приложений**.

3. Нажмите на кнопку **Обзор**, чтобы выбрать и загрузить конфигурационный файл в формате PLIST.

4. При необходимости отредактируйте текст файла PLIST после его импорта.

5. Нажмите на кнопку **ОК**, чтобы применить конфигурацию приложения.

6. Нажмите на кнопку **ОК**, чтобы закрыть окно **Изменение параметров мобильного приложения**.

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

Чтобы удалить конфигурацию управляемого приложения, выполните следующие действия:

1. В разделе **Управляемые приложения** выберите управляемое приложение из списка и нажмите на кнопку **Изменить**.

   Откроется окно **Изменение параметров мобильного приложения**.

2. В окне **Изменение параметров мобильного приложения** нажмите на кнопку **Удалить конфигурацию**.

Примененная конфигурация управляемого приложения будет удалена.

Установка приложения на мобильное устройство

Чтобы установить приложение на мобильное устройство iOS MDM, выполните следующие действия:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите подпапку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте устройства iOS MDM. Для этого:

   a. Перейдите по ссылке **Фильтр не указан, всего записей: <количество>**.

   b. В списке **Протокол управления** выберите **iOS MDM**.

3. Выберите мобильное устройство, на которое вы хотите установить приложение.

   Вы можете выбрать несколько мобильных устройств, чтобы установить на них приложение одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Установить приложение** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню мобильного устройства пункт **Все команды**, затем **Установить приложение**.

Откроется окно **Выбор приложений** со списком управляемых приложений. Выберите в списке приложение, которое нужно установить на мобильное устройство. Вы можете выбрать и установить на мобильное устройство несколько приложений одновременно. Чтобы выбрать диапазон приложений, используйте клавишу **SHIFT**. Для объединения отдельных приложений в группу используйте клавишу **CTRL**.

6. Нажмите на кнопку **OK**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранное приложение будет установлено на мобильное устройство пользователя. В случае успешного выполнения команды текущий статус команды в журнале команд принимает значение *Завершена*.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз. По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

   В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

7. Нажмите на кнопку **OK**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Информация об установленном приложении отображается в свойствах мобильного устройства iOS MDM. Вы можете удалить приложение с мобильного устройства с помощью журнала команд или из контекстного меню мобильного устройства.

Удаление приложения с устройства

Чтобы удалить приложение с мобильного устройства:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте устройства iOS MDM. Для этого:

   a. Перейдите по ссылке **Фильтр не указан, всего записей: <количество>**.

   b. В списке **Протокол управления** выберите **iOS MDM**.

3. Выберите мобильное устройство, с которого нужно удалить приложение.

   Вы можете выбрать несколько мобильных устройств, чтобы удалить с них приложение одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Удалить приложение** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню мобильного устройства пункт **Все команды**, затем **Удалить приложение**.

   В результате откроется окно **Удаление приложений** со списком приложений.

6. Выберите в списке приложение, которое нужно удалить с мобильного устройства. Вы можете выбрать и удалить с устройства несколько приложений одновременно. Чтобы выбрать диапазон приложений, используйте клавишу **SHIFT**. Для объединения отдельных приложений в группу используйте клавишу **CTRL**.

7. Нажмите на кнопку **OK**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранное приложение будет удалено с мобильного устройства пользователя. В случае успешного выполнения команды текущий статус команды примет значение *Завершена*.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

   По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

   В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

8. Нажмите на кнопку **OK**, чтобы закрыть окно **Команды для управления мобильным устройством**.

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**.

Настройка роуминга на iOS MDM-устройстве

Чтобы настроить роуминг, выполните следующие действия:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите подпапку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте устройства iOS MDM. Для этого:

   a. Перейдите по ссылке **Фильтр не указан, всего записей: <количество>**.

   b. В списке **Протокол управления** выберите **iOS MDM**.

3. Выберите мобильное устройство, принадлежащее пользователю, для которого вы хотите настроить роуминг.

   Вы можете выбрать несколько мобильных устройств для одновременной настройки роуминга.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

5. В окне **Команды для управления мобильным устройством <имя устройства>** перейдите в раздел **Настроить параметры роуминга** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню устройства **Все команды → Настроить параметры роуминга**.

6. В окне **Параметры роуминга** укажите соответствующие параметры:

   - **Включить роуминг данных**

     Если этот параметр включен, на мобильном устройстве iOS MDM включен роуминг данных. Пользователь мобильного устройства iOS MDM может выходить в интернет в роуминге.

     По умолчанию этот параметр отключен.

Для выбранных устройств настроен роуминг.

Просмотр информации о iOS MDM-устройстве

Чтобы просмотреть информацию о iOS MDM-устройстве, выполните следующие действия:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите подпапку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте устройства iOS MDM. Для этого:

   a. Перейдите по ссылке **Фильтр не указан, всего записей: <количество>**.

   b. В списке **Протокол управления** выберите **iOS MDM**.

3. Выберите мобильное устройство, информацию о котором нужно просмотреть.

4. В контекстном меню мобильного устройства выберите пункт **Свойства**.

   В результате откроется окно свойств iOS MDM-устройства.

В окне свойств мобильного устройства отображается информация о подключенном iOS MDM-устройстве.

Отключение устройства iOS MDM от управления

Для прекращения управления устройством iOS MDM можно отключить его от управления в Kaspersky Security Center.

В качестве альтернативы вы или владелец устройства можете удалить профиль iOS MDM с устройства. Однако после этого вам все же придется отключить устройство от управления по инструкции, приведенной в этом разделе. В противном случае вы не сможете снова включить управление устройством.

Чтобы отключить устройство iOS MDM от Сервера iOS MDM, выполните следующие действия:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите подпапку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте устройства iOS MDM. Для этого:

   a. Перейдите по ссылке **Фильтр не указан, всего записей: <количество>**.

   b. В списке **Протокол управления** выберите **iOS MDM**.

3. Выберите мобильное устройство, которое необходимо отключить.

4. В контекстном меню мобильного устройства выберите пункт **Удалить**.

   Устройство iOS MDM будет отмечено в списке на удаление. В течение минуты мобильное устройство будет удалено из базы данных Сервера iOS MDM, а затем – из списка управляемых устройств.

В результате отключения мобильного устройства iOS MDM от управления с него будут удалены все установленные конфигурационные профили, профиль iOS MDM и приложения, для которых в настройках Сервера iOS MDM был выбран параметр **Удалять вместе с профилем iOS MDM**.

Настройка режима киоска для iOS MDM-устройств

Режим киоска — это функция iOS, которая позволяет ограничить список приложений, доступных пользователю устройства, одним приложением. В этом режиме пользователю устройства разрешено открывать на устройстве только одно приложение, которое указано в настройках режима киоска.

Параметры режима киоска применяются к iOS MDM-устройствам, управляемым через Kaspersky Security Center.

Переход в настройки режима киоска

Чтобы открыть настройки режима киоска:

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 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 **Режим киоска**.

Настройка режима киоска

Чтобы включить режим киоска:

1. Установите флажок **Включить режим киоска (только для supervised)**, чтобы активировать режим киоска на контролируемом устройстве.

2. В поле **Идентификатор пакета приложения (bundle ID)** введите уникальный идентификатор приложения, выбранного для режима киоска (например, com.apple.calculator). **Как получить идентификатор пакета приложения**

Чтобы получить идентификатор пакета предустановленного приложения на iPhone или iPad,

Следуйте инструкциям в документации Apple.

Чтобы получить идентификатор пакета любого приложения для iPhone или iPad:

1. Откройте App Store.
2. Найдите нужное приложение и откройте его страницу.

   URL приложения оканчивается его числовым идентификатором (например, https://apps.apple.com/us/app/google-chrome/id**535886823**).
3. Скопируйте этот идентификатор (без букв "id").
4. Откройте страницу https://itunes.apple.com/lookup?id=<скопированный идентификатор>.

   Будет загружен текстовый файл.
5. Откройте загруженный файл и найдите в нем "bundleId".

Текст, следующий за "bundleId" – идентификатор пакета необходимого приложения.

Чтобы получить идентификатор пакета приложения, которое было добавлено в Kaspersky Security Center:

1. В дереве консоли Kaspersky Security Center выберите **Дополнительно** > **Удаленная установка** > **Инсталляционные пакеты**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Управление пакетами мобильных приложений**.

В открывшемся окне **Управление пакетами мобильных приложений** в столбце **Название приложения** отображаются идентификаторы управляемых приложений.

Если пакет приложения представлен файлом в формате .apk или .ipa, и необходимо узнать идентификатор приложения, можно добавить этот пакет приложения в окне **Управление пакетами мобильных приложений**, нажав на кнопку **Новый** и следуя инструкциям на экране.

Чтобы выбрать другое приложение, необходимо отключить режим киоска, сохранить изменения в политике и включить режим киоска для нового приложения.

Приложение, используемое в режиме киоска, должно быть установлено на устройстве. В противном случае устройство будет заблокировано до тех пор, пока режим киоска не будет отключен.

Использование выбранного приложения должно быть разрешено политикой. В противном случае режим киоска не будет включен до тех пор, пока выбранное приложение не будет удалено из списка запрещенных приложений.

В некоторых случаях, если использование выбранного приложения запрещено политикой, режим киоска все равно может быть включен.

3. Укажите настройки, которые будут включены на устройстве в режиме киоска. С доступными ограничениями можно ознакомиться ниже в разделе "Ограничения режима киоска".

4. Укажите настройки, которые пользователь может менять на устройстве в режиме киоска.

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

После сохранения изменений в политике режим киоска будет включен. Выбранное приложение принудительно открывается на контролируемом устройстве, в то время как использование других приложений запрещено. Выбранное приложение открывается сразу после перезапуска устройства.

Чтобы изменить параметры режима киоска, необходимо отключить режим киоска, сохранить изменения в политике, а затем снова включить режим киоска с новыми параметрами.

Чтобы отключить режим киоска:

1. Установите флажок **Выключить режим киоска (только для supervised)**, чтобы отключить режим киоска на контролируемом устройстве.

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

После сохранения изменений в политике режим киоска отключится. Использование всех приложений разрешено на контролируемом устройстве.

Теперь вы можете снова включить режим киоска с новыми настройками.

Параметры режима киоска

- **Автоблокировка**

  Если флажок установлен, автоблокировка устройства включена. Экран устройства блокируется автоматически.

  Если флажок снят, автоблокировка устройства отключена.

  По умолчанию флажок установлен.

- **Касание (не рекомендуется выключать)**

  Если флажок установлен, сенсорный ввод на устройстве включен.

  Если флажок снят, сенсорный ввод на устройстве отключен.

  По умолчанию флажок установлен.

- **Альтернативное управление устройством (AssistiveTouch)**

Если флажок установлен, альтернативное управление устройством включено. Экран устройства адаптируется к уникальным физическим потребностям пользователя.

Если флажок снят, альтернативное управление устройством отключено.

По умолчанию флажок снят.

- **Управление голосом**

  Если флажок установлен, управление голосом включено. Пользователь может управлять и взаимодействовать с устройством при помощи голосовых команд.

  Если флажок снят, управление голосом выключено.

  По умолчанию флажок снят.

- **Чтение с экрана (VoiceOver)**

  Если флажок установлен, чтение с экрана включено. Озвучивается описание того, что изображено на экране.

  Если флажок снят, чтение с экрана выключено.

  По умолчанию флажок снят.

- **Озвучивание выбранного текста**

  Если флажок установлен, озвучивание выбранного текста включено. Озвучивается текст, выбранный на экране.

  Если флажок снят, озвучивание выбранного текста отключено.

  По умолчанию флажок снят.

- **Кнопки регулировки громкости**

  Если флажок установлен, кнопки регулировки громкости включены. Пользователь может регулировать громкость на устройстве.

  Если флажок снят, кнопки регулировки громкости отключены.

  По умолчанию флажок установлен.

- **Моно-аудио**

  Если флажок установлен, моно-аудио включено. В левом и правом каналах наушников воспроизводится один и тот же контент.

  Если флажок снят, моно-аудио отключено.

  По умолчанию флажок снят.

- **Масштаб**

Если флажок установлен, возможность масштабирования включена. Пользователь может увеличивать или уменьшать масштаб объектов на экране.

Если флажок снят, возможность масштабирования отключена.

По умолчанию флажок установлен.

- **Автоповорот экрана**

  Если флажок установлен, автоматический поворот экрана включен. Ориентация экрана автоматически меняется при повороте устройства.

  Если флажок снят, автоматический поворот экрана отключен.

  По умолчанию флажок установлен.

- **Инверсия цвета**

  Если флажок установлен, инверсия цветов на экране включена. Цвета на экране заменены на противоположные.

  Если флажок снят, инверсия цветов на экране отключена.

  По умолчанию флажок снят.

- **Переключатель "Звонок/Бесшумно"**

  Если флажок установлен, переключение между режимами "Звонок" и "Бесшумно" включено. Пользователь может переключаться между режимами для включения или выключения рингтонов и предупреждений.

  Если флажок снят, переключение между режимами "Звонок" и "Бесшумно" отключено.

  По умолчанию флажок установлен.

- **Кнопка "Режим сна/Пробуждение"**

  Если флажок установлен, кнопка "Режим сна/Пробуждение" включена. Пользователь может включать или выключать режим сна на устройстве.

  Если флажок снят, кнопка "Режим сна/Пробуждение" отключена.

  По умолчанию флажок установлен.

Управление параметрами мобильных устройств

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

Настройка подключения к сети Wi-Fi

В этом разделе содержатся инструкции по настройке автоматического подключения к корпоративной сети Wi-Fi на Android- и iOS MDM-устройствах.

Подключение Android-устройств к сети Wi-Fi

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.

   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 **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. Если вы выбрали протокол безопасности 802.1.x EAP, укажите следующие параметры защиты сети:

    - Метод EAP

Определяет метод аутентификации в сети EAP (Extensible Authentication Protocol). Возможные значения:

- TLS (по умолчанию);
- PEAP;
- TTLS.

- **Корневой сертификат**

Определяет корневой сертификат, который будет использоваться сетью Wi-Fi, если выбран метод TLS EAP.

Вы можете указать сертификат одним из следующих способов:

- Выберите любой доступный сертификат из раскрывающегося списка. Он содержит сертификаты, ранее добавленные в раздел **Корневые сертификаты**. На устройствах эти сертификаты устанавливаются в доверенное хранилище сертификатов.
- Загрузите новый файл сертификата (`.cer`, `.pem` или `.key`), нажав на кнопку **Обзор**. Этот сертификат не будет добавлен в раздел **Корневые сертификаты**. Сертификат будет использоваться на устройствах только для настройки этой сети Wi-Fi и не будет установлен в доверенное хранилище сертификатов.

- **Домен**

Определяет условие для имени домена сервера.

Если указано полное доменное имя (FQDN), оно используется в качестве требования к совпадению суффикса для корневого сертификата в элементе(-ах) SubjectAltName dNSName. Если найден совпадающий dNSName, условие соблюдается.

Вы можете указать несколько вариантов строк для поиска совпадений, используя точку с запятой в качестве разделителя. Совпадение с любым из значений считается достаточным совпадением для сертификата (то есть используется оператор ИЛИ).

Если указать *, любой корневой сертификат будет считаться действительным. Это значение указано по умолчанию.

- **Сертификат пользователя**

Определяет сертификат пользователя, который будет использоваться сетью Wi-Fi, если выбран метод TLS EAP.

В раскрывающемся списке доступны следующие значения:

- **Не задан** – сертификат пользователя не указан.
- **VPN-сертификат** - последний VPN-сертификат, добавленный в разделе **Управление мобильными устройствами** > **Сертификаты** Консоли администрирования Kaspersky Security Center и установленный на устройстве пользователя. При выборе этого варианта, если на устройстве пользователя не установлен VPN-сертификат, сертификат пользователя не будет использоваться для этой сети Wi-Fi.
- Список профилей сертификатов SCEP, настроенных в разделе **SCEP и NDES** и используемых для получения сертификатов.

- **Тип двухфакторной аутентификации**

  Определяет тип двухфакторной аутентификации. Возможные значения:

  - нет (по умолчанию);
  - MSCHAP;
  - MSCHAPV2;
  - GTC.

- **Идентификатор пользователя**

  Определяет идентификатор пользователя, который будет использоваться, если выбран метод TLS EAP. Вы можете ввести значение или выбрать его в раскрывающемся списке **Доступные макросы**.

- **Анонимный идентификатор**

  Определяет анонимный идентификатор, который отличается от идентификатора пользователя и используется, если выбран метод аутентификации в сети PEAP. 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.

- Пароль

Определяет пароль для доступа к беспроводной сети, защищенной по протоколу WEP или WPA2 PSK. Пароль передается с QR-кодом.

Не используйте пароль от конфиденциальной сети Wi-Fi. Пароль передается пользователю в открытом виде вместе с другими данными, необходимыми для настройки устройства.

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 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.

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**.

    Этот список содержит имена предлагаемых беспроводных сетей.

    На личных устройствах под управлением Android 10 или выше операционная система предлагает пользователю подключиться к таким сетям. Предлагаемые сети не отображаются в списке сохраненных сетей на этих устройствах.

    На устройствах, работающих в режиме device owner, и на личных устройствах под управлением Android 9 или ниже после синхронизации устройства с Сервером администрирования пользователь может выбрать предлагаемую беспроводную сеть в списке сохраненных сетей и подключиться к ней, при этом не потребуется задавать никакие настройки сети.

    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 изменены после очередной синхронизации устройства с Kaspersky Security Center.

На устройствах под управлением Android 10 и выше, если пользователь отказывается подключаться к предлагаемой сети Wi-Fi, разрешение приложения на изменение состояния Wi-Fi аннулируется. Пользователю необходимо предоставить это разрешение вручную.

Подключение iOS MDM-устройств к сети Wi-Fi

Для автоматического подключения iOS MDM-устройства к доступной сети Wi-Fi и обеспечения безопасности данных следует настроить параметры подключения.

Чтобы настроить подключение iOS MDM-устройства к сети Wi-Fi, выполните следующие действия:

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

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

3. Откройте окно свойств политики двойным щелчком мыши 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 **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 **Пропустить страницу авторизации**.

   Для использования подписной сети необходимо оформить подписку, принять соглашение или внести плату. Подписные сети развернуты, например, в кафе или гостиницах.

9. Чтобы сеть Wi-Fi не отображалась в списке доступных сетей на iOS MDM-устройстве, установите флажок **Скрытая сеть**.

   В этом случае для подключения к сети пользователю потребуется вручную ввести на мобильном устройстве идентификатор сети SSID, заданный в параметрах маршрутизатора Wi-Fi.

10. В раскрывающемся списке **Защита сети** выберите тип защиты подключения к сети Wi-Fi:

    - **Выключена**. Аутентификация пользователя не требуется.
    - **WEP**. Сеть защищена по протоколу шифрования WEP (Wireless Encryption Protocol).
    - **WPA/WPA2 (личная)**. Сеть защищена по протоколу шифрования WPA/WPA2 (Wi-Fi Protected Access).
    - **WPA2 (личная)**. Сеть защищена по протоколу шифрования WPA2 (Wi-Fi Protected Access 2.0). Тип защиты WPA2 доступен на устройствах под управлением iOS версии 8 и выше. WPA2 не доступен на устройствах Apple TV.
    - **Любая (личная)**. Сеть защищена по протоколу шифрования WEP, WPA или WPA2 в зависимости от типа маршрутизатора Wi-Fi. Для аутентификации используется индивидуальный для каждого пользователя ключ шифрования.
    - **WEP (динамическая)**. Сеть защищена по протоколу шифрования WEP с использованием динамического ключа.
    - **WPA/WPA2 (корпоративная)**. Сеть защищена по протоколу шифрования WPA/WPA2 с использованием протокола 802.1X.
    - **WPA2 (корпоративная)**. Сеть защищена по протоколу шифрования WPA2 с использованием одного ключа шифрования для всех пользователей (802.1X). Тип защиты WPA2 доступен на устройствах под управлением iOS версии 8 и выше. WPA2 не доступен на устройствах Apple TV.
    - **Любая (корпоративная)**. Сеть защищена по протоколу шифрования WEP или WPA/WPA2 в зависимости от типа маршрутизатора Wi-Fi. Для аутентификации используется один ключ шифрования для всех пользователей.

Если в списке **Защита сети** вы выбрали **WEP (динамическая)**, **WPA/WPA2 (корпоративная)**, **WPA2 (корпоративная)** или **Любая (корпоративная)**, в блоке **Протоколы** вы можете выбрать типы протоколов EAP (Extensible Authentication Protocol) для идентификации пользователя в сети Wi-Fi.

В блоке **Доверенные сертификаты** вы также можете сформировать список доверенных сертификатов для аутентификации пользователя iOS MDM-устройства на доверенных серверах.

11. Настройте параметры учетной записи для аутентификации пользователя при подключении iOS MDM-устройства к сети Wi-Fi:

    a. В блоке **Аутентификация** нажмите кнопку **Настроить**.

    Откроется окно **Аутентификация**.

    b. В поле **Имя пользователя** введите имя учетной записи для аутентификации пользователя при подключении к сети Wi-Fi.

    c. Чтобы требовать у пользователя ввести пароль вручную при каждом подключении к сети Wi-Fi, установите флажок **Требовать пароль при каждом подключении**.

    d. В поле **Пароль** введите пароль учетной записи для аутентификации в сети Wi-Fi.

    e. В раскрывающемся списке **Сертификат для аутентификации** выберите сертификат для аутентификации пользователя в сети Wi-Fi. Если в списке отсутствуют сертификаты, вы можете их добавить в разделе Сертификаты.

    f. В поле **Идентификатор пользователя** введите идентификатор пользователя, который будет отображаться во время передачи данных при аутентификации вместо реального имени пользователя.

    Идентификатор пользователя предназначен для повышения уровня безопасности аутентификации, так как имя пользователя не представлено в открытом виде, а отображается в зашифрованном TLS-туннеле.

    g. Нажмите кнопку **ОК**.

В результате на iOS MDM-устройстве будут настроены параметры учетной записи для аутентификации пользователя при подключении к сети Wi-Fi.

12. Настройте (если требуется) параметры подключения к сети Wi-Fi через прокси-сервер:

    a. В блоке **Прокси-сервер** нажмите на кнопку **Настроить**.

    b. В открывшемся окне **Прокси-сервер** выберите режим настройки прокси-сервера и укажите параметры подключения.

    c. Нажмите кнопку **ОК**.

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

13. Нажмите кнопку **ОК**.

    Новая сеть Wi-Fi отобразится в списке.

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

В результате на iOS MDM-устройстве пользователя после применения политики будет настроено подключение к сети Wi-Fi. Мобильное устройство пользователя будет автоматически подключаться к доступной сети Wi-Fi. Безопасность данных при подключении к сети Wi-Fi обеспечивается технологией аутентификации.

Настройка электронной почты

Этот раздел содержит информацию о настройке почтовых ящиков на мобильных устройствах.

Настройка почтового ящика на iOS MDM-устройствах

Чтобы пользователь iOS MDM-устройства мог работать с электронной почтой, следует добавить учетную запись электронной почты в список учетных записей на iOS MDM-устройстве.

По умолчанию добавляется учетная запись электронной почты со следующими параметрами:

- протокол электронной почты – IMAP;
- пользователь может перемещать сообщения электронной почты между своими учетными записями и синхронизировать адреса учетных записей;
- для работы с почтой пользователь может использовать любые почтовые клиенты (не только Mail);
- при передаче сообщений не используется SSL-соединение.

Вы можете изменить указанные параметры при добавлении учетной записи.

Чтобы добавить учетную запись электронной почты пользователя iOS MDM-устройства, выполните следующие действия:

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

      Если вы хотите запретить сохранять, перемещать и отправлять вложения из корпоративного почтового ящика, снимите флажки **Разрешить перемещать сообщения между учетными записями**, **Разрешить передачу документов из управляемых в неуправляемые приложения** и **Разрешить передачу документов из неуправляемых в управляемые приложения**.

    - 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 **Настроить** настройте параметры подключения к серверам:

    - **Адрес сервера и порт**: имена хостов или IP-адреса серверов входящей и исходящей почты и номера портов серверов.

    - **Имя учетной записи**: имя учетной записи пользователя для авторизации на сервере входящей и исходящей почты.

    - **Тип аутентификации**: тип аутентификации учетной записи пользователя электронной почты на серверах входящей и исходящей почты.

- **Пароль**: пароль учетной записи для авторизации на сервере входящей и исходящей почты, защищенный выбранным методом аутентификации.

- **Использовать один пароль для серверов входящей и исходящей почты**: использование одного пароля для аутентификации пользователя на серверах входящей и исходящей почты.

- **Использовать SSL-соединение**: использование транспортного протокола передачи данных SSL (Secure Sockets Layer), который применяет шифрование и аутентификацию на базе сертификатов для защиты передачи данных.

14. Нажмите кнопку **ОК**.

    Новая учетная запись электронной почты отобразится в списке.

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

В результате на мобильное устройство пользователя после применения политики будут добавлены учетные записи электронной почты из сформированного списка.

Настройка почтового ящика Exchange на iOS MDM-устройствах

Чтобы пользователь iOS MDM-устройства мог работать с корпоративной электронной почтой, календарем, контактами, заметками и задачами, на сервер Microsoft Exchange следует добавить учетную запись Exchange ActiveSync.

По умолчанию на сервер Microsoft Exchange добавляется учетная запись со следующими параметрами:

- почта синхронизируется один раз в неделю;

- пользователь может перемещать сообщения между своими учетными записями и синхронизировать адреса учетных записей;

- для работы с почтой пользователь может использовать любые почтовые клиенты (не только Mail);

- при передаче сообщений не используется SSL-соединение.

Вы можете изменить указанные параметры при добавлении учетной записи Exchange ActiveSync.

Чтобы добавить учетную запись Exchange ActiveSync пользователя iOS MDM-устройства, выполните следующие действия:

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

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

3. Откройте окно свойств политики двойным щелчком мыши 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 **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**;

      Если вы хотите запретить сохранять, перемещать и отправлять вложения из корпоративного почтового ящика, снимите флажки **Разрешить перемещать сообщения между учетными записями**, Разрешить передачу документов из управляемых в неуправляемые приложения и Разрешить передачу документов из неуправляемых в управляемые приложения.

    - **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 **OK**.

    Новая учетная запись Exchange ActiveSync отобразится в списке.

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

В результате на мобильное устройство пользователя после применения политики будут добавлены учетные записи Exchange ActiveSync из сформированного списка.

Настройка почтового ящика Exchange на Android-устройствах (только Samsung)

Для работы с корпоративной почтой, контактами и календарем на мобильном устройстве следует настроить параметры почтового ящика Exchange (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.

   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 → Управление Samsung-устройством**.
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 изменены после очередной синхронизации устройства с Kaspersky Security Center.

Настройка статуса устройства в Kaspersky Security Center

Чтобы настроить статус устройства 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.

   В течение 15 минут выполните следующие действия. По истечении этого времени при сохранении изменений политики может возникнуть ошибка.

4. В окне **Свойства: <Название политики>** выберите раздел **Информация об устройстве**.
5. В открывшемся окне выберите статус **OK**, **Критический** или **Предупреждение** для каждого из следующих условий:
   - **Постоянная защита не работает**
   - **Веб-Фильтр не работает**
   - **Контроль приложений не работает**
   - **Блокирование устройства недоступно**
   - **Определение местоположения устройства недоступно**
   - **Версии Положения о KSN не совпадают**
   - **Версии Маркетингового положения не совпадают**
6. Нажмите на кнопку **OK**.

Управление настройками приложения

В этом разделе приведены инструкции по управлению параметрами и редактированию конфигураций приложений, установленных на устройствах ваших пользователей.

Управление настройками Google Chrome

В разделе **Настройки Google Chrome** вы можете настроить следующие параметры, применимые к браузеру Google Chrome, установленному в рабочем профиле Android или на устройствах, управляемых Kaspersky Endpoint Security 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.

   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 **Конфигурация приложения** > **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**
  - 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 (на основе базы данных злоупотреблений от Google)

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.

  Будут блокироваться только те всплывающие окна, которые присутствуют в базе данных злоупотреблений от Google.

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 (на основе базы данных злоупотреблений от Google)** 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 (на основе базы данных злоупотреблений от Google)

Список сайтов, которым запрещено показывать всплывающие окна. Также вы можете задавать шаблоны URL, например: [*.]example.com.

Будут блокироваться только те всплывающие окна, которые присутствуют в базе данных злоупотреблений от Google.

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 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 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 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.

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.
  - 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 перевода

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.

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.

Управление Exchange ActiveSync для Gmail

Раздел **Exchange ActiveSync** позволяет управлять настройками Exchange ActiveSync для Gmail, установленного в рабочем профиле Android или на устройствах, управляемых через приложение Kaspersky Endpoint Security для Android, 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.

   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 **Конфигурация приложения** > **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.

- **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 на кнопку **Применить**, чтобы сохранить внесенные изменения.

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

Настройка прочих приложений

Параметры в блоке **Прочие приложения** позволяют настраивать приложения, установленные на устройствах под управлением Kaspersky Endpoint Security для Android в режиме device owner или установленные в рабочем профиле Android.

При настройке некоторых приложений можно использовать сертификаты, установленные на устройства через Kaspersky Security Center. В этом случае вам необходимо указать псевдоним сертификата в конфигурации приложения:

- `VpnCert` для сертификатов VPN.
- `MailCert` для почтовых сертификатов.
- `SCEP_profile_name` для сертификатов, полученных с помощью SCEP.

*Чтобы настроить приложения в разделе **Прочие 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.

   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 **Конфигурация приложения** > **Прочие приложения**.
5. В разделе **Список конфигураций приложений** нажмите на кнопку **Добавить**.

   Откроется окно **Добавить конфигурацию приложения**.

6. В открывшемся окне укажите следующие параметры:

   - **Активировать**

     Определяет, будет ли конфигурация применена к приложению на устройствах, попадающих под действие политики.

     По умолчанию флажок установлен.

   - **Название приложения (обязательно для заполнения)**

     Название приложения, к которому будет применена конфигурация.

     При импорте конфигурации из APK-файла или инсталляционного пакета значение подставляется автоматически.

- **Имя пакета (обязательно для заполнения)**

  Название пакета приложения, к которому будет применена конфигурация. **Как получить имя пакета приложения**

  Чтобы получить имя пакета приложения:

  1. Откройте Google Play.
  2. Найдите нужное приложение и откройте его страницу.

     URL приложения оканчивается именем пакета приложения (например, https://play.google.com/store/apps/details?id=**com.android.chrome**).

  Чтобы получить имя пакета приложения, которое было добавлено в Kaspersky Security Center:

  1. В дереве консоли Kaspersky Security Center выберите **Дополнительно** > **Удаленная установка** > **Инсталляционные пакеты**.
  2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Управление пакетами мобильных приложений**.

     В открывшемся окне **Управление пакетами мобильных приложений** в столбце **Название приложения** отображаются идентификаторы управляемых приложений.

     Если пакет приложения представлен файлом в формате APK, и необходимо узнать идентификатор приложения, можно добавить этот пакет приложения в окне **Управление пакетами мобильных приложений**, нажав на кнопку **Новый** и следуя инструкциям на экране.

  При импорте конфигурации из APK-файла или инсталляционного пакета значение подставляется автоматически.

  Для одного имени пакета можно добавить только одну конфигурацию.

- **Версия**

  Версия приложения, на основе которой будет создана конфигурация.

  При импорте конфигурации из APK-файла или инсталляционного пакета значение подставляется автоматически.

- **Комментарий**

  Необязательный комментарий.

7. В этом же окне выберите способ добавления конфигурации:

- **Вручную**

Если выбран этот метод, нажмите кнопку **Добавить**, чтобы добавить новую настройку в конфигурацию. Для каждой настройки конфигурации необходимо указать следующие параметры:

- **Идентификатор**

  Обязателен для заполнения. Значение этого параметра заполняется вручную.

- **Тип**

  Обязателен для заполнения. Значение этого параметра выбирается из выпадающего списка.

  Доступны следующие типы:

  - String — последовательность букв, цифр или символов, всегда рассматривается как текст.
  - Boolean — значения True или False.
  - Integer — числовой тип данных для чисел без дробной части.
  - Choice — тип данных, позволяющий выбрать один вариант из списка возможных.
  - Multiple choice — тип данных, позволяющий выбрать один или несколько вариантов из списка возможных.
  - Bundle — набор полей любого типа, кроме Bundle и BundleArray.
  - BundleArray — множество наборов полей типа Bundle.

- **Значение**

  Необязательный параметр, значение зависит от типа настройки.

  Для некоторых типов настроек можно настроить дополнительные параметры. Например, вы можете добавить макросы для настройки типа **String**, добавить поле в настройку типа **Bundle** или добавить пакет в настройку типа **BundleArray**.

  Также можно отредактировать настройку, которая будет добавлена в BundleArray, нажав кнопку **Изменить** и настроив параметры настройки.

  Для получения информации о правилах настройки конфигурации обратитесь к официальной документации для настраиваемого приложения.

- **С помощью инсталляционного пакета из Kaspersky Security Center**

  При добавлении конфигурации приложения с помощью инсталляционного пакета из Kaspersky Security Center необходимо выбрать файл из списка пакетов мобильных приложений.

  После этого можно просмотреть описание каждой настройки конфигурации. Описания являются частью файла конфигурации.

  Настройки конфигураций, добавленных с помощью инсталляционных пакетов, недоступны для удаления.

- С помощью APK-файла на вашем компьютере

  При добавлении конфигурации приложения с помощью APK-файла необходимо выбрать файл, сохраненный на вашем компьютере.

  После этого можно просмотреть описание каждой настройки конфигурации. Описания являются частью файла конфигурации.

  Настройки конфигураций, добавленных с помощью APK-файлов, недоступны для удаления.

Пример настройки основных параметров для приложения Microsoft Outlook.

Конфигурация приложения Microsoft Outlook

Ключ конфигурации	Описание	Тип	Значение	Зн ум
`com.microsoft.outlook.EmailProfile.EmailAccountName`	Имя пользователя	String	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**. Например, `User`.	
`com.microsoft.outlook.EmailProfile.EmailAddress`	Адрес электронной почты	String	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**. Например, `user@companyname.com`.	
`com.microsoft.outlook.EmailProfile.EmailUPN`	Имя участника-пользователя или имя пользователя для профиля электронной почты, который используется для аутентификации учетной записи	String	Имя пользователя в формате адреса электронной почты. Например, `userupn@companyname.com`.	
`com.microsoft.outlook.EmailProfile.ServerAuthentication`	Метод аутентификации	String	`Username and Password` – запрашивает пароль у пользователя устройства. `Certificates` – проверка подлинности на основе сертификатов.	Us an Pa
`com.microsoft.outlook.EmailProfile.ServerHostName`	Полное доменное имя ActiveSync	String	URL почтового сервера Exchange ActiveSync. Перед URL не обязательно использовать HTTP:// или HTTPS://. Например, `mail.companyname.com`.	
`com.microsoft.outlook.EmailProfile.AccountDomain`	Домен электронной почты	String	Домен учетной записи пользователя. Вы можете ввести значение или выбрать его в раскрывающемся списке **Доступные макросы**. Например, `companyname`.	
`com.microsoft.outlook.EmailProfile.AccountType`	Тип аутентификации	String	`ModernAuth` – использует метод аутентификации на основе маркеров. Укажите ModernAuth в качестве типа учетной записи для Exchange Online.	Ba

			`BasicAuth` – запрашивает пароль у пользователя устройства. Укажите BasicAuth в качестве типа учетной записи для локальной версии Exchange.	

8. Нажмите на кнопку **OK**, чтобы применить конфигурацию.

   Конфигурация появится в **Списке конфигураций приложений**.

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

Конфигурация применена. Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Kaspersky Security Center.

Чтобы изменить конфигурацию приложения:

1. В разделе **Прочие приложения** выберите приложение из списка и нажмите на кнопку **Изменить**.

   Откроется окно **Изменить конфигурацию приложения**.

2. В окне **Изменить конфигурацию приложения** можно отредактировать конфигурацию выбранного приложения:

   - Чтобы загрузить новый APK-файл со своего компьютера, нажмите на кнопку **Выбрать**.
   - Чтобы добавить новую настройку в конфигурацию, нажмите на кнопку **Добавить** под всеми параметрами, а затем укажите необходимые параметры.
   - Чтобы удалить настройку, добавленную вручную, нажмите кнопку **X** в правом верхнем углу поля настройки.

3. Нажмите на кнопку **OK**, чтобы закрыть окно **Изменить конфигурацию приложения**.

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

Примененная конфигурация изменена. Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Kaspersky Security Center.

Чтобы включить или отключить конфигурацию приложения:

1. В разделе **Прочие программы** выберите приложение из списка.

2. Выполните одно из следующих действий:

   - Установите переключатель в положение Вкл., чтобы включить конфигурацию.
   - Установите переключатель в положение Выкл., чтобы отключить конфигурацию.

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

Примененная конфигурация изменена. Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Kaspersky Security Center.

Чтобы удалить конфигурацию приложения:

1. В разделе **Прочие программы** выберите приложение из списка и нажмите на кнопку **Удалить**.

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

   Примененная конфигурация удалена. Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Kaspersky Security Center.

Управление разрешениями приложений

Параметры в блоке **Управление разрешениями приложений** позволяют настраивать правила выдачи дополнительных разрешений приложениям, установленным на устройствах под управлением Kaspersky Endpoint Security для Android в режиме device owner или установленным в рабочем профиле Android.

Вы можете настроить правила выдачи дополнительных разрешений путем создания или изменения файлов конфигурации для определенных приложений.

Правила выдачи разрешений, настроенные для отдельных приложений, имеют приоритет над общей политикой выдачи разрешений для приложений, установленных на устройствах или в рабочем профиле Android. Например, если вы сначала выберете параметр **Отклонять разрешения автоматически** в разделе Рабочий профиль Android, а затем выберете параметр **Выдавать разрешения автоматически** для определенного приложения в разделе **Управление разрешениями приложений**, разрешение для этого приложения будет выдано автоматически.

Чтобы добавить разрешения для приложения:

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 окне **Свойства: <Название политики>** выберите раздел **Управление разрешениями приложений**.

5. Нажмите на кнопку **Добавить**.

   Откроется окно **Добавить правила выдачи разрешений**.

6. Выберите способ добавления конфигурации с правилами выдачи разрешений:

   - Вручную

     При добавлении конфигурации вручную необходимо нажать на кнопку **Добавить разрешение** и в раскрывающихся списках выбрать разрешение и действие, выполняемое для него.

   - С помощью инсталляционного пакета из Kaspersky Security Center

При добавлении конфигурации приложения с помощью инсталляционного пакета из Kaspersky Security Center необходимо выбрать файл из списка пакетов мобильных приложений.

После этого можно просмотреть список дополнительных разрешений и выбрать действие, выполняемое для каждого разрешения.

- **С помощью APK-файла на вашем компьютере**

  При добавлении конфигурации приложения с помощью APK-файла необходимо выбрать файл, сохраненный на вашем компьютере.

  После этого можно просмотреть список дополнительных разрешений и выбрать действие, выполняемое для каждого разрешения.

7. Задайте следующие параметры:

- **Название приложения (обязательно для заполнения)**

  Название приложения, для которого нужно настроить разрешения.

  При импорте конфигурации из APK-файла или инсталляционного пакета значение подставляется автоматически.

- **Имя пакета (обязательно для заполнения)**

Название пакета приложения, для которого нужно настроить разрешения.

Как получить имя пакета приложения

Чтобы получить имя пакета приложения:

1. Откройте Google Play.
2. Найдите нужное приложение и откройте его страницу.

   URL приложения оканчивается именем пакета приложения (например, https://play.google.com/store/apps/details?id=**com.android.chrome**).

Чтобы получить имя пакета приложения, которое было добавлено в Kaspersky Security Center:

1. В дереве консоли Kaspersky Security Center выберите **Дополнительно** > **Удаленная установка** > **Инсталляционные пакеты**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Управление пакетами мобильных приложений**.

   В открывшемся окне **Управление пакетами мобильных приложений** в столбце **Название приложения** отображаются идентификаторы управляемых приложений.

   Если пакет приложения представлен файлом в формате APK, и необходимо узнать идентификатор приложения, можно добавить этот пакет приложения в окне **Управление пакетами мобильных приложений**, нажав на кнопку **Новый** и следуя инструкциям на экране.

При импорте конфигурации из APK-файла или инсталляционного пакета значение подставляется автоматически.

- **Комментарий**

  Необязательный комментарий.

8. Нажмите на кнопку **Добавить разрешение**, чтобы открыть блок настройки разрешений для приложения. Вы можете добавить несколько разрешений.

   Выберите одно из следующих **разрешений**.

- Разрешение на продолжение вызова из другого приложения
- Разрешения на использование местоположения
- Разрешение на использование сохраненных местоположений
- Разрешение на распознавание физической активности
- Разрешение на запись голосовых сообщений в автоответчике
- Разрешение на ответ на телефонные звонки
- Разрешения для Bluetooth
- Разрешения на доступ к данным биометрических датчиков
- Разрешение на совершение телефонных звонков
- Разрешения на доступ к камере
- Разрешение на доступ к списку учетных записей
- Разрешение на доступ к ближайшим устройствам через Wi-Fi
- Разрешение на отправку уведомлений
- Разрешение на управление исходящими звонками
- Разрешение на чтение данных календаря
- Разрешение на чтение данных журнала звонков
- Разрешение на чтение данных списка контактов
- Разрешения на чтение данных внешнего хранилища
- Разрешение на чтение телефонных номеров устройства
- Разрешение на чтение состояния телефона
- Разрешение на отслеживание входящих SMS и MMS сообщений
- Разрешение на получение push-сообщений WAP
- Разрешение на запись звука
- Разрешение на отправку SMS
- Разрешение на использование SIP-телефонии
- Разрешение на доступ к устройствам, использующим сверхширокополосной доступ (UWB)
- Разрешение на запись данных в календаре

- Разрешение на запись и чтение данных в журнале звонков
- Разрешение на запись в списке контактов
- Разрешение на запись данных во внешнем хранилище

Чтобы настроить правила выдачи дополнительных разрешений, для каждого разрешения необходимо выбрать одно из следующих действий:

- **Запрашивать разрешения у пользователя**

  Пользователь решает, выдавать ли разрешение приложению.

  Этот параметр выбран по умолчанию.

- **Выдавать разрешения автоматически**

  Разрешение для приложения выдается без участия пользователя.

- **Отклонять разрешения автоматически**

  Запрос на разрешение для приложения отклоняется без участия пользователя.

Для каждого разрешения можно сохранить только одно правило.

9. Нажмите на кнопку **OK**, чтобы применить конфигурацию.

   Конфигурация появится в **Списке разрешений приложений**.

10. Нажмите на кнопку **Применить**, чтобы сохранить изменения.

Конфигурация с правилами выдачи разрешений применена. Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Kaspersky Security Center.

Чтобы изменить разрешения для приложения:

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 окне **Свойства: <Название политики>** выберите раздел **Управление разрешениями приложений**.
5. Выберите приложение в блоке **Список разрешений приложений** и нажмите на кнопку **Изменить**.

   Откроется окно **Изменить правила выдачи разрешений**.

6. Отредактируйте выбранное правило выдачи разрешений:

- Чтобы добавить новое разрешение в конфигурацию, нажмите на кнопку **Добавить разрешение** под всеми параметрами, а затем выберите разрешение и действие, которое нужно выполнить для этого разрешения.

  Вы можете добавить несколько разрешений.

- Чтобы изменить действие для существующего разрешения, выберите другое действие в списке.

- Чтобы удалить разрешение, добавленное вручную, нажмите на кнопку **X** в правом верхнем углу поля настройки.

7. Нажмите на кнопку **OK**, чтобы закрыть окно **Изменить правила выдачи разрешений**.

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

Выбранная конфигурация с правилами выдачи разрешений изменена. Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Kaspersky Security Center.

Чтобы удалить разрешения для приложения:

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 окне **Свойства: <Название политики>** выберите раздел **Управление разрешениями приложений**.

5. Выберите приложение в блоке **Список разрешений приложений** и нажмите на кнопку **Удалить**.

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

Настроенные разрешения для выбранного приложения удалены. Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Kaspersky Security Center.

Создание отчета об установленных мобильных приложениях

Отчет об установленных мобильных приложениях позволяет получить подробную информацию о приложениях, установленных на Android-устройствах пользователей, сохранить эту информацию в файл, отправить по электронной почте и распечатать.

Чтобы отчет отображал информацию, необходимо установить флажок **Отправлять данные об установленных приложениях** в разделе **Контроль приложений** и включить сохранение в базе данных Сервера администрирования информационного события типа **Установлено или удалено приложение (список установленных приложений)**.

Чтобы разрешить отправку 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.

   В течение 15 минут выполните следующие действия. По истечении этого времени при сохранении изменений политики может возникнуть ошибка.

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

5. В разделе **Отчет об установленных мобильных приложениях** установите флажок **Отправлять данные об установленных приложениях**.

   Стали доступны следующие параметры:

   - Установите флажок **Отправлять данные о системных приложениях**, чтобы отправлять информацию о системных приложениях. Если системное приложение настроено в параметрах раздела **Контроль приложений**, данные о нем будут отправляться независимо от состояния этого флажка.

   - Установите флажок **Отправлять данные о служебных приложениях**, чтобы отправлять информацию о служебных приложениях без интерфейса. Если служебное приложение настроено в параметрах раздела **Контроль приложений**, данные о нем будут отправляться независимо от состояния этого флажка.

6. Нажмите на кнопку **Применить**, чтобы применить изменения.

7. В окне **Свойства: <Название политики>** выберите раздел **Настройка событий**.

8. В рабочей области группы выберите закладку **Информационное сообщение**.

9. Откройте свойства события **Установлено или удалено приложение (список установленных приложений)** с помощью двойного щелчка мыши на любом столбце.

10. В окне **Свойства** события установите флажок **Хранить в базе данных Сервера администрирования в течение (сут)** и настройте значение срока хранения. Срок, заданный по умолчанию, – 30 дней.

    По истечении срока хранения Сервер администрирования удаляет устаревшую информацию из базы данных. Дополнительная информация о событиях приведена в справке Kaspersky Security Center.

11. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Отправка данных разрешена.

Чтобы настроить отчет по установленным мобильным приложениям:

1. В дереве консоли перейдите в папку Сервера администрирования.

2. В рабочей области папки Сервера администрирования выберите закладку **Отчеты**.

3. В контекстном меню шаблона отчета **Отчет об установленных мобильных приложениях** выберите пункт **Свойства**.

4. В открывшемся окне вы можете изменить свойства шаблона отчета:

- В разделе **Общие** укажите следующие параметры:
  - **Название шаблона отчета.**
  - Максимальное число отображаемых записей

    Если этот параметр включен, количество отображаемых в таблице записей с подробными данными отчета не превышает указанное значение.

    Записи отчета сначала сортируются в соответствии с правилами, указанными в разделе **Графы → Детальные данные** свойств шаблона отчета, а затем сохраняется только первая часть результирующих записей. В заголовке таблицы с подробными данными отчета показано отображаемое количество записей и общее количество записей, соответствующее другим параметрам шаблона отчета.

    Если этот параметр выключен, в таблице с подробными данными отчета отображаются все записи. Не рекомендуется выключать этот параметр. Ограничение количества отображаемых записей отчета снижает нагрузку на систему управления базами данных и время, требуемое для формирования и экспорта отчета. В некоторых отчетах содержится слишком большое количество записей. В таких случаях просмотр и анализ всех записей может оказаться слишком трудоемким. Также на устройстве при формировании такого отчета может закончиться память. Это может привести к тому, что вам не удастся просмотреть отчет.

    По умолчанию параметр включен. По умолчанию указано значение 1000.

  - Print version

    Отчет оптимизирован для печати: добавлены пробелы, между некоторыми значениями для лучшей визуальной доступности.

    По умолчанию параметр включен.

- В разделе **Поля** выберите поля, которые будут отображаться в отчете, и порядок этих полей, а также настройте необходимость сортировки и фильтрации информации в отчете по каждому из полей.
- В разделе **Группа** измените набор клиентских устройств, для которых создается отчет.
- В разделе **Иерархия Серверов администрирования** укажите следующие параметры:
  - Включать данные подчиненных и виртуальных Серверов администрирования

    Если этот параметр включен, отчет содержит информацию с подчиненных и виртуальных Серверов администрирования, которые подчинены Серверу администрирования, для которого создан шаблон отчета.

    Выключите этот параметр, если вы хотите просматривать данные только текущего Сервера администрирования.

    По умолчанию параметр включен.

  - До уровня вложенности

Отчет содержит данные подчиненных и виртуальных Серверов администрирования, которые находятся под текущим Сервером администрирования на уровне вложенности ниже или равном указанному значению.

По умолчанию указано значение 1. Вы можете изменить это значение, если вы хотите видеть в отчете информацию подчиненных Серверов администрирования, расположенных на более низких уровнях вложенности дерева.

- **Период ожидания данных (мин)**

  Сервер администрирования, для которого создан шаблон отчета, ожидает данные от подчиненных Серверов администрирования в течение указанного времени для создания отчета. Если данные не получены от подчиненного Сервера администрирования в течение указанного интервала времени, отчет запускается в любом случае. Вместо фактических данных в отчете отображаются данные, полученные из кеша (если включен параметр **Кешировать данные с подчиненных Серверов администрирования**), или **N / A** (недоступно) в противном случае.

  По умолчанию время ожидания составляет 5 минут.

- **Кешировать данные с подчиненных Серверов администрирования**

  Подчиненные Серверы администрирования регулярно передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Переданные данные хранятся в кеше.

  Если Сервер администрирования не может получить данные подчиненного Сервера администрирования во время генерации отчета, в отчете отобразятся данные из кеша. В этом случае отображается дата, когда данные были переданы в кеш.

  Включение этой опции позволяет просматривать информацию, полученную от подчиненных Серверов администрирования, даже если невозможно получить актуальные данные. Однако отображаемые данные могут быть устаревшими.

  По умолчанию этот параметр отключен.

- **Период обновления данных в кеше (ч)**

  Подчиненные Серверы администрирования регулярно передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Вы можете указать этот период в часах. Если установлено значение 0, данные передаются только во время генерации отчета.

  По умолчанию указано значение 0.

- **Передавать подробную информацию с подчиненных Серверов администрирования**

  В созданном отчете таблица с подробными данными включает информацию с подчиненных Серверов администрирования главного Сервера администрирования, для которого создан шаблон отчета.

  Если этот параметр включен, то замедляется создание отчета и увеличивается трафик между Серверами администрирования. Однако вы можете просмотреть все данные в одном отчете.

  Чтобы не включать этот параметр, вы можете проанализировать данные отчета для нахождения неисправного подчиненного Сервера администрирования, а затем сформировать этот же отчет только для него.

  По умолчанию этот параметр отключен.

5. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Измененный шаблон отчета появится в списке шаблонов отчетов.

Чтобы создать и просмотреть отчет об установленных мобильных приложениях:

1. В дереве консоли перейдите в папку Сервера администрирования.
2. В рабочей области папки Сервера администрирования выберите закладку **Отчеты**.
3. Выберите шаблон отчета с именем **Отчет об установленных мобильных приложениях** с помощью двойного щелчка мыши на любом столбце.

Откроется отчет об установленных мобильных приложениях.

В этом отчете отображаются следующие данные:

- **Сводная информация**

  Отображает общие сведения об установленных приложениях, а также график установки приложений. Информация в таблице группируется по полю **Имя пакета**.

  Таблица содержит следующие поля:

  Имя пакета

  Название пакета установленного приложения.

  Название приложения

  Название установленного приложения, может зависеть от языковых настроек устройства.

  Количество устройств

  Количество устройств, на которых установлено приложение.

  Количество групп

  Количество групп, содержащих устройства с установленным приложением.

- **Подробнее**

Отображает информацию о каждом приложении, установленном на каждом устройстве.

Таблица содержит следующие поля:

Имя пакета

Название пакета установленного приложения.

Название приложения

Название установленного приложения, может зависеть от языковых настроек устройства.

Версия приложения

Версия установленного приложения.

Профиль

Профиль с установленным приложением: рабочий профиль Android или личный профиль.

Виртуальный Сервер администрирования

Идентификатор виртуального Сервера администрирования, который управляет устройством с установленным приложением.

Группа

Идентификатор группы, содержащей устройство с установленным приложением.

Устройство

Идентификатор устройства, на котором установлено приложение.

Последнее подключение к Серверу администрирования

Время последней синхронизации устройства с Сервером администрирования.

Дополнительная информация об использовании отчетов, управлении пользовательскими шаблонами отчетов, использовании шаблонов отчетов для создания новых отчетов и создании задач доставки отчетов приведена в справке Kaspersky Security Center.

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, которые будут установлены на Android-устройствах, в хранилище доверенных сертификатов.

Эти сертификаты устанавливаются на пользовательских устройствах следующим образом:

- На устройствах, работающих в режиме device owner, сертификаты устанавливаются автоматически.

  При удалении корневого сертификата в параметрах политики он автоматически удалится с устройства во время следующей синхронизации с Сервером администрирования.

- На личных устройствах (не работающих в режиме device owner):

  - Если рабочий профиль не был создан, пользователю устройства предлагается установить каждый сертификат вручную в личном профиле, следуя инструкциям в уведомлении.

  - Если рабочий профиль был создан, сертификаты автоматически установятся в этот профиль. Если флажок **Дублировать установку корневых сертификатов в личный профиль** установлен в настройках рабочего профиля, можно также установить сертификаты в личном профиле. Пользователю устройства предлагается сделать это вручную, следуя инструкциям в уведомлении.

    При удалении корневого сертификата в параметрах политики он автоматически удалится с устройства во время следующей синхронизации с Сервером администрирования.

    Инструкции по установке сертификатов в личном профиле можно найти в разделе Установка корневых сертификатов на устройстве.

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.

   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 **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.

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

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

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.

   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 **Дополнительно**.
5. В разделе **Уведомления приложения** нажмите на кнопку **Настроить**.

Откроется окно **Параметры уведомлений на устройстве**.

6. Выберите проблемы Kaspersky Endpoint Security для Android, которые вы хотите скрыть на мобильном устройстве пользователя и нажмите на кнопку **OK**.

   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 базы вредоносного ПО).

   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 изменены после очередной синхронизации устройства с Kaspersky Security Center. На мобильном устройстве пользователя не будут отображаться уведомления Kaspersky Endpoint Security для Android, которые вы выключили.

Основные функции управления мобильными устройствами в Консоли администрирования на базе MMC

Kaspersky Secure Mobility Management предоставляет следующие функции:

- Подключение Android-устройств к Kaspersky Security Center с использованием инсталляционного пакета приложения для скачивания с сервера Kaspersky Security Center.
- Подключение iOS-устройств к Kaspersky Security Center с помощью рассылки сообщений электронной почты со ссылкой и QR-кодом для скачивания iOS MDM-профиля с Сервера iOS MDM.
- Дистанционное подключение мобильных устройств к Kaspersky Security Center и другим сторонним EMM-системам (например, VMWare AirWatch, MobileIron, IBM Maas360, Microsoft Intune, 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.
- Обнаружение и устранение угроз на мобильных устройствах (Защита от вредоносного ПО).

- Предотвращение утечек корпоративной информации, хранящейся на мобильных устройствах, в случае их кражи или потери (Анти-Вор).
- Контроль использования интернета на мобильных устройствах (Веб-Фильтр).
- Контроль установки и удаления приложений (Контроль приложений).
- Контроль соблюдения требований корпоративной безопасности (Контроль соответствия).
- 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 или 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.
- Управление групповыми политиками безопасности мобильных устройств.
- Приложение Kaspersky Endpoint Security for Android app может быть обновлено до указанной версии с использованием 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).
- Отправка команд для удаленного управления мобильными устройствами. Например, если мобильное устройство потеряно или украдено, вы можете отправить команду, чтобы найти устройство или стереть все 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 сайтов с главного экрана мобильных устройств.

Kaspersky Secure Mobility Management включает следующие компоненты защиты и управления:

- Для Android-устройств:
  - Защита от вредоносного ПО

- Анти-Вор
- Веб-Фильтр
- Контроль приложений
- Контроль соответствия

- Для iOS MDM-устройств:
  - Защита паролем
  - Управление сетями
  - Веб-Фильтр
  - Контроль соответствия

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 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 **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 (только для supervised)**. Для этого добавьте в список разрешенных устройств MAC-адреса устройств AirPlay.

   К устройствам AirPlay, не входящим в список разрешенных устройств, доступ запрещен. Если оставить список разрешенных устройств пустым, Kaspersky Device Management для iOS разрешит доступ ко всем устройствам AirPlay.

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

В результате мобильное устройство пользователя после применения политики будет автоматически подключаться к устройствам AirPlay для передачи медиа-контента.

Подключение iOS MDM-устройств к AirPrint

Для печати документов с iOS MDM-устройства беспроводным способом с помощью технологии AirPrint следует настроить автоматическое подключение к принтерам AirPrint. Мобильное устройство и принтер должны быть подключены к одной беспроводной сети. На принтере AirPrint требуется настроить общий доступ для всех пользователей.

Чтобы настроить подключение iOS MDM-устройства к принтеру AirPrint, выполните следующие действия:

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

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

3. Откройте окно свойств политики двойным щелчком мыши 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 **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.

Отключение блокировки активации на контролируемых iOS-устройствах

Блокировка активации – это функция iOS, которая предотвращает использование потерянного или украденного iOS-устройства посторонними лицами или его повторную активацию без разрешения владельца. Kaspersky Security Center позволяет отключить блокировку активации на контролируемых iOS-устройствах без ввода Apple ID и пароля пользователя. Для этого используется код отключения блокировки.

Этот код создается, когда iOS-устройство подключается к Kaspersky Security Center и становится контролируемым.

Для отключения блокировки активации с помощью кода выполните следующие действия:

1. В дереве консоли выберите **Управление мобильными устройствами → Мобильные устройства**.
2. В списке устройств двойным щелчком выберите устройство, код отключения блокировки которого вы хотите посмотреть.

   Откроется окно свойств выбранного устройства.
3. В окне свойств выбранного устройства выберите закладку **Расширенные параметры iOS MDM**.
4. На закладке **Расширенные параметры iOS MDM** нажмите на значок перечеркнутого глаза рядом с параметром **Код отключения блокировки активации (только для контролируемых устройств)**.

   Отобразится код отключения блокировки активации.
5. Введите этот код в поле Пароль для Apple ID на экране блокировки активации контролируемого iOS-устройства. Поле Имя пользователя оставьте пустым.

   Блокировка активации на устройстве отключена.

Настройка точки доступа (APN)

Для подключения мобильного устройства к услугам передачи данных в мобильной сети следует настроить параметры APN (Access Point Name).

Настройка APN на Android-устройствах (только Samsung)

Настройка APN возможна только для Samsung-устройств.

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.

   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 → 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 изменены после очередной синхронизации устройства с Kaspersky Security Center.

Настройка APN на iOS MDM-устройствах

Для подключения пользователя iOS MDM-устройства к услугам передачи данных в мобильной сети следует настроить точку доступа (APN).

Раздел **APN** устарел. Рекомендуется настраивать параметры APN в разделе **Сотовая связь**. Перед настройкой параметров сотовой связи убедитесь, что параметры раздела **APN** не применены на устройстве (снят флажок **Применить параметры на устройстве**). Совместное использование параметров разделов **APN** и **Сотовая связь** невозможно.

Чтобы настроить точку доступа на iOS MDM-устройстве пользователя, выполните следующие действия:

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

Настройка рабочего профиля Android

Этот раздел содержит информацию о работе с рабочим профилем Android.

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.

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.

   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 **Рабочий профиль Android**.
5. В рабочей области **Рабочий профиль Android** установите флажок **Создать рабочий профиль**.
6. Укажите параметры рабочего профиля:

   - На закладке **Общие** настройте параметры передачи данных, контактов и другие.

- В разделе **Доступ к данным и передача данных** настройте параметры следующим образом:

  - **Запретить передачу данных из приложений личного профиля в приложения рабочего профиля**

    Ограничение передачи файлов, изображений и прочих данных из приложений личного профиля в приложения рабочего профиля.

    Если флажок установлен, приложения личного профиля не могут передавать данные в приложения рабочего профиля.

    Если флажок снят, приложения личного профиля могут передавать данные в приложения рабочего профиля.

    > Ограничение не распространяется на поиск контактов, доступ к календарю и копирование данных через буфер обмена между личным и рабочим профилями. Вы можете настроить эти функции, выбрав опции **Запретить доступ к контактам рабочего профиля приложениям из личного профиля**, **Синхронизация календарей личного и рабочего профилей** и **Запретить использование содержимого буфера обмена между личным и рабочим профилями** соответственно.

    По умолчанию флажок установлен.

  - **Запретить передачу данных из приложений рабочего профиля в приложения личного профиля**

    Ограничение передачи файлов, изображений и прочих данных из приложений рабочего профиля в приложения личного профиля.

    Если флажок установлен, приложения рабочего профиля не могут передавать данные в приложения личного профиля.

    Если флажок снят, приложения рабочего профиля могут передавать данные в приложения личного профиля.

    > Ограничение не распространяется на поиск контактов, доступ к календарю и копирование данных через буфер обмена между личным и рабочим профилями. Вы можете настроить эти функции, выбрав опции **Запретить доступ к контактам рабочего профиля приложениям из личного профиля**, **Синхронизация календарей личного и рабочего профилей** и **Запретить использование содержимого буфера обмена между личным и рабочим профилями** соответственно.

    По умолчанию флажок установлен.

  - **Запретить приложениям из рабочего профиля доступ к файлам в личном профиле**

    Ограничение доступа приложений рабочего профиля к файлам личного профиля.

    Если флажок установлен, у пользователя отсутствует доступ к файлам в личном профиле при использовании приложений рабочего профиля.

    Если флажок снят, пользователь имеет доступ к файлам в личном профиле при использовании приложений рабочего профиля. Доступ также должен поддерживаться используемыми приложениями.

    По умолчанию флажок установлен.

- **Запретить приложениям из личного профиля доступ к файлам в рабочем профиле**

  Ограничение доступа приложений личного профиля к файлам рабочего профиля.

  Если флажок установлен, у пользователя отсутствует доступ к файлам в рабочем профиле при использовании приложений личного профиля.

  Если флажок снят, пользователь имеет доступ к файлам в рабочем профиле при использовании приложений личного профиля. Доступ также должен поддерживаться используемыми приложениями.

  По умолчанию флажок установлен.

- **Запретить использование содержимого буфера обмена между личным и рабочим профилями**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства копировать данные через буфер обмена между личным и рабочим профилями.

  По умолчанию флажок установлен.

- **Запретить включать режим отладки по USB**

  Ограничение использования режима отладки по USB на мобильном устройстве пользователя в рабочем профиле. В режиме отладки по USB пользователь может, например, загрузить приложение через рабочую станцию.

  Если флажок установлен, пользователю недоступен режим отладки по USB. Пользователь не может настраивать мобильное устройство через USB при подключении устройства к рабочей станции.

  Если флажок снят, пользователь может перейти в режим отладки по USB, подключить мобильное устройство к рабочей станции с помощью USB и настроить устройство.

  По умолчанию флажок установлен.

- **Запретить пользователю добавление и удаление учетных записей в рабочем профиле**

  Если флажок установлен, пользователю запрещено добавлять и удалять учетные записи в рабочем профиле через Настройки или приложения Google. В частности, ограничена возможность первичного входа в приложения Google. Тем не менее, пользователь может входить в некоторые другие сторонние приложения в рабочем профиле, а также добавлять и удалять учетные записи с их помощью.

  Учетные записи, добавленные до установки ограничения, не будут удалены, доступ к ним не ограничен.

  По умолчанию флажок установлен.

- **Запретить трансляцию, запись и снимки экрана в приложениях рабочего профиля**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства делать снимки экрана, а также записывать и демонстрировать экран устройства в приложениях рабочего профиля. Помимо этого установка или снятие флажка определяет, разрешен ли захват экрана в целях работы искусственного интеллекта.

  По умолчанию флажок установлен.

- В разделе **Контакты** настройте параметры следующим образом:

- **Запретить отображение имени контакта из рабочего профиля для входящих вызовов, полученных в личном профиле**

  Установка или снятие флажка определяет, будет ли имя контакта из рабочего профиля отображаться в личном профиле для входящих вызовов.

  По умолчанию флажок установлен.

- **Запретить доступ к контактам рабочего профиля приложениям из личного профиля**

  Установка или снятие флажка определяет, разрешен ли приложениям для управления контактами (например, встроенному Диспетчеру контактов Google) в личном профиле доступ к контактам рабочего профиля.

  По умолчанию флажок установлен.

- На закладке **Приложения** настройте параметры следующим образом:

  - **Включить Контроль приложений только в рабочем профиле**

    Контроль запуска приложений в рабочем профиле на мобильном устройстве пользователя. Вы можете создавать списки разрешенных, запрещенных, рекомендованных и обязательных приложений, а также разрешенных и запрещенных категорий приложений, в разделе **Контроль приложений**.

    Если флажок установлен, в зависимости от параметров Контроля приложений Kaspersky Endpoint Security блокирует или разрешает запуск приложений только в рабочем профиле. При этом в личном профиле Контроль приложений не работает.

    По умолчанию флажок снят.

  - **Включить Веб-Фильтр только в рабочем профиле**

    Ограничение доступа пользователя устройства к веб-сайтам в рабочем профиле. Вы можете указать параметры доступа к веб-сайтам (создать список запрещенных категорий веб-сайтов или список разрешенных веб-сайтов) в разделе **Веб-Фильтр**. Если Веб-Фильтр выключен, Kaspersky Endpoint Security ограничивает доступ пользователей только к веб-сайтам категорий **Фишинг** и **Вредоносное программное обеспечение**. Эти категории выбраны по умолчанию в области **Запрещены веб-сайты выбранных категорий** в Веб-Фильтре.

    Если флажок установлен, Веб-Фильтр для Google Chrome запрещает или разрешает доступ к веб-сайтам только в рабочем профиле Android. При этом в личном профиле Веб-Фильтр не работает.

    Если флажок снят, в зависимости от параметров Веб-Фильтра Kaspersky Endpoint Security запрещает или разрешает доступ к веб-сайтам в личном и рабочем профилях мобильного устройства.

    Для Samsung Internet Browser, HUAWEI Browser и Яндекс Браузера 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.

    По умолчанию флажок снят.

Для Samsung Internet Browser, HUAWEI Browser и Яндекс Браузера 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**.

- **Запретить установку приложений в рабочий профиль из неизвестных источников**

  Ограничение на установку приложений в рабочий профиль из всех источников, кроме корпоративного Google Play.

  Если флажок установлен, пользователь может устанавливать приложения только из Google Play. Для установки приложений пользователь использует свою корпоративную учетную запись Google.

  Если флажок снят, пользователь может устанавливать приложения любым доступным способом. Недоступны для установки только запрещенные приложения, список которых вы можете создать в разделе **Контроль приложений**.

  По умолчанию флажок снят.

- **Запретить удаление приложений из рабочего профиля**

  Установка или снятие флажка определяет, запрещено ли пользователю удалять приложения из рабочего профиля.

  По умолчанию флажок снят.

- **Запретить показывать уведомления от приложений из рабочего профиля на заблокированном экране**

  Ограничивает отображение содержимого уведомлений от приложений рабочего профиля на экране блокировки устройства.

  Если флажок установлен, содержимое уведомлений из приложений рабочего профиля не отображается на экране блокировки устройства. Для просмотра уведомлений необходимо разблокировать устройство \ рабочий профиль.

  Если флажок снят, уведомления из приложений рабочего профиля отображаются на экране блокировки устройства.

  По умолчанию флажок снят.

- **Запретить приложениям из рабочего профиля использовать камеру**

  Установка или снятие флажка определяет, могут ли приложения из рабочего профиля получить доступ к камере устройства.

  По умолчанию флажок установлен.

  На устройствах под управлением операционной системы Android 10 или выше, если в разделе **Управление устройством** установлен флажок **Запретить использование камеры**, камера устройства может быть заблокирована в рабочем профиле, даже если снят флажок **Запретить приложениям из рабочего профиля использовать камеру**.

- **Выдача дополнительных разрешений для работы приложений в рабочем профиле**

Параметр **Выдача дополнительных разрешений для работы приложений в рабочем профиле** позволяет выбрать действие, которое будет выполняться, когда приложения из рабочего профиля запрашивают дополнительные разрешения. Это неприменимо к разрешениям, выданным в Настройках устройства (например, Доступ ко всем файлам).

- **Запрашивать разрешения у пользователя**

  Пользователь решает, выдавать ли разрешение приложению.

  Этот параметр выбран по умолчанию.

- **Выдавать разрешения автоматически**

  Разрешения для всех приложений в рабочем профиле выдаются без участия пользователя.

- **Отклонять разрешения автоматически**

  Запросы на разрешения для всех приложений в рабочем профиле отклоняются без участия пользователя.

  Пользователи могут настраивать разрешения приложений в параметрах устройства, прежде чем эти разрешения будут автоматически запрещены.

На Android 12 или выше следующие разрешения не могут быть выданы автоматически, но могут быть автоматически отклонены. При выборе **Выдавать разрешения автоматически** следующие разрешения будут запрашиваться у пользователя:

- разрешения на использование местоположения;
- разрешения на доступ к камере;
- разрешения на запись звука;
- разрешение на распознавание физической активности;
- разрешение на отслеживание входящих SMS и MMS сообщений;
- разрешения на доступ к данным биометрических датчиков.

- Добавление виджетов приложений из рабочего профиля на главный экран устройства

Параметр **Добавление виджетов приложений из рабочего профиля на главный экран устройства** позволяет выбрать, разрешено ли пользователю устройства добавлять виджеты приложений рабочего профиля на главный экран устройства.

- **Запретить всем приложениям**

  Пользователю устройства запрещено добавлять виджеты приложений, установленных в рабочем профиле.

  Этот параметр выбран по умолчанию.

- **Разрешить всем приложениям**

  Пользователю устройства разрешено добавлять виджеты всех приложений, установленных в рабочем профиле.

- **Разрешить только перечисленным приложениям**

  Пользователю устройства разрешено добавлять виджеты перечисленных приложений, установленных в рабочем профиле.

  Чтобы добавить приложение в список, нажмите **Добавить** и введите имя пакета приложения. **Как получить имя пакета приложения**

  Чтобы получить имя пакета приложения:

  1. Откройте Google Play.
  2. Найдите нужное приложение и откройте его страницу.

     URL приложения оканчивается именем пакета приложения (например, https://play.google.com/store/apps/details?id=**com.android.chrome**).

  Чтобы получить имя пакета приложения, которое было добавлено в Kaspersky Security Center:

  1. В дереве консоли Kaspersky Security Center выберите **Дополнительно** > **Удаленная установка** > **Инсталляционные пакеты**.
  2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Управление пакетами мобильных приложений**.

     В открывшемся окне **Управление пакетами мобильных приложений** в столбце **Название приложения** отображаются идентификаторы управляемых приложений.

     Если пакет приложения представлен файлом в формате APK, и необходимо узнать идентификатор приложения, можно добавить этот пакет приложения в окне **Управление пакетами мобильных приложений**, нажав на кнопку **Новый** и следуя инструкциям на экране.

  Чтобы удалить приложение из списка, выберите приложение и нажмите **Удалить**.

- На вкладке **Сертификаты** вы можете настроить следующие параметры:

  - **Дублировать установку VPN-сертификатов в личный профиль**

Установка или снятие флажка определяет, будет ли VPN-сертификат, добавленный в разделе **Управление мобильными устройствами** > **Сертификаты** Консоли администрирования Kaspersky Security Center и установленный в рабочий профиль, также установлен и в личный профиль.

По умолчанию VPN-сертификаты, полученные из Kaspersky Security Center, устанавливаются в рабочий профиль. Этот параметр будет применен при выпуске нового VPN-сертификата.

По умолчанию флажок снят.

- **Дублировать установку корневых сертификатов в личный профиль**

  Установка или снятие флажка определяет, будут ли корневые сертификаты, добавленные в разделе политики **Корневые сертификаты** и установленные в рабочий профиль, также установлены и в личный профиль.

  По умолчанию флажок снят.

- На закладке **Пароль** настройте пароль рабочего профиля следующим образом:

  - **Требовать установить пароль для рабочего профиля**

    Позволяет определить требования к паролю для рабочего профиля в соответствии с принятыми в компаниями требованиями безопасности.

    Если флажок установлен, требования к паролю доступны для настройки. Когда политика будет применена, пользователь получит уведомление о необходимости задать пароль для рабочего профиля в соответствии с требованиями, принятыми в компании.

    Если флажок снят, редактирование настроек пароля недоступно.

    По умолчанию флажок снят.

  - **Минимальное количество символов**

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

По умолчанию пароль пользователя содержит 4 символа.

Следующие правила применимы только к личным и рабочим профилям:

- В личном профиле Kaspersky Endpoint Security сводит требования к надежности пароля к одному из системных значений: средний или высокий уровень для устройств под управлением Android 10 или выше.

- В рабочем профиле Kaspersky Endpoint Security сводит требования к надежности пароля к одному из системных значений: средний или высокий уровень для устройств под управлением Android 12 или выше.

Значения уровня надежности 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 сложности пароля (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.

- **Требования не заданы**

  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 (например, !@#$%)**
  - **Минимальное количество заглавных букв**
  - **Минимальное количество строчных букв**
  - **Минимальное количество небуквенных символов (например, 1^&*9)**

- **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.

Этот параметр применим только для устройств под управлением Android 12 или ниже.

- Максимальное количество неудачных попыток ввода пароля до удаления рабочего профиля

Определяет максимальное количество попыток ввести пароль разблокировки устройства, доступных пользователю. Если применить политику, рабочий профиль будет удаляться с устройства после превышения максимального количество попыток.

Возможные значения: от 4 до 16.

Значение по умолчанию не задано. Это означает, что количество попыток неограниченно.

- **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 о необходимости смены пароля**

  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.

- **Количество последних паролей, которые нельзя использовать в качестве нового пароля**

  Определяет максимальное количество ранее использованных пользователем паролей, которые не могут быть установлены в качестве нового пароля. Этот параметр применяется, только когда пользователь устанавливает новый пароль на устройстве.

  По умолчанию указано значение 0. Это означает, что новый пароль пользователя может совпадать с любым ранее использованным паролем, кроме текущего.

- **Период неактивности без блокировки рабочего профиля, 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 после разблокировки биометрическими методами до ввода пароля, в минутах (Android 8.0 или выше)**

  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 Android 8.0 или выше.

- **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 или выше. Начиная с Android 10, эта настройка применима только для режима device owner.

- **Разрешить использование отпечатков пальцев**

  Использование отпечатков пальцев для разблокировки экрана.

  > Флажок не ограничивает использование сканера отпечатков пальцев при входе в приложения или подтверждении покупок.

  Если флажок установлен, использование отпечатков пальцев на мобильном устройстве разрешено.

  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 или выше; Android 10 или выше в режиме device owner)**.

  По умолчанию флажок установлен.

  > Эта настройка применима к устройствам с любыми поддерживаемыми версиями Android. Начиная с Android 10, эта настройка применима только для режима device owner.

  > На некоторых устройствах Xiaomi рабочий профиль Android можно разблокировать с помощью отпечатка пальца только в том случае, если значение параметра **Период неактивности без блокировки экрана устройства** будет установлено после установки отпечатка пальца в качестве метода разблокировки экрана.

- **Разрешить распознавание лица (Android 9 или выше)**

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 или выше; Android 10 или выше в режиме device owner)**.

По умолчанию флажок установлен.

Этот параметр применим только для устройств под управлением Android 9 или выше. Начиная с Android 10, эта настройка применима только для режима device owner.

- **Разрешить распознавание по радужной оболочке глаза (Android 9 или выше)**

  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 или выше; Android 10 или выше в режиме device owner)**.

  По умолчанию флажок установлен.

  Этот параметр применим только для устройств под управлением Android 9 или выше. Начиная с Android 10, эта настройка применима только для режима device owner.

- На закладке **Код разблокировки** укажите одноразовый код. Это код, который пользователю нужно будет ввести для разблокировки рабочего профиля, если он был заблокирован.

  - **Длина кода разблокировки**

    Количество цифр в коде разблокировки. Возможные значения: 4, 8, 12 или 16 символов.

    Длина кода разблокировки по умолчанию – 4 цифры.

  - **Код разблокировки**

    Это поле отображается при просмотре параметров политики для конкретного устройства пользователя, а не для группы устройств.

    В этом поле отображается код разблокировки для рабочего профиля. После того как пользователь разблокирует рабочий профиль с помощью этого кода разблокировки, формируется новый код разблокировки.

    Это поле недоступно для изменения.

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 изменены после очередной синхронизации устройства с Kaspersky Security Center. Пространство мобильного устройства пользователя будет разделено на рабочий и личный профили.

Разблокирование рабочего профиля

Если устройство не соответствует требованиям безопасности, указанным в Контроле соответствия, рабочий профиль может быть заблокирован.

Для разблокирования рабочего профиля пользователь мобильного устройства должен ввести одноразовый код на заблокированном экране. Этот код создается в Консоли администрирования на базе MMC. Он уникален для каждого мобильного устройства. После разблокирования рабочего профиля устройства пароль рабочего профиля будет изменен на пароль по умолчанию (1234).

Администратор может просматривать одноразовый код в параметрах политики, применяемых на мобильном устройстве. Длину кода можно изменить (4, 8, 12 или 16 цифр).

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 разблокировки которого вы хотите получить одноразовый код.
3. Откройте окно свойств мобильного устройства.
4. Выберите **Приложения → Kaspersky Endpoint Security для мобильных устройств**.
5. Откройте окно свойств приложения Kaspersky Endpoint Security.
6. Выберите раздел **Рабочий профиль Android**.

   Одноразовый код для разблокировки выбранного устройства отображается на закладке **Код разблокировки** в поле **Код разблокировки**.

Сообщите пользователю заблокированного мобильного устройства одноразовый код любым доступным способом (например, в сообщении электронной почты).

Пользователь должен ввести одноразовый код разблокировки на своем устройстве.

После блокирования рабочего профиля история паролей рабочего профиля очищается. Это означает, что пользователь может повторно использовать один из недавних паролей, независимо от параметров пароля для рабочего профиля.

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 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 **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 (обязательно для заполнения)** введите имя домена сервера LDAP. Вы можете использовать макросы из раскрывающегося списка **Добавить макрос**.

10. Чтобы использовать транспортный протокол передачи данных SSL для защиты передачи сообщений, установите флажок **Использовать SSL-соединение**.

11. Сформируйте список поисковых запросов для доступа пользователя iOS MDM-устройства к папкам с корпоративными данными на сервере LDAP:

    a. В блоке **Параметры поиска** нажмите на кнопку **Добавить**.

       В таблице поисковых запросов отобразится пустая строка.

    b. В графе **Название** введите название поискового запроса.

    c. В графе **Глубина поиска** выберите уровень вложенности папки для поиска корпоративных данных на сервере LDAP:

       - **Корень дерева** – поиск в базовой папке сервера LDAP.
       - **Один уровень** – поиск в папках на первом уровне вложенности от базовой папки.
       - **Поддерево** – поиск в папках на всех уровнях вложенности от базовой папки.

    d. В графе **База поиска** укажите путь к папке на сервере LDAP, с которой начинается поиск (например, "ou=people", "o=example corp").

    e. Повторите пункты a-d для всех поисковых запросов, которые вы хотите добавить на iOS MDM-устройство.

12. Нажмите кнопку **ОК**.

    Новая учетная запись LDAP отобразится в списке.

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

В результате на мобильном устройстве пользователя после применения политики будут добавлены учетные записи LDAP из сформированного списка. Пользователь может получить доступ к корпоративным контактам в стандартных приложениях iOS Контакты, Сообщения и Mail.

Добавление учетной записи календаря

Чтобы пользователь iOS MDM-устройства мог работать со своими событиями календаря на сервере CalDAV, следует добавить учетную запись на CalDAV. Синхронизация с сервером CalDAV позволит пользователю создавать и принимать приглашения, получать обновления событий и синхронизировать задачи с приложением Напоминания.

Чтобы добавить учетную запись CalDAV пользователя iOS MDM-устройства, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши 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 **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 (обязательно для заполнения)** введите имя хоста или IP-адрес сервера CalDAV и номер порта сервера CalDAV.
8. В поле **Основной веб-адрес** задайте веб-адрес учетной записи CalDAV пользователя iOS MDM-устройства на сервере CalDAV (например, http://example.com/caldav/users/mycompany/user).

   Веб-адрес должен начинаться с `"http://"` или `"https://"`.
9. В поле **Имя учетной записи** задайте имя учетной записи пользователя для авторизации на сервере CalDAV.
10. В поле **Пароль** задайте пароль учетной записи CalDAV для авторизации на сервере CalDAV.
11. Чтобы использовать транспортный протокол передачи данных SSL для защиты передачи данных о событиях между сервером CalDAV и мобильным устройством, установите флажок **Использовать SSL-соединение**.
12. Нажмите кнопку **ОК**.

    Новая учетная запись CalDAV отобразится в списке.
13. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на мобильном устройстве пользователя после применения политики будут добавлены учетные записи CalDAV из сформированного списка.

Добавление учетной записи контактов

Чтобы пользователь iOS MDM-устройства мог синхронизировать свои контакты с сервером CardDAV, следует добавить учетную запись CardDAV. Синхронизация с сервером CardDAV позволит пользователю получить доступ к данным контактов с любого устройства.

Чтобы добавить учетную запись CardDAV пользователя iOS MDM-устройства, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши 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 **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 (обязательно для заполнения)** введите имя хоста или IP-адрес сервера CardDAV и номер порта сервера CardDAV.
8. В поле **Основной веб-адрес** задайте веб-адрес учетной записи CardDAV пользователя iOS MDM-устройства на сервере CardDAV (например, http://example.com/carddav/users/mycompany/user).

   Веб-адрес должен начинаться с `"http://"` или `"https://"`.
9. В поле **Имя учетной записи** задайте имя учетной записи пользователя для авторизации на сервере CardDAV. Вы можете использовать макросы из раскрывающегося списка **Добавить макрос**.
10. В поле **Пароль** задайте пароль учетной записи CardDAV для авторизации на сервере CardDAV.
11. Чтобы использовать транспортный протокол передачи данных SSL для защиты передачи контактов между сервером CardDAV и мобильным устройством, установите флажок **Использовать SSL-соединение**.
12. Нажмите кнопку **ОК**.

    Новая учетная запись CardDAV отобразится в списке.
13. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на мобильном устройстве пользователя после применения политики будут добавлены учетные записи CardDAV из сформированного списка.

Настройка подписки на календарь

Чтобы пользователь iOS MDM-устройства мог добавить в свой календарь события сторонних календарей (например, корпоративного календаря), нужно добавить на календарь подписку. *Сторонние календари* – календари других пользователей, у которых есть учетная запись CalDAV, календари iCal, а также другие открыто опубликованные календари.

Чтобы добавить подписку на календарь, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши 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 **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 (обязательно для заполнения)** 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**.

    Новая подписка на календарь отобразится в списке.

12. 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.

Управление веб-клипами

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, удалять веб-клипы с устройств и указывать значки веб-клипов, которые отображаются на экране.

Управление веб-клипами на Android-устройствах

Для управления веб-клипами на Android-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.

   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 устройством**.
5. В разделе **Добавление веб-клипов на главный экран устройства** выполните одно из следующих действий:

   - Чтобы добавить веб-клип:

     a. Нажмите на кнопку **Добавить**.

     Откроется окно **Добавить веб-клип**.

     b. В поле **Название** введите название веб-клипа, которое будет отображаться на главном экране Android-устройства.

     c. В поле **Веб-адрес** введите адрес веб-сайта, который будет открываться при нажатии на значок веб-клипа. Адрес должен начинаться с "http://" или "https://".

     d. 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.

     e. Нажмите на кнопку **ОК**.

     Новый веб-клип отобразится в списке.

     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.

   - Чтобы изменить веб-клип:

     a. Выберите веб-клип, параметры которого вы хотите отредактировать, и нажмите на кнопку **Изменить**.

Откроется окно **Добавить веб-клип**.

b. Укажите новые параметры веб-клипа, как описано выше в этом разделе.

c. Нажмите на кнопку **OK**.

- Чтобы удалить веб-клип:

a. Выберите веб-клип, который вы хотите удалить, и нажмите на кнопку **Удалить**.

Веб-клип исчезнет из списка.

6. 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.

Удаленные веб-клипы будут отключены на главном экране Android-устройства. Если пользователь нажмет на соответствующий значок, появится уведомление о том, что веб-клип больше не доступен. Пользователь должен самостоятельно удалить такой веб-клип с главного экрана (процедура зависит от производителя устройства).

Управление веб-клипами 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.

Для управления веб-клипами 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 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 **Веб-клипы**.
5. В разделе **Веб-клипы** выполните одно из следующих действий:

- Чтобы добавить веб-клип:

a. Нажмите на кнопку **Добавить**.

Откроется окно **Веб-клипы**.

b. В поле **Название** введите название веб-клипа, которое будет отображаться на главном экране iOS MDM-устройства.

c. В поле **Веб-адрес** введите адрес веб-сайта, который будет открываться при нажатии на значок веб-клипа. Адрес должен начинаться с `"http://"` или `"https://"`.

d. Чтобы разрешить пользователю удалить веб-клип с iOS MDM-устройства, установите флажок **Разрешить удаление**.

e. Нажмите на кнопку **Выбрать** и укажите файл с изображением для значка веб-клипа, который будет отображаться 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**.

f. Если вы хотите, чтобы при нажатии на значок веб-сайт открывался на весь экран iOS MDM-устройства, установите флажок **Полноэкранный веб-клип**.

> В полноэкранном режиме панель инструментов Safari скрыта и на экране устройства отображается только веб-страница.

g. Нажмите на кнопку **ОК**.

Новый веб-клип отобразится в списке.

- Чтобы редактировать веб-клип:

a. Выберите веб-клип, параметры которого вы хотите отредактировать, и нажмите на кнопку **Изменить**.

Откроется окно **Веб-клипы**.

b. Укажите новые параметры веб-клипа, как описано выше в этом разделе.

c. Нажмите на кнопку **ОК**.

- Чтобы удалить веб-клип:

a. Выберите веб-клип, который вы хотите удалить, и нажмите на кнопку **Удалить**.

Веб-клип исчезнет из списка.

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

Когда политика будет применена, на главный экран мобильного устройства пользователя будут добавлены значки веб-клипов из сформированного списка.

Значки удаленных веб-клипов исчезнут с главного экрана iOS MDM-устройства.

Установка обоев

Вы можете установить одно и то же изображение в качестве обоев для домашнего экрана и экрана блокировки на устройствах пользователей, попадающих под действие одной политики.

Чтобы установить обои на Android-устройства пользователей:

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 устройством**.
5. В разделе **Установка обоев рабочего стола и экрана блокировки** нажмите **Установить**.

   Откроется окно **Установка обоев**.

6. В раскрывающемся списке **Способ установки обоев** выберите способ установки обоев:

   - **Скачать изображение из интернета**

     Для этого способа необходимо указать URL, начинающийся с `http://` или `https://`. Используйте только доверенные веб-адреса.

   - **Загрузить изображение**

     Для этого способа необходимо загрузить изображение в формате PNG или JPEG размером не более 1 МБ.

7. После импорта изображения вы можете просмотреть его в окне **Установка обоев**.

   Предпросмотр

При способе **Загрузить изображение** предпросмотр изображения всегда доступен. Изображение для предпросмотра сохраняется в политике и доступно при дальнейшем редактировании установленных обоев.

При выборе варианта **Скачать изображение из интернета** кнопка **Предпросмотр** появится, если изображение скачано по ссылке, которая начинается с `http://`. Нажмите на эту кнопку, чтобы отобразить изображение для предпросмотра. Изображение для предпросмотра не сохраняется в политике. Поэтому при редактировании установленных обоев необходимо снова загружать изображение для предпросмотра.

Функция **Предпросмотр** не работает для изображений, скачанных по ссылкам, которые начинаются с `https://`.

8. Если вы хотите использовать то же изображение в качестве обоев для экрана блокировки, установите флажок **Применить для экрана блокировки**. В противном случае изображение используется только в качестве обоев рабочего стола.

   По умолчанию флажок снят.

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

Импортированное изображение устанавливается в качестве обоев на устройствах пользователей.

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 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 **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.

Работа с командами для мобильных устройств

Этот раздел содержит информацию о командах для управления мобильными устройствами, которые поддерживает Kaspersky Security Center. В разделе приведены инструкции по отправке команд на мобильные устройства, а также по просмотру статуса выполнения команд в журнале команд.

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.

Команды для Android-устройств

Команда	Результат выполнения команды
Заблокировать	Мобильное устройство заблокировано. Для получения доступа к данным необходимо разблокировать устройство.
Разблокировать	Мобильное устройство разблокировано. После разблокировки устройства под управлением операционной системы Android 5.0–6 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 с устройства. Перечень удаленных данных зависит от режима работы

корпоративные данные	устройства. • На личном устройстве удалены KNOX-контейнер и почтовый сертификат. • Если устройство работает в режиме device owner, удалены KNOX-контейнер и сертификаты, установленные приложением Kaspersky Endpoint Security для Android (почтовые и VPN-сертификаты, сертификаты, полученные через профили SCEP, кроме мобильных сертификатов). • Дополнительно, если установлен рабочий профиль Android, удален рабочий профиль (содержимое, настройки и ограничения) и сертификаты, установленные в рабочем профиле (почтовые и VPN-сертификаты, сертификаты, полученные через профили SCEP, кроме мобильных сертификатов).
Синхронизировать устройство	Данные с мобильного устройства синхронизированы с Сервером администрирования.
Определить местоположение устройства	Получены координаты местоположения мобильного устройства. Чтобы посмотреть местоположение устройства на карте, перейдите в папку **Управление мобильными устройствами → Мобильные устройства**. Затем в контекстном меню устройства выберите **Все команды → Определить местоположение → Посмотреть координаты 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. Если на устройстве Android отключена служба Google "Точность местоположения", команда **Определить местоположение устройства** работать не будет. Обращаем внимание, что не на всех устройствах Android есть эта служба.
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 данные приложения	Данные указанного приложения удалены с мобильного устройства. Действие применимо только к устройствам с Android 9 или выше в режиме device owner или с установленным рабочим профилем Android. Для выполнения действия необходимо указать имя пакета приложения, данные которого должны быть удалены. Как получить имя пакета приложения В результате выполнения команды приложение возвращается в состояние по умолчанию. Данные системных приложений и приложений-администраторов не удаляются.

	Чтобы получить имя пакета приложения: 1. Откройте Google Play. 2. Найдите нужное приложение и откройте его страницу. URL приложения оканчивается именем пакета приложения (например, https://play.google.com/store/apps/details?id=**com.android.chrome**). *Чтобы получить имя пакета приложения, которое было добавлено в Kaspersky Security Center:* 1. В дереве консоли Kaspersky Security Center выберите **Дополнительно** > **Удаленная установка** > **Инсталляционные пакеты**. 2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Управление пакетами мобильных приложений**. В открывшемся окне **Управление пакетами мобильных приложений** в столбце **Название приложения** отображаются идентификаторы управляемых приложений. Если пакет приложения представлен файлом в формате APK, и необходимо узнать идентификатор приложения, можно добавить этот пакет приложения в окне **Управление пакетами мобильных приложений**, нажав на кнопку **Новый** и следуя инструкциям на экране.
Удалить данные всех приложений	Данные всех приложений удалены с мобильного устройства. Действие применимо только к устройствам с Android 9 или выше в режиме device owner или с установленным рабочим профилем Android. Если устройство работает в режиме device owner, данные всех приложений на устройстве удалены. Если на устройстве создан рабочий профиль Android, данные всех приложений в рабочем профиле удалены. В результате выполнения команды приложения возвращаются в состояние по умолчанию. Данные системных приложений и приложений-администраторов не удаляются.
Отправить сообщение	Сообщение с указанными параметрами (темой и текстом) отправлено на мобильное устройство пользователя. Вы можете отправить либо push-уведомление вместе со всплывающим окном, либо только push-уведомление. Эта команда доступна только при выданном разрешении **Отправление команд на мобильные устройства**. Дополнительная информация приведена в справке Kaspersky Security Center.
Получить историю местоположений устройства	Отображается история местоположений мобильного устройства за последние 14 дней. Чтобы посмотреть местоположение устройства на карте, перейдите в папку **Управление мобильными устройствами → Мобильные устройства**. Затем в контекстном меню устройства выберите **Все команды → Получить историю местоположений устройства → Посмотреть на карте**.

Эта команда работает только в том случае, если в базе Сервера администрирования хранится тип информационного события **История местоположений устройства**. События настраиваются в разделе **События** свойств политики. Дополнительная информация о событиях приведена в справке Kaspersky Security Center.

Из-за технических ограничений на устройствах Android фактическое получение местоположения устройства может происходить реже, чем указано в разделе **Синхронизация** свойств политики.

Команды для iOS MDM-устройств

Команда	Результат выполнения команды
Заблокировать	Мобильное устройство заблокировано. Для получения доступа к данным необходимо разблокировать устройство.
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.
Запланировать обновление ОС (только для контролируемых устройств)	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 (только для контролируемых устройств)	Включение или выключение Bluetooth на мобильном устройстве. Эта команда поддерживается только на устройствах в режиме supervised, работающих под управлением iOS 11.3 и выше.
Включить режим пропажи (только для контролируемых устройств)	На контролируемом мобильном устройстве включен режим пропажи, устройство заблокировано. На экране устройства появилось сообщение и номер телефона, которые вы можете редактировать.

	Если вы отправите команду **Включить режим пропажи** на контролируемое устройство iOS MDM без SIM-карты и это устройство будет перезапущено, оно не сможет подключиться к сети Wi-Fi и получить команду **Отключить режим пропажи**. Эта проблема связана с особенностями iOS-устройств. Чтобы этого избежать, можно отправлять эту команду только на устройства с SIM-картой или вставить SIM-карту в заблокированное устройство – в этом случае оно сможет получить команду **Отключить режим пропажи** по мобильной сети.
Определить местоположение (только для контролируемых устройств)	Получены данные о местоположении устройства. Перейдите по ссылке в журнале команд, чтобы получить координаты устройства и посмотреть его местоположение на карте. Чтобы посмотреть местоположение устройства на карте, перейдите в папку **Управление мобильными устройствами** → **Мобильные устройства**. Затем в контекстном меню устройства выберите **Все команды** → **Определить местоположение** → **Посмотреть координаты устройства**. Эта команда доступна только для контролируемых устройств в режиме пропажи.
Воспроизвести звук (только для контролируемых устройств)	На потерянном мобильном устройстве воспроизводится звуковой сигнал. Эта команда доступна только для контролируемых устройств в режиме пропажи.
Отключить режим пропажи (только для контролируемых устройств)	На мобильном устройстве отключен режим пропажи, устройство разблокировано. Эта команда поддерживается только на устройствах в режиме supervised.

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 и выше необходимо предоставить разрешение "Всегда" для доступа к местоположению устройства. На устройствах с операционной системой Android 11 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.

Отправка команд

Чтобы отправить команду на мобильное устройство пользователя:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите подпапку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. Выберите мобильное устройство пользователя, на которое нужно отправить команду.

3. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

4. В окне **Команды для управления мобильным устройством** перейдите в раздел с названием команды, которую нужно отправить на мобильное устройство, и нажмите на кнопку **Отправить команду**.

В зависимости от выбранной команды после нажатия на кнопку **Отправить команду** может открыться окно настройки дополнительных параметров команды. Например, при отправке команды на удаление с мобильного устройства provisioning-профиля программа предлагает выбрать provisioning-профиль, который нужно удалить с мобильного устройства. Укажите в окне дополнительные параметры команды и подтвердите свой выбор. После этого команда будет отправлена на мобильное устройство.

По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

5. Нажмите на кнопку **ОК**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Просмотр статусов команд в журнале команд

Программа сохраняет информацию о всех командах, отправленных на мобильные устройства, в журнале команд. В журнале команд сохраняется информация о времени и дате отправления команд на мобильное устройство, статусы команд, а также подробные описания результатов выполнения команд. Например, в случае неудачного выполнения команды в журнале отображается причина ошибки. Записи в журнале команд хранятся не более 30 дней.

Команды, отправленные на мобильные устройства, могут иметь следующие статусы:

- *Выполняется* – команда отправлена на мобильное устройство.
- *Завершена* – выполнение команды успешно завершено.
- *Завершена с ошибкой* – выполнить команду не удалось.
- *Удаляется* – команда удаляется из очереди команд, отправленных на мобильное устройство.
- *Удалена* – команда успешно удалена из очереди команд, отправленных на мобильное устройство.
- *Удаление завершено с ошибкой* – команду не удалось удалить из очереди команд, отправленных на мобильное устройство.

Программа ведет журнал команд для каждого мобильного устройства.

Чтобы просмотреть журнал команд, отправленных на мобильное устройство:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите подпапку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. Выберите в списке мобильное устройство, для которого вы хотите просмотреть журнал команд.

3. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

   Откроется окно **Команды для управления мобильным устройством**. Разделы окна **Команды для управления мобильным устройством** соответствуют командам, которые можно отправить на мобильное устройство.

4. Выбирайте разделы с нужными вам командами и просматривайте информацию об отправке и выполнении команд в блоке **Журнал команд**.

В блоке **Журнал команд** можно просмотреть список команд, отправленных на мобильное устройство, и информацию о командах. С помощью фильтра **Показать команды** можно показывать в списке только команды с выбранным статусом.

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.

Если вы хотите использовать стороннюю EMM-систему только для развертывания приложения Kaspersky Endpoint Security для Android, после развертывания вы можете управлять мобильными устройствами в Консоли администрирования.

Для управления устройствами невозможно одновременно использовать Консоль администрирования и сторонние EMM-системы.

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 Защиты от вредоносного ПО;
  - настраивать расписание запуска проверки устройства на наличие вредоносного ПО;
  - включать обнаружение рекламных приложений и приложений, которые могут быть использованы злоумышленниками для нанесения вреда устройству или данным пользователя;
  - настраивать расписание обновления баз приложения.

Начало работы

Приложение Kaspersky Endpoint Security для Android в настоящее время недоступно в Google Play.

Для развертывания приложения на мобильных устройствах пользователей необходимо добавить Kaspersky Endpoint Security для Android в магазин приложений EMM. Вы можете добавить Kaspersky Endpoint Security для Android в магазин приложений EMM с помощью ссылки Google Play. Подробнее о работе с приложениями в EMM-Консоли см. на *сайте Службы технической поддержки поставщика услуг EMM*.

Приложение Kaspersky Endpoint Security для Android разворачивается в рабочем профиле Android. Приложение изолировано от персональных данных пользователя и защищает только корпоративные данные в рабочем профиле. Рекомендуется обеспечить защиту Kaspersky Endpoint Security для Android от удаления средствами EMM-Консоли.

Как установить приложение

Если вы хотите управлять устройствами в сторонней EMM-консоли, вы можете развернуть приложение с помощью APK-файла с сайта "Лаборатории Касперского".

Для работы приложения требуются следующие разрешения:

- Разрешение "Память" для доступа к файлам при работе Защиты от вредоносного ПО (только для Android 6 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.

Защита 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.

Для работы Веб-Фильтра должны быть выполнены следующие условия:

- 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.

- Пользователи устройств приняли Политику конфиденциальности и Положение о Веб-Фильтре в мастере первоначальной настройки или параметрах приложения.

  Администратор может принять Положение о Веб-Фильтре в Консоли администрирования Kaspersky Security Center.

- В параметрах приложения включен Веб-Фильтр:

  `EnableWebFilter = True`, `EnableWebFilterLock = True`.

- В параметрах приложения включено использование KSN: `UseKsnMode = Recommended` или `UseKsnMode = Extended`.

Чтобы настроить прокси-сервер Google Chrome с помощью консоли VMware Workspace ONE, выполните следующие действия:

1. В консоли выберите **Книги и приложения** → **Приложения** → **Собственные**.

   Откроется каталог приложений.

2. Выберите раздел **Общедоступные**.

3. Выберите приложение Google Chrome.

   Откроется окно свойств приложения.

4. Выберите раздел **Назначение**.

5. В открывшемся окне нажмите на кнопку **Назначить**.

   Откроется список устройств, которым назначено приложение.

6. Нажмите на кнопку **Изменить**.

7. В открывшемся окне нажмите **Настроить**.

   Откроется конфигурация приложения. Информация о каждом параметре приложения содержится во всплывающих подсказках.

8. Укажите обязательные параметры:

   - **Режим прокси-сервера** – использовать фиксированный прокси-сервер.
   - **URL прокси-сервера** – 127.0.0.1:3128.
   - **Поддержка протокола SPDY** – выключено.
   - **Сжатие данных через прокси-сервер** – выключено.

9. Сохраните изменения.

Чтобы включить Веб-Фильтр в Google Chrome с помощью консоли VMware Workspace ONE, выполните следующие действия:

1. В консоли выберите **Книги и приложения** → **Приложения** → **Собственные**.

   Откроется каталог приложений.

2. Выберите раздел **Общедоступные**.

3. Выберите приложение Kaspersky Endpoint Security.

   Откроется окно свойств приложения.

4. Выберите раздел **Назначение**.

5. В открывшемся окне нажмите на кнопку **Назначить**.

   Откроется список устройств, которым назначено приложение.

6. Нажмите на кнопку **Изменить**.

7. В открывшемся окне нажмите **Настроить**.

   Откроется конфигурация приложения. Информация о каждом параметре приложения содержится во всплывающих подсказках.

8. Укажите обязательные параметры:

   - **Веб-Фильтр** – включить.
   - **Запретить настраивать Веб-Фильтр** – включить. Параметры Веб-Фильтра недоступны для пользователя в настройках приложения.
   - **Режим Kaspersky Security Network** – Рекомендуемый или Расширенный.

     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.

9. Сохраните изменения.

Если устройства пользователей подключены к Kaspersky Security Center, включите Веб-Фильтр в групповой политике. Также вы можете принять Положение о Веб-Фильтре в Консоли администрирования Kaspersky Security Center.

После включения Веб-Фильтра в приложении Kaspersky Endpoint Security для Android и настройки Google Chrome проверьте защиту от веб-угроз. Для проверки защиты вы можете использовать тестовый файл EICAR.

Как активировать приложение

Информация о лицензии передается на мобильное устройство вместе с остальными параметрами в файле конфигурации.

Если активация приложения не произошла в течение 30 дней с момента установки на мобильное устройство, то срок действия пробной лицензии истекает. По истечении срока действия пробной лицензии мобильное приложение Kaspersky Endpoint Security для Android прекращает выполнять все свои функции.

По истечении срока действия коммерческой лицензии мобильное приложение продолжает работу, но с ограниченной функциональностью (например, недоступно обновление баз Kaspersky Endpoint Security для Android). Чтобы продолжить использование приложения в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии.

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

1. В EMM-Консоли откройте настройки приложения Kaspersky Endpoint Security для Android.
2. В поле параметра `LicenseActivationCode` введите код активации приложения.

   Для активации приложения на устройстве требуется доступ к серверам активации "Лаборатории Касперского".

Как подключить устройство к Kaspersky Security Center

После установки приложения Kaspersky Endpoint Security для Android на мобильное устройство вы можете подключить устройство к Kaspersky Security Center. Данные для подключения устройства к Kaspersky Security Center передаются на мобильное устройство вместе с остальными параметрами, перечисленными в файле конфигурации. После подключения устройства к Kaspersky Security Center вы можете централизовано настраивать параметры приложения с помощью групповых политик. Также вы можете получать отчеты и статистику о работе приложения Kaspersky Endpoint Security для Android.

Перед подключением устройств к Kaspersky Security Center убедитесь, что выполнены следующие условия:

- На рабочем месте администратора установлен плагин управления Kaspersky Endpoint Security для Android.
- В свойствах Сервера администрирования открыт порт для подключения мобильных устройств.
- В Консоли администрирования включено отображение папки **Управление мобильными устройствами**.
- В хранилище сертификатов Kaspersky Security Center создан 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, следующим образом:

- На персональных устройствах с Android версии 9 и ниже приложение использует IMEI. Для более поздних версий Android приложение использует SSAID (идентификатор Android) или контрольную сумму других данных, полученных от устройства.
- В режиме device owner приложение использует IMEI для всех версий Android.
- При создании рабочего профиля на устройствах с Android версии 11 и ниже приложение использует IMEI. Для других версий Android приложение использует SSAID (идентификатор Android) или контрольную сумму других данных, полученных от устройства.

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.

Тихий режим работы приложения

Пользователь Android-устройства может выключить все уведомления от Kaspersky Endpoint Security для Android в настройках панели уведомлений. Если уведомления выключены, пользователь не отслеживает работу приложения и может пропустить важную информацию (например, об угрозах в режиме реального времени). Чтобы пользователь узнал статус работы приложения, ему необходимо открыть 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).

Параметры тихого режима передаются на мобильное устройство вместе с другими параметрами в файле конфигурации. Установите значение `True` для параметра `DisableNotification`.

Чтобы включить тихий режим работы приложения через консоль VMware Workspace ONE:

1. В консоли выберите **Книги и приложения** → **Приложение** → **Собственные**.

   Откроется каталог приложений.

2. Выберите раздел **Общедоступные**.

3. Выберите приложение Kaspersky Endpoint Security.

   Откроется окно свойств приложения.

4. Выберите раздел **Назначение**.

5. В открывшемся окне нажмите на кнопку **Назначить**.

   Откроется список устройств, которым назначено приложение.

6. Нажмите на кнопку **Изменить**.

7. В открывшемся окне нажмите **Настроить**.

   Откроется конфигурация приложения. Информация о каждом параметре приложения содержится во всплывающих подсказках.

8. В параметре **Выключить уведомления приложения до подключения к Kaspersky Security Center**.

   Если вы используете Kaspersky Security Center, включите также тихий режим в групповой политике.

9. Сохраните изменения.

В результате приложение будет отображать только уведомление о статусе защиты. Другие уведомления и всплывающие окна будут отключены.

Файл AppConfig

Конфигурационный файл создается для настройки приложения в EMM-консоли. Параметры приложения в конфигурационном файле приведены в следующей таблице.

Параметры конфигурационного файла

Ключ конфигурации	Описание	Тип	Значение	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. *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.	
`EulaAcceptanceCodesV2`	Коды Лицензионных соглашений	String		

			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. Если вы укажете значения в обоих полях, будут приняты условия всех указанных в них лицензионных соглашений.	
`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.	`<адрес сервера>:13292`
`DisableNotification`	Выключить уведомления приложения до подключения к Kaspersky Security Center	Boolean	`True` – Kaspersky Endpoint Security для Android скрывает все 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`
`ScanScheduleType`	Режим запуска проверки	Choice	`AfterUpdate` – запуск проверки на наличие вредоносного ПО после обновления баз. Приложение обновляет базы вредоносного ПО по сформированному расписанию (`UpdateScheduleType`). `Daily` – запуск проверки на наличие вредоносного ПО раз в день. Настройте время запуска проверки (`ScanScheduleTime`). `Weekly` – запуск проверки на наличие вредоносного ПО раз в неделю. Выберите день недели для запуска проверки на наличие вредоносного ПО (`ScanScheduleDay`) и настройте время (`ScanScheduleTime`). `Off` – автоматический запуск проверки на наличие вредоносного ПО выключен. При любом значении параметра пользователь устройства может вручную запустить проверку на наличие вредоносного ПО.	`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 поиска вредоносного ПО недоступны для пользователя в настройках приложения. False – пользователь может настроить режим запуска поиска вредоносного ПО и, например, выключить автоматический запуск поиска вредоносного ПО.	True
ScanOnlyExecutableFiles	Типы файлов для проверки (Поиск вредоносного ПО)	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
ScanActionOnThreatFound	Действие при обнаружении угрозы (Поиск вредоносного ПО)	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.	Quarantine
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,	Boolean	True – приложение обнаруживает рекламные приложения и приложения,	True

	средства автодозвона и приложения, которые могут использоваться злоумышленниками для нанесения вреда устройству и данным пользователя		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.	
`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`
`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 Защиты от вредоносного ПО 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.	`Quarantine`

			`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.	
`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`
`UpdateScheduleType`	Режим запуска обновления баз	Choice	`Daily` – проверка наличия новых баз вредоносного ПО и загрузка их на устройства раз в день. Настройте время запуска обновления баз (`UpdateScheduleTime`). `Weekly` – проверка наличия баз вредоносного ПО и загрузка их на устройства раз в неделю. Выберите день недели запуска обновления баз (`UpdateScheduleDay`) и настройте время (`UpdateScheduleTime`). `Off` – автоматическое обновление баз вредоносного ПО выключено. При любом значении параметра пользователь устройства может вручную запустить обновление баз вредоносного ПО.	`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 баз вредоносного ПО.	`True`
`AllowUpdateInRoaming`	Обновлять базы в роуминге	Boolean	`True` – приложение загружает базы вредоносного ПО, если устройство находится в зоне роуминга. Приложение загружает базы вредоносного ПО по сформированному расписанию (`UpdateScheduleType`). `False` – приложение загружает базы вредоносного ПО, только если устройство находится в домашней сети.	`False`
`EnableWebFilter`	Веб-Фильтр	Boolean	`True` – приложение блокирует вредоносные и фишинговые веб-сайты в интернете с помощью компонента Веб-Фильтр. Веб-Фильтр на Android-устройствах поддерживается только	`False`

			браузерами Google Chrome, HUAWEI Browser, Samsung Internet и Яндекс Браузер.
			
			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 браузера.
			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`.
			• Рекомендуется выбрать Google Chrome, HUAWEI Browser, Samsung Internet Browser или Yandex Browser в качестве браузера по умолчанию в настройках операционной системы.	

`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".	
`AllowGoogleAnalytics`	Передавать данные в сервисы Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics	Boolean	`True` – приложение автоматически передает данные о работе Kaspersky Endpoint Security для Android в сервисы Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics. Данные необходимы для повышения качества работы приложения и анализа удовлетворенности пользователей. Передача данных в сервисы Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics осуществляется по защищенному каналу. Доступ к данным и защита данных регламентируются	`True`

			соответствующими условиями использования сервисов Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics. `False` – передача данных в сервисы Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics выключена.	
`KscDeviceNameTag`	Тег названия устройства для Kaspersky Security Center	String	Этот параметр доступен только для VMware AirWatch. Тег будет добавлен к названию устройства в Kaspersky Security Center. Тег и название устройства разделены пробелом. Это 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`
`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.	

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 баз вредоносного ПО (объем трафика может отличаться из-за размера баз вредоносного ПО), МБ	0.04	2.21	2.25
Синхронизация мобильного устройства с Kaspersky Security Center, МБ	0.03	0.02	0.05
Регулярное обновление баз вредоносного ПО (объем трафика может отличаться из-за размера баз вредоносного ПО), МБ	0.08	3.06	3.14
Выполнение команд Анти-Вора. Определение местоположения (объем трафика может отличаться из-за характеристик встроенной камеры и качества изображений), МБ	0.09	0.8	0.17
Выполнение команд Анти-Вора. Фотографирование, МБ	1.0	0.02	1.02
Выполнение команд Анти-Вора. Блокировка устройства, МБ	0.06	0.05	0.11
Средний расход за сутки, МБ	0.22	6.96	7.18

Участие в Kaspersky Security Network

Чтобы повысить эффективность защиты мобильных устройств, Kaspersky Endpoint Security для Android использует данные, полученные от пользователей со всего мира. Для обработки этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (KSN) – инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Ваше участие в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках новых угроз, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний Kaspersky Endpoint Security для Android. Кроме того, участие в Kaspersky Security Network обеспечивает доступ к данным о репутации программ и веб-сайтов.

Когда вы участвуете в Kaspersky Security Network, 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: Защита от вредоносного ПО, 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 могут быть недоступны в решении на территории США.

Обмен информацией с Kaspersky Security Network

Для повышения уровня оперативной защиты Kaspersky Secure Mobility Management использует облачную службу Kaspersky Security Network в работе следующих компонентов:

- **Защита от вредоносного ПО.** 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 базы вредоносного ПО, но уже содержится в KSN. Облачная служба Kaspersky Security Network обеспечивает полноценную работу Защиты от вредоносного ПО 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 Защита от вредоносного ПО 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.

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: Защита от вредоносного ПО (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 изменены после очередной синхронизации устройства с Kaspersky Security Center. После применения политики компоненты, использующие Kaspersky Security Network, будут выключены и настройка компонентов будет недоступна.

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.

Предоставление данных сторонним сервисам

Kaspersky Endpoint Security для Android использует сервисы Google: Firebase Cloud Messaging, Google Analytics для Firebase, 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, Firebase Performance Monitoring и Crashlytics для повышения качества работы приложения и формирования "Лабораторией Касперского" эффективных маркетинговых материалов.

Обмен информацией с Firebase Cloud Messaging

Kaspersky Endpoint Security для Android использует сервис Firebase Cloud Messaging (FCM) для своевременной доставки команд на мобильные устройства и принудительной синхронизации при изменении параметров политики. При этом приложение использует механизм push-уведомлений.

Для использования сервиса Firebase Cloud Messaging необходимо настроить параметры сервиса в Kaspersky Security Center. 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.). 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 регулируется соответствующими условиями использования сервисов Firebase: https://firebase.google.com/terms/data-processing-terms/, https://firebase.google.com/support/privacy/.

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

1. В дереве консоли выберите **Управление мобильными устройствами → Мобильные устройства**.
2. В контекстном меню папки **Мобильные устройства** выберите пункт **Свойства**.
3. В окне свойств папки **Мобильные устройства** выберите раздел **Параметры Google Firebase Cloud Messaging**.
4. Нажмите на кнопку **Сбросить параметры**.

Обмен информацией с Google Analytics для Firebase, 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 Secure Mobility Management осуществляет обмен данными с сервисами Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics по следующим причинам:

- В целях повышения качества работы приложения.

  Для обмена данными с сервисами Google Analytics для Firebase, 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, Firebase Performance Monitoring и Crashlytics в целях формирования "Лабораторией Касперского" эффективных 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, Firebase Performance Monitoring и Crashlytics в настройках групповой политики (см. ниже).

[Предоставление данных в Google Analytics для Firebase, 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;
- 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 баз вредоносного ПО 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.

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, 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 изменены после очередной синхронизации устройства с Kaspersky Security Center.

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.

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 **Дополнительно**.
5. В разделе **Отправка статистики** 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.

Samsung KNOX

Samsung KNOX – мобильное решение для настройки и защиты мобильных устройств Samsung под управлением операционной системы Android. Подробная информация о Samsung KNOX приведена на *сайте Службы технической поддержки Samsung*.

Установка приложения Kaspersky Endpoint Security для Android с помощью KNOX Mobile Enrollment

KNOX Mobile Enrollment (KME) является частью мобильного решения Samsung KNOX и используется для массовой установки и первоначальной настройки приложений на новых устройствах Samsung, приобретенных у официальных поставщиков.

Установка приложения Kaspersky Endpoint Security для Android через KNOX Mobile Enrollment состоит из следующих этапов:

1. **Создание профиля KNOX MDM с приложением Kaspersky Endpoint Security для Android.**
2. **Добавление устройств в KNOX Mobile Enrollment.**
3. **Установка приложения Kaspersky Endpoint Security для Android на мобильных устройствах пользователя.**

Подробная информация о работе с KNOX Mobile Enrollment приведена в *Руководстве пользователя KNOX Mobile Enrollment*.

Развертывание через KNOX Mobile Enrollment возможно только для Samsung-устройств. Список поддерживаемых устройств приведен на *сайте Службы технической поддержки Samsung*.

Создание профиля KNOX MDM

Профиль KNOX MDM – профиль, который содержит ссылки на приложения для их быстрого развертывания и первоначальной настройки на мобильных устройствах.

Чтобы создать профиль KNOX MDM, выполните следующие действия:

1. Войдите в консоль Samsung KNOX → **KNOX Mobile Enrollment**.
2. Выберите раздел **Профили MDM**.
3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания профиля KNOX MDM.
4. На шаге **Подключение сервера MDM** выберите **URI сервера не требуется для моего сервиса MDM** и нажмите на кнопку **Далее**.
5. На шаге **Сведения о профиле MDM** выполните следующие действия:

   a. Введите общую информацию о профиле KNOX MDM: **Название профиля** и **Описание**.

   b. Введите путь к установочному файлу APK по кнопке **Добавить приложения MDM**.

   Установочный файл Kaspersky Endpoint Security для Android входит в комплект поставки Kaspersky Secure Mobility Management. Предварительно разместите установочный файл APK на Веб-сервере Kaspersky Security Center или на другом сервере, доступном для загрузки с устройства.

   c. Введите параметры подключения устройства к Kaspersky Security Center в поле **Пользовательские данные JSON** в формате:
   `{"serverAddress":"ksc.server.com","serverPort":"12345","groupName":"MOBILE GROUP"}`.

   Подключение устройства к Kaspersky Security Center требуется для активации приложения, настройки устройства и отправки команд.

   d. Установите флажок **Добавление соглашений, связанных с Knox**.

   Для установки Kaspersky Endpoint Security для Android через KNOX Mobile Enrollment пользователь мобильного устройства должен принять условия Лицензионного соглашения Samsung. Вы можете ознакомиться с условиями Лицензионного соглашения Samsung в блоке **Лицензионные соглашения с конечным пользователем, условия обслуживания и пользовательские соглашения**. Также вы можете добавить другие юридические документы вашей компании, необходимые для развертывания профиля KNOX MDM, по кнопке **Добавить пользовательское соглашение**.

   e. Снимите флажок **Привяжите лицензию Knox к этому профилю**.

   Информация о лицензии Samsung KNOX передается на мобильное устройство вместе с политикой при синхронизации устройства с Kaspersky Security Center.
6. Нажмите на кнопку **Сохранить**.

В результате новый профиль KNOX MDM с приложением Kaspersky Endpoint Security для Android будет добавлен в список в консоли KME.

Добавление устройств в KNOX Mobile Enrollment

Добавление устройств в консоли KNOX Mobile Enrollment (KME) может быть выполнено следующими способами:

- Поставщик автоматически добавляет устройства в консоль KME после приобретения устройства.

Выберите этот способ, если ваша организация сотрудничает с официальным поставщиком Samsung-устройств.

- Администратор устанавливает приложение KNOX Deployment из Google Play на свое мобильное устройство и переносит профиль KNOX MDM на устройства пользователей с помощью Bluetooth, 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**.

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`).

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 или выше.

О KNOX-контейнере

KNOX-контейнер – безопасная среда на устройстве пользователя с отдельным рабочим столом, панелью запуска, приложениями, виджетами. KNOX-контейнер позволяет изолировать корпоративные приложения и данные от персональных. KNOX-контейнер является компонентом мобильного решения Samsung KNOX.

Samsung KNOX – мобильное решение для настройки и защиты мобильных устройств Samsung под управлением операционной системы Android. Подробная информация о Samsung KNOX приведена на *сайте Службы технической поддержки Samsung*.

KNOX-контейнеры позволяют разделить персональные и корпоративные данные на мобильном устройстве. Например, невозможно отправить файл, расположенный в KNOX-контейнере, с помощью личного почтового ящика. Рекомендуется разворачивать KNOX-контейнер, если для работы с корпоративными данными используются личные мобильные устройства сотрудников.

Для использования KNOX-контейнеров требуется активировать Samsung KNOX. После синхронизации устройства с Kaspersky Security Center пользователю мобильного устройства будет предложено установить KNOX-контейнер. Перед установкой KNOX-контейнера пользователь должен принять условия Лицензионного соглашения от компании Samsung.

После установки KNOX-контейнера на рабочий стол мобильного устройства будет добавлен значок KNOX . Или рабочая область будет добавлена в список приложений на мобильном устройстве. Для работы с корпоративными данными пользователю нужно запустить приложение из KNOX-контейнера.

Kaspersky Endpoint Security для Android не устанавливается в KNOX-контейнер и не защищает корпоративные данные. Kaspersky Endpoint Security для Android не обнаруживает загрузку вредоносных файлов и не блокирует вредоносные сайты в KNOX-контейнере. В KNOX-контейнере невозможно контролировать загрузку приложений и запретить использование камеры. Kaspersky Endpoint Security для Android защищает только личные данные. Корпоративные данные можно защитить с помощью инструментов Samsung KNOX. Подробная информация о Samsung KNOX приведена на *сайте Службы технической поддержки Samsung*.

Активация Samsung KNOX

Чтобы использовать KNOX-контейнер на мобильном устройстве пользователя, требуется активировать Samsung KNOX. 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.

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.

   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 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 на кнопку **OK**.

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

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

Настройка почтового ящика Exchange в KNOX

Для работы с корпоративной почтой, контактами и календарем в KNOX-контейнере следует настроить параметры почтового ящика Exchange (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.

> 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 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 изменены после очередной синхронизации устройства с Kaspersky Security Center.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

Права на настройку групповых политик

Администраторы Kaspersky Security Center могут настраивать права доступа пользователей Консоли администрирования к различным функциям программы в зависимости от служебных обязанностей пользователей.

Для каждой функциональной области администратор может назначать следующие права доступа:

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

Права доступа к разделам плагина управления Kaspersky Endpoint Security для Android

Функциональная область	Раздел политики
рабочий профиль Android;	Рабочий профиль Android
Анти-Вор	Анти-Вор
Контроль приложений	Контроль приложений
Защита	Проверка, Защита, Обновление баз данных
Контроль соответствия	Контроль соответствия
Управление устройствами	Управление устройствами, Синхронизация
Управление Samsung-устройствами	APN, Управление Samsung-устройствами, KNOX-контейнеры, Сетевой экран
Управление системой	Дополнительно, Wi-Fi
Веб-Фильтр	Веб-Фильтр
Режим device owner	Ограничение функций, параметры Google Chrome, Exchange ActiveSync, режим киоска, NDES и SCEP

Права доступа к разделам плагина управления Kaspersky Device Management для iOS

Функциональная область	Раздел политики
Дополнительные	Веб-клипы, Шрифты, AirPlay, AirPrint
Exchange ActiveSync	Общие, Пароль, Синхронизация, Ограничения функций, Ограничения приложений
Общие	Общие, Единая учетная запись, Веб-Фильтр, Wi-Fi, Точка доступа (APN), Exchange ActiveSync, Электронная почта, Конфигурационные параметры
LDAP (календарь/контакты)	LDAP, Календарь, Контакты, Подписки на календарь
Ограничения и безопасность	Ограничения функций, Ограничения приложений, Ограничения медиаконтента, Пароль, VPN, Глобальный HTTP-прокси, Сертификаты, SCEP

Категории приложений

Контроль приложений поддерживает категоризацию приложений. Режим работы, заданный для категории приложений, будет применен для всех приложений из этой категории. Категорию для каждого приложения определяет облачная служба Kaspersky Security Network.

Категории приложений

Категория	Описание
Развлечения	Приложения для интерактивных развлечений.
IM-клиенты, телефонные программы	Приложения для обмена мгновенными сообщениями, голосовой и видеосвязи через IP-телефонию.
Социальные сети	Приложения для работы с социальными сетями, блогами.
ПО для бизнеса	Приложения для подсчета налогов, управления банковскими операциями, работы с таблицами, бухгалтерского учета, а также другие приложения для бизнеса. Текстовые редакторы.
Дом, Семья, Хобби, Здоровье	Приложения, которые содержат рецепты, рекомендации по стилю. Приложения для фитнеса, ведения графика тренировок, получения рекомендаций по диете, здоровому питанию, технике безопасности, охране труда.
Медицина	Приложения, которые содержат справочники симптомов и лекарств, приложения для работников здравоохранения, журналы и новости о медицине.
Мультимедиа	Службы подписки на фильмы, мультимедийные и видеопроигрыватели. Музыкальные службы, проигрыватели, радиовещание.
ПО для графического дизайна	Приложения для работы с камерой, графические редакторы, приложения для управления фотографиями и их публикации.
Плагины для чтения новостных и RSS-лент	Приложения для чтения газет, журналов, блогов, агрегаторы новостей.
Погода	Приложения для отображения прогноза погоды.
Программы для образования	Приложения для чтения книг, справочники, учебники, словари, тезаурусы, энциклопедии. Приложения для подготовки к экзаменам, учебные материалы, словари, развивающие игры, средства изучения языков.
Онлайн-покупки	Приложения для совершения покупок в интернете и участия в аукционах, подарочные купоны, средства сравнения цен и ведения списка покупок, чтение отзывов о продуктах.
Утилиты для запуска	Приложения, предназначенные для изменения вида рабочего стола, виджетов, ярлыков.
Операционные системы и утилиты	Системные приложения, обеспечивающие управление операционной системой, взаимодействие с пользователем, управление оперативной памятью.
Программы для просмотра карт	Путеводители по городам, информация о местных компаниях, средства планирования поездки.
Другие 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 необходимы 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.

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.

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 Защита от вредоносного ПО.

Защита от вредоносного ПО 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 базы вредоносного ПО.

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.
- 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 базы вредоносного ПО 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.

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 о вашей лицензии.
- Переходить между главным окном и настройками приложения с помощью кнопок внизу.

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 с защитой (например, базы вредоносного ПО устарели или установлено новое непроверенное приложение).

Проверка устройства

Защита от вредоносного ПО имеет ряд ограничений:

- При работе Защиты от вредоносного ПО в рабочем профиле 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.

- На устройствах с операционной системой Android 11 или 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.

Чтобы запустить проверку устройства, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **Защита от вредоносного ПО** → **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 поиска вредоносного ПО может быть ограничен вашим администратором.

Чтобы настроить поиск вредоносного ПО, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **Защита от вредоносного ПО** → **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 Защиты от вредоносного ПО.

Проверка устройства по расписанию

Защита от вредоносного ПО имеет ряд ограничений:

- При работе Защиты от вредоносного ПО в рабочем профиле 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.

- На устройствах с операционной системой Android 11 или 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.

Чтобы настроить расписание полной проверки устройства, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **Защита от вредоносного ПО** → **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.

Если устройство находится в режиме экономии заряда батареи, приложение может выполнить эту задачу позже, чем указано. Для своевременного реагирования KES-устройств под управлением Android на команды администратора, следует включить использование сервиса Firebase Cloud Messaging.

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 базы вредоносного ПО 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** → **Защита от вредоносного ПО** → **Режим постоянной защиты**.
2. Выберите режим защиты устройства:
   - **Выключена**. Защита выключена.
   - **Рекомендуемый**. В процессе поиска вредоносного ПО проверяются только установленные приложения и файлы из папки "Загрузки". Защита от вредоносного ПО проверяет новые приложения один раз, сразу после их установки.
   - **Расширенный**. Защита от вредоносного ПО проверяет на наличие вредоносных объектов все файлы на устройстве при любом действии с ними (например, сохранении, перемещении или изменении). Также Защита от вредоносного ПО 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** → **Защита от вредоносного ПО** 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 базы вредоносного ПО, но уже содержится в KSN. Облачная служба Kaspersky Security Network обеспечивает полноценную работу Защиты от вредоносного ПО 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 → Защита от вредоносного ПО → 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 Защиты от вредоносного ПО.

Обновление баз вредоносного ПО

Чтобы обновить базы вредоносного ПО:

В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **Защита от вредоносного ПО** → **Запустить обновление баз**.

Обновление баз по расписанию

Приложение может автоматически обновлять базы вредоносного ПО по заданному расписанию.

Чтобы настроить расписание обновления, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **Защита от вредоносного ПО** → **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 баз вредоносного ПО будет запускаться согласно расписанию.

Если устройство находится в режиме экономии заряда батареи, приложение может выполнить эту задачу позже, чем указано. Для своевременного реагирования KES-устройств под управлением Android на команды администратора, следует включить использование сервиса Firebase Cloud Messaging.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в решении на территории США.

Действия в случае кражи или потери устройства

В случае кражи или потери устройства обратитесь к системному администратору. Администратор дистанционно запустит на устройстве функции Анти-Вора в соответствии с требованиями корпоративной безопасности.

Если на устройство отправлена команда сброса настроек до заводских, контроль над устройством будет потерян, и остальные команды Анти-Вора выполняться не будут.

Веб-Фильтр

Для включения Веб-Фильтра должны быть выполнены следующие условия:

- 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.

Веб-Фильтр на Android-устройствах поддерживается только браузерами Google Chrome, HUAWEI Browser, Samsung Internet и Яндекс Браузер.

Если приложение Kaspersky Endpoint Security для Android в режиме device owner не установлено в качестве службы Специальных возможностей, Веб-Фильтр поддерживается только браузером Google Chrome и проверяет только домен сайта. Чтобы Веб-Фильтр поддерживался другими браузерами (Samsung Internet Browser, Яндекс Браузер и HUAWEI Browser), приложение Kaspersky Endpoint Security должно быть включено в качестве службы Специальных возможностей. Это также позволит использовать функцию Custom Tabs.

Функция Custom Tabs поддерживается браузерами Google Chrome, HUAWEI Browser и Samsung Internet Browser.

Чтобы использовать Веб-Фильтр в приложении Telegram, выключите просмотр ссылок во встроенном браузере в настройках Telegram.

В браузерах HUAWEI Browser, Samsung Internet Browser и Яндекс Браузер Веб-Фильтр не блокирует сайты на мобильном устройстве, если используется рабочий профиль и установлен флажок Включить Веб-Фильтр только в рабочем профиле.

Для постоянного использования Веб-Фильтра для проверки сайтов во время работы в интернете, назначьте Google Chrome, HUAWEI Browser, Samsung Internet Browser или Яндекс Браузер 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.

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. Логин должен иметь один из следующих форматов:

   - `userPrincipalName@DNSDomainName`
   - `sAMAccountName`
   - `sAMADomain\sAMAccountName`

   Для получения дополнительных сведений об этих атрибутах перейдите на веб-сайт Microsoft в раздел Техническая документация. Обратитесь к вашему администратору для получения подробной информации.

3. Если вы получили от администратора одноразовый пароль, установите флажок **Одноразовый пароль** и введите полученный пароль.

   Запустится мастер установки сертификата.

4. Следуйте указаниям мастера.

Синхронизация с Kaspersky Security Center

Синхронизация мобильного устройства с системой удаленного администрирования Kaspersky Security Center необходима для защиты и настройки вашего устройства в соответствии с требованиями корпоративной безопасности. Синхронизация устройства с Kaspersky Security Center выполняется автоматически. Можно также запускать синхронизацию вручную. После первой синхронизации ваше устройство добавляется в список мобильных устройств, управляемых через Kaspersky Security Center. После этого администратор может настраивать ваше устройство в соответствии с требованиями корпоративной безопасности.

Вы можете задать значения параметров синхронизации во время работы мастера первоначальной настройки или в настройках Kaspersky Endpoint Security. 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**.

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.

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.

Приложение Kaspersky Endpoint Security для Android можно установить одним из следующих способов.

- С помощью QR-кода, сгенерированного в Kaspersky Security Center, для установки приложения на устройства под управлением Android версии 7 и выше.
- С помощью пакета установки, загруженного из Kaspersky Security Center, и выполнения команды в ADB. Этот способ подходит для установки приложения на устройства под управлением Android версий 5–6 и на устройства под управлением более поздних версий Android, на которых не установлен сканер QR-кода.

Настройка приложения в режиме device owner на устройствах с Android версии 7 и 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.

   На устройствах Xiaomi под управлением Android 12 автоматический запуск Kaspersky Endpoint Security для Android не предусмотрен. Запустите приложение вручную.

5. Активируйте приложение, следуя указаниям мастера первоначальной настройки.

Если для развертывания приложения используется пакет установки, загруженный из Kaspersky Security Center, после сброса настроек устройства до заводских и сканирования QR-кода на экране устройства может появиться сообщение **Заблокировано Play Защитой**. Это связано с тем, что сертификат подписи пакета установки отличается от указанного в Google Play. Для продолжения установки необходимо нажать кнопку **Все равно установить**. При нажатии кнопки **OK** процесс установки будет прерван, а настройки устройства будут сброшены до заводских.

Приложение Kaspersky Endpoint Security для Android будет установлено и активировано на устройстве в режиме device owner.

Настройка приложения в режиме device owner на устройствах с Android версий 5–6

На устройствах с Android версий 5–6 процедура настройки режима device owner отличается от стандартной. Необходимо предварительно настроить устройство, установить приложение и настроить дополнительные параметры с помощью Android Debug Bridge (ADB).

Этот способ подходит для установки приложения на устройства под управлением других версий Android, а также на устройства без сканера QR-кода.

Предварительная настройка

Для создания пакета установки в Консоли администрирования в разделе **Тип устройства** выберите **Персональное устройство**, а на странице **Способ установки Kaspersky Endpoint Security для Android** выберите **Загрузить пакет установки из Kaspersky Security Center**. Подробнее см. в разделе Установка Kaspersky Endpoint Security для Android на персональные устройства.

Развертывание

Чтобы развернуть Kaspersky Endpoint Security для Android на устройстве с Android версий 5–6 в режиме device owner, выполните следующие действия:

1. Сбросьте настройки устройства до заводских. Если устройство ранее не использовалось, пропустите этот шаг и перейдите к шагу 3.
2. Перейдите в раздел **Параметры** → **Учетные записи** и удалите с устройства все учетные записи.
3. Отключите блокировку экрана.
4. Включите режим разработчика. Для этого:
   a. Перейдите в раздел **Параметры** → **Сведения о телефоне**.
   b. Нажмите на параметр **Номер сборки** семь раз. Появится сообщение "**Вы стали разработчиком!**"

   На некоторых устройствах эти разделы могут находиться в другом расположении или иметь другие названия. Подробнее смотрите в документации к Android.
5. Перейдите в раздел **Параметры** → **Параметры разработчика** и включите параметр **Отладка по USB**.
6. Разрешите установку приложений, полученных не из Google Play. Для этого:
   a. Перейдите в раздел **Параметры** → **Безопасность**.
   b. Включите параметр **Неизвестные источники**.
7. Для установки Kaspersky Endpoint Security для Android на устройство используйте пакет установки, загруженный из Kaspersky Security Center, или другой подходящий способ (например, файл .apk).
8. После установки приложения в открывшемся окне нажмите **Готово**, чтобы завершить работу мастера установки.

   Для успешной реализации этого сценария приложение следует запускать только после выполнения команды ADB (см. шаг 11).
9. Установите ADB на компьютер.
10. Подключите устройство к компьютеру с помощью USB-кабеля.

    Появится диалоговое окно с запросом на разрешение отладки устройства на компьютере. Нажмите на кнопку **OK**.
11. Запустите ADB и выполните следующую команду:

    `adb shell dpm set-device-owner com.kaspersky.kes/com.kms.selfprotection.DeviceAdmin`.

12. Запустите приложение Kaspersky Endpoint Security для Android и активируйте его, следуя инструкциям мастера первоначальной настройки.

На некоторых устройствах Xiaomi невозможно развернуть приложение в этом режиме через ADB, если включена оптимизация MIUI. Для развертывания приложения в этом режиме необходимо отключить оптимизацию MIUI. Для этого перейдите в раздел **Параметры** → **Номер сборки**. Нажмите на номер сборки 6–8 раз, чтобы перейти в **Параметры разработчика** для отключения оптимизации MIUI. Повторите перечисленные шаги для развертывания приложения на этих устройствах.

Установка корневых сертификатов на устройстве

Корневой сертификат – это сертификат открытого ключа, выпущенный доверенным центром сертификации (CA). Корневые сертификаты используются, чтобы проверять пользовательские сертификаты и гарантировать их подлинность.

Ваш администратор может указать корневые сертификаты, которые необходимо установить на устройство. На устройства, работающие в режиме device owner и использующие рабочий профиль, эти сертификаты устанавливаются автоматически. Если вы используете личный профиль, то будете получать уведомления, при этом вам нужно будет вручную устанавливать каждый сертификат, следуя приведенным ниже инструкциям.

Чтобы вручную установить корневой сертификат на устройстве:

1. Откройте **Параметры** устройства.
2. Перейдите в параметры безопасности. Путь зависит от модели устройства и версии операционной системы. Например, вам может понадобиться перейти в **Расширенные настройки** → **Безопасность** или **Безопасность и экран блокировки** → **Хранилище учетных данных**.
3. Выберите **Установить из встроенной памяти** / **Установить с SD-карты** или аналогичную опцию.
4. Нажмите **Сертификат ЦС**.
5. В окне подтверждения нажмите **Все равно установить**.
6. В открывшемся файловом менеджере выберите необходимый корневой сертификат.

   На некоторых устройствах загруженные сертификаты могут не отображаться в списке **Последние файлы**. Подождите 3–5 минут и снова откройте файловый менеджер. Время ожидания зависит от модели устройства. Если через 3–5 минут файлы не появились, перейдите в папку **Внутреннее хранилище\Загрузки\kesm_certs** или **Карта памяти\Загрузки\kesm_certs** и выберите требуемый корневой сертификат.

Корневой сертификат будет установлен на устройство.

Установка и использование почтовых и VPN-сертификатов на устройстве

Ваш администратор может указать почтовые и VPN-сертификаты, которые необходимо установить на устройство. На устройства, работающие в режиме device owner или использующие рабочий профиль, эти сертификаты устанавливаются автоматически.

Почтовый сертификат устанавливается на устройство только если ваш администратор заранее настроил параметры Exchange ActiveSync.

VPN-сертификат также можно установить в хранилище доверенных сертификатов в личном профиле и использовать в любом приложении. Вы получите уведомление, и вам нужно будет вручную установить VPN-сертификат, следуя приведенным ниже инструкциям.

Чтобы вручную установить VPN-сертификат на устройстве:

1. Откройте Kaspersky Endpoint Security для Android.
2. Нажмите **Уведомления**.
3. В уведомлении о сертификате нажмите **Установить**.

   Откроется окно с паролем сертификата.
4. Запомните или запишите пароль и нажмите **OK**.
5. В окне с запросом пароля сертификата введите пароль и нажмите **OK**.
6. Нажмите **OK**, чтобы подтвердить установку сертификата.

VPN-сертификат будет установлен на устройство.

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 **OK**.

   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 **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.

Включение специальных возможностей для приложения на Android 13 или выше

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 **OK**.

   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 **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.

Обновление приложения

Kaspersky Endpoint Security можно обновить следующими способами:

- Вручную с помощью сайта "Лаборатории Касперского". Вы загружаете с сайта "Лаборатории Касперского" новую версию приложения и устанавливаете ее на свое устройство.
- С помощью администратора. Администратор дистанционно обновляет версию приложения на вашем устройстве с помощью системы удаленного администрирования Kaspersky Security Center.

Обновление приложения с сайта "Лаборатории Касперского"

Чтобы обновить приложение с сайта "Лаборатории Касперского":

1. Перейдите на сайт "Лаборатории Касперского".
2. Найдите Kaspersky Security для мобильных устройств на сайте.
3. Нажмите **Показать версии для загрузки**.
4. Выберите версию приложения и нажмите **Скачать**.
5. Откройте загруженный файл APK и следуйте инструкциям на экране.

Приложение Kaspersky Endpoint Security для Android будет обновлено.

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 могут быть недоступны в решении на территории США.

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.

Приложения с "портфелем"

Значок приложения в рабочем профиле Android

Приложения, отмеченные значком портфеля (корпоративные приложения), находятся на вашем устройстве в рабочем профиле Android (далее также "Рабочий профиль"). *Рабочий профиль Android* – это безопасная среда на вашем устройстве, в которой администратор может управлять приложениями и учетными записями, не ограничивая ваши возможности работы с персональными данными.

Рабочий профиль позволяет хранить корпоративные данные отдельно от персональных данных. Это обеспечивает конфиденциальность корпоративных данных и их защиту от вредоносных приложений. При создании рабочего профиля на вашем устройстве в рабочий профиль автоматически устанавливаются следующие корпоративные приложения: Google Play Маркет, Google Chrome, Загрузки, Kaspersky Endpoint Security для Android и другие.

Приложение Knox

Значок Knox

Приложение Knox открывает Knox-контейнер на вашем устройстве. *Knox-контейнер* – безопасная среда на вашем устройстве с отдельным рабочим столом, панелью запуска, приложениями, виджетами. Администратор может управлять приложениями и учетными записями в Knox-контейнере, не ограничивая ваши возможности работы с персональными данными.

Knox-контейнер позволяет хранить корпоративные данные отдельно от персональных данных. Это обеспечивает конфиденциальность корпоративных данных и их защиту от вредоносных приложений.

В Knox-контейнере вам доступны корпоративный почтовый ящик, контактные данные сотрудников организации, хранилище файлов и другие приложения.

Подробная информация о работе с Knox приведена на сайте Службы технической поддержки Samsung.

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.

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.

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.

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 вашей лицензии и проблемах безопасности.

Приложение Kaspersky Security для iOS на вашем устройстве будет активировано.

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.

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.

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 могут быть недоступны в решении на территории США.

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.

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).

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.

Комплект поставки

В комплект поставки Kaspersky Secure Mobility Management могут входить различные компоненты в зависимости от выбранной версии программы.

Kaspersky Security Center

- `ksc_14_<version>_full_<language>.exe`

  Программа установки Kaspersky Security Center. Эта версия создана специально для работы с Kaspersky Secure Mobility Management.

- `ksc_14_<version>_Console_<language>.exe`

  Программа установки Консоли администрирования на базе MMC. Эта версия создана специально для работы с Kaspersky Secure Mobility Management.

  Можно установить Консоль администрирования на другое устройство и управлять Сервером администрирования Kaspersky Security Center удаленно.

Управление мобильными устройствами в Консоли администрирования на базе MMC

- `klcfginst.exe`

  Программа установки Плагина управления Kaspersky Endpoint Security для Android.

- `klmdminst.exe`

  Программа установки Плагина управления Kaspersky Device Management для iOS.

Управление мобильными устройствами в Kaspersky Security Center Web Console

- `on_prem_ksm_devices_<version>.zip`

  Архив, содержащий файлы 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_<version>.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*.

Файл приложения Kaspersky Endpoint Security для Android

`kesandroid10<version><languages>.apk` – пакетный файл Android для приложения Kaspersky Endpoint Security для Android.

Файл Корпоративного каталога приложений

`Install_<version>.exe` – дистрибутив Корпоративного каталога приложений. Дистрибутив содержит следующие компоненты:

- Корпоративный каталог приложений
- Консоль управления корпоративным каталогом приложений
- Сервер Apache

Дополнительная информация об установке Корпоративного каталога приложений приведена в *справке по Корпоративному каталогу приложений*.

Дополнительные файлы

- `sc_package_<languages>.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.

  - `kesandroid10<version><languages>.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.

  Если вы создадите инсталляционный пакет с архивом `sc_package.exe` в Kaspersky Security Center версии ниже 14.2, Kaspersky Endpoint Security для Android не удастся установить на устройствах под управлением Android 10 и выше. Чтобы избежать этой проблемы, обновитесь до Kaspersky Security Center 14.2 или обратитесь в Службу технической поддержки для получения соответствующей версии архива.

Комплект документации

- Справка Kaspersky Secure Mobility Management.

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

Kaspersky Secure Mobility Management 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.

  Приложение Kaspersky Endpoint Security для Android в настоящее время недоступно в 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 Secure Mobility Management включает следующие компоненты защиты и управления:

- Защита от вредоносного ПО (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.

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:

- **Защита от вредоносного ПО**. Этот компонент обнаруживает и устраняет угрозы на устройствах, используя базы вредоносного ПО и облачную службу Kaspersky Security Network. В состав Защиты от вредоносного ПО 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 базы вредоносного ПО 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.

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.

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.

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.

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 или выше (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.

Известные проблемы и рекомендации

Следующие известные проблемы не являются критичными для работы решения.

Известные проблемы при управлении мобильными устройствами

- Если вы отредактируете поля **Имя** и **Описание** на вкладке **Общие** в свойствах устройства, изменения не отобразятся в списке мобильных устройств, подключенных к Kaspersky Security Center из-за технических ограничений.

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 Защита от вредоносного ПО и Веб-Фильтр. Администратор может настраивать параметры Защиты от вредоносного ПО 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 Защиты от вредоносного ПО

- 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 базы вредоносного ПО, 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 баз вредоносного ПО с Сервера администрирования может завершиться ошибкой на мобильных устройствах. В этом случае запустите задачу обновления баз вредоносного ПО на Сервере администрирования.

- На некоторых устройствах Kaspersky Endpoint Security для Android не обнаруживает устройства, подключенные по USB OTG. Выполнить поиск вредоносного ПО на таких устройствах невозможно.

- На устройствах с операционной системой Android 11 или 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 и выше может некорректно отображаться окно настройки расписания запуска поиска вредоносного ПО (не отображаются элементы управления). Проблема связана с известным дефектом в Android 7.

- На устройствах под управлением Android 7 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 Kaspersky Endpoint Security для Android не обнаруживает загрузку вредоносного файла в память устройства. Вредоносный файл может быть обнаружен Защитой от вредоносного ПО при запуске файла или во время поиска вредоносного ПО на устройстве. Проблема связана с известным дефектом в Android 6. Для обеспечения безопасности устройства рекомендуется настроить запуск поиска вредоносного ПО по расписанию.

Известные проблемы в работе Веб-Фильтра

- Веб-Фильтр на Android-устройствах поддерживается только браузерами Google Chrome, HUAWEI Browser, Samsung Internet Browser и Яндекс Браузер.

- Функция Custom Tabs поддерживается браузерами Google Chrome, HUAWEI Browser и Samsung Internet Browser.

- В браузерах HUAWEI Browser, Samsung Internet Browser и Яндекс Браузер Веб-Фильтр не блокирует сайты на мобильном устройстве, если используется рабочий профиль и установлен флажок Включить Веб-Фильтр только в рабочем профиле.

- 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.

- На iOS-устройствах с Kaspersky Security для iOS при смене языка на устройстве или перезагрузке устройства выключается Веб-Фильтр. Чтобы включить Веб-Фильтр, подождите около минуты после смены языка или перезагрузки устройства и откройте Kaspersky Security для iOS.

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.

- 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.

- На некоторых личных устройствах HUAWEI и Honor приложения из разрешенных категорий могут быть заблокированы, а приложения из запрещенных категорий могут оставаться разблокированными. Это связано с тем, что категория для некоторых приложений из AppGallery не может быть определена правильно.

- На некоторых устройствах Samsung и Oppo после снятия флажка **Блокировать системные приложения** значки приложений могут остаться скрытыми на рабочем столе. Это связано с особенностями операционной системы Android.

Известные проблемы при настройке надежности пароля разблокировки устройства

- На устройствах под управлением Android 10 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 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 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 и выше запрет на использование сетей Wi-Fi не поддерживается.

- 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.

- На Android-устройствах, когда запрещено использование камеры, некоторые приложения могут автоматически закрываться. Эта проблема связана с особенностями работы таких сервисов и функций, как Android System Intelligence и Адаптивный спящий режим, которые используют камеру, чтобы экран не выключался, пока пользователь смотрит на него.

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.

- Если на устройстве Android отключена служба Google "Точность местоположения", команда **Определить местоположение устройства** работать не будет. Обращаем внимание, что не на всех устройствах Android есть эта служба.

- Если вы отправите команду **Включить режим пропажи** на контролируемое устройство iOS MDM без SIM-карты и это устройство будет перезапущено, оно не сможет подключиться к сети Wi-Fi и получить команду **Отключить режим пропажи**. Эта проблема связана с особенностями iOS-устройств. Чтобы этого избежать, можно отправлять эту команду только на устройства с SIM-картой или вставить SIM-карту в заблокированное устройство – в этом случае оно сможет получить команду **Отключить режим пропажи** по мобильной сети.

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 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 устройствах HUAWEI 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 устройствах HUAWEI с прошивкой EMUI под управлением Android 7 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 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 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 или 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.

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.

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.

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.

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.

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 **OK**.

f. В разделе **Точки распространения** нажмите **OK**, 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.

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.

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*.

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".

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.

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**.

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.

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.

  Приложение Kaspersky Endpoint Security для Android в настоящее время недоступно в Google Play.

  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.

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.

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 список, Kaspersky Endpoint Security для Android прекращает выполнять все свои функции после перезагрузки мобильного устройства.

На устройствах с операционной системой Android 11 или выше, либо Android 6-10 (при использовании сервисов Google Play) необходимо выключить системную настройку **Удалять 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)	Подключение к Kaspersky Security Center (идентификатор устройства)
Память (обязательно)	Защита от вредоносного ПО
Доступ на управление всеми файлами (для Android 11 или выше)	Защита от вредоносного ПО
Устройства Bluetooth поблизости (для Android 12 или выше)	Ограничение использования Bluetooth
Уведомления (для Android 13)	Уведомление пользователя о проблемах безопасности и событиях приложения

Разрешение на работу в фоновом режиме (для Android 12 или выше)	Обеспечение непрерывной работы приложения. Если разрешение не предоставлено, приложение может быть выгружено из памяти и не сможет перезапуститься.
Администратор устройства (обязательно)	Анти-Вор – блокировка устройства (только для Android 5.0 – 6)
	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 или выше необходимо при появлении запроса предоставить разрешение "При использовании приложения".
Местоположение	Анти-Вор – определение местоположения устройства На устройствах с операционной системой Android 10 или выше необходимо при появлении запроса предоставить разрешение "Всегда".
Специальные возможности	Анти-Вор – блокировка устройства (только для Android 7.0 или выше)
	Веб-Фильтр
	Контроль приложений
	Защита приложения от удаления (только для Android 7.0 или выше)
	Отображение предупреждений Kaspersky Endpoint Security для Android (только для Android 10 или выше)
	Ограничение использования камеры (только для Android 11 или выше)
Отображать всплывающее окно (на некоторых устройствах Xiaomi)	Веб-Фильтр
Отображать всплывающие окна при работе в фоновом режиме (на некоторых устройствах Xiaomi)	Веб-Фильтр
Работа в фоновом режиме (для устройств Xiaomi с прошивкой MIUI под управлением Android 11 или ниже)	Контроль приложений
	Веб-Фильтр
	Анти-Вор

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*.

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**.

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.

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.

     Логин пользователя устройства должен иметь один из следующих форматов:

     - `userPrincipalName@DNSDomainName`
     - `sAMAccountName`
     - `sAMADomain\sAMAccountName`

   - 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*.

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**.

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.

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.

Если вы используете Kaspersky Security Center Web Console с Kaspersky Security Center Windows 15.1, вы можете задать параметры FCM только в Консоли администрирования. После этого вы сможете отправлять команды на устройства с помощью FCM в Kaspersky Security Center Web 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. Укажите параметры Firebase Cloud Messaging:

   - Введите Sender ID в поле **Номер проекта Firebase**.
   - Откройте файл приватного ключа, скопируйте его содержимое и введите в поле **Приватный ключ**.

   Firebase Cloud Messaging включен.

Чтобы получить Sender ID и файл приватного ключа, выполните следующие действия:

1. Зарегистрируйтесь на портале Google.
2. Перейдите в консоль Firebase.
3. Выполните одно из следующих действий:

   - Чтобы создать новый проект, нажмите на кнопку **Create a project** и следуйте инструкциям на экране.
   - Откройте существующий проект.

4. Нажмите на значок шестеренки и выберите **Project settings**.

   Откроется окно **Project settings**.

5. Выберите вкладку **Cloud Messaging**.
6. Скопируйте Sender ID из поля **Sender ID** в разделе **Firebase Cloud Messaging API (V1)**.
7. Выберите вкладку **Service accounts** и нажмите на кнопку **Generate new private key**.
8. В открывшемся окне нажмите на кнопку **Generate key**, чтобы сгенерировать и загрузить файл приватного ключа.

Подробная информация об операциях в консоли Firebase приведена в соответствующей документации.

Теперь у вас есть значение параметра Sender ID и файл приватного ключа 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 **ОК**, чтобы подтвердить сброс.

Настройки Firebase Cloud Messaging будут сброшены.

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.

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 **OK**, 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.

Если вы отредактируете поля **Имя** и **Описание** на вкладке **Общие** в свойствах устройства, изменения не отобразятся в списке мобильных устройств, подключенных к Kaspersky Security Center из-за технических ограничений.

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.

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.

После разблокировки устройства под управлением операционной системы Android 5.0–6 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**

  Корпоративные данные удалены с устройства. Перечень удаленных данных зависит от режима работы устройства.

  - На личном устройстве удалены KNOX-контейнер и почтовый сертификат.
  - Если устройство работает в режиме device owner, удалены KNOX-контейнер и сертификаты, установленные приложением Kaspersky Endpoint Security для Android (почтовые и VPN-сертификаты, сертификаты, полученные через профили SCEP, кроме мобильных сертификатов).
  - Дополнительно, если установлен рабочий профиль Android, удален рабочий профиль (содержимое, настройки и ограничения) и сертификаты, установленные в рабочем профиле (почтовые и VPN-сертификаты, сертификаты, полученные через профили SCEP, кроме мобильных сертификатов).

- **Определить местоположение устройства**

  Определено местоположение устройства. После нажатия кнопки **Посмотреть местоположение устройства** координаты устройства передаются в Яндекс Карты, и устройство отображается на карте. 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 на кнопку **OK**.
4. Нажмите **OK**, если предлагается подтвердить операцию.

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

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.

Управление групповыми политиками

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

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*.

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.

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**.

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.

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.

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 **ОК**, 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).

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).

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 **OK**, чтобы подтвердить операцию.

Групповая политика будет удалена.

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.

Настройка защиты от вредоносного ПО

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 проверки на наличие вредоносного ПО.

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.

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.

Настройка автоматического запуска поиска вредоносного ПО на мобильном устройстве

Вы можете определить эти параметры политики только для устройств Android.

Чтобы настроить автоматический запуск проверки на наличие вредоносного ПО 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. 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 баз вредоносного ПО.

   - **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**.

Если устройство находится в режиме энергосбережения, приложение может выполнить эту задачу позже, чем указано. Для своевременного реагирования KES-устройств под управлением Android на команды администратора, следует включить использование сервиса Firebase Cloud Messaging.

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.

Настройка обновления баз вредоносного ПО

Вы можете определить эти параметры политики только для устройств Android.

Чтобы настроить обновления баз вредоносного ПО, 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 баз вредоносного ПО отключено.

   - **Раз в день**

     Обновление баз вредоносного ПО выполняется каждый день.

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

   - **Раз в неделю**

     Обновление баз вредоносного ПО 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**.

   Если устройство находится в режиме экономии заряда батареи, приложение может выполнить эту задачу позже, чем указано. Для своевременного реагирования KES-устройств под управлением Android на команды администратора, следует включить использование сервиса Firebase Cloud Messaging.

4. В блоке **Источник обновления баз** укажите источник обновлений, из которого Kaspersky Endpoint Security для Android будет получать и устанавливать обновления баз вредоносного ПО:

   - **Серверы "Лаборатории Касперского"**

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

- **Другой источник**

  Kaspersky Endpoint Security для Android использует сторонний сервер в качестве источника обновлений для загрузки баз вредоносного ПО 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 баз вредоносного ПО по заданному расписанию, когда устройство пользователя находится в роуминге, в разделе **Обновление антивирусных баз в роуминге** установите флажок **Разрешать обновление 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 могут быть недоступны в решении на территории США.

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.

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.

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.

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, базы вредоносного ПО 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.

  Если устройство находится в режиме экономии заряда батареи, приложение может выполнить эту задачу позже, чем указано. Для своевременного реагирования KES-устройств под управлением Android на команды администратора, следует включить использование сервиса Firebase Cloud Messaging.

Для настройки контроля соответствия можно выполнить следующие действия:

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

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.

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.

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.

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.

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**.

  Базы вредоносного ПО Kaspersky Endpoint Security для Android должны регулярно обновляться.

  Дополнительная информация о настройке параметров обновления баз вредоносного ПО 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.

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**.

Корпоративные данные удалены с устройства. Перечень удаленных данных зависит от режима работы устройства.

- На личном устройстве удалены KNOX-контейнер и почтовый сертификат.
- Если устройство работает в режиме device owner, удалены KNOX-контейнер и сертификаты, установленные приложением Kaspersky Endpoint Security для Android (почтовые и VPN-сертификаты, сертификаты, полученные через профили SCEP, кроме мобильных сертификатов).
- Дополнительно, если установлен рабочий профиль Android, удален рабочий профиль (содержимое, настройки и ограничения) и сертификаты, установленные в рабочем профиле (почтовые и VPN-сертификаты, сертификаты, полученные через профили SCEP, кроме мобильных сертификатов).

- **Сброс устройства до заводских настроек**.

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

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.

На iOS-устройствах, если веб-адрес переадресовывается на другую страницу, Веб-Фильтр проверяет только конечную страницу.

Чтобы включить Веб-Фильтр на Android-устройствах:

- 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 поддерживается только браузерами Google Chrome, HUAWEI Browser, Samsung Internet и Яндекс Браузер.

Если приложение Kaspersky Endpoint Security для Android в режиме device owner не установлено в качестве службы Специальных возможностей, Веб-Фильтр поддерживается только браузером Google Chrome и проверяет только домен сайта. Чтобы Веб-Фильтр поддерживался другими браузерами (Samsung Internet Browser, Яндекс Браузер и HUAWEI Browser), приложение Kaspersky Endpoint Security должно быть включено в качестве службы Специальных возможностей. Это также позволит использовать функцию Custom Tabs.

Функция Custom Tabs поддерживается браузерами Google Chrome, HUAWEI Browser и Samsung Internet Browser.

В браузерах HUAWEI Browser, Samsung Internet Browser и Яндекс Браузер Веб-Фильтр не блокирует сайты на мобильном устройстве, если используется рабочий профиль и установлен флажок Включить Веб-Фильтр только в рабочем профиле.

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. Вы можете добавить веб-сайты, используя ссылку (полный URL, включая протокол, например, `https://example.com`).

     Kaspersky Endpoint Security для Android также поддерживает регулярные выражения. При вводе адреса разрешенного или заблокированного веб-сайта используйте следующие шаблоны:

- `https://example\.com/.*` — этот шаблон блокирует или разрешает все дочерние страницы сайта, доступные при использовании протокола HTTPS (например, `https://example.com/about`).

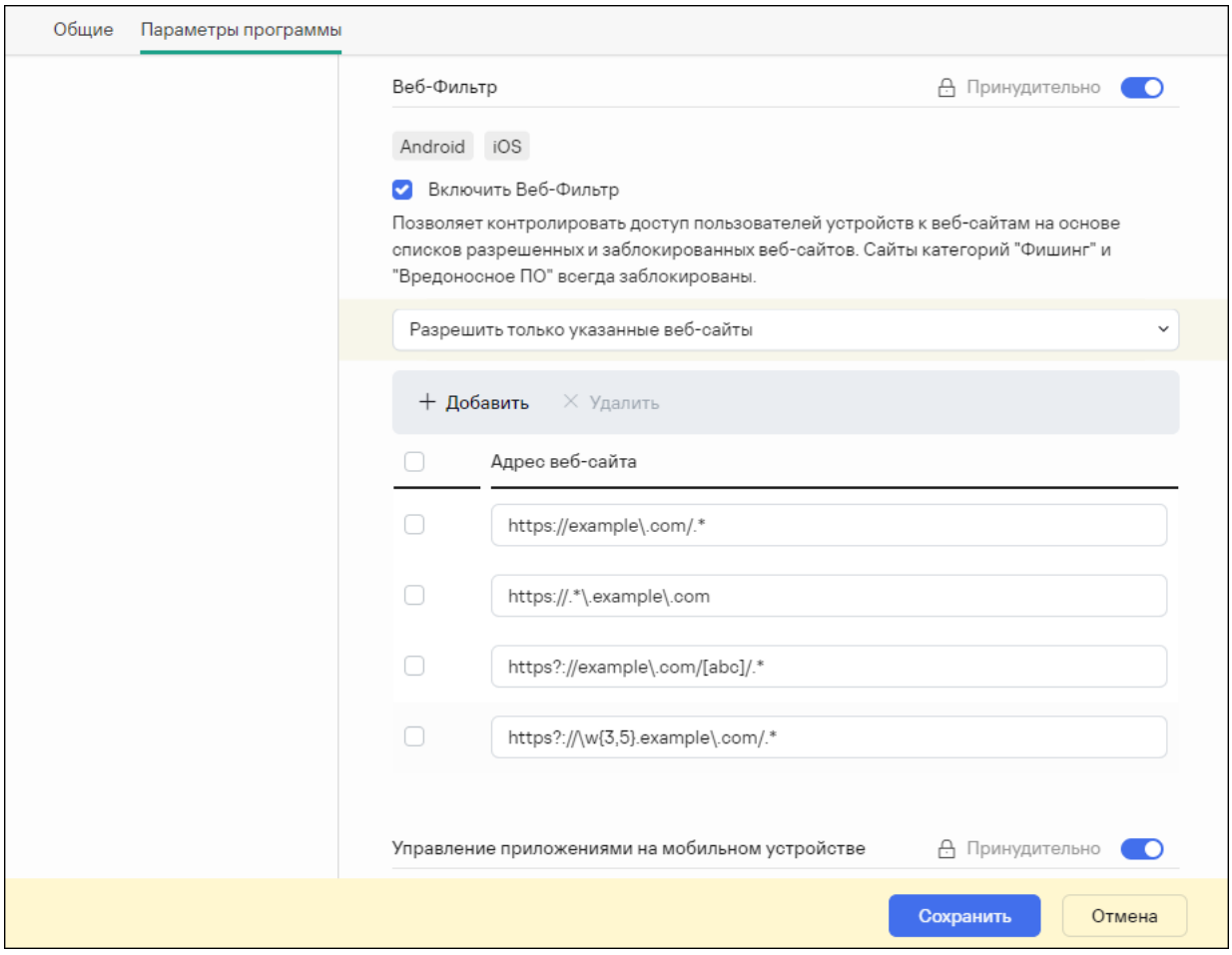
- `https?://example\.com/.*` — этот шаблон блокирует или разрешает все дочерние страницы веб-сайта, доступные при использовании протоколов HTTP и HTTPS.

- `https?://.*\.example\.com` — этот шаблон блокирует или разрешает страницы всех субдоменов веб-сайта (например, `https://pictures.example.com`).

- `https?://example\.com/[abc]/.*` — этот шаблон блокирует или разрешает все дочерние страницы веб-сайта, URL-путь которых начинается с буквы "a", "b" или "c" в качестве первого каталога (например, `https://example.com/b/about`).

- `https?://\w{3,5}.example\.com/.*` — этот шаблон блокирует или разрешает все дочерние страницы веб-сайта, у которых субдомен содержит от 3 до 5 букв (например, `http://abde.example.com/about`).

Используйте выражение `https?`, чтобы выбрать оба протокола — HTTP и HTTPS. Подробнее о регулярных выражениях см. на сайте Службы технической поддержки Oracle.



Раздел Веб-Фильтр с примерами регулярных выражений

- 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.

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 и выше запрет на использование сетей Wi-Fi не поддерживается.

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

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.

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.

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 7 или 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.

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.

- **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. Это может быть полезно, если устройство находится в режиме экономии заряда батареи, поскольку в этом случае приложение может выполнять задачи позже, чем указано. Если вы хотите использовать принудительную синхронизацию, убедитесь что параметры FSM в Kaspersky Security Center настроены.

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.

   При выставлении малых периодов синхронизации фактический период синхронизации может быть немного больше из-за технических ограничений. Это особенно актуально для устройств в режиме экономии заряда батареи. Частые синхронизации приводят к повышенному расходу заряда аккумулятора устройства.

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.

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 Защита от вредоносного ПО, 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.

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.

Вы можете в любой момент отказаться от участия в Kaspersky Security Network.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в решении на территории США.

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:

- **Защита от вредоносного ПО.** 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 базы вредоносного ПО, но уже содержится в KSN. Облачная служба Kaspersky Security Network обеспечивает полноценную работу Защиты от вредоносного ПО 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 Защита от вредоносного ПО 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.

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.

Обмен информацией с Google Analytics для Firebase, 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, Firebase Performance Monitoring и Crashlytics для улучшения качества, внешнего вида и производительности программного обеспечения, продуктов, сервисов и инфраструктуры "Лаборатории Касперского" по результатам анализа работы пользователей, функций, статуса и используемых настроек устройств.

Обмен информацией с сервисами Google Analytics для Firebase, 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.

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 базы вредоносного ПО 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.

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).

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**.

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.

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*.

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.

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 баз вредоносного ПО (объем трафика может отличаться из-за размера баз вредоносного ПО), МБ	0.04	2.21	2.25
Синхронизация мобильного устройства с Kaspersky Security Center, МБ	0.03	0.02	0.05
Регулярное обновление баз вредоносного ПО (объем трафика может отличаться из-за размера баз вредоносного ПО), 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

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием Kaspersky Secure Mobility Management.

О Лицензионном соглашении

Лицензионное соглашение – это юридически обязывающее соглашение между вами и АО "Лаборатория Касперского", в котором определены условия использования Kaspersky Secure Mobility Management.

Рекомендуется внимательно ознакомиться с условиями Лицензионного соглашения перед началом работы с Kaspersky Secure Mobility Management.

Условия и положения Лицензионного соглашения можно посмотреть следующими способами:

- Во время установки компонентов Kaspersky Secure Mobility Management.
- 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 Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки компонентов Kaspersky Secure Mobility Management. Если вы не согласны с условиями Лицензионного соглашения, следует прервать установку компонентов Kaspersky Secure Mobility Management и отказаться от их использования.

О лицензии

Лицензия - это ограниченное по времени право на использование Kaspersky Secure Mobility Management, предоставляемое в соответствии с условиями подписанного Лицензионного соглашения с конечным пользователем.

Объем предоставляемых услуг и срок использования программы зависят от лицензии, по которой используется программа.

Предусмотрены следующие типы лицензий:

- *Пробная*

  Бесплатная лицензия, предназначенная для ознакомления с Kaspersky Secure Mobility Management.

  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*

  Платная лицензия.

  По истечении срока действия коммерческой лицензии мобильные приложения продолжают работу, но с ограниченной функциональностью.

  В режиме ограниченной функциональности в зависимости от приложения доступны следующие компоненты:

  - Приложение Kaspersky Endpoint Security для Android:
    - Защита от вредоносного ПО. Доступна постоянная защита и поиск вредоносного ПО на устройстве, но не доступно обновление баз вредоносного ПО.
    - 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, Firebase Performance Monitoring и Crashlytics в случае блокировки ключа, выданного "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 мобильных приложений недоступны пользователю устройства. Вы можете использовать групповые политики для управления этими компонентами в режиме ограниченной функциональности, но настроить другие компоненты приложений 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.

О подписке

Подписка на Kaspersky Secure Mobility Management – это заказ на использование мобильного приложения с выбранными параметрами (дата окончания подписки, количество защищаемых мобильных устройств). Подписку на Kaspersky Secure Mobility Management можно заказать 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 использования Kaspersky Secure Mobility Management 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 Secure Mobility Management 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 Secure Mobility Management.

О лицензионном ключе

Лицензионный ключ – последовательность битов, с помощью которой вы можете активировать и затем использовать комплексное решение Kaspersky Secure Mobility Management в соответствии с условиями Лицензионного соглашения. Лицензионные ключи создаются специалистами "Лаборатории Касперского".

Вы можете добавить лицензионный 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. Лицензионный ключ отображается в интерфейсе Kaspersky Security Center и интерфейсе мобильного приложения для Android в виде уникальной буквенно-цифровой последовательности.

  После добавления лицензионных 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. Лицензионный ключ отображается в интерфейсе мобильного приложения в виде уникальной буквенно-цифровой последовательности.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если, например, условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, мобильное приложение прекращает выполнять все свои функции, кроме синхронизации с Сервером администрирования. Чтобы продолжить использование приложения, вам нужно добавить другой лицензионный ключ.

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 Secure Mobility Management или после заказа пробной версии Kaspersky Secure Mobility Management.

Чтобы активировать приложение с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Если код активации был потерян после активации мобильного приложения, вы можете восстановить код активации. Вам может потребоваться код активации, например, для регистрации в Kaspersky CompanyAccount. Для восстановления кода активации требуется обратиться в Службу технической поддержки "Лаборатории Касперского".

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления ключа, активирующего 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 Secure Mobility Management или после заказа пробной версии Kaspersky Secure Mobility Management.

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.

Предоставление данных в Kaspersky Endpoint Security для Android

Kaspersky Secure Mobility Management соответствует требованиям Общего регламента по защите 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:

- **Защита от вредоносного ПО.** 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 базы вредоносного ПО, но уже содержится в KSN. Облачная служба Kaspersky Security Network обеспечивает полноценную работу Защиты от вредоносного ПО 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 Защита от вредоносного ПО 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 базах вредоносного ПО; временная метка сработавшей записи в базах вредоносного ПО; тип сработавшей записи в базах вредоносного 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 в целях 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 базах вредоносного ПО; временная метка сработавшей записи в базах вредоносного ПО; тип сработавшей записи в базах вредоносного 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 компонентом Защиты от вредоносного 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 служб 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 облачной службы 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;
- 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 баз вредоносного ПО 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.

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.

Предоставление данных в Kaspersky Security для iOS

Kaspersky Secure Mobility Management соответствует требованиям Общего регламента по защите 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.

Сравнение функций решения 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 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			
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 поиска вредоносного ПО на мобильных устройствах	Доступно	Доступно	Доступно

Настройка защиты мобильных устройств	Доступно	Доступно	Доступно
Настройка обновления баз вредоносного ПО	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

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky Secure Mobility Management, обратитесь в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Secure Mobility Management.

"Лаборатория Касперского" обеспечивает поддержку Kaspersky Secure Mobility Management 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

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.

Источники информации о программе

Страница Kaspersky Secure Mobility Management на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Secure Mobility Management приведена общая информация о программе, ее возможностях и особенностях работы.

Страница Kaspersky Secure Mobility Management содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница Kaspersky Secure Mobility Management в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Secure Mobility Management в Базе знаний приведены статьи, которые содержат полезную информацию, рекомендации и ответы на распространенные вопросы о приобретении, установке и использовании программы.

В статьях Базы знаний можно найти ответы на вопросы не только о Kaspersky Secure Mobility Management, но и о других программах "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Справка

В состав справки программы входят файлы справки.

В контекстной справке для плагинов управления Kaspersky Secure Mobility Management вы можете найти информацию об окнах в Kaspersky Security Center: описание параметров Kaspersky Secure Mobility Management 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 под управлением iOS и iPadOS.

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.

KES-устройство

Мобильное устройство, подключенное к Серверу администрирования Kaspersky Security Center и управляемое через приложение Kaspersky Endpoint Security для Android.

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.

Агент администрирования

Компонент программы Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и приложениями "Лаборатории Касперского", установленными на конкретном сетевом узле (рабочей станции или сервере).

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.

Базы вредоносного ПО

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска баз вредоносного ПО. Записи в базах вредоносного ПО позволяют обнаруживать вредоносный код в проверяемых объектах. Базы вредоносного ПО формируются экспертами "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.

Виртуальный Сервер администрирования

Компонент программы Kaspersky Security Center, предназначенный для управления системой защиты сети организации-клиента.

Виртуальный Сервер администрирования является частным случаем подчиненного Сервера администрирования и, по сравнению с физическим Сервером администрирования, имеет следующие основные ограничения:

- Виртуальный Сервер администрирования может функционировать только в составе главного Сервера администрирования.
- Виртуальный Сервер администрирования при работе использует основную базу данных главного Сервера администрирования. Задачи резервного копирования и восстановления данных, а также задачи проверки и загрузки обновлений, не поддерживаются на виртуальном Сервере администрирования.

- Для виртуального Сервера не поддерживается создание подчиненных Серверов администрирования (в том числе и виртуальных).

Вредоносное ПО

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 вредоносным программным обеспечением – 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, базы вредоносного ПО 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

Устройство под управлением iOS или iPadOS, параметры которого контролируются в Apple Configurator – программе для групповой настройки устройств под управлением iOS или iPadOS. 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.

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.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe, Flash и PostScript являются либо зарегистрированными товарными знаками, либо товарными знаками компании Adobe в США и/или других странах.

AMD64 – товарный знак или зарегистрированный товарный знак Advanced Micro Devices, Inc.

Amazon, Amazon EC2, Amazon Web Services, AWS и AWS Marketplace являются товарными знаками Amazon.com, Inc. или аффилированных лиц компании.

Apache является либо зарегистрированным товарным знаком, либо товарным знаком Apache Software Foundation.

Apple, Apple Configurator, AirDrop, AirPlay, AirPort, AirPort Express, AirPrint, Aperture, App Store, Apple Music, Apple TV, Apple Watch, AppleScript, Bonjour, Face ID, FaceTime, FileVault, Find My, Find My Friends, Handoff, iBeacon, iBooks, iBooks Store, iCal, iCloud, iCloud Keychain, iMessage, iPad, iPadOS, iPhone, iPhoto, iTunes, iTunes Store, iTunes U, Keychain, macOS, 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.

F5 – товарный знак F5 Networks, Inc. в США и в некоторых других странах.

Google, Android, Chrome, Chromebook, Chromium, Crashlytics, Firebase, Gmail, Google Analytics, Google Assistant, Google Chrome, Google Mail, Google Maps, Google Mobile, Google Play, Google Safe Browsing, Google SafeSearch, Google Translate, Nexus, SPDY и YouTube – товарные знаки Google LLC.

HTC – товарный знак HTC Corporation.

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, Forefront, Microsoft Intune, Outlook, Tahoma, Windows, Windows Mobile, Windows Phone и Windows Server являются товарными знаками группы компаний Microsoft.

MOTOROLA и стилизованный логотип M являются зарегистрированными товарными знаками Motorola Trademark Holdings, LLC.

Mozilla и Firefox являются товарными знаками Mozilla Foundation в США и других странах.

OPPO является товарным знаком или зарегистрированным товарным знаком компании Guangdong OPPO Mobile Telecommunications Co., Ltd.

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 – товарные знаки SOTI Inc., зарегистрированные в США и других юрисдикциях.

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 – зарегистрированные товарные знаки и/или товарные знаки VMware, Inc. в США и других странах.