kaspersky

# Kaspersky Secure Mobility Management

© 2025 АО "Лаборатория Касперского"

# Содержание


Справка Kaspersky Secure Mobility Management

Что нового

Работа в Kaspersky Security Center Web Console

- О Kaspersky Secure Mobility Management
  - Комплект поставки
  - О приложении Kaspersky Endpoint Security для Android
  - О приложении Kaspersky Protection для iOS
  - О Kaspersky Mobile Devices Protection and Management
  - Аппаратные и программные требования
  - Известные проблемы и рекомендации
- Начало работы
  - Архитектура решения
  - Сценарии развертывания
  - Развертывание решения для управления мобильными устройствами в Kaspersky Security Center Web Console
    - Развертывание Kaspersky Security Center Linux и Kaspersky Security Center Web Console
    - Развертывание плагинов для управления мобильными устройствами
    - Настройка параметров Сервера администрирования для подключения мобильных устройств
      - Сценарий: Настройка шлюза соединения для подключения мобильных устройств к Kaspersky Security Center Web Console
      - Добавление инсталляционных пакетов в хранилище Сервера администрирования
      - Добавление лицензионного ключа в хранилище Сервера администрирования
      - Установка Агента администрирования для Linux
      - Настройка параметров Веб-сервера Kaspersky Security Center Linux
        - Настройка Веб-сервера на шлюзе соединения (Агент администрирования для Linux)
        - Передача на устройства сертификата Веб-сервера на шлюзе соединения
    - Перенос данных из Kaspersky Security Center Windows в Kaspersky Security Center Linux
      - Резервное копирование и восстановление данных Сервера администрирования с помощью утилиты klbackup
        - Создание резервной копии данных Сервера администрирования на устройстве Windows
        - Восстановление данных Сервера администрирования на устройстве Linux
      - Резервное копирование и восстановление данных Сервера iOS MDM с помощью утилиты kliosbackup
  - Развертывание системы управления iOS-устройствами
    - О режимах работы iOS-устройств
    - Об управляющих профилях
    - Развертывание Kaspersky Protection для iOS
      - О Kaspersky Protection для iOS
      - Активация Kaspersky Protection для iOS
    - Развертывание системы управления по протоколу iOS MDM
      - Развертывание Сервера iOS MDM
        - Настройка инсталляционного пакета Сервера iOS MDM
        - Установка Сервера iOS MDM с помощью задачи удаленной установки
        - Локальная установка Сервера iOS MDM на устройстве с помощью инсталляционного пакета
        - Обновление Сервера iOS MDM с помощью задачи удаленной установки или локально
        - Удаление Сервера iOS MDM с помощью задачи удаленной деинсталляции

Просмотр списка установленных Серверов iOS MDM и настройка их параметров
Настройка сертификата Сервера iOS MDM
Настройка резервного сертификата Сервера iOS MDM
Получение или обновление APNs-сертификата
Установка APNs-сертификата на Сервер iOS MDM
Настройка доступа к сервису Apple Push Notification
События Сервера iOS MDM
Получение диагностических данных Сервера iOS MDM
Развертывание системы управления Android-устройствами
О режимах работы Android-устройств
Использование Firebase Cloud Messaging
Развертывание Kaspersky Endpoint Security для Android
О приложении Kaspersky Endpoint Security для Android
Установка Kaspersky Endpoint Security для Android
Создание инсталляционного пакета Kaspersky Endpoint Security для Android
Установка Kaspersky Endpoint Security для Android вручную
Установка Kaspersky Endpoint Security для Android на корпоративные устройства в закрытой сети
Разрешения для Kaspersky Endpoint Security для Android
Запуск и остановка Kaspersky Endpoint Security для Android
Активация Kaspersky Endpoint Security для Android
Обновление Kaspersky Endpoint Security для Android
Удаление Kaspersky Endpoint Security для Android
Разрешение пользователям удалять Kaspersky Endpoint Security для Android
Удаление Kaspersky Endpoint Security для Android пользователем
Дистанционное удаление Kaspersky Endpoint Security для Android с корпоративных устройств
Управление мобильными устройствами в Kaspersky Security Center Web Console
Создание групп администрирования
Настройка политик
Создание политики
Изменение политики
Копирование политики
Перенос политики в другую группу администрирования
Просмотр списка политик
Просмотр результатов применения политики
Работа с ревизиями политик
Ограничение прав на настройку политик
Настройка управления доступом на основе ролей
Настройка профилей политик
Удаление политики
Подключение мобильных устройств к Kaspersky Security Center Web Console
Прямое подключение Android-устройств к Kaspersky Security Center
Перемещение нераспределенных мобильных устройств в группы администрирования
Действия на мобильных устройствах для подключения к Серверу администрирования
Настройка параметров синхронизации
Управление сертификатами мобильных устройств
Перевыпуск мобильного сертификата Сервера администрирования
Настройка правил выпуска сертификатов

- Выпуск сертификатов для мобильных устройств
- Обновление сертификатов мобильных устройств
- Удаление сертификатов мобильных устройств
- Интеграция с инфраструктурой открытых ключей
- Просмотр списка сертификатов мобильных устройств

Настройка и управление

- Контроль
  - Настройка ограничений
    - Настройка ограничений для личных Android-устройств
    - Настройка ограничений для iOS MDM-устройств
  - Настройка доступа пользователей к сайтам
    - Настройка доступа к сайтам на Android-устройствах
    - Настройка доступа к сайтам на iOS MDM-устройствах
  - Контроль соответствия
    - Контроль соответствия Android-устройств
    - Контроль соответствия iOS MDM-устройств
  - Контроль приложений
    - Контроль приложений на Android-устройствах
    - Контроль приложений на iOS MDM-устройствах
  - Уровни защиты мобильных устройств
  - Инвентаризация программного обеспечения на Android-устройствах
- 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
  - Настройка надежности пароля разблокировки устройства
    - Настройка надежности пароля разблокировки Android-устройства
    - Настройка надежности пароля разблокировки iOS MDM-устройства
  - Настройка виртуальной частной сети (VPN)
    - Настройка VPN на Android-устройствах (только Samsung)
    - Настройка VPN на iOS MDM-устройствах
    - Настройка Per App VPN для системных приложений для iOS
    - Настройка Per App VPN для сторонних приложений для iOS
  - Настройка Сетевого экрана на Android-устройствах (только Samsung)
  - Защита Kaspersky Endpoint Security для Android от удаления
  - Обнаружение взлома устройств
  - 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
  - Удаленный доступ к Android-устройствам
    - Установка и настройка TURN-сервера
    - Настройка сервера удаленного управления в Kaspersky Security Center
    - Запуск сессии удаленного управления

- Управление Android-устройствами
  - Корпоративные устройства
    - Ограничение функций Android на устройствах
    - Настройка режима киоска для Android-устройств
    - Подключение к NDES/SCEP-серверу
  - Включение проверки подлинности на основе сертификатов устройств
  - Создание пакета мобильного приложения для Android-устройств
  - Отправка файлов на Android-устройства
  - Просмотр информации об Android-устройстве
  - Отключение Android-устройства от управления
- Управление iOS MDM-устройствами
  - Подписание управляющих профилей сертификатом
  - Добавление конфигурационного профиля
  - Установка конфигурационного профиля на устройство
  - Удаление конфигурационного профиля с устройства
  - Настройка управляемых приложений
  - Установка приложения на мобильное устройство
  - Обновление приложения, установленного на устройстве
  - Удаление приложения с устройства
  - Настройка роуминга на iOS MDM-устройстве
  - Просмотр информации об iOS MDM-устройстве
  - Отключение iOS MDM-устройства 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
  - Настройка уровней защиты 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
  - Выбор загрузчика для Android-устройств
  - Подключение iOS MDM-устройств к AirPlay
  - Подключение iOS MDM-устройств к AirPrint
  - Настройка точки доступа (APN)
    - Настройка APN на Android-устройствах (только Samsung)
    - Настройка APN на iOS MDM-устройствах

Корпоративный контейнер
О корпоративных контейнерах
Настройка корпоративного контейнера
Разблокировка корпоративного контейнера
Добавление учетной записи LDAP
Добавление учетной записи контактов
Добавление учетной записи календаря
Настройка подписки на календарь
Настройка единого входа
Управление веб-клипами
Установка обоев
Добавление шрифтов
Работа с командами для мобильных устройств
Команды для мобильных устройств
Отправка команд
Просмотр статусов команд в истории команд
Управление приложением с помощью сторонних EMM-решений (только Android)
Начало работы
Как установить приложение
Защита устройств в интернете
Как активировать приложение
Как подключить устройство к Kaspersky Security Center
Тихий режим
Файл AppConfig
Участие в Kaspersky Security Network
Обмен информацией с Kaspersky Security Network
Включение и выключение использования Kaspersky Security Network
Использование Kaspersky Private Security Network
Samsung Knox
Установка приложения Kaspersky Endpoint Security для Android с помощью Knox Mobile Enrollment
Создание профиля Knox
Добавление устройств в Knox Mobile Enrollment
Установка приложения
Настройка Knox
Настройка ограничений на использование SD-карт в Knox
Настройка VPN в Knox
Настройка почтового ящика Exchange в Knox
Настройка APN в Knox
Настройка Сетевого экрана в Knox
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-Защита
- Получение сертификата
- Синхронизация с Kaspersky Security Center
- Предоставление удаленного доступа к вашему устройству
- Активация Kaspersky Endpoint Security для Android без использования Kaspersky Security Center
- Установка приложения на корпоративные устройства
  - Настройка приложения на корпоративных устройствах с Android 7 или выше
  - Настройка приложения на корпоративных устройствах с Android 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 Protection для iOS
- Возможности приложения
- Установка приложения
- Активация приложения
- Активация приложения с помощью кода активации
- Обзор главного окна
- Обновление приложения
- Использование диагностики для устранения неисправностей
- Удаление приложения

Лицензирование программы
- О Лицензионном соглашении
- О лицензии
- Просмотр информации 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 Protection для iOS

Сравнение функций решения в зависимости от средства 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 profile
- iOS MDM-устройство
- Kaspersky Private Security Network (KPSN)

Kaspersky Security Center Web Server
Kaspersky Security Network (KSN)
Manifest-файл
POP3
SSL
Автономный пакет установки
Агент администрирования
Администратор Kaspersky Security Center
Администратор устройства
Активация программы
Базовая защита
Базовый контроль
Базы вредоносного ПО
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
Корпоративное устройство
Корпоративный контейнер
Лицензионное соглашение
Лицензия
Личное устройство
Плагин для управления мобильными устройствами
Подписка
Политика
Прокси-сервер
Рабочее место администратора
Рабочий профиль Android
Сервер iOS MDM
Сервер администрирования
Серверы обновлений "Лаборатории Касперского"
Срок действия лицензии
Управляющий профиль
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.

**Комплект поставки**

Узнайте о компонентах, доступных в вашей версии решения.

**Развертывание**

Узнайте, как развернуть решение в вашей организации и настроить системы управления для Android-устройств и iOS-устройств.

**Команды**

Управляйте мобильными устройствами удаленно с помощью команд: Заблокировать устройство, Удалить корпоративные данные, Определить местоположение, Сделать фотографии, Воспроизвести звуковой сигнал и других.

**Корпоративный контейнер**

Настройте корпоративный контейнер на своем устройстве и пользуйтесь его преимуществами.

**Корпоративный каталог приложений**

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

**Настройка защиты устройств**

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

**Изменение параметров устройства**

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

**Настройка контроля устройств**

Отслеживайте мобильные устройства удаленно, в том числе настраивайте ограничения, доступ пользователей к сайтам, Контроль соответствия, Контроль приложений и другие функции.

**Настройка корпоративных устройств**

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

**Другое**

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

# Что нового

## Версия 8.0

В этой версии мы добавили новые функции в плагин Kaspersky Mobile Devices Protection and Management для Kaspersky Security Center Linux Web Console:

- Теперь Kaspersky Security Center Web Console позволяет удаленно подключаться к Android-устройствам через приложение Kaspersky Endpoint Security для Android, установленное на устройстве. После начала сессии удаленного управления вы сможете просматривать экран устройства, делать снимки экрана и выполнять действия на устройстве.

- Добавлена поддержка новых протоколов шифрования для защиты сетей Wi-Fi на Android-устройствах:

  - WPA3 PSK

  - WPA3-Enterprise

  - WPA3-Enterprise 192-бит

- Добавлена поддержка новых команд для Android-устройств:

  - Перезагрузить устройство

  - Сбросить пароль

- Теперь вы можете настроить, чтобы приложение Kaspersky Endpoint Security для Android переключалось на использование публичных серверов Kaspersky Security Network при недоступности прокси-сервера KSN. Это обеспечивает непрерывную работу следующих компонентов: Защита от вредоносного ПО, Веб-Защита, Веб-Контроль и Контроль приложений.

# Работа в Kaspersky Security Center Web Console

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

# 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.

## Комплект поставки

В комплект поставки Kaspersky Secure Mobility Management могут входить различные компоненты в зависимости от выбранной версии решения. Подробную информацию о совместимости версии плагина с версиями Kaspersky Security Center смотрите в аппаратных и программных требованиях.

### Управление мобильными устройствами в Kaspersky Security Center Web Console

Этот компонент совместим с Kaspersky Security Center Linux 15.1. Подробную информацию о версии, совместимой с Kaspersky Security Center Windows, см. в справке Kaspersky Secure Mobility Management 4.1.

- `on_prem_ksm_policies_<версия>.zip`

  Архив, содержащий файлы, необходимые для установки плагина Kaspersky Mobile Devices Protection and Management:

  - `plugin.zip`

    Архив, содержащий плагин Kaspersky Mobile Devices Protection and Management.

  - `signature.txt`

    Файл, содержащий подпись для плагина Kaspersky Mobile Devices Protection and Management.

## Плагин параметров Сервера iOS MDM

Этот компонент совместим с Kaspersky Security Center Linux 15.1. Подробную информацию о версии, совместимой с Kaspersky Security Center Windows, см. в справке Kaspersky Secure Mobility Management 4.1.

- `on_prem_iosmdm_<версия>.zip`

  Архив, содержащий файлы, необходимые для установки плагина параметров Сервера iOS MDM:

  - `plugin.zip`

    Архив, содержащий плагин параметров Сервера iOS MDM.

  - `signature.txt`

    Файл, содержащий подпись для плагина параметров Сервера iOS MDM.

## Сервер iOS MDM

Этот компонент совместим с Kaspersky Security Center Linux 15.1. Подробную информацию о версии, совместимой с Kaspersky Security Center Windows, см. в справке Kaspersky Secure Mobility Management 4.1.

- `kliosmdm-<архитектура>-<версия>-<менеджер пакетов>_<язык>.tar.gz`

  Архив, содержащий файлы, необходимые для установки Сервера iOS MDM, в зависимости от менеджера пакетов и архитектуры:

  - `kliosmdm.kpd`

    Файл, содержащий описание Сервера iOS MDM.

  - `akinstall.sh`

    Скрипт, позволяющий автоматизировать установку Сервера iOS MDM.

  - `kliosmdm-<версия>.<архитектура>.rpm` или `kliosmdm_<версия>_<архитектура>.deb`

    Инсталляционный пакет Сервера iOS MDM.

  - `kpd.loc/`

    Папка с CFG-файлами, определяющими пути к Лицензионным соглашениям.

  - `license/`

    Папка с Лицензионными соглашениями и Политикой конфиденциальности на разных языках в формате TXT.

## Приложение Kaspersky Endpoint Security для Android

- `<версия>_sc_package.zip`

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

- `installer.ini`

  Конфигурационный файл с параметрами подключения к Серверу администрирования.

- `kesandroid<версия>_<языки>_Prod_Release.apk`

  Пакетный файл Android для приложения Kaspersky Endpoint Security для Android.

- `eula/`

  Папка с Лицензионными соглашениями на разных языках в формате TXT.

- `kpd.loc/`

  INI-файлы, определяющие пути к Лицензионным соглашениям.

- `ksm.kpd`

  Файл, содержащий описание программы.

### Файл Корпоративного каталога приложений

`Install_<версия>.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*.

### 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**. 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 или 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:
  - **Определить местоположение**. Получение координат местоположения устройства.
  - **Воспроизвести звуковой сигнал**. Устройство издает громкий сигнал тревоги.
  - **Удалить корпоративные данные**. Удаление корпоративных данных, чтобы защитить конфиденциальную информацию компании.
- **Веб-Защита** и **Веб-Контроль**. Веб-Защита блокирует вредоносные сайты, цель которых – распространить вредоносный код. Веб-Защита также блокирует поддельные (фишинговые) сайты, цель которых – украсть конфиденциальные данные пользователя (например, пароли от интернет-банка или платежных систем) и получить доступ к его финансовым счетам. Веб-Защита проверяет сайты перед открытием, используя облачную службу Kaspersky Security Network. По результатам проверки Веб-Защита разрешает загрузку сайтов, признанных надежными, и блокирует сайты, признанные вредоносными. Веб-Контроль поддерживает фильтрацию сайтов по категориям, определенным в облачной службе Kaspersky Security Network. Это позволяет администратору ограничить доступ пользователей к некоторым категориям веб-страниц (например, "Азартные игры, лотереи, тотализаторы" или "Общение в сети").
- **Контроль приложений**. Позволяет устанавливать рекомендуемые и обязательные приложения на Android-устройство, а также удалять заблокированные приложения, нарушающие требования корпоративной безопасности.
- **Контроль соответствия**. 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, задав соответствующие параметры политик.

На личных устройствах и устройствах с корпоративным контейнером под управлением Android 15 пользователи могут создать частное пространство. Kaspersky Endpoint Security для Android не может сканировать приложения, фотографии и другие файлы, хранящиеся в частном пространстве. Веб-Защита, Веб-Контроль и Контроль приложений не работают для приложений, установленных в частном пространстве. Kaspersky Endpoint Security для Android нельзя установить в частном пространстве.

# О приложении Kaspersky Protection для iOS

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

Kaspersky Protection для iOS предоставляет следующие ключевые функции:

- **Веб-Защита**. Позволяет блокировать вредоносные сайты, цель которых – распространить вредоносный код. Веб-Защита также блокирует поддельные (фишинговые) сайты, цель которых – украсть конфиденциальные данные пользователя (например, пароли от интернет-банка или платежных систем) и получить доступ к его финансовым счетам. Веб-Защита проверяет сайты перед открытием, используя облачную службу Kaspersky Security Network. По результатам проверки Веб-Защита разрешает загрузку сайтов, признанных надежными, и блокирует сайты, признанные вредоносными. Вы можете настроить этот компонент в Kaspersky Security Center Web Console, определив настройки групповых политик.

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

# О Kaspersky Mobile Devices Protection and Management

Плагин Kaspersky Mobile Devices Protection and Management позволяет управлять мобильными устройствами и установленными на них приложениями в Kaspersky Security Center Web Console. С помощью плагина Kaspersky Mobile Devices Protection вы можете:

- 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 приложения Kaspersky Endpoint Security для Android на мобильных устройствах пользователей;

- удаленно настраивать iOS-устройства, подключенные по протоколу iOS MDM (далее "iOS MDM-устройства") и iOS-устройства, на которых установлено приложение Kaspersky Protection для iOS;

- удаленно настраивать устройства под управлением ОС Аврора, на которых установлено приложение Kaspersky Endpoint Security для ОС Аврора.

Плагин Kaspersky Mobile Devices Protection and Management можно установить во время настройки Kaspersky Security Center Web Console. Дополнительная информация о сценариях развертывания приведена в разделе Развертывание плагинов управления мобильными устройствами.

# 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

Хост сервера Kaspersky Security Center Linux должен удовлетворять следующим требованиям:

- Программные требования:
  - Сервер администрирования Kaspersky Security Center Linux 15.2 или выше;
  - Web Console Kaspersky Security Center Linux 15.2 или выше;
  - плагин Kaspersky Mobile Devices Protection and Management 10.53 или выше;
  - Сервер iOS MDM для Linux 15.2 или выше;
  - плагин параметров Сервера iOS MDM 15.2 или выше.
- Аппаратные требования:
  - Для развертывания Kaspersky Secure Mobility Management должны удовлетворяться аппаратные требования Kaspersky Security Center.
  - Для Сервера iOS MDM:
    - процессор с частотой 1 ГГц или выше; для 64-разрядных операционных систем – 1,4 ГГц или выше;
    - 4 ГБ оперативной памяти;
    - 4 ГБ свободного места на диске.

## Совместимость версий

Поддерживаются следующие комбинации версий:

- Плагин Kaspersky Mobile Devices Protection and Management версии 10.53 поддерживает только Kaspersky Security Center Linux 15.1 или выше.
- Плагин Kaspersky Mobile Devices Protection and Management версии 10.54 или выше поддерживает только Kaspersky Security Center Linux 15.2 или выше.

Полная совместимость обеспечивается между следующими версиями:

- Плагин Kaspersky Mobile Devices Protection and Management 10.53 и Kaspersky Security Center Linux 15.1 или выше.
- Плагин Kaspersky Mobile Devices Protection and Management версии 10.54 поддерживает только Kaspersky Security Center Linux 15.2 или выше.
- Плагин Kaspersky Mobile Devices Protection and Management версии 10.55 поддерживает только Kaspersky Security Center Linux 15.3 или выше.
- Плагин Kaspersky Mobile Devices Protection and Management версии 10.56 поддерживает только Kaspersky Security Center Linux 16.1 или выше.

## Совместимость со сторонними EMM-системами

Приложение Kaspersky Endpoint Security для Android может работать в составе сторонних EMM-систем:

- VMware AirWatch 9.3 или выше;
- MobileIron 10.0 или выше;
- IBM MaaS360 10.68 или выше;
- Microsoft Intune 1908 или выше;
- SOTI MobiControl 14.1.4 (1693) или выше.

## Аппаратные и программные требования Kaspersky Endpoint Security для Android

Для установки Kaspersky Endpoint Security для Android мобильное устройство должно удовлетворять следующим требованиям:

- смартфон или планшет с разрешением экрана от 320x480 пикселей;
- 65 МБ свободного места в основной памяти устройства;
- Android 5 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 Kaspersky Protection для iOS

Для установки Kaspersky Protection для iOS мобильное устройство должно удовлетворять следующим требованиям:

- iOS 15 или выше / iPadOS 15 или выше;
- подключение к интернету.

## Аппаратные и программные требования к мобильному устройству пользователя для управляющего профиля

Для установки управляющего профиля мобильное устройство должно удовлетворять следующим требованиям:

- iOS 10 или выше / iPadOS 13 или выше;
- подключение к интернету.

# Известные проблемы и рекомендации

Следующие известные проблемы не являются критичными для работы решения.

## Известные проблемы при подключении мобильных устройств к Kaspersky Security Center

- Если в качестве HTTPS-порта Веб-сервера используется порт 8061, ссылка для подключения мобильных устройств или ссылка на скачивание инсталляционного пакета могут не открыться в одном браузере с Kaspersky Security Center Web Console из-за ошибки `NET::ERR_CERT_AUTHORITY_INVALID`. Так происходит, если Веб-сервер использует самоподписанный сертификат. Чтобы открыть ссылку, скопируйте и вставьте ее в другой браузер, либо замените самоподписанный сертификат на пользовательский, выпущенный доверенным центром сертификации. Заменить сертификат можно в свойствах Сервера администрирования на вкладке **Общие** в разделе **Веб-сервер**.

## 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.

- Мобильные устройства не поддерживают кнопку **Синхронизировать сейчас** и флажок **Не разрывать соединение с Сервером администрирования** в окне свойств устройства. Используйте команду **Синхронизировать устройство**, чтобы принудительно синхронизировать Android-устройство или iOS MDM-устройство.

- В списке управляемых мобильных устройств общий объем хранилища личных iOS устройства в режиме базовой защиты отображается с округлением в большую сторону.

## Известные проблемы Kaspersky Protection для iOS

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

- Для стабильной работы приложения Kaspersky Protection для iOS необходимо удалить с устройства устаревшее приложение Kaspersky Security для iOS.

- Фоновые задачи (например, синхронизация с Kaspersky Security Center или замена ключа активации на новый) на некоторых iOS-устройствах могут выполняться позже, чем ожидается, если пользователь закрыл Kaspersky Protection для iOS смахиванием из переключателя приложений. Это связано с ограничениями iOS на выполнение в фоновом режиме. Чтобы принудительно запустить выполнение, откройте приложение повторно.

  Соблюдение следующих условий увеличит шансы на выполнение фоновых задач:

  - Приложение Kaspersky Protection для iOS открыто в переключателе приложений.
  - Режим экономии данных выключен и устройство подключено к Wi-Fi сети или точке доступа.
  - Устройство подключено к сети с высоким качеством связи.

- Устройство заряжается.
- Режим модема выключен.

## Известные проблемы при установке Kaspersky Endpoint Security для Android

- Kaspersky Endpoint Security для Android устанавливается только в основную память устройства.
- На устройствах под управлением Android 7 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 или 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) без подключения к Kaspersky Security Center 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).
- При установке Kaspersky Endpoint Security для Android на корпоративное устройство с помощью ADB, если вы установили пароль разблокировки экрана на устройстве после сброса его до заводских настроек, нужно снова сбросить устройство до заводских настроек перед установкой приложения с помощью ADB.

## Известные проблемы при обновлении Kaspersky Endpoint Security для Android

- 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 при удалении Kaspersky Endpoint Security для Android

- 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, связанные с Wi-Fi

- На iOS MDM-устройствах, если вы выключите автоматическое подключение к уже добавленной сети Wi-Fi в параметрах политики, вы не сможете снова включить автоматическое подключение к этой сети. Это связано с проблемой, известной Apple.

- iOS MDM-устройства под управлением iOS 18 и iOS 26 могут не подключиться автоматически к Wi-Fi сетям с протоколом шифрования WEP, WPA или WPA3, если в параметрах Wi-Fi политики выбран тип защиты сети **Личная сеть (любой тип)**, несмотря на то что установлен флажок **Подключаться автоматически**. Для автоматического подключения к Wi-Fi сети с нужным протоколом шифрования укажите этот протокол в качестве типа защиты сети.

## Известные проблемы при настройке VPN

- Если на iOS MDM-устройстве установить приложение с настроенным Per App VPN, затем выключить VPN в политике и синхронизировать это устройство, то в информации о конфигурационном профиле все равно может отображаться сообщение "Приложение будет использовать VPN для подключения к сети". Для актуальной информации о приложении обновите или переустановите его.

## 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 дальнейшей 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 или выше пользователю необходимо предоставить разрешение "Разрешить доступ на управление всеми файлами".

- На устройствах под управлением Android 7 или 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-Защиты и Веб-Контроля

- Веб-Контроль 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 Browser и Яндекс Браузер Веб-Контроль не блокирует сайты на мобильном устройстве, если используется корпоративный контейнер и Веб-Защита включена только в корпоративном контейнере.

- Для работы Веб-Защиты и Веб-Контроля требуется включить использование Kaspersky Security Network. Веб-Контроль 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-Контролем, 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, если пользователь открывает их в фоновом режиме из контекстного меню или из сторонних приложений, например, из приложения IM-клиента.

- Для работы Веб-Защиты и Веб-Контроля Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей.

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

- Разрешенные веб-сайты могут блокироваться в браузере Samsung Internet в режиме Веб-Контроля **Разрешить только указанные 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-Контроля выбран режим **Запретить все сайты**, то Kaspersky Endpoint Security для Android не блокирует поиск в виджете Google Поиск. Вместо этого блокируется доступ к результатам поиска.

- Если в корпоративном контейнере для Веб-Контроля выбран режим **Запретить все сайты**, то Kaspersky Endpoint Security для Android постоянно перезагружает главную страницу Google Chrome, блокирует браузер и мешает работе устройства.

- В Яндекс Браузере и Samsung Internet вредоносные и фишинговые веб-адреса могут оставаться незаблокированными. Это связано с тем, что проверяется только домен сайта. Если он является вредоносным или фишинговым, Веб-Защита блокирует угрозу. Если домен не был классифицирован как вредоносный или фишинговый, конкретный веб-адрес не блокируется.

- Список разрешенных сайтов, созданный в карточке **Веб-Контроль**, не отображается в Safari на iOS MDM-устройствах под управлением iOS 26 или ниже. Тем не менее, Веб-Контроль продолжает работать, и пользователи могут получить доступ только к разрешенным сайтам. Чтобы разрешенные сайты отобразились в Safari, установите флажок **Добавить в закладки на устройстве** в карточке **Веб-Контроль** и укажите название закладки для каждого сайта из списка.

- Если в разделе "Веб-Контроль" параметров политики включен параметр **Проверять полный веб-адрес при использовании Custom Tabs**, переход в полную версию поддерживаемых браузеров работает только для фишинговых и вредоносных сайтов.

- На iOS-устройствах, работающих в режиме базовая защита, при смене языка на устройстве или перезагрузке устройства выключается Веб-Защита. Чтобы включить Веб-Защиту, подождите около минуты после смены языка или перезагрузки устройства и откройте Kaspersky Protection 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 7 или 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 или 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. Это не относится к корпоративным устройствам.

- 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 проблемам 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.

- При настройке корпоративного контейнера на устройстве рекомендуется снимать флажок **Блокировать системные приложения**. Блокировка системных приложений может привести к проблемам при создании корпоративного контейнера.

- Если установлен флажок **Блокировать системные приложения**, то в числе системных приложений может быть заблокирован системный механизм запроса разрешений для приложений. Чтобы снять блокировку с этого механизма, найдите его имя (например, `com.google.android.permissioncontroller`) в журнале событий и добавьте его в исключения.

- На некоторых Android-устройствах обязательные приложения не будут загружены, пока пользователь не разблокирует экран устройства.

## Известные проблемы в работе Контроля соответствия

- Если в критерии **Версия операционной системы** указана несуществующая версия, устройство обновится до последней загруженной версии.

## Известные проблемы при управлении сертификатами

- Когда в разделе **Правила выпуска** включен параметр **Интегрировать выпуск сертификатов с Microsoft Certification Authority (CA) через PKI**, параметры почтового и VPN-сертификатов могут перестать быть активными на некоторое время, пока ожидается ответ от PKI.

- Вы не можете автоматически обновить почтовый или VPN-сертификат, загруженный из файла (с выключенным параметром **Интегрировать выпуск сертификатов с Microsoft Certification Authority (CA) через PKI** в разделе **Параметры PKI** раздела **Правила выпуска**), поскольку у такого сертификата нет доступа к Certification Authority (CA). Чтобы обновить сертификат, вам необходимо вручную загрузить новый файл сертификата.

- Не получится установить новый мобильный, VPN или почтовый сертификат для другого пользователя на устройство, на котором уже установлен мобильный сертификат текущего пользователя. При этом выписать новые сертификаты для текущего пользователя можно.

## Известные проблемы при настройке надежности пароля разблокировки устройства

- На устройствах под управлением Android 10 или 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 или 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 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, связанные с защитой Kaspersky Endpoint Security for Android от удаления

- Kaspersky Endpoint Security для Android должен быть установлен в качестве администратора устройства.
- На устройствах под управлением Android 7 или 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 личных устройствах и устройствах с созданным рабочим профилем под управлением Android 10 или выше запрет на использование сетей Wi-Fi не поддерживается.
- На устройствах с Android 11 или 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 iOS MDM-устройствах у пользователя может быть возможность разрешить результаты поиска Spotlight в интернете в предложениях Siri, даже если установлен флажок **Запретить предложения Spotlight**. Это связано с проблемой, известной Apple.
- 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 Android 12 или 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** завершится с ошибкой.
- Если на Android-устройстве отключена служба Google "Точность местоположения", команда **Определить местоположение** работать не будет. Обращаем внимание, что не на всех Android-устройствах есть эта служба.
- Если вы отправите команду **Включить Режим пропажи** на iOS MDM-устройство в режиме supervised без SIM-карты, и это устройство будет перезапущено, оно не сможет подключиться к сети Wi-Fi и получить команду **Выключить 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 **Выключить Режим пропажи** по мобильной сети.
- Команда **Сбросить настройки до заводских** недоступна для личных устройств и устройств с корпоративным контейнером под управлением Android 14 или выше.

- Перед выполнением команды **Сбросить пароль** экран устройства должен быть заблокирован и разблокирован хотя бы раз.

- Команда **Сбросить пароль** не может быть выполнена на корпоративном устройстве, если вы задали пароль разблокировки экрана перед установкой Kaspersky Endpoint Security для Android. Чтобы этого избежать, настройки устройства должны быть сброшены до заводских непосредственно перед установкой приложения.

## 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.

  - Если устройство было заблокировано, разблокировать устройство с помощью команды невозможно. Вы можете разблокировать устройство только с помощью одноразового кода разблокировки.

  - На устройствах под управлением Xiaomi HyperOS Kaspersky Endpoint Security для Android может не проверять уведомления от мессенджеров на наличие вредоносных и фишинговых веб-адресов.

- На некоторых устройствах (например, Meizu, Asus) под управлением Android 6 или выше после шифрования данных и перезагрузки Android-устройства 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. После этого пользовательское устройство становится незащищенным. 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 Android 7 или 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-Защита и Веб-Контроль, 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 расширенные права приложению "Недавние экраны" (Recent screens). 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 HUAWEI P60 Pro недоступно создание корпоративного контейнера.

- На некоторых iOS MDM-устройствах в режиме работы "Базовый контроль" под управлением iOS 18.2 - iOS 18.3.1 может применяться запрет на использование Safari. Это связано с проблемой, известной Apple.

- Некоторые личные устройства (например, OnePlus, Honor) под управлением Android 10 или выше могут запрашивать пароль при подключении к Wi-Fi сетям с протоколом шифрования WPA2 PSK или WPA3 PSK. Это связано с проблемами в работе API предложения Wi-Fi (Suggestion API).

- На iOS MDM-устройствах под управлением iOS 18.0 политика с настроенным AirPlay не может быть доставлена на устройство. Это связано с проблемой, известной Apple. Для корректной работы обновите iOS на устройстве.

- На некоторых устройствах во время сессии удаленного управления администратор не может выдавать системные разрешения приложениям (кроме Kaspersky Endpoint Security для Android) из-за ограничений операционной системы при включенной службе Специальных возможностей.

## 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, связанные с профилями политик

- При выборе лицензии с базовой функциональностью параметры, доступные только с лицензией с продвинутой функциональностью, не сбрасываются до значений по умолчанию в профилях политики.

## Известные проблемы, связанные с управлением доступом на основе ролей

- Если право на управление лицензионным ключом не предоставлено, при открытии уже созданной политики может возникнуть ошибка. Это не влияет на работу политики.
- Если право на управление лицензионным ключом не предоставлено, вы можете создать политику без выбора лицензии в Мастере создания политики для мобильных устройств. Однако в этом случае вы не сможете настроить параметры политики.

## Известные проблемы при настройке параметров Веб-сервера на шлюзе соединения (Network Agent Linux)

- Если при настройке параметров Веб-сервера на шлюзе соединения изменены порты или выпущены или обновлены сертификаты, синхронизация новых параметров с Kaspersky Security Center может занять некоторое время. Подождите до 15 минут или нажмите **Синхронизировать сейчас** на вкладке **Общие** свойств шлюза соединения (**Управление активами** → **Активы (Устройства)**).
- Если при настройке пользовательского сертификата Веб-сервера значения в полях **Адрес Веб-сервера** и **Адрес сертификата** не совпадают, отобразится ошибка. В этом случае для сохранения параметров вам необходимо загрузить другой сертификат. Однако если вы измените адрес Веб-сервера в свойствах точки распространения Kaspersky Security Center, оставив сертификат прежним, вы все равно сможете сохранить указанные параметры, даже если адреса не совпадают.

## Известные проблемы при переносе данных из Kaspersky Security Center Windows в Kaspersky Security Center Linux

- При переносе настроек Сервера iOS MDM с Kaspersky Security Center Windows 14.2 в Kaspersky Security Center Linux параметры уведомлений и хранения событий Сервера iOS MDM не переносятся и принимают значения по умолчанию. После переноса вам потребуется указать необходимые значения вручную.
- Если в ходе переноса данных пользователь был удален или отсутствует на сервере, мобильный сертификат отображается в списке сертификатов без имени пользователя.

## Известные проблемы, связанные с Сервером iOS MDM

- Доставка на устройство выпущенного резервного сертификата Сервера iOS MDM может занимать от 6 часов.

## Известные проблемы, связанные с прокси-сервером KSN

- Если мобильные устройства подключены к Kaspersky Security Center через шлюз соединения, прокси-сервер KSN не работает. В этом случае выключите переключатель **Включить прокси-сервер KSN на Сервере администрирования Включено** в разделе **Прокси-сервер KSN** окна свойств Сервера администрирования. Подробная информация о включении и выключении прокси-сервера KSN приведена в справке Kaspersky Security Center.

## Известные проблемы в режиме корпоративного устройства

- На корпоративных 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.

## Известные проблемы в режиме киоска

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

- На iOS MDM-устройствах под управлением iOS 26 или выше и iPadOS 26 или выше после выключения режима киоска значки приложений на главном экране могут выглядеть заблокированными, хотя приложения можно открыть. Попробуйте провести пальцем по экрану, чтобы обновить их состояние.

- На iPhone 15 или выше, если в параметрах режима киоска снят флажок **Переключатель "Звонок/Бесшумно"**, пользователь все равно может переключаться между этими режимами, используя кнопку действия.

## Известные проблемы, связанные с удаленным управлением Android-устройствами

- На некоторых устройствах передача содержимого экрана может быть прервана при блокировке экрана устройства.

- Сессии удаленного управления не устанавливаются при запуске из Яндекс Браузера. Ошибка вызвана проблемой в Яндекс Браузере и может возникнуть при первом запуске или после перезагрузки браузера или компьютера администратора. Мы рекомендуем использовать для запуска удаленных сессий другие браузеры, поддерживаемые плагином Kaspersky Mobile Protection and Management, такие как Google Chrome, Microsoft Edge, Mozilla Firefox и Safari.

- Управление приложением Kaspersky Endpoint Security for Android с помощью сторонних решений для удаленного управления мобильными устройствами может работать с ошибками.

### Известные проблемы, связанные с событиями

- При обновлении плагина Kaspersky Mobile Devices Protection and Management новые события могут отображаться некорректно в ранее созданной политике: на вкладке **Настройка событий** они выглядят включенными, однако информация о них не передается. Чтобы после обновления плагин предоставил актуальный список событий для ранее созданной политики, необходимо пересохранить эту политику.

# Начало работы

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.

- Мобильное приложение Kaspersky Protection для iOS.

  Kaspersky Protection для iOS защищает мобильные устройства от фишинга и веб-угроз и позволяет обнаруживать jailbreak на устройствах.

- Плагин Kaspersky Mobile Devices Protection and Management.

  Плагин Kaspersky Mobile Devices Protection and Management позволяет управлять устройствами на Android и iOS в Kaspersky Security Center Web Console.

- Сервер iOS MDM.

  Сервер iOS MDM позволяет подключать iOS-устройства к Серверу администрирования и управлять iOS-устройствами.

- Плагин параметров Сервера iOS MDM.

  Плагин параметров Сервера iOS MDM позволяет настраивать параметры Сервера iOS MDM.

## Сценарии развертывания

Развертывание Kaspersky Secure Mobility Management в Kaspersky Security Center Web Console состоит из следующих шагов:

1. Развертывание Kaspersky Security Center Linux и Kaspersky Security Center Web Console
2. Развертывание плагинов для управления мобильными устройствами

3. Настройка параметров Сервера администрирования для подключения мобильных устройств
4. Развертывание системы управления iOS-устройствами
5. Развертывание системы управления Android-устройствами
6. Управление мобильными устройствами в Kaspersky Security Center Web Console

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

Для подключения и управления мобильными устройствами с помощью Kaspersky Security Center Web Console необходимо развернуть решение для управления мобильными устройствами. В этом разделе описаны действия, которые вам рекомендуется выполнить при начале работы с Kaspersky Secure Mobility Management.

## Развертывание Kaspersky Security Center Linux и Kaspersky Security Center Web Console

Выберите устройство с операционной системой Linux, которое будет использовано в качестве рабочей станции администратора; убедитесь, что аппаратное и программное обеспечение устройства соответствует требованиям, и установите на это устройство Kaspersky Security Center Web Console.

Инструкции по установке Kaspersky Security Center Linux приведены в справке Kaspersky Security Center.

Инструкции по установке Kaspersky Security Center Web Console приведены в справке Kaspersky Security Center Linux.

## Развертывание плагинов для управления мобильными устройствами

Для использования решения Kaspersky Secure Mobility Management и подключения мобильных устройств необходимо добавить и установить следующие плагины:

- Плагин Kaspersky Mobile Devices Protection and Management
  - `on_prem_ksm_policies_<версия>.zip`

    Архив, содержащий файлы, необходимые для установки плагина Kaspersky Mobile Devices Protection and Management:
    - `plugin.zip`

      Архив, содержащий плагин Kaspersky Mobile Devices Protection and Management.
    - `signature.txt`

      Файл, содержащий подпись для плагина Kaspersky Mobile Devices Protection and Management.
- Плагин параметров Сервера iOS MDM
  - `on_prem_iosmdm_<версия>.zip`

Архив, содержащий файлы, необходимые для установки плагина параметров Сервера iOS MDM:

- `plugin.zip`

  Архив, содержащий плагин параметров Сервера iOS MDM.

- `signature.txt`

  Файл, содержащий подпись для плагина параметров Сервера iOS MDM.

*Чтобы установить плагин управления:*

1. В главном окне Kaspersky Security Center Web Console выберите **Параметры** > **Веб-плагины**.
2. В открывшемся окне нажмите **Добавить**.

   Отобразится список доступных плагинов.
3. В списке доступных плагинов нажмите на имя плагина, который требуется установить.

   Отобразится страница с описанием плагина.
4. На странице описания плагина нажмите **Установить плагин**.
5. После завершения установки нажмите **ОК**.

Плагин управления будет загружен в конфигурации по умолчанию и появится в списке плагинов управления.

Вы можете добавлять плагины и обновлять загруженные плагины из файла. Вы можете загрузить плагины управления с сайта Службы технической поддержки "Лаборатории Касперского".

*Чтобы загрузить или обновить плагин управления из файла:*

1. В главном окне Kaspersky Security Center Web Console выберите **Параметры** > **Веб-плагины**.
2. В открывшемся окне:
   - Нажмите **Добавить из файла**, чтобы загрузить плагин из файла.
   - Нажмите **Обновить из файла**, чтобы загрузить обновление для плагина из файла.
3. Укажите файл и подпись файла.
4. Загрузите указанные файлы.

Плагин управления будет загружен из файла и появится в списке плагинов управления.

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

Подробную информацию о совместимости версии плагина с версиями Kaspersky Security Center смотрите в аппаратных и программных требованиях.

# Настройка параметров Сервера администрирования для подключения мобильных устройств

Перед подключением мобильных устройств к Kaspersky Security Center Web Console необходимо настроить параметры подключения в свойствах Сервера администрирования.

*Чтобы настроить параметры Сервера администрирования для подключения мобильных устройств:*

1. В главном окне Kaspersky Security Center Web Console нажмите на имя Сервера администрирования.
2. В открывшемся окне свойств Сервера администрирования настройте порт Сервера администрирования, который будет использоваться для мобильных устройств:
   a. На вкладке **Общие** выберите раздел **Дополнительные порты**.
   b. Включите переключатель **Открыть порт для мобильных устройств**.
      Если этот параметр включен, порт Сервера администрирования открыт 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 **Открыть порт для мобильных устройств** выключен или порт указан неверно, мобильные устройства не смогут подключаться к Серверу администрирования.
3. При необходимости замените сертификат, используемый устройствами для подключения к Серверу администрирования.

   По умолчанию используется сертификат, созданный после открытия порта для мобильных устройств. Замените сертификат, выданный Сервером администрирования, на другой сертификат или перевыпустите его.

   Чтобы изменить сертификат:
   a. На вкладке **Общие** выберите раздел **Сертификаты**.
   b. Задайте необходимые параметры.
      Подробная информация о работе с сертификатами Kaspersky Security Center Linux приведена в справке Kaspersky Security Center.
4. Нажмите **Сохранить**, чтобы сохранить внесенные изменения и закрыть окно свойств Сервера администрирования.

Параметры для подключения мобильных устройств настроены.

## Сценарий: Настройка шлюза соединения для подключения мобильных устройств к Kaspersky Security Center Web Console

Шлюз соединения – это Агент администрирования, работающий в особом режиме. Агент администрирования является компонентом Kaspersky Security Center, который осуществляет взаимодействие между Сервером администрирования и приложениями "Лаборатории Касперского". Шлюз соединения принимает соединения от других Агентов администрирования и туннелирует их к Серверу администрирования через собственное соединение с Сервером.

В отличие от обычного Агента администрирования, шлюз соединения ожидает соединений от Сервера администрирования, а не устанавливает соединения с ним. Шлюз соединения принимает подключение от Сервера администрирования в демилитаризированной зоне по TLS-порту 13000. Так как шлюз соединения в демилитаризованной зоне не может получить доступ к портам Сервера администрирования, Сервер администрирования создает и поддерживает постоянное сигнальное соединение с шлюзом соединения. Сигнальное соединение не используется для передачи данных - оно используется только для отправки приглашения к сетевому взаимодействию. Когда шлюзу соединения необходимо подключиться к Серверу администрирования, он уведомляет Сервер через сигнальное соединение, а затем Сервер устанавливает необходимое соединение для передачи данных.

Шлюз соединения позволяет более эффективно применять средства безопасности для защиты сетевой инфраструктуры от потенциальных уязвимостей.

- Использование шлюза соединения упрощает мониторинг подозрительной активности на отдельном сетевом узле за пределами локальной сети (LAN). Это позволяет избежать прямых вредоносных атак по мобильному протоколу за счет реализации отдельного протокола для связи между шлюзом соединения и Kaspersky Security Center.

- Уменьшается поверхность потенциальных сетевых атак, поскольку шлюз соединения принимает подключение от Сервера администрирования по одному порту (по умолчанию 13000), через который обрабатываются все запросы.

- Использование шлюза соединения позволяет проверять мобильный сертификат за пределами локальной сети и запрещать устройствам отправлять данные в Kaspersky Security Center до их аутентификации, что защищает сетевую инфраструктуру от уязвимостей протоколов более низкого уровня, таких как TLS/SSL.

### Требования

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

- На хосте со шлюзом соединения должен быть открыт один из портов - 13293 или 13292.

  Эти порты предназначены для подключения и синхронизации мобильных устройств.

  - При использовании порта 13293 на шлюзе соединения проверяется TLS-сертификат (без отправки сертификата на Сервер администрирования).

  - При использовании порта 13292 сертификат не проверяется (при этом игнорируется флаг LP_MobileMustUseTwoWayAuthOnPort13292).

- Между шлюзом соединения и Kaspersky Security Center должен быть открыт порт 13000, по которому шлюз соединения принимает подключение от Сервера администрирования. Его открытие наружу из демилитаризованной зоны не требуется.

- Хост должен иметь статический адрес, доступный из интернета.

## Этапы

Настройка включает в себя следующие шаги:

1. **Установка Агента администрирования на хост, выполняющий роль шлюза соединения**

   Сначала нужно установить Агент администрирования на выбранном устройстве-хосте, который будет выступать в качестве шлюза соединения.

   Информация о создании инсталляционного пакета Агента администрирования приведена в справке Kaspersky Security Center.

   Вы можете установить Агент администрирования в интерактивном режиме, указав параметры установки шаг за шагом. Вы также можете использовать файл ответов – текстовый файл, который содержит пользовательский набор параметров установки: переменные и их соответствующие значения. Использование файла ответов позволяет запустить установку в тихом режиме, то есть без участия пользователя. Информация об установке Агента администрирования в тихом режиме приведена в справке Kaspersky Security Center.

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

   После установки Агента администрирования в качестве шлюза соединения нужно 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.

   Нужно создать новую группу в группе **Управляемые устройства** и добавить устройство, выступающее в качестве шлюза соединения, в созданную группу. Информация о том, как вручную добавлять устройства в группы в Kaspersky Security Center Web Console, приведена в справке Kaspersky Security Center.

   После этого назначьте устройство точкой распространения и настройте точку распространения для работы в качестве шлюза соединения в разделе **Шлюз соединения** свойств точки распространения. Затем включите параметры **Открыть порт для мобильных устройств (SSL-аутентификация только Сервера администрирования)** и **Открыть порт для мобильных устройств (двусторонняя SSL-аутентификация)** и укажите порты и имена DNS-доменов точки распространения для подключения мобильных устройств.

   > Если в основных ограничениях пользовательского мобильного сертификата Сервера администрирования не установлено свойство "CA: true", на шлюзе соединения будет использоваться тот же сертификат, что и на Сервере администрирования. Если свойство "CA: true" установлено, на шлюзе соединения будет использоваться отдельный сертификат, выпущенный от пользовательского мобильного сертификата Сервера администрирования.

3. **Перевыпустите мобильный сертификат**

   Перевыпустите мобильный сертификат с новым адресом подключения, указанном при настройке шлюза соединения (в окне свойств Сервера администрирования выберите **Общие** → **Сертификаты**). Дополнительная информация о перевыпуске мобильных сертификатов приведена в разделе Перевыпуск мобильного сертификата Сервера администрирования.

### Результаты

Будет настроен шлюз соединения. Теперь вы сможете добавлять новые мобильные устройства, указав адрес шлюза соединения.

Чтобы мобильные устройства синхронизировались с Kaspersky Security Center на шлюзе соединения, в свойствах инсталляционных пакетов Kaspersky Endpoint Security для Android необходимо указать адрес подключения, заданный при настройке шлюза соединения (**Операции** → **Хранилища** → **Инсталляционные пакеты**).

## Добавление инсталляционных пакетов в хранилище Сервера администрирования

Для дальнейшего развертывания систем управления мобильными устройствами необходимо добавить в хранилище Сервера администрирования следующие инсталляционные пакеты:

- Инсталляционный пакет Агента администрирования для Linux (для последующей установки Агента администрирования на рабочую станцию).
- Инсталляционный пакет Сервера iOS MDM (для последующей установки Сервера iOS MDM для подключения и управления iOS-устройствами).
- Инсталляционный пакет Kaspersky Endpoint Security для Android (для последующей установки Kaspersky Endpoint Security для Android на устройства).

Инструкции по добавлению инсталляционных пакетов в хранилище Сервера администрирования приведены в справке Kaspersky Security Center.

## Добавление лицензионного ключа в хранилище Сервера администрирования

Для подключения мобильных устройств к Kaspersky Security Center Web Console и управления ими необходимо указать лицензионный ключ, поддерживающий решение для управления мобильными устройствами.

Используемая лицензия определяет набор базовых и расширенных параметров, которые вы можете настраивать. С лицензией без поддержки расширенной функциональности Kaspersky Secure Mobility Management в плагине Kaspersky Mobile Devices Protection and Management доступны только базовые параметры защиты устройств. Подробная информация о лицензиях приведена в разделе О лицензии.

*Чтобы указать лицензионный ключ в параметрах действующей лицензии свойств Сервера администрирования:*

- В главном окне Kaspersky Security Center Web Console нажмите на имя Сервера администрирования.

Откроется окно свойств Сервера администрирования.

a. На вкладке **Общие** выберите раздел **Лицензионные ключи**.

b. В блоке параметров **Действующая лицензия** нажмите **Выбрать** и выполните одно из следующих действий:

- Выберите один из существующих лицензионных ключей.
- Укажите файл в формате KEY, который вы хотите добавить.

> Выбранная лицензия должна поддерживать решение для управления мобильными устройствами.

c. Нажмите **Сохранить**.

Лицензионный ключ указан в параметрах действующей лицензии свойств Сервера администрирования.

*Чтобы добавить лицензионный ключ в хранилище Сервера администрирования:*

1. В главном окне Kaspersky Security Center Web Console выберите **Операции** → **Лицензии**.
2. Нажмите **Добавить**.
3. В открывшемся окне нажмите **Добавить файл ключа**.
4. Нажмите **Выберите файл ключа** и укажите файл в формате KEY, который вы хотите добавить.

> Выбранная лицензия должна поддерживать решение для управления мобильными устройствами.

5. Нажмите **Сохранить**.

Лицензионный ключ добавлен в хранилище Сервера администрирования.

## Установка Агента администрирования для Linux

Агент администрирования для Linux - это компонент Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и приложениями "Лаборатории Касперского", установленными на рабочей станции или сервере.

Для развертывания системы управления iOS-устройствами необходимо установить Агент администрирования на рабочую станцию, на которой в дальнейшем будет развернут Сервер iOS MDM. После установки Агента администрирования вы сможете настроить и установить Сервер iOS MDM для последующего подключения и управления iOS-устройствами.

Инструкции по установке Агента администрирования для Linux приведены в справке Kaspersky Security Center.

## Настройка параметров Веб-сервера Kaspersky Security Center Linux

Веб-сервер Kaspersky Security Center Linux - это компонент Kaspersky Security Center Linux, который устанавливается в составе Сервера администрирования. Веб-сервер предназначен для передачи по сети автономных пакетов установки, управляющих профилей, а также файлов из папки общего доступа.

Созданные инсталляционные пакеты публикуются на Веб-сервере автоматически и удаляются после первой загрузки. Администратор может передать сформированную ссылку пользователю любым удобным способом, например, по электронной почте.

Дополнительная информация приведена в справке Kaspersky Security Center.

*Для подключения мобильных устройств убедитесь, что в свойствах Сервера администрирования правильно указан FQDN веб-сервера:*

1. В главном окне Kaspersky Security Center Web Console нажмите на имя Сервера администрирования.
2. В открывшемся окне свойств Сервера администрирования на вкладке **Общие** выберите раздел **Веб-сервер**.
3. Убедитесь, что указанное в поле **FQDN Веб-сервера** полное доменное имя (FQDN) является публичным и определяется DNS-серверами.

## Настройка Веб-сервера на шлюзе соединения (Агент администрирования для Linux)

На точке распространения в режиме шлюза соединения реализована отдельная служба Веб-сервера, которая позволяет работать с мобильными устройствами, подключенными к Kaspersky Security Center. С помощью этой службы вы можете передавать устройствам инсталляционные пакеты приложений и управляющие профили без прямого подключения устройств к Серверу администрирования. Передача происходит через обработку службой на шлюзе соединения HTTP/HTTPS-запросов файлов.

Служба Веб-сервера на шлюзе соединения работает только для загрузки на мобильные устройства следующих видов файлов:

- Мобильные приложения "Лаборатории Касперского"

  Инсталляционные пакеты мобильных приложений "Лаборатории Касперского", добавленные администратором в политику через Kaspersky Security Center Web Console.

- Сторонние мобильные приложения

  Инсталляционные пакеты сторонних мобильных приложений, созданные администратором для их последующей установки на устройства из локального файла.

- Управляющие профили для iOS MDM-устройств

Для подключения новых устройств к Kaspersky Security Center инсталляционные пакеты и управляющие профили публикуются на Веб-сервере на шлюзе соединения в случае, если он развернут.

Ссылки на инсталляционные пакеты размещены в параметрах политики и разделах "Приложения и файлы" и "Инсталляционные пакеты" Kaspersky Security Center.

Эта функциональность доступна с Kaspersky Security Center Linux 15.2 или выше.

Служба Веб-сервера на шлюзе соединения устанавливается вместе с Агентом администрирования для Linux. Для использования службы вам необходимо назначить устройство, которое будет выполнять роль точки распространения в режиме шлюза соединения для использования в качестве Веб-сервера, и указать необходимые настройки.

## Назначьте устройство, которое будет выполнять роль точки распространения в режиме шлюза соединения

*Чтобы назначить устройство, которое будет выполнять роль точки распространения в режиме шлюза соединения:*

1. В главном окне Kaspersky Security Center Web Console нажмите на имя Сервера администрирования.
2. В открывшемся окне свойств Сервера администрирования на вкладке **Общие** выберите раздел **Точки распространения**.
3. Нажмите **Назначить**.
4. В открывшемся окне выберите устройство, которое будет выполнять роль точки распространения.
5. Нажмите **ОК**.

   Выбранное устройство появится в списке точек распространения.
6. Нажмите на имя устройства.
7. В открывшемся окне свойств точки распространения перейдите в раздел **Шлюз соединения**.
8. Включите переключатель **Шлюз соединения**.
9. Задайте имя DNS-домена точки распространения, под которым она будет доступна мобильным устройствам.
10. Нажмите **ОК**.

Устройство, которое будет выполнять роль точки распространения в режиме шлюза соединения, назначено.

## Настройте параметры Веб-сервера на шлюзе соединения

*Чтобы настроить параметры Веб-сервера на шлюзе соединения:*

1. В главном окне Kaspersky Security Center Web Console нажмите на имя Сервера администрирования.
2. В открывшемся окне свойств Сервера администрирования на вкладке **Общие** выберите раздел **Веб-сервер**.
3. В блоке параметров **Параметры Веб-сервера на шлюзе соединения (Агент администрирования для Linux)** установите флажок **Запустить дополнительный Веб-сервер на шлюзе соединения**.

   Этот Веб-сервер будет использоваться для передачи файлов устройствам.
4. В появившемся поле **Шлюз соединения** укажите устройство, на котором будет развернут Веб-сервер для использования в качестве шлюза соединения. В выпадающем списке отображаются только те устройства, которые поддерживают эту функциональность.

5. В появившемся блоке параметров **Параметры Веб-сервера для выбранного шлюза соединения** настройте порты Веб-сервера:

   a. Выберите **Открыть HTTPS-порт Веб-сервера**, если вы хотите, чтобы Веб-сервер был доступен по HTTPS-порту и обрабатывал HTTPS-запросы. Для защиты этого порта также потребуется настройка соответствующего сертификата.

      a. Укажите **HTTPS-порт**.

      b. Укажите **Источник сертификата** для HTTPS-порта Веб-сервера.

      По умолчанию используется сертификат, выпущенный Сервером администрирования – он действителен в течение 397 дней и обновляется автоматически по истечении этого срока. При необходимости сертификат можно обновить вручную по кнопке **Перевыпустить**.

      Чтобы продолжить использование этого сертификата, выберите **Выпустить сертификат средствами Сервера администрирования**. Чтобы загрузить пользовательский сертификат вручную, выберите **Загрузить сертификат из файла**.

      Чтобы загрузить сертификат из файла:

      - Нажмите **Загрузить из файла**.
      - В открывшемся окне загрузки сертификата выберите **Формат сертификата**.
      - Для формата **PKCS #12** укажите путь к файлу сертификата (P12 или PFX) и введите пароль сертификата.

        Для формата **X.509** укажите пути к файлам открытого и закрытого ключей и введите пароль закрытого ключа.
      - Нажмите **Сохранить**.

   c. Убедитесь, что адреса в полях **Адрес Веб-сервера** (адрес Веб-сервера, запросы от которого будет обрабатывать Kaspersky Security Center) и **Адрес сертификата** (адрес выпущенного сертификата) совпадают. В противном случае необходимо перевыпустить сертификат, выданный Сервером администрирования, или загрузить другой пользовательский сертификат.

   Чтобы устройства могли безопасно загружать файлы с Веб-сервера на шлюзе соединения через HTTPS, на них должен быть установлен сертификат Веб-сервера.

   b. Выберите **Открыть HTTP-порт Веб-сервера**, если вы хотите, чтобы Веб-сервер был доступен по HTTP-порту и обрабатывал HTTP-запросы.

      a. Укажите **HTTP-порт**.

   c. Нажмите **Сохранить**.

Параметры Веб-сервера на шлюзе соединения настроены.

При изменении параметров HTTP или HTTPS-порта необходимо обновить ссылки на ранее опубликованные инсталляционные пакеты для мобильных устройств, подключенных к Веб-серверу на шлюзе соединения. Обновите ссылки в параметрах политики и разделах "Приложения и файлы" и "Инсталляционные пакеты" Kaspersky Security Center.

*Чтобы обновить ссылки на инсталляционные пакеты:*

- В разделе "Приложения и файлы":

  a. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Мобильные → Приложения и файлы**.

  b. Нажмите **Android** или **iOS** в зависимости от требуемой операционной системы.

  c. В открывшемся списке приложений выполните одно из действий:

  - Установите флажок рядом с названиями приложений, ссылки на инсталляционные пакеты которых необходимо обновить, а затем нажмите **Опубликовать повторно**.
  - Нажмите на название приложения, ссылку на инсталляционный пакет которого необходимо обновить, а затем в открывшемся окне нажмите **Опубликовать повторно**.

- В разделе "Инсталляционные пакеты":

  a. В главном окне Kaspersky Security Center Web Console выберите **Операции → Хранилища → Инсталляционные пакеты**.

  b. В открывшемся окне нажмите **Просмотреть список автономных пакетов**.

  c. Выберите приложение, ссылку на инсталляционный пакет которого необходимо обновить, а затем нажмите **Отменить публикацию**.

  d. Нажмите **Опубликовать**.

Ссылки на инсталляционные пакеты обновлены.

## Передача на устройства сертификата Веб-сервера на шлюзе соединения

Чтобы устройства могли безопасно загружать файлы с Веб-сервера на шлюзе соединения через HTTPS, на них должен быть установлен сертификат Веб-сервера.

### Передача сертификата Веб-сервера на iOS MDM-устройства

При подключении новых iOS MDM-устройств Kaspersky Security Center автоматически добавляет открытый ключ сертификата Веб-сервера на шлюзе соединения в управляющие профили.

Таким образом, устройства могут проверять корректность HTTPS-соединения и безопасно загружать сторонние приложения с Веб-сервера на шлюзе соединения.

В случае изменения сертификата он обновляется на iOS MDM-устройствах в процессе синхронизации с Сервером iOS MDM.

### Передача сертификата Веб-сервера на Android-устройства

Если вы используете сертификат Веб-сервера на шлюзе соединения, выпущенный Kaspersky Security Center, стандартный загрузчик Android позволяет вам скачивать файлы с Веб-сервера на шлюзе соединения только через HTTP.

Чтобы безопасно скачивать на устройства файлы с сертификатом, выпущенным Kaspersky Security Center, вы можете использовать встроенный загрузчик Kaspersky Endpoint Security для Android, который всегда скачивает файлы через HTTPS. Подробная информация доступна в статье Выбор загрузчика для Android-устройств.

# Перенос данных из Kaspersky Security Center Windows в Kaspersky Security Center Linux

Вы можете перенести данные мобильных устройств из Kaspersky Security Center Windows в Kaspersky Security Center Linux, переместив инфраструктуру управления мобильными устройствами с серверов Windows на Linux. После переноса мобильные устройства автоматически устанавливают связь с Kaspersky Security Center Linux без необходимости ручного переподключения и управляются той же политикой, что и на серверах Windows.

## Предварительные требования

Прежде чем начать:

- Убедитесь, что необходимые функции Kaspersky Security Center Windows поддерживаются в Kaspersky Security Center Linux. Подробная информация об основных возможностях Kaspersky Security Center как решения на базе Windows или Linux приведена в справке Kaspersky Security Center.
- Ознакомьтесь с **СУБД и версиями Kaspersky Security Center и Сервера iOS MDM**, между которыми возможен перенос.

  - Перенос данных мобильных устройств возможен между следующими СУБД:
    - Kaspersky Security Center Windows + Microsoft SQL Server → Kaspersky Security Center Linux + PostgreSQL, Postgres Pro
    - Kaspersky Security Center Windows + MariaDB → Kaspersky Security Center Linux + PostgreSQL, Postgres Pro
    - Kaspersky Security Center Windows + MySQL → Kaspersky Security Center Linux + PostgreSQL, Postgres Pro
    - Kaspersky Security Center Windows + PostgreSQL, Postgres Pro → Kaspersky Security Center Linux + PostgreSQL, Postgres Pro
    - Kaspersky Security Center Windows + MariaDB → Kaspersky Security Center Linux + MariaDB
    - Kaspersky Security Center Windows + MySQL → Kaspersky Security Center Linux + MySQL

Для поддержки переноса данных в PostgreSQL или Postgres Pro необходимо установить патч для соответствующей в версии Сервера администрирования Kaspersky Security Center Windows. Обратитесь в Службу технической поддержки "Лаборатории Касперского", чтобы получить необходимый патч.

Для Kaspersky Secure Mobility Management на базе Kaspersky Security Center Windows 14.2: 14.2.0.26967-pf5

Для Kaspersky Security Center Windows 14.2: 14.2.0.48079-pf5

Для Kaspersky Security Center Windows 15.1: 15.1.0.20748-pf2

Вышеперечисленные патчи обязательны для установки. Во избежание возможных ошибок во время переноса данных мы рекомендуем установить не только обязательные версии патчей, но и все предыдущие (начиная с pf1), соответствующие версии Kaspersky Security Center, с которой вы выполняете перенос.

Если вы используете MySQL или MariaDB в качестве СУБД для Kaspersky Security Center Windows и Kaspersky Security Center Linux, убедитесь, что параметр `lower_case_table_names` совпадает в текущей и новой СУБД.

При установке MySQL или MariaDB для Kaspersky Security Center Linux вам нужно установить то же значение параметра, которое указано для этого параметра на Windows. Подробная информация о резервном копировании и восстановлении данных Сервера администрирования при использовании MySQL или MariaDB приведена в справке Kaspersky Security Center.

- Перенос данных возможен между следующими версиями Kaspersky Security Center:
  - Консоль администрирования Kaspersky Security Center Windows 14.2 на базе MMC (локально) → Kaspersky Security Center Linux 15.4 Web Console (локально)
  - Консоль администрирования Kaspersky Security Center Windows 14.2.0.48079 на базе MMC (для Kaspersky Secure Mobility Management) (локально) → Kaspersky Security Center Linux 15.4 Web Console (локально)
  - Консоль администрирования Kaspersky Security Center Windows 15.1 на базе MMC (локально) → Kaspersky Security Center Linux 15.4 Web Console (локально)
  - Kaspersky Security Center Windows 14.2 Web Console и Cloud Console (локально) → Kaspersky Security Center Linux 15.4 Web Console (локально)
  - Kaspersky Security Center Windows 15.1 Web Console и Cloud Console (локально) → Kaspersky Security Center Linux 15.4 Web Console (локально)
- Перенос данных возможен между следующими версиями Сервера iOS MDM:
  - Сервер iOS MDM Windows 14.2 (для Kaspersky Secure Mobility Management) → Сервер iOS MDM Linux 15.4
  - Сервер iOS MDM Windows 14.2 → Сервер iOS MDM Linux 15.4
  - Сервер iOS MDM Windows 15.1 → Сервер iOS MDM Linux 15.4

- Изучите, **какие данные будут перенесены**.

  Переносятся следующие данные:

  - Настройки Kaspersky Security Center
    - FQDN для подключения мобильных устройств к Kaspersky Security Center
    - Настройки, специфичные для мобильных устройств: лицензии, параметры интеграции с Firebase Cloud Messaging (FCM), сертификаты для подписания управляющих профилей, параметры выпуска мобильных сертификатов, информация о принятых Лицензионных соглашениях, параметры прокси-сервера Kaspersky Security Network (KSN), конфигурационные файлы Kaspersky Private Security Network (KPSN)

      Если вы используете Kaspersky Security Center 14.2.0.26967, для корректного переноса настроек FCM в Postgres необходимо установить патч 14.2.0.26967-pf4. Если патч не установлен, перенос завершится ошибкой в базе данных. В этом случае, чтобы избежать ошибок, удалите все настройки FCM перед началом переноса данных.

      Параметры интеграции с PKI для выпуска мобильных сертификатов не переносятся.

    - Конфигурационные файлы управления доступом на основе ролей
    - Параметры обновления баз Kaspersky Endpoint Security для Android
    - Ключи подписи для APK-файлов Kaspersky Endpoint Security для Android
  - Мобильные устройства
    - Информация о мобильных устройствах под управлением Kaspersky Endpoint Security для Android и Kaspersky Protection для iOS
    - Журналы событий мобильных устройств под управлением Kaspersky Endpoint Security для Android и Kaspersky Protection для iOS
    - История ранее выполненных и ожидающих выполнения команд на Android-устройствах и их результаты
    - Информация о ссылках, инсталляционных пакетах и управляющих профилях для мобильных устройств, ожидающих подключения
    - Настройки и инсталляционные пакеты Kaspersky Endpoint Security для Android
    - Настройки и инсталляционные пакеты Серверов iOS MDM

      Информация об Android-устройствах, ожидающих подключения, не переносится.

- Политики
  - Политики для управления мобильными устройствами в Консоли администрирования Kaspersky Security Center на базе MMC (Android и iOS)
  - Политики для управления мобильными устройствами в Kaspersky Security Center Web Console и Cloud Console (Android и iOS)
- Сертификаты
  - Мобильные сертификаты Сервера администрирования (основной и резервный сертификаты, сертификаты Веб-сервера)
  - Информация о пользовательских сертификатах (мобильных, почтовых, VPN-сертификатах) и их статусах
- Серверы iOS MDM
  - Установленные Серверы iOS MDM
  - Журналы событий Серверов iOS MDM
- Параметры, сертификаты (сертификат Сервера iOS MDM, APNs-сертификат) и конфигурационные профили Серверов iOS MDM

  Приложения Серверов iOS MDM не переносятся.

  Данные, специфичные для хоста, такие как информация о профилях для мобильных устройств, ожидающих подключения, и командах, ожидающих выполнения, не переносятся.

  При переносе настроек Сервера iOS MDM с Kaspersky Security Center Windows 14.2 в Kaspersky Security Center Linux параметры уведомлений и хранения событий Сервера iOS MDM не переносятся и принимают значения по умолчанию. После переноса вам потребуется указать необходимые значения вручную.
- Веб-сервер
  - Настройки и инсталляционные пакеты Kaspersky Endpoint Security для Android
  - Настройки и инсталляционные пакеты Серверов iOS MDM

  Мобильные приложения, хранящиеся на Веб-сервере Kaspersky Security Center, не переносятся с помощью утилиты klbackup и должны быть перенесены вручную.
- Настройки шлюза соединения (Агент администрирования)

Установленные плагины для управления мобильными устройствами не переносятся. После восстановления данных Сервера администрирования и Сервера iOS MDM из резервной копии,

необходимо скачать и установить плагин Kaspersky Mobile Devices Protection and Management и плагин Сервера iOS MDM.

## Этапы

Процесс миграции предполагает создание резервной копии с помощью утилиты *klbackup* для переноса данных Сервера администрирования и утилиты *kliosbackup* для переноса данных Сервера iOS MDM.

Чтобы перенесенные мобильные устройства корректно отображались в Kaspersky Security Center Web Console, необходимо перенести и Сервер администрирования, и Сервер iOS MDM. Сначала необходимо перенести Сервер администрирования, а затем Сервер iOS MDM, как описано в сценарии ниже.

Перенос данных состоит из следующих этапов:

1. **Подготовка к переносу**

   1. Убедитесь, что у вас есть внутренняя учетная запись администратора для входа на Сервер администрирования.

      Для входа на Сервер администрирования Kaspersky Security Center Linux будет использоваться учетная запись администратора. Если у вас нет такой учетной записи и вы вошли только под локальной учетной записью Windows или под доменной учетной записью, то после восстановления из резервной копии вы не сможете выполнить вход на Сервер администрирования Kaspersky Security Center Linux. Сервер администрирования Kaspersky Security Center Linux не поддерживает вход с использованием локальной учетной записи Windows. Вход под доменной учетной записью возможен, но может потребовать дополнительной настройки Сервера администрирования.

      Если у вас нет учетной записи администратора, вам нужно будет создать ее с помощью утилиты kladduser после восстановления из резервной копии.

   2. В Kaspersky Security Center Windows в разделе **Безопасность** окна свойств группы администрирования **Управляемые устройства** включите параметр **Наследовать параметры Сервера администрирования или родительской группы**, чтобы обеспечить наследование прав и доступ к настройкам политики.

      Раздел **Безопасность** доступен, если в окне параметров интерфейса установлен флажок **Отображать разделы с параметрами безопасности**.

   3. Создайте задачу для загрузки обновлений в хранилище Сервера администрирования.

      Эта задача необходима для скачивания последней версии конфигурационного файла управления доступом на основе ролей с серверов "Лаборатории Касперского" в хранилище Сервера администрирования. Подробная информация о создании этой задачи приведена в справке Kaspersky Security Center.

   4. Если вам необходимо перенести политики, созданные в плагине Kaspersky Security for Mobile (Policies) Kaspersky Security Center Web Console и Cloud Console, удалите все его профили политик. Политики этого плагина, содержащие профили политик, перенесены не будут.

2. **Создание актуальной резервной копии данных Сервера администрирования Kaspersky Security Center Windows**

В зависимости от типа СУБД, используемой Kaspersky Security Center Windows и Kaspersky Security Center Linux, выполните одно из следующих действий:

- Для переноса данных с MySQL или MariaDB в MySQL или MariaDB: создайте резервную копию с помощью утилиты klbackup на устройстве, на котором установлен Сервер администрирования.
- Для переноса данных с Microsoft SQL Server в MySQL или MariaDB: создайте резервную копию данных с помощью утилиты klbackup с включенным параметром **Перенос данных в формате MySQL/MariaDB**.
- Для переноса данных Microsoft SQL Server в PostgreSQL или Postgres Pro:

  a. Установите патч для соответствующей версии Сервера администрирования Kaspersky Security Center Windows для поддержки переноса данных в PostgreSQL и Postgres Pro:

  - Для Kaspersky Secure Mobility Management на базе Kaspersky Security Center Windows 14.2: 14.2.0.26967-pf5
  - Для Kaspersky Security Center Windows 14.2: 14.2.0.48079-pf5
  - Для Kaspersky Security Center Windows 15.1: 15.1.0.20748-pf2

  Обратитесь в Службу технической поддержки "Лаборатории Касперского", чтобы получить необходимый патч.

  b. Создайте резервную копию данных с помощью утилиты klbackup.

  - Если вы запускаете утилиту klbackup из командной строки, используйте флаг `-migrate postgres`.
  - Если вы используете интерфейс утилиты klbackup, включите параметр **Перенести в формат Postgres**.

  c. Отключите Сервер администрирования Kaspersky Security Center Windows от сети.

3. **Подготовка нового устройства к установке Kaspersky Security Center Linux**

1. Выберите новое устройство, на которое будет установлен Сервер администрирования. Это устройство должно соответствовать аппаратным и программным требованиям.
2. Проверьте доступность портов, используемых на Сервере администрирования.
3. Назначьте новому устройству то же имя хоста и FQDN, что и на сервере Windows.
4. Установите значение 1 для переменной среды `KLCS_FF_UMDM_POLICIES_MIGRATION`:

   ```
   export KLCS_FF_UMDM_POLICIES_MIGRATION=1
   ```

   В качестве альтернативы, сразу после установки Kaspersky Security Center Linux используйте утилиту klscflag, чтобы настроить соответствующий флаг сервера с помощью команды:

   ```
   klscflag -fset -pv .core/.independent -s klcsff -n KLCS_FF_UMDM_POLICIES_MIGRATION -t d -v 1
   ```

### 4 Установка и настройка СУБД

1. Выберите тип СУБД, который обеспечивает оптимальную производительность с учетом количества сетевых устройств, топологии сети и нагрузки на сеть. Вы можете выбрать любую поддерживаемую СУБД.

2. Установите СУБД в соответствии с типом СУБД, выбранным при создании резервной копии. Информацию об установке выбранной СУБД см. в документации к этой СУБД.

   > Новая версия базы данных не должна быть ниже текущей.

3. Настройте СУБД для работы с Kaspersky Security Center Linux.

### 5 Установка Kaspersky Security Center Linux и завершение переноса данных Сервера администрирования

1. Установите Kaspersky Security Center Linux на новом устройстве.

   Внутренняя учетная запись администратора, созданная во время установки, а также другие объекты (группы, политики, задачи, пользователи), созданные до восстановления данных Сервера администрирования из резервной копии, будут утеряны после восстановления. Эти объекты будут заменены объектами из резервной копии.

2. После завершения установки восстановите данные Сервера администрирования на новом устройстве с помощью утилиты klbackup.

   > Из-за ограничений PostgreSQL необходимо временно предоставить права суперпользователя PostgreSQL учетной записи, которую использует Сервер администрирования для подключения к СУБД.

   > Мы рекомендуем начинать процесс восстановления данных сразу после установки Kaspersky Security Center Linux без промежуточных перезагрузок.

3. Если у вас не было внутренней учетной записи администратора для входа на Сервер администрирования Kaspersky Security Center Windows, и вы использовали локальную учетную запись Windows или доменную учетную запись, создайте учетную запись администратора с помощью утилиты kladduser:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>
   ```

   где `<пароль>` соответствует следующим требованиям:

   - Пароль пользователя не может содержать менее 8 или более 256 символов
   - Пароль должен содержать символы как минимум трех групп из списка ниже:
     - верхний регистр (A–Z);
     - нижний регистр (a–z);
     - числа (0–9);
     - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).

4. Проверьте статус восстановления данных (например, используя команду `journalctl -u kladminserver_srv.service -b`), чтобы убедиться, что политики для мобильных устройств успешно переносятся.

5. Установите Kaspersky Security Center Web Console.

6. Выполните вход в Kaspersky Security Center Web Console под внутренней учетной записью администратора.

   Процесс инициализации данных обычно занимает до 15 минут после восстановления данных Сервера администрирования. Точное время зависит от производительности оборудования и размера данных Сервера администрирования. В течение этого периода Kaspersky Security Center Web Console может не подключаться и отображать ошибки.

7. Разверните плагины для управления мобильными устройствами.

8. Установите Агент администрирования для Linux.

9. Проверьте работу основных функций Сервера администрирования после завершения инициализации данных в базе данных. Убедитесь, что Сервер администрирования синхронизируется с управляемыми устройствами и данные Сервера администрирования восстановлены.

   > Для проверки подключения мобильных устройств после переноса данных выполняется принудительная синхронизация с ними.

10. Выполните опрос контроллеров доменов для восстановления информации о структуре домена, учетных записях пользователей, группах и DNS-именах устройств, входящих в домены.

11. При необходимости удалите Сервер администрирования и сервер баз данных с предыдущего устройства.

    > В одной сети не должно быть нескольких Серверов администрирования с одинаковым адресом подключения и сертификатом Сервера администрирования.

    Теперь у администратора есть доступ к данным Сервера администрирования и устройствам, ранее управляемым Kaspersky Security Center Windows, с учетом функциональности, поддерживаемой в Kaspersky Security Center Linux.

    > Для корректной работы параметра **Сохранение историй местоположений** настроек политики **Определение местоположения** убедитесь, что на вкладке **Настройка событий** добавлен тип события **История местоположений устройства**, а в свойствах события включено его хранение в базе данных Сервера администрирования. Это действие должно быть выполнено для всех перенесенных политик.

### 6 Перенос данных Сервера iOS MDM Windows

Если у вас установлено несколько Серверов iOS MDM, необходимо выполнить процедуру переноса данных для каждого из них.

1. Убедитесь, что FQDN Сервера iOS MDM Linux совпадает с FQDN Сервера iOS MDM Windows.
2. При наличии резервных сертификатов Сервера iOS MDM убедитесь, что файл kliosmdm.ini, расположенный в рабочей директории iOS MDM, содержит пароль SrvResCertPwd.

   Если в файле kliosmdm.ini нет пароля, перевыпустите или удалите резервный сертификат Сервера iOS MDM (kliosmdmserver2_cert.pem), пароль для которого отсутствует в файле.
3. Создайте резервную копию данных Сервера iOS MDM с помощью утилиты kliosbackup.
4. Разверните Сервер iOS MDM на новом устройстве с установленным Kaspersky Security Center Linux.
5. Перенесите файлы с резервной копией данных Сервера iOS MDM на новое устройство.
6. Восстановите данные из резервной копии с помощью утилиты kliosbackup.

   Если какое-либо значение настроек не удается перенести, оно будет заменено значением по умолчанию.

После завершения процесса переноса данных все подключенные устройства автоматически синхронизируются с Сервером iOS MDM Linux без необходимости ручного переподключения.

## Резервное копирование и восстановление данных Сервера администрирования с помощью утилиты klbackup

Перенос данных из Kaspersky Security Center Windows в Kaspersky Security Center Linux осуществляется с помощью утилиты klbackup, которая входит в состав дистрибутива Kaspersky Security Center. После установки Сервера администрирования утилита находится в корне папки назначения, указанной при установке.

*Чтобы перенести данные Сервера администрирования Windows с помощью утилиты klbackup:*

1. Создайте резервную копию данных Сервера администрирования на устройстве Windows с установленным Сервером администрирования
2. Восстановите данные Сервера администрирования из созданной резервной копии на устройстве Linux

## Создание резервной копии данных Сервера администрирования на устройстве Windows

Вы можете создать резервную копию данных Сервера администрирования Windows с помощью утилиты klbackup, которая работает в двух режимах:

- Интерактивный
- Тихий

## Создание резервной копии данных Сервера администрирования Windows в интерактивном режиме

*Чтобы создать резервную копию данных Сервера администрирования Windows в интерактивном режиме:*

1. На устройстве Windows запустите утилиту klbackup из установочной папки Kaspersky Security Center (по умолчанию `C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center\klbackup.exe`).

2. В первом окне мастера выберите **Выполнить резервное копирование данных Сервера администрирования**.

   Нажмите **Далее**.

3. В следующем окне мастера:

   a. Укажите путь в поле **Папка назначения для резервного копирования**.

   b. Включите параметр **Перенос данных базы данных**.

   c. Выберите один из параметров:

   a. **Перенос данных в формате MySQL/MariaDB**

   Включите этот параметр, если в настоящее время вы используете SQL Server в качестве СУБД для Сервера администрирования и хотите перенести данные из SQL Server в MySQL или MariaDB. Kaspersky Security Center создаст резервную копию данных, совместимую с MySQL и MariaDB. После этого вы можете восстановить данные из резервной копии в MySQL или MariaDB.

   b. **Перенести в формат Postgres**

   Включите этот параметр, если в настоящее время вы используете SQL Server в качестве СУБД для Сервера администрирования и хотите перенести данные из SQL Server в PostgreSQL или Postgres Pro. Kaspersky Security Center создаст резервную копию данных, совместимую с PostgreSQL и Postgres Pro. После этого можно будет восстановить данные из этой резервной копии в PostgreSQL или Postgres Pro.

   Этот параметр становится доступным только после установки патча для соответствующей версии Сервера администрирования Kaspersky Security Center Windows: Обратитесь в Службу технической поддержки "Лаборатории Касперского", чтобы получить необходимый патч.

   Для Kaspersky Secure Mobility Management на базе Kaspersky Security Center Windows 14.2: 14.2.0.26967-pf5

   Для Kaspersky Security Center Windows 14.2: 14.2.0.48079-pf5

   Для Kaspersky Security Center Windows 15.1: 15.1.0.20748-pf2

d. Включите параметр **Включать текущую дату и время в имя папки назначения для резервных копий**.

e. Установите пароль для защиты конфиденциальных данных.

Нажмите **Далее**, чтобы начать процесс резервного копирования.

Резервная копия данных Сервера администрирования создана.

При восстановлении данных Сервера администрирования из резервной копии, созданной с помощью утилиты klbackup в интерактивном режиме, может возникнуть ошибка. Если вы создаете резервную копию с помощью утилиты klbackup с установленным патчем 15.1.0.20748-pf2 и выключенным параметром **Перенос данных базы данных**, при восстановлении этой копии возникает ошибка (для всех СУБД, кроме MySQL и MariaDB). Если вы хотите создать резервную копию с установленным патчем 15.1.0.20748-pf2 без перехода на другую СУБД, запустите утилиту klbackup из командной строки.

## Создание резервной копии данных Сервера администрирования Windows в тихом режиме

Чтобы создать резервную копию данных Сервера администрирования Windows в тихом режиме, запустите утилиту klbackup с необходимым набором ключей в командной строке устройства, на котором установлен Сервер администрирования.

Пример:

```
cd 'C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center\'
klbackup.exe -migrate postgres -path BACKUP_PATH -use_ts -password PASSWORD
```

Если не задать пароль в командной строке klbackup, утилита запросит ввести его интерактивно.

Описания ключей:

- `-path BACKUP_PATH` — сохранить информацию в папке `BACKUP_PATH` (обязательный параметр).

  Учетная запись сервера базы данных и утилита klbackup должны обладать правами на изменение данных в папке `BACKUP_PATH`.

- `-migrate mysql` — создать резервную копию данных Сервера администрирования, хранящихся в базе данных SQL Server, совместимой с MySQL (включая MariaDB). Данные из этой резервной копии можно восстановить в MySQL.

- `-migrate postgres` — создать резервную копию данных Сервера администрирования, хранящихся в базе данных SQL Server, совместимой с PostgreSQL и Postgres Pro. Данные из этой резервной копии можно восстановить в PostgreSQL или Postgres Pro.

  Этот параметр становится доступным только после установки патча для соответствующей версии Сервера администрирования Kaspersky Security Center Windows. Обратитесь в Службу технической поддержки "Лаборатории Касперского", чтобы получить необходимый патч.

  Для Kaspersky Secure Mobility Management на базе Kaspersky Security Center Windows 14.2: 14.2.0.26967-pf5

  Для Kaspersky Security Center Windows 14.2: 14.2.0.48079-pf5

  Для Kaspersky Security Center Windows 15.1: 15.1.0.20748-pf2

- `-use_ts` — при сохранении данных копировать информацию в папку `BACKUP_PATH`, в подпапку с именем в формате `klbackup ГГГГ-ММ-ДД # ЧЧ-ММ-СС`, которая включает в себя текущую дату и время операции в формате UTC. Если ключ не задан, информация сохраняется в корне папки `BACKUP_PATH`.

  При попытке сохранить информацию в папку, в которой уже есть резервная копия, появится сообщение об ошибке. В этом случае информация не обновится.

  Наличие ключа `-use_ts` позволяет вести архив данных Сервера администрирования. Например, если ключом `-path` была задана папка `C:\KLBackups`, то в папке `klbackup 2025-06-19 # 11-30-18` сохранится информация о состоянии Сервера администрирования на момент 19 июня 2025 года, 11 часов 30 минут 18 секунд.

- `-password PASSWORD` — установить пароль для защиты конфиденциальных данных.

  Забытый пароль невозможно восстановить. Требования к паролю отсутствуют. Длина пароля не ограничена, а также возможна нулевая длина (отсутствие) пароля.

Полный список ключей утилиты приведен в справке Kaspersky Security Center.

## Восстановление данных Сервера администрирования на устройстве Linux

Вы можете восстановить данные Сервера администрирования Windows из резервной копии на устройстве с Linux в тихом режиме, запустив утилиту klbackup с необходимым набором ключей из командной строки.

При использовании утилиты klbackup флаги Агента администрирования не восстанавливаются и должны быть настроены вручную.

Пример:
```
/opt/kaspersky/ksc64/sbin/klbackup -path BACKUP_PATH -restore -password PASSWORD
```

Описания ключей:

- `-path BACKUP_PATH` — использовать для восстановления данные из папки `BACKUP_PATH` (обязательный параметр).

  Учетная запись сервера базы данных и утилита klbackup должны обладать правами на изменение данных в папке `BACKUP_PATH`.

- `-restore` — выполнить восстановление данных Сервера администрирования. Восстановление данных осуществляется на основании информации, представленной в папке `BACKUP_PATH`. Если ключ отсутствует, производится резервное копирование данных в папку `BACKUP_PATH`.

- `-password PASSWORD` — установить пароль для защиты конфиденциальных данных.

  При восстановлении данных необходимо указать тот же пароль, который был введен во время резервного копирования

Полный список ключей утилиты приведен в справке Kaspersky Security Center.

### Резервное копирование и восстановление данных Сервера iOS MDM с помощью утилиты kliosbackup

Перенос данных с Сервера iOS MDM Windows на Сервер iOS MDM Linux выполняется с помощью утилиты kliosbackup, которая позволяет создавать резервные копии и восстанавливать информацию обо всех подключенных iOS MDM-устройствах и их свойствах. Утилита работает в тихом режиме.

Чтобы перенесенные мобильные устройства корректно отображались в Kaspersky Security Center Web Console, необходимо перенести и Сервер администрирования, и Сервер iOS MDM. Подробная информация о сценарии переноса приведена в разделе Перенос данных из Kaspersky Security Center Windows в Kaspersky Security Center Linux.

По умолчанию утилита kliosbackup находится в следующей установочной папке:

- Windows: `C:\Program Files(x86)\Kaspersky Lab\Mobile Device Management for IOS`
- Linux: `/opt/kaspersky/iosmdm/bin/`

*Чтобы перенести данные Сервера iOS MDM Windows с помощью утилиты kliosbackup:*

1. Создайте резервную копию данных Сервера iOS MDM на устройстве Windows с установленным Сервером iOS MDM.

   Запустите kliosbackup из командной строки с необходимым набором ключей.

   Пример:
   ```
   kliosbackup -backup -path BACKUP_PATH [-pwd PASSWORD]
   ```

2. Восстановите данные Сервера iOS MDM из созданной резервной копии на устройстве Linux.

   Перенесите файлы с данными резервной копии Сервера iOS MDM на устройство Linux, а затем запустите kliosbackup с необходимым набором ключей из командной строки.

   Пример:
   ```
   kliosbackup -restore -path BACKUP_PATH [-pwd PASSWORD]
   ```

Описания ключей:

- `-backup` — создать резервную копию данных Сервера iOS MDM.
- `-restore` — восстановить данные Сервера iOS MDM из резервной копии. Восстановление данных осуществляется на основании информации, представленной в папке `BACKUP_PATH`.
- `-path BACKUP_PATH` — указать локальный путь к папке с данными резервной копии.
- `-pwd PASSWORD` — установить пароль для резервной копии.

# Развертывание системы управления iOS-устройствами

Kaspersky Secure Mobility Management позволяет управлять мобильными устройствами под управлением iOS. В этом разделе описано развертывание системы управления iOS-устройствами.

# О режимах работы iOS-устройств

Режим работы устройства зависит от того, кому принадлежит мобильное устройство (личное или корпоративное) и требований корпоративной безопасности. Вы можете выбрать наиболее подходящий для компании режим работы, а также использовать несколько режимов одновременно.

Для iOS-устройств доступны следующие режимы работы:

- Базовая защита
- Базовый контроль
- Расширенный контроль

## Базовая защита

*Базовая защита* - это режим работы для личных или корпоративных iOS-устройств. Этот режим работы позволяет защищать от веб-угроз и обнаруживать jailbreak на устройствах с помощью приложения Kaspersky Protection для iOS.

## Базовый контроль

*Базовый контроль* - это режим работы для личных и корпоративных iOS-устройств. Этот режим работы позволяет защищать устройства и выполнять базовое управление ими.

В этом режиме пользователю разрешено использовать персональный Apple ID, работать с любыми приложениями и хранить персональные данные на устройстве. Вы можете настроить параметры политики для контроля доступа пользователей к корпоративным ресурсам и управления другими требованиями безопасности.

Для управления iOS-устройствами в режиме "Базовый контроль" необходимо установить и настроить Сервер iOS MDM.

### Расширенный контроль

*Расширенный контроль* - это режим работы для корпоративных iOS-устройств. Этот режим работы предлагает наиболее широкий набор параметров для настройки в политике по сравнению с другими режимами, например:

- Отправка дополнительных команд для управления настройками Bluetooth, обновления операционной системы, определения местоположения устройства или воспроизведения звукового сигнала в Режиме пропажи.
- Управление дополнительными ограничениями:
  - Ограничения сети (запрет на изменение настроек Режима модема и создание конфигураций VPN, принудительное включение Wi-Fi и подключение к разрешенным сетям, запрет на изменение настроек Bluetooth).
  - Ограничения приложений (например, запрет на установку приложений из Apple Configurator и iTunes).
  - Запрет доступа к USB-устройствам в приложении "Файлы" и отключение доступа к USB-устройствам, когда устройство заблокировано.
- Настройка расширенных параметров Контроля приложений (например, создание собственных списков разрешенных и запрещенных приложений).
- Настройка Веб-Контроля.
- Настройка HTTP-прокси для отслеживания интернет-трафика на устройстве в корпоративной сети.

Для управления iOS-устройствами в режиме "Расширенный контроль" необходимо установить и настроить Сервер iOS MDM, а также перевести устройства в управляемый режим в Apple Configurator. Дополнительная информация о работе с Apple Configurator приведена на сайте Службы технической поддержки Apple.

## Об управляющих профилях

*Управляющий профиль* - это профиль, который содержит параметры для подключения iOS-устройств к Kaspersky Security Center. После установки управляющего профиля и синхронизации устройства с Сервером iOS MDM, устройство становится управляемым (iOS MDM-устройством). Управление iOS MDM-устройствами осуществляется через службу уведомлений Apple Push (APNs).

С помощью управляющего профиля можно выполнять следующие действия:

- Удаленно настраивать параметры iOS MDM-устройств с помощью политик.
- Отправлять команды на iOS MDM-устройства.
- Удаленно устанавливать приложения "Лаборатории Касперского" и сторонние приложения.

Развертывание управляющего профиля осуществляется через Kaspersky Security Center Web Console с помощью Мастера подключения мобильного устройства. Пользователь устанавливает управляющий профиль после получения письма с информацией для подключения мобильного устройства к Kaspersky Security Center. Дополнительной подготовки управляющего профиля к работе не требуется.

Перед установкой управляющего профиля необходимо развернуть систему управления iOS-устройствами.

# Развертывание Kaspersky Protection для iOS

В этом разделе содержится общий обзор приложения Kaspersky Protection для iOS и процесса его активации.

Подробная информация о возможностях Kaspersky Protection для iOS, установке, обновлении и удалении приложения приведена в разделе Использование приложения Kaspersky Protection для iOS.

## О Kaspersky Protection для iOS

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

Kaspersky Protection для iOS предоставляет следующие ключевые функции:

- *Веб-Защита*. Позволяет блокировать вредоносные веб-сайты, цель которых – распространить вредоносный код. Веб-Защита также блокирует поддельные (фишинговые) сайты, цель которых – украсть конфиденциальные данные пользователя (например, пароли от интернет-банка или платежных систем) и получить доступ к его финансовым счетам. Веб-Защита проверяет сайты перед открытием, используя облачную службу Kaspersky Security Network. После сканирования Веб-Защита разрешает загрузку надежных сайтов и блокирует вредоносные. Этот компонент можно настроить в Kaspersky Security Center Web Console, указав соответствующие параметры политики.

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

## Активация Kaspersky Protection для iOS

В Kaspersky Security Center лицензия может распространяться на различные группы функциональности. Для полноценного функционирования приложения Kaspersky Protection для iOS необходимо, чтобы приобретенная организацией лицензия на Kaspersky Security Center распространялась на функциональность Управление мобильными устройствами.

Подробная информация о вариантах лицензирования приведена в разделе О лицензии.

Активация приложения Kaspersky Protection для iOS на мобильном устройстве осуществляется путем предоставления приложению корректной информации о лицензии. Информация о лицензии передается на мобильное устройство вместе с параметрами политики 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 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. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Нажмите на кнопку **Лицензия**.

4. В раскрывающемся списке в открывшемся окне 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 Protection для iOS не сможет его обработать, потому что не поддерживает такой формат активации. Чтобы активировать Kaspersky Protection для iOS, нужно добавить код активации в Kaspersky Security Center.

   Вы можете заменить существующий ключ активации на мобильном устройстве, если он отличается от ключа, выбранного в раскрывающемся списке. Для этого установите флажок **Заменить ключ, если на устройствах добавлен другой ключ**.

   Однако на некоторых iOS-устройствах существующий ключ активации может замениться на новый позже, чем ожидается, если пользователь закрыл Kaspersky Protection для iOS смахиванием из переключателя приложений. Чтобы принудительно заменить ключ активации, пользователю необходимо повторно открыть приложение. Подробная информация об ограничениях и рекомендациях по оптимизации выполнения фоновых задач приведена в разделе Известные проблемы Kaspersky Protection для iOS.

5. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Приложение будет активировано после очередной синхронизации устройства с Сервером администрирования.

Пользователь также может обратиться к администратору за кодом активации и ввести его вручную.

# Развертывание системы управления по протоколу iOS MDM

Управление iOS-устройствами в режимах "Базовый контроль" и "Расширенный контроль" осуществляется через протокол iOS MDM. Чтобы развернуть систему управления мобильными устройствами с использованием протокола iOS MDM и подключить iOS-устройства к Kaspersky Security Center, выполните следующие шаги:

1. **Развертывание Сервера iOS MDM**
2. **Получение APNs-сертификата**
3. **Установка APNs-сертификата на Сервер iOS MDM**
4. **Подключение iOS-устройств к Kaspersky Security Center**

## Развертывание Сервера iOS MDM

Сервер iOS MDM - это компонент Kaspersky Secure Mobility Management, который позволяет iOS MDM-устройствам подключаться к Kaspersky Security Center и упрощает управление ими через службу уведомлений Apple Push (APNs) путем установки на устройства управляющих профилей.

Сервер iOS MDM принимает входящие соединения от мобильных устройств на свой TLS-порт (по умолчанию порт 443) и управляется со стороны Kaspersky Security Center с помощью Агента администрирования. Агент администрирования устанавливается локально на устройстве, на котором будет развернут Сервер iOS MDM.

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

Обратите внимание, что рекомендуемое максимальное количество мобильных устройств, которыми можно управлять через Сервер iOS MDM, составляет 50 000. С целью уменьшения нагрузки устройства можно распределить между несколькими серверами с установленным Сервером iOS MDM.

## Настройка инсталляционного пакета Сервера iOS MDM

Перед установкой Сервера iOS MDM необходимо настроить свойства его инсталляционного пакета.

Инсталляционный пакет Сервера iOS MDM - это архив, содержащий файлы, необходимые для установки Сервера, в зависимости от менеджера пакетов и архитектуры: `kliosmdm-<architecture>-<version>-<package manager>_<language>.tar.gz`

*Чтобы настроить инсталляционный пакет Сервера iOS MDM:*

1. В главном окне Kaspersky Security Center Web Console выберите **Операции** > **Хранилища** > **Инсталляционные пакеты**.
2. В открывшемся окне выберите инсталляционный пакет Сервера iOS MDM, который вы хотите настроить.

   Откроется окно свойств инсталляционного пакета.

3. На вкладке **Параметры** укажите настройки Сервера iOS MDM.

   a. В блоке настроек **Параметры подключения** укажите следующие значения:

   Рекомендуется использовать значения по умолчанию.

   - **Внешний порт подключения к службе iOS MDM**. В этом поле 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 устройств к Серверу iOS MDM по умолчанию используется порт 443. Если порт 443 уже используется другой службой или приложением, вместо него можно использовать, например, порт 9443.

     Порт 2197 используется Сервером iOS MDM 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.

   - **Порт подключения к Агенту администрирования**. В этом поле укажите порт для подключения службы iOS MDM к Агенту администрирования. Порт по умолчанию: 9799.

   - **Локальный порт подключения к службе iOS MDM**. В этом поле укажите локальный порт подключения Агента администрирования к службе iOS MDM. Порт по умолчанию: 9899.

   b. В блоке настроек **Адрес Сервера iOS MDM** укажите адрес устройства, на который будет установлен Сервер iOS MDM. Этот адрес будет использоваться для подключения управляемых мобильных устройств к службе iOS MDM. Устройство должно быть доступно для подключения iOS MDM-устройств.

   Выберите один из следующих вариантов:

   - **Использовать FQDN-имя устройства**. Будет использоваться полное доменное имя (FQDN) устройства.

   - **Использовать указанный адрес**. Введите адрес устройства вручную.

     Не включайте в строку с адресом URL-схему и номер порта. Эти значения будут добавлены автоматически.

4. Нажмите **Сохранить**.

Свойства инсталляционного пакета Сервера iOS MDM настроены. Теперь вы можете установить Сервер iOS MDM с указанными настройками.

## Установка Сервера iOS MDM с помощью задачи удаленной установки

Kaspersky Security Center Web Console позволяет установить Сервер iOS MDM с помощью задачи удаленной установки. Эта задача создается и назначается устройствам (до 1000 устройств) с помощью соответствующего мастера. С помощью мастера можно установить Сервер iOS MDM в группе администрирования, на устройствах с определенными IP-адресами или на выбранных управляемых устройствах.

Обратите внимание, что вы не сможете указать настройки Сервера iOS MDM во время установки. Эти параметры настраиваются в свойствах инсталляционного пакета Сервера iOS MDM.

Перед установкой Сервера iOS MDM на устройстве убедитесь, что установлены плагины Kaspersky Mobile Devices Protection and Management и Параметры Сервера iOS MDM.

*Чтобы установить Сервер iOS MDM с помощью задачи удаленной установки:*

1. Установите Агент администрирования на устройство, на котором будет развернут Сервер iOS MDM.
2. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Серверы iOS MDM**.
3. Нажмите **Установить**.

   Запустится Мастер создания задачи. Для продолжения работы мастера нажмите **Далее**.
4. В открывшемся окне **Параметры новой задачи**:
   a. В поле **Название задачи** при необходимости укажите произвольное имя задачи (имя по умолчанию - "Установить Сервер iOS MDM").
   b. В блоке настроек **Устройства, которым будет назначена задача** выберите **Задать адреса устройств вручную или импортировать из списка**. Вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.
5. На шаге **Область действия задачи**:
   a. Нажмите **Добавить устройства**.
   b. В открывшемся окне из выпадающего списка выберите **Выбрать устройства, обнаруженные в сети Сервером администрирования**.
   c. Укажите устройства или выборку устройств.
   d. Нажмите **Добавить**.

   Добавленные устройства отобразятся в таблице.
6. На шаге **Инсталляционные пакеты** укажите следующие параметры:
   a. В поле **Выбор инсталляционного пакета** выберите настроенный инсталляционный пакет Сервера iOS MDM.
   b. В поле **Выбор Агент администрирования** выберите установленный Агент администрирования.

c. В блоке настроек **Принудительно скачать инсталляционный пакет** выберите **С помощью Агента администрирования**, чтобы доставить на устройства файлы, необходимые для установки Сервера iOS MDM, с помощью Агента администрирования.

d. В поле **Максимальное количество одновременных загрузок** укажите максимально допустимое количество устройств, на которые Сервер администрирования может одновременно передавать файлы.

e. В поле **Максимальное количество попыток установок** укажите максимально допустимое количество запусков приложения установки.

f. Укажите дополнительные параметры:

- Установите флажок **Не устанавливать приложение, если оно уже установлено**. Приложение не будет устанавливаться заново, если оно уже установлено на устройстве.

- Установите флажок **Предварительно проверять тип операционной системы перед загрузкой**. Перед передачей файлов на устройства Kaspersky Security Center проверит, применимы ли параметры утилиты установки к операционной системе устройства. Если параметры не применимы, Kaspersky Security Center не передаст файлы и не попытается установить приложение. Например, чтобы установить некоторые приложения с устройств группы администрирования, в которую входят устройства с различными операционными системами, вы можете назначить задачу установки группе администрирования, а затем включить этот параметр, чтобы пропускать устройства с операционной системой, отличной от требуемой.

7. На следующем шаге мастера вам будет предложено указать, требуется ли перезагрузка устройства при установке приложения. Выберите **Не перезагружать устройство** или пропустите этот шаг, так как он не применим к операционной системе Linux.

8. На шаге **Выбор учетных записей для доступа к устройствам** выберите **Учетная запись не требуется (Агент администрирования уже установлен)**. Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор приложения. Задача запускается под учетной записью, под которой работает служба Сервера администрирования. Если Агент администрирования не установлен на устройствах, вариант недоступен.

9. На шаге **Завершение создания задачи** нажмите **Готово**, чтобы создать задачу и закрыть мастер.

Сервер iOS MDM установлен с помощью задачи удаленной установки.

При переустановке Сервера iOS MDM с нуля необходимо удалить папку /var/opt/kaspersky/iosmdm на устройстве с установленным Сервером iOS MDM. Если папка не была удалена, при установке будет автоматически использован сертификат старого Сервера iOS MDM, а резервный сертификат будет выписан на новый адрес Сервера iOS MDM, если он был изменен.

Если необходимо обновить Сервер iOS MDM без переустановки с нуля, удалять указанную папку не требуется.

## Локальная установка Сервера iOS MDM на устройстве с помощью инсталляционного пакета

Kaspersky Security Center Web Console позволяет установить Сервер iOS MDM на устройстве локально с помощью инсталляционного пакета, то есть без интерактивного ввода параметров установки.

Перед установкой Сервера iOS MDM на устройстве убедитесь, что установлены плагины Kaspersky Mobile Devices Protection and Management и Параметры Сервера iOS MDM.

*Чтобы установить и настроить Сервер iOS MDM вручную на локальном устройстве:*

1. Установите Сервер iOS MDM:

   a. Прочитайте Лицензионное соглашение. Используйте команду ниже, только если вы поняли и принимаете условия Лицензионного соглашения.

   b. В зависимости от вашей операционной системы выполните одну из следующих команд для запуска установочного файла:

      a. Для Debian:
      ```
      apt install /<path>/kliosmdm_<version_number>_amd64.deb
      ```

      b. Для Red Hat Enterprise Linux:
      ```
      yum install /<path>/kliosmdm_<version_number>.x86_64.rpm -y
      ```

      Сервер iOS MDM установлен. Установщик предлагает начать процедуру установки, выполнив скрипт postinstall.pl.

2. Настройте Сервер iOS MDM одним из способов:

   a. Настройка с параметрами *postinstall*, заданными интерактивным пошаговым мастером:

      a. Выполните следующую команду:
      ```
      /opt/kaspersky/iosmdm/lib/bin/setup/postinstall.pl
      ```

   b. Настройка с ключевыми аргументами, указанными в качестве параметров *postinstall*:

      a. Выполните следующую команду:
      ```
      opt/kaspersky/bin/postinstall.pl -- <params>
      ```

      где `<params>` - это один из параметров, указанных в таблице *Параметров установки Сервера iOS MDM* ниже.

Имена и возможные значения параметров, которые можно использовать при установке Сервера iOS MDM, приведены в таблице. Параметры можно указывать в любом порядке.

| Имя параметра | Описание параметра | Значения |
|---|---|---|
| EULA_ACCEPTED | Согласие с условиями Лицензионного соглашения.<br>Этот параметр является обязательным. | • *1* - Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Лицензионного соглашения<br>• *Другое значение или не задано* - не согласны с условиями Лицензионного соглашения (установка не выполняется) |
| DONT_USE_ANSWER_FILE | Использовать файл ответов в формате TXT с параметрами установки Сервера iOS MDM или нет.<br>Файл TXT идет в комплекте с инсталляционным пакетом или находится на Сервере администрирования. Дополнительно путь к файлу указывать не нужно.<br>Этот параметр является обязательным. | • *1* - не использовать файл ответов с параметрами<br>• *Другое значение или не задано* - использовать файл ответов с параметрами |
| CONNECTORPORT | Локальный порт для подключения службы iOS MDM к Агенту администрирования.<br>Порт по умолчанию: 9799.<br>Этот параметр является необязательным. | Числовое значение - *9799* |
| LOCALSERVERPORT | Локальный порт для подключения Агента администрирования к службе iOS MDM.<br>Порт по умолчанию: 9899.<br>Этот параметр является необязательным. | Числовое значение - *9899* |
| EXTERNALSERVERPORT | Порт для подключения устройства к Серверу iOS MDM.<br>Порт по умолчанию: 443.<br>Этот параметр является необязательным. | Числовое значение - *443* |
| EXTERNAL_SERVER_URL | Внешний адрес устройства, на котором будет установлен Сервер iOS MDM. Этот адрес будет использоваться для подключения управляемых мобильных устройств к службе iOS MDM. Устройство должно быть доступно для подключения iOS MDM-устройств.<br>Адрес не должен включать URL-схему и номер порта; эти значения будут добавлены автоматически.<br>Этот параметр является необязательным. | Полное доменное имя устройства (FQDN) - *example.fqdn.com* |

Пример:
```
/opt/kaspersky/bin/postinstall.pl --EULA 1 --DONT_USE_ANSWER_FILE 1 --EXTERNALSERVERPORT 9443 --CONNECTORPORT 9799
```

*Чтобы установить и настроить Сервер iOS MDM автоматически в тихом режиме с использованием файла ответов:*

*Файл ответов* - это текстовый файл, содержащий пользовательский набор параметров установки (переменные и соответствующие им значения).

1. Создайте файл ответов (в формате TXT) в каталоге, где будет выполняться установка: `/tmp/answers.txt`.
2. Укажите требуемые значения в файле ответов:
   - EULA_ACCEPTED=1

     Согласие с условиями Лицензионного соглашения.
   - KLIOSMDM_AUTOINSTALL=1

     Использование файла ответов в формате TXT с параметрами установки Сервера iOS MDM.

- EXTERNALSERVERPORT=443

  Порт для подключения устройства к Серверу iOS MDM.

- CONNECTORPORT=9799

  Локальный порт для подключения службы iOS MDM к Агенту администрирования.

- LOCALSERVERPORT=9899

  Локальный порт для подключения Агента администрирования к службе iOS MDM.

- EXTERNAL_SERVER_URL=example.fqdn.com

  Внешний адрес устройства, на котором будет установлен Сервер iOS MDM.

3. Задайте значение переменной среды KLAUTOANSWERS, введя полное имя файла ответов (включая путь), например, следующим образом: `export KLAUTOANSWERS=/tmp/answers.txt`.

4. Запустите установку Сервера iOS MDM.

Сервер iOS MDM установлен и настроен автоматически в тихом режиме с использованием файла ответов.

При переустановке Сервера iOS MDM с нуля необходимо удалить папку /var/opt/kaspersky/iosmdm на устройстве с установленным Сервером iOS MDM. Если папка не была удалена, при установке будет автоматически использован сертификат старого Сервера iOS MDM, а резервный сертификат будет выписан на новый адрес Сервера iOS MDM, если он был изменен.

Если необходимо обновить Сервер iOS MDM без переустановки с нуля, удалять указанную папку не требуется.

## Обновление Сервера iOS MDM с помощью задачи удаленной установки или локально

Kaspersky Security Center Web Console позволяет обновить Сервер iOS MDM с помощью задачи удаленной установки или локально на устройстве.

Обратите внимание, что вы не сможете указать настройки Сервера iOS MDM во время обновления. Эти параметры настраиваются в свойствах инсталляционного пакета Сервера iOS MDM.

*Чтобы обновить Сервер iOS MDM с помощью задачи удаленной установки:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Серверы iOS MDM**.

2. Нажмите **Обновить**.

   Запустится Мастер создания задачи. Для продолжения работы мастера нажмите **Далее**.

3. В открывшемся окне **Параметры новой задачи**:

   a. В поле **Название задачи** при необходимости укажите произвольное имя задачи (имя по умолчанию - "Обновить Сервер iOS MDM").

   b. В блоке настроек **Устройства, которым будет назначена задача** отобразится устройство, на котором установлен Сервер iOS MDM.

4. На шаге **Инсталляционные пакеты** укажите следующие параметры:

   a. В поле **Выбор инсталляционного пакета** выберите настроенный инсталляционный пакет Сервера iOS MDM.

   b. В блоке настроек **Принудительно скачать инсталляционный пакет** выберите **С помощью Агента администрирования**, чтобы доставить на устройства файлы, необходимые для обновления Сервера iOS MDM, с помощью Агента администрирования.

   c. В поле **Максимальное количество одновременных загрузок** укажите максимально допустимое количество клиентских устройств, на которые Сервер администрирования может одновременно передавать файлы.

   d. В поле **Максимальное количество попыток установок** укажите максимально допустимое количество запусков приложения установки.

   e. Укажите дополнительные параметры:

   - Установите флажок **Не устанавливать приложение, если оно уже установлено**. Приложение не будет устанавливаться заново, если оно уже установлено на устройстве.

   - Установите флажок **Предварительно проверять тип операционной системы перед загрузкой**. Перед передачей файлов на устройства Kaspersky Security Center проверит, применимы ли параметры утилиты установки к операционной системе устройства. Если параметры не применимы, Kaspersky Security Center не передаст файлы и не попытается установить приложение. Например, чтобы установить некоторые приложения с устройств группы администрирования, в которую входят устройства с различными операционными системами, вы можете назначить задачу установки группе администрирования, а затем включить этот параметр, чтобы пропускать устройства с операционной системой, отличной от требуемой.

5. На следующем шаге мастера вам будет предложено указать, требуется ли перезагрузка устройства при установке приложения. Выберите **Не перезагружать устройство** или пропустите этот шаг, так как он не применим к операционной системе Linux.

6. На шаге **Выбор учетных записей для доступа к устройствам** выберите **Учетная запись не требуется (Агент администрирования уже установлен)**. Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор приложения. Задача запускается под учетной записью, под которой работает служба Сервера администрирования. Если Агент администрирования не установлен на устройствах, вариант недоступен.

7. На шаге **Завершение создания задачи** нажмите **Готово**, чтобы создать задачу и закрыть мастер.

Сервер iOS MDM обновлен с помощью задачи удаленной установки.

Чтобы обновить Сервер iOS MDM локально, выполните действия, описанные в разделе Локальная установка Сервера iOS MDM на устройстве с помощью инсталляционного пакета, с использованием более новой версии инсталляционного пакета.

## Удаление Сервера iOS MDM с помощью задачи удаленной деинсталляции

Kaspersky Security Center Web Console позволяет удалить Сервер iOS MDM с помощью задачи удаленной деинсталляции.

Перед удалением Сервера iOS MDM убедитесь, что инсталляционный пакет Сервера iOS MDM создан и добавлен в хранилище Сервера администрирования (**Операции** > **Хранилища** > **Инсталляционные пакеты**).

*Чтобы удалить Сервер iOS MDM:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Серверы iOS MDM**.

2. Выберите Сервер iOS MDM, который вы хотите удалить, и нажмите **Удалить**.

   Запустится Мастер создания задачи. Следуйте указаниям мастера, как описано в справке Kaspersky Security Center.

## Просмотр списка установленных Серверов iOS MDM и настройка их параметров

Kaspersky Security Center Web Console позволяет просматривать список установленных Серверов iOS MDM и настраивать их.

*Чтобы просмотреть установленные Серверы iOS MDM:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Серверы iOS MDM**.

2. В открывшемся списке установленных Серверов iOS MDM:

   a. Чтобы установить Сервер iOS MDM, нажмите **Установить**.

   b. Чтобы обновить Сервер iOS MDM, нажмите **Обновить**.

   c. Чтобы удалить Сервер iOS MDM, нажмите **Удалить**.

   d. Чтобы просмотреть или настроить параметры Сервера iOS MDM, выполните одно из следующих действий:

   - Установите флажок рядом с Сервером iOS MDM, параметры которого вы хотите просмотреть или настроить, и нажмите **Изменить параметры**.

     В окне настроек Сервера iOS MDM откроется вкладка **Параметры приложения**.

   - Нажмите на имя Сервера iOS MDM, параметры которого вы хотите просмотреть или настроить.

     В открывшемся окне настроек Сервера iOS MDM перейдите на вкладку **Параметры приложения**.

*Чтобы просмотреть или настроить параметры Сервера iOS MDM:*

1. Перейдите на вкладку **Параметры приложения** настроек Сервера iOS MDM по инструкции, указанной выше.

   a. В разделе **Общие** вы можете просмотреть общие свойства Сервера iOS MDM.

   - **Имя**. Пользовательское имя Сервера iOS MDM.
   - **Версия**. Версия установленного Сервера iOS MDM.
   - **Дата изменения**. Дата и время последнего обновления или изменения Сервера iOS MDM.
   - **Имя устройства**. Имя устройства, на котором установлен Сервер iOS MDM.

- **Путь на устройстве**. Путь к Серверу iOS MDM на устройстве, на котором он установлен.

  Вы не можете изменять настройки в этом разделе.

b. В разделе **Прокси-сервер для APNs** вы можете указать следующие настройки для службы уведомлений Apple Push (APNs):

- **Адрес**. Адрес прокси-сервера APNs.
- **Порт**. Порт прокси-сервера APNs.
- **Имя пользователя**. Имя пользователя прокси-сервера APNs.
- **Пароль**. Пароль прокси-сервера APNs.

  Если доступ к APNs со стороны службы iOS MDM будет предоставляться через прокси-сервер, опция **Использовать прокси-сервер для подключения к APNs** должна быть включена.

  Подробная информация о прокси-сервере APNs приведена в разделе Настройка доступа к службе уведомлений Apple Push.

c. В разделе **Сертификаты** вы можете управлять сертификатами, необходимыми для работы Сервера iOS MDM.

- **Сертификат службы уведомлений Apple Push (APNs)**. Сертификат APNs подписывается Apple и позволяет использовать службу уведомлений Apple Push. С помощью этой службы Сервер iOS MDM может управлять iOS-устройствами. Подробная информация об APNs-сертификате приведена в разделе Получение или обновление APNs-сертификата.
- **Сертификат Сервера iOS MDM**. Сертификат Сервера iOS MDM используется для установления соединения и проверки доверия между iOS-устройствами и Сервером iOS MDM.
- **Резервный сертификат Сервера iOS MDM**. Резервный сертификат Сервера iOS MDM обеспечивает бесперебойное переключение iOS-устройств после истечения срока действия основного сертификата Сервера iOS MDM. Подробная информация об APNs-сертификате приведена в разделе Настройка резервного сертификата Сервера iOS MDM.
- **Корневой сертификат Сервера iOS MDM**. Корневой сертификат Сервера iOS MDM хранится и управляется в Kaspersky Security Center. Он передается на Сервер iOS MDM при подключении к Kaspersky Security Center и используется для выписки мобильных сертификатов средствами Kaspersky Security Center для аутентификации iOS MDM-устройств по протоколу mTLS.

d. В разделе **Параметры подключения** вы можете просмотреть и настроить параметры подключения устройств к Серверу iOS MDM.

- В блоке настроек **Синхронизация** вы можете включить или выключить синхронизацию управляемых устройств с Сервером iOS MDM и указать **Период синхронизации (мин)**.
- В блоке настроек **Локальная точка доступа** вы можете указать **Порт подключения к Агенту администрирования** (порт для подключения iOS-устройств к Агенту администрирования) и **Локальный порт подключения к службе iOS MDM** (локальный порт для подключения Агента администрирования к службе iOS MDM). Подробная информация об этих параметрах приведена в разделе Настройка инсталляционного пакета Сервера iOS MDM.
- В блоке настроек **Внешняя точка доступа** вы можете указать **Внешний порт подключения к службе iOS MDM** (внешний порт для подключения мобильных устройств к службе iOS MDM).
- В блоке настроек **Управляющий профиль** вы можете указать свойства инсталляционного профиля. Заполните поля **Имя профиля** (обязательное поле), **Компания** и **Описание профиля**.

  Обратите внимание, что параметры в этом разделе применяются к новым подключенным iOS MDM-устройствам или к ранее подключенным устройствам при обновлении их мобильных сертификатов.

- В разделе **Конфигурационные профили** вы можете просматривать и управлять конфигурационными профилями, которые используются для централизованного управления iOS MDM-устройствами и ограничения их функций. Подробная информация об управлении конфигурационными профилями приведена в разделах Добавление конфигурационного профиля, Установка конфигурационного профиля на устройство и Удаление конфигурационного профиля с устройства.

## Настройка сертификата Сервера iOS MDM

Сертификат Сервера iOS MDM используется для установления соединения и проверки доверия между iOS MDM-устройством и Сервером iOS MDM.

Сертификат Сервера iOS MDM выпускается Kaspersky Security Center автоматически при первоначальном развертывании Сервера iOS MDM и устанавливается на устройстве с развернутым Сервером iOS MDM. Если вы хотите использовать сертификат, выданный вашим центром сертификации, вам необходимо указать пользовательский файл сертификата, который будет использоваться в качестве сертификата Сервера iOS MDM.

Если вы укажете пользовательский сертификат Сервера iOS MDM, кнопка **Выпустить** для резервного сертификата Сервера iOS MDM станет недоступной. В этом случае резервный сертификат необходимо указать вручную, нажав кнопку **Установить**.

*Чтобы указать пользовательский сертификат Сервера iOS MDM:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Серверы iOS MDM**. В открывшемся списке Серверов iOS MDM выберите Сервер iOS MDM, параметры которого вы хотите настроить.
2. В окне параметров Сервера iOS MDM выберите **Параметры приложения**.

3. Выберите вкладку **Сертификаты**.

   a. В блоке настроек **Сертификат Сервера iOS MDM** нажмите **Установить**.

   b. В открывшемся окне File Explorer укажите файл сертификата в формате PEM, PFX или P12 и нажмите **Открыть**.

   Убедитесь, что устанавливаемый вами сертификат соответствует следующим требованиям безопасности:

   - указано Общее имя (CN);
   - указано альтернативное имя субъекта (SAN) типа DNS-имени;
   - указан издатель сертификата;
   - указана правильная дата истечения срока действия сертификата;
   - цепочка сертификатов завершена;
   - расширенное использование ключа (EKU) соответствует XKU_SSL_SERVER (1.3.6.1.5.5.7.3.1 serverAuth);
   - размер ключа RSA в цепочке сертификатов составляет не менее 2048 бит;
   - размер ключа RSA корневого сертификата составляет не менее 4096 бит;
   - алгоритм хеширования в цепочке сертификатов принадлежит к семейству SHA-2.

   c. В открывшемся окне **Установка сертификата** введите пароль сертификата и нажмите **Установить**.

   d. Нажмите **Сохранить**.

Пользовательский сертификат Сервера iOS MDM установлен. Информация о сертификате отображена в блоке настроек **Сертификат Сервера iOS MDM**.

Если вам нужно обновить сертификат Сервера iOS MDM, мы рекомендуем использовать резервный сертификат Сервера iOS MDM без перевыпуска основного.

Если вы все же хотите перевыпустить сертификат, сначала остановите программы Kaspersky Security Center, Агент администрирования и Сервер iOS MDM, удалите сертификат kliosmdmserver_cert.pem и его пароль (строка SrvCertPwd= в файле kliosmdm.ini), а затем перезапустите Kaspersky Security Center, Агент администрирования и Сервер iOS MDM. Обратите внимание, что эти действия приведут к потере соединения Сервера iOS MDM с устройствами.

## 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.

Обратите внимание, что резервный сертификат Сервера iOS MDM не выпускается автоматически, если вы используете пользовательский сертификат Сервера iOS MDM. Если вы используете пользовательский сертификат, мы рекомендуем вам указать резервный сертификат при установке Сервера iOS MDM или не позднее, чем за 30 дней до окончания срока действия существующего сертификата Сервера iOS MDM.

Если срок действия сертификата истек, а резервный сертификат не указан, связь между Сервером iOS MDM и iOS MDM-устройствами будет потеряна. В этом случае для повторного подключения устройств необходимо указать новый сертификат и переустановить управляющие профили на каждом из управляемых устройств.

*Чтобы выпустить резервный сертификат Сервера iOS MDM или указать пользовательский резервный сертификат в качестве резервного:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Серверы iOS MDM**. В открывшемся списке Серверов iOS MDM выберите Сервер iOS MDM, параметры которого вы хотите настроить.

2. В окне параметров Сервера iOS MDM выберите **Параметры приложения**.

3. Выберите вкладку **Сертификаты**.

4. В блоке настроек **Резервный сертификат Сервера iOS MDM** выполните одно из следующих действий:

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

     a. Нажмите **Выпустить**.

     Если указан пользовательский сертификат Сервера iOS MDM, кнопка **Выпустить** для резервного сертификата Сервера iOS MDM будет недоступна. В этом случае резервный сертификат необходимо указать вручную, нажав кнопку **Установить**.

     b. В открывшемся окне **Применить резервный сертификат Сервера iOS MDM** выберите один из двух вариантов даты, когда необходимо применить резервный сертификат:

        - Если вы хотите применить резервный сертификат при истечении срока действия текущего сертификата, выберите параметр **Когда истечет срок действия основного сертификата**.

        - Если вы хотите применить резервный сертификат до истечения срока действия текущего сертификата, выберите параметр **После указанного периода (дни)**. 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 **OK**.

Самозаверенный сертификат Сервера iOS MDM выпущен и указан в качестве резервного сертификата Сервера iOS MDM.

Обратите внимание, что при указании даты, когда должен быть применен резервный сертификат, сертификат будет выдан до того, как вы сохраните изменения в разделе **Сертификаты**. Если вы хотите выпустить новый резервный сертификат, откройте параметры Сервера iOS MDM, удалите ранее выпущенный резервный сертификат, нажав **Удалить**, и выпустите новый резервный сертификат, следуя инструкции выше.

- Если вы планируете использовать пользовательский сертификат, выпущенный вашим центром сертификации:

  a. Нажмите **Установить**.

  b. В открывшемся окне File Explorer укажите файл сертификата в формате PEM, PFX или P12 и нажмите **Открыть**.

  Убедитесь, что устанавливаемый вами сертификат соответствует следующим требованиям безопасности:

  - указано альтернативное имя субъекта (SAN) типа DNS-имени;
  - указан правильный издатель сертификата;
  - указана правильная дата истечения срока действия сертификата;
  - цепочка сертификатов завершена;
  - расширенное использование ключа (EKU) соответствует XKU_SSL_SERVER (1.3.6.1.5.5.7.3.1 serverAuth);
  - размер ключа RSA в цепочке сертификатов составляет не менее 2048 бит;
  - размер ключа RSA корневого сертификата составляет не менее 4096 бит;
  - алгоритм хеширования в цепочке сертификатов принадлежит к семейству SHA-2.

  c. В открывшемся окне **Установка сертификата** введите пароль сертификата и нажмите **Установить**.

  d. Нажмите **Сохранить**.

Пользовательский сертификат указан как резервный сертификат Сервера iOS MDM.

Обратите внимание, что при указании даты, когда должен быть применен резервный сертификат, сертификат будет выдан до того, как вы сохраните изменения в разделе **Сертификаты**. Если вы хотите выпустить новый резервный сертификат, откройте параметры Сервера iOS MDM, удалите ранее выпущенный резервный сертификат, нажав **Удалить**, и выпустите новый резервный сертификат, следуя инструкции выше.

Резервный сертификат Сервера iOS MDM указан. Информация о сертификате отображена в блоке настроек **Резервный сертификат Сервера iOS MDM**.

## Получение или обновление APNs-сертификата

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

Если у вас уже есть APNs-сертификат, попробуйте обновить его вместо получения нового. При замене существующего APNs-сертификата на новый Kaspersky Security Center теряет возможность управления ранее подключенными iOS MDM-устройствами.

*Чтобы выпустить или обновить APNs-сертификат:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Серверы iOS MDM**. В открывшемся списке Серверов iOS MDM выберите Сервер iOS MDM, параметры которого вы хотите настроить.
2. В окне параметров Сервера iOS MDM выберите **Параметры приложения**.
3. Выберите вкладку **Сертификаты**.
4. В разделе настроек **Сертификат службы уведомлений Apple Push (APNs)** нажмите **Выпустить или обновить**.

   Откроется мастер выпуска и обновления APNs-сертификата. Нажмите **Начать** и продолжайте работу мастера с помощью кнопок **Назад** и **Далее**.

   После создания запроса Certificate Signing Request (CSR-запроса) на первом шаге мастера его закрытый ключ сохраняется в оперативной памяти устройства. Соответственно, все шаги должны быть выполнены без перерыва в рамках одной сессии мастера.

### Шаг 1. Создание запроса Certificate Signing Request (CSR)

*Чтобы создать CSR-запрос:*

a. Укажите информацию, необходимую для формирования файла запроса: **Общее имя (CN)**, **Компания (O)**, **Отдел (OU)**, **Город (L)**, **Регион (S)**, **Страна (C)**.

b. Нажмите **Скачать**.

   После сохранения изменений будет создан CSR-файл, а закрытый ключ сертификата сохранится в памяти устройства.

## Шаг 2. Подписание CSR-файла

*На этом шаге отправьте CSR-файл, полученный на предыдущем этапе мастера, на заверение в "Лабораторию Касперского":*

a. Нажмите **Перейти на портал Kaspersky CompanyAccount**.

b. Отправьте сформированный CSR-файл на подписание в "Лабораторию Касперского".

> Обратите внимание, что подписание CSR-файла возможно только после загрузки на портал ключа, позволяющего использовать решение для управления мобильными устройствами.

c. После успешной обработки запроса вы получите файл CSR-запроса, заверенный "Лабораторией Касперского".

d. Сохраните полученный файл.

## Шаг 3. Получение открытого ключа APNs-сертификата

На этом шаге выполните одно из следующих действий в зависимости от того, необходимо ли выпустить новый сертификат или обновить существующий:

*Чтобы выпустить новый сертификат:*

a. Нажмите **Перейти на портал Apple**.

b. Авторизуйтесь на портале Apple с корпоративным Apple ID.

> Использовать личный Apple ID не рекомендуется. Создайте отдельный Apple ID для корпоративных целей. Привяжите созданный Apple ID к почтовому ящику организации, а не отдельного сотрудника.

c. Загрузите подписанный CSR-файл.

На основе файла будет сформирован открытый ключ APNs-сертификата.

d. После обработки CSR-запроса в Apple вы получите открытый ключ APNs-сертификата.

Сохраните полученный файл.

*Чтобы обновить сертификат:*

a. Нажмите **Перейти на портал Apple**.

b. Авторизуйтесь на портале Apple с корпоративным Apple ID.

> Использовать личный Apple ID не рекомендуется. Создайте отдельный Apple ID для корпоративных целей. Привяжите созданный Apple ID к почтовому ящику организации, а не отдельного сотрудника.

c. Укажите сертификат, который необходимо обновить.

d. Загрузите подписанный CSR-файл.

На основе файла будет сформирован открытый ключ APNs-сертификата.

e. После обработки CSR-запроса в Apple вы получите открытый ключ APNs-сертификата.

Сохраните полученный файл.

### Шаг 4. Загрузка открытого ключа APNs-сертификата

*На этом шаге укажите файл открытого ключа, полученный от Apple на предыдущем этапе мастера:*

a. Нажмите **Выбрать**.

b. В открывшемся окне File Explorer укажите файл сертификата в формате PEM, PFX или P12 и нажмите **Открыть**.

### Шаг 5. Указание пароля закрытого ключа APNs-сертификата

*На этом шаге введите имя сертификата и пароль для закрытого ключа:*

a. В поле **Имя сертификата** укажите произвольное имя сертификата.

b. В поле **Пароль закрытого ключа** укажите пароль закрытого ключа для сертификата.

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

c. В поле **Подтвердите пароль** введите пароль еще раз.

### Шаг 6. Завершение CSR-запроса

На этом шаге APNs-сертификат сформирован и готов к установке на Сервер iOS MDM.

a. Для завершения CSR-запроса нажмите **Скачать APNs-сертификат** и сохраните сертификат.

b. Нажмите **Готово**, чтобы выйти из мастера.

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

Теперь вы можете установить APNs-сертификат на Сервер iOS MDM.

## Установка APNs-сертификата на Сервер iOS MDM

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

*Чтобы установить APNs-сертификат на Сервер iOS MDM:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Мобильные → Серверы iOS MDM**. В открывшемся списке Серверов iOS MDM выберите Сервер iOS MDM, параметры которого вы хотите настроить.

2. В окне параметров Сервера iOS MDM выберите **Параметры приложения**.

3. Выберите вкладку **Сертификаты**.

4. В разделе настроек **Сертификат службы уведомлений Apple Push (APNs)**:

   a. Нажмите **Установить**.

   b. В открывшемся окне File Explorer укажите файл сертификата в формате PEM и нажмите **Открыть**.

   Убедитесь, что устанавливаемый вами сертификат соответствует следующим требованиям безопасности:

   - указано Общее имя (CN);
   - указан APNs topic;
   - указан правильный издатель сертификата;
   - указана правильная дата истечения срока действия сертификата.

   c. В открывшемся окне **Установка сертификата** введите пароль закрытого ключа, указанный при получении APNs-сертификата, и нажмите **Установить**.

APNs-сертификат установлен на Сервер iOS MDM. Информация о сертификате отображена в блоке настроек **Сертификат службы уведомлений Apple Push (APNs)**.

## Настройка доступа к сервису Apple Push Notification

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

Взаимодействуя со службой Apple Push Notification (APNs), служба iOS MDM подключается к внешнему адресу api.push.apple.com по исходящему порту 2197. Для этого 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 службы iOS MDM будет предоставляться через прокси-сервер, необходимо включить использование прокси-сервера для подключения к APNs.

*Чтобы включить использование прокси-сервера для подключения к APNs:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Мобильные → Серверы iOS MDM**. В открывшемся списке Серверов iOS MDM выберите Сервер iOS MDM, параметры которого вы хотите настроить.

2. В окне параметров Сервера iOS MDM выберите **Параметры приложения**.

3. Выберите вкладку **Прокси-сервер для APNs**.

4. В открывшемся окне включите переключатель **Использовать прокси-сервер для подключения к APNs**.

5. Настройте следующие параметры:

   a. В поле **Адрес** укажите адрес прокси-сервера APNs.

   b. В поле **Порт** укажите порт прокси-сервера APNs.

   c. В поле **Имя пользователя** укажите имя пользователя прокси-сервера APNs.

   d. В поле **Пароль** укажите пароль прокси-сервера APNs.

6. Нажмите **Сохранить**.

Теперь для подключения к APNs используется прокси-сервер.

## События Сервера iOS MDM

Kaspersky Security Center Web Console позволяет просматривать события, связанные с Сервером iOS MDM. События имеют разные уровни важности: *Информация*, *Предупреждение*, *Критическое событие*, *Функциональный сбой*.

Для каждого события, которое может быть сгенерировано Сервером iOS MDM, вы можете указать настройки уведомлений и хранения на вкладке **Настройка событий** свойств Сервера iOS MDM. Мы рекомендуем настроить параметры для каждого типа события после развертывания Сервера iOS MDM, чтобы ограничить количество отображаемых событий и сократить время загрузки списка событий.

Если вы хотите настроить параметры уведомлений для всех событий сразу, настройте общие параметры уведомлений в свойствах Сервера администрирования. Дополнительная информация приведена в справке Kaspersky Security Center.

*Чтобы просмотреть события Сервера iOS MDM:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Серверы iOS MDM**. В открывшемся списке Серверов iOS MDM выберите Сервер iOS MDM, события которого вы хотите просмотреть.

2. В окне параметров Сервера iOS MDM выберите **Параметры приложения**.

3. Выберите вкладку **События**.

Отобразятся события Сервера iOS MDM.

Подробная информация о просмотре событий в Kaspersky Security Center Web Console приведена в справке Kaspersky Security Center.

В таблице ниже представлены события Сервера iOS MDM с уровнем важности *Информация*.

События Сервера iOS MDM "Информация"

| Отображаемое имя типа события | Тип события | Срок хранения по умолчанию |
|---|---|---|
| **Общие сведения о мобильном устройстве запрошены** | DEVICEINFORMATION_COMMAND_SUCCESSFUL | 30 дней |
| **Сведения о безопасности запрошены** | SECURITYINFO_COMMAND_SUCCESSFUL | 30 дней |
| **Новое мобильное устройство подключено** | NEW_DEVICE_CONNECTED | 30 дней |
| **Список профилей запрошен** | PROFILELIST_COMMAND_SUCCESSFUL | 30 дней |
| **Профиль установлен** | INSTALLPROFILE_COMMAND_SUCCESSFUL | 30 дней |
| **Профиль удален** | REMOVEPROFILE_COMMAND_SUCCESSFUL | 30 дней |
| **Список provisioning-профилей запрошен** | PROVISIONINGPROFILELIST_COMMAND_SUCCESSFUL | 30 дней |
| **Provisioning-профиль установлен** | INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFUL | 30 дней |
| **Provisioning-профиль удален** | REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFUL | 30 дней |
| **Список установленных сертификатов запрошен** | CERTIFICATELIST_COMMAND_SUCCESSFUL | 30 дней |
| **Список установленных приложений запрошен** | INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFUL | 30 дней |
| **Список управляемых приложений запрошен** | MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFUL | 30 дней |
| **Установка приложения запрошена** | INSTALLAPPLICATION_COMMAND_SUCCESSFUL | 30 дней |
| **Конфигурация приложения применена** | APPCONFIG_APPLIED_SUCCESSFUL | 30 дней |
| **Управляемое приложение удалено** | REMOVEAPPLICATION_COMMAND_SUCCESSFUL | 30 дней |
| **Код погашения для приложения установлен** | APPLYREDEMPTIONCODE_COMMAND_SUCCESSFUL | 30 дней |
| **Мобильное устройство заблокировано** | DEVICELOCK_COMMAND_SUCCESSFUL | 30 дней |
| **Пароль сброшен** | CLEARPASSCODE_COMMAND_SUCCESSFULL | 30 дней |
| **Данные с мобильного устройства удалены** | ERASEDEVICE_COMMAND_SUCCESSFUL | 30 дней |
| **Обновление операционной системы запланировано** | SCHEDULEOSUPDATE_COMMAND_SUCCESSFULL | 30 дней |
| **Параметры роуминга применены** | SETROAMINGSETTINGS_COMMAND_SUCCESSFUL | 30 дней |
| **Параметры Bluetooth применены** | SETBLUETOOTHSETTINGS_COMMAND_SUCCESSFUL | 30 дней |
| **Режим пропажи включен** | ENABLE_LOST_MODE_COMMAND_SUCCESSFUL | 30 дней |
| **Воспроизведен звуковой сигнал в режиме пропажи** | PLAY_LOST_MODE_SOUND_COMMAND_SUCCESSFUL | 30 дней |
| **Местоположение мобильного устройства получено** | GET_DEVICE_LOCATION_COMMAND_SUCCESSFUL | 30 дней |
| **Режим пропажи выключен** | DISABLE_LOST_MODE_COMMAND_SUCCESFUL | 30 дней |
| **Код обхода блокировки активации получен** | GET_ACTIVATION_LOCK_BYPASS_CODE_COMMAND_SUCCESSFUL | 30 дней |
| **Проверка Контроля соответствия началась** | COMPLIANCE_CONTROL_CHEKING_RULES_STARTED | 30 дней |
| **Проверка Контроля соответствия завершена** | COMPLIANCE_CONTROL_CHEKING_RULES_COMPLETED | 30 дней |
| **Реакция Контроля соответствия началась** | COMPLIANCE_CONTROL_ACTION_STARTED | 30 дней |
| **Реакция Контроля соответствия завершена** | COMPLIANCE_CONTROL_ACTION_COMPLETED | 30 дней |

В таблице ниже представлены события Сервера iOS MDM с уровнем важности *Предупреждение*.

События Сервера iOS MDM "Предупреждение"

| Отображаемое имя типа события | Тип события | Срок хранения по умолчанию |
|---|---|---|
| **Попытка подключения заблокированного мобильного устройства** | INACTICE_DEVICE_TRY_CONNECTED | 30 дней |
| **Управляющий профиль удален** | MDM_PROFILE_WAS_REMOVED | 30 дней |
| **Попытка повторного использования сертификата пользователя** | CLIENT_CERT_ALREADY_IN_USE | 30 дней |
| **Обнаружено несоответствие критерию Контроля соответствия** | COMPLIANCE_CONTROL_CONDITIONS_MATCH_DETECTED | 30 дней |
| **Не удалось применить реакцию Контроля соответствия** | COMPLIANCE_CONTROL_ACTION_FAILED | 30 дней |
| **Обнаружено неактивное мобильное устройство** | FOUND_INACTIVE_DEVICE | 30 дней |
| **Требуется код погашения** | NEED_REDEMPTION_CODE | 30 дней |
| **Управляющий профиль удален с мобильного устройства** | UMDM_PROFILE_WAS_REMOVED | 30 дней |

В таблице ниже представлены события Сервера iOS MDM с уровнем важности *Функциональный сбой*.

События Сервера iOS MDM "Функциональный сбой"

| Отображаемое имя типа события | Тип события | Срок хранения по умолчанию |
|---|---|---|
| **Не удалось запросить общие сведения о мобильном устройстве** | DEVICEINFORMATION_COMMAND_FAILED | 30 дней |
| **Не удалось запросить сведения о безопасности** | SECURITYINFO_COMMAND_FAILED | 30 дней |
| **Не удалось запросить список профилей** | PROFILELIST_COMMAND_FAILED | 30 дней |
| **Не удалось установить профиль** | INSTALLPROFILE_COMMAND_FAILED | 30 дней |
| **Не удалось удалить профиль** | REMOVEPROFILE_COMMAND_FAILED | 30 дней |
| **Не удалось запросить список provisioning-профилей** | PROVISIONINGPROFILELIST_COMMAND_FAILED | 30 дней |
| **Не удалось установить provisioning-профиль** | INSTALLPROVISIONINGPROFILE_COMMAND_FAILED | 30 дней |
| **Не удалось удалить provisioning-профиль** | REMOVEPROVISIONINGPROFILE_COMMAND_FAILED | 30 дней |
| **Не удалось запросить список установленных сертификатов** | CERTIFICATELIST_COMMAND_FAILED | 30 дней |
| **Не удалось запросить список установленных приложений** | INSTALLEDAPPLICATIONLIST_COMMAND_FAILED | 30 дней |
| **Не удалось запросить список управляемых приложений** | MANAGEDAPPLICATIONLIST_COMMAND_FAILED | 30 дней |
| **Не удалось запросить установку приложения** | INSTALLAPPLICATION_COMMAND_FAILED | 30 дней |
| **Не удалось применить конфигурацию приложения** | APPCONFIG_APPLIED_FAILED | 30 дней |
| **Не удалось удалить управляемое приложение** | REMOVEAPPLICATION_COMMAND_FAILED | 30 дней |
| **Не удалось установить код погашения для приложения** | APPLYREDEMPTIONCODE_COMMAND_FAILED | 30 дней |
| **Не удалось заблокировать мобильное устройство** | DEVICELOCK_COMMAND_FAILED | 30 дней |
| **Не удалось сбросить пароль** | CLEARPASSCODE_COMMAND_FAILED | 30 дней |
| **Не удалось удалить данные с мобильного устройства** | ERASEDEVICE_COMMAND_FAILED | 30 дней |
| **Не удалось запланировать обновление операционной системы** | SCHEDULEOSUPDATE_COMMAND_FAILED | 30 дней |

| Отображаемое имя типа события | Тип события | Срок хранения по умолчанию |
|---|---|---|
| **Не удалось применить параметры роуминга** | SETROAMINGSETTINGS_COMMAND_FAILED | 30 дней |
| **Не удалось применить параметры Bluetooth** | SETBLUETOOTHSETTINGS_COMMAND_FAILED | 30 дней |
| **Не удалось включить режим пропажи** | ENABLE_LOST_MODE_COMMAND_FAILED | 30 дней |
| **Не удалось воспроизвести звуковой сигнал в режиме пропажи** | PLAY_LOST_MODE_SOUND_COMMAND_FAILED | 30 дней |
| **Не удалось получить местоположение мобильного устройства** | GET_DEVICE_LOCATION_COMMAND_FAILED | 30 дней |
| **Не удалось выключить режим пропажи** | DISABLE_LOST_MODE_COMMAND_FAILED | 30 дней |
| **Не удалось получить код обхода блокировки активации** | GET_ACTIVATION_LOCK_BYPASS_CODE_COMMAND_FAILED | 30 дней |
| **Ошибка в работе приложения** | PRODUCT_FAILURE | 30 дней |
| **Результат выполнения команды содержит неверные данные** | MALFORMED_COMMAND | 30 дней |
| **Не удалось отправить сообщение** | SEND_PUSH_NOTIFICATION_FAILED | 30 дней |
| **Не удалось отправить команду (Контроль соответствия)** | SEND_COMMAND_FAILED | 30 дней |
| **Не удалось найти устройство** | DEVICE_NOT_FOUND | 30 дней |
| **Не удалось настроить Per App VPN для приложения** | PERAPP_VPN_SETUP_FAILED | 30 дней |

## Получение диагностических данных Сервера iOS MDM

При создании запроса в службу технической поддержки "Лаборатории Касперского" вам может быть предложено создать и прикрепить файл трассировки. Файлы трассировки используются Службой технической поддержки в диагностических целях. Эти файлы содержат записи всех шагов выполнения команд приложения, что позволяет обнаружить шаг, на котором возникла ошибка.

Мы рекомендуем создавать трассировки Сервера iOS MDM вместе с трассировками Агента администрирования, так как они содержат сведения о коннекторе Сервера iOS MDM.

Для Сервера iOS MDM существует несколько уровней трассировки:

- 0 - CRITICAL
- 1 - ERROR
- 2 - MESSAGE
- 3 - DEBUG

Уточните у специалиста службы поддержки, какой уровень трассировки следует установить. Если специалист технической поддержки не указал уровень трассировки, мы рекомендуем создавать трассировки уровня 2.

*Чтобы включить трассировку Сервера iOS MDM и создать файлы трассировки:*

1. Откройте файл настроек Сервера iOS MSM `/var/opt/kaspersky/iosmdm/settings.ini`.
2. Укажите значения, необходимые для включения трассировки. Мы рекомендуем указать следующие значения по умолчанию:
   - *LogCommEnabled*=1

     Включение или выключение трассировки библиотеки коммуникации Сервера iOS MDM и коннектора.
   - *LogSettingsEnabled*=1

     Включение или выключение трассировки библиотеки настроек Сервера iOS MDM и коннектора.
   - *LogCommVerboseLevel*=2

     Уровень трассировки библиотеки коммуникации Сервера iOS MDM и коннектора.
   - *LogSettingsVerboseLevel*=2

     Уровень трассировки библиотеки настроек Сервера iOS MDM и коннектора.
   - *LogVerboseLevel*=2

     Уровень трассировки Сервера iOS MDM.
   - *LogFolder*=/var/opt/kaspersky/iosmdm

     Каталог для записи файлов трассировки.
3. Перезапустите службы Сервера iOS MDM и Агента администрирования, выполнив следующие команды:

   ```
   systemctl restart klnagent
   systemctl restart kliosmdm
   ```

Трассировка Сервера iOS MDM включена. Файлы трассировки созданы в каталоге, который вы указали в качестве значения *LogFolder*: *klcon_comm.log*, *klcon_settings.log*, *klsrv.log*, *klsrv_comm.log*, *klsrv_settings.log*.

*Чтобы выключить трассировку Сервера iOS MDM:*

1. Откройте файл настроек Сервера iOS MSM `/var/opt/kaspersky/iosmdm/settings.ini`.
2. Измените файл, удалив строки, которые были созданы для включения трассировки:
   - *LogCommEnabled*=1
   - *LogSettingsEnabled*=1
   - *LogCommVerboseLevel*=2
   - *LogSettingsVerboseLevel*=2
   - *LogVerboseLevel*=2
   - *LogFolder*=/var/opt/kaspersky/iosmdm
3. Перезапустите службы Сервера iOS MDM и Агента администрирования, выполнив следующие команды:

   ```
   systemctl restart klnagent
   ```

```
systemctl restart kliosmdm
```

Трассировка Сервера iOS MDM выключена.

# Развертывание системы управления Android-устройствами

Kaspersky Secure Mobility Management позволяет управлять мобильными устройствами с операционной системой Android. В этом разделе описано развертывание системы управления Android-устройствами.

## О режимах работы Android-устройств

Режим работы устройства зависит от того, кому принадлежит мобильное устройство (личное или корпоративное) и требований корпоративной безопасности. Вы можете выбрать наиболее подходящий для компании режим работы, а также использовать несколько режимов одновременно.

Для Android-устройств доступны следующие режимы работы:

- Личное устройство
- Устройство с корпоративным контейнером
- Корпоративное устройство

### Личное устройство

*Личное устройство* — режим работы для личных Android-устройств. Этот режим работы позволяет защищать устройства и выполнять базовое управление ими.

### Устройство с корпоративным контейнером

*Устройство с корпоративным контейнером* — режим работы для личных Android-устройств с рабочим профилем Android, который обеспечивает изолированную корпоративную среду на устройстве.

Этот режим работы позволяет управлять приложениями и учетными записями пользователей в безопасной среде на устройстве, при этом не ограничивая пользователю доступ к личным данным. При создании рабочего профиля на мобильном устройстве пользователя в контейнер автоматически устанавливаются следующие корпоративные приложения (если применимо): Google Play, Google Chrome, Загрузки, Kaspersky Endpoint Security для Android и другие. Корпоративные приложения, размещенные в рабочем профиле, а также уведомления от этих приложений, отмечены синим значком портфеля. Приложения, размещенные в рабочем профиле, отображаются в общем списке приложений.

### Корпоративное устройство

*Корпоративное устройство* — режим работы для корпоративных Android-устройств. Этот режим работы позволяет вам полностью контролировать устройство и настраивать расширенный набор параметров и функций безопасности:

- ограничения функций Android;
- управление настройками Google Chrome;
- тихая установка обязательных приложений и удаление запрещенных приложений в разделе Контроль приложений;
- режим киоска;
- управление Exchange ActiveSync;
- подключение NDES и SCEP.

## Использование Firebase Cloud Messaging

Для своевременной доставки команд на Android-устройства в Kaspersky Security Center используется механизм push-уведомлений. Обмен push-уведомлениями между Android-устройствами и Сервером администрирования осуществляется с помощью сервиса Firebase Cloud Messaging (далее – FCM). В Kaspersky Security Center Web Console вы можете указать параметры сервиса Firebase Cloud Messaging, чтобы подключить Android-устройства к этому сервису.

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

*Чтобы включить использование FCM:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.
2. Откройте меню с 3 точками ( ⋮ ) и выберите **Синхронизация Android-устройств**.
3. В поле **Номер проекта Firebase** укажите Sender ID FCM.
4. В поле **Закрытый ключ** выберите файл закрытого ключа.

   При следующей синхронизации с Сервером администрирования Android-устройства будут подключены к службе Firebase Cloud Messaging.

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

Сервис FCM работает на следующих диапазонах адресов:

- Со стороны Android-устройства необходим доступ к портам 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) и 5230 (HTTPS) следующих адресов:
  - google.com;
  - fcm.googleapis.com;
  - oauth2.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 Web Console в свойствах Сервера администрирования заданы параметры прокси-сервера, они будут использоваться для взаимодействия с FCM.

## Настройка FCM: получение Sender ID и файла закрытого ключа

*Чтобы настроить FCM:*

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 закрытого ключа.

Firebase Cloud Messaging настроен.

# Развертывание Kaspersky Endpoint Security для Android

В этом разделе содержится общая информация о приложении Kaspersky Endpoint Security для Android и способах его установки, обновления и удаления.

Подробную информацию о Kaspersky Endpoint Security для Android смотрите в разделе Использование приложения Kaspersky Endpoint Security для Android.

## 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**. 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 или 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:
  - **Определить местоположение**. Получение координат местоположения устройства.
  - **Воспроизвести звуковой сигнал**. Устройство издает громкий сигнал тревоги.
  - **Удалить корпоративные данные**. Удаление корпоративных данных, чтобы защитить конфиденциальную информацию компании.
- **Веб-Защита** и **Веб-Контроль**. Веб-Защита блокирует вредоносные сайты, цель которых – распространить вредоносный код. Веб-Защита также блокирует поддельные (фишинговые) сайты, цель которых – украсть конфиденциальные данные пользователя (например, пароли от интернет-банка или платежных систем) и получить доступ к его финансовым счетам. Веб-Защита проверяет сайты перед открытием, используя облачную службу Kaspersky Security Network. По результатам проверки Веб-Защита разрешает загрузку сайтов, признанных надежными, и блокирует сайты, признанные вредоносными. Веб-Контроль поддерживает фильтрацию сайтов по категориям, определенным в облачной службе Kaspersky Security Network. Это позволяет администратору ограничить доступ пользователей к некоторым категориям веб-страниц (например, "Азартные игры, лотереи, тотализаторы" или "Общение в сети").

- **Контроль приложений**. Позволяет устанавливать рекомендуемые и обязательные приложения на Android-устройство, а также удалять заблокированные приложения, нарушающие требования корпоративной безопасности.

- **Контроль соответствия**. 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, задав соответствующие параметры политик.

На личных устройствах и устройствах с корпоративным контейнером под управлением Android 15 пользователи могут создать частное пространство. Kaspersky Endpoint Security для Android не может сканировать приложения, фотографии и другие файлы, хранящиеся в частном пространстве. Веб-Защита, Веб-Контроль и Контроль приложений не работают для приложений, установленных в частном пространстве. Kaspersky Endpoint Security для Android нельзя установить в частном пространстве.

## Установка Kaspersky Endpoint Security для Android

Существует несколько способов развертывания приложения Kaspersky Endpoint Security для Android. Вы можете выбрать наиболее подходящий для вашей организации способ установки, а также использовать несколько способов установки одновременно.

Существуют следующие способы установки:

- Установка через Kaspersky Security Center с помощью одного из источников установки:

  - **Сайт "Лаборатории Касперского"** (для всех режимов работы)

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

  - **Инсталляционный пакет** (для всех режимов работы)

    Инсталляционный пакет Kaspersky Endpoint Security для Android будет загружен с сервера Kaspersky Security Center и обновлен через Kaspersky Security Center с помощью параметров политики. Выберите этот способ, если у мобильных устройств в вашей компании нет доступа к интернету.

    Для этого источника установки создайте инсталляционный пакет Kaspersky Endpoint Security для Android перед подключением мобильных устройств.

- Установка вручную

## Создание инсталляционного пакета Kaspersky Endpoint Security для Android

Приложение Kaspersky Endpoint Security для Android можно развернуть с помощью инсталляционного пакета.

Выберите этот способ установки, если у мобильных устройств в вашей компании нет доступа к интернету.

Для этого способа установки нужно создать инсталляционный пакет Kaspersky Endpoint Security для Android до подключения Android-устройств к Kaspersky Security Center. Инсталляционный пакет будет загружен с сервера Kaspersky Security Center и обновлен через Kaspersky Security Center с помощью параметров политики.

Инсталляционный пакет Kaspersky Endpoint Security для Android — это архив с файлами, необходимыми для установки приложения Kaspersky Endpoint Security для Android:

- `installer.ini`

  Конфигурационный файл с параметрами подключения к Серверу администрирования.

- `kesandroid<версия>_<языки>_Prod_Release.apk`

  Пакетный файл Android для приложения Kaspersky Endpoint Security для Android.

- `ksm.kpd`

  Файл, содержащий описание программы.

- `eula/`

  Папка с Лицензионными соглашениями на разных языках в формате TXT.

- `kpd.loc/`

  INI-файлы, определяющие пути к Лицензионным соглашениям.

*Чтобы создать инсталляционный пакет Kaspersky Endpoint Security для Android:*

1. В главном окне Kaspersky Security Center Web Console выберите **Операции** > **Хранилища** > **Инсталляционные пакеты**.
2. В открывшемся списке инсталляционных пакетов нажмите **Добавить**. Запустится Мастер создания инсталляционного пакета. Следуйте шагам мастера, как описано в справке Kaspersky Security Center, чтобы создать инсталляционный пакет из файла или создать автономный инсталляционный пакет.

*Чтобы настроить инсталляционный пакет Kaspersky Endpoint Security для Android:*

1. В главном окне Kaspersky Security Center Web Console выберите **Операции** > **Хранилища** > **Инсталляционные пакеты**.
2. В открывшемся списке инсталляционных пакетов нажмите на инсталляционный пакет Kaspersky Endpoint Security для Android, который вы хотите настроить.
3. В окне свойств инсталляционного пакета выберите вкладку **Параметры**.

   a. В блоке параметров **Подключение к Серверу администрирования** настройте следующие значения:

   - **Адрес сервера**. Укажите адрес сервера, к которому будут подключаться Android-устройства.
   - **SSL-порт для синхронизации устройств**. Укажите номер порта, открытого на Сервере администрирования для подключения мобильных устройств. По умолчанию указан порт 13292.

   b. Для автономных инсталляционных пакетов в поле **Имя подгруппы** в блоке параметров **Подгруппа в разделе "Нераспределенные устройства"** укажите имя группы, в которую будут добавлены Android-устройства после первой синхронизации с Сервером администрирования. По умолчанию указано KES10.

c. В блоке параметров **Действия при установке на устройство** установите флажок **Запрашивать у пользователя адрес электронной почты**, чтобы при первом запуске приложение Kaspersky Endpoint Security для Android запрашивало у пользователя адрес корпоративной электронной почты.

Адрес электронной почты пользователя используется для формирования имени мобильного устройства при добавлении его в группу администрирования.

4. Нажмите **Сохранить**.

Инсталляционный пакет Kaspersky Endpoint Security для Android настроен.

## 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.

## Установка Kaspersky Endpoint Security для Android на корпоративные устройства в закрытой сети

При развертывании Kaspersky Endpoint Security для Android в режиме работы для корпоративного устройства 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 Kaspersky Endpoint Security для Android в режиме работы для корпоративного устройства 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 "Лаборатории Касперского" и загрузите его в закрытую сеть.

     В качестве источника выберите общую версию приложения.

4. Отправьте ссылку для установки приложения и QR-код пользователю, следуя указаниям Мастера подключения мобильного устройства.

   На шаге **Операционные системы** мастера, в разделе **Параметры установки**, 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 параметров **Сеть для установки** выберите **Предложить 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 параметров **Сеть для установки** выберите **Использовать только заданную сеть Wi-Fi** (Android 9 или выше), нажмите кнопку **Выбрать сеть**, после чего вставьте ссылку на ранее созданный PAC-файл (шаг 2) в поле **URL-адрес PAC-файла**.

   Если инсталляционный APK-файл был загружен с сайта "Лаборатории Касперского" (шаг 3), то вам необходимо изменить ссылку в QR-коде на адрес закрытой сети.

   Если для развертывания приложения используется инсталляционный пакет, 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 инсталляционного пакета отличается от указанного в Google Play. Для продолжения установки необходимо нажать **Все равно установить**. При нажатии **OK** процесс установки будет прерван, а настройки устройства будут сброшены до заводских.

Приложение Kaspersky Endpoint Security для Android будет установлено на устройство, работающее в режиме "Корпоративное устройство" в закрытой сети.

## Разрешения для Kaspersky Endpoint Security для Android

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 и 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 корпоративного устройства; для Android 10–11 в режиме устройства с корпоративным контейнером) |
| | 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 поблизости** (для Android 12 или выше) | Ограничение использования Bluetooth<br><br>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. |

| Разрешение | Функция приложения |
| --- | --- |
| **Администратор устройства** (обязательно) | Анти-Вор – блокировка устройства (только для Android 5–6) |
| | 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<br>На устройствах с операционной системой Android 11 или выше необходимо при появлении запроса предоставить разрешение "При использовании приложения". |
| **Местоположение** | Анти-Вор – определение местоположения устройства<br>На устройствах с операционной системой Android 10 или выше необходимо при появлении запроса предоставить разрешение "Всегда". |
| | Команды – получение истории местоположений |
| | |
| **Специальные возможности** | Анти-Вор – блокировка устройства (только для Android 7 или выше) |
| | Веб-Защита |
| | Контроль приложений |
| | Защита приложения от удаления (только для Android 7 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 |

## Запуск и остановка Kaspersky Endpoint Security для Android

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 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 поиска вредоносного ПО по расписанию или синхронизации устройства с Kaspersky Security Center. Проблема связана с особенностями встроенного программного обеспечения этих устройств.

## Активация Kaspersky Endpoint Security для Android

В Kaspersky Security Center лицензия может распространяться на различные группы функциональности. Для полноценного функционирования Kaspersky Endpoint Security для Android нужно, чтобы с приобретенной организацией лицензией на Kaspersky Security Center была доступна функциональность Управление мобильными устройствами.

Подробная информация о вариантах лицензирования приведена в разделе О лицензии.

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 параметрами политики 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 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. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Нажмите на кнопку **Лицензия**.

4. В раскрывающемся списке в открывшемся окне 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 **Заменить ключ, если на устройствах добавлен другой ключ**.

5. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Приложение будет активировано после очередной синхронизации устройства с Kaspersky Security Center.

# Обновление 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 можете дистанционно обновить версию приложения на устройстве с помощью 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 Web Console, во время установки приложения Kaspersky Endpoint Security для Android шаг принятия Лицензионного соглашения будет пропущен.

## 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 той версии Kaspersky Endpoint Security для Android, которая соответствует требованиям корпоративной безопасности.

Вы можете выполнить обновление через Kaspersky Security Center, если приложение Kaspersky Endpoint Security для Android было установлено с помощью инсталляционного пакета в Kaspersky Security Center или с помощью автономного пакета установки. 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:*

1. Создайте новый инсталляционный пакет Kaspersky Endpoint Security для Android.
2. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
3. В окне свойств политики выберите **Параметры приложения**.
4. Выберите **Android** и перейдите в раздел **Параметры KES для Android**.
5. На карточке **Обновление приложения** нажмите **Параметры**.

   Откроется окно **Обновление приложения**.
6. Включите параметры с помощью переключателя **Обновление приложения**.
7. Нажмите **Выбрать**.

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

   Обновить Kaspersky Endpoint Security для Android до более старой версии невозможно.
9. Нажмите **Выбрать**.

10. Нажмите **OK**.

11. Нажмите **Сохранить**, 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 подтверждения новая версия приложения будет установлена на мобильное устройство.

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

# 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, удаление приложения необходимо разрешить в карточке **Параметры доступа к настройкам приложения** раздела **Параметры KES для Android** политики.

2. Удаление приложения администратором (только для корпоративных устройств)

   Администратор удаляет приложение удаленно с помощью Kaspersky Security Center Web Console. Можно удалить приложение с отдельного устройства или с нескольких устройств одновременно.

## Разрешение пользователям удалять Kaspersky Endpoint Security для Android

На устройствах под управлением 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.

*Чтобы разрешить удаление приложения, в групповой политике:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Параметры KES для Android**.

4. На карточке **Параметры доступа к настройкам приложения** нажмите **Параметры**.

   Откроется окно **Параметры доступа к настройкам приложения**.

5. Установите флажок **Разрешить удаление приложения с устройства**.

6. Нажмите **OK**.

7. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

В результате после синхронизации с Сервером администрирования пользователям будет разрешено удалять приложение с мобильных устройств. В настройках Kaspersky Endpoint Security для Android будет доступна кнопка удаления приложения.

*Чтобы удалить приложение с устройства:*

1. В главном окне Kaspersky Endpoint Security для Android выберите **Настройки** → **Настройки приложения** → **Дополнительно** → **Удаление приложения**.

   На корпоративных устройствах Kaspersky Endpoint Security для Android может удалить только администратор.

2. Подтвердите удаление Kaspersky Endpoint Security для Android.

Приложение Kaspersky Endpoint Security для Android будет удалено с устройства.

## Удаление Kaspersky Endpoint Security для Android пользователем

На корпоративных устройствах Kaspersky Endpoint Security для Android может удалить только администратор.

*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 выберите **Настройки** → **Настройки приложения** → **Дополнительно** → **Удаление приложения**.

   Если кнопка **Удаление приложения** отсутствует, значит администратор включил защиту Kaspersky Endpoint Security для Android от удаления или устройство работает в режиме корпоративного устройства.

2. Подтвердите удаление Kaspersky Endpoint Security для Android.

Приложение Kaspersky Endpoint Security для Android будет удалено с устройства.

Мы рекомендуем удалять Kaspersky Endpoint Security для Android только через настройки приложения, как описано в инструкции выше. Другие способы удаления могут привести к неполному удалению корпоративных контейнеров и вызвать другое непредсказуемое поведение.

### Дистанционное удаление Kaspersky Endpoint Security для Android с корпоративных устройств

Вы можете дистанционно удалить приложение Kaspersky Endpoint Security для Android с корпоративных устройств, отправив команду **Сбросить настройки до заводских**.

Выполнение команды **Сбросить настройки до заводских** стирает все данные с устройства и возвращает настройки устройства к заводским значениям. Android Enterprise рекомендует использовать этот метод удаления приложений для гарантированного удаления данных с корпоративного устройства.

*Чтобы удалить приложение:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.
2. В открывшемся списке устройств выберите устройства, на которые вы хотите отправить команду.

   Можно выбрать несколько устройств.
3. Нажмите **Отправить команду**.
4. В открывшемся окне **Отправить команду** в поле **Команда** выберите команду **Сбросить настройки до заводских**.
5. Нажмите **Отправить**.

   Вы можете просматривать и отменять команды в окне **История команд**.

   Команда будет отправлена на выбранные вами устройства. Приложение Kaspersky Endpoint Security для Android удалено с этих устройств.
6. Выберите устройство из списка устройств и нажмите **Удалить**.

   Устройство удалено из списка управляемых устройств в Kaspersky Security Center Web Console.

   Если устройство не будет удалено из Kaspersky Security Center Web Console, то при последующей установке приложений "Лаборатории Касперского" на устройство могут возникнуть проблемы.

# Управление мобильными устройствами в Kaspersky Security Center Web Console

Для централизованной конфигурации мобильных устройств необходимо настроить политики. Политика - это набор параметров безопасности для управления мобильными устройствами с определенными операционными системами и режимами работы в рамках группы администрирования, а также для конфигурации управляющих приложений, установленных на устройствах.

В этом разделе описано, как создать группы администрирования, настроить политики для мобильных устройств, а также подключить мобильные устройства к Kaspersky Security Center для последующего управления ими.

## Создание групп администрирования

Чтобы применить политику к группе устройств, рекомендуется создать для этих устройств отдельную группу перед установкой приложений для управления мобильными устройствами.

*Группа администрирования* - это набор устройств, объединенных по какому-либо признаку с целью управления устройствами группы как единым целым в Kaspersky Security Center.

Для всех управляемых устройств в группе администрирования устанавливаются:

- Единые параметры – с помощью политик.
- Единый режим работы всех приложений – с помощью создания групповых задач с определенным набором параметров. Примеры групповых задач включают создание и установку общего инсталляционного пакета, обновление баз и модулей приложений, проверку устройства по требованию и включение постоянной защиты.

Управляемое устройство может входить в состав только одной группы администрирования.

Для Серверов администрирования и групп администрирования можно создавать иерархии с любым уровнем вложенности. На одном уровне иерархии могут располагаться подчиненные и виртуальные Серверы администрирования, группы и управляемые устройства. Можно переводить устройства из одной группы в другую.

Сразу после установки Kaspersky Security Center в иерархии групп администрирования находится только одна группа администрирования – "Управляемые устройства". При создании иерархии групп администрирования в состав папки "Управляемые устройства" можно включать устройства и добавлять вложенные группы.

*Чтобы создать группу администрирования:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** > **Иерархия групп**.
2. В структуре группы администрирования выберите группу, в состав которой должна входить новая группа администрирования.
3. Нажмите **Добавить**.
4. В открывшемся окне **Имя новой группы администрирования** введите имя группы и нажмите **Добавить**.

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

*Чтобы автоматически создать структуру групп администрирования:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** > **Иерархия групп**.
2. Нажмите **Импортировать**.

Запустится Мастер создания структуры групп администрирования. Следуйте указаниям мастера.

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

# Настройка политик

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

## Создание политики

Kaspersky Security Center Web Console позволяет создавать политики для настройки параметров безопасности групп мобильных устройств под управлением Android, iOS и ОС Аврора. Параметры безопасности, настроенные в политиках, сохраняются на Сервере администрирования, распространяются на мобильные устройства при синхронизации и используются в качестве текущих настроек.

Вы можете создать политику с помощью Мастера создания политики для мобильных устройств.

*Чтобы создать политику:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**.
2. В открывшемся списке политик нажмите **Текущий путь**, чтобы выбрать группу администрирования, для которой вы хотите создать политику.

   По умолчанию новая политика применяется к группе **Активы (Устройства)**.
3. Нажмите **Добавить**, чтобы запустить Мастер создания политики для мобильных устройств.
4. В окне **Выберите приложение** выберите **Kaspersky Mobile Devices Protection and Management** и нажмите **Далее**.

   Запустится Мастер создания политики для мобильных устройств. Нажмите **Начать** и продолжайте работу мастера с помощью кнопок **Назад** и **Далее**.

### Шаг 1. Лицензия

На этом шаге выберите лицензию.

От выбранной лицензии зависит набор параметров безопасности, которые вы сможете настраивать в политике. По умолчанию предварительно выбрана лицензия, поддерживающая функциональность Kaspersky Secure Mobility Management. Вы можете выбрать другую лицензию вручную.

## Шаг 2. Операционные системы и режимы работы устройств

На этом шаге выберите операционные системы, на которые будет распространяться политика, и укажите режимы работы устройств.

- **Android**
  - **Личное устройство** (базовая защита и управление личным Android-устройством).
  - **Устройство с корпоративным контейнером** (изолированная корпоративная среда на Android-устройстве).
  - **Корпоративное устройство** (расширенный набор параметров для управления корпоративным Android-устройством).

    Подробная информация приведена в разделе О режимах работы Android-устройств.
- **iOS**
  - **Базовая защита** (защита от веб-угроз и обнаружение jailbreak на iOS-устройствах).
  - **Базовый контроль** (базовое управление личным iOS-устройством).
  - **Расширенный контроль** (расширенный набор параметров для управления iOS-устройством).

    Подробная информация приведена в разделе О режимах работы iOS-устройств.

    Для подключения и управления iOS-устройствами в режимах "Базовый контроль" и "Расширенный контроль" в выбранной группе администрирования должен быть установлен Сервер iOS MDM. Подробная информация об установке Сервера iOS MDM приведена в разделе Развертывание Сервера iOS MDM.

    Для режима "Базовая защита" вы можете создать отдельную группу администрирования без Сервера iOS MDM и распространить политику.

    Для режимов "Базовый контроль" или "Расширенный контроль" вы можете создать группы администрирования с разными Серверами iOS MDM и распространить разные политики соответственно.

    Также вы можете объединить устройства, работающие в режимах "Базовый контроль" и "Расширенный контроль", в одну группу администрирования и распространить политику для режима "Расширенный контроль". В этом случае, на устройствах будут применены параметры, поддерживаемые соответствующим режимом работы.
- **Аврора**
  - **Защита** (защита устройств с ОС Аврора от угроз).

    Для подключения устройств с ОС Аврора на устройствах должно быть предварительно установлено приложение Kaspersky Endpoint Security для ОС Аврора.

*В окне "Новая политика":*

1. В поле **Название** введите имя новой политики. Если вы укажете имя уже существующей политики, к нему автоматически будет добавлено окончание (1).

2. В разделе настроек **Состояние политики** выберите состояние политики:

   - **Активна**. Мастер сохраняет созданную политику на Сервере администрирования. После следующей синхронизации мобильных устройств с Сервером администрирования политика начнет использоваться на устройствах в качестве активной.

   - **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.

3. На вкладке **Общие** раздела настроек **Наследование параметров** можно настроить параметры наследования политики:

   - **Наследовать параметры родительской политики**

     Если вы включите этот параметр в дочерней политике, а администратор заблокирует некоторые параметры в родительской политике, вы не сможете изменить эти параметры в дочерней политике.

     Если вы выключили этот параметр в дочерней политике, вы можете изменить все параметры в дочерней политике, даже если некоторые параметры "заблокированы" в родительской политике.

   - **Обеспечить принудительное наследование параметров для дочерних политик**

     Если этот параметр включен в родительской политике, для всех дочерних политик будет включен параметр **Наследовать параметры родительской политики**. В этом случае вы не сможете выключить этот параметр для всех дочерних политик. Все параметры, заблокированные в родительской политике, принудительно наследуются в дочерних политиках, и вы не сможете изменить эти параметры в дочерних группах.

   По умолчанию параметр **Наследовать параметры родительской политики** включен, а параметр **Обеспечить принудительное наследование параметров для дочерних политик** - выключен.

   Наследование параметров политики работает только если для родительской и дочерней политики выбраны одинаковые режимы работы устройств, либо в выбранных для дочерней политики режимах работы устройств доступно больше параметров безопасности. Например, дочерняя политика для Android-устройств с корпоративным контейнером может наследовать параметры родительской политики для личных устройств, но не может наследовать параметры родительской политики для корпоративных устройств.
   Если вы создали дочернюю политику, несовместимую с родительской политикой, то чтобы управлять устройствами, нужно удалить ее и создать новую дочернюю политику.

4. Нажмите **Сохранить**.

Создана новая политика для мобильных устройств.

## Изменение политики

Kaspersky Security Center Web Console позволяет изменять политики.

*Чтобы изменить политику:*

1. Откройте окно свойств политики, выполнив одно из следующих действий:

   - В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите изменить.

   - В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите изменить, а затем выберите политику на вкладке **Действующие политики и профили политик**.

2. В окне свойств политики перейдите на вкладку **Параметры приложения**, а затем укажите параметры политики.

   Вы можете настроить общие параметры, наследование параметров, профили политик, запись событий и уведомления, а также просмотреть историю ревизий. Дополнительная информация приведена в справке Kaspersky Security Center.

   Вы не можете настроить, как долго должны храниться события на мобильном устройстве пользователя. Срок хранения журнала событий на устройстве не ограничен. Однако ограничен объем журнала: при достижении 200 записей автоматически удаляются 50 самых старых записей.

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

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

## Копирование политики

В Kaspersky Security Center Web Console можно создавать копии политик.

*Чтобы создать копию политики:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**.

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

3. В открывшемся дереве групп администрирования выберите целевую группу, в которой вы хотите создать политику.

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

4. Нажмите **Копировать**.

5. Нажмите **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, совпадающим с именем новой созданной или перемещенной политики, к имени новой политики добавляется индекс (<порядковый номер>), например: (1).

## Перенос политики в другую группу администрирования

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

*Чтобы перенести политику в другую группу администрирования:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Политики**.

2. В открывшемся списке 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, в которую вы хотите переместить политику.

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

4. Нажмите **Переместить**.

5. Нажмите **ОК** для подтверждения.

Результат зависит от свойств наследования политики:

- Если политика не наследовалась в исходной группе, то она будет перемещена в целевую группу.
- Если политика наследовалась в исходной группе, то 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, совпадающим с именем новой созданной или перемещенной политики, к имени новой политики добавляется индекс (<порядковый номер>), например: (1).

## Просмотр списка политик

Kaspersky Security Center Web Console позволяет просматривать список созданных политик, их статусы и свойства.

*Чтобы просмотреть список политик:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Политики**.
2. Откроется список политик с краткой информацией о них. На этой странице вы можете создавать, изменять, копировать, перемещать и удалять политики.

## Просмотр результатов применения политики

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

*Чтобы просмотреть результаты распространения политики:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Политики**.
2. В открывшемся списке политик установите флажок рядом с названием политики, для которой вы хотите просмотреть результаты распространения, и нажмите **Результаты применения**.

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 **Настроить параметры политики**.

## Работа с ревизиями политик

В Kaspersky Security Center Web Console можно просматривать изменения, внесенные в политику за определенный период, а также сохранять информацию об этих изменениях в файле.

*Чтобы просмотреть ревизию политики:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Политики**.
2. В открывшемся списке политик выберите политику, ревизию которой вы хотите просмотреть, а затем перейдите в раздел **История ревизий**.
3. В списке ревизий политики выберите номер ревизии, которую вы хотите просмотреть.

Если размер ревизии превышает 10 МБ, вы не сможете просмотреть ее с помощью Kaspersky Security Center Web Console. Вам будет предложено сохранить выбранную ревизию в файл JSON.

Если размер ревизии не превышает 10 МБ, то отображается отчет в формате HTML с параметрами выбранной ревизии. Отчет отображается во всплывающем окне, поэтому убедитесь, что в вашем браузере разрешены всплывающие окна.

Чтобы сохранить ревизию политики в файл JSON, в списке ревизий политики выберите нужную ревизию, а затем нажмите **Сохранить в файл**.

Ревизия сохраняется в файле JSON.

Подробная информация об управлении ревизиями политик приведена в справке Kaspersky Security Center.

## Ограничение прав на настройку политик

Администраторы Kaspersky Security Center могут настраивать права доступа пользователей Web Console к различным функциям решения Kaspersky Secure Mobility Management в зависимости от служебных обязанностей пользователей.

В интерфейсе Web Console вы можете настроить права доступа на вкладках **Безопасность** и **Роли пользователей** в окне свойств Сервера администрирования. На вкладке **Роли пользователей** можно добавлять типовые роли пользователей с заранее 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 областям действия.

Для каждой функциональной области администратор может назначать следующие права доступа:

- **Разрешить изменение**. Пользователю Web Console разрешено изменять параметры политики в окне ее свойств.

- **Запретить изменение**. Пользователю Web Console запрещено изменять параметры политики в окне ее свойств. Вкладки политики, входящие в функциональную область, для которой назначено это право, не отображаются в интерфейсе.

## Настройка управления доступом на основе ролей

С помощью Kaspersky Security Center Web Console можно предоставлять доступ к функциям Kaspersky Secure Mobility Management на основе ролей.

Вы можете настроить права доступа к функциям Kaspersky Secure Mobility Management одним из следующих способов:

- Настроить права отдельно для каждого пользователя или группы.

- Создать типовые роли пользователей с предопределенным набором прав и назначить эти роли пользователям в соответствии с их обязанностями.

Назначение ролей упрощает и сокращает процедуру настройки прав доступа пользователей. Права доступа для роли настраиваются в соответствии с типовыми задачами и обязанностями пользователей.

Ролям пользователей можно присваивать имена, соответствующие их назначению. В программе можно создавать неограниченное количество ролей. Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать новые роли и самостоятельно настраивать необходимые права.

Подробная информация о настройке доступа пользователей в Kaspersky Security Center приведена в справке Kaspersky Security Center.

У некоторых предопределенных ролей пользователей нет прав на работу с мобильными устройствами. Предопределенные роли пользователей, доступные для функций Kaspersky Secure Mobility Management, перечислены в таблице ниже.

Предопределенные роли пользователей для работы с Kaspersky Secure Mobility Management

| Роль | Чтение | Запись | Управление лицензионными ключами: создание политик и изменение параметров лицензионного ключа | Системное администрирование: просмотр непринятых Лицензионных соглашений и принятие Лицензионных соглашений |
|---|---|---|---|---|
| Администратор Kaspersky Endpoint Security | + | + | - | - |
| Оператор Kaspersky Endpoint Security | + | - | - | - |
| Главный администратор | + | + | - | - |
| Главный оператор | + | - | - | - |
| Администратор управления мобильными устройствами | + | + | + | + |
| Оператор управления мобильными устройствами | + | - | - | - |

Дополнительная информация о предопределенных ролях пользователей приведена в справке Kaspersky Security Center.

Права доступа к функциям Kaspersky Secure Mobility Management

| Функциональная область | Право |
|---|---|
| Kaspersky Mobile Devices Protection and Management > Kaspersky Security Center Web Console > Конфигурация приложений | • **Чтение:** Право на чтение во всех параметрах в разделе соответствующей политики<br>• **Запись:** Право на запись во всех параметрах в разделе соответствующей политики<br>Обратите внимание: для настройки параметров Веб-Защиты и Веб-Контроля у администратора должны быть права на **Чтение** и **Запись** в функциональных областях **Защита** и **Контроль безопасности**. |
| Kaspersky Mobile Devices Protection and Management > Kaspersky Security Center Web Console > Контроль безопасности | |
| Kaspersky Mobile Devices Protection and Management > Kaspersky Security Center Web Console > Корпоративный контейнер | |
| Kaspersky Mobile Devices Protection and Management > Kaspersky Security Center Web Console > Конфигурация устройств | |
| Kaspersky Mobile Devices Protection and Management > Kaspersky Security Center Web Console > Конфигурация приложений "Лаборатории Касперского" для управления устройствами | |
| Kaspersky Mobile Devices Protection and Management > Kaspersky Security Center Web Console > Защита | |
| Kaspersky Mobile Devices Protection and Management > Kaspersky Security Center Web Console > Ограничения | |
| Kaspersky Mobile Devices Protection and Management > Kaspersky Security Center Web Console > Параметры Samsung Knox | |

| Право | Действие пользователя: право, необходимые для выполнения действия |
|---|---|
| **Управление мобильными устройствами** > **Общие** > **Чтение** | • Просмотр раздела **Мобильные** в Kaspersky Security Center Web Console |
| **Управление мобильными устройствами** > **Общие** > **Запись** | • Выполнять любые действия с сертификатами (кроме просмотра сертификатов)<br>Также должно быть предоставлено право **Управление сертификатами**.<br>• Настройка параметров Firebase Cloud Messaging |
| **Управление мобильными устройствами** > **Общие** > **Подключение новых устройств** | • Подключение новых мобильных устройств и Серверов iOS MDM<br>• Удаление устройств |
| **Управление мобильными устройствами** > **Общие** > **Управление сертификатами** | • Выполнять любые действия с сертификатами<br>• Настройка правил выпуска сертификатов<br>Также должно быть предоставлено право **Запись**. |
| **Управление мобильными устройствами** > **Общие** > **Отправка только информационных команд на мобильные устройства** | • Отправка и отмена команды **Синхронизировать устройство** |
| **Управление мобильными устройствами** > **Общие** > **Отправка команд на мобильные устройства** | • Отправка и отмена любой команды |
| **Управление мобильными устройствами** > **Общие** > **Запуск RDP-сеансов** | • Установление удаленных подключений к устройствам |

## Настройка профилей политик

Может возникнуть необходимость создать и централизованно изменить несколько копий одной политики для группы администрирования. Эти копии могут отличаться одним или двумя параметрами.

Чтобы избежать создания нескольких копий одной политики, Kaspersky Security Center Web Console позволяет создавать профили политик. Профили политики нужны для того, чтобы устройства внутри одной группы администрирования могли иметь разные параметры политики.

Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – условия активации профиля. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на управляемом устройстве. При активации профиля изменяются параметры "базовой" политики, которые исходно действовали на устройстве. Эти параметры принимают значения, указанные в профиле.

Вы можете менять условия, которые влияют на активацию создаваемого профиля политики. Для мобильных устройств доступны следующие условия:

- **Правила для выбранного владельца устройства**

Активация профиля на устройстве по владельцу устройства.

- **Владелец устройства**
- **Владелец устройства включен во внутреннюю группу безопасности**

- **Правила для назначения роли**

  Активация профиля на устройстве в зависимости от наличия определенной роли у его владельца.

  - **Активировать профиль политики по наличию роли у владельца устройства**

- **Правила для использования тега**

  Активация профиля на устройстве в зависимости от тегов, назначенных устройству.

  - **Список тегов**
  - **Применить к устройствам без выбранных тегов**

- **Правила для использования Active Directory**

  Активация профиля на устройстве в зависимости от размещения устройства в подразделении Active Directory или же от членства устройства или его владельца в группе безопасности Active Directory. Область настройки зависит от текущей используемой политики.

  - **Членство владельца устройства в группе безопасности Active Directory**
  - **Членство устройства в группе безопасности Active Directory**
  - **Размещение устройства в подразделении Active Directory**

Подробная информация о настройке правил активации, а также создании, удалении и копировании профилей политики приведена в справке Kaspersky Security Center.

## Удаление политики

В Kaspersky Security Center Web Console можно удалять политики.

> Удалять можно только те 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:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**.
2. В открывшемся списке политик установите флажок рядом с названием политики, которую вы хотите удалить, и нажмите **Удалить**.
3. В открывшемся окне нажмите **OK** для подтверждения.

Политика будет удалена. До применения новой политики мобильные устройства, входящие в группу администрирования, продолжат работу с параметрами, заданными в удаленной политике.

# Подключение мобильных устройств к Kaspersky Security Center Web Console

Для управления мобильными устройствами и установленными на них управляющими приложениями необходимо подключить эти устройства к Kaspersky Security Center.

Перед подключением убедитесь, что в разделе **Лицензионные ключи** свойств Сервера администрирования настроена лицензия, поддерживающая решение для управления мобильными устройствами.

*Чтобы подключить мобильное устройство к Kaspersky Security Center:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.
2. В открывшемся списке мобильных устройств нажмите **Добавить**.

   Запустится Мастер подключения мобильного устройства. Нажмите **Начать** и продолжайте работу мастера с помощью кнопок **Назад** и **Далее**.

## Добро пожаловать

На экране приветствия можно прочитать краткое описание шагов Мастера подключения мобильного устройства.

## Шаг 1. Политика

На этом шаге выберите политику для подключаемых устройств. Устройства работают в соответствии с настройками безопасности, указанными в политике.

- **Использовать существующую политику**

  Укажите группу администрирования для политики, которую вы хотите выбрать. Отобразится название политики, а также операционные системы и режимы работы устройств, которыми управляет эта политика.

  Если необходимо, нажмите **Перейти к политике**, чтобы просмотреть свойства выбранной политики.

- **Создать новую политику**

  Нажмите на появившуюся кнопку **Создать политику**. Вы будете перенаправлены в Мастер создания политики для мобильных устройств. После создания политики с необходимыми параметрами вы можете вернуться к Мастеру подключения мобильного устройства.

## Шаг 2. Операционные системы

На этом шаге выберите операционные системы подключаемых устройств. Доступные операционные системы зависят от указанных в настройках политики: Android, iOS, Аврора.

- **Android**

После выбора этой операционной системы отобразятся **Параметры установки** Kaspersky Endpoint Security для Android. Чтобы изменить их, нажмите **Изменить параметры**.

a. Выберите **Источник установки** приложения Kaspersky Endpoint Security для Android.

- **Сайт "Лаборатории Касперского"**

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

  Этот источник установки доступен для всех режимов работы устройств.

- **RuStore**

  Пользователь получит ссылку на RuStore. Установка из RuStore выполняется обычным способом, принятым для платформы Android.

  Ссылка содержит следующие данные:

  - Параметры синхронизации с Kaspersky Security Center.
  - Информация для автоматического получения мобильного сертификата при первой синхронизации.
  - Информация о том, принято ли Лицензионное соглашение для Kaspersky Endpoint Security для Android и другие соглашения. Если администратор принял соглашения в Kaspersky Security Center Web Console, приложение пропускает этап принятия соглашений при установке.

  Этот источник установки доступен только для личных устройств и устройств с корпоративным контейнером.

- **Инсталляционный пакет**

  Инсталляционный пакет Kaspersky Endpoint Security для Android будет загружен с сервера Kaspersky Security Center и обновлен через Kaspersky Security Center с помощью параметров политики. Выберите этот способ, если у мобильных устройств в вашей компании нет доступа к интернету.

  Для этого источника установки создайте инсталляционный пакет Kaspersky Endpoint Security для Android перед подключением мобильных устройств.

  Этот источник установки доступен для всех режимов работы устройств.

  - Чтобы указать инсталляционный пакет, нажмите **Выбрать инсталляционный пакет** и выберите инсталляционный пакет из открывшегося списка.
  - Если доступных инсталляционных пакетов нет, вам будет предложено создать их. Нажмите **Создать инсталляционный пакет** и следуйте шагам Мастера создания инсталляционного пакета, как описано в справке Kaspersky Security Center, чтобы создать инсталляционный пакет из файла или автономный инсталляционный пакет. После создания инсталляционного пакета вы можете вернуться к Мастеру подключения мобильного устройства.

При этом способе установки недоступны автоматические обновления через магазин приложений. Обновить приложение можно вручную в разделе **Обновление приложения** параметров политики.
Для установки приложения на устройства используется последний инсталляционный пакет, загруженный в Kaspersky Security Center.

Если вы подключаете корпоративные устройства, убедитесь, что установлен флажок **Разрешить использование HTTP для загрузки приложения**, чтобы обеспечить загрузку Kaspersky Endpoint Security для Android. В противном случае приложение будет загружено по протоколу HTTPS только в том случае, если сертификат Веб-сервера Kaspersky Security Center выдан доверенным центром сертификации.

Подробная информация о способах установки приведена в секции Установка Kaspersky Endpoint Security для Android.

b. Выберите **Сеть для установки** Kaspersky Endpoint Security для Android (только для корпоративных устройств):

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

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

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

  Чтобы выбрать сеть для установки, нажмите **Выбрать сеть**.

  В открывшемся окне укажите следующие параметры:

  - **Идентификатор сети SSID**

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

  - **Скрытая сеть**

    Определяет, будет ли выбранная сеть транслировать свой SSID.

  - **Защита сети**

    Определяет тип защиты беспроводной сети. Возможные значения:

    - **NONE**

      Сеть не защищена.

    - **WPA**

      Сеть защищена по протоколу безопасности WPA. Этот параметр требует ввода пароля для доступа к сети.

    - **WEP**

      Сеть защищена по протоколу WEP. Этот параметр требует ввода пароля для доступа к сети и применим только для устройств под управлением Android 9 или ниже.

- **Пароль**

  Определяет пароль для доступа к беспроводной сети, защищенной по протоколу WPA или WEP. Пароль будет передан пользователю с QR-кодом.

  Не отправляйте пароль для конфиденциальной сети Wi-Fi, которая не должна быть общедоступной. Пароль передается пользователю в открытом виде вместе с другими данными, необходимыми для настройки устройства.

- **Использовать прокси-сервер**

  Определяет использование прокси-сервера. 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 65536.

- **Веб-адрес PAC-файла**

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

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

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

  Введите адрес в формате `example.com`. Если вы введете `example.com`, прокси-сервер не будет использоваться для адресов `pictures.example.com`, `example.com/movies` и т. п. Протокол (например, `http://`) указывать необязательно.

Не отправляйте пароль для конфиденциальной сети Wi-Fi, которая не должна быть общедоступной. Пароль передается пользователю в открытом виде вместе с другими данными, необходимыми для настройки устройства.

- **По возможности использовать мобильную сеть** (Android 8 или выше)

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

c. Выберите флажок **Включить все системные приложения** (только для корпоративных устройств), чтобы системные приложения на устройстве остались включенными. При необходимости их можно будет отключить в разделе Контроль приложений.

- **iOS**

  Для подключения и управления iOS-устройствами в режимах "Базовый контроль" и "Расширенный контроль" в выбранной группе администрирования должен быть установлен Сервер iOS MDM. Подробная информация об установке Сервера iOS MDM приведена в разделе Развертывание Сервера iOS MDM.

  На личные устройства в режиме "Базовая защита" будет установлено приложение *Kaspersky Protection для iOS*.

  На устройства в режимах "Базовый контроль" и "Расширенный контроль" будет установлен *управляющий профиль*.

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

- **Аврора**

  Для подключения устройств с ОС Аврора на устройствах должно быть предварительно установлено приложение Kaspersky Endpoint Security для ОС Аврора.

## Шаг 3. Принятие соглашений

На этом шаге выберите, кому необходимо принять Лицензионное соглашение и Политику конфиденциальности.

- **Администратор**

  Соглашения будут приняты администратором на следующем шаге мастера. В этом случае приложение пропустит этап принятия соглашений во время установки.

- **Пользователи**

  Соглашения будут приняты пользователями на мобильных устройствах.

Этот шаг применим только к операционным системам Android и iOS. При подключении устройств с ОС Аврора соглашения принимаются пользователями на мобильных устройствах.

Обратите внимание, что администратору будет предложено принять Лицензионное соглашение только после того, как эта же версия соглашения будет впервые принята пользователями на устройствах. После подключения и первой синхронизации устройств с Kaspersky Security Center администратор сможет принимать данную версию Лицензионного соглашения при последующих подключениях устройств.

Список принятых соглашений можно просмотреть в разделе **Лицензионные соглашения** свойств Сервера администрирования.

## Шаг 4. Лицензионное соглашение и Политика конфиденциальности

Если на предыдущем шаге мастера в качестве принимающего соглашения был выбран **Администратор**, вам будет предложено ознакомиться с Политикой конфиденциальности, Лицензионным соглашением и всеми связанными с ним документами. Перед установкой управляющих приложений на устройства необходимо принять условия и положения Лицензионного соглашения и Политики конфиденциальности.

## Шаг 5. Пользователи

На этом шаге выберите одного или нескольких пользователей подключаемых устройств. Выбранные пользователи получат информацию по установке приложения для подключения устройств к Kaspersky Security Center. Если пользователя нет в списке, можно добавить новую учетную запись, не выходя из мастера.

- Чтобы выбрать существующего пользователя, установите флажки рядом с соответствующими именами пользователей.
- Чтобы добавить нового пользователя, нажмите **Добавить пользователя**.

  a. Укажите учетные данные пользователя в разделе настроек **Учетные данные**.

  - **Имя пользователя**
  - **Пароль**

    Пароль должен соответствовать следующим требованиям сложности:

    - Пароль должен содержать от 8 до 16 символов.
    - Пароль должен содержать символы как минимум трех групп: верхний регистр (A-Z), нижний регистр (A-Z) (a-z), числа (0-9), специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).

  b. При необходимости укажите дополнительные данные в разделе параметров **Необязательная информация**.

  - **Полное имя пользователя**
  - **Описание**
  - **Адрес электронной почты**
  - **Номер телефона**

  c. Нажмите **OK**, чтобы сохранить изменения.

  Новый пользователь будет добавлен и отображен в списке пользователей.

- Чтобы изменить информацию о пользователе, нажмите **Изменить пользователя**.

  Поля, доступные для редактирования, зависят от подтипа пользователя - *внутренний* или *доменный*.

> После подключения устройства вы не сможете назначить другого пользователя владельцем устройства или удалить назначенного пользователя. Однако, если вы не назначили пользователя во время подключения устройства, вы можете назначить его позже через доставку мобильного сертификата.

## Шаг 6. Передача информации для подключения

На этом шаге выберите способ отправки QR-кодов и ссылок для установки управляющих приложений или управляющих профилей. Вы можете выбрать один из следующих способов:

- **Отправить письмо на адреса электронной почты пользователей**

  Выберите этот способ, чтобы отправить сведения о подключении по электронной почте выбранным пользователям. Чтобы установить приложение или управляющий профиль, пользователю необходимо отсканировать QR-код с помощью камеры мобильного устройства или открыть ссылку на инсталляционный пакет.

  > Адреса электронной почты должны быть указаны в учетных данных пользователей в Kaspersky Security Center.
  >
  > Если вы хотите отправить информацию для подключения на электронную почту, не указанную в учетных данных в Kaspersky Security Center, установите флажок **Отправить копию письма на дополнительный адрес электронной почты** и укажите нужный адрес.

- **Показать QR-коды и ссылки после завершения мастера**

  Выберите этот способ, чтобы отсканировать QR-код с помощью камеры мобильного устройства или перейти по ссылке в мастере.

## Шаг 7. Подтверждение

На этом шаге проверьте данные для подключения мобильного устройства, указанные на предыдущих шагах, и нажмите **Готово** для подтверждения операции.

> При выборе большого количества пользователей или групп пользователей создание QR-кодов и ссылок для подключения может занять несколько минут.

## Готово

На экране "Готово":

- Если вы выбрали **Отправить письмо на адреса электронной почты пользователей**, указанным пользователям будут отправлены электронные письма с QR-кодами и ссылками для подключения мобильных устройств к Серверу администрирования.

- Если вы выбрали **Показать QR-коды и ссылки после завершения мастера**, информация для подключения отобразится на экране "Готово". Информацию можно просмотреть на экране мастера или нажать **Скачать список**, чтобы получить файл с данными для подключения.

Нажмите **Закрыть**, чтобы выйти из мастера.

Когда пользователи установят управляющие приложения, устройства подключатся к Серверу администрирования и отобразятся на вкладке **Устройства** в Kaspersky Security Center Web Console.

Теперь вы можете настраивать параметры устройств и приложений для управления мобильными устройствами с помощью политик. Вы также сможете отправлять на мобильные устройства команды для защиты данных в случае потери или кражи устройств.

## Прямое подключение Android-устройств к Kaspersky Security Center

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

В зависимости от используемого метода аутентификации возможны два варианта подключения.

### Подключение с пользовательским сертификатом

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

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

### Подключение без пользовательского сертификата

При подключении устройства без пользовательского сертификата оно не будет привязано к учетной записи пользователя на Сервере администрирования. При этом, 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 аутентифицироваться с помощью сертификата будет только Сервер администрирования. После получения устройством пользовательского сертификата тип аутентификации будет изменен на двустороннюю (взаимную) SSL-аутентификацию.

## Перемещение нераспределенных мобильных устройств в группы администрирования

При подключении мобильных устройств к Kaspersky Security Center они отображаются на странице **Обнаружение устройств и развертывание** > **Нераспределенные устройства** Kaspersky Security Center Web Console. Для управления новыми подключенными устройствами можно создать правило для автоматического распределения устройств по группам администрирования, либо переместить их в группу администрирования вручную.

*Чтобы переместить нераспределенное мобильное устройство в группу администрирования:*

1. В главном окне Kaspersky Security Center Web Console выберите **Обнаружение устройств 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, в которую вы хотите переместить устройство.

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

4. Нажмите **Переместить**.

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

## Действия на мобильных устройствах для подключения к Серверу администрирования

В зависимости от режима, в котором будет работать устройство, вам может потребоваться выполнить дополнительные действия для защиты устройства и подключения его к Серверу администрирования.

### Установка мобильного сертификата

Если вы получили пароль сертификата, нужно использовать его для установки мобильного сертификата на устройство.

*Чтобы установить мобильный сертификат:*

1. Запомните или запишите пароль, который вы получили от администратора по электронной почте.

2. Выполните одно из следующих действий:

   - На Android-устройстве введите пароль сертификата при появлении запроса от Kaspersky Endpoint Security для Android.

   - На iOS-устройстве введите пароль сертификата при установке управляющего профиля.

Мобильный сертификат будет установлен на устройство.

### Предварительная настройка корпоративных Android-устройств

Чтобы подключить корпоративное Android-устройство к Серверу администрирования, нужно выполнить предварительную настройку устройства в зависимости от версии операционной системы и наличия сканера QR-кодов.

### Установка Kaspersky Endpoint Security для ОС Аврора

QR-код, который вы получили от вашего администратора, содержит параметры для подключения устройства к Серверу администрирования. Перед подключением устройства нужно установить Kaspersky Endpoint Security для ОС Аврора. Подробная информация об установке Kaspersky Endpoint Security для ОС Аврора приведена в справке Kaspersky Endpoint Security для ОС Аврора.

# Настройка параметров синхронизации

Для управления мобильными устройствами и получения отчетов или статистик от мобильных устройств пользователей требуется настроить параметры синхронизации. Синхронизация выполняется с помощью протокола HTTPS. Синхронизация мобильных устройств с Сервером администрирования может выполняться следующими способами:

- **По расписанию**. Вы можете настроить расписание синхронизации в параметрах политики. Изменения параметров политики, команды и задачи будут выполняться во время синхронизации устройства с Kaspersky Security Center по расписанию, то есть с задержкой.

  Из-за ограничений Doze, при выборе короткого периода синхронизации устройства могут синхронизироваться с Сервером администрирования реже.

  Использование коротких периодов синхронизации сокращает время работы устройства от батареи.

- **Принудительно**. Для синхронизации используются push-уведомления 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.

  Используйте команду **Синхронизировать устройство**, чтобы принудительно синхронизировать Android-устройство или iOS MDM-устройство.

  > Мобильные устройства не поддерживают кнопку **Синхронизировать сейчас** и флажок **Не разрывать соединение с Сервером администрирования** в окне свойств устройства.

*Чтобы настроить параметры синхронизации Android-устройств:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Параметры KES для Android**.
4. На карточке **Синхронизация по расписанию** нажмите **Параметры**.

   Откроется окно **Синхронизация по расписанию**.
5. Включите синхронизацию с помощью переключателя **Синхронизация по расписанию**.
6. В раскрывающемся списке **Период синхронизации** выберите интервал между операциями синхронизации устройств с Kaspersky Security Center. По умолчанию указано значение 3 часа.
7. Чтобы выключить синхронизацию устройств с Kaspersky Security Center в роуминге, установите флажок **Выключить синхронизацию в роуминге**.

   Пользователь устройства может выполнять синхронизацию вручную в настройках приложения (**Настройки** → **Настройки приложения** → **Синхронизация** → **Синхронизировать**).
8. Нажмите **OK**.
9. Нажмите **Сохранить**, 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.

*Чтобы настроить параметры синхронизации iOS-устройств в режиме "Базовая защита":*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Параметры KP для iOS**.
4. На карточке **Синхронизация по расписанию** нажмите **Параметры**.

   Откроется окно **Синхронизация по расписанию**.
5. Включите синхронизацию с помощью переключателя **Синхронизация по расписанию**.
6. В раскрывающемся списке **Период синхронизации** выберите интервал между операциями синхронизации устройств с Kaspersky Security Center. По умолчанию указано значение 6 часов.
7. Нажмите **OK**.
8. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

На некоторых iOS-устройствах синхронизация в фоновом режиме может быть выполнена позже, чем ожидается, если пользователь закрыл Kaspersky Protection для iOS смахиванием из переключателя приложений. Чтобы принудительно выполнить синхронизацию, пользователю необходимо повторно открыть приложение. Подробная информация об ограничениях и рекомендациях по оптимизации выполнения фоновых задач приведена в разделе Известные проблемы Kaspersky Protection для iOS.

## Управление сертификатами мобильных устройств

Kaspersky Security Center Web Console позволяет выпускать, обновлять или удалять мобильные, почтовые и VPN-сертификаты мобильных устройств.

В этом разделе содержится информация о том, как управлять сертификатами мобильных устройств и настраивать правила их выпуска.

## Перевыпуск мобильного сертификата Сервера администрирования

Вам необходимо указать резервный мобильный сертификат Сервера администрирования, чтобы обеспечить соответствие требованиям безопасности вашей организации и поддержать постоянное соединение управляемых устройств с Сервером. Мобильный сертификат, выпущенный средствами Kaspersky Security Center, перевыпускается 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** (в главном меню выберите → **Общие** → **Сертификаты**).

Максимальный срок действия любого сертификата Сервера администрирования – 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 нужно 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 главном окне Kaspersky Security Center Web Console нажмите на имя Сервера администрирования.
2. В окне свойств Сервера администрирования выберите **Общие** → **Сертификаты**.
3. Если вы планируете и дальше использовать сертификат, выпущенный Kaspersky Security Center:
   a. Нажмите **Перевыпустить**.
   b. В открывшемся окне:
      1. В разделе **Адрес подключения** выберите пункт **Оставить адрес подключения прежним** или пункт **Изменить адрес подключения на**, если будет использован новый адрес подключения.
      2. В разделе **Активировать новый сертификат** выберите **Через указанный срок (сут)** и укажите количество дней, через которое сертификат станет активным.

         Мы рекомендуем 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.

      3. Нажмите **OK**.

Если вы планируете использовать собственный сертификат:

a. Проверьте, соответствует ли ваш сертификат требованиям Kaspersky Security Center. При необходимости измените сертификат.

b. Выберите параметр **Другой сертификат** и нажмите **Управление сертификатом**.

c. В открывшемся окне нажмите **Обзор**.

d. В открывшемся окне выберите тип вашего сертификата и укажите расположение сертификата и параметры:

- Если вы выбрали **PKCS #12**, нажмите на кнопку **Обзор** рядом с полем **Сертификат** и укажите файл сертификата на жестком диске. Если файл сертификата защищен паролем, введите пароль в поле **Пароль**.
- Если вы выбрали **X.509**, нажмите на кнопку **Обзор** рядом с полем **Закрытый ключ** и укажите закрытый ключ на жестком диске. Если закрытый ключ защищен паролем, введите пароль в поле **Пароль**. Нажмите на кнопку **Обзор** рядом с полем **Сертификат** и укажите открытый ключ на жестком диске.

e. В разделе **Активировать новый сертификат** выберите **Через указанный срок (сут)** и укажите количество дней, через которое сертификат станет активным.

f. Нажмите **Сохранить**.

g. Нажмите **ОК**.

h. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Сертификат перевыпущен в качестве резервного сертификата.

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

Мы не рекомендуем 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 главном окне Kaspersky Security Center Web Console нажмите на имя Сервера администрирования.
2. В окне свойств Сервера администрирования выберите **Общие** → **Сертификаты**.

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

   a. Нажмите **Перевыпустить**.

   b. В открывшемся окне:

      1. В разделе **Адрес подключения** выберите пункт **Оставить адрес подключения прежним** или пункт **Изменить адрес подключения на**, если будет использован новый адрес подключения.

      2. В разделе **Активировать новый сертификат** выберите **Немедленно**.

      3. Нажмите **ОК**.

   Если вы планируете использовать собственный сертификат:

   a. Проверьте, соответствует ли ваш сертификат требованиям Kaspersky Security Center. При необходимости измените сертификат.

   b. Выберите параметр **Другой сертификат** и нажмите **Управление сертификатом**.

   c. В открывшемся окне нажмите **Обзор**.

   d. В открывшемся окне выберите тип вашего сертификата и укажите расположение сертификата и параметры:

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

      - Если вы выбрали **X.509**, нажмите на кнопку **Обзор** рядом с полем **Закрытый ключ** и укажите закрытый ключ на жестком диске. Если закрытый ключ защищен паролем, введите пароль в поле **Пароль**. Нажмите на кнопку **Обзор** рядом с полем **Сертификат** и укажите открытый ключ на жестком диске.

   e. В разделе **Активировать новый сертификат** выберите **Немедленно**.

   f. Нажмите **Сохранить**.

   g. Нажмите **ОК**.

   h. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

   Сертификат перевыпущен в качестве основного сертификата Сервера администрирования.

Дополнительная информация о сертификатах представлена в справке Kaspersky Security Center.

## Настройка правил выпуска сертификатов

Kaspersky Security Center Web Console позволяет настраивать порядок выпуска, обновления и защиты сертификатов для мобильных устройств.

*Чтобы настроить правила выпуска сертификатов:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Сертификаты**.

2. В открывшемся списке сертификатов выберите **Правила выпуска**.

   - В разделе **Параметры PKI**:

     a. В блоке настроек **Интеграция с PKI** включите переключатель **Интегрировать выпуск сертификатов с Microsoft Certification Authority (CA) через PKI** для автоматического выпуска сертификатов.

     Нажмите **Выбрать устройство** и укажите устройство с установленным Агентом администрирования, которое будет подключаться к Microsoft CA.

     Подробная информация об интеграции с PKI приведена в разделе Интеграция с инфраструктурой открытых ключей.

     b. В блоке настроек **Доменная учетная запись для передачи запросов на выпуск сертификатов** укажите **Имя учетной записи PKI** (имя учетной записи пользователя, которая будет использоваться для интеграции с PKI в формате `userPrincipalName@DNSDomainName`) и **Пароль** (доменный пароль учетной записи).

     c. Нажмите **Сохранить**, чтобы сохранить изменения.

   - В разделе **Мобильные сертификаты** можно настроить следующие параметры:

     a. В блоке настроек **Срок действия** в поле **Срок действия сертификата (дней)** укажите срок действия сертификата в днях. Срок действия сертификата по умолчанию составляет 365 дней. По истечении этого срока мобильное устройство не сможет подключиться к Серверу администрирования.

     b. В разделе настроек **Обновление** в поле **Обновить сертификат, когда осталось (дней)** укажите количество дней до окончания срока действия текущего сертификата, когда 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 30.

     Установите флажок **Обновлять сертификат автоматически** для автоматического выпуска сертификатов. Если флажок не установлен, сертификаты необходимо обновлять вручную по мере истечения срока их действия. По умолчанию флажок установлен.

     c. В блоке настроек **Защита паролем** установите флажок **Запрашивать пароль при установке сертификата** для запроса пароля у пользователя при установке сертификата на мобильное устройство. Пароль используется только один раз — при установке сертификата на мобильное устройство. Пароль будет автоматически сгенерирован Сервером администрирования и отправлен пользователю по электронной почте. В поле **Длина пароля** можно указать длину пароля.

     > Защита паролем доступна только для мобильных сертификатов.

     d. Нажмите **Сохранить**, чтобы сохранить изменения.

- В разделах **Почтовые сертификаты** и **VPN-сертификаты**, если настроена интеграция с PKI:

  a. В блоке настроек **Обновление** в поле **Обновить сертификат, когда осталось (дней)** укажите количество дней до окончания срока действия текущего сертификата, когда Сервер администрирования должен выпустить новый сертификат. Например, если указано значение 4, Сервер администрирования выпускает новый сертификат за четыре дня до окончания срока действия текущего.

  Установите флажок **Обновлять сертификат автоматически** для автоматического выпуска сертификатов. Если флажок не установлен, сертификаты необходимо обновлять вручную по мере истечения срока их действия. По умолчанию флажок установлен.

  b. В блоке настроек **Параметры PKI** укажите **Имя шаблона сертификата в системе PKI** (шаблон сертификата, который будет использоваться для выпуска сертификатов доменным пользователям).

  Под указанной учетной записью на устройстве, которое подключается к CA, запускается служба Агента администрирования для Windows. 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.

  c. В блоках настроек **Автоматический выпуск почтового сертификата при подключении устройства** или **Автоматический выпуск VPN-сертификата при подключении устройства** установите флажки **Выпускать для устройств под управлением Kaspersky Endpoint Security для Android** или **Выпускать для iOS MDM-устройств** для включения автоматического выпуска почтового или VPN-сертификата при подключении устройств к Kaspersky Security Center.

  Если вы установили флажок **Выпускать для iOS MDM-устройств**, выберите псевдоним сертификата в раскрывающемся списке. Псевдоним сертификата - это имя, которое идентифицирует сертификат. Вы можете настроить дальнейшее использование выбранного псевдонима для выпуска сертификата в следующих разделах:

  - Для почтовых сертификатов: в разделах Настройка почтового ящика на iOS MDM-устройствах и Настройка почтового ящика Exchange на iOS MDM-устройствах.
  - Для VPN-сертификатов: в разделах Настройка VPN на iOS MDM-устройствах и Подключение iOS MDM-устройств к сети Wi-Fi.

  Вы также можете изменить псевдоним для одного или нескольких почтовых и VPN-сертификатов, нажав кнопку **Изменить псевдоним** в списке сертификатов (**Управление активами** → **Мобильные** → **Сертификаты**).

  d. Нажмите **Сохранить**, чтобы сохранить изменения.

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

## Выпуск сертификатов для мобильных устройств

Вы можете выпускать мобильные, почтовые или VPN-сертификаты для мобильных устройств.

*Чтобы выпустить сертификат:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Сертификаты**.

2. В открывшемся списке сертификатов нажмите **Добавить**.

   Запустится Мастер выпуска сертификата. Нажмите **Начать** и продолжайте работу мастера с помощью кнопок **Назад** и **Далее**.

## Добро пожаловать

На экране приветствия можно прочитать краткое описание шагов Мастера выпуска сертификата.

Обратите внимание, что нумерация и набор шагов могут различаться в зависимости от типа сертификата, операционной системы и правил выпуска, указанных в разделе **Правила выпуска**.

## Шаг 1. Тип сертификата

На этом шаге выберите сертификат для выпуска.

- **Почтовый сертификат** (для корпоративной почты на устройствах).
- **VPN-сертификат** (для доступа к частным сетям и корпоративным веб-ресурсам).
- **Мобильный сертификат** (для идентификации мобильных устройств на Сервере администрирования).

## Шаг 2. Операционная система

На этом шаге выберите операционную систему устройств, для которых будет выпущен сертификат.

- **Android**
- **iOS**

## Шаг 3. Способ подключения

Этот шаг отображается только в случае, если вы выбрали **Почтовый сертификат** или **VPN-сертификат** в качестве типа сертификата и **Android** в качестве операционной системы устройств, для которых будет выпущен сертификат.

На этом шаге выберите способ подключения устройств к Серверу администрирования.

- **Подключение с помощью аутентификации по мобильному сертификату**

  Выберите этот параметр, чтобы мобильный сертификат использовался для идентификации пользователя при подключении к Серверу администрирования.

- **Подключение без аутентификации по мобильному сертификату**

Выберите этот вариант, если вы хотите установить сертификат на устройство без аутентификации по сертификату.

> Если на устройстве есть мобильный сертификат, он всегда будет использоваться для аутентификации.

## Шаг 4. Пользователи

На этом этапе выберите пользователей, которые получат информацию для установки сертификатов. Если пользователя нет в списке, можно добавить новую учетную запись, не выходя из мастера.

- Чтобы выбрать существующего пользователя, установите флажки рядом с соответствующими именами пользователей.
- Чтобы добавить нового пользователя, нажмите **Добавить пользователя**.

  a. Укажите учетные данные пользователя в разделе настроек **Учетные данные**.

  - **Имя пользователя**
  - **Пароль**

    Пароль должен соответствовать следующим требованиям сложности:

    - Пароль должен содержать от 8 до 16 символов.
    - Пароль должен содержать символы как минимум трех групп: верхний регистр (A-Z), нижний регистр (A-Z) (a-z), числа (0-9), специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).

  b. При необходимости укажите дополнительные данные в разделе параметров **Необязательная информация**.

  - **Полное имя пользователя**
  - **Описание**
  - **Адрес электронной почты**
  - **Номер телефона**

  c. Нажмите **OK**, чтобы сохранить изменения.

  Новый пользователь будет добавлен и отображен в списке пользователей.
- Чтобы изменить информацию о пользователе, нажмите **Изменить пользователя**.

Поля, доступные для редактирования, зависят от подтипа пользователя - *внутренний* или *доменный*.

## Шаг 5. Псевдоним и источник сертификата

На этом шаге выберите псевдоним и источник загрузки сертификата.

- **Псевдоним сертификата**

*Псевдоним сертификата* – это имя, которое идентифицирует сертификат. Вы можете настроить дальнейшее использование выбранного псевдонима в разделах политики: Настройка почтового ящика на iOS MDM-устройствах; Настройка почтового ящика Exchange на iOS MDM-устройствах; Настройка VPN на iOS MDM-устройствах; Подключение iOS MDM-устройств к сети Wi-Fi.

> Этот шаг доступен только в случае, если вы выбрали **Почтовый сертификат** или **VPN-сертификат** в качестве типа сертификата.

- **Интегрировать выпуск с Microsoft CA через PKI**

  Для этого параметра в поле **Шаблон PKI** укажите один из доступных шаблонов, импортированных из Microsoft CA.

  > Этот параметр доступен только в случае, если на вкладке Правила выпуска настроена интеграция с PKI.

- **Загрузить файл**

  Для этого параметра укажите **Формат сертификата**:

  - Для формата PKCS #12 в поле **Файл сертификата** нажмите **Выбрать** и укажите файл в формате P12 или PFX.
  - Для формата X.509 в поле **Файл приватного ключа** нажмите **Выбрать** и укажите файл в формате PRK или PEM.

    В поле **Файл сертификата** нажмите **Выбрать** и укажите файл в формате CER, CRT или CERT.

    После загрузки файлов вы также можете ввести пароль в поле **Пароль сертификата**.

## Шаг 6. Способ аутентификации

> Этот шаг отображается только в случае, если вы указали **Мобильный сертификат** в качестве типа сертификата, или если вы выбрали **Почтовый сертификат** или **VPN-сертификат** для Android-устройств и указали **Подключение без аутентификации по мобильному сертификату** в качестве способа подключения.

На этом шаге выберите способ аутентификации пользователя для получения сертификата.

- **Доменные или внутренние учетные данные пользователя**. Пользователи получат доступ к сертификату, используя доменные или внутренние учетные данные. Пользователям будет необходимо указать логин на мобильных устройствах в одном из форматов:
  - `userPrincipalName@DNSDomainName`
  - `sAMAccountName`
  - `sAMADomain\sAMAccountName`
- **Пароль**. Пользователи получат доступ к сертификату с помощью пароля, полученного по электронной почте или отображенного после завершения работы мастера.

В блоке настроек **Использование сертификата на устройстве** установите флажок **Разрешить повторное использование сертификата на одном устройстве (только для устройств с установленным приложением Kaspersky Endpoint Security для Android)**, если вы хотите разрешить использование одного сертификата несколько раз на одном устройстве.

Флажок доступен только в случае, если **Android** указан в качестве операционной системы устройств, для которых будет выпущен сертификат.

## Шаг 7. Передача информации о сертификате

На этом шаге выберите способ отправки информации для установки сертификата. Вы можете выбрать один из следующих способов:

- **Отправить письмо на адреса электронной почты пользователей**

  Выберите этот способ, чтобы отправить сведения для установки сертификата по электронной почте выбранным пользователям. Адреса электронной почты должны быть указаны в учетных данных пользователей в Kaspersky Security Center.

  Если вы хотите отправить информацию для установки сертификата на электронную почту, не указанную в учетных данных в Kaspersky Security Center, установите флажок **Отправить копию письма на дополнительный адрес электронной почты** и укажите нужный адрес.

- **Показать информацию после завершения мастера**

  Выберите этот параметр, чтобы отобразить сведения для установки сертификата на последнем этапе работы Мастера выпуска сертификата.

## Шаг 8. Подтверждение

На этом шаге проверьте данные для выпуска сертификата, указанные на предыдущих шагах, и нажмите **Подтвердить и выпустить сертификат** для подтверждения операции.

## Готово

На экране "Готово":

- Если вы выбрали **Отправить письмо на адреса электронной почты пользователей**, указанные пользователи получат электронные письма со сведениями для установки сертификата.

- Если вы выбрали **Показать информацию после завершения мастера**, сведения для установки сертификата будут отображены на экране "Готово". Информацию можно просмотреть на экране мастера или нажать **Скачать список**, чтобы получить файл с данными для подключения.

Нажмите **Закрыть**, чтобы выйти из мастера.

После завершения Мастера выпуска сертификата сертификаты будут выпущены и добавлены в список сертификатов. Вы можете удалять или обновлять выпущенные сертификаты, а также просматривать их свойства.

## Обновление сертификатов мобильных устройств

Если срок действия одного из сертификатов истекает, вы можете продлить его с помощью Kaspersky Security Center Web Console.

Выполнив действия, описанные ниже, вы можете обновить мобильный сертификат, а также почтовый или VPN-сертификат, выпущенный через PKI.

*Чтобы обновить сертификат:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Сертификаты**.
2. В открывшемся списке сертификатов выберите сертификат, который вы хотите обновить, и нажмите **Обновить**.

Статус сертификата изменился на **Сертификат обновлен**.

## Удаление сертификатов мобильных устройств

Вы можете удалить сертификаты мобильных устройств с помощью Kaspersky Security Center Web Console.

Обратите внимание, что в случае удаления мобильного сертификата устройство больше не сможет синхронизироваться с Сервером администрирования и им нельзя будет управлять средствами Kaspersky Security Center.

Сертификат удаляется только из Kaspersky Security Center Web Console и больше не обновляется, но остается на устройстве. Чтобы удалить сертификат с iOS MDM-устройств, корпоративных устройств или устройств с корпоративным контейнером, необходимо отправить команду Удалить корпоративные данные. На личных Android-устройствах пользователям необходимо удалить сертификат вручную.

При удалении мобильного сертификата iOS MDM-устройства устройство не удаляется из Kaspersky Security Center Web Console, но теряет возможность синхронизации с Сервером iOS MDM и ему присваивается статус "Неактивно". В этом случае необходимо удалить это устройство из списка управляемых устройств в Kaspersky Security Center Web Console, а затем подключить его заново с помощью Мастера подключения мобильного устройства.

*Чтобы удалить сертификат из Kaspersky Security Center Web Console:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Сертификаты**.
2. В открывшемся списке сертификатов выберите сертификат, который вы хотите удалить, и нажмите **Удалить**.

Сертификат удален и больше не отображается в списке сертификатов.

## Интеграция с инфраструктурой открытых ключей

Вы можете интегрировать выпуск сертификатов с Microsoft Certification Authority (CA) через инфраструктуру открытых ключей (PKI). Интеграция с PKI в первую очередь предназначена для упрощения выпуска доменных пользовательских сертификатов Сервером администрирования. В результате интеграции выписка сертификатов происходит автоматически.

Вы можете указать настройки для интеграции с PKI и назначить PKI в качестве источника сертификатов для определенных типов сертификатов. Параметры PKI задаются на вкладке **Правила выпуска** и позволяют выбрать индивидуальный шаблон по умолчанию для всех типов сертификатов.

Особенности использования интеграции с PKI для выпуска сертификатов:

- По умолчанию интеграция с PKI выключена. Ее можно включить используя переключатель **Интегрировать выпуск сертификатов с Microsoft Certification Authority (CA) через PKI**. Подробная информация о включении и настройке параметров PKI приведена в разделе Настройка правил выпуска сертификатов.

- Выпуск сертификатов осуществляется с помощью Агента администрирования для Windows, который обеспечивает интеграцию между Сервером администрирования и Microsoft CA. Поскольку устройств с установленным Агентом администрирования может быть несколько, вы можете указать конкретное устройство, которое будет подключаться к Microsoft CA, на вкладке **Правила выпуска**. На этом устройстве в хранилище сертификатов учетной записи, под которой выполняется интеграция с PKI, должен быть установлен сертификат Enrollment Agent (EA). Его предоставляет администратор доменного Центра сертификации.

- Учетная запись, под которой выполняется интеграция с PKI, должна принадлежать доменному пользователю и обладать разрешением на *Вход в качестве службы*.

- Kaspersky Security Center может одновременно работать только с одной интеграцией PKI (Microsoft CA).

Подробная информация о настройке интеграции с PKI для выпуска сертификатов приведена в разделе Настройка правил выпуска сертификатов.

## Настройка интеграции с PKI через Агент администрирования Windows

Доменные устройства на базе Linux не поддерживают нативную интеграцию с PKI. Для обеспечения интеграции между Сервером администрирования и Microsoft CA необходимо настроить промежуточное устройство Windows с установленным Агентом администрирования, который будет направлять запросы домена к CA.

*Чтобы настроить Microsoft Active Directory и CA для интеграции с PKI:*

1. Создайте доменную учетную запись пользователя, от имени которой будет осуществляться интеграция с PKI. Эта учетная запись будет использоваться для передачи запросов в Microsoft CA на выпуск сертификатов.

   a. Запустите secpol.msc.

   b. В открывшемся окне выберите **Local Policies** → **User Rights Assignment** → **Allow log as a service**, чтобы выдать доменной учетной записи разрешение *Log on as Service*.

2. Выдайте доменной учетной записи права на работу с CA.

   a. На стороне сервера с CA откройте оснастку certsrv.msc CA.

   b. Выберите CA и нажмите **Properties**.

c. На вкладке **Security** нажмите **Add**, а затем укажите ранее созданную доменную учетную запись.

d. Выдайте доменной учетной записи права **Issue and Manage certificates**.

e. Сохраните изменения.

3. Добавьте шаблон сертификата **Enrollment Agent** в список сертификатов для выпуска:

a. В оснастке CA нажмите правой кнопкой мыши **Certificate Templates** → **New** → **Certificate Template to Issue**.

b. Выберите шаблон **Enrollment Agent**, а затем нажмите **OK**.

c. Убедитесь, что у доменного пользователя есть доступ к шаблону сертификата:

a. В оснастке certsrv.msc нажмите **Certificate Templates** → **Manage**.

b. В открывшемся окне выберите **Properties** → **Security**.

c. В открывшемся окне убедитесь, что у пользователя есть права *Read & Enroll*.

*Чтобы настроить интеграцию с PKI через промежуточное устройство Windows с установленным Агентом администрирования:*

1. Подготовьте сервер, который будет выступать в качестве посредника между Kaspersky Security Center Linux и CA.

   Это должен быть сервер Windows в том же домене, что и CA.

2. Выдайте ранее созданной доменной учетной записи разрешение на доступ к промежуточному серверу Windows.

3. Войдите на сервер под доменной учетной записью, чтобы создать постоянный профиль пользователя и установить сертификат Enrollment Agent:

a. Войдите в устройство Windows, где будет развернут Агент администрирования.

b. Запустите certmgr.msc от имени администратора.

c. Нажмите **Personal** → **All Tasks** → **Request New Certificate...**, чтобы запустить мастер Certificate Enrollment.

   Следуйте шагам мастера с настройками по умолчанию.

d. На шаге **Request Certificates** выберите тип сертификата **Enrollment Agent**, а затем нажмите **Enroll**.

   После изменения статуса на "Succeeded" нажмите **Finish**.

> В случае возникновения ошибок подождите, пока политика будет применена на устройстве, или проверьте, что права пользователя в параметрах Permissions for Domain Controllers настроены правильно.

4. Выдайте доменной учетной записи на устройстве Windows разрешение *Log on as Service*.

    a. Запустите secpol.msc.

    b. В открывшемся окне выберите **Local Policies** → **User Rights Assignment** → **Allow log as a service**.

5. Установите Агент администрирования для Linux. Подробная информация об установке приведена в справке Kaspersky Security Center.

    - Установите Агент администрирования с настройками по умолчанию, за исключением адреса Сервера администрирования. Убедитесь, на устройстве с установленным Kaspersky Security Center открыт порт 13000.
    - Убедитесь, что соединение с устройством Windows установлено (в Kaspersky Security Center Web Console нажмите **Обнаружение устройств и развертывание** → **Нераспределенные устройства**).
    - Подождите 15 минут, пока не будет установлена первая синхронизация по расписанию Агента администрирования с Kaspersky Security Center.

## Просмотр списка сертификатов мобильных устройств

Kaspersky Security Center Web Console позволяет просматривать выпущенные сертификаты мобильных устройств и их свойства.

*Чтобы просмотреть список всех сертификатов и их свойства:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Сертификаты**.
2. В открывшемся окне вы можете просмотреть список всех созданных сертификатов и их свойства в таблице.

*Чтобы просмотреть свойства отдельного сертификата:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Сертификаты**.
2. В открывшемся списке сертификатов выберите сертификат, свойства которого вы хотите просмотреть.
3. В окне **Информация о сертификате** просмотрите свойства сертификата:
    - **Имя пользователя**
    - **Статус**
    - **Тип**
    - **Протокол**
    - **Источник**
    - **Дата истечения**
    - **Дата выпуска**

- **Последнее изменение статуса**
- **Псевдоним**
- **Автоматическое обновление выключено**
- **Отпечаток**

*Чтобы просмотреть сертификаты, установленные на iOS MDM устройстве:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.
2. В открывшемся списке устройств выберите устройство, сертификаты которого вы хотите просмотреть.
3. В открывшемся окне свойств устройства выберите раздел **Сертификаты**.

   Отобразится список установленных на устройстве сертификатов и их свойства.

   - **Имя сертификата**
   - **Сертификат пользователя**
   - **Отпечаток сертификата**

# Настройка и управление

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

# Контроль

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

## Настройка ограничений

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

### Настройка ограничений для личных Android-устройств

Эти параметры применяются к личным устройствам и устройствам с корпоративным контейнером.

Для обеспечения безопасности Android-устройств Kaspersky Mobile Devices Protection and Management позволяет настроить доступ пользователей к следующим функциям устройств:

- Wi-Fi;
- камера;
- Bluetooth.

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

*Чтобы настроить ограничения использования на устройстве Wi-Fi, камеры и Bluetooth:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Ограничения**.
4. На карточке **Ограничения функций устройств** нажмите **Параметры**.

   Откроется окно **Ограничения функций устройств**.
5. Включите параметры с помощью переключателя **Ограничения функций устройств**.
6. Настройте использование Wi-Fi, камеры и Bluetooth:

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

     На личных устройствах и устройствах с корпоративным контейнером под управлением Android 10 или 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 или 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 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.

7. Нажмите **OK**.
8. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

Вы также можете ограничить дополнительные функции операционной системы на корпоративных устройствах.

## Настройка ограничений для iOS MDM-устройств

Для выполнения требований корпоративной безопасности настройте ограничения в работе iOS MDM-устройств.

Функции, разрешенные в разделе политики **Ограничения**, но запрещенные в установленных на устройствах конфигурационных профилях, недоступны на устройствах.

### Настройка ограничений функций

*Чтобы настроить ограничения функций iOS MDM-устройств:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Ограничения**.
4. На карточке **Ограничения функций устройств** нажмите **Параметры**.

   Откроется окно **Ограничения функций устройств**.
5. Включите параметры с помощью переключателя **Ограничения функций устройств**.
6. Включите ограничения функций iOS MDM-устройств с помощью переключателей на соответствующих вкладках и выберите необходимые ограничения.

### Список ограничений функций устройств

- Ограничения на вкладке **Общие**:
  - В разделе **Параметры устройств**:
    - **Запретить голосовой набор на заблокированном устройстве**

      Использование функции голосового набора на заблокированном мобильном устройстве пользователя.

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

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

      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.

    - **Запретить 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 снят, пользователю доступна функция Handoff.

      Если флажок установлен, функция Handoff недоступна.

      По умолчанию флажок снят.

    - **Запретить изменение имени устройства**

      Возможность изменить имя мобильного устройства.

      Если флажок снят, пользователь может изменять имя мобильного устройства.

      Если флажок установлен, изменение имени устройства недоступно.

      По умолчанию флажок снят.

    - **Запретить изменение ограничений**

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 снят, пользователь может настроить параметры ограничений на мобильном устройстве.

Если флажок установлен, настройка параметров ограничения на мобильном устройстве недоступна.

По умолчанию флажок снят.

- **Запретить предложения Spotlight**

  Использование результатов поиска Spotlight в интернете в предложениях Siri. При использовании предложений Spotlight поисковые запросы и связанные с ними данные пользователя отправляются в компанию Apple.

  Если флажок снят, пользователь может разрешить отображение результатов поиска Spotlight в интернете в предложениях Siri.

  Если флажок установлен, результаты поиска Spotlight в интернете будут недоступны в предложениях Siri. Пользовательские данные не отправляются в компанию Apple.

  У пользователя может быть возможность разрешить результаты поиска Spotlight в интернете в предложениях Siri, даже если этот флажок установлен. Это связано с проблемой, известной Apple.

  По умолчанию флажок снят.

- В разделе **Защита от потери данных**:

  - **Запретить снимки и запись экрана**

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

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

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

    По умолчанию флажок снят.

  - **Запретить передачу документов из управляемых приложений в неуправляемые**

    Возможность открывать в неуправляемых (личных) приложениях на iOS MDM-устройстве документы, созданные с использованием управляемых (корпоративных) приложений и учетных записей. Неуправляемые приложения – приложения, установленные, настроенные и управляемые пользователем мобильного устройства.

Если флажок снят, пользователь может использовать неуправляемые приложения для открытия документов, созданных в управляемых корпоративных приложениях.

Если флажок установлен, пользователю не разрешается использовать неуправляемые приложения для открытия документов, созданных с использованием управляемых приложений. Например, этот параметр позволяет предотвратить открытие конфиденциального почтового вложения из управляемой учетной записи электронной почты в личных приложениях пользователя.

По умолчанию флажок снят.

- **Запретить передачу документов из неуправляемых приложений в управляемые**

  Возможность открывать в управляемых (корпоративных) приложениях на iOS MDM-устройстве документы, созданные с использованием неуправляемых (личных) приложений и учетных записей пользователя. Неуправляемые приложения – приложения, установленные, настроенные и управляемые пользователем мобильного устройства.

  Если флажок снят, пользователь может использовать управляемые приложения для открытия документов, созданных с использованием неуправляемых приложений.

  Если флажок установлен, пользователю не разрешается использовать управляемые приложения для открытия документов, созданных с использованием неуправляемых приложений. Например, параметр позволяет предотвратить открытие документа из личной учетной записи iCloud в корпоративном приложении.

  По умолчанию флажок снят.

- **Ограничить передачу содержимого буфера обмена между управляемыми и неуправляемыми приложениями**

  Ограничивает возможность копировать и вставлять содержимое, если выбран хотя бы один из следующих флажков:

  - **Запретить передачу документов из управляемых приложений в неуправляемые**
  - **Запретить передачу документов из неуправляемых приложений в управляемые**

  Если флажок установлен, пользователь устройства не может использовать буфер обмена.

  Если флажок снят, пользователь устройства может использовать буфер обмена.

  По умолчанию флажок снят.

  Если этот флажок выбран, использование пользователем буфера обмена определяется различными комбинациями ограничений **Запретить передачу документов из управляемых приложений в неуправляемые** и **Запретить передачу документов из неуправляемых приложений в управляемые**.

| Запретить передачу документов из управляемых приложений в неуправляемые | Запретить передачу документов из неуправляемых приложений в управляемые | Ограничение функций |
|---|---|---|
| Включено | Включено | Пользователь не может копировать и вставлять данные. |
| Включено | Выключено | Пользователь может копировать данные из управляемых приложений и вставлять их в неуправляемые приложения.<br>Пользователь не может копировать данные из неуправляемых приложений и вставлять их в управляемые приложения. |

| | | |
|---|---|---|
| Выключено | Включено | Пользователь может копировать данные из неуправляемых приложений и вставлять их в управляемые приложения.<br>Пользователь не может копировать данные из управляемых приложений и вставлять их в неуправляемые приложения. |
| Выключено | Выключено | Пользователь может копировать данные из управляемых приложений и вставлять их в неуправляемые приложения.<br>Пользователь может копировать данные из неуправляемых приложений и вставлять их в управляемые приложения. |

- **Выключить шифрование резервных копий**

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

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

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

  По умолчанию флажок снят.

- **Запретить сброс настроек до заводских**

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

  Если флажок снят, пользователю доступна функция удаления всех данных с устройства и сброса настроек до заводских.

  Если флажок установлен, функция сброса настроек до заводских недоступна.

  По умолчанию флажок снят.

- **Запретить изменение параметров учетной записи**

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

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

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

  По умолчанию флажок снят.

- В разделе **Безопасность и конфиденциальность**:

  - **Запретить 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 снят, пользователь после предупреждения может разрешить отправку отчетов с диагностической информацией и сведений об использовании мобильного устройства в компанию Apple.

Если флажок установлен, отправка отчетов с диагностической информацией и сведениями об использовании мобильного устройства в компанию Apple блокируется.

По умолчанию флажок снят.

- **Запретить изменение пароля**

  Возможность установки, изменения или удаления пароля разблокировки мобильного устройства.

  Если флажок снят, пользователь может установить, изменить или удалить пароль для разблокировки мобильного устройства.

  Если флажок установлен, управление паролем разблокировки устройства недоступно.

  По умолчанию флажок снят.

- **Запретить изменение параметров Touch ID и Face ID**

  Возможность добавления и удаления отпечатков Touch ID или данных Face ID.

  Если флажок снят, пользователь может добавлять и удалять отпечатки Touch ID или данные Face ID.

  Если флажок установлен, управление отпечатками Touch ID и данными Face ID недоступно.

  По умолчанию флажок снят.

- **Запретить использование Touch ID и Face ID для разблокировки устройства**

  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, Book Store и входа в приложения.

  Если флажок снят, пользователь может использовать отпечаток пальца или распознавание лица вместо ввода пароля для разблокировки мобильного устройства.

  Если флажок установлен, пользователь не может использовать Touch ID и Face ID для разблокирования мобильного устройства.

  По умолчанию флажок снят.

- **Запрашивать пароль для каждой покупки в iTunes Store**

  Использование пароля при покупке медиаконтента в iTunes Store.

  Если флажок установлен, перед совершением первой покупки в iTunes Store пользователь должен задать пароль 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 в течение следующих 15 минут.

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

По умолчанию флажок снят.

- **Запрашивать 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.

- **Запретить установку конфигурационных профилей**

  Использование дополнительных конфигурационных профилей на iOS MDM-устройстве.

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

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

  По умолчанию флажок снят.

- **Запретить сторонние соединения**

  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 снят, пользователь может синхронизировать iOS MDM-устройство с другими устройствами, а также с сервисами Apple.

  Если флажок установлен, сторонние соединения на мобильном устройстве пользователя блокируются.

  По умолчанию флажок снят.

- **Запретить изменение параметров отправки диагностических данных**

  Автоматическое получение диагностической информации и сведений об использовании iOS MDM-устройства и отправка отчета с этими данными в компанию Apple для анализа.

  Если флажок снят, пользователь может настраивать отправку отчетов с диагностической информацией и сведений об использовании мобильного устройства в компанию Apple.

  Если флажок установлен, настройка параметров отправки отчетов с диагностической информацией недоступна.

  По умолчанию флажок снят.

- В разделе **iCloud**:

  - **Запретить 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 снят, 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 установлен, пользователь не может сохранять резервные копии данных мобильного устройства в iCloud.

По умолчанию флажок снят.

- **Запретить хранение документов и данных в iCloud**

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

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

  Если флажок установлен, пользователю запрещено сохранять документы в iCloud.

  По умолчанию флажок снят.

- **Запретить Связку ключей iCloud**

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

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

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

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

  По умолчанию флажок снят.

- **Запретить управляемым приложениям хранить данные в iCloud**

  Создание резервной копии данных управляемых приложений в iCloud.

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

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

  По умолчанию флажок снят.

- **Запретить 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 снят, пользователю доступно резервное копирование корпоративных книг с помощью iCloud или iTunes.

Если флажок установлен, резервное копирование корпоративных книг невозможно.

По умолчанию флажок снят.

- **Запретить синхронизировать заметки и выделения цветом в корпоративных книгах**

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

  Если флажок снят, пользователь может синхронизировать заметки, закладки и выделенный текст в корпоративных книгах. При этом изменения будут доступны на всех Apple-устройствах пользователя, подключенных к iCloud.

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

  По умолчанию флажок снят.

- **Запретить 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 снят, 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 установлен, функция общий доступ к фото в iCloud недоступна пользователю мобильного устройства. 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 снят.

- **Запретить медиатеку iCloud**

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

  Если флажок снят, пользователю доступна медиатека iCloud при работе с приложением "Фото".

  Если флажок установлен, пользователю недоступна медиатека iCloud. Фотографии и видео пользователя, сохраненные в медиатеке iCloud, удаляются с сервера iCloud.

  По умолчанию флажок снят.

- В разделе **Сертификаты**.

  - **Запретить пользователям использовать недоверенные TLS-сертификаты**

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

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

Если флажок установлен, использование недоверенных TLS-сертификатов заблокировано.

По умолчанию флажок снят.

- **Запретить автоматическое обновление доверенных сертификатов**

  Автоматические обновления доверенных сертификатов на iOS MDM-устройстве.

  Если флажок снят, изменения в параметрах доверия сертификата принимаются автоматически.

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

  По умолчанию флажок снят.

- Ограничения на вкладке **Приложения**:
  - В разделе **Общие**:
    - **Запретить использование камеры**

      Использование камеры на мобильном устройстве пользователя.

      Если флажок снят, пользователь может использовать камеру устройства.

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

      По умолчанию флажок снят.

    - **Запретить FaceTime**

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

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

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

      По умолчанию флажок снят.

    - **Запретить iMessage**

      Использование службы iMessage на мобильном устройстве пользователя.

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

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

По умолчанию флажок снят.

- **Запретить Book Store**

  Доступ в интернет-магазин Book Store из приложения "Книги" на мобильном устройстве пользователя.

  Если флажок снят, пользователь может переходить в интернет-магазин Book Store из приложения "Книги", установленного на устройстве.

  Если флажок установлен, пользователь не может переходить в Book Store из приложения "Книги".

  По умолчанию флажок снят.

- **Запретить устанавливать приложения из Apple Configurator и iTunes**

  Возможность самостоятельно устанавливать приложения на iOS MDM-устройство.

  Если флажок снят, пользователь может самостоятельно устанавливать или обновлять приложения на мобильном устройстве из App Store с помощью iTunes или Apple Configurator.

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

  По умолчанию флажок снят.

- **Запретить устанавливать приложения из App Store**

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

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

  Если флажок установлен, 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 снят.

- **Запретить автоматическую загрузку приложений**

  Использование автоматической загрузки приложений на мобильном устройстве пользователя. Флажок доступен, если снят флажок **Запретить устанавливать приложения из Apple Configurator и iTunes**.

Если флажок снят, автоматическая загрузка приложений доступна для пользователя. После включения этой функции приложения, которые пользователь загрузил из App Store, автоматически устанавливаются на другие Apple-устройства пользователя.

Если флажок установлен, автоматическая загрузка приложений выключена и недоступна.

По умолчанию флажок снят.

- **Запретить встроенные покупки**

  Использование системы встроенных покупок на мобильном устройстве.

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

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

  По умолчанию флажок снят.

- **Запретить 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.

  Если флажок снят, пользователь может настраивать доверие к корпоративным приложениям.

  Если флажок установлен, пользователь не может установить доверие к корпоративным приложениям при установке приложения вручную.

  По умолчанию флажок снят.

- **Запретить удалять приложения**

  Возможность удаления приложений с мобильного устройства.

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

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

  По умолчанию флажок снят.

- В разделе **AirPrint**:

  - **Запретить AirPrint**

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

    По умолчанию флажок снят.

- **Запретить хранение учетных данных AirPrint**

  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 11 и выше.

  По умолчанию флажок снят.

- **Запретить обнаружение iBeacon для принтеров AirPrint**

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

  Ограничение поддерживается на устройствах с iOS 11 и выше.

  По умолчанию флажок снят.

- **Принудительно использовать доверенный TLS-сертификат для AirPrint**

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

  Ограничение поддерживается на устройствах с iOS 11 и выше.

  По умолчанию флажок снят.

- В разделе **AirDrop**:

  - **Запретить AirDrop**

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

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

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

    По умолчанию флажок снят.

  - **Считать AirDrop управляемым приложением**

    Использование AirDrop в качестве управляемого приложения для передачи данных с мобильного устройства на другие устройства Apple. Для работы этого ограничения необходимо установить флажок **Запретить передачу документов из управляемых приложений в неуправляемые**. Неуправляемые приложения – приложения, установленные, настроенные и управляемые пользователем мобильного устройства.

    Если флажок снят, AirDrop считается неуправляемым приложением.

    Если флажок установлен, AirDrop считается управляемым приложением.

    По умолчанию флажок снят.

- В разделе **Apple Music**:
  - **Запретить Apple Music**

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

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

    Если флажок установлен, сервис Apple Music недоступен для пользователя.

    По умолчанию флажок снят.

  - **Запретить радио в Apple Music**

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

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

    Если флажок установлен, прослушивание радио недоступно для пользователя.

    По умолчанию флажок снят.

- В разделе **Apple Watch**:
  - **Выключить распознавание запястья для Apple Watch**

    Автоматическое блокирование Apple Watch, когда пользователь снимает часы с руки.

    Если флажок снят, часы Apple Watch блокируются, когда пользователь снимает их с руки. Для разблокирования пользователь должен ввести пароль на своем мобильном устройстве.

    Если флажок установлен, блокировка Apple Watch после снятия с руки недоступна.

    По умолчанию флажок снят.

  - **Запретить создавать пару с Apple Watch**

    Создание пары Apple Watch и контролируемого мобильного устройства.

    Если флажок снят, пользователь контролируемого мобильного устройства может создать пару с Apple Watch.

    Если флажок установлен, создание пары с Apple Watch недоступно.

    По умолчанию флажок снят.

- В разделе **Siri**:
  - **Запретить использование Siri**

    Использование приложения Siri на мобильном устройстве пользователя.

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

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

По умолчанию флажок снят.

- **Запретить на заблокированном устройстве**

  Использование голосовых команд Siri, когда мобильное устройство пользователя заблокировано. На мобильном устройстве пользователя должен быть установлен пароль.

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

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

  По умолчанию флажок снят.

- **Запретить фильтр нецензурной лексики**

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

  Если флажок снят, при использовании Siri фильтруется нецензурная лексика.

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

  По умолчанию флажок снят.

- **Запретить Siri поиск в интернете**

  Этот параметр запрещает Siri использовать поиск в интернете для голосовых команд на iOS MDM-устройстве.

  Если флажок снят, Siri может искать в интернете ответы на вопросы пользователя.

  Если флажок установлен, Siri не сможет искать информацию в интернете.

  По умолчанию флажок снят.

- В разделе **Локатор**:

  - **Запретить поиск устройств в приложении "Локатор"**

    Установка или снятие флажка определяет, может ли пользователь искать устройства в приложении "Локатор".

    Ограничение поддерживается на устройствах с iOS 13 и выше.

    По умолчанию флажок снят.

  - **Запретить поиск друзей в приложении "Локатор"**

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

    Ограничение поддерживается на устройствах с iOS 13 и выше.

По умолчанию флажок снят.

- В разделе **Класс**:
  - **Запретить просматривать экраны в "Классе"**

    Возможность для преподавателя просматривать экраны iPad студентов с помощью программы "Класс".

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

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

    По умолчанию флажок снят.

- Ограничения на вкладке **Хранилище**:
  - В разделе **Общие**:
    - **Запретить доступ к USB-устройствам в приложении "Файлы"**

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

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

      Параметр доступен для мобильных устройств под управлением iOS 13.1 и выше.

      По умолчанию флажок снят.

    - **Выключать доступ к USB-устройствам, когда устройство заблокировано**

      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.

      Параметр доступен для мобильных устройств под управлением iOS 11.4.1 и выше.

      По умолчанию флажок снят.

- Ограничения на закладке **Сеть**:
  - В разделе **Общие**:
    - **Запретить использование NFC**

      Если флажок снят, использование NFC разрешено.

      Если флажок установлен, использование NFC запрещено.

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

По умолчанию флажок снят.

- **Запретить создавать конфигурации VPN**

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

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

  Параметр доступен для мобильных устройств под управлением iOS 11 и выше.

  По умолчанию флажок снят.

- **Запретить изменение параметров eSIM**

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

  Ограничение поддерживается на устройствах с iOS 11 и выше.

  По умолчанию флажок снят.

- В разделе **Wi-Fi**:

  - **Принудительно включать Wi-Fi**

    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.

    Параметр доступен для мобильных устройств под управлением iOS 13 и выше.

    По умолчанию флажок снят.

  - **Принудительно подключаться только к разрешенным сетям Wi-Fi**

    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.

    Параметр доступен для мобильных устройств под управлением iOS 14.5 и выше.

    По умолчанию флажок снят.

  - **Запретить изменять настройки Режима модема**

    Если флажок снят, пользователь устройства может изменять настройки Режима модема.

    Если флажок установлен, пользователь устройства не может изменять настройки Режима модема.

Параметр доступен для мобильных устройств под управлением iOS 12.2 и выше.

По умолчанию флажок снят.

- В разделе **Bluetooth**:
  - **Запретить изменять настройки Bluetooth**

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

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

    Параметр доступен для мобильных устройств под управлением iOS 11 и выше.

    По умолчанию флажок снят.

- В разделе **Сотовая связь**:
  - **Запретить автоматическую синхронизацию в роуминге**

    Запретить автоматическую синхронизацию данных пользователя, когда iOS MDM-устройство находится в роуминге.

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

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

    По умолчанию флажок снят.

  - **Запретить изменение параметров сотовой связи**

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

    Если флажок снят, пользователь может настраивать параметры передачи данных по сотовой сети.

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

    По умолчанию флажок снят.

- Ограничения на вкладке **Дополнительные параметры**:
  - В разделе **Экран**:
    - **Запретить изменение обоев**

      Возможность выбрать изображение, которое будет отображаться на экране блокировки или экране "Домой".

      Если флажок снят, пользователь может выбрать обои для мобильного устройства.

      Если флажок установлен, выбор обоев недоступен.

По умолчанию флажок снят.

- В разделе **Текст**:
  - **Запретить проверку правописания**

    Использование функции правописания при наборе текста на мобильном устройстве. Проверка правописания подчеркивает неправильно введенные слова и предлагает варианты замены.

    Если флажок снят, пользователь может включить и использовать функцию правописания.

    Если флажок установлен, при наборе текста проверка правописания недоступна.

    По умолчанию флажок снят.

  - **Запретить автокоррекцию**

    Использование функции автокоррекции при наборе текста.

    Если флажок снят, пользователь может включить и использовать функцию автокоррекции.

    Если флажок установлен, при наборе текста автокоррекция недоступна.

    По умолчанию флажок снят.

  - **Запретить поиск слова в словаре**

    Использование словаря для получения определений слов на мобильном устройстве. Словарь является функцией только виртуальной клавиатуры.

    Если флажок снят, пользователь может выделить любое слово на экране мобильного устройства и получить его определение.

    Если флажок установлен, поиск слова в словаре недоступен.

    По умолчанию флажок снят.

- В разделе **Клавиатура**:
  - **Запретить предиктивный набор**

    Использование функции предиктивного набора текста. Функция предиктивного набора текста показывает варианты окончания слов и предложений на основе имеющихся словарей.

    Если флажок снят, пользователь может включить и использовать функцию предиктивного набора текста.

    Если флажок установлен, функция предиктивного набора текста недоступна. При наборе текста подсказки не отображаются.

    По умолчанию флажок снят.

  - **Запретить сочетания клавиш**

Использование сочетаний клавиш для быстрого доступа к функциям мобильного устройства.

Если флажок снят, пользователь может включить функцию сочетания клавиш и использовать ее при работе с мобильным устройством.

Если флажок установлен, функция сочетания клавиш недоступна.

По умолчанию флажок снят.

- В разделе **Уведомления**:
  - **Запретить Wallet показывать уведомления на заблокированном экране**

    Использование уведомлений приложения Wallet на экране блокировки iOS MDM-устройства.

    Если флажок снят, на экране блокировки мобильного устройства отображаются уведомления Wallet.

    Если флажок установлен, уведомления Wallet на экране блокировки мобильного устройства не отображаются. Для работы с Wallet пользователь должен разблокировать устройство.

    По умолчанию флажок снят.

  - **Скрывать Пункт управления на заблокированном экране**

    Возможность перейти в Пункт управления iOS MDM-устройством, когда устройство заблокировано.

    Если флажок снят, пользователь может перейти в Пункт управления, когда мобильное устройство заблокировано.

    Если флажок установлен, пользователь не может перейти в Пункт управления, когда мобильное устройство заблокировано.

    По умолчанию флажок снят.

  - **Скрывать Центр уведомлений на заблокированном экране**

    Возможность перейти в Центр уведомлений iOS MDM-устройства, когда оно заблокировано.

    Если флажок снят, пользователь может перейти в Центр уведомлений, смахнув экран блокировки вниз.

    Если флажок установлен, пользователь не может перейти в Центр уведомлений, когда мобильное устройство заблокировано.

    По умолчанию флажок снят.

  - **Скрывать представление "Сегодня" на заблокированном экране**

Отображение сведений из представления "Сегодня" на заблокированном iOS MDM-устройстве. В представлении "Сегодня" Центра уведомлений отображаются следующие сведения:

- события в календаре;
- напоминания;
- акции;
- погода.

Если флажок снят, пользователь может просматривать уведомления из представления "Сегодня" на заблокированном мобильном устройстве.

Если флажок установлен, представление "Сегодня" не отображается на заблокированном мобильном устройстве.

По умолчанию флажок снят.

- **Запретить изменение параметров уведомлений**

Возможность настройки отображения уведомлений на мобильном устройстве.

Если флажок снят, пользователь может настроить параметры отображения уведомлений на мобильном устройстве.

Если флажок установлен, настройка параметров отображения уведомлений недоступна.

По умолчанию флажок снят.

- Ограничения на закладке **Обновление ОС**:
  - В разделе **Общие**:
    - **Отложить обновление операционной системы (дней)**

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 **Количество дней от 1 до 90**.

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

Параметр доступен для мобильных устройств под управлением iOS 11.3 и выше.

По умолчанию флажок снят.

7. Нажмите **ОК**.

8. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

В результате после применения политики на мобильном устройстве пользователя будут настроены ограничения функций.

## Настройка ограничений приложений

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **iOS** и перейдите в раздел **Ограничения**.

4. На карточке **Ограничения приложений** нажмите **Параметры**.

   Откроется окно **Ограничения приложений**.

5. Включите параметры с помощью переключателя **Ограничения приложений**.

6. Настройте ограничения приложений на iOS MDM-устройствах.

   **Список ограничений приложений**

   Ограничения в разделе **Safari**:

   - **Разрешить использование Safari**

     Использование браузера Safari на iOS MDM-устройстве.

     Если флажок установлен, пользователь может использовать браузер Safari.

     Если флажок снят, пользователю запрещено использовать браузер Safari. Значок Safari скрыт с главного экрана iOS MDM-устройства.

     По умолчанию флажок установлен.

   - **Разрешить использование автозаполнения**

     Сохранение и автоматическая подстановка данных, которые пользователь вводит при заполнении веб-форм в браузере Safari.

     Если флажок установлен, пользовательские данные, введенные в веб-формы, будут сохраняться. Позднее они будут автоматически подставляться в веб-формы.

     Если флажок снят, пользовательские данные не подставляются в веб-формы.

     По умолчанию флажок установлен.

   - **Предупреждать пользователя о переходе на опасный сайт**

     Параметр, включающий предупреждение пользователя перед посещением сайта, который решение Kaspersky Mobile Devices Protection and Management признало опасным.

     Если флажок установлен, Kaspersky Mobile Devices Protection and Management предупреждает пользователя при посещении опасных сайтов.

     Если флажок снят, Kaspersky Mobile Devices Protection and Management не предупреждает пользователя о посещении опасных сайтов.

     По умолчанию флажок снят.

   - **Разрешить использование JavaScript**

     Использование JavaScript браузером Safari.

Если флажок установлен, браузер Safari использует JavaScript при открытии сайтов.

Если флажок снят, браузер Safari не использует JavaScript при открытии сайтов.

По умолчанию флажок установлен.

- **Блокировать всплывающие окна**

  Блокирование всплывающих окон в браузере Safari.

  Если флажок установлен, Kaspersky Mobile Devices Protection and Management блокирует всплывающие окна в браузере Safari.

  Если флажок снят, Kaspersky Mobile Devices Protection and Management не блокирует всплывающие окна в браузере Safari.

  По умолчанию флажок снят.

- **Параметры cookie**

  Выбор условия приема файлов cookie:

  - **Разрешить cookie и отслеживание на сайтах**. Браузер Safari принимает файлы cookie и позволяет отслеживать действия пользователей.
  - **Разрешить cookie и запретить отслеживание на сайтах**. Браузер Safari принимает файлы cookie и блокирует отслеживание действий пользователей.
  - **Запретить cookie и отслеживание на сайтах**. Браузер Safari блокирует файлы cookie и отслеживание действий пользователей.

  Значение по умолчанию: **Разрешить cookie и отслеживание на сайтах**.

Ограничения в разделе **Game Center**:

- **Разрешить использование Game Center**

  Доступ к игровому сервису Game Center из приложения Game Center на iOS MDM-устройстве.

  Если флажок установлен, пользователь может переходить в игровой сервис Game Center из приложения Game Center на мобильном устройстве.

  Если флажок снят, пользователь не может переходить в игровой сервис Game Center из приложения Game Center на мобильном устройстве. Значок Game Center удален с главного экрана iOS MDM-устройства.

  По умолчанию флажок установлен.

- **Разрешить добавление друзей в Game Center**

  Добавление пользователей в игровом сервисе Game Center на iOS MDM-устройстве.

  Если флажок установлен, пользователь может добавлять других пользователей в игровом сервисе Game Center на мобильном устройстве.

  Если флажок снят, пользователю запрещено добавлять других пользователей в игровом сервисе Game Center на мобильном устройстве.

  По умолчанию флажок установлен.

- **Разрешить многопользовательские игры в Game Center**

Использование игрового сервиса Game Center в многопользовательском режиме на iOS MDM-устройстве.

Если флажок установлен, пользователь может участвовать в многопользовательских играх в приложении Game Center на мобильном устройстве.

Если флажок снят, пользователь не может участвовать в многопользовательских играх в приложении Game Center на мобильном устройстве.

Даже если флажок снят, пользователи могут вместе играть в игры с помощью SharePlay или сторонней службы.

По умолчанию флажок установлен.

Ограничения в разделе **Дополнительные параметры**:

- **Разрешить использование iTunes Store**

  Доступ к медиасервису iTunes Store из приложения iTunes на iOS MDM-устройстве.

  Если флажок установлен, пользователь может просматривать, покупать и загружать медиаконтент из сервиса iTunes Store с помощью приложения iTunes на мобильном устройстве.

  Если флажок снят, пользователь не может просматривать, покупать и загружать медиаконтент из сервиса iTunes Store с помощью приложения iTunes на мобильном устройстве. Значок iTunes скрыт с главного экрана iOS MDM-устройства.

  По умолчанию флажок установлен.

- **Разрешить использование News**

  Просмотр новостей на мобильном устройстве пользователя с помощью приложения News.

  Если флажок установлен, пользователь может просматривать новости с помощью приложения News.

  Если флажок снят, приложение News недоступно для пользователя.

  По умолчанию флажок установлен.

- **Разрешить использование приложения "Подкасты"**

  Прослушивание подкастов на мобильном устройстве пользователя с помощью приложения "Подкасты".

  Если флажок установлен, пользователь может искать, воспроизводить и загружать подкасты с помощью приложения "Подкасты".

  Если флажок снят, загрузка подкастов на мобильное устройства недоступна.

  По умолчанию флажок установлен.

7. Нажмите **OK**.

8. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

В результате после применения политики на мобильном устройстве пользователя будут настроены ограничения приложений.

## Настройка ограничений медиаконтента

Категории, используемые для ограничений медиаконтента, определяются Apple. В некоторых случаях фактические результаты настройки ограничений медиаконтента могут отличаться от ожидаемых.

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Ограничения**.
4. На карточке **Ограничения медиаконтента** нажмите **Параметры**.

   Откроется окно **Ограничения медиаконтента**.
5. Включите параметры с помощью переключателя **Ограничения медиаконтента**.
6. Настройте ограничения медиаконтента на iOS MDM-устройствах.

   **Список ограничений медиаконтента**

   **Регион**

   Выбор страны, система рейтингов которой автоматически применяется к медиаконтенту на iOS MDM-устройстве.

   По умолчанию выбрано значение **United States**.

   Параметры в разделе **Возрастной рейтинг**:

   - **Видео**

     Выбор ограничительного рейтинга для доступа к фильмам на iOS MDM-устройстве.

     Список рейтингов зависит от выбранного региона.

     Если выбран вариант **Разрешить все**, пользователь может просматривать любые фильмы на мобильном устройстве.

     Вариант **Разрешить все** выбран по умолчанию.

   - **Телевизионные передачи**

     Выбор ограничительного рейтинга для доступа к телевизионным передачам на iOS MDM-устройстве.

     Список рейтингов зависит от выбранного региона.

     Если выбран вариант **Разрешить все**, пользователь может просматривать любые телевизионные передачи на мобильном устройстве.

     Вариант **Разрешить все** выбран по умолчанию.

- **Приложения**

  Выбор ограничительного рейтинга для доступа к сторонним приложениям на iOS MDM-устройстве.

  Список рейтингов зависит от выбранной системы рейтингов.

  Если выбран вариант **Разрешить все**, пользователь может использовать любые сторонние приложения на мобильном устройстве.

  Вариант **Разрешить все** выбран по умолчанию.

  Ограничения приложений могут применяться даже в том случае, если выбран вариант **Разрешить все**. Это связано с проблемой, известной Apple.

- **Разрешить загрузку книг с пометкой "эротика" в Apple Books**

  Доступ к контенту с содержанием для взрослых в интернет-магазине Book Store на мобильном устройстве пользователя.

  Если флажок установлен, пользователь может загрузить контент с содержанием для взрослых из приложения "Книги" на iOS MDM-устройство.

  Если флажок снят, пользователь не может загрузить контент с содержанием для взрослых из приложения "Книги" на iOS MDM-устройство.

  По умолчанию флажок установлен.

- **Разрешить воспроизведение откровенного контента**

  Доступ к откровенному медиаконтенту из приложения iTunes Store на iOS MDM-устройстве. Ограничения накладываются провайдерами iTunes Store.

  Если флажок установлен, откровенный медиаконтент, приобретенный в iTunes Store, доступен пользователю мобильного устройства.

  Если флажок снят, откровенный медиаконтент, приобретенный в iTunes Store, скрыт от пользователя мобильного устройства.

  По умолчанию флажок установлен.

7. Нажмите **OK**.

8. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

В результате после применения политики на мобильном устройстве пользователя будут настроены ограничения медиаконтента.

## Настройка доступа пользователей к сайтам

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

## Настройка доступа к сайтам на Android-устройствах

Вы можете настраивать доступ пользователей Android-устройств к сайтам с помощью Веб-Контроля. Веб-Контроль поддерживает фильтрацию сайтов по категориям, определенным в облачной службе Kaspersky Security Network. Фильтрация позволяет вам ограничить доступ пользователей к отдельным сайтам или категориям сайтов (например, "Азартные игры, лотереи, тотализаторы" или "Общение в сети"). По умолчанию Веб-Контроль включен.

В Яндекс Браузере и Samsung Internet вредоносные и фишинговые веб-адреса могут оставаться незаблокированными. Это связано с тем, что проверяется только домен сайта. Если он является вредоносным или фишинговым, Веб-Защита блокирует угрозу. Если домен не был классифицирован как вредоносный или фишинговый, конкретный веб-адрес не блокируется.

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

На корпоративных устройствах, если приложение Kaspersky Endpoint Security для Android не включено в качестве службы Специальных возможностей, Веб-Контроль поддерживается только в Google Chrome и проверяет только домен сайта. Чтобы Веб-Контроль поддерживался другими браузерами (Samsung Internet, Яндекс Браузер и HUAWEI Browser), приложение Kaspersky Endpoint Security должно быть включено в качестве службы Специальных возможностей. Это также позволит использовать функцию Custom Tabs.

Если приложение Kaspersky Endpoint Security для Android не включено в качестве службы Специальных возможностей, и параметры прокси включены в карточке **Параметры Google Chrome**, Веб-Контроль не будет работать.

*Чтобы настроить доступ пользователя устройства к сайтам:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Контроль безопасности**.
4. На карточке **Веб-Контроль** нажмите **Параметры**.

   Откроется окно **Веб-Контроль**.
5. Выберите один из следующих вариантов:

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

     a. В раскрывающемся списке **Режим работы** выберите **Запретить сайты выбранных категорий**.

     b. В разделе **Категории** сформируйте список запрещенных категорий, установив флажки для категорий сайтов, доступ к которым приложение будет блокировать.

- Если вы хотите, чтобы приложение разрешало или блокировало доступ пользователя только к указанным сайтам, выполните следующие действия:

  a. В раскрывающемся списке **Режим работы** выберите **Разрешить только указанные сайты** или **Разрешить любые сайты, кроме указанных**.

  b. Нажмите **Добавить**.

  c. В открывшемся окне сформируйте список сайтов, доступ к которым приложение будет разрешать или блокировать в зависимости от значения, выбранного в раскрывающемся списке. Вы можете добавить сайты, используя ссылку (полный URL, включая протокол, например, `https://example.com`).

  Чтобы гарантировать, что приложение разрешает или ограничивает доступ к сайту во всех поддерживаемых версиях Google Chrome, HUAWEI Browser, Samsung Internet и Яндекс Браузер, 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 сайта разрешена или заблокирована. Этот URL доступен только при использовании протокола HTTP.
  - `http://example.com` — главная страница 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 сайта.

  Приложение также поддерживает регулярные выражения. При вводе адреса разрешенного или запрещенного 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 сайта, доступные при использовании протоколов HTTP и HTTPS.
  - `https?://.*\.example\.com` — этот шаблон блокирует или разрешает страницы всех субдоменов сайта (например, `https://pictures.example.com`).
  - `https?://example\.com/[abc]/.*` — этот шаблон блокирует или разрешает все дочерние страницы 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 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.

d. Нажмите **Добавить**.

- Если вы хотите, чтобы приложение ограничивало доступ пользователя к любым сайтам, в разделе **Режим работы** в раскрывающемся списке выберите **Запретить все сайты**.

6. 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 страницы, не покидая приложение и не переходя в полную версию браузера. Этот параметр обеспечивает лучшее распознавание URL-адресов и проверяет URL-адреса на соответствие настроенным правилам Веб-Контроля. 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.

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

7. Если вы хотите снять ограничения на доступ пользователей к сайтам на основе контента, выключите параметры с помощью переключателя **Веб-Контроль** и нажмите **Выключить**.

8. Нажмите **ОК**.

9. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

## Управление списком сайтов

Для управления списком сайтов используются следующие кнопки:

- **Добавить** – добавляет в список сайт, заданный по URL-адресу или с помощью регулярного выражения.
- **Загрузить** – добавляет в список несколько сайтов из файла в формате 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.
- **Изменить** – позволяет изменить адрес сайта.
- **Удалить** – удаляет один или несколько сайтов из списка.

## Настройка доступа к сайтам на iOS MDM-устройствах

Эти параметры применяются к устройствам в режиме "Расширенный контроль".

Настройка параметров Веб-Контроля позволяет контролировать доступ пользователей iOS MDM-устройств к сайтам. Веб-Контроль управляет доступом пользователей к сайтам на основе списков разрешенных и запрещенных сайтов. Также Веб-Контроль позволяет добавлять закладки сайтов на панель закладок Safari.

По умолчанию доступ к сайтам не ограничен.

Если веб-адрес переадресовывается на другую страницу, Веб-Контроль проверяет только конечную страницу.

*Чтобы настроить доступ пользователя устройства к сайтам:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Контроль безопасности**.
4. На карточке **Веб-Контроль** нажмите **Параметры**.

   Откроется окно **Веб-Контроль**.
5. Включите параметры с помощью переключателя **Веб-Контроль**.
6. В раскрывающемся списке **Режим работы** выполните одно из следующих действий:
   - Если вы хотите создать список разрешенных сайтов, выберите **Разрешить только указанные сайты**.
   - Если вы хотите создать список запрещенных сайтов, выберите **Разрешить любые сайты, кроме указанных**.
7. Выполните одно из следующих действий:
   - Если вы хотите добавить сайты вручную:
     a. Нажмите **Добавить**.
     b. Добавьте адреса сайтов, к которым приложение будет разрешать или ограничивать доступ (в зависимости от значения, выбранного в раскрывающемся списке).

        Адрес сайта должен начинаться с `http://` или `https://`. Kaspersky Mobile Devices Protection and Management разрешает или блокирует доступ ко всем сайтам домена. Например, если добавить в список разрешенных сайтов `http://www.example.com`, доступ к `http://pictures.example.com` и `http://example.com/movies` будет разрешен.

        Если вы хотите добавить разрешенный сайт в закладки Safari на мобильных устройствах, установите флажок **Добавить в закладки на устройстве** под адресом сайта.
     c. Нажмите **Добавить**.
   - Если вы хотите загрузить файл TXT со списком сайтов, нажмите **Загрузить**.

     Файл TXT должен быть сохранен с кодировкой UTF-8 и разрывами строк LF или CR+RF.

8. Нажмите **OK**.

9. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

В результате после применения политики на мобильных устройствах будет настроен Веб-Контроль.

# Контроль соответствия

В этом разделе приведены инструкции по контролю соблюдения корпоративных требований на устройствах и настройке правил контроля соответствия.

## Контроль соответствия Android-устройств

Вы можете проверять 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);
- реакции, которые будут применены на устройстве, если пользователь не устранит несоответствие в течение указанного времени (например, блокирование устройства).

> Если устройство находится в режиме экономии заряда батареи, Kaspersky Endpoint Security для Android может выполнить эту задачу позже, чем указано.

*Чтобы добавить правило проверки устройств на соответствие политике:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Контроль безопасности**.

4. На карточке **Контроль соответствия** нажмите **Параметры**.

   Откроется окно **Контроль соответствия**.

5. Включите параметры с помощью переключателя **Контроль соответствия**.

6. В разделе **При обнаружении несоответствия**:

   - Установите флажок **Уведомить пользователя**, чтобы сообщить пользователю, что устройство не соответствует политике.

     Если флажок не установлен, пользователь не будет уведомлен о случае несоответствия, и по истечении времени, отведенного на устранение несоответствия, на устройстве будет применена соответствующая реакция.

   - Установите флажок **Уведомить администратора в разделе "Выборки событий"**, чтобы сообщить администратору, что устройство не соответствует политике.

7. Нажмите **Добавить**.

   Запустится Мастер добавления правила. С помощью мастера можно создать набор правил для проверки соответствия устройства политике. Следуйте шагам мастера, используя кнопки **Далее** и **Назад**.

## Шаг 1. Критерий несоответствия

Нажмите **Добавить критерий**, чтобы указать критерий несоответствия для срабатывания правила.

Доступны следующие критерии:

- **Постоянная защита выключена**

  Kaspersky Endpoint Security для Android не установлен или не запущен на устройстве.

- **Базы вредоносного ПО на устройстве устарели**

  Базы вредоносного ПО последний раз обновлялись 3 или более дней назад.

- **Установлены запрещенные приложения**

  Список приложений на устройстве содержит приложения, запрещенные в параметрах политики **Контроль приложений**.

- **Установлены приложения из запрещенных категорий**

  Список приложений на устройстве содержит приложения из категорий, запрещенных в параметрах политики **Контроль приложений**.

- **Не установлены все обязательные приложения**

  Список приложений на устройстве не содержит приложение, установленное в качестве обязательного в параметрах политики **Контроль приложений**.

- **Версия операционной системы устарела**

  Версия Android на устройстве не соответствует заданному диапазону разрешенных версий.

  Для этого критерия укажите минимальную и максимальную разрешенные версии Android в полях **Минимальная версия** и **Максимальная версия**. Если в качестве максимальной разрешенной версии выбрано значение **Любая**, то будущие версии Android, поддерживаемые Kaspersky Endpoint Security для Android, будут также разрешены.

- **Устройство давно не синхронизировалось**

  Проверяется последняя синхронизация устройства с Сервером администрирования.

  Для этого критерия укажите максимальный период с момента последней синхронизации в поле **Период без синхронизации**.

- **На устройстве получены root-права**

  Устройство взломано (на устройстве получены права суперпользователя).

- **Пароль разблокировки экрана не соответствует параметрам безопасности, указанным в политике**

  Пароль разблокировки устройства не соответствует параметрам, заданным в карточке **Параметры разблокировки экрана**.

- **Установлена неактуальная версия Kaspersky Endpoint Security для Android**

  Установленная на устройстве версия Kaspersky Endpoint Security для Android устарела.

  Критерий применяется, только если приложение установлено с помощью инсталляционного пакета Kaspersky Endpoint Security для Android и если в параметрах политики **Обновление приложения** указана минимальная разрешенная версия приложения.

- **Использование SIM-карты не соответствует требованиям безопасности**

  SIM-карта устройства была заменена или извлечена относительно предыдущего состояния проверки, или была установлена дополнительная SIM-карта.

  Для этого критерия выберите условие, которое необходимо проверять:

  - **SIM-карта не должна быть заменена или удалена**
  - **SIM-карта не должна быть заменена или удалена; не должны быть установлены дополнительные SIM-карты**

- **Местоположение устройства**

  Устройство находится за пределами установленных геозон.

  > Указание геозоны приведет к увеличению энергопотребления устройства.

  Для этого критерия выберите условие, которое необходимо проверять:

  - **Устройство находится в пределах указанной геозоны** (геозоны объединяются с помощью логического оператора "ИЛИ").
  - **Устройство находится за пределами указанных геозон** (геозоны объединяются с помощью логического оператора "И").

  *Чтобы добавить геозону:*

  1. Нажмите **Добавить геозоны**.

     Откроется окно **Добавить геозоны**.

  2. Укажите **Название геозоны**.

  3. Обозначьте периметр геозоны, указав широту и долготу для каждой точки геозоны.

     > 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.

При необходимости вы можете указать более 3 точек, нажав **Добавить точку**.

Чтобы удалить точку, нажмите кнопку **X**.

Вы можете просмотреть указанную геозону в программе "Яндекс Карты", нажав **Посмотреть на карте**.

4. Нажмите **OK**, чтобы добавить указанные геозоны.

- **У Kaspersky Endpoint Security для Android нет доступа к точному или фоновому местоположению**

  У Kaspersky Endpoint Security для Android нет разрешения на определение точного местоположения устройства или использование данных о местоположении в фоновом режиме.

## Шаг 2. Реакции при несоответствии требованиям безопасности

Добавьте действия, которые будут выполняться на устройстве при обнаружении указанного критерия несоответствия.

Выберите один из следующих вариантов:

- **Добавить реакцию**. Реакция применяется немедленно после обнаружения критерия несоответствия.
- **Добавить отложенную реакцию**. Реакция применяется спустя период времени, указанный в поле **Время на устранение**.

  Доступны следующие реакции:

  - **Блокировка всех приложений, кроме системных**

    На устройстве заблокирован запуск всех приложений, кроме системных.

    Как только критерий несоответствия правилу перестанет обнаруживаться на устройстве, приложения автоматически разблокируются.

  - **Блокировка устройства**

    Мобильное устройство заблокировано. Чтобы получить доступ к данным, необходимо разблокировать устройство с помощью ввода одноразового кода или выполнив команду "**Разблокировать устройство**".

  - **Удаление корпоративных данных**

    Корпоративные данные удалены с устройства. Перечень удаленных данных зависит от режима работы устройства.

    - С личного устройства удалены профиль Knox и почтовый сертификат.
    - С корпоративного устройства удалены профиль Knox и сертификаты, установленные приложением Kaspersky Endpoint Security для Android (почтовые и VPN-сертификаты, а также сертификаты, полученные через профили SCEP, кроме мобильных сертификатов).
    - Дополнительно на устройстве с корпоративным контейнером удалены корпоративный контейнер (его содержимое, настройки и ограничения) и установленные в нем сертификаты (почтовые и VPN-сертификаты, а также сертификаты, полученные через профили SCEP, кроме мобильных сертификатов).

  - **Сброс настроек до заводских**

    Удалены все данные с устройства; настройки устройства сброшены до заводских. После применения этой реакции 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 корпоративного устройства.

- **Блокировка корпоративного контейнера**

  Корпоративный контейнер на устройстве заблокирован. Для получения доступа к корпоративному контейнеру необходимо его разблокировать.

  > Реакция применяется только на устройствах под управлением Android 6 или выше.

  > После блокировки корпоративного контейнера история паролей корпоративного контейнера очищается. Это означает, что пользователь может повторно использовать один из недавних паролей, независимо от параметров пароля для корпоративного контейнера.

- **Удалить данные всех приложений**

  На корпоративном устройстве удалены данные всех приложений.

  На устройстве с корпоративным контейнером удалены данные всех приложений в контейнере.

  В результате настройки приложений сброшены до установленных по умолчанию.

  > Реакция применяется только на корпоративных устройствах или устройствах с корпоративным контейнером под управлением Android 9 или выше.

- **Удаление данных указанного приложения**

  Для этой реакции необходимо указать имя 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 главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Приложения и файлы**.
  2. Выберите **Android** → **Приложения**.

     В открывшемся списке приложений отображаются идентификаторы приложений в столбце **Имя пакета**.

  В результате настройки приложения сброшены до установленных по умолчанию.

Реакция применяется только на корпоративных устройствах или устройствах с корпоративным контейнером под управлением Android 9 или выше.

- **Запрет на запуск устройства в безопасном режиме**

  Пользователю запрещено запускать устройство в безопасном режиме.

  Реакция применяется только на корпоративных устройствах под управлением Android 6 или выше.

- **Запрет на использование камеры**

  Пользователю запрещено использовать все имеющиеся на устройстве камеры.

- **Запрет на использование Bluetooth**

  Пользователю устройства запрещено включать Bluetooth и изменять его параметры.

  Реакция применяется только на личных устройствах под управлением Android 12 или ниже, корпоративных устройствах или устройствах с корпоративным контейнером.

- **Запрет на использование Wi-Fi**

  Пользователю устройства запрещено включать Wi-Fi и изменять его параметры.

  Реакция применяется только на личных устройствах под управлением Android 9 или ниже или на корпоративных устройствах.

- **Запрет на использование функций отладки по USB**

  Пользователю запрещено использовать функции отладки по USB и режим разработчика на устройстве.

  Реакция применяется только на корпоративных устройствах или устройствах с корпоративным контейнером.

- **Запрет режима полета**

  Пользователю запрещено включать режим полета на устройстве.

  Это действие применяется только на устройствах под управлением Android 9 или выше.

Нажмите **Добавить правило**, чтобы завершить Мастер добавления правила. Новое правило и краткая информация о нем отобразятся в списке правил Контроля соответствия. Чтобы временно выключить правило, используйте переключатель рядом с выбранным правилом.

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 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 корпоративного устройства.

Для этих настроек необходима интеграция с Microsoft Active Directory.

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. В результате профиль политики больше не будет распространяться на учетную запись этого пользователя, поэтому данные не будут удалены с устройства.

Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

## Контроль соответствия iOS MDM-устройств

Контроль соответствия позволяет проверять 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);
- реакции, которые будут применены на устройстве, если пользователь не устранит несоответствие в течение указанного времени (например, удаление корпоративных данных или отправка сообщения пользователю).

*Чтобы добавить правило проверки устройств на соответствие политике:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Контроль безопасности**.
4. На карточке **Контроль соответствия** нажмите **Параметры**.

   Откроется окно **Контроль соответствия**.
5. Включите параметры с помощью переключателя **Контроль соответствия**.

6. Нажмите **Добавить**.

   Запустится Мастер добавления правила. С помощью мастера можно создать набор правил для проверки соответствия устройства политике. Следуйте шагам мастера, используя кнопки **Далее** и **Назад**.

## Шаг 1. Критерий несоответствия

Нажмите **Добавить критерий**, чтобы указать критерий несоответствия для срабатывания правила.

Доступны следующие критерии:

- **Список установленных приложений**

  В списке приложений на устройстве есть запрещенные приложения или отсутствуют обязательные.

  Для этого критерия выберите условие (**Содержит** или **Не содержит**) и укажите **Идентификатор пакета (Bundle ID)**. **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 главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Приложения и файлы**.
  2. Нажмите **iOS**.

     В открывшемся списке приложений идентификаторы приложений отображаются в столбце **Идентификатор пакета**.

- **Версия операционной системы**

  Версия операционной системы на устройстве не соответствует заданному диапазону разрешенных версий.

Для этого критерия выберите условие (**Равна**, **Не равна**, **Ниже**, **Ниже или равна**, **Выше** или **Выше или равна**) и укажите версию iOS.

Операторы **Равна** и **Не равна** проверяют полное соответствие версии операционной системы указанному значению. Например, если в правиле указать версию 15, а устройство работает на iOS 15.2, то условие **Равна** не будет выполнено. Если необходимо указать диапазон версий, вы можете создать два критерия, использовав операторы **Ниже** и **Выше**.

- **Статус управления**

  Статус управления устройством не соответствует требуемому.

  Для этого критерия выберите режим работы устройства (**Расширенный контроль** или **Базовый контроль**).

- **Тип устройства**

  Тип устройства не соответствует требуемому.

  Для этого критерия выберите тип устройства (**iPhone** или **iPad**).

- **Модель устройства**

  Модель устройства не соответствует требуемой.

  Для этого критерия выберите условие (**Равна** или **Не равна**) и укажите модели, которые будут проверены или исключены из проверки.

  Чтобы указать модель, в поле **Идентификатор модели** выберите требуемую модель из списка или введите значение вручную. 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 **Добавить: "<значение>"** и добавить введенное значение к критерию.

  > Если указаны противоречащие друг другу критерии (например, в поле **Тип устройства** указано значение **iPhone**, а списке значений **Модель устройства** с выбранным оператором **Равна** - модель iPad), отобразится сообщение об ошибке. Вы не можете сохранить правило с такими критериями.

- **Нахождение в роуминге**

  Статус роуминга устройства не соответствует требуемому.

  Для этого критерия выберите условие (**Устройство в роуминге** или **Устройство не в роуминге**).

- **Пароль на устройстве**

  Пароль не установлен или не соответствует параметрам, указанным в разделе политики **Параметры разблокировки экрана**.

  Для этого критерия выберите условие (**Не установлен**, **Установлен, но не соответствует требованиям** или **Установлен и соответствует требованиям**).

- **Свободное место на устройстве**

Объем свободного места на устройстве меньше указанного порогового значения.

Для этого критерия укажите пороговое значение свободного места (**Меньше**) и выберите единицу измерения (**МБ** или **ГБ**).

- **Устройство не зашифровано**

  Устройство не зашифровано.

  На iOS-устройствах шифрование данных включено по умолчанию, если установлен пароль для разблокировки устройства (**Настройки** > **Touch ID / 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: перейдите в **Управление активами** → **Мобильные** → **Устройства** и выберите необходимое устройство).

- **Действия с SIM-картой**

  SIM-карта устройства была заменена или извлечена относительно предыдущего состояния проверки, или была установлена дополнительная SIM-карта.

  Для этого критерия выберите условие (**SIM-карта не должна быть заменена или удалена** или **SIM-карта не должна быть заменена или удалена; не должны быть установлены дополнительные SIM-карты**).

  > На устройствах, совместимых с eSIM, обнаруженное несоответствие невозможно устранить, 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.

- **Устройство давно не синхронизировалось**

  Проверяется последняя синхронизация устройства с Сервером iOS MDM.

  Для этого критерия укажите максимальный период с момента последней синхронизации в поле **Период без синхронизации** и выберите единицы измерения (**Часы** или **Дни**).

  > Не рекомендуется выбирать значение меньше значения параметра **Период синхронизации (мин)**, указанного в параметрах Сервера iOS MDM.

## Шаг 2. Реакции при несоответствии требованиям безопасности

Добавьте действия, которые будут выполняться на устройстве при обнаружении указанного критерия несоответствия.

Выберите один из следующих вариантов:

- **Добавить реакцию**. Реакция применяется немедленно после обнаружения критерия несоответствия.
- **Добавить отложенную реакцию**. Реакция применяется спустя период времени, указанный в поле **Время на устранение**.

  > Реакции применяются во время проверки соблюдения правил соответствия (1 раз в 40 минут) до следующей синхронизации с Сервером iOS MDM. Чтобы предотвратить повторные реакции по одному и тому же случаю несоответствия, в поле **Период синхронизации (мин)** в параметрах Сервера iOS MDM укажите значение 30 минут.

Если вы укажете реакции, которые противоречат друг другу, отобразится сообщение об ошибке. Такое правило нельзя сохранить.

Когда критерии несоответствия правилу перестанут обнаруживаться на устройстве, можно отменить реакцию, отправив устройству соответствующую команду.

Доступны следующие реакции:

- **Отправить пользователю сообщение**

  Пользователь будет уведомлен о случае несоответствия по электронной почте.

  Для этой реакции укажите адрес электронной почты пользователя в полях **Адрес электронной почты** и **Дополнительный адрес электронной почты**. При необходимости вы также можете изменить тему письма и текст по умолчанию.

  Убедитесь, что в свойствах Сервера администрирования в разделе **Электронная почта** настроены уведомления. Дополнительная информация о настройке уведомлений приведена в справке Kaspersky Security Center.

- **Удалить корпоративные данные**

  С устройства удалены все установленные конфигурационные профили, provisioning-профили, управляющий профиль и приложения, для которых был установлен флажок **Удалять при удалении управляющего профиля**. Реакция применяется через отправку команды **Удалить корпоративные данные**.

- **Изменить профиль**

  Для этой реакции укажите одно из действий:

  - **Установить профиль**. Конфигурационный профиль установлен на устройстве. Действие выполняется через отправку команды **Установить конфигурационный профиль**. Для этого действия необходимо указать идентификатор устанавливаемого профиля.

    Перед установкой профиля убедитесь, что профиль добавлен в список конфигурационных профилей в разделе параметров Сервера iOS MDM **Конфигурационные профили**.

  - **Удалить указанный профиль**. Конфигурационный профиль удален с устройства. Действие выполняется через отправку команды **Удалить конфигурационный профиль**. Для этого действия необходимо указать идентификатор удаляемого профиля.

  - **Удалить все профили**. Все ранее установленные конфигурационные профили удалены с устройства.

    Когда критерии несоответствия правилу перестанут обнаруживаться на устройстве, можно установить удаленные конфигурационные профили один за другим, отправив устройству соответствующую команду.

- **Обновить операционную систему**

Для этой реакции укажите **Версия ОС** и одно из действий:

- **Загрузить и установить**. Операционная система устройства загружена и установлена.

  Если в критерии **Версия операционной системы** указана несуществующая версия, устройство обновится до последней загруженной версии.

- **Только загрузить**. Операционная система устройства загружена.

- **Только установить**. Ранее загруженная операционная система установлена.

Это реакция применима только к устройствам с режимом работы "Расширенный контроль".

- **Изменить параметры Bluetooth**

  Для этой реакции укажите, требуется ли включить или отключить Bluetooth на устройстве.

  Это реакция применима только к устройствам с режимом работы "Расширенный контроль".

- **Сбросить настройки до заводских**

  Удалены все данные с устройства; настройки устройства сброшены до установленных по умолчанию. После применения этой реакции устройство перестает быть управляемым. Для подключения устройства к Kaspersky Security Center необходимо переустановить на устройстве управляющий профиль.

- **Изменить приложения**

  Для этой реакции укажите одно из действий:

  - **Удалить указанное приложение**. Указанное приложение удалено с устройства.

    Вы можете удалить только управляемое приложение. Приложение считается управляемым, если оно установлено с помощью Kaspersky Security Center через команду **Установить приложение**.

    Когда критерии несоответствия правилу перестанут обнаруживаться на устройстве, можно отменить действие, отправив устройству соответствующую команду.

    Для этого действия необходимо указать **Идентификатор пакета (Bundle ID)** удаляемого 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 главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Приложения и файлы**.
2. Нажмите **iOS**.

   В открывшемся списке приложений идентификаторы приложений отображаются в столбце **Идентификатор пакета**.

- **Удалить все приложения**. Все управляемые приложения удалены с устройства.

Вы можете удалить только управляемые приложения. Приложение считается управляемым, если оно установлено с помощью Kaspersky Security Center через команду **Установить приложение**.

Когда критерии несоответствия правилу перестанут обнаруживаться на устройстве, можно установить удаленные приложения одно за другим, отправив устройству соответствующую команду.

Для этого действия необходимо указать **Идентификатор пакета (Bundle ID)** удаляемых приложений.
**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 главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Приложения и файлы**.
2. Нажмите **iOS**.

   В открывшемся списке приложений идентификаторы приложений отображаются в столбце **Идентификатор пакета**.

- **Удалить профиль указанного типа**

  Для этого действия необходимо указать **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 этой реакции необходимо указать, требуется ли включить или отключить роуминг данных на устройстве.

Нажмите **Добавить правило**, чтобы завершить Мастер добавления правила. Новое правило и краткие сведения о нем появятся в списке правил Контроля соответствия. Чтобы временно выключить правило, используйте переключатель рядом с выбранным правилом.

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 действий:

- **Удалить корпоративные данные**
- **Сбросить настройки до заводских**

Для этих настроек необходима интеграция с Microsoft Active Directory.

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. В результате профиль политики больше не будет распространяться на учетную запись этого пользователя, поэтому данные не будут удалены с устройства.

Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

# 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 и настраивать их использование на Android-устройствах, чтобы обеспечивать безопасность этих устройств.

Вы можете ограничить работу 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 нужно выбрать критерий **Установлены запрещенные приложения**, **Установлены приложения из 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. Если пользователь сделает это, Контроль приложений не запустится.

На корпоративных устройствах 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 нужно указать ссылку на APK-файл обязательного приложения в параметрах политики.
- Запрещенные приложения можно удалять с устройства автоматически. Для тихого удаления приложений нужно установить флажок **Удалять запрещенные приложения автоматически** в параметрах политики.

*Чтобы настроить параметры запуска приложений на мобильном устройстве:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Контроль безопасности**.
4. На карточке **Контроль приложений** нажмите **Параметры**.

   Откроется окно **Контроль приложений**.

5. Включите параметры с помощью переключателя **Контроль приложений**.

6. Настройте параметры на следующих вкладках:

- Если вы хотите настроить общие правила управления приложениями, **перейдите на вкладку Использование приложений**.

  1. В раскрывающемся списке **Режим работы** выберите режим Контроля приложений:

     - Чтобы разрешить пользователю запускать все приложения, кроме указанных в списке как запрещенные, выберите режим **Использовать любые приложения, кроме запрещенных**. Kaspersky Endpoint Security для Android скроет значки запрещенных приложений. Этот параметр выбран по умолчанию.

     - Чтобы разрешить пользователю запускать только приложения, указанные в списке как разрешенные, рекомендованные или обязательные, выберите режим **Использовать только разрешенные приложения**. Kaspersky Endpoint Security для Android скроет значки всех приложений, кроме тех, которые указаны в списке разрешенных, рекомендованных или обязательных приложений и системных приложений.

  2. Чтобы приложение Kaspersky Endpoint Security для Android отправляло данные о запрещенных приложениях в журнал событий, не блокируя их, установите флажок **Не блокировать запрещенные приложения, только записывать в журнал событий**.

  3. Если вы хотите, чтобы приложение Kaspersky Endpoint Security для Android блокировало запуск системных приложений (например, Календарь, Камера, Настройки) на мобильном устройстве пользователя, установите флажок **Блокировать системные приложения**. Этот флажок отображается в режиме **Использовать только разрешенные приложения**.

     Мы рекомендуем не блокировать системные приложения, поскольку это может привести к сбою в работе устройства.

     В числе системных приложений может быть заблокирован системный механизм запроса разрешений для приложений. Чтобы снять блокировку с этого механизма, найдите его имя (например, `com.google.android.permissioncontroller`) в журнале событий и добавьте его в исключения.

     Перед удалением Kaspersky Endpoint Security для Android с устройства снимите этот флажок или выключите Контроль приложений.

  4. Если вы хотите, чтобы приложение Kaspersky Endpoint Security для Android удаляло запрещенные приложения с устройства в фоновом режиме без уведомления пользователя, установите флажок **Удалять запрещенные приложения автоматически**. Этот флажок отображается в политиках управления корпоративными устройствами.

  5. Нажмите **Добавить**, чтобы добавить приложения и категории, для которых вы хотите установить правила.

     Откроется окно **Добавить приложение или категорию**.

6. В поле **Объект** выберите **Приложение** или **Категория приложений** и выполните следующие действия:

   - Если выбран вариант **Приложение**, выберите инсталляционный пакет или укажите имя пакета и название приложения в соответствующих полях.
   - Если выбран вариант **Категория приложений**, выберите категорию и введите описание в соответствующих полях.
   - Нажмите **Добавить**.

   Приложение или категория будут добавлены в список.

7. Если вы хотите настроить исключения для перечисленных запрещенных или разрешенных приложений, нажмите **Исключения**, в открывшемся окне укажите имена пакетов и нажмите **ОК**.

8. Если вы хотите получать отчеты об установленных приложениях, в разделе **Отчет об установленных приложениях** установите флажок **Отправлять данные об установленных приложениях**. Затем вы можете установить следующие флажки:

   - **Отправлять данные о встроенных приложениях** – для отправки данных о системных приложениях.
   - **Отправлять данные о служебных приложениях** – для отправки данных о служебных приложениях, которые не имеют интерфейса и не могут быть запущены вручную.

   Если системное или служебное приложение настроено в параметрах Контроля приложений, данные о нем будут отправляться независимо от состояния этих флажков.

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

- Если вы хотите настроить действия для конкретных приложений, **перейдите на вкладку Управление приложениями**.

1. В таблице **Действия с приложениями** нажмите **Добавить**.

2. В открывшемся окне выполните следующие действия:

   a. В поле **Действие** выберите одно из следующих действий:

      - **Установить**. Пользователю будет предложено установить приложение.
      - **Удалить**. Приложение будет удалено с устройства пользователя.
      - **Рекомендовать к установке**. Пользователь получит рекомендацию установить приложение.

   b. Заполните следующие поля:

Используйте только легитимные и доверенные источники. Настраивая параметры в этом разделе, вы несете полную ответственность за потенциальные риски и последствия, связанные с использованием ненадежных источников.

- **Имя пакета**
- **Название приложения**
- **Ссылка**

  Ссылки на пакеты приложений должны начинаться с http:// или https://.

  Для тихой установки укажите прямую ссылку на скачивание APK-файла, которая запустит загрузку без взаимодействия с пользователем. Ссылки на страницы магазинов приложений не поддерживаются для тихой установки. Вы можете разместить APK-файлы на Веб-сервере или другом источнике.

- **Версия**

  Это поле – строка в формате регулярных выражений Oracle. Подробнее о регулярных выражениях см. на сайте Службы технической поддержки Oracle.

  Поля **Ссылка** и **Версия** не отображаются, если вы выбрали **Удалить** в поле **Действие**.

c. Нажмите **Добавить**.

Настроенное действие будет добавлено в список.

7. Нажмите **ОК.**
8. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

## Контроль приложений на iOS MDM-устройствах

Эти параметры применяются к устройствам в режиме "Расширенный контроль".

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.

*Чтобы настроить список приложений, которые разрешено или запрещено устанавливать на устройствах:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **iOS** и перейдите в раздел **Контроль безопасности**.

4. На карточке **Контроль приложений** нажмите **Параметры**.

   Откроется окно **Контроль приложений**.

5. Включите параметры с помощью переключателя **Контроль приложений**.

6. В поле **Режим работы** выберите один из следующих вариантов:

   - **Использовать любые приложения, кроме запрещенных**

     На устройстве будут отображаться и будут доступны для запуска все приложения, кроме указанных в списке.

     > Не добавляйте приложения "Настройки" и "Телефон" в список запрещенных, иначе управляющий профиль не будет обновлен на устройстве.

   - **Использовать только разрешенные приложения**

     Этот параметр выбран по умолчанию. Если вы выберете этот вариант, пользователь сможет открывать на устройстве только следующие приложения:

     - Приложения из списка разрешенных приложений
     - Системные приложения: "Настройки" (для iOS и iPadOS) и "Телефон" (для iOS)

     Все остальные приложения будут скрыты.

7. Нажмите **Добавить**, чтобы добавить приложения в список.

8. В открывшемся окне укажите идентификатор пакета приложения в соответствующем поле. Укажите значение `com.apple.webapp`, чтобы разрешить или 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 главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Приложения и файлы**.
2. Нажмите **iOS**.

   В открывшемся списке приложений идентификаторы приложений отображаются в столбце **Идентификатор пакета**.

При необходимости можно указать несколько идентификаторов пакетов, нажав кнопку **Добавить идентификатор пакета**.

9. Нажмите **Сохранить**.
10. Нажмите **ОК**.
11. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

В результате после применения политики на устройствах будут настроены указанные параметры для приложений.

# Уровни защиты мобильных устройств

## Уровни защиты мобильных устройств, определяемые Kaspersky Security Center

Web Console позволяет быстро оценить текущий уровень защиты управляемых мобильных устройств в разделе **Управление активами** → **Мобильные** → **Устройства**.

Устройство может иметь один из следующих уровней защиты: **ОК**, **Предупреждение**, **Критический**.

Уровни защиты присваиваются и отправляются в Kaspersky Security Center в соответствии со следующими требованиями:

- На устройстве обнаружена одна причина для присвоения уровня защиты — устройству присваивается статус, отображающийся в списке управляемых устройств.
- На устройстве обнаружено несколько причин для присвоения уровня защиты — Kaspersky Mobile Devices Protection and Management присваивает статус наиболее критического.

- Причины для присвоения уровня защиты на устройстве не обнаружены — Kaspersky Mobile Devices Protection and Management не отправляет статус в Kaspersky Security Center и присваивает статус *OK*.

Уровни защиты и их значение

| Уровень защиты | Значение |
|---|---|
| **OK** | Вмешательство администратора не требуется. |
| **Предупреждение** | Зарегистрированы события, связанные с угрозами для безопасности управляемых устройств. |
| **Критический** | Имеются серьезные проблемы. Требуется вмешательство администратора для их решения. |

Цель администратора – убедиться, что всем устройствам присвоен уровень защиты *OK*.

## Уровни защиты мобильных устройств, определяемые Kaspersky Mobile Devices Protection and Management

Kaspersky Mobile Devices Protection and Management определяет уровень защиты мобильных устройств на основе параметров политики и отправляет уровни защиты в Kaspersky Security Center во время синхронизации. Администратор может изменить уровень защиты в политике, в зависимости от критичности условия (см. таблицу *Значения по умолчанию, причины и условия присвоения уровней защиты на Android-устройствах*). В этом случае заданное администратором значение имеет приоритет над значением по умолчанию, заданным Kaspersky Mobile Devices Protection and Management.

Значения по умолчанию, причины и условия присвоения уровней защиты на Android-устройствах

| Условие | Причина присвоения уровня защиты | Значение по умолчанию |
|---|---|---|
| Постоянная защита не работает | Одна из следующих причин:<br>• Доступ для управления всеми файлами не предоставлен.<br>• Kaspersky Security Network выключен. | *Критический* |
| Веб-Защита и Веб-Контроль не работают | Одна из следующих причин:<br>• Разрешение Специальные возможности не предоставлено.<br>• Веб-Защита выключена пользователем в параметрах Kaspersky Endpoint Security.<br>• Разрешение Игнорировать оптимизацию батареи не предоставлено.<br>• Положение о Веб-Фильтре не принято. | *Предупреждение* |
| Контроль приложений не работает | Разрешение Специальные возможности не предоставлено. | *Предупреждение* |
| Блокирование устройства недоступно | Одна из следующих причин:<br>• Разрешение Администратор устройства не предоставлено.<br>• Разрешение Специальные возможности не предоставлено.<br>• Приложению запрещено наложение поверх других окон. | *Предупреждение* |
| Определение геолокации на устройстве недоступно | Одна из следующих причин:<br>• Разрешение Местоположение не предоставлено.<br>• Местоположение устройства не может быть определено (при наличии разрешения). | *Предупреждение* |
| Версии Положения о Kaspersky Security Network 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 Положения о маркетинге 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. | *OK* |

# Инвентаризация программного обеспечения на Android-устройствах

Вы можете выполнять инвентаризацию приложений на Android-устройствах, подключенных к Серверу администрирования. 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**. В этом разделе можно просмотреть подробную информацию о каждом установленном приложении.

*Чтобы включить инвентаризацию программного обеспечения:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Контроль безопасности**.
4. На карточке **Контроль приложений** нажмите **Параметры**.

   Откроется окно **Контроль приложений**.
5. В разделе **Отчет об установленных приложениях** установите флажок **Отправлять данные об установленных приложениях**.
6. Если вы хотите получать данные о системных приложениях, установите флажок **Отправлять данные о встроенных приложениях**.
7. Если вы хотите получать данные о служебных приложениях, которые не имеют интерфейса и не могут быть открыты пользователем, установите флажок **Отправлять данные о служебных приложениях**.
8. Нажмите **ОК**.
9. Нажмите **Сохранить**, 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.

# Защита

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

## Настройка защиты от вредоносного ПО на Android-устройствах

Для своевременного обнаружения угроз, поиска вирусов, а также других вредоносных программ можно 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;
- легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным пользователей.

Защита от вредоносного ПО имеет несколько ограничений:

- 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 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.

## Настройка постоянной защиты

*Чтобы настроить параметры постоянной защиты для мобильных устройств:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Защита**.
4. На карточке **Постоянная защита** нажмите **Параметры**.

   Откроется окно **Постоянная защита**.
5. Включите параметры с помощью переключателя **Постоянная защита**.

   Если этот переключатель включен, защита устройства включена, и пользователь не может отключить ее вручную.

   Если этот переключатель выключен, защита устройства включена, но пользователь может отключить ее вручную.
6. В раскрывающемся списке **Проверка приложений** выберите режим проверки приложений:
   - **Не проверять приложения**
   - **Проверять только новые приложения и файлы из папки Загрузки**
   - **Проверять все приложения и контролировать действия с файлами**
7. В выпадающем 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 удален или перемещен. Чтобы получить актуальный список угроз, запустите полную проверку устройства. Для надежной защиты ваших данных устраните все обнаруженные объекты.

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

8. Чтобы включить дополнительную проверку новых приложений до их первого запуска на устройстве пользователя с помощью облачной службы Kaspersky Security Network, установите флажок **Дополнительная защита с помощью Kaspersky Security Network**.

9. Чтобы заблокировать рекламные программы и приложения, которые могут быть использованы злоумышленниками для нанесения вреда устройству или данным пользователя, установите флажок **Обнаруживать рекламные приложения, средства автодозвона и легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройству и данным пользователя**.

10. Нажмите **ОК**.

11. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

## Настройка автоматического поиска вредоносного ПО

*Чтобы настроить автоматический запуск проверки на наличие вредоносного ПО на мобильном устройстве:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Защита**.

4. На карточке **Проверка** нажмите **Параметры**.

   Откроется окно **Проверка**.

5. Включите параметры с помощью переключателя **Проверка**.

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 удален или перемещен. Чтобы получить актуальный список угроз, запустите полную проверку устройства. Для надежной защиты ваших данных устраните все обнаруженные объекты.

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

- **Запросить действие**

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

  Для отображения уведомлений на мобильных устройствах под управлением операционной системы Android 10 или 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, 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**.

Вредоносные программы, установленные на корпоративные устройства и 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 отображение и запуск на устройствах пользователей запрещаются.

В корпоративном контейнере установленные вредоносные программы, обнаруженные Kaspersky Endpoint Security для Android, не удаляются, их отображение и запуск на устройствах пользователей запрещаются без уведомления пользователей.

Если выбран вариант **Запросить действие**, Kaspersky Endpoint Security для Android предлагает пользователям выбрать действие для каждого обнаруженного приложения как на корпоративных устройствах, так и на устройствах с корпоративным контейнером.

Установленные вредоносные программы нельзя переместить в карантин. Соответственно, если выбран вариант **Удалить и сохранить резервную копию файла в карантине**, обнаруженная вредоносная программа будет удалена.

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 разделе **Проверка по расписанию** можно настроить автоматический запуск полной проверки файловой системы устройства.

8. Если выбрана еженедельная или ежедневная проверка, укажите день недели (для еженедельных проверок) и время начала проверки в полях **День** и **Время**.

   Если устройство находится в режиме экономии заряда батареи, приложение может выполнить эту задачу позже, чем указано.

9. Нажмите **ОК**.

10. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

    Параметры на мобильном устройстве будут изменены 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 настройте параметры обновления баз вредоносного ПО.

По умолчанию обновление баз вредоносного ПО в зоне роуминга выключено. Обновление баз вредоносного ПО по расписанию не выполняется.

## Настройка обновления баз

*Чтобы настроить параметры обновления баз вредоносного ПО:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Защита**.

4. На карточке **Обновление баз** нажмите **Параметры**.

   Откроется окно **Обновление баз**.

5. Включите параметры с помощью переключателя **Обновление баз**.

6. В поле **Обновление баз по расписанию** можно настроить параметры автоматического запуска обновлений баз вредоносного ПО на устройстве пользователя.

7. Если выбрано еженедельное или ежедневное обновление баз, укажите день недели (для еженедельных обновлений баз) и время начала обновления в полях **День** и **Время**.

   Если устройство находится в режиме экономии заряда батареи, приложение может выполнить эту задачу позже, чем указано.

8. 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"**

     Использование сервера обновлений "Лаборатории Касперского" в качестве источника для загрузки обновлений баз Kaspersky Endpoint Security для Android на мобильные устройства пользователей. Для обновления баз с помощью 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 для загрузки обновлений баз приложения Kaspersky Endpoint Security для Android на мобильные устройства пользователей.

   - **Другой источник**

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

9. Чтобы приложение Kaspersky Endpoint Security для Android загружало обновления баз по расписанию, когда устройство находится в зоне роуминга, в блоке **Обновление баз в роуминге** установите флажок **Разрешить обновление баз в роуминге**.

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

10. Нажмите **ОК**.

11. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

## Защита Android-устройств в интернете

Вы можете использовать Веб-Защиту для защиты персональных данных пользователей мобильных устройств в интернете. Веб-Защита блокирует вредоносные сайты, цель которых – распространить вредоносный код, а также фишинговые сайты, цель которых – украсть ваши конфиденциальные данные и получить доступ к вашим финансовым счетам. Веб-Защита проверяет сайты до открытия, используя облачную службу Kaspersky Security Network. По умолчанию Веб-Защита включена.

В Яндекс Браузере и Samsung Internet вредоносные и фишинговые веб-адреса могут оставаться незаблокированными. Это связано с тем, что проверяется только домен сайта. Если он является вредоносным или фишинговым, Веб-Защита блокирует угрозу. Если домен не был классифицирован как вредоносный или фишинговый, конкретный веб-адрес не блокируется.

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

На корпоративных устройствах, если приложение Kaspersky Endpoint Security для Android не включено в качестве службы Специальных возможностей, Веб-Защита поддерживается только в Google Chrome и проверяет только домен сайта. Чтобы Веб-Защита поддерживалась другими браузерами (Samsung Internet, Яндекс Браузер и HUAWEI Browser), приложение Kaspersky Endpoint Security должно быть включено в качестве службы Специальных возможностей.

*Чтобы включить Веб-Защиту, выполните следующие действия:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Защита**.
4. На карточке **Веб-Защита** активируйте параметры с помощью переключателя **Веб-Защита**.
5. Нажмите **Включить**.

   Если вы выключите Веб-Защиту, Веб-Контроль также будет выключен.

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

## Проверка уведомлений от мессенджеров

Kaspersky Endpoint Security для Android может обнаруживать вредоносные и фишинговые веб-адреса в уведомлениях от Telegram, MAX, WhatsApp, приложения для SMS и других распространенных мессенджеров. Проверяются только веб-адреса, указанные в открытом виде. Гиперссылки внутри текста не проверяются.

Для включения проверки уведомлений должны быть выполнены следующие условия:

- Включена Веб-Защита.
- Для нужных мессенджеров разрешено отображение уведомлений. Kaspersky Endpoint Security для Android проверяет только уведомления, которые могут быть показаны на экране устройства.
- На устройствах Google Pixel и Vivo выдано разрешение "Разговоры" для Kaspersky Endpoint Security в настройках доступа к уведомлениям.

*Чтобы включить проверку уведомлений:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Защита**.

4. На карточке **Веб-Защита** установите флажок **Блокировать уведомления, содержащие вредоносные и фишинговые веб-адреса**.

5. Подробная информация о том, как разрешить доступ к уведомлениям на устройстве, приведена в разделе Веб-Защита.

Теперь приложение проверяет уведомления на наличие вредоносных и фишинговых веб-адресов. Если обнаружен опасный веб-адрес, уведомление блокируется и появляется блокирующий экран с информацией о заблокированном уведомлении.

Если Kaspersky Endpoint Security не включен в качестве службы Специальных возможностей, то вместо отображения блокирующего экрана приложение пришлет push-уведомление об обнаруженных опасных веб-адресах. При нажатии на это push-уведомление появится экран с информацией о заблокированных уведомлениях.

# 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 |
| --- | --- |
| **Заблокировать устройство** | Мобильное устройство заблокировано. Чтобы получить доступ к данным, необходимо разблокировать устройство с помощью команды **Разблокировать устройство** или одноразового кода. |
| **Разблокировать устройство** | Мобильное устройство разблокировано.<br>После разблокировки устройства под управлением Android 5–6 пароль разблокировки экрана будет заменен на "1234". На устройствах под управлением Android 7 или выше после разблокировки пароль разблокировки экрана останется прежним. |

| Команда | Результат |
| --- | --- |
| **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.<br><br>Эта команда недоступна для личных устройств и устройств с корпоративным контейнером под управлением Android 14 или выше. |
| **Удалить корпоративные данные** | Корпоративные данные удалены с устройства. Перечень удаляемых данных зависит от режима работы устройства:<br>• На личном устройстве удалены Knox-контейнер, корпоративные файлы, отправленные на устройство, и почтовый сертификат.<br>• С корпоративных устройств удалены Knox-контейнер, корпоративные файлы, отправленные на устройство, и сертификаты, установленные приложением Kaspersky Endpoint Security для Android (почтовые и VPN-сертификаты, сертификаты, полученные через профили SCEP, кроме мобильных сертификатов).<br>• Дополнительно, если создан корпоративный контейнер, удален корпоративный контейнер (его содержимое, корпоративные файлы, отправленные на устройство, настройки и ограничения) и сертификаты, установленные в корпоративном контейнере (почтовые и VPN-сертификаты, сертификаты, полученные через профили SCEP, кроме мобильных сертификатов). |
| **Определить местоположение** | Получены координаты местоположения мобильного устройства.<br><br>Чтобы посмотреть местоположение устройства в программе "Яндекс Карты", перейдите в раздел **Управление активами → Мобильные → Устройства**. Затем выберите устройство и нажмите **История команд → Определить местоположение → Координаты устройства → Посмотреть на карте**. После нажатия кнопки **Посмотреть на карте** координаты устройства передаются в Яндекс Карты, и устройство отображается на карте.<br><br>На устройствах с Android 12 или выше, если пользователем 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 не выполняется.<br><br>Если на Android-устройстве отключена служба Google "Точность местоположения", команда работать не будет. Обращаем внимание, что не на всех Android-устройствах есть эта служба. |
| **Сделать фотографии** | Мобильное устройство заблокировано. Фотографии сделаны фронтальной камерой устройства при попытке разблокировать устройство. На устройствах с выдвижной фронтальной камерой фотография будет черной, если камера закрыта.<br><br>При попытке разблокировки устройства пользователь автоматически соглашается на фотографирование с помощью устройства.<br><br>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 выше, уведомление не отображается, но сделанная фотография будет черной. |
| **Воспроизвести звуковой сигнал** | Мобильное устройство воспроизводит звуковой сигнал в течение 5 минут (в течение 1 минуты, если заряд батареи устройства низкий) или до тех пор, пока пользователь не разблокирует устройство. |
| **Удалить данные приложения** | Данные указанного приложения удалены с мобильного устройства.<br><br>Для этого действия необходимо указать имя пакета приложения, данные которого нужно удалить.<br><br>В результате приложение возвращается в состояние по умолчанию.<br><br>Данные системных приложений и приложений-администраторов не удаляются. |

| Команда | Результат |
| --- | --- |
| **Удалить данные всех приложений** | Данные всех приложений удалены с мобильного устройства.<br><br>На корпоративном устройстве удаляются данные всех приложений.<br><br>На устройстве с корпоративным контейнером удаляются данные всех приложений в корпоративном контейнере.<br><br>В результате приложения возвращаются в состояние по умолчанию.<br><br>Данные системных приложений и приложений-администраторов не удаляются. |
| **Получить историю местоположений** | Отображается история местоположений мобильного устройства за последние 14 дней.<br><br>Чтобы посмотреть местоположение устройства в программе "Яндекс Карты", перейдите в раздел **Управление активами** → **Мобильные** → **Устройства**. Затем выберите устройство и нажмите **История команд** → **Получить историю местоположений** → **Посмотреть на карте**. После нажатия кнопки **Посмотреть на карте** координаты устройства передаются в Яндекс Карты, и устройство отображается на карте.<br><br>Из-за технических ограничений Android-устройств фактическое определение местоположения устройства может происходить реже, чем указано в параметрах политики **Определение местоположения**. |

## Команды для iOS MDM-устройств

Команды для защиты данных при потере или краже iOS MDM-устройства

| Команда | Результат |
| --- | --- |
| **Заблокировать устройство** | Мобильное устройство заблокировано. Для получения доступа к данным необходимо разблокировать устройство. |
| **Сбросить пароль разблокировки** | 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** | С устройства удалены все установленные конфигурационные профили, provisioning-профили, управляющий профиль и приложения, для которых был установлен флажок **Удалять при удалении управляющего профиля**. |
| **Включить Режим пропажи (для режима "Расширенный контроль")** | На мобильном устройстве в режиме "Расширенный контроль" включен Режим пропажи, устройство заблокировано. На экране устройства появилось сообщение и номер телефона, которые вы можете редактировать.<br><br>Если вы отправите команду **Включить режим пропажи** на iOS MDM-устройство в режиме "Расширенный контроль" без SIM-карты, и это устройство будет перезапущено, оно не сможет подключиться к сети Wi-Fi и получить команду **Выключить 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 **Выключить режим пропажи** по мобильной сети. |
| **Определить местоположение (только в Режиме пропажи)** | Получены данные о местоположении устройства.<br><br>Чтобы посмотреть местоположение устройства в программе "Яндекс Карты", перейдите в раздел **Управление активами** → **Мобильные** → **Устройства**. Затем выберите устройство и нажмите **История команд** → **Определить местоположение** → **Координаты устройства** → **Посмотреть на карте**. После нажатия кнопки **Посмотреть на карте** координаты устройства передаются в Яндекс Карты, и устройство отображается на карте. |

| Команда | Результат |
| --- | --- |
| **Воспроизвести звуковой сигнал (только в Режиме пропажи)** | На потерянном мобильном устройстве воспроизводится звуковой сигнал. |
| **Выключить Режим пропажи (для режима "Расширенный контроль")** | На мобильном устройстве выключен Режим пропажи, устройство разблокировано. |

## 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 отозвать разрешения в параметрах устройства позднее. В этом случае выполнение команд невозможно.

На устройствах с Android 10 или выше необходимо предоставить разрешение "Всегда" для доступа к местоположению устройства. На устройствах с Android 11 или 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. Мы рекомендуем 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 (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. Разблокировать устройство с помощью команд невозможно.

Подробная информация об отправке команд из списка мобильных устройств в Web Console приведена в разделе Отправка команд.

*Одноразовый код* – секретный код для разблокировки мобильного устройства. Этот код создается в Kaspersky Security Center. Он уникален для каждого мобильного устройства. Вы можете изменить длину одноразового кода (4, 8, 12 или 16 цифр) в параметрах **Анти-Вор** политики.

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

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.

2. Выберите мобильное устройство, для разблокировки которого вы хотите получить одноразовый код.

3. Выберите **Приложения** → **Kaspersky Mobile Devices Protection and Management**.

   Откроется окно свойств Kaspersky Mobile Devices Protection and Management.

4. Выберите вкладку **Параметры приложения**.

   В поле **Одноразовый код** в разделе **Одноразовый код разблокировки устройства** будет указан уникальный для выбранного устройства код.

5. Сообщите пользователю заблокированного мобильного устройства одноразовый код любым доступным способом (например, в сообщении электронной почты).

   Затем пользователю нужно ввести одноразовый код на экране устройства, заблокированном Kaspersky Endpoint Security для Android.

Мобильное устройство пользователя будет разблокировано.

После разблокировки устройства под управлением операционной системы Android 5–6 пароль разблокировки экрана будет заменен на "1234". На устройствах под управлением Android 7 или выше после разблокировки пароль разблокировки экрана останется прежним.

*Чтобы изменить длину одноразового кода разблокировки устройства:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Защита**.

4. На карточке **Анти-Вор** нажмите **Параметры**.

   Откроется окно **Анти-Вор**.

5. Выберите длину одноразового кода устройства в соответствующем раскрывающемся списке. По умолчанию код состоит из 4 цифр.

6. Если вы хотите связаться с человеком, который нашел мобильное устройство, в поле **Текст, отображаемый на заблокированном устройстве** введите текст сообщения, которое будет отображаться на экране блокировки.

7. Нажмите **ОК**.

8. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Будет установлена выбранная длина одноразового кода разблокировки.

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

# 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 разблокировке устройства.

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 или выше при попытке пользователя настроить неподдерживаемые способы разблокировки устройства (например, графический пароль) оно 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.

### Настройка параметров пароля разблокировки

*Чтобы настроить использование пароля разблокировки:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Контроль безопасности**.

4. На карточке **Параметры разблокировки экрана** нажмите **Параметры**.

   Откроется окно **Параметры разблокировки экрана**.

5. Включите параметры с помощью переключателя **Параметры разблокировки экрана**, если нужно, чтобы приложение проверяло, установлен ли пароль разблокировки.

   Переключатель на этой карточке не включает и не выключает соответствующую функциональность на устройствах. Включение переключателя позволяет настроить пользовательские параметры. Выключение переключателя позволяет использовать параметры по умолчанию.

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

6. При необходимости укажите следующие параметры:

- **Минимальная длина пароля**

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

  По умолчанию пароль пользователя состоит из 4 символов.

  Следующая информация относится только к личному пространству пользователя и корпоративному контейнеру:

  - В личном пространстве пользователя Kaspersky Endpoint Security сводит требования к надежности пароля к одному из значений, доступных в системе: средний или высокий уровень для устройств под управлением Android 10 или выше.
  - В корпоративном контейнере Kaspersky Endpoint Security сводит требования к надежности пароля к одному из значений, доступных в системе: 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 сложности пароля**

  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**
  - **Минимальное количество строчных букв**
  - **Минимальное количество заглавных букв**
  - **Минимальное количество небуквенных символов**

- **Сложный числовой**

  Пользователь может установить пароль, включающий в себя числа без повторений (например, 4444) или упорядоченных последовательностей (например, 1234, 4321, 2468), или любой более надежный сложный пароль.

- **Максимальный срок действия пароля (дней)**

  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 установить 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 экрана (сек)**

  Определяет период неактивности перед блокировкой экрана устройства.

  По умолчанию указано значение 0. Это означает, что экран устройства не будет блокироваться после окончания какого-либо периода.

- **Период после биометрической разблокировки до запрашивания пароля (мин)**

  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.

- **Разрешить биометрические методы разблокировки**

  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.

- **Разрешить разблокировку по отпечатку пальца**

  Указывает, можно ли использовать отпечатки 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 устройства пункт установки отпечатков пальцев будет недоступен.

  Флажок доступен, только если установлен флажок **Разрешить биометрические методы разблокировки**.

  По умолчанию флажок установлен.

  На некоторых устройствах Xiaomi с корпоративным контейнером этот контейнер можно разблокировать с помощью отпечатка пальца только в том случае, если значение параметра **Период неактивности без блокировки корпоративного контейнера (сек)** будет установлено после установки отпечатка пальца в качестве способа разблокировки экрана.

- **Разрешить распознавание лица**

  Если флажок установлен, на мобильном устройстве разрешено использование распознавания лица.

  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**.

По умолчанию флажок установлен.

- **Разрешить распознавание по радужной оболочке глаза**

  Если флажок установлен, на мобильном устройстве разрешено использование распознавания радужной оболочки глаза.

  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**.

  По умолчанию флажок установлен.

- **Сбрасывать настройки до заводских после неудачных попыток ввода пароля**

  Позволяет ограничить количество попыток ввода пароля разблокировки экрана.

  Если флажок установлен, приложение удаляет все данные на устройстве, когда пользователю не удается ввести правильный пароль после указанного количества попыток.

  Если флажок снят, количество попыток не ограничено.

  По умолчанию флажок снят.

- **Максимальное количество неудачных попыток ввода пароля**

  Определяет количество попыток ввода пароля, которые пользователь может совершить, чтобы разблокировать устройство. По умолчанию указано значение 8. Максимальное доступное значение – 20.

  Поле доступно, если установлен флажок **Сбрасывать настройки до заводских после неудачных попыток ввода пароля**.

- **Установить новый пароль**

  Этот параметр позволяет установить пароль на корпоративном устройстве пользователя.

  Нажмите эту кнопку, чтобы открыть окно **Новый пароль разблокировки экрана** и ввести новый пароль.

  Сложность вводимого пароля должна соответствовать требованиям, заданным ранее в карточке **Параметры разблокировки экрана** политики.

  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 защищено паролем или 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 **OK**.

8. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

## Установка нового пароля разблокировки

*Чтобы установить новый пароль на корпоративном устройстве пользователя:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Ограничения**.

4. На карточке **Новый пароль разблокировки экрана** нажмите **Параметры**.

   Откроется окно **Новый пароль разблокировки экрана**.

5. Включите параметры с помощью переключателя **Новый пароль разблокировки экрана**.

6. Введите новый пароль, который будет использоваться для разблокировки экрана мобильного устройства пользователя. Этот пароль должен соответствовать текущим параметрам пароля разблокировки экрана.

7. Если вы хотите изменить текущие параметры пароля разблокировки, нажмите кнопку **Настроить параметры разблокировки экрана**.

   В открывшемся окне **Параметры разблокировки экрана** настройте параметры пароля разблокировки экрана требуемым образом.

8. Нажмите **OK**.

   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 защищено паролем или работает под управлением операционной системы Android 11 или выше, Kaspersky Endpoint Security для Android предлагает пользователю применить новый пароль.

9. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Новый пароль будет установлен на мобильном устройстве пользователя. Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Kaspersky Security Center.

## Установка PIN-кода на устройствах HUAWEI

На некоторых устройствах HUAWEI отображается сообщение о слишком простом способе разблокировки экрана.

*Чтобы установить подходящий PIN-код на устройстве HUAWEI, пользователь должен выполнить следующие действия:*

1. В сообщении о проблеме нажмите **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 будет установлен правильный PIN-код.

## Настройка надежности пароля разблокировки iOS MDM-устройства

Эти параметры применяются к устройствам в режимах "Расширенный контроль" и "Базовый контроль".

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 буквенно-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:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Контроль безопасности**.
4. На карточке **Параметры разблокировки экрана** нажмите **Параметры**.

   Откроется окно **Параметры разблокировки экрана**.
5. Включите параметры с помощью переключателя **Параметры разблокировки экрана**.

   Переключатель на этой карточке не включает и не выключает соответствующую функциональность на устройствах. Включение переключателя позволяет настроить пользовательские параметры. Выключение переключателя позволяет использовать параметры по умолчанию.

6. Настройте параметры надежности пароля разблокировки:

- Чтобы разрешить пользователю использовать простой пароль, установите флажок **Разрешить простой пароль**. Если этот флажок снят, пользователь по-прежнему может установить пароль длиной менее 6 символов.

  Если установлен только флажок **Разрешить простой пароль**, пароль запрашиваться не будет. Чтобы предложить пользователю задать пароль, установите флажки **Разрешить простой пароль** и **Принудительно использовать пароль**.

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

- Чтобы сделать использование пароля обязательным, установите флажок **Принудительно использовать пароль**. Если флажок снят, мобильное устройство можно использовать без пароля.

  Если включен один из параметров – **Требовать ввод буквенно-цифрового значения**, **Минимальная длина пароля** или **Минимальное количество специальных символов**, – пароль запрашивается, даже если снят флажок **Принудительно использовать пароль**.

- В списке **Минимальная длина пароля** выберите минимальное количество символов в пароле.

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

  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.

- В поле **Максимальный срок действия пароля (дней)** укажите период времени в днях, в течение которого будет действовать пароль. По истечении установленного срока Сервер iOS MDM запрашивает у пользователя смену пароля.

- В списке **Автоблокировка** выберите период времени, по истечении которого должна включаться автоблокировка на iOS MDM-устройстве. Если в течение выбранного времени мобильным устройством не пользуются, оно переходит в режим сна.

  На разных iOS MDM-устройствах фактическое время включения автоблокировки устройства может отличаться от заданного значения:

  На устройствах iPhone: если выбрана автоблокировка через 10 или 15 минут, устройство будет заблокировано через 5 минут.

  На устройствах iPad: если выбрана автоблокировка через 1–4 минуты, устройство будет заблокировано через 2 минуты.

  Для других вариантов фактическое время включения автоблокировки устройства соответствует заданному.

- В поле **Повторное использование предыдущих паролей** укажите количество использованных паролей (включая текущий), которые Сервер iOS MDM будет сравнивать с новым паролем при изменении пользователем текущего пароля. 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 поле **Максимальное количество неудачных попыток ввода пароля** выберите количество попыток, которое пользователь может предпринять для ввода пароля разблокировки на iOS MDM-устройстве.

7. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

В результате после применения политики Сервер iOS MDM проверит надежность пароля на мобильном устройстве пользователя. Если надежность пароля разблокировки на устройстве не соответствует политике, пользователю будет предложено изменить пароль.

# 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 интернету и защиты передачи данных можно настроить параметры VPN (Virtual Private Network).

Настройка VPN возможна только для Samsung-устройств под управлением Android 11 или ниже.

При использовании виртуальной частной сети необходимо учитывать следующие требования:

- Приложение, использующее VPN-соединение, должно быть разрешено в параметрах **Сетевой экран**.
- Параметры VPN, 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:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Параметры Samsung Knox**.
4. На карточке **VPN** нажмите **Параметры**.

   Откроется окно **VPN**.
5. Включите параметры с помощью переключателя **VPN**.

6. Укажите следующие параметры VPN:

- Параметры в разделе **Сеть**:
  - В поле **Имя сети** введите имя VPN-туннеля.
  - В раскрывающемся списке **Протокол** выберите тип VPN-соединения:
    - **IPSec Xauth PSK**. Туннельный протокол типа "шлюз-шлюз", позволяющий пользователю мобильного устройства устанавливать защищенное соединение с VPN-сервером с использованием утилиты авторизации Xauth.
    - **L2TP IPSec PSK**. Туннельный протокол типа "шлюз-шлюз", позволяющий пользователю мобильного устройства устанавливать защищенное соединение с VPN-сервером по протоколу IKE с использованием предварительно установленного ключа. Это протокол выбран по умолчанию.
    - **PPTP**. Туннельный протокол типа "точка-точка", позволяющий пользователю мобильного устройства устанавливать защищенное соединение с VPN-сервером за счет создания специального туннеля в стандартной, незащищенной сети.
  - В поле **Адрес сервера** введите сетевое имя или IP-адрес VPN-сервера.
- Параметры в разделе **Параметры протокола**:
  - 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.
  - В поле **DNS-сервер(ы)** введите полное доменное имя или IP-адрес DNS-сервера.

    Вы можете ввести несколько DNS-серверов через пробел.
  - 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.

7. Дополнительно настройте следующие параметры:

- Для протоколов **IPSec Xauth PSK** и **L2TP IPSec PSK**:
  - В поле **Общий ключ IPSec** введите пароль от предварительно установленного ключа безопасности IPSec.
  - В поле **Идентификатор IPSec** введите имя пользователя мобильного устройства.
- Для типа протокола **L2TP IPSec PSK** укажите пароль для ключа L2TP в поле **Ключ L2TP**.
- 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.

8. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

## Настройка VPN на iOS MDM-устройствах

Эти параметры применяются к устройствам в режимах "Расширенный контроль" и "Базовый контроль".

Для подключения iOS MDM-устройства к виртуальной частной сети (VPN) и обеспечения безопасности данных при подключении к сети VPN нужно настроить параметры подключения к сети VPN. Протоколы VPN IKEv2 и IPSec также позволяют настроить соединение Per App VPN.

*Чтобы настроить VPN-соединение на iOS MDM-устройстве пользователя:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **VPN** нажмите **Параметры**.

   Откроется окно **VPN**.
5. Включите параметры с помощью переключателя **VPN**.
6. Нажмите **Добавить**.

   Откроется окно **Добавить конфигурацию VPN**.
7. На вкладке **Общие** в разделе **Сеть** настройте следующие параметры:

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

   b. В раскрывающемся списке **Протокол** 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 открытого ключа.
   - **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**. Соединение поддерживает аутентификацию пользователей с помощью паролей, двухфакторную аутентификацию и автоматическую аутентификацию с помощью открытого 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 нужно 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 нужно 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 нужно 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 нужно установить на iOS MDM-устройство приложение SonicWALL Mobile Connect из App Store.

- **Aruba VIA**. Соединение поддерживает контроллеры мобильного доступа Aruba Networks. Для их настройки нужно 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.

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

8. Настройте **параметры VPN-соединения** в соответствии с выбранным типом виртуальной частной сети.

- L2TP
  - Параметры в разделе **Аутентификация**:
    - **Тип аутентификации**

      Двухфакторная аутентификация пользователя iOS MDM-устройства с использованием токена RSA SecurID или аутентификация на основе пароля.

    - **Имя учетной записи**

      Имя учетной записи для авторизации на VPN-сервере.

    - **Пароль**

      Пароль учетной записи для аутентификации в виртуальной частной сети.

    - **Метод аутентификации**

      Метод аутентификации пользователей iOS MDM-устройств в виртуальной частной сети.

    - **Общий ключ**

Пароль для предварительно установленного ключа безопасности IPSec для протоколов L2TP и IPSec (Cisco).

- **Сертификат аутентификации**

  Сертификат, используемый для аутентификации пользователя.

- Параметры в разделе **Прочее**:

  - **Отправлять весь трафик через VPN**

    Передача через VPN-соединение всего исходящего трафика, даже если используется другая сетевая служба (например, AirPort или Ethernet).

    Если флажок установлен, весь исходящий трафик передается через VPN-соединение.

    Если флажок снят, исходящий трафик передается без обязательного использования VPN-соединения.

    По умолчанию флажок снят.

- **IPSec**

  - Параметры в разделе **Аутентификация**:

    - **Метод аутентификации**

      Метод аутентификации пользователей iOS MDM-устройств в виртуальной частной сети.

    - **Имя учетной записи**

      Имя учетной записи для авторизации на VPN-сервере.

    - **Пароль**

      Пароль учетной записи для аутентификации в виртуальной частной сети.

    - **Общий ключ**

      Пароль для предварительно установленного ключа безопасности IPSec для протоколов L2TP и IPSec (Cisco).

    - **Имя группы**

      Имя группы iOS MDM-устройств, которые подключаются к VPN-сети по протоколам L2TP и IPSec (Cisco). Если установлен флажок **Использовать гибридную аутентификацию**, имя группы должно заканчиваться на "[hybrid]" (например, "mycompany [hybrid]").

- **Использовать гибридную аутентификацию**

  Использование гибридной аутентификации при подключении пользователя к VPN-сети. Для аутентификации VPN-сервер использует сертификат, а пользователь iOS MDM-устройства вводит открытый ключ для аутентификации по протоколу IPSec (Cisco).

  Если флажок установлен, при подключении пользователя к VPN-сети используется гибридная аутентификация.

  Если флажок снят, гибридная аутентификация не используется.

  По умолчанию флажок снят.

- **Сертификат аутентификации**

  Сертификат, используемый для аутентификации пользователя.

- Параметры в разделе **Домены**:

  - **Включать VPN при подключении указанных доменов**

    Домены, для которых будет включено VPN-соединение.

- Параметры в разделе **Прочее**:

  - **Требовать PIN**

    Проверка наличия системного пароля при включении мобильного устройства.

    Если флажок установлен, Kaspersky Mobile Devices Protection and Management проверяет на устройстве наличие системного пароля. Если системный пароль на устройстве не задан, пользователю нужно задать его. Пароль должен быть задан с учетом параметров, настроенных администратором.

    Если флажок снят, Kaspersky Mobile Devices Protection and Management не требует наличия системного пароля.

    По умолчанию флажок снят.

- **IKEv2**

  - Параметры в разделе **Сеть**:

    - **Интервал обнаружения неработающих узлов (DPD)**

      Периодичность, с которой VPN-клиент IKEv2 должен запускать алгоритм обнаружения неработающих узлов (DPD). Доступны следующие значения:

      - **Не выбрано**. Не запускать DPD.
      - **Низкий**. Запускать DPD каждые 30 минут.
      - **Средний**. Запускать DPD каждые 10 минут.
      - **Высокий**. Запускать DPD 1 раз в минуту.

По умолчанию выбран вариант **Средний**.

- Параметры в разделе **Аутентификация**:
  - **Метод аутентификации**

    Метод аутентификации пользователей iOS MDM-устройств в виртуальной частной сети.

  - **Локальный идентификатор**

    Идентификатор VPN-клиента IKEv2 (iOS MDM-устройство).

  - **Удаленный идентификатор**

    Идентификатор VPN-сервера IKEv2.

  - **Общий ключ**

    Общий ключ, используемый для аутентификации VPN IKEv2.

  - **Общее имя (CN) сертификата сервера**

    Имя используется для проверки сертификата, отправленного VPN-сервером IKEv2. Если этот параметр не задан, сертификат проверяется с помощью удаленного идентификатора.

  - **Общее имя (CN) издателя сертификата сервера**

    Если задан этот параметр, IKEv2 отправляет на сервер запрос на сертификат на основе этого поставщика сертификата.

  - **Сертификат аутентификации**

    Сертификат, используемый для аутентификации пользователя.

  - **Аутентификация по EAP**

    Тип аутентификации по EAP, используемый для VPN-соединения IKEv2. Доступны следующие значения:

    - **Учетные данные**
    - **Сертификат**

    По умолчанию указано значение **Учетные данные**.

  - **Имя учетной записи**

Имя учетной записи для авторизации на VPN-сервере.

- **Пароль**

  Пароль учетной записи для аутентификации в виртуальной частной сети.

- **Минимальная версия TLS**

  Минимальная версия TLS, используемая для аутентификации по EAP. Доступны следующие значения:

  - **TLS 1.0**
  - **TLS 1.1**
  - **TLS 1.2**

  По умолчанию указано значение **TLS 1.0**.

- **Максимальная версия TLS**

  Максимальная версия TLS, используемая для аутентификации по EAP. Доступны следующие значения:

  - **TLS 1.0**
  - **TLS 1.1**
  - **TLS 1.2**

  По умолчанию указано значение **TLS 1.2**.

- Параметры в разделе **Ассоциация безопасности (SA)**:

  - **Параметры SA**

    Определяет объект, в котором отправляются параметры. Возможные значения:

    - **IKEv2**
    - **Дочерняя**

    По умолчанию указано значение **IKEv2**.

  - **Алгоритм шифрования**

    Определяет алгоритм шифрования, используемый для соединения. Возможные значения:

    - **DES**
    - **3DES**
    - **AES-128**

- **AES-256**
- **AES-128-GCM**
- **AES-256-GCM**
- **ChaCha20Poly1305**

По умолчанию указано значение **AES-256**.

- **Алгоритм целостности**

Определяет алгоритм целостности, используемый для соединения. Возможные значения:

- **SHA1-96**
- **SHA1-160**
- **SHA2-256**
- **SHA2-384**
- **SHA2-512**

По умолчанию указано значение **SHA2-256**.

- **Группа Диффи-Хеллмана**

Определяет группу Диффи – Хеллмана, используемую при настройке VPN-туннеля.

По умолчанию указано значение 14.

- **Время жизни SA (мин)**

Интервал смены ключа в минутах.

- Параметры в разделе **Прочее**:
  - **Запретить перенаправление**

Определяет, запрещено ли перенаправление на VPN-сервере IKEv2.

Если флажок установлен, VPN-соединение IKEv2 не перенаправляется.

Если флажок снят, VPN-соединение IKEv2 перенаправляется, когда от сервера получен запрос на перенаправление.

По умолчанию флажок снят.

  - **Запретить протокол Mobility and Multi-Homing (MOBIKE)**

Определяет, запрещен ли протокол Mobility and Multi-Homing (MOBIKE) для VPN-соединения IKEv2.

Если флажок установлен, MOBIKE запрещен.

Если флажок снят, MOBIKE разрешен.

По умолчанию флажок снят.

- **Использовать атрибуты конфигурации IPv4 и IPv6**

  Определяет, должен ли VPN-клиент IKEv2 использовать атрибуты конфигурации INTERNAL_IP4_SUBNET и INTERNAL_IP6_SUBNET, отправляемые VPN-сервером IKEv2.

  Если флажок установлен, атрибуты INTERNAL_IP4_SUBNET и INTERNAL_IP6_SUBNET используются.

  Если флажок снят, атрибуты INTERNAL_IP4_SUBNET и INTERNAL_IP6_SUBNET не используются.

  По умолчанию флажок снят.

- **Активировать туннель через сотовые данные**

  Определяет, включен ли откат.

  Если флажок установлен, устройство активирует туннель через сотовые данные, чтобы пропускать трафик, подходящий для функции Помощь Wi-Fi и требующий наличия VPN.

  Если флажок снят, откат выключен.

  По умолчанию флажок снят.

- **Включить Perfect Forward Secrecy**

  Определяет, включено ли свойство Perfect Forward Secrecy (PFS) для VPN-соединения IKEv2.

  Если флажок установлен, PFS включено.

  Если флажок снят, PFS выключено.

  По умолчанию флажок снят.

- **Cisco AnyConnect**
  - Параметры в разделе **Сеть**:
    - **Время бездействия до прерывания соединения (мин)**

      Время ожидания перед отключением соединения по требованию.

  - Параметры в разделе **Аутентификация**:
    - **Метод аутентификации**

      Метод аутентификации пользователей iOS MDM-устройств в виртуальной частной сети.

    - **Имя учетной записи**

Имя учетной записи для авторизации на VPN-сервере.

- **Пароль**

  Пароль учетной записи для аутентификации в виртуальной частной сети.

- **Группа**

  Псевдоним группы туннелирования для клиентов Cisco AnyConnect при подключении к VPN-сети.

- **Сертификат аутентификации**

  Сертификат, используемый для аутентификации пользователя.

- Параметры в разделе **Домены**:

  - **Включать VPN при подключении указанных доменов**

    Домены, для которых будет включено VPN-соединение.

- Параметры в разделе **Прочее**:

  - **Отправлять весь трафик через VPN**

    Маршрутизирует весь трафик через VPN.

  - **Исключить локальный трафик**

    Исключает локальный трафик из трафика, маршрутизируемого через VPN-соединение.

    Этот флажок доступен, если установлен флажок **Отправлять весь трафик через VPN**.

- **Juniper SSL**

  - Параметры в разделе **Сеть**:

    - **Время бездействия до прерывания соединения (мин)**

      Время ожидания перед отключением соединения по требованию.

  - Параметры в разделе **Аутентификация**:

    - **Метод аутентификации**

Метод аутентификации пользователей iOS MDM-устройств в виртуальной частной сети.

- **Имя учетной записи**

  Имя учетной записи для авторизации на VPN-сервере.

- **Пароль**

  Пароль учетной записи для аутентификации в виртуальной частной сети.

- **Область действия**

  Имя сети, в состав которой входят VPN-серверы и iOS MDM-устройства для VPN-соединения с помощью Juniper SSL.

- **Роль**

  Название роли пользователя, в соответствии с которой пользователь получает доступ к ресурсам с помощью Juniper SSL. Роль может объединять несколько пользователей, выполняющих одинаковые функции.

- **Сертификат аутентификации**

  Сертификат, используемый для аутентификации пользователя.

- Параметры в разделе **Домены**:

  - **Включать VPN при подключении указанных доменов**

    Домены, для которых будет включено VPN-соединение.

- Параметры в разделе **Прочее**:

  - **Отправлять весь трафик через VPN**

    Маршрутизирует весь трафик через VPN.

  - **Исключить локальный трафик**

    Исключает локальный трафик из трафика, маршрутизируемого через VPN-соединение.

    Этот флажок доступен, если установлен флажок **Отправлять весь трафик через VPN**.

- F5 SSL
  - Параметры в разделе **Сеть**:
    - **Время бездействия до прерывания соединения (мин)**

      Время ожидания перед отключением соединения по требованию.
  - Параметры в разделе **Аутентификация**:
    - **Метод аутентификации**

      Метод аутентификации пользователей iOS MDM-устройств в виртуальной частной сети.
    - **Имя учетной записи**

      Имя учетной записи для авторизации на VPN-сервере.
    - **Пароль**

      Пароль учетной записи для аутентификации в виртуальной частной сети.
    - **Сертификат аутентификации**

      Сертификат, используемый для аутентификации пользователя.
  - Параметры в разделе **Домены**:
    - **Включать VPN при подключении указанных доменов**

      Домены, для которых будет включено VPN-соединение.
  - Параметры в разделе **Прочее**:
    - **Отправлять весь трафик через VPN**

      Маршрутизирует весь трафик через VPN.
    - **Исключить локальный трафик**

      Исключает локальный трафик из трафика, маршрутизируемого через VPN-соединение.

      Этот флажок доступен, если установлен флажок **Отправлять весь трафик через VPN**.

- **SonicWALL Mobile Connect**
  - Параметры в разделе **Сеть**:
    - **Время бездействия до прерывания соединения (мин)**

      Время ожидания перед отключением соединения по требованию.
  - Параметры в разделе **Аутентификация**:
    - **Метод аутентификации**

      Метод аутентификации пользователей iOS MDM-устройств в виртуальной частной сети.
    - **Имя учетной записи**

      Имя учетной записи для авторизации на VPN-сервере.
    - **Пароль**

      Пароль учетной записи для аутентификации в виртуальной частной сети.
    - **Домен или группа**

      Доменное имя сервера SSL VPN (например, vpn.company.com) или имя группы пользователей SonicWALL Mobile Connect.
    - **Сертификат аутентификации**

      Сертификат, используемый для аутентификации пользователя.
  - Параметры в разделе **Домены**:
    - **Включать VPN при подключении указанных доменов**

      Домены, для которых будет включено VPN-соединение.
  - Параметры в разделе **Прочее**:
    - **Отправлять весь трафик через VPN**

      Маршрутизирует весь трафик через VPN.
    - **Исключить локальный трафик**

      Исключает локальный трафик из трафика, маршрутизируемого через VPN-соединение.

Этот флажок доступен, если установлен флажок **Отправлять весь трафик через VPN**.

- **Aruba VIA**
  - Параметры в разделе **Сеть**:
    - **Время бездействия до прерывания соединения (мин)**

      Время ожидания перед отключением соединения по требованию.
  - Параметры в разделе **Аутентификация**:
    - **Метод аутентификации**

      Метод аутентификации пользователей iOS MDM-устройств в виртуальной частной сети.
    - **Имя учетной записи**

      Имя учетной записи для авторизации на VPN-сервере.
    - **Пароль**

      Пароль учетной записи для аутентификации в виртуальной частной сети.
    - **Сертификат аутентификации**

      Сертификат, используемый для аутентификации пользователя.
  - Параметры в разделе **Домены**:
    - **Включать VPN при подключении указанных доменов**

      Домены, для которых будет включено VPN-соединение.
  - Параметры в разделе **Прочее**:
    - **Отправлять весь трафик через VPN**

      Маршрутизирует весь трафик через VPN.
    - **Исключить локальный трафик**

      Исключает локальный трафик из трафика, маршрутизируемого через VPN-соединение.

Этот флажок доступен, если установлен флажок **Отправлять весь трафик через VPN**.

- **Custom SSL**
  - Параметры в разделе **Сеть**:
    - **Время бездействия до прерывания соединения (мин)**

      Время ожидания перед отключением соединения по требованию.
  - Параметры в разделе **Конфигурационные данные**:
    - **Ключ**

      Содержит ключ с дополнительными параметрами соединения Custom SSL.
    - **Значение**

      Содержит значение с дополнительными параметрами соединения Custom SSL.
  - Параметры в разделе **Аутентификация**:
    - **Метод аутентификации**

      Метод аутентификации пользователей iOS MDM-устройств в виртуальной частной сети.
    - **Имя учетной записи**

      Имя учетной записи для авторизации на VPN-сервере.
    - **Пароль**

      Пароль учетной записи для аутентификации в виртуальной частной сети.
    - **Сертификат аутентификации**

      Сертификат, используемый для аутентификации пользователя.
    - **Идентификатор пакета (Bundle ID)**

      Если настраиваемая конфигурация VPN работает с решением VPN, которое использует поставщика расширений сети, укажите в этом поле идентификатор пакета приложения, содержащего поставщика. Обратитесь к поставщику решения VPN, чтобы узнать значение идентификатора.

- Параметры в разделе **Домены**:
  - **Включать VPN при подключении указанных доменов**

    Домены, для которых будет включено VPN-соединение.

9. При необходимости на вкладке **Дополнительные** в разделе **Прокси-сервер** настройте параметры VPN-соединения через прокси-сервер:

   a. Установите флажок **Использовать прокси-сервер**.

   b. Настройте подключение к прокси-серверу:

      a. Если вы хотите, чтобы подключение было настроено автоматически:

      - Выберите **Автоматически**.
      - В поле **Веб-адрес PAC-файла** укажите адрес PAC-файла прокси.
      - 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**.

      b. Если вы хотите настроить подключение вручную:

      - Выберите **Вручную**.
      - В полях **Адрес прокси-сервера** и **Порт прокси-сервера** укажите IP-адрес или DNS-имя прокси-сервера и номер порта.
      - В поле **Имя пользователя** выберите макрос, который будет использоваться в качестве имени пользователя для подключения к прокси-серверу.

      c. В поле **Пароль** укажите пароль для подключения к прокси-серверу.

10. При необходимости для подключений по протоколам **IKEv2** и **IPSec** настройте Per App VPN для поддерживаемых системных приложений (Почта, Календарь, Контакты и Safari) или для сторонних приложений.

11. Нажмите **Добавить**.

    Новая сеть VPN отобразится в списке.

    Вы можете изменять или удалять VPN-соединения с помощью кнопок **Изменить** и **Удалить** в верхней части списка.

12. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

В результате после применения политики на iOS MDM-устройстве пользователя будет настроено VPN-соединение.

## Настройка Per App VPN для системных приложений для iOS

Эти параметры применяются к устройствам в режимах "Расширенный контроль" и "Базовый контроль".

Per App VPN позволяет подключать устройства к сети VPN при запуске поддерживаемых системных приложений или сторонних приложений. Эта функция доступна при подключении по протоколам IKEv2 и IPSec.

Соединения Per App VPN поддерживаются следующими системными приложениями:

- Почта
- Календарь
- Контакты
- Safari
- Сообщения

Для корректной работы функциональности Per App VPN версия Сервера iOS MDM должна быть не ниже 15.4.0.2019.

*Чтобы включить Per App VPN для поддерживаемых системных приложений:*

1. Выполните первоначальную настройку VPN-соединения.
2. На вкладке **Дополнительные** в разделе **Per App VPN** установите флажок **Включить Per App VPN**.
3. Настройте Per App VPN для поддерживаемых системных приложений в соответствующих параметрах политики.

### Почта

*Чтобы указать конфигурацию Per App VPN для приложения Почта:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **Электронная почта** нажмите **Параметры**.

   Откроется окно **Электронная почта**.
5. Включите параметры с помощью переключателя **Электронная почта**.
6. Добавьте новую учетную запись электронной почты или измените существующую учетную запись.

7. На вкладке **Дополнительные** в разделе **Per App VPN** установите флажок **Включить Per App VPN**.
8. Выберите конфигурацию из раскрывающегося списка **Конфигурация Per App VPN**.
9. Нажмите **Сохранить**.
10. Нажмите **OK**.
11. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

    Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

    В результате после применения политики для приложения Почта будет настроен Per App VPN.

### Календарь

*Чтобы указать конфигурацию Per App VPN для приложения Календарь:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **Календарь** нажмите **Параметры**.

   Откроется окно **Календарь**.
5. Включите параметры с помощью переключателя **Календарь**.
6. Добавьте новую учетную запись календаря или измените существующую учетную запись.
7. В разделе **Per App VPN** установите флажок **Включить Per App VPN**.
8. Выберите конфигурацию из раскрывающегося списка **Конфигурация Per App VPN**.
9. Нажмите **Добавить**.
10. Нажмите **OK**.
11. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

    Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

    В результате после применения политики для приложения Календарь будет настроен Per App VPN.

### Подписки на календари

Список подписок на календари других пользователей CalDAV, календари iCal и другие опубликованные календари.

*Чтобы указать конфигурацию VPN для подписок на календари:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **Подписки на календари** нажмите **Параметры**.

   Откроется окно **Подписки на календари**.
5. Включите параметры с помощью переключателя **Подписки на календари**.
6. Добавьте новую подписку на календарь или измените существующую подписку.
7. В разделе **Per App VPN** установите флажок **Включить Per App VPN**.
8. Выберите конфигурацию из раскрывающегося списка **Конфигурация Per App VPN**.
9. Нажмите **Добавить**.
10. Нажмите **OK**.
11. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

    Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

    В результате после применения политики для подписок на календари будет настроен Per App VPN.

## Контакты

*Чтобы указать конфигурацию Per App VPN для приложения Контакты:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **Контакты** нажмите **Параметры**.

   Откроется окно **Контакты**.
5. Включите параметры с помощью переключателя **Контакты**.
6. Добавьте новую учетную запись контактов или измените существующую учетную запись.
7. В разделе **Per App VPN** установите флажок **Включить Per App VPN**.
8. Выберите конфигурацию из раскрывающегося списка **Конфигурация Per App VPN**.

9. Нажмите **Добавить**.

10. Нажмите **OK**.

11. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

В результате после применения политики для приложения Контакты будет настроен Per App VPN.

## Safari

*Чтобы указать конфигурацию Per App VPN для Safari:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.

4. На карточке **Per App VPN для Safari** нажмите **Параметры**.

   Откроется окно **Per App VPN для Safari**.

5. Включите параметры с помощью переключателя **Per App VPN для Safari**.

6. Нажмите **Добавить**.

   Откроется окно **Добавить домен сайта**.

7. Выберите конфигурацию из раскрывающегося списка **Конфигурация Per App VPN**.

8. В поле **Имя домена** укажите домен сайта, который будет активировать VPN-соединение в Safari. Домен необходимо указывать в формате `www.example.com`.

9. Нажмите **Добавить**.

   Новый домен появится в списке **Домены сайтов Safari**.

   > Вы можете изменять или удалять домены веб-сайтов Safari с помощью кнопок **Изменить** и **Удалить** в верхней части списка.

10. Нажмите **OK**.

11. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

В результате после применения политики для доменов сайтов Safari будет настроен Per App VPN.

## LDAP

Учетная запись LDAP позволяет получить доступ к корпоративным данным и контактам в стандартных приложениях iOS: Контакты, Сообщения и Почта.

*Чтобы указать конфигурацию Per App VPN для учетной записи LDAP:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **LDAP** нажмите **Параметры**.

   Откроется окно **LDAP**.
5. Включите параметры с помощью переключателя **LDAP**.
6. Добавьте новую учетную запись LDAP или измените существующую учетную запись.
7. В разделе **Per App VPN** установите флажок **Включить Per App VPN**.
8. Выберите конфигурацию из раскрывающегося списка **Конфигурация Per App VPN**.
9. Нажмите **Добавить**.
10. Нажмите **OK**.
11. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

    Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

    В результате после применения политики для учетной записи LDAP будет настроен Per App VPN.

## Exchange ActiveSync

Учетная запись Exchange ActiveSync позволяет синхронизировать корпоративную электронную почту, календарь, контакты, заметки и задачи с сервера Microsoft Exchange.

*Чтобы указать конфигурацию Per App VPN для учетной записи Exchange ActiveSync:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **Exchange ActiveSync** нажмите **Параметры**.

   Откроется окно **Exchange ActiveSync**.

5. Включите параметры с помощью переключателя **Exchange ActiveSync**.
6. Добавьте новую учетную запись Exchange ActiveSync или измените существующую учетную запись.
7. На вкладке **Дополнительные** в разделе **Per App VPN** установите флажок **Включить Per App VPN**.
8. Выберите конфигурацию из раскрывающегося списка **Конфигурация Per App VPN**.
9. Нажмите **Добавить**.
10. Нажмите **OK**.
11. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

    Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

    В результате после применения политики для учетной записи Exchange ActiveSync будет настроен Per App VPN.

## Настройка Per App VPN для сторонних приложений для iOS

Эти параметры применяются к устройствам в режимах "Расширенный контроль" и "Базовый контроль".

Per App VPN позволяет подключать устройства к сети VPN при запуске поддерживаемых системных приложений или сторонних приложений. Эта функция доступна при подключении по протоколам IKEv2 и IPSec.

Для корректной работы функциональности Per App VPN версия Сервера iOS MDM должна быть не ниже 15.4.0.2019.

*Чтобы настроить Per App VPN для стороннего приложения:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **VPN** нажмите **Параметры**.

   Откроется окно **VPN**.
5. Настройте VPN-соединение с протоколом **IKEv2** или **IPSec**.
6. На вкладке **Дополнительные** в разделе **Per App VPN** установите флажок **Включить Per App VPN**.
7. Выберите псевдоним конфигурации Per App VPN, который вы хотите присвоить этой конфигурации VPN.

   Псевдоним позволяет использовать соответствующую конфигурацию VPN для инсталляционного пакета стороннего приложения.

Если псевдоним конфигурации Per App VPN не выбран, Per App VPN доступен только для системных приложений.

Если изменить выбранный ранее псевдоним конфигурации Per App VPN, VPN будет выключен для всех сторонних приложений, использующих эту конфигурацию, после их повторной установки или обновления.

8. Нажмите **Добавить**.

   Новая конфигурация VPN, поддерживающая функциональность Per App VPN, отобразится в списке.

9. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

10. Чтобы настроить Per App VPN для необходимого стороннего приложения, выполните одно из следующих действий:

- **Укажите псевдоним конфигурации Per App VPN для нового стороннего приложения**

  1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Приложения и файлы** → **iOS**.
  2. Нажмите **Добавить**.

     Откроется окно **Добавить приложение**.
  3. Настройте приложение.
  4. В разделе **Per App VPN** нажмите **Включить Per App VPN** и выберите псевдоним для конфигурации VPN, которую вы хотите включать при использовании приложения.

     Настроенные параметры будут применены после установки приложения.
  5. Нажмите **Добавить**.

  Новое управляемое приложение с настроенным Per App VPN отобразится в списке.

- **Укажите псевдоним конфигурации Per App VPN для уже установленного стороннего приложения**

  1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Приложения и файлы** → **iOS**.
  2. В списке нажмите на имя приложения, для которого вы хотите настроить Per App VPN.

     Откроется окно **Информация о приложении**.
  3. В разделе **Per App VPN** нажмите **Включить Per App VPN** и выберите псевдоним для конфигурации VPN, которую вы хотите включать при использовании приложения.

     Настроенные параметры будут применены после переустановки или обновления приложения.
  4. Нажмите **OK**.

Указанная конфигурация Per App VPN для этого управляемого приложения отобразится в соответствующей колонке таблицы.

Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

После установки необходимого стороннего приложения Per App VPN будет настроен для этого приложения.

## Настройка Сетевого экрана на Android-устройствах (только Samsung)

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

Сетевой экран можно настроить только для следующих режимов работы устройств Samsung:

- корпоративное устройство;
- личное устройство под управлением Android 15 или ниже;
- устройство с корпоративным контейнером под управлением Android 15 или ниже.

*Чтобы настроить Сетевой экран на мобильном устройстве пользователя:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Параметры Samsung Knox**.
4. На карточке **Сетевой экран** нажмите **Параметры**.

   Откроется окно **Сетевой экран**.
5. Включите параметры с помощью переключателя **Сетевой экран**.
6. В раскрывающемся списке **Доступ в интернет** выберите режим Сетевого экрана. В соответствии с режимом работы Сетевой экран контролирует соединения на мобильном устройстве пользователя:
   - Если вы хотите разрешить входящие и исходящие соединения для всех установленных приложений, выберите **Разрешить для всех приложений**. Этот режим выбран по умолчанию.
   - Если вы хотите заблокировать сетевую активность для всех приложений, кроме нескольких указанных, выберите **Разрешить для указанных приложений**.
7. Если выбран режим Сетевого экрана **Разрешить для указанных приложений**, создайте список приложений, которым разрешена вся сетевая активность:
   a. В разделе **Приложения с доступом в интернет** нажмите **Добавить**.

      Откроется окно **Добавить приложение**.
   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 **Добавить**.

Новое приложение, для которого выключен Сетевой экран, появится в списке.

Вы можете изменять или удалять мобильные приложения из списка с помощью кнопок **Изменить** и **Удалить** в верхней части списка.

8. Нажмите **OK**.

9. Нажмите **Сохранить**, 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 мобильных устройств 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 Android 7 или выше при попытке пользователя настроить неподдерживаемые способы разблокировки устройства (например, графический пароль) оно 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 устройствах под управлением 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 разрешения. Пользователь может пропустить эти шаги или отозвать разрешения в параметрах устройства позднее. В этом случае защита приложения от удаления не работает.

*Чтобы включить защиту Kaspersky Endpoint Security для Android от удаления:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Параметры KES для Android**.

4. На карточке **Параметры доступа к настройкам приложения** нажмите **Параметры**.

   Откроется окно **Параметры доступа к настройкам приложения**.

5. Включите параметры с помощью переключателя **Параметры доступа к настройкам приложения**.

   Переключатель на этой карточке не включает и не выключает соответствующую функциональность на устройствах. Включение переключателя позволяет настроить пользовательские параметры. Выключение переключателя позволяет использовать параметры по умолчанию.

6. Снимите флажок **Разрешить удаление приложения с устройства**.

7. Нажмите **OK**.

8. Нажмите **Сохранить**, 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 устройств

Kaspersky Security Center Web Console позволяет обнаруживать взлом устройства (получение root-прав) на Android-устройствах и модификацию прошивки (jailbreak) на iOS-устройствах. На взломанном устройстве системные файлы не защищены и доступны для изменения. После обнаружения взлома рекомендуется восстановить нормальную работу устройства.

При взломе устройства вы получите уведомление. Вы можете просмотреть уведомления о взломах в Kaspersky Security Center Web Console в разделе **Мониторинг → 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**.

## Настройка глобального HTTP-прокси на iOS MDM-устройствах

Эти параметры применяются к устройствам в режиме "Расширенный контроль".

Для маршрутизации интернет-трафика пользователя настройте подключение iOS MDM-устройства к интернету через прокси-сервер.

Будьте осторожны при настройке этих параметров. В случае неправильной настройки устройства могут потерять подключение к интернету и не будут синхронизироваться с Сервером iOS MDM. Если это произойдет, вам придется заново добавить эти устройства.

*Чтобы настроить глобальный HTTP-прокси на iOS MDM-устройстве:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.

4. На карточке **Глобальный HTTP-прокси** нажмите **Параметры**.

   Откроется окно **Глобальный HTTP-прокси**.

5. Включите параметры с помощью переключателя **Глобальный HTTP-прокси**.

6. Выберите тип настройки глобального HTTP-прокси:

   - Чтобы вручную задать параметры подключения к прокси-серверу:

     a. В разделе **Тип настройки** выберите **Вручную**.

     b. В полях **Адрес прокси-сервера** и **Порт прокси-сервера** введите имя хоста 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.

     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 сетям с авторизацией без подключения к прокси-серверу**.

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

     a. В разделе **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 сетям с авторизацией без подключения к прокси-серверу**.

7. Нажмите **OK**.

8. Нажмите **Сохранить**, 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

Эти параметры применяются к устройствам в режимах "Расширенный контроль" и "Базовый контроль".

Вы можете добавлять сертификаты на iOS MDM-устройства, чтобы упростить аутентификацию пользователей и обеспечить безопасность данных. Данные, подписанные сертификатом, защищены от изменений при передаче по сети. Шифрование данных с помощью сертификата обеспечивает дополнительную защиту информации. Сертификат также может использоваться для удостоверения личности пользователя.

Kaspersky Mobile Devices Protection and Management 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-устройства:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **Управление сертификатами** нажмите **Параметры**.

   Откроется окно **Управление сертификатами**.
5. Включите параметры с помощью переключателя **Управление сертификатами**.
6. Нажмите **Загрузить** и укажите путь к сертификату.

   Файлы сертификатов PKCS#1 имеют расширения CER, DER или PEM. Файлы сертификатов PKCS#12 имеют расширения P12 или PFX. Пароль для сертификата PKCS#12 не должен быть пустым.
7. Нажмите **Открыть**.

   Если сертификат защищен паролем, введите пароль. Новый сертификат отобразится в списке.
8. Нажмите **ОК**.
9. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

В результате после применения политики сертификаты будут автоматически установлены на устройствах.

## Добавление профиля SCEP на iOS MDM-устройства

Эти параметры применяются к устройствам в режимах "Расширенный контроль" и "Базовый контроль".

Чтобы пользователь iOS MDM-устройства мог автоматически получать сертификаты из Центра сертификации через интернет, нужно 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, нужно 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:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **SCEP** нажмите **Параметры**.

   Откроется окно **SCEP**.
5. Включите параметры с помощью переключателя **SCEP**.
6. Нажмите **Добавить**.

   Откроется окно **Добавить профиль SCEP**.
7. В разделе **Сервер SCEP** укажите следующие параметры SCEP-сервера:

   - В поле **Имя конфигурации** укажите название Центра сертификации, развернутого на SCEP-сервере. Центр сертификации обеспечивает пользователя iOS MDM-устройства сертификатами при помощи простого протокола регистрации SCEP.
   - 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`.
   - В поле **Максимальное количество попыток опроса** укажите максимальное количество попыток опроса SCEP-сервера для подписания сертификата. Значение по умолчанию – 3 попытки.

     Если все попытки подписать сертификат были неудачными, нужно сформировать новый запрос на подписание сертификата.
   - В поле **Интервал между попытками (сек)** укажите период времени в секундах между попытками опроса SCEP-сервера для подписания сертификата. Значение по умолчанию – 10 секунд.
   - В поле **Статическая контрольная фраза** 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.

- В раскрывающемся списке **Метод загрузки отпечатка сертификата** выберите способ добавления отпечатка сертификата. Вы можете использовать отпечатки сертификатов с алгоритмом хеширования SHA-1 или MD5.

  - Если вы выбрали вариант **Вручную**, в появившемся поле **Отпечаток сертификата** введите уникальный отпечаток сертификата для проверки подлинности ответа Центра сертификации.

  - Если вы выбрали вариант **Из файла**, загрузите файл в формате CER, KEY или PEM. Отпечаток будет сгенерирован и добавлен автоматически.

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

8. В разделе **Субъект** укажите следующие параметры:

- В поле **Имя субъекта** введите строку с атрибутами пользователя iOS MDM-устройства, которые содержатся в сертификате X.500.

  Атрибуты могут содержать сведения о стране (C), местоположении (L), стране (ST), организации (O), подразделении (OU) и общем имени пользователя (CN). Например, `/C=RU/O=MyCompany/CN=User/`.

  Вы можете использовать и другие атрибуты, которые приведены в RFC 5280.

  Атрибуты используются DNS-службами для проверки подлинности сертификата, выданного Центром сертификации по запросу пользователя.

- Нажмите **Добавить альтернативное имя субъекта**, чтобы добавить поле для указания альтернативного имени субъекта:

  - В раскрывающемся списке **Тип альтернативного имени субъекта** выберите тип альтернативного имени субъекта SCEP-сервера. Можно добавить только одно альтернативное имя каждого типа.

    Вы можете использовать альтернативное имя субъекта для идентификации пользователя iOS MDM-устройства. По умолчанию идентификация на основе альтернативного имени не используется.

    - **DNS-имя**. Идентификация по доменному имени.

    - **Имя субъекта NT**. DNS-имя пользователя iOS MDM-устройства в сети Windows NT. Имя субъекта NT содержится в запросе на сертификат в SCEP-сервер. Вы также можете использовать имя субъекта NT для идентификации пользователя iOS MDM-устройства.

    - **Адрес электронной почты**. Идентификация по адресу электронной почты. Адрес электронной почты должен быть представлен в соответствии с RFC 822.

    - **Унифицированный идентификатор ресурса (URI)**. Идентификация по IP-адресу или адресу в формате FQDN.

  - В поле **Альтернативное имя субъекта (SAN)** введите альтернативное имя субъекта сертификата X.500. Значение альтернативного имени субъекта зависит от выбранного типа субъекта: адрес электронной почты пользователя, домен или веб-адрес.

9. В разделе **Ключ** настройте параметры ключа шифрования:

   - В раскрывающемся списке **Размер ключа (бит)** выберите размер ключа регистрации в битах: 1024, 2048 или 4096. По умолчанию указано значение 1024 бита.

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

     Подпись данных защищает данные от изменений. Например, Safari может проверить подлинность сертификата и установить безопасный сеанс обмена данными.

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

     Шифрование данных также защищает конфиденциальные данные при обмене данными по сети. Например, Safari может установить безопасный сеанс обмена данными с использованием шифрования. Это гарантирует подлинность сайта и подтверждает, что соединение с сайтом зашифровано для предотвращения перехвата личных и конфиденциальных данных.

     Вы не можете одновременно использовать сертификат SCEP-сервера в качестве сертификата для подписи данных и сертификата шифрования данных.

   - Если вы хотите разрешить всем установленным приложениям доступ к закрытому ключу из сертификата SCEP-сервера, установите флажок **Разрешить всем приложениям доступ к закрытому ключу**.

   - Если вы не хотите, чтобы закрытый ключ экспортировался из связки ключей, установите флажок **Запретить экспорт закрытого ключа из Связки ключей**.

10. Нажмите **Добавить**.

    Новый профиль SCEP отобразится в списке.

    Вы можете изменять или удалять профили SCEP с помощью кнопок **Изменить** и **Удалить** в верхней части списка.

11. Нажмите **OK**.

12. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

    Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

    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)

Настройте ограничения для SD-карт, чтобы контролировать их использование на устройстве Samsung с поддержкой Knox.

*Чтобы ограничить использование SD-карт на мобильном устройстве:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Параметры Samsung Knox**.
4. На карточке **Ограничения функций устройств** нажмите **Параметры**.

   Откроется окно **Ограничения функций устройств**.
5. Включите параметры с помощью переключателя **Ограничения функций устройств**.
6. В разделе **Параметры SD-карты** укажите необходимые ограничения:

   - **Запретить доступ к SD-карте**

     Этот параметр применим для устройств с Android 5-12.

     Установка или снятие этого флажка определяет, включен или отключен доступ к SD-карте на устройстве.

     По умолчанию флажок снят.

   - **Запретить запись на SD-карту**

     Установка или снятие этого флажка определяет, включена или отключена запись на SD-карту на устройстве.

     По умолчанию флажок снят.

   - **Запретить перенос приложений на SD-карту**

     Установка или снятие флажка определяет, разрешено ли пользователю устройства перемещать приложения на SD-карту.

     По умолчанию флажок снят.
7. В разделе **Дополнительные параметры** можно указать дополнительные ограничения:

   - **Запретить отправку отчетов о сбоях в Google**

     Этот параметр применим только для устройств под управлением Android 11 или ниже.

     Если флажок установлен, Kaspersky Endpoint Security для Android блокирует отправку отчетов о сбоях в Google.

     Если флажок снят, отправка отчетов разрешена.

По умолчанию флажок снят.

- **Запретить режим разработчика**

  Этот параметр применим только для устройств с Android 11 или ниже.

  Если флажок установлен, пользователю запрещено включать режим разработчика на устройстве.

  Если флажок снят, пользователю разрешено включать режим разработчика на устройстве.

  По умолчанию флажок снят.

8. Нажмите **OK**.
9. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

   Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Kaspersky Security Center. Параметры SD-карты настроены.

# Управление мобильными устройствами

Этот раздел содержит информацию о том, как удаленно управлять мобильными устройствами в Kaspersky Security Center Web Console.

## Удаленный доступ к Android-устройствам

Kaspersky Security Center Web Console позволяет удаленно подключаться к Android-устройствам через приложение Kaspersky Endpoint Security для Android, установленное на устройстве. После начала сессии удаленного управления вы сможете просматривать экран устройства, делать снимки экрана и выполнять действия на устройстве.

Процесс удаленного подключения состоит из следующих этапов:

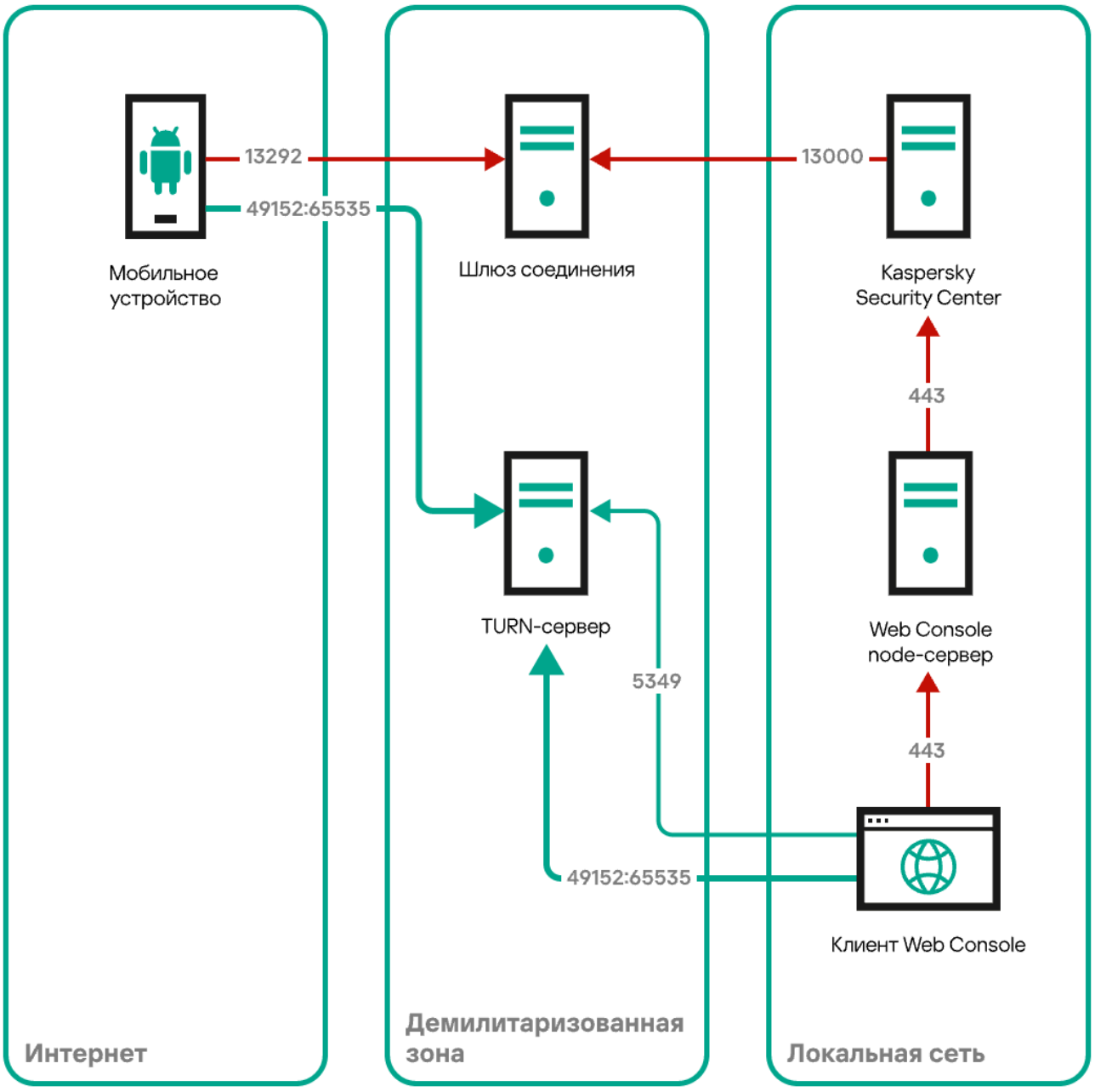
1. Установка и настройка TURN-сервера
2. Настройка сервера удаленного управления в Kaspersky Security Center
3. Запуск сессии удаленного управления

# Установка и настройка TURN-сервера

## Обзор удаленного подключения

Удаленный доступ к Android-устройству предполагает установление соединения с помощью *WebRTC (Web Real-Time Communication)* - технологии потоковой передачи данных, которая обеспечивает одноранговые соединения между двумя браузерами или мобильными приложениями. Передача данных с использованием WebRTC осуществляется через *сервер TURN (Traversal Using Relays around NAT)*, который выступает в качестве посредника и ретранслирует трафик между участниками соединения.

Процесс удаленного подключения представлен на рисунке ниже.




TURN-сервер должен быть доступен как для браузера, с которого вы подключаетесь к устройству, так и для самого устройства. Если браузер находится в локальной сети, а мобильное устройство - в интернете, TURN-сервер можно разместить в демилитаризованной зоне. Информация для установления соединения передается на устройство по мобильному протоколу. Для установления соединения необходимо настроить диапазон портов на TURN-сервере. Для одного соединения используются два порта.

TURN-сервер выполняет следующие функции:

- Установление соединения

  TURN-сервер обеспечивает процесс обмена кандидатами ICE (Interactive Connectivity Establishment) для выбора оптимального пути соединения между Kaspersky Security Center Web Console и мобильным устройством. По запросу от устройства TURN-сервер возвращает ICE-кандидат - потенциальный сетевой маршрут (порт 5349 на рисунке выше), который можно использовать для установления соединения.

- Передача видеоданных

  TURN-сервер действует как туннель, который принимает подключения от Kaspersky Security Center и мобильного устройства. Оба участника соединения отправляют свои медиапотоки на TURN-сервер, который затем передает их другому участнику и тем самым обеспечивает передачу данных.

## Установка и настройка TURN-сервера

### 1 Установите TURN-сервер

Системные требования для TURN-сервера:

- 2 CPU или vCPU;
- 4 ГБ ОЗУ;
- 15 ГБ HDD;
- 512 КБ/с на одно активное соединение.

Мы рекомендуем использовать одну из реализаций TURN-сервера - *coturn*. Coturn можно установить из репозитория GitHub или пакетного менеджера вашей операционной системы.

Ниже приведена инструкция по установке coturn на примере операционной системы Ubuntu:

1. Установите пакет coturn на сервере в демилитаризованной зоне, используя команды:
   ```
   sudo apt-get update
   sudo apt install coturn
   ```
2. После успешного завершения установки проверьте статус запущенного сервиса coturn:
   ```
   systemctl status coturn.service
   ```
3. Добавьте службу coturn в автозапуск:
   ```
   sudo systemctl enable coturn
   ```

### 2 Настройте TURN-сервер

1. Укажите необходимые параметры в конфигурационном файле TURN-сервера, используя текстовый редактор, например, *Vim* или *nano*. Путь к файлу: `/etc/turnserver.conf`.

   Используйте параметры TURN-сервера, **приведенные в примере**. Неиспользуемые параметры необходимо закомментировать.

Пример параметров TURN-сервера

| Параметр | Тип | Описание |
|---|---|---|
| `tls-listening-port=5349` | Обязательный | Порт прослушивания для TLS-соединений |
| `server-name=<example.abc.com>` | Обязательный | FQDN-имя или IP-адрес сервера |
| `realm=<abc.com>` | Обязательный | Доменное имя сервера |
| `min-port=50010` | Обязательный | Нижнее значение диапазона портов для ретрансляции UDP (User Datagram Protocol)<br>Для одной сессии удаленного управления используются два UDP-порта. |

| Параметр | Тип | Описание |
| --- | --- | --- |
| `max-port=50120` | Обязательный | Верхнее значение диапазона портов для ретрансляции UDP |
| `verbose` | Опциональный | Использовать подробное ведение журналов |
| `fingerprint` | Обязательный | Использовать цифровой отпечаток для идентификации и повышения безопасности сервера |
| `use-auth-secret` | Обязательный | Метод аутентификации |
| `static-auth-secret=<секрет>` | Обязательный | Статическое значение секрета аутентификации для REST API TURN-сервера<br><br>Это строковое значение, которое сервер использует для проверки первоначального ICE-запроса. После этого секрет подключения генерируется динамически.<br><br>Статический секрет следует периодически менять с учетом требований безопасности и политики паролей организации. |
| `no-udp` | Опциональный | Ограничить прослушивание незашифрованного UDP |
| `no-tcp` | Опциональный | Ограничить прослушивание незашифрованного TCP (Transmission Control Protocol) |
| `stale-nonce=300` | Опциональный | Время ожидания предоставления учетных данных от неавторизованного пользователя (сек) |
| `cert=/AFMH/SSL/cert.pem` | Обязательный | Путь к сертификату в формате PEM |
| `pkey=/AFMH/SSL/key.pem` | Обязательный | Путь к ключу сертификата в формате PEM |
| `log-file=/var/tmp/turn.log` | Обязательный | Путь для хранения файлов журналов |
| `new-log-timestamp` | Опциональный | Включить добавление времени в файлы журналов |
| `log-binding` | Опциональный | Включить подробное ведение журналов для конечной точки UDP |
| `no-stun` | Опциональный | Выключить функциональность STUN (Session Traversal Utilities for NAT), чтобы сервер работал только в режиме TURN |
| `no-multicast-peers` | Опциональный | Выключить поддержку мультикаст-пиров в качестве дополнительной меры безопасности для предотвращения отправки данных нескольким получателям одновременно |
| `no-tlsv1` | Опциональный | Выключить небезопасные версии TLS v1 |
| `no-tlsv1_1` | Опциональный | Выключить небезопасные версии TLS v1_1 |
| `cipher-list=ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-CHACHA20-POLY1305` | Опциональный | Включить использование разрешенных шифров для TLS 1.2 |
| `denied-peer-ip=10.0.0.0-10.255.255.255`<br>`denied-peer-ip=192.168.0.0-192.168.255.255`<br>`denied-peer-ip=172.16.0.0-172.31.255.255` | Опциональный | Запретить клиентам TURN-сервера доступ к сегментам локальной сети |

| Параметр | Тип | Описание |
|---|---|---|
| `allowed-peer-ip=ipv4, ipv4-ipv4` | Опциональный | Разрешить адрес или диапазон адресов локальной подсети, исключив его из запрещенного списка |
| `max-bps=200000` | Опциональный | Максимальная пропускная способность одной сессии TURN-сервера (бит/с) |
| `bps-capacity` | Опциональный | Максимальная общая пропускная способность, которую разрешено выделять TURN-серверу (бит/с) |

2. Настройте Firewall на сервере, открыв порты, указанные в конфигурационном файле TURN-сервера:
```
sudo ufw allow 5349/tcp
sudo ufw allow 50010:50120/udp
```

### 3 Получите и настройте сертификат TURN-сервера

Вы можете получить сертификат от центра сертификации (CA) или сгенерировать самоподписанный сертификат.

- Сертификат от CA должен быть выдан в формате PEM для полного доменного имени сервера, указанного в конфигурационном файле TURN-сервера.

- Чтобы сгенерировать самоподписанный сертификат (например, с использованием утилиты OpenSSL):

  1. Сгенерируйте ключ CA:
  ```
  openssl genrsa -out ca_key.key 2048
  ```

  2. Сгенерируйте самоподписанный сертификат CA, используя данные для вашей организации или произвольные данные:
  ```
  openssl req -x509 -new -nodes -key ca_key.key -sha256 -days 365 -subj "/C=
  <Country>/ST=<State or Province>/L=<Locality>/O=<Organization>/CN=<Common
  Name>" -out root_cert.pem
  ```

  3. Сгенерируйте закрытый ключ сервера:
  ```
  openssl genrsa -out cert_key.key 2048
  ```

  4. Создайте Certificate Signing Request (CSR) для сервера, используя данные для вашей организации или произвольные данные:
  ```
  openssl req -new -key cert_key.key -subj "/C=<Country>/ST=<State or
  Province>/L=<Locality>/O=<Organization>" -out server_cert.csr
  ```

  5. Создайте конфигурацию для расширений SAN, EKU и KeyUsage - файл `ext.cnf` с содержимым:
  ```
  [ v3_req ]
  subjectAltName = @alt_names
  extendedKeyUsage = serverAuth
  keyUsage = digitalSignature, keyCertSign, cRLSign
  [ alt_names ]
  DNS.1 = <TURN server FQDN>
  ```

  6. Подпишите серверный сертификат CA:
  ```
  openssl x509 -req -in server_cert.csr -CA root_cert.pem -CAkey ca_key.key -
  CAcreateserial -out server_cert.crt -days 365 -sha256 -extfile ext.cnf -
  extensions v3_req
  ```

  7. Преобразуйте закрытый ключ сервера в формат PEM для использования в конфигурационном файле TURN-сервера:
  ```
  openssl rsa -in cert_key.key -out cert_key.pem -outform PEM
  ```

8. Преобразуйте серверный сертификат, подписанный CA, в формат PEM для использования в конфигурационном файле TURN-сервера:
   ```
   openssl x509 -in server_cert.crt -out server_cert.pem
   ```

9. Преобразуйте самоподписанный корневой сертификат в формат CRT для установки в хранилище сертификатов доверенного центра сертификации на компьютере администратора:
   ```
   openssl x509 -in root_cert.pem -out root_cert.crt
   ```

10. Укажите путь к ранее полученным файлам `server_cert.pem` и `cert_key.pem` в конфигурационном файле TURN-сервера. Этот путь должен быть доступен TURN-серверу, например, `/var/opt/turn`.

    Убедитесь, что пользователю `turnserver` выданы права на чтение.

11. Установите файл `root_cert.crt` в хранилище сертификатов доверенного центра сертификации на компьютере администратора, а затем перезапустите браузер.

**4 Завершение настройки**

1. Перезапустите coturn:
   ```
   systemctl restart coturn.service
   ```

2. Перезапустите UFW:
   ```
   systemctl restart ufw
   ```

## Настройка сервера удаленного управления в Kaspersky Security Center

После установки и настройки TURN-сервера необходимо указать параметры удаленного управления в Kaspersky Security Center, чтобы Kaspersky Security Center мог получить доступ к этому TURN-серверу. Настройки не передаются на TURN-сервер автоматически. Они должны быть заданы отдельно и соответствовать значениям, указанным в конфигурационном файле TURN-сервера.

Когда будут указаны необходимые параметры, Kaspersky Security Center сможет сгенерировать данные для сессии удаленного управления и отправить их на Android-устройство по мобильному протоколу.

*Чтобы указать настройки сервера удаленного управления в Kaspersky Security Center:*

1. В главном окне Kaspersky Security Center Web Console нажмите на имя Сервера администрирования.

2. В открывшемся окне свойств Сервера администрирования на вкладке **Общие** выберите раздел **Порты подключения**.

3. В разделе настроек **Параметры Сервера удаленного управления для Android** включите переключатель **Использовать Сервер удаленного управления для Android-устройств**.

   Положение переключателя определяет, будет ли Kaspersky Security Center использовать TURN-сервер для удаленного доступа к Android-устройствам.

4. Укажите **FQDN TURN-сервера**.

   Этот параметр задает FQDN (DNS-имя), которое Kaspersky Security Center будет использовать для получения публичного адреса и порта ICE-кандидата для удаленного управления устройством.

   > В этом поле нельзя указывать IP-адрес.

5. Укажите **Порт TURN-сервера для запроса ICE-кандидата**.

Этот порт необходим для того, чтобы Kaspersky Endpoint Security для Android и Kaspersky Security Center могли запрашивать ICE-кандидат у TURN-сервера. TURN-сервер ответит на запрос, указав адрес и порт, с которого был получен этот запрос.

ICE-кандидаты запрашиваются в незашифрованном виде.

Порт TURN-сервера должен совпадать со значением `tls-listening-port`, указанным в конфигурационном файле TURN-сервера.

6. Установите **Постоянный секрет TURN-сервера**.

   Этот параметр необходим для того, чтобы Kaspersky Security Center мог генерировать секретные сессионные ключи для подключения к TURN-серверу. Постоянный секрет - это произвольная строка с требованиями, аналогичными паролю.

   Указанный постоянный секрет TURN-сервера не отображается в поле настроек и остается невидимым.

   Убедитесь, что секрет совпадает со значением `static-auth-secret`, указанным в конфигурационном файле TURN-сервера.

7. Загрузите **Сертификат TURN-сервера**.

   Загрузите открытый ключ `root_cert.crt` сертификата, который вы получили на 9 шаге 3 этапа настройки TURN-сервера, нажав **Загрузить**. Открытый ключ будет использоваться браузером администратора и Kaspersky Endpoint Security для Android для проверки подлинности TURN-сервера, который будет возвращать ICE-кандидаты.

   Сертификат может быть загружен в формате PEM, CER или CRT и должен быть идентичен сертификату, установленному на TURN-сервере, включая формат адреса сервера (FQDN или DNS-имя).

8. Нажмите **Сохранить**.

Настройки сервера удаленного управления указаны. Теперь вы можете начать сессию удаленного управления устройством.

## Запуск сессии удаленного управления

*Чтобы запустить удаленную сессию и управлять ей:*

1. Убедитесь, что соблюдены необходимые **условия для удаленного подключения**.

   - Версия Kaspersky Security Center Web Console - 16.1 или выше.
   - Версия плагина Kaspersky Mobile Devices Protection and Management - 10.56 или выше.
   - Установлен и настроен TURN-сервер.

- В Kaspersky Security Center указаны параметры сервера удаленного управления.
- В хранилище Сервера администрирования установлена лицензия с поддержкой продвинутой функциональности Kaspersky Secure Mobility Management.
- Администратору выданы права **Запуск RDP-сеансов** и **Отправка команд на мобильные устройства** для установления удаленных соединений.
- Мобильное устройство, к которому будет осуществляться удаленный доступ, работает под управлением Android 8 или выше.
- Версия Kaspersky Endpoint Security для Android на устройстве - 10.56.1.11 или выше.
- Пользователь устройства принял Лицензионное соглашение (EULA), которое содержит функциональность удаленного управления.

2. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.
3. В открывшемся списке мобильных устройств установите флажок рядом с устройством, к которому вы хотите получить удаленный доступ.
4. Откройте меню с 3 точками ( ⋮ ) и выберите **Удаленное управление для Android**, чтобы начать сессию удаленного управления.

   Нельзя начать сессию удаленного управления устройством, которое в настоящий момент находится под удаленным управлением другого администратора.

   Откроется окно удаленного управления, и удаленная сессия будет инициирована. После синхронизации мобильного устройства с Kaspersky Security Center пользователь получит запрос на удаленное подключение. При настроенной интеграции с Firebase Cloud Messaging (FCM) синхронизация произойдет автоматически. В противном случае, дождитесь синхронизации по расписанию или попросите пользователя синхронизировать устройство вручную.

   Время ожидания подключения пользователя не превышает одного часа. По истечении этого времени сессию необходимо перезапустить.

   Если мобильное устройство работает в режиме корпоративного устройства, вы можете попробовать подключиться к нему без запроса согласия пользователя.

   В параметрах **Настройка уведомлений** раздела **Параметры KES для Android** можно настроить, будет ли запрашиваться согласие пользователя при запуске сессии удаленного управления.
5. Как только пользователь примет запрос и начнется сессия удаленного управления, отобразится экран устройства. Изображение располагается в соответствии с ориентацией экрана мобильного устройства.

Пока сессия активна, вы можете:

- Просматривать экран устройства и проверять скорость соединения.

  Не получится просмотреть содержимое экрана, если он защищен от создания скриншотов и видеозаписи (например, в режиме инкогнито в браузере, или если экран устройства заблокирован).

- Выполнять действия на устройстве:

  - Нажимая кнопки **Главный экран**, **Назад** и **Обзор** под отображаемым экраном устройства.

  - Управляя устройством с помощью жестов. Жесты применяются путем нажатия курсором на область дисплея. Вы можете имитировать касание или длительное касание нажатием или длительным нажатием курсора на изображение экрана устройства, а также передвигать курсор в зажатом состоянии и отпускать его.

- Делать скриншоты, нажав **Сделать снимок экрана**.

  Скриншот сохраняется в папке "Загрузки" браузера; его название содержит имя устройства, дату и точное время снимка.

- Завершить сессию по кнопке **Остановить** и запустить ее снова для того же устройства, не закрывая окно.

  После начала сессии удаленного управления вы можете продолжить работу в Kaspersky Security Center Web Console в новой вкладке браузера, не прерывая текущую сессию. Вы также можете открыть Kaspersky Security Center в другой вкладке или окне и начать еще одну сессию удаленного управления для другого устройства.

  Выход из окна удаленного подключения прерывает сессию удаленного управления. Чтобы работать с другими разделами Kaspersky Security Center, сохраняя активную сессию, откройте Kaspersky Security Center в другом окне или вкладке браузера.

Пользователь может прекратить сеанс удаленного управления в любой момент на своем устройстве.

## Управление Android-устройствами

Kaspersky Security Center Web Console позволяет управлять Android-устройствами следующими способами:

- централизованно управлять устройствами с помощью команд;
- просматривать информацию о параметрах управления Android-устройствами;
- устанавливать приложения с помощью пакетов мобильных приложений;
- подключаться к устройствам и удаленно управлять ими;
- отключать Android-устройства от управления.

## Корпоративные устройства

Этот раздел содержит информацию об управлении параметрами корпоративных Android-устройств. Информация об установке Kaspersky Endpoint Security для Android на корпоративные устройства доступна в этом разделе.

## Ограничение функций Android на устройствах

Эти параметры применяются к корпоративным устройствам.

Вы можете ограничить функции операционной системы Android на корпоративных устройствах. 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 управление обновлениями системы. Вы также можете ограничить функции операционной системы на личных устройствах и устройствах с корпоративным контейнером.

*Чтобы ограничить функции Android:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Ограничения**.
4. На карточке **Ограничения функций устройств** нажмите **Параметры**.

   Откроется окно **Ограничения функций устройств**.
5. Включите параметры с помощью переключателя **Ограничения функций устройств**.
6. Включите ограничения функций устройств с помощью переключателей на соответствующих вкладках и выберите необходимые ограничения.
7. Нажмите **OK**.
8. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

## Ограничение функций устройств

На вкладке **Общие** вы можете включить или выключить следующие функции:

- В разделе **Защита от потери данных**:
  - **Запретить сброс настроек до заводских**

    Установка или снятие флажка определяет, разрешено ли пользователю устройства сбрасывать настройки устройства до заводских.

По умолчанию флажок снят.

- **Запретить снимки экрана**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства делать снимки экрана, 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 запуск устройства в безопасном режиме**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства запускать устройство в безопасном режиме.

  Ограничение поддерживается на устройствах с Android 6 или выше.

  По умолчанию флажок снят.

- В разделе **Звонки и SMS**:

  - **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.

- В разделе **Службы геолокации**:

  - **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.

    Разные комбинации значений для флажков **Запретить отслеживание местоположения** и **Запретить изменение параметров местоположения** приводят к разным результатам настройки и работы функции определения местоположения.

| Запретить отслеживание местоположения | Запретить изменение параметров местоположения | Результат ограничения функции |
|---|---|---|
| Включено | Включено | Службы геолокации выключены, и пользователь устройства не может включить их. |
| Включено | Выключено | Службы геолокации выключены, но пользователь устройства может включить их.<br><br>Выключение ограничения **Запретить изменение параметров местоположения** позволяет пользователю выключить службы геолокации на устройстве, что может привести к недоступности некоторых функций. |
| Выключено | Включено | Службы геолокации включены, и пользователь устройства не может выключить их. |
| Выключено | Выключено | Службы геолокации включены, но пользователь устройства может выключить их.<br><br>Выключение ограничения **Запретить изменение параметров местоположения** позволяет пользователю выключить службы геолокации 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 параметров местоположения**

  Запрещает изменение настроек местоположения.

  Если флажок установлен, пользователь устройства не может изменять настройки местоположения или отключать службы геолокации.

  Если флажок снят, пользователь устройства может изменять настройки местоположения.

  Ограничение поддерживается на устройствах с Android 9 или выше.

  По умолчанию флажок снят.

  Разные комбинации значений для флажков **Запретить отслеживание местоположения** и **Запретить изменение параметров местоположения** приводят к разным результатам настройки и работы функции определения местоположения.

| Запретить отслеживание местоположения | Запретить изменение параметров местоположения | Результат ограничения функции |
|---|---|---|
| Включено | Включено | Службы геолокации выключены, и пользователь устройства не может включить их. |
| Включено | Выключено | Службы геолокации выключены, но пользователь устройства может включить их.<br><br>Выключение ограничения **Запретить изменение параметров местоположения** позволяет пользователю выключить службы геолокации на устройстве, что может привести к недоступности некоторых функций. |

| | | |
|---|---|---|
| Выключено | Включено | Службы геолокации включены, и пользователь устройства не может выключить их. |
| Выключено | Выключено | Службы геолокации включены, но пользователь устройства может выключить их.<br><br>Выключение ограничения **Запретить изменение параметров местоположения** позволяет пользователю выключить службы геолокации на устройстве, что может привести к недоступности некоторых функций. |

- В разделе **Функции keyguard**:
  - **Запретить функции 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 отключение уведомлений на защищенных экранах keyguard**

    Установка или снятие флажка определяет, запрещены ли уведомления, когда экран устройства заблокирован.

    По умолчанию флажок снят.

  - **Запретить использование камеры в keyguard**

    Установка или снятие флажка определяет, запрещено ли пользователю устройства использовать камеру, когда устройство заблокировано.

    По умолчанию флажок снят.

  - **Запретить использование доверительных агентов**

    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.

    По умолчанию флажок снят.

- В разделе **Пользователи и учетные записи**:
  - **Запретить добавление учетных записей Google**

    Установка или снятие флажка определяет, разрешено ли пользователю устройства добавлять и удалять аккаунты Google.

    По умолчанию флажок снят.

- **Запретить добавление пользователей**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства добавлять пользователей.

  По умолчанию флажок установлен. Если корпоративное устройство было подключено к Kaspersky Security Center с помощью QR-кода, это ограничение включено и не может быть выключено.

  Ограничение можно выключить только на устройствах, отвечающих следующим требованиям:

  - Корпоративное устройство подключено к Kaspersky Security Center с помощью инсталляционного пакета `adb.exe`.
  - Устройство должно поддерживать несколько пользователей.

- **Запретить смену пользователя**

  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 корпоративное устройство было подключено к Kaspersky Security Center с помощью QR-кода, это ограничение нельзя выключить.

  Ограничение можно выключить только на устройствах, отвечающих следующим требованиям:

  - Корпоративное устройство подключено к Kaspersky Security Center с помощью инсталляционного пакета `adb.exe`.
  - Устройство должно поддерживать несколько пользователей.

- **Запретить изменение учетных данных**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства менять учетные данные в операционной системе.

  По умолчанию флажок снят.

## Ограничение функций приложений

На вкладке **Приложения** вы можете включить или выключить следующие функции:

- В разделе **Общие**:

  - **Запретить установку приложений**

    Установка или снятие флажка определяет, разрешено ли пользователю устройства устанавливать приложения 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 отключение проверки приложения**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства отключать проверку приложений.

  По умолчанию флажок снят.

- **Запретить удаление приложений**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства удалять приложения с устройства.

  По умолчанию флажок снят.

- В разделе **Приложения Google**:

  - **Запретить Google Play**

    Установка или снятие флажка определяет, разрешено ли пользователю устройства использовать Google Play.

    По умолчанию флажок снят.

- **Запретить 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 Google Assistant**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства использовать Google Assistant на устройстве.

  По умолчанию флажок снят.

- В разделе **Камера**:

  - **Запретить использование камеры**

    Установка или снятие флажка определяет, разрешено ли пользователю устройства использовать все имеющиеся на устройстве камеры.

    Если флажок установлен, решение обычно блокирует использование камеры. Однако на устройствах Asus, Honor и OnePlus значок приложения "Камера" полностью скрыт, если флажок установлен.

    По умолчанию флажок снят.

  - **Запретить выключение камеры**

    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 под управлением Android 12 это ограничение не работает. Проблема связана с особенностями прошивки MIUI на устройствах Xiaomi и прошивки EMUI на устройствах HUAWEI.

- **Выдача дополнительных разрешений для работы приложений**

  Этот параметр позволяет выбрать действие, которое будет выполняться, когда приложения, установленные на корпоративных устройствах, запускаются и запрашивают дополнительные разрешения. Это неприменимо к разрешениям, выданным в Настройках устройства (например, Доступ ко всем файлам).

  - **Разрешить настройку пользователям**

Пользователь решает, выдавать ли разрешение приложению.

Этот параметр выбран по умолчанию.

- **Выдавать разрешения автоматически**

  Для всех приложений, установленных на корпоративных устройствах, разрешения выдаются без взаимодействия с пользователем.

- **Отклонять разрешения автоматически**

  Для всех приложений, установленных на корпоративных устройствах, разрешения отклоняются без взаимодействия с пользователем.

  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;
- разрешения на отслеживание входящих SMS и MMS сообщений;
- разрешения на доступ к данным биометрических датчиков.

## Ограничение функций памяти

На вкладке **Хранилище** в разделе **Общие** вы можете включить или выключить 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 подключать 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**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства включать или выключать сервис резервного копирования.

  Ограничение поддерживается на устройствах с Android 8 или выше.

  По умолчанию флажок снят.

## Ограничение функций сети

На вкладке **Сеть** вы можете включить или выключить следующие функции:

- В разделе **Общие**:

  - **Запретить режим полета**

    Установка или снятие флажка определяет, разрешено ли пользователю включать режим полета на устройстве.

    Ограничение поддерживается на устройствах с Android 9 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.

  - **Запретить изменение параметров VPN**

    Запрещает изменение параметров 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 параметров сетей**

  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.

- В разделе **Wi-Fi**:

  - **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**

    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 параметров 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**

    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**

    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**

    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.

- В разделе **Bluetooth**:

  - **Запретить использование Bluetooth**

    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 или выше.

    По умолчанию флажок снят.

  - **Запретить изменение параметров Bluetooth**

    Установка или снятие флажка определяет, разрешено ли пользователю устройства изменять параметры Bluetooth в Настройках.

    По умолчанию флажок снят.

  - **Запретить обмен данными через Bluetooth**

    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.

- В разделе **Мобильные сети**:

  - **Запретить изменение параметров 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**

    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 параметрах **Обновление баз** политики.

Чтобы разрешить синхронизацию устройств с Сервером администрирования в роуминге, этот флажок, а также флажок **Выключить синхронизацию в роуминге** в параметрах **Синхронизация по расписанию** политики должны быть сняты.

Ограничение поддерживается на устройствах с Android 7 или выше.

По умолчанию флажок снят.

## Дополнительные ограничения

На вкладке **Дополнительные параметры** вы можете включить или выключить следующие функции:

- В разделе **Язык, дата и время**:
  - **Запретить изменение языка**

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

  - **Запретить изменение даты, времени и часового пояса**

    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.

- В разделе **Экран**:
  - **Запретить изменение обоев**

    Установка или снятие флажка определяет, разрешено ли пользователю устройства изменять обои экрана мобильного устройства.

    Ограничение поддерживается на устройствах с Android 7 или выше.

    По умолчанию флажок снят.

  - **Запретить изменение яркости**

    Установка или снятие флажка определяет, разрешено ли пользователю устройства регулировать яркость экрана мобильного устройства.

    Ограничение поддерживается на устройствах с Android 9 или выше.

По умолчанию флажок снят.

- **Запретить строку состояния**

  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 6 или выше.

  По умолчанию флажок снят.

- **Запретить автоматическое включение экрана**

  Если этот параметр включен, пользователь не может использовать функцию автоматического включения экрана на устройстве.

  По умолчанию этот параметр отключен.

- В разделе **Включение экрана**:

  - **Принудительно включать экран при подключении к сетевому зарядному устройству**

    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**

    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 во время беспроводной зарядки**

    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.

- В разделе **Микрофон**:

  - **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**

  Если этот параметр включен, 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 под управлением Android 12 это ограничение не работает. Проблема связана с особенностями прошивки MIUI на устройствах Xiaomi и прошивки EMUI на устройствах HUAWEI.

- В разделе **Громкость**:

  - **Запретить изменение громкости**

    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 игнорировать это ограничение, чтобы воспроизвести звуковой сигнал на устройстве. Ограничение выключается, чтобы разрешить воспроизведение звукового сигнала, а затем снова включается.

    По умолчанию флажок снят.

## 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 **Обновление ОС** вы можете настроить следующие параметры:

- В разделе **Режим обновления**:

  - **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.

  Вам нужно указать начало и завершение ежедневного периода обслуживания в полях **Время начала** и **Время окончания**.
- **Отложить обновления 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.

- В разделе **Периоды приостановки**:
  - **Периоды приостановки обновления системы**

    В этом блоке можно задать один или несколько периодов приостановки обновления системы до 90 дней, в течение которых обновления не будут устанавливаться на устройство. 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 **Дата начала** и **Дата окончания**.

    > 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

> Эти параметры применяются к корпоративным устройствам.

*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.

Режим киоска не влияет на работу приложения Kaspersky Endpoint Security для Android. Оно продолжает работать в фоновом режиме, присылает 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 9 или выше приложение запускается непосредственно в режиме киоска. На устройствах с Android 8 или 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.

## Действия перед настройкой режима киоска

Перед настройкой режима киоска выполните следующие действия:

- Перед тем как указать приложения, которые можно запускать на устройстве в режиме киоска, нужно выбрать действие **Установить** для этих приложений на вкладке **Управление приложениями** в параметрах политики **Контроль приложений**. Затем они появятся в списке **Пакет приложения** в параметрах политики **Режим киоска**.

- Если вы хотите указать доверенные приложения, в которые пользователи могут переходить из разрешенных в режиме киоска, сначала добавьте эти приложения как разрешенные в параметрах политики **Контроль приложений**. Выполните одно из следующих действий:

  - На вкладке **Использование приложений** добавьте приложение в список **Разрешенные приложения**.

  - На вкладке **Управление приложениями** выберите для приложения действие **Установить** или **Рекомендовать к установке**.

Затем указанные приложения появятся в разделе **Доверенные приложения** параметров политики **Режим киоска**.

- Перед включением режима киоска мы рекомендуем запретить запуск Google Assistant, включив соответствующее ограничение в разделе **Управление активами → Политики → Параметры приложения → Android → Ограничения → Ограничения функций устройств → Приложения → Запретить Google Assistant**. В противном случае Google Assistant запустится в режиме киоска и позволит открывать недоверенные приложения.

## Переход в настройки режима киоска

*Чтобы открыть настройки режима киоска:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Ограничения**.
4. На карточке **Режим киоска** нажмите **Параметры**.

Откроется окно **Режим киоска**.

## Настройка режима одного приложения

*Чтобы настроить режим одного приложения:*

1. Включите параметры с помощью переключателя **Режим киоска**.
2. В раскрывающемся списке **Режим работы** выберите **Режим одного приложения**.
3. В раскрывающемся списке **Пакет приложения** выберите пакет приложения с приложением, которое разрешено запускать на устройстве.
4. Укажите любые необходимые ограничения. С доступными ограничениями можно ознакомиться ниже в разделе "Ограничения режима киоска".
5. Установите флажок **Разрешить переход в доверенные приложения**, если хотите разрешить пользователю устройства переход в другие приложения. Подробнее см. ниже в разделе "Добавление дополнительных приложений".
6. Нажмите **OK**.
7. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

## Настройка режима с несколькими приложениями

*Чтобы настроить режим с несколькими приложениями:*

1. Включите параметры с помощью переключателя **Режим киоска**.
2. В раскрывающемся списке **Режим работы** выберите **Режим с несколькими приложениями**.
3. Нажмите на кнопку **Добавить пакет** и выберите приложения, которые разрешено запускать на устройстве.
4. Укажите любые необходимые ограничения. С доступными ограничениями можно ознакомиться ниже в разделе "Ограничения режима киоска".
5. Установите флажок **Разрешить переход в доверенные приложения**, если хотите разрешить пользователю устройства переход в другие приложения. Подробнее см. ниже в разделе "Добавление дополнительных приложений".
6. Нажмите **OK**.
7. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

## Ограничения режима киоска

В режиме киоска вы можете установить следующие ограничения:

- **Запретить кнопку "Обзор"**

  Установка или снятие флажка определяет, будет ли скрыта кнопка "Обзор". Ограничение поддерживается на устройствах с Android 9 или выше.

  По умолчанию флажок установлен.

- **Запретить кнопку "Главный экран"**

  Установка или снятие флажка определяет, будет ли скрыта кнопка "Главный экран". Ограничение поддерживается на устройствах с Android 9 или выше.

  По умолчанию флажок установлен.

- **Запретить строку состояния**

  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 9 или выше.

  По умолчанию флажок установлен.

- **Запретить системные уведомления**

  Установка или снятие флажка определяет, будут ли скрыты системные уведомления. Ограничение поддерживается на устройствах с Android 9 или выше.

  По умолчанию флажок установлен.

- **Запретить включение режима киоска, если не все выбранные приложения обновлены или установлены**

  Установка или снятие флажка определяет, можно ли включить режим киоска, если одно или несколько приложений не обновлены или не установлены на устройстве.

  Если флажок установлен, режим киоска нельзя включить, пока не установлены или не обновлены все необходимые приложения. Если приложения не удается обновить в уже включенном режиме киоска, Kaspersky Endpoint Security для Android отображает блокирующий экран, чтобы ограничить использование устройства. Чтобы продолжить использование режима киоска с более ранними версиями приложений, пользователю нужно нажать **Вернуться в режим киоска** на блокирующем экране. Этот блокирующий экран появится снова, если приложения режима киоска не были обновлены в течение 24 часов, либо если для приложений режима киоска были изменены параметры политики **Контроль приложений** и необходимые приложения все еще не обновлены.

  Если флажок снят, режим киоска можно включить, даже если не все необходимые приложения обновлены или установлены.

  Этот флажок доступен, только если режим киоска работает в режиме с несколькими приложениями.

  По умолчанию флажок установлен.

## Выключение режима киоска по одноразовому коду

*Одноразовый код* – секретный код для выключения режима киоска. Этот код создается в Kaspersky Security Center. Он уникален для каждого мобильного устройства. Вы можете изменить длину одноразового кода (4, 8, 12 или 16 цифр) в параметрах **Режим киоска** политики.

*Чтобы настроить выключение режима киоска:*

1. В разделе **Выключение по одноразовому коду** установите флажок **Разрешить выключение режима киоска по одноразовому коду**.
2. При необходимости измените длину одноразового кода в соответствующем раскрывающемся списке. По умолчанию код состоит из 4 цифр.
3. Нажмите **ОК**.
4. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Теперь режим киоска может быть выключен по одноразовому коду. Будет установлена выбранная длина одноразового кода.

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

*Чтобы выключить режим киоска на мобильном устройстве пользователя по одноразовому коду:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.
2. Выберите мобильное устройство, для которого вы хотите получить одноразовый код.
3. Выберите **Приложения** → **Kaspersky Mobile Devices Protection and Management**.

   Откроется окно свойств **Kaspersky Mobile Devices Protection and Management**.
4. Выберите вкладку **Параметры приложения**.

   В поле **Одноразовый код** в разделе **Одноразовый код выключения режима киоска** будет указан уникальный для выбранного устройства код.
5. Сообщите пользователю заблокированного мобильного устройства одноразовый код любым доступным способом (например, в сообщении электронной почты).
6. После получения одноразового кода пользователь должен сделать следующее:

   a. Чтобы открыть окно с полем для ввода одноразового кода, выполните одно из следующих действий:

   - Нажмите кнопку "Назад" более 3 раз.
   - Нажмите кнопку "Главный экран" более 3 раз, если снят флажок **Запретить кнопку "Главный экран"** в разделе **Ограничения** карточки **Режим киоска**.
   - Нажмите и удерживайте изображение щита на главном экране Kaspersky Endpoint Security для Android.

   b. Введите одноразовый код.

Режим киоска будет выключен на мобильном устройстве пользователя.

Чтобы снова включить режим киоска после выключения его по одноразовому коду, вам необходимо настроить параметры режима киоска и синхронизировать мобильное устройство пользователя с Kaspersky Security Center. Затем пользователь должен подтвердить включение режима киоска в сообщении, которое появится на устройстве.

## Добавление дополнительных приложений

Помимо настройки устройства для работы с одним или несколькими приложениями, вы можете добавить дополнительные приложения, которые разрешено использовать основному приложению. Дополнительные приложения позволяют приложениям, добавленным в режиме киоска, выполнять все свои функции. Например, пользователь может просмотреть документ или получить доступ к сайту, который открыт из главного приложения. По умолчанию дополнительные приложения скрыты на устройстве и пользователь не может запустить их вручную. Дополнительные приложения не требуются для запуска режима киоска.

*Чтобы добавить дополнительные приложения:*

1. В разделе **Доверенные приложения** установите флажок **Разрешить переход в доверенные приложения**.
2. Чтобы указать доверенное приложение, выполните одно из следующих действий:
   - Нажмите **Добавить из Контроля приложений** и выберите приложение из списка ранее добавленных в параметрах политики **Контроль приложений**.

     Будут доступны только приложения, для которых выбрано действие **Установить** или **Рекомендовать к установке**, а также приложения из списка **Разрешенные приложения**.

   - Нажмите **Добавить по имени пакета** и укажите 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 главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Приложения и файлы**.
     2. Выберите **Android** → **Приложения**.

        В открывшемся списке приложений отображаются идентификаторы приложений в столбце **Имя пакета**.

3. Нажмите **ОК**.
4. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Дополнительные приложения добавлены.

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

## Подключение к NDES/SCEP-серверу

Эти параметры применяются к корпоративным устройствам.

Вы можете подключиться к NDES/SCEP-серверу, чтобы получить сертификат от центра сертификации (CA) с помощью простого протокола регистрации сертификатов (SCEP). Для этого нужно добавить подключение к центру сертификации и профиль сертификата.

*Чтобы добавить подключение к центру сертификации и профиль сертификата:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **SCEP и NDES** нажмите **Параметры**.

   Откроется окно **SCEP и NDES**.
5. Включите параметры с помощью переключателя **SCEP и NDES**.

   Откроется окно **Добавить подключение к центру сертификации**.
6. Добавьте подключение к центру сертификации:

   a. В поле **Имя подключения** введите имя подключения к центру сертификации.

   b. В раскрывающемся списке **Тип протокола** выберите версию протокола.

   c. В поле **Веб-адрес сервера** введите адрес сервера NDES или SCEP.

   > Формат URL сервера NDES: `http://<ИмяСервера>/certsrv/mscep/mscep.dll`.

   d. В раскрывающемся списке **Тип контрольной фразы** выберите один из следующих вариантов, чтобы настроить запрос аутентификации:

   - **Не задан**

     > Запрос на ответ выключен. Никаких данных для аутентификации не требуется.

   - **Статический**

     > Запрос на ответ включен. Требуется ввести фразу для аутентификации в поле **Статическая контрольная фраза**.

   e. Если вы выбрали вариант **Статический**, в поле **Статическая контрольная фраза** введите фразу для аутентификации.

   f. Нажмите **Добавить**.

   Будет добавлено подключение к центру сертификации. Вы можете добавить несколько подключений к центрам сертификации.
7. Выберите вкладку **Профиль сертификата** и нажмите **Добавить**.

   Откроется окно **Добавить профиль**.

8. Добавьте профиль сертификата:

   a. В разделе **Общие параметры** в поле **Имя профиля** введите уникальное имя профиля сертификата.

   b. В раскрывающемся списке **Центр сертификации (CA)** выберите центр сертификации, который вы добавили на вкладке **Центр сертификации**.

   c. В поле **Имя субъекта** укажите субъект сертификата. *Имя субъекта* – уникальный идентификатор, который содержит информацию о сертификации, например общее имя, организацию, организационную единицу и код страны. Вы можете ввести значение или выбрать макрос, нажав кнопку +.

   d. Если вы хотите добавить альтернативное имя субъекта сертификата, нажмите **Добавить альтернативное имя субъекта** и настройте следующие параметры:

      1. В раскрывающемся списке **Тип альтернативного имени субъекта** выберите тип альтернативного имени субъекта.

      2. В поле **Альтернативное имя субъекта (SAN)** введите альтернативное имя. Вы можете ввести значение или выбрать макрос, нажав кнопку +.

      Вы можете добавить несколько альтернативных имен субъекта.

   e. В разделе **Ключ** в раскрывающемся списке **Размер ключа (бит)** выберите длину закрытого ключа сертификата.

   f. В раскрывающемся списке **Тип закрытого ключа** выберите тип закрытого ключа сертификата:

   g. Если вы хотите, чтобы сертификат автоматически перевыпускался до истечения срока его действия, в разделе **Сертификат** установите флажок **Обновлять сертификат автоматически**. По умолчанию флажок снят.

   h. Если вы установили флажок **Обновлять сертификат автоматически**, введите количество дней до даты истечения срока действия сертификата в поле **Обновить, когда осталось (дней)**.

   i. Нажмите **Добавить**.

   Будет добавлен профиль сертификата. Вы можете добавить несколько профилей сертификатов.

9. Нажмите **OK**.

10. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

Добавленные подключения к центрам сертификации и профили сертификатов можно изменять или удалять с помощью кнопок **Изменить** или **Удалить** в верхней части списка.

При удалении подключения к центру сертификации также удаляются все профили сертификатов, которые используют это подключение.

## Включение проверки подлинности на основе сертификатов устройств

*Чтобы включить проверку подлинности на основе сертификатов устройства:*

1. Откройте командную строку на устройстве, на котором установлен Сервер администрирования.
2. Перейдите в каталог, содержащий утилиту klscflag.

   По умолчанию утилита находится в каталоге `/opt/kaspersky/ksc64/sbin`.

3. Выполните следующую команду под учетной записью с привилегиями root, чтобы настроить проверку подлинности на основе сертификатов устройств на Сервере администрирования:
   ```
   ./klscflag -fset -pv ".core/.independent" -s KLLIM -n
   LP_MobileMustUseTwoWayAuthOnPort13292 -t d -v 1
   ```
4. Перезапустите службу Сервера администрирования.

После запуска службы Сервера администрирования проверка подлинности на основе сертификатов устройства с использованием общего сертификата станет обязательной.

При первом подключении устройства к Серверу администрирования наличие сертификата не обязательно.

По умолчанию проверка подлинности на основе сертификатов устройств выключена.

## Создание пакета мобильного приложения для Android-устройств

*Чтобы создать пакет мобильного приложения:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Приложения и файлы**.
2. Нажмите **Android**.
3. Нажмите **Приложения**, а затем нажмите **Добавить**.

   Откроется окно **Добавить приложение**.
4. Укажите название приложения в поле **Название приложения**. Это название будет использоваться для идентификации приложения в параметрах политики.
5. Нажмите **Выбрать** и выберите APK-файл на компьютере.
6. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Созданный пакет приложения отобразится в списке приложений на вкладке **Приложения**.

Если вы выберете APK-файл большого размера, загрузка приложения может занять некоторое время. Не закрывайте раздел **Приложения и файлы**, пока приложение не будет загружено.

В разделе **Приложения и файлы** вы также можете добавить приложения для iOS.

## Отправка файлов на Android-устройства

Эта функциональность доступна с Kaspersky Security Center Linux 15.2 или выше.

Kaspersky Security Center Web Console позволяет отправлять файлы в любом формате на Android-устройства во всех режимах работы.

Отправка файлов доступна при наличии лицензии с поддержкой расширенной функциональности Kaspersky Secure Mobility Management. Подробная информация о лицензиях приведена в разделе О лицензии.

Перед тем, как отправлять файлы на устройство, нужно добавить их на Сервер администрирования. Вы можете добавить файлы в разделе **Приложения и файлы**, а затем выбрать, какие файлы вы хотите отправить на устройства, в параметрах политики **Отправка файлов**.

Размер каждого файла не может превышать 1,5 ГБ.

Для отправки файлов приложению Kaspersky Endpoint Security для Android должно быть предоставлено разрешение на доступ ко всем файлам на устройствах с Android 11 или выше или разрешение "Память" на устройствах с Android 10 или ниже.

На устройствах с корпоративным контейнером вы можете копировать в личное пространство пользователя файлы, отправленные в корпоративный контейнер.

### Добавление и управление файлами

*Чтобы добавить файлы на Сервер администрирования:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Приложения и файлы**.
2. Выберите **Android** → **Файлы**.

   Откроется список файлов.
3. Нажмите **Добавить**.

   Откроется окно **Добавить файл**.
4. Нажмите **Выбрать** и выберите файл, который хотите добавить.

5. При необходимости в поле **Описание** можно указать дополнительную информацию о файле.

6. Нажмите **Добавить**.

   Файл будет добавлен на Сервер администрирования.

Вы можете удалять файлы и скачивать их на свой компьютер с помощью соответствующих кнопок в верхней части списка.

> При удалении файла в разделе **Приложения и файлы** он удаляется с Сервера администрирования, но остается на устройствах. Чтобы удалить файл с устройств, удалите его в параметрах политики **Отправка файлов**.

Вы можете просмотреть информацию о любом файле в списке, нажав на его имя.

## Отправка файлов на устройства

*Чтобы отправить файлы на устройства:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Конфигурация устройств**.

4. На карточке **Отправка файлов** нажмите **Параметры**.

   Откроется окно **Отправка файлов**.

5. Включите параметры с помощью переключателя **Отправка файлов**.

6. Нажмите **Добавить**.

   Откроется окно **Добавить файл**.

7. В раскрывающемся списке **Имя файла** выберите файл, который вы добавили в разделе **Приложения и файлы**.

8. В раскрывающемся списке **Корневая папка** выполните одно из следующих действий:

   - Выберите стандартную корневую папку на устройствах.
   - Выберите **Указать папку вручную**, чтобы вручную указать папку в поле **Папка**.

9. В поле **Папка** выполните одно из следующих действий:

   - Если вы выбрали стандартную корневую папку, укажите оставшуюся часть пути до папки, в которую будет отправлен файл.
   - Если вы выбрали **Указать папку вручную**, укажите полный путь до папки, в которую будет отправлен файл.

Для указания пути вы можете использовать буквы, цифры, символы подчеркивания (_) и дефисы (-). В качестве разделителя должна использоваться косая черта (/).

Если указанной папки нет на устройствах, Kaspersky Endpoint Security для Android создает ее автоматически.

10. Если вы хотите отправить на устройства несколько файлов, нажмите **Добавить файл** и повторите шаги 7-9.

11. Нажмите **Добавить**.

    Новый файл отобразится в списке.

12. Нажмите **OK**.

13. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Файлы будут отправлены на устройства после очередной синхронизации устройства с Kaspersky Security Center. Из-за технических ограничений отправка больших файлов на устройства может занять некоторое время.

Вы можете удалять файлы с устройств с помощью соответствующей кнопки в верхней части списка.

При удалении файла в параметрах политики **Отправка файлов** он удаляется с устройств, но остается на Сервере администрирования.

## Просмотр информации об Android-устройстве

*Чтобы просмотреть информацию об Android-устройстве:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.

   Откроется список управляемых мобильных устройств.

2. Чтобы отфильтровать Android-устройства, щелкните заголовок столбца **ОС** и выберите **Android**.

   Отобразится список Android-устройств.

   В зависимости от используемой базы данных при поиске может учитываться регистр.

3. Выберите мобильное устройство, информацию о котором вы хотите посмотреть.

   Откроется окно свойств Android-устройства.

В окне свойств мобильного устройства отобразится информация о подключенном Android-устройстве.

IMEI отображается только для устройств под управлением Android 5–9, корпоративных устройств под управлением Android 10 или выше и устройств с корпоративным контейнером под управлением Android 10–11.

Если на устройствах установлена устаревшая версия Kaspersky Endpoint Security для Android (10.52.1.3 и ранее), для значения **Режим работы** установлено значение **Неизвестно**.

### Отключение Android-устройства от управления

Чтобы отключить Android-устройство от управления, пользователь должен удалить Kaspersky Endpoint Security для Android с мобильного устройства. После удаления пользователем Kaspersky Endpoint Security для Android администратор может удалить мобильное устройство из списка управляемых устройств в Web Console.

Если приложение Kaspersky Endpoint Security для Android не удалено с мобильного устройства, то после синхронизации с Сервером администрирования мобильное устройство снова появится в списке управляемых устройств.

*Чтобы удалить Android-устройство из списка управляемых устройств:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Мобильные → Устройства**.

   Откроется список управляемых мобильных устройств.

2. Чтобы отфильтровать Android-устройства, щелкните заголовок столбца **ОС** и выберите **Android**.

   Отобразится список Android-устройств.

3. Выберите мобильное устройство, которое нужно отключить.

4. Нажмите **Удалить**.

В результате мобильное устройство будет удалено из списка управляемых устройств.

## Управление iOS MDM-устройствами

В этом разделе описаны дополнительные возможности управления iOS MDM-устройствами в Kaspersky Security Center Web Console.

### Подписание управляющих профилей сертификатом

Эта функциональность доступна с Kaspersky Security Center Linux 15.2 или выше.

Вы можете подписать управляющие профили сертификатом, полученным от доверенного центра сертификации.

Сертификат необязателен для корректной работы управляющего профиля. Если управляющий профиль не подписан сертификатом, то при установке управляющего профиля отобразится предупреждение, и пользователям будет предложено подтвердить, что они доверяют организации, приславшей сертификат.

*Чтобы подписывать управляющие профили сертификатом:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Серверы iOS MDM**.

   Откроется список Серверов iOS MDM.

2. Нажмите **Сертификат для подписи**.

   Откроется окно **Сертификат для подписи**.

3. В поле **Формат сертификата** укажите открытый или закрытый тип сертификата:

   - Если выбрано значение **PKCS #12**, укажите файл сертификата и пароль.
   - Если выбрано значение **X.509**:

     a. Укажите пароль закрытого ключа.

     b. Укажите файл открытого ключа.

     c. Укажите пароль закрытого ключа.

4. Нажмите **Сохранить**.

Управляющие профили, которые вы будете создавать, теперь будут подписываться указанным сертификатом.

## Добавление конфигурационного профиля

Чтобы создать конфигурационный профиль, вы можете использовать приложение Apple Configurator 2, которое доступно на сайте Apple. Apple Configurator 2 работает только на устройствах на базе macOS. Если у вас нет таких устройств, вы можете использовать iPhone Configuration Utility. Однако Apple больше не поддерживает iPhone Configuration Utility.

*Чтобы добавить конфигурационный профиль на Сервер iOS MDM:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Серверы iOS MDM**. В открывшемся списке Серверов iOS MDM выберите Сервер iOS MDM, параметры которого вы хотите настроить.

2. В окне параметров Сервера iOS MDM выберите **Параметры приложения**.

3. Выберите вкладку **Конфигурационные профили**.

4. Чтобы добавить новый конфигурационный профиль, нажмите **Добавить**.

5. В открывшемся окне выберите конфигурационный профиль, который вы хотите добавить.

   Длина имени конфигурационного профиля не должна превышать 100 символов. Более длинное имя отобразится лишь частично.

Новый конфигурационный профиль отобразится в списке конфигурационных профилей.

Вы можете установить профиль, который вы создали, на iOS MDM-устройства.

## Установка конфигурационного профиля на устройство

Вы можете установить конфигурационный профиль на iOS MDM-устройство в окне **Отправить команду** или на вкладке **Конфигурационные профили** в окне свойств устройства.

В окне **Отправить команду** вы можете установить конфигурационные профили на несколько устройств одновременно.

*Чтобы установить конфигурационный профиль в окне Отправить команду:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.
2. В открывшемся списке устройств выберите устройства, на которые вы хотите установить конфигурационные профили.
3. Нажмите **Отправить команду**.
4. В открывшемся окне **Отправить команду** в поле **Команда** выберите команду **Установить конфигурационный профиль**.
5. В разделе **Конфигурационные профили** выберите конфигурационные профили, которые вы хотите установить на устройства.
6. Нажмите **Отправить**.

Команда будет отправлена на выбранные вами устройства.

*Чтобы установить конфигурационный профиль в окне свойств устройства:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.
2. В открывшемся списке устройств нажмите на имя устройства, на которое вы хотите установить конфигурационные профили.

   Откроется окно свойств устройства.
3. Выберите вкладку **Конфигурационные профили**.

4. В верхней части списка конфигурационных профилей нажмите **Установить**.

5. В открывшемся окне выберите конфигурационные профили, которые вы хотите установить на устройство, и нажмите **Установить**.

Команда будет отправлена на устройство.

Установка профилей может занять несколько минут. Команда выполняется только когда устройство подключено к интернету. Чтобы проверить, был ли установлен профиль, нажмите **Обновить список**.

## Удаление конфигурационного профиля с устройства

Вы можете удалить конфигурационный профиль с iOS MDM-устройства в окне **Отправить команду** или на вкладке **Конфигурационные профили** в окне свойств устройства.

В окне **Отправить команду** вы можете удалить конфигурационные профили с нескольких устройств одновременно.

*Чтобы удалить конфигурационный профиль в окне Отправить команду:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.

2. В открывшемся списке устройств выберите устройства, с которых вы хотите удалить конфигурационные профили.

3. Нажмите **Отправить команду**.

4. В открывшемся окне **Отправить команду** в поле **Команда** выберите команду **Удалить конфигурационный профиль**.

5. В разделе **Конфигурационные профили** выберите профили, которые вы хотите удалить с устройств.

6. Нажмите **Отправить**.

Команда будет отправлена на выбранные вами устройства.

Профиль может отображаться в списке конфигурационных профилей, установленных на устройстве, в течение нескольких минут после его удаления.

*Чтобы удалить конфигурационный профиль в окне свойств устройства:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.

2. В открывшемся списке устройств нажмите на имя устройства, с которого вы хотите удалить конфигурационные профили.

Откроется окно свойств устройства.

3. Выберите вкладку **Конфигурационные профили**.

4. В списке конфигурационных профилей выберите профили, которые вы хотите удалить с устройства, и нажмите **Удалить**.

Команда будет отправлена на устройство.

Удаление профилей может занять несколько минут. Команда выполняется только когда устройство подключено к интернету. Чтобы проверить, был ли удален профиль, нажмите **Обновить список**.

## Настройка управляемых приложений

Перед установкой приложения на iOS MDM-устройстве, нужно добавить приложение на Сервер администрирования. Приложение считается управляемым, если оно установлено на устройство с помощью Kaspersky Mobile Devices Protection and Management. Таким приложением можно управлять удаленно с помощью Kaspersky Mobile Devices Protection and Management.

*Чтобы добавить управляемое приложение на Сервер iOS MDM:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Мобильные → Приложения и файлы**.

2. Нажмите **iOS**, а затем нажмите **Добавить**.

   Откроется окно **Добавить приложение**.

3. Укажите название приложения в поле **Название приложения**. Это название будет использоваться для идентификации приложения в параметрах политики.

4. В поле **Способ установки** выберите один из следующих способов добавления приложения:

   - **Инсталляционный пакет**

   - **Ссылка на файл манифеста**

     Файл манифеста – файл в формате PLIST, который нужен для установки приложения на iOS-устройство. Эти файлы – словари, которые содержат параметры установки приложения (например, расположение инсталляционного пакета). Когда вы используете файл манифеста для добавления приложения, вам нужно заполнить эти параметры вручную. Когда вы добавляете приложение из App Store или с помощью файла в формате IPA, файл манифеста создается автоматически.

     Чтобы получить файл манифеста для приложения, мы рекомендуем сначала добавить приложение на Сервер iOS MDM с помощью файла IPA. В этом случае Сервер iOS MDM автоматически генерирует файл манифеста, который вы затем сможете скачать и изменить.

   - **App Store**

5. Выполните одно из следующих действий:

Используйте только легитимные и доверенные источники. Настраивая параметры в этом разделе, вы несете полную ответственность за потенциальные риски и последствия, связанные с использованием ненадежных источников.

- Если вы выбрали **Инсталляционный пакет**, нажмите **Выбрать** и загрузите файл в формате IPA с компьютера.
- Если вы выбрали **Ссылка на файл манифеста**, укажите ссылку на файл манифеста, который можно использовать для загрузки приложения.
- Если вы выбрали **App Store**, укажите ссылку или идентификатор приложения, которое нужно добавить из App Store.

6. При необходимости в разделе **Per App VPN** настройте Per App VPN.
7. При необходимости настройте следующие параметры:
   - Установите флажок **Удалять при удалении управляющего профиля**, если хотите, чтобы приложение удалялось с мобильного устройства пользователя вместе с управляющим профилем. По умолчанию флажок установлен.
   - Установите флажок **Запретить резервное копирование данных приложения в iCloud**, если хотите заблокировать резервное копирование данных приложения в iCloud.
8. Если вы хотите добавить пользовательскую конфигурацию приложения, в разделе **Конфигурация приложения** нажмите **Выбрать** и выберите на компьютере конфигурационный файл в формате PLIST.

   Чтобы сгенерировать конфигурационный файл, вы можете использовать генератор конфигураций (например, https://appconfig.jamfresearch.com/generator) или обратиться к официальной документации по настраиваемому приложению.

   **Пример базовой конфигурации 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. 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`. | |

| Ключ конфигурации | Описание | Тип | Значение | Зн<br>ум |
|---|---|---|---|---|
| `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.<br>`Certificates` – проверка подлинности на основе сертификатов. | `Us`<br>`an`<br>`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.<br>`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:<br>`Enabled` - приложение требует, чтобы пользователь вошел в управляемую учетную запись, заданную ключом `IntuneMAMUPN`, для получения данных организации.<br>`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>
```

Вы можете использовать макросы в соответствующих полях конфигурационного файла для замены значений. **Доступные макросы**

Макросы, которые можно использовать в конфигурационных файлах

| Макрос | Описание |
|---|---|
| %full_name% | Полное имя пользователя |
| %email% | Основной адрес электронной почты пользователя |
| %email1% | Первый резервный адрес электронной почты пользователя |
| %email2% | Второй резервный адрес электронной почты пользователя |
| %mobile_phone% | Номер мобильного телефона пользователя |
| %phone_number% | Основной номер телефона пользователя |
| %phone_number1% | Первый резервный номер телефона пользователя |
| %phone_number2% | Второй резервный номер телефона пользователя |
| %short_name% | Имя пользователя |
| %domain_name% | Имя домена пользователя |
| %job_title% | Должность пользователя |
| %department% | Название отдела |
| %company% | Название компании |

9. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Созданное приложение отобразится в таблице приложений на вкладке **iOS**.

Если вы выбрали IPA-файл большого размера, загрузка приложения может занять некоторое время. Не закрывайте раздел **Приложения и файлы**, пока приложение не будет загружено.

Вы можете просматривать и редактировать свойства приложений, выбрав приложение в списке, или удалить приложение с помощью кнопки **Удалить**.

## Установка приложения на мобильное устройство

*Чтобы установить приложение на мобильное устройство:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.
2. В открывшемся списке устройств выберите устройства, на которые вы хотите установить приложения.
3. Нажмите **Отправить команду**.
4. В открывшемся окне **Отправить команду** в поле **Команда** выберите команду **Установить приложение**.
5. В поле **Приложения** выберите приложения, которые вы хотите установить на устройства.
6. Нажмите **Отправить**.

Команда будет отправлена на выбранные вами устройства.

## Обновление приложения, установленного на устройстве

Вы можете обновить приложение на iOS MDM-устройстве в окне **Отправить команду** или на вкладке **Приложения** в окне свойств устройства.

В окне **Отправить команду** вы можете обновить приложения на нескольких устройствах одновременно.

*Чтобы обновить приложение на iOS MDM-устройстве в окне Отправить команду:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.
2. В открывшемся списке устройств выберите устройства, на которых вы хотите обновить приложения.
3. Нажмите **Отправить команду**.
4. В открывшемся окне **Отправить команду** в поле **Команда** выберите команду **Обновить приложение**.
5. В разделе **Приложения** выберите приложения, которые вы хотите обновить на устройствах.
6. Нажмите **Отправить**.

Команда будет отправлена на выбранные вами устройства.

*Чтобы обновить приложение на iOS MDM-устройстве в окне свойств устройства:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.
2. В открывшемся списке устройств нажмите на имя устройства, на которых вы хотите обновить приложения.

   Откроется окно свойств устройства.
3. Выберите вкладку **Приложения**.
4. В верхней части списка приложений нажмите **Обновить**.
5. В открывшемся окне выберите приложения, которые вы хотите обновить на устройствах, и нажмите **Обновить**.

Команда будет отправлена на устройство.

> Обновление приложений может занять несколько минут. Команда выполняется только когда устройство подключено к интернету. Чтобы проверить, было ли обновлено приложение, нажмите **Обновить список**.

## Удаление приложения с устройства

Вы можете удалить приложение с iOS MDM-устройства в окне **Отправить команду** или на вкладке **Приложения** в окне свойств устройства.

> В окне **Отправить команду** вы можете удалить приложения с нескольких устройств одновременно.

*Чтобы удалить приложение с iOS MDM-устройства в окне Отправить команду:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.
2. В открывшемся списке устройств выберите устройства, с которых вы хотите удалить приложения.
3. Нажмите **Отправить команду**.
4. В открывшемся окне **Отправить команду** в поле **Команда** выберите команду **Удалить приложение**.
5. В разделе **Приложения** выберите приложения, которые вы хотите удалить с устройств.
6. Нажмите **Отправить**.

Команда будет отправлена на выбранные вами устройства.

*Чтобы удалить приложение с iOS MDM-устройства в окне свойств устройства:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.
2. В открывшемся списке устройств нажмите на имя устройства, с которого вы хотите удалить приложения.

   Откроется окно свойств устройства.
3. Выберите вкладку **Приложения**.
4. В списке приложений выберите приложения, которые вы хотите удалить с устройства, и нажмите **Удалить**.

Команда будет отправлена на устройство.

Удаление приложений может занять несколько минут. Команда выполняется только когда устройство подключено к интернету. Чтобы проверить, было ли удалено приложение, нажмите **Обновить список**.

## Настройка роуминга на iOS MDM-устройстве

*Чтобы настроить роуминг:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.
2. В открывшемся списке устройств выберите устройства, для которых вы хотите настроить параметры роуминга.
3. Нажмите **Отправить команду**.
4. В открывшемся окне **Отправить команду** в поле **Команда** выберите команду **Изменить параметры роуминга**.
5. В разделе **Действие** выполните одно из следующих действий:
   - Если вы хотите включить роуминг данных, выберите **Включить роуминг данных**.
   - Если вы хотите выключить роуминг данных, выберите **Выключить роуминг данных**.
6. Нажмите **Отправить**.

Команда будет отправлена на выбранные вами устройства.

## Просмотр информации об iOS MDM-устройстве

*Чтобы просмотреть информацию об iOS MDM-устройстве:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.

   Откроется список управляемых мобильных устройств.

2. Чтобы отфильтровать iOS MDM-устройства, нажмите на заголовок столбца **Режим работы** и выберите режим работы iOS MDM-устройства, информацию о котором вы хотите посмотреть.

   Отобразится список iOS MDM-устройств.

   > В зависимости от используемой базы данных при поиске может учитываться регистр.

3. Выберите мобильное устройство, информацию о котором вы хотите посмотреть.

   Откроется окно свойств iOS MDM-устройства.

   > При отображении числовых значений возможна погрешность в несколько сотых.

На вкладке **Общие** отображается информация о подключенном iOS MDM-устройстве.

> Могут не отображаться следующие свойства iOS MDM-устройств под управлением iOS 26 или выше: **IMEI**, **Номер телефона**, **MEID**, **ICCID**, **Имя текущей мобильной сети**, **Имя домашней мобильной сети**, **Версия настроек оператора**, **Голосовой роуминг включен**, **В роуминге**, **Код страны домашней сети**, **Код домашней сети**, **Код страны пребывания**, **Код текущей сети**.

На вкладке **Сертификаты** отображается информация о сертификатах, установленных на выбранном iOS MDM-устройстве.

На вкладке **Приложения** отображается информация о приложениях, установленных на выбранном iOS MDM-устройстве.

На вкладке **Конфигурационные профили** отображается информация о конфигурационных профилях, установленных на выбранном iOS MDM-устройстве.

## Отключение iOS MDM-устройства от управления

Для прекращения управления iOS MDM-устройством можно отключить его от управления в Kaspersky Security Center.

> Мы не рекомендуем отключать устройство от управления путем удаления управляющего профиля, поскольку при повторном подключении такое устройство может работать некорректно. Для прекращения управления iOS MDM-устройством необходимо отключить его от Сервера iOS MDM по инструкции, приведенной в этом разделе.

*Чтобы отключить iOS MDM-устройство от Сервера iOS MDM:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.

   Откроется список управляемых мобильных устройств.

2. Чтобы отфильтровать iOS MDM-устройства, нажмите на заголовок столбца **Режим работы** и выберите режим работы iOS MDM-устройства, которое вы хотите отключить.

   Отобразится список iOS MDM-устройств, работающих в выбранном режиме.

3. Выберите мобильное устройство, которое необходимо отключить.

4. Нажмите **Удалить**.

   iOS MDM-устройство в списке будет отмечено для удаления. В течение минуты мобильное устройство будет удалено из базы данных Сервера iOS MDM, а затем – из списка управляемых устройств.

В результате отключения iOS MDM-устройства от управления с него будут удалены все установленные конфигурационные профили, управляющий профиль и приложения, для которых в настройках Сервера iOS MDM был установлен флажок **Удалять при удалении управляющего профиля**. Политика iOS MDM также будет удалена.

## Настройка режима киоска для iOS MDM-устройств

Эти параметры применяются к устройствам в режиме "Расширенный контроль".

*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.

### Переход в настройки режима киоска

*Чтобы открыть настройки режима киоска:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **iOS** и перейдите в раздел **Ограничения**.

4. На карточке **Режим киоска** нажмите **Параметры**.

   Откроется окно **Режим киоска**.

### Настройка режима киоска

*Чтобы включить режим киоска:*

1. Включите параметры с помощью переключателя **Режим киоска**, чтобы включить режим киоска на устройстве в режиме "Расширенный контроль".

2. В поле **Идентификатор пакета (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 главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Приложения и файлы**.
2. Нажмите **iOS**.

   В открывшемся списке приложений идентификаторы приложений отображаются в столбце **Идентификатор пакета**.

Чтобы выбрать другое приложение, нужно выключить 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 выключен.

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 режим киоска может быть включен, даже если использование выбранного приложения запрещено в параметрах политики.

3. Укажите параметры, которые будут включены на устройстве в режиме киоска в соответствующем разделе. С доступными ограничениями можно ознакомиться ниже в разделе "Параметры режима киоска".
4. Укажите параметры, которые пользователь может менять на устройстве в режиме киоска в соответствующем разделе.
5. Нажмите **ОК**.
6. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

В результате после применения политики будет включен режим киоска. Выбранное приложение принудительно открывается на устройстве в режиме "Расширенный контроль", в то время как использование других приложений запрещено. Выбранное приложение открывается сразу после перезапуска устройства.

Чтобы изменить параметры режима киоска, нужно выключить режим киоска, сохранить изменения в политике, а затем снова включить режим киоска с новыми параметрами.

*Чтобы выключить режим киоска:*

1. Выключите параметры с помощью переключателя **Режим киоска**, чтобы выключить режим киоска на устройстве в режиме "Расширенный контроль".
2. Нажмите **OK**.
3. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

В результате после применения политики режим киоска выключится и на устройстве в режиме "Расширенный контроль" будет разрешено использование всех приложений.

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.

- **Сенсорный ввод (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 Kaspersky Security Center Web Console.

## 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 защиты данных необходимо настроить параметры подключения.

*Чтобы подключить мобильное устройство к сети Wi-Fi:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Конфигурация устройств**.

4. На карточке **Wi-Fi** нажмите **Параметры**.

   Откроется окно **Wi-Fi**.

5. Включите параметры с помощью переключателя **Wi-Fi**.

6. Нажмите **Добавить**.

   Откроется окно **Добавить сеть Wi-Fi**.

7. В поле **Идентификатор сети SSID** укажите имя сети Wi-Fi, содержащей точку доступа (SSID).

8. Установите флажок **Подключаться автоматически**, если хотите, чтобы Android-устройства автоматически подключались к сети Wi-Fi.

9. Установите флажок **Скрытая сеть**, если хотите скрыть сеть Wi-Fi из списка 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.

10. В разделе **Защита** выберите тип безопасности сети Wi-Fi (открытая или защищенная по протоколу WEP, WPA2 PSK, WPA3 PSK, WPA3-Enterprise, WPA3-Enterprise 192-bit или 802.1.x EAP).

    Протокол безопасности 802.1.x EAP поддерживается только в приложении Kaspersky Endpoint Security для Android 10.48.1.1 и выше. Протокол шифрования WEP поддерживается только в Android 9 или ниже. Протоколы шифрования WPA3 PSK, WPA3-Enterprise и WPA3-Enterprise 192-bit поддерживаются только в Android 10 или выше.

11. Если вы выбрали протокол безопасности 802.1.x EAP, WPA3-Enterprise или WPA3-Enterprise 192-bit, укажите следующие параметры защиты сети:

    - **Метод EAP**

      Определяет метод аутентификации в сети EAP (Extensible Authentication Protocol). Возможные значения:

      - **TLS** (по умолчанию)
      - **PEAP**
      - **TTLS**

- **Метод загрузки корневого сертификата**

  Указывает способ загрузки корневого сертификата. Возможные значения:

  - **Из списка корневых сертификатов** – позволяет выбрать любой доступный сертификат из раскрывающегося списка.
  - **Из файла** – позволяет загрузить файл сертификата со своего компьютера.

- **Корневой сертификат**

  Определяет корневой сертификат, который будет использоваться сетью Wi-Fi.

- **Сертификат пользователя**

  Определяет сертификат пользователя, который будет использоваться сетью Wi-Fi, если выбран метод TLS EAP.

  В раскрывающемся списке доступны следующие значения:

  - **Не выбрано** – сертификат пользователя не указан.
  - **Сертификаты пользователя** – VPN-сертификаты, которые были добавлены в разделе **Сертификаты** и установлены 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.
  - **Профили SCEP** – список профилей сертификатов SCEP, настроенных в разделе **SCEP и NDES** и используемых для получения сертификатов.

- **Имя домена**

  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.

- **Тип двухфакторной аутентификации**

  Определяет тип двухфакторной аутентификации. Возможные значения:

  - **Не выбрано** (по умолчанию)
  - **MSCHAP**

- MSCHAPV2
- GTC

- **Идентификатор пользователя**

  Определяет идентификатор пользователя, который будет использоваться для подключения к сети Wi-Fi.

- **Анонимный идентификатор**

  Определяет анонимный идентификатор, который отличается от идентификатора пользователя и используется, если выбран метод аутентификации в сети PEAP или TTLS.

- **Пароль**

  Определяет пароль для доступа к беспроводной сети. Пароль передается с QR-кодом.

  Не отправляйте пароль для конфиденциальной сети Wi-Fi, которая не должна быть общедоступной. Пароль передается в незашифрованном виде вместе с другими данными для настройки устройства.

12. В поле **Пароль** задайте пароль для доступа к сети, если на шаге 9 вы выбрали защищенную сеть.

13. На вкладке **Дополнительные** установите флажок **Использовать прокси-сервер**, если вы хотите использовать прокси-сервер для подключения к сети Wi-Fi.

14. Если вы выбрали вариант **Использовать прокси-сервер**, в полях **Адрес прокси-сервера** и **Порт прокси-сервера** укажите IP-адрес или DNS-имя прокси-сервера и номер порта (если требуется).

    На устройствах с Android 8 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 не используете прокси-сервер для подключения к сети Wi-Fi, вы можете управлять подключением к сети Wi-Fi с помощью политик без ограничений.

15. Добавьте веб-адреса, для соединения с которыми не нужно использовать прокси-сервер, в поле **Не использовать прокси-сервер для указанных адресов**.

    Например, вы можете 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 с Android 8 или выше исключение веб-адресов для прокси-сервера не работает.

16. Нажмите **Добавить**.

    Добавленная сеть Wi-Fi отобразится в списке сетей 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 корпоративных и личных устройствах под управлением Android 9 или ниже после синхронизации с Сервером администрирования пользователь может выбрать предлагаемую беспроводную сеть в списке сохраненных сетей и подключиться к ней без необходимости указывать какие-либо настройки сети.

Вы можете изменять или удалять сети Wi-Fi, входящие в список сетей, с помощью кнопок **Изменить** и **Удалить** в верхней части списка.

17. Нажмите **OK**.

18. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

На устройствах с Android 10 или выше, если пользователь отказывается подключаться к предлагаемой сети Wi-Fi, разрешение приложения на изменение состояния Wi-Fi аннулируется. Пользователю нужно предоставить это разрешение вручную.

## Подключение iOS MDM-устройств к сети Wi-Fi

Для автоматического подключения iOS MDM-устройства к доступной сети Wi-Fi и защиты данных необходимо настроить параметры подключения.

*Чтобы настроить подключение iOS MDM-устройства к сети Wi-Fi:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.

4. На карточке **Wi-Fi** нажмите **Параметры**.

   Откроется окно **Wi-Fi**.

5. Включите параметры с помощью переключателя **Wi-Fi**.

6. Нажмите **Добавить**.

   Откроется окно **Добавить сеть Wi-Fi**.

7. В поле **Идентификатор сети SSID** укажите имя сети Wi-Fi, содержащей точку доступа (SSID).

8. Если вы хотите, чтобы iOS MDM-устройства автоматически подключались к сети Wi-Fi, установите флажок **Подключаться автоматически**.

   Если вы выключите автоматическое подключение к уже добавленной сети Wi-Fi в параметрах политики, вы не сможете снова включить автоматическое подключение к этой сети. Это связано с проблемой, известной Apple.

9. Если вы не хотите, чтобы iOS MDM-устройства подключались к сетям Wi-Fi, требующим предварительной аутентификации (подписным сетям), установите флажок **Выключить обнаружение сетей с авторизацией**.

   Для использования подписной сети необходимо оформить подписку, принять соглашение или внести плату. Подписные сети развернуты, например, в кафе или гостиницах.

10. 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.

11. Если вы хотите, чтобы iOS MDM-устройства использовали статические MAC-адреса при подключении к сети Wi-Fi, установите флажок **Выключить рандомизацию MAC-адресов**.

12. В разделе **Защита** выберите тип безопасности сети Wi-Fi (открытая или защищенная по протоколу WEP, WPA, WPA2 или WPA3).

    На устройствах с iOS 15 или ниже варианты WPA, WPA2 или WPA3 идентичны и позволяют подключаться к любой сети, защищенной по протоколу WPA.

    - **Открытая сеть**. Аутентификация пользователя не требуется.
    - **WEP**. Сеть защищена по протоколу шифрования WEP (Wireless Encryption Protocol).

      Тип защиты WEP доступен на устройствах с iOS 5 и выше.

    - **WPA**. Сеть защищена по протоколу шифрования WPA (Wi-Fi Protected Access) или WPA2.
    - **WPA2**. Сеть защищена по протоколу шифрования WPA2 или WPA3.
    - **WPA3**. Сеть защищена по протоколу шифрования WPA3.
    - **Личная сеть (любой тип)**. Сеть защищена по протоколу шифрования WEP, WPA, WPA2 или WPA3 в зависимости от типа маршрутизатора Wi-Fi. Для аутентификации используется индивидуальный для каждого пользователя ключ шифрования.
    - **WEP (корпоративная сеть)**. Сеть защищена по протоколу шифрования WEP с использованием динамического ключа.
    - **WPA (корпоративная сеть)**. Сеть защищена по протоколу шифрования WPA или WPA2 с использованием протокола 802.1X.
    - **WPA2 (корпоративная сеть)**. Сеть защищена по протоколу шифрования WPA2 или WPA3 с использованием одного ключа шифрования для всех пользователей (802.1X).

- **WPA3 (корпоративная сеть)**. Сеть защищена по протоколу шифрования WPA3 с использованием одного ключа шифрования для всех пользователей (802.1X).

- **Корпоративная сеть (любой тип)**. Сеть защищена по протоколу шифрования WEP, WPA, WPA2 или WPA3 в зависимости от типа маршрутизатора Wi-Fi. Аутентификация выполняется с использованием одного ключа шифрования для всех пользователей.

Если вы выбрали какой-либо из вариантов для корпоративной сети, в разделе **Протокол EAP** вы можете выбрать типы протоколов EAP (Extensible Authentication Protocol) для идентификации пользователя в сети Wi-Fi.

В разделе **Доверенные сертификаты** вы также можете сформировать список доверенных сертификатов для аутентификации пользователя iOS MDM-устройства на доверенных серверах.

13. В разделе **Аутентификация** настройте параметры учетной записи для аутентификации пользователя при подключении iOS MDM-устройства к сети Wi-Fi:

    a. В поле **Имя пользователя** введите имя учетной записи для аутентификации пользователя при подключении к сети Wi-Fi.

    b. 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.

    c. В поле **Пароль** введите пароль учетной записи для аутентификации в сети Wi-Fi.

    d. Если вы хотите, чтобы пользователь вводил пароль вручную при каждом подключении к сети Wi-Fi, установите флажок **Запрашивать пароль при каждом подключении**.

    e. В раскрывающемся списке **Сертификат аутентификации** выберите сертификат для аутентификации пользователя в сети Wi-Fi.

    f. В раскрывающемся списке **Минимальная версия TLS** выберите минимально допустимую версию TLS.

    g. В раскрывающемся списке **Максимальная версия TLS** выберите максимально допустимую версию TLS.

14. При необходимости на вкладке **Дополнительные** настройте параметры подключения к сети Wi-Fi через прокси-сервер:

    a. Установите флажок **Использовать прокси-сервер**.

    b. Настройте подключение к прокси-серверу:

        a. Если вы хотите, чтобы подключение было настроено автоматически:

        - Выберите **Автоматически**.

        - В поле **Веб-адрес PAC-файла** укажите адрес PAC-файла прокси.

        - 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**.

b. Если вы хотите настроить подключение вручную:

- Выберите **Вручную**.
- В полях **Адрес прокси-сервера** и **Порт прокси-сервера** укажите IP-адрес или DNS-имя прокси-сервера и номер порта.
- В поле **Имя пользователя** выберите макрос, который будет использоваться в качестве имени пользователя для подключения к прокси-серверу.
- В поле **Пароль** укажите пароль для подключения к прокси-серверу.

15. Нажмите **Добавить**.

    Новая сеть Wi-Fi отобразится в списке.

16. Нажмите **OK**.

17. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

    В результате после применения политики на iOS MDM-устройстве пользователя будет настроено подключение к сети Wi-Fi. Мобильное устройство пользователя будет автоматически подключаться к доступным сетям Wi-Fi. Безопасность данных при подключении к сети Wi-Fi обеспечивается выбранным методом аутентификации.

# Настройка электронной почты

Этот раздел содержит информацию о настройке почтовых ящиков на мобильных устройствах.

## Настройка почтового ящика на iOS MDM-устройствах

Эти параметры применяются к устройствам в режимах "Расширенный контроль" и "Базовый контроль".

Чтобы пользователь iOS MDM-устройства мог работать с электронной почтой, нужно 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 Почта);
- 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:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **Электронная почта** нажмите **Параметры**.

   Откроется окно **Электронная почта**.
5. Включите параметры с помощью переключателя **Электронная почта**.
6. Нажмите **Добавить**.

   Откроется окно **Добавить учетную запись**.
7. Укажите параметры учетной записи электронной почты:

   - На вкладке **Общие** настройте следующие параметры:

     a. В поле **Имя пользователя** укажите имя пользователя iOS MDM-устройства. Вы можете ввести значение или выбрать макрос, нажав кнопку +.

     b. В поле **Адрес электронной почты** укажите адрес электронной почты пользователя iOS MDM-устройства. Вы можете ввести значение или выбрать макрос, нажав кнопку +.

     c. В поле **Описание учетной записи** введите описание учетной записи электронной почты пользователя.

     d. В поле **Протокол электронной почты** выберите один из следующих протоколов:

     - **POP**
     - **IMAP**

     e. Если вы выбрали **IMAP**, укажите префикс пути IMAP в поле **Префикс пути IMAP**.

     > Префикс пути IMAP нужно указывать прописными буквами (например, GMAIL для Google Mail).

     f. В разделах **Параметры сервера входящей почты** и **Параметры сервера исходящей почты** настройте параметры подключения к серверу:

     - В поле **Адрес сервера** укажите имена узлов или IP-адреса серверов входящей и исходящей почты.
     - В полях **Порт сервера** укажите номера портов серверов входящей и исходящей почты.

Чтобы настроить дополнительные параметры для серверов входящей и исходящей почты, нажмите **Дополнительные параметры** и выполните следующие действия:

- В поле **Имя пользователя** укажите имя учетной записи пользователя для авторизации на серверах входящей и исходящей почты. Вы можете ввести значение или выбрать макрос, нажав кнопку +.
- В поле **Тип аутентификации** выберите тип аутентификации учетной записи электронной почты пользователя на серверах входящей и исходящей почты.
- В поле **Пароль** укажите пароль учетной записи для аутентификации на серверах входящей и исходящей почты, защищенных с помощью выбранного метода аутентификации.
- Если вы хотите использовать транспортный протокол передачи данных SSL, установите флажок **Использовать SSL-соединение**.
- Если вы хотите использовать один и тот же пароль для аутентификации пользователей на серверах входящей и исходящей почты, установите флажок **Использовать один пароль для серверов исходящей и входящей почты**.

- На вкладке **Дополнительные** настройте дополнительные параметры учетной записи электронной почты:

  a. В разделе **Разрешения** при необходимости установите или снимите следующие флажки:

  - **Разрешить синхронизировать последние используемые адреса**

    Перемещение сообщений электронной почты между учетными записями.

    Если флажок установлен, пользователь может перемещать сообщения электронной почты из одной учетной записи в другую.

    Если флажок снят, пользователю запрещено перемещать сообщения электронной почты учетной записи в другую учетную запись.

    По умолчанию флажок установлен.

    Если вы хотите запретить сохранять, перемещать и отправлять вложения из корпоративного почтового ящика, снимите флажок **Разрешить перемещать сообщения между учетными записями (в том числе между рабочими и личными)** и установите флажки Запретить передачу документов из управляемых приложений в неуправляемые и Запретить передачу документов из неуправляемых приложений в управляемые.

  - **Разрешить перемещать сообщения между учетными записями (в том числе между рабочими и личными)**

    Синхронизация используемых адресов электронной почты между учетными записями.

    Если флажок установлен, при создании сообщений пользователь может использовать историю адресов другой учетной записи электронной почты.

    Если флажок снят, используемые адреса электронной почты не синхронизируются. При создании сообщения пользователь iOS MDM-устройства не может использовать историю адресов другой учетной записи электронной почты.

    По умолчанию флажок установлен.

- **Разрешить Mail Drop**

  Использование службы Mail Drop для передачи вложений большого размера.

  Если флажок установлен, пользователь может использовать Mail Drop.

  Если флажок снят, Mail Drop недоступен для пользователя.

  По умолчанию флажок снят.

- **Разрешить использовать только приложение Почта**

  Использование только стандартного почтового клиента iOS для работы с сообщениями.

  Если флажок установлен, пользователь может работать с электронной почтой только в стандартном почтовом клиенте iOS.

  Если флажок снят, пользователь может работать с электронной почтой и в стандартном почтовом клиенте iOS, и в других приложениях.

  По умолчанию флажок снят.

b. В разделах **Подпись** и **Шифрование** настройте параметры подписи и шифрования исходящей почты с использованием протокола S/MIME в приложении Почта.

   S/MIME – это протокол для передачи зашифрованных сообщений с цифровой подписью. S/MIME предоставляет возможности криптографической безопасности, такие как проверка подлинности, обеспечение целостности сообщений и гарантия сохранения авторства (с помощью цифровых подписей). Протокол также помогает повысить уровень конфиденциальности и безопасности данных сообщений электронной почты с помощью шифрования.

   - **Подписывать сообщения**

     Цифровая подпись исходящих сообщений в приложении Почта.

     Если флажок установлен, исходящие сообщения подписываются цифровой подписью с использованием протокола S/MIME. Цифровая подпись подтверждает подлинность отправителя и указывает получателю, что содержимое сообщения не изменилось в процессе передачи. Для подписи сообщений необходимо выбрать сертификат получателя (открытый ключ).

     По умолчанию флажок снят.

   - **Сертификат для подписи исходящих сообщений**

     Сертификат для подписания исходящих сообщений цифровой подписью по протоколу S/MIME. Цифровая подпись гарантирует, что сообщение отправлено пользователем iOS MDM-устройства. Вы можете добавить сертификаты в карточке **Управление сертификатами** или в разделе **Сертификаты** в Web Console.

     Этот раскрывающийся список доступен, только если установлен флажок **Подписывать сообщения**.

   - **Шифровать сообщения по умолчанию**

     Шифрование исходящих сообщений в приложении Почта.

Если флажок установлен, исходящие сообщения по умолчанию шифруются по протоколу S/MIME. Для отправки зашифрованных сообщений необходимо выбрать сертификат получателя (открытый ключ). Если сертификат получателя не установлен, выполнить шифрование сообщений невозможно. Просмотреть зашифрованные сообщения могут только пользователи, на устройстве которых установлен сертификат.

По умолчанию флажок снят.

- **Сертификат для шифрования**

  Сертификат для шифрования исходящих сообщений по протоколу S/MIME. Шифрование сохраняет конфиденциальность сообщений во время передачи и хранения. Вы можете добавить сертификаты в карточке **Управление сертификатами** или в разделе **Сертификаты** в Web Console.

  Этот раскрывающийся список доступен, только если установлен флажок **Шифровать сообщения по умолчанию**.

- **Показывать переключатель для шифрования отдельных сообщений**

  Отображение значка в приложении Почта в поле **Кому** для отправки зашифрованных сообщений.

  Если этот флажок установлен, пользователь мобильного устройства может шифровать отдельные сообщения, щелкнув значок.

  Если флажок снят, значок для шифрования сообщений не отображается. В этом случае флажок **Шифровать сообщения по умолчанию** определяет, будут ли шифроваться исходящие сообщения.

- При необходимости в разделе **Per App VPN** настройте Per App VPN.

8. Нажмите **Сохранить**.

   Новая учетная запись электронной почты отобразится в списке.

   Вы можете изменять или удалять учетные записи электронной почты в списке с помощью кнопок **Изменить** и **Удалить**.

9. Нажмите **ОК**.

10. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

    Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

    В результате после применения политики на мобильное устройство пользователя будут добавлены учетные записи электронной почты из сформированного списка.

    Мы рекомендуем закрыть и открыть приложение "Настройки" на iOS MDM-устройстве после настройки почтового ящика.

## Настройка почтового ящика Exchange на iOS MDM-устройствах

Эти параметры применяются к устройствам в режимах "Расширенный контроль" и "Базовый контроль".

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 Почта);
- 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:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **Exchange ActiveSync** нажмите **Параметры**.

   Откроется окно **Exchange ActiveSync**.
5. Включите параметры с помощью переключателя **Exchange ActiveSync**.
6. Нажмите **Добавить**.

   Откроется окно **Добавить аккаунт Exchange ActiveSync**.
7. Укажите параметры Exchange ActiveSync:
   - На вкладке **Общие** укажите данные пользователя:
     - В поле **Имя учетной записи** введите имя учетной записи для авторизации на сервере Microsoft Exchange. Вы можете ввести значение или выбрать макрос, нажав кнопку +.
     - В поле **Адрес сервера Exchange ActiveSync** введите DNS-имя или IP-адрес сервера Microsoft Exchange.

- Параметры в разделе **Учетные данные пользователя**:
  - В поле **Домен пользователя** введите имя домена пользователя iOS MDM-устройства. Вы можете ввести значение или выбрать макрос, нажав кнопку +.
  - В поле **Имя пользователя** введите имя пользователя iOS MDM-устройства. Вы можете ввести значение или выбрать макрос, нажав кнопку +.

    Если оставить это поле пустым, при применении политики на iOS MDM-устройстве Kaspersky Mobile Devices Protection and Management запросит имя у пользователя.
  - В поле **Адрес электронной почты** введите адрес электронной почты пользователя iOS MDM-устройства. Вы можете ввести значение или выбрать макрос, нажав кнопку +.
- Параметры в разделе **Аутентификация**:
  - В поле **Пароль** введите пароль аккаунта Exchange ActiveSync для авторизации на сервере Microsoft Exchange.
  - В раскрывающемся списке **Сертификат аутентификации** выберите сертификат, используемый для аутентификации пользователя iOS MDM-устройства на сервере Microsoft Exchange. Вы можете добавить сертификаты в карточке **Управление сертификатами** или в разделе **Сертификаты** в Web Console.

- На вкладке **Дополнительные** настройте дополнительные параметры учетной записи Exchange ActiveSync:
  - В разделе **Синхронизация электронной почты** в раскрывающемся списке **Период синхронизации** выберите интервал времени, в течение которого электронная почта будет автоматически синхронизироваться и сохраняться на iOS MDM-устройстве. Чем больше период синхронизации электронной почты, тем больше требуется свободного места в памяти мобильного устройства. Несинхронизированные сообщения недоступны без подключения к интернету. Значение по умолчанию: **1 неделя**.
  - В разделе **Ограничения** при необходимости установите или снимите следующие флажки:
    - **Разрешить перемещать сообщения между учетными записями (в том числе между рабочими и личными)**

      Перемещение сообщений электронной почты между учетными записями.

      Если флажок установлен, пользователь может перемещать сообщения электронной почты из одной учетной записи в другую.

      Если флажок снят, пользователю запрещено перемещать сообщения электронной почты учетной записи в другую учетную запись.

      По умолчанию флажок установлен.

      Если вы хотите запретить сохранять, перемещать и отправлять вложения из корпоративного почтового ящика, снимите флажок **Разрешить перемещать сообщения между учетными записями (в том числе между рабочими и личными)** и установите флажки Запретить передачу документов из управляемых приложений в неуправляемые и Запретить передачу документов из неуправляемых приложений в управляемые.
    - **Разрешить синхронизировать последние используемые адреса**

Синхронизация используемых адресов электронной почты между учетными записями.

Если флажок установлен, при создании сообщений пользователь может использовать историю адресов другой учетной записи электронной почты.

Если флажок снят, используемые адреса электронной почты не синхронизируются. При создании сообщения пользователь iOS MDM-устройства не может использовать историю адресов другой учетной записи электронной почты.

По умолчанию флажок установлен.

- **Разрешить использовать только приложение Почта**

  Использование только стандартного почтового клиента iOS для работы с сообщениями.

  Если флажок установлен, пользователь может работать с электронной почтой только в стандартном почтовом клиенте iOS.

  Если флажок снят, пользователь может работать с электронной почтой и в стандартном почтовом клиенте iOS, и в других приложениях.

  По умолчанию флажок снят.

- **Использовать SSL-соединение**

  Установите этот флажок, чтобы использовать транспортный протокол передачи данных SSL для защиты передачи данных.

  По умолчанию флажок установлен.

- В разделе **Подпись и шифрование** настройте параметры подписи и шифрования исходящей почты с использованием протокола S/MIME в приложении Почта. *S/MIME* – это протокол для передачи зашифрованных сообщений с цифровой подписью. S/MIME предоставляет возможности криптографической безопасности, такие как проверка подлинности, обеспечение целостности сообщений и гарантия сохранения авторства (с помощью цифровых подписей). Протокол также помогает повысить уровень конфиденциальности и безопасности данных сообщений электронной почты с помощью шифрования.

  - **Подписывать сообщения**

    Цифровая подпись исходящих сообщений в приложении Почта.

    Если флажок установлен, исходящие сообщения подписываются цифровой подписью с использованием протокола S/MIME. Цифровая подпись подтверждает подлинность отправителя и указывает получателю, что содержимое сообщения не изменилось в процессе передачи. Для подписи сообщений необходимо выбрать сертификат получателя (открытый ключ).

    По умолчанию флажок снят.

  - **Сертификат для подписи исходящих сообщений**

    Сертификат для подписания исходящих сообщений цифровой подписью по протоколу S/MIME. Цифровая подпись гарантирует, что сообщение отправлено пользователем iOS MDM-устройства. Вы можете добавить сертификаты в карточке **Управление сертификатами** или в разделе **Сертификаты** в Web Console.

Этот раскрывающийся список доступен, только если установлен флажок **Подписывать сообщения**.

- **Шифровать сообщения по умолчанию**

  Шифрование исходящих сообщений в приложении Почта.

  Если флажок установлен, исходящие сообщения по умолчанию шифруются по протоколу S/MIME. Для отправки зашифрованных сообщений необходимо выбрать сертификат получателя (открытый ключ). Если сертификат получателя не установлен, выполнить шифрование сообщений невозможно. Просмотреть зашифрованные сообщения могут только пользователи, на устройстве которых установлен сертификат.

  По умолчанию флажок снят.

- **Сертификат для шифрования**

  Сертификат для шифрования исходящих сообщений по протоколу S/MIME. Шифрование сохраняет конфиденциальность сообщений во время передачи и хранения. Вы можете добавить сертификаты в карточке **Управление сертификатами** или в разделе **Сертификаты** в Web Console.

  Этот раскрывающийся список доступен, только если установлен флажок **Шифровать сообщения по умолчанию**.

- **Показывать переключатель для шифрования отдельных сообщений**

  Отображение значка в приложении Почта в поле **Кому** для отправки зашифрованных сообщений.

  Если этот флажок установлен, пользователь мобильного устройства может шифровать отдельные сообщения, щелкнув значок.

  Если флажок снят, значок для шифрования сообщений не отображается. В этом случае флажок **Шифровать сообщения по умолчанию** определяет, будут ли шифроваться исходящие сообщения.

- При необходимости в разделе **Per App VPN** настройте Per App VPN.

8. Нажмите **Добавить**.

   Новая учетная запись Exchange ActiveSync отобразится в списке.

   Вы можете изменять или удалять учетные записи Exchange ActiveSync с помощью кнопок **Изменить** и **Удалить** в верхней части списка.

9. Нажмите **OK**.

10. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

В результате после применения политики на мобильное устройство пользователя будут добавлены учетные записи Exchange ActiveSync из сформированного списка.

## Настройка почтового ящика Exchange на Android-устройствах

Для работы с корпоративной почтой, контактами и календарем на мобильном устройстве можно настроить параметры почтового ящика Exchange.

Почтовый ящик Exchange можно настроить только для устройств Samsung под управлением Android 9 или ниже.

*Чтобы настроить почтовый ящик Exchange на мобильном устройстве пользователя:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Параметры Samsung Knox**.
4. На карточке **Exchange ActiveSync** нажмите **Параметры**.

   Откроется окно **Exchange ActiveSync**.
5. Включите параметры с помощью переключателя **Exchange ActiveSync**.
6. В поле **Адрес сервера** введите IP-адрес или DNS-имя сервера, на котором размещен почтовый сервер.
7. В поле **Имя домена** введите доменное имя пользователя мобильного устройства в корпоративной сети.
8. В раскрывающемся списке **Период синхронизации** выберите период синхронизации мобильного устройства с сервером Microsoft Exchange.
9. Чтобы использовать транспортный протокол передачи данных SSL, установите флажок **Использовать SSL-соединение**. Протокол SSL использует шифрование и проверку подлинности на основе сертификатов для защиты передачи данных. По умолчанию флажок установлен.
10. Чтобы использовать цифровые сертификаты для защиты передачи данных между мобильным устройством пользователя и сервером Microsoft Exchange, установите флажок **Проверять сертификат сервера**. Будет выполняться проверка, выписан ли сертификат сервера с помощью доверенного корневого сертификата. По умолчанию флажок установлен.
11. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

# Настройка уровней защиты в Kaspersky Security Center

Эти параметры применяются к Android-устройствам.

*Чтобы настроить правила присвоения уровней защиты в Kaspersky Security Center:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Параметры KES для Android**.

4. На карточке **Параметры критичности уровня защиты для устройств** нажмите **Параметры**.

   Откроется окно **Параметры критичности уровня защиты для устройств**.

5. Включите параметры с помощью переключателя **Параметры критичности уровня защиты для устройств**.

6. Выберите уровень защиты **OK**, **Предупреждение** или **Критический** для каждого из следующих условий:

   - **Постоянная защита не работает**

     Раскрывающийся список, в котором можно выбрать уровень защиты мобильного устройства с неработающей постоянной защитой.

     Постоянная защита позволяет обнаруживать угрозы в открываемых файлах, а также проверять новые приложения и останавливать заражение устройств в реальном времени.

     Постоянная защита может не работать по следующим причинам:

     - Пользователь отказался использовать Kaspersky Security Network на мобильном устройстве в настройках Защиты от вредоносного ПО Kaspersky Endpoint Security для Android.
     - Пользователь не предоставил приложению доступ для управления всеми файлами.

     Если постоянная защита не запущена, вы также можете настроить ограничения на работу мобильного устройства в параметрах **Контроль соответствия** политики.

   - **Веб-Защита и Веб-Контроль не работают**

     Раскрывающийся список, в котором можно выбрать уровень защиты мобильного устройства с неработающими Веб-Защитой и Веб-Контролем.

     Веб-Защита позволяет проверять сайты, блокировать вредоносные и фишинговые сайты.

     Веб-Контроль позволяет настраивать доступ пользователей к определенным сайтам и категориям сайтов.

     Веб-Защита и Веб-Контроль могут не работать по следующим причинам:

     - Пользователь выключил Веб-Защиту на мобильном устройстве в настройках Kaspersky Endpoint Security для Android.
     - Пользователь не включил Kaspersky Endpoint Security для Android в качестве службы Специальных возможностей.
     - Разрешение Игнорировать оптимизацию батареи не предоставлено.
     - Положение о Веб-Фильтре не принято.

     Если Веб-Защита и Веб-Контроль не запущены, вы также можете настроить ограничения на работу мобильного устройства в параметрах **Контроль соответствия** политики.

- **Контроль приложений не работает**

  Раскрывающийся список, в котором можно выбрать уровень защиты мобильного устройства с неработающим Контролем приложений.

  Контроль приложений позволяет блокировать на мобильных устройствах запуск приложений, которые не удовлетворяют требованиям корпоративной безопасности.

  Контроль приложений может не работать, если на устройствах под управлением Android 5 или выше пользователь не включил приложение в качестве службы Специальных возможностей.

  Если Контроль приложений не запущен, вы также можете настроить ограничения на работу мобильного устройства в параметрах **Контроль соответствия** политики.

- **Блокирование устройства недоступно**

  Раскрывающийся список, в котором можно выбрать уровень защиты мобильного устройства, которое невозможно заблокировать.

  Блокирование устройства может выполняться в следующих случаях:

  - После получения команды Анти-Вора.
  - После смены SIM-карты или включения устройства без нее.
  - При попытке удаления Kaspersky Endpoint Security для Android, если включена защита от удаления приложения.

  Блокирование устройства может быть недоступно по следующим причинам:

  - Пользователь не установил приложение в качестве администратора устройства.
  - На устройствах под управлением Android 7 или выше пользователь не включил приложение в качестве службы Специальных возможностей.
  - На устройствах под управлением Android 7 или выше пользователь не разрешил приложению наложение поверх других окон.

- **Определение геолокации на устройстве недоступно**

  Раскрывающийся список, в котором можно выбрать уровень защиты мобильного устройства, определить местоположение которого невозможно.

  Определение местоположения выполняется после получения команды **Определить местоположение**.

  Определение местоположения может быть недоступно по следующим причинам:

  - Пользователь не предоставил приложению разрешение на определение местоположения.
  - Пользователь выключил модуль GPS в настройках устройства.

- **Версии Положения о Kaspersky Security Network не совпадают**

  Раскрывающийся список, в котором можно выбрать уровень защиты мобильного устройства, если версия Положения о Kaspersky Security Network, принятая администратором, не совпадает с версией, принятой пользователем устройства. Статистическая информация, не указанная в принятой пользователем версии Положения, не отправляется в Kaspersky Security Network.

- **Версии Положения о маркетинге не совпадают**

  Раскрывающийся список, в котором можно выбрать уровень защиты мобильного устройства, если версия Положения об обработке данных в маркетинговых целях, принятая администратором, не совпадает с версией, принятой пользователем устройства. Передача данных в сторонние сервисы не осуществляется.

  Список сторонних сервисов см. в Положении об обработке данных в маркетинговых целях.

7. Нажмите **OK**.
8. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

Подробная информация о значениях по умолчанию, причинах и условиях присвоения уровней защиты приведена в разделе Уровни защиты мобильных устройств.

# Управление настройками приложения

В этом разделе приведены инструкции по управлению параметрами и редактированию конфигураций приложений, установленных на устройствах ваших пользователей.

## Управление настройками Google Chrome

Эти параметры применяются к корпоративным устройствам и устройствам с корпоративным контейнером.

*Чтобы настроить Google Chrome:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Конфигурация приложений**.
4. На карточке **Параметры Google Chrome** нажмите **Параметры**.

   Откроется окно **Параметры Google Chrome**.
5. Включите параметры с помощью переключателя **Параметры Google Chrome**.

   Переключатель на этой карточке не включает и не выключает соответствующую функциональность на устройствах. Включение переключателя позволяет настроить пользовательские параметры. Выключение переключателя позволяет использовать параметры по умолчанию.

6. Задайте необходимые параметры.

7. Нажмите **OK**.

8. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

## Управление настройками контента

На вкладке **Контент** вы можете настроить следующие параметры:

- В разделе **Файлы cookie**:
  - **Режим по умолчанию**

    Настройки файлов cookie по умолчанию.

    Доступные варианты:
    - **Разрешить всем сайтам сохранять локальные данные** (по умолчанию)
    - **Запретить всем сайтам сохранять локальные данные**
    - **Задать настройки для отдельных сайтов**
    - **Не задавать параметры cookie**

  - **Исключения**

    Исключения для сайтов, на которых запрещено или разрешено сохранять локальные данные.

    Дополнительную информацию о шаблонах URL-адресов см. в документации Chrome Enterprise.

  - **Сайты**

    Сайты, на которых запрещено или разрешено сохранять локальные данные.

    Дополнительную информацию о шаблонах URL-адресов см. в документации Chrome Enterprise.

- В разделе **JavaScript**:
  - **Режим по умолчанию**

    Настройки JavaScript по умолчанию.

    Доступные варианты:
    - **Разрешить всем сайтам запускать JavaScript** (по умолчанию)
    - **Запретить всем сайтам запускать JavaScript**

- **Исключения**

  Исключения для сайтов, на которых запрещено или разрешено использование JavaScript.

  Дополнительную информацию о шаблонах URL-адресов см. в документации Chrome Enterprise.

- В разделе **Всплывающие окна**:

  - **Режим по умолчанию**

    Режим работы по умолчанию для всплывающих окон.

    Доступные варианты:

    - **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.

    Всплывающие окна будут блокироваться на основе базы данных злоупотреблений от Google.

  - **Исключения**

    Исключения для сайтов, на которых запрещено или разрешено отображать всплывающие окна.

- В разделе **Определение местоположения**:

  - **Режим по умолчанию**

    Настройки местоположения по умолчанию.

    Доступные варианты:

    - **Разрешить всем сайтам отслеживать местоположение пользователя**
    - **Запретить всем сайтам отслеживать местоположение пользователя**
    - **Спрашивать, если сайт пытается отследить местоположение пользователя** (по умолчанию)

## Управление настройками прокси

На вкладке **Прокси** вы можете настроить следующие параметры:

- **Режим по умолчанию**

  Настройки прокси для Google Chrome и ARC-приложений.

Доступные варианты:

- **Никогда не использовать прокси**. Запрещает использование прокси, все остальные настройки прокси игнорируются.
- **Определять настройки прокси автоматически**. Определяет настройки прокси автоматически, все остальные опции игнорируются.
- **Использовать PAC-файл**. Использует PAC-файл прокси, указанный в поле **Веб-адрес PAC-файла**.
- **Использовать фиксированные прокси-серверы**. Использует данные, указанные в поле **Веб-адрес прокси-сервера** и списке **Исключения**.
- **Использовать системные настройки прокси**. Использует системные настройки прокси. Этот параметр выбран по умолчанию.

- **Веб-адрес PAC-файла**

  URL PAC-файла прокси.

- **Веб-адрес прокси-сервера**

  URL прокси-сервера.

- **Исключения**

  Список хостов, для которых прокси будет игнорироваться.

## Управление настройками поиска

На вкладке **Поиск** вы можете настроить следующие параметры:

- В разделе **Быстрый поиск**:
  - **Разрешить быстрый поиск**

    Установка или снятие флажка определяет, разрешено ли пользователю устройства использовать быстрый поиск, включать и выключать его.

    По умолчанию флажок установлен.

- В разделе **Поисковая система**:
  - **Режим работы**

    Этот параметр позволяет определить, будет ли настроена поисковая система, которая будет использоваться на устройствах пользователей.

    Если выбран вариант **Включить поисковую систему по умолчанию**, вы можете указать параметры поисковой системы.

- **Название поисковой системы**

  Имя поисковой системы по умолчанию.

  Примеры:

  ```
  Google
  Yandex
  Mail.ru
  Bing
  ```

- **Веб-адрес поиска**

  URL поисковой системы, используемой во время поиска по умолчанию.

  Примеры:

  ```
  https://www.google.com/search?q={searchTerms}
  https://ya.ru/search/?text={searchTerms}
  https://go.mail.ru/search?q={searchTerms}
  https://www.bing.com/search?q={searchTerms}
  ```

- **Веб-адрес запроса подсказок**

  URL поисковой системы, предоставляющей поисковые подсказки.

  Примеры:

  ```
  https://www.google.com/complete/search?client=chrome&hl=ru&q={searchTerms}
  https://suggest.yandex.net/suggest-ff.cgi?part={searchTerms}
  https://go.mail.ru/suggest?q={searchTerms}
  https://api.bing.com/osjson.aspx?query={searchTerms}
  ```

- **Веб-адрес значка**

  Используйте только легитимные и доверенные источники. Настраивая параметры в этом поле, вы несете полную ответственность за потенциальные риски и последствия, связанные с использованием ненадежных источников.

  URL значка поисковой системы по умолчанию.

  Примеры:

  ```
  https://www.google.com/favicon.ico
  https://ya.ru/favicon.ico
  https://go.mail.ru/favicon.ico
  https://www.bing.com/sa/simg/bing_p_rr_teal_min.ico
  ```

- **Кодировки**

  Кодировки символов, поддерживаемые поисковой системой. Поддерживаемые кодировки:

  - UTF-8
  - UTF-16
  - GB2312
  - ISO-8859-1

- **Дополнительные веб-адреса**

  Список дополнительных URL для извлечения поисковых запросов из поисковой системы.

- **Веб-адрес поиска изображений**

  URL поисковой системы, используемой для поиска изображений.

- **Веб-адрес страницы быстрого доступа**

  URL поисковой системы, используемый для открытия страницы быстрого доступа.

  Примеры:

  ```
  https://www.google.com
  https://ya.ru
  https://go.mail.ru
  https://www.bing.com
  ```

- **Параметры для запросов POST к веб-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
  ```

- **Параметры для запросов POST к веб-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
  ```

- **Параметры для запросов POST к веб-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}
  ```

## Управление параметрами безопасности

На вкладке **Безопасность** вы можете настроить следующие параметры:

- В разделе **Безопасный просмотр и Безопасный поиск Google**:

  - **Режим работы Безопасного просмотра**

    Уровень защиты Безопасного просмотра Google.

    Доступные варианты:

    - **Защита отключена**. Полностью отключает Безопасный просмотр Google.
    - **Стандартная защита.** Безопасный просмотр Google будет всегда включен в режиме стандартной защиты. Этот параметр выбран по умолчанию.
    - **Улучшенная защита**. Безопасный просмотр Google будет всегда включен в режиме улучшенной защиты, но данные о работе пользователя устройства в интернете будут отправляться в Google.

  - **Принудительно использовать Безопасный поиск**

    Установка или снятие флажка определяет, будет ли применяться Безопасный поиск Google для запросов в Google Поиске.

    По умолчанию флажок снят.

  - **Отключить переход со страницы предупреждения Безопасного просмотра**

    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.

    По умолчанию флажок снят.

- В разделе **Блокировка сайтов**:

  - **Заблокировать доступ к этим сайтам**

    Список запрещенных URL. Также вы можете задавать шаблоны URL, например: `[*.]example.com`.

- **Исключения**

  Список URL, которые являются исключениями из списка, указанного в пункте **Заблокировать доступ к этим сайтам**. Также вы можете задавать шаблоны URL, например: `[*.]example.com`.

- В разделе **Пароли и автозаполнение**:

  - **Включить сохранение паролей**

    Установка или снятие флажка определяет, будет ли Google Chrome запоминать пароли, вводимые пользователем, и предлагать их при следующем входе.

    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 адресов не используется, а также не сохраняется дополнительная информация об адресах, вводимых пользователем во время работы в интернете.

    По умолчанию флажок установлен.

  - **Включить автозаполнение данных банковских карт**

    Настройки автозаполнения данных банковских карт.

    Если флажок установлен, пользователю устройства разрешено управлять предложениями автозаполнения для банковских карт через интерфейс.

    Если флажок снят, автозаполнение данных банковских карт не используется, а также не сохраняется дополнительная информация о банковских картах, которую пользователь вводит во время работы в интернете.

    По умолчанию флажок установлен.

- В разделе **Сеть**:

  - **Минимальная версия TLS**

    Минимально допустимая версия TLS.

    Доступные варианты:

    - **TLS 1.0** (по умолчанию)
    - **TLS 1.1**
    - **TLS 1.2**

- **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.

  По умолчанию флажок установлен.

## Управление дополнительными параметрами

На вкладке **Дополнительные параметры** вы можете настроить следующие параметры:

- В разделе **Закладки**:

  - **Управляемые закладки**

    Список закладок, управляемых администратором. Список представляет собой словарь 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:

    Без ключа "children":

    ```
    "Managed bookmarks":
    [
      {
        //Изменяет имя папки по умолчанию
        "toplevel_name": "Kaspersky Secure Mobility Management"
      },
      {
        //Добавляет закладку в папку с управляемыми закладками
        "name": "Help",
        "url": "https://support.kaspersky.com/help/KSMM/7.0/ru-RU/254248.htm"
      },
      {
        "name": "Official website",
        "url": "https://www.kaspersky.ru/enterprise-security/mobile"
      }
    ]
    ```

    С ключом "children":

    ```
    "Managed bookmarks":
    [
      {
        "toplevel_name": "Company bookmarks"
      },
      {
    ```

```
    "name": "Homepage",
    "url": "mydomain.com"
  },
  {
    "children": [
      {
        "name": "HR",
        "url": "mydomain.com/hr"
      },
      {
        "name": "Submit a ticket",
        "url": "mydomain.com/it-support"
      }
    ],
    "name": "Internal URLs"
  },
  {
    "name": "Android resources",
    "url": "https://developer.android.com/"
  }
]
```

- **Включить возможность изменения закладок**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства добавлять, удалять или изменять закладки.

  По умолчанию флажок установлен.

- В разделе **История и режим инкогнито**:

  - **Доступность режима инкогнито**

    Указывает, может ли пользователь устройства включать режим инкогнито в Google Chrome.

    Доступные варианты:

    - **Режим инкогнито доступен** (по умолчанию)
    - **Режим инкогнито выключен**

  - **Отключить сохранение истории браузера**

    Установка или снятие флажка определяет, сохраняется ли история браузера и выполняется ли синхронизация вкладок.

    По умолчанию флажок снят.

- В разделе **Другое**:

  - **Безопасный режим для YouTube**

    Минимальный требуемый уровень Безопасного режима для YouTube.

Доступные варианты:

- **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 безопасный режим на YouTube.
- **Включить обязательное использование Строгого безопасного режима**. Включает постоянное использование Строгого безопасного режима на YouTube.

- **Режим работы Google Переводчика**

  Функция перевода.

  Доступные варианты:

  - **Всегда предлагать перевод**. Отображает уведомление о переводе и опцию перевода в верхней части экрана.
  - **Никогда не предлагать перевод**. Выключает все встроенные функции перевода.
  - **Запрашивать действие у пользователя**. Позволяет пользователю решить, использовать ли функции перевода. Этот параметр выбран по умолчанию.

- **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".

  По умолчанию флажок снят.

- **Включить печать**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства производить печать в Google Chrome.

  По умолчанию флажок установлен.

- **Включить поисковые подсказки**

  Установка или снятие флажка определяет, включены ли поисковые подсказки в адресной строке Google Chrome.

  По умолчанию флажок установлен.

## Управление Exchange ActiveSync для Gmail

Эти параметры применяются к корпоративным устройствам и устройствам с корпоративным контейнером.

Параметры **Exchange ActiveSync** позволяют управлять Exchange ActiveSync для приложения Gmail.

*Чтобы настроить параметры Exchange ActiveSync:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Конфигурация приложений**.
4. На карточке **Exchange ActiveSync** нажмите **Параметры**.

   Откроется окно **Exchange ActiveSync**.
5. Включите параметры с помощью переключателя **Exchange ActiveSync**.
6. Укажите параметры Exchange ActiveSync:
   - На вкладке **Общие** укажите следующие параметры:
     - **Адрес сервера Exchange ActiveSync**

       URL почтового сервера Exchange ActiveSync. Перед URL не обязательно использовать `http://` или `https://`.
     - Параметры в разделе **Учетные данные пользователя**:
       - **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 макрос, нажав кнопку +.
       - **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 макрос, нажав кнопку +.
       - **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 макрос, нажав кнопку +.
     - Параметры в разделе **Аутентификация**:
       - **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.

- **Сертификат аутентификации**

Сертификат для аутентификации, используемый для проверки идентификатора пользователя, упрощения аутентификации пользователя и обеспечения безопасности данных.

В раскрывающемся списке доступны следующие значения:

- **Не выбрано**. Сертификат для аутентификации не указан.
- **Сертификаты пользователя**. Список почтовых сертификатов, настроенных в разделе **Управление активами → Мобильные → Сертификаты**.
- **Профили SCEP**. Список профилей сертификатов SCEP, настроенных на карточке **SCEP и NDES** в разделе **Конфигурация устройств** политики и используемых для получения сертификатов.

- На вкладке **Дополнительные** укажите следующие параметры:
  - Параметры в разделе **Синхронизация электронной почты**:
    - **Период синхронизации**

Интервал времени по умолчанию для синхронизации элементов почты между серверами Exchange ActiveSync и Gmail. Возможные значения:

- 1 день
- 3 дня
- 1 неделя (по умолчанию)
- 2 недели
- 1 месяц

  - Параметры в разделе **Ограничения**:
    - **Использовать SSL-соединение**

Установка или снятие флажка определяет, будет ли для связи с портом сервера, указанным в поле **Адрес сервера Exchange ActiveSync**, использоваться протокол SSL.

По умолчанию флажок установлен.

- **Отключить проверку SSL-сертификатов**

  Установка или снятие флажка определяет, будут ли осуществляться проверки SSL-сертификатов, используемых на серверах Exchange ActiveSync. Проверка полезна, если сертификаты являются самозаверенными.

  По умолчанию флажок снят.

- **Разрешить неуправляемые учетные записи**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства добавлять другие учетные записи в приложение Gmail.

  По умолчанию флажок установлен.

- Параметры в разделе **Подпись**:

  - **Подпись для электронной почты по умолчанию**

    Подпись для электронной почты по умолчанию, которая автоматически добавляется в конце электронных писем.

7. Нажмите **ОК**.
8. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

## Настройка прочих приложений

Эти параметры применяются к корпоративным устройствам и устройствам с корпоративным контейнером.

Параметры **Настройка прочих приложений** позволяют настраивать установленные приложения, поддерживающие конфигурации.

*Чтобы добавить конфигурации приложений:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Конфигурация приложений**.
4. На карточке **Настройка прочих приложений** нажмите **Параметры**.

   Откроется окно **Настройка прочих приложений**.
5. Включите параметры с помощью переключателя **Настройка прочих приложений**.

6. Нажмите **Добавить**.

   Откроется окно **Добавить конфигурацию приложения**.

7. В выпадающем списке **Способ добавления конфигурации** выберите способ добавления конфигурации:

   - **Пакет приложения, загруженный администратором**

     При добавлении конфигурации приложения с помощью APK-файла необходимо выбрать файл, сохраненный на вашем компьютере.

     После этого можно просмотреть описание каждого параметра конфигурации. Описания являются частью файла конфигурации.

     Ключи конфигурации, загруженные из пакета приложения, не могут быть удалены. Если вы хотите добавить новый параметр в загруженную конфигурацию, нажмите **Добавить параметр**.

   - **Инсталляционный пакет 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 каждого параметра конфигурации. Описания являются частью файла конфигурации.

     Параметры конфигураций, добавленных с помощью инсталляционных пакетов, недоступны для удаления.

   - **Вручную**

     Если выбран этот метод, нажмите **Добавить параметр**, чтобы добавить новый параметр в конфигурацию.

8. В разделе **Данные конфигурации** настройте следующие параметры:

   - **Название приложения**

     Название приложения, к которому будет применена конфигурация.

     При импорте конфигурации из APK-файла или инсталляционного пакета значение подставляется автоматически.

   - **Имя пакета**

     Имя 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 главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Приложения и файлы**.
2. Выберите **Android** → **Приложения**.

   В открывшемся списке приложений отображаются идентификаторы приложений в столбце **Имя пакета**.

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.

**Пример настройки основных параметров для приложения Microsoft Outlook.**

Конфигурация приложения Microsoft Outlook

| Ключ конфигурации | Описание | Тип | Значение | Зн<br>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 макрос, нажав кнопку +. 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 макрос, нажав кнопку +. Например, `user@companyname.com`. | |

| Ключ конфигурации | Описание | Тип | Значение | Зн<br>ум |
|---|---|---|---|---|
| `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.<br>`Certificates` – проверка подлинности на основе сертификатов. | `Us`<br>`an`<br>`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 макрос, нажав кнопку +. 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.<br>`BasicAuth` – запрашивает пароль у пользователя устройства. Укажите BasicAuth в качестве типа учетной записи для локальной версии Exchange. | `Ba` |

9. Нажмите **Добавить параметр**, чтобы добавить блок параметров конфигурации приложения. Вы можете добавить несколько блоков параметров.

   Для каждого блока параметров конфигурации укажите следующие параметры:

   - **Ключ**

     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.
     - **Bool**. Значения True или False.

- **Integer**. Числовой тип данных для чисел без дробной части.
- **Bundle**. Набор полей любого типа, кроме Bundle и BundleArray.
- **BundleArray**. Множество наборов полей типа Bundle.

- **Значение**

  Необязательный параметр, значение зависит от типа параметра.

Для некоторых типов настроек можно настроить дополнительные параметры. Например:

- Вы можете добавить макросы для типа **String**.
- Вы можете добавить поле в **Bundle**.
- Вы можете добавить Bundle в **BundleArray**.

Также можно изменить параметр, который будет добавлен в BundleArray, нажав **Настроить Bundle** и настроив параметры.

Для получения информации о правилах настройки конфигурации обратитесь к официальной документации для настраиваемого приложения.

10. Нажмите **Добавить**.

    Конфигурация появится в списке конфигураций приложений.

    Вы можете изменять или удалять конфигурации приложений с помощью кнопок **Изменить** и **Удалить** в верхней части списка.

11. Нажмите **ОК**.
12. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Конфигурация приложения применена.

Некоторые приложения могут не уведомлять Kaspersky Endpoint Security для Android о применении конфигурации приложения.

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.

# Управление разрешениями приложений

Эти параметры применяются к корпоративным устройствам и устройствам с корпоративным контейнером.

Параметры **Управление разрешениями приложений** позволяют настраивать правила выдачи разрешений, запрашиваемых у пользователя устройства в процессе работы приложения.

*Чтобы добавить разрешения для приложения:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Конфигурация приложений**.
4. На карточке **Управление разрешениями приложений** нажмите **Параметры**.

   Откроется окно **Управление разрешениями приложений**.
5. Включите параметры с помощью переключателя **Управление разрешениями приложений**.
6. Нажмите **Добавить**.

   Откроется окно **Добавить приложение с правилами выдачи разрешений**.
7. В разделе **Способ добавления конфигурации** выберите способ добавления конфигурации с правилами выдачи разрешений:

   - **Пакет приложения, загруженный администратором**

     При добавлении конфигурации путем загрузки пакета приложения вам необходимо выбрать APK-файл, сохраненный на вашем компьютере.

     После этого можно просмотреть список дополнительных разрешений и выбрать действие, выполняемое для каждого разрешения.

   - **Инсталляционный пакет 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.

   - **Вручную**

     При добавлении конфигурации вручную необходимо нажать кнопку **Добавить правило**, чтобы выбрать разрешение и соответствующее действие из раскрывающихся списков.

8. В разделе **Данные приложения** настройте следующие параметры:

- **Название приложения**

  Название приложения, для которого нужно настроить разрешения.

  При импорте конфигурации из APK-файла или инсталляционного пакета значение подставляется автоматически.

- **Имя пакета**

  Имя 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 главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Приложения и файлы**.
  2. Выберите **Android** → **Приложения**.

     В открывшемся списке приложений отображаются идентификаторы приложений в столбце **Имя пакета**.

  При импорте конфигурации из APK-файла или инсталляционного пакета значение подставляется автоматически.

- **Комментарий**

  Необязательный комментарий.

9. Нажмите кнопку **Добавить правило**, чтобы добавить и настроить новое правило. 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

  Отклонение этого разрешения запретит приложению сканировать данные устройства в фоновом режиме, но пользователь по-прежнему сможет выбирать файлы для обмена.
- 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:

- **Разрешить настройку пользователям**

  Пользователь решает, выдавать ли разрешение приложению.

  Этот параметр выбран по умолчанию.

- **Выдавать разрешения автоматически**

  Разрешение для приложения выдается без участия пользователя.

  На устройствах с корпоративным контейнером на базе Android 12 или выше следующие разрешения не могут быть выданы автоматически, но могут быть автоматически отклонены. При выборе этого параметра следующие разрешения будут запрашиваться у пользователя:

  - разрешения на использование местоположения;
  - разрешения на доступ к камере;
  - разрешения на запись звука;
  - разрешение на распознавание физической активности;
  - разрешения на отслеживание входящих SMS и MMS сообщений;
  - разрешения на доступ к данным биометрических датчиков.

- **Отклонять разрешения автоматически**

  Запрос на разрешение для приложения отклоняется без участия пользователя.

Для каждого разрешения можно сохранить только одно правило.

Если пользователь ранее выдал или отклонил разрешение, то действия **Выдавать разрешения автоматически** и **Отклонять разрешения автоматически** сделают недоступной последующую настройку разрешений на устройстве. Чтобы пользователь смог поменять настройки, выберите в политике действие **Разрешить настройку пользователям** и синхронизируйте устройство, либо попросите пользователя переустановить приложение.

10. Нажмите **Добавить**.

    Конфигурация появится в списке **Приложения с настроенными правилами выдачи разрешений**.

    Вы можете изменять или удалять конфигурации с помощью кнопок **Изменить** и **Удалить** в верхней части списка.

11. Нажмите **ОК**.

12. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Конфигурация с правилами выдачи разрешений применена. Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Kaspersky Security Center.

Правила выдачи разрешений, настроенные для определенных приложений, имеют приоритет над общей политикой выдачи разрешений. Например, если вы сначала выберете параметр **Отклонять разрешения автоматически** в карточке Корпоративный контейнер на устройствах, а затем выберете параметр **Выдавать разрешения автоматически** для определенного приложения в карточке **Управление разрешениями приложений**, разрешение для этого приложения будет выдано автоматически.

## Создание отчета об установленных мобильных приложениях

**Отчет об установленных мобильных приложениях** позволяет получить подробную информацию о приложениях, установленных на Android-устройствах пользователей.

Чтобы отчет отображал информацию, нужно установить флажок **Отправлять данные об установленных приложениях** в карточке **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 главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Контроль безопасности**.
4. На карточке **Контроль приложений** нажмите **Параметры**.

   Откроется окно **Контроль приложений**.
5. В разделе **Отчет об установленных приложениях** установите флажок **Отправлять данные об установленных приложениях**.
6. Если вы хотите получать данные о системных приложениях, установите флажок **Отправлять данные о встроенных приложениях**.
7. Если вы хотите получать данные о служебных приложениях, которые не имеют интерфейса и не могут быть открыты пользователем, установите флажок **Отправлять данные о служебных приложениях**.
8. Нажмите **ОК**.
9. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.
10. Нажмите на имя политики и выберите **Настройка событий**.
11. Перейдите в раздел **Информационное сообщение**.
12. Щелкните событие **Установлено или удалено приложение (список установленных приложений)**, чтобы открыть его свойства.

13. В окне свойств события включите опцию **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.

14. Нажмите **OK**.

15. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Отправка данных разрешена.

*Чтобы настроить отчет по установленным мобильным приложениям:*

1. В главном окне Kaspersky Security Center Web Console выберите **Мониторинг → Отчеты**.

2. Нажмите на шаблон отчета **Отчет об установленных мобильных приложениях**, чтобы открыть его свойства.

3. В открывшемся окне нажмите **Изменить**.

4. Отредактируйте свойства шаблона отчета:

   - На вкладке **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 **Поля** > **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. Некоторые отчеты содержат чрезмерное количество записей. В таких случаях просмотр и анализ всех записей может оказаться слишком трудоемким. Кроме того, при формировании такого отчета на вашем устройстве может не хватить памяти. Следовательно, вы не сможете просмотреть отчет.

       По умолчанию параметр включен. По умолчанию указано значение 1000.

     - **Группа**

       Набор клиентских устройств, для которых создается отчет.

- **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.

- **Интервал 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 актуальных 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 на этом Сервере администрирования.

  Если Сервер администрирования не может получить данные подчиненного Сервера администрирования во время создания 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 выключен.

- **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 выключен.

- На вкладке **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.

5. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Измененный шаблон отчета появится в списке шаблонов отчетов.

*Чтобы создать и просмотреть отчет об установленных мобильных приложениях:*

1. В главном окне Kaspersky Security Center Web Console выберите **Мониторинг → Отчеты**.

2. Нажмите на отчет с типом **Отчет об установленных мобильных приложениях**.

Будет сформирован и отображен отчет по выбранному шаблону.

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 Web Console позволяет добавлять корневые сертификаты для установки в хранилище доверенных сертификатов на Android-устройствах.

Эти сертификаты устанавливаются на пользовательских устройствах следующим образом:

- На корпоративных устройствах 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:

  - Если корпоративный контейнер не был создан, пользователю устройства предлагается установить каждый сертификат вручную в личном пространстве, следуя инструкциям в уведомлении.

  - Если корпоративный контейнер был создан, сертификаты автоматически установятся в контейнер. Если флажок **Дублировать установку корневых сертификатов в личное пространство пользователя** установлен в настройках корпоративного контейнера, можно также установить сертификаты в личном пространстве. 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:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **Корневые сертификаты** нажмите **Параметры**.

   Откроется окно **Корневые сертификаты**.
5. Включите параметры с помощью переключателя **Корневые сертификаты**.
6. Нажмите **Добавить**.

   Откроется проводник.
7. Выберите файл сертификата (файл в формате CER, PEM, KEY или CRT) и нажмите **Открыть**.

   Размер файла сертификата не должен превышать 10 МБ.

   Сертификат появится в списке корневых сертификатов.
8. Нажмите **ОК**.
9. Нажмите **Сохранить**, 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 для Android 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 безопасности в приложении, нажмите на уведомление.

- **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 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:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Параметры KES для Android**.

4. На карточке **Настройка уведомлений** нажмите **Параметры**.

   Откроется окно **Настройка уведомлений**.

5. Включите параметры с помощью переключателя **Настройка уведомлений**.

6. Если вы хотите скрыть все уведомления и всплывающие сообщения, в разделе **Уведомления от Kaspersky Endpoint Security** установите флажок **Не отображать уведомления, пока Kaspersky Endpoint Security работает в фоновом режиме**.

   Kaspersky Endpoint Security для Android будет показывать только уведомление о состоянии защиты. В уведомлении отображается статус защиты устройства (например, ) и количество проблем.

   Уведомления в приложении (например, когда пользователь обновляет базы вредоносного ПО вручную) по-прежнему будут отображаться.

   Мы рекомендуем включить уведомления и всплывающие сообщения. Если уведомления и всплывающие сообщения выключены, когда приложение работает в фоновом режиме, приложение не уведомляет пользователей об угрозах в реальном времени. В этом случае пользователи мобильных устройств не увидят статус защиты устройства, пока не откроют приложение.

7. В разделе **Уведомления в приложении Kaspersky Endpoint Security** выберите проблемы Kaspersky Endpoint Security для Android, уведомления о которых требуется отображать на мобильном устройстве пользователя.

   Отображение уведомлений о некоторых проблемах Kaspersky Endpoint Security для Android является обязательным. Уведомления об этих проблемах всегда отображаются на устройстве (например, об окончании срока действия лицензии).

8. Нажмите **OK**.

9. Нажмите **Сохранить**, 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, которые вы выключили.

## Выбор загрузчика для Android-устройств

Если вы используете Веб-сервер с самоподписанным сертификатом, а не сертификатом, подписанным центром сертификации (ЦА), стандартный загрузчик Android позволяет вам скачивать файлы, приложения и инсталляционные пакеты Kaspersky Endpoint Security для Android с Веб-сервера на устройства только через HTTP.

Чтобы безопасно скачивать на устройства файлы с Веб-сервера с самоподписанным сертификатом, вы можете использовать встроенный загрузчик Kaspersky Endpoint Security для Android, который всегда скачивает файлы через HTTPS.

Встроенный загрузчик Kaspersky Endpoint Security для Android включен по умолчанию.

*Чтобы изменить загрузчик, используемый Kaspersky Endpoint Security для Android:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Параметры KES для Android**.

4. Выполните одно из следующих действий:

   - Чтобы использовать загрузчик Kaspersky Endpoint Security для Android, включите переключатель **Встроенный загрузчик**.
   - Чтобы использовать стандартный загрузчик Android, выключите переключатель **Встроенный загрузчик**.

Будет настроен загрузчик, используемый на устройствах.

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

# 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 поколения и выше), устройства AirPort Express, колонки, телевизоры и радиоприемники с поддержкой AirPlay.

Автоматическое подключение к устройствам AirPlay доступно для устройств, работающих в режиме "Базовый контроль" и "Расширенный контроль".

*Чтобы настроить подключение iOS MDM-устройства к устройствам AirPlay:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **AirPlay** нажмите **Параметры**.

   Откроется окно **AirPlay**.
5. Включите параметры с помощью переключателя **AirPlay**.
6. В разделе **Пароли** нажмите **Добавить пароль**.
7. В поле **Устройство** введите имя устройства AirPlay, подключенного к беспроводной сети.
8. В поле **Пароль** введите пароль от устройства AirPlay.
9. Если вы хотите, чтобы iOS MDM-устройство подключалось только к определенным устройствам AirPlay, сформируйте список разрешенных устройств в разделе **Разрешенные устройства**. Для этого нажмите **Добавить устройство** и укажите MAC-адреса устройств AirPlay.

   Чтобы подключить iOS MDM-устройства с iOS 18 или выше к любым устройствам AirPlay, необходимо указать **Имя устройства**.

   Чтобы подключить iOS MDM-устройства с iOS 17 или ниже к любым устройствам AirPlay, необходимо указать и адрес Wi-Fi, и адрес Ethernet для каждого устройства.

   К устройствам AirPlay, не входящим в список разрешенных устройств, доступ запрещен. Если список разрешенных устройств пуст, Kaspersky Mobile Devices Protection and Management разрешает доступ ко всем устройствам AirPlay.

10. Нажмите **OK**.

11. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

В результате после применения политики мобильное устройство пользователя будет автоматически подключаться к устройствам AirPlay для передачи медиаконтента.

## Подключение iOS MDM-устройств к AirPrint

Для печати документов с iOS MDM-устройства беспроводным способом с помощью AirPrint настройте автоматическое подключение к принтерам AirPrint. Мобильное устройство и принтер должны быть подключены к одной беспроводной сети. На принтере AirPrint нужно настроить общий доступ для всех пользователей.

*Чтобы настроить подключение iOS MDM-устройства к принтеру AirPrint:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.

4. На карточке **AirPrint** нажмите **Параметры**.

   Откроется окно **AirPrint**.

5. Включите параметры с помощью переключателя **AirPrint**.

6. Нажмите **Добавить**.

   Откроется окно **Добавить принтер**.

7. В поле **IP-адрес или FQDN** введите IP-адрес или полное доменное имя (FQDN) принтера AirPrint.

8. В поле **Порт** введите порт прослушивания назначения AirPrint.

9. 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.

10. Если вы хотите защитить подключение к принтеру AirPrint с помощью протокола TLS, установите флажок **Использовать TLS**.

11. Нажмите **Добавить**.

    Добавленный принтер AirPrint отобразится в списке.

12. Нажмите **OK**.

13. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

В результате после применения политики пользователь мобильного устройства сможет печатать документы на принтере AirPrint по беспроводной связи.

# Настройка точки доступа (APN)

В этом разделе приведены инструкции по подключению мобильного устройства к услугам сотовой связи в мобильной сети.

## Настройка APN на Android-устройствах (только Samsung)

APN можно настроить только для устройств Samsung.

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) на мобильном устройстве пользователя:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Параметры Samsung Knox**.

4. На карточке **Параметры APN** нажмите **Параметры**.

   Откроется окно **Параметры APN**.

5. Включите параметры с помощью переключателя **Параметры APN**.

   Переключатель на этой карточке не включает и не выключает соответствующую функциональность на устройствах. Включение переключателя позволяет настроить пользовательские параметры. Выключение переключателя позволяет использовать параметры по умолчанию.

6. Укажите следующие параметры точки доступа для подключения пользователя к услуге передачи данных:

   - В раскрывающемся списке **Тип APN** выберите тип точки доступа для передачи данных в мобильной сети GPRS/3G/4G:

     - **Интернет**. Подключение мобильного устройства пользователя к интернету.

     - **MMS**. Обмен мультимедийными сообщениями MMS.

     - **Интернет и MMS**. Подключение к интернету и обмен мультимедийными сообщениями. Это значение установлено по умолчанию.

   - В поле **Имя APN** укажите имя точки доступа.

   - В поле **MCC** укажите мобильный код страны (MCC).

   - В поле **MNC** укажите мобильный код сети (MNC).

7. Если в качестве типа точки доступа вы выбрали **MMS** или **Интернет и MMS**, укажите следующие дополнительные параметры для MMS в разделе **Сервер MMS**:

   - В поле **Имя сервера MMS** укажите полное доменное имя сервера мобильного оператора для обмена MMS (например, `mms.mobile.com`).

   - В поле **Адрес прокси-сервера MMS** введите имя сети или IP-адрес прокси-сервера.

   - В поле **Порт прокси-сервера MMS** укажите номер порта сервера мобильного оператора для обмена MMS.

8. В разделе **Аутентификация** укажите параметры аутентификации:

   - В раскрывающемся списке **Тип аутентификации** выберите тип аутентификации пользователя мобильного устройства на сервере мобильного оператора для доступа к сети. По умолчанию аутентификация пользователя не требуется. Доступны следующие типы:

     - **Нет**. Для доступа к мобильной сети аутентификация пользователя не требуется.

     - **PAP** (протокол аутентификации по паролю). Протокол аутентификации, использующий пароли в виде простого незашифрованного текста.

     - **CHAP** (Challenge Handshake Authentication Protocol). Протокол аутентификации типа "запрос-ответ", использующий стандартную схему хеширования MD5 для шифрования ответа.

     - **Совместно**. Совместное использование протоколов CHAP и PAP.

   - В поле **Имя пользователя** укажите имя пользователя для авторизации в мобильной сети.

   - В поле **Пароль** укажите пароль для авторизации пользователя в мобильной сети.

9. В разделе **Сеть** укажите следующие параметры сети:

   - В поле **Имя сети** введите название сети.

   - В поле **Адрес сервера** укажите сетевое имя сервера оператора мобильной связи, через который осуществляется доступ к услугам передачи данных.

10. В разделе **Прокси-сервер** укажите следующие параметры прокси-сервера:

    - Установите флажок **Использовать прокси-сервер**, чтобы разрешить использование прокси-сервера. По умолчанию флажок снят.
    - В поле **Адрес прокси-сервера** укажите сетевое имя или IP-адрес прокси-сервера мобильного оператора для доступа к сети. Это поле доступно, только если установлен флажок **Использовать прокси-сервер**.
    - В поле **Порт прокси-сервера** укажите номер порта прокси-сервера мобильного оператора для доступа к сети. Это поле доступно, только если установлен флажок **Использовать прокси-сервер**.

11. Нажмите **ОК**.

12. Нажмите **Сохранить**, 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).

*Чтобы настроить точку доступа на iOS MDM-устройстве пользователя:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.

4. На карточке **Параметры APN** нажмите **Параметры**.

   Откроется окно **Параметры APN**.

5. Включите параметры с помощью переключателя **Параметры APN**.

   Переключатель на этой карточке не включает и не выключает соответствующую функциональность на устройствах. Включение переключателя позволяет настроить пользовательские параметры. Выключение переключателя позволяет использовать параметры по умолчанию.

6. В раскрывающемся списке **Тип APN** выберите тип точки доступа для передачи данных в мобильной сети GPRS/3G/4G:

   - **Встроенная APN**. Настройка 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 сайте Службы поддержки Apple.
   - **APN**. Настройка параметров сотовой связи для передачи данных через оператора мобильной сети вставленной SIM-карты.
   - **Встроенная APN и APN**. Настройка 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 сайте Службы поддержки Apple.

7. Если вы выбрали вариант **APN**, в разделе **APN** нажмите **Добавить**.

   Откроется окно **Добавить APN**.

8. Настройте следующие параметры:

   a. В поле **Имя APN** укажите название точки доступа.

   b. В раскрывающемся списке **Тип аутентификации** выберите тип аутентификации пользователя на сервере мобильного оператора для доступа к сети (интернет и MMS).

   c. В поле **Имя пользователя** укажите имя пользователя для авторизации в мобильной сети.

   d. В поле **Пароль** укажите пароль для авторизации пользователя в мобильной сети.

   e. В поле **Адрес прокси-сервера** введите имя хоста или IP-адрес прокси-сервера.

   f. В поле **Порт прокси-сервера** введите номер порта прокси-сервера.

   g. В раскрывающемся списке **Разрешенный протокол** выберите интернет-протокол.

   h. В раскрывающемся списке **Разрешенный протокол для роуминга** выберите интернет-протокол, который будет использоваться во время международного роуминга.

   i. В раскрывающемся списке **Разрешенный протокол для внутреннего роуминга** выберите интернет-протокол, который будет использоваться во время внутреннего роуминга.

   j. Если вы хотите, чтобы устройства в сетях, поддерживающих только IPv6, могли получать доступ к интернет-службам с поддержкой только IPv4, установите флажок **Использовать технологию 464XLAT**.

   k. Нажмите **OK**.

9. Если вы выбрали вариант **Встроенная APN**, настройте следующие параметры:

   a. В поле **Имя встроенной APN** укажите название точки доступа.

   b. В раскрывающемся списке **Тип аутентификации** выберите тип аутентификации пользователя на сервере мобильного оператора для доступа к сети (интернет и MMS).

   c. В поле **Имя пользователя** укажите имя пользователя для авторизации в мобильной сети.

d. В поле **Пароль** укажите пароль для авторизации пользователя в мобильной сети.

e. В раскрывающемся списке **Разрешенный протокол** выберите интернет-протокол.

10. Нажмите **ОК**.

11. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

В результате после применения политики на мобильном устройстве пользователя будет настроена точка доступа (APN).

# Корпоративный контейнер

Этот раздел содержит информацию о работе с корпоративным контейнером.

## О корпоративных контейнерах

Android Enterprise – платформа для управления мобильной инфраструктурой компании, предоставляющая сотрудникам компании безопасную рабочую среду на мобильных устройствах. Подробная информация о работе с Android Enterprise приведена на сайте технической поддержки Google.

Вы можете создать корпоративный контейнер, использующий рабочий профиль Android, на личном мобильном устройстве пользователя. Корпоративный контейнер – безопасная среда, в которой администратор может управлять приложениями и учетными записями пользователей, не ограничивая использование пользователями их собственных данных. При создании на мобильном устройстве пользователя корпоративного контейнера в него автоматически устанавливаются следующие корпоративные приложения: Google Play, Google Chrome, Загрузки, Kaspersky Endpoint Security для Android и другие. Приложения, установленные в корпоративном контейнере, а также уведомления от этих приложений, отмечены значком портфеля. Для приложения Google Play нужно создать отдельную корпоративную учетную запись Google. Приложения, установленные в корпоративном контейнере, отображаются в общем списке приложений.

## Настройка корпоративного контейнера

*Чтобы настроить параметры корпоративного контейнера:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Корпоративный контейнер**.

4. На карточке **Корпоративный контейнер на устройствах** нажмите **Параметры**.

   Откроется окно **Корпоративный контейнер на устройствах**.

5. Включите параметры с помощью переключателя **Корпоративный контейнер на устройствах**.

6. Укажите параметры корпоративного контейнера:

- На вкладке **Общие** можно настроить параметры передачи данных, контактов и другие.
  - Параметры в разделе **Доступ и передача данных**:
    - **Запретить передачу данных из личных приложений в приложения корпоративного контейнера**

      Ограничение передачи файлов, изображений и прочих данных из личных приложений в приложения корпоративного контейнера.

      Если флажок установлен, личные приложения не могут передавать данные в приложения корпоративного контейнера.

      Если флажок снят, личные приложения могут передавать данные в приложения корпоративного контейнера.

      По умолчанию флажок установлен.

    - **Запретить передачу данных из приложений корпоративного контейнера в личные приложения**

      Ограничение передачи файлов, изображений и прочих данных из приложений корпоративного контейнера в личные приложения.

      Если флажок установлен, приложения корпоративного контейнера не могут передавать данные в личные приложения.

      Если флажок снят, приложения корпоративного контейнера могут передавать данные в личные приложения.

      По умолчанию флажок установлен.

    - **Запретить приложениям корпоративного контейнера доступ к личным файлам**

      Ограничивает доступ приложений корпоративного контейнера к личным файлам.

      Если флажок установлен, у пользователя отсутствует доступ к личным файлам при использовании приложений корпоративного контейнера.

      Если флажок снят, пользователь имеет доступ к личным файлам при использовании приложений корпоративного контейнера. Доступ также должен поддерживаться используемыми приложениями.

      По умолчанию флажок установлен.

    - **Запретить личным приложениям доступ к файлам в корпоративном контейнере**

      Ограничивает доступ личных приложений к файлам в корпоративном контейнере.

      Если флажок установлен, у пользователя отсутствует доступ к файлам в корпоративном контейнере при использовании личных приложений.

      Если флажок снят, пользователь имеет доступ к файлам в корпоративном контейнере при использовании личных приложений. Доступ также должен поддерживаться используемыми приложениями.

      По умолчанию флажок установлен.

- **Запретить использование буфера обмена между личными приложениями и корпоративным контейнером**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства копировать данные через буфер обмена между личными приложениями и корпоративным контейнером.

  По умолчанию флажок установлен.

- **Запретить включать режим отладки по USB**

  Ограничение использования отладки по USB на мобильном устройстве пользователя в корпоративном контейнере. 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 пользователям добавление и удаление учетных записей в корпоративном контейнере**

  Если флажок установлен, пользователю запрещено добавлять и удалять учетные записи в корпоративном контейнере 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 корпоративном контейнере, 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 корпоративного контейнера**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства делать снимки экрана, а также записывать и демонстрировать экран устройства в приложениях корпоративного контейнера. Помимо этого установка или снятие флажка определяет, разрешен ли захват экрана в целях работы искусственного интеллекта.

  По умолчанию флажок установлен.

- Параметры в разделе **Отправка файлов**:

  - **Копировать отправленные файлы в личное пространство пользователя**

    Установка или снятие флажка определяет, будут ли файлы, отправленные на устройство с корпоративным контейнером копироваться в личное пространство пользователя.

    Этот флажок применяется только для файлов, которые еще не были отправлены на устройство. Файлы, которые были отправлены на устройство до того, как был установлен флажок, не копируются в личное пространство пользователя.

По умолчанию флажок снят.

- Параметры в разделе **Контакты**:
  - **Запретить отображение имени контакта из корпоративного контейнера для личных входящих вызовов**

    Установка или снятие флажка определяет, будет ли имя контакта из корпоративного контейнера отображаться для личных входящих вызовов.

    По умолчанию флажок установлен.

  - **Запретить личным приложениям доступ к контактам корпоративного контейнера**

    Установка или снятие флажка определяет, разрешен ли доступ личным приложениям для управления контактами к контактам корпоративного контейнера.

    По умолчанию флажок установлен.

- На вкладке **Приложения** настройте параметры следующим образом:
  - Параметры в разделе **Общие**:
    - **Включить Контроль приложений только в корпоративном контейнере**

      Контроль запуска приложений в корпоративном контейнере на мобильном устройстве пользователя. Вы можете создавать списки разрешенных, запрещенных и рекомендованных приложений, а также разрешенных и запрещенных категорий приложений в карточке **Контроль приложений**.

      Если флажок установлен, в зависимости от параметров Контроля приложений Kaspersky Endpoint Security блокирует или разрешает запуск приложений только в корпоративном контейнере. При этом в личном пространстве пользователя Контроль приложений не работает.

      По умолчанию флажок установлен.

    - **Включить Веб-Защиту и Веб-Контроль только в корпоративном контейнере**

      Ограничение доступа пользователя устройства к сайтам в корпоративном контейнере. Вы можете указать параметры доступа к сайтам в карточке **Веб-Контроль**.

      Если флажок установлен, Веб-Защита и Веб-Контроль запрещают или разрешают доступ к сайтам только в корпоративном контейнере. При этом в личном пространстве пользователя Веб-Защита и Веб-Контроль не работают.

      Если флажок снят, в зависимости от параметров Веб-Защиты и Веб-Контроля Kaspersky Endpoint Security блокирует или разрешает доступ к сайтам в личном пространстве пользователя и в корпоративном контейнере.

      По умолчанию флажок установлен.

    - **Запретить установку приложений из неизвестных источников в корпоративном контейнере**

      Ограничение на установку приложений в корпоративный контейнер 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. Нельзя устанавливать только приложения, запрещенные в карточке **Контроль приложений**.

По умолчанию флажок снят.

- **Запретить удаление приложений из корпоративного контейнера**

  Установка или снятие флажка определяет, запрещено ли пользователю удалять приложения из корпоративного контейнера.

  По умолчанию флажок снят.

- **Запретить показывать уведомления от приложений корпоративного контейнера на заблокированном экране**

  Ограничение отображения содержимого уведомлений от приложений корпоративного контейнера на экране блокировки устройства.

  Если флажок установлен, содержимое уведомлений из приложений корпоративного контейнера не отображается на экране блокировки устройства. Для просмотра уведомлений необходимо разблокировать устройство или корпоративный контейнер.

  Если флажок снят, уведомления из приложений корпоративного контейнера отображаются на экране блокировки устройства.

  По умолчанию флажок установлен.

- **Запретить приложениям корпоративного контейнера использовать камеру**

  Установка или снятие флажка определяет, могут ли приложения из корпоративного контейнера получить доступ к камере устройства.

  По умолчанию флажок установлен.

- В разделе **Выдача разрешений для работы приложений в корпоративном контейнере** вы можете выбрать действие, которое будет выполняться, когда приложения из корпоративного контейнера запрашивают дополнительные разрешения. Это неприменимо к разрешениям, выданным в настройках устройства (например, Доступ ко всем файлам).

  - **Разрешить настройку пользователям**

    Пользователь решает, выдавать ли разрешение приложению.

    Этот параметр выбран по умолчанию.

  - **Выдавать разрешения автоматически**

    Разрешения для всех приложений в корпоративном контейнере выдаются без участия пользователя.

На Android 12 или выше следующие разрешения не могут быть выданы автоматически, но могут быть автоматически отклонены. При выборе этого параметра следующие разрешения будут запрашиваться у пользователя:

- разрешения на использование местоположения;
- разрешения на доступ к камере;
- разрешения на запись звука;
- разрешение на распознавание физической активности;
- разрешения на отслеживание входящих SMS и MMS сообщений;
- разрешения на доступ к данным биометрических датчиков.

- **Отклонять разрешения автоматически**

  Запросы на разрешения для всех приложений в корпоративном контейнере отклоняются без участия пользователя.

  Пользователи могут настраивать разрешения приложений в параметрах устройства, прежде чем эти разрешения будут автоматически отклонены.

- В разделе **Добавление виджетов приложений из корпоративного контейнера на главный экран устройства** вы можете выбрать, разрешено ли пользователю устройства добавлять виджеты приложений корпоративного контейнера на главный экран устройства.

  - **Запретить для всех приложений**

    Пользователю устройства запрещено добавлять виджеты приложений, установленных в корпоративном контейнере.

    Этот параметр выбран по умолчанию.

  - **Разрешить для всех приложений**

    Пользователю устройства разрешено добавлять виджеты всех приложений, установленных в корпоративном контейнере.

  - **Разрешить только перечисленным приложениям**

    Пользователю устройства разрешено добавлять виджеты перечисленных приложений, установленных в корпоративном контейнере.

    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 главном окне Kaspersky Security Center Web Console выберите **Управление активами → Мобильные → Приложения и файлы**.
2. Выберите **Android → Приложения**.

   В открывшемся списке приложений отображаются идентификаторы приложений в столбце **Имя пакета**.

- На вкладке **Сертификаты** вы можете настроить следующие параметры:
  - **Дублировать установку VPN-сертификатов в личное пространство пользователя**

    Установка или снятие флажка определяет, будет ли VPN-сертификат, добавленный в разделе **Мобильные → Сертификаты** Kaspersky Security Center Web Console и установленный в корпоративный контейнер, также установлен и в личном пространстве пользователя.

    По умолчанию VPN-сертификаты, полученные от Kaspersky Security Center, устанавливаются в корпоративном контейнере. Этот параметр применяется при выпуске нового VPN-сертификата.

    По умолчанию флажок снят.

  - **Дублировать установку корневых сертификатов в личное пространство пользователя**

    Установка или снятие флажка определяет, будут ли корневые сертификаты, добавленные в карточке **Корневые сертификаты** и установленные в корпоративный контейнер, также установлены и в личном пространстве пользователя.

    По умолчанию флажок снят.

- На вкладке **Пароль** укажите параметры пароля для корпоративного контейнера:
  - **Требовать установку пароля для корпоративного контейнера**

    Позволяет определить требования к паролю для корпоративного контейнера в соответствии с принятыми в компании требованиями безопасности.

    Если флажок установлен, требования к паролю доступны для настройки. После применения политики пользователь получит уведомление о необходимости задать пароль для корпоративного контейнера в соответствии с требованиями, принятыми в компании.

    Если флажок снят, изменение настроек пароля недоступно.

По умолчанию флажок снят.

- **Минимальная длина пароля**

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

  По умолчанию пароль пользователя состоит из 4 символов.

  Следующая информация относится только к личному пространству пользователя и корпоративному контейнеру:

  - В личном пространстве пользователя Kaspersky Endpoint Security сводит требования к надежности пароля к одному из значений, доступных в системе: средний или высокий уровень для устройств под управлением Android 10 или выше.
  - В корпоративном контейнере Kaspersky Endpoint Security сводит требования к надежности пароля к одному из значений, доступных в системе: 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**

  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.

- **Максимальное количество неудачных попыток ввода пароля до удаления корпоративного контейнера**

  Задает максимальное количество попыток пользователя ввести пароль для разблокировки корпоративного контейнера. После применения политики корпоративный контейнер будет удаляться с устройства в результате превышения максимального количества попыток.

  Возможные значения: от 4 до 16.

  Значение по умолчанию не задано. Это означает, что количество попыток неограниченно.

- **Максимальный срок действия пароля (дней)**

  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 установить 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 корпоративного контейнера (сек)**

  Определяет период неактивности перед блокировкой экрана устройства.

  По умолчанию указано значение 0. Это означает, что экран устройства не будет блокироваться после окончания какого-либо периода.

- **Период после биометрической разблокировки до запрашивания пароля (мин)**

  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.

- **Разрешить биометрические методы разблокировки**

  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.

- **Разрешить разблокировку по отпечатку пальца**

  Указывает, можно ли использовать отпечатки 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 устройства пункт установки отпечатков пальцев будет недоступен.

  Флажок доступен, только если установлен флажок **Разрешить биометрические методы разблокировки**.

  По умолчанию флажок установлен.

  На некоторых устройствах Xiaomi с корпоративным контейнером этот контейнер можно разблокировать с помощью отпечатка пальца только в том случае, если значение параметра **Период неактивности без блокировки корпоративного контейнера (сек)** будет установлено после установки отпечатка пальца в качестве способа разблокировки экрана.

- **Разрешить распознавание лица**

  Если флажок установлен, на мобильном устройстве разрешено использование распознавания лица.

  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**.

  По умолчанию флажок установлен.

- **Разрешить распознавание по радужной оболочке глаза**

  Если флажок установлен, на мобильном устройстве разрешено использование распознавания радужной оболочки глаза.

  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**.

  По умолчанию флажок установлен.

- На вкладке **Код разблокировки** настройте параметры одноразового кода. Это код, который пользователю нужно будет ввести для разблокировки корпоративного контейнера, 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 символа.

7. Нажмите **ОК**.

8. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Kaspersky Security Center. Мобильное устройство пользователя будет разделено на корпоративный контейнер и личное пространство.

## Разблокировка корпоративного контейнера

Если устройство не соответствует требованиям безопасности, указанным в Контроле соответствия, корпоративный контейнер может быть заблокирован.

Для разблокировки корпоративного контейнера пользователь мобильного устройства должен ввести одноразовый код на заблокированном экране. Этот код создается в Kaspersky Security Center. Он уникален для каждого мобильного устройства. После разблокировки корпоративного контейнера пароль корпоративного контейнера 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) в параметрах **Корпоративный контейнер на устройствах** политики.

*Чтобы разблокировать корпоративный контейнер с помощью одноразового кода:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.
2. Выберите мобильное устройство, для разблокировки которого вы хотите получить одноразовый код.
3. Выберите **Приложения** → **Kaspersky Mobile Devices Protection and Management**.

   Откроется окно свойств Kaspersky Mobile Devices Protection and Management.
4. Выберите вкладку **Параметры приложения**.

   В поле **Одноразовый код** в разделе **Одноразовый код разблокировки корпоративного контейнера** будет указан уникальный для выбранного устройства код.
5. Сообщите пользователю заблокированного мобильного устройства одноразовый код любым доступным способом (например, в сообщении электронной почты).

   Затем пользователь должен ввести полученный одноразовый код разблокировки на своем устройстве.

Корпоративный контейнер мобильного устройства пользователя будет разблокирован.

После блокировки корпоративного контейнера история паролей корпоративного контейнера очищается. Это означает, что пользователь может повторно использовать один из недавних паролей, независимо от параметров пароля для корпоративного контейнера.

## Добавление учетной записи LDAP

Эти параметры применяются к устройствам в режимах "Расширенный контроль" и "Базовый контроль".

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:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **LDAP** нажмите **Параметры**.

   Откроется окно **LDAP**.
5. Включите параметры с помощью переключателя **LDAP**.
6. Нажмите **Добавить**.

   Откроется окно **Добавить учетную запись LDAP**.

7. На закладке **Общие** настройте LDAP следующим образом:

   - В разделе **Сервер** укажите следующие параметры сервера:

     - В поле **Описание** введите описание учетной записи LDAP пользователя. Вы можете ввести значение или выбрать макрос, нажав кнопку +.

     - В поле **Адрес сервера** введите имя домена сервера LDAP.

   - В разделе **Аутентификация** укажите учетные данные пользователя:

     - В поле **Имя учетной записи** введите имя учетной записи для авторизации на сервере LDAP. Вы можете ввести значение или выбрать макрос, нажав кнопку +.

     - В поле **Пароль** введите пароль учетной записи LDAP для авторизации на сервере LDAP.

     - Чтобы использовать транспортный протокол передачи данных SSL для защиты передачи сообщений, установите флажок **Использовать SSL-соединение**.

   - При необходимости в разделе **Per App VPN** настройте Per App VPN.

8. На вкладке **Поиск** сформируйте список поисковых запросов для доступа пользователя iOS MDM-устройства к папкам с корпоративными данными на сервере LDAP:

   a. Нажмите **Добавить параметр**, чтобы добавить блок настроек поискового запроса.

   b. В поле **Название** введите название поискового запроса.

   c. В раскрывающемся списке **Глубина поиска** выберите уровень вложенности папки для поиска корпоративных данных на сервере LDAP:

      - **Корневая папка сервера LDAP**. Поиск в базовой папке сервера LDAP.

      - **Папки на первом уровне вложенности**. Поиск в папках на первом уровне вложенности от базовой папки.

      - **Папки на всех уровнях вложенности**. Поиск в папках на всех уровнях вложенности от базовой папки.

   d. В поле **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.

9. Нажмите **Добавить**.

   Новая учетная запись LDAP отобразится в списке.

   Вы можете изменять или удалять учетные записи LDAP с помощью кнопок **Изменить** и **Удалить** в верхней части списка.

10. Нажмите **ОК**.

11. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

В результате после применения политики на мобильном устройстве пользователя будут добавлены учетные записи LDAP из сформированного списка. Пользователь может получить доступ к корпоративным контактам в стандартных приложениях iOS: Контакты, Сообщения и Почта.

## Добавление учетной записи контактов

Эти параметры применяются к устройствам в режимах "Расширенный контроль" и "Базовый контроль".

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:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **Контакты** нажмите **Параметры**.

   Откроется окно **Контакты**.
5. Включите параметры с помощью переключателя **Контакты**.
6. Нажмите **Добавить**.

   Откроется окно **Добавить учетную запись CardDAV**.
7. В разделе **Сервер** в поле **Описание** введите описание учетной записи CardDAV пользователя.
8. В полях **Адрес сервера** и **Порт сервера** введите имя хоста или IP-адрес сервера CardDAV и номер порта сервера CardDAV.
9. В поле **Веб-адрес контакта** укажите веб-адрес учетной записи CardDAV пользователя iOS MDM-устройства на сервере CardDAV (например, `http://example.com/carddav/users/mycompany/user`).

   Веб-адрес должен начинаться `http://` или `https://`.
10. В разделе **Аутентификация** в поле **Имя учетной записи** введите имя учетной записи пользователя для авторизации на сервере CardDAV.
11. В поле **Пароль** введите пароль учетной записи CardDAV для авторизации на сервере CardDAV.
12. Если вы хотите использовать транспортный протокол передачи данных SSL для защиты передачи данных между сервером CardDAV и мобильным устройством, установите флажок **Использовать SSL-соединение**.
13. При необходимости в разделе **Per App VPN** настройте Per App VPN.

14. Нажмите **Добавить**.

    Новая учетная запись CardDAV отобразится в списке.

    Вы можете изменять или удалять учетные записи CardDAV с помощью кнопок **Изменить** и **Удалить** в верхней части списка.

15. Нажмите **OK**.

16. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

    Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

    В результате после применения политики на мобильном устройстве пользователя будут добавлены учетные записи CardDAV из сформированного списка.

Если у вас возникли проблемы при добавлении или обновлении учетных записей, проверьте правильность заданных вами параметров.

## Добавление учетной записи календаря

Чтобы пользователь iOS MDM-устройства мог работать со своими событиями календаря на сервере CalDAV, добавьте учетную запись 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:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.

4. На карточке **Календарь** нажмите **Параметры**.

   Откроется окно **Календарь**.

5. Включите параметры с помощью переключателя **Календарь**.

6. Нажмите **Добавить**.

   Откроется окно **Добавить учетную запись CalDAV**.

7. В разделе **Сервер** в поле **Описание** введите описание учетной записи CalDAV пользователя.

8. В полях **Адрес сервера** и **Порт сервера** введите имя хоста или IP-адрес сервера CalDAV и номер порта сервера CalDAV.

9. В поле **Веб-адрес календаря** 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 `http://` или `https://`.

10. В разделе **Аутентификация** в поле **Имя учетной записи** задайте имя учетной записи пользователя для авторизации на сервере CalDAV.

11. В поле **Пароль** задайте пароль учетной записи CalDAV для авторизации на сервере CalDAV.

12. Если вы хотите использовать транспортный протокол передачи данных SSL для защиты передачи данных о событиях между сервером CalDAV и мобильным устройством, установите флажок **Использовать SSL-соединение**.

13. При необходимости в разделе **Per App VPN** настройте Per App VPN.

14. Нажмите **Добавить**.

    Новая учетная запись CalDAV отобразится в списке.

    Вы можете изменять или удалять учетные записи CalDAV в списке с помощью кнопок **Изменить** и **Удалить** в верхней части списка.

15. Нажмите **ОК**.

16. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

В результате после применения политики на мобильном устройстве пользователя будут добавлены учетные записи CalDAV из сформированного списка.

Если у вас возникли проблемы при добавлении или обновлении учетных записей, проверьте правильность заданных параметров.

## Настройка подписки на календарь

Эти параметры применяются к устройствам в режимах "Расширенный контроль" и "Базовый контроль".

Чтобы пользователь iOS MDM-устройства мог добавлять в свой календарь события сторонних календарей (например, корпоративного календаря), нужно добавить подписку на эти календари. *Сторонние календари* – календари других пользователей, у которых есть учетная запись CalDAV, календари iCal, а также другие открыто опубликованные календари.

*Чтобы добавить подписку на календарь:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.

4. На карточке **Подписки на календари** нажмите **Параметры**.

   Откроется окно **Подписки на календари**.

5. Включите параметры с помощью переключателя **Подписки на календари**.

6. Нажмите **Добавить**.

   Откроется окно **Добавить подписку на календарь**.

7. В поле **Описание** введите описание подписки на календарь.

8. В поле **Адрес сервера** укажите URL стороннего календаря.

   Вы можете указать в поле основной URL учетной записи CalDAV пользователя, на календарь которого оформляется подписка. Также вы можете указать URL календаря iCal или другого открыто опубликованного календаря.

9. В поле **Имя пользователя** введите имя учетной записи пользователя для аутентификации на сервере стороннего календаря.

10. В поле **Пароль** введите пароль от подписки на календарь для аутентификации на сервере стороннего календаря.

11. Если требуется использовать транспортный протокол передачи данных SSL для защиты передачи данных о событиях между сервером CalDAV и мобильным устройством, установите флажок **Использовать SSL-соединение**.

12. При необходимости в разделе **Per App VPN** настройте Per App VPN.

13. Нажмите **Добавить**.

    Новая подписка на календарь отобразится в списке.

    > Вы можете изменять или удалять подписки на календари с помощью кнопок **Изменить** и **Удалить** в верхней части списка.

14. Нажмите **ОК**.

15. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

В результате после применения политики в календарь мобильного устройства пользователя будут добавлены события сторонних календарей из сформированного списка.

## Настройка единого входа

> Эти параметры применяются к устройствам в режимах "Расширенный контроль" и "Базовый контроль".

Параметры **SSO** позволяют настроить параметры учетной записи для использования технологии единого входа. *Единый вход (SSO)* – это метод аутентификации, который позволяет пользователю входить в разные сервисы, используя один идентификатор. Для аутентификации пользователя используется протокол Kerberos.

*Чтобы настроить использование единого входа на iOS MDM-устройствах:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.

4. На карточке **SSO** нажмите **Параметры**.

   Откроется окно **SSO**.

5. Включите параметры с помощью переключателя **SSO**.

6. Укажите следующие параметры:

   - В поле **Имя учетной записи** укажите имя учетной записи единого входа пользователя для авторизации на сервере Kerberos. Вы можете ввести значение или выбрать макрос, нажав кнопку +.

   - В разделе **Аутентификация** укажите параметры аутентификации:

     - **Имя пользователя Kerberos**

       Основное имя учетной записи пользователя iOS MDM-устройства на сервере Kerberos. Имя пользователя Kerberos требуется указывать с учетом регистра в формате `<основа>/<экземпляр>`, где:

       1. `<основа>` – имя пользователя.

       2. `<экземпляр>` – описание основного имени, например "admin". Экземпляр можно не указывать.

       Пример: если имя пользователя Kerberos – `mycompany/admin@EXAMPLE.COM` или `mycompany@EXAMPLE.COM`, вы должны ввести `mycompany/admin` или `mycompany`, соответственно.

       Вы можете ввести значение или выбрать макрос, нажав кнопку +.

       Не используйте коммерческое at (@) в этом поле. В противном случае профиль SSO не будет применен на устройстве.

     - **Рабочая область Kerberos**

       Имя сети, в состав которой входят серверы Kerberos и iOS MDM-устройства. Рабочую область требуется указывать прописными буквами.

       Имя сети может совпадать с именем домена. Например, если имена совпадают, для домена example.com рабочая область имеет имя `EXAMPLE.COM`.

       Пример: если имя пользователя Kerberos – `mycompany/admin@EXAMPLE.COM`, вы должны ввести `EXAMPLE.COM`.

- **Сертификат аутентификации**

  Сертификат, используемый для аутентификации пользователя.

- В разделе **URL-префиксы** укажите адреса сайтов, на которых Kaspersky Mobile Devices Protection and Management разрешает использовать единый вход:

  - **Использовать учетную запись только для указанных веб-адресов**

    Использование единой учетной записи для автоматического входа только на сайтах, которые добавлены в список разрешенных веб-адресов. Вы можете сформировать список разрешенных веб-адресов, нажав кнопку **Добавить URL** рядом с флажком.

    Если флажок установлен, пользователь может использовать единую учетную запись для авторизации только на сайтах, которые добавлены в список разрешенных веб-адресов.

    Если флажок снят или список пуст, пользователь может использовать единый вход для всех сайтов в **рабочей области Kerberos**.

    Имя сети, в состав которой входят серверы Kerberos и iOS MDM-устройства. Рабочую область требуется указывать прописными буквами.

    Имя сети может совпадать с именем домена. Например, если имена совпадают, для домена example.com рабочая область имеет имя `EXAMPLE.COM`.

    Пример: если имя пользователя Kerberos – `mycompany/admin@EXAMPLE.COM`, вы должны ввести `EXAMPLE.COM`.

    По умолчанию флажок снят.

  - **Добавить URL**

    При нажатии на кнопку добавляется поле **URL-префикс** для указания нового сайта в списке веб-адресов, для которых разрешен автоматический единый вход.

    Кнопка доступна, если установлен флажок **Использовать учетную запись только для указанных веб-адресов**.

    Веб-адрес должен начинаться с `http://` или `https://`. Автоматический вход с помощью единой учетной записи выполняется только при точном совпадении адреса сайта с шаблоном. Например, адрес сайта `https://example.com/` не совпадает с адресом `https://example.com:443/`.

    Чтобы разрешить доступ с использованием единого входа только к сайтам с протоколом HTTP, введите значение `http://`. Чтобы разрешить доступ только к сайтам с защищенным протоколом HTTPS, введите `https://`.

    Если веб-адрес не заканчивается символом "/", Kaspersky Mobile Devices Protection and Management автоматически добавит этот символ.

    Если список разрешенных веб-адресов пуст, пользователь может использовать единую учетную запись для автоматического входа на всех сайтах в **рабочей области Kerberos**.

    Имя сети, в состав которой входят серверы Kerberos и iOS MDM-устройства. Рабочую область требуется указывать прописными буквами.

    Имя сети может совпадать с именем домена. Например, если имена совпадают, для домена example.com рабочая область имеет имя `EXAMPLE.COM`.

Пример: если имя пользователя Kerberos – `mycompany/admin@EXAMPLE.COM`, вы должны ввести `EXAMPLE.COM`.

- В разделе **Идентификаторы пакетов** укажите идентификаторы приложений, для которых Kaspersky Mobile Devices Protection and Management разрешает использовать единый вход:

  - **Использовать учетную запись только для указанных приложений**

    Использование единого входа для автоматического входа только в приложениях, которые добавлены в список идентификаторов пакетов. Вы можете сформировать список идентификаторов пакетов, нажав кнопку **Добавить приложение** рядом с флажком.

    Если флажок установлен, пользователь может использовать единый вход для авторизации только в приложениях, которые добавлены в список идентификаторов пакетов.

    Если флажок снят или список пуст, пользователь может использовать единый вход для всех приложений в **рабочей области Kerberos**.

    Имя сети, в состав которой входят серверы Kerberos и iOS MDM-устройства. Рабочую область требуется указывать прописными буквами.

    Имя сети может совпадать с именем домена. Например, если имена совпадают, для домена example.com рабочая область имеет имя `EXAMPLE.COM`.

    Пример: если имя пользователя Kerberos – `mycompany/admin@EXAMPLE.COM`, вы должны ввести `EXAMPLE.COM`.

    По умолчанию флажок снят.

  - **Добавить приложение**

    При нажатии на кнопку добавляется поле **Идентификатор пакета (Bundle ID)** для указания нового идентификатора пакета в списке приложений, для которых разрешен автоматический единый вход.

    Кнопка доступна, если установлен флажок **Использовать учетную запись только для указанных приложений**.

    Автоматический единый вход выполняется только при точном совпадении добавленного идентификатора с идентификатором пакета. Например: `com.mycompany.myapp`.

    Для предоставления доступа к нескольким приложениям с помощью единой учетной записи используйте символ "*" после знака ".". Например: `com.mycompany.*`. Доступ будет предоставлен ко всем приложениям, идентификатор пакета которых начинается с указанного префикса.

    Если список идентификаторов пакетов приложений пуст, пользователь может использовать единую учетную запись для автоматического входа во все приложения в **рабочей области Kerberos**.

    Имя сети, в состав которой входят серверы Kerberos и iOS MDM-устройства. Рабочую область требуется указывать прописными буквами.

    Имя сети может совпадать с именем домена. Например, если имена совпадают, для домена example.com рабочая область имеет имя `EXAMPLE.COM`.

    Пример: если имя пользователя Kerberos – `mycompany/admin@EXAMPLE.COM`, вы должны ввести `EXAMPLE.COM`.

7. Нажмите **OK**.

8. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

   Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

   В результате после применения политики на iOS MDM-устройстве пользователя будет настроен единый вход.

## 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). Также веб-клипы могут всплыть, если пользователь коснется и удержит значок приложения Kaspersky Endpoint Security для Android.

Вы можете добавлять веб-клипы на устройства пользователей, удалять веб-клипы с устройств и указывать значки веб-клипов, которые отображаются на экране. Веб-клипы можно добавлять как на Android-устройства, так и на iOS MDM-устройства.

### Управление веб-клипами на Android-устройствах

*Чтобы управлять веб-клипами на Android-устройстве пользователя:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Конфигурация устройств**.

4. На карточке **Веб-клипы** нажмите **Параметры**.

   Откроется окно **Веб-клипы**.

5. Включите параметры с помощью переключателя **Веб-клипы**.

6. Нажмите **Добавить**.

   Откроется окно **Добавить веб-клип**.

7. В поле **Имя веб-клипа** введите название веб-клипа, которое будет отображаться на главном экране Android-устройства.

8. В поле **URL сайта** введите адрес сайта, который будет открываться при нажатии на значок веб-клипа. Адрес должен начинаться с `http://` или `https://`.

   Используйте только легитимные и доверенные источники. Настраивая параметры в этом поле, вы несете полную ответственность за потенциальные риски и последствия, связанные с использованием ненадежных источников.

Если указанный сайт запрещен или отсутствует в списке разрешенных сайтов в параметрах политики **Веб-Контроль**, пользователи не смогут перейти на этот сайт через веб-клип.

9. Нажмите **Выбрать**, чтобы указать изображение для значка веб-клипа. Поддерживаются форматы файлов PNG, JPEG и ICO. Если вы не выберете изображение для веб-клипа, в качестве значка будет отображаться пустой квадрат.

10. Нажмите **Добавить**.

    Новый веб-клип отобразится в списке.

    Вы можете изменять или удалять веб-клипы с помощью кнопок **Изменить** и **Удалить** в верхней части списка веб-клипов.

11. Нажмите **ОК**.

12. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

После применения политики на устройстве приложение Kaspersky Endpoint Security для Android будет показывать уведомления, предлагающие пользователю установить созданные вами веб-клипы. После того как пользователь установит веб-клипы, соответствующие значки будут добавлены на главный экран устройства.

Если в приложении не отображаются уведомления, предлагающие пользователю установить созданные вами веб-клипы, убедитесь, что установлен флажок **Устройство давно не синхронизировалось с Сервером администрирования** в параметрах **Настройка уведомлений** раздела **Параметры KES для Android**.

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. Пользователю нужно самостоятельно удалить такой веб-клип с главного экрана (процедура зависит от производителя устройства).

## Управление веб-клипами на iOS MDM-устройствах

По умолчанию к веб-клипам применяются следующие ограничения:

- Пользователь не может самостоятельно удалять веб-клипы с мобильного устройства.
- К значку веб-клипа на экране применяются визуальные эффекты сглаживания углов, тени и глянца.
- Веб-сайты, которые отображаются при нажатии на значок веб-клипа, открываются не на весь экран устройства.

*Чтобы управлять веб-клипами на iOS MDM-устройстве пользователя:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.

4. На карточке **Веб-клипы** нажмите **Параметры**.

   Откроется окно **Веб-клипы**.

5. Включите параметры с помощью переключателя **Веб-клипы**.

6. Нажмите **Добавить**.

   Откроется окно **Добавить веб-клип**.

7. В поле **Имя веб-клипа** введите название веб-клипа, которое будет отображаться на главном экране iOS MDM-устройства.

8. В поле **URL сайта** введите адрес сайта, который будет открываться при нажатии на значок веб-клипа. Адрес должен начинаться с `http://` или `https://`.

   Используйте только легитимные и доверенные источники. Настраивая параметры в этом поле, вы несете полную ответственность за потенциальные риски и последствия, связанные с использованием ненадежных источников.

   Если указанный сайт запрещен или отсутствует в списке разрешенных сайтов в параметрах политики **Веб-Контроль**, пользователи не смогут перейти на этот сайт через веб-клип.

9. Нажмите **Выбрать**, чтобы указать изображение для значка веб-клипа.

   Изображение должно удовлетворять следующим требованиям:

   - размер изображения не более 400 x 400 пикселей;
   - формат файла: PNG, JPEG или ICO;
   - размер файла не более 1 МБ.

   Если вы не выберете изображение для веб-клипа, в качестве значка будет отображаться пустой квадрат.

   Если у выбранного изображения прозрачный фон, на устройстве он будет черным.

10. В разделе **Опции** укажите следующие дополнительные параметры:

    a. Если вы хотите разрешить пользователю удалять веб-клип с iOS MDM-устройства, установите флажок **Разрешить удаление веб-клипа**.

    b. 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**.

    c. Если вы хотите, чтобы при нажатии на значок 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.

11. Нажмите **Добавить**.

Новый веб-клип отобразится в списке.

Вы можете изменять или удалять веб-клипы с помощью кнопок **Изменить** и **Удалить** в верхней части списка веб-клипов.

12. Нажмите **ОК**.
13. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

После применения политики значки веб-клипов из сформированного списка будут добавлены на главный экран мобильного устройства пользователя.

Значки удаленных веб-клипов исчезнут с главного экрана iOS MDM-устройства.

## Установка обоев

Вы можете установить изображение в качестве обоев для главного экрана и экрана блокировки на устройствах пользователей, подпадающих под одну и ту же политику.

*Чтобы установить обои на Android-устройства пользователей:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **Пользовательские обои** нажмите **Параметры**.

   Откроется окно **Пользовательские обои**.
5. Включите параметры с помощью переключателя **Пользовательские обои**.
6. В разделе **Обои главного экрана** в раскрывающемся списке **Способ установки обоев** выберите способ добавления обоев:

   - **Загрузить файл**

     Для использования этого способа нужно загрузить изображение в формате PNG или JPEG размером не более 1 МБ с вашего компьютера.

   - **Скачать изображение из интернета**

     Для этого способа нужно указать URL, начинающийся с `http://` или `https://`. Используйте только доверенные URL-адреса.
7. Добавьте изображение, которое будет использоваться в качестве обоев:

Используйте только легитимные и доверенные источники. Настраивая параметры в этом разделе, вы несете полную ответственность за потенциальные риски и последствия, связанные с использованием ненадежных источников.

- Если выбран вариант **Загрузить файл**, нажмите **Выбрать** для загрузки изображения. Когда загрузка будет завершена, откроется предварительный просмотр изображения.
- Если выбран вариант **Скачать изображение из интернета**, укажите ссылку на изображение в поле **Ссылка на изображение**. Вы можете нажать **Предварительный просмотр**, чтобы просмотреть изображение в новой вкладке браузера.

8. Если вы хотите использовать то же изображение в качестве обоев экрана блокировки, в разделе **Обои экрана блокировки** установите флажок **Использовать обои главного экрана для экрана блокировки**.
9. Нажмите **ОК**.
10. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Импортированное изображение будет установлено в качестве обоев на устройствах пользователей.

## Добавление шрифтов

Эти параметры применяются к устройствам в режимах "Расширенный контроль" и "Базовый контроль".

*Чтобы добавить шрифт на iOS MDM-устройство пользователя:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **iOS** и перейдите в раздел **Конфигурация устройств**.
4. На карточке **Пользовательские шрифты** нажмите **Параметры**.

   Откроется окно **Пользовательские шрифты**.
5. Включите параметры с помощью переключателя **Пользовательские шрифты**.
6. Нажмите **Добавить**.
7. Выберите файл шрифта, сохраненный на вашем компьютере. Файл должен иметь расширение .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 ошибке.

8. Нажмите **Открыть**.

   Новый шрифт отобразится в списке.

   > Вы можете удалять шрифты из списка с помощью кнопки **Удалить** в верхней части списка.

9. Нажмите **OK**.

10. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

    Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Сервером iOS MDM.

    В результате 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 нем приведены инструкции по отправке команд на мобильные устройства, а также по просмотру статуса выполнения команд в истории 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.

Вы можете отменять команды в окне **История команд**.

> Команды могут практически мгновенно доставляться на устройства, подключенные к интернету. Поэтому отмена команд может не удаться, несмотря на то, что они отображаются как отмененные.

# Команды для Android-устройств

| Команда | Результат |
| --- | --- |
| **Заблокировать устройство** | Мобильное устройство заблокировано. Чтобы получить доступ к данным, необходимо разблокировать устройство с помощью команды **Разблокировать устройство** или одноразового кода. |
| **Разблокировать устройство** | Мобильное устройство разблокировано.<br><br>После разблокировки устройства под управлением Android 5–6 пароль разблокировки экрана будет заменен на "1234". На устройствах под управлением Android 7 или выше после разблокировки 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.<br><br>Эта команда недоступна для личных устройств и устройств с корпоративным контейнером под управлением Android 14 или выше. |
| **Удалить корпоративные данные** | Корпоративные данные удалены с устройства. Перечень удаляемых данных зависит от режима работы устройства:<br>• На личном устройстве удалены Knox-контейнер, корпоративные файлы, отправленные на устройство, и почтовый сертификат.<br>• С корпоративных устройств удалены Knox-контейнер, корпоративные файлы, отправленные на устройство, и сертификаты, установленные приложением Kaspersky Endpoint Security для Android (почтовые и VPN-сертификаты, сертификаты, полученные через профили SCEP, кроме мобильных сертификатов).<br>• Дополнительно, если создан корпоративный контейнер, удален корпоративный контейнер (его содержимое, корпоративные файлы, отправленные на устройство, настройки и ограничения) и сертификаты, установленные в корпоративном контейнере (почтовые и VPN-сертификаты, сертификаты, полученные через профили SCEP, кроме мобильных сертификатов). |
| **Синхронизировать устройство** | Данные с мобильного устройства синхронизированы с Сервером администрирования.<br><br>Статус *Выполнена* может отображаться, если команда была успешно отправлена, но еще не получена устройством. |
| **Определить местоположение** | Получены координаты местоположения мобильного устройства.<br>Чтобы посмотреть местоположение устройства в программе "Яндекс Карты", перейдите в раздел **Управление активами → Мобильные → Устройства**. Затем выберите устройство и нажмите **История команд → Определить местоположение → Координаты устройства → Посмотреть на карте**. После нажатия кнопки **Посмотреть на карте** координаты устройства передаются в Яндекс Карты, и устройство отображается на карте.<br><br>На устройствах с Android 12 или выше, если пользователем 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 не выполняется.<br><br>Если на Android-устройстве отключена служба Google "Точность местоположения", команда работать не будет. Обращаем внимание, что не на всех Android-устройствах есть эта служба. |

| Команда | Результат |
| --- | --- |
| **Сделать фотографии** | Мобильное устройство заблокировано. Фотографии сделаны фронтальной камерой устройства при попытке разблокировать устройство. На устройствах с выдвижной фронтальной камерой фотография будет черной, если камера закрыта.<br><br>При попытке разблокировки устройства пользователь автоматически соглашается на фотографирование с помощью устройства.<br><br>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 выше, уведомление не отображается, но сделанная фотография будет черной. |
| **Воспроизвести звуковой сигнал** | Мобильное устройство воспроизводит звуковой сигнал в течение 5 минут (в течение 1 минуты, если заряд батареи устройства низкий) или до тех пор, пока пользователь не разблокирует устройство. |
| **Удалить данные приложения** | Данные указанного приложения удалены с мобильного устройства.<br><br>Для этого действия необходимо указать имя пакета приложения, данные которого нужно удалить.<br><br>В результате приложение возвращается в состояние по умолчанию.<br><br>Данные системных приложений и приложений-администраторов не удаляются. |
| **Удалить данные всех приложений** | Данные всех приложений удалены с мобильного устройства.<br><br>На корпоративном устройстве удаляются данные всех приложений.<br><br>На устройстве с корпоративным контейнером удаляются данные всех приложений в корпоративном контейнере.<br><br>В результате приложения возвращаются в состояние по умолчанию.<br><br>Данные системных приложений и приложений-администраторов не удаляются. |
| **Отправить сообщение** | Сообщение с указанными параметрами (заголовком и текстом) отправлено на мобильное устройство пользователя. Вы можете отправить push-уведомление вместе с предупреждением, либо только push-уведомление. |
| **Получить историю местоположений** | Отображается история местоположений мобильного устройства за последние 14 дней.<br>Чтобы посмотреть местоположение устройства в программе "Яндекс Карты", перейдите в раздел **Управление активами** → **Мобильные** → **Устройства**. Затем выберите устройство и нажмите **История команд** → **Получить историю местоположений** → **Посмотреть на карте**. После нажатия кнопки **Посмотреть на карте** координаты устройства передаются в Яндекс Карты, и устройство отображается на карте.<br><br>Из-за технических ограничений Android-устройств фактическое определение местоположения устройства может происходить реже, чем указано в параметрах политики **Определение местоположения**. |
| **Перезагрузить устройство** | Мобильное устройство перезагружено. Результат выполнения команды будет отправлен в Kaspersky Security Center после того, как пользователь разблокирует свое устройство.<br><br>Устройство не может быть перезагружено во время звонка. Kaspersky Endpoint Security для Android попытается выполнить команду снова после окончания звонка.<br><br>Эта команда доступна только для корпоративных устройств под управлением Android 7 или выше. |
| **Сбросить пароль** | Пароль разблокировки корпоративного устройства или корпоративного контейнера сброшен.<br>Эта команда недоступна для личных устройств. |

# Команды для iOS MDM-устройств

| Команда | Результат |
|---|---|
| **Заблокировать устройство** | Мобильное устройство заблокировано. Для получения доступа к данным необходимо разблокировать устройство. |
| **Сбросить пароль разблокировки** | 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** | С устройства удалены все установленные конфигурационные профили, управляющий профиль и приложения, для которых был установлен флажок **Удалять при удалении управляющего профиля**. |
| **Синхронизировать устройство** | Данные с мобильного устройства синхронизированы с Сервером администрирования. |
| **Установить конфигурационный профиль** | Конфигурационный профиль установлен на мобильном устройстве.<br>Нельзя установить конфигурационный профиль с параметрами для устройства, работающего в режиме "Расширенный контроль", на устройстве, работающем в режиме "Базовый контроль". |
| **Удалить конфигурационный профиль** | Конфигурационный профиль удален с мобильного устройства.<br>Профиль может отображаться в списке конфигурационных профилей, установленных на устройстве, в течение нескольких минут после его удаления. |
| **Установить приложение** | Указанное приложение установлено на мобильном устройстве. |
| **Обновить приложение** | Указанное приложение обновлено на мобильном устройстве. |
| **Удалить приложение** | Указанное приложение удалено с мобильного устройства. |
| **Обновить ОС (для режима "Расширенный контроль")** | На мобильном устройстве запланированы обновления операционной системы в соответствии с указанными настройками обновлений.<br>Эта команда может не быть выполнена, если на устройстве недостаточно места для хранения данных или указанная версия ОС недоступна для выбранного устройства. Рекомендуем указывать последнюю доступную версию ОС. |
| **Изменить параметры роуминга** | Включение или выключение роуминга данных или роуминга голосовой связи. |
| **Настроить Bluetooth (для режима "Расширенный контроль")** | Включение или выключение Bluetooth на мобильном устройстве.<br>Эта команда поддерживается только на устройствах в режиме "Расширенный контроль" под управлением iOS 11.3 и выше. |
| **Включить Режим пропажи (для режима "Расширенный контроль")** | На мобильном устройстве в режиме "Расширенный контроль" включен Режим пропажи, устройство заблокировано. На экране устройства появилось сообщение и номер телефона, которые вы можете редактировать.<br>Если вы отправите команду Включить режим пропажи на iOS MDM-устройство в режиме "Расширенный контроль" без SIM-карты, и это устройство будет перезапущено, оно не сможет подключиться к сети Wi-Fi и получить команду Выключить 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 Выключить режим пропажи по мобильной сети. |

| Команда | Результат |
| --- | --- |
| **Определить местоположение (только в Режиме пропажи)** | Получены данные о местоположении устройства.<br>Чтобы посмотреть местоположение устройства в программе "Яндекс Карты", перейдите в раздел **Управление активами → Мобильные → Устройства**. Затем выберите устройство и нажмите **История команд → Определить местоположение → Координаты устройства → Посмотреть на карте**. После нажатия кнопки **Посмотреть на карте** координаты устройства передаются в Яндекс Карты, и устройство отображается на карте. |
| **Воспроизвести звуковой сигнал (только в Режиме пропажи)** | На потерянном мобильном устройстве воспроизводится звуковой сигнал. |
| **Выключить Режим пропажи (для режима "Расширенный контроль")** | На мобильном устройстве выключен Режим пропажи, устройство разблокировано. |

### 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 отозвать разрешения в параметрах устройства позднее. В этом случае выполнение команд невозможно.

На устройствах с Android 10 или выше необходимо предоставить разрешение "Всегда" для доступа к местоположению устройства. На устройствах с Android 11 или 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. Мы рекомендуем связаться с пользователем напрямую при повторном запросе разрешения для камеры.

## Отправка команд

*Чтобы отправить команду на мобильное устройство пользователя:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Мобильные → Устройства**.
2. В открывшемся списке устройств выберите устройства, на которые вы хотите отправить команду.

   Можно выбрать несколько устройств.
3. Нажмите **Отправить команду**.
4. В открывшемся окне **Отправить команду** в поле **Команда** выберите нужную команду.
5. Настройте команду, которую вы хотите отправить.

6. Нажмите **Отправить**.

   Вы можете просматривать и отменять команды в окне **История команд**.

Команда будет отправлена на выбранные вами устройства.

## Просмотр статусов команд в истории команд

Приложение сохраняет в истории команд информацию обо всех командах, отправленных на мобильные устройства. В истории команд сохраняется информация о времени и дате отправления команд на мобильное устройство, статусы команд, а также описания результатов. Например, в случае сбоя команды в истории отображается причина ошибки.

Команды, отправленные на мобильные устройства, могут иметь следующие статусы:

- *Отправлена*

  Команда отправлена на мобильное устройство.

- *Выполнена*

  Команда выполнена успешно.

- *Ошибка*

  Не удалось выполнить команду.

- *Отменяется*

  Команда удаляется из очереди команд, отправленных на мобильное устройство.

- *Отменена*

  Команда успешно удалена из очереди команд, отправленных на мобильное устройство.

Приложение ведет историю команд для каждого мобильного устройства.

*Чтобы просмотреть историю команд:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.

2. Выберите в списке мобильное устройство, для которого вы хотите просмотреть историю команд.

3. Нажмите **История команд**.

   Откроется окно **История команд**. Разделы окна **История команд** соответствуют командам, которые можно отправить на мобильное устройство.

4. Выберите разделы с нужными командами и посмотрите информацию об отправке и выполнении команд.

# Управление приложением с помощью сторонних EMM-решений (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.

Также вы можете использовать стороннее EMM-решение только для развертывания Kaspersky Endpoint Security для Android, а после развертывания управлять устройствами в Web Console.

Если приложение Kaspersky Endpoint Security для Android развернуто с помощью стороннего EMM-решения, вы не сможете управлять приложением с помощью Kaspersky Endpoint Security Cloud, но сможете управлять приложением в EMM-консоли, Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console.

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, созданный сторонним EMM-решением.
- 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 устройствах пользователей необходимо добавить Kaspersky Endpoint Security для Android в магазин приложений EMM с помощью инсталляционного APK-файла с сайта "Лаборатории Касперского". Подробнее о работе с приложениями в EMM-Консоли см. на *сайте Службы технической поддержки поставщика услуг EMM*.

Kaspersky Endpoint Security для Android разворачивается в рабочем профиле Android, созданном сторонним EMM-решением. Приложение изолировано от персональных данных пользователя и защищает только корпоративные данные в рабочем профиле.

Рекомендуется обеспечить защиту от удаления Kaspersky Endpoint Security для Android 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.
- Разрешение "Администратор устройства" для работы основных функций защиты, таких как Анти-Вор и Контроль приложений.
- 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.

Kaspersky Endpoint Security для Android устанавливается в рабочем профиле Android, созданном сторонним EMM-решением. Затем приложение будет обновляться с сайта "Лаборатории Касперского" или с помощью HUAWEI AppGallery, Samsung Galaxy Store, RuStore или Xiaomi GetApps.

Для работы Веб-Фильтра в параметрах Google Chrome дополнительно требуется настроить прокси-сервер с помощью файла AppConfig сторонней EMM-системы:

- 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 сайты перед открытием, 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 Kaspersky Security Center Web Console.

- 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** → **Приложение** → **Собственные**.

   Откроется конфигурация приложения.

2. Выберите раздел **Общедоступные**.

3. Выберите приложение Google Chrome.

   Откроется окно свойств устройства.

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 конфигурация приложения.

2. Выберите раздел **Общедоступные**.

3. Выберите приложение Kaspersky Endpoint Security.

   Откроется окно свойств устройства.

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 Kaspersky Security Center Web Console.

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 Kaspersky Endpoint Security для Android прекращает выполнять все свои функции.

По истечении срока действия коммерческой лицензии приложение продолжает работу, но с ограниченной функциональностью (например, недоступно обновление баз Kaspersky Endpoint Security для Android). Чтобы продолжить использование всех функций приложения, вам нужно продлить срок действия коммерческой лицензии.

*Чтобы активировать приложение Kaspersky Endpoint Security для Android:*

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 хосте Kaspersky Security Center Web Console установлен плагин Kaspersky Mobile Devices Protection and Management.
- В свойствах Сервера администрирования открыт порт для подключения мобильных устройств.
- В свойствах Сервера администрирования 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 политики для мобильных устройств, создайте отдельную группу администрирования для мобильных устройств. Сторонние EMM-решения поддерживают только режим работы "Личное устройство".
- 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 `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 на использование камеры для работы Анти-Вора (команда **Сделать фотографии**).
- Разрешение на определение местоположения для работы Анти-Вора (команда **Определить местоположение**).
- Права администратора устройства (владельца рабочего профиля Android) для работы следующих функций приложения:
  - настройка Wi-Fi;
  - ограничение использования камеры, Bluetooth, Wi-Fi.

Из-за особенностей работы стороннего рабочего профиля Android в приложении недоступен Анти-Вор, а также Контроль приложений не может блокировать приложения по категориям.

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 [идентификатор устройства, электронная почта].

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**
- **Параметры разблокировки экрана**
- Вкладка **Контроль приложений** в разделе **Использование приложений**.
- **Корпоративный контейнер на устройствах**
- **Параметры Samsung Knox**

Способ развертывания стороннего рабочего профиля не позволяет применить параметры групповой политики из раздела **Корпоративный контейнер на устройствах**. Эти параметры можно применить, только если корпоративный контейнер создан с помощью Kaspersky Security Center.

# Тихий режим

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**. Это уведомление закреплено в панели уведомлений. Уведомление о состоянии защиты нельзя удалить. В нем 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`.

Если устройства подключены к Kaspersky Security Center, вы можете включить тихий режим только в групповой политике.

*Чтобы включить тихий режим работы приложения через консоль VMware Workspace ONE:*

1. В консоли выберите **Книги и приложения** → **Приложение** → **Собственные**.

   Откроется конфигурация приложения.

2. Выберите раздел **Общедоступные**.

3. Выберите приложение Kaspersky Endpoint Security.

   Откроется окно свойств устройства.

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. Выключите уведомления приложения с помощью соответствующего параметра.

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.

| 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".<br>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.<br>`Accepted` – я подтверждаю, что полностью прочитал(а), понимаю и принимаю положения и условия настоящего Лицензионного соглашения<br>`Declined` – я не принимаю условия и положения настоящего Лицензионного соглашения.<br>Чтобы принять условия и положения Лицензионного соглашения для всех мобильных устройств, необходим доступ в интернет для подключения к серверам "Лаборатории Касперского".<br>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.<br>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>;...`".<br>Код Лицензионного соглашения содержится в Лицензионном соглашении. | |

| Ключ конфигурации | Описание | Тип | Значение | Значение по умолчанию |
|---|---|---|---|---|
| `EulaAcceptanceCodesV2` | Коды Лицензионных соглашений | String | *Чтобы просмотреть код Лицензионного соглашения, выполните следующие действия:*<br>1. Скопируйте ссылку на Лицензионное соглашение (`EulaAcceptanceConfirmationV1`) из EMM-консоли.<br>2. Вставьте ссылку в браузер.<br>Откроется Лицензионное соглашение.<br>3. Ознакомьтесь с условиями и положениями Лицензионного соглашения и определите код Лицензионного соглашения.<br>Чтобы принять условия и положения Лицензионных соглашений для всех мобильных устройств, необходим доступ в интернет для подключения к серверам "Лаборатории Касперского".<br>Если вы не заполните эти поля, приложение предложит пользователю принять условия и положения 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.<br>Пользователь устройства может изменить адрес Сервера администрирования Kaspersky Security Center на свой.<br>Если вы укажете значения в обоих полях, будут приняты условия всех указанных в них лицензионных соглашений. | `<адрес сервера>:13292` |
| `DisableNotification` | Выключить уведомления приложения до подключения к Kaspersky Security Center | Boolean | `True` – Kaspersky Endpoint Security для Android скрывает все уведомления до подключения устройства к Kaspersky Security Center. После подключения приложение показывает все уведомления. Вы можете выключить некоторые уведомления приложения в параметрах политики.<br>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.<br>`False` – Kaspersky Endpoint Security для Android показывает все уведомления о работе приложения. | `False` |

| Ключ конфигурации | Описание | Тип | Значение | Значение по умолчанию |
|---|---|---|---|---|
| `ScanScheduleType` | Режим запуска проверки | Choice | `AfterUpdate` – запуск проверки на наличие вредоносного ПО после обновления баз. Приложение обновляет базы вредоносного ПО по сформированному расписанию (`UpdateScheduleType`).<br>`Daily` – запуск проверки на наличие вредоносного ПО раз в день. Настройте время запуска проверки (`ScanScheduleTime`).<br>`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`).<br>`Off` – автоматический запуск проверки на наличие вредоносного ПО выключен.<br>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`<br>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.<br>`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.<br>`OnlyExecutables` – проверка только исполняемых файлов. К исполняемым файлам относятся файлы с расширением .apk (.zip), .dex, .so.<br>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.<br>`False` – приложение проверяет только файлы архивов.<br>Приложение проверяет только архивы с расширением .zip (.apk). | `True` |

| Ключ конфигурации | Описание | Тип | Значение | Значение по умолчанию |
|---|---|---|---|---|
| `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.<br>`Delete` – приложение удаляет обнаруженные объекты.<br>`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.<br>`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.<br>Приложение записывает информацию об обнаруженных угрозах и выполненных действиях в отчеты приложения. | `Карантин` |
| `ScanLock` | Запретить настраивать параметры проверки | Boolean | `True` – следующие параметры проверки недоступны для пользователя в настройках приложения: тип файлов для проверки, проверка архивов, действие при обнаружении угрозы.<br>`False` – пользователь может настроить параметры проверки и, например, выбрать действие `Skip` при обнаружении угрозы. | `True` |
| `ScanAndProtectionAdwareRiskware` | Блокировать рекламное ПО, средства автодозвона и приложения, которые могут использоваться злоумышленниками для нанесения вреда устройству и данным пользователя | Boolean | `True` – приложение обнаруживает рекламные приложения и приложения, которые могут быть использованы злоумышленниками для нанесения вреда устройству и данным пользователя.<br>`False` – приложение пропускает рекламные приложения и приложения, которые могут быть использованы злоумышленниками для нанесения вреда устройству или данным пользователя. | `True` |
| `ProtectionMode` | Режим постоянной защиты | Choice | `Recommended` – приложение только однократно проверяет новые приложения (сразу после установки) и файлы из папки Загрузки.<br>`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.<br>`Disabled` – постоянная защита выключена. | `Recommended` |

| Ключ конфигурации | Описание | Тип | Значение | Значение по умолчанию |
|---|---|---|---|---|
| `UseKsnMode` | Режим Kaspersky Security Network | Choice | `Recommended` – приложение обменивается данными с Kaspersky Security Network (KSN). Kaspersky Endpoint Security для Android использует KSN для постоянной защиты устройства от угроз (Облачная защита) и работы Веб-Фильтра в интернете.<br><br>`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.<br><br>`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.<br><br>`OnlyExecutables` – проверка только исполняемых файлов. К исполняемым файлам относятся файлы с расширением .apk (.zip), .dex, .so.<br><br>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.<br><br>`Delete` – приложение удаляет обнаруженные объекты.<br><br>`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.<br><br>Приложение записывает информацию об обнаруженных угрозах и выполненных действиях в отчеты приложения. | `Карантин` |
| `ProtectionLock` | Запретить настраивать параметры постоянной защиты | Boolean | `True` – следующие параметры постоянной защиты недоступны для пользователя в настройках приложения: режим постоянной защиты, тип файлов для проверки и действие при обнаружении угрозы.<br><br>`False` – пользователь может настроить параметры постоянной защиты и, например, выбрать действие `Skip` при обнаружении угрозы. | `True` |

| Ключ конфигурации | Описание | Тип | Значение | Значение по умолчанию |
|---|---|---|---|---|
| `UpdateScheduleType` | Режим запуска обновления баз | Choice | `Daily` – проверка наличия новых баз вредоносного ПО и загрузка их на устройства раз в день. Настройте время запуска обновления баз (`UpdateScheduleTime`).<br>`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`).<br>`Off` – автоматическое обновление баз вредоносного ПО выключено.<br>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`<br>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.<br>`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`).<br>`False` – приложение загружает базы вредоносного ПО, только если устройство находится в домашней сети. | `False` |

| Ключ конфигурации | Описание | Тип | Значение | Значение по умолчанию |
|---|---|---|---|---|
| `EnableWebFilter` | Веб-Фильтр | Boolean | `True` – приложение блокирует вредоносные и фишинговые веб-сайты в интернете с помощью компонента Веб-Фильтр. Веб-Фильтр на Android-устройствах поддерживается только браузерами Google Chrome, HUAWEI Browser, Samsung Internet и Яндекс Браузер.<br>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.<br>`False` – защита от вредоносных и фишинговых веб-сайтов выключена.<br>Для работы Веб-Фильтра должны быть выполнены следующие условия:<br>• Пользователи устройств приняли Политику конфиденциальности и Положение о Веб-Фильтре в мастере первоначальной настройки или параметрах приложения.<br>• В параметрах браузера настроен прокси-сервер:<br>`ProxyMode = "fixed_servers"`<br>`ProxyServer = "127.0.0.1:3128"`<br>`DisableSpdy = true`<br>`DataCompressionProxyEnabled = false`<br>Конфигурации прокси-сервера могут различаться в зависимости от версии браузера.<br>После удаления приложения Kaspersky Endpoint Security для Android с мобильного устройства сбросьте настройки прокси-сервера.<br>• В параметрах приложения включено использование KSN: `UseKsnMode = Recommended` или `UseKsnMode = Extended`.<br>• Рекомендуется выбрать Google Chrome, HUAWEI Browser, Samsung Internet Browser или Yandex Browser в качестве браузера по умолчанию в настройках операционной системы. | `False` |
| `EnableWebFilterLock` | Запретить настраивать Веб-Фильтр | Boolean | `True` – параметры Веб-Фильтра недоступны для пользователя в настройках приложения.<br>`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`.<br>Если оставить поле пустым, Kaspersky Endpoint Security для Android использует серверы обновлений баз "Лаборатории Касперского". | |

| Ключ конфигурации | Описание | Тип | Значение | Значение по умолчанию |
|---|---|---|---|---|
| `AllowGoogleAnalytics` | Передавать данные в сервисы Google Analytics для Firebase, 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 соответствующими условиями использования сервисов Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics.<br>`False` – передача данных в сервисы Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics выключена. | `True` |
| `KscDeviceNameTag` | Тег названия устройства для Kaspersky Security Center | String | Этот параметр доступен только для VMware AirWatch.<br>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.<br>• `{DeviceSerialNumber}` – серийный номер устройства.<br>• `{DeviceUid}` – уникальный идентификатор устройства (UDID).<br>• `{DeviceAssetNumber}` – инвентарный номер устройства. Это внутренний номер, создаваемый в организации.<br>Можно добавить несколько значений (например, `{DeviceSerialNumber} {DeviceUid}`).<br>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 в разделе **Обнаружение устройств и развертывание** > **Развертывание и назначение** > **Правила перемещения**.<br>Если это поле не заполнено, устройство автоматически добавляется в корень папки **Нераспределенные устройства**. | `KES10` |

| Ключ конфигурации | Описание | Тип | Значение | Значение по умолчанию |
|---|---|---|---|---|
| `KscCorporateEmail` | Корпоративная электронная почта пользователя | String | В консоли EMM можно указать корпоративные адреса электронной почты пользователей. Эти адреса электронной почты будут отображаться в Kaspersky Security Center.<br>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.<br>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. | |

# Участие в Kaspersky Security Network

Чтобы повысить эффективность защиты мобильных устройств, Kaspersky Endpoint Security для Android и Kaspersky Protection 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 Kaspersky Endpoint Security для Android и Kaspersky Protection для iOS. Кроме того, участие в Kaspersky Security Network обеспечивает доступ к данным о репутации программ и сайтов.

Когда вы участвуете в Kaspersky Security Network, статистика, полученная в результате работы Kaspersky Endpoint Security для Android и Kaspersky Protection для iOS, 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.

Для работы Kaspersky Endpoint Security для Android и Kaspersky Protection для iOS использование Kaspersky Security Network является обязательным.

Следующие компоненты приложений используют облачную службу Kaspersky Security Network:

- В приложении Kaspersky Endpoint Security для Android компоненты Защита от вредоносного ПО, Веб-Защита, Веб-Контроль и Контроль приложений.
- В приложении Kaspersky Protection для iOS компонент Веб-Защита.

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 и Kaspersky Protection для iOS передают 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 и Kaspersky Protection для iOS передают в Kaspersky Security Network. Вы можете использовать Kaspersky Security Network, если срок действия лицензии на интегрированное решение не истек и ключ не был запрещен.

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-Защита** и **Веб-Контроль**. Приложение выполняет проверку сайтов перед открытием с учетом данных, полученных от KSN. Также приложение определяет категорию 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 эту информацию.

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

Подробная информация о предоставлении данных в KSN приведена 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 Protection для iOS

Для повышения уровня оперативной защиты Kaspersky Protection для iOS использует облачную службу Kaspersky Security Network в работе следующих компонентов:

- **Веб-Защита**. Приложение выполняет проверку сайтов перед открытием с учетом данных, полученных от KSN.

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

Подробная информация о предоставлении данных в KSN приведена в разделе Предоставление данных в Kaspersky Protection 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

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 или Kaspersky Protection для iOS.

- 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.

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 и Kaspersky Protection для iOS, использующих Kaspersky Security Network, выполняется отправка запросов в облачные службы. Запросы содержат данные, описанные в разделах Предоставление данных в Kaspersky Endpoint Security для Android и Предоставление данных в Kaspersky Protection для iOS соответственно.

Если использование Kaspersky Security Network на устройстве выключено, компоненты Защита от вредоносного ПО, Веб-Защита, Веб-Контроль и Контроль приложений автоматически выключаются.

*Чтобы включить или выключить использование Kaspersky Security Network на Android-устройствах:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Параметры KES для Android**.
4. На карточке **Kaspersky Security Network** нажмите **Параметры**.

   Откроется окно **Kaspersky Security Network**.
5. С помощью переключателя **Kaspersky Security Network** включите работу следующих компонентов: Защита от вредоносного ПО, Веб-Защита, Веб-Контроль и Контроль приложений.
6. При необходимости в разделе **Прокси-сервер KSN** установите флажок **Переключаться на использование публичных серверов Kaspersky Security Network при недоступности прокси-сервера KSN**.
7. Нажмите **OK**.
8. На карточке **Отправка дополнительных данных** нажмите **Параметры**.
9. В разделе **Отправка данных в Kaspersky Security Network** установите флажок **Разрешить отправку статистических данных в Kaspersky Security Network** для передачи данных в "Лабораторию Касперского".

   Эти данные позволят увеличить скорость реакции приложения Kaspersky Endpoint Security для Android на угрозы, улучшить производительность компонентов защиты, снизить вероятность ложных срабатываний.
10. В разделе **Отправка данных для маркетинговых целей** установите флажок **Разрешить обработку данных, чтобы помочь улучшить качество работы, интерфейс и производительность приложения** для улучшения качества, внешнего вида и производительности программного обеспечения, продуктов, служб и инфраструктуры "Лаборатории Касперского" по результатам анализа работы пользователей, функций, статуса и используемых настроек устройств.

11. Выберите, кто должен принять Положения:

    - Если вы выбрали **Положения принимаются администратором**, вам будет предложено принять Положения в открывшемся окне.

    - Если вы выбрали **Положения принимаются пользователями**, пользователю устройства будет предложено принять Положения.

12. Нажмите **OK**.

13. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

*Чтобы включить или выключить использование Kaspersky Security Network на iOS-устройстве:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами → Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **iOS** и перейдите в раздел **Параметры KP для iOS**.

4. Включите работу компонента Веб-Защита с помощью переключателя на карточке **Kaspersky Security Network**.

5. На карточке **Отправка дополнительных данных** нажмите **Параметры**.

6. В разделе **Отправка данных в Kaspersky Security Network** установите флажок **Разрешить отправку статистических данных в Kaspersky Security Network** для передачи данных в "Лабораторию Касперского".

   Эти данные позволят увеличить скорость реакции приложения Kaspersky Protection для iOS на угрозы, улучшить производительность компонентов защиты, снизить вероятность ложных срабатываний.

7. Выберите, кто должен принять Положения:

    - Если вы выбрали **Положения принимаются администратором**, вам будет предложено принять Положения в открывшемся окне.

    - Если вы выбрали **Положения принимаются пользователями**, пользователю устройства будет предложено принять Положения.

8. Нажмите **OK**.

9. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

# 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.

KPSN применяется только для Android-устройства под управлением Kaspersky Endpoint Security для Android. Kaspersky Protection для iOS продолжает отправлять статистические данные с устройств пользователей в KSN.

*Чтобы включить использование KPSN в Kaspersky Security Center:*

1. В главном окне Kaspersky Security Center Web Console нажмите на имя Сервера администрирования.
2. В открывшемся окне свойств Сервера администрирования на вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.
3. Установите переключатель в положение **Использовать Kaspersky Private Security Network Включено**.
4. Нажмите **Файл с параметрами прокси-сервера KSN**, а затем выберите конфигурационный файл с расширением PKCS7 или PEM (предоставляется "Лабораторией Касперского").
5. Нажмите **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 для подключения к KPSN**. В противном случае запросы от управляемых программ не попадут в KPSN.
7. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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.

Если мобильные устройства подключены к Kaspersky Security Center через шлюз соединения, прокси-сервер KSN не работает. В этом случае выключите переключатель **Включить прокси-сервер KSN на Сервере администрирования Включено** в разделе **Прокси-сервер KSN** окна свойств Сервера администрирования. Подробная информация о включении и выключении прокси-сервера KSN приведена в справке Kaspersky Security Center.

# Samsung Knox

*Samsung Knox* – мобильное решение для настройки и развертывания 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. Решение используется для массовой установки и первоначальной настройки приложений на новых устройствах Samsung.

Установка приложения Kaspersky Endpoint Security для Android через Knox Mobile Enrollment состоит из следующих этапов:

1. **Создание профиля Knox 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 поддерживаемых Samsung-устройств.

## Создание профиля Knox

*Профиль Knox* – это профиль, который содержит ссылки на приложения для их быстрого развертывания и первоначальной настройки на мобильных устройствах.

*Чтобы создать профиль Knox:*

1. Войдите в консоль Samsung Knox → **Knox Mobile Enrollment**.
2. Выберите раздел **Профили**.
3. Нажмите **Действия** > **Создать профиль**.

   Запустится мастер создания нового профиля.
4. Выберите **Android Enterprise** в качестве типа профиля.

5. В открывшемся окне **Сведения о профиле Android Enterprise** укажите следующие параметры:

   a. В разделе **Основная информация** введите общую информацию о профиле Knox: **Название профиля** и **Описание**.

   b. В разделе **Информация о EMM** в поле **Выберите свой EMM** выберите **Другое**.

   c. В поле **APK агента EMM** введите путь к инсталляционному APK-файлу.

      Инсталляционный файл Kaspersky Endpoint Security для Android входит в комплект поставки Kaspersky Secure Mobility Management. Сначала загрузите инсталляционный APK-файл. Затем разместите установочный файл APK на Веб-сервере Kaspersky Security Center или на другом сервере, доступном для загрузки с устройства.

6. Нажмите **Продолжить**.

7. В открывшемся окне **Параметры профиля Android Enterprise** укажите следующие параметры:

   a. В разделе **Конфигурация EMM** введите параметры подключения устройства к Kaspersky Security Center в поле **Пользовательские данные JSON (по определению EMM)** в следующем формате:

   b. `{"serverAddress":"myServer.domain.com","serverPort":"12345","vsrv":"virtualServerID","groupName":"NOT_ASSIGNED_GROUP","eulas":"cmFuZG9tYmFzZTY0c3RyaW5n"}`.

      Сейчас поддерживаются следующие поля файла JSON:

      - `serverAddress` - адрес Kaspersky Security Center;
      - `serverPort` - номер порта для синхронизации мобильного устройства с Сервером администрирования по указанному адресу;
      - `vsrv` (необязательно) - Виртуальный Сервер администрирования;
      - `groupName` (необязательно) - имя подгруппы в разделе "Нераспределенные устройства";
      - `eulas` (необязательно) - список принятых лицензионных соглашений (массив двоичных идентификаторов длиной 16 байт).

      > Параметр `connectionString` больше не поддерживается для KME (Knox Mobile Enrollment).

   c. 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 разделе **Политика конфиденциальности, Лицензионные соглашения и Условия обслуживания**. Также вы можете добавить другие юридические документы вашей компании, необходимые для развертывания профиля Knox, по кнопке **Добавить юридическое соглашение**.

8. Нажмите **Сохранить**.

В результате новый профиль Knox 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.
- Администратор устанавливает приложение Knox Deployment из Google Play на свое мобильное устройство и переносит профиль Knox на устройства пользователей с помощью Bluetooth, Wi-Fi Direct или QR-кода.

После сброса настроек устройства к заводским профиль Knox будет установлен. После разворачивания профиля Knox устройство автоматически будет добавлено в консоль KME.

## 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, Wi-Fi Direct или QR-кода. Для этого потребуется мобильное устройство администратора, с помощью которого будет выполняться доставка профилей Knox на мобильные устройства пользователей.

Для добавления устройств с помощью приложения Knox Deployment должны быть выполнены следующие условия:

- На мобильных устройствах должны быть включены Bluetooth или Wi-Fi в зависимости от выбранного режима доставки.
- Мобильные устройства должны быть подключены к интернету.

*Чтобы доставить профиль Knox с помощью приложения Knox Deployment:*

1. Установите на мобильное устройство администратора приложение Knox Deployment из Google Play.
2. Запустите приложение Knox Deployment.
3. Введите данные своей учетной записи Samsung, чтобы войти в систему.
4. В окне **Knox Deployment** настройте параметры развертывания профиля Knox:
   a. В разделе **Knox services** выберите **Knox Mobile Enrollment**.
   b. Выберите нужный профиль Knox из списка.

c. Выберите **Режим развертывания**:

- **Bluetooth**. Установите продолжительность соединения Bluetooth и укажите, будет ли соединение Bluetooth автоматическим или ручным.

  При использовании Bluetooth вы можете добавить профиль Knox сразу на несколько устройств.

- **Wi-Fi Direct**. Укажите, будет ли соединение Wi-Fi Direct автоматическим или ручным. Следуйте указаниям на экране.

d. Нажмите **Начать развертывание**.

5. На принимающем устройстве нарисуйте жест плюса (+) в окне **Welcome**, чтобы начать развертывание.

6. В открывшемся меню **Knox Deployment** выберите, хотите ли вы использовать Bluetooth или Wi-Fi Direct для регистрации устройства:

   a. Если вы выбрали **Bluetooth**, подтвердите запрос на сопряжение, отображаемый на основном устройстве. После этого принимающее устройство загрузит профиль. Следуйте указаниям на экране.

   В результате после установки профиля Knox в консоли KME будет добавлено новое устройство с тегом **Bluetooth**.

   b. Если вы выбрали **Wi-Fi Direct**, следуйте инструкциям на экране.

   В результате после установки профиля Knox в консоли KME будет добавлено новое устройство с тегом **Wi-Fi**.

7. Когда принимающее устройство настроено, нажмите **Завершить развертывание** на основном устройстве, чтобы завершить регистрацию.

После сброса настроек устройства к заводским профиль Knox будет установлен.

*Чтобы доставить профиль Knox с помощью QR-кода:*

1. На принимающем устройстве нарисуйте жест плюса (+) в окне **Welcome**, чтобы начать развертывание.

2. В открывшемся меню **Knox Deployment** выберите **QR-код**.

3. В консоли KME выберите нужный профиль в разделе **Профили**.

4. Если рядом с названием профиля нет QR-кода, откройте параметры профиля и нажмите **Добавить QR-код** на второй странице.

5. Следуйте инструкциям на экране и сохраните профиль.

   Сгенерированный QR-код появится рядом с названием профиля.

6. Отсканируйте QR-код из консоли KME с помощью камеры на мобильном устройстве пользователя под управлением Android 10 или выше.

   В результате после установки профиля Knox в консоли KME будет добавлено новое устройство с тегом **QR-код**.

После сброса настроек устройства к заводским профиль Knox будет установлен.

## 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. Чтобы добавить поставщика Samsung-устройств в консоль KME, вам потребуется идентификатор посредника. Чтобы получить идентификатора посредника, вам необходимо отправить запрос поставщику. В запросе укажите ваш идентификатор клиента Knox.

*Чтобы просмотреть ваш идентификатор клиента Knox:*

1. Войдите в консоль Samsung Knox → **Knox Mobile Enrollment**.
2. Выберите раздел **Посредники**.
3. Ваш идентификатор отображается в поле **Идентификатор клиента Knox**.

После получения ответа от поставщика с идентификатором посредника зарегистрируйте поставщика в консоли KME. Перед регистрацией поставщика вы можете создать профиль Knox, чтобы автоматически разворачивать его при добавлении новых устройств.

*Чтобы зарегистрировать официального поставщика в консоли KME:*

1. Войдите в консоль Samsung Knox → **Knox Mobile Enrollment**.
2. Выберите раздел **Посредники**.
3. Нажмите **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, в окне регистрации поставщика выберите Knox профиль.

   При добавлении новых устройств автоматически устанавливается профиль Knox.

   Подробная информация о настройке других параметров приведена на сайте технической поддержки Samsung.
6. Нажмите **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 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 с приложением Knox.

# Установка приложения

Перед установкой приложения Kaspersky Endpoint Security для Android выпустите мобильный сертификат для пользователей мобильных устройств в Kaspersky Security Center Web Console. Мобильный сертификат требуется для идентификации пользователя мобильного устройства в Kaspersky Security Center Web Console.

*Чтобы доставить профиль Knox на устройства:*

1. Войдите в консоль Samsung Knox → **Knox Mobile Enrollment**.
2. Выберите раздел **Устройства** → **Все устройства**.
3. Выберите устройства, на которые вы хотите установить профиль Knox.

   Откроется окно **Информация об устройстве**.
4. В списке **Профили** выберите профиль Knox с приложением Kaspersky Endpoint Security для Android.
5. В поле **Теги** введите теги для группировки и маркировки устройств, а также для оптимизации поиска в консоли KME.
6. 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 (**Имя** и **Пароль** в свойствах учетной записи пользователя).

   Чтобы получить мобильный сертификат только с паролем и без логина, введите значение `"DO_NOT_USE_LOGIN"` в поле **Идентификатор пользователя**. Kaspersky Endpoint Security для Android не будет использовать логин для запроса сертификата.
7. Выберите профиль Knox для остальных устройств.
8. Нажмите **Сохранить**.

После сброса настроек устройства к заводским профиль Knox будет установлен.

После начала развертывания профиля Knox на мобильном устройстве автоматически будет загружен установочный файл APK. Установка приложения Kaspersky Endpoint Security для Android запустится автоматически. Дополнительной настройки приложения не требуется. После первоначальной настройки устройства и установки программы синхронизация с Kaspersky Security Center будет выполнена автоматически. Мобильное устройство будет добавлено в Kaspersky Security Center Web Console.

# Настройка Knox

Этот раздел содержит информацию о работе с Knox на Samsung-устройствах.

Использование Knox доступно только на Samsung-устройствах под управлением Android 6 или выше.

## Настройка ограничений на использование SD-карт в Knox

Настройте ограничения для SD-карт, чтобы контролировать их использование на устройстве Samsung с поддержкой Knox.

*Чтобы ограничить использование SD-карт на мобильном устройстве:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Параметры Samsung Knox**.
4. На карточке **Ограничения функций устройств** нажмите **Параметры**.

   Откроется окно **Ограничения функций устройств**.
5. Включите параметры с помощью переключателя **Ограничения функций устройств**.
6. В разделе **Параметры SD-карты** укажите необходимые ограничения:

   - **Запретить доступ к SD-карте**

     Этот параметр применим для устройств с Android 5-12.

     Установка или снятие этого флажка определяет, включен или отключен доступ к SD-карте на устройстве.

     По умолчанию флажок снят.

   - **Запретить запись на SD-карту**

     Установка или снятие этого флажка определяет, включена или отключена запись на SD-карту на устройстве.

     По умолчанию флажок снят.

- **Запретить перенос приложений на SD-карту**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства перемещать приложения на SD-карту.

  По умолчанию флажок снят.

7. В разделе **Дополнительные параметры** можно указать дополнительные ограничения:

   - **Запретить отправку отчетов о сбоях в Google**

     Этот параметр применим только для устройств под управлением Android 11 или ниже.

     Если флажок установлен, Kaspersky Endpoint Security для Android блокирует отправку отчетов о сбоях в Google.

     Если флажок снят, отправка отчетов разрешена.

     По умолчанию флажок снят.

   - **Запретить режим разработчика**

     Этот параметр применим только для устройств с Android 11 или ниже.

     Если флажок установлен, пользователю запрещено включать режим разработчика на устройстве.

     Если флажок снят, пользователю разрешено включать режим разработчика на устройстве.

     По умолчанию флажок снят.

8. Нажмите **OK**.

9. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

   Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Kaspersky Security Center. Параметры SD-карты настроены.

## Настройка VPN в Knox

Для безопасного подключения Android-устройства к интернету и защиты передачи данных можно настроить параметры VPN (Virtual Private Network).

Настройка VPN возможна только для Samsung-устройств под управлением Android 11 или ниже.

При использовании виртуальной частной сети необходимо учитывать следующие требования:

- Приложение, использующее VPN-соединение, должно быть разрешено в параметрах **Сетевой экран**.
- Параметры VPN, 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:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Параметры Samsung Knox**.
4. На карточке **VPN** нажмите **Параметры**.

   Откроется окно **VPN**.
5. Включите параметры с помощью переключателя **VPN**.
6. Укажите следующие параметры VPN:
   - Параметры в разделе **Сеть**:
     - В поле **Имя сети** введите имя VPN-туннеля.
     - В раскрывающемся списке **Протокол** выберите тип VPN-соединения:
       - **IPSec Xauth PSK**. Туннельный протокол типа "шлюз-шлюз", позволяющий пользователю мобильного устройства устанавливать защищенное соединение с VPN-сервером с использованием утилиты авторизации Xauth.
       - **L2TP IPSec PSK**. Туннельный протокол типа "шлюз-шлюз", позволяющий пользователю мобильного устройства устанавливать защищенное соединение с VPN-сервером по протоколу IKE с использованием предварительно установленного ключа. Это протокол выбран по умолчанию.
       - **PPTP**. Туннельный протокол типа "точка-точка", позволяющий пользователю мобильного устройства устанавливать защищенное соединение с VPN-сервером за счет создания специального туннеля в стандартной, незащищенной сети.
     - В поле **Адрес сервера** введите сетевое имя или IP-адрес VPN-сервера.
   - Параметры в разделе **Параметры протокола**:
     - 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.

- В поле **DNS-сервер(ы)** введите полное доменное имя или IP-адрес DNS-сервера.

  Вы можете ввести несколько DNS-серверов через пробел.

- 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.

7. Дополнительно настройте следующие параметры:

   - Для протоколов **IPSec Xauth PSK** и **L2TP IPSec PSK**:

     - В поле **Общий ключ IPSec** введите пароль от предварительно установленного ключа безопасности IPSec.

     - В поле **Идентификатор IPSec** введите имя пользователя мобильного устройства.

   - Для типа протокола **L2TP IPSec PSK** укажите пароль для ключа L2TP в поле **Ключ L2TP**.

   - 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.

8. Нажмите **Сохранить**, 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 на мобильном устройстве можно настроить параметры почтового ящика Exchange.

> Почтовый ящик Exchange можно настроить только для устройств Samsung под управлением Android 9 или ниже.

*Чтобы настроить почтовый ящик Exchange на мобильном устройстве пользователя:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Параметры Samsung Knox**.

4. На карточке **Exchange ActiveSync** нажмите **Параметры**.

   Откроется окно **Exchange ActiveSync**.

5. Включите параметры с помощью переключателя **Exchange ActiveSync**.

6. В поле **Адрес сервера** введите IP-адрес или DNS-имя сервера, на котором размещен почтовый сервер.
7. В поле **Имя домена** введите доменное имя пользователя мобильного устройства в корпоративной сети.
8. В раскрывающемся списке **Период синхронизации** выберите период синхронизации мобильного устройства с сервером Microsoft Exchange.
9. Чтобы использовать транспортный протокол передачи данных SSL, установите флажок **Использовать SSL-соединение**. Протокол SSL использует шифрование и проверку подлинности на основе сертификатов для защиты передачи данных. По умолчанию флажок установлен.
10. Чтобы использовать цифровые сертификаты для защиты передачи данных между мобильным устройством пользователя и сервером Microsoft Exchange, установите флажок **Проверять сертификат сервера**. Будет выполняться проверка, выписан ли сертификат сервера с помощью доверенного корневого сертификата. По умолчанию флажок установлен.
11. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

## Настройка APN в Knox

APN можно настроить только для устройств Samsung.

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) на мобильном устройстве пользователя:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Выберите **Android** и перейдите в раздел **Параметры Samsung Knox**.
4. На карточке **Параметры APN** нажмите **Параметры**.

   Откроется окно **Параметры APN**.
5. Включите параметры с помощью переключателя **Параметры APN**.

   Переключатель на этой карточке не включает и не выключает соответствующую функциональность на устройствах. Включение переключателя позволяет настроить пользовательские параметры. Выключение переключателя позволяет использовать параметры по умолчанию.

6. Укажите следующие параметры точки доступа для подключения пользователя к услуге передачи данных:

   - В раскрывающемся списке **Тип APN** выберите тип точки доступа для передачи данных в мобильной сети GPRS/3G/4G:

     - **Интернет**. Подключение мобильного устройства пользователя к интернету.

     - **MMS**. Обмен мультимедийными сообщениями MMS.

     - **Интернет и MMS**. Подключение к интернету и обмен мультимедийными сообщениями. Это значение установлено по умолчанию.

   - В поле **Имя APN** укажите имя точки доступа.

   - В поле **MCC** укажите мобильный код страны (MCC).

   - В поле **MNC** укажите мобильный код сети (MNC).

7. Если в качестве типа точки доступа вы выбрали **MMS** или **Интернет и MMS**, укажите следующие дополнительные параметры для MMS в разделе **Сервер MMS**:

   - В поле **Имя сервера MMS** укажите полное доменное имя сервера мобильного оператора для обмена MMS (например, `mms.mobile.com`).

   - В поле **Адрес прокси-сервера MMS** введите имя сети или IP-адрес прокси-сервера.

   - В поле **Порт прокси-сервера MMS** укажите номер порта сервера мобильного оператора для обмена MMS.

8. В разделе **Аутентификация** укажите параметры аутентификации:

   - В раскрывающемся списке **Тип аутентификации** выберите тип аутентификации пользователя мобильного устройства на сервере мобильного оператора для доступа к сети. По умолчанию аутентификация пользователя не требуется. Доступны следующие типы:

     - **Нет**. Для доступа к мобильной сети аутентификация пользователя не требуется.

     - **PAP** (протокол аутентификации по паролю). Протокол аутентификации, использующий пароли в виде простого незашифрованного текста.

     - **CHAP** (Challenge Handshake Authentication Protocol). Протокол аутентификации типа "запрос-ответ", использующий стандартную схему хеширования MD5 для шифрования ответа.

     - **Совместно**. Совместное использование протоколов CHAP и PAP.

   - В поле **Имя пользователя** укажите имя пользователя для авторизации в мобильной сети.

   - В поле **Пароль** укажите пароль для авторизации пользователя в мобильной сети.

9. В разделе **Сеть** укажите следующие параметры сети:

   - В поле **Имя сети** введите название сети.

   - В поле **Адрес сервера** укажите сетевое имя сервера оператора мобильной связи, через который осуществляется доступ к услугам передачи данных.

10. В разделе **Прокси-сервер** укажите следующие параметры прокси-сервера:

    - Установите флажок **Использовать прокси-сервер**, чтобы разрешить использование прокси-сервера. По умолчанию флажок снят.

    - В поле **Адрес прокси-сервера** укажите сетевое имя или IP-адрес прокси-сервера мобильного оператора для доступа к сети. Это поле доступно, только если установлен флажок **Использовать прокси-сервер**.

    - В поле **Порт прокси-сервера** укажите номер порта прокси-сервера мобильного оператора для доступа к сети. Это поле доступно, только если установлен флажок **Использовать прокси-сервер**.

11. Нажмите **ОК**.

12. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

## Настройка Сетевого экрана в Knox

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

Сетевой экран можно настроить только для следующих режимов работы устройств Samsung:

- корпоративное устройство;
- личное устройство под управлением Android 15 или ниже;
- устройство с корпоративным контейнером под управлением Android 15 или ниже.

*Чтобы настроить Сетевой экран на мобильном устройстве пользователя:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.

2. В окне свойств политики выберите **Параметры приложения**.

3. Выберите **Android** и перейдите в раздел **Параметры Samsung Knox**.

4. На карточке **Сетевой экран** нажмите **Параметры**.

   Откроется окно **Сетевой экран**.

5. Включите параметры с помощью переключателя **Сетевой экран**.

6. В раскрывающемся списке **Доступ в интернет** выберите режим Сетевого экрана. В соответствии с режимом работы Сетевой экран контролирует соединения на мобильном устройстве пользователя:

    - Если вы хотите разрешить входящие и исходящие соединения для всех установленных приложений, выберите **Разрешить для всех приложений**. Этот режим выбран по умолчанию.

    - Если вы хотите заблокировать сетевую активность для всех приложений, кроме нескольких указанных, выберите **Разрешить для указанных приложений**.

7. Если выбран режим Сетевого экрана **Разрешить для указанных приложений**, создайте список приложений, которым разрешена вся сетевая активность:

   a. В разделе **Приложения с доступом в интернет** нажмите **Добавить**.

      Откроется окно **Добавить приложение**.

   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 **Добавить**.

   Новое приложение, для которого выключен Сетевой экран, появится в списке.

   > Вы можете изменять или удалять мобильные приложения из списка с помощью кнопок **Изменить** и **Удалить** в верхней части списка.

8. Нажмите **ОК**.

9. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

# 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 7 или 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-Защита.

Веб-Защита блокирует вредоносные сайты, цель которых – распространить вредоносный код, а также фишинговые сайты, цель которых – украсть ваши конфиденциальные данные и получить доступ к вашим финансовым счетам. Веб-Защита проверяет 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 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 корпоративном контейнере невозможно автоматически устранить угрозу, обнаруженную во внешней памяти устройства (например, на SD-карте). У Kaspersky Endpoint Security для Android в корпоративном контейнере 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:*

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:*

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 корпоративном контейнере невозможно автоматически устранить угрозу, обнаруженную во внешней памяти устройства (например, на SD-карте). У Kaspersky Endpoint Security для Android в корпоративном контейнере 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:*

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 Android-устройств 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:*

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):*

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:*

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**.

При использовании Kaspersky Endpoint Security для Android может возникнуть проблема **Обнаружена блокировка доменного имени службы "Лаборатории Касперского"**, что означает, что проблемы сети не дают приложению связаться со службами "Лаборатории Касперского". Это может повлиять на работу Защиты от вредоносного ПО и угрожать безопасности ваших данных. Изменение параметров подключения может решить возникшую проблему.

В этом разделе приведены общие инструкции. Для более подробной информации обратитесь к руководству пользователя для вашего устройства.

*Чтобы изменить параметры подключения:*

1. Перейдите в раздел **Настройки** на устройстве.
2. Откройте настройки подключения.
3. Перейдите в раздел **Частный DNS-сервер**.
4. Выберите **Имя хоста частного DNS-провайдера** и введите имя DNS-сервера. Например, можно ввести "dns.google", чтобы использовать общедоступные DNS-серверы Google.
5. Сохраните изменения.

Параметры подключения будут изменены.

# Обновление баз по расписанию

Приложение может автоматически обновлять базы вредоносного ПО по заданному расписанию.

*Чтобы настроить расписание обновления:*

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 Android-устройств 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-Защита

Для включения Веб-Защиты 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 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-Защита будет недоступна.

В Яндекс Браузере и Samsung Internet вредоносные и фишинговые веб-адреса могут оставаться незаблокированными. Это связано с тем, что проверяется только домен сайта. Если он является вредоносным или фишинговым, Веб-Защита блокирует угрозу. Если домен не был классифицирован как вредоносный или фишинговый, конкретный веб-адрес не блокируется.

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

Если на корпоративном устройстве приложение Kaspersky Endpoint Security для Android не установлено в качестве службы Специальных возможностей, Веб-Защита поддерживается только браузером Google Chrome и проверяет только домен сайта. Чтобы Веб-Защита поддерживалась другими браузерами (Samsung Internet, 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.

Чтобы использовать Веб-Защиту в приложении Telegram, выключите просмотр ссылок во встроенном браузере в настройках Telegram.

В браузерах HUAWEI Browser, Samsung Internet и Яндекс Браузер Веб-Защита не блокирует сайты на мобильном устройстве, если используется корпоративный контейнер и установлен флажок Включить Веб-Защиту только в корпоративном контейнере.

Для постоянного использования Веб-Защиты для проверки сайтов во время работы в интернете, назначьте Google Chrome, HUAWEI Browser, Samsung Internet или Яндекс Браузер браузером по умолчанию.

*Чтобы назначить поддерживаемый браузер браузером по умолчанию и использовать Веб-Защиту для постоянной проверки сайтов:*

1. В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **Веб-Защита**.
2. Включите переключатель **Веб-Защита**.
3. Нажмите **Установить браузер по умолчанию**.

   Эта кнопка отображается, если Веб-Защита включена, 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 будет назначен браузером по умолчанию. Веб-Защита будет постоянно проверять сайты во время работы в интернете.

## Проверка уведомлений от мессенджеров

Kaspersky Endpoint Security для Android может обнаруживать вредоносные и фишинговые веб-адреса в уведомлениях от Telegram, MAX, WhatsApp, приложения для SMS и других распространенных мессенджеров. Проверяются только веб-адреса, указанные в открытом виде. Гиперссылки внутри текста не проверяются.

Для включения проверки уведомлений должны быть выполнены следующие условия:

- Включена Веб-Защита.
- Для нужных мессенджеров разрешено отображение уведомлений. Kaspersky Endpoint Security для Android проверяет только уведомления, которые могут быть показаны на экране устройства.
- На устройствах Google Pixel и Vivo выдано разрешение "Разговоры" для Kaspersky Endpoint Security в настройках доступа к уведомлениям.

*Чтобы разрешить доступ к уведомлениям для их проверки:*

1. В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **Веб-Защита**.
2. Включите переключатель **Блокировать уведомления, содержащие вредоносные и фишинговые веб-адреса**.

   Откроется окно **Необходим доступ к уведомлениям**.
3. Нажмите **Продолжить**.

   Откроется соответствующий раздел настроек.
4. Включите переключатель Kaspersky Endpoint Security.
5. В открывшемся окне разрешите приложению просматривать все уведомления.
6. Вернитесь в Kaspersky Endpoint Security.

Теперь приложение проверяет уведомления на наличие вредоносных и фишинговых веб-адресов. Если обнаружен опасный веб-адрес, уведомление блокируется и появляется блокирующий экран с информацией о заблокированном уведомлении.

Если Kaspersky Endpoint Security не включен в качестве службы Специальных возможностей, то вместо отображения блокирующего экрана приложение пришлет push-уведомление об обнаруженных опасных веб-адресах. При нажатии на это push-уведомление появится экран с информацией о заблокированных уведомлениях.

# Получение сертификата

*Чтобы получить сертификат для доступа к ресурсам сети организации:*

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:*

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**.

# Предоставление удаленного доступа к вашему устройству

Администратор может запросить удаленный доступ к вашему устройству. В этом случае после очередной синхронизации вашего устройства с Kaspersky Security Center вы получите уведомление с предложением подключиться к сессии удаленного управления.

Во время сессии администратор сможет просматривать экран устройства, делать снимки экрана и выполнять действия на устройстве. Kaspersky Endpoint Security для Android будет информировать вас о статусе удаленного подключения. Вы можете прекратить сессию в любое время.

Прежде чем подключиться к сессии удаленного управления:

- Примите предложенные вам соглашения. Они содержат информацию о функциональности удаленного управления.
- Включите специальные возможности для Kaspersky Endpoint Security для Android.
- Разрешите просмотр экрана устройства. Это разрешение необходимо предоставлять каждый раз перед началом демонстрации экрана.

*Чтобы начать сессию удаленного управления:*

1. Убедитесь, что предложенные соглашения приняты, а для Kaspersky Endpoint Security для Android включены специальные возможности.
2. Нажмите **Разрешить** в полученном уведомлении или запросе на начало сессии удаленного управления.

   Уведомление приходит после синхронизации устройства с Kaspersky Security Center. Если синхронизация не происходит автоматически, администратор может попросить вас синхронизировать устройство вручную.
3. Предоставьте разрешение на просмотр всего экрана устройства.
4. В окне с инструкциями по подключению к сессии нажмите **Разрешить и начать сессию**.

   Начинается сессия удаленного управления.

   Если вы хотите завершить сессию, нажмите **Остановить**.

# 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:*

1. В сообщении, 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 на корпоративные устройства

*Корпоративное устройство* – это режим работы корпоративных Android-устройств. Этот режим позволяет администратору осуществлять полный контроль над устройством и настраивать множество функций.

Перед установкой приложения на корпоративное устройство необходимо выполнить сброс настроек устройства до заводских и провести предварительную настройку.

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 с Android 7 или 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 на корпоративных устройствах с Android 7 или выше

Для развертывания приложения на корпоративных устройствах нужно сбросить настройки устройств до заводских и установить приложение, используя QR-код, сгенерированный в Kaspersky Security Center. QR-код содержит все необходимые данные для настройки приложения.

*Чтобы установить приложение Kaspersky Endpoint Security для Android на корпоративном устройстве.*

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 корпоративном устройстве.

# Настройка приложения на корпоративных устройствах с Android 5-6

На корпоративных устройствах с Android 5–6 процедура настройки приложения 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.

*Чтобы развернуть Kaspersky Endpoint Security для Android на корпоративном устройстве с Android 5–6:*

1. Сбросьте настройки устройства до заводских. Если устройство ранее не использовалось, пропустите этот шаг и перейдите к шагу 2.

   Если вы установили пароль разблокировки экрана на устройстве после сброса его до заводских настроек, нужно снова сбросить устройство до заводских настроек перед установкой приложения с помощью ADB.

2. 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.

3. Перейдите в раздел **Параметры** → **Параметры разработчика** и включите параметр **Отладка по USB**.

4. Разрешите установку приложений, полученных не из Google Play. Для этого:

   a. Перейдите в раздел **Параметры** → **Безопасность**.

   b. Включите параметр **Неизвестные источники**.

5. Для установки Kaspersky Endpoint Security для Android на устройство используйте пакет установки, загруженный из Kaspersky Security Center, или другой подходящий способ (например, файл в формате APK).

6. 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 9).

7. Установите ADB на компьютер.

8. Подключите устройство к компьютеру с помощью USB-кабеля.

   Появится диалоговое окно с запросом на разрешение отладки устройства на компьютере. Нажмите **OK**.

9. Запустите ADB и выполните следующую команду:

   `adb shell dpm set-device-owner com.kaspersky.kes/com.kms.selfprotection.DeviceAdmin`.

10. 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 корпоративные устройства и устройства с корпоративным контейнером такие сертификаты устанавливаются автоматически. На личных устройствах вы 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 корпоративные устройства или устройства с корпоративным контейнером такие 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 пространстве пользователя 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:*

1. Откройте страницу **Специальные возможности** в настройках устройства и найдите Kaspersky Endpoint Security.
2. Включите переключатель Kaspersky Endpoint Security. В окне, в котором говорится, что доступ к специальным возможностям ограничен, нажмите **ОК**.

   Теперь вы можете предоставить Kaspersky Endpoint Security доступ к ограниченным настройкам.
3. Откройте страницу с информацией о Kaspersky Endpoint Security в настройках устройства. Например, перейдите в **Настройки** > **Приложения**, а затем найдите приложение в списке.
4. На странице с информацией о Kaspersky Endpoint Security нажмите ⋮ в правом верхнем углу и выберите **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:*

1. В окне включения служб специальных возможностей нажмите **Включить**.

   Откроется страница **Специальные возможности** в настройках устройства.
2. Включите переключатель Kaspersky Endpoint Security. В окне, в котором говорится, что доступ к специальным возможностям ограничен, нажмите **ОК**.

   Теперь вы можете предоставить Kaspersky Endpoint Security доступ к ограниченным настройкам.
3. Откройте страницу с информацией о Kaspersky Endpoint Security в настройках устройства. Например, перейдите в **Настройки** > **Приложения**, а затем найдите приложение в списке.

4. На странице с информацией о Kaspersky Endpoint Security нажмите ⋮ в правом верхнем углу и выберите **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 корпоративных устройствах 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 7 или 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"

Приложения, отмеченные значком портфеля (корпоративные приложения), хранятся на вашем устройстве в корпоративном контейнере. *Корпоративный контейнер* – это безопасная среда на вашем устройстве, в которой администратор может управлять приложениями и учетными записями, не ограничивая ваши возможности работы с персональными данными.

Корпоративный контейнер позволяет хранить корпоративные данные отдельно от персональных данных. Это обеспечивает конфиденциальность корпоративных данных и их защиту от вредоносных приложений. При создании корпоративного контейнера на вашем устройстве в корпоративный контейнер 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 Protection для iOS

В этом разделе справки описаны функции и действия, доступные пользователям приложения Kaspersky Protection 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 Protection для iOS обладает следующими основными возможностями.

### Защита от интернет-угроз

Для защиты от интернет-угроз используется компонент Веб-Защита.

Веб-Защита блокирует вредоносные сайты, цель которых – распространить вредоносный код, а также фишинговые сайты, цель которых – украсть ваши конфиденциальные данные и получить доступ к вашим финансовым счетам. Веб-Защита проверяет сайты перед открытием, используя облачную службу Kaspersky Security Network.

Проверяется только домен сайта. Если он является вредоносным или фишинговым, Веб-Защита блокирует угрозу. Если домен является доверенным, сайт не блокируется.

Веб-Защита также проверяет сетевую активность приложений на вашем устройстве.

Чтобы Веб-Защита работала, вы должны разрешить приложению добавлять конфигурацию VPN.

### Обнаружение модификации прошивки (jailbreak)

Если приложение Kaspersky Protection 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 Protection для iOS, выполните следующие действия:*

1. Найдите в электронной почте письмо от вашего администратора с приглашением установить приложение Kaspersky Protection для iOS из App Store.
2. Перейдите в App Store одним из следующих способов:
   - Если вы открыли письмо на iOS-устройстве, на котором хотите установить приложение, нажмите на ссылку в этом письме.
   - Если вы открыли письмо на компьютере, отсканируйте QR-код с помощью iOS-устройства, 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 Protection для iOS будет установлено на вашем устройстве. Чтобы защитить устройство, активируйте приложение.

# Активация приложения

*Чтобы активировать приложение Kaspersky Protection 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 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 Protection для iOS на вашем устройстве будет активировано.

# Активация приложения с помощью кода активации

Когда вы устанавливаете приложение Kaspersky Protection 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 Protection 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 Protection 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.

# Использование диагностики для устранения неисправностей

Если у вас возникают проблемы с Kaspersky Protection для iOS, специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас прислать им *файл с диагностической информацией*. Этот файл позволяет специалистам Службы технической поддержки отследить причины проблем в работе приложения.

Чтобы поделиться файлом с диагностической информацией, в Kaspersky Protection для iOS должна быть включена диагностика.

Мы рекомендуем включать диагностику только под руководством специалиста Службы технической поддержки "Лаборатории Касперского".

Сохранение диагностической информации может снижать скорость интернет-соединения, а также скорость работы устройства, Kaspersky Protection для iOS и других приложений.

Файл с диагностической информацией можно удалить вручную в приложении Файлы.

Чтобы включить диагностику:

1. В главном окне нажмите ⓘ.
2. В открывшемся окне **О приложении** нажмите **Диагностика**.
3. В открывшемся окне **Диагностика** включите диагностику с помощью переключателя **Диагностика**.
4. Примите Положение о технической поддержке. В Положении о технической поддержке описаны данные, сохраняемые в файле с диагностической информацией.
5. Нажмите **ОК**.

На устройстве будет включена диагностика. Данные о работе Kaspersky Protection для iOS будут сохраняться в файл с диагностической информацией. При возникновении проблем вы можете поделиться этим файлом со специалистом Службы технической поддержки "Лаборатории Касперского".

# Удаление приложения

*Чтобы удалить приложение Kaspersky Protection для iOS, выполните стандартную процедуру удаления на платформе iOS:*

1. На главном экране коснитесь и удерживайте значок приложения.
2. Удалите приложение.

Приложение Kaspersky Protection для iOS будет удалено с вашего устройства.

# 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 Protection 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.
- В разделе **Общие** → **Лицензионные соглашения** в свойствах Сервера администрирования в Kaspersky Security Center Web Console.
- На шаге 4 процесса подключения мобильных устройств к Kaspersky Security Center Web Console, если на шаге 3 был выбран **Администратор**. Администратору будет предложено принять Лицензионное соглашение.
- При установке приложения, если на шаге 3 процесса подключения мобильных устройств к Kaspersky Security Center Web Console были выбраны **Пользователи**. Пользователю мобильного устройства будет предложено принять Лицензионное соглашение.

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 решение.

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 мобильные приложения Kaspersky Endpoint Security для Android и Kaspersky Protection для iOS прекращают выполнять большинство функций, кроме синхронизации с Сервером администрирования. Чтобы продолжить использование приложений, 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 политики).

  - Приложение Kaspersky Protection для iOS:

    - Синхронизация с Сервером администрирования.

    Kaspersky Protection для iOS прекращает обмен информацией с Kaspersky Security Network, если срок действия пробной лицензии истек или лицензия отсутствует (код активации удален из политики).

Остальные компоненты мобильных приложений недоступны пользователю устройства, и вы не можете настраивать параметры политик.

Чтобы продолжить использование всех функций приложений и настраивать параметры политик, 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 бесперебойную защиту компьютера от всех угроз безопасности.

С лицензией без поддержки расширенной функциональности Kaspersky Secure Mobility Management в плагине Kaspersky Mobile Devices Protection and Management доступны только базовые параметры защиты устройств.

# Просмотр информации о лицензии

Плагин Kaspersky Mobile Devices Protection and Management позволяет просматривать следующую информацию о действующей лицензии:

- лицензионный ключ;
- количество устройств, на которых можно использовать лицензионный ключ;
- тип лицензии;
- дата и время окончания срока действия лицензии;
- количество дней до завершения срока действия лицензии;
- тип функциональности, доступной по действующей лицензии.

*Чтобы просмотреть информацию о действующей лицензии:*

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Политики**. В открывшемся списке политик выберите политику, которую вы хотите настроить.
2. В окне свойств политики выберите **Параметры приложения**.
3. Нажмите **Лицензия**.

Откроется окно **Лицензия**, содержащее информацию о лицензии.

# 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 Protection 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 Protection 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 Protection 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 Mobile Devices Protection and Management 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-Защита** и **Веб-Контроль.** Приложение выполняет проверку 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-Защиты, 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.

Если последняя версия Положения о Kaspersky Security Network не принята, в Kaspersky Security Network отправляется только статистика, указанная в ранее принятой версии Положения.

## 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-Защиты. Заявленная цель включает обнаружение веб-угроз и определение категорий посещаемых веб-сайтов с помощью 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 службы 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 Protection 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;
- Положение о технической поддержке.

Пользователь может просмотреть условия этих документов в любое время в разделе **О приложении** → **Соглашения и положения** в настройках Kaspersky Protection 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 Protection для iOS использует облачную службу Kaspersky Security Network в работе компонента **Веб-Защита**. 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-Защита, 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 Protection 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.

## Предоставление данных в рамках Положения о технической поддержке

Когда в Kaspersky Protection для iOS включена диагностика, приложение обрабатывает и сохраняет следующие персональные данные для дальнейшего анализа Службой технической поддержки:

- Дата и время события.

- HTTP-коды и данные по сетевым запросам к системам Правообладателя: тело запроса; URL запроса; ответы сервера; ошибки.

- Данные по всем сетевым запросам: URL запроса; статус проверки трафика.

- Информация о лицензии: идентификатор и код активации; срок действия пакета данных о текущей лицензии; текущий статус ключа ПО; режим работы после истечения лицензии; дата активации ПО; дата окончания срока действия лицензии; номер заказа, для которого была выписана данная лицензия.

- Информация о подключении к Серверу администрирования: пароль для получения сертификата; адрес Сервера администрирования; уникальный идентификатор устройства; данные о пользовательских сертификатах; данные о сертификатах Сервера администрирования; настройки ПО полученные от Сервера администрирования.

- Системные события: открытие и закрытие ПО; push-уведомления от ПО.

- Информация о работе ПО и его модулей.
- Версия ОС; тип ОС.
- Идентификатор устройства; тип устройства.
- Идентификатор ПО; идентификатор языка ПО; версия ПО; идентификатор установки ПО.
- Информация об ошибках ПО.

Предоставление указанных данных Службе технической поддержки является добровольным.

# Сравнение функций решения в зависимости от средства управления

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

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

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

Доступность функций решения в зависимости от средства управления

| | Консоль администрирования | Web Console |
|---|---|---|
| **Управление мобильными устройствами** | | |
| Управление Android-устройствами | Доступно | Доступно |
| Управление iOS-устройствами | Доступно | Доступно |
| Защита устройств на ОС Аврора | Недоступно | Доступно |
| **Развертывание** | | |
| Добавление устройств с помощью ссылки на App Store | Доступно | Доступно |
| Добавление устройств путем создания инсталляционного пакета | Доступно | Доступно |
| Добавление устройств напрямую в группу администрирования после подключения | Недоступно | Доступно |
| Создание политик, разделенных по режимам работы | Недоступно | Доступно |
| Отправка команд на мобильные устройства | Доступно | Доступно |
| Удаление мобильных устройств из Kaspersky Security Center | Доступно | Доступно |
| **Управление сертификатами** | | |
| Выпуск почтовых сертификатов | Доступно | Доступно |
| Выпуск VPN-сертификатов | Доступно | Доступно |
| Выпуск мобильных сертификатов | Доступно | Доступно |
| Выпуск мобильных сертификатов средствами Сервера администрирования | Доступно | Доступно |
| Выбор файлов сертификатов | Доступно | Доступно |
| Интеграция с инфраструктурой открытых ключей | Доступно | Доступно |
| **Управление политиками** | | |
| Доступ к параметрам групповых политик на основе ролей | Доступно | Доступно |
| Настройка синхронизации мобильных устройств с Kaspersky Security Center | Доступно | Доступно |
| Настройка поиска вредоносного ПО на мобильных устройствах | Доступно | Доступно |
| Настройка обновления баз вредоносного ПО | Доступно | Доступно |
| Настройка защиты устройств в интернете | Доступно | Доступно |
| Настройка защиты данных при потере или краже устройства | Доступно | Доступно |
| Настройка надежности пароля разблокировки устройства | Доступно | Доступно |
| Настройка доступа пользователей к сайтам | Доступно | Доступно |
| Настройка Контроля приложений | Доступно | Доступно |

| | Консоль администрирования | Web Console |
|---|---|---|
| Настройка Контроля соответствия | Доступно | Доступно |
| Настройка правил предоставления разрешений для установленных приложений | Доступно | Доступно |
| Настройка рабочих профилей Android / корпоративных контейнеров | Доступно | Доступно |
| Настройка ограничений функций устройств | Доступно | Доступно |
| Настройка подключения к сетям Wi-Fi | Доступно | Доступно |
| Настройка VPN | Доступно | Доступно |
| Управление конфигурациями приложений | Доступно | Доступно |
| Отправка файлов на Android-устройства | Недоступно | Доступно |
| Samsung Knox | Доступно | Доступно |
| **Функции Сервера iOS MDM** | | |
| Установка и настройка Сервера iOS MDM | Доступно | Доступно |
| Выпуск APNs-сертификатов | Доступно | Доступно |
| Подключение iOS MDM-устройств | Доступно | Доступно |
| Подписание управляющего профиля сертификатом | Доступно | Доступно |
| События Сервера iOS MDM | Доступно | Доступно |
| Установка приложений | Доступно | Доступно |
| Добавление конфигурационного профиля | Доступно | Доступно |
| Добавление provisioning-профиля | Доступно | Недоступно |
| **Прочие функции** | | |
| Централизованное принятие условий Лицензионного соглашения в Kaspersky Security Center | Доступно | Доступно |
| Настройка Kaspersky Private Security Network | Доступно | 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 Protection 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 устройствами 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-устройство

Мобильное устройство на платформе iOS, находящееся под управлением Сервера iOS MDM.

## Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network – это решение, предоставляющее пользователям устройств с установленными программами "Лаборатории Касперского" доступ к репутационным базам данных Kaspersky Security Network и другим статистическим данным без отправки данных с устройств в Kaspersky Security Network. Kaspersky Private Security Network разработан для корпоративных клиентов, которые не могут участвовать в Kaspersky Security Network по следующим причинам:

- Устройства не подключены к интернету.
- Передача любых данных за пределы страны или корпоративной локальной сети запрещена законом или корпоративными политиками безопасности.

## Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к базе данных "Лаборатории Касперского" с постоянно обновляемой информацией о репутации файлов, веб-ресурсов и программного обеспечения. Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

## Manifest-файл

Файл в формате PLIST, содержащий ссылку на файл приложения (ipa-файл), расположенный на веб-сервере. Используется iOS-устройством для поиска, загрузки и установки приложений с веб-сервера.

## POP3

Сетевой протокол получения сообщений почтовым клиентом с почтового сервера.

## 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.

## Базовая защита

Режим работы личных iOS-устройств. Этот режим работы позволяет защищать устройства от веб-угроз и обнаруживать jailbreak на устройствах с помощью приложения Kaspersky Protection для iOS.

## Базовый контроль

Режим работы личных iOS-устройств. Этот режим работы позволяет защищать устройства и выполнять базовое управление ими.

## 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, управляющих 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).

## Корпоративное устройство

Режим работы Android-устройств, принадлежащих компании. Этот режим работы позволяет вам полностью контролировать устройство и настраивать расширенный набор параметров и функций безопасности.

## Корпоративный контейнер

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 на мобильном устройстве пользователя корпоративного контейнера в него автоматически устанавливаются следующие корпоративные приложения: Google Play, Google Chrome, Загрузки, Kaspersky Endpoint Security для Android и другие. Корпоративные приложения, размещенные в корпоративном контейнере, а также уведомления этих приложений, отмечены значком портфеля. Для приложения Google Play нужно создать отдельную корпоративную учетную запись Google. Приложения, установленные в корпоративном контейнере, отображаются в общем списке приложений.

## 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.

## Личное устройство

Режим работы личных Android-устройств. Этот режим работы позволяет защищать устройства и выполнять базовое управление ими.

## Плагин для управления мобильными устройствами

Специализированный компонент, предоставляющий интерфейс для управления мобильными устройствами через Kaspersky Security Center Web Console.

## 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

Устройство, на котором развернута Kaspersky Security Center Web Console. Используя рабочее место администратора с установленными плагинами для управления мобильными устройствами, администратор выполняет централизованное управление мобильными устройствами.

## Рабочий профиль Android

Автономный профиль, который можно настроить на Android-устройстве, чтобы обеспечить разделение рабочих и личных данных. Рабочий профиль Android позволяет организациям полностью контролировать рабочие приложения и данные на устройстве, в то время как личные приложения и данные пользователя остаются конфиденциальными.

## 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.

## Управляющий профиль

Профиль, который содержит набор параметров для подключения мобильных устройств iOS к Серверу администрирования. Управляющий 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 управляющий профиль нужно отправлять пользователю для того, чтобы Сервер iOS MDM мог обнаружить и подключить его мобильное устройство под управлением iOS.

## 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 Protection для iOS)
- legal_notices_KMDPM.txt (для плагина Kaspersky Mobile Devices Protection and Management)
- legal_notices_iOS_MDM.txt (для Сервера iOS MDM и плагина параметров Сервера iOS MDM)

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 в Соединенных Штатах и/или других странах.

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.

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.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

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 – является товарным знаком или зарегистрированным товарным знаком HTC Corporation и ее филиалов в США и/или других странах.

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.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Mail.ru – зарегистрированный товарный знак, правообладателем которого является ООО "Мэйл.Ру".

Microsoft, Active Directory, ActiveSync, Bing, Forefront, Microsoft Intune, Microsoft Edge, Outlook, SQL Server, 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.

Red Hat и Red Hat Enterprise Linux – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних 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.