

kaspersky

Kaspersky IoT Secure Gateway

© 2021 АО «Лаборатория Касперского»

Содержание

[О Kaspersky IoT Secure Gateway.](#)

[Комплект поставки](#)

[Аппаратные и программные требования](#)

[Типовая схема развертывания Kaspersky IoT Secure Gateway.](#)

[Компоненты Kaspersky IoT Secure Gateway.](#)

[Рекомендации по обеспечению безопасной работы Kaspersky IoT Secure Gateway.](#)

[Что нового](#)

[Включение и выключение устройства Advantech UTX-3117FS-S6A1N](#)

[Подключение к веб-интерфейсу Kaspersky IoT Secure Gateway.](#)

[Завершение и возобновление сеанса подключения к веб-интерфейсу Kaspersky IoT Secure Gateway.](#)

[Веб-интерфейс Kaspersky IoT Secure Gateway.](#)

[Цели и предположения безопасности](#)

[Обработка и хранение данных в Kaspersky IoT Secure Gateway.](#)

[Предоставление данных](#)

[О хранении журналов Kaspersky IoT Secure Gateway.](#)

[Лицензирование Kaspersky IoT Secure Gateway.](#)

[Настройка Kaspersky IoT Secure Gateway.](#)

[Сценарий: Быстрый старт для администратора](#)

[Сценарий: Настройка доступа из внешней сети к устройствам внутренней сети](#)

[Настройка параметров сети](#)

[Настройка параметров внутренней сети](#)

[Настройка параметров внешней сети](#)

[Настройка параметров подключения к Kaspersky Security Center](#)

[Настройка параметров сотового соединения](#)

[Таблица профилей модема](#)

[Включение и выключение сотового соединения](#)

[Создание профиля модема](#)

[Копирование профиля модема](#)

[Заполнение пустого профиля модема](#)

[Изменение профиля модема](#)

[Переключение на другой профиль модема](#)

[Удаление профиля модема](#)

[Управление безопасностью Kaspersky IoT Secure Gateway.](#)

[Создание сертификата сервера Kaspersky Security Center](#)

[Создание сертификата администратора](#)

[Обновление сертификатов](#)

[Настройка параметров MQTT-брокера](#)

[Таблица профилей MQTT-брокера](#)

[Создание профиля MQTT-брокера](#)

[Копирование профиля MQTT-брокера](#)

[Заполнение пустого профиля MQTT-брокера](#)

[Изменение профиля MQTT-брокера](#)

[Переключение на другой профиль MQTT-брокера](#)

[Удаление профиля MQTT-брокера](#)

[Ограничения при настройке MQTT-брокера](#)

[Настройка веб-сервера](#)

[Таблица профилей веб-сервера](#)

[Создание профиля веб-сервера](#)

[Копирование профиля веб-сервера](#)

[Заполнение пустого профиля веб-сервера](#)

[Изменение профиля веб-сервера](#)

[Переключение на другой профиль веб-сервера](#)

[Удаление профиля веб-сервера](#)

[Настройка отправки уведомлений при регистрации событий](#)

[Настройка отправки журналов событий на сервер Syslog](#)

[Настройка отправки push-уведомлений](#)

[Настройка отправки MQTT-уведомлений](#)

[Настройка даты и времени](#)

[Изменение языка веб-интерфейса Kaspersky IoT Secure Gateway.](#)

[Решение типовых задач](#)

[Мониторинг состояния Kaspersky IoT Secure Gateway.](#)

[Мониторинг состояния сотового соединения](#)

[Мониторинг устройств Kaspersky IoT Secure Gateway.](#)

[Просмотр списка устройств](#)

[Добавление и удаление устройств из списка разрешенных устройств](#)

[Мониторинг событий Kaspersky IoT Secure Gateway.](#)

[О событиях Kaspersky IoT Secure Gateway.](#)

[О журналах Kaspersky IoT Secure Gateway.](#)

[Обнаружение вторжений](#)

[Просмотр журнала безопасности сети](#)

[Просмотр журнала аудита](#)

[Экспорт журнала аудита](#)

[Экспорт журналов событий Kaspersky IoT Secure Gateway.](#)

[Управление программой через Kaspersky Security Center Web Console](#)

[О веб-плагине управления Kaspersky IoT Secure Gateway.](#)

[Установка веб-плагина управления Kaspersky IoT Secure Gateway.](#)

[Обновление веб-плагина управления Kaspersky IoT Secure Gateway.](#)

[Удаление веб-плагина управления Kaspersky IoT Secure Gateway.](#)

[Вход и выход из Kaspersky Security Center Web Console](#)

[Добавление устройства Kaspersky IoT Secure Gateway в группу управляемых устройств Kaspersky Security Center Web Console](#)

[Управление политиками](#)

[Настройка параметров Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console](#)

[Настройка параметров сети через Kaspersky Security Center Web Console](#)

[Настройка параметров сотового соединения Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console](#)

[Включение и выключение сотового соединения Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console](#)

[Создание профиля модема Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console](#)

[Изменение профиля модема Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console](#)

[Удаление профиля модема Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console](#)

[Управление сертификатами через Kaspersky Security Center Web Console](#)

[Просмотр списка профилей веб-сервера через Kaspersky Security Center Web Console](#)

[Настройка параметров MQTT-брокера через Kaspersky Security Center Web Console](#)

[Создание профиля MQTT-брокера через Kaspersky Security Center Web Console](#)

[Изменение профиля MQTT-брокера через Kaspersky Security Center Web Console](#)
[Удаление профиля MQTT-брокера через Kaspersky Security Center Web Console](#)
[Настройка уведомлений через Kaspersky Security Center Web Console](#)
[Настройка отправки уведомлений на сервер Syslog через Kaspersky Security Center Web Console](#)
[Настройка отправки push-уведомлений через Kaspersky Security Center Web Console](#)
[Настройка отправки MQTT-уведомлений через Kaspersky Security Center Web Console](#)
[Настройка параметров синхронизации с Kaspersky Security Center](#)
[Настройка даты и времени через Kaspersky Security Center Web Console](#)
[Управление событиями Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console](#)
[Просмотр событий Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console](#)
[Настройка регистрации событий Kaspersky IoT Secure Gateway в Kaspersky Security Center Web Console](#)
[Настройка маскардинга](#)
[Обновление и перезагрузка Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console](#)
[Управление системой предотвращения вторжений](#)
[Включение и выключение системы предотвращения вторжений](#)
[Добавление IP-адреса в список разрешенных IP-адресов](#)
[Удаление IP-адреса из списка разрешенных IP-адресов](#)
[Включение и выключение списка запрещенных IP-адресов](#)
[Управление межсетевым экраном](#)
[О правилах межсетевого экрана](#)
[Порядок обработки сетевого трафика](#)
[Создание правил межсетевого экрана](#)
[Изменение правил межсетевого экрана](#)
[Удаление правил межсетевого экрана](#)
[Обращение в Службу технической поддержки](#)
[Приложения](#)
[Подготовка к установке Kaspersky IoT Secure Gateway](#)
[Установка Kaspersky IoT Secure Gateway](#)
[Глоссарий](#)
[Kaspersky Security Center Web Console](#)
[KasperskyOS](#)
[Message Queuing Telemetry Transport \(MQTT\)](#)
[MQTT-брокер](#)
[MQTT-топик](#)
[SSL](#)
[TLS](#)
[Администратор Kaspersky Security Center](#)
[Безопасный шлюз Интернета вещей](#)
[Группа администрирования](#)
[Задача](#)
[Интернет вещей](#)
[Компонент Kaspersky IoT Secure Gateway](#)
[Плагин управления программой](#)
[Политика](#)
[Политика паролей](#)
[Сервер администрирования](#)
[Сертификат администратора](#)
[Сертификат сервера Kaspersky Security Center](#)

[Событие](#)

[Управляемые устройства](#)

[Устройство с защитой на уровне UEFI](#)

[Информация о стороннем коде](#)

[Уведомления о товарных знаках](#)

О Kaspersky IoT Secure Gateway

Kaspersky IoT Secure Gateway (далее также "система") представляет собой кибериммунную информационную систему на базе операционной системы KasperskyOS с предварительно настроенным набором прикладного программного обеспечения. Kaspersky IoT Secure Gateway устанавливается на встраиваемый компьютер модели Advantech UTX-3117-S6A1N и предназначен для работы в качестве безопасного шлюза Интернета вещей (Internet of Things) в сети организации.

Kaspersky IoT Secure Gateway выполняет следующие функции:

- Получает, проверяет и распределяет сообщения датчиков и других устройств, передаваемые по протоколу MQTT.
- Регистрирует события безопасности системы и сети.
- Обнаруживает устройства во внутренней сети организации.
- Обнаруживает попытки вторжения во внутреннюю сеть организации.
- Обеспечивает кибербезопасность самого устройства и предоставляет способы контроля подключенных устройств.

Также Kaspersky IoT Secure Gateway может работать в качестве межсетевого экрана, DHCP-сервера и преобразователя сетевых адресов (NAT).

Вы можете управлять Kaspersky IoT Secure Gateway через [локальный веб-интерфейс](#) или удаленно с помощью [веб-плагина для Kaspersky Security Center Web Console](#).

Комплект поставки

В комплект поставки Kaspersky IoT Secure Gateway входят следующие файлы:

- Установочный образ Kaspersky IoT Secure Gateway: kiscg-<номер версии программы>-ru-en.tgz.
- Архив с установочным образом веб-плагина для Kaspersky Security Center Web Console и файлом подписи: WEB_Plugin_KISG_<номер версии плагина>.zip.
- Файл с информацией о стороннем коде (Legal Notices).
- Онлайн-справка.
- Информация о версии (Release Notes).

Аппаратные и программные требования

USB-разъемы Advantech UTX-3117-S6A1N могут быть использованы только для подключения клавиатуры и мыши при [первоначальной настройке Kaspersky IoT Secure Gateway](#) или загрузочного USB [при установке Kaspersky IoT Secure Gateway](#). Подключение других устройств к Advantech UTX-3117-S6A1N через USB-разъемы не предусмотрено.

Требования к Kaspersky IoT Secure Gateway

Kaspersky IoT Secure Gateway может быть установлен только на встраиваемый компьютер Advantech UTX-3117FS-S6A1N.

Подключение к веб-интерфейсу Kaspersky IoT Secure Gateway осуществляется с компьютера администратора сети.

Корректная работа веб-интерфейса системы гарантируется при использовании следующих браузеров:

- Google™ Chrome™ версии 88 и выше.
- Mozilla™ Firefox™ версии 78 и выше.

Требования к компонентам Kaspersky Security Center

Для подключения к Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console в локальной сети организации должна быть установлена программа Kaspersky Security Center версии 13.1.

Для работы Kaspersky IoT Secure Gateway требуются следующие компоненты Kaspersky Security Center:

- Сервер администрирования Kaspersky Security Center 13.1.
- Kaspersky Security Center Web Console 13.1.

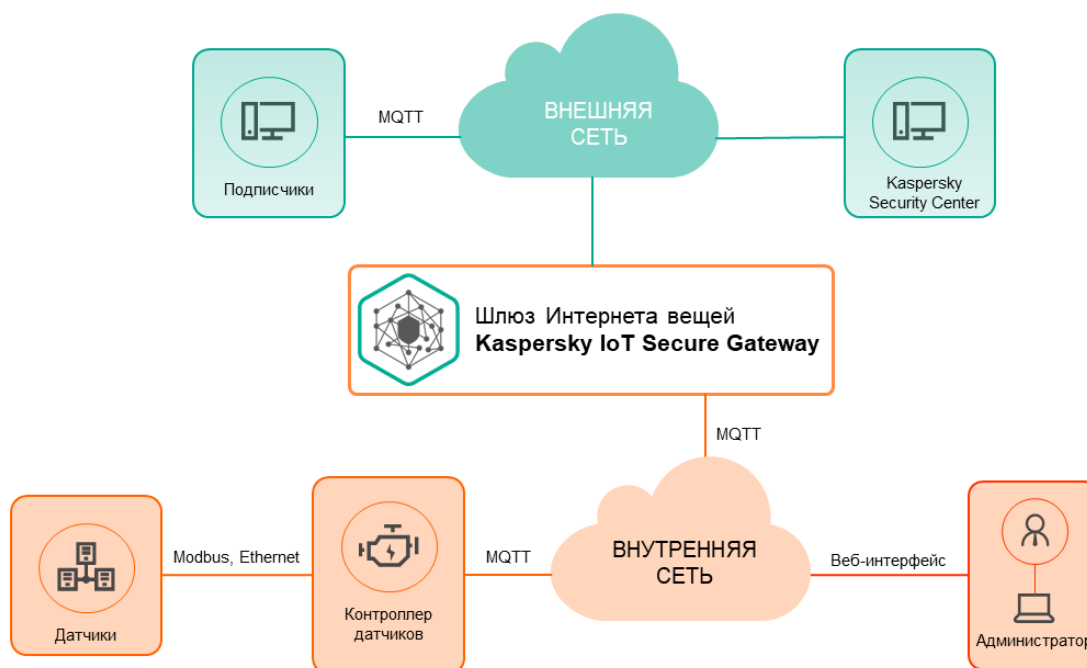
Сведения об установке компонентов Kaspersky Security Center см. в документации Kaspersky Security Center.

Типовая схема развертывания Kaspersky IoT Secure Gateway

Типовая схема развертывания Kaspersky IoT Secure Gateway (см. рис. ниже) предполагает следующее:

1. Датчики передают телеметрические данные (например, по протоколу Modbus) на контроллер датчиков.
2. Контроллер датчиков публикует данные измерений во внутреннюю сеть в виде MQTT-топиков.
3. Шлюз Интернета вещей Kaspersky IoT Secure Gateway получает MQTT-топики и передает их подписчикам, находящимся во внешней сети. В качестве подписчиков, как правило, выступают серверы получения и визуализации данных.

Администратор может управлять системой и следить за ее состоянием из внутренней сети через веб-интерфейс и с помощью сервера Kaspersky Security Center.



Типовая схема развертывания Kaspersky IoT Secure Gateway

Компоненты Kaspersky IoT Secure Gateway

Kaspersky IoT Secure Gateway включает в себя следующие компоненты:

- *WEB Server*. Обеспечивает работу веб-интерфейса Kaspersky IoT Secure Gateway.
- *MQTTbroker*. Обеспечивает функциональность MQTT-брокера Eclipse Mosquitto™.
- *Modem*. Обеспечивает передачу данных журналов событий системы с использованием сотового соединения.
- *MQTT*. Обеспечивает отправку событий системы по протоколу MQTT (Message Queuing Telemetry Transport).
- *Syslog*. Обеспечивает отправку событий системы на сторонний сервер Syslog по протоколу Syslog.
- *Push*. Обеспечивает отправку событий системы с помощью Firebase™ Cloud Messaging по протоколу HTTPS.
- *Firewall*. Обеспечивает функционал межсетевого экранирования и контроля соединений.
- *Kaspersky Security Center*. Обеспечивает централизованное управление Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console.
- *DeviceDetection*. Обеспечивает обнаружение устройств в сети, их классификацию.
- *IPS*. Обеспечивает функциональность предотвращения вторжений из внешней сети.
- *Update*. Обеспечивает обновление компонентов системы.

- *DHCPserver*. Обеспечивает работу DHCP-сервера.
- *DHCPclient*. Обеспечивает работу DHCP-клиента.
- *Events& Audit*. [Обеспечивает работу с событиями безопасности Kaspersky IoT Secure Gateway и событиями безопасности во внутренней сети.](#)

Рекомендации по обеспечению безопасной работы Kaspersky IoT Secure Gateway

Для обеспечения безопасной работы Kaspersky IoT Secure Gateway, рекомендуется ограничить и контролировать доступ к оборудованию, на котором работает программа.

Физическая безопасность оборудования

При внедрении Kaspersky IoT Secure Gateway на предприятии рекомендуется принять следующие меры по обеспечению безопасной работы:

- Ограничить доступ в помещение, в котором расположено оборудование с установленной программой, а также к сетевому оборудованию выделенной сети. Доступ в помещение должен предоставляться только доверенным лицам, например персоналу, обладающему полномочиями по установке и настройке программы.
- Обеспечить контроль физического доступа к оборудованию, на котором работает программа, с помощью технических средств или службы охраны. Проводить мониторинг доступа в контролируемые помещения с помощью средств охранной сигнализации.
- Осуществлять видеонаблюдение в контролируемых помещениях.

Информационная безопасность

Для использования средств управления работой программы рекомендуется дополнительно принять следующие меры по обеспечению информационной безопасности интранет-системы:

- Обеспечить защиту трафика внутри интранет-системы.
- Обеспечить первичную настройку Kaspersky IoT Secure Gateway только в контролируемом контуре.
- Использовать цифровые сертификаты, изданные доверенными центрами сертификации. При компрометации сертификатов рекомендуется их обновить.
- Завершать сеанс подключения к веб-интерфейсу Kaspersky IoT Secure Gateway при завершении работы пользователя в веб-браузере. Для принудительного [завершения сеанса подключения](#) в веб-браузере нужно использовать пункт **Выход** в меню пользователя.

Что нового

В Kaspersky IoT Secure Gateway 2.1 появились следующие возможности и доработки:

- Кибериммунность – добавлена функциональность, позволяющая Kaspersky IoT Secure Gateway выполнять [цели и предположения безопасности](#), при которых Kaspersky IoT Secure Gateway представляет собой кибериммунную информационную систему.
- Сотовое подключение к внешней сети – добавлена поддержка модема Huawei ME909s-120 v1 и v2, позволяющая [Kaspersky IoT Secure Gateway передавать данные через каналы сотовой связи](#).
- Управление и мониторинг параметров соединения через сотовую связь – реализована возможность создания нового профиля соединения через сотовую связь и переключение между профилями. Вы можете управлять параметрами такого соединения через [веб-интерфейс Kaspersky IoT Secure Gateway](#) и через [Kaspersky Security Center Web Console](#).
- Авторизация пользователя только с использованием сертификата – вместо авторизации пользователя с помощью учетных данных добавлена функциональность, позволяющая [подключаться к веб-интерфейсу Kaspersky IoT Secure Gateway](#) с помощью [сертификата администратора](#).
- Продление сессии пользователя с использованием сертификата – добавлена функциональность, позволяющая [возобновлять подключение](#) к веб-интерфейсу Kaspersky IoT Secure Gateway с помощью загруженного при авторизации [сертификата администратора](#).
- Подключение к Kaspersky Security Center с использованием сертификата – добавлена функциональность, обеспечивающая безопасное [взаимодействие Kaspersky IoT Secure Gateway и Kaspersky Security Center](#). Безопасность обеспечивается за счет использования [сертификата сервера Kaspersky Security Center](#).
- Система обнаружения вторжений (IDS) – обновлены базы [правил обнаружения вторжений](#). Правила обнаружения вторжений описывает аномалию трафика, которая может быть признаком атаки из внешней сети. Правила содержат условия, по которым система обнаружения вторжений анализирует трафик.
- Журнал событий Kaspersky IoT Secure Gateway – добавлена возможность [экспорта журнала событий](#) в файл формата GZIP через интерфейс Kaspersky IoT Secure Gateway.
- Уведомление по протоколу MQTT – добавлена функциональность, позволяющая включить или выключить отправку зарегистрированных событий Kaspersky IoT Secure Gateway по протоколу MQTT (Message Queuing Telemetry Transport) через [веб-интерфейс Kaspersky IoT Secure Gateway](#) и через [Kaspersky Security Center Web Console](#).

Включение и выключение устройства Advantech UTX-3117FS-S6A1N

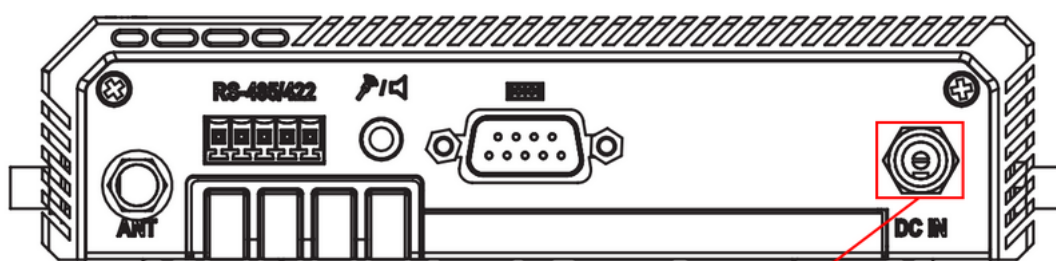
Прежде, чем начать работу с Kaspersky IoT Secure Gateway, требуется подключить устройство Advantech UTX-3117FS-S6A1N к сети и включить.

[Подготовку к установке](#) и [установку Kaspersky IoT Secure Gateway](#) выполняют специалисты "Лаборатории Касперского".

После первого включения Kaspersky IoT Secure Gateway рекомендуется [настроить сеть](#), [создать и загрузить сертификат администратора](#), [настроить дату и время](#) и [изменить сертификат веб-сервера](#) на используемый в вашей организации.

Чтобы включить устройство Advantech UTX-3117FS-S6A1N:

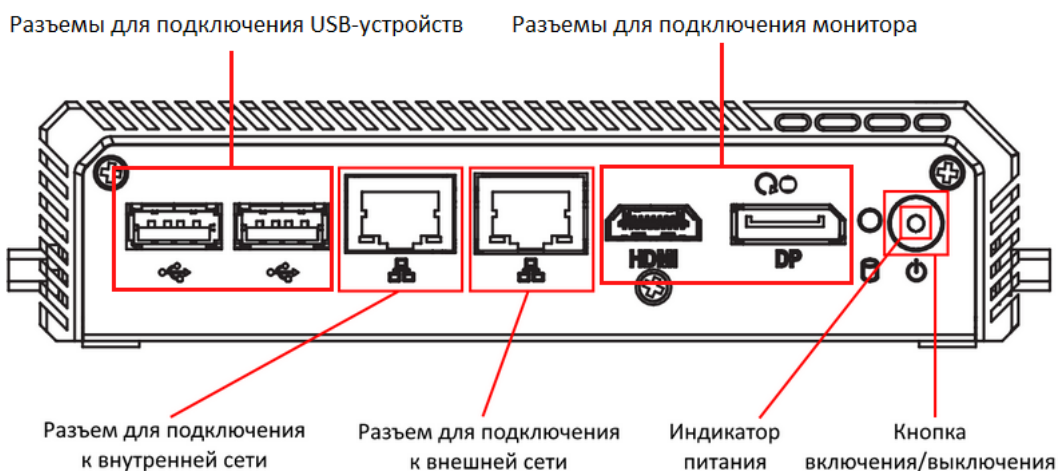
1. Подсоедините кабель электропитания к разъему на задней панели Advantech UTX-3117FS-S6A1N (см. рис. ниже).



Разъем для подключения кабеля электропитания

Задняя панель Advantech UTX-3117FS-S6A1N

2. Подсоедините сетевой кабель, ведущий во внешнюю сеть, к разъему для подключения к внешней сети на лицевой панели Advantech UTX-3117FS-S6A1N (см. рис. ниже).



Лицевая панель Advantech UTX-3117

3. Если требуется включить устройство Advantech UTX-3117FS-S6A1N, нажмите на кнопку включения / выключения в правой части лицевой панели.

Advantech UTX-3117FS-S6A1N включится, Kaspersky IoT Secure Gateway запустится автоматически.

4. Если требуется выключить устройство Advantech UTX-3117FS-S6A1N, [завершите сеанс подключения в веб-интерфейсу Kaspersky IoT Secure Gateway](#) и нажмите на кнопку включения / выключения в правой части лицевой панели.

Advantech UTX-3117FS-S6A1N выключится.

Подключение к веб-интерфейсу Kaspersky IoT Secure Gateway

Вы можете подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway с использованием любого [поддерживаемого браузера](#). Браузер должен быть установлен на компьютере, который имеет доступ к Kaspersky IoT Secure Gateway через внутреннюю сеть.

Kaspersky IoT Secure Gateway поставляется со статически настроенным IP-адресом – 192.168.1.1.

По умолчанию в Kaspersky IoT Secure Gateway включен DHCP-сервер. При подключении вашего компьютера к сети, к которой подключен Kaspersky IoT Secure Gateway через разъем для подключения к внутренней сети, ваш компьютер получит IP-адрес автоматически.

Чтобы подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway:

1. Откройте [браузер](#).
2. Если вы в первый раз подключаетесь к веб-интерфейсу Kaspersky IoT Secure Gateway, добавьте в браузере [доверенный сертификат, созданный совместно с сертификатом администратора](#). Подробнее о добавлении файла сертификата в браузер см. в руководстве используемого браузера.
3. В адресной строке браузера введите IP-адрес Kaspersky IoT Secure Gateway – 192.168.1.1.
Откроется страница входа в Kaspersky IoT Secure Gateway.
4. Если вы в первый раз подключаетесь к веб-интерфейсу Kaspersky IoT Secure Gateway, загрузите [сертификат администратора](#). Для этого нажмите на кнопку **Загрузить**, расположенную справа от наименования нужного типа сертификата, и выберите файл сертификата в формате CRT, CER, DER и PEM.

Создание сертификата администратора должно производиться на доверенном устройстве в условиях безопасной среды (отсутствуют уязвимости и доступ устройства к интернету).

Загрузка доверенного сертификата и сертификат администратора является обязательным условием для подключения к веб-интерфейсу Kaspersky IoT Secure Gateway.

При загрузке сертификата его поля могут хранить персональные данные пользователя. Вам нужно контролировать содержимое этих полей перед загрузкой сертификата в веб-интерфейсе Kaspersky IoT Secure Gateway.

При последующих подключениях к веб-интерфейсу Kaspersky IoT Secure Gateway повторная загрузка указанных сертификатов не требуется, браузер предлагает выбрать ключ для уже загруженных сертификатов.

5. Если требуется управлять программой через Kaspersky Security Center Web Console, загрузите [сертификат сервера Kaspersky Security Center](#). Для этого нажмите на кнопку **Загрузить**, расположенную справа от наименования нужного типа сертификата, и выберите файл сертификата в формате CRT, CER, DER и PEM. Вы можете [загрузить этот сертификат позже](#).

Если в системе отсутствует сертификат сервера Kaspersky Security Center, [настройка параметров подключения к Kaspersky Security Center](#) недоступна.

6. Нажмите на кнопку **Вход**.


В окне браузера откроется страница веб-интерфейса Kaspersky IoT Secure Gateway.

Завершение и возобновление сеанса подключения к веб-интерфейсу Kaspersky IoT Secure Gateway

В целях безопасности в Kaspersky IoT Secure Gateway разрешен только один сеанс подключения к веб-интерфейсу (если один пользователь подключился к веб-интерфейсу, то другие не смогут подключиться). Поэтому по окончании работы с Kaspersky IoT Secure Gateway через веб-интерфейс рекомендуется завершать сеанс подключения в браузере.

Если вы закрыли окно браузера без завершения сеанса подключения, сеанс остается действующим. Время действия незавершенного сеанса составляет пять минут. В течение этого времени система может предоставить доступ к веб-интерфейсу Kaspersky IoT Secure Gateway без запроса нового сертификата администратора, если для повторного подключения используются те же компьютер и браузер.

Чтобы завершить или возобновить сеанс подключения к веб-интерфейсу Kaspersky IoT Secure Gateway:

1. В левой части страницы в меню веб-интерфейса выберите пункт  **<имя пользователя>**.
2. В открывшемся меню пользователя выберите пункт **Выход**.

В окне браузера отобразится страница возобновления сеанса подключения к веб-интерфейсу Kaspersky IoT Secure Gateway.

Также в целях безопасности в Kaspersky IoT Secure Gateway сеанс подключения к веб-интерфейсу завершается по истечении пяти минут бездействия системы. Вы можете возобновить сеанс подключения к веб-интерфейсу Kaspersky IoT Secure Gateway, нажав на кнопку **Вход** на странице возобновления сеанса подключения к веб-интерфейсу Kaspersky IoT Secure Gateway.

Веб-интерфейс Kaspersky IoT Secure Gateway

Работа с Kaspersky IoT Secure Gateway осуществляется через веб-интерфейс. В этом разделе приведено описание основных элементов веб-интерфейса Kaspersky IoT Secure Gateway.

Главное окно веб-интерфейса программы содержит следующие элементы:

- меню – разделы в левой части окна веб-интерфейса программы;
- закладки в верхней части окна веб-интерфейса программы для некоторых разделов программы (например, для раздела **Параметры**);
- рабочую область в центральной части окна веб-интерфейса программы.

Разделы веб-интерфейса программы

Меню веб-интерфейса программы Kaspersky IoT Secure Gateway содержит следующие разделы:

- **Информационная панель.** В этом разделе вы можете просматривать сводную информацию о работе системы: последние события, обнаруженные устройства и состояние компонентов системы.
- **События.** В этом разделе вы можете [просматривать события безопасности сети](#), произошедшие во время текущей сессии подключения пользователя к системе через браузер. События безопасности сети включают в себя обнаружение устройств в сети, а также попытки подключения к веб-интерфейсу программы Kaspersky IoT Secure Gateway.
- **Аудит.** В этом разделе вы можете [просматривать журнал аудита](#) Kaspersky IoT Secure Gateway.
- **Устройства.** В этом разделе вы можете [просматривать список устройств](#), обнаруженных во внутренней сети, [добавлять доверенные устройства в список разрешенных и удалять устройства из списка разрешенных](#).
- **MQTT-брокер.** В этом разделе вы можете [просматривать и изменять параметры в профиле MQTT-брокера](#).
- **Параметры.** В этом разделе расположены следующие закладки, на которых вы можете просматривать и изменять параметры системы:
 - **Сеть.** На этой закладке вы можете [настроить параметры внутренней сети и внешней сети](#) Kaspersky IoT Secure Gateway, а также [настроить параметры сотового подключения](#).
 - **Безопасность системы.** На этой закладке вы можете [управлять сертификатами](#) администратора Kaspersky IoT Secure Gateway и сервера Kaspersky Security Center.
 - **Веб-сервер.** На этой закладке вы можете [управлять профилями веб-сервера](#).
 - **Инструменты.** На этой закладке вы можете просматривать и изменять параметры [push-уведомлений](#) и [MQTT-уведомлений](#), а также настраивать [параметры отправки журналов безопасности сети и аудита](#) на сторонний сервер Syslog.
 - **Общие.** На этой закладке вы можете просматривать и изменять [параметры даты и времени](#) Kaspersky IoT Secure Gateway.
 - **Kaspersky Security Center.** На этой закладке вы можете просматривать и [изменять адрес подключения к серверу Kaspersky Security Center](#).

- **О программе.** Этот раздел содержит информацию об установленной на вашем устройстве версии Kaspersky IoT Secure Gateway, а также ссылки для перехода к онлайн-справке и информации о стороннем коде.

Рабочая область окна веб-интерфейса программы

В рабочей области отображается информация, просмотр которой вы выбираете в меню и на закладках окна веб-интерфейса программы, а также элементы управления, с помощью которых вы можете настроить отображение информации.

Меню пользователя

В левом нижнем углу окна веб-интерфейса расположено меню пользователя, позволяющее выполнить следующие действия:

- [изменить язык веб-интерфейса](#);
- [выйти из системы](#).

Цели и предположения безопасности

Кибериммунная информационная система – система, гарантирующая достижение целей безопасности во всех возможных сценариях использования системы, предусмотренных разработчиками.

Необходимым условием разработки кибериммунной информационной системы является определение целей безопасности и предположений безопасности (условий, в которых будет эксплуатироваться система).

Цели безопасности – это требования, предъявляемые к кибериммунной информационной системе, выполнение которых обеспечивает безопасное функционирование в любых возможных сценариях ее использования с учетом предположений безопасности.

Предположения безопасности – дополнительные ограничения, накладываемые на условия эксплуатации системы, облегчающие или усложняющие выполнение целей безопасности.

Цели безопасности

К целям безопасности Kaspersky IoT Secure Gateway относятся следующие цели:

- Kaspersky IoT Secure Gateway обеспечивает безопасный (конфиденциальность и целостность) канал связи от устройства в цифровые платформы (Yandex IOT Core, Microsoft® Azure IoT hub).
- Kaspersky IoT Secure Gateway обеспечивает обновление версии системы безопасным образом. Допускается установка только обновления, подписанного "Лабораторией Касперского", в том числе при получении обновления через недоверенные каналы связи.
- Kaspersky IoT Secure Gateway обеспечивает безопасное получение и хранение параметров системы и конфигурационных файлов (от доверенного источника).
- Kaspersky IoT Secure Gateway обеспечивает накопление и безопасное хранение событий безопасности устройства (Secure audit: перезагрузка, обновление, события информационной безопасности) и их передачу в Kaspersky Security Center безопасным образом.
- Kaspersky IoT Secure Gateway обеспечивает возможность администрирования системы из внутренней сети после авторизации пользователя через сертификат при установке безопасного канала.

Предположения безопасности

К предположениям безопасности Kaspersky IoT Secure Gateway относятся следующие предположения:

- Kaspersky IoT Secure Gateway может быть развернут двумя способами:
 - С поддержкой управления через Kaspersky Security Center, расположенный во внутренней или внешней сети. Доверенным источником получения параметров и конфигурационных файлов Kaspersky IoT Secure Gateway является Kaspersky Security Center.
 - Без поддержки управления через Kaspersky Security Center. При развертывании задается список сертификатов, с помощью которых администратор может подключаться к веб-интерфейсу Kaspersky IoT Secure Gateway. Доверенным источником получения параметров и конфигурационных файлов Kaspersky IoT Secure Gateway является веб-интерфейс Kaspersky IoT Secure Gateway.
- Первоначальная настройка параметров Kaspersky IoT Secure Gateway должна производиться в условиях, когда отсутствует угроза подмены Kaspersky Security Center.

- Kaspersky Security Center считается доверенным, если в Kaspersky IoT Secure Gateway настроено взаимодействие с Kaspersky Security Center с помощью сертификата сервера Kaspersky Security Center. Не рассматриваются угрозы, связанные с компрометацией Kaspersky Security Center.
- Устройство, на котором установлен Kaspersky IoT Secure Gateway, имеет отдельные порты для подключения к внутренней и внешней сетям.
- Устройство, на котором установлен Kaspersky IoT Secure Gateway, работает в окружении, гарантирующем отсутствие физического доступа со стороны злоумышленника, в том числе для подключения напрямую к устройству.
- Предполагается средний (базовый повышенный) уровень угроз со стороны внешней сети.
- Предполагается низкий (базовый) уровень угроз со стороны внутренней сети.
Подробную информацию об оценке уровня угроз безопасности информации вы можете получить на сайте Федеральной службы по техническому и экспортному контролю России.
- Не рассматриваются угрозы, связанные с уязвимостью аппаратной платформы.
- Не рассматриваются угрозы, связанные с нарушением конфиденциальности, целостности или утратой данных при передаче от устройств во внутренней сети к Kaspersky IoT Secure Gateway.
- Не рассматриваются угрозы, связанные с нарушением доступности инфраструктуры:
 - каналы связи между участниками сетевого взаимодействия;
 - сервер Kaspersky Security Center;
 - цифровые платформы.

Обработка и хранение данных в Kaspersky IoT Secure Gateway

Этот раздел содержит информацию о предоставлении данных и об используемых журналах для хранения данных.

Предоставление данных

Kaspersky IoT Secure Gateway не передает пользовательские персональные данные в "Лабораторию Касперского". Обработка персональных данных пользователей на устройствах Kaspersky IoT Secure Gateway не производится.

При каждом запуске Kaspersky IoT Secure Gateway журнал безопасности сети и список обнаруженных в сети устройств, не входящих в список разрешенных устройств, удаляются. При перезагрузке устройства и при завершении сеанса подключения записи журнала безопасности сети и список обнаруженных устройств ведутся заново. Все данные сертификатов хранятся в отдельно выделенном пространстве диска.

При работе с Kaspersky IoT Secure Gateway в файлах cookies сохраняется следующая информация:

- идентификатор текущего соединения;
- последний выбранный язык веб-интерфейса Kaspersky IoT Secure Gateway;
- последний посещенный раздел веб-интерфейса Kaspersky IoT Secure Gateway, в случае если пользователь не завершил сеанс подключения к Kaspersky IoT Secure Gateway или закрыл веб-интерфейс до завершения сеанса подключения.

При загрузке сертификата его поля могут хранить персональные данные пользователя. Вам нужно контролировать содержимое этих полей перед загрузкой сертификата в веб-интерфейсе Kaspersky IoT Secure Gateway.

При обнаружении устройств в сети организации имя устройства может хранить персональные данные пользователя. Вам нужно переименовать устройство при добавлении его в список разрешенных.

При настройке параметров MQTT-брокера содержимое конфигурационного файла может содержать персональные данные. Вам нужно контролировать данные, загружаемые в профиль MQTT-брокера Kaspersky IoT Secure Gateway.

Kaspersky IoT Secure Gateway хранит следующую информацию, которая не относится к персональным данным:

- Журнал безопасности сети.
- Журнал аудита.
- Набор правил системы предотвращения вторжений (IPS).
- IP-адреса, MAC-адреса и имена устройств сети, которые находятся в списке разрешенных устройств.
- Параметры MQTT-брокера:

- признак доступности профиля для изменения;
 - признак активности профиля;
 - имя профиля;
 - сертификат удостоверяющего центра для сервера MQTT (сертификат может являться самоподписанным);
 - клиентский сертификат для сервера MQTT;
 - закрытый ключ для клиентского сертификата сервера MQTT;
 - информация о конфигурационных файлах: имя файла, тип файла, содержимое файла.
- Общие параметры Kaspersky IoT Secure Gateway:
 - Параметры внутренней сети:
 - IP-адрес Kaspersky IoT Secure Gateway во внутренней сети;
 - маска подсети;
 - параметры DHCP-сервера:
 - использование DHCP-сервера (включено или выключено);
 - начало и конец диапазона IP-адресов;
 - адрес основного DNS-сервера;
 - адрес дополнительного DNS-сервера.
 - Параметры внешней сети:
 - использование DHCP-клиента (включено или выключено);
 - IP-адрес;
 - маска подсети;
 - сетевой шлюз по умолчанию;
 - адрес основного DNS-сервера;
 - адрес дополнительного DNS-сервера.
 - Параметры сотового соединения Kaspersky IoT Secure Gateway:
 - использование модема как основного канала связи (включено или выключено);
 - адреса DNS-серверов модема;
 - данные о профилях операторов связи:
 - признак активности профиля;

- признак доступности для изменения профиля;
 - имя профиля;
 - данные о конфигурационном файле профиля: тип файла, имя файла, содержимое файла.
- Параметры безопасности Kaspersky IoT Secure Gateway:
 - сертификат администратора для подключения в веб-интерфейсу Kaspersky IoT Secure Gateway;
 - сертификат сервера Kaspersky Security Center.
- Параметры веб-сервера Kaspersky IoT Secure Gateway:
 - признак доступности для изменения профиля;
 - признак активного профиля;
 - имя профиля;
 - конфигурационные файлы;
 - сертификат веб-сервера;
 - закрытый ключ сертификата веб-сервера.
- Параметры Syslog-уведомлений:
 - использование уведомлений для сервера Syslog (включено или выключено);
 - IP-адрес и порт сервера Syslog;
 - режим передачи уведомлений: UDP, TCP, TLS;
 - сертификат сервера Syslog.
- Параметры push-уведомлений:
 - имя устройства, на которое осуществляется отправка push-уведомлений;
 - ключ авторизации устройства, на которое осуществляется отправка push-уведомлений;
 - сертификат сервера Google FCM для push-уведомлений.
- Параметры MQTT-уведомлений:
 - использование уведомлений по протоколу MQTT (включено или выключено);
 - адрес и порт сервера MQTT;
 - имя MQTT-топика;
 - использование аутентификации при отправке уведомлений по протоколу MQTT (включено или выключено);
 - имя и пароль пользователя;

- использования защищенного SSL-соединения (включено или выключено);
- сертификат удостоверяющего центра для отправки уведомлений по протоколу MQTT;
- клиентский сертификат для отправки MQTT-уведомления;
- закрытый ключ для клиентского сертификата для отправки MQTT-уведомлений.
- Параметры даты и времени Kaspersky IoT Secure Gateway.
- Параметры подключения к серверу Kaspersky Security Center: адрес сервера и порт.
- Информация о версии Kaspersky IoT Secure Gateway.

Если Kaspersky IoT Secure Gateway подключен к Kaspersky Security Center, Kaspersky IoT Secure Gateway сохраняет и обрабатывает следующую информацию, не относящуюся к персональным данным:

- Параметры MQTT-брокера:
 - признак доступности профиля для изменения;
 - признак активного профиля;
 - имя профиля;
 - сертификат удостоверяющего центра для сервера MQTT (сертификат может являться самоподписанным);
 - клиентский сертификат сервера MQTT;
 - закрытый ключ для клиентского сертификата сервера MQTT;
 - информация о конфигурационных файлах: имя файла, тип файла, содержимое файла.
- Параметры сети Kaspersky IoT Secure Gateway:
 - Параметры внутренней сети:
 - IP-адрес Kaspersky IoT Secure Gateway во внутренней сети;
 - маска подсети;
 - параметры DHCP-сервера:
 - состояние DHCP-сервера (включен или выключен);
 - начало и конец диапазона IP-адресов;
 - адрес основного DNS-сервера;
 - адрес дополнительного DNS-сервера.
 - Параметры внешней сети:
 - состояние DHCP-клиента (включен или выключен);

- IP-адрес;
- маска подсети;
- сетевой шлюз по умолчанию;
- адрес основного DNS-сервера;
- адрес дополнительного DNS-сервера.
- Параметры правил межсетевого экрана:
 - список правил;
 - состояние правила (включено или выключено);
 - действие, которое межсетевой экран должен выполнять над сетевым трафиком, попадающим под правило;
 - область, к которой применяется правило;
 - IP-адрес источника трафика;
 - порт источника трафика, если этот параметр применим к используемому протоколу;
 - IP-адрес получателя трафика;
 - порт получателя трафика, если этот параметр применим к используемому протоколу;
 - используемый протокол.
- Параметры системы предотвращения вторжений:
 - использование системы предотвращения вторжений (включено или выключено);
 - доступность системы предотвращения вторжений;
 - IP-адреса, занесенные в список запрещенных IP-адресов;
 - использование списка запрещенных IP-адресов (при выключенном списке запрещенных IP-адресов атаки будут обнаружены, но IP-адреса, с которых они были произведены не будут заблокированы);
 - идентификаторы сигнатур, по которым IP-адреса были занесены в список запрещенных IP-адресов;
 - IP-адреса, занесенные в список разрешенных IP-адресов.
- Параметры маскардинга: состояние маскардинга (включено или выключено).
- Параметры Kaspersky IoT Secure Gateway:
 - Параметры веб-сервера Kaspersky IoT Secure Gateway:
 - признак доступности профиля для изменения;
 - признак активности профиля;

- имя профиля.
- Параметры даты и времени Kaspersky IoT Secure Gateway.
- Параметры сотового соединения Kaspersky IoT Secure Gateway:
 - статус работы модема;
 - уровень сигнала модема;
 - использование модема как основного канала связи (включено или выключено);
 - адреса DNS-серверов модема;
 - данные для работы оператора связи:
 - признак активности конфигурационного файла;
 - признак доступности конфигурационного файла для изменения;
 - тип конфигурационного файла;
 - имя конфигурационного файла;
 - содержимое конфигурационного файла.
- Параметры безопасности Kaspersky IoT Secure Gateway:
 - сертификат администратора для подключения в веб-интерфейсу Kaspersky IoT Secure Gateway;
 - сертификат сервера Kaspersky Security Center.
- Параметры отправки Syslog-уведомлений:
 - отправка уведомлений на сервер Syslog (включено или выключено);
 - IP-адрес и порт сервера Syslog;
 - режим передачи уведомлений: UDP, TCP, TLS;
 - сертификат сервера Syslog.
- Параметры отправки push-уведомлений:
 - имя устройства, на которое осуществляется отправка push-уведомлений;
 - ключ авторизации;
 - сертификат сервера Google FCM для отправки push-уведомлений.
- Параметры отправки MQTT-уведомлений:
 - отправка уведомлений по протоколу MQTT (включено или выключено);
 - адрес и порт сервера MQTT;

- имя MQTT-топика;
- использование аутентификации при отправке уведомлений по протоколу MQTT (включено или выключено);
- имя и пароль пользователя;
- использование защищенного SSL-соединения (включено или выключено);
- сертификат удостоверяющего центра для отправки MQTT-уведомлений;
- клиентский сертификат для отправки MQTT-уведомлений;
- закрытый ключ клиентского сертификата для отправки MQTT-уведомлений.
- Параметры взаимодействия Kaspersky IoT Secure Gateway и Kaspersky Security Center Web Console:
 - период синхронизации параметров Kaspersky IoT Secure Gateway и Kaspersky Security Center Web Console;
 - список команд, которые Kaspersky Security Center Web Console может отправить в Kaspersky IoT Secure Gateway;
 - адрес обновления Kaspersky IoT Secure Gateway.
- Информация о версии Kaspersky IoT Secure Gateway.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

О хранении журналов Kaspersky IoT Secure Gateway

Kaspersky IoT Secure Gateway сохраняет данные о событиях безопасности сети и аудита. В зависимости от типа журнала для размещения данных Kaspersky IoT Secure Gateway использует следующие методы хранения:

- Блок данных конкретных секторов диска.
В блоке данных конкретных секторов диска хранится содержимое [журнала аудита](#). Вы можете [просмотреть журнал аудита через веб-интерфейс Kaspersky IoT Secure Gateway или сохранить его на локальный компьютер](#).
- Память устройства.
В памяти устройства хранится содержимое [журнала безопасности сети](#). Вы можете [просмотреть журнал безопасности сети через веб-интерфейс Kaspersky IoT Secure Gateway или через Kaspersky Security Center Web Console](#).

Kaspersky IoT Secure Gateway позволяет сохранять в файл журнал всех событий. Вы можете [сохранить на локальный компьютер файл, содержащий журнал всех событий](#), используя веб-интерфейс Kaspersky IoT Secure Gateway.

Также при необходимости вы можете настроить [передачу данных журнала событий безопасности сети и аудита](#) через протоколы MQTT, Syslog и с помощью push-уведомлений.

Лицензирование Kaspersky IoT Secure Gateway

Условия использования программы изложены в лицензионном договоре, на основании которого используется программа.

Настройка Kaspersky IoT Secure Gateway

Этот раздел содержит информацию о настройке Kaspersky IoT Secure Gateway.

Сценарий: Быстрый старт для администратора

В этом разделе приводится последовательность действий, которые требуется выполнить администратору, чтобы установить и настроить Kaspersky IoT Secure Gateway, Kaspersky Security Center, а также установить между ними соединение.

Сценарий установки Kaspersky IoT Secure Gateway, Kaspersky Security Center и настройки между ними соединения состоит из следующих этапов:

1 Установка Kaspersky Security Center

Загрузите дистрибутив Kaspersky Security Center 13 и установите полную версию Kaspersky Security Center на сервере. Дистрибутив полной версии Kaspersky Security Center включает Kaspersky Security Center Web Console. При установке рекомендуется выбрать стандартную установку. Подробную информацию об установке Kaspersky Security Center вы можете получить в разделе онлайн-справки Kaspersky Security Center 13 *Основной сценарий установки*.

2 Настройка правил межсетевого экрана

Для межсетевого экрана операционной системы сервера, на котором установлен Kaspersky Security Center, настройте правила, разрешающие подключение Kaspersky IoT Secure Gateway к серверу Kaspersky Security Center по протоколу TCP через порт 13294. Подробную информацию о настройке правил межсетевого экрана вы можете получить в руководстве используемой операционной системы.

3 Установка веб-плагины управления Kaspersky IoT Secure Gateway

В интерфейсе Kaspersky Security Center Web Console [установите веб-плагин управления Kaspersky IoT Secure Gateway](#). ZIP-архив с дистрибутивом веб-плагины Kaspersky IoT Secure Gateway входит в [комплект поставки](#).

4 Настройка подключения устройств с защитой на уровне UEFI

На Сервере администрирования Kaspersky Security Center включите использование порта 13294 для протокола TCP для настройки подключения Kaspersky IoT Secure Gateway к Kaspersky Security Center. Подробную информацию о включении порта 13294 на Сервере администрирования Kaspersky Security Center вы можете получить в разделе онлайн-справки Kaspersky Security Center 13 *Устройства с защитой на уровне UEFI*.

5 Установка Kaspersky IoT Secure Gateway

[Выполните подготовку к установке](#) и [установите Kaspersky IoT Secure Gateway](#) на устройстве Advantech UTX-3117FS-S6A1N.

6 Подключение к веб-интерфейсу Kaspersky IoT Secure Gateway

[Подключитесь к веб-интерфейсу Kaspersky IoT Secure Gateway](#). Предварительно требуется [создать сертификат администратора и доверенный сертификат](#). Доверенный сертификат требуется добавить в браузер, с помощью которого вы подключаетесь к веб-интерфейсу Kaspersky IoT Secure Gateway. Подробнее о добавлении файла сертификата в браузер см. в руководстве используемого браузера.

7 Настройка параметров Kaspersky IoT Secure Gateway

После подключения к веб-интерфейсу Kaspersky IoT Secure Gateway настройте следующие параметры:

- [подключение к внешней и внутренней сети](#);

- [профиль модема](#).

8 Создание и загрузка сертификата сервера Kaspersky Security Center.

[Создайте новый сертификат сервера Kaspersky Security Center](#) и сохраните его на локальное устройство. В веб-интерфейсе Kaspersky IoT Secure Gateway [загрузите сертификат сервера Kaspersky Security Center](#) для настройки соединения с Kaspersky Security Center Web Console.

9 Настройка подключения Kaspersky IoT Secure Gateway к Kaspersky Security Center

В веб-интерфейсе Kaspersky IoT Secure Gateway настройте [подключение к Kaspersky Security Center](#).

10 Добавление Kaspersky IoT Secure Gateway в список управляемых устройств

Подключитесь к Kaspersky Security Center Web Console и [добавьте Kaspersky IoT Secure Gateway в список управляемых устройств Kaspersky Security Center](#). Только для управляемых устройств в Kaspersky Security Center Web Console можно создавать политики и задачи.

11 Создание активной политики Kaspersky Security Center для Kaspersky IoT Secure Gateway

[Создайте активную политику для Kaspersky IoT Secure Gateway](#). Активная политика требуется для получения программой Kaspersky Security Center журналов [событий](#) Kaspersky IoT Secure Gateway.

В результате выполнения этих действий Kaspersky IoT Secure Gateway будет готов к работе, и вы сможете управлять Kaspersky IoT Secure Gateway через [веб-интерфейс Kaspersky IoT Secure Gateway](#) или через [Kaspersky Security Center Web Console](#), а также осуществлять [мониторинг устройств](#) и [событий в сети](#).

Сценарий: Настройка доступа из внешней сети к устройствам внутренней сети

В этом разделе описана последовательность действий, которые требуется выполнить для настройки доступа из внешней сети к устройствам внутренней сети, используя Kaspersky IoT Secure Gateway.

Перед выполнением настройки требуется убедиться, что порт, по которому планируется подключение к устройству внутренней сети, доступен для подключения.

Сценарий настройки доступа состоит из следующих этапов:

1 Настройка маршрутизации транзитных IP-пакетов

На устройстве, которое расположено во внешней сети, настройте маршрутизацию транзитных IP-пакетов таким образом, чтобы сетевые пакеты, предназначенные для устройства внутренней сети, к которому требуется получить доступ, отправлялись через внешний сетевой интерфейс Kaspersky IoT Secure Gateway (WAN).

Подробную информацию о настройке маршрутизации транзитных IP-пакетов на устройстве внешней сети см. в руководстве по использованию устройства.

2 Выключение маскардинга

[Выключите функцию маскардинга](#) для динамического преобразования IP-адресов транзитных пакетов, полученных Kaspersky IoT Secure Gateway от устройства во внешней сети.

3 Создание правила для устройства во внешней сети

[Создайте правило межсетевого экрана](#), которое открывает на внешнем интерфейсе Kaspersky IoT Secure Gateway (WAN) прохождение сетевых пакетов от устройства внешней сети к устройству во внутренней сети.

4 Создание правила для устройства во внутренней сети

[Создайте правило межсетевого экрана](#), которое открывает на внутреннем интерфейсе Kaspersky IoT Secure Gateway (LAN) прохождение сетевых пакетов от устройства во внутренней сети к устройству внешней сети.

5 Проверьте подключение к устройству внутренней сети

На устройстве, которое находится во внешней сети, проверьте подключение к устройству во внутренней сети.

Подробную информацию о вариантах проверки подключения к другим устройствам сети см. в руководстве по использованию устройства.

Настройка доступа выполнена. Вы сможете подключиться из внешней сети к устройствам, расположенным во внутренней сети Kaspersky IoT Secure Gateway, например, для выгрузки данных от этих устройств или настройки их параметров.

Настройка параметров сети

Kaspersky IoT Secure Gateway поставляется со статически настроенным IP-адресом – 192.168.1.1. Чтобы система могла работать в качестве безопасного шлюза Интернета вещей, требуется выполнить настройку параметров внешней и внутренней сети.

Внешняя сеть – это сеть, через которую Kaspersky IoT Secure Gateway выходит в интернет или взаимодействует с Kaspersky Security Center.

Внутренняя сеть – это сеть организации, в которой датчики передают системе телеметрические данные.

Вы можете просматривать и изменять параметры сети Kaspersky IoT Secure Gateway в подразделе **Сеть** на закладке **Внутренняя сеть** или **Внешняя сеть**.

Внутренняя сеть Kaspersky IoT Secure Gateway может быть использована для выполнения следующих задач:

- [подключение к веб-интерфейсу Kaspersky IoT Secure Gateway](#);
- [отправка журналов событий на внутренний сервер Syslog](#);
- [мониторинг подключенных к Kaspersky IoT Secure Gateway устройств](#).

Внешняя сеть Kaspersky IoT Secure Gateway может быть использована для выполнения следующих задач:

- [настройка взаимодействия Kaspersky IoT Secure Gateway с Kaspersky Security Center](#);
- [обеспечение функциональности предотвращения вторжений \(компонент IPS\)](#);
- [отправка журналов событий на внешний сервер Syslog](#).

Настройка параметров внутренней сети

При изменении IP-адреса Kaspersky IoT Secure Gateway во внутренней сети, сеанс подключения к веб-интерфейсу будет завершен, вы будете перенаправлены на страницу возобновления сеанса подключения к веб-интерфейсу Kaspersky IoT Secure Gateway.

При изменении маски подсети Kaspersky IoT Secure Gateway во внутренней сети необходимо заново настроить параметры внутренней сети.

При включении или выключении функции **Использовать DHCP-сервер** требуется перезагрузить Kaspersky IoT Secure Gateway.

Чтобы настроить параметры внутренней сети:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Сеть**.
2. На закладке **Внутренняя сеть** укажите значения следующих параметров:
 - **IP-адрес**. По умолчанию этот параметр имеет значение 192.168.1.1.
 - **Маска подсети**. По умолчанию этот параметр имеет значение 255.255.255.0.
В поле **MAC-адрес** отображается MAC-адрес системы во внутренней сети.
3. Если требуется настроить параметры сети автоматически по протоколу DHCP, установите переключатель **Использовать DHCP-сервер** в положение включено. По умолчанию переключатель **Использовать DHCP-сервер** выключен.
4. Если требуется настроить параметры сети вручную, установите переключатель **Использовать DHCP-сервер** в положение выключено и укажите значения для следующих параметров:
 - **Начало диапазона IP-адресов**.
 - **Конец диапазона IP-адресов**.
 - **Адрес основного DNS-сервера**.
 - **Адрес дополнительного DNS-сервера**.
5. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.
6. [Перезагрузите](#) Kaspersky IoT Secure Gateway, чтобы изменения параметров сети вступили в силу.

Настройка параметров внешней сети

Чтобы настроить параметры внешней сети:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Сеть**.
2. На закладке **Внешняя сеть** выполните одно из следующих действий:
 - Если требуется настроить параметры сети автоматически по протоколу DHCP, установите переключатель **Автоматическое получение (по DHCP)** в положение включено. По умолчанию переключатель **Автоматическое получение (по DHCP)** находится во включенном положении.

Если при включении автоматического получения параметров внешней сети DHCP-сервер выдал Kaspersky IoT Secure Gateway нулевые адреса DNS-серверов, то по умолчанию для преобразования доменного имени в IP-адрес будет использоваться IP-адрес – 208.67.222.222 (сервер OpenDNS).

- Если требуется настроить параметры сети вручную, установите переключатель **Автоматическое получение (по DHCP)** в положение выключено и укажите значения для следующих параметров:
 - IP-адрес.
 - Маска подсети.
 - Шлюз по умолчанию.
 - Адрес основного DNS-сервера.
 - Адрес дополнительного DNS-сервера.

В поле **MAC-адрес** отображается MAC-адрес системы во внешней сети.

3. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

4. [Перезагрузите](#) Kaspersky IoT Secure Gateway, чтобы изменения параметров сети вступили в силу.

Настройка параметров подключения к Kaspersky Security Center

Для безопасного управления Kaspersky IoT Secure Gateway из Kaspersky Security Center Web Console требуется настроить параметры подключения к Kaspersky Security Center.

Если в системе отсутствует [сертификат сервера Kaspersky Security Center](#), настройка параметров подключения к Kaspersky Security Center недоступна.

Чтобы настроить параметры подключения к Kaspersky Security Center:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Kaspersky Security Center**.
Откроется окно **Параметры подключения к Kaspersky Security Center**.
2. В поле **Доменный адрес** укажите доменный адрес сервера Kaspersky Security Center, к которому осуществляется подключение.
В поле **Порт** указан номер порта, по которому осуществляется подключение.
3. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Настройка параметров сотового соединения

Если в устройстве отсутствует модем, использование сотового соединения и настройка параметров такого соединения недоступны.

Работу сотового соединения Kaspersky IoT Secure Gateway обеспечивает модем Huawei ME909s-120. Параметры сотового соединения хранятся в профиле модема. Kaspersky IoT Secure Gateway поставляется с предустановленными профилями модема, в которые входит конфигурационный файл, содержащий базовые скрипты для настройки параметров сотового соединения. Также конфигурационный файл профиля модема содержит AT-команды для модема, обеспечивающие установку и поддержку соединения, а также описание параметров настройки протокола PPP (англ. Point-to-Point Protocol).



Kaspersky IoT Secure Gateway позволяет [создавать новые профили модема](#), [изменять существующие профили](#) и [переключаться между профилями](#). Разные профили модема позволяют работать с разными операторами сотовой связи. Для использования сотового соединения требуется, чтобы один из профилей модема был активным. По умолчанию активным является один из предустановленных профилей модема.


Таблица профилей модема


В системе предусмотрено два типа профилей модема:

- *Предустановленный профиль* – профиль, поставляемый вместе с устройством. Предустановленный профиль доступен только для чтения.
- *Пользовательский профиль* – профиль, созданный при настройке сотового соединения. Пользовательский профиль доступен для изменения и удаления.

Сведения о профилях модема представлены в таблице **Профили** в разделе **Параметры** → **Сеть** → **Модем**. В таблице для каждого профиля модема отображается следующая информация:

-  – доступ на изменение профиля. Значок, информирующий о том, что профиль доступен только для чтения, отображается только для предустановленного профиля.
- **Активный** – значком  отмечен профиль модема, который используется в программе в текущий момент.
- **Имя** – имя профиля.
- **Изменен** – дата и время последнего изменения профиля.

Нажав на значок , расположенный слева от имени профиля, вы можете просмотреть параметры выбранного профиля. Для каждого файла в таблице **Параметры профиля** отображается следующая информация:

-  – доступ на изменение конфигурационного файла. Значок, информирующий о том, что конфигурационный файл доступен только для чтения, отображается только для главного конфигурационного файла (для предустановленного профиля).
- **Тип** – тип конфигурационного файла.
- **Имя** – имя конфигурационного файла.
- **Изменен** – дата и время последнего изменения конфигурационного файла.

Включение и выключение сотового соединения

Kaspersky IoT Secure Gateway позволяет обрабатывать исходящий и входящий сетевой трафик с использованием сотового соединения (через оператора сотовой связи).

Чтобы включить или выключить использование сотового соединения Kaspersky IoT Secure Gateway:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Сеть**.
2. Перейдите на закладку **Модем** и в блоке **Параметры модема** включите или выключите использование модема с помощью переключателя **Использовать модем как основной канал связи**.
3. Нажмите на кнопку **Сохранить**, чтобы сохранить изменение параметров.
4. [Перезагрузите](#) Kaspersky IoT Secure Gateway, чтобы изменения параметров вступили в силу.

Создание профиля модема

Вы можете создавать новые профили модема. Разные профили модема позволяют работать с разными операторами сотовой связи.

Чтобы создать новый профиль модема:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Сеть**.
2. Выберите закладку **Модем**.
Отобразится окно **Параметры модема**, в нижней части которого содержится таблица профилей модема.
3. Нажмите на кнопку **Создать** в нижней части страницы.
Справа откроется панель **Создание профиля модема**.
4. В раскрывающемся списке **Шаблон** выберите профиль модема, на базе которого вы хотите создать новый профиль. Конфигурационный файл модема выбранного профиля добавится в новый профиль.
Если вы хотите создать пустой профиль, в раскрывающемся списке **Шаблон** выберите **Пустой**. Вы можете [заполнить пустой профиль модема](#) позже.
5. В поле **Имя** введите имя профиля латинскими буквами.
6. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.
Новый профиль модема будет создан и отобразится в таблице **Профили**.

Копирование профиля модема

Вы можете копировать созданный ранее или предустановленный профиль модема, если требуется создать новый профиль модема на базе существующего профиля и не нужно вносить изменений в параметры нового профиля.

Чтобы копировать созданный ранее профиль модема:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Сеть**.

2. Выберите закладку **Модем**.

3. В нижней части окна в таблице **Профили** в графе **Имя** нажмите на имя профиля, на основе которого вы хотите создать новый профиль.

Справа откроется панель **Изменение профиля модема**.

4. Нажмите на значок , расположенный в нижней части панели.

Откроется панель **Копирование профиля модема**.

5. В поле **Имя** введите имя нового профиля латинскими буквами.

6. Нажмите на кнопку **Копировать** в нижней части панели.

Новый профиль модема на основе созданного ранее профиля будет создан и отобразится в таблице **Профили**.


Заполнение пустого профиля модема

Профиль является пустым, если он был создан на базе шаблона **Пустой** и в нем отсутствует конфигурационный файл. Перед использованием пустой профиль требуется заполнить.

Чтобы заполнить пустой профиль модема:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Сеть**.

2. Выберите закладку **Модем**.

3. В нижней части страницы в таблице **Профили**, в графе **Имя** нажмите на значок  рядом с пустым профилем.

Отобразится таблица **Параметры профиля**.

4. Создайте конфигурационный файл модема, нажав на кнопку **Создать файл**.

5. В открывшейся справа панели **Создание конфигурационного файла модема** в поле **Имя** введите имя конфигурационного файла латинскими буквами.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить конфигурационный файл модема.

Панель **Создание конфигурационного файла модема** закроется.

7. Если требуется загрузить готовый конфигурационный файл модема, нажмите на кнопку **Загрузить** в нижней части страницы и в открывшемся окне загрузки файла в систему выберите конфигурационный файл.

Конфигурационный файл загрузится в систему и отобразится в параметрах профиля.

8. Если требуется изменить параметры конфигурационного файла, в таблице параметров профиля нажмите на имя только что созданного (загруженного) конфигурационного файла.

Справа откроется панель **Изменение конфигурационного файла модема**.

9. В нижней части панели нажмите на значок .

Откроется окно текстового редактора для изменения конфигурационного файла.

10. Введите в окне текстового редактора требуемые параметры конфигурационного файла модема.

11. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Изменение профиля модема


Вы можете изменять имя и параметры профиля модема.

Чтобы изменить имя профиля модема:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Сеть**.
2. Выберите закладку **Модем**.
3. В нижней части окна в таблице **Профили** в графе **Имя** нажмите на имя профиля, который вы хотите изменить.
Справа откроется панель **Изменение профиля модема**.
4. В поле **Имя** введите новое имя профиля.
5. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Измененный профиль модема отобразится в таблице **Профили**.

Чтобы изменить параметры профиля модема:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Сеть**.
2. Выберите закладку **Модем**.
3. В нижней части страницы в таблице **Профили**, в графе **Имя** нажмите на значок  рядом с профилем, который вы хотите изменить.

Отобразится таблица **Параметры профиля**, которая содержит список конфигурационных файлов и сертификатов, входящих в профиль. Если профиль был создан на основе шаблона **Пустой**, то список файлов будет пустым. Пустой профиль нужно [заполнить](#).

4. Если требуется изменить конфигурационный файл, нажмите на имя конфигурационного файла и в открывшейся справа панели **Изменение конфигурационного файла модема** выполните следующие действия:
 - a. Нажмите на значок , расположенный в нижней части панели.
 - b. В открывшемся окне текстового редактора измените параметры модема на те, которые требуются.
 - c. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.
Выбранный конфигурационный файл будет изменен. Окно текстового редактора закроется.
5. Если требуется удалить конфигурационный файл, нажмите на имя конфигурационного файла и в открывшейся справа панели **Изменение конфигурационного файла модема** нажмите на значок , расположенный в нижней части панели. Подтвердите удаление файла.
Выбранный конфигурационный файл будет удален из параметров профиля модема.
6. Если требуется загрузить готовый конфигурационный файл модема, нажмите на кнопку **Загрузить** в нижней части страницы и в открывшемся окне загрузки файла в систему выберите конфигурационный

файл.


Конфигурационный файл загрузится в систему и отобразится в параметрах профиля.

Переключение на другой профиль модема

Kaspersky IoT Secure Gateway позволяет переключаться между профилями модема. Разные профили модема позволяют работать с разными операторами сотовой связи. По умолчанию активным является один из предустановленных профилей модема.

Чтобы переключиться на другой профиль модема:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Сеть**.
2. Выберите закладку **Модем**.
3. В нижней части окна в таблице **Профили** в графе **Имя** нажмите на имя профиля, который вы хотите сделать активным.
Справа откроется панель **Изменение профиля модема**.
4. В нижней части панели нажмите на кнопку **Сделать активным**.
5. [Перезагрузите](#) Kaspersky IoT Secure Gateway, чтобы изменения вступили в силу.


В таблице **Профили** в графе **Активный** рядом с выбранным профилем появится значок , профиль станет активным и будет использоваться при подключении к сети.

Удаление профиля модема

Вы можете удалить профиль модема в веб-интерфейсе Kaspersky IoT Secure Gateway.

Kaspersky IoT Secure Gateway не позволяет удалить активный и предустановленные профили модема. Если требуется удалить профиль, который сейчас является активным, сначала нужно [переключиться на другой профиль модема](#).

Чтобы удалить профиль модема:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Сеть**.
2. Выберите закладку **Модем**.
3. В нижней части окна в таблице **Профили** в графе **Имя** нажмите на имя профиля, который вы хотите удалить.
Справа откроется панель **Изменение профиля модема**.
4. Нажмите на значок , расположенный в нижней части панели и подтвердите удаление профиля.

Выбранный профиль модема будет удален из таблицы **Профили**.

Управление безопасностью Kaspersky IoT Secure Gateway

Криптографический протокол TLS обеспечивает безопасность передачи данных с использованием сертификатов SSL-соединений. *Сертификат SSL-соединения* (далее "сертификат") – это блок данных, содержащий информацию о владельце сертификата, открытом ключе владельца, датах начала и окончания действия сертификата.

В Kaspersky IoT Secure Gateway используются следующие сертификаты:

- *Сертификат администратора* для безопасного подключения к веб-интерфейсу Kaspersky IoT Secure Gateway через браузер.
- *Сертификат сервера Kaspersky Security Center* для безопасного подключения к Kaspersky IoT Secure Gateway из веб-интерфейса Kaspersky Security Center Web Console.
- *Сертификат для [отправки уведомлений](#)* MQTT, push и Syslog о событиях, зарегистрированных Kaspersky IoT Secure Gateway.

Рекомендуется обновлять сертификаты в следующих случаях:

- текущие сертификаты скомпрометированы;
- закончился срок действия сертификатов;
- нужно выполнить регулярное обновление сертификатов в соответствии с требованиями информационной безопасности вашей организации.

Вы можете просматривать загруженные ранее сертификаты, добавлять новые или удалять сертификаты из Kaspersky IoT Secure Gateway.

Создание сертификата сервера Kaspersky Security Center

Сертификат сервера Kaspersky Security Center требуется для безопасного подключения к Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console.

Подробную информацию о требованиях, которые предъявляются к сертификатам сервера Kaspersky Security Center, см. в разделе *Требования к пользовательским сертификатам, используемым в Kaspersky Security Center* в онлайн-справке Kaspersky Security Center 13.

Вы можете выпустить новый сертификат сервера Kaspersky Security Center в Kaspersky Security Center Web Console.

Чтобы выпустить новый сертификат сервера Kaspersky Security Center через Kaspersky Security Center Web Console, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console нажмите на значок  рядом с именем нужного Сервера администрирования Kaspersky Security Center.

Откроется окно **Свойства Сервера администрирования**.

2. Перейдите в раздел **Сертификаты**.

3. В блоке параметров **Аутентификация Сервера администрирования устройствами с защитой на уровне UEFI** выберите **Сертификат выпущен средствами Сервера администрирования**.

4. Нажмите на кнопку **Перевыпустить**.

5. В открывшемся окне настройте адрес подключения:

- [Оставить адрес подключения прежним](#) 

Адрес Сервера администрирования, к которому подключается Kaspersky IoT Secure Gateway, останется прежним.

По умолчанию выбран этот вариант.

- [Изменить адрес подключения на](#) 

Если необходимо, чтобы Kaspersky IoT Secure Gateway подключался по другому адресу, укажите в поле требуемый адрес.

6. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Новый сертификат сервера Kaspersky Security Center будет выпущен.

Для загрузки файла сертификата Kaspersky Security Center в веб-интерфейсе Kaspersky IoT Secure Gateway требуется сохранить на локальном компьютере созданный через веб-интерфейс Kaspersky Security Center Web Console файл сертификата Kaspersky Security Center.

Чтобы сохранить файл сертификата Kaspersky Security Center, созданный в Kaspersky Security Center Web Console, выполните следующие действия:

1. В меню веб-интерфейса Kaspersky Security Center Web Console нажмите на значок  рядом с именем нужного Сервера администрирования Kaspersky Security Center.

Откроется окно **Свойства Сервера администрирования**.


2. Перейдите в раздел **Сертификаты**.

3. В группе параметров **Аутентификация Сервера администрирования устройствами с защитой на уровне UEFI** выберите **Сертификат выпущен средствами Сервера администрирования**.

4. Нажмите на кнопку **Управление сертификатом**.

5. В открывшейся справа панели в блоке **Адрес подключения** нажмите на IP-адрес Kaspersky IoT Secure Gateway, для которого был выпущен сертификат.

Начнется автоматическая загрузка файла сертификата.

Также вы можете использовать утилиту `klsrcertgen2.exe` для создания сертификатов сервера Kaspersky Security Center (подробнее см. в разделе Базы знаний [Как сгенерировать сертификат для веб-сервера Kaspersky Security Center 10](#) ).

В Kaspersky IoT Secure Gateway возможно загрузить файл сертификата Kaspersky Security Center только в формате CRT, CER, DER и PEM. Если требуется, вы можете изменить формат файла сертификата Kaspersky Security Center, используя утилиту OpenSSL. Например, для изменения формата файла сертификата с P12 на CRT в консоли выполните команду:

```
openssl pkcs12 -in <имя сертификата>.p12 -clcerts -nokeys -out <имя сертификата>.crt
```

Созданный файл сертификата сервера Kaspersky Security Center нужно [добавить](#) в Kaspersky IoT Secure Gateway для [настройки соединения с Kaspersky Security Center](#).

Создание сертификата администратора

Протокол TLS (англ. Transport Layer Security) – безопасный протокол передачи данных в локальных сетях и в интернете с использованием шифрования. Протокол TLS используется в веб-приложениях для создания защищенных соединений между клиентским приложением и веб-сервером.

Протокол TLS используется в Kaspersky IoT Secure Gateway для организации защищенного канала связи между браузером, с которого пользователь подключается к веб-интерфейсу Kaspersky IoT Secure Gateway, и веб-сервером Kaspersky IoT Secure Gateway. На этапе первичного подключения в веб-интерфейсу Kaspersky IoT Secure Gateway требуется создать и загрузить сертификат администратора. Загруженный сертификат администратора в дальнейшем будет использоваться для повторной аутентификации пользователя при повторном подключении в веб-интерфейсу Kaspersky IoT Secure Gateway.

Создание сертификата администратора должно производиться на доверенном устройстве в условиях безопасной среды (отсутствуют уязвимости и доступ устройства к интернету).

Для создания сертификата администратора вы можете использовать утилиту OpenSSL.

Чтобы создать сертификат администратора с помощью утилиты OpenSSL, выполните следующие действия:

1. Создайте [конфигурационный файл self_signed_config](#) и укажите в нем нужные параметры для выпуска сертификата администратора.

В конфигурационном файле `self_signed_config` требуется указать следующие параметры:

- `default_bits` – параметр, определяющий длину закрытого ключа.
- `default_keyfile` – имя закрытого ключа сертификата аутентификации администратора.
- `distinguished_name` – блок параметров, в котором требуется указать следующие регистрационные данные о компании, выпускающей сертификат:
 - `C` – страна регистрации компании.
 - `ST` – регион регистрации компании.
 - `L` – город регистрации компании.
 - `O` – наименование компании.
 - `OU` – наименование подразделения компании.
 - `CN` – имя сертификата.
 - `emailAddress` – электронный адрес компании.
- `req_extensions` – блок параметров (например, `req_extensions = v3_ca`), в котором требуется указать следующую информацию о выпускаемом сертификате и закрытом ключе к нему.
 - `basicConstraints` – параметр, определяющий является ли данный сертификат корневым, а также определяющий максимальное количество валидных цепочек сертификатов.
 - `keyUsage` – параметр, определяющий цели использования созданного ключа сертификата.
 - `extendedKeyUsage` – параметр, определяющий расширение для параметра `keyUsage`.

Ниже представлен пример конфигурационного файла `self_signed_config`.

Пример параметров в конфигурационном файле `self_signed_config`

```
[ req ]
default_bits = 4096
default_keyfile = cert_key.pem
distinguished_name = req_distinguished_name
req_extensions = v3_ca
[ req_distinguished_name ]
C = Ru
ST = Moscow
L = Moscow
O = Some Organization
OU = Some Organizational Unit
CN = KISGAuthCert
emailAddress = test@email.address
[ v3_ca ]
```

```
basicConstraints = critical, CA:FALSE
keyUsage = digitalSignature, keyAgreement, keyEncipherment, dataEncipherment
extendedKeyUsage = clientAuth
```

2. Запустите консоль и перейдите в директорию, в которой расположен конфигурационный файл `self_signed_config`.

3. В консоли запустите утилиту OpenSSL и выполните команду:

```
openssl req -x509 -newkey rsa:4096 -keyout cert_key.pem -out cert.pem -days 365 \
-subj
'/C=RU/ST=Moscow/L=Moscow/O=SomeOrganization/OU=SomeUnit/emailAddress=test@example.com/
\
-config self_signed_config -extensions v3_ca
```

где:

- `-x509` – параметр, определяющий создание самоподписанного сертификата. В этом случае используется стандарт инфраструктуры открытых ключей протоколов SSL и TLS для управления ключами и сертификатами.
- `-newkey` – параметр, определяющий необходимость создания нового сертификата и нового ключа одновременно.
- `rsa:4096` – параметр, определяющий тип и длину ключа. В результате применения этого параметра будет создан ключ с использованием алгоритма шифрования RSA, длиной 4096 бит.
- `-keyout cert_key.pem` – имя файла, в котором будет сохранен закрытый ключ созданного сертификата.
- `-out cert.pem` – имя файла, в котором будет сохранен созданный сертификат.
- `-days 365` – параметр, определяющий срок действия созданного сертификата администратора.

4. Введите и повторите пароль для закрытого ключа сертификата.

В результате в директории, в которой расположен конфигурационный файл `self_signed_config`, будет создано два файла:

- `cert.pem` – файл сертификата администратора;
- `cert_key.pem` – закрытый ключ сертификата администратора.

Созданный файл сертификата администратора `cert.pem` требуется загрузить при первой [авторизации в веб-интерфейсе Kaspersky IoT Secure Gateway](#).

5. В консоли выполните команду:

```
openssl pkcs12 -export -in cert.pem -inkey cert_key.pem -out cert.p12 -name "cert_key"
```

6. Введите пароль, который вы указали в пункте 4 этой инструкции.

В результате в директории, в которой расположен конфигурационный файл `self_signed_config`, будет создан файл доверенного сертификата `cert.p12`.

Созданный файл доверенного сертификата `cert.p12` требуется добавить в браузере, который вы используете для подключения к веб-интерфейсу Kaspersky IoT Secure Gateway. Подробнее о добавлении файла доверенного сертификата в браузер см. в руководстве используемого браузера.

Обновление сертификатов

Рекомендуется обновлять сертификаты администратора или сервера Kaspersky Security Center в следующих случаях:

- текущие сертификаты скомпрометированы;
- закончился срок действия сертификатов;
- нужно выполнить регулярное обновление сертификатов в соответствии с требованиями информационной безопасности.

При обновлении сертификата администратора в веб-интерфейсе Kaspersky IoT Secure Gateway может потребоваться перезапуск браузера для очистки кеша текущей сессии пользователя в Kaspersky IoT Secure Gateway.

Не рекомендуется загружать широко известные сертификаты удостоверяющего центра, так как доверенными будут являться все серверы, использующие сертификаты, подписанные этими сертификатами удостоверяющего центра. Такая ситуация приведет к компрометации Kaspersky IoT Secure Gateway.

Чтобы добавить или удалить сертификат, выполните следующие действия:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Безопасность системы**.
Отобразится окно, в котором указана следующая информация о сертификатах:

- В области **Сертификат администратора** указаны данные о текущем сертификате администратора.
- В области **Сертификат сервера Kaspersky Security Center** указаны данные о текущем сертификате сервера Kaspersky Security Center.

2. Если требуется добавить сертификат администратора, в блоке **Сертификат администратора** нажмите на кнопку **Загрузить** и открывшемся окне выберите файл сертификата.

Для добавления в качестве сертификата доступны файлы только в формате CRT, CER, DER и PEM.

Новый сертификат администратора будет загружен в систему, загруженный ранее сертификат будет удален.

Kaspersky IoT Secure Gateway не позволяет удалить сертификат администратора.

3. Если требуется добавить или удалить ранее загруженный сертификат сервера Kaspersky Security Center, в блоке **Сертификат сервера Kaspersky Security Center** выполните одно из следующих действий:

- Если требуется загрузить сертификат сервера Kaspersky Security Center, нажмите на кнопку **Загрузить** и в открывшемся окне выберите файл сертификата.

Для добавления в качестве сертификата доступны файлы только в формате CRT, CER, DER и PEM.

Новый сертификат сервера Kaspersky Security Center будет загружен в систему, загруженный ранее сертификат будет удален.

- Если требуется удалить сертификат сервера Kaspersky Security Center, нажмите на кнопку **Удалить** и подтвердите удаление.

Если в системе отсутствует сертификат сервера Kaspersky Security Center, [настройка параметров подключения к серверу Kaspersky Security Center](#) и подключение к серверу Kaspersky Security Center недоступны.

Настройка параметров MQTT-брокера

В Kaspersky IoT Secure Gateway MQTT-брокер Eclipse Mosquitto обеспечивает обмен данными телеметрии по протоколу MQTT (Message Queuing Telemetry Transport). Параметры MQTT хранятся в профиле MQTT-брокера. Профиль MQTT-брокера представляет собой связку из конфигурационного файла Eclipse Mosquitto и сертификатов безопасности. Kaspersky IoT Secure Gateway поставляется с предустановленным профилем, в который входит конфигурационный файл MQTT-брокера. Kaspersky IoT Secure Gateway позволяет [создавать новые профили](#), [изменять существующие профили](#) и [переключаться между профилями](#). Для передачи данных по протоколу MQTT требуется, чтобы один из профилей MQTT-брокера был активным. По умолчанию активным является предустановленный профиль.

MQTT-брокер не поддерживает TLS соединение для трафика, поступающего от контроллеров и датчиков оборудования внутренней сети предприятия.

При настройке параметров MQTT-брокера содержимое конфигурационного файла может содержать персональные данные. Вам нужно контролировать данные, загружаемые в профиль MQTT-брокера Kaspersky IoT Secure Gateway.

В меню веб-интерфейса Kaspersky IoT Secure Gateway рядом с разделом **MQTT-брокер** отображается один из следующих статусов настройки параметров MQTT-брокера:






-  – означает, что параметры MQTT-брокера настроены правильно.
-  – означает, что MQTT-брокер не может подключиться к сети, требуется настроить параметры сети.
-  – означает, что параметры MQTT-брокера настроены неправильно, требуется настроить параметры MQTT-брокера.


Таблица профилей MQTT-брокера


В Kaspersky IoT Secure Gateway предусмотрено два типа профилей MQTT-брокера:

- *Предустановленный профиль* – профиль, поставляемый вместе с устройством. Предустановленный профиль доступен только для чтения.
- *Пользовательский профиль* – профиль, созданный при настройке MQTT-брокера. Пользовательский профиль доступен для изменения и удаления.

Сведения о профилях MQTT-брокера представлены в таблице **Профили** в разделе **MQTT-брокер**. В таблице для каждого профиля MQTT-брокера отображается следующая информация:

-  – доступ на изменение профиля. Значок, информирующий о том, что профиль доступен только для чтения, отображается только для предустановленного профиля.
- **Активный** – значком  отмечен профиль MQTT-брокера, который используется в программе в текущий момент.
- **Имя** – имя профиля.
- **Изменен** – дата и время последнего изменения профиля.

Нажав на значок , расположенный слева от имени профиля, вы можете просмотреть параметры выбранного профиля. Для каждого файла в таблице **Параметры профиля** отображается следующая информация:

-  – доступ на изменение конфигурационного файла. Значок, информирующий о том, что конфигурационный файл доступен только для чтения, отображается только для главного конфигурационного файла (для предустановленного профиля).
- **Тип** – тип конфигурационного файла.
- **Имя** – имя конфигурационного файла.
- **Изменен** – дата и время последнего изменения конфигурационного файла.

Создание профиля MQTT-брокера

Вы можете создавать новые профили MQTT-брокера. Разные профили MQTT-брокера позволяют работать с разными серверами и цифровыми платформами, которые принимают события от Kaspersky IoT Secure Gateway по протоколу MQTT.

Чтобы создать новый профиль MQTT-брокера:

1. В меню в левой части страницы веб-интерфейса выберите раздел **MQTT-брокер**.
Отобразится таблица, в которой перечислены профили MQTT-брокера.
2. Нажмите на кнопку **Создать** в нижней части страницы.
Справа откроется панель **Создание профиля MQTT-брокера**.
3. В раскрывающемся списке **Шаблон** выберите профиль MQTT-брокера, на базе которого вы хотите создать новый профиль.
Конфигурационный файл Eclipse Mosquitto и сертификаты безопасности выбранного профиля добавятся в новый профиль.
Если вы хотите создать пустой профиль, в раскрывающемся списке **Шаблон** выберите **Пустой**. Вы можете [заполнить](#) пустой профиль позже.
4. В поле **Имя** введите имя профиля латинскими буквами.
5. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Новый профиль MQTT-брокера будет создан и отобразится в таблице **Профили**.

Копирование профиля MQTT-брокера

Вы можете копировать созданный ранее или предустановленный профиль MQTT-брокера, если требуется создать новый профиль MQTT-брокера на базе существующего профиля и не нужно вносить изменений в параметры нового профиля.

Чтобы копировать созданный ранее профиль MQTT-брокера:

1. В меню в левой части страницы веб-интерфейса выберите раздел **MQTT-брокер**.

Отобразится таблица, в которой перечислены профили MQTT-брокера.

2. В графе **Имя** нажмите на имя профиля, который вы хотите изменить.

Справа откроется панель **Изменение профиля MQTT-брокера**.

3. Нажмите на значок , расположенный в нижней части панели.

Откроется панель **Копирование профиля MQTT-брокера**.

4. В поле **Имя** введите имя профиля латинскими буквами.

5. Нажмите на кнопку **Копировать** в нижней части панели.

Новый профиль MQTT-брокера на основе созданного ранее профиля будет создан и отобразится в таблице **Профили**.

Заполнение пустого профиля MQTT-брокера

Профиль MQTT-брокера является пустым, если он был создан на базе шаблона **Пустой** и не был заполнен ранее. В параметрах пустого профиля отсутствуют конфигурационные файлы и сертификаты.

Чтобы заполнить пустой профиль MQTT-брокера:

1. В меню в левой части страницы веб-интерфейса выберите раздел **MQTT-брокер**.

2. В таблице **Профили**, в графе **Имя** нажмите на значок , расположенный рядом с профилем, который требуется заполнить.

Отобразится таблица **Параметры профиля**.

3. Добавьте в профиль MQTT-брокера сертификат безопасности, нажав на кнопку **Загрузить** в нижней части страницы и в открывшемся окне загрузки файла в систему выберите файл сертификата в формате PEM. Размер файла не должен превышать 131 КБ.

Файл сертификата загрузится в систему и отобразится в параметрах профиля MQTT-брокера.


Профиль MQTT-брокера требует несколько сертификатов безопасности: сертификат, выданный удостоверяющим центром, сертификат сервера и файл приватного ключа. Если ваш профиль предполагает использование SSL/TLS, повторите этот шаг столько раз, сколько требуется, чтобы загрузить в систему все необходимые сертификаты.

4. Создайте конфигурационный файл в профиле MQTT-брокера, нажав на кнопку **Создать файл**.

Справа откроется панель **Создание конфигурационного файла MQTT-брокера**.

5. В раскрывающемся списке **Тип** выберите тип конфигурационного файла. Для выбора доступны следующие варианты:

- **Главный конфигурационный файл.** Содержит основные параметры для работы MQTT-брокера. Главный конфигурационный файл требуется добавить в профиль MQTT-брокера, чтобы этот профиль можно было активировать.
 - **Конфигурационный файл.** Содержит дополнительные параметры для работы MQTT-брокера.
6. В поле **Имя** введите имя конфигурационного файла латинскими буквами.
 7. Нажмите на кнопку **Сохранить**, чтобы сохранить конфигурационный файл Eclipse Mosquitto MQTT-брокера.
Панель **Создание конфигурационного файла MQTT-брокера** закрывается.
 8. В таблице **Параметры профиля** нажмите на имя только что созданного конфигурационного файла.
 9. В нижней части открывшейся справа панели **Изменение конфигурационного файла MQTT-брокера** нажмите на значок .
 - Откроется окно текстового редактора для изменения конфигурационного файла.
 10. Введите в окне текстового редактора требуемые параметры конфигурационного файла Eclipse Mosquitto MQTT-брокера.

Подробную информацию о параметрах конфигурационного файла Eclipse Mosquitto MQTT-брокера вы можете узнать в документации на [веб-сайте разработчика](#) . Настройка MQTT-брокера в Kaspersky IoT Secure Gateway доступна с [ограничениями](#).

11. Если требуется добавить в профиль готовый конфигурационный файл, нажмите на кнопку **Загрузить** в нижней части страницы и в открывшемся окне загрузки файла в систему выберите файл в формате CONF. Конфигурационный файл загрузится в систему и отобразится в параметрах профиля MQTT-брокера.

Kaspersky IoT Secure Gateway не позволяет загружать главный конфигурационный файл. Файл этого типа можно только создать.

12. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Изменение профиля MQTT-брокера


Вы можете изменять имя и параметры профиля MQTT-брокера.

Чтобы изменить имя профиля MQTT-брокера:

1. В меню в левой части страницы веб-интерфейса выберите раздел **MQTT-брокер**.
Отобразится таблица **Профили**.
2. В графе **Имя** нажмите на имя профиля, который вы хотите изменить.
Справа откроется панель **Изменение профиля MQTT-брокера**.
3. В поле **Имя** введите новое имя профиля.
4. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Измененный профиль MQTT-брокера отобразится в таблице **Профили**.

Чтобы изменить параметры профиля MQTT-брокера:


1. В меню в левой части страницы веб-интерфейса выберите раздел **MQTT-брокер**.
2. В таблице **Профили**, в графе **Имя** нажмите на значок , расположенный рядом с профилем, который вы хотите изменить.

Отобразится таблица **Параметры профиля**, которая содержит список конфигурационных файлов и сертификатов, входящих в профиль MQTT-брокера. Если профиль был создан на основе шаблона **Пустой**, то список файлов будет пустым. Пустой профиль нужно [заполнить](#).

3. Если требуется добавить в профиль готовый конфигурационный файл, нажмите на кнопку **Загрузить** в нижней части страницы и в открывшемся окне загрузки файла в систему выберите файл в формате CONF. Конфигурационный файл загрузится в систему и отобразится в параметрах профиля MQTT-брокера.

Kaspersky IoT Secure Gateway не позволяет загружать главный конфигурационный файл. Файл этого типа можно только создать.


4. Если требуется изменить конфигурационный файл в профиле MQTT-брокера, нажмите на имя конфигурационного файла, который вы хотите изменить и в открывшейся справа панели **Изменение конфигурационного файла MQTT-брокера** выполните следующие действия:

- a. Нажмите на значок , расположенный в нижней части панели.
- b. В открывшемся окне текстового редактора измените параметры на те, которые требуются.

Подробную информацию о параметрах конфигурационного файла Eclipse Mosquitto вы можете узнать в документации на [веб-сайте разработчика](#)². Настройка профиля MQTT-брокера в Kaspersky IoT Secure Gateway доступна с [ограничениями](#).

- c. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.


Выбранный конфигурационный файл будет изменен. Окно текстового редактора закроется.

5. Если требуется удалить конфигурационный файл из профиля MQTT-брокера, нажмите на имя конфигурационного файла и в открывшейся справа панели **Изменение конфигурационного файла MQTT-брокера** нажмите на значок , расположенный в нижней части панели. Подтвердите удаление файла.

Выбранный конфигурационный файл будет удален из параметров профиля MQTT-брокера.

6. Если требуется добавить в профиль MQTT-брокера сертификат безопасности, нажмите на кнопку **Загрузить** в нижней части страницы и в открывшемся окне загрузки файла в систему выберите файл сертификата в формате PEM. Размер файла не должен превышать 131 КБ.

Файл сертификата загрузится в систему и отобразится в параметрах профиля MQTT-брокера.

7. Если требуется удалить из профиля сертификат безопасности, нажмите на имя этого сертификата в таблице **Параметры профиля** и в открывшейся справа панели нажмите на значок . Подтвердите удаление сертификата.


Выбранный файл сертификата безопасности будет удален из параметров профиля MQTT-брокера.

Переключение на другой профиль MQTT-брокера

Kaspersky IoT Secure Gateway позволяет переключаться между профилями MQTT-брокера. В Kaspersky IoT Secure Gateway разные профили MQTT-брокера позволяют работать с разными серверами и цифровыми платформами при получении от них данных телеметрии по протоколу MQTT. По умолчанию активным является предустановленный профиль MQTT-брокера.

Чтобы переключиться на другой профиль MQTT-брокера:

1. В меню в левой части страницы веб-интерфейса выберите раздел **MQTT-брокер**.
2. В таблице **Профили** в графе **Имя** нажмите на имя профиля, который вы хотите сделать активным.
Откроется окно **Изменение профиля MQTT-брокера**.
3. В нижней части открывшегося окна нажмите на кнопку **Сделать активным**.


В таблице **Профили** в графе **Активный** рядом с выбранным профилем появится значок , профиль станет активным и будет использоваться Kaspersky IoT Secure Gateway при получении данных по протоколу MQTT.

Удаление профиля MQTT-брокера

Kaspersky IoT Secure Gateway позволяет удалять профили MQTT-брокера.

Kaspersky IoT Secure Gateway не позволяет удалить активный и предустановленный профили MQTT-брокера. Если требуется удалить профиль, который сейчас является активным, сначала нужно [переключиться на другой профиль MQTT-брокера](#).

Чтобы удалить профиль MQTT-брокера:

1. В меню в левой части страницы веб-интерфейса выберите раздел **MQTT-брокер**.
Отобразится таблица **Профили**, в которой перечислены профили MQTT-брокера.
2. В графе **Имя** нажмите на имя профиля, который вы хотите удалить.
Справа откроется панель **Изменение профиля MQTT**.
3. Нажмите на значок , расположенный в нижней части панели и подтвердите удаление профиля.
Выбранный профиль MQTT-брокера будет удален из таблицы **Профили**.

Ограничения при настройке MQTT-брокера

Kaspersky IoT Secure Gateway поддерживает настройку параметров MQTT-брокера Eclipse Mosquitto со следующими ограничениями:

- Не допускается использование параметров `capath` и `bridge_capath` для назначения пути расположения файлов.

- Требуется явно указывать идентификатор клиента `clientid` (например, через `use_username_as_clientid`).
- Не допускается использование протокола TLS для конфигурации соединения с сервером (`listener`).
Для настройки соединения с сервером не поддерживаются следующие параметры: `cafile`, `certfile`, `ciphers_tls1.3`, `crlfile`, `dhparamfile`, `keyfile`, `require_certificate`, `tls_engine`, `tls_engine_kpass_sha1`, `tls_keyform`, `use_identity_as_username`, `use_subject_as_username`, `psk_hint`.
- Для соединения с клиентом (`bridge`) допускается использование только протокола TLS.
Для настройки соединения с клиентом не поддерживаются следующие параметры: `bridge_insecure` (всегда `false`), `bridge_alpn`, `bridge_cpath`, `bridge_identity`, `bridge_psk`, `bridge_require_ocsp`, `bridge_tls_version`.
- Для каждого профиля MQTT-брокера возможно соединение только с одним клиентским приложением (возможно указать только один параметр `bridge` в конфигурационном файле). Одновременная работа с несколькими клиентскими соединениями не поддерживается. Для установки соединения с другим клиентом требуется [переключиться на другой профиль MQTT-брокера](#).
- При настройке профиля MQTT-брокера не поддерживаются следующие параметры: `bridge_require_ocsp`, `log_dest_file`, `pid_file` и `http_dir`, `persistence`, `websockets`, `auth_plugin`, `password_file`, `allow_anonymous`.
- Для соединения MQTT-брокера с цифровой платформой, поддерживающей протокол MQTT, требуется указывать стандартный порт для подключения – 8883.
- Для соединения конечного устройства с Kaspersky IoT Secure Gateway требуется использовать порт 1883.

Настройка веб-сервера

Работу веб-интерфейса Kaspersky IoT Secure Gateway обеспечивает веб-сервер CivetWeb. Параметры веб-сервера хранятся в профиле веб-сервера. Профиль веб-сервера представляет собой связку из конфигурационного файла CivetWeb и сертификата безопасности. Kaspersky IoT Secure Gateway поставляется с предустановленным профилем, в который входит сертификат безопасности, подписанный "Лабораторией Касперского".

После первого включения требуется заменить сертификат безопасности, установленный по умолчанию для [веб-сервера](#), на сертификат безопасности, используемый в вашей организации.



Kaspersky IoT Secure Gateway позволяет [создавать новые профили](#), [изменять существующие профили](#) и [переключаться между профилями](#). Разные профили позволяют работать с разными сертификатами безопасности. Для работы веб-интерфейса Kaspersky IoT Secure Gateway требуется, чтобы один из профилей веб-сервера был активным. По умолчанию активным является предустановленный профиль.


Таблица профилей веб-сервера


В Kaspersky IoT Secure Gateway предусмотрено два типа профилей веб-сервера:

- *Предустановленный профиль* – профиль, поставляемый вместе с устройством. Предустановленный профиль доступен только для чтения.
- *Пользовательский профиль* – профиль, созданный при настройке веб-сервера. Пользовательский профиль доступен для изменения и удаления.

Сведения о профилях веб-сервера представлены в таблице **Профили** в разделе **Параметры** → **Веб-сервер**. В таблице для каждого профиля веб-сервера отображается следующая информация:

-  – доступ на изменение профиля веб-сервера. Значок, информирующий о том, что профиль доступен только для чтения, отображается только для предустановленного профиля.
- **Активный** – значком  отмечен профиль веб-сервера, который используется в программе в текущий момент.
- **Имя** – имя профиля веб-сервера.
- **Изменен** – дата и время последнего изменения профиля.

Нажав на значок , расположенный слева от имени профиля веб-сервера, вы можете просмотреть параметры выбранного профиля. Для каждого файла в таблице **Параметры профиля** отображается следующая информация:

-  – доступ на изменение файла. Значок, информирующий о том, что файл доступен только для чтения, отображается только для файлов предустановленного профиля.
- **Тип** – тип файла.
- **Имя** – имя файла.
- **Изменен** – дата и время последнего изменения файла.

Создание профиля веб-сервера

Вы можете создавать новые профили веб-сервера. Разные профили веб-сервера позволяют работать с разными сертификатами безопасности.

Чтобы создать новый профиль веб-сервера:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Веб-сервер**.
Откроется окно, в котором отображается таблица профилей веб-сервера.
2. Нажмите на кнопку **Создать** в нижней части страницы.
Справа откроется панель **Создание профиля веб-сервера**.
3. В раскрывающемся списке **Шаблон** выберите профиль веб-сервера, на базе которого вы хотите создать новый профиль.
Конфигурационный файл CivetWeb и сертификат безопасности выбранного профиля добавятся в новый профиль.
Если вы хотите создать пустой профиль, в раскрывающемся списке **Шаблон** оставьте **Пустой**. Вы можете [заполнить](#) пустой профиль веб-сервера позже.
4. В поле **Имя** введите имя профиля латинскими буквами.


5. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Новый профиль веб-сервера будет создан и отобразится в таблице **Профили**.

Копирование профиля веб-сервера

Вы можете копировать созданный ранее или предустановленный профиль веб-сервера, если требуется создать новый профиль веб-сервера на базе существующего профиля и не нужно вносить изменений в параметры нового профиля.

Чтобы копировать созданный ранее профиль веб-сервера:


1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Веб-сервер**.
Откроется окно, в котором отображается таблица профилей веб-сервера.
2. В графе **Имя** нажмите на имя профиля, который вы хотите изменить.
Справа откроется панель **Изменение профиля веб-сервера**.
3. Нажмите на значок , расположенный в нижней части панели.
Откроется панель **Копирование профиля веб-сервера**.
4. В поле **Имя** введите имя профиля латинскими буквами.
5. Нажмите на кнопку **Копировать** в нижней части панели.

Новый профиль веб-сервера на основе созданного ранее профиля будет создан и отобразится в таблице **Профили**.


Заполнение пустого профиля веб-сервера

Профиль веб-сервера является пустым, если он был создан на базе шаблона **Пустой** и не был заполнен ранее. В параметрах пустого профиля отсутствуют конфигурационные файлы и сертификаты.

Чтобы заполнить пустой профиль веб-сервера:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Веб-сервер**.
2. В таблице **Профили**, в графе **Имя** нажмите на значок , расположенный рядом с профилем, который требуется заполнить.
Отобразится таблица **Параметры профиля**.
3. Добавьте в профиль веб-сервера сертификат безопасности, нажав на кнопку **Загрузить** в нижней части страницы и в открывшемся окне загрузки файла в систему выберите файл сертификата в формате PEM.
Файл сертификата загрузится в систему и отобразится в параметрах профиля.
4. Создайте конфигурационный файл в профиле веб-сервера, нажав на кнопку **Создать файл**.
Справа откроется панель **Создание конфигурационного файла веб-сервера**.
5. В открывшейся панели в поле **Имя** введите имя конфигурационного файла латинскими буквами.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить конфигурационный файл.

Панель **Создание конфигурационного файла веб-сервера** закрывается.

7. В таблице **Параметры профиля** нажмите на имя только что созданного конфигурационного файла. Справа откроется панель **Изменение конфигурационного файла веб-сервера**.
8. В нижней части открывшейся панели нажмите на значок .
9. Введите в окне текстового редактора имя файла сертификата, загруженного в пункте 3, чтобы в профиль веб-сервера загрузился нужный сертификат.
`ssl_certificate <certificate name>`

В текущей версии Kaspersky IoT Secure Gateway поддерживаются только параметры CivetWeb: `ssl_certificate` и `ssl_key`.

10. Если требуется добавить в профиль готовый конфигурационный файл, нажмите на кнопку **Загрузить** в нижней части страницы и в открывшемся окне загрузки файла в систему выберите файл в формате CONF. Конфигурационный файл загрузится в систему и отобразится в параметрах профиля веб-сервера.
11. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Изменение профиля веб-сервера


Вы можете изменять имя и параметры профиля веб-сервера.




Чтобы изменить имя профиля веб-сервера:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Веб-сервер**. Отобразится таблица **Профили**.
2. В графе **Имя** нажмите на имя профиля веб-сервера, который вы хотите изменить. Справа откроется панель **Изменение профиля веб-сервера**.
3. В поле **Имя** введите новое имя профиля.
4. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Измененный профиль веб-сервера отобразится в таблице **Профили**.

Чтобы изменить параметры профиля веб-сервера:


1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Веб-сервер**. Отобразится таблица **Профили**.
2. В таблице **Профили**, в графе **Имя** нажмите на значок , расположенный рядом с профилем веб-сервера, параметры которого вы хотите изменить. Отобразится таблица **Параметры профиля**, которая содержит список конфигурационных файлов и сертификатов, входящих в профиль веб-сервера. Если профиль был создан на основе шаблона **Пустой**, то список файлов будет пустым. Пустой профиль веб-сервера нужно [заполнить](#).

3. Если требуется добавить в профиль готовый конфигурационный файл, нажмите на кнопку **Загрузить** в нижней части страницы и в открывшемся окне загрузки файла в систему выберите файл в формате CONF. Конфигурационный файл загрузится в систему и отобразится в параметрах профиля веб-сервера.
4. Если требуется изменить конфигурационный файл, нажмите на имя конфигурационного файла и в открывшейся справа панели **Изменение конфигурационного файла веб-сервера** выполните следующие действия:
 - a. Нажмите на значок , расположенный в нижней части панели.
 - b. В открывшемся окне текстового редактора измените параметры веб-сервера на те, которые требуются.
 - c. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения. Выбранный конфигурационный файл будет изменен. Окно текстового редактора закроется.
5. Если требуется удалить конфигурационный файл, нажмите на имя конфигурационного файла и в открывшейся справа панели **Изменение конфигурационного файла веб-сервера** нажмите на значок , расположенный в нижней части панели. Подтвердите удаление файла. Выбранный конфигурационный файл будет удален из параметров профиля веб-сервера.
6. Если требуется добавить в профиль сертификат безопасности, нажмите на кнопку **Загрузить** в нижней части страницы и в открывшемся окне загрузки файла в систему выберите файл сертификата в формате PEM. Файл сертификата загрузится в систему и появится в параметрах профиля.
7. Если требуется удалить из профиля сертификат безопасности, нажмите на имя этого сертификата в таблице **Параметры профиля** и в открывшейся справа панели нажмите на значок . Подтвердите удаление сертификата. Файл сертификата будет удален из системы.

Переключение на другой профиль веб-сервера

Kaspersky IoT Secure Gateway позволяет переключаться между профилями веб-сервера. Разные профили позволяют работать с разными сертификатами безопасности. По умолчанию активным является предустановленный профиль веб-сервера.

Чтобы переключиться на другой профиль веб-сервера:


1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Веб-сервер**.
2. В таблице **Профили** в графе **Имя** нажмите на имя профиля веб-сервера, который вы хотите сделать активным. Откроется окно **Изменение профиля веб-сервера**.
3. В нижней части открывшегося окна нажмите на кнопку **Сделать активным**. В таблице **Профили** в графе **Активный** рядом с выбранным профилем появится значок , профиль станет активным и будет использоваться при работе веб-интерфейса Kaspersky IoT Secure Gateway.

Удаление профиля веб-сервера

Kaspersky IoT Secure Gateway позволяет удалять профили веб-сервера.

Kaspersky IoT Secure Gateway не позволяет удалить активный и предустановленный профили веб-сервера. Если требуется удалить профиль, который сейчас является активным, сначала нужно [переключиться на другой профиль веб-сервера](#).

Чтобы удалить профиль веб-сервера:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Веб-сервер**.
2. В нижней части окна в таблице **Профили** в графе **Имя** нажмите на имя профиля веб-сервера, который вы хотите удалить.
Справа откроется панель **Изменение профиля веб-сервера**.
3. Нажмите на значок , расположенный в нижней части панели и подтвердите удаление профиля.
Выбранный профиль веб-сервера будет удален из таблицы **Профили**.

Настройка отправки уведомлений при регистрации событий

Этот раздел содержит информацию о настройке отправки уведомлений при регистрации [событий](#) в Kaspersky IoT Secure Gateway.

Настройка отправки журналов событий на сервер Syslog

Kaspersky IoT Secure Gateway может отправлять [журналы событий безопасности сети и аудита](#) на сервер Syslog.

Чтобы настроить отставку журналов событий безопасности сети и аудита на сервер Syslog:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Инструменты**.
Откроется страница на закладке **Syslog**.
2. Установите переключатель **Использовать сервер Syslog для передачи событий** в положение включено.
3. Настройте параметры отправки журналов событий, указав следующие параметры:
 - В поле **IP-адрес** введите IP-адрес и порт стороннего сервера Syslog, например 198.51.100.0:514.
 - В раскрывающемся списке **Режим** выберите протокол, по которому Kaspersky IoT Secure Gateway будет передавать журналы событий безопасности сети и аудита на сторонний сервер Syslog:
 - UDP.
 - TCP.
 - TCP/TLS.
 - Если для отправки журналов выбран протокол **TCP/TLS**, загрузите сертификат безопасности. Для этого нажмите на кнопку **Загрузить новый сертификат** и в открывшемся окне выберите нужный

сертификат безопасности.

4. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Настройка отправки push-уведомлений

Firebase Cloud Messaging (FCM) – это кроссплатформенное решение для обмена сообщениями, которое позволяет надежно отправлять сообщения бесплатно.

Kaspersky IoT Secure Gateway отправляет push-уведомления о событиях с помощью [Firebase Cloud Messaging](#) по протоколу HTTPS на адрес <https://fcm.googleapis.com/fcm/send> в виде JSON-сообщений. Система транслирует информацию о своем имени и предоставляемых топиках push-уведомлений каждые четыре секунды в топик `/topics/DevicesandTopics`, находящийся в облачной службе FCM.

Например, система с именем `Device-1` позволяет подписаться на push-уведомления о событиях типа `NewRecord`, `NewDevice` и `DeviceUpdate`.

Пример данных JSON, отправляемых системой о своем имени и предоставляемых топиках push-уведомлений:

```
{
  "data": {
    "Device" : "Device-1",
    "Audit" : "NewRecord",
    "TrafficProcessor" : "NewDevice, DeviceUpdate",
  },
  "to": "/topics/DevicesAndTopics"
}
```

Push-уведомление о событии отправляется в топик `/topics/DeviceName_EntityName_EventType`, где:

- `DeviceName` – имя устройства.
- `EntityName` – имя сущности, зарегистрировавшей событие.
- `EventType` – тип события.

Пример данных JSON, отправляемых системой о произошедшем событии:

```
{
  "data": {
    "data" : "Some data about new device",
  },
  "to": "/topics/Device-1_TrafficProcessor_NewDevice"
}
```

Для получения push-уведомлений вы можете создать собственное приложение, работающее с FCM. Для этого вам понадобятся конфигурационный файл `google-services.json` и имя системы. Подробную информацию о создании приложения для получения push-уведомлений см. в [документации Firebase Cloud Messaging](#).

Чтобы настроить имя системы для отправки push-уведомлений:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Инструменты**.
2. Выберите закладку **Push-уведомления**.

3. В поле **Имя устройства** введите имя, под которым система будет отправлять push-уведомления.
4. В поле **Ключ авторизации** введите ключ авторизации Firebase.
5. Если требуется загрузить сертификат безопасности, нажмите на кнопку **Загрузить новый сертификат** и в открывшемся окне выберите нужный сертификат безопасности. Отобразится информация о загруженном сертификате.
6. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Настройка отправки MQTT-уведомлений

Kaspersky IoT Secure Gateway может отправлять уведомления о событиях безопасности и аудита по протоколу MQTT.

Чтобы настроить отправку MQTT-уведомлений:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Инструменты**.
2. Выберите закладку **MQTT-уведомления**.
3. Включите отправку MQTT-уведомлений, установив переключатель **Использовать MQTT для передачи событий** в положение включено.
4. Настройте параметры отправки MQTT-уведомлений:
 - a. В поле **IP-адрес** введите IP-адрес используемого MQTT-брокера
 - b. В поле **Порт** введите номер порта используемого MQTT-брокера.

Для соединения Kaspersky IoT Secure Gateway с MQTT-брокером, который находится во внутренней сети вы можете использовать порты 1883 и 8883.

Для соединения Kaspersky IoT Secure Gateway с MQTT-брокером, который находится во внешней сети вы можете использовать порт 8883.

- c. В поле **Имя MQTT-топика** укажите имя MQTT-топика для отправки уведомлений о событиях аудита.
- d. Если требуется отправлять уведомления о событиях аудита от имени определенного пользователя, установите переключатель **Использовать аутентификацию** в положение включено и укажите следующие данные:
 - В поле **Имя пользователя** введите имя учетной записи пользователя для авторизации на сервере.
 - В поле **Пароль** введите пароль учетной записи пользователя для авторизации на сервере.
Учетные данные пользователя вы можете получить у администратора системы. По умолчанию отправка от имени определенного пользователя выключена.
- e. Если требуется использовать защищенное SSL-соединение, установите переключатель **Использовать защищенное SSL-соединение** в положение включено и выполните следующие действия:

1. Загрузите сертификат удостоверяющего центра. Для этого нажмите на кнопку **Загрузить сертификат** и выберите файл сертификата на локальном устройстве.

Информация о загруженном сертификате удостоверяющего центра отобразится на странице.

Не рекомендуется загружать широко известные сертификаты удостоверяющего центра, так как доверенными будут являться все серверы, использующие сертификаты, подписанные этими сертификатами удостоверяющего центра. Такая ситуация приведет к компрометации Kaspersky IoT Secure Gateway.

2. Загрузите сертификат клиента. Для этого нажмите на кнопку **Загрузить сертификат клиента** и выберите файл сертификата на локальном устройстве.

Информация о загруженном сертификате клиента отобразится на странице.

3. Загрузите ключ к сертификату клиента. Для этого нажмите на кнопку **Загрузить ключ** и выберите файл ключа на локальном устройстве.

По умолчанию использование защищенного SSL-соединения выключено.

5. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Настройка даты и времени

В Kaspersky IoT Secure Gateway вы можете настроить дату и время.

Чтобы настроить дату и время:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Общие** → **Дата и время**.
2. В раскрывающихся списках **День**, **Месяц** и **Год** укажите текущую дату.
3. Нажмите на кнопку **Сохранить** в блоке изменения даты, чтобы сохранить изменения.
4. В раскрывающихся списках **Часы**, **Минуты**, **Секунды** укажите текущее время.


Указывайте текущее время в часовом поясе UTC.

5. Нажмите на кнопку **Сохранить** в блоке изменения времени, чтобы сохранить изменения.

Изменение языка веб-интерфейса Kaspersky IoT Secure Gateway

Kaspersky IoT Secure Gateway позволяет выбрать язык веб-интерфейса.

Чтобы изменить язык веб-интерфейса Kaspersky IoT Secure Gateway:

1. В меню в левой части страницы веб-интерфейса выберите пункт  **<имя пользователя>**.
Появится меню пользователя.

2. В меню пользователя в пункте **Язык** выберите **Русский** или **Английский**.

Язык веб-интерфейса Kaspersky IoT Secure Gateway будет изменен на выбранный.

Также вы можете изменить язык веб-интерфейса на странице входа в Kaspersky IoT Secure Gateway или странице возобновления сеанса подключения к Kaspersky IoT Secure Gateway в верхней части страницы справа.

Решение типовых задач

Этот раздел содержит описание типовых пользовательских задач и инструкции по их выполнению.

Мониторинг состояния Kaspersky IoT Secure Gateway

Сводная информация о состоянии Kaspersky IoT Secure Gateway и состоянии безопасности сети отображается в разделе веб-интерфейса **Информационная панель**. Раздел содержит следующие информационные блоки:

- **Информация.** Содержит название и серийный номер аппаратной платформы, версию программы Kaspersky IoT Secure Gateway.
- **События.** Содержит информацию о количестве событий безопасности сети для каждого компонента, зарегистрировавшего события.

События безопасности сети не хранятся в системе и доступны, только пока активна текущая сессия подключения к веб-интерфейсу Kaspersky IoT Secure Gateway.

- **Аудит.** Содержит информацию о наличии событий, связанных с безопасностью Kaspersky IoT Secure Gateway, которые записываются в журнал аудита. Возможны следующие статусы безопасности системы:
 - **Проблемы** – зарегистрированы события с уровнем важности *Важные* или *Критические*.
 - **Нет ошибок** – отсутствуют события или есть события с уровнем важности *Информационные*.
- **MQTT-брокер.** Содержит информацию о статистике работы Kaspersky IoT Secure Gateway по протоколу MQTT и информацию о наличии проблем с передачей данных по протоколу MQTT:
 - **Проблемы** – обнаружены проблемы с передачей данных по протоколу MQTT.
 - **Нет ошибок** – отсутствуют проблемы.
- **Устройства.** Содержит информацию о количестве устройств, [обнаруженных в сети](#).

Вы можете просмотреть подробную информацию в каждом информационном блоке, нажав **Показать** в правой части блока.

Мониторинг состояния сотового соединения

Если в устройстве отсутствует модем, использование сотового соединения и настройка параметров такого соединения недоступны.

Вы можете следить за состоянием сотового соединения Kaspersky IoT Secure Gateway в разделе **Параметры** → **Сеть** → **Модем**. В области **Параметры модема** отображается следующая информация о состоянии сотового соединения:

- **Статус модема** – параметр, отображающий состояние сотового соединения Kaspersky IoT Secure Gateway. Возможны следующие значения параметра:

- Серый значок означает, что модем недоступен для использования в текущий момент.
- Зеленый значок означает, что Kaspersky IoT Secure Gateway подключен к внешней сети через модем, и есть соединение.
- Красный значок означает, что Kaspersky IoT Secure Gateway не подключен к внешней сети через модем, и соединение отсутствует.
- **Уровень сигнала** – параметр, отображающий качество сотового соединения Kaspersky IoT Secure Gateway с внешней сетью.

Количество линий показывает уровень сигнала сети сотовой связи, к которой подключено устройство. При ухудшении уровня сигнала количество линий уменьшается

В блоке **Адреса DNS-серверов модема** вы можете просмотреть информацию об IP-адресах основного и дополнительного DNS-серверов модема.

При отсутствии подключения через сотовую связь требуется проверить выполнение следующих условий:

- используемая в модеме SIM-карта является исправной, и подключен тариф, поддерживающий интернет-соединение через модем;
- выбранный профиль модема соответствует используемой SIM-карте;
- модем доступен для использования (отображается зеленый значок в блоке **Параметры модема**).

Если модем недоступен для использования (отображается серый или красный значок в блоке **Параметры модема**) требуется выполнить [перезагрузку Kaspersky IoT Secure Gateway](#) и снова проверить доступность модема для использования. Устройствам, которые выходят в интернет через Kaspersky IoT Secure Gateway, необходимо получать параметры внутренней сети через DHCP-сервер Kaspersky IoT Secure Gateway. Нужные адреса DNS-серверов от операторов сотовой сети будут получены вместе с этими параметрами.

Мониторинг устройств Kaspersky IoT Secure Gateway

Этот раздел содержит инструкции по мониторингу устройств Kaspersky IoT Secure Gateway и работе со списком разрешенных устройств.

Просмотр списка устройств

В разделе **Устройства** отображается информация об устройствах, которые Kaspersky IoT Secure Gateway обнаружил в сети.

Kaspersky IoT Secure Gateway разделяет обнаруженные устройства на авторизованные и неавторизованные. Каждое новое устройство, обнаруженное системой в сети, считается неавторизованным. Чтобы сделать устройство авторизованным, нужно добавить его в список разрешенных.

При появлении недоверенного устройства в сети, обратитесь к сотруднику, ответственному за информационную безопасность в вашей организации.

Чтобы просмотреть список обнаруженных Kaspersky IoT Secure Gateway устройств:

1. В левой части страницы в меню веб-интерфейса Kaspersky IoT Secure Gateway выберите раздел **Устройства**.

Отобразится страница **Устройства**, на которой представлена таблица обнаруженных в сети устройств.

В таблице отображаются устройства, обнаруженные системой на момент открытия раздела **Устройства**. Таблица устройств не обновляется автоматически. По умолчанию в таблице отображаются все неавторизованные устройства всех обнаруженных типов.

При обнаружении устройств в сети организации имя устройства может хранить персональные данные пользователя. Вам нужно переименовать устройство при добавлении его в список разрешенных.

Если авторизованное устройство отсутствует в сети в течение трех минут, то в таблице обнаруженных устройств удаляется информация о его IP-адресе, при повторном обнаружении этого устройства в сети, IP-адрес этого устройства обновляется. Если неавторизованное устройство отсутствует в сети в течение трех минут, то оно автоматически удаляется из таблицы обнаруженных устройств.

Для каждого обнаруженного системой устройства отображается следующая информация:

- **Имя** – имя устройства.
- **Тип** – тип устройства.
- **Статус** – статус устройства (*Неавторизованный* или *Авторизованный*).
- **MAC-адрес** – MAC-адрес устройства.
- **IP-адрес** – IP-адрес устройства.
- **Сведения** – дополнительная информация об устройстве, если ее удалось определить, например операционная система и производитель устройства.

2. Если требуется выполнить сортировку устройств в таблице, нажмите на заголовок соответствующей графы. Например, для сортировки устройств по типу нажмите на заголовок графы **Тип**.

3. Если требуется обновить список обнаруженных устройств, нажмите на кнопку **Обновить** в верхней части страницы.

4. Если требуется отфильтровать список выводимых устройств по типу устройства, нажмите на кнопку с названием типа устройства в блоке **Тип** над таблицей.

Устройства выбранного типа больше не будут отображаться в таблице **Устройства**, а кнопка с типом устройства отобразится без подсветки. Если требуется включить отображение устройств, нажмите еще раз на кнопку с названием этого типа устройства (кнопка снова будет подсвечена синим цветом).

5. Если требуется отображать только устройства, находящиеся в списке разрешенных, переведите переключатель **Список разрешенных** в положение включено.

Добавление и удаление устройств из списка разрешенных устройств

Kaspersky IoT Secure Gateway разделяет обнаруженные устройства на авторизованные и неавторизованные. Каждое новое устройство, обнаруженное системой в сети, считается неавторизованным. Чтобы сделать устройство авторизованным, нужно добавить его в список разрешенных устройств.

В разделе **Устройства** вы можете добавлять устройства в список разрешенных или удалять устройства из этого списка.

Чтобы добавить или удалить устройство из списка разрешенных:

1. В разделе **Устройства** установите флажок около имени устройства, которое вы хотите добавить или удалить из списка разрешенных.
2. В открывшейся справа панели выполните одно из следующих действий:
 - Если требуется добавить устройство в список разрешенных, нажмите на кнопку **Добавить в список разрешенных**.
Панель со значком устройства закроется. Устройство появится в списке разрешенных, статус устройства изменится на *Авторизованный*.
 - Если требуется удалить устройство из списка разрешенных, нажмите на кнопку **Удалить из списка разрешенных**.
Панель справа закроется. Устройство исчезнет из списка разрешенных, статус устройства изменится на *Неавторизованный*.

Мониторинг событий Kaspersky IoT Secure Gateway

Этот раздел содержит инструкции по мониторингу событий, зарегистрированных в Kaspersky IoT Secure Gateway.



О событиях Kaspersky IoT Secure Gateway


Событие – запись, содержащая информацию об обнаружении данных в системе или во внутренней сети, которые требуют внимания сотрудника, ответственного за информационную безопасность в вашей организации, и сохраняемая в памяти встраиваемого компьютера Advantech UTX-3117.

Kaspersky IoT Secure Gateway регистрирует следующие события, связанные с безопасностью сети:

- *Attack detected* – событие, регистрируемое при обнаружении или при обнаружении и блокировке атаки (в зависимости от параметров настройки IPS).
- *Unknown Device* – событие, регистрируемое при подключении в сети недоверенного устройства.
- *Device removed* – событие, регистрируемое при удалении устройства из сети.

События безопасности сети подразделяются по следующим уровням важности:

-  – *Информационные*. Информационные события содержат сведения справочного характера. Эти события обычно не требуют немедленной реакции.
-  – *Важные*. Важные события содержат сведения, на которые нужно обратить внимание. Эти события могут требовать реакции.

-  – *Критические*. Критические события содержат сведения, которые могут оказать критическое влияние на безопасность сети, в которой расположен Kaspersky IoT Secure Gateway. Эти события требуют немедленной реакции.

Kaspersky IoT Secure Gateway регистрирует следующие события, связанные с безопасностью Kaspersky IoT Secure Gateway:

- *All secure entities started and running*. Все компоненты Kaspersky IoT Secure Gateway запущены и работают в нормальном режиме.
- *Internal error*. Возникла внутренняя ошибка Kaspersky IoT Secure Gateway.
- *Partition reverted*. Компонент Kaspersky IoT Secure Gateway был восстановлен.
- *Update committed*. Выполнено обновление Kaspersky IoT Secure Gateway.
- *Update requested*. Запрошено обновление Kaspersky IoT Secure Gateway.
- *Unable to start device detector*. Не удалось запустить мониторинг устройств в сети.
- *Unable to restart device detector*. Повторно не удалось запустить мониторинг устройств в сети.
- *FW: Firewall config is changed*. Произошло изменение параметров межсетевого экрана.
- *Package verification problem*. Не удалось выполнить проверку пакета обновления Kaspersky IoT Secure Gateway.
- *An error occurred while unpacking or deploying package*. Произошла ошибка при распаковке или развертывании пакета обновления Kaspersky IoT Secure Gateway.
- *An error occurred while applying package*. Произошла ошибка при установке пакета обновления Kaspersky IoT Secure Gateway.
- *UBOOT: Update image authentication failed!* Произошла ошибка верификации образа Kaspersky IoT Secure Gateway.
- *UBOOT: Failed to cancel update!* Произошла ошибка при отмене обновления Kaspersky IoT Secure Gateway.
- *UBOOT: Image authentication failed, reverting!* Произошла ошибка верификации образа Kaspersky IoT Secure Gateway при откате обновления.
- *UBOOT: Failed to revert!* Произошла ошибка при откате обновления.
- *UBOOT: No update image found!* Не найден образ Kaspersky IoT Secure Gateway.
- *UBOOT: No image found, reverting!* Не найден образ Kaspersky IoT Secure Gateway и был выполнен откат к предыдущей версии.
- *UBOOT: Failed to set update flag while loading*. Не удалось установить флаг обновления при загрузке образа Kaspersky IoT Secure Gateway.

О журналах Kaspersky IoT Secure Gateway

Kaspersky IoT Secure Gateway ведет два типа журналов событий:

- *Журнал безопасности сети* сохраняет события, связанные с безопасностью сети, например обнаружение в сети новых устройств.
- *Журнал аудита* сохраняет события, связанные с безопасностью Kaspersky IoT Secure Gateway, например статус безопасности компонентов после загрузки программы.

Kaspersky IoT Secure Gateway позволяет [просматривать события, связанные с безопасностью сети](#) и [события аудита](#) через веб-интерфейс, а также [передавать их на сторонний сервер Syslog](#). При необходимости вы также можете настроить [отправку push-уведомлений](#) и [MQTT-уведомлений](#) о зарегистрированных событиях.

Обнаружение вторжений

Kaspersky IoT Secure Gateway позволяет обнаруживать вторжения из внешней сети во внутреннюю сеть организации, используя правила обнаружения вторжений.

Правило обнаружения вторжений описывает аномалию трафика, которая может быть признаком атаки из внешней сети. Правила содержат условия, по которым система обнаружения вторжений анализирует трафик. Правила обнаружения вторжений хранятся в Kaspersky IoT Secure Gateway.

Правила обнаружения вторжений поставляются "Лабораторией Касперского" и предназначены для обнаружения признаков наиболее часто встречающихся атак или подозрительной сетевой активности. Правила обнаружения вторжений доступны сразу после установки Kaspersky IoT Secure Gateway. Правила обнаружения вторжений обновляются вместе с обновлением Kaspersky IoT Secure Gateway.

В Kaspersky Security Center Web Console дополнительно вы можете управлять [системой предотвращения вторжений Kaspersky IoT Secure Gateway](#) (по умолчанию она включена). Система предотвращения вторжений позволяет добавлять IP-адреса устройств в список разрешенных IP-адресов. При включенной системе предотвращения вторжений Kaspersky IoT Secure Gateway на один час блокирует трафик от IP-адресов устройств, в трафике которых была обнаружена подозрительная активность, а также добавляет IP-адреса этих устройств в список запрещенных IP-адресов. Если система предотвращения вторжений включена, но при этом список запрещенных IP-адресов выключен, трафик не блокируется, то события безопасности будут записываться в журнал безопасности сети. Вы можете просмотреть список обнаруженных (обнаруженных и/или заблокированных) вторжений в [журнале безопасности сети](#).

Просмотр журнала безопасности сети

Kaspersky IoT Secure Gateway позволяет просматривать события безопасности сети, произошедшие в течение текущего сеанса подключения пользователя к системе через браузер.

Чтобы просмотреть события безопасности сети:

1. В меню в левой части страницы веб-интерфейса программы выберите раздел **События**.

Отобразится страница **События безопасности сети**, на которой представлена таблица записей журнала событий безопасности сети. Для каждой записи таблицы отображается следующая информация:

- **Компонент** – название архитектурного компонента Kaspersky IoT Secure Gateway, зарегистрировавшего событие, например *Traffic processor*.
- **Событие** – тип события.
- **Описание** – информация о зарегистрированном событии безопасности сети. Например, что обнаружено неизвестное устройство или обнаружена и заблокирована атака.

- **Дата и время** – дата и время, когда было зарегистрировано событие безопасности сети.
2. Если требуется выполнить сортировку событий в таблице, нажмите на заголовок соответствующей графы. Например, для сортировки по названию компонента, нажмите на графу **Компонент**.
 3. Если требуется включить режим автоматического обновления записей журнала событий на странице, установите переключатель **Автоматическое обновление** в положение включено.
Если **Автоматическое обновление** выключено, на странице отображаются только те события, которые находились в журнале на момент открытия раздела **События безопасности сети**. По умолчанию **Автоматическое обновление** выключено.
 4. Если требуется отфильтровать список событий, зарегистрированных определенным компонентом, нажмите на кнопку с названием компонента над таблицей.
События, зарегистрированные этим компонентом больше не будут отображаться в таблице **События безопасности сети**, а кнопка с названием компонента отобразится без подсветки. Если требуется включить отображение событий, нажмите еще раз на кнопку с названием нужного компонента (кнопка снова станет подсвечена синим цветом).


Просмотр журнала аудита

Kaspersky IoT Secure Gateway сохраняет в журнале аудита события, связанные с безопасностью системы.

При возникновении события с критическим уровнем важности, обратитесь к сотруднику, ответственному за информационную безопасность в вашей организации.

Экспорт журнала аудита на локальном компьютере приводит к удалению журнала аудита из системы.

Чтобы просмотреть журнал аудита:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Аудит**.
Откроется раздел **Аудит безопасности системы**, в котором отображается таблица с событиями безопасности системы. Для каждой записи журнала аудита отображается следующая информация:
 -  – уровень важности события.
 - **Описание** – подробная информация о зарегистрированном событии, например об изменении параметров межсетевого экрана.
 - **Компонент** – название архитектурного компонента Kaspersky IoT Secure Gateway, зарегистрировавшего событие.
 - **Дата и время** – дата и время, когда зарегистрировано событие.
2. Если требуется скрыть в таблице события с определенным уровнем важности, нажмите на значок уровня важности события над таблицей.
События с этим уровнем важности будут скрыты в таблице **Аудит безопасности системы**, а кнопка со значком уровня важности отобразится без подсветки. Если требуется вернуть в таблицу события, отображение которых было отключено, нажмите еще раз на кнопку со значком нужного уровня важности (кнопка снова станет подсвечена синим цветом).

3. Если требуется скрыть события, зарегистрированные определенным компонентом, нажмите на кнопку с названием компонента над таблицей.

События, зарегистрированные этим компонентом, будут скрыты в таблице **Аудит безопасности системы**, а кнопка с названием компонента отобразится без подсветки. Если требуется вернуть в таблицу события, отображение которых было отключено, нажмите еще раз на кнопку с названием нужного компонента (кнопка снова станет подсвечена синим цветом).

4. Если требуется выбрать период, за который отображаются события, в раскрывающемся списке **Период** выберите одно из следующих значений:

- **Все периоды.**
- **Последние 24 часа.**
- **Последняя неделя.**
- **Последний месяц.**

5. Если требуется выполнить сортировку событий в таблице, нажмите на заголовок соответствующей графы. Например, для сортировки событий по тексту описания, нажмите на заголовок графы **Описание**.

6. Если требуется включить режим автоматического обновления записей журнала событий на странице, установите переключатель **Автоматическое обновление** в положение включено.

Если **Автоматическое обновление** выключено, на странице отображаются только те события, которые находились в журнале аудита на момент открытия раздела **Аудит**. По умолчанию **Автоматическое обновление** выключено.

а. Если требуется просмотреть информацию о параметрах журнала аудита, в разделе **Аудит безопасности системы** наведите курсор мыши на значок ⓘ в верхней части окна.

Отобразится окно со следующей информацией:

- **Всего записей** – текущее количество записей в журнале аудита.
- **Максимально** – максимальное количество записей в журнале аудита.
- **Политика** – политика ведения записей в журнале аудита:
 - *Циклическая* – при переполнении журнала аудита новые записи будут перезаписывать старые.
 - *Ограниченная* – при переполнении журнала аудита система остановится.

Параметры журнала аудита настраивают специалисты "Лаборатории Касперского" на этапе сборки Kaspersky IoT Secure Gateway и их невозможно изменить через веб-интерфейс Kaspersky IoT Secure Gateway.

1. Если требуется сохранить журнал аудита на локальном компьютере, выполните следующие действия:

а. В разделе **Аудит безопасности системы** нажмите на кнопку **Сохранить в файл**.


Откроется окно, предупреждающее о том, что после сохранения файла журнал аудита будет удален из Kaspersky IoT Secure Gateway.

б. Подтвердите удаление журнала аудита из системы.

Откроется окно, позволяющее сохранить журнал аудита в файл.

с. В открывшемся окне укажите путь сохранения файла журнала аудита на локальном компьютере и сохраните файл.

По умолчанию файл аудита сохраняется с именем audit.csv.

d. Если требуется просмотреть информацию о параметрах журнала аудита, в разделе **Аудит безопасности системы** наведите курсор мыши на значок  в верхней части окна.

Отобразится окно со следующей информацией:

- **Всего записей** – текущее количество записей в журнале аудита.
- **Максимально** – максимальное количество записей в журнале аудита.
- **Политика** – политика ведения записей в журнале аудита:
 - *Циклическая* – при переполнении журнала аудита новые записи будут перезаписывать старые.
 - *Ограниченная* – при переполнении журнала аудита система остановится.

Параметры журнала аудита настраивают специалисты "Лаборатории Касперского" на этапе сборки Kaspersky IoT Secure Gateway и их невозможно изменить через веб-интерфейс Kaspersky IoT Secure Gateway.

Экспорт журнала аудита

Вы можете сохранить журнал аудита Kaspersky IoT Secure Gateway на локальном компьютере.

Чтобы сохранить журнал аудита на локальном компьютере:

1. В разделе **Аудит безопасности системы** нажмите на кнопку **Сохранить в файл**.

Откроется окно, предупреждающее о том, что после сохранения файла журнал аудита будет удален из Kaspersky IoT Secure Gateway.

2. Подтвердите удаление журнала аудита из системы.

Откроется окно, позволяющее сохранить журнал аудита в файл.

3. В открывшемся окне укажите путь сохранения файла журнала аудита на локальном компьютере и сохраните файл.

Журнал аудита Kaspersky IoT Secure Gateway будет сохранен на локальном компьютере. По умолчанию он сохраняется с именем audit.csv.

Экспорт журналов событий Kaspersky IoT Secure Gateway

Вы можете экспортировать информацию о событиях Kaspersky IoT Secure Gateway в файл формата GZIP. Этот архив содержит файлы журналов, включающие события безопасности сети, события аудита, а также диагностическую информацию. Файлы можно использовать для анализа безопасности сети и аудита Kaspersky IoT Secure Gateway, а также для диагностики возможных проблем системы.

Чтобы сохранить журналы событий Kaspersky IoT Secure Gateway на локальном компьютере:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Общие** → **Информация о событиях**.

2. Нажмите на кнопку **Сохранить в файл** и сохраните архив на локальном компьютере.

Архив будет сохранен на локальном компьютере. По умолчанию имя архива – log_files.tar.gz.

Управление программой через Kaspersky Security Center Web Console

Kaspersky Security Center Web Console представляет собой программу (веб-приложение), предназначенную для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Web Console является компонентом Kaspersky Security Center, предоставляющим пользовательский интерфейс. Подробную информацию о Kaspersky Security Center Web Console см. в *онлайн-справке Kaspersky Security Center 13*.

С помощью Kaspersky Security Center Web Console вы можете выполнять следующие действия:

- контролировать состояние системы безопасности вашей организации;
- устанавливать программы "Лаборатории Касперского" на устройства вашей сети;
- управлять установленными программами;
- просматривать отчеты о состоянии системы безопасности.

О веб-плагине управления Kaspersky IoT Secure Gateway

Веб-плагин управления Kaspersky IoT Secure Gateway (далее также веб-плагин) обеспечивает взаимодействие Kaspersky IoT Secure Gateway и Kaspersky Security Center Web Console. Веб-плагин позволяет [управлять Kaspersky IoT Secure Gateway с помощью политик](#).

Веб-плагин позволяет централизованно через Kaspersky Security Center Web Console выполнять следующие действия:

- [Настраивать параметры Kaspersky IoT Secure Gateway](#).
- [Получать события из Kaspersky IoT Secure Gateway](#).
- [Управлять межсетевым экраном](#).
- [Управлять системой предотвращения вторжений](#).
- [Управлять безопасностью Kaspersky IoT Secure Gateway](#).
- [Перезагружать и обновлять Kaspersky IoT Secure Gateway](#).

Установка веб-плагины управления Kaspersky IoT Secure Gateway

Веб-плагин управления Kaspersky IoT Secure Gateway по умолчанию не установлен в Kaspersky Security Center Web Console. Веб-плагин управления Kaspersky IoT Secure Gateway входит в [комплект поставки Kaspersky IoT Secure Gateway](#). Веб-плагин требуется установить на компьютер с установленной программой Kaspersky Security Center Web Console. При этом функции веб-плагины доступны всем администраторам, у которых есть доступ к Kaspersky Security Center Web Console в браузере. Вы можете просмотреть список установленных веб-плагинов в интерфейсе Kaspersky Security Center Web Console (**Параметры Консоли** → **Веб-плагины**).

На Сервере администрирования, на котором установлен Kaspersky Security Center, должен быть доступен порт 13294. Порт 13294 требуется для подключения устройств с защитой на уровне UEFI. Подробнее об управлении устройств с защитой на уровне UEFI см. в разделе *Устройства с защитой на уровне UEFI* в онлайн-справке Kaspersky Security Center 13. Подробнее о портах для подключения к Kaspersky Security Center см. в разделе *Порты, используемые Kaspersky Security Center* в онлайн-справке Kaspersky Security Center 13.

Kaspersky Security Center 13 не поставляется в [комплекте поставки Kaspersky IoT Secure Gateway](#).

Чтобы установить веб-плагин управления Kaspersky IoT Secure Gateway в Kaspersky Security Center Web Console:

1. В меню Kaspersky Security Center Web Console выберите **Параметры Консоли** → **Веб-плагины**.
Отобразится список доступных плагинов управления Kaspersky Security Center Web Console.
2. Нажмите на кнопку **Добавить из файла**.
3. В открывшейся справа панели добавьте следующие файлы:
 - ZIP-архив с дистрибутивом веб-плагина, полученный в комплекте поставки Kaspersky IoT Secure Gateway, нажав на кнопку **Загрузить файл формата ZIP**;
 - файл подписи, полученный в комплекте поставки Kaspersky IoT Secure Gateway, нажав на кнопку **Загрузить подпись**.
4. Нажмите на кнопку **Добавить**.
5. После завершения установки веб-плагина нажмите на кнопку **ОК**.

Веб-плагин управления Kaspersky IoT Secure Gateway будет загружен в конфигурации по умолчанию и появится в списке плагинов управления Kaspersky Security Center Web Console.

Обновление веб-плагина управления Kaspersky IoT Secure Gateway

Вы можете обновить веб-плагин управления Kaspersky IoT Secure Gateway в Kaspersky Security Center Web Console.

Чтобы обновить веб-плагин управления Kaspersky IoT Secure Gateway в Kaspersky Security Center Web Console:

1. В меню Kaspersky Security Center Web Console выберите **Параметры Консоли** → **Веб-плагины**.
Отобразится список доступных плагинов управления Kaspersky Security Center Web Console.
2. В списке плагинов управления установите флажок около веб-плагина управления Kaspersky IoT Secure Gateway.
3. Нажмите на кнопку **Обновить из файла**.
4. В открывшейся справа панели добавьте следующие файлы:

- ZIP-архив с дистрибутивом веб-плагина, полученный в комплекте поставки Kaspersky IoT Secure Gateway, нажав на кнопку **Загрузить файл формата ZIP**;
- файл подписи, полученный в комплекте поставки Kaspersky IoT Secure Gateway, нажав на кнопку **Загрузить подпись**.

5. Нажмите на кнопку **Обновление**.

6. После завершения обновления нажмите на кнопку **ОК**.

Веб-плагин управления Kaspersky IoT Secure Gateway будет обновлен, и в таблице плагинов управления Kaspersky Security Center Web Console отобразится информация о его версии и времени обновления.

Удаление веб-плагина управления Kaspersky IoT Secure Gateway

Вы можете удалить веб-плагин управления Kaspersky IoT Secure Gateway в Kaspersky Security Center Web Console. После удаления веб-плагина, управление Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console будет недоступно.

Чтобы удалить веб-плагин управления Kaspersky IoT Secure Gateway из Kaspersky Security Center Web Console:

1. В меню веб-интерфейса Kaspersky Security Center Web Console выберите **Параметры Консоли** → **Веб-плагины**.

Отобразится список доступных плагинов управления Kaspersky Security Center Web Console.

2. В списке плагинов управления установите флажок около веб-плагина управления Kaspersky IoT Secure Gateway.

3. Нажмите на кнопку **Удалить**.

4. В открывшемся окне подтверждения удаления плагина, выполните одно из следующих действий:

- Если требуется сохранить резервную копию плагина, нажмите на кнопку **ОК**.

Резервная копия плагина будет создана. Веб-плагин управления Kaspersky IoT Secure Gateway будет удален из Kaspersky Security Center Web Console.

- Если не требуется сохранять резервную копию плагина, нажмите на кнопку **Пропустить резервное копирование данных**.

Веб-плагин управления Kaspersky IoT Secure Gateway будет удален из Kaspersky Security Center Web Console.

5. В появившемся окне с информацией об удалении плагина нажмите на кнопку **ОК**.

Вход и выход из Kaspersky Security Center Web Console

Для входа в Kaspersky Security Center Web Console, требуется получить у администратора веб-адрес Сервера администрирования Kaspersky Security Center и номер порта, указанные во время установки (по умолчанию используется порт 8080). Также требуется включить JavaScript в браузере.

Чтобы войти в Kaspersky Security Center Web Console:

1. В браузере перейдите по адресу `https://<адрес>:<порт>`.

Требования к браузеру, который используется для работы с Kaspersky Security Center Web Console см. в разделе *Аппаратные и программные требования* в онлайн-справке Kaspersky Security Center.

Откроется страница входа.

2. Войдите с использованием имени пользователя и пароля локального администратора.

Если Сервер администрирования Kaspersky Security Center не отвечает или вы указали неверные учетные данные, отобразится сообщение об ошибке.

После входа отобразится информационная панель с последним используемым языком и темой.

Если вы вошли в Kaspersky Security Center Web Console впервые, в нижней части экрана отобразится учебник. Вы можете следовать инструкциям учебника или закрыть его.

Вход в Kaspersky Security Center Web Console выполнен и вы можете работать с Kaspersky Security Center Web Console. Дополнительная информация о работе Kaspersky Security Center Web Console приведена в онлайн-справке Kaspersky Security Center.

Чтобы выйти из Kaspersky Security Center Web Console:

1. В меню Kaspersky Security Center Web Console нажмите на имя пользователя.

2. В открывшемся меню выберите пункт **Выход**.

Kaspersky Security Center Web Console закроется и отобразится страница входа.

Добавление устройства Kaspersky IoT Secure Gateway в группу управляемых устройств Kaspersky Security Center Web Console

Для управления устройством, на котором установлен Kaspersky IoT Secure Gateway, через Kaspersky Security Center Web Console, нужно перенести это устройство в группу управляемых устройств и [создать политику](#) для этого устройства.

Чтобы добавить устройство в группу управляемых устройств Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.

Отобразится список всех обнаруженных нераспределенных устройств.

2. Установите флажок рядом с именем устройства, которое вы хотите добавить в группу управляемых устройств.

3. Нажмите на кнопку **Переместить в группу**.

Справа появится панель **Переместить в группу**.

4. Установите флажок рядом с группой администрирования **Управляемые устройства**.

5. Нажмите на кнопку **Переместить**.

Устройство будет перемещено в группу управляемых устройств.

Управление политиками

Политика – это набор параметров работы программы, определенный для группы администрирования. Для одной программы можно настроить несколько политик с различными значениями. Для разных групп администрирования параметры работы программы могут быть различными. В каждой группе администрирования может быть создана собственная политика для программы. Более подробную информацию о концепции управления программой с помощью политик Kaspersky Security Center вы можете прочитать в *онлайн-справке Kaspersky Security Center*.

В текущей версии Kaspersky IoT Secure Gateway 2.1 не поддерживается управление группой устройств с помощью политик Kaspersky Security Center. Вы можете управлять каждым устройством отдельно.

Чтобы создать политику для получения событий из Kaspersky IoT Secure Gateway:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Политики и профили политик**.

Откроется окно, в котором отображается список политик Kaspersky Security Center Web Console.

2. Выберите **Устройства** → **Политики и профили политик**.

3. Нажмите на кнопку **Добавить**.

Откроется окно **Новая политика**, в котором отображается список доступных для создания политики программ.

4. В списке программ выберите Kaspersky IoT Secure Gateway и нажмите на кнопку **Далее**.

5. В окне настройки новой политики на закладке **Общие** укажите следующие параметры:

- В поле **Имя** введите имя политики. По умолчанию в поле отображается имя программы – Kaspersky IoT Secure Gateway.
- В блоке **Состояние политики** выберите один из статусов: *Активна, Неактивна, Для автономных пользователей*.
- Если требуется настроить наследование параметров политики, настройте следующие параметры в блоке **Наследование параметров**:
 - Включите или выключите параметр **Наследовать параметры родительской политики**.
 - Включите или выключите параметр **Обеспечить принудительное наследование параметров для дочерних политик**.

6. Нажмите на кнопку **Сохранить** в нижней части страницы.

Политика будет создана и появится в списке политик Kaspersky Security Center Web Console.

Настройка параметров Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console

Этот раздел содержит информацию о настройке параметров Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console.

Настройка параметров сети через Kaspersky Security Center Web Console

Система Kaspersky IoT Secure Gateway поставляется со статически настроенным IP-адресом. Для работы системы в качестве безопасного шлюза Интернета вещей, требуется выполнить настройку параметров внешней и внутренней сетей. Также вы можете [настроить параметры сети с помощью веб-интерфейса Kaspersky IoT Secure Gateway](#).

Чтобы настроить параметры сети через Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **Сеть** → **Внутренняя сеть** и настройте следующие параметры:
 - a. В поле **IP-адрес** введите IP-адрес устройства Kaspersky IoT Secure Gateway во внутренней сети.
 - b. В поле **Маска подсети** введите маску подсети.
 - c. Если требуется, чтобы Kaspersky IoT Secure Gateway выступал в качестве DHCP-сервера, переведите переключатель в положение **Использовать DHCP-сервер** и укажите следующие параметры:
 - В поле **Начало диапазона IP-адресов** введите IP-адрес начала диапазона.
 - В поле **Конец диапазона IP-адресов** введите IP-адрес окончания диапазона.
 - В поле **Основной DNS-сервер** введите IP-адрес основного DNS-сервера.
 - В поле **Дополнительный DNS-сервер** введите IP-адрес дополнительного DNS-сервера.

В поле **MAC-адрес** отображается MAC-адрес системы во внутренней сети.
7. Нажмите на кнопку **Сохранить**.
8. В разделе **Сеть** выберите закладку **Внешняя сеть** и настройте следующие параметры:
 - Если вы хотите настроить параметры внешней сети автоматически по протоколу DHCP, переведите переключатель в положение **Использовать DHCP-клиент**.

Если при включении автоматического получения параметров внешней сети DHCP-сервер выдал Kaspersky IoT Secure Gateway нулевые адреса DNS-серверов, то по умолчанию для преобразования доменного имени в IP-адрес будет использоваться IP-адрес – 208.67.222.222 (сервер OpenDNS).

- Если вы хотите настроить параметры внешней сети вручную, переведите переключатель в положение **Не использовать DHCP-клиент** и выполните следующие действия:
 - В поле **IP-адрес** введите IP-адрес, который вы хотите назначить системе во внешней сети.
 - В поле **Маска подсети** введите маску подсети.
 - В поле **Сетевой шлюз** введите IP-адрес сетевого шлюза.
 - В поле **Основной DNS-сервер** введите IP-адрес основного DNS-сервера.
 - В поле **Дополнительный DNS-сервер** введите IP-адрес дополнительного DNS-сервера.

В поле **MAC-адрес** отображается MAC-адрес системы во внешней сети.

9. Нажмите на кнопку **Сохранить**.

10. [Перезагрузите Kaspersky IoT Secure Gateway](#), чтобы изменения параметров сети вступили в силу.

Настройка параметров сотового соединения Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console

Вы можете просматривать и настраивать параметры сотового соединения Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console.

Если в устройстве отсутствует модем, использование сотового соединения в Kaspersky IoT Secure Gateway и настройка параметров такого соединения Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console недоступны.

Чтобы просмотреть параметры сотового соединения Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.

6. Выберите раздел **Сеть** → **Модем**.

Отобразится окно, в котором указана следующая информация о сотовом соединении Kaspersky IoT Secure Gateway:

- Блок **Параметры модема**, в котором указана информация о статусе работы модема и текущем уровне сигнала.
- Блок **Адреса DNS-серверов модема**, в котором указана информация об IP-адресах основного и дополнительного DNS-серверов модема.
- Таблица **Профили модема**, в которой отображается информация о [доступных профилях модема](#).

В Kaspersky IoT Secure Gateway предусмотрено два типа профилей модема:

- *Предустановленный профиль* – профиль, поставляемый вместе с устройством. Предустановленный профиль доступен только для чтения.
- *Пользовательский профиль* – профиль, созданный при настройке сотового соединения. Пользовательский профиль доступен для изменения и удаления.

Разные профили модема позволяют работать с разными операторами сотовой связи. Для использования сотового соединения требуется, чтобы один из профилей модема был активным. По умолчанию активным является предустановленный профиль модема.

При отсутствии подключения через сотовую связь требуется проверить выполнение следующих условий:

- используемая в модеме SIM-карта является исправной, и подключен тариф, поддерживающий интернет-соединение через модем;
- выбранный профиль модема соответствует используемой SIM-карте;
- модем доступен для использования (отображается зеленый значок в блоке **Параметры модема**).

Если модем недоступен для использования (отображается серый или красный значок в блоке **Параметры модема**) требуется выполнить [перезагрузку Kaspersky IoT Secure Gateway](#) и снова проверить доступность модема для использования. Устройствам, которые выходят в интернет через Kaspersky IoT Secure Gateway, необходимо получать параметры внутренней сети через DHCP-сервер Kaspersky IoT Secure Gateway. Нужные адреса DNS-серверов от операторов сотовой сети будут получены вместе с этими параметрами.

Включение и выключение сотового соединения Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console

Kaspersky IoT Secure Gateway обрабатывает исходящий и входящий сетевой трафик с использованием сотового соединения (через оператора сотовой связи). Вы можете включить или выключить использование сотового соединения Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console. По умолчанию использование сотового соединения выключено.

Чтобы включить или выключить использование сотового соединения Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.

2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).

Откроется окно свойств компьютера.

3. Выберите закладку **Программы**.

4. Нажмите на название Kaspersky IoT Secure Gateway.

Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.

5. Выберите закладку **Параметры программы**.

6. Выберите раздел **Сеть** → **Модем**.

7. В блоке **Параметры модема** переведите переключатель в положение **Использовать модем как основной канал связи**, чтобы включить использование сотового соединения, или в положение **Не использовать модем как основной канал связи**, чтобы выключить использование сотового соединения.

Сотовое соединение Kaspersky IoT Secure Gateway будет включено или выключено.

Создание профиля модема Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console

Вы можете создавать новые профили модема Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console. Разные профили модема позволяют работать с разными операторами сотовой связи.

Чтобы создать новый профиль модема Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.

2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).

Откроется окно свойств компьютера.

3. Выберите закладку **Программы**.

4. Нажмите на название Kaspersky IoT Secure Gateway.

Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.


5. Выберите закладку **Параметры программы**.

6. Выберите раздел **Сеть** → **Модем**.

7. В таблице **Профили модема** нажмите на кнопку **Добавить**.

Справа откроется панель добавления профиля модема.

8. В раскрывающемся списке **Статус** выберите статус активности профиля. Для выбора доступны следующие значения:

- **Активный**. Выбранный профиль модема будет использоваться как основной для работы сотового соединения Kaspersky IoT Secure Gateway. В таблице **Профили** в графе **Активный** рядом с активным профилем появится значок .

- **Неактивный.**

9. В поле **Имя профиля** введите имя профиля.

10. В поле **Конфигурационный файл** введите параметры настройки профиля модема.

11. Нажмите на кнопку **ОК** в нижней части панели.

Панель добавления профиля модема закроется. Новый профиль отобразится в таблице **Профили модема**.

12. Нажмите на кнопку **Сохранить** в нижней части окна настройки параметров модема, чтобы сохранить изменения.

Изменение профиля модема Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console

Вы можете изменять параметры профиля модема Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console.

Чтобы изменить параметры профиля модема Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.

2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).

Откроется окно свойств компьютера.

3. Выберите закладку **Программы**.

4. Нажмите на название Kaspersky IoT Secure Gateway.

Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.


5. Выберите закладку **Параметры программы**.

6. Выберите раздел **Сеть** → **Модем**.

7. В таблице **Профили модема** установите флажок около того профиля модема, который требуется изменить и нажмите на кнопку **Изменить** в верхней части таблицы.

8. В открывшейся справа панели изменения профиля модема выполните следующие действия:

a. Если требуется изменить статус активности профиля, в раскрывающемся списке **Статус** выберите одно из следующих значений:

- **Активный.** После сохранения изменений, выбранный профиль модема будет использоваться как основной для работы сотового соединения Kaspersky IoT Secure Gateway. В таблице **Профили** в графе **Активный** рядом с активным профилем появится значок .

- **Неактивный.**

При изменении статуса профиля модема на **Активный** потребуется [перезагрузить](#) Kaspersky IoT Secure Gateway, чтобы изменения вступили в силу.

b. Если требуется, в поле **Имя профиля** введите новое имя профиля.

c. Если требуется, в поле **Конфигурационный файл** введите новые параметры настройки профиля модема или измените текущие.

d. Нажмите на кнопку **ОК** в нижней части панели.

Панель изменения профиля модема закроется. Измененный профиль отобразится в таблице **Профили модема**.

9. Нажмите на кнопку **Сохранить** в нижней части окна настройки параметров модема, чтобы сохранить изменения.

Удаление профиля модема Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console

Вы можете удалить профиль модема через Kaspersky Security Center Web Console.

Kaspersky IoT Secure Gateway не позволяет удалить активный и предустановленный профили модема. Если требуется удалить профиль, который сейчас является активным, сначала нужно [выбрать активным другой профиль модема](#).

Чтобы удалить профиль Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **Сеть** → **Модем**.
7. В таблице **Профили модема** установите флажок около того профиля модема, который требуется удалить и нажмите на кнопку **Удалить**.
Выбранный профиль модема оператора будет удален из таблицы **Профили модема**.
8. Нажмите на кнопку **Сохранить** в нижней части окна настройки параметров модема, чтобы сохранить изменения.

Выбранный профиль модема будет удален.

Управление сертификатами через Kaspersky Security Center Web Console

Вы можете просматривать загруженные ранее [сертификаты](#), добавлять новые или удалять сертификаты в Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console.

Не рекомендуется загружать широко известные сертификаты удостоверяющего центра, так как доверенными будут являться все серверы, использующие сертификаты, подписанные этими сертификатами удостоверяющего центра. Такая ситуация приведет к компрометации Kaspersky IoT Secure Gateway.

Чтобы добавить или удалить сертификаты в Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **Параметры** → **Сертификаты**.
Отобразится окно, в котором указана следующая информация о сертификатах:
 - В области **Сертификат администратора** указаны данные о текущем сертификате администратора.
 - В области **Сертификат сервера Kaspersky Security Center** указаны данные о текущем сертификате сервера Kaspersky Security Center.
7. Если требуется добавить новый сертификат администратора, в блоке **Сертификат администратора** нажмите на кнопку **Загрузить** и в открывшемся окне выберите файл сертификата.
Для добавления в качестве сертификата доступны файлы только в формате CRT, PEM, DER и CER.
Новый сертификат администратора будет загружен в систему, загруженный ранее сертификат будет удален.

Kaspersky IoT Secure Gateway не позволяет удалить сертификат администратора.

8. Если требуется добавить или удалить ранее загруженный сертификат сервера Kaspersky Security Center, в блоке **Сертификат сервера Kaspersky Security Center** выполните одно из следующих действий:

- Если требуется загрузить сертификат сервера Kaspersky Security Center, нажмите на кнопку **Загрузить** и в открывшемся окне выберите файл сертификата.

Для добавления в качестве сертификата доступны файлы только в формате CRT, PEM, DER и CER.

Новый сертификат сервера Kaspersky Security Center будет загружен в систему, загруженный ранее сертификат будет удален.

- Если требуется удалить сертификат сервера Kaspersky Security Center, нажмите на кнопку **Удалить** и подтвердите действие удаления.

Сертификат сервера Kaspersky Security Center будет удален.



При удалении сертификата сервера Kaspersky Security Center соединение Kaspersky IoT Secure Gateway с сервером Kaspersky Security Center будет разорвано. Вы не сможете управлять Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console.

9. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Просмотр списка профилей веб-сервера через Kaspersky Security Center Web Console

Работу веб-интерфейса Kaspersky IoT Secure Gateway обеспечивает веб-сервер. Параметры веб-сервера хранятся в профиле веб-сервера. Через Kaspersky Security Center Web Console вы можете только просматривать существующие профили веб-сервера. [Управление профилями веб-сервера](#) доступно через веб-интерфейс Kaspersky IoT Secure Gateway.

Чтобы просмотреть список профилей веб-сервера:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **Параметры** → **Веб-сервер**.
Отобразится таблица профилей веб-сервера, в которой для каждого профиля веб-сервера отображается следующая информация:
 -  – доступ на изменение профиля веб-сервера. Значок, информирующий о том, что профиль доступен только для чтения, отображается только для предустановленного профиля.
 - **Активный** – значком  отмечен профиль веб-сервера, который используется в программе в текущий момент.

- **Имя** – имя профиля веб-сервера.
- **Изменен** – дата и время последнего изменения профиля.

Настройка параметров MQTT-брокера через Kaspersky Security Center Web Console

В Kaspersky Security Center Web Console вы можете создавать новые [профили MQTT-брокера](#), изменять существующие профили и переключаться между профилями.

Этот раздел содержит информацию о настройке параметров MQTT-брокера через Kaspersky Security Center Web Console.

Создание профиля MQTT-брокера через Kaspersky Security Center Web Console

Вы можете создавать новые профили MQTT-брокера через Kaspersky Security Center Web Console. Разные профили MQTT-брокера позволяют работать с разными серверами и цифровыми платформами, которые принимают события от Kaspersky IoT Secure Gateway по протоколу MQTT.

Чтобы создать новый профиль MQTT-брокера через Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **MQTT**.
Отобразится таблица профилей MQTT-брокера.
7. Нажмите на кнопку **Добавить** в верхней части таблицы профилей MQTT-брокера.
Откроется окно **Изменение профиля**.
8. В раскрывающемся списке **Статус** выберите одно из следующих значений:
 - **Активный**, если вы хотите сделать новый профиль активным. В этом случае параметры настройки профиля загружаются в MQTT-брокер и активируется доступ к сертификатам из профиля для MQTT-брокера.
 - **Неактивный**.

Активным может быть только один профиль.

9. В поле **Имя** введите имя профиля латинскими буквами.

10. Добавьте конфигурационный файл или сертификат к новому профилю, нажав на кнопку **Добавить** в верхней части таблицы **Список файлов**.

11. В открывшейся справа панели загрузки файлов выполните следующие действия:

а. В раскрывающемся списке **Тип** выберите тип файла, который вы хотите добавить:

- **Главный конфигурационный файл.** Содержит основные параметры для работы MQTT-брокера. Главный конфигурационный файл требуется добавить в профиль MQTT-брокера, чтобы этот профиль можно было активировать. Для выбора доступны файлы в формате CONF.
- **Конфигурационный файл.** Содержит дополнительные параметры для работы MQTT-брокера. Для выбора доступны файлы в формате CONF.
- **Сертификат.** Для выбора доступны файлы в формате CRT, CER, DER, PEM.
- **Прочее.** Содержит дополнительную информацию для работы MQTT-брокера. Для выбора доступны любые типы файлов.

б. Нажмите на кнопку **Загрузить файл** и в открывшемся окне загрузки файла выберите файл. Размер файла не должен превышать 131 КБ.

Файл загрузится в систему и отобразится в профиле MQTT-брокера.

с. Нажмите на кнопку **ОК** в нижней части панели.

Панель загрузки файлов закроется.

12. Нажмите на кнопку **ОК** в нижней части окна **Изменение профиля**.

Окно **Изменение профиля** закроется.

13. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить новый профиль MQTT-брокера.

Изменение профиля MQTT-брокера через Kaspersky Security Center Web Console

Вы можете изменять параметры профиля MQTT-брокера через Kaspersky Security Center Web Console.

Чтобы изменить профиль MQTT-брокера через Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.

2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).

Откроется окно свойств компьютера.

3. Выберите закладку **Программы**.

4. Нажмите на название Kaspersky IoT Secure Gateway.

Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.

5. Выберите закладку **Параметры программы**.

6. Выберите раздел **MQTT**.

Отобразится таблица профилей MQTT-брокера.

7. В таблице профилей MQTT-брокера выберите профиль, который вы хотите изменить и нажмите на кнопку **Изменить** в верхней части таблицы.

Откроется окно **Изменение профиля**.

8. В раскрывающемся списке **Статус** выберите **Активный**, если вы хотите сделать этот профиль активным. В этом случае параметры настройки профиля загружаются в MQTT-брокер и активируется доступ к сертификатам из профиля для брокера.

Активным может быть только один профиль.

9. Если требуется изменить имя профиля, в поле **Имя** введите имя профиля латинскими буквами.

Для профиля, поставляемого вместе с устройством (предустановленного профиля) поле **Имя** недоступно для изменения.

10. Если вы хотите добавить конфигурационный файл или сертификат к профилю, в верхней части таблицы **Список файлов** нажмите на кнопку **Добавить**.

Справа откроется панель загрузки файлов.

a. В раскрывающемся списке **Тип** выберите тип файла, который вы хотите добавить:

- **Главный конфигурационный файл.** Содержит основные параметры для работы MQTT-брокера. Главный конфигурационный файл требуется добавить в профиль MQTT-брокера, чтобы этот профиль можно было активировать. Для выбора доступны файлы в формате CONF.
- **Конфигурационный файл.** Содержит дополнительные параметры для работы MQTT-брокера. Для выбора доступны файлы в формате CONF.
- **Сертификат.** Для выбора доступны файлы в формате CRT, CER, DER, PEM.
- **Прочее.** Содержит дополнительную информацию для работы MQTT-брокера. Для выбора доступны любые типы файлов.

b. Нажмите на кнопку **Загрузить файл** и в открывшемся окне загрузки файла в систему выберите файл. Размер файла не должен превышать 131 КБ.

Файл загрузится в систему и появится в профиле.

c. Нажмите на кнопку **ОК** в нижней части панели.

Панель загрузки файлов закроется. Файл будет добавлен в профиль MQTT-брокера и отобразится в таблице **Список файлов**.

11. Если вы хотите изменить добавленный ранее конфигурационный файл или сертификат в профиле MQTT-брокера, выберите файл, который нужно изменить и нажмите на кнопку **Изменить** в верхней части таблицы **Список файлов**.

Справа откроется панель загрузки файлов.

Выполните подпункты а–с, описанные в пункте 10 этой инструкции.

12. Если вы хотите удалить добавленный ранее конфигурационный файл или сертификат в профиле MQTT-брокера, выберите файл, который нужно удалить и нажмите на кнопку **Удалить** в верхней части таблицы **Список файлов**.

Файл будет удален из профиля MQTT-брокера.

13. Нажмите на кнопку **ОК** в нижней части окна **Изменение профиля**.

Окно **Изменение профиля** закроется.

14. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Удаление профиля MQTT-брокера через Kaspersky Security Center Web Console

Вы можете удалять профили MQTT-брокера через Kaspersky Security Center Web Console.

Kaspersky IoT Secure Gateway не позволяет удалить активный и предустановленный профили MQTT-брокера. Если требуется удалить профиль, который сейчас является активным, сначала нужно [выбрать активным другой профиль MQTT-брокера](#).

Чтобы удалить профиль MQTT-брокера через Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **MQTT**.
7. В таблице профилей MQTT-брокера выберите профиль, который вы хотите удалить и нажмите на кнопку **Удалить** в верхней части таблицы.
8. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.
Выбранный профиль MQTT-брокера будет удален.

Настройка уведомлений через Kaspersky Security Center Web Console

Этот раздел содержит информацию о настройке уведомлений через Kaspersky Security Center Web Console при регистрации [событий](#) в системе.

Настройка отправки уведомлений на сервер Syslog через Kaspersky Security Center Web Console

Kaspersky IoT Secure Gateway включает в себя Syslog-клиент, с помощью которого вы можете отправлять уведомления о событиях безопасности и аудита на сервер Syslog. Вы можете настраивать отправку уведомлений на сервер Syslog через Kaspersky Security Center Web Console.

Чтобы настроить отправку уведомлений на сервер Syslog:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **Уведомления** → **Syslog**.
7. Установите переключатель в верхней части окна в положение **Использовать сервер Syslog** и укажите следующие параметры:
 - В поле **IP-адрес** укажите IP-адрес сервера Syslog.
 - В поле **Порт** укажите порт, по которому будет осуществляться подключение.
 - В раскрывающемся списке **Режим** выберите один из вариантов подключения:
 - UDP.
 - TCP.
 - TLS.
8. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Kaspersky IoT Secure Gateway будет отправлять уведомления о событиях безопасности и аудита на сервер Syslog.

Настройка отправки push-уведомлений через Kaspersky Security Center Web Console

Firebase Cloud Messaging (FCM) – это кроссплатформенное решение для обмена сообщениями, которое позволяет надежно отправлять сообщения бесплатно.

Kaspersky IoT Secure Gateway отправляет push-уведомления о событиях с помощью [Firebase Cloud Messaging](#) по протоколу HTTPS на адрес <https://fcm.googleapis.com/fcm/send> в виде JSON-сообщений. Система транслирует информацию о своем имени и предоставляемых топиках push-уведомлений каждые четыре секунды в топик /topics/DevicesandTopics, находящийся в облачной службе FCM. Вы можете настроить получение push-уведомлений через Kaspersky Security Center Web Console.

Чтобы включить отправку push-уведомлений через Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **Уведомления** → **Push-уведомления**.
7. В поле **Имя устройства** введите имя, под которым система будет отправлять push-уведомления.
8. В поле **Ключ авторизации** введите код авторизации для устройства, на которое будут приходить уведомления. Информацию о получении кода авторизации см. в [документации Firebase Cloud Messaging](#).
9. Если требуется добавить или удалить сертификат SSL-соединения для безопасной отправки уведомлений в приложение FCM, выполните одно из следующих действий:
 - Если требуется добавить сертификат, нажмите на кнопку **Загрузить сертификат** и в открывшемся окне загрузки файла в систему выберите файл сертификата.
Файл сертификата загрузится в систему и информация о нем появится в профиле.
 - Если требуется удалить сертификат, нажмите на кнопку **Удалить сертификат**.
Файл сертификата будет удален из системы.
10. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Kaspersky IoT Secure Gateway будет отправлять push-уведомления на авторизованные устройства.

Настройка отправки MQTT-уведомлений через Kaspersky Security Center Web Console

Kaspersky IoT Secure Gateway может отправлять уведомления о событиях безопасности и аудита по протоколу MQTT. Вы можете настроить отправку MQTT-уведомлений через Kaspersky Security Center Web Console.

Чтобы включить отправку MQTT-уведомлений через Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **Уведомления** → **MQTT-уведомления**.
7. Переведите переключатель в положение **MQTT-уведомления включены**.
8. В поле **Адрес сервера** введите IP-адрес используемого сервера MQTT.
9. В поле **Порт** введите номер порта, используемого для соединения с сервером MQTT.
Для соединения Kaspersky IoT Secure Gateway с сервером MQTT, который находится во внутренней сети вы можете использовать порты 1883 и 8883.
Для соединения Kaspersky IoT Secure Gateway с сервером MQTT, который находится во внешней сети вы можете использовать порт 8883.
10. В поле **Имя MQTT-топика** укажите имя MQTT-топика для отправки уведомлений.
11. Если требуется отправлять уведомления о событиях аудита от имени определенного пользователя, переведите переключатель **Использовать аутентификацию** в положение включено и заполните поля **Имя пользователя** и **Пароль**. Учетные данные пользователя, от имени которого требуется отправлять уведомления, вы можете узнать у администратора используемого сервера MQTT.
По умолчанию отправка уведомлений от имени пользователя выключена.
12. Если требуется использовать защищенное SSL-соединение, установите переключатель **Использовать защищенное SSL-соединение** в положение включено и выполните следующие действия:
 - a. Загрузите сертификат удостоверяющего центра. Для этого нажмите на кнопку **Загрузить сертификат** и выберите файл сертификата на локальном устройстве.
Информация о загруженном сертификате удостоверяющего центра отобразится на странице.

Не рекомендуется загружать широко известные сертификаты удостоверяющего центра, так как доверенными будут являться все серверы, использующие сертификаты, подписанные этими сертификатами удостоверяющего центра. Такая ситуация приведет к компрометации Kaspersky IoT Secure Gateway.

b. Загрузите сертификат клиента. Для этого нажмите на кнопку **Загрузить сертификат клиента** и выберите файл сертификата на локальном устройстве.

Информация о загруженном сертификате клиента отобразится на странице.

c. Загрузите ключ к сертификату клиента. Для этого нажмите на кнопку **Загрузить ключ** и выберите файл ключа на локальном устройстве.

По умолчанию использование защищенного SSL-соединения выключено.

13. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Kaspersky IoT Secure Gateway будет отправлять уведомления о событиях безопасности и аудита по протоколу MQTT.

Настройка параметров синхронизации с Kaspersky Security Center

Вы можете настроить период синхронизации Kaspersky Security Center с Kaspersky IoT Secure Gateway, через который информация о зарегистрированных в Kaspersky IoT Secure Gateway событиях безопасности сети будет поступать в Kaspersky Security Center Web Console. События безопасности сети Kaspersky IoT Secure Gateway включают в себя обнаружение устройств в сети, а также попытки подключения к веб-интерфейсу Kaspersky IoT Secure Gateway.

Чтобы настроить время синхронизации с Kaspersky Security Center:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.

2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).

Откроется окно свойств компьютера.

3. Выберите закладку **Программы**.

4. Нажмите на название Kaspersky IoT Secure Gateway.

Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.

5. Выберите закладку **Параметры программы**.

6. Выберите раздел **Kaspersky Security Center** → **Синхронизация**.

7. В раскрывающемся списке **Период синхронизации** выберите одно из следующих значений:

- **30 секунд;**
- **1 минута;**
- **15 минут.**

8. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Настройка даты и времени через Kaspersky Security Center Web Console

Вы можете настроить дату и время Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console.

Чтобы настроить дату и время через Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **Параметры** → **Время**.
7. В блоке **Дата** укажите дату системы.
8. В блоке **Время** укажите время системы.

Указывайте текущее время в часовом поясе UTC.

9. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Управление событиями Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console

Этот раздел содержит инструкции по мониторингу событий, зарегистрированных в Kaspersky IoT Secure Gateway, через Kaspersky Security Center Web Console

Просмотр событий Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console

Вы можете просматривать [события, зарегистрированные Kaspersky IoT Secure Gateway](#), через Kaspersky Security Center Web Console.

Чтобы просмотреть события, зарегистрированные Kaspersky IoT Secure Gateway, через Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.

2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway.

Откроется окно свойств компьютера.

3. Выберите закладку **Программы**.

4. Нажмите на название Kaspersky IoT Secure Gateway.

Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.

5. Нажмите на закладку **События**.

Откроется окно, в котором отображается таблица событий, зарегистрированных на устройстве. Для каждой записи таблицы отображается следующая информация:

- **Время** – дата и время, когда было зарегистрировано событие.
- **Событие** – тип события.
- **Уровень критичности** – уровень критичности события (*Критическое, Отказ функционирования, Предупреждение* или *Информационное сообщение*).

Настройка регистрации событий Kaspersky IoT Secure Gateway в Kaspersky Security Center Web Console

Для [событий Kaspersky IoT Secure Gateway](#) вы можете дополнительно настроить регистрацию событий в Kaspersky Security Center Web Console, а также оповещение о регистрации таких событий. Каждое событие в Kaspersky Security Center имеет собственный уровень важности. В зависимости от условий возникновения, событию может быть присвоен один из следующих уровней важности:

- *Критическое событие* – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- *Отказ функционирования* – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы программы или выполнения процедуры.
- *Предупреждение* – событие, на которое нужно обратить внимание, поскольку оно отражает важные ситуации в работе Kaspersky IoT Secure Gateway и может указывать на возможную проблему в будущем. Чаще всего события относятся к Предупреждениям, если после их возникновения работа программы может быть восстановлена без потери данных или функциональных возможностей.
- *Информационное сообщение* – событие, информирующее об успешном выполнении операции, корректной работе программы или завершении процедуры.

Чтобы настроить регистрацию событий Kaspersky IoT Secure Gateway в Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.

2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway.

Откроется окно свойств компьютера.

3. Выберите закладку **Программы**.

4. Нажмите на название Kaspersky IoT Secure Gateway.

Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.

5. Нажмите на закладку **Настройка событий**.

6. Выберите уровень важности, для которого требуется настроить регистрацию событий:

- **Критическое.**
- **Отказ функционирования.**
- **Предупреждение.**
- **Информационное сообщение.**

Отобразится таблица событий для выбранного уровня важности.

7. Добавьте типы [событий Kaspersky IoT Secure Gateway](#), которые требуется регистрировать в Kaspersky Security Center Web Console для выбранного уровня важности, нажав на кнопку **Добавить события**.

8. Установите флажок около тех типов событий, которые вы хотите добавить, и нажмите на кнопку **ОК**.

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

Выбранные типы событий Kaspersky IoT Secure Gateway будут добавлены для выбранного уровня важности и будут регистрироваться и храниться на Сервере администрирования Kaspersky Security Center. По умолчанию срок хранения событий составляет 30 дней.

Подробную информацию о настройке оповещений при регистрации событий в Kaspersky Security Center Web Console см. в разделе онлайн-справки Kaspersky Security Center *13 Настройка параметров доставки уведомлений*.

Настройка маскардинга

Маскардинг (англ. Masquerading) – тип трансляции сетевого адреса, при котором адрес отправителя подставляется динамически, в зависимости от назначенного интерфейсу адреса. Вы можете использовать функцию маскардинга, если для устройств во внутренней сети требуется подмена параметров в заголовках IP-пакетов. Это позволит устройствам, расположенным во внутренней сети и не имеющим реальных IP-адресов, отправлять и получать IP-пакеты из внешней сети.

Чтобы включить функцию маскардинга через Kaspersky Security Center Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.

2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).

Откроется окно свойств компьютера.

3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **Параметры** → **NAT**.
7. Включите или выключите функцию маскардинга, установив переключатель в положение **Маскардинг включен** или **Маскардинг выключен**.

Вне зависимости от выбранного положения переключателя, маршрутизация транзитных IP-пакетов всегда остается включенной.

8. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Обновление и перезагрузка Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console

Вы можете обновить или перезагрузить Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console.

Чтобы обновить или перезагрузить Kaspersky IoT Secure Gateway, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **Kaspersky Security Center**.
7. Если требуется обновить Kaspersky IoT Secure Gateway, выберите закладку **Обновление** и выполните следующие действия:
 - a. В открывшемся окне в поле **Адрес обновления** укажите путь, по которому находится пакет обновлений для Kaspersky IoT Secure Gateway, в формате `http://<ip-адрес сервера>/путь_к_пакету_обновлений` (например, `http://10.10.100.10/update.pkg`).
 - b. Выберите закладку **Команды**.
 - c. В открывшемся окне в раскрывающемся списке **Команды** выберите **Обновление**.

d. Нажмите на кнопку **Сохранить** в нижней части страницы.

Обновления Kaspersky IoT Secure Gateway будут загружены.

8. Если требуется перезагрузить Kaspersky IoT Secure Gateway, выберите закладку **Команды** и выполните следующие действия:

a. В открывшемся окне в раскрывающемся списке **Команды** выберите **Перезагрузка**.

b. Нажмите на кнопку **Сохранить** в нижней части страницы.

Kaspersky IoT Secure Gateway будет перезагружен.

Управление системой предотвращения вторжений

Kaspersky IoT Secure Gateway может обнаруживать в трафике внешней и внутренней сети подозрительную сетевую активность с помощью системы предотвращения вторжений (компонент IPS). При анализе трафика применяются правила предотвращения вторжений.

Правило предотвращения вторжений описывает аномалию трафика, которая может быть признаком вторжения в защищаемую инфраструктуру предприятия. Правила содержат условия, по которым система предотвращения вторжений анализирует трафик и обнаруживает признаки наиболее часто встречающихся атак или подозрительной сетевой активности. Правила предотвращения вторжений поставляются "Лабораторией Касперского" и хранятся в Kaspersky IoT Secure Gateway. Они доступны сразу после установки Kaspersky IoT Secure Gateway.

В список разрешенных IP-адресов входят IP-адреса внутренней и внешней сети, сетевой трафик от которых Kaspersky IoT Secure Gateway не блокирует. Вы можете самостоятельно создавать списки разрешенных IP-адресов и добавлять в эти списки IP-адреса устройств, трафик от которых требуется разрешить. Сетевой трафик от IP-адресов новых устройств, появившихся в сети, разрешен и не блокируется системой.

В список запрещенных IP-адресов входят IP-адреса внутренней и внешней сети, сетевой трафик от которых блокируется Kaspersky IoT Secure Gateway. Вы можете удалять из этих списков IP-адреса устройств, которые были ранее добавлены Kaspersky IoT Secure Gateway в список запрещенных и трафик от которых требуется разрешить.

Если система предотвращения вторжений и список запрещенных IP-адресов включены, при обнаружении совпадения с правилом Kaspersky IoT Secure Gateway автоматически блокирует трафик с IP-адреса, в котором была обнаружена подозрительная сетевая активность.

Если система предотвращения вторжений и список запрещенных IP-адресов выключены, при обнаружении совпадения с правилом Kaspersky IoT Secure Gateway не блокирует трафик с IP-адреса, в котором была обнаружена подозрительная сетевая активность, а регистрирует событие безопасности и записывает его в [журнал безопасности сети](#).

Включение и выключение системы предотвращения вторжений

Вы можете включить или выключить систему предотвращения вторжений Kaspersky IoT Secure Gateway. По умолчанию система предотвращения вторжений выключена.

Чтобы включить или выключить систему предотвращения вторжений:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **Сеть** → **IPS** и установите переключатель в положение **Система предотвращения вторжений включена** или в положение **Система предотвращения вторжений выключена**. По умолчанию система предотвращения вторжений включена.
7. Нажмите на кнопку **Сохранить** в нижней части окна.

Добавление IP-адреса в список разрешенных IP-адресов

Вы можете добавлять IP-адреса устройств, сетевой трафик от которых требуется разрешить, в список разрешенных IP-адресов.

Чтобы добавить IP-адрес в список разрешенных IP-адресов:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **Сеть** → **IPS**.
7. Нажмите на кнопку **Показать список** напротив заголовка **Список разрешенных IP-адресов**.
Отобразится окно **Список разрешенных IP-адресов**.
8. Нажмите на кнопку **Добавить**.
9. В открывшейся справа панели в поле **IP-адрес (источник)** укажите IP-адрес, трафик от которого вы хотите разрешить.
10. Нажмите на кнопку **ОК**, а затем на кнопку **Сохранить** в нижней части страницы.

IP-адрес устройства будет добавлен в список разрешенных IP-адресов.

Удаление IP-адреса из списка разрешенных IP-адресов

Вы можете удалять IP-адреса устройств из списка разрешенных IP-адресов.

Чтобы удалить IP-адрес из списка разрешенных IP-адресов:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **Сеть** → **IPS**.
7. Нажмите на кнопку **Показать список** напротив заголовка **Список разрешенных IP-адресов**.
Отобразится окно **Список разрешенных IP-адресов**.
8. Выберите IP-адрес устройства, который требуется удалить из списка разрешенных IP-адресов, и нажмите на кнопку **Удалить** в верхней части таблицы.
9. Нажмите на кнопку **ОК**, а затем на кнопку **Сохранить** в нижней части страницы.

Выбранный IP-адрес будет удален из списка разрешенных IP-адресов.

Включение и выключение списка запрещенных IP-адресов

В Kaspersky Security Center Web Console вы можете включить или выключить список запрещенных IP-адресов, если требуется блокировать сетевой трафик, поступающий от этих IP-адресов.

Если список запрещенных IP-адресов выключен Kaspersky IoT Secure Gateway определяет IP-адреса, от которых поступает подозрительная сетевая активность, но не блокирует их.

Чтобы включить список запрещенных IP-адресов:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.

3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **Сеть** → **IPS**.
7. Нажмите на кнопку **Показать список** напротив заголовка **Список запрещенных IP-адресов**.
Отобразится окно **Список запрещенных IP-адресов**.
8. Установите переключатель в положение **Применять список запрещенных IP-адресов** или в положение **Не применять список запрещенных IP-адресов**.
9. Нажмите на кнопку **ОК**, а затем на кнопку **Сохранить** в нижней части страницы.

Управление межсетевым экраном

Вы можете использовать встроенный в Kaspersky IoT Secure Gateway межсетевой экран, чтобы контролировать и фильтровать проходящий через устройство трафик. [Обработка сетевого трафика](#) определяется [правилами межсетевого экрана](#), которые задаются через Kaspersky Security Center Web Console. Трафик, прохождение которого не разрешено правилами межсетевого экрана, запрещен.

О правилах межсетевого экрана

Правила межсетевого экрана разделяются на *служебные правила межсетевого экрана* и *пользовательские правила межсетевого экрана*.

Служебные правила межсетевого экрана используются, чтобы обеспечить полноценную работу Kaspersky IoT Secure Gateway. Вы не можете изменять эти правила, и они не отображаются в веб-плагине Kaspersky IoT Secure Gateway.

При необходимости вы можете [создавать](#) дополнительные правила. Такие правила называются пользовательскими правилами межсетевого экрана. Вы также можете [изменять](#) или [удалять](#) правила этого типа. Пользовательские правила межсетевого экрана выполняются в заданном в Kaspersky Security Center Web Console порядке сверху вниз. Вы можете создать до 1000 пользовательских правил межсетевого экрана.

Kaspersky IoT Secure Gateway поддерживает правила для протоколов TCP и UDP (только IPv4).

Для этих протоколов включена инспекция пакетов с хранением состояния (англ. Stateful Packet Inspection).

Служебные правила разрешают следующие соединения Kaspersky IoT Secure Gateway:

- исходящие соединения с Kaspersky Security Center Web Console по протоколу TCP;
- исходящие соединения с сервером обновлений по протоколам TCP, UDP, TCP / TLS;
- входящие соединения с локальным веб-сервером по протоколу HTTPS;

- исходящие соединения с сервером Syslog по протоколам TCP, UDP;
- исходящие и входящие соединения с источниками MQTT-данных по протоколу TCP;
- исходящие и входящие соединения с внешними и внутренними серверами DNS по протоколу UDP.

Порядок обработки сетевого трафика

Kaspersky IoT Secure Gateway обрабатывает сетевой трафик в соответствии с [правилам межсетевого экрана](#) и списками разрешенных и запрещенных, которые задаются [системой предотвращения вторжений](#).

Kaspersky IoT Secure Gateway при обработке сетевого трафика применяет правила в следующем порядке:

1. Разрешающие служебные правила межсетевого экрана.
2. Список разрешенных IP-адресов.
3. Список запрещенных IP-адресов.
4. Пользовательские правила межсетевого экрана.
5. Запрещающие служебные правила межсетевого экрана.

Создание правил межсетевого экрана

Вы можете создавать правила межсетевого экрана через Kaspersky Security Center Web Console.

Пользовательские правила межсетевого экрана выполняются в заданном в Kaspersky Security Center Web Console порядке сверху вниз, до первого совпадения.

Чтобы создать новое правило межсетевого экрана:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **Сеть** → **Межсетевой экран**.
Отобразится таблица, содержащая пользовательские правила для межсетевого экрана.

7. Нажмите на кнопку **Добавить** в верхней части таблицы правил межсетевого экрана.
Справа появится панель добавления правила межсетевого экрана.
8. В раскрывающемся списке **Статус правила** выберите статус правила: **Включено** или **Выключено**.
9. В раскрывающемся списке **Действие** выберите действие, применяемое к проходящему через межсетевой экран трафику: **Разрешить** или **Запретить**.
10. В раскрывающемся списке **Область** выберите область, к которой должно применяться правило: **Внутренняя сеть** или **Внешняя сеть**.
11. В поле **IP-адрес (источник)** укажите IP-адрес источника трафика.
12. В поле **Порт (источник)** укажите порт источника трафика, если этот параметр применим к протоколу.
13. В поле **IP-адрес (получатель)** укажите IP-адрес получателя трафика.
14. В поле **Порт (получатель)** укажите порт получателя трафика, если этот параметр применим к протоколу.
15. В раскрывающемся списке **Протокол** выберите используемый протокол. Для выбора доступны следующие протоколы:
 - TCP (IPv4).
 - UDP (IPv4).
 - Любой.
16. Нажмите на кнопку **ОК** в панели добавления правила межсетевого экрана.
Панель закроется, новое правило отобразится в таблице правил для межсетевого экрана.
17. Если требуется изменить порядок выполнения правила в таблице правил, установите флажок около правила и с помощью кнопок **Вверх** или **Вниз** повысьте или понизьте приоритет обработки правила.
18. Нажмите на кнопку **Сохранить**.

Изменение правил межсетевого экрана

Вы можете изменять правила межсетевого экрана через Kaspersky Security Center Web Console.

Чтобы изменить правило межсетевого экрана:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.

Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.

5. Выберите закладку **Параметры программы**.

6. Выберите раздел **Сеть** → **Межсетевой экран**.

Отобразится таблица, содержащая пользовательские правила для межсетевого экрана.

7. Установите флажок напротив правила, которое вы хотите изменить.

8. Нажмите на кнопку **Изменить** в верхней части таблицы правил межсетевого экрана.

Справа появится панель изменения правила межсетевого экрана.

9. Если требуется изменить статус правила, в раскрывающемся списке **Статус** выберите статус правила: **Включено** или **Выключено**.

10. Если требуется изменить разрешение прохождения трафика, в раскрывающемся списке **Действие** выберите одно из возможных действий, применяемых к проходящему через межсетевой экран трафику: **Разрешить** или **Запретить**.

11. Если требуется изменить направление трафика, в раскрывающемся списке **Область** выберите область, к которой должно применяться правило: **Внутренняя сеть** или **Внешняя сеть**.

12. При необходимости измените IP-адрес источника трафика в поле **IP-адрес (источник)**.

13. При необходимости измените порт источника трафика в поле **Порт (источник)**, если этот параметр применим к протоколу.

14. При необходимости измените IP-адрес получателя в поле **IP-адрес (получатель)**.

15. При необходимости измените порт получателя в поле **Порт (получатель)**.

16. При необходимости выберите протокол в раскрывающемся списке **Протокол**. Для выбора доступны следующие варианты:

- **TCP (IPv4)**.
- **UDP (IPv4)**.
- **Любой**.

17. Нажмите на кнопку **ОК** в панели изменения правила межсетевого экрана.

Панель закроется, изменения в правиле отобразятся в таблице правил для межсетевого экрана.

18. Если требуется изменить порядок выполнения правила в таблице правил, установите флажок рядом с правилом и с помощью кнопок **Вверх** или **Вниз** повысьте или понизьте приоритет обработки правила.

Пользовательские правила межсетевого экрана будут выполняться в порядке расположения их в таблице правил сверху вниз, до первого совпадения.

19. Нажмите на кнопку **Сохранить**.

Удаление правил межсетевого экрана

Вы можете удалять правила межсетевого экрана через Kaspersky Security Center Web Console.

Чтобы удалить правило межсетевого экрана:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором запущен Kaspersky IoT Secure Gateway. Если имя компьютера отсутствует в списке, [добавьте его в группу Управляемые устройства](#).
Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на название Kaspersky IoT Secure Gateway.
Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
5. Выберите закладку **Параметры программы**.
6. Выберите раздел **Сеть** → **Межсетевой экран**.
Отобразится таблица, содержащая пользовательские правила для межсетевого экрана.
7. Установите флажок около правила, которое вы хотите удалить.
8. Нажмите на кнопку **Удалить** в верхней части таблицы правил межсетевого экрана.
Правило будет удалено из таблицы правил межсетевого экрана.
9. Нажмите на кнопку **Сохранить**.

Обращение в Службу технической поддержки

Если вы не нашли решения вашей проблемы в документации к Kaspersky IoT Secure Gateway, рекомендуем обратиться в Службу технической поддержки "Лаборатории Касперского". Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании системы.

Для получения дополнительной информации о состоянии сетевых интерфейсов и таблицы маршрутизации вы можете перейти на страницу устранения неисправностей, которая находится по адресу: <адрес веб-интерфейса Kaspersky IoT Secure Gateway>/troubleshooting.html.

Информация на странице <адрес веб-интерфейса Kaspersky IoT Secure Gateway>/troubleshooting.html отображается только если вы предварительно вошли в веб-интерфейс Kaspersky IoT Secure Gateway.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить по телефону +7 (495) 780-33-67.

Этот способ позволяет проконсультироваться по телефону со специалистами русскоязычной Службы технической поддержки.

- Отправить сообщение электронной почты на адрес Службы технической поддержки tasupport@kaspersky.com.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

Подготовка к установке Kaspersky IoT Secure Gateway

Прежде, чем установить Kaspersky IoT Secure Gateway, требуется подготовить устройство Advantech UTX-3117FS-S6A1N к установке Kaspersky IoT Secure Gateway.

[Подготовку к установке Kaspersky IoT Secure Gateway](#) выполняют специалисты "Лаборатории Касперского". Описанные в этом разделе инструкции приведены для ознакомительных целей.

Чтобы подготовить устройство Advantech UTX-3117FS-S6A1N к установке Kaspersky IoT Secure Gateway:

1. [Включите устройство Advantech UTX-3117FS-S6A1N](#).
2. Подключите монитор и клавиатуру к соответствующим разъемам на лицевой панели Advantech UTX-3117FS-S6A1N.
3. Нажмите на кнопку включения / выключения в правой части лицевой панели Advantech UTX-3117.
На лицевой панели Advantech UTX-3117 загорится индикатор питания, и устройство начнет запускаться.
4. Во время загрузки на клавиатуре нажмите на клавишу **DELETE**.
Откроется главное меню BIOS устройства Advantech UTX-3117FS-S6A1N.
5. Восстановите настройки по умолчанию:
 - a. Выберите закладку **Save & Exit**.
 - b. В меню **Default Options** выберите пункт **Restore Defaults**.
 - c. Выйдите из закладки **Save & Exit**, нажав клавишу **F4**.Advantech UTX-3117FS-S6A1N начнет перезагружаться.
6. Во время перезагрузки на клавиатуре нажмите на клавишу **DELETE**.
Откроется главное меню BIOS устройства Advantech UTX-3117FS-S6A1N.
7. Проверьте настройки безопасной загрузки системы:
 - a. Выберите закладку **Security**.
 - b. Выберите пункт **Secure Boot**.
 - c. Проверьте, что параметр **Secure Boot** имеет значение **Not Active**:
 - Если **Secure Boot** имеет значение **Not Active**, перейдите к следующему шагу.
 - Если **Secure Boot** имеет значение **Active**, измените его на **Not Active** и перезагрузите устройство Advantech UTX-3117FS-S6A1N.

- d. Выйдите из закладки **Security**, нажав клавишу **ESC**.
8. Настройте южный мост:
 - a. Выберите закладку **Chipset**.
 - b. В открывшемся меню выберите пункт **South Bridge**.
 - c. В качестве значения параметра **OS Selection** выберите **Intel Linux**.
 - d. Выйдите из закладки **Chipset**, нажав клавишу **ESC**.
 9. Настройте расширенные параметры:
 - a. Выберите закладку **Advanced**.
 - b. В открывшемся меню выберите пункт **CSM Configuration**.
 - c. В качестве значения параметра **CSM Support** выберите **Enabled**.
 - d. В качестве значений параметров **Network** и **Other PCI devices Support** выберите **Do not launch**.
 - e. Вернитесь на закладку **Advanced**, нажав клавишу **ESC**.
 - f. В открывшемся меню выберите пункт **CPU Configuration**. В качестве значения параметра **VT-d** выберите **Enabled**.
 - g. Вернитесь на закладку **Advanced**, нажав клавишу **ESC**.
 - h. В открывшемся меню выберите пункт **Network Stack Configuration**. В качестве значения параметра **Network Stack** выберите **Enabled**.
 - i. Вернитесь на закладку **Advanced**, нажав клавишу **ESC**.
 - j. В открывшемся меню выберите пункт **Serial Port Console Redirection**.
 - k. В качестве значения параметра **Console Redirection** выберите **Enabled**.
 - l. Выберите пункт **Console Redirection Settings**.
 - m. В качестве значения параметра **Terminal Type** выберите **VT100+**.
 - n. Выйдите из закладки **Advanced**, нажав клавишу **ESC**.
 10. Настройте параметры загрузки:
 - a. Выберите закладку **Boot**.
 - b. В качестве значения параметра **Boot Option #1** выберите **UEFI OS**.
 - c. Выйдите из закладки **Boot**, нажав клавишу **ESC**.
 11. Выйдите из BIOS с сохранением изменений:
 - a. Выберите закладку **Save & Exit**.

b. На закладке **Save & Exit** выберите пункт **Save Changes & Exit**.

Advantech UTX-3117FS-S6A1N перезапустится с настроенными параметрами. При следующем включении устройство также будет запускаться с настроенными параметрами. Перед установкой Kaspersky IoT Secure Gateway устройство требуется выключить.

Установка Kaspersky IoT Secure Gateway

Для начала работы с Kaspersky IoT Secure Gateway требуется его установить на устройство Advantech UTX-3117FS-S6A1N.

[Установку Kaspersky IoT Secure Gateway](#) выполняют специалисты "Лаборатории Касперского".
Описанные в этом разделе инструкции приведены для ознакомительных целей.

Чтобы установить Kaspersky IoT Secure Gateway:

1. Загрузите образ дистрибутива SystemRescueCd с официального сайта [SystemRescue](#).
2. На локальном компьютере создайте загрузочный USB с дистрибутивом SystemRescueCd, например, используя утилиту dd:

```
$ dd if=systemrescuecd-6.0.3.iso of=/dev/%имя USB устройства%
```

Утилита dd доступна только в некоторых UNIX™-подобных операционных системах.
3. Вставьте загрузочный USB с дистрибутивом SystemRescueCd в USB-разъем на Advantech UTX-3117FS-S6A1N.
4. Нажмите на кнопку включения / выключения в правой части лицевой панели Advantech UTX-3117.
5. На клавиатуре нажмите на клавишу **DELETE**.
Откроется главное меню BIOS устройства Advantech UTX-3117FS-S6A1N.
6. Настройте параметры загрузки Kaspersky IoT Secure Gateway с загрузочного USB:
 - a. Выберите закладку **Boot**.
 - b. В разделе **Boot Option Priorities** с помощью клавиш **+** или **-** поднимите на первое место значение **UEFI: <имя_загрузочного_USB>**.
 - c. Выйдите из закладки **Boot**, нажав клавишу **ESC**.
7. Выйдите из BIOS с сохранением изменений:
 - a. Выберите закладку **Save & Exit**.
 - b. На закладке **Save & Exit** выберите пункт **Save Changes & Exit**.

После завершения установки Kaspersky IoT Secure Gateway и извлечения загрузочного USB параметры, установленные на этом шаге инструкции будут сброшены. При следующей загрузке Kaspersky IoT Secure Gateway будут применяться параметры загрузки настроенные при [подготовке к установке Kaspersky IoT Secure Gateway](#).

8. Перейдите в директорию /tmp, используя командную строку:

```
$ cd /tmp
```

9. Загрузите установочный образ Kaspersky IoT Secure Gateway из внутренней сети, например, используя утилиту wget:

```
$ wget %путь до установочного образа Kaspersky IoT Secure Gateway%
```

Предварительно требуется разместить установочный образ Kaspersky IoT Secure Gateway, полученный в комплекте поставки, на HTTP-сервере, который развернут во внутренней сети.

HTTP-сервер и устройство Advantech UTX-3117FS-S6A1N должны располагаться в одной сети.

10. Распакуйте образ, используя командную строку:

```
$ tar -xzf latest-kos-mqtt-broker.tgz
```

```
$ cd kos-mqtt-broker/install
```

```
$ tar -xzf install.tar.gz
```

11. Запустите установку:

```
$ ./install.sh
```

12. Когда установка завершится, выключите Advantech UTX-3117FS-S6A1N средствами SystemRescueCd, выполнив команду:

```
$ shutdown -h now
```

13. Извлеките загрузочный USB с дистрибутивом SystemRescueCd.

14. Включите Advantech UTX-3117FS-S6A1N, нажав на кнопку включения / выключения в правой части лицевой панели.

Kaspersky IoT Secure Gateway запустится автоматически.

После первого включения Kaspersky IoT Secure Gateway рекомендуется [настроить сеть](#), [создать и загрузить сертификат администратора](#), [настроить дату и время](#) и [сменить сертификат веб-сервера](#) на используемый в вашей организации.

Глоссарий

Kaspersky Security Center Web Console

Программа (веб-приложение), предназначенная для контроля состояния системы безопасности сетей организации, находящихся под защитой программ "Лаборатории Касперского".

KasperskyOS

Микроядерная операционная система для построения безопасных решений.

Message Queuing Telemetry Transport (MQTT)

Сетевой протокол, работающий поверх стека протоколов TCP/IP, предназначенный для обмена сообщениями между устройствами в Интернете вещей.

MQTT-брокер

Сервер, принимающий, фильтрующий и пересылающий сообщения по протоколу MQTT.

MQTT-топик

Иерархический путь к источнику данных, на базе которого отправляются сообщения по протоколу MQTT.

SSL

Протокол шифрования данных в локальных сетях и в интернете. SSL используется в веб-приложениях для создания защищенных соединений между клиентом и сервером.

TLS

Безопасный протокол передачи данных в локальных сетях и в интернете с использованием шифрования. TLS используется в веб-приложениях для создания защищенных соединений между клиентом и сервером.

Администратор Kaspersky Security Center

Лицо, управляющее работой программы через систему удаленного централизованного администрирования Kaspersky Security Center.

Безопасный шлюз Интернета вещей

Система, которая обеспечивает безопасную передачу пользовательского трафика между датчиками и платформой Интернета вещей.

Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждой из установленных в группе программ могут быть созданы групповые политики и сформированы групповые задачи.

Задача

Функции, выполняемые программой "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

Интернет вещей

Вычислительная сеть электронных устройств ("вещей"), оснащенных встроенными возможностями взаимодействия с внешней средой или друг с другом без участия человека.

Компонент Kaspersky IoT Secure Gateway

Часть Kaspersky IoT Secure Gateway, предназначенная для обеспечения функциональности системы (например, аутентификации).

Плагин управления программой

Специализированный компонент, предоставляющий интерфейс для управления работой программы через Консоль администрирования. Для каждой программы существует свой плагин управления. Он входит в состав всех программ "Лаборатории Касперского", управление которыми может осуществляться при помощи Kaspersky IoT Secure Gateway.

Политика

Политика определяет параметры работы программы и доступ к настройке программы, установленной на устройствах группы администрирования. Для каждой программы требуется создать свою политику. Вы можете создать неограниченное количество различных политик для программ, установленных на устройствах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться одновременно к каждой программе.

Политика паролей

Функция, реализующая определенное правило задания сложности новых паролей.

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского" и управления ими.

Сертификат администратора

Сертификат, на основании которого осуществляется аутентификация пользователя в веб-интерфейсе Kaspersky IoT Secure Gateway.

Сертификат сервера Kaspersky Security Center

Сертификат, на основании которого осуществляется безопасное взаимодействие Kaspersky IoT Secure Gateway и Kaspersky Security Center при управлении Kaspersky IoT Secure Gateway через Kaspersky Security Center Web Console.

Событие

Запись, содержащая информацию об обнаружении данных в системе или во внутренней сети, которые требуют внимания сотрудника, ответственного за информационную безопасность в вашей организации, сохраняемая в памяти встраиваемого компьютера Advantech UTX-3117.

Управляемые устройства

Устройства сети организации, включенные в одну из групп администрирования.

Устройство с защитой на уровне UEFI

Устройство со встроенным на уровне BIOS программным обеспечением Антивирус Касперского для UEFI. Встроенная защита обеспечивает безопасность устройства еще с начала запуска системы, в то время как защита устройств, не имеющих встроенного ПО, начинает действовать только после запуска программы защиты.

Информация о стороннем коде

Информация о стороннем коде содержится в файле `legal_notices.txt`, который расположен на локальном веб-сервере. Открыть файл можно из раздела **О программе**.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Eclipse Mosquitto – товарный знак Eclipse Foundation, Inc.

Google, Chrome и Firebase – товарные знаки Google, Inc.

HUAWEI является зарегистрированным товарным знаком Huawei Technologies Co., Ltd в Китае и других странах.

Intel – товарный знак Intel Corporation, зарегистрированный в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft – товарный знак Microsoft Corporation, зарегистрированный в Соединенных Штатах Америки и в других странах.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

JavaScript – зарегистрированный товарный знак Oracle Corporation и / или ее аффилированных компаний.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.