kaspersky

Kaspersky IoT Secure Gateway

Содержание

Уведомления о товарных знаках

О Kaspersky IoT Secure Gateway

Kaspersky IoT Secure Gateway (далее также "система") представляет собой операционную систему KasperskyOS с предварительно настроенным набором прикладного программного обеспечения. Kaspersky IoT Secure Gateway предназначен для установки на встраиваемый компьютер модели Advantech UTX-3117-S6A1N.

Система Kaspersky IoT Secure Gateway предназначена для работы в качестве безопасного шлюза Интернета вещей (Internet of Things) в сети организации.

Версия системы: Kaspersky IoT Secure Gateway 2.0 Beta

Kaspersky IoT Secure Gateway 2.0 Beta распространяется исключительно с целью проведения тестирования в практических условиях информационно-коммуникационной среды юридического лица.

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:

- Установочный образ Kaspersky IoT Secure Gateway: kisg-<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-документация.
- Информация о версии (Release Notes).

Аппаратные и программные требования

Система Kaspersky IoT Secure Gateway может быть установлена 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:

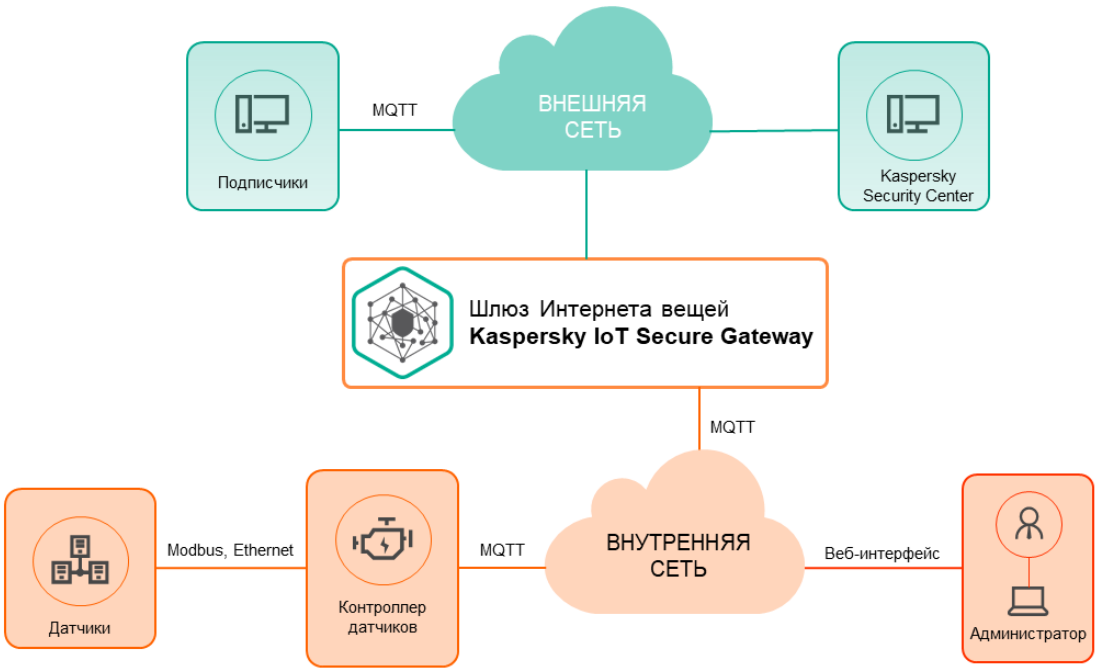
- Google Chrome™ версии 76 и выше.
- Mozilla™ Firefox™ версии 68 и выше.

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.



Компоненты Kaspersky IoT Secure Gateway

Kaspersky IoT Secure Gateway включает в себя следующие компоненты:

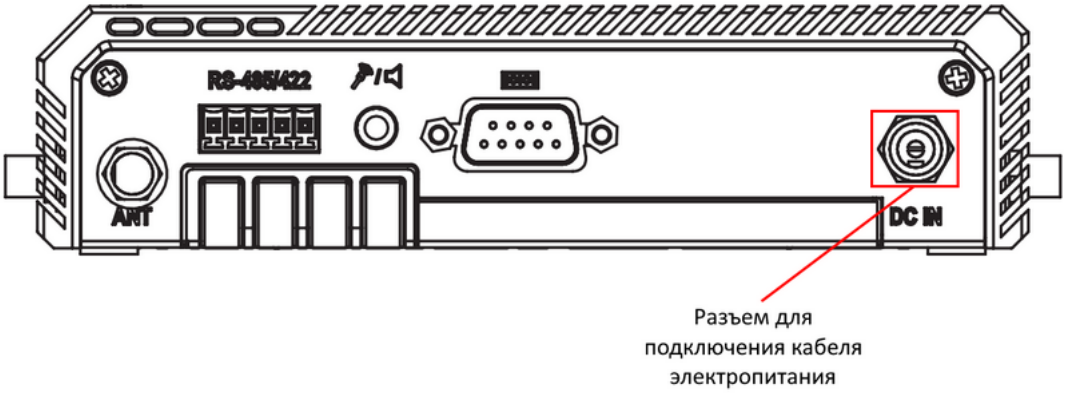
- *Secure manager*. Обеспечивает обмен данными между компонентами Kaspersky IoT Secure Gateway, является точкой получения информации о безопасном состоянии остальных компонентов.
- *Auth server*. Обеспечивает аутентификацию учетной записи (запрашивает у компонента *Secure storage* данные о корректности пароля).
- *Traffic processor*. Обеспечивает функциональность обнаружения устройств в сети и работу устройств из списка разрешенных.
- *Secure storage*. Используется для хранения открытых ключей сертификатов и учетных записей пользователей системы.
- *Config manager*. Используется для хранения конфигурационных параметров всех компонентов системы.
- *Traffic controller*. Обеспечивает работу сетевых интерфейсов системы.
- *Web server*. Обеспечивает работу веб-интерфейса системы.
- *MQTT broker*. Обеспечивает функциональность MQTT-брокера.
- *Blocker*. Обеспечивает блокировку узлов, вредоносная деятельность которых обнаружена компонентом IDS.
- *IPS*. Обеспечивает функциональность предотвращения вторжений.
- *Logger*. Обеспечивает хранение отладочных журналов системы.
- *Tee manager*. Контролирует рабочее состояние всех компонентов системы.
- *Bootloader*. Обеспечивает безопасную загрузку программного обеспечения системы.
- *Firewall*. Обеспечивает функционал межсетевого экранирования и контроля соединений.
- *KSC controller*. Обеспечивает подключение к системе централизованного управления Kaspersky Security Center.

Подготовка к установке Kaspersky IoT Secure Gateway

Прежде, чем установить Kaspersky IoT Secure Gateway, вам нужно настроить Advantech UTX-3117FS-S6A1N.

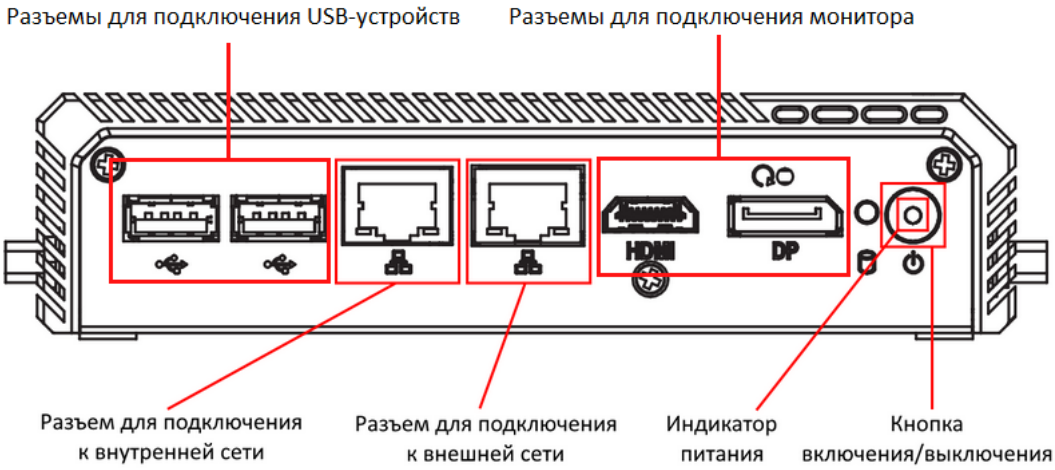
Чтобы настроить Advantech UTX-3117FS-S6A1N, выполните следующие действия:

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



Задняя панель Advantech UTX-3117FS-S6A1N

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



Лицевая панель Advantech UTX-3117

3. Подключите монитор и клавиатуру к соответствующим разъемам на лицевой панели Advantech UTX-3117FS-S6A1N.

4. Нажмите на кнопку включения / выключения в правой части лицевой панели Advantech UTX-3117.

   На лицевой панели Advantech UTX-3117 загорится индикатор питания, и система начнет запускаться.

5. Нажмите клавишу **DELETE**.

   Откроется главное меню BIOS.

6. Восстановите настройки по умолчанию:

   a. Выберите закладку **Save & Exit**.

   b. В меню **Default Options** выберите пункт **Restore Defaults**.

c. Выйдите из закладки **Save & Exit**.

7. Проверьте настройки Secure Boot:

   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 Advantech UTX-3117FS-S6A1N.

   d. Выйдите из закладки **Security**.

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**.

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**.

   f. В открывшемся меню выберите пункт **CPU Configuration**. В качестве значения параметра **VT-d** выберите **Enabled**.

   g. Вернитесь на закладку **Advanced**.

   h. В открывшемся меню выберите пункт **Serial Port Console Redirection**.

   i. В качестве значения параметра **Console Redirection** выберите **Enabled**.

   j. Выберите пункт **Console Redirection Settings**.

   k. В качестве значения параметра **Terminal Type** выберите **VT100+**.

   l. Выйдите из закладки **Advanced**.

10. Настройте параметры загрузки:

a. Выберите закладку **Boot**.

b. В качестве значения параметра **Boot Option #1** выберите **UEFI: Build-in EFI shell**.

c. Выйдите из закладки **Boot**.

11. Выйдите из BIOS с сохранением изменений:

a. Выберите закладку **Save & Exit**.

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

Установка Kaspersky IoT Secure Gateway

Чтобы установить Kaspersky IoT Secure Gateway, выполните следующие действия:

1. Загрузите образ дистрибутива SystemRescueCd с официального сайта.
2. Создайте загрузочный USB с дистрибутивом SystemRescueCd, например, используя утилиту dd:

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

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.

   SystemRescueCd загрузится автоматически.

5. Перейдите в директорию /tmp, используя командную строку:

   ```
   $ cd /tmp
   ```

6. Загрузите установочный образ Kaspersky IoT Secure Gateway из сети, например, используя утилиту wget:

   ```
   $ wget %путь до установочного образа Kaspersky IoT Secure Gateway%
   ```

7. Распакуйте образ, используя командную строку:

   ```
   $ tar -xzf latest-kos-mqtt-broker.tgz
   $ cd kos-mqtt-broker/install
   $ tar -xzf install.tar.gz
   ```

8. Запустите установку:

   ```
   $ ./install.sh
   ```

9. Когда установка завершится, перезагрузите Advantech UTX-3117FS-S6A1N средствами SystemRescueCd.
10. Извлеките загрузочный USB с дистрибутивом SystemRescueCd.

После перезагрузки Kaspersky IoT Secure Gateway запустится автоматически.

После первого включения рекомендуется настроить сеть, сменить пароль администратора по умолчанию, настроить дату и время и сменить сертификат веб-сервера на используемый в вашей организации.

Подключение к веб-интерфейсу Kaspersky IoT Secure Gateway

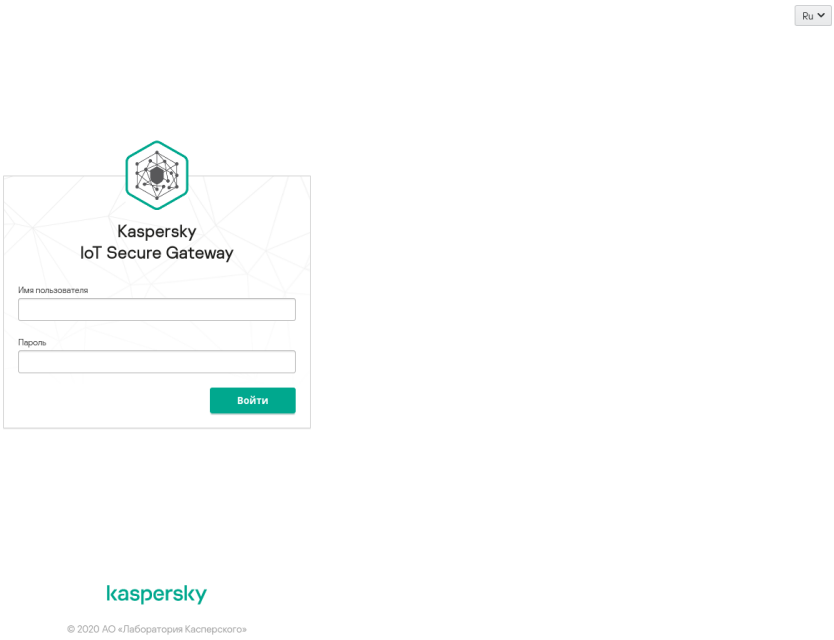
Вы можете подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway с использованием любого поддерживаемого браузера. Браузер должен быть установлен на компьютере, который имеет доступ к Kaspersky IoT Secure Gateway через внутреннюю сеть.

Система Kaspersky IoT Secure Gateway поставляется со статически настроенным IP-адресом. Чтобы подключиться к системе и выполнить первоначальную настройку, нужно настроить IP-адрес вашего компьютера так, чтобы он находился в одной сети с Kaspersky IoT Secure Gateway. IP-адрес Kaspersky IoT Secure Gateway можно узнать у специалистов Службы технической поддержки "Лаборатории Касперского".

Чтобы подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway, выполните следующие действия:

1. Откройте браузер.
2. В адресной строке браузера введите IP-адрес.

   Откроется страница ввода учетных данных.



Страница ввода учетных данных в окне браузера

3. В поле **Имя пользователя** введите имя пользователя.
4. В поле **Пароль** введите пароль.
5. Нажмите на кнопку **Войти**.

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

Завершение 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 10 минут. В течение этого времени система может предоставить доступ к веб-интерфейсу Kaspersky IoT Secure Gateway без запроса учетных данных пользователя, если для повторного подключения используются те же компьютер и браузер.

Чтобы завершить сеанс подключения к веб-интерфейсу Kaspersky IoT Secure Gateway, выполните следующие действия:

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

   Появится меню пользователя.

2. В меню пользователя выберите пункт **Выйти**.

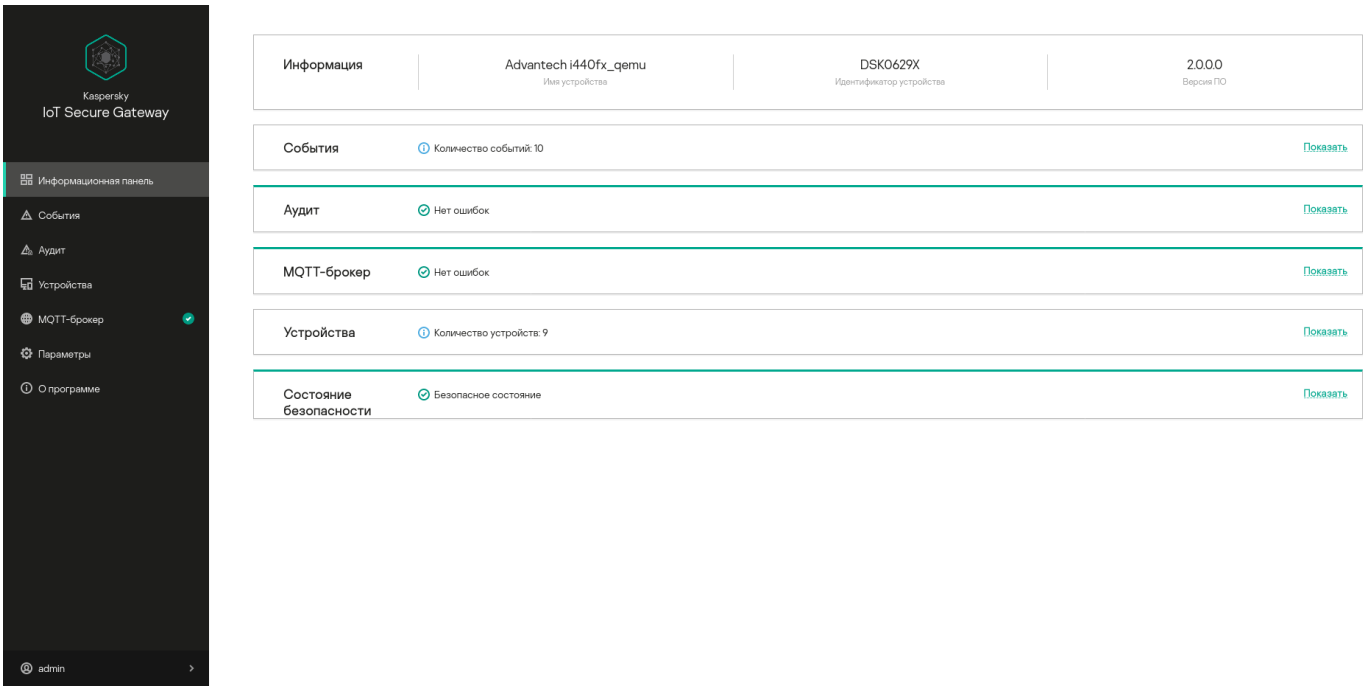
   В окне браузера отобразится страница ввода учетных данных.

Веб-интерфейс Kaspersky IoT Secure Gateway

Этот раздел содержит информацию об основных элементах веб-интерфейса Kaspersky IoT Secure Gateway.

Меню веб-интерфейса Kaspersky IoT Secure Gateway

В левой части страницы веб интерфейса Kaspersky IoT Secure Gateway отображается меню. Справа отображается содержимое выбранного в меню раздела (см. рис. ниже).



Страница веб-интерфейса программы в окне браузера

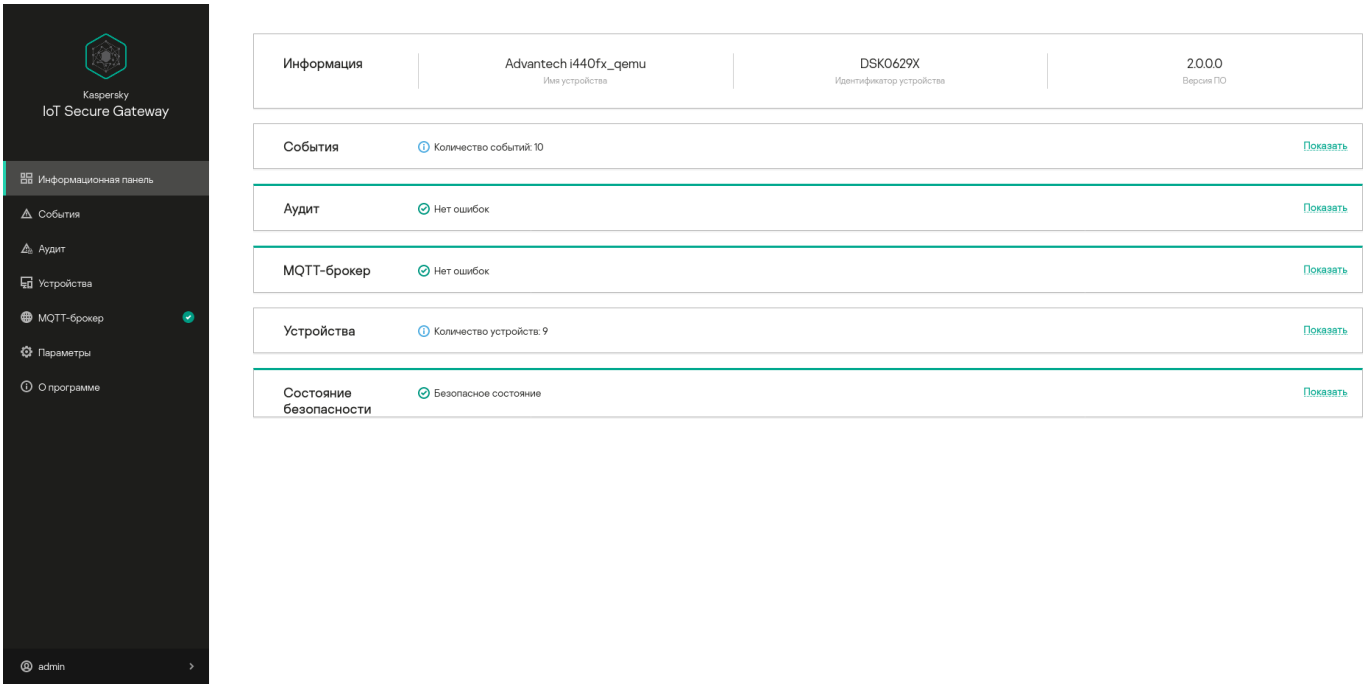
Меню веб-интерфейса содержит следующие разделы:

	Информационная панель Открывает раздел, который содержит информацию о последних событиях, обнаруженных устройствах и состоянии компонентов системы.		**События** Открывает раздел, в котором отображаются события безопасности сети.
	Аудит Открывает раздел, в котором отображаются события безопасности системы.		**Устройства** Открывает раздел, в котором отображаются обнаруженные в сети устройства.
	MQTT-брокер Открывает раздел, в котором отображаются профили MQTT-брокера.		**Параметры** Открывает раздел, в котором можно просматривать и изменять параметры системы.
	О программе		**<Имя пользователя>**

	Открывает раздел, который содержит краткую информацию о системе.		Разворачивает или сворачивает меню пользователя.

Раздел Информационная панель

В разделе **Информационная панель** (см. рис. ниже) вы можете просматривать сводную информацию о системе.



Раздел **Информационная панель**

В разделе **Информационная панель** отображаются следующие информационные блоки:

- **Информация** – название и серийный номер аппаратной платформы, версия системы Kaspersky IoT Secure Gateway.

- **События** – количество событий безопасности сети. Если развернуть блок **События** по ссылке **Показать**, отобразится количество 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.

- **Аудит** – информация о наличии событий безопасности системы, которые записываются в журнал аудита. Если система зарегистрировала события с уровнем важности *Важные* или *Критические*, то в блоке отображается **Проблемы**. Если события с уровнем важности *Важные* или *Критические* отсутствуют, в блоке отображается **Нет ошибок**. По ссылке **Показать** вы можете развернуть блок **Аудит**, чтобы просмотреть количество событий безопасности системы для каждого уровня важности.

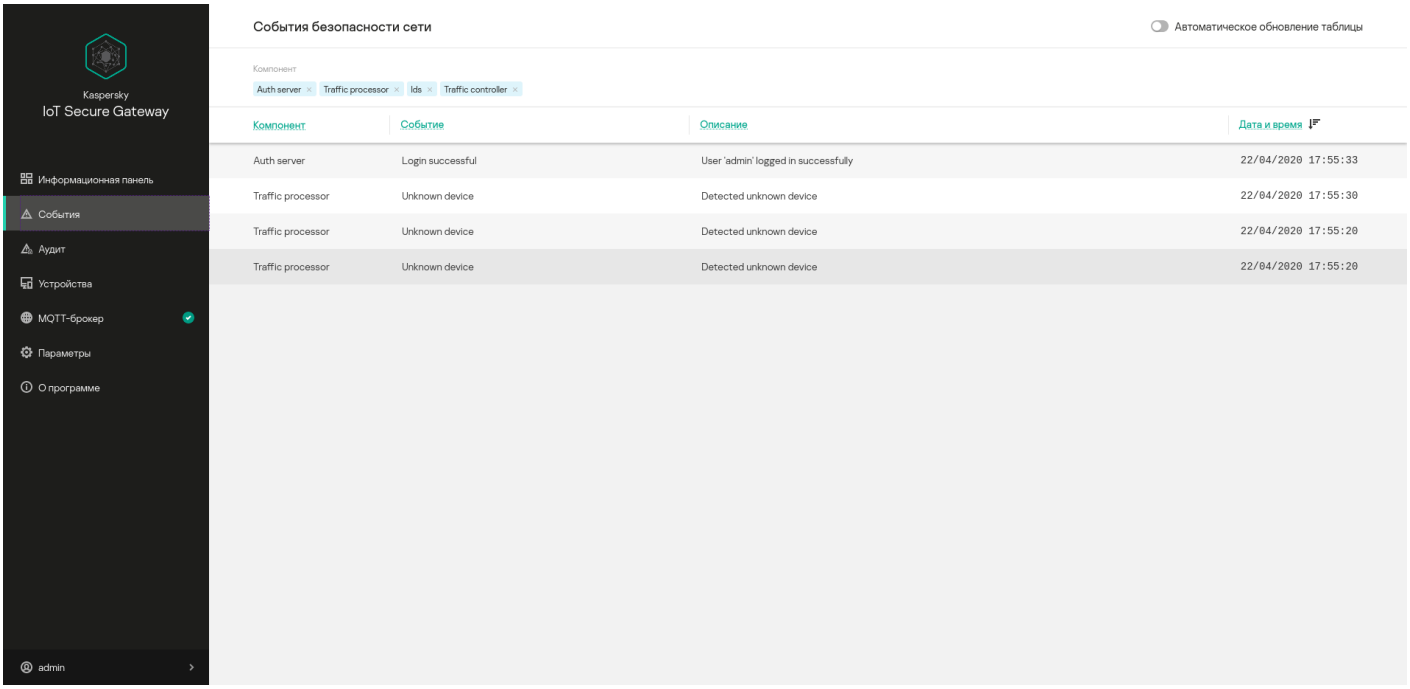
- **MQTT-брокер** – статистика работы системы по протоколу MQTT. Если система обнаружила проблемы с передачей данных по протоколу MQTT, в блоке отображается **Проблемы**. Если проблемы с передачей данных по протоколу MQTT отсутствуют, в блоке отображается **Нет ошибок**.

- **Устройства** – количество устройств, обнаруженных в сети.

- **Состояние безопасности** – статус безопасности компонентов системы.

Раздел События

В разделе **События** (см. рис. ниже) вы можете просматривать события безопасности сети, произошедшие в течение текущей сессии подключения пользователя к системе через браузер. События безопасности сети включают в себя появление и исчезновение устройств в сети, а также попытки подключения к веб-интерфейсу устройства.



Раздел **События**

В верхней части раздела **События** расположена панель инструментов, которая содержит следующие элементы управления таблицей событий безопасности сети:

- **Автоматическое обновление таблицы** – включает режим автоматического обновления записей журнала событий на странице. Если переключатель **Автоматическое обновление таблицы** выключен, то на странице отображаются только те события, которые находились в журнале на момент открытия раздела **События безопасности сети**.

- **Компонент** – группирует кнопки для включения и выключения фильтрации событий по компоненту, зарегистрировавшему событие: *Auth server, Traffic processor*.

Для каждой записи журнала событий безопасности сети отображается следующая информация:

- **Компонент** – название компонента, зарегистрировавшего событие.

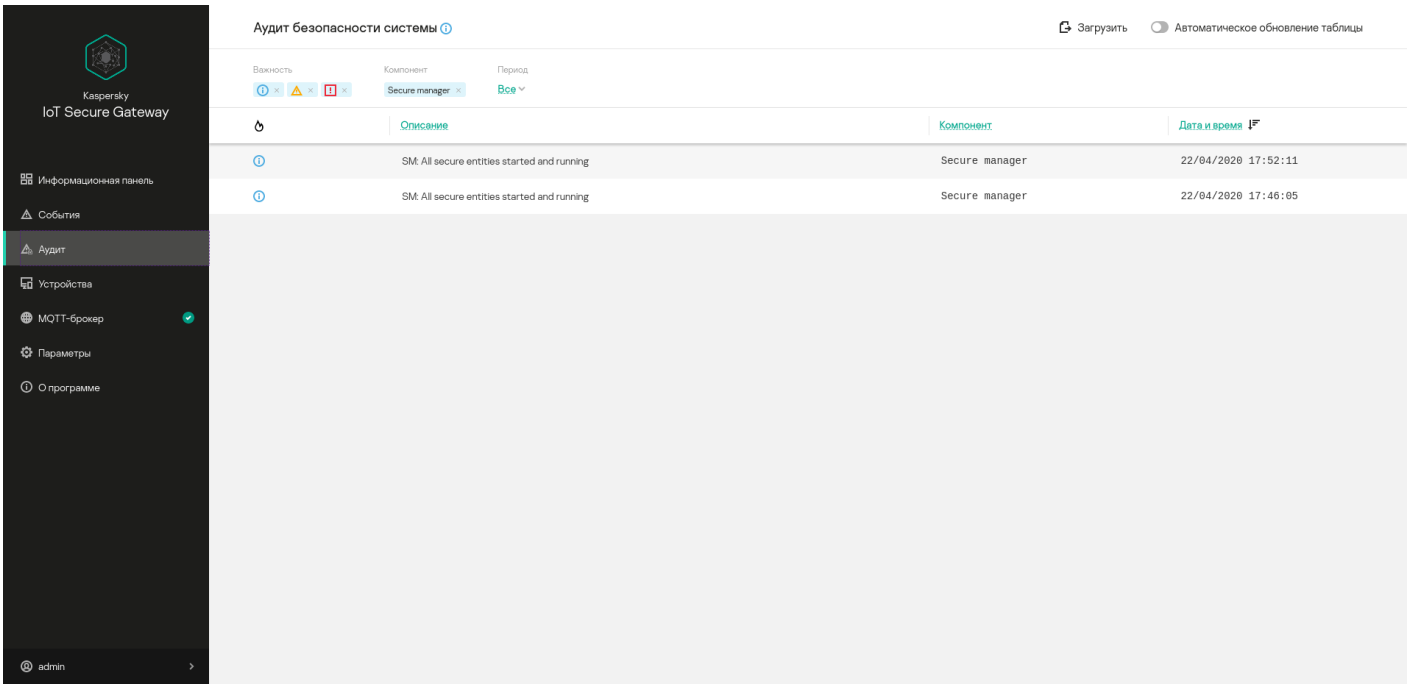
- **Событие** – тип события.

- **Описание** – информация о событии.

- **Дата и время** – дата и время, когда произошло событие.

Раздел Аудит

В разделе **Аудит** (см. рис. ниже) вы можете просматривать журнал аудита, в котором хранятся события безопасности системы.



Раздел **Аудит**

В верхней части раздела **Аудит** расположен значок ⓘ, позволяющий получить информацию о параметрах аудита, и панель инструментов, которая содержит следующие элементы управления таблицей событий безопасности системы:

- **Загрузить** – позволяет загрузить журнал аудита из системы на компьютер администратора.

  Загрузка журнала аудита приводит к удалению журнала аудита из системы.

- **Автоматическое обновление таблицы** – включает режим автоматического обновления записей журнала событий на странице. Если переключатель **Автоматическое обновление таблицы** выключен, то на странице отображаются только те события, которые находились в журнале аудита на момент открытия раздела **Аудит**.

- **Важность** – группирует кнопки для включения и выключения фильтрации событий по уровню важности: ⓘ *Информационные*, ⚠ *Важные* и ! *Критические*.

- **Период** – позволяет выбрать период, за который отображаются события:

  - **Все** – за все время работы устройства.

  - **Последние 24 часа** – за последние 24 часа.

  - **Последняя неделя** – за последнюю неделю.

  - **Последний месяц** – за последний месяц.

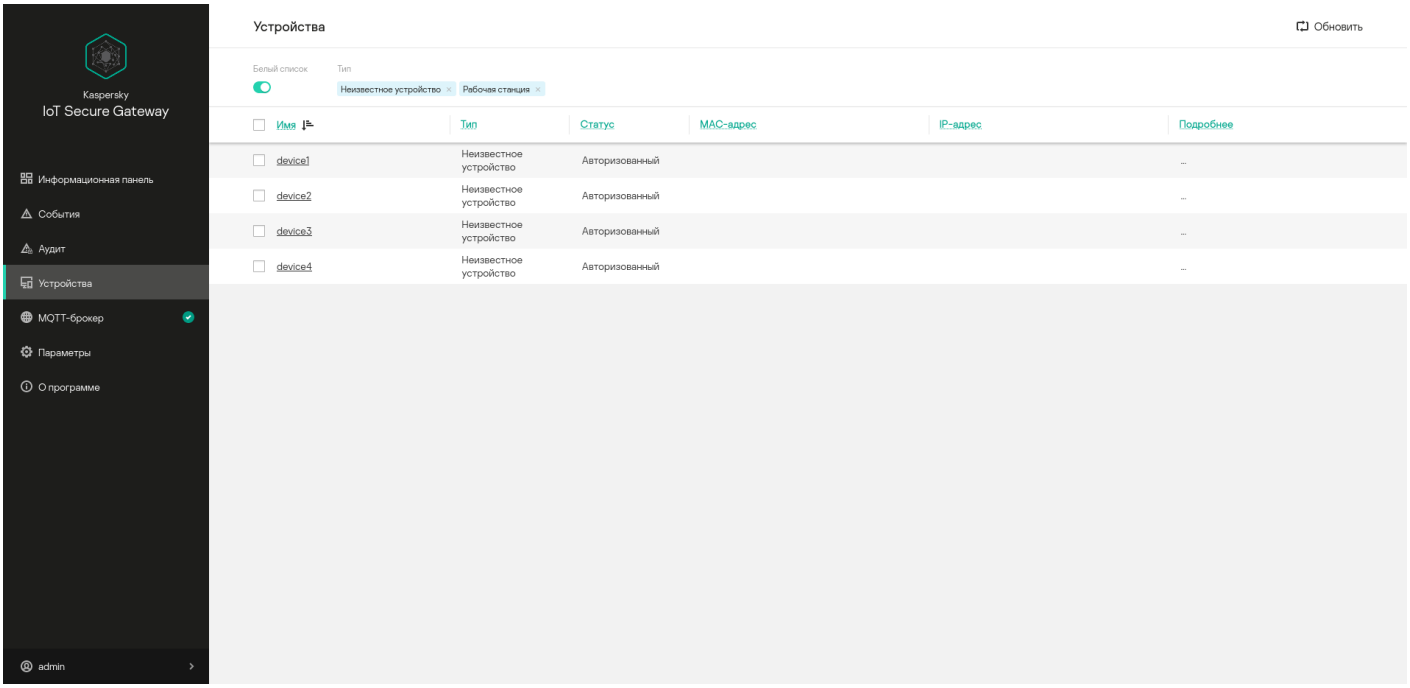
Для каждой записи журнала аудита отображается следующая информация:

- 🔥 – уровень важности события.
- **Описание** – информация о событии.
- **Компонент** – название компонента, зарегистрировавшего событие.
- **Дата и время** – дата и время, когда произошло событие.

Раздел Устройства

В разделе **Устройства** (см. рис. ниже) вы можете просматривать таблицу, которая содержит таблицу устройств, обнаруженных во внутренней сети, добавлять доверенные устройства в список разрешенных и удалять устройства из списка разрешенных.

> Программа автоматически удаляет устройство из таблицы обнаруженных устройств, если это устройство в течение трех минут отсутствует в сети.



Раздел **Устройства**

В верхней части раздела **Устройства** расположена панель инструментов, которая содержит следующие элементы управления таблицей устройств:

- **Обновить** – позволяет обновить список обнаруженных устройств.
- **Белый список** – позволяет отобразить все неавторизованные устройства в сети (если переключатель выключен) или только устройства, находящиеся в списке разрешенных (если переключатель включен).
- **Тип** – позволяет отобразить все устройства одного типа.

Для каждого устройства отображается следующая информация:

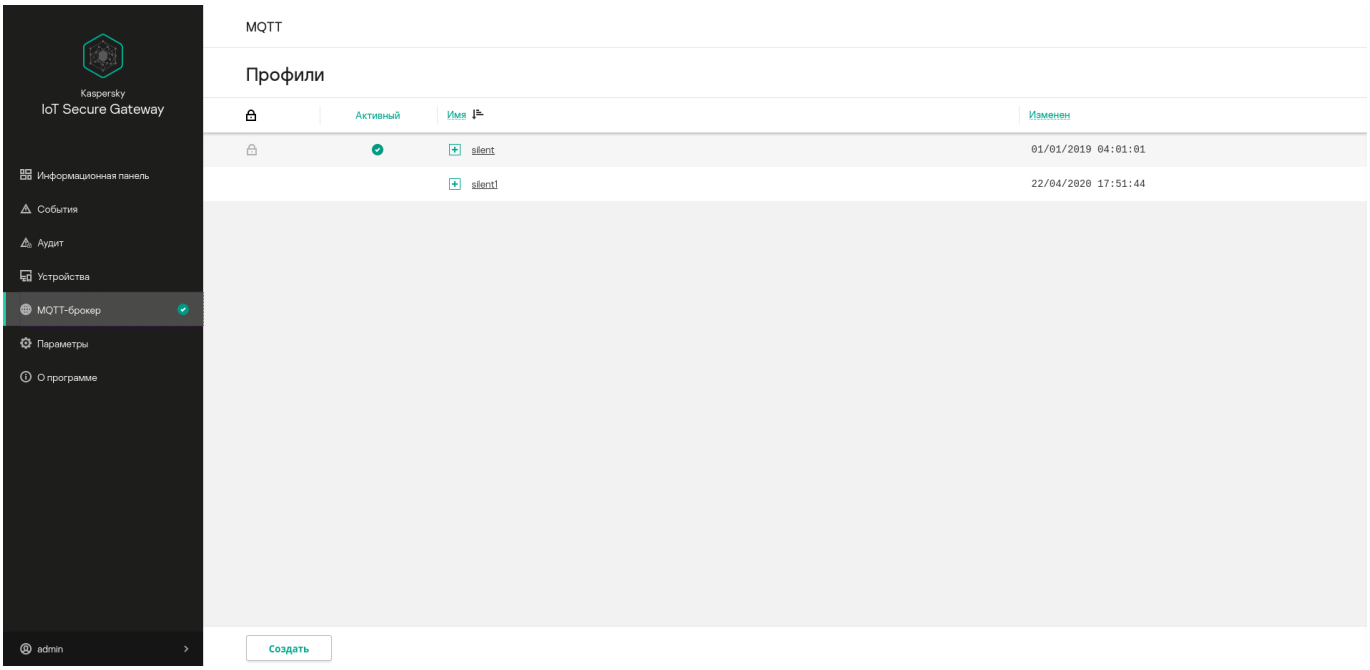
- **Имя** – имя устройства.
- **Тип** – тип устройства.
- **Статус** – статус устройства.
- **MAC-адрес** – MAC-адрес устройства.
- **IP-адрес** – IP-адрес устройства.
- **Подробнее** – операционная система и производитель устройства, если удалось определить.

Раздел MQTT-брокер

В разделе **MQTT-брокер** (см. рис. ниже) вы можете просматривать и изменять параметры MQTT-брокера.

В зависимости от корректности настройки параметров MQTT-брокера в меню рядом с пунктом **MQTT-брокер** может отображаться один из следующих значков:

- Значок . Означает, что параметры MQT-брокера настроены корректно.
- Значок . Означает, что параметры MQTT-брокера настроены некорректно.
- Значок . Означает, что MQTT-брокер не может подключиться к сети.



Раздел **MQTT-брокер**

В этом разделе отображается таблица с профилями MQTT-брокера Eclipse Mosquitto™, а также кнопка **Создать**, позволяющая создать новый профиль.

В таблице отображается следующая информация:

- – доступ на изменение профиля. Предустановленный профиль доступен только для чтения. Все профили, созданные пользователем, можно изменять.

- **Активный** – значком отмечен активный профиль.
- **Имя** – имя профиля. При нажатии на значок открывается список параметров профиля.
- **Изменен** – дата и время последнего изменения профиля.

Раздел Параметры

В разделе **Параметры** вы можете настраивать параметры системы.

Раздел **Параметры** содержит следующие блоки параметров:

- Сеть.
- Безопасность системы.
- Веб-сервер.
- Инструменты.
- Общие.
- KSC.

Блок параметров Сеть

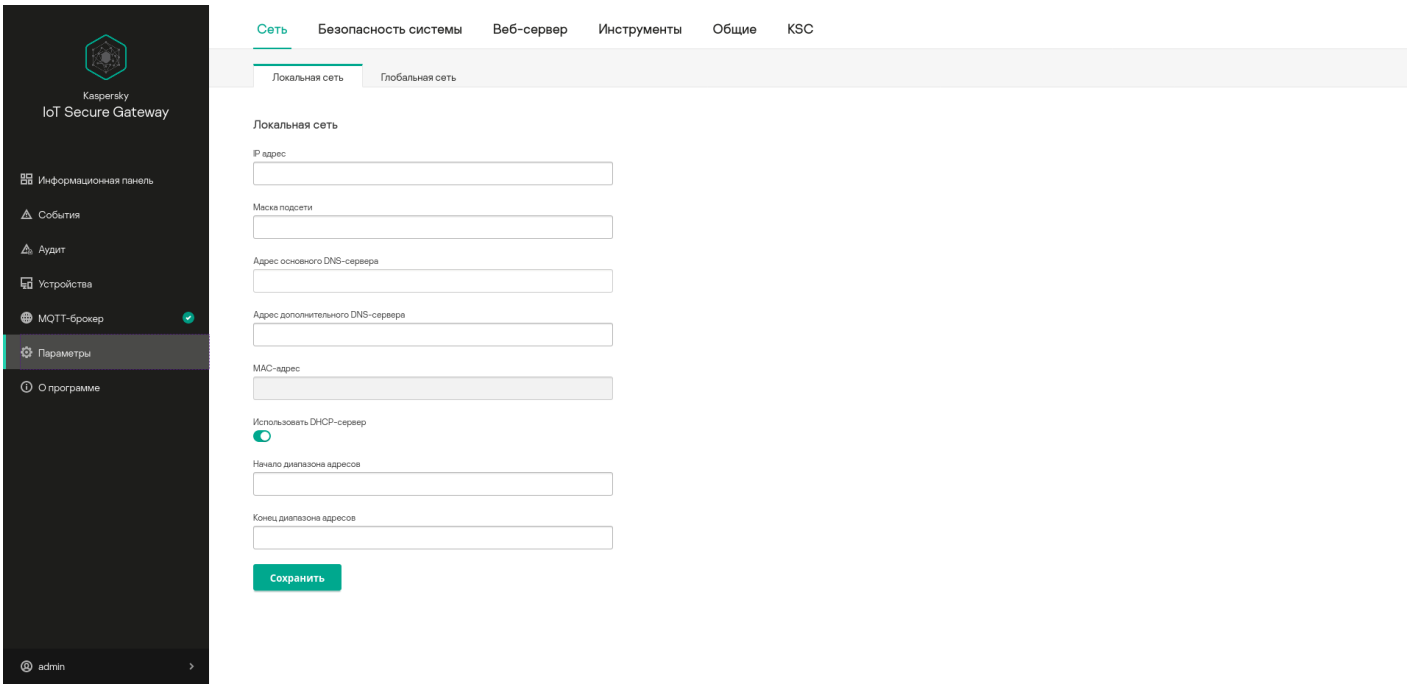
В блоке параметров **Сеть** вы можете просматривать и изменять параметры сети Kaspersky IoT Secure Gateway.

Блок параметров **Сеть** содержит следующие закладки:

- **Локальная сеть**.
- **Глобальная сеть**.

Закладка Локальная сеть

На закладке **Локальная сеть** (см. рис. ниже) вы можете просматривать и изменять параметры подключения Kaspersky IoT Secure Gateway к внутренней сети.



Блок параметров **Сеть**. Закладка **Локальная сеть**

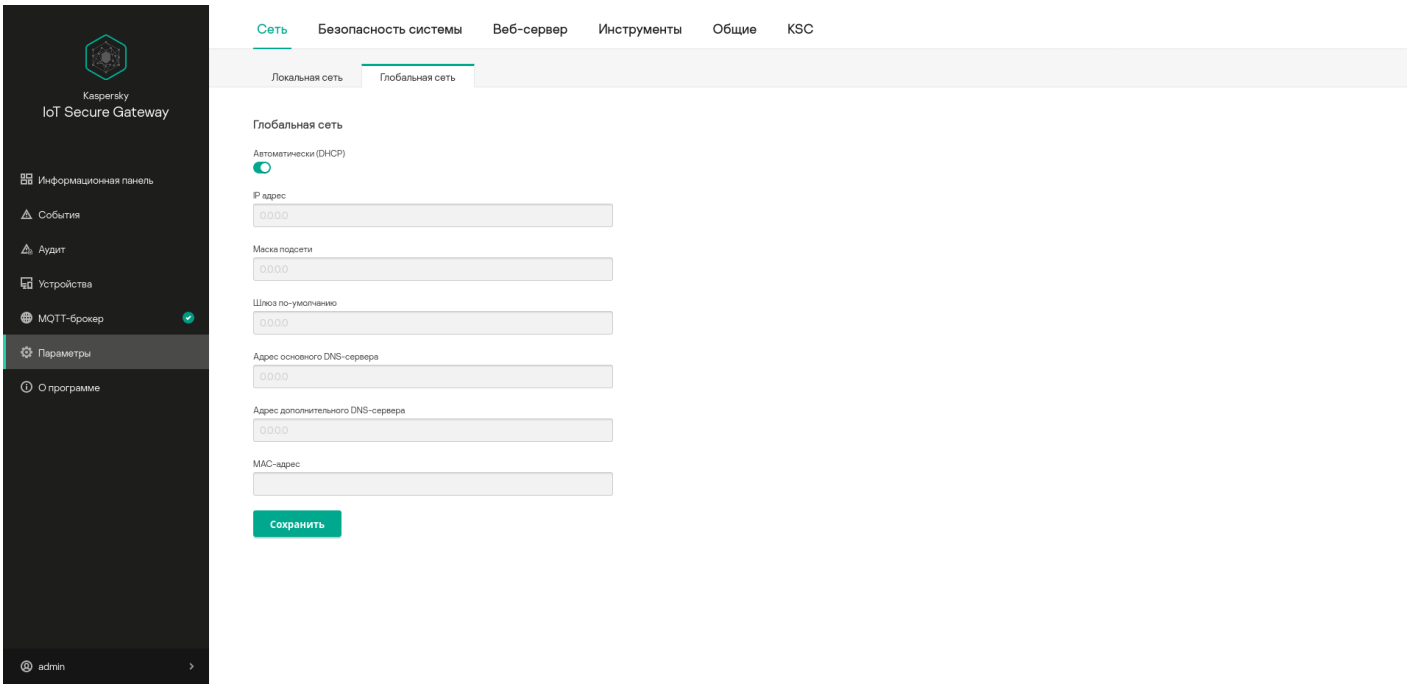
На этой закладке расположен переключатель **Использовать DHCP-сервер**, позволяющий настраивать параметры сети автоматически, а также поля, позволяющие настраивать параметры внутренней сети вручную.

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

- получение доступа к веб-интерфейсу Kaspersky IoT Secure Gateway;
- получение доступа к DHCP-серверу;
- отправка журналов событий на внутренний сервер Syslog;
- мониторинг подключенных к Kaspersky IoT Secure Gateway устройств.

Закладка Глобальная сеть

На закладке **Глобальная сеть** (см. рис. ниже) вы можете просматривать и изменять параметры подключения Kaspersky IoT Secure Gateway к внешней сети.



Блок параметров **Сеть**. Закладка **Глобальная сеть**

На этой закладке расположен переключатель **Автоматически (DHCP)**, позволяющий настраивать параметры сети автоматически, а также поля, позволяющие настраивать параметры внешней сети вручную.

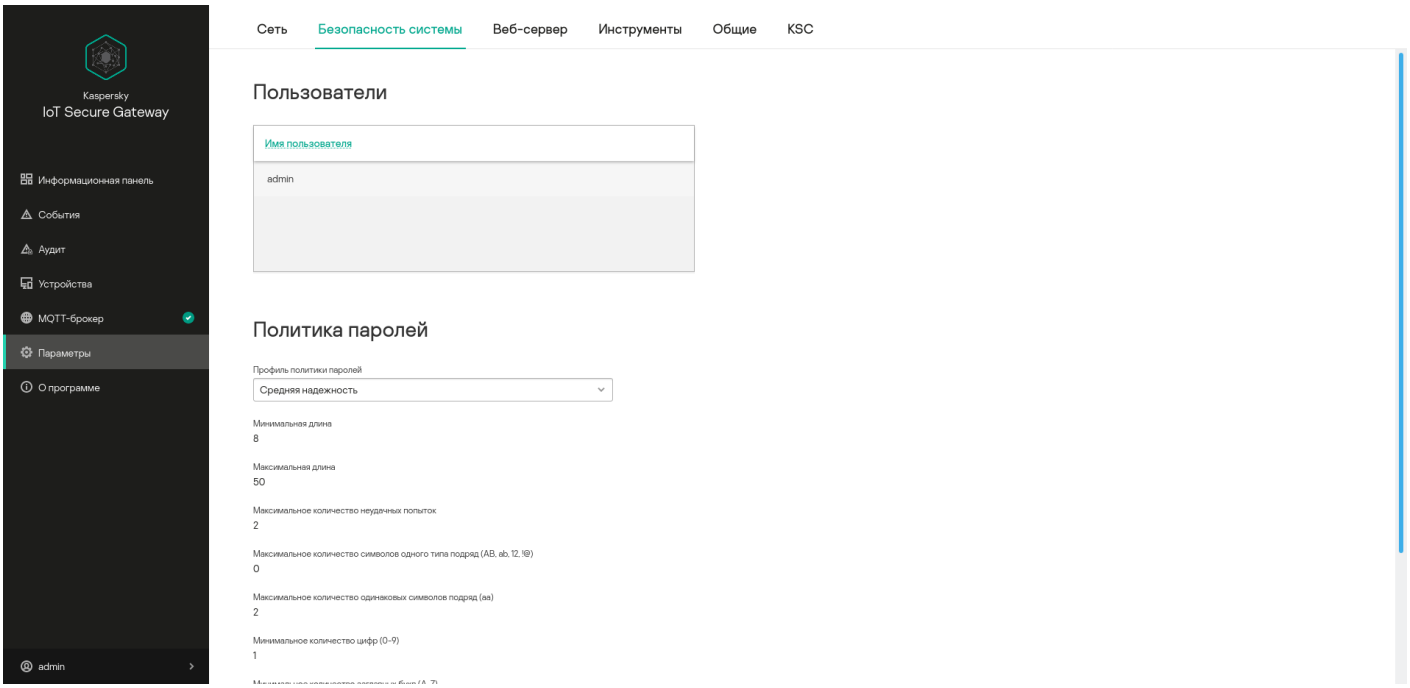
Внешняя сеть Kaspersky IoT Secure Gateway может быть использована для выполнения следующих задач:

- интеграция Kaspersky IoT Secure Gateway и Kaspersky Security Center;
- обеспечение функциональности предотвращения вторжений (компонент IPS);
- отправка журналов событий на внешний сервер Syslog.

Блок параметров Безопасность системы

В блоке параметров **Безопасность системы** вы можете просматривать и изменять параметры безопасности системы Kaspersky IoT Secure Gateway.

В блоке **Пользователи** (см. рис. ниже) вы можете управлять пользователями системы и политикой паролей.



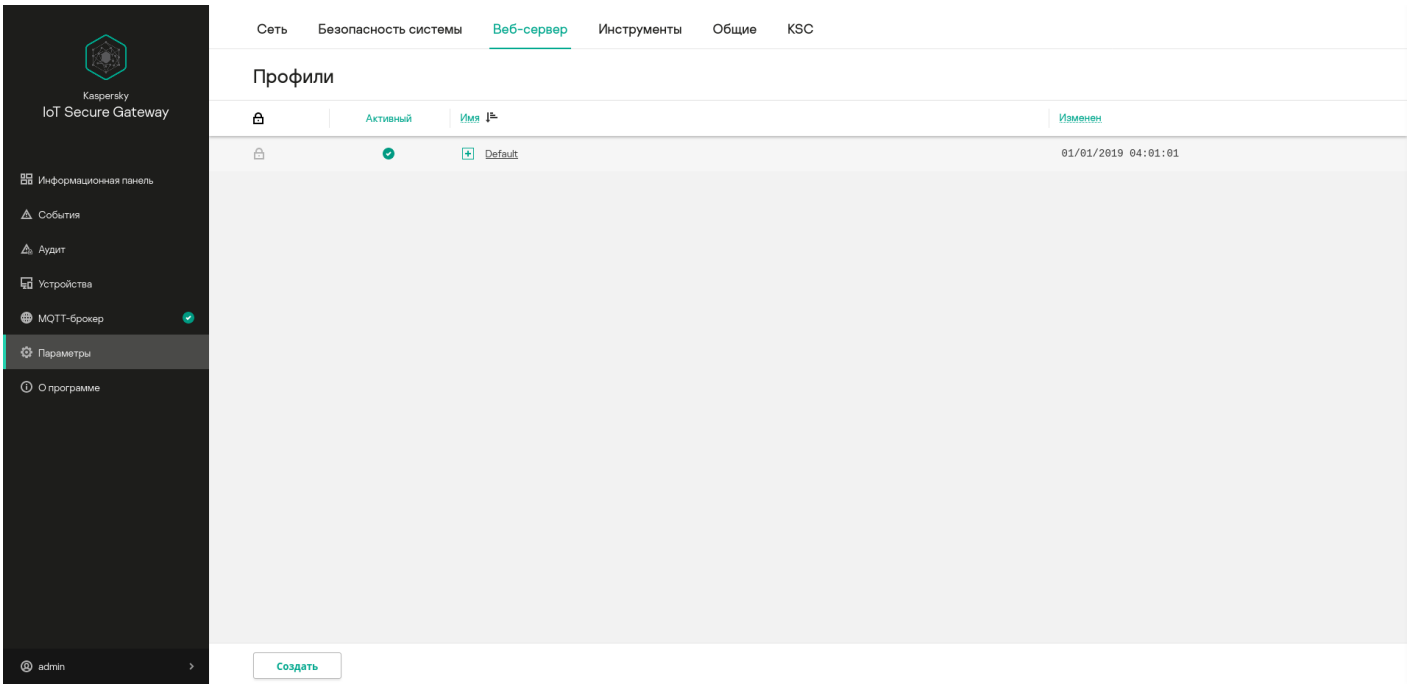
Блок параметров **Безопасность системы**

В основной части блока **Пользователи** расположена таблица пользователей системы Kaspersky IoT Secure Gateway. В графе **Имя пользователя** указано имя учетной записи пользователя.

Под таблицей располагается блок **Политика паролей**, позволяющий настроить политику паролей для пользователей системы.

Блок параметров Веб-сервер

В блоке параметров **Веб-сервер** (см. рис. ниже) вы можете просматривать, создавать, удалять и изменять профили веб-сервера CivetWeb. В этом блоке отображается таблица, содержащая профили веб-сервера CivetWeb, а также кнопка **Создать**, позволяющая создать новый профиль.



Блок параметров **Веб-сервер**

В таблице отображается следующая информация:

- 🔒 – доступ на изменение профиля. Предустановленный профиль доступен только для чтения. Все профили, созданные пользователем, можно изменять.
- **Активный** – значком ✔ отмечен активный профиль.
- **Имя** – имя профиля. При нажатии на значок ⊞ открывается список параметров профиля.
- **Изменен** – дата и время последнего изменения профиля.

Блок параметров Инструменты

В блоке параметров **Инструменты** вы можете просматривать и изменять параметры push-уведомлений и отправки журналов безопасности сети и аудита на сторонний Syslog-сервер.

Блок параметров **Инструменты** содержит следующие закладки:

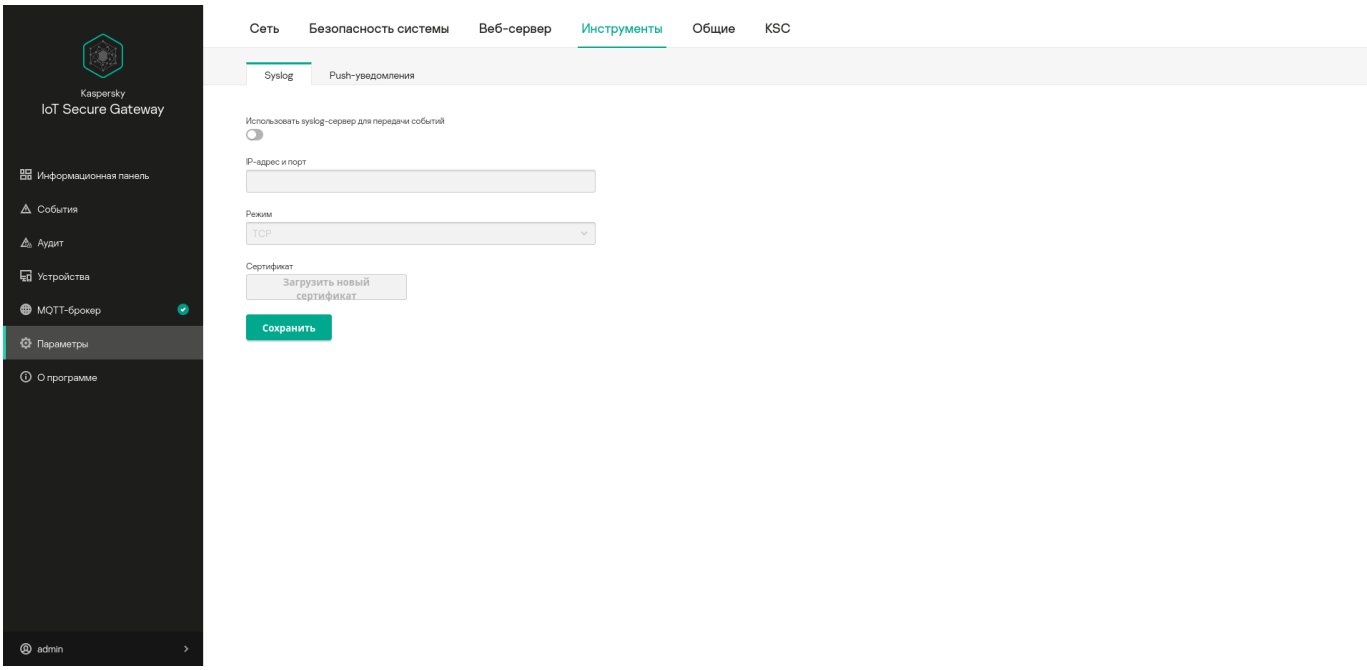
- **Syslog**.
- **Push-уведомления**.

Закладка Syslog

На закладке **Syslog** (см. рис. ниже) вы можете просматривать и изменять параметры отправки журналов с событиями безопасности сети и аудита безопасности системы на сторонний Syslog-сервер.

В основной части закладки **Syslog** отображаются следующие элементы:

- Поле **IP-адрес и порт**, содержащее IP-адрес и порт Syslog-сервера, на который отправляются журналы безопасности сети и аудита.
- Поле **Режим**, позволяющее выбрать протокол отправки журналов.
- Кнопка **Загрузить новый сертификат** для загрузки сертификата безопасности в программу.
- Кнопка **Сохранить** для сохранения параметров.



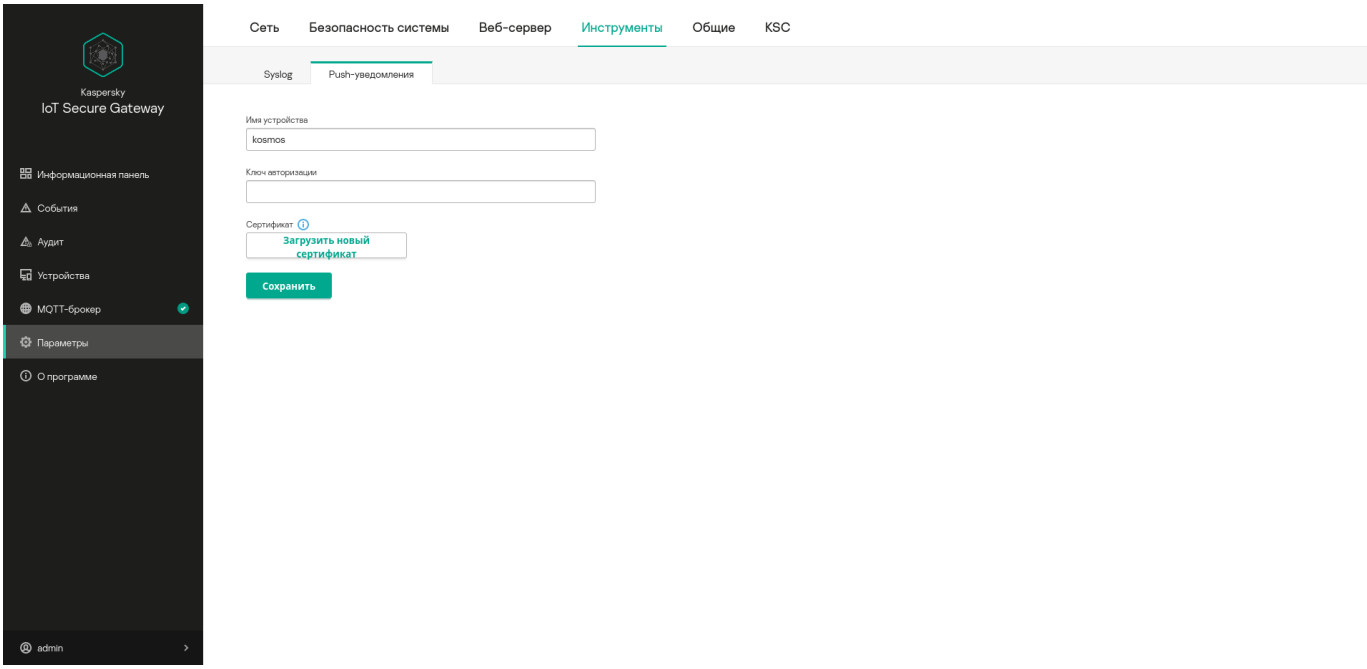
Блок параметров **Инструменты**. Закладка **Syslog**

Закладка Push-уведомления

На закладке **Push-уведомления** (см. рис. ниже) вы можете настраивать параметры отправки push-уведомлений на мобильный телефон.

В основной части закладки **Push-уведомления** отображаются следующие элементы:

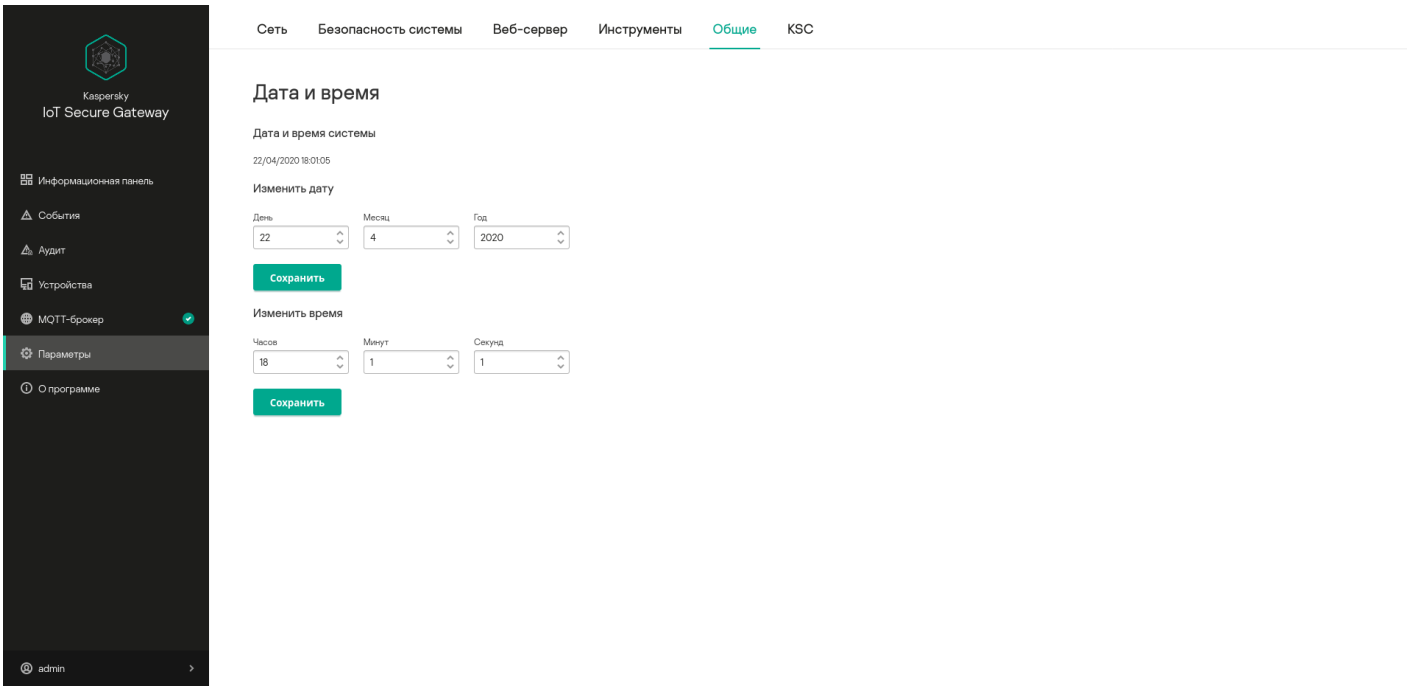
- Поле **Имя устройства**, содержащее имя устройства, на которое отправляются push-уведомления.
- Поле **Ключ авторизации**, содержащее ключ авторизации Firebase.
- Кнопка **Загрузить новый сертификат** для загрузки сертификата.
- Значок ⓘ, при наведении на который можно просмотреть информацию о загруженном сертификате.
- Кнопка **Сохранить** для сохранения имени устройства.



Блок параметров Общие

В блоке параметров **Общие** вы можете просматривать и изменять параметры даты и времени Kaspersky IoT Secure Gateway.

В блоке **Дата и время** (см. рис. ниже) отображаются текущие значения даты и времени, настроенные на Kaspersky IoT Secure Gateway.



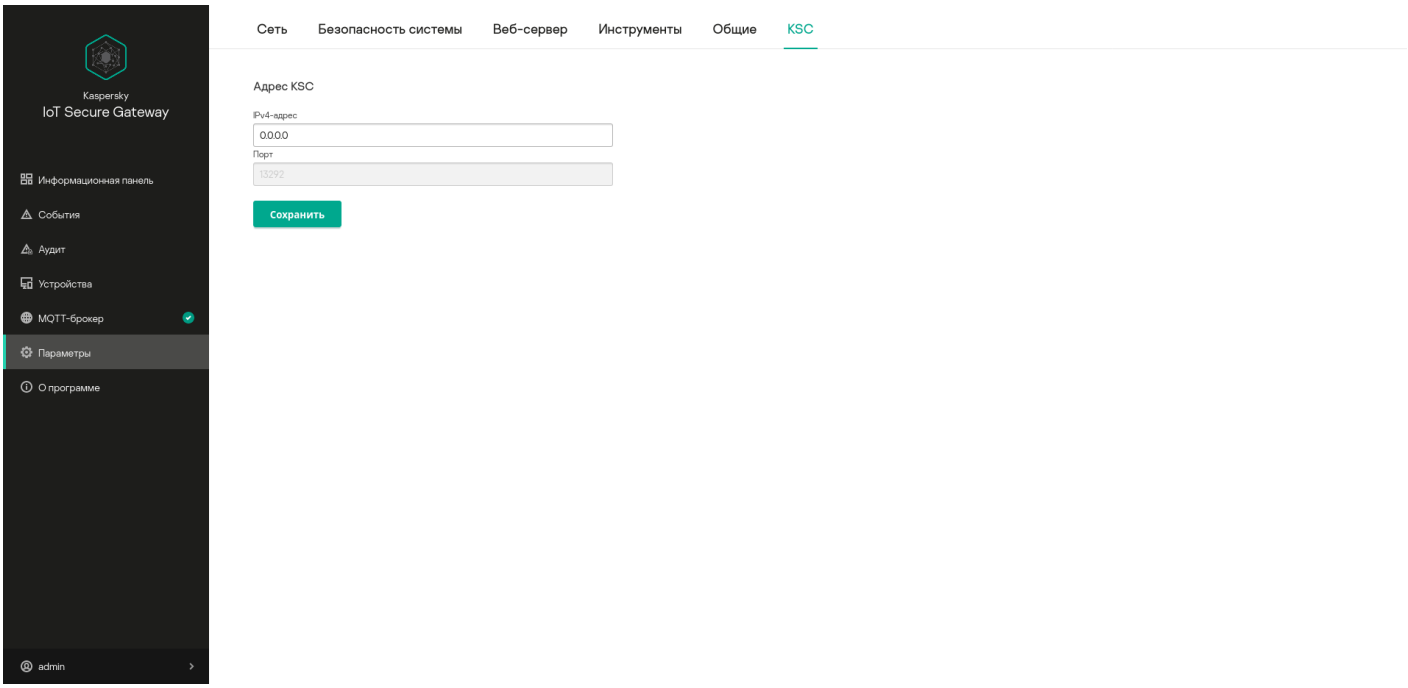
Блок параметров **Общие**

В блоках параметров **Изменить дату (UTC)** и **Изменить время (UTC)** располагаются поля, позволяющие указать текущие дату и время, а также кнопка **Сохранить**, позволяющая сохранить изменения.

Указывайте текущее время в часовом поясе UTC.

Блок параметров KSC

В блоке параметров **KSC** вы можете просматривать и изменять адрес сервера Kaspersky Security Center.



Блок параметров **KSC**

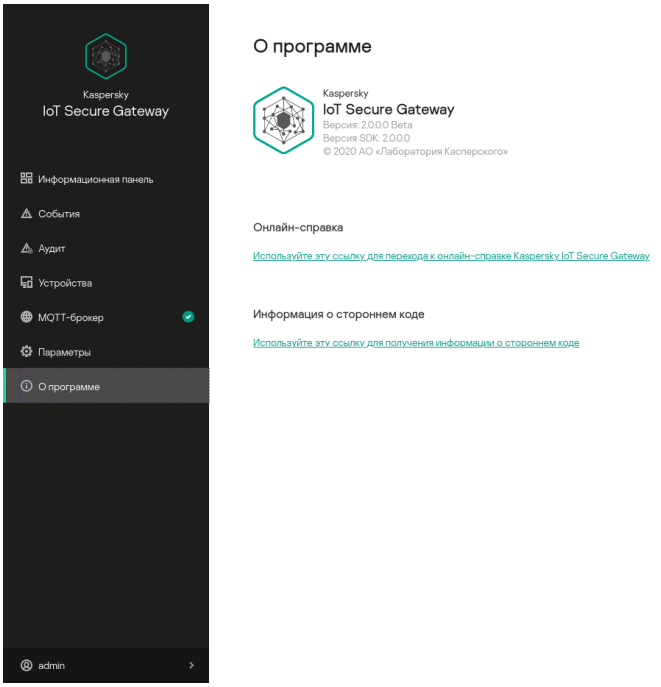
Эта закладка содержит поля для указания IP-адреса и порта сервера Kaspersky Security Center, а также кнопку **Сохранить**, позволяющую сохранить изменения.

Раздел О программе

В разделе **О программе** (см. рис. ниже) вы можете получить краткую информацию о версиях системы Kaspersky IoT Secure Gateway и операционной системы KasperskyOS.

В блоке **Онлайн-справка** вы можете открыть онлайн-справку по ссылке **Используйте эту ссылку для перехода к онлайн-справке Kaspersky IoT Secure Gateway**.

В блоке **Информация о стороннем коде** вы можете открыть файл legal_notices.txt с информацией о стороннем коде по ссылке **Используйте эту ссылку для получения информации о стороннем коде**.



Меню пользователя

Меню пользователя включает следующие элементы:

- **Изменить пароль** – открывает окно, в котором вы можете изменить пароль для входа в Kaspersky IoT Secure Gateway.
- **Язык** – позволяет переключаться между русским и английским языками.
- **Выйти** – выход из системы.

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.

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

- Имя учетной записи пользователя.
- IP-адреса, MAC-адреса и имена устройств, которые были обнаружены в сети.
- Журнал событий.
- Журнал аудита.
- Пользовательские сертификаты безопасности.
- Пользовательские параметры, указанные при настройке системы.

При каждом перезапуске системы журнал событий и список устройств удаляются. При повторном входе записи в журнал событий и список устройств ведутся с нуля. Все данные сертификатов хранятся в отдельно выделенном пространстве диска и шифруются.

При работе с Kaspersky IoT Secure Gateway, в файлах cookies сохраняется информация об идентификаторе сеанса, имени пользователя и последней посещенной странице веб-интерфейса (если сеанс был завершен автоматически по истечении 10 минут).

Если Kaspersky IoT Secure Gateway подключен к Kaspersky Security Center Web Console, он может сохранять и обрабатывать следующую информацию, не относящуюся к персональным данным:

- Параметры внутренней сети:
  - Включена ли автоматическая настройка параметров внутренней сети автоматически по протоколу DHCP.
  - IP-адрес Kaspersky IoT Secure Gateway во внутренней сети.
  - Маска подсети.
  - IP-адреса DNS-серверов.
  - MAC-адрес Kaspersky IoT Secure Gateway во внутренней сети.
  - Начальный и конечный IP-адреса диапазона адресов внутренней сети.
- Параметры внешней сети:
  - Включена ли автоматическая настройка параметров внешней сети по протоколу DHCP.
  - IP-адрес шлюза по умолчанию.
  - IP-адрес Kaspersky IoT Secure Gateway во внешней сети.
  - Маска подсети.

    - MAC-адрес Kaspersky IoT Secure Gateway во внешней сети.
    - IP-адреса DNS-серверов.
- Параметры правил межсетевого экрана:
    - Включено или выключено правило.
    - Действие, которое межсетевой экран должен выполнить над 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.
- Информация о системе предотвращения вторжений:
    - Включена ли система предотвращения вторжений.
    - Доступна ли служба предотвращения вторжений.
    - IP-адреса, занесенные в список запрещенных.
    - Идентификаторы сигнатур, по которым IP-адреса были занесены в список запрещенных.
    - IP-адреса, занесенные в список разрешенных.
- Параметры профилей MQTT-брокера:
    - Является ли профиль предустановленным.
    - Является ли профиль активным.
    - Имя профиля.
    - Параметры конфигурационных файлов и сертификатов MQTT: имя файла, тип и содержимое файла.
- Параметры профилей веб-сервера:
    - Является ли профиль предустановленным.
    - Является ли профиль активным.
    - Имя профиля.
- Параметры syslog-сервера:
    - Включена ли отправка событий на syslog-сервер.

    - IP-адрес syslog-сервера.
    - Порт syslog-сервера.
    - Режим отправки.
    - Параметры сертификата.
- Параметры push-уведомлений:
    - Имя устройства, на которое Kaspersky IoT Secure Gateway посылает push-уведомления.
    - Ключ аутентификации.
    - Параметры сертификата.
- Дату и время, установленные на Kaspersky IoT Secure Gateway.
- Политику паролей.
- Период синхронизации параметров между Kaspersky Security Center Web Console и Kaspersky IoT Secure Gateway.
- Команды, которые Kaspersky Security Center Web Console может послать Kaspersky IoT Secure Gateway.
- Включен ли маскарадинг.
- Адрес сервера обновлений.
- Информация о версии продукта.

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

Лицензирование Kaspersky IoT Secure Gateway

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

Настройка Kaspersky IoT Secure Gateway

Этот раздел содержит информацию о настройке Kaspersky IoT Secure Gateway.

Настройка параметров сети

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

Внешняя сеть – это сеть, через которую Kaspersky IoT Secure Gateway выходит в интернет.

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

Чтобы настроить параметры сети, выполните следующие действия:

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

   Откроется блок параметров **Сеть** в разделе **Параметры**.

2. На закладке **Глобальная сеть** настройте параметры внешней сети:

   - Если требуется настроить параметры сети автоматически по протоколу DHCP, включите переключатель **Автоматически (DHCP)**. По умолчанию переключатель **Автоматически (DHCP)** включен.

   - Если требуется настроить параметры сети вручную, выключите переключатель **Автоматически (DHCP)** и укажите следующие параметры:

     - В поле **IP-адрес** введите IP-адрес, который вы хотите назначить системе во внешней сети.

     - В поле **Маска подсети** введите маску подсети.

     - В поле **Шлюз по умолчанию** введите IP-адрес сетевого шлюза.

     - В поле **Адрес основного DNS-сервера** введите IP-адрес основного DNS-сервера.

     - В поле **Адрес дополнительного DNS-сервера** введите IP-адрес дополнительного DNS-сервера.

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

3. На закладке **Локальная сеть** настройте параметры внутренней сети:

   - Если требуется настроить параметры сети автоматически по протоколу DHCP, включите переключатель **Использовать DHCP-сервер**. По умолчанию переключатель **Использовать DHCP-сервер** включен.

   - Если требуется настроить параметры сети вручную, выключите переключатель **Использовать DHCP-сервер** и укажите следующие параметры:

     - В поле **IP-адрес** введите IP-адрес, который вы хотите назначить системе во внутренней сети.

     - В поле **Маска подсети** введите маску подсети.

- В поле **Адрес основного DNS-сервера** введите IP-адрес основного DNS-сервера.
- В поле **Адрес дополнительного DNS-сервера** введите IP-адрес дополнительного DNS-сервера.
- В поле **MAC-адрес** отображается MAC-адрес системы во внутренней сети.
- В поле **Начало диапазона адресов** введите IP-адрес начала диапазона адресов.
- В поле **Конец диапазона адресов** введите IP-адрес конца диапазона адресов.

4. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.
5. Перезагрузите Kaspersky IoT Secure Gateway, чтобы изменения параметров сети вступили в силу.

Управление политикой паролей

Kaspersky IoT Secure Gateway позволяет настраивать уровень сложности паролей для пользователей системы с помощью политики паролей.

Чтобы изменить политику паролей для новых пользователей системы, выполните следующие действия:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры**.
2. В разделе **Параметры** откройте блок параметров **Безопасность системы**.
3. В раскрывающемся списке **Профиль политики паролей** в блоке **Политика паролей** выберите необходимую политику: *Низкая надежность*, *Средняя надежность*, *Высокая надежность*. Каждой политике соответствуют предустановленные требования к сложности паролей, указанные под раскрывающимся списком.
4. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Изменение пароля пользователя

Чтобы сменить пароль вашей учетной записи, выполните следующие действия:

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

   Появится меню пользователя.
2. В меню пользователя выберите пункт **Изменить пароль**.

   Откроется окно для смены пароля. По ссылке **Текущая политика паролей** можно посмотреть текущую политику пароля.
3. В поле **Изменить пароль** введите текущий пароль вашей учетной записи.
4. В полях **Новый пароль** и **Повторите новый пароль** введите новый пароль.

   Текущую политику паролей можно посмотреть по ссылке **Текущая политика паролей**.

5. Нажмите на кнопку **Изменить**.

Настройка параметров MQTT-брокера

MQTT-брокер Eclipse Mosquitto обеспечивает работу Kaspersky IoT Secure Gateway по протоколу MQTT. 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.

Создание нового профиля MQTT-брокера

Чтобы создать новый профиль MQTT-брокера, выполните следующие действия:

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.

   Откроется панель **Создать профиль MQTT**.

3. В открывшемся окне выберите в раскрывающемся списке **Шаблон** профиль MQTT-брокера, на базе которого вы хотите создать новый профиль (конфигурационный файл Eclipse Mosquitto и сертификаты безопасности выбранного профиля добавятся в новый профиль) или оставьте **Пустой**, если хотите создать пустой профиль (пустой профиль нужно будет заполнить).

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

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

Заполнение пустого профиля MQTT-брокера

Чтобы заполнить пустой профиль, выполните следующие действия:

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

2. В таблице **Профили**, в графе **Имя** нажмите на значок ⊞ рядом с пустым профилем (профиль пустой, если вы создали его на базе шаблона **Пустой** и еще не заполняли. Профиль заполнен, если в нем отображается список конфигурационных файлов и сертификатов).

3. Нажмите на кнопку **Загрузить** в нижней части страницы.

   Откроется окно загрузки файла в систему.

4. В открывшемся окне выберите файл сертификата. Размер файла не должен превышать 131 КБ.

   Файл сертификата загрузится в систему и появится в профиле.

Профиль Eclipse Mosquitto 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.

5. Нажмите на кнопку **Создать файл**.

   Откроется панель **Создать конфигурационный файл MQTT**.

6. В открывшемся окне в раскрывающемся списке **Тип конфигурационного файла** выберите **Главный конфигурационный файл**.

7. В поле **Имя** введите имя нового конфигурационного файла латинскими буквами.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить конфигурационный файл Eclipse Mosquitto.

   Панель **Создать конфигурационный файл MQTT** закроется.

9. В таблице профиля нажмите на имя только что созданного конфигурационного файла.

   Откроется окно свойств конфигурационного файла.

10. В нижней части открывшегося окна нажмите на значок .

    Откроется окно текстового редактора для изменения конфигурационного файла.

11. Введите в окне текстового редактора требуемые параметры Eclipse Mosquitto.

    Более подробно о параметрах конфигурационного файла Eclipse Mosquitto можно узнать в документации на веб-сайте разработчика. Обратите внимание, что настройка MQTT-брокера Eclipse Mosquitto на Kaspersky IoT Secure Gateway доступна с ограничениями.

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

Изменение профиля MQTT-брокера

Чтобы изменить профиль MQTT-брокера, выполните следующие действия:

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

2. В таблице **Профили**, в графе **Имя** нажмите на значок рядом с профилем, который вы хотите изменить.

   Если профиль создавался на базе другого профиля, отобразится список конфигурационных файлов и сертификатов, входящих в профиль. Если создавался пустой профиль, то список файлов будет пустым – профиль нужно заполнить.

3. Нажмите на имя конфигурационного файла профиля.

   Откроется окно **Изменить конфигурационный файл MQTT**.

4. В нижней части открывшегося окна нажмите на значок .

   Откроется окно текстового редактора для изменения конфигурационного файла.

Более подробно о параметрах конфигурационного файла Eclipse Mosquitto можно узнать в документации на веб-сайте разработчика. Обратите внимание, что настройка MQTT-брокера Eclipse Mosquitto на Kaspersky IoT Secure Gateway доступна с ограничениями.

5. В окне текстового редактора измените параметры MQTT-брокера на те, которые требуются.
6. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

   Окно текстового редактора закроется.
7. Если требуется добавить в профиль сертификат безопасности, нажмите на кнопку **Загрузить** в нижней части страницы.

   Откроется окно загрузки файла в систему.
8. В открывшемся окне выберите файл сертификата.

   Файл сертификата загрузится в систему и появится в профиле.
9. Если требуется удалить из профиля сертификат безопасности, нажмите на имя этого сертификата в таблице **Профили**.

   Откроется окно свойств сертификата.
10. Нажмите на значок 🗑.
11. В открывшемся окне подтвердите удаление сертификата.

Переключение на другой профиль MQTT-брокера

Чтобы переключиться на другой профиль MQTT-брокера, выполните следующие действия:

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 **Изменить профиль MQTT**.
3. В нижней части открывшегося окна нажмите на кнопку **Сделать активным**.

В таблице **Профили** в графе **Активный** рядом с активным профилем появится значок ✔.

Ограничения при настройке MQTT-брокера

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

- В параметре `include_dir` можно указать только одну папку с конфигурационными файлами.
- Не допускается указание файловых путей с помощью параметров `capath` и `bridge_capath`.
- Параметр `log_dest stdout` выводит журнал MQTT с помощью API Kaspersky IoT Secure Gateway.
- Параметр `bridge_require_ocsp` не поддерживается.

- Параметры `persistence` и `websockets` не поддерживаются.
- Идентификатор клиента clientid должен быть указан явно (например, через `use_username_as_clientid`).
- Параметр `auth_plugin` не поддерживается.
- Аргументы параметра `ciphers` задаются в формате mbedtls, а не openssl.
- Параметры `log_dest file`, `pid_file` и `http_dir` не поддерживаются.

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.

Создание нового профиля веб-сервера

Чтобы создать новый профиль веб-сервера, выполните следующие действия:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры**.
2. В разделе **Параметры** выберите закладку **Веб-сервер**.

   Отобразится таблица, в которой перечислены профили веб-сервера.
3. Нажмите на кнопку **Создать** в нижней части страницы.

   Откроется панель **Создать профиль веб-сервера**.
4. В открывшейся панели выберите в раскрывающемся списке **Шаблон** профиль веб-сервера, на базе которого вы хотите создать новый профиль (конфигурационный файл CivetWeb и сертификат безопасности выбранного профиля добавятся в новый профиль) или оставьте **Пустой**, если хотите создать пустой профиль (пустой профиль нужно будет заполнить).
5. В поле **Имя** введите имя профиля латинскими буквами.
6. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Заполнение пустого профиля веб-сервера

Чтобы заполнить пустой профиль, выполните следующие действия:

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

2. В разделе **Параметры** выберите закладку **Веб-сервер**.

3. В таблице **Профили**, в графе **Имя** нажмите на значок ⊞ рядом с пустым профилем (профиль пустой, если вы создали его на базе шаблона **Пустой** и еще не заполняли. Профиль заполнен, если в нем отображается конфигурационный файл).

4. Нажмите на кнопку **Загрузить** в нижней части страницы.

   Откроется окно загрузки файла в систему.

5. В открывшемся окне выберите файл сертификата в формате PEM. Размер файла не должен превышать 131 КБ.

   Файл сертификата загрузится в систему и появится в профиле.

6. Нажмите на кнопку **Создать файл**.

   Откроется панель **Создать конфигурационный файл веб-сервера**.

7. В открывшемся окне в поле **Имя** введите имя нового конфигурационного файла латинскими буквами.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить конфигурационный файл CivetWeb.

   Панель **Создать конфигурационный файл веб-сервера** закроется.

9. В таблице профиля нажмите на имя только что созданного конфигурационного файла.

   Откроется панель **Изменить конфигурационный файл веб-сервера**.

10. В нижней части панели нажмите на значок ✎.

    Откроется окно текстового редактора для изменения конфигурационного файла.

11. Введите в окне текстового редактора параметры CivetWeb: `ssl_certificate <certificate name>`, где <certificate name> – имя файла сертификата, загруженного в пункте 5.

    > В текущей версии Kaspersky IoT Secure Gateway поддерживается только один параметр CivetWeb: ssl_certificate.

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

Изменение профиля веб-сервера

Чтобы изменить профиль веб-сервера, выполните следующие действия:

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

2. В разделе **Параметры** откройте блок параметров **Веб-сервер**.

3. В таблице **Профили**, в графе **Имя** нажмите на значок ⊞ рядом с профилем, который вы хотите изменить.

   Если профиль создавался на базе другого профиля, появится список файлов, входящих в профиль. Если создавался пустой профиль, то список файлов будет пустым – профиль нужно заполнить.

4. Нажмите на имя конфигурационного файла профиля.

   Откроется панель **Изменить конфигурационный файл веб-сервера**.

5. В нижней части открывшегося окна нажмите на значок .

   Откроется окно текстового редактора для изменения конфигурационного файла.

6. В окне текстового редактора измените параметры веб-сервера на те, которые требуются.

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

   Окно текстового редактора закроется.

8. Если требуется добавить в профиль сертификат безопасности, нажмите на кнопку **Загрузить** в нижней части страницы.

   Откроется окно загрузки файла в систему.

9. В открывшемся окне выберите файл сертификата.

   Файл сертификата загрузится в систему и появится в профиле.

10. Если требуется удалить из профиля сертификат безопасности, нажмите на имя этого сертификата в таблице **Профили**.

    Откроется окно свойств сертификата.

11. Нажмите на значок .

12. В открывшемся окне подтвердите удаление сертификата.

Переключение на другой профиль веб-сервера

Чтобы переключиться на другой профиль веб-сервера, выполните следующие действия:

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

2. В разделе **Параметры** выберите закладку **Веб-сервер**.

3. В таблице **Профили** в графе **Имя** нажмите на имя профиля, который вы хотите сделать активным.

   Откроется окно **Изменить профиль веб-сервера**.

4. В нижней части открывшегося окна нажмите на кнопку **Сделать активным**.

В таблице **Профили** в графе **Активный** рядом с активным профилем появится значок .

Настройка даты и времени

Чтобы настроить параметры даты и времени, выполните следующие действия:

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

   Откроется блок параметров **Сеть** в разделе **Параметры**.

2. В разделе **Параметры** откройте блок параметров **Общие**.

3. Настройте параметры даты. Для этого в блоке **Дата** с помощью раскрывающихся списков **День**, **Месяц** и **Год** укажите текущую дату.

4. Нажмите на кнопку **Сохранить** в блоке **Дата**, чтобы сохранить изменения.

5. Настройте параметры времени. Для этого в блоке **Время** с помощью раскрывающихся списков **Часы**, **Минуты**, **Секунды** укажите текущее время.

6. Нажмите на кнопку **Сохранить** в блоке **Время**, чтобы сохранить изменения.

Указывайте текущее время в часовом поясе UTC.

Мониторинг устройств

В разделе **Устройства** отображается информация об устройствах, которые система обнаружила в сети.

Система разделяет обнаруженные устройства на доверенные и недоверенные. Каждое новое устройство, обнаруженное системой в сети, считается недоверенным. Чтобы сделать устройство доверенным, нужно добавить его в список разрешенных.

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

Информация об обнаруженных устройствах сведена в таблицу, которая содержит следующие графы:

- **Имя** – имя устройства.
- **Тип** – тип устройства.
- **Статус** – статус устройства (*Неавторизованный* или *Авторизованный*).
- **MAC-адрес** – MAC-адрес устройства.
- **IP-адрес** – IP-адрес устройства.
- **Подробнее** – операционная система и производитель устройства, если удалось определить.

Если требуется, можно отсортировать таблицу устройств по любой из этих граф, нажав на заголовок графы.

В таблице отображаются устройства, обнаруженные системой на момент открытия раздела **Устройства**. Таблица устройств не обновляется автоматически.

Чтобы обновить список обнаруженных устройств,

в разделе **Устройства** нажмите на кнопку **Обновить** в верхней части страницы.

По умолчанию в таблице **Устройства** отображаются все неавторизованные устройства всех обнаруженных типов, а все кнопки в блоке **Тип** подсвечены синим цветом. Если переключатель **Белый список** включен, отображаются все авторизованные устройства.

Чтобы отфильтровать список выводимых устройств по типу устройства,

в разделе **Устройства** нажмите на кнопку с названием типа устройства в блоке **Тип**, расположенном над таблицей.

Устройства выбранного типа пропадут из таблицы **Устройства**, а кнопка с типом устройства отобразится без подсветки. Если требуется вернуть в таблицу устройства, отображение которых было отключено, нужно снова нажать на кнопку с названием этого типа устройства (кнопка снова станет подсвечена синим цветом).

Работа со списком разрешенных устройств

В списке разрешенных находятся авторизованные устройства.

Чтобы показать только устройства, входящие в список разрешенных, выполните следующие действия:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Устройства**.
2. В разделе **Устройства** включите переключатель **Белый список** в верхней части страницы.

Чтобы показать все неавторизованные устройства,

в разделе **Устройства** выключите переключатель **Белый список** в верхней части страницы.

Чтобы добавить устройство в список разрешенных, выполните следующие действия:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Устройства**.
2. Установите флажок напротив названия неавторизованного устройства, которое вы хотите добавить в список разрешенных.

   В правой части страницы откроется панель со значком устройства.
3. В открывшейся панели нажмите на кнопку **Добавить в белый список**.

Панель со значком устройства закроется. Устройство появится в списке разрешенных.

Чтобы удалить устройство из списка разрешенных, выполните следующие действия:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Устройства**.
2. Установите флажок напротив названия доверенного устройства, которое вы хотите удалить из списка разрешенных.

   В правой части страницы откроется панель со значком устройства.
3. В открывшейся панели нажмите на кнопку **Удалить из белого списка**.

Панель со значком устройства закроется. Устройство исчезнет из списка разрешенных.

Мониторинг событий

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 журналы безопасности сети и аудита через веб-интерфейс, а также передавать их на сторонний Syslog-сервер.

Kaspersky IoT Secure Gateway позволяет отправлять уведомления о произошедших событий с помощью технологии push и по протоколу MQTT.

Просмотр журнала безопасности сети

Kaspersky IoT Secure Gateway позволяет просматривать события безопасности сети, произошедшие в течение текущего сеанса подключения пользователя к системе через браузер. Эти события создаются компонентами системы. В графе **Компонент** для каждого события указано название компонента-источника (например, событие *Auth server. LoginError. Bad login or password* отправлено компонентом *Auth server* и говорит о том, что произошла попытка входа в систему с неверным именем учетной записи или паролем).

Чтобы просмотреть события безопасности сети,

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

Отобразится таблица с событиями безопасности сети.

*Чтобы отсортировать события в таблице раздела **События безопасности сети**, выполните следующие действия:*

- Для сортировки по названию сущности, зарегистрировавшей событие, нажмите на заголовок графы **Компонент**.
- Для сортировки по типу события, нажмите на заголовок графы **Событие**.
- Для сортировки по тексту события, нажмите на заголовок графы **Описание**.
- Для сортировки по дате и времени, нажмите на заголовок графы **Дата и время**.

Просмотр журнала аудита

Kaspersky IoT Secure Gateway сохраняет в журнале аудита события, связанные с безопасностью системы. Эти события создаются компонентами системы. В каждом событии указывается название компонента-источника.

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

Чтобы просмотреть журнал аудита,

в меню в левой части страницы веб-интерфейса выберите раздел **Аудит**.

Откроется раздел **Аудит безопасности системы**, в котором отображается таблица с событиями безопасности системы.

*Чтобы отсортировать события в таблице раздела **Аудит безопасности системы**, выполните следующие действия:*

- Для сортировки по важности события, нажмите на заголовок графы 🔥.
- Для сортировки по тексту события, нажмите на заголовок графы **Описание**.
- Для сортировки по названию сущности, зарегистрировавшей событие, нажмите на заголовок графы **Компонент**.
- Для сортировки по дате и времени, нажмите на заголовок графы **Дата и время**.

Чтобы сохранить журнал аудита на свой компьютер, выполните следующие действия:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Аудит**.
2. В разделе **Аудит безопасности системы** нажмите на кнопку **Загрузить**.

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

   Откроется окно, позволяющее сохранить журнал аудита в файл.
4. В открывшемся окне укажите путь сохранения файла журнала аудита.

   По умолчанию файл аудита сохраняется с именем audit.csv.
5. Сохраните файл.

Чтобы просмотреть информацию о параметрах аудита, выполните следующие действия:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Аудит**.
2. Наведите курсор мыши на значок ⓘ в верхней части окна.

   Откроется всплывающее окно со следующей информацией:

   - **Всего** – текущее количество записей в журнале аудита.
   - **Емкость** – максимальное количество записей в журнале аудита.
   - **Политика** – политика ведения журнала аудита:
     - *Круговая* – при переполнении журнала аудита новые записи будут перезаписывать старые.

- *Ограниченная* – при переполнении журнала аудита система остановится.

Отправка журналов событий на Syslog-сервер

Kaspersky IoT Secure Gateway может отправлять журналы событий безопасности сети и аудита на Syslog-сервер.

Чтобы настроить отправку журналов событий на Syslog-сервер, выполните следующие действия:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры**.
2. В разделе **Параметры** откройте блок параметров **Инструменты**.

   Откроется закладка **Syslog** в блоке параметров **Инструменты**.
3. Чтобы включить отправку журналов событий на Syslog-сервер, включите переключатель **Использовать syslog-сервер для передачи событий**.
4. Настройте параметры отправки журналов событий безопасности сети и аудита на сторонний Syslog-сервер. Для этого на закладке **Syslog** укажите следующие параметры:
   - В поле **IP-адрес и порт** введите IP-адрес и порт стороннего Syslog-сервера через двоеточие, 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 Syslog-сервер:
     - **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.
5. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Отправка push-уведомлений

Kaspersky IoT Secure Gateway отправляет push-уведомления о событиях с помощью Firebase™ Cloud Messaging (FCM) 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 4 секунды в топик /topics/DevicesandTopics, находящийся в облачной службе FCM.

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"
}
```

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

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"
  }
  ```

Чтобы получать push-уведомления, вы можете создать собственное приложение, работающее с FCM. Для этого вам понадобятся конфигурационный файл google-services.json и имя системы.

Чтобы настроить имя системы для отправки push-уведомлений, выполните следующие действия:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры**.
2. В разделе **Параметры** откройте закладку **Инструменты**.
3. Выберите закладку **Push-уведомления**.
4. В поле **Имя устройства** введите имя, под которым система будет отправлять push-уведомления.
5. В поле **Ключ авторизации** введите ключ авторизации Firebase.
6. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Более подробно о создании приложения для получения push-уведомлений, см. в документации Firebase Cloud Messaging.

Отправка MQTT-уведомлений

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

Чтобы настроить отправку MQTT-уведомлений, выполните следующие действия:

1. В меню в левой части страницы веб-интерфейса выберите раздел **MQTT-брокер**.
2. В таблице **Профили**, в графе **Имя** нажмите на значок ⊞ рядом с активным профилем.
3. Выберите конфигурационный файл профиля.

Откроется окно **Изменить конфигурационный файл MQTT**.

4. В нижней части открывшегося окна нажмите на значок .

   Откроется окно текстового редактора для изменения конфигурационного файла.

5. В окне текстового редактора добавьте параметры MQTT-брокера в начало файла.

   Система поддерживает следующие дополнительные параметры для настройки MQTT-уведомлений:

   - Параметр `kos_audit <значение>`. Если установлено значение `true`, Kaspersky IoT Secure Gateway отправляет события аудита по протоколу MQTT. Если установлено значение `false`, Kaspersky IoT Secure Gateway не отправляет события аудита по протоколу MQTT. По умолчанию установлено значение `true`.

   - Параметр `kos_event <значение>`. Если установлено значение `true`, Kaspersky IoT Secure Gateway отправляет события безопасности по протоколу MQTT. Если установлено значение `false`, Kaspersky IoT Secure Gateway не отправляет события безопасности по протоколу MQTT. По умолчанию установлено значение `false`.

   - Параметр `kos_audit_topic <Имя топика>`. Позволяет задать топик для отправки событий аудита. Параметр игнорируется, если для параметра `kos_audit` установлено значение `false`. По умолчанию установлено имя топика `SGW/audit`.

   - Параметр `kos_event_topic <Имя топика>`. Позволяет задать топик для отправки событий аудита. Параметр игнорируется, если для параметра `kos_event` установлено значение `false`. По умолчанию установлено имя топика `SGW/event`.

6. Если вы используете сетевой мост, настройте мэппинг топиков в разделе `Connection` конфигурационного файла. Более подробно о параметрах конфигурационного файла Eclipse Mosquitto можно узнать в документации на веб-сайте разработчика.

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

   Окно текстового редактора закроется.

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. Вы можете обновлять правила обнаружения вторжений, устанавливая обновления.

Дополнительно вы можете включить систему предотвращения вторжений Kaspersky IoT Secure Gateway (по умолчанию она выключена). Система предотвращения вторжений позволяет добавлять IP-адреса устройств в список разрешенных и запрещенных. В список запрещенных вы можете добавить IP-адреса устройств, в трафике которых была обнаружена подозрительная активность. Если система предотвращения вторжений выключена, события безопасности будут записываться в журнал безопасности.

Просмотреть список обнаруженных и заблокированных вторжений можно в журнале безопасности сети. Управлять параметрами компонента IPS можно через веб-плагин Kaspersky Security Center Web Console.

Мониторинг состояния Kaspersky IoT Secure Gateway

Вы можете следить за состоянием системы Kaspersky IoT Secure Gateway через веб-интерфейс. Этот раздел содержит инструкции по мониторингу состояния Kaspersky IoT Secure Gateway.

Просмотр информации о пользователях системы

В текущей версии Kaspersky IoT Secure Gateway существует только один пользователь – администратор системы.

Чтобы просмотреть информацию о пользователях системы, выполните следующие действия:

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

2. В разделе **Параметры** выберите закладку **Безопасность системы**.

   На закладке **Безопасность системы** в таблице в блоке **Пользователи** перечислены все пользователи системы.

Просмотр состояния компонентов

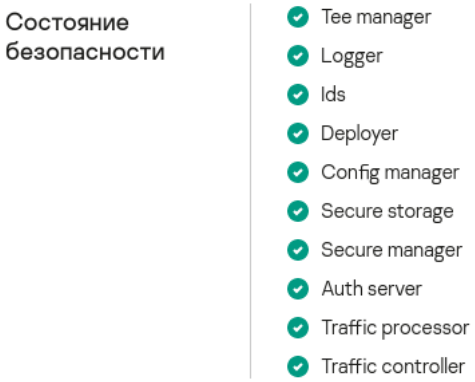
Kaspersky IoT Secure Gateway позволяет следить за состоянием безопасности компонентов системы.

Чтобы просмотреть состояние безопасности компонентов системы, выполните следующие действия:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Информационная панель**.

2. По ссылке **Показать** в блоке **Состояние безопасности** откройте список компонентов системы.

   Отобразится список компонентов системы. Слева от названия каждого компонента показывается его состояние безопасности (см. рис. ниже). По ссылке **Скрыть** можно закрыть список компонентов системы.



Состояние безопасности компонентов системы

Если рядом с названием хотя бы одного компонента отображается красный значок, обратитесь к сотруднику, ответственному за информационную безопасность в вашей организации.

Управление программой через Kaspersky Security Center Web Console

Kaspersky Security Center Web Console позволяет вам удаленно управлять работой программы Kaspersky IoT Secure Gateway. Используя возможности Kaspersky Security Center Web Console, вы можете:

- Настраивать параметры MQTT-брокера.
- Настраивать параметры сети.
- Управлять межсетевым экраном.
- Управлять системой обнаружения вторжений.
- Настраивать параметры веб-сервера.
- Настраивать отправку сообщений на syslog-сервер.
- Настраивать отправку push-уведомлений.
- Настраивать дату и время.
- Управлять политикой паролей.
- Настраивать параметры взаимодействия с Kaspersky Security Center Web Console.
- Перезагружать и обновлять Kaspersky IoT Secure Gateway.

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 с Kaspersky Security Center.

Веб-плагин позволяет централизованно выполнять следующие действия:

- Управлять параметрами Kaspersky IoT Secure Gateway.
- Получать события из Kaspersky IoT Secure Gateway.

Для взаимодействия Kaspersky IoT Secure Gateway и Kaspersky Security Center должны быть выполнены следующие условия:

- При настройке Kaspersky IoT Secure Gateway указаны параметры Kaspersky Security Center.
- В Kaspersky Security Center Web Console установлен плагин управления Kaspersky IoT Secure Gateway.

Установка веб-плагина управления Kaspersky IoT Secure Gateway

Веб-плагин по умолчанию не установлен в Kaspersky Security Center Web Console. Веб-плагин требуется установить на компьютер с установленной программой Kaspersky Security Center Web Console. При этом функции веб-плагина 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** → **Плагины**).

Чтобы установить веб-плагин в Kaspersky Security Center Web Console,

добавьте ZIP-архив с дистрибутивом веб-плагина, полученный вами в составе комплекта поставки, в Kaspersky Security Center Web Console. Подробнее о процессе добавления дистрибутива в Kaspersky Security Center Web Console см. в *онлайн-справке Kaspersky Security Center.*

Обратите внимание, что в качестве протокола взаимодействия между Kaspersky IoT Secure Gateway и Kaspersky Security Center используется "мобильный протокол". Убедитесь, что на сервере администрирования, на который установлен Kaspersky Security Center, доступен порт 13292, который требуется для подключения мобильных устройств. Подробнее об управлении мобильными устройствами см. раздел "Сценарий: Развертывание Управления мобильными устройствами" в *онлайн-справке Kaspersky Security Center 12*.

Вход и выход из Kaspersky Security Center Web Console

Чтобы войти в Kaspersky Security Center Web Console, вам нужно получить у администратора веб-адрес Сервера администрирования и номер порта, указанные во время установки (по умолчанию используется порт 8080). Так же требуется включить JavaScript в браузере.

Чтобы войти в Kaspersky Security Center Web Console, выполните следующие действия:

1. В браузере перейдите по адресу `<Веб-адрес Сервера администрирования>:<Номер порта>`.

   Откроется страница входа.

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

   Если Сервер администрирования 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. Можно следовать инструкциям учебника или закрыть его соответствующей кнопкой (X).

Вы можете переходить по страницам Kaspersky Security Center Web Console и работать с ней. Дополнительная информация о работе Kaspersky Security Center Web Console приведена в *онлайн-справке Kaspersky Security Center*.

Чтобы выйти из Kaspersky Security Center Web Console, выполните следующие действия:

1. В правом верхнем углу экрана щелкните по вашему имени пользователя.

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

   Kaspersky Security Center Web Console закроется и отобразится страница входа.

Настройка отображения событий в Kaspersky Security Center Web Console

Чтобы события, происходящие на устройстве, на котором установлен Kaspersky IoT Secure Gateway, отображались в Kaspersky Security Center Web Console, нужно перенести это устройство в группу управляемых устройств и создать политику для этого устройства.

Чтобы настроить отображение событий в Kaspersky Security Center Web Console, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания политики.
3. В списке **Выберите программу** выберите Kaspersky IoT Secure Gateway и нажмите **Далее**.
4. Нажмите на кнопку **Сохранить**.
5. В главном окне Kaspersky Security Center Web Console выберите **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.
6. Установите флажок рядом с именем устройства.
7. Нажмите на кнопку **Переместить в группу**.

   Появится панель **Переместить в группу**.
8. Установите флажок рядом с группой администрирования **Управляемые устройства**.
9. Нажмите на кнопку **Переместить**.

Устройство будет перемещено в группу управляемых устройств, и вы сможете просматривать события, происходящие на этом устройстве.

Чтобы просмотреть события, произошедшие на устройстве, 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.

   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**.

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

Вы можете настроить параметры Kaspersky IoT Secure Gateway через веб-плагин для Kaspersky Security Center Web Console.

Настройка параметров MQTT-брокера через Kaspersky Security Center Web Console

Kaspersky Security Center Web Console позволяет создавать новые профили MQTT-брокера, изменять существующие профили и переключаться между профилями.

Создание нового профиля MQTT-брокера через Kaspersky Security Center Web Console

Чтобы создать новый профиль MQTT-брокера через Kaspersky Security Center Web Console, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   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. Нажмите на кнопку **Добавить** над списком профилей MQTT-брокера.

   Откроется окно **Изменить профиль**.

8. В раскрывающемся списке **Статус** выберите одно из следующих значений:

   - **Активный**, если вы хотите сделать новый профиль активным. В этом случае конфигурации из профиля загружаются в MQTT-брокер и активируется доступ к сертификатам из профиля для брокера. Только один профиль может быть активным.

   - **Неактивный**, если вы не хотите делать новый профиль активным.

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

10. Если вы хотите добавить конфигурационный файл или сертификат к новому профилю, выполните следующие действия:

    a. В области **Список файлов** нажмите на кнопку **Добавить**.

    Откроется панель загрузки файлов.

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

    c. Нажмите на кнопку **Загрузить файл**.

    Откроется окно загрузки файла в систему.

    d. В открывшемся окне выберите конфигурационный файл или сертификат. Размер файла не должен превышать 131 КБ.

    Файл загрузится в систему и появится в профиле.

    e. Нажмите на кнопку **OK** в нижней части панели.

    Панель загрузки файлов закроется.

11. Нажмите на кнопку **OK** в нижней части окна **Изменить профиль**.

    Окно **Изменить профиль** закроется.

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

Изменение профиля MQTT-брокера через Kaspersky Security Center Web Console

Чтобы изменить профиль MQTT-брокера через Kaspersky Security Center Web Console, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   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 списке профилей MQTT-брокера выберите профиль, который вы хотите изменить.

8. Нажмите на кнопку **Изменить** над списком профилей MQTT-брокера.

Откроется окно **Изменить профиль**.

9. Измените параметры профиля на те, которые требуются:

   - Чтобы поменять параметры активного профиля:

     a. В раскрывающемся списке **Статус** выберите **Неактивный**.

     b. Нажмите на кнопку **OK** в нижней части окна **Изменить профиль**.

     Окно **Изменить профиль** закроется.

     c. Выполните шаги этой инструкции заново, начиная с шага 7.

   - В неактивном профиле вы можете менять любые параметры.

10. Нажмите на кнопку **OK** в нижней части окна **Изменить профиль**.

    Окно **Изменить профиль** закроется.

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

Удаление профиля MQTT-брокера через Kaspersky Security Center Web Console

Если вы удалите все профили, то функционал MQTT-брокера будет отключен, но Kaspersky IoT Secure Gateway продолжит работу.

Чтобы удалить профиль MQTT-брокера через Kaspersky Security Center Web Console, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   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 списке профилей MQTT-брокера выберите профиль, который вы хотите удалить.

8. Нажмите на кнопку **Удалить** над списком профилей MQTT-брокера.

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

Настройка параметров сети через Kaspersky Security Center Web Console

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

Вы можете настроить сеть с помощью веб-интерфейса Kaspersky IoT Secure Gateway или через Kaspersky Security Center Web Console.

Чтобы настроить параметры сети через Kaspersky Security Center Web Console, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   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**.

7. В разделе **Сеть**, выберите закладку **LAN**.

8. Настройте параметры внутренней сети:

   - Если вы хотите настроить параметры внутренней сети автоматически по протоколу DHCP, включите переключатель **Автоматически (DHCP)**.

   - Если вы хотите настроить параметры внутренней сети вручную, выполните следующие действия:

     - В поле **IP-адрес** введите IP-адрес, который вы хотите назначить системе во внутренней сети.

     - В поле **Маска подсети** введите маску подсети.

     - 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.

     - В поле **Начало диапазона адресов** введите IP-адрес начала диапазона адресов.

- В поле **Конец диапазона адресов** введите IP-адрес конца диапазона адресов.

9. Нажмите на кнопку **Сохранить**.

10. В разделе **Сеть**, выберите закладку **WAN**.

11. Настройте параметры внешней сети:

    - Если вы хотите настроить параметры внешней сети автоматически по протоколу DHCP, включите переключатель **Автоматически (DHCP)**.

    - Если вы хотите настроить параметры внешней сети вручную, 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.

12. Нажмите на кнопку **Сохранить**.

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 следующих протоколов:

- TCP.
- UDP (только IPv4).

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

Служебные правила разрешают следующие соединения Kaspersky IoT Secure Gateway:

- исходящие соединения к серверу Kaspersky Security Center Web Console по протоколу TCP;
- исходящие соединения к серверу обновлений по протоколам TCP, UDP, TCP / TLS;
- входящие соединения к локальному веб-серверу по протоколу HTTPS;
- исходящее соединение к серверу 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.

Создание правил межсетевого экрана

Чтобы создать новое правило межсетевого экрана, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".
3. Откроется окно свойств компьютера.
4. Выберите закладку **Программы**.
5. Нажмите на название Kaspersky IoT Secure Gateway.
6. Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.
7. Выберите закладку **Параметры программы**.
8. Выберите раздел **Сеть**.
9. Выберите закладку **Межсетевой экран**.
10. Нажмите на кнопку **Добавить** над списком правил межсетевого экрана.

    Появится панель добавления правила межсетевого экрана.
11. Укажите параметры нового правила:
    - В раскрывающемся списке **Статус** выберите должно ли быть включено правило:

- **Включено**.

  Правило включено.

- **Выключено**.

  Правило выключено.

- В раскрывающемся списке **Действие** выберите действие, которое межсетевой экран должен выполнять над трафиком, попадающим под правило:

  - **Accept**.

    Разрешить прохождение трафика.

  - **Deny**.

    Запретить прохождение трафика.

- В раскрывающемся списке **Область** выберите область, к которой должно применяться правило:

  - **LAN**.

    Правило применяется к трафику, проходящему из внутренней сети во внешнюю.

  - **WAN**.

    Правило применяется к трафику, проходящему из внешней сети во внутреннюю.

- В поле **IP-адрес (источник)** укажите IP-адрес источника трафика.

- В поле **Порт (источник)** укажите порт источника трафика, если этот параметр применим к протоколу.

- В поле **IP-адрес (получатель)** укажите IP-адрес цели трафика.

- В поле **Порт (получатель)** укажите порт цели трафика, если этот параметр применим к протоколу.

- В раскрывающемся списке **Протокол** выберите используемый протокол.

12. Нажмите на кнопку **Сохранить**.

Пользовательские правила межсетевого экрана выполняются в заданном в Kaspersky Security Center Web Console порядке сверху вниз, до первого совпадения. О том, как изменить порядок пользовательских правил межсетевого экрана см. раздел "Изменение порядка правил межсетевого экрана".

Изменение правил межсетевого экрана

Чтобы изменить правило межсетевого экрана, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

Откроется окно свойств компьютера.

3. Выберите закладку **Программы**.

4. Нажмите на название Kaspersky IoT Secure Gateway.

5. Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.

6. Выберите закладку **Параметры программы**.

7. Выберите раздел **Сеть**.

8. Выберите закладку **Межсетевой экран**.

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

10. Нажмите на кнопку **Изменить** над списком правил межсетевого экрана.

    Появится панель изменения правила межсетевого экрана.

11. Измените параметры правила на те, которые требуются.

12. Нажмите на кнопку **Сохранить**.

Изменение порядка правил межсетевого экрана

Чтобы поднять или опустить правило межсетевого экрана, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   Откроется окно свойств компьютера.

3. Выберите закладку **Программы**.

4. Нажмите на название Kaspersky IoT Secure Gateway.

5. Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.

6. Выберите закладку **Параметры программы**.

7. Выберите раздел **Сеть**.

8. Выберите закладку **Межсетевой экран**.

9. Установите флажок напротив правила, которое вы хотите поднять или опустить.

10. Выполните одно из следующих действий:

    - Если вы хотите поднять правило межсетевого экрана, нажмите на кнопку **Вверх**.

- Если вы хотите опустить правило межсетевого экрана, нажмите на кнопку **Вниз**.

11. Нажмите на кнопку **Сохранить**.

Удаление правил межсетевого экрана

Чтобы удалить правило межсетевого экрана, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   Откроется окно свойств компьютера.

3. Выберите закладку **Программы**.

4. Нажмите на название Kaspersky IoT Secure Gateway.

5. Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway.

6. Выберите закладку **Параметры программы**.

7. Выберите раздел **Сеть**.

8. Выберите закладку **Межсетевой экран**.

9. Выберите правило, которое вы хотите удалить.

10. Нажмите на кнопку **Удалить** над списком правил межсетевого экрана.

    Правило будет удалено.

11. Нажмите на кнопку **Сохранить**.

Управление системой предотвращения вторжений

Kaspersky IoT Secure Gateway может выполнять анализ и фильтрацию проходящего трафика с помощью встроенной системы предотвращения вторжений. Для обнаружения вторжений Kaspersky IoT Secure Gateway использует базу сигнатур, которая обновляется при перепрошивке устройства. При обнаружении совпадения с сигнатурой из базы Kaspersky IoT Secure Gateway автоматически блокирует трафик с IP-адреса, с которого произведена атака.

По умолчанию система предотвращения вторжений отключена.

Чтобы включить систему предотвращения вторжений, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   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**.

7. Выберите закладку **IPS**.

8. Установите переключатель в верхней части окна в положение **Система предотвращения вторжений включена**.

9. Нажмите на кнопку **Сохранить**.

Чтобы включить список запрещенных, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   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**.

7. Выберите закладку **IPS**.

8. Нажмите на кнопку **Показать список** напротив заголовка **Черный список**.

   Откроется страница **Черный список**.

9. Установите переключатель в положение **Черный список включен**.

10. Нажмите на кнопку **Сохранить**.

Чтобы добавить IP-адрес в список разрешенных, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   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**.

7. Выберите закладку **IPS**.

8. Нажмите на кнопку **Показать список** напротив заголовка **Белый список**.

   Откроется страница **Белый список**.

9. Нажмите на кнопку **Добавить**.

   Откроется страница **Изменить**.

10. В поле **IP-адрес (источник)** укажите IP-адрес, трафик с которого вы хотите разрешить.

11. Нажмите на кнопку **Сохранить**.

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 применяет правила в следующем порядке:

1. Разрешающие служебные правила межсетевого экрана.

2. Список разрешенных.

3. Список запрещенных.

4. Пользовательские правила межсетевого экрана.

5. Запрещающие служебные правила межсетевого экрана.

Работа с веб-сервером через Kaspersky Security Center Web Console

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".

Просмотр профилей веб-сервера

Чтобы просмотреть список профилей веб-сервера, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   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**.
7. Выберите закладку **Веб-сервер**.

Вы увидите список созданных профилей веб-сервера.

Настройка syslog

Kaspersky IoT Secure Gateway включает в себя syslog-клиент, с помощью которого вы можете отправлять syslog-сообщения о событиях на устройствах в вашей сети на syslog-сервер. Управление syslog-клиентом осуществляется через Kaspersky Security Center Web Console.

Чтобы настроить отправку syslog-сообщений на syslog-сервер, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   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**.
7. Выберите закладку **Syslog**.
8. Установите переключатель в верхней части окна в положение **Syslog включен**.

9. Укажите параметры syslog-сервера:
   - В поле **IP-адрес** укажите IP-адрес syslog-сервера.
   - В поле **Порт** укажите порт.
   - В выпадающем списке выберите **Режим** один из вариантов:
     - **UPD**.
     - **TCP**.
     - **TLS**.
10. Нажмите на кнопку **Загрузить сертификат**.

    Откроется окно загрузки файла в систему.
11. В открывшемся окне выберите сертификат.

    Файл загрузится в систему и появится в профиле.
12. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Чтобы удалить сертификат, выполните следующие действия:

1. Под описанием сертификата, который вы хотите удалить, нажмите кнопку **Удалить сертификат**.
2. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Настройка push-уведомлений через Kaspersky Security Center Web Console

Kaspersky IoT Secure Gateway может отправлять push-уведомления на авторизованные устройства. Вы можете авторизировать ваши устройства через Kaspersky Security Center Web Console.

Чтобы включить отправку push-уведомлений на устройство, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   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**.

7. Выберите закладку **Push-уведомления**.

8. В поле **Имя устройства** введите имя, под которым система будет отправлять push-уведомления.

9. В поле **Ключ авторизации** введите код авторизации Firebase.

10. Нажмите на кнопку **Загрузить сертификат**.

    Откроется окно загрузки файла в систему.

11. В открывшемся окне выберите сертификат.

    Файл загрузится в систему и появится в профиле.

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

Настройка даты и времени

Чтобы настроить дату и время, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   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**.

7. Выберите закладку **Время**.

8. В блоке **Дата** укажите дату системы.

9. В блоке **Время** укажите время системы.

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

Указывайте текущее время в часовом поясе UTC.

Настройка политики паролей

Чтобы изменить политику паролей для новых пользователей системы через Kaspersky Security Center Web Console, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   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**.

7. Выберите закладку **Политика паролей**.

8. В раскрывающемся списке **Профиль политики паролей** необходимую политику: **Низкая надежность**, **Средняя надежность**, **Высокая надежность**.

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

Настройка параметров синхронизации с Kaspersky Security Center

Чтобы настроить время синхронизации с Kaspersky Security Center, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   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**.

7. Выберите закладку **KSC: Синхронизация.**

8. В раскрывающемся списке **Период синхронизации** выберите интервал, через который Kaspersky IoT Secure Gateway синхронизируется с Kaspersky Security Center.

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

Настройка маскарадинга

Маскарадинг (англ. Masquerading) – тип трансляции сетевого адреса, при которой адрес отправителя подставляется динамически, в зависимости от назначенного интерфейсу адреса.

Чтобы включить маскарадинг, 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   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**.

7. Выберите закладку **NAT**.

8. Установите переключатель настройки маскарадинга в нужное вам положение:

   - **Маскарадинг включен**, если нужно включить маскарадинг.

   - **Маскарадинг выключен**, если нужно выключить маскарадинг.

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

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

Перезагрузка и обновление программного обеспечения

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

Чтобы обновить 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   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**.

7. Выберите закладку **KSC: Команды**.

8. Выберите закладку **Обновление**.

9. В поле **Адрес сервера обновлений** укажите адрес, где находится пакет обновлений для Kaspersky IoT Secure Gateway, в формате https://<ip-адрес сервера>/путь_к_пакету_обновлений (например, https://10.10.100.10/update.pkg).

10. В раскрывающемся списке **Команда** выберите **Обновление**.

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

    Обновления Kaspersky IoT Secure Gateway будут загружены.

Чтобы 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 вы не видите имя компьютера в списке, добавьте его в группу **Управляемые устройства** как описано в разделе "Настройка отображения событий в Kaspersky Security Center Web Console".

   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**.

7. Выберите закладку **KSC: Команды**.

8. В раскрывающемся списке **Команда** выберите **Перезагрузка**.

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

   Kaspersky IoT Secure Gateway будет перезагружен.

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 в веб-интерфейсе. Страница 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 под учетной записью.

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.

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.

Безопасный шлюз Интернета вещей

Система, которая обеспечивает безопасную передачу пользовательского трафика между датчиками и платформой Интернета вещей.

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).

Политика паролей

Функция, реализующая определенное правило задания сложности новых паролей.

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.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном на 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.

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.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

JavaScript – зарегистрированный товарный знак Oracle Corporation и / или ее аффилированных компаний.