kaspersky

Kaspersky IoT Secure Gateway 1000

© 2024 АО "Лаборатория Касперского"

Содержание

Справка Kaspersky IoT Secure Gateway 1000

Что нового

Узнайте, что нового в этой версии Kaspersky IoT Secure Gateway 1000.

Обновление

Как обновить версию Kaspersky IoT Secure Gateway 1000.

Аппаратные и программные требования

Проверьте требования к Kaspersky IoT Secure Gateway 1000 и к компонентам системы.

Управление приложениями

Как скачать, установить, запустить, остановить, настроить правила запуска и удалить приложение в Kaspersky IoT Secure Gateway 1000.

Управление сертификатами приложений в Kaspersky Security Center 14.2 Web Console.

Управление маршрутизацией между приложениями в Kaspersky Security Center 14.2 Web Console.

Начало работы

Как подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.

Как настроить Kaspersky IoT Secure Gateway 1000 для начала работы.

Как настроить доступ из внешней сети к устройствам внутренней сети.

Как настроить параметры Kaspersky IoT Secure Gateway 1000.

Основные возможности

Как настроить функцию маскарадинга.

Как настроить адресную трансляцию через Kaspersky Security Center 14.2 Web Console

Как настроить маршрутизацию.

Как настроить маршрутизацию через Kaspersky Security Center 14.2 Web Console.

Управление сетевым экраном.

Мониторинг

Как просмотреть сводную информацию о состоянии Kaspersky IoT Secure Gateway 1000.

Как просмотреть журналы событий аудита Kaspersky IoT Secure Gateway 1000.

Как скачать журнал событий приложений, установленных в Kaspersky IoT Secure Gateway 1000.

Как просмотреть события Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console.

Дополнительные возможности

Управление учетными записями в Kaspersky IoT Secure Gateway 1000.

Как просмотреть страницу диагностики неисправностей.

Как перезагрузить Kaspersky IoT Secure Gateway 1000.

О Kaspersky IoT Secure Gateway 1000

Kaspersky IoT Secure Gateway 1000 (далее также "система") представляет собой кибериммунную систему на базе операционной системы KasperskyOS с предварительно настроенным набором прикладного программного обеспечения. Kaspersky IoT Secure Gateway 1000 устанавливается на встраиваемый компьютер модели Kraftway Рубеж-H и предназначена для работы в качестве безопасного шлюза Интернета вещей (Internet of Things) в сети организации.

Kaspersky IoT Secure Gateway 1000 выполняет следующие функции:

- Получает, проверяет и распределяет сообщения датчиков и других устройств, передаваемые по протоколу MQTT.
- Регистрирует события аудита сетевого экрана и аудита операционной системы.
- Обеспечивает кибербезопасность устройства.
- Блокирует или разрешает трафик от IP-адресов устройств в соответствии с правилами сетевого экрана.
- Может работать в качестве DHCP-сервера и преобразователя сетевых адресов (NAT).

Kaspersky IoT Secure Gateway 1000 поставляется с предустановленным приложением Kaspersky IoT Secure Gateway Network Protector, которое обеспечивает функционал сетевого экрана на уровне промышленных протоколов. Приложение может контролировать и фильтровать сетевой трафик промышленных протоколов от IP-адресов в соответствии с правилами анализа содержимого сетевых пакетов, создавая запрещающие правила для IP-адресов. Правила анализа содержимого сетевых пакетов поставляются в комплекте Kaspersky IoT Secure Gateway 1000. Также приложение позволяет создавать и применять разрешающие правила для прохождения трафика от конкретных IP-адресов.

Вы можете управлять Kaspersky IoT Secure Gateway 1000 через локальный веб-интерфейс или удаленно с помощью веб-плагина для Kaspersky Security Center 14.2 Web Console.

Комплект поставки

В комплект поставки Kaspersky IoT Secure Gateway 1000 входят следующие файлы:

- Установочный образ Kaspersky IoT Secure Gateway 1000. Файл образа имеет имя вида kisg-<тип сетевого устройства>-<номер версии системы>_ru_en.tar.gz, где <тип сетевого устройства> может быть `diode` для однонаправленного шлюза или `router` для сетевого роутера, <номер версии системы> имеет вид четырех разделенных точками десятичных чисел, например: `1.2.3.4`.

  Kaspersky IoT Secure Gateway 1000 поставляется с предустановленным приложением Kaspersky IoT Secure Gateway Network Protector.
- Скрипт для создания загрузочного образа Kaspersky IoT Secure Gateway 1000.
- Архив с установочным образом веб-плагина для Kaspersky Security Center 14.2 Web Console и файлом подписи: WEB_Plugin_KISG_<номер версии системы>.zip.
- Файлы сертификатов:
  - TlsClientAdmin.p12 – архив, который содержит сертификат администратора и его закрытый ключ.
  - TlsClientUser.p12 – архив, который содержит сертификат пользователя и его закрытый ключ.

- CaCert.crt – корневой сертификат, которым подписаны сертификаты администратора и пользователя.

Предоставляемые по умолчанию файлы сертификатов могут использоваться только для первого подключения к веб-интерфейсу, после которого администратору необходимо обновить сертификаты.

- Файл с информацией о стороннем коде (Legal Notices).
- Онлайн-справка.
- Информация о версии (Release Notes).

Аппаратные и программные требования

USB-разъемы встраиваемого компьютера Kraftway Рубеж-Н могут быть использованы только для подключения клавиатуры и мыши при первоначальной настройке Kaspersky IoT Secure Gateway 1000 или загрузочного USB при установке Kaspersky IoT Secure Gateway 1000. Подключение других устройств к встраиваемым компьютерам через USB-разъемы не предусмотрено.

Требования к Kaspersky IoT Secure Gateway 1000 и аппаратной платформе

Система Kaspersky IoT Secure Gateway 1000 может быть установлена только на встраиваемый компьютер модели Kraftway Рубеж-Н.

Подключение к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 осуществляется с компьютера администратора сети или пользователя.

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

- Google™ Chrome™ версии 118 и выше.
- Mozilla™ Firefox™ версии с 118 по 123. Версии 124 и выше не поддерживаются.

Требования к компонентам Kaspersky Security Center

Для подключения к Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console в локальной сети организации должна быть установлена программа Kaspersky Security Center версии 14.2.

Для работы Kaspersky IoT Secure Gateway 1000 требуются следующие компоненты Kaspersky Security Center:

- Сервер администрирования Kaspersky Security Center 14.2.
- Kaspersky Security Center 14.2 Web Console.

Kaspersky Security Center и Kaspersky Security Center 14.2 Web Console не поставляются в комплекте поставки Kaspersky IoT Secure Gateway 1000, их требуется установить отдельно.

Сведения об установке компонентов Kaspersky Security Center см. в онлайн-справке Kaspersky Security Center.

Типовая схема развертывания Kaspersky IoT Secure Gateway 1000

Типовая схема развертывания Kaspersky IoT Secure Gateway 1000 предполагает установку системы на границе сегментов сетей, чтобы предоставить возможность задать набор правил фильтрации трафика. Администратор может управлять системой и следить за ее состоянием из внутренней сети через веб-интерфейс Kaspersky IoT Secure Gateway 1000 и с помощью веб-плагина Kaspersky Security Center 14.2 Web Console.

Основные сценарии обеспечивают работу Kaspersky IoT Secure Gateway 1000 в качестве типов сетевого устройства *однонаправленный шлюз* и *сетевой роутер*.

Типовая схема развертывания для типа устройства однонаправленный шлюз

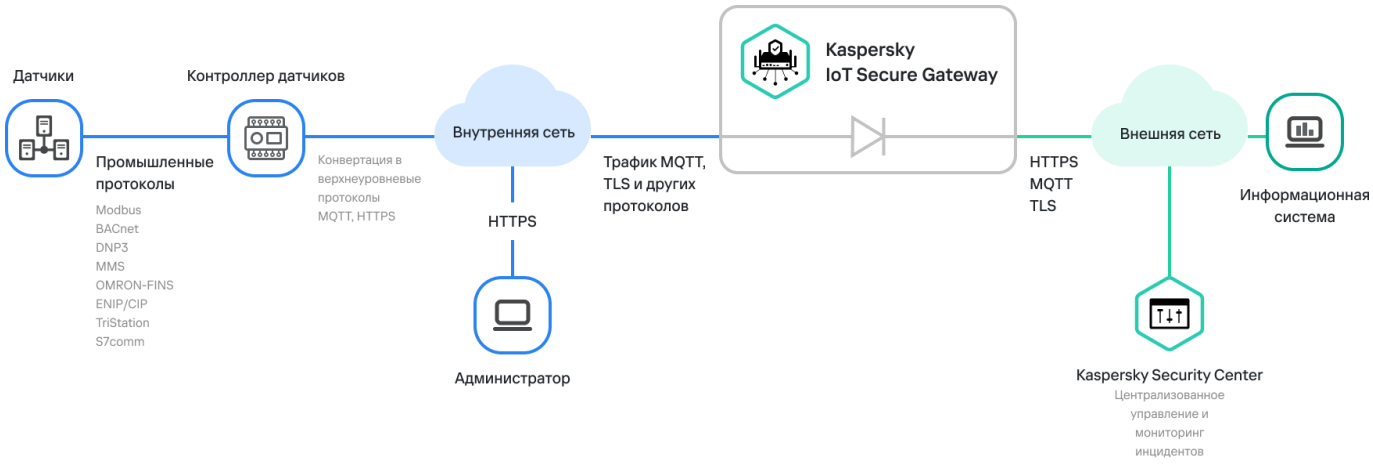
Типовая схема развертывания Kaspersky IoT Secure Gateway 1000 в качестве типа устройства однонаправленный шлюз (см. рис. ниже) предполагает следующее:

1. Устройство представляет собой программный однонаправленный шлюз.
2. Сетевые стеки, относящиеся к внутренней и внешней сетям, разделены на уровне процессов.
3. Передача данных между внутренней и внешней сетями возможна только через специальный программный интерфейс MessageConsumer.

   Он обеспечивает однонаправленную передачу телеметрической информации (промышленных протоколов) из внутренней сети к информационным системам во внешней сети. Для обеспечения конфиденциальности передаваемой информации используется протокол TLS.

   Программный интерфейс MessageConsumer реализован в следующих приложениях:

   - Message Sender для обработки трафика из внутренней сети;
   - Message Receiver для обработки трафика во внешней сети.
4. Приложение Message Sender подключено к внутренней сети.
5. Приложение Kaspersky IoT Secure Gateway Network Protector подключено только к внутренней сети.

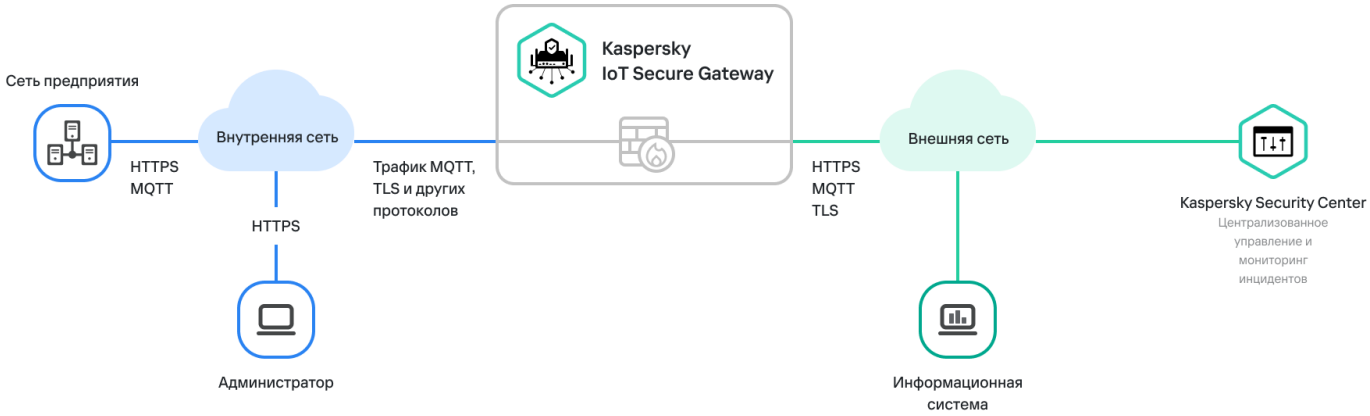


Типовая схема развертывания Kaspersky IoT Secure Gateway 1000 для типа сетевого устройства однонаправленный шлюз

Типовая схема развертывания для типа устройства сетевой роутер

Типовая схема развертывания Kaspersky IoT Secure Gateway 1000 в качестве типа устройства сетевой роутер (см. рис. ниже) предполагает следующее:

1. Устройство представляет собой сетевой маршрутизатор.
2. Единый сетевой стек отвечает за маршрутизацию трафика между сетевыми интерфейсами и обеспечивает возможность использовать для передачи сообщений MQTT-брокер (Eclipse Mosquitto™), работающий во внутренней и внешней сетях.
3. Приложение Kaspersky IoT Secure Gateway Network Protector подключено ко внешней и внутренней сетям.



Типовая схема развертывания Kaspersky IoT Secure Gateway 1000 для типа сетевого устройства сетевой роутер

Подсистемы Kaspersky IoT Secure Gateway 1000

Kaspersky IoT Secure Gateway 1000 включает в себя подсистемы, которые обеспечивает работу ее функционала. Каждая подсистема состоит из *компонентов*, которые обеспечивают выполнение отдельных функций Kaspersky IoT Secure Gateway 1000.

Kaspersky IoT Secure Gateway 1000 включает следующие подсистемы:

- *Подсистема общих компонентов* включает ядро микроядерной операционной системы KasperskyOS, предоставляющее минимальную функциональность, включая планирование исполнения программ, управление памятью и вводом-выводом, а также обеспечивает и контролирует взаимодействие всех процессов и компонентов системы, содержит политики безопасности и обеспечивает загрузку динамическим библиотек.
- *Драйверы* обеспечивают взаимодействие операционной системы KasperskyOS с разъемами, устройствами и платами аппаратной платформы.
- *Файловая система* содержит набор исполняемых файлов, библиотек и файлов описаний, позволяющих использовать файловые системы и/или сетевой стек, вынесенные в отдельный процесс VFS (Virtual File System, рус. виртуальная файловая система). Подробное описание VFS представлено в справке *KasperskyOS Community Edition*.
- *BootControl* обеспечивает управление процессами загрузки Kaspersky IoT Secure Gateway 1000.
- *WebServer* обеспечивает работу веб-интерфейса Kaspersky IoT Secure Gateway 1000 и функционала аутентификации администратора и пользователя.

- *IdsProxy* обеспечивает взаимодействие с приложением Kaspersky IoT Secure Gateway Network Protector и получение уведомлений от него.
- *ApplicationsPlatform* обеспечивает управление приложениями, в том числе скачивание, установку и удаление приложений, а также работу с сертификатами и разрешениями.
- *Notifiers* обеспечивает отправку событий Kaspersky IoT Secure Gateway 1000 по протоколу MQTT (Message Queuing Telemetry Transport) и на сторонний сервер Syslog по протоколу Syslog.
- *Troubleshooting* обеспечивает работу утилит диагностики Kaspersky IoT Secure Gateway 1000 и выводит информацию о результатах диагностики на странице диагностики неисправностей.
- *Kaspersky Security Center* (плагин) обеспечивает централизованное управление Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console.
- *Update* обеспечивает обновление Kaspersky IoT Secure Gateway 1000, в том числе скачивание, проверку и установку обновлений.
- *NetworkManagement* обеспечивает управление и работу внутренней и внешней сети (в том числе с использованием сотового соединения через модем), сетевого экрана, а также работу DHCP-сервера и DHCP-клиента.
- *Events/Audit* обеспечивает хранение событий аудита сетевого экрана и аудита операционной системы.
- *MQTTbroker* обеспечивает функциональность MQTT-брокера Eclipse Mosquitto.

  Эта подсистема функционирует только для типа сетевого устройства *сетевой роутер*.

- *Log* обеспечивает управление журналами Kaspersky IoT Secure Gateway 1000.
- *SelfTesting* обеспечивает функционал самотестирования и проверки целостности Kaspersky IoT Secure Gateway 1000 и компонентов, а также создания резервной копии и восстановления операционной системы.

Рекомендации по обеспечению безопасной работы Kaspersky IoT Secure Gateway 1000

Для обеспечения безопасной работы Kaspersky IoT Secure Gateway 1000, рекомендуется ограничить и контролировать доступ к оборудованию, на котором работает программа.

Физическая безопасность оборудования

При внедрении Kaspersky IoT Secure Gateway 1000 на предприятии рекомендуется принять следующие меры по обеспечению безопасной работы:

- Ограничить доступ в помещение, в котором расположено оборудование с установленной программой, а также к сетевому оборудованию выделенной сети. Доступ в помещение должен предоставляться только доверенным лицам, например персоналу, обладающему полномочиями по установке и настройке программы.

- Обеспечить контроль физического доступа к оборудованию, на котором работает программа, с помощью технических средств или службы охраны. Проводить мониторинг доступа в контролируемые помещения с помощью средств охранной сигнализации.

- Осуществлять видеонаблюдение в контролируемых помещениях.

Информационная безопасность

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

- Обеспечить защиту трафика внутри интранет-системы.

- Обеспечить первичную настройку Kaspersky IoT Secure Gateway 1000 только в контролируемом контуре.

- Использовать цифровые сертификаты, изданные доверенными центрами сертификации. При компрометации сертификатов рекомендуется их обновить.

- Завершать сеанс подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 при завершении работы пользователя в веб-браузере. Для принудительного завершения сеанса подключения в веб-браузере нужно использовать пункт **Выход** в меню пользователя.

Что нового

В Kaspersky IoT Secure Gateway 1000 версии 3.0 появились следующие возможности и доработки:

- Пограничные вычисления (англ. edge computing) – добавлена функциональность, обеспечивающая возможность работать с приложениями, включая запуск приложений в изолированной среде и управление ими, управление сертификатами приложений и маршрутизацией данных между приложениями.

  Использование сторонних приложений по обработке данных позволяет расширить функционал Kaspersky IoT Secure Gateway 1000.

- Однонаправленный шлюз – Kaspersky IoT Secure Gateway 1000 может работать в качестве сетевого устройства типа однонаправленный шлюз для создания однонаправленного потока данных и команд.

- Переадресация портов (англ. port forwarding или destination NAT) – добавлена функциональность адресной трансляции, которая обеспечивает устройствам, расположенным во внешней сети, доступ к ресурсам во внутренней сети по отдельным портам.

- Фильтрация прикладных протоколов – добавлена функциональность фильтрации трафика для сетевого экрана, позволяющая блокировать сетевые соединения на основании используемого в них прикладного протокола.

- Приложение Kaspersky IoT Secure Gateway Network Protector – добавлено приложение, обеспечивающее контроль промышленных данных (анализ и фильтрацию аномального трафика на уровне промышленных протоколов), в том числе на основании передаваемых команд.

  Приложение Kaspersky IoT Secure Gateway Network Protector предустановлено в Kaspersky IoT Secure Gateway 1000.

- Сетевой кластер – добавлена функциональность, позволяющая объединить несколько шлюзов в отказоустойчивую сетевую конфигурацию, где один шлюз является основным, а остальные – дублирующими на случай отказа основного.

- Маршрутизация - добавлена возможность настройки маршрутизации для управления сетевыми пакетами, проходящими через устройство с Kaspersky IoT Secure Gateway 1000.

  Эта функциональность доступна только для типа сетевого устройства *сетевой роутер*.

- Двухфакторная аутентификация – подключение к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 осуществляется в два этапа: с использованием сертификата и с использованием учетных данных (имени и пароля).

- Ролевая модель – Kaspersky IoT Secure Gateway 1000 поддерживает две роли учетной записи: администратор и пользователь. В зависимости от роли учетная запись имеет доступ к разному набору функционала, параметров и данных Kaspersky IoT Secure Gateway 1000.

  В Kaspersky IoT Secure Gateway 1000 может быть только одна учетная запись администратора и одна учетная запись пользователя.

- Самотестирование и контроль целостности - добавлена функциональность, позволяющая запускать самотестирование ключевых подсистем для мониторинга работоспособности функций безопасности, а также проводить контроль целостности файлов системы и установленных приложений.

- Скачивание приложений из веб-портала Kaspersky Appicenter for Developers - добавлена функциональность, позволяющая скачивать и устанавливать в Kaspersky IoT Secure Gateway 1000 приложения, загруженные на веб-портал Kaspersky Appicenter for Developers.

- Поддержка аппаратной платформы Kraftway Рубеж-Н – Kaspersky IoT Secure Gateway 1000 может быть установлена на встраиваемый компьютер Kraftway Рубеж-Н.

- Обновление Kaspersky IoT Secure Gateway 1000 – обновление Kaspersky IoT Secure Gateway 1000 осуществляется с серверов обновлений "Лаборатории Касперского".

- Просмотр страницы диагностики неисправностей – расширена функциональность, позволяющая получать дополнительную информацию о работе Kaspersky IoT Secure Gateway 1000 и выполнять диагностику неисправностей Kaspersky IoT Secure Gateway 1000.

- Переработан и улучшен функционал подсистемы аудита.

- Добавлена поддержка ключевых сценариев настройки и управления устройством через веб-интерфейс Kaspersky IoT Secure Gateway 1000.

- Добавлен API для разработки VPN-клиента.

- Удалена поддержка функционала обнаружения и анализа проходящего трафика (IPS). Функционал блокировки проходящего трафика обеспечивается приложением Kaspersky IoT Secure Gateway Network Protector.

- Удалена поддержка обнаружения устройств.

- Обновлен веб-интерфейс Kaspersky IoT Secure Gateway 1000.

Включение и выключение устройства Kraftway Рубеж-Н

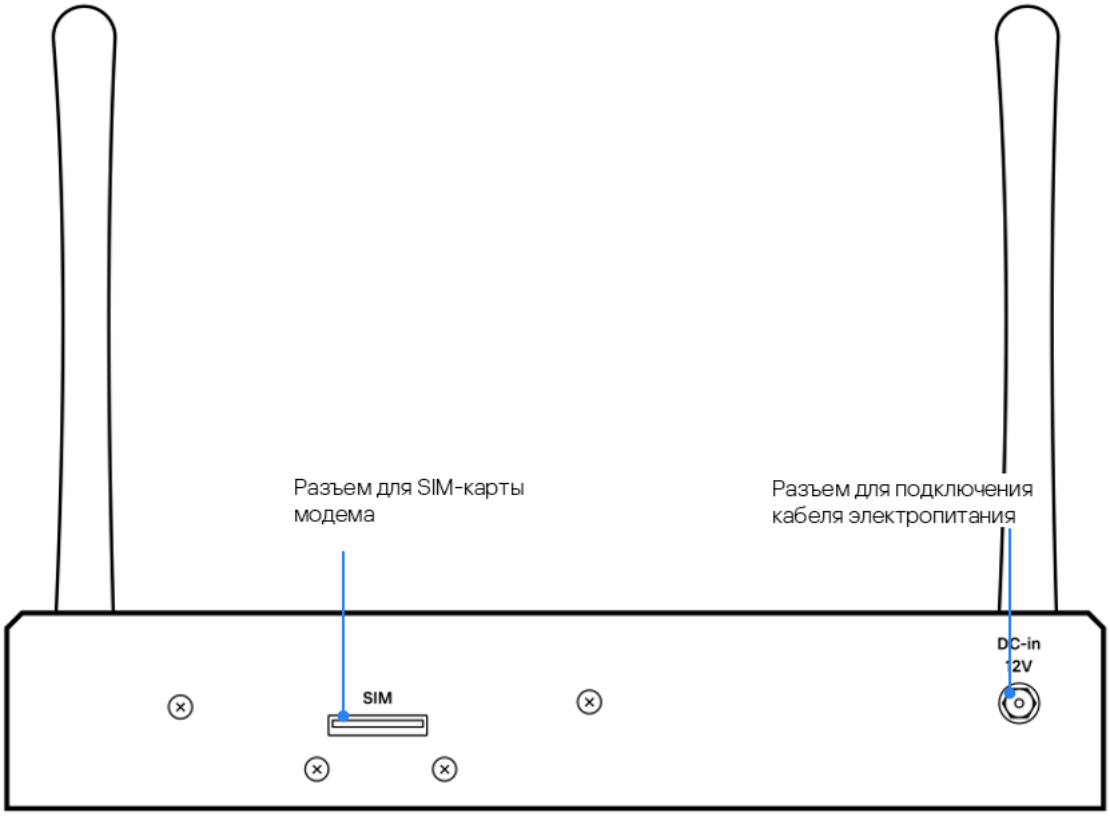
Прежде, чем начать работу с Kaspersky IoT Secure Gateway 1000, требуется подключить устройство Kraftway Рубеж-Н к сети и включить.

Подготовку к установке и установку Kaspersky IoT Secure Gateway 1000 выполняют специалисты "Лаборатории Касперского".

После первого включения Kaspersky IoT Secure Gateway 1000 рекомендуется настроить сеть, создать и загрузить сертификат администратора, настроить дату и время и изменить сертификат веб-сервера на используемый в вашей организации.

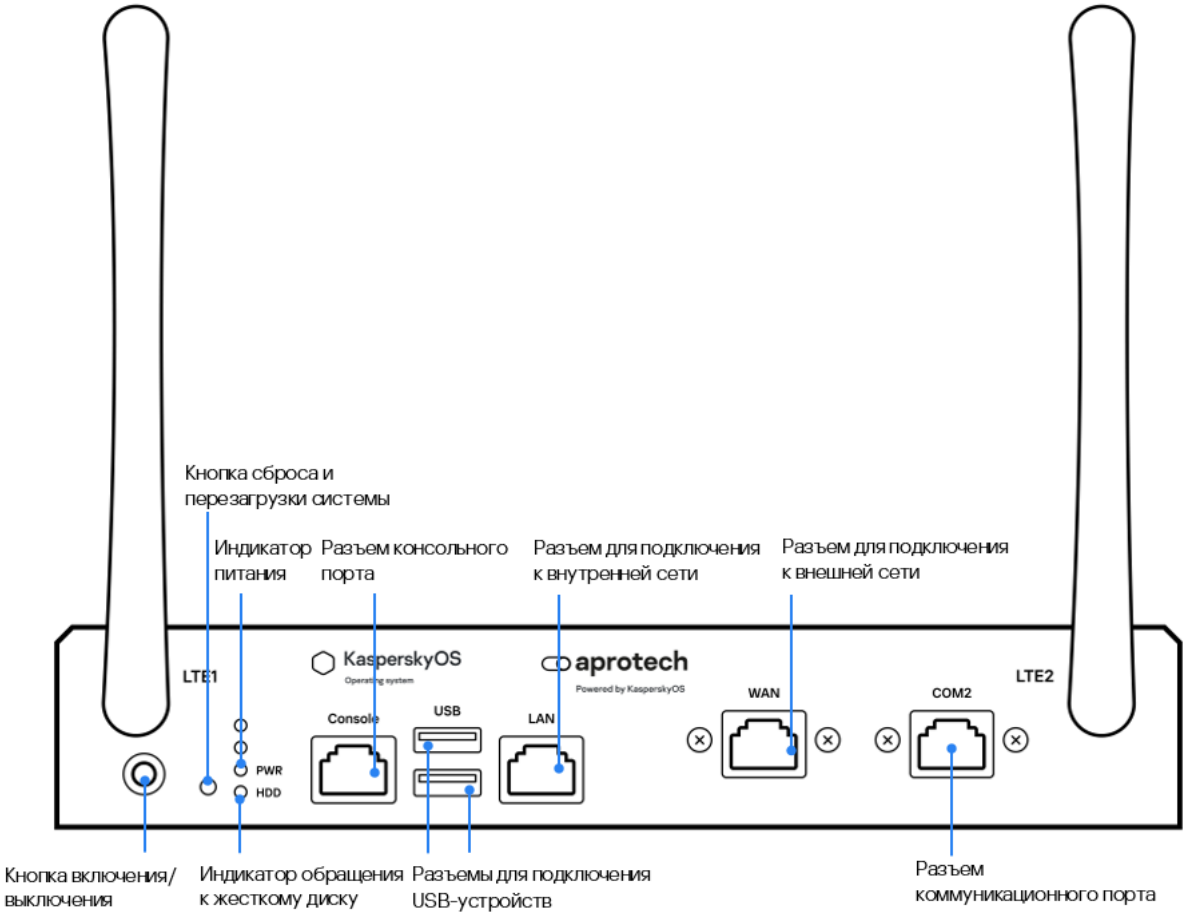
Чтобы включить устройство Kraftway Рубеж-Н:

1. Подсоедините кабель электропитания к разъему на задней панели Kraftway Рубеж-Н (см. рис. ниже).



Разъем для подключения кабеля электропитания на задней панели Kraftway Рубеж-Н

2. Подсоедините сетевой кабель, ведущий во внешнюю сеть, к разъему для подключения к внешней сети на лицевой панели Kraftway Рубеж-Н (см. рис. ниже).



Лицевая панель Kraftway Рубеж-H

3. Если требуется включить устройство Kraftway Рубеж-H, нажмите на кнопку включения/выключения в левой части лицевой панели.

   Kraftway Рубеж-H включится, Kaspersky IoT Secure Gateway 1000 запустится автоматически.

4. Если требуется выключить устройство Kraftway Рубеж-H, завершите сеанс подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 и нажмите на кнопку включения/выключения в левой части лицевой панели.

   Kraftway Рубеж-H выключится.

Подключение к веб-интерфейсу Kaspersky IoT Secure Gateway 1000

Вы можете подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 с использованием любого поддерживаемого браузера. Браузер должен быть установлен на компьютере, который имеет доступ к Kaspersky IoT Secure Gateway 1000 через внутреннюю сеть. Kaspersky IoT Secure Gateway 1000 поставляется со статически настроенным IP-адресом – 192.168.1.1. По умолчанию в Kaspersky IoT Secure Gateway 1000 включен DHCP-сервер, поэтому при подключении вашего компьютера к сети, к которой подключен Kaspersky IoT Secure Gateway 1000 через внутренний сетевой разъем, ваш компьютер получит IP-адрес автоматически.

Подключение к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 осуществляется с помощью двухфакторной аутентификации, для которой требуются следующие данные:

- Имя и пароль учетной записи.

  Имя и пароль учетной записи администратора для *первого подключения* к веб-интерфейсу вы можете найти в инструкции по первому подключению ниже. Эти учетные данные являются временными и изменяются администратором после первого входа в веб-интерфейс.

- Сертификат администратора или пользователя.

  Сертификаты для *первого подключения* администратора к веб-интерфейсу загружены в Kaspersky IoT Secure Gateway 1000 по умолчанию. После первого подключения, администратору необходимо обновить эти сертификаты.

Сертификат администратора или пользователя также используется для создания безопасного соединения между Kaspersky IoT Secure Gateway 1000 и браузером, который используется для подключения. Архив с сертификатом для первого подключения администратора к веб-интерфейсу входит в комплект поставки. Администратору необходимо загрузить этот архив в браузер перед первым подключением к Kaspersky IoT Secure Gateway 1000. После обновления сертификатов, администратору и пользователю также необходимо загружать новые сертификаты в браузер.

В зависимости от вашей роли в системе (администратор или пользователь) вам нужно выполнить различные шаги для подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.

При подключении к Kaspersky IoT Secure Gateway 1000 одновременно возможна только одна активная сессия. Если администратор подключится к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 во время активной сессии пользователя, сессия подключения пользователя будет завершена. Пользователь также не сможет подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 во время активной сессии администратора.

Администратор

Перед подключением к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 убедитесь, что у вас есть USB-накопитель или токен с действительным сертификатом.

В зависимости от того, подключаетесь вы к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 в первый раз или повторно, вы можете подключиться одним из следующих способов:

- **Первое подключение к веб-интерфейсу Kaspersky IoT Secure Gateway 1000**

Чтобы в первый раз подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway 1000:

1. Подключите USB-накопитель с архивом TlsClientAdmin.p12, содержащим сертификат администратора, к компьютеру, с которого вы хотите подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.

   Архив TlsClientAdmin.p12 для первого подключения к веб интерфейсу входит в комплект поставки.

2. Загрузите сертификат из архива TlsClientAdmin.p12 в браузер. Информацию о том, как загрузить архив с сертификатом в браузер вы можете найти в документации браузера.

   Для загрузки сертификата в браузер потребуется пароль. Пароль от сертификата по умолчанию: **adminadmin**.

3. Откройте браузер и в адресной строке введите IP-адрес веб-интерфейса Kaspersky IoT Secure Gateway 1000 – https://192.168.1.1.

   Откроется страница входа в Kaspersky IoT Secure Gateway 1000.

4. Введите имя и пароль по умолчанию и нажмите на кнопку **Продолжить**.

   Имя пользователя для первого входа в веб-интерфейс: **admin**.

   Пароль для первого входа в веб-интерфейс: **adminadmin**.

   Эти учетные данные являются временными и необходимы только для первого подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000. Вам потребуется изменить их на следующем шаге.

5. В открывшемся окне изменения учетных данных введите новые имя и пароль и нажмите на кнопку **Сохранить**.

   Пароль должен содержать 8 и более различных неповторяющихся символов. Данные вашей учетной записи будут обновлены, и откроется страница веб-интерфейса Kaspersky IoT Secure Gateway 1000.

После первого подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 администратору необходимо обновить сертификаты и создать учетную запись пользователя.

- **Повторное подключение к веб-интерфейсу Kaspersky IoT Secure Gateway 1000**

Чтобы повторно подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway 1000:

1. Если для доступа к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 используется USB-токен:
   - Убедитесь, что на компьютере, с которого осуществляется доступ, установлено программное обеспечение, поставляемое для поддержки работы с токеном.
   - Убедитесь, что токен подключен к компьютеру, с которого осуществляется доступ.
2. Если USB-токен *не используется*, убедитесь, что в браузер загружен архив с сертификатом администратора, необходимым для создания безопасного соединения. Информацию о том, как загрузить архив с сертификатом в браузер вы можете найти в документации браузера.
3. Откройте браузер и в адресной строке введите IP-адрес веб-интерфейса Kaspersky IoT Secure Gateway 1000 – https://192.168.1.1.
4. Если для доступа к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 используется USB-токен:
   a. В открывшемся окне выбора сертификата выберите сертификат, расположенный на USB-токене и нажмите на кнопку **OK**.
   b. Введите пароль от токена.

   Если USB-токен *не используется*, пропустите этот шаг.
5. Введите имя и пароль и нажмите на кнопку **Продолжить**.

   Если вы несколько раз введете неверные данные учетной записи, система будет временно заблокирована (время блокировки по умолчанию составляет пять минут). По истечении времени блокировки вы сможете повторить попытку.

При успешном подключении в окне браузера откроется страница веб-интерфейса Kaspersky IoT Secure Gateway 1000.

Пользователь

Перед подключением к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 выполните следующие действия:

- Убедитесь, что у вас есть USB-накопитель или токен с действительным сертификатом пользователя.
- Запросите ваши имя пользователя и пароль у администратора (при первом подключении или после истечения срока действия данных вашей учетной записи).

Вы можете подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 только после того, как администратор создаст вашу учетную запись пользователя.

Чтобы подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway 1000:

1. Если для доступа к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 используется USB-токен:
   - Убедитесь, что на компьютере, с которого осуществляется доступ, установлено программное обеспечение, поставляемое для поддержки работы с токеном.

- Убедитесь, что токен подключен к компьютеру, с которого осуществляется доступ.

2. Если USB-токен *не используется*, убедитесь, что в браузер загружен архив с сертификатом пользователя, необходимым для создания безопасного соединения. Информацию о том, как загрузить архив с сертификатом в браузер вы можете найти в документации браузера.

3. Откройте браузер и в адресной строке введите IP-адрес веб-интерфейса Kaspersky IoT Secure Gateway 1000 – https://192.168.1.1.

4. Если для доступа к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 используется USB-токен:

   a. В открывшемся окне выбора сертификата выберите сертификат, расположенный на USB-токене и нажмите на кнопку **OK**.

   b. Введите пароль от токена.

   Если USB-токен *не используется*, пропустите этот шаг.

5. Введите имя и пароль и нажмите на кнопку **Продолжить**.

   Если вы несколько раз введете неверные данные учетной записи, система будет временно заблокирована (время блокировки по умолчанию составляет пять минут). По истечении времени блокировки вы сможете повторить попытку.

При успешном подключении в окне браузера откроется страница веб-интерфейса Kaspersky IoT Secure Gateway 1000.

Завершение и возобновление сеанса подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000

В целях безопасности в Kaspersky IoT Secure Gateway 1000 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 1000 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 по умолчанию составляет пять минут. В течение этого времени система может предоставить доступ к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 без повторного запроса сертификата и ввода имени пользователя и пароля, если для повторного подключения используются те же компьютер и браузер. При необходимости администратор может изменить время действия незавершенного сеанса.

Чтобы завершить сеанс подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000:

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

   В окне браузера отобразится страница входа в Kaspersky IoT Secure Gateway 1000.

Также в целях безопасности сеанс подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 завершается по истечении пяти минут бездействия системы, и открывается страница входа. Чтобы возобновить сеанс подключения, вам потребуется ввести ваши имя пользователя и пароль.

Веб-интерфейс Kaspersky IoT Secure Gateway 1000

Работа с Kaspersky IoT Secure Gateway 1000 осуществляется через веб-интерфейс. В этом разделе приведено описание основных элементов веб-интерфейса Kaspersky IoT Secure Gateway 1000.

Главное окно веб-интерфейса содержит следующие элементы:

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

Разделы веб-интерфейса

Меню веб-интерфейса Kaspersky IoT Secure Gateway 1000 содержит следующие разделы:

- **Статус**. В этом разделе вы можете просматривать сводную информацию о работе системы: информация об устройстве, тип сетевого устройства Kaspersky IoT Secure Gateway 1000 и статус подключения к Kaspersky Security Center. Этот раздел также содержит ссылки для перехода к статьям в онлайн-справке.
- **События**. В этом разделе вы можете просматривать события аудита сетевого экрана, в том числе от приложения Kaspersky IoT Secure Gateway Network Protector. События аудита сетевого экрана включают в себя, например, блокировку трафика от устройств, изменение конфигурации правил сетевого экрана.

  При возникновении критического события в меню возле раздела **События** в меню отображается *сигнализация* в виде значка с восклицательным знаком .
- **Аудит**. В этом разделе вы можете просматривать события аудита операционной системы. События аудита операционной системы включают в себя, например, подключение к веб-интерфейсу Kaspersky IoT Secure Gateway 1000, действия с приложениями, обновление системы и ее компонентов.

  При возникновении критического события в меню возле раздела **Аудит** в меню отображается *сигнализация* в виде значка с восклицательным знаком .
- **Пользователи**. В этом разделе расположены следующие вкладки, на которых вы можете управлять учетными записями пользователей и параметрами веб-сервера:
  - **Параметры пользователей**. На этой вкладке вы можете просматривать и изменять данные учетных записей, а также обновлять сертификаты подключения.
  - **Параметры веб-сервера**. На этой вкладке вы можете обновлять сертификат подключения к веб-серверу.
- **Приложения**. В этом разделе расположены следующие вкладки, на которых вы можете управлять приложениями:
  - **Все приложения**. На этой вкладке вы можете просматривать информацию о всех приложениях, доступных для установки в Kaspersky IoT Secure Gateway 1000, и устанавливать необходимые приложения.
  - **Установленные приложения**. На этой вкладке вы можете управлять установленными приложениями: запускать или останавливать, настраивать параметры запуска, или удалять.
  - **Журнал приложений**. На этой вкладке вы можете скачивать журналы установленных приложений.

- **Сеть**. В этом разделе расположены следующие вкладки, на которых вы можете настраивать параметры сети:
  - **Внутренняя сеть**. На этой вкладке вы можете просматривать и изменять параметры внутренней сети.
  - **Внешняя сеть**. На этой вкладке вы можете просматривать и изменять параметры трансляции сетевого адреса, внешней сети и модема.
  - **Маршрутизация**. На этой вкладке вы можете просматривать и управлять маршрутами сетевых пакетов.
  - **Фильтрация**. На этой вкладке вы можете выбирать протоколы, трафик по которым вы хотите заблокировать.
  - **MQTT-брокер**. На этой вкладке вы можете просматривать и изменять параметры в профиле MQTT-брокера.
- **Самодиагностика**. В этом разделе вы можете запускать тестирование состояния и проверку целостности системы, а также просматривать ее текущее состояние и результаты проверок.
- **Параметры**. В этом разделе расположены следующие вкладки, на которых вы можете просматривать и изменять параметры системы:
  - **Общие**. На этой вкладке вы можете просматривать и изменять имя устройства и параметры даты и времени Kaspersky IoT Secure Gateway 1000.
  - **Уведомления**. На этой вкладке вы можете просматривать и изменять параметры отправки журналов аудита сетевого экрана и аудита системы на сторонний сервер Syslog, а также настраивать параметры MQTT-уведомлений.
  - **Сервер администрирования**. На этой вкладке вы можете просматривать и изменять параметры подключения к Серверу администрирования Kaspersky Security Center.
  - **Диагностика**. На этой вкладке вы можете сохранять системный журнал Kaspersky IoT Secure Gateway 1000 на локальном компьютере.
  - **Конфигурация**. На этой вкладке вы можете просматривать и изменять параметры конфигурации Kaspersky IoT Secure Gateway 1000.
  - **Обновление**. На этой вкладке вы можете обновлять Kaspersky IoT Secure Gateway 1000.
  - **Команды**. На этой вкладке вы можете перезагружать устройство.
  - **Резервное копирование и восстановление**. На этой вкладке вы можете управлять резервированием и восстановлением системы из резервной копии: создавать и скачивать резервную копию конфигурации системы, а также восстанавливать конфигурацию системы из сохраненной ранее резервной копии.
- **О продукте**. Этот раздел содержит информацию об установленной на вашем устройстве версии системы, а также ссылки для перехода к онлайн-справке (прямая ссылка и QR-код) и информации о стороннем коде.
- **KasperskyOS**. При нажатии на логотип открывается окно, в котором отображается версия операционной системы KasperskyOS (SDK) и ссылка на информацию о стороннем коде.

Рабочая область окна веб-интерфейса

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

Меню пользователя

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

- изменить язык веб-интерфейса;
- выйти из системы.

Цели и предположения безопасности

Термины и общие положения

Целью кибериммунного подхода к разработке является создание *кибериммунной системы* – системы, декларированные активы которой защищены от нежелательных событий при любых условиях, даже под атакой, при условии заданных ограничений.

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

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

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

Приложение – компонент, устанавливаемый поверх образа системы и запускаемый средствами Kaspersky IoT Secure Gateway 1000. Может быть разработан "Лабораторией Касперского" или поставляться партнером. Приложение взаимодействует с Kaspersky IoT Secure Gateway 1000 и другими приложениями посредством API, предоставляемого Kaspersky IoT Secure Gateway 1000.

Пакет приложения – набор всех файлов, из которых состоит приложение.

Образ приложения – набор исполняемых файлов и библиотек, из которых состоит приложение.

Событие аудита - событие безопасности (например, перезагрузка, обновление версии системы, события информационной безопасности).

Аппаратная платформа – конечное устройство, на которое устанавливается образ системы.

Данные и информация – любая информация в электронном виде, например, файлы приложений и данные в базах данных.

Типы сетевого устройства Kaspersky IoT Secure Gateway 1000

Kaspersky IoT Secure Gateway 1000 может работать в качестве одного из следующих типов сетевого устройства:

- *Сетевой роутер* – тип сетевого устройства, в котором применена политика, обеспечивающая маршрутизацию проходящего через устройство сетевого трафика.

- *Однонаправленный шлюз* – тип сетевого устройства, в котором применена политика, обеспечивающая передачу данных от устройств, расположенных во внутренней сети, во внешнюю сеть без возможности воздействия на внутренние ресурсы со стороны внешней сети.

Переключение типа сетевого устройства происходит во время функционирования устройства. Для вступления изменений в силы требуется полная переустановка Kaspersky IoT Secure Gateway 1000.

Цели безопасности Kaspersky IoT Secure Gateway 1000

К целям безопасности Kaspersky IoT Secure Gateway 1000 относятся следующие цели:

- Kaspersky IoT Secure Gateway 1000 обеспечивает безопасное (целостность и аутентичность) обновление версии системы и приложений, в том числе через недоверенные каналы связи.
- Kaspersky IoT Secure Gateway 1000 обеспечивает безопасное (целостность и аутентичность) хранение параметров и конфигураций системы, полученных от доверенного источника. Доверенными источниками информации являются:
  - Сервер администрирования Kaspersky Security Center.
  - Администратор, авторизованный посредством сертификата при установке безопасного канала между компьютером администратора и Kaspersky IoT Secure Gateway 1000.
- Kaspersky IoT Secure Gateway 1000 обеспечивает безопасное (целостность) хранение событий аудита и их передачу на Сервер администрирования Kaspersky Security Center безопасным (целостность и аутентичность) образом.
- Kaspersky IoT Secure Gateway 1000 обеспечивает компонентам безопасный (целостность и конфиденциальность) канал связи с удаленным сервером (через TLS-терминатор).
- Kaspersky IoT Secure Gateway 1000 обеспечивает целостность и аутентичность пакетов приложений при динамической установке в процессе своей работы.
- Kaspersky IoT Secure Gateway 1000 обеспечивает целостность и аутентичность образов приложений перед запуском.
- Kaspersky IoT Secure Gateway 1000 обеспечивает возможность наделения динамически запускаемых приложений привилегиями в процессе своей работы.
- Kaspersky IoT Secure Gateway 1000 обеспечивает применение политик безопасности Kaspersky Security System к любому взаимодействию между приложениями и Kaspersky IoT Secure Gateway 1000.
- Kaspersky IoT Secure Gateway 1000 обеспечивает безопасное (целостность и конфиденциальность) персональное хранилище данных для каждого приложения. Доступ к этому хранилищу имеет только приложение, данные которого в нем хранятся.
- Kaspersky IoT Secure Gateway 1000 гарантирует взаимодействие приложений с внешними системами только посредством безопасного (целостность и конфиденциальность) канала связи (через TLS-терминатор).
- При работе в режиме однонаправленного шлюза Kaspersky IoT Secure Gateway 1000 обеспечивает однонаправленную передачу данных от приложений, взаимодействующих с внутренней сетью, с приложениями, взаимодействующими с внешней сетью, без возможности воздействия на внутренние ресурсы со стороны внешней сети.

Предположения безопасности Kaspersky IoT Secure Gateway 1000

К предположениям безопасности Kaspersky IoT Secure Gateway 1000 относятся следующие предположения:

- Не рассматриваются угрозы, связанные с уязвимостью аппаратной платформы. Предполагается, что аппаратная платформа является доверенной.
- Устройство, на котором установлен Kaspersky IoT Secure Gateway 1000, работает в окружении, гарантирующем отсутствие физического доступа со стороны злоумышленника, в том числе для подключения напрямую к устройству. Не рассматриваются угрозы, связанные с соответствующими уязвимостями.

- Предполагается средний (базовый повышенный) уровень угроз со стороны внешней сети.
- Предполагается низкий (базовый) уровень угроз со стороны внутренней сети.

  Подробную информацию об оценке уровня угроз безопасности информации вы можете получить на сайте Федеральной службы по техническому и экспортному контролю России.
- Первоначальная настройка решения должна производиться в условиях, когда отсутствует угроза подмены Сервера администрирования Kaspersky Security Center (то есть доверенным администратором в контролируемой зоне).
- При работе в режиме однонаправленного шлюза:
  - Не гарантируется целостность данных, передаваемых во внутренней сети от устройств к шлюзу.
  - Не обеспечивается защита безопасности устройств, подключенных к шлюзу, от атак из внутренней сети.
  - Аппаратная платформа должна иметь отдельные физические порты для подключения к внутренней и внешней сети.
- Доступность Kaspersky IoT Secure Gateway 1000 не является целью безопасности.
- Не гарантируется выполнение целей безопасности при установке приложений VPN или службы отладки Kaspersky Debug Service (KDS). При установке одного из этих приложений устройство перезагружается и выходит из кибериммунного режима. Для возврата в кибериммунный режим требуется полная переустановка Kaspersky IoT Secure Gateway 1000 и повторная первоначальная настройка.

Обработка и хранение данных в Kaspersky IoT Secure Gateway 1000

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

Предоставление данных

Kaspersky IoT Secure Gateway 1000 не передает пользовательские персональные данные в "Лабораторию Касперского". Обработка персональных данных пользователей на устройствах Kaspersky IoT Secure Gateway 1000 не производится.

Журнал событий аудита операционной системы, журнал событий аудита сетевого экрана, системный журнал и журналы приложений не удаляются при запуске Kaspersky IoT Secure Gateway 1000. Все данные сертификатов хранятся в отдельно выделенном пространстве диска.

При удалении информации или файлов (автоматически или вручную) используется специальный метод стирания, при котором удаляемые объекты файловой системы перезаписываются дважды специальными битовыми последовательностями. Например, этот метод используется для удаления сертификатов пользователя и администратора при их обновлении.

При работе с Kaspersky IoT Secure Gateway 1000 в файлах cookies сохраняется следующая информация:

- идентификатор текущего соединения;
- последний выбранный язык веб-интерфейса Kaspersky IoT Secure Gateway 1000;
- последний посещенный раздел веб-интерфейса Kaspersky IoT Secure Gateway 1000, в случае если пользователь не завершил сеанс подключения к Kaspersky IoT Secure Gateway 1000 или закрыл веб-интерфейс до завершения сеанса подключения.

При загрузке сертификата его поля могут хранить персональные данные пользователя. Вам нужно контролировать содержимое этих полей перед загрузкой сертификата в веб-интерфейсе Kaspersky IoT Secure Gateway 1000.

При настройке параметров MQTT-брокера содержимое конфигурационного файла может содержать персональные данные. Вам нужно контролировать данные, загружаемые в профиль MQTT-брокера Kaspersky IoT Secure Gateway 1000.

Kaspersky IoT Secure Gateway 1000 хранит следующую информацию, которая не относится к персональным данным:

- Тип сетевого устройства.
- Статус подключения к Серверу администрирования Kaspersky Security Center.
- Журнал событий аудита сетевого экрана.
- Журнал событий аудита операционной системы.
- Параметры учетных записей пользователей:

- Общие параметры:
  - количестве неуспешных попыток входа до блокировки;
  - время ожидания при неуспешном входе.
- Параметры корневого сертификата:
  - имя файла сертификата;
  - оставшийся срок действия сертификата.
- Параметры учетной записи администратора:
  - имя учетной записи;
  - срок окончания действия учетных данных;
  - срок окончания действия сертификата.
- Параметры учетной записи пользователя:
  - имя учетной записи;
  - срок окончания действия учетных данных;
  - срок окончания действия сертификата.

- Параметры веб-сервера Kaspersky IoT Secure Gateway 1000:
  - имя сертификата веб-сервера;
  - имя субъекта;
  - издатель сертификата;
  - срок действия сертификата.
- Список приложений, доступных для установки.
- Список установленных приложений:
  - название приложения;
  - версия приложения;
  - размер;
  - тип приложения;
  - правила запуска приложения;
  - манифест;
  - состояние приложения;

- набор правил фильтрации трафика промышленных протоколов от приложения Kaspersky IoT Secure Gateway Network Protector (если приложение установлено).

- Журналы приложений.
- Параметры сети:
  - Параметры внутренней сети:
    - IP-адрес Kaspersky IoT Secure Gateway 1000 во внутренней сети.
    - Маска подсети.
    - MAC-адрес
    - Параметры DHCP-сервера:
      - использование DHCP-сервера (включено или выключено);
      - начало и конец диапазона IP-адресов;
      - адрес основного DNS-сервера;
      - адрес дополнительного DNS-сервера.
  - Параметры внешней сети:
    - Параметры адресной трансляции: состояние маскарадинга (включено или выключено).
    - Параметры DHCP-клиента:
      - использование DHCP-клиента (включено или выключено);
      - IP-адрес;
      - маска подсети;
      - сетевой шлюз по умолчанию;
      - адрес основного DNS-сервера;
      - адрес дополнительного DNS-сервера;
      - MAC-адрес.
    - Параметры сотового соединения Kaspersky IoT Secure Gateway 1000:
      - статус работы модема;
      - уровень сигнала модема;
      - Использование модема как основного канала связи (включено или выключено);
      - адреса DNS-серверов модема;

- данные о профилях операторов связи: признак активности профиля, признак доступности для изменения профиля, имя профиля, данные о конфигурационном файле профиля (тип файла, имя файла, содержимое файла).

- Параметры маршрутизации:
  - тип маршрута;
  - IP-адрес маршрута;
  - маска сети;
  - шлюз;
  - состояние маршрута.
- Параметры MQTT-брокера:
  - признак доступности профиля для изменения;
  - признак активности профиля;
  - имя профиля;
  - дата и время последнего изменения профиля;
  - сертификат удостоверяющего центра для сервера MQTT (сертификат может являться самоподписанным);
  - клиентский сертификат для сервера MQTT;
  - закрытый ключ для клиентского сертификата сервера MQTT;
  - информация о конфигурационных файлах: имя файла, тип файла, содержимое файла.
- Параметры фильтрации прикладных протоколов:
  - Список протоколов, по которым можно заблокировать трафик:
    - FTP;
    - HTTP;
    - MQTT;
    - Modbus;
    - SMTP;
    - IMAP;
    - POP3.
  - Состояние блокировки трафика по протоколу (запрещен или разрешен).

- Информация о самодиагностике:

- Информация о проверке целостности: дата последней проверки.
- Информация о самотестировании:
  - общий статуса самотестирования;
  - название теста;
  - статус теста;
  - тип теста;
  - дата последней проверки;
  - сведения о тесте.

- Общие параметры Kaspersky IoT Secure Gateway 1000:
  - Имя устройства.
  - Дата и время системы.
  - Параметры уведомлений:
    - Параметры Syslog-уведомлений:
      - отправка уведомлений для сервера Syslog (включена или выключена);
      - IP-адрес и порт сервера Syslog;
      - режим передачи уведомлений: UDP, TCP, TLS;
      - сертификат сервера Syslog.
    - Параметры MQTT-уведомлений:
      - отправка уведомлений по протоколу MQTT (включена или выключена);
      - адрес и порт сервера MQTT;
      - имя MQTT-топика;
      - использование аутентификации при отправке уведомлений по протоколу MQTT (включено или выключено);
      - имя и пароль пользователя для аутентификации;
      - использование защищенного SSL-соединения для аутентификации (включено или выключено);
      - сертификат удостоверяющего центра для отправки уведомлений по протоколу MQTT;
      - клиентский сертификат для отправки MQTT-уведомления;
      - закрытый ключ для клиентского сертификата для отправки MQTT-уведомлений.
  - Параметры подключения к Серверу администрирования Kaspersky Security Center:

        - сертификат Сервера администрирования Kaspersky Security Center;
        - адрес и порт Сервера администрирования Kaspersky Security Center.
    - Системный журнал с диагностической информацией.
    - Конфигурация устройства в формате JSON.
- Информация о Kaspersky IoT Secure Gateway 1000:
    - версия Kaspersky IoT Secure Gateway 1000;
    - ссылки на онлайн-справку;
    - информация о стороннем коде.
- Информация об операционной системе KasperskyOS:
    - версия операционной системы;
    - информация о стороннем коде.

Если Kaspersky IoT Secure Gateway 1000 подключен к Kaspersky Security Center, Kaspersky IoT Secure Gateway 1000 сохраняет и обрабатывает следующую информацию, не относящуюся к персональным данным:

- Список приложений, доступных для установки.
- Список установленных приложений:
    - название приложения;
    - версия приложения;
    - дата публикации;
    - категория;
    - состояние приложения;
    - конфигурация приложения.
- Параметры установленных приложений:
    - Информация об установленных приложениях:
        - название приложения;
        - версия приложения;
        - тип приложения;
        - статус приложения;
        - правило запуска приложения;
        - манифест приложения.

- Сертификаты работы приложений:
  - имя файла сертификата удостоверяющего центра;
  - основное имя сертификата удостоверяющего центра;
  - издатель сертификата удостоверяющего центра;
  - срок действия сертификата удостоверяющего центра (дата, до которой действителен сертификат);
  - имя файла сертификата клиента;
  - имя субъекта сертификата клиента;
  - издатель сертификата клиента;
  - срок действия сертификата клиента (дата, до которой действителен сертификат);
  - имя файла ключа сертификата клиента.
- Маршрутизация приложений:
  - статус маршрута;
  - приложение отправитель в маршруте;
  - точка подключения отправителя;
  - приложение получатель в маршруте;
  - точка подключения получателя.
- Параметры MQTT-брокера:
  - признак доступности профиля для изменения;
  - признак активности профиля;
  - имя профиля;
  - сертификат удостоверяющего центра для сервера MQTT (сертификат может являться самоподписанным);
  - клиентский сертификат сервера MQTT;
  - закрытый ключ для клиентского сертификата сервера MQTT;
  - информация о конфигурационных файлах: имя файла, тип файла, содержимое файла;
  - сертификата для отправки MQTT-уведомлений.
- Параметры сети Kaspersky IoT Secure Gateway 1000:
  - Параметры внутренней сети:
    - IP-адрес Kaspersky IoT Secure Gateway 1000 во внутренней сети.

- Маска подсети.
- MAC-адрес.
- Параметры DHCP-сервера:
  - использование DHCP-сервера (включено или выключено);
  - начало и конец диапазона IP-адресов;
  - адрес основного DNS-сервера;
  - адрес дополнительного DNS-сервера.

- Параметры внешней сети:
  - Параметры адресной трансляции: состояние маскарадинга (включено или выключено).
  - Параметры DHCP-сервера:
    - использование DHCP-клиента (включено или выключено);
    - IP-адрес;
    - маска подсети;
    - сетевой шлюз по умолчанию;
    - адрес основного DNS-сервера;
    - адрес дополнительного DNS-сервера;
    - MAC-адрес.
- Параметры маршрутизации:
  - тип маршрута;
  - IP-адрес;
  - маска сети;
  - шлюз;
  - состояние маршрута.
- Правила сетевого экрана:
  - список правил;
  - состояние правила (включено или выключено);
  - действие, которое сетевой экран должен выполнять над сетевым трафиком, попадающим под правило;
  - область, к которой применяется правило;

- IP-адрес источника трафика;
- порт источника трафика, если этот параметр применим к используемому протоколу;
- IP-адрес получателя трафика;
- порт получателя трафика, если этот параметр применим к используемому протоколу;
- используемый протокол.

- Параметры сотового соединения Kaspersky IoT Secure Gateway 1000:
  - статус работы модема;
  - уровень сигнала модема;
  - использование модема как основного канала связи (включено или выключено);
  - адреса DNS-серверов модема;
  - данные для работы оператора связи: признак активности конфигурационного файла, признак доступности конфигурационного файла для изменения, тип конфигурационного файла, имя конфигурационного файла, содержимое конфигурационного файла.
- Параметры приложения Kaspersky IoT Secure Gateway Network Protector (если приложение установлено):
  - набор правил фильтрации трафика промышленных протоколов;
  - список запрещенных IP-адресов;
  - список разрешенных IP-адресов.
- Параметры фильтрации прикладных протоколов:
  - Список протоколов, по которым можно заблокировать трафик:
    - FTP;
    - HTTP;
    - MQTT;
    - Modbus;
    - SMTP;
    - IMAP;
    - POP3.
  - Состояние блокировки трафика по протоколу (запрещен или разрешен).
- Параметры сетевого кластера:
  - состояние сетевого кластера (включен или выключен);

- приоритет устройства в кластере;
- виртуальный IP-адрес;
- виртуальная маска IP-адреса;
- идентификатор кластера.

- Общие параметры устройства Kaspersky IoT Secure Gateway 1000:
  - Имя устройства.
  - Время последней синхронизации с устройством.
  - Информация о сертификатах подключения:
    - Информация о сертификате администратора для подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000:
      - имя файла сертификата;
      - имя субъекта;
      - издатель сертификата;
      - срок действия сертификата.
    - Информация о сертификате Сервера администрирования Kaspersky Security Center:
      - имя файла сертификата;
      - имя субъекта;
      - издатель сертификата;
      - срок действия сертификата.
  - Параметры веб-сервера:
    - Информация о сертификате веб-сервера:
      - имя файла сертификата;
      - имя субъекта;
      - издатель сертификата;
      - срок действия сертификата.
    - Информация о ключе сертификата: имя файла ключа.
  - Параметры уведомлений:
    - Параметры Syslog-уведомлений:
      - отправка уведомлений на сервер Syslog (включена или выключена);

- IP-адрес и порт сервера Syslog;
- режим передачи уведомлений: UDP, TCP, TLS;
- сертификат сервера Syslog.

- Параметры MQTT-уведомлений:
  - отправка уведомлений по протоколу MQTT (включена или выключена);
  - адрес и порт сервера MQTT;
  - имя MQTT-топика;
  - использование аутентификации при отправке уведомлений по протоколу MQTT (включено или выключено);
  - имя и пароль пользователя для аутентификации;
  - использование защищенного SSL-соединения для аутентификации (включено или выключено);
  - сертификат удостоверяющего центра для отправки MQTT-уведомлений;
  - клиентский сертификат для отправки MQTT-уведомлений;
  - закрытый ключ клиентского сертификата для отправки MQTT-уведомлений.

- Параметры взаимодействия Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center 14.2 Web Console:
  - период синхронизации параметров Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center 14.2 Web Console;
  - список команд, которые Kaspersky Security Center 14.2 Web Console может отправить в Kaspersky IoT Secure Gateway 1000.
- Информация о версии Kaspersky IoT Secure Gateway 1000.

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

О хранении журналов Kaspersky IoT Secure Gateway 1000

Kaspersky IoT Secure Gateway 1000 сохраняет данные о событиях аудита сетевого экрана и событиях аудита системы в соответствующих журналах. Содержимое журналов хранится в памяти устройства Kraftway Рубеж-Н.

Kaspersky IoT Secure Gateway 1000 позволяет сохранять журнал событий аудита сетевого экрана и журнал событий аудита системы. Вы можете сохранить на локальный компьютер файл, содержащий журнал событий аудита сетевого экрана и журнал событий аудита системы, используя веб-интерфейс Kaspersky IoT Secure Gateway 1000.

Также при необходимости вы можете настроить передачу данных журнала событий аудита сетевого экрана и аудита системы через протоколы MQTT и Syslog.

Лицензирование Kaspersky IoT Secure Gateway 1000

Условия использования системы Kaspersky IoT Secure Gateway 1000 изложены в Лицензионном соглашении или подобном документе (например, лицензионном договоре или лицензионном сертификате), на основании которого используется система.

О режимах работы Kaspersky IoT Secure Gateway 1000

При возникновении в Kaspersky IoT Secure Gateway 1000 ситуаций, не предусмотренных стандартными сценариями работы, система автоматически переходит в один из следующих нештатных режимов: *неиммунный режим*, *режим разработчика*, *режим аварийной поддержки*.

После активации какого-либо режима его название отображается в правом верхнем углу на всех страницах веб-интерфейса Kaspersky IoT Secure Gateway 1000, а также в правом верхнем углу Kaspersky Security Center 14.2 Web Console после каждой синхронизации. Вы можете посмотреть описание активного режима, нажав на его имя. События об активации режимов записываются в журнал аудита системы.

Неиммунный режим

Неиммунный режим активируется после того, как вы в первый раз запускаете приложение VPN. Когда Kaspersky IoT Secure Gateway 1000 работает в неиммунном режиме, иммунность устройства не гарантируется. При этом ограничения на доступ к функционалу и работу Kaspersky IoT Secure Gateway 1000 отсутствуют.

Неиммунный режим невозможно выключить через веб-интерфейс Kaspersky IoT Secure Gateway 1000 или Kaspersky Security Center 14.2 Web Console. Выйти из неиммунного режима возможно только после полной переустановки Kaspersky IoT Secure Gateway 1000 на устройстве.

Режим разработчика

Режим разработчика активируется после запуска службы отладки Kaspersky Debug Service (KDS), которая необходима для тестирования и отладки компонентов.

> Служба отладки Kaspersky Debug Service поставляется в составе Kaspersky IoT Secure Gateway 1000 SDK в отдельном пакете для установки. При запуске Kaspersky Debug Service режим разработчика активируется только для того пользователя (разработчика), который запустил службу отладки.

Если Kaspersky IoT Secure Gateway 1000 работает в режиме разработчика, подписи приложений при установке в Kaspersky IoT Secure Gateway 1000 проверяются следующим способом:

- Если приложение устанавливается через Kaspersky IoT Secure Gateway 1000 или через Kaspersky Security Center 14.2 Web Console, подпись приложения проверяется на всех этапах (скачивание, установка и запуск приложения).
- Если приложение устанавливается через службу отладки KDS, подпись приложения не проверяется.
- Если приложение предустановлено в Kaspersky IoT Secure Gateway 1000, подпись приложения не проверяется во время запуска. Этапы скачивания и установки отсутствуют, так как приложение предустановлено.

Ограничения на работу и доступ к функционалу Kaspersky IoT Secure Gateway 1000 отсутствуют.

Режим разработчика невозможно выключить через веб-интерфейс Kaspersky IoT Secure Gateway 1000 или Kaspersky Security Center 14.2 Web Console. Выйти из режима разработчика возможно только после полной переустановки Kaspersky IoT Secure Gateway 1000 на устройстве, на котором была запущена служба отладки Kaspersky Debug Service.

Режим аварийной поддержки

Режим аварийной поддержки активируется, если произошло одно или несколько из следующих событий:

- ошибка в результате проведения самотестирования;
- ошибка при автоматической проверке целостности файлов при запуске;
- аварийное завершение приложений, обеспечивающих функции безопасности (например, Kaspersky IoT Secure Gateway Network Protector).

  Аварийное завершение приложения Kaspersky IoT Secure Gateway Network Protector может произойти, если не удается загрузить правила фильтрации трафика промышленных протоколов или правила не заданы, самодиагностика приложения завершилась с ошибкой или приложение не отвечает.

При активации режима аварийной поддержки происходит следующее:

- В журнал аудита системы записывается сообщение о произошедшем сбое и его причине. Если режим аварийной поддержки был активирован в результате аварийного завершения приложения Kaspersky IoT Secure Gateway Network Protector, сообщение о произошедшем сбое также записывается в журнал аудита сетевого экрана.
- Завершается активная сессия подключения пользователя.
- Инициируется остановка всех запущенных приложений.
- Если режим аварийной поддержки был активирован в результате аварийного завершения приложения Kaspersky IoT Secure Gateway Network Protector, блокируется передача любого трафика, кроме служебного, который обеспечивает работу Kaspersky IoT Secure Gateway 1000 и работу в сети (определяется служебными разрешающими правилами).

Режим аварийной поддержки невозможно выключить через Kaspersky IoT Secure Gateway 1000 или Kaspersky Security Center 14.2 Web Console. Выйти из режима аварийной поддержки возможно следующими способами:

- перезагрузка устройства (возможен повторный переход в режим аварийной поддержки);
- восстановление из резервной копии;
- полная переустановка Kaspersky IoT Secure Gateway 1000 на устройстве.

Настройка Kaspersky IoT Secure Gateway 1000

Этот раздел содержит информацию о настройке Kaspersky IoT Secure Gateway 1000.

Этот функционал доступен только администратору.

Сценарий: Быстрый старт для администратора

В этом разделе приводится последовательность действий, которые требуется выполнить администратору, чтобы установить и настроить Kaspersky IoT Secure Gateway 1000, Kaspersky Security Center, а также установить между ними соединение.

Сценарий установки Kaspersky IoT Secure Gateway 1000, Kaspersky Security Center и настройки между ними соединения состоит из следующих этапов:

1. **Установка Kaspersky Security Center**

   Загрузите дистрибутив Kaspersky Security Center 14.2 и установите полную версию Kaspersky Security Center на сервере. Дистрибутив полной версии Kaspersky Security Center 14.2 включает Kaspersky Security Center 14.2 Web Console. При установке рекомендуется выбрать стандартную установку. Подробную информацию об установке Kaspersky Security Center вы можете получить в разделе онлайн-справки Kaspersky Security Center 14.2 *Основной сценарий установки*.

2. **Настройка правил сетевого экрана**

   Для сетевого экрана операционной системы сервера, на котором установлен Kaspersky Security Center, настройте правила, разрешающие подключение Kaspersky IoT Secure Gateway 1000 к серверу Kaspersky Security Center по протоколу TCP через порт 13294. Подробную информацию о настройке правил сетевого экрана вы можете получить в руководстве используемой операционной системы.

3. **Установка веб-плагина управления Kaspersky IoT Secure Gateway 1000**

   В интерфейсе Kaspersky Security Center 14.2 Web Console установите веб-плагин управления Kaspersky IoT Secure Gateway 1000. ZIP-архив с дистрибутивом веб-плагина Kaspersky IoT Secure Gateway 1000 входит в комплект поставки.

4. **Настройка подключения устройств с защитой на уровне UEFI**

   На Сервере администрирования Kaspersky Security Center включите использование порта 13294 для протокола TCP для настройки подключения Kaspersky IoT Secure Gateway 1000 к Kaspersky Security Center. Подробную информацию о включении порта 13294 на Сервере администрирования Kaspersky Security Center вы можете получить в разделе онлайн-справки Kaspersky Security Center 14.2 *Устройства с защитой на уровне UEFI*.

5. **Включение устройства Kraftway Рубеж-Н**

   Включите устройство Kraftway Рубеж-Н.

6. **Подключение к веб-интерфейсу Kaspersky IoT Secure Gateway 1000**

   Подключитесь к веб-интерфейсу Kaspersky IoT Secure Gateway 1000, используя имя и пароль по умолчанию, а также сертификат администратора.

7. **Настройка параметров Kaspersky IoT Secure Gateway 1000**

   После подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 настройте следующие параметры:

- подключение к внешней и внутренней сети;
- профиль модема.

8. **Создание и загрузка сертификата сервера Kaspersky Security Center**

   Создайте новый сертификат сервера Kaspersky Security Center и сохраните его на локальное устройство. В веб-интерфейсе Kaspersky IoT Secure Gateway 1000 загрузите сертификат сервера Kaspersky Security Center для настройки соединения с Kaspersky Security Center 14.2 Web Console.

9. **Настройка подключения Kaspersky IoT Secure Gateway 1000 к Kaspersky Security Center**

   В веб-интерфейсе Kaspersky IoT Secure Gateway 1000 настройте подключение к Kaspersky Security Center.

10. **Обновление корневого и пользовательских сертификатов Kaspersky IoT Secure Gateway 1000**

    Обновите корневой и пользовательские сертификаты.

11. **Добавление Kaspersky IoT Secure Gateway 1000 в список управляемых устройств**

    Подключитесь к Kaspersky Security Center 14.2 Web Console и добавьте Kaspersky IoT Secure Gateway 1000 в список управляемых устройств Kaspersky Security Center.

12. **Настройка фильтрации трафика в приложении Kaspersky IoT Secure Gateway Network Protector**

    Если у вас установлено приложение Kaspersky IoT Secure Gateway Network Protector, настройте правила фильтрации трафика промышленных протоколов и запустите приложение. До тех пор пока вы не настроите и не запустите приложение Kaspersky IoT Secure Gateway Network Protector, транзитный трафик на устройстве будет заблокирован для обеспечения безопасности подключенных устройств.

    Вы также можете настроить правила фильтрации трафика и запустить приложение через Kaspersky Security Center 14.2 Web Console, если вы установили соединение между Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center.

В результате выполнения этих действий система Kaspersky IoT Secure Gateway 1000 будет готова к работе, и вы сможете управлять Kaspersky IoT Secure Gateway 1000 через веб-интерфейс или через Kaspersky Security Center 14.2 Web Console, а также осуществлять мониторинг событий аудита.

Сценарий: Настройка доступа из внешней сети к устройствам внутренней сети

В этом разделе описана последовательность действий, которые требуется выполнить для настройки доступа из внешней сети к устройствам внутренней сети, используя Kaspersky IoT Secure Gateway 1000.

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

Сценарий настройки доступа состоит из следующих этапов:

1. **Настройка маршрутизации транзитных IP-пакетов**

   На устройстве во внешней сети, с которого требуется получить доступ к устройствам во внутренней сети, настройте маршрутизацию транзитных IP-пакетов на порт внешней сети Kaspersky IoT Secure Gateway 1000 (WAN).

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

2. **Выключение маскарадинга**

Выключите функцию маскарадинга для динамического преобразования IP-адресов транзитных пакетов, полученных Kaspersky IoT Secure Gateway 1000 от устройства во внешней сети.

3. **Создание правила доступа из внешней сети**

   Создайте разрешающее правило сетевого экрана для прохождения сетевых пакетов от устройства во внешней сети Kaspersky IoT Secure Gateway 1000 (WAN) к устройству во внутренней сети.

   Созданное правило будет применяться одновременно для всех доступных интерфейсов подключения к внешней сети, в том числе для подключения к внешней сети через встроенный модем.

4. **Создание правила доступа из внутренней сети**

   Создайте разрешающее правило сетевого экрана для прохождения сетевых пакетов от устройства во внутренней сети Kaspersky IoT Secure Gateway 1000 (LAN) к устройству во внешней сети.

5. **Проверьте подключение к устройству внутренней сети**

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

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

Настройка доступа выполнена. Вы сможете подключиться из внешней сети к устройствам, расположенным во внутренней сети Kaspersky IoT Secure Gateway 1000, например, для выгрузки данных от этих устройств или настройки их параметров.

Управление учетными записями

Этот раздел содержит информацию о настройке данных учетных записей администратора и пользователя Kaspersky IoT Secure Gateway 1000, а также параметров подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.

Этот функционал доступен только администратору.

О ролях учетных записей

В Kaspersky IoT Secure Gateway 1000 есть две роли учетных записей:

- **Администратор**. Имеет полный доступ ко всем функциям, параметрам и данным Kaspersky IoT Secure Gateway 1000.
- **Пользователь**. Имеет ограниченный доступ к функциям.

По умолчанию в Kaspersky IoT Secure Gateway 1000 существует одна учетная запись администратора. Администратор может создать только одну учетную запись пользователя.

Создание дополнительных учетных записей не поддерживается.

В таблице ниже описаны разделы веб-интерфейса, которые доступны администратору и пользователю.

Разделы веб-интерфейса, доступные администратору и пользователю

Раздел веб-интерфейса	Администратор	Пользователь
Статус	✓	✓
События	✓	✓
Аудит	✓	—
Пользователи	✓	—
Приложения	✓	Только просмотр списков установленных и запущенных приложений и списков журналов приложений
Сеть	✓	—
Самодиагностика	✓	—
Параметры	✓	—
О продукте	✓	✓

Просмотр информации об учетных записях и параметрах подключения

Чтобы просмотреть информацию об учетных записях и параметрах подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000,

В меню в левой части страницы веб-интерфейса выберите раздел **Пользователи** → **Параметры пользователей**.

Отобразится страница, в которой указана следующая информация:

- В блоке **Общие параметры** отображаются основные параметры подключения, установленные в системе: количество доступных попыток подключения к Kaspersky IoT Secure Gateway 1000 до временной блокировки, а также время (в минутах), в течение которого вы не можете подключаться к Kaspersky IoT Secure Gateway 1000, если вы несколько раз (настраиваемое значение) ввели неверные данные учетной записи.
- В блоке **Корневой сертификат** отображается информация о корневом сертификате, который используется для безопасного подключения к веб-интерфейсу через браузер, и срок действия этого сертификата.
- В блоке **Администратор** отображаются данные учетной записи администратора: имя, срок действия учетных данных, а также срок действия сертификата.
- В блоке **Пользователь** отображаются данные учетной записи пользователя: имя, срок действия учетных данных, а также срок действия сертификата.

В этом разделе вы также можете настраивать параметры подключения к веб-интерфейсу, а также обновлять данные учетных записей и сертификаты подключения.

Настройка параметров подключения

Вы можете настроить параметры подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 для администратора и пользователя, такие как срок действия учетных данных, время бездействия системы до блокировки, количество возможных попыток авторизации и другие.

Чтобы настроить параметры подключения:

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

2. В блоке **Общие параметры** нажмите на кнопку **Изменить**.

3. В открывшемся окне настройки параметров укажите значения необходимых параметров:

   - **Срок действия учетных данных** – количество дней, в течение которого пользователь и администратор могут использовать имя и пароль для подключения.

     Вы можете указать значение от 180 до 365 дней. По истечении указанного срока действия вам нужно будет обновить учетные данные администратора и пользователя.

   - **Период бездействия** – время (в минутах), в течение которого сессия подключения остается активной при бездействии администратора или пользователя.

     Вы можете указать значение от 1 до 30 минут. По истечении указанного времени при бездействии пользователя или администратора сессия подключения будет завершена.

   - **Период отображения уведомлений об окончании срока действия учетных данных** – количество дней до конца срока действия учетных данных администратора и пользователя, когда вы хотите начать получать уведомления.

     Вы можете указать значение от 3 до 30 дней. Пользователь также получит уведомление об окончании действия учетных данных его учетной записи в указанный срок.

   - **Период отображения уведомлений об окончании срока действия сертификата** – количество дней до конца срока действия сертификата администратора и пользователя, когда вы хотите начать получать уведомления.

     Вы можете указать значение от 3 до 30 дней. Пользователь также получит уведомление об окончании действия сертификата в указанный срок.

   - **Количество неуспешных попыток входа** – максимальное количество попыток ввода неверных данных администратором или пользователем при попытке подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.

     Вы можете указать значение от 3 до 10. После указанного числа неуспешных попыток авторизации Kaspersky IoT Secure Gateway 1000 будет временно заблокирован.

   - **Время ожидания при неуспешном входе** – время (в минутах), в течение которого подключение к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 будет недоступно после нескольких неуспешных попыток авторизации для администратора или пользователя.

     Вы можете указать значение от 1 до 30 минут. Если вы несколько раз вводите неверные данные для подключения, по истечении указанного времени вы сможете повторить попытку подключения.

4. Нажмите на кнопку **Сохранить**.

Параметры подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 будут обновлены.

Создание учетной записи пользователя

Вы можете создать учетную запись пользователя Kaspersky IoT Secure Gateway 1000, обновив учетные данные по умолчанию и указав сертификат пользователя. Пользователь сможет подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 и будет иметь ограниченный доступ к функционалу. Вы можете создать только одну учетную запись пользователя.

Чтобы создать учетную запись пользователя:

1. Подключите USB-накопитель или токен с сертификатом пользователя и закрытым ключом сертификата к компьютеру.

2. В меню в левой части экрана веб-интерфейса выберите раздел **Пользователи** → **Параметры пользователей**.

3. В блоке **Пользователь** нажмите на кнопку **Обновить учетные данные** и в открывшемся окне обновления данных выполните следующие действия:

   a. При необходимости в поле **Имя пользователя** введите новое имя пользователя.

   Имя может состоять только из букв латинского алфавита, цифр и специальных символов @ . _ -.

   b. В поле **Старый пароль** введите пароль пользователя по умолчанию. Пароль для пользователя, предоставляемый по умолчанию: **useruser**.

   c. В поле **Новый пароль** введите новый пароль.

   Пароль должен удовлетворять следующим требованиям:

   - Содержит восемь и более различных неповторяющихся символов.
   - Не совпадает с ранее использованными паролями.

   d. В поле **Повторите новый пароль** введите новый пароль еще раз.

   e. Нажмите на кнопку **Сохранить**.

   Данные учетной записи пользователя будут обновлены.

4. В блоке **Пользователь** нажмите на кнопку **Обновить сертификат**.

5. В открывшемся окне обновления сертификата пользователя нажмите на кнопку **Выбрать сертификат** и выберите сертификат пользователя с USB-накопителя или токена.

   Для добавления в качестве сертификата доступны файлы только в формате CRT, CER, DER и PEM. Хеш сертификата будет загружен в Kaspersky IoT Secure Gateway 1000.

   > Сертификат пользователя должен быть подписан тем корневым сертификатом, который загружен в Kaspersky IoT Secure Gateway 1000. Если сертификат пользователя подписан другим корневым сертификатом, вам нужно сначала обновить корневой сертификат и сертификат администратора.

6. Дождитесь успешной загрузки и нажмите на кнопку **Сохранить**.

Учетная запись пользователя будет создана с обновленными данными. Пользователь сможет использовать эти учетные данные и сертификат пользователя для подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.

Обновление данных учетной записи

Вы можете обновлять данные учетных записей (имя и пароль) администратора и пользователя для подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000. Требуется обновлять данные учетных записей в следующих случаях:

- текущие учетные данные скомпрометированы;
- закончился срок действия учетных данных;
- нужно выполнить регулярное обновление учетных данных в соответствии с требованиями информационной безопасности вашей организации.

Если срок действия данных учетной записи администратора или пользователя подходит к концу, вы получите соответствующее уведомление, и в меню в левой части экрана возле раздела **Пользователи** отобразится значок , и в журнал аудита операционной системы будет записано соответствующее событие. Пользователь также получит уведомление об истечении срока действия данных его учетной записи. Если вы не обновите данные учетной записи, после окончания срока действия произойдет следующее:

- Если истек срок действия данных учетной записи пользователя, учетная запись будет заблокирована и пользователь не сможет подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway 1000, пока администратор не обновить учетные данные. Администратор получит уведомление о необходимости обновить данные учетной записи пользователя.
- Если истек срок действия данных вашей учетной записи администратора, при подключении к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 вы будете перенаправлены на страницу обновления данных вашей учетной записи.

Если срок действия учетных данных администратора или пользователя истек во время активной сессии, эта сессия будет завершена. Обновите данные учетной записи, чтобы восстановить доступ.

Обновление данных учетной записи администратора

Чтобы обновить имя и пароль администратора:

1. В меню в левой части экрана веб-интерфейса выберите раздел **Пользователи** → **Параметры пользователей**.
2. В блоке **Администратор** нажмите на кнопку **Обновить учетные данные**.
3. В окне обновления учетных данных выполните следующие действия:
   a. При необходимости введите новое имя администратора.
      Имя может состоять только из букв латинского алфавита, цифр и специальных символов @ . _ -.
   b. Введите ваш старый пароль администратора, новый пароль и подтвердите новый пароль.
      Новый пароль должен удовлетворять следующим требованиям:
      - Содержит восемь и более различных неповторяющихся символов.
      - Не совпадает с ранее использованными паролями.

Требуется изменить пароль, чтобы обновить срок действия учетных данных.

4. Нажмите на кнопку **Сохранить**.

   Данные учетной записи администратора будут обновлены.

Обновление данных учетной записи пользователя

Чтобы обновить имя и пароль пользователя:

1. В меню в левой части экрана веб-интерфейса выберите раздел **Пользователи** → **Параметры пользователей**.

2. В блоке **Пользователь** нажмите на кнопку **Обновить учетные данные**.

3. В окне обновления учетных данных выполните следующие действия:

   a. При необходимости введите новое имя пользователя.

      Имя может состоять только из букв латинского алфавита, цифр и специальных символов @ . _ -.

   b. Введите старый пароль пользователя, новый пароль и подтвердите новый пароль.

      Новый пароль должен удовлетворять следующим требованиям:

      - Содержит восемь и более различных неповторяющихся символов.
      - Не совпадает с ранее использованными паролями.

      Требуется изменить пароль, чтобы обновить срок действия учетных данных.

4. Нажмите на кнопку **Сохранить**.

   Данные учетной записи пользователя будут обновлены.

Управление сертификатами подключения

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

Для безопасного подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 через браузер требуются следующие сертификаты:

- сертификат администратора для подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 через учетную запись администратора;
- сертификат пользователя для подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 через учетную запись пользователя;
- корневой сертификат, которым подписаны сертификаты администратора и пользователя.

Сертификаты могут быть выпущены специальной инфраструктурой на индивидуальных USB-накопителях или токенах. В этом случае, чтобы обновить сертификат, вам нужен USB-накопитель или токен с набором действующих сертификатов. Вы также можете создать необходимые сертификаты вручную и использовать их для подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.

Ручное создание сертификатов

Создание корневого сертификата

Корневой сертификат может быть выпущен удостоверяющим центром и хранится на USB-накопителе или токене, либо вы можете создать его самостоятельно по инструкции ниже.

Загруженный в Kaspersky IoT Secure Gateway 1000 корневой сертификат в дальнейшем будет использоваться для проверки сертификатов администратора и пользователя при подключении к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.

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

Ниже приведен пример использования утилиты OpenSSL для создания корневого сертификата. Подробную информацию по работе с утилитой вы можете получить в документации по OpenSSL.

Чтобы создать корневой сертификат с помощью утилиты OpenSSL:

1. В консоли запустите утилиту OpenSSL, выполнив команду:

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

   где:

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

2. Введите и повторите пароль для закрытого ключа сертификата. Пароль должен отличаться от пароля сертификата, предоставляемого по умолчанию.

   В результате в директории, в которой была выполнена команда, будет создано два файла:

   - cert.pem – файл корневого сертификата;
   - cert_key.pem – закрытый ключ корневого сертификата.

   Созданный файл корневого сертификата cert.pem требуется загрузить при необходимости обновить корневой сертификат.

Создание сертификатов администратора и пользователя

Сертификаты администратора и пользователя могут быть созданы с помощью заранее созданного корневого сертификата.

Загруженные в Kaspersky IoT Secure Gateway 1000 сертификаты администратора и пользователя в дальнейшем будет использоваться для подключения к в веб-интерфейсу Kaspersky IoT Secure Gateway 1000.

Ниже приведен пример использования утилиты OpenSSL для создания сертификата администратора или пользователя. Подробную информацию по работе с утилитой вы можете получить в документации по OpenSSL.

Чтобы создать сертификат администратора или пользователя с помощью утилиты OpenSSL:

1. Чтобы создать новый сертификат, в консоли запустите утилиту OpenSSL, выполнив команду:
   ```
   openssl req -new -newkey rsa:4096 -keyout TlsClientAdminKey.pem -out
   TlsClientAdmin.csr
   ```

2. Чтобы подписать создаваемый сертификат ранее созданным корневым сертификатом, выполните следующую команду и введите пароль от закрытого ключа корневого сертификата:
   ```
   openssl x509 -req -days 365 -in TlsClientAdmin.csr -CA cert.pem -CAkey cert_key.pem -
   CAcreateserial -out TlsClientAdmin.crt -extensions v3_req
   ```
   Созданный файл сертификата в формате CRT необходим при обновлении сертификата администратора или пользователя.

3. Чтобы создать архив, содержащий новый сертификат и его закрытый ключ, выполните следующую команду:
   ```
   openssl pkcs12 -export -in TlsClientAdmin.crt -inkey TlsClientAdminKey.pem -out
   TlsClientAdmin.p12 -name TlsClientAdmin -descert -nomaciter
   ```
   Созданный файл архива в формате P12 требуется загрузить в браузер при подключении к веб интерфейсу Kaspersky IoT Secure Gateway 1000.

Обновление сертификатов

Для безопасного подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 через браузер требуются сертификат администратора, сертификат пользователя и корневой сертификат, которым подписаны сертификаты администратора и пользователя.

Требуется обновлять сертификаты в следующих случаях:

- текущие сертификаты скомпрометированы;

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

Если срок действия сертификата администратора или пользователя подходит к концу, вы получите соответствующее уведомление, и в меню в левой части экрана возле раздела **Пользователи** отобразится значок , и в журнал аудита операционной системы будет записано соответствующее событие. Пользователь также получит уведомление об истечении срока действия его сертификата. При истечении срока действия сертификатов произойдет следующее:

- Если истек срок действия сертификата пользователя, учетная запись будет заблокирована и пользователь не сможет подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway 1000. Активная сессия подключения будет завершена. Вы получите уведомление о необходимости обновить сертификат пользователя.
- Если истек срок действия сертификата администратора, учетная запись будет заблокирована и администратор не сможет подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.
- Если истек срок действия корневого сертификата, требуется обновить все сертификаты: корневой сертификат, сертификат администратора и сертификат пользователя.

При обновлении сертификата может потребоваться перезапуск браузера для очистки кеша текущей сессии подключения к Kaspersky IoT Secure Gateway 1000.

Не рекомендуется загружать широко известные сертификаты удостоверяющего центра, так как доверенными будут являться все серверы, использующие сертификаты, подписанные этими сертификатами удостоверяющего центра. Такая ситуация может привести к компрометации Kaspersky IoT Secure Gateway 1000.

Использование USB-токенов

Вы можете использовать USB-токены с длиной ключа сертификата равной 4096 бит или 8192 бит для подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.

Чтобы использовать USB-токен:

1. Подключите USB-токен к компьютеру, с которого будет осуществляться доступ к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.
2. Установите программное обеспечение, поставляемое для поддержки работы с USB-токеном.
3. Экспортируйте сертификат токена, используя это программное обеспечение.
4. Загрузите экспортированный сертификат в Kaspersky IoT Secure Gateway 1000 в качестве сертификата администратора или пользователя, как описано ниже.

Обновление корневого сертификата

Перед обновлением корневого сертификата, необходимо загрузить архив .p12 с сертификатом администратора, подписанным новым корневым сертификатом в браузер, с помощью которого осуществляется доступ. Инструкцию по загрузке сертификата вы можете найти в документации браузера.

Обновление корневого сертификата невозможно в браузере Mozilla Firefox начиная с версии 124. Подробнее о поддерживаемых браузерах см. "Аппаратные и программные требования".

Чтобы обновить данные корневого сертификата:

1. Если новый корневой сертификат хранится на USB-накопителе или токене, подключите его к компьютеру, с которого вы подключены к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.
2. В меню в левой части страницы веб-интерфейса выберите раздел **Пользователи** → **Параметры пользователей**.
3. В блоке **Корневой сертификат** нажмите на кнопку **Обновить сертификат**.
4. В окне обновления сертификата нажмите на кнопку **Выбрать сертификат** и в открывшемся окне выберите файл действующего корневого сертификата.

   Для добавления в качестве сертификата доступны файлы только в формате CRT, CER, DER и PEM. Хеш сертификата будет загружен в Kaspersky IoT Secure Gateway 1000.
5. Дождитесь успешной загрузки и нажмите на кнопку **Сохранить**.

Информация о загруженном корневом сертификате и срок его действия отобразятся в блоке **Корневой сертификат**. После этого вам нужно обновить сертификаты администратора и пользователя на подписанные новым корневым сертификатом.

После обновления корневого сертификата, сертификат администратора нужно обновить не завершая сессии подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.

Обновление сертификата администратора

Чтобы обновить данные сертификата администратора:

1. Если новый сертификат администратора хранится на USB-накопителе или токене, подключите его к компьютеру, с которого вы подключены к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.
2. В меню в левой части страницы веб-интерфейса выберите раздел **Пользователи** → **Параметры пользователей**.
3. Если новый сертификат администратора подписан другим корневым сертификатом, загрузите необходимый корневой сертификат по инструкции выше.

   В этом случае вам также потребуется обновить сертификат пользователя, чтобы пользователь мог подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.
4. В блоке **Администратор** нажмите на кнопку **Обновить сертификат**.

5. В окне обновления сертификата нажмите на кнопку **Выбрать сертификат** и в открывшемся окне выберите файл действующего сертификата администратора.

   Для добавления в качестве сертификата доступны файлы только в формате CRT, CER, DER и PEM. Хеш сертификата будет загружен в Kaspersky IoT Secure Gateway 1000.

6. Дождитесь успешной загрузки и нажмите на кнопку **Сохранить**.

Информация о сертификате администратора будет обновлена, информация о загруженном ранее сертификате будет удалена. Сессия подключения будет завершена, вам нужно повторно подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.

После обновления сертификата администратора, если вы также обновили корневой сертификат, необходимо удалить из браузера сертификат администратора, подписанный старым корневым сертификатом. Инструкцию по удалению сертификата вы можете найти в документации браузера.

Обновление сертификата пользователя

Чтобы обновить данные сертификата пользователя:

1. Если новый сертификат пользователя хранится на USB-накопителе или токене, подключите его к компьютеру, с которого вы подключены к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.

2. В меню в левой части страницы веб-интерфейса выберите раздел **Пользователи** → **Параметры пользователей**.

3. Если новый сертификат пользователя подписан другим корневым сертификатом, загрузите необходимый корневой сертификат по инструкции выше.

4. В блоке **Пользователь** нажмите на кнопку **Обновить сертификат**.

5. В окне обновления сертификата нажмите на кнопку **Выбрать сертификат** и в открывшемся окне выберите файл действующего сертификата пользователя.

   Для добавления в качестве сертификата доступны файлы только в формате CRT, CER, DER и PEM. Хеш сертификата будет загружен в Kaspersky IoT Secure Gateway 1000.

6. Дождитесь успешной загрузки и нажмите на кнопку **Сохранить**.

Информация о сертификате пользователя будет обновлена, информация о загруженном ранее сертификате будет удалена. Пользователь сможет использовать обновленный сертификат для подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000.

Настройка веб-сервера

Работу веб-интерфейса Kaspersky IoT Secure Gateway 1000 обеспечивает веб-сервер CivetWeb. Параметры веб-сервера хранятся в конфигурационном файле, безопасность подключения обеспечивает сертификат веб-сервера. Kaspersky IoT Secure Gateway 1000 поставляется с предустановленным сертификатом веб-сервера, который подписан "Лабораторией Касперского".

Требуется обновлять сертификаты веб-сервера в следующих случаях:

- текущие сертификаты скомпрометированы;

- изменился IP-адрес Kaspersky IoT Secure Gateway 1000.

После первого подключения требуется заменить сертификат веб-сервера, установленный по умолчанию, на сертификат, используемый в вашей организации.

Чтобы загрузить новый сертификат веб-сервера:

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

   Откроется страница, на которой отображается информация сертификате и ключе веб-сервера.

2. Выполните одно из следующих действий:

   - Если у вас не добавлен сертификат, нажмите на кнопку **Загрузить сертификат**.
   - Если у вас уже добавлен сертификат и вы хотите его заменить, нажмите на значок карандаша в правом верхнем углу блока информации о сертификате.

3. В открывшемся окне **Загрузка сертификата веб-сервера** выполните следующие действия:

   a. В поле **Сертификат** нажмите **Выбрать сертификат** и в открывшемся окне загрузки выберите файл сертификата в формате CRT, CER, DER или PEM.

   Убедитесь, что при генерации сертификата веб-сервера в параметре subjAltName указан IP-адрес Kaspersky IoT Secure Gateway 1000 в локальной сети.

   b. В поле **Ключ сертификата** нажмите **Выбрать ключ сертификата** и в открывшемся окне загрузки выберите файл ключа в формате KEY.

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

4. Обновите страницу, чтобы новый сертификат вступил в силу.

Если у вас уже были загружены сертификат и ключ, они будут заменены.

В разделе **Пользователи** → **Параметры веб-сервера** отобразится следующая информация об используемом сертификате:

- Имя файла сертификата и его формат;
- **Имя субъекта** – информация о программе, для которой выпущен сертификат;
- **Издатель** – информация об организации, выпустившей сертификат;
- **Срок действия сертификата** – дата окончания действия сертификата.

Настройка параметров сети

Kaspersky IoT Secure Gateway 1000 поставляется со статически настроенным IP-адресом – 192.168.1.1, который вы можете изменить при необходимости. Чтобы система могла работать в качестве безопасного шлюза Интернета вещей, требуется выполнить настройку параметров внутренней и внешней сети.

Вы также можете настроить следующие параметры сети для передачи данных:

- трансляция сетевого адреса, или *маскарадинг* (включить или выключить);
- профиль модема для работы сотового соединения на устройстве с Kaspersky IoT Secure Gateway 1000 (если модем подключен к устройству);
- маршрутизация для более гибкого управления сетевыми пакетами, которые проходят через устройство с Kaspersky IoT Secure Gateway 1000;
- MQTT-брокер для обмена данными телеметрии по протоколу MQTT (Message Queuing Telemetry Transport).

Вы можете просматривать и изменять параметры сети Kaspersky IoT Secure Gateway 1000 в разделе **Сеть** на соответствующих вкладках.

Этот функционал доступен только администратору.

Настройка параметров внутренней сети

Внутренняя сеть – это сеть организации, в которой датчики передают системе телеметрические данные. Внутренняя сеть Kaspersky IoT Secure Gateway 1000 может быть использована для выполнения следующих задач:

- подключение к веб-интерфейсу Kaspersky IoT Secure Gateway 1000;
- отправка журналов событий на внутренний сервер Syslog;
- взаимодействие с устройствами внутренней сети, подключенными к Kaspersky IoT Secure Gateway 1000 (например, датчики, сенсоры).

При изменении IP-адреса Kaspersky IoT Secure Gateway 1000 во внутренней сети, сеанс подключения к веб-интерфейсу будет завершен, вам потребуется повторно подключиться к Kaspersky IoT Secure Gateway 1000 по новому IP-адресу.

При изменении маски подсети Kaspersky IoT Secure Gateway 1000 во внутренней сети необходимо заново настроить параметры внутренней сети.

При включении или выключении функции **Использовать DHCP-сервер** требуется перезагрузить Kaspersky IoT Secure Gateway 1000.

Чтобы настроить параметры внутренней сети:

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

2. На вкладке **Внутренняя сеть** укажите значения следующих параметров:

   - **IP-адрес**. По умолчанию этот параметр имеет значение 192.168.1.1.
   - **Маска подсети**. По умолчанию этот параметр имеет значение 255.255.255.0.

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

3. Если требуется для устройств во внутренней сети настраивать параметры сети автоматически по протоколу DHCP, установите переключатель **Использовать DHCP-сервер** в положение включено и укажите значения для следующих параметров:

   - **Начало диапазона IP-адресов**.
   - **Конец диапазона IP-адресов**.
   - **Адрес основного DNS-сервера**. По умолчанию этот параметр имеет значение 8.8.8.8.
   - **Адрес дополнительного DNS-сервера**. По умолчанию этот параметр имеет значение 8.8.4.4.

   По умолчанию переключатель **Использовать DHCP-сервер** включен.

4. Если требуется для устройств во внутренней сети настраивать параметры сети вручную, установите переключатель **Использовать DHCP-сервер** в положение выключено.

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

6. Перезагрузите Kaspersky IoT Secure Gateway 1000, чтобы изменения параметров сети вступили в силу.

Настройка маскарадинга

Вы можете настроить трансляцию сетевых адресов с помощью функции маскарадинга.

Маскарадинг (англ. Masquerading) – тип трансляции сетевого адреса, при котором адрес отправителя во внутренней сети подменяется динамически в зависимости от адреса, назначенного интерфейсу, на адрес во внешней сети. Вы можете использовать функцию маскарадинга, если для устройств во внутренней сети требуется подмена параметров в заголовках IP-пакетов, а также для скрытия инфраструктуры за одним адресом. Это позволит устройствам, расположенным во внутренней сети и не имеющим реальных IP-адресов, отправлять и получать IP-пакеты из внешней сети.

Чтобы включить маскарадинг:

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

2. На вкладке **Внешняя сеть** в блоке **Параметры трансляции** установите переключатель **Включить маскарадинг** в положение включено.

   Маскарадинг будет применен только для канала связи, назначенного основным (внешняя сеть или модем).

Настройка параметров внешней сети

Внешняя сеть – это сеть, через которую Kaspersky IoT Secure Gateway 1000 выходит в интернет или взаимодействует с Kaspersky Security Center. Внешняя сеть Kaspersky IoT Secure Gateway 1000 может быть использована для выполнения следующих задач:

- настройка взаимодействия Kaspersky IoT Secure Gateway 1000 с Kaspersky Security Center;
- отправка журналов событий на внешний сервер Syslog.

Чтобы настроить параметры внешней сети:

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

     Если при включении автоматического получения параметров внешней сети DHCP-сервер выдал Kaspersky IoT Secure Gateway 1000 нулевые адреса DNS-серверов, то подключение к ресурсам и маршрутизация по доменному имени будет недоступны. В этом случае вам нужно отключить автоматическое получение параметров сети по DHCP и задать адреса основного и дополнительного DNS-серверов вручную.

   - Если требуется настроить параметры сети вручную, установите переключатель **Автоматическое получение (по DHCP)** в положение выключено и укажите значения для следующих параметров:
     - **IP-адрес**. По умолчанию этот параметр имеет значение последнего адреса, полученного от сервера DHCP. Если такой адрес отсутствует, то этот параметр имеет значение IP-адреса внутренней сети (по умолчанию, 192.168.1.1).
     - **Маска подсети**. По умолчанию этот параметр имеет значение 255.255.255.0.
     - **Шлюз**.
     - **Адрес основного DNS-сервера**.
     - **Адрес дополнительного DNS-сервера**.

     В поле **MAC-адрес** отображается MAC-адрес системы во внешней сети.
3. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.
4. Перезагрузите Kaspersky IoT Secure Gateway 1000, чтобы изменения параметров сети вступили в силу.

Настройка параметров сотового соединения

Если в устройстве отсутствует модем, использование сотового соединения недоступна, и параметры сотового соединения скрыты.

Работу сотового соединения на устройстве с Kaspersky IoT Secure Gateway 1000 обеспечивает модем HUAWEI ME909s-120 или SIMCom SIM7600. Параметры сотового соединения хранятся в профиле модема. Kaspersky IoT Secure Gateway 1000 поставляется с предустановленными профилями модема, в которые входит конфигурационный файл, содержащий базовые скрипты для настройки параметров сотового соединения. Также конфигурационный файл профиля модема содержит AT-команды для модема, обеспечивающие установку и поддержку соединения, а также описание параметров настройки протокола PPP (англ. Point-to-Point Protocol).

Вы можете просматривать и настраивать параметры сотового соединения в разделе **Сеть → Внешняя сеть**. Раздел содержит блок параметров **Параметры модема**, в котором представлена следующая информация о сотовом соединении:

- статус работы модема и текущий уровень сигнала;
- блок **Адреса DNS-серверов модема**, в котором указаны IP-адреса основного и дополнительного DNS-серверов модема;
- таблица **Профили**, в которой отображается информация о доступных профилях модема.

Kaspersky IoT Secure Gateway 1000 также позволяет создавать новые профили модема, изменять существующие профили и переключаться между профилями. Разные профили модема позволяют работать с разными операторами сотовой связи. Для использования сотового соединения требуется, чтобы один из профилей модема был активным. По умолчанию активным является один из предустановленных профилей модема.

Таблица профилей модема

В системе предусмотрено два типа профилей модема:

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

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

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

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

- – доступ на изменение конфигурационного файла. Значок, информирующий о том, что конфигурационный файл доступен только для чтения, отображается только для конфигурационного файла предустановленного профиля.

- **Тип** – тип конфигурационного файла.
- **Имя** – имя конфигурационного файла.
- **Изменен** – дата и время последнего изменения конфигурационного файла.

Включение и выключение сотового соединения

Kaspersky IoT Secure Gateway 1000 позволяет обрабатывать исходящий и входящий сетевой трафик с использованием сотового соединения (через оператора сотовой связи).

Чтобы включить или выключить использование сотового соединения на устройстве с Kaspersky IoT Secure Gateway 1000:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Сеть**.
2. Выберите вкладку **Внешняя сеть** и в блоке **Параметры модема** включите или выключите использование модема с помощью переключателя **Использовать модем как основной канал связи**.
3. Нажмите на кнопку **Сохранить**, чтобы сохранить изменение параметров.

Создание профиля модема

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

Чтобы создать новый профиль модема:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Сеть**.
2. Выберите вкладку **Внешняя сеть**.
3. В блоке параметров **Параметры модема** нажмите на кнопку **Создать** в нижней части страницы.

   Справа откроется панель **Создание профиля модема**.
4. В раскрывающемся списке **Шаблон** выберите профиль модема, на базе которого вы хотите создать новый профиль. Конфигурационный файл модема выбранного профиля добавится в новый профиль.

   Если вы хотите создать пустой профиль, в раскрывающемся списке **Шаблон** выберите **Пустой**. Вы можете заполнить пустой профиль модема позже.
5. В поле **Имя** введите имя профиля латинскими буквами.
6. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Новый профиль модема будет создан и отобразится в таблице **Профили**.

Копирование профиля модема

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

Чтобы копировать созданный ранее профиль модема:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Сеть**.
2. Выберите вкладку **Внешняя сеть**.
3. В нижней части окна в таблице **Профили** в столбце **Имя** нажмите на имя профиля, на основе которого вы хотите создать новый профиль.

   Справа откроется панель **Изменение профиля модема**.
4. Нажмите на значок , расположенный в нижней части панели.

   Откроется панель **Копирование профиля модема**.
5. В поле **Новое имя** введите имя нового профиля латинскими буквами.
6. Нажмите на кнопку **Копировать** в нижней части панели.

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

Заполнение пустого профиля модема

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

Чтобы заполнить пустой профиль модема:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Сеть**.
2. Выберите вкладку **Внешняя сеть**.
3. В блоке **Параметры модема** в таблице **Профили** нажмите на значок плюса в столбце **Имя** рядом с именем пустого профиля.

   Отобразится таблица **Параметры профиля**.
4. Нажмите на кнопку **Создать файл**, чтобы создать конфигурационный файл модема.
5. В открывшейся справа панели **Создание конфигурационного файла модема** в поле **Имя** введите имя конфигурационного файла латинскими буквами.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить конфигурационный файл модема.

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

   Конфигурационный файл загрузится в систему и отобразится в параметрах профиля.

Мы не рекомендуем загружать или создавать более одного файла конфигурации в профиле модема. При загрузке или создании нового файла уже загруженный файл конфигурации будет перезаписан.

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

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

9. В нижней части панели нажмите на значок карандаша .

   Откроется окно текстового редактора для изменения конфигурационного файла.

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

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

Изменение профиля модема

Вы можете изменять имя и параметры профиля модема.

Чтобы изменить имя профиля модема:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Сеть**.
2. Выберите вкладку **Внешняя сеть**.
3. В блоке параметров **Параметры модема** в таблице **Профили** в графе **Имя** нажмите на имя профиля, который вы хотите изменить.

   Справа откроется панель **Изменение профиля модема**.

4. В поле **Имя** введите новое имя профиля.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменение параметров.

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

Чтобы изменить параметры профиля модема:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Сеть**.
2. Выберите вкладку **Внешняя сеть**.
3. В блоке **Параметры модема** в таблице **Профили** нажмите на значок плюса в столбце **Имя** рядом с профилем, который вы хотите изменить.

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

4. Если требуется изменить конфигурационный файл, нажмите на имя конфигурационного файла и в открывшейся справа панели **Изменение конфигурационного файла модема** выполните следующие действия:

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

b. В открывшемся окне текстового редактора измените параметры модема на те, которые требуются.

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

Выбранный конфигурационный файл будет изменен. Окно текстового редактора закроется.

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

   Выбранный конфигурационный файл будет удален из параметров профиля модема.

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

   Конфигурационный файл загрузится в систему и отобразится в параметрах профиля.

> Мы не рекомендуем загружать или создавать более одного файла конфигурации в профиле модема. При загрузке или создании нового файла уже загруженный файл конфигурации будет перезаписан.

Переключение на другой профиль модема

Kaspersky IoT Secure Gateway 1000 позволяет переключаться между профилями модема. Разные профили модема позволяют работать с разными операторами сотовой связи. По умолчанию активным является один из предустановленных профилей модема.

Чтобы переключиться на другой профиль модема:

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

2. Выберите вкладку **Внешняя сеть**.

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

   Справа откроется панель **Изменение профиля модема**.

4. В нижней части панели нажмите на кнопку **Сделать активным**.

5. Перезагрузите Kaspersky IoT Secure Gateway 1000, чтобы изменения вступили в силу.

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

Удаление профиля модема

Вы можете удалить профиль модема.

Kaspersky IoT Secure Gateway 1000 не позволяет удалить активный и предустановленные профили модема. Если требуется удалить профиль, который сейчас является активным, сначала нужно переключиться на другой профиль модема.

Чтобы удалить профиль модема:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Сеть**.
2. Выберите вкладку **Внешняя сеть**.
3. В блоке параметров **Параметры модема** в таблице **Профили** в столбце **Имя** нажмите на имя профиля, который вы хотите удалить.

   Справа откроется панель **Изменение профиля модема**.
4. Нажмите на значок , расположенный в нижней части панели и подтвердите удаление профиля.

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

Настройка маршрутизации

Для более гибкого управления сетевыми пакетами, которые проходят через устройство с Kaspersky IoT Secure Gateway 1000, вы можете настроить маршрутизацию. *Маршрутизация* – процесс определения маршрута данных в сетях связи.

Передача данных с помощью статических маршрутов для внутренней сети возможна только для типа сетевого устройства *сетевой роутер*.

В разделе **Сеть** на вкладке **Маршрутизация** отображается таблица маршрутизации Kaspersky IoT Secure Gateway 1000. Для каждого маршрута в таблице отображается следующая информация:

- **Тип** – тип маршрута:
  - **Статический** – маршрут, для которого вручную определены параметры следования сетевых пакетов.
  - **Динамический** – маршрут, для которого параметры следования сетевых пакетов определяются автоматически, например с помощью DHCP-сервера.
- **IP-адрес** – IP-адрес сети или узла назначения.
- **Маска** – маска сети назначения.
- **Шлюз** – IP-адрес шлюза в сети, на который нужно передать трафик, следующий до указанного IP-адреса сети или узла назначения.
- **Состояние** – состояние маршрута:
  - **Активный** – маршрут применен и используется для передачи данных.
  - **Ошибка** – маршрут не применен и не может использоваться для передачи данных, так как при создании маршрута была допущена ошибка. Справа от состояния отображается описание ошибки.

Состояние **Ошибка** отображается, если IP-адрес шлюза в сети недостижим или в качестве назначения были указаны недопустимые IP-адрес сети (узла назначения) или маска сети.

- **Ожидание** – промежуточное состояние, которое присваивается, если маршрут был создан через Kaspersky Security Center 14.2 Web Console. После проверки корректности параметров маршрута текущее состояние изменится на **Активный** или **Ошибка**.

- **Изменение** и **Удаление** – действия, которые вы можете выполнить для выбранного маршрута. Изменение и удаление доступно только для статических маршрутов.

Также вы можете создавать, изменять и удалять маршруты Kaspersky IoT Secure Gateway 1000.

Таблица маршрутизации обновляется автоматически каждые 30 секунд. Новые маршруты, которые были созданы через Kaspersky Security Center 14.2 Web Console, отображаются в таблице после ее обновления. Если требуется, вы можете выполнить принудительное обновление таблицы маршрутизации, нажав на кнопку **Обновить таблицу**.

Создание статического маршрута

Вы можете создавать новые статические маршруты, которые позволят направлять сетевой трафик так, как этого требует инфраструктура вашей организации.

Kaspersky IoT Secure Gateway 1000 не позволяет создавать дублирующие маршруты по умолчанию (второй маршрут для IP-адреса сети назначения 0.0.0.0/0) и маршруты, в которых в качестве IP-адреса узла назначения указан IP-адрес, принадлежащий сети 127.0.0.0/8.

При создании пересекающихся маршрутов, рекомендуется учитывать, что для отправки сетевого пакета на IP-адрес сети или узла назначения будет выбираться маршрут с более длинной маской, описывающей меньшее количество узлов назначения.

Чтобы создать новый статический маршрут:

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

2. Выберите вкладку **Маршрутизация**.

   Отобразится окно, в нижней части которого содержится таблица маршрутов Kaspersky IoT Secure Gateway 1000.

3. Нажмите на кнопку **Добавить маршрут**.

4. В открывшемся окне **Добавление маршрута** укажите следующие данные:

   - В поле **IP-адрес** введите IP-адрес сети или узла назначения.

   - В поле **Маска** введите маску сети назначения.

   - В поле **Шлюз** введите IP-адрес шлюза. IP-адрес шлюза должен быть достижимым.

     IP-адрес шлюза является достижимым, если этот IP-адрес расположен в подключенной сети и является одним из узлов сети, настроенной на внутреннем или внешнем интерфейсе.

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

Новый статический маршрут будет создан и отобразится в таблице маршрутов.

Изменение статического маршрута

Чтобы изменить статический маршрут:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Сеть**.
2. Выберите вкладку **Маршрутизация**.

   Отобразится окно с таблицей маршрутов Kaspersky IoT Secure Gateway 1000.
3. Для маршрута, который вы хотите изменить, в столбце **Изменение** нажмите на значок .
4. В открывшемся окне **Изменение маршрута** внесите изменения и нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Статический маршрут будет изменен и новые данные по нему отобразятся в таблице маршрутизации.

Удаление статического маршрута

Чтобы удалить статический маршрут:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Сеть**.
2. Выберите вкладку **Маршрутизация**.

   Отобразится окно с таблицей маршрутов Kaspersky IoT Secure Gateway 1000.
3. Для маршрута, который вы хотите удалить, в столбце **Удалить** нажмите на значок и подтвердите удаление.

Статический маршрут будет удален из таблицы маршрутизации.

Настройка параметров MQTT-брокера

Настройка параметров MQTT-брокера доступна только для типа сетевого устройства *сетевой роутер*.

В Kaspersky IoT Secure Gateway 1000 MQTT-брокер Eclipse Mosquitto обеспечивает обмен данными телеметрии по протоколу MQTT (Message Queuing Telemetry Transport). Параметры MQTT хранятся в профиле MQTT-брокера. Профиль MQTT-брокера представляет собой связку из конфигурационного файла Eclipse Mosquitto и сертификатов безопасности. Kaspersky IoT Secure Gateway 1000 поставляется с предустановленным профилем, в который входит конфигурационный файл MQTT-брокера. Kaspersky IoT Secure Gateway 1000 позволяет создавать новые профили, изменять существующие профили и переключаться между профилями. Для передачи данных по протоколу MQTT требуется, чтобы один из профилей MQTT-брокера был активным. По умолчанию активным является предустановленный профиль.

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

При настройке параметров MQTT-брокера содержимое конфигурационного файла может содержать персональные данные. Вам нужно контролировать данные, загружаемые в профиль MQTT-брокера Kaspersky IoT Secure Gateway 1000.

Таблица профилей MQTT-брокера

В Kaspersky IoT Secure Gateway 1000 предусмотрено два типа профилей MQTT-брокера:

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

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

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

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

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

Создание профиля MQTT-брокера

Вы можете создавать новые профили MQTT-брокера. Разные профили MQTT-брокера позволяют работать с разными серверами и цифровыми платформами, которые принимают события от Kaspersky IoT Secure Gateway 1000 по протоколу MQTT.

Чтобы создать новый профиль MQTT-брокера:

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

Отобразится таблица, в которой перечислены профили MQTT-брокера.

2. Нажмите на кнопку **Создать** в нижней части страницы.

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

3. В раскрывающемся списке **Шаблон** выберите профиль MQTT-брокера, на базе которого вы хотите создать новый профиль.

   Конфигурационный файл Eclipse Mosquitto и сертификаты безопасности выбранного профиля добавятся в новый профиль.

   Если вы хотите создать пустой профиль, в раскрывающемся списке **Шаблон** выберите **Пустой**. Вы можете заполнить пустой профиль позже.

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

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

Новый профиль MQTT-брокера будет создан и отобразится в таблице профилей. Вы также можете создать профиль MQTT-брокера через Kaspersky Security Center 14.2 Web Console.

Копирование профиля MQTT-брокера

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

Чтобы копировать созданный ранее профиль MQTT-брокера:

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

   Отобразится таблица, в которой перечислены профили MQTT-брокера.

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

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

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

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

4. В поле **Новое имя** введите новое имя профиля латинскими буквами.

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

Новый профиль MQTT-брокера на основе созданного ранее профиля будет создан и отобразится в таблице профилей. Конфигурационный файл Eclipse Mosquitto и сертификаты безопасности выбранного профиля добавятся в новый профиль.

Заполнение пустого профиля MQTT-брокера

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

Чтобы заполнить пустой профиль MQTT-брокера:

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

   Отобразится таблица, в которой перечислены профили MQTT-брокера.

2. В столбце **Имя** нажмите на значок ⊞, расположенный рядом с профилем, который требуется заполнить.

   Отобразится таблица **Параметры профиля**.

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

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

   > Профиль MQTT-брокера требует несколько сертификатов безопасности: сертификат, выданный удостоверяющим центром, клиентский сертификат сервера и файл закрытого ключа. В зависимости от требований MQTT-сервера клиентский сертификат сервера и файл закрытого ключа должны быть подписаны действующим сертификатом удостоверяющего центра. Если ваш профиль предполагает использование защищенного соединения SSL/TLS, повторите этот шаг столько раз, сколько требуется, чтобы загрузить в систему все необходимые сертификаты. Без сертификатов безопасности не гарантируется работа защищенного соединения.

   > Мы не рекомендуем загружать более трех файлов сертификатов безопасности в MQTT-профиль. При загрузке более трех файлов будут использоваться последние загруженные файлы сертификатов.

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

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

5. В поле **Имя** введите имя конфигурационного файла латинскими буквами.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить конфигурационный файл Eclipse Mosquitto MQTT-брокера.

   Панель **Создание конфигурационного файла MQTT-брокера** закроется. Конфигурационный файл будет создан. Вы можете создать только один конфигурационный файл.

   > Вы можете создать только один конфигурационный файл. Если его требуется заменить, вам нужно удалить действующий файл конфигурации и создать его заново. Вы можете сделать активным только профиль MQTT, для которого добавлен конфигурационный файл.

7. В таблице **Параметры профиля** нажмите на имя только что созданного конфигурационного файла.

8. В нижней части открывшейся справа панели **Изменение конфигурационного файла MQTT-брокера** нажмите на значок ✎.

   Откроется окно текстового редактора для изменения конфигурационного файла.

9. Введите в окне текстового редактора требуемые параметры конфигурационного файла Eclipse Mosquitto MQTT-брокера.

   Подробную информацию о параметрах конфигурационного файла Eclipse Mosquitto MQTT-брокера вы можете узнать в документации на веб-сайте разработчика. Настройка MQTT-брокера в Kaspersky IoT Secure Gateway 1000 доступна с ограничениями.

10. Если требуется добавить в профиль готовый конфигурационный файл, нажмите на кнопку **Загрузить** в нижней части страницы и в открывшемся окне загрузки файла в систему выберите файл в формате CONF.

    Конфигурационный файл загрузится в систему и отобразится в параметрах профиля MQTT-брокера.

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

Изменение профиля MQTT-брокера

Вы можете изменять имя и параметры профиля MQTT-брокера.

Kaspersky IoT Secure Gateway 1000 не позволяет изменить предустановленный профиль MQTT-брокера.

Для профиля, который сейчас назначен активным, можно изменить только имя. Если требуется изменить параметры активного профиля, сначала нужно переключиться на другой профиль MQTT-брокера.

Чтобы изменить имя профиля MQTT-брокера:

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

    Отобразится таблица, в которой перечислены профили MQTT-брокера.

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

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

3. В поле **Имя** введите новое имя профиля.

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

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

Чтобы изменить параметры профиля MQTT-брокера:

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

    Отобразится таблица, в которой перечислены профили MQTT-брокера.

2. В столбце **Имя** нажмите на значок ⊞, расположенный рядом с профилем, который вы хотите изменить.

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

    Если профиль активный или предустановленный, изменение его параметров недоступно. Для активного профиля можно изменить только его имя.

3. Если требуется добавить в профиль готовый конфигурационный файл, нажмите на кнопку **Загрузить** в нижней части страницы и в открывшемся окне загрузки файла в систему выберите файл в формате CONF.

    Конфигурационный файл загрузится в систему и отобразится в параметрах профиля MQTT-брокера.

4. Если требуется изменить имя конфигурационного файла, нажмите на имя конфигурационного файла и в открывшейся справа панели **Изменение конфигурационного файла MQTT-брокера** укажите новое имя в поле **Имя** и нажмите на кнопку **Сохранить**.

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

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

   b. В открывшемся окне текстового редактора измените параметры на те, которые требуются.

   > Подробную информацию о параметрах конфигурационного файла Eclipse Mosquitto вы можете узнать в документации на веб-сайте разработчика. Настройка профиля MQTT-брокера в Kaspersky IoT Secure Gateway 1000 доступна с ограничениями.

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

   Выбранный конфигурационный файл будет изменен. Окно текстового редактора закроется.

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

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

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

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

   > Профиль MQTT-брокера требует несколько сертификатов безопасности: сертификат, выданный удостоверяющим центром, клиентский сертификат сервера и файл закрытого ключа. В зависимости от требований MQTT-сервера клиентский сертификат сервера и файл закрытого ключа должны быть подписаны действующим сертификатом удостоверяющего центра. Если ваш профиль предполагает использование защищенного соединения SSL/TLS, повторите этот шаг столько раз, сколько требуется, чтобы загрузить в систему все необходимые сертификаты. Без сертификатов безопасности не гарантируется работа защищенного соединения.

   > Мы не рекомендуем загружать более трех файлов сертификатов безопасности в MQTT-профиль. При загрузке более трех файлов будут использоваться последние загруженные файлы сертификатов.

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

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

Переключение на другой профиль MQTT-брокера

Kaspersky IoT Secure Gateway 1000 позволяет переключаться между профилями MQTT-брокера. В Kaspersky IoT Secure Gateway 1000 разные профили MQTT-брокера позволяют работать с разными серверами и цифровыми платформами при получении от них данных телеметрии по протоколу MQTT. По умолчанию активным является предустановленный профиль MQTT-брокера.

Вы можете сделать профиль MQTT-брокера активным, только если в профиле есть конфигурационный файл.

Чтобы переключиться на другой профиль MQTT-брокера:

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

   Отобразится таблица, в которой перечислены профили MQTT-брокера.

2. В столбце **Имя** нажмите на имя профиля, который вы хотите сделать активным.

   Откроется окно **Изменение профиля MQTT-брокера**.

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

В таблице профилей в столбце **Активный** рядом с выбранным профилем появится значок , профиль станет активным и будет использоваться Kaspersky IoT Secure Gateway 1000 при получении данных по протоколу MQTT.

Удаление профиля MQTT-брокера

Kaspersky IoT Secure Gateway 1000 позволяет удалять профили MQTT-брокера.

Kaspersky IoT Secure Gateway 1000 не позволяет удалить активный и предустановленный профили MQTT-брокера. Если требуется удалить профиль, который сейчас является активным, сначала нужно переключиться на другой профиль MQTT-брокера.

Чтобы удалить профиль MQTT-брокера:

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

   Отобразится таблица, в которой перечислены профили MQTT-брокера.

2. В столбце **Имя** нажмите на имя профиля, который вы хотите удалить.

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

3. Нажмите на значок , расположенный в нижней части панели и подтвердите удаление профиля.

Выбранный профиль MQTT-брокера будет удален из таблицы профилей.

Ограничения при настройке MQTT-брокера

Соединение с локальными устройствами осуществляется без использования протокола TLS. Соединение с устройствами, которые находятся во внешней сети, осуществляется с использование протокола TLS.

Kaspersky IoT Secure Gateway 1000 поддерживает настройку параметров MQTT-брокера Eclipse Mosquitto со следующими ограничениями:

- Не допускается использование параметров `capath`, `bridge_capath` и `include_dir` для назначения пути расположения файлов.
- Не допускается использование протокола TLS для конфигурации соединения оборудования с Kaspersky IoT Secure Gateway 1000.

  Для настройки соединения с Kaspersky IoT Secure Gateway 1000 из внутренней сети не поддерживаются следующие параметры: `cafile`, `certfile`, `ciphers_tls1.3`, `crlfile`, `dhparamfile`, `keyfile`, `require_certificate`, `tls_engine`, `tls_engine_kpass_sha1`, `tls_keyform`, `use_identity_as_username`, `use_subject_as_username`, `psk_hint`.
- Для соединения Kaspersky IoT Secure Gateway 1000 с устройствами или облачными сервисами во внешней сети требуется использование только протокола TLS.

  Для настройки соединения не поддерживаются следующие параметры: `bridge_insecure` (всегда `false`), `bridge_alpn`, `bridge_capath`, `bridge_cafile`, `bridge_certfile`, `bridge_keyfile`, `bridge_identity`, `bridge_psk`, `bridge_require_ocsp`, `bridge_tls_version`.
- Для каждого профиля MQTT-брокера возможно соединение только с одним клиентским приложением (возможно указать только один параметр `bridge` в конфигурационном файле). Одновременная работа с несколькими клиентскими соединениями не поддерживается. Для установки соединения с другим клиентом требуется переключиться на другой профиль MQTT-брокера.
- При настройке профиля MQTT-брокера не поддерживаются следующие параметры: `bridge_require_ocsp`, `log_dest file`, `pid_file`, `http_dir`, `persistence`, `websockets`, `auth_plugin`, `password_file`.
- При настройке профиля MQTT-брокера требуется использовать параметр `allow_anonymous`.
- Для соединения MQTT-брокера с цифровой платформой, поддерживающей протокол MQTT, требуется указывать стандартный порт для подключения – 8883.
- Для соединения конечного устройства с Kaspersky IoT Secure Gateway 1000 требуется использовать порт 1883.

Фильтрация трафика прикладных протоколов

Вы можете настроить фильтрацию сетевого трафика прикладных протоколов через веб-интерфейс Kaspersky IoT Secure Gateway 1000. Фильтрация позволяет заблокировать или разблокировать сетевой трафик, проходящий на уровне прикладных протоколов FTP, HTTP, MQTT, Modbus, SMTP, IMAP, POP3.

Для протокола MQTT поддерживается только фильтрация версии 3.1.1. Для протокола SMTP поддерживается фильтрация только базового SMTP, и не поддерживается фильтрация протокола Extended SMTP.

Чтобы настроить фильтрацию трафика прикладных протоколов:

1. В меню в левой части экрана выберите раздел **Сеть** → **Фильтрация**.
2. Настройте фильтрацию трафика прикладных протоколов, выполнив следующие действия:
   - Установите флажок напротив тех протоколов, для которых вы хотите заблокировать прохождение трафика.
   - Снимите флажок напротив тех протоколов, для которых вы хотите разрешить прохождение трафика.

   По умолчанию трафик разрешен для всех прикладных протоколов.
3. Нажмите на кнопку **Сохранить**.

Kaspersky IoT Secure Gateway 1000 заблокирует весь трафик для выбранных прикладных протоколов, кроме служебного трафика, а также разрешит прохождение трафика на уровне прикладных протоколов, для которых вы сняли флажок.

При получении пакета трафика, содержащего признаки заблокированного прикладного протокола, Kaspersky IoT Secure Gateway 1000 разрывает соединение, по которому проходил обмен этим трафиком. При этом после обнаружения трафика несколько пакетов, необходимые для установления соединения, могут пройти через Kaspersky IoT Secure Gateway 1000, но затем соединение будет разорвано.

Добавление имени устройства

Чтобы задать имя устройства:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Общие**.
2. В поле **Имя устройства** введите имя.

   Имя устройства может содержать только цифры и латинские буквы. Максимальная длина имени – 32 символа.
3. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Настройка даты и времени

В Kaspersky IoT Secure Gateway 1000 вы можете настроить дату и время.

Чтобы настроить дату и время:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Общие**.
2. В блоке **Дата и время** укажите текущие дату и время:
   - Нажмите на дату и в выпадающем календаре выберите текущие день, месяц и год.

     Вы можете перейти к выбору месяца или года, нажав на дату в верхней части календаря.

- Нажмите на время и в выпадающем циферблате выберите текущее время (часы и минуты).

  Укажите текущее время в часовом поясе UTC+00:00. Время будет отображаться в соответствии с часовым поясом устройства.

3. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Настройка отправки уведомлений при регистрации событий

Этот раздел содержит информацию о настройке отправки уведомлений при регистрации событий в Kaspersky IoT Secure Gateway 1000.

Настройка отправки журналов событий на сервер Syslog

Kaspersky IoT Secure Gateway 1000 может отправлять журналы событий аудита сетевого экрана и аудита системы на сервер Syslog.

Чтобы настроить отправку журналов событий аудита сетевого экрана и аудита системы на сервер Syslog:

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

2. В блоке параметров **Syslog** установите переключатель **Использовать сервер Syslog для передачи событий** в положение включено.

3. Настройте параметры отправки журналов событий, указав следующие параметры:

   - В поле **IP-адрес и порт** введите IP-адрес и порт стороннего сервера Syslog, например `198.51.100.0:514`.

   - В раскрывающемся списке **Режим** выберите протокол, по которому Kaspersky IoT Secure Gateway 1000 будет передавать журналы событий на сторонний сервер Syslog:

     - **UDP**.

     - **TCP**.

     - **TCP/TLS**.

   - Если для отправки журналов выбран протокол **TCP/TLS**, загрузите сертификат безопасности. Для этого нажмите на кнопку **Загрузить новый сертификат** и в открывшемся окне выберите нужный сертификат безопасности.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Настройка отправки MQTT-уведомлений

Kaspersky IoT Secure Gateway 1000 может отправлять уведомления о событиях аудита сетевого экрана и аудита системы по протоколу MQTT.

Чтобы настроить отправку MQTT-уведомлений:

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

      Для соединения Kaspersky IoT Secure Gateway 1000 с MQTT-брокером, который находится во внутренней сети вы можете использовать порты 1883 и 8883.

      Для соединения Kaspersky IoT Secure Gateway 1000 с MQTT-брокером, который находится во внешней сети вы можете использовать порт 8883.

   c. В поле **Имя MQTT-топика** укажите имя MQTT-топика для отправки уведомлений о событиях.
   d. Если требуется отправлять уведомления о событиях от имени определенного пользователя, установите переключатель **Использовать аутентификацию** в положение включено и укажите следующие данные:
      - В поле **Имя пользователя** введите имя учетной записи пользователя для авторизации на сервере.
      - В поле **Пароль** введите пароль учетной записи пользователя для авторизации на сервере.

        Учетные данные пользователя вы можете получить у администратора системы. По умолчанию отправка от имени определенного пользователя выключена.

   e. Если требуется использовать защищенное SSL-соединение, установите переключатель **Использовать защищенное SSL-соединение** в положение включено и выполните следующие действия:
      1. Загрузите сертификат удостоверяющего центра. Для этого нажмите на кнопку **Загрузить сертификат** и выберите файл сертификата на локальном устройстве.

         Информация о загруженном сертификате удостоверяющего центра отобразится на странице.

         Не рекомендуется загружать широко известные сертификаты удостоверяющего центра, так как доверенными будут являться все серверы, использующие сертификаты, подписанные этими сертификатами удостоверяющего центра. Такая ситуация может привести к компрометации Kaspersky IoT Secure Gateway 1000.

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

         Информация о загруженном сертификате клиента отобразится на странице.

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

         По умолчанию использование защищенного SSL-соединения выключено.

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

Настройка параметров Сервера администрирования Kaspersky Security Center

Этот раздел содержит информацию об управлении сертификатами и настройке параметров подключения к Серверу администрирования Kaspersky Security Center.

Создание сертификата Сервера администрирования Kaspersky Security Center

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

Сертификат сервера Kaspersky Security Center требуется для безопасного подключения к Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console. Подробную информацию о требованиях, которые предъявляются к сертификатам сервера Kaspersky Security Center, см. в разделе *Требования к пользовательским сертификатам, используемым в Kaspersky Security Center* в онлайн-справке Kaspersky Security Center 14.2.

Вы можете выпустить новый сертификат сервера Kaspersky Security Center в Kaspersky Security Center 14.2 Web Console.

Чтобы выпустить новый сертификат сервера Kaspersky Security Center через Kaspersky Security Center 14.2 Web Console:

1. В главном окне Kaspersky Security Center 14.2 Web Console нажмите на значок рядом с именем нужного Сервера администрирования Kaspersky Security Center.

   Откроется окно **Свойства Сервера администрирования**.

2. Перейдите в раздел **Сертификаты**.

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

4. Нажмите на кнопку **Перевыпустить**.

5. В открывшемся окне настройте адрес подключения:

   - **Оставить адрес подключения прежним**

     Адрес Сервера администрирования, к которому подключается Kaspersky IoT Secure Gateway 1000, останется прежним.

     По умолчанию выбран этот вариант.

   - **Изменить адрес подключения на**

Если необходимо, чтобы Kaspersky IoT Secure Gateway 1000 подключался по другому адресу, укажите в поле требуемый адрес.

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

Новый сертификат сервера Kaspersky Security Center будет выпущен.

Для загрузки файла сертификата Kaspersky Security Center в Kaspersky IoT Secure Gateway 1000 требуется сохранить на локальном компьютере созданный через веб-интерфейс Kaspersky Security Center 14.2 Web Console файл сертификата Kaspersky Security Center.

Чтобы сохранить файл сертификата Kaspersky Security Center, созданный в Kaspersky Security Center 14.2 Web Console:

1. В меню веб-интерфейса Kaspersky Security Center 14.2 Web Console нажмите на значок рядом с именем нужного Сервера администрирования Kaspersky Security Center.

   Откроется окно **Свойства Сервера администрирования**.

2. Перейдите в раздел **Сертификаты**.

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

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

5. В открывшейся справа панели в блоке **Адрес подключения** нажмите на IP-адрес Kaspersky IoT Secure Gateway 1000, для которого был выпущен сертификат.

Начнется автоматическая загрузка файла сертификата.

В Kaspersky IoT Secure Gateway 1000 возможно загрузить файл сертификата Kaspersky Security Center только в формате CRT, CER, DER и PEM. Если требуется, вы можете изменить формат файла сертификата Kaspersky Security Center, используя утилиту OpenSSL. Например, для изменения формата файла сертификата с P12 на CRT в консоли выполните команду:

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

Созданный файл сертификата сервера Kaspersky Security Center нужно добавить в Kaspersky IoT Secure Gateway 1000 для настройки соединения с Kaspersky Security Center.

Обновление сертификата Сервера администрирования Kaspersky Security Center

Требуется обновлять сертификат сервера Kaspersky Security Center в следующих случаях:

- текущий сертификат скомпрометирован;
- закончился срок действия сертификата;
- изменился IP-адрес устройства с Kaspersky IoT Secure Gateway 1000;

- нужно выполнить регулярное обновление сертификата в соответствии с требованиями информационной безопасности вашей организации.

Не рекомендуется загружать широко известные сертификаты удостоверяющего центра, так как доверенными будут являться все серверы, использующие сертификаты, подписанные этими сертификатами удостоверяющего центра. Такая ситуация приведет к компрометации Kaspersky IoT Secure Gateway 1000.

Чтобы добавить или удалить сертификат:

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

   На странице **Сервер администрирования Kaspersky Security Center** в блоке параметров **Сертификат** отобразятся данные о текущем сертификате Сервера администрирования Kaspersky Security Center, если загружен.

2. В блоке **Сертификат** выполните одно из следующих действий:

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

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

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

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

     Если в системе отсутствует сертификат сервера Kaspersky Security Center, настройка параметров подключения к серверу Kaspersky Security Center и подключение к серверу Kaspersky Security Center недоступны.

Настройка параметров подключения к Kaspersky Security Center

Для безопасного управления Kaspersky IoT Secure Gateway 1000 из Kaspersky Security Center 14.2 Web Console требуется настроить параметры подключения к серверу администрирования Kaspersky Security Center.

Если в системе отсутствует сертификат сервера Kaspersky Security Center, настройка параметров подключения к серверу администрирования Kaspersky Security Center недоступна.

Чтобы настроить параметры подключения к серверу администрирования Kaspersky Security Center:

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

   Откроется страница настройки параметров подключения **Сервер администрирования Kaspersky Security Center**.

2. В блоке **Параметры подключения** в поле **Доменный адрес** укажите доменный адрес сервера администрирования Kaspersky Security Center, к которому осуществляется подключение.

В поле **Порт** указан номер порта, по которому осуществляется подключение. Вы не можете изменить номер порта подключения.

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

Ручное изменение конфигурации Kaspersky IoT Secure Gateway 1000

Вы можете просматривать, а также напрямую изменять конфигурацию Kaspersky IoT Secure Gateway 1000. Параметры конфигурации в текстовом виде представляют собой пары `ключ: значение` в формате JSON. Список основных ключей конфигурации указан в таблице ниже.

Чтобы просмотреть и изменить конфигурацию Kaspersky IoT Secure Gateway 1000, выполните следующие действия:

1. В веб-интерфейсе Kaspersky IoT Secure Gateway 1000 перейдите на вкладку **Параметры** → **Конфигурация**.

   В открывшейся вкладке отобразится актуальная конфигурация Kaspersky IoT Secure Gateway 1000 в формате JSON.

2. Если необходимо, измените значения параметров в поле конфигурации.

   > Поля и параметры в поле конфигурации чувствительны к регистру. При добавлении или изменении полей или параметров вам нужно соблюдать указанный регистр.

3. Нажмите на кнопку **Сохранить**, чтобы применить новые параметры конфигурации.

Ручное изменение конфигурации может повлечь сбои в работе Kaspersky IoT Secure Gateway 1000 вплоть до необходимости полной переустановки. Рекомендуется изменять параметры конфигурации с помощью соответствующих параметров в веб-интерфейсе Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center Web Console.

Основные ключи конфигурации

Имя ключа	Тип значения	Описание	Обязательный	Возможн
`ABOUT`	Объект	Объект, содержащий информацию о версии Kaspersky IoT Secure Gateway 1000 и версии SDK.	Да	-
`text`	Строка	Информация о версиях.	Нет	Строка с верси Secure Gateway SDK, например: `"Kaspersky\n` `Gateway**\n\` `3.0.0.0\n\nKa` `version: 3.0.`
`<Имя пакета приложения>`	Объект	Информация о	Нет	Имя пакета из п

			конфигурации приложения. Требуется только для приложений, содержащих конфигурацию.		других парамет приложениями. Например, `kaspersky.ki` для приложени Secure Gatewa Protector.
	`<Любое имя>`	Любой тип	Содержимое конфигурации приложения.	Нет	Значения конф приложения.
`APPLICATIONS`		Объект	Информация об установленных приложениях.	Да	Объект APPLIC
`MARKETPLACE`		Объект	Объект, содержащий список приложений, доступных для установки.	Да	Заполняется ав данными из маг приложений.
	`apps_requested`	Список строк	Список приложений, доступных в магазине.	Нет	
	`package_id`	Строка	Идентификатор пакета приложения.	Да, если `apps_requesred` содержит хотя бы одну запись	
	`requested_state`	Строка	Запрашиваемое действие от приложения.		
	`buildSdkVersion`	Строка	Версия платформы.		
	`kosappversion`	Строка	Версия приложения.		
`MODE_SWITCH`		Объект	Объект, содержащий информацию о текущем состоянии режимов работы Kaspersky IoT Secure Gateway 1000 и типе сетевого устройства.	Нет	-
	`is_developer_mode`	Литерал	Режим разработчика.	Нет	`true` – режим р активен, `false` разработчика н
	`is_no_secure_mode`	Литерал	Небезопасный режим.	Нет	`true` – небезоп активен, `false` режим не актив
	`router_mode`	Литерал	Тип сетевого	Нет	`true` – тип устр

			устройства. Смена типа сетевого устройства возможна только с помощью переустановки Kaspersky IoT Secure Gateway 1000.		роутер, `false` - однонаправле
`MQTT`			Объект	Объект, содержащий параметры MQTT-брокера.	Да	Список объект MQTT/LIST/pro
	`LIST`		Объект			
		`profileList`	Список объектов	Список объектов, содержащий параметры профиля MQTT-брокера.		
`NETWORK`			Объект	Объект, содержащий параметры сети.	Да	Объект NETWO
`SETTINGS`			Объект	Объект, содержащий общие параметры Kaspersky IoT Secure Gateway 1000.	Да	Объект SETTIN

Объект APPLICATIONS

Ручное изменение конфигурации может повлечь сбои в работе Kaspersky IoT Secure Gateway 1000 вплоть до необходимости полной переустановки. Рекомендуется изменять параметры конфигурации с помощью соответствующих параметров в веб-интерфейсе Kaspersky IoT Secure Gateway 1000 и веб-плагине управления Kaspersky IoT Secure Gateway 1000 для Kaspersky Security Center 14.2 Web Console.

Объект `APPLICATIONS` включает в себя ключи, содержащие информацию об установленных приложениях, а также параметры их работы в Kaspersky IoT Secure Gateway 1000. Список этих ключей указан в таблице ниже.

Список ключей объекта APPLICATIONS

Имя ключа			Тип значения	Описание	Обязательный	Возмо значе
`APPS_CONTROL`			Объект	Объект, содержащий список установленных приложений и их параметров.	Да	-
	`applications`		Список	Список объектов,	Да	-

			объектов	содержащий параметры приложений.		
		`configured`	Литерал	Флаг, отражающий, сконфигурировано приложение или нет.	Нет	`true` – приложен сконфигур `false` – приложен сконфигур
		`execute`	Литерал	Флаг, отвечающий за запуск приложения.	Да, если `applications` содержит хотя бы одну запись	`true` – приложен запущено приложен будет зап
		`restart_on_failure`	Литерал	Флаг, отвечающий за режим перезапуска приложения при неожиданном завершении.		`true` – ре перезапус активен, `f` режим перезапус активен.
		`state`	Целое число	Состояние приложения.	Нет	`0` – приложе запускает `1` – приложе запущено `4` – приложе остановле `5` – приложе останавли
		`subtype`	Строка	Подтип приложения.		Получаетс автоматич данных приложен
		`ksc_plugin_ui_content`	Строка	Содержимое для отображения в веб-плагине управления Kaspersky Security Center 14.2 Web Console.		
		`ksc_plugin_md5`	Строка	Контрольная сумма содержимого для отображения в веб-плагине управления		

				Kaspersky Security Center 14.2 Web Console.		
		`manifest`	Строка	Содержимое манифеста приложения.		
		`package_id`	Строка	Имя пакета приложения.	Да, если `applications` содержит хотя бы одну запись	
		`launchRule`	Строка	Правило запуска приложения.		`forbidde` приложен запрещен запуска, `a` приложен функцию автозапус – для прил нет особь запуска.
		`logLevel`	Целое число	Текущий уровень журналирования сообщений приложения.	Да	`0` – критич сообщени сообщени ошибках, предупре сообщени информац сообщени отладочны сообщени сообщени действиях приложен Каждый следующи уровень журналир включает сообщени предыдущ уровня.
		`version`	Строка	Версия приложения.	Нет	Получаетс автоматич данных приложен
		`name`	Строка	Имя приложения.		
		`type`	Строка	Тип приложения.		
`APPS_ROUTING`			Объект	Объект, содержащий список доступных маршрутов приложений.	Да	-
	`routes`		Список объектов	Список маршрутов.	Да	-
		`active`	Литерал	Флаг, отражающий	Да, если `routes`	`true` – ма

				активность маршрута.	содержит хотя бы одну запись	активен, `f` маршрут неактивен
		`destination`		Объект	Объект назначения маршрута.	-
			`application_id`	Строка	Идентификатор приложения	Получается автоматич данных приложен
			`endpoint`	Строка	Имя конечной точки приложения.	
		`source`		Объект	Объект источника маршрута.	-
			`application_id`	Строка	Идентификатор приложения.	Получается автоматич данных приложен
			`endpoint`	Строка	Имя конечной точки приложения.	

Параметры приложений, которые содержат конфигурацию, настраиваются в отдельных объектах, соответствующих значению параметра `package_id`. Например, параметры фильтрации трафика промышленных протоколов для приложения Kaspersky IoT Secure Gateway Network Protector находятся в объекте `kaspersky.kisg.netprotector`.

Список объектов MQTT/LIST/profileList

Ручное изменение конфигурации может повлечь сбои в работе Kaspersky IoT Secure Gateway 1000 вплоть до необходимости полной переустановки. Рекомендуется изменять параметры конфигурации с помощью соответствующих параметров в веб-интерфейсе Kaspersky IoT Secure Gateway 1000 и веб-плагине управления Kaspersky IoT Secure Gateway 1000 для Kaspersky Security Center 14.2 Web Console.

Список объектов `MQTT/LIST/profileList` включает в себя ключи, содержащие параметры профиля MQTT-брокера. Список этих ключей указан в таблице ниже.

Список ключей для описания экземпляра профиля MQTT-брокера в списке объектов MQTT/LIST/profileList

Имя ключа		Тип значения	Описание	Обязательный	Возможные значения
`fileList`		Список объектов	Список файлов профиля.	Да, если `profileList` содержит хотя бы одну запись	-
	`fileContent`	Строка	Содержимое файла профиля в кодировке Base64.	Да, если `fileList` содержит	Получается автоматически из файла.

	`name`	Строка	Имя файла профиля.	хотя бы одну запись	Получается автоматически из пути до файла.
	`type`	Строка	Тип файла профиля.		`main_conf_file` – главный конфигурационный файл, `cert_file` – файл, содержащий сертификат, `key_file` – файл, содержащий ключ.
	`uuid`	Строка	Уникальный идентификатор файла профиля.	Нет	Строковое представление `boost::uuids::uuid`.
`locked`		Строка	Профиль заблокирован.	Нет	Определяется автоматически на основе полей `predefined` и `status`.
`modified`		Строка	Дата и время последнего изменения профиля.	Да	Получается автоматически из файла.
`name`		Строка	Имя профиля.	Да	Произвольное строковое значение.
`predefined`		Литерал	Предварительно определенный.	Да	`true` – профиль является предопределенным, `false` – профиль является пользовательским.
`status`		Строка	Статус профиля.	Да	`active` – профиль активен, `inactive` – профиль не активен.
`uuid`		Строка	Уникальный идентификатор профиля.	Нет	Строковое представление `boost::uuids::uuid`.

Объект NETWORK

Ручное изменение конфигурации может повлечь сбои в работе Kaspersky IoT Secure Gateway 1000 вплоть до необходимости полной переустановки. Рекомендуется изменять параметры конфигурации с помощью соответствующих параметров в веб-интерфейсе Kaspersky IoT Secure Gateway 1000 и веб-плагине управления Kaspersky IoT Secure Gateway 1000 для Kaspersky Security Center 14.2 Web Console.

Объект `NETWORK` включает в себя ключи, содержащие параметры сети. Список этих ключей указан в таблице ниже.

Список ключей объекта NETWORK

Имя ключа	Тип значения	Описание	Обязательный	Возможны
`APP_PROTO`	Объект	Параметры фильтрации сетевых протоколов.	Да	-

	`filtered_protos`		Объект	Объект, содержащий информацию о фильтрации сетевых протоколах.	Да	-
		`ftp`	Литерал	Фильтрация протокола FTP.	Да	`true` – фильтра протокола вклю фильтрация про выключена.
		`http`	Литерал	Фильтрация протокола HTTP/HTTPS.	Да	
		`imap`	Литерал	Фильтрация протокола IMAP.	Да	
		`modbus`	Литерал	Фильтрация протокола Modbus.	Да	
		`mqtt`	Литерал	Фильтрация протокола MQTT. Поддерживается только фильтрация протокола MQTT версии 3.1.1.	Да	
		`pop3`	Литерал	Фильтрация протокола POP3.	Да	
		`smtp`	Литерал	Фильтрация протокола SMTP. Поддерживается фильтрация только базового протокола SMTP.	Да	
`CARP`			Объект	Параметры сетевого кластера.	Да	-
	`advskew`		Целое число	Приоритет Kaspersky IoT Secure Gateway 1000 в кластере.	Да	От `0` до `254`, гд максимальный `254` – минимал приоритет.
	`clusterId`		Строка	Идентификатор кластера. Требуется для того, чтоб узлы кластера могли однозначно распознавать друг друга.	Да	Идентификатор Для избежания идентификатор рекомендуем у пользовательск идентификатор

			Использование идентификатора не гарантирует защиту от действий третьих лиц. При создании сети вам нужно также обеспечить безопасность сетевого контура кластера.			
	`enabled`	Литерал	Включение и отключение функции сетевого кластера.	Да		`true` – функция кластера включ функция сетево выключена.
	`ip`	Строка	IP-адрес кластера.	Да		Строка в форма `XXX.XXX.XXX.X` `"ip": "192.1`
	`mask`	Строка	Маска подсети кластера.	Да		Строка в форма `XXX.XXX.XXX.X` `"mask": "255`
`FIREWALL`		Объект	Правила сетевого экрана.	Да		-
	`rules`	Список объектов	Список правил сетевого экрана. Максимальный размер списка – 512 объектов.	Да		-
		`status`	Литерал	Включение и отключение правила сетевого экрана.	Да, если `rules` содержит хотя бы одну запись	`true` – правило включено, `false` – правило выключено.
		`action`	Строка	Тип правила.		`accept` – разрешающее правило, `deny` – запрещающее правило.
		`ipAddrSource`	Строка	IP-адрес источника.		Строка в формате `XXX.XXX.XXX.XXX`, например: `"ipAddrSource": "192.168.110.125"`.
		`ipAddrDest`	Строка	IP-адрес получателя.		Строка в формате `XXX.XXX.XXX.XXX`, например: `"ipAddrDest": "192.168.110.126"`.
		`portSource`	Строка	Порт источника.		Число, определяющее порт источника.
		`portDest`	Строка	Порт получателя.		Число, определяющее порт

						получателя.
		`protocol`	Строка	Протокол взаимодействия.		Доступные значения для задания в правиле: `any`, `icmp`, `tcp`, `udp`.
		`zone`	Строка	Зона действия правила.		Доступные значения для задания в правиле: `In`, `Out`.
`IDS_PROXY`			Объект	Параметры списков запрещенных и разрешенных адресов. Используется только при наличии установленного приложения Kaspersky IoT Secure Gateway Network Protector.	Да	-
	`IPSFlag`		Литерал	Включение и отключение списков запрещенных и разрешенных адресов.	Да	`true` – списки `false` – списки
	`IPSStatusFlag`		Литерал	Флаг статуса функционирования списков запрещенных и разрешенных адресов.	Нет	Всегда `true`.
	`blockedList`		Список объектов	Список запрещенных адресов.	Да	-

		`ipAddrSource`	Строка	Запрещенный IP-адрес.	Да, если `blockedList` содержит хотя бы одну запись	Строка в форм
						`XXX.XXX.XXX.X`
						`"ipAddrSourc`
						`"192.168.1.2`

		`timestamp`	Дата и время	Метка времени.		Метка времени POSIX-времени
		`signatureName`	Строка	Имя сигнатуры, по которой был установлен запрет.		Имя сигнатуры.
	`blockedListFlag`		Литерал	Включение и отключение доступа к ресурсам из списка запрещенных адресов.	Да	`true` – доступ выключен, `fals` ресурсам вклю

	`allowList`		Список объектов	Список разрешенных адресов.	Да	-
		`ipAddrSource`	Строка	Разрешенный IP-адрес.	Да, если `allowList` содержит хотя бы одну запись	Строка в форма `XXX.XXX.XXX.X` `"ipAddrSource` `"192.168.1.26`
`LAN`			Объект	Параметры внутренней сети.	Да	-
	`DHCPFlag`		Литерал	Включение и отключение автоматического получения IP-адреса с помощью протокола DHCP.	Да	`true` – автомат получение IP-ад включено, `fals` автоматическо IP-адреса выкл
	`FirstDHCPAddress`		Строка	Основной IP-адрес DHCP-сервера.	Да	Строка в форма `XXX.XXX.XXX.X` `"FirstDHCPAd` `"192.168.1.26`
	`FirstDNSServer`		Строка	Основной IP-адрес DNS-сервера.	Да	Строка в форма `XXX.XXX.XXX.X` `"FirstDNSServ` `"192.168.1.26`
	`IP`		Строка	IP-адрес сетевого адаптера внутренней сети.	Да	Строка в форма `XXX.XXX.XXX.X` `"IP": "192.1`
	`LastDHCPAddress`		Строка	Дополнительный IP-адрес DHCP-сервера.	Да	Строка в форма `XXX.XXX.XXX.X` `"LastDHCPAddr` `"192.168.1.46`
	`MAC`		Строка	MAC-адрес сетевого адаптера внутренней сети.	Нет	Строка в форма `XX:XX:XX:XX:X` например: `"MAC` `"1A:2B:3C:4D:`
	`Mask`		Строка	Маска внутренней подсети.	Да	Строка в форма `XXX.XXX.XXX.X` `"Mask": "255`
	`SecondDNSServer`		Строка	Дополнительный IP-адрес DNS-сервера.	Да	Строка в форма `XXX.XXX.XXX.X` `"SecondDNSSer` `"192.168.1.46`
`NAPT`			Объект	Правила маскарадинга.	Да	-
	`rules`		Список объектов	Список правил маскарадинга. Максимальный размер списка – 256 правил.	Да	-
		`comment`	Строка	Комментарий к правилу.	Да, если `rules` содержит хотя бы одну запись	Произвольная с

		`ipAddrInternal`	Строка	IP-адрес внутреннего хоста.		Строка в форма `XXX.XXX.XXX.` `"ipAddrInter` `"192.168.1.4`
		`portExternal`	Целое число	Внешний порт.		Число, определ внешний порт.
		`portInternal`	Целое число	Внутренний порт.		Число, определ внутренний пор
		`protocol`	Строка	Протокол правила.		Доступные зна задания в прави
		`zone`	Строка	Интерфейс, к которому применяется правило.		Доступные зна задания в прави `wan`.
`NAT`			Объект	Включение и отключение маскарадинга.	Да	-
	`masquerading`		Литерал		Да	`true` – маскара `false` – маскар выключен.
`ROUTING_TABLE`			Объект	Таблица маршрутизации.	Да	-
	`routes`		Список объектов	Список маршрутов.	Да	-
		`action`	Строка	Действие для маршрута.	Да, если `routes` содержит хотя бы одну запись	`add` – добавить маршрут, `delete` – удалить маршрут, `no action` – действие не требуется.
		`ipaddr`	Строка	IP-адрес.	Да, если `routes` содержит хотя бы одну запись и значение ключа `action` не равно `no action`	Строка в формате `XXX.XXX.XXX.XXX`, например: `"ipaddr": "192.168.2.1"`.
		`mask`	Строка	Маска подсети.		Строка в формате `XXX.XXX.XXX.XXX`, например: `"mask": "255.255.255.0"`.
		`gateway`	Строка	IP-адрес шлюза.		Строка в формате `XXX.XXX.XXX.XXX`, например: `"gateway": "192.168.1.100"`.
		`state`	Строка	Состояние маршрута.	Нет	`failed` – ошибка при выполнении действия с маршрутом, `active` – маршрут активен, `pending` – выполняется действие с маршрутом.

		`type`	Строка	Тип маршрута.	Нет	`static` – статический маршрут, `dynamic` – динамический маршрут.
		`error`	Строка	Сообщение об ошибке.	Нет	Сообщение об ошибке при выполнении действия с маршрутом.
`WAN`			Объект	Параметры внешней сети.	Да	-
	`DHCPFlag`		Литерал	Включение и отключение автоматического получения IP-адреса с помощью протокола DHCP.	Да	`true` – автомат получение IP-а включено, `fals` автоматическо IP-адреса выкл
	`DefaultGateway`		Строка	IP-адрес шлюза по умолчанию.	Да	Строка в форм `XXX.XXX.XXX.` `"DefaultGate` `"192.168.1.1`
	`FirstDNSAddress`		Строка	Основной IP-адрес DNS-сервера.	Да	Строка в форм `XXX.XXX.XXX.` `"FirstDNSSer` `"8.8.8.8"`.
	`IP`		Строка	IP-адрес сетевого адаптера внешней сети.	Да	Строка в форм `XXX.XXX.XXX.` `"IP": "192.1`
	`MAC`		Строка	MAC-адрес сетевого адаптера внешней сети.	Нет	Строка в форм `XX:XX:XX:XX:` например: `"MA` `"1A:2B:3C:4D`
	`Mask`		Строка	Маска внешней подсети.	Да	Строка в форм `XXX.XXX.XXX.` `"Mask": "255`
	`SecondDNSAddress`		Строка	Дополнительный IP-адрес DNS-сервера.	Да	Строка в форм `XXX.XXX.XXX.` `"SecondDNSSe` `"8.8.4.4"`.

Объект SETTINGS

Ручное изменение конфигурации может повлечь сбои в работе Kaspersky IoT Secure Gateway 1000 вплоть до необходимости полной переустановки. Рекомендуется изменять параметры конфигурации с помощью соответствующих параметров в веб-интерфейсе Kaspersky IoT Secure Gateway 1000 и веб-плагине управления Kaspersky IoT Secure Gateway 1000 для Kaspersky Security Center 14.2 Web Console.

Объект `SETTINGS` включает в себя ключи, содержащие общие параметры Kaspersky IoT Secure Gateway 1000. Список этих ключей указан в таблице ниже.

Список ключей объекта SETTINGS

Имя ключа	Тип значения	Описание	Обязательный	Возм
`AUTH_CERTS`	Объект	Информация о сертификатах пользователей, приложений, веб-сервера и Kaspersky Security Center.	Да	-
`certificate_admin`	Строка	Сертификат администратора.		Base6 предс серти
`certificate_admin_name`	Строка	Имя сертификата администратора.		Имя ф содер серти
`certificate_app_ca`	Строка	Корневой сертификат приложений.		Base6 предс серти
`certificate_app_ca_name`	Строка	Имя корневого сертификата приложений.		Имя ф содер серти
`certificate_app_cl`	Строка	Клиентский сертификат приложений		Base6 предс серти
`certificate_app_cl_key`	Строка	Ключ клиентского сертификата приложений.		Base6 предс
`certificate_app_cl_key_name`	Строка	Имя ключа клиентского сертификата приложений.		Имя ф содер
`certificate_app_cl_name`	Строка	Имя клиентского сертификата приложений.		Имя ф содер серти
`certificate_ksc_server`	Строка	Сертификат Kaspersky Security Center.		Base6 предс серти
`certificate_ksc_server_name`	Строка	Имя сертификата Kaspersky Security Center.		Имя ф содер серти
`certificate_web_tls`	Строка	Сертификат веб-сервера.		Base6 предс серти
`certificate_web_tls_key`	Строка	Ключ сертификата веб-сервера.		Base6 предс
`certificate_web_tls_key_name`	Строка	Имя ключа сертификата веб-		Имя ф содер

			сервера.		
	`certificate_web_tls_name`	Строка	Имя сертификата веб сервера.		Имя ф содер серти
`DEVICE`		Объект	Имя устройства.	Да	-
	`device_name`	Строка			Имя ус отобр Kaspe Cente
`KSC`		Объект	Объект, содержащий информацию о взаимодействии с Kaspersky Security Center.	Да	-
	`command`	Строка	Команда, подготовленная для отправки на Kaspersky IoT Secure Gateway 1000.	Нет	`reboo` – пере устро
	`heartbeat`	Целое число	Период синхронизации с Kaspersky Security Center в секундах.		Целое
`MODEM`		Объект	Информация о модеме и параметры для операторов связи.	Да	-
	`connection_quality`	Целое число	Показатель текущего качества связи.	Нет	Получ автом
	`connection_status`	Строка	Статус связи.	Нет	`on` – м подкл данны прису систе соеди неакти модем систе статус
	`is_enable`	Литерал	Включение и отключение модема.	Да	`true` включ модем

	`primary_dns`	Строка	Основной DNS-сервер.	Нет	Строк
					`XXX.X`
					напри
					`"prim`
					`"8.8.`

	`profileList`	Список объектов	Список профилей операторов	Да	-

				сотовой связи.		
		`fileContent`	Строка	Содержимое файла профиля.	Да	Получ автом файла
		`locked`	Строка	Указывает, заблокирован профиль для изменений или нет.	Нет	Опред основ `prede` `statu`
		`modified`	Строка	Дата и время последнего изменения профиля.	Да	Строк време
		`name`	Строка	Имя профиля.		Произ профи
		`predefined`	Литерал	Флаг, определяющий, является профиль предустановленным или нет.		`true` - предус `false` добав. пользо
		`status`	Строка	Текущий статус профиля.		`activ` активе профи
		`uuid`	Строка	Уникальный идентификатор профиля.	Нет	Строк предс `boost`
	`secondary_dns`		Строка	Дополнительный DNS-сервер.	Нет	Строк `XXX.X` напри `"seco` `"8.8.`
`MQTT_NOTIFICATION`			Объект	Параметры MQTT-уведомлений.	Да	-
	`auth_enabled`		Литерал	Включение и отключение отправки MQTT-уведомлений от имени определенного пользователя.	Да	`true` - имени включ отпра пользо выклю
	`certificate_cert`		Строка	Клиентский сертификат, соответствующий корневому сертификату.	Да, если `"certs_enable": true`	Base6 предс серти
	`certificate_key`		Строка	Клиентский ключ, соответствующий клиентскому сертификату.	Да, если `"certs_enable": true`	Base6 предс
	`certificate_root`		Строка	Корневой сертификат	Да, если `"certs_enable": true`	Base6 предс серти

			удостоверяющего центра.		
	`certs_enabled`	Литерал	Включение и отключение использования защищенного TLS-соединения для отправки MQTT-уведомлений.	Да	`true` - соеди `false` соеди выклю
	`event_topic`	Строка	Имя MQTT-топика для отправки MQTT-уведомлений.	Да	Имя М
	`login`	Строка	Имя пользователя.	Да, если `"auth_enabled": true`	Имя по
	`notifications_enabled`	Литерал	Включение и отключение отправки событий по протоколу MQTT.	Да	`true` - прото включ отпра MQTT
	`password`	Строка	Пароль пользователя.	Да, если `"auth_enabled": true`	Парол соотв имени
	`server_address`	Строка	IP-адрес MQTT-брокера.	Да	Строк `XXX.X` напри `"serv "192.`
	`server_port`	Целое число	Порт MQTT-брокера.	Да	Для со Kaspe Gatew броке находи внутре может порты внешн
`SYSLOG`		Объект	Параметры отправки журнала syslog.	Да	-
	`certificate`	Строка	Содержимое сертификата безопасности для передачи событий по протоколу `TCP/TLS`.		Base6 предс серти
	`enable`	Литерал	Включение и отключение сервера syslog для отправки событий.		`true` - серве отпра включ

					испол syslog событ

	`host`	Строка	IP-адрес сервера syslog.		Строк
					`XXX.X`
					напри
					`"192.`

	`mode`	Строка	Протокол передачи событий.		`"tcp"` событ TCP, `"` событ UDP, `"` событ TCP с испол соеди
	`port`	Целое число	Порт сервера syslog.		Порт с
`TIME`		Объект	Текущие дата и время. Доступно только для чтения.	Да	-

	`date`	Строка	Текущая дата.	Нет	Дата в
					`"YYYY`
					напри
					`"2023`

	`time`	Строка	Текущее время.	Нет	Время
					`"HH:M`
					напри
					`"23:5`

`UPDATE`		Объект	Информация об обновлениях.	Да	-
	`firmware_update_start`	Литерал	Запуск процедуры обновления Kaspersky IoT Secure Gateway 1000.		`true` запущ обнов значе умолч

Настройка фильтрации трафика промышленных протоколов

Вы можете настроить правила для блокировки и фильтрации трафика, проходящего на уровне промышленных протоколов, с помощью приложения Kaspersky IoT Secure Gateway Network Protector через параметры конфигурации Kaspersky IoT Secure Gateway 1000. Фильтрация трафика промышленных протоколов осуществляется с помощью правил анализа содержимого сетевых пакетов и включает следующие проверки:

- фильтрация команд в протоколах MQTT и Modbus;
- проверка на аномалии трафика на уровне протоколов MQTT и Modbus.

Для работы приложения Kaspersky IoT Secure Gateway Network Protector вам нужно сначала настроить его конфигурацию. Если вы запустите приложение без настроенных параметров конфигурации, Kaspersky IoT Secure Gateway 1000 перейдет в аварийный режим, так как приложение не может получить правила фильтрации трафика для обеспечения безопасного состояния.

Чтобы настроить правила фильтрации трафика промышленных протоколов:

1. С помощью утилиты Kaspersky Update Utility скачайте файлы со списками поддерживаемых правил анализа содержимого сетевых пакетов:

   - Файл industrial_commands.rules содержит список поддерживаемых правил фильтрации команд на уровне промышленных протоколов.
   - Файл industrial_anomalies.rules содержит список поддерживаемых правил обнаружения аномалий в трафике, проходящем на уровне промышленных протоколов.

   Идентификатор (sid) 90000001 используется для служебных нужд и не может быть присвоен ни одному правилу.

   Подробную информацию по работе с утилитой вы можете узнать в документации по Kaspersky Update Utility.

2. Если необходимо, выберите из файлов те правила, которые вы хотите применить для фильтрации трафика промышленных протоколов.

3. Закодируйте список правил фильтрации команд и список правил обнаружения аномалий как две отдельные строки в кодировке Base64.

4. Остановите приложение Kaspersky IoT Secure Gateway Network Protector, если оно запущено.

   Пока приложение Kaspersky IoT Secure Gateway Network Protector остановлено, транзитный трафик на устройстве будет заблокирован для обеспечения безопасности подключенных устройств.

5. В меню в левой части экрана веб-интерфейса выберите раздел **Параметры** → **Конфигурация**.

6. В поле конфигурации в блоке `kaspersky.kisg.netprotector` добавьте объект `"APP_CONFIGURATION": {}`.

7. Внутри объекта `APP_CONFIGURATION` укажите следующие параметры, чтобы включить и настроить фильтрацию трафика промышленных протоколов:

   - Добавьте параметр `"industrial_commands_rules": ""` и укажите для него список правил в кодировке Base64 для фильтрации команд на уровне промышленных протоколов.
   - Добавьте параметр `"industrial_anomaly_rules": ""` и укажите для него список правил в кодировке Base64 для обнаружения аномалий в трафике, проходящем на уровне промышленных протоколов.

   В результате конфигурация параметров внутри блока `kaspersky.kisg.netprotector` будет выглядеть следующим образом:

   ```
   "APP_CONFIGURATION": {
     "industrial_commands_rules": "<правила в кодировке Base64>",
     "industrial_anomaly_rules": "<правила в кодировке Base64>"
   }
   ```

Для работы приложения Kaspersky IoT Secure Gateway Network Protector требуется указать значение хотя бы одного параметра конфигурации, иначе Kaspersky IoT Secure Gateway 1000 перейдет в аварийный режим после запуска приложения, так как приложение не может получить правила фильтрации трафика для обеспечения безопасного состояния. Вы можете выключить только один из параметров, указав пустые кавычки `""` в качестве значения этого параметра.

После того, как вы добавите объект `APP_CONFIGURATION` и его параметры, вы не сможете его удалить, так как он является обязательным для работы приложения.

8. Нажмите на кнопку **Сохранить**, чтобы применить параметры конфигурации.

9. Запустите приложение Kaspersky IoT Secure Gateway Network Protector.

Сетевой трафик, проходящий на уровне промышленных протоколов, будет фильтроваться с использованием указанных правил. В случае срабатывания правила сетевой трафик, соответствующий этому правилу, будет заблокирован, а IP-адрес, от которого идет трафик, будет добавлен в список запрещенных IP-адресов. Информация о блокировке IP-адреса передается в сетевой экран Kaspersky IoT Secure Gateway 1000. Событие о блокировке трафика будет записано в журнал событий аудита.

Изменение языка веб-интерфейса Kaspersky IoT Secure Gateway 1000

Kaspersky IoT Secure Gateway 1000 позволяет выбрать язык веб-интерфейса.

Чтобы изменить язык веб-интерфейса Kaspersky IoT Secure Gateway 1000:

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

   Откроется меню пользователя.

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

Язык веб-интерфейса Kaspersky IoT Secure Gateway 1000 будет изменен на выбранный.

Также вы можете изменить язык веб-интерфейса на странице входа в Kaspersky IoT Secure Gateway 1000 или странице возобновления сеанса подключения к Kaspersky IoT Secure Gateway 1000 в верхней части страницы справа.

Решение типовых задач

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

Мониторинг состояния Kaspersky IoT Secure Gateway 1000

Сводная информация о состоянии Kaspersky IoT Secure Gateway 1000 и об устройстве под управлением Kaspersky IoT Secure Gateway 1000 отображается в разделе **Статус**. Раздел содержит следующие информационные блоки:

- Информация об устройстве, которая содержит имя устройства, его IP-адрес и идентификатор, а также версию Kaspersky IoT Secure Gateway 1000, которая установлена на устройстве.
- Тип сетевого устройства, который был выбран при установке Kaspersky IoT Secure Gateway 1000 на устройство. Возможен один из следующих типов:
  - *Сетевой роутер* – тип сетевого устройства, обеспечивающий передачу сетевых пакетов по IP-протоколу в прямом и обратном направлении (от шлюза и к шлюзу).

    Для сетевого роутера применяется политика, обеспечивающая маршрутизацию проходящего через устройство сетевого трафика.
  - *Однонаправленный шлюз* – типа сетевого устройства, обеспечивающий передачу сетевых пакетов по IP-протоколу в одном направлении и не позволяющий передачу в обратном.

    Для однонаправленного шлюза применяется политика, обеспечивающая передачу данных от устройств, расположенных во внутренней сети, во внешнюю сеть без возможности воздействия на внутренние ресурсы со стороны внешней сети.
- Статус подключения к Серверу администрирования Kaspersky Security Center.
- Ссылки для перехода к статьям в онлайн-справке Kaspersky IoT Secure Gateway 1000.

Мониторинг состояния сотового соединения

Если в устройстве отсутствует модем, использование сотового соединения недоступно, и параметры модема скрыты.

Этот функционал доступен только администратору.

Если вы хотите использовать модем как основной канал связи, предварительно требуется включить использование сотового соединения.

Вы можете следить за состоянием сотового соединения Kaspersky IoT Secure Gateway 1000 в разделе **Сеть** → **Внешняя сеть**. В блоке **Параметры модема** отображается следующая информация о состоянии сотового соединения:

- **Статус модема** – параметр, отображающий состояние сотового соединения Kaspersky IoT Secure Gateway 1000. Возможны следующие значения параметра:
  - **Подключен** – модем подключен к устройству и соединение модема с оператором сети установлено.
  - **Недоступен** – модем подключен к устройству, но соединение модема с оператором сети отсутствует.
- **Уровень сигнала** – параметр качества сотового соединения. Количество линий показывает уровень сигнала сети сотовой связи, к которой подключено устройство с Kaspersky IoT Secure Gateway 1000. При ухудшении уровня сигнала количество линий уменьшается

В блоке **Адреса DNS-серверов модема** отображается информация об IP-адресах основного и дополнительного DNS-серверов модема. В таблице **Профили** отображается информация о доступных профилях модема.

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

- Используемая в модеме SIM-карта является исправной, и подключен тариф, поддерживающий интернет-соединение через модем.
- Выбранный профиль модема соответствует используемой SIM-карте.
- Модем доступен для использования (отображается статус **Подключен**).

  Если модем недоступен для использования (отображается статус **Недоступен**) требуется перезагрузить Kaspersky IoT Secure Gateway 1000 и снова проверить доступность модема для использования.
  Устройствам, которые выходят в интернет через Kaspersky IoT Secure Gateway 1000, необходимо получать параметры внутренней сети через DHCP-сервер Kaspersky IoT Secure Gateway 1000. Нужные адреса DNS-серверов от операторов сотовой сети будут получены месте с этими параметрами.

Мониторинг событий аудита Kaspersky IoT Secure Gateway 1000

Этот раздел содержит инструкции по мониторингу событий, зарегистрированных в Kaspersky IoT Secure Gateway 1000.

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

Kaspersky IoT Secure Gateway 1000 регистрирует следующие типы событий:

- События аудита сетевого экрана, в том числе приходящие от приложения Kaspersky IoT Secure Gateway Network Protector. Вы можете просматривать их в журнале событий в разделе **События**.
- События аудита операционной системы. Вы можете просматривать их в журнале аудита в разделе **Аудит**.

Вы также можете просматривать события аудита сетевого экрана и события аудита операционной системы через Kaspersky Security Center 14.2 Web Console. При необходимости вы также можете настроить отправку журнала событий на сервер Syslog или настроить отправку MQTT-уведомлений о регистрации событий.

Мониторинг событий аудита сетевого экрана

Этот раздел содержит инструкции по мониторингу событий аудита сетевого экрана, зарегистрированных в Kaspersky IoT Secure Gateway 1000, в том числе с помощью приложения Kaspersky IoT Secure Gateway Network Protector.

О событиях аудита сетевого экрана

В таблице ниже описаны события аудита сетевого экрана, которые регистрирует Kaspersky IoT Secure Gateway 1000 и приложение Kaspersky IoT Secure Gateway Network Protector.

События аудита сетевого экрана

Название события	Текст события	Критичность	Идентификатор субъекта
Audit: Запуск подсистемы аудита	Подсистема аудита запущена	Информационное	Система: Audit
admin: Экспорт журнала user: Экспорт журнала	Журнал экспортирован	Информационное	Администратор или пользователь
admin: Ошибка экспорта журнала user: Ошибка экспорта журнала	Не удалось экспортировать журнал	Важное	Администратор или пользователь
Audit: Перезапись журнала аудита	Журнал аудита перезаписан, так как закончилось место хранения	Информационное	Система: Audit
Audit: Заканчивается место в журнале аудита	Через `<количество записей>` записей журнал аудита будет перезаписан	Важное	Система: Audit
TrafficController: Блокировка трафика	Трафик от устройства `<IP-адрес>` заблокирован	Важное	Система: TrafficController
TrafficController: Предел создания правил для IDSProxy	Не удалось заблокировать устройство `<IP-адрес>`, так как создано предельное количество блокирующих правил (`<максимальное количество правил>`)	Критическое	Система: TrafficController
TrafficController: Изменение конфигурации правил сетевого экрана	Конфигурация правил сетевого экрана изменена	Информационное	Система: TrafficController
KscController: Изменение маршрутов приложений	Маршруты приложений изменены	Информационное	Система: KscController
Launcher: Переход Kaspersky IoT Secure Gateway Network Protector в аварийный режим	Аварийный режим активирован для приложения Kaspersky IoT Secure Gateway Network Protector	Критическое	Система: Launcher
Audit: Тестовое сообщение подсистемы аудита	Тестовое сообщение успешно записано в рамках диагностики подсистемы аудита	Информационное	Система: Audit

TrafficController: Ошибка создания маршрута	Созданный пользователем маршрут не применен: <описание>	Важное	Система: TrafficController

Просмотр журнала событий аудита сетевого экрана

Kaspersky IoT Secure Gateway 1000 сохраняет в журнале события аудита сетевого экрана, в том числе те события, которые регистрируются приложением Kaspersky IoT Secure Gateway Network Protector.

При возникновении критического события аудита в меню слева возле раздела **События** появляется *сигнализация* об этом в виде красного значка с восклицательным знаком . В этом случае обратитесь к сотруднику, ответственному за информационную безопасность в вашей организации.

Чтобы просмотреть журнал событий аудита сетевого экрана:

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

   Откроется страница **События**, которая содержит таблицу всех зарегистрированных событий аудита сетевого экрана. События в таблице обновляются автоматически каждые 30 секунд. Первыми в таблице отображаются новые события. В таблице могут отображаться до 1024 последних зарегистрированных событий. При превышении количества событий журнал перезаписывается, начиная с самых старых.

   Если язык событий аудита в таблице не соответствует языку системы, вам нужно выбрать нужный язык веб-интерфейса в меню и обновить страницу, чтобы применить изменения.

   Для каждой записи журнала отображается следующая информация:

   - **Дата и время** – дата и время регистрации события.
   - **Название события** – название зарегистрированного события.
   - **Текст события** – подробная информация о зарегистрированном событии, например об изменении параметров сетевого экрана.
   - **Идентификатор субъекта** – источник зарегистрированного события:
     - **Администратор** – событие вызвано действием администратора в системе.
     - **Пользователь** – событие вызвано действием пользователя в системе.
     - **Система** – событие вызвано действием системы. Для каждого события также отображается имя подсистемы, выполнившей событие.
   - **Критичность** – уровень критичности зарегистрированного события.

     События подразделяются по следующим уровням критичности:

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

- – *Критические*. Критические события содержат сведения, которые могут оказать критическое влияние на безопасность сети, в которой расположен Kaspersky IoT Secure Gateway 1000. Эти события требуют немедленной реакции. Критические события аудита выделены красным цветом в таблице.

2. Если требуется просмотреть события за определенную дату или период, нажмите на поле **Дата**, выберите конкретную дату или даты начала и окончания периода и нажмите на кнопку **Применить**.

   События за выбранную дату или период отобразятся в таблице.

3. Если требуется просмотреть события с определенным уровнем критичности, в верхней части таблицы в раскрывающемся списке **Критичность** выберите нужный уровень критичности и нажмите на кнопку **Применить**. Вы можете выбрать одно или несколько значений. По умолчанию отображаются события всех уровней критичности.

   События с выбранным уровнем критичности отобразятся в таблице.

4. Если требуется просмотреть события из определенных источников, в верхней части таблицы в раскрывающемся списке **Идентификатор субъекта** выберите имя нужного субъекта и нажмите на кнопку **Применить**. Вы можете выбрать одно или несколько значений. По умолчанию отображаются все зарегистрированные события.

   События из выбранных источников отобразятся в таблице.

5. Если требуется сбросить все установленные фильтры отображения событий в таблице, нажмите **Сбросить все**.

   В таблице снова отобразятся все зарегистрированные события.

6. Если требуется отобразить более старые события, нажмите на кнопку **Загрузить еще** под таблицей.

   Кнопка **Загрузить еще** доступна всегда, даже если более ранние события отсутствуют.

Экспорт журнала событий аудита сетевого экрана

Вы можете сохранить журнал событий аудита сетевого экрана на локальном компьютере.

Чтобы сохранить журнал событий аудита сетевого экрана на локальном компьютере:

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

   Откроется страница **События**, которая содержит таблицу всех зарегистрированных событий аудита сетевого экрана.

2. Нажмите на кнопку **Скачать журнал**.

3. В открывшемся окне укажите путь сохранения файла журнала событий на локальном компьютере, при необходимости задайте его имя и сохраните файл.

Журнал событий аудита сетевого экрана будет сохранен на локальном компьютере в формате CSV. Если вы применили фильтры в таблице событий аудита перед тем, как сохранить журнал, в нем будут отображаться только отфильтрованные события.

Мониторинг событий аудита операционной системы

Этот раздел содержит инструкции по мониторингу событий аудита операционной системы.

Этот функционал доступен только администратору.

О событиях аудита операционной системы

В таблице ниже описаны события аудита операционной системы, которые регистрирует Kaspersky IoT Secure Gateway 1000.

События аудита операционной системы

Название события	Текст события	Критичность	Идентификатор субъекта
Audit: Запуск подсистемы аудита	Подсистема аудита запущена	Информационное	Система: Audit
Audit: Тестовое сообщение подсистемы аудита	Тестовое сообщение успешно записано в рамках диагностики подсистемы аудита	Информационное	Система: Audit
admin: Экспорт журнала	Журнал экспортирован	Информационное	Администратор
admin: Ошибка экспорта журнала	Не удалось экспортировать журнал	Важное	Администратор
Audit: Перезапись журнала аудита	Журнал аудита перезаписан, так как закончилось место хранения	Информационное	Система: Audit
Audit: Заканчивается место в журнале аудита	Через <количество записей> записей журнал аудита будет перезаписан	Важное	Система: Audit
KscController: Перезагрузка устройства	Устройство перезагружается	Информационное	Система: KscController
KscController: Загрузка сертификата приложения	Сертификат приложения загружен в хранилище сертификатов	Информационное	Система: KscController
Launcher: Попытка запуска несовместимой версии приложения	Обнаружена попытка запуска версии приложения, которая несовместима с системой	Важное	Система: Launcher
Launcher: Попытка запуска запрещенного приложения	Обнаружена попытка запустить запрещенное приложение	Важное	Система: Launcher
Launcher: Запуск приложения	Приложение <название приложения> запущено	Информационное	Система: Launcher
Launcher: Ошибка	Не удалось запустить приложение	Важное	Система: Launcher

запуска приложения	<название приложения>		
Launcher: Недоверенное приложение	Не удалось проверить целостность приложения <название приложения>	Критическое	Система: Launcher
Launcher: Остановка приложения	Приложение <название приложения> остановлено	Информационное	Система: Launcher
Launcher: Аварийное завершение работы приложения	Приложение <название приложения> завершилось с ошибкой	Важное	Система: Launcher
Launcher: Изменение автозапуска приложений	Список приложений для автозапуска изменен	Информационное	Система: Launcher
Launcher: Ошибка изменения автозапуска приложений	Не удалось изменить список приложений для автозапуска	Важное	Система: Launcher
Launcher: Активация режима неиммунности	Устройство работает в неиммунном режиме, иммунность устройства не гарантируется	Важное	Система: Launcher
Launcher: Активация режима разработчика	Устройство работает в режиме разработчика	Важное	Система: Launcher
Launcher: Попытка скачивания новой версии приложения	Обнаружена попытка скачать новую версию установленного приложения	Критическое	Система: Launcher
Orchestrator: Скачивание приложения	Началось скачивание приложения <название приложения>	Информационное	Система: Orchestrator
Orchestrator: Успешное скачивание приложения	Приложение <название приложения> успешно скачано на устройство	Информационное	Система: Orchestrator
Orchestrator: Успешная установка приложения	Приложение <название приложения> успешно установлено	Информационное	Система: Orchestrator
Orchestrator: Удаление приложения	Началось удаление приложения <название приложения>	Информационное	Система: Orchestrator
Orchestrator: Успешное удаление приложения	Приложение <название приложения> успешно удалено	Информационное	Система: Orchestrator
Orchestrator: Ошибка скачивания приложения	Не удалось скачать приложение <название приложения>	Важное	Система: Orchestrator
Orchestrator: Ошибка проверки подписи приложения	Не удалось проверить подлинность подписи приложения <название приложения>	Критическое	Система: Orchestrator
Orchestrator: Ошибка установки приложения	Не удалось установить приложение <название приложения>	Важное	Система: Orchestrator
Orchestrator: Ошибка установки приложения	Не удалось установить приложение <название приложения>. Достигнут предел по количеству	Важное	Система: Orchestrator

	приложений, установленных на устройстве.		
Orchestrator: Ошибка удаления приложения	Не удалось удалить приложение <название приложения>	Важное	Система: Orchestrator
TrafficController: Включение сетевого кластера	Сетевой кластер включен, и его параметры настроены	Важное	Система: TrafficController
TrafficController: Выключение сетевого кластера	Сетевой кластер выключен	Важное	Система: TrafficController
EmergencyManager: Активация режима аварийной поддержки	Обнаружена критическая ошибка операционной системы. Режим аварийной поддержки активирован: <описание>	Критическое	Система: EmergencyManager
EmergencyManager: Ограничение функций операционной системы	Функции операционной системы <описание> ограничены, так как активирован режим аварийной поддержки	Критическое	Система: EmergencyManager
BlobContainer: Запрет запуска компонента	Запуск компонента <компонент> с нарушением целостности запрещен	Критическое	Система: BlobContainer
Updater: Обновление системы	Запущено полное обновление системы	Информационное	Система: Updater
Updater: Проверка обновлений	Скачанные обновления проверены и готовы к установке	Информационное	Система: Updater
Updater: Скачивание обновлений	Обновления скачаны успешно	Информационное	Система: Updater
Updater: Успешное обновление системы	Обновление системы завершено успешно	Информационное	Система: Updater
Updater: Обновление не требуется	Обновление не требуется. Установлена последняя версия системы	Информационное	Система: Updater
Updater: Ошибка обновления системы	Во время обновления системы произошла ошибка <описание>	Критическое	Система: Updater
Updater: Ошибка скачивания обновлений	Не удалось скачать обновления	Информационное	Система: Updater
Updater: Ошибка перезагрузки устройства	Не удалось перезагрузить устройство при установке обновлений	Критическое	Система: Updater
Updater: Некорректные обновления	Скачанные обновления некорректны и не могут быть установлены	Важное	Система: Updater
admin: Изменение даты и времени	Дата и время системы изменено вручную	Информационное	Администратор
KscController: Синхронизация времени с источником	Время системы синхронизировано с Kaspersky Security Center	Информационное	Система: KscController

admin: Истечение срока действия учетных данных user: Истечение срока действия учетных данных	Срок действия имени и пароля пользователя истекает через <количество дней> дней	Информационное	Администратор или пользователь
admin: Истечение срока действия сертификата user: Истечение срока действия сертификата	Срок действия сертификата пользователя истекает через <количество дней> дней	Информационное	Администратор или пользователь
admin: Учетные данные пользователя просрочены user: Учетные данные пользователя просрочены	Срок действия имени и пароля пользователя истек, обновите учетные данные	Важное	Администратор или пользователь
admin: Сертификат пользователя просрочен user: Сертификат пользователя просрочен	Срок действия сертификата пользователя истек	Важное	Администратор или пользователь
Authenticator: Блокировка пользователя	Пользователь заблокирован в связи с превышением попыток ввода пароля	Критическое	Система: Authenticator
WebServer: Блокировка сеанса подключения	Сеанс подключения заблокирован по причине бездействия системы	Информационное	Система: WebServer
admin: Изменение времени ожидания после неуспешных попыток ввода пароля user: Изменение времени ожидания после неуспешных попыток ввода пароля	Время ожидания после неуспешных попыток ввода пароля изменено, новое значение: <новое значение> мин	Информационное	Администратор или пользователь
admin: Изменение времени бездействия пользователя до блокировки user: Изменение времени бездействия пользователя до блокировки	Время бездействия пользователя до блокировки изменено, новое значение: <новое значение> мин	Информационное	Администратор или пользователь
admin: Изменение количества неуспешных попыток входа user: Изменение количества неуспешных попыток входа	Максимальное количество неуспешных попыток входа изменено, новое значение: <новое значение>	Информационное	Администратор или пользователь

admin: Изменение учетных данных user: Изменение учетных данных	Пароль администратора для первоначального входа изменен	Информационное	Администратор или пользователь
admin: Изменение учетных данных user: Изменение учетных данных	Пароль пользователя <имя пользователя> изменен	Информационное	Администратор или пользователь
admin: Изменение учетных данных user: Изменение учетных данных	Сертификат пользователя <имя пользователя> изменен	Информационное	Администратор или пользователь
admin: Изменение учетных данных user: Изменение учетных данных	Имя пользователя <имя пользователя> изменено	Информационное	Администратор или пользователь
admin: Создание учетной записи пользователя	Учетная запись пользователя <имя пользователя> создана	Информационное	Администратор
admin: Ошибка создания учетной записи пользователя	Учетная запись пользователя <имя пользователя> уже существует	Важное	Администратор
admin: Удаление учетной записи пользователя	Учетная запись пользователя <имя пользователя> удалена	Информационное	Администратор
admin: Аутентификация пользователя user: Аутентификация пользователя	Пользователь <имя пользователя> вошел в систему	Информационное	Администратор или пользователь
Authenticator: Ошибка аутентификации пользователя	Ошибка аутентификации пользователя <имя пользователя> в системе: введен неверный пароль	Важное	Система: Authenticator
Authenticator: Ошибка аутентификации пользователя	Ошибка аутентификации пользователя <имя пользователя> в системе: неверный сертификат	Важное	Система: Authenticator
Authenticator: Ошибка аутентификации пользователя	Ошибка аутентификации пользователя <имя пользователя> в системе: пользователь с указанным именем не найден	Важное	Система: Authenticator
admin: Восстановление конфигурации системы	Статус восстановления конфигурации операционной системы из резервной копии: <статус>	Информационное	Администратор
admin: Создание резервной копии конфигурации системы	Статус создания резервной копии из конфигурации операционной системы: <статус>	Информационное	Администратор

admin: Создание отчета о проверке целостности	Началось создание отчета о проверке целостности: <описание>	Информационное	Администратор
IntegrityService: Статус проверки целостности	Статус проверки целостности: <статус>	Информационное	Система: IntegrityService
IntegrityService: Нарушение целостности объекта	Целостность <объект> нарушена: <описание>	Критическое	Система: IntegrityService
admin: Запуск самотестирования операционной системы	Началось самотестирование операционной системы	Информационное	Администратор
SelfTestManager: Сбой операционной системы в ходе самотестирования	Обнаружен сбой операционной системы в ходе самотестирования: <описание>	Критическое	Система: SelfTestManager
SelfTestManager: Результат самотестирования операционной системы	Результат самотестирования операционной системы: завершено успешно	Информационное	Система: SelfTestManager
SelfTestManager: Результат самотестирования операционной системы	Результат самотестирования операционной системы: обнаружены ошибки	Информационное	Система: SelfTestManager
SelfTestManager: Результат самотестирования операционной системы	Результат самотестирования операционной системы: отменено вручную	Информационное	Система: SelfTestManager

Просмотр журнала событий аудита операционной системы

Kaspersky IoT Secure Gateway 1000 сохраняет в журнале аудита операционной системы события, связанные с безопасностью системы. Эти события создаются компонентами системы. В каждом событии указывается идентификатор субъекта (имя пользователя или название компонента), зарегистрировавшего это событие.

При возникновении критического события аудита в меню слева возле раздела **Аудит** появляется *сигнализация* об этом в виде красного значка с восклицательным знаком . В этом случае обратитесь к сотруднику, ответственному за информационную безопасность в вашей организации.

Чтобы просмотреть журнал аудита событий операционной системы:

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

   Откроется страница **Аудит**, которая содержит таблицу всех зарегистрированных событий аудита операционной системы. События в таблице обновляются автоматически каждые 30 секунд и отображаются в обратном хронологическом порядке (первыми отображаются новые события). В таблице максимально могут отображаться до 1024 последних зарегистрированных событий. При превышении количества событий журнал перезаписывается, начиная с самых старых.

Если язык событий аудита в таблице не соответствует языку системы, вам нужно выбрать нужный язык веб-интерфейса в меню и обновить страницу, чтобы применить изменения.

Для каждой записи журнала отображается следующая информация:

- **Дата и время** – дата и время регистрации события.
- **Название события** – название зарегистрированного события.
- **Текст события** – подробная информация о зарегистрированном событии.
- **Идентификатор субъекта** – источник зарегистрированного события:
  - **Администратор** – событие вызвано действием администратора в системе.
  - **Пользователь** – событие вызвано действием пользователя в системе.
  - **Система** – событие вызвано действием системы. Для каждого события также отображается имя подсистемы, выполнившей событие.
- **Критичность** – уровень критичности зарегистрированного события.

  События подразделяются по следующим уровням критичности:

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

  При возникновении критического события аудита в меню слева напротив раздела **Аудит** появляется *сигнализация* об этом в виде красного значка с восклицательным знаком . В таблице событие аудита с критическим уровнем выделено красным цветом.

2. Если требуется просмотреть события за определенную дату или период, нажмите на поле **Дата**, выберите конкретную дату или даты начала и окончания периода и нажмите на кнопку **Применить**.

   События за выбранную дату или период отобразятся в таблице.

3. Если требуется просмотреть события с определенным уровнем критичности, в верхней части таблицы в раскрывающемся списке **Критичность** выберите нужный уровень критичности и нажмите на кнопку **Применить**. Вы можете выбрать одно или несколько значений. По умолчанию отображаются события всех уровней критичности.

   События с выбранным уровнем критичности отобразятся в таблице.

4. Если требуется просмотреть события из определенных источников, в верхней части таблицы в раскрывающемся списке **Идентификатор субъекта** выберите имя нужного субъекта и нажмите на кнопку **Применить**. Вы можете выбрать одно или несколько значений. По умолчанию отображаются все зарегистрированные события.

   События из выбранных источников отобразятся в таблице.

5. Если требуется сбросить все установленные фильтры отображения событий в таблице, нажмите **Сбросить все**.

В таблице снова отобразятся все зарегистрированные события.

6. Если требуется отобразить более старые события, нажмите на кнопку **Загрузить еще** под таблицей.

> Кнопка **Загрузить еще** доступна всегда, даже если более ранние события отсутствуют.

Экспорт журнала событий аудита системы

Вы можете сохранить журнал аудита операционной системы на локальном компьютере.

Чтобы сохранить журнал аудита операционной системы на локальном компьютере:

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

   Откроется страница **Аудит**, которая содержит таблицу всех зарегистрированных событий аудита операционной системы.

2. Нажмите на кнопку **Скачать журнал**.

3. В открывшемся окне укажите путь сохранения файла журнала аудита на локальном компьютере, при необходимости задайте его имя и сохраните файл.

Журнал аудита операционной системы будет сохранен на локальном компьютере в формате CSV. Если вы применили фильтры в таблице событий аудита перед тем, как сохранить журнал, в нем будут отображаться только отфильтрованные события.

Просмотр событий при подключении к Kaspersky IoT Secure Gateway 1000 через консольный порт

Kaspersky IoT Secure Gateway 1000 позволяет просматривать журналы событий Kaspersky IoT Secure Gateway 1000 в режиме реального времени. Для этого требуется выполнить подключение встраиваемого компьютера Kraftway Рубеж-Н к локальному компьютеру через консольный порт.

Консольный порт – это порт управления, обеспечивающий возможность внеполосного доступа к встраиваемому компьютеру.

Чтобы просмотреть журналы событий Kaspersky IoT Secure Gateway 1000 в режиме реального времени через подключение по консольному порту:

1. Подключите консольный кабель с разъемами RJ-45 DB-9/RS-232 одним концом к разъему на передней панели встраиваемого компьютера Kraftway Рубеж-Н, а другим – к компьютеру или ноутбуку.

   Если на вашем компьютере нет разъема для подключения через нужный кабель, вы можете использовать адаптер USB-COM.

2. Включите встраиваемый компьютер.

3. На локальном компьютере с помощью используемой программы эмуляции терминала выполните подключение к встраиваемому компьютеру.

   Предварительно в используемой программе эмуляции терминала требуется указать следующие параметры подключения:

- Скорость информационного потока – 115200 бод или другое значение, если оно явно установлено в параметре **Recovery mode**.
- Количество бит данных, наличие и тип бита четности, количество стоп-бит – 8n1.
- Аппаратное управление потоком.

На мониторе компьютера или ноутбука в интерфейсе используемой программы эмуляции терминала отобразятся события Kaspersky IoT Secure Gateway 1000 в режиме реального времени.

Экспорт системного журнала

Вы можете сохранить системный журнал, который содержит диагностическую информацию о работе Kaspersky IoT Secure Gateway 1000, на локальном компьютере. Вы можете использовать этот журнал для диагностики возможных проблем системы.

Этот функционал доступен только администратору.

Чтобы сохранить системный журнал на локальном компьютере:

1. В меню в левой части экрана выберите раздел **Параметры** → **Диагностика**.
2. Нажмите на кнопку **Сохранить в файл**.
3. В открывшемся окне укажите путь сохранения файла журнала на локальном компьютере, при необходимости задайте новое имя и сохраните файл.

Системный журнал будет сохранен на локальном компьютере. По умолчанию файл сохраняется с именем log_files.tar.gz.

Работа с приложениями

Управление приложениями доступно только администратору. Пользователь может только просматривать список приложений и список журналов приложений.

Все приложения, доступные для установки, отображаются в веб-интерфейсе Kaspersky IoT Secure Gateway 1000 в разделе **Приложения** → **Все приложения**. По умолчанию, приложения в таблице **Все приложения** отсортированы по названию. Вы можете нажать на заголовок столбца, чтобы отсортировать таблицу по этому столбцу.

Для каждого приложения во вкладке **Все приложения** отображается следующая информация:

- **Название** – название приложения и его значок. Вы можете просмотреть подробную информацию о приложении и его разработчике, Политику конфиденциальности и Лицензионное соглашение приложения, нажав на имя этого приложения в таблице.
- **Описание** – краткое описание приложения.
- **Версия** – номер последней версии приложения, доступной для установки.

- **Размер** – размер установочного пакета приложения.
- **Категория** – категории, к которым относится приложение.
- **Дата публикации** – дата публикации последней версии приложения.
- **Статус** – статус установки приложения (в процессе установки или удаления, ошибка, если приложение не удалось установить). Если безопасность приложения скомпрометирована, для такого приложения отображается статус **Скомпрометировано**. Скомпрометированное приложение невозможно установить.
- **Управление** – кнопка для установки приложения, если приложение доступно для установки, или статус установки.

Все установленные приложения отображаются в веб-интерфейсе Kaspersky IoT Secure Gateway 1000 в разделе **Приложения → Установленные приложения**. По умолчанию, приложения в таблице **Установленные приложения** отсортированы по названию. Вы можете нажать на заголовок столбца, чтобы отсортировать таблицу по этому столбцу.

Для каждого установленного приложения во вкладке **Установленные приложения** отображается следующая информация:

- **Название** – название приложения и его значок. Вы можете просмотреть подробную информацию о приложении и его разработчике, Политику конфиденциальности и Лицензионное соглашение приложения, нажав на имя этого приложения в таблице.
- **Издатель** – название компании, выпустившей приложение.
- **Версия** – номер установленной версии приложения.
- **Тип приложения** – тип приложения по функционированию в Kaspersky IoT Secure Gateway 1000.
- **Правило запуска** – способ запуска приложения на устройстве: автоматический запуск, запуск вручную или запрет на запуск.

  Вы можете настроить правило запуска только для сконфигурированных приложений в статусе **Запущено** или **Остановлено**.
- **Манифест** – конфигурационный файл приложения. Вы можете просмотреть содержимое манифеста, нажав на кнопку **Просмотреть**.
- **Состояние** – состояние работы приложения (запущено или остановлено). Если приложение не сконфигурировано или сконфигурировано неправильно, отображается состояние **Ожидание**. В этом случае требуется настроить конфигурацию приложения, например, через Kaspersky Security Center 14.2 Web Console.
- **Управление** – кнопка для запуска или остановки приложения.
- **Удаление** – кнопка для удаления приложения.

Скачивание и установка приложений

Вы можете скачать и установить в Kaspersky IoT Secure Gateway 1000 не более 20 приложений.

Чтобы скачать и установить приложение в Kaspersky IoT Secure Gateway 1000:

1. В меню в левой части экрана выберите раздел **Приложения → Все приложения**.

   Отобразится таблица всех приложений, которые доступны для установки.

2. Если вы хотите вручную обновить список приложений в таблице, нажмите на кнопку **Обновить таблицу** в верхней части страницы.

3. Если вы хотите отсортировать приложения в таблице, нажмите на заголовок столбца, по которому вы хотите отсортировать.

   По умолчанию, приложения отсортированы по названию в алфавитном порядке.

4. Если вы хотите посмотреть подробную информацию о приложении перед установкой, нажмите на название приложения.

   Откроется окно с подробной информацией о приложении.

5. Нажмите на кнопку **Установить** в столбце **Действие** напротив того приложения, которое вы хотите установить в Kaspersky IoT Secure Gateway 1000.

   Для типа сетевого устройства *однонаправленный шлюз* гарантируется работа всех доступных приложений. Для типа сетевого устройства *сетевой роутер* гарантируется работа только приложений Kaspersky IoT Secure Gateway Network Protector и Kaspersky Debug Service. Вы можете установить другие приложения, но их работа на устройстве не гарантируется.

Приложение будет скачано и установлено в Kaspersky IoT Secure Gateway 1000. Информация о скачивании и установке приложения сохраняется в журнале аудита системы. Установленное приложение отобразится в разделе **Приложения → Установленные приложения**. В этом разделе вы можете запустить или остановить приложение, управлять правилами его запуска, а также удалить.

Установленные приложения не обновляются автоматически. Чтобы обновить приложение, вам нужно сначала удалить установленную версию приложения и затем установить его новую версию. Если вы удалите версию приложения, которая снята с публикации (не отображается во вкладке **Все приложения**), вы не сможете вернуться к этой версии.

Запуск и остановка приложений

Вы можете запускать и останавливать приложения в веб-интерфейсе Kaspersky IoT Secure Gateway 1000.

Чтобы запустить приложение на устройстве:

1. В меню в левой части экрана выберите раздел **Приложения → Установленные приложения**.

   Отобразится таблица всех приложений, которые установлены в Kaspersky IoT Secure Gateway 1000.

2. Если вы хотите отсортировать приложения в таблице, нажмите на заголовок столбца, по которому вы хотите отсортировать.

   По умолчанию, приложения отсортированы по названию в алфавитном порядке.

3. В строке приложения, которое вы хотите запустить, нажмите на кнопку **Запустить** в столбце **Управление**.

   Вы можете запустить приложение в следующих случаях:

   - Приложение установлено и сконфигурировано без ошибок и находится в состоянии **Остановлено**.

- Для приложения выбрано правило запуска **Запуск вручную** или **Автозапуск**.

> Для приложений, которые находятся в состоянии **Ожидание**, требуется сначала настроить конфигурацию через Kaspersky Security Center 14.2 Web Console и дождаться появления состояния **Остановлено**.

Приложение будет запущено, в таблице отобразится соответствующее состояние. Информация о запуске приложения сохраняется в журнале аудита операционной системы.

Если приложение не удается запустить, отображается состояние **Ошибка**. В этом случае требуется удалить приложение и установить его заново.

Чтобы остановить приложение на устройстве:

1. В меню в левой части экрана выберите раздел **Приложения** и выберите вкладку **Установленные приложения**.

   Отобразится таблица всех приложений, установленных в Kaspersky IoT Secure Gateway 1000.

2. Если вы хотите отсортировать приложения в таблице, нажмите на заголовок столбца, по которому вы хотите отсортировать.

   По умолчанию, приложения отсортированы по названию в алфавитном порядке.

3. В строке приложения, которое вы хотите остановить, нажмите на кнопку **Остановить** в столбце **Управление**.

   Вы можете остановить приложение, если оно сконфигурировано без ошибок и находится в состоянии **Запущено**.

Приложение будет остановлено, и в таблице отобразится соответствующее состояние. Информация об остановке приложения сохраняется в журнале аудита операционной системы.

Управление правилами запуска приложений

Вы можете настроить, как приложение будет запускаться в Kaspersky IoT Secure Gateway 1000 (автоматически или вручную), или запретить запуск приложения с помощью веб-интерфейса Kaspersky IoT Secure Gateway 1000.

Чтобы настроить правила запуска приложения:

1. В меню в левой части экрана выберите раздел **Приложения → Установленные приложения**.

   Отобразится таблица всех приложений, которые установлены в Kaspersky IoT Secure Gateway 1000.

2. Если вы хотите отсортировать приложения в таблице, нажмите на заголовок столбца, по которому вы хотите отсортировать.

   По умолчанию, приложения отсортированы по названию в алфавитном порядке.

3. В строке приложения, для которого вы хотите настроить правило запуска, в столбце **Правило запуска** выберите одно из следующих значений в раскрывающемся списке:

   - **Автозапуск** – приложение будет запускаться автоматически при включении или перезагрузке Kaspersky IoT Secure Gateway 1000.

     При необходимости вы можете останавливать и запускать приложение вручную.

- **Запуск вручную** – приложение будет запускаться только вручную по нажатию кнопки **Запустить**.

  По умолчанию для приложения после установки применяется правило ручного запуска.

- **Запрет на запуск** – приложение будет недоступно для запуска. Кнопка **Запустить** будет недоступна.

Если вы изменили правило запуска для запущенного приложения, правило запуска будет применено только после остановки приложения. Вы можете остановить приложение вручную, чтобы применить правило запуска.

Для приложений, которые находятся в состоянии **Ожидание**, требуется сначала настроить конфигурацию через Kaspersky Security Center 14.2 Web Console и дождаться появления состояния **Запущено** или **Остановлено**.

Правило запуска будет применено для выбранного приложения в Kaspersky IoT Secure Gateway 1000. Информация об изменении списка правил запуска сохраняется в журнале аудита системы.

Вы также можете управлять правилами запуска приложений через Kaspersky Security Center 14.2 Web Console.

Удаление приложений

Вы можете удалять приложения в веб-интерфейсе Kaspersky IoT Secure Gateway 1000.

Чтобы удалить приложение:

1. В меню в левой части экрана выберите раздел **Приложения → Установленные приложения**.

   Отобразится таблица всех приложений, которые установлены в Kaspersky IoT Secure Gateway 1000.

2. Если вы хотите отсортировать приложения в таблице, нажмите на заголовок столбца, по которому вы хотите отсортировать.

   По умолчанию, приложения отсортированы по названию в алфавитном порядке.

3. В строке приложения, которое вы хотите удалить, нажмите на значок корзины в столбце **Удаление** и подтвердите удаление в открывшемся окне.

Приложение, а также его конфигурация, журнал и файлы будут удалены из Kaspersky IoT Secure Gateway 1000. Приложение будет удалено из таблицы установленных приложений. Информация об удалении приложения сохраняется в журнале аудита операционной системы.

Если вы удалите версию приложения, которая снята с публикации (не отображается во вкладке **Все приложения**), вы не сможете снова установить эту версию.

Если при удалении возникла ошибка, в столбце **Состояние** отобразится состояние **Ошибка**, вы не сможете запустить или остановить приложение, настроить правило запуска или посмотреть манифест. В этом случае вам нужно переустановить приложение.

Связанные с удаленным приложением маршруты, настроенные в Kaspersky Security Center 14.2 Web Console, перестанут работать (перейдут в статус **Ошибка**). Рекомендуется перенастроить маршруты, связанные с удаленными приложениями через Kaspersky Security Center 14.2 Web Console.

Мониторинг состояния приложений

Kaspersky IoT Secure Gateway 1000 записывает события, которые генерируются установленными приложениями, в журналы.

Для каждого приложения журналы хранятся в виде архива log_files_<app_id>.tar.gz. Архив содержит не более пяти файлов журнала в формате LOG, размер одного файла не более 10 МБ (максимальный размер архива составляет 50 МБ). При достижении предельного размера хранимых файлов в архиве Kaspersky IoT Secure Gateway 1000 удаляет самый старый файл, новые события записываются в новый файл.

Kaspersky IoT Secure Gateway 1000 обеспечивает сохранность журналов приложений при перезагрузке, выключении или обновлении системы. При удалении или обновлении приложения Kaspersky IoT Secure Gateway 1000 удаляет журнал этого приложения.

Чтобы сохранить журнал приложения на локальном компьютере:

1. В меню веб-интерфейса выберите раздел **Приложения** и выберите вкладку **Журнал приложений**.
2. Если вы хотите обновить таблицу журналов приложений, нажмите на кнопку **Обновить таблицу** в верхней части страницы.
3. На открывшейся странице нажмите **Скачать** в столбце **Журнал** напротив нужного приложения. Для доступных для скачивания журналов указан их размер.
4. В открывшемся окне сохранения журнала на локальном компьютере укажите путь, при необходимости укажите имя файла и сохраните файл.

   Журнал приложений log_files_<app_id>.tar.gz будет сохранен на локальном компьютере в папку для скачивания по умолчанию (например, в папку загрузок браузера).

   Пока скачивание журнала приложения не завершилось, вы не можете скачать журнал другого приложения (кнопка **Скачать** будет недоступна). Если для приложения еще нет записанных событий, журнал будет недоступен для скачивания, и в столбце **Журнал** будет указан соответствующий статус.

Самотестирование и контроль целостности Kaspersky IoT Secure Gateway 1000

Этот функционал доступен только администратору.

Самотестирование

Самотестирование Kaspersky IoT Secure Gateway 1000 – процесс, выполняющий мониторинг работоспособности функций безопасности KasperskyOS, а также наложенных средств защиты.

Система самотестирования запрашивает диагностику следующих функций:

- аудит;
- инструмент идентификации и аутентификации пользователей;
- инструмент блокировки сетевого трафика;
- приложение Kaspersky IoT Secure Gateway Network Protector.

Чтобы запустить самотестирование, выполните следующие действия:

1. В меню в левой части экрана выберите раздел **Самодиагностика**.
2. В блоке **Самотестирование** нажмите на кнопку **Запустить тестирование**.

   Результаты самотестирования каждой из функций отображаются в таблице **Самотестирование**, а общий статус тестирования отображается рядом с кнопкой **Запустить тестирование**. При возникновении ошибок в процессе самотестирования Kaspersky IoT Secure Gateway 1000 переходит в режим аварийной поддержки.

События запуска и результаты самотестирования записываются в журнал аудита системы.

Контроль целостности

Контроль целостности проводит проверку файлов системных и пользовательских приложений, а также их данных на основе проверки электронной подписи (контрольной суммы).

В Kaspersky IoT Secure Gateway 1000 реализовано два типа проверки – автоматическая и ручная.

Автоматическая проверка выполняется при запуске Kaspersky IoT Secure Gateway 1000 и проверяет контрольные суммы пользовательских приложений. При нарушении целостности пользовательских приложений, Kaspersky IoT Secure Gateway 1000 записывает в журнал аудита информацию о нарушении целостности и автоматически переходит в режим аварийной поддержки.

Ручную проверку может запускать только администратор.

Чтобы запустить проверку контроля целостности вручную и посмотреть результаты, выполните следующие действия:

1. В меню в левой части экрана выберите раздел **Самодиагностика**.
2. В блоке **Проверка целостности** нажмите на кнопку **Запустить проверку**.

   По результатам проверки будет сформирован файл отчета. Статус, а также дата и время запуска последней ручной проверки целостности отображаются рядом с кнопкой **Скачать отчет**.
3. Нажмите на кнопку **Скачать отчет**, чтобы сохранить файл отчета с результатами ручной проверки целостности в формате TXT на локальный компьютер.

В случае нарушения целостности при ручной проверке автоматический переход в режим аварийной поддержки не предусмотрен, требуется рассмотреть отчет и принять решение о дальнейших действиях.

Файл отчета с результатами ручной проверки целостности состоит из заголовка и тела отчета. В заголовке файла отчета содержится следующая информация:

- идентификатор хоста;
- дата и время составления отчета;
- имя функции для подсчета контрольной суммы файла отчета;
- контрольная сумма файла отчета;
- разделитель между заголовком и телом отчета.

Тело отчета состоит из строк со статусом проверки для каждого файла, участвующего в процедуре контроля целостности. Строка состоит из следующих полей, разделенных символом **|**:

- путь и имя проверяемого файла;
- дата и время проверки;
- имя функции для подсчета контрольной суммы;
- эталонная контрольная сумма файла;
- вычисленная контрольная сумма файла;
- статус проверки. Возможные статусы:
  - *File integrity verified successfully* – эталонная и вычисленная контрольные суммы совпадают. Любой статус, кроме этого, может указывать на потенциальное нарушение целостности и администратору рекомендуется провести анализ инцидента.
  - *File content changed against reference!* – вычисленная контрольная сумма отличается от эталонной.
  - *File isn`t present in integrity database!* – обнаружен файл, не находящийся под контролем целостности. В этом случае поле с эталонной контрольной суммой будет заполнено нолями.
  - *The file under integrity control was deleted or moved!* – файл, находящийся под контролем целостности перемещен или удален. В этом случае поле с вычисленной контрольной суммой будет заполнено нолями.
  - *Package integrity violation!* – файл, содержащий эталонные контрольные суммы файлов, поврежден или отсутствует.

Следующие исполняемые файлы и библиотеки должны успешно проходить проверку контроля целостности:

- системные библиотеки в папке /lib;
- файл образа системы /loader_active/image.fit;
- файлы локального веб-интерфейса:

- файлы в папке html/assets;
- файлы в папке html/css;
- файлы в папке html/js;
- файлы authorization.html, index.html, troubleshooting.html.

- цифровые сертификаты системы:
  - файл 3520p1.der (для релизной версии системы);
  - файл 3020d1.der (для версии системы для разработчиков).
- файлы для работы с приложениями:
  - файл контейнера /packages/helpers/container;
  - файлы валидации приложений в папке /packages/schema.

Для этих файлов и библиотек в отчете должен быть указан статус File integrity verified successfully, который означает, что их код не изменился, и их контрольная сумма совпадает с эталонной.

Для остальных файлов вам нужно самостоятельно проанализировать допустимость изменений.

Резервирование и восстановление из резервной копии

В Kaspersky IoT Secure Gateway 1000 реализована функция резервного копирования и восстановления, предназначенная для восстановления работоспособного состояния системы в случае сбоев. Резервирование и восстановление из резервной копии доступны администратору.

Корректное резервирование и восстановление из резервной копии параметров MQTT-брокера, веб-сервера, а также дополнительных приложений, установленных на Kaspersky IoT Secure Gateway 1000, не гарантируется.

Этот функционал доступен только администратору.

Резервирование конфигурации

Для получения резервной копии конфигурации:

1. В меню в левой части экрана выберите раздел **Параметры** → **Резервное копирование и восстановление**.
2. В блоке **Создание резервной копии** нажмите на кнопку **Создать файл**.
3. Дождитесь окончания процедуры создания резервной копии конфигурации.
4. Нажмите на кнопку **Сохранить файл**.

5. В открывшемся окне выберите папку для хранения резервной копии и сохраните файл.

Восстановление конфигурации

Восстановление конфигурации возможно только в случае, если версия Kaspersky IoT Secure Gateway 1000, на которой выполнялось создание резервной копии, соответствует версии Kaspersky IoT Secure Gateway 1000, на которой выполняется восстановление.

Для восстановления конфигурации устройства из резервной копии:

1. В меню в левой части экрана выберите раздел **Параметры** → **Резервное копирование и восстановление**.
2. В блоке **Восстановление системы** нажмите на кнопку **Выбрать файл**.
3. В открывшемся окне выберите файл резервной копии.
4. Дождитесь окончания операции восстановления.

   В случае успешного восстановления конфигурации устройство будет перезагружено.

Обновление Kaspersky IoT Secure Gateway 1000

Вы можете выполнить полное обновление Kaspersky IoT Secure Gateway 1000 на устройстве через веб-интерфейс.

Обновление системы возможно, только если система Kaspersky IoT Secure Gateway 1000 подключена к Kaspersky Security Center. Полное обновление Kaspersky IoT Secure Gateway 1000 с серверов обновлений "Лаборатории Касперского" доступно только для версии 3.0.

Этот функционал доступен только администратору.

После обновления Kaspersky IoT Secure Gateway 1000 устройство будет перезагружено.

Чтобы выполнить полное обновление Kaspersky IoT Secure Gateway 1000:

1. В меню в левой части страницы веб-интерфейса выберите раздел **Параметры** → **Обновление**.
2. Нажмите на кнопку **Запустить обновление**.

   Начнется проверка наличия доступных обновлений для Kaspersky IoT Secure Gateway 1000. Если обновление найдено, оно будет загружено, и будет выполнено полное обновление Kaspersky IoT Secure Gateway 1000 на устройстве. В процессе обновления устройство будет перезагружено.

   Информация об успешной проверке и загрузке обновлений, а также о процессе обновления Kaspersky IoT Secure Gateway 1000 записывается в журнал аудита системы.

Перезагрузка Kaspersky IoT Secure Gateway 1000

Этот функционал доступен только администратору.

Чтобы перезагрузить Kaspersky IoT Secure Gateway 1000:

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

2. Нажмите на кнопку **Перезагрузить устройство** и подтвердите свои действия.

   Устройство с Kaspersky IoT Secure Gateway 1000 будет перезагружено. Соединение Kaspersky Security Center и Kaspersky IoT Secure Gateway 1000 во время перезагрузки будет недоступно.

Управление системой через Kaspersky Security Center 14.2 Web Console

Kaspersky Security Center 14.2 Web Console (далее также Web Console) представляет собой веб-приложение, предназначенное для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Web Console является компонентом Kaspersky Security Center 14.2, предоставляющим пользовательский интерфейс. Подробную информацию о Kaspersky Security Center 14.2 Web Console см. в онлайн-справке Kaspersky Security Center 14.2.

Kaspersky Security Center 14.2 и Kaspersky Security Center 14.2 Web Console не поставляются в комплекте поставки Kaspersky IoT Secure Gateway 1000, их требуется установить отдельно.

С помощью Kaspersky Security Center 14.2 Web Console вы можете выполнять следующие действия:

- контролировать состояние системы безопасности вашей организации;
- управлять установленными приложениями;
- просматривать отчеты о состоянии системы безопасности.

В Web Console при просмотре информации об устройстве с Kaspersky IoT Secure Gateway 1000 на вкладке **Общие** в разделах меню **Общие**, **Сеть**, **Система**, **Защита**, **Статус устройства определен программой** может не отображаться информация о Kaspersky IoT Secure Gateway 1000.

Период синхронизации Kaspersky IoT Secure Gateway 1000 с Kaspersky Security Center составляет 30 секунд. Через этот период в Kaspersky Security Center 14.2 Web Console поступает информация о зарегистрированных в Kaspersky IoT Secure Gateway 1000 событиях, а также синхронизируется информация об установленных в интерфейсе Kaspersky IoT Secure Gateway 1000 и с помощью Web Console параметрах.

О веб-плагине управления Kaspersky IoT Secure Gateway 1000

Веб-плагин управления Kaspersky IoT Secure Gateway 1000 (далее также веб-плагин) обеспечивает взаимодействие Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center 14.2 Web Console.

Веб-плагин позволяет централизованно через Kaspersky Security Center 14.2 Web Console выполнять следующие действия:

- Настраивать параметры Kaspersky IoT Secure Gateway 1000.
- Получать события из Kaspersky IoT Secure Gateway 1000.
- Управлять сетевым экраном.
- Управлять параметрами приложения Kaspersky IoT Secure Gateway Network Protector и списками запрещенных и разрешенных IP-адресов.
- Управлять безопасностью Kaspersky IoT Secure Gateway 1000.
- Обновлять и перезагружать Kaspersky IoT Secure Gateway 1000.
- Управлять приложениями и их конфигурацией.

Установка веб-плагина управления Kaspersky IoT Secure Gateway 1000

Веб-плагин управления Kaspersky IoT Secure Gateway 1000 по умолчанию не установлен в Kaspersky Security Center 14.2 Web Console. Веб-плагин управления Kaspersky IoT Secure Gateway 1000 входит в комплект поставки Kaspersky IoT Secure Gateway 1000. Веб-плагин требуется установить на компьютер с установленным приложением Kaspersky Security Center 14.2 Web Console. При этом функции веб-плагина доступны всем администраторам, у которых есть доступ к Kaspersky Security Center 14.2 Web Console в браузере. Вы можете просмотреть список установленных веб-плагинов в интерфейсе Kaspersky Security Center 14.2 Web Console (**Параметры консоли** → **Веб-плагины**).

На Сервере администрирования, на котором установлен Kaspersky Security Center, должен быть доступен порт 13294. Порт 13294 требуется для подключения устройств с защитой на уровне UEFI. Подробнее об управлении устройств с защитой на уровне UEFI см. в разделе *Устройства с защитой на уровне UEFI* в онлайн-справке Kaspersky Security Center 14.2. Подробнее о портах для подключения к Kaspersky Security Center см. в разделе *Порты, используемые Kaspersky Security Center* в онлайн-справке Kaspersky Security Center 14.2.

Kaspersky Security Center 14.2 и Kaspersky Security Center 14.2 Web Console не поставляются в комплекте поставки Kaspersky IoT Secure Gateway 1000, их требуется установить отдельно.

Чтобы установить веб-плагин управления Kaspersky IoT Secure Gateway 1000 в Kaspersky Security Center 14.2 Web Console:

1. В меню Kaspersky Security Center 14.2 Web Console выберите **Параметры консоли** → **Веб-плагины**.

   Отобразится список доступных плагинов управления Kaspersky Security Center 14.2 Web Console.

2. Нажмите на кнопку **Добавить из файла**.

3. В открывшейся справа панели добавьте следующие файлы:

   - ZIP-архив с дистрибутивом веб-плагина, полученный в комплекте поставки Kaspersky IoT Secure Gateway 1000, нажав на кнопку **Загрузить файл формата ZIP**;
   - файл подписи, полученный в комплекте поставки Kaspersky IoT Secure Gateway 1000, нажав на кнопку **Загрузить подпись**.

4. Нажмите на кнопку **Добавить**.

5. После завершения установки веб-плагина нажмите на кнопку **OK**.

   Веб-плагин управления Kaspersky IoT Secure Gateway 1000 будет загружен в конфигурации по умолчанию и появится в списке плагинов управления Kaspersky Security Center 14.2 Web Console.

Обновление веб-плагина управления Kaspersky IoT Secure Gateway 1000

Вы можете обновить веб-плагин управления Kaspersky IoT Secure Gateway 1000 в Kaspersky Security Center 14.2 Web Console.

Чтобы обновить веб-плагин управления Kaspersky IoT Secure Gateway 1000 в Kaspersky Security Center 14.2 Web Console:

1. В меню Kaspersky Security Center 14.2 Web Console выберите **Параметры консоли → Веб-плагины**.

   Отобразится список доступных плагинов управления Kaspersky Security Center 14.2 Web Console.

2. В списке плагинов управления установите флажок около веб-плагина управления Kaspersky IoT Secure Gateway 1000.

3. Нажмите на кнопку **Обновить из файла**.

4. В открывшейся справа панели добавьте следующие файлы:

   - ZIP-архив с дистрибутивом веб-плагина, полученный в комплекте поставки Kaspersky IoT Secure Gateway 1000, нажав на кнопку **Загрузить файл формата ZIP**;

   - файл подписи, полученный в комплекте поставки Kaspersky IoT Secure Gateway 1000, нажав на кнопку **Загрузить подпись**.

5. Нажмите на кнопку **Обновление**.

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

Веб-плагин управления Kaspersky IoT Secure Gateway 1000 будет обновлен, и в таблице плагинов управления Kaspersky Security Center 14.2 Web Console отобразится информация о его версии и времени обновления.

Удаление веб-плагина управления Kaspersky IoT Secure Gateway 1000

Вы можете удалить веб-плагин управления Kaspersky IoT Secure Gateway 1000 в Kaspersky Security Center 14.2 Web Console. После удаления веб-плагина, управление Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console будет недоступно.

Чтобы удалить веб-плагин управления Kaspersky IoT Secure Gateway 1000 из Kaspersky Security Center 14.2 Web Console:

1. В меню веб-интерфейса Kaspersky Security Center 14.2 Web Console выберите **Параметры консоли → Веб-плагины**.

   Отобразится список доступных плагинов управления Kaspersky Security Center 14.2 Web Console.

2. В списке плагинов управления установите флажок около веб-плагина управления Kaspersky IoT Secure Gateway 1000.

3. Нажмите на кнопку **Удалить**.

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

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

     Резервная копия плагина будет создана. Веб-плагин управления Kaspersky IoT Secure Gateway 1000 будет удален из Kaspersky Security Center 14.2 Web Console.

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

Веб-плагин управления Kaspersky IoT Secure Gateway 1000 будет удален из Kaspersky Security Center 14.2 Web Console.

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

Вход и выход из Kaspersky Security Center 14.2 Web Console

Для входа в Kaspersky Security Center 14.2 Web Console, требуется получить у администратора веб-адрес Сервера администрирования Kaspersky Security Center и номер порта, указанные во время установки (по умолчанию используется порт 8080). Также требуется включить JavaScript в браузере.

Чтобы войти в Kaspersky Security Center 14.2 Web Console:

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

   Требования к браузеру, который используется для работы с Kaspersky Security Center 14.2 Web Console, см. в разделе *Аппаратные и программные требования* в онлайн-справке Kaspersky Security Center 14.2.

   Откроется страница входа.

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

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

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

   Если вы вошли в Kaspersky Security Center 14.2 Web Console впервые, в нижней части экрана отобразится учебник. Вы можете следовать инструкциям учебника или закрыть его.

Вход в Kaspersky Security Center 14.2 Web Console выполнен и вы можете работать с Kaspersky Security Center 14.2 Web Console. Дополнительная информация о работе Kaspersky Security Center 14.2 Web Console приведена в онлайн-справке Kaspersky Security Center 14.2.

Чтобы выйти из Kaspersky Security Center 14.2 Web Console:

1. В меню Kaspersky Security Center 14.2 Web Console нажмите на имя пользователя.

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

Kaspersky Security Center 14.2 Web Console закроется и отобразится страница входа.

Добавление устройства Kaspersky IoT Secure Gateway 1000 в группу управляемых устройств Kaspersky Security Center 14.2 Web Console

Для управления устройством, на котором установлен Kaspersky IoT Secure Gateway 1000, через Kaspersky Security Center 14.2 Web Console, нужно перенести это устройство в группу управляемых устройств.

Чтобы добавить устройство в группу управляемых устройств Kaspersky Security Center 14.2 Web Console:

1. В главном окне Kaspersky Security Center 14.2 Web Console выберите **Обнаружение устройств и развертывание → Нераспределенные устройства**.

   Отобразится список всех обнаруженных нераспределенных устройств.

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

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

   Справа появится панель **Переместить в группу**.

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

5. Нажмите на кнопку **Переместить**.

Устройство будет перемещено в группу управляемых устройств.

Настройка параметров Kaspersky IoT Secure Gateway 1000 через Web Console

Этот раздел содержит информацию о настройке параметров Kaspersky IoT Secure Gateway 1000 через Web Console.

Настройка параметров MQTT-брокера через Web Console

Настройка параметров MQTT-брокера доступна только для типа сетевого устройства *сетевой роутер*.

Этот раздел содержит информацию о настройке параметров MQTT-брокера через Web Console. В Kaspersky Security Center 14.2 Web Console вы можете создавать новые профили MQTT-брокера, изменять существующие профили и переключаться между профилями.

Чтобы просмотреть таблицу профилей MQTT-брокера через Web Console:

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

2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.

3. В открывшемся окне свойств устройства выберите вкладку **Программы**.

4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.

5. Выберите вкладку **Параметры программы**.

6. Выберите раздел **MQTT-брокер**.

   Отобразится таблица профилей MQTT-брокера. В таблице для каждого профиля MQTT-брокера отображается следующая информация:

   - **Доступ** – доступ на изменение профиля. Значок замка, информирующий о том, что профиль доступен только для чтения, отображается только для предустановленного профиля, который поставляется вместе с устройством.

   - **Статус** – значком отмечен профиль MQTT-брокера, который используется в текущий момент.

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

Создание профиля MQTT-брокера через Web Console

Вы можете создавать новые профили MQTT-брокера через Kaspersky Security Center 14.2 Web Console. Разные профили MQTT-брокера позволяют работать с разными серверами и цифровыми платформами, которые принимают события от Kaspersky IoT Secure Gateway 1000 по протоколу MQTT.

Чтобы создать новый профиль MQTT-брокера через Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **MQTT-брокер**.

   Отобразится таблица профилей MQTT-брокера.
7. Нажмите на кнопку **Добавить** в верхней части таблицы профилей MQTT-брокера.

   Откроется окно **Изменение профиля**.
8. В раскрывающемся списке **Статус** выберите одно из следующих значений:
   - **Активный**, если вы хотите сделать новый профиль активным. В этом случае параметры настройки профиля загружаются в MQTT-брокер и активируется доступ к сертификатам из профиля для MQTT-брокера.
   - **Неактивный**.

   > Активным может быть только один профиль. Вы можете сделать активным только профиль MQTT-брокера, в котором добавлен файл конфигурации.
9. В поле **Имя** введите имя профиля латинскими буквами.
10. Добавьте конфигурационный файл или сертификат к новому профилю, нажав на кнопку **Добавить** в верхней части таблицы **Список файлов**.
11. В открывшейся справа панели загрузки файлов выполните следующие действия:
    a. В раскрывающемся списке **Тип** выберите тип файла, который вы хотите добавить:

- **Конфигурационный файл**. Содержит основные параметры для работы MQTT-брокера. Конфигурационный файл требуется добавить в профиль MQTT-брокера, чтобы этот профиль можно было сделать активным. Для выбора доступны файлы в формате CONF.

- **Сертификат**. Для выбора доступны файлы в формате CRT, CER, DER, PEM.

  Профиль MQTT-брокера требует несколько сертификатов безопасности: сертификат, выданный удостоверяющим центром, клиентский сертификат сервера и файл закрытого ключа. В зависимости от требований MQTT-сервера клиентский сертификат сервера и файл закрытого ключа должны быть подписаны действующим сертификатом удостоверяющего центра. Если ваш профиль предполагает использование защищенного соединения SSL/TLS, повторите этот шаг столько раз, сколько требуется, чтобы загрузить в систему все необходимые сертификаты. Без сертификатов безопасности не гарантируется работа защищенного соединения.

  Мы не рекомендуем загружать более трех файлов сертификатов безопасности в MQTT-профиль. При загрузке более трех файлов будут использоваться последние загруженные файлы сертификатов.

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

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

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

   Панель загрузки файлов закроется.

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

    Окно **Изменение профиля** закроется.

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

Изменение профиля MQTT-брокера через Web Console

Чтобы изменить профиль MQTT-брокера через Web Console:

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

2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.

3. В открывшемся окне свойств устройства выберите вкладку **Программы**.

4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.

5. Выберите вкладку **Параметры программы**.

6. Выберите раздел **MQTT-брокер**.

   Отобразится таблица профилей MQTT-брокера.

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

   Откроется окно **Изменение профиля**.

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

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

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

   Справа откроется панель загрузки файлов.

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

   - **Конфигурационный файл**. Содержит основные параметры для работы MQTT-брокера. Конфигурационный файл требуется добавить в профиль MQTT-брокера, чтобы этот профиль можно было активировать. Для выбора доступны файлы в формате CONF.
   - **Сертификат**. Для выбора доступны файлы в формате CRT, CER, DER, PEM.

     Профиль MQTT-брокера требует несколько сертификатов безопасности: сертификат, выданный удостоверяющим центром, клиентский сертификат сервера и файл закрытого ключа. В зависимости от требований MQTT-сервера клиентский сертификат сервера и файл закрытого ключа должны быть подписаны действующим сертификатом удостоверяющего центра. Если ваш профиль предполагает использование защищенного соединения SSL/TLS, повторите этот шаг столько раз, сколько требуется, чтобы загрузить в систему все необходимые сертификаты. Без сертификатов безопасности не гарантируется работа защищенного соединения.

     Мы не рекомендуем загружать более трех файлов сертификатов безопасности в MQTT-профиль. При загрузке более трех файлов будут использоваться последние загруженные файлы сертификатов.

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

      Файл загрузится в систему и появится в профиле.

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

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

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

    Файл будет удален из профиля MQTT-брокера.

    Kaspersky IoT Secure Gateway 1000 не позволяет удалить файлы активного и предустановленного профилей MQTT-брокера. Если требуется удалить файлы активного профиля, сначала нужно переключиться на другой профиль MQTT-брокера.

11. Нажмите на кнопку **OK** в нижней части окна **Изменение профиля**.

Окно **Изменение профиля** закроется.

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

Переключение на другой профиль MQTT-брокера через Web Console

Чтобы изменить профиль MQTT-брокера через Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **MQTT-брокер**.

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

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

   Активным может быть только один профиль.
9. Нажмите на кнопку **ОК** в нижней части окна **Изменение профиля**.

   Окно **Изменение профиля** закроется.
10. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

В таблице профилей в столбце **Статус** рядом с выбранным профилем появится значок , профиль станет активным и будет использоваться Kaspersky IoT Secure Gateway 1000 при получении данных по протоколу MQTT.

Удаление профиля MQTT-брокера через Web Console

Kaspersky IoT Secure Gateway 1000 не позволяет удалить активный и предустановленный профили MQTT-брокера. Если требуется удалить профиль, который сейчас является активным, сначала нужно выбрать активным другой профиль MQTT-брокера.

Чтобы удалить профиль MQTT-брокера через Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **MQTT-брокер**.
7. В таблице профилей MQTT-брокера выберите профиль, который вы хотите удалить и нажмите на кнопку **Удалить** в верхней части таблицы.
8. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Выбранный профиль MQTT-брокера будет удален.

Настройка параметров внешней и внутренней сетей через Web Console

Kaspersky IoT Secure Gateway 1000 поставляется со статически настроенным IP-адресом. Для работы системы в качестве безопасного шлюза Интернета вещей, требуется выполнить настройку параметров внешней и внутренней сетей. Также вы можете настроить параметры сети с помощью веб-интерфейса Kaspersky IoT Secure Gateway 1000.

Чтобы настроить параметры сети через Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Сеть** → **Внутренняя сеть** и настройте следующие параметры:

   a. В поле **IP-адрес** введите IP-адрес устройства Kaspersky IoT Secure Gateway 1000 во внутренней сети.

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

   c. Если требуется, чтобы Kaspersky IoT Secure Gateway 1000 выступал в качестве DHCP-сервера, установите переключатель **Использовать DHCP-сервер** в положение включено и укажите следующие параметры:

- В поле **Начало диапазона IP-адресов** введите IP-адрес начала диапазона.
- В поле **Конец диапазона IP-адресов** введите IP-адрес окончания диапазона.
- В поле **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 устройства во внутренней сети.

7. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.
8. Выберите раздел **Сеть** → **Внешняя сеть** и в блоке **Параметры внешней сети** настройте следующие параметры:

- Если вы хотите настроить параметры внешней сети автоматически по протоколу DHCP, установите переключатель **Автоматическое получение (по DHCP)** в положение включено.

  Если при включении автоматического получения параметров внешней сети DHCP-сервер выдал Kaspersky IoT Secure Gateway 1000 нулевые адреса DNS-серверов, то по умолчанию для преобразования доменного имени в IP-адрес будет использоваться IP-адрес – 208.67.222.222 (сервер OpenDNS).

- Если вы хотите настроить параметры внешней сети вручную, установите переключатель **Автоматическое получение (по DHCP)** в положение выключено и выполните следующие действия:
  - В поле **IP-адрес** введите IP-адрес, который вы хотите назначить системе во внешней сети.
  - В поле **Маска подсети** введите маску подсети.
  - В поле **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 устройства во внешней сети.

- Если вы хотите включить трансляцию сетевых адресов для внешней сети, установите переключатель **Включить маскарадинг** в положение включено.

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

Настройка маскарадинга через Web Console

Вы можете настроить трансляцию сетевых адресов для основного канала связи с помощью функции маскарадинга через Web Console.

Маскарадинг (англ. Masquerading) – тип трансляции сетевого адреса, при котором адрес отправителя во внутренней сети подменяется динамически в зависимости от адреса, назначенного интерфейсу, на адрес во внешней сети. Вы можете использовать функцию маскарадинга, если для устройств во внутренней сети требуется подмена параметров в заголовках IP-пакетов, а также для скрытия инфраструктуры за одним адресом. Это позволит устройствам, расположенным во внутренней сети и не имеющим реальных IP-адресов, отправлять и получать IP-пакеты из внешней сети.

Чтобы включить маскарадинг для основного канала связи через Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Сеть** → **Внешняя сеть**.
7. В блоке **Параметры трансляции** установите переключатель **Включить маскарадинг** в положение включено.

   Маскарадинг будет применен только для канала связи, назначенного основным: внешняя сеть или модем.

Добавление имени устройства через Web Console

Чтобы задать имя устройства через Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Параметры** → **Имя устройства**.
7. В поле **Имя устройства** введите имя.

   Имя устройства может содержать только цифры и латинские буквы. Максимальная длина имени – 32 символа.
8. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Управление сертификатами через Web Console

Вы можете просматривать загруженные ранее корневой сертификат и сертификат Сервера администрирования Kaspersky Security Center, а также обновлять их через Web Console.

Не рекомендуется загружать широко известные сертификаты удостоверяющего центра, так как доверенными будут являться все серверы, использующие сертификаты, подписанные этими сертификатами удостоверяющего центра. Такая ситуация может привести к компрометации Kaspersky IoT Secure Gateway 1000.

Необходимо загрузить правильный файл действующего сертификата. Загрузка неправильного файла сертификата может привести к неработоспособности устройства.

Чтобы загрузить или обновить корневой сертификат Kaspersky IoT Secure Gateway 1000 через Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Параметры** → **Сертификаты**.

   Отобразится окно, в котором указана информация о корневом сертификате и сертификате Сервера администрирования Kaspersky Security Center (если загружены).
7. Если требуется загрузить новый корневой сертификат, в блоке **Корневой сертификат** нажмите на кнопку **Загрузить** и в открывшемся окне выберите файл сертификата. Для добавления в качестве сертификата доступны файлы только в формате CRT, PEM, DER и CER.

   Корневой сертификат будет загружен в систему.
8. Если у вас есть загруженный корневой сертификат и его требуется обновить, в блоке **Корневой сертификат** нажмите на кнопку **Обновить** и в открывшемся окне выберите файл сертификата. Для добавления в качестве сертификата доступны файлы только в формате CRT, PEM, DER и CER.

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

   Kaspersky IoT Secure Gateway 1000 не позволяет удалить корневой сертификат без замены сертификата на новый.
9. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Чтобы загрузить или обновить сертификат Сервера администрирования Kaspersky Security Center через Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Параметры** → **Сертификаты**.

   Отобразится окно, в котором указана информация о сертификате администратора и сертификате Сервера администрирования Kaspersky Security Center (если загружены).

   Если для Сервера администрирования Kaspersky Security Center был выпущен новый сертификат, соединение, установленное ранее между Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center будет разорвано. Для восстановления соединения требуется в веб-интерфейсе Kaspersky IoT Secure Gateway 1000 добавить выпущенный сертификат в качестве сертификата Сервера администрирования Kaspersky Security Center.
7. Если требуется загрузить новый сертификат администратора, в блоке **Сертификат сервера Kaspersky Security Center** нажмите на кнопку **Загрузить** и в открывшемся окне выберите файл сертификата. Для добавления в качестве сертификата доступны файлы только в формате CRT, PEM, DER и CER.

   Сертификат Сервера администрирования Kaspersky Security Center будет загружен в систему.
8. Если у вас есть загруженный сертификат администратора и его требуется обновить, в блоке **Сертификат сервера Kaspersky Security Center** нажмите на кнопку **Обновить** и в открывшемся окне выберите файл сертификата. Для добавления в качестве сертификата доступны файлы только в формате CRT, PEM, DER и CER.

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

   Kaspersky IoT Secure Gateway 1000 не позволяет удалить сертификат Сервера администрирования Kaspersky Security Center без замены сертификата на новый.
9. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Настройка маршрутизации через Web Console

Для более гибкого управления сетевыми пакетами, которые проходят через устройство с Kaspersky IoT Secure Gateway 1000, вы можете настроить маршрутизацию.

Передача данных с помощью статических маршрутов для внутренней сети возможна только для типа сетевого устройства *сетевой роутер*.

Чтобы просмотреть таблицу маршрутизации Kaspersky IoT Secure Gateway 1000:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите **Сеть** → **Маршрутизация**.
7. Отобразится таблица маршрутизации Kaspersky IoT Secure Gateway 1000, которая содержит следующую информацию:

   - **Тип** – тип маршрута:
     - **Статический** – маршрут, для которого вручную определены параметры следования сетевых пакетов.
     - **Динамический** – маршрут, для которого параметры следования сетевых пакетов определяются автоматически, например с помощью DHCP-сервера.
   - **IP-адрес** – IP-адрес сети или узла назначения.
   - **Маска** – маска сети назначения.
   - **Шлюз** – IP-адрес шлюза в сети, на который нужно передать трафик, следующий до указанного IP-адреса сети или узла назначения.
   - **Состояние** – состояние маршрута:
     - **Активный** – маршрут применен и используется для передачи данных.
     - **Ошибка** – маршрут не применен и не может использоваться для передачи данных, так как при создании маршрута была допущена ошибка. Справа от состояния отображается описание ошибки. Состояние **Ошибка** отображается, если IP-адрес шлюза в сети недостижим или в качестве назначения были указаны недопустимые IP-адрес сети (узла назначения) или маска сети.
     - **Ожидание** – промежуточное состояние. После выполнения синхронизации с Kaspersky IoT Secure Gateway 1000 текущее состояние изменится на **Активный** или **Ошибка**.

Вы можете создавать, изменять и удалять маршруты Kaspersky IoT Secure Gateway 1000 через Web Console. Также вы можете настроить маршрутизацию в интерфейсе Kaspersky IoT Secure Gateway 1000.

Создание статического маршрута через Web Console

Вы можете создавать новые статические маршруты Kaspersky IoT Secure Gateway 1000 через Web Console.

Kaspersky IoT Secure Gateway 1000 не позволяет создавать дублирующие маршруты по умолчанию (второй маршрут для IP-адреса сети назначения 0.0.0.0/0) и маршруты, в которых в качестве IP-адреса узла назначения указан IP-адрес, принадлежащий сети 127.0.0.0/8.

При создании пересекающихся маршрутов, рекомендуется учитывать, что для отправки сетевого пакета на IP-адрес сети или узла назначения будет выбираться маршрут с более длинной маской, описывающей меньшее количество узлов назначения.

Чтобы создать новый статический маршрут Kaspersky IoT Secure Gateway 1000 через Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите **Сеть** → **Маршрутизация**.

   Отобразится окно с таблицей маршрутизации Kaspersky IoT Secure Gateway 1000.
7. Нажмите на кнопку **Добавить** в верхней части страницы.
8. В открывшейся справа панели **Добавление маршрута** укажите следующие данные:
   - В поле **IP-адрес** введите IP-адрес сети или узла назначения.
   - В поле **Маска** введите маску сети назначения.
   - В поле **Шлюз** введите IP-адрес шлюза. IP-адрес шлюза должен быть достижимым.

     IP-адрес шлюза является достижимым, если этот IP-адрес расположен в подключенной сети и является одним из узлов сети, настроенной на внутреннем или внешнем интерфейсе.
9. Нажмите на кнопку **OK** в нижней части панели, чтобы сохранить изменения.

Новый статический маршрут будет создан и отобразится в таблице маршрутизации.

Изменение статического маршрута через Web Console

Чтобы изменить статический маршрут Kaspersky IoT Secure Gateway 1000 через Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.

6. Выберите раздел **Сеть** → **Маршрутизация**.

   Отобразится окно с таблицей маршрутизации Kaspersky IoT Secure Gateway 1000.

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

8. В открывшейся справа панели **Изменение маршрута** внесите изменения и нажмите на кнопку **ОК**, чтобы сохранить изменения.

Статический маршрут будет изменен, и новые данные по нему отобразятся в таблице маршрутизации.

Удаление статического маршрута через Web Console

Чтобы удалить статический маршрут Kaspersky IoT Secure Gateway 1000 через Web Console:

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

2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.

3. В открывшемся окне свойств устройства выберите вкладку **Программы**.

4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.

5. Выберите вкладку **Параметры программы**.

6. Выберите раздел **Сеть** → **Маршрутизация**.

   Отобразится окно с таблицей маршрутов Kaspersky IoT Secure Gateway 1000.

7. В таблице установите флажок около того маршрута, который требуется удалить, нажмите на кнопку **Удалить** в верхней части таблицы и подтвердите свои действия.

Статический маршрут будет удален из таблицы маршрутизации.

Настройка параметров сотового соединения Kaspersky IoT Secure Gateway 1000 через Web Console

Если к устройству не подключен модем, использование сотового соединения в Kaspersky IoT Secure Gateway 1000 и настройка параметров такого соединения через Web Console недоступны.

Вы можете просматривать и настраивать параметры сотового соединения Kaspersky IoT Secure Gateway 1000 через Web Console в разделе **Сеть** → **Модем**. Раздел содержит следующую информацию о сотовом соединении Kaspersky IoT Secure Gateway 1000:

- Блок **Параметры модема**, в котором указана информация о статусе работы модема и текущем уровне сигнала.

- Блок **Адреса DNS-серверов модема**, в котором указана информация об IP-адресах основного и дополнительного DNS-серверов модема.

- Таблица **Профили модема**, в которой отображается информация о доступных профилях модема.
- Блок **Параметры трансляции**, в котором вы можете настроить использование маскарадинга для сотового соединения.

  При включении маскарадинга адрес отправителя во внутренней сети подменяется динамически, в зависимости от назначенного интерфейсу адреса, на адрес во внешней сети.

В Kaspersky IoT Secure Gateway 1000 предусмотрено два типа профилей модема:

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

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

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

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

  Если модем недоступен для использования (отображается статус модема **Недоступен**) требуется выполнить перезагрузку Kaspersky IoT Secure Gateway 1000 и снова проверить доступность модема для использования. Устройствам, которые выходят в интернет через Kaspersky IoT Secure Gateway 1000, необходимо получать параметры внутренней сети через DHCP-сервер Kaspersky IoT Secure Gateway 1000. Нужные адреса DNS-серверов от операторов сотовой сети будут получены месте с этими параметрами.

Включение и выключение сотового соединения Kaspersky IoT Secure Gateway 1000 через Web Console

Kaspersky IoT Secure Gateway 1000 позволяет обрабатывать исходящий и входящий сетевой трафик с использованием сотового соединения (через оператора сотовой связи). Вы можете включить или выключить использование сотового соединения Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console. По умолчанию использование сотового соединения выключено.

Чтобы включить или выключить использование сотового соединения Kaspersky IoT Secure Gateway 1000 через Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.

5. Выберите вкладку **Параметры программы**.

6. Выберите раздел **Сеть → Модем**.

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

Сотовое соединение Kaspersky IoT Secure Gateway 1000 будет включено или выключено. При необходимости вы можете включить трансляцию сетевых адресов для модема.

Создание профиля модема Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console

Вы можете создавать новые профили модема Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console. Разные профили модема позволяют работать с разными операторами сотовой связи.

Чтобы создать новый профиль модема Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console:

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

2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.

3. В открывшемся окне свойств устройства выберите вкладку **Программы**.

4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.

5. Выберите вкладку **Параметры программы**.

6. Выберите раздел **Сеть → Модем**.

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

   Справа откроется панель добавления профиля модема.

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

   - **Активный**. Выбранный профиль модема будет использоваться как основной для работы сотового соединения Kaspersky IoT Secure Gateway 1000. В таблице **Профили** в столбце **Статус** рядом с активным профилем появится значок .
   - **Неактивный**.

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

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

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

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

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

Изменение профиля модема Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console

Вы можете изменять параметры профиля модема Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console.

Чтобы изменить параметры профиля модема Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Сеть** → **Модем**.
7. В таблице **Профили модема** установите флажок около того профиля модема, который требуется изменить и нажмите на кнопку **Изменить** в верхней части таблицы.
8. В открывшейся справа панели изменения профиля модема выполните следующие действия:

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

   - **Активный**. После сохранения изменений, выбранный профиль модема будет использоваться как основной для работы сотового соединения Kaspersky IoT Secure Gateway 1000. В таблице **Профили** в столбце **Статус** рядом с активным профилем появится значок .
   - **Неактивный**.

   При изменении статуса профиля модема на **Активный** потребуется перезагрузить Kaspersky IoT Secure Gateway 1000, чтобы изменения вступили в силу.

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

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

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

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

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

Удаление профиля модема Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console

Вы можете удалить профиль модема через Kaspersky Security Center 14.2 Web Console.

Kaspersky IoT Secure Gateway 1000 не позволяет удалить активный и предустановленный профили модема. Если требуется удалить профиль, который сейчас является активным, сначала нужно выбрать активным другой профиль модема.

Чтобы удалить профиль Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Сеть** → **Модем**.
7. В таблице **Профили модема** установите флажок около того профиля модема, который требуется удалить и нажмите на кнопку **Удалить**.

   Выбранный профиль модема оператора будет удален из таблицы **Профили модема**.
8. Нажмите на кнопку **Сохранить** в нижней части окна настройки параметров модема, чтобы сохранить изменения.

Выбранный профиль модема будет удален.

Настройка веб-сервера через Web Console

Работу веб-интерфейса Kaspersky IoT Secure Gateway 1000 обеспечивает веб-сервер CivetWeb. Параметры веб-сервера хранятся в конфигурационном файле, безопасность подключения обеспечивает сертификат веб-сервера. Kaspersky IoT Secure Gateway 1000 поставляется с предустановленным сертификатом веб-сервера, который подписан "Лабораторией Касперского".

Через Web Console вы можете загрузить новый сертификат веб-сервера и ключ к нему.

Если вы не заменили сертификат веб-сервера по умолчанию при первом подключении к веб-интерфейсу Kaspersky IoT Secure Gateway 1000, после первого подключения к Web Console требуется заменить сертификат веб-сервера по умолчанию на сертификат, используемый в вашей организации.

Чтобы загрузить новый сертификат веб-сервера:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Параметры** → **Веб-сервер**.
7. Чтобы загрузить сертификат, в блоке **Сертификат веб-сервера** выполните одно из следующих действий:
   - Если у вас не добавлен сертификат, нажмите на кнопку **Загрузить сертификат** и в открывшемся окне загрузки выберите файл сертификата в формате CRT, CER, DER или PEM.
   - Если у вас уже добавлен сертификат и вы хотите его заменить, нажмите на кнопку **Заменить** и в открывшемся окне загрузки выберите файл сертификата в формате CRT, CER, DER или PEM.

   Необходимо загрузить правильный файл действующего сертификата. Загрузка неправильного файла сертификата может привести к неработоспособности устройства.
8. Чтобы загрузить ключ сертификата, в блоке **Ключ сертификата** выполните одно из следующих действий:
   - Если у вас не добавлен ключ, нажмите на кнопку **Загрузить ключ** и в открывшемся окне загрузки выберите файл ключа в формате KEY.
   - Если у вас уже добавлен ключ и вы хотите его заменить, нажмите на кнопку **Заменить** и в открывшемся окне загрузки выберите файл ключа в формате KEY.
9. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

В разделе **Параметры** → **Веб-сервер** отобразится следующая информация об используемом сертификате и ключе веб-сервера:

- В блоке **Сертификат веб-сервера**:
  - **Имя файла** – имя файла сертификата и его формат.
  - **Имя субъекта** – информация о программе, для которой выпущен сертификат.
  - **Издатель** – информация об организации, выпустившей сертификат.
  - **Действителен до** – дата и время окончания действия сертификата.

- В блоке **Ключ сертификата** отобразится **Имя файла** – имя файла ключа сертификата и его формат.

Фильтрация трафика прикладных протоколов через Web Console

Вы можете настроить фильтрацию сетевого трафика для прикладных протоколов через Web Console. Фильтрация позволяет заблокировать или разблокировать сетевой трафик, проходящий на уровне прикладных протоколов FTP, HTTP, MQTT, Modbus, SMTP, IMAP, POP3.

Для протокола MQTT поддерживается только фильтрация версии 3.1.1. Для протокола SMTP поддерживается фильтрация только базового SMTP, и не поддерживается фильтрация протокола Extended SMTP.

Чтобы настроить фильтрацию трафика прикладных протоколов:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Сеть** → **Фильтрация**.
7. Настройте фильтрацию трафика прикладных протоколов, выполнив следующие действия:
   - Установите флажок напротив тех протоколов, для которых вы хотите заблокировать прохождение трафика.
   - Снимите флажок напротив тех протоколов, для которых вы хотите разрешить прохождение трафика.

   По умолчанию трафик разрешен для всех прикладных протоколов.
8. Нажмите на кнопку **Сохранить** в нижней части страницы, чтобы сохранить изменения.

Kaspersky IoT Secure Gateway 1000 заблокирует весь трафик для выбранных прикладных протоколов, кроме служебного трафика, а также разрешит прохождение трафика на уровне прикладных протоколов, для которых вы сняли флажок.

При получении пакета трафика, содержащего признаки заблокированного прикладного протокола, Kaspersky IoT Secure Gateway 1000 разрывает соединение, по которому проходил обмен этим трафиком. При этом после обнаружения трафика несколько пакетов, необходимые для установления соединения, могут пройти через Kaspersky IoT Secure Gateway 1000, но затем соединение будет разорвано.

Настройка сетевого кластера

Вы можете объединить несколько устройств Kaspersky IoT Secure Gateway 1000 в отказоустойчивый сетевой кластер во внутренней сети. Объединение устройств в сетевой кластер позволяет вам назначить одно основное устройство, которое будет получать и передавать трафик, и одно или несколько дублирующих устройств. В случае отказа основного устройства трафик будет проходить через дублирующее устройство.

Вам нужно настроить параметры сетевого кластера на каждом устройстве Kaspersky IoT Secure Gateway 1000, которое вы хотите добавить в сетевой кластер.

В целях безопасности мы рекомендуем настраивать на портах, к которым подключен Kaspersky IoT Secure Gateway 1000 как сетевой кластер, функцию Port Security с фиксацией MAC-адресов в списке разрешенных, а так же запретить отправку IP-пакетов с адресом назначения 224.0.0.18/32 с других портов. Это необходимо, чтобы только устройства с фиксированными MAC-адресами с определенных портов могли отправлять VRRP-пакеты.

Устройства в сетевом кластере независимы друг от друга. Синхронизация данных и конфигураций между устройствами не предусмотрена.

Чтобы настроить параметры сетевого кластера через Kaspersky Security Center 14.2 Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Сеть** → **Сетевой кластер**.
7. Переведите переключатель в положение **Включить сетевой кластер** и укажите следующие параметры:

   a. В поле **Приоритет устройства** введите значение приоритета для текущего устройства в сетевом кластере.

   Вы можете указать значение от 0 до 254. Приоритет определяет роль устройства в кластере. Устройство с наименьшим числом в значении приоритета считается основным, устройства с большим числом в значении приоритета считаются дублирующими. Чем меньше число приоритета дублирующего устройства, тем выше оно в очереди в случае отказа основного устройства.

   В сетевом кластере может быть только одно основное устройство.

   b. В поле **IP-адрес кластера** введите IP-адрес кластера во внутренней сети.

   Указанный IP-адрес будет развернут на устройстве.

c. В поле **Маска IP-адреса кластера** введите маску подсети IP-адреса сетевого кластера.

d. В поле **Идентификатор кластера** введите уникальный идентификатор сетевого кластера.

Идентификатор требуется того, чтоб узлы кластера могли однозначно распознавать друг друга. Однако использование идентификатора не гарантирует защиту от действий третьих лиц. При создании сети вам нужно также обеспечить безопасность сетевого контура кластера.

Для избежания наложения идентификаторов мы рекомендуем указать пользовательское значение идентификатора.

Для каждого устройства, которое вы хотите объединить в сетевой кластер, необходимо указать одинаковые значения виртуального IP-адреса, маски IP-адреса и идентификатор кластера.

8. Если вы хотите сбросить указанные параметры сетевого кластера, нажмите на кнопку **Отмена**.

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

Устройство будет добавлено в сетевой кластер по указанному IP-адресу.

Настройка уведомлений через Kaspersky Security Center 14.2 Web Console

Этот раздел содержит информацию о настройке уведомлений через Kaspersky Security Center 14.2 Web Console при регистрации событий в системе.

Настройка отправки уведомлений на сервер Syslog через Kaspersky Security Center 14.2 Web Console

Kaspersky IoT Secure Gateway 1000 включает в себя Syslog-клиент, с помощью которого вы можете отправлять уведомления о событиях на сервер Syslog. Вы можете настраивать отправку уведомлений на сервер Syslog через Kaspersky Security Center 14.2 Web Console.

Чтобы настроить отправку уведомлений на сервер Syslog:

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

2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.

3. В открывшемся окне свойств устройства выберите вкладку **Программы**.

4. Нажмите **Kaspersky IoT Secure Gateway**.

Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.

5. Выберите вкладку **Параметры программы**.

6. Выберите раздел **Параметры** → **Уведомления** → **Syslog**.

7. Установите переключатель в верхней части окна в положение **Использовать сервер Syslog для передачи событий** и укажите следующие параметры:

   - В поле **IP-адрес** укажите IP-адрес сервера Syslog.
   - В поле **Порт** укажите порт, по которому будет осуществляться подключение.
   - В раскрывающемся списке **Режим** выберите один из вариантов подключения:
     - **UDP**.
     - **TCP**.
     - **TLS**.
   - Если для отправки журналов выбран протокол TLS, загрузите сертификат безопасности. Для этого нажмите на кнопку **Загрузить сертификат** и в открывшемся окне выберите нужный сертификат безопасности.

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

Kaspersky IoT Secure Gateway 1000 будет отправлять уведомления о событиях на сервер Syslog.

Настройка отправки MQTT-уведомлений через Kaspersky Security Center 14.2 Web Console

Kaspersky IoT Secure Gateway 1000 может отправлять уведомления о событиях аудита по протоколу MQTT. Вы можете настроить отправку MQTT-уведомлений через Kaspersky Security Center 14.2 Web Console.

Чтобы включить отправку MQTT-уведомлений через Kaspersky Security Center 14.2 Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Параметры** → **Уведомления** → **MQTT-уведомления**.
7. Переведите переключатель в положение **Использовать MQTT для передачи событий**.
8. В поле **Адрес сервера** введите IP-адрес используемого сервера MQTT.
9. В поле **Порт** введите номер порта, используемого для соединения с сервером MQTT.

   Для соединения Kaspersky IoT Secure Gateway 1000 с сервером MQTT, который находится во внутренней сети вы можете использовать порты 1883 и 8883.

Для соединения Kaspersky IoT Secure Gateway 1000 с сервером MQTT, который находится во внешней сети вы можете использовать порт 8883.

10. В поле **Имя MQTT-топика** укажите имя MQTT-топика для отправки уведомлений.

11. Если требуется отправлять уведомления о событиях аудита от имени определенного пользователя, переведите переключатель **Использовать аутентификацию** в положение включено и заполните поля **Имя пользователя** и **Пароль**. Учетные данные пользователя, от имени которого требуется отправлять уведомления, вы можете узнать у администратора используемого сервера MQTT.

    По умолчанию отправка уведомлений от имени пользователя выключена.

12. Если требуется использовать защищенное SSL-соединение, установите переключатель **Использовать защищенное SSL-соединение** в положение включено и выполните следующие действия:

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

       Информация о загруженном сертификате удостоверяющего центра отобразится на странице.

       > Не рекомендуется загружать широко известные сертификаты удостоверяющего центра, так как доверенными будут являться все серверы, использующие сертификаты, подписанные этими сертификатами удостоверяющего центра. Такая ситуация может привести к компрометации Kaspersky IoT Secure Gateway 1000.

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

       Информация о загруженном сертификате клиента отобразится на странице.

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

    По умолчанию использование защищенного SSL-соединения выключено.

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

Kaspersky IoT Secure Gateway 1000 будет отправлять уведомления о событиях аудита по протоколу MQTT.

Управление событиями Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console

Этот раздел содержит инструкции по мониторингу событий аудита, зарегистрированных в Kaspersky IoT Secure Gateway 1000, через Kaspersky Security Center 14.2 Web Console.

Просмотр событий Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console

Вы можете просматривать события аудита, зарегистрированные Kaspersky IoT Secure Gateway 1000, через Kaspersky Security Center 14.2 Web Console. События аудита включают события аудита операционной системы и события аудита сетевого экрана.

Чтобы просмотреть события аудита, зарегистрированные Kaspersky IoT Secure Gateway 1000, через Kaspersky Security Center 14.2 Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Нажмите на вкладку **События**.

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

   - **Время** – дата и время, когда было зарегистрировано событие.
   - **Событие** – текст и описание события.
   - **Уровень критичности** – уровень критичности события:
     - 4 – критическое;
     - 3 – отказ функционирования;
     - 2 – предупреждение;
     - 1 – информационное сообщение.

Настройка регистрации событий Kaspersky IoT Secure Gateway 1000 в Kaspersky Security Center 14.2 Web Console

Вы можете включить регистрацию событий аудита Kaspersky IoT Secure Gateway 1000 в Kaspersky Security Center 14.2 Web Console и настроить оповещение при регистрации событий аудита. Подробную информацию о настройке оповещений при регистрации событий аудита в Web Console см. в разделе *Настройка параметров доставки уведомлений* в онлайн-справке Kaspersky Security Center 14.2. Для настройки регистрации событий аудита предварительно требуется создать политику для устройства, от которого планируется получать события аудита. Подробную информацию о создании политики см. в разделе *Создание политики* в онлайн-справке Kaspersky Security Center 14.2.

> В версии Kaspersky IoT Secure Gateway 1000 3.0 не поддерживается управление группой устройств с помощью политик Kaspersky Security Center. Вы можете управлять каждым устройством отдельно.

Каждое событие аудита в Kaspersky Security Center имеет определенный уровень критичности. В зависимости от условий возникновения, событию аудита может быть присвоен один из следующих уровней критичности:

- *Критическое* – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.

- *Отказ функционирования* – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы системы или выполнения процедуры.
- *Предупреждение* – событие, на которое нужно обратить внимание, поскольку оно отражает важные ситуации в работе Kaspersky IoT Secure Gateway 1000 и может указывать на возможную проблему в будущем. Чаще всего события относятся к предупреждениям, если после их возникновения работа системы может быть восстановлена без потери данных или функциональных возможностей.
- *Информационное сообщение* – событие, информирующее об успешном выполнении операции, корректной работе системы или завершении процедуры.

Если регистрация событий аудита Kaspersky IoT Secure Gateway 1000 выключена в Web Console, то события аудита не приходят и не отображаются в Web Console. После включения регистрации в Web Console будут поступать только новые события аудита. Все события аудита, зарегистрированные Kaspersky IoT Secure Gateway 1000 до включения регистрации в Web Console, не будут переданы в Web Console, их просмотр возможен только в веб-интерфейсе Kaspersky IoT Secure Gateway 1000.

Чтобы включить регистрацию событий аудита Kaspersky IoT Secure Gateway 1000 в Kaspersky Security Center 14.2 Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства, на котором запущен Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Нажмите на вкладку **Настройка событий**.
6. В меню в левой части окна выберите уровень важности, для которого требуется включить регистрацию событий:
   - **Критическое**.
   - **Отказ функционирования**.
   - **Предупреждение**.
   - **Информационное сообщение**.

   Отобразится таблица событий аудита для выбранного уровня важности.
7. Нажмите на кнопку **Добавить событие**.
8. Установите флажок около тех типов событий, для которых требуется включить регистрацию в Web Console, и нажмите на кнопку **ОК**.
9. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Выбранные типы событий аудита Kaspersky IoT Secure Gateway 1000 для выбранного уровня важности будут регистрироваться и храниться на Сервере администрирования Kaspersky Security Center. По умолчанию срок хранения событий составляет 30 дней.

Настройка правил адресной трансляции через Web Console

Правила адресной трансляции доступны только для типа сетевого устройства *сетевой роутер*.

В Kaspersky IoT Secure Gateway 1000 реализована переадресация портов (англ. port forwarding или destination NAT) – тип адресной трансляции, который подменяет адрес отправителя во внешней сети на адрес во внутренней сети, обеспечивая доступ из внешней сети во внутреннюю по отдельным портам. Правила адресной трансляции описывают параметры преобразования сетевых адресов IP-пакетов, отправленных во внутреннюю сеть от устройств, расположенных во внешней сети.

Все правила адресной трансляции отображаются в таблице в разделе **Сеть** → **NAT**. Для каждого правила отображаются следующие параметры:

- **Сетевой интерфейс** – интерфейс, для которого применяется правило: **Внешняя сеть** или **Модем**.
- **Внешний порт** – транспортный порт внешнего интерфейса, для которого применяется правило.
- **Протокол** – протокол, для которого примеряется правило: **TCP** или **UDP**.
- **IP-адрес** – IP-адрес узла назначения.
- **Порт** – порт узла назначения.
- **Комментарий** – описание правила, не более 255 символов.

Вы можете создавать, изменять и удалять правила адресной трансляции.

Создание правила адресной трансляции через Web Console

Чтобы создать новое правило адресной трансляции через Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите **Сеть** → **NAT**.

   Откроется окно с таблицей правил адресной трансляции Kaspersky IoT Secure Gateway 1000.
7. Нажмите на кнопку **Добавить** в верхней части страницы.
8. В открывшейся справа панели **Добавление правила** укажите следующие данные:

- В раскрывающемся списке **Сетевой интерфейс** выберите интерфейс, для которого будет применяться правило: **Внешняя сеть** или **Модем**.
- В поле **Внешний порт** введите номер транспортного порта внешнего интерфейса, для которого будет применяться правило.
- В раскрывающемся списке **Протокол** выберите один из протоколов, для которого примеряется правило: **TCP** или **UDP**.
- В поле **IP-адрес** введите IP-адрес узла назначения.
- В поле **Порт** введите порт узла назначения.
- В поле **Комментарий** введите описание правила, не более 255 символов.

9. Нажмите на кнопку **OK** в нижней части панели, чтобы сохранить изменения.

Новое правило будет создано и отобразится в таблице правил адресной трансляции.

Изменение правила адресной трансляции через Web Console

Чтобы изменить правило адресной трансляции через Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите **Сеть** → **NAT**.

   Откроется окно с таблицей правил адресной трансляции Kaspersky IoT Secure Gateway 1000.
7. В таблице установите флажок около того правила, которое требуется изменить, и нажмите на кнопку **Изменить** в верхней части таблицы.
8. В открывшейся справа панели **Изменение правила** внесите изменения и нажмите на кнопку **OK**, чтобы сохранить изменения.

Правило будет изменено, и новые данные по нему отобразятся в таблице правил адресной трансляции.

Удаление правила адресной трансляции через Web Console

Чтобы удалить правило адресной трансляции через Web Console:

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

2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.

3. В открывшемся окне свойств устройства выберите вкладку **Программы**.

4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.

5. Выберите вкладку **Параметры программы**.

6. Выберите **Сеть** → **NAT**.

   Откроется окно с таблицей правил адресной трансляции Kaspersky IoT Secure Gateway 1000.

7. В таблице выберите правило, которое требуется удалить, нажмите на кнопку **Удалить** в верхней части таблицы и подтвердите свои действия.

Правило адресной трансляции будет удалено из таблицы правил.

Управление приложением Kaspersky IoT Secure Gateway Network Protector

Kaspersky IoT Secure Gateway Network Protector позволяет блокировать IP-адреса, трафик от которых во внутренней и внешней сети требуется запретить, и разблокировать IP-адреса, трафик от которых требуется разрешить.

Kaspersky IoT Secure Gateway Network Protector может блокировать IP-адреса на основе правил анализа содержимого сетевых пакетов промышленных протоколов, которые включают правила фильтрации команд и правила обнаружения аномалий. Вы можете задать правила фильтрации в параметрах приложения.

В случае срабатывания правила Kaspersky IoT Secure Gateway Network Protector блокирует подозрительный сетевой трафик и добавляет IP-адрес, от которого идет трафик, в список запрещенных IP-адресов. Вы можете вручную удалить IP-адрес из списка запрещенных, если вам нужно разрешить сетевой трафик от этого IP-адреса.

> Kaspersky IoT Secure Gateway Network Protector может создать до 1000 правил в списке запрещенных IP-адресов.

Kaspersky IoT Secure Gateway Network Protector передает информацию о блокировке трафика и IP-адреса в Kaspersky IoT Secure Gateway 1000. Соответствующее событие регистрируется в журнале событий (в Kaspersky Security Center) и в журнале аудита сетевого экрана (в веб-интерфейсе Kaspersky IoT Secure Gateway 1000).

В список разрешенных IP-адресов входят IP-адреса внутренней и внешней сети, сетевой трафик от которых Kaspersky IoT Secure Gateway 1000 не блокирует. Вы можете вручную добавлять IP-адреса устройств, трафик от которых требуется разрешить, в список разрешенных. Сетевой трафик от IP-адресов новых устройств, появившихся в сети, по умолчанию разрешен, и эти IP-адреса не блокируется системой. При необходимости вы также можете удалять IP-адреса устройств из списка разрешенных.

Настройка фильтрации трафика промышленных протоколов через Web Console

Вы можете настроить правила для блокировки и фильтрации трафика, проходящего на уровне промышленных протоколов, с помощью приложения Kaspersky IoT Secure Gateway Network Protector. Фильтрация трафика промышленных протоколов осуществляется с помощью правил анализа содержимого сетевых пакетов и включает следующие проверки:

- фильтрация команд в протоколах MQTT и Modbus;
- проверка на аномалии трафика на уровне протоколов MQTT и Modbus.

Для работы приложения Kaspersky IoT Secure Gateway Network Protector вам нужно сначала настроить его конфигурацию. Если вы запустите приложение без настроенных параметров конфигурации, Kaspersky IoT Secure Gateway 1000 перейдет в аварийный режим, так как приложение не может получить правила фильтрации трафика для обеспечения безопасного состояния.

Чтобы настроить правила фильтрации трафика промышленных протоколов:

1. С помощью утилиты Kaspersky Update Utility скачайте файлы со списками поддерживаемых правил анализа содержимого сетевых пакетов:

   - Файл industrial_commands.rules содержит список поддерживаемых правил фильтрации команд на уровне промышленных протоколов.
   - Файл industrial_anomalies.rules содержит список поддерживаемых правил обнаружения аномалий в трафике, проходящем на уровне промышленных протоколов.

   Идентификатор (sid) 90000001 используется для служебных нужд и не может быть присвоен ни одному правилу.

   Подробную информацию по работе с утилитой вы можете узнать в документации по Kaspersky Update Utility.

2. Если необходимо, выберите из файлов те правила, которые вы хотите применить для фильтрации трафика промышленных протоколов.
3. Закодируйте список правил фильтрации команд и список правил обнаружения аномалий как две отдельные строки в Base64.
4. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
5. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
6. В открывшемся окне свойств устройства выберите вкладку **Программы**.
7. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
8. Выберите вкладку **Параметры программы**.
9. Выберите раздел **Параметры приложений** → **Приложения**.

   Отобразится таблица установленных приложений.
10. Остановите приложение Kaspersky IoT Secure Gateway Network Protector, если оно запущено.

Пока приложение Kaspersky IoT Secure Gateway Network Protector остановлено, транзитный трафик на устройстве будет заблокирован для обеспечения безопасности подключенных устройств.

11. Нажмите на название приложения Kaspersky IoT Secure Gateway Network Protector.

    Справа откроется панель **Kaspersky IoT Secure Gateway Network Protector application management**.

12. Укажите правила фильтрации трафика промышленных протоколов:

    - В поле **Rules for filtering commands in industrial protocols** укажите правила фильтрации команд на уровне промышленных протоколов в кодировке Base64.
    - В поле **Rules for searching anomalies in industrial protocols** укажите правила обнаружения аномалий в трафике, проходящем на уровне промышленных протоколов в кодировке Base64.

    Вы можете указать правила только в одном из этих полей или в обоих полях.

    > Для работы приложения Kaspersky IoT Secure Gateway Network Protector требуется указать значение хотя бы одного параметра конфигурации, иначе Kaspersky IoT Secure Gateway 1000 перейдет в аварийный режим после запуска приложения, так как приложение не может получить правила фильтрации трафика для обеспечения безопасного состояния.

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

14. Запустите приложение Kaspersky IoT Secure Gateway Network Protector.

Сетевой трафик, проходящий на уровне промышленных протоколов, будет фильтроваться с использованием указанных правил. В случае срабатывания правила сетевой трафик, соответствующий этому правилу, будет заблокирован, а IP-адрес, от которого идет трафик, будет добавлен в список запрещенных IP-адресов. Информация о блокировке IP-адреса передается в сетевой экран Kaspersky IoT Secure Gateway 1000. Событие о блокировке трафика будет записано в журнал событий аудита.

Добавление IP-адреса в список разрешенных IP-адресов

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

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

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Сеть** → **Network Protector**.
7. Нажмите на кнопку **Показать список** напротив заголовка **Список разрешенных IP-адресов**.

Отобразится окно **Список разрешенных IP-адресов**.

8. Если вы хотите отфильтровать список IP-адресов, нажмите на кнопку **Фильтр**, укажите и примените критерии фильтрации.

9. Нажмите на кнопку **Добавить**.

10. В открывшейся справа панели в поле **IP-адрес (источник)** укажите IP-адрес, трафик от которого вы хотите разрешить.

    Введенный IP-адрес должен соответствовать следующим требованиям:

    - содержит четыре числа от 0 до 255 и знак разделения `.` между ними;
    - не начинается с 0;
    - не пустой;
    - не соответствует 255.255.255.255.

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

12. Нажмите на кнопку **Сохранить** в нижней части страницы **Список разрешенных IP-адресов**.

IP-адрес устройства будет добавлен в список разрешенных IP-адресов. После синхронизации Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center 14.2 Web Console изменения в списке разрешенных IP-адресов будут переданы в Kaspersky IoT Secure Gateway 1000.

Изменение IP-адреса в списке разрешенных IP-адресов

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

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

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

2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.

3. В открывшемся окне свойств устройства выберите вкладку **Программы**.

4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.

5. Выберите вкладку **Параметры программы**.

6. Выберите раздел **Сеть** → **Network Protector**.

7. Нажмите на кнопку **Показать список** напротив заголовка **Список разрешенных IP-адресов**.

   Отобразится окно **Список разрешенных IP-адресов**.

8. Если вы хотите отфильтровать список IP-адресов, нажмите на кнопку **Фильтр**, укажите и примените критерии фильтрации.

9. Выберите IP-адрес устройства, который требуется изменить, и нажмите на кнопку **Изменить** в верхней части таблицы.

10. В открывшейся справа панели в поле **IP-адрес (источник)** измените IP-адрес, трафик от которого вы хотите разрешить.

    Введенный IP-адрес должен соответствовать следующим требованиям:

    - содержит четыре числа от 0 до 255 и знак разделения **.** между ними;
    - не начинается с 0;
    - не пустой;
    - не соответствует 255.255.255.255.

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

12. Нажмите на кнопку **Сохранить** в нижней части страницы **Список разрешенных IP-адресов**.

    IP-адрес устройства в списке разрешенных IP-адресов будет обновлен. После синхронизации Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center 14.2 Web Console изменения в списке разрешенных IP-адресов будут переданы в Kaspersky IoT Secure Gateway 1000.

Удаление IP-адреса из списка разрешенных IP-адресов

Вы можете удалить IP-адрес из списка разрешенных IP-адресов устройств.

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

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

2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.

3. В открывшемся окне свойств устройства выберите вкладку **Программы**.

4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.

5. Выберите вкладку **Параметры программы**.

6. Выберите раздел **Сеть** → **Network Protector**.

7. Нажмите на кнопку **Показать список** напротив заголовка **Список разрешенных IP-адресов**.

   Отобразится окно **Список разрешенных IP-адресов**.

8. Если вы хотите отфильтровать список IP-адресов, нажмите на кнопку **Фильтр**, укажите и примените критерии фильтрации.

9. Выберите IP-адрес устройства, который требуется удалить из списка разрешенных IP-адресов, и нажмите на кнопку **Удалить** в верхней части таблицы.

10. Нажмите на кнопку **Сохранить** в нижней части панели.

11. Нажмите на кнопку **Сохранить** в нижней части страницы **Список разрешенных IP-адресов**.

    Выбранный IP-адрес будет удален из списка разрешенных IP-адресов. После синхронизации Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center 14.2 Web Console изменения в списке разрешенных IP-адресов будут переданы в Kaspersky IoT Secure Gateway 1000.

Удаление IP-адреса из списка запрещенных IP-адресов

Вы можете удалить IP-адрес из списка запрещенных IP-адресов устройств, сетевой трафик от которых требуется запретить. Список запрещенных IP-адресов формируется на основе правил фильтрации промышленных протоколов.

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

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Сеть** → **Network Protector**.
7. Нажмите на кнопку **Показать список** напротив заголовка **Список запрещенных IP-адресов**.

   Отобразится окно **Список запрещенных IP-адресов**.
8. Если вы хотите отфильтровать список IP-адресов, нажмите на кнопку **Фильтр**, укажите и примените критерии фильтрации.
9. Выберите IP-адрес устройства, который требуется удалить из списка запрещенных IP-адресов, и нажмите на кнопку **Удалить** в верхней части таблицы.
10. Нажмите на кнопку **Сохранить** в нижней части панели.
11. Нажмите на кнопку **Сохранить** в нижней части страницы **Список разрешенных IP-адресов**.

    Выбранный IP-адрес будет удален из списка запрещенных IP-адресов. После синхронизации Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center 14.2 Web Console изменения в списке запрещенных IP-адресов будут переданы в Kaspersky IoT Secure Gateway 1000.

Управление сетевым экраном

Вы можете использовать сетевой экран Kaspersky IoT Secure Gateway 1000, чтобы контролировать и фильтровать входящий трафик из внутренней и внешней сети. Обработка сетевого трафика определяется *правилами сетевого экрана*. Трафик, прохождение которого не разрешено правилами сетевого экрана, запрещен.

Сетевой экран Kaspersky IoT Secure Gateway 1000 отслеживает состояние активных сетевых подключений и анализирует трафик с учетом параметров соединения. Это позволяет ответным пакетам проходить через сетевой экран к источнику сетевого соединения, используя те же правила сетевого экрана.

По умолчанию при запуске Kaspersky IoT Secure Gateway 1000 запрещен весь трафик (кроме служебного), следующий из внутренней сети во внешнюю. После перезагрузки Kaspersky IoT Secure Gateway 1000 загружается последняя актуальная конфигурация правил сетевого экрана.

О правилах сетевого экрана

Правила сетевого экрана разделяются на *служебные* и *пользовательские*. Kaspersky IoT Secure Gateway 1000 поддерживает правила для протоколов TCP и UDP (только IPv4). Для этих протоколов включена инспекция сетевых пакетов с хранением состояния (англ. Stateful Packet Inspection). Дополнительно сетевой экран Kaspersky IoT Secure Gateway 1000 проверяет сетевой трафик на совпадение со списками запрещенных и разрешенных IP-адресов.

Служебные правила сетевого экрана

Служебные правила поставляются в составе Kaspersky IoT Secure Gateway 1000 и обеспечивают полноценную работу сетевого экрана Kaspersky IoT Secure Gateway 1000. Вы не можете изменять эти правила, и они не отображаются в Kaspersky Security Center 14.2 Web Console. Служебные правила разрешают следующие типы соединений Kaspersky IoT Secure Gateway 1000:

- исходящие соединения с Kaspersky Security Center 14.2 Web Console по протоколу TCP;
- входящие соединения с локальным веб-сервером по протоколу HTTPS;
- исходящие соединения с сервером Syslog по протоколам TCP, UDP;
- исходящие и входящие соединения с источниками MQTT-данных по протоколу TCP;
- исходящие и входящие соединения с внешними и внутренними серверами DNS по протоколу UDP;
- исходящие и входящие соединения с устройствами, объединенными в сетевой кластер (если активирован и настроен).

Пользовательские правила сетевого экрана

Вы можете создавать пользовательские правила сетевого экрана вручную, а также изменять или удалять правила этого типа. Изменения в конфигурации пользовательских правил применяются к системе после синхронизации Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center. Пользовательские правила сетевого экрана выполняются в заданном в Kaspersky Security Center 14.2 Web Console порядке сверху вниз. Вы можете создать до 512 пользовательских правил сетевого экрана. События о создании, изменении и удалении пользовательских правил, а также о достижении их предельного количества фиксируются в журнале событий.

Пользовательские правила также могут поставляться от сторонних средств обнаружения вторжений, с которыми интегрирован Kaspersky IoT Secure Gateway 1000 с помощью Kaspersky Security Center OpenAPI™.

Kaspersky IoT Secure Gateway 1000 не может самостоятельно обнаруживать атаки из внешней сети. Для этого требуется интеграция со сторонними средствами обнаружения вторжений. Kaspersky IoT Secure Gateway 1000 и средства обнаружения вторжений должны быть подключены к одному Серверу администрирования Kaspersky Security Center.

При обнаружении подозрительной сетевой активности или возможного вторжения из внешней сети сторонняя система обнаружения вторжений передает в Kaspersky IoT Secure Gateway 1000 правило для блокировки источника подозрительной сетевой активности. Kaspersky IoT Secure Gateway 1000 создает это правило в сетевом экране и на основании этого правила блокирует источник по IP-адресу.

Созданное правило действует бессрочно. При необходимости вы можете удалить правило вручную.

Вы можете просмотреть таблицу пользовательских правил сетевого экрана в Kaspersky Security Center 14.2 Web Console в разделе **Сеть** → **Сетевой экран**. Для каждого правила отображается следующая информация:

- **Статус правила** – статус активности пользовательского правила: **Включено** или **Выключено**.
- **Действие** – действие, применяемое к проходящему через сетевой экран трафику: **Разрешить** или **Запретить**.
- **Область** – область применения пользовательского правила: **Внутренняя сеть** или **Внешняя сеть**.
- **IP-адрес (источник)** – IP-адрес источника сетевого трафика.
- **Порт (источник)** – порт источника сетевого трафика.
- **IP-адрес (получатель)** – IP-адрес получателя сетевого трафика.
- **Порт (получатель)** – порт получателя сетевого трафика.
- **Протокол** – протокол, используемый при проверке сетевого трафика: **TCP**, **UDP**.

Существуют следующие ограничения для пользовательских правил сетевого экрана Kaspersky IoT Secure Gateway 1000:

- Не допускается в качестве IP-адреса источника и получателя сетевого трафика указывать доменное имя устройства (в том числе localhost – стандартное доменное имя для частных IP-адресов).
- Не допускается в качестве порта источника и получателя использовать служебные порты, зарезервированные системой: 53, 67, 68, 443, 13294, 1883, 8883, 514.

Порядок обработки сетевого трафика

Kaspersky IoT Secure Gateway 1000 обрабатывает сетевой трафик на уровне пакетов в соответствии с правилами сетевого экрана и списками разрешенных и запрещенных IP-адресов.

Kaspersky IoT Secure Gateway 1000 прекращает обработку сетевого пакета при первом совпадении с правилом, все нижестоящие правила будут проигнорированы.

Порядок обработки сетевого трафика отличается для типов сетевого устройства однонаправленный шлюз и сетевой роутер. Тип сетевого устройства задается при установке Kaspersky IoT Secure Gateway 1000.

Порядок обработки сетевого трафика для типа устройства однонаправленный шлюз

Если Kaspersky IoT Secure Gateway 1000 работает как однонаправленный шлюз, при обработке сетевого трафика правила применяются в разном порядке в зависимости от типа сети.

Для трафика внешней сети правила применяются в следующем порядке:

1. Разрешающие диагностические правила сетевого экрана.

   Эти правила поставляются в составе Kaspersky IoT Secure Gateway 1000. Они необходимы для прохождения трафика при запуске самодиагностики Kaspersky IoT Secure Gateway 1000.

   Вы не можете изменять эти правила, и они не отображаются в Kaspersky Security Center 14.2 Web Console.

2. Разрешающие правила прохождения исходящего трафика.

   Эти правила поставляются в составе Kaspersky IoT Secure Gateway 1000. Они необходимы для прохождения трафика от устройства во внутренней сети к устройству во внешней сети.

   Вы не можете изменять эти правила, и они не отображаются в Kaspersky Security Center 14.2 Web Console.

3. Разрешающие служебные правила сетевого экрана.

   Эти правила поставляются в составе Kaspersky IoT Secure Gateway 1000. Они разрешают прохождение трафика с использованием протокола ICPM.

   Вы не можете изменять эти правила, и они не отображаются в Kaspersky Security Center 14.2 Web Console.

4. Разрешающие правила приложения VPN.

   Эти правила поставляются автоматически после установки приложения VPN. Они необходимы для прохождения трафика, инициированного приложением VPN.

   Вы не можете изменять эти правила, и они не отображаются в Kaspersky Security Center 14.2 Web Console.

5. Запрещающие служебные правила сетевого экрана.

   Эти правила поставляются в составе Kaspersky IoT Secure Gateway 1000. Они необходимы для блокировки всего входящего трафика.

   Вы не можете изменять эти правила, и они не отображаются в Kaspersky Security Center 14.2 Web Console.

Для трафика внутренней сети правила применяются в следующем порядке:

1. Разрешающие диагностические правила сетевого экрана.

   Эти правила поставляются в составе Kaspersky IoT Secure Gateway 1000. Они необходимы для прохождения трафика при запуске самодиагностики Kaspersky IoT Secure Gateway 1000.

   Вы не можете изменять эти правила, и они не отображаются в Kaspersky Security Center 14.2 Web Console.

2. Разрешающие правила прохождения исходящего трафика.

   Эти правила поставляются в составе Kaspersky IoT Secure Gateway 1000. Они необходимы для прохождения трафика между устройствами во внутренней сети.

   Вы не можете изменять эти правила, и они не отображаются в Kaspersky Security Center 14.2 Web Console.

3. Разрешающие служебные правила сетевого экрана для трафика.

   Эти правила поставляются в составе Kaspersky IoT Secure Gateway 1000. Они разрешают прохождение трафика с использованием протоколов ICPM и CARP, а также трафика веб-интерфейса Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center 14.2 Web Console.

   Вы не можете изменять эти правила, и они не отображаются в Kaspersky Security Center 14.2 Web Console.

4. Запрещающие правила фильтрации трафика прикладных протоколов.

Вы можете самостоятельно выбрать прикладные протоколы, для которых вы хотите заблокировать прохождение трафика. На основе вашего выбора будут сформированы правила обработки трафика.

5. Запрещающие правила режима аварийной поддержки.

   Этот список правил применяется, только если был активирован режим аварийной поддержки. В этом случае блокируется весь трафик. Вы не можете изменять эти правила.

6. Список разрешенных IP-адресов.

   Вы можете добавлять в список разрешенных, изменять и удалять IP-адреса устройств, сетевой трафик от которых требуется разрешить, с помощью приложения Kaspersky IoT Secure Gateway Network Protector.

7. Список запрещенных IP-адресов.

   Этот список формируется автоматически на основе информации о подозрительном сетевом трафике на уровне промышленных протоколов, который фильтруется на основе правил в приложении Kaspersky IoT Secure Gateway Network Protector. Вы можете настроить правила фильтрации, с помощью которых будет блокироваться трафик, проходящий с использованием промышленных протоколов. Вы также можете удалять IP-адреса, добавленные в список запрещенных IP-адресов при необходимости.

8. Запрещающие пользовательские правила сетевого экрана.

   Эти правила для внутренней и внешней сети вы можете создавать, изменять и удалять их самостоятельно.

9. Разрешающие пользовательские правила сетевого экрана.

   Эти правила для внутренней и внешней сети вы можете создавать, изменять и удалять их самостоятельно.

10. Разрешающие служебные правила для трафика Syslog и DHCP.

    Эти правила поставляются в составе Kaspersky IoT Secure Gateway 1000. Вы не можете изменять эти правила, и они не отображаются в Kaspersky Security Center 14.2 Web Console.

11. Разрешающие правила прохождения исходящего трафика по установленным соединениям.

    Эти правила поставляются в составе Kaspersky IoT Secure Gateway 1000. Они необходимы для того, чтобы отправлять ответный трафик на запросы из внешней сети.

    Вы не можете изменять эти правила, и они не отображаются в Kaspersky Security Center 14.2 Web Console.

12. Запрещающие служебные правила сетевого экрана.

    Эти правила поставляются в составе Kaspersky IoT Secure Gateway 1000. Вы не можете изменять эти правила, и они не отображаются в Kaspersky Security Center 14.2 Web Console.

Порядок обработки сетевого трафика для типа устройства сетевой роутер

Если Kaspersky IoT Secure Gateway 1000 работает как сетевой роутер, при обработке сетевого трафика правила применяются в следующем порядке:

1. Разрешающие диагностические правила сетевого экрана.

   Эти правила поставляются в составе Kaspersky IoT Secure Gateway 1000. Они необходимы для прохождения трафика при запуске самодиагностики Kaspersky IoT Secure Gateway 1000.

   Вы не можете изменять эти правила, и они не отображаются в Kaspersky Security Center 14.2 Web Console.

2. Разрешающие служебные правила сетевого экрана для трафика.

   Эти правила поставляются в составе Kaspersky IoT Secure Gateway 1000. Они разрешают прохождение трафика с использованием протоколов ICPM и CARP, а также трафика веб-интерфейса Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center 14.2 Web Console.

Вы не можете изменять эти правила, и они не отображаются в Kaspersky Security Center 14.2 Web Console.

3. Запрещающие правила фильтрации трафика прикладных протоколов.

   Вы можете самостоятельно выбрать прикладные протоколы, для которых вы хотите заблокировать прохождение трафика. На основе вашего выбора будут сформированы правила обработки трафика.

4. Запрещающие правила режима аварийной поддержки.

   Этот список правил применяется, только если был активирован режим аварийной поддержки. В этом случае блокируется весь трафик. Вы не можете изменять эти правила.

5. Список разрешенных IP-адресов.

   Вы можете добавлять в список разрешенных, изменять и удалять IP-адреса устройств, сетевой трафик от которых требуется разрешить, с помощью приложения Kaspersky IoT Secure Gateway Network Protector.

6. Список запрещенных IP-адресов.

   Этот список формируется автоматически на основе информации о подозрительном сетевом трафике на уровне промышленных протоколов, который фильтруется на основе правил в приложении Kaspersky IoT Secure Gateway Network Protector. Вы можете настроить правила фильтрации, с помощью которых будет блокироваться трафик, проходящий с использованием промышленных протоколов. Вы также можете удалять IP-адреса, добавленные в список запрещенных IP-адресов при необходимости.

7. Разрешающие правила адресной трансляции (NAT).

   Вы можете самостоятельно создавать, изменять и удалять эти правила.

8. Запрещающие пользовательские правила сетевого экрана.

   Эти правила для внутренней и внешней сети вы можете создавать, изменять и удалять их самостоятельно.

9. Разрешающие пользовательские правила сетевого экрана.

   Эти правила для внутренней и внешней сети вы можете создавать, изменять и удалять их самостоятельно.

10. Разрешающие служебные правила для трафика Syslog, MQTT, DHCP, DNS.

    Эти правила поставляются в составе Kaspersky IoT Secure Gateway 1000. Вы не можете изменять эти правила, и они не отображаются в Kaspersky Security Center 14.2 Web Console.

11. Разрешающие правила прохождения исходящего трафика по установленным соединениям.

    Эти правила поставляются в составе Kaspersky IoT Secure Gateway 1000. Они необходимы для того, чтобы отправлять ответный трафик на запросы из внешней сети.

    Вы не можете изменять эти правила, и они не отображаются в Kaspersky Security Center 14.2 Web Console.

12. Запрещающие служебные правила сетевого экрана.

    Эти правила блокируют весь входящий трафик. Они поставляются в составе Kaspersky IoT Secure Gateway 1000. Вы не можете изменять эти правила, и они не отображаются в Kaspersky Security Center 14.2 Web Console.

Создание правил сетевого экрана

Пользовательские правила сетевого экрана выполняются в заданном в Kaspersky Security Center 14.2 Web Console порядке сверху вниз, до первого совпадения.

Вы можете создать не более 512 пользовательских правил сетевого экрана через Kaspersky Security Center 14.2 Web Console.

Чтобы создать новое правило сетевого экрана:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Сеть** → **Сетевой экран**.

   Отобразится таблица, содержащая пользовательские правила для сетевого экрана.
7. Нажмите на кнопку **Добавить** в верхней части таблицы правил сетевого экрана.

   Справа появится панель добавления правила сетевого экрана.
8. В раскрывающемся списке **Статус правила** выберите статус правила: **Включено** или **Выключено**.
9. В раскрывающемся списке **Действие** выберите действие, применяемое к проходящему через сетевой экран трафику: **Разрешить** или **Запретить**.
10. В раскрывающемся списке **Область** выберите область, к которой должно применяться правило: **Внутренняя сеть** или **Внешняя сеть**.
11. В поле **IP-адрес (источник)** укажите IP-адрес источника трафика.
12. В поле **Порт (источник)** укажите порт источника трафика, если этот параметр применим к протоколу.
13. В поле **IP-адрес (получатель)** укажите IP-адрес получателя трафика.
14. В поле **Порт (получатель)** укажите порт получателя трафика, если этот параметр применим к протоколу.
15. В раскрывающемся списке **Протокол** выберите используемый протокол. Для выбора доступны следующие варианты: **TCP (IPv4)**, **UDP (IPv4)** и **Любой**.
16. Нажмите на кнопку **OK** в панели добавления правила сетевого экрана.

    Панель закроется, новое правило отобразится в таблице правил для сетевого экрана.
17. Если требуется изменить порядок выполнения правила в таблице правил, установите флажок около правила и с помощью кнопок **Вверх** или **Вниз** повысьте или понизьте приоритет обработки правила.
18. Нажмите на кнопку **Сохранить**.

Изменение правил сетевого экрана

Чтобы изменить правило сетевого экрана:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Сеть** → **Сетевой экран**.

   Отобразится таблица, содержащая пользовательские правила для сетевого экрана.
7. Установите флажок напротив правила, которое вы хотите изменить.
8. Нажмите на кнопку **Изменить** в верхней части таблицы.

   Справа появится панель изменения правила сетевого экрана.
9. Если требуется изменить статус правила, в раскрывающемся списке **Статус** выберите статус правила: **Включено** или **Выключено**.
10. Если требуется изменить разрешение прохождения трафика, в раскрывающемся списке **Действие** выберите одно из возможных действий, применяемых к проходящему через сетевой экран трафику: **Разрешить** или **Запретить**.
11. Если требуется изменить направление трафика, в раскрывающемся списке **Область** выберите область, к которой должно применяться правило: **Внутренняя сеть** или **Внешняя сеть**.
12. При необходимости измените IP-адрес источника трафика в поле **IP-адрес (источник)**.
13. При необходимости измените порт источника трафика в поле **Порт (источник)**, если этот параметр применим к протоколу.
14. При необходимости измените IP-адрес получателя в поле **IP-адрес (получатель)**.
15. При необходимости измените порт получателя в поле **Порт (получатель)**.
16. При необходимости выберите протокол в раскрывающемся списке **Протокол**. Для выбора доступны следующие варианты: **TCP (IPv4)**, **UDP (IPv4)**, **Любой**.
17. Нажмите на кнопку **OK** в панели изменения правила сетевого экрана.

    Панель закроется, изменения в правиле отобразятся в таблице правил для сетевого экрана.
18. Если требуется изменить порядок выполнения правила в таблице правил, установите флажок рядом с правилом и с помощью кнопок **Вверх** или **Вниз** повысьте или понизьте приоритет обработки правила.

    > Пользовательские правила сетевого экрана будут выполняться в порядке расположения их в таблице правил сверху вниз, до первого совпадения.
19. Нажмите на кнопку **Сохранить**.

Удаление правил сетевого экрана

Чтобы удалить правило сетевого экрана:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Сеть** → **Сетевой экран**.
7. В отобразившейся таблице установите флажок около правила, которое вы хотите удалить и нажмите на кнопку **Удалить** в верхней части таблицы.

   Правило будет удалено из таблицы правил сетевого экрана.
8. Нажмите на кнопку **Сохранить**.

Обновление Kaspersky IoT Secure Gateway 1000 через Web Console

Вы можете выполнить полное обновление Kaspersky IoT Secure Gateway 1000. Информация об успешной загрузке и проверке обновлений, а также об обновлении Kaspersky IoT Secure Gateway 1000 записывается в разделе **Аудит**. После обновления Kaspersky IoT Secure Gateway 1000 устройство будет перезагружено.

Обновление системы возможно, только если система Kaspersky IoT Secure Gateway 1000 подключена к Kaspersky Security Center. Обновление Kaspersky IoT Secure Gateway 1000 с серверов обновлений "Лаборатории Касперского" доступно только для версии 3.0.

Чтобы выполнить полное обновление Kaspersky IoT Secure Gateway 1000:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.

6. Выберите раздел **Параметры** → **Обновления**.

7. В блоке **Полное обновление системы** нажмите на кнопку **Запустить обновление**.

   Будет выполнено полное обновление Kaspersky IoT Secure Gateway 1000. В процессе обновления устройство будет перезагружено.

Перезагрузка Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console

Чтобы перезагрузить Kaspersky IoT Secure Gateway 1000:

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

2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.

3. В открывшемся окне свойств устройства выберите вкладку **Программы**.

4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.

5. Выберите вкладку **Параметры программы**.

6. Выберите раздел **Синхронизация**.

7. В блоке **Команды** нажмите на кнопку **Перезагрузить устройство**, затем нажмите на кнопку **Сохранить** в нижней части страницы, чтобы отправить команду перезагрузки на устройство.

Устройство с Kaspersky IoT Secure Gateway 1000 будет перезагружено. Соединение Kaspersky Security Center и Kaspersky IoT Secure Gateway 1000 во время перезагрузки будет недоступно.

Управление приложениями Kaspersky IoT Secure Gateway 1000 через Web Console

Этот раздел содержит информацию об управлении приложениями Kaspersky IoT Secure Gateway 1000 через Web Console.

Работа с приложениями через Web Console

Все приложения, доступные для установки в Kaspersky IoT Secure Gateway 1000, отображаются в Web Console на вкладке **Параметры программы** → **Менеджер приложений** → **Все приложения**. Для каждого приложения в таблице отображается следующая информация:

- **Название** – название приложения. Вы можете просмотреть подробную информацию о приложении, нажав на его название.
- **Описание** – краткое описание приложения.
- **Версия** – номер последней версии приложения, доступной для установки.
- **Размер** – размер установочного пакета приложения.
- **Категория** – категории, к которым относится приложение.
- **Дата публикации** – дата публикации приложения в магазине приложений.
- **Статус** – статус установки и доступность установки приложения. Если безопасность приложения скомпрометирована, для такого приложения отображается статус **Скомпрометировано**. Скомпрометированное приложение невозможно установить.

Все установленные в Kaspersky IoT Secure Gateway 1000 приложения отображаются в Web Console на вкладке **Параметры программы** → **Менеджер приложений** → **Установленные приложения**. Для каждого установленного приложения в таблице отображается следующая информация:

- **Название** – название приложения. Вы можете просмотреть подробную информацию о приложении, нажав на его название.
- **Версия** – номер установленной версии приложения.
- **Дата публикации** – дата публикации приложения в магазине приложений.
- **Категория** – категории, к которым относится приложение.
- **Состояние** – состояние приложения (установлено или ошибка, если приложение не удалось установить или удалить).

Управление установленными в Kaspersky IoT Secure Gateway 1000 приложениями доступно на вкладке **Параметры программы** → **Параметры приложений** → **Приложения**. Для каждого приложения в таблице отображается следующая информация:

- **Название** – название приложения. Вы можете настроить конфигурацию приложения (если доступно), нажав на его название.
- **Версия** – версия установленного приложения.

- **Тип приложения** – тип приложения по функционированию в Kaspersky IoT Secure Gateway 1000.
- **Статус** – статус работы приложения (запущено или остановлено).
- **Правило запуска** – способ запуска приложения на устройстве: автоматический запуск, запуск вручную или запрет на запуск.

  Вы можете настроить правило запуска только для сконфигурированных приложений в статусе **Запущено** или **Остановлено**.
- **Манифест** – конфигурационный файл приложения. Вы можете просмотреть содержимое манифеста, нажав **Просмотреть**.

На вкладке **Параметры программы** → **Параметры приложений** → **Приложения** вы можете запустить, остановить или удалить приложение на устройстве.

Скачивание и установка приложений через Web Console

Вы можете скачать и установить в Kaspersky IoT Secure Gateway 1000 не более 20 приложений.

Чтобы скачать и установить приложение в Kaspersky IoT Secure Gateway 1000:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Менеджер приложений** → **Все приложения**.

   Отобразится таблица приложений. Для приложений, которые вы можете установить в Kaspersky IoT Secure Gateway 1000, отображается статус **Доступно для установки**.
7. Установите флажок около тех приложений, которые вы хотите скачать и установить в Kaspersky IoT Secure Gateway 1000, и нажмите на кнопку **Сохранить** в нижней части страницы.

   Для типа сетевого устройства *однонаправленный шлюз* гарантируется работа всех доступных приложений. Для типа сетевого устройства *сетевой роутер* гарантируется работа только приложений Kaspersky IoT Secure Gateway Network Protector и Kaspersky Debug Service. Вы можете установить другие приложения, но их работа на устройстве не гарантируется.

Выбранные приложения будут скачаны и установлены в Kaspersky IoT Secure Gateway 1000. После синхронизации Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center в таблице приложений для них отобразится статус **Установлено**. Информация об успешном или неуспешном скачивании и установке приложений сохраняется в журнал событий.

Установленные приложения не обновляются автоматически. Чтобы обновить приложение, вам нужно сначала удалить установленную версию приложения и затем установить его новую версию. Если вы удалите версию приложения, которая снята с публикации (не отображается во вкладке **Все приложения**), вы не сможете установить снова эту версию.

Настройка конфигурации приложения через Web Console

После установки приложения в Kaspersky IoT Secure Gateway 1000 рекомендуется настроить его конфигурацию. Параметры конфигурации для каждого приложения могут отличаться, так как определяются на стороне издателя этого приложения.

При возникновении вопросов о параметрах конфигурации приложения вы можете обратиться к компании-издателю.

Вы можете настроить правила запуска только для сконфигурированных приложений.

Чтобы настроить параметры конфигурации приложения:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Параметры приложений** → **Приложения**.

   Отобразится таблица установленных приложений.
7. Нажмите на название приложения, конфигурацию которого вы хотите настроить.

   Справа откроется панель настройки параметров приложения.
8. Укажите необходимые параметры, чтобы настроить конфигурацию приложения для его работы.
9. Нажмите на кнопку **Сохранить** в нижней части панели, чтобы сохранить изменения.

   Панель параметров приложения закроется.
10. Нажмите на кнопку **Сохранить** в нижней части страницы установленных приложений, чтобы сохранить изменения.

Параметры конфигурации приложения будут применены.

Запуск и остановка приложений через Web Console

Чтобы запустить или остановить приложение на устройстве:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Параметры приложений** → **Приложения**.

   Отобразится таблица установленных приложений.
7. Установите флажок около тех приложений, которые вы хотите запустить или остановить, и нажмите **Запустить/Остановить** в верхней части таблицы.

   Для приложений, которые имеют пользовательский интерфейс и находятся в статусе в статусе **Не настроено**, требуется сначала настроить конфигурацию и дождаться появления статуса **Остановлено**.

   После синхронизации Kaspersky Security Center с устройством ранее запущенное приложение будет остановлено в Kaspersky IoT Secure Gateway 1000, а ранее остановленное приложение будет запущено.

Управление правилами запуска приложений через Web Console

Вы можете настроить, как приложение будет запускаться в Kaspersky IoT Secure Gateway 1000 (автоматически или вручную), или запретить запуск приложения.

Чтобы настроить правила запуска приложения:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Параметры приложений** → **Приложения**.

   Отобразится таблица установленных приложений.
7. В строке приложения, для которого вы хотите настроить правило запуска, в столбце **Правило запуска** выберите одно из следующих значений в раскрывающемся списке:

   - **Автозапуск** – приложение будет запускаться автоматически при включении или перезагрузке Kaspersky IoT Secure Gateway 1000.

При необходимости вы можете останавливать и запускать приложение вручную.

- **Запуск вручную** – приложение будет запускаться только вручную по нажатию кнопки **Запустить/Остановить**.

  По умолчанию для установленного приложения применяется правило ручного запуска.

- **Запрет на запуск** – приложение будет недоступно для запуска. Кнопка **Запустить/Остановить** будет недоступна.

Если вы изменили правило запуска для запущенного приложения, правило запуска будет применено только после остановки приложений. Вы можете остановить приложение вручную, чтобы применить выбранное правило запуска.

Для приложений, которые имеют пользовательский интерфейс и находятся в статусе в статусе **Не настроено**, требуется сначала настроить конфигурацию и дождаться появления статуса **Запущено** или **Остановлено**.

После синхронизации Kaspersky Security Center с устройством правило запуска для выбранного приложение будет применено в Kaspersky IoT Secure Gateway 1000.

Удаление приложений через Web Console

Чтобы удалить приложение из Kaspersky IoT Secure Gateway 1000:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Менеджер приложений** → **Установленные приложения**.

   Отобразится таблица установленных приложений.
7. В столбце **Удаление** установите флажок около тех приложений, которые вы хотите удалить, нажмите на кнопку **Сохранить** в нижней части страницы.

Выбранные приложения будут удалены из таблицы установленных приложений. Связанные с этими приложениями маршруты перестанут работать (перейдут в статус **Ошибка**). Рекомендуется перенастроить маршруты, связанные с удаленными приложениями. После синхронизации Kaspersky Security Center с устройством, выбранные приложения, их метаданные, а также журналы событий приложений будут удалены из Kaspersky IoT Secure Gateway 1000. Информация об успешном или не успешном удалении приложений сохраняется в журнал событий.

Работа с сертификатами приложений

Сертификат приложения – это специальный файл цифровой подписи, обеспечивающий безопасную работу приложения в Kaspersky IoT Secure Gateway 1000, а также зашифрованный канал связи для обмена данными между установленным приложением и сервером приложения. Вы можете использовать сертификат удостоверяющего центра и/или сертификат клиента. Для сертификата клиента требуется также добавить ключ.

Для приложений, установленных в Kaspersky IoT Secure Gateway 1000, вы можете добавлять, обновлять и удалять сертификаты и ключи к ним.

Так же вы можете просмотреть текущие сертификаты в разделе Web Console **Параметры программы** → **Параметры приложений** → **Сертификаты**. В зависимости от типа для каждого сертификата отображается следующая информация:

- Для сертификата удостоверяющего центра отображается следующая информация:
  - **Имя файла** – имя файла сертификата удостоверяющего центра и его формат.
  - **Субъект** – информация о приложении, для которого выпущен сертификат удостоверяющего центра.
  - **Издатель** – информация об удостоверяющем центре, выпустившем сертификат.
  - **Действителен до** – дата окончания действия сертификата удостоверяющего центра.
- Для сертификата клиента отображается следующая информация:
  - **Имя файла** – имя файла сертификата клиента и его формат.
  - **Субъект** – информация о приложении, для которого выпущен сертификат клиента.
  - **Издатель** – информация об организации, выпустившей сертификат.
  - **Действителен до** – дата окончания действия сертификата клиента.
- Для ключа сертификата клиента отображается **Имя файла** ключа и его формат.

Добавление сертификатов приложений

Для приложений, установленных в Kaspersky IoT Secure Gateway 1000, вы можете добавить полный комплект сертификатов, который включает сертификат удостоверяющего центра и сертификат клиента, или только один из этих сертификатов. Для сертификата клиента вам также нужно добавить ключ.

Чтобы добавить новый сертификат удостоверяющего центра для приложения:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.

4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.

5. Выберите вкладку **Параметры программы**.

6. Выберите раздел **Параметры приложений → Сертификаты**.

7. В блоке **Сертификат удостоверяющего центра** нажмите на кнопку **Загрузить сертификат** и в открывшемся окне выберите файл сертификата. Для загрузки разрешены только следующие форматы файлов: CRT, CER, DER и PEM.

   Файл сертификата будет загружен, информация о нем отобразится на странице.

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

После синхронизации Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center сертификат удостоверяющего центра будет также добавлен в Kaspersky IoT Secure Gateway 1000. Установленное приложение, для которого выпущен сертификат удостоверяющего центра, будет использовать загруженный сертификат.

Чтобы добавить новый сертификат клиента для приложения и ключ к сертификату:

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

2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.

3. В открывшемся окне свойств устройства выберите вкладку **Программы**.

4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.

5. Выберите вкладку **Параметры программы**.

6. Выберите раздел **Параметры приложений → Сертификаты**.

7. В блоке **Сертификат клиента** выполните следующие действия:

   - Нажмите на кнопку **Загрузить сертификат** и в открывшемся окне выберите файл сертификата. Для загрузки разрешены только следующие форматы файлов: CRT, CER, DER и PEM.

   - Нажмите на кнопку **Загрузить ключ** и в открывшемся окне выберите файл ключа. Для загрузки разрешены файлы в формате KEY.

   Файлы сертификата и ключа к нему будут загружены, информация о них отобразится на странице.

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

   Вы не сможете сохранить изменения, если вы загрузили только сертификат клиента или только ключ. Требуется загрузить оба файла (сертификата и ключа), чтобы продолжить.

После синхронизации Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center сертификат клиента и ключ будут также добавлены в Kaspersky IoT Secure Gateway 1000. Установленное приложение, для которого выпущен сертификат клиента, будет использовать загруженный сертификат и ключ.

Обновление сертификатов приложений

Чтобы обновить сертификат удостоверяющего центра для приложения:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Параметры приложений** → **Сертификаты**.
7. В блоке **Сертификат удостоверяющего центра** нажмите на кнопку **Заменить** и в открывшемся окне выберите новый файл сертификата. Для загрузки разрешены только следующие форматы файлов: CRT, CER, DER и PEM.

   Файл сертификата будет обновлен, информация о новом сертификате отобразится на странице.
8. Нажмите на кнопку **Сохранить** в нижней части страницы.

После синхронизации Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center сертификат удостоверяющего центра также обновится в Kaspersky IoT Secure Gateway 1000. Приложение, для которого выпущен сертификат, будет использовать новый сертификат.

Чтобы обновить сертификат клиента для приложения и ключ к сертификату:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Параметры приложений** → **Сертификаты**.
7. В блоке **Сертификат клиента** выполните следующие действия:

   - В блоке **Сертификат** нажмите на кнопку **Заменить** и в открывшемся окне выберите новый файл сертификата. Для загрузки разрешены только следующие форматы файлов: CRT, CER, DER и PEM.
   - В блоке **Ключ сертификата** нажмите на кнопку **Заменить** и в открывшемся окне выберите новый файл ключа сертификата. Для загрузки разрешены файлы в формате KEY.

Файлы сертификата и ключа к нему будут обновлены, информация о них отобразится на странице.

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

   Вы не сможете сохранить изменения, если вы загрузили только сертификат клиента или только ключ. Требуется загрузить оба файла (сертификата и ключа), чтобы продолжить.

После синхронизации Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center сертификат клиента и ключ будет также обновлены в Kaspersky IoT Secure Gateway 1000. Приложение, для которого выпущен сертификат, будет использовать новый сертификат и ключ.

Удаление сертификатов приложений

Чтобы удалить сертификат удостоверяющего центра для приложения:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Параметры приложений** → **Сертификаты**.
7. В блоке **Сертификат удостоверяющего центра** нажмите на кнопку **Удалить** и подтвердите свои действия.

   Файл сертификата будет удален.
8. Нажмите на кнопку **Сохранить** в нижней части страницы.

После синхронизации Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center сертификат удостоверяющего центра будет также удален в Kaspersky IoT Secure Gateway 1000.

Чтобы удалить сертификат клиента для приложения и ключ к сертификату:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Параметры приложений** → **Сертификаты**.
7. В блоке **Сертификат клиента** выполните следующие действия:

- В блоке **Сертификат** нажмите на кнопку **Удалить** и подтвердите свои действия.
- В блоке **Ключ сертификата** нажмите на кнопку **Удалить** и подтвердите свои действия.

Файлы сертификата и ключа к нему будут удалены.

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

После синхронизации Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center сертификат клиента и ключ к нему будут также удалены в Kaspersky IoT Secure Gateway 1000.

Маршрутизация приложений

Вы можете настроить маршрутизацию данных между приложениями, установленными в Kaspersky IoT Secure Gateway 1000. Маршруты для приложений отображаются в Web Console на вкладке **Параметры программы** → **Параметры приложений** → **Маршрутизация**. Для каждого маршрута в таблице отображается следующая информация:

- **Статус** – статус активности маршрута (**Активный** или **Ошибка**).
- **Приложение-отправитель** – имя приложения, которое оправляет данные.
- **Точка подключения отправителя** – имя точки подключения приложения-отправителя.
- **Приложение-получатель** – имя приложения, которое получает данные.
- **Точка подключения получателя** – имя точки подключения приложения-получателя.

Чтобы найти маршрут или настроить отображение данных в таблице маршрутов приложений:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Параметры приложений** → **Маршрутизация**.

   Откроется таблица, на которой для каждого приложения отображаются созданные ранее маршруты.
7. Если вы хотите найти маршрут, в верхней части таблицы в поле поиска введите значение и нажмите на значок или на кнопку **ENTER**.

   В таблице отобразятся только найденные маршруты. Если предварительно вы настроили фильтрацию данных в таблице маршрутизации приложений, поиск будет выполнен только по отфильтрованным значениям.
8. Если вы хотите сортировать данные в таблице по одному из столбцов, нажмите на его заголовок.

9. Если требуется настроить отображение столбцов в таблице или группировать одинаковые значения в рамках одного столбца, нажмите на значок и в открывшейся справа панели на вкладке **Графы** установите флажки около тех столбцов, которых требуется отображать данные. На вкладке **Группировка** выберите значения, которые требуется группировать в рамках одного столбца.

10. Если требуется настроить отображение маршрутов приложений по определенным условиям, нажмите на значок и в открывшейся справа панели настройте условия отображения маршрутов в таблице. Вы можете добавлять новые условия или удалять существующие.

Так же вы можете создать, изменить или удалить маршрут для приложения.

Создание маршрута для приложения

Чтобы создать новый маршрут для приложения:

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

2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.

3. В открывшемся окне свойств устройства выберите вкладку **Программы**.

4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.

5. Выберите вкладку **Параметры программы**.

6. Выберите раздел **Параметры приложений** → **Маршрутизация**.

   Откроется таблица, на которой для каждого приложения отображаются созданные ранее маршруты.

7. Нажмите на кнопку **Добавить** в верхней части таблицы и в открывшейся справа панели выполните следующие действия:

   a. В раскрывающемся списке **Приложение-отправитель** выберите приложение, от которого будут отправляться данные. В раскрывающемся списке отображаются только запущенные приложения.

   b. В раскрывающемся списке **Точка подключения отправителя** выберите точку подключения. Тип и формат данных, а также протокол передачи данных определяется разработчиком в манифесте приложения.

   c. В раскрывающемся списке **Приложение-получатель** выберите приложение, которое будет получать данные. В раскрывающемся списке отображаются только запущенные приложения.

   d. В раскрывающемся списке **Точка подключения получателя** выберите точку подключения. Тип и формат данных, а также протокол передачи данных определяется разработчиком в манифесте приложения.

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

   Маршрут для приложения будет создан и отобразится в таблице. По умолчанию новый маршрут создается активным.

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

Изменение маршрута для приложения

Чтобы изменить маршрут для приложения:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.
3. В открывшемся окне свойств устройства выберите вкладку **Программы**.
4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.
5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Параметры приложений** → **Маршрутизация**.

   Откроется таблица, на которой для каждого приложения отображаются созданные ранее маршруты.
7. Установите флажок напротив того маршрута, который вы хотите изменить.
8. Нажмите на кнопку **Изменить** в верхней части таблицы и в открывшейся справа панели выполните следующие действия:

   a. В раскрывающемся списке **Приложение-отправитель** выберите приложение, от которого будут отправляться данные. В раскрывающемся списке отображаются только запущенные приложения.

   b. В раскрывающемся списке **Точка подключения отправителя** выберите точку подключения. Тип и формат данных, а также протокол передачи данных определяется разработчиком в манифесте приложения.

   c. В раскрывающемся списке **Приложение-получатель** выберите приложение, которое будет получать данные. В раскрывающемся списке отображаются только запущенные приложения.

   d. В раскрывающемся списке **Точка подключения получателя** выберите точку подключения. Тип и формат данных, а также протокол передачи данных определяется разработчиком в манифесте приложения.

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

   Маршрут для приложения будет изменен и с новыми данными отобразится в таблице.
9. Нажмите на кнопку **Сохранить** в нижней части страницы.

Удаление маршрута для приложения

Чтобы удалить маршрут для приложения:

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

2. Нажмите на имя устройства с Kaspersky IoT Secure Gateway 1000. Если имя устройства отсутствует в списке, добавьте его в группу **Управляемые устройства**.

3. В открывшемся окне свойств устройства выберите вкладку **Программы**.

4. Нажмите **Kaspersky IoT Secure Gateway**.

   Откроется окно, содержащее информацию о Kaspersky IoT Secure Gateway 1000.

5. Выберите вкладку **Параметры программы**.

6. Выберите раздел **Параметры приложений** → **Маршрутизация**.

   Откроется таблица, на которой для каждого приложения отображаются созданные ранее маршруты.

7. Установите флажок напротив маршрута, который вы хотите удалить.

8. Нажмите на кнопку **Удалить** в верхней части таблицы и подтвердите свои действия.

   Маршрут для приложения будет удален.

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

Обращение в Службу технической поддержки

Если у вас возникли вопросы по аппаратному комплексу Kraftway Рубеж-Н или Kaspersky IoT Secure Gateway 1000 и вы не нашли решения вашей проблемы в справке Kaspersky IoT Secure Gateway 1000, рекомендуется обратиться в Службу технической поддержки ООО "НПО АПРОТЕХ", направив письмо по электронной почте support@aprotech.ru.

Для получения дополнительной информации о состоянии сетевых интерфейсов и таблицы маршрутизации вы можете перейти на страницу диагностики неисправностей, которая находится по адресу: <веб-адрес Kaspersky IoT Secure Gateway 1000>/troubleshooting.html. Информация на странице <веб-адрес Kaspersky IoT Secure Gateway 1000>/troubleshooting.html отображается, только если вы предварительно вошли в Kaspersky IoT Secure Gateway 1000.

Просмотр страницы диагностики неисправностей Kaspersky IoT Secure Gateway 1000

Вы можете получить дополнительную информацию о состоянии сетевых интерфейсов и таблицы маршрутизации Kaspersky IoT Secure Gateway 1000 на странице диагностики неисправностей.

Чтобы перейти на страницу диагностики неисправностей,

В меню в левой части веб-интерфейса выберите раздел **Параметры** → **Диагностика** и нажмите на ссылку.

Откроется страница диагностики неисправностей <веб-адрес Kaspersky IoT Secure Gateway 1000>/troubleshooting.html.

На странице диагностики неисправностей отображается следующая информация:

- **Режим работы (включено или выключено) сетевых компонентов**
  - Маскарадинг.
  - IP-форвардинг.
  - DHCP-сервер.
  - DHCP-клиент.
- **Информация о состоянии памяти встраиваемого компьютера**

- Количество запущенных процессов.
- Статус загруженности CPU встраиваемого компьютера.
- Информация об используемой памяти
- Таблица запущенных процессов:
  - ID процесса;
  - приоритет процесса;
  - количество потоков внутри процесса;
  - размер памяти, зарезервированной под процесс;
  - объем памяти, реально используемой процессом;
  - статус процесса;
  - время работы;
  - разбивка CPU по запущенным процессам;
  - название компонентов и сущностей процесса.

- Информация о сетевых интерфейсах Kaspersky IoT Secure Gateway 1000.
  - Название интерфейса.
  - MAC-адрес.
  - IP-адрес.
  - Широковещательный адрес.
  - Маска подсети.
  - Режим работы широковещательного адреса.
  - Максимальный размер полезного блока данных одного пакета.
  - Количество принятых и отправленных сетевых пакетов:
    - Если Kaspersky IoT Secure Gateway 1000 функционирует в качестве типа сетевого устройства сетевой роутер, отображается информация для интерфейсов внешней и внутренней сети, локального устройства и сетевого туннеля.
    - Если Kaspersky IoT Secure Gateway 1000 функционирует в качестве типа сетевого устройства однонаправленный шлюз, отображается информация для интерфейсов внешней сети, локального устройства и сетевого туннеля.

- **Информация о маршрутах Kaspersky IoT Secure Gateway 1000 в таблице маршрутизации**.

  - Статус маршрута (активный или ошибка).
  - Тип маршрута (статический или динамический).
  - IP-адрес пункта назначения.
  - Маска сети пункта назначения.
  - Шлюз.
  - Код ошибки, если маршрут находится в статусе ошибка.

- **Информации о правилах сетевого экрана Kaspersky IoT Secure Gateway 1000**.

  - Системные правила сетевого экрана.
  - Пользовательские правила сетевого экрана.
  - Правила приложения Kaspersky IoT Secure Gateway Network Protector.

- **Информация о правилах адресной трансляции**.

  - Сетевой интерфейс, для которого применяется правило.
  - Внешний порт.
  - Протокол.
  - IP-адрес узла назначения.
  - Порт узла назначения.
  - Комментарий.

  Информация о правилах адресной трансляции отображается только для типа сетевого устройства *сетевой роутер*.

- **Информация о сетевом кластере**.

  - IP-адрес кластера.
  - Маска IP-адреса.
  - Роль устройства в кластере.

Также на странице диагностики неисправностей вы можете выполнить следующие действия:

- Скачать файл-архив с системным журналом Kaspersky IoT Secure Gateway 1000.

  На странице диагностики неисправностей <веб-адрес Kaspersky IoT Secure Gateway 1000>/troubleshooting.html нажмите на кнопку **Download system logs**.

  Загрузка архива с системным журналом Kaspersky IoT Secure Gateway 1000 начнется автоматически.

- Проверить сетевой доступ устройства (ping).

  1. На странице диагностики неисправностей <веб-адрес Kaspersky IoT Secure Gateway 1000>/troubleshooting.html в форме **Check connection via ping command** введите DNS-имя или IP-адрес устройства, доступность которого в сети вы хотите проверить.
  2. Нажмите на кнопку **Submit**.

  Под формой ниже отобразится информация о результатах выполнения проверки (размер и количество отправленных пакетов, время прохождения пакета, статистика потерянных пакетов).

  В Kaspersky IoT Secure Gateway 1000 не предусмотрена возможность задавать ключи для команды проверки сетевой доступности DNS-имени или IP-адреса устройства.

Дополнительная информация

Этот раздел содержит информацию, которая дополняет основной текст документа.

Подготовка к установке Kaspersky IoT Secure Gateway 1000

Прежде чем установить Kaspersky IoT Secure Gateway 1000, требуется подготовить устройство Kraftway Рубеж-Н к установке Kaspersky IoT Secure Gateway 1000.

Подготовку к установке Kaspersky IoT Secure Gateway 1000 выполняют специалисты "Лаборатории Касперского". Описанные в этом разделе инструкции приведены для ознакомительных целей.

Подготовка устройства Kraftway Рубеж-Н

Чтобы подготовить устройство Kraftway Рубеж-Н к установке Kaspersky IoT Secure Gateway 1000:

1. Включите устройство Kraftway Рубеж-Н.
2. Подключите устройство Kraftway Рубеж-Н через COM-порт к локальному компьютеру с помощью кабеля с разъемом RJ45-DB9.

   Вам нужно подключить кабель к консольному разъему (Console) на устройстве Kraftway Рубеж-Н.
3. На локальном компьютере запустите программу-терминал для работы с COM-портом (например, PuTTY или Minicom).
4. Нажмите на кнопку включения/выключения в левой части лицевой панели Kraftway Рубеж-Н.

   На лицевой панели Kraftway Рубеж-Н загорится индикатор питания, и устройство начнет запускаться.
5. Во время загрузки на клавиатуре нажмите на клавишу **DELETE**.

   В терминале откроется главное меню BIOS устройства Kraftway Рубеж-Н.
6. Проверьте параметры даты и времени:

   a. Выберите закладку **Main**.

   b. Выберите пункт **System Date**. При необходимости укажите правильную дату.

   c. Выберите пункт **System Time**. При необходимости укажите правильное время.
7. Выйдите из BIOS с сохранением изменений:

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

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

Kraftway Рубеж-Н перезапустится с настроенными параметрами. При следующем включении устройство также будет запускаться с настроенными параметрами. Перед установкой Kaspersky IoT Secure Gateway 1000 устройство требуется выключить.

Установка Kaspersky IoT Secure Gateway 1000

Для начала работы с Kaspersky IoT Secure Gateway 1000 требуется установить ее на устройство Kraftway Рубеж-Н.

Установку Kaspersky IoT Secure Gateway 1000 выполняют специалисты "Лаборатории Касперского". Описанные в этом разделе инструкции приведены для ознакомительных целей.

Чтобы установить Kaspersky IoT Secure Gateway 1000:

1. Подготовьте компьютер с операционной системой Ubuntu версии 20.04 или выше для создания загрузочного USB-носителя с образом Kaspersky IoT Secure Gateway 1000. Дальнейшие действия требуется выполнять на этом компьютере.

2. Установите утилиты `wget` и `sha512sum`, выполнив следующую команду с root-правами:

```
sudo apt-get install wget coreutils
```

3. Добавьте в систему PGP™-ключ репозитория утилиты `docker`, выполнив следующие команды с root-правами:

```
sudo apt-get update
sudo apt-get install ca-certificates curl gnupg
sudo install -m 0755 -d /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o
/etc/apt/keyrings/docker.gpg
sudo chmod a+r /etc/apt/keyrings/docker.gpg
```

4. Добавьте в систему адрес репозитория утилиты `docker`, выполнив следующие команды:

```
echo \
  "deb [arch="$(dpkg --print-architecture)" signed-by=/etc/apt/keyrings/docker.gpg]
https://download.docker.com/linux/ubuntu \
  "$(. /etc/os-release && echo "$VERSION_CODENAME")" stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

5. Обновите данные о пакетах и установите утилиту `docker`, выполнив следующие команды с root-правами:

```
sudo apt-get update
sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin
docker-compose-plugin
```

6. Подготовьте утилиту `docker` к запуску с правами пользователя, выполнив следующие команды с root-правами:

```
sudo groupadd docker
sudo usermod -aG docker <имя пользователя в системе>
```

```
newgrp docker
```

7. Проверьте, что утилита `docker` запускается без ошибок, запустив тестовый образ:

```
docker run hello-world
```

8. Подключите USB-накопитель с утилитой `flasher`, содержащей скрипт для создания загрузочного образа, к компьютеру и скопируйте ее в отдельную директорию.

9. Перейдите в директорию с утилитой `flasher`.

10. Поместите образ Kaspersky IoT Secure Gateway 1000 в директорию `resources`. Образ должен иметь имя вида kisg-<тип сетевого устройства>-<номер версии системы>_ru_en.tar.gz, где <тип сетевого устройства> может быть `diode` для однонаправленного шлюза или `router` для сетевого роутера, <номер версии системы> имеет вид четырех разделенных точками десятичных чисел, например: `1.2.3.4`.

    Вы можете поместить в директорию один установочный образ, если вы хотите работать только с одним типом сетевого устройства, или оба установочных образа (для однонаправленного шлюза и сетевого роутера), если вы хотите иметь возможность выбрать тип сетевого устройства при установке Kaspersky IoT Secure Gateway 1000.

11. Измените конфигурационный файл `flasher.conf` так, чтобы он содержал только следующие строки:

```
set -eu
KISG_images=()
KISG_device=kraftway
```

12. Убедитесь, что утилите `wget` доступна загрузка образа ОС Debian, выполнив следующую команду:

```
wget https://www.debian.org/CD/
```

> Если с помощью утилиты `wget` не удалось получить образ ОС Debian, то вам требуется поместить в директорию `resources` образ ОС Debian 11.4.0 и контрольные суммы SHA512. При отсутствии интернет-соединения на компьютере с утилитой `flasher`, вам также требуется получить docker-образ ОС Debian на компьютере, имеющем интернет соединение, с помощью команды `docker pull debian:bullseye` и поместить полученный образ в директорию с утилитой `flasher`.

13. Выполните сборку загрузочного образа Kaspersky IoT Secure Gateway 1000, запустив скрипт сборки с помощью следующей команды:

```
./build.sh
```

14. Убедитесь, что сборка загрузочного образа Kaspersky IoT Secure Gateway 1000 выполнена успешно, запустив следующую команду:

```
file KISGFlasher.iso
```

15. Подключите к компьютеру с утилитой `flasher` новый USB-накопитель.

16. Запишите загрузочный образ Kaspersky IoT Secure Gateway 1000 на USB-накопитель, выполнив следующую команду с root-правами:

    ```
    dd bs=4M if=$(pwd)/KISGFlasher.iso of=/dev/sdx status=progress oflag=sync
    ```

    где `/dev/sdx` – имя USB-накопителя, на который нужно записать образ.

17. Дождитесь успешного завершения записи и извлеките USB-накопитель.

18. Подключите USB-накопитель к устройству Kraftway Рубеж-Н.

19. Подключите устройство Kraftway Рубеж-Н через COM-порт к локальному компьютеру с помощью кабеля с разъемом RJ45-DB9 и на локальном компьютере запустите программу-терминал для работы с COM-портом.

    Все дальнейшие действия требуется выполнять в терминале компьютера, к которому подключено устройство Kraftway Рубеж-Н.

20. Нажмите на кнопку включения/выключения в левой части лицевой панели Kraftway Рубеж-Н.

21. Во время старта устройства в консоли на клавиатуре нажмите на клавишу **DELETE**.

    В консоли откроется главное меню BIOS устройства Kraftway Рубеж-Н.

22. Настройте параметры загрузки Kaspersky IoT Secure Gateway 1000 с загрузочного USB-накопителя:

    a. Выберите вкладку **Save & Exit**.

    b. В разделе **Boot Override** с помощью клавиш ↑ и ↓ выберите **UEFI: <имя загрузочного USB>**.

    c. Нажмите на клавишу **ENTER** для старта загрузки с USB-накопителя.

23. Дождитесь загрузки образа с USB-накопителя.

24. В форме для входа `debian login`, появившейся в консоли, введите имя пользователя и пароль от дистрибутива Debian Live CD по умолчанию для входа в систему LiveUSB.

25. Если вы собрали загрузочный образ для двух типов сетевого устройства, выберите в меню образ Kaspersky IoT Secure Gateway 1000 для установки на устройство (однонаправленный шлюз и сетевой роутер) и нажмите клавишу **ENTER**.

    Если вы собрали загрузочный образ только для одного типа сетевого устройства, установка начнется автоматически.

26. Дождитесь окончания процесса установки. После установки устройство Kraftway Рубеж-Н будет выключено.

27. Извлеките USB-накопитель из устройства Kraftway Рубеж-Н.

28. Нажмите на кнопку включения/выключения в левой части лицевой панели Kraftway Рубеж-Н.

29. Во время старта устройства в консоли на клавиатуре нажмите на клавишу **DELETE**.

    В консоли откроется главное меню BIOS устройства Kraftway Рубеж-Н.

30. Настройте порядок загрузки Kaspersky IoT Secure Gateway 1000:

    a. Выберите вкладку **Boot**.

    b. Для параметра **Boot Option #1** выберите значение **UEFI OS**.

31. Выйдите из BIOS с сохранением изменений:

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

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

32. Дождитесь окончания загрузки и визуально проверьте корректность запуска Kaspersky IoT Secure Gateway 1000.

После первого включения Kaspersky IoT Secure Gateway 1000 рекомендуется настроить сеть, создать и загрузить сертификат администратора, настроить дату и время и сменить сертификат веб-сервера на используемый в вашей организации.

Ошибка подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000

Проблема

При подключении к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 с использованием поддерживаемого браузера Google Chrome не загружается страница входа в веб-интерфейс Kaspersky IoT Secure Gateway 1000.

Решение

Для корректного подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 с использованием браузера Google Chrome требуется, чтобы в операционной системе при подключениях по протоколу TCP использовался стандартный системный диапазон портов.

Некоторые программы, установленные на персональном компьютере с операционной системой семейства Windows®, могут изменять системный диапазон портов, которые используются по умолчанию при подключении по протоколу TCP.

Чтобы восстановить корректное подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 с использованием браузера Google Chrome:

1. На компьютере, в браузере которого вы пытаетесь подключиться к веб-интерфейсу Kaspersky IoT Secure Gateway 1000, запустите консоль.

2. В консоли выполните команду, которая выводит диапазон используемых системой портов для протокола TCP:

   ```
   netsh int ipv4 show dynamicport tcp
   ```

   В консоли отобразится диапазон портов, используемых для протокола TCP.

3. Если отобразившийся диапазон портов начинается с порта 1024, то в консоли от имени администратора выполните команду, которая возвращает системный диапазон портов для протокола TCP к значениям по умолчанию:

   ```
   netsh int ipv4 set dynamicport tcp start=49152 num=16384
   ```

4. Повторите попытку подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 с использованием браузера Google Chrome.

   Откроется страница входа в Kaspersky IoT Secure Gateway 1000.

Глоссарий

Kaspersky Security Center 14.2 Web Console

Приложение (веб-приложение), предназначенное для контроля состояния системы безопасности сетей организации, находящихся под защитой приложений "Лаборатории Касперского".

KasperskyOS

Микроядерная операционная система для построения безопасных решений.

Message Queuing Telemetry Transport (MQTT)

Сетевой протокол, работающий поверх стека протоколов TCP/IP, предназначенный для обмена сообщениями между устройствами в Интернете вещей.

MQTT-брокер

Сервер, принимающий, фильтрующий и пересылающий сообщения по протоколу MQTT.

MQTT-топик

Иерархический путь к источнику данных, на базе которого отправляются сообщения по протоколу MQTT.

SSL

Протокол шифрования данных в локальных сетях и в интернете. SSL используется в веб-приложениях для создания защищенных соединений между клиентом и сервером.

TLS

Безопасный протокол передачи данных в локальных сетях и в интернете с использованием шифрования. TLS используется в веб-приложениях для создания защищенных соединений между клиентом и сервером.

Администратор Kaspersky Security Center

Лицо, управляющее работой приложения через систему удаленного централизованного администрирования Kaspersky Security Center.

Безопасный шлюз Интернета вещей

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

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 1000

Часть Kaspersky IoT Secure Gateway 1000, предназначенная для обеспечения функциональности системы (например, аутентификации).

Плагин управления приложением

Специализированный компонент, предоставляющий интерфейс для управления работой приложения через Консоль администрирования. Для каждого приложения существует свой плагин управления. Он входит в состав всех приложений "Лаборатории Касперского", управление которыми может осуществляться при помощи Kaspersky IoT Secure Gateway 1000.

Сервер администрирования

Компонент приложения Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации приложениях "Лаборатории Касперского" и управления ими.

Сертификат администратора

Сертификат, на основании которого осуществляется аутентификация пользователя в веб-интерфейсе Kaspersky IoT Secure Gateway 1000.

Сертификат сервера Kaspersky Security Center

Сертификат, на основании которого осуществляется безопасное взаимодействие Kaspersky IoT Secure Gateway 1000 и Kaspersky Security Center при управлении Kaspersky IoT Secure Gateway 1000 через Kaspersky Security Center 14.2 Web Console.

Событие

Запись, содержащая информацию об обнаружении данных в системе или во внутренней сети, которые требуют внимания сотрудника, ответственного за информационную безопасность в вашей организации, сохраняемая в памяти встраиваемого компьютера Kraftway Рубеж-Н.

Управляемые устройства

Устройства сети организации, включенные в одну из групп администрирования.

Устройство с защитой на уровне UEFI

Устройство со встроенным на уровне BIOS программным обеспечением Антивирус Касперского для UEFI. Встроенная защита обеспечивает безопасность устройства еще с начала запуска системы, в то время как защита устройств, не имеющих встроенного ПО, начинает действовать только после запуска приложения защиты.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, который расположен на локальном веб-сервере. Открыть файл можно из раздела **О продукте**.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Ubuntu является зарегистрированным товарным знаком Canonical Ltd.

Eclipse Mosquitto – товарный знак Eclipse Foundation, Inc.

Google и Google Chrome – товарные знаки Google LLC.

HUAWEI является товарным знаком Huawei Technologies Co., Ltd.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Kraftway – зарегистрированный товарный знак ЗАО "Крафтвэй корпорэйшн ПЛС".

OpenAPI – товарный знак компании The Linux Foundation.

Windows является товарным знаком группы компаний Microsoft.

Mozilla и Firefox являются товарными знаками Mozilla Foundation в США и других странах.

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

OpenSSL является товарным знаком правообладателя OpenSSL Software Foundation.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

PGP – товарный знак или зарегистрированный в США и других странах товарный знак Symantec Corporation или аффилированных компаний.