kaspersky

# Kaspersky IoT Secure Gateway 100

# Содержание

# О Kaspersky IoT Secure Gateway 100

Kaspersky IoT Secure Gateway 100 представляет собой программно-аппаратный комплекс на базе промышленного компьютера Siemens™ SIMATIC™ IoT2040 с установленной операционной системой KasperskyOS и прикладным программным обеспечением. Kaspersky IoT Secure Gateway 100 предназначен для работы в качестве безопасного шлюза промышленного Интернета вещей (Industrial Internet of Things) в сети организации.

В этом документе описана только программная составляющая Kaspersky IoT Secure Gateway 100.

Информацию о технических характеристиках компьютера Siemens SIMATIC IoT2040 вы можете получить на сайте производителя. Информацию по использованию устройства Siemens SIMATIC IoT2040 вы можете получить из руководства пользователя.

Kaspersky IoT Secure Gateway 100 выполняет следующие функции:

- Получает по протоколу OPC UA данные от оборудования, расположенного во внутренней сети предприятия.
- Распределяет и отправляет полученные данные в облачную платформу Siemens MindSphere®.
- Обеспечивает кибербезопасность оборудования предприятия и поддерживает передачу зашифрованных данных.

Установку и предварительную настройку программного обеспечения Kaspersky IoT Secure Gateway 100 выполняют специалисты ООО "НПО "Апротех" или его доверенные в настройке партнеры.

Запуск Kaspersky IoT Secure Gateway 100 выполняется при включении устройства Siemens SIMATIC IoT2040 в сеть. Остановка Kaspersky IoT Secure Gateway 100 выполняется при отключении устройства от сети.

## Комплект поставки

В комплект поставки Kaspersky IoT Secure Gateway 100 входят следующие компоненты:

- Промышленный компьютер Siemens SIMATIC IoT2040 в комплектации, поставляемой производителем.
- Руководство пользователя к промышленному компьютеру Siemens SIMATIC IoT2040.
- SD-карта с предварительно установленным Kaspersky IoT Secure Gateway 100. SD-карта установлена в SD-слот компьютера Siemens SIMATIC IoT2040.
- Кабель UART.
- Файл с информацией о стороннем коде (legal_notices.txt), расположенный на SD-карте.
- Онлайн-справка к программной составляющей Kaspersky IoT Secure Gateway 100.
- Информация о версии программной составляющей Kaspersky IoT Secure Gateway 100 (Release Notes).

## Аппаратные и программные требования

Kaspersky IoT Secure Gateway 100 работает только на промышленном компьютере модели Siemens SIMATIC IoT2040.

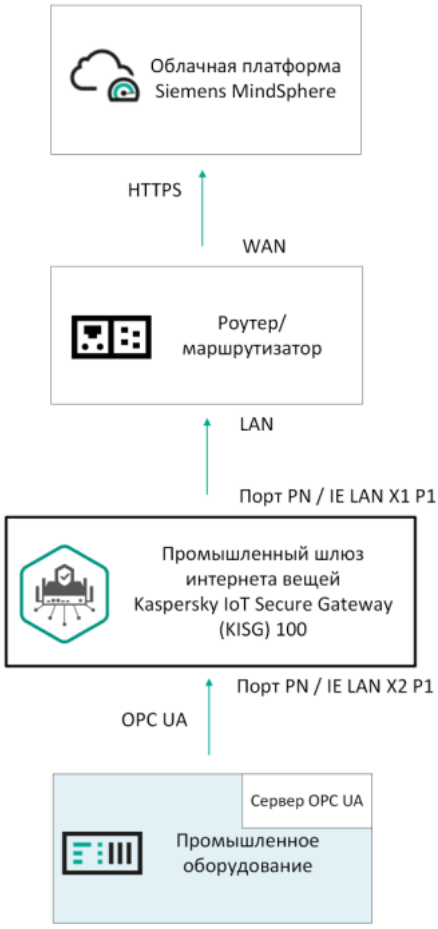
Для настройки передачи данных в облачную платформу Siemens MindSphere требуется получить доступ к Siemens MindSphere. Информацию о способах получения доступа, настройке платформы Siemens MindSphere, а также аппаратных и программных требованиях к компьютеру, который используется для подключения к облачной платформе, вы можете получить в документации Siemens MindSphere.

Для получения данных Kaspersky IoT Secure Gateway 100 от промышленного оборудования предприятия по протоколу OPC UA на оборудовании предприятия требуется настроить параметры отправки данных. Вы можете ознакомиться со спецификацией протокола OPC UA на сайте разработчика. В текущей версии Kaspersky IoT Secure Gateway 100 поддерживается протокол OPC UA версии 1.04.

# Типовая схема развертывания

Типовая схема развертывания Kaspersky IoT Secure Gateway 100 (см. рис. ниже) предполагает следующее:

- Данные от промышленного оборудования предприятия по протоколу OPC UA поступают в Kaspersky IoT Secure Gateway 100.
- Шлюз Интернета вещей Kaspersky IoT Secure Gateway 100 получает данные и передает их в облачную платформу Siemens MindSphere.




Типовая схема развертывания Kaspersky IoT Secure Gateway 100

# Цели и предположения безопасности

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

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

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

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

## Цели безопасности

К целям безопасности Kaspersky IoT Secure Gateway 100 относятся следующие цели:

- Kaspersky IoT Secure Gateway 100 обеспечивает безопасную (однонаправленную) передачу данных от промышленного оборудования, расположенного во внутренней сети предприятия, в облачную платформу Siemens MindSphere без возможности воздействия на внутренние ресурсы предприятия со стороны облачной системы.
- Kaspersky IoT Secure Gateway 100 обеспечивает целостность данных, передаваемых в облачную платформу Siemens MindSphere.

Целями безопасности Kaspersky IoT Secure Gateway 100 не являются:

- Доступность Kaspersky IoT Secure Gateway 100.
- Конфиденциальность данных, передаваемых от Kaspersky IoT Secure Gateway 100 в облачную платформу.

## Предположения безопасности

К предположениям безопасности Kaspersky IoT Secure Gateway 100 относятся следующие предположения:

- Kaspersky IoT Secure Gateway 100 обеспечивает получение данных от оборудования, расположенного во внутренней сети предприятия, только по протоколу OPC UA.
- Физический доступ к Kaspersky IoT Secure Gateway 100 ограничивается организационными мерами предприятия (регламентами доступа в помещение и доступа к оборудованию) с целью предотвращения несанкционированного доступа к Kaspersky IoT Secure Gateway 100.
- У Kaspersky IoT Secure Gateway 100 отсутствуют внутренние средства администрирования. Программная составляющая Kaspersky IoT Secure Gateway 100 и конфигурационные файлы хранятся на извлекаемой SD-карте, доступ к которой имеется только у администратора.
- При работе Kaspersky IoT Secure Gateway 100 параметры, сертификаты и ключи шифрования, хранящиеся на SD-карте, доступны только в режиме чтения.
- 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.

Kaspersky IoT Secure Gateway 100 не гарантирует целостность данных, передаваемых во внутренней сети от оборудования к Kaspersky IoT Secure Gateway 100.

Kaspersky IoT Secure Gateway 100 не обеспечивает безопасность устройств, подключенных к Kaspersky IoT Secure Gateway 100, от атак из внутренней сети.

Не рассматриваются угрозы, связанные с уязвимостью аппаратной платформы.

Не рассматриваются угрозы, связанные с нарушением доступности инфраструктуры:

- каналов связи между участниками сетевого взаимодействия;
- облачной платформы Siemens MindSphere.

# Лицензирование

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

# Предоставление данных

Kaspersky IoT Secure Gateway 100 не собирает, не использует и не обрабатывает пользовательские персональные данные.

# Администрирование

В этом разделе приведены инструкции по настройке параметров Kaspersky IoT Secure Gateway 100 для передачи данных, полученных от промышленных объектов внутренней сети предприятия, в облачную платформу Siemens MindSphere.

Чтобы произвести настройку, необходимо извлечь SD-карту из SD-слота устройства Siemens SIMATIC IoT2040, установить SD-карту в рабочую станцию, выполнить действия, описанные в этом разделе, и установить SD-карту обратно. Обратите внимание, что раздел TGW-HW-BOOT на SD-карте размечен в файловой системе FAT32. Все остальные разделы размечены в файловой системе ext3.

Для корректной передачи данных от оборудования предприятия в облачную платформу Siemens MindSphere через Kaspersky IoT Secure Gateway 100 требуется выполнить следующие действия:

1. Сгенерировать сертификаты для клиентов протокола OPC UA в случае, если используется защищенное соединение и/или авторизация пользователя.

2. На промышленном объекте предприятия (оборудовании) настроить узлы передачи данных по протоколу OPC UA.

   Вы можете ознакомиться со спецификацией протокола OPC UA на сайте разработчика. В текущей версии Kaspersky IoT Secure Gateway 100 поддерживается протокол OPC UA версии 1.04.

3. Получить доступ к облачной платформе Siemens MindSphere и настроить точки получения данных агента MindConnect Lib.

   Подробную информацию о способах получения доступа, настройке точек данных в платформе Siemens MindSphere см. в документации Siemens MindSphere.

4. Настроить параметры Kaspersky IoT Secure Gateway 100 для передачи данных, полученных от промышленных объектов внутренней сети предприятия, в облачную платформу Siemens MindSphere.

# Настройка параметров сети

Для подключения устройства к внешней и внутренней сети требуется установить физическое подключение (по кабелю RJ45) к сети и, при необходимости, настроить параметры внешней и внутренней сети. По умолчанию Kaspersky IoT Secure Gateway 100 поставляется с динамической конфигурацией для внутренней и внешней сети.

> Для настройки динамического получения параметров сети требуется наличие настроенного DHCP-сервера, расположенного в той же сети.

Для подключения Kaspersky IoT Secure Gateway 100 к сети передачи данных вы можете использовать следующие порты Ethernet на устройстве Siemens SIMATIC IoT2040:

- PN/IE LAN X1 P1 – для доступа во *внешнюю* сеть для передачи данных, полученных от промышленных объектов, в облачную платформу Siemens MindSphere.

- PN/IE LAN X2 P1 – для доступа во *внутреннюю* сеть предприятия для получения данных от промышленных объектов по протоколу OPC UA.

Схема расположения портов Ethernet на устройстве Siemens SIMATIC IoT2040 представлена на рисунке ниже.

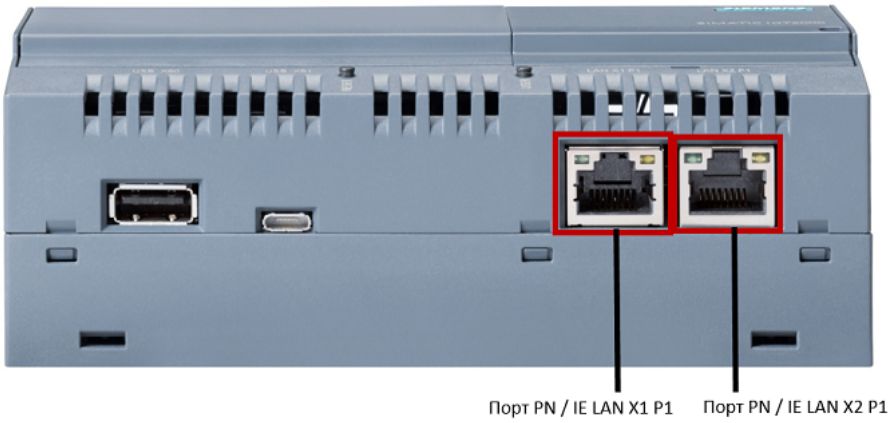



Схема расположения портов Ethernet на устройстве Siemens SIMATIC IoT2040

Настройка параметров внешней сети осуществляется в конфигурационном файле dhcpcd.conf, который расположен в директории /etc в разделе TGW-HW-**ENW** SD-карты.

Настройка параметров внутренней сети осуществляется в конфигурационном файле dhcpcd.conf, который расположен в директории /etc в разделе TGW-HW-**INW** SD-карты.

SD-карта входит в комплект поставки.

Чтобы настроить параметры внешней или внутренней сети, в файле dhcpcd.conf укажите необходимые параметры в соответствии с документацией и сохраните изменения.

Параметры, указанные в файле dhcpcd.conf, будут применены при следующем запуске Kaspersky IoT Secure Gateway 100.

## Настройка параметров получения данных по протоколу OPC UA

Kaspersky IoT Secure Gateway 100 получает данные от оборудования, расположенного во внутренней сети организации, по протоколу OPC UA, который описан спецификацией OPC Unified Architecture (унифицированная архитектура OPC). Вы можете ознакомиться со спецификацией протокола OPC UA на сайте разработчика. Kaspersky IoT Secure Gateway 100 поддерживает протокол OPC UA версии 1.04.

Профиль безопасности `None` в настройках Kaspersky IoT Secure Gateway 100 является наиболее совместимым с разными видами промышленного оборудования для соединения по OPC UA.

При генерации сертификатов для соединения клиента (Kaspersky IoT Secure Gateway 100) и сервера OPC UA удостоверьтесь, что сертификаты удовлетворяют следующим параметрам:

- Параметры ключей и сертификатов соответствуют выбранной политике безопасности.
- Формат DER или PEM для сертификатов и ключей клиента.
- Для сертификата клиента значение поля Subject Alt Name содержит значение URI:urn:aprotech:KISG100:OpcUaClient.

Kaspersky IoT Secure Gateway 100 для хранения сертификатов и ключей для соединения с сервером OPC UA использует следующие директории:

- /app/Core/pki/private/transfer/opc_ua/client/ – директория в разделе TGW-HW-IDS SD-карты для хранения ключей клиента OPC UA.
- /app/Core/pki/certs/transfer/opc_ua/client/ – директория в разделе TGW-HW-IDS SD-карты для хранения сертификатов клиента OPC UA и сервера OPC UA.

Вы можете настроить параметры получения данных от объектов мониторинга по протоколу OPC UA в конфигурационном файле OpcUaClientSettings-0.json.

*Чтобы настроить параметры получения данных по протоколу OPC UA:*

1. Создайте и расположите конфигурационный файл OpcUaClientSettings-0.json в директории /app/Core/config/transfer/opc_ua/client в разделе TGW-HW-IDS SD-карты.

   Все действия, описанные далее, выполняются в файле OpcUaClientSettings-0.json.

2. Для корректной маршрутизации данных от промышленного оборудования в хранилище MindSphere укажите идентификатор и имя клиента OPC UA:

   a. В обязательном параметре `id` укажите идентификатор клиента OPC UA, который будет принимать данные от сервера OPC UA (производственного объекта). Например, `"id": 0`.

   b. В обязательном параметре `name` укажите имя клиента OPC UA, который будет принимать данные от сервера OPC UA (производственного объекта). Например, `"name": "Kaspersky IoT Secure Gateway 100 OPC UA Client"`.

3. При необходимости для удобства чтения конфигурации в необязательном параметре `description` укажите описание клиента OPC UA, который будет принимать данные от сервера OPC UA (производственного объекта). Например, `"description": "Collect data from CNC by Kaspersky IoT Secure Gateway 100"`.

4. Для подключения клиента OPC UA к оборудованию укажите адрес и порт сервера OPC UA в обязательном параметре `url`. Например, `"url": "opc.tcp://192.168.177.7:4840"`.

5. Для установки частоты считывания данных шлюзом в параметре `readingCycle` укажите интервал времени в секундах. Например, `"readingCycle": 1`.

6. Настройте параметры безопасности в обязательном блоке параметров `security`:

   a. В поле `mode` укажите режим управления безопасностью подключения клиентского приложения, который используется на вашем сервере OPC UA. Возможны следующие варианты режимов управления безопасностью:

   - `Sign` – режим, в котором для подключения требуется использовать цифровую подпись данных.
   - `SignAndEncrypt` – режим, в котором для подключения требуется одновременно использовать цифровую подпись данных и шифрование данных.
   - `None` – режим, в котором для подключения не требуется использовать цифровую подпись данных и шифрование данных. Не рекомендуется использовать этот режим, так как он не обеспечивает безопасное подключение клиента OPC UA к серверу OPC UA.
   - `Any` – режим, в котором для подключения будет использован любой из перечисленных режимов (при условии поддержки сервером): `Sign`, `SignAndEncrypt`, `None`.

b. В поле `policy` укажите название профиля безопасности, который используется на вашем сервере OPC UA. Возможны следующие варианты профиля безопасности:

- `Basic128Rsa15`.
- `Basic256`.
- `Basic256Sha256`.
- `None`.
- `Any` – возможно использование любой из перечисленных политик (при условии поддержки сервером): `Basic128Rsa15`, `Basic256`, `Basic256Sha256`, `None`.

c. Для безопасного взаимодействия по OPC UA вам требуется создать приватный ключ и сертификат и поместить их в конфигурацию клиента и сервера. Для организации безопасного соединения по OPC UA в блоке параметров `clientPkiData` укажите следующие параметры:

- В поле `certificate` укажите имя файла сертификата для клиента OPC UA. Например, `"certificate": "client.crt"`.
- В поле `privateKey` укажите имя файла закрытого ключа для сертификата клиента OPC UA. Например, `"privateKey": "client.key"`.

> Блок параметров `clientPkiData` требуется заполнить даже в случае, если полям `mode` и `policy` установлено значение `None`.

d. В поле `trustList` укажите массив, который содержит имена файлов доверенных сертификатов. Например, `"trustList": ["server.crt"]`. Если конфигурация сервера OPC UA предполагает использование собственного доверенного листа, то добавьте сертификат клиента в список доверенных сертификатов сервера. Если проверка сертификатов не требуется, укажите для этого параметра значение `AllowAll`.

> Если не требуется заполнять блоки параметров `mode`, `policy` и `clientPkiData`, то укажите для блока параметров `security` значение `null`. При этом будет использоваться режим безопасности `None`.

7. Для аутентификации клиента OPC UA на сервере OPC UA в обязательном блоке параметров `userCredentials` укажите учетные данные пользователя для подключения:

a. В поле `username` укажите имя учетной записи пользователя для авторизации на сервере OPC UA.

b. В поле `password` укажите пароль учетной записи пользователя для авторизации на сервере OPC UA.

> Если вы хотите разрешить анонимное подключение клиента OPC UA к серверу OPC UA, то в блоке `userCredentials` укажите значение `null`. В таком случае заполнять поля `username` и `password` не нужно.

8. Если вы хотите настроить периодическую отправку сигнала работоспособности Kaspersky IoT Secure Gateway 100 в облачную платформу Siemens MindSphere, выполните следующие действия:

a. Убедитесь, что в облачной платформе Siemens MindSphere заведена точка данных для реализации механизма передачи сигнала работоспособности.

b. В необязательном блоке параметров `heartbeat` укажите следующие параметры:

- В поле `id` укажите идентификатор узла данных. Например, `"id": 0`.
- В поле `name` укажите имя узла данных. Например, `"name": "Heartbeat"`.
- В поле `timeout` укажите период в секундах между генерацией сигналов работоспособности. Например, `"timeout": 60`. Заполнение этого поля не обязательно, по умолчанию установлено значение периода между генерацией сигналов в 30 секунд.

Если вы пропустите настройку периодической отправки сигнала работоспособности или укажете `"heartbeat": null`, то сигналы работоспособности отправляться не будут.

9. В обязательном блоке параметров `nodes` для каждого узла данных укажите следующие параметры:

a. В поле `id` укажите идентификатор узла данных.

b. В поле `name` укажите имя узла данных.

c. В блоке параметров `nodeId` укажите следующие данные:

1. Идентификатор пространства имен сервера OPC UA в поле `ns` (namespace index).
2. Идентификатор узла данных в пространстве имен сервера OPC UA. Возможны следующие варианты:

- `s` (string identifier) – строковое значение идентификатора узла данных. Например, `"nodeId": "ns=1;s=Variable temperature"`.
- `i` (numeric) – числовое значение идентификатора узла данных. Например, `"nodeId": "ns=2;i=2045"`.

10. Сохраните изменения в файле OpcUaClientSettings-0.json.

Параметры, указанные в файле OpcUaClientSettings-0.json, будут применены при следующем запуске Kaspersky IoT Secure Gateway 100.

Kaspersky IoT Secure Gateway 100 будет получать данные от производственных объектов внутренней сети предприятия по протоколу, который описан спецификацией OPC Unified Architecture.

## Частные случаи настройки параметров получения данных по протоколу OPC UA

Kaspersky IoT Secure Gateway 100 не устанавливает соединение в следующих случаях:

- сервер не имеет сертификата и не разрешено небезопасное подключение;
- в параметре `trustList` отсутствует сертификат сервера и не установлено значение `AllowAll`;

- сертификат клиента, сертификат сервера или ключи не удовлетворяют параметрам выбранной политики безопасности.

Клиент и сервер OPC UA устанавливают небезопасное соединение в следующих случаях:

- установлено значение `null` для блоков параметров `security` и `userCredentials` (и сервер поддерживает такое соединение);
- установлено значение `Any` для полей `mode` и `policy` (и сервер предлагает выбор небезопасного соединения).

Любое понижение параметров безопасности снижает защищенность соединения. Например, следующие настройки параметров снижают защищенность соединения по протоколу OPC UA:

- использование значения `null` для блока параметров `security` приводит к использованию соединения без шифрования и подписи;
- использование значения `AllowAll` для поля `trustList` отключает проверку сертификата сервера;
- использование значения `null` для блока параметров `userCredentials` отключает возможность подключения к серверу с использованием логина и пароля;
- использование значений `Basic128Rsa15` или `Basic256` для поля `policy` спецификацией протокола OPC UA v.1.4 считаются устаревшими, так как алгоритм хеширования SHA-1 больше не считается безопасным;
- использование значения `None` для полей `policy` или `mode` приводит к:
  - использованию соединения без шифрования и подписи данных;
  - передаче пароля серверу в открытом виде.
- использование значения `Any` для полей `policy` или `mode` может привести к использованию соединения без шифрования и подписи, если такой вариант будет предложен сервером как приоритетный.

## Настройка параметров передачи данных из Kaspersky IoT Secure Gateway 100 в Siemens MindSphere

Kaspersky IoT Secure Gateway 100 отправляет в облачную платформу Siemens MindSphere данные, полученные от производственных объектов, расположенных во внутренней сети предприятия.

*Siemens MindSphere* – это облачная платформа, разработанная компанией Siemens для получения и анализа промышленных данных Интернета вещей (IoT). Облачная платформа Siemens MindSphere хранит и анализирует все виды производственных данных, полученных от объектов предприятия. Вы можете использовать эту информацию для оптимизации производственных процессов.

Передача данных из Kaspersky IoT Secure Gateway 100 в облачную платформу Siemens MindSphere осуществляется через компонент Siemens MindSphere – агент MindConnect Lib.

Kaspersky IoT Secure Gateway 100 хранит информацию, необходимую для передачи данных в облачную платформу Siemens MindSphere, в следующих директориях:

- /app/Core/pki/certs/transfer/mind_sphere/agent/ – директория в разделе TGW-HW-IDS SD-карты для хранения сертификата удостоверяющего центра Siemens MindSphere. Файл сертификата в этой

директории должен иметь имя `mindsphere.io`.

- /app/Core/config/transfer/mind_sphere/agent/ – директория в разделе TGW-HW-IDS SD-карты для хранения файлов, содержащих параметры соединения с облачной платформой Siemens MindSphere.
- /app/Core/data/transfer/mind_sphere/credentials/ – директория в разделе TGW-HW-EDS SD-карты для хранения файлов с регистрационными данными для получения доступа к облачной платформе Siemens MindSphere.

Вы можете настроить параметры передачи данных из Kaspersky IoT Secure Gateway 100 в облачную платформу Siemens MindSphere в конфигурационном файле MindSphereAgentSettings-0.json.

Перед настройкой параметров требуется получить регистрационные данные Siemens MindSphere средствами MindConnect LIB plugin. Подробную информацию о получении регистрационных данных средствами MindConnect LIB plugin вы можете получить в документации MindSphere. Ниже представлен пример регистрационных данных MindConnect LIB.

Пример регистрационных данных MindConnect LIB:

```
{
        "content": {
            "baseUrl": "https://southgate.eu1.mindsphere.io",
            "iat":
"eyJraWQiOiJrZXktaWQtMSIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJpc3MiOiJTQ0kiLCJzdWIiOiI
C781RRabMRrNpPcOZxucv4n9jIpIZjUx9owGNXT0g-zYb8HYjB13HSvOBZW2_wmPLthxYEFlHU1dqi8ThPtcNE0C
            "clientCredentialProfile": [
                "SHARED_SECRET"
            ],
            "clientId": "3a990ec12fd94a8e81f5f11df8a634d9",
            "tenant": "aprotech"
        },
        "expiration": "2019-08-12T13:00:15.000Z"
    }
```

*Чтобы настроить параметры передачи данных из Kaspersky IoT Secure Gateway 100 в Siemens MindSphere:*

1. Создайте и расположите конфигурационный файл MindSphereAgentSettings-0.json в директории /app/Core/config/transfer/mind_sphere/agent в разделе TGW-HW-IDS SD-карты.

   Все действия, описанные далее, выполняются в файле MindSphereAgentSettings-0.json.

2. Для корректной маршрутизации данных от промышленного оборудования в хранилище MindSphere укажите идентификатор и имя агента MindSphere, через который данные будут отправляться в облако:

   a. В обязательном параметре `id` укажите идентификатор агента MindConnect LIB. Например, `"id": 0`.

   b. В обязательном параметре `name` укажите имя агента MindConnect LIB. Например, `"name": "Kaspersky IoT Secure Gateway 100 MindSphere Agent"`.

3. При необходимости для удобства учета и чтения конфигурации укажите описание для этого клиента в необязательном параметре `description`. Например, `"description": "Transfer data to MindSphere by Kaspersky IoT Secure Gateway 100"`.

4. В обязательном блоке параметров `boardingConfiguration` укажите регистрационные данные, полученные средствами MindConnect LIB plugin. Пример регистрационных данных MindConnect LIB представлен выше.

5. Если для передачи данных от агента в облако MindSphere требуется использовать прокси-сервер, в необязательном блоке параметров `proxySettings` укажите следующие данные:

   a. В поле `type` укажите тип подключения HTTP: `"type": "HTTP"`.

   b. В поле `host` укажите IP-адрес прокси-сервера, через который будет осуществляться подключение. Например, `"host": "192.168.188.1"`.

   c. В поле `port` укажите порт прокси-сервера, через который будет осуществляться подключение. Например, `"port": 3128`.

   Поля `type`, `host` и `port` обязательны для заполнения в случае, если блок параметров `proxySettings` не пустой.

6. Для настройки собственных параметров группировки по временной метке укажите в необязательном блоке параметров `limits` следующие данные:

   a. В поле `maxStorageSize` укажите максимальное количество элементов, которые будут храниться в кольцевом буфере Kaspersky IoT Secure Gateway 100. Например, `"maxStorageSize": 90000`. Значение по умолчанию – 90000, минимальное значение – 1.

   b. В поле `itemGroupTimeout` укажите время ожидания (в секундах) элементов данных с одинаковой временной меткой. Например, `"itemGroupTimeout": 5`. Значение по умолчанию – 5, минимальное значение – 0.

   c. В поле `maxTimeseriesSize` укажите максимальное количество элементов данных в одной временной последовательности. Например, `"maxTimeseriesSize": 64`. Значение по умолчанию – 64, минимальное значение – 1.

   d. В поле `maxHttpPayloadSize` укажите максимальный размер HTTP-запроса (в байтах) к MindConnect Lib. Например, `"maxHttpPayloadSize": 16384`. Значение по умолчанию – 16384, минимальное значение – 400, максимальное значение – 10485760.

   Если вы пропустите настройку параметров группировки по временной метке, то для полей блока параметров `limits` будут установлены значения по умолчанию.

7. В обязательном блоке параметров `dataPoints` для каждой точки данных, созданной в облачной платформе MindSphere, укажите следующие данные:

   a. В поле `id` укажите идентификатор точки данных. Например, `"id": 0`.

   b. В поле `name` укажите имя точки данных. Например, `"name": "Heartbeat"`.

      Имя точки данных облачной платформы MindSphere должно совпадать с именем узла данных сервера OPC UA, которое вы указали в блоке параметров `nodes` в конфигурационном файле OpcUaClientSettings-0.json.

   c. В поле `dataPointId` укажите идентификатор точки, заданный для этой точки в MindSphere. Например, `"dataPointId": "1625019234863"`.

      Вы можете получить идентификатор точки данных, заданный для этой точки в MindSphere, с помощью средств MindConnect LIB plugin. Подробную информацию о получении идентификатора точки данных средствами MindConnect LIB plugin вы можете получить в документации на MindSphere.

8. Сохраните изменения в файле MindSphereAgentSettings-0.json.

Параметры, указанные в файле MindSphereAgentSettings-0.json, будут применены при следующем запуске Kaspersky IoT Secure Gateway 100.

Kaspersky IoT Secure Gateway 100 будет отправлять данные, полученные от объектов мониторинга во внутренней сети вашей организации, в облачную платформу Siemens MindSphere.

## Настройка маршрутизации при передаче данных из Kaspersky IoT Secure Gateway 100 в Siemens MindSphere

Для корректной передачи данных, полученных от оборудования предприятия по протоколу OPC UA, от Kaspersky IoT Secure Gateway 100 в облачную платформу Siemens MindSphere требуется сопоставить точки данных MindConnect и соответствующие им узлы данных сервера OPC UA.

Вы можете настроить соответствие точек данных MindConnect и узлов данных сервера OPC UA в конфигурационном файле GuideSettings-0.json.

*Чтобы настроить соответствие точек данных MindConnect и сервера OPC UA:*

1. Создайте и расположите конфигурационный файл GuideSettings-0.json в директории /app/Core/config/transfer/navigation в разделе TGW-HW-IDS SD-карты.

   Все действия, описанные далее, выполняются в файле GuideSettings-0.json.

2. В обязательном параметре `id` укажите идентификатор маршрута данных. Например, `"id": 0`.

3. В обязательном параметре `receivingHubId` укажите идентификатор клиента OPC UA, который вы указали в конфигурационном файле OpcUaClientSettings-0.json (параметр `id`). Например, `"receivingHubId": 0`.

4. В обязательном параметре `sendingHubId` укажите идентификатор агента MindSphere, который вы указали в конфигурационном файле MindSphereAgentSettings-0.json (параметр `id`). Например, `"sendingHubId": 0`.

5. В обязательном блоке параметров `roadmap` для каждого соединения укажите следующие данные:

   a. В поле `sourcePortId` укажите идентификатор узла данных сервера OPC UA, который вы указали в блоке параметров `nodes` в конфигурационном файле OpcUaClientSettings-0.json. Например, `"sourcePortId": 0`.

   b. В поле `targetPortId` укажите идентификатор точки данных MindConnect Lib, который вы указали в блоке параметров `dataPoints` в конфигурационном файле MindSphereAgentSettings.json-0. Например, `"targetPortId": 0`.

   Блок параметров `roadmap` может быть пустым.

6. Сохраните изменения в файле GuideSettings-0.json.

Параметры, указанные в файле GuideSettings-0.json, будут применены при следующем запуске Kaspersky IoT Secure Gateway 100. Данные, полученные от оборудования по протоколу OPC UA, от Kaspersky IoT Secure Gateway 100 будут поступать в облачную платформу Siemens MindSphere.

# Работа с журналом состояния Kaspersky IoT Secure Gateway 100

Kaspersky IoT Secure Gateway 100 позволяет настроить параметры журнала состояния системы. Настройка параметров журнала состояния осуществляется в конфигурационном файле .log, который расположен в разделе TGW-HW-LOG SD-карты. SD-карта входит в комплект поставки. Журналы состояния системы хранятся в директории /logs.

Чтобы настроить параметры журнала состояния Kaspersky IoT Secure Gateway 100, в конфигурационном файле .log:

1. В параметре `LogFileSizeLimit` укажите максимальный размер в байтах одного файла журнала состояния системы. Например, `LogFileSizeLimit=100000000`.

2. В параметре `DirectorySizeLimit` укажите максимальный размер в байтах для директории, в которой содержатся все файлы журнала состояния системы. Например, `DirectorySizeLimit=1500000000`.

   Kaspersky IoT Secure Gateway 100 по умолчанию не обрабатывает события переполнения дискового пространства, поэтому убедитесь, что параметры размера директории для хранения журнала соответствуют доступному дисковому пространству устройства.

3. Сохраните изменения в файле .log.

> В случае отсутствия файла .log системный журнал будет считаться отключенным и запись журнала в директорию /logs осуществляться не будет.

Параметры, указанные в файле .log, будут применены при следующем запуске Kaspersky IoT Secure Gateway 100.

## Правила записи и ротации файлов журнала

Запись и ротация файлов журнала осуществляется по следующим правилам:

- Если при записи превышен лимит на размер одного файла журнала, то создается новый файл и запись осуществляется в новый файл.
- Если при записи не удалось записать строку целиком из-за превышения лимита на размер одного файла журнала, то создается новый файл, строка записывается в него и дальнейшая запись осуществляется в новый файл.
- Если при записи строки превышены лимиты на размеры одного файла и на все файлы журнала, то удаляется старый файл журнала, создается новый файл и дальнейшая запись осуществляется в новый файл.
- Если при записи строки превышен лимит на все файлы журнала, то удаляется старый файл, а строка записывается в текущий файл.
- Старые файлы журнала удаляются таким образом, чтобы обеспечить достаточный объем памяти для записи строки.
- В начале каждой рабочей сессии (загрузка\перезагрузка шлюза) создаётся новый файл для записи журнала.

## Журналирование информации

Журналируется следующая информация:

- статус инициализации аппаратных компонент;
- статус загрузки ОС;
- статус инициализации системных компонент;
- статус инициализации и работы:
  - сетевых сервисов;
  - хранилища данных;
  - сервиса системного журналирования;
  - компонент приложения:
    - менеджера и клиента OPC UA;
    - менеджера и агента MindSphere;
    - компонента трансфера данных.
- передаваемые элементы данных;
- ошибки инициализации и загрузки.

# Приложения

Этот раздел содержит информацию о расположении основных конфигурационных файлов на SD-карте, а также примеры структуры для каждого их этих файлов.

## Пример конфигурационного файла dhcpcd.conf

Конфигурационный файл dhcpcd.conf расположен в директории /etc в разделах TGW-HW-ENW и TGW-HW-INW SD-карты. SD-карта входит в комплект поставки.

Ниже приведен пример конфигурационного файла dhcpcd.conf, в котором требуется указать параметры для внешней или внутренней сети.

Пример конфигурационного файла dhcpcd.conf:

```
static ip_address=192.168.1.177/23
static routers=192.168.1.1
```

## Пример конфигурационного файла OpcUaClientSettings-0.json

Конфигурационный файл OpcUaClientSettings-0.json расположен в директории /app/Core/config/transfer/opc_ua/client в разделе TGW-HW-IDS SD-карты. SD-карта входит в комплект поставки.

Ниже приведен пример конфигурационного файла OpcUaClientSettings-0.json, в котором требуется указать параметры для получения данных от объекта мониторинга по протоколу OPC UA.

Пример конфигурационного файла OpcUaClientSettings-0.json:

```
{
  "id": 0,
  "name": "Kaspersky IoT Secure Gateway 100 OPC UA Client",
  "description": "Collects data from CNC by Kaspersky IoT Secure Gateway 100",
  "url": "opc.tcp://192.168.177.7:4840",
  "readingCycle": 1,
  "security": {
    "mode": "SignAndEncrypt",
    "policy": "Basic256Sha256",
    "clientPkiData": {
      "certificate": "client.crt",
      "privateKey": "client.key"
    },
    "trustList": ["server.crt"]
  },
  "userCredentials":
  {
    "username": "KISG100",
    "password": "0R20jN#yZd~zaLKe?2J#@~|YC"
  },
  "heartbeat": {
    "id": 0,
    "name": "Heartbeat",
    "timeout": 60
  },
```

```
  "nodes": [
    {
      "id": 1,
      "name": "Temperature",
      "nodeId": "ns=1;s=VariableTemperature"
    },
    {
      "id": 2,
      "name": "Speed",
      "nodeId": "ns=2;i=2045"
    }
  ]
}
```

## Пример конфигурационного файла MindSphereAgentSettings-0.json

Конфигурационный файл MindSphereAgentSettings-0.json расположен в директории /app/Core/config/transfer/mind_shere/agent в разделе TGW-HW-IDS SD-карты. SD-карта входит в комплект поставки.

Ниже приведен пример конфигурационного файла MindSphereAgentSettings-0.json.

Пример конфигурационного файла MindSphereAgentSettings-0.json:

```
{
  "id": 0,
  "name": "Kaspersky IoT Secure Gateway 100 MindSphere Agent",
  "description": "Transfers data to MindSphere by Kaspersky IoT Secure Gateway 100",
  "boardingConfiguration": {
    "content": {
      "baseUrl": "https://southgate.eu1.mindsphere.io",
      "iat":
"eyJraWQiOiJrZXktaWQtMSIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJpc3MiOiJTQ0kiLCJzdWIiOiI
55bKT5DHR3JEYEChbUxRx1xz-TlX9elZPokstLCb58l7pjlNnkg8YhW43Od0vixNOHWGKjVnLhwwJ0yyB9z4S54W
      "clientCredentialProfile": [
        "SHARED_SECRET"
      ],
      "clientId": "4e0ab70efc724445a5f483f344a22f1c",
      "tenant": "aprotech"
    },
    "expiration": "2021-03-24T18:53:51.000Z"
  },
  "configurationId": "1606380355815",
  "proxySettings": {
    "type": "HTTP",
    "host": "192.168.188.1",
    "port": 3128
  },
  "limits": {
    "maxStorageSize": 90000,
    "itemGroupTimeout": 5,
    "maxTimeseriesSize": 64,
    "maxHttpPayloadSize": 16384
  },
  "dataPoints": [
    {
      "id": 0,
```

```
      "name": "Heartbeat",
      "dataPointId": "1625019234863"
    },
    {
      "id": 1,
      "name": "Temperature",
      "dataPointId": "1616007325504"
    },
    {
      "id": 2,
      "name": "Speed",
      "dataPointId": "1616007338184"
    },
  ]
}
```

## Пример конфигурационного файла GuideSettings-0.json

Конфигурационный файл GuideSettings-0.json расположен в директории /app/Core/config/transfer/navigation в разделе TGW-HW-IDS SD-карты. SD-карта входит в комплект поставки.

Ниже приведен пример конфигурационного файла GuideSettings-0.json, в котором требуется указать параметры для настройки передачи данных между узлом источника данных протокола OPC UA и точками данных в MindSphere.

Пример конфигурационного файла GuideSettings-0.json

```
{
  "id": 0,
  "receivingHubId": 0,
  "sendingHubId": 0,
  "roadmap": [
    {
      "sourcePortId": 0,
      "targetPortId": 0
    },
    {
      "sourcePortId": 1,
      "targetPortId": 1
    },
    {
      "sourcePortId": 2,
      "targetPortId": 2
    }
  ]
}
```

# Ограничения

Kaspersky IoT Secure Gateway 100 1.2 имеет следующие ограничения:

- Без перезагрузки Kaspersky IoT Secure Gateway 100 не применяются новые параметры безопасности сервера OPC UA после переподключения.
- Не проводится проверка сертификата клиента OPC UA.
- Клиент OPC UA проверяет сертификат сервера в списке доверенных сертификатов: проверяется совпадение с серверным сертификатом и срок его действия.
- Если настроено доверие любым сертификатам (`"trustList": "AllowAll"`), то клиент не проверяет сертификат сервера.
- При указании в настройках Kaspersky IoT Secure Gateway 100 режима и политики безопасности `None`, требуется также указать сертификат и ключ клиента OPC UA.
- Поддерживаются только следующие типы данных, описанные в спецификации OPC UA:
  - Boolean;
  - SByte;
  - Byte;
  - Int16;
  - UInt16;
  - Int32;
  - UInt32;
  - Int64;
  - UInt64;
  - Float;
  - Double;
  - String;
  - DateTime;
  - XmlElement;
  - NodeId (только numeric и string);
  - ExpandedNodeId (аналогично NodeId);
  - StatusCode;
  - QualifiedName;

    - LocalizedText (частично);
    - Variant.

- Данные, полученные по протоколу OPC UA типа Double и Float, округляются с точностью до шести значащих цифр.
- Для сбора данных по OPC UA сервер должен поддерживать коммуникационную модель издатель-подписчик.
- Доступно подключение только одного клиента OPC UA к одному серверу OPC UA.
- На ранних этапах инициализации агента MindSphere информация от него не выводится в журнал состояния Kaspersky IoT Secure Gateway 100. Это связано с ограничениями, накладываемыми политиками безопасности KasperskyOS.
- В журнал не выводится предупреждение при неверном именовании файла с настройками агента MindSphere.
- До истечения значения lease time (срока аренды IP-адреса) Kaspersky IoT Secure Gateway 100 не применяет новые сетевые настройки, полученные от DHCP-сервера.
- При отключении питания Kaspersky IoT Secure Gateway 100 не сохраняет неотправленные данные, так как не хранит их в постоянной памяти.
- Kaspersky IoT Secure Gateway 100 не обрабатывает события переполнения дискового пространства при ведении журнала состояния.

# Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, который расположен на SD-карте. SD-карта входит в комплект поставки.

# Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Siemens, MindSphere – зарегистрированные товарные знаки Siemens AG.