aprotech Kaspersky IoT company

Release Notes

OPC UA Client & MQTT Publisher [RU]

Содержание

1. Release Notes OPC UA Client & MQTT Publisher

Дата редакции документа: 13.05.2024.

Номер сборки: 1.1.0-alpha.0+date-20240425.git-53a446b2.id-31187.

Документ содержит информацию о новых возможностях и известных ограничениях приложений OPC UA Client & MQTT Publisher версии 1.0.0. Полное описание приложений представлено в руководстве пользователя.

Приложения OPC UA Client и MQTT Publisher представляют собой прикладное программное обеспечение, созданное для работы на платформе кибериммунной системы Kaspersky IoT Secure Gateway 1000 на базе операционной системы KasperskyOS.

Приложение OPC UA Client получает данные от сервера OPC UA, расположенного во внутренней сети предприятия. Приложение MQTT Publisher передает полученные данные по протоколу MQTT в MQTT-брокер с шифрованием TLS. Kaspersky IoT Secure Gateway 1000 обеспечивает безопасный сбор данных по протоколу OPC UA, конвертацию данных из протокола OPC UA в протокол MQTT и однонаправленную передачу данных от сервера OPC UA в MQTT-брокер.

2. Что нового

Приложения OPC UA Client и MQTT Publisher запускаются на платформе шлюза Kaspersky IoT Secure Gateway 1000 версии 3.0. В Kaspersky IoT Secure Gateway 1000 версии 3.0 реализованы следующие функции и возможности, значимые для работы приложений OPC UA Client и MQTT Publisher:

- Kaspersky IoT Secure Gateway 1000 действует в качестве программной платформы, которая поддерживает пограничные вычисления (англ. edge computing). Приложения располагаются на этой программной платформе, запускаются в изолированной среде и управляются с помощью платформы.
- Kaspersky IoT Secure Gateway 1000 работает в качестве однонаправленного шлюза (диода данных). Приложения OPC UA Client и MQTT Publisher запускаются, только когда Kaspersky IoT Secure Gateway 1000 работает в режиме однонаправленного шлюза. В документации к Kaspersky IoT Secure Gateway 1000 представлена информация о других режимах работы системы.
- Доступно управление приложениями с помощью веб-плагина для Kaspersky Security Center 14.2 Web Console. Включая такие действия как:
    - Скачивание и установка приложений; настройка конфигурации; запуск и остановка приложений, а также их удаление.
    - Работа с сертификатами приложений, включая добавление, обновление и удаление сертификатов приложений. Сертификат приложения — это специальный файл цифровой подписи, обеспечивающий безопасную работу приложения в Kaspersky IoT Secure Gateway 1000.
    - Настройка маршрутов передачи данных между приложениями, включая создание, изменение и удаление маршрута для приложения.
- Возможность ручного изменения конфигурации Kaspersky IoT Secure Gateway 1000 с помощью веб-интерфейса. В частности, таким образом возможно настроить перезапуск для приложений.
- Возможность выгружать журналы работы приложений с помощью веб-интерфейса Kaspersky IoT Secure Gateway 1000. Kaspersky IoT Secure Gateway 1000 записывает события, которые генерируются установленными приложениями, в журналы и обеспечивает сохранность этих журналов приложений при перезагрузке, выключении или обновлении системы.
- Возможность управлять уровнем журналирования приложений с помощью веб-интерфейса Kaspersky IoT Secure Gateway 1000. Доступен выбор между 6 уровнями логирования, которые различаются между собой по степени подробности и влиянию на производительность.

3. Известные ограничения_RN OPC UA Client & MQTT Publisher

1.1 Общие ограничения

Следующие ограничения затрагивают оба приложения, OPC UA Client и MQTT Publisher, а также программную платформу:

- Если с помощью веб-интерфейса Kaspersky IoT Secure Gateway 1000 удалить с устройства какое-либо одно из приложений: OPC UA Client или MQTT Publisher, то второе приложение будет автоматически тоже удалено.
- Kaspersky IoT Secure Gateway 1000 поддерживает передачу данных приложениями по не более чем 256 маршрутам одновременно.
- При запуске или остановке приложений вручную запускать или останавливать приложения OPC UA Client и MQTT Publisher необходимо только парой. Для запуска необходимо сначала запустить MQTT Publisher, затем OPC UA Client. Останавливать в обратном порядке: сначала OPC UA Client, затем MQTT Publisher. Рекомендуемая конфигурация запуска приложений — автоматический запуск для обоих приложений.
- Во время подключения к веб-интерфейсу Kaspersky IoT Secure Gateway 1000 при изменении пароля форма ввода пароля будет указывать, что пароль соответствует требованиям, в том числе и в тех случаях, когда пароль в действительности не соответствует требованиям. Убедитесь самостоятельно в соответствии пароля требованиям, не ориентируясь на информацию от формы ввода пароля.
- В случае ошибки передачи данных между приложениями OPC UA Client и MQTT Publisher нет достоверного способа понять, какие данные были доставлены корректно и какие нет. Возможны ситуации, когда некоторые данные будут отмечены в журнале как утерянные, даже если в действительности они были переданы корректно.
- Размер пространства для хранения журналов приложений OPC UA Client и MQTT Publisher имеет ограничение по 50 мб для каждого из приложений.
- Kaspersky IoT Secure Gateway 1000 не оборудован встроенным источником бесперебойного питания, поэтому рекомендуем использование внешнего ИБП во избежание потери данных в случае нереднамеренного отключения питания.
- При изменении конфигурации любого из приложений (OPC UA Client или MQTT Publisher) маршруты передачи данных инвалидируются. В такой ситуации Kaspersky Security Center 14.2 Web Console автоматически переведёт все маршруты в состояние "Активен" и предложит "Сохранить изменения".
- Инвалидация (перевод маршрутов из состояния "Активен") носит уведомительный характер. Kaspersky IoT Secure Gateway 1000 оповещает приложения об инвалидации маршрутов, но не запрещает передачу данных по ним.
- В Kaspersky Security Center 14.2 Web Console не предусмотрена возможность скачивания файлов, загруженных пользователем на страницу с конфигурацией приложений (например, файлов сертификатов).
- Kaspersky Security Center 14.2 Web Console при попытке установить, удалить или обновить приложение на управляемом с его помощью Kaspersky IoT Secure Gateway 1000 в меню «Программы» во вкладке «Параметры программы» в подменю «Менеджер приложений» не отображает список доступных приложений.

1.2 Ограничения OPC UA Client

Приложение OPC UA Client имеет следующие ограничения поддержки протокола OPC UA:

- Отсутствует возможность безопасного подключения по протоколу OPC UA. Подключение выполняется при использовании политики безопасности «None». Аутентификация на сервер OPC UA производится по имени пользователя и паролю. Учётные данные передаются в открытом виде. Также возможно анонимное подключение посредством указания параметра null в блоке параметров userCredentials.
- 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 (только numeric и string);
    - StatusCode;
    - QualifiedName;
    - LocalizedText (частично);
    - Variant.
- Полученные по протоколу OPC UA данные типа Double и Float, округляются с точностью до шести значащих цифр.
- Для передачи данных по OPC UA сервер должен поддерживать наборы служб MonitoredItem и Subscription.
- Доступно подключение только одного клиента OPC UA к одному серверу OPC UA.

1.3 Ограничения MQTT Publisher

Приложение MQTT Publisher имеет следующие ограничения поддержки протокола MQTT:

- Доступно подключение только одного клиента MQTT к одному MQTT-брокеру.

- MQTT Publisher использует значение «1» для флага Clean Session при каждом подключении к MQTT-брокеру.
- Значение параметра qualityOfService является общим для всех публикуемых сообщений от MQTT Publisher в топики (параметр topics), включая служебные топики (heartbeat, lastWill).
- Значение параметра qualityOfService не может быть настроено для каждого публикуемого сообщения от MQTT Publisher в топики (параметр topics).
- MQTT Publisher не использует флаг `retain` при отправке сообщений, а также для LWT-сообщения (сообщения, которое уведомляет о некорректном отключении клиента).
- Установка значения `0` для параметра `keepAlive` MQTT Publisher не приводит к отключению механизма "keep alive" (механизма для отключения клиента на основании его бездействия).
- MQTT Publisher игнорирует отсутствие ответа от MQTT-брокера в течение длительного времени и не закрывает соединение.
- В случае обрыва соединения не более 10 публикуемых сообщений может быть утеряно после восстановления соединения и при наличии свободного места в буфере.

1.4 Ограничения TLS

Приложение MQTT Publisher имеет следующие ограничения поддержки протокола TLS:

- Поддерживаются версии протокола TLS не ниже 1.2.
- Компонент Kaspersky IoT Secure Gateway 1000, отвечающий за поддержание зашифрованного канала связи передачи данных, не поддерживает использование поля subjectAltName и не позволяет установить соединение с MQTT-брокером, если поле subjectAltName использовано в сертификате.
- Компонент Kaspersky IoT Secure Gateway 1000, отвечающий за поддержание зашифрованного канала связи передачи данных требует, чтобы поле Common name в сертификате содержало IP-адрес MQTT-брокера.
- Поддерживаются только наборы шифров TLS:
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,
  - TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256,
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- Поддерживаются только следующие алгоритмы цифровой подписи:
  - `ecdsa_secp521r1_sha512`;
  - `ecdsa_secp384r1_sha384`;
  - `ecdsa_secp256r1_sha256`;
  - `ed25519`;
  - `ed448`;

- `rsa_pss_pss_sha512`;
- `rsa_pss_rsae_sha512`;
- `rsa_pss_pss_sha384`;
- `rsa_pss_rsae_sha384`;
- `rsa_pss_pss_sha256`;
- `rsa_pss_rsae_sha256`;
- `rsa_pkcs1_sha384`;
- `rsa_pkcs1_sha512`;
- `rsa_pkcs1_sha256`.