aprotech Kaspersky IoT company

Release Notes

OPC UA Client & MQTT Publisher [ENG]

Table of Contents

1 Release Notes OPC UA Client & MQTT Publisher

Date of the document revision: 05.13.2024.

Build Number: 1.1.0-alpha.0+date-20240425.git-53a446b2.id-31187.

This document contains information about new features and known limitations of the OPC UA Client and MQTT Publisher applications version 1.0.0. A full description of the applications is provided in the user manual.

The OPC UA Client and MQTT Publisher applications (hereinafter also *applications*) are software designed to run on the Kaspersky IoT Secure Gateway 1000 cyberimmune system platform, which is based on the KasperskyOS operating system.

OPC UA Client uses the OPC UA protocol to receive data from the OPC UA server residing in the internal enterprise network. MQTT Publisher forwards data received over the MQTT protocol to the MQTT broker with TLS encryption. Kaspersky IoT Secure Gateway 1000 provides secure data collection over OPC UA, data conversion from the OPC UA protocol to the MQTT protocol, and unidirectional data transfer from the OPC UA server to the MQTT broker.

2 What's new

Kaspersky IoT Secure Gateway 1000 version 3.0 includes the following functions and capabilities, which are significant for the OPC UA Client and MQTT Publisher operation:

- Kaspersky IoT Secure Gateway 1000 acts as a software platform that supports edge computing. Applications are hosted on this software platform, run in an isolated environment, and managed using the platform.
- Kaspersky IoT Secure Gateway 1000 acts as a unidirectional gateway (data diode). OPC UA Client and MQTT Publisher start only when Kaspersky IoT Secure Gateway 1000 operates in the unidirectional gateway mode. Information on other operating modes is provided in the Kaspersky IoT Secure Gateway 1000 documentation.
- Applications can be managed using the web plug-in for Kaspersky Security Center 14.2 Web Console. Including such actions as:
- Downloading and installation of applications, configuration, start, stop, and uninstallation of the applications.
- Managing application certificates, including adding, updating, and deleting application certificates. An application certificate is a special digital signature file that ensures secure application operation in Kaspersky IoT Secure Gateway 1000.
- Configuring data transfer routes between the applications, including creating, modifying, and deleting an application route.
- Ability to manually reconfigure Kaspersky IoT Secure Gateway 1000 using the web interface. This approach allows you to configure a restart of the applications.
- Capability to upload application operation logs using the Kaspersky IoT Secure Gateway 1000 web interface. Kaspersky IoT Secure Gateway 1000 logs events generated by installed applications and ensures the safety of these application logs when the system is restarted, turned off, or updated.
- Capability to manage the application logging level using the Kaspersky IoT Secure Gateway 1000 web interface. You can choose one of the 6 logging levels, which differ in the level of detail and performance impact.

3 Known limitations

3.1 General limitations

The following limitations apply to both applications:

- If one of the applications (OPC UA Client or MQTT Publisher) is deleted from the device using the Kaspersky IoT Secure Gateway 1000 web interface, the second application is deleted automatically.
- Kaspersky IoT Secure Gateway 1000 supports data transfer by applications on no more than 256 routes simultaneously.
- When starting or stopping applications manually, it is necessary to start or stop the OPC UA Client and MQTT Publisher applications only as a pair. To run, you must first run MQTT Publisher, then the OPC UA Client. Stop in reverse order: first OPC UA Client, then MQTT Publisher. The recommended application startup configuration is automatic startup for both applications.
- When connecting to the Kaspersky IoT Secure Gateway 1000 web interface, when changing the password, the password entry form will indicate that the password meets the requirements, including in cases where the password does not actually meet the requirements. Make sure that the password meets the requirements yourself, without relying on the information from the password entry form.
- In case of a data transfer error between the OPC UA Client and MQTT Publisher applications, there is no reliable way to understand which data was delivered correctly and which was not. There may be situations when some data will be marked as lost in the log, even if in fact it was transmitted correctly.
- The size of the storage space for the logs of the OPC UA Client and MQTT Publisher applications has a limit of 50 MB for each of the applications.
- Kaspersky IoT Secure Gateway 1000 is not equipped with an integrated uninterruptible power supply, so we recommend using an external UPS to avoid data loss in the event of an unintentional power outage.
- Changing the configuration of any of the applications (OPC UA Client or MQTTPublisher) disables data transmission routes. In such a situation, Kaspersky Security Center 14.2 Web Console will automatically switch all routes to the "Active" state and offer to "Save changes".
- The disability of data transfer routes between applications (the transfer of routes from the "Active" state) is of a notification nature. Kaspersky Iot Secure Gateway 1000 notifies applications about route invalidation, but does not prohibit data transmission over them.
- Kaspersky Security Center 14.2 Web Console does not provide the ability to download files uploaded by the user to the application configuration page (for example, certificate files).
- Kaspersky Security Center 14.2 Web Console when trying to install, uninstall or update an application on a Kaspersky IoT Secure Gateway 1000 managed with it, the list of available applications does not display in the "Programs" menu in the "Program Settings" tab in the "Application Manager" submenu.

3.2 OPC UA Client limitations

OPC UA Client has the following limitations of the OPC UA protocol support:

- There is no secure connection over the OPC UA protocol. The connection is established when the None security policy is used. Authentication on the OPC UA

server is performed using a user name and password. The credentials are transmitted in clear format. It is also possible to connect anonymously by specifying null in the userCredentials section.

- Only the following data types described in the OPC UA specification are supported:
- Boolean
- SByte
- Byte
- Int16
- UInt16
- Int32
- UInt32
- Int64
- UInt64
- Float
- Double
- String
- DateTime
- XmlElement
- NodeId (only numeric and string)
- ExpandedNodeId (only numeric and string)
- StatusCode
- QualifiedName
- LocalizedText (partially)
- Variant
- Double- and Float-type data received over the OPC UA protocol is rounded to the nearest six significant digits.
- To transmit data over OPC UA, the server must support the MonitoredItem and Subscription service sets.
- Only one OPC UA client connection to one OPC UA server is available.

3.3 MQTT Publisher limitations

MQTT Publisher has the following limitations of the MQTT protocol support:

- Only one MQTT client connection to one MQTT broker is available.
- MQTT Publisher uses the "1" value for the Clean Session flag each time it connects to the MQTT broker.
- The value of the qualityOfService setting is common for all published messages from MQTT Publisher to topics (the topics setting), including service topics (heartbeat, lastWill).
- The qualityOfService setting cannot be configured for every published message from MQTT Publisher to topics (the topics setting).

- The MQTT client does not use the retain flag when sending messages nor for the LWT message (message informing that the client was improperly disconnected).
- Setting the keepAlive parameter of the MQTT client to 0 will not disable the "keep alive" mechanism (this mechanism disconnects a client that is inactive for too long).
- The MQTT client ignores the lack of response from the MQTT broker for a prolonged period of time and does not close the connection.
- If the connection is disrupted, no more than 10 published messages may be lost after the connection is restored and if the buffer has sufficient free space.
- MQTT Publisher may stop sending data to the MQTT broker after it is stopped and restarted. To restore the proper operation of the application, restart Kaspersky IoT Secure Gateway 1000.
- If you use the configuration where manual startup is selected for MQTT Publisher and automatic startup is selected for the OPC UA Client, then when Kaspersky IoT Secure Gateway 1000 is turned on, both applications are stopped. The reverse configuration (manual OPC UA Client startup and automatic MQTT Publisher startup) works properly.

3.4 TLS limitations

MQTT Publisher has the following limitations of the TLS protocol support:

- Only TLS protocol versions 1.2 or later are supported.
- The Kaspersky IoT Secure Gateway 1000 component, responsible for maintaining an encrypted data communication channel, does not support the use of the subjectAltName field and does not allow establishing a connection with the MQTT broker if the subjectAltName field is used in the certificate.
- The Kaspersky IoT Secure Gateway 1000 component, responsible for maintaining an encrypted data communication channel, requires that the Common name field in the certificate contain the IP address of the MQTT broker.
- Only TLS cipher suites are supported:
- 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
- Only the following digital signature algorithms are supported:
- 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