

MQTT Client Communication Driver

This document has the specific information related to this driver configuration. For a generic explanation on Device Module, Channels, Nodes and Points configuration, please refer to reference guide.

Contents

Section 1 – Summary Information	2
Section 2 – Channel Configuration	2
Protocol Options	2
Section 3 – Node Configuration	2
Station Configuration	2
Station Examples	3
Section 4 – Point Configuration	4
Address	4
Section 5 – Troubleshoot	4
Revision History	5

Section 1 – Summary Information

Communication Driver Name: MQTT

Implementation DLL: T.ProtocolDriver.MQTT.dll

Interface: TCPIP

Protocol: MQTT (Message Queuing Telemetry Transport) is a machine-to-machine (M2M)/"Internet of Things" connectivity protocol.

PC Hardware requirements: Ethernet board

Implemented Methods: Connect, Disconnect, Subscribe, UnSubscribe and Publish.

Section 2 – Channel Configuration

Protocol Options

Not used in this driver.

Section 3 – Node Configuration

Station Configuration

Station syntax: <URL>; <Port>; [Username]; [Password]; [X509Certificate]

Where:

< **URL** > = MQTT Broker (Server) name. It must be the same name is configured in the *bind_address* parameter in the Broker.

< **Port** > = MQTT Broker port. It must be the same *port* is configured in the Broker to be listening. Default value is 1883.

[**Username**], *optional* = Username defined on MQTT Broker. This will be requested if the Broker has the *allow_anonymous* parameter as false. Whether this parameter is set as true on Broker, keep this field empty. Default value is empty.

[**Password**], *optional* = Password defined on MTQQ Broker. This will be requested if the Broker has the *allow_anonymous* parameter as false. Whether this parameter is set as true on Broker, keep this field empty. Default value is empty.

[**X509Certificate**], *optional* = Path of X509 Certificate using TLS v1.0. This must be the complete path of X509 certificate in the client computer. The certificate must be installed in the computer.

Note: One of the easiest ways to install the certificate on client computer is to use the wizard to import the certificates is through the "Internet Options" to import the certificate in the "Trusted Root Certification Authorities". You need to import the certificate in DER format.

Station Examples

1. Broker configuration with no Username and Password and no SSL/TLS

Station Configuration

URL: test.mosquitto.org

Port: 1883

Username: <empty>

Password: <empty>

X509Certificate: <empty>

2. Broker configuration with Username and Password and no SSL/TLS

Station Configuration

URL: MSI

Port: 1883

Username: Guest

Password: 1234

X509Certificate: <empty>

3. Broker configuration with SSL/TLS and no Username and Password

Station Configuration

URL: MSI

Port: 8883

Username: <empty>

Password: <empty>

X509Certificate: C:\Certificates\mqtt_ca.der

4. Broker configuration with SSL/TLS and Username and Password

Station Configuration

URL: MSI

Port: 8883

Username: Guest

Password: 1234

X509Certificate: C:\mqtt_ca.der

Section 4 – Point Configuration

Address

The syntax for the MQTT communication points are:

- **<Topic>:<QoS>**

<Topic> is a string, which is used by the broker to filter messages for each connected client. A topic consists of one or more topic levels. Each topic level is separated by a forward slash (topic level separator). Wildcards are not supported.

<QoS> Quality of Service (*QoS*) is an agreement between sender and receiver of a message regarding the guarantees of delivering a message. There are 3 QoS levels:

- ***AtMostOnce***
- ***AtLeastOnce***
- ***ExactlyOnce***

E.g.: USA/Houston/Station1/Level:AtMostOnce

Section 5 – Troubleshoot

The status of the driver execution can be observed through the diagnostic tools, which are:

- Trace window
- Property Watch
- Module Information

Status value of 0 (zero) means communication success. Negative values indicate internal driver error.

Revision History

Revision	Version	Description	Date
A	1.0.0.0	Initial Revision	<i>February 2016</i>
B	2.0.0.0	Implemented the login and SSL/TLS	<i>April 2016</i>