RUT300 MQTT

The information in this page is updated in accordance with firmware version **RUT30X_R_00.07.06.8**.

□

Contents

- 1 Summary
- 2 MQTT Broker
- 3 Broker Settings
  - 3.1 Security
  - 3.2 Bridge
  - 3.3 Miscellaneous
- 4 MQTT Publisher

Summary

MQTT (MQ Telemetry Transport or Message Queue Telemetry Transport) is an ISO standard (ISO/IEC PRF 20922) publish-subscribe-based "lightweight" messaging protocol for use on top of the TCP/IP protocol. It is designed to send short messages from one client (*publisher*) to another (*subscriber*) through *brokers*, which are responsible for message delivery to the end point.

RUT300 devices support this functionality via an open source Mosquitto broker. The messages are sent this way: a client (subscriber) subscribes to a topic(s); a publisher posts a message to that specific topic(s). The broker then checks who is subscribed to that particular topic(s) and transmits data from the publisher to the subscriber.

This chapter is an overview of the MQTT page for RUT300 devices.

Note: MQTT is additional software that can be installed from the **System → Package Manager** page.

MQTT Broker

The **MQTT Broker** is an entity that listens for connections on the specified port and relays received messages to MQTT client. To begin using this devices as an MQTT Broker, enable it in this page. In order to make the device accept MQTT connections from WAN (remote networks), you also need to turn the 'Enable Remote Access' slider on.

Field	Value	Description
Enable	off | on; default: **off**	Turn MQTT Broker on or off.
Custom configuration	off | on; default: **off**	Enables reading of custom configuration.
Local Port	integer [0..65535]; default: **1883**	The TCP port(s) on which the MQTT broker will listen for connections. Click the plus sign to add multiple ports.
Enable Remote Access	off | on; default: **off**	Turns remote access to this MQTT broker on or off.

Broker Settings

Security

The **Security** section is used to configure TLS/SSL .



Field name	value	description
Use TLS/SSL	off | on; default: **off**	Turns the use of TLS/SSL for this MQTT connection on or off.
TLS type	Certificate based | Pre-shared key based; default: **Certificate based**	Select type of TLS.
Require certificate	off | on; default: **on**	Demand client certificate and key from the client.
Certificate files from device	off | on; default: **off**	When turned on, provides the possibility to use certificate files generated on this device instead of uploading certificate files. You can generate TLS certificates on your device in the System → Administration → Certificates page.
CA File	.ca file; default: **none**	Uploads a Certificate Authority (CA) file. A Certificate Authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.
CERT File	.crt file; default: **none**	Uploads a server (broker) certificate file. A certificate file is a type of digital certificate that is used by client systems to make authenticated requests to a remote server.
Key File	.key file; default: **none**	Uploads a server (broker) key file.
TLS version	tlsv1 | tlsv1.1 | tlsv1.2 | Support all; default: **Support all**	Specifies which TLS version(s) is will be supported by this broker.
Pre-shared key based: Pre-Shared-Key	string; default: **none**	The pre-shared-key in hex format with no leading "0x".
Pre-shared key based: Identity	string; default: **none**	The identity of this client. May be used as the username depending on the server settings.

Bridge

An **MQTT Bridge** is used for the communication between MQTT brokers. The window of Bridge parameters is presented below.

Note: this table has a coloring scheme to indicate which fields can be seen with different configuration.



Field	Value	Description
Enable	off | on; default: **off**	Turns MQTT Bridge on and off.
Connection Name	string; default: **none**	Name of the Bridge connection. This is used for easier management purposes.
Protocol version	3.1 | 3.1.1; default: **3.1**	Selects protocol version
Remote Address	ip; default: **none**	Remote Broker's address.
Remote Port	integer [0..65535]; default: **1883**	Specifies which port the remote broker uses to listen for connections.
Use Remote TLS/SSL	off | **on**; default: **off**	Enables the use of TSL/SSL certificates of the remote broker. If this is checked, you will be prompted to upload TLS/SSL certificates. More information can be found in the Security section of this chapter.
On: Certificate files from device	off | on; default: **off**	When turned on, provides the possibility to use certificate files generated on this device instead of uploading certificate files. You can generate TLS certificates on your device in the System → Administration → Certificates page.
On: Bridge CA File	.ca file; default: **none**	Uploads a Certificate Authority (CA) file. A Certificate Authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.
On: Bridge certificate File	.crt file; default: **none**	Uploads a server (broker) certificate file. A certificate file is a type of digital certificate that is used by client systems to make authenticated requests to a remote server.
On: Bridge Key File	.key file; default: **none**	Uploads a server (broker) key file.
On: Bridge TLS version	tlsv1 | tlsv1.1 | tlsv1.2; default: **tlsv1**	TLS version used by the other broker.
On: Bridge ALPN	string; default: **none**	Configure the application layer protocol negotiation option for the TLS session. Useful for brokers that support both websockets and MQTT on the same port.
Use Remote Bridge Login	off | **on**; default: **off**	Indicates whether the remote side of the connection requires login information. If this is turned on, you will be required to enter a remote client ID, username and password.
On: Remote ID	string; default: **none**	Identifier of the remote broker

On: Remote Username	string; default: **none**	Username for authentication to the remote broker.
On: Require password	on | off; default: **off**	Password for authentication to the remote broker.
On: Remote Password	string; default: **none**	Password for authentication to the remote broker.
Try Private	off | on; default: **off**	Check if the remote Broker is another instance of a daemon.
Clean Session	off | on; default: **off**	When turned on, discards session state after connecting or disconnecting.
Enable notification	off | on; default: **off**	Publish notification messages to the local and remote brokers giving information about the state of the bridge connection.
Enable local notifications	off | on; default: **off**	Only publish notification messages to the local broker giving information about the state of the bridge connection.
Keepalive interval	(5-65535); default: **60**	Set the keepalive interval for this bridge connection, in seconds.

You can also create and manage MQTT topics in the **Topics** list below the Bridge section. To add a new topic, click the 'Add' button.



You can then configure the newly added topic from the same page.



Field	value	description
Topic Name	string; default: **none**	The name of the topics that the broker will subscribe to.
Direction	OUT | IN | BOTH; default: **OUT**	The direction that the messages will be shared.
QoS Level	At most once (0) | At least once (1) | Exactly once (2); default: **At most once (0)**	Sets the publish/subscribe QoS level used for this topic.

Miscellaneous

The **Miscellaneous** section is used to configure MQTT broker parameters that are related to neither Security nor Bridge.



field name	value	description
ACL File	ACL file; default: **none**	Uploads an ACL file. The contents of this file are used to control client access to topics of the broker.

Password File	password file; default: **none**	Uploads a password. A password file stores usernames and corresponding passwords, used for authentication.
Persistence	off | on; default: **off**	When turned on, connection, subscription and message data will be written to the disk. Otherwise, the data is stored in the device memory only.
Allow Anonymous	off | on; default: **off**	Turns anonymous access to this broker on or off.
Max queued messages	[0..65535]; default: **1000**	The maximum number of QoS 1 and 2 messages to hold in a queue per client above those that are currently in-flight. Set to 0 for no maximum (not recommended).
Maximum packet size	[1..268435456]; default: **1048576**	Maximum size of packet before it will be dropped.

MQTT Publisher

An **MQTT Publisher** is a client instance that can send messages to the Broker, who can forward these messages to other clients (subscribers).

Note: this table has coloring scheme to indicate which fields can be seen with different configuration.



Field	Value	Description
Enable	off | on; default: **off**	Toggles the MQTT Publisher ON or OFF.
Hostname	host | ip; default: **none**	Broker's IP address or hostname.
Port	integer [0..65535]; default: **1883**	Broker's port number.
Client ID	string; default: **empty**	Client ID to send with the data. If empty, a random client ID will be generated.
Username	string; default: **none**	Username used for authentication to the Broker.
Require password	check | uncheck; default: **Uncheck**	Requires password for authentication.
Password	string; default: **none**	Password used for authentication to the Broker.
TLS	off | **on**; default: **off**	Turns the use of Transport Layer Security (TLS) on or off.
On: Allow insecure connection	off | on; default: **off**	Allows connections without verifying server authenticity.
TLS type	Certificate based | Pre-shared key based; default: **Certificate based**	Select type of TLS.
On: Certificate files from device	off | on; default: **off**	When turned on, provides the possibility to use certificate files generated on this device instead of uploading certificate files. You can generate TLS certificates on your device in the System → Administration → Certificates page.

On: CA file	.ca file; default: **none**	Certificate authority file used in Transport Layer Security.
On: Certificate file	.crt file; default: **none**	Certificate file used in Transport Layer Security.
On: Key file	.key file; default: **none**	Key file used in Transport Layer Security.
Pre-shared key based: Pre-Shared-Key	string; default: **none**	The pre-shared-key in hex format with no leading "0x".
Pre-shared key based: Identity	string; default: **none**	The identity of this client. May be used as the username depending on the server settings.
Publish topic prefix	string; default: **empty**	Prefix of the topic to be used during publish. More information.
Subscribe topic prefix	string; default: **empty**	Prefix of the topic to be used during subscription. More information.