

# RUT200 MQTT

[Main Page](#) > [RUT Routers](#) > [RUT200](#) > [RUT200 Manual](#) > [RUT200 WebUI](#) > [RUT200 Services section](#) > **RUT200 MQTT**

The information in this page is updated in accordance with firmware version [RUT2M\\_R\\_00.07.04.5](#).

□

## 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.

RUT200 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 RUT200 devices.

**Note:** MQTT is additional software that can be installed from the **Services** → [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.

MQTT broker  off on

Local port  +

Enable remote access  off on

Field	Value	Description
Enable	off   on; default: <b>off</b>	Turn MQTT Broker on or off.
Local Port	integer [0..65535]; default: <b>1883</b>	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: <b>off</b>	Turns remote access to this MQTT broker on or off.

## Broker Settings

### Security

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

^ BROKER SETTINGS

SECURITY

BRIDGE

MISCELLANEOUS

Use TLS/SSL  off on

TLS Type

Certificate files from device  off on

CA File  No file selected

CERT File  No file selected

Key File  No file selected

TLS version

field name	value	description
Use TLS/SSL	off   on; default: <b>off</b>	Turns the use of TLS/SSL for this MQTT connection on or off.
TLS type	Certificate based   <b>Pre-shared key based</b> ; default: <b>Certificate based</b>	Select type of TLS.

Certificate files from device	off   on; default: <b>off</b>	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 → <a href="#">Certificates</a> page.
CA File	.ca file; default: <b>none</b>	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: <b>none</b>	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: <b>none</b>	Uploads a server (broker) key file.
TLS version	tlsv1   tlsv1.1   tlsv1.2   Support all; default: <b>Support all</b>	Specifies which TLS version(s) is will be supported by this broker.
<b>Pre-shared key based:</b> Pre-Shared-Key	string; default: <b>none</b>	The pre-shared-key in hex format with no leading "0x".
<b>Pre-shared key based:</b> Identity	string; default: <b>none</b>	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.

### ^ BROKER SETTINGS

SECURITY

**BRIDGE**

MISCELLANEOUS

Enable

Connection Name

Protocol Version

Remote Address

Remote Port

Use Remote TLS/SSL

Use Remote Bridge Login

Try Private

Clean Session

**Field**

**Value**

**Description**

Enable	off   on; default: <b>off</b>	Turns MQTT Bridge on and off.
Connection Name	string; default: <b>none</b>	Name of the Bridge connection. This is used for easier management purposes.
Protocol version	3.1   3.1.1; default: <b>3.1</b>	Selects protocol version
Remote Address	ip; default: <b>none</b>	Remote Broker's address.
Remote Port	integer [0..65535]; default: <b>1883</b>	Specifies which port the remote broker uses to listen for connections.
Use Remote TLS/SSL	off   <b>on</b> ; default: <b>off</b>	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 <a href="#">Security</a> section of this chapter.
<b>On:</b> Certificate files from device	off   on; default: <b>off</b>	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 → <a href="#">Certificates</a> page.
<b>On:</b> Bridge CA File	.ca file; default: <b>none</b>	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.
<b>On:</b> Bridge CERT File	.crt file; default: <b>none</b>	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.
<b>On:</b> Bridge Key File	.key file; default: <b>none</b>	Uploads a server (broker) key file.
<b>On:</b> Bridge TLS version	tls1   tls1.1   tls1.2; default: <b>tls1</b>	TLS version used by the other broker.
Use Remote Bridge Login	off   <b>on</b> ; default: <b>off</b>	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.
<b>On:</b> Remote ID	string; default: <b>none</b>	Identifier of the remote broker
<b>On:</b> Remote Username	string; default: <b>none</b>	Username for authentication to the remote broker.
<b>On:</b> Remote Password	string; default: <b>none</b>	Password for authentication to the remote broker.
Try Private	off   on; default: <b>off</b>	Check if the remote Broker is another instance of a daemon.
Clean Session	off   on; default: <b>off</b>	When turned on, discards session state after connecting or disconnecting.

---

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.

## TOPICS

TOPIC NAME

DIRECTION

QOS LEVEL

There are no topics created yet.

ADD

SAVE & APPLY

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

## TOPICS

TOPIC NAME

DIRECTION

QOS LEVEL

Topic

OUT

At most once (0)

X

ADD

SAVE & APPLY

Field	value	description
Topic Name	string; default: <b>none</b>	The name of the topics that the broker will subscribe to.
Direction	OUT   IN   BOTH; default: <b>OUT</b>	The direction that the messages will be shared.
QoS Level	At most once (0)   At least once (1)   Exactly once (2); default: <b>At most once (0)</b>	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.

## BROKER SETTINGS

SECURITY

BRIDGE

MISCELLANEOUS

ACL File  No file selected

Password File  No file selected

Persistence  off  on

Allow Anonymous  off  on

SAVE & APPLY

field name	value	description
ACL File	ACL file; default: <b>none</b>	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: <b>none</b>	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.

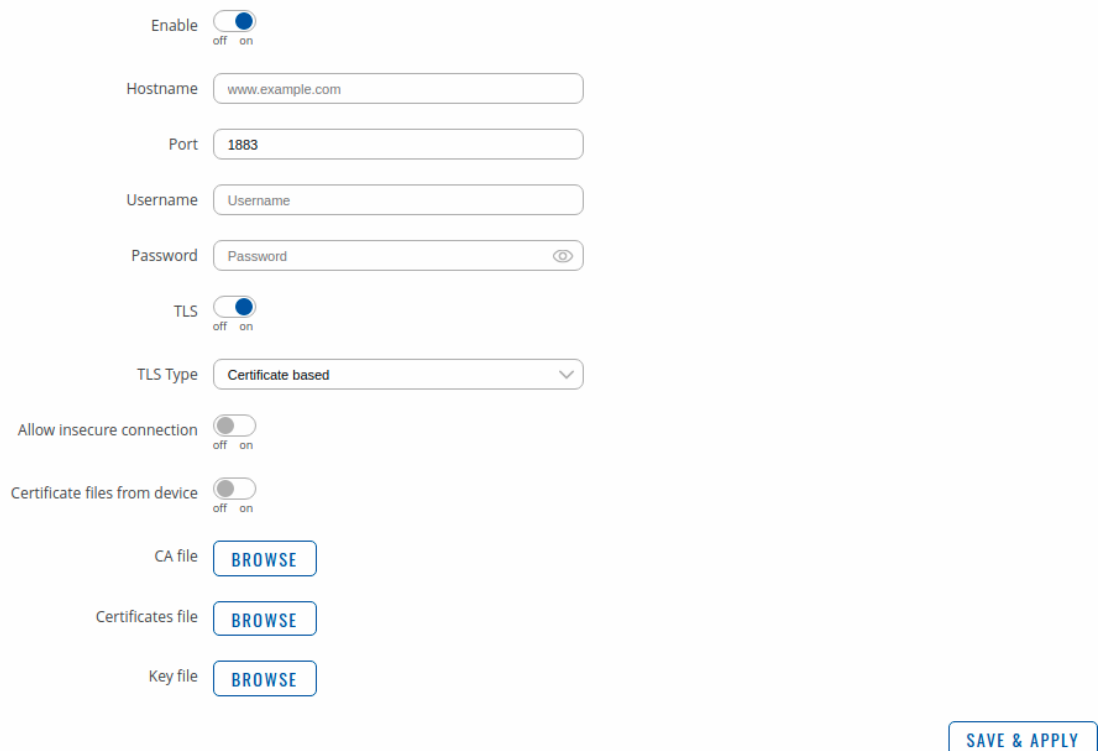
Allow Anonymous off | on; default: **on** Turns anonymous access to this broker on or off.

## 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.

### MQTT PUBLISHER



The image shows a configuration form for the MQTT Publisher. It includes several fields and controls:

- Enable:** A toggle switch currently set to 'on'.
- Hostname:** A text input field containing 'www.example.com'.
- Port:** A text input field containing '1883'.
- Username:** A text input field containing 'Username'.
- Password:** A text input field containing 'Password' with an eye icon for visibility.
- TLS:** A toggle switch currently set to 'on'.
- TLS Type:** A dropdown menu set to 'Certificate based'.
- Allow insecure connection:** A toggle switch currently set to 'off'.
- Certificate files from device:** A toggle switch currently set to 'off'.
- CA file:** A 'BROWSE' button.
- Certificates file:** A 'BROWSE' button.
- Key file:** A 'BROWSE' button.
- SAVE & APPLY:** A button at the bottom right.

Field	Value	Description
Enable	off   on; default: <b>off</b>	Toggles the MQTT Publisher ON or OFF.
Hostname	host   ip; default: <b>none</b>	Broker's IP address or hostname.
Port	integer [0..65535]; default: <b>1883</b>	Broker's port number.
Username	string; default: <b>none</b>	Username used for authentication to the Broker.
Password	string; default: <b>none</b>	Password used for authentication to the Broker.
TLS	off   <b>on</b> ; default: <b>off</b>	Turns the use of Transport Layer Security (TLS) on or off.
<b>On:</b> Allow insecure connection	off   on; default: <b>off</b>	Allows connections without verifying server authenticity.

TLS type	Certificate based   <b>Pre-shared key based</b> ; default: <b>Certificate based</b>	Select type of TLS.
<b>On:</b> Certificate files from device	off   on; default: <b>off</b>	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 → <a href="#">Certificates</a> page.
<b>On:</b> CA file	.ca file; default: <b>none</b>	Certificate authority file used in Transport Layer Security.
<b>On:</b> Certificate file	.crt file; default: <b>none</b>	Certificate file used in Transport Layer Security.
<b>On:</b> Key file	.key file; default: <b>none</b>	Key file used in Transport Layer Security.
<b>Pre-shared key based:</b> Pre-Shared-Key	string; default: <b>none</b>	The pre-shared-key in hex format with no leading "0x".
<b>Pre-shared key based:</b> Identity	string; default: <b>none</b>	The identity of this client. May be used as the username depending on the server settings.