Helmholz
COMPATIBLE WITH YOU

MQTT Broker

Manual

Version 1 | 8.12.2023 | for firmware V1.08 and above

Order numbers: 700-462-MQB01

Link to newest version of manual

Helmholz GmbH & Co. KG | Hannberger Weg 2 | D-91091 Großenseebach | Germany
Phone +49 9135 7380-0 | Fax +49 9135 7380-110 | info@helmholz.de | www.helmholz.com

Notes

To download the latest version of this manual, please visit our website at www.helmholz.de.

We welcome all ideas and suggestions.

Helmholz GmbH & Co. KG

Hannberger Weg 2 | 91091 Großenseebach

Revision Record:

Version	Date	Change
1	8.12.2023	First version for Firmware V1.08

Contents

1 General

This operating manual applies only to devices, assemblies, software, and services of Helmholz GmbH & Co. KG.

1.1 Structure of the manual

This manual is divided into 10 sections.

Section 1 contains **general information** and **safety instructions**.

Section 2 refers to **Security Recommendations**.

Section 3 explains the **system overview** and **features of the product**.

Section 4 explains the **installation and removal**.

Section 5 shows the **initial hardware commissioning**

Section 6 explains the **basic settings** of the MQTT Broker

Section 7 describes the **advanced setting** options

The **technical data** of the device is listed in section 8

1.2 Target audience for this manual

This description is only intended for trained personnel qualified in control and automation engineering who are familiar with the applicable national standards. For installation, commissioning, and operation of the components, compliance with the instructions and explanations in this operating manual is essential.

Configuration, execution, and operating errors can interfere with the proper operation of the device and result in personal injury, as well as material or environmental damage. Only suitably qualified personnel may operate the devices!

Qualified personnel must ensure that the application and use of the products described meet all the safety requirements, including all relevant laws, regulations, provisions, and standards.

1.3 Safety instructions

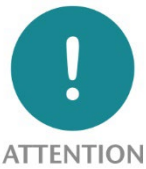
The safety instructions must be observed in order to prevent harm to living creatures, material goods, and the environment. The safety notes indicate possible hazards and provide information about how hazardous situations can be prevented.

1.4 Note symbols and signal words

If the hazard warning is ignored, there is an imminent danger to life and health of people from electrical voltage.

If the warning is ignored, there is a probable danger to life and health of people.

If the caution note is ignored, people can be injured or harmed.



Draws attention to sources of error that can damage equipment or the environment.

Gives an indication for better understanding or preventing errors.

1.5 Intended use

The MQTT broker (hereinafter referred to as "the device") can be used to transmit and forward MQTT messages.

All components are supplied with a factory hardware and software configuration. The user must carry out the hardware and software configuration for the conditions of use. Modifications to hardware or software configurations which are beyond the documented options are not permitted and nullify the liability of Helmholz GmbH & Co. KG.

The device may not be used as the only means for preventing hazardous situations on machinery and systems.

The MQTT Broker cannot be used for a direct connection to the Internet. Always use a dedicated router with a sufficiently dimensioned Internet firewall for an Internet connection. Observe the security recommendations for project planning, use and maintenance.

Problem-free and safe operation of the device presumes proper transport, storage, setup, assembly, installation, commissioning, operation, and maintenance.

The ambient conditions provided in the technical specifications must be adhered to.

The device has a protection rating of IP20 and must be installed in an electrical operating room or a control box/cabinet to protect it against environmental influences. To prevent unauthorized access, the doors of control boxes/cabinets must be closed and possibly locked during operation.

1.6 Improper use

WARNING

The consequences of improper use may include personal injuries of the user or third parties as well as property damage to the control system, the product, or the environment. Use the FLEXtra PROFINET-Switch only as intended!

1.7 Liability

The contents of this manual are subject to technical changes resulting from the continuous development of products of Helmholz GmbH & Co. KG. In the event that this manual contains technical or clerical errors, we reserve the right to make changes at any time without notice.

No claims for modification of delivered products can be asserted based on the information, illustrations, and descriptions in this documentation. Beyond the instructions contained in the operating manual, the applicable national and international standards and regulations must also be observed in any case.

1.7.1 Disclaimer of liability

Helmholz GmbH &Co. KG is not liable for damages if these were caused by use or application of products that was improper or not as intended.

Helmholz GmbH & Co. KG assumes no responsibility for any printing errors or other inaccuracies that may appear in the operating manual unless there are serious errors about which Helmholz GmbH & Co. KG was already demonstrably aware.

Beyond the instructions contained in the operating manual, the applicable national and international standards and regulations must also be observed in any case.

Helmholz GmbH & CO. KG is not liable for damage caused by software that is running on the user's equipment which compromises, damages, or infects additional equipment or processes through the remote maintenance connection and which triggers or permits unwanted data transfer.

1.7.2 Warranty

Report any defects to the manufacturer immediately after discovery of the defect.

The warranty is not valid in case of:

- Failure to observe these operating instructions
- Use of the device that is not as intended
- Improper work on and with the device
- Operating errors
- Unauthorized modifications to the device

The agreements met upon contract conclusion under "General Terms and Conditions of Helmholz GmbH & Co. KG" apply.

1.8 Open Source

Among other things, our products contain open-source software. This software is subject to the relevant license terms. The relevant license terms, including a copy of the full license text, are downloadable from the product website. They are also provided in our download area of the respective products at www.helmholz.de.

Furthermore, we offer to send the complete corresponding source code of the respective open-source software to you and to any third party as a DVD upon your request for a contribution towards expenses of Euro 10.00. This offer is valid for a period of three years. This offer is valid for a period of three years, calculated from the delivery of the product.

2 Security recommendations

Managed switches are network infrastructure components, and thus an important element in the security considerations of a system or network. When using the device, therefore please consider the following recommendations to prohibit unauthorized access to plants and systems.

General:

- Ensure at regular intervals that all relevant components fulfill these recommendations and possibly any other internal security guidelines.
- Evaluate your system holistically with a view to security. Use a cell protection concepts (“defense-in-depth”) with corresponding products, such as the WALL IE.
- Regularly inform yourself about security threats for all your components

Physical access:

- Limit physical access to components of relevance to security to qualified personnel.

Security of the software:

- Always keep the firmware of all communications components up to date.
- Inform yourself regularly of firmware updates for the product.
- Only activate protocols and functions you really need
- If possible, always use those variants of protocols that provide more security

Passwords:

- Define rules and roles for usage of the devices and the awarding of passwords
- Change standard passwords
- Only use strong passwords. Avoid weak passwords like, for example, “password1”, “123456789”, or similar.
- Ensure that all passwords are inaccessible to unauthorized personnel.
- Don’t use one password for various users and systems.

Helmholz is a member of the **CERT@VDE**. In addition to our technical newsletter, we communicate our security-relevant updates, patches and advisories to you as a user of Helmholz products. Find out more and use the services and database of the **CERT@VDE** to make your systems secure and keep them secure.

The Helmholz "**Product Security Incident Response Team**" **(PSIRT)** supports you proactively to protect your machines as best as possible in the context of industrial communication. Whenever new potential threats occur or are reported to us, we evaluate and process them immediately and provide you with recommended actions, patches and updates as quickly as possible to reduce the risk to a minimum.

You can help too: Report any product incidents to our **Product Security Incident Response Team** at psirt@helmholz.de or support@helmholz.de.

You can find more information on the topic of security here, for example:

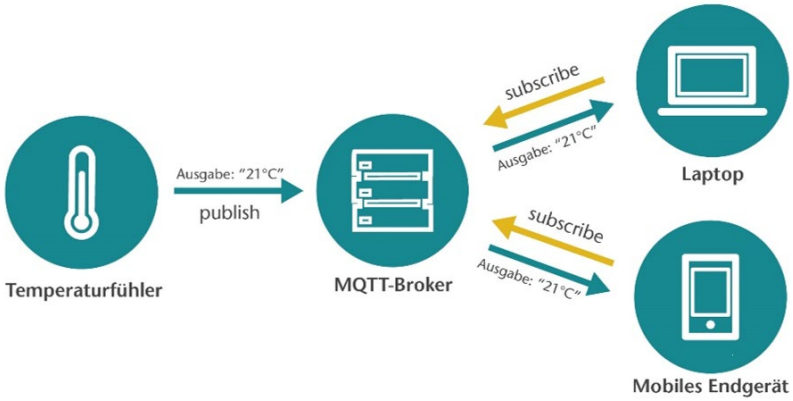
- Helmholz PSIRT webpage
- CERT@VDE
- Sichere-industrie.de
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Allianz für Cyber-Sicherheit

3 System overview

3.1 How MQTT works

MQTT stands for "Message Queuing Telemetry Transport". MQTT is an open message protocol for cases where clients need a small code footprint. It is mainly used for machine-to-machine communication (M2M) or connection to the cloud.

MQTT runs on TCP/IP with a PUBLISH/SUBSCRIBE topology. There are two types of systems in the MQTT architecture: Clients and brokers. A broker is a server with which the clients communicate. The broker receives the communication from the clients and sends it on to other clients. Clients do not communicate directly with each other but connect to the broker. Each client can be either a publisher ("sender"), a subscriber ("subscriber") or both.



MQTT is an event-driven protocol. There is no periodic or continuous data transmission, which keeps transmissions to a minimum. A client only publishes when there is information to send, and a broker only sends information to subscribers when new data arrives.

Messages within MQTT are published as topics. Topics are structured in a hierarchy in which the forward slash (/) is used as a separator. This structure is similar to the directory structure of a computer file system. With a structure such as "Machine1/Sensors/Temperatures/", a subscriber can request data coming from customers who publish messages on the topic "Temperature". In a broader sense, this can also be all data from customers who publish messages on any topic within the "Machine1/Sensors" area.

Topics are not explicitly created in MQTT. When a broker receives data that is published to a topic that does not yet exist, the topic is simply created. The message for the topic is saved and clients can subscribe to the new topic later.

The MQTT protocol is available in 2 versions: V3.1.1 and V5. Protocol V3.1.1 is currently the most common. The V5 protocol contains some improvements compared to V3.

Source and further information:

- https://mqtt.org/faq/
- http://www.steves-internet-guide.com/mqtt/

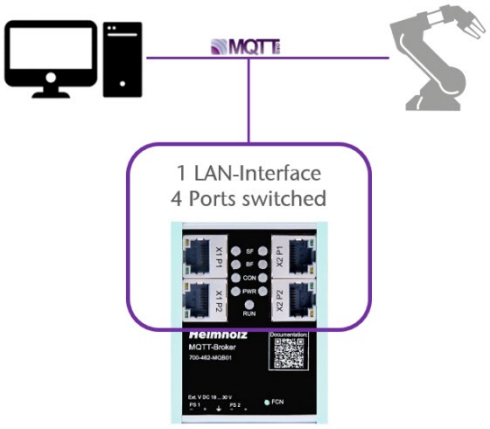
3.2 Structure and operating modes of the MQTT Broker

The MQTT broker enables MQTT messages to be saved and forwarded. The MQTT broker has 4 Ethernet interfaces with up to 100 MBps. Configuration takes place via the web interface.

The MQTT broker can be configured in two operating modes depending on the application: “**Switch**” and “**Firewall**”.

If the MQTT Broker is to store and distribute the MQTT messages within a closed machine network, all 4 Ethernet connections in the same IP subnet can be used.

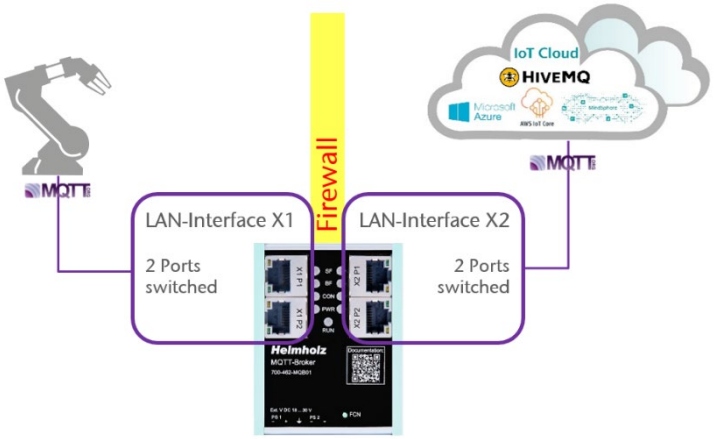
In "**Switch**" operating mode, the MQTT broker can be accessed via an IP address.



The operating mode "**Firewall**" enables MQTT communication between two different networks, e.g. the machine-network and a high-level or company network. This also enables a secure connection to the cloud.

In this operating mode, the left and right Ethernet sockets are in different IP subnets, each with its own IP address.

The special feature here is that only the MQTT content is exchanged between the two networks via the MQTT broker. Each network side has its own MQTT broker in which only the message content is exchanged.



No direct network communication is exchanged between the two network sides. The MQTT broker therefore represents a completely blocked firewall.

In the context of machine security, the MQTT broker is a secure transition ("conduit") between two zones exclusively for MQTT messages.

Further features of the MQTT broker:

- Full MQTT V3.1.1 & V5 feature set
- User management
- ACL management
- TLS Encryption
- Export/import of the configuration in editable file format

3.3 Status LEDs

SF (yellow)	On	Currently no function
	Flashing	Flashes together with BF LED: Firmware update in progress
BF (red)	Off	There is an MQTT connection with at least one device
	On	No MQTT connection active
	Flashing	Flashes together with SF LED: Firmware update in progress
CON (yellow)	Off	No MQTT connection active
	On	There is at least one MQTT connection
	Flashing	Active MQTT data exchange
PWR (green)	Off	No power supply (PS1 or PS2)
	On	Device is correctly supplied with power (PS1 or PS2)
RUN (green)	Off	The device has no power supply or is defective
	On	The device is in operation

The **SF-LED** does not yet have a function in the current firmware.

The **BF-LED** indicates a missing connection.

The **CON-LED** indicates an existing or active MQTT connection. In firewall operating mode, the statuses for the left and right sides are displayed separately. In "Switch" operating mode, the statuses are displayed on both LEDs simultaneously.

The **PWR-LED** is on as soon as the MQTT broker is connected to a power supply.

The left LED indicates a power supply to PS1, the right LED indicates a power supply to PS2.

3.4 Ethernet LEDs (RJ45)

Off		No network cable connected or network cable defective or connected device off
Green	On	Ethernet connection with 10/100 Mbit/s
Orange	flashing	Data transmission at the port is running

3.5 Factor Reset

The "Factory reset" function can be carried out via the web interface or directly on the device using the "FNC" button.

The factory reset via the button works as follows:

1. disconnect the power supply
2. press the "FNC" button and hold it down
3. restore the power supply
4. when the two "BF" LEDs light up, release the "FNC" button
5. the MQTT Broker should now restart and is ready in the factory state

4 Installation and removal

4.1 Access restriction

The modules are open operating equipment and must only be installed in electrical equipment rooms, cabinets, or housings.

Access to the electrical equipment rooms, cabinets, or housings must only be possible using a tool or key, and access should only be granted to trained or authorized personnel.

4.2 Mounting and minimum distances

The FLEXtra PROFINET switches can be mounted on a DIN rail and installed in any position. It is recommended to keep minimum distances when mounting. By keeping the minimum distances

- the modules can be mounted or dismantled without having to dismantle other parts of the system.
- there is enough space to connect all existing connections and contacting possibilities with commercially available accessories.
- There is space for any necessary cable routing.

ATTENTION

Installation must be carried out in accordance with VDE 0100/IEC 364 and applicable national standards. The device has protection level IP20. If a higher degree of protection is required, it must be installed in an enclosure or a control cabinet.

4.3 Electrical installation

Observe the regional safety regulations.

4.4 Protection against electrostatic discharges

To prevent damage through electrostatic discharges, the following safety measures are to be followed during assembly and service work:

- Never place components and modules directly on plastic items (such as polystyrene, PE film) or in their vicinity.
- Before starting work, touch the grounded housing to discharge static electricity.
- Only work with discharged tools.
- Do not touch components and assemblies on contacts.

4.5 EMC protection

To ensure electromagnetic compatibility (EMC) in your control cabinets in electrically harsh environments, the known rules of EMC-compliant configuration are to be observed in the design and construction.

ATTENTION

Observe all standards, regulations and rules regarding shielding when setting up the system and laying the necessary cables. Errors in the shielding can lead to malfunctions or even failure of the system.

4.6 Operation

Operate the device only in flawless condition. The permissible operating conditions and performance limits must be adhered to.

Retrofits, changes, or modifications to the device are strictly forbidden.

The device is a piece of operating equipment intended for use in industrial plants. During operation, all covers on the unit and the installation must be closed in order to ensure protection against contact

ATTENTION

When the MQTT Broker is switched off, connections are interrupted! Before starting any work on the device, make sure that no impermissible interference occurs in connected systems when the bus connections are interrupted.

4.7 Recycling / WEEE

The company Helmholz GmbH & Co. KG is registered as a manufacturer with the HELMHOLZ brand and the device type "Small devices of information and telecommunications technology for exclusive use in households other than private households" as well as the following registration data:

Helmholz GmbH & Co. KG,
Location / Headquarters: 91091 Großenseebach,
Address: Hannberger Weg 2,
Name of authorized representative: Carsten Bokholt,

Registration number: **DE 44315750**

The electrical devices described in this document are to be recycled. According to Directive 2012/19/EU on waste electrical and electronic equipment (WEEE), they must not be disposed of by municipal waste disposal companies.

5 Preparing the MQTT broker

5.1 Power supply

The MQTT Broker must - at the wide-range input DC 18 ... 28 V - be supplied with DC 24 V via the supplied connector plug. The power supply is designed redundantly, at least one supply path "PS 1" or "PS 2" must be connected.

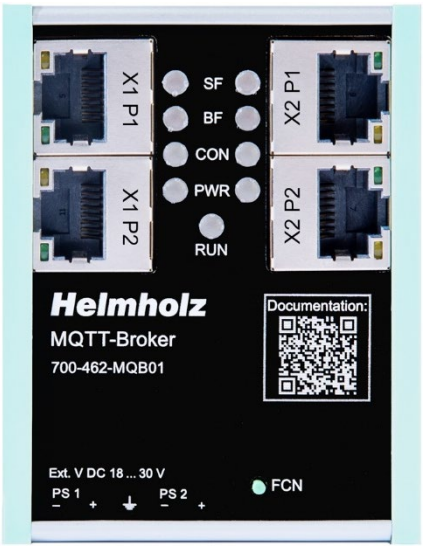
NOTE

The housing of the MQTT Broker is not earthed. Please connect the functional earth connection (FE) of the switch properly to the reference potential.

5.2 Network

The RJ45 sockets "X1 P1" and "X1 P2" are for connecting the left network, the RJ45 sockets "X2 P1" and "X2 P2" are for connecting the right network. Ports X1 P1 and X1 P2, as well as X2 P1 and X2 P2 are each connected internally to a switch.

Depending on the operating mode, the X1 and X2 interfaces are either logically separate networks ("firewall") or work in the same subnet ("switch"). See also chapter 3.2.



6 Configuration and diagnostics via the web interface

6.1 Login

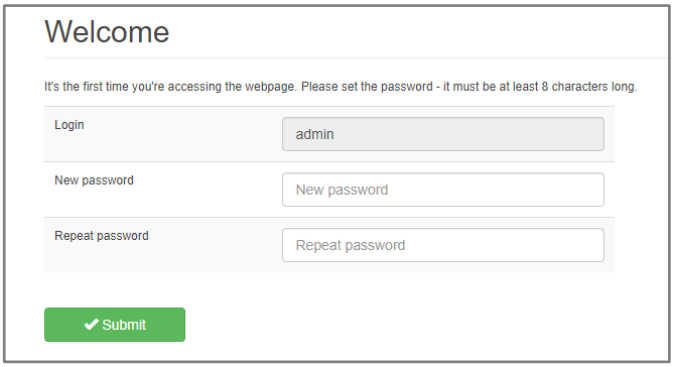
The web interface of the MQTT broker can be used to fully configure the broker and query the status of the device.

The web interface has the following network configuration on delivery:

- X1 (left Ethernet sockets): 192.168.0.100
- X2 (right Ethernet sockets): DHCP On

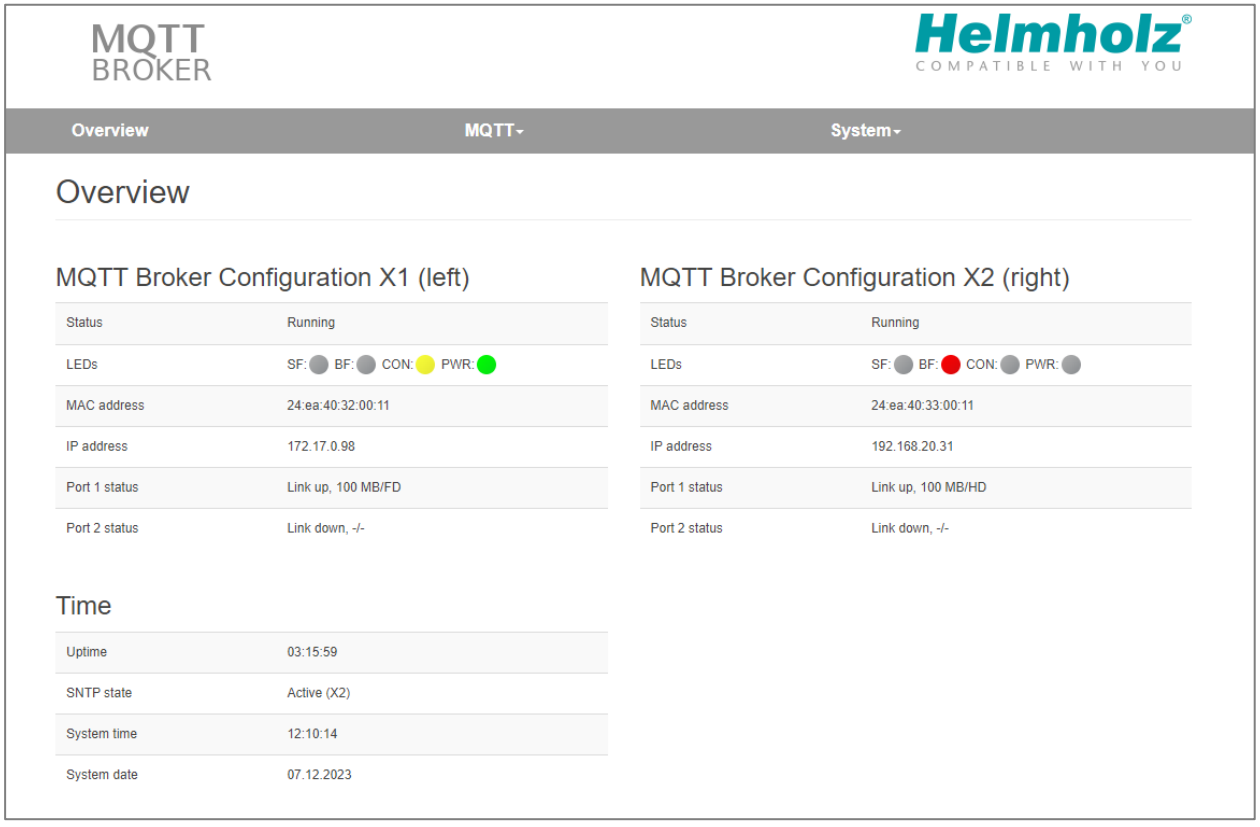
Connect the device to your network or PC using one of the two Ethernet sockets on the left side and set the PC to a free IP address in the subnet 192.168.0.x (255.255.255.0).

When accessing the web interface for the first time and after a factory reset, the password for the admin user must first be reassigned.



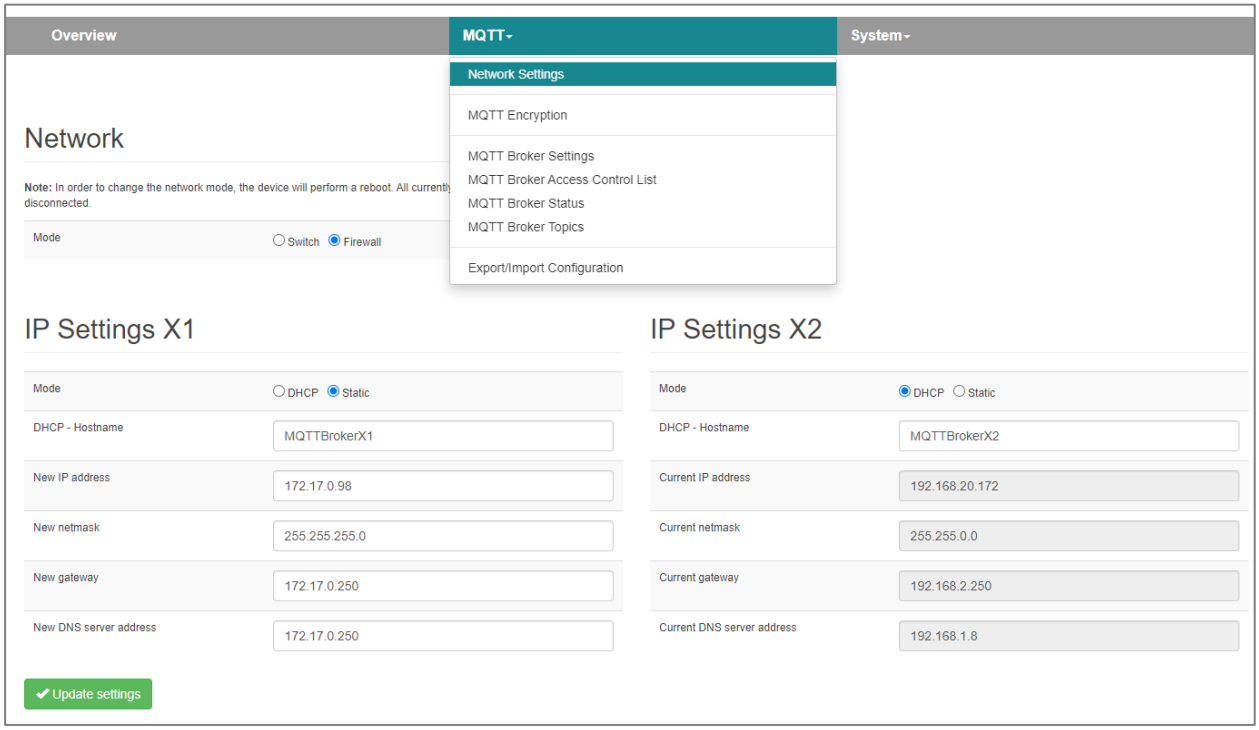
6.2 Overview

The page "Overview" provides an overview of the current status of the MQTT broker.



6.3 Operating mode and network settings

The important basic settings for operation and the network can be found in the "MQTT" menu under "Network Settings".



First, the operating mode of the MQTT broker can be selected between "Switch" and "Firewall". For explanations of the operating mode, see chapter 3.2.

ATTENTION

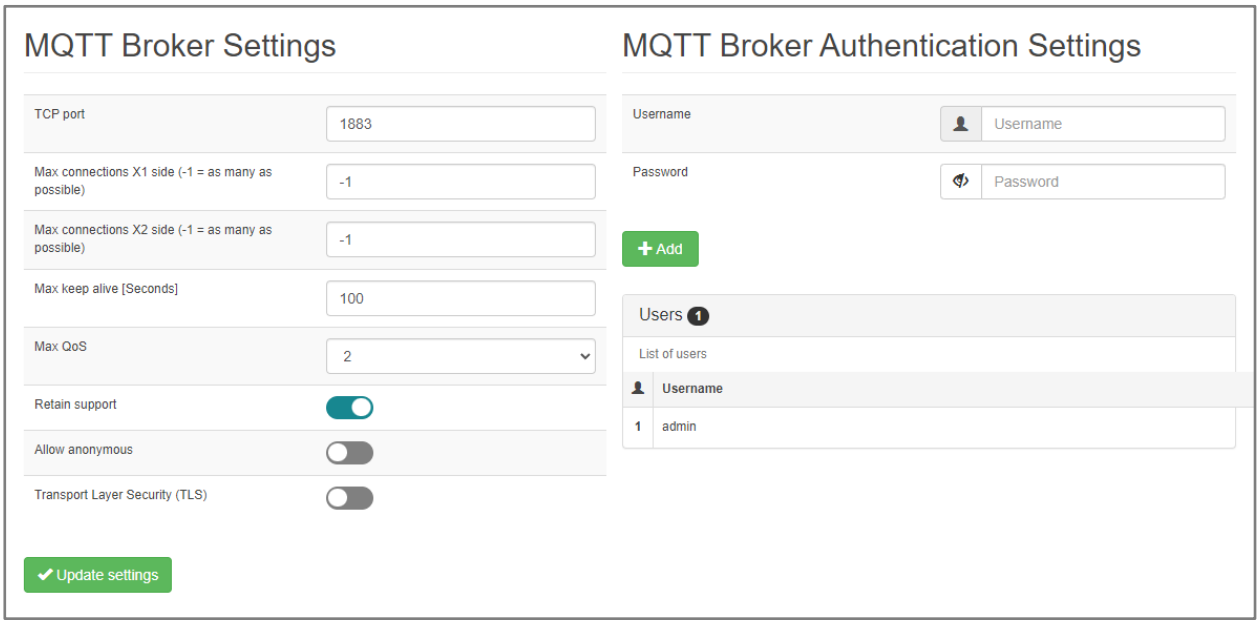
When the "Mode" operating mode is changed, a restart of the device is triggered with "Update settings". Changes to the network parameters alone do not trigger a restart, but the active connections may be interrupted.

In "Firewall" operating mode, the setting options for both network interfaces X1 and X2 are available separately. Please note that the subnets of the two network interfaces must also be configured differently.

In "Switch" operating mode, only one network configuration is available, which is active on all 4 Ethernet connections.

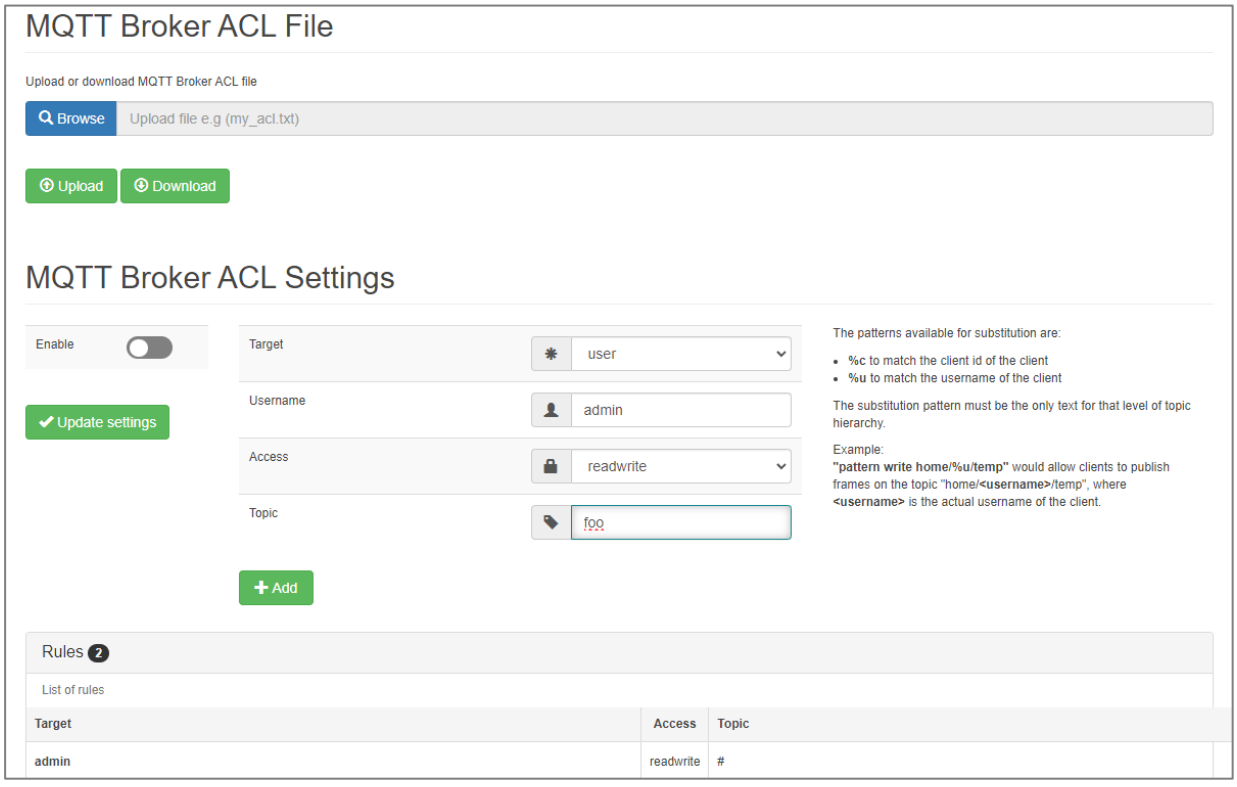
6.4 MQTT Broker Settings

The basic settings of the MQTT broker and MQTT user can be edited in the "MQTT Broker Settings" dialog.



6.5 Set MQTT Broker access rights (ACL)

In the "MQTT Broker Access Control List" dialog, the access rights of the various users to the topics can be defined. Either a prepared ACL file can be transferred to the MQTT Broker or the rules can be defined individually.



The ACL file is a text file that defines the access rights of users to the topics in a simple format.

ACL-File Example:

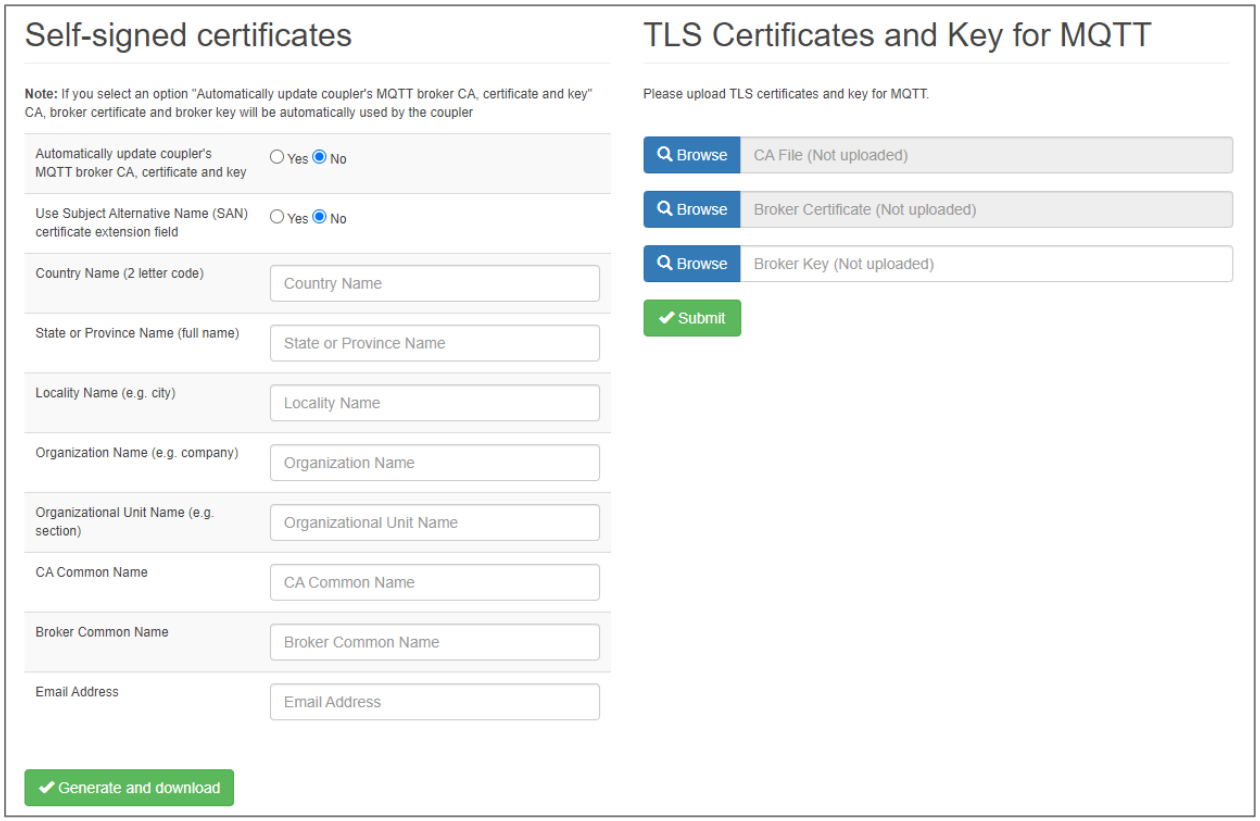
```
# This affects access control for clients with no username.
topic read $SYS/#

# This only affects clients with username "roger".
user roger
topic foo/bar

# This affects all clients.
pattern write $SYS/broker/connection/%c/state
```

An existing ACL configuration can also be downloaded from the MQTT broker and saved on the PC.

Further information on ACL files can be found on the documentation pages of the "mosquitto" MQTT broker.

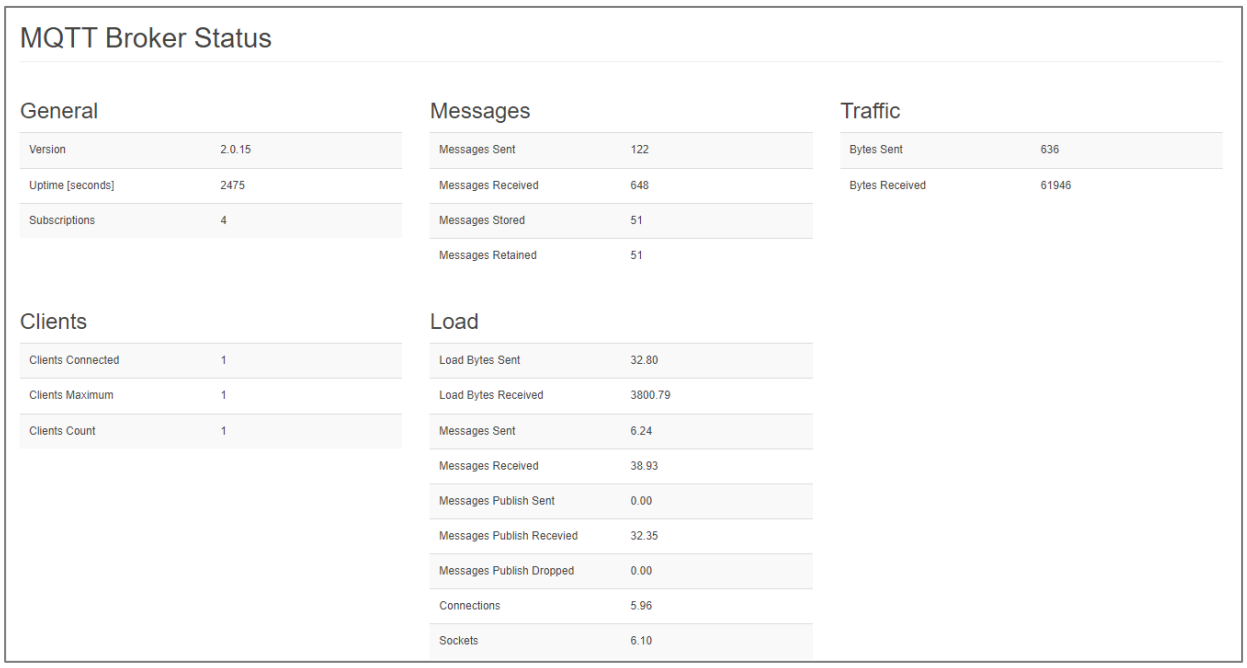
6.6 Set MQTT encryption

The MQTT broker can either create its own certificate for authentication via MQTT with SSL ("self-signed certificates") or an externally created certificate can be uploaded to the broker.



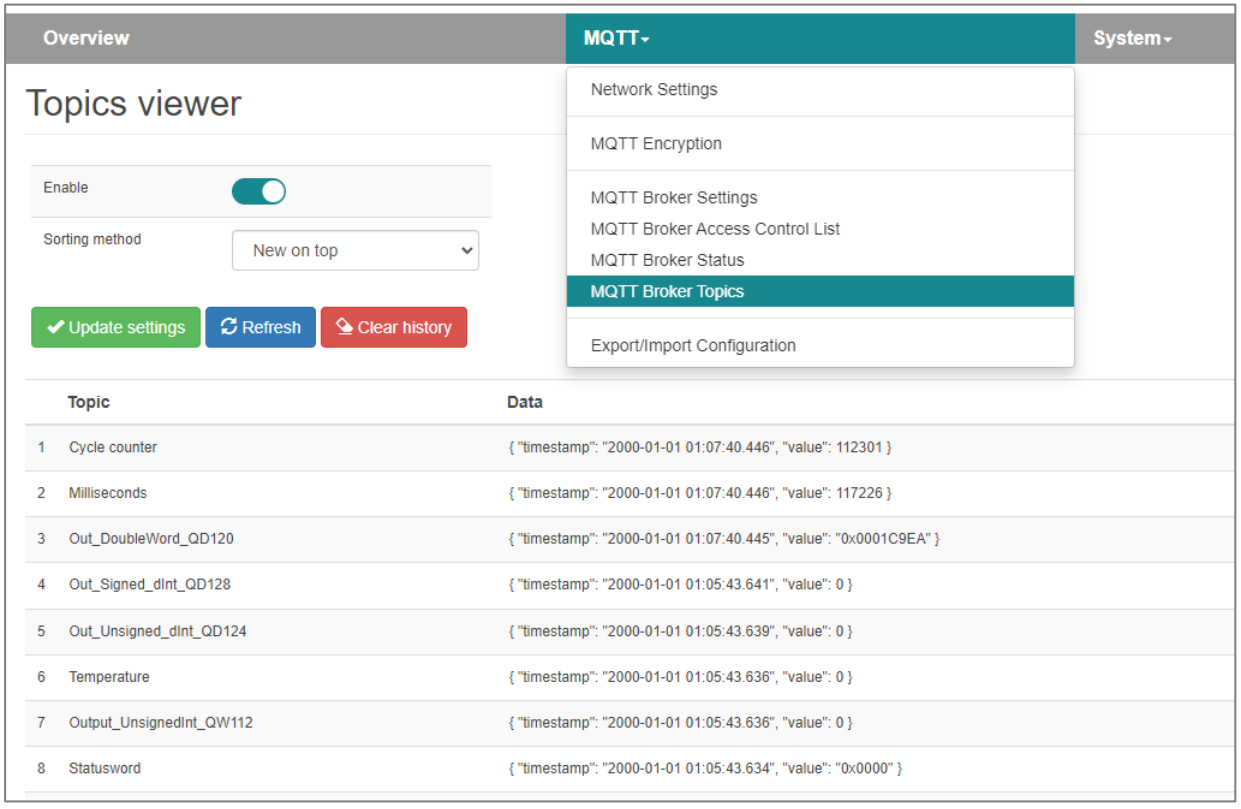
6.7 MQTT Broker Status

The MQTT Broker Status website provides information about the current status of the broker. For diagnostic purposes, you can see whether the MQTT publishers and subscribers are actively working and exchanging data.



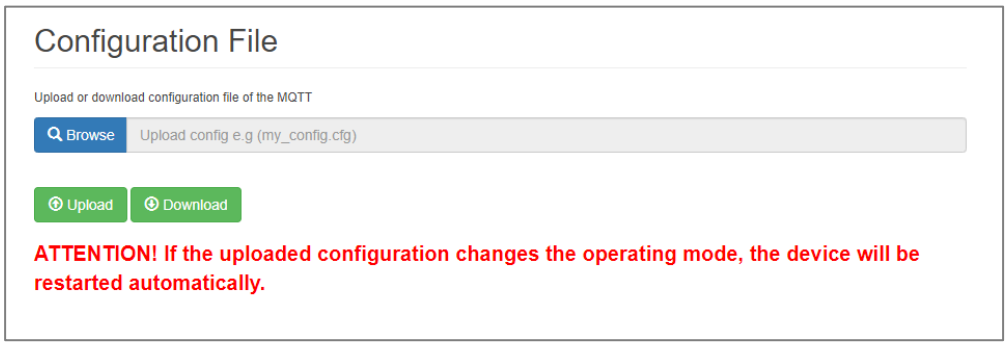
6.8 Topics Viewer

The Topics Viewer can be used to view the current MQTT topic content of the broker. All received messages are displayed here with their topic name and the last message content.



6.9 Export/import of the configuration

The entire configuration of the MQTT Broker can be exported. This configuration file can be used to update a factory-fresh device to the same configuration status at any time.



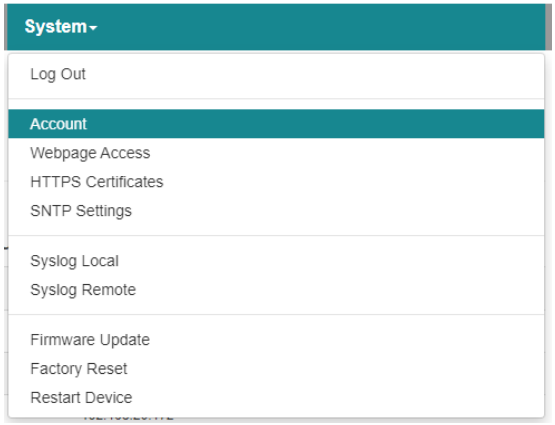
"Download" downloads the configuration as a file to a PC. "Upload" uploads a previously saved configuration back to the device. The device restarts with the uploaded configuration if necessary.

ATTENTION

The ACL list may have to be downloaded and saved separately during a device backup.

7 Further settings

Further settings can be made and information read out in the "System" menu.

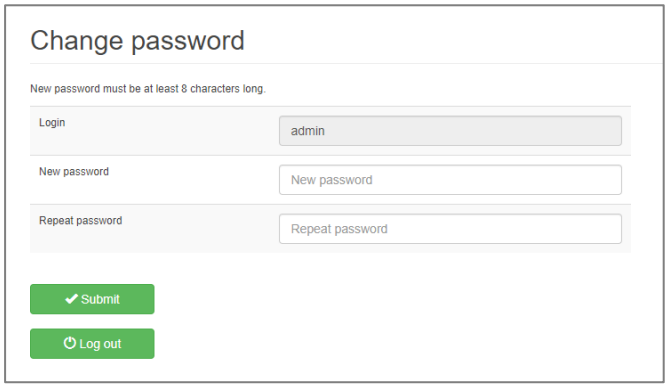


7.1 Change password for website

The password of the web administrator "admin" can be changed in the "Account / Change Password" menu.

Additional users cannot currently be created.

The user and password are only active for website access. Adjustments have no effect on MQTT operation.



7.2 Restricting access to the website

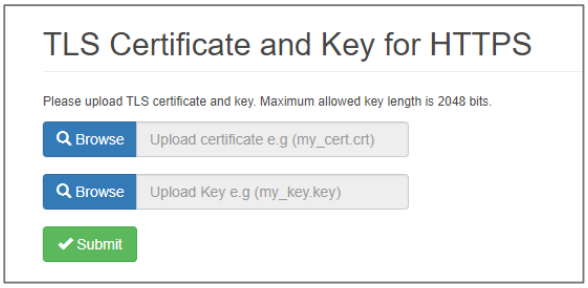
Access to the web interface can be restricted to one of the two interfaces for security reasons.

The setting only has an effect in "Firewall" operating mode.

7.3 Upload certificates for HTTPS access

A company certificate can be stored for the MQTT Broker website.

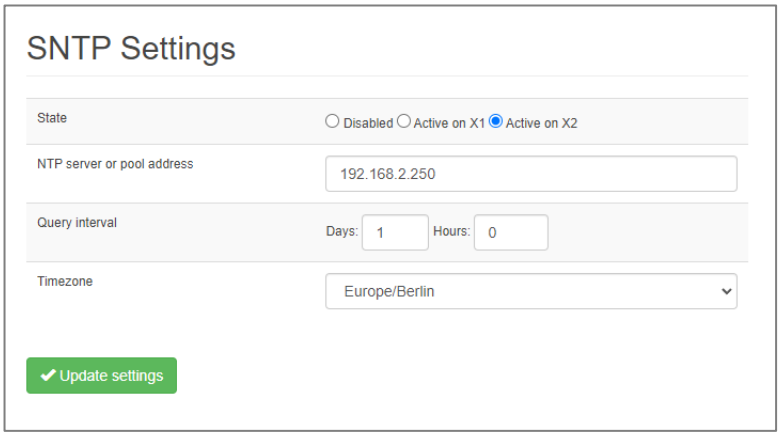
This ensures that calling up the configuration website is trustworthy in addition to HTTPS encryption.



7.4 Setting the time server (SNTP)

An SNTP server can be set in the "SNTP Settings" menu to update the time of the MQTT broker.

The time is mainly required for the syslog records and for checking certificates.



7.5 Syslog Server

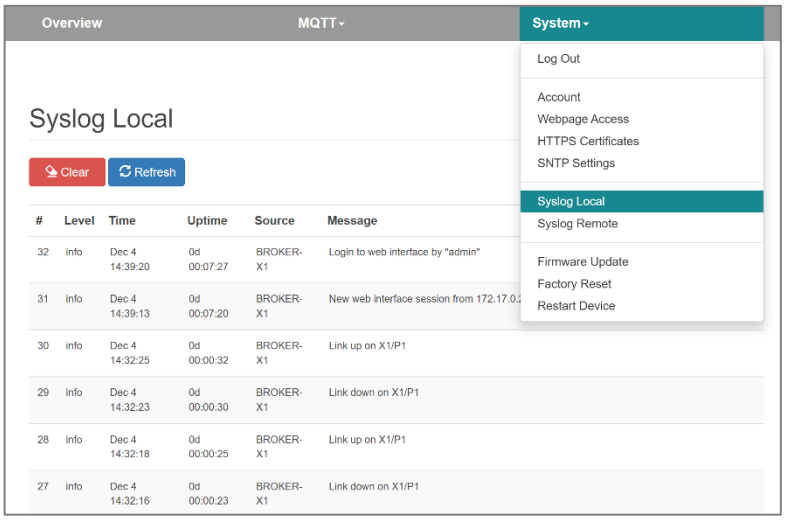
The syslog server built into the MQTT Broker logs all user and system events with time and date. User events are changes to the configuration or user logins. The system events come from the operating system or the running application. For the syslog server to display the time correctly, it must be set in the "Time" menu (see section above).

7.5.1 System-Log Local

The local syslog display lists the recorded events.

The syslog memory can be deleted with "Clear".

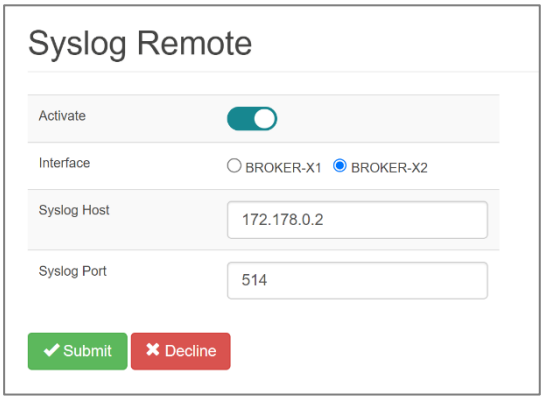
The system log display can be refreshed with "Refresh".



7.5.2 System Log Remote

The syslog messages can also be sent from the MQTT broker to a PC via the network on which a program for syslog recording is running.

The IP address of the host, the port and the network interface can be specified here.



7.6 Firmware Upgrade

The firmware stored in the device can be updated. New firmware versions are delivered in files with the extension ".huf" and are available via the Helmholz homepage www.helmholz.de.

Link to firmware: https://www.helmholz.de/goto/700-462-MQB01

Under "Firmware" ("System" menu), a firmware file can be selected and loaded into the device. After the firmware has been loaded, the device restarts.

ATTENTION

The active update process is indicated by the SF & BF LEDs flashing together.

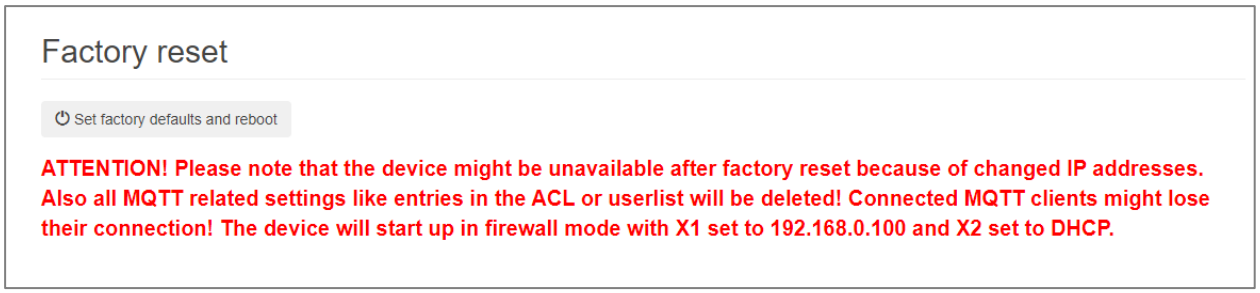
Interrupting the power supply during the update process can render the device unusable. The device must then be sent in for repair.

NOTE

The configuration of the MQTT Broker is retained when updating to a higher version, insofar as this is technically possible. A "downgrade" to an older firmware version can lead to configuration errors. It is recommended to perform a factory reset before a downgrade.

7.7 Factory Reset

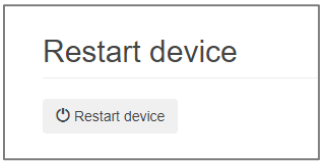
The "Factory Reset" function resets the MQTT broker to the factory settings.



7.8 Restart Device

The "Restart Device" function can be used to trigger a restart of the MQTT broker.

Please note that this will interrupt all connections and cached MQTT messages will be lost.



8 Technical data

Order number	**700-462-MQB01**
Name	MQTT-Broker
Scope of delivery	MQTT-Broker with power supply plug
Dimensions (DxWxH)	32,5 x 58,5 x 76 mm
Weight	Ca. 135 g
Ethernet interface(X1/X2)	
Number / Connection	4 / integrated Switch
Connection	RJ45
Transmission rate	10/100 Mbit/s
Protocols	MQTT V3.1.1 & V5; HTTPS
Features	TLS Encryption; User management, ACL management
Status indication	
Functional status	9 LEDs
Ethernet status	8 LEDs, two-colored
Power supply	
Voltage supply	2x 24 V DC, 18 ... 30 V DC, redundant
Current draw	max. 140 mA at DC 24 V
Power dissipation	max. 3,4 W
Ambient conditions	
Ambient temperature	0°C ... +60°C
Transport- and storage temperature	-40°C ... +85°C
Relative air humidity	95 % r H without condensation
Protection rating	IP20
Pollution degree	2
Mounting position	As desired
Approvals	CE