ETHERLINE® GUARD PM03T / PM02TWA

Operating instructions

Issue 1.1 | 23.11.2022 | from firmware V 1.00

Link to the latest version of
the operating instructions

U.I. Lapp GmbH | Schulze-Delitzsch-Straße 25 | D-70565 Stuttgart | Germany
Phone +49 (711) 78 38 - 01 | Fax +49 (711) 78 38 - 26 40 | info@lapp.de | www.lappkabel.de

Notes

All rights reserved, including those of translation, reprinting and reproduction of these operating instructions or parts thereof.

No part of these operating instructions may be reproduced, processed, duplicated or distributed in any form (photocopy, photograph, microfilm or other process), not even for the purpose of teaching, or using electronic systems without the written permission of U.I. Lapp GmbH.

The latest version of the operating instructions can be found on the Internet at www.lappkabel.com

We are happy to receive suggestions for improvement and ideas.

Furthermore, we offer to send the complete corresponding source code of the respective open source software to you and any third party as a DVD upon your request for a contribution towards costs of Euro 10,00. This offer is valid for a period of three years, calculated from the delivery of the product.

Changes in this document:

Stand	Date	Change
1.0	04.03.2022	First Version / Firmware V1.00.18
1.1	23.11.2022	Appendices A (setting up an MQTT connection) and B (SSL and secure MQTT connection certificates) added, additional hint in the power supply requirement

Content

1 General

These operating instructions apply exclusively to devices, assemblies, software and services provided by U.I. Lapp GmbH.

1.1 Safety instructions

The safety instructions must be observed in order to protect persons and living beings, material goods and the environment from damage. The safety instructions point out possible dangers and give advice on how to avoid dangerous situations.

1.2 Signs and signal words

⚠ CAUTION

If the danger notice is not observed, there is an immediate danger to the health and life of persons due to electrical voltage.

⚠ WARNING

If the danger notice is not observed, there is a probable danger to the health and life of persons.

❗ ATTENTION

If the danger notice is not observed, persons may be injured or harmed.

❗ ATTENTION

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

ℹ NOTE

Gives a hint for better understanding or to avoid mistakes.

1.3 Target group of the operating instructions

This description is intended exclusively for trained specialists in control and automation technology who are familiar with the applicable national standards. For installation, commissioning and operation of the components, it is absolutely necessary to observe the notes and explanations in these operating instructions.

⚠ WARNING

Project planning, design and operating errors can impair the proper operation of the ETHERLINE® GUARD and result in personal injury, property damage or environmental damage.
Only adequately qualified personnel may operate the units!

The qualified personnel must ensure that the application or use of the products described complies with all safety requirements, including all applicable laws, regulations, provisions and standards.

ℹ NOTE

The minimum length of the Ethernet cable to be monitored is 2m.

Before using the unit, please check whether a newer version of the firmware is available on the website (for more information on firmware updates, see chapter 9) is available.

1.4 Intended use

The LAPP ETHERLINE® GUARD is used for condition monitoring of Ethernet-based data lines with the 100BASE-TX transmission standard, with a focus on dynamic applications.

All components are delivered with a factory hardware and software configuration. The hardware and software configuration to suit the application conditions must be carried out by the user. Changes to the hardware or software configuration that go beyond the documented possibilities are not permitted and will result in the exclusion of liability on the part of U.I. Lapp GmbH.

⚠

CAUTION

The device must not be used as the sole means of averting dangerous conditions on machinery and equipment.

Faultless and safe operation of the unit requires proper transport, storage, set-up, assembly, installation, commissioning, operation and maintenance.

The ambient conditions specified in the technical data must be observed.

The unit has protection level IP 20 and must be installed in an electrical operating room or a control box/switch cabinet to protect it from environmental influences. To prevent unauthorised operation, the doors of the switch boxes/switch cabinets must be closed and secured if necessary during operation.

1.5 Abuse

⚠

WARNING

The consequences of improper use may include personal injury to the user or third parties, data protection violations as well as property damage to the control unit, the product or environmental damage. Only use the unit as intended!

1.6 Assembly / Disassembly

1.6.1 Access restriction

The assemblies are open equipment and may only be installed in electrical operating rooms, cabinets or enclosures. Access to the electrical operating rooms, cabinets or enclosures must only be possible using tools or keys and must only be permitted to instructed or approved personnel.

1.6.2 Installation position and minimum distances

The module is suitable for mounting on a top-hat rail in any position. No minimum distances need to be observed, but accessibility for connectors and the SD card must be ensured.

1.6.3 Electrical installation

The regionally applicable safety regulations must be observed.

1.6.4 Protection against electrostatic discharges

To prevent damage caused by electrostatic discharges, the following safety measures must be followed during assembly and service work:

- Never place components and assemblies directly on plastic objects (e.g. polystyrene, PE film) and also avoid their proximity.

- Use ESD-compliant tools and clothing.
- Do not touch components and assemblies at contacts.

1.6.5 EMC protection

In order to ensure electromagnetic compatibility (EMC) in your control cabinets and in an electrically harsh environment, the known rules of EMC-compliant construction must be observed during design and assembly. In particular, the functional earth (FE) connection must be connected to the potential equalisation.

1.6.6 Operation

Only operate the unit when it is in technically perfect condition. The permissible operating conditions and performance limits must be observed.

Retrofitting, modifications or conversions to the unit are strictly prohibited.

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

1.6.7 Liability

The contents of these operating instructions are subject to technical changes resulting from the continuous further development of the products of U.I. Lapp GmbH. In the event that these operating instructions contain technical errors or editorial mistakes, we reserve the right to make changes at any time and without notice.

No claims for changes to products already supplied can be made on the basis of the information, illustrations and descriptions in this documentation. In addition to the instructions contained in the operating instructions, the applicable national and international standards and regulations must always be observed.

1.6.8 Disclaimer

U.I. Lapp GmbH is not liable for damage caused by improper use or application of the products.

U.I. Lapp GmbH accepts no liability for any printing errors or other inaccuracies contained in the operating instructions, unless they are serious errors of which U.I. Lapp GmbH is already demonstrably aware.

In addition to the instructions contained in the operating instructions, the applicable national and international standards and regulations must always be observed.

U.I. Lapp GmbH is not liable for damage caused by software that is active on the user's devices and impairs, damages or infects other devices or processes via the remote maintenance connection and triggers or enables undesired data transfer.

U.I. Lapp GmbH shall not be liable in the event of incorrect calculation.

1.6.9 Warranty

Report defects to the manufacturer immediately after the defect has been detected.

The warranty expires in the event of:

- Disregard of these operating instructions
- Improper use of the appliance
- Improper work on and with the unit
- Operating errors

- Changes to the unit

The agreements made upon conclusion of the contract under "General Terms and Conditions of U.I. Lapp GmbH " shall apply.

1.6.10 Recycling and disposal / WEEE

LAPP complies with all legal requirements and is registered with the national registers for WEEE in accordance with the directives.

The products described in this document are low-polluting, recyclable and meet the requirements of the WEEE Directive 2012/19/EU for the disposal of waste electrical and electronic equipment.

The electrical appliances described are designed for the business-to-business (B2B) sector and are to be recycled.

According to Directive 2012/19/EU on Waste Electrical and Electronic Equipment (WEEE), such devices may not be disposed of via municipal waste disposal companies.

Therefore, do not dispose of the products at public disposal points.

For environmentally sound recycling and disposal of your old device, contact a certified disposal company for electronic waste or your LAPP contact person.

More at www.lappkabel.de/weee.html

Note different country-specific regulations.

2 Security recommendations

ETHERLINE® GUARD is a network component and therefore an important element when considering security aspects within a facility or network. Therefore, when using ETHERLINE® GUARD, observe the following recommendations to prevent unauthorised access to installations and systems.

General:

- Ensure at regular intervals that all relevant components comply with these recommendations and, if applicable, other internal safety guidelines.
- Evaluate your system holistically with regard to safety. Use a cell protection concept ("defence-in-depth") with appropriate products.
- Keep yourself regularly informed about security threats to all your components.

Physical access:

- Restrict physical access to safety-related components to qualified personnel.

Security of the software:

- Keep the firmware and all communication components up to date at all times.
- Check regularly for firmware updates for the product.
- Only activate protocols and functions that you really need.
- Switch off accesses that are not required for operation after configuration
- Deactivate access options after configuration that are not required for continuous operation.
- If possible, always use those variants of protocols that offer more security.

Passwords:

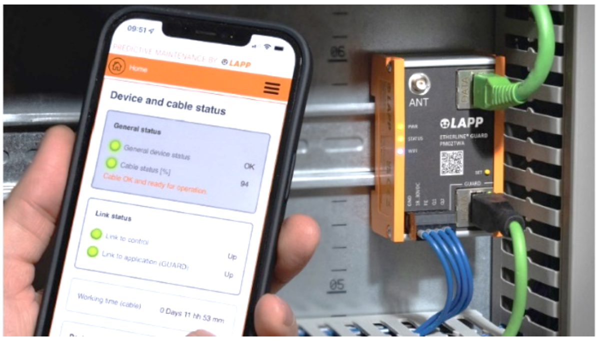
- Define rules and roles for the use of the devices and the assignment of passwords.
- Change default passwords.
- Only use passwords with a high password strength.
- Ensure that all passwords are inaccessible to unauthorised personnel.
- Do not use the same password for different users and systems.

Further information on the topic of security can be found here, for example:

- Federal Office for Information Security (BSI)
- CERT@VDE
- Safe-industry.com
- Alliance for Cyber Security

3 Overview

The ETHERLINE® GUARD can be used to monitor Ethernet-based data lines with a transmission speed of 100Mbit/s (100Base-TX). The ETHERLINE® GUARD is looped into the cable harness and can provide information about the quality of the cable connection via a separate network connection (LAN or WiFi) or via a digital output.



Benefit:

- Increased plant availability due to plannable downtimes→ Reduction of maintenance costs
- Simple commissioning with automated parameterisation ("teach-in" in a few seconds)
- Requires no new data line or changes to the cable design; retrofit into the existing network structure is possible at any time
- Reliable IIoT communication thanks to MQTT interface

Fields of application:

- For monitoring the service life of a data line at risk of failure (e.g. function-critical data line in dynamic or mechanically loaded applications).
- Suitable for data lines according to transmission standard 100BASE-TX (with 100 Mbit/s) according to IEEE 802.3
- Also suitable for EtherCAT, EtherNet/IP and 2-pair PROFINET applications
- For use in the control cabinet (protection class IP 20)
- Space-saving due to uniquely compact design
- For use in Ethernet-based networks in automation technology

Features:

- Feedback of the expected service life via LED display "STATUS", via the web server or via digital output.
- Threshold value for alarm triggering individually adjustable (service life 99 - 50%).
- Can be integrated into IIoT structures for status/data evaluation via MQTT interface
- WiFi connection as access point (AP) for mobile access or as client in a WLAN network

Versions:

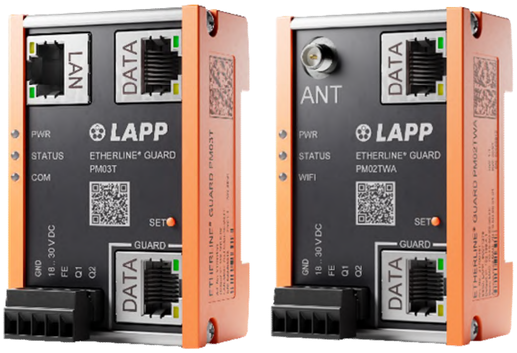
- ETHERLINE® GUARD PM03T, LAN connection
- ETHERLINE® GUARD PM02TWA, WiFi connection

4 Structure and connection of the ETHERLINE® GUARD

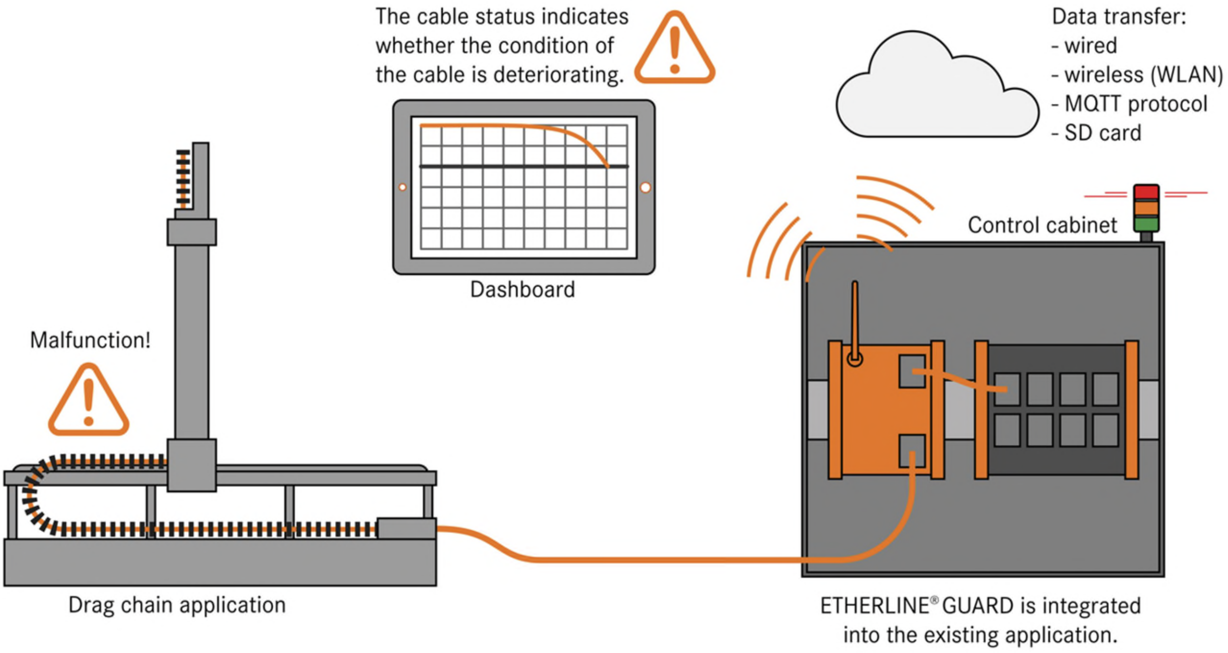
The ETHERLINE® GUARD has two RJ45 connections (DATA) for the cable to be monitored and a LAN connection (PM03T) or an antenna connection for WiFi (PM02TWA) configuration via the web interface.

The LEDs on the left edge of the housing indicate the status of the unit (PWR / STATUS / COM / WIFI) and the status of the monitored data line.

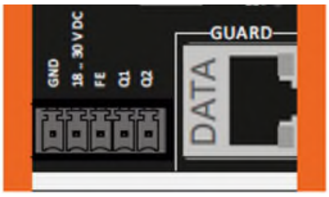
Various functions can be carried out via the function button (SET).



Application example:


The cable status indicates whether the condition of the cable is deteriorating.
Dashboard
Data transfer:
- wired
- wireless (WLAN)
- MQTT protocol
- SD card
Control cabinet
Malfunction!
Drag chain application
ETHERLINE® GUARD is integrated into the existing application.

4.1 Connection of the power supply



The ETHERLINE GUARD has to be connected with 24 V DC at the wide-range input "18 ... 30 V DC" and "GND". The "FE" connection is for the functional earth. Connect this properly to the reference potential.

NOTE The housing of the ETHERLINE® GUARD is not earthed.
Please be sure to connect the functional earth connection ("FE") of the unit to the reference potential of your control cabinet or system structure to ensure correct ESD discharge of the antenna and network sockets.

ATTENTION If the unit is used in a manner not specified by the manufacturer, the protection provided by the unit may be impaired. Pay particular attention to correct contacting when installing the cables. Always refer to the current documentation first in case of problems. Connected circuits must comply with the requirements for limited energy circuits according to UL61010-1.

4.2 Connection of the line to be monitored (DATA)

The ETHERLINE® GUARD has two RJ45 connections (DATA) for the link to be monitored, whereby the cable to be monitored must be connected to the RJ45 connection marked DATA + GUARD. The ETHERLINE® GUARD is looped into the cable to be monitored via these two connections.

The cable to be monitored (e.g. a trailing cable) must be connected to the lower connection ("Guard"). The upper DATA port should then be connected to the communication partner (e.g. the control unit) with another commercially available industrial Ethernet cable.

NOTE

The cable measurement is carried out at the lower connection "Guard DATA" over the entire cable (minimum length 2m) to the connected communication partner.

The ETHERLINE® GUARD does not change the content of the data transmission between the DATA connections.

ATTENTION

Data transmission between the two DATA connections only works when the ETHERLINE® GUARD is supplied with voltage and is in normal operating mode!

4.3 Connecting the data connection (LAN / WIFI)

The data connection "LAN" (PM03T) or "WIFI" (PM02TWA) allows access to the web server of the monitoring electronics via Ethernet line or via WiFi. The web page displays the status of the cable to be monitored and enables configuration of the ETHERLINE® GUARD. Furthermore, the status of the cable to be monitored can also be sent to databases or a cloud via MQTT.

For more information on how to access the website, see the chapter 6.
The use of the MQTT Publisher is explained in Chapter 8.

ATTENTION ETHERLINE® GUARD WIFI (PM02TWA)

The unit should be installed and operated with a minimum distance of 20 cm between the radiator/antenna and your body. For information on the transmitting power, see the technical data in chapter 12.2.

4.4 Connection of the digital outputs (Q1/Q2)

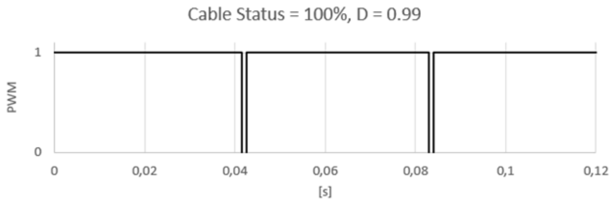
The digital outputs Q1 and Q2 are only active after the teach-in has been completed.

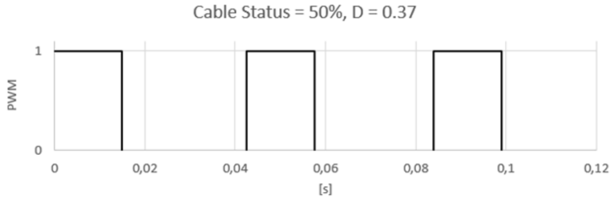
The digital output Q1 can signalize that maintenance is required for the cable if the value falls below a configurable threshold ("**Alarm threshold for Q1**"). The default value is 80%. The output changes its state to HIGH (normally open function) when it falls below this value. For more information on configuring the threshold value, see chapter 7.1. If data communication is interrupted at the "Guard" connection, output Q1 also changes its state to HIGH.

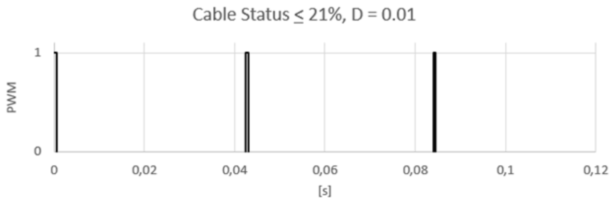
The digital output Q2 emits a pulse-width modulated signal whose duty cycle D is directly assigned to the "Cable Status". The basic frequency is 24 Hz, the duty cycle varies from 99% (Cable Status = 100%) to 1% (Cable Status < 21%). If data communication is interrupted at the "Guard" connection, a duty cycle of D = 1% is emitted.

A measured duty cycle of D % results in the following cable status (in %):

$$Cable\ Status\ [\%] = \frac{D\ [\%]}{1.24} + 20$$

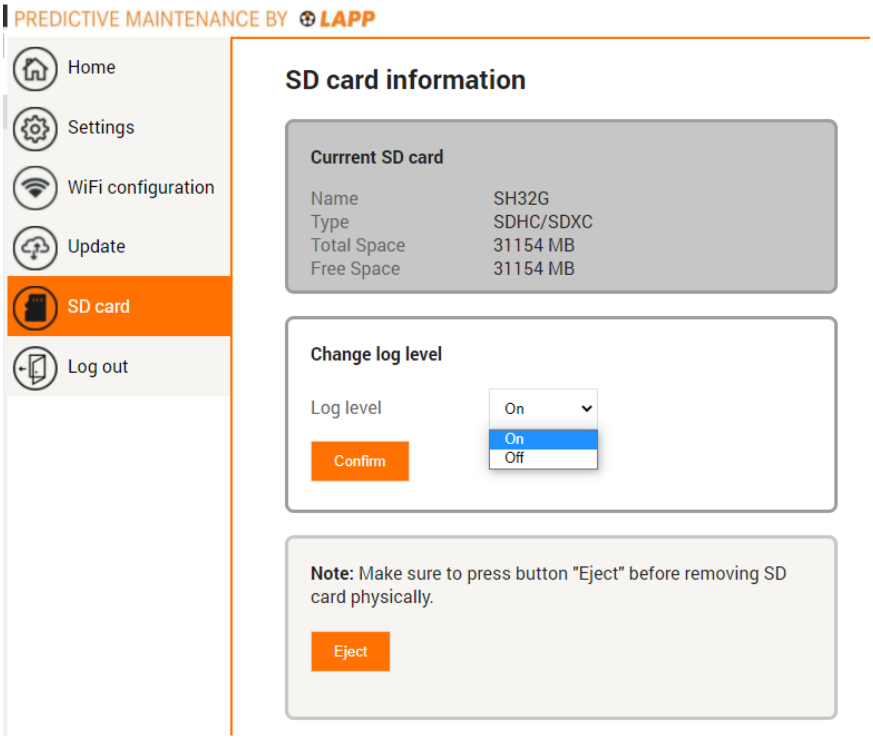

Cable Status = 100%, D = 0.99


Cable Status = 50%, D = 0.37


Cable Status ≤ 21%, D = 0.01

4.5 Using the microSD card

A microSD card can be inserted into the left side of the housing. This card can record data for the diagnosis of the unit and the measurement. The microSD card is not necessary for normal operation of the unit! The measurement recordings can be used by the LAPP Support to analyse the unit.



SD card information

Currrent SD card

Name	SH32G
Type	SDHC/SDXC
Total Space	31154 MB
Free Space	31154 MB

Change log level

Log level: On (On / Off)

Note: Make sure to press button "Eject" before removing SD card physically.

If there is an SD card in the unit, the cable readings are automatically stored there.

Logging = off: Only the cable-specific measured values are saved on the card

Logging = on: In addition to the measured values, internal device data is stored (recommended).

When using an SD card, we recommend activating logging in order to have access to more diagnostic data in case of an evaluation.

Requirements regarding the SD card:

File system: FAT32

Max. size: 32 GByte

5 First commissioning ("teach-in")

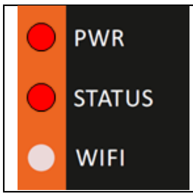
The Ethernet data line to be monitored is connected to the lower DATA socket (GUARD). The upper DATA socket is for the connection to the communication partner. A commercially available Ethernet data line suitable for industrial use can be used here.

After the two DATA sockets have been connected via Ethernet lines and the Ethernet links of the communication connection have been recognised (the other end of each cable is also connected), a **teach-in** must be carried out once for the unit to work correctly.

A correct communication connection between the two communication partners can be recognised by the LEDs of the DATA RJ45 sockets. If the green LED lights up at both RJ45 sockets, the Ethernet connection is established. The flashing yellow LED at the RJ45 sockets indicates active data transmission.

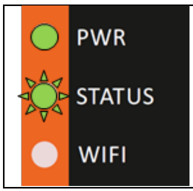
During the following teach-in procedure, the cable connected to DATA GUARD is now calibrated up to the communication partner.

To start the teach-in process, please press the SET button for at least 20s. As soon as the PWR LED and the STATUS LED both light up red simultaneously, release the SET button again.

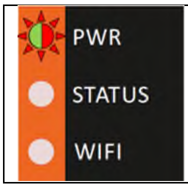
 after **20s**	**Teach-in** PWR and STATUS light up permanently red.

- All measurement data (cable status, teach-in values) are deleted.
- The teach-in is carried out.
- Other settings (network, MQTT, digital outputs) are retained.
- WiFi Access Point remains activated/deactivated according to the initial position.
- The LEDs switch off after releasing the SET button, the selected function is executed.

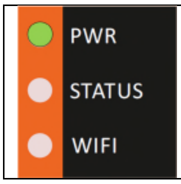
The calibration of the data line is now carried out during operation. This is indicated by a green flashing STATUS LED. During this process, there may be brief interruptions in the data connection at the respective link partners.

	**Teach-in / initialisation** PWR lights up permanently green. STATUS flashes green (approx. 2Hz, duration approx. 1min.).

- Teach-in or initialisation in progress.
- After successful completion, change to operating state Ready for operation.

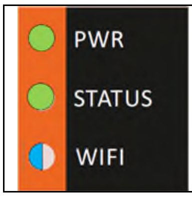
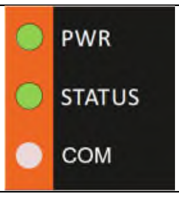
	**Faulty teach-in** PWR flashes alternately red/green (approx. 2Hz, duration unlimited until a factory reset or teach-in is carried out).

- Teach-in could not be executed.
- Check wiring and earthing concept if necessary.
- Then carry out the teach-in again.

	**No teach-in carried out** PWR lights up permanently green.

- No teach-in has been carried out.
- Cable status is neither determined nor output.
- Perform teach-in.

When the teach-in process is complete, the PWR LED and the STATUS LED should light up green continuously.

 	**Ready for operation** PWR and STATUS light up permanently green. WiFi blue, green or alternating according to the operating status.

- ETHERLINE GUARD is in normal operation.
- Monitored line OK.
  Cable condition > set alarm threshold (default = 80%)
- Digital outputs switch depending on configuration (Q1 = NO "low", Q2 = PWM)
- WiFi
  - Blue = Access point active
  - Green = Client active
  - Green flashing (1Hz) = Device is trying to establish a connection to an access point
  - Blue and green alternately (every 3s) = Access point and client active

If an error occurs during the teach-in process, the PWR LED flashes green/red.

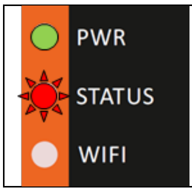
NOTE

The teach-in procedure must be repeated after each cable exchange!

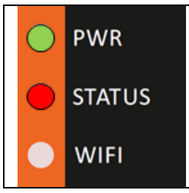
The teach-in values are permanently stored in the unit and are retained even in the event of a power failure or a firmware update (software update).

The ETHERLINE® GUARD is now in measuring and monitoring mode. The status of the cable is indicated via the STATUS LED, the web interface and by the two outputs Q1 & Q2. In addition, the cable status can be sent via MQTT.

If the STATUS LED lights up or flashes red, the measurement has shown that the electrical characteristic values of the cable have deteriorated and the monitoring threshold value has been undercut. Replacement is advisable (soon).

		**Maintenance required** PWR lights up permanently green. STATUS flashes red (approx. 1Hz).

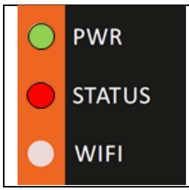
- ETHERLINE GUARD is in normal operation.
- Maintenance of the monitored cable necessary
  Set alarm threshold (default = 80%) > Cable condition > 20%
- Digital outputs switch depending on configuration (Q1 = "high", Q2 = PWM)

		**Line defective** PWR lights up permanently green. STATUS lights up permanently red

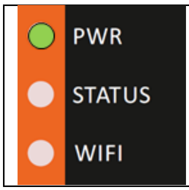
- ETHERLINE GUARD is in normal operation.
- Monitored line is defective: Cable condition < 20% or
- Monitored line is not connected.
- Digital outputs switch as follows (Q1 = "high", Q2 = PWM, D = 0.01)

NOTE

If the ETHERLINE® GUARD is restarted after a successful teach-in or if there was a power failure, the measurement requires a few seconds until a measured value is available again.
This is indicated after the restart by a green flashing STATUS LED (initialisation).

	after **10s**	**Soft reset** PWR lights up permanently green. STATUS lights up permanently red

- The unit is restarted and the data traffic is briefly interrupted.
- All parameters are retained.
- WiFi Access point remains activated/deactivated according to the initial position.
- The LEDs go out after releasing the set button, the selected function is executed.

	after **25s**	**Demolition** PWR lights up permanently green.

- WiFi access point, soft reset and teach-in are cancelled.
- WiFi Access point remains activated/deactivated according to the initial position.
- The LEDs switch off after releasing the set button, the selected function is executed.

6 Access to the web interface

The web page for displaying the cable status and configuring the ETHERLINE® GUARD can be accessed via the "LAN" interface (PM03T) or via WIFI (PM02TWA).

The ETHERLINE® GUARD website has a default IP address when delivered and after a factory reset. This is printed on the right-hand side of the unit.

For the ETHERLINE® GUARD version "LAN" it is the IP address **192.168.0.32**

For the ETHERLINE® GUARD version "WIFI" it is the IP address **192.168.4.1**

NOTE

For optimal use and display, Lapp recommends using Google Chrome as your browser.

6.1 Access via LAN

Connect the LAN interface of the ETHERLINE® GUARD to your PC via a standard Ethernet cable. The LAN interface supports 10 and 100 Mbit/s. When accessing the website for the first time, set your PC interface to the appropriate subnet, e.g. with the IP address 192.168.0.1 with subnet mask 255.255.255.0 for LAN access.

Open the website in a current browser with https://192.168.0.32.

NOTE

For security reasons, the web interface can only be accessed via a secure HTTPS connection. To reach the website, an exception rule may have to be confirmed in the browser.

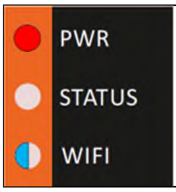
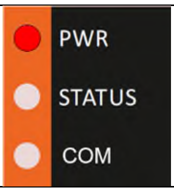
If required, a separate certificate for the connection protection can be stored in the "Settings" menu. Further information on how to handle and set up certificates can be found on the ETHERLINE® GUARD homepage.

6.2 Access via WIFI

The ETHERLINE® GUARD with WiFi activates its own access point (AP) with the SSID name "LAPP_xxxxxxxx" in the factory state. The unique device SSID can be read on the right side panel of the device. The default WiFi password is "12345678".

As soon as you have established the connection with the WLAN network of the ETHERLINE® GUARD, the web interface can be accessed in the browser at https://192.168.4.1.

If the ETHERLINE® GUARD is to be integrated into an existing WLAN, it can be switched to client operation. Information on WiFi configuration can be found in chapter 7.3.

		after **3s**	**WiFi Access point** **(available at PM02TWA)** PWR lights up permanently red. WiFi lights up blue according to the function.

- Deactivation/activation of the WiFi access point depending on the initial situation.
- The LEDs switch off after releasing the set button, the selected function is executed.

6.3 Initial registration

When logging in for the first time, you will be asked to set a password for the default user "admin". The password must be at least 8 characters long.

ATTENTION

Please memorise the password well! For security reasons, there is no way to reset the password without resetting the unit to factory settings.

6.4 Main view "Home“

After logging in, the "Home" web page of the ETHERLINE® GUARD always opens. The main view contains information about the device and cable status.

The menu contains further functions for configuration, firmware update, etc.

With the last menu item "Log out", access to the web interface can be blocked again.

Details of the menu item "Home" show the status and information of the ETHERLINE® GUARD.

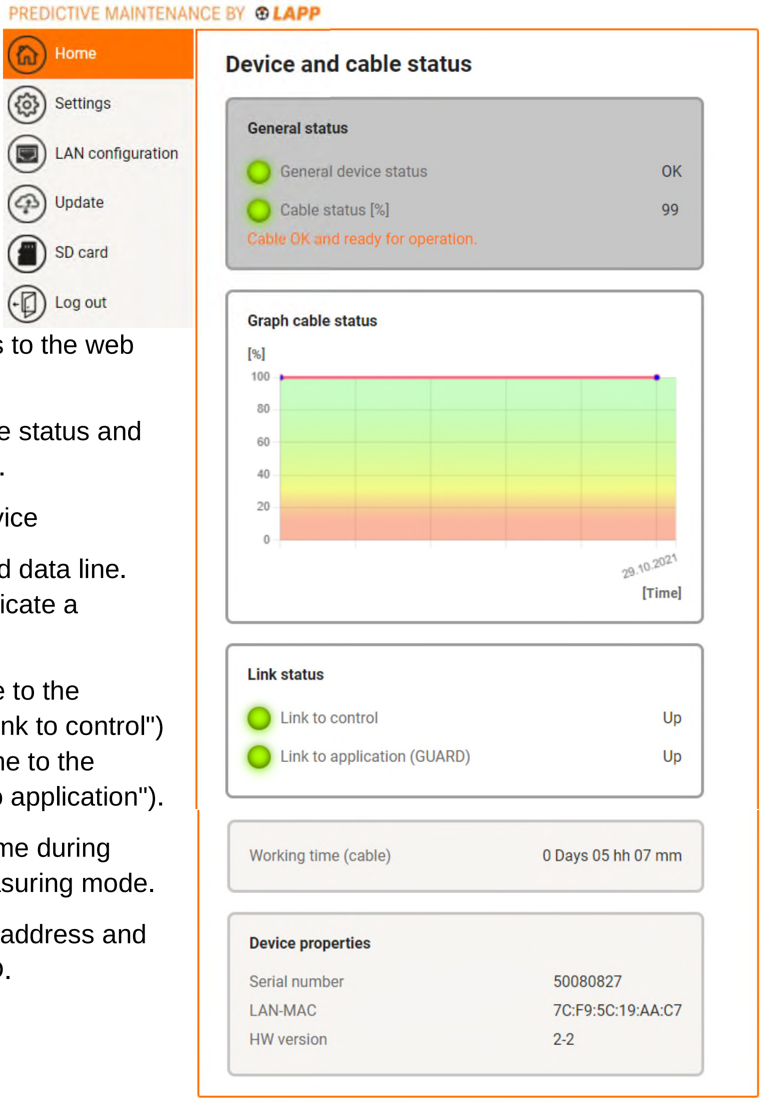
General device status: Status of the device

Cable status [%]: Status of the monitored data line. 100% is the initial state. Lower values indicate a deterioration of the cable status.

Link status: Connection status of the line to the network/controller (upper DATA RJ45, "Link to control") and connection status of the monitored line to the application (GUARD DATA RJ45, "Link to application").

Working time (cable): The cumulative time during which the monitored data line was in measuring mode.

Device properties: Serial number, MAC address and HW version of the ETHERLINE® GUARD.



Device and cable status

General status

● General device status	OK
● Cable status [%]	99

Cable OK and ready for operation.

Graph cable status

Link status

● Link to control	Up
● Link to application (GUARD)	Up

Working time (cable) 0 Days 05 hh 07 mm

Device properties

Serial number	50080827
LAN-MAC	7C:F9:5C:19:AA:C7
HW version	2-2

NOTE

Please check the product's website to see if there is a newer firmware version available. The firmware update is described in chapter 9. Link to firmware: https://www.lappkabel.de/etherlineguard

7 Configuration

7.1 Basic configuration "Settings“

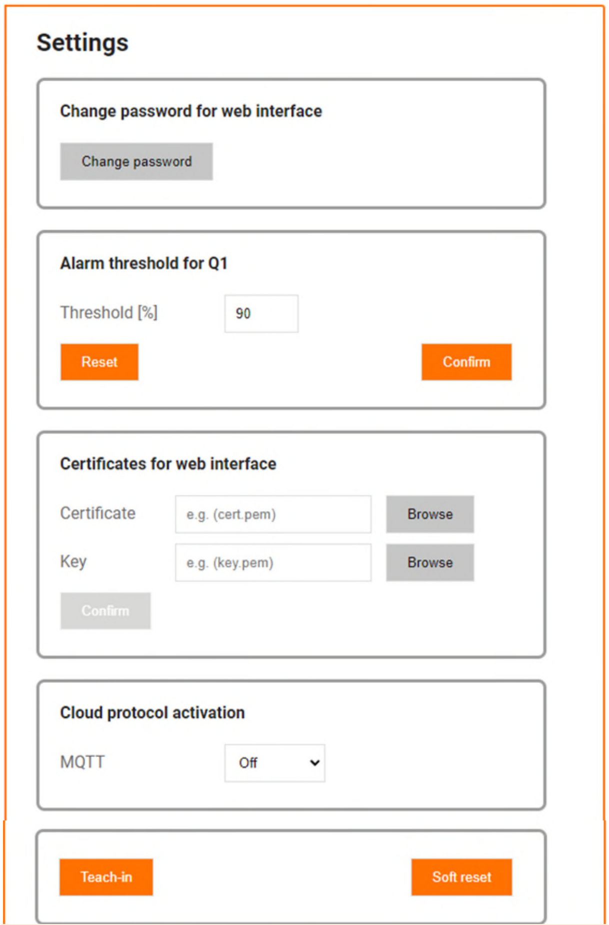
The basic settings can be made in the "Settings" menu.

With the button "**Change password**" the password of the standard user "admin" can be changed.

With "**Alarm threshold for Q1**", the "cable status" limit value for activating output Q1 can be set. If the "cable status" reaches or falls below the value set here, output Q1 is activated permanently.

The ETHERLINE® GUARD website is transmitted to the browser in an SSL-secured manner. In the factory state, an internal certificate is used for this purpose. This cannot be authenticated by the browser, the confirmation of the identity of the device is not possible for the browser. To enable this, the ETHERLINE® GUARD can be provided with a **certificate** and an associated public key suitable for the network in which it is used.

The MQTT Publisher can be activated under "**Cloud protocol activation**". For more information on this, please refer to the chapter 8.



Settings

Change password for web interface

Alarm threshold for Q1

Threshold [%]: 90

Certificates for web interface

Certificate: e.g. (cert.pem)

Key: e.g. (key.pem)

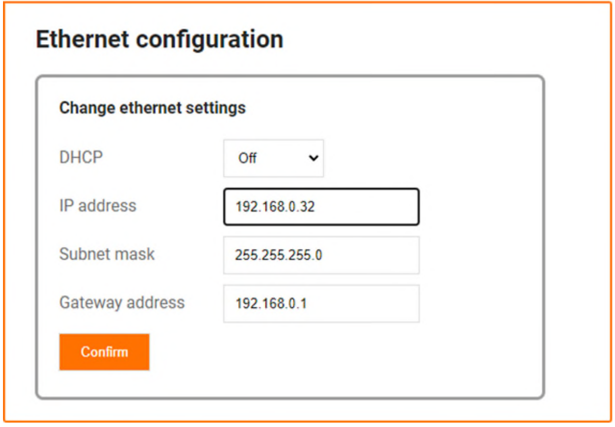
Cloud protocol activation

MQTT: Off

7.2 Ethernet configuration (LAN)

In the "Ethernet Configuration" dialogue you can set the LAN IP address, the subnet mask and the gateway to suit your network.

If a DHCP server is available in your network for assigning the IP address, you can use "DHCP: On" to set that the ETHERLINE® GUARD is assigned the IP address from this server.



Ethernet configuration

Change ethernet settings

DHCP: Off

IP address: 192.168.0.32

Subnet mask: 255.255.255.0

Gateway address: 192.168.0.1

7.3 WiFi configuration

The ETHERLINE® GUARD works as an access point (AP) in the factory setting. The first access therefore takes place via direct access, e.g. with a mobile phone or tablet. The SSID name ("LAPP_xxxxxxxx") can be read on the right side of the device. The default WiFi password is "12345678".

As soon as you have established the connection to the WLAN network of the ETHERLINE® GUARD, the web interface can be accessed in the browser at https://192.168.4.1.

For security reasons, the web interface can only be accessed via a secure HTTPS connection. To reach the website, an exception rule may have to be confirmed in the browser.

In the WiFi configuration, the WiFi operating mode can be changed (see next chapter) and the SSID name of the access point can be adjusted.

Das verknüpfte Bild kann nicht angezeigt werden. Möglicherweise wurde die Datei verschoben, umbenannt oder gelöscht. Stellen Sie sicher, dass die Verknüpfung auf die korrekte Datei und den korrekten Speicherort zeigt.

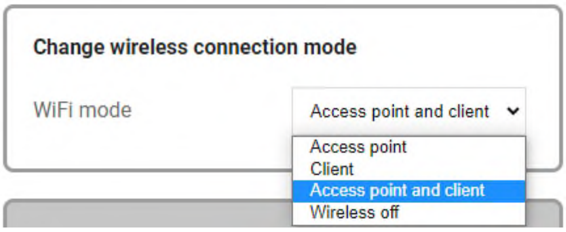
ATTENTION

If the ETHERLINE® GUARD is still to be accessible as an AP, the SSID and the WLAN password should be changed for security reasons.

7.3.1 Switch WiFi operating mode

To integrate the ETHERLINE® GUARD into an existing WLAN network (client operation), change the "**WiFi mode**" in the WiFi configuration under "**Change wireless connection mode"** accordingly.

It is possible to switch to client mode or to have both operating modes (access point and client) active. If both operating modes are active, the ETHERLINE® GUARD can be accessed both via direct access, e.g. from a tablet, and via the access point of the company network.



Change wireless connection mode

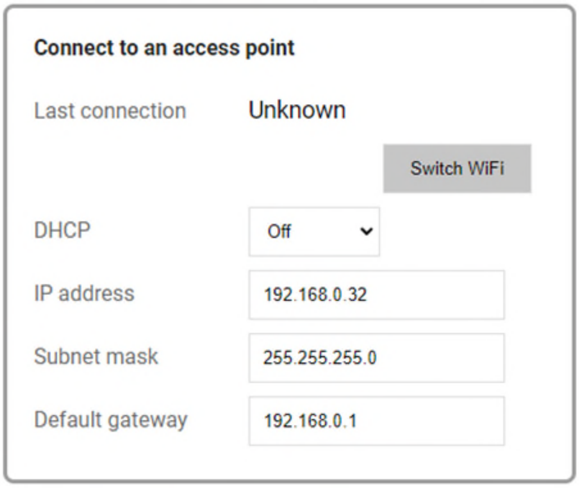
WiFi mode: Access point and client

In client mode, the ETHERLINE® GUARD must still be told which WiFi network or access point it should connect to and which IP settings it should use in the WiFi network.

These settings can be made in the section "**Connect to an access point**".

The desired **WiFi** network can be selected with the "**Switch WiFi**" button.

The selection of the WiFi network is stored voltage-proof in the ETHERLINE® GUARD.



Connect to an access point

Last connection: Unknown

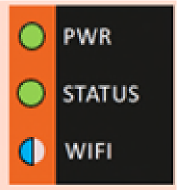
DHCP: Off

IP address: 192.168.0.32

Subnet mask: 255.255.255.0

Default gateway: 192.168.0.1

7.3.2 Functions of the WiFi LED



Blue = Access point operation is active

Green = Client operation is active

Green flashing (1Hz) = Device is trying to establish a connection to an access point

Blue and green alternately (every 3s) = access point and client operation active

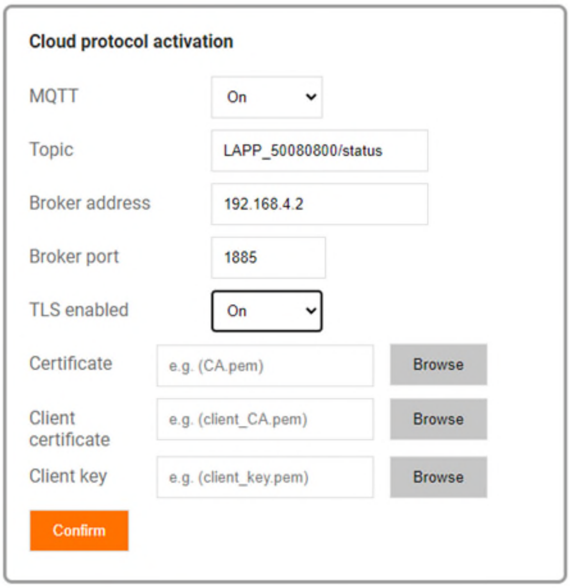
8 Sending the cable status via MQTT

The built-in MQTT Publisher can be activated in the "**Settings"** menu under "**Cloud protocol activation".** The MQTT Publisher regularly sends the "cable status" as an MQTT message to an MQTT broker, which can be located in the local network or in the cloud.

An MQTT message always consists of a name ("Topic") and the content ("Payload").

The name of the message can be freely chosen in the input field "**Topic**", but should be in a meaningful context. No spaces or special characters are allowed in the topic name.

MQTT messages are always sent to a broker, which then forwards the message to subscribers. The IP address and the port of the broker can be specified in "**Broker address**" and "**Broker port".**



Cloud protocol activation

MQTT	On	
Topic	LAPP_50080800/status	
Broker address	192.168.4.2	
Broker port	1885	
TLS enabled	On	
Certificate	e.g. (CA.pem)	Browse
Client certificate	e.g. (client_CA.pem)	Browse
Client key	e.g. (client_key.pem)	Browse

MQTT also enables TLS (SSL) encryption of the transmission. For this, a certificate for the broker ("**Certificate**") and the certificate ("**Client certificate**") and the public key ("**Client key**") for the client/MQTT publisher must be uploaded.

The structure of the payload sent in the MQTT message is fixed and uses the JSON format:

```
{
        "CableStatus":      99,
        "General":   1,
        "LinkToControl":    1,
        "LinkToApplication":      1,
"uptime":    "49680",
}
```

"`CableStatus`" shows the cable quality from 0 to 100%; if no teach-in has been carried out, this value is 0.

"`General`": Corresponds to "General device status" from the web interface (0 = Not OK / 1 = OK).

"`LinkToControl`": Link status of the upper DATA RJ45 (0 = no link / 1 = link present).

"`LinkToApplication`": Link status of the upper GUARD DATA RJ45 (0 = no link / 1 = link present).

"`Uptime`": Measuring time in seconds for the cable measurement; if no teach-in has been carried out, this value is 0.

9 Firmware update

The firmware of the ETHERLINE® GUARD can be updated very easily via the web interface. You can obtain the firmware from the LAPP website or from LAPP Support.

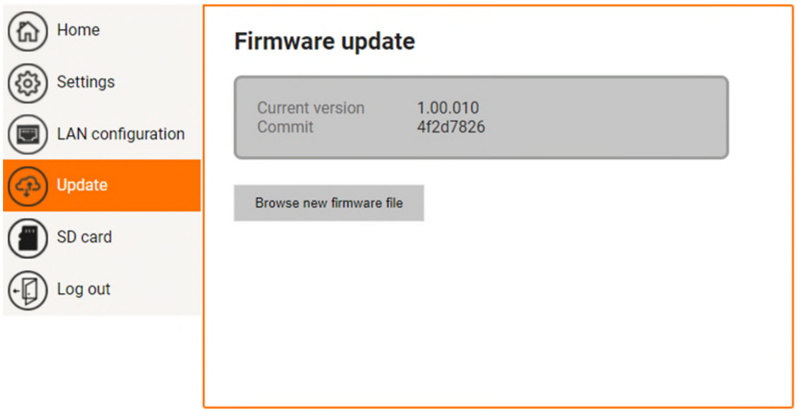
Link to the current firmware in zip archive sub folder

Place the firmware file on your PC.

On the ETHERLINE® GUARD website, select the menu item "Update".

The current firmware version is displayed on the firmware update web page.

With "**Browse new firmware file**" the firmware stored on the PC can be selected for update.



Firmware update

Current version 1.00.010
Commit 4f2d7826

The ETHERLINE® GUARD saves the firmware file in its internal memory. After restarting the device , the firmware is checked. If the content is correct, the firmware is used, otherwise the device is restarted with the old firmware.

ATTENTION

During the update process, the operation of the ETHERLINE® GUARD is interrupted.

The data transmission between the two DATA connections is interrupted during the update.

Do not switch off the unit during the update process! Switching off the power supply can destroy the unit.

All settings, the teach-in values and the current measurement of the cable are not changed or influenced by the firmware update.

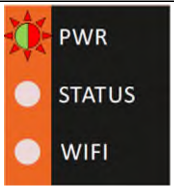
10 Reset to factory setting

Resetting the ETHERLINE® GUARD to factory settings can be done with the "SET" button when the unit is switched on.

When the ETHERLINE® GUARD is reset, the configuration is irretrievably deleted and the IP and WiFi settings are reset to the factory settings. The firmware remains up to date.

To activate a factory reset, disconnect the ETHERLINE® GUARD from the power supply. Now press and hold the SET button and switch the power supply back on. After 8 seconds, the PWR LED flashes alternately red/green. Now release the SET button.

The factory reset is now carried out and the ETHERLINE® GUARD is restarted.

 Disconnect the appliance from the mains SET while holding down the SET button and energising the appliance after **8s**	**Factory reset** PWR flashes alternately red/green (approx. 1Hz, duration approx. 5s)

- Reset to factory settings.
- All measurement data and settings are deleted.
- The LEDs switch off after releasing the set button, the selected function is executed.
- After termination of the function Factory reset, there is an automatic change to the operating state, no teach-in will be performed.

NOTE

After a factory reset, a new teach-in of the cable is necessary, see chapter 5 - First commissioning ("teach-in").

11 FAQ

What is ETHERLINE® GUARD?

ETHERLINE® GUARD is a stationary monitoring device that evaluates the current status of a data line and indicates it as a percentage. This is based on data determined from the physical properties of the data transmission.

What exactly is the determined "cable condition"?

The real-time display of the cable condition makes it possible to recognise the wear limit of a cable and to plan the optimal replacement time in advance. It is a value for the performance condition of the cable determined from several measured variables. This is indicated in 100% to 20%; below 20%, reliable conclusions about the functionality of the cable are no longer possible.

How does the measurement of the condition of the pipe work?

The output of the "cable status" is based on an algorithm which collects, converts and continuously evaluates measured values from various physical transmission parameters as raw values. The raw values consist, for example, of protocol-related transmission parameters and/or a quality indicator, which can be calculated from a statistic of the level values.

The "user data" (data transmission) are neither influenced nor evaluated. If a teach-in is carried out, the line is calibrated, and limit values are set according to the parameters. If these limit values are violated during operation, correction values flow into the algorithm.

It is important that the algorithm includes historical values. This leads to the following consequence: If a line is subjected to such mechanical stress (far above the specifications) that it cannot physically "age", the "prediction" may be delayed. Example: if the data cable is cut with a side cutter, the cable "ages" abruptly; logically, no "prediction" can take place in advance.

What exactly does the "cable status" say?

The "cable status" is a quality value of the transmission properties of the data line on the GUARD DATA socket including the connectors. The classification of the areas is based on the model of a traffic light: Green area = cable / transmission properties are OK. Yellow area = maintenance/replacement required. Red area = line defective.

How do customers benefit from using ETHERLINE® GUARD?

In highly dynamic, demanding movements with high speeds and strong torsion, it is advantageous and cost-saving if the connection systems are monitored to avoid unforeseen downtimes and thus an impairment of productivity. ETHERLINE® GUARD determines the condition of a data line and indicates the performance in percent. If the performance falls below a certain value, the device sounds an alarm and the line must be checked or replaced if necessary.

What can ETHERLINE® GUARD do?

ETHERLINE® GUARD determines the current performance of a data line from various measured variables and indicates this as a percentage. The scope of analysis of ETHERLINE® GUARD is deliberately reduced and monitors a data line and indicates its functionality. This makes it possible to better plan maintenance work.

For which industry is ETHERLINE® GUARD suitable?

ETHERLINE® GUARD can be used wherever data cables are used. Especially in moving applications with high speeds and strong torsion. Such applications are often found in (intra-)logistics, the automotive sector and medical technology. In principle, however, it is suitable for a wide range of industries.

Where is ETHERLINE® GUARD used?

ETHERLINE® GUARD is particularly suitable for data cables that are constantly exposed to "stress", such as

- Movements with high speeds and accelerations
- Changing movement sequences
- Rotations with axially very high angles of twist
- fast cycle times
- small bending radii

The monitored data line is also used in critical processes where high to extremely high downtime costs or even personal injury would occur in
the event of a shutdown.

ETHERLINE® GUARD is suitable

- for use in Ethernet-based networks in automation technology.
- for monitoring data lines in dynamic applications.
- for EtherCAT, EtherNET/IP, PROFINET and many other Ethernet-based applications.
- for use in the control cabinet

Can cables from market companions also be monitored? / Is ETHERLINE® GUARD also interesting for customers with competitor products?

ETHERLINE® GUARD can be operated with inexpensive, non-specific data cables as well as with high-quality, customised data cables.

In principle, the ETHERLINE® GUARD can monitor all data lines of the 100Base-TX transmission standard specified according to IEEE802.3. However, the algorithm for evaluating the cable condition is tested and optimised for LAPP cables.

Can ETHERLINE® GUARD qualify cables from competitors?

No, the ETHERLINE® GUARD cannot perform cable qualification by recording standardised measured variables. It also does not recognise whether it is a LAPP cable or a cable of the market competitors.

Can ETHERLINE® GUARD monitor any type of data line?

LAPP recommends ETHERLINE® GUARD especially for data cables according to the 100BASE-TX transmission standard (with 100 Mbit/s) according to IEEE 802.3, but also for EtherCAT, EtherNET/IP and PROFINET applications, such as the ETHERLINE® TORSION Cat. 5 or the ETHERLINE® PN Cat. 5 FD. These cables are often used in drag chains or torsionally stressed cable runs, such as those found in robot arms.

Can ETHERLINE® GUARD be used on a multi-axis kinematic system / robot?

Yes, it should be noted that the ETHERLINE® GUARD is intended for installation in the control cabinet (protection class IP20, not IP67).

Does ETHERLINE® GUARD also work across several plug-in points?

Yes, the ETHERLINE® GUARD can be used with passively linked network components. No active component may be interconnected. It is not possible to draw conclusions about the faulty cable (localisation).

Can ETHERLINE® GUARD only monitor one data line?

Yes, ETHERLINE® GUARD monitors the distance between two active network components (one or more passively linked data lines). Often there are only a few data lines in the dynamically moving part of the system, e.g. in dresspacks of the robots.

How can costs be saved with ETHERLINE® GUARD?

ETHERLINE® GUARD enables the optimisation of maintenance cycles and thus more efficient personnel and resource planning for planned maintenance work. By determining the performance status, ETHERLINE® GUARD contributes to predictive maintenance and increases machine availability with optimised maintenance operations.

What does ETHERLINE® GUARD cost?

ETHERLINE® GUARD has a low entry price compared to other competitive monitoring solutions, providing interested parties with a quick and easy solution to monitor a data line.

How high is the cost saving by using ETHERLINE® GUARD?

This depends on, for example, the previous maintenance cycles, the size of the machine park, the number of critical mating points, as well as the level of expected costs in the event of a production stoppage, and much more. It also depends on the respective scenario in which the customer operates, the goods produced as well as their critical failure prognosis and many other factors. By using predictive maintenance solutions, maintenance operations can be optimised and thus costs can be reduced by using fewer personnel resources. In addition, planned downtimes can avoid unforeseen machine failures and thus downtime costs.

Does the ETHERLINE GUARD influence the data transmission?

The Ethernet transmission is not affected in any way. However, the measuring electronics delay the data transmission on a physical level by 735 ns (delay at 100 Mbit/s).

What is the maximum length of the line to be monitored?

The ETHERLIN® GUARD supports Ethernet cables up to 100m.

What happens if the ETHERLINE GUARD has no power supply?

Communication via the line to be monitored is interrupted until the power supply is restored.

12 Technical data

12.1 ETHERLINE GUARD with LAN connection

Article number	21700150
Name	ETHERLINE® GUARD PM03T
Dimensions (D x W x H)	35 x 48.5 x 75.5 mm (without power supply connector); 43.5 x 48.5 x 75.5 mm (with power supply connector)
Weight	approx. 110 g
LAN interface ("LAN")	
Number	1
Type	10 Base-T/100 Base-TX
Connection	RJ45 jack
Transmission rate	10/100 Mbit/s
Protocols	HTTPS, MQTT V3.1.1
Test interfaces ("DATA")	
Number	2
Type	100 Base-TX
Connection	RJ45 sockets
Transmission rate	100 Mbit/s
Delay at 100 Mbit/s	735 ns
Outputs ("Q1, Q2")	
Signal voltage at the output	24 V DC
Number and type of outputs	2 / max. 0.2 A
PWM frequency	24 Hz
PWM duty cycle	0,99 ... 0
Protection against overload and short circuit	Yes
Status display	3 LEDs: Power, Status, COM
Power supply	DC 24 V, 18-30 V DC
Power consumption	max. 75 mA at DC 24 V (without output power of Q1 and Q2)
Power loss	1,92 W
MTBF	10.9 years (according to MIL-HDBK-217F)
Mounting position	Any
Environmental conditions	
Ambient temperature	-40 °C ... +65°C
Transport and storage temperature	-40 °C ... +85°C
Relative humidity	95 % r. h. without condensation
Pollution level	2
Protection class	IP20 according to EN 60529
Protection class	III according to DIN EN 61140

Vibration and shock resistance	DIN EN 60068-2-6:2008-10 "Vibration";
	DIN EN 60068-2-27:2010-02 "Shock";
	DIN EN 60068-2-31:2009-04 "Free fall".

Approvals	CE, UL (in preparation), FCC (in preparation)
RoHS, REACH	Yes

12.2 ETHERLINE GUARD with WIFI connection

Article number	21700151
Name	ETHERLINE® GUARD PM02TWA
Dimensions (D x W x H)	35 x 48.5 x 75.5 mm (without power supply connector); 43.5 x 48.5 x 75.5 mm (with power supply connector)
Weight	approx. 110 g
WLAN interface ("WiFi")	
Number	1
Type	IEEE802.11b/g/n
Connection	SMA Jack, reverse polarity
Recommended antenna	monopole 2.33 dBi
Frequency bands	EU (2.412 GHz - 2.472 GHz, channels 1-11)
Transmitting power	max. 19.22 dBm

Transmission rate	802.11b: max. 11 Mbit/s;
	802.11g: max. 54 Mbit/s;
	802.11n: max. 150 Mbit/s (HT20,MCS0, MCS7)

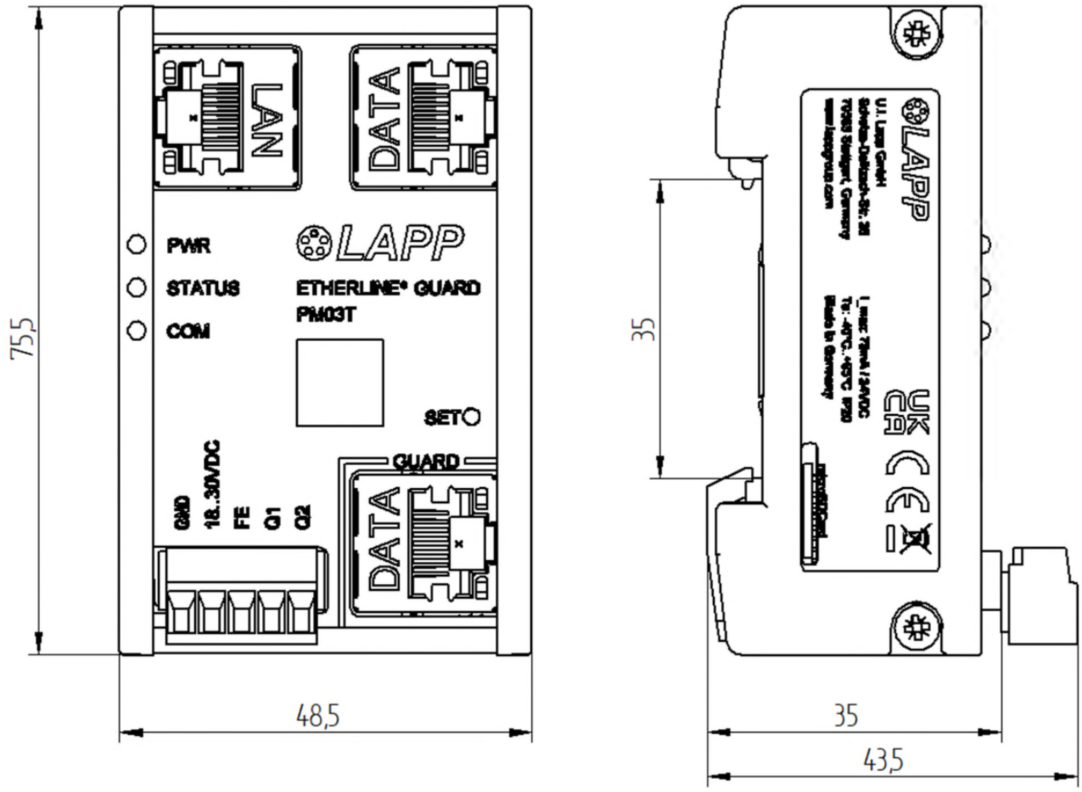
Operating modes	Access Point, Client
Data security	CORRUGATOR 2
Protocols	HTTPS, MQTT V3.1.1
Test interfaces ("DATA")	
Number	2
Type	100-base TX
Connection	RJ45 sockets
Transmission rate	100 Mbit/s
Delay at 100 Mbit/s	735 ns
Outputs ("Q1, Q2")	
Signal voltage at the output	24 V DC
Number and type of outputs	2 / max. 0.2 A
PWM frequency	24 Hz
PWM duty cycle	0,99 ... 0
Protection against overload and short circuit	Yes
Status display	3 LEDs: Power, Status, WIFI".
Power supply	DC 24 V (18−30 V DC, SELV and limited energy circuit)
Power consumption	max. 90 mA at DC 24 V (without output power of Q1 and Q2)
Power loss	2,16 W
MTBF	12.23 years (according to MIL-HDBK-217F)
Mounting position	Any
Environmental conditions	
Ambient temperature	-40 °C ... +65°C
Transport and storage temperature	-40 °C ... +85°C
Relative humidity	95 % r. h. without condensation
Pollution level	2
Protection class	IP20 according to EN 60529
Protection class	III according to DIN EN 61140

Vibration and shock resistance	DIN EN 60068-2-6:2008-10 "Vibration";
	DIN EN 60068-2-27:2010-02 "Shock";
	DIN EN 60068-2-31:2009-04 "Free fall".

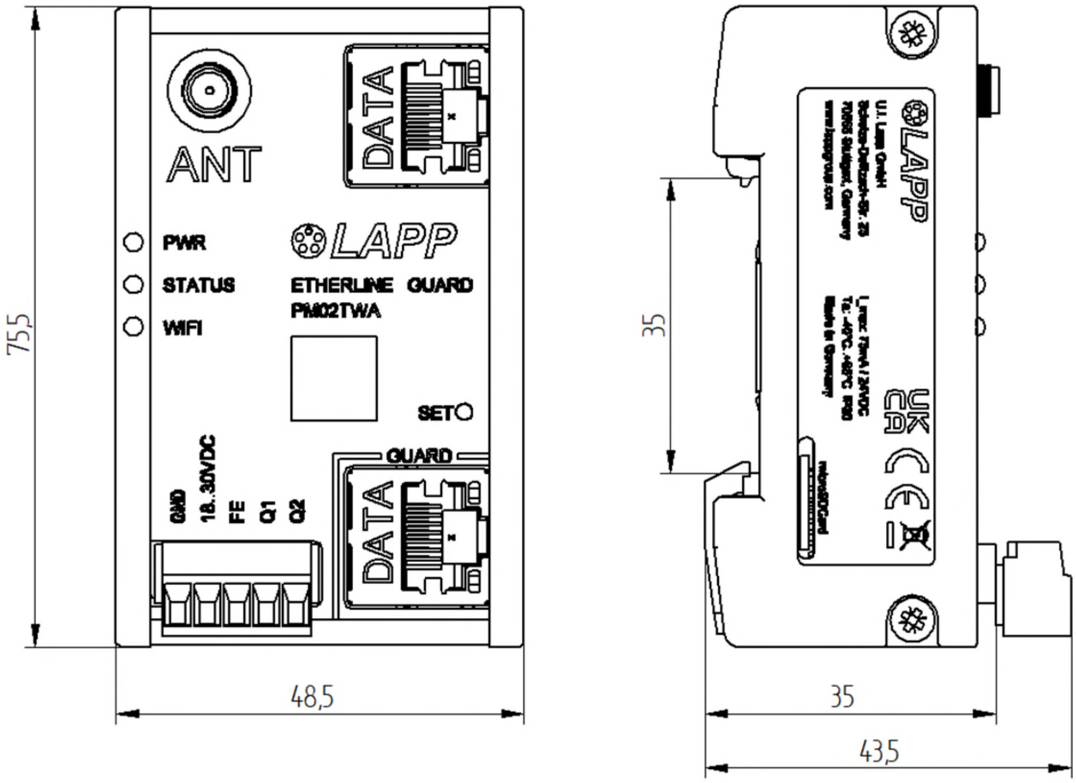
Approvals	CE, UL (in preparation), FCC (in preparation)
RoHS, REACH	Yes

12.3 Dimensioned drawing

12.3.1 PM03T



12.3.2 PM02TWA



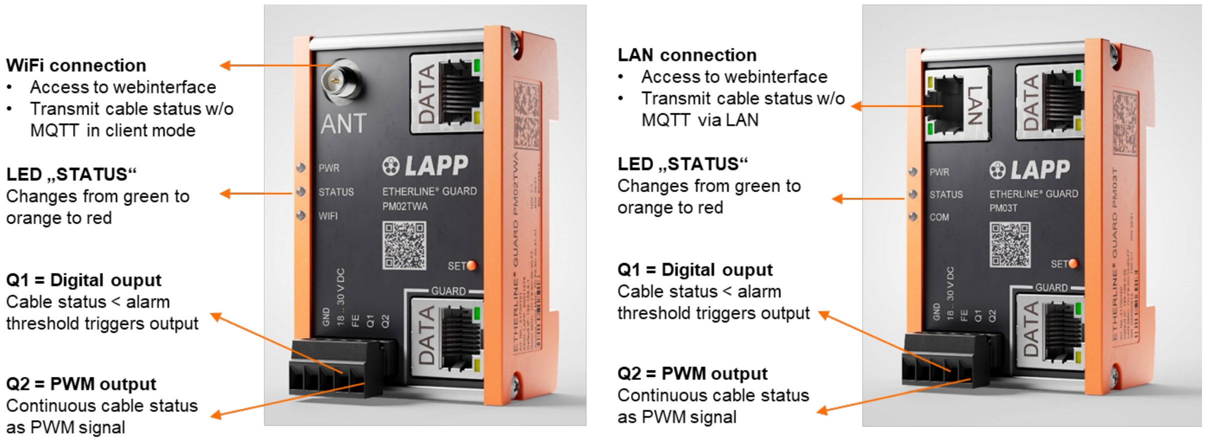
13 Appendix A – Setting up an MQTT connection

ETHERLINE® GUARD monitors the service life of a data cable at risk of failure in an Ethernet-based automation technology network and has built-in MQTT functionality. The MQTT protocol can be used to connect multiple devices to a cloud and monitor different critical applications at once. This chapter covers the MQTT functionality and options of ETHERLINE® GUARD in chapter 13.1 ETHERLINE® GUARD MQTT and a simple test/example setup in chapter 13.2 Example for basic MQTT demonstration. If any further help or instructions are needed, please contact LAPP at www.lappkabel.com/etherlineguard.

13.1 ETHERLINE® GUARD MQTT

ETHERLINE® GUARD can publish various status information including the "cable status" for monitoring the cable deterioration over time via MQTT. This information is matching the one on the web interface. With the MQTT functionality the monitoring of different ETHERLINE® GUARD devices can be automated so that an alarm is triggered as soon as a cable has reached the near end of its lifetime. With reference to this manual, this functionality is an additional output option to

- LED "STATUS" for indicating cable status
- Digital output Q1 where configurable alarm threshold triggers output
- PWM output Q2 for continuous cable status output
- Web interface for graphical display of cable status.



WiFi connection
- Access to webinterface
- Transmit cable status w/o MQTT in client mode

LED „STATUS“
Changes from green to orange to red

Q1 = Digital ouput
Cable status < alarm threshold triggers output

Q2 = PWM output
Continuous cable status as PWM signal

LAN connection
- Access to webinterface
- Transmit cable status w/o MQTT via LAN

LED „STATUS“
Changes from green to orange to red

Q1 = Digital ouput
Cable status < alarm threshold triggers output

Q2 = PWM output
Continuous cable status as PWM signal

Figure 1: ETHERLINE® GUARD Interfaces

MQTT is an OASIS standard messaging protocol for the Internet of Things (IoT). It is designed as an extremely lightweight publish/subscribe messaging transport that is ideal for connecting remote devices with a small code footprint and minimal network bandwidth.[1] A basic understanding of the main functionalities "Connect", "Publish" and "Subscribe" is assumed in the following.

[1] Adapted from https://mqtt.org/

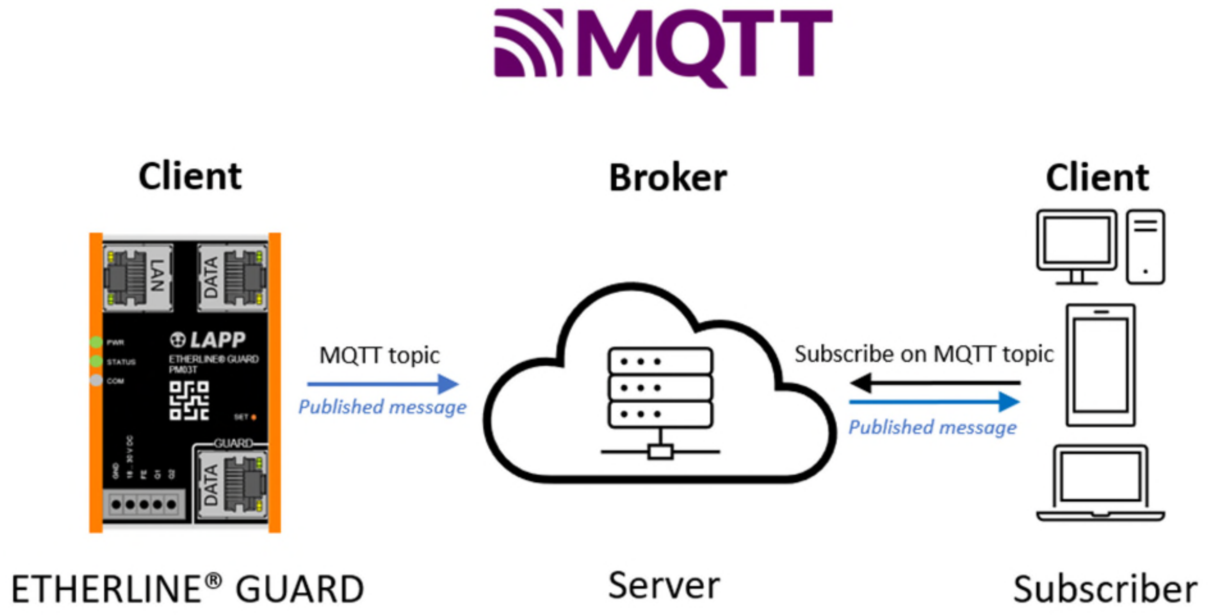


Figure 2: Functional illustration of the MQTT Protocol[2]

13.1.1 Default MQTT Topic

In MQTT, the word topic refers to a string that the broker uses to filter messages for each connected client. For the ETHERLINE® GUARD, the *default MQTT topics* start with “LAPP_” follows by the serial number of the device with an added by the appendix “/status”:

```
LAPP_<Serial_Number>/status
```

The ”`<Serial_Number>`” is replaced by the serial number of the device, which is printed on the right side plate. This *default MQTT topic* is changeable. For more information, please refer to **13.1.4**.

13.1.2 Transmitted variables

Within the ETHERLINE® GUARD application, there are some relevant variables that are part of the published messages. A listing and explanations are given in the following.

[2] https://mqtt.org/

- The ETHERLINE® GUARD will send the following variables on the MQTT topic ***/status*** topic:

Data	Type	Possible Values	Explanation
“CableStatus”	Integer	Between 100 and 0 (decreasing)	Indicates the Cable Status of the monitored data cable
“General”	Boolean as Integer	1: Ok 0: Not Ok	General status of the Device from functionality perspective
“LinkToControl”	Boolean as Integer	1: Link established 0: No Link	Shows if a cable at the DATA port (RJ45) to control is connected
“LinkToApplication”	Boolean as Integer	1: Link established 0: No Link	Shows if a cable at the GUARD DATA port to the application is connected
“Uptime”	String	Timestamp in seconds	Operating time in seconds since last Teach-in

Table 1: Transmitted data with MQTT

13.1.3 Syntax of published messages

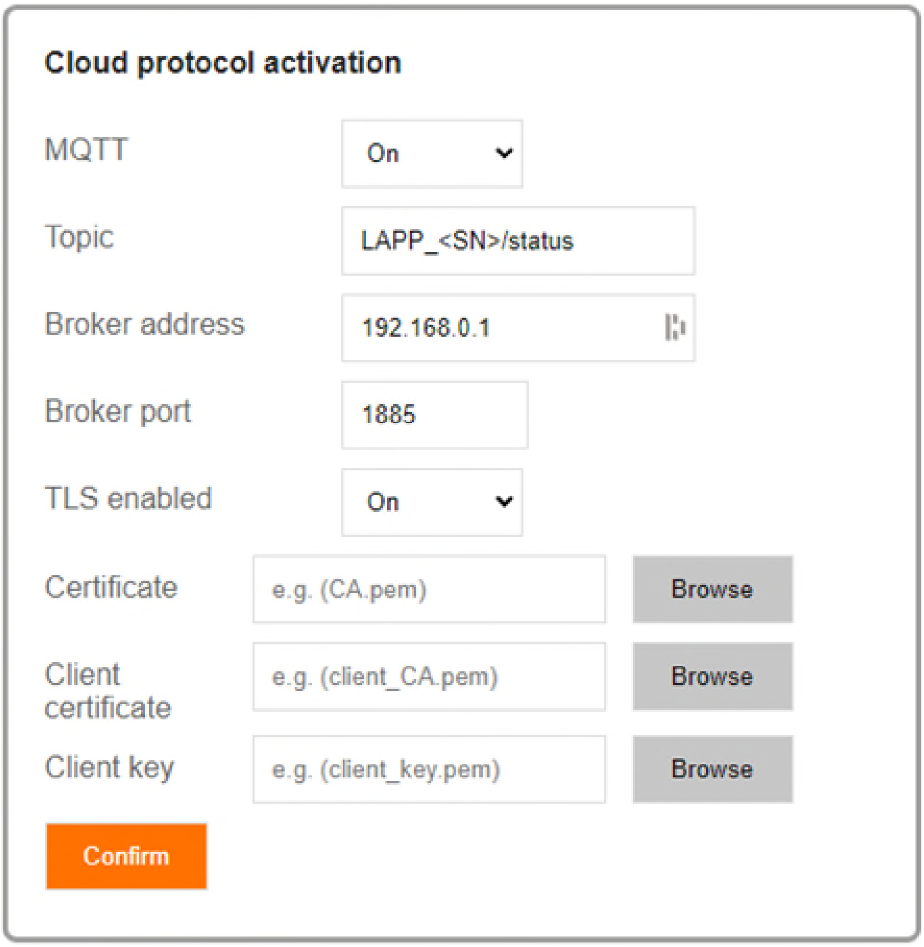
The published messages have a pre-defined syntax for each sent MQTT topic.

- Syntax of the MQTT topic “`/status”:`

```
{
    “CableStatus”:       100,
    “General”:           1,
    “LinkToControl”:     0,
    “LinkToApplication”: 1,
    “Uptime”:            “1234”
}
```

13.1.4 Adjustment of the MQTT settings via the web interface – available MQTT Settings

The available setting parameters for a transmission via MQTT can be found in the web interface under *Menu -> Settings -> Cloud activation protocol*:



Cloud protocol activation

MQTT	On
Topic	LAPP_<SN>/status
Broker address	192.168.0.1
Broker port	1885
TLS enabled	On
Certificate	e.g. (CA.pem)
Client certificate	e.g. (client_CA.pem)
Client key	e.g. (client_key.pem)

Figure 3: ETHERLINE® GUARD web interface MQTT settings

- **MQTT:** Use of the protocol can be turned “*On*” and “*Off*”.
- **Topic**: String for defining the topic on which the status message of the device is. (“<SN>” stands for “Serial Number” which is replaced by the serial number of the device. It is printed find it on the right-side plate).
- **Broker address**: IP address of the MQTT broker.
- **Broker port**: Port of broker that is listening for MQTT messages.
- **TLS**: MQTT communication is secured by enabling this option; here certificates which have to be used by the broker and ETHERLINE® GUARD as a client are imported.

  More information can be found in the chapter about setting up an SSL connection.

13.2 Example for basic MQTT demonstration

In this chapter a basic MQTT setup for ETHERLINE® GUARD and an example setup of an MQTT Broker with the open-source software Mosquitto is presented.

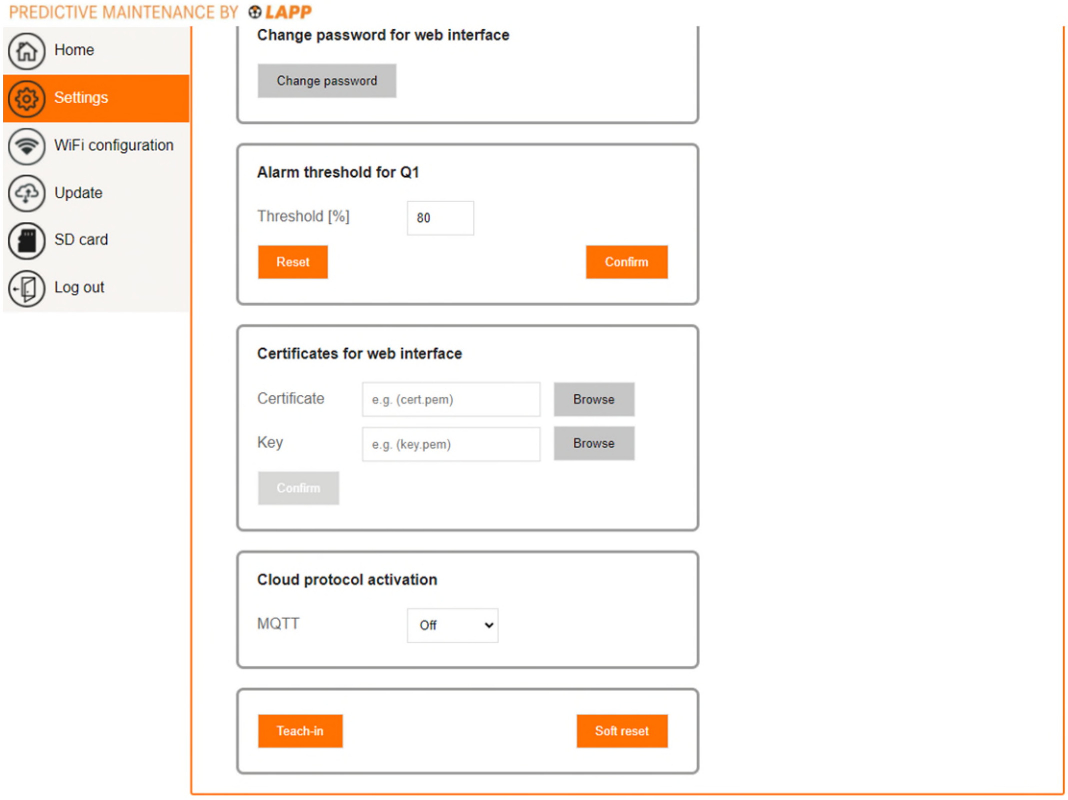
Remark: Mosquitto is listed here as an example and representative of several available MQTT broker software; there is no compelling need to use Mosquitto in combination with ETHERLINE® GUARD.

The described procedure can be used as first introduction into MQTT or for demonstration purposes. For a secure deployment TLS should be enabled, which is not covered in chapter 14.

13.2.1 Step 1: Setup of ETHERLINE® GUARD as MQTT client

Connect to web interface of ETHERLINE® GUARD (Note: it doesn't matter if the device runs as an access-point or is in client mode).

After logging in with the respective credentials, please locate the Settings tab (Note: Appearance may vary for mobile version).



Change password for web interface

Alarm threshold for Q1

Threshold [%] 80

Certificates for web interface

Certificate e.g. (cert.pem)

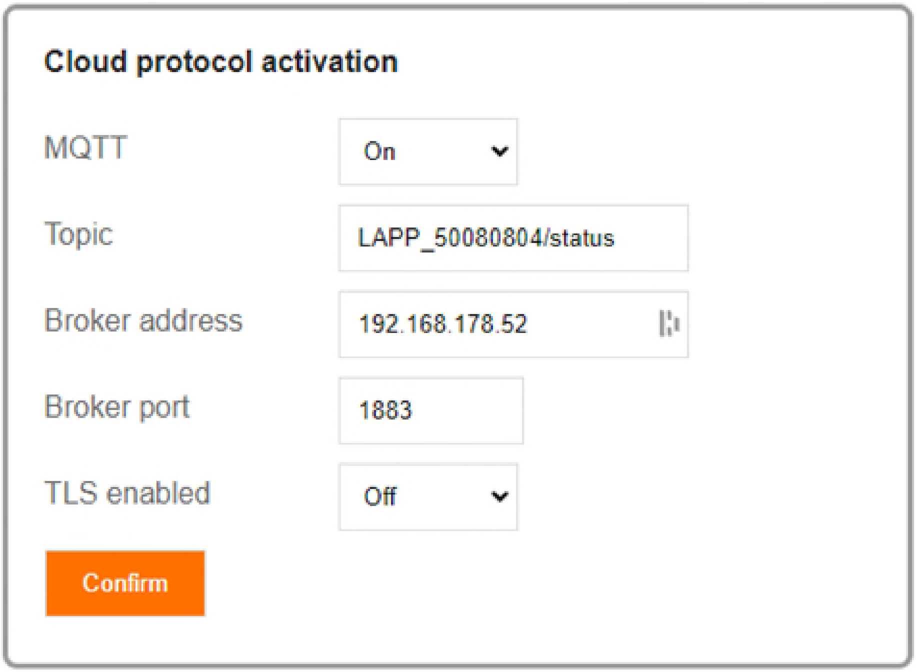
Key e.g. (key.pem)

Cloud protocol activation

MQTT Off

Figure 4: ETHERLINE® GUARD Web interface → Settings tab

Now scroll down to the option “Cloud protocol activation” and select “On” in the drop-down menu. The following setting options will appear:



Cloud protocol activation

MQTT: On

Topic: LAPP_50080804/status

Broker address: 192.168.178.52

Broker port: 1883

TLS enabled: Off

Figure 5: ETHERLINE® GUARD web interface option “Cloud protocol activation”

1. If Broker IP address is already known, it can be inserted here.
   a. If IP of the device on which the MQTT broker will be installed, is unknown, please proceed as follows:

      For Windows:

      i. Open a command prompt (Windows key and type “cmd”).
      ii. Type “ipconfig -all”.
      iii. Find the network to which the ETHERLINE® GUARD is connected to.
      iv. Scroll down until “IPv4” is → This is the correct Broker address.

2. The default port for the MQTT broker is 1883 (in some cases 1885).

Note: These settings are not permanent and can be changed anytime.

Now go ahead and press “*Confirm*”. ETHERLINE® GUARD device is now starting to publish MQTT messages to the configured Broker on the configured topic.

13.2.2 Step 2: Setting up the Mosquitto broker

Mosquitto[3] is an open-source MQTT software, which can be used as a broker and as client. In the following a basic MQTT Broker will be set up to observe and receive the data sent by ETHERLINE® GUARD.

[3] For more information on Mosquitto software, please refer to → here.

13.2.2.1 Windows Installation

1. Download the MQTT Mosquitto software: https://mosquitto.org/download/
2. ETHERLINE® GUARD is communicating over the network, hence a configuration file for Mosquitto broker must be added to open a port with the following contents:

   ```
   listener 1883
   allow_anonymous true
   ```

   The „`listener`“ defines the Broker’s port which has to match the settings in the web interface of the device.
   The “`allow_anonymous`” option configures the MQTT Broker to allow all connections
   Note: This is only a basic setup, please use a secure connection with the TLS option for real deployment.

   a. To create the configuration file, please locate the Mosquitto installation directory (default is at “`C:\program files\mosquitto`”).

   b. Create a new file in this folder, i.e. “`mosquitto_config.conf`” and right click on created file →> Open with editor.

   c. Now paste the contents from above and save the file

   ```
   listener 1883
   allow_anonymous true
   ```

3. The Mosquitto broker server needs to be restarted, please proceed as follows:

   a. Open a Command prompt (Windows key and type “`cmd`”)

   b. Change directory to Mosquitto installation with command:

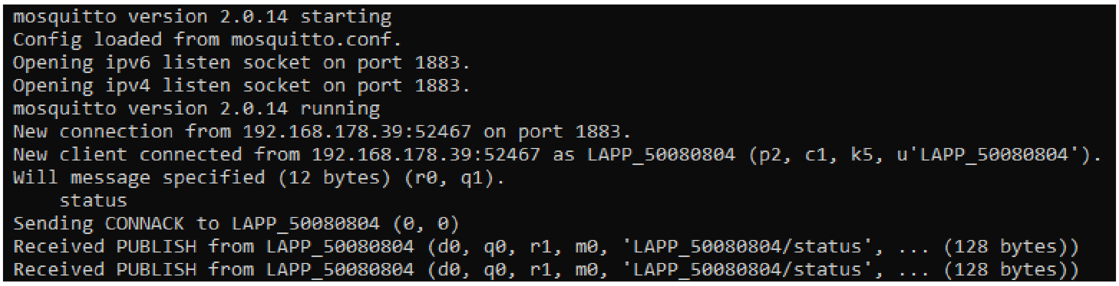
   ```
   cd C:\program files\mosquitto
   ```

   c. Start Mosquitto broker with created configuration file by typing:

   ```
   mosquitto.exe -c mosquitto.conf -v
   ```

   The option ”`-c [configuration file]`” allows for loading your created configuration file. The option “`-v`” will give verbose information of the Brokers activities.

Now the broker will start, and the following should be visible in the command prompt:



```
mosquitto version 2.0.14 starting
Config loaded from mosquitto.conf.
Opening ipv6 listen socket on port 1883.
Opening ipv4 listen socket on port 1883.
mosquitto version 2.0.14 running
New connection from 192.168.178.39:52467 on port 1883.
New client connected from 192.168.178.39:52467 as LAPP_50080804 (p2, c1, k5, u'LAPP_50080804').
Will message specified (12 bytes) (r0, q1).
    status
Sending CONNACK to LAPP_50080804 (0, 0)
Received PUBLISH from LAPP_50080804 (d0, q0, r1, m0, 'LAPP_50080804/status', ... (128 bytes))
Received PUBLISH from LAPP_50080804 (d0, q0, r1, m0, 'LAPP_50080804/status', ... (128 bytes))
```

Figure 6: Mosquitto MQTT Broker in command prompt (Windows)

The regular appearing “`Received PUBLISH from LAPP_` …” message indicates, that ETHERLINE® GUARD publishes data constantly.

To view the published messages, a second Moquitto client is set-up. It subscribes to the MQTT topic for that ETHERLINE® GUARD publishes its data:

1. Open a second Command prompt (Windows key and type "`cmd`")
2. Change the directory to the Mosquitto installation with the command:

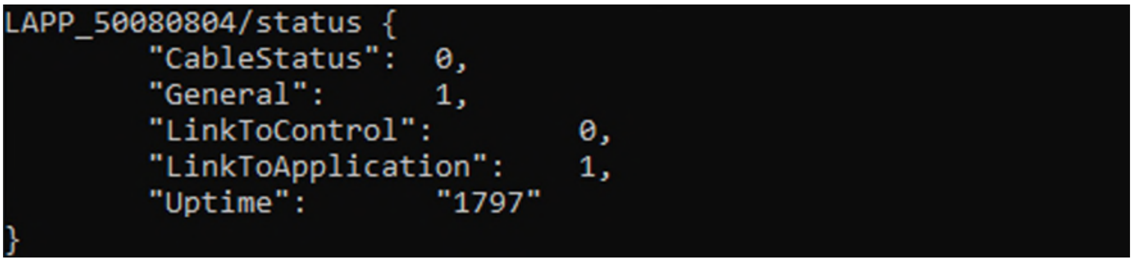
   ```
   cd C:\program files\mosquitto
   ```

3. Start the Mosquitto client which subscribes to a given topic by typing:

   ```
   mosquitto_sub.exe -t "+/status" -h <IP-address> -v
   ```

   The option "`-t [topic]`" defines the topic to which a subscription is needed. The syntax "`+`" before "`/status`" tells the client software to select every device. The "`/status`" then selects the send status from these devices. This syntax is used if serial number of the ETHERLINE® GUARD is unknown or multiple "`/status`" messages from different devices should be received.
   The parameter "-h <IP-address>" specifies the host address on which the broker is running.
   The option "`-v`" sets a verbose mode for more detailed information.
   For more information regarding MQTT subscription possibilities go to https://mosquitto.org/man/mqtt-7.html.

Now the messages published on the topic "`/status`" can be seen from every ETHERLINE® GUARD connected. The command prompt now could look like this:



```
LAPP_50080804/status {
        "CableStatus":  0,
        "General":      1,
        "LinkToControl":        0,
        "LinkToApplication":    1,
        "Uptime":       "1797"
}
```

Figure 7: Mosquitto MQTT client with subscription in command prompt

For Information about the received data go to 13.1.2**.**

13.2.2.2 Linux Installation

For an installation under Linux, please proceed as follows:

1. Download the MQTT Mosquitto software: https://mosquitto.org/download/; Mosquitto is a Debian proper. It`s also included with Raspbian, hence an additional download of Mosquitto is not necessary.

   Be sure to use the latest version, by updating it

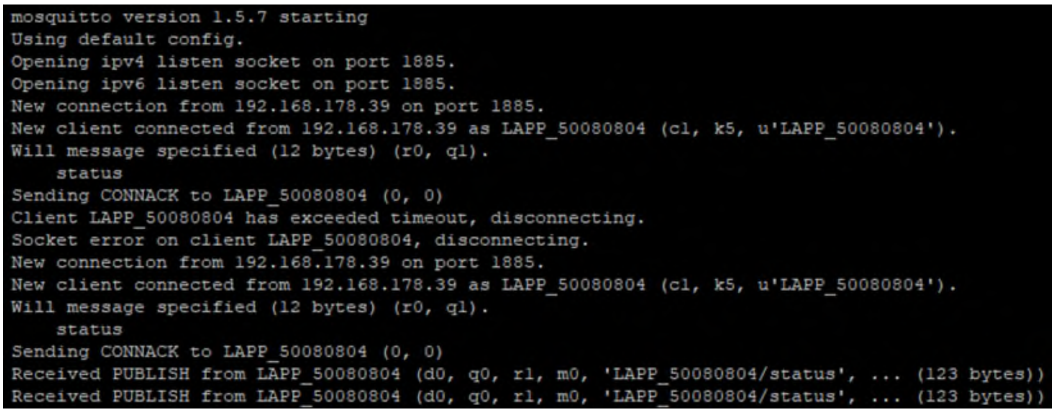
   ```
   sudo apt-get update
   ```

2. The Mosquitto broker can now be started with the command

   ```
   mosquitto -p 1885 -v
   ```

   Note: Port is defined here, because the default for Linux installation is 1883, and a broker might be already running in the background. Furthermore, the settings of ETHERLINE® GUARD in the web interface must match.
   Troubleshooting: *If no messages are received, please check if the port is correct and if the port is open!*
   The option "`-c`" can be added to use configuration file.

Once the broker is started, the following should be visible in the terminal:



```
mosquitto version 1.5.7 starting
Using default config.
Opening ipv4 listen socket on port 1885.
Opening ipv6 listen socket on port 1885.
New connection from 192.168.178.39 on port 1885.
New client connected from 192.168.178.39 as LAPP_50080804 (c1, k5, u'LAPP_50080804').
Will message specified (12 bytes) (r0, q1).
    status
Sending CONNACK to LAPP_50080804 (0, 0)
Client LAPP_50080804 has exceeded timeout, disconnecting.
Socket error on client LAPP_50080804, disconnecting.
New connection from 192.168.178.39 on port 1885.
New client connected from 192.168.178.39 as LAPP_50080804 (c1, k5, u'LAPP_50080804').
Will message specified (12 bytes) (r0, q1).
    status
Sending CONNACK to LAPP_50080804 (0, 0)
Received PUBLISH from LAPP_50080804 (d0, q0, r1, m0, 'LAPP_50080804/status', ... (123 bytes))
Received PUBLISH from LAPP_50080804 (d0, q0, r1, m0, 'LAPP_50080804/status', ... (123 bytes))
```

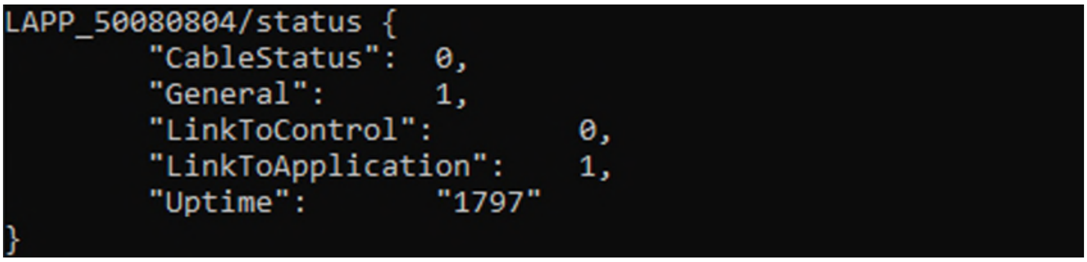
Figure 8: Mosquitto MQTT Broker in terminal (Linux)

To see the sent messages, a subscription to the MQTT topic is done in a new terminal window:

1. Type in the command

```
mosquitto_sub -p 1885 -t “+/status” -v
```

The option ”`-t [topic]`” defines the topic to which a subscription is needed. The syntax “+” before “`/status`” tells the client software to select every device. The “`/status`” then selects the sent status from these devices. This syntax is used if serial number of ETHERLINE® GUARD is unknown or multiple ”`/status`” messages from different devices should be received. The option “`-v`” sets a verbose mode for more detailed information.
For more information regarding MQTT subscription possibilities go to https://mosquitto.org/man/mqtt-7.html.



```
LAPP_50080804/status {
        "CableStatus":  0,
        "General":      1,
        "LinkToControl":        0,
        "LinkToApplication":    1,
        "Uptime":       "1797"
}
```

Figure 9: Mosquitto MQTT Client with subscription in terminal

14 Appendix B - SSL and secure MQTT connection certificates

ETHERLINE® GUARD has a built-in webinterface for device configuration and MQTT functionality. This chapter covers the installation and creation of SSL- for a secure connection to the Webinterface and TLS-certificates for a secure MQTT connection. The certificates for the webinterface must be installed in each web browser in order to establish an https connection to the ETHERLINE® GUARD. Please follow the procedure stated in chapter 14.2. To establish a secure MQTT connection follow the steps in chapter 14.3. If any further help or instructions are needed, please contact LAPP at www.lappkabel.com/etherlineguard.

14.1 Get OpenSSL

For an easy way to create your own SSL certificates you can use the open-source software OpenSSL.

14.1.1 Windows

Under windows the easiest way to get a working OpenSSL is with GIT. If you already use Git you will just need the Git Bash.

Download Git here https://git-scm.com/downloads

After Installation open the Git Bash (Press Windows key and type Git Bash).

14.1.2 Linux

OpenSSL is probably already installed; you can check by typing:

```
➔ openssl version
```

Otherwise install OpenSSL with:

```
➔ sudo apt-get install libssl-dev
```

14.2 Certificate and keys for Web browsers

You will have to use the same certificate and key on the device and in your browser.

To create your certificate, you need a configuration file. Lapp provides you with a template "ssl_config.cnf" for this purpose, which you can adapt to your requirements. For example, the IP address of the Etherline Guard to which the encrypted connection is to be established is defined here. If encrypted connections are to be established to several devices, each individual IP address is listed (see example file).

It’s important to use the same configuration file for every certificate you will create in this chapter.

14.2.1 Create SSL Certificate with OpenSSL

The following commands create the files "server.pem", "serverkey.pem" and "server.p12".

1. Open Git Bash
2. Change directory to the downloaded or self-created configuration file, then type the following commands, which will create three files at the same location your “config.cnf” file is located:

➔
```
openssl req -x509 -nodes -days 7300 -newkey rsa:2048 -keyout serverkey.pem -out server.pem -config ssl_config.cnf
```

➔
```
openssl pkcs12 -export -out server.p12 -in server.pem -inkey serverkey.pem -passin pass:lapp -passout pass:lapp
```

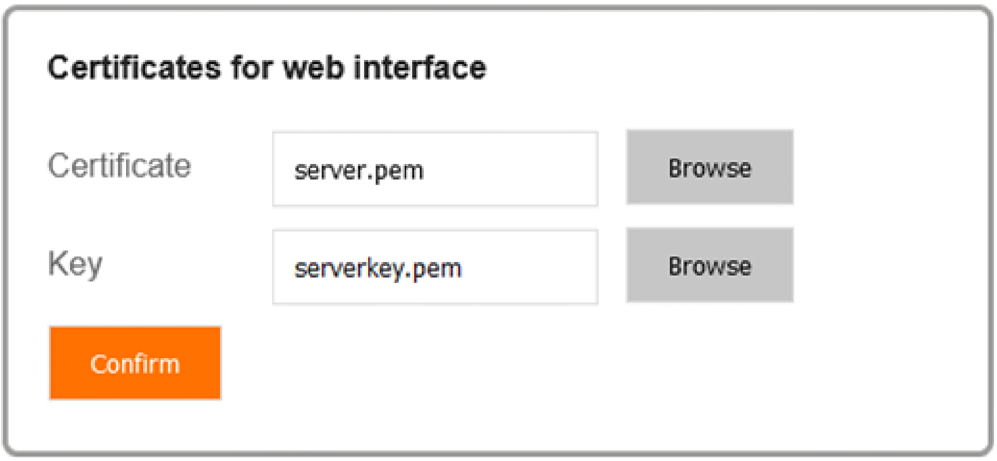
Please enter your own secure password for the password following "-passin pass:" and "-passout pass:". The password "lapp" used here serves only as an example.

14.2.2 Installing SSL Certificates

After you have created your certificates and key, you will have to install them on the ETHERLINE® GUARD and in your preferred browser (you can also install them on your local certificate server).

14.2.2.1 Install on ETHERLINE® GUARD

To install the certificates on the ETHERLINE® GUARD open the Webinterface and navigate to the Settings tab. Under “Certificates for web interface” click browse and select the files as shown in Figure 10. Then click Confirm, the webserver will restart.



Certificates for web interface

Certificate: server.pem

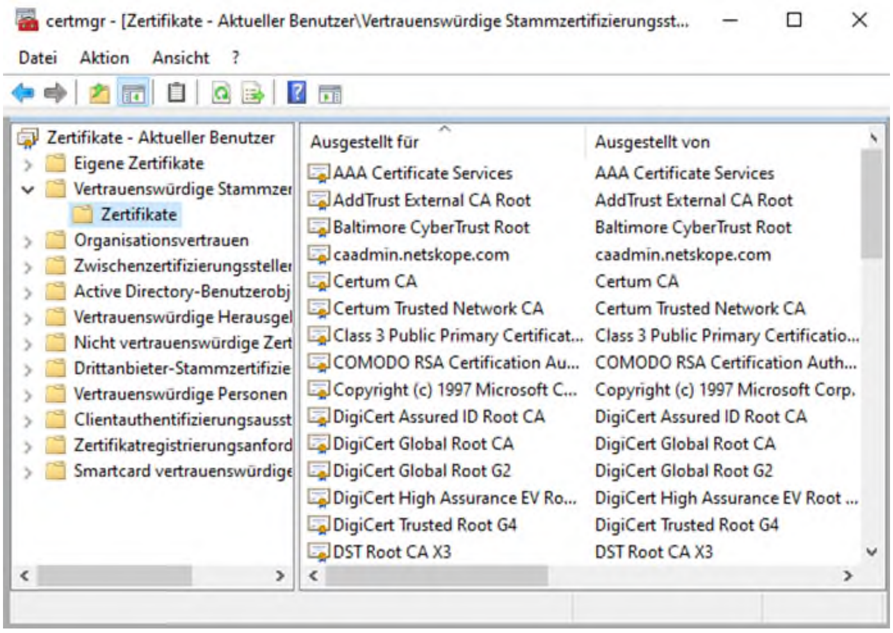
Key: serverkey.pem

Figure 10: Certificate selection ETHERLINE® GUARD

14.2.2.2 Firefox

The installation of the certificates in Firefox is the most difficult of the browsers:

1. Press Win+R and enter “certmgr.msc”, the following window will open. This is the Certification Manager which lists all your digital certificates:



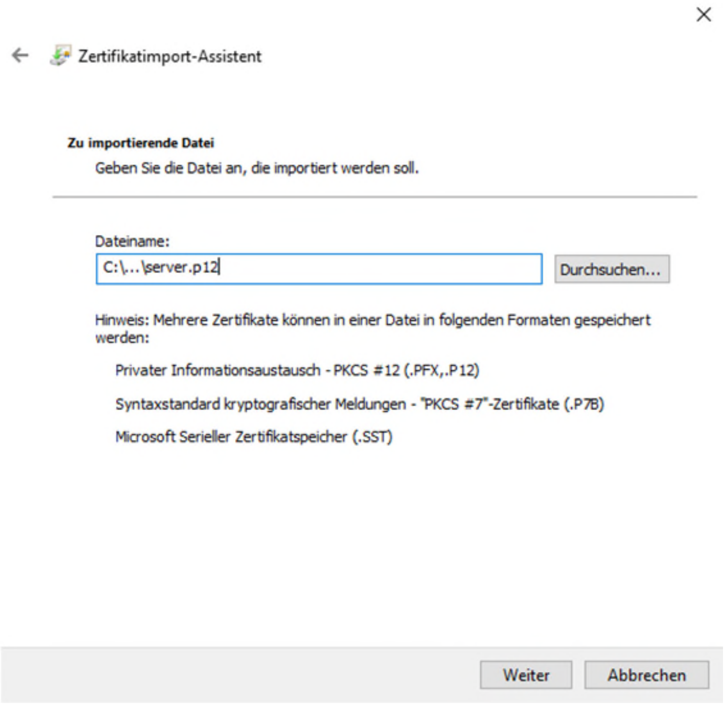
certmgr - [Zertifikate - Aktueller Benutzer\Vertrauenswürdige Stammzertifizierungsst...

- Zertifikate - Aktueller Benutzer
  - Eigene Zertifikate
  - Vertrauenswürdige Stammzer
    - Zertifikate
  - Organisationsvertrauen
  - Zwischenzertifizierungssteller
  - Active Directory-Benutzerobj
  - Vertrauenswürdige Herausgel
  - Nicht vertrauenswürdige Zert
  - Drittanbieter-Stammzertifizie
  - Vertrauenswürdige Personen
  - Clientauthentifizierungsausst
  - Zertifikatregistrierungsanford
  - Smartcard vertrauenswürdige

Ausgestellt für	Ausgestellt von
AAA Certificate Services	AAA Certificate Services
AddTrust External CA Root	AddTrust External CA Root
Baltimore CyberTrust Root	Baltimore CyberTrust Root
caadmin.netskope.com	caadmin.netskope.com
Certum CA	Certum CA
Certum Trusted Network CA	Certum Trusted Network CA
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...
COMODO RSA Certification Au...	COMODO RSA Certification Auth...
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA
DigiCert Global Root CA	DigiCert Global Root CA
DigiCert Global Root G2	DigiCert Global Root G2
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...
DigiCert Trusted Root G4	DigiCert Trusted Root G4
DST Root CA X3	DST Root CA X3

Figure 11: Windows Certification Manager

2. Click Trusted Root Certification Authorities and right-click Certificates to open a context menu.
3. Select All Tasks -> Import on the context menu to open the window shown below.
4. Click next until you can select a file. Then browse to the location where you created the certificates and select “server.p12”.



Zu importierende Datei

Geben Sie die Datei an, die importiert werden soll.

Dateiname:

C:\...\server.p12

Hinweis: Mehrere Zertifikate können in einer Datei in folgenden Formaten gespeichert werden:

Privater Informationsaustausch - PKCS #12 (.PFX,.P12)

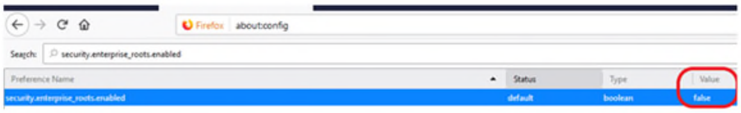
Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)

Microsoft Serieller Zertifikatspeicher (.SST)

Figure 12: Windows certificate import wizard

5. The password for the file was configured in the “ssl_config.cnf”.
6. Then you can press Next -> Finish to wrap up the import wizard. A window will open confirming that “the import was successful.”
7. Now you will have to add a permit to Firefox to trust root authorities:

- Type “about: config” into the Firefox address bar.
- Press the **I accept the risk!** button.
- Search for security.enterprise_roots.enabled.

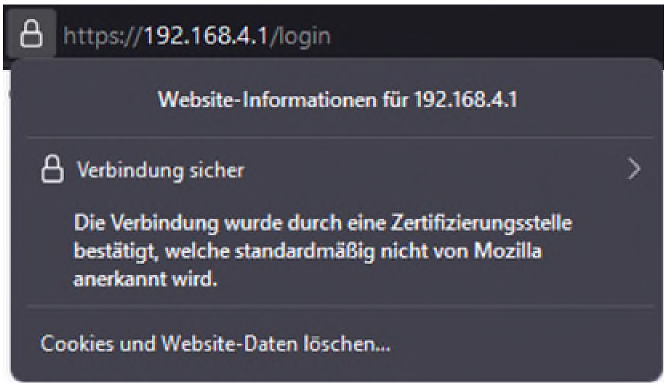


Search: security.enterprise_roots.enabled

Preference Name	Status	Type	Value
security.enterprise_roots.enabled	default	boolean	false

- In the **security.enterprise_roots.enabled** window, look to the right side of the screen. If the value is **False**, double-click on it. The value will get changed to **True**.
- Restart Firefox.

8. After successful installation and a browser restart the connection should be secure:



https://192.168.4.1/login

Website-Informationen für 192.168.4.1

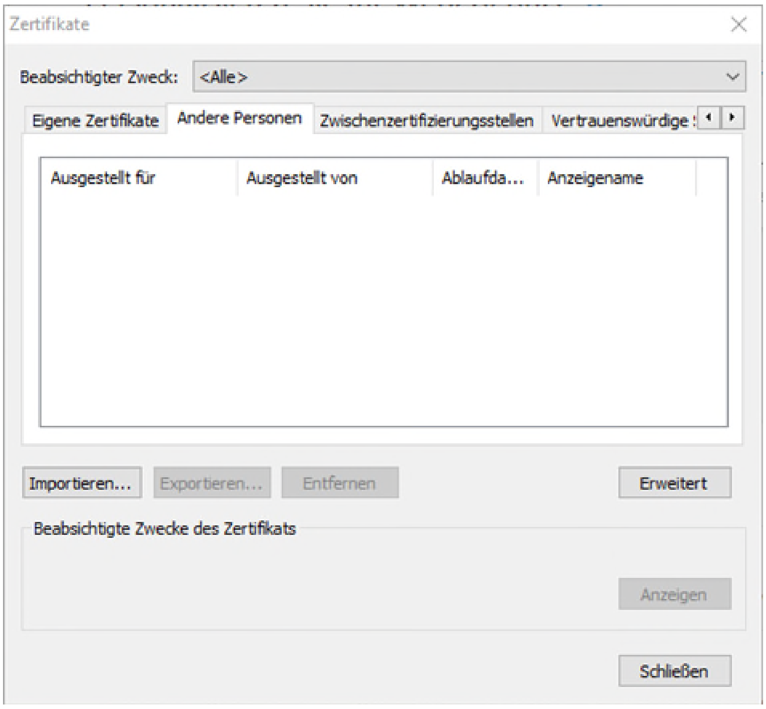
Verbindung sicher

Die Verbindung wurde durch eine Zertifizierungsstelle bestätigt, welche standardmäßig nicht von Mozilla anerkannt wird.

Figure 13: Firefox secure connection

14.2.2.3 Chrome and Edge

1. Open your Browser and navigate to Settings.
   - In Chrome search for “Privacy and Security“
   - In Edge go to “Privacy”
2. Click on Manage Certificates. The following window will open:



Zertifikate

Beabsichtigter Zweck: <Alle>

Figure 14: Chrome and Edge certificate manager

3. Now click on Import and follow the wizard.
4. After selecting “server.p12” you will be asked for a password which was configured in the “ssl_config.cnf”. The default is “lapp”.
5. After wrapping the import wizard restart your browser.

14.3 Certificate and Keys for MQTT

For a secure TLS-MQTT connection you will have to create your own certificates like before if you plan to use other IP addresses for your ETHERLINE® GUARD. For this you will need the “mqtt_ca_config.cnf” and “ssl_config.cnf” files, provided in the download section of the ETHERLINE® GUARD.

14.3.1 Create with OpenSSL

In the following nine files will be created:

- CA certificate -> for broker and client:
  - “ca.pem”, “ca.srl”, “cakey.pem”
- MQTT Server certificate and key -> for broker:
  - “mqttserver.csr”, “mqttserver.pem”, “mqttserverkey.pem”
- MQTT Client certificate and key -> for client:

- o “mqttclient.csr”, ” mqttclient.pem”, “mqttclientkey.pem”

1. First open Git Bash
2. Change directory to the downloaded or self-created configuration file, then type the following commands:

➔
```
openssl req -x509 -nodes -days 7300 -newkey rsa:2048 -keyout cakey.pem -out ca.pem -config mqtt_ca_config.cnf
```

➔
```
openssl genrsa -out mqttserverkey.pem 2048
```

➔
```
openssl req -new -out mqttserver.csr -key mqttserverkey.pem -config ssl_config.cnf
```

➔
```
openssl x509 -req -in mqttserver.csr -CA ca.pem -CAkey cakey.pem -CAcreateserial -out mqttserver.pem -days 7300
```

➔
```
openssl genrsa -out mqttclientkey.pem 2048
```

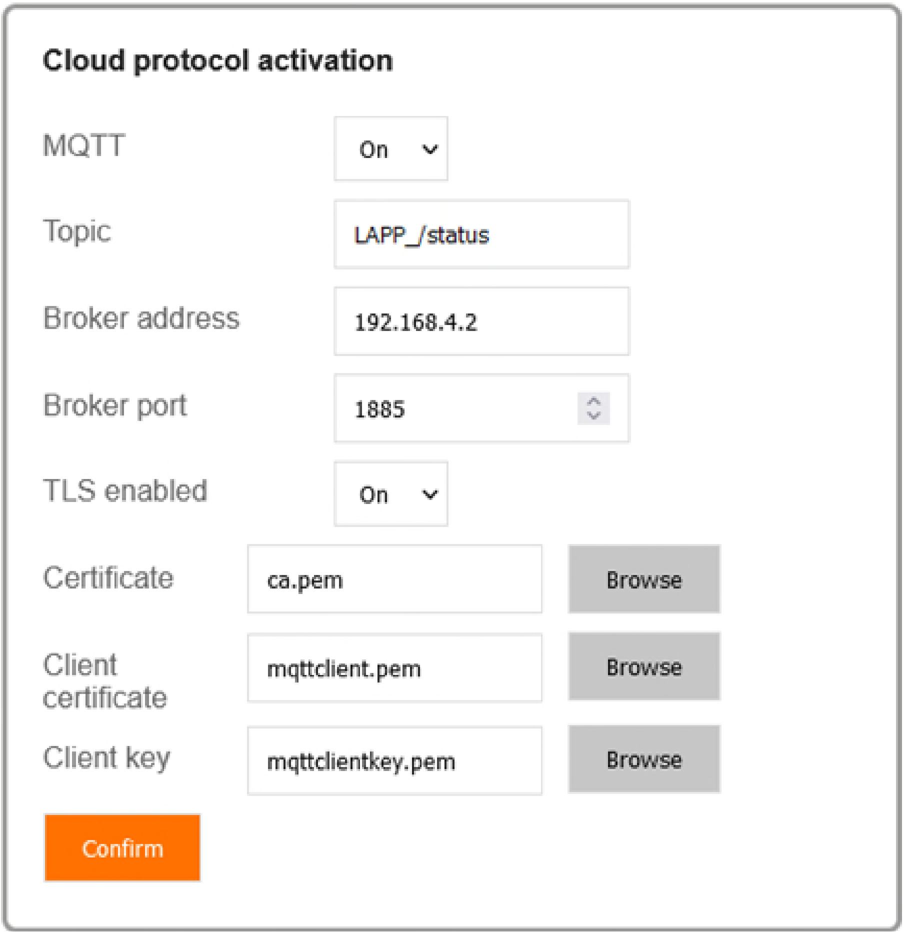
➔
```
openssl req -new -out mqttclient.csr -key mqttclientkey.pem -config ssl_config.cnf
```

➔
```
openssl x509 -req -in mqttclient.csr -CA ca.pem -CAkey cakey.pem -CAcreateserial -out mqttclient.pem -days 7300
```

14.3.2 Installing MQTT Certificates on ETHERLINE® GUARD

From these files you will have to upload the CA certificate “ca.pem” and the MQTT Client certificate and key “mqttclient.pem” and “mqttclientkey.pem”.

1. Open the webinterface of the ETHERLINE® GUARD and navigate to Settings
2. Under the option “Cloud protocol activation” enable TLS. If you want to configure a MQTT Connection first take a look in chapter 13 - Appendix A – Setting up an MQTT connection.
3. Select the files as shown in Figure 15:



Cloud protocol activation

MQTT	On
Topic	LAPP_/status
Broker address	192.168.4.2
Broker port	1885
TLS enabled	On
Certificate	ca.pem
Client certificate	mqttclient.pem
Client key	mqttclientkey.pem

Figure 15: MQTT certificate installation on ETHERLINE® GUARD

4. Click Confirm, “Settings Changed!” will appear.