Your Global Automation Partner

TURCK

TBEN-L...-SE-M2
10-Port Ethernet Switch

Instructions for Use

Table of Contents

1 About These Instructions

These instructions for use describe the structure, functions and the use of the product and will help you to operate the product as intended. Read these instructions carefully before using the product. This is to avoid possible damage to persons, property or the device. Retain the instructions for future use during the service life of the product. If the product is passed on, pass on these instructions as well.

1.1 Target groups

These instructions are aimed at qualified personnel and must be carefully read by anyone mounting, commissioning, operating, maintaining, dismantling or disposing of the device.

When operating the device in a hazardous area, the user must have a working knowledge of explosion protection (EN 60079-14, etc.).

1.2 Explanation of symbols used

The following symbols are used in these instructions:

	**DANGER** DANGER indicates a dangerous situation with high risk of death or severe injury if not avoided.
	**WARNING** WARNING indicates a dangerous situation with medium risk of death or severe injury if not avoided.
	**CAUTION** CAUTION indicates a dangerous situation of medium risk which may result in minor or moderate injury if not avoided.
	**NOTICE** NOTICE indicates a situation which may lead to property damage if not avoided.
	**NOTE** NOTE indicates tips, recommendations and useful information on specific actions and facts. The notes simplify your work and help you to avoid additional work.
▶	**CALL TO ACTION** This symbol denotes actions that the user must carry out.
⇨	**RESULTS OF ACTION** This symbol denotes relevant results of actions.

1.3 Additional documents

The following additional documents are available online at www.turck.com

- Data sheet
- Declarations of conformity (current version)
- Notes on Use in Ex zone 2 and 22 (100022986)
- Approvals

1.4 Feedback about these instructions

We make every effort to ensure that these instructions are as informative and as clear as possible. If you have any suggestions for improving the design or if some information is missing in the document, please send your suggestions to techdoc@turck.com.

2 Notes on the Product

2.1 Product identification

These instructions are valid for the following manageable IP67-Switches:

- TBEN-L4-SE-M2 (ID 100044426)
- TBEN-L5-SE-M2 (ID 100044425)
- TBEN-LL-SE-M2 (ID 100044427)

2.2 Scope of delivery

The scope of delivery includes:

- TBEN switch
- Closing caps for M12 sockets
- Labelling clips

2.3 Legal requirements

The device falls under the following EU directives:

- 2014/30/EU (electromagnetic compatibility)
- 2011/65/EU (RoHS directive)
- 2014/34/EU (ATEX directive)

2.4 Turck service

Turck supports you with your projects, from initial analysis to the commissioning of your application. The Turck product database under www.turck.com contains software tools for programming, configuration or commissioning, data sheets and CAD files in numerous export formats.

The contact details of Turck subsidiaries worldwide can be found on p. [▷ 68].

3 For Your Safety

The product is designed according to state-of-the-art technology. However, residual risks still exist. Observe the following warnings and safety notices to prevent damage to persons and property. Turck accepts no liability for damage caused by failure to observe these warning and safety notices.

3.1 Intended use

These devices are designed solely for use in industrial areas.

The manageable switch TBEN-L…-SE-M2 is used within a machine or cell for decentralized connection of Industrial Ethernet devices to controllers. Line, star, ring and mixed topologies are supported. With its integrated firewall, NAT routing, the VLAN function and a second configurable Ethernet interface (designated as WAN), the device is used to network machine cells or to integrate machines into higher-level factory networks. The device is only suitable for use in Local Area Networks.

The devices may only be used as described in these instructions. Any other use is not in accordance with the intended use. Turck accepts no liability for any resulting damage.

3.2 General safety notes

- The device may only be assembled, installed, operated, parameterized and maintained by professionally-trained personnel.
- The device may only be used in accordance with applicable national and international regulations, standards and laws.
- The device only meets the EMC requirements for industrial areas and is not suitable for use in residential areas.
- Change the default password of the integrated web server after the first login. Turck recommends using a secure password.

3.3 Notes on UL approval

- Use UL certified PVVA or CYJV cables that are suitable for the current/voltage rating and have an insulation temperature of at least 90 °C.
- Only use the device in an area of not more than pollution degree 2.

3.4 Notes on Ex protection

- When using the device in explosion-protection circuits, the user must have a working knowledge of explosion protection (EN 60079-14 etc.).
- Observe national and international regulations for explosion protection.
- Use the device only within the permissible operating and ambient conditions (see approval data and Ex approval specifications).

3.5 ATEX and IECEx approval requirements for use in Ex area

- Only use the device in an area with no more than pollution degree 2.
- Only disconnect and connect circuits when no voltage is applied.
- Only operate the switches if no voltage is present.
- Connect the metal protective cover to the equipotential bonding in the Ex area.
- Ensure impact resistance in accordance with EN IEC 60079-0 – alternative measures:
  - Install the device in the TB-SG-L protective housing (available in the set with Ultem window: ID 100014865) and replace the service window with an Ultem window.
  - Install the device in an area offering impact protection (e.g. in robot arm) and attach a warning: "DANGER: Only connect and disconnect circuits when no voltage is present. Do not operate switch when energized.".
- Do not install the device in areas critically exposed to UV light.
- Prevent risks caused by electrostatic charge.
- Protect unused connectors with dummy plugs to ensure protection class IP67.

4 Product Description

The devices are designed in a fully encapsulated housing with degree of protection IP65/IP67/IP69K.

Der TBEN-L…-SE-M2 is a 10-port Ethernet switch. The switch has two 8-pin, X coded M12 Gigabit Ethernet ports (XF9 and XF10) with a transmission speed of 10/100/1000 Mbps and eight 4-pin, D coded M12 Fast Ethernet ports (XF1…XF8) with a transmission speed of 10/100 Mbps.

For connecting the supply voltage, 4-pin (TBEN-L4) 7/8" connectors, 5-pin (TBEN-L5) 7/8" connectors or 5-pin M12 connectors (TBEN-LL) are available.

4.1 Device overview

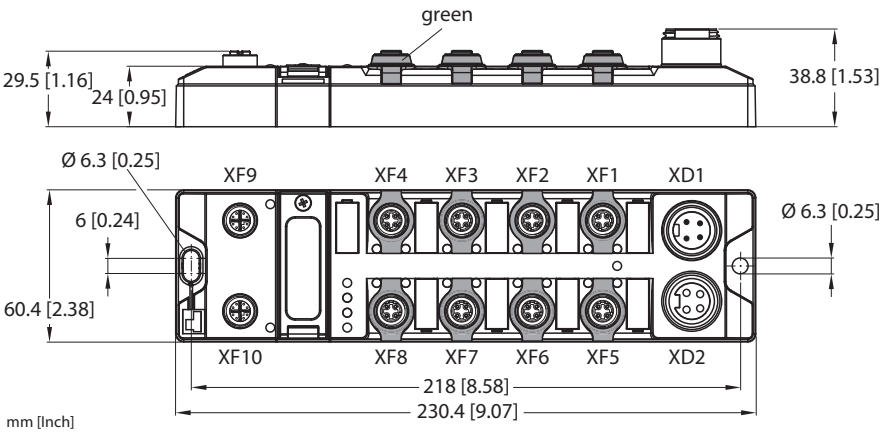

Fig. 1: Dimensions TBEN-L4-SE-M2

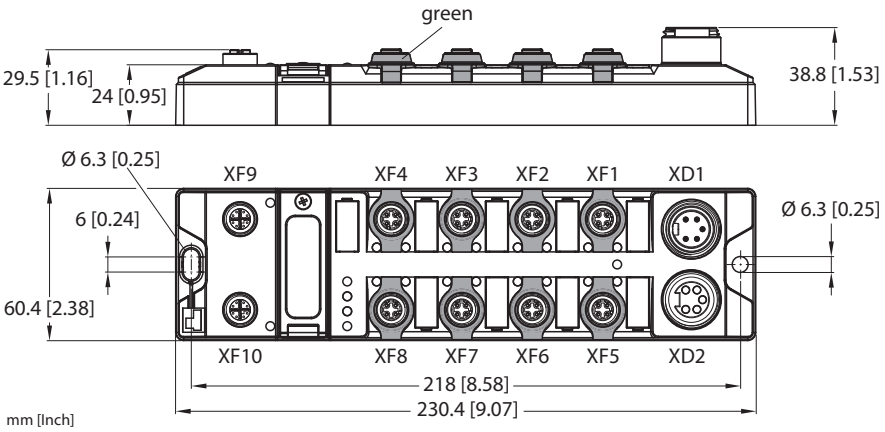

Fig. 2: Dimensions TBEN-L5-SE-M2

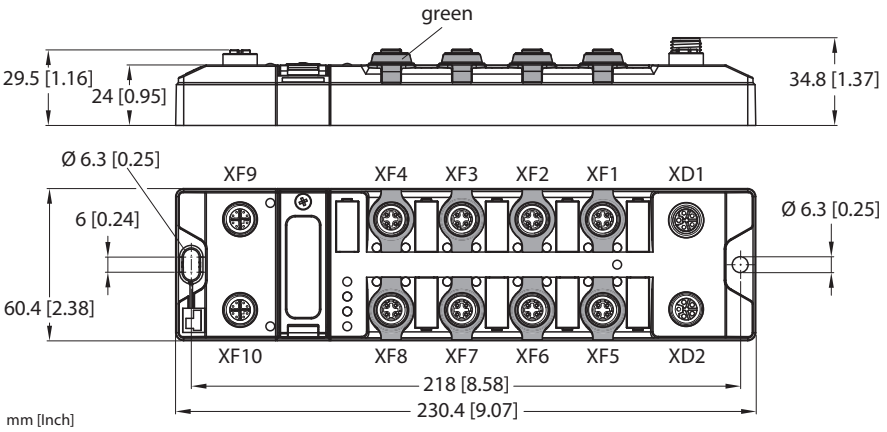

Fig. 3: Dimensions TBEN-LL-SE-M2

4.1.1 Operating elements

The devices are provided with the following operating elements:

- Rotary coding switches and DIP switch for setting the IP address
- SET button for executing USB Host functions

4.1.2 Display elements

The device has the following LED indicators:

- Supply voltage
- Status

4.2 Properties and features

- Fibre-glass reinforced housing
- Shock and vibration tested
- Fully potted module electronics
- Protection class IP65/IP67/IP69K
- UV-resistant according to DIN EN ISO 4892-2
- Metal connectors
- Ethernet ports:
  - 2 × M12, X coded, 1 Gbps
  - 8 × M12, D coded, 10/100 Mbps
- Web based management
- Configurable LAN and WAN zones
- Configurable Layer 3 features

4.3 Operating principle

The TBEN-L…-SE-M2 is used to build industrial Ethernet networks according to IEEE 802.3. and connects up to ten network segments. The switch controls the data traffic within a network domain and forwards data telegrams specifically to connected devices. A switch can send and receive messages simultaneously.

The switch can manage two different network zones (LAN and WAN). All Ethernet ports that are assigned to one of the two zones are switched with each other.

In the delivery state, the device behaves as a layer 2 switch. Layer 3 functions can be activated optionally.

4.4 Functions and operating modes

4.4.1 SNMP agent

The switch supports SNMP (Simple Network Management Protocol) V1, V2c and V3. The SNMP function of the device can be configured via the web server.

4.4.2 Neighborhood detection via LLDP (Link Layer Discovery Protocol)

The switch uses the LLDP protocol for neighborhood detection. Like all LLDP-capable network devices, the switch sends information about itself and stores information received from its neighbors. This information is queried by a network management system via the Simple Network Management Protocol (SNMP) and used for topology detection.

4.4.3 Prioritization/classification of data packets via QoS

The function QoS (Quality of Service) enables the prioritization (via PCP) or classification (via DSCP) of data telegrams.

- PCP (Priority Code Point)
  This function prevents time-critical data traffic from being disrupted by less time-critical data traffic in heavily loaded networks. By assigning high priorities for time-critical data and low priorities for less time-critical data, an optimal data flow for high-priority data is achieved. Frames to be transmitted are divided into priority classes from 0 to 7. 0 is used for frames that are not assigned a specific priority.
- DSCP (Differentiated Services Codepoint)
  DDSCPs are used to classify data packets. A DSCP (0...63) specifies a forwarding behavior for a data packet, i.e. it determines how a packet is handled.

4.4.4 DHCP

The switch supports the following DHCP options:

- DHCP server
- DHCP client
- DHCP server option 82, port-based IP address assignment

4.4.5 Network redundancy

The switch supports network redundancy via STP and RSTP.

Network redundancy via STP (Spanning Tree Protocol)

STP is an open protocol for setting up closed, loop-free networks with redundant paths via so-called spanning trees. In the event of a node failure or a line break in the network, the data is redirected via a backup path. The switching times for STP are usually between 20 and 30 seconds.

Network redundancy via RSTP (Rapid Spanning Tree Protocol)

RSTP is a further development of the STP with shorter switching times of 1 to 10 seconds. With RSTP on network participant acts as root. Unnecessary ports of network participants that lead to network loops and thus to unnecessary data traffic are deactivated and only activated in the event of an error to form a backup path.

Network redundancy via MSTP (Multiple Spanning Tree Protocol)

MSTP is an extension of the RSTP. MSTP enables different instances of the Spanning Tree in conjunction with Virtual Local Area Networks (VLANs). For a VLAN or a group of VLANs, independent STP instances can be formed that use their own spanning trees within a LAN.

4.4.6 Routing

Routing is used to forward data packets between networks with different IP address ranges. Several routing rules can be defined in the switch for data transfer between the configurable LAN and WAN network zones.

NOTE
IP forwarding (forwarding of data packets between networks with different IP address ranges) must be activated.

4.4.7 Firewall

The switch firewall offers the possibility to set up rules for incoming and outgoing data packets as well as forwarding rules for data packets. The rules can be defined network-wide or IP-address-based and apply to all data packets or only to UDP-based or TCP-based packets.

4.4.8 NAT (Network Address Translation)

If IP forwarding (forwarding of data packets between networks with different IP address ranges) is activated, IP addresses of one network are translated into IP addresses of another network. Example: IP addresses of network participants of an internal network are assigned to IP addresses of an external network.

4.4.9 Mirroring – mirroring switch ports

With the Mirroring function, data present on one port of the switch can be mirrored to another port. Only incoming, only outgoing or both types of data packets can be mirrored.

4.4.10 IGMP (Internet Group Management Protocol)

IGMP is the protocol for IP multicast applications in TCP/IP networks and is used to organize multicast groups. The switch can log on or off by sending IGMP messages to a router to receive multicast telegrams.

5 Installing

5.1 Installing the device in Zone 2 and Zone 22

In Zone 2 and Zone 22, the devices can be used in conjunction with the protective housing set .

DANGER
Potentially explosive atmosphere
Risk of explosion through spark ignition
For use in Zone 2 and Zone 22:

- ▶ Only install the device if there is no potentially explosive atmosphere present.
- ▶ Observe requirements for Ex approval.

- ▶ Unscrew the housing. Use Torx T8 screwdriver.
- ▶ Replace the service window with the enclosed Ultem window.
- ▶ Place the device on the base plate of the protective housing and fasten both together on the mounting plate, see [▷ 14].
- ▶ Connect the device, see [▷ 17].
- ▶ Mount and screw the housing cover according to the following figure. The tightening torque for the Torx T8 screw is 0.5 Nm.

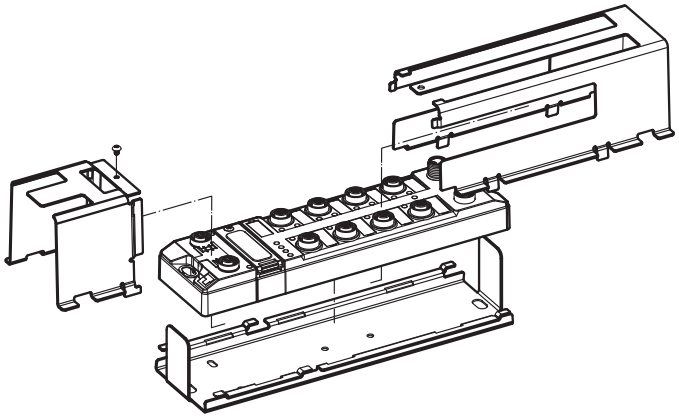

Fig. 4: Mounting the device in protection housing TB-SG-L

5.2 Mounting onto a mounting plate

NOTICE
Mounting on uneven surfaces
Device damage due to stresses in the housing
- ▶ Fix the device on a flat mounting surface.
- ▶ Use two M6 screws to mount the device.

The device can be screwed onto a flat mounting plate.

- ▶ Attach the module to the mounting surface with two M6 screws. The maximum tightening torque for the screws is 1.5 Nm.
- ▶ Avoid mechanical stresses.
- ▶ Optional: Ground the device.

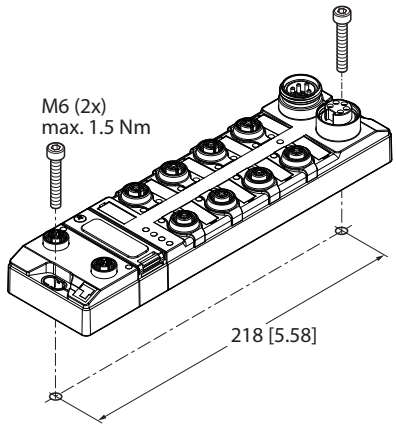

Fig. 5: Mounting the device onto a mounting plate

5.3 Mounting the device outdoors

The device is UV-resistant according to DIN EN ISO 4892-2. Direct sunlight can cause material abrasion and color changes. The mechanical and electrical properties of the device are not affected.

- ▶ To avoid material abrasion and color changes: Protect the device from direct sunlight, e.g. by using protective shields.

5.4 Grounding the device

5.4.1 Equivalent wiring diagram and shielding concept

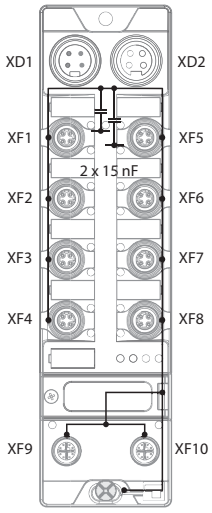

Fig. 6: TBEN-L4-SE-M2– equivalent wiring diagram and shielding concept

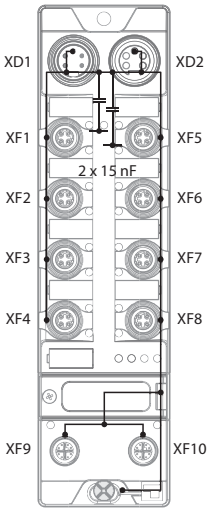

Fig. 7: TBEN-L5-SE-M2– equivalent wiring diagram and shielding concept

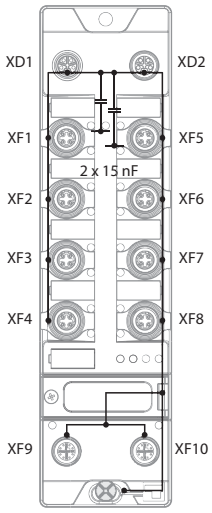

Fig. 8: TBEN-LL-SE-M2– equivalent wiring diagram and shielding concept

5.4.2 Shielding the Ethernet ports

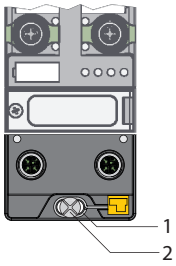

Fig. 9: Grounding ring (1) and mounting screw (2)

The grounding ring (1) is the module grounding. The shielding of the Ethernet ports is permanently connected to the module grounding. The module grounding is only connected to the reference potential of the installation when the module is mounted.

In the device variants TBEN-L5-SE-M2 and TBEN-LL-SE-M2, the earthing can also be connected via pin 5 of the connector for the supply voltage.

5.4.3 Grounding the device

Grounding the device – mounting on a mounting plate

- ▶ For mounting onto a mounting plate: Fix the module with an M6 metal screw through the lower mounting hole.
- ⇨ The shielding of the M12 flanges for the I/O level is connected to the reference potential of the installation via the M6 metal screw.

6 Connecting

The TBEN-L…-SE-M2 is only suitable for use in LAN networks.

NOTICE
Intrusion of liquids or foreign bodies through leaking connections
Loss of protection class IP65/IP67/IP69K, device damage possible

- Tighten M12 connectors with a tightening torque of 0.6 Nm.
- Tighten 7/8" connectors with a tightening torque of 0.8 Nm.
- Only use accessories that guarantee the protection class.
- Always seal unused connectors with suitable screw caps or blind caps. The tightening torque for the screw caps is 0.5 Nm.

6.1 Connecting the device in Zone 2 and Zone 22

DANGER
Potentially explosive atmosphere
Risk of explosion through spark ignition
When used in Zone 2 and Zone 22:

- Only disconnect and connect circuits when no voltage is applied.
- Only use connecting cables that are approved for use in potentially explosive atmospheres.
- Use all connectors or seal them with blind plugs.
- Observe requirements for Ex approval.

6.2 Connecting network segments

To connect the Ethernet network segments, the device has two 8-pin , X coded M12 Gigabit Ethernet connectors and eight 4-pin, d coded M12 Fast Ethernet connectors. The maximum tightening torque is 0.6 Nm.

Gigabit ports (10/100/100 Mbps)

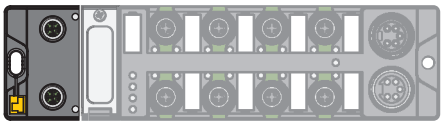

Fig. 10: M12 Gigabit Ethernet connector

- Connect the device to Ethernet according to the pin assignment below.

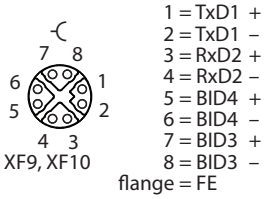

Fig. 11: M12 Gigabit Ethernet connector

Fast Ethernet ports (10/100 Mbps)

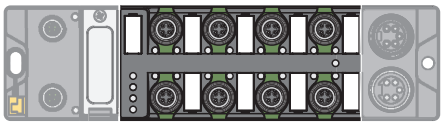

Fig. 12: M12 Fast Ethernet connector

▶ Connect the device to Ethernet according to the pin assignment below.

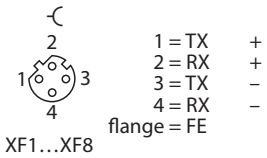

Fig. 13: M12 Fast Ethernet connector

6.3 Connecting the power supply

TBEN-L4-SE-M2/TBEN-L5-SE-M2

For the connection to the power supply, the device has two 5-pin 7/8" connectors. The power supply connectors are designed as 4-pin (TBEN-L4) or 5-pin (TBEN-L5) 7/8" connectors. V1 and V2 are galvanically isolated. The maximum tightening torque is 0.8 Nm.

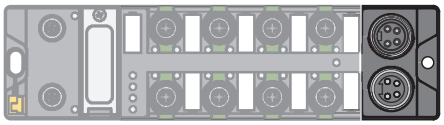

Fig. 14: TBEN-L4-SE-M2 – 7/8" for connecting the supply voltage

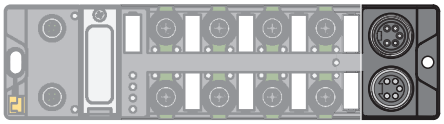

Fig. 15: TBEN-L5-SE-M2 – 7/8" for connecting the supply voltage

▶ Connect the device to the power supply according to the pin assignment shown below.

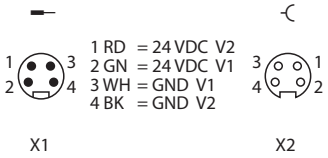

Fig. 16: TBEN-L4-… – pin assignment power supply connectors

Fig. 17: TBEN-L5-… – pin assignment power supply connectors

Connector	Function
X1	Power feed
X2	Continuation of the power to the next node

Voltage	Function
V1	System voltage: power supply 1 (incl. supply of electronics)
V2	Load voltage: power supply 2, fed through, not used in device

TBEN-LL-SE-M2

For the connection to the supply voltage, the device has two 5-pin, L coded M12 connectors. V1 and V2 are galvanically isolated. The maximum tightening torque is 0.6 Nm.

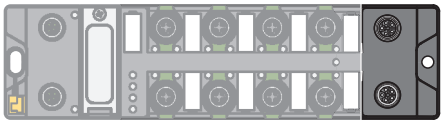

Fig. 18: M12 connector for connecting the supply voltage

- ▶ Connect the device to the power supply according to the pin assignment shown below.
- ▶ Always seal unused connectors with suitable screw caps or blind caps. The tightening torque for the screw caps is 0.5 Nm.

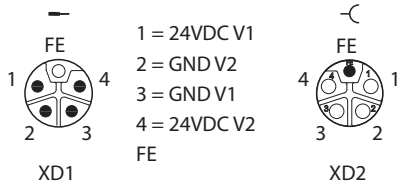

Fig. 19: Pin assignment power supply connectors

Connector	Function
XD1	Power feed
XD2	Continuation of the power to the next node

Voltage	Function
V1	System voltage: power supply 1 (incl. supply of electronics)
V2	Load voltage: power supply 2, fed through, not used in device

6.3.1 Supply concept

The device is supplied via V1. All Ethernet ports are galvanically isolated. V2 is fed through.

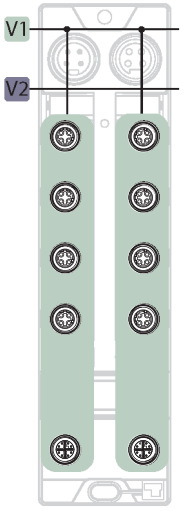

Fig. 20: Supply TBEN-L4-SE-M2

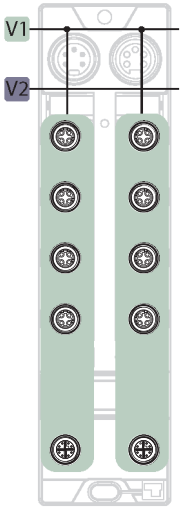

Fig. 21: Supply TBEN-L5-SE-M2

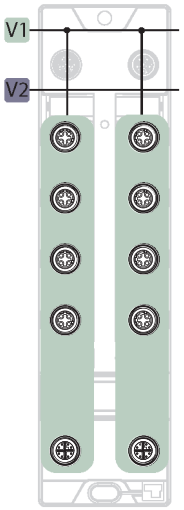

Fig. 22: Supply TBEN-LL-SE-M2

7 Commissioning

7.1 Opening the web server

The web server can be opened via a web browser or via the Turck Service Tool. Calling the web server via the Turck Service Tool is described in the section "Setting the Network address".

7.1.1 Web server login

- Open the web server.
- Log on to the device as administrator. The default user for the web server is "admin", the default password is "password".
- Enter user name and password in the login field on the start page of the web server.
- Click **Login**.

NOTE
The password is transmitted in plain text for HTTP connections. The password is only encrypted if access to the web server is established via an HTTPS connection.

7.1.2 Securing device access with password

NOTICE
Inadequately secured devices
Unauthorized access to sensitive data
- Change password after first login. Turck recommends using a secure password.
- Adapt the password to the requirements of the network security concept of the system in which the devices are installed.

7.2 Adjusting network settings

The network settings for the LAN network zone of the switch can be set via two decimal rotary coding switches and DIP switches on the device, via the web server or via the Turck Service Tool.

The network settings for the WAN network zone on the switch can only be set via the web server.

7.2.1 Adjusting network settings via switches on the device

The network settings can be adjusted via two decimal rotary coding switches and the DIP switch [Mode] on the device. The switches are located under a service window together with the USB ports and the SET button.

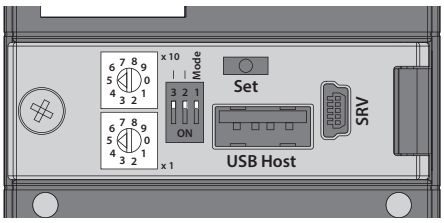

Fig. 23: Switches for setting the IP address

- Open the service window above the switches.
- Set the rotary coding switch to the desired position according to the table below.
- Set DIP switch [Mode] to the desired position according to the table below.
- Execute a power cycle.
- NOTICE! IP67 or IP69K protection is not guaranteed when the service window above the rotary coding switches is opened. Damage to the device due to foreign material or liquids penetrating the device is possible. Tightly close the service window above the switches.

Switch positions

The network settings of the device depend on the selected mode. Changes to the settings become active after a voltage reset.

Switch position			
DIP switch [MODE]	**Rotary coding switches**	**Setting option**	**Description**
0	00	Network reset	The network reset resets the following network settings to the default values: IP address: 192.168.1.100 Subnet mask: 255.255.255.0 Gateway: 192.168.1.1
0	1…99	Rotary	In rotary mode (static rotary), the last byte of the IP address can be set manually at the device. The other network settings are stored non-volatile in the memory of the device and cannot be changed in rotary mode. Addresses from 1...99 can be set.
1	40	DHCP	In DHCP mode, the network settings are by a DHCP server in the network. The subnet mask assigned by the DHCP server and the default gateway address are stored non-volatile in the memory of the device. DHCP supports three mechanisms for IP address allocation: ■ Automatic address assignment: The DHCP server assigns a permanent IP address to the client. ■ Dynamic address assignment: The IP address assigned by the server is only reserved for a certain period of time. After this time has elapsed or after the explicit release by a client, the IP address is reassigned. ■ Manual address assignment: A network administrator assigns an IP address to the client. In this case, DHCP is only used to transmit the assigned IP address to the client. ■ Default IP address: 192.168.1.254
1	50	PGM	In PGM mode, the network settings are assigned manually via the Turck Service Tool, FDT/DTM or via a web server. The setting are stored to non-volatile the device. ■ Default IP address: 192.168.1.254
1	60	PGM-DHCP	In PGM DHCP mode, the device initially operates a DHCP client and sends DHCP requests until it is assigned a permanent IP address. The DHCP client is automatically deactivated as soon as the device has received an IP address via the DTM, the or the web server. ■ Default IP address: 192.168.1.254
1	90	Factory reset	The factory(F_Reset) all settings to the default values: ■ Network setting (IP address, subnet mask, gateway) ■ Device parameters
1	00	Restore	Enter the device name and the device's IP address. ■ IP address: 192.168.1.254

7.2.2 Adjusting network setting via Turck Service Tool

NOTE
The IP address can only be assigned using the Turck Service Tool if the switch is connected to the PC via one of its LAN ports. Connection to a WAN port is not possible.

- Connect the device to the PC via the Ethernet interface.
- Open the Turck Service Tool.
- Click **Search** or press [F5].

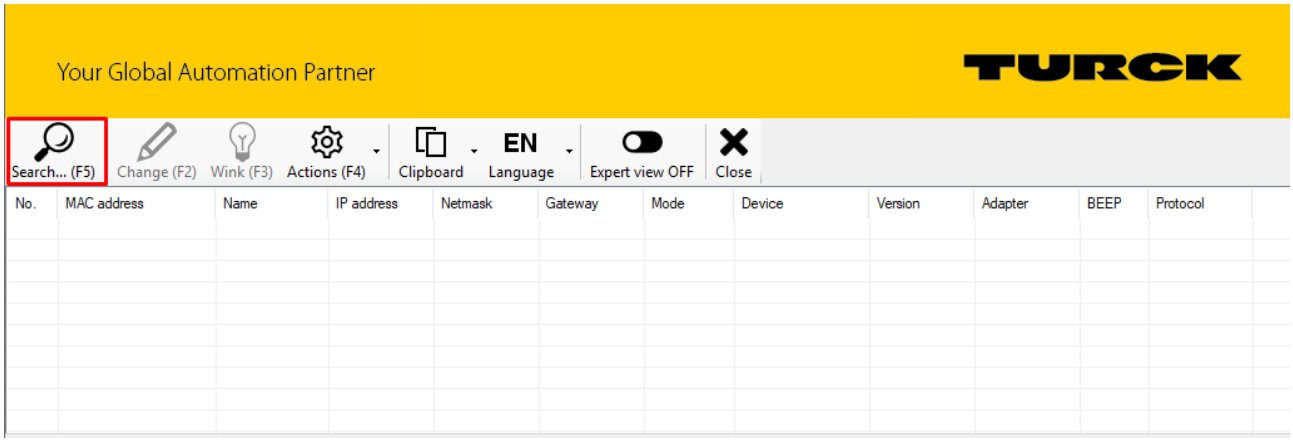

Fig. 24: Turck Service Tool – start dialog

Turck Service Tool shows the connected devices.

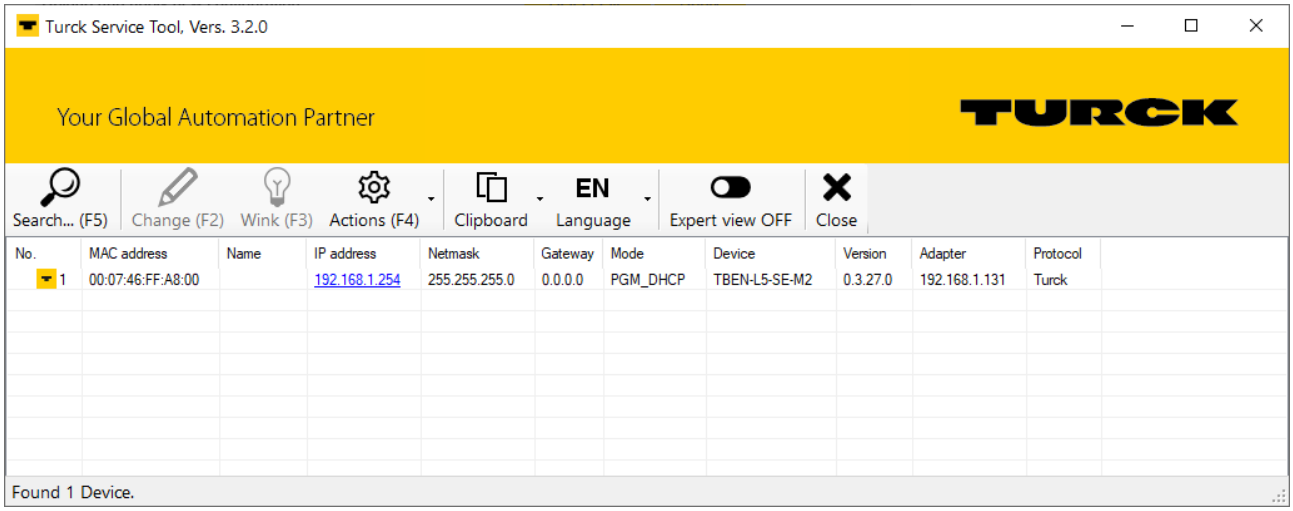

Fig. 25: Turck Service Tool – found devices

- ▶ Click on the desired device.
- ▶ Click **Change** or press [F2].

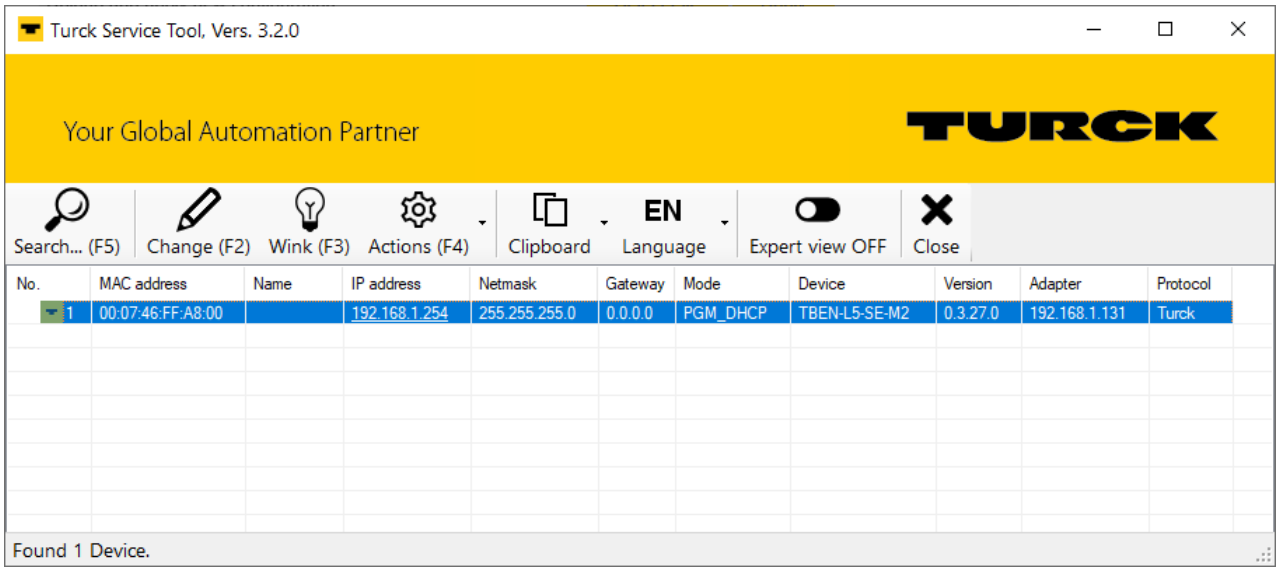

Fig. 26: Turck Service Tool – select the device to be addressed

NOTE
Clicking the device's IP address opens the web server.

- ▶ Change the IP address and the network mask if necessary.
- ▶ Accept the changes with **Set in device** .

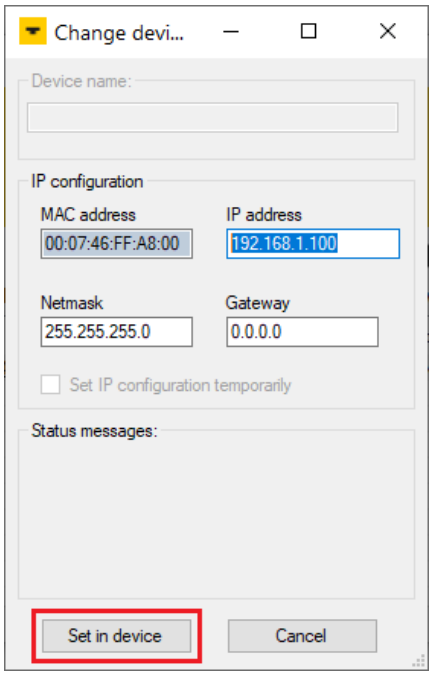

Fig. 27: Turck Service Tool – Change device configuration

NOTE
An IP address assigned vie the Turck Service Tool is not stored permanently in the switch.

7.2.3 Adjusting network settings via the web server

NOTE
To be able to adjust the network settings via the web server, the device must be in PGM mode.

- Open the web server.
- Log on to the device as administrator. The default user for the web server is "admin", the default password is "password".
- Click **Configuration** → **IP**.
- Change IP address and subnet mask if applicable as well as default gateway for zone LAN and/or or zone WAN. Zone WAN only appears if at least one of the switch's interfaces has been assigned to the WAN under Interfaces [▷ 30].
- Write the new IP address, subnet mask and default gateway via **Set Addresses** into the device.

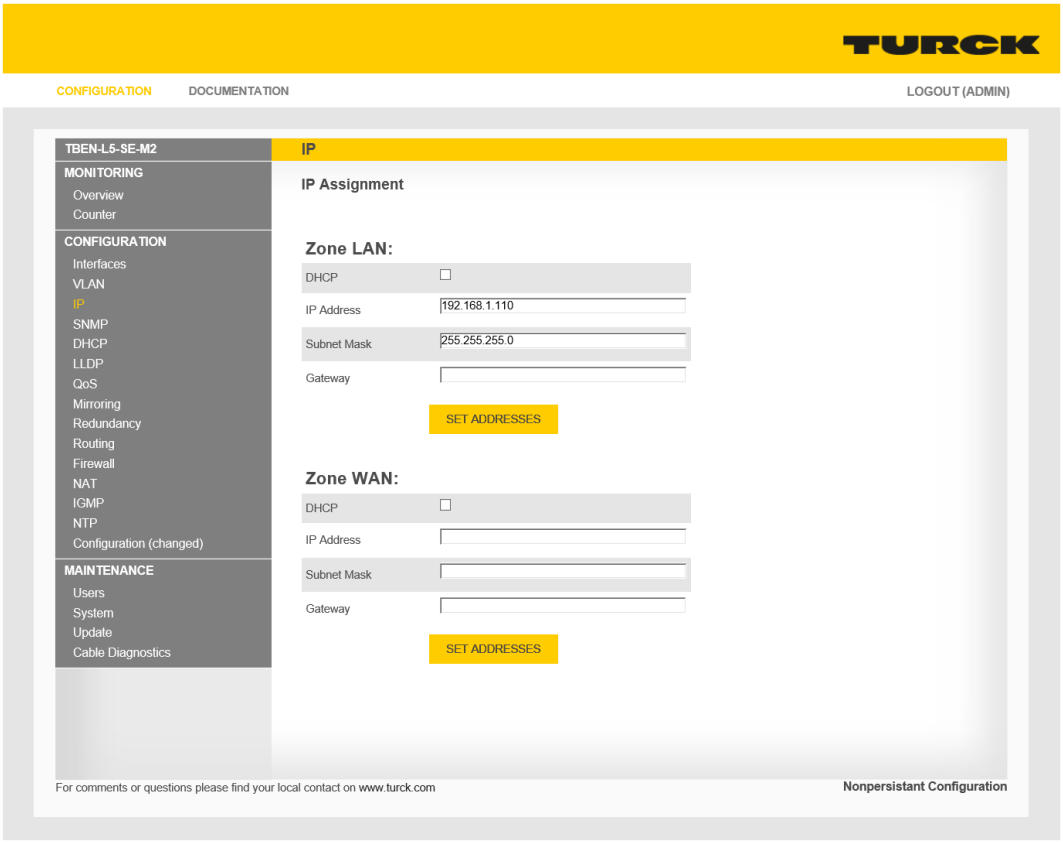

Fig. 28: Adjusting network settings via the web server

7.3 User management and rights assignment

Users are created in the web server under **Maintenance** → **Users**.

Security in the web server

In the web server, a default-password is assigned in Turck-module for the administrator login.

NOTICE
Inadequately secured devices
Unauthorized access to sensitive data

- ▶ Change password after first login. Turck recommends using a secure password.
- ▶ Adapt the password to the requirements of the network security concept of the system in which the devices are installed.

The password is transmitted in plain text for HTTP connections. The password is only encrypted if access to the web server is established via an HTTPS connection.

In the delivery state or after a factory reset, the default settings are as follows:

- User: admin
- Password: password

7.3.1 Authorization levels

The following table lists the authorization levels and the associated user rights.

Authorization level	Meaning	Rights
0	Admin	The user has full access to all functions of the device: ■ Configuration of the general switch functions (interfaces, VLAN, IP addresses, SNMP, DHCP, …) ■ Accept and reset the changed configuration, upload and download a configuration ■ User administration ■ Firmware update
1	Configuration	The user has access to the configuration of the general switch functions (interfaces, VLAN, IP addresses, SNMP, DHCP, …).
2	Read access	The user has read-only access.

7.3.2 Adding a user

✓ The logged in user is a user with admin rights (area permission level 0).

▶ Assign a user name and an initial password for the new user under **Maintenance** → **Users** → **Users**.

▶ Select the authorization level and create the new user via **Add user**.

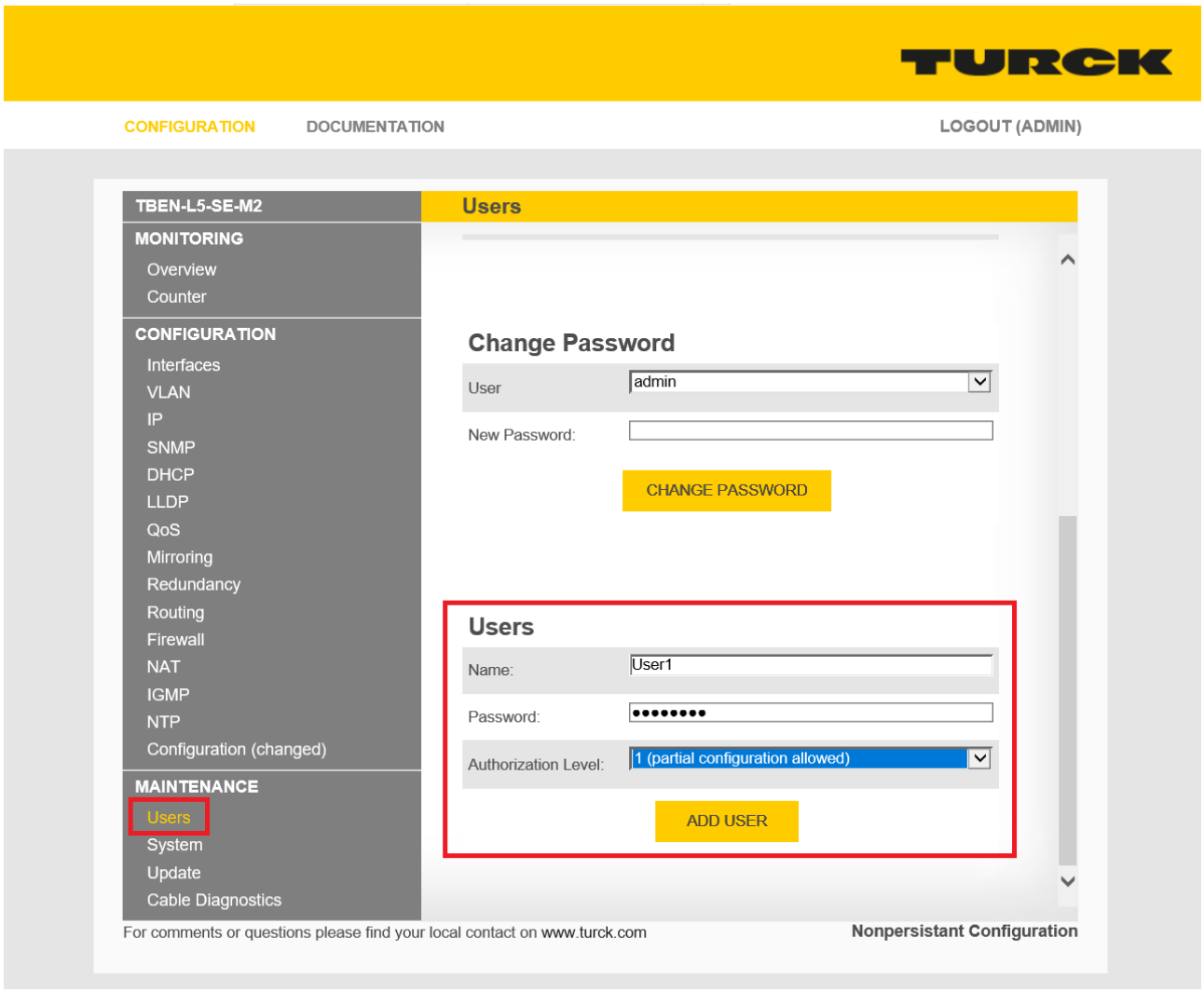

Fig. 29: Web server – Add user

NOTICE

Inadequately secured devices

Unauthorized access to sensitive data

▶ Change password after first login. Turck recommends using a secure password.

▶ Adapt the password to the requirements of the network security concept of the system in which the devices are installed.

8 Parameterizing and Configuring

8.1 Configuring device functions with the web server

NOTE
Changes to the configuration of the device are stored non-fail-safe in the device. Unsaved configuration changes are displayed via the **Nonpersistant Configuration** addition on the web server interface. In order to store a changed configuration fail-safe, it must be saved via **Configuration (changed)** → **Make current configuration persistent** [▶ 55].

8.1.1 Interfaces – configuring Ethernet interfaces

Interfaces is used to configure the Ethernet ports of the device.

Interface Settings

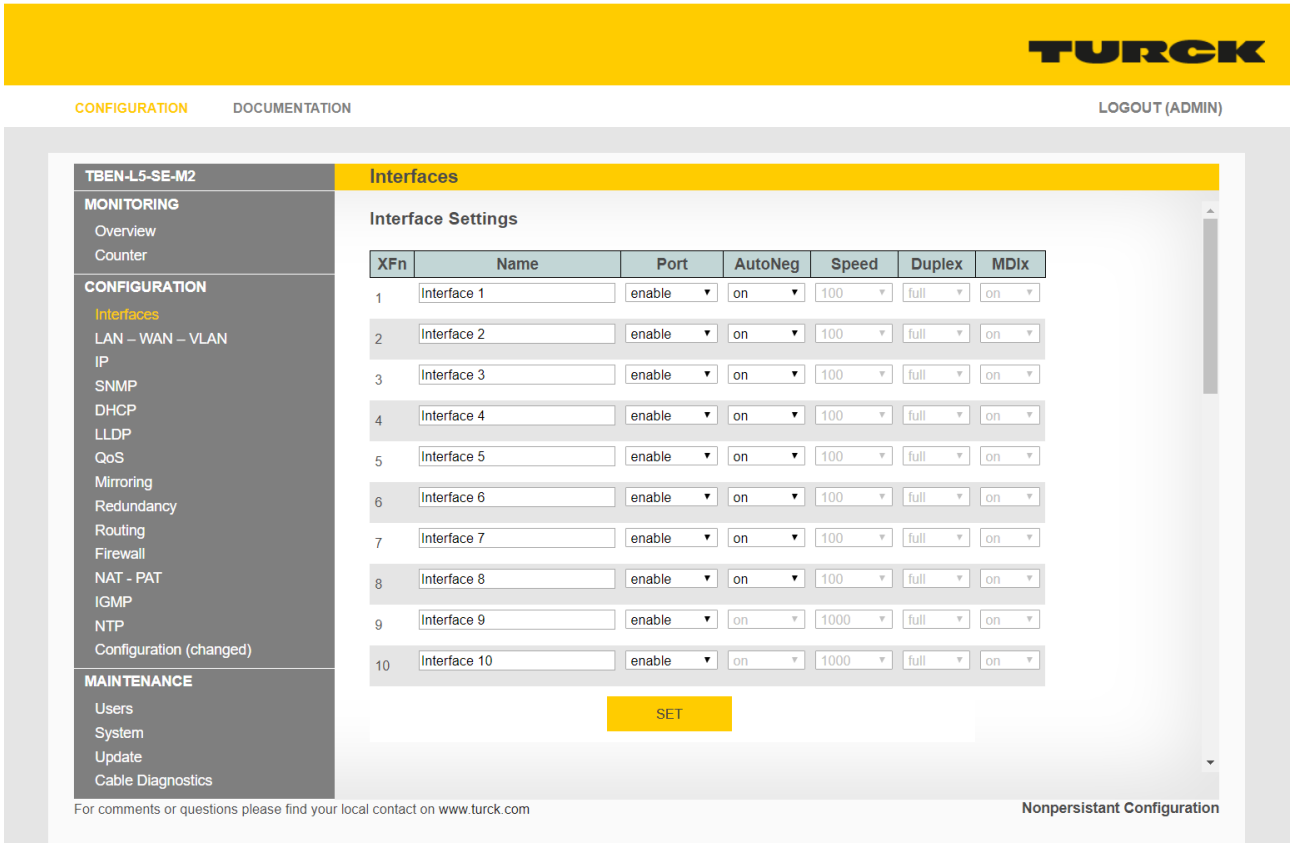

Fig. 30: Webserver – Interfaces

▶ Make settings on ports XF1...XF10 and accept changes with SET.

Setting	Value	Meaning	
XFn	1…10	Number of the Ethernet port	
Name		Freely selectable name	
Port	Enable	Port activated	
	Disable	Port deactivated	
AutoNeg	On	Autonegotiation activated	
	Off	Autonegotiation deactivated	
Speed	10	Setting the transmission rate of the Ethernet port	These settings can only be configured if autonegotiation is disabled.
	100		
	1000 (only valid for XF9 and XF10)		
Duplex	Full	Setting the data transfer	
	Half		
MDIx	On	Auto MDIx activated	
	Off	Auto MDIx deactivated	

Switching

Function	Meaning	
Broadcast Storm Protection		Reduces the forwarding of broadcast messages. The function should only be activated if problems occur due to broadcast storms. In PROFINET applications, relevant PROFINET frames may be suppressed if Broadcast Storm Protection is activated.
Flood unknown Multicasts/ Unicasts	On	Activates the forwarding of multicast or unicast telegrams to all ports. The function must be activated for PROFINET applications.
	Off	Deactivates the forwarding of multicast or unicast telegrams.
	IGMP only	Activates the reception of IGMP telegrams, other multicast or unicast telegrams are not received.

▶ Make settings and accept changes with SET.

Interface Status and Interface MAC Addresses

The I**nterface Status** and Interface **MAC Addresses** areas show status information (activity, transmission speed, MAC addresses, etc.) for the Ethernet ports.

8.1.2 IP – assigning IP addresses

On the IP Assignment page, the IP addresses for the LAN and WAN network zones are assigned. The assignment of the IP address via the web server is described in the chapter "Commissioning" [▶ 27].

8.1.3 LAN – WAN – VLAN – coding switches and VLAN configuring network zones

Zones

In the **Zones** area, the Ethernet ports of the switch are assigned to the LAN or WAN network zones. If ports are assigned to the WAN, an **IP** address for the WAN must be assigned under **IP**.

- ▶ Assign the zones and write them to the device via **SET ZONES**.

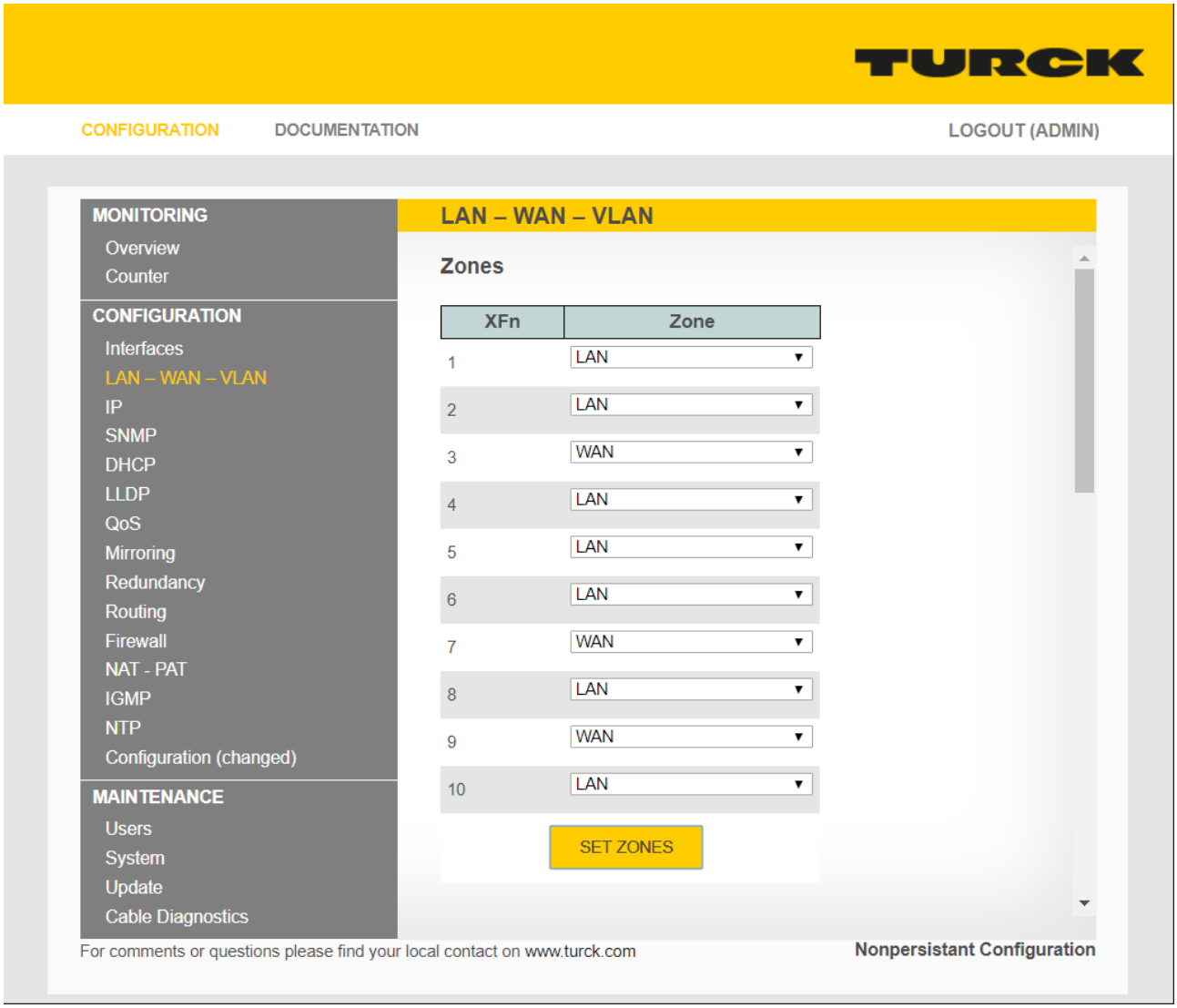

Fig. 31: Webserver – zone assignment

- ▶ Set the IP address for the WAN as described in the under "Setting the IP Address via the web server" [▶ 27].

VLAN Interface Settings

Under **VLAN Interface Settings** area, the Ethernet ports are assigned to the previously defined VLANs.

- Assign the VLAN ID and name if necessary and create them via **ADD ID**.
- Set the VLAN tag on the Ethernet port to **enabled** and enter the VLAN ID under **Default VLAN ID** to make the assignment.

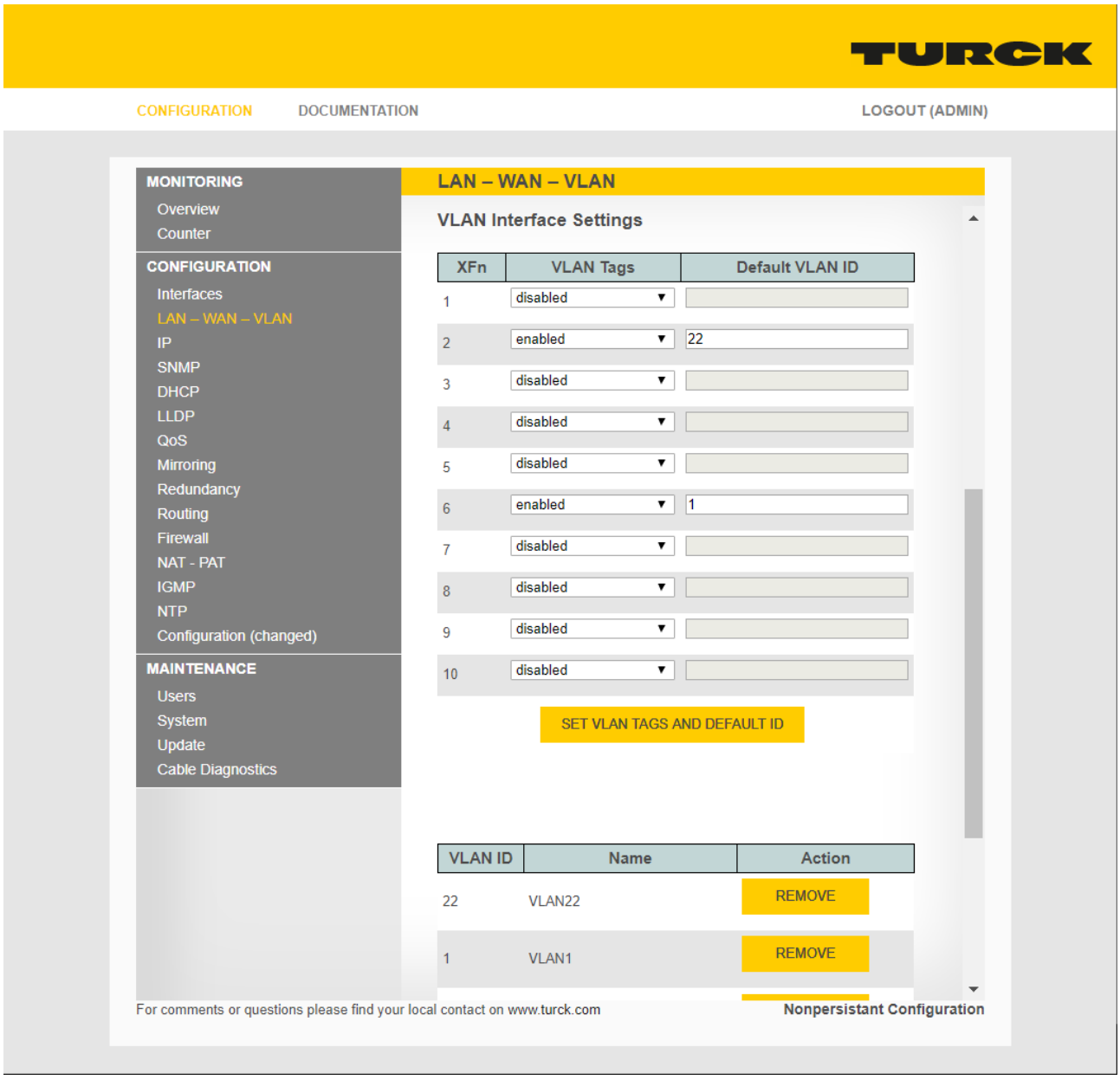

Fig. 32: Web Server - defining VLAN IDs and assigning Ethernet ports

▶ Under **VLAN ID/Interface Mapping**, define how the switch port is handled in the VLAN.

Option	Description
Not a member	The port is not assigned to a VLAN.
Untagged	The port is an untagged member of the VLAN. Forwarded packets are untagged. The VLAN is port-based, which means one VLAN can be set per switch port.
Tagged	The port is a tagged member of the VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information. Tagged VLANs allow multiple VLANs to be used on one switch port.

8.1.4 SNMP – setting up SNMP

SNMP configuration

In the section **SNMP Configuration** the supported SNMP versions as well as the read and write communities for authentication with SNMP V1 and SNMP V2c are configured.

- ▶ Configure and transfer settings to the device with SET.

SNMP User

The **SNMP User** section contains a list of all users created under Add User for SNMP version 3.

REMOVE is used to delete created SNMP users.

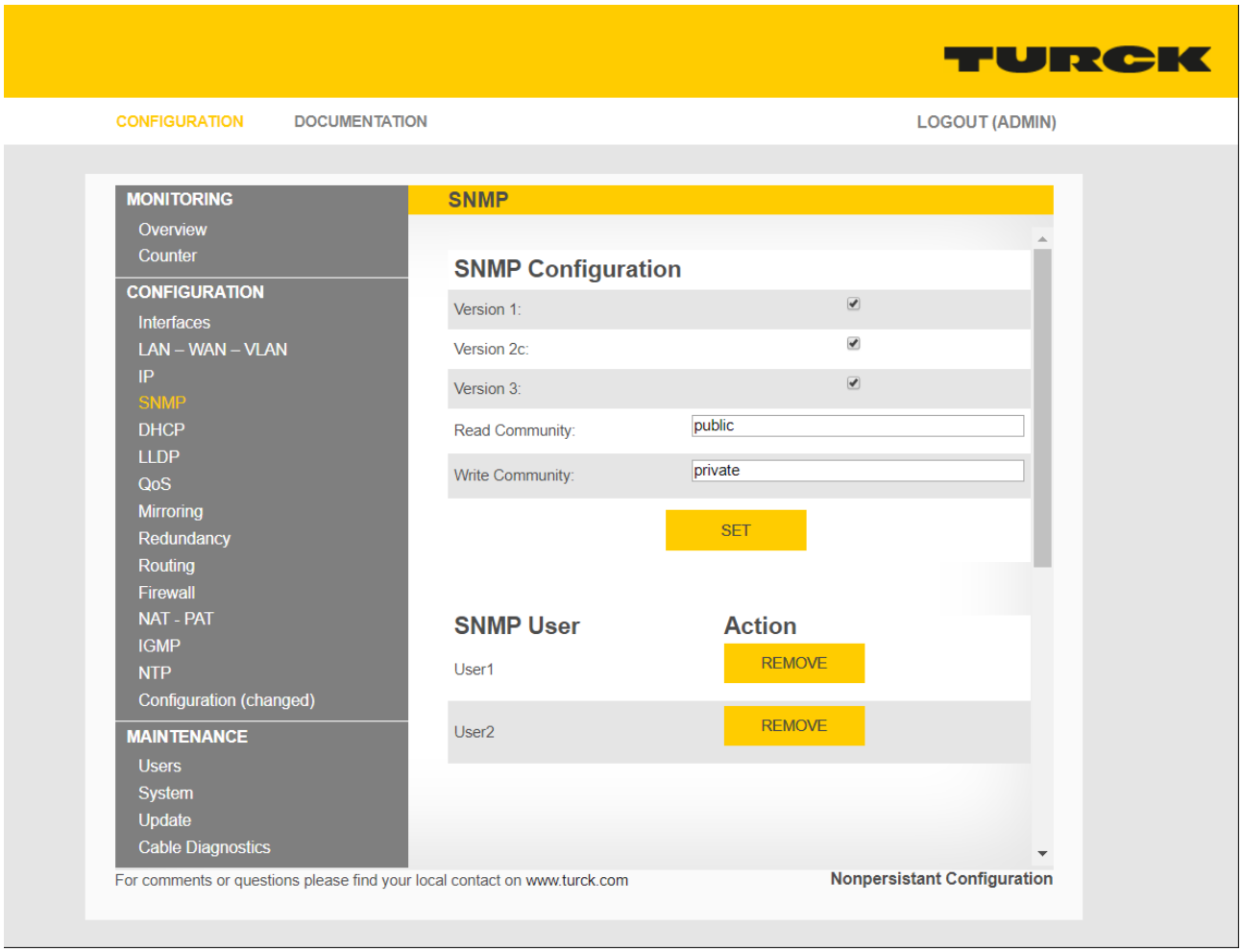

Fig. 33: Webserver – configuring SNMP

Add User

In the section **Add User**, SNMP users are created for the authentication of devices with SNMP V3.

- ▶ Assign user name (User Name) and passwords.
- ▶ Add user via **ADD USER**.

Traps

SNMP traps are a standard for error and change notifications in network management. If a device detects an error or change, it sends a notification to one or more trap recipients, a trap community.

The switch sends traps on the following events:

Trap	Description
Link up	A new connection is established, a device is connected to one of the ports.
Link down	The connection to a connected device is interrupted.
Reboot	The switch is restarted.

- ▶ Under **Destination**, specify the IP address of the device on the network that is to receive the traps.
- ▶ Under **Community**, specify the community to which the traps are to be sent.
- ▶ Send the configuration to the device via SET.

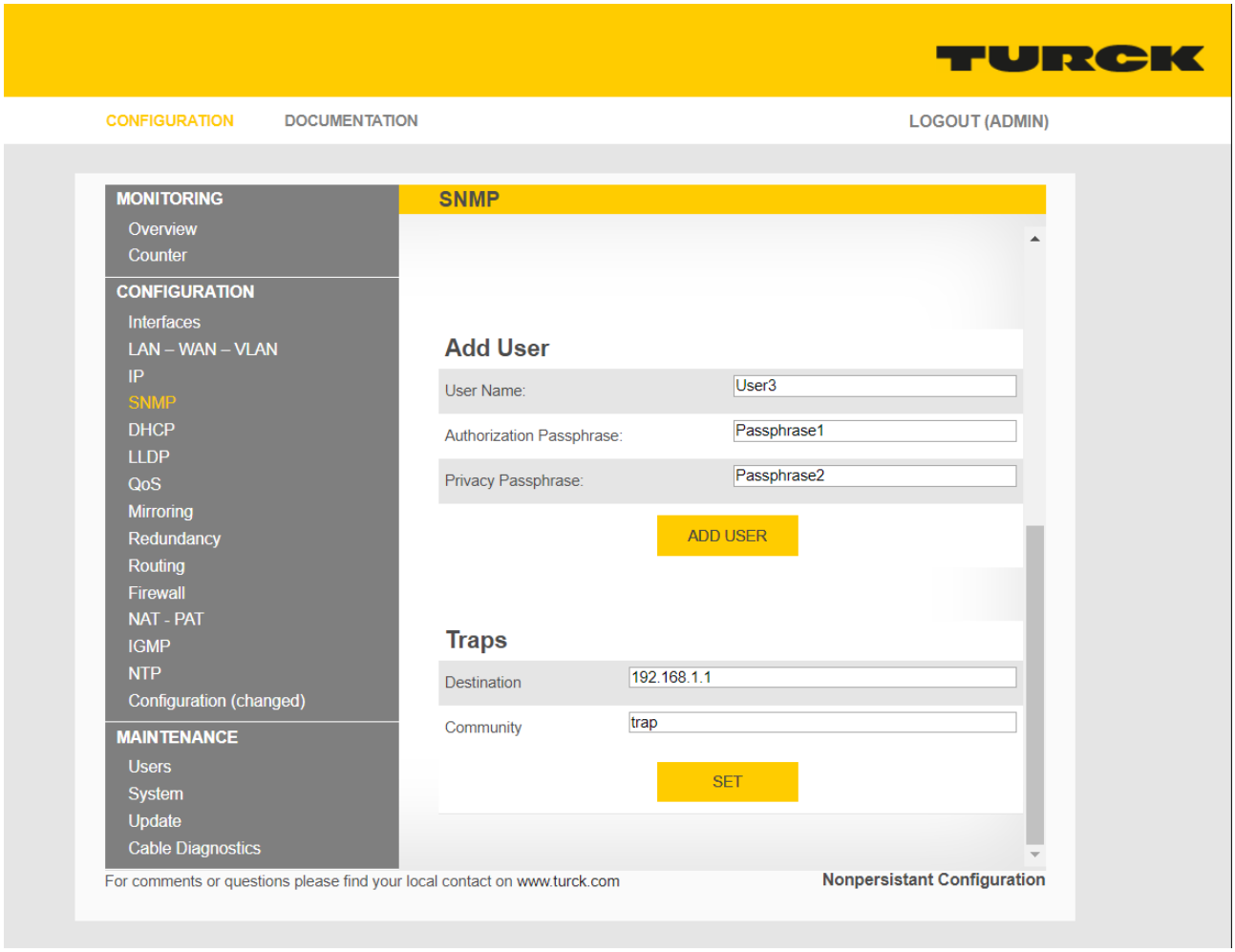

Fig. 34: Web Server - adding users and configuring traps

8.1.5 DHCP – setting up a DHCP server

DHCP Server Configuration

The section **DHCP Server Configuration** is used to configure the DHCP server in the device.

- Activate DHCP server via **Enable**.
- Use **Pool Start** and **Pool End** to define the IP address range from which the switch assigns addresses to other network participants.
- Define other settings (subnet mask, gateway, lease time, etc.).
- Under **Zone**, select the network zone (LAN or WAN) in which the switch is to function as a DHCP server. The network zone WAN only appears if Ethernet ports have been assigned to the WAN [▶ 32] and an IP address has been assigned to the WAN zone under [▶ 27].
- If necessary, define one or more DNS servers. By default, the Google DNS server (8.8.8.8) is used.
- Send the configuration to the device via SET.

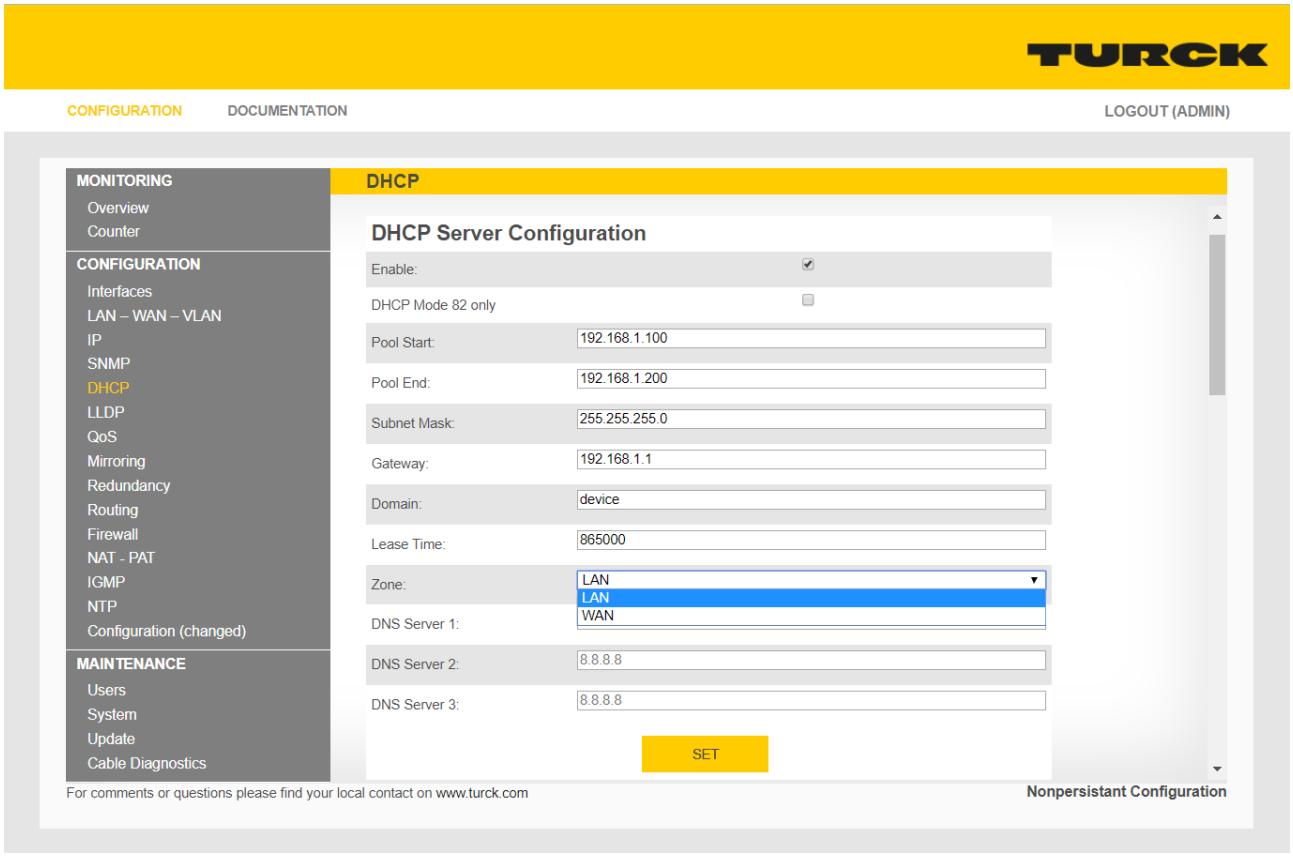

Fig. 35: Webserver – DHCP server configuration

DHCP Mode 82 only

In DHCP mode 82, fixed IP addresses are assigned to the switch ports. The IP address is also assigned independently of the connected device in the event of a device exchange. The fixed IP addresses are defined under **Interface-based IP Assigment.** The DHCP Mode 82 is only suitable for applications with only one device per switch port.

Static Leases

In the section **Static Leases**, devices can be defined for which a static IP address is to be assigned independently of the lease time. Static addresses are permanently stored. They are not deleted after the Aging Time has expired or when the switch is restarted.

- ▶ Enter the IP address that is to be permanently assigned. This IP address must be beyond the previously defined IP address range.
- ▶ Enter the MAC address of the device that will be permanently assigned this IP address.

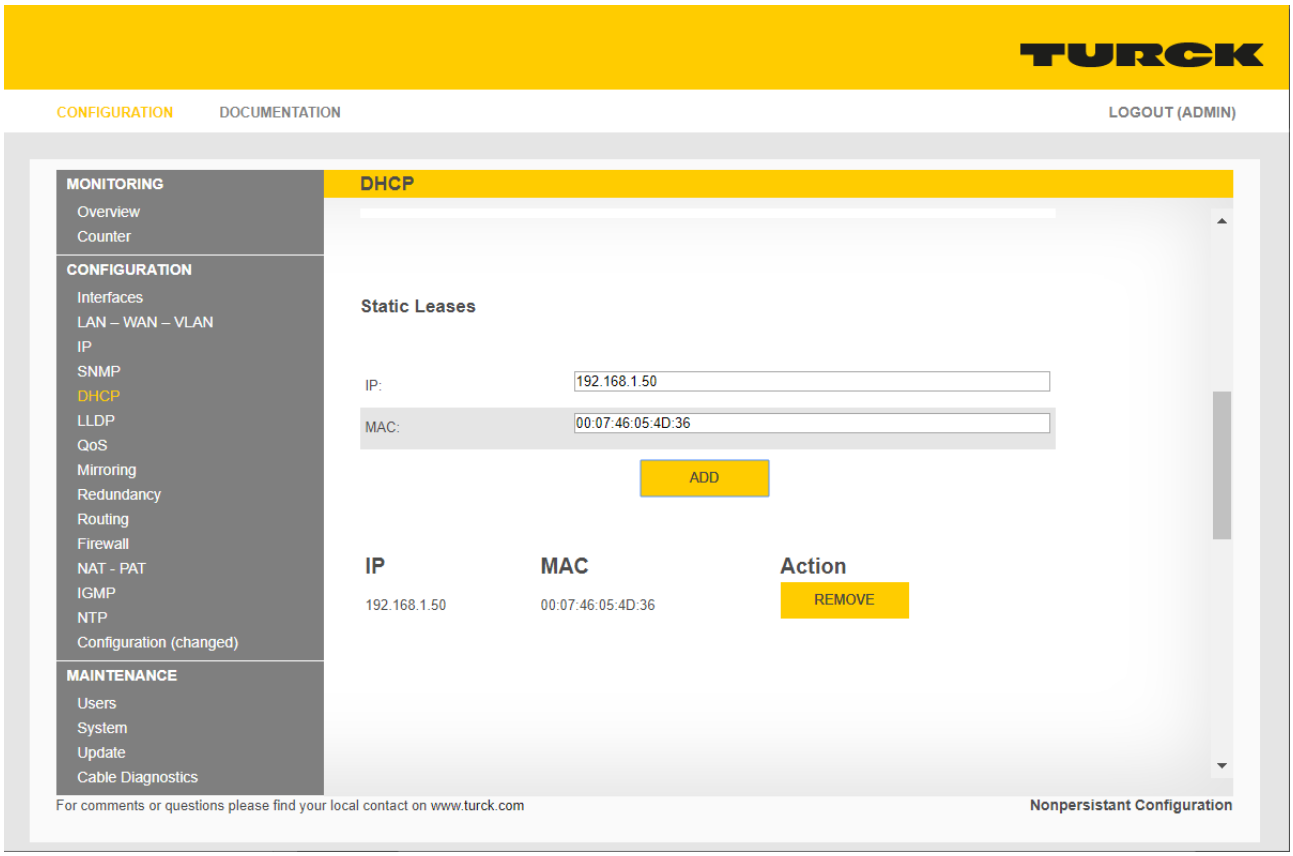

Fig. 36: Web server – assigning static IP addresses

Hans Turck GmbH & Co. KG | T +49 208 4952-0 | F +49 208 4952-264 | more@turck.com | www.turck.com

Interface-based IP Assignment

In the section **Interface-based IP Assignment**, Ethernet port-dependent IP addresses can be assigned. The IP addresses are assigned independently of the device for the first connected device that sends a DHCP request. If further devices are connected to the port, these devices receive an IP address from the DHCP address pool.

- ▶ Enter IP addresses at the respective port.
- ▶ Send the configuration to the device via SET.

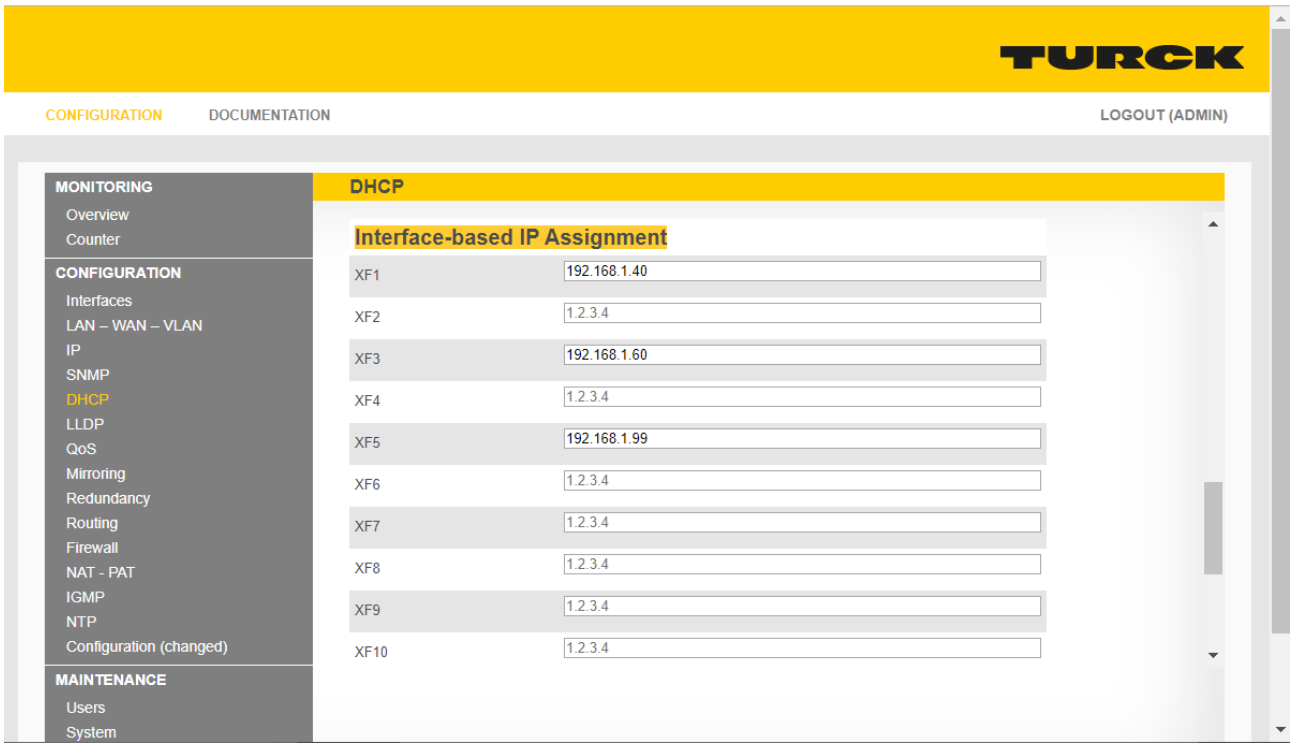

Fig. 37: Web Server – Ethernet port dependent IP address assignment

Active Leases

The section **Active Leases** contains a list of devices that have already been assigned an IP address via DHCP.

8.1.6 LLDP – configuring neighborhodd detection

- ▶ Set up LLDP port by port for incoming (Receive) or for incoming and outgoing (Receive & Transmit).
- ▶ Transfer settings to the device with **SET**.

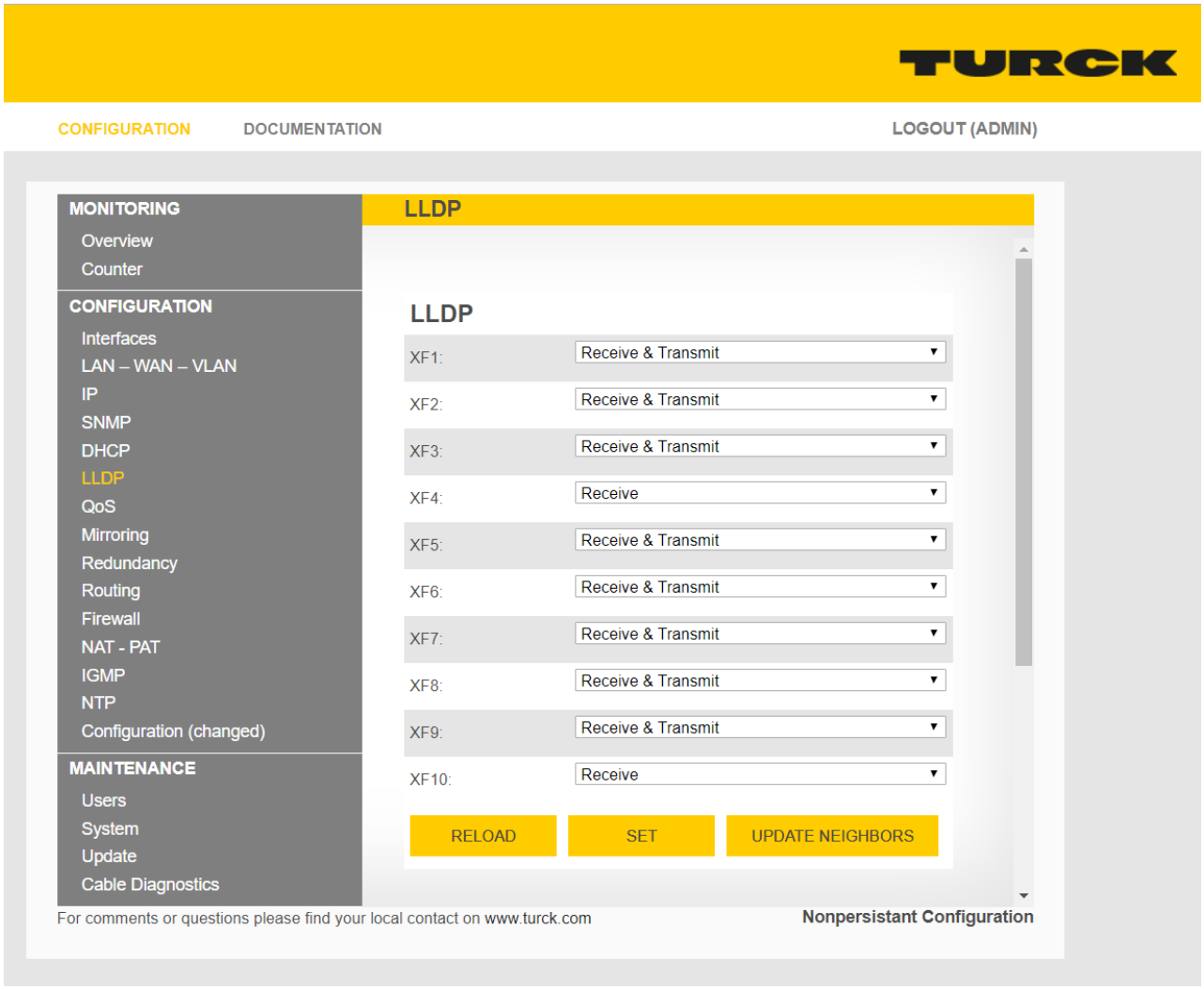

Fig. 38: Webserver – setting up LLDP

➪ The table below shows a list of all neighboring devices.

Device							Port		
Port	DeviceName	Age	Type	Value	Desc	Mgmt-IP	Type	Value	Desc
XF4	DT-XXX	0 day, 04:47:48	local	dt-xxx	Hewlett-Packard HP ProBook 650 G1,A3009DD10303,5CG43501GH	192.168.1.131	local	port-001	
XF4	00:13:3b:a0:14:c6	0 day, 04:45:20	mac	00:13:3b:a0:14:c6		-	mac	00:13:3b:a0:14:c6	
XF6	turck-tben-s2-4iol	0 day, 04:45:30	local	turck-tben-s2-4iol	Turck, TBEN-S2-4IOL, 6814024, HW: 1, SW: V1.6.6.0	192.168.1.125	local	port-001	Turck TBEN-Sx port-001

Fig. 39: Webserver – LLDP – neighboring devices

RELOAD restores the original configuration of the LLDP settings.

UPDATE NEIGHBORS updates the list of adjacent devices.

8.1.7 QoS – prioritizing or classifying data packets

Interface Settings

In the section **Interface Settings** the prioritization or classification of data packets can be set port by port.

The default setting are written in **bold**.

Function	Value	Meaning
XFn	1…10	
Prio Choice	**Default**	Telegrams are processed according to default prioritization or default classification.
	PCP > default	Telegrams that have been prioritized via PCP are always processed first.
	DSCP > default	Telegrams that have been prioritized via DSCP are always processed first.
	PCP > DSCP > default	Telegrams that have been prioritized via PCP are always processed first. This is followed by the processing of telegrams that have been classified via DSCP. All other telegrams are then processed
Default Queue	Q0 (weighted, 1×)	Queue 0: the data is processed with a weighting of 1.
	Q1 (weighted, 2×)	Queue 1: the data is processed with a weighting of 2.
	Q2 (weighted, 3×)	Queue 2: the data is processed with a weighting of 3.
	Q3 (weighted, 6×)	Queue 3: the data is processed with a weighting of 6.
	Q4 (weighted, 12×)	Queue 4: the data is processed with a weighting of 12.
	Q5 (3rd, strict)	Queue 5: Strict priority (3)
	Q6 (2nd, strict)	Queue 6: Strict priority (2)
	Q7 (1st, strict)	Queue 7: Strict priority (1)
Default PCP	Prioritization level according to IEEE 802.1, the prioritization according to PCPs is part of the VLAN tagging.	
	0	Lowest priority, for background processes the process
	1	Best effort
	2	Excellent effort
	3	Critical applications
	4	Video, < 100 ms delay
	5	Voice, < 10 ms delay
	6	Internetwork control
	7	Highest priority, network control

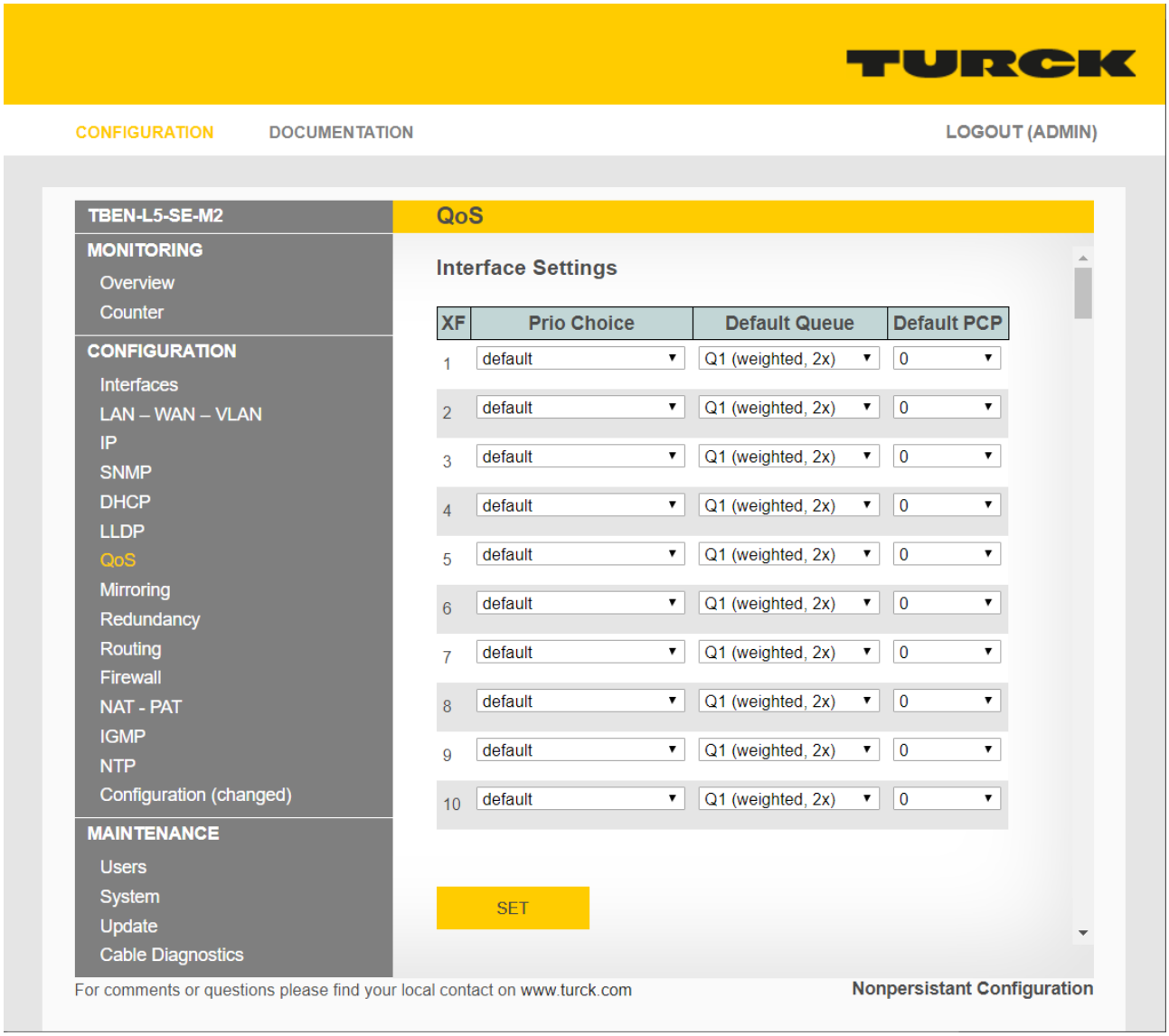

Fig. 40: Web server – QoS: port-wise prioritization of telegrams

- ▶ Set the prioritization for Ethernet ports.
- ▶ Accept the changes via **SET**.

PCP → Queue Mapping

The section **PCP → Queue Mapping** defines to which output queues telegrams are assigned based on their PCP priorities.

Default-settings:

PCP Value	Transmit Queue	PCP Value	Transmit Queue
0	Q1 (weighted, 2×)	4	Q4 (weighted, 12×)
1	Q0 (weighted, 1×)	5	Q5 (3rd, strict)
2	Q2 (weighted, 3×)	6	Q6 (2nd, strict)
3	Q3 (weighted, 6×)	7	Q7 (1st, strict)

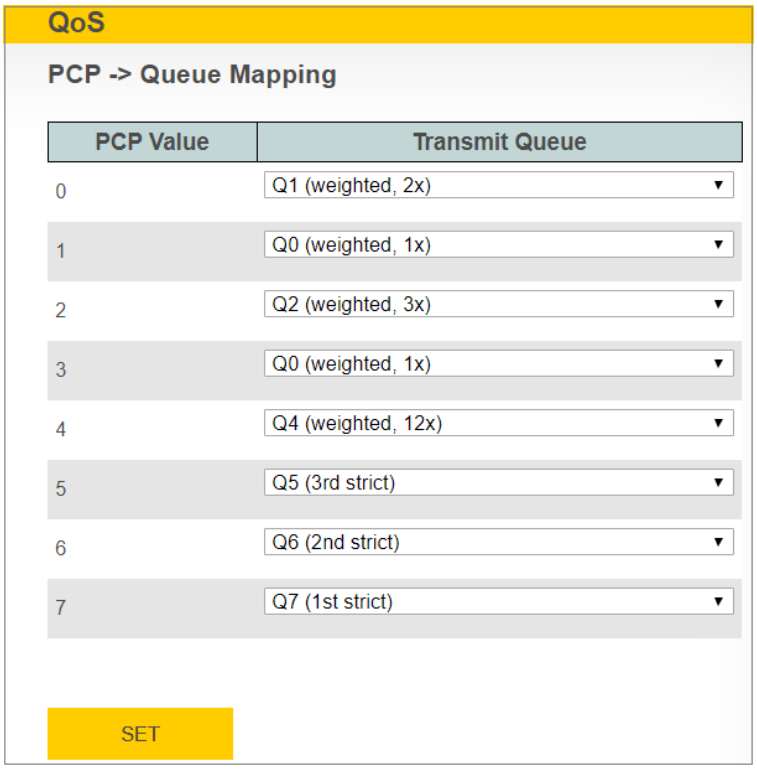

Fig. 41: Web server – QoS: PCP Queue Mapping

- ▶ Set the queue mapping.
- ▶ Accept the changes via **SET**.

DSCP → Queue Mapping

The section **DSCP → Queue Mapping** defines to which output queues telegrams are assigned based on their DSCP priorities.

Default settings:

DSCP Value	Transmit Queue	DSCP Value	Transmit Queue
0…7	Q0 (weighted, 1×)	32…39	Q4 (weighted, 12×)
8…15	Q1 (weighted, 2×)	40…47	Q5 (3rd, strict)
16…23	Q2 (weighted, 3×)	48…55	Q6 (2nd, strict)
24…31	Q3 (weighted, 6×)	56…63	Q7 (1st, strict)

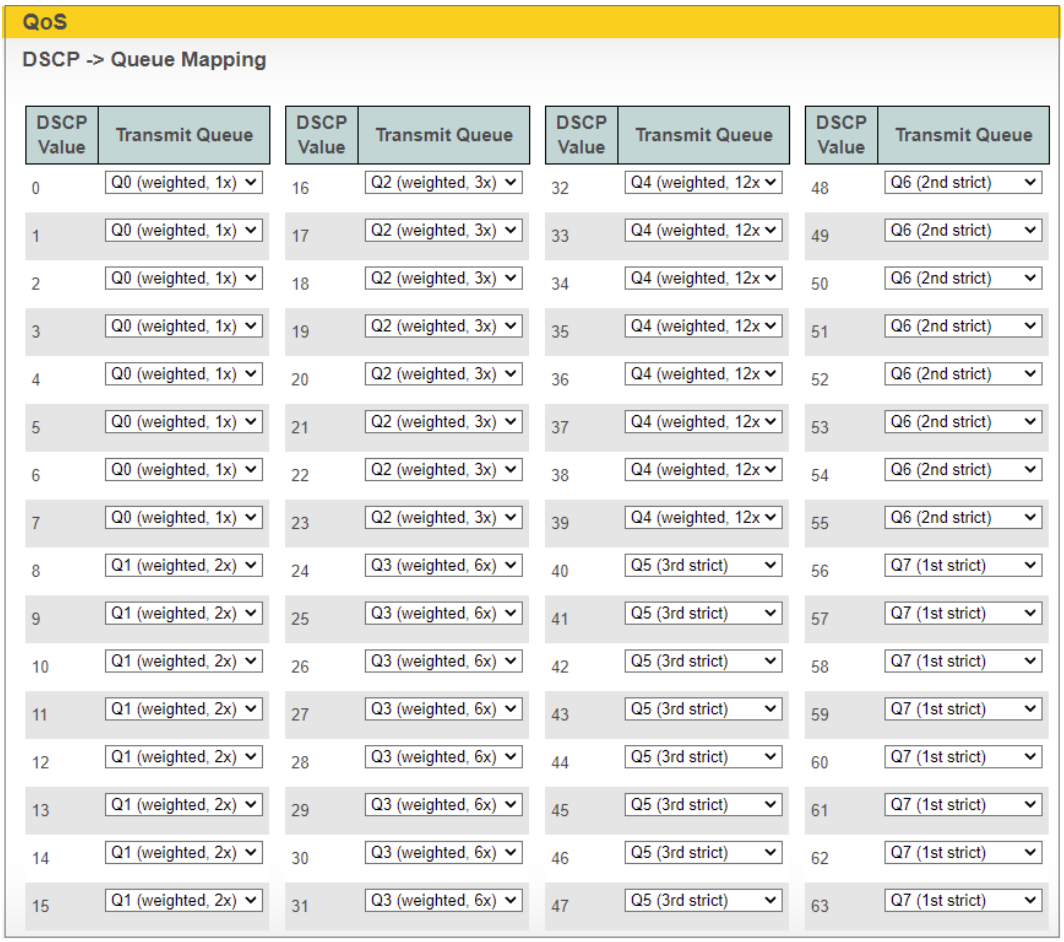

Fig. 42: Web server – QoS: DSCP Queue Mapping

- ▶ Set the queue mapping.
- ▶ Accept the changes via **SET**.

DSCP → PCP Mapping

In the section **DSCP → PCP Mapping**, the DSCP entries are assigned to PCP priorities. In the following example, telegrams that were classified via a DSCP of 5 received the highest priority (7).

Default settings:

DSCP Value	Transmit Queue	DSCP Value	Transmit Queue
0…7	0	21…39	4
8…15	1	40…47	5
16…23	2	48…55	6
24…31	3	56…63	7

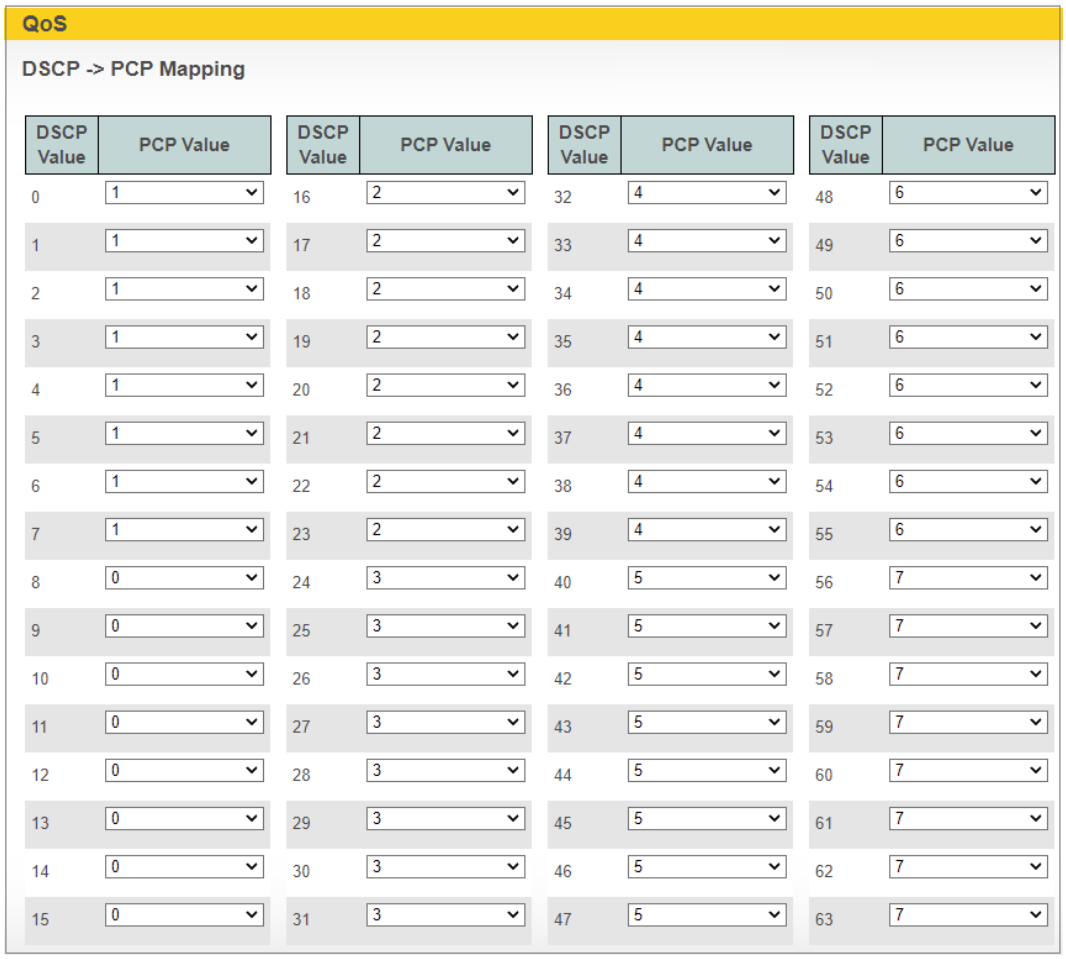

Fig. 43: Web server – QoS: DSCP → PCP queue mapping

- ▶ Set the queue mapping.
- ▶ Accept the changes via **SET**.

8.1.8 Mirroring – configuring the mirroring of switch ports

Mirroring configures the mirroring of one or more switch ports to another port. Only the incoming telegrams (mirror recieve only), the outgoing telegrams (mirror transmit only) or both directions (mirror revceive and transmit) can be mirrored.

- ▶ Define the port to which the port or ports to be mirrored are to be mirrored under **Destination → Destination Interface**.
- ▶ Activate the desired mirroring at the switch ports XF1...XF10.
- ▶ Transfer settings to the device via **SET**.

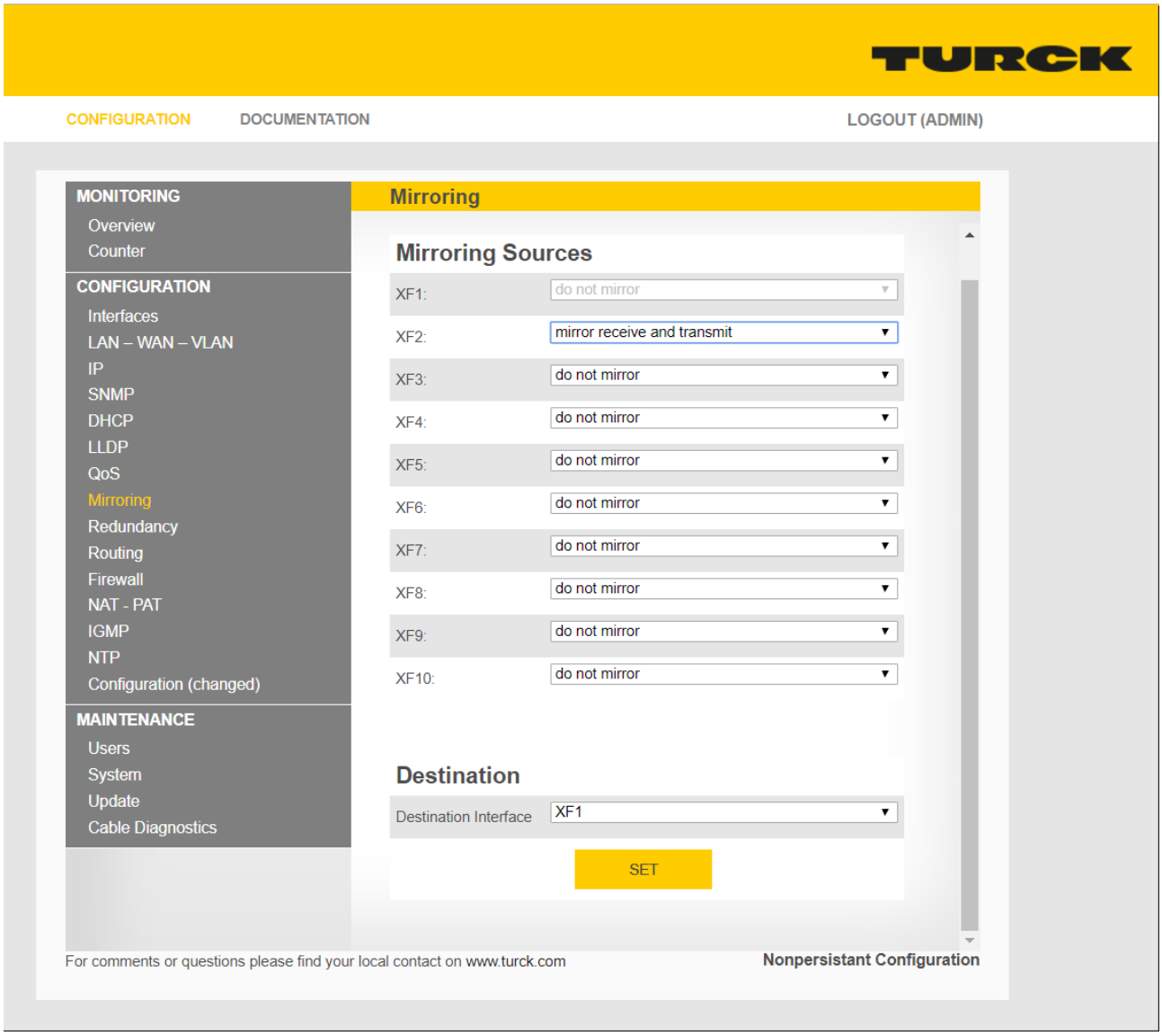

Fig. 44: Web server - configuring mirroring

8.1.9 Redundancy – configuring network redundancy

(R)STP Variant

The section **(R)STP Variant** defines which network redundancy protocol [▶ 11] is used in the network zones LAN, WAN, LAN-VLAN and WAN-VLAN.

- ▶ Select the network redundancy protocol.
- ▶ Send the configuration to the device via **SET**.

8.1.10 Routing – configuring rules (routes)

Routing defines forwarding rules (routes) for data transmission between the configurable LAN and WAN network zones.

NOTE
IP forwarding (forwarding of data packets between networks with different IP address ranges) must be activated.

Add Route

Example:

Telegrams from station 1 at port 2 of the switch will be forwarded to station 2 of another network.

Station 1	Station 2
IP address: 10.17.2.12	IP address: 192.168.1.100
WAN: IP address: 10.17.2.0	LAN: IP address: 192.168.1.0
Subnet mask: 255.255.255.0	Subnet mask: 255.255.255.0

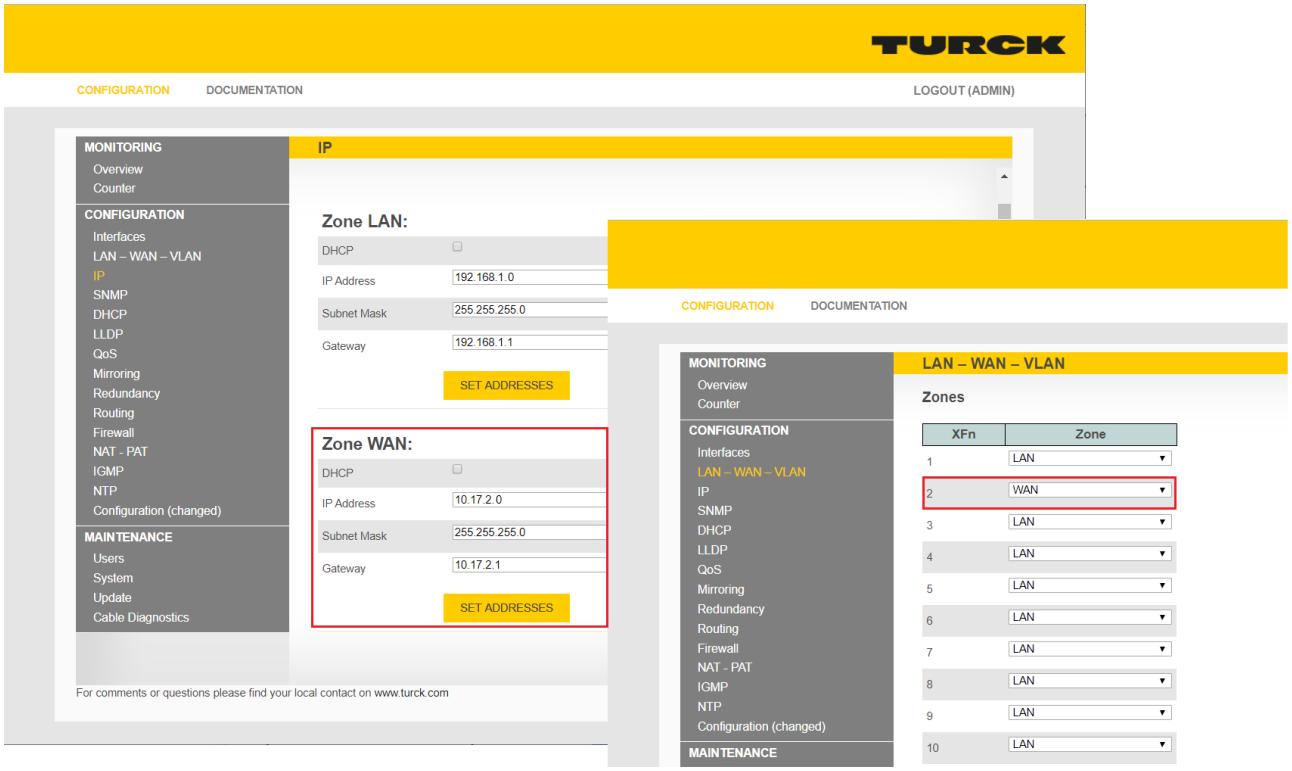

Fig. 45: Web server – IP addresses for LAN and WAN

Make the following settings and add rules using **ADD**.

Function	Value	Meaning
Source Network	10.17.2.12	Address of station 1 in the WAN
Source Subnet Mask	255.255.255.0	Subnet mask of the WAN
Outgoing Zone	LAN	
Next Hop/Gateway	192.168.1.100	IP address of station 2
Metric	0	Number of networks in between

8.1.11 Firewall – configuring firewall rules

The firewall is deactivated when the device is delivered and must first be activated, e.g. via a block-any rule (all telegrams are blocked). After that, exceptions to this rule can be defined.

Firewall rules can be created separately for incoming and outgoing packets.

In addition, forwarding rules can be defined.

Application example – defining firewall rules

Access to the switch via HTTP (port 80) is blocked. The device can only be accessed from outside the WAN via HTTPS. For this purpose, port 443 is enabled for HTTPS. All other ports are blocked.

- ▶ First incoming rule, which allows access via port 433 for HTTPS:

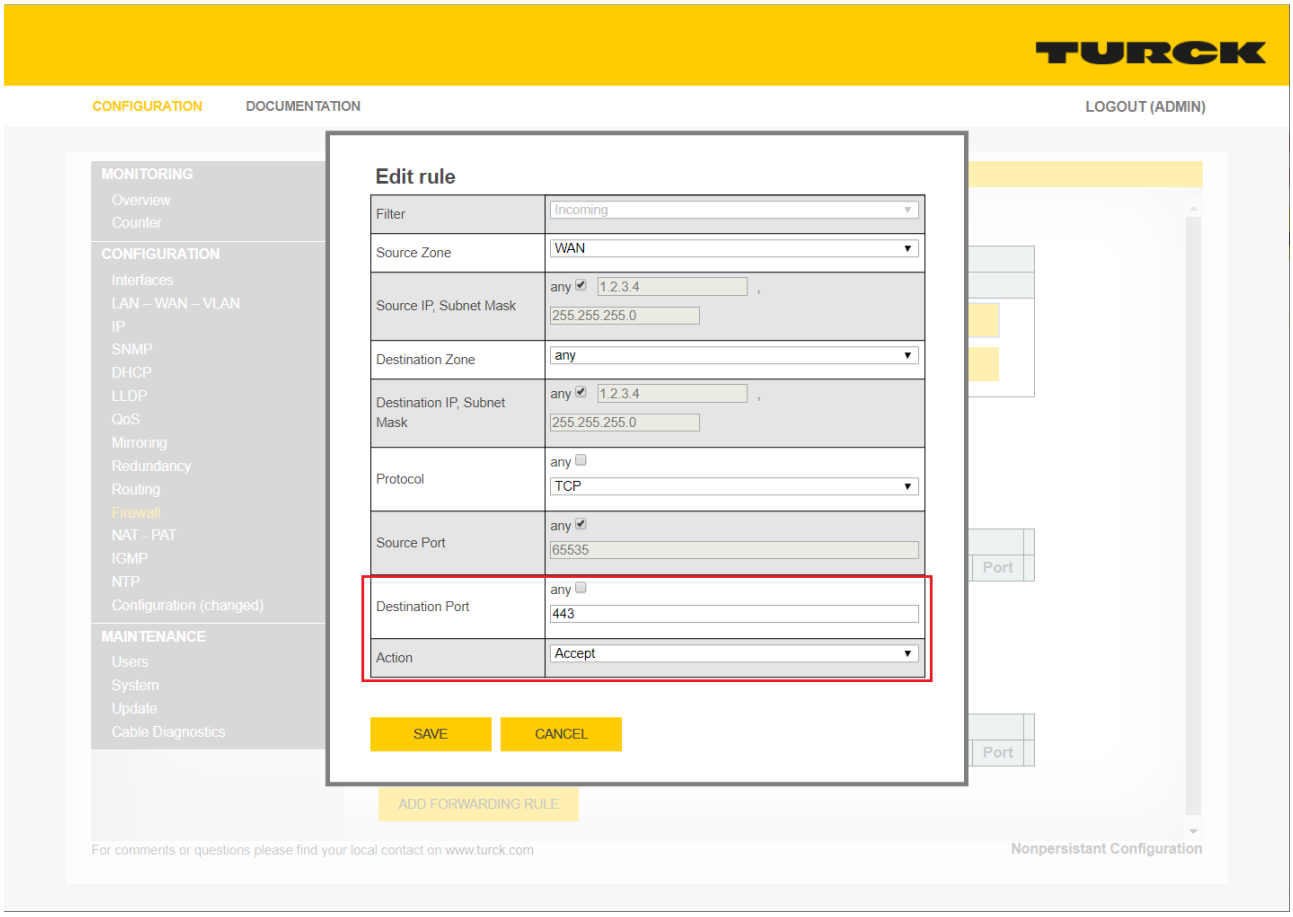

Fig. 46: Web server – enable access via HTTPS

- ▶ Create firewall rule via **SAVE**.

▶ Set up second incoming rule that blocks access via HTTP (port 80):

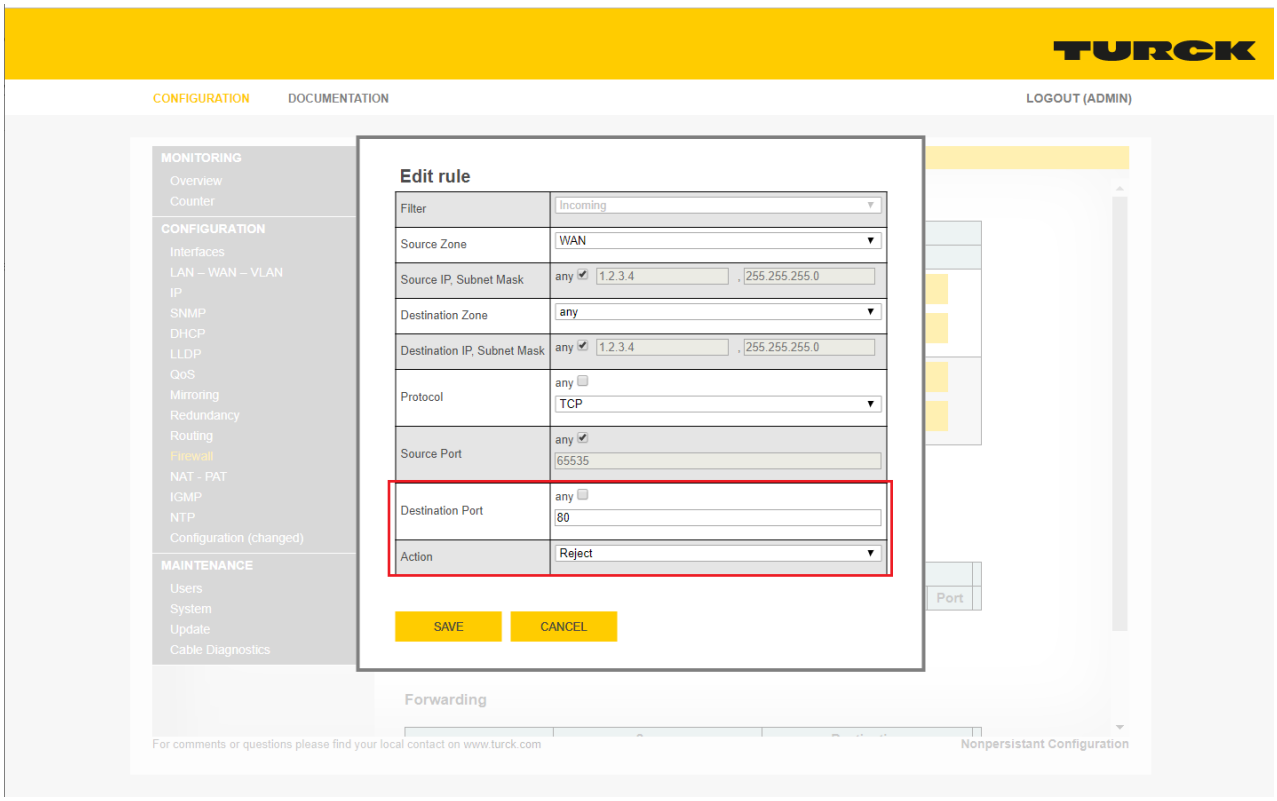

Fig. 47: Web server – block access via HTTP

▶ Create firewall rule via **SAVE**.

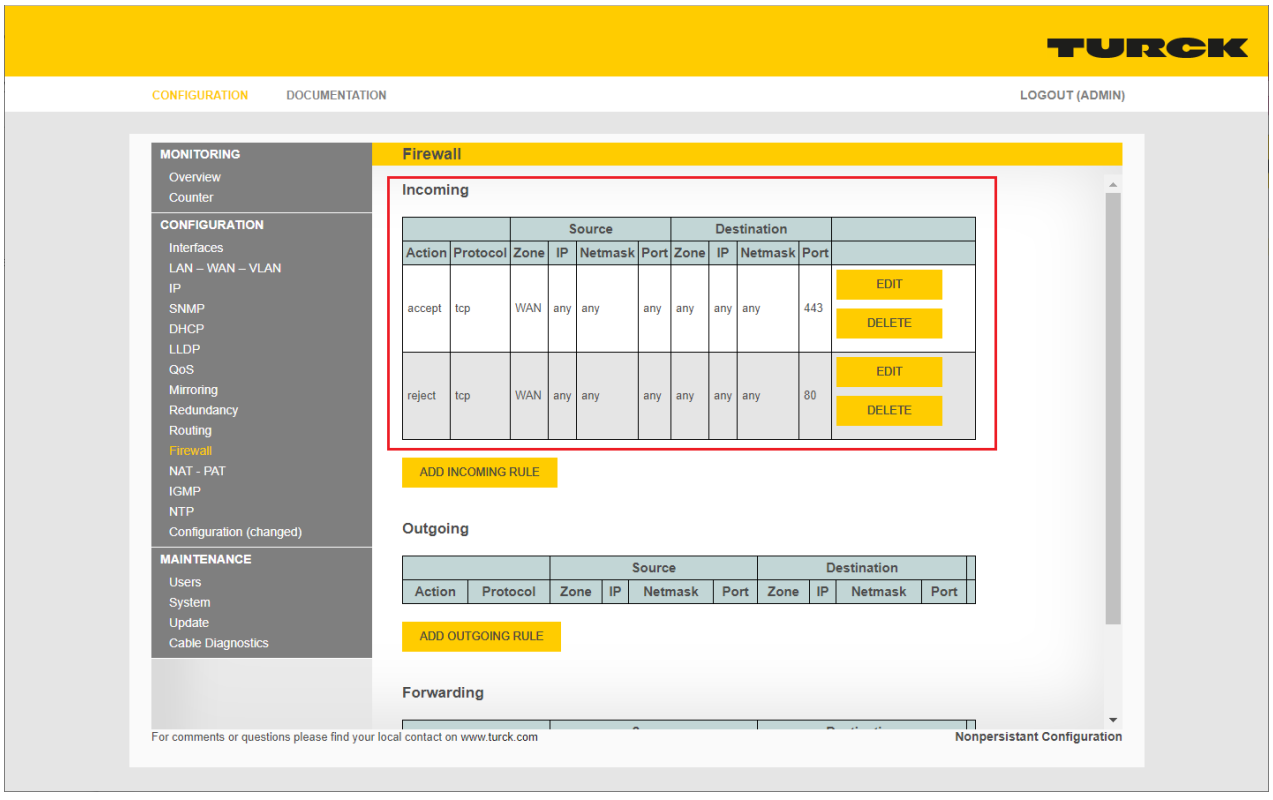

Fig. 48: Web server – incoming rules

8.1.12 NAT – configuring NAT/PAT rules

The NAT – PAT page is used to configure rules for NAT (Network Address Translation) and PAT (Port Address Translation).

NAT (Network Address Translation)

In NAT, IP addresses of one network are translated into IP addresses of another network.

PAT (Port Address Translation)

With PAT, all IP addresses of a network are mapped with port numbers (TCP/UDP ports). PAT rules define how data traffic is redirected from an incoming port to another port.

NOTE
IP forwarding (forwarding of data packets between networks with different IP address ranges) must be activated.

Add NAT Rule (Source NAT)

In the Add NAT Rule section, rules for the translation of IP addresses for outgoing telegrams are created.

Example:

Function	Value	Meaning
Desired priority	1…64	Order number to prioritize the rules, beginning with 1 and assigned consecutively
Source IP Network	12.222.2.0	IP address of an external network
Source IP Subnet Mask	255.255.255.0	Subnet mask of the external network
Outgoing Zone	LAN WAN	IP addresses of telegrams which are set here and sent from the network zone to participants of the source network (Source IP Network) are translated into IP addresses of the other network.

- ▶ Creating a Source NAT rule.
- ▶ Add the rule via **ADD** and send the rule to the device via **SET**.

Add Destination NAT/PAT Rule (Destination NAT)

In the **Add Destination NAT/PAT Rule** section, rules for the translation of IP addresses are created. For PAT rules, port numbers are specified in addition to IP addresses.

Function	Value	Meaning
Index	1…64	Order number to prioritize the rules, beginning with 1 and assigned consecutively
Incoming Zone	LAN WAN	Network zone from which incoming telegrams are to be forwarded
Original IP	12.222.2.95	IP address assigned to the device in the external network
Destination IP	192.168.1.15	IP address in the internal network via which an external device device is to be accessed
Protocol	TCP	Defines for which telegrams the rule applies (TCP, UDP, all = OFF).
Incoming Dest. Port	80	Port number of the service (e.g. web server = port 80)
Outgoing Dest. Port	80	

- ▶ Sett the NAT/PAT rule.
- ▶ Add the rule via **ADD** and send the rule to the device via **SET**.

Example:

The web server of a TBEN-L5-PLC-10 (original IP: 12.222.2.95) in a plant network (WAN: 12.222.2.0) is accessed from a PC in the company network (LAN: 192.168.1.0) via a defined IP address (destination IP).

For this purpose, two PAT rules are defined, one for each communication direction.

- PAT rule 1:

Function	Value	Meaning
Index	1	
Incoming Zone	WAN	Plant network
Original IP	12.222.2.95	IP address of the TBEN-L5-PLC-10 in the WAN that is to be accessed via the LAN IP address 192.168.1.15 (Destination IP)
Destination IP	192.168.1.15	
Protocol	TCP	Defines for which telegrams the rule applies (TCP, UDP, all = OFF).
Incoming Dest. Port	80	Port number of the web server
Outgoing Dest. Port	80	

- PAT rule 2:

Function	Value	Meaning
Index	2	
Incoming Zone	LAN	Company network
Original IP	192.168.1.15	IP address in the LAN via which the TBEN-L5-PLC-10 is to be accessed
Destination IP	12.222.2.95	IP address of the TBEN-L5-PLC-10 in the WAN that is to be accessed via the LAN IP address 192.168.1.15 (Destination IP)
Protocol	TCP	Defines for which telegrams the rule applies (TCP, UDP, all = OFF).
Incoming Dest. Port	80	Port number of the web server
Outgoing Dest. Port	80	

8.1.13 IGMP – configuring Multicast

The device supports the functions **IGMP Snooper** and **IGMP Querier**.

The IGMP configuration is only effective if **Flood unknown Multicasts/Unicasts** under **Interfaces → Switching** is set to **off** or **IGMP only**.

NOTE
In PROFINET networks, the **IGMP Snooper** function must be deactivated.

Function	Value	Meaning
Snooper		If the IGMP Snooper function is activated, IGMP telegrams are received and evaluated. The device logs on to receive multicast telegrams by sending IGMP messages to a router and is recorded as a receiver in a multicast table.
Querier		If the IGMP Querier function is activated, the device itself also sends IGMP requests, which trigger responses from connected IGMP-capable participants.
Version	1	A host can join a multicast group. Logoff is not implemented. After a timeout, the host is deregistered.
	2	Starting with IGMP version 2, devices can log off from receiving IGMP messages with a leave message.
Interval [s]	0.01…1000000 s	Query (Snooper) or transmit interval (Querier)
Time out [s]	0.01…1000000 s	Time after which a device no longer receives multicast telegrams and is automatically deleted from the multicast table.

IGMP Settings

In the **IGMP Settings** section, the IGMP settings are made separately for the two networks LAN and WAN.

- Under LAN or WAN, activate the IGMP **Snooper** and/or or **Querier** function.
- Select the IGMP version.
- Define the polling or transmission interval.
- Send settings to the device via **SET IGMP**.

Active IGMP

The **Active IGMP** table shows all active IGMP requests and responses from connected devices.

8.1.14 NTP – configuring the time server

The switch is an NTP relay. The device requests date and time information from an external NTP server and makes it available to the connected devices.

- Enable time synchronization via NTP server with enable.
- Define NTP time server using the IP address of the server. In this example, the time server of the TU Berlin with the IP address 130.149.17.21 is used.
- Set the interval for the time query.
- Use **SET CONFIG** to send changes to the device.

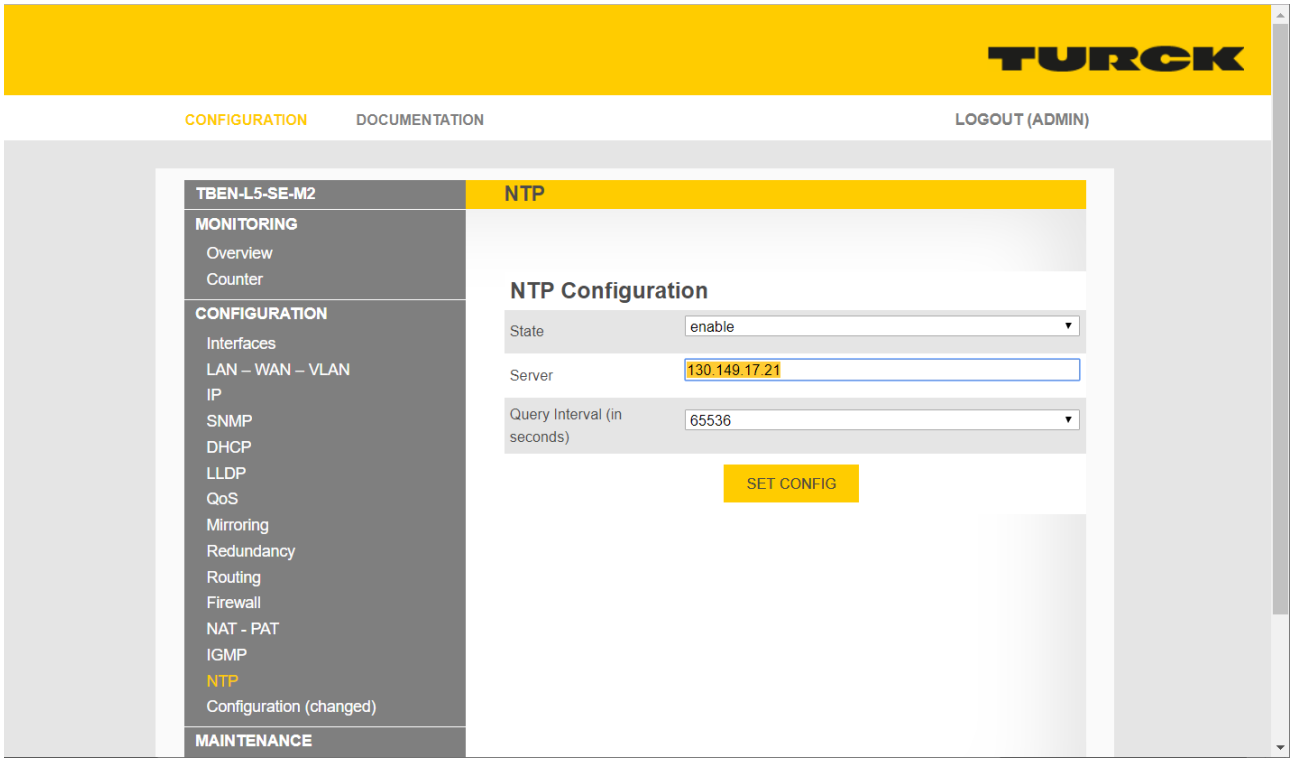

Fig. 49: Webserver – DHCP server configuration

Hans Turck GmbH & Co. KG | T +49 208 4952-0 | F +49 208 4952-264 | more@turck.com | www.turck.com

8.1.15 Configuration – accept, reset, load or download the configuration

NOTE

If changes have been made to the configuration compared to the configuration stored in the device, this is indicated by the entry **Nonpersistent Configuration** at the bottom of the web server screen. Configuration changes are only stored in the device until a device failure or power reset.

- If the configuration is to be accepted as a permanent configuration: Activate the configuration via **Make current configuration persistent** → **SAVE** as permanent configuration.

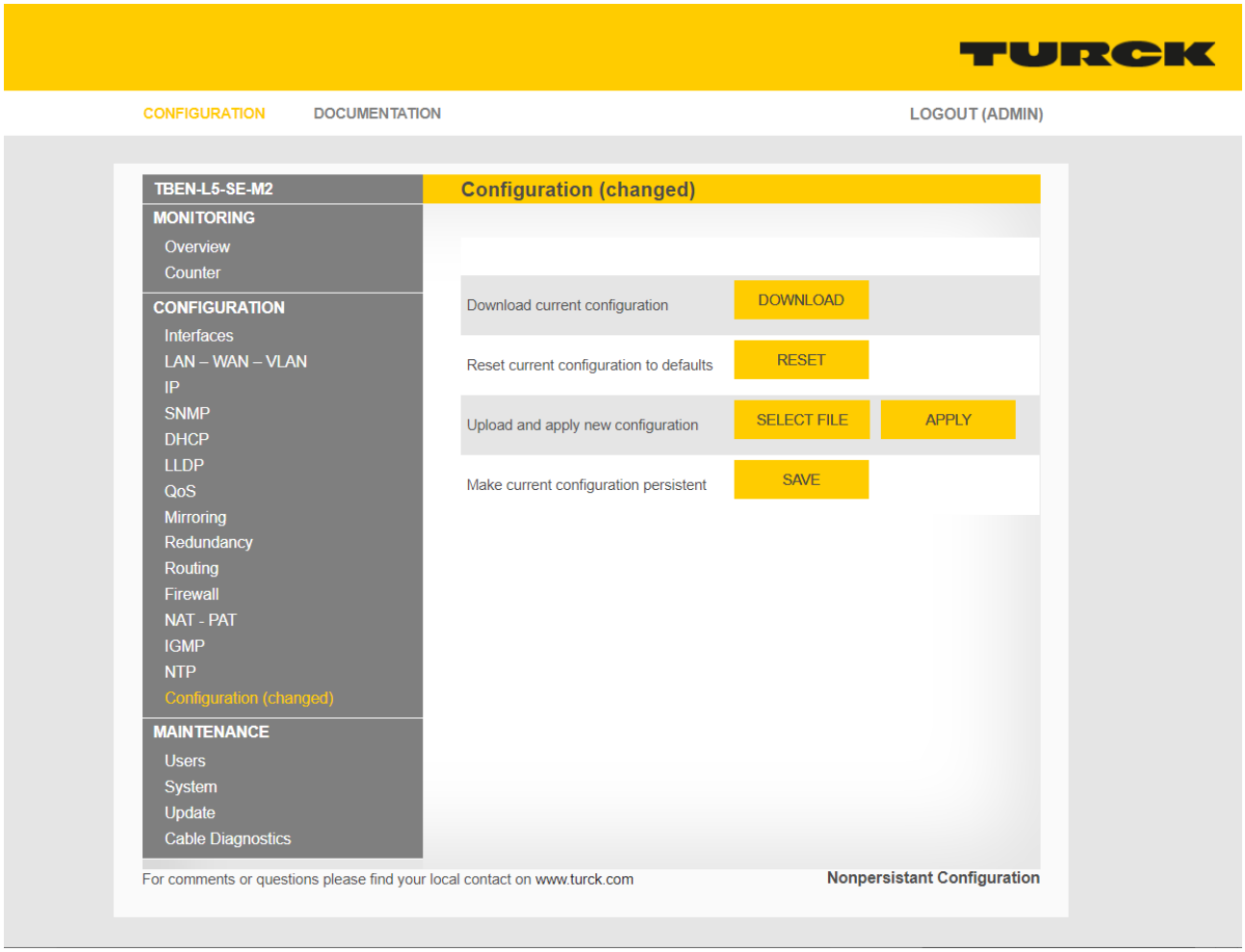

Fig. 50: Web server – configuration

Save configuration permanently in the device

- Accept changed configuration via **Make current configuration persistent** as permanent configuration.

Resetting the configuration to default configuration

- Restore configuration via **Reset current configuration to defaults**.

Load saved configuration

- Select the file with the saved configuration (*.cfg) via **Upload and apply new configuration → SELECT FILE**.
- Write the configuration to the device via **APPLY**. The configuration is not stored permanently in the device.
- To save the configuration permanently in the device, use **Make current configuration persistent → SAVE** as permanent configuration.

Storing the configuration

- Save configuration via **Download current configuration**. The configuration is stored in the folder that is defined as the download folder in the browser.

8.2 Downloading the configuration to the device via USB stick

The configuration is transferred via a USB stick using a command file (cmd.json). The file is available on the product page of the switch at ww.turck.com or can be created in a text editor as shown below.

✓ The configuration of the device was downloaded from the web server via **Configuration → Download current configuration**.

▶ Download the file **cmd.json** from the folder **...\usb_commands\apply_and_save_config** and the configuration file ***.cfg** to the USB stick.

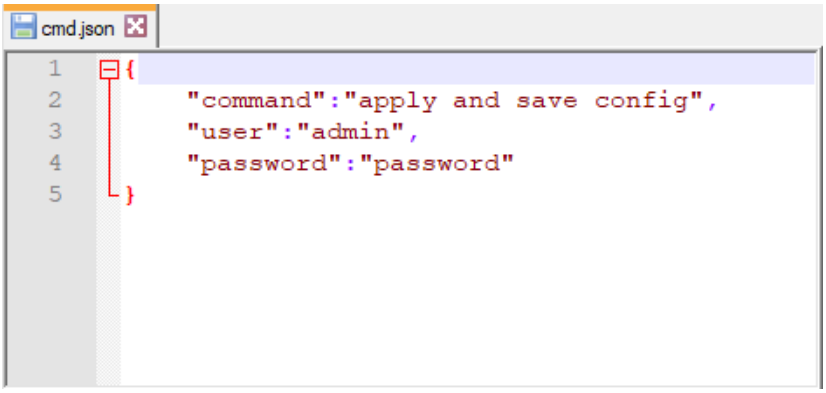

Fig. 51: Program file "cmd.json"

Program code:

```
{"command":"apply and save config",
"user":"admin",
"password":"password"}
```

▶ Insert the USB stick with the file **cmd.json** into the device.
⇨ The RUN LED flashes 3 × green at 1 Hz.
⇨ The RUN LED flashes green at 0.5 Hz.

▶ Within 30 seconds, hold down the Set button for at least 3 seconds to start the update.
⇨ The RUN LED turns off.
⇨ When the RUN LED flashes green (1 Hz), the transfer of the configuration to the device is complete.

▶ Remove the USB stick.

Compatible USB sticks

FAT or FAT32 formatted USB sticks can be connected to the USB host port. It is not possible to connect NTFS formatted sticks or USB devices such as external hard disks, keyboards, PC mice, etc.

Depending on the power consumption of the USB stick, compatibility problems may occur. To ensure error-free data exchange, Turck recommends using the industrial USB stick USB 2.0 Industrial Memory Stick (ID 6827348).

9 Operating

9.1 LED displays

The device has the following LED indicators:

- Power supply
- Status

LED PWR	Meaning
Off	No voltage connected or under voltage at V1
Green	Voltage at V1 OK

NOTE
Each of the Ethernet ports XF1…XF10 has an LED L/A.

LED L/A	Meaning
Off	No Ethernet connection
Green	Ethernet connection established,100 Mbps (XF1…XF10) or respectively 1 Gbps (XF9 and XF10)
Yellow	Ethernet connection established, 10 Mbps
Green flashing	Data transfer, 100 Mbps (XF1…XF10) or respectively 1 Gbps (XF9 and XF10)
Yellow blinking	Data transfer, 10 Mbps

LED BUS
No function

LED ERR
No function

NOTE
The flashing pattern of the RUN LED indicates the configuration process when using the USB host function [▶ 57].

LED RUN	Meaning
Off	No USB function active
Green flashing (twice, 1 Hz)	USB host function is being activated
Green flashing (0.5 Hz)	USB function active

LED APP	Meaning
White flashing	Wink command active

9.2 Monitoring function

9.2.1 Monitoring – Overview (device overview)

The **Overview** page shows an overview of all Ethernet interfaces of the device, the device data (name, firmware version, etc.) and the current device settings (VLAN, DHCP, routing, etc.).

A click on the respective entries opens the corresponding configuration page.

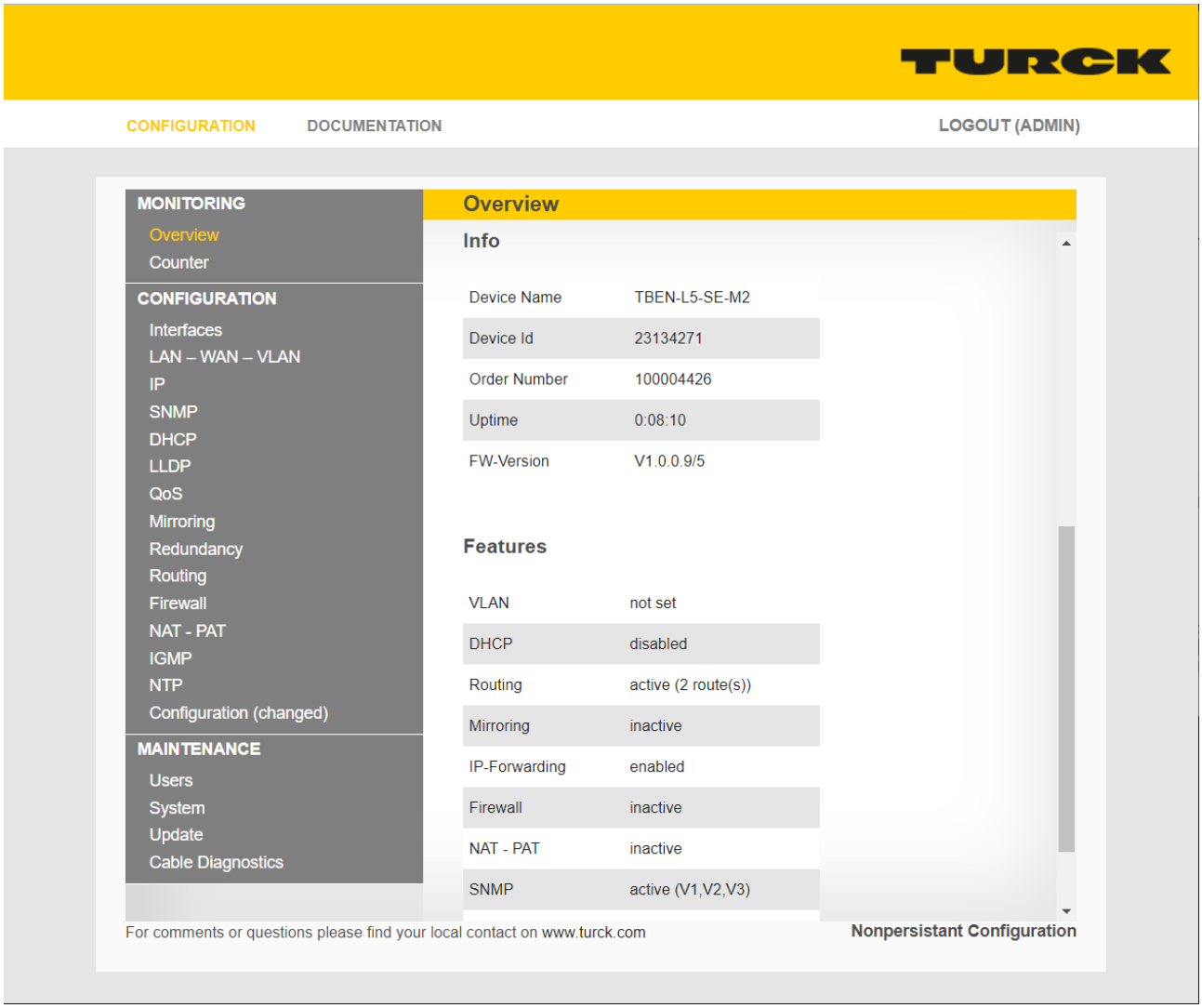

Fig. 52: Web server – overview

9.2.2 Monitoring – Counter (network load monitoring)

The **Counter** page shows all sent and received telegrams as well as the calculated network load in percent.

The values can also be displayed graphically:

- ▶ Select the values by double-clicking them.
- ▶ Use the Graph button to switch to the graphical view.

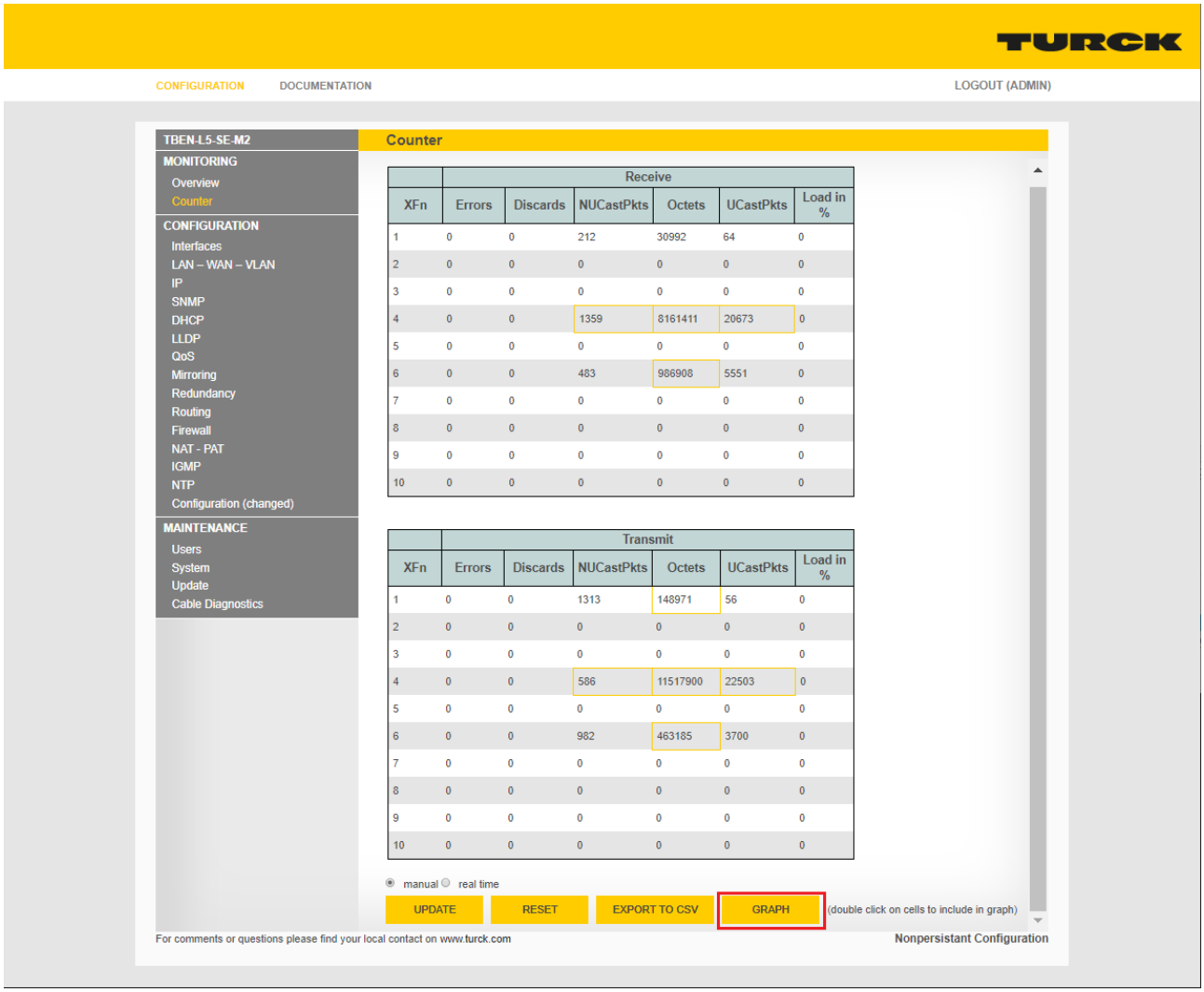

Fig. 53: Webserver – Counter (tables)

➪ The values are displayed graphically.

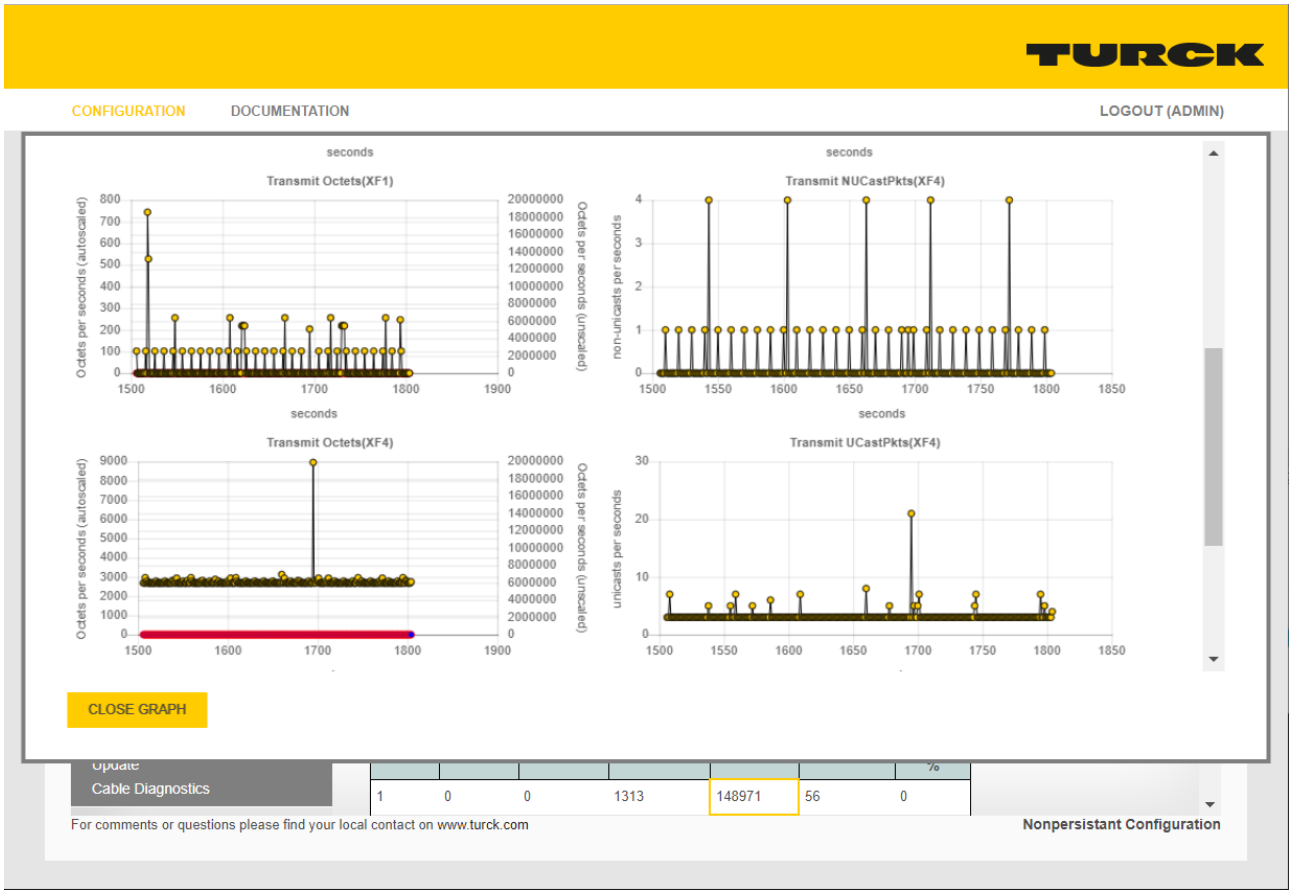

Fig. 54: Webserver – Counter (graphical representation)

9.3 Cable diagnostics

The cable diagnostics detects cable breaks in the Ethernet line.

- ▶ Select the Ethernet ports for which line diagnostics are to be performed.
- ▶ Start line diagnostics via **START CABLE DIAGNOSTCS**.
- ⇨ The lines on the selected Ethernet ports are checked.
- ⇨ Cable breaks are detected and localized wire by wire.

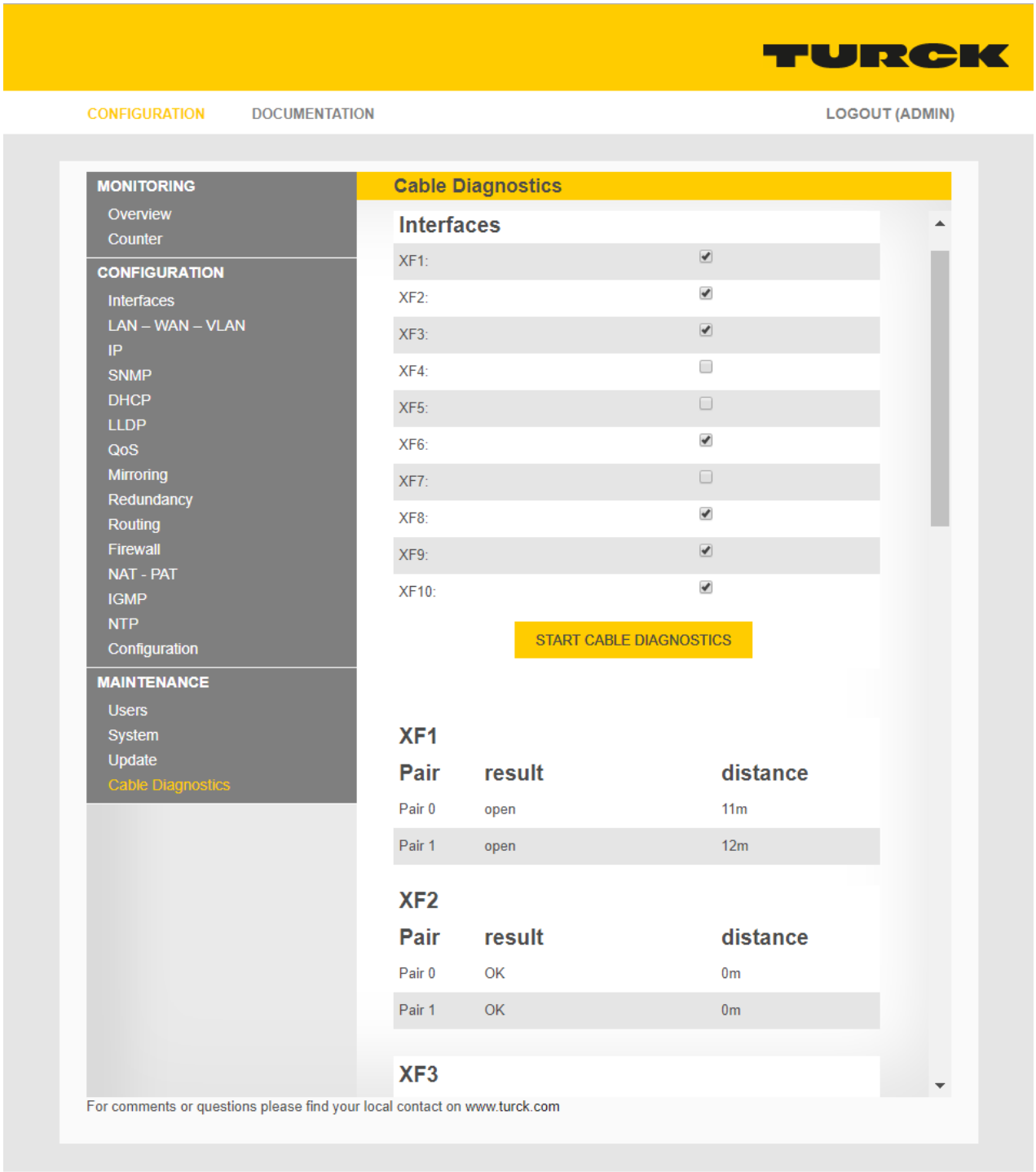

Fig. 55: Web server – cable diagnostics

Hans Turck GmbH & Co. KG | T +49 208 4952-0 | F +49 208 4952-264 | more@turck.com | www.turck.com

10 Troubleshooting

If the device does not function as expected, first check whether ambient interference is present. If there is no ambient interference present, check the connections of the device for faults.

If there are no faults, there is a device malfunction. In this case, decommission the device and replace it with a new device of the same type.

11 Maintenance

Ensure that the plug connections and cables are always in good condition.

The devices are maintenance-free, clean dry if required.

12 Repair

The device must not be repaired by the user. The device must be decommissioned if it is faulty. Observe our return acceptance conditions when returning the device to Turck.

12.1 Returning devices

Returns to Turck can only be accepted if the device has been equipped with a Decontamination declaration enclosed. The decontamination declaration can be downloaded from
https://www.turck.de/en/retoure-service-6079.php
and must be completely filled in, and affixed securely and weather-proof to the outside of the packaging.

13 Disposal

The devices must be disposed of correctly and must not be included in general household garbage.

14 Technical Data

Technical data	
Power supply	
Supply voltage	24 VDC
Permissible range	8…30 VDC with load dump protection
Current feedthrough	
■ TBEN-L4/TBEN-L5 (X1 to X2)	Max. 9 A per voltage group
■ TBEN-LL (XD1 to XD2)	Max. 16 A per voltage group
Current consumption at 24 VDC	Max. 200 mA
Power loss	≤ 4,8 W
Connectors	
Power supply	
■ TBEN-L4	■ X1: 7/8“ male connector, 4-pin ■ X2: 7/8'' female connector, 4-pin
■ TBEN-L5	■ X1: 7/8“ male connector, 5-pin ■ X2: 7/8'' female connector, 5-pin
■ TBEN-LL	■ XD1: M12 male connector, 5-pin, L-coded ■ XD2: M12 female connector, 5-pin, L-coded
Ethernet	2 x M12, 8-pin, X-coded 8 x M12, 4-pin, D-coded
Permissible torques ■ Ethernet ■ Mounting (M6 screws)	 0.6 Nm 1.5 Nm
Isolation voltages	
V1 to V2	≤ 500 V AC
V1/V2 to field bus	≤ 500 V AC
System data	
Transmission rate	XF1…XF8: 10/100 Mbps XF9…XF10: 10/100/1000 Mbps
Web server	Integrated Default IP address: 192.168.1.254
Mounting	
Type of mounting	Via 2 mounting holes, Ø 6.3 mm
Mounting distance (device to device)	≥ 50 mm Valid for operation in the ambient temperatures mentioned below with sufficient ventilation as well as maximum load (horizontal mounting). For low simultaneity factors and low ambient temperatures, mounting distances of < 50 mm may also be realizable.
Standard/directive conformity	
Vibration test	According to EN 60068-2-6
Acceleration	Up to 20 g
Shock test	According to EN 60068-2-27
Drop and topple	According to IEC 60068-2-31/IEC 60068-2-32

Technical data	
Electro magnetic compatibility	According to EN 61131-2
Approvals and certificates	CE UL UV-resistant according to DIN EN ISO 4892-2A (2013)
General Information	
Dimensions (B × L × H)	64 × 230.4 × 39 mm
Operating temperature	-40…+70 °C
Storage temperature	-40…+85 °C
Relative humidity	100 %, indoor use (UL only)
Overvoltage category	II
Weight	605 g
Operating height	Max. 5000 m
Protection class	IP65 IP67/IP69K (not evaluated by UL)
Pollution degree	2
MTTF	
■ TBEN-L4-SE-M2 and TBEN-L5-SE-M2	82 years acc. to SN 29500 (Ed. 99) 20 °C
■ TBEN-LL-SE-M2	81 years acc. to SN 29500 (Ed. 99) 20 °C
Housing material	PA6-GF30
Halogen-free	Yes

FCC declaration

NOTE
This device complies with the limits for a Class A digital device, according to Part 15 of the FCC Rules. Operation of this equipment in a residential area may cause harmful interference. In this case, the user must correct the interference at his own expense.

15 Appendix: Approvals and Markings

Approvals	Marking according to ATEX directive	EN 60079-0/-7/-31
ATEX approval no.: TÜV 20 ATEX 264795 X	⟨Ex⟩ II 3 G ⟨Ex⟩ II 3 D	Ex ec IIC T4 Gc Ex tc IIIC T115 °C Dc
IECEx approval no.: IECEx TUN 20.0010X		Ex ec IIC T4 Gc Ex tc IIIC T115 °C Dc

Ambient temperature T_{amb}.: -25 °C…+60 °C

Type designation	TBEN-L_-SE-…
Supply voltage	24 VDC ±10 %
Input current I_{max}	9 A (total per module)
Output current I_{max}	1,5 A (per output)

16 Turck Subsidiaries - Contact Information

Germany	Hans Turck GmbH & Co. KG Witzlebenstraße 7, 45472 Mülheim an der Ruhr **www.turck.de**
Australia	Turck Australia Pty Ltd Building 4, 19-25 Duerdin Street, Notting Hill, 3168 Victoria **www.turck.com.au**
Belgium	TURCK MULTIPROX Lion d'Orweg 12, B-9300 Aalst **www.multiprox.be**
Brazil	Turck do Brasil Automação Ltda. Rua Anjo Custódio Nr. 42, Jardim Anália Franco, CEP 03358-040 São Paulo **www.turck.com.br**
China	Turck (Tianjin) Sensor Co. Ltd. 18,4th Xinghuazhi Road, Xiqing Economic Development Area, 300381 Tianjin **www.turck.com.cn**
France	TURCK BANNER S.A.S. 11 rue de Courtalin Bat C, Magny Le Hongre, F-77703 MARNE LA VALLEE Cedex 4 **www.turckbanner.fr**
Great Britain	TURCK BANNER LIMITED Blenheim House, Hurricane Way, GB-SS11 8YT Wickford, Essex **www.turckbanner.co.uk**
India	TURCK India Automation Pvt. Ltd. 401-403 Aurum Avenue, Survey. No 109 /4, Near Cummins Complex, Baner-Balewadi Link Rd., 411045 Pune - Maharashtra **www.turck.co.in**
Italy	TURCK BANNER S.R.L. Via San Domenico 5, IT-20008 Bareggio (MI) **www.turckbanner.it**
Japan	TURCK Japan Corporation Syuuhou Bldg. 6F, 2-13-12, Kanda-Sudacho, Chiyoda-ku, 101-0041 Tokyo **www.turck.jp**
Canada	Turck Canada Inc. 140 Duffield Drive, CDN-Markham, Ontario L6G 1B5 **www.turck.ca**
Korea	Turck Korea Co, Ltd. B-509 Gwangmyeong Technopark, 60 Haan-ro, Gwangmyeong-si, 14322 Gyeonggi-Do **www.turck.kr**
Malaysia	Turck Banner Malaysia Sdn Bhd Unit A-23A-08, Tower A, Pinnacle Petaling Jaya, Jalan Utara C, 46200 Petaling Jaya Selangor **www.turckbanner.my**

Mexico	Turck Comercial, S. de RL de CV Blvd. Campestre No. 100, Parque Industrial SERVER, C.P. 25350 Arteaga, Coahuila **www.turck.com.mx**
Netherlands	Turck B. V. Ruiterlaan 7, NL-8019 BN Zwolle **www.turck.nl**
Austria	Turck GmbH Graumanngasse 7/A5-1, A-1150 Wien **www.turck.at**
Poland	TURCK sp.z.o.o. Wroclawska 115, PL-45-836 Opole **www.turck.pl**
Romania	Turck Automation Romania SRL Str. Siriului nr. 6-8, Sector 1, RO-014354 Bucuresti **www.turck.ro**
Russian Federation	TURCK RUS OOO 2-nd Pryadilnaya Street, 1, 105037 Moscow **www.turck.ru**
Sweden	Turck Sweden Office Fabriksstråket 9, 433 76 Jonsered **www.turck.se**
Singapore	TURCK BANNER Singapore Pte. Ltd. 25 International Business Park, #04-75/77 (West Wing) German Centre, 609916 Singapore **www.turckbanner.sg**
South Africa	Turck Banner (Pty) Ltd Boeing Road East, Bedfordview, ZA-2007 Johannesburg **www.turckbanner.co.za**
Czech Republic	TURCK s.r.o. Na Brne 2065, CZ-500 06 Hradec Králové **www.turck.cz**
Turkey	Turck Otomasyon Ticaret Limited Sirketi Inönü mah. Kayisdagi c., Yesil Konak Evleri No: 178, A Blok D:4, 34755 Kadiköy/ Istanbul **www.turck.com.tr**
Hungary	TURCK Hungary kft. Árpád fejedelem útja 26-28., Óbuda Gate, 2. em., H-1023 Budapest **www.turck.hu**
USA	Turck Inc. 3000 Campus Drive, USA-MN 55441 Minneapolis **www.turck.us**

TURCK

Over 30 subsidiaries and over
60 representations worldwide!

100013016 | 2021/11

www.turck.com