

# PROmesh P10X

## User Manual



PROFINET/Industrial Ethernet IP67-Switch

Indu-Sol GmbH

Blumenstraße 3

D-042626 Schmölln

Phone: +49 (0)34491 / 58 18 0

Fax: +49 (0)34491 / 5818-99

Email: [info@indu-sol.com](mailto:info@indu-sol.com)

Web: <https://www.indu-sol.com>

Our **technical support** team is available at +49 (0)34491 / 58 18 14, weekdays between 7:30 – 16:30 (CET).  
You can also email us at: [support@indu-sol.com](mailto:support@indu-sol.com)

**Is your plant standing still?** You can reach our emergency service around the clock at:  
+49 (0)34491 / 58 18 0.

## Revision Overview

Date	Revision	Change(s)
15/09/2021	0	First version

© Copyright 2021 Indu-Sol GmbH

We reserve the right to amend this document without notice. We continuously work on further developing our products. We reserve the right to make changes to the scope of supply in terms of form, features, and technology. No claims can be derived from the specifications, figures, or descriptions in this documentation. Any kind of reproduction, subsequent editing, or translation of this document, as well as excerpts from it, requires the written consent of Indu-Sol GmbH. All rights under copyright law are expressly reserved for Indu-Sol GmbH.

### WARNING

Commissioning and operation of this device must only be performed by qualified personnel. Qualified personnel within the meaning of the safety notices in this manual are persons authorised to commission, ground, and mark devices, systems, and circuits in accordance with safety engineering standards.

Improper use or configuration of the **PROmesh P10X** in the network may cause severe physical injury as well as property and material damage, also due to uncontrolled machine movements.

## Table of Contents

Revision Overview	3
Table of Contents	4
1 General Information	6
1.1 Overview of the <i>PROmesh P10X</i> – Function Scope	6
1.2 Scope of Supply	7
1.3 Safety Notices	7
2 Connections and Status Indicators on the Device	8
2.1 Device Connections	8
2.2 Installation and Integration	9
2.3 Connection of Power Supply and Error Relay	10
2.4 LED Displays	11
2.5 Network Integration & Commissioning	12
2.5.1 Data Ports	12
2.5.2 Media Connection	12
2.5.3 Wiring	12
2.6 Network Topologies & Redundancy	13
2.6.1 Network Topologies	13
2.6.2 Ring Structure	13
3 Web Application	14
3.1 Preparations	14
3.2 System Login	16
3.3 Web Interface	16
3.4 Start	17
3.5 System Information	19
3.6 Diagnosis	19
3.6.1 Line Diagnosis	19
3.6.2 Leakage Current	21
3.6.3 Network Statistics	21
3.6.4 Neighbourhood Detection	23
3.6.5 Port Mirroring	23
3.6.6 Alarms/Messages	24
3.6.7 Messages	26
3.7 PROFINET	27
3.8 Switching	27
3.8.1 Port Configuration	27

## Table of Contents

---

3.8.2	Quality of Service	29
3.8.3	VLAN	30
3.8.4	Bandwidth Control	32
3.9	Redundancy	33
3.9.1	MRP	33
3.9.2	RSTP	34
3.10	System Configuration	37
3.10.1	Device Information	38
3.10.2	IP Configuration	38
3.10.3	Password	39
3.10.4	Time Setting	40
3.10.5	SNMP	42
3.10.6	Access Time	42
3.10.7	Backup	42
3.10.8	Recovery	43
3.10.9	Firmware Update	43
3.10.10	Factory Settings	44
3.10.11	Reboot	44
3.11	Support	45
4	Troubleshooting Advice	46
5	Technical Specifications	47

## 1 General Information

Please read this document thoroughly from start to finish before you begin installing the device and taking the device into operation.

### 1.1 Overview of the *PROmesh P10X* – Function Scope

The *PROmesh P10X* is an industrial Ethernet switch with management and PROFINET functions that can be configured easily and conveniently via a web application. It supports the effective setup of all network topologies, such as bus, star, and ring structure in your plant, with its comprehensive functions with cut through technology.

#### Features:

- Web application for configuration
- Reverse polarity protected supply 12-48V DC; redundant operation possible
- Line diagnostics
- Leakage current monitoring
- Port statistics (network load in ms, errors, discards)
- Alarm management
- 8 x 10/100 Mbit/s M12 D-coded
- 2 x 10/100/1000 Mbit/s X-coded
- Switch technology: Cut-through
- MAC address table: 16K (16384 addresses)
- PROFINET Conformance Class B
- PROFINET Netload Class III
- Quality of Service (QoS) with eight priority queues
- Prioritisation by class of service (COS), type of service (TOS), or port priority
- Limitation of incoming and outgoing packets
- Port Mirroring (Rx/Rx and Tx packets)
- Port-based VLAN with 4096 possible VLAN IDs
- Simple Network Time Protocol (SNTP)
- Simple Mail Transfer Protocol (SMTP)
- Web interface access via HTTP/HTTPS
- Simple Network Management Protocol (SNMP), v1, v2c, v3
- Update, save, and backup the system configuration via web interface, TFTP

## 1.2 Scope of Supply

The scope of supply comprises the following individual parts:

- **PROmesh P10X**
- User quick start guide (hardcopy)
- USB stick with the following files: Manual (PDF), user quick start guide (PDF), GSDML file for integrating the switch into the project, service tool (ZIP), switch explanation video (MP4)

Check that the content of your delivery is complete before commissioning. In case of questions, contact our technical support team immediately before commissioning.

## 1.3 Safety Notices



Check that it is in perfect condition externally before commissioning of the device. If any damage is suspected, return the PROmesh P10X to your supplier immediately and do not operate the unit. Our technical support team will be happy to answer any questions you may have.



The **PROmesh P10X** was developed for use in PROFINET applications in accordance with conformance class B. Also note the selection of the data lines used in accordance with the standard to fully support the PROFINET standards.



Always observe the technical specification of the device to ensure safe and optimum use. The device is designed for IP67 protected environments. This requires special protective caps for unassigned ports, which you can purchase from Indu-Sol as an accessory. If such caps are not used, operation under IP67 conditions cannot be guaranteed. Take appropriate measures in case of deviating operating environment to ensure proper operation of the device.



Do not open the housing under any circumstances. No parts that require servicing have been installed. Unauthorised opening of the housing will void any warranty claims.

## 2 Connections and Status Indicators on the Device

### Device Connections

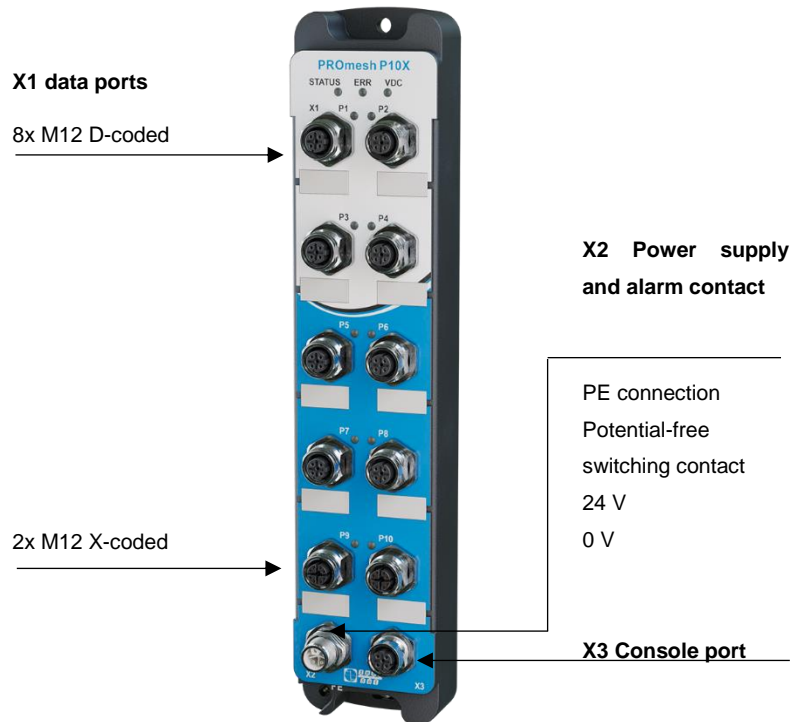


Figure 1: Device connections



## 2.2 Installation and Integration

The PROMesh P10X is designed for use in the open field (IP67 range). It may be installed by wall mounting. There are recesses for M5 screws at the top and bottom of the housing with which the PROMesh P10X can be attached to a wall.

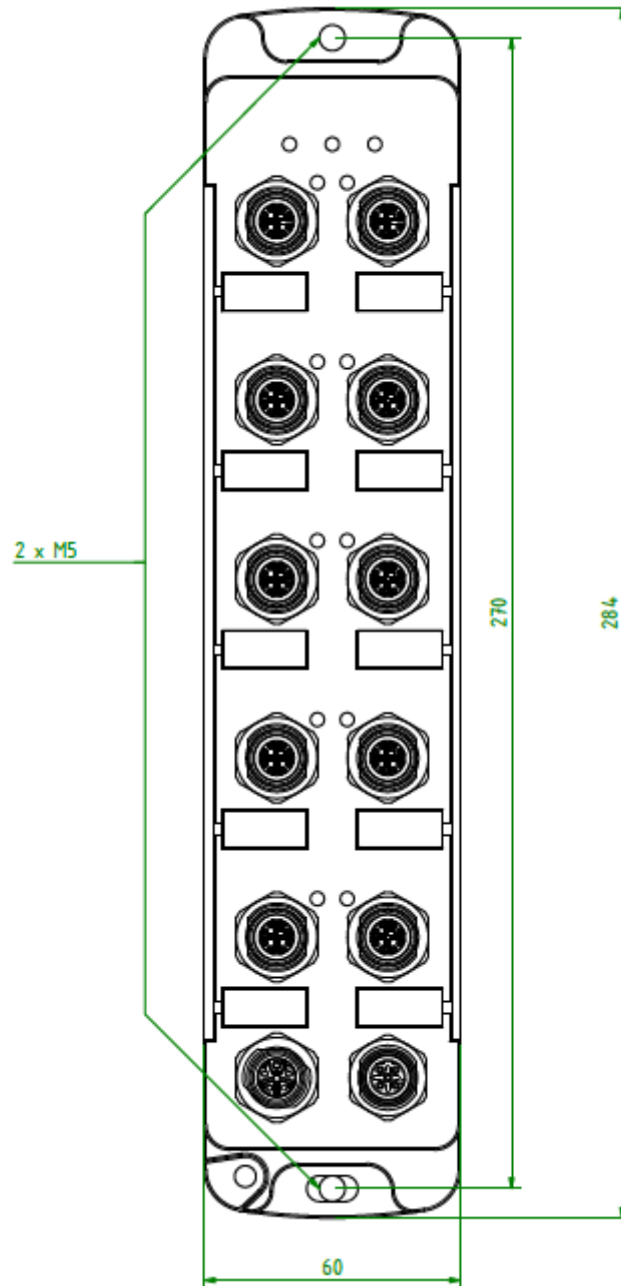


Figure 2: Hole drawing



The following distances to other assemblies must be observed for correct mounting:

- To the left and right: 50 mm
- Up and down: 50 mm



Do not mount the **PROmesh P10X switches** directly adjacent to any devices that generate strong electromagnetic interference fields, such as transformers, contactors, frequency converters, etc.



Do not mount the **PROmesh P10X switches** directly adjacent to any heat-generating devices and protect the switch from direct sunlight to avoid unwanted heating. Protect the PROmesh P10X from any additional heat radiation and observe the permitted storage and operating temperature range.

### 2.3 Connection of Power Supply and Error Relay

Operate your **PROmesh P10X** with a nominal voltage of DC 12 V to 48 V. Use the redundant power supply (pin 1+2 and pin 3+4) to ensure your system availability and connect the VU. The voltage must be a PELV-compliant voltage in accordance with IEC 60950-1 / EN60950-1 / VDE0805-1.

The M12 L-coded connection marked X2 is assigned as follows:

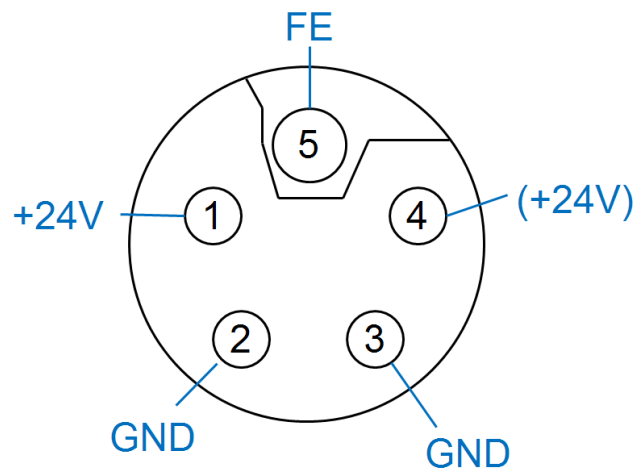


Figure 3: M12 L-coded connection assignment

## 2.4 LED Displays

There are three diagnostic LEDs on the front panel of the switch.

Each of the 10 data ports also has a status LED.

The LEDs display the most important diagnostic information about the device and connection status of the PROmesh P10X in your PROFINET network (see Table 1).

LED	Status	Meaning
<b>VDC1</b>	Green	Voltage at connection sufficient
	Off	Voltage at connection insufficient
<b>Status</b>	Green	Active PROFINET connection to the controller
	Yellow	No PROFINET connection to the controller
<b>Err</b>	Red	Power outage, port error or configured alarm active
	Flashing	No power outage, no port error, and no configured alarm active
<b>LED ports 1-10</b>	Off	No link
	Flashing	Link + data exchange (flashing speed reflects link speed)
	On	Link

Table 1: LED functions

### 2.5 Network Integration & Commissioning

#### 2.5.1 Data Ports

The **PROmesh P10X** is equipped with 10 data ports that allow data transmission at up to 1.0 Gbit/s in compliance with PROFINET standard 2.4. The actual data rate is negotiated by the device using auto-negotiation.

Ports 1-8 are equipped with M12 D-coded ports, ports 9-10 with M12 X-coded ports.

#### 2.5.2 Media Connection

The PROmesh P10X offers the possibility to connect M12 D-coded connectors (medium copper) on ports 1-8 and M12 X-coded connectors (medium copper) on ports 9-10.

This permits a high-performance connection of the field switch to the central control cabinet switch via Gigabit ports. End devices can continue to be controlled via 100 Mbit/s.

Observe the applicable standards and fixed connections in the connector application when designing, selecting, assigning, and assembling your data cable in order to ensure the longest possible cable length and cascading of network segments in accordance with your media type.

#### 2.5.3 Wiring



Connect your PROmesh P10X via the existing RJ-45 data ports using twisted pair cables of category 5 (Cat 5) or higher with a maximum cable length of up to 100 m. We recommend the PROFINET RJ45 connectors from Indu-Sol to improve the shielding.

## 2.6 Network Topologies & Redundancy

The devices of the *PROmesh product family* can be used in redundant networks, such as meshed networks or rings, via different protocols in addition to being used in star-shaped switched Ethernet networks.

### 2.6.1 Network Topologies

Classical Ethernet star structures (see Figure 4) can be linked to the *PROmesh P10X switches* without additional configuration. The devices are ready for use immediately.

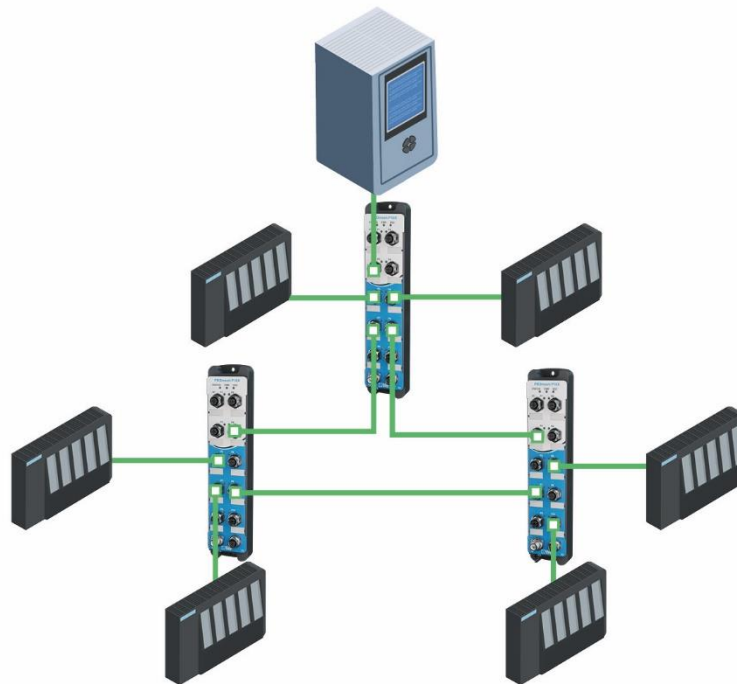


Figure 4: *PROmesh P10X* in a star network

### 2.6.2 Ring Structure

The *PROmesh P10X* fully supports the IEC 62439 standard, thereby enabling deterministic reconfiguration of information forwarding in simple redundancy (ring topologies, see figure 7). This enables reconfiguration times of up to 200 ms, depending on the size of your system.

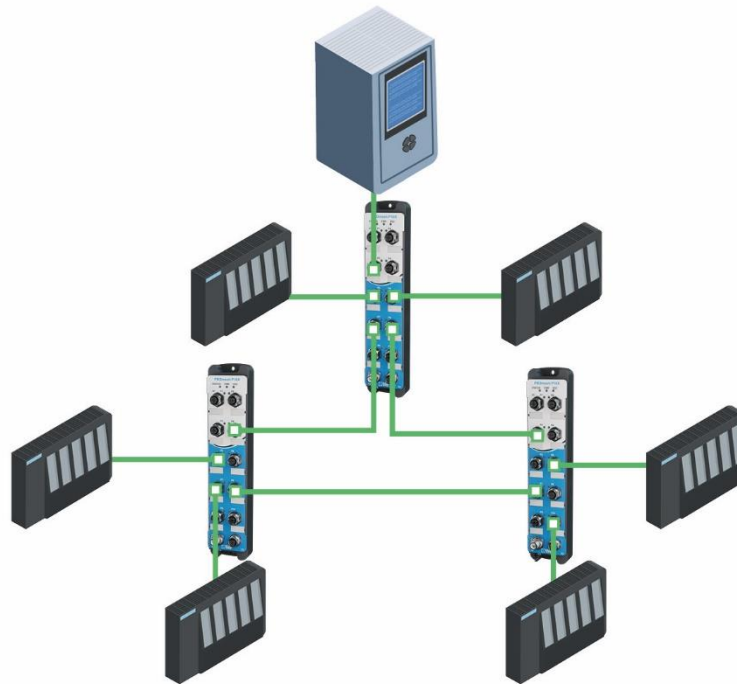


Figure 5: *PROmesh P10X* in a ring-shaped network

### 3 Web Application

The *PROmesh P10X* switches are equipped with a modern web interface that may be configured comfortably from any web browser.

#### 3.1 Preparations

Install the *PROmesh P10X* switch on the network before using web management and ensure that the PC designated to configure the switches can access the switch through the web browser. The *PROmesh P10X* and the client PC to be connected must be in the same IP address range and IP subnet. You must assign an *PROmesh P10X* IP address at first use for this.

The following IP address, subnet mask, administrator username, and administrator password are set when the device is shipped from the factory:

- IP address: **0.0.0.0**
- Subnet mask: **0.0.0.0**
- Gateway: **0.0.0.0**
- Username: **admin**
- Password: **admin**



Make sure to change the factory-set password when logging in for the first time. You are responsible for documenting this password and protecting it from unauthorised access.

You can easily set your intended user addresses with the **Indu-Sol ServiceTool**. This is part of the scope of delivery or can be downloaded for free via the following link:

<https://www.indu-sol.com/servicetool>

Our software is updated regularly. Please ensure that you have the latest version.

Establish a network connection from your computer to a port of the switch and scan the system with the search setting *PROFINET device* after installing and opening the software. You can then make the appropriate entries in the input mask and save them.

The corresponding address settings are then made automatically this way if you include the switch in a PROFINET system in the hardware configuration of the controller.

## 3.2 System Login

1. Launch a web browser on your computer.
2. Enter the IP address of the **PROmesh P10X** switch you are using into the address line of the web browser and confirm your entry with the *Enter* key.
3. The login mask of the device now appears on the screen.

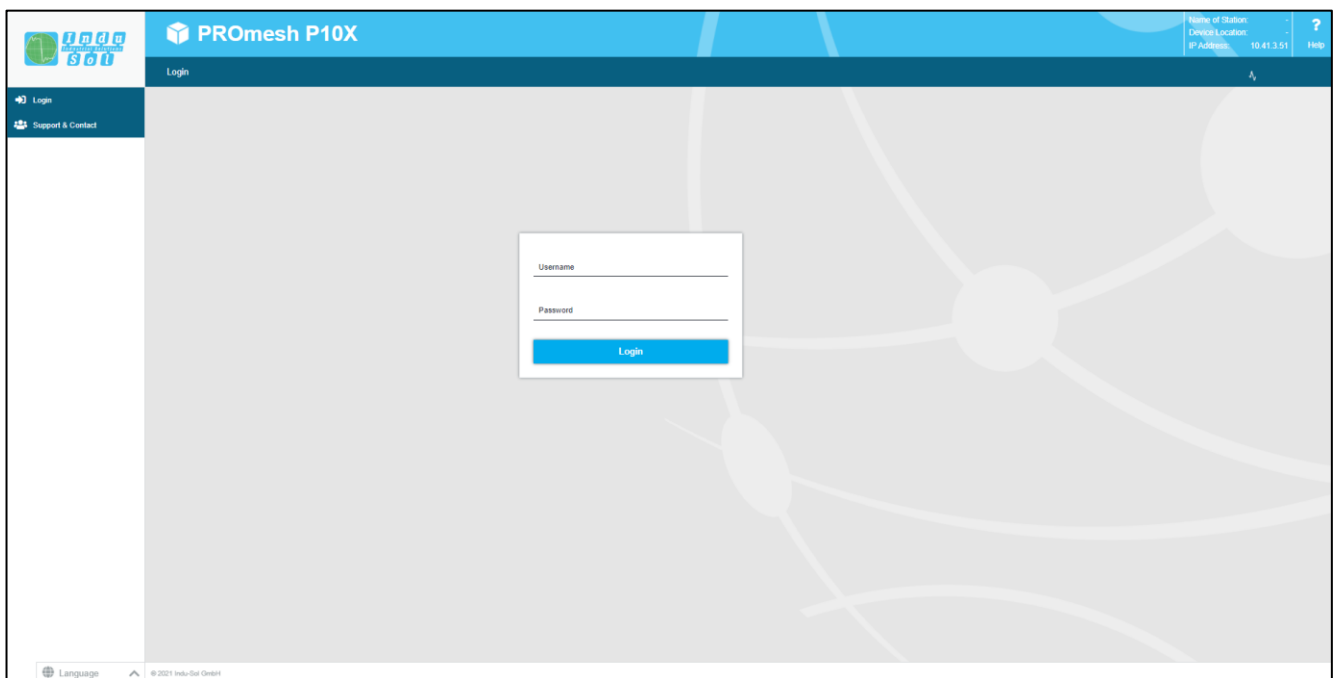


Figure 6: Login mask

4. Select the desired menu language (DE / EN). You can change this at any time, in any menu of the web interface.
5. Then enter the username and password.
6. Pressing the *Enter* key or clicking *Login* will take you to the switch web interface.

## 3.3 Web Interface

The following symbols are used in the web interface for a simple status display of the individual ports:



**No error:** The communication works without any errors.



**Warning:** At least one communication error (discards, error) has occurred on the corresponding port, which has not yet led to a failure. The cause of these events should be located and corrected.





**Error:** A critical fault has occurred on the corresponding port, resulting in a communication interruption. Urgent action is needed to correct the disruption.



There is no communication at the respective port. Either no device is connected (potentially also at line interruption) or no telegram traffic can be detected (serious fault in the network) or the devices no longer communicate.

### 3.4 Start

Successful login will lead to the main overview with the information bar, where the device name, the installation location, and the IP address are displayed. The current user is displayed under the logout button at the right end of the bar. You can log out by pushing the button. The help button displays notes and explanations for the individual pages.

The port statistics provide an overall view of the state of the existing ports since the switch was started or reset (history) and within the last second (last second). You can choose between two views. In the Overview view:

- Current partners
- Transmission speed
- Diagnostic messages

are displayed. In the Details view, the parameters of the overview and:

- Mains load per s
- Mains load per ms
- Discards
- Errors
- Line quality value

are displayed.

The number of messages that have occurred is displayed in the message window. Clicking on the alarm bell will automatically call up the entries in the message list. The messages as well as the counter status of the ports can be deleted with the corresponding buttons.

The leakage current overview shows the current value between the RJ45 ports and the device's top-hat rail. It is possible to switch between the display of the peak value (peak) and the effective value (RMS) or this. This information makes interference currents visible at an early stage, which can lead to direct communication disturbances.



The top-hat rail must have been grounded properly in order to measure the leakage current correctly.

Selection in the menu bar allows you to call up the individual pages and make settings there. The displayed menu items are subdivided into further subitems.

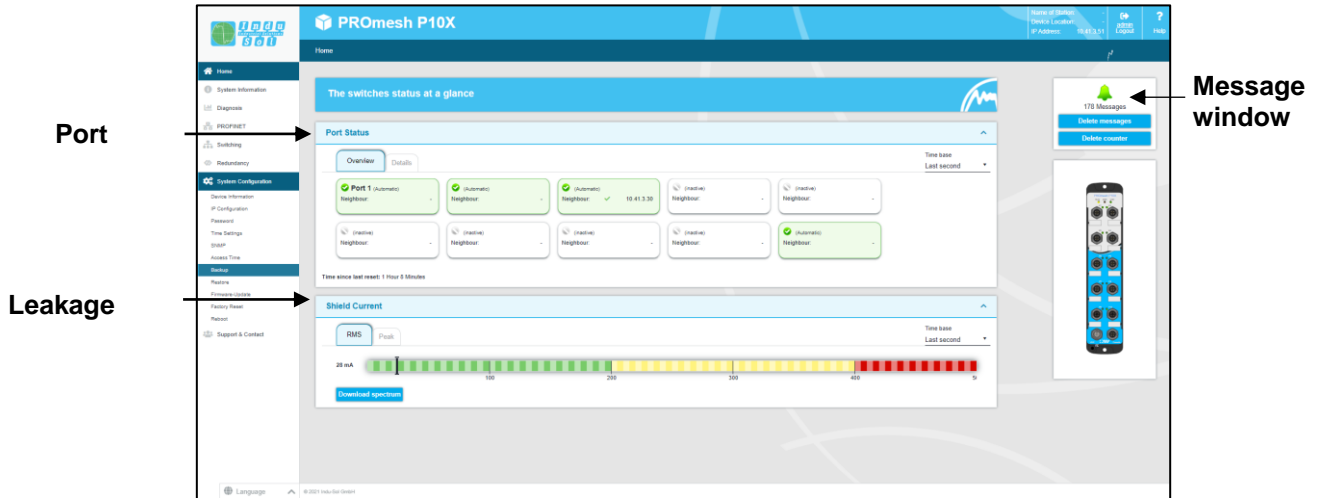
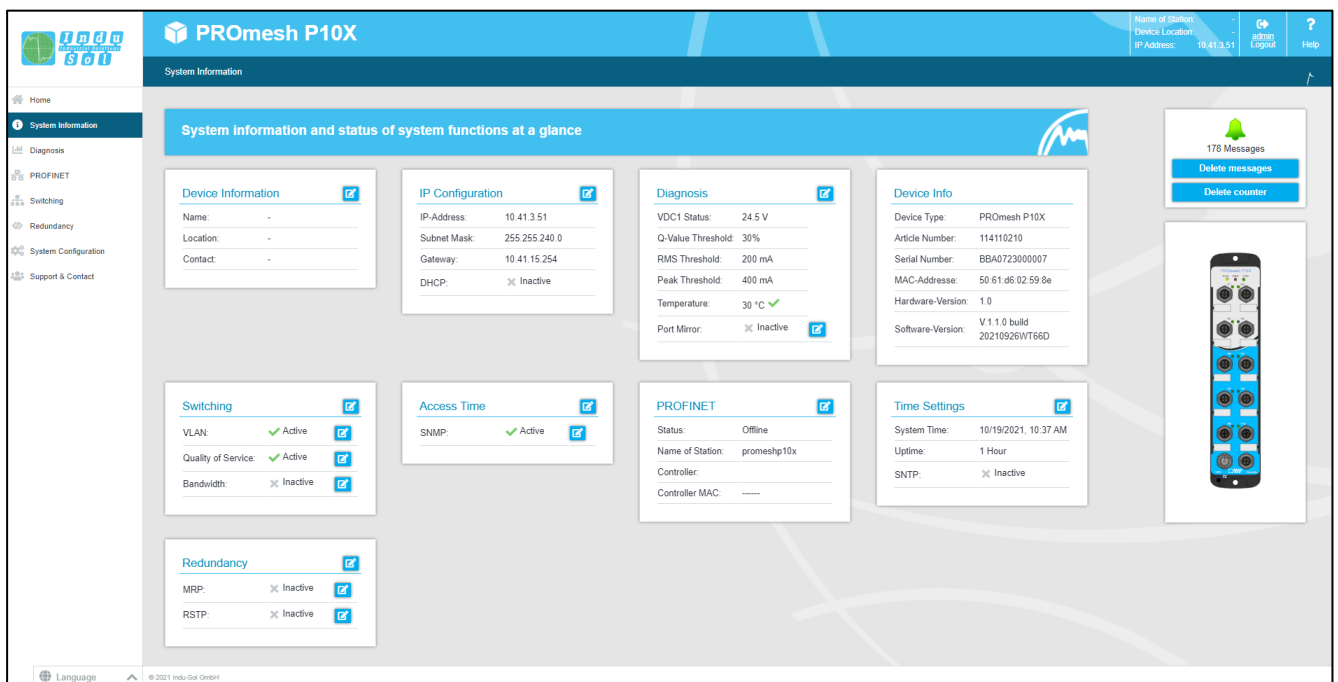


Figure 7: Start

### 3.5 System Information

An overview of the activated or deactivated protocols and functions is displayed under this menu item in addition to the device information. You can switch directly to the corresponding protocols and functions in order to make settings there by selecting the respective edit button.



The screenshot shows the 'System Information' page for a PROmesh P10X device. The page is organized into several sections, each with an 'edit' button (represented by a pencil icon):

- Device Information:** Name: -, Location: -, Contact: -
- IP Configuration:** IP-Address: 10.41.3.51, Subnet Mask: 255.255.240.0, Gateway: 10.41.15.254, DHCP:  Inactive
- Diagnosis:** VDC1 Status: 24.5 V, Q-Value Threshold: 30%, RMS Threshold: 200 mA, Peak Threshold: 400 mA, Temperature: 30 °C , Port Mirror:  Inactive
- Device Info:** Device Type: PROmesh P10X, Article Number: 114110210, Serial Number: BBA0723000007, MAC-Address: 50:61:d8:02:59:8a, Hardware-Version: 1.0, Software-Version: V 1.1.0 build 20210926WT66D
- Switching:** VLAN:  Active, Quality of Service:  Active, Bandwidth:  Inactive
- Access Time:** SNMP:  Active
- PROFINET:** Status: Offline, Name of Station: promeshp10x, Controller: -, Controller MAC: -
- Time Settings:** System Time: 10/19/2021, 10:37 AM, Uptime: 1 Hour, SNTP:  Inactive
- Redundancy:** MRP:  Inactive, RSTP:  Inactive

On the right side, there is a notification area showing '178 Messages' with 'Delete messages' and 'Delete counter' buttons, and a mobile device image.

Figure 8: Status and diagnosis

### 3.6 Diagnosis

The diagnosis page provides an overview of the status of configured alarm triggers (alarm trigger configured or not) for the individual diagnostic data acquired by the PROmesh P10X. The status for topology determination and port mirroring is also displayed.

#### 3.6.1 Line Diagnosis

Line diagnosis is available for ports 1 – 8. The quality of the connected connections is checked cyclically (every second). The line quality can lie between the values 100 and 0%. In this context, 0% corresponds to a defective cable, i.e. no data exchange is possible.

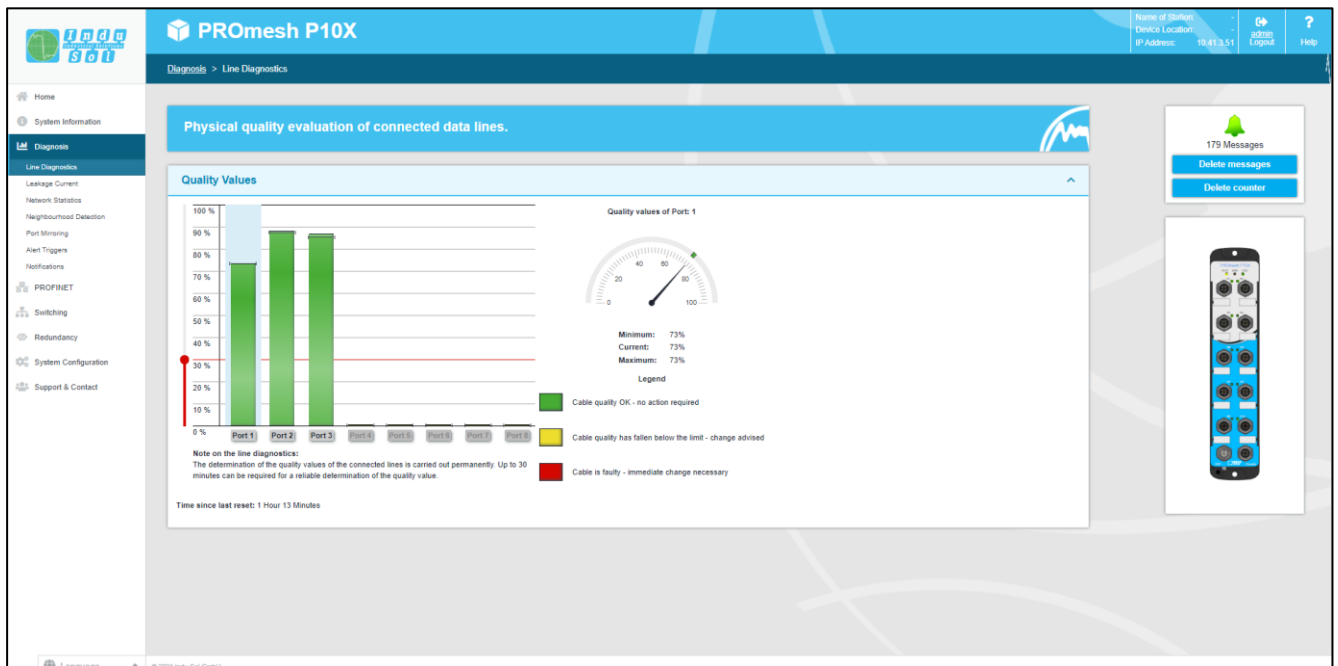


Figure 9: Quality value

### Information bar chart

3 values are displayed per bar.

The grey part of each bar shows its maximum value. The lesser coloured part, bordered by a black line, shows the current quality value. The colour-saturated part, which is bordered by a line with 2 arrows, shows the worst quality value of the connection so far. Colouring of the bars is based on this, which is done in accordance with the traffic light colour principle with green-yellow-red:

- Green: The line quality is in order; no measures required.
- Yellow: The defined threshold value of 30% was not reached. The line quality is not sufficient. The connection should be checked at the next maintenance interval.
- Red: No more data exchange can take place. Check the plug contacts and the data line.

A cable designation can be stored for each port in the port configuration menu. This can be displayed with a “mouse-over” (moving the mouse pointer over the port).

### Miscellaneous

The threshold value that turns the bar yellow and recommends checking the connection, can be adjusted by the user. It is not recommended to set the threshold below 30%. The alarms menu can be used to define alarms for the line quality value, which send messages via relay, SNMP, PROFINET, or email when a threshold value is undershot.

### 3.6.2 Leakage Current

Leakage current monitoring (Figure 10) permits permanent recording and evaluation of the sum of all shield currents of the PROFINET lines that are discharged via the device into the equipotential bonding system. The associated spectrum with the respective frequency components is specified for this purpose, in addition to the current value. The PROMesh series offers mechanisms for detecting EMC interference or coupling with this function.

#### Other functions:

- Download of the frequency spectrum after a threshold value has been exceeded
- Switching the axes between decimal and logarithmic scaling

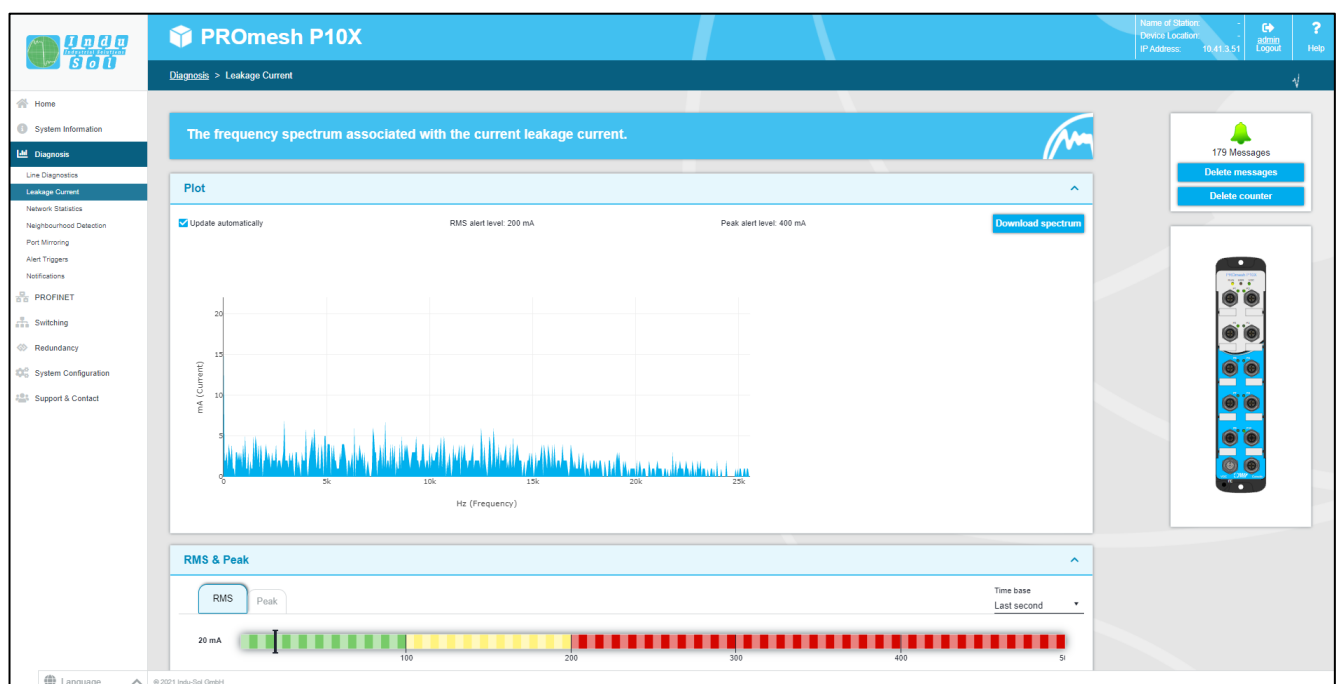


Figure 10: Leakage current

### 3.6.3 Network Statistics

The Network statistics page provides information about the traffic on each port. This information is useful for diagnostic purposes or in case of network problems.

In the main overview of the network statistics, the following information is provided for each port:

- Received data packets
- Data packets sent
- Mains load per second
- Mains load per millisecond
- Errors (destroyed telegrams)

- Discards (rejected telegrams due to too much data)

The graphical port load display shows the current network load in incoming or outgoing direction, as well as the minimum, average and maximum value, depending on the selected port.

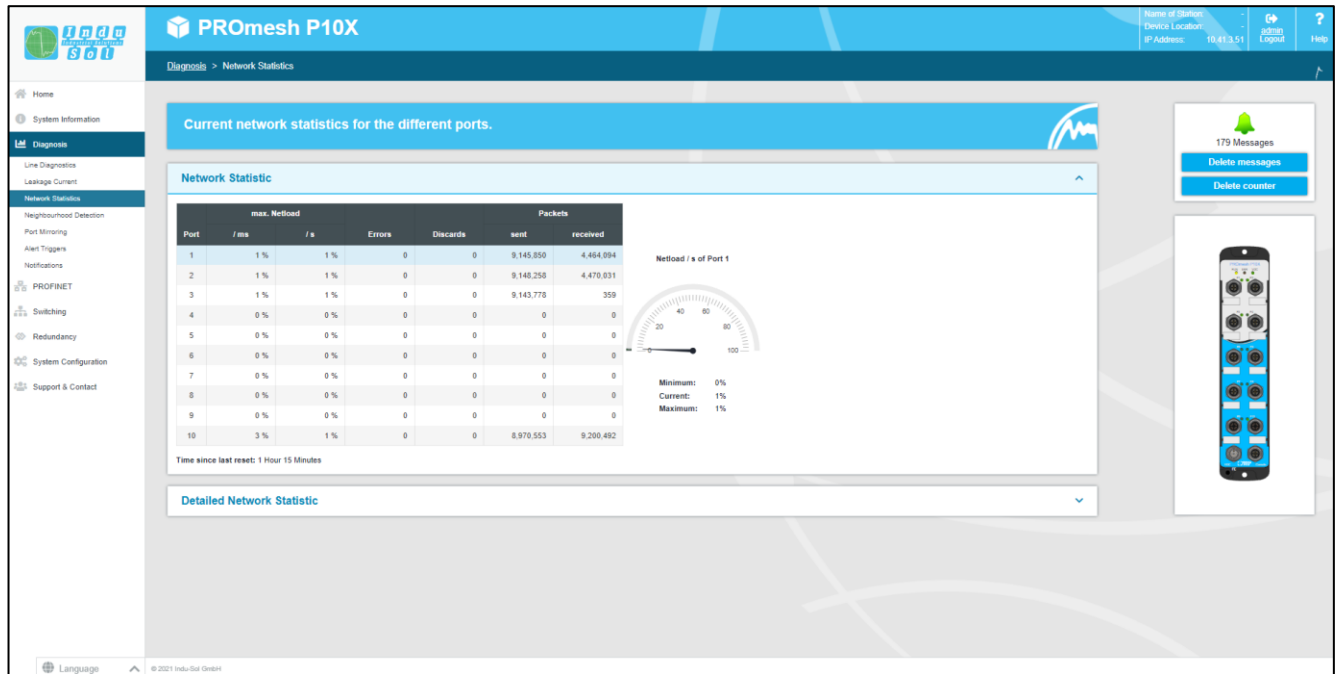


Figure 11: Network statistics

### Resetting the values

All counters can be reset via the button “Clear counters” in the upper right area.

### Detailed network statistics

The size of the individual packets is recorded statistically up to various threshold values in the statistics details (up to 64, 127, 255, 511, 1023, or 1518 bytes).

The packets sent are distinguished as follows:

- Number of unicast packets (packets to one receiver)
- Number of non-unicast packets

The received packets are distinguished between:

- Number of all packets
- Total bytes received
- Number of received fragments

The line *Packets up to bytes* gives information about the number of packets in different sizes. This records the number of packets received up to 63, 127, 255, 511, 1023, or 1518 bytes in size.

In addition, packet collisions are detected and distinguished by:

- Late (a collision that occurs after more than 512 bits)
- Total

. Such collisions and the associated data loss always occur when several participants want to send simultaneously on one medium.

### 3.6.4 Neighbourhood Detection

The Link Layer Discovery Protocol (LLDP) is a vendor-independent layer-2 protocol that provides the ability to exchange information (addresses, names, and descriptions) between neighbouring devices. An LLDP agent operates on every device that supports LLDP. This sends information about its own state at periodic intervals and receives information from neighbouring devices.

Since this is done independently, LLDP is also referred to as a one-way protocol.

The following information is compiled and sent by LLDP:

- System name and description
- Port name and description
- VLAN name
- IP address

#### LLDP interval

The LLDP interval parameter can be used to define the time intervals (in seconds) where the device-specific LLDP telegram is sent to the neighbouring devices. The default setting is 5 seconds.

#### Forwarding database

The forwarding database provides information about which MAC address is connected to which port of the switch.

### 3.6.5 Port Mirroring

Port mirroring is a method of simultaneously directing traffic from one port (source) to a second port (destination) in networks for inspection. This means that the received and sent packets of the source port are duplicated to the monitoring port.

Monitoring of the source ports takes place without affecting the traffic of this port. The resulting mirror port can be connected to a LAN analyser or used for diagnosis and debugging.

- Port and port name: All ports are displayed here in order to select a destination port and one or more source ports.
- Destination port: If port mirroring is enabled, select a port on which to mirror the data. The mirrored packets can be forwarded to exactly one destination port.
- Source port: You can select which ports to monitor and forward their packets to the destination port here. It is possible to route only sent packets (TX for transmit/transmit) to the destination port or to monitor both directions, i.e. sent (TX for transmit) and received (RX for receive) packets. Check the respective checkbox to select a port.

After you have set the respective parameters, click the Apply button to save and apply the settings.

### 3.6.6 Alarms/Messages

The menu item alarms/messages is used to configure alarm triggers and alarm receivers. Alarms can be created for the following events:

- Undercutting of the line quality value
- Exceeding of a leakage current
- Exceeding the network load on a port
- Voltage value of the 24 V power supply too high or too low
- Changing the status of a port
- Temperature too high or too low
- MRP protocol event (ring open/closed)
- Wrong connected neighbour

The alarms created can be linked to one or more alarm receivers, these include:

- Error relay
- SNMP traps
- Email addresses
- PROFINET

If one of the alarms set up is detected and triggered, the software will forward the event to the corresponding alarm receiver and document the event as a log message.



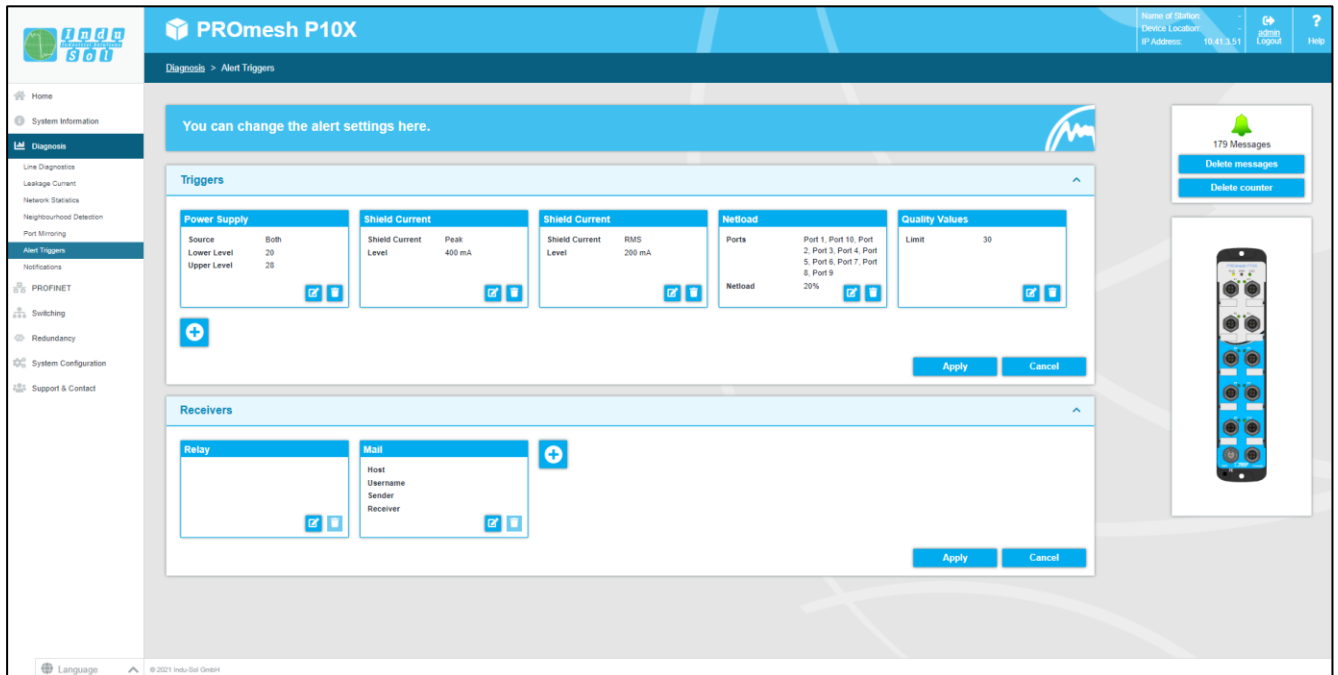


Figure 12: Alarm trigger

The configured alarm assignments are displayed in lists with consecutive ID.

- Alarm triggers with assigned receivers
- Alarm receivers with associated triggers

### Add and edit alarm triggers

New alarms and messages can be added by clicking on the button with the “+” symbol. If alarms are already present, the user has the option of editing or deleting them using a button. In the upper part of the “Alarm trigger” pop-up, the user can select the different alarms. The associated recipients can be selected in the lower part of the pop-up and linked to the alarm trigger in this way when the alarms are set up and edited, provided that the alarm recipients have already been defined.

### Adding and editing alarm recipients

New alarm recipients can be added by clicking on the button with the “+” symbol. The relay is already present as an alarm receiver and cannot be deleted, only linked to alarm triggers. The recipient email, SNMP, and PROFINET can be selected as well. The associated alarm triggers can be linked to the current recipient in the lower part of the pop-up.

- Error notifications are generated by the device and sent to a management station without being requested with Simple Network Management Protocol (SNMP). The device cannot determine whether the manager received the information since the packets are not acknowledged.
- The user can specify an email address and an SMTP (Simple Mail Transfer Protocol) server when using the email function. The device sends an email to the user if there is an alarm. Authentication can be activated as an option. The required access data must be entered for this purpose.
- Once the switch has been integrated and parametrised in a Profinet network, the “PROFINET” alarm receiver is permanently set in the system and cannot be changed in the device. The alarm triggers for the individual events are activated in the hardware configuration of the controller. If a trigger is released, the switch sends an alarm message to the controller. This information can then be processed programme-technically within the PLC.

### 3.6.7 Messages

The messages help the user view status and error messages of the various functions. The messages are displayed in the overview with date and time, as well as a code, description, and reference. Since the log entries are not stored in the device, they are no longer available after a device restart or a power interruption. It is possible to use an external syslog server or the SD card to archive the messages permanently.

#### Statistics

This tab provides a summary of the individual error codes that have occurred and their frequency.

##### Message backup

- Syslog server: Activate this function to save the messages on a syslog server. Enter the IP address of the syslog server in decimal point notation, select “File” from media type, and save the settings using the Apply button. Check if the server is reachable and saves the messages in a file.

### Resetting the entries

- The button “Delete entries” removes all entries from the table. The time of deletion of the entries is then possible at the first entry with the description “user log clear” and reference “MONO”.

## 3.7 PROFINET

The abbreviation Profinet means Process Field Network. It refers to the open Industrial Ethernet standard for automation.

The device is developed as a Profinet IO device for connection of decentralised peripherals to a Profinet controller. The device supports conformance Class B. This page offers the option of making port settings for DCP and downloading the configuration file.

DCP settings:

- You can specify for each port whether it supports the discovery and configuration protocol (DCP). DCP is used to distribute addresses and names to the individual stations in a Profinet IO system.

### Additional information

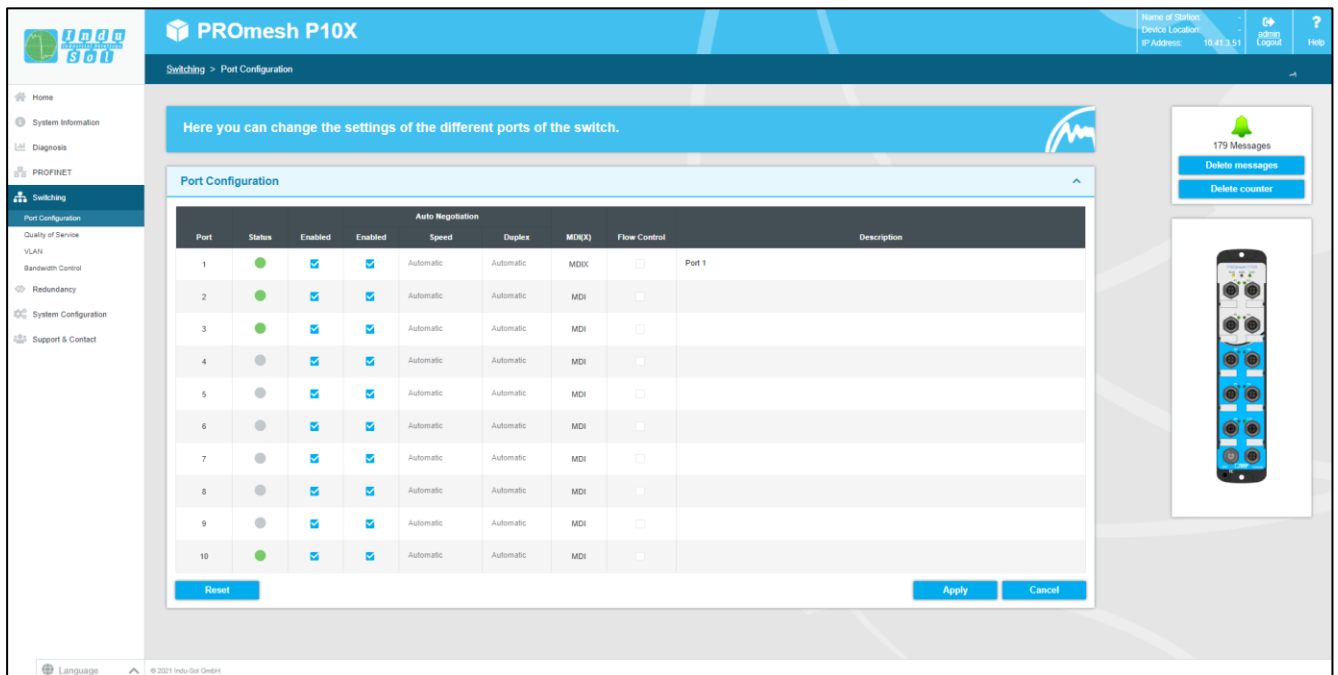
The configuration file stored on this page is used to describe Profinet field devices. The file is written in General Station Description Markup Language (GSDML). The file serves as a basis for planning the configuration of a Profinet IO system. Furthermore, the current status of the device in PROFINET as well as its controller (if available) is displayed.

## 3.8 Switching

This page provides an overview of the activated and deactivated functions in the Switching area. You can see which functions are currently activated right away. Clicking the edit button takes you directly to the various pages to make further settings there.

### 3.8.1 Port Configuration

The table provides an overview of the current configuration of the individual ports. The columns Enabled, Autonegotiation, Flow Control, and Designation can also be edited.



PROmesh P10X

Switching > Port Configuration

Here you can change the settings of the different ports of the switch.

Port Configuration

Port	Status	Auto Negotiation		Speed	Duplex	MDI(X)	Flow Control	Description
		Enabled	Enabled					
1	●	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Automatic	Automatic	MDIX	<input type="checkbox"/>	Port 1
2	●	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Automatic	Automatic	MDI	<input type="checkbox"/>	
3	●	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Automatic	Automatic	MDI	<input type="checkbox"/>	
4	●	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Automatic	Automatic	MDI	<input type="checkbox"/>	
5	●	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Automatic	Automatic	MDI	<input type="checkbox"/>	
6	●	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Automatic	Automatic	MDI	<input type="checkbox"/>	
7	●	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Automatic	Automatic	MDI	<input type="checkbox"/>	
8	●	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Automatic	Automatic	MDI	<input type="checkbox"/>	
9	●	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Automatic	Automatic	MDI	<input type="checkbox"/>	
10	●	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Automatic	Automatic	MDI	<input type="checkbox"/>	

Reset Apply Cancel

179 Messages  
Delete messages  
Delete counter

Language © 2021 InduSol GmbH

Figure 13: Port configuration

Details on the columns:

- **Port:** Specifies the port number, also marked on the housing.
- **Enabled:** The individual ports can be enabled or disabled. This specifies whether a port can be used or not.
- **Status:** Status signals the current state of the ports:
  - green: The port is activated and there is a connection.
  - grey: The port is inactive or disabled.
- **Autonegotiation:** If this function is enabled, the transmission speed and duplex mode are configured automatically. The machine and the connected remote party negotiate the settings automatically. If autonegotiation is disabled, the settings can be firmly set manually:
  - **Speed:** The data rate of the ports can be firmly set. A data rate of 10 Mbps or 100 Mbps can be set.
  - **Duplex:** Duplex mode can be switched between half and full duplex. This setting is thus set firmly for a connection.
- **MDI(X):** The device can perform autocrossover detection by default. This means that the switch automatically detects whether the subscriber is connected via a crossed or non-crossed cable.
- **Flow control:** Flow control ensures that if a port is overloaded, the received data packets are ignored, and the connected device is signalled to stop sending.
- **Designation:** You can give the ports names in this column. The names are displayed throughout the configuration and facilitate the selection of the correct settings as well as diagnosis in the event of an error. Click the port name to edit the name in the line.

### 3.8.2 Quality of Service

Quality of service (QoS) includes all procedures that influence the data flow in the device. With the assignment to queues with different priorities, certain user data can be treated preferentially. For example, real-time data, control data, audio or video data may be preferred over file transfers.

The switch supports eight different queues that are processed with different priorities. It is possible to use only one of the classification methods listed below or to combine several.

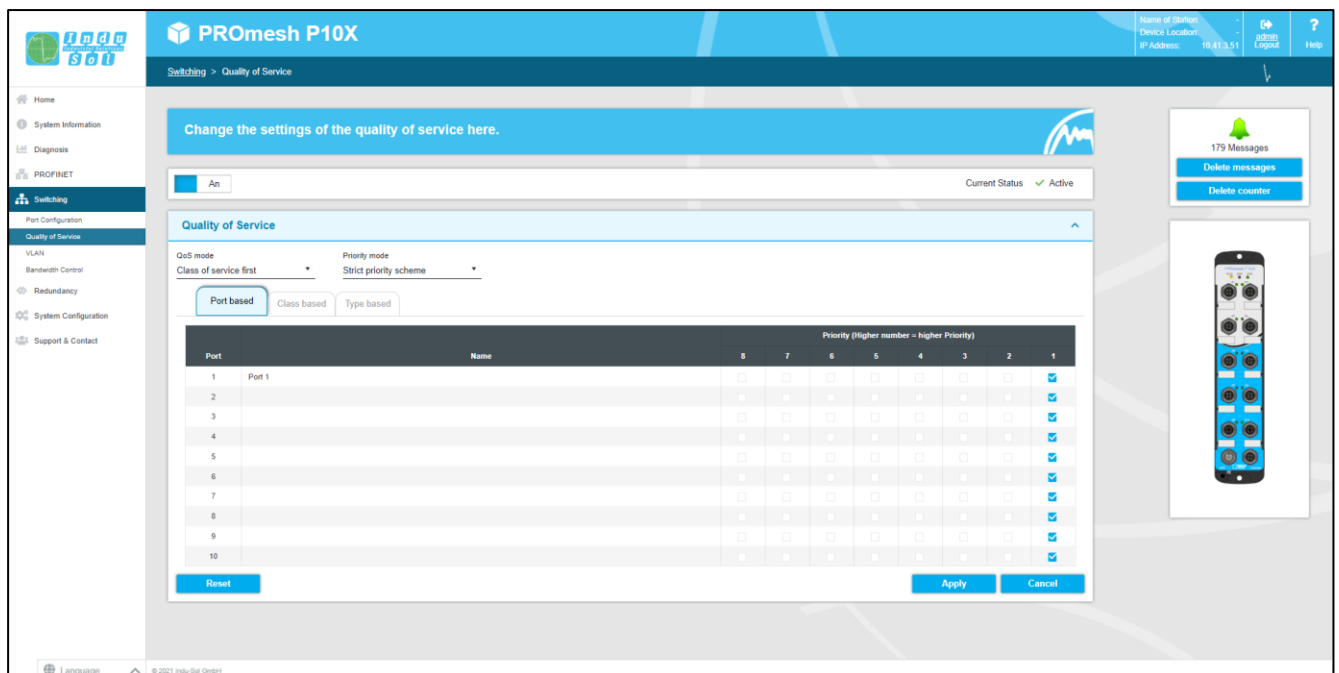


Figure 14: Quality of service

#### QoS mode and priority scheme

The QoS mode distinguishes between the following settings:

- **Port based:** You can set a priority for data transmission for each port and the switch will forward the data packets of that port in accordance with your priority.
- **Class of service (COS):** COS uses a data field present in the VLAN tag with priority information. Eight different priority values from best effort (BE,0-low) to network Control (NC,7-high) are specified. Assign the COS priorities to the switch's eight queues as needed in your application.
- **Type of service (TOS):** TOS uses a differentiated services code point (DSCP) data field in the IP header of packets that can have up to 64 different priorities. As with COS, you can use these priorities to prioritize real-time control data, Voice over IP (VoIP), or audio data over normal data transfer, for example. Adjust the settings to your requirements.
- **QoS mode:**
  - **Port-based only:** Priorities are based only on the priority of the ports.

- Class of service only: Priorities are based solely on the class of service data field of the packets.
- Type of service only: Priorities are based solely on the type of service data field of the packets.
- Class of service first: In this variant, priorities are determined first by COS, then (if necessary) by TOS, and finally by port.
- Type of service first: Here, priorities are determined first by TOS, then (if necessary) by COS, and finally by port.
- Priority scheme:
  - Strict priority scheme: In the strict priority scheme, all packets leave a port until the associated priority queue is empty. Only then are packets sent from the lower priority queues. If packets arrive permanently in the highest priority queue, packets in the lowest priority queue may never be sent. This mode is recommended when there are very high real-time requirements.
  - Weighted order: This approach prevents low-priority packets from never being sent when there are permanent high-priority packets to be sent. There is only a slightly higher latency for the high priority packets. The switch primarily sends high priority packets and also processes all low priority queues in one send cycle.

### 3.8.3 VLAN

A virtual LAN (VLAN) is a logical group of network nodes. It allows the isolation of a network part. Any traffic from network members of a VLAN group is transferred only within the VLAN group.

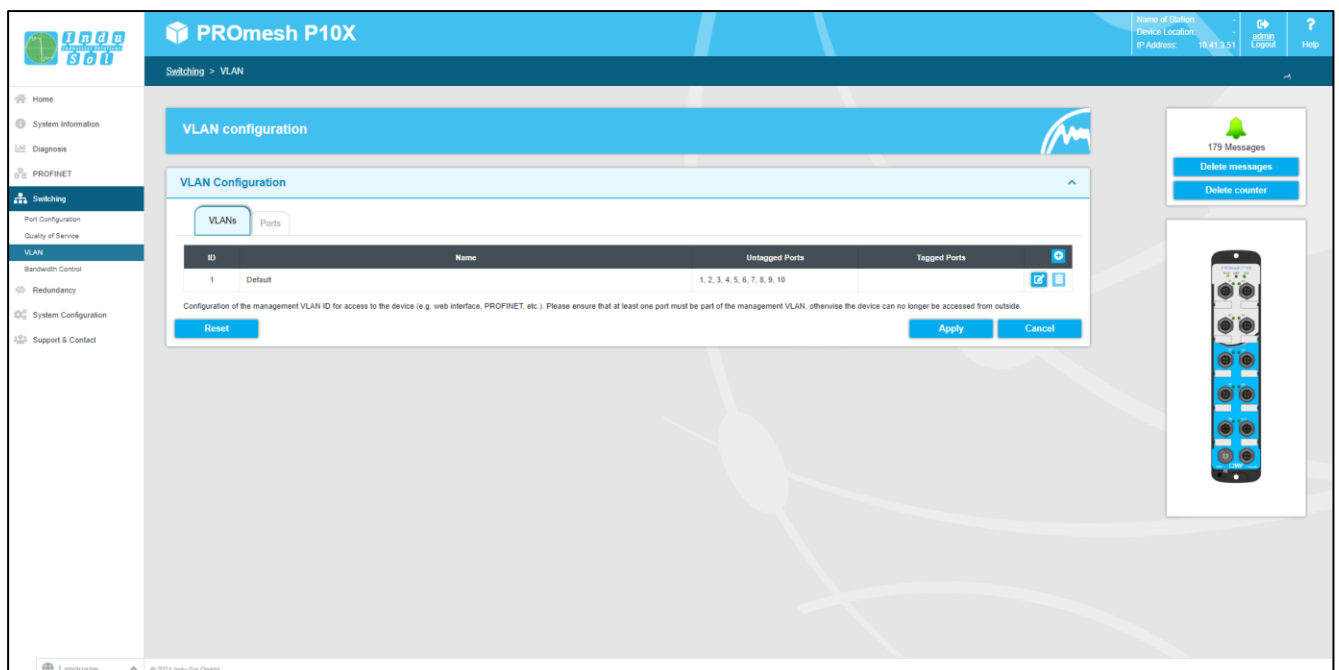


Figure 15: VLAN

Here you can make the settings for a VLAN based on 802.1Q (tagged VLAN). In tag-based VLAN, the VLAN control information is required from the packet header. The tags contain a VLAN identifier, which indicates the affiliation of the packet to the corresponding VLAN. In this way, it is possible to set up a VLAN across networks.

You can add a new tagged VLAN using the Add button if the VLAN 802.1Q function is enabled. Furthermore, you may select an existing VLAN from the list and edit or delete it with a button.

You can choose between two views. The overview by VLAN shows you the IDs and names of all virtual LANs and indicates the tagged and untagged ports by port number. You can also set which VLAN is treated as management and which VLAN is treated as default here. The overview by port shows the port number and name of a port and lists all VLANs with ID in which the port is a tagged or untagged member.

### **Adding a new VLAN**

Create a new VLAN the “+” button and define the following settings:

- **ID:** This identification number is uniquely assigned to a VLAN. VLAN IDs between 1 and 4094 are possible. Ensure that the ID is not being used by another VLAN on your network.
- **VLAN description:** Enter the name for the new VLAN here. The maximum length allowed for the VLAN name is 50 characters
- **Port ID:** Select how a port should behave in the newly created VLAN.
- **Status:** Shows whether a device is connected to the respective port or not.
- **Description:** A more detailed explanation of the port is possible here.
- **Ignore:** The port ignores the ID tag of the current VLAN and cannot communicate with this VLAN.
- **Untagged:** The port is part of the VLAN and can only communicate within this VLAN ID.
- **Tagged:** All output data packets of this port are tagged with a VLAN tag of the associated ID. Multiple VLAN IDs can be sent via this port
- **Port name:** This displays the port name assigned in the port configuration menu.

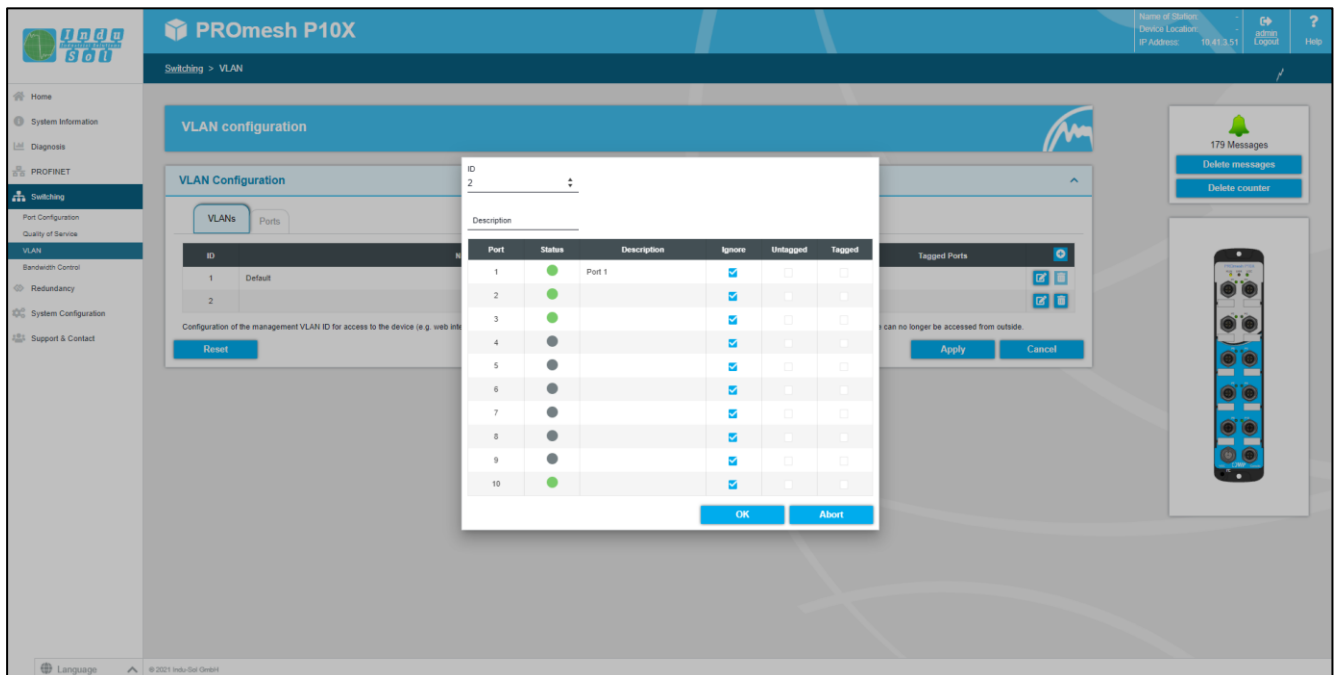


Figure 16: Adding a new VLAN

Notice: When you add ports to your VLAN, the untagged outbound traffic from those ports is tagged with the VLAN ID of your VLAN. This uniquely assigns the packet to your VLAN.

### Default and management VLAN

The default VLAN is relevant if no VLAN is activated. All ports are in the default VLAN in this case. If the VLAN function is activated, ports can also be assigned to other VLANs. There is no functional difference between the default and other VLANs except that the default VLAN cannot be deleted. This situation differs in the management VLAN. The PROmesh P10X can only be accessed via the management VLAN. At least one port must be stored in the management VLAN for this reason. Otherwise, the switch is no longer accessible. It should be noted in the context of network management that the network management system can access the management VLAN. Otherwise, no data can be retrieved from the PROmesh P10X.

### 3.8.4 Bandwidth Control

Bandwidth control makes it possible to enforce bandwidth limits on a port. You can set different send and receive rates for each port (incoming/outgoing packets) and apply them to specific packet types.

The tabular overview offers the following settings:

- ID: Specifies the port number, also marked on the housing.
- Packet type: Select a packet type to filter by.
  - All: The specified limits are observed for all packets transported via the port.



- Broadcasts: The set limits apply to all broadcast packets (to all devices in the network).
- Broadcast & multicasts: The set limits apply to all broadcast and multicast packets (to all or multiple devices on the network).
- Broadcast, multicast & unknown unicasts: The limits apply to all broadcast, multicast, and unknown unicast packets (to one subscriber).
- Limit of incoming packets: Select the effective ingress rate of the port. Possible are 128 kbit/s, 256 kbit/s, 512 kbit/s, 1 Mbit/s, 2 Mbit/s, 4 Mbit/s, and 8 Mbit/s. “No limit” is defined as the default value.
- Outgoing packet limit: The data rates for outgoing packets refer to all packet types. Select the effective egress rate of the port. Possible are 128 kbit/s, 256 kbit/s, 512 kbit/s, 1 Mbit/s, 2 Mbit/s, 4 Mbit/s and 8 Mbit/s. “No limit” is defined as the default value.

After you have made the desired settings, click “Apply” to save them.

### 3.9 Redundancy

This page provides an overview of the available redundancy protocols and their status. It is not possible to have multiple redundancy protocols running at the same time, so only one can be enabled. With the help of the edit buttons, you can access the protocols and carry out the configuration there.

The following protocols are available:

- MRP: The media redundancy protocol is a ring protocol for highly available networks, which is achieved by inserting redundant paths.
- RSTP: The rapid spanning tree protocol is a standardised method to manage mixed structures in the network and contains a mechanism for automatic reconfiguration.

The use of redundancy protocols guarantees your network increased reliability and availability in the event of a fault. The failure of a component is absorbed, and the participants not affected by the failure can continue to communicate.

#### 3.9.1 MRP

The media redundancy protocol is a ring protocol for highly available networks. The high availability is made possible by redundant communication paths, which are switched off during normal operation. The nodes connected in the network operate in a line topology, although it is physically a ring. In the event of an error, communication can take place via the previously deactivated path after a very short recovery time.

MRP uses a redundancy manager that tests the continuity of the ring by means of special test packets and reconfigures the network in the event of an error and informs the participants accordingly. The guaranteed reconfiguration time, with up to 50 devices in the ring, is 200 ms. The reconfiguration time usually is less than 50 ms in a typical application.

### Ring configuration

Please note that the ring must not be physically closed until MRP is fully configured. One device per ring must be configured as manager. The other devices must be configured as clients. The following settings are required for MRP:

- First ring port: Please select a port to work as primary ring port.
- Second ring port: Specify a second port to operate as a secondary ring port. Please note that the secondary ring port and the primary ring port must be different.
- This device operates as: Please specify whether the device should act as a manager or as a client. Please note that only one manager may be used per ring.

### 3.9.2 RSTP

The rapid spanning tree protocol (RSTP) is a standardised method for managing mixed structures, including a ring, on the network. It prevents network loops that can result from redundant transmission paths and includes a mechanism for automatic reconfiguration after a device or connection failure.

Enable the RSTP function globally before configuring the corresponding parameters.

#### Root bridge information

The following parameters are displayed in this field:

- Root port: Indicates which port is working as the root port. This port is the shortest path to the root bridge
- Root bridge ID: Identification number of the current root bridge negotiated between the devices.
- Designated cost: Path cost calculated for the connection to the root bridge.
- Root bridge MAC address: Displays the MAC address of the root bridge.

#### Device settings

Configure the protocol for your application:

- Forward delay: The time a port waits before switching from the RSTP learning and listening state to the forwarding state. Enter a value between 4 and 30 seconds.

- **Maximum age:** The amount of time a bridge waits before attempting to reconfigure without receiving spanning tree configuration protocol messages. Enter a value between 6 and 40 seconds.
- **Bridge priority:** This value is used for negotiating the root bridge. The bridge with the lowest value has the highest priority and is chosen as the root bridge. The value must be between 0 and 61440 and a multiple of 4096.
- **Hello Time:** The time interval at which the switch sends BPDUs (Bridge Protocol Data Unit) packets to check the current status of the RSTP. Enter a value between 1 and 10 seconds.
- **TX hold count:** Specifies the maximum number of Hello packets transmitted within an interval. A minimum of 1 and a maximum of 10 packets are allowed.

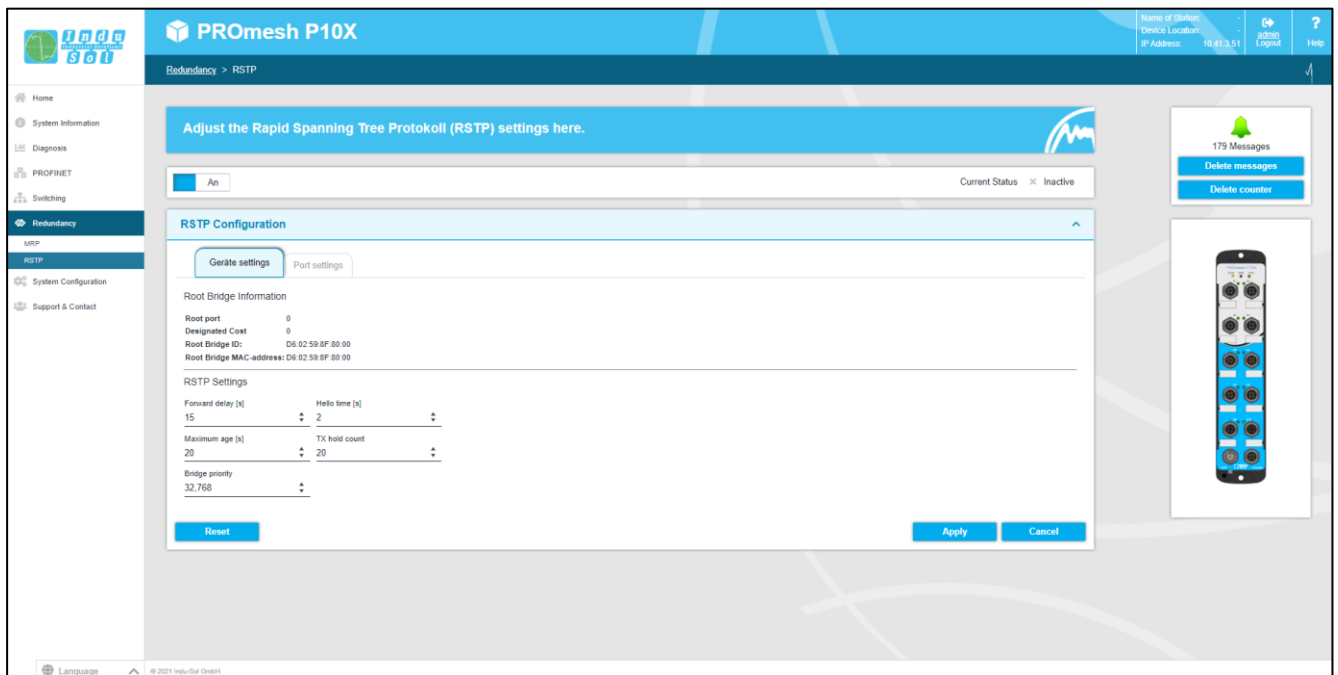


Figure 17: Device settings RSTP

Notice: Follow the rule to configure Forward Delay, Maximum Age and Hello Time:

$$2 * (\text{Forward Delay Time} - 1) \geq \text{MaxAge} \geq 2 * (\text{Hello Time} + 1).$$

Recommended procedure: Select a value for "Hello Time" and calculate with the formula  $2 * (\text{Hello Time} + 1)$  in accordance with the rule given above to get the lower limit of the Maximum Age. Select a value for "Forward Delay Time" and use the formula  $2 * (\text{Forward Delay Time} - 1)$  of the above rule to calculate the upper limit of the Maximum Age. Then select a Maximum Age between 6 and 40 seconds, which lies between the previously calculated limits.

When you have set the parameters, click “Apply” to apply the changes. The root bridge information is now displayed at the top of the page.

### Port settings

Set the following port-related settings per port:

- Port: You can configure each ports individually.
- RSTP on: For each port, select whether or not to enable the Rapid Spanning Tree Protocol on that port.
- Status: Displays the current status of each port. The following are distinguished:
  - Blocking: Discards packets; does not learn addresses; receives and processes BPDUs
  - Listening: Discards packets; does not learn addresses; receives, processes, and transmits BPDUs
  - Learning: Discards packets; learns addresses; receives, processes, and transmits BPDUs
  - Forwarding: Forwards packets; learns addresses; receives, processes, and transmits BPDUs
  - Disabled: Discards packets; does not learn addresses; does not receive and process BPDUs
- Role: Each port can run in one of the following modes:
  - Root port: A port in the forwarding state. Shortest way to the root bridge.
  - Designated port: A port in the forwarding state that allows communication to other bridges in the spanning tree.
  - Alternate port: An alternate path to the root bridge, in addition to the current root port.
  - Backup port: A backup path provided through a designated port towards the branches of the tree structure. Backup ports can only exist where two ports are connected as a loopback by a point-to-point connection or a bridge with two or more connections to a common LAN segment.
  - Disabled port: A port without any operational function in the tree structure.
- Priority: This allows the assignment of higher priorities to certain ports to influence the tree structure. Enter a number from 0 to 240. The value must be a multiple of 16.
- Costs: The cost from the sending bridge on the respective port of another bridge. Enter a number from 1 to 200,000,000. You can use this parameter to influence the structure of the tree.
  - defined: The cost of a connection to the root bridge can be specified.
  - designated: The designated costs are calculated by the RSTP and displayed here.
- Edge port: Specifies a port directly connected to an end device and not to another bridge (a switch). These ports cannot cause loops and therefore immediately switch to Forwarding mode.

Changing the status of an edge port does not change the topology in any case. They speed up the reconfiguration time of the redundancy protocol by setting edge ports fixed.

- force: The port is configured as an edge port by default.
- Auto: Edge ports are detected is automatically.

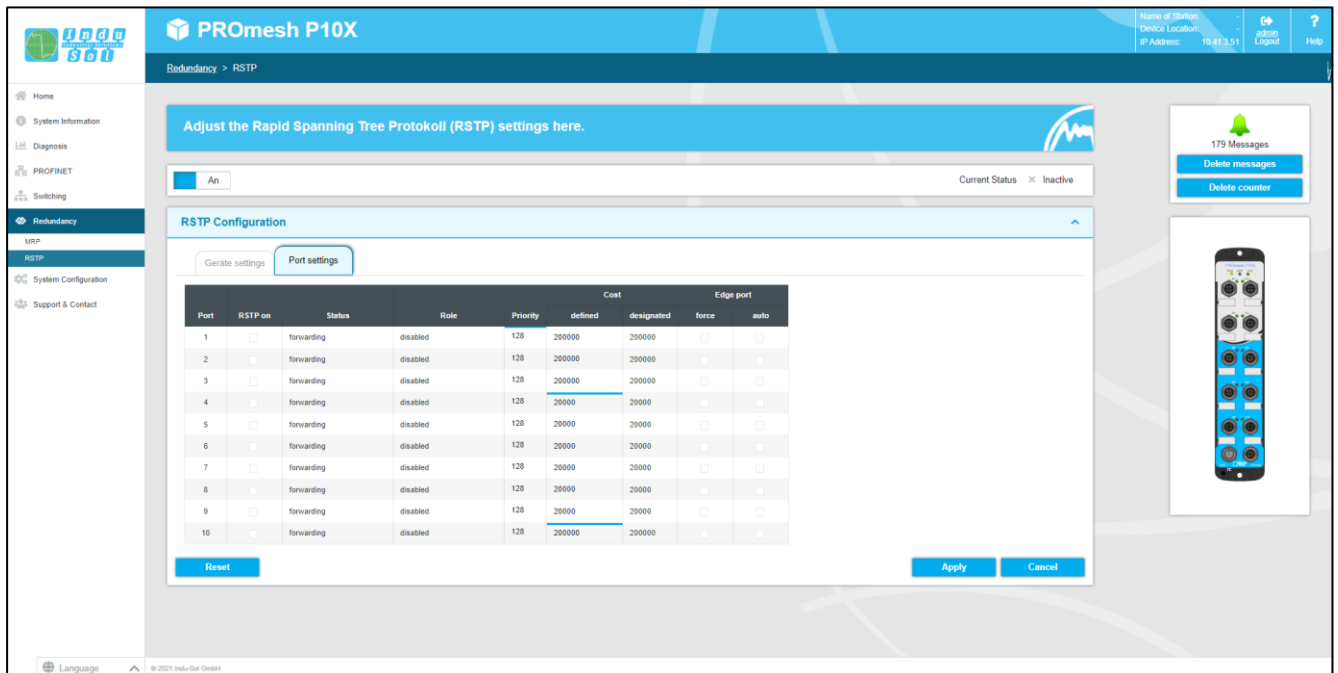


Figure 18: Port settings

Click Apply to apply the settings after you have set the respective parameters.

### 3.10 System Configuration

The system configuration page displays IP address settings, time settings, access options to the device, and general device information.

This page is to provide a concise view of the system configuration menu to help you understand how the unit works and where action is needed.

You can switch directly to the corresponding protocols and functions in order to make the other settings there with the respective edit button.

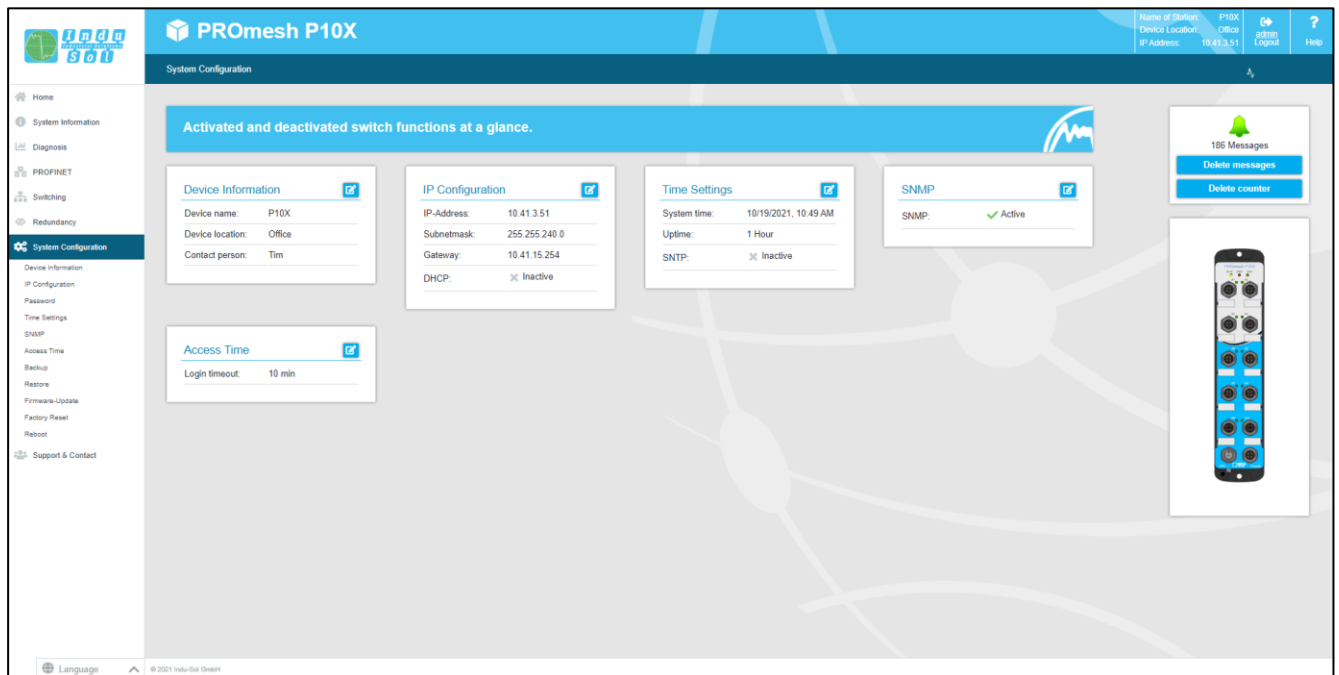


Figure 19: System configuration

### 3.10.1 Device Information

The device information page allows you to assign a unique device name, installation location, and contact person to the device.

- Device name: This name corresponds to the PROFINET name and is assigned by means of DCP.
- Installation site: Specify the installation location of the device to facilitate localisation.
- Contact: Enter a contact person for the device.

The input fields are configured so that you may use up to 50 characters. Special characters may be used. The device name and installation location are displayed in the information bar at the top right and help you to keep track of the device.

### 3.10.2 IP Configuration

The IP configuration can be performed either by the PROFINET controller, automatically using the Dynamic Host Configuration Protocol (DHCP) or manually. When the address is assigned automatically, the IP may change after a device restart, depending on the settings of the DHCP server.

## PROFINET

If the device is configured in a PROFINET network, the device receives its IP configuration from the PROFINET controller. The IP configuration cannot be performed automatically or manually with an existing PROFINET connection.

### Automatic

The subnet mask and the default gateway from a server working in the network with corresponding function, select the checkbox “automatic (DHCP)” to get a configuration of the IP address.

The device sends a request to the server and adopts the configuration received from the DHCP server after you have saved the settings by clicking on the Apply button. The device can no longer be reached via the default IP because now has a new IP address. Please contact your network administrator or use an appropriate tool (Indu-Sol ServiceTool) to obtain the new IP address.

### Manual

If your network does not have a DHCP server or you want to make the settings manually, deactivate the “automatic (DHCP)” button and enter the following data:

- IP address: Please note that the IP address you set must be accessible from your PC so that you can connect to the device again to make the other settings.
- Subnet mask: Enter the subnet mask of the IP address, this separates the IP address into a network part and a device part. This defines which IP addresses can be reached directly by the device and which addresses must be addressed via a gateway.
- Gateway: Enter a default gateway. The gateway is used to communicate with devices outside your subnet.

Please check the settings carefully to avoid problems with duplicate IP addresses. The format of the IP address, the subnet mask and the gateway must be entered in decimal notation.

### 3.10.3 Password

On this page the default password for the users Admin and User can be changed. The usernames and rights of the administrator and the user are fixed and cannot be changed.

#### Form fields

- New password: Enter the password set for the previously selected user in this field. Please also note the information on assigning passwords in the section below.

- Confirm password: Repeat the password in this field to make sure that you have entered your password correctly.
- Current password: Please enter your current password here to ensure that you are authorised to change the password.

### **Notes on passwords**

The security of your system is essentially related to the security of your passwords. Therefore, passwords generally should:

- not to use dictionary entries
- be as complex as possible
- use combinations of letters, numbers, and special characters
- use lower- and upper-case letters
- have at least eight characters
- never be written down

### **3.10.4 Time Setting**

This menu adjusts the device system time. Here you can choose between automatic (deposit of a time server) and manual mode.

#### **Automatic**

An NTP server can be used to obtain the system time automatically. Set the following information for this:

- SNTP server IP address: Enter the IP address of a time server.
- SNTP server IP address (redundant): Furthermore, a redundant time server can be stored optionally.
- Update interval: Set here the update interval with which the internal time of the device is updated.
- Time zone: Select your valid time zone.



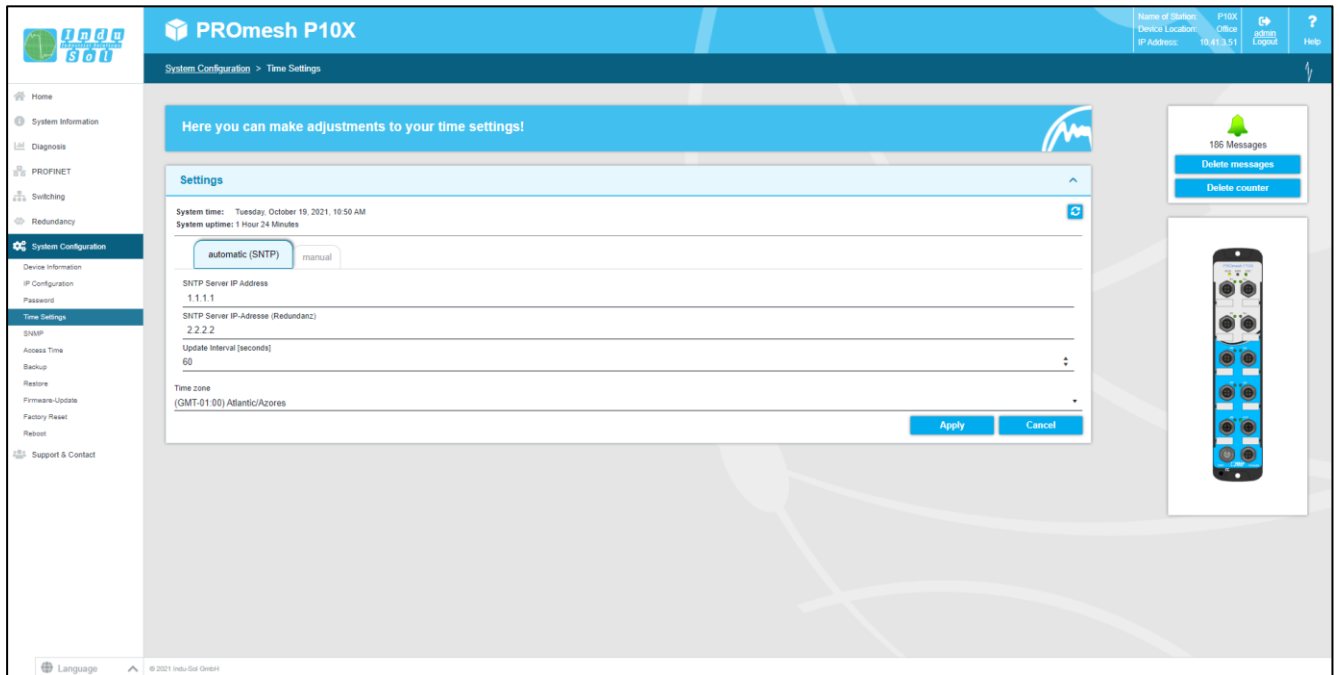


Figure 20: automatic time settings

### Manual

The device time cannot be entered manually if you cannot use an NTP server. Select the calendar button and choose the desired date for this.

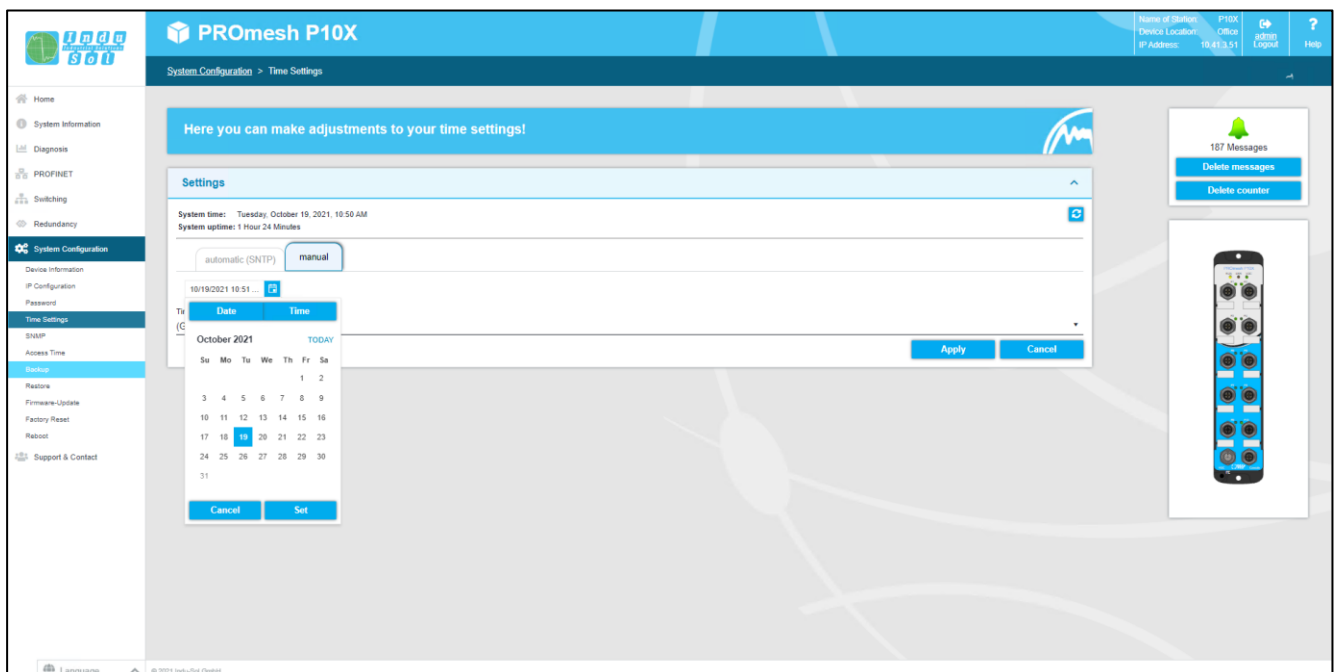


Figure 21: Manual time settings

Notice: A device time assigned manually will be reset every time the device restarts.

### 3.10.5 SNMP

The Simple Network Management Protocol (SNMP) controls communication between the monitored devices and the monitoring station. It enables the reading and writing of system variables.

#### Current SNMP accesses

The overview table shows you the currently defined community strings and access permissions.

- Community string: The accesses are defined by unique names that you can change.
- Read only: The community string allows read-only access.
- Read and write: The community string allows read and write access.
- Delete: You can mark the community strings to be deleted and then remove them with the “Delete” button.

#### Creating SNMP access

Click the “+” button to create a new community string. The following parameters are required:

- Community string: Enter a unique name for the new SNMP access. A maximum of 32 characters is allowed.
- Access: Specify whether read-only or read and write access is allowed.

Save the settings by clicking on the “Apply” button.

The device supports SNMP versions V1, V2C and V3. Select the desired version.

### 3.10.6 Access Time

#### Settings

The time to automatic logout defines how long a session in web management remains without activity before an automatic logout occurs. You can set a time between 3 and 30 minutes. The default setting is 10 minutes.

Save your settings with the “Apply” button.

### 3.10.7 Backup

This menu item allows you to back the current configuration of the device up in a file. The backup can be saved as a download.

The device creates and saves a backup file with all settings, which can be loaded at a later time using the Restore function.

Click “Start backup” to save the backup file. Confirm the settings in the message box.

### 3.10.8 Recovery

This menu item is used to import a previously saved backup file. The menu item Backup is used to create the backup file.

Select the “.conf” file to restore and drag it into the field provided.

Then use the “Start recovery” button to perform the action and confirm it in the window that opens.

Notice: The device will then reboot.

### 3.10.9 Firmware Update

Here you can update the firmware of the device. Please only use firmware versions that you have received from Indu-Sol and that have been developed for the PROmesh switches.

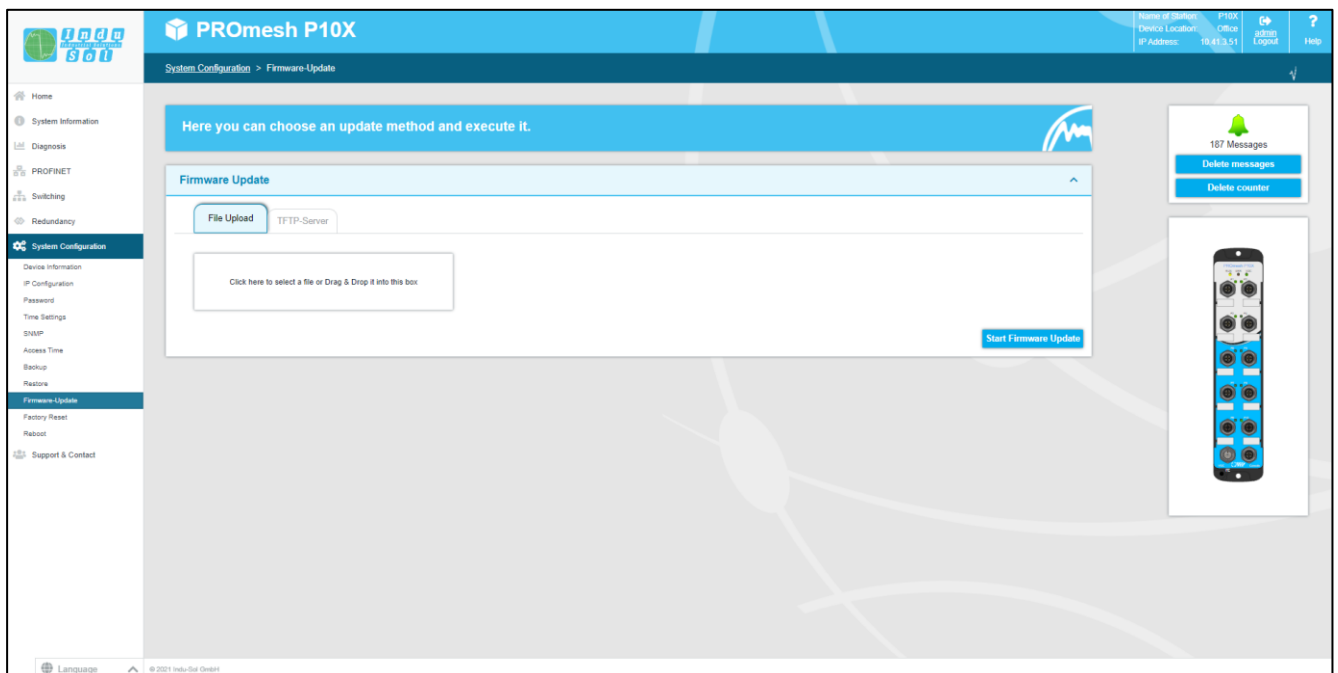


Figure 22: Firmware update

The firmware file is either provided by a TFTP server or uploaded to the device. Before updating, check that you have selected the correct firmware image.

- Upload: The firmware update is located on the computer currently in use and is transferred from there to the device.

- TFTP server: The firmware update is downloaded from a TFTP server on the network.

### **Preparation:**

It is not recommended to perform the update if the MRP protocol is enabled. Please open the MRP ring first by pulling out one of the cables and then disable the media redundancy protocol. Now perform the firmware update.

### **Settings**

- TFTP server IP address: Specify the IP address of the TFTP server available on the network in decimal dot notation.
- File name: Enter the name of the new firmware file to be installed here. Please specify the name relative to the root directory of the server.

Use the button “Start firmware update” to execute the action and confirm it in the window that opens. Please make sure that the firmware update can be executed completely.

### **Important:**

Do not perform the following actions while the firmware update is in progress.

- Do not disconnect the device from the supply voltage under any circumstances.
- Do not pull or change any network connectors.

A message will tell you when the update is complete. The device will restart automatically at that point.

Notice: The device will reboot during the firmware update.

### **3.10.10 Factory Settings**

This menu item is used to reset the device to its factory settings.

Click the “Reset to default” button for this and confirm it in the window that opens.

Notice: The device must then be rebooted.

### **3.10.11 Reboot**

A reboot of the switch can be performed here. Pressing the reboot button will exit the switch software and reboot the device.



You can also turn both supply voltages of the switch off and on again.

### 3.11 Support

The support section contains relevant contact information in case of any uncertainties regarding the product.

#### **Manufacturer**

Please contact the device manufacturer Indu-Sol if you have serious problems with the configuration of the switch or if questions arise that are not answered in the data sheet or in the operating instructions.

#### **License information**

The linked license.txt file contains information regarding the “Open-Source Software” used.

## 4 Troubleshooting Advice

- Check that the power supply is correct. The VDC LED must light up green.
- Check the link LEDs of the wired M12 sockets. The link LEDs must light up when the connection is established.
- If in doubt, disconnect redundant network structures and reset the **PROMesh P10X** switch to factory defaults. Make your settings again bit by bit and observe where the error occurs if the communication works afterwards.

## 5 Technical Specifications

<b>Network connections</b>	8 x up to 100 Mbit/s M12 D-coded 2x up to 1.0 Gbit/s M12 X-coded
<b>Power supply</b>	12 V ... 48 V DC redundant power supply
<b>Power consumption</b>	Maximum 10 W
<b>Dimensions (HxWxD)</b>	284 mm x 60 mm x 28 mm
<b>Weight</b>	0.85 kg
<b>Housing</b>	Aluminium, anodised
<b>Storage temperature</b>	-40 °C ... 75 °C
<b>Operating temperature</b>	-40 °C ... 85 °C
<b>Humidity</b>	Humidity 5% ... 95% RHD non-condensing
<b>Protection class</b>	IP67
<b>Assembly</b>	Wall mounting
<b>EMC</b>	2014/30/EU EN 61000-6-2 / IEC61000-4-2 / EN 55032
<b>LED display</b>	Status LEDs/Port LEDs/Power supply/Error
<b>Management</b>	SNMP management Web interface management
<b>Switching technology</b>	Cut-through
<b>MAC address table</b>	16 K MAC address table
<b>Ring</b>	MRP Spanning Tree
<b>VLAN</b>	Port based VLAN Tagged VLAN IEEE 802.1Q
<b>Class of service</b>	IEEE802.1p Class of service with eight priority queues per port
<b>Port mirror</b>	RX packets only or TX and RX packets
<b>Firmware update</b>	TFTP server, from local PC
<b>Bandwidth contr.</b>	Incoming and outgoing
<b>DHCP client</b>	DHCP client function to obtain an IP address from the DHCP server

**Indu-Sol GmbH**

Blumenstraße 3

04626 Schmölln

Telefon: +49 (0) 34491 580-0

Telefax: +49 (0) 34491 580-499

[info@indu-sol.com](mailto:info@indu-sol.com)

[www.indu-sol.com](http://www.indu-sol.com)

Wir sind zertifiziert nach DIN EN ISO 9001:2015