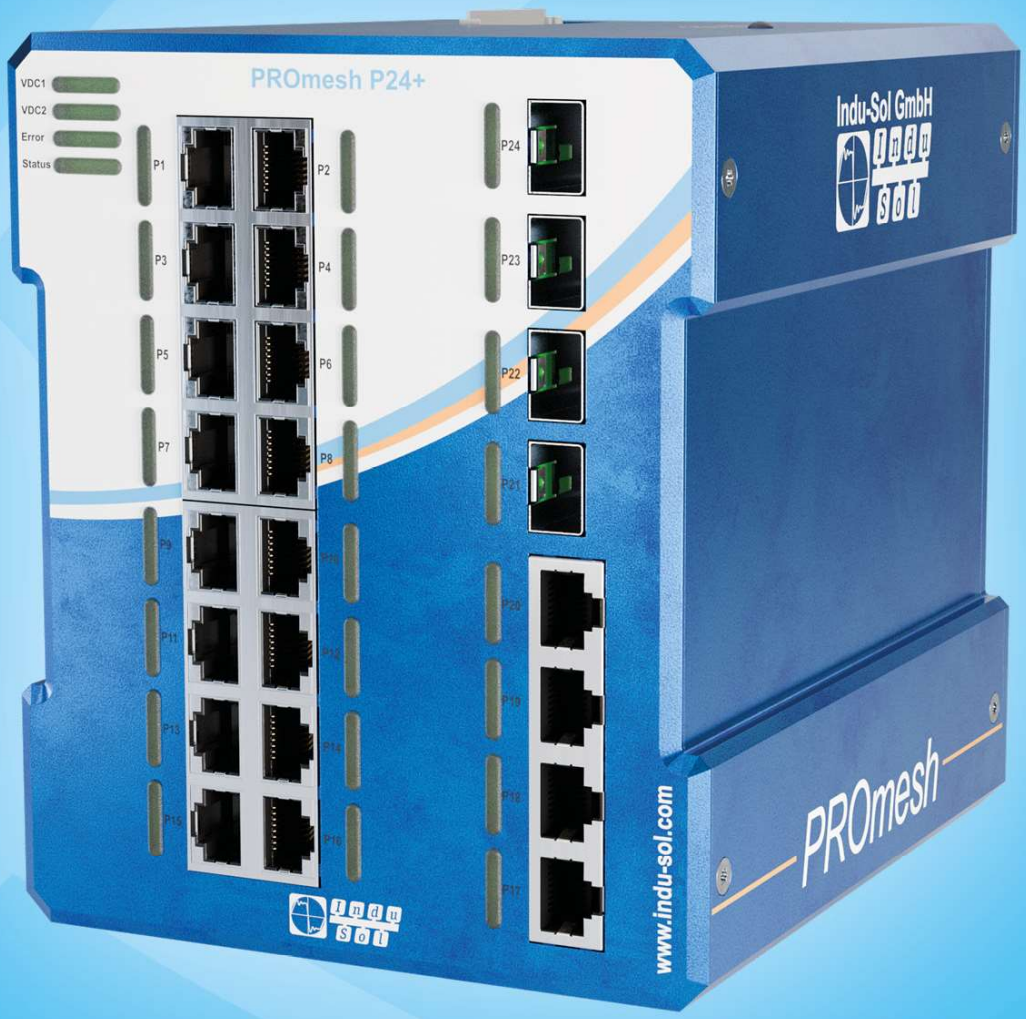
Indu-Sol GmbH – Specialist in Industrial Networks

PROmesh P24+

UserManual



Full-Managed Switch für PROFINET & EtherNet/IP

PROFIBUS PROFINET INDUSTRIAL ETHERNET CAN DeviceNet SafetyBUS p ASi INTERBUS EMC WIRELESS

Indu-Sol Ltd

Blumenstraße 3

042626 Schmölln

Tel.: +49 (0)34491 / 580-0

Fax: +49 (0)34491 / 580-499

Email: info@indu-sol.com

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

Our **technical support** team can be reached on +49 (0)34491 / 580-321, on weekdays between 7.30 am and 4.30 pm (CET). Alternatively, you can email us at: support@indu-sol.com

Is your system down? You can reach our emergency service 24 hours a day on: +49 (0)34491 / 580-0.

Revision history

Date	Revision	Change(s)
19.03.2026	0	First version

Table of contents

1 Legal notices and safety and industrial security requirements

1. Copyright and documentation notice

We reserve the right to make technical changes in the course of product development. Specifications, illustrations and descriptions are provided for information purposes only and do not constitute guaranteed characteristics. No legal claims may be derived from the content of this documentation.

The content has been carefully checked. However, discrepancies between the documentation and the product cannot be entirely ruled out. Necessary corrections will be made in subsequent versions.

---

2. Intended Use

The device is part of an Industrial Automation and Control System (IACS) and is intended exclusively for the applications described in the technical documentation.

Safe and proper operation requires:

- proper transport and storage
- professional assembly, installation and commissioning
- operation in accordance with the intended use
- operation within specified environmental conditions
- regular maintenance
- Integration into a suitable industrial security concept

Any deviation from these points is considered improper use.

---

3. **Safety – Personal and plant safety**

Commissioning, operation and maintenance must be carried out exclusively by qualified personnel.

Persons are considered qualified if they are authorised in accordance with relevant safety standards to:

- commission equipment and systems
- to earth electrical circuits correctly
- to label installations safely

Physical access to the device must be restricted to authorised persons (IEC 62443-3-3, SR 1.1, SR 7.6). Removable storage media may contain sensitive configuration or access data.

Unused physical interfaces must be deactivated or technically secured (IEC 62443-3-3, SR 5.2, SR 7.6).

4. Industrial Security in accordance with IEC 62443

4.1 Scope and Security Level

The device supports security measures to achieve:

Security Level 0 to Security Level 2 (SL0–SL2) in accordance with IEC 62443-3-3.

SL2 addresses protection against deliberate attacks using simple means, limited resources, generic capabilities and a moderate level of motivation.

The product is not intended for SL3 or SL4.

Overall responsibility for risk assessment, zoning, protective measures and operation lies with the operator.

4.2 Security by Default

(IEC 62443-3-3: SR 1.1, SR 2.1, SR 5.2, SR 7.6)

The device is delivered in a secure default state:

- Insecure protocols are disabled by default
- Secure communication protocols are enabled
- Default passwords must be changed before commissioning
- Unnecessary services can be disabled

Insecure services may only be enabled deliberately and within protected network areas.

4.3 Security architecture (defence-in-depth)

(IEC 62443-3-3: SR 5.1, SR 5.2, SR 5.3)

The device must be operated within a zone and conduit model. Internal and external networks must be separated logically or physically.

A direct connection to untrusted networks is only permitted if appropriate protective measures are in place, e.g.:

- VPN (IPsec, OpenVPN)
- Network segmentation
- VLAN structuring

The number of services offered externally must be limited to the minimum necessary.

4.4 Identification and Authentication

(IEC 62443-3-3: SR 1.1, SR 1.2, SR 1.3, SR 1.5, SR 1.7)

The device has a role-based access concept.

All default passwords must be changed prior to commissioning. Strong password policies must be applied.

The following is recommended:

- Use of complex passwords
- No reuse of identical passwords
- Regular password changes
- Immediate change if compromise is suspected
- Secure storage of login details

The loss of access data may necessitate a reset to factory settings, which will delete all configuration data.

4.5 System integrity and patch management

(IEC 62443-3-3: SR 3.1, SR 3.2, SR 3.4, SR 7.8)

The firmware is digitally signed. Security updates are provided via a dedicated update service.

The operator is obliged to:

- check for available updates on a regular basis
- to install security updates promptly
- Use only supported firmware versions

Updates are carried out manually; there is no automatic installation.

4.6 Secure communication

(IEC 62443-3-3: SR 2.1, SR 2.2, SR 2.6, SR 4.1)

Secure protocols such as HTTPS, SSH, SNMPv3 or NTP are to be preferred.

Insecure protocols such as Telnet or TFTP are disabled by default and may only be used within protected network zones.

When using SNMP:

- Community names must be changed
- Restrict write permissions
- Use SNMPv3 authentication and encryption mechanisms

4.7 Protection against network attacks

(IEC 62443-3-3: SR 5.1, SR 5.2, SR 7.1, SR 7.6)

To minimise DoS and Layer 2 risks, appropriate measures must be implemented, e.g.:

- VLAN structuring
- Segmentation
- Restriction of physical access
- Deactivation of unused ports

Link-layer protocols without their own authentication mechanisms (e.g. ARP) can represent attack vectors and must be secured through appropriate architectural measures.

4.8 Logging and monitoring

(IEC 62443-3-3: SR 6.1, SR 6.2, SR 6.3, SR 6.4)

The device logs security-related events, in particular:

- Login attempts
- Configuration changes
- Restarts
- Firmware updates

System events must be transmitted to a central logging server (Syslog). The logging server must be operated within a protected security zone.

Log data must be analysed regularly for security-related events or anomalies.

4.9 Operation in an insecure infrastructure

Operation within non-segmented or unprotected networks increases the risk of cyber attacks.

No product liability is accepted for damage or security incidents resulting from improper integration or a lack of protective measures.

---

5. Life cycle considerations

(IEC 62443-3-3: overarching governance requirements)

The security of the device must be ensured throughout its entire operational lifecycle.

This includes:

- regular security assessments of the entire system
- documentation of security-related changes
- continuous review of the network architecture
- Integration into an overarching security or ISMS framework

---

6. Decommissioning and data protection

(IEC 62443-3-3: SR 3.4, SR 7.8)

Before decommissioning:

- the device must be reset to factory settings
- reset any storage media

This is to protect confidential configuration and access data.

---

7. Recycling and disposal

The product is recyclable and complies with the requirements of the WEEE Directive 2012/19/EU.

Electrical and electronic equipment must not be disposed of with household waste. Disposal must be carried out by authorised waste management companies in accordance with national regulations.

---

8. Repair and service

Please contact your Indu-Sol representative or use Indu-Sol's general contact point for handling complaints or technical support to determine the appropriate course of action (repair, replacement, etc.).

2 General Information

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

2.1 Overview of the *PROmesh P24+* – Range of functions

The ***PROmesh P24+*** is an industrial Ethernet switch with management and PROFINET functionality that can be configured easily and conveniently via a web application. Thanks to its comprehensive features, it supports the effective implementation of all network topologies, such as bus, star and ring structures, within your facility.

features:

- Web application for configuration
- Reverse-polarity-protected 12–48 V DC power supply, redundant operation possible
- Line diagnostics
- Leakage current monitoring
- Port statistics (network load in ms, errors, discards)
- Alarm management
- 20 x RJ45 ports (10/100/1000 Mbit/s)
- 4 x SFP+ ports (10/100/1000/2500/10,000 Mbit/s)
- MAC address table: 16K (16,384 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)
- Web interface access via HTTP / HTTPS
- Simple Network Management Protocol (SNMP), v1, v2c, v3
- Updating, saving and backing up the system configuration via web interface, TFTP

2.2 Contents of the package

The scope of delivery includes the following items:

- ***PROmesh P24+*** including port caps for RJ45 and SFP
- 7-pin pluggable terminal block, 2.5 mm² (power supply and alarm contact)
- SD card
- User quick start guide (hard copy)

Please check the contents of your delivery for completeness before commissioning. If you have any questions, please contact our Technical Support team immediately before commissioning.

Before initial commissioning, insert the external memory card into the corresponding slot on the rear of the device (see Figure 1).

2.3 Device-specific safety instructions

Before commissioning the device, check that it is in perfect external condition. If you suspect any damage, return the ***PROmesh P24+*** to your supplier immediately and do not put the device into operation. Our Technical Support team will be happy to assist you with any queries.

The ***PROmesh P24+*** has been developed for use in PROFINET applications in accordance with Conformance Class B. To ensure full compliance with PROFINET standards, please also ensure that the data cables used are selected in accordance with the standard.

Always observe the technical specifications of the device to ensure safe and optimal use. The device has been developed for protection environments in accordance with IP20. Take appropriate measures in the event of a different operating environment to ensure the proper functioning of the device.

Do not open the housing under any circumstances. There are no serviceable parts inside. Unauthorised opening of the housing will invalidate any warranty claims.

3 Connections and status indicators on the device

3.1 Device connections

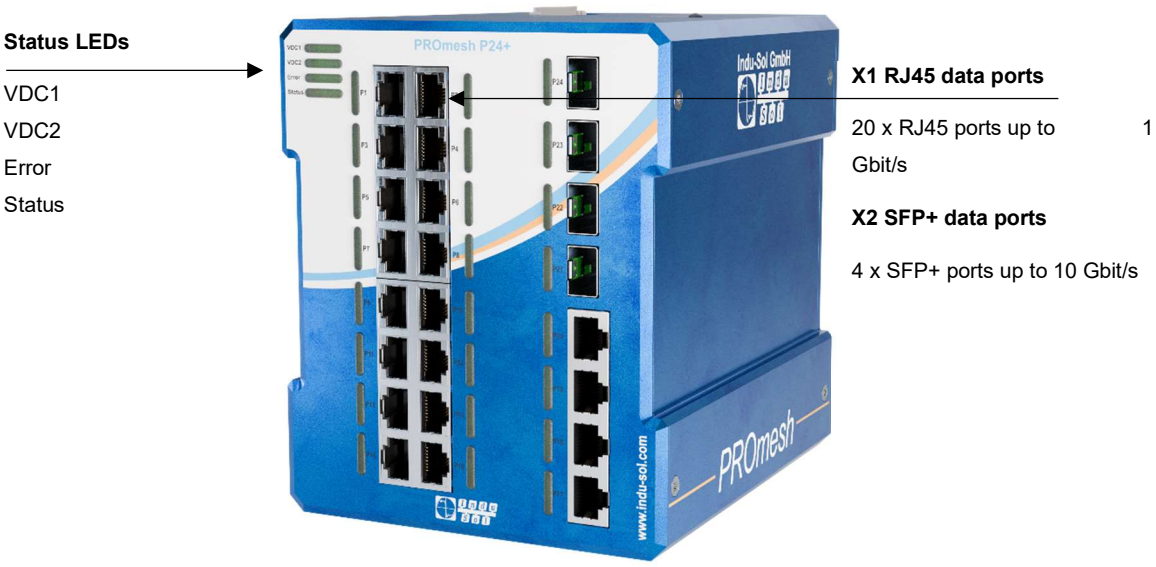


Figure1: Device connections – front

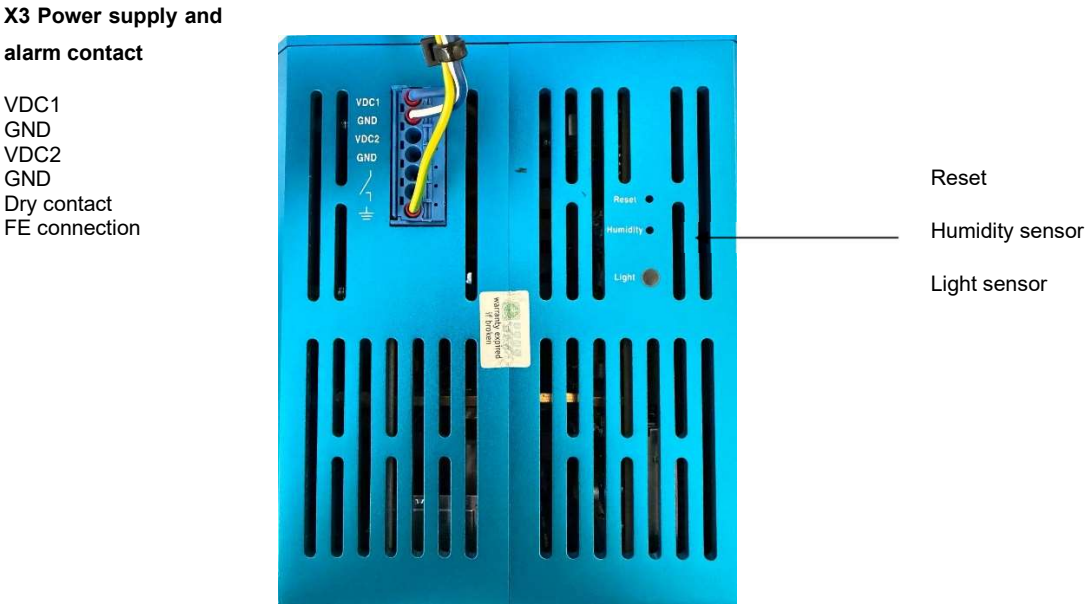


Figure2: Device connection – top view

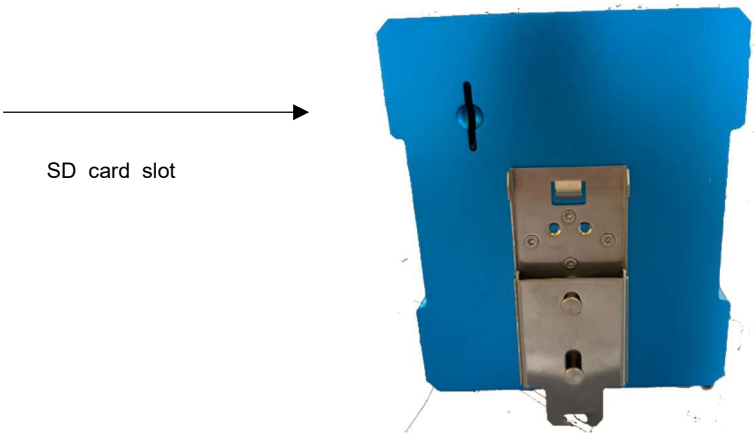


Figure3: Device connections – rear view

3.2 Installation and mounting

The ***PROmesh P24+*** is designed for individual use in various types of control cabinets and can be mounted on a standard 35 mm DIN rail.

To secure the device, use only the existing DIN rail mounting or, if necessary, purchase appropriate spare parts to ensure adequate electrical contact and the mechanical load-bearing capacity of the device

The ***PROmesh P24+*** is mounted vertically in the control cabinet on a 35 mm DIN rail in accordance with DIN EN 60715.

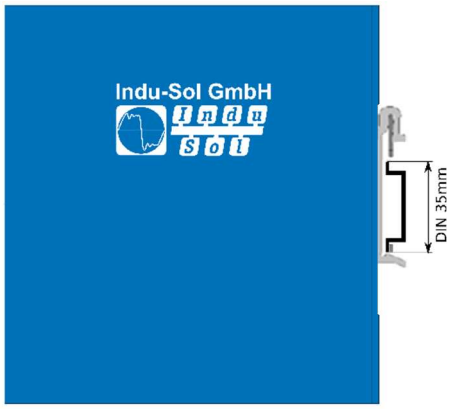


Figure4: Side view with terminal block on the right

To ensure correct installation, it is recommended that the following clearances from other components are maintained:

- To the left and right: 20 mm
- Upwards and downwards: 50 mm

Installation:

1. Position the top of the unit against the top-hat rail with the rear edge.
2. Use a screwdriver to pull the lower locking spring downwards or release it.
3. Press the device downwards or tilt it, allowing the lower locking spring to return to its original position.
4. Check the fit – the device must sit firmly on the rail.

Removal:

1. Use a screwdriver to pull the lower locking spring downwards or release it.
2. Tilt the device forwards.
3. Lift it upwards off the rail.

Do not install the ***PROmesh P24+*** switches directly next to devices that generate strong electromagnetic interference fields, such as transformers, contactors, frequency converters, etc.

Do not install the ***PROmesh P24+*** switches directly next to devices that generate a lot of heat, and protect the switch from direct sunlight to prevent unwanted heating. Protect the ***PROmesh P24+*** from additional heat radiation and observe the approved storage and operating temperature range.

3.3 Power supply connection

Operate your ***PROmesh P24+*** with a nominal voltage of 12 V to 48 V DC. To ensure system availability, connect the redundant power supplies VDC1 and VDC2 to the correspondingly labelled terminals on the supplied 7-pin terminal block adapter (VDC1, GND and VDC2, GND). The power supply must comply with UL60950-1/UL62368-1, Class 2 (NEC), limited energy source (UL61010-1).
The 7-pin 2.5 mm² terminal block on the top of the device is assigned as follows:

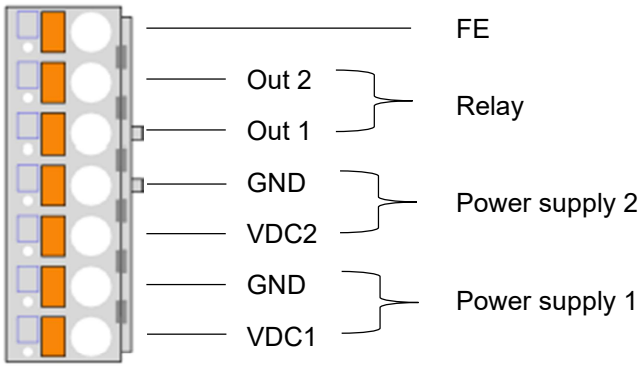


Figure5: Terminal block pin assignment

The labels listed are also found on the device next to the terminal block.

There is a potential-free fault relay contact (normally closed) on the device's internal OUT terminals. The relay serves as an alarm receiver and can be linked to various alarm triggers in the software. Depending on the configuration, the relay contact then opens, for example, in the event of a power failure or a change in the port's status.

3.4 LED indicators

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

In addition, each of the 24 data ports has a status LED.

The LEDs display the most important diagnostic information regarding the device and connection status of the ***PROmesh P24+*** in your network (see Table 1).

LED	Status	Meaning
VDC1/VDC2	Green	Sufficient voltage at connection
	Off	Insufficient voltage at connection
Status	Green	Active communication link to the controller
	Yellow	No communication link to the controller
Err	Red	Power failure, port error or configured alarm active
	Off	No power failure, no port error and no configured alarm active
LED Port 1–24	Off	No link
	Flashing	Link + data exchange (flashing speed indicates link speed)
	On	Link

1 table: LED- functions

3.5 Reset button

Should any unforeseen issues arise with the ***PROmesh P24+*** that render it inaccessible, the reset button can be used. This allows the ***PROmesh P24+*** to be either restarted or reset to its factory settings. To do this, follow the procedure below:

- Restart the device: Press the reset button for 1 second
- Reset to factory settings: Press the reset button until all LEDs go out (approx. 10 seconds)

3.6 Network integration & commissioning

3.6.1 Data ports

The ***PROmesh P24+*** is equipped with 24 data ports, which, in accordance with the PROFINET 2.4 standard, enable data transfer at speeds of up to 10 Gbit/s. The actual data rate is negotiated by the device via autonegotiation.

3.6.2 Media connection

The ***PROmesh P24+*** offers RJ45 connectivity on 20 ports and 4 ports with SFP slots, which can be configured via a respective SFP module.

When designing, selecting, assigning and terminating your data cable, ensure compliance with applicable standards and secure connections in the connector application to guarantee the maximum possible cable length and cascading of network segments in accordance with your media type.

3.6.3 Cabling

To connect your ***PROmesh P24+*** via the existing data ports, use Category 5 (Cat 5) or higher twisted-pair cables with a maximum cable length of up to 100m. To improve shielding contact, we recommend the PROFINET RJ45 connectors (Item No.: 114030006) from Indu-Sol.

If fibre optic cables are to be connected to the ***PROmesh P24+***, we recommend using SFP modules from Indu-Sol GmbH. When laying the fibre optic cables, please note the maximum length, which is limited by the selected SFP modules.

3.7 Network topologies & redundancy

The devices in the PROmesh product family can be used in redundant networks, such as mesh networks or rings, as well as in star-shaped switched Ethernet networks, by utilising various protocols.

3.7.1 Network Topologies

Classic Ethernet star structures (see figure 6) can be networked with the ***PROmesh P24+*** switches without any additional configuration. The devices are ready for immediate use.

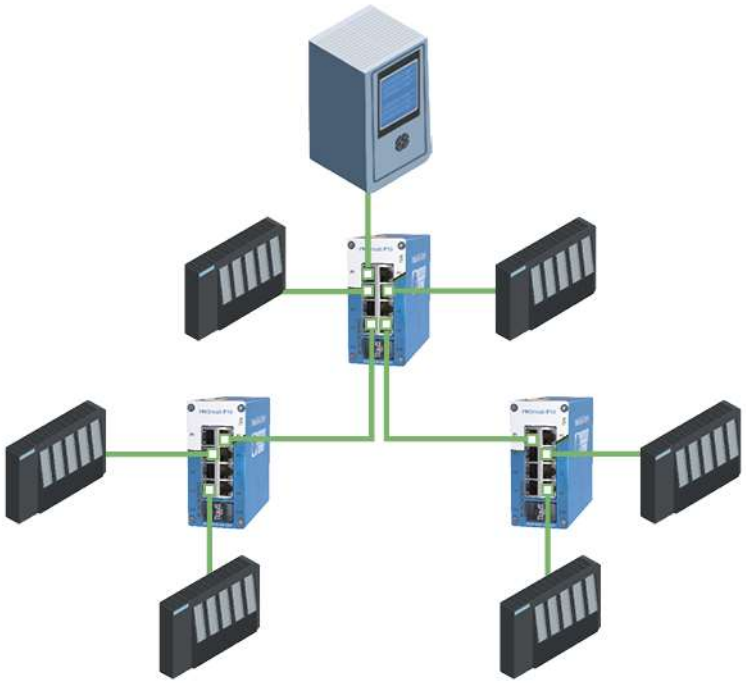


Figure6: ***PROmesh P-switches*** (illustrative image) in a star-shaped network

3.7.2 Ring structure

The ***PROmesh P24+*** fully supports the IEC 62439 standard, thereby enabling deterministic reconfiguration of data forwarding in simple redundancy (ring topologies, see Figure 7). Depending on the size of your system, this enables reconfiguration times of up to 200 ms.

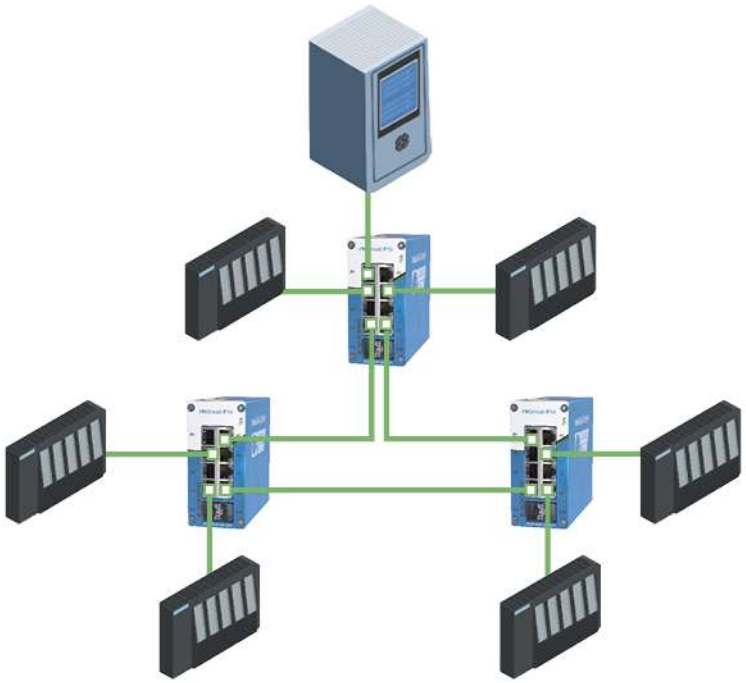


Figure7: ***PROmesh P-Switches*** (illustrative image) in a star-shaped network

4 Web application

The ***PROmesh P24+*** switches are equipped with a modern web interface, allowing them to be conveniently configured from any web browser.

4.1 Preparations

Before using the web management interface, install the ***PROmesh P24+*** switch in the network and ensure that the PC intended for configuring the switches can access the switch via a web browser. The ***PROmesh P24+*** and the client PC to be connected must be in the same IP address range and IP subnet. To do this, you must first assign a suitable IP address to your ***PROmesh P24***+.

The following IP address, subnet mask, administrator username and administrator password are set by default:

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

When you log in for the first time, you will be prompted to change the factory-set password. It is your responsibility to record this password and protect it from unauthorised access.

You can easily configure your intended user addresses using the **Indu-Sol ServiceTool**. This is included in the scope of delivery or is available for free download via the following link:
https://www.indu-sol.com/documentation/servicetool

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

After installing and opening the software, establish a network connection from your computer to a port on the switch and scan the system using the *PROFINET device* search setting. You can then enter the relevant details in the input screen and save them.

If you include the switch in the hardware configuration of the controller within a PROFINET system, the relevant address settings will then be configured automatically via the controller.

4.2 System Login

1. Open a web browser on your computer.
2. Enter the IP address of the ***PROmesh P24+*** switch you are using into the address bar of the web browser and confirm your entry by pressing the *Enter* key.
3. The device's login screen will now appear on the screen.

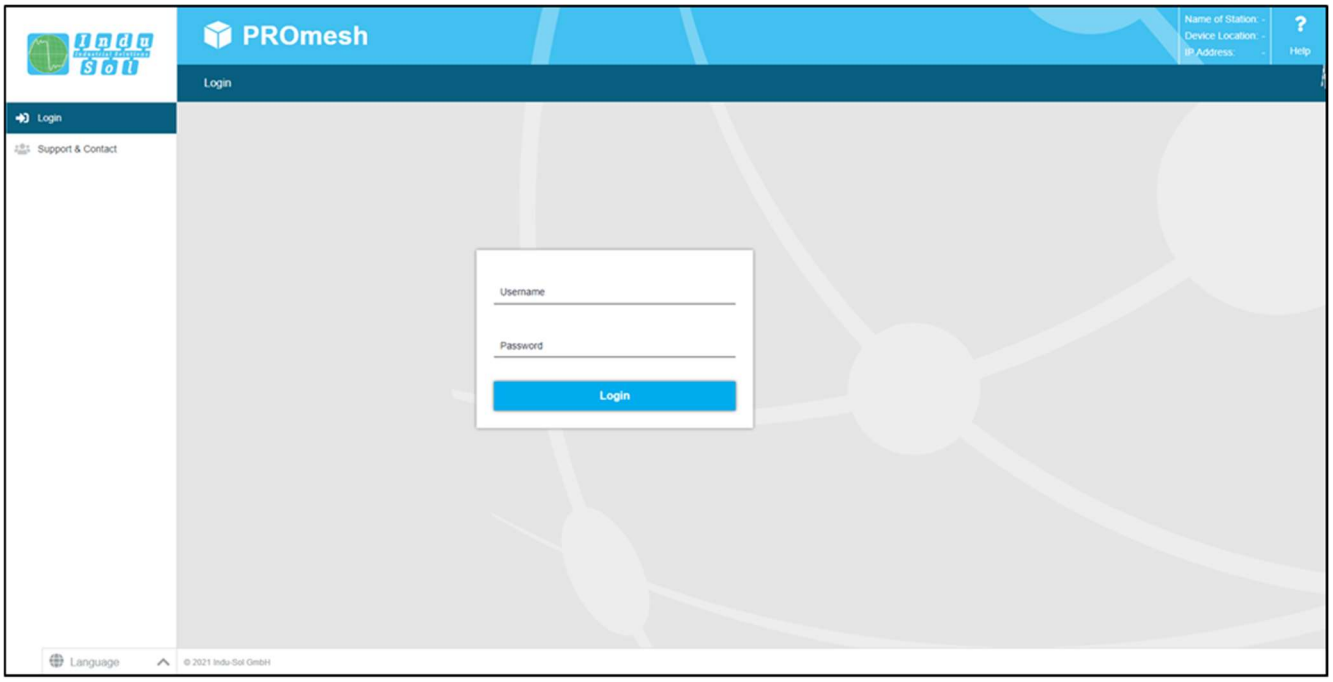


Figure8: Login screen

4. Select your preferred menu language (DE / EN). This can be changed at any time in any menu of the web interface.
5. Then enter your username and password.
6. Press the *Enter* key or click on *Log in* to access the switch's web interface.

4.3 Web interface

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

No error: Communication is working correctly.

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

Error: A critical fault has occurred on the relevant port, resulting in a communication interruption. Urgent action is required to rectify the fault.

No communication is taking place on the respective port. Either no device is connected (possibly also a line interruption) or no telegram traffic can be detected (serious network fault) or the devices are no longer communicating.

4.4 Start

After successfully logging in, you will be taken to the switch's web interface. On the left-hand side are the individual menu items, which are subdivided into further sub-items.

By default, you are taken to the home page after logging in. This overview provides you with a quick and clear overview of the most important information at a glance, such as the device name, PROFINET name (if assigned), the installation location and the IP address. The current user is displayed below the logout button at the right-hand end of the bar. You can log out by clicking the button. The Help button displays tips and explanations for the individual pages.

Under the 'Port Status' sub-section, you can view an overview of the status of the available ports since the switch was cold-booted or reset (Since Last Reset) and within the time frame of the last second (Last Second).

You can switch between two views. The Overview view displays:

- Current partners
- Transmission speed
- Diagnostic messages

are displayed. In the Details view, in addition to the parameters shown in the Overview:

- Line quality value
- Network load per second
- Discards
- Errors
- IP address of the device on the partner port (LLDP)

displayed.

The message window displays the number of events that have occurred. Messages are counted by the switch based on configured alarm triggers and displayed with precise information. Clicking on the alarm bell automatically opens the entries in the message list. The messages, as well as the port count, can be cleared using the corresponding buttons.

The overview of the individual sensors, such as temperature and leakage current, is displayed below the port status.

The leakage current represents the current value measured at the ports and discharged via the switch housing. You can switch between displaying the peak value and the root mean square (RMS) value. This information enables early detection of fault currents that could lead to direct communication faults.

To measure the leakage current correctly, proper earthing of the housing must be ensured.

The other sensor values, such as light, humidity and acceleration, are also displayed in this overview.

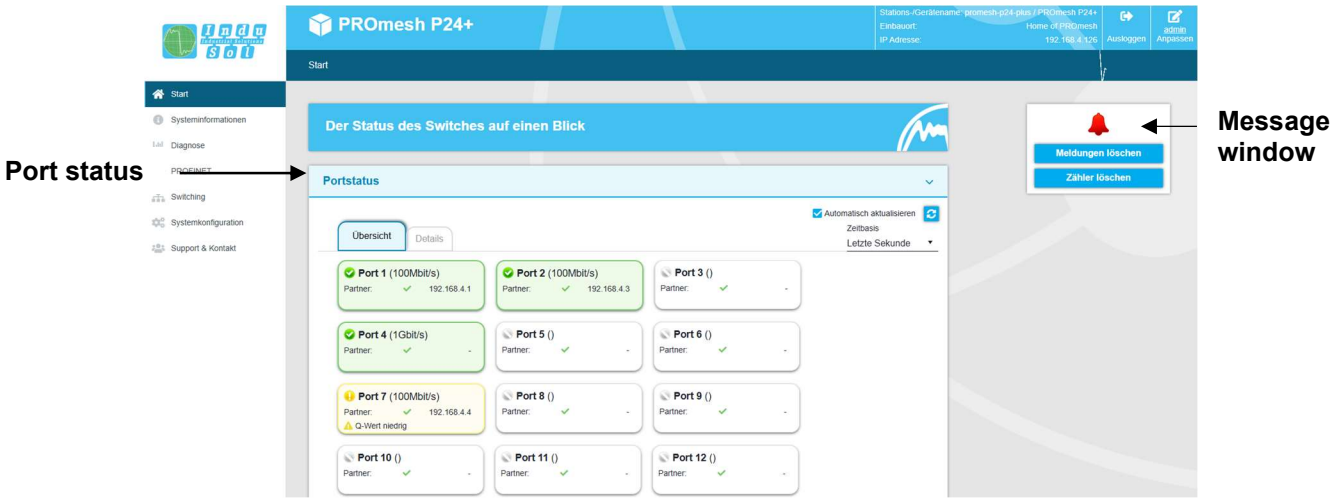


Figure9 : Start screen

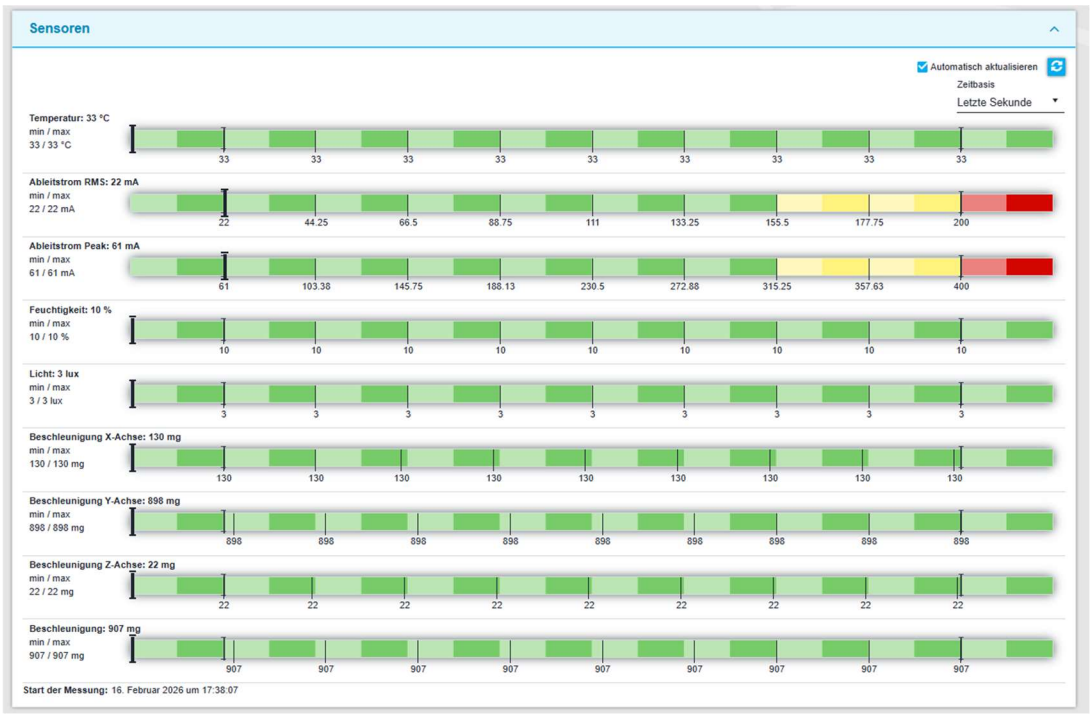


Figure10: Sensor overview

4.5 System information

This menu option displays an overview of the enabled and disabled protocols and functions, alongside the device information. By selecting the relevant edit button, you can navigate directly to the corresponding protocols and functions to adjust their settings.

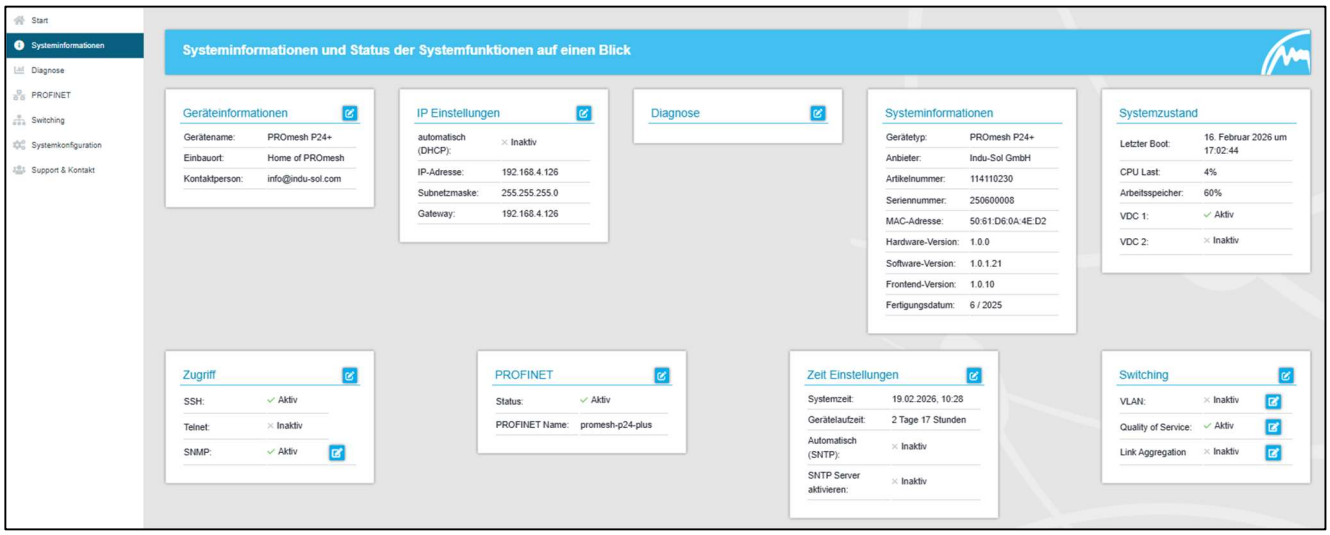


Figure11 : System information

4.6 Diagnostics

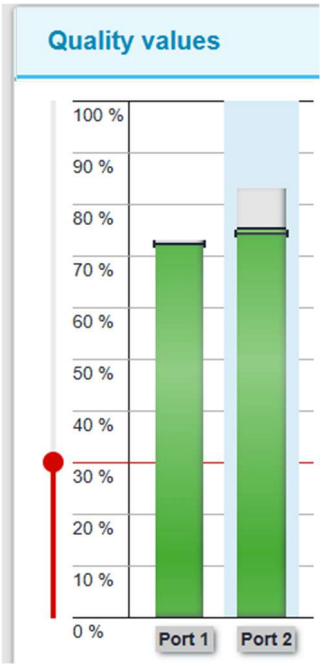
The Diagnostics page provides an overview of the system status of the ***PROmesh P24+*** switch. Further submenus can be opened via the Diagnostics tab.

4.6.1 Link Diagnostics

Link diagnostics are available for ports 1–20, although only active ports are displayed. The quality of the connected links is checked cyclically (every second). The link quality can range from 100% to 0%, with 0% indicating a faulty cable, meaning no data exchange is possible.

Figure12: Quality value

Information bar chart



Three values are displayed per bar.

The grey section of each bar shows its maximum value. The lighter-coloured section, which is bordered by a black line, shows the current quality value. The fully coloured section, which is bounded by a line with two arrows, represents the worst quality value recorded for the connection to date. The colouring of the bars is based on this, following the traffic light colour scheme of green-yellow-red:

- Green: The line quality is fine; no action is required.
- Yellow: The defined threshold value (via alarm trigger, default at 30%) has been undershot. The line quality is insufficient. The connection should be checked during the next maintenance interval.
- Red: No further data exchange is possible. Check the plug contacts and the data cable.

Miscellaneous

The threshold value that turns the bar yellow and recommends a connection check can be adjusted by the user. It is not recommended to set the threshold value below 30%. In the Alarms menu, alarms can be defined for the line quality value, which send notifications via SNMP, PROFINET or email if the threshold value is not met.

SFP diagnostic data

The SFP diagnostic data provides an overview of the status, speed, transmit power, receive strength and temperature.

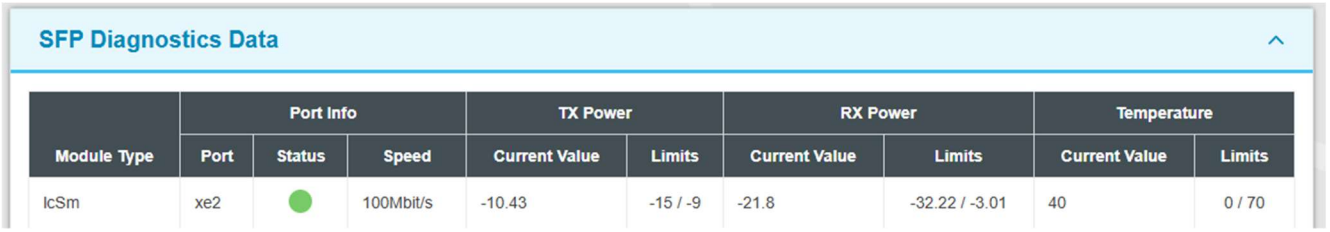


Figure13: SFP diagnostic data

4.6.2 Neighbour Discovery

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Layer 2 protocol that enables the exchange of information (addresses, names and descriptions) between neighbouring devices. An LLDP agent operates on every device that supports LLDP. This agent sends information about its own status at regular intervals and receives information from neighbouring devices.

As this occurs independently of one another, 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

4.6.3 Alarm triggers

The Alarm Trigger menu item is used to configure alarm triggers and alarm recipients. Alarms can be created for the following events:

- Line quality value falling below the threshold
- Exceeding a leakage current
- Error and discard messages with individual threshold settings

- Exceeding the network utilisation on a port
- Power supply status
- Port status change
- Alarm triggers with upper and lower threshold limits for temperature, light, humidity and acceleration

The alarms created can be linked to one or more alarm recipients, including:

- SNMP traps
- PROFINET

If one of the configured alarms is detected and triggered, the software forwards the event to the relevant alarm receiver and additionally documents the event as a log message.

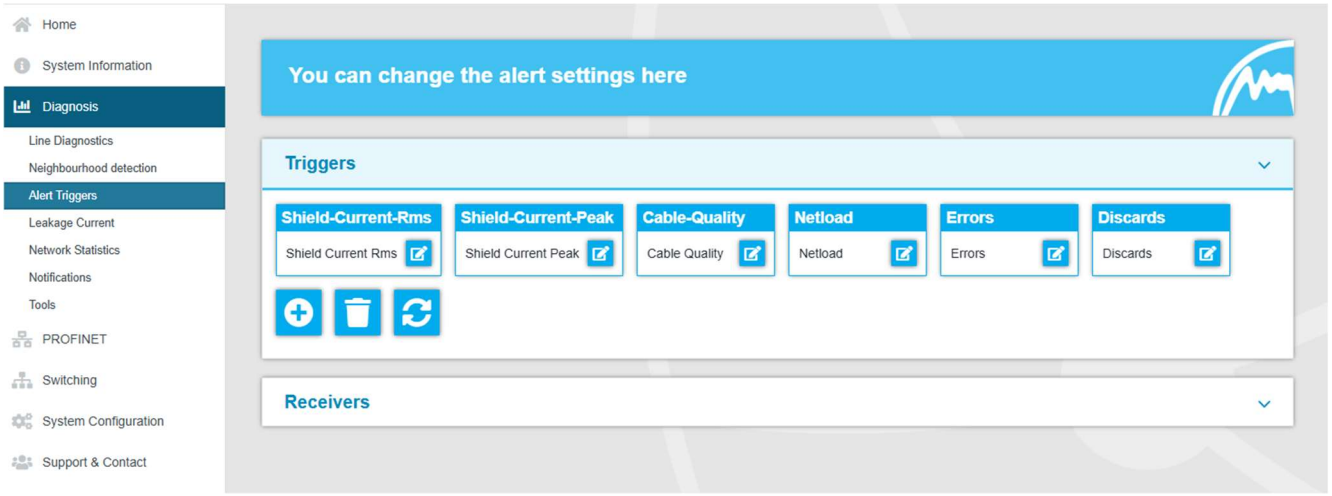


Figure14: Alarm triggers

Add and edit alarm triggers

New alarms and notifications can be added by clicking the button with the "+" symbol. If alarms already exist, the user can edit or delete them using the button. In the upper part of the "Alarm Trigger" pop-up, the user can select the various alarms. Whilst creating and editing alarms, the associated recipients can be selected in the lower part of the pop-up and linked to the alarm trigger in this way, provided the alarm recipients have already been defined.

Adding and editing alarm recipients

New alarm recipients can be added by clicking the button with the "+" symbol. In addition to this, the recipients Email, SNMP and Message can be selected. The associated alarm triggers can be linked to the current recipient in the lower part of the pop-up.

- With the Simple Network Management Protocol (SNMP), error notifications are generated by the device and sent unsolicited to a management station. As the packets are not acknowledged, the device cannot determine whether the manager has received the information.
- When using the email function, the user can specify an email address and an SMTP (Simple Mail Transfer Protocol) server. In the event of an alarm, the device sends an email to the user. Authentication can be enabled as an option. To do this, the necessary login details must be entered.
- The 'PROFINET' alarm receiver is permanently set within the system following the integration and configuration of the switch in a Profinet network and cannot be changed within the device. The alarm triggers for the individual events are activated in the controller's hardware configuration. If a trigger is activated, the switch sends an alarm message to the controller. This information can then be processed further within the PLC via the programming.

4.6.4 Leakage current

Leakage current monitoring (Fig. 15) enables the sum of all shield currents from the cables, which are discharged via the device into the equipotential bonding system, to be continuously recorded and evaluated. For this purpose, in addition to the current value, the corresponding spectrum with the respective frequency components is provided. With this function, the PROmesh series provides mechanisms for detecting EMC interference or coupling.

Further functions:

- Download of the frequency spectrum following a threshold exceedance
- Switching between decimal and logarithmic scales

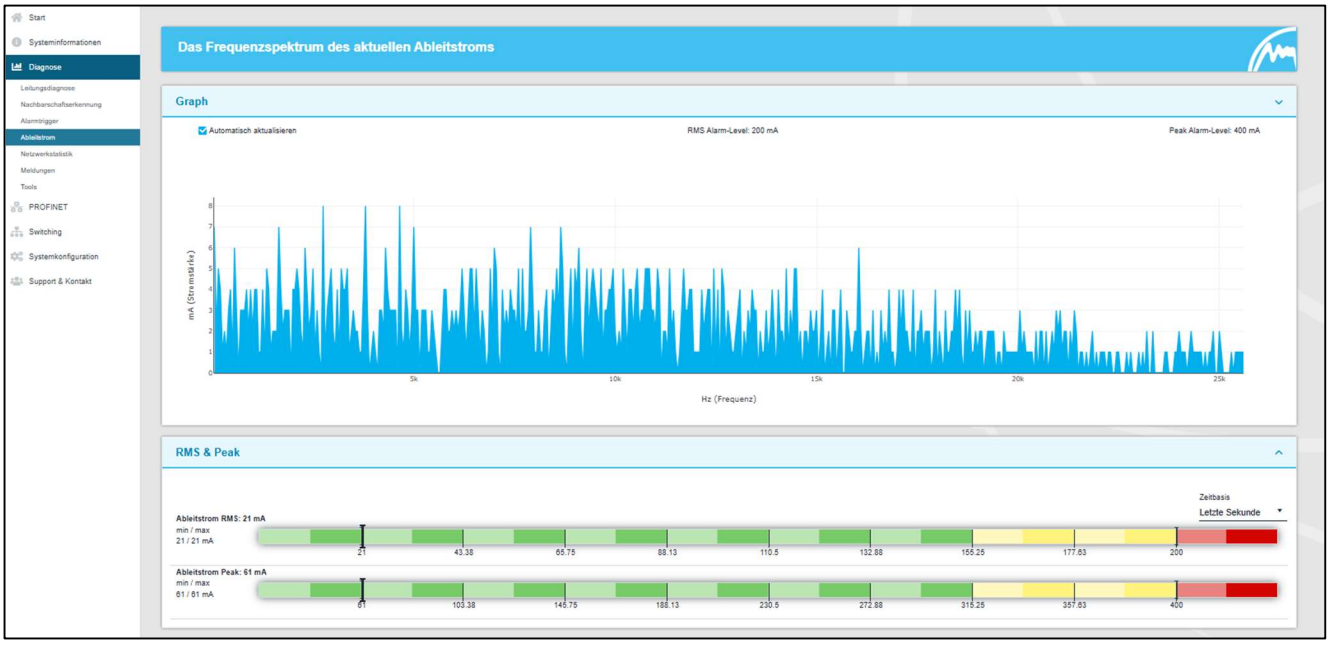


Figure15 : Leakage current

4.6.5 Network statistics

The Network Statistics page provides information on the data traffic of the individual ports. This information is useful for diagnostic purposes or in the event of network problems.
The main overview of the network statistics provides the following information for each port:

- Data packets received
- Data packets sent
- Network load per second
- Network load per millisecond
- Errors (corrupted telegrams)
- Discards (telegrams discarded due to excessive data volumes)

Network Statistics

Port	max. Netload		Errors	Discards	Packets	
	/ ms	/ s			sent	received
1	0 %	0 %	0	0	391,718	22,961
2	0 %	0 %	0	0	412,503	55,612
3	0 %	0 %	0	0	395,093	562,013
4	0 %	0 %	0	0	416,402	47,473
5	0 %	0 %	0	0	0	0
6	0 %	0 %	0	0	0	0
7	0 %	0 %	0	0	15,634	10,187
8	0 %	0 %	0	0	0	0
9	0 %	0 %	0	0	14,438	1,243
10	0 %	0 %	0	0	12,908	2,962
11	0 %	0 %	0	0	0	0
12	0 %	0 %	0	0	15,626	2,565
13	0 %	0 %	0	0	15,177	1,467
14	0 %	0 %	0	0	0	0
15	0 %	0 %	0	0	539,178	286,769
16	0 %	0 %	0	0	391,874	39,542
17	0 %	0 %	0	0	0	0
18	0 %	0 %	0	0	0	0
19	0 %	0 %	0	0	0	0
20	0 %	0 %	0	0	0	0
21	0 %	0 %	0	0	0	0
22	0 %	0 %	0	0	14,802	3,042
23	0 %	0 %	0	0	0	0
24	0 %	0 %	0	0	0	0

Time since last reset: 23 Hours 15 Minutes

Figure16: Network statistics

Resetting the values

In the top-right corner, you can reset all counters using the ‘Clear counters’ button.

Detailed network statistics

The statistics details record the size of individual packets statistically up to various thresholds (up to 64, 127, 255, 511, 1023, or 1518 bytes).

For sent packets, a distinction is made between:

- Number of unicast packets (packets sent to a single recipient)
- Number of non-unicast packets

For received packets, a distinction is made between:

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

The *‘Packets up to bytes’* row provides information on the number of packets of various sizes. Here, the number of received packets up to 63, 127, 255, 511, 1023, or 1518 bytes in size is recorded.

4.6.6 Messages

The messages are intended to help the user view status and error messages relating to the various functions. The messages are displayed in the overview with the date and time, a description and a source. As the log entries are not stored in the device, they are no longer available after a device restart or a power failure. To archive the messages permanently, it is possible to use an external syslog server or the SD card.

Backing up messages

- Syslog server: To save the messages on a syslog server, enable this function. Enter the IP address of the syslog server in dotted decimal notation, select ‘File’ under Media Type and save the settings using the Apply button. Please check that the server is accessible and that it saves the messages to a file.

Resetting entries

- The “Delete Messages” button removes all entries from the table. The time at which the entries were deleted can then be identified from the first entry with the description “user log clear” and source “IMI”.

SD card export

- Under the ‘SD Card Export’ tab, you can save the messages to the SD card after you have specified the file path where the messages are to be saved.

4.6.7 Tools

Under the "Tools" tab, you can perform a ping and a traceroute by entering the destination IP address in the corresponding field.

4.7 PROFINET

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

The device is designed as a Profinet IO device for connecting decentralised peripherals to a Profinet controller. The device supports Conformance Class B. For this, the switch's GSDML file is required and must be loaded into your hardware configuration tool. You can find the GSDML file, for example, at the following link:

https://www.indu-sol.com/documentation/promesh-p24-plus

Under the PROFINET menu item, you will see an overview of the stored settings, such as the PROFINET name, DCP forwarding for the ports and, provided there is an active communication link to a PROFINET controller, information about the controller and how long the communication link has been active.

If a communication connection is active, the parameters are read-only; if this is not the case, you can also configure them on the page.

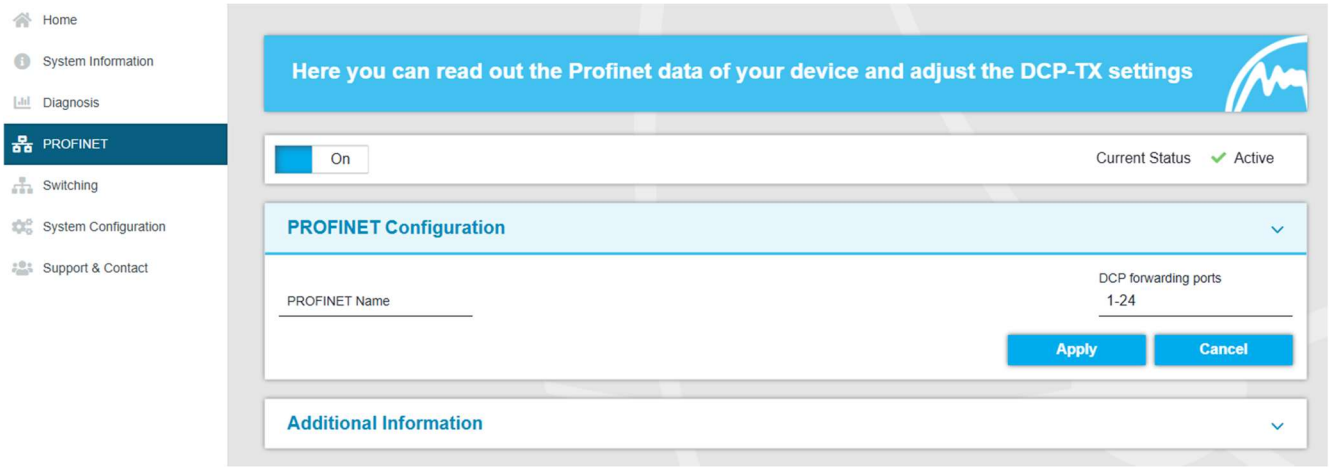


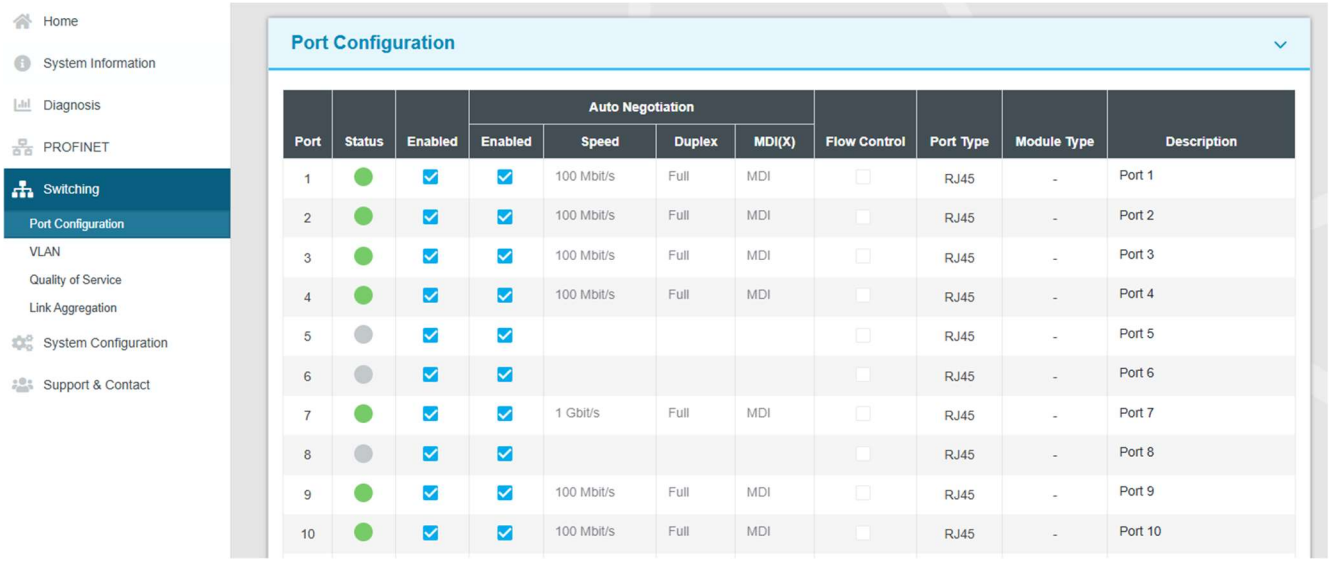
Figure17: PROFINET

4.8 Switching

This page provides an overview of the enabled and disabled functions in the Switching section. You can immediately see which functions are currently enabled. By clicking the Edit button, you can go directly to the various pages and make further settings there.

4.8.1 Port configuration

The table provides an overview of the current configuration of the individual ports. The columns Enabled, Autonegotiation, Flow Control and Description are also editable.



Port	Status	Enabled	Auto Negotiation				Flow Control	Port Type	Module Type	Description
			Enabled	Speed	Duplex	MDI(X)				
1		☑	☑	100 Mbit/s	Full	MDI	☐	RJ45	-	Port 1
2		☑	☑	100 Mbit/s	Full	MDI	☐	RJ45	-	Port 2
3		☑	☑	100 Mbit/s	Full	MDI	☐	RJ45	-	Port 3
4		☑	☑	100 Mbit/s	Full	MDI	☐	RJ45	-	Port 4
5		☑	☑				☐	RJ45	-	Port 5
6		☑	☑				☐	RJ45	-	Port 6
7		☑	☑	1 Gbit/s	Full	MDI	☐	RJ45	-	Port 7
8		☑	☑				☐	RJ45	-	Port 8
9		☑	☑	100 Mbit/s	Full	MDI	☐	RJ45	-	Port 9
10		☑	☑	100 Mbit/s	Full	MDI	☐	RJ45	-	Port 10

Figure18: Port configuration

The columns in detail:

- Port: Specifies the port number, which is also marked on the housing.
- Status: Status indicates the current state of the ports:
  - green: The port is active and a connection is established.
  - grey: The port is inactive or deactivated
- Enabled: Individual ports can be enabled or disabled. This allows you to specify whether a port can be used or not.
- Autonegotiation: If this function is enabled, the transmission speed and duplex mode are configured automatically. The device and the connected remote station negotiate the settings automatically. If autonegotiation is disabled, the settings can be set manually:
  - Speed: The data rate of the ports can be set to a fixed value. You can set a data rate of 10 Mbit/s, 100 Mbit/s or 1 Gbit/s.
  - Duplex: The duplex mode can be switched between half-duplex and full-duplex. This setting is therefore fixed for a connection.
  - MDI(X): The device can perform auto-crossover detection by default. This means that the switch automatically detects whether the device is connected via a crossover or non-crossover cable.
- Flow control: Flow control ensures that, in the event of a port becoming overloaded, the received data packets are ignored and the connected device is signalled to stop transmitting.
- Port type: This indicates whether the port is an RJ45 or SFP port.

- Module type: In the case of an SFP port, this shows which SFP module (multimode, single-mode or copper) is connected.
- Name: In this column, you can assign a name to the ports. The names are displayed throughout the configuration process and make it easier to select the correct settings and diagnose faults. Click directly on the port name and edit the name in the line.

4.8.2 VLAN

A virtual LAN (VLAN) is a logical group of network devices. It allows a section of the network to be isolated. All data traffic from network devices in a VLAN group is transferred only within that VLAN group.

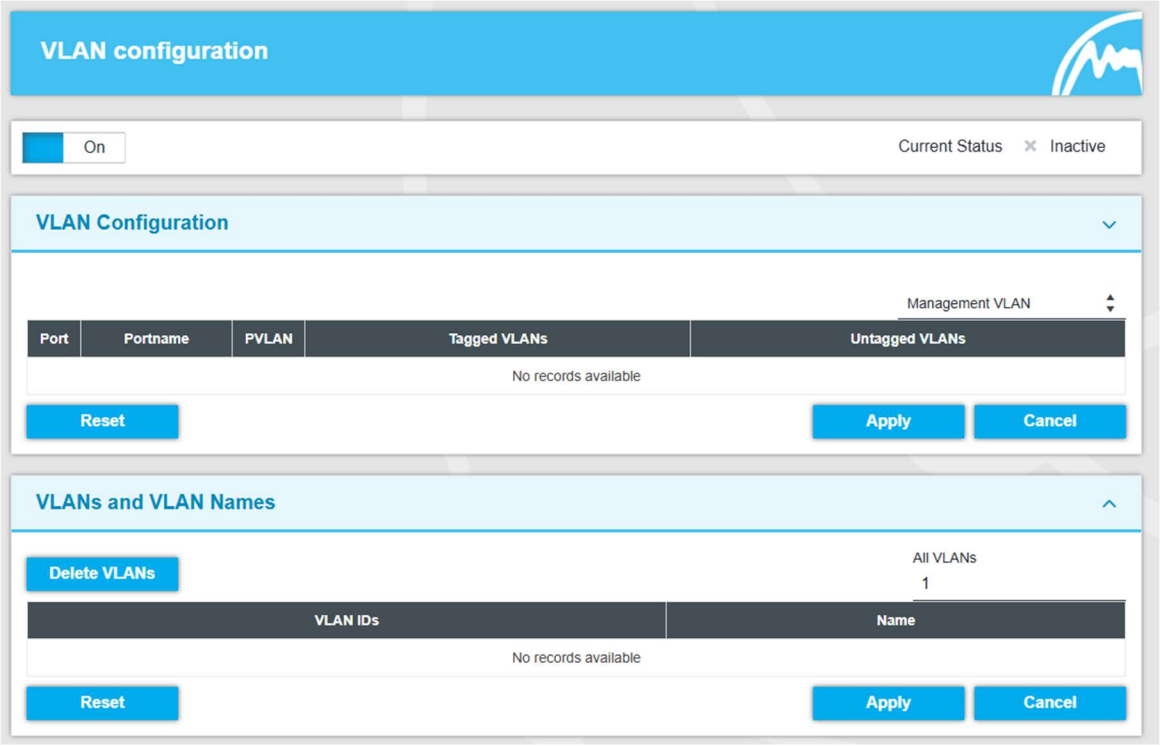


Figure19: VLAN

In the VLAN menu, VLAN settings can be configured for each individual port. Here, you can define on a port-by-port basis which VLAN a port should belong to, as well as in which VLANs the port should be untagged or tagged. You can also set in this menu which VLAN should be the management VLAN.

By default, VLAN is disabled. This means the switch operates in transparent mode. If VLAN is enabled, the switch switches to bridge mode.

- Management VLAN:
  - There is only one management VLAN
  - Can be set globally
  - Defines the VLAN via which the switch management functions (e.g. web interface, PROFINET connection, etc.) can be accessed

    - At least one port must be assigned to the switch's management VLAN
    - If, for example, the switch is assigned to a controller via TIA in a PROFINET communication, it is important that the switch's management VLAN is in the same VLAN as the PROFINET communication
- PVLAN (PVID):
    - Only one ID can be assigned to each port
    - The PVID determines which internal switch VLAN group the incoming packet is assigned to
    - This does not yet change the VLAN tag in the packet header. Only when the packet leaves the switch via a tagged port is the VLAN tag set according to the PVID of the incoming port.
- Untagged port (also referred to as an access port in IT):
    - Ports that are configured as untagged within a VLAN can receive and forward packets with that VLAN ID
    - A port can be configured as an untagged port in multiple VLANs if the devices connected to this port are required to communicate with multiple VLANs
    - Untagged ports do not add a VLAN tag to the packet when sending
    - As a rule, untagged ports should be used in the connection between the switch and the end device
- Tagged port (also referred to as a trunk port in IT):
    - Ports configured as tagged within a VLAN mark outgoing packets with a VLAN tag
    - A port can be configured as a tagged port in multiple VLANs
    - A port that is configured as a tagged port in multiple VLANs must be configured as an untagged port in another VLAN
    - A port must not be both a tagged and an untagged port in a VLAN at the same time
    - As a rule, tagged ports should be used in switch-to-switch connections
    - This means that VLANs are not limited to individual switches, but can also be operated across multiple switches

Application example:

For a more detailed explanation of VLANs and their configuration, the following practical example is set up and configured.

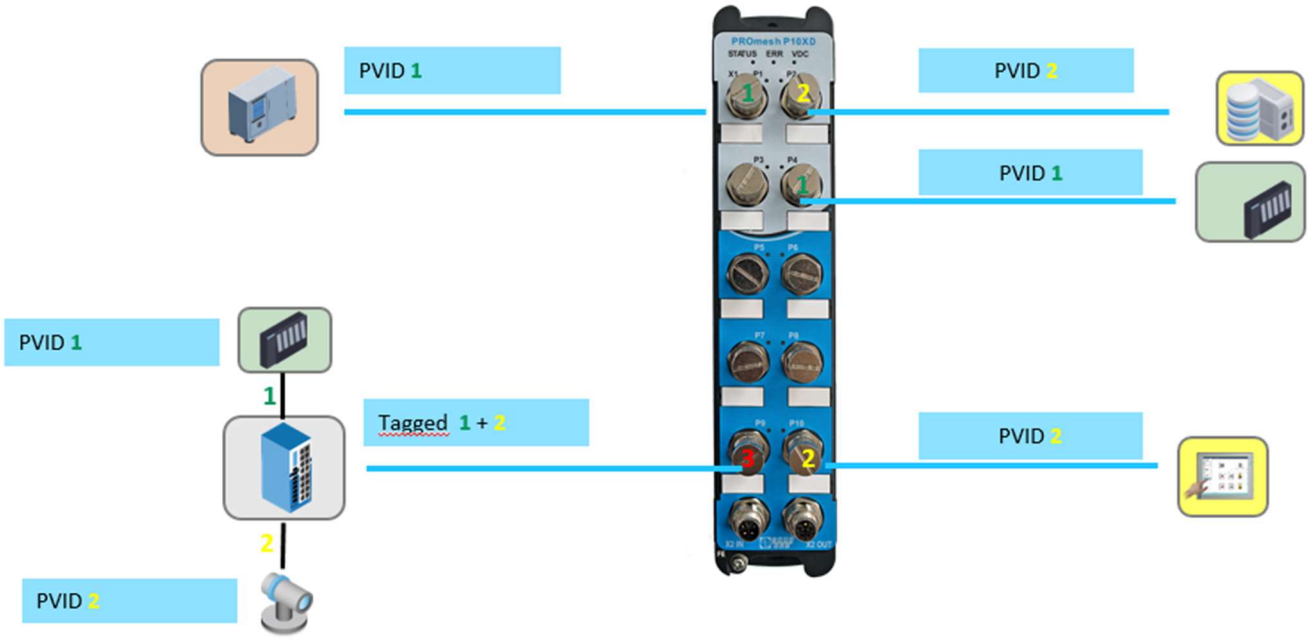


Figure20: VLAN application using the P10XD as an example

To separate PROFINET communication (VLAN 1 – marked green) from other TCP/IP communications (VLAN 2 – yellow), the switch must be logically separated via VLAN. PROFINET devices are connected to Port 1 and Port 4; therefore, these two ports are to be assigned to VLAN 1 and are configured accordingly with PVID 1. As the switch itself is in communication with the controller, it is essential that the switch's management VLAN is assigned to VLAN 1. As these are end devices, the ports are configured as untagged ports.

TCP/IP devices are connected to ports 3 and 10, so these two ports should be assigned to VLAN 2. Consequently, these two ports are configured with PVID 2. The connected devices are again end devices, so the ports are configured as untagged.

Another switch is connected to Port 9, to which in turn a PROFINET device and a TCP/IP device are connected. Therefore, Port 9 of the switch must be configured as a tagged port, with VLAN 1 and VLAN 2, in order to send the telegrams with tags. This enables the next switch to know which ports to assign the respective telegrams to.

As each port must be assigned its own PVID, but this cannot be configured as a tagged VLAN on the port at the same time, port 9 is assigned PVID 3.

Once all configurations are complete, it is possible to assign individual names to the created VLANs under the VLAN Names tab.

Step 1:

- Open the switch's website and access the VLAN menu
- Switch VLAN to "On"

Step 2:

- Assign PVIDs (PVLANs) to the ports
    - Port 1→ PVLAN 1
    - Port 2→ s PVLAN 2
    - Port 4→ s PVLAN 1
    - Port 9→ s PVLAN 3
    - Port 10→ PVLAN 2
- All other ports can be ignored or assigned to a VLAN for future network expansions
- Confirm by clicking "Apply"

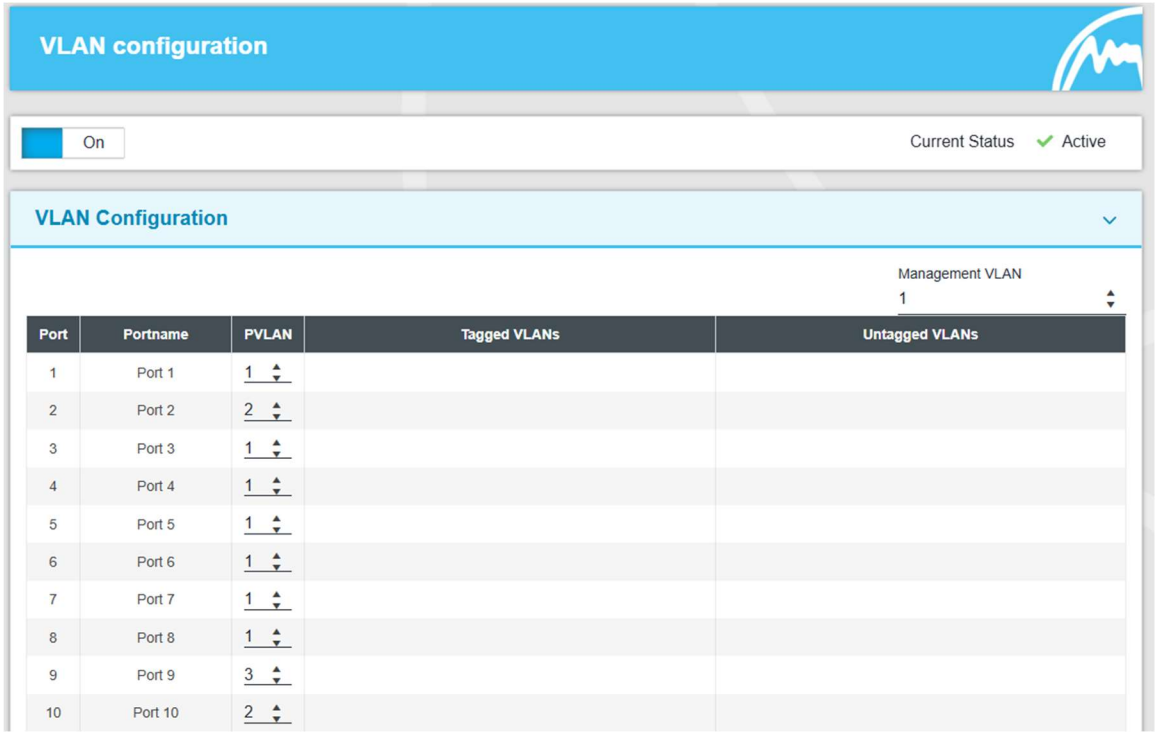


Figure21: VLAN configuration step 2

Step 3:

- Refresh page
- The individual ports have been automatically assigned the corresponding untagged VLANs.

  (In the ***PROmesh P24+,*** the untagged VLANs are not displayed separately again. If a port is assigned to a PVLAN ID, the port is created as an untagged VLAN as before, but is not displayed individually again.)
- This has already enabled us to separate PROFINET and TCP/IP communication

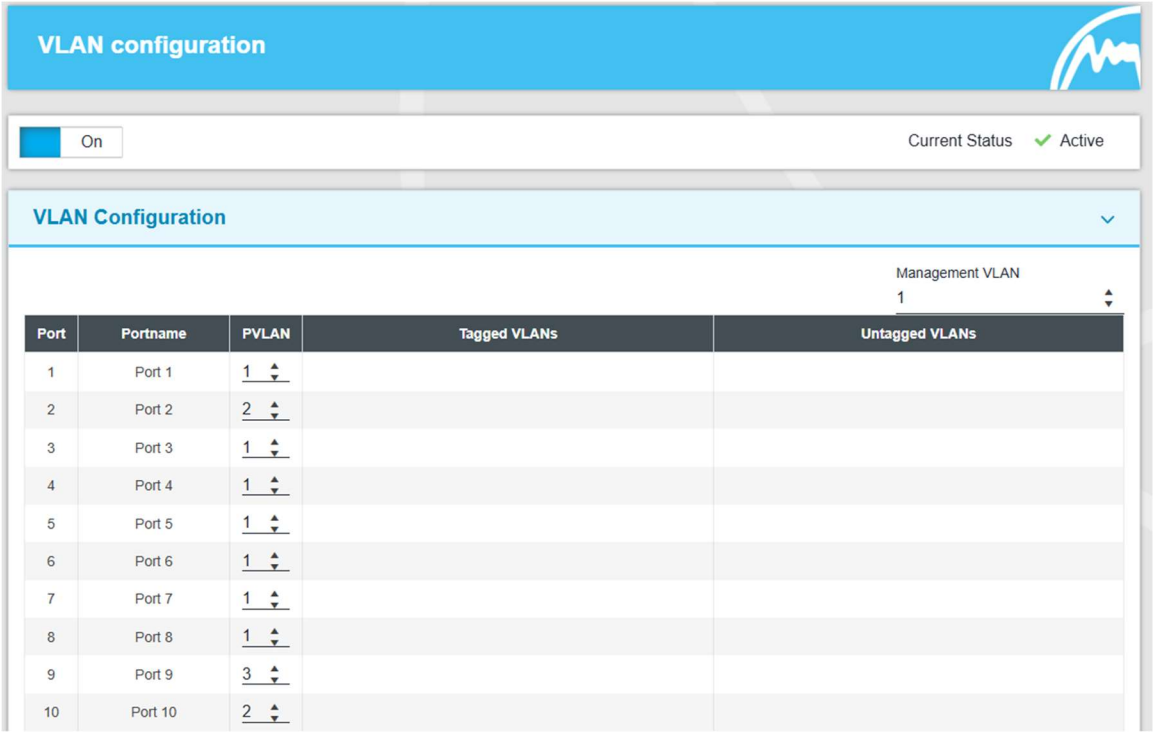


Figure22: VLAN configuration Step 3

Step 4:

- To ensure that PROFINET telegrams from VLAN 1 and TCP/IP telegrams from VLAN 2 can be sent and received via Port 9, VLANs 1 and 2 must be assigned to Port 9 as tagged VLANs
- The VLANs can be separated by commas or hyphens when listing multiple VLANs in a single step.
- Confirm by clicking “Apply”

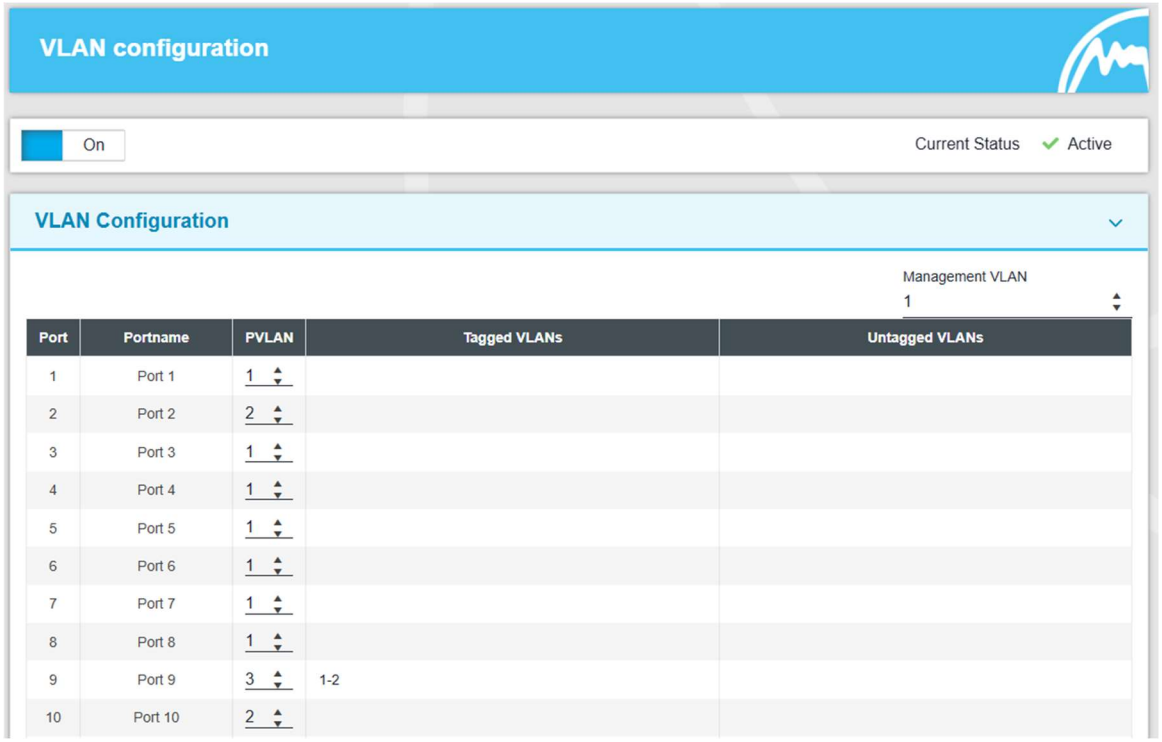


Figure23: VLAN configuration step 4

Step 5:

- To change the names of the created VLANs, open the VLAN Names drop-down menu
- The table contains all created VLANs, whose names can be quickly and easily modified
- The VLAN configuration is complete

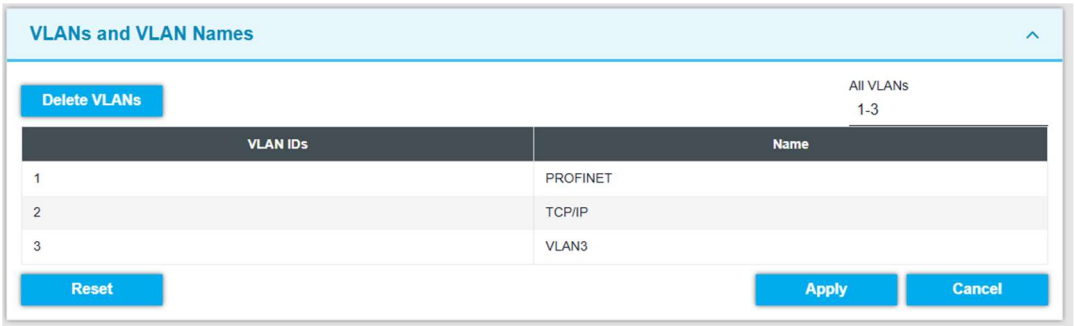


Figure24 : VLAN configuration step 5

4.8.3 Quality of Service

Quality of Service (QoS) encompasses all procedures that influence data flow within the device. By assigning data to different prioritised queues, certain user data can be given preferential treatment. For example, real-time data, control data, audio or video data can be prioritised over file transfers.

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

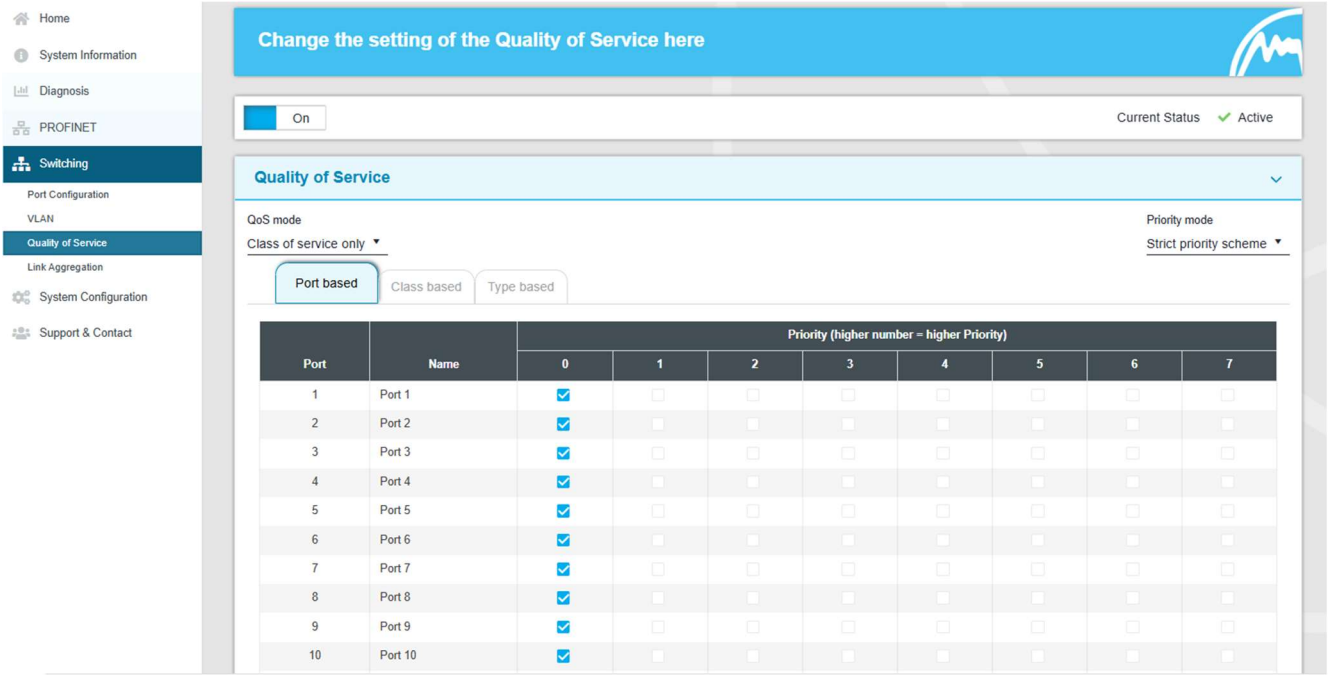


Figure25: Quality of Service using the PROmesh P10XD as an example

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 from the respective port according to their priority.
- Class of Service (COS): COS uses a data field containing priority information within the VLAN tag. Eight different priority values are specified, ranging from Best Effort (BE, 0–low) to Network Control (NC, 7–high). Assign the COS priorities to the switch's eight queues as required by your application.
- Type of Service (TOS): TOS uses a Differentiated Services Code Point (DSCP) data field in the IP header of the packets, which can have up to 64 different priorities. As with COS, you can use these priorities to give preference to, for example, real-time control data, Voice over IP (VoIP) or audio data over normal data transfer. Adjust the settings to suit your requirements.
- QoS Mode:
    - Port-based only: Prioritisation is based solely on the priority of the ports.
    - Class of Service only: Prioritisation is based solely on the Class of Service data field of the packets.
    - Type of Service only: Prioritisation is based solely on the Type of Service data field of the packets.
- Priority scheme:

- Strict priority scheme: With the strict priority scheme, all packets leave a port until the associated priority queue is empty. Only then are packets from the lower-priority queues sent. If packets are constantly arriving in the queue with the highest priority, it is possible that packets from the lowest-priority queue will never be sent. This mode is recommended where there are very high real-time requirements.
- Weighted order: This approach prevents low-priority packets from never being sent when high-priority packets are constantly being 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 within a single transmission cycle.

4.8.4 Link Aggregation

The Link Aggregation function allows multiple physical connections to be combined into a single logical connection. This enables you to transfer higher data volumes between two devices. (If you combine two physical connections between two PROmesh P10+ units using Link Aggregation, you can transfer up to 2 x 1 Gbit/s instead of 1 x 1 Gbit/s)

Link aggregation can be configured statically or dynamically.

You can add a new Link Aggregation group using the '+' button. You can then:

Static

The following settings must be configured:

- Type: Static
- Ports: Here you can select the physical ports that are to belong to a link aggregation group (a logical connection).

Click the "OK" button to accept and apply the settings.

Dynamic (LACP)

The following settings must be configured:

- Type: Dynamic
- Ports: Here you can select the physical ports that should belong to a link aggregation group (a logical connection).
- Mode: This setting applies to dynamic LACP. In active mode, the LACP protocol is active for the port. In passive mode, the LACP protocol is only active for the port if the remote end of the port connection is also in passive mode. The protocol is sent to bridge a connection failure without packet loss. With dynamic link aggregation, at least one side of the connection must be configured as the active part.

- Port Priority: This setting is relevant for dynamic LACP. If an additional port is required for a logical link, the free dynamic port with the highest port priority is selected. The lower the number, the higher the priority.

To delete an LACP group, press the ‘Bin’ button, then select the relevant group(s) and confirm with ‘OK’.

4.9 System Configuration

The System Configuration page displays the IP address settings, time settings, device access options and general device information.

This page is designed to provide you with a concise overview of the System Configuration menu, helping you to understand how the device works and identify where action is required.

Using the edit buttons, you can navigate directly to the relevant logs and functions to configure further settings there.

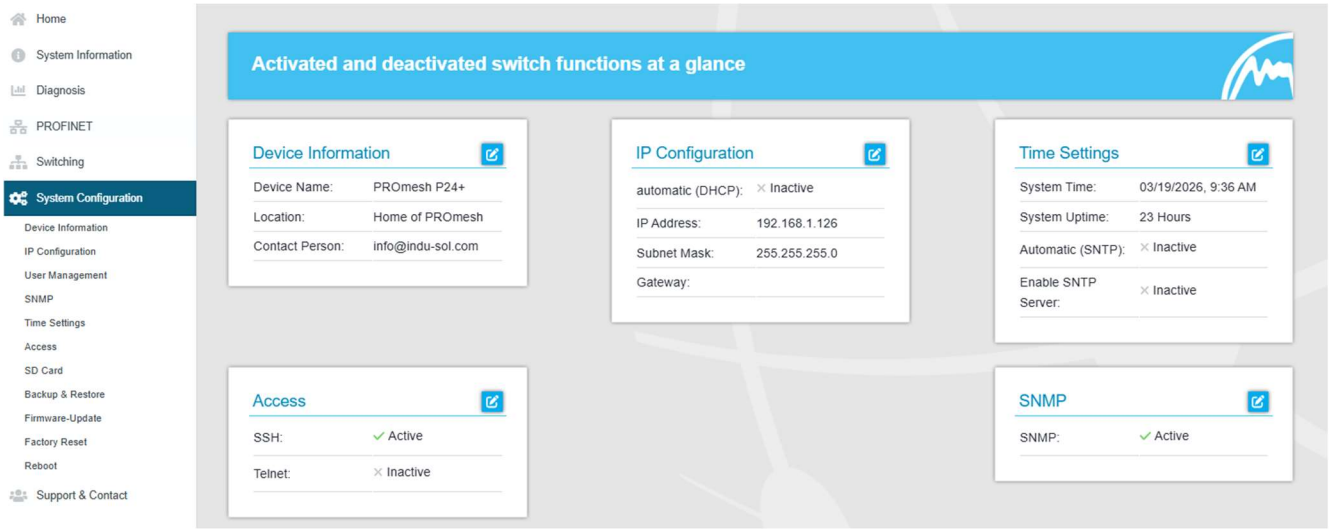


Figure26: System configuration

4.9.1 Device Information

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

- Device name: Give the device a name to simplify identification. The device name is independent of the PROFINET name.
- Installation location: Specify the installation location of the device to simplify localisation.
- Contact person: Enter a contact person for the device.

The input fields are configured to allow 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 keep track of things.

4.9.2 IP configuration

The IP configuration can be carried out either by the PROFINET controller, automatically using the Dynamic Host Configuration Protocol (DHCP), or manually. If 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, it obtains its IP configuration from the PROFINET controller. If a PROFINET connection already exists, the IP configuration cannot be set automatically or manually.

Automatic

To obtain a configuration of the IP address, subnet mask and default gateway from a server operating on the network with the appropriate functionality, tick the “Automatic (DHCP)” checkbox.
Once you have saved the settings by clicking the Apply button, the device sends a request to the server and adopts the configuration received from the DHCP server. As the device has now been assigned a new IP address, it is no longer accessible via the default IP. Please contact your network administrator or use a suitable tool (Indu-Sol ServiceTool) to obtain the new IP address.

Manual

If your network does not have a DHCP server or you wish to configure the settings manually, deactivate the “Automatic (DHCP)” button and enter the following details:

- IP address: Please note that the IP address you set must be accessible from your PC so that you can reconnect to the device to configure the remaining settings.
- Subnet mask: Enter the subnet mask for the IP address; this divides the IP address into a network portion and a device portion. This determines which IP addresses are directly accessible from the device and which addresses must be accessed via a gateway.
- Gateway: Enter a default gateway. The gateway is used to communicate with devices outside your subnet.

Please check carefully which settings you are configuring to avoid problems with duplicate IP addresses. The IP address, subnet mask and gateway must be entered in decimal notation.

4.9.3 User Management

- On this page, you can view an overview of existing users, including their roles (admin/user), and create or delete additional users.

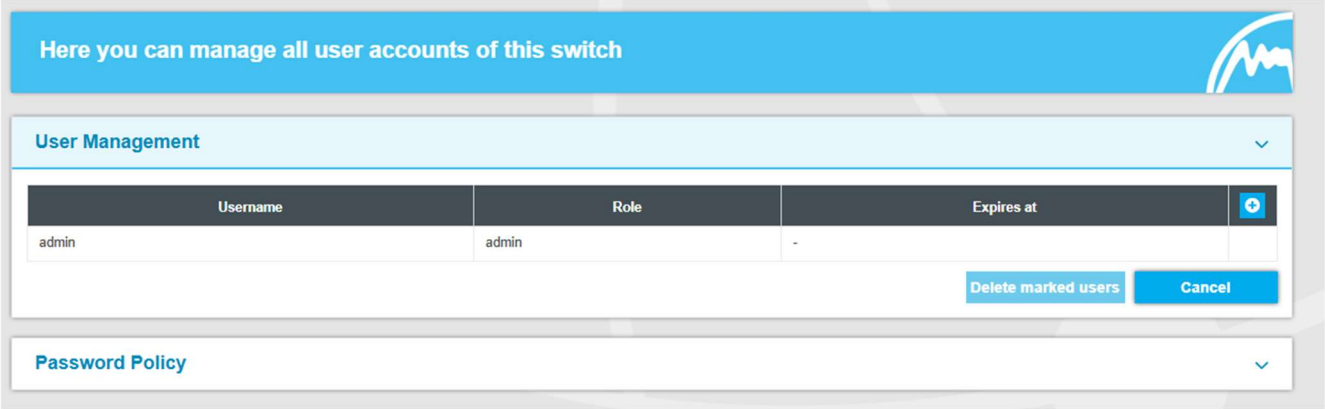


Figure27: User management

Admin rights:

As a logged-in user with the ‘Admin’ role, you have full access to the switch’s functionality. This includes: read and write access to all functions and pages.

User rights:

As a logged-in user with the ‘User’ role, you do NOT have full access to the switch’s functions. As a ‘User’, you cannot perform write operations, and not all pages provided within the ‘Read’ function will be displayed to you.

Password policy

Within the password policies, you can specify individually which components must be included in passwords as a minimum. By default, all are required (lower-case letters, upper-case letters, special characters and numbers).

Notes on passwords

The security of your system is largely dependent on the strength of your passwords. It is therefore generally recommended that you:

- not to use dictionary words
- to use passwords that are as complex as possible
- use combinations of letters, numbers and special characters
- to use both lowercase and uppercase letters
- to use a password of at least eight characters
- Do not write down passwords

Changing your password

To change your password, please click on ‘Edit *your username’* in the top right-hand corner of the header. This will take you to a pop-up window where you can change your password.

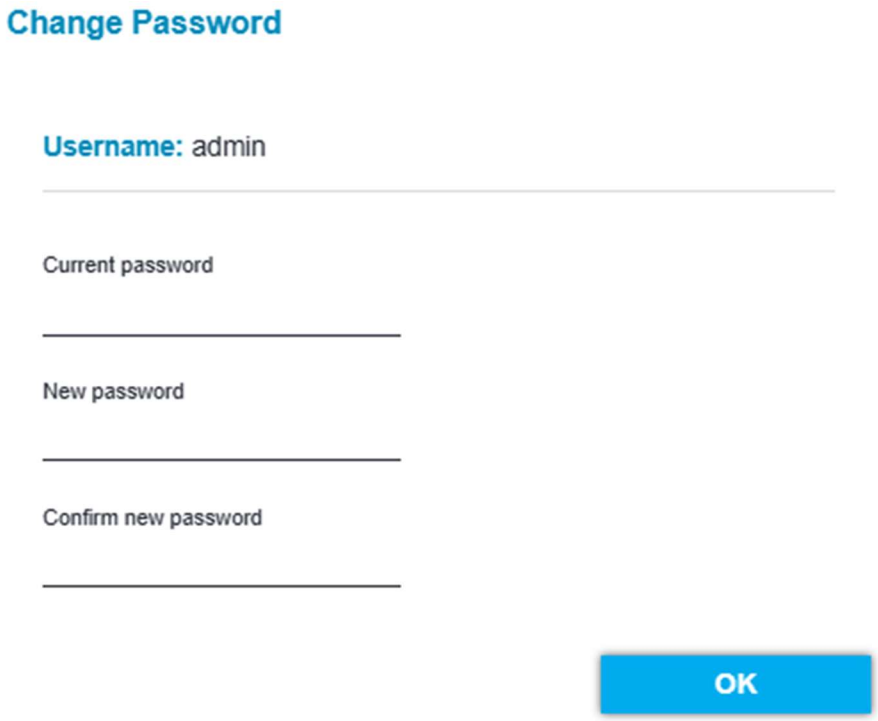


Figure28: Change password

4.9.4 SNMP

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

Current SNMP accesses

The overview table shows you the currently defined community strings. Via .

- Community string: The access points are defined by unique names, which you can customise.
- Read-only: The community string allows read-only access.
- Delete: You can delete the community strings by using the "Trash" button.

Create SNMP access

To create a new community string, click the "+" button. The following setting is required:

- Community string: Enter a unique name for the new SNMP access. A maximum of 32 characters is permitted.

Save the settings by clicking the "Apply" button.

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

Create SNMP V3 access

To create a new string, click on the "+" button. The following setting is required:

- Username
- Authentication can be enabled
- Encryption can be enabled

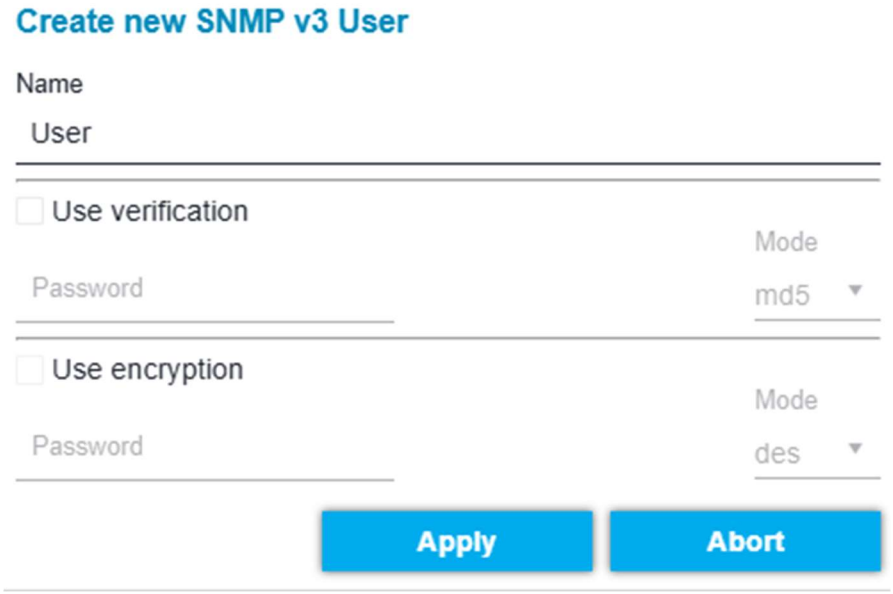


Figure29: SNMP V3

4.9.5 Time settings

In this menu, the device's system time can be adjusted. Here, you can choose between automatic (specifying a time server) and manual mode.

Automatic

To obtain the system time automatically, an NTP server can be used. To do this, enter the following information:

- SNTP server IP address: Enter the IP address of a time server.
- SNTP server IP address (redundant): You can also optionally enter a redundant time server.
- Time zone: Select your applicable time zone.

Figure30: Automatic time settings

Manual

If you are unable to use an NTP server, you can set the device time manually. To do this, select the calendar button and choose the desired date.

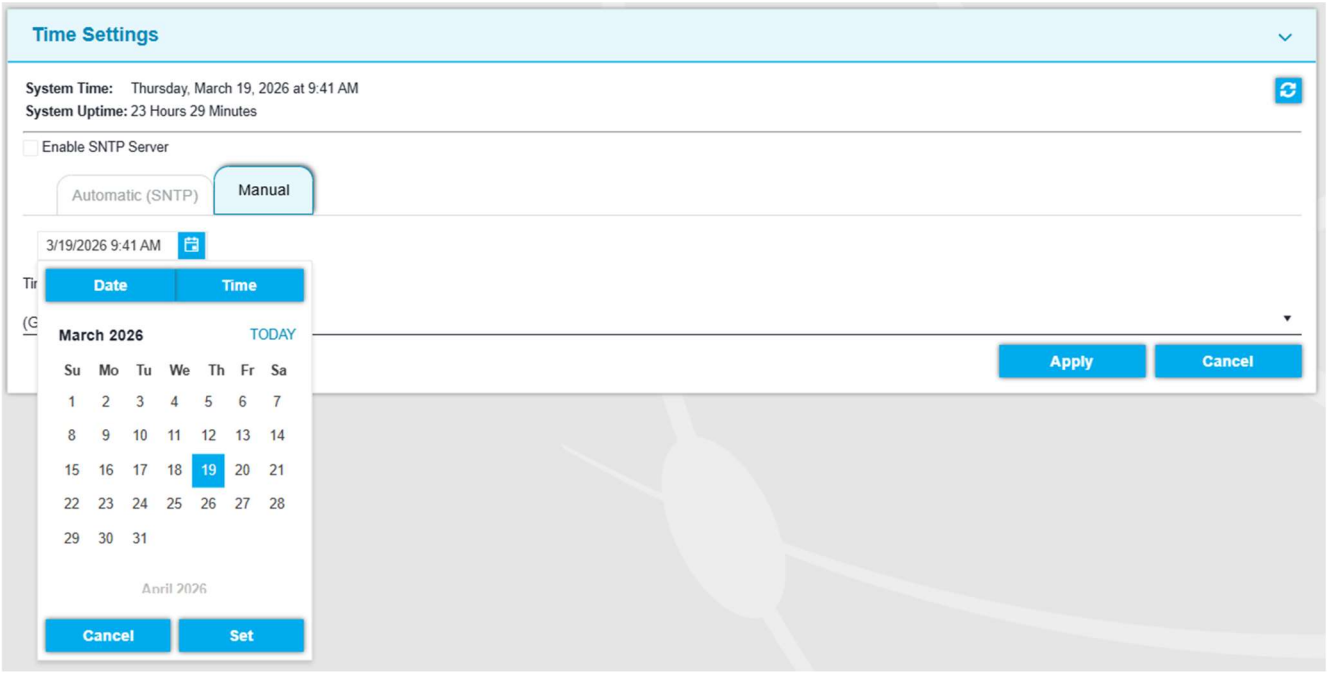


Figure31: Manual time settings

Note: If you set the device time manually, it will be reset every time the device is restarted.

Enable *PROmesh P24+* as an SNTP server

If you wish to use the ***PROmesh P24+*** as an SNTP server for other devices, you can tick the relevant checkbox and enter its IP address on other devices.

4.9.6 Access

In this menu, you can specify which additional access methods should be available for the switch. You can choose between SSH and Telnet. By default, SSH is enabled and Telnet is disabled.

You can also enter a custom message that will appear on the switch’s login page.

Use the "Apply" button to save the settings.

4.9.7 SD card

In this menu, you can check whether an SD card is inserted and is being recognised. If a card is recognised, you can specify a file name and format the SD card accordingly.

4.9.8 Backup and Restore

Backup

This menu option allows you to save the device’s current configuration to a file. The backup can be saved as a download or on the SD card.

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

Click on "Create backup" to save the backup file. Confirm the settings in the pop-up window.

In the Restore tab, you can re-upload a previously saved backup file. Here, you can select the option “Upload”, “TFTP” or “SD card”.

Restore

Upload

To restore, select the ".conf" file and drag it into the designated field.

TFTP

Enter the file path and the relevant TFTP server IP address.

SD card

Enter the file path.

You can then also specify (via a checkbox) for all options whether the switch should be restarted after the file has been successfully uploaded.

Then use the "Restore backup" button to carry out the action and confirm this in the window that opens.

4.9.9 Firmware Update

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

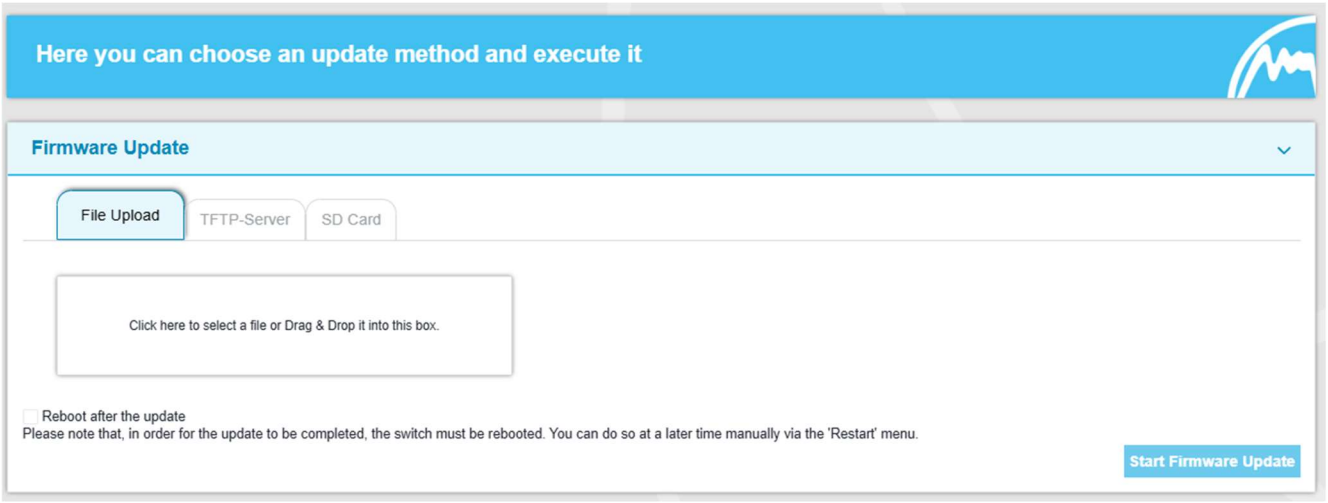


Figure32: Firmware Update

The firmware file is either provided by a TFTP server or an SD card, 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.
- SD card: The firmware update is located on the SD card currently in use and is transferred from there to the device.

Preparation:

It is not recommended to perform the update whilst the MRP protocol is enabled. Please first open the MRP ring by disconnecting one of the cables and then disable the Media Redundancy Protocol. Now carry out the firmware update.

Settings

- TFTP server IP address: Enter 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 enter the name relative to the server's root directory.

Use the "Start firmware update" button to execute the action and confirm this in the window that opens. Please ensure that the firmware update can be completed in full.

Important:

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

- Under no circumstances disconnect the device from the power supply.
- Do not unplug or reconnect any network cables.

A message will appear as soon as the update is complete. The device will then restart automatically.

Note: The device will restart during the firmware update.

4.9.10 Factory settings

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

Click the "Start reset" button to carry out the action and confirm this in the window that opens.

Note: The device must be restarted afterwards.

4.9.11 Restart

Here you can restart the switch. Pressing the restart button will terminate the switch's software and the device will reboot.

Alternatively, you can switch the switch's two power supplies off and on again.

4.10 Support & Contact

In the Support section, you will find relevant contact information should you have any queries regarding the product.

Manufacturer

Please contact Indu-Sol, the manufacturer of the device, if you encounter serious problems configuring the switch or have questions that are not answered in the data sheet or the user manual.

Licence Information

The linked file licence.txt contains information regarding the "open source software" used.

5 Troubleshooting

- Check that the power supply is correct. The VDC LED must be lit green.
- Check the link LEDs on the wired M12 sockets. The link LEDs must be lit when a connection is established.
- If in doubt, disconnect redundant network structures and reset the ***PROmesh P24***+ switch to its factory settings. If communication then works, gradually reapply your settings whilst observing at which point the error occurs.

6 Technical specifications and

Network connections	20 x up to 1 Gbps RJ45 4 x up to 10 Gbps SFP+
Power supply	12 V ... 48 V DC redundant power supply
Dimensions (HxWxD)	155 mm x 130 mm x 155 mm
Weight	2.2 kg
Housing	Anodised aluminium
Operating temperature	-40 °C to 75 °C
Storage temperature	-40 °C to 85 °C
Humidity	Humidity 5 % ... 95 % RH, non-condensing
Protection rating	IP20
Mounting	Top-hat rail mounting
EMC	2014/30/EU EN 61000-6-2 / IEC 61000-4-2 / EN 55032
LED display	Status LEDs / Port LEDs / Power supply / Error
Management	SNMP management Web interface management
Switching technology	Store-and-forward
MAC address table	16K MAC address table
Ring	MRP Spanning Tree
VLAN	Port-based VLAN Tagged VLAN IEEE 802.1Q
Class of Service	IEEE 802.1p Class of Service with eight priority queues per port
Port mirror	RX packets only or TX and RX packets
Firmware update	TFTP server, from local PC, SD card
Bandwidth control	Incoming and outgoing
DHCP client	DHCP client function to obtain an IP address from the DHCP server

Indu-Sol GmbH
Blumenstrasse 3
04626 Schmoelln

Telephone: +49 (0) 34491 580-0
Telefax: +49 (0) 34491 580-499

info@indu-sol.com
www.indu-sol.com

We are certified according to DIN EN ISO 9001:2015