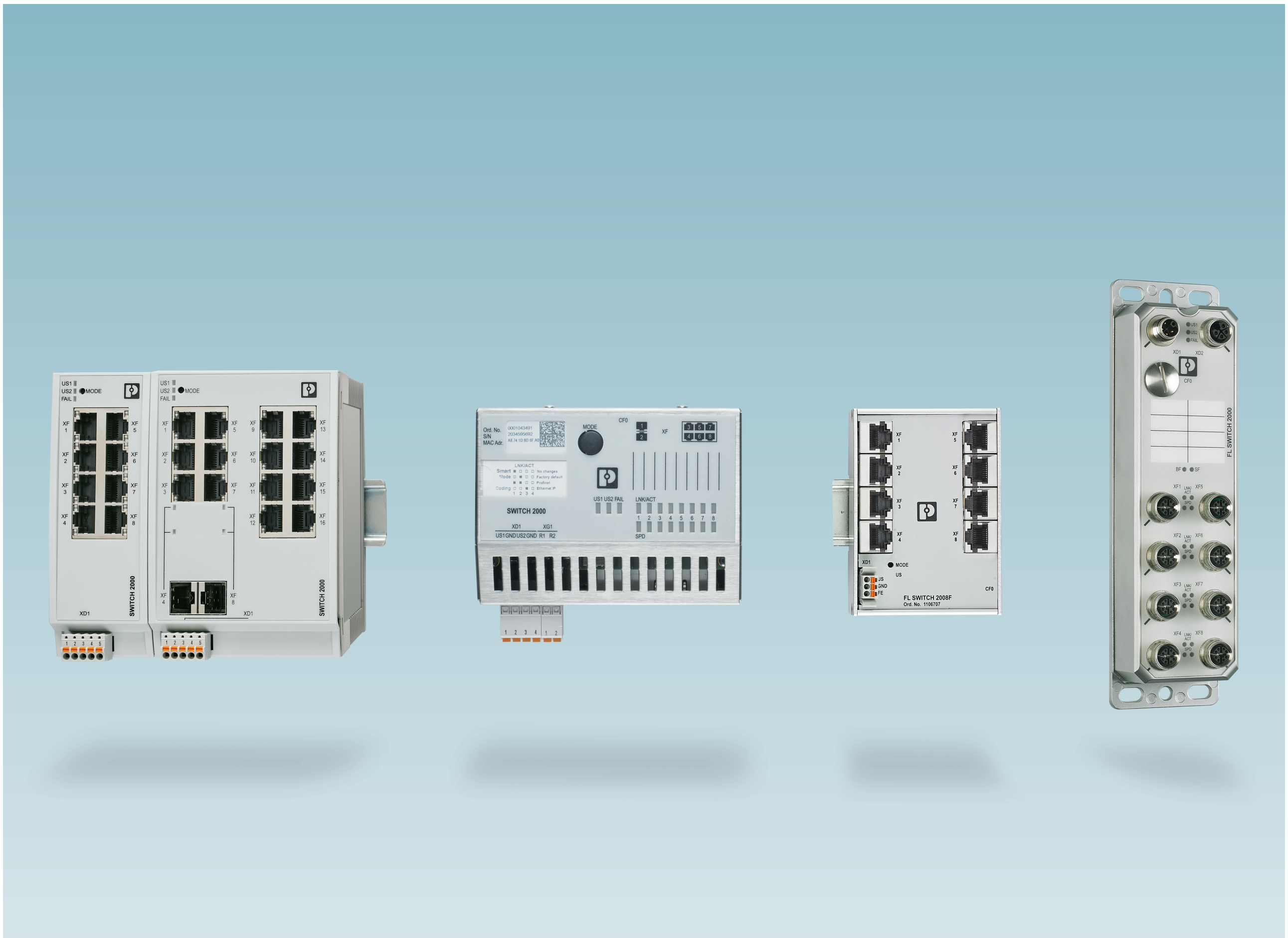


Configuration of the FL SWITCH 2000 and FL NAT 2000 product family

User manual

PHOENIX CONTACT
INSPIRING INNOVATIONS

User manual

Configuration of the FL SWITCH 2000 and FL NAT 2000 product family

UM EN SW FL SWITCH 2000, Revision 06 2023-02-09

This manual is valid for:

Designation	Item No.	Designation	Item No.	Designation	Item No.
FL SWITCH 2005	2702323	FL SWITCH 2306-2SFP	2702970	FL SWITCH 2608	1106500
FL SWITCH 2008	2702324	FL SWITCH 2306-2SFP PN	1009222	FL SWITCH 2608 PN	1106616
FL SWITCH 2008F	1106707	FL SWITCH 2304-2GC-2SFP	2702653	FL SWITCH 2708	1106615
FL SWITCH 2016	2702903	FL SWITCH 2316	2702909	FL SWITCH 2708 PN	1106610
FL SWITCH 2105	2702665	FL SWITCH 2316 PN	1031673	FL NAT 2008	2702881
FL SWITCH 2108	2702666	FL SWITCH 2314-2SFP	1006191	FL NAT 2208	2702882
FL SWITCH 2116	2702908	FL SWITCH 2314-2SFP PN	1031683	FL NAT 2304-2GC-2SFP	2702981
FL SWITCH 2205	2702326	FL SWITCH 2312-2GC-2SFP	2702910	FL SWITCH 2303-8SP1	1278397
FL SWITCH 2208	2702327	FL SWITCH 2408	1043412		
FL SWITCH 2208C	1095627	FL SWITCH 2408 PN	1089133		
FL SWITCH 2208 PN	1044024	FL SWITCH 2406-2SFX	1043414		
FL SWITCH 2207-FX	2702328	FL SWITCH 2406-2SFX PN	1089126		
FL SWITCH 2207-FX SM	2702329	FL SWITCH 2404-2TC-2SFX	1088853		
FL SWITCH 2206-2FX	2702330	FL SWITCH 2416	1043416		
FL SWITCH 2206C-2FX	1095628	FL SWITCH 2416 PN	1089150		
FL SWITCH 2206-2FX SM	2702331	FL SWITCH 2414-2SFX	1043423		
FL SWITCH 2206-2FX ST	2702332	FL SWITCH 2414-2SFX PN	1089139		
FL SWITCH 2206-2FX SM ST	2702333	FL SWITCH 2412-2TC-2SFX	1088875		
FL SWITCH 2206-2SFX	2702969	FL SWITCH 2508	1043484		
FL SWITCH 2206-2SFX PN	1044028	FL SWITCH 2508/K1	1215350		
FL SWITCH 2204-2TC-2SFX	2702334	FL SWITCH 2508 PN	1089134		
FL SWITCH 2216	2702904	FL SWITCH 2506-2SFP	1043491		
FL SWITCH 2216 PN	1044029	FL SWITCH 2506-2SFP/K1	1215329		
FL SWITCH 2214-2FX	2702905	FL SWITCH 2506-2SFP PN	1089135		
FL SWITCH 2214-2FX SM	2702906	FL SWITCH 2504-2GC-2SFP	1088872		
FL SWITCH 2214-2SFX	1006188	FL SWITCH 2516	1043496		
FL SWITCH 2214-2SFX PN	1044030	FL SWITCH 2516 PN	1089205		
FL SWITCH 2212-2TC-2SFX	2702907	FL SWITCH 2514-2SFP	1043499		
FL SWITCH 2308	2702652	FL SWITCH 2514-2SFP PN	1089154		
FL SWITCH 2308 PN	1009220	FL SWITCH 2512-2GC-2SFP	1088856		

Also observe the associated manual for configuring the listed items.
(Document 108998)

The manual and additional user documentation can be downloaded from our website:

phoenixcontact.com

Enter one of the item numbers listed here in the search field.

PHOENIX CONTACT GmbH & Co. KG • Flachsmarktstraße 8 • 32825 Blomberg • Germany
phoenixcontact.com

Table of contents

1 For your safety

Read this user manual carefully and keep it for future reference.

1.1 Identification of warning notes

⚠ This symbol indicates hazards that could lead to personal injury.

There are three signal words indicating the severity of a potential injury.

DANGER
Indicates a hazard with a high risk level. If this hazardous situation is not avoided, it will result in death or serious injury.

WARNING
Indicates a hazard with a medium risk level. If this hazardous situation is not avoided, it could result in death or serious injury.

CAUTION
Indicates a hazard with a low risk level. If this hazardous situation is not avoided, it could result in minor or moderate injury.

ⓘ This symbol together with the **NOTE** signal word warns the reader of actions that might cause property damage or a malfunction.

ℹ Here you will find additional information or detailed sources of information.

1.2 Qualification of users

The use of products described in this user manual is oriented exclusively to:

– Electrically skilled persons or persons instructed by them. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.
– Qualified application programmers and software engineers. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.

1.3 Field of application of the product

1.3.1 Intended use

The switches from the FL SWITCH 2000 product family are recommended for use in industrial networks. They are designed for use in control cabinets or control boxes that meet the requirements of IEC/EN 62368-1 with respect to fire protection enclosures. The devices may only be used under the approved ambient conditions and in the approved supply voltage range (see UM EN HW FL SWITCH 2000 and UM EN HW FL SWITCH 2000 SPE).

The prescribed mounting position is vertical on a horizontally mounted DIN rail. To allow air to circulate freely, the vents must not be covered. A clearance of 3 cm to the vents of the housing is recommended.

1.3.2 Product changes

Modifications to hardware and firmware of the device are not permitted.

Incorrect operation or modifications to the device can endanger your safety or damage the device. Do not repair the device yourself. If the device is defective, please contact Phoenix Contact.

1.4 Scope of application of this manual

This configuration manual contains information about how to configure the FL SWITCH 2xxx and FL NAT 2xxx product family for firmware version 3.21.

Unless otherwise stated, the information provided in this manual also applies to the SPE versions.

For information about commissioning, refer to the separate manual UM EN HW FL SWITCH 2000 (item number 108997) at phoenixcontact.net/qr/<item_number>.

For information about commissioning the SPE versions, refer to the separate manual UM EN HW FL SWITCH 2000 SPE (item number 110712) at phoenixcontact.net/qr/<item_number>.

For information about configuration and diagnostics via the Command Line Interface (CLI), refer to the separate manual UM EN CLI (item number 110152) at phoenixcontact.net/qr/<item_number>.

1.5 Safety and installation instructions

WARNUNG: Dangerous contact voltage
The device is live. Only qualified personnel may work on it. The personnel must be familiar with the necessary safety precautions.

WARNUNG: Explosion hazard in potentially explosive areas
Only use genuine accessories.

Observe all relevant safety and installation instructions in this documentation as well as in the documentation supplied with the accessories.

CAUTION: Risk of burns from hot surfaces
At high ambient temperatures, the surfaces of the device may get hot. Therefore, make sure to allow the device to cool down before working on it.

NOTE: Installation only by qualified personnel
Installation, startup, and maintenance of the product may only be performed by qualified specialist personnel who have been authorized for this by the system operator. An electrically skilled person is someone who, because of their professional training, skills, experience, and their knowledge of relevant standards, can assess any required operations and recognize any possible dangers. Specialist personnel must read and understand this documentation and comply with instructions. Observe the applicable national regulations with respect to the operation, function testing, repair, and maintenance of electronic devices.

NOTE: Electrostatic discharge
Electrostatic discharge can damage or destroy components. When handling the device, observe the necessary safety precautions against electrostatic discharge (ESD) in accordance with EN 61340-5-1 and IEC 61340-5-1.

NOTE: Requirement for power supply
The device is designed exclusively for operation with safety extra-low voltage (SELV) or functional extra-low voltage with electrical safe isolation (PELV). In redundant operation, both power supplies must satisfy the requirements of the safety extra-low voltage.

NOTE: Radio interference (Class A, EN 55032)
Operating this device may cause radio interference in residential areas.

NOTE: Requirement for control cabinet/control box
This module snaps onto a standard DIN rail inside a control cabinet or control box. This control cabinet/control box must meet the requirements of IEC/EN 62368-1 with respect to fire protection enclosures.

NOTE: Requirement for functional grounding
Mount the module on a grounded DIN rail. The module is grounded when it is snapped onto the DIN rail.

NOTE: Requirement for mounting location
The prescribed mounting position is vertical on a horizontally mounted DIN rail. To allow air to circulate freely, the vents must not be covered. A clearance of 3 cm to the vents of the housing is recommended.

The symbol with the crossed-out trash can indicates that this item must be collected and disposed of separately from other waste. Phoenix Contact or public collection sites will take the item back for free disposal. For information on the available disposal options, visit phoenixcontact.com. Collect and dispose of included batteries separately from other waste. Delete personal data before returning the item.

The symbol informs you that you have to observe the instructions. Only install and operate the device once you have familiarized yourself with its properties by means of the user documentation.

Opening or modifying the device is not permitted. Do not repair the device yourself; replace it with an equivalent device. Repairs may only be carried out by the manufacturer. The manufacturer is not liable for damage resulting from noncompliance.

The IP20 degree of protection (IEC 60529/EN 60529) of the 20xx/21xx/22xx/23xx/24xx/25xx and NAT 2xxx versions is intended for a clean and dry environment. Do not subject the device to mechanical and/or thermal stress that exceeds the specified limits.

The IP67 degree of protection of the 26xx/27xx versions is intended for a dusty and wet environment. The device is dust-tight and protected against temporary submersion. Do not subject the device to mechanical and/or thermal stress that exceeds the specified limits.

1.6 Security in the network

NOTE: Network security jeopardized by unauthorized access
Connecting devices to a network entails the danger of unauthorized access to the network.

Observe the following safety notes:

- If possible, deactivate unused communication channels.
- Use secure passwords reflecting the complexity and service life recommended in the latest guidelines.
- Only allow authorized persons to access the device. Limit the number of authorized persons to the necessary minimum.
- Always install the latest firmware version. The firmware can be downloaded via the item (phoenixcontact.net/products).
- Observe the IT security requirements and the standards applicable to your application. Take the necessary protective measures. These may include, for example, virtual networks for remote maintenance access or a firewall.
- In security-critical applications, always use the device with an additional security appliance.

  Phoenix Contact offers security appliances in the mGuard product range. The mGuard routers connect various networks for the remote maintenance and protection of the local network and protect these networks against cyberattacks.
- You must take defense-in-depth strategies into consideration when planning networks.

Additional measures for protection against unauthorized network access can be found in the “INDUSTRIAL SECURITY” application note. The application note can be downloaded via the item (phoenixcontact.net/products).
German: AH DE INDUSTRIAL SECURITY, 107913
English: AH EN INDUSTRIAL SECURITY, 107913

If a security vulnerability exists for products, solutions, or services from Phoenix Contact, it will be published on the PSIRT (Product Security Incident Response Team) website: phoenixcontact.com/psirt

2 Commissioning and function

2.1 Properties and versions

2.1.1 FL SWITCH 2xxx device versions

Table 2-1 FL SWITCH 2xxx device versions

Item designation	Pre-configuration in factory default state	Copper ports		Fiberglass ports	
		10/100 Mbps	10/100/1000 Mbps	100 Mbps	100/1000 Mbps
FL SWITCH 2005		5x RJ45			
FL SWITCH 2008		8x RJ45			
FL SWITCH 2008F		8x RJ45			
FL SWITCH 2016		16x RJ45			
FL SWITCH 2105			5x RJ45		
FL SWITCH 2108			8x RJ45		
FL SWITCH 2116			16x RJ45		
FL SWITCH 2205		5x RJ45			
FL SWITCH 2208		8x RJ45			
FL SWITCH 2208C		8x RJ45			
FL SWITCH 2208 PN	PROFINET mode	8x RJ45			
FL SWITCH 2207-FX		7x RJ45		1x MM SC	
FL SWITCH 2207-FX SM		7x RJ45		1x SM SC	
FL SWITCH 2206-2FX		6x RJ45		2x MM SC	
FL SWITCH 2206C-2FX		6x RJ45		2x MM SC	
FL SWITCH 2206-2FX SM		6x RJ45		2x SM SC	
FL SWITCH 2206-2FX ST		6x RJ45		2x MM ST	
FL SWITCH 2206-2FX SM ST		6x RJ45		2x SM ST	
FL SWITCH 2206-2SFX		6x RJ45		2x SFP	
FL SWITCH 2206-2SFX PN	PROFINET mode	6x RJ45		2x SFP	
FL SWITCH 2204-2TC-2SFX		4x RJ45		2x combo, 2x SFP	
FL SWITCH 2216		16x RJ45			
FL SWITCH 2216 PN	PROFINET mode	16x RJ45			
FL SWITCH 2214-2FX		14x RJ45		2x MM SC	
FL SWITCH 2214-2FX SM		14x RJ45		2x SM SC	
FL SWITCH 2214-2SFX		14x RJ45		2x SFP	

Table 2-1 FL SWITCH 2xxx device versions

Item designation	Pre-configuration in factory default state	Copper ports		Fiberglass ports	
		10/100 Mbps	10/100/1000 Mbps	100 Mbps	100/1000 Mbps
FL SWITCH 2214-2SFX PN	PROFINET mode	14x RJ45		2x SFP	
FL SWITCH 2212-2TC-2SFX		12x RJ45		2x combo, 2x SFP	
FL SWITCH 2308			8x RJ45		
FL SWITCH 2308 PN	PROFINET mode		8x RJ45		
FL SWITCH 2306-2SFP			6x RJ45		2x SFP
FL SWITCH 2306-2SFP PN	PROFINET mode		6x RJ45		2x SFP
FL SWITCH 2304-2GC-2SFP			4x RJ45		2x combo, 2x SFP
FL SWITCH 2316			16x RJ45		
FL SWITCH 2316 PN	PROFINET mode		16x RJ45		
FL SWITCH 2314-2SFP			14x RJ45		2x SFP
FL SWITCH 2314-2SFP PN	PROFINET mode		14x RJ45		2x SFP
FL SWITCH 2312-2GC-2SFP			12x RJ45		2x combo, 2x SFP
FL SWITCH 2408		8x RJ45			
FL SWITCH 2408 PN	PROFINET mode	8x RJ45			
FL SWITCH 2406-2SFX		6x RJ45		2x SFP	
FL SWITCH 2406-2SFX PN	PROFINET mode	6x RJ45		2x SFP	
FL SWITCH 2404-2TC-2SFX		4x RJ45		2x combo, 2x SFP	
FL SWITCH 2416		16x RJ45			
FL SWITCH 2416 PN	PROFINET mode	16x RJ45			
FL SWITCH 2414-2SFX		14x RJ45		2x SFP	
FL SWITCH 2414-2SFX PN	PROFINET mode	14x RJ45		2x SFP	
FL SWITCH 2412-2TC-2SFX		12x RJ45		2x combo, 2x SFP	
FL SWITCH 2508			8x RJ45		
FL SWITCH 2508/K1			8x RJ45		
FL SWITCH 2508 PN	PROFINET mode		8x RJ45		
FL SWITCH 2506-2SFP			6x RJ45		2x SFP
FL SWITCH 2506-2SFP/K1			6x RJ45		2x SFP
FL SWITCH 2506-2SFP PN	PROFINET mode		6x RJ45		2x SFP
FL SWITCH 2504-2GC-2SFP			4x RJ45		2x combo, 2x SFP

Table 2-1 FL SWITCH 2xxx device versions

Item designation	Pre-configuration in factory default state	Copper ports		Fiberglass ports	
		10/100 Mbps	10/100/1000 Mbps	100 Mbps	100/1000 Mbps
FL SWITCH 2516			16x RJ45		
FL SWITCH 2516 PN	PROFINET mode		16x RJ45		
FL SWITCH 2514-2SFP			14x RJ45		2x SFP
FL SWITCH 2514-2SFP PN	PROFINET mode		14x RJ45		2x SFP
FL SWITCH 2512-2GC-2SFP			12x RJ45		2x combo, 2x SFP
FL SWITCH 2608		8x M12 (D-coded)			
FL SWITCH 2608 PN	PROFINET mode	8x M12 (D-coded)			
FL SWITCH 2708			8x M12 (X-coded)		
FL SWITCH 2708 PN	PROFINET mode		8x M12 (X-coded)		

2.1.2 FL NAT 2xxx device versions

Table 2-2 FL NAT 2xxx device versions

Item designation	Copper ports		Fiberglass ports	
	10/100 Mbps	10/100/1000 Mbps	100 Mbps	100/1000 Mbps
FL NAT 2008	8x RJ45			
FL NAT 2208	8x RJ45			
FL NAT 2304-2GC-2SFP		4x RJ45		2x combo, 2x SFP

2.1.3 FL SWITCH 2xxx SPE device versions

Table 2-3 FL SWITCH 2xxx SPE device versions

Item designation	Copper ports		SPE ports
	10/100 Mbps	10/100/1000 Mbps	10BASE T1L
FL SWITCH 2303-8SP1		3x RJ45	8x SPE

2.1.4 Description of Ethernet interfaces

The properties of the standard Ethernet interfaces of the FL SWITCH 2000 and FL NAT 2000 product families described below fully meet the requirements of the IEEE 802.3 specification.

Copper ports:

- TX ports (RJ45), 10/100 Mbps (20xx, 22xx, 24xx versions)
- TX ports (RJ45), 10/100/1000 Mbps (21xx, 23xx, 25xx versions)
- TX ports (M12), 10/100 Mbps (26xx versions)
- TX ports (M12), 10/100/1000 Mbps (27xx versions)
- SPE ports, SPE 10 base T1L incl. PoDL power class 11

Fiberglass ports:

- FO ports (ST duplex, SC duplex), 100 Mbps (22xx versions)
- SFP ports (SFX), 100 Mbps (22xx, 24xx versions)
- SFP ports (SFP), 100/1000 Mbps (23xx, 25xx versions)

NOTE: Device damage
To avoid damage to the device, we recommend to only use plastic patch cables.

2.2 Function overview table

The functions listed in Table 2-4 are up to date at the time of publication of this manual. For information on the date of publication of individual functions, please refer to the firmware release note. This can be downloaded as part of the software package in the firmware update area on the product page (e.g., http://phoenixcontact.net/product/2702324).

Table 2-4 Device functions

	FL SWITCH / FL NAT / FL SPE								
	20xx	**21xx**	**22xx**	**23xx**	**24xx**	**25xx**	**25xx/K1**	**26xx**	**27xx**
Alarm output/signal contact	No		Yes				No		
Temperature range	0°C ... +60°C		-40°C … +70°C						
Data transmission									
Jumbo frames	No	Yes	No	Yes	No	Yes	Yes	No	Yes
Supply voltage									
Supply voltage range	18 ... 32 V DC		12 ... 57 V DC		19.2 ... 32 V DC		12 ... 32 V DC	9 ...57 V DC	
Redundant power supply	No		Yes						
Filter functions									
Quality of Service	Yes		Yes						
DSCP/DiffServ	Yes		Yes						
VLAN	Yes		Yes						
Multicast/IGMP snooping	Yes		Yes						
Redundancy									
Rapid Spanning Tree (RSTP)	Yes		Yes						

Table 2-4 Device functions [...]

	FL SWITCH / FL NAT / FL SPE								
	20xx	**21xx**	**22xx**	**23xx**	**24xx**	**25xx**	**25xx/K1**	**26xx**	**27xx**
MRP manager/client	No/yes		Yes (optional)/yes						
Fast ring detection (FRD)	No		Yes						
Large Tree Support	No		Yes						
Link aggregation (LACP)	No		Yes						
Management functions									
Role-based user management	Yes		Yes						
Port configuration	Yes		Yes						
Address conflict detection (ACD)	Yes		Yes						
DHCP server	Port-based		Pool-/port-based, option 82						
Command Line Interface (CLI)	Yes		Yes						
Diagnostic functions									
Link Layer Discovery Protocol (LLDP)	Yes		Yes						
Port statistics and utilization	Yes		Yes						
SNMPv1/v2/v3	Yes		Yes						
SNMP traps	Yes		Yes						
Syslog	Yes		Yes						
Time synchronization									
Simple Network Time Protocol (SNTP)	Yes		Yes						
Automation protocols									
PROFINET conformance class	A		B						
PROFINET device	No		Yes						
Extended multicast filtering for EtherNet/IP	Yes		Yes						
Security									
MAC-based port security	No		Yes						
RADIUS authentication (IEEE 802.1X)	No		Yes						
Layer 3 functions (FL NAT versions only)									
Static routing	Yes	–[1]	Yes		–[1]				
1:1-NAT	Yes	–[1]	Yes		–[1]				
Port forwarding (1:n NAT)	Yes	–[1]	Yes		–[1]				
Virtual NAT	Yes	–[1]	Yes		–[1]				
SPE functions (SPE versions only)									
PoDL power management	–[2]			Yes	–[2]				

[1] No FL NAT versions for these series.

[2] No SPE versions are available for these series.

2.3 Delivery state/default settings

2.3.1 Initial IP configuration in the delivery state

ℹ The PN versions do not have an initial IP configuration in the delivery state.

Firmware revision 2.72 and earlier

The device does not have an initial IP configuration.

Firmware revision 2.80

In the delivery state, the device has an initial static IP configuration, which enables you to access web-based management and to assign an IP address.

– IP address: 169.254.2.1
– Subnet mask: 255.255.0.0

This initial IP configuration is deactivated as soon as the switch is assigned an IP configuration via a different IP address assignment mechanism, e.g., via BootP, DHCP, web-based management.

Firmware revision 2.90 or later

In the delivery state, the device has an initial IP configuration and an individual DNS host name. This way, you can access web-based management and configure the device.

Requirement:

– The device is set to the default settings and has firmware version 2.90 or higher.
– The connected PC must be set to “Obtain an IP address automatically”. A static IP address cannot be used here.

Automatic private IP addressing (APIPA)

- You can access your device via link-local IPv4 via the IP address 169.254.2.1.
- If you want to commission several devices in your network, one IP address has the IP address 169.254.2.1. All other devices are assigned a random IP address from the range 169.254.2.1 to 169.254.255.255. You can determine these IP addresses using external software such as Wireshark or access the device via its host name.

With this dynamic method, it is difficult to find out which switch has which IP address when dealing with multiple devices. You can therefore also access the device via a DNS host name.

DNS host name

The host name consists of two portions:

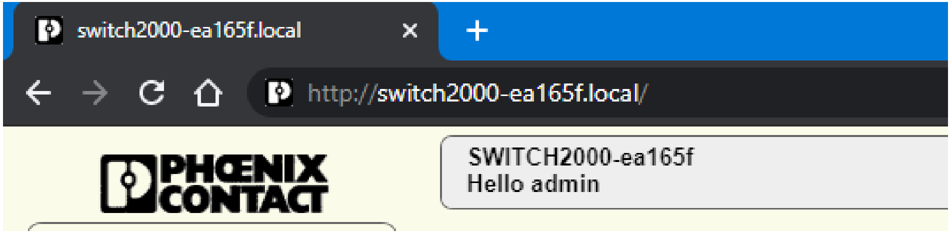
1. Device family: SWITCH2000 or NAT2000
2. The individual part of the MAC address of the device, e.g., a8:74:1d:**ea:16:5f**

The complete host name in this example is therefore: SWITCH2000-EA165F

- Enter the host name in your browser as follows:
  http://SWITCH2000-ea165f.local

For name resolution, mDNS (standard for Linux and Mac systems) and LLMNR (usually used for Windows systems) are supported.

Figure 2-1 Access via the DNS host name



This initial IP configuration is deactivated as soon as the switch is assigned an IP configuration via a different IP address assignment mechanism, e.g., via BootP, DHCP, web-based management.

If you want to reactivate the initial IP configuration at a later date, you can reset the device using web-based management or the Smart mode button.

For information on which Smart modes activate the initial IP configuration, refer to Section "Using Smart mode" on page 22.

2.3.2 Configuration in the delivery state

In the delivery state or after the system is reset to the default settings, the following functions and properties are available:

- All IP parameters are deleted. The switch has no valid IP address. An exception is the initial IP configuration in the delivery state (see "Initial IP configuration in the delivery state" on page 18).
- BootP for assigning IP parameters is activated.
- DNS name resolution is activated and the device can be accessed via the individual host name.
- The DHCP server is deactivated.
- There is an admin account with the user name "admin" and the password "private".
- The available RJ45 ports are set to auto negotiation and auto crossing.
- All counters of the SNMP agent have been reset.
- The web server (HTTP) and SNMPv2 are activated.
- CLI (Telnet) is activated.
- Port mirroring and MRP are deactivated.
- Rapid Spanning Tree (RSTP) is activated (firmware version 2.01 or later).
- The digital alarm output/signal contact is activated for the "Power Supply Lost" event.
- The MAC address table does not contain any entries.
- LLDP is activated.
- SNTP is deactivated.
- 802.1X and port-based security are deactivated.
- The "Universal" Quality of Service profile is activated.
- Syslog is deactivated.
- Port statistics have been reset.
- Individual VLAN learning is activated.

Delivery state of the NAT versions in relation to the layer 3 functions:

- Routing globally activated.
- LAN1 created (IP addressing: BOOTP, ports: 2 ... 8)

- LAN2 created (IP addressing: DHCP, port: 1)

Delivery state of the SPE versions:

- Power Sourcing Equipment (PSE) Port Status is deactivated.
- Power Sourcing Equipment (PSE) Port Mode is set to AutoSignature.

The delivery state of the PROFINET versions (PN) differs as follows:

- PROFINET mode is activated.
- PROFINET device is activated.
- DCP for assigning the device name and the IP parameters is activated.
- The “PROFINET” Quality of Service profile is activated.

2.3.3 Diagnostic and status indicators

Please note that the meaning of the LEDs differs in Smart mode (see “Using Smart mode” on page 22).

Table 2-5 Diagnostic and status indicators

Designation	Color	Status	Meaning
US1	Green	On	Supply voltage 1 is within the tolerance range.
		Off	Supply voltage 1 is too low.
US2 (for 22xx/23xx/24xx/25xx/26xx/27xx versions only)	Green	On	Supply voltage 2 is within the tolerance range.
		Off	Supply voltage 2 is too low.
FAIL[1] (for 22xx/23xx/24xx/25xx/26xx/27xx versions only)	Red	On	An error has occurred. The digital alarm output (22xx/23xx versions) is floated, the signal contact (24xx/25xx versions) is closed. In the default settings, redundant power supply monitoring is active. An error is indicated if only one power supply is connected.
		Off	No error. The digital alarm output (22xx/23xx versions) is connected to ground potential (ground), the signal contact (24xx/25xx versions) is open.
LNK/ACT[2]	Green/ orange	On	Green: Link active Orange: SFP link at combo port active
		Flashing	Data transmission
		Off	Link not active
SPD[2]	Green/ orange	On	Green: 100 Mbps Orange: 1000 Mbps (for 21xx/23xx/25xx/27xx versions only)
		Off	10 Mbps if Link LED is active

Table 2-5 Diagnostic and status indicators

Designation	Color	Status	Meaning
BF (for PN versions only)	Red	On	The device does not have an active link.
		Flashing	The device has at least one active link but no active PROFINET connection.
		Off	The device has at least one active link and at least one active PROFINET connection.
SF (for PN versions only)	Red	On	A PROFINET alarm is present and was reported to the control system.
		Off	No PROFINET alarm present.
LED1 (for SPE versions only)	Green	On	Link and data transmission active
		Off	Link and data transmission not active
LED2 (for SPE versions only)	Green	On	Auto mode: PD power supply active Force mode: Force mode active
		Flashing	Auto mode: Searching for PD
		Off	PSE status deactivated
	Red	Flashing	PSE error

[1] The 26xx/27xx and 2500/K1 versions do not feature an alarm output/signal contact. Only the FAIL LED indicates a pre-defined error.

[2] 20xx/20xxF/21xx/22xx/23xx/26xx/27xx versions: The LNK/ACT LED is located directly at the top of the port. The SPD LED is always located at the bottom of the port. 24xx/25xx versions: The LEDs are located on the device front.

2.3.4 General sequence for commissioning

To commission the device, proceed as follows:

- Supply the device with operating voltage (nominal value: 24 V DC).
- Connect the device via the Ethernet interface using an RJ45 connector to the PC that will be used for configuration.
- Assign an IP address to the device via BootP. The IP address is allocated by a corresponding server in the network or a PC tool (see “Assigning the IP address” on page 25).

ℹ Alternatively, you can access web-based management via the host name (see “DNS host name” on page 18).

⇒ The device can now be configured via web-based management (WBM) or the Command Line Interface (CLI).

ℹ Make sure that the PC that will be used for configuration via WBM or CLI has an IP address in the same IP range.

ℹ For further information on the Command Line Interface, refer to the separate manual at phoenixcontact.net/qr/<item_number>.

2.3.5 Resetting to the default settings

The following options are available for resetting the device to the default settings:

– Resetting via Smart mode (see “Using Smart mode” on page 22).

– Resetting via web-based management (see “System” on page 50).

2.4 Using Smart mode

In Smart mode, you can change the operating mode of the switch, without having access to one of the management interfaces.

Press the Smart mode button to enter Smart mode, select the desired setting, and exit Smart mode. The four mode LEDs indicate the setting that is currently selected and will apply when Smart mode is exited.

The following setting options can be selected via Smart mode:

– Resetting the IP configuration

– Operation in EtherNet/IP mode (default setting on standard versions)

– Operation in PROFINET mode (default setting on PROFINET versions)

– Operation with static IP address

– Operation in Unmanaged mode

– Resetting to the default settings

ℹ On the 26xx/27xx versions, the Smart mode button is located underneath the M16 metal cap.

2.4.1 Calling up Smart mode

- Connect the device to the supply voltage.
- Wait approximately 30 seconds for the device to boot up and be ready for operation.

ℹ Once the device is booted and ready for operation, the LEDs for all ports go out.

- Press and hold down the Smart mode button for at least five seconds.

⇒ If Smart mode is active, the four LEDs of port XF1 and XF2 will flash. The active state is indicated alternately by the flashing sequence of all four LEDs.

When Smart mode is started, the switch is initially in the “Exit without changes” state.

2.4.2 Selecting the desired setting

- To select the various settings, press the Smart mode button briefly and select the desired operating mode (see Table 2-6).

2.4.3 Possible operating modes in Smart mode

The switch supports the selection of the following operating modes in Smart mode:

Table 2-6 Operating modes in Smart mode

Mode	LED 1[1]	LED 2[1]	LED 3[1]	LED 4[1]
Exit Smart mode without changes	**On**	Off	Off	Off
Set Universal mode (default setting on standard versions)	Off	**On**	Off	Off
Set PROFINET mode (default setting on PROFINET versions)[2]	**On**	**On**	Off	Off
Set EtherNet/IP mode	Off	Off	**On**	Off
Operation with default IP address	Off	**On**	**On**	Off
Reset the IP configuration	**On**	**On**	**On**	Off
Operation in Unmanaged mode	Off	**On**	Off	**On**

[1] On the 20xx/21xx/22xx/23xx/26xx/27xx versions, the two LEDs (LNK/ACT and SPD) of port 1 and 2 respectively are used – the reading direction on the device is from top to bottom (LED 1 = LNK/ACT of port 1, LED 4 = SPD of port 2).
On the 24xx/25xx versions, the four LNK/ACT LEDs of port 1-4 are used – the port number corresponds to the LED number.

[2] The 20xx/21xx versions do not support PROFINET mode.

2.4.4 Exiting Smart mode

- To exit this mode, press and hold down the Smart mode button for at least five seconds. The previously selected operating mode is saved and activated as soon as you release the Smart mode button.

2.4.5 Operation in Universal mode

Activating Universal mode resets the device as described in "Configuration in the delivery state" on page 19. This deletes any configurations stored on the device. An automation protocol is not activated in this mode. The initial IP configuration is activated (see Section "Initial IP configuration in the delivery state" on page 18).

2.4.6 Operation in PROFINET mode

Activating PROFINET mode resets the device as described in "Configuration in the delivery state" on page 19 and activates the PROFINET device and DCP functions for IP address assignment. In addition, the "PROFINET" Quality of Service profile is activated. This deletes any configurations stored on the device. The PROFINET automation protocol is activated in this mode.

In PROFINET mode, the initial IP configuration (see Section "Initial IP configuration in the delivery state" on page 18) is not supported and therefore deactivated.

2.4.7 Operation in EtherNet/IP mode

Activating EtherNet/IP mode resets the device as described in “Configuration in the delivery state” on page 19 and activates the IGMP snooping and IGMP querier (version 2) functions. In addition, the “EtherNet/IP” Quality of Service profile is activated. This deletes any configurations stored on the device. The initial IP configuration is activated (see Section “Initial IP configuration in the delivery state” on page 18).

2.4.8 Operation with default IP address

For operation with a default IP address, the device is assigned a fixed IP address. A DHCP server is activated on the switch and assigns an IP address to the connected PC via DHCP.

ℹ To start up the device with a default IP address, activate the “Operation with static IP address” Smart mode (see “Using Smart mode” on page 22).

- In the network settings on your PC, select the “Obtain an IP address automatically” option.

ℹ Deactivate all other network interfaces on your PC.

- Connect the switch to your PC.
- Select the “Operation with default IP address” Smart mode (see “Using Smart mode” on page 22).

⇒ The switch assigns an IP address to the PC via DHCP.
⇒ The switch can now be accessed via IP address “192.168.0.254”.

- Set the desired IP address via web-based management.

2.4.9 Resetting the IP configuration

When the “Reset IP configuration” Smart mode is activated, the IP address, subnet mask, and default gateway are reset to 0.0.0.0 and BootP is activated. Any other configurations stored on the device are retained and are not deleted. The initial IP configuration is activated (see “Initial IP configuration in the delivery state” on page 18).

2.4.10 Operation in Unmanaged mode

During operation in Unmanaged mode, the switch can be used without an IP address. Here, the switch uses the static IP address 0.0.0.0. The subnet mask and gateway are also configured to 0.0.0.0. This means that web-based management can no longer be accessed and the switch no longer sends BootP and DHCP requests.

Major functions remain active in Unmanaged mode:

– Redundancy mechanisms for loop suppression (RSTP, FRD, LTS)
– Functions for hardening the network (broadcast/multicast limiter)
– Functions for reducing the network load (IGMP snooping)

ℹ Use of IGMP in Unmanaged mode is limited to IGMP snooping. The switch requires an IP address if the device is also to be used as an IGMP querier.

The functions must be configured in Managed mode and will remain active when switching to Unmanaged mode. Alternatively, Unmanaged mode can be activated using a configuration file and SD card (see UM EN HW FL SWITCH 2000, item number 108997).

ℹ Unmanaged mode can only be exited by switching to a different Smart mode or by resetting the switch to the default settings.

2.5 Assigning the IP address

ℹ On the standard versions, BootP is activated in the delivery state. On the PROFINET versions, DCP is activated in the delivery state.

Notes on BootP

During initial startup, the device sends BootP requests without interruption until it receives a valid IP address. As soon as the device receives a valid IP address, it stops sending further BootP requests.

If the device has already been configured, it sends three BootP requests when a restart is performed. If these three BootP requests do not receive a response, the device starts with the IP address that was last assigned via BootP.

ℹ An activated firewall on the PC can hinder the allocation of IP addresses via BootP.

Numerous BootP servers are available on the Internet. You can use any of these programs for address assignment.

This section explains IP address assignment using the “FL Network Manager Basic” (item number 2702889) and the “IP Assignment Tool” software tools from Phoenix Contact.

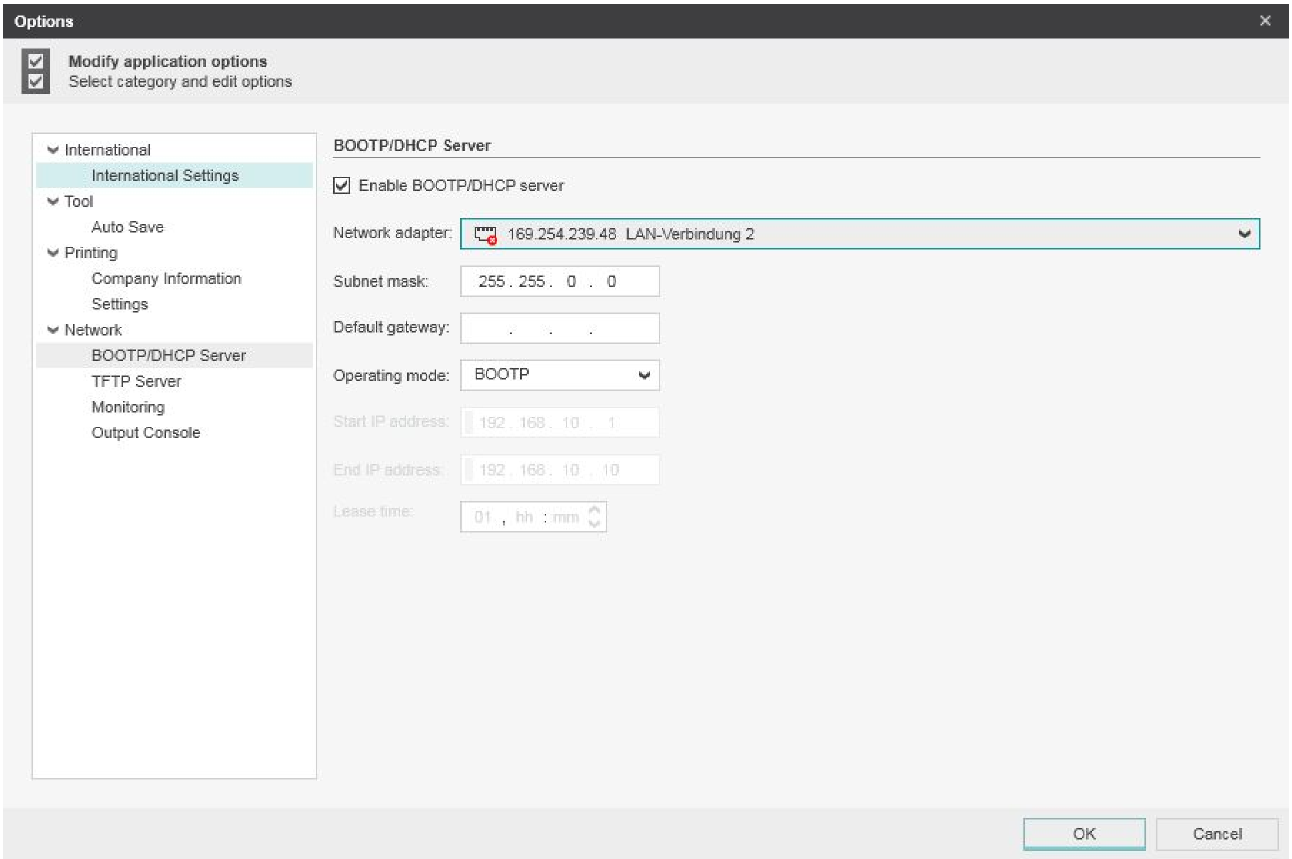
2.5.1 Assigning the IP address via BootP using Network Manager

Requirements

The device is connected to a PC with a Microsoft Windows operating system, and the FL Network Manager has been successfully installed.

Step 1: Parameterizing the BootP server

Figure 2-2 Parameterizing the BootP server



☑ Enable BOOTP/DHCP server

Network adapter: 169.254.239.48 LAN-Verbindung 2

Subnet mask: 255 . 255 . 0 . 0

Default gateway: . . .

Operating mode: BOOTP

Start IP address: 192 . 168 . 10 . 1

End IP address: 192 . 168 . 10 . 10

Lease time: 01 , hh : mm

- Open the FL NETWORK MANAGER software.
- Open a new project in the software.
- Under “Extras, Options”, select the “BOOTP/DHCP Server” menu item.
- Activate the “Enable BOOTP/DHCP server” check box.
- Here, configure the network interface on your PC to which the device is connected and select the “BootP” operating mode. You can also adjust the subnet mask and configure a default gateway.
- Confirm the parameterization with “OK”.

Step 2: Starting the BootP server

Figure 2-3 Opening the BootP window

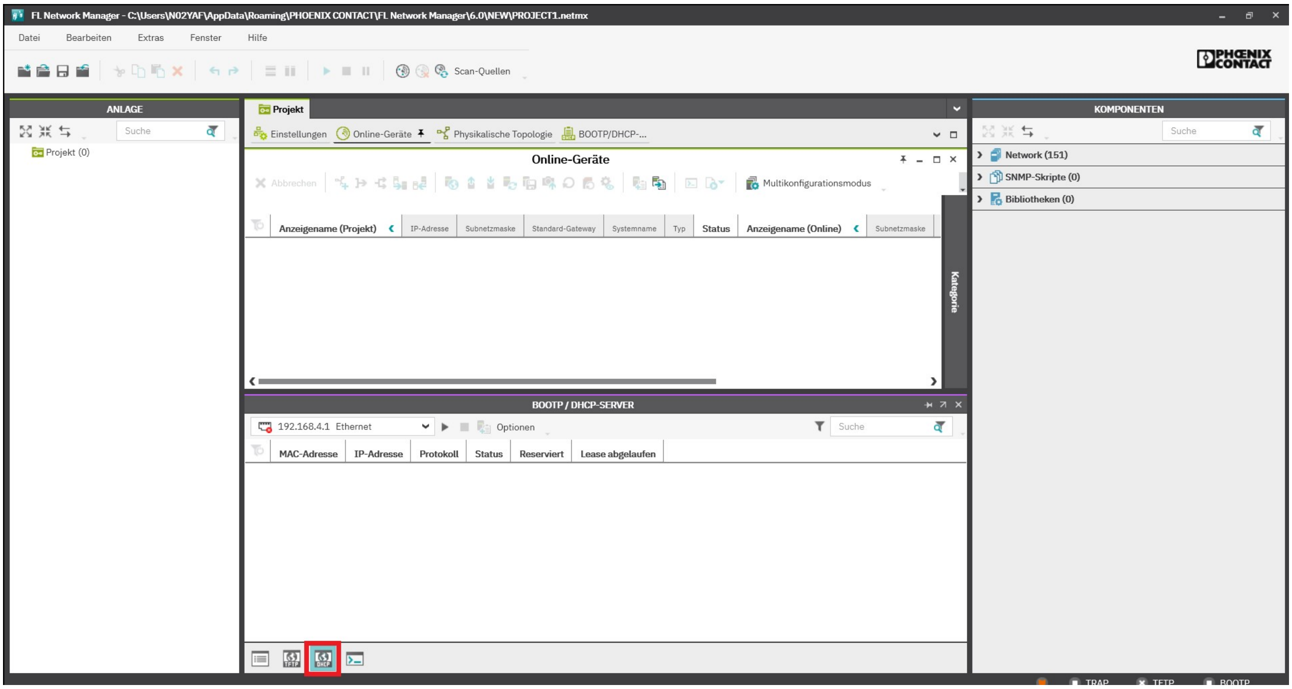
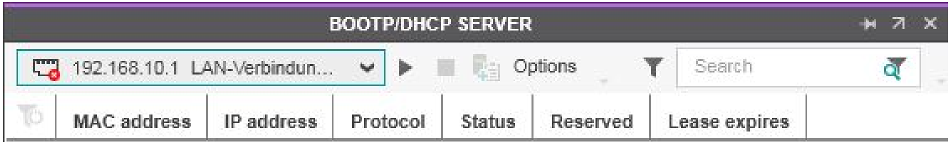


Figure 2-4 Starting the BootP server



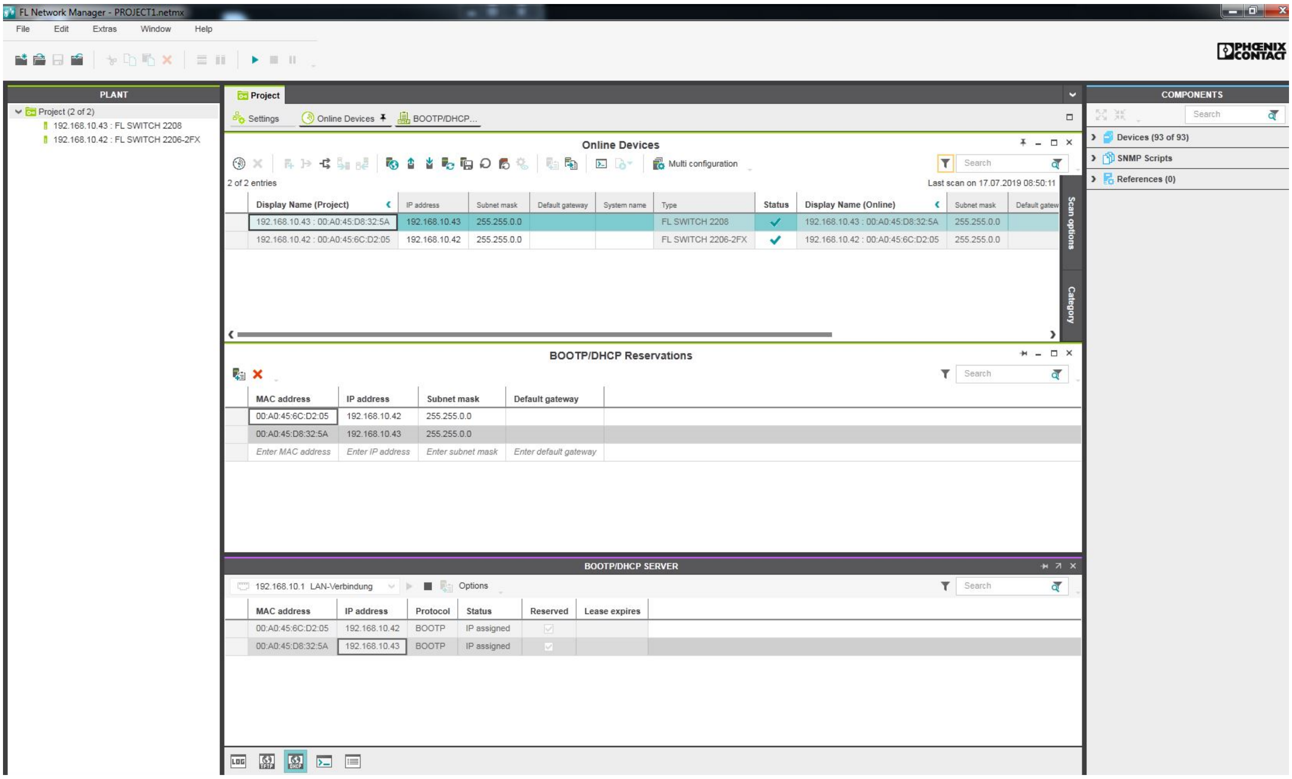
- Open the “BOOTP/DHCP SERVER” window.
- Click on the “play” icon next to the selected network interface.

⇒ The BootP server is activated.

⇒ BootP requests that are received are listed in the “BOOTP/DHCP SERVER” window in table format.

Step 3: Inserting BootP requests in the reservation list and assigning IP parameters

Figure 2-5 Inserting BootP requests in the reservation list



Online Devices

2 of 2 entries

Last scan on 17.07.2019 08:50:11

Display Name (Project)	IP address	Subnet mask	Default gateway	System name	Type	Status	Display Name (Online)	Subnet mask	Default gatew
192.168.10.43 : 00:A0:45:D8:32:5A	192.168.10.43	255.255.0.0			FL SWITCH 2208	✓	192.168.10.43 : 00:A0:45:D8:32:5A	255.255.0.0	
192.168.10.42 : 00:A0:45:6C:D2:05	192.168.10.42	255.255.0.0			FL SWITCH 2206-2FX	✓	192.168.10.42 : 00:A0:45:6C:D2:05	255.255.0.0	

BOOTP/DHCP Reservations

MAC address	IP address	Subnet mask	Default gateway
00:A0:45:6C:D2:05	192.168.10.42	255.255.0.0	
00:A0:45:D8:32:5A	192.168.10.43	255.255.0.0	
Enter MAC address	*Enter IP address*	*Enter subnet mask*	*Enter default gateway*

BOOTP/DHCP SERVER

192.168.10.1 LAN-Verbindung

MAC address	IP address	Protocol	Status	Reserved	Lease expires
00:A0:45:6C:D2:05	192.168.10.42	BOOTP	IP assigned	☑	
00:A0:45:D8:32:5A	192.168.10.43	BOOTP	IP assigned	☑	

- If you want to assign IP parameters to a device, such as IP address, subnet mask, or default gateway, right-click on an incoming BootP request in the “BOOTP/DHCP SERVER” window. Then, select “Add to BOOTP/DHCP reservations”.
- Enter the IP address to be assigned in the “BOOTP/DHCP Reservations” window. The IP parameters are immediately transferred to the device.
- You can check whether IP address assignment was successful in the “IP address” column in the “BOOTP/DHCP SERVER” window.

The IP parameters set here can be changed in web-based management.

2.5.2 Assigning the IP address via BootP using IPAssign.exe

This section deals with IP address assignment using the “IP Assignment Tool” Windows software (IPAssign.exe).

The software can be downloaded free of charge at phoenixcontact.net/qr/<item_number>.

Requirement:

The device is connected to a computer with a Windows operating system.

Step 1: Downloading and running the software

You can download the software from the Internet.

- Go to phoenixcontact.net/qr/<item_number>.

- Under “Software”, download the BootP IP addressing tool.
- Double-click on the “IPAssign.exe” file and, if necessary, click on “Execute”.

⇒ The software is opened.

Step 2: IP Assignment Wizard

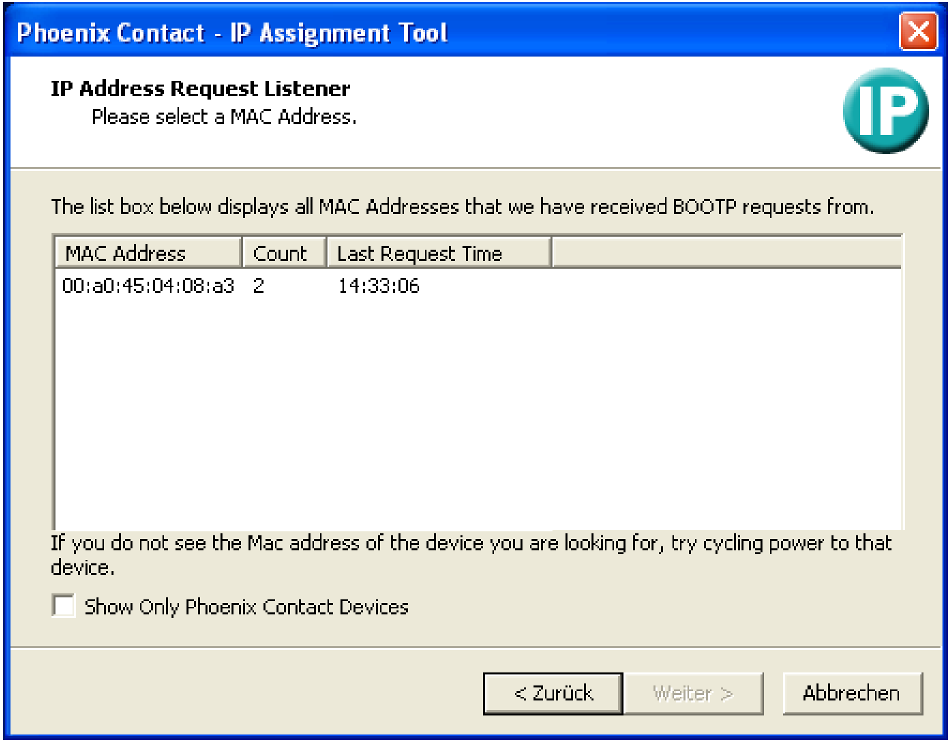
The software is in English for international purposes. However, the software buttons change according to your country-specific settings.

- Click on “Next”.

⇒ You now see a list of all devices that send BootP requests and are waiting for an IP address.

Step 3: IP Address Request Listener

Figure 2-6 “IP Address Request Listener” window



Phoenix Contact - IP Assignment Tool

IP Address Request Listener

Please select a MAC Address.

The list box below displays all MAC Addresses that we have received BOOTP requests from.

MAC Address	Count	Last Request Time
00:a0:45:04:08:a3	2	14:33:06

If you do not see the Mac address of the device you are looking for, try cycling power to that device.

□ Show Only Phoenix Contact Devices

In this example, the device has MAC address 00:a00:45:04:08:a3.

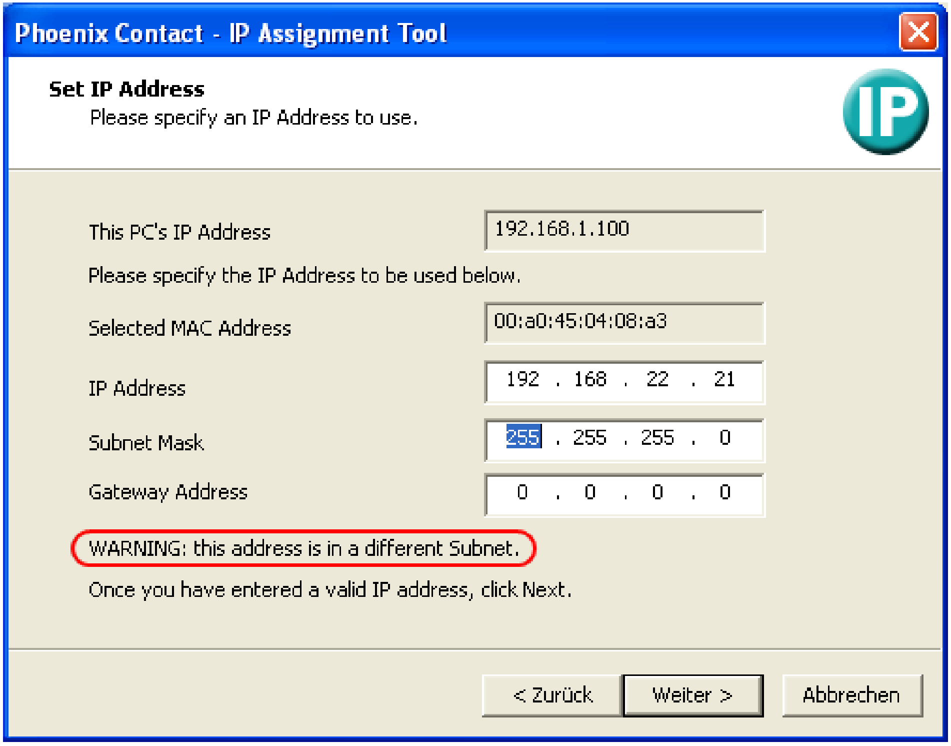
The MAC address of your switch can be found on the sticker on the side.

- Select the device you want to assign an IP address for.
- Click on “Next”.

Step 4: Setting the IP Address

In the “Set IP Address” window, you can view and define various parameters:

Figure 2-7 “Set IP Address” window



Set IP Address

Please specify an IP Address to use.

This PC's IP Address: 192.168.1.100

Please specify the IP Address to be used below.

Selected MAC Address: 00:a0:45:04:08:a3

IP Address: 192 . 168 . 22 . 21

Subnet Mask: 255 . 255 . 255 . 0

Gateway Address: 0 . 0 . 0 . 0

WARNING: this address is in a different Subnet.

Once you have entered a valid IP address, click Next.

Table 2-7 “Set IP Address” window: Parameters

Parameter	Description
This PC‘s IP Address	The IP address of the currently used PC is displayed here.
Selected MAC Address	The MAC address selected in the previous step is displayed here.
IP Address	In this input field, enter the desired IPv4 address for the connected device. Make sure to enter a valid IP address.
Subnet Mask	In this input field, enter the desired subnet mask for the connected device.
Gateway Address	In this input field, enter the desired gateway address for the connected device.

- Adjust the IP parameters according to your requirements.

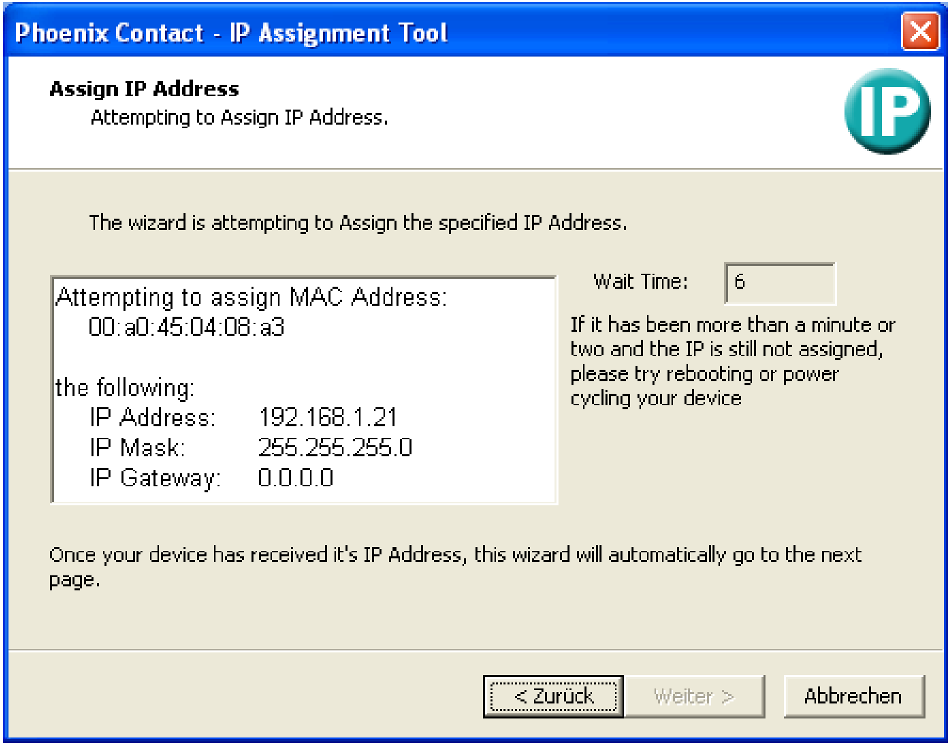
⇒ If no inconsistencies are detected, a message appears indicating that a valid IP address has been set.

- Click on “Next”.

Step 5: Assigning an IP Address

The software now attempts to transfer the set IP parameters to the device. Following successful transfer, the next window automatically opens.

Figure 2-8 “Assign IP Address” window



Assign IP Address
Attempting to Assign IP Address.

The wizard is attempting to Assign the specified IP Address.

```
Attempting to assign MAC Address:
   00:a0:45:04:08:a3

the following:
   IP Address:     192.168.1.21
   IP Mask:        255.255.255.0
   IP Gateway:     0.0.0.0
```

Wait Time: 6

If it has been more than a minute or two and the IP is still not assigned, please try rebooting or power cycling your device

Once your device has received it's IP Address, this wizard will automatically go to the next page.

Step 6: Completing IP address assignment

The window informs you that IP address assignment has been completed successfully. It provides an overview of the IP parameters that have been transferred to the selected device.

- To assign IP parameters for additional devices, click on “Back”.
- To exit the IP address assignment, click on “Finish”.

ℹ The IP parameters set here can be changed in web-based management.

3 Frame switching

The switch operates in store-and-forward mode. When receiving a data packet, the switch analyzes the source and destination addresses. The switch stores up to 8192 MAC addresses in its address table with an adjustable aging time of 10 seconds to 825 seconds.

3.1 Store and forward

All data telegrams received by the switch are stored and checked for their validity. Invalid or faulty data packets (e.g., CRC errors) and fragments (<64 bytes) are discarded. The switch forwards valid data telegrams.

3.2 Multi-address function

The switch learns all the source addresses for each port. Only packets with the following attributes are forwarded via the relevant port:

- Unknown source addresses
- A source address for this port
- A multicast or broadcast address

The switch can learn up to 8192 addresses. This is necessary if more than one end device is connected to one or more ports. You can connect several independent subnets to one switch.

3.2.1 Learning addresses

The switch independently learns the addresses of the end devices that are connected via this port. The switch does this by evaluating the source addresses in the data telegrams. When the switch receives a data telegram, it forwards this data telegram only to the port that connects to the specified device (if the address could be learned beforehand).

The switch monitors the age of the learned addresses. The switch automatically deletes address entries that exceed a specific age from its address table (default: 40 seconds of aging time, adjustable from 10 seconds to 825 seconds).

ℹ All learned address entries are deleted upon restart. A link down deletes all the entries of the affected port.

ℹ You will find a list of all detected MAC addresses in the MAC address table. You can clear the MAC address table using the “Clear” button (see “MAC Address Table” on page 43).

ℹ The aging time is set using the “dot1dTpAgingTime” MIB object (OID 1.3.6.1.2.1.17.4.2). The possible setting range is 10 seconds to 825 seconds. For static configuration, an aging time of 300 seconds is recommended.

3.2.2 Prioritization

The switch supports eight priority queues for the purpose of influencing the internal packet processing sequence (traffic classes in accordance with IEEE 802.1Q).

Data telegrams received are assigned to these classes in accordance with the data packet priority specified in the VLAN/prioritization tag. The value “0” in the tag signifies the lowest priority, while the value “7” in the tag signifies the highest priority.

Furthermore, the switch also supports the detection and high prioritization of automation protocols (PROFINET and EtherNet/IP) in certain profiles.

Processing rules

The switch controller in the device forwards received packets to the available receive queues based on the following decisions:

– BPDU packets are always assigned to a high-priority queue.

– If the corresponding Quality of Service profile is activated, PROFINET and EtherNet/IP packets will also be assigned to a queue with a high priority.

– According to their priority, packets with VLAN/prioritization tag are assigned to the aforementioned queues in a descending order. Which priority tag is assigned to which queue depends on the selected Quality of Service profile.

– All remaining data is assigned to the low-priority queue.

ℹ For a description of the configuration options, refer to Section “Quality of Service” on page 99.

Class of Service – CoS

Class of Service refers to a mechanism used to take into consideration the value of the priority field (values 1 to 7) in VLAN data packets with a tag. The switch assigns the data streams to various processing queues, depending on the priority information contained in the CoS tag. The switch supports eight internal processing queues.

Quality of Service – QoS

Quality of Service affects the forwarding of data streams and results in individual data streams being treated differently (usually preferential). QoS can be used to guarantee a transmission bandwidth for individual data streams, for example. The switch uses QoS in connection with prioritization (see “Class of Service – CoS” on page 34).

4 Configuration and diagnostics in web-based management

4.1 General information

You can use web-based management (WBM) to manage your device from anywhere in the network using a standard browser (e.g., Microsoft Edge). The configuration and diagnostic functions are clearly displayed on a graphical user interface. Depending on the permission, each user has read and/or write access to the device. A wide range of information about the device itself, the set parameters, and the operating state can be viewed.

ℹ Modifications to the device can only be made with an account with corresponding rights. In the default settings, the user name is “admin” and the password is “private”.

NOTE: Changing the initial password

With the initial password, unauthorized access is possible.

– Change the administrator password immediately after the first login.

– Do not share the password.

4.1.1 Accessing web-based management

- Perform the initial startup (see “General sequence for commissioning” on page 21).

ℹ Make sure that the PC that will be used for configuration has an IP address in the same IP range.

ℹ Device login is only possible if cookies are enabled in the browser settings.

ℹ Some functions are opened in pop-up windows. Use of all the functions is therefore only possible if pop-ups are permitted in the browser settings.

ℹ The web server operates using the Hypertext Transfer Protocol (HTTP). A standard browser can therefore be used. For full operation of the web pages, the browser must support JavaScript 1.2 and Cascading Style Sheets Level 1.

- Open a browser and enter the IP address of the device in the address line.

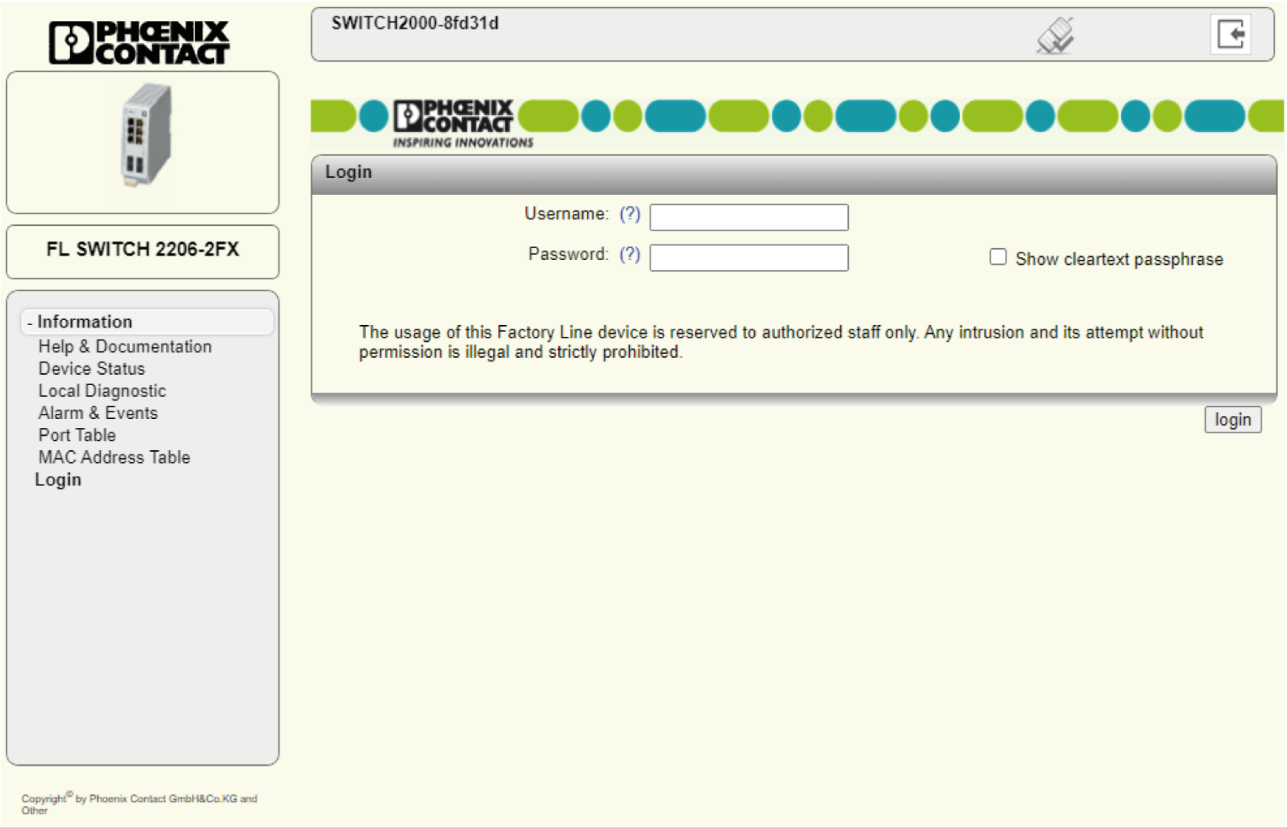
⇒ Web-based management opens.

- Click on “Login” and log in using your access data.

ℹ In the default settings, the user name is “admin” and the password is “private”.

ℹ Up to ten users each can log in at the same time either via web-based management or CLI.

Figure 4-1 Login area



Login

Username:

Password:

□ Show cleartext passphrase

The usage of this Factory Line device is reserved to authorized staff only. Any intrusion and its attempt without permission is illegal and strictly prohibited.

Copyright© by Phoenix Contact GmbH&Co.KG and Other

Depending on the configuration of the device, a user account may be locked for a period of time after a certain number of failed login attempts. During this time, it is not possible to access WBM, even if the correct user data is entered (see “User Management” on page 46).

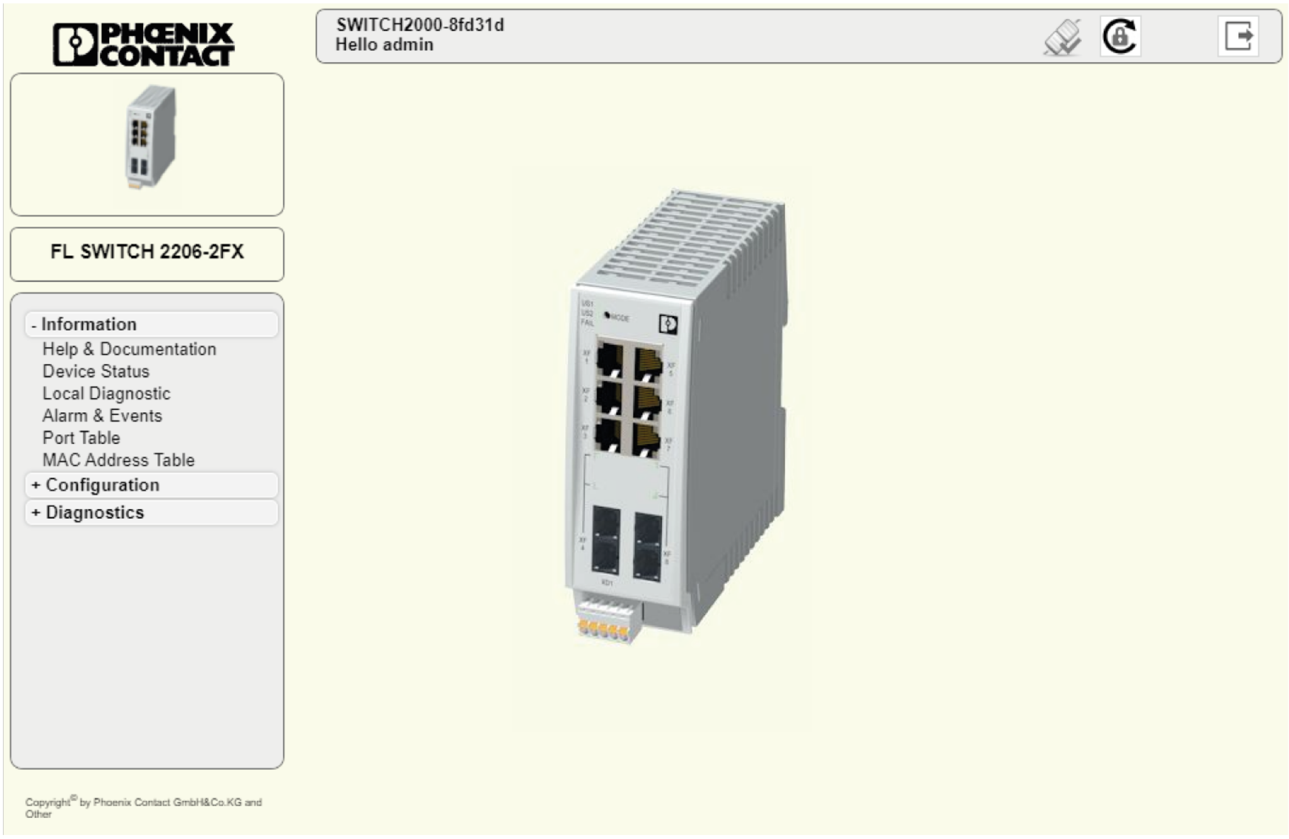
4.1.2 Areas in web-based management

The visibility and configurability of the individual areas and parameters depend on the scope of permissions of the respective user account.

Web-based management (WBM) is split into the following areas:

- Information: General device information
- Configuration: Device configuration
- Diagnostics: Device-specific diagnostics

Figure 4-2 Start page for web-based management (example)



4.1.3 Icons and buttons in web-based management

At the top and bottom of WBM are icons and buttons that provide an overview of important device functions (see Figure 4-3).

Figure 4-3 WBM with icons (selection)

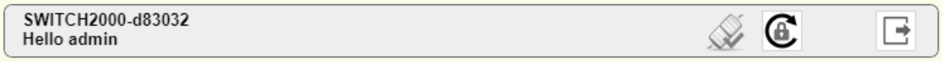


Table 4-1 Explanation of icons

Icon	Explanation
🔌	Connection status: Connected This icon indicates that there is currently a connection between the device and the PC used.
✖🔌	Connection status: Disconnected This icon indicates that there is currently no connection between the device and the PC used. This is the case if a configuration change is currently being carried out. Alternatively, this is the case after a configuration change has been performed via WLAN and resulted in changes that require a new login.
⇥	A user is logged into the device at present. The icon is also the logout button.
⇤	No user is logged into the device at present. The icon is also the login button.
💾	The active configuration differs from the saved configuration for the device. To save the active configuration, click on the icon.
🔒	The administrator password has not yet been changed and is the initial password. For security reasons, we recommend changing the existing password to a new one known only to you. ❗ **NOTE: Changing the initial password** With the initial password, unauthorized access is possible. – Change the administrator password immediately after the first login. – Do not share the password.

Table 4-2 Explanation of the buttons

Button	Explanation
Revert	This button deletes all the changes that have been made since the last save.
Apply	This button applies the current settings, but does not save the configuration. The changes confirmed with “Apply” are lost during the next voltage reset.
Apply&Save	This button applies the current settings and saves the configuration. The settings made are also retained after a voltage reset. ⓘ If an SD card is inserted, clicking on “Apply&Save” additionally saves the configuration to the SD card. If there is an existing configuration on the SD card, it will be overwritten.

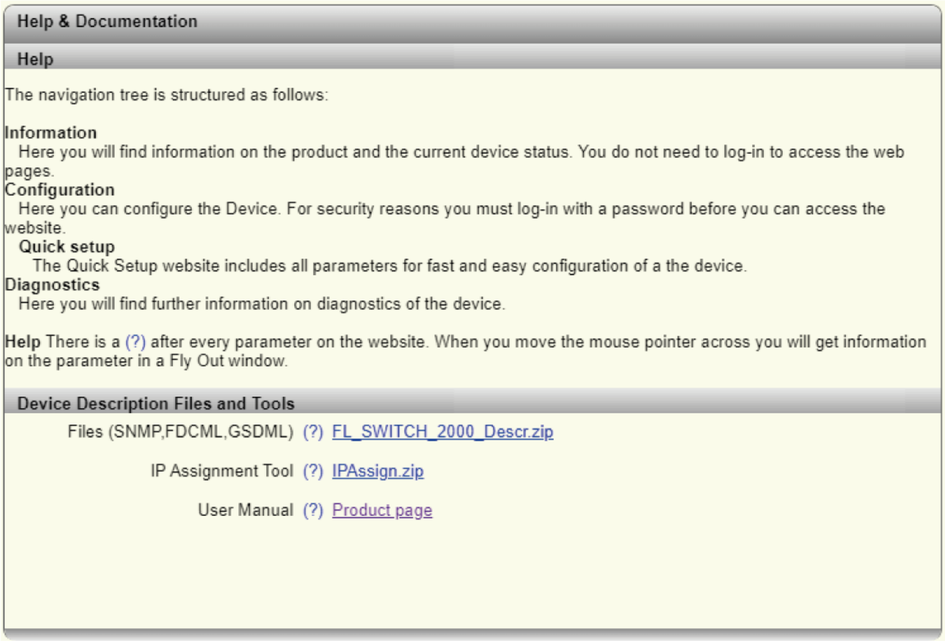
4.2 WBM Information area

4.2.1 Help & Documentation

On this page, you will find useful information on how to use web-based management (WBM).

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Information, Help & Documentation”.

Figure 4-4 Help & Documentation



Help & Documentation

Help

The navigation tree is structured as follows:

Information
Here you will find information on the product and the current device status. You do not need to log-in to access the web pages.
Configuration
Here you can configure the Device. For security reasons you must log-in with a password before you can access the website.
Quick setup
The Quick Setup website includes all parameters for fast and easy configuration of a the device.
Diagnostics
Here you will find further information on diagnostics of the device.

Help There is a (?) after every parameter on the website. When you move the mouse pointer across you will get information on the parameter in a Fly Out window.

Device Description Files and Tools

Files (SNMP,FDCML,GSDML) (?) FL_SWITCH_2000_Descr.zip

IP Assignment Tool (?) IPAssign.zip

User Manual (?) Product page

On this page, you can also download the following files and software directly from the device:

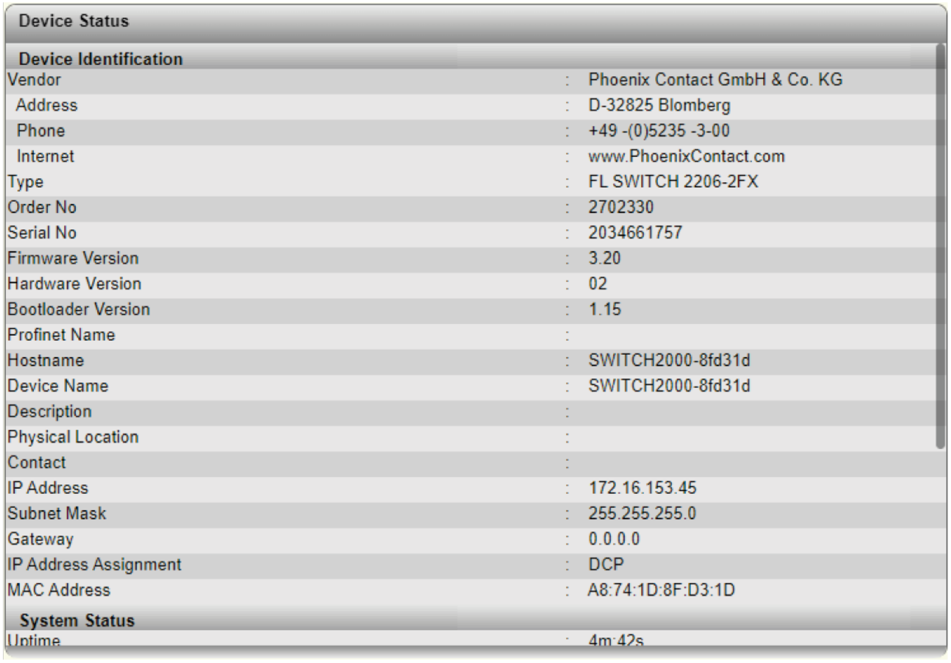
- Files (SNMP, FDCML, GSDML)
- IP Assignment Tool
- User Manual: Click on “Product page” to be brought to the product page. Here, you can download the current documentation.

4.2.2 Device Status

On this page, you will find general information about your device, such as the serial number, firmware version, or hardware revision.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Information, Device Status”.

Figure 4-5 Device Status



Device Status

Device Identification

Vendor	Phoenix Contact GmbH & Co. KG
Address	D-32825 Blomberg
Phone	+49 -(0)5235 -3-00
Internet	www.PhoenixContact.com
Type	FL SWITCH 2206-2FX
Order No	2702330
Serial No	2034661757
Firmware Version	3.20
Hardware Version	02
Bootloader Version	1.15
Profinet Name	
Hostname	SWITCH2000-8fd31d
Device Name	SWITCH2000-8fd31d
Description	
Physical Location	
Contact	
IP Address	172.16.153.45
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
IP Address Assignment	DCP
MAC Address	A8:74:1D:8F:D3:1D

System Status

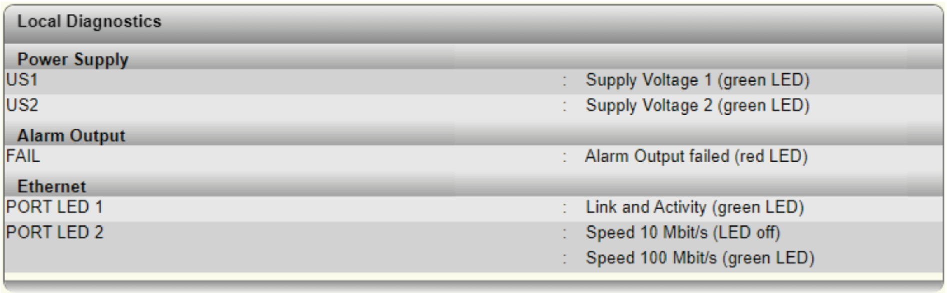
Uptime	4m:42s

4.2.3 Local Diagnostics

On this page, you will find a brief explanation of the individual LEDs on the device.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Information, Local Diagnostics”.

Figure 4-6 Local Diagnostics



Local Diagnostics

Power Supply

US1	Supply Voltage 1 (green LED)
US2	Supply Voltage 2 (green LED)

Alarm Output

FAIL	Alarm Output failed (red LED)

Ethernet

PORT LED 1	Link and Activity (green LED)
PORT LED 2	Speed 10 Mbit/s (LED off)
	Speed 100 Mbit/s (green LED)

4.2.4 Alarm & Events

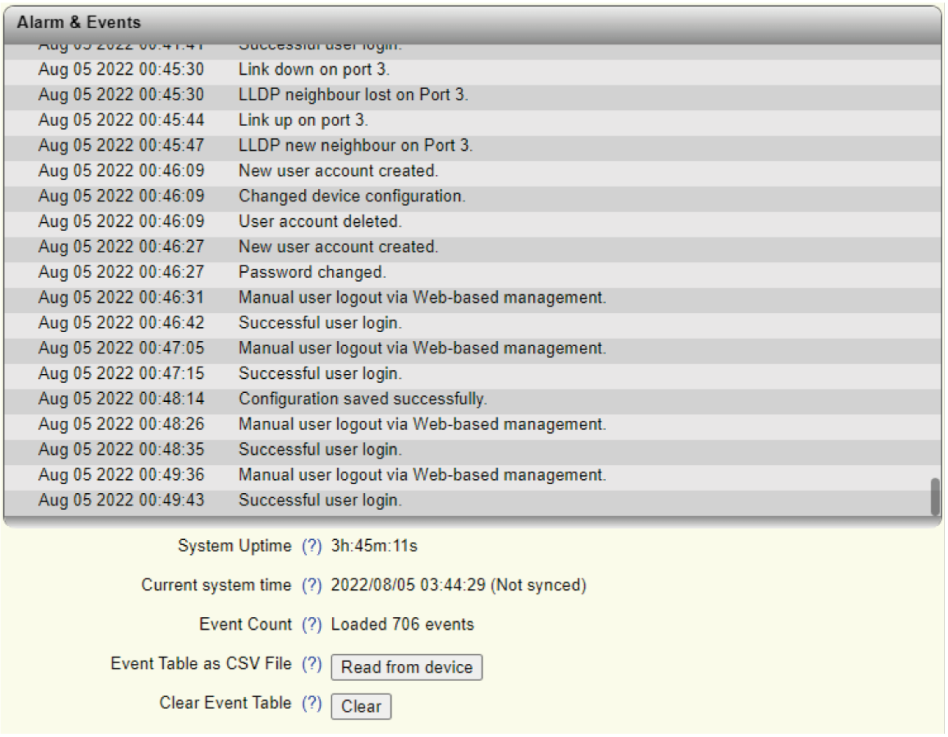
On this page, you will find a list of alarms and events in a table. For Event Table entries to be retained after the device is restarted, you can save them. You can download the Event Table from the device in CSV format.

ℹ A maximum of 3000 entries can be stored in the Event Table. The oldest entries are overwritten. If there is a large number of entries, it may take a few seconds to load the Event Table.

The persistent storage of events is deactivated in the factory default state. This means that the events are deleted when the device is restarted. You can activate the function via the “Persistent Event Logging” item on the “Service” page (see “Service” on page 58).

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Information, Alarm & Events”.

Figure 4-7 Alarm & Events



Alarm & Events

```
Aug 05 2022 00:41:41   Successful user login.
Aug 05 2022 00:45:30   Link down on port 3.
Aug 05 2022 00:45:30   LLDP neighbour lost on Port 3.
Aug 05 2022 00:45:44   Link up on port 3.
Aug 05 2022 00:45:47   LLDP new neighbour on Port 3.
Aug 05 2022 00:46:09   New user account created.
Aug 05 2022 00:46:09   Changed device configuration.
Aug 05 2022 00:46:09   User account deleted.
Aug 05 2022 00:46:27   New user account created.
Aug 05 2022 00:46:27   Password changed.
Aug 05 2022 00:46:31   Manual user logout via Web-based management.
Aug 05 2022 00:46:42   Successful user login.
Aug 05 2022 00:47:05   Manual user logout via Web-based management.
Aug 05 2022 00:47:15   Successful user login.
Aug 05 2022 00:48:14   Configuration saved successfully.
Aug 05 2022 00:48:26   Manual user logout via Web-based management.
Aug 05 2022 00:48:35   Successful user login.
Aug 05 2022 00:49:36   Manual user logout via Web-based management.
Aug 05 2022 00:49:43   Successful user login.
```

System Uptime (?) 3h:45m:11s

Current system time (?) 2022/08/05 03:44:29 (Not synced)

Event Count (?) Loaded 706 events

Event Table as CSV File (?) [Read from device]

Clear Event Table (?) [Clear]

Table 4-3 Alarm & Events: Parameters

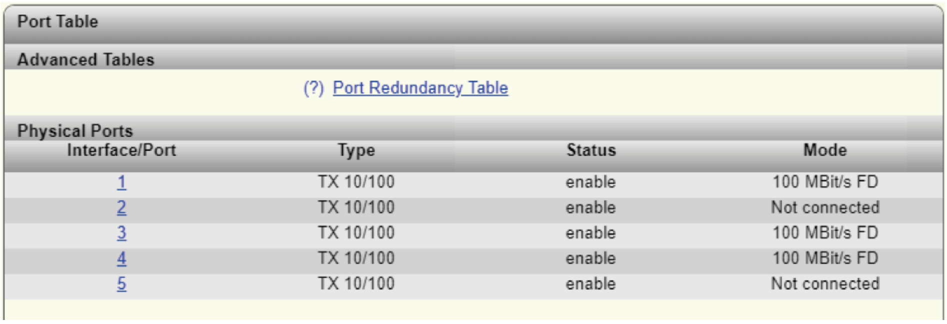
Parameter	Description
System Uptime	Shows how long the device has been in operation since the last restart.
Current system time	The current system time is displayed here. If the time is not synchronized, there may be discrepancies between the system time and the actual time (see “Service” on page 58).
Event Count	The number of currently loaded events in the Event Table is displayed here.
Event Table as CSV File	Click on “Read from device” to download the currently displayed Event Table as a CSV file and save it.
Clear Event Table	Click on “Clear” to delete all the currently displayed events in the Event Table.

4.2.5 Port Table

On this page, you will find a list of the current states of the individual ports.

- Open web-based management (see "Accessing web-based management" on page 35) and log in.
- Click on "Information, Port Table".

Figure 4-8 Port Table



Port Table

Advanced Tables

(?) Port Redundancy Table

Physical Ports

Interface/Port	Type	Status	Mode
1	TX 10/100	enable	100 MBit/s FD
2	TX 10/100	enable	Not connected
3	TX 10/100	enable	100 MBit/s FD
4	TX 10/100	enable	100 MBit/s FD
5	TX 10/100	enable	Not connected

Table 4-4 Port Table: Parameters

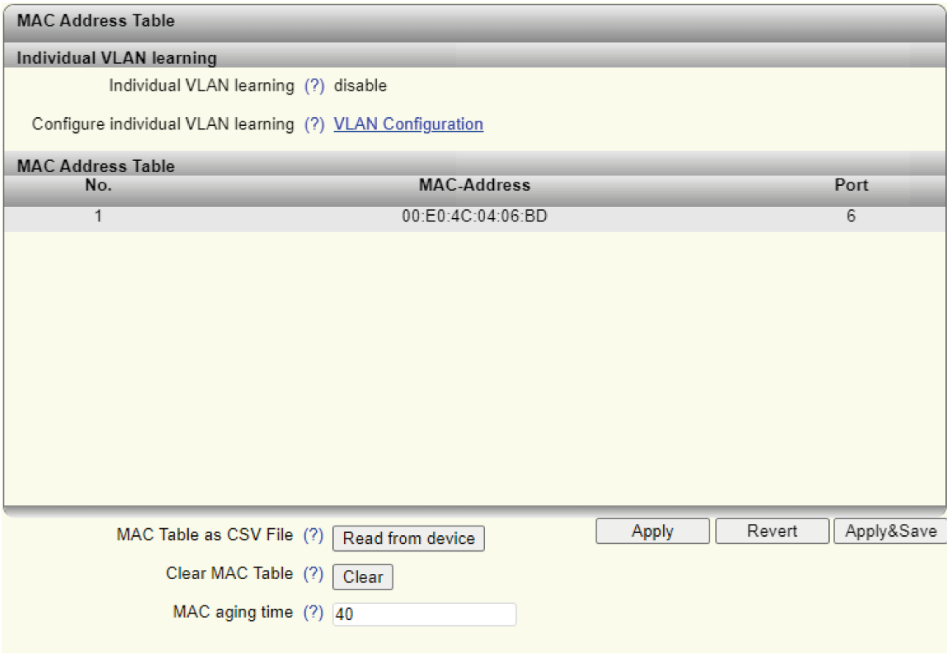
Parameter	Description
Port Redundancy Table	Click on "Port Redundancy Table" to open a table with information on the individual ports and their redundancy mechanism assignments (see "Pop-up window: Redundancy Port Table" on page 104).
Interface/Port	Click on a port number to open the "Port Configuration" window (see "Port Configuration" on page 66).
Type	This column shows whether the port is copper (e.g., TX 10/100) or fiberglass (e.g., FX 100).
Status	This column shows whether the port is activated or deactivated.
Mode	The current connection status of the port is displayed here. – Not connected: No active link at the port. – 1000 Mbps FD (or comparable status): The link is active. The transmission speed and the duplex mode are displayed. – Far-End Fault: A fault has occurred on a fiber of a bidirectional fiberglass connection (e.g., due to a defective fiberglass cable). If the device at the other end also supports far-end fault, it detects a communication failure on its own receiver connection and sends a far-end fault signal pattern to the peer.
Member of LAG-Trunk/ Member Ports	This option is only available if trunks are configured via link aggregation on the device (see "LACP – Link Aggregation Control Protocol" on page 145). The assignment between the port and virtual trunk port is displayed here.
PSE Status	This option is only available on the SPE versions. The PSE status of the relevant port is displayed here.

4.2.6 MAC Address Table

On this page, you will find a list of the current devices in the network. You can download the list from the device in CSV format.

- Open web-based management (see "Accessing web-based management" on page 35) and log in.
- Click on "Information, MAC Address Table".

Figure 4-9 MAC Address Table



MAC Address Table

Individual VLAN learning

Individual VLAN learning (?) disable

Configure individual VLAN learning (?) VLAN Configuration

MAC Address Table

No.	MAC-Address	Port
1	00:E0:4C:04:06:BD	6

MAC Table as CSV File (?) Read from device

Clear MAC Table (?) Clear

MAC aging time (?) 40

MAC Address Table: Individual VLAN learning

This section is only available if Individual VLAN learning has been deactivated (see "VLAN Configuration" on page 159).

Table 4-5 MAC Address Table: Parameters

Parameter	Description
Individual VLAN learning	This shows that Individual VLAN learning is deactivated.
Configure Individual VLAN learning	Click on "VLAN Configuration" to configure the individual VLAN (see "VLAN Configuration" on page 159).

MAC Address Table: MAC Address Table

Table 4-6 MAC Address Table: Parameters

Parameter	Description
MAC Table as CSV File	Click on "Read from device" to download the current MAC address table from the device in CSV format.
Clear MAC Table	Click on "Clear" to clear the MAC address table.
MAC aging time	Enter the maximum time in seconds by that a device must report back again in order to remain in the table. The time can be between ten and 1000000 seconds (default: 40).

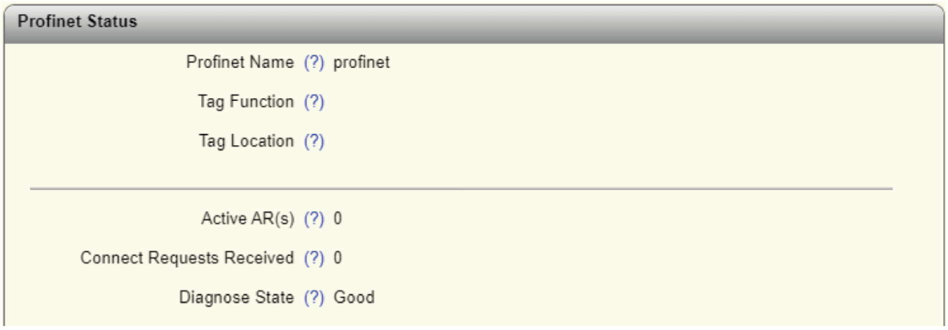
4.2.7 PROFINET Status

On this page, you will find an overview of the PROFINET status of the device.

The page is only displayed when PROFINET mode is active. The 20xx/21xx versions do not support PROFINET mode.

- Open web-based management (see "Accessing web-based management" on page 35) and log in.
- Click on "Information, PROFINET Status".

Figure 4-10 PROFINET Status



Profinet Status

Profinet Name (?) profinet

Tag Function (?)

Tag Location (?)

Active AR(s) (?) 0

Connect Requests Received (?) 0

Diagnose State (?) Good

Table 4-7 PROFINET Status: Parameters

Parameter	Description
Profinet Name	The assigned PROFINET device name is displayed here.
Tag Function	The text for the device function is displayed here. The text can be set via I&M1.
Tag Location	The text for the device location is displayed here. The text can be set via I&M1.
Active AR(s)	The number of active PROFINET I/O connections is displayed here.
Connect Requests Received	The number of connection requests received is displayed here.
Diagnose State	The current device status is displayed here.

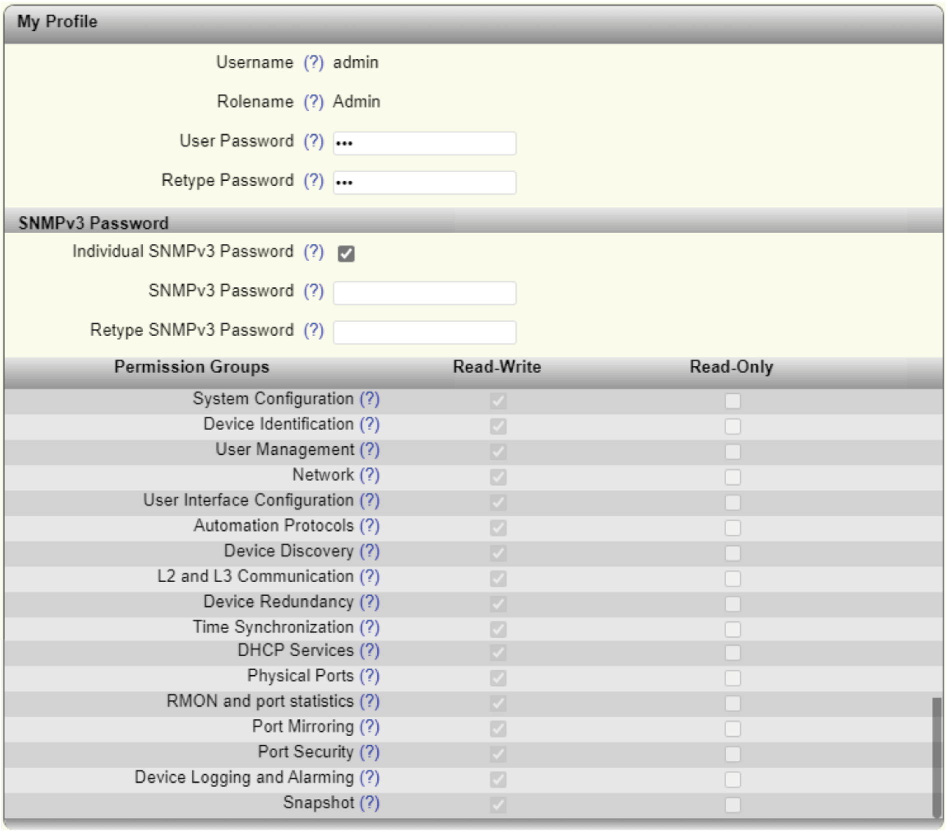
4.3 WBM Configuration area

4.3.1 My Profile

On the "My Profile" page, you will find an overview of the rights assigned to your user profile. As a logged-in user you can also change your password.

- Open web-based management (see "Accessing web-based management" on page 35) and log in.
- Click on "Configuration, My Profile".

Figure 4-11 My Profile



My Profile

Username (?) admin

Rolename (?) Admin

User Password (?) •••

Retype Password (?) •••

SNMPv3 Password

Individual SNMPv3 Password (?) ☑

SNMPv3 Password (?)

Retype SNMPv3 Password (?)

Permission Groups	Read-Write	Read-Only
System Configuration (?)	☑	□
Device Identification (?)	☑	□
User Management (?)	☑	□
Network (?)	☑	□
User Interface Configuration (?)	☑	□
Automation Protocols (?)	☑	□
Device Discovery (?)	☑	□
L2 and L3 Communication (?)	☑	□
Device Redundancy (?)	☑	□
Time Synchronization (?)	☑	□
DHCP Services (?)	☑	□
Physical Ports (?)	☑	□
RMON and port statistics (?)	☑	□
Port Mirroring (?)	☑	□
Port Security (?)	☑	□
Device Logging and Alarming (?)	☑	□
Snapshot (?)	☑	□

Table 4-8 My Profile: Parameters

Parameter	Description
Username	Your user name as the logged-in user is displayed here. You cannot change the name yourself.
Rolename	The role name your user is assigned to is displayed here.
User Password	Enter the desired password in the input field. The new password must be between eight and 64 characters long. Letters, numbers, and the following special characters are permitted: $%@&/\()=?![]{}+*-_<>#^.,:~l and space. For security reasons, your password is not displayed as plain text. ℹ Depending on your local password policy, your password may need to meet certain requirements.
Retype Password	Re-enter the new password. The new password will be activated after saving and logging out.

My Profile: SNMPv3 Password

Table 4-9 SNMPv3 Password: Parameters

Parameter	Description
Individual SNMPv3 Password	The “SNMPv3 Password” area is only available to the “admin” user account that was created in the factory default state. Activate the check box to assign an individual SNMPv3 password.
SNMPv3 Password	This option is only available if the check box next to “Individual SNMPv3 Password” has been activated. Enter the desired SNMPv3 password in the input field. The password must be between eight and 64 characters long. For security reasons, your password is not displayed as plain text. If you do not assign an SNMPv3 password, the password of the “admin” user account will be used. If you use this password, a user account with the name “snmpv3_user” will be created. The user is assigned read-only rights and **cannot** access the device via SNMPv3. If you delete the user account “snmpv3_user”, the “Individual SNMPv3 Password” option is deactivated.
Retype SNMPv3 Password	This option is only available if the check box next to “Individual SNMPv3 Password” has been activated. Re-enter the new password.

4.3.2 User Management

The “User Management” page allows you to create and manage user accounts. You can assign permissions to users via various user roles.

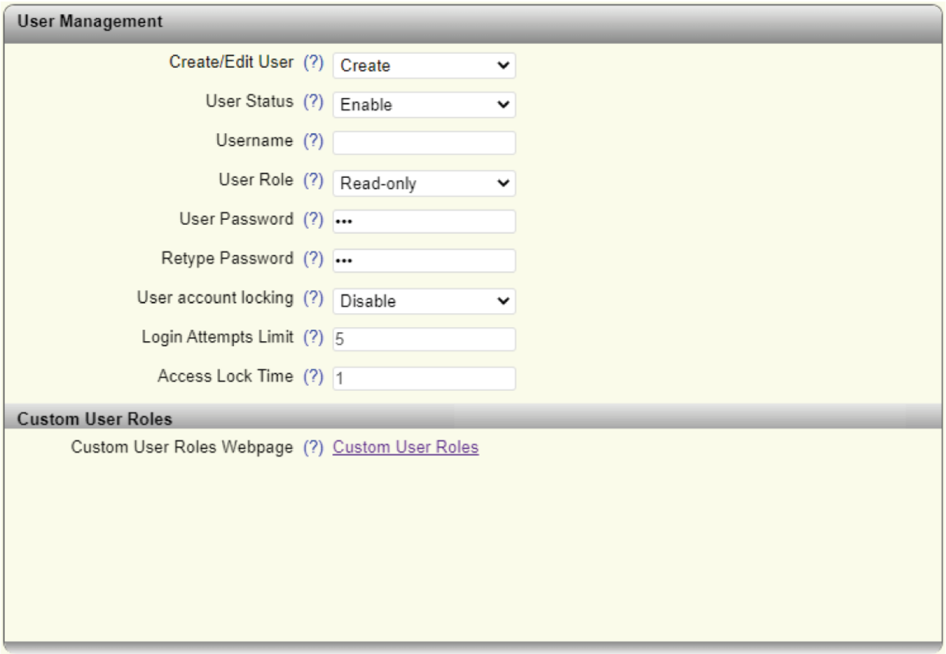
The device also provides the option of server-based user authentication via LDAP or RADIUS. Configure these settings on the “Security” webpage (see “Security” on page 80).

When a user logs in, the device always searches the local user accounts first. The server-based user authentication is only used if the user name is not available locally.

Up to ten users each can log in at the same time either via web-based management or CLI.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, User Management”.

Figure 4-12 User Management



User Management

Create/Edit User (?) Create

User Status (?) Enable

Username (?)

User Role (?) Read-only

User Password (?) •••

Retype Password (?) •••

User account locking (?) Disable

Login Attempts Limit (?) 5

Access Lock Time (?) 1

Custom User Roles

Custom User Roles Webpage (?) Custom User Roles

Table 4-10 User Management: Parameters

Parameter	Description
Create/Edit User	Select the user account that you wish to edit or delete. Select “Create” to create a new user account.
Delete	This option is only available if you selected an existing user account for “Create/Edit User”. Click on “Delete” to delete the currently selected user account. This action cannot be undone. The “admin” user account cannot be deleted.
User Status	Select whether the account is activated or deactivated. When the account is deactivated, access to the device is blocked, even if the correct login parameters are entered.
Username	Enter the desired user name in the text field. The user name can be up to 32 characters long. Letters, numbers, and the following special characters are permitted: -_.@.

Table 4-10 User Management: Parameters

Parameter	Description
User Role	From the drop-down list, select the desired role. The role determines the rights the account has in WBM. You can select the following roles in the factory default state: – Read-only: The user has read access to the device and therefore access to the webpages in the Information and Diagnostics areas. Furthermore, the user has permission to change their own access password. – Expert: The user has extensive read and write access to the device and can therefore modify a good portion of the configuration parameters. However, this excludes User Management. – Admin: The user has all administration rights. This includes unrestricted read and write access to the device. You can create further user roles, see “Custom User Roles” on page 49.
User Password	Enter the desired initial password in the text field. The password must be between eight and 64 characters long. Letters, numbers, and the following special characters are permitted: $%@&/\()=?![]{}+*-_<>#^.,:~| and space. The user can change the password later on.
Retype Password	Enter the initial password again.
User account locking	Select whether the account should be locked after failed login attempts. If a user repeatedly attempts to log in using the wrong password, access to the device can be blocked for a certain period of time.
Login Attempts Limit	This option is only available if you selected “Enable” for “User account locking”. Enter the desired number of login attempts until the account will be locked. The number must be between one and 100.
Access Lock Time	This option is only available if you selected “Enable” for “User account locking”. Enter the desired time in minutes that an account will remain locked for after failed login attempts. The time must be between one and 1440 minutes.
Custom User Roles Webpage	Click on “Custom User Roles” to open the “Custom User Roles” pop-up window. Here, you can define the desired permissions for each role (see “Custom User Roles” on page 49).

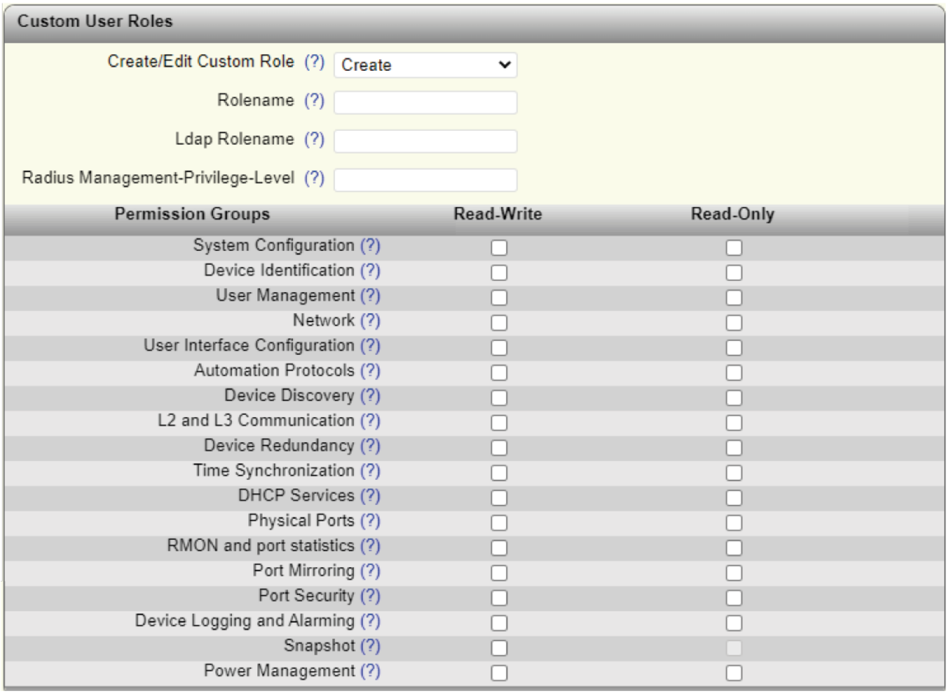
For further information on user roles and permissions, see “Creating user roles” on page 133.

4.3.3 Custom User Roles

On this page, you can create custom user roles and define the desired permissions for them.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, User Management, Custom User Roles”.

Figure 4-13 Custom User Roles



Custom User Roles

Create/Edit Custom Role (?) Create

Rolename (?)

Ldap Rolename (?)

Radius Management-Privilege-Level (?)

Permission Groups	Read-Write	Read-Only
System Configuration (?)	□	□
Device Identification (?)	□	□
User Management (?)	□	□
Network (?)	□	□
User Interface Configuration (?)	□	□
Automation Protocols (?)	□	□
Device Discovery (?)	□	□
L2 and L3 Communication (?)	□	□
Device Redundancy (?)	□	□
Time Synchronization (?)	□	□
DHCP Services (?)	□	□
Physical Ports (?)	□	□
RMON and port statistics (?)	□	□
Port Mirroring (?)	□	□
Port Security (?)	□	□
Device Logging and Alarming (?)	□	□
Snapshot (?)	□	□
Power Management (?)	□	□

Table 4-11 Custom User Roles: Parameters

Parameter	Description
Create/Edit Custom Role	Select the user account that you wish to edit or delete. Select “Create” to create a new user account.
Delete	Click on “Delete” to delete the currently selected role. This action cannot be undone. The preconfigured roles “Admin”, “Expert”, and “Read-only” cannot be deleted.
Rolename	Enter the desired name for the user role in the text field. The name for the user role can be up to 32 characters long. Letters, numbers, and the following special characters are permitted: -_.@. Once the role name has been created, it cannot be changed.

Table 4-11 Custom User Roles: Parameters

Parameter	Description
Ldap Rolename	The LDAP role name is made available to a user via the LDAP server. The role name is used to assign a user to a user role and therefore to assign rights on the device. The LDAP role name is mapped to a local user role here. For further information on LDAP, see "Security" on page 80.
Radius Management-Privilege-Level	Here, you can enter a numerical value that is made available to a user via the RADIUS server during server-based authentication. This value is used to assign a user to a user role and therefore to assign rights on the device. The management privilege level is mapped to a local user role here. For further information on RADIUS, see "RADIUS certificates" on page 167.
Permission Groups	In the table, you can assign and edit the read and write permissions for user-defined user roles. The predefined permissions of the "Admin", "Expert", and "Read-only" roles available by default cannot be changed. – Read-Write: Activate the respective check box to assign read and write permissions for the function group to the selected user role. – Read-Only: Activate the respective check box to assign read permissions for the respective function group to the selected user role. – No selection: If you do not select either of the two check boxes for a function group, the user role will not be assigned permission for this function group.

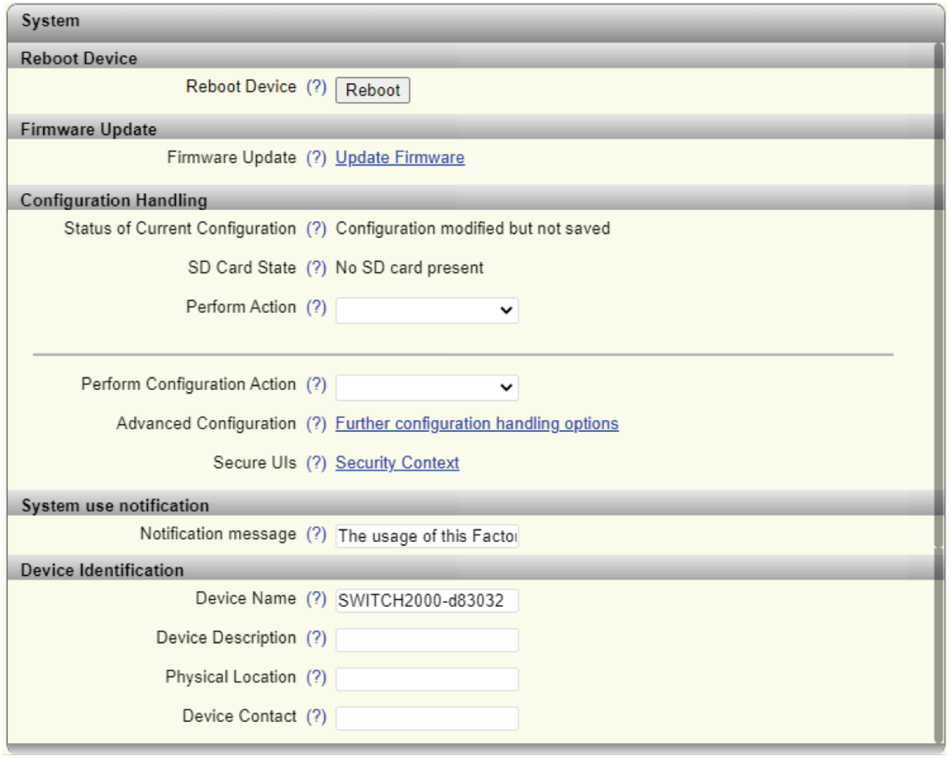
For further information on user roles and permissions, see "Creating user roles" on page 133.

4.3.4 System

On this page, you can make basic system settings such as firmware updates or renaming the device.

- Open web-based management (see "Accessing web-based management" on page 35) and log in.
- Click on "Configuration, System".

Figure 4-14 System


System

Reboot Device

Reboot Device (?) Reboot

Firmware Update

Firmware Update (?) Update Firmware

Configuration Handling

Status of Current Configuration (?) Configuration modified but not saved

SD Card State (?) No SD card present

Perform Action (?)

Perform Configuration Action (?)

Advanced Configuration (?) Further configuration handling options

Secure UIs (?) Security Context

System use notification

Notification message (?) The usage of this Factoı

Device Identification

Device Name (?) SWITCH2000-d83032

Device Description (?)

Physical Location (?)

Device Contact (?)

System: Reboot Device

Table 4-12 Reboot Device: Parameters

Parameter	Description
Reboot Device	Click on “Reboot” to restart the device. All unsaved parameters will be lost. ℹ The connection to the device is interrupted for the boot phase.

System: Firmware Update

Table 4-13 Firmware Update: Parameters

Parameter	Description
Firmware Update	Click on “Update Firmware” to perform a firmware update. For additional information, refer to “Firmware update” on page 127.

System: Configuration Handling

Table 4-14 Configuration Handling: Parameters

Parameter	Description
Status of Current Configuration	The status of the active configuration is displayed here. – Configuration saved: The active configuration is saved to the device. – Configuration modified but not saved: The active configuration has been changed, but not yet saved to the device. Click on “Apply&Save” to save the configuration to the device.
SD Card State	This shows whether an SD card is inserted. ℹ You need to reload the page to see the current status. ℹ You can only use FAT-formatted SD cards.
Perform Action	Select the action to be performed. – Compare: The action compares the configuration file on the SD card with the one on the device. You are shown whether the configuration on the SD card is identical or different, or whether there is no configuration. – Clear: The action deletes the configuration file on the SD card.
Perform Configuration Action	In the drop-down list, select an option. – Factory Default: The action resets the device configuration to the default settings. – Save Configuration: The action saves the active configuration to the device. The settings made are retained after a voltage reset. – Reload Configuration: The action loads the most recently saved configuration and applies it. The configuration might have been saved using “Save Configuration” or the “Apply&Save” button.
Advanced Configuration	Click on “Further configuration handling options” to open the “File Transfer” pop-up window (see “File Transfer” on page 129).
Secure UIs	Click on “Certificate Management” to open the “Certificate Management” pop-up window (see “Pop-up window: Certificate Management” on page 85).

System: System use notification

Table 4-15 System use notification: Parameters

Parameter	Description
Notification message	Enter the desired text to be displayed prior to login. The text is freely editable and can be up to 256 characters long.

System: Device Identification

Table 4-16 Device Identification: Parameters

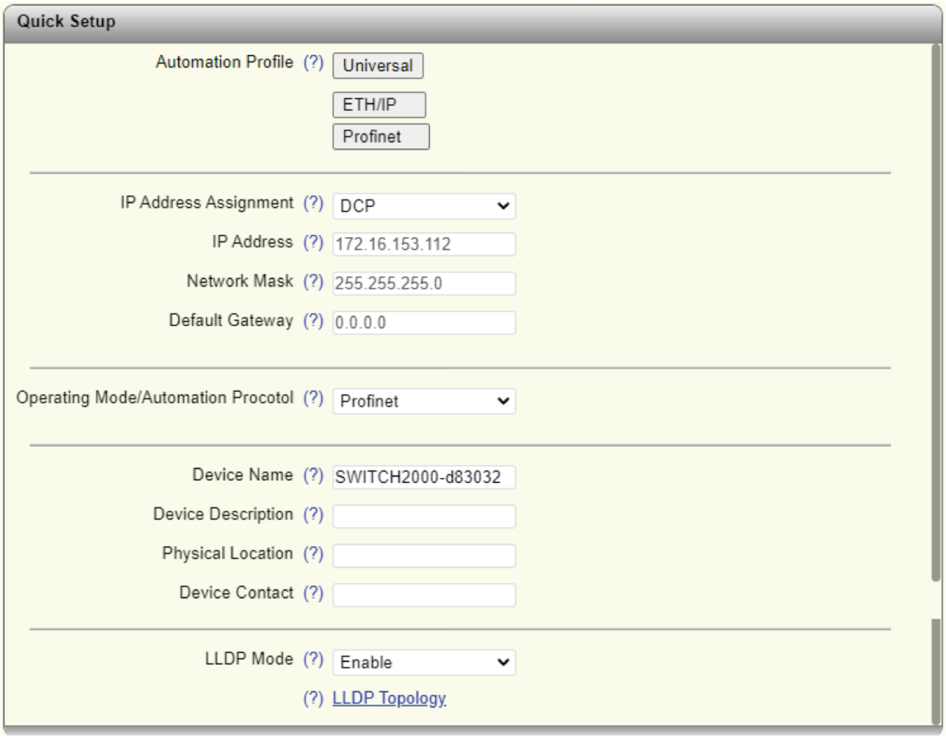
Parameter	Description
Device Name	Enter the desired device name. In the factory default state, the device name corresponds to the device host name.
Device Description	Optionally, enter a device description.
Physical Location	Optionally, enter the location of the device, such as the building in which it is installed.
Device Contact	Optionally, enter a contact address for the device.

4.3.5 Quick Setup

The “Quick Setup” page allows you to quickly configure the minimum requirements of a network. A wizard will guide you through the individual steps.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, Quick Setup”.

Figure 4-15 Quick Setup



Quick Setup

Automation Profile (?) Universal | ETH/IP | Profinet

IP Address Assignment (?) DCP

IP Address (?) 172.16.153.112

Network Mask (?) 255.255.255.0

Default Gateway (?) 0.0.0.0

Operating Mode/Automation Procotol (?) Profinet

Device Name (?) SWITCH2000-d83032

Device Description (?)

Physical Location (?)

Device Contact (?)

LLDP Mode (?) Enable

(?) LLDP Topology

Table 4-17 Quick Setup: Parameters

Parameter	Description
Automation Profile	Select a profile that is optimized for the desired operating mode. – Universal: In Universal mode, the automation protocols (PN device) are deactivated and BootP is activated for IP address assignment. – ETH/IP: In EtherNet/IP mode, IGMP snooping, IGMP querier (version 2), the “EtherNet/IP” Quality of Service profile, and address conflict detection (ACD) are activated. – PROFINET: In PROFINET mode, LLDP, the PROFINET device, DCP for IP address assignment, and the “PROFINET” Quality of Service profile are activated. ℹ The “PROFINET” automation profile is not available on 20xx/21xx versions. ℹ If you activate an automation profile from within WBM, it only has an effect on the functions that are relevant for this mode. Any other configurations stored on the device are retained and are not deleted. If, on the other hand, you make changes using the Smart mode button, all configurations are affected (see “Using Smart mode” on page 22).
IP Address Assignment	Select the type of IP address assignment. – STATIC: Static IP address – BOOTP: Assignment via the Bootstrap protocol – DHCP: Assignment via a DHCP server – DCP: Assignment via the PROFINET engineering tool or controller (not possible on the 20xx/21xx versions)
IP Address	This option is only available if you selected “STATIC” for “IP Address Assignment”. Enter the desired IP address.
Network Mask	This option is only available if you selected “STATIC” for “IP Address Assignment”. Enter the desired subnet mask.
Default Gateway	This option is only available if you selected “STATIC” for “IP Address Assignment”. Enter the default gateway.

Table 4-17 Quick Setup: Parameters

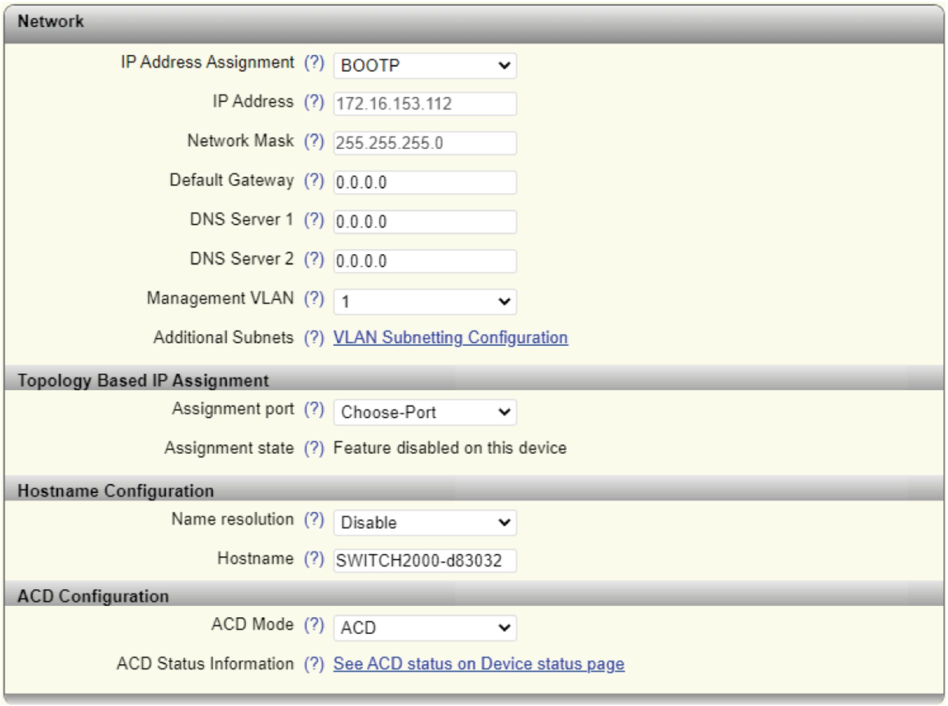
Parameter	Description
Operating Mode/Automation Protocol	Select the device operating mode. – None: BootP for IP address assignment is activated. The Quality of Service profile is set to "Universal". – Profinet: The "Topology based IP assignment" function is deactivated. LLDP is activated. DCP for IP address assignment is activated. The Quality of Service profile is set to "Profinet". If the device supports ACD, ACD is deactivated. The configuration is saved before the device is restarted.
Device Name	Enter the desired device name. In the factory default state, the device name corresponds to the device host name.
Device Description	Optionally, enter a device description.
Physical Location	Optionally, enter the location of the device, such as the building in which it is installed.
Device Contact	Optionally, enter a contact address for the device.

4.3.6 Network

On this page, you can make the basic network settings.

- Open web-based management (see "Accessing web-based management" on page 35) and log in.
- Click on "Configuration, Network".

Figure 4-16 Network



Network

IP Address Assignment (?) BOOTP

IP Address (?) 172.16.153.112

Network Mask (?) 255.255.255.0

Default Gateway (?) 0.0.0.0

DNS Server 1 (?) 0.0.0.0

DNS Server 2 (?) 0.0.0.0

Management VLAN (?) 1

Additional Subnets (?) VLAN Subnetting Configuration

Topology Based IP Assignment

Assignment port (?) Choose-Port

Assignment state (?) Feature disabled on this device

Hostname Configuration

Name resolution (?) Disable

Hostname (?) SWITCH2000-d83032

ACD Configuration

ACD Mode (?) ACD

ACD Status Information (?) See ACD status on Device status page

Table 4-18 Network: Parameters

Parameter	Description
IP Address Assignment	Select the type of IP address assignment. – STATIC: Static IP address – BOOTP: Assignment via the Bootstrap protocol – DHCP: Assignment via a DHCP server – DCP: Assignment via the PROFINET engineering tool or controller (not possible on the 20xx/21xx versions) For further information on IP address assignment, refer to “Assigning the IP address” on page 25.
IP Address	This option is only available if you selected “STATIC” for “IP Address Assignment”. Enter the desired IP address.
Network Mask	This option is only available if you selected “STATIC” for “IP Address Assignment”. Enter the desired subnet mask.
Default Gateway	This option is only available if you selected “STATIC” for “IP Address Assignment”. Enter the default gateway.
DNS Server 1	Here, enter the IP address of the primary DNS server.
DNS Server 2	Here, enter the IP address of the secondary DNS server.

Table 4-18 Network: Parameters

Parameter	Description
Management VLAN	Select the VLAN in which web-based management is to be accessible. The value “1” is set by default. You can set up further management VLANs via CLI. However, it is recommended that you keep management VLAN 1.
DHCP Configuration	This option is only available if you selected “STATIC” for “IP Address Assignment”. Click on “DHCP Services” to open the “DHCP Service” page (see “DHCP Service” on page 92).
Additional Subnets	Click on “VLAN Subnetting Configuration” to open the “VLAN Subnet” window (see “VLAN Subnet” on page 163).

Network: Topology Based IP Assignment

This section is only available if PROFINET has been deactivated.

Table 4-19 Topology Based IP Assignment: Parameters

Parameter	Description
Assignment port	Select the port on which the function is to be activated. This configuration step only needs to be implemented on the root device. As soon as a port is selected, the “Accept BootP” option is automatically deactivated in the DHCP server configuration.
Assignment state	The current status of the topology-based IP address assignment is displayed here. If the function is active, the status shows whether the selected device is a root device or a client that was assigned an IP address via another device. For the root device, the active port is also displayed.

For further information on topology-based IP address assignment, refer to Section “Topology-based IP assignment” on page 157.

Network: Hostname Configuration

Table 4-20 Hostname Configuration: Parameters

Parameter	Description
Name resolution	Select whether you want to activate DNS name resolution via mDNS and LLMNR. If you activate the function, you can also access the device via the host name (e.g., http://switch2000-dd5d5c.local/).
Hostname	Here, enter the host name of your device. The host name must be between two and 63 characters long. Alphanumeric characters and dashes are permitted. A host name must not start with a dash. In the factory default configuration, this host name is made up of the product family name and part of the device MAC address (see "DNS host name" on page 18).

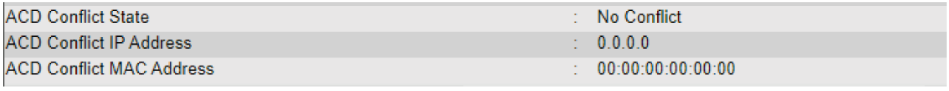
When you deactivate DNS name resolution, it may take some time until the device can be accessed via the host name. This is due to the DNS cache.

Network: ACD Configuration

Table 4-21 ACD Configuration: Parameters

Parameter	Description
ACD Mode	Here, activate or deactivate the "Address Conflict Detection" function.
ACD Status Information	Click on "See ACD status on Device status page" to open the "Device Status" page (see "Device Status" on page 39).

Figure 4-17 ACD status information on the "Device Status" page



ACD Conflict State	:	No Conflict
ACD Conflict IP Address	:	0.0.0.0
ACD Conflict MAC Address	:	00:00:00:00:00:00

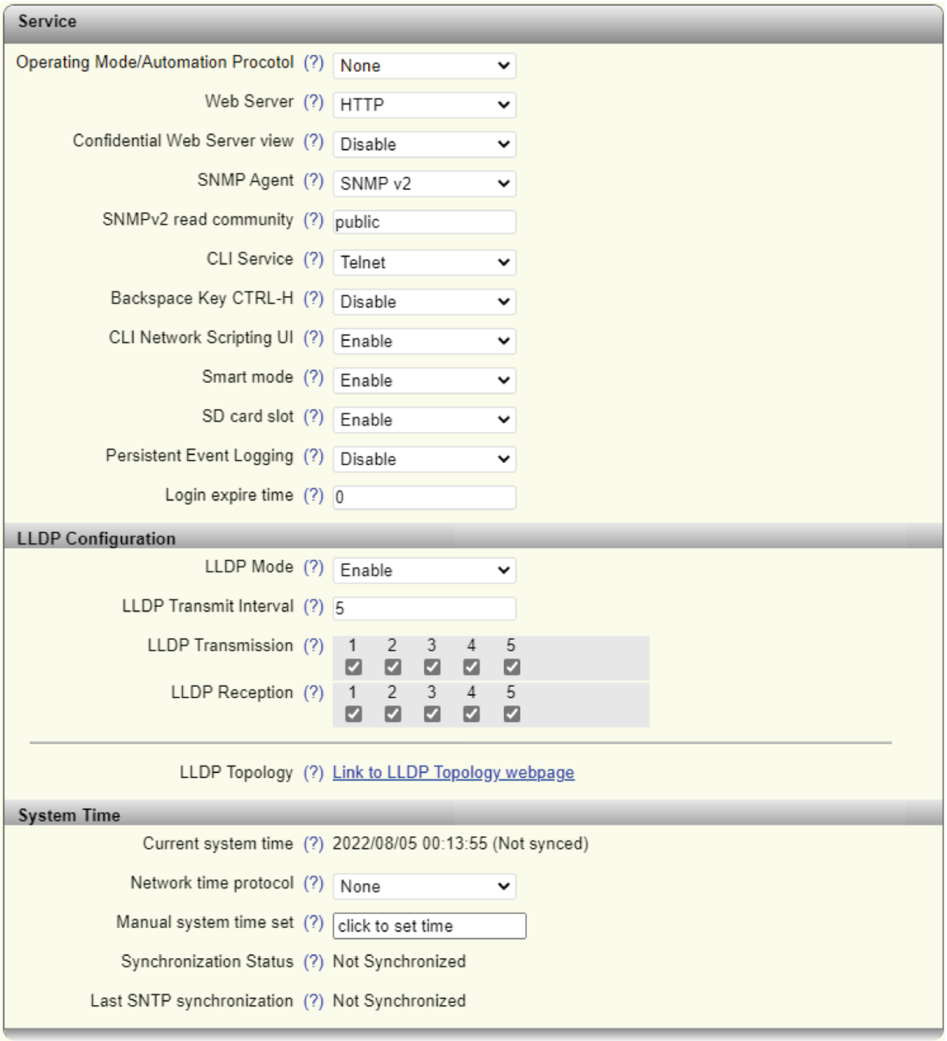
4.3.7 Service

On the "Service" page, you can activate and deactivate various interfaces and displays, for example, the CLI service, the LEDs, or the SNMP agent.

NOTE: Threat to network security
Deactivate unused interfaces to prevent unauthorized access.

- Open web-based management (see "Accessing web-based management" on page 35) and log in.
- Click on "Configuration, Service".

Figure 4-18 Service



Service

Operating Mode/Automation Procotol (?) None

Web Server (?) HTTP

Confidential Web Server view (?) Disable

SNMP Agent (?) SNMP v2

SNMPv2 read community (?) public

CLI Service (?) Telnet

Backspace Key CTRL-H (?) Disable

CLI Network Scripting UI (?) Enable

Smart mode (?) Enable

SD card slot (?) Enable

Persistent Event Logging (?) Disable

Login expire time (?) 0

LLDP Configuration

LLDP Mode (?) Enable

LLDP Transmit Interval (?) 5

		1	2	3	4	5
LLDP Transmission	(?)	☑	☑	☑	☑	☑
LLDP Reception	(?)	☑	☑	☑	☑	☑

LLDP Topology (?) Link to LLDP Topology webpage

System Time

Current system time (?) 2022/08/05 00:13:55 (Not synced)

Network time protocol (?) None

Manual system time set (?) click to set time

Synchronization Status (?) Not Synchronized

Last SNTP synchronization (?) Not Synchronized

Table 4-22 Service: Parameters

Parameter	Description
Operating Mode/Automation Protocol	Select the device operating mode. – None: BootP for IP address assignment is activated. The Quality of Service profile is set to “Universal”. – Profinet: The “Topology based IP assignment” function is deactivated. LLDP is activated. DCP for IP address assignment is activated. The Quality of Service profile is set to “Profinet”. If the device supports ACD, ACD is deactivated. The configuration is saved before the device is restarted.
Web Server	Select whether the web server functionality should be activated. – Disable: The web server is deactivated. Access to web-based management is deactivated. – HTTP: The web server is activated in “HTTP” mode. The connection is not secured. – HTTPS: The web server is activated in “HTTPS” mode. Use “https://” to access web-based management. The connection is secured. If you deactivate the web server, web-based management can no longer be accessed.
Confidential Web Server view	Here, select whether the “Information” area in web-based management should be visible without login. – Disable: The “Information” area of web-based management is visible without login data. Access to other areas is controlled using user roles (see “User Management” on page 46). – Enable: Web-based management is only visible with previous login.
SNMP Agent	Here, select the SNMP server functionality (see “SNMP – Simple Network Management Protocol” on page 149). – Disabled: The SNMP server is deactivated. – SNMP v2: The SNMP server is activated in “SNMP v2” mode. SNMP v1 is also supported in this mode. – SNMP v3: The SNMP server is activated in “SNMP v3” mode. **NOTE: Threat to network security** SNMPv2 is not a secure encryption method.
SNMPv2 read community	This option is only available if you selected “SNMP v2” for “SNMP Agent”. Here, enter the string for the SNMPv2 read community. This password must be entered for read access to objects.

Table 4-22 Service: Parameters

Parameter	Description
SNMPv3 Authentication	This option is only available if you selected „SNMP v3“ for „SNMP Agent“. Here, select the authentication mode for SNMP v3. The first part of the selection (MD5 or SHA) is the authentification protocol based on hash numbers. The second part (DES or AES) is the encryption protocol. – MD5/DES: Default – SHA/AES – SHA/DES – MD5/AES For the AES protocol, only AES-128 is supported.
CLI Service	Here, select whether entry of CLI commands via Telnet or Secure Shell should be activated. – Disable: Entry of CLI commands is deactivated. – Telnet: Entry of CLI commands via Telnet is activated. – SSH: Entry of CLI commands via Secure Shell (SSH) is activated. For information about configuration and diagnostics via the Command Line Interface (CLI), refer to the separate manual at phoenixcontact.net/qr/<item_number>.
Backspace Key CTRL-H	Select whether the key combination Ctrl+H should additionally be used as a backspace function. Some terminal programs use the backspace key as Delete. If you activate this option, you can instead use the key combination Ctrl+H in your terminal program to delete the last character.
CLI Network Scripting UI	– Disable: Transmission of CLI commands via the network is deactivated. – Enable: Transmission of CLI commands via the network is activated.
Smart mode	Select whether the Smart mode button should be activated. **NOTE: Access no longer possible** If you deactivate the Smart mode button and the SD card slot, and access is no longer possible via the Ethernet ports (e.g., due to incorrect configuration or forgotten access data), it is no longer possible to reset the device. The device must then be sent in to be reset by the manufacturer – this is subject to a fee. If the SD card slot is disabled, you can also no longer access MRP manager licenses (MRM).

Table 4-22 Service: Parameters

Parameter	Description
SD card slot	Select whether the SD card slot should be activated. ⓘ **NOTE: Access no longer possible** If you deactivate the Smart mode button and the SD card slot, and access is no longer possible via the Ethernet ports (e.g., due to incorrect configuration or forgotten access data), it is no longer possible to reset the device. The device must then be sent in to be reset by the manufacturer – this is subject to a fee. If the SD card slot is disabled, you can also no longer access MRP manager licenses (MRM).
Persistent Event Logging	Here, select whether the persistent storage of events should be activated. Persistent storage means that events are not deleted when the device is restarted.
Login expire time	Here, enter the time until automatic logout. You can set a number between 30 and 3600 seconds. The default is 1200 seconds. If you set a value of “0”, automatic logout is deactivated.

Service: LLDP Configuration

For further information on LLDP, refer to Section “LLDP – Link Layer Discovery Protocol” on page 153.

Service: System Time

Table 4-23 Service: Parameters

Parameter	Description
Current system time	The current system time is displayed here. “Not synced” means that the system time has either been configured manually or it is not synchronized with an (S)NTP server. The device does not have a battery-backed real-time clock. If the time is not synchronized, there may be discrepancies between the system time and the actual time.
Network time protocol	Here, select a protocol for synchronizing the time via a web server. – None: No synchronization via a web server. You can set the time manually. – Unicast: For this option you must configure at least an SNTP server. – Broadcast: With this option, the device eavesdrops on all broadcasts by broadcast SNTP servers.
Manual system time set	This option is only available if you selected “None” for “Network time protocol”. Select “click to set time” to set the device system time manually. You can set the current date and the current time. ℹ The switch does not have a battery-backed real-time clock. If the time is entered manually, the time may deviate after the device is restarted.
Primary SNTP server	This option is only available if you selected “Unicast” for “Network time protocol”. Here, enter the IP address of your SNTP server. SNTP stands for Simple Network Time Protocol and is a time synchronization protocol used to synchronize the system time in networks.
Primary server description	This option is only available if you selected “Unicast” for “Network time protocol”. Here, enter a description of your SNTP server.
Secondary SNTP server	This option is only available if you selected “Unicast” for “Network time protocol”. Here, enter the IP address of your secondary SNTP server. SNTP stands for Simple Network Time Protocol and is a time synchronization protocol used to synchronize the system time in networks. If the primary server is not accessible, the secondary SNTP server will be used.
Secondary server description	This option is only available if you selected “Unicast” for “Network time protocol”. Here, enter a description of your secondary SNTP server.

Table 4-23 Service: Parameters

Parameter	Description
UTC offset	This option is only available if you selected “Unicast” or “Broadcast” for “Network time protocol”. Here, select the difference between the coordinated world time (UTC) and your time zone.
Synchronization Status	The current status of synchronization with the SNTP server is displayed here.
Last SNTP synchronization	The time of the last synchronization with the SNTP server is displayed here.

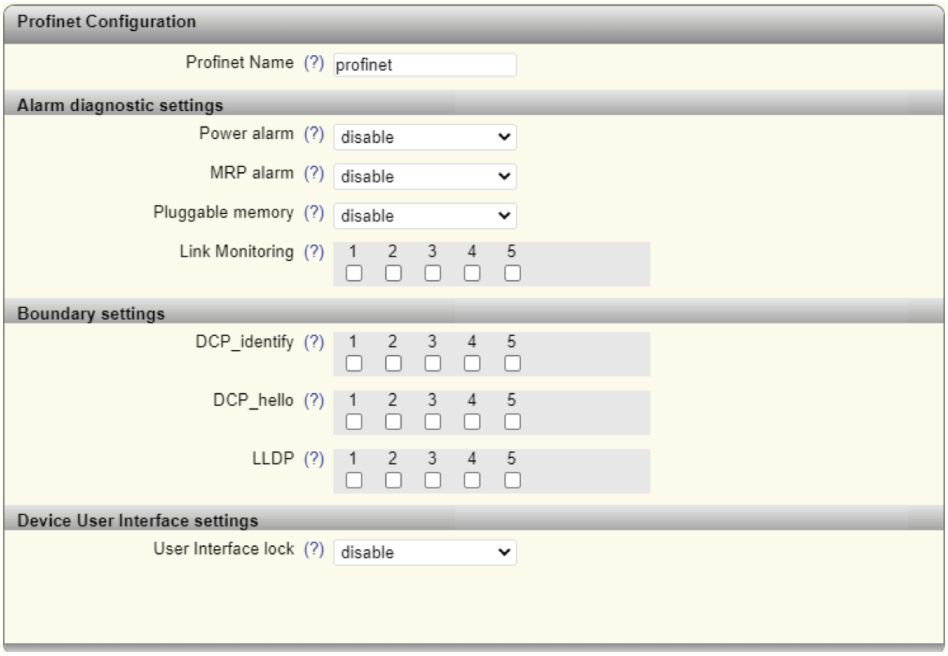
4.3.8 PROFINET Configuration

On this page, you can configure PROFINET.

The “PROFINET Configuration” page is only displayed when PROFINET mode is active (see “Service” on page 58). The 20xx/21xx versions do not support PROFINET mode.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, PROFINET Configuration”.

Figure 4-19 PROFINET Configuration



Profinet Configuration

Profinet Name (?) profinet

Alarm diagnostic settings

Power alarm (?) disable

MRP alarm (?) disable

Pluggable memory (?) disable

Link Monitoring (?) 1 □ 2 □ 3 □ 4 □ 5 □

Boundary settings

DCP_identify (?) 1 □ 2 □ 3 □ 4 □ 5 □

DCP_hello (?) 1 □ 2 □ 3 □ 4 □ 5 □

LLDP (?) 1 □ 2 □ 3 □ 4 □ 5 □

Device User Interface settings

User Interface lock (?) disable

Table 4-24 PROFINET Configuration: Parameters

Parameter	Description
Profinet Name	Here, enter the desired name for your PROFINET device.

PROFINET Configuration: Alarm diagnostic settings

Table 4-25 Alarm diagnostic settings: Parameters

Parameter	Description
Power alarm	Select whether the PROFINET alarm should be activated in the event of no power supply.
MRP alarm	Select whether the PROFINET alarm should be activated for MRP ring errors.
Pluggable memory	Select whether the PROFINET alarm should be activated in the event of no configuration memory (SD card).
Link Monitoring	Here, activate or deactivate the port-specific PROFINET alarm for link monitoring (link down behavior).
SFP module	This option is only available for devices with SFP or combo ports. Here, activate or deactivate the port-specific PROFINET alarm for a missing SFP module.

PROFINET Configuration: Boundary settings

Table 4-26 Boundary settings: Parameters

Parameter	Description
DCP_identify	Here, activate port-specific forwarding of DCP identify packets. ℹ If you check a check box, the forwarding of DCP identify packets will be deactivated.
DCP_hello	Here, activate port-specific forwarding of DCP hello packets. ℹ If you check a check box, the forwarding of DCP hello packets will be deactivated.
LLDP	Here, activate port-specific forwarding of LLDP packets. ℹ If you check a check box, the forwarding of LLDP packets will be deactivated.

PROFINET Configuration: Device User Interface settings

Table 4-27 Device User Interface settings: Parameters

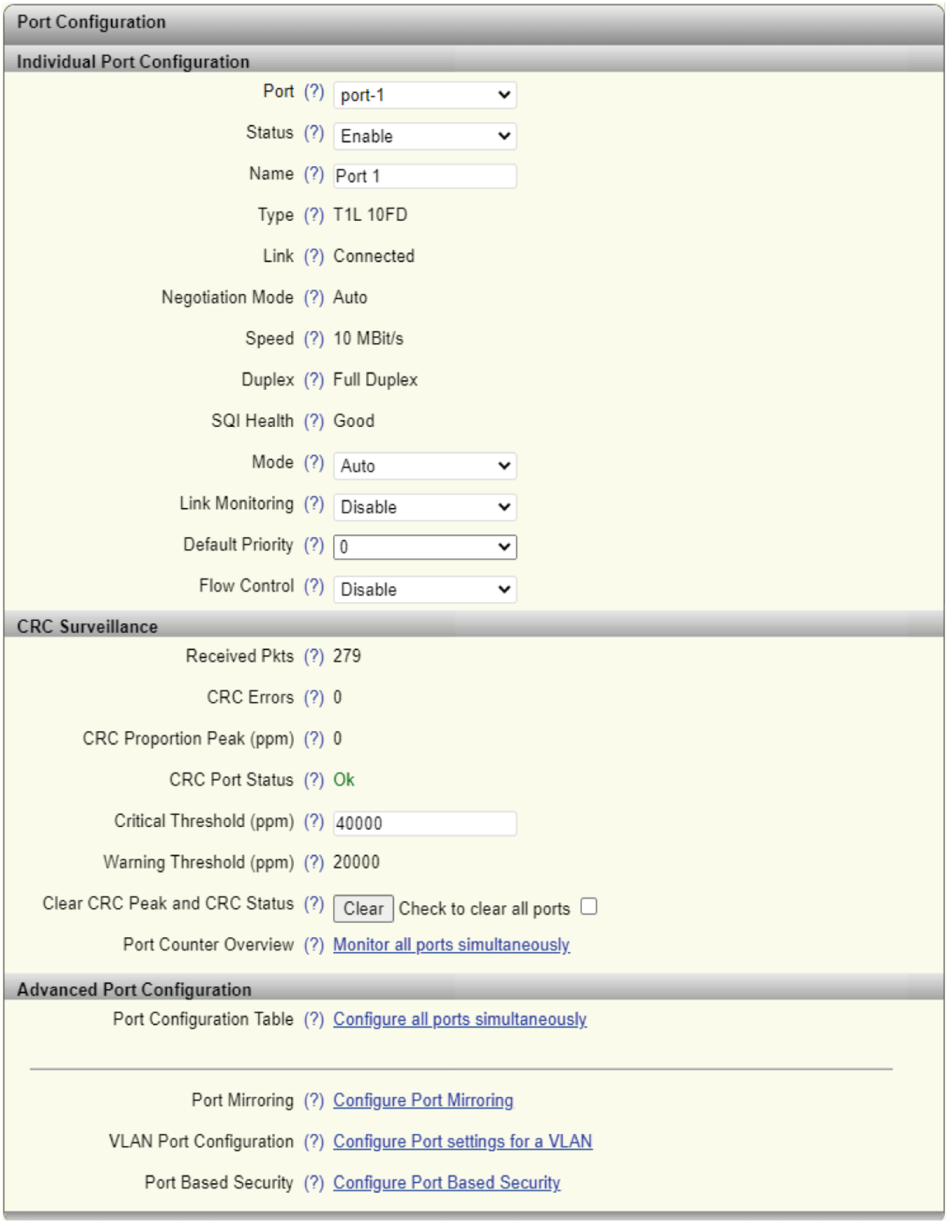
Parameter	Description
User Interface lock	Select whether all device functions and parameters (including this one) that can be set via PROFINET I/O are blocked for configuration in web-based management during an active PROFINET connection (AR).

4.3.9 Port Configuration

On this page, you can individually configure the individual ports.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, Port Configuration”.

Figure 4-20 Port Configuration



Port Configuration

Individual Port Configuration

Port	(?)	port-1
Status	(?)	Enable
Name	(?)	Port 1
Type	(?)	T1L 10FD
Link	(?)	Connected
Negotiation Mode	(?)	Auto
Speed	(?)	10 MBit/s
Duplex	(?)	Full Duplex
SQI Health	(?)	Good
Mode	(?)	Auto
Link Monitoring	(?)	Disable
Default Priority	(?)	0
Flow Control	(?)	Disable

CRC Surveillance

Received Pkts	(?)	279
CRC Errors	(?)	0
CRC Proportion Peak (ppm)	(?)	0
CRC Port Status	(?)	Ok
Critical Threshold (ppm)	(?)	40000
Warning Threshold (ppm)	(?)	20000
Clear CRC Peak and CRC Status	(?)	Clear Check to clear all ports □
Port Counter Overview	(?)	Monitor all ports simultaneously

Advanced Port Configuration

Port Configuration Table	(?)	Configure all ports simultaneously
Port Mirroring	(?)	Configure Port Mirroring
VLAN Port Configuration	(?)	Configure Port settings for a VLAN
Port Based Security	(?)	Configure Port Based Security

Port Configuration: Individual Port Configuration

Table 4-28 Individual Port Configuration: Parameters

Parameter	Description
Port	Select the port that you want to configure individually.
Status	Select whether the port should be activated or deactivated.
Name	Optionally, assign an individual name to the port.
Type	The physical properties of the port are displayed here.
Link	The current port link status is displayed here.
Negotiation Mode	The current auto negotiation status is displayed here.
Speed	The current transmission speed at which the port is operating is displayed here.
Duplex	The port transmission mode is displayed here.
SQI Health	This option is only available on the SPE versions. The signal quality of the SPE ports is displayed here.
Mode	Select the transmission speed and mode for the port. You can also select Fast Startup here. – Auto: The transmission speed and mode are selected automatically. – 10 Mbps Half Duplex: The port transmits at a speed of 10 Mbps in half-duplex mode. – 10 Mbps Full Duplex: The port transmits at a speed of 10 Mbps in full-duplex mode. – 100 Mbps Half Duplex: The port transmits at a speed of 100 Mbps in half-duplex mode. – 100 Mbps Full Duplex: The port transmits at a speed of 100 Mbps in full-duplex mode. – Fast Startup: Select this mode if you wish to connect special PROFINET devices (FSU devices) or EtherNet/IP devices (Quick Connect) to the switch. The switch can then be accessed at the same speed. ℹ If you use the “Fast Startup” function for fast link establishment, RSTP is automatically deactivated on this port (see “Network Redundancy” on page 74).

Table 4-28 Individual Port Configuration: Parameters

Parameter	Description
Link Monitoring	Select whether the link behavior at the selected port is to be monitored. An alarm message is then generated under “Alarm&Events”. If the link drops, you receive an alarm message on the alarm output (22xx/23xx versions) or signal contact (24xx/25xx versions). Some versions (e.g., 26xx/27xx) do not feature an alarm output or signal contact. For these versions, the alarm is solely signaled via the FAIL LED. You can also make this setting under “Configuration, Local Events”. Activate the “Monitored Link Down” check box for this (see “Local Events: Alarm Output 1” on page 98).
Default Priority	Select the priority for incoming data packets at this port. The lower the value, the higher the priority.
Jumbo Frames	This option is only available for 21xx/23xx/25xx/27xx Gigabit versions. Select whether jumbo frames (>1518 bytes) should be supported. If you activate this option, the MTU size is set to 9600 bytes.
MTU	Here, select the maximum transmission unit (MTU). Packet sizes between 1522 bytes and 9600 bytes are activated.
Flow Control	Select whether flow control should be activated for the selected port. The switch and its neighboring device can then send a pause frame to the switch to prevent packet loss due to overload. The pause frame receiver then pauses transmission. For time-critical automation scenarios, this option should be deactivated.

Port Configuration: CRC Surveillance

Table 4-29 CRC Surveillance: Parameters

Parameter	Description
Received Pkts	The number of packets received at the selected port since the last reboot or counter reset is displayed here.
CRC Errors	The number of CRC errors at the selected port since the last reboot or counter reset is displayed here.
CRC Proportion Peak (ppm)	The highest proportion of CRC errors relative to the total number of packets received in an interval since the last reboot or counter reset is displayed here. The interval is 30 seconds.
CRC Port Status	The status of the current port is displayed here.

Table 4-29 CRC Surveillance: Parameters

Parameter	Description
Critical Threshold (ppm)	Enter the threshold value at which the CRC Port Status switches to Critical. Enter a value between 1000 ppm and 1000000 ppm.
Warning Threshold (ppm)	The threshold value in ppm at which the CRC Port Status switches to “Warning” (50% of Critical Threshold) is displayed here.
Clear CRC Peak and CRC Status	Click on “Clear” to reset the CRC Proportion Peak and the CRC Port Status. Additionally, check the “Check to clear all ports” check box and click on “Clear” to reset the values for all ports.
Port Counter Overview	Click on “Monitor all ports simultaneously” to open the “Port Counter” page (see “Port Counter” on page 109).

Port Configuration: Advanced Port Configuration

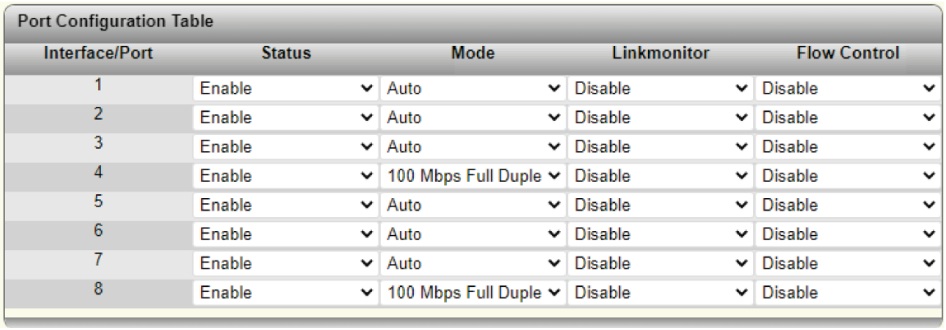
Table 4-30 Advanced Port Configuration: Parameters

Parameter	Description
Port Configuration Table	Click on “Configure all ports simultaneously” to open the “Port Configuration Table” page (see “Pop-up window: Port Configuration Table” on page 69).
Port Mirroring	Click on “Configure Port Mirroring” to open the “Port Mirroring” page (see “Port Mirroring” on page 106).
VLAN Port Configuration	Click on “Configure Port settings for a VLAN” to open the “VLAN Port configuration” page (see “Pop-up window: VLAN Port Configuration” on page 161).
Link Aggregation	Click on “Configure Link Aggregation” to open the “Link Aggregation” page (see “LACP – Link Aggregation Control Protocol” on page 145).
Port Based Security	Click on “Configure Port Based Security” to open the “Port Based Security” page (see “Pop-up window: Port Based Security” on page 85).

Pop-up window: Port Configuration Table

On this page, you can configure the port in a tabular format.

Figure 4-21 Pop-up window: Port Configuration Table



Port Configuration Table

Interface/Port	Status	Mode	Linkmonitor	Flow Control
1	Enable	Auto	Disable	Disable
2	Enable	Auto	Disable	Disable
3	Enable	Auto	Disable	Disable
4	Enable	100 Mbps Full Duple	Disable	Disable
5	Enable	Auto	Disable	Disable
6	Enable	Auto	Disable	Disable
7	Enable	Auto	Disable	Disable
8	Enable	100 Mbps Full Duple	Disable	Disable

Table 4-31 Pop-up window: Port Configuration Table: Parameters

Parameter	Description
Interface/Port	This column shows the port for which you can make settings.
Status	Select whether the port should be activated or deactivated.

Table 4-31 Pop-up window: Port Configuration Table: Parameters

Parameter	Description
Mode	Select the transmission speed and mode for the port. You can also select Fast Startup here. – Auto: The transmission speed and mode are selected automatically. – 10 Mbps Half Duplex: The port transmits at a speed of 10 Mbps in half-duplex mode. – 10 Mbps Full Duplex: The port transmits at a speed of 10 Mbps in full-duplex mode. – 100 Mbps Half Duplex: The port transmits at a speed of 100 Mbps in half-duplex mode. – 100 Mbps Full Duplex: The port transmits at a speed of 100 Mbps in full-duplex mode. – Fast Startup: Select this mode if you wish to connect special PROFINET devices (FSU devices) or EtherNet/IP devices (Quick Connect) to the switch. The switch can then be accessed at the same speed. ℹ If you use the “Fast Startup” function for fast link establishment, RSTP is automatically deactivated on this port (see “Network Redundancy” on page 74).
Linkmonitor	Select whether the link behavior at the selected port is to be monitored. An alarm message is then generated under “Alarm&Events”. If the link drops, you receive an alarm message on the alarm output (22xx/23xx versions) or signal contact (24xx/25xx versions). Some versions (e.g., 26xx/27xx) do not feature an alarm output or signal contact. For these versions, the alarm is solely signaled via the FAIL LED. ℹ You can also make this setting under “Configuration, Local Events”. Activate the “Monitored Link Down” check box for this (see “Local Events: Alarm Output 1” on page 98).
Flow Control	Select whether flow control should be activated for the selected port. The switch and its neighboring device can then send a pause frame to the switch to prevent packet loss due to overload. The pause frame receiver then pauses transmission. For time-critical automation scenarios, this option should be deactivated.

4.3.10 VLAN Configuration

On this page, you can configure VLAN.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, VLAN Configuration”.

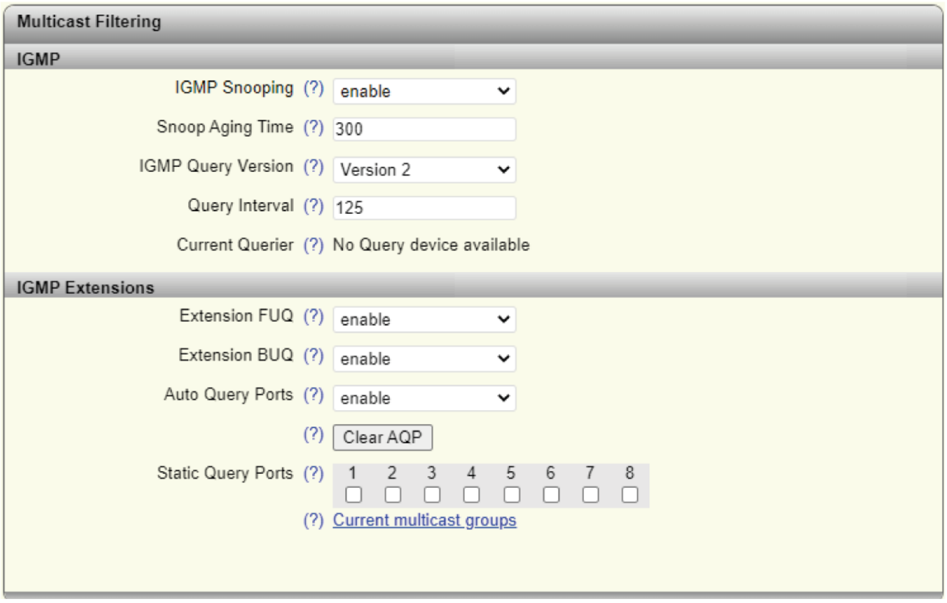
For further information on VLAN, refer to Section “VLAN – Virtual Local Area Network” on page 159.

4.3.11 Multicast Filtering

On the “Multicast Filtering” page, you can make settings for the Internet Group Management Protocol (IGMP). The network protocol is used to organize and manage multicast groups. A device with activated IGMP snooping, which is called a querier, eavesdrops on the multicast data traffic in the network and forwards the multicasts only to the devices the information is intended for. This increases the information security in the network and reduces the data traffic.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, Multicast Filtering”.

Figure 4-22 Multicast Filtering



Multicast Filtering

IGMP

IGMP Snooping (?) enable

Snoop Aging Time (?) 300

IGMP Query Version (?) Version 2

Query Interval (?) 125

Current Querier (?) No Query device available

IGMP Extensions

Extension FUQ (?) enable

Extension BUQ (?) enable

Auto Query Ports (?) enable

(?) Clear AQP

Static Query Ports (?)

1	2	3	4	5	6	7	8
□	□	□	□	□	□	□	□

(?) Current multicast groups

Multicast Filtering: IGMP

Table 4-32 IGMP: Parameters

Parameter	Description
IGMP Snooping	Here, select whether the “IGMP Snooping” function should be activated.
Snoop Aging Time	Here, enter the snoop aging time. The snoop aging time is the period of time during which the querier waits for membership reports. If no membership reports are received during this time, the associated ports are removed from the multicast groups. The value must be between 30 and 3600 (default: 300).
IGMP Query Version	Here, select the IGMP query version which the device should use to send the queries. The devices support IGMP query versions v1 and v2. For EtherNet/IP applications, it is recommended that you activate version v2.
Query Interval	Here, enter the interval at which the device should send the queries. The value must be between ten and 3600 seconds.
Current Querier	The IP address of the current querier in the network is displayed here.

Multicast Filtering: IGMP Extensions

Table 4-33 IGMP Extensions: Parameters

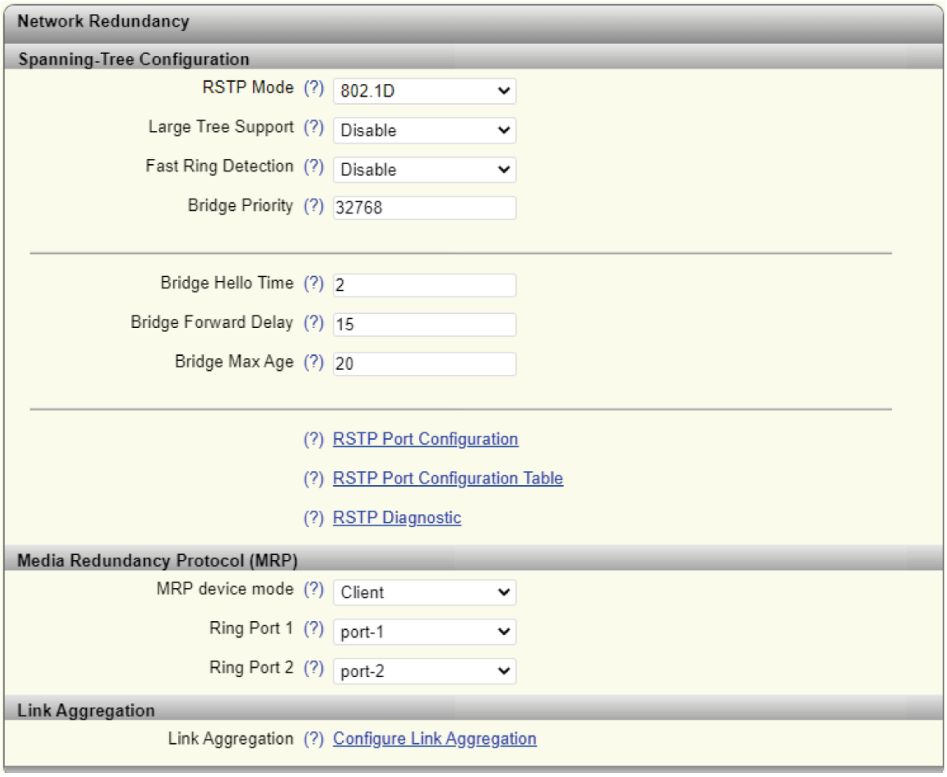
Parameter	Description
Extension FUQ	Select whether unknown multicasts should be forwarded to the querier.
Extension BUQ	Select whether unknown multicasts should be blocked at the querier.
Auto Query Ports	Select whether query ports should be automatically detected. This happens based on redundancy information. For this, the “Fast Ring Detection” function must be activated (see “Network Redundancy: Spanning-Tree Configuration” on page 75). Ports are then automatically added when they are detected in a redundant network. This enables faster switch-over in the event of a failure.
Clear AQP	Click on “Clear AQP” to clear query ports that have been automatically learned.
Static Query Ports	Activate the check boxes for the corresponding ports to automatically add the ports to all existing multicast groups.
Current multicast groups	Click on “Current multicast groups” to open the “Current Multicast Groups” pop-up window (see “Current Multicast Groups” on page 105). This contains an overview of all current multicast groups in tabular form.

4.3.12 Network Redundancy

On this page, you can make settings for network redundancy.

- Open web-based management (see "Accessing web-based management" on page 35) and log in.
- Click on "Configuration, Network Redundancy".

Figure 4-23 Network Redundancy



Network Redundancy

Spanning-Tree Configuration

RSTP Mode (?) 802.1D

Large Tree Support (?) Disable

Fast Ring Detection (?) Disable

Bridge Priority (?) 32768

Bridge Hello Time (?) 2

Bridge Forward Delay (?) 15

Bridge Max Age (?) 20

(?) RSTP Port Configuration

(?) RSTP Port Configuration Table

(?) RSTP Diagnostic

Media Redundancy Protocol (MRP)

MRP device mode (?) Client

Ring Port 1 (?) port-1

Ring Port 2 (?) port-2

Link Aggregation

Link Aggregation (?) Configure Link Aggregation

Network Redundancy: Spanning-Tree Configuration

The Rapid Spanning Tree Protocol (RSTP) is a network protocol in accordance with IEEE 802.1D-2004 that deactivates redundant paths and activates them quickly in the event of a connection failure.

Table 4-34 Spanning-Tree Configuration: Parameters

Parameter	Description
RSTP Mode	– Disable: RSTP is deactivated. – 802.1D: RSTP is activated globally and operates in accordance with standard IEEE 802.1D-2004.
Large Tree Support	This option is only available if you selected “802.1D” for “RSTP Mode”. ℹ This option is only available on the 22xx/23xx/24xx/25xx/26xx/27xx versions. Activate this option to increase the maximum possible number of switches in an RSTP topology.
Fast Ring Detection	This option is only available if you selected “802.1D” for “RSTP Mode”. ℹ This option is only available on the 22xx/23xx/24xx/25xx/26xx/27xx versions. Activate this option to speed up the switch-over to a redundant path in the event of an error and to enable easy diagnostics. Each ring is assigned an ID. This ID is communicated to every switch in the corresponding ring. One switch can belong to several rings at the same time.
Bridge Priority	This option is only available if you selected “802.1D” for “RSTP Mode”. Here, enter a value for the priority. The value must be between zero and 61440. Only multiples of 4096 are permitted. The entered value is automatically rounded to the next multiple of 4096 (default: 32768). Click on “Apply&Save” to start the initialization process.
Bridge Hello Time	This option is only available if you selected “802.1D” for “RSTP Mode”. Enter the time interval within which the root bridge reports to the other switches via BPDU. The value must be between one and ten seconds. ℹ This setting must only be made on the root bridge. ℹ We recommend that you keep the default setting.

Table 4-34 Spanning-Tree Configuration: Parameters

Parameter	Description
Bridge Forward Delay	This option is only available if you selected “802.1D” for “RSTP Mode”. Enter the time for which the switches should remain in the “Listening” and “Learning” status respectively (2x Forward Delay). The value must be between four and 30 seconds. The device only switches to the “Forwarding” status once this time has elapsed. In the “Listening” and “Learning” status, the device does not forward any user traffic and consequently prevents transient loops. ℹ This setting must only be made on the root bridge. ℹ We recommend that you keep the default setting.
Bridge Max Age	This option is only available if you selected “802.1D” for “RSTP Mode”. Enter the maximum aging time. The value must be between six and 40 seconds. This parameter is set by the root bridge and used by all switches in the ring. The parameter is sent to ensure that each switch in the network has a constant value, which is used as the basis for testing the age of the saved configuration. ℹ This setting must only be made on the root bridge. ℹ We recommend that you keep the default setting.
RSTP Port Configuration	This option is only available if you selected “802.1D” for “RSTP Mode”. Click on “RSTP Port Configuration” to open the “RSTP Port Configuration” pop-up window (see “Network Redundancy: Media Redundancy Protocol (MRP)” on page 76).
RSTP Port Configuration Table	This option is only available if you selected “802.1D” for “RSTP Mode”. Click on “RSTP Port Configuration Table” to open the “RSTP Port Configuration Table” pop-up window (see “Pop-up window: RSTP Port Configuration Table” on page 80).
RSTP Diagnostic	This option is only available if you selected “802.1D” for “RSTP Mode”. Click on “RSTP Diagnostic” to open the “RSTP Diagnostic” page (see “RSTP Diagnostic” on page 102).

Network Redundancy: Media Redundancy Protocol (MRP)

The Media Redundancy Protocol (MRP) is a network protocol for ring topologies in accordance with IEC 62439 that deactivates a redundant path and activates it quickly in the event of a connection failure. A ring may contain a maximum of 50 switches, one of which is defined as the MRP manager. All other devices in the ring must support the MRP client function. The ring is created using dedicated ports. The MRP ports are configured in the management for the respective switch. When configured correctly, MRP offers a guaranteed maximum switch-over time of 200 ms.

ℹ The MRP manager function is only available on the 22xx/23xx/24xx/25xx/26xx/27xx versions.

ℹ For firmware versions 2.90 or earlier, this function can only be implemented with inserted FL SD FLASH/MRM configuration memory.

Table 4-35 Media Redundancy Protocol (MRP): Parameters

Parameter	Description
MRP device mode	– Disable: MRP is deactivated. – Client: MRP is activated. The switch is an MRP client. – Manager: MRP is activated. The switch is the ring manager.
VLAN	This option is only available if you selected “Manager” for “MRP device mode”. If you selected “Tagging” for the VLAN mode, here you can select the VLAN to which the MRP control packets should be forwarded (see “VLAN Configuration” on page 72 and “VLAN – Virtual Local Area Network” on page 159).
Ring Port 1	This option is only available if you selected “Client” or “Manager” for “MRP device mode”. Select the first MRP ring port.
Ring Port 2	This option is only available if you selected “Client” or “Manager” for “MRP device mode”. Select the second MRP ring port.

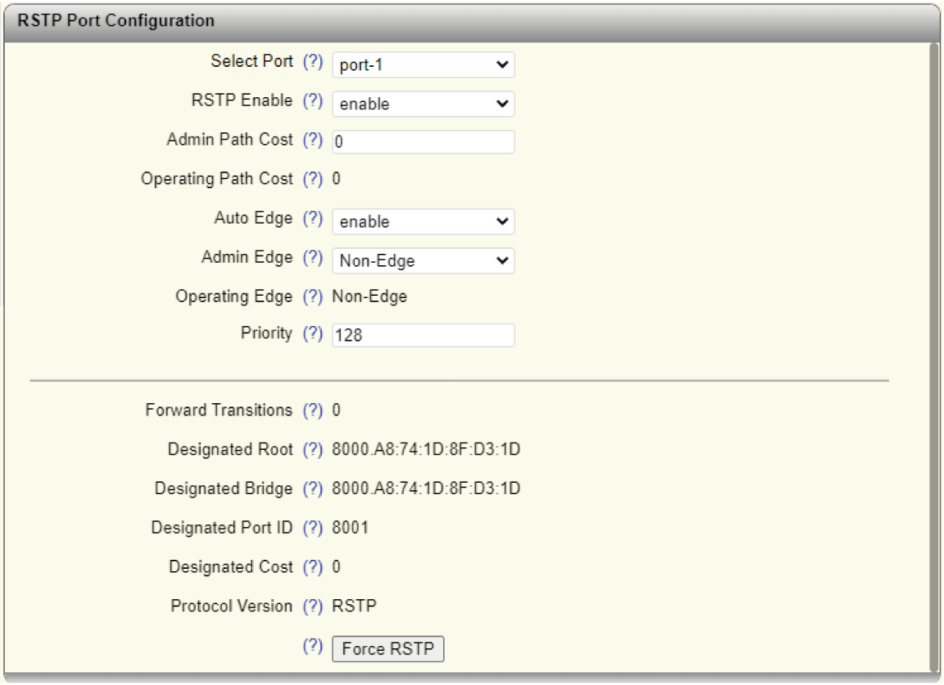
Network Redundancy: Link Aggregation

Table 4-36 Media Redundancy Protocol (MRP): Parameters

Parameter	Description
Link Aggregation	Click on “Configure Link Aggregation” to open the “Link Aggregation” window (see “LACP – Link Aggregation Control Protocol” on page 145).

Pop-up window: RSTP Port Configuration

Figure 4-24 Pop-up window: RSTP Port Configuration



RSTP Port Configuration

Select Port (?) port-1

RSTP Enable (?) enable

Admin Path Cost (?) 0

Operating Path Cost (?) 0

Auto Edge (?) enable

Admin Edge (?) Non-Edge

Operating Edge (?) Non-Edge

Priority (?) 128

Forward Transitions (?) 0

Designated Root (?) 8000.A8:74:1D:8F:D3:1D

Designated Bridge (?) 8000.A8:74:1D:8F:D3:1D

Designated Port ID (?) 8001

Designated Cost (?) 0

Protocol Version (?) RSTP

Table 4-37 Pop-up window: RSTP Port Configuration

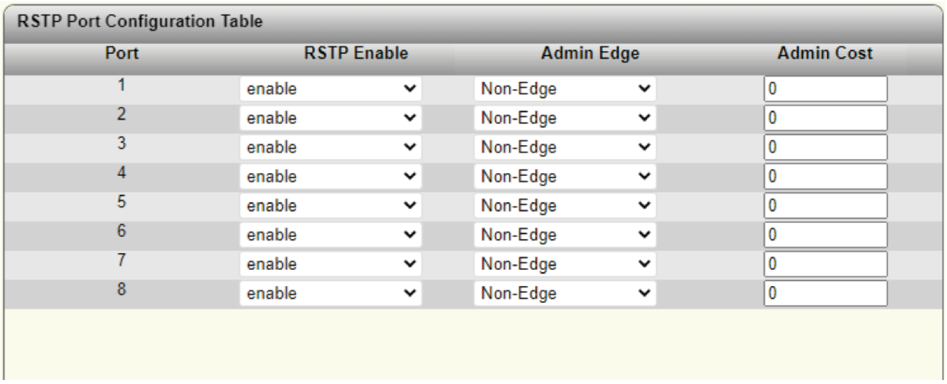
Parameter	Description
Select Port	Select the port for which you want to make RSTP settings.
RSTP Enable	Select the ports for which RSTP should be activated. – Enable: RSTP is activated for the port. – Disable: RSTP is deactivated for the port. BPDUs are neither received nor sent. If you activate RSTP on a port, the “Fast Startup” function is automatically deactivated on this port (see “Port Configuration: Individual Port Configuration” on page 67).
Admin Path Cost	Enter the path costs for the selected port. The value must be between zero and 200000000. If you enter “0”, cost calculation according to the transmission speed is activated (10 Mbps = 2000000; 100 Mbps = 200000).
Operating Path Cost	The path costs used for this port are displayed here. If this device is the root bridge, this value is added to each BPDU.

Table 4-37 Pop-up window: RSTP Port Configuration

Parameter	Description
Auto Edge	Select whether to automatically switch from non-edge port to edge port after a link up. A link becomes an edge if three seconds have passed since the last link up. An edge port is a port at the end of the topology. End devices or devices that do not themselves support RSTP can be connected to this port.
Admin Edge	Select whether this port should be operated as an edge port (default setting) or non-edge port once the link is established. The port becomes a non-edge port as soon as a BPDU is received.
Operating Edge	This shows whether this port is currently operated as an edge port or a non-edge port.
Priority	Enter the priority for this port. The value must be between zero and 140. Multiples of 16 are permitted. The entered value is automatically rounded to the next multiple of 16 (default: 128).
Forward Transitions	The number of times the port has switched from the “Discarding” state to the “Forwarding” state is displayed here.
Designated Root	The MAC address of the root bridge for this spanning tree is displayed here.
Designated Bridge	The MAC address of the switch of which the port receives the best BPDUs is displayed here.
Designated Port ID	The port via which the BPDUs are sent from the designated bridge is displayed here. The value consists of the port priority (two digits) and the port number. The value is displayed in hexadecimal numbers.
Designated Cost	The path cost of this segment to the root switch is displayed here.
Protocol Version	The protocol version is displayed here.
Force RSTP	Click on “Force RSTP” to activate RSTP for the selected port if it was previously operated in STP mode.

Pop-up window: RSTP Port Configuration Table

Figure 4-25 Pop-up window: RSTP Port Configuration Table



RSTP Port Configuration Table

Port	RSTP Enable	Admin Edge	Admin Cost
1	enable	Non-Edge	0
2	enable	Non-Edge	0
3	enable	Non-Edge	0
4	enable	Non-Edge	0
5	enable	Non-Edge	0
6	enable	Non-Edge	0
7	enable	Non-Edge	0
8	enable	Non-Edge	0

Table 4-38 Pop-up window: RSTP Port Configuration Table

Parameter	Description
Port	This column shows the ports for which RSTP is available.
RSTP Enable	Select the ports for which RSTP should be activated. – Enable: RSTP is activated for the port. – Disable: RSTP is deactivated for the port. BPDUs are neither received nor sent. If you activate RSTP on a port, the “Fast Startup” function is automatically deactivated on this port (see “Port Configuration: Individual Port Configuration” on page 67).
Admin Edge	Select whether this port is to be operated, if possible, as an edge port (default) or non-edge port.
Admin Cost	Enter the path costs for the selected port. If you enter “0”, cost calculation according to the transmission speed is activated (10 Mbps = 2,000,000; 100 Mbps = 200,000).

For further information on RSTP, refer to Section “RSTP – Rapid Spanning Tree Protocol” on page 137.

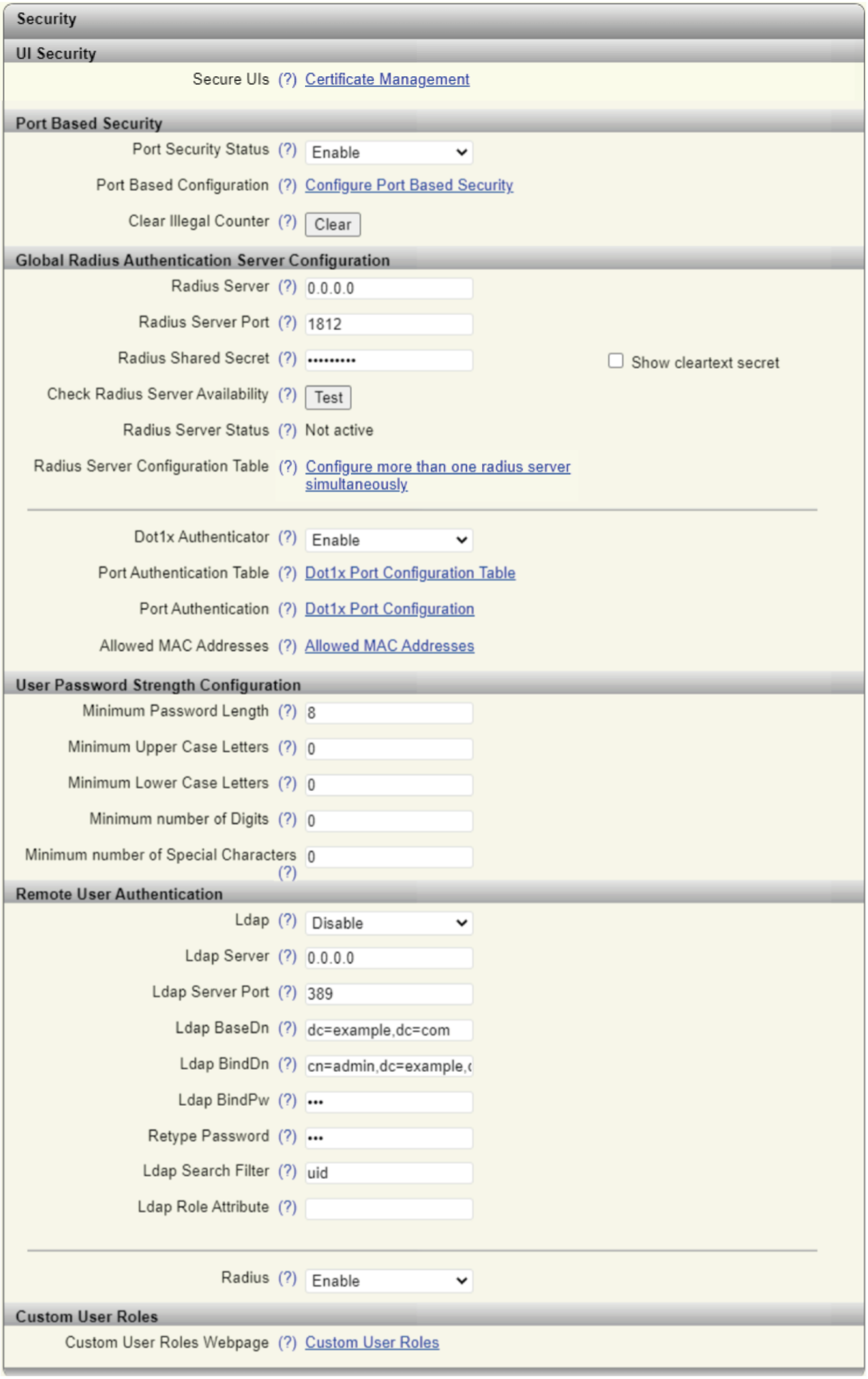
4.3.13 Security

On the “Security” page, you can make numerous settings related to security and network access.

NOTE: Threat to network security
Make sure that the configuration is secure to prevent unauthorized access to your network. More information is available in the AH EN INDUSTRIAL SECURITY application note. The application note can be downloaded at phoenixcontact.net/qr/<item_number>.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, Security”.

Figure 4-26 Security



Security

UI Security

Secure UIs (?) Certificate Management

Port Based Security

Port Security Status (?) Enable

Port Based Configuration (?) Configure Port Based Security

Clear Illegal Counter (?) Clear

Global Radius Authentication Server Configuration

Radius Server (?) 0.0.0.0

Radius Server Port (?) 1812

Radius Shared Secret (?) ••••••••• □ Show cleartext secret

Check Radius Server Availability (?) Test

Radius Server Status (?) Not active

Radius Server Configuration Table (?) Configure more than one radius server simultaneously

Dot1x Authenticator (?) Enable

Port Authentication Table (?) Dot1x Port Configuration Table

Port Authentication (?) Dot1x Port Configuration

Allowed MAC Addresses (?) Allowed MAC Addresses

User Password Strength Configuration

Minimum Password Length (?) 8

Minimum Upper Case Letters (?) 0

Minimum Lower Case Letters (?) 0

Minimum number of Digits (?) 0

Minimum number of Special Characters (?) 0

Remote User Authentication

Ldap (?) Disable

Ldap Server (?) 0.0.0.0

Ldap Server Port (?) 389

Ldap BaseDn (?) dc=example,dc=com

Ldap BindDn (?) cn=admin,dc=example,

Ldap BindPw (?) •••

Retype Password (?) •••

Ldap Search Filter (?) uid

Ldap Role Attribute (?)

Radius (?) Enable

Custom User Roles

Custom User Roles Webpage (?) Custom User Roles

Security: UI Security

Table 4-39 UI Security: Parameters

Parameter	Description
Secure UIs	Click on “Certificate Management” to open the “Certificate Management” pop-up window (see “Pop-up window: Certificate Management” on page 85). Here, you can create the necessary keys and certificates for operation with HTTPS and SSH.

Security: Port Based Security

ℹ The 20xx and 21xx versions do not support port-based security.

Table 4-40 Port Based Security: Parameters

Parameter	Description
Port Security Status	Select whether port-based security should be activated globally.
Port Based Configuration	Click on “Configure Port Based Security” to open the “Port Based Security” pop-up window (see “Pop-up window: Port Based Security” on page 85).
Clear Illegal Counter	Click on “Clear” to set the illegal access counter for all ports to zero.

Security: Global Radius Authentication Server Configuration

Table 4-41 Global Radius Authentication Server Configuration: Parameters

Parameter	Description
Radius Server	Here, enter the IP address of the RADIUS server.
Radius Server Port	Here, enter the port of the RADIUS server.
Radius Shared Secret	Here, enter the shared secret that is required for encrypted communication with the RADIUS server. The shared secret must have between eight and 64 characters. Letters, numbers, and the following special characters are permitted: $%@&/\()=?[]{}+*-_<>#^.,:~|
Check Radius Server Availability	Click on “Test” to check whether the configured RADIUS server is reachable.
Radius Server Status	The status of the RADIUS server that can be checked via “Check Radius Server Availability” is displayed here.
Radius Server Configuration Table	Click on “Configure more than one radius server simultaneously” to open the “Radius Server Configuration Table” window (see “Pop-up window: Radius Server Configuration Table” on page 87). Here you can configure up to five RADIUS servers.
Dot1x Authenticator	Select whether the device should be an 802.1X authenticator. ℹ One end device can be authenticated via 802.1X per port.

Table 4-41 Global Radius Authentication Server Configuration: Parameters

Parameter	Description
Port Authentication Table	Click on “Dot1x Port Configuration Table” to open the “Dot1x Port Configuration Table” page (see “Pop-up window: Dot1x Port Configuration Table” on page 88). Here, you can make settings for RADIUS authentication in tabular form.
Port Authentication	Click on “Dot1x Port Configuration” to open the “Dot1x Port Configuration” page (see “Pop-up window: Dot1x Port Configuration” on page 90). Here, you can make settings for RADIUS authentication on a port-specific basis.
Allowed MAC Addresses	Click on “Allowed MAC Addresses” to open a list of all MAC addresses currently permitted (see “Pop-up window: Allowed MAC Addresses” on page 91).

For further information on RADIUS certificates, see “RADIUS certificates” on page 167.

Security: User Password Strength Configuration

With the following parameters, you can define minimum requirements for the user passwords, e.g., that all passwords must contain a special character.

Table 4-42 User Password Strength Configuration: Parameters

Parameter	Description
Minimum Password Length	Here, enter the desired minimum length for passwords. The value can have between eight and 64 characters (default: 8).
Minimum Upper Case Letters	Here, enter the desired minimum number of uppercase letters (A–Z). The value can have between zero and eight characters (default: 0).
Minimum Lower Case Letters	Here, enter the desired minimum number of lowercase letters (a–z). The value can have between zero and eight characters (default: 0).
Minimum number of Digits	Here, enter the desired minimum number of digits (0–9). The value can have between zero and eight characters (default: 0).
Minimum number of Special Characters	Here, enter the desired minimum number of special characters (e.g., .#:!?). The value can have between zero and eight characters (default: 0).

Security: Remote User Authentication

When a user logs in, databases are searched for a valid user name and password combination, where the user rights are also correctly assigned.

The local database is searched first. Then, the LDAP is searched, followed by the RADIUS database (if activated and configured in each case). If a valid combination is found, the search is terminated and the user is logged in.

Table 4-43 Remote User Authentication: Parameters

Parameter	Description
Ldap	Select whether LDAP server-based user authentication should be activated.
Ldap Server	Here, enter the address of the LDAP server as an IP address or DNS name.
Ldap Server Port	Here, enter the TCP port for connection with the LDAP server (default: 389). ℹ An encrypted connection to the LDAP server (e.g., via SSL/TLS and Port 636) is not currently supported by the device.
Ldap BaseDn	Here, enter the LDAP Base Distinguished Name. The BaseDN describes the base address or the storage location under which the user data is stored in the directory on the LDAP server.
Ldap BindDn	Here, enter the LDAP Bind Distinguished Name. The BindDn is the user name for logging the device into the LDAP server in order to be able to perform operations on the LDAP server such as browsing user data.
Ldap BindPw	Here, enter the LDAP Bind Password. The Bind password is required for authenticating the device on the LDAP server. This password is linked to the BindDn.
Retype Password	Here, enter the Bind password again.
Ldap Search Filter	Here, enter the server attribute under which the user name is to be found when logging into the server. Optional: With the wildcard operator {0}, you can define the part of the attribute that is to be entered during login (e.g., mail={0}@phoenixcontact.com).
Ldap Role Attribute	Here, enter the attribute under which the designation of the user roles are stored on the LDAP server. This attribute is mapped on the device with a local role designation so that rights can be assigned to a user. On the “Custom User Roles” page, you can map the LDAP role name from the server to a local user role under “Ldap Rolename” (see “Custom User Roles” on page 49).
Radius	Here, select whether RADIUS server-based user authentication should be activated. To establish a connection to the RADIUS server, the settings under “Global Radius Authentication Server Configuration” are used (see “Security: Global Radius Authentication Server Configuration” on page 82).

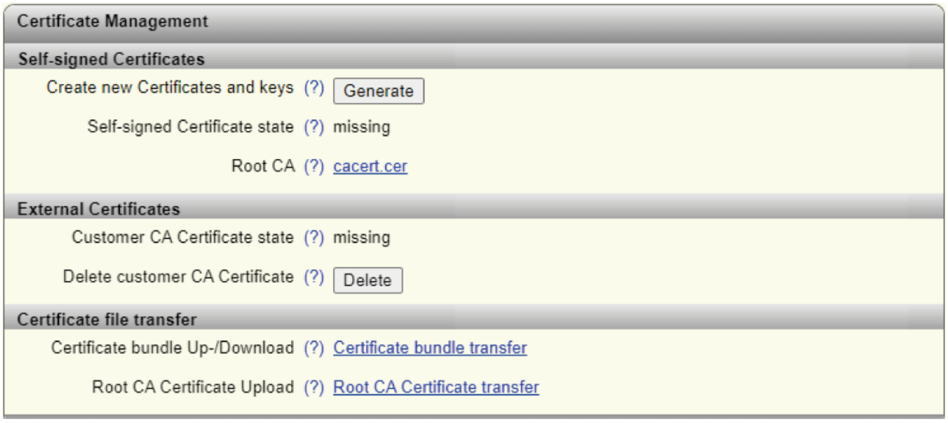
Security: Custom User Roles

Table 4-44 Custom User Roles: Parameters

Parameter	Description
Custom User Roles Webpage	Click on “Custom User Roles” to open the “Custom User Roles” pop-up window. Here, you can define the desired permissions for each role (see “Custom User Roles” on page 49).

Pop-up window: Certificate Management

Figure 4-27 Pop-up window: Certificate Management.



Certificate Management

Self-signed Certificates

Create new Certificates and keys (?) Generate

Self-signed Certificate state (?) missing

Root CA (?) cacert.cer

External Certificates

Customer CA Certificate state (?) missing

Delete customer CA Certificate (?) Delete

Certificate file transfer

Certificate bundle Up-/Download (?) Certificate bundle transfer

Root CA Certificate Upload (?) Root CA Certificate transfer

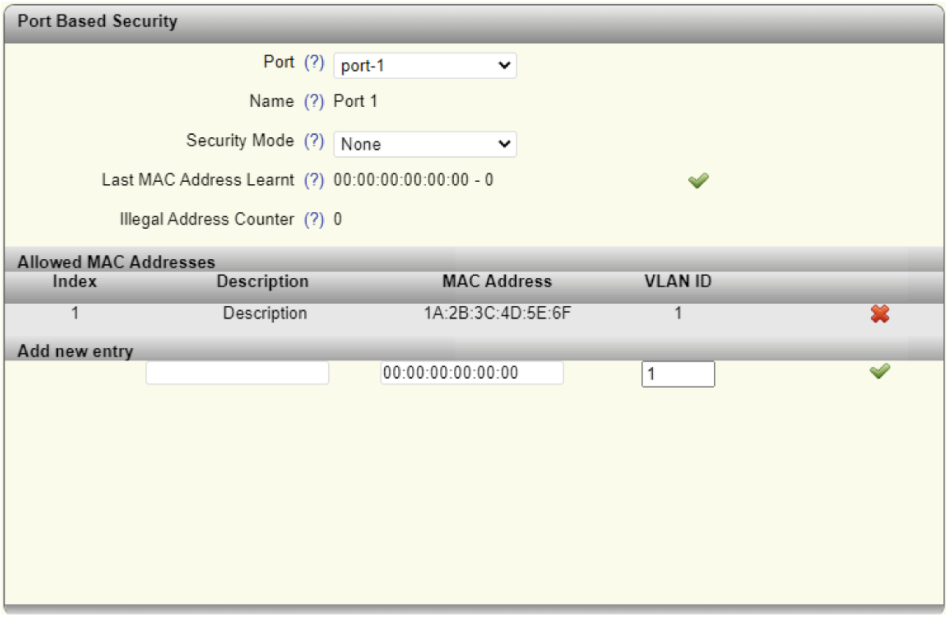
Table 4-45 Pop-up window: Certificate Management: Parameters

Parameter	Description
Create new Certificates and keys	Click on “Generate” to create all the necessary keys and certificates for operation with HTTPS and SSH.
Self-signed Certificate state	The current availability of the self-signed certificate is displayed here.
Root CA	Click on “cacert.cer” to download the created root CA certificate for the installation from the device.
Customer CA Certificate state	The current status of the customer CA certificate is displayed here. You can provide your own signed certificate. Your browser’s security warnings will then no longer be triggered.
Delete customer CA Certificate	Click on “Delete” to delete your own signed certificate.
Certificat bundle Up-/Download	Click on “Certificate bundle transfer” to open the “File Transfer” pop-up window (see “File Transfer” on page 129).
Root CA Certificate Upload	Click on “Root CA Certificate transfer” to open the “File Transfer” pop-up window (see “File Transfer” on page 129).

Pop-up window: Port Based Security

All the configurations in the “Port Based Security” pop-up window only become effective if the “Port Security Status” function is activated on the “Security” page (see “Security: Port Based Security” on page 82).

Figure 4-28 Pop-up window: Port Based Security



Port Based Security

Port (?) port-1

Name (?) Port 1

Security Mode (?) None

Last MAC Address Learnt (?) 00:00:00:00:00:00 - 0 ✓

Illegal Address Counter (?) 0

Allowed MAC Addresses

Index	Description	MAC Address	VLAN ID	
1	Description	1A:2B:3C:4D:5E:6F	1	✖

Add new entry

		00:00:00:00:00:00	1	✓

Table 4-46 Pop-up window: Port Based Security: Parameters

Parameter	Description
Port	Select the port or interface for which you want to make security settings.
Name	The name of the selected port is displayed here.
Security Mode	Select what happens if a MAC address that is not permitted is detected by the device. – None: No security settings for this port. Unknown MAC addresses are not blocked. – Trap: If a MAC address that is not permitted is detected at the port, a trap is sent to the defined SNMP trap server. The packets are not blocked (see "Trap Manager" on page 107). – Block: If a MAC address that is not permitted is detected at the port, all packets are blocked at the port and a trap is sent to the defined SNMP trap server. The packets at this port remain blocked until an allowed MAC address is detected (see "Trap Manager" on page 107).
Last MAC Address Learnt	The MAC address of the last connected device is displayed here. Click on the green check mark to add this MAC address to the list of allowed MAC addresses.
Illegal Address Counter	The number of times the port has been accessed illegally is displayed here. Each initial access by a MAC address is counted. Repeated access by the first MAC address are counted again if a different MAC address has accessed the port in the meantime.

Pop-up window: Port Based Security: Allowed MAC Addresses

You can allow up to 50 MAC addresses per port. Each MAC address can only be allowed at one port. MAC addresses that are allowed at one port cannot be learned at other ports, not even dynamically.

Web-based management or the network cannot be accessed via a MAC address that is allowed at another port.

Table 4-47 Allowed MAC Addresses: Parameters

Parameter	Description
Index	The index of the allowed MAC addresses is displayed here.
Description	The description of an allowed MAC address is displayed here.
MAC Address	The MAC address is displayed here.
VLAN ID	The associated VLAN ID is displayed here.
Delete	Click on the red “X” to delete an allowed MAC address.

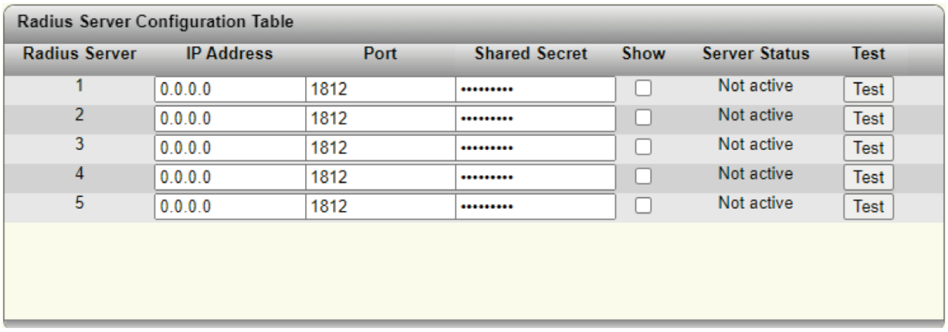
Pop-up window: Port Based Security: Add new entry

Table 4-48 Add new entry: Parameters

Parameter	Description
Description	Here, enter a description for an allowed MAC address.
MAC Address	Enter a MAC address for which you wish to allow access. Alternatively, click on the green check mark next to “Last MAC Address Learnt” to accept this MAC address.
VLAN ID	Enter the VLAN where the device with the allowed MAC address is located.
Confirm	Click on the green check mark to add an allowed MAC address.

Pop-up window: Radius Server Configuration Table

Figure 4-29 Pop-up window: Radius Server Configuration Table



Radius Server Configuration Table

Radius Server	IP Address	Port	Shared Secret	Show	Server Status	Test
1	0.0.0.0	1812	•••••••••	□	Not active	Test
2	0.0.0.0	1812	•••••••••	□	Not active	Test
3	0.0.0.0	1812	•••••••••	□	Not active	Test
4	0.0.0.0	1812	•••••••••	□	Not active	Test
5	0.0.0.0	1812	•••••••••	□	Not active	Test

Table 4-49 Pop-up window: Radius Server Configuration Table: Parameters

Parameter	Description
Radius Server	The ID of the RADIUS server is displayed here.
IP Address	Here, enter the IP address of the RADIUS server.
Port	Here, enter the port of the RADIUS server.

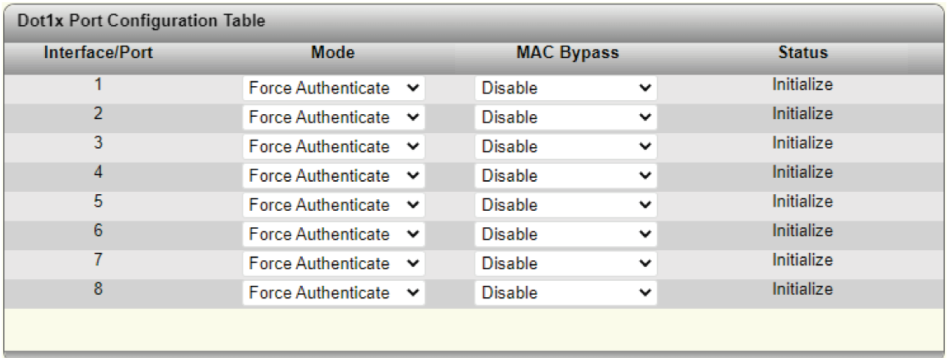
Table 4-49 Pop-up window: Radius Server Configuration Table: Parameters

Parameter	Description
Shared Secret	Here, enter the shared secret that is required for encrypted communication with the RADIUS server. The shared secret must have between eight and 64 characters. Letters, numbers, and the following special characters are permitted: $%@&/\()=?[]{}+*-_<>#^.,:~|
Show	Activate the check box to display the shared secret.
Server Status	The status of the RADIUS server that can be tested via “Test” is displayed here.
Test	Click on “Test” to check whether the configured RADIUS server is reachable.

If more than one RADIUS server is configured and RADIUS server 1 is not available, it can take up to 30 seconds for the page to load.

Pop-up window: Dot1x Port Configuration Table

Figure 4-30 Pop-up window: Dot1x Port Configuration Table



Dot1x Port Configuration Table

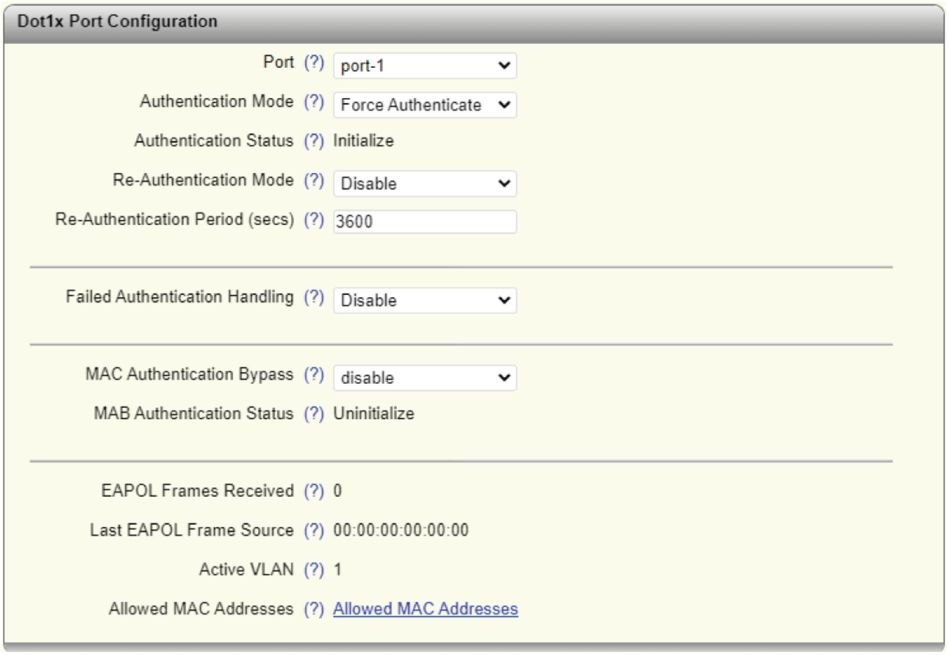
Interface/Port	Mode	MAC Bypass	Status
1	Force Authenticate	Disable	Initialize
2	Force Authenticate	Disable	Initialize
3	Force Authenticate	Disable	Initialize
4	Force Authenticate	Disable	Initialize
5	Force Authenticate	Disable	Initialize
6	Force Authenticate	Disable	Initialize
7	Force Authenticate	Disable	Initialize
8	Force Authenticate	Disable	Initialize

Table 4-50 Pop-up window: Dot1x Port Configuration Table: Parameters

Parameter	Description
Interface/Port	The port number is displayed here.
Mode	Select the authentication mode for the port. – Auto: Devices connected to the port are authenticated via 802.1X. The “Dot1x Authenticator” option must be activated for this (see “Security: Global Radius Authentication Server Configuration” on page 82). – Force Authenticate: All the devices connected to the port are authenticated. – Force Unauthenticate: None of the devices connected to the port are authenticated.
MAC Bypass	Select whether the “MAC Authentication Bypass” (MAB) function should be activated for the port. The authentication is performed based on the MAC address of the connected device. The MAC address is automatically detected. ! **NOTE: Threat to network security** Activating the “MAC Bypass” function poses a threat to your network security.
Status	The port authentication status is displayed here.

Pop-up window: Dot1x Port Configuration

Figure 4-31 Pop-up window: Dot1x Port Configuration



Dot1x Port Configuration

Port (?)	port-1
Authentication Mode (?)	Force Authenticate
Authentication Status (?)	Initialize
Re-Authentication Mode (?)	Disable
Re-Authentication Period (secs) (?)	3600
Failed Authentication Handling (?)	Disable
MAC Authentication Bypass (?)	disable
MAB Authentication Status (?)	Uninitialize
EAPOL Frames Received (?)	0
Last EAPOL Frame Source (?)	00:00:00:00:00:00
Active VLAN (?)	1
Allowed MAC Addresses (?)	Allowed MAC Addresses

Table 4-51 Pop-up window: Dot1x Port Configuration: Parameters

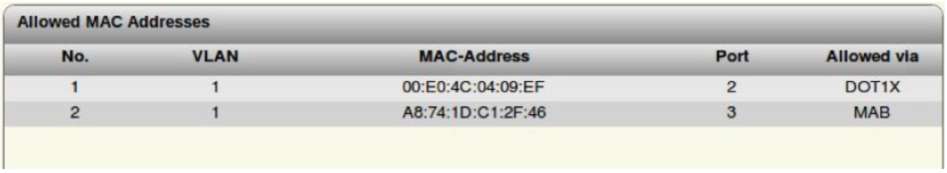
Parameter	Description
Port	Select the port for which you wish to carry out RADIUS configuration.
Authentication Mode	Select the authentication mode for the port. – Auto: Devices connected to the port are authenticated via 802.1X. The “Dot1x Authenticator” option must be activated for this (see “Security: Global Radius Authentication Server Configuration” on page 82). – Force Authenticate: All the devices connected to the port are authenticated. – Force Unauthenticate: None of the devices connected to the port are authenticated.
Authentication Status	The port authentication status is displayed here.
Re-Authentication Mode	Select whether a client should be re-authenticated at a regular interval.
Re-Authentication Period (secs)	Enter the interval in seconds after which a client should be re-authenticated (1 ... 65535 seconds).
Failed Authentication Handling	Select what should happen if non-authenticated clients are rejected by the RADIUS server: – Disable: Non-authenticated clients are rejected. – Guest-VLAN: Non-authenticated clients are assigned to a guest VLAN. – Port Disable: If a non-authenticated client is rejected by the RADIUS server, the port in question is disabled for a set time.

Table 4-51 Pop-up window: Dot1x Port Configuration: Parameters

Parameter	Description
Guest VLAN	This option is only available if you selected “Guest-VLAN” for “Failed Authentication Handling”. Select the guest VLAN to which clients should be assigned if they cannot be authenticated via the RADIUS server. The assignment then takes place automatically.
Port Re-Enable Timer	This option is only available if you selected “Port Disable” for “Failed Authentication Handling”. Enter the time in seconds for which the port should remain deactivated after an unauthenticated connection attempt. The value must be between one and 3600 seconds.
Port Re-Enable Timer Status	This option is only available if you selected “Port Disable” for “Failed Authentication Handling”. This shows whether the port is currently deactivated and the timer is running.
MAC Authentication Bypass	Select whether the “MAC Authentication Bypass” (MAB) function should be activated for the port. The clients that are not certified with EAPOL can be authenticated by the RADIUS server via their MAC address.
MAB Authentication Status	The MAB authentication status is displayed here.
EAPOL Frames Received	The number of EAPOL packets received is displayed here.
Last EAPOL Frame Source	The last MAC address from which an EAPOL packet was received at the port is displayed here.
Active VLAN	The port-specific VLAN ID assigned by the RADIUS server is displayed here.
Allowed MAC Addresses	Click on “Allowed MAC Addresses” to open the “Allowed MAC Addresses” pop-up window (see “Pop-up window: Allowed MAC Addresses” on page 91).

Pop-up window: Allowed MAC Addresses

Figure 4-32 Pop-up window: Allowed MAC Addresses



Allowed MAC Addresses

No.	VLAN	MAC-Address	Port	Allowed via
1	1	00:E0:4C:04:09:EF	2	DOT1X
2	1	A8:74:1D:C1:2F:46	3	MAB

Table 4-52 Pop-up window: Allowed MAC Addresses: Parameters

Parameter	Description
No.	A serial number that numbers the allowed MAC addresses consecutively is displayed here.
VLAN	The VLAN to which the MAC address is assigned is displayed here.

Table 4-52 Pop-up window: Allowed MAC Addresses: Parameters

Parameter	Description
MAC-Address	The MAC address is displayed here.
Port	The port number via which the MAC address is connected to the device is displayed here.
Allowed via	This shows whether the MAC address was allowed via Dot1x or MAB.

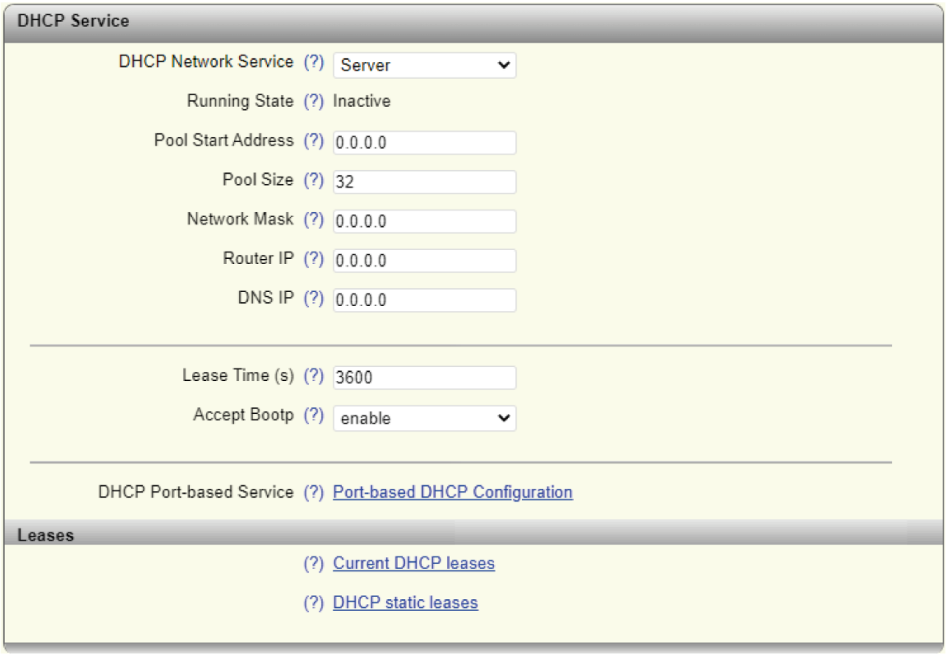
4.3.14 DHCP Service

On this page, you can make settings for DHCP.

DHCP network services are only available on the 22xx/23xx/24xx/25xx/26xx/27xx versions.

- Open web-based management (see "Accessing web-based management" on page 35) and log in.
- Click on "Configuration, DHCP Service".

Figure 4-33 DHCP Service



DHCP Service

DHCP Network Service (?) Server

Running State (?) Inactive

Pool Start Address (?) 0.0.0.0

Pool Size (?) 32

Network Mask (?) 0.0.0.0

Router IP (?) 0.0.0.0

DNS IP (?) 0.0.0.0

Lease Time (s) (?) 3600

Accept Bootp (?) enable

DHCP Port-based Service (?) Port-based DHCP Configuration

Leases

(?) Current DHCP leases

(?) DHCP static leases

Table 4-53 DHCP Service: Parameters

Parameter	Description
DHCP Network Service	Select the DHCP service you want to use. – None: The device will not use any DHCP service. – Relay Agent: The DHCP relay agent (DHCP option 82) is activated. – Server: The device is used as the DHCP server.
Option 82 Remote ID	This option is only available if you selected “Relay Agent” for “DHCP Network Service”. Select the address that is used as the remote ID. – IP: The IP address of the device is used as the remote ID. – MAC: The MAC address of the device is used as the remote ID. – STRING: The string in the “Option82 Unique String” field is used as the remote ID.
Remote ID Unique String	This option is only available if you selected “STRING” for “Option 82 Remote ID”. Enter a unique string that is used as the remote ID.
Server IP Address	This option is only available if you selected “Relay Agent” for “DHCP Network Service”. Enter the IP address of the DHCP server in your network.
Port Mode	This option is only available if you selected “Relay Agent” for “DHCP Network Service”. Select the ports for which the DHCP relay agent should be activated.
Running State	This option is only available if you selected “Server” for “DHCP Network Service”. The current DHCP server status is displayed here. If “Inactive” is displayed, check your settings.
Pool Start Address	This option is only available if you selected “Server” for “DHCP Network Service”. Enter the first IP address of the DHCP server address pool. The parameters “Pool Start Address”, “Pool Size”, and “Network Mask” must be aligned with each other. The IP range 169.254.x.x cannot be configured.
Pool Size	This option is only available if you selected “Server” for “DHCP Network Service”. Enter the number of IP addresses in the DHCP server address pool. Please note that the number of IP addresses must match the configured subnet.

Table 4-53 DHCP Service: Parameters

Parameter	Description
Network Mask	This option is only available if you selected “Server” for “DHCP Network Service”. Enter the subnet mask that is assigned to the DHCP clients.
Router IP	This option is only available if you selected “Server” for “DHCP Network Service”. Enter the IP address of the router or default gateway that is assigned to the DHCP clients.
DNS IP	This option is only available if you selected “Server” for “DHCP Network Service”. Enter the DNS IP address that is assigned to the DHCP clients.
Lease Time (s)	This option is only available if you selected “Server” for “DHCP Network Service”. Enter the time in seconds for which the DHCP server leases an IP address to a client before it has to report to the server again. The value must be between 300 and 2592000 seconds (default: 3600). If no time limit is required, enter a value of “0”.
Accept Bootp	This option is only available if you selected “Server” for “DHCP Network Service”. Select whether the device, acting as the DHCP server, accepts BootP requests. If this function is activated, an IP address with an infinite lease time is assigned to the requesting DHCP clients.
DHCP Port-based Service	This option is only available if you selected “Server” for “DHCP Network Service”. Click on “Port-based DHCP Configuration” to open the “DHCP Port Local Service” pop-up window (see “Pop-up window: DHCP Port Local Service” on page 95).

DHCP Service: Leases

Table 4-54 Leases: Parameters

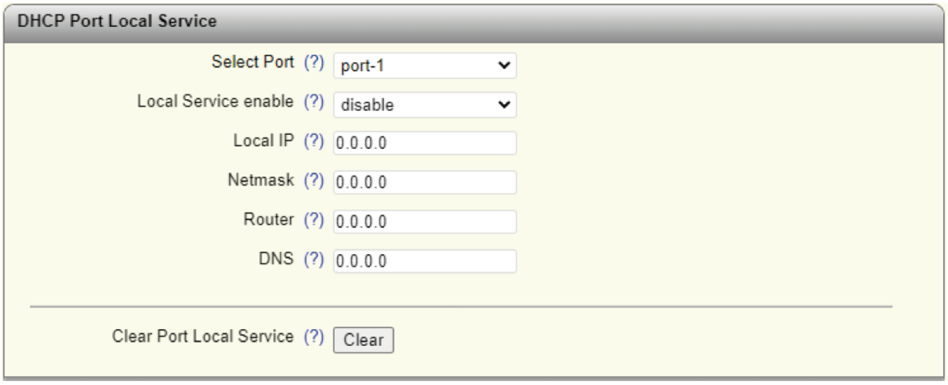
Parameter	Description
Current DHCP leases	Click on “Current DHCP leases” to open the “Current DHCP leases” pop-up window containing an overview of all IP addresses that are currently assigned (see “Pop-up window: Current DHCP leases” on page 96).
DHCP static leases	Click on “DHCP static leases” to open the “DHCP Static Leases” pop-up window for configuring static IP address assignments (see “Pop-up window: DHCP Static Leases” on page 97).

Pop-up window: DHCP Port Local Service

You can configure the port-based DHCP server function in this pop-up window.

If you want to use the port-based DHCP server function on one or more ports and have configured a pool-based DHCP server at the same time, port-based configuration always has priority on the respective ports.

Figure 4-34 DHCP Port Local Service



DHCP Port Local Service

Select Port (?) port-1

Local Service enable (?) disable

Local IP (?) 0.0.0.0

Netmask (?) 0.0.0.0

Router (?) 0.0.0.0

DNS (?) 0.0.0.0

Clear Port Local Service (?) Clear

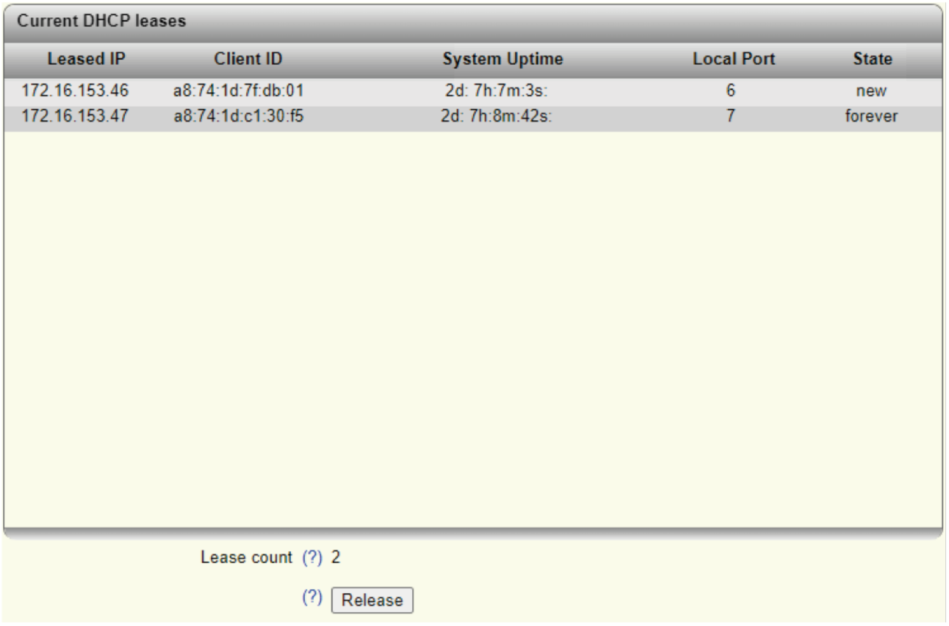
Table 4-55 Pop-up window: DHCP Port Local Service: Parameters

Parameter	Description
Select Port	Select the port for which you want to carry out port-based DHCP server configuration.
Local Service enable	Select whether the port-based DHCP server functionality should be activated for the selected port.
Local IP	Enter the IP address that is assigned to the client at the selected port.
Netmask	Enter the subnet mask that is assigned to the client at the selected port.
Router	Enter the gateway address that is assigned to the client at the selected port.
DNS	Enter the DNS address that is assigned to the client at the selected port.
Clear Port Local Service	Click on “Clear” to delete the port-based DHCP configurations of all ports.

Pop-up window: Current DHCP leases

The table shows the IP addresses that are currently assigned via DHCP.

Figure 4-35 Pop-up window: Current DHCP leases



Current DHCP leases

Leased IP	Client ID	System Uptime	Local Port	State
172.16.153.46	a8:74:1d:7f:db:01	2d: 7h:7m:3s:	6	new
172.16.153.47	a8:74:1d:c1:30:f5	2d: 7h:8m:42s:	7	forever

Lease count (?) 2

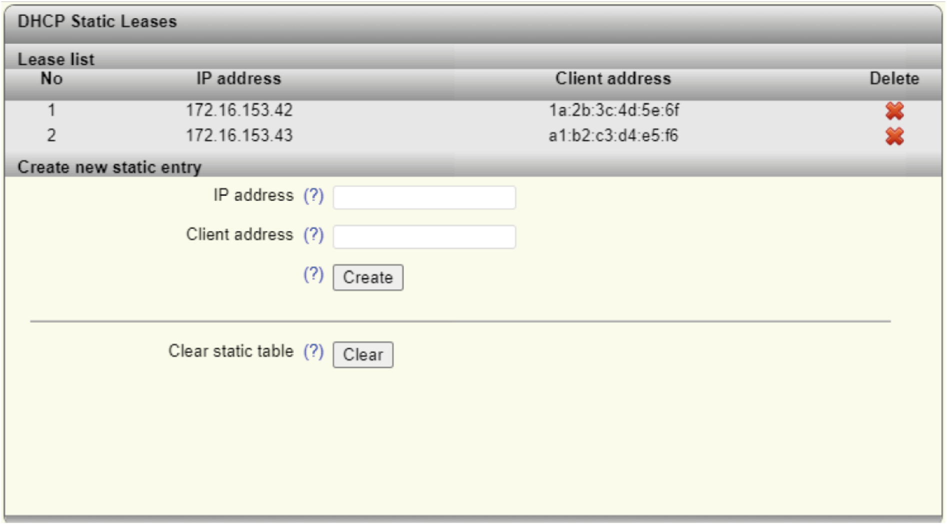
Table 4-56 Current DHCP leases: Parameters

Parameter	Description
Leased IP	This column shows the assigned IP addresses.
Client ID	This column shows the MAC address of the client to which the IP address is assigned.
System Uptime	This column shows the time that has elapsed since the IP address was assigned to the client.
Local Port	This column shows the interface to which the client is connected.
State	This column shows the status of the client.
Lease count	This field shows the number of assigned IP addresses.
Release	Click on “Release” to release unused entries again.

Pop-up window: DHCP Static Leases

The pop-up window shows the configured static IP address assignments. In addition, you can create new static IP address assignments here. To do so, assign a fixed IP address to MAC addresses.

Figure 4-36 Pop-up window: DHCP Static Leases



DHCP Static Leases

Lease list

No	IP address	Client address	Delete
1	172.16.153.42	1a:2b:3c:4d:5e:6f	✖
2	172.16.153.43	a1:b2:c3:d4:e5:f6	✖

Create new static entry

Table 4-57 DHCP Static Leases: Parameters

Parameter	Description
Lease list:	
No	This column numbers the entries consecutively.
IP address	This column shows the statically assigned IP address.
Client address	This column shows the MAC address of the client.
Delete	Click on the red “X” to delete the entry.
Create new static entry	
IP address	Enter the static IP address that you wish to assign.
Client address	Enter the MAC address of the device for which you wish to assign a static IP address.
Create	Click on “Create” to carry out static assignment.
Clear static table	Click on “Clear” to delete all the static DHCP leases.

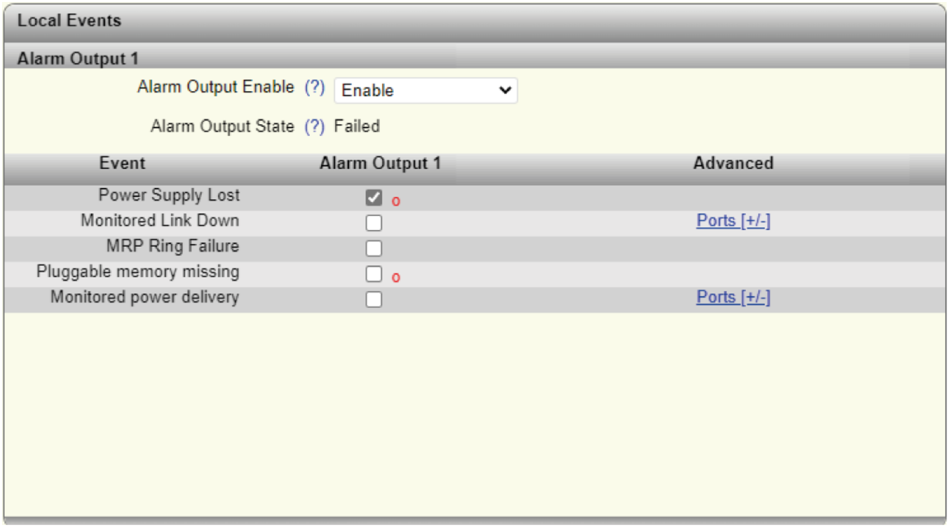
4.3.15 Local Events

On the “Local Events” page, you can make settings for the alarm output and signal contact.

The 20xx and 21xx versions do not feature an alarm output or signal contact.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, Local Events”.

Figure 4-37 Local Events



Local Events

Alarm Output 1

Alarm Output Enable (?) Enable

Alarm Output State (?) Failed

Event	Alarm Output 1	Advanced
Power Supply Lost	☑ o	
Monitored Link Down	□	Ports [+/-]
MRP Ring Failure	□	
Pluggable memory missing	□ o	
Monitored power delivery	□	Ports [+/-]

Local Events: Alarm Output 1

Table 4-58 Alarm Output 1: Parameters

Parameter	Description
Alarm Output Enable	Select whether the digital alarm output (22xx/23xx versions) or the signal contact (24xx/25xx versions) as well as the alarm message via the FAIL LED on the device should be activated. Some versions (e.g., 26xx/27xx) do not feature an alarm output or signal contact. For these versions, the alarm is solely signaled via the FAIL LED.
Alarm Output State	The current alarm message status is displayed here.

Specify the conditions under which the digital alarm output or signal contact and the FAIL LED should report an error.

If a red “**o**” is displayed, this event has occurred.

Table 4-59 Event: Parameters

Parameter	Description
Power Supply Lost	The device outputs an error message if supply voltage US1 or US2 is lost.
Monitored Link Down	The device outputs an error message if a link down occurs. Click on “Ports” to select the ports for which this error should be indicated.

Table 4-59 Event: Parameters

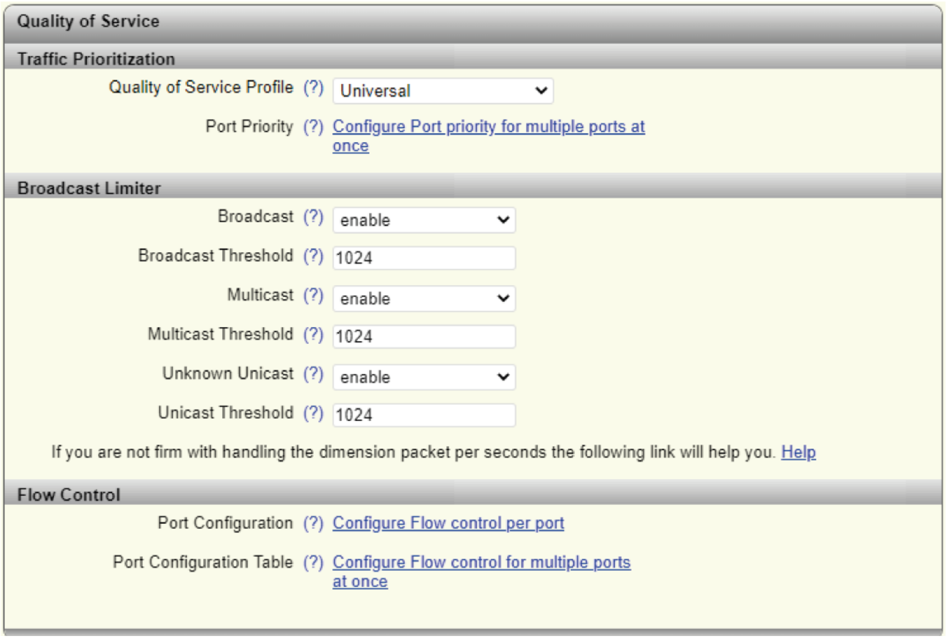
Parameter	Description
MRP Ring Failure	The device outputs an error message if an MRP ring error occurs.
Plugable Memory Missing	The device outputs an error message if no memory card is present.
Monitored power delivery	This option is only available on the SPE versions. The device outputs an error message if no voltage is transmitted via the port. Click on “Ports” to select the ports for which this error should be indicated.

4.3.16 Quality of Service

On this page, you can make settings for Quality of Service.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, Quality of Service”.

Figure 4-38 Quality of Service



Quality of Service

Traffic Prioritization

Quality of Service Profile (?) Universal

Port Priority (?) Configure Port priority for multiple ports at once

Broadcast Limiter

Broadcast (?) enable

Broadcast Threshold (?) 1024

Multicast (?) enable

Multicast Threshold (?) 1024

Unknown Unicast (?) enable

Unicast Threshold (?) 1024

If you are not firm with handling the dimension packet per seconds the following link will help you. Help

Flow Control

Port Configuration (?) Configure Flow control per port

Port Configuration Table (?) Configure Flow control for multiple ports at once

Quality of Service: Traffic Prioritization

The devices have eight priority queues into which incoming data traffic is sorted in accordance with specific criteria. These queues are processed in descending order of priority. High-priority data traffic is therefore always forwarded first.

Table 4-60 Traffic Prioritization: Parameters

Parameter	Description
Quality of Service Profile	Select a profile for prioritizing data traffic. – Universal: This profile is the default setting on standard versions. Class of Service (VLAN tag priority) is activated for data prioritization. – PROFINET: This profile is the default setting on PROFINET versions. Data prioritization based on Ethertype is activated in addition to Class of Service. In this profile, PROFINET data packets are always forwarded with high priority. Only control packets of redundancy protocols (RSTP and MRP) are given even higher priority. – EtherNet/IP: In this profile, prioritization via DSCP values and TCP/UDP ports is enabled in addition to Class of Service. This means that preferential treatment is given to EtherNet/IP data traffic. Only control packets of redundancy protocols (RSTP and MRP) are given even higher priority. – EtherNet/IP_L4PortOnly: in this profile, EtherNet/IP data traffic (e.g., CIP Motion, CIP Safety) is prioritized based on TCP/UDP ports. – CC-Link: This profile prioritizes packets with CC-Link and time synchronization packets in accordance with 802.1AS.
Port Priority	Click on “Configure Port priority for multiple ports at once” to open the “VLAN Port Configuration Table” page (see “Pop-up window: VLAN Port Configuration Table” on page 162). Here, you can configure the default priority. Incoming data traffic on the device that does not have a priority tag is marked in accordance with the setting and is assigned to a priority queue. ℹ You must additionally select the “Tagged” VLAN mode to activate these settings.

Quality of Service: Broadcast Limiter

In this area, you can set threshold values in data packets or frames per second for different data streams. This allows you to protect your network against overload.

Table 4-61 Broadcast Limiter: Parameters

Parameter	Description
Broadcast	Select whether the broadcast limiter should be activated.
Broadcast Threshold	Select the threshold value in frames per second for the broadcast limiter. The value entered is rounded down to the next valid value.
Multicast	Select whether the multicast limiter should be activated.

Table 4-61 Broadcast Limiter: Parameters

Parameter	Description
Multicast Threshold	Select the threshold value in frames per second for the multicast limiter. The value entered is rounded down to the next valid value.
Unknown Unicast	Select whether the unicast limiter for unknown unicasts should be activated. Unicasts from MAC addresses that the device has already learned are not affected by this.
Unicast Threshold	Select the threshold value in frames per second for the unicast limiter. The value entered is rounded down to the next valid value.
Help	Click on “Help” to open the “Storm Control Help” window (see “Quality of Service: Flow Control” on page 101).

Quality of Service: Flow Control

If you activate the flow control function on a port, there are two types of reactions:

- If the device detects a data overload at this port, a pause frame is sent to the connected device. This corresponds to the request to pause the sending of packets.
- If the device receives a pause frame on this port, the sending of packets is briefly interrupted.

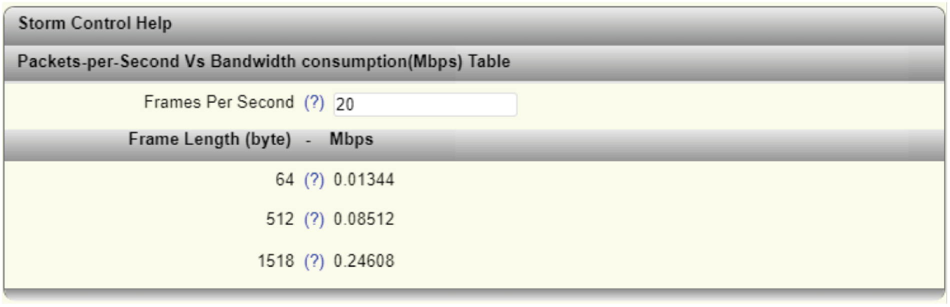
Table 4-62 Flow Control: Parameters

Parameter	Description
Port Configuration	Click on “Configure Flow control per port” to open the “Port Configuration” page (see “Port Configuration” on page 66).
Port Configuration Table	Click on “Configure Flow control for multiple ports at once” to open the “Port Configuration Table” page (see “Pop-up window: Port Configuration Table” on page 69).

The layer 3 functions supported by the NAT versions are described in Section “Layer 3 functions – routing and NAT (FL NAT 2xxx only)” on page 197.

Pop-up window: Storm Control Help

Figure 4-39 Storm Control Help



Storm Control Help

Packets-per-Second Vs Bandwidth consumption(Mbps) Table

Frames Per Second (?) 20

Frame Length (byte)	-	Mbps
64	(?)	0.01344
512	(?)	0.08512
1518	(?)	0.24608

Table 4-63 Flow Control: Parameters

Parameter	Description
Frames Per Second	Enter the desired number of frames per second and press the Enter key.
Frame Length (byte)	This column shows three sample frame lengths in bytes.
Mbps	This column shows you the required Mbps, based on the number of frames per second and the frame length.

4.4 WBM Diagnostics area

4.4.1 LLDP Topology

On this page, you will find information on the LLDP topology.

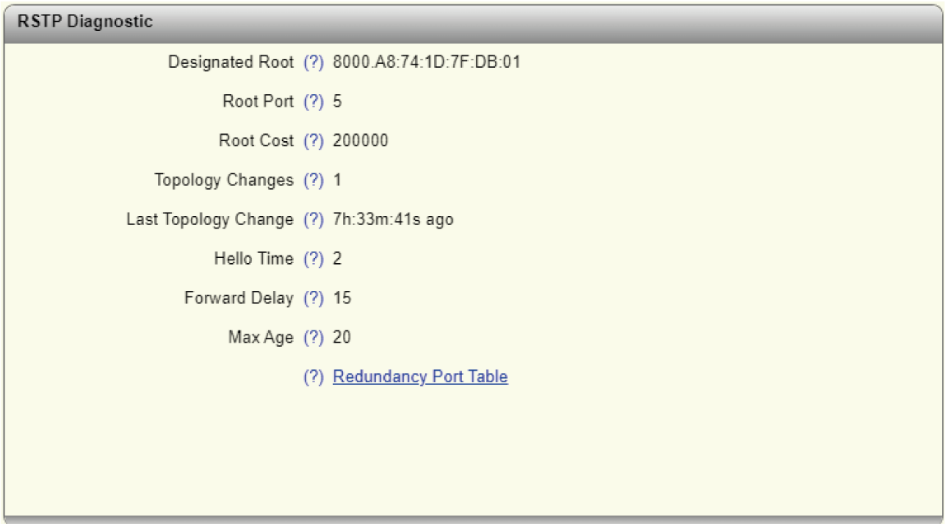
For further information on LLDP, refer to Section "LLDP – Link Layer Discovery Protocol" on page 153.

4.4.2 RSTP Diagnostic

On this page, you will find diagnostic information on the Rapid Spanning Tree Protocol (RSTP).

- Open web-based management (see "Accessing web-based management" on page 35) and log in.
- Click on "Diagnostics, RSTP Diagnostic".

Figure 4-40 RSTP Diagnostic



RSTP Diagnostic

Designated Root (?) 8000.A8:74:1D:7F:DB:01

Root Port (?) 5

Root Cost (?) 200000

Topology Changes (?) 1

Last Topology Change (?) 7h:33m:41s ago

Hello Time (?) 2

Forward Delay (?) 15

Max Age (?) 20

(?) Redundancy Port Table

Table 4-64 RSTP Diagnostic: Parameters

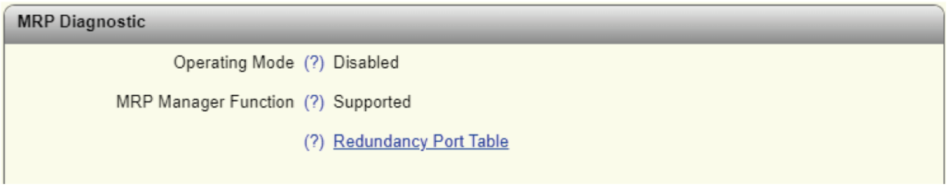
Parameter	Description
Designated Root	The root bridge for this spanning tree is displayed here. Alternatively, information is provided that RSTP is deactivated on the device.
Root Port	The port to which the root is connected is displayed here. If the root is not connected directly, it shows the direction of the root.
Root Cost	The total path costs to the root are displayed here.
Topology Changes	The number of topology changes is displayed here.
Last Topology Change	The elapsed time since the last topology change is displayed here.
Hello Time	The hello time set on the root is displayed here. This is the time after which a device has to contact the root again.
Forward Delay	The forward delay set on the root is displayed here.
Max Age	The maximum age time set on the root is displayed here.
Redundancy Port Table	Click on “Redundancy Port Table” to open the “Redundancy Port Table” pop-up window (see “Pop-up window: Redundancy Port Table” on page 104). It contains a table with the individual ports and their assignment to redundancy mechanisms.

4.4.3 MRP Diagnostic

On this page, you will find diagnostic information on the Media Redundancy Protocol (MRP).

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Diagnostics, MRP Diagnostic”.

Figure 4-41 MRP Diagnostic



MRP Diagnostic

Operating Mode (?) Disabled

MRP Manager Function (?) Supported

(?) Redundancy Port Table

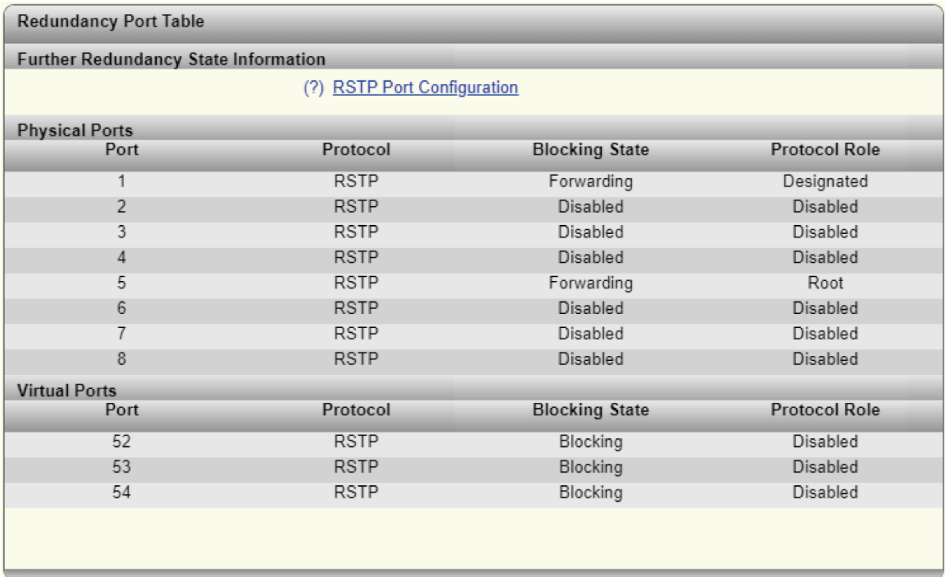
Table 4-65 MRP Diagnostic: Parameters

Parameter	Description
Operating Mode	The current MRP device status is displayed here.
MRP Manager Function	This shows whether the MRP manager function is supported on the device.
Ring status	This option is only available if you selected “Manager” for the operating mode of the MRP (see “Network Redundancy: Media Redundancy Protocol (MRP)” on page 76). The current MRP ring status is displayed here.
Change Counter	This option is only available if you selected “Manager” for the operating mode of the MRP (see “Network Redundancy: Media Redundancy Protocol (MRP)” on page 76). The number of status changes in the MRP ring is displayed here.
Redundancy Port Table	Click on “Redundancy Port Table” to open the “Redundancy Port Table” pop-up window (see “Pop-up window: Redundancy Port Table” on page 104). It contains a table with the individual ports and their assignment to redundancy mechanisms.

Pop-up window: Redundancy Port Table

The window contains a table with the individual ports and their assignment to redundancy mechanisms.

Figure 4-42 Pop-up window: Redundancy Port Table



Redundancy Port Table

Further Redundancy State Information

(?) RSTP Port Configuration

Physical Ports

Port	Protocol	Blocking State	Protocol Role
1	RSTP	Forwarding	Designated
2	RSTP	Disabled	Disabled
3	RSTP	Disabled	Disabled
4	RSTP	Disabled	Disabled
5	RSTP	Forwarding	Root
6	RSTP	Disabled	Disabled
7	RSTP	Disabled	Disabled
8	RSTP	Disabled	Disabled

Virtual Ports

Port	Protocol	Blocking State	Protocol Role
52	RSTP	Blocking	Disabled
53	RSTP	Blocking	Disabled
54	RSTP	Blocking	Disabled

Table 4-66 Pop-up window: Redundancy Port Table: Parameters

Parameter	Description
RSTP Port Configuration	Click on “RSTP Port Configuration” to open the “RSTP Port Configuration” window (see “Pop-up window: RSTP Port Configuration” on page 78). Here, you can make your RSTP settings for the individual ports.
Port	This column shows the respective port.
Protocol	This column shows the redundancy protocol selected for this port.
Blocking State	This column shows how the protocol deals with incoming data packets.
Protocol Role	This column shows whether the data packets are sent towards or away from the root.

4.4.4 Current VLANs

On this page, you will find diagnostic information on the current VLANs.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Diagnostics, Current VLANs”.

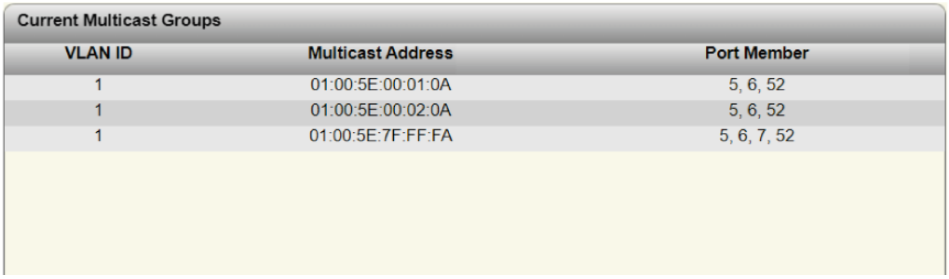
For further information on VLAN, refer to “VLAN – Virtual Local Area Network” on page 159.

4.4.5 Current Multicast Groups

On this page, you will find diagnostic information on the current multicast groups.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Diagnostics, Current Multicast Groups”.

Figure 4-43 Current Multicast Groups



Current Multicast Groups

VLAN ID	Multicast Address	Port Member
1	01:00:5E:00:01:0A	5, 6, 52
1	01:00:5E:00:02:0A	5, 6, 52
1	01:00:5E:7F:FF:FA	5, 6, 7, 52

Table 4-67 Current Multicast Groups: Parameters

Parameter	Description
VLAN ID	The VLAN ID of the corresponding multicast group is displayed here.
Multicast Address	The MAC address of the multicast group is displayed here.
Port Member	The associated ports of the multicast group are displayed here.

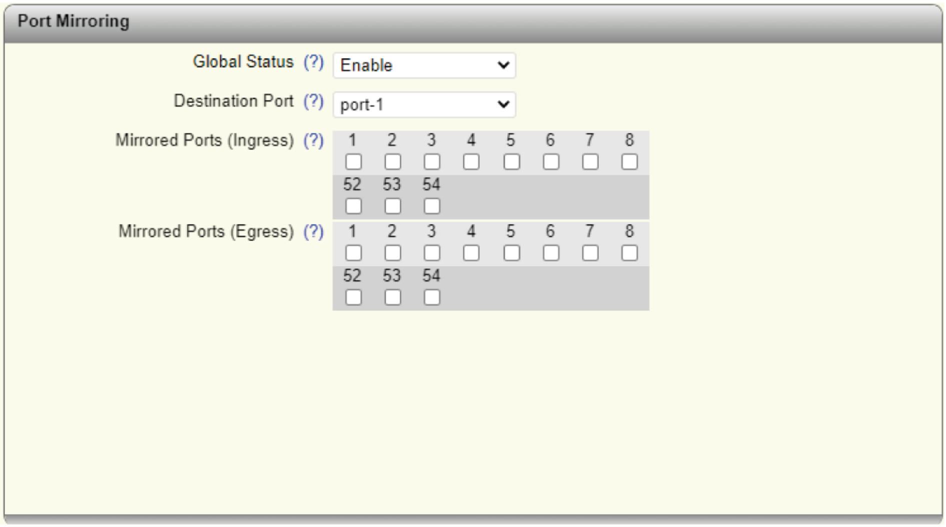
For further information on multicast filtering, refer to “Multicast Filtering” on page 72.

4.4.6 Port Mirroring

Port mirroring allows you to mirror the incoming and outgoing data traffic of individual ports to one port where it can be analyzed using a connected diagnostic device or tool.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Diagnostics, Port Mirroring”.

Figure 4-44 Port Mirroring



Port Mirroring

Global Status (?) Enable

Destination Port (?) port-1

Mirrored Ports (Ingress) (?)

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☐	☐	☐	☐
52	53	54					
☐	☐	☐					

Mirrored Ports (Egress) (?)

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☐	☐	☐	☐
52	53	54					
☐	☐	☐					

Table 4-68 Port Mirroring: Parameters

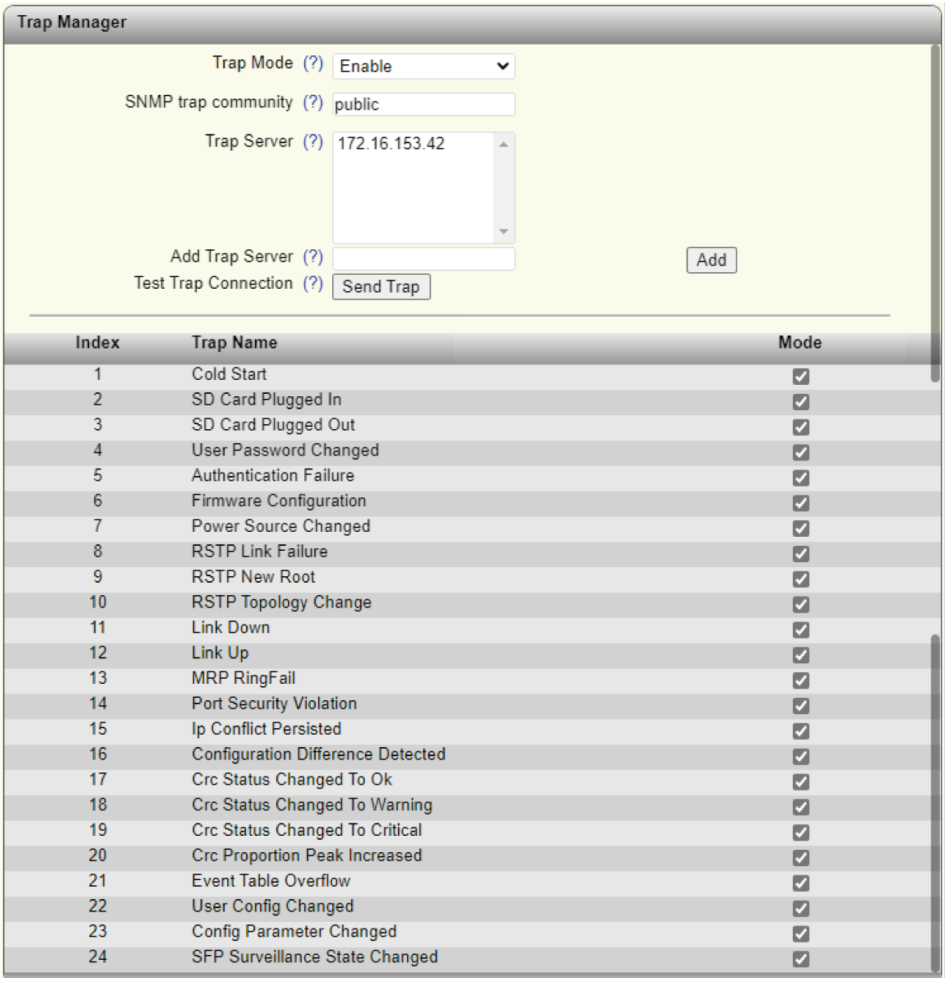
Parameter	Description
Global Status	– Enable: Port mirroring is activated globally. – Disable: Port mirroring is deactivated globally.
Destination Port	Select the port to which the diagnostic device or tool is connected.
Mirrored Ports (Ingress)	Activate the check boxes of the ports from which the incoming data traffic should be mirrored.
Mirrored Ports (Egress)	Activate the check boxes of the ports from which the outgoing data traffic should be mirrored.

4.4.7 Trap Manager

On the “Trap Manager” page you can configure the Trap Manager, which provides notifications when specific events occur. For example, you can be informed about a password change or a firmware change and in this way detect unauthorized access more easily.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Diagnostics, Trap Manager”.

Figure 4-45 Trap Manager



Trap Manager

Trap Mode (?) Enable

SNMP trap community (?) public

Trap Server (?) 172.16.153.42

Add Trap Server (?)

Test Trap Connection (?)

Index	Trap Name	Mode
1	Cold Start	☑
2	SD Card Plugged In	☑
3	SD Card Plugged Out	☑
4	User Password Changed	☑
5	Authentication Failure	☑
6	Firmware Configuration	☑
7	Power Source Changed	☑
8	RSTP Link Failure	☑
9	RSTP New Root	☑
10	RSTP Topology Change	☑
11	Link Down	☑
12	Link Up	☑
13	MRP RingFail	☑
14	Port Security Violation	☑
15	Ip Conflict Persisted	☑
16	Configuration Difference Detected	☑
17	Crc Status Changed To Ok	☑
18	Crc Status Changed To Warning	☑
19	Crc Status Changed To Critical	☑
20	Crc Proportion Peak Increased	☑
21	Event Table Overflow	☑
22	User Config Changed	☑
23	Config Parameter Changed	☑
24	SFP Surveillance State Changed	☑

Table 4-69 Trap Manager: Parameters

Parameter	Description
Trap Mode	– Enable: Sending of SNMP traps is activated. – Disable: Sending of SNMP traps is deactivated.
SNMP trap community	Here, enter the name or string of the SNMP trap community.
Trap Server	All trap servers that are to receive SNMP traps from this device are displayed here.
Add Trap Server	Here, enter the IP address or DNS name of a trap server. Click on “Add” to add the trap server. Click on “Apply&Save” to save this trap server.
Test Trap Connection	Click on “Send Trap” to test the connection to the trap server.

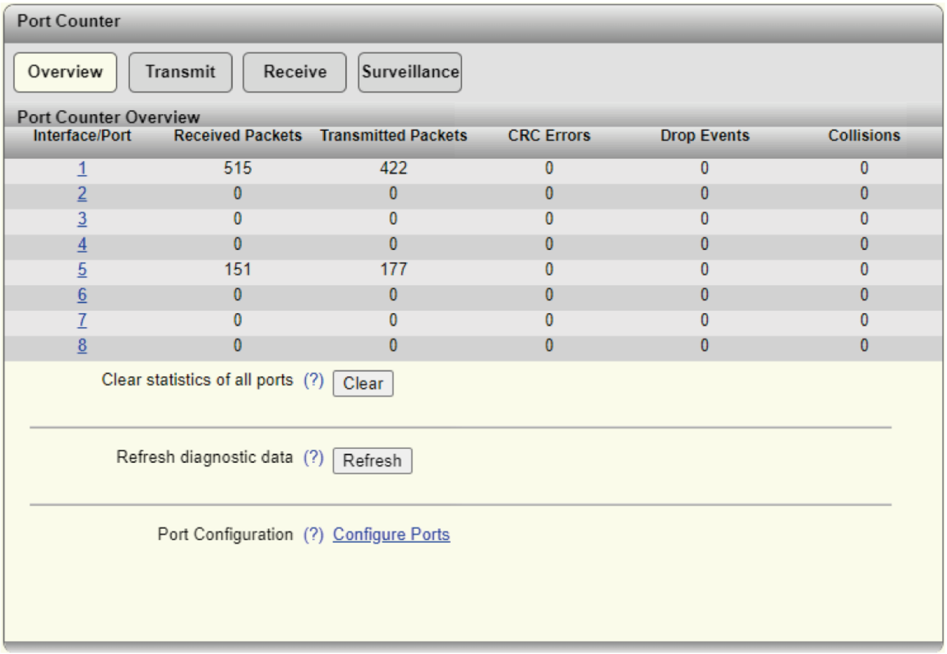
The table lists the SNMP traps that the device can send. Select the actions for which SNMP traps are to be sent. The possible SNMP traps may vary slightly depending on the device version.

4.4.8 Port Counter

This page provides an overview of the port statistics for the device.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Diagnostics, Port Counter”.

Figure 4-46 Port Counter



Port Counter Overview

Interface/Port	Received Packets	Transmitted Packets	CRC Errors	Drop Events	Collisions
1	515	422	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	151	177	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0
8	0	0	0	0	0

Clear statistics of all ports (?) Clear

Refresh diagnostic data (?) Refresh

Port Configuration (?) Configure Ports

Four different views provide an overview of the general, transmitted, and received packets, errors, and collisions on the individual ports.

- Overview: Provides an overview of the general packets.
- Transmit: Provides an overview of the transmitted packets.
- Receive: Provides an overview of the received packets.
- Surveillance: Provides an overview of errors and collisions on the individual ports.

Table 4-70 Port Counter: Parameters

Parameter	Description
Interface/Port	Click on one of the port numbers in the “Interface/Port” column to open the “Port Counter Details” page (see “Pop-up window: Port Counter Details” on page 112). Here you can view detailed statistics for each port. In addition, the current and maximum port utilization is displayed as a percentage.

Table 4-70 Port Counter: Parameters

Parameter	Description
Clear statistics of all ports	Click on “Clear” to reset all of the port counters in the “Overview”, “Transmit”, and “Receive” views. In the “Surveillance” view, you also reset the “CRC Proportion Peak” and “CRC Status” of all ports.
Refresh diagnostic data	Click on “Refresh” to reset the port counter statistics.
Port Configuration	Click on “Configure Ports” to open the “Port Configuration” window (see “Port Configuration” on page 66).

Port Counter: Transmit

Table 4-71 Transmit: Parameters

Parameter	Description
Interface/Port	Click on one of the port numbers in the “Interface/Port” column to open the “Port Counter Details” page (see “Pop-up window: Port Counter Details” on page 112). Here you can view detailed statistics for each port. In addition, the current and maximum port utilization is displayed as a percentage.
Unicast (Tx)	The number of unicasts sent on the selected port since the last counter reset is displayed here.
Multicast (Tx)	The number of multicasts sent on the selected port since the last counter reset is displayed here.
Broadcast (Tx)	The number of broadcasts sent on the selected port since the last counter reset is displayed here.
Collisions	The total number of collisions on the selected port since the last counter reset is displayed here.

Port Counter: Receive

Table 4-72 Receive: Parameters

Parameter	Description
Interface/Port	Click on one of the port numbers in the “Interface/Port” column to open the “Port Counter Details” page (see “Pop-up window: Port Counter Details” on page 112). Here you can view detailed statistics for each port. In addition, the current and maximum port utilization is displayed as a percentage.
Unicast (Rx)	The number of unicasts received on the selected port since the last counter reset is displayed here.
Multicast (Rx)	The number of multicasts received on the selected port since the last counter reset is displayed here.
Broadcast (Rx)	The number of broadcasts received on the selected port since the last counter reset is displayed here.

Table 4-72 Receive: Parameters

Parameter	Description
CRC Errors	The number of CRC errors on the selected port since the last counter reset is displayed here. CRC errors are often caused by noise in the transmission channels.
Drop Events	The total number of events in which packets get lost because the device receives too many packets at once is displayed here.
Oversize	The number of oversized packets received on the selected port since the last counter reset is displayed here.
Undersize	The number of undersized packets received on the selected port since the last counter reset is displayed here.

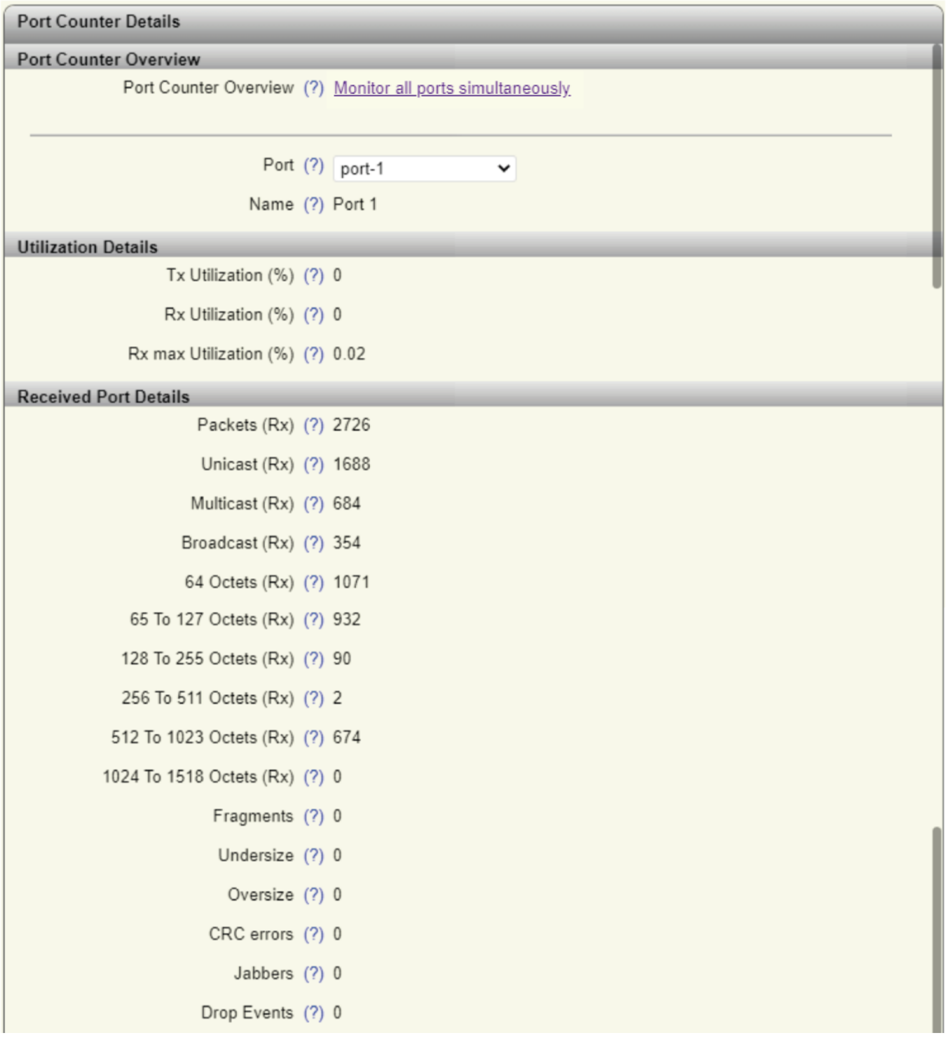
Port Counter: Surveillance

Table 4-73 Surveillance: Parameters

Parameter	Description
Interface/Port	Click on one of the port numbers in the “Interface/Port” column to open the “Port Counter Details” page (see “Pop-up window: Port Counter Details” on page 112). Here you can view detailed statistics for each port. In addition, the current and maximum port utilization is displayed as a percentage.
CRC Errors	The number of CRC errors on the selected port since the last counter reset is displayed here. CRC errors are often caused by noise in the transmission channels.
Crit. Threshold (ppm)	The threshold value at which the CRC port switches to Critical in the event of faulty packets is displayed here. You can set this value for each port on the “Port Configuration” page (see “Port Configuration” on page 66
Proportion Peak (ppm)	The highest value of the CRC port since the last device restart is displayed here.
Status	The status of the CRC port is displayed here. If the proportion of faulty packets exceeds the warning threshold or the threshold value, the status changes to “Warning” or “Critical”.

Pop-up window: Port Counter Details

Figure 4-47 Pop-up window: Port Counter Details (part 1)



Port Counter Details

Port Counter Overview

Port Counter Overview (?) Monitor all ports simultaneously

Port (?) port-1

Name (?) Port 1

Utilization Details

Tx Utilization (%) (?) 0

Rx Utilization (%) (?) 0

Rx max Utilization (%) (?) 0.02

Received Port Details

Packets (Rx) (?) 2726

Unicast (Rx) (?) 1688

Multicast (Rx) (?) 684

Broadcast (Rx) (?) 354

64 Octets (Rx) (?) 1071

65 To 127 Octets (Rx) (?) 932

128 To 255 Octets (Rx) (?) 90

256 To 511 Octets (Rx) (?) 2

512 To 1023 Octets (Rx) (?) 674

1024 To 1518 Octets (Rx) (?) 0

Fragments (?) 0

Undersize (?) 0

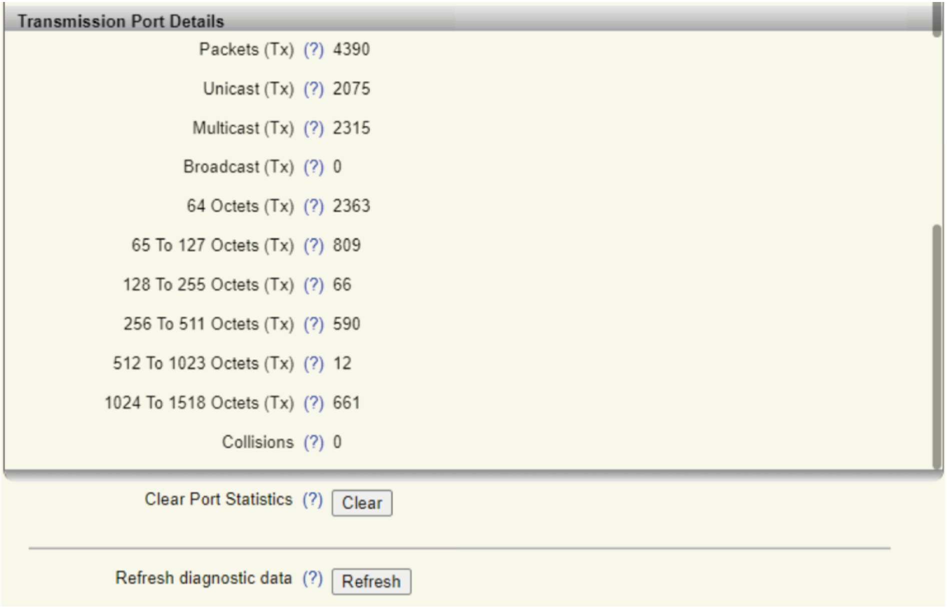
Oversize (?) 0

CRC errors (?) 0

Jabbers (?) 0

Drop Events (?) 0

Figure 4-48 Pop-up window: Port Counter Details (part 2)



Transmission Port Details

Packets (Tx) (?) 4390

Unicast (Tx) (?) 2075

Multicast (Tx) (?) 2315

Broadcast (Tx) (?) 0

64 Octets (Tx) (?) 2363

65 To 127 Octets (Tx) (?) 809

128 To 255 Octets (Tx) (?) 66

256 To 511 Octets (Tx) (?) 590

512 To 1023 Octets (Tx) (?) 12

1024 To 1518 Octets (Tx) (?) 661

Collisions (?) 0

Clear Port Statistics (?) Clear

Refresh diagnostic data (?) Refresh

Pop-up window: Port Counter Details: Port Counter Overview

Table 4-74 Port Counter Overview: Parameters

Parameter	Description
Port Counter Overview	Click on “Monitor all ports simultaneously” to return to the “Port Counter” page (see “Port Counter” on page 109).
Port	Select the port for which you want to adjust the settings.
Name	The name of the selected port is displayed here.
Clear Port Statistics	Click on “Clear” to reset all counters for the selected port.
Refresh diagnostic data	Click on “Refresh” to update the page.

Pop-up window: Port Counter Details: Utilization Details

Table 4-75 Utilization Details: Parameters

Parameter	Description
Tx Utilization (%)	The current utilization in terms of sent data packets is displayed here.
Rx Utilization (%)	The current utilization in terms of received data packets is displayed here.
Rx max Utilization (%)	The maximum utilization in terms of received data packets since the last switch restart is displayed here.

Pop-up window: Port Counter Details: Received Port Details

Table 4-76 Received Port Details: Parameters

Parameter	Description
Packets (Rx)	The total number of packets received on the selected port since the last counter reset is displayed here.
Unicast (Rx)	The number of unicasts received on the selected port since the last counter reset is displayed here.
Multicast (Rx)	The number of multicasts received on the selected port since the last counter reset is displayed here.
Broadcast (Rx)	The number of broadcasts received on the selected port since the last counter reset is displayed here.
64 Octets (Rx)	The number of packets with a length of 64 octets received on the selected port since the last counter reset is displayed here.
65 To 127 Octets (Rx)	The number of packets with a length of 65 to 127 octets received on the selected port since the last counter reset is displayed here.
128 To 255 Octets (Rx)	The number of packets with a length of 128 to 255 octets received on the selected port since the last counter reset is displayed here.
256 To 511 Octets (Rx)	The number of packets with a length of 256 to 511 octets received on the selected port since the last counter reset is displayed here.
512 To 1023 Octets (Rx)	The number of packets with a length of 512 to 1023 octets received on the selected port since the last counter reset is displayed here.
1024 To 1518 Octets (Rx)	The number of packets with a length of 1024 to 1518 octets received on the selected port since the last counter reset is displayed here.
Fragments	The number of fragments received on the selected port since the last counter reset is displayed here.
Undersize	The number of undersized packets received on the selected port since the last counter reset is displayed here.
Oversize	The number of oversized packets received on the selected port since the last counter reset is displayed here.
CRC errors	The number of CRC errors on the selected port since the last counter reset is displayed here. CRC errors are often caused by noise in the transmission channels.
Jabbers	The number of jabbers on the selected port since the last counter reset is displayed here. Jabbers are received packets that are longer than 1518 octets and that contain an incorrect frame check sequence (FCS).
Drop Events	The total number of events in which packets get lost because the device receives too many packets at once is displayed here.

Pop-up window: Port Counter Details: Transmission Port Details

Table 4-77 Transmission Port Details: Parameters

Parameter	Description
Packets (Tx)	The total number of packets sent on the selected port since the last counter reset is displayed here.
Unicast (Tx)	The number of unicasts sent on the selected port since the last counter reset is displayed here.
Multicast (Tx)	The number of multicasts sent on the selected port since the last counter reset is displayed here.
Broadcast (Tx)	The number of broadcasts sent on the selected port since the last counter reset is displayed here.
64 Octets (Tx)	The number of packets with a length of 64 octets sent on the selected port since the last counter reset is displayed here.
65 To 127 Octets (Tx)	The number of packets with a length of 65 to 127 octets sent on the selected port since the last counter reset is displayed here.
128 To 255 Octets (Tx)	The number of packets with a length of 128 to 255 octets sent on the selected port since the last counter reset is displayed here.
256 To 511 Octets (Tx)	The number of packets with a length of 256 to 511 octets sent on the selected port since the last counter reset is displayed here.
512 To 1023 Octets (Tx)	The number of packets with a length of 512 to 1023 octets sent on the selected port since the last counter reset is displayed here.
1024 To 1518 Octets (Tx)	The number of packets with a length of 1024 to 1518 octets sent on the selected port since the last counter reset is displayed here.
Collisions	The total number of collisions on the selected port since the last counter reset is displayed here.

4.4.9 Port Utilization

On this page, you will find an overview of the port utilization for your device displayed as a percentage.

- Open web-based management (see "Accessing web-based management" on page 35) and log in.
- Click on "Diagnostics, Port Utilization".

Figure 4-49 Port Utilization

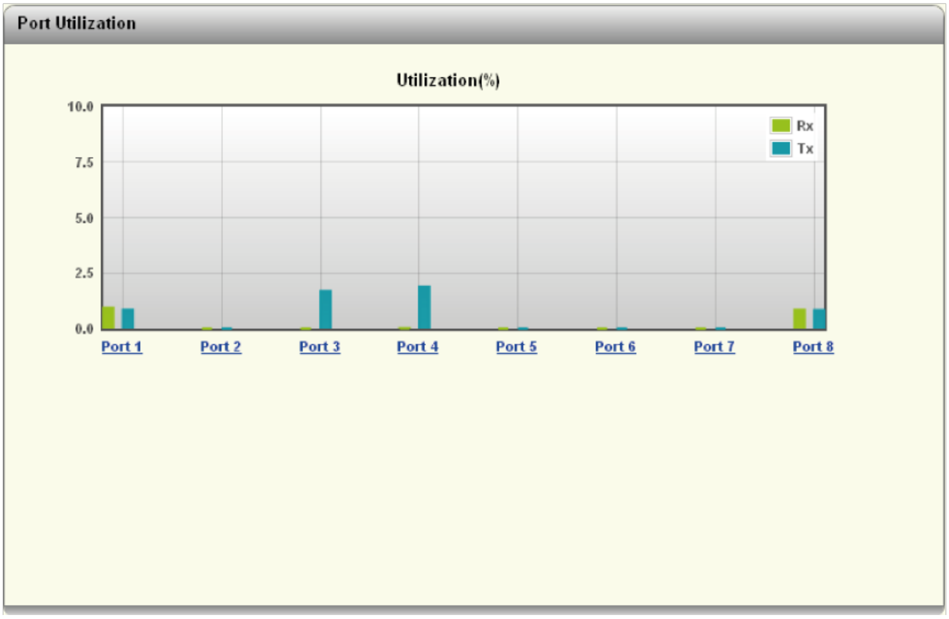


Table 4-78 Port Status: Parameters

Parameter	Description
Port 1–8	Click on a port for a detailed overview of the corresponding port.

4.4.10 Snapshot

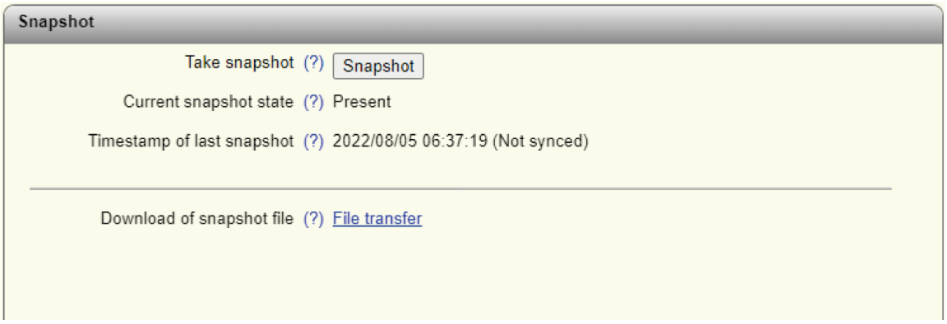
On the “Snapshot” page, you can save device configurations and logs with a click for diagnostic purposes and then download them to send to a service technician for analysis.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Diagnostics, Snapshot”.
- Click on the “Snapshot” button.

⇒ The snapshot of the device is created.

- Click on “File transfer” to download the snapshot (see “File Transfer” on page 129).

Figure 4-50 Snapshot



Snapshot

Take snapshot (?) Snapshot

Current snapshot state (?) Present

Timestamp of last snapshot (?) 2022/08/05 06:37:19 (Not synced)

Download of snapshot file (?) File transfer

Table 4-79 Snapshot: Parameters

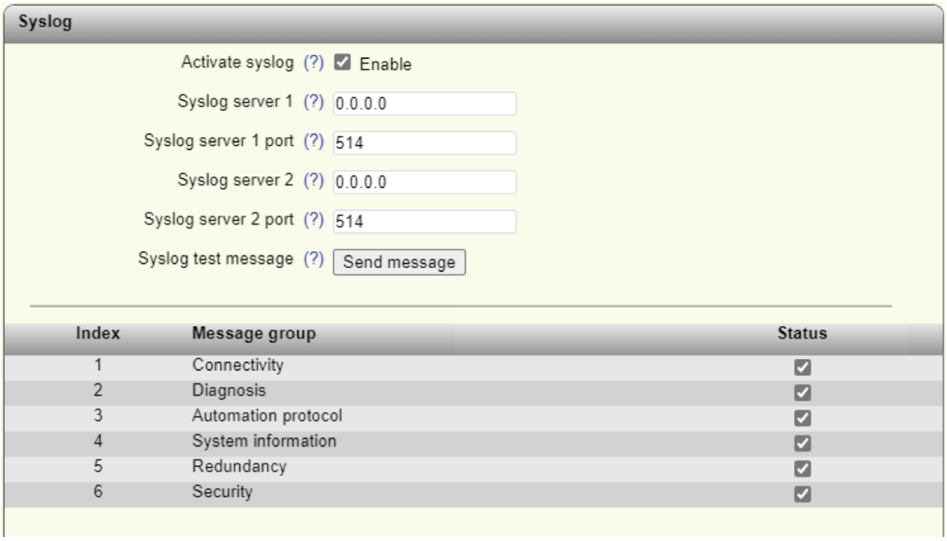
Parameter	Description
Take snapshot	Click on “Snapshot” to create a snapshot of the current device configuration.
Current snapshot state	The snapshot status is displayed here (e.g., whether it is currently being generated, is available, or does not exist).
Timestamp of last snapshot	The time at which the last snapshot was generated is displayed here.
Download of snapshot file	Click on “File transfer” to download the snapshot (see “File Transfer” on page 129).

4.4.11 Syslog for diagnostic purposes

On the “Syslog” page you can transmit messages or events to one or more servers via UDP. This allows you to analyze the environment and the quality of the connection.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Diagnostics, Syslog”.

Figure 4-51 Syslog



Syslog

Activate syslog (?) ☑ Enable

Syslog server 1 (?) 0.0.0.0

Syslog server 1 port (?) 514

Syslog server 2 (?) 0.0.0.0

Syslog server 2 port (?) 514

Syslog test message (?) Send message

Index	Message group	Status
1	Connectivity	☑
2	Diagnosis	☑
3	Automation protocol	☑
4	System information	☑
5	Redundancy	☑
6	Security	☑

Table 4-80 Syslog: Parameters

Parameter	Description
Activate syslog	Activate the check box to activate the Syslog functionality.
Syslog server 1	Here, enter the IP address or DNS name of the first Syslog server.
Syslog server 1 port	Here, enter the UDP port of the first Syslog server. Default: 514.
Syslog server 2	Here, enter the IP address or DNS name of the second Syslog server. If you configure two Syslog servers, all device messages and events are sent to both servers.
Syslog server 2 port	Here, enter the UDP port of the second Syslog server. Default: 514.
Syslog test message	Click on “Send message” to test the connection to the Syslog server. With Syslog, the server does not confirm the receipt of messages. Therefore the connection status can only be checked on the server, and not in web-based management of the device.
Status	Activate the check boxes in the “Status” column to select the categories whose events are to be sent to the Syslog server.

Table 4-81 Syslog

Category	Detail
Connectivity	IP conflict detected
	TFTP connection failed
	ACD conflict detected IP
	LLDP new neighbour on port
	LLDP neighbour information changed on port
	Link monitor alarm raises on port
	IP address changed on interface
	Port Link up/down
	SFP module plugged on Port
	ACD device has no IP
	MTU size changed
Diagnosis	CRC status and peak on port reset
	CRC status on port changed to ok
	CRC status on port changed to critical
	CRC thresholds on port changed by user
	Alarm output failed
	CRC status on port changed to warning
Automation protocol	PROFINET diagnosis available
	IP address changed via PROFINET
	Name of the device changed via PROFINET
	PROFINET connection lost
	PROFINET module different on slot

Category	Detail
System information	System time synchronized
	Pluggable memory removed
	Update firmware successful
	Configuration saved/loaded on/from pluggable memory
	Update failed
	Configuration difference detected
	Configuration saved/loaded successfully
	Configuration parameter changed
	Smart Mode entered
	Smart Mode button enabled/disabled
	SD card slot enabled/disabled
	Error in configuration file
	Pluggable memory cleared
	New interface created
	Power supply lost
	Name of the device changed
	Parameter has been changed by the user
	FW image not valid
	Update processing
	Write to flash memory
	Wrong update image
	IGMP Snooping mode changed
	IGMP Snooping aging time changed
	Syslog test message
	Start FW update
	Write FW image into flash
Redundancy	RSTP ring detected
	RSTP topology changed
	RSTP root changed
	RSTP ring failed
	MRP client/manager activated
	MRP ring failed
	MRP link failed at port

Category	Detail
Security	Port access violation on Port
	Radius Authentication Server shared secret changed
	Port successfully authenticated
	Password changed
	User authentication failed
	Radius Authentication Server IP/UDP address changed
	User configuration changed
	User Login/Logout
	Unauthorized access

4.4.12 SFP Diagnostics (only devices with SFP ports)

On this page, you will find information on the SFP ports.

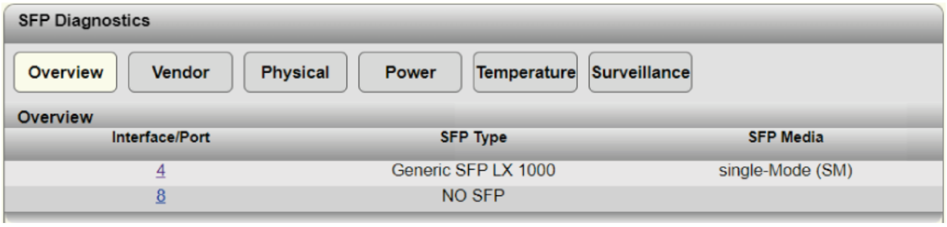
This page is only available on devices with SFP ports. Not every SFP module makes all of the data requested from the switch available.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Diagnostics, SFP Diagnostics”.

The “Overview”, “Vendor”, “Physical”, “Power”, and “Temperature” areas provide various diagnostic data made available by the respective SFP modules used. The data provided largely follows the Digital Diagnostic Monitoring Interface (DDMI) in accordance with SFF-8472 Rev 9.3.

“Overview” area

Figure 4-52 SFP Diagnostics: Overview

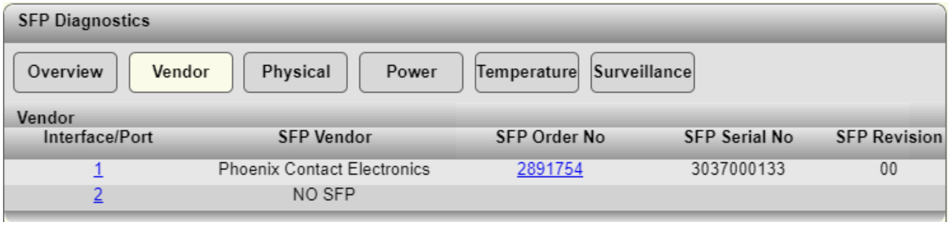


Interface/Port	SFP Type	SFP Media
4	Generic SFP LX 1000	single-Mode (SM)
8	NO SFP	

Table 4-82 SFP Diagnostics: Overview: Parameters

Parameter	Description
Interface/Port	The ports that can be used with SFP modules are displayed here. Click on a port number to open the “SFP Diagnostics Details” window for this port (see “SFP Diagnostics Details” on page 125). There you will find all the SFP details at a glance.
SFP Type	The type of SFP module used is displayed here. If no SFP module is inserted, “NO SFP” is displayed.
SFP Media	This column shows whether a multimode or singlemode SFP module is present.

"Vendor" area



Interface/Port	SFP Vendor	SFP Order No	SFP Serial No	SFP Revision
1	Phoenix Contact Electronics	2891754	3037000133	00
2	NO SFP			

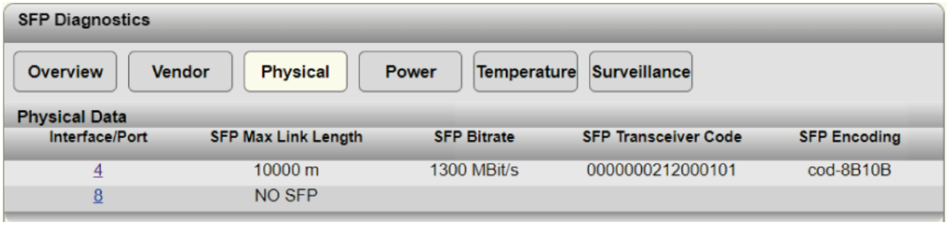
Figure 4-53 SFP Diagnostics: Vendor

Table 4-83 SFP Diagnostics: Vendor: Parameters

Parameter	Description
Interface/Port	The ports that can be used with SFP modules are displayed here. Click on a port number to open the “SFP Diagnostics Details” window for this port (see “SFP Diagnostics Details” on page 125). There you will find all the SFP details at a glance.
SFP Vendor	The manufacturer of the SFP module is displayed here. If no SFP module is inserted, “NO SFP” is displayed.
SFP Order No	The order number of the SFP module used is displayed here. If you are using a Phoenix Contact SFP module, click on the order number to go to the product page.
SFP Serial No	The serial number of the SFP module used is displayed here.
SFP Revision	The item revision of the SFP module used is displayed here.

“Physical” area

Figure 4-54 SFP Diagnostics: Physical



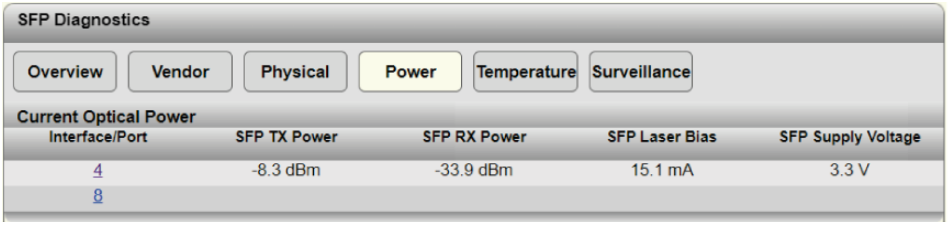
Interface/Port	SFP Max Link Length	SFP Bitrate	SFP Transceiver Code	SFP Encoding
4	10000 m	1300 MBit/s	0000000212000101	cod-8B10B
8	NO SFP			

Table 4-84 SFP Diagnostics: Physical: Parameters

Parameter	Description
Interface/Port	The ports that can be used with SFP modules are displayed here. Click on a port number to open the “SFP Diagnostics Details” window for this port (see “SFP Diagnostics Details” on page 125). There you will find all the SFP details at a glance.
SFP Max Link Strength	The maximum supported SFP module link length in meters is displayed here. If no SFP module is inserted, “NO SFP” is displayed.
SFP Bitrate	The nominal bit rate of the SFP module is displayed here. The bit rate includes the bits that are required for coding and delimiting the signal and the bits that carry data information. Therefore, it explicitly does not refer to the transmission speed available on the port.
SFP Transceiver Code	The transceiver code of the SFP module is displayed here. The transceiver code describes the electronic or optical interfaces that are supported by the transceiver. For optical receivers, values such as the fiber channel speed, transmission media, transmitter technology, and distance capability should be indicated.
SFP Encoding	The serial encryption mechanism of the SFP module is displayed here.

“Power” area

Figure 4-55 SFP Diagnostics: Power



Current Optical Power

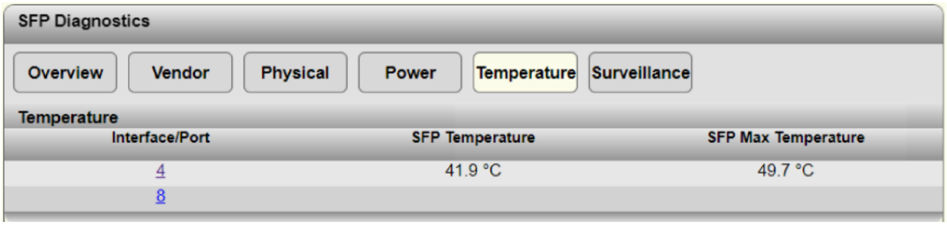
Interface/Port	SFP TX Power	SFP RX Power	SFP Laser Bias	SFP Supply Voltage
4	-8.3 dBm	-33.9 dBm	15.1 mA	3.3 V
8				

Table 4-85 SFP Diagnostics: Power: Parameters

Parameter	Description
Interface/Port	The ports that can be used with SFP modules are displayed here. Click on a port number to open the “SFP Diagnostics Details” window for this port (see “SFP Diagnostics Details” on page 125). There you will find all the SFP details at a glance.
SFP TX Power	The current outgoing power level is displayed in dBm here.
SFP RX Power	The current incoming power level is displayed in dBm here.
SFP Laser Bias	The current laser bias current strength of the SFP module used is displayed in mA here.
SFP Supply Voltage	The current power supply of the SFP module used is displayed in V here.

“Temperature” area

Figure 4-56 SFP Diagnostics: Temperature



Temperature

Interface/Port	SFP Temperature	SFP Max Temperature
4	41.9 °C	49.7 °C
8		

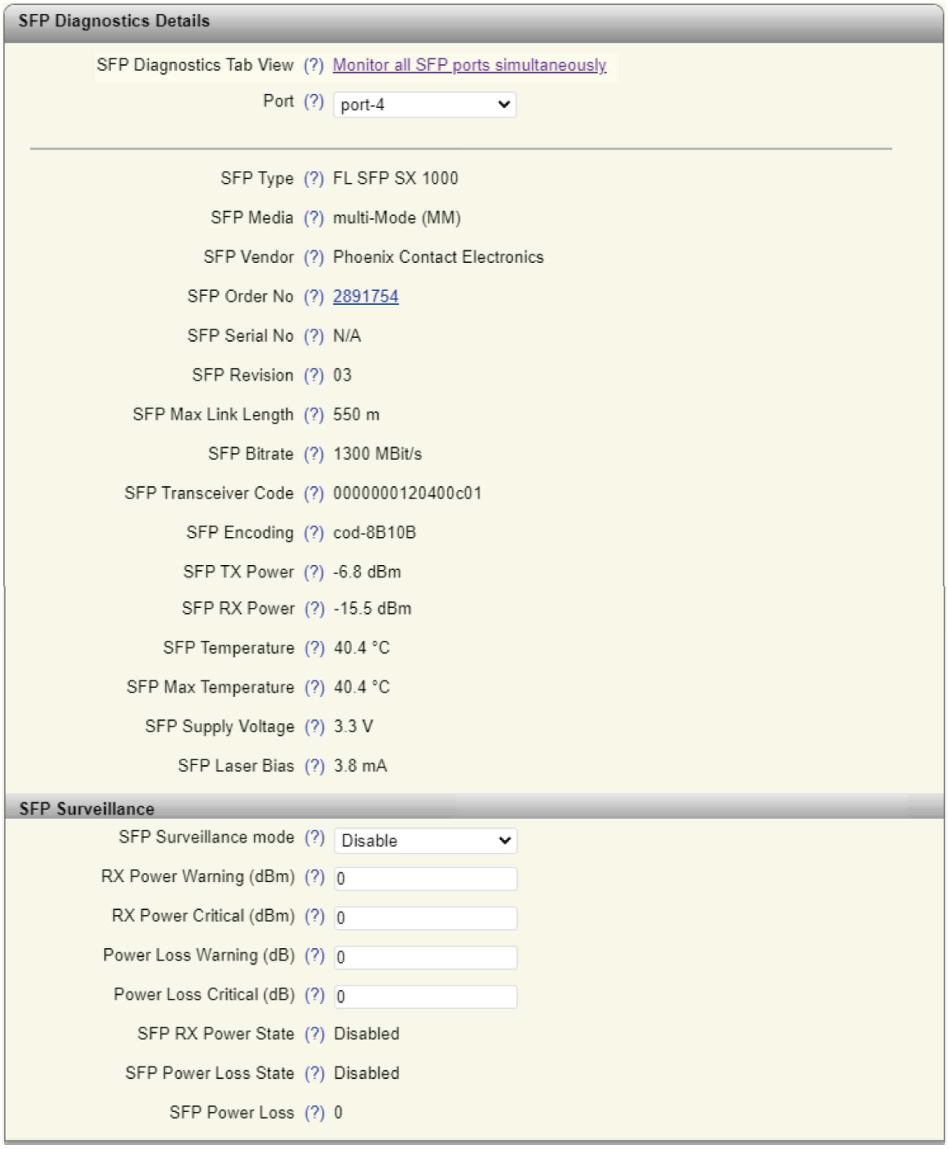
Table 4-86 SFP Diagnostics: Temperature: Parameters

Parameter	Description
Interface/Port	The ports that can be used with SFP modules are displayed here. Click on a port number to open the “SFP Diagnostics Details” window for this port (see “SFP Diagnostics Details” on page 125). There you will find all the SFP details at a glance.
SFP Temperature	The current temperature in °C measured in the SFP module is displayed here.
SFP Top Temperature	The maximum temperature in °C measured in the SFP module since the last switch restart is displayed here.

The SFP Top Temperature on a port can only be reset via a device restart. Even replacing an SFP module on a port **does not** cause the SFP Top Temperature value to be reset.

SFP Diagnostics Details

The SFP Diagnostics Details page provides a summary of all diagnostic information on the SFP module used.



SFP Diagnostics Details

SFP Diagnostics Tab View (?) Monitor all SFP ports simultaneously

Port (?) port-4

SFP Type (?) FL SFP SX 1000

SFP Media (?) multi-Mode (MM)

SFP Vendor (?) Phoenix Contact Electronics

SFP Order No (?) 2891754

SFP Serial No (?) N/A

SFP Revision (?) 03

SFP Max Link Length (?) 550 m

SFP Bitrate (?) 1300 MBit/s

SFP Transceiver Code (?) 0000000120400c01

SFP Encoding (?) cod-8B10B

SFP TX Power (?) -6.8 dBm

SFP RX Power (?) -15.5 dBm

SFP Temperature (?) 40.4 °C

SFP Max Temperature (?) 40.4 °C

SFP Supply Voltage (?) 3.3 V

SFP Laser Bias (?) 3.8 mA

SFP Surveillance

SFP Surveillance mode (?) Disable

RX Power Warning (dBm) (?) 0

RX Power Critical (dBm) (?) 0

Power Loss Warning (dB) (?) 0

Power Loss Critical (dB) (?) 0

SFP RX Power State (?) Disabled

SFP Power Loss State (?) Disabled

SFP Power Loss (?) 0

Figure 4-57 SFP Diagnostics Details

Table 4-87 SFP Diagnostics Details: Parameters

Parameter	Description
SFP Diagnostics Tab View	Click on “Monitor all SFP ports simultaneously” to return to the “SFP Diagnostics” page (see ““Overview” area” on page 121).
Port	Select the port you wish to configure.
SFP Type	The Gigabit Ethernet conformity type of the selected port is displayed here.

Table 4-87 SFP Diagnostics Details: Parameters

Parameter	Description
SFP Media	The media type that should be used with this SFP module is displayed here. ℹ For multimode modules, pay attention to different core diameters.
SFP Vendor	The name of the SFP module manufacturer is displayed here.
SFP Order No	The order number of the SFP module is displayed here. If you are using a Phoenix Contact product, you can click on the order number to open the corresponding page in the e-shop.
SFP Serial No	The serial number of the SFP module is displayed here.
SFP Revision	The revision number of the SFP module is displayed here.
SFP Max Link Length	The maximum link length in meters supported by this SFP module is displayed here.
SFP Bitrate	The nominal bit rate of the SFP module is displayed here.
SFP Transceiver Code	A code in hexadecimal format for the electronic or optical compatibility is displayed here.
SFP Encoding	The encoding mechanism of the SFP module is displayed here.
SFP TX Power	The current optical power of the transmission unit is displayed here in increments of 0.1 dBm.
SFP RX Power	The current optical power that is received is displayed here in increments of 0.1 dBm.
SFP Temperature	The current temperature in °C measured in the SFP module is displayed here.
SFP Top Temperature	The maximum temperature in °C measured in the SFP module since the last switch restart is displayed here.
SFP Supply Voltage	The current supply voltage of the SFP module in V is displayed here.
SFP Laser Bias	The current laser bias current of the SFP module in mA is displayed here.

SFP Diagnostics Details: SFP Surveillance

Table 4-88 SFP Surveillance: Parameters

Parameter	Description
SFP Surveillance mode	Select whether surveillance mode should be activated for the selected port.
RX Power Warning (dBm)	Enter a value in dBm at which a warning about incoming voltage will be displayed. Enter “0” to deactivate surveillance of the threshold value.
RX Power Critical (dBm)	Enter a value in dBm at which a warning about incoming voltage will be displayed. Enter “0” to deactivate surveillance of the threshold value.

Table 4-88 SFP Surveillance: Parameters

Parameter	Description
Power Loss Warning (dB)	Enter a value in dB at which a warning will be displayed. Enter “0” to deactivate surveillance of the threshold value.
Power Loss Critical (dB)	Enter a value in dB at which a warning will be displayed. Enter “0” to deactivate surveillance of the threshold value.
SFP RX Power State	The current status of the optical power is displayed here.
SFP Power Loss State	The current status of the power loss is displayed here.
SFP Power Loss	The current power loss is displayed here in increments of 0.1 dB.

4.5 Firmware update

You can perform a firmware update directly via web-based management.

NOTE: We recommend that you always install the latest firmware revision.
All devices can be updated to a more current firmware version regardless of their delivery state. Firmware updates are available on the Phoenix Contact website.

We explicitly advise against installing firmware revisions that are older than the one supplied on delivery. Continuous improvements, for example, for the bootloader, may prevent compatibility with older firmware revisions.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, System”.
- Click on “Update Firmware”.

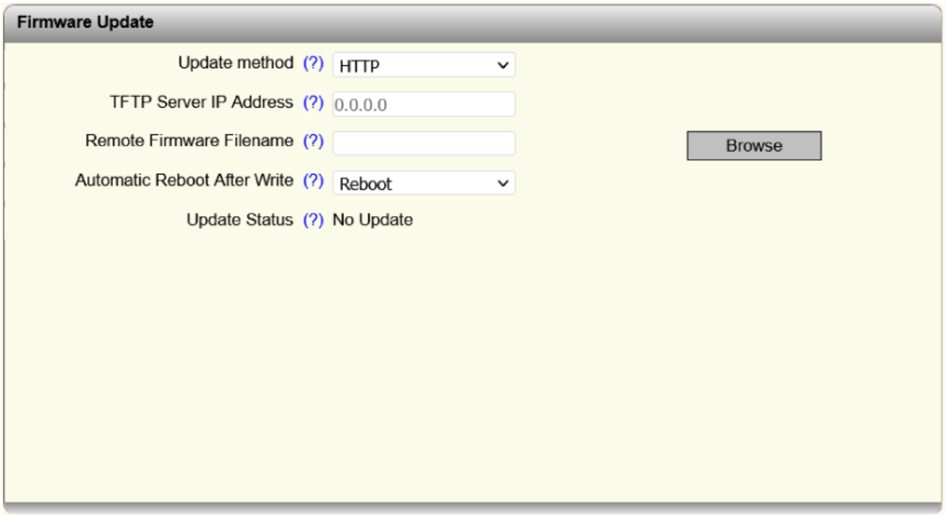
⇒ The “Firmware Update” dialog opens.

Configuration settings of the device may be lost when you downgrade the firmware.

4.5.1 Update via HTTP

- Select “HTTP” for “Update method”.

Figure 4-58 Update via HTTP



Firmware Update

Update method (?) HTTP

TFTP Server IP Address (?) 0.0.0.0

Remote Firmware Filename (?)

Automatic Reboot After Write (?) Reboot

Update Status (?) No Update

- Click on “Browse” and select the directory containing the new firmware.

The firmware file type is “.bin”.

- For “Automatic Reboot After Write”, select whether the device should be automatically restarted after the update.
- Click on “Apply”.

⇒ The firmware is downloaded. The update status is displayed under “Update Status”.

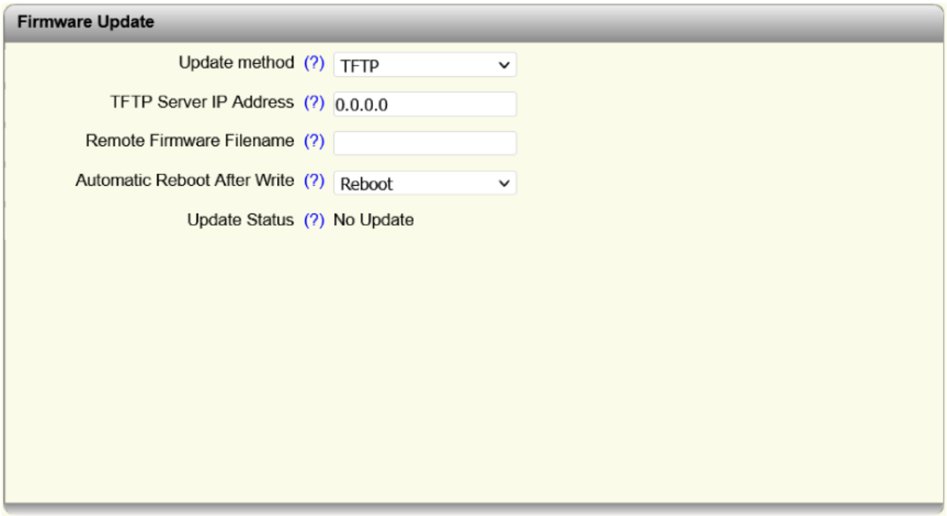
- Wait until “Update Status” shows the message “Firmware Update successful”.
- Close the “Firmware Update” window.

To activate the new firmware, you must restart the device.

4.5.2 Update via TFTP

- Select “TFTP” for “Update method”.

Figure 4-59 Update via TFTP



Firmware Update

Update method (?) TFTP

TFTP Server IP Address (?) 0.0.0.0

Remote Firmware Filename (?)

Automatic Reboot After Write (?) Reboot

Update Status (?) No Update

- For “TFTP Server IP Address”, enter the IP address of the TFTP server.
- For “Remote Firmware Filename”, enter the file path and name of the firmware file.
- Click on “Apply”.

⇒ The firmware is downloaded. The update status is displayed under “Update Status”.

- Wait until “Update Status” shows the message “Firmware Update successful”.
- Close the “Firmware Update” window.

To activate the new firmware, you must restart the device.

4.6 File Transfer

You can perform data transmission directly via web-based management.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, System”.
- Click on “Further configuration handling options”.

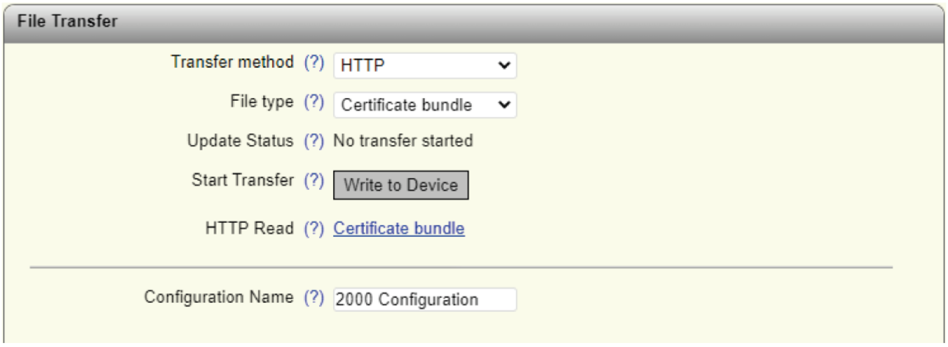
⇒ The “File Transfer” pop-up window opens.

4.6.1 Transfer via HTTP

- Select “HTTP” for “Transfer method”.

Transferring configuration files or certificate bundle

Figure 4-60 File Transfer HTTP: Configuration files or certificate bundle


File Transfer

Transfer method (?) HTTP

File type (?) Certificate bundle

Update Status (?) No transfer started

Start Transfer (?) Write to Device

HTTP Read (?) Certificate bundle

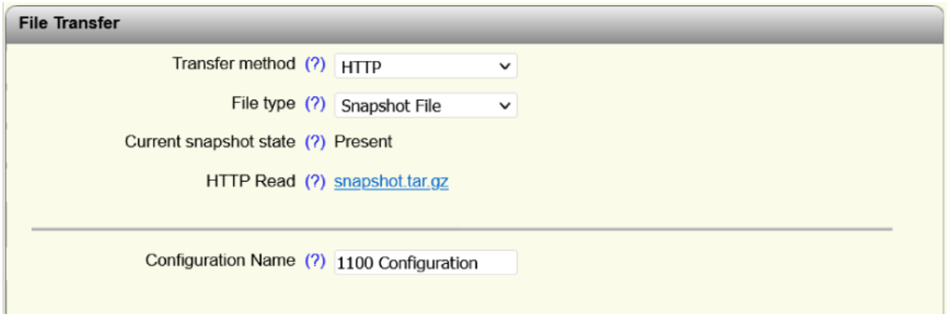
Configuration Name (?) 2000 Configuration

- Select “Configuration” or “Certificate bundle” for “File type”.
- Optionally, enter a name for your configuration or your certificate bundle in the “Configuration Name” field.
- Click on “Write to Device” to select a file on your PC that is to be transferred to the device.
- Click on the “config.cfg” link to download the active configuration to your PC.

⇒ The selected file is uploaded or downloaded. The current status is displayed under “Update Status”.

Transferring snapshot files

Figure 4-61 File Transfer HTTP: Snapshot


File Transfer

Transfer method (?) HTTP

File type (?) Snapshot File

Current snapshot state (?) Present

HTTP Read (?) snapshot.tar.gz

Configuration Name (?) 1100 Configuration

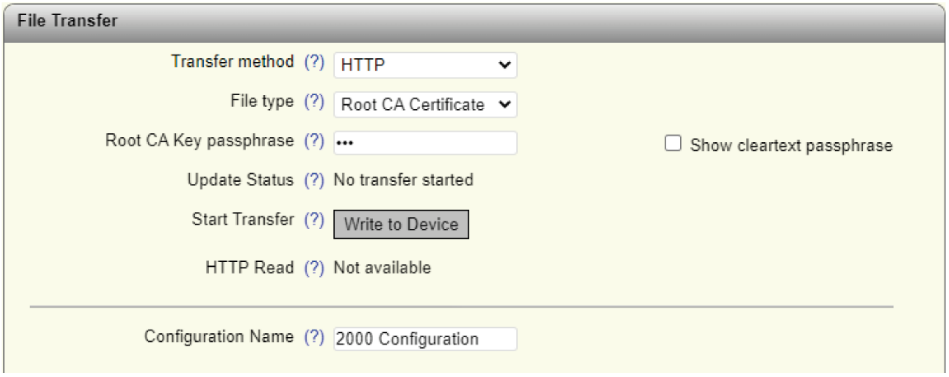
First you need to create a snapshot, see “Snapshot” on page 117.

- Select “Snapshot” for “File type”.
- Optionally, enter a name for your snapshot file in “Configuration Name”.
- Click on “snapshot.tar.gz” to download the snapshot to your PC.

⇒ The snapshot file is downloaded to your PC.

Transferring root CA certificate files

Figure 4-62 File Transfer HTTP: Root CA Certificate



File Transfer

Transfer method (?) HTTP

File type (?) Root CA Certificate

Root CA Key passphrase (?) •••

□ Show cleartext passphrase

Update Status (?) No transfer started

Start Transfer (?) Write to Device

HTTP Read (?) Not available

Configuration Name (?) 2000 Configuration

- Select “Root CA Certificate” for “File type”.
- Enter the password in “Root CA Key passphrase” to decrypt the root CA private key.
- Optionally, enter a name for your root CA certificate in the “Configuration Name” field.
- Click on “Write to Device” to select a file on your PC that is to be transferred to the device. The file extension is *.pfx or *.pem. Note that for both formats, certificate and the root CA private key have to be included in one file.

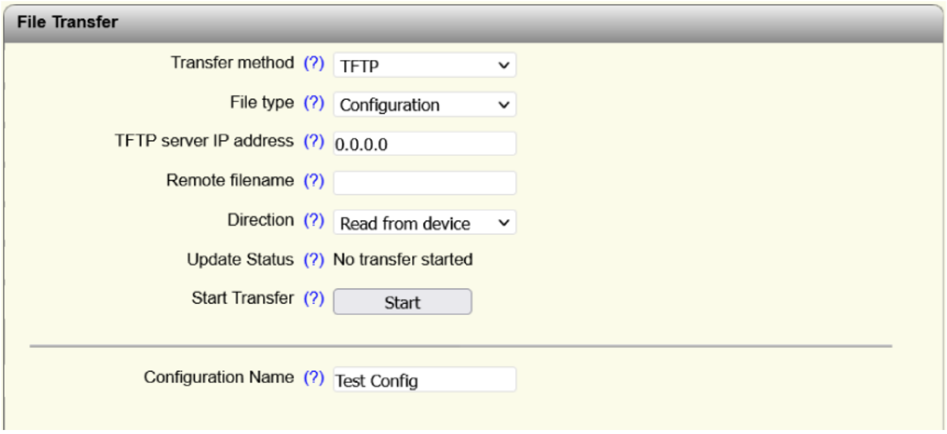
⇒ The selected file is downloaded to the device. The current status is displayed under “Update Status”.

4.6.2 Transfer via TFTP

- Select “TFTP” for “Transfer method”.

Transferring configuration files or certificate bundle

Figure 4-63 File Transfer TFTP: Configuration files or certificate bundle



File Transfer

Transfer method (?) TFTP

File type (?) Configuration

TFTP server IP address (?) 0.0.0.0

Remote filename (?)

Direction (?) Read from device

Update Status (?) No transfer started

Start Transfer (?) Start

Configuration Name (?) Test Config

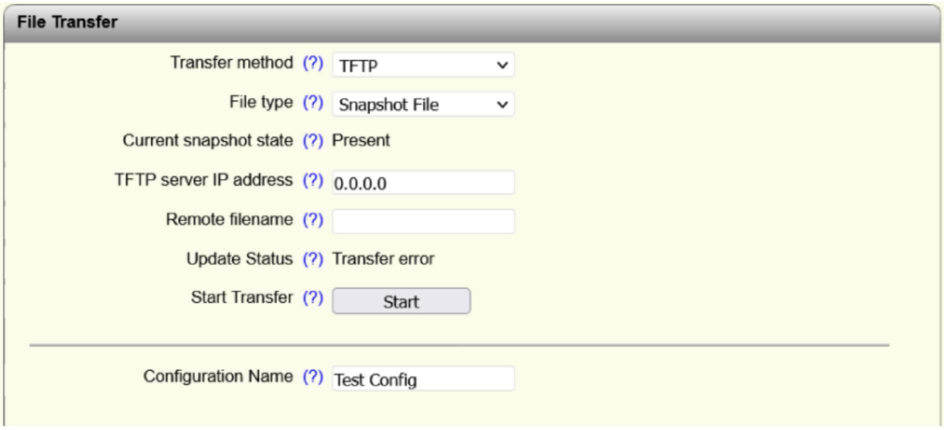
- Select “Configuration” or “Certificate bundle” for “File type”.
- For “TFTP server IP address”, enter the IP address of the TFTP server.
- For “Remote filename”, specify the file name including file extension. The file extension is *.cfg for a configuration file or *.ctx for a security bundle.

- For “Direction”, select whether the file should be uploaded to or downloaded from the device.
  - Select “Read from device” to download the file from the device to the PC.
  - Select “Write to device” to upload the file to the device.
- Optionally, enter a name for your configuration or your certificate bundle in the “Configuration Name” field.
- Click on “Start” to start the transfer.

⇒ The selected file is uploaded or downloaded. The current status is displayed under “Update Status”.

Transferring snapshot files

Figure 4-64 File Transfer TFTP: Snapshot



File Transfer

Transfer method (?)	TFTP
File type (?)	Snapshot File
Current snapshot state (?)	Present
TFTP server IP address (?)	0.0.0.0
Remote filename (?)	
Update Status (?)	Transfer error
Start Transfer (?)	Start
Configuration Name (?)	Test Config

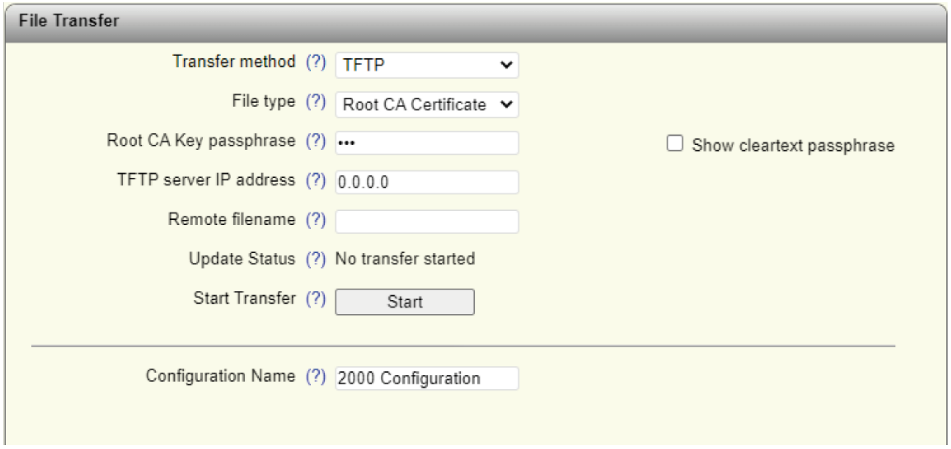
First you need to create a snapshot, see “Snapshot” on page 117.

- Select “Snapshot” for “File type”.
- For “TFTP server IP address”, enter the IP address of the TFTP server.
- For “Remote filename”, specify the file name including file extension. The file extension for a snapshot file is *.tar.gz.
- Optionally, enter a name for your snapshot file in “Configuration Name”.
- Click on “Start” to download the snapshot to your PC.

⇒ The snapshot file is downloaded to your PC. The current status is displayed under “Update Status”.

Transferring root CA certificate files

Figure 4-65 File Transfer TFTP: Root CA certificate



File Transfer

Transfer method (?) TFTP

File type (?) Root CA Certificate

Root CA Key passphrase (?) •••

□ Show cleartext passphrase

TFTP server IP address (?) 0.0.0.0

Remote filename (?)

Update Status (?) No transfer started

Start Transfer (?) Start

Configuration Name (?) 2000 Configuration

- Select “Root CA Certificate” for “File type”.
- Enter the password in “Root CA Key passphrase” to decrypt the root CA private key.
- For “TFTP server IP address”, enter the IP address of the TFTP server.
- For “Remote filename”, specify the file name including file extension. The file extension is *.pfx or *.pem. Note that for both formats, certificate and the root CA private key have to be included in one file.
- Optionally, enter a name for your root CA certificate in the “Configuration Name” field.
- Click on “Start” to start the transfer to the device.

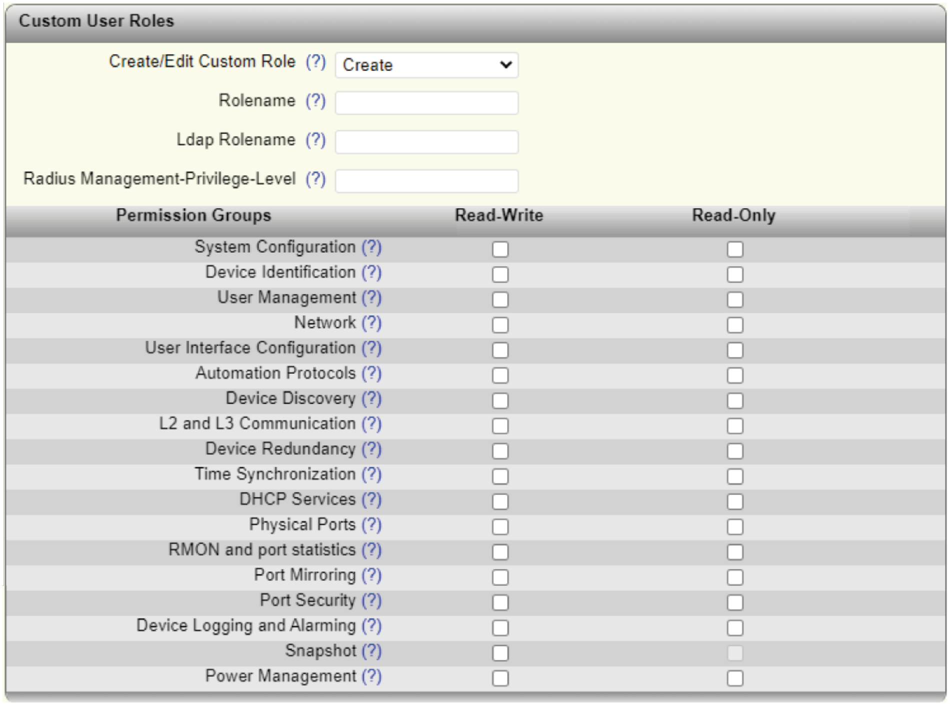
⇒ The selected file is downloaded to the device. The current status is displayed under “Update Status”.

4.7 Creating user roles

As of firmware version 2.70, you can create custom user roles and assign detailed rights via the “Custom User Roles” pop-up window. You can choose between read permission (“Read-Only”), read and write permission (“Read-Write”), or no permission.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, User Management”.
- Click on “Custom User Roles”.

Figure 4-66 Custom User Roles



Custom User Roles

Create/Edit Custom Role (?)	Create
Rolename (?)	
Ldap Rolename (?)	
Radius Management-Privilege-Level (?)	

Permission Groups	Read-Write	Read-Only
System Configuration (?)	□	□
Device Identification (?)	□	□
User Management (?)	□	□
Network (?)	□	□
User Interface Configuration (?)	□	□
Automation Protocols (?)	□	□
Device Discovery (?)	□	□
L2 and L3 Communication (?)	□	□
Device Redundancy (?)	□	□
Time Synchronization (?)	□	□
DHCP Services (?)	□	□
Physical Ports (?)	□	□
RMON and port statistics (?)	□	□
Port Mirroring (?)	□	□
Port Security (?)	□	□
Device Logging and Alarming (?)	□	□
Snapshot (?)	□	□
Power Management (?)	□	□

- Select “Create” for “Create/Edit Custom Role” to create a new user role.
- Enter a name for the user role in “Rolename”.
- Optionally, makes entries in “Ldap Rolename” and “Radius Management-Privilege-Level” to connect the new user role to the LDAP and RADIUS server.
- Activate the desired check boxes under “Permission Groups”. If you omit to activate a check box in a row, the user role will not have access to these settings.

Table 4-89 Custom User Roles: Explanation of permission groups

Permission group	Description
System Configuration	The following pages/functions can be edited and/or viewed with this user role: – Firmware updates – Creating and importing a configuration file – Resetting the device to default settings – File transfer
Device Identification	The following pages/functions can be edited and/or viewed with this user role: – Device names – Device location, contact, device description
User Management	The following pages/functions can be edited and/or viewed with this user role: – Creating, editing, and deleting user roles

Table 4-89 Custom User Roles: Explanation of permission groups

Permission group	Description
Network	The following pages/functions can be edited and/or viewed with this user role: – Network parameters such as IP address and host name ℹ DHCP services cannot be edited with this permission.
User Interface Configuration	The following pages/functions can be edited and/or viewed with this user role: – Configuring and deactivating interfaces such as WBM, CLI, and SNMP – Editing, exporting, and importing certificate management
Automation Protocols	The following pages/functions can be edited and/or viewed with this user role: – Automation – Operating Mode – PROFINET Settings
Device Discovery	The following pages/functions can be edited and/or viewed with this user role: – Device Discovery (LLDP)
L2 and L3 Communication	The following pages/functions can be edited and/or viewed with this user role: – VLAN – Multicast – QoS – MAC table
Device Redundancy	The following pages/functions can be edited and/or viewed with this user role: – Redundancy functions (RSTP, MRP, LAG)
Time Synchronization	The following pages/functions can be edited and/or viewed with this user role: – Time synchronization – Setting up an SNTP server
DHCP Services	The following pages/functions can be edited and/or viewed with this user role: – DHCP Services: Setting up a DHCP server
Physical Ports	The following pages/functions can be edited and/or viewed with this user role: – Port Configuration – Port Configuration Table
RMON and port statistics	The following pages/functions can be edited and/or viewed with this user role: – RMON (Port Counter, CRC Monitoring)

Table 4-89 Custom User Roles: Explanation of permission groups

Permission group	Description
Port Mirroring	The following pages/functions can be edited and/or viewed with this user role: – Port Mirroring
Port Security	The following pages/functions can be edited and/or viewed with this user role: – Port-based security: 802.1X, RADIUS, MAC-based security
Routing and NAT	The following pages/functions can be edited and/or viewed with this user role: – Routing parameters – NAT parameters ℹ To be able to fully configure the routing and NAT parameters, the user role additionally requires read-write permission for "L2 and L3 Communication".
Device Logging and Alarming	The following pages/functions can be edited and/or viewed with this user role: – Syslog – Event table – SNMP Trap Manager
Snapshot	The following pages/functions can be edited and/or viewed with this user role: – Creating and downloading a snapshot ℹ "Read-Only" permission is not available for this permission group. "Read/write" permission is required to create a snapshot.
Power Management	This option is only available on the SPE versions. The following pages/functions can be edited and/or viewed with this user role: – Power Management – Power Diagnostics

- Confirm your settings with "Apply&Save".
- Click on "Configuration, User Management".
- For "Create/Edit User", select the user to whom you want to assign the user role. Alternatively, create a new user.
- For "User Role", select the desired role.
- Confirm your settings with "Apply&Save".

5 RSTP – Rapid Spanning Tree Protocol

This function is not available on the SPE ports.

5.1 Terms

Loops

The RSTP protocol enables the use of Ethernet networks with redundant data paths. These networks form a meshed topology, initially with impermissible loops. These loops can lead to data packets circulating endlessly within the network or even being duplicated. As a consequence, the network becomes overloaded due to circulating data packets. Communication is interrupted.

Therefore, the meshed structure is replaced with a logical, deterministic path using the Rapid Spanning Tree algorithm. The path has a tree structure which no longer contains any loops. In the event of data path failures, some of the previously disabled connections are reconnected. This ensures that the network operates without interruption.

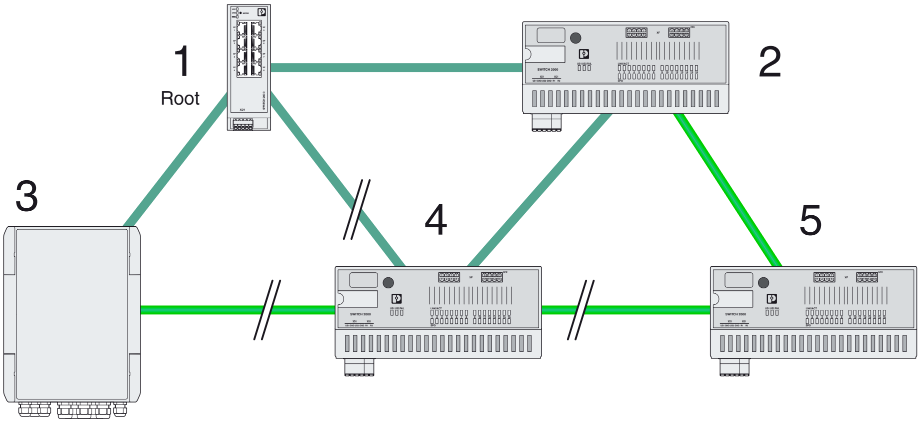
IEEE 802.1D-2004

The RSTP protocol supported by the FL SWITCH 2000 and FL NAT 2000 product families is standardized in the IEEE 802.1D-2004 standard. RSTP is event-driven. As a result, the switch-over times are significantly shorter than with time-based STP.

Example

To ensure continued access to all devices in the network in the event of a data path failure, there are six redundant paths in the following network topology. These redundant paths are impermissible loops. The RSTP protocol automatically converts this topology into a tree by disabling selected ports. In this case the root (root bridge) of the tree is one switch. Every other switch can be accessed from the root bridge via just one data path.

Figure 5-1 Possible tree structure with RSTP



Root bridge

The switch with the lowest bridge priority is the root bridge. If this root bridge fails, the next root bridge is selected based on the bridge priority. If two switches have the same bridge priority value, the root bridge with the lower MAC address is selected.

BPDU

The root bridge continuously sends BPDUs (Bridge Protocol Data Units) at the set hello time interval. If a topology change is detected, alternative paths are calculated.

Hello time

The hello time is the time interval at which the root bridge sends BPDUs (default: two seconds).

Path costs

The path costs are used to decide which ports are to be blocked and which are to be preferred. The path costs are determined automatically based on the bandwidth. However, you can also specify a value manually.

5.2 Port roles

Root port

The root port connects a switch to the root bridge, either directly or via another switch (designated switch).

Designated port

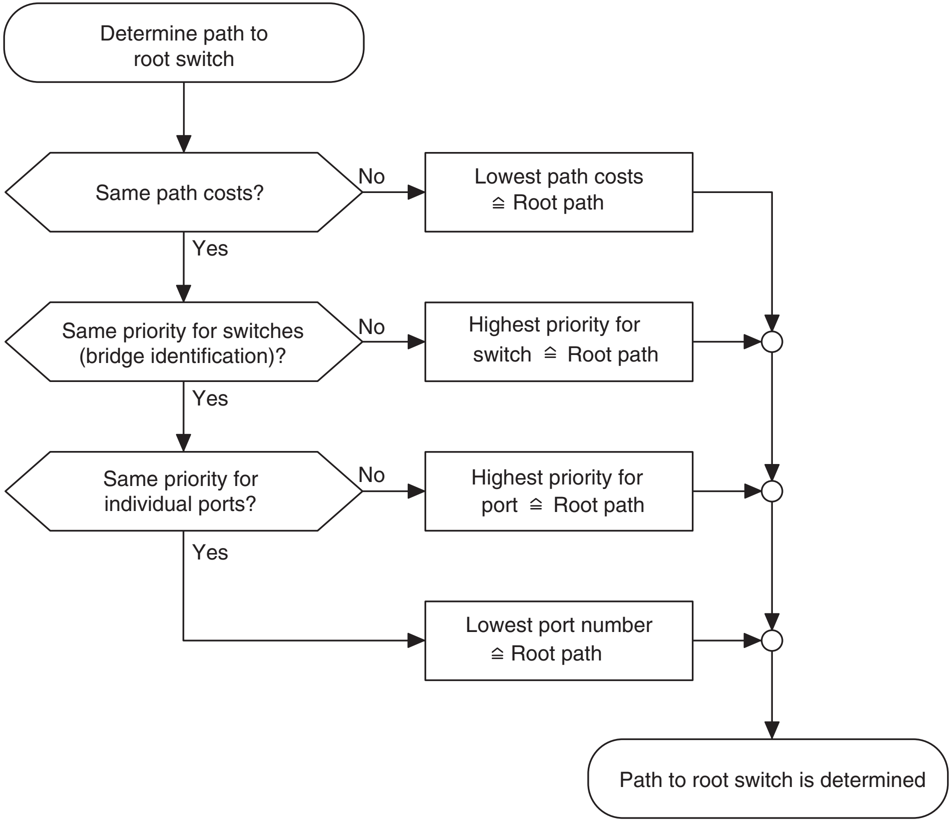
The designated port is a port on a designated switch that is connected to the root port of the next switch.

Alternate port

The alternate port could be a path to the root, but was not selected as the root port. The alternate port does not participate in the active topology.

5.3 Flow chart for determining the root path

Figure 5-2 Flow chart for determining the root path


Determine path to root switch
Same path costs?
No
Lowest path costs ≙ Root path
Yes
Same priority for switches (bridge identification)?
No
Highest priority for switch ≙ Root path
Yes
Same priority for individual ports?
No
Highest priority for port ≙ Root path
Yes
Lowest port number ≙ Root path
Path to root switch is determined

5.4 Port status

Discarding

The port is blocked, because otherwise it would cause a loop. The port does not send or receive user data; it only receives BPDU data.

If a link fails, the blocked port switches to the "forwarding" status.

Forwarding

Normal operation: The port receives frames and forwards them. The BPDUs are monitored.

5.5 Connecting switches to form a meshed topology

Having activated Rapid Spanning Tree for all switches, you can create a meshed topology with redundant data paths. You can now establish any data connections without having to take the creation of loops into consideration. You can also add loops intentionally to establish redundant connections.

In this context, a data path between Rapid Spanning Tree switches can be:

- A direct connection.
- A connection via one or more other switches that do not support Rapid Spanning Tree.

ℹ If Rapid Spanning Tree is not supported by all of the switches used:

The reconfiguration time of the Spanning Tree is extended by the aging time of the switches not supported by the Rapid Spanning Tree.

Furthermore, a data path can consist of the connection of a Rapid Spanning Tree switch to the following:

- An end device
- A network segment consisting of several infrastructure components not supported by Rapid Spanning Tree. In this network segment, **no** loops are permitted.

Observe the following rules if you intend to use infrastructure components without Rapid Spanning Tree support (e.g., unmanaged switches):

- **Rule 1: Rapid Spanning Tree transparency for all infrastructure components**

  All infrastructure components used in your network that do not actively support Rapid Spanning Tree must be transparent for Rapid Spanning Tree messages (BPDUs). They must forward all BPDUs to all ports without modifying them.

  The series 2000 switches are transparent for BPDUs if Rapid Spanning Tree is disabled.
- **Rule 2: At least one active Rapid Spanning Tree component per loop**

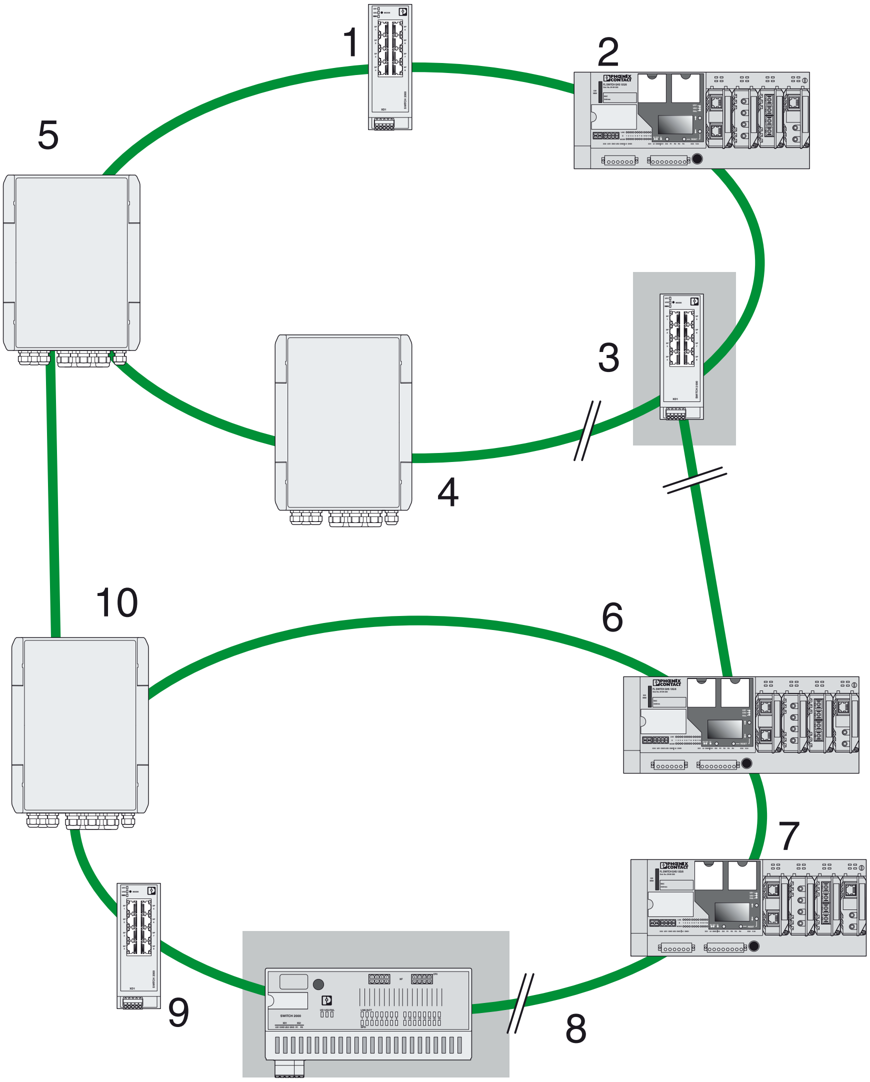
  An active Rapid Spanning Tree component supports the Rapid Spanning Tree Protocol, sends and receives BPDUs, evaluates them, and sets its ports to the corresponding RSTP states.

  Each loop in a network must have at least one active Rapid Spanning Tree component to interrupt the loop.

5.6 Example topology

In this example, two network segments are connected via redundant data paths. Two RSTP components have ports in the “Blocking” state (highlighted in gray). This is sufficient to operate the network.

Figure 5-3 Redundant coupling of network segments



5.7 Advanced configuration

It may be practical to actively specify the topology that is formed via RSTP, and not to leave this to the random MAC addresses of the switches involved. This means you can influence the non-blocking and blocking data paths, for example, and thus specify a load distribution.

Specifying the root switch

- On the? “Network Redundancy” page under “Bridge Priority”, set the lowest value (highest priority).
- Ensure that a higher value (lower priority) is set for all other switches in the network. Here, the set path costs are not evaluated.

Specifying the root port or designated port

The root port and designated port are always the ports with the lowest path costs. If the costs are the same, the priority is the decisive criterion. If this is also identical, the port number is the decisive criterion.

- On the “Network Redundancy” page, set a suitable combination of costs and priority for the port.
- Make sure that all the other network switches either have higher costs or a lower priority (higher value).

Disabling RSTP

If RSTP is disabled, the fast-forwarding function will be used at this port.

To disable RSTP, one of the following conditions must be met:

– An end device is connected to the port.

– Additional infrastructure components are connected to the port. The respective network segment does not contain any loops.

– Additional infrastructure components are connected to the port, and form a separate Rapid Spanning Tree. No additional redundant connections to this network segment are permitted.

Changing the protocol timers

NOTE: Malfunction
Changing the protocol timers may lead to unstable networks.

If, for example, you wish to use more than 20 active Rapid Spanning Tree components in a ring topology, it may be necessary to change the protocol timers. You can also try to reduce the reconfiguration times by changing the timers. However, care should be taken to prevent unstable networks.

The protocol times are specified by the root switch and distributed to all devices via BPDU. Initially therefore, it is sufficient to change the values in the root switch. If the root switch fails, the timer values of another active RSTP switch (the new root switch) become valid for the entire network segment. Consider this behavior when configuring your components.

Setting the timer values

– Maximum number of active Rapid Spanning Tree components along the path beginning at the root switch:

(MaxAge / 2) - Hello time + +1

- If you set the MaxAge to 40 seconds, for example, you increase the maximum distance of an infrastructure component from the root bridge to 19 hops. This also increases the maximum possible number of devices in a ring topology.

  MaxAge ≥ 2 × Hello time + 1 s

5.8 Fast ring detection

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, Network Redundancy”.
- Activate the “Fast Ring Detection” function.

This function speeds up the switch-over to a redundant path in the event of an error and enables easy diagnostics. Fast Ring Detection assigns an ID to each ring. This ID is communicated to every switch in the respective ring. One switch can belong to several different rings at the same time.

The “Fast Ring Detection” function is proprietary. It can only be used if all devices in the structure support this function.

Structure of the ring ID

The ring ID consists of the port number of the blocking port and the MAC address of the corresponding switch.

Advantages of the ring ID:

- Redundant paths are identified more easily.
- Blocking ports are located more easily.
- It is possible to check whether the desired topology corresponds to the actual topology.

When using Fast Ring Detection, note the following:

- With RSTP Fast Ring Detection, only use devices that support this function.
- Enable RSTP Fast Ring Detection on **all** devices.
- All data paths must be in full-duplex mode.

Fast Ring Detection switch-over times

With the maximum permissible number of switches in a ring, typical switch-over times range from 100 ms to 300 ms with Fast Ring Detection.

It is only possible to access the maximum number of switches when “Large Tree Support” is activated at the same time.

5.9 Large Tree Support

The “Large Tree Support” function increases the maximum possible number of switches in an RSTP topology.

Properties of Large Tree Support

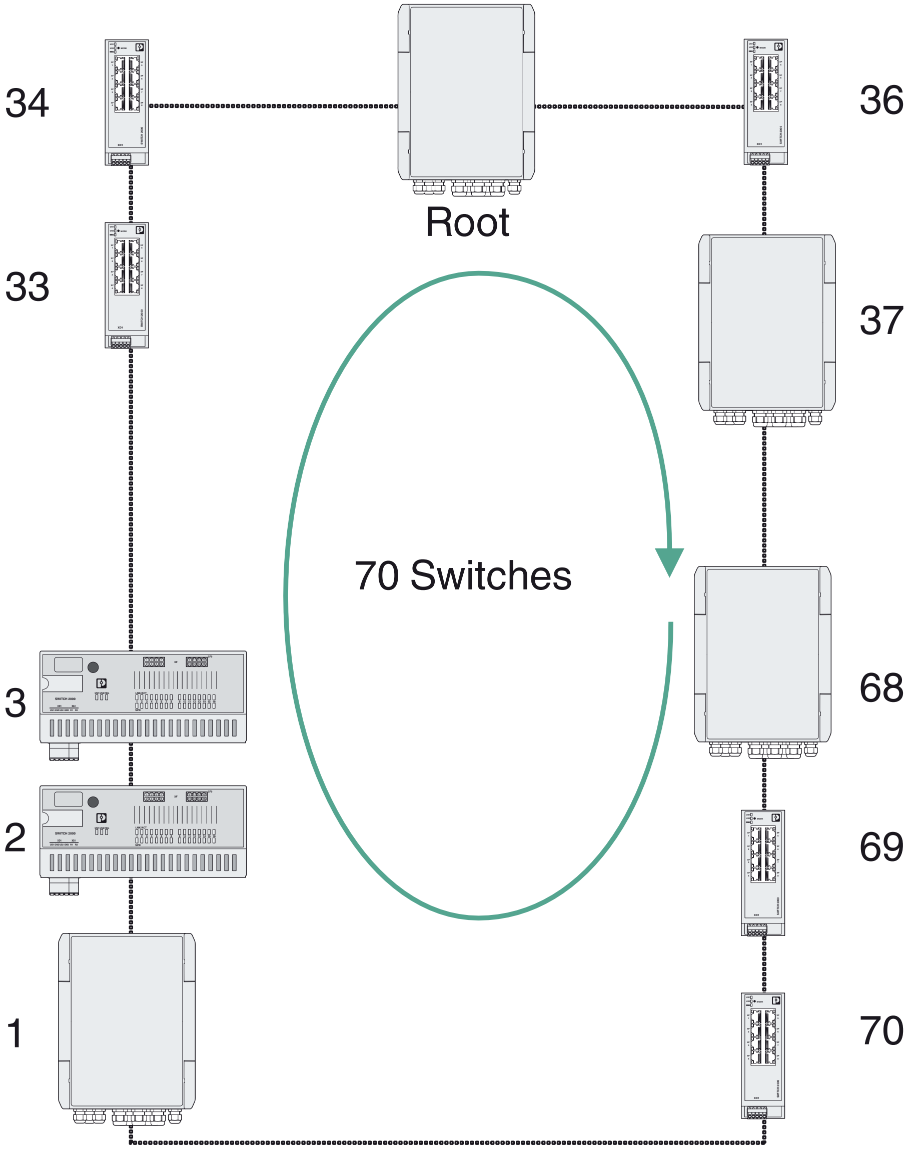
The “Fast Ring Detection” function is proprietary. It can only be used if all devices in the structure support this function.

When using Large Tree Support, note the following:

- Only use devices in the topology that support Large Tree Support.

- Enable Large Tree Support on all devices.
- We recommend that you only enable Large Tree Support when your network has more switches than possible for the standard RSTP.

Figure 5-4 Example of Large Tree Support topology



5.10 Topology sizes

The RSTP protocol permits the setup of redundant networks and enables simple ring topologies as well as meshed structures.

With the devices of the FL SWITCH 2000 and FL NAT 2000 series, you can use RSTP in accordance with IEEE 802.1D-2004 in these networks. To prevent failures, you have to observe the following maximum values during planning and setup.

5.10.1 Ring topologies (Large Tree Support deactivated)

With default parameters (especially MaxAge = 20):	20 devices in the ring, maximum
With adapted MaxAge = 40:	40 devices in the ring, maximum

5.10.2 Ring topologies (Large Tree Support activated)

ℹ If the “Large Tree Support” function is activated, we recommend not to use the default parameters.

With default parameters (especially MaxAge = 20):	70 devices in the ring, maximum

5.10.3 Meshed topologies (Large Tree Support deactivated)

With default parameters (especially MaxAge = 20):	Maximum distance to root bridge (intermediate data paths): 9 hops
With adapted MaxAge = 40:	Maximum distance to root bridge: 19 hops

5.10.4 Meshed topologies (Large Tree Support activated)

ℹ If the “Large Tree Support” function is activated, we recommend not to use the default parameters.

With default parameters (especially MaxAge = 20):	Maximum distance to root bridge (intermediate data paths): 34 hops

6 LACP – Link Aggregation Control Protocol

This function is not available on the SPE versions.

The Link Aggregation function enables you to bundle several physical LAN interfaces to create a logical channel referred to as a trunk. This makes it possible to transfer larger quantities of data and improve failsafe performance. If one or more physical connections of a trunk fail, the remaining connections handle the data load as far as possible.

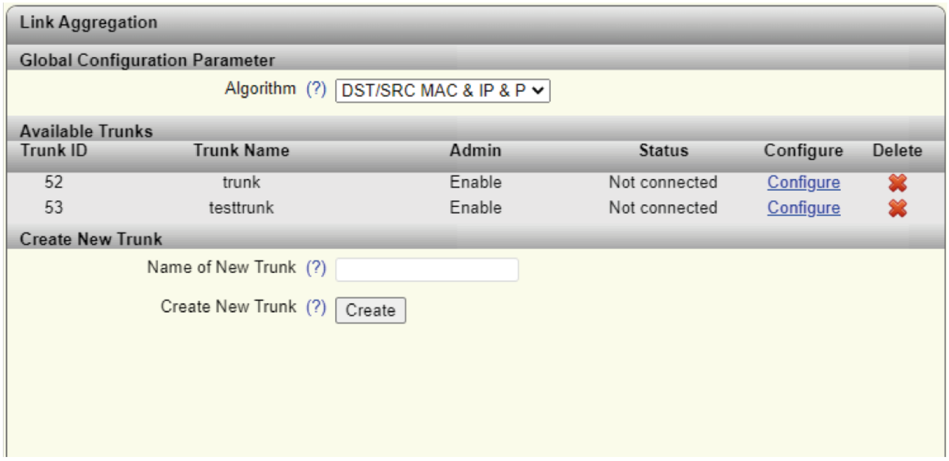
Using a trunk does not mean that the data throughput is multiplied, as all data communication frames are always processed via a single connection only. This means that a trunk with two connections cannot automatically transmit 2 Gbps in the case of a Gigabit switch.

Link Aggregation

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, Port Configuration”.
- Click on “Configure Link Aggregation”.

⇒ The “Link Aggregation” page opens.

Figure 6-1 Link Aggregation



Link Aggregation

Global Configuration Parameter

Algorithm (?) DST/SRC MAC & IP & P

Available Trunks

Trunk ID	Trunk Name	Admin	Status	Configure	Delete
52	trunk	Enable	Not connected	Configure	✖
53	testtrunk	Enable	Not connected	Configure	✖

Create New Trunk

Name of New Trunk (?)

Create New Trunk (?) Create

Link Aggregation: Global Configuration Parameters

Table 6-1 Global Configuration Parameters: Parameters

Parameter	Description
Algorithm	Here, select the algorithm that is responsible for the load distribution and that decides which physical connection is used for data communication. The various algorithms use the MAC or IP addresses of the source or destination fields, or the VLAN ID and the TCP/UDP port numbers. – SRC MAC: The algorithm uses the MAC address of the source. – DST MAC: The algorithm uses the MAC address of the destination. – DST/SRC MAC: The algorithm uses the MAC addresses of the source and destination. – DST/SRC IP & Port: The algorithm uses the IP addresses and TCP/UDP port numbers of the source and destination. – DST/SRC MAC & IP & Port: The algorithm uses the MAC addresses, IP addresses, and TCP/UDP port numbers of the source and destination.

Link Aggregation: Available Trunks

Table 6-2 Available Trunks: Parameters

Parameter	Description
Trunk ID	This column shows the trunk ID.
Trunk Name	This column shows the trunk name.
Admin	This column shows whether the trunk is enabled for administration.
Status	This column shows the trunk connection status.
Configure	Click on “Configure” to open the “Configure Trunk” pop-up window (see “Link Aggregation: Create New Trunk” on page 146).
Delete	Click on the red “X” to delete the selected trunk.

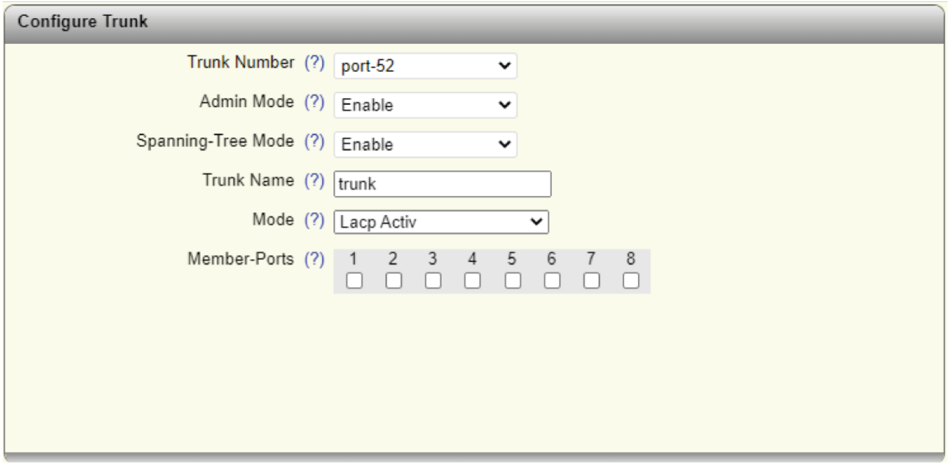
Link Aggregation: Create New Trunk

Table 6-3 Create New Trunk: Parameters

Parameter	Description
Name of New Trunk	Enter the desired name for the new trunk.
Create New Trunk	Click on “Create” to create the trunk with the selected name.

Pop-up window: Configure Trunk

Figure 6-2 Pop-up window: Configure Trunk



Configure Trunk

Trunk Number (?) port-52

Admin Mode (?) Enable

Spanning-Tree Mode (?) Enable

Trunk Name (?) trunk

Mode (?) Lacp Activ

Member-Ports (?) 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □

Table 6-4 Pop-up window: Configure Trunk: Parameters

Parameter	Description
Trunk Number	Here, select the trunk number for which the settings should be made.
Admin Mode	Select whether Admin mode should be activated. The trunk is then enabled for administration.
Spanning-Tree Mode	Select whether spanning tree should be activated for this trunk.
Trunk Name	Enter the desired name for the trunk.
Mode	Select how ports are added to the trunk: – Static: Ports are immediately added to the trunk. – LACP Active/Passive: The two members of a link aggregation first exchange information via LACPDUs: – Active: Information is exchanged regardless of whether the peer also has LACP. – Passive: Information is only exchanged after LACPDUs have been received by the peer. ℹ If the switch is used as an MRP client and if a trunk port was selected for at least one ring port, increased recovery times may be required in the MRP ring if “LACP Active/Passive” is activated. In this case, it is recommended to select “Static” mode.
Member-Ports	Select up to four ports that are to belong to the trunk. ℹ If you remove a member port as a trunk port, it is assigned the “Blocking” status. This prevents network loops. After a link down and link up or RSTP, the port functions again as intended.

7 SNMP – Simple Network Management Protocol

7.1 General function

The Simple Network Management Protocol (SNMP) is a manufacturer-independent standard for Ethernet management. It defines commands for reading and writing information, and defines formats for error and status messages. SNMP is also a structured model that consists of agents, their respective Management Information Base (MIB), and a manager. The manager is a software tool that is executed on a network management station. The agents are located inside switches, bus terminals, routers, and other devices that support SNMP. The task of the agents is to collect and provide data in the MIB. The manager regularly requests and displays this information. The devices can be configured via data that is written to the MIB by the manager. In the event of an emergency, the agents can also send messages (traps) directly to the manager.

ℹ All configuration changes that are to take effect after a device restart must be saved permanently.

ℹ For the SNMP commands supported by this device, refer to the download area for your device at phoenixcontact.net/qr/<item_number>.

- Download the current firmware for this.
- Unzip the firmware.
- Navigate to the folder “SNMP”.
- Open the file “FL-MGD-INFRASTRUCT-MIB.mi2” with an editor of your choice.

⇒ In this file you will find all the SNMP commands supported by this device.

7.2 SNMP interface

All Factoryline components have an SNMP agent. The agent of the device manages the Management Information Base II (MIB 2):

- FL Managed Infrastructure MIB
- lldpMIB
- RFC1213 MIB
- rmon
- snmpMIB
- ifMIB
- snmpFrameworkMIB
- etherMIB
- pBridgeMIB
- qBridgeMIB
- dot1dBridge
- rstpMIB
- IP MIB

Via the Simple Network Management Protocol, network management stations, such as a PC with the Network Manager, can read and change the configuration and diagnostic data of the network devices. You can use any SNMP tools or network management tools to access Factoryline products via SNMP. To do this, you must make the MIBs supported by the respective device available to the SNMP management tools.

On the one hand, these are globally valid MIBs, which are defined and described in Requests for Comments (RFCs). For example, this includes MIB 2 in accordance with RFC 1213, which is supported by all SNMP-capable network devices. On the other hand, manufacturers can define their own private SNMP objects, which are then assigned to a private manufacturer area in the large SNMP object tree. Manufacturers are responsible for their own private (enterprise) areas. For example, they may assign an object (object name and parameters) to an object ID and publish it only once. If this object is then no longer needed, it is labeled as expired, but it cannot be reused, for example, with other parameters.

Phoenix Contact provides notification of the ASN1 SNMP objects by publishing their descriptions on the Internet pages.

ℹ For SNMP, the password “public” is used for read access and the password “private” is used for read/write access.

Reading SNMP objects is not password protected. A password must be specified in SNMP in case of read access. In the factory default state, the password is “public”. It can be changed for SNMPv2 (see “Service” on page 58).

In the delivery state, the password for write access is “private” and can be changed by the user.

ℹ SNMP in write access mode and web-based management use the same password.

7.2.1 Using SNMPv3

When using SNMPv3, you must observe several points when accessing the SNMP objects. In contrast to SNMPv2, SNMPv3 is a protected protocol where the message contents and passwords are transmitted in encrypted format.

To use SNMPv3, you must first configure the switch accordingly (see “Service” on page 58). In addition, you need to switch your MIB browser to SNMPv3 and set the settings according to the settings on your decive. In delivery state those would be:

- MD5 as the algorithm for authentication
- DES as the algorithm for privacy
- User name: “admin”
- Password: current device password of the user “admin”

ℹ The password must have a minimum length of eight characters. If the default password is “private”, you have to use “private_” for access. If the “Individual SNMPv3 Password” option is activated, the user name is “admin” (see “My Profile: SNMPv3 Password” on page 46).

ℹ Even if the username “admin” for the administration account is changed, the username “admin” stays the same for access via SNMPv3.

Another benefit for the user is the option of sending traps using the Simple Network Management Protocol (see “Trap Manager” on page 107).

7.2.2 Management Information Base (MIB)

The Management Information Base (MIB) is a database which contains all the data (objects and variables) required for network management.

7.2.3 Agent

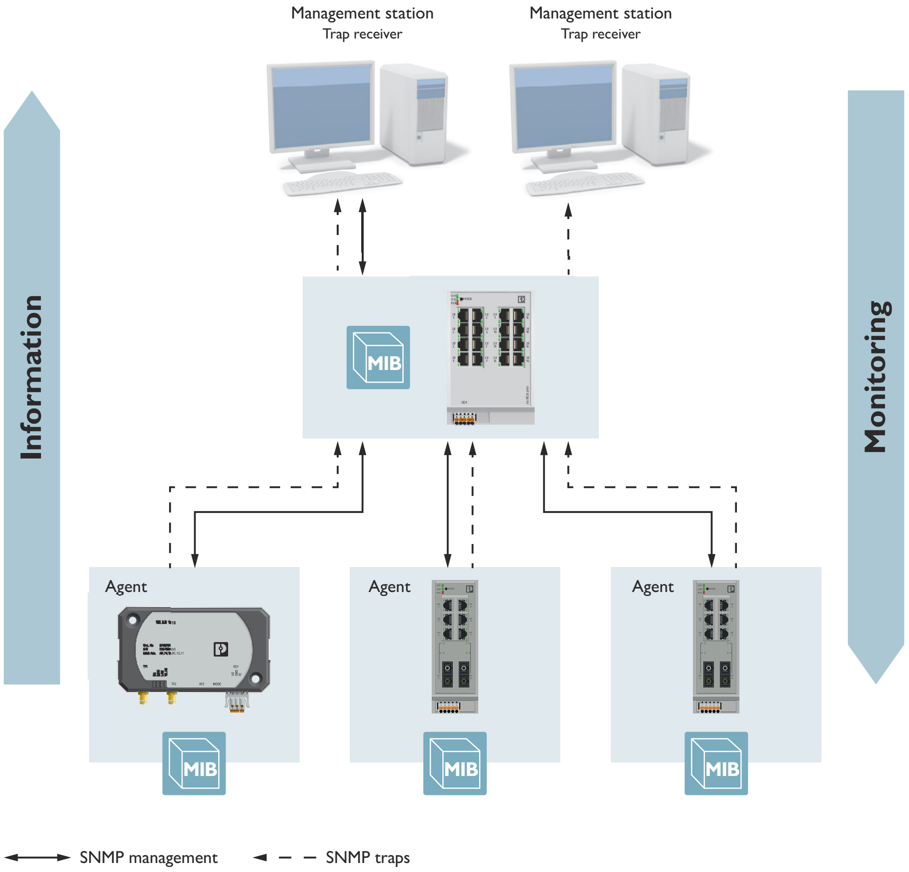
An agent is a software tool which collects data from the network device on which it is installed, and transmits this data on request. Agents reside in all managed network components and transmit the values of specific settings and parameters to the management station. On request by a manager or in response to a specific event, the agent transmits the collected information to the management station.

Not all devices support all object classes:

- If an unsupported object class is requested, an error message is generated.
- If an attempt is made to modify an unsupported object class, an error message is generated.

The descriptions of the SNMP objects are located in the respective MIBs and can be downloaded from the Phoenix Contact e-shop (see “General function” on page 149).

Figure 7-1 Schematic view of SNMP management



8 LLDP – Link Layer Discovery Protocol

8.1 Basic principles

LLDP

The switch supports the Link Layer Discovery Protocol (LLDP) in accordance with IEEE 802.1AB and enables topology detection of devices that also have LLDP activated.

Advantages of using LLDP:

- Improved error location detection
- Improved device replacement
- More efficient network configuration

The following information is received by or sent to neighboring devices as long as LLDP is activated:

- The device transmits its own management and connection information to neighboring devices.
- The device receives management and connection information from a neighboring device.

ℹ Note that a port that is blocked by RSTP does not receive any LLDP BPDUs, but is still able to send them.

LLDP general

The Link Layer Discovery Protocol (LLDP) in accordance with IEEE 802.1AB is used by network devices to learn and maintain the individual neighbor relationships.

8.2 Function

A network infrastructure component sends a port-specific BPDU (Bridge Protocol Data Unit), which contains the individual device information, at the “Message Transmit Interval” to each port in order to distribute topology information. The peer connected to the respective port learns the corresponding port-specific neighbors from these BPDUs.

The information learned from the BPDUs is saved for a defined period of time, known as the TTL (Time To Live) value. Subsequent receipt of the same BPDUs increases the TTL value again and the information is still saved. If the TTL expires, the neighbor information is deleted.

ℹ The switch manages a maximum of 50 items of neighbor information. All other information is ignored.

If several neighbors are displayed at one switch port, at least one other switch/hub that does not support LLDP or in which LLDP is not activated is installed between this switch and the neighbor displayed.

Table 8-1 Event table for LLDP

Event	Action of the individual LLDP agent	Response of the neighboring LLDP agent
Activate LLDP agent or start device	Transmit LLDP BPDUs to all ports	Include sender in the list of neighbors
Deactivate LLDP agent or reset software	Transmit LLDP BPDUs with a TTL value of zero seconds to all ports	Delete sender from the list of neighbors
Link up	Transmit port-specific LLDP BPDUs	Include sender in the list of neighbors
Link down	Delete all neighbors for this port	–
Timer (Message Transmit Interval)	Cyclic transmission of BPDUs to all ports	Update information
Aging (Time To Live)	Delete neighbor information	–
Receipt of a BPDU from a new neighbor	Extend list of neighbors and respond with port-specific BPDU	Include sender in the list of neighbors

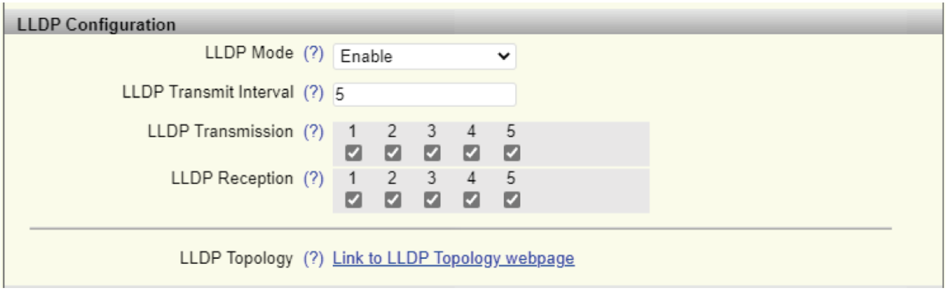
LLDP configuration in web-based management

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, Service”.
- Activate the “LLDP Mode” option and make the desired settings.

For 20xx/21xx version devices, LLDP can be activated or deactivated globally for all ports.

The 22xx/23xx/24xx/25xx/26xx/27xx version devices also offer a port-based configuration option for sending and receiving LLDP BPDUs.

Figure 8-1 LLDP Configuration



LLDP Configuration

LLDP Mode (?) Enable

LLDP Transmit Interval (?) 5

LLDP Transmission (?) 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑

LLDP Reception (?) 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑

LLDP Topology (?) Link to LLDP Topology webpage

Table 8-2 LLDP Configuration: Parameters

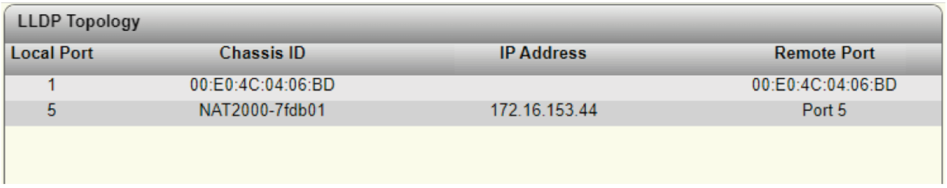
Parameter	Description
LLDP Mode	– Disable: LLDP is switched off. – Enable: LLDP is switched on. – Send only: LLDP BPDUs are only sent. – Receive only: LLDP BPDUs are only received.
LLDP Transmit Interval	This option is only available if you selected “Enable” or “Send only” for “LLDP Mode”. Here, enter the interval at which LLDP telegrams are to be sent. The value must be between five and 32786 seconds (default: five seconds).
LLDP Transmission	This option is only available if you selected “Enable” or “Send only” for “LLDP Mode”. Here, activate or deactivate the forwarding of LLDP telegrams for specific ports.
LLDP Reception	This option is only available if you selected “Enable” or “Receive only” for “LLDP Mode”. Here, activate or deactivate the ignoring of LLDP telegrams for specific ports.
LLDP Topology	Click on “Link to LLDP Topology webpage” to open the “LLDP Topology” pop-up window (see “LLDP diagnostics in web-based management” on page 155).

- Click on “Apply&Save” to save your settings.

LLDP diagnostics in web-based management

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Diagnostics, LLDP Topology”.

Figure 8-2 LLDP Topology



LLDP Topology

Local Port	Chassis ID	IP Address	Remote Port
1	00:E0:4C:04:06:BD		00:E0:4C:04:06:BD
5	NAT2000-7fdb01	172.16.153.44	Port 5

A table is created for known neighbors and contains the following four columns:

Table 8-3 LLDP Topology: Parameters

Parameter	Description
Local Port	The number of the port that is used to connect the neighbor to this device is specified here.

Table 8-3 LLDP Topology: Parameters

Parameter	Description
Chassis ID	The address of the connected neighbor is displayed here.
IP Address	The IP address of the connected neighbor is displayed here.
Remote Port	The number of the neighbor device port that is used to connect the neighbor to this device is specified here.

9 Topology-based IP assignment

The “Topology-based IP assignment” function enables automatic assignment of incremented IP addresses via LLDP and DHCP. This way, manual assignment of IP addresses to individual devices in the network becomes obsolete.

Observe the following requirements to be able to use the function:

– The function is proprietary and is only supported by devices of the FL SWITCH 2xxx, FL SWITCH TSN 2xxx, and FL NAT 2xxx product families.
– The function can only be used in pure line topologies or ring topologies.
  Additional branching with managed switches of the FL SWITCH 2xxx, FL SWITCH TSN 2xxx, and FL NAT 2xxx product families in the topology is not permitted and may result in IP address conflicts.
– LLDP must be activated on all switches.

Perform the following steps:

- Assign an IP address to a switch manually (see “Assigning the IP address” on page 25). This device is then called the root device.
- For the IP address assignment to additional switches (clients), configure a DHCP server in the same network.

For this, you can use the integrated pool-based DHCP server, for example (see “DHCP Service” on page 92). Please take into consideration that the IP pool permits incremented IP assignment to all connected switches. The pool start address should be the address of the root device + 1, and the pool size must be configured large enough.

- On the root device, configure the assignment port to which the clients are connected (“Network” on page 55). In a ring topology, you must select one of the two ring ports.

To prevent IP assignment via BootP, the DHCP server should not accept BootP requests. Configuration of an assignment port on the root device automatically deactivates the “Accept BootP” function of the device-internal DHCP server.

The switches connected as clients should be set to the default settings. Incremented assignment of an IP address corresponding to the position in the topology is then carried out automatically. Each switch will receive the next higher IP address compared to its neighbor provided that this address is not yet assigned in the network.

Example configuration:

The following example shows how the “Topology-based IP assignment” function should be used to prevent conflicts during assignment of IP addresses via the DHCP server. The parameters have to be adapted in the corresponding target application.

– IP address of the root device: 172.16.1.**100**
– DHCP pool start address: 172.16.1.**10**
– DHCP pool size:200

Based on the topology, the switches of the FL SWITCH 2xxx, FL SWITCH TSN 2xxx, and FL NAT 2xxx product families connected to the root device as a line or ring topology would therefore be assigned the following IP addresses:

172.16.1.**101**, 172.16.1.**102**, …

Other devices in the network requesting an IP would initially be assigned the following IP addresses via the DHCP server:

172.16.1.**10**, 172.16.1.**11**, …

In principle, such a configuration can be used to separate the “Topology-based IP assignment” function from further DHCP requests.

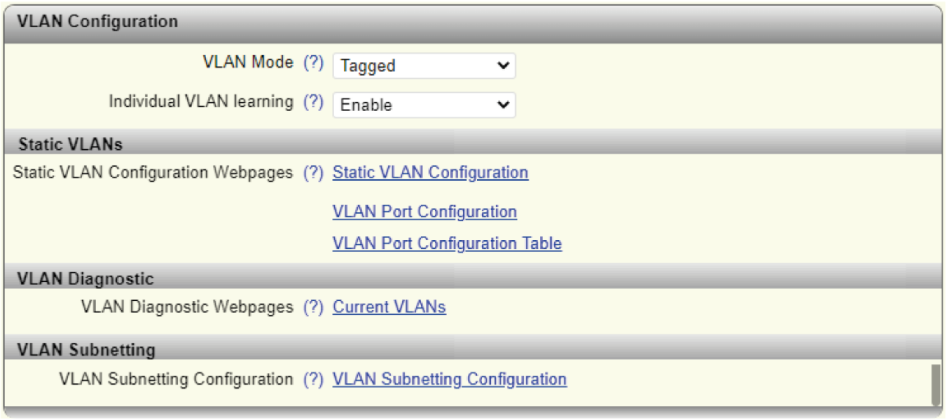
10 VLAN – Virtual Local Area Network

10.1 VLAN Configuration

On this page, you can configure VLAN.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, VLAN Configuration”.

Figure 10-1 VLAN Configuration



VLAN Configuration

VLAN Mode (?) Tagged

Individual VLAN learning (?) Enable

Static VLANs

Static VLAN Configuration Webpages (?) Static VLAN Configuration

VLAN Port Configuration

VLAN Port Configuration Table

VLAN Diagnostic

VLAN Diagnostic Webpages (?) Current VLANs

VLAN Subnetting

VLAN Subnetting Configuration (?) VLAN Subnetting Configuration

Table 10-1 VLAN Configuration: Parameters

Parameter	Description
VLAN Mode	Select the desired VLAN mode. – Transparent: In Transparent mode, the switch processes the incoming data packets as described in Section “Frame switching” on page 33. Neither the structure nor the contents of the data packets are changed. The information about VLAN assignment from a tag that may be contained in the data packet is ignored. – Tagged: In Tagged mode, the switch forwards the data packets based on their VLAN assignment (taken from the tag).
Individual VLAN learning	This option is not available on the FL NAT versions. Select whether Individual VLAN learning should be activated. If you deactivate this function, you can use asymmetric VLAN. The function can only be deactivated if you selected “Tagged” for “VLAN Mode”. ℹ If you deactivate the function, you cannot use the MAC-based Port Security function.

VLAN Configuration: Static VLANs

The following parameters are only available if you selected “Tagged” for “VLAN Mode”.

Table 10-2 Static VLANs: Parameters

Parameter	Description
Static VLAN Configuration Webpages	Click on “Static VLAN Configuration” to open the “Static VLAN Configuration” pop-up window (see “Pop-up window: Static VLAN Configuration” on page 161). Up to eight (20xx/21xx versions) or 32 (22xx/23xx/24xx/25xx/26xx/27xx versions) static VLANs can be set up here. Click on “VLAN Port Configuration” to open the “VLAN Port Configuration” pop-up window (see “Pop-up window: VLAN Port Configuration” on page 161). You can make port-specific settings for your VLANs here. Click on “VLAN Port Configuration Table” to open the “VLAN Port Configuration Table” pop-up window (see “Pop-up window: VLAN Port Configuration Table” on page 162). In a tabular view, you can make port-specific settings for your VLANs here.

VLAN Configuration: VLAN Diagnostic

The following parameters are only available if you selected “Tagged” for “VLAN Mode”.

Table 10-3 VLAN Diagnostic: Parameters

Parameter	Description
VLAN Diagnostic Webpages	Click on “Current VLANs” to open the “Current VLANs” page (see “Current VLANs” on page 105). It lists the current VLANs and shows the ports for each VLAN, which are either “Tagged” or “Untagged”.

VLAN Configuration: VLAN Subnetting

The following parameters are only available if you selected “Tagged” for “VLAN Mode”.

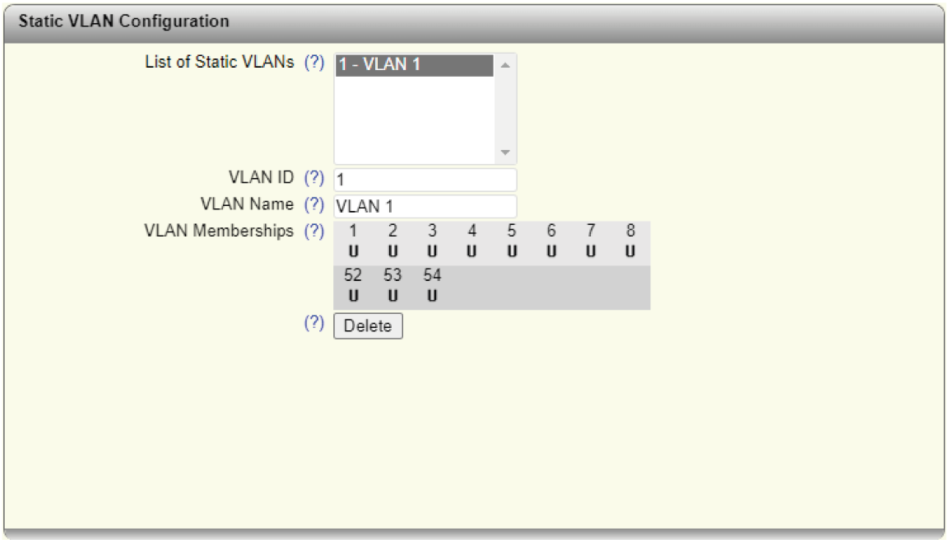
Table 10-4 VLAN Subnetting: Parameters

Parameter	Description
VLAN Subnetting Configuration	Click on “VLAN Subnetting Configuration” to open the “VLAN Subnetting Configuration” pop-up window (see “VLAN Subnet” on page 163).

Pop-up window: Static VLAN Configuration

On this page, up to eight (20xx/21xx versions) or 32 (22xx/23xx/24xx/25xx/26xx/27xx versions) static VLANs can be set up.

Figure 10-2 Pop-up window: Static VLAN Configuration



Static VLAN Configuration

List of Static VLANs (?) 1 - VLAN 1

VLAN ID (?) 1

VLAN Name (?) VLAN 1

VLAN Memberships (?)

1	2	3	4	5	6	7	8
U	U	U	U	U	U	U	U
52	53	54					
U	U	U					

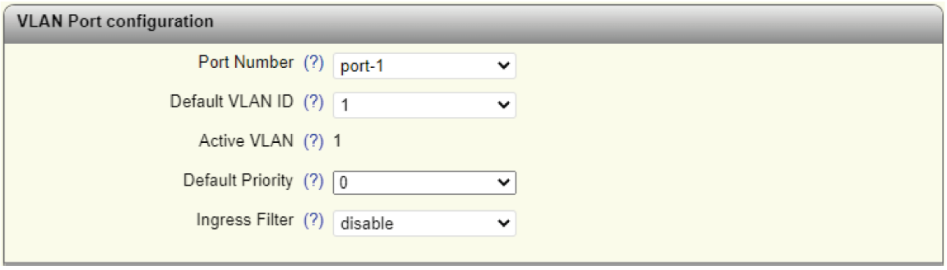
Table 10-5 Pop-up window: Static VLAN Configuration: Parameters

Parameter	Description
List of Static VLANs	All static VLANs created up to this point are displayed here.
VLAN ID	Enter the VLAN ID that you want to assign to the new VLAN. The value must be between two and 4094.
VLAN Name	Enter the name for the VLAN you want to create.
VLAN Memberships	Specify which ports are to be located in the VLAN. – T: Tagged port – U: Untagged port – –: Not a member of the VLAN
Delete	Click on “Delete” to delete the VLAN selected in the list. ℹ VLAN 1 cannot be deleted.

Pop-up window: VLAN Port Configuration

On this page, you can make port-specific settings for your VLANs.

Figure 10-3 Pop-up window: VLAN Port Configuration



VLAN Port configuration

Port Number (?) port-1

Default VLAN ID (?) 1

Active VLAN (?) 1

Default Priority (?) 0

Ingress Filter (?) disable

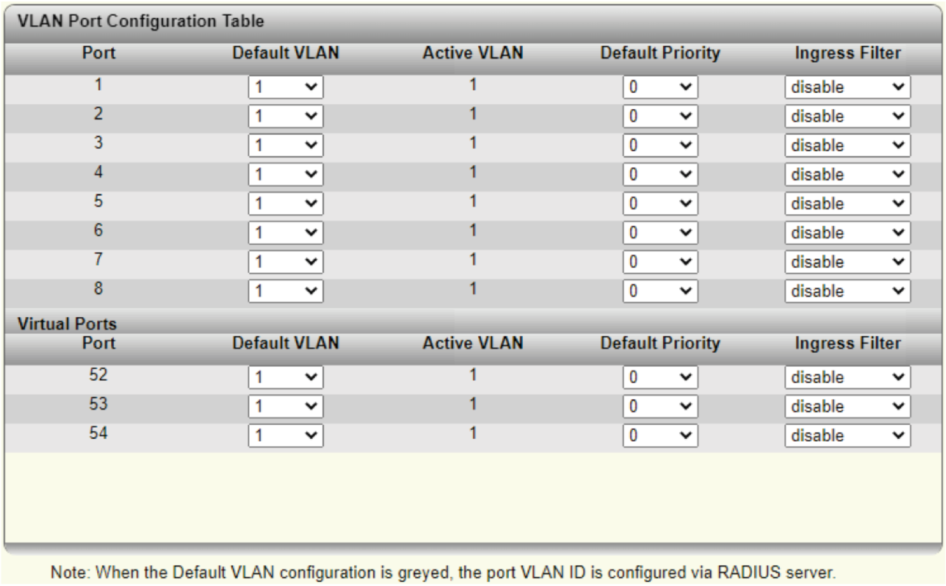
Table 10-6 Pop-up window: VLAN Port Configuration: Parameters

Parameter	Description
Port Number	Select the port for which you want to change the VLAN settings.
Default VLAN ID	Select the VLAN ID that is to be assigned to the port.
Active VLAN	If the port-specific VLAN ID is assigned via a RADIUS server, the “Active VLAN” display appears and the configured “Default VLAN ID” is grayed out. “Active VLAN” then shows the VLAN ID assigned to this port by the RADIUS server.
Default Priority	Select the VLAN priority for the selected port.
Ingress Filter	Select whether the ingress filter should be activated. An ingress filter protects networks from unwanted incoming data traffic. Packets arriving with a VLAN ID that does not match the port membership will be filtered out.

Pop-up window: VLAN Port Configuration Table

On this page, you can make port-specific settings for your VLANs in a tabular view.

Figure 10-4 Pop-up window: VLAN Port Configuration Table



VLAN Port Configuration Table

Port	Default VLAN	Active VLAN	Default Priority	Ingress Filter
1	1	1	0	disable
2	1	1	0	disable
3	1	1	0	disable
4	1	1	0	disable
5	1	1	0	disable
6	1	1	0	disable
7	1	1	0	disable
8	1	1	0	disable

Virtual Ports

Port	Default VLAN	Active VLAN	Default Priority	Ingress Filter
52	1	1	0	disable
53	1	1	0	disable
54	1	1	0	disable

Note: When the Default VLAN configuration is greyed, the port VLAN ID is configured via RADIUS server.

Table 10-7 Pop-up window: VLAN Port Configuration Table: Parameters

Parameter	Description
Port	This column shows the port for which you are changing the VLAN settings.

Table 10-7 Pop-up window: VLAN Port Configuration Table: Parameters

Parameter	Description
Default VLAN	Select the VLAN ID that is to be assigned to the port.
Default Priority	Select the VLAN priority for the selected port.
Ingress Filter	Select whether the ingress filter should be activated. An ingress filter protects networks from unwanted incoming data traffic. Packets arriving with a VLAN ID that does not match the port membership will be filtered out.

10.2 VLAN Subnet

On this page, you can configure an additional IP interface for the device. This makes it possible to access the device from various subnets or VLANs via dedicated IP addresses, e.g., to separate the administrative access and PROFINET IO.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, Network, VLAN Subnetting Configuration”.

The “LAN 1” button shows the network parameters of the primary IP interface, which you can also configure on the “Network” page (see “Network” on page 55). The following functions are only available on the LAN 1 interface: PROFINET, DHCP server, ACD.

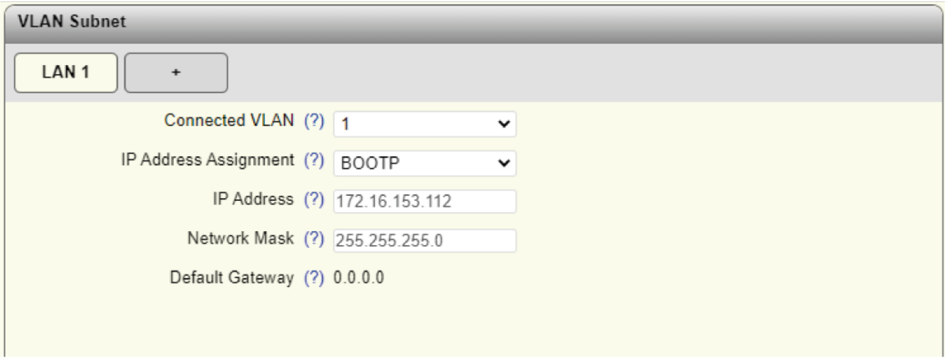
- Click on “+” to open the configuration page of the second IP interface.

⇒ After the configuration is saved, the button designation changes to “LAN 2”.

- Click on the “x” to delete the second IP interface.

You cannot delete the “LAN 1” interface.

Figure 10-5 VLAN Subnet



Connected VLAN (?) 1
IP Address Assignment (?) BOOTP
IP Address (?) 172.16.153.112
Network Mask (?) 255.255.255.0
Default Gateway (?) 0.0.0.0

Table 10-8 VLAN Subnet: Parameters

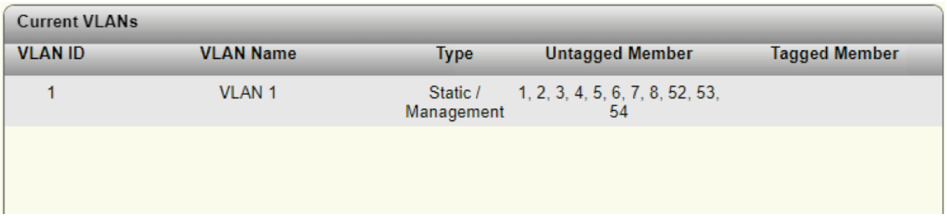
Parameter	Description
Connected VLAN	Select the VLAN that is to be assigned to the IP interface. Only VLANs configured on the device are available. Each VLAN can only be assigned to one IP interface.
IP Address Assignment	Select the type of IP address assignment. – STATIC: Static IP address – BOOTP: Assignment via the Bootstrap protocol – DHCP: Assignment via a DHCP server – DCP: Assignment via the PROFINET engineering tool or controller For further information on IP address assignment, refer to "Assigning the IP address" on page 25.
IP Address	This option is only available if you selected "STATIC" for "IP Address Assignment". Enter the desired IP address.
Network Mask	This option is only available if you selected "STATIC" for "IP Address Assignment". Enter the desired subnet mask.
Default Gateway	This option is only available if you selected "STATIC" for "IP Address Assignment". The default gateway is displayed here, which you can configure on the "Network" page (see "Network" on page 55). ℹ The default gateway is a device-wide parameter and cannot be configured to be interface-specific. ℹ A default gateway that was received dynamically via DHCP will only be used if a static default gateway has not yet been configured on the device.

10.3 Current VLANs

On this page, you will find diagnostic information on the current VLANs.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Diagnostics, Current VLANs”.

Figure 10-6 Current VLANs



Current VLANs

VLAN ID	VLAN Name	Type	Untagged Member	Tagged Member
1	VLAN 1	Static / Management	1, 2, 3, 4, 5, 6, 7, 8, 52, 53, 54	

Table 10-9 Current VLANs: Parameters

Parameter	Description
VLAN ID	The VLAN ID is displayed here.
VLAN Name	The VLAN name is displayed here.
Type	The VLAN type is displayed here.
Untagged Member	The untagged members of the VLAN are displayed here.
Tagged Member	The tagged members of the VLAN are displayed here.

11 RADIUS certificates

11.1 General information

RADIUS stands for “Remote Authentication Dial-in User Service”. It is a client/server protocol that is also referred to as a “triple-A” protocol. The three A’s stand for authentication, authorization, and accounting.

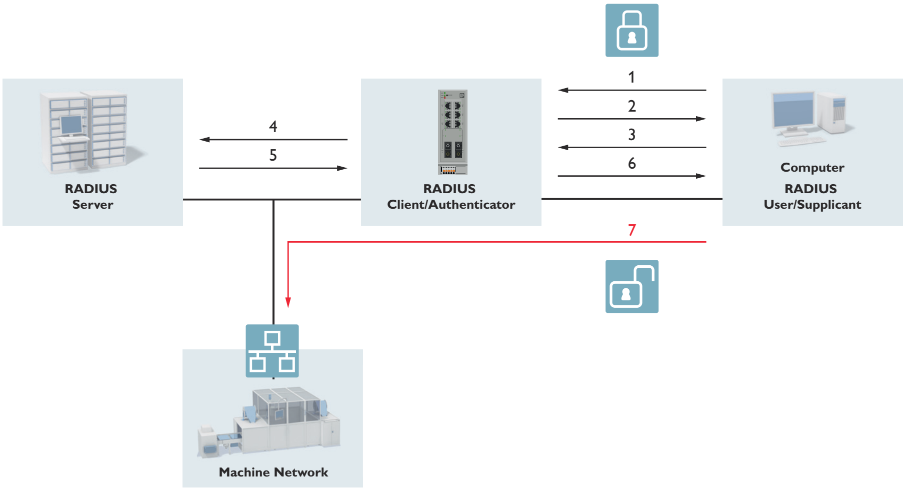
RADIUS authentication implements the authentication method in accordance with standard IEEE 802.1X. This standard provides a general method for authentication and authorization in IEEE 920 networks. When a person (the “supplicant”) attempting access to the network connects to the device (the “authenticator”), a physical port on the device sends the PC’s certificates to a RADIUS authentication server using the Extensible Authentication Protocol (EAP). This verifies and, if applicable, sends a command back to the device that then permits access to the service offered by the device. By using an authentication server, you can also grant local, unrecognized devices access to the network. For example, members of an external service team can log into a network.

This authorization is usually performed once when the device initially connects. Once the device is disconnected, the device closes the port until the next connection. To guard against sophisticated attempts at unauthorized access, you can configure the device to re-authenticate on a periodic timed basis.

The devices of the FL SWITCH 2000 and FL NAT 2000 product family can be used as an authenticator for RADIUS authentication (see “Configuring the authenticator” on page 170). A computer, for example, can take the role of supplicant (see “Configuring the supplicant (computers with Windows 10)” on page 171).

11.1.1 Sequence of the 802.1X authentication process

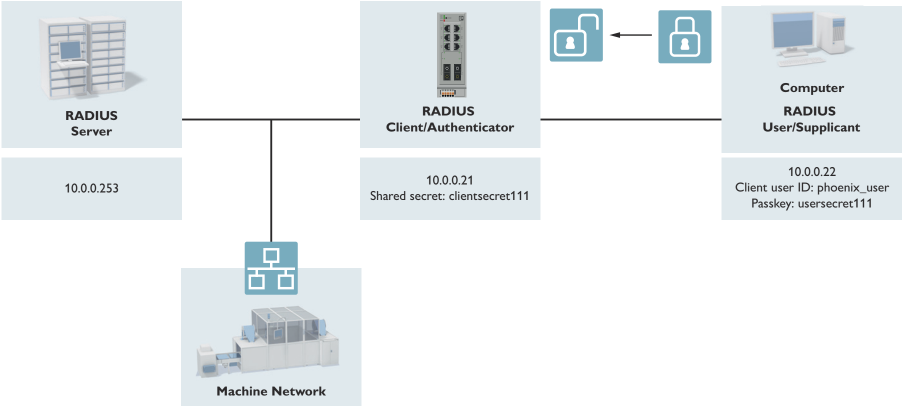
Figure 11-1 802.1X RADIUS process (simplified)



1. The supplicant sends a start packet to the authenticator.
2. The authenticator prompts the supplicant for the access data.
3. The supplicant sends the access data to the authenticator.
4. The authenticator sends the supplicant’s access data as well as its own access data to the RADIUS server.
5. The RADIUS server sends its response (accept or refuse) to the authenticator.
6. If the response is positive, the authenticator opens the port for the supplicant and notifies the supplicant.
7. The supplicant can now access the network.

11.1.2 Example configuration

Figure 11-2 RADIUS: Example configuration



The RADIUS server requires the access data of the authenticator and the supplicant:

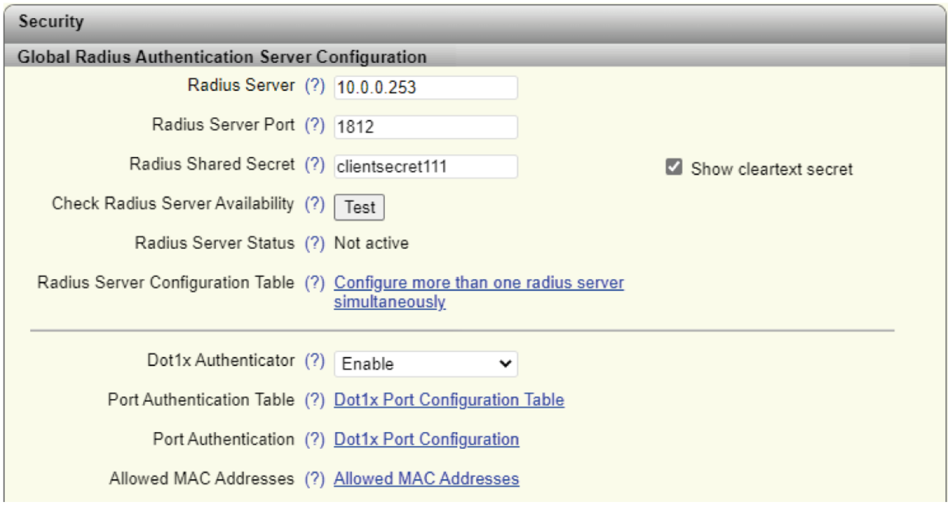
- Authenticator’s access data:
  - Authenticator’s IP address: 10.0.0.21
  - Authenticator’s shared secret: clientsecret111
- Supplicant’s access data:
  - User name: phoenix_user
  - Passkey: usersecret111

11.2 Configuring RADIUS

11.2.1 Configuring the authenticator

- Open web-based management on the authenticator (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, Security”.

Figure 11-3 Configuring the authenticator: Security



Security

Global Radius Authentication Server Configuration

Radius Server	(?)	10.0.0.253
Radius Server Port	(?)	1812
Radius Shared Secret	(?)	clientsecret111 ☑ Show cleartext secret
Check Radius Server Availability	(?)	Test
Radius Server Status	(?)	Not active
Radius Server Configuration Table	(?)	Configure more than one radius server simultaneously
Dot1x Authenticator	(?)	Enable
Port Authentication Table	(?)	Dot1x Port Configuration Table
Port Authentication	(?)	Dot1x Port Configuration
Allowed MAC Addresses	(?)	Allowed MAC Addresses

- For “Radius Server”, enter the IP address of your RADIUS server.
- For “Radius Server Port”, enter the RADIUS server port in use.
- For “Radius Shared Secret”, enter the authenticator’s shared secret.
- Click on “Apply&Save” to save your settings.

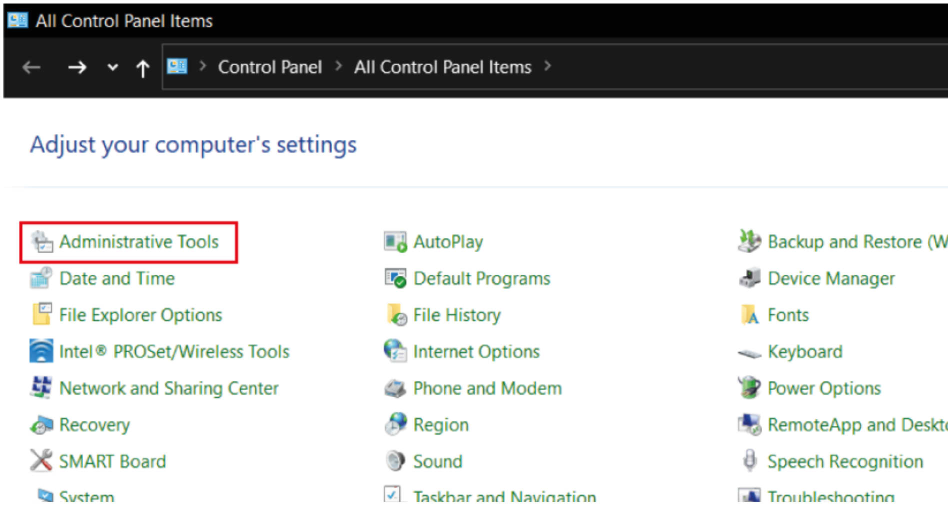
Alternatively, you can also configure the RADIUS server(s) via the RADIUS Server Configuration Table. For this, click on “Configure more than one radius server simultaneously”.

11.2.2 Configuring the supplicant (computers with Windows 10)

For computers with other operating systems or other Windows versions, the steps required may differ.

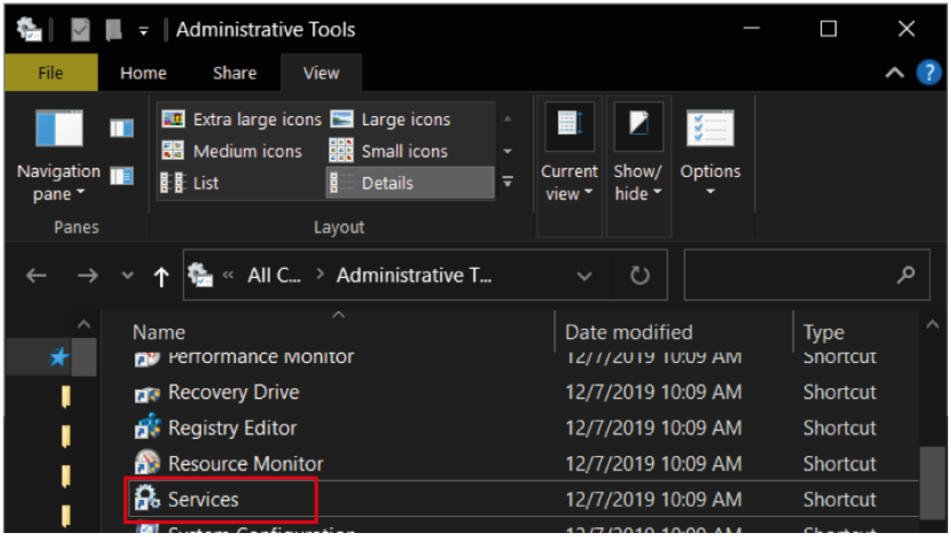
- Open the Control Panel and click on “Administration”.

Figure 11-4 Configuring the supplicant (Windows 10): Control Panel



- Double-click on “Services”.

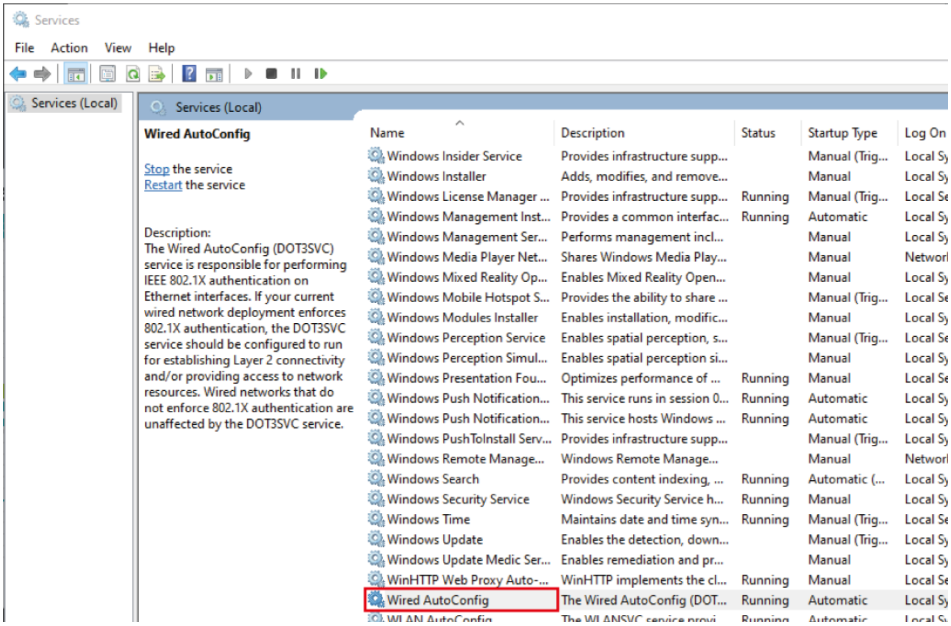
Figure 11-5 Configuring the supplicant (Windows 10): Administration



Name	Date modified	Type
Performance Monitor	12/7/2019 10:09 AM	Shortcut
Recovery Drive	12/7/2019 10:09 AM	Shortcut
Registry Editor	12/7/2019 10:09 AM	Shortcut
Resource Monitor	12/7/2019 10:09 AM	Shortcut
Services	12/7/2019 10:09 AM	Shortcut
System Configuration	12/7/2019 10:09 AM	Shortcut

- Select “Wired AutoConfig” from the list and double-click on it.

Figure 11-6 Configuring the supplicant (Windows 10): Services



Wired AutoConfig

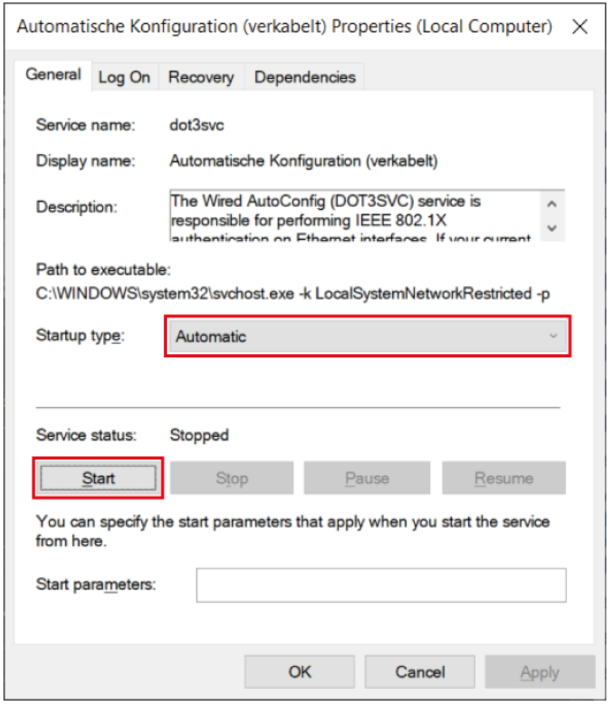
Stop the service
Restart the service

Description:
The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X authentication, the DOT3SVC service should be configured to run for establishing Layer 2 connectivity and/or providing access to network resources. Wired networks that do not enforce 802.1X authentication are unaffected by the DOT3SVC service.

Name	Description	Status	Startup Type	Log On
Windows Insider Service	Provides infrastructure supp...		Manual (Trig...	Local Sy
Windows Installer	Adds, modifies, and remove...		Manual	Local Sy
Windows License Manager ...	Provides infrastructure supp...	Running	Manual (Trig...	Local Se
Windows Management Inst...	Provides a common interfac...	Running	Automatic	Local Sy
Windows Management Ser...	Performs management incl...		Manual	Local Sy
Windows Media Player Net...	Shares Windows Media Play...		Manual	Networ
Windows Mixed Reality Op...	Enables Mixed Reality Open...		Manual	Local Sy
Windows Mobile Hotspot S...	Provides the ability to share ...		Manual (Trig...	Local Se
Windows Modules Installer	Enables installation, modific...		Manual	Local Sy
Windows Perception Service	Enables spatial perception, s...		Manual (Trig...	Local Se
Windows Perception Simul...	Enables spatial perception si...		Manual	Local Sy
Windows Presentation Fou...	Optimizes performance of ...	Running	Manual	Local Se
Windows Push Notification...	This service runs in session 0...	Running	Automatic	Local Sy
Windows Push Notification...	This service hosts Windows ...	Running	Automatic	Local Sy
Windows PushToInstall Serv...	Provides infrastructure supp...		Manual (Trig...	Local Sy
Windows Remote Manage...	Windows Remote Manage...		Manual	Networ
Windows Search	Provides content indexing, ...	Running	Automatic (...	Local Sy
Windows Security Service	Windows Security Service h...	Running	Manual	Local Sy
Windows Time	Maintains date and time syn...	Running	Manual (Trig...	Local Se
Windows Update	Enables the detection, down...		Manual (Trig...	Local Sy
Windows Update Medic Ser...	Enables remediation and pr...		Manual	Local Sy
WinHTTP Web Proxy Auto-...	WinHTTP implements the cl...	Running	Manual	Local Se
Wired AutoConfig	The Wired AutoConfig (DOT...	Running	Automatic	Local Sy
WLAN AutoConfig	The WLANSVC service provi...	Running	Automatic	Local Sy

- Select “Automatic” from the drop-down menu for “Startup type”.
- Click on “Start”.

Figure 11-7 Configuring the supplicant (Windows 10): AutoConfig



Automatische Konfiguration (verkabelt) Properties (Local Computer)

Service name: dot3svc

Display name: Automatische Konfiguration (verkabelt)

Description: The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current

Path to executable:
C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p

Startup type: Automatic

Service status: Stopped

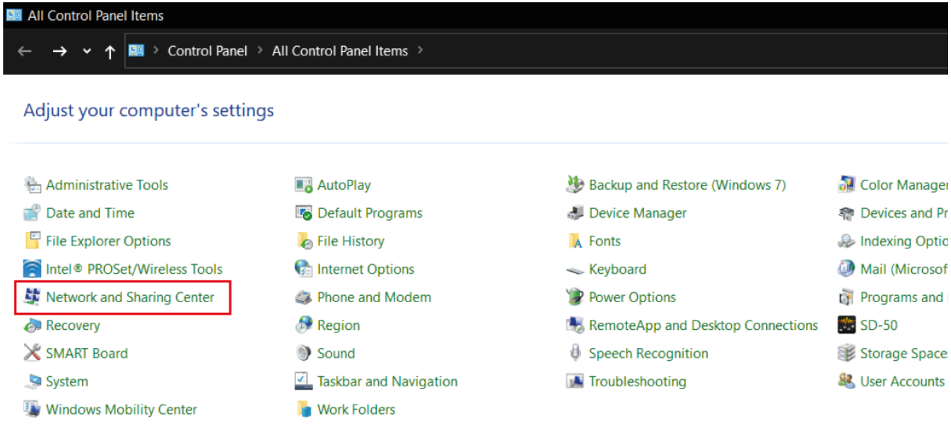
You can specify the start parameters that apply when you start the service from here.

Start parameters:

- Close the window.

- Open the Control Panel again and click on “Network and Sharing Center”.

Figure 11-8 Configuring the supplicant (Windows 10): Control Panel



All Control Panel Items

Control Panel > All Control Panel Items >

Adjust your computer's settings

Administrative Tools
Date and Time
File Explorer Options
Intel® PROSet/Wireless Tools
Network and Sharing Center
Recovery
SMART Board
System
Windows Mobility Center

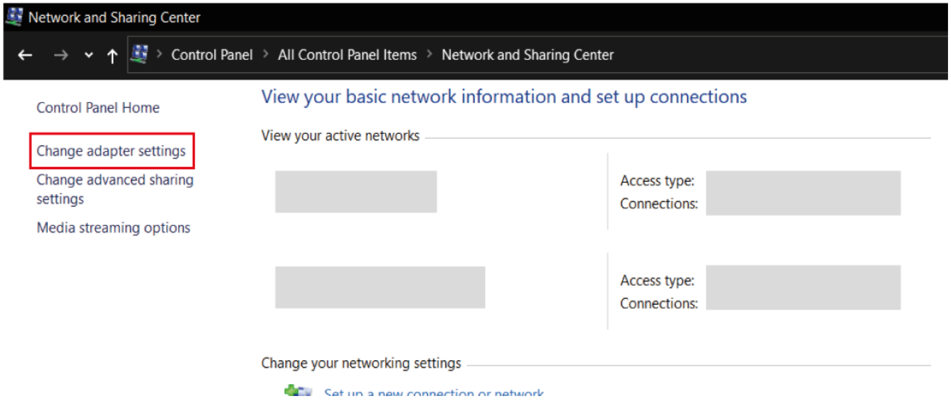
AutoPlay
Default Programs
File History
Internet Options
Phone and Modem
Region
Sound
Taskbar and Navigation
Work Folders

Backup and Restore (Windows 7)
Device Manager
Fonts
Keyboard
Power Options
RemoteApp and Desktop Connections
Speech Recognition
Troubleshooting

Color Managei
Devices and Pr
Indexing Optic
Mail (Microsof
Programs and
SD-50
Storage Space
User Accounts

- Click on “Change adapter settings” on the left.

Figure 11-9 Configuring the supplicant (Windows 10): Network and Sharing Center



Network and Sharing Center

Control Panel > All Control Panel Items > Network and Sharing Center

Control Panel Home

Change adapter settings

Change advanced sharing settings

Media streaming options

View your basic network information and set up connections

View your active networks

Access type:
Connections:

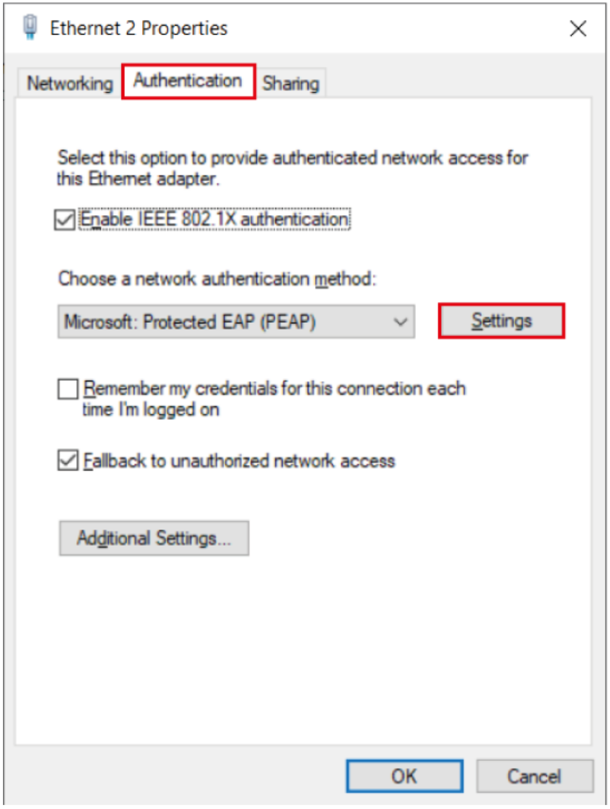
Access type:
Connections:

Change your networking settings

Set up a new connection or network

- Select “Properties” in the context menu for the LAN connection to your device.
- Select the Authentication tab and click on “Settings”.

Figure 11-10 Configuring the supplicant (Windows 10): Ethernet Properties



Ethernet 2 Properties

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

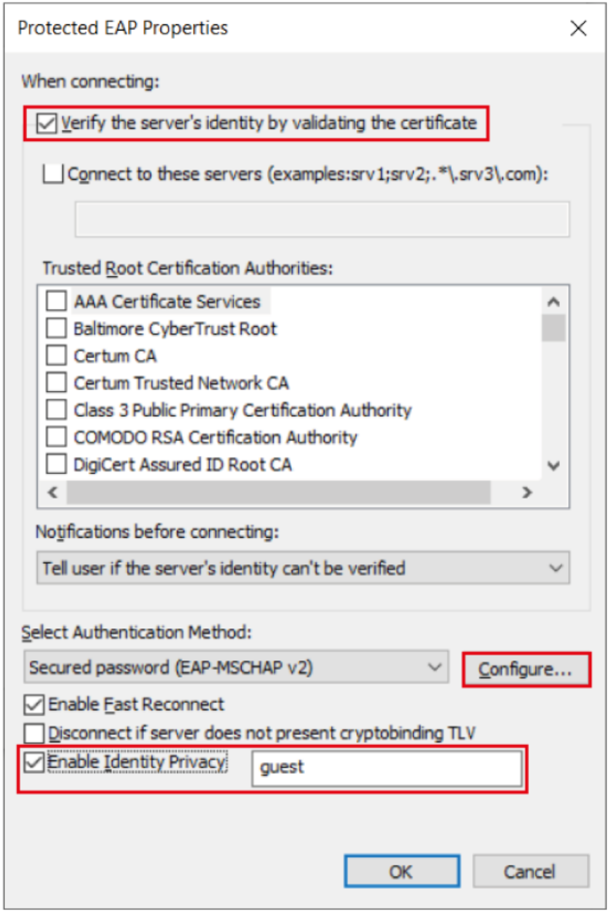
Microsoft: Protected EAP (PEAP)

□ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

- Activate the check box “Verify the server’s identity by validating the certificate”.
- Activate the check box “Enable Identity Privacy” and enter “guest” in the field.

Figure 11-11 Configuring the supplicant (Windows 10): Protected EAP Properties



Protected EAP Properties

When connecting:

☑ Verify the server's identity by validating the certificate

□ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):

Trusted Root Certification Authorities:

- □ AAA Certificate Services
- □ Baltimore CyberTrust Root
- □ Certum CA
- □ Certum Trusted Network CA
- □ Class 3 Public Primary Certification Authority
- □ COMODO RSA Certification Authority
- □ DigiCert Assured ID Root CA

Notifications before connecting:

Tell user if the server's identity can't be verified

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect

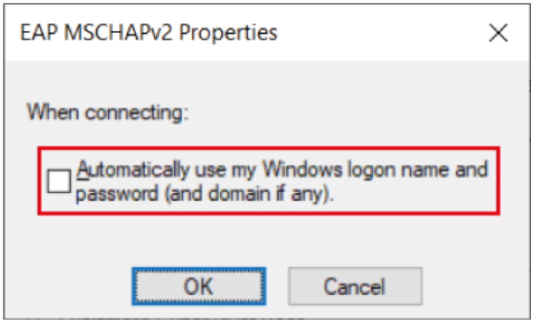
□ Disconnect if server does not present cryptobinding TLV

☑ Enable Identity Privacy: guest

- Click on “Configure”.

- Deactivate the check box “Automatically use my Windows logon name and password” and click on “OK”.

Figure 11-12 Configuring the supplicant (Windows 10): EAP-MSCHAPv2 Properties



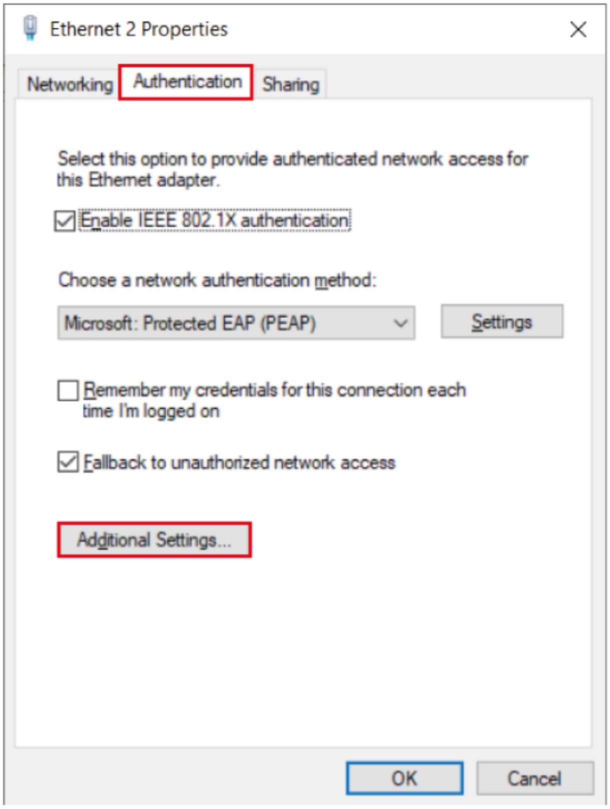
EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

- Close the window with “OK”.
- Click on “Additional Properties”.

Figure 11-13 Configuring the supplicant (Windows 10): Ethernet Properties



Ethernet 2 Properties

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

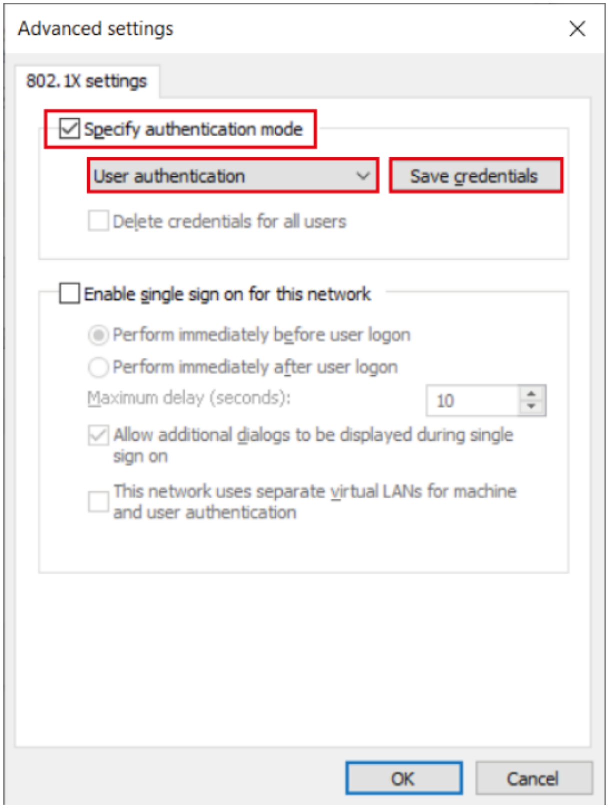
Microsoft: Protected EAP (PEAP)

□ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

- Activate the check box “Specify authentication mode” and select “User authentication”.
- Click on “Save credentials”.

Figure 11-14 Configuring the supplicant (Windows 10): Advanced settings



Advanced settings

802.1X settings

☑ Specify authentication mode

User authentication

□ Delete credentials for all users

□ Enable single sign on for this network

● Perform immediately before user logon

○ Perform immediately after user logon

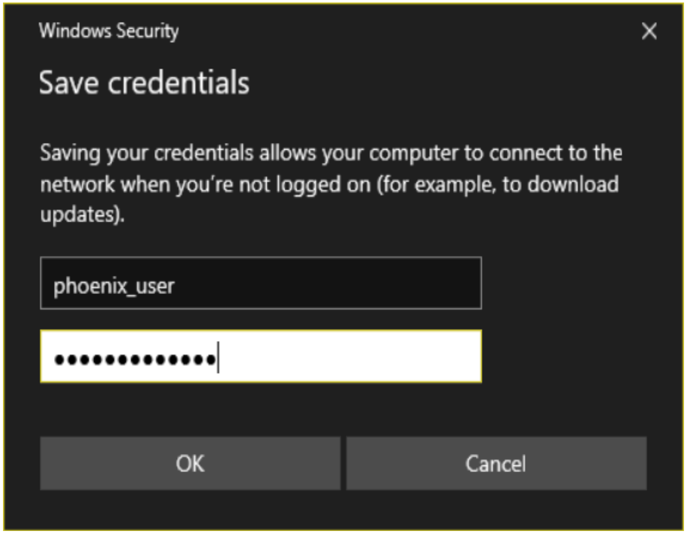
Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication

- Enter the credentials saved for you on the RADIUS server.

Figure 11-15 Configuring the supplicant (Windows 10):



Windows Security

Save credentials

Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).

phoenix_user

••••••••••••••

- Close all windows with “OK”.

⇒ The RADIUS functionality is set up and ready for operation.

12 Operation as a PROFINET device

In PLCnext Engineering, the switch is supported as a PROFINET device. The PROFINET controller can therefore support the startup of the switch within a PROFINET application. This includes the assignment of the IP parameters, comparison of the target/actual configuration, and archiving of the alarms sent by the switch. In the event that a device is replaced, the controller recognizes the replacement device and starts it up automatically. As a PROFINET device, the switch provides, for example, the link states for the control program as process data items.

ℹ The 20xx/21xx versions do not support PROFINET mode. They cannot be operated as PROFINET devices.

12.1 Preparing the switch for PROFINET operating mode

In the delivery state, the standard versions of the
FL SWITCH 22xx/23xx/24xx/25xx/26xx/27xx and FL NAT 22xx/23xx are in universal mode. They must be set to PROFINET mode once.

The following options are available for switching to PROFINET mode:

– After startup and IP address assignment, you can change the operating mode/automation profile on the “Quick Setup” page in web-based management (see “Quick Setup” on page 53).
– You can use Smart mode (see “Using Smart mode” on page 22).

When you activate PROFINET mode, the following default settings are made for operation:

– The Link Layer Discovery Protocol (LLDP) is enabled with the following configuration specifications for PROFINET components:
  a) The Discovery and Configuration Protocol (DCP) is activated as the mechanism for assigning IP parameters.
  b) The MRP protocol is deactivated.

When you switch to PROFINET mode, the configuration is saved automatically and the device is restarted.

The switch then starts up in PROFINET mode for the first time, and waits for a name and PROFINET IP address to be assigned (see “Device naming” on page 190 and “Operating in the PROFINET Environment” on page 190).

If you activate universal mode again, the following settings are made:

– LLDP remains active with the delivery state values.
– IP address assignment is set to BootP.
– The station name for the switch does not change. If no station name has been specified, the device type is entered.

ℹ We recommend: After changing the operating mode, save the new configuration. Please note that some configuration changes only take effect after a restart.

12.2 Switch as a PROFINET device

12.2.1 Configuring in the engineering tool

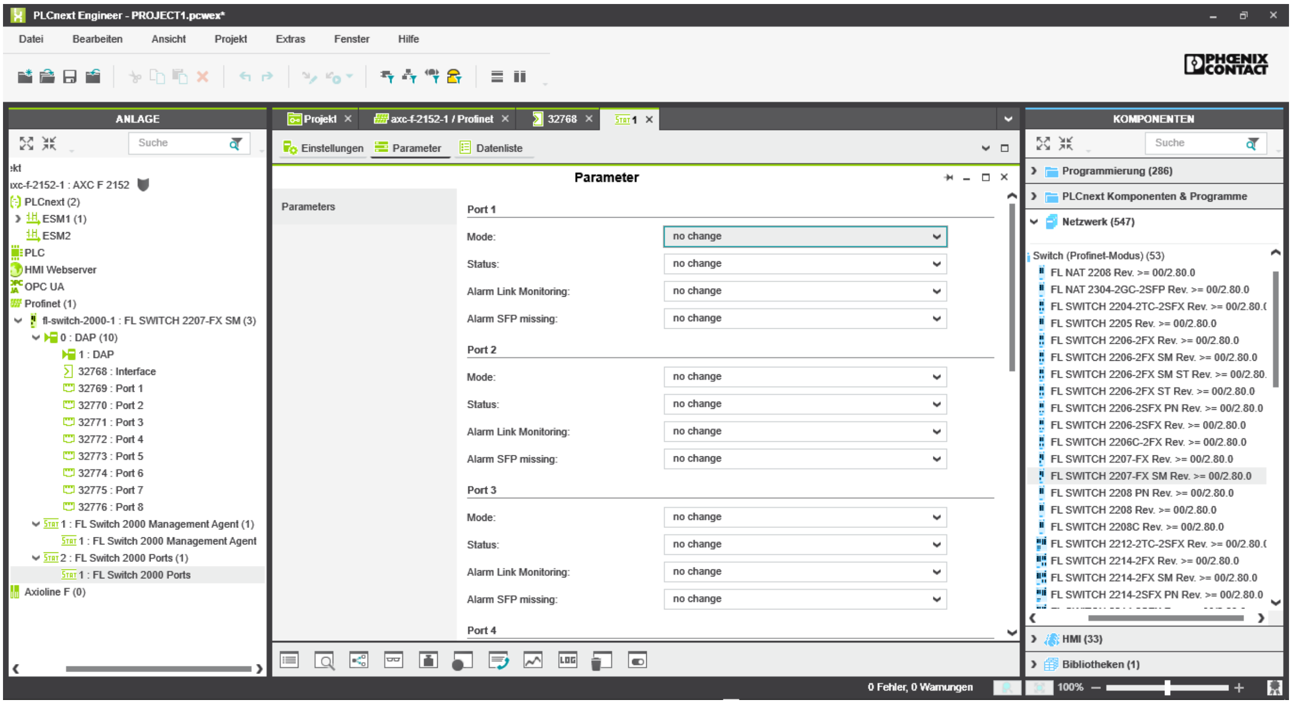
Specifying the bus configuration

The switch can be operated as a PROFINET device if it is integrated under a controller in the bus configuration in the engineering tool. For this integration, a GSD and an FDCML file are available to download at phoenixcontact.net/products.

ℹ The device description files (GSD and FDCML files) provided for integrating the switch do not need to be replaced in the configuration when the firmware is updated. Each version of the files is compatible with more current firmware releases.

Exception: If module parameters have been added to a new firmware revision, the device description files must be updated in the engineering tool in order to be able to use the module parameters. If you do not require the new parameters in the application, you can continue to use the older versions of the GSD and FDCML files.

Figure 12-1 Integrating devices in the engineering tool


PLCnext Engineer - PROJECT1.pcwex*
Datei
Bearbeiten
Ansicht
Projekt
Extras
Fenster
Hilfe
PHOENIX CONTACT
ANLAGE
Suche
ekt
axc-f-2152-1 : AXC F 2152
PLCnext (2)
ESM1 (1)
ESM2
PLC
HMI Webserver
OPC UA
Profinet (1)
fl-switch-2000-1 : FL SWITCH 2207-FX SM (3)
0 : DAP (10)
1 : DAP
32768 : Interface
32769 : Port 1
32770 : Port 2
32771 : Port 3
32772 : Port 4
32773 : Port 5
32774 : Port 6
32775 : Port 7
32776 : Port 8
1 : FL Switch 2000 Management Agent (1)
1 : FL Switch 2000 Management Agent
2 : FL Switch 2000 Ports (1)
1 : FL Switch 2000 Ports
Axioline F (0)
Projekt
axc-f-2152-1 / Profinet
32768
1
Einstellungen
Parameter
Datenliste
Parameters
KOMPONENTEN
Suche
Programmierung (286)
PLCnext Komponenten & Programme
Netzwerk (547)
Switch (Profinet-Modus) (53)
FL NAT 2208 Rev. >= 00/2.80.0
FL NAT 2304-2GC-2SFP Rev. >= 00/2.80.0
FL SWITCH 2204-2TC-2SFX Rev. >= 00/2.80.(
FL SWITCH 2205 Rev. >= 00/2.80.0
FL SWITCH 2206-2FX Rev. >= 00/2.80.0
FL SWITCH 2206-2FX SM Rev. >= 00/2.80.0
FL SWITCH 2206-2FX SM ST Rev. >= 00/2.80.
FL SWITCH 2206-2FX ST Rev. >= 00/2.80.0
FL SWITCH 2206-2SFX PN Rev. >= 00/2.80.0
FL SWITCH 2206-2SFX Rev. >= 00/2.80.0
FL SWITCH 2206C-2FX Rev. >= 00/2.80.0
FL SWITCH 2207-FX Rev. >= 00/2.80.0
FL SWITCH 2207-FX SM Rev. >= 00/2.80.0
FL SWITCH 2208 PN Rev. >= 00/2.80.0
FL SWITCH 2208 Rev. >= 00/2.80.0
FL SWITCH 2208C Rev. >= 00/2.80.0
FL SWITCH 2212-2TC-2SFX Rev. >= 00/2.80.(
FL SWITCH 2214-2FX Rev. >= 00/2.80.0
FL SWITCH 2214-2FX SM Rev. >= 00/2.80.0
FL SWITCH 2214-2SFX PN Rev. >= 00/2.80.0
HMI (33)
Bibliotheken (1)
0 Fehler, 0 Warnungen
100%

Parameter

Port 1

Mode: no change

Status: no change

Alarm Link Monitoring: no change

Alarm SFP missing: no change

Port 2

Mode: no change

Status: no change

Alarm Link Monitoring: no change

Alarm SFP missing: no change

Port 3

Mode: no change

Status: no change

Alarm Link Monitoring: no change

Alarm SFP missing: no change

Port 4

If the switch is not listed in the device catalog, the device description provided by Phoenix Contact needs to be imported. The latest device description is available on the Internet at phoenixcontact.net/products.

If the device description is available in the device catalog, the following options are available for bus configuration:

- Manual: The components are transferred to the bus configuration from the device catalog using drag and drop.

– Automatic: The devices are entered via the “Read PROFINET” function, which means that they can be accessed in the network via DCP (Discovery and Configuration Protocol). For this, the devices must be supplied with voltage and “PROFINET mode” must be activated.

For further information on integrating switches in PLCnext Engineer and TIA 17, refer to the corresponding quick-start guides. These are available to download on the product page of your device, e.g., phoenixcontact.net/qr/2702327.

12.2.2 Configuring the switch as a PROFINET device

After all the switches have been added to the bus configuration, you need to make the following settings for the individual switches via the “Detail View” tab (device details):

- Check the PROFINET device name. Change it, if necessary.
- Check the IP address and subnet mask. Change both, if necessary.
- The update time for inputs should be set to “512 ms” (default).
- The update time for outputs should be set to “512 ms” (default).
- The monitoring time should be set to “2000 ms” (default).

After that, you can create and use the PROFINET variables in the control program. In addition to the “PNIO_DATA_STATE” standard variable, the switch provides the link status for each port as a process data byte.

If the “PNIO_DATA_VALID” bit for the “PNIO_DATA_STATE” variable declares the switch process data as valid, the process data item for a port can have the following values (see “Other cyclic process data” on page 189):

Value = 1: Active link

Value = 2: Link available but the peer cannot establish the link (for FX ports only – Far-end default detection)

Process data can only be accessed if the configured target configuration matched the actual configuration on device startup.

12.2.3 Configuring via an engineering tool

The switch can be configured via an engineering tool (e.g., PLCnext Engineering) using the universal parameter editor (UPE).

12.2.3.1 Structure of the process data

The tables below provide an overview of the information contained in the various slots.

Table 12-1 Slot 1/1 inputs

Byte	PN information	Table
1, 2	Status word	Table 12-11
3	Link states of ports 1–8	Table 12-12
4	Link states of ports 9–16	
5	Link states of ports 17–24	
6	Link states of ports 25–32	
7	Diagnostics	Table 12-12

Table 12-2 Slot 1/1 outputs

Byte	PN information	Table
1, 2	Control word	Table 12-11

Table 12-3 Slot 2/1 inputs

Byte	PN information	Table
1	Port 1	Table 12-13
2	Port 2	
3	Port 3	
...	...	
16	Port 16	

12.2.3.2 PN records (acyclic)

Table 12-4 Record index 0x0PP (PP - port number) – Slot2 Subslot1

Byte no.	Item	Data type	Parameter permission	Default	Valid options
0	Block version	Byte	Read only	0	0 – Indicates this data set
1	Port mode	Byte	Read/write	0	0 – No changes 1 – Auto negotiation 2 – 10 Mbps HD 3 – 10 Mbps FD 4 – 100 Mbps HD 5 – 100 Mbps FD 20 – Auto negotiation 10/100 only 21 – Fast startup
2	Port enable status	Byte	Read/write	0	0 – No changes 1 – Disable 2 – Enable
3	Alarm link monitoring	Byte	Read/write	0	0 – No changes 1 – Disable 2 – Enable
4	Reserved				
5	Alarm SFP missing	Byte	Read/write	0	0 – No changes 1 – Disable 2 – Enable

Table 12-5 Record index 0x1PP (PP - port number) – Slot2 Subslot1

Byte no.	Item	Data type	Parameter permission	Default	Valid options
0	Block version	Byte	Read only	0	0 – Indicates this data set
1	Port speed	Byte	Read only	0	0 – Not connected 1 – 10 Mbps 2 – 100 Mbps 3 – 1 Gbps port duplex
2	Port duplex	Byte	Read only	0	0 – Unknown 1 – Full duplex 2 – Half duplex
3	Port utilization RX	Byte	Read only	0	In %
4	Port utilization TX	Byte	Read only	0	In %
5	Max. utilization RX	Byte	Read only	0	In %
6–9	Reserved				
10–11	Fiber transceiver RX power	Int16	Read only	0	Value in 0.1 dBm
12–13	Fiber transceiver TX power	Int16	Read only	0	Value in 0.1 dBm
14–15	Reserved				
16–19	RX unicasts packet count	Uint32	Read only	0	
20–23	RX broadcasts packet count	Uint32	Read only	0	
24–27	RX multicasts packet count	Uint32	Read only	0	
28–31	Fragment error count	Uint32	Read only	0	
32–35	Undersized packet count	Uint32	Read only	0	
36–39	Oversized packet count	Uint32	Read only	0	
40–43	CRC error count	Uint32	Read only	0	

Table 12-6 Record index 1 – Slot1 Subslot1

Byte no.	Item	Data type	Parameter permission	Default	Valid options
0	Block version	Byte	Read only	0	0 – Indicates this data set
1	Alarm power supply	Byte	Read/write	0	0 – No changes 1 – Disable 2 – Enable
2	Alarm module remove	Byte	Read/write	0	0 – No changes 1 – Disable 2 – Enable
3	Alarm MRP ring failure	Byte	Read/write	0	0 – No changes 1 – Disable 2 – Enable
4	PlugMem missing	Byte	Read/write	0	0 – No changes 1 – Disable 2 – Enable
5–9	Reserved				

Table 12-6 Record index 1 – Slot1 Subslot1 [...]

Byte no.	Item	Data type	Parameter permission	Default	Valid options
10	RSTP mode	Byte	Read/write	0	0 – No changes 1 – RSTP 2 – RSTP/FRD 3 – RSTP/LTS 4 – RSTP/LTS/FRD
11	RSTP priority	Byte	Read/write	16	0 ... 15 – Priority value as multiple of 4K 16 – No changes
12	Web server	Byte	Read/write	0	0 – No changes 1 – Disable 2 – HTTP 3 – HTTPS
13	SNMP agent	Byte	Read/write	0	0 – No changes 1 – Disable 2 – SNMPv2 3 – SNMPv3
14	CLI service	Byte	Read/write	0	0 – No changes 1 – Disable 2 – Telnet 3 – SSH
15	CLI network scripting	Byte	Read/write	0	0 – No changes 1 – Disable 2 – Enable
16	Alarm output: power supply	Byte	Read/write	0	0 – No changes 1 – Disable 2 – Enable
17	Alarm output: link monitoring	Byte	Read/write	0	0 – No changes 1 – Disable 2 – Enable
18	Alarm output: MRP	Byte	Read/write	0	0 – No changes 1 – Disable 2 – Enable
19	Alarm output: pluggable memory missing	Byte	Read/write	0	0 – No changes 1 – Disable 2 – Enable
20–29	Reserved				
30	UI lock state	Byte	Read/write	0	0 – No changes 1 – Disable 2 – Enable
31	Password encryption state	Byte	WRITE	0	0 – Not encrypted 1 – Encrypted
32–95	Current admin password (valid access used when setting new password)	Char array	WRITE	0	Empty string if not used
96–159	New password to configure	Byte	Read/write	0	Empty string if not used

Table 12-6 Record index 1 – Slot1 Subslot1 [...]

Byte no.	Item	Data type	Parameter permission	Default	Valid options
160	SNTP mode	Byte	Read/write	0	0 – No changes 1 – Disable 2 – Unicast mode 3 – Broadcast mode
161	SNTP UTC offset	Byte	Read/write	0	0 – No changes Offset values 1-25 representing offset from -12h until +12h
162–177	SNTP server IP address	Char array	Read/write	0	Empty string – No changes IP address in dotted string notation, e.g., 192.168.0.1
178–193	SNTP backup IP address	Char array	Read/write	0	Empty string – No changes IP address in dotted string notation, e.g., 192.168.0.1
194–209	DNS server IP address	Char array	Read/write	0	Same as above
210	Second DNS server IP address	Char array	Read/write	0	Same as above

Table 12-7 Record index 2 – Slot1 Subslot1

Byte no.	Item	Data type	Parameter permission	Default	Valid options
0	Block version	Byte	Read only	0	0 – Indicates this data set
1	Pluggable memory status	Byte	Read only	0	0 – Unknown 1 – Present valid 2 – Present invalid 3 – Not present
2	Reserved				
3	Power supply	Byte	Read only	0	Bit mask of valid power source

Table 12-8 Record index 3 – Slot1 Subslot1

Byte no.	Item	Data type	Parameter permission	Default	Valid options
0	Block version	Byte	Read only	0	0 – Indicates this data set
1	Clear packet statistics	Byte	Read/write	0	0 – Do nothing 255 – Clear statistics of all ports Any other – Select port number to clear

12.2.3.3 PDEV standard records

- Port mode
  - Status of PDEV port
- Link state
  - Read/enable alarm
  - Device properties/status of PDEV port

- Neighbor
  - Read/enable alarm by setting expected neighbor
  - Device properties/status of PDEV port
- MRP role
  - Read/write
  - Device properties/status of PDEV interface
- MRP ports
  - Read/write
  - Device properties/status of PDEV interface
- MRP ring state
  - Read/enable alarm
  - Device properties/status of PDEV interface
- Fiber optic type
  - Read/write
  - Device properties/status of PDEV port
- Port statistics counter
  - Read statistics counter of PDEV port

Table 12-9 Standard records information

Item	Identifier	Elements	Step7 dialog window
PDPortDataReal	0x802A	Getting mediaType, mauType, and neighborhood information from the device	Device status of PDEV port subslot (X1 py)
PDPortDataAdjust	0x802F	Setting mauType of this port (auto neg., 10/100, HD/FD)	Device properties of PDEV port subslot (X1 py)
PDPortDataCheck	0x802B	Enable alarm for data transmission impossible and remote mismatch by specifying expected mautype, linkstate, and neighbor	Device properties of PDEV port subslot (X1 py)
PDInterfaceMrpDataReal	0x8050	Get current MRP role (client, manager) and ring state from the device	Device status of PDEV interface (X1)
PDInterfaceMrpDataAdjust	0x8052	Set MRP role	Device properties of PDEV interface subslot (X1)
PDInterfaceMrpDataCheck	0x8051	Enable alarm for MRP mismatch	Device properties of PDEV interface subslot (X1)
PDPortMrpDataReal	0x8054	Get MRP port state	Device properties of PDEV interface subslot (X1)
PDPortMrpDataAdjust	0x8053	Set MRP ports	Device properties of PDEV interface subslot (X1)
PDPortFODataReal	0x8060	Get adjusted fiberOpticType and fiberOpticCableType as well as the current powerbudget	Device status of PDEV interface subslot (X1 py)

Table 12-9 Standard records information [...]

Item	Identifier	Elements	Step7 dialog window
PDPortFODataAdjust	0x8062	Set fiberOpticType and fiberOpticCableType (will be saved together with the system configuration)	Device properties of PDEV port subslot (X1 py)
PDPortFODataCheck	0x8061	Enable alarm for fiber optic mismatch	Device properties of PDEV port subslot (X1 py)
PDPortStatistic	0x8072	Statistics counter of the port corresponding to IF MIB: ifInOctets, ifOutOctets, ifInDiscards, ifOutDiscards, ifInErrors, ifOutErrors	Not available yet

12.2.3.4 I&M record data

- I&M0
  - Vendor ID, device order ID, and serial number, HW and SW revision
  - Device status of the DAP module (slot 0)/0xAFF0
- I&M1
  - String containing location and function description
  - Device identification/0xAFF1
- I&M2
  - String containing installation date
  - Device identification/0xAFF2
- I&M3
  - String containing description text
  - Device identification/0xAFF3
- I&M4
  - String containing signature
  - Device identification/0xAFF4

12.2.4 Control word/status word

The control word is a special process data item which is used to make settings that cannot be implemented using standard process data.

A command consisting of two bytes is written to the control word of the management agent:

- Byte 0 specifies the action and the new status.
- Byte 1 specifies the port number. If a command is to apply to all ports, the value 0xFF can be sent instead of the port number.

A command should only be sent once, but never in a process data communication cycle. The device responds to each new command exactly once.

The device responds with the same command in the status word.

The following alarms and settings can be activated or deactivated via the control word:

Table 12-10 Alarms and settings

Word		0															
Signal		**High byte**								**Low byte**							
Bit		**15**	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
Alarm link monitoring	Enable	Portnum or 0xFF								0x01							
	Disable	Portnum or 0xFF								0x02							
Alarm power supply	Enable	0x00								0x05							
	Disable	0x00								0x06							
Alarm MRP ring failure	Enable	0x00								0x09							
	Disable	0x00								0x0a							
PlugMem missing	Enable	0x00								0x0b							
	Disable	0x00								0x0c							
SFP missing	Enable	Portnum or 0xFF								0x0d							
	Disable	Portnum or 0xFF								0x0e							
Reset packet error indicator	Reset	0x00								0x1F							
Link enable status	Enable	Portnum								0x20							
	Disable	Portnum								0x21							
Reset packet counter (RMON statistic)	Reset	Portnum or 0xFF															
Configure CRC threshold	–	Threshold value in packets								0x30							
Configure utilization threshold	–	Threshold value in %								0x31							

For detailed information on monitoring CRC errors and port utilization using process data, refer to Sections "CRC error monitoring via PROFINET process data" on page 195 and "Bandwidth monitoring via PROFINET process data" on page 195.

12.2.5 Other cyclic process data

Diagnostic data:

- Link states of all ports (up to 4 bytes)

Table 12-11 Link states

Byte	**Byte 3**						**Byte 2**						**Byte 1**					**Byte 0**				
Bit	**7**	**6**	**5**	**...**	**1**	**0**	**15**	**14**	**13**	**...**	**9**	**8**	**23**	**22**	**...**	**18**	**17**	**32**	**31**	**...**	**25**	**24**
Port	32	31	30	...	26	25	24	23	22	...	18	17	16	15	...	11	10	9	8	...	2	1

- MRP ring failure
- Packet error indicator: At least one packet error or packet loss has occurred at a port due to memory utilization.
- Alarm contact

Table 12-12 Diagnostic data/port states

Bit	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
Port	MRP status 0 – No diagnostics 1 – MRP ring failure			Packet error indicator 0 – No error 1 – Error counter increased				Alarm contact 1 0 – Closed 1 – Open

- Port information, one byte per port (ports constitute individual slot 2, subslot 1)
  - Blocking state
  - CRC threshold
  - Utilization threshold
  - SFP module available
  - Port enable status
  - Far end fault status
  - Link status

Table 12-13 Diagnostic data/meaning

Bit	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
Port	Blocking state 0 – Forwarding 1 – Blocking	CRC threshold 0 – Not reached 1 – Reached[1]	Utilization threshold 0 – Not reached 1 – Reached[1]		SFP module 0 – None 1 – Available	Port enable status 0 – Enabled 1 – Disabled	Far end fault 0 – No fault 1 – FEFI	Link status 0 – Link down 1 – Link up

[1] Additional bit for changing an error counter.
The bit should be acknowledged before it is reset to “0” in order to prevent the loss of information.

12.2.6 Device naming

In order to commission a switch in “PROFINET” operating mode, each switch must be assigned a name once, i.e., each PROFINET device is assigned a unique device name.

To do this, complete a device search via the engineering tool (“Read PROFINET” function in PLCnext Engineer) during which all the accessible devices in the network are listed. After identifying unknown devices via the specified MAC address or the “flashing” function, the device name configured in the engineering tool is saved permanently on the switch using the “Assign Name” function.

12.2.7 Operating in the PROFINET Environment

A switch that has already been assigned a name starts in “PROFINET” operating mode without an IP address and waits for an IP configuration to be assigned. After the project has been translated and downloaded to the controller, the controller implements startup and configuration.

As soon as a communication relationship has been successfully established between the switch and the controller, the switch starts its management interfaces. The switch indicates that the PROFINET connection has been established correctly by means of an entry in the Event Table.

12.2.8 Adding blocks to TIA

Various acyclic data is stored in TIA 17 that goes beyond the data offered as standard by TIA. This includes, for example, information on whether there is an SD card inserted in the device or the alarm contact status. You will find the complete list in Section “PN records (acyclic)” on page 182.

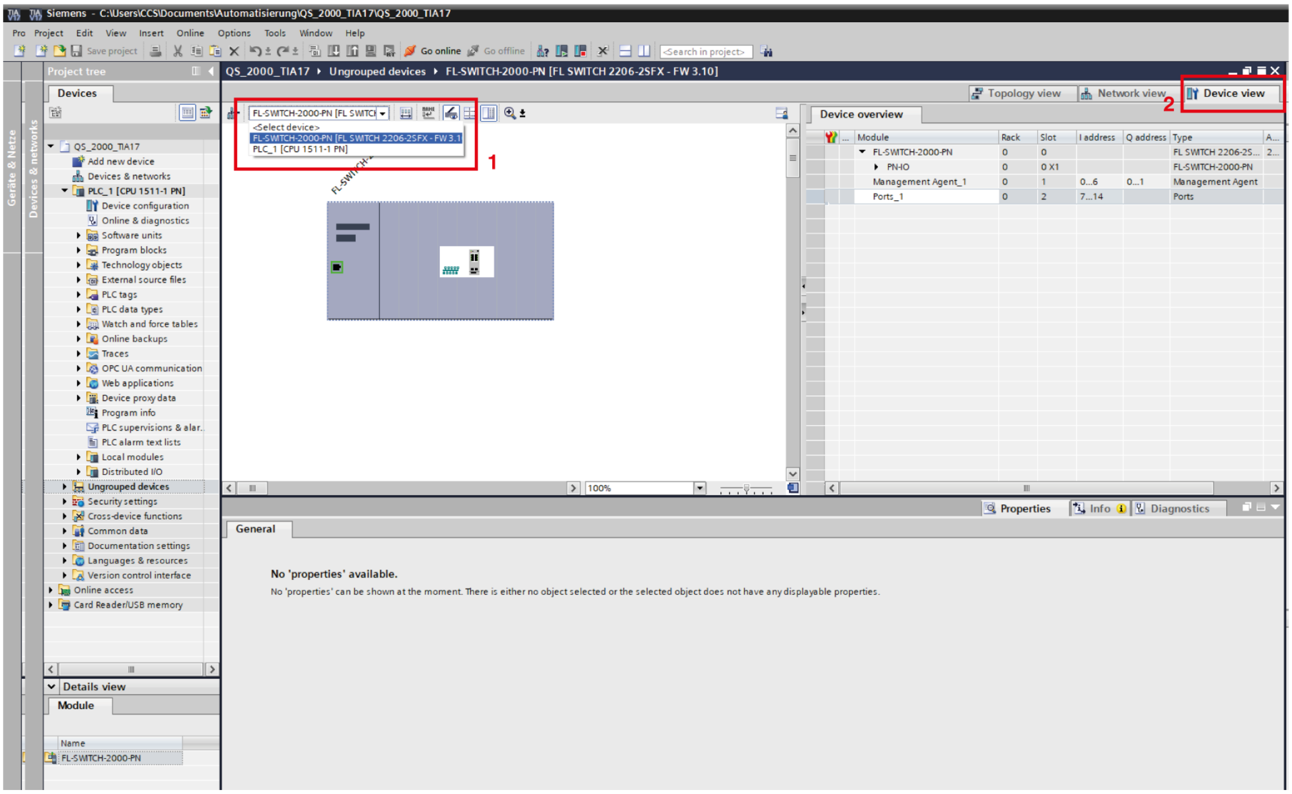
You need a custom-programmed function to call up and interpret this data. You will find examples of such functions in TIA’s integrated help feature.

The following section explains how you can obtain the variables required to call up the data.

12.2.8.1 Finding the internal hardware identifier

The internal hardware identifier must be stored in the variable “Ihw_ID”.

Figure 12-2 TIA: Opening the device view



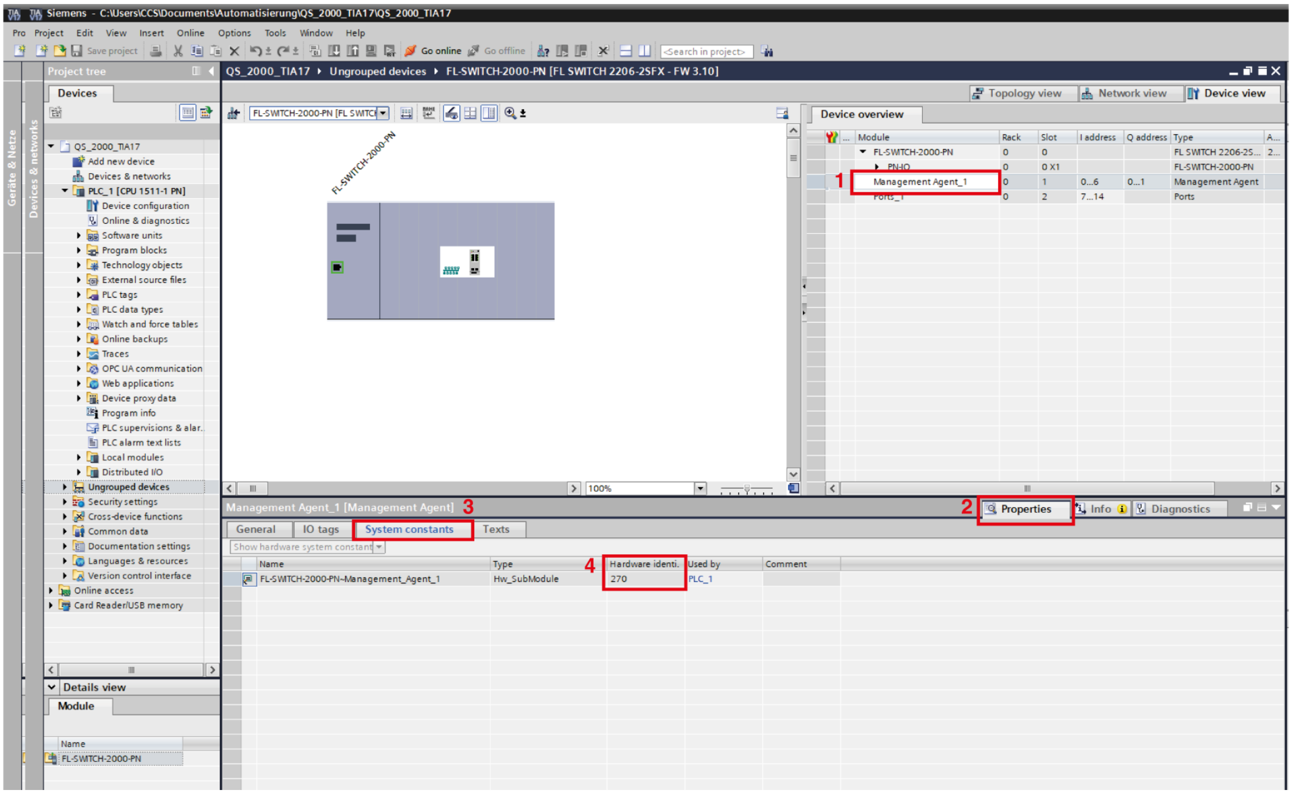
	...	Module	Rack	Slot	I address	Q address	Type	A...
		FL-SWITCH-2000-PN	0	0			FL SWITCH 2206-2S...	2...
		PN-IO	0	0 X1			FL-SWITCH-2000-PN	
		Management Agent_1	0	1	0...6	0...1	Management Agent	
		Ports_1	0	2	7...14		Ports	

No 'properties' available.

No 'properties' can be shown at the moment. There is either no object selected or the selected object does not have any displayable properties.

- Open the device view and select the desired device from the drop-down list.
- Open the device overview on the right.

Figure 12-3 TIA: Finding the internal hardware identifier



Module	Rack	Slot	I address	Q address	Type	A...
FL-SWITCH-2000-PN	0	0			FL SWITCH 2206-2S...	2...
PN-IO	0	0 X1			FL-SWITCH-2000-PN	
Management Agent_1	0	1	0...6	0...1	Management Agent	
Ports_1	0	2	7...14		Ports	

Management Agent_1 [Management Agent]

Name	Type	Hardware identi.	Used by	Comment
FL-SWITCH-2000-PN~Management_Agent_1	Hw_SubModule	270	PLC_1	

- Click on “Ports_1” (slot 1) or “Management Agent_1” (slot 2).

Note that the two slots have different hardware identifiers.

- Click on “Properties, System constants”.

⇒ You will find the internal hardware identifier in the “Hardware identifier” field. The internal hardware identifier is automatically assigned by TIA and cannot be changed.

12.2.8.2 Finding the record index

The record index of the desired data must be stored in the variable “Iw_Index”.

- Select the desired date from the table, see “PN records (acyclic)” on page 182.

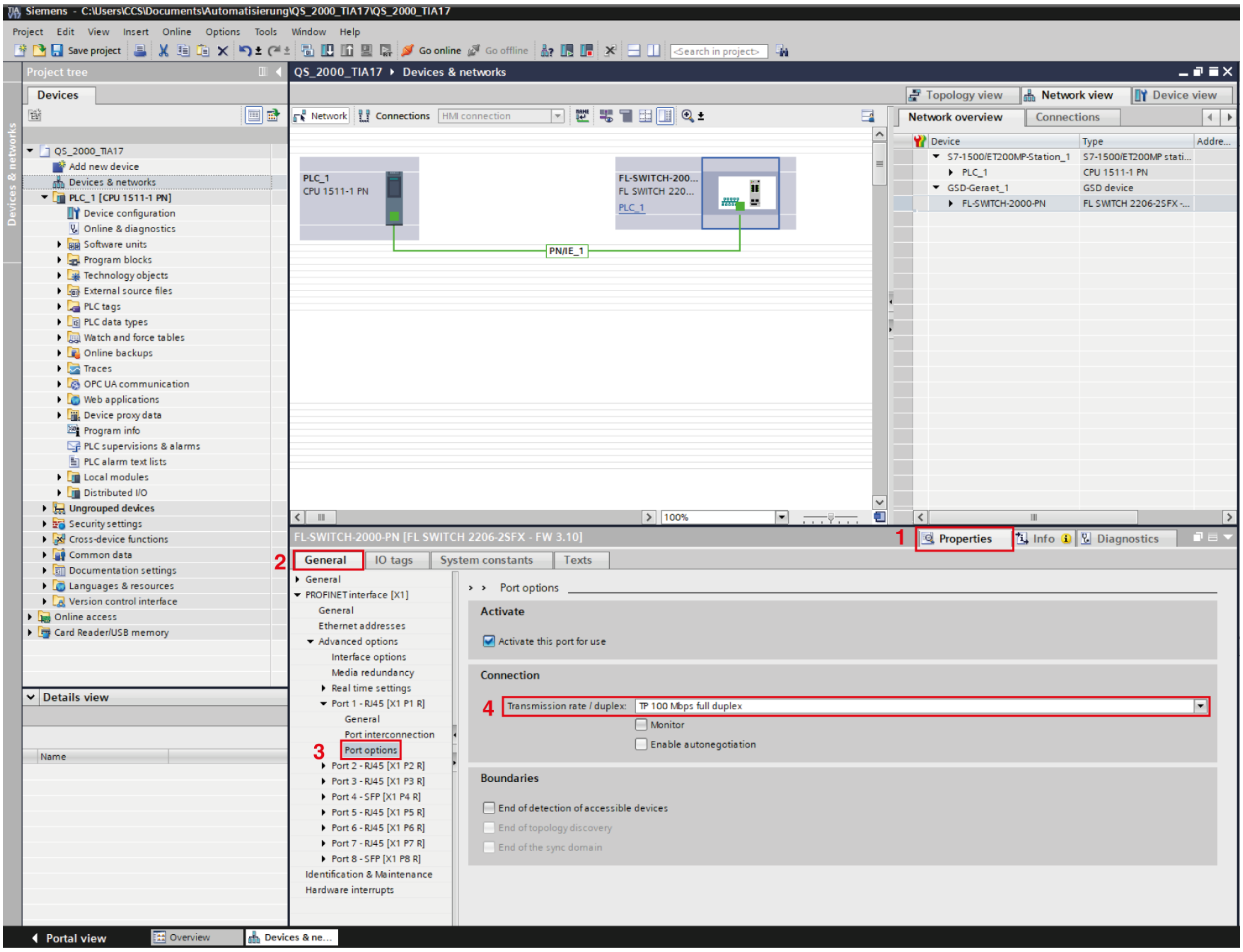
⇒ You will find the record index, e.g., “0x0PP”, in the header of the corresponding table. For port 1, the record index would then be, e.g., “0x001”.

Note that the amount of data returned may be significant.

12.2.9 Fast startup in TIA

To activate Fast Startup mode in TIA, perform the following steps:

Figure 12-4 Fast Startup mode in TIA



Device	Type	Addre...
S7-1500/ET200MP-Station_1	S7-1500/ET200MP stati...	
PLC_1	CPU 1511-1 PN	
GSD-Geraet_1	GSD device	
FL-SWITCH-2000-PN	FL SWITCH 2206-2SFX -...	

› › Port options

Activate

☑ Activate this port for use

Connection

Transmission rate / duplex: TP 100 Mbps full duplex

□ Monitor

□ Enable autonegotiation

Boundaries

□ End of detection of accessible devices

□ End of topology discovery

□ End of the sync domain

- In the desired device, click on “Properties, General” and then on the desired port.
- Click on “Port options”.
- In the “Connection” area, select “TP 100 Mbps full duplex” for “Transmission rate / duplex”.

⇒ Fast startup is set up for this port.

Note that the transmission rate on the connected device must also be set to 100 Mbps with full duplex.

12.3 PROFINET alarms

The FL SWITCH 22xx/23xx/24xx/25xx/26xx/27xx versions are able to send the following alarms (the alarms are deactivated upon device start):

- Power supply management agent
  - (Slot 1) appears when redundant power supply is lost
- MRP ring failure management agent
  - (Slot 1) appears when MRP manager detects ring failure, MRP clients do not support this alarm, PlugMem missing
- PlugMem missing
  - (Slot 1) appears when pluggable memory is missing
- Link monitoring
  - (SFP, interface or fixed) appears when link is down on that port
- SFP module missing

Standard PROFINET alarms

- Data transmission impossible
  - Appears when link is down or port mode does not match the specified value (default: disabled)
- Remote mismatch
  - Appears when neighbor information does not match the specified one (default: disabled)
- Media redundancy mismatch
  - Appears when MRP manager detects a ring failure (default: disabled)
- Fiber optic mismatch
  - Appears when system reserve is reached or consumed on POF SCRJ ports (default: disabled)

12.3.1 Alarms in web-based management

In PROFINET mode, you can activate all alarms supported by the PROFINET device on the “PROFINET Configuration” page (see “PROFINET Configuration” on page 64). The PN devices transmit the PROFINET alarms to the controller.

ℹ The settings made for the PROFINET alarms can be saved with the configuration. The controller can transmit a differing alarm configuration to the switch and thereby overwrite the configuration settings.

12.4 PDEV function description

The PDEV function provides an extended range of functions for switches in PROFINET mode. This includes displaying of neighbor and topology information in the engineering tool. This information is determined using the Link Layer Discovery Protocol (LLDP) and can be used, for example, to compare the target and actual network.

In addition, the PDEV function is used to display the transmitted information via the respective Ethernet ports.

The PDEV function uses two submodules:

- Interface submodule with port number 0x8X00 (X: from 0 to F)

– Port submodule with port number 0x8IXX (I: interface ID; X: port number)

These submodules are represented in the Step 7 engineering tool. PROFINET communication enables information about the port speed, duplex mode, and the link status to be read. An engineering tool reads and then shows the neighbor and topology information via SNMP.

12.5 CRC error monitoring via PROFINET process data

Use this optional function to monitor the number of CRC errors on the device via the status word and control word.

The control word can be used to activate the function and configure a threshold value for monitoring (see “Configure CRC threshold” in Table 12-11).

This threshold value applies to all ports. Port-specific threshold values cannot be configured. Resetting the threshold value to “0” deactivates the function.

The CRC error value of each port is then checked against the configured threshold value.

– If the threshold value is exceeded on a port, the bit flag of the port data in the status word is set to “1” (see Table 12-13).

The bit flag can be reset for individual ports via the control word:

– Resetting the port-specific packet counter (see “Reset packet counter (RMON statistic)“ in Table 12-11)

– Resetting the CRC threshold to “0” (see “Configure CRC threshold” in Table 12-11)

12.6 Bandwidth monitoring via PROFINET process data

Use this optional function to monitor the proportional utilization of the maximum bandwidth of individual ports via the status word and control word.

The control word can be used to activate the function and configure a threshold value for monitoring (see “Configure utilization threshold” in Table 12-11).

This threshold value applies to all ports. Port-specific threshold values cannot be configured. Resetting the threshold value to “0” deactivates the function.

RX utilization of each port is then checked against the configured threshold value.

– If the threshold value is exceeded on a port, the bit flag of the port data in the status word is set to “1” (see Table 12-13).

– If the utilization falls below the threshold value, the bit flag is automatically reset. Changing the threshold value to “0” (see “Configure utilization threshold” in Table 12-11) also resets the bit flag.

ℹ RX utilization of the individual ports is determined as a mean value over an interval of 30 seconds. For this reason, status changes remain active for at least 30 seconds.

13 Layer 3 functions – routing and NAT (FL NAT 2xxx only)

The NAT switches of the FL NAT 2000 product family provide a flexible port constellation and can thus be adapted to practically any application. After the necessary interfaces have been created, you can define the relevant ports and configure the NAT mechanism or routing function.

ℹ In a NAT application, all of the LAN devices that should be accessible from the WAN require a gateway address.

ℹ An FL NAT 2000 switch should not simultaneously operate in NAT mode and as an MRP manager because temporary connection interruptions can occur as a result of switch-over or topology changes. This particularly applies to applications with real-time data communication (e.g., PROFINET).

ℹ Since no firewall mechanisms are activated when NAT mode is switched on, normal routing to the LAN IP addresses is still possible.
When using NAT, connected network devices on the WAN side cannot have an IP address that is also used on the LAN side. The same applies to any secondary addresses.

13.1 Factory default

To set the device to the factory default configuration, see “Using Smart mode” on page 22. The following NAT configuration is preset in the default state:

- Routing active
- LAN1 created (IP addressing: BootP, ports: two to eight)
- LAN2 created (IP addressing: DHCP, ports: 1)

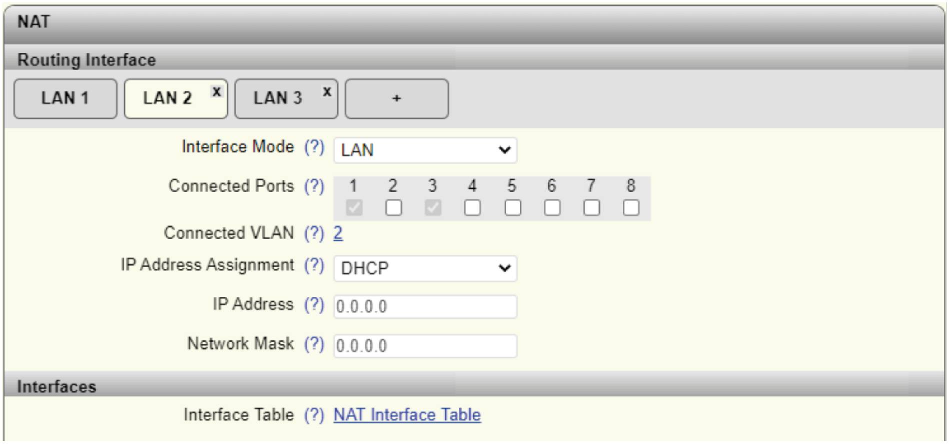
13.2 Creating interfaces

You can create new interfaces for NAT in web-based management.

ℹ Note that NAT mode should not be configured on the interface “LAN 1” if possible. This interface provides additional LAN services (e.g., PROFINET and DHCP server).

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, NAT”.

Figure 13-1 NAT



Interface Mode (?) LAN

Connected Ports (?)

1	2	3	4	5	6	7	8
☑	□	☑	□	□	□	□	□

Connected VLAN (?) 2

IP Address Assignment (?) DHCP

IP Address (?) 0.0.0.0

Network Mask (?) 0.0.0.0

Interface Table (?) NAT Interface Table

- Click on “+” to create a new routing interface.
- Make the desired settings.

Table 13-1 Routing Interface: Parameters

Parameter	Description
Interface Mode	– LAN: This option creates a simple routing interface. Select this option, if the NAT switch is to be operated in a simple router mode or used as an interface for a LAN area that is to be translated to another network. – 1-to-1-NAT: This option creates a WAN interface that uses the 1:1 NAT mechanism to translate IP addresses from a LAN area to the WAN (see “Configuring 1:1 NAT” on page 201). – Virtual NAT: This option creates a WAN interface that uses the virtual NAT mechanism to translate IP addresses from a LAN area to the WAN (see “Configuring virtual NAT” on page 203). – IP Masquerading: This option creates a WAN interface that uses the IP masquerading mechanism to translate IP addresses from a LAN area to the WAN (see “Configuring IP masquerading” on page 204).
Connected Ports	Activate the check boxes for the ports that you want to add to the interface.
Connected VLAN	The assigned VLAN is displayed here.
IP Address Assignment	Select the type of IP address assignment. – STATIC: Static IP address – BOOTP: Assignment via the Bootstrap protocol – DHCP: Assignment via a DHCP server

Table 13-1 Routing Interface: Parameters

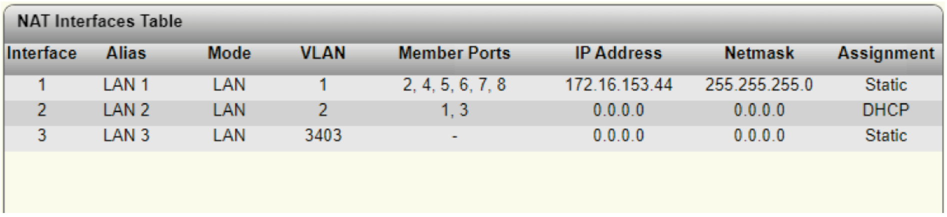
Parameter	Description
IP Address	This option is only available if you selected “STATIC” for “IP Address Assignment”. Here, enter the IP address of the new interface.
Network Mask	This option is only available if you selected “STATIC” for “IP Address Assignment”. Here, enter the subnet mask of the new interface.
Interface Table	Click on “NAT Interface Table” to open the “NAT Interfaces Table” page (see “Pop-up window: NAT Interfaces Table” on page 199). This contains an overview table of all configured interfaces.

- Save your settings with “Apply&Save”.

Pop-up window: NAT Interfaces Table

The table contains an overview of all NAT interfaces as well as the settings made for each.

Figure 13-2 Pop-up window: NAT Interfaces Table

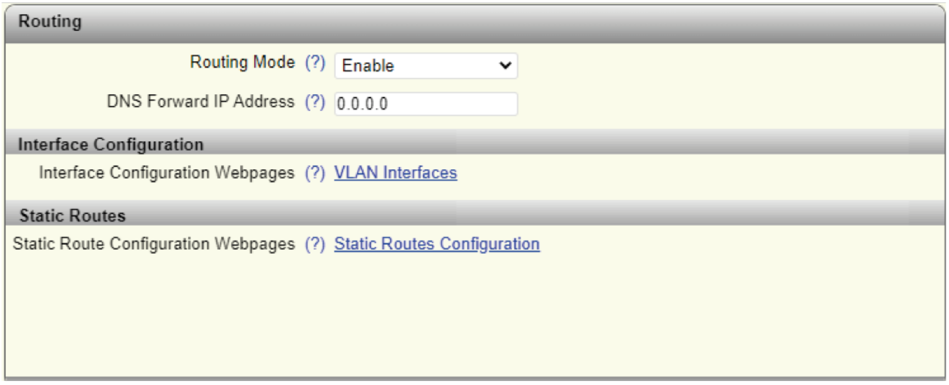


NAT Interfaces Table

Interface	Alias	Mode	VLAN	Member Ports	IP Address	Netmask	Assignment
1	LAN 1	LAN	1	2, 4, 5, 6, 7, 8	172.16.153.44	255.255.255.0	Static
2	LAN 2	LAN	2	1, 3	0.0.0.0	0.0.0.0	DHCP
3	LAN 3	LAN	3403	-	0.0.0.0	0.0.0.0	Static

13.3 Routing

Figure 13-3 Routing



Routing

Routing Mode (?) Enable

DNS Forward IP Address (?) 0.0.0.0

Interface Configuration

Interface Configuration Webpages (?) VLAN Interfaces

Static Routes

Static Route Configuration Webpages (?) Static Routes Configuration

Table 13-2 Routing: Parameters

Parameter	Description
Routing Mode	Select whether routing should be activated globally for the device.
DNS Forward IP Address	Enter the IP address to which the DNS queries to this device should be forwarded.

Routing: Interface Configuration

Table 13-3 Interface Configuration: Parameters

Parameter	Description
Interface Configuration Webpages	Click on “VLAN Interfaces” to open the “VLAN Interface Configuration” pop-up window (see “Pop-up window: VLAN Interface Configuration” on page 200).

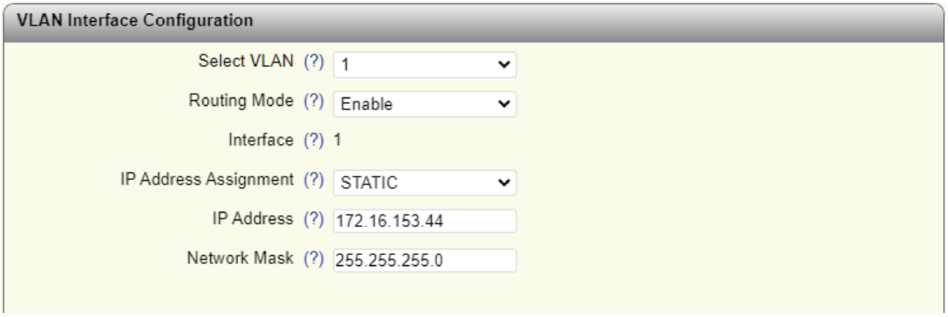
Routing: Static Routes

Table 13-4 Static Routes: Parameters

Parameter	Description
Static Route Configuration Webpages	Click on “Static Routes Configuration” to open the “Static Routes Configuration” pop-up window (see “Routing: Static Routes” on page 200).

Pop-up window: VLAN Interface Configuration

Figure 13-4 Pop-up window: VLAN Interface Configuration



VLAN Interface Configuration

Select VLAN (?) 1

Routing Mode (?) Enable

Interface (?) 1

IP Address Assignment (?) STATIC

IP Address (?) 172.16.153.44

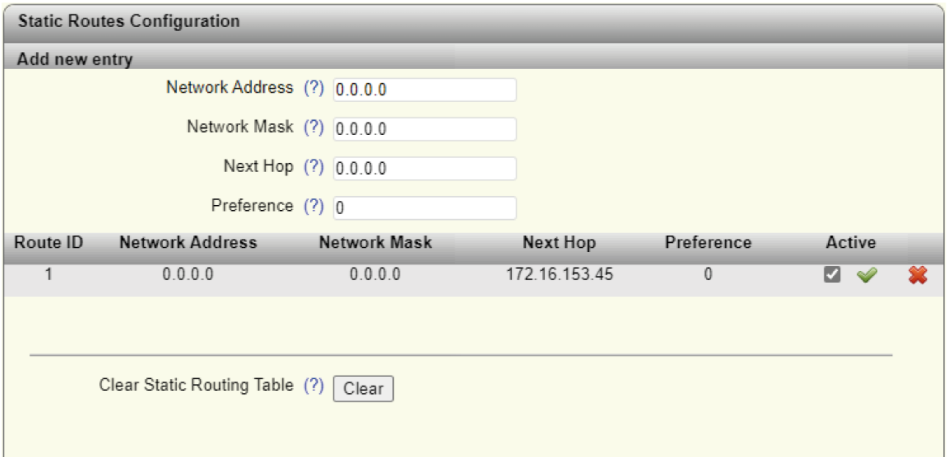
Network Mask (?) 255.255.255.0

Table 13-5 Routing: Parameters

Parameter	Description
Select VLAN	Select the VLAN for which you wish to configure routing.
Routing Mode	Select whether routing should be activated for the selected VLAN.
Interface	The layer 3 interface that is connected to the routing VLAN is displayed here.
IP Address Assignment	Select the type of IP address assignment. – STATIC: Static IP address – BOOTP: Assignment via the Bootstrap protocol – DHCP: Assignment via a DHCP server
IP Address	This option is only available if you selected “STATIC” for “IP Address Assignment”. Here, enter the IP address of the new interface.
Network Mask	This option is only available if you selected “STATIC” for “IP Address Assignment”. Here, enter the subnet mask of the new interface.

Pop-up window: Static Routes Configuration

Figure 13-5 Pop-up window: Static Routes Configuration



Static Routes Configuration

Add new entry

Network Address (?) 0.0.0.0

Network Mask (?) 0.0.0.0

Next Hop (?) 0.0.0.0

Preference (?) 0

Route ID	Network Address	Network Mask	Next Hop	Preference	Active	
1	0.0.0.0	0.0.0.0	172.16.153.45	0	☑ ✓	✖

Clear Static Routing Table (?) Clear

Table 13-6 Pop-up window: Static Routes Configuration: Parameters

Parameter	Description
Network Address	Here, enter the IP address of the destination network to which the static route refers.
Network Mask	Here, enter the subnet mask of the destination network to which the static route refers.
Next Hop	Here, enter the IP address of the next router on the way to the destination network.
Preference	Here, specify the priority of the static route. The lower the value, the higher the priority. Enter “0” for no priority.
Clear Static Routing Table	Click on “Clear” to delete all static routes.

13.4 Static routing

Static routing enables communication between two or more different subnets. The devices of the FL NAT 2000 product family automatically route between the created LAN interfaces.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, Routing, Static Routes Configuration”.
- Enter the desired details (see “Pop-up window: Static Routes Configuration” on page 201).
- Click on “Apply” or “Apply&Save” to add the new static route.

For a default route, set the value 0.0.0.0 for the network address and the network mask.

13.5 Configuring 1:1 NAT

With 1:1 NAT, each device in the LAN is assigned an IP address from the higher-level network (WAN). The device can then be addressed from the WAN via this assigned address.

Advantages:

- No route/gateway configuration necessary in the WAN
- Communication can be established from both the LAN and WAN.
- Not restricted to dedicated protocols.

Disadvantage:

- An IP address must be reserved in the WAN for each device that should be accessible in the LAN.

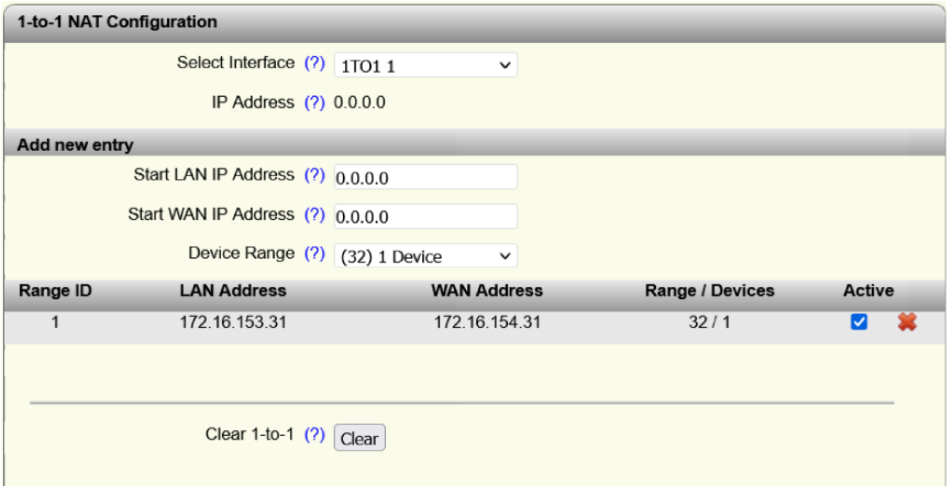
When using 1:1 NAT, connected network devices on the WAN side cannot have an IP address that is also used on the LAN side. The same applies to any secondary addresses.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, NAT, +”.
- For “Interface Mode”, select the “1-to-1 NAT” option.
- Click on “Apply”.

Once you have clicked on “Apply”, the additional option “NAT 1-to-1” appears.

- Click on “NAT 1-to-1” to open the “1-to-1 NAT Configuration” pop-up window.

Figure 13-6 Pop-up window: 1-to-1 NAT Configuration



1-to-1 NAT Configuration

Select Interface (?) 1TO1 1

IP Address (?) 0.0.0.0

Add new entry

Start LAN IP Address (?) 0.0.0.0

Start WAN IP Address (?) 0.0.0.0

Device Range (?) (32) 1 Device

Range ID	LAN Address	WAN Address	Range / Devices	Active	
1	172.16.153.31	172.16.154.31	32 / 1	☑	✖

Clear 1-to-1 (?) Clear

Table 13-7 1-to-1 NAT Configuration: Parameters

Parameter	Description
Select Interface	The interface is displayed here. There is only ever one interface available.
IP Address	The IP address of the client is displayed here.
Start LAN IP Address	Here, enter the start IP address of the area that is to be translated.

Table 13-7 1-to-1 NAT Configuration: Parameters

Parameter	Description
Start WAN IP Address	Here, enter the start IP address of the area that is to be translated to. The IP addresses must be reserved in the higher-level network. Using 1:1-NAT, the device translates them to the LAN IP address specified above.
Device Range	Here, select the number of IP addresses that are to be translated.
Clear 1-to-1	Click on “Clear” to delete the complete table for the selected interface.

- Set the parameters as desired.
- Click on “Apply” to populate the table with the entered data.
- To populate the table with more data, enter the desired parameters again and click on “Apply”.

13.6 Configuring virtual NAT

Virtual NAT combines 1:1 NAT with a virtual router level. In this router level, the address is mapped from the LAN and is then transferred to the WAN from the virtual intermediate level as with standard routing.

Advantage:

– Only one IP address is required from the WAN: for the NAT interface itself

Disadvantage:

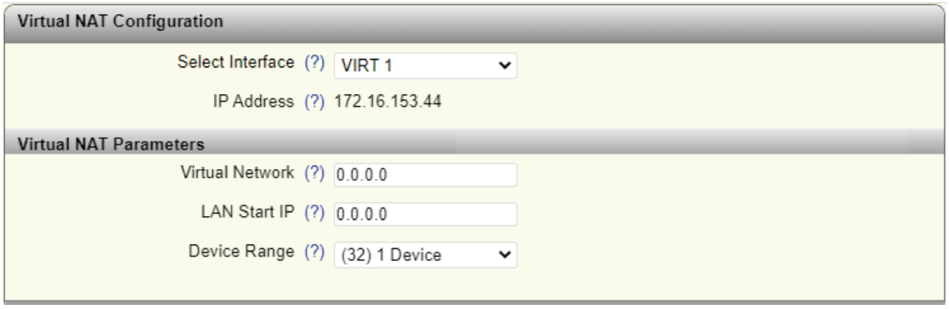
– In the WAN, the route to the (virtual) network must be indicated and the NAT WAN interface entered as the next hop or gateway address.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, NAT, +”.
- For “Interface Mode”, select the “Virtual NAT” option.
- Click on “Apply”.

Once you have clicked on “Apply”, the additional option “NAT Virtual” appears.

- Click on “NAT Virtual” to open the “Virtual NAT Configuration” pop-up window.

Figure 13-7 Pop-up window: Virtual NAT Configuration



Virtual NAT Configuration

Select Interface (?) VIRT 1

IP Address (?) 172.16.153.44

Virtual NAT Parameters

Virtual Network (?) 0.0.0.0

LAN Start IP (?) 0.0.0.0

Device Range (?) (32) 1 Device

Table 13-8 Virtual NAT Configuration: Parameters

Parameter	Description
Select Interface	The interface is displayed here. There is only ever one interface available.
IP Address	The IP address of the client is displayed here.
Virtual Network	Here, enter the IP address of the virtual network.
LAN Start IP	Here, enter the start IP address of the area that is to be translated.
Device Range	Here, select the number of IP addresses that are to be translated.

- Set the parameters as desired.
- Click “Apply” to save the settings.

13.7 Configuring IP masquerading

The NAT device acts as a proxy, so that all of the LAN devices communicate externally using the IP address of the NAT/WAN port. Various TCP/UDP ports are used to differentiate between the different LAN devices.

Advantages:

– No additional WAN addresses are required aside from the address for the NAT device itself.

– No route/gateway configuration necessary in the WAN

Disadvantage:

– WAN devices can only communicate with LAN devices via port forwarding.

Standard IP masquerading does not require any detailed configuration and is automatically active following creation of the interface. All LAN areas are then translated to this interface.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, NAT, +”.
- For “Interface Mode”, select the “IP Masquerading” option.
- Click on “Apply”.

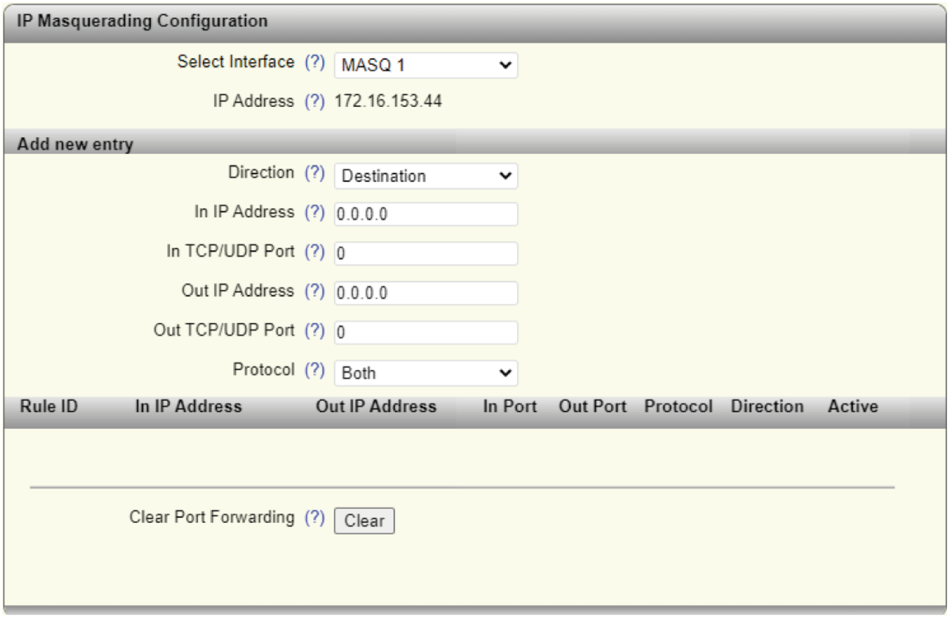
Once you have clicked on “Apply”, the additional option “NAT Port Forwarding” appears.

- Click on “NAT Port Forwarding” to open the “IP Masquerading Configuration” pop-up window (see “Configuring port forwarding” on page 205).

13.8 Configuring port forwarding

With port forwarding, you can access a specific service of a specific LAN device from the WAN network. The WAN interface of the NAT device is addressed using a defined TCP/UDP port number in order to implement forwarding to the desired LAN device.

Figure 13-8 Pop-up window: IP Masquerading Configuration



IP Masquerading Configuration

Select Interface (?) MASQ 1

IP Address (?) 172.16.153.44

Add new entry

Direction (?) Destination

In IP Address (?) 0.0.0.0

In TCP/UDP Port (?) 0

Out IP Address (?) 0.0.0.0

Out TCP/UDP Port (?) 0

Protocol (?) Both

Rule ID	In IP Address	Out IP Address	In Port	Out Port	Protocol	Direction	Active

Clear Port Forwarding (?)

Table 13-9 IP Masquerading Configuration: Parameters

Parameter	Description
Select Interface	The interface is displayed here.
IP Address	The IP address of the client is displayed here.
Direction	Select the port forwarding direction. – Destination: Select this option for WAN to LAN (see “IP Masquerading Configuration: Destination” on page 206). – Source: Select this option for LAN to WAN (see “IP Masquerading Configuration: Source” on page 206).
Clear Port Forwarding	Click on “Clear” to delete the complete table for the selected interface.

IP Masquerading Configuration: Destination

Table 13-10 IP Masquerading Configuration: Destination: Parameters

Parameter	Description
In IP Address	Enter the IP address for incoming packets from the WAN to the device. These packets are forwarded to the defined destination in the LAN. If you enter “0.0.0.0”, each incoming packet will be forwarded to the defined destination in the LAN using the defined port.
In TCP/UDP Port	Enter the TCP/UDP port for incoming packets from the WAN to the device. These packets are forwarded to the defined destination in the LAN.
Out IP Address	Enter the IP address in the LAN to which the incoming packets should be forwarded in the device.
Out TCP/UDP Port	Enter the TCP/UDP port in the LAN to which the incoming packets should be forwarded in the device.
Protocol	Select the protocol to be used for sending packets. – TCP – UDP – Both: TCP and UDP are used.

IP Masquerading Configuration: Source

The “Source” option is only necessary if protocols are used that have a fixed port number as the specified source and that do not support dynamic port assignment.

Table 13-11 IP Masquerading Configuration: Source: Parameters

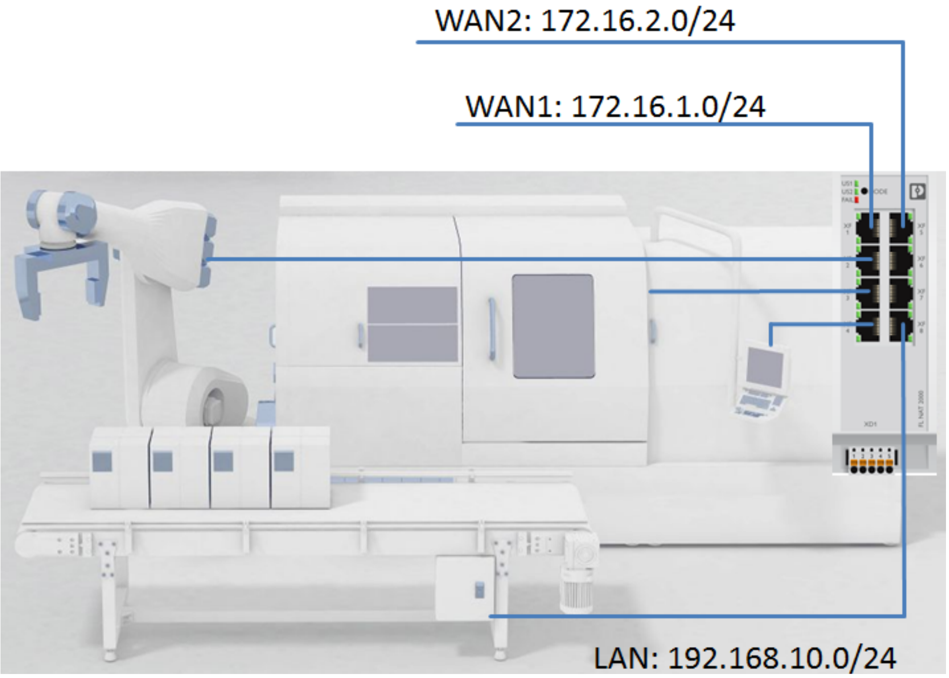
Parameter	Description
In IP Address	Enter the IP address for incoming packets from the LAN to the device. These packets are forwarded to the defined destination in the WAN.
In TCP/UDP Port	Enter the TCP/UDP port for incoming packets from the LAN to the device. These packets are forwarded to the defined destination in the WAN.
Out IP Address	Enter the IP address in the WAN to which the incoming packets should be forwarded in the device.
Out TCP/UDP Port	Enter the TCP/UDP port in the WAN to which the incoming packets should be forwarded in the device.
Protocol	Select the protocol to be used for sending packets. – TCP – UDP – Both: TCP and UDP are used.

- Set the parameters as desired.
- Click on “Apply” to populate the table with the entered data.
- To populate the table with more data, enter the desired parameters again and click on “Apply”.

13.9 Example applications

To illustrate the configuration sequence, the following shows how a machine is connected to two higher-level WAN networks via 1:1 NAT. Five devices from the machine should be accessible from both higher-level networks: 192.168.10.2–192.168.10.6.

Figure 13-9 Sample application: Connecting a machine using 1:1 NAT



Step 1: Setting up the LAN interface

- After an IP address has been assigned on the LAN side, it can be used to access the web interface via the LAN ports.

  In this example, the NAT switch on the LAN has IP address 192.168.10.254.
- The configuration options for the NAT function are available under the “NAT” menu item.
- Two LAN interfaces have already been created in default mode: LAN1 with ports 2 to 8, and LAN2 with port 1.

  LAN1 is configured as the internal LAN interface with ports 3 to 8. LAN port assignment is based on the WAN configuration.

Step 2: Setting up both WAN interfaces

Set up the first WAN interface:

1. Select LAN2 and set it up as a 1:1 NAT interface via the drop-down menu.
2. Set the WAN IP parameters.
3. Click “Apply” to save the settings.

Set up the second WAN interface:

1. Create another interface using “+”.
2. Select “1:1-NAT” and set the IP parameters.

3. Click “Apply” to save the settings.
4. Use the check box to assign Port2 to the second WAN interface. The port is automatically deleted from LAN1.
5. Click “Apply” to save the settings.

Step 3: Configuring both NAT tables

To configure the 1:1-NAT tables, click on “NAT 1-to-1”.

Set the following parameters:

Parameters for WAN 1 (1TO1 1)

- Start LAN IP address: 192.168.10.8
- Start WAN IP address: 172.16.1.8
- Device range: 8 devices

Parameters for WAN2 (1TO1 2)

- Start LAN IP address: 192.168.10.8
- Start WAN IP address: 172.16.2.8
- Device range: 8 devices

14 Power management (SPE versions only)

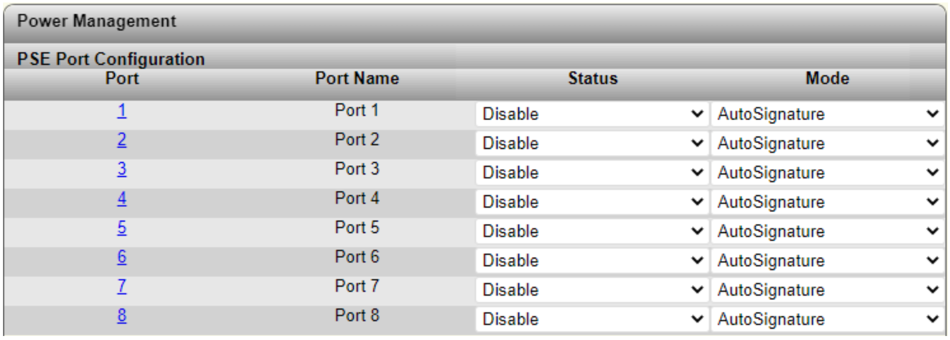
The SPE versions of the switches offer Single Pair Ethernet connections for efficient data transmission in factory and process automation. The reduced cabling provides the basis for future-proof Ethernet communication.

14.1 Power Management

On this page, you can make settings for SPE.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Configuration, Power Management”.

Figure 14-1 Power Management



Power Management

PSE Port Configuration

Port	Port Name	Status	Mode
1	Port 1	Disable	AutoSignature
2	Port 2	Disable	AutoSignature
3	Port 3	Disable	AutoSignature
4	Port 4	Disable	AutoSignature
5	Port 5	Disable	AutoSignature
6	Port 6	Disable	AutoSignature
7	Port 7	Disable	AutoSignature
8	Port 8	Disable	AutoSignature

Table 14-1 Power Management: Parameters

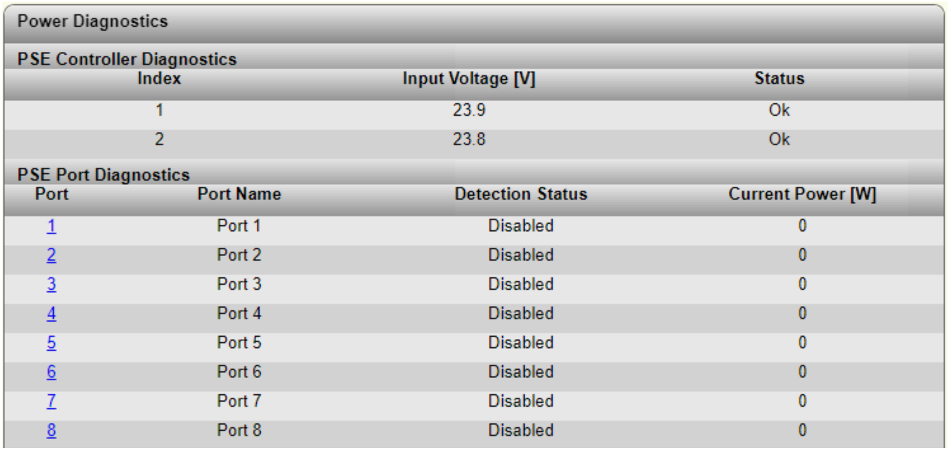
Parameter	Description
Port	Click on the relevant port number to open the “Port Configuration” window for this port (see “Port Configuration” on page 66).
Port Name	The name of the respective port is displayed here. You can change the name on the “Port Configuration” page (see “Port Configuration” on page 66).
Status	Select whether the respective port should be supplied with power.
Mode	Select the mode. – AutoSignature: In this mode, the device checks whether a power device is connected. Only then is the voltage switched on. – Force: In this mode, the voltage is switched on directly. A warning message is displayed.

14.2 Power Diagnostics

On this page, you can view diagnostic data for your SPE device.

- Open web-based management (see “Accessing web-based management” on page 35) and log in.
- Click on “Diagnostics, Power Diagnostics”.

Figure 14-2 Power Diagnostics



Power Diagnostics

PSE Controller Diagnostics

Index	Input Voltage [V]	Status
1	23.9	Ok
2	23.8	Ok

PSE Port Diagnostics

Port	Port Name	Detection Status	Current Power [W]
1	Port 1	Disabled	0
2	Port 2	Disabled	0
3	Port 3	Disabled	0
4	Port 4	Disabled	0
5	Port 5	Disabled	0
6	Port 6	Disabled	0
7	Port 7	Disabled	0
8	Port 8	Disabled	0

Power Diagnostics: PSE Controller Diagnostics

Table 14-2 PSE Controller Diagnostics: Parameters

Parameter	Description
Index	A running index of all entries is displayed here.
Input Voltage [V]	The input voltage of the respective PSE controller is displayed here.
Status	The status of the respective PSE controller is displayed here.

Power Diagnostics: PSE Port Diagnostics

Table 14-3 PSE Port Diagnostics: Parameters

Parameter	Description
Port	Click on the relevant port number to open the “Port Configuration” window for this port (see “Port Configuration” on page 66).
Port Name	The name of the respective port is displayed here. You can change the name on the “Port Configuration” page (see “Port Configuration” on page 66).
Detection Status	This shows the port status, e.g., “Delivering Power” or “Disabled”.
Current Power [W]	The current power is displayed here.

A Revision history

Revision	Date	Contents
00	2019-07-31	First publication of the firmware manual – Separation of hardware and firmware manual – Update to firmware version 2.80
01	2020-07-07	– Update to firmware version 2.90
02	2021-02-04	– Update to firmware version 3.00 – Addition of new IP67 versions (FL SWITCH 26xx/27xx)
03	2021-11-25	– Update to firmware version 3.10
04	2021-12-15	– Addition of a note
05	2023-01-23	– Update to firmware version 3.20 – Addition of the new SPE versions – New section: RADIUS certificates – New section: Power management – Adjustments to layout – General additions
06	2023-02-09	– Update to formware version 3.21 – Addition of the Root CA Certificates description – Error correction in section „File Transfer“ – Change of behaviour of LED2 (SPE versions) with active Force Mode – Addition of parameter „SNMPv3 authentication“ in section „Service“

ℹ The changes to the firmware can be found in the respective release notes available to download with the firmware in the e-shop.

B Appendixes

B 1 List of figures

Section 1

Section 2

Section 3

Section 4

Section 5

Section 6

Section 7

Section 8

Section 9

Section 10

Section 11

Section 12

Section 13

Section 14

Appendix A

Appendix B

B 2 List of tables

Section 1

Section 2

Section 3

Section 4

Section 5

Section 6

Section 7

Section 8

Section 9

Section 10

Section 11

Section 12

Section 13

Section 14

Appendix A

Appendix B

Please observe the following notes

General Terms and Conditions of use for technical documentation

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular user documentation) does not constitute any further duty on the part of Phoenix Contact to furnish information on modifications to products and/or technical documentation. You are responsible to verify the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

In general, the provisions of the current general Terms and Conditions of Phoenix Contact apply exclusively, in particular as concerns any warranty liability.

This manual, including all illustrations contained herein, is copyright protected. Any changes to the contents or the publication of extracts of this document are prohibited.

Phoenix Contact reserves the right to register its own intellectual property rights for the product identifications of Phoenix Contact products that are used here. Registration of such intellectual property rights by third parties is prohibited.

Other product identifications may be afforded legal protection, even where they may not be indicated as such.

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:
phoenixcontact.com

Make sure you always use the latest documentation.
It can be downloaded at:
phoenixcontact.net/products

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary.
Subsidiary contact information is available at phoenixcontact.com.

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
GERMANY

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to:
tecdoc@phoenixcontact.com

© PHOENIX CONTACT 2023-02-09

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Fax: +49 5235 3-41200
E-mail: info@phoenixcontact.com
phoenixcontact.com

108998_en_06
Order No. —06

PHOENIX CONTACT
INSPIRING INNOVATIONS