

MACMON NAC WHITE PAPER
FL SWITCH Series
Phoenix Contact GmbH & Co. KG

Table of Contents

1.	Motivation	3
1.1.	Devices That Can Be Managed in macmon with a Similar Scope of Functions	3
1.2.	Overview of Functions	3
2.	Switch Configurations.....	4
2.1.	Configuring the Password and User Name of the Switch Administrator	4
2.2.	Network Configuration.....	5
3.	SNMP Configuration	5
3.1.	SNMPv2c	5
3.2.	SNMPv3	5
3.3.	Trap Transmission.....	6
4.	VLAN Configuration.....	6
4.1.	VLAN Mode.....	6
4.2.	Static VLAN Configuration	7
4.3.	VLAN Port Configuration Table.....	7
4.4.	Current VLAN Configuration	7
5.	802.1X/RADIUS	8
5.1.	Configuration of the RADIUS Server	8
5.2.	802.1X Port Configuration Table	8
5.3.	802.1X Port Configuration.....	9
6.	Settings in macmon.....	10
6.1.	SNMP Settings	10
6.2.	Class Configuration.....	10

1. Motivation

The following white paper deals with the scope of features and configuration of the FL series from the manufacturer Phoenix Contact GmbH & Co. KG in combination with the NAC solution macmon. It lists the steps required to implement the respective sub-features (monitoring, SNMP-NAC, RADIUS-NAC via 802.1x). The configuration is depicted in this documentation using the switch model FL SWITCH 2208 as an example.

1.1. Devices That Can Be Managed in macmon with a Similar Scope of Features

Intelligent switches for mechanical engineering, 100 Mbit

FL SWITCH 2005, FL SWITCH 2008, FL SWITCH 2016

Intelligent switches for mechanical engineering, 1000 Mbit

FL SWITCH 2105, FL SWITCH 2108, FL SWITCH 2116

Managed switches for automation applications, 100 Mbit

FL SWITCH 2205, FL SWITCH 2208, FL SWITCH 2207-FX, FL SWITCH 2207-FX SM, FL SWITCH 2206-2FX, FL SWITCH 2206-2FX SM, FL SWITCH 2206-2FX ST, FL SWITCH 2206-2FX SM ST, FL SWITCH 2206-2SFX, FL SWITCH 2204-2TC-2SFX, FL SWITCH 2208 PN, FL SWITCH 2206-2SFX PN, FL SWITCH 2216, FL SWITCH 2214-2FX, FL SWITCH 2214-2FX SM, FL SWITCH 2214-2SFX, FL SWITCH 2212-2TC-2SFX, FL SWITCH 2216 PN, FL SWITCH 2214-2SFX PN,

Managed switches for automation applications, 1000 Mbit

FL SWITCH 2308, FL SWITCH 2306-2SFP, FL SWITCH 2304-2GC-2SFP, FL SWITCH 2308 PN, FL SWITCH 2306-2SFP PN, FL SWITCH 2316, FL SWITCH 2314-2SFP, FL SWITCH 2312-2TC-2SFP, FL SWITCH 2316 PN, FL SWITCH 2314-2SFP PN

Managed switches for automation applications, 100 Mbit (metal housing)

FL SWITCH 2406-2SFX, FL SWITCH 2404-2TC-2SFX, FL SWITCH 2408 PN, FL SWITCH 2406-2SFX PN, FL SWITCH 2416, FL SWITCH 2414-2SFX, FL SWITCH 2412-2TC-2SFX, FL SWITCH 2416 PN, FL SWITCH 2414-2SFX PN

Managed switches for automation applications, 1000 Mbit (metal housing)

FL SWITCH 2508, FL SWITCH 2506-2SFP, FL SWITCH 2504-2GC-2SFP, FL SWITCH 2508 PN, FL SWITCH 2506-2SFP PN, FL SWITCH 2516, FL SWITCH 2514-2SFP, FL SWITCH 2512-2GC-2SFP, FL SWITCH 2516 PN, FL SWITCH 2514-2SFP PN

1.2. Feature overview

The following table contains an overview of the general macmon feature options with the switches specified above. The features with a check mark have been verified in our laboratory.

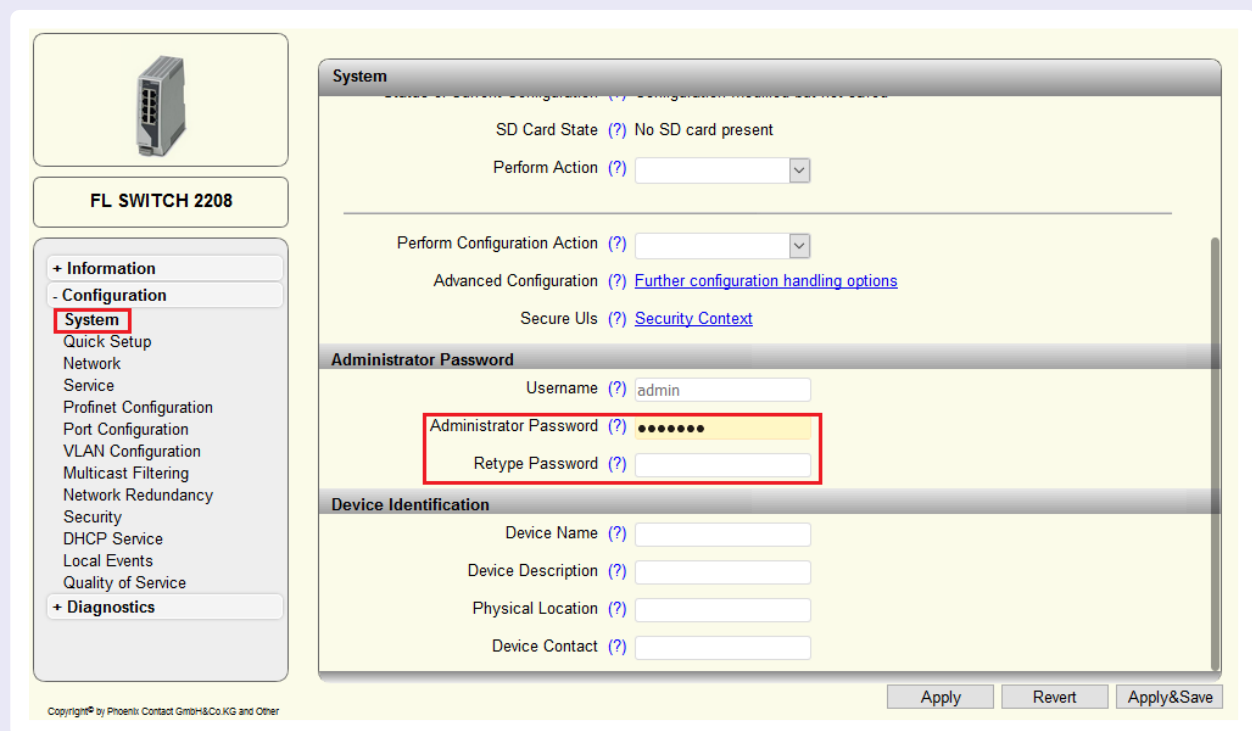
Reading the MAC addresses	✓
Reading the MAC addresses including MAC VLANs	
Reading the VLANs on the interfaces	✓
Configuring the VLANs on the interfaces	✓
Reading interfaces	✓
Reading interface statuses	✓
Disabling/enabling interfaces	✓
Reading 802.1X statuses	✓
Configuring 802.1X statuses	
Reading LLDP information	✓

Reading CDP information	
Bypassing MAC addresses with RADIUS VLAN	
Bypassing MAC addresses without RADIUS VLAN	
802.1X with RADIUS VLAN for one device on one port	
802.1X with RADIUS VLAN for multiple devices on one port	
802.1X without RADIUS VLAN for one device on one port	✓
802.1X without RADIUS VLAN for multiple devices on one port	
Change of authorization	

2. Switch Configurations

2.1. Configuring the Password and User Name of the Switch Administrator

Configuration → System → Administrator → Password



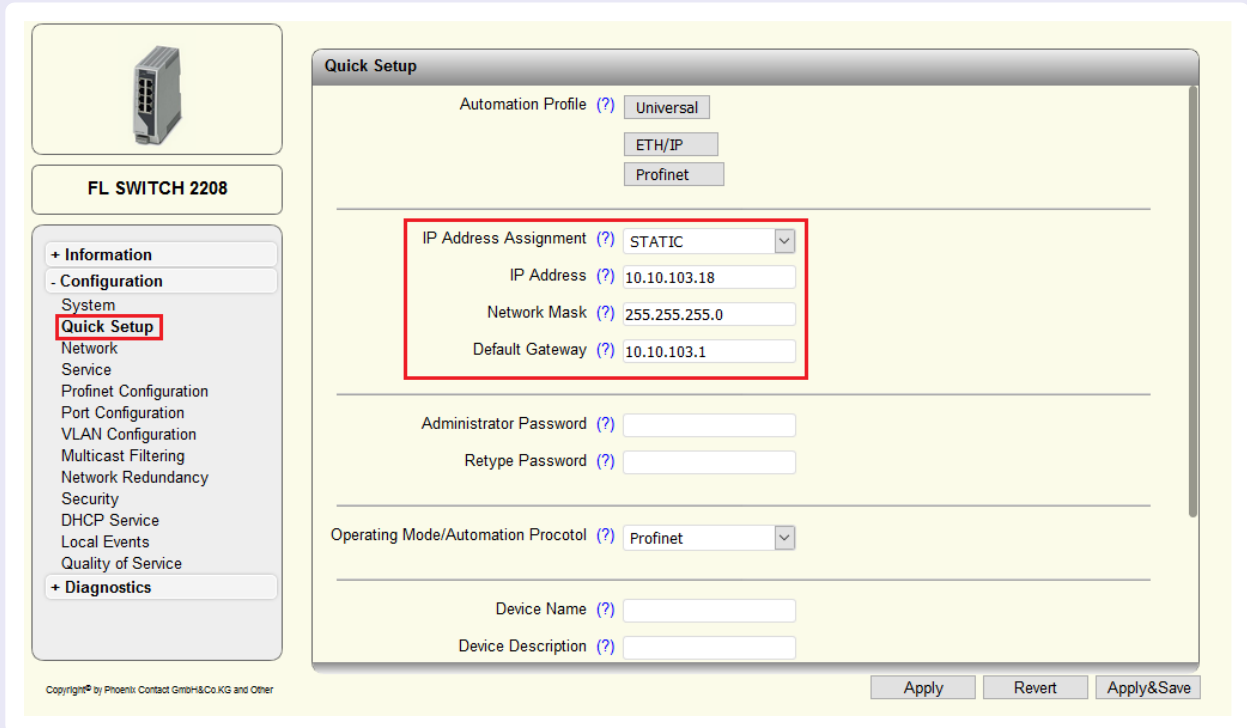
The screenshot shows the macmon web interface for configuring a switch. On the left, a sidebar menu lists various configuration options, with 'System' highlighted. The main content area is titled 'System' and contains several sections:

- SD Card State:** A dropdown menu showing 'No SD card present'.
- Perform Action:** A dropdown menu.
- Perform Configuration Action:** A dropdown menu.
- Advanced Configuration:** A link to 'Further configuration handling options'.
- Secure UIs:** A link to 'Security Context'.
- Administrator Password:** A section with three input fields: 'Username' (containing 'admin'), 'Administrator Password' (masked with dots), and 'Retype Password'.
- Device Identification:** A section with four input fields: 'Device Name', 'Device Description', 'Physical Location', and 'Device Contact'.

At the bottom of the interface, there are three buttons: 'Apply', 'Revert', and 'Apply&Save'.

2.2. Network Configuration

Configuration → Quick Setup



FL SWITCH 2208

- + Information
- Configuration
 - System
 - Quick Setup**
 - Network
 - Service
 - Profinet Configuration
 - Port Configuration
 - VLAN Configuration
 - Multicast Filtering
 - Network Redundancy
 - Security
 - DHCP Service
 - Local Events
 - Quality of Service
- + Diagnostics

Quick Setup

Automation Profile (?)

IP Address Assignment (?) ▼

IP Address (?)

Network Mask (?)

Default Gateway (?)

Administrator Password (?)

Retype Password (?)

Operating Mode/Automation Protocol (?) ▼

Device Name (?)

Device Description (?)

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

3. SNMP Configuration

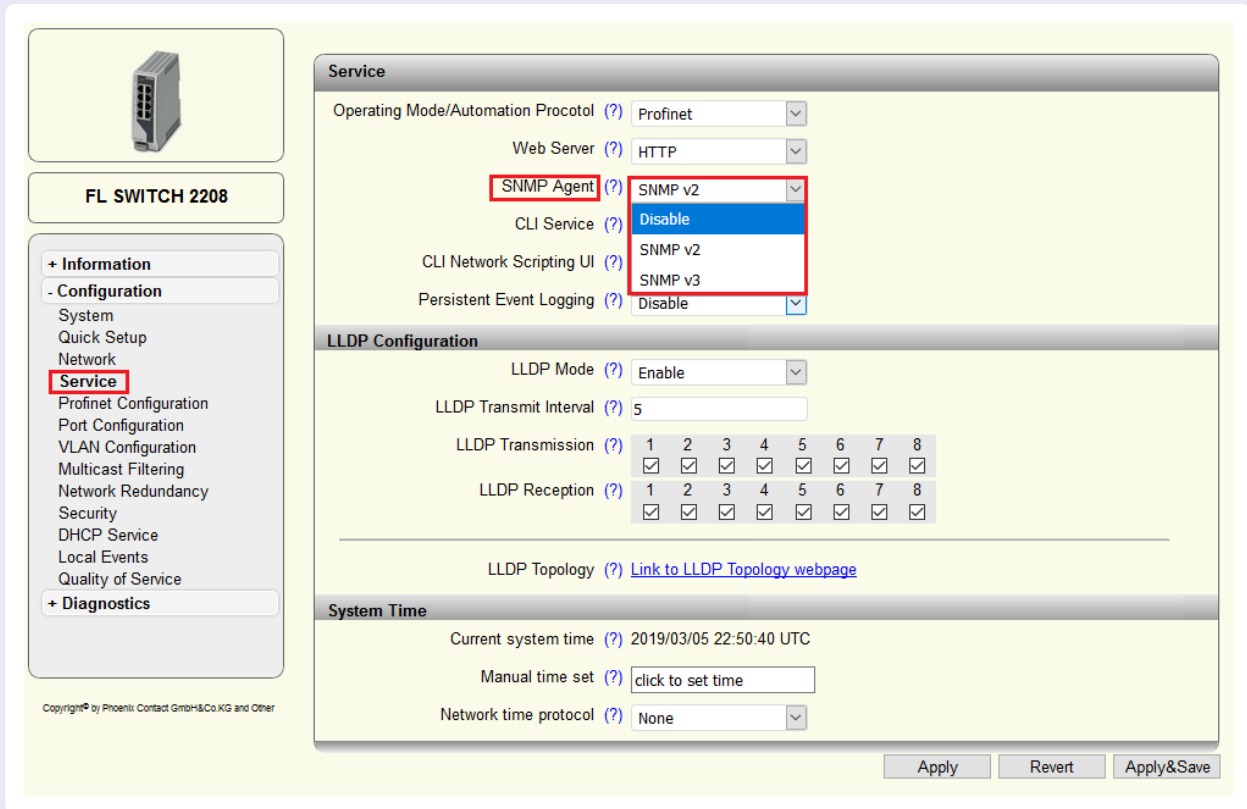
Configuration → Quick Setup → Service → SNMP Agent

3.1. SNMPv2c

- The SNMPv2c read community is always *public* and cannot be changed to a different value.
- The SNMPv2c write community automatically matches the password of the switch administrator.

3.2. SNMPv3

- By default, the user name is the same as the name of the switch administrator.
- Only the *authentication type MD5* can be used.
- **Only** the *privacy type DES* can be used.
- *Authentication passphrase* and *privacy passphrase* **automatically match the** password of the switch administrator.



FL SWITCH 2208

- + Information
- Configuration
 - System
 - Quick Setup
 - Network
 - Service**
 - Profinet Configuration
 - Port Configuration
 - VLAN Configuration
 - Multicast Filtering
 - Network Redundancy
 - Security
 - DHCP Service
 - Local Events
 - Quality of Service
- + Diagnostics

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

Service

Operating Mode/Automation Protocol (?) Profinet

Web Server (?) HTTP

SNMP Agent (?) SNMP v2

CLI Service (?) Disable

CLI Network Scripting UI (?) SNMP v2

Persistent Event Logging (?) Disable

LLDP Configuration

LLDP Mode (?) Enable

LLDP Transmit Interval (?) 5

LLDP Transmission (?)

	1	2	3	4	5	6	7	8
LLDP Transmission	☒	☒	☒	☒	☒	☒	☒	☒

LLDP Reception (?)

	1	2	3	4	5	6	7	8
LLDP Reception	☒	☒	☒	☒	☒	☒	☒	☒

LLDP Topology (?) [Link to LLDP Topology webpage](#)

System Time

Current system time (?) 2019/03/05 22:50:40 UTC

Manual time set (?) click to set time

Network time protocol (?) None

Apply Revert Apply&Save

3.3. Sending traps

Diagnostics → Trap-Manager

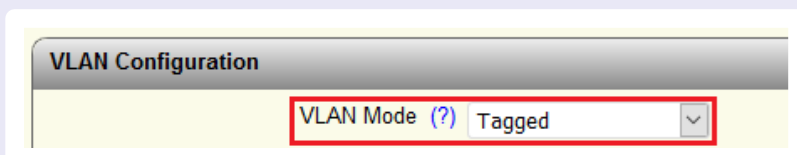
The format of the configurable linkup/linkdown traps is not currently supported by macmon.

4. VLAN Configuration

4.1. VLAN Mode

Configuration → VLAN Configuration → VLAN Mode

The *VLAN Mode* field defines whether VLAN tagging can be used in general or whether only a default untagged VLAN can be available. To enable VLAN segmentation and VLAN management with macmon, the value must be set to *tagged*.



VLAN Configuration

VLAN Mode (?) Tagged

4.2. Static VLAN Configuration

Configuration → VLAN Configuration → Static VLAN Configuration

The VLANs and their ID and name are created in this menu. It also sets the type of VLAN membership on the port (*T*=*tagged*, *U*=*untagged*). A port that has more than one untagged VLAN membership is not supported by macmon and also quite uncommon in the industry.

Static VLAN Configuration

List of Static VLANs (?) 1 - VLAN 1
 800 - LAB
 801 - Client A
 802 - Client B
 803 - Client C

VLAN ID (?)

VLAN Name (?)

VLAN Memberships (?)

1	2	3	4	5	6	7	8
U	U	U	U	U	U	U	U

(?)

4.3. VLAN Port Configuration Table

Configuration → VLAN Configuration → Static VLAN-Configuration

The PVID (port VLAN ID) is set for each port in the [Static VLAN Configuration](#) table. The PVID of a port and the untagged port membership (see [4.2. Static VLAN Configuration → VLAN Membership](#)) must be configured identically. Only this combination is a valid untagged VLAN configuration for a port!

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

4.4. Current VLAN Configuration

Configuration → VLAN Configuration → Current VLANs

The current untagged and tagged port VLAN membership can be checked in the [Current VLANs](#) table.

Current VLANs			
VLAN ID	Type	Untagged Member	Tagged Member
1	Static / Management	1, 2, 3, 4, 5, 6, 7, 8	
800	Static		2
801	Static		2
802	Static		2
803	Static		2
890	Static		2

5. 802.1X/RADIUS

On the switch model, an 802.1X authentication can be configured for each port. Since processing of sent VLAN attributes is not supported by the switch, dynamic VLAN management using 802.1X is not possible with macmon. The 802.1X session is going to use the Access VLAN configured on the port.

5.1. Configuration of the RADIUS Server

Configuration → Security → Global Radius Authentication Server Configuration

In this menu, you configure the *radius server IP address* (IP address of the macmon appliance) and the *radius shared secret*. You must also globally specify that the switch operates as the *Dotx authenticator* for the 802.1X authentication.

Port Based Configuration (?) [Configure Port Based Security](#)

Clear Illegal Counter (?) [Clear](#)

Global Radius Authentication Server Configuration

Radius Server IP Address (?) 10.10.15.37

Radius Server Port (?) 1812

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

Dot1x Authenticator (?) Enable

Port Authentication Table (?) [Dot1x Port Configuration Table](#)

Port Authentication (?) [Dot1x Port Configuration](#)

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

Apply Revert Apply&Save

5.2. 802.1X Port Configuration Table

Configuration → Security → Dot1x Port Configuration Table

In this table, the mode for 802.1X authentication is configured for each port.

- *Force Authenticate*: The supplicant (client) is always authorized.
- *Auto*: The RADIUS server specifies whether the supplicant is authorized.
- *Unauthenticated*: The supplicant is not authorized.

Dot1x Port Configuration Table		
Interface/Port	Mode	Status
1	Force Authenticate ▾	Initialize
2	Force Authenticate ▾	Force Authenticate
3	Force Authenticate ▾	Initialize
4	Auto ▾	Connecting
5	Force Authenticate ▾	Initialize
6	Force Authenticate ▾	Force Authenticate
7	Force Authenticate ▾	Initialize
8	Force Authenticate ▾	Initialize

Apply Revert Apply&Save

5.3. 802.1X Port Configuration

Configuration → Security → Dot1x Port Configuration

In this menu, you can also define whether the supplicant should be authenticated again for the table above and, if so, at which interval. In addition, authentication statistics are displayed for each port.

Dot1x Port Configuration	
Port (?)	port-1 ▾
Authentication Mode (?)	Force Authenticate ▾
Authentication Status (?)	Initialize
Re-Authentication Mode (?)	Disable ▾
Re-Authentication Period (secs) (?)	3600
EAPOL Frames Received (?)	0
Last EAPOL Frame Source (?)	00:00:00:00:00:00

6. Settings in macmon

6.1. SNMP Settings

Settings → Scan engine → SNMP

With the default SNMP settings in macmon, the switch model is unable not fully supply all the data. The values of the following settings should therefore be adapted:

snmp_max_bindings	1	Quantity
snmp_max_repetition_count	8	Quantity

These values can also be set on the network device itself or on a network device group, which slightly optimizes overall scanning performance. In the menu *Settings → User-defined properties*, the following properties must be created for this purpose:

- *engine_snmp_max_bindings*
- *engine_snmp_max_repetition_count*

The fields are then displayed on the network device or the network device group, depending on the selected object. Adding the values above to those fields will then optimize the SNMP scan.

6.2. Class Configuration

Network → Network devices → This switch model → Network device class

The following class configuration can be used to successfully read from the switch and manipulate it too.

Action	Method
ARP readout Read ARP table of a network device.	MIB-II:atEntry This method reads the atEntry table of MIB-II. Method IP-MIB:ipNetToPhysicalEntry should be used preferable.
Dot1X status readout Reads the 802.1X information of a network device.	IEEE802.1-PAE-MIB This method requests the 802.1X configuration and status of the interfaces.
Interfaces readout Reads the interfaces of a network device.	IF-MIB:ifEntry This method reads out all interfaces via SNMP MIB-II (RFC 1213), IF-MIB (RFC 2011), IF-MIB (RFC 1573), BRIDGE-MIB (RFC 4188).
Interface status readout Reads the status information of network device interfaces (up/down).	IF-MIB:ifOperStatus This method determines the operational status of interfaces via SNMP IF-MIB (RFC 1573). This data is required to generate the interface_up and interface_down events.
Inventory status readout Reads the inventory information of a network device.	ENTITY-MIB This method reads out inventory information via ENTITY-MIB (RFC 4133).
MAC address readout Reads the list of all MAC addresses known by a device.	Q-Bridge New standard method. Reads out MAC addresses and their VLAN membership (RFC 2674, 4363).
Topology readout Reads the topology information of network device.	Topology (LLDP, CDP) Standard method (IEEE Std 802.1AB-2005) and Cisco Discovery Protocol
VLANs readout Reads the VLANs of a network device and the VLAN/Port configuration.	Q-Bridge (untagged) Default method (RFC 2674, untagged)
Enable/disable interface Changes the admin status in order to enable or disable an interface.	IF-MIB:ifAdminStatus Standard method to set admin status

Contact

macmon secure GmbH
 Alte Jakobstrasse 79-80 | 10179 Berlin
 Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu