MACMON NAC WHITE PAPER

FL SWITCH Series

Phoenix Contact GmbH & Co. KG

Table of Contents

Version 1.0

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.

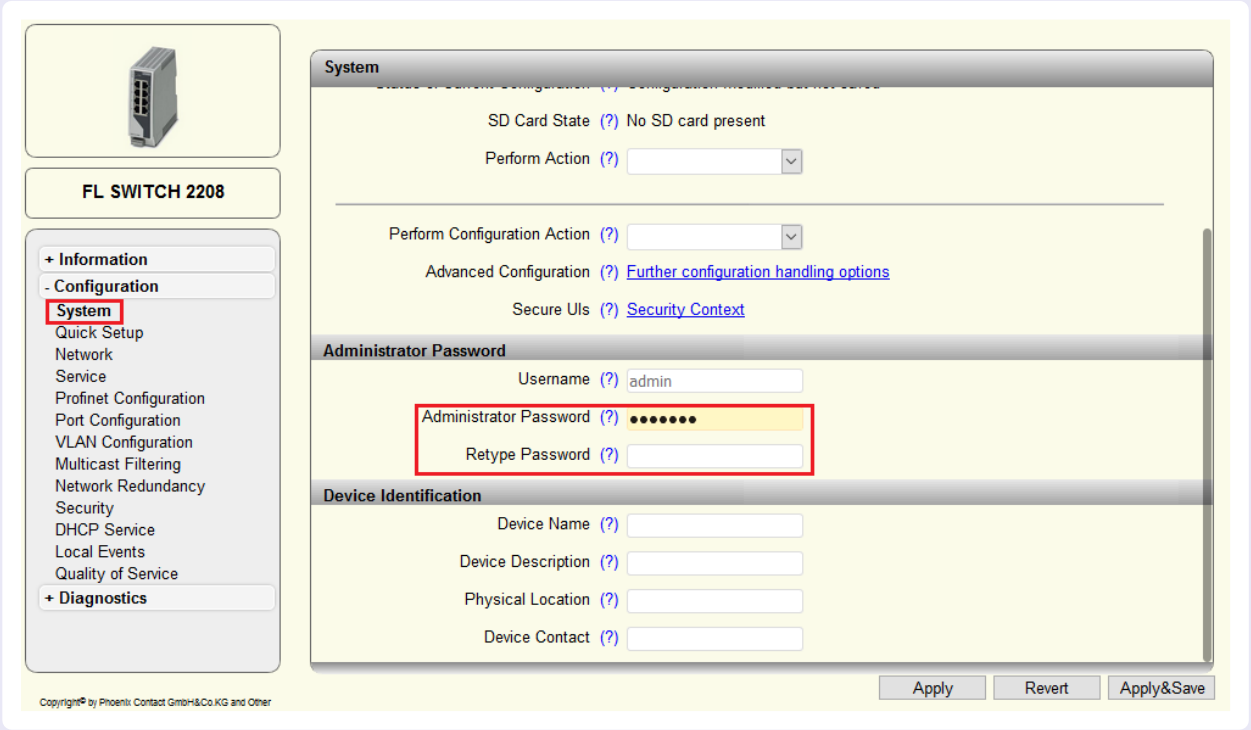
Reading the MAC addresses	✓
Reading the MAC addresses including MAC VLANs	
Reading the VLANs on the interfaces	✓
Configuring the VLANs on the interfaces	✓
Reading interfaces	✓
Reading interface statuses	✓
Disabling/enabling interfaces	✓
Reading 802.1X statuses	✓
Configuring 802.1X statuses	
Reading LLDP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

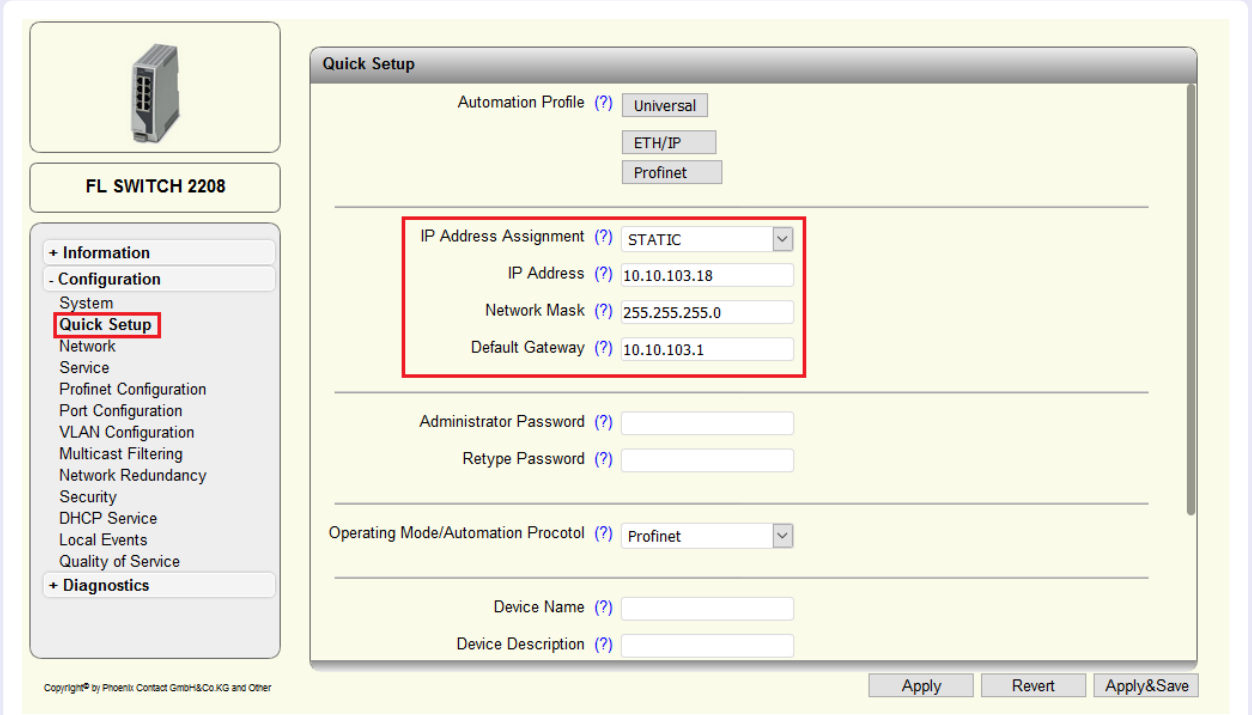
2.1. Configuring the Password and User Name of the Switch Administrator

Configuration → System → Administrator → Password



2.2. Network Configuration

Configuration → Quick Setup



3. SNMP Configuration

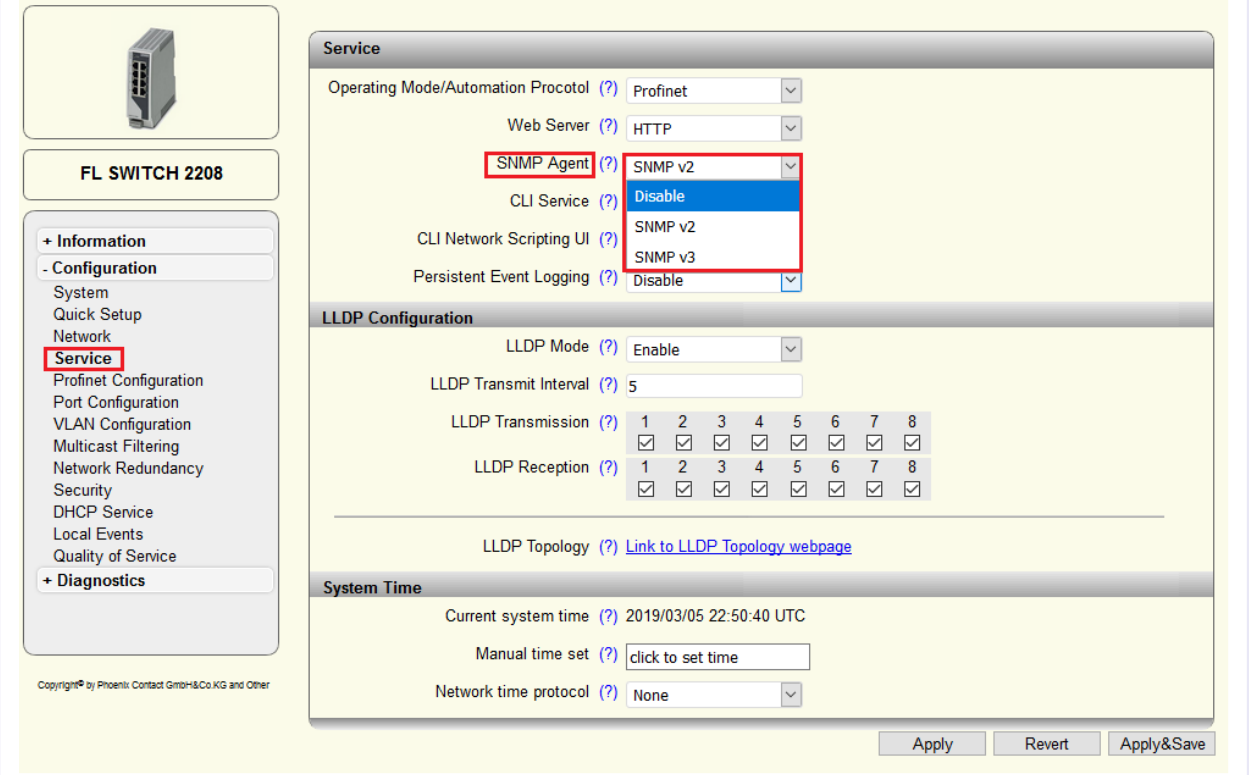
Configuration → Quick Setup → Service → SNMP Agent

3.1. SNMPv2c

- The SNMPvc2 read community is always *public* and cannot be changed to a different value.
- The SNMPvc2 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.



3.3. Sending traps

Diagnostics → Trap-Manager

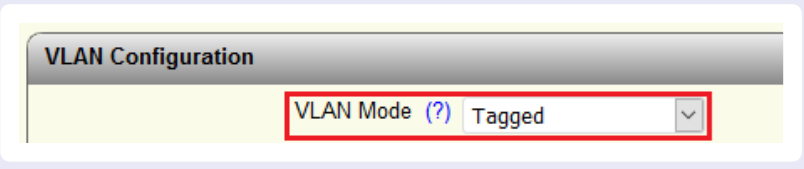
The format of the configurable linkup/linkdown traps is not currently supported by macmon.

4. VLAN Configuration

4.1. VLAN Mode

Configuration → VLAN Configuration → VLAN Mode

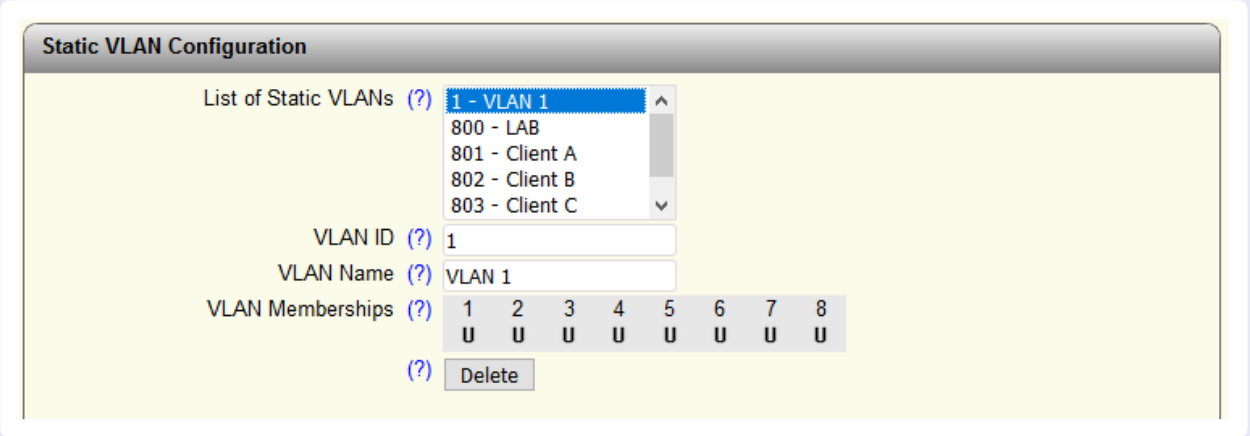
The *VLAN Mode* field defines whether VLAN tagging can be used in general or whether only a default untagged VLAN can is available. To enable VLAN segmentation and VLAN management with macmon, the value must be set to *tagged*.



4.2. Static VLAN Configuration

Configuration → VLAN Configuration → Static VLAN Configuration

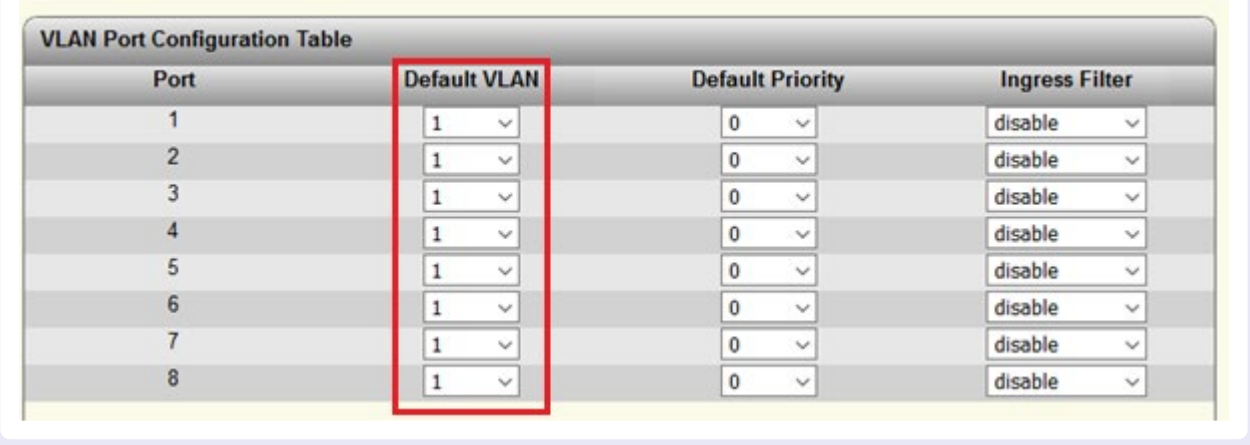
The VLANs and their ID and name are created in this menu. It also sets the type of VLAN membership on the port (*T*=*tagged*, *U*=*untagged*). A port that has more than one untagged VLAN membership is not supported by macmon and also quite uncommon in the industry.



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!



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

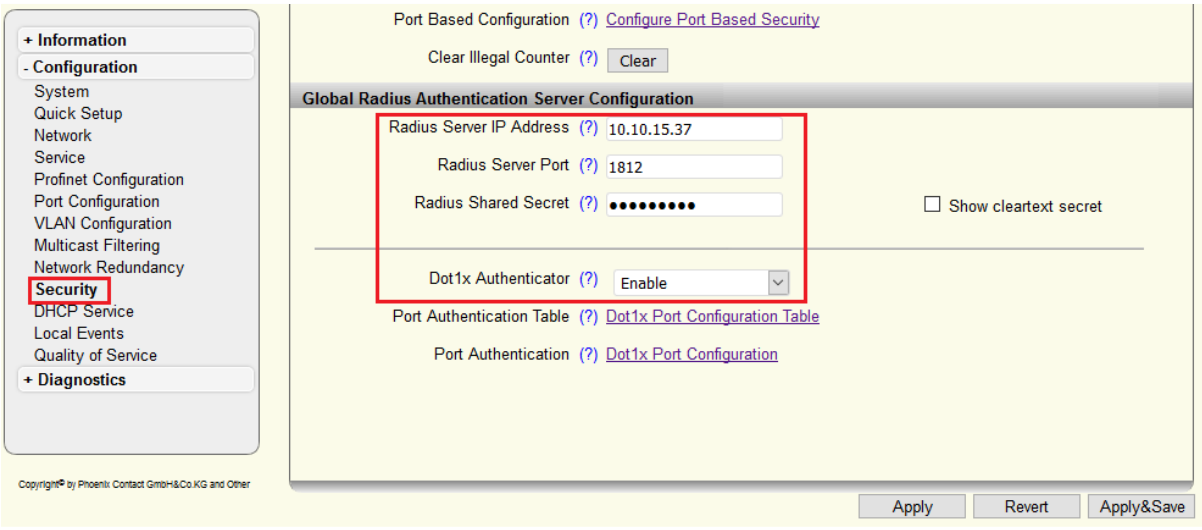
5. 802.1X/RADIUS

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.

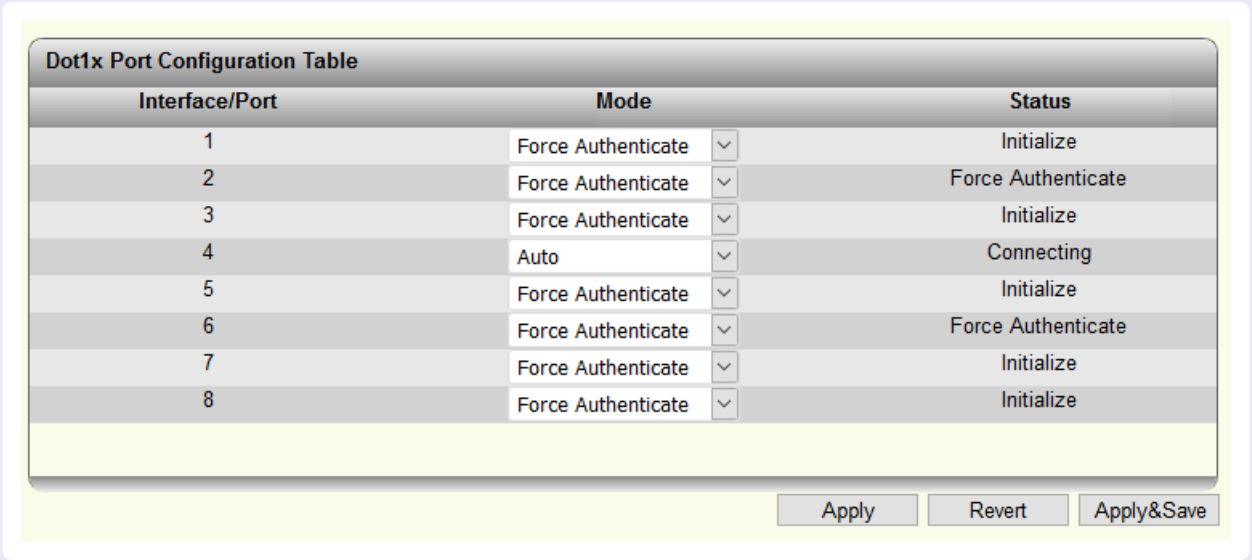


5.2. 802.1X Port Configuration Table

Configuration → Security → Dot1x Port Configuration Table

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

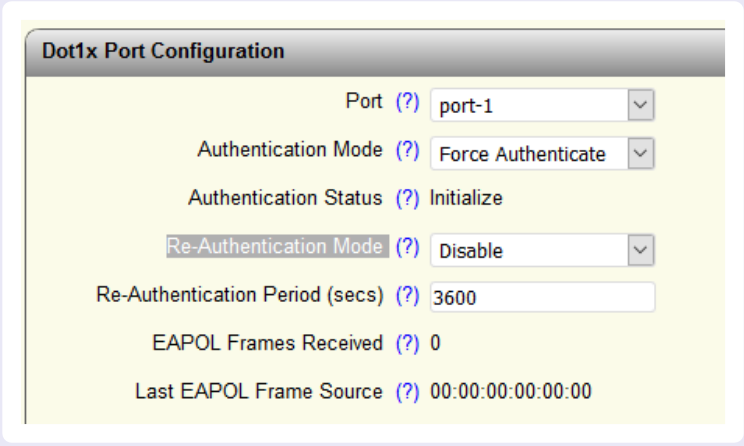
- *Force Authenticate*: The supplicant (client) is always authorized.
- *Auto*: The RADIUS server specifies whether the supplicant is authorized.
- *Unauthenticate*: The supplicant is not authorized.



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.

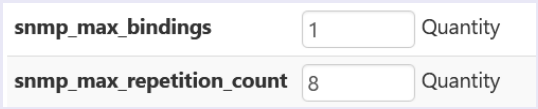


6. Settings in macmon

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:



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:

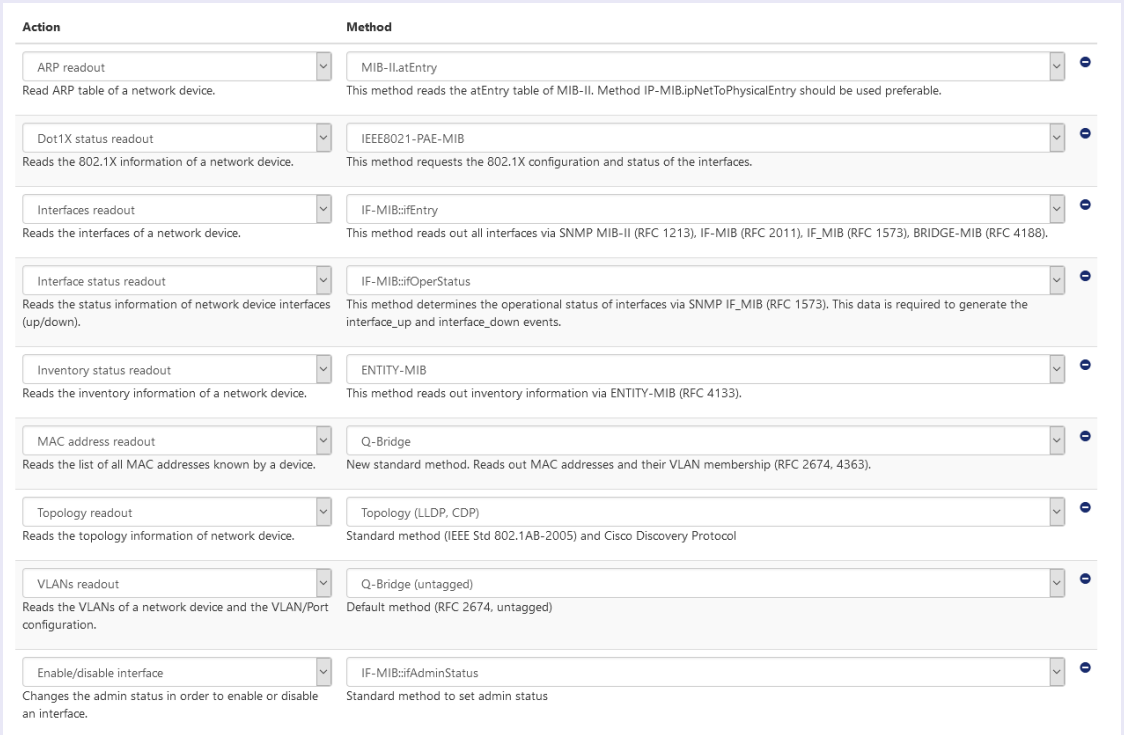
- *engine_snmp_max_bindings*
- *engine_snmp_max_repetition_count*

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.



Contact

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