

MACMON NAC WHITEPAPER
FL SWITCH Serie
Phoenix Contact GmbH & Co. KG

Inhaltverzeichnis

1.	Motivation	3
1.1.	In macmon managebare Geräte mit ähnlichem Funktionsumfang.....	3
1.2.	Funktionsübersicht.....	3
2.	Switch-Konfigurationen	4
2.1.	Passwort und Username des Switch-Administrators konfigurieren.....	4
2.2.	Netzwerkkonfiguration.....	5
3.	SNMP-Konfiguration	5
3.1.	SNMPv2c	5
3.2.	SNMPv3	5
3.3.	Trap-Versand	6
4.	VLAN-Konfiguration	6
4.1.	VLAN Mode.....	6
4.2.	Statische VLAN-Konfiguration.....	7
4.3.	VLAN-Port-Konfigurationstabelle	7
4.4.	Aktuelle VLAN-Konfiguration	7
5.	802.1X/RADIUS	8
5.1.	Konfiguration des RADIUS-Servers	8
5.2.	802.1X-Port-Konfigurationstabelle.....	8
5.3.	802.1X-Port-Konfiguration.....	9
6.	Einstellungen in macmon	10
6.1.	SNMP-Einstellungen.....	10
6.2.	Die Klassenkonfiguration.....	10

1. Motivation

Das folgende Whitepaper behandelt den Funktionsumfang und die Konfiguration der FL-Serie des Herstellers Phoenix Contact GmbH & Co. KG in Verbindung mit der NAC-Lösung macmon. Es werden nötige Schritte für die Umsetzung der jeweiligen Teilfunktionen (Monitoring, SNMP-NAC, RADIUS-NAC via 802.1x) aufgeführt. Die Darstellung der Konfiguration erfolgt in dieser Dokumentation am Beispiel des Switch-Modells FL SWITCH 2208.

1.1. In macmon managebare Geräte mit ähnlichem Funktionsumfang

Intelligente Switches für Maschinenbau 100MBit

FL SWITCH 2005, FL SWITCH 2008, FL SWITCH 2016

Intelligente Switches für Maschinenbau 1000Mbit

FL SWITCH 2105, FL SWITCH 2108, FL SWITCH 2116

Managed Switches für Automationsapplikationen 100Mbit

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 für Automationsapplikationen 1000Mbit

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 für Automationsapplikationen 100Mbit (Metallgehäuse)

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 für Automationsapplikationen 1000Mbit (Metallgehäuse)

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. Funktionsübersicht

Die folgende Tabelle enthält eine Übersicht der generellen macmon-Funktionsmöglichkeiten mit den o. g. Switches. Die gekennzeichneten Funktionen konnten wir in unserem Labor bestätigen.

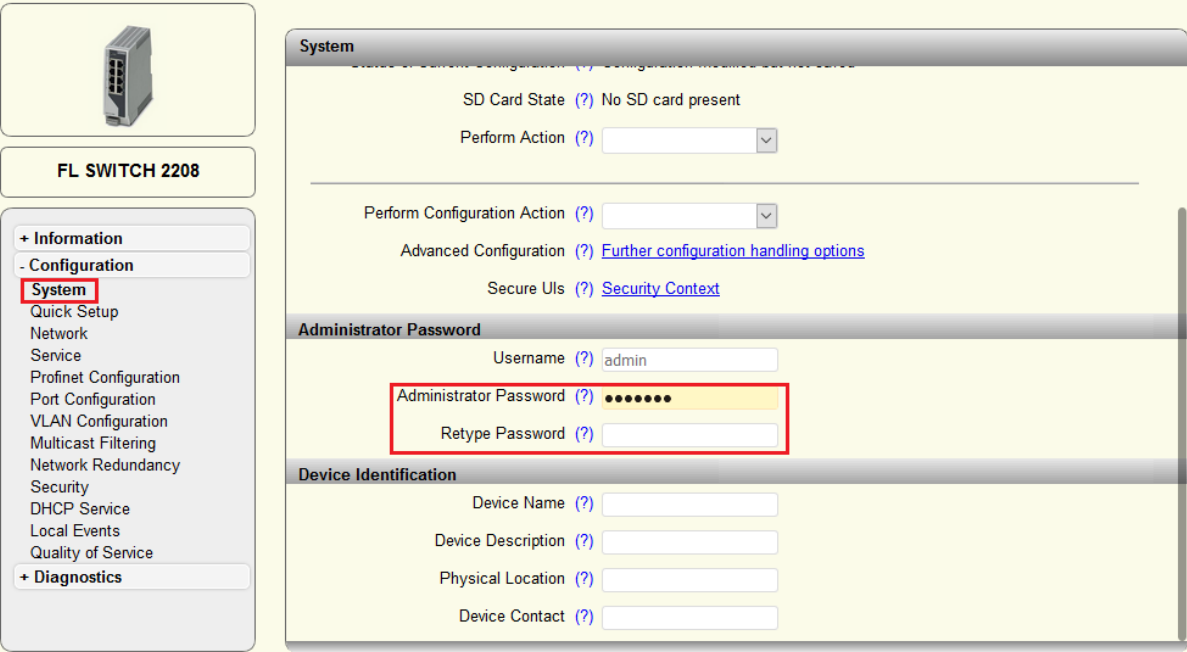
Auslesen der MAC-Adressen	✓
Auslesen der MAC-Adressen inklusive MAC-VLANs	
Auslesen der VLANs an den Interfaces	✓
Setzen der VLANs an den Interfaces	✓
Interfaces auslesen	✓
Interface Status auslesen	✓
Interface (ent)sperren	✓
802.1X-Status auslesen	✓
802.1X-Status setzen	

LLDP auslesen	✓
CDP auslesen	
MAC-Adress-Bypass mit RADIUS-VLAN	
MAC-Adress-Bypass ohne RADIUS-VLAN	
802.1X mit RADIUS-VLAN für ein Gerät an einem Port	
802.1X mit RADIUS-VLAN für mehrere Geräte an einem Port	
802.1X ohne RADIUS-VLAN für ein Gerät an einem Port	✓
802.1X ohne RADIUS-VLAN für mehrere Geräte an einem Port	
Change of Autorisation	

2. Switch-Konfigurationen

2.1. Passwort und Username des Switch-Administrators konfigurieren

Configuration → System → Administrator → Password



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

System

SD Card State (?) No SD card present

Perform Action (?)

Perform Configuration Action (?)

Advanced Configuration (?) [Further configuration handling options](#)

Secure UIs (?) [Security Context](#)

Administrator Password

Username (?)

Administrator Password (?)

Retype Password (?)

Device Identification

Device Name (?)

Device Description (?)

Physical Location (?)

Device Contact (?)

Apply Revert Apply&Save

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

2.2. Netzwerkkonfiguration

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-Konfiguration

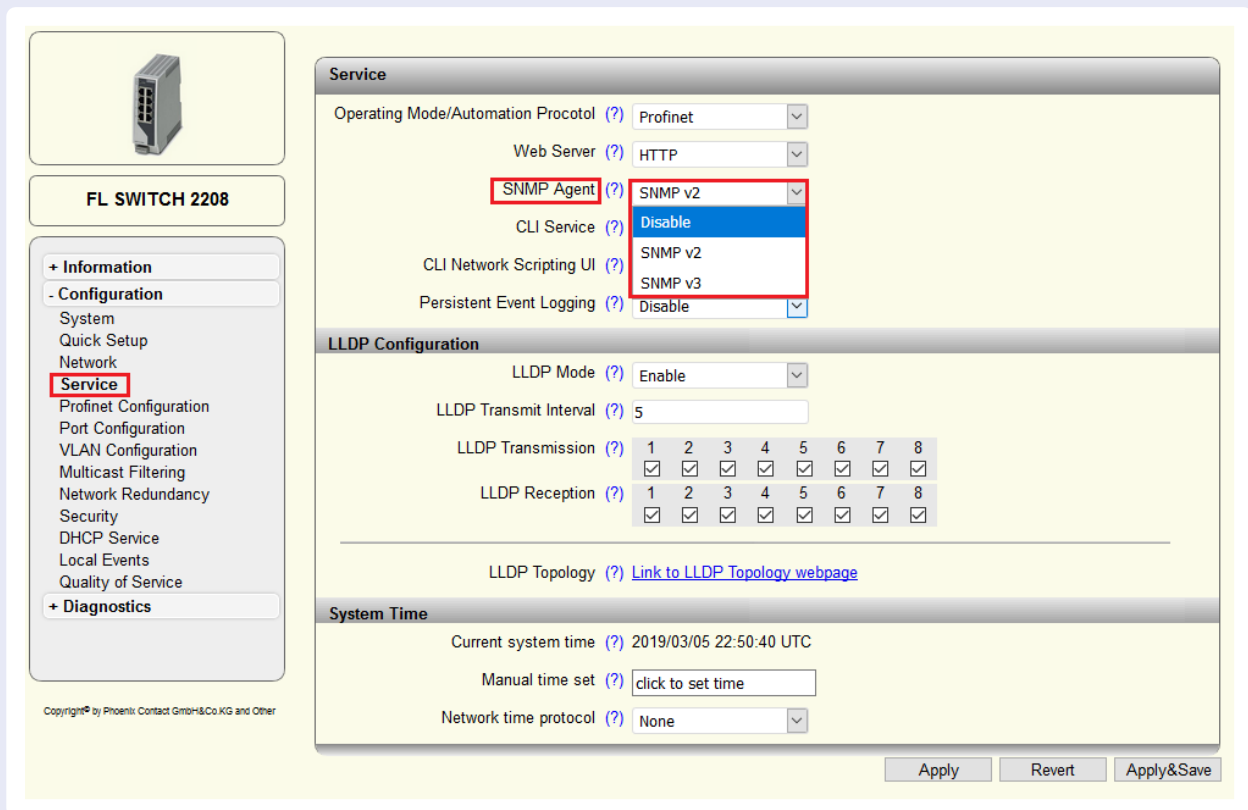
Configuration → Quick Setup → Service → SNMP Agent

3.1. SNMPv2c

- Die SNMPv2c-Read-Community ist immer *public* und kann nicht auf einen anderen Wert geändert werden.
- Die SNMPv2c-Write-Community entspricht automatisch dem Passwort des Switch-Administrators.

3.2. SNMPv3

- Per Voreinstellung ist der Benutzername gleich dem Namen des Switch-Administrators.
- Es wird ausschließlich *authentication type MD5* verwendet.
- Es wird ausschließlich *privacy type DES* verwendet.
- *authentication passphrase* und *privacy passphrase* entsprechen automatisch dem Passwort des Switch-Administrators.



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 Reception (?)

1	2	3	4	5	6	7	8
☒	☒	☒	☒	☒	☒	☒	☒

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. Trap-Versand

Diagnostics → Trap-Manager

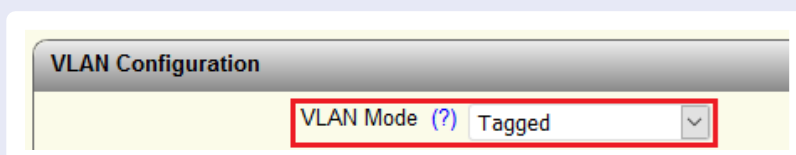
Das Format der konfigurierbaren Linkup-/Linkdown-Traps wird derzeit von macmon nicht unterstützt.

4. VLAN-Konfiguration

4.1. VLAN Mode

Configuration → VLAN Configuration → VLAN Mode

Im Feld *VLAN Mode* wird definiert, ob VLAN-Tagging generell genutzt werden soll oder ob nur mit einem default untagged VLAN gearbeitet wird. Um eine VLAN-Segmentierung sowie das VLAN-Management durch macmon zu ermöglichen, muss der Wert auf *tagged* gesetzt werden.



VLAN Configuration

VLAN Mode (?) Tagged

4.2. Statische VLAN-Konfiguration

Configuration → VLAN Configuration → Static VLAN Configuration

In diesem Menü werden die VLANs mit ID und Namen angelegt. Ebenfalls wird bestimmt, wie die Port-VLAN-Zugehörigkeit jeweils definiert ist (*T=tagged*, *U=untagged*). Die eher weniger gebräuchliche untagged-Mitgliedschaft eines Ports in mehreren VLANs wird von macmon nicht unterstützt.

Static VLAN Configuration

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

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

(?) Delete

4.3. VLAN-Port-Konfigurationstabelle

Configuration → VLAN Configuration → Static VLAN-Configuration

In der Tabelle *Static VLAN Configuration* wird die PVID (Port-VLAN-ID) pro Port gesetzt. Die PVID eines Ports und die untagged-Portzugehörigkeit (siehe 4.2. *Static VLAN Configuration* → *VLAN Membership*) müssen identisch konfiguriert sein. Nur diese Kombination ist eine gültige untagged VLAN-Konfiguration für einen 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. Aktuelle VLAN-Konfiguration

Configuration → VLAN Configuration → Current VLANs

Die aktuelle untagged und tagged Port-VLAN-Zugehörigkeit kann in der Tabelle *Current VLANs* überprüft werden.

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

Auf dem Switch-Modell kann pro Port eine 802.1X-Authentifizierung konfiguriert werden. Da das Verarbeiten von gesendeten VLAN-Attributen nicht vom Switch unterstützt wird, ist ein dynamisches VLAN-Management per 802.1X mit macmon nicht möglich. Die 802.1X-Session wird mit dem am Port konfigurierten Access-VLAN durchgeführt.

5.1. Konfiguration des RADIUS-Servers

Configuration → Security → Global Radius Authentication Server Configuration

In diesem Menü wird die *Radius Server IP Address* (IP-Adresse der macmon-Appliance) sowie das *Radius Shared Secret* konfiguriert. Des Weiteren muss global definiert werden, dass der Switch als *Dotx Authenticator* für die 802.1X-Authentifizierung arbeitet.

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

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

Global Radius Authentication Server Configuration

Radius Server IP Address (?)

Radius Server Port (?)

Radius Shared Secret (?)

☐ Show cleartext secret

Dot1x Authenticator (?)

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-Konfigurationstabelle

Configuration → Security → Dot1x Port Configuration Table

In diese Tabelle wird pro Port der Modus der 802.1X-Authentifizierung konfiguriert.

- *Force Authenticate*: Der Supplikant (Client) wird immer autorisiert.
- *Auto*: Der RADIUS-Server gibt vor, ob der Supplikant autorisiert wird.

- *Unauthenticate*: Der Supplikant wird nicht autorisiert.

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-Konfiguration

Configuration → Security → Dot1x Port Configuration

In diesem Menü kann zusätzlich zur o. g. Tabelle noch definiert werden, ob der Supplikant sich erneut authentifizieren soll und wenn ja, in welchem Intervall. Des Weiteren werden Statistiken der Authentifizierung pro Port angezeigt.

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. Einstellungen in macmon

6.1. SNMP-Einstellungen

Einstellungen → Scan-Engine → SNMP

Das Switch-Modell liefert mit den in macmon voreingestellten SNMP-Einstellungen nicht alle Daten vollständig. Es sollten daher die Werte der folgenden Einstellungen angepasst werden:

snmp_max_bindings	1	Anzahl
snmp_max_repetition_count	8	Anzahl

Diese Werte können auch an das Netzwerkgerät selbst oder an eine Netzwerkgerätegruppe gebunden werden, was die Scan-Performance insgesamt etwas optimiert. Im Menüpunkt [Einstellungen](#) → [benutzerdefinierte Eigenschaften](#) müssen hierzu die folgenden Eigenschaften erstellt werden:

- [engine_snmp_max_bindings](#)
- [engine_snmp_max_repetition_count](#)

Im Anschluss werden die Felder, je nach Konfiguration, am Netzwerkgerät oder an der Netzwerkgerätegruppe angezeigt. Das Eintragen der o. g. Werte optimiert dann den SNMP-Scan.

6.2. Die Klassenkonfiguration

Netzwerk → Netzwerkgeräte → [dieses Switch-Modell](#) → Netzwerkgeräteklasse

Mit der folgenden Klassenkonfiguration kann der Switch erfolgreich ausgelesen und geschaltet werden.

Aktion	Methode
Interfaces auslesen Liest die Interfaces eines Netzwerkgerätes.	IF-MIB::ifEntry Diese Methode liest alle Interfaces via SNMP aus unter Nutzung von MIB-II (RFC 1213), IF-MIB (RFC 2011), IF_MIB (RFC 1573), BRIDGE-MIB (RFC 4188).
Dot1X-Status auslesen Liest die 802.1X-Informationen eines Netzwerkgerätes.	IEEE8021-PAE-MIB Diese Methode fragt die 802.1X-Konfiguration und -Status der Interfaces ab.
MAC-Adressen auslesen Liest die Liste aller bekannter MAC-Adressen eines Netzwerkgerätes aus.	BridgeMIB Veraltete Standardmethode (RFC 1493). Die Standardmethode QBridge liefert umfangreichere Daten und soll bevorzugt werden.
VLANs auslesen Liest die VLANs und die VLAN/Port-Konfiguration eines Netzwerkgerätes.	Q-Bridge (pvid) Standardmethode (RFC 2674, pvid)
Interface-Status auslesen Liest die Status-Informationen der Interfaces (up/down) eines Netzwerkgerätes.	IF-MIB::ifOperStatus Diese Methode ermittelt den betriebsbereiten (operational) Status der Interfaces via SNMP unter Nutzung von IF_MIB (RFC 1573). Die Daten sind eine Voraussetzung für die Generierung des Ereignisses interface_up bzw. interface_down.
ARP auslesen Liest die ARP-Tabelle eines Netzwerkgerätes.	IP-MIB::ipNetToPhysicalEntry Diese Methode liest die ipNetToPhysicalEntry-Tabelle der MIB-II aus (RFC 4293).
VLAN setzen Setzt ein VLAN an einem bestimmten Interface eines Switches.	Q-Bridge Standardmethode
Interface (ent)sperren Setzt den AdminStatus eines Interfaces, um dieses zu (ent)sperren.	IF-MIB::ifAdminStatus Standardmethode zum Setzen des Adminstatus.
Topologie auslesen Liest die Topologie-Informationen eines Netzwerkgerätes aus.	Topologie (LLDP) Standardmethode (IEEE Std 802.1AB-2005)

Kontakt

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