Increased network security thanks to series 2000 switches

Guidelines for network security

PHOENIX CONTACT
INSPIRING INNOVATIONS

Guidelines for network security
Increased network security thanks to series 2000 switches

UM EN QS FL SWITCH 2000 SECURITY, Revision 01 2020-07-30

This user manual is valid for:

Designation	Order No.	Designation	Order No.
FL NAT 2208	2702882	FL SWITCH 2312-2GC-2SFP	2702910
FL NAT 2304-2GC-2SFP	2702981	FL SWITCH 2314-2SFP	1006191
FL SWITCH 2204-2TC-2SFX	2702334	FL SWITCH 2314-2SFP PN	1031683
FL SWITCH 2206-2FX	2702330	FL SWITCH 2316	2702909
FL SWITCH 2206-2FX SM	2702331	FL SWITCH 2316 PN	1031673
FL SWITCH 2206-2FX SM ST	2702333	FL SWITCH 2404-2TC-2SFX	1088853
FL SWITCH 2206-2FX ST	2702332	FL SWITCH 2406-2SFX	1043414
FL SWITCH 2206-2SFX	2702969	FL SWITCH 2406-2SFX PN	1089126
FL SWITCH 2206-2SFX PN	1044028	FL SWITCH 2408	1043412
FL SWITCH 2206C-2FX	1095628	FL SWITCH 2408 PN	1089133
FL SWITCH 2207-FX	2702328	FL SWITCH 2412-2TC-2SFX	1088875
FL SWITCH 2207-FX SM	2702329	FL SWITCH 2414-2SFX	1043423
FL SWITCH 2208 PN	1044024	FL SWITCH 2414-2SFX PN	1089139
FL SWITCH 2208C	1095627	FL SWITCH 2416	1043416
FL SWITCH 2212-2TC-2SFX	2702907	FL SWITCH 2416 PN	1089150
FL SWITCH 2214-2FX	2702905	FL SWITCH 2504-2GC-2SFP	1088872
FL SWITCH 2214-2FX SM	2702906	FL SWITCH 2506-2SFP	1043491
FL SWITCH 2214-2SFX	1006188	FL SWITCH 2506-2SFP PN	1089135
FL SWITCH 2214-2SFX PN	1044030	FL SWITCH 2508	1043484
FL SWITCH 2216	2702904	FL SWITCH 2508 PN	1089134
FL SWITCH 2216 PN	1044029	FL SWITCH 2512-2GC-2SFP	1088856
FL SWITCH 2304-2GC-2SFP	2702653	FL SWITCH 2514-2SFP	1043499
FL SWITCH 2306-2SFP	2702970	FL SWITCH 2514-2SFP PN	1089154
FL SWITCH 2306-2SFP PN	1009222	FL SWITCH 2516	1043496
FL SWITCH 2308	2702652	FL SWITCH 2516 PN	1089205
FL SWITCH 2308 PN	1009220		

109652_en_01

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

Table of contents

1 Increased network security thanks to series 2000 switches

This quick start guide describes the options for increasing the security of your network using the series 2000 switches (FL SWITCH 2.../FL NAT2...) from Phoenix Contact. In the following, the individual functions and the configuration are explained step by step.

1.1 Overview of measures

Ethernet networks allow for seamless communication from the sensor to the office network and are therefore suitable for the networking of all areas. However, digital progress also means being more vulnerable to cyber attacks. Therefore, you have to protect components, networks, and systems against unauthorized access and ensure the integrity of data. As a part of this, you have to take organizational and technical measures to protect network-capable devices.

We recommend that the following measures should be considered at the very least.

Options for increasing network security

- Changing the default password
- Using the current firmware version
- Using safe transmission protocols for device management
- Disabling unused services
- Disabling unused automation protocols
- Disabling unused routers or switch ports
- Disabling the SD card
- Disabling smart mode buttons
- Using the RADIUS protocol and MAC-based port security

1.2 Changing the default password

The passwords for login are a major obstacle for an attacker, and they are easy to configure. In delivery state, the password is “private”. The default password is given in the user manuals and therefore accessible for everybody. Attackers try to access systems via known default passwords or weak passwords (e.g., PW01, PW02, test1234, etc.)

Change the password directly during startup. The password must have a certain complexity and minimum length of eight characters.

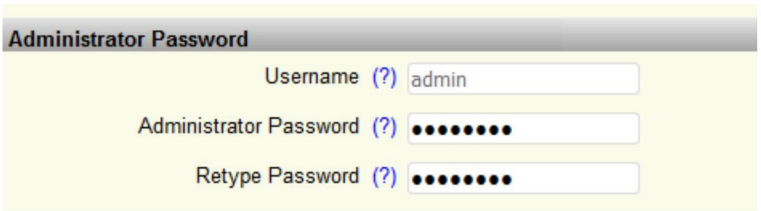
Facts

– In delivery state, the password is “private”.
– The default password is given in the user manual and therefore accessible for everybody.
– Attackers try to access the system via default passwords.
⇒ **Immediately change the default password during startup. The minimum password length is eight characters.**

Configuration via web interface

- Log in to the web-based management of the switch. Log in using the corresponding password.
- Switch to the “Quick Setup” tab.
- Enter the new password.
- Repeat the password in the field below.

Figure 1-1 Changing the password



1.3 Using the current firmware version

Phoenix Contact regularly releases firmware updates for network components. The firmware updates fix bugs and security gaps and may contain new firmware functions. To make best use of the switch, always use the latest firmware version.

Facts

– Outdated firmware may be an open door to attackers. Regularly check the firmware version.

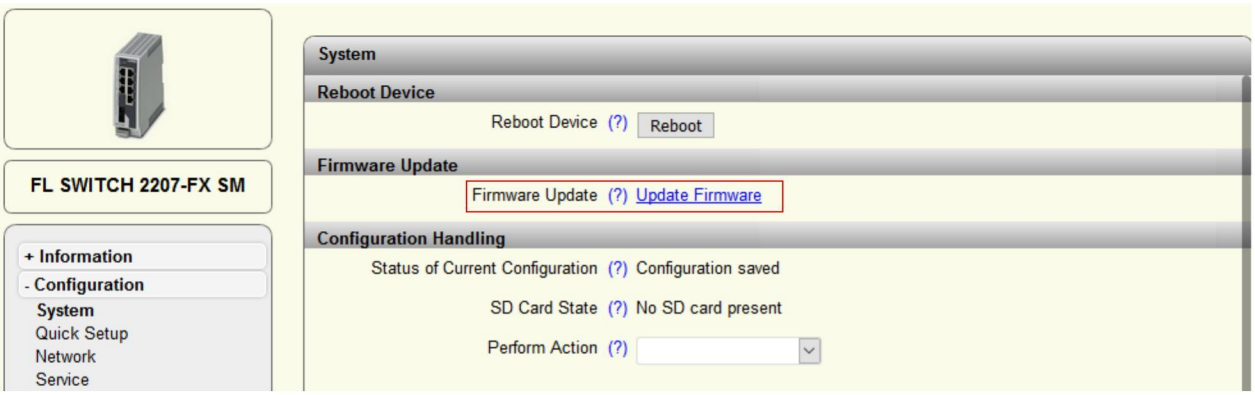
⇒ **Install new firmware promptly. Download the latest firmware from the product page of the corresponding switch at phoenixcontact.net/products.**

Configuration via web interface

- Log in to the web-based management of the switch. Log in using the corresponding password.
- You can read the current firmware status in the web-based management of the switch under “Device Status”.

Figure 1-2 Displaying the firmware version

Figure 1-3 Firmware update



- To update the firmware, use the “System” menu item, and there the “Update Firmware” link.
- You can implement the firmware update via HTTP or TFTP.

For detailed instruction please refer to the user manual UM EN SW FL SWITCH 2000 configuration “Configuration of the FL SWITCH 2000 and FL NAT 2000 product family” at **phoenixcontact.net/qr/2702323**.

1.4 Using safe transmission protocols for device management

In delivery state, communication with the Phoenix Contact switches can be started via the unsafe protocols Telnet, HTTP and SNMP. This enables easy initial startup.

Initial startup is possible via the web interface. The FL NETWORK MANAGER software from Phoenix Contact is available for starting up entire network structures.

During operation, you should disable the unsafe access points or switch to a safe transmission mode.

Facts

Telnet

- Telnet is activated in delivery state.
- No security features
- Passwords are transmitted in plain text.

⇒ **Use SSH instead of Telnet or disable the function.**

HTTP (Hyper Text Transfer Protocol)

- HTTP is activated in delivery state.
- HTTP is uncoded with few security features.
- Access point for attacks and worms

⇒ **Use HTTPS (Hypertext Transfer Protocol Secure) or disable this function.**

SNMP (Simple Network Management Protocol)

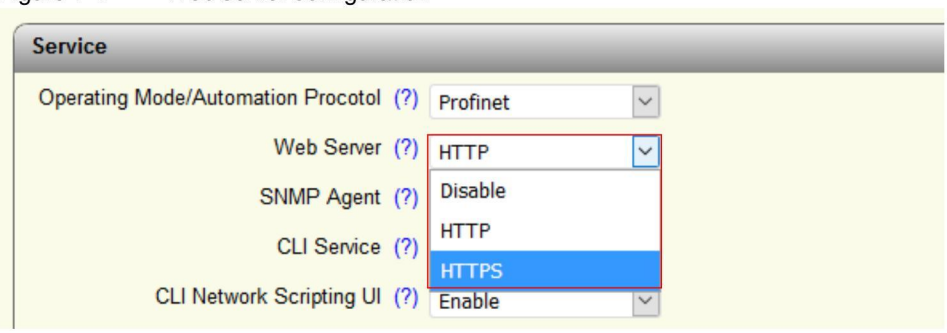
- SNMPv2 is activated in delivery state.
- SNMPv2 only uses communities (similar to a password) that are transmitted in plain text.
- SNMPv3 is a secure protocol (with user and password).

⇒ **Use SNMPv3 or disable the function.**

Configuration via web interface

- Log in to the web-based management of the switch. Log in using the corresponding password.
- On the “Service” web page, you can either disable the services HTTP, Telnet and SNMP or switch to secure services.

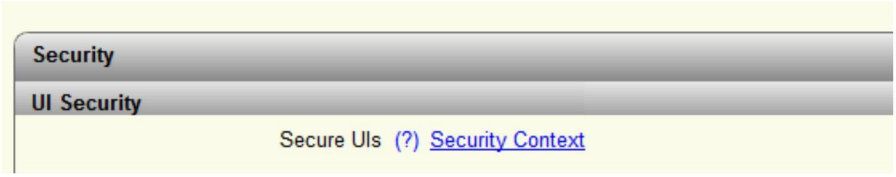
Figure 1-4 Web server configuration



When using SSH, you have to create the “Security Context”.

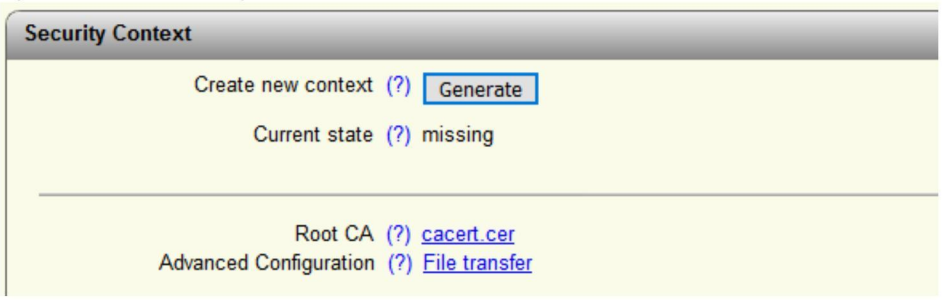
During creation of the security context, a certificate is created for communication via HTTPS. The certificate is used for the browser.

Figure 1-5 Security context



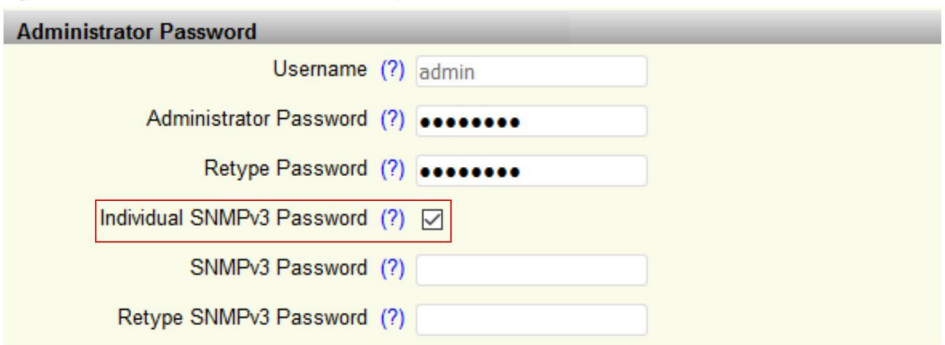
- Change to the “Security” web page.
- Use the “Generate” button to create a “Security Context”.
- For communication via HTTPS, download the “Root CA” certificate and install it in your browser.

Figure 1-6 Creating a security context



- After switching to SNMPv3, the admin password is automatically set as the SNMPv3 password.
- On the “System” web page, a password can be customized under “Administrator Password”.

Figure 1-7 Customized SNMPv3 password



1.5 Disabling unused services

Different services are of great benefit during startup. They include dynamic allocation options for the management IP address of a switch. IP parameters can be allocated from a central point via DHCP, BootP or DCP.

Another service is LLDP (Link Layer Discovery Protocol). With this service, a switch sends neighborhood information to all directly connected devices. In a PROFINET network, e.g., this way, the controller receives all information required for a PROFINET device change. In addition, LLDP is also used by different network, configuration and monitoring tools to read the topology. The Phoenix Contact software for the FL NETWORK MANAGER network monitoring also uses this service.

Facts

Disabling DHCP and BootP

- DHCP and BootP are active services and are used for the reception of dynamic IP information.
- Attackers can misuse this service.

⇒ **Use static IP addresses.**

Disabling LLDP

- LLDP is used for neighborhood detection.
- The switch regularly transmits information about itself.
- Via LLDP, configuration characteristics of the switch can be read.
- LLDP is enabled in delivery state.
- Attackers can receive information.

⇒ **Only enable LLDP for PROFINET applications or for network monitoring software (such as the FL NETWORK MANAGER).**

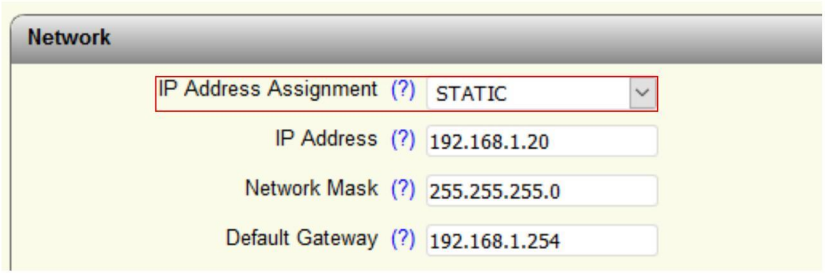
Configuration via web interface

- Log in to the web-based management of the switch. Log in using the corresponding password.
- On the “Network” web page, you can disable the BootP and DHCP services by setting the IP address assignment mode to “STATIC”.

The following parameters can now be configured statically:

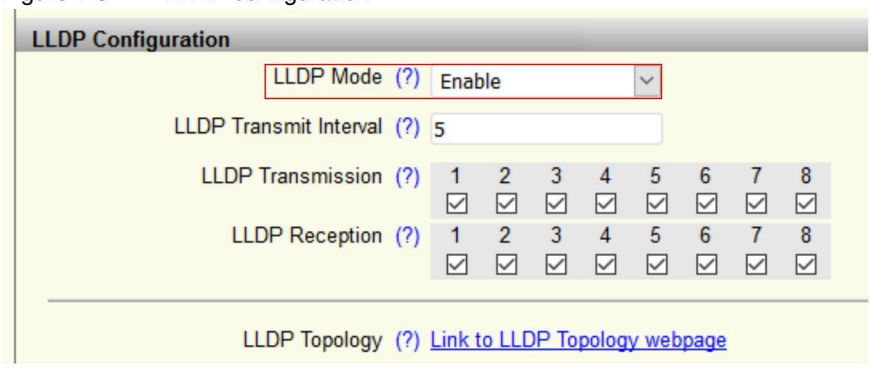
IP Address	Set the desired IP address.
Network Mask	Set the desired subnet mask here.
Default Gateway	Set the desired default gateway here.
DNS Server	Set the IP address of the DNS server here. You can configure up to two DNS server addresses.

Figure 1-8 BootP configuration



- Navigate to the “Service” web page.
  You can disable LLDP globally for the switch.
  As an alternative, you can exclude only certain ports from transmission and/or reception.
  You will also find a link to the LLDP topology.

Figure 1-9 LLDP configuration



1.6 Disabling unused automation protocols

Most Phoenix Contact switches support both a mode for PROFINET and a mode for EtherNet/IP™. In these modes, special information is exchanged between a controller and the switches. For the standard versions these protocols are not enabled in delivery state and should only be used in appropriate networks. If for a switch of the FL SWITCH 2... series, the order designation contains “PN”, PROFINET is enabled in delivery state.

Facts

PROFINET

- The PROFINET mode enables the functions that are typical for PROFINET (PN device, LLDP, ...).
- The “PROFINET Configuration” web page is only visible if PROFINET mode is enabled.
- Via LLDP, configuration characteristics of the switch can be read.
- By default, LLDP is enabled.

⇒ **Disable LLDP if it is not required.**

EtherNet/IP

- The EtherNet/IP mode enables the functions typical for EtherNet/IP (e.g., multicast filtering).
- Via EtherNet/IP, data relevant for asset management systems can be independently identified and read.

⇒ **Only enable EtherNet/IP if it is required.**

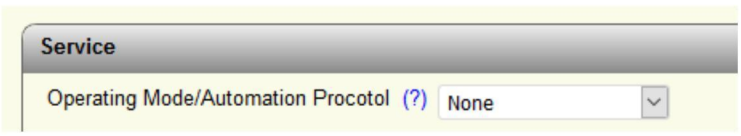
Configuration via web interface

In delivery state, the automation protocols are disabled for the standard versions.

If for a switch of the FL SWITCH 2... series, the order designation contains “PN”, PROFINET is enabled in delivery state.

The configurable modes can be found on the “Service” web page under “Operating Mode”.

Figure 1-10 Changing the operating mode



1.7 Disabling unused routers or switch ports

Openly accessible Ethernet ports enable easy on-site access to the corresponding network. Free Ethernet ports also provide a good opportunity for connecting a laptop for maintenance or network diagnostics. During planning, take into consideration additional free ports that are disabled during regular operation. This way you prevent security gaps.

Facts

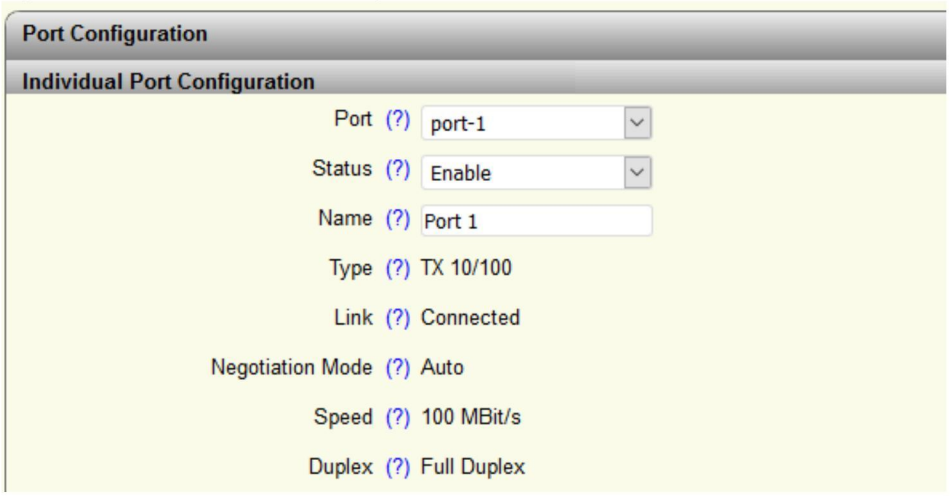
- Unauthorized access via open ports
- During planning, consider diagnostic ports.
- Diagnostic ports play an important role in a network.
- During regular operation, diagnostic ports have to be switched off.

⇒ **Disable all free ports at routers and switches.**

Configuration via web interface

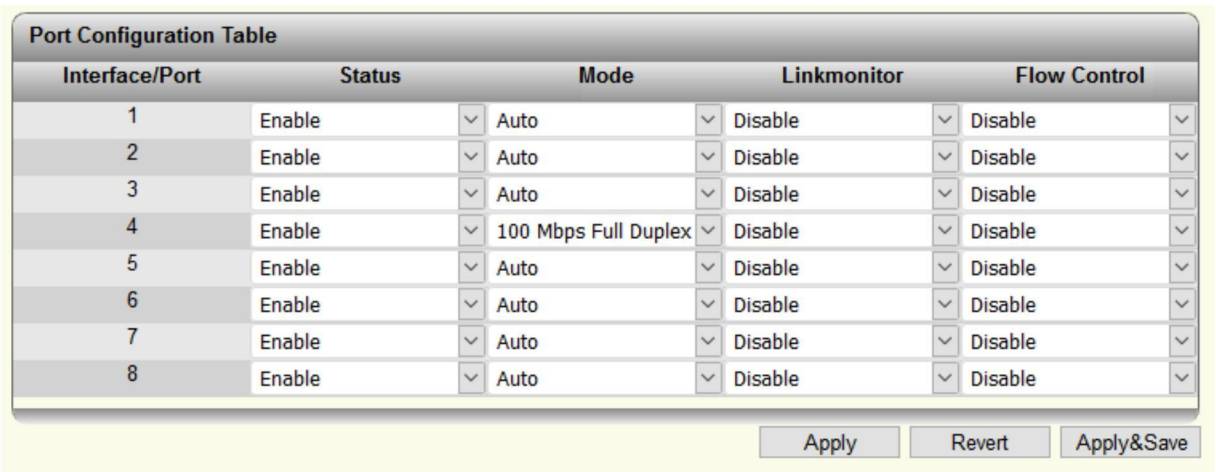
- Log in to the web-based management of the switch. Log in using the corresponding password.
  On the “Port Configuration” web page, you can disable individual ports.

Figure 1-11 Individual port configuration



- The port configuration table is useful if you want to disable several ports at the same time. You can reach the table via the “Port Configuration Table” link at the end of the port configuration web page:

Figure 1-12 Port configuration table



1.8 Disabling the SD card

The SD card in the series 2000 switches serves for saving the configuration. However, the SD card can also be used for manipulation. The use of SD cards is not limited to SD cards from Phoenix Contact.

To receive an alarm when an SD card is used, you can use the alarm contact or an SNMP trap.

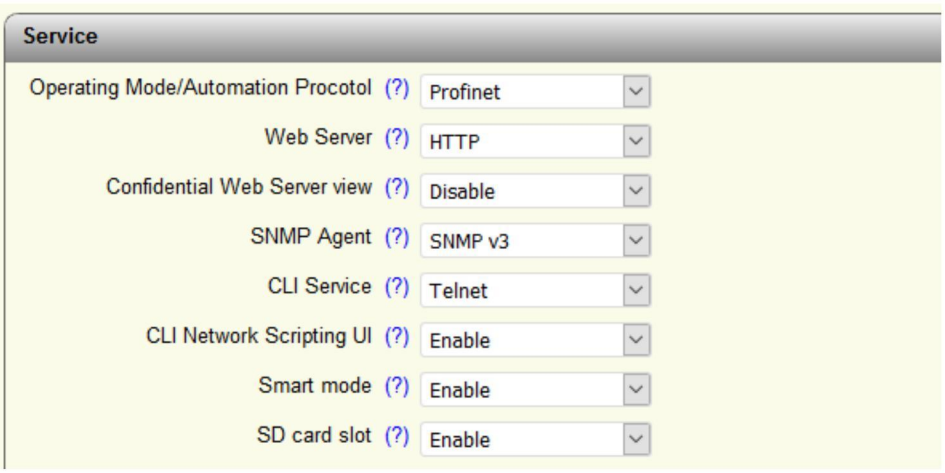
Facts

– The SD card is an interface that can be used for manipulation.
– The SD card enables quick configuration after a device exchange.
⇒ **Disable the SD card slot if no SD card is used.**

Configuration via web interface

- Log in to the web-based management of the switch. Log in using the corresponding password.
- On the “Service” web page, you can disable the SD card slot.

Figure 1-13 Disabling the SD card slot



1.9 Disabling smart mode buttons

The series 2000 switches support the “Smart Mode”. This mode allows for setting different modes using a mode button. Different automation protocols can be enabled, but the mode button can also be used to reset the device to delivery state. The function is explained in the user manual and accessible to everyone. To prevent unauthorized manipulation of the switch, disable the smart mode.

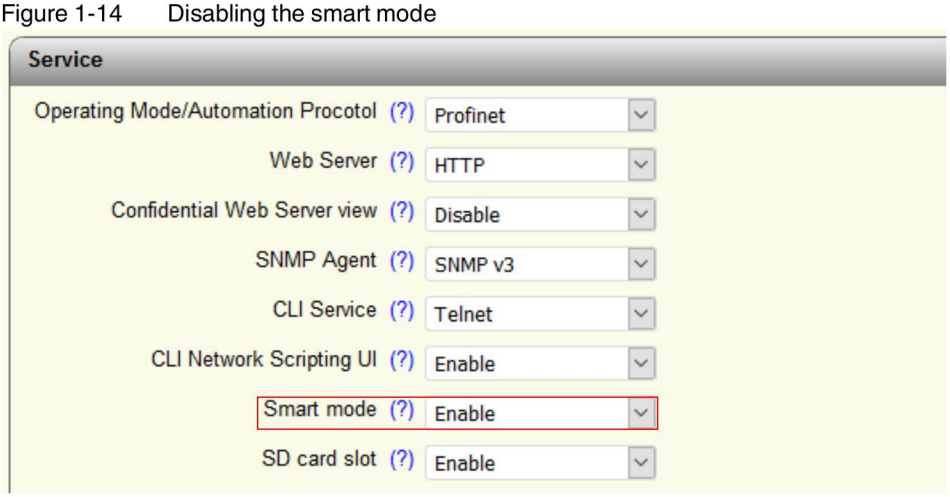
Facts

– Via the mode button, the switch can be reset to delivery state without a password.
– The function of the smart mode is explained in the user manual and accessible to everyone.
⇒ **During operation, switch off the smart mode.**

Configuration via web interface

- Log in to the web-based management of the switch. Log in using the corresponding password.
- On the “Service” web page, you can disable the smart mode.

Figure 1-14 Disabling the smart mode



1.10 Using the RADIUS protocol and MAC-based port security

The RADIUS protocol and the MAC-based port security serve as access protection. Both mechanisms check if a device is authorized to participate in network communication.

The MAC-based port security is a local mechanism on the switch. Here, the communication of a device can be allowed for using the MAC address and for individual ports.

The RADIUS protocol serves for the same purpose. Here, access to a network is also limited. However, authentication is not implemented via the MAC address, but via a user and password. The switch then forwards this information to a RADIUS server. The server checks the data and allows or prohibits the switch to let the connected end device participate in network communication.

Facts

MAC-based port security

- Access regulation using the MAC address
- Up to 50 MAC addresses are permitted per port.
- Each MAC address can only be permitted at one port.
- MAC addresses that are permitted at one port cannot be statically or dynamically learned at other ports.

⇒ **The web-based management or network cannot be accessed via a MAC address that is permitted at another port.**

RADIUS authentication

- Access regulation using user and password
- Users are created on a server.
- If new devices are connected, the switch requests from the server if the device is allowed to participate in network traffic.

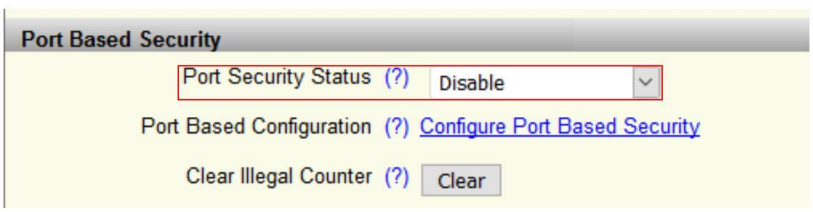
⇒ **The web-based management or network can only be accessed via an authenticated MAC address.**

Configuration via web interface

MAC-based port security

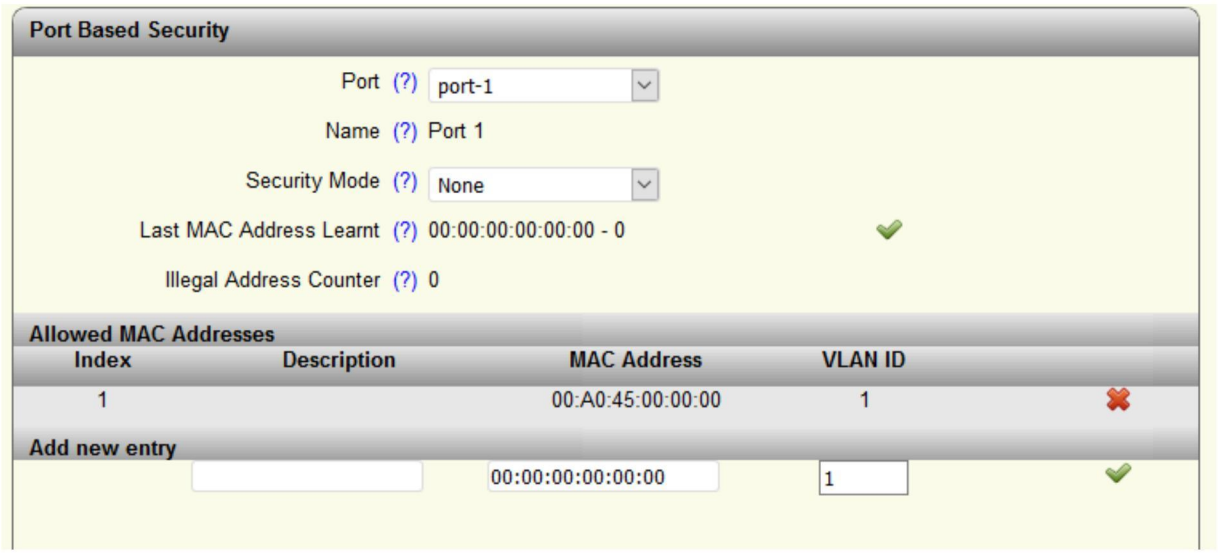
- Log in to the web-based management of the switch. Log in using the corresponding password.
  The “Security” web page provides an option to enable the “Port Based Security”.

Figure 1-15 Enabling Port Based Security



- The settings can be found in the “Configure Port Based Security” link, directly below the global enable option.
  Here, you can enter the MAC address for the corresponding port into the whitelist.

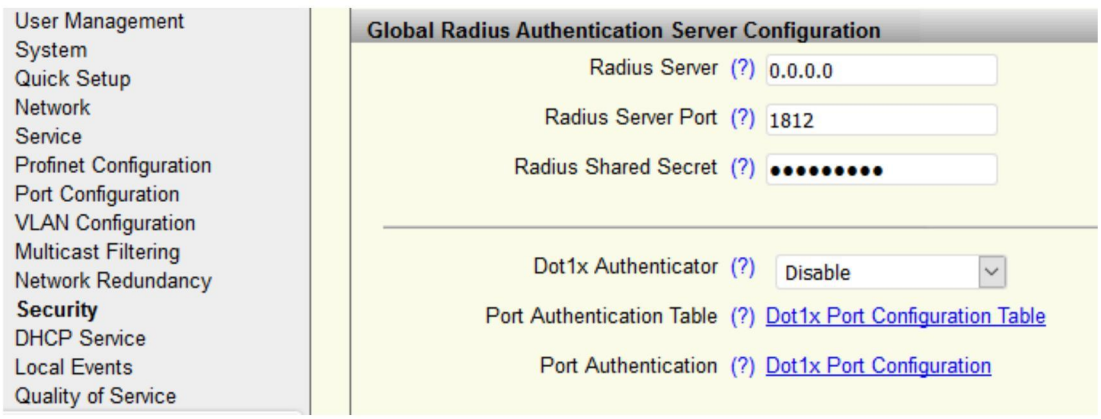
Figure 1-16 Entering the MAC addresses for Port Based Security



RADIUS authentication

- Log in to the web-based management of the switch. Log in using the corresponding password.
- On the “Security” web page, you will find the “Global RADIUS Authentication Server Configuration” area.
  Here, you enter the data for the RADIUS server.

Figure 1-17 RADIUS configuration



- Under the “Dot1x Port Configuration Table”, you can configure all switch ports simultaneously.
  For port-specific detailed configurations, use the “Dot1x Port Configuration Table”.

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.

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 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

109652_en_01
Order No. —01

INSPIRING INNOVATIONS