Basic security for industrial networks for FL SWITCH 30..., 40..., and 48...E

User manual

UM EN IND SECURITY

INSPIRING INNOVATIONS

User manual

Basic security for industrial networks for FL SWITCH 30..., 40..., and 48...E

2016-05-05

Designation: UM EN IND SECURITY

Revision: A

This user manual is valid for:

Designation	Version	Order No.
FL SWITCH 30..., 40..., and 48...E		

Please observe the following notes

User group of this manual

The use of products described in this manual is oriented exclusively to qualified application programmers and software engineers, who are familiar with the safety concepts of automation technology and applicable standards.

Explanation of symbols used and signal words

⚠ This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety measures that follow this symbol to avoid possible injury or death.

There are three different categories of personal injury that are indicated with a signal word.

DANGER This indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING This indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION This indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

❗ This symbol together with the signal word **NOTE** and the accompanying text alert the reader to a situation which may cause damage or malfunction to the device, hardware/software, or surrounding property.

ℹ This symbol and the accompanying text provide the reader with additional information or refer to detailed sources of information.

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

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 standard 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 is 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.

Table of contents

1 Introduction 3

2 Security vulnerability 5

2.1 General management 5
2.1.1 Factory-default passwords 5
2.1.2 Open RJ45 connector security 6

2.2 Device information 6
2.2.1 Minimum firmware release level 6

2.3 General configuration 8
2.3.1 SNTP servers not specified 8
2.3.2 Two trap servers are not specified 9

2.4 Management interface 10
2.4.1 Insecure SNMP in use 10
2.4.2 SNMP community names use factory defaults (SNMP v1/2) 10
2.4.3 HTTP server isn't disabled 11

2.5 User account management 12
2.5.1 Assign lowest level of privilege to user accounts 12
2.5.2 Unnecessary user accounts 13
2.5.3 Switch 802.1x Port Access Control uses weak EAP protocol 14

2.6 Configuration management 14
2.6.1 Configuration in the RAM and nonvolatile RAM aren't synchronized ... 14
2.6.2 Restrict access to backup configuration files 14
2.6.3 TFTP server access is not restricted 15

2.7 Services 15
2.7.1 Login expiration is greater than 15 minutes 15

2.8 Extended port configuration 16
2.8.1 802.1x ports must start in force unauthorized state 16

2.9 VLAN vulnerability 17
2.9.1 VLAN 1 is being used as an industrial production VLAN 17
2.9.2 Access ports assigned to the trunk VLAN 17
2.9.3 Disabled ports aren't assigned to an unused VLAN 18

A Appendixes 21

A 1 List of figures 21

1 Introduction

In the past, the industrial network used fieldbus technologies that weren’t connected to other networks, and the maintenance of network security was easy. Because of this, fieldbus-connected machines were “standalone islands”. Nowadays, the industrial network is a quickly growing subset of the Ethernet network. This network is very “changeable”, meaning it’s never static, with additional devices being added and removed from the industrial network.

These industrial networks are based on Ethernet technology, so network security must be applied to prevent any disruptions in normal production activity.

This document provides guidance on preventing security incidents in the Ethernet network and the loss or corruption of industrial communication technology and the information within the system. The FL SWITCH 30..., 40..., and 48...E switches are used as a reference, but implementing best practices for network security can be extended beyond these specific switch models.

2 Security vulnerability

2.1 General management

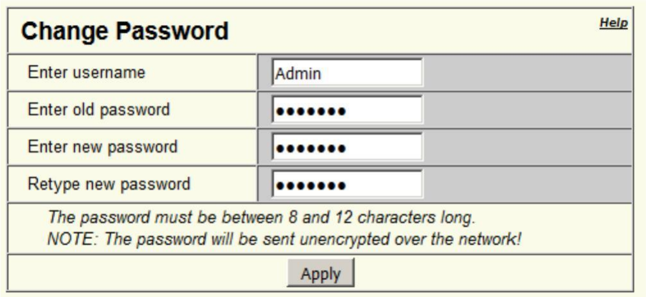
2.1.1 Factory-default passwords

Be sure all factory-default passwords are changed.

Switches that aren't protected with a strong password offer anyone the opportunity to crack the login credentials and access the device, possibly causing device denial or denial of network. If the default password isn't changed when the switch is commissioned, it increases the possibility of someone capturing the password and gaining unauthorized access to the network.

Prevention

The network administrator must change the password on the “General Configuration/Change Password” page.



Change Password

Enter username	Admin
Enter old password	•••••••
Enter new password	•••••••
Retype new password	•••••••

The password must be between 8 and 12 characters long.
NOTE: The password will be sent unencrypted over the network!

Figure 2-1 “Change Password” page

A password should be at least eight characters long and not contain your user name, real name, company name, or any actual word that can be guessed after a few characters. A strong password is considered one that uses characters from at least three of the following four categories:

- uppercase letters (A, B, C...)
- lowercase letters (a, b, c...)
- numeric characters (0, 1, 2...)
- special characters (+, #, [...)

2.1.2 Open RJ45 connector security

Be sure any open RJ45 ports are secured using port security (MAC-based security or 802.1x port authentication) on all accessible RJ45 ports in the switch.

Access to the industrial network from inside the facility can be quite simple using only a laptop connected to an unsecured RJ45 port. Reducing this unauthorized access at all RJ45 ports is important in keeping the network secure.

Prevention

The industrial network should use either MAC-based security or 802.1x port authentication. This requires a password for any device that connects through any port of the switch.

2.2 Device information

2.2.1 Minimum firmware release level

Be sure the latest released firmware version is installed on the industrial switches.

Industrial switches not running the latest version of the firmware are vulnerable to network attacks. By using the latest released version of the firmware, a stable base of bug and security fixes is maintained.

Prevention

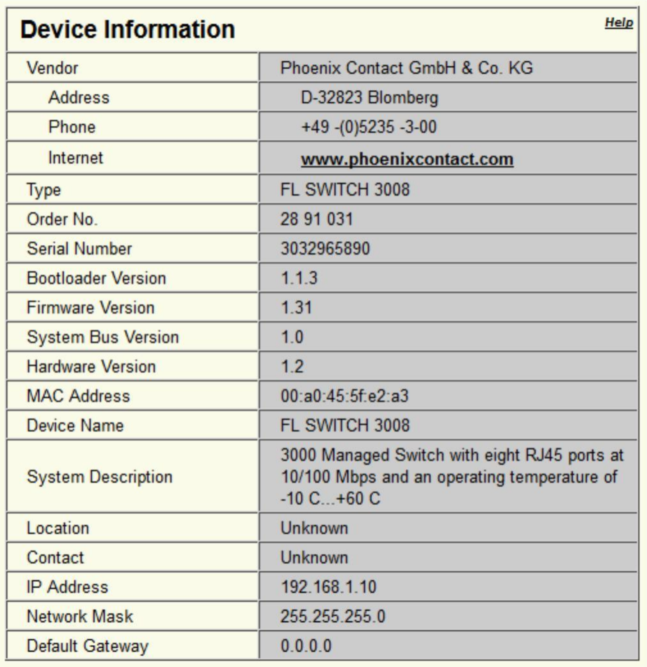
Firmware updates are available for download at phoenixcontact.com. This should be checked occasionally for any new updates and those updates installed, when applicable.

Information on the firmware upgrade process can be found in the application note:

– Upgrading the firmware on FL SWITCH… network switches

This document can be found at phoenixcontact.com on the “Downloads” tab of the product.

To determine the currently installed firmware version, go to the “Device Information/General” page and note the Firmware Version listed.

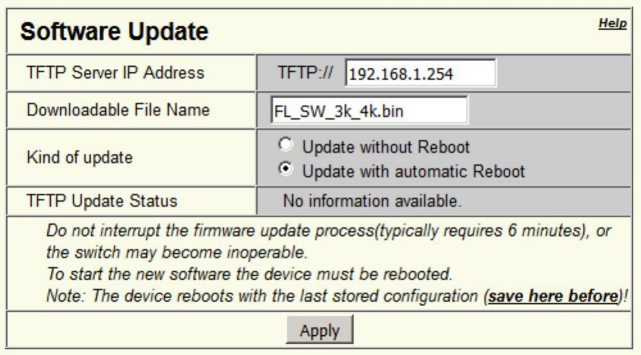


Device Information Help

Vendor	Phoenix Contact GmbH & Co. KG
Address	D-32823 Blomberg
Phone	+49 -(0)5235 -3-00
Internet	www.phoenixcontact.com
Type	FL SWITCH 3008
Order No.	28 91 031
Serial Number	3032965890
Bootloader Version	1.1.3
Firmware Version	1.31
System Bus Version	1.0
Hardware Version	1.2
MAC Address	00:a0:45:5f:e2:a3
Device Name	FL SWITCH 3008
System Description	3000 Managed Switch with eight RJ45 ports at 10/100 Mbps and an operating temperature of -10 C...+60 C
Location	Unknown
Contact	Unknown
IP Address	192.168.1.10
Network Mask	255.255.255.0
Default Gateway	0.0.0.0

Figure 2-2 “Device Information” page

Installation of a firmware update is made on the “General Configuration/Software Update” page.



Software Update Help

TFTP Server IP Address	TFTP:// 192.168.1.254
Downloadable File Name	FL_SW_3k_4k.bin
Kind of update	○ Update without Reboot ● Update with automatic Reboot
TFTP Update Status	No information available.

Do not interrupt the firmware update process(typically requires 6 minutes), or the switch may become inoperable.
To start the new software the device must be rebooted.
*Note: The device reboots with the last stored configuration (**save here before**)!*

Figure 2-3 “Software Update” page

2.3 General configuration

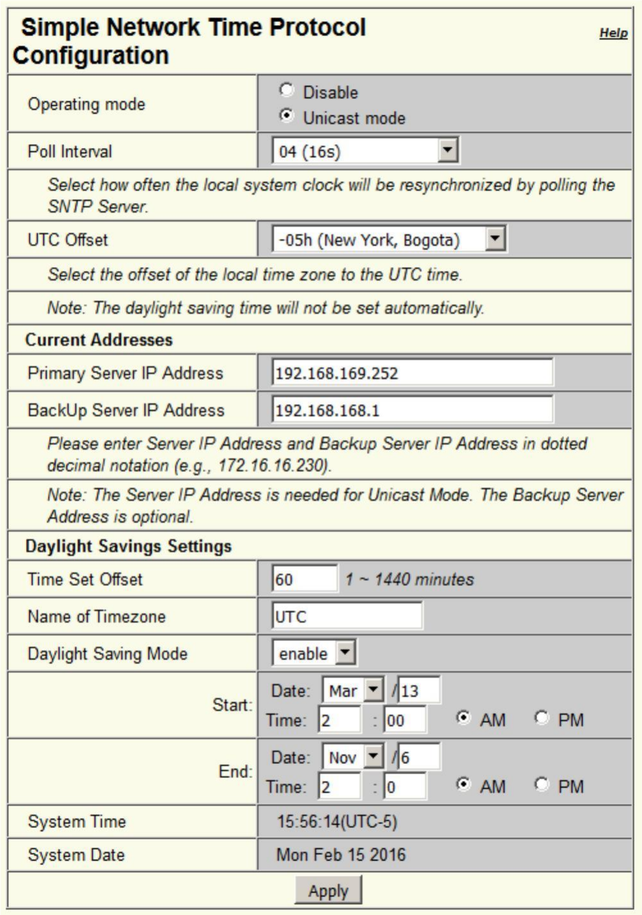
2.3.1 SNTP servers not specified

Be sure SNTP time server IP addresses (primary and backup) have a live connection to the SNTP server.

Maintaining accurate, synchronized time between switches is very important. Without this common time, any logs generated by the switches cannot be compared. When information is needed for a security reason, only synchronized time provides a reliable image of the incident.

Prevention

The network administrator must set the SNTP server IP address on the “General Configuration/SNTP Configuration” page. Both the “Primary Server IP Address” and “BackUp Server IP Address” fields should be set.



Simple Network Time Protocol Configuration

Operating mode	○ Disable ● Unicast mode
Poll Interval	04 (16s)
Select how often the local system clock will be resynchronized by polling the SNTP Server.	
UTC Offset	-05h (New York, Bogota)
Select the offset of the local time zone to the UTC time.	
Note: The daylight saving time will not be set automatically.	
Current Addresses	
Primary Server IP Address	192.168.169.252
BackUp Server IP Address	192.168.168.1
Please enter Server IP Address and Backup Server IP Address in dotted decimal notation (e.g., 172.16.16.230).	
Note: The Server IP Address is needed for Unicast Mode. The Backup Server Address is optional.	
Daylight Savings Settings	
Time Set Offset	60 *1 ~ 1440 minutes*
Name of Timezone	UTC
Daylight Saving Mode	enable
Start:	Date: Mar / 13 Time: 2 : 00 ● AM ○ PM
End:	Date: Nov / 6 Time: 2 : 0 ● AM ○ PM
System Time	15:56:14(UTC-5)
System Date	Mon Feb 15 2016

Figure 2-4 “Simple Network Time Protocol Configuration” page

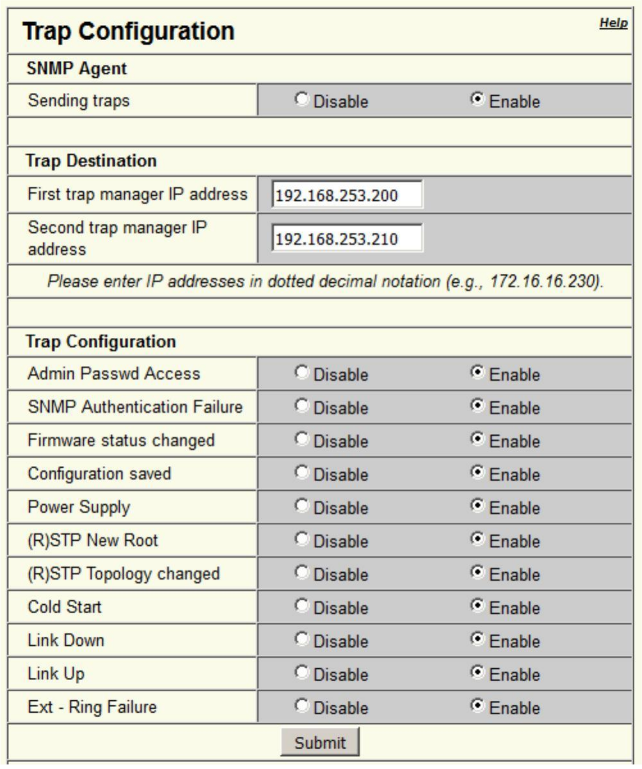
2.3.2 Two trap servers are not specified

Be sure the trap server IP addresses (primary and backup) have a live connection to the trap server.

The trap information is very important in the switches. SNMP traps are log messages sent by network devices to an SNMP trap server, where those messages are received and processed. These messages provide information about the operation of the switch that can help to detect a physical attack (device connected to a switch port) or incident (switch was manually rebooted by a power loss).

Prevention

The trap servers are configured in the “General Configuration/Trap Configuration” page. Both the “First trap manager IP address” and “Second trap manager IP address” must be set.



Trap Configuration

SNMP Agent		
Sending traps	○ Disable	● Enable
Trap Destination		
First trap manager IP address	192.168.253.200	
Second trap manager IP address	192.168.253.210	
Please enter IP addresses in dotted decimal notation (e.g., 172.16.16.230).		
Trap Configuration		
Admin Passwd Access	○ Disable	● Enable
SNMP Authentication Failure	○ Disable	● Enable
Firmware status changed	○ Disable	● Enable
Configuration saved	○ Disable	● Enable
Power Supply	○ Disable	● Enable
(R)STP New Root	○ Disable	● Enable
(R)STP Topology changed	○ Disable	● Enable
Cold Start	○ Disable	● Enable
Link Down	○ Disable	● Enable
Link Up	○ Disable	● Enable
Ext - Ring Failure	○ Disable	● Enable

Figure 2-5 “Trap Configuration” page

2.4 Management interface

2.4.1 Insecure SNMP in use

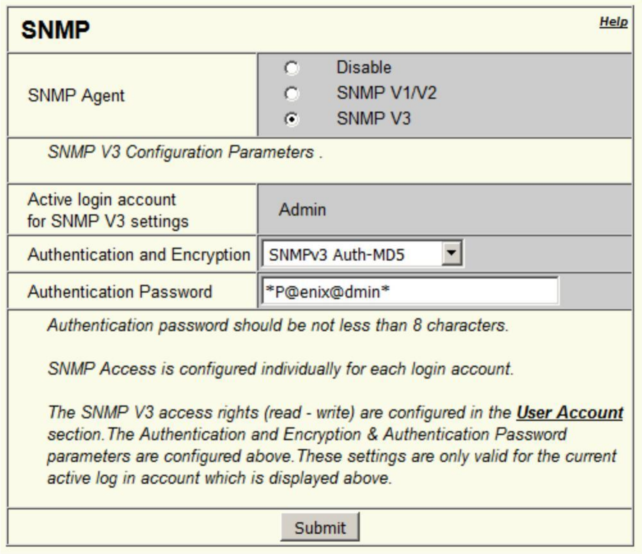
Use SNMP v3 across the entire industrial network.

SNMP v1 and v2 don’t support encryption of packets, so these packets could be captured and used by an unauthorized person. This information can be used to launch attacks on the industrial network. SNMP v3 requires the use of a password.

Prevention

The network administrator must examine the configuration of the switches and, if the industrial application allows, enable SNMP v3 in the switch.

The SNMP settings are configured on the “General Configuration/Management/SNMP” page. Click the “SNMP v3” button to activate v3 and enter an appropriate password in the “Authentication Password” field.



SNMP

SNMP Agent	○ Disable ○ SNMP V1/V2 ● SNMP V3

SNMP V3 Configuration Parameters .

Active login account for SNMP V3 settings	Admin
Authentication and Encryption	SNMPv3 Auth-MD5
Authentication Password	*P@enix@dmin*

Authentication password should be not less than 8 characters.

SNMP Access is configured individually for each login account.

The SNMP V3 access rights (read - write) are configured in the ***User Account*** *section. The Authentication and Encryption & Authentication Password parameters are configured above. These settings are only valid for the current active log in account which is displayed above.*

Figure 2-6 “SNMP” page

2.4.2 SNMP community names use factory defaults (SNMP v1/2)

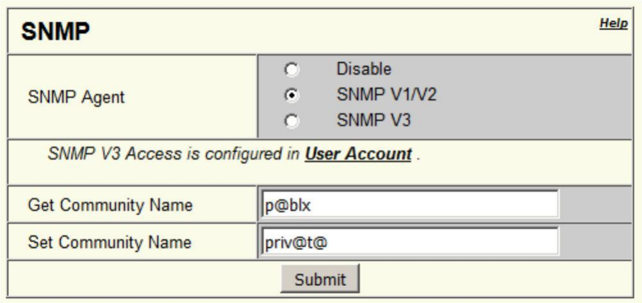
SNMP v1 and v2 are not recommended because of limited security. If they must be used, always change the factory default community names.

Be sure the “Get Community Name” and “Set Community Name” are changed from the factory default values.

The default “Get Community Name” value is **public** and the default “Set Community Name” value is **private**. These community names are known to everyone, so a network attack can be easily initiated.

Prevention

The network administrator should examine the configuration of the switches and change the factory default community names. The community names are configured on the “General Configuration/Management Interface/SNMP” page in the “Get Community Name” and “Set Community Name” fields.



SNMP Help

SNMP Agent
○ Disable
● SNMP V1/V2
○ SNMP V3

SNMP V3 Access is configured in ***User Account*** *.*

Get Community Name: p@blx

Set Community Name: priv@t@

Submit

Figure 2-7 “SNMP” page

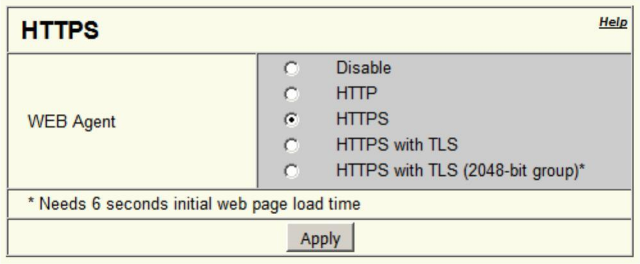
2.4.3 HTTP server isn't disabled

Be sure the HTTP WBM access is disabled.

HTTP (Hypertext Transfer Protocol) provides an unsecured method to access the WBM of the managed industrial switch. Authentication access to the switch via HTTP sends the credentials in clear text across the network; this method makes the HTTP a relatively risky choice.

Prevention

The network administrator must disable the HTTP protocol and enable either HTTPS, HTTPS with TLS, or HTTPS with TLS (2048-bit group) mode if allowed by the industry application. These settings can be configured on the “General Configuration/ Management Interfaces/HTTP/HTTPS” page.



HTTPS Help

WEB Agent
○ Disable
○ HTTP
● HTTPS
○ HTTPS with TLS
○ HTTPS with TLS (2048-bit group)*

* Needs 6 seconds initial web page load time

Apply

Figure 2-8 “HTTPS” page

- **HTTPS**: Includes SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 with 1024-bit protocols.
- **HTTPS with TLS**: Includes TLSv1.0, TLSv1.1, and TLSv1.2 with 1024-bit protocols.
- **HTTPS with TLS (2048-bit group)**: Includes TLSv1.0, TLSv1.1, and TLSv1.2 with 2048-bit protocols.

2.5 User account management

2.5.1 Assign lowest level of privilege to user accounts

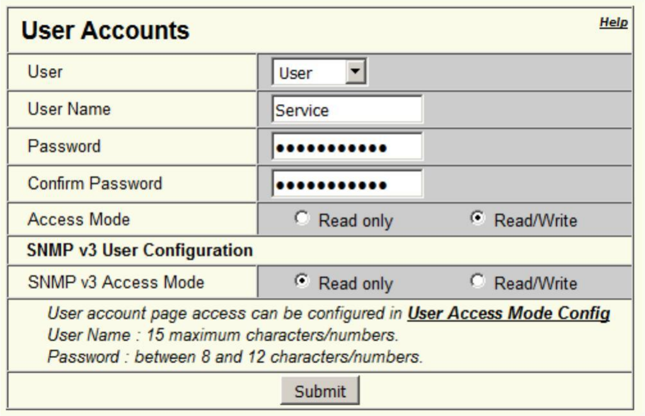
Be sure all users have only the privilege necessary that allows them to perform their tasks.

A user with higher privilege levels than necessary may have access to areas that he is not qualified to serve.

Prevention

The network administrator should review the users' privilege and the level of privilege required for the users' duties.

User accounts are configured on the "General Configuration/User Account Management/User Accounts" page and "General Configuration/User Access Mode Config" page.

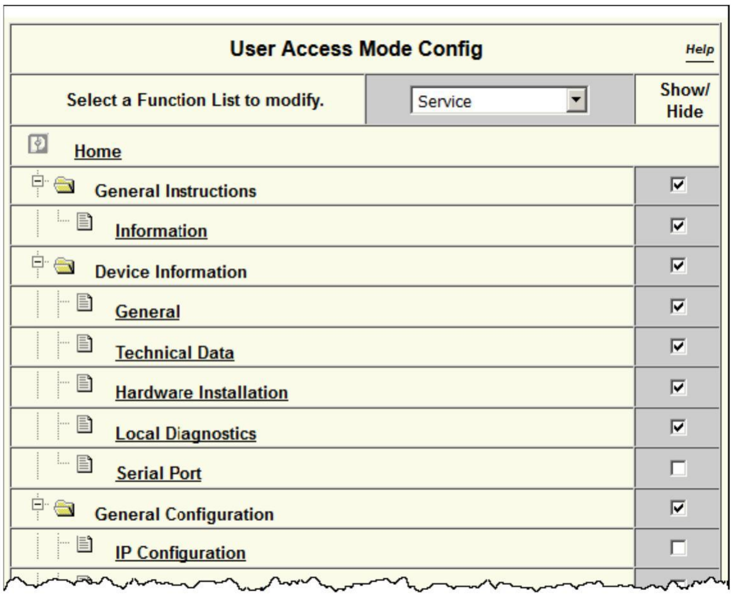


User Accounts

User	User
User Name	Service
Password	••••••••••••
Confirm Password	••••••••••••
Access Mode	○ Read only ● Read/Write
SNMP v3 User Configuration	
SNMP v3 Access Mode	● Read only ○ Read/Write

User account page access can be configured in ***User Access Mode Config***
User Name : 15 maximum characters/numbers.
Password : between 8 and 12 characters/numbers.

Figure 2-9 "User Accounts" page



User Access Mode Config Help

Select a Function List to modify.	Service	Show/ Hide
Home		
General Instructions		☑
Information		☑
Device Information		☑
General		☑
Technical Data		☑
Hardware Installation		☑
Local Diagnostics		☑
Serial Port		□
General Configuration		☑
IP Configuration		□

Figure 2-10 “User Access Mode Config” page

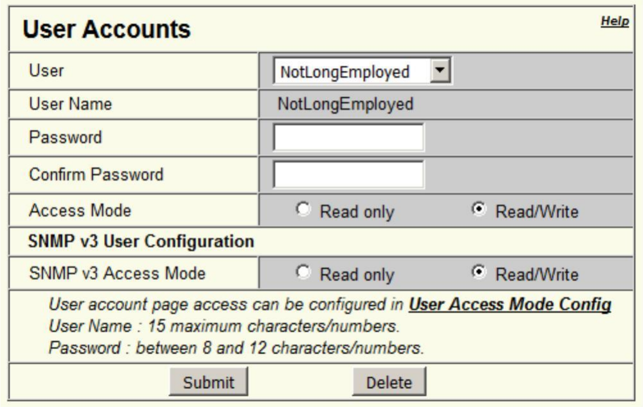
2.5.2 Unnecessary user accounts

Immediately remove any accounts that are no longer required from the local switch and from the authentication server.

Unnecessary user accounts may allow a user to get partial or full control of a switch.

Prevention

The network administrator should review the user accounts in the switch locally and in the authentication server and disable or remove them when they are not needed. User accounts are configured on the “General Configuration/User Account Management” page.



User Accounts Help

User	NotLongEmployed
User Name	NotLongEmployed
Password	
Confirm Password	
Access Mode	○ Read only ● Read/Write
SNMP v3 User Configuration	
SNMP v3 Access Mode	○ Read only ● Read/Write

User account page access can be configured in ***User Access Mode Config***
User Name : 15 maximum characters/numbers.
Password : between 8 and 12 characters/numbers.

Figure 2-11 “User Accounts” page

2.5.3 Switch 802.1x Port Access Control uses weak EAP protocol

When 802.1x port authentication is utilized, a secure connection is established between the authentication server and the client side.

For example, Protected Extensible Authentication Protocol (PEAP) provides strong security for the client and is supported by most operating systems.

Prevention

Use the strongest authentication protocol possible for the operating system.

2.6 Configuration management

2.6.1 Configuration in the RAM and nonvolatile RAM aren't synchronized

Be sure the configuration in the RAM and nonvolatile RAM are synchronized.

If the configuration in the nonvolatile RAM isn’t synchronized with the configuration in the RAM and a switch malfunctions, the switch won’t restart with the latest changes. If the recent changes include security-related modifications, the switch will restart with security issues and still be vulnerable to attack.

Prevention

When any change is made, click the “Save” icon in the upper right-hand corner to go to the “Configuration Management” page and save the changes to the nonvolatile memory.

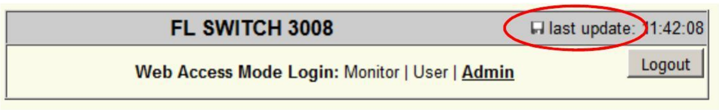


Figure 2-12 “Save” icon

2.6.2 Restrict access to backup configuration files

Be sure that the system where the configuration files are stored is sufficiently protected by the local system security mechanism.

If the backup copies of the configuration files are stored in an insecure location, attacks can be launched easily and large parts of the network can be incapacitated.

Prevention

System administration must use security tools to control accessibility to the configuration files and prevent access by unauthorized users.

2.6.3 TFTP server access is not restricted

Be sure the TFTP server resides in the management LAN and only authorized people and devices have access to the server.

The TFTP server requires limited and restricted access.

Prevention

Set the TFTP Server so LAN traffic is restricted by the TFTP Server, and access is controlled by ACLs.

2.7 Services

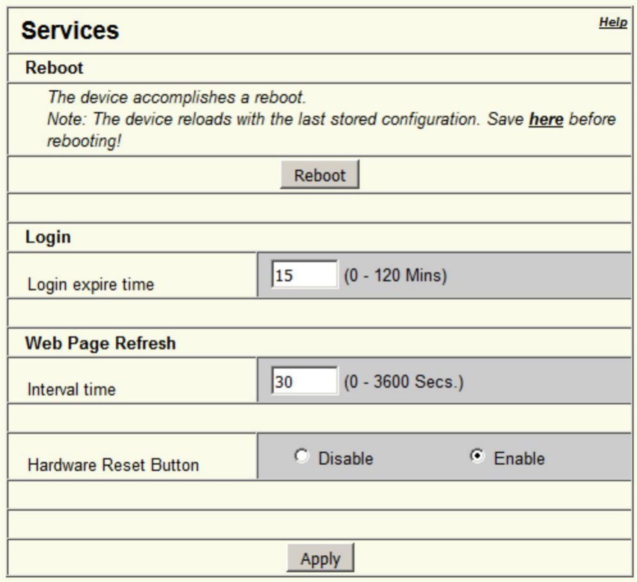
2.7.1 Login expiration is greater than 15 minutes

Be sure the login expire time is configured to time out after 15 minutes or less of inactivity.

Reducing the login expire time to 15 minutes or less reduces the time frame available for attack.

Prevention

The login expire time is set on the “Switch Station/Services” page.



Services

Reboot

The device accomplishes a reboot.
*Note: The device reloads with the last stored configuration. Save **here** before rebooting!*

Login

Login expire time: 15 (0 - 120 Mins)

Web Page Refresh

Interval time: 30 (0 - 3600 Secs.)

Hardware Reset Button: ○ Disable ● Enable

Figure 2-13 “Services” page

Set the “Login expire time” field to **15** or less.

2.8 Extended port configuration

2.8.1 802.1x ports must start in force unauthorized state

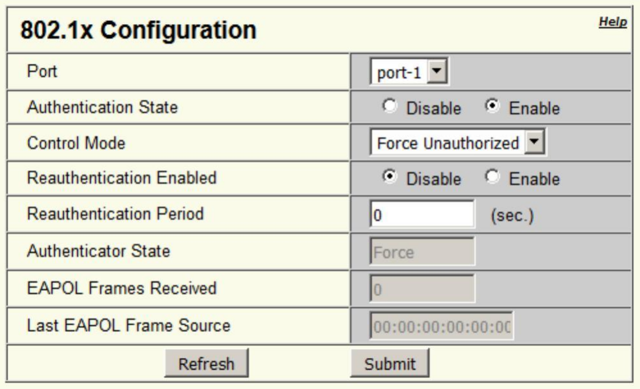
Be sure 802.1x port authentication is implemented on all ports available for service access to the network and that all service access ports start in the force unauthorized state.

IEEE 802.1x port authentication helps to prevent unauthorized access to the network and keeps the network secure. Internal access to the network can be very easy, requiring only a laptop or device connected to an open RJ45 port.

> Information on IEEE 802.1x port authentication can be found in two application notes:
> - Configuring the FL SWITCH for RADIUS IEEE 802.1x port authentication with Cisco Secure ACS systems
> - Configuring the FL SWITCH for RADIUS IEEE 802.1x port authentication with FreeRADIUS Server (Linux)
>
> These documents can be found at phoenixcontact.com on the “Downloads” tab of the product.

Prevention

Service access is set on the “Switch Station/Ports/Extended Configuration/802.1x Configuration Table” page.



802.1x Configuration

Port	port-1
Authentication State	○ Disable ● Enable
Control Mode	Force Unauthorized
Reauthentication Enabled	● Disable ○ Enable
Reauthentication Period	0 (sec.)
Authenticator State	Force
EAPOL Frames Received	0
Last EAPOL Frame Source	00:00:00:00:00:0C

Figure 2-14 “802.1x Configuration” page

In the “Control Mode” field, select **Force Unauthorized** from the drop-down menu.

2.9 VLAN vulnerability

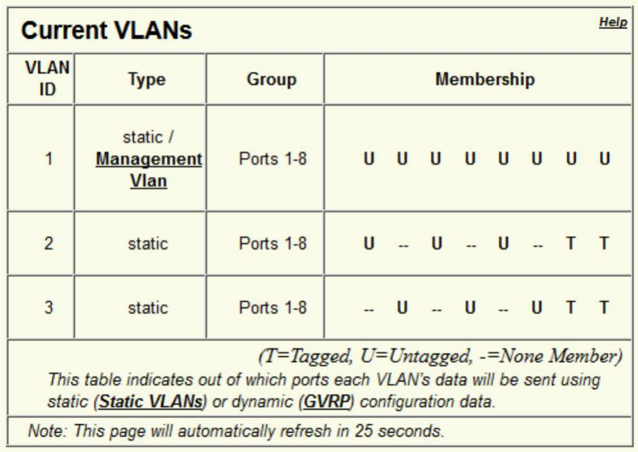
2.9.1 VLAN 1 is being used as an industrial production VLAN

Be sure the management VLAN 1 isn't used as an industrial production VLAN.

Switches use VLAN 1 as the default VLAN in the VLAN-based network. VLAN 1 can span the entire network, if its scope is large enough, and management traffic can increase the risk significantly.

Prevention

Check the "Current VLANs" setting on the "Switch Station/VLAN" page and verify that no access ports are assigned membership to VLAN 1 from the industrial production network.



Current VLANs Help

VLAN ID	Type	Group	Membership							
1	static / Management Vlan	Ports 1-8	U	U	U	U	U	U	U	U
2	static	Ports 1-8	U	--	U	--	U	--	T	T
3	static	Ports 1-8	--	U	--	U	--	U	T	T

(T=Tagged, U=Untagged, -=None Member)
This table indicates out of which ports each VLAN's data will be sent using static (Static VLANs) or dynamic (GVRP) configuration data.

Note: This page will automatically refresh in 25 seconds.

Figure 2-15 "Current VLANs" page

Figure 2-15 shows that ports 1, 3, and 5 are part of VLAN 2 and ports 2, 4, and 6 are part of VLAN 3. The management VLAN is VLAN 1, and it cannot be edited or deleted. As a special VLAN, all ports of the switch are assigned as Untagged ports (U) in VLAN 1.

2.9.2 Access ports assigned to the trunk VLAN

The network administrator has to be sure access end ports aren't assigned to the trunk VLAN.

When an attacker has access to a switch port belonging to the native VLAN of the trunk port, double encapsulation can be made (the outer tag will have the attacker's VLAN ID and the inner tag will have the victim's VLAN ID).

Prevention

Review and verify that the end ports aren't connected to a trunk VLAN port in the switch.

2.9.3 Disabled ports aren't assigned to an unused VLAN

Be sure disabled ports are assigned to an unused VLAN.

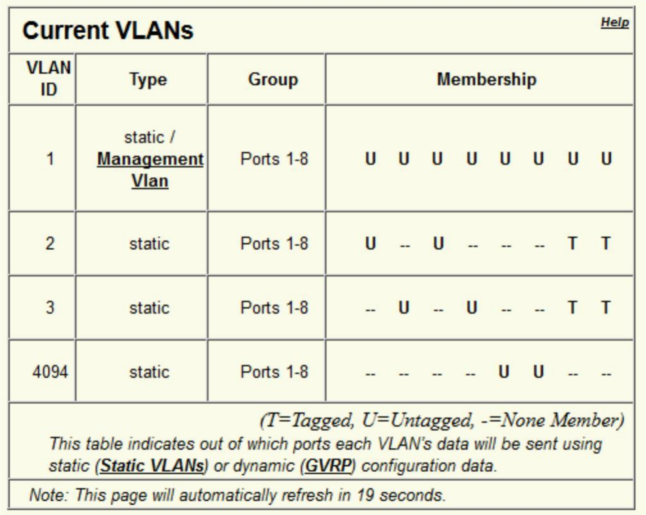
NOTE:

Do not assign disabled ports to VLAN 1.

There is a chance that a disabled port assigned to the industrial production or management VLAN can become enabled accidentally or by an attacker, allowing someone to gain access to that VLAN as a member port.

Prevention

Review the “Current VLANs” configurations on the “Switch Station/VLAN” page.



Current VLANs

VLAN ID	Type	Group	Membership							
1	static / **Management Vlan**	Ports 1-8	U	U	U	U	U	U	U	U
2	static	Ports 1-8	U	--	U	--	--	--	T	T
3	static	Ports 1-8	--	U	--	U	--	--	T	T
4094	static	Ports 1-8	--	--	--	--	U	U	--	--

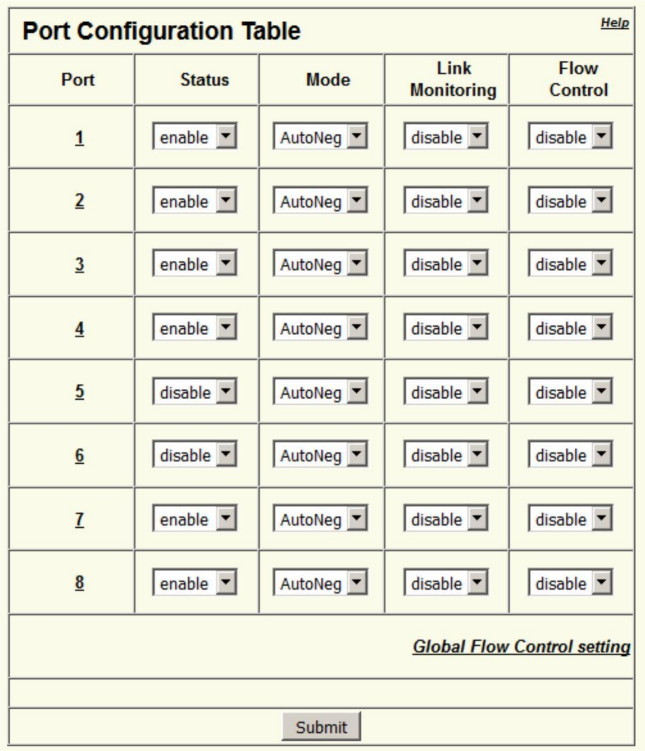
(T=Tagged, U=Untagged, -=None Member)

*This table indicates out of which ports each VLAN's data will be sent using static (**Static VLANs**) or dynamic (**GVRP**) configuration data.*

Note: This page will automatically refresh in 19 seconds.

Figure 2-16 “Current VLANs” page showing unused VLAN 4094

Verify that all ports not being used are disabled and assigned to a VLAN that isn't used for any other purpose. The VLAN ID can be the last one, such as 4094, and can be used specifically for this purpose. The unused ports should be disabled on the “Switch Station/Ports/Port Configuration Table” page.



Port Configuration Table

Port	Status	Mode	Link Monitoring	Flow Control
1	enable	AutoNeg	disable	disable
2	enable	AutoNeg	disable	disable
3	enable	AutoNeg	disable	disable
4	enable	AutoNeg	disable	disable
5	disable	AutoNeg	disable	disable
6	disable	AutoNeg	disable	disable
7	enable	AutoNeg	disable	disable
8	enable	AutoNeg	disable	disable

Figure 2-17 “Port Configuration Table” page

Figure 2-17 shows the “Status” field for ports 5 and 6 disabled, as is also shown in Figure 2-16.

A Appendixes

A 1 List of figures

Section 2

Figure 2-1: “Change Password” page 5

Figure 2-2: “Device Information” page 7

Figure 2-3: “Software Update” page 7

Figure 2-4: “Simple Network Time Protocol Configuration” page 8

Figure 2-5: “Trap Configuration” page 9

Figure 2-6: “SNMP” page 10

Figure 2-7: “SNMP” page 11

Figure 2-8: “HTTPS” page 11

Figure 2-9: “User Accounts” page 12

Figure 2-10: “User Access Mode Config” page 13

Figure 2-11: “User Accounts” page 13

Figure 2-12: “Save” icon 14

Figure 2-13: “Services” page 15

Figure 2-14: “802.1x Configuration” page 16

Figure 2-15: “Current VLANs” page 17

Figure 2-16: “Current VLANs” page showing unused VLAN 4094 18

Figure 2-17: “Port Configuration Table” page 19