Weidmüller

Industrial Ethernet Training 17

Configuring the security features of Weidmueller switches

Abstract:

Security in Ethernet Switches is important to ensure that unauthorized users/devices will not be able to access the network. Security can be categorized in two levels: the port access and the access to the Switch's management. This application note explains the main configuration options to ensure security on both port access level and switch's management access level.

Hardware reference

No.	Component name	Article No.	Hardware / Firmware version
1	IE-Training Kit-01	2881730000	1.1.2 (Build 125086)
2			
3			

IE-Training Kit Content

No.	Component name	Article No.	Hardware / Firmware version
1	IE-SR-4TX	2751270000	1.4.7
2	IE-SW-AL08M-8TX	2682280000	1.08
3	IE-SW-AL05M-5TX	2682250000	1.14
4	IE-CS-MBGW-2TX-1COM	2682600000	3.11

Software reference

No.	Software name	Article No.	Software version
1			
2			
3			

File reference

No.	Name	Description	Version
1			
2			

Contact
Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
www.weidmueller.com

For any further support please contact your local sales representative:
https://www.weidmueller.com/countries

Content

1 Warning and Disclaimer

Warning
Controls may fail in unsafe operating conditions, causing uncontrolled operation of the controlled devices. Such hazardous events can result in death and / or serious injury and / or property damage. Therefore, there must be safety equipment provided / electrical safety design or other redundant safety features that are independent from the automation system.

Disclaimer
This Application Note / Quick Start Guide / Example Program does not relieve you of the obligation to handle it safely during use, installation, operation and maintenance. Each user is responsible for the correct operation of his control system. By using this Application Note / Quick Start Guide / Example Program prepared by Weidmüller, you accept that Weidmüller cannot be held liable for any damage to property and / or personal injury that may occur because of the use.

Note
The given descriptions and examples do not represent any customer-specific solutions, they are simply intended to help for typical tasks. The user is responsible for the proper operation of the described products. Application notes / Quick Start Guides / Example Programs are not binding and do not claim to be complete in terms of configuration as well as any contingencies. By using this Application Note / Quick Start Guide / Example Program, you acknowledge that we cannot be held liable for any damages beyond the described liability regime. We reserve the right to make changes to this application note / quick start guide / example at any time without notice. In case of discrepancies between the proposals Application Notes / Quick Start Guides / Program Examples and other Weidmüller publications, like manuals, such contents have always more priority to the examples. We assume no liability for the information contained in this document. Our liability, for whatever legal reason, for damages caused using the examples, instructions, programs, project planning and performance data, etc. described in this Application Note / Quick Start Guide / Example is excluded.

Security notes
In order to protect equipment, systems, machines and networks against cyber threats, it is necessary to implement (and maintain) a complete state-of-the-art industrial security concept. The customer is responsible for preventing unauthorized access to his equipment, systems, machines and networks. Systems, machines and components should only be connected to the corporate network or the Internet if necessary and appropriate safeguards (such as firewalls and network segmentation) have been taken.

2 Prerequisites for doing

You need to have the following hardware and documentation

- Industrial Ethernet Training Kit
- Application Note Industrial Ethernet Training 01 “Setting up default configuration of IE Training Kit” for applying default IP address configuration

3 Security Menu in Advanced Line switches

The Advanced Line includes three different subfamilies of switches:

- Lite Managed models
- Fast Ethernet and Fast/Gigabit models
- Full Gigabit models

The security features are not the same in these three subfamilies and below can be seen the available Security menu depending on the product we are using.

Security menu in Lite Managed switches

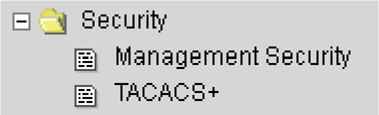


Figure 1: Security menu in Lite Managed switches

Security menu in Fast Ethernet or Fast/Gigabit switches

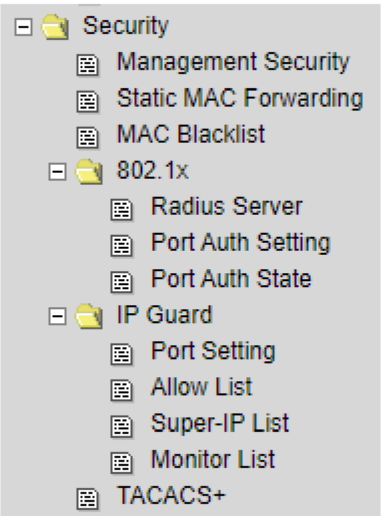


Figure 2: Security menu in Fast Ethernet or Fast Gigabit switches

Security menu in Full Gigabit switches

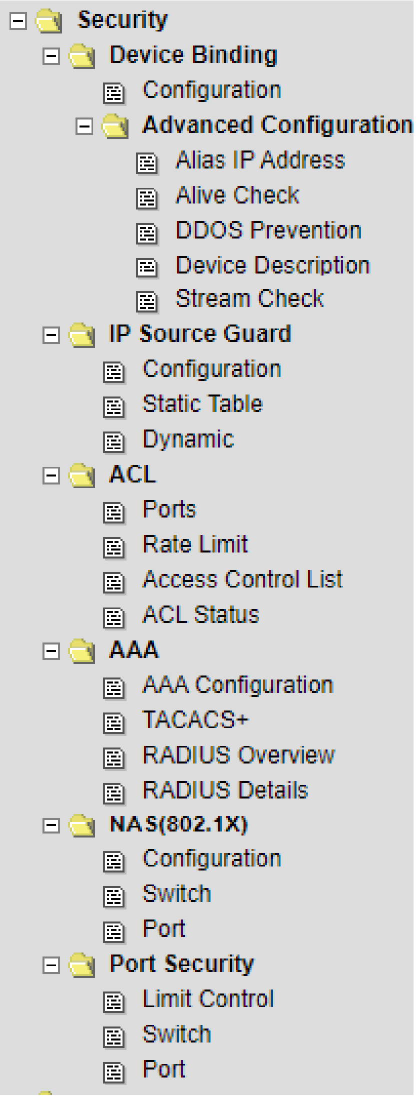


Figure 3: Security menu in Full Gigabit switches

This application note focuses on the main security features of the Lite Managed and Fast/Gigabit switches because these models are the ones, that are used in the Training Kit. Anyway, the most differentiating features of the Full Gigabit switches will also be briefly described in the last section of this application note (Additional security features in Full Gigabit models).

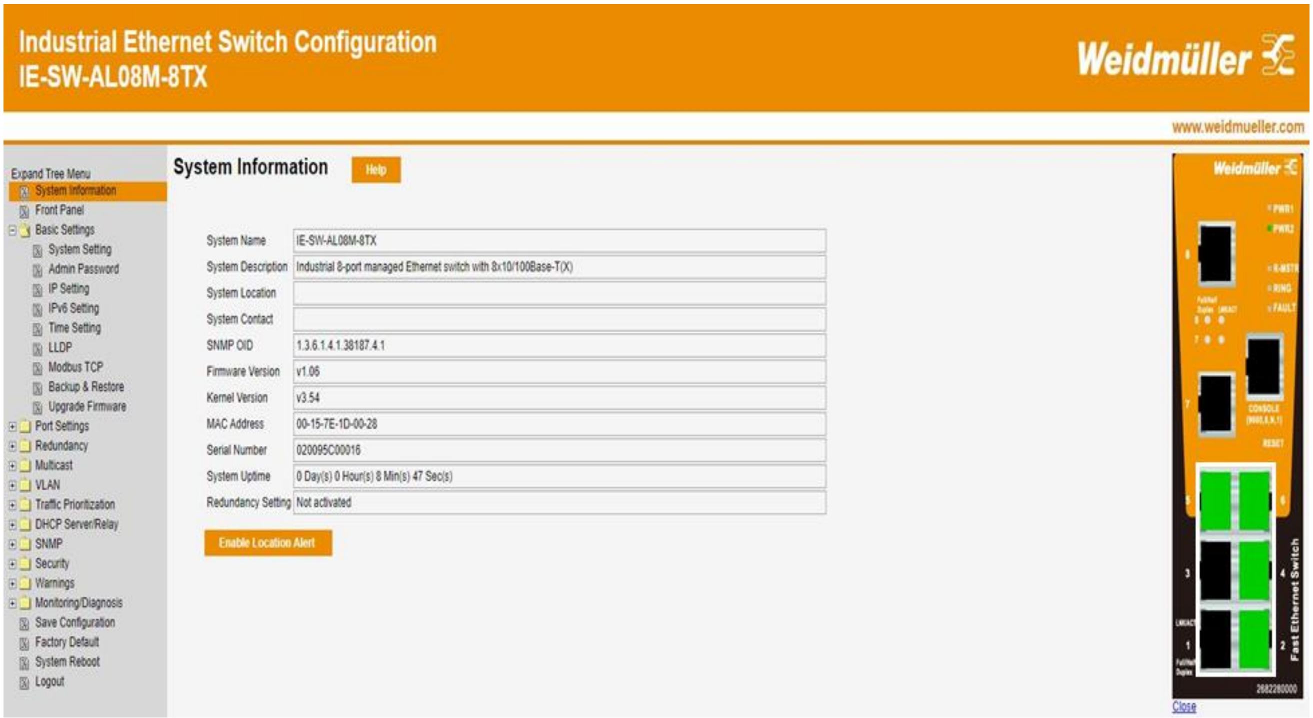
4 Security in Port Access level

4.1 Disable unused ports

One of the simplest security actions that can be programmed in a switch is to disable the unused ports. Then we can be sure that nobody “unknown/unauthorized” will use the free ports of a switch to access to our Ethernet network.

This option is available in both IE-SW-AL05M-5TX (Lite Managed) and IE-SW-AL08M-8TX (Fast Ethernet) models of the Training Kit.

The example below shows an 8-port Ethernet switch with 4 ports used (2, 4, 5 and 6).

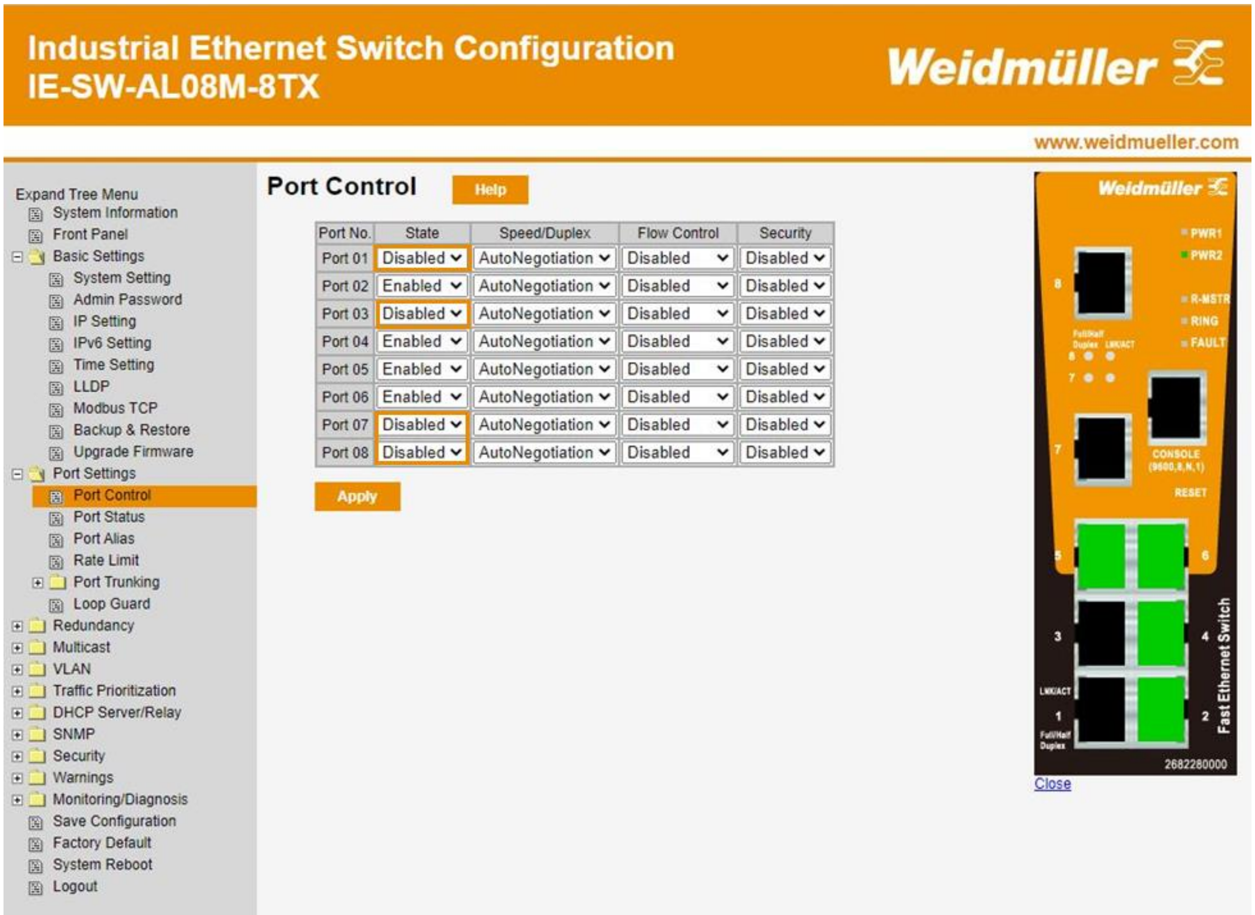


System Information

System Name	IE-SW-AL08M-8TX
System Description	Industrial 8-port managed Ethernet switch with 8x10/100Base-T(X)
System Location	
System Contact	
SNMP OID	1.3.6.1.4.1.38187.4.1
Firmware Version	v1.06
Kernel Version	v3.54
MAC Address	00-15-7E-1D-00-28
Serial Number	020095C00016
System Uptime	0 Day(s) 0 Hour(s) 8 Min(s) 47 Sec(s)
Redundancy Setting	Not activated

Figure 4: 8-port Ethernet switch

In the Menu "*Port Settings*" – Option "*Port Control*", disable the ports not used (in our case: 1, 3, 7 and 8).



Port Control

Port No.	State	Speed/Duplex	Flow Control	Security
Port 01	Disabled	AutoNegotiation	Disabled	Disabled
Port 02	Enabled	AutoNegotiation	Disabled	Disabled
Port 03	Disabled	AutoNegotiation	Disabled	Disabled
Port 04	Enabled	AutoNegotiation	Disabled	Disabled
Port 05	Enabled	AutoNegotiation	Disabled	Disabled
Port 06	Enabled	AutoNegotiation	Disabled	Disabled
Port 07	Disabled	AutoNegotiation	Disabled	Disabled
Port 08	Disabled	AutoNegotiation	Disabled	Disabled

Figure 5: Disable unused ports

Then Apply those changes in the switch. If you want to permanently save this change (Flash memory), use the "*Save Configuration*" option in the menu tree. Otherwise, this configuration change will be lost in the next switch reboot.

We can now connect any device to any of the disabled ports and we will see that it is not detected by the switch (no link – no access to network).

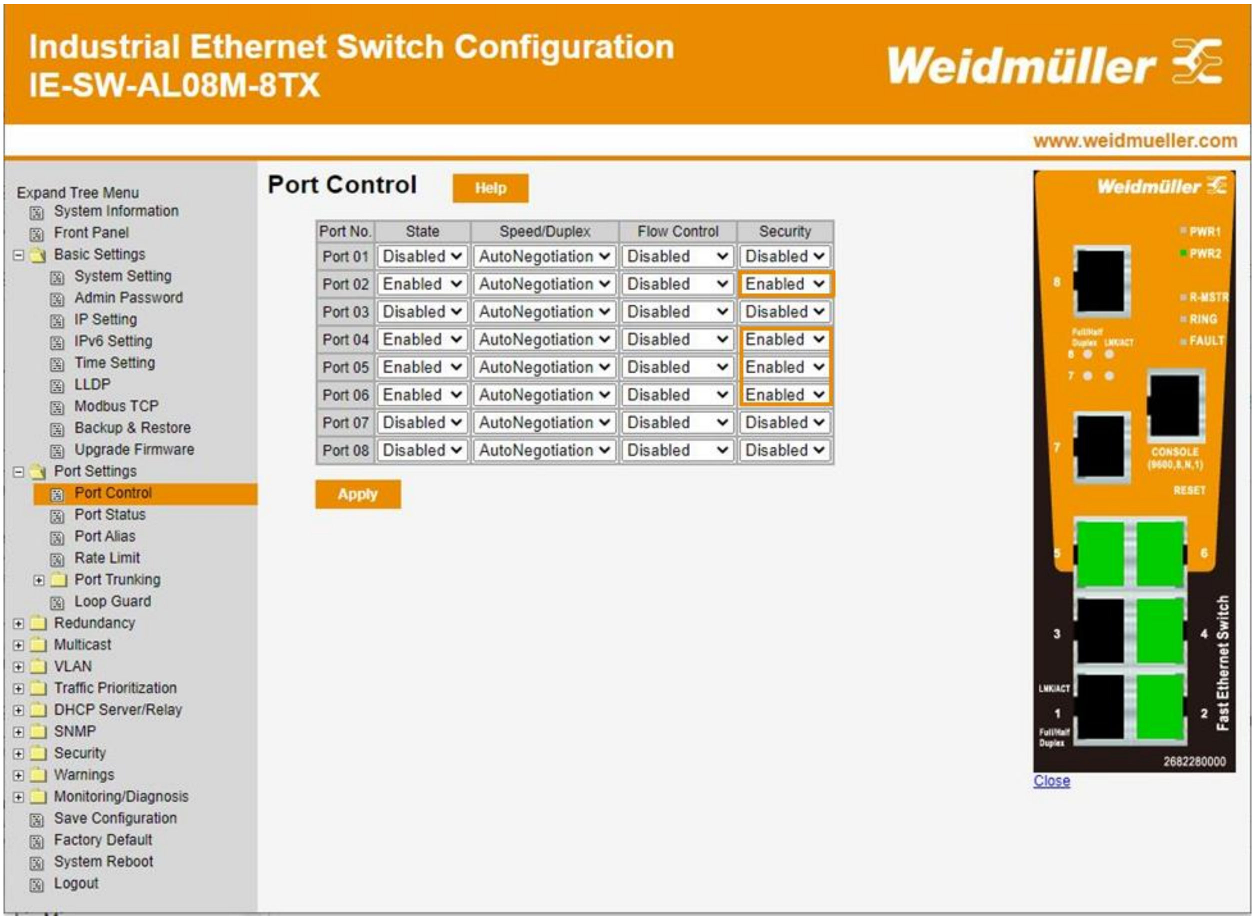
4.2 Define authorized devices (MAC addresses)

By disabling unused ports, we can be sure that free ports will never be used by “unknown / unauthorized” devices to access the network. However, it is still possible that somebody could replace an “authorized” connected device by an “unknown / unauthorized” device in the same enabled port. How can we prevent this?

The option “*Static MAC Forwarding*” allows the user to link the unique MAC address of any device to any specific port of the switch. The switch will never accept traffic from a different MAC address (a different device).

This option is NOT available in the Lite Managed models (IE-SW-AL05M-5TX of the Training Kit)

To program the “*Static MAC Forwarding*” option we first have to enable security in that port through the option “*Port Control*” (menu “*Port Settings*”). In the example below, we enable security in ports 2, 4, 5 and 6 (ports with a connected device).


Industrial Ethernet Switch Configuration
IE-SW-AL08M-8TX

Port Control

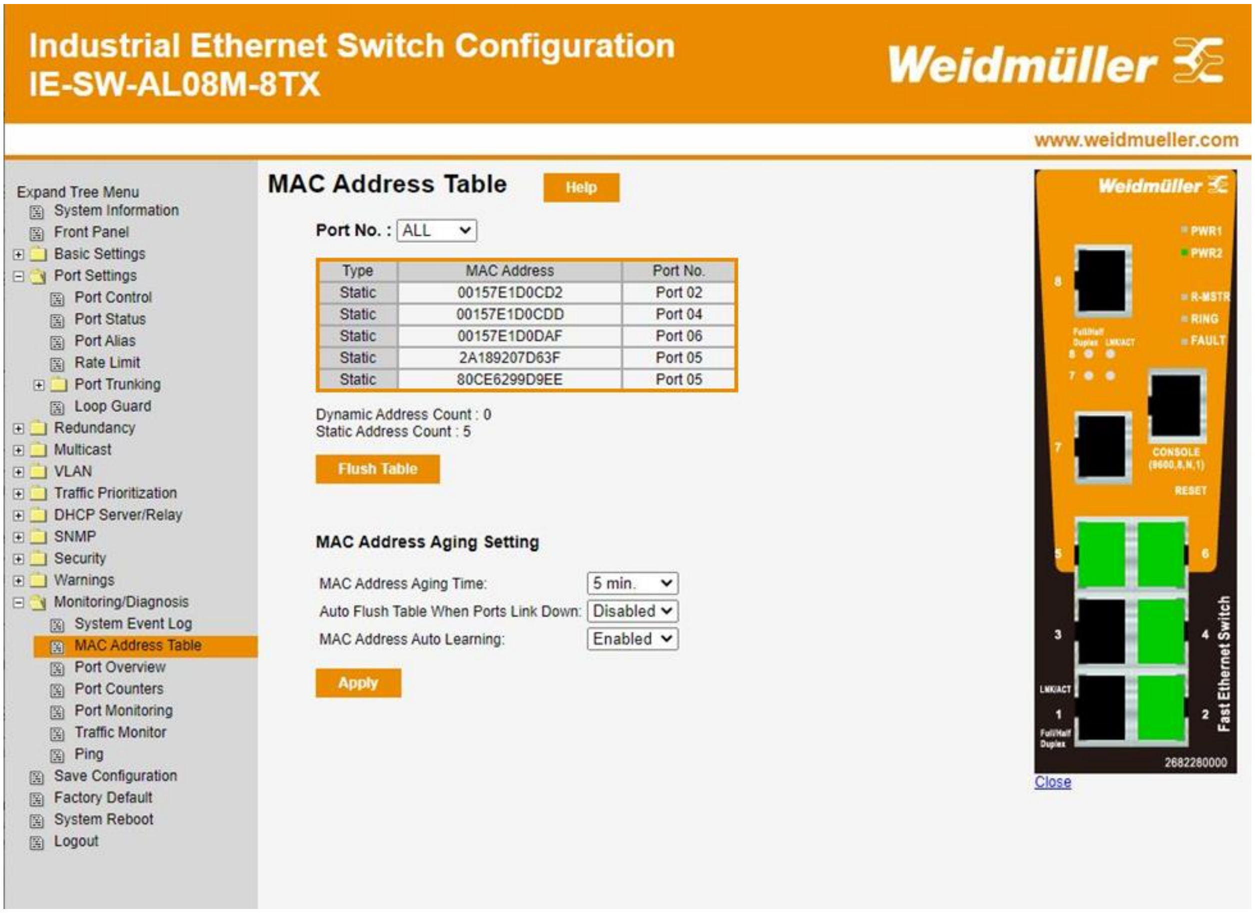
Port No.	State	Speed/Duplex	Flow Control	Security
Port 01	Disabled	AutoNegotiation	Disabled	Disabled
Port 02	Enabled	AutoNegotiation	Disabled	Enabled
Port 03	Disabled	AutoNegotiation	Disabled	Disabled
Port 04	Enabled	AutoNegotiation	Disabled	Enabled
Port 05	Enabled	AutoNegotiation	Disabled	Enabled
Port 06	Enabled	AutoNegotiation	Disabled	Enabled
Port 07	Disabled	AutoNegotiation	Disabled	Disabled
Port 08	Disabled	AutoNegotiation	Disabled	Disabled

Figure 6: Enable security in ports

In order to program the “*Static MAC Forwarding*” feature we need to know the MAC addresses of the connected devices. An easy way to get this information is through the option “*MAC Address Table*” of the “*Monitoring/Diagnosis*” menu. This option will show the different MAC addresses identified by the switch.

It may be necessary to generate some traffic between the connected devices (e.g.: using *ping* command) to learn their MAC addresses in the switch.

Below we can see the MAC address table of the 8-port switch used for this Application Note.



MAC Address Table

Port No. : ALL

Type	MAC Address	Port No.
Static	00157E1D0CD2	Port 02
Static	00157E1D0CDD	Port 04
Static	00157E1D0DAF	Port 06
Static	2A189207D63F	Port 05
Static	80CE6299D9EE	Port 05

Dynamic Address Count : 0
Static Address Count : 5

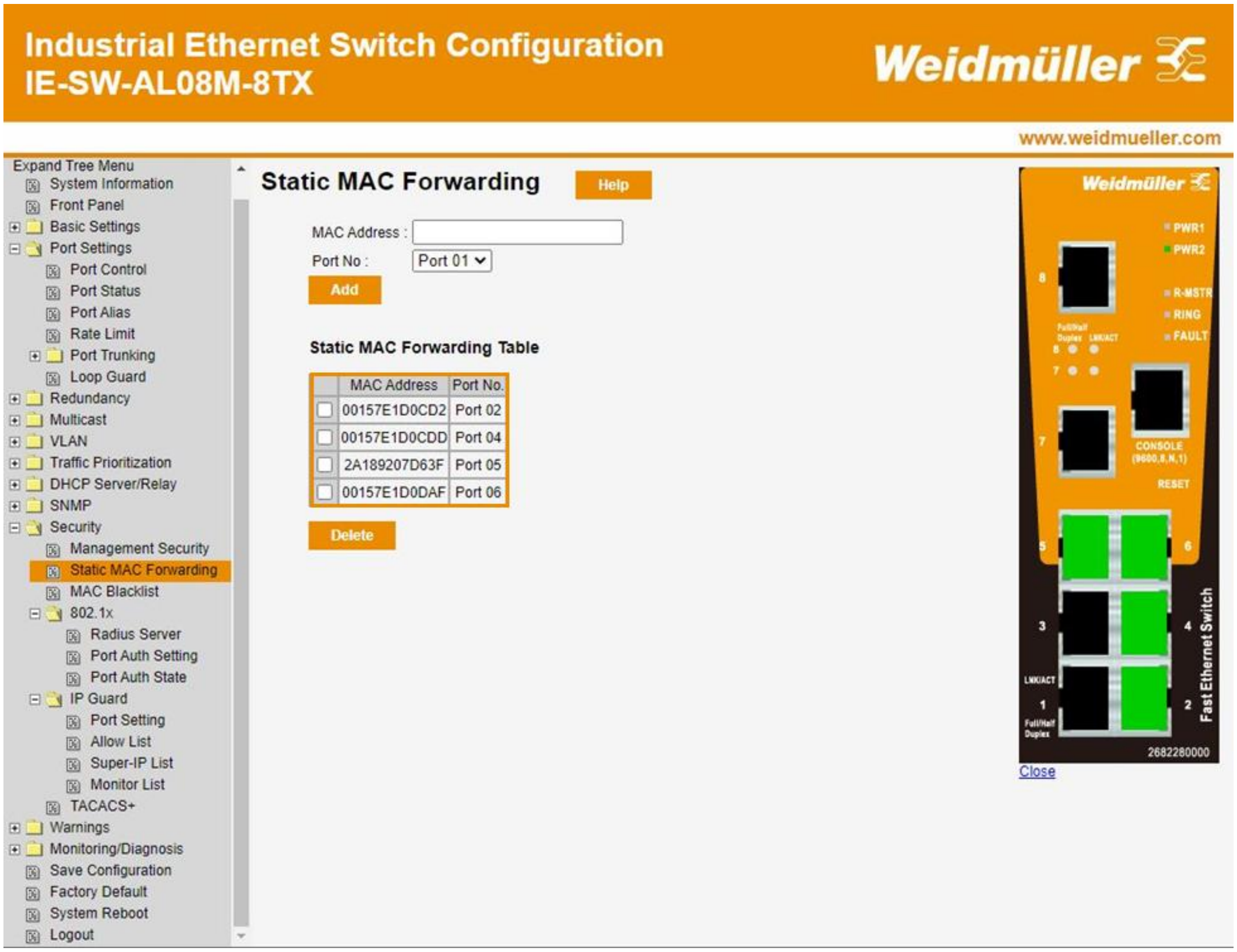
MAC Address Aging Setting

MAC Address Aging Time: 5 min.
Auto Flush Table When Ports Link Down: Disabled
MAC Address Auto Learning: Enabled

Figure 7: MAC Address table of the switch

As we can see above, the switch has learnt four different MAC addresses in the ports 2, 4, 5 and 6. Our port number 5 shows two different MAC-Addresses. This is caused by the router redirecting the traffic to the computer. You can tell that this is your end device by comparing the first 6 digits of the MAC Address. All Weidmüller products in the kit start with the following string of characters: “*00157E*” (note: the router has two different MAC-Addresses for its LAN and WAN network interfaces which is why the router may have a different MAC address string, like in our example).

Assuming that this is our working environment, we are going to set that these MAC addresses are the only ones allowed for these ports using the “*Static MAC Forwarding*” function.



Static MAC Forwarding

MAC Address :

Port No : Port 01

Static MAC Forwarding Table

	MAC Address	Port No.
□	00157E1D0CD2	Port 02
□	00157E1D0CDD	Port 04
□	2A189207D63F	Port 05
□	00157E1D0DAF	Port 06

Figure 8: Static MAC Forwarding Table

We enter the MAC addresses in the “*MAC Address*” field one by one and select the corresponding port number in the drop-down menu (we can copy the addresses from the MAC Address table) and then press the button “*Add*”.

Now we can check that our network is really robust in terms of security.

- When executing a ping command from the switch or a recognized end device we will see that all pings work perfectly fine within the defined static MAC address table

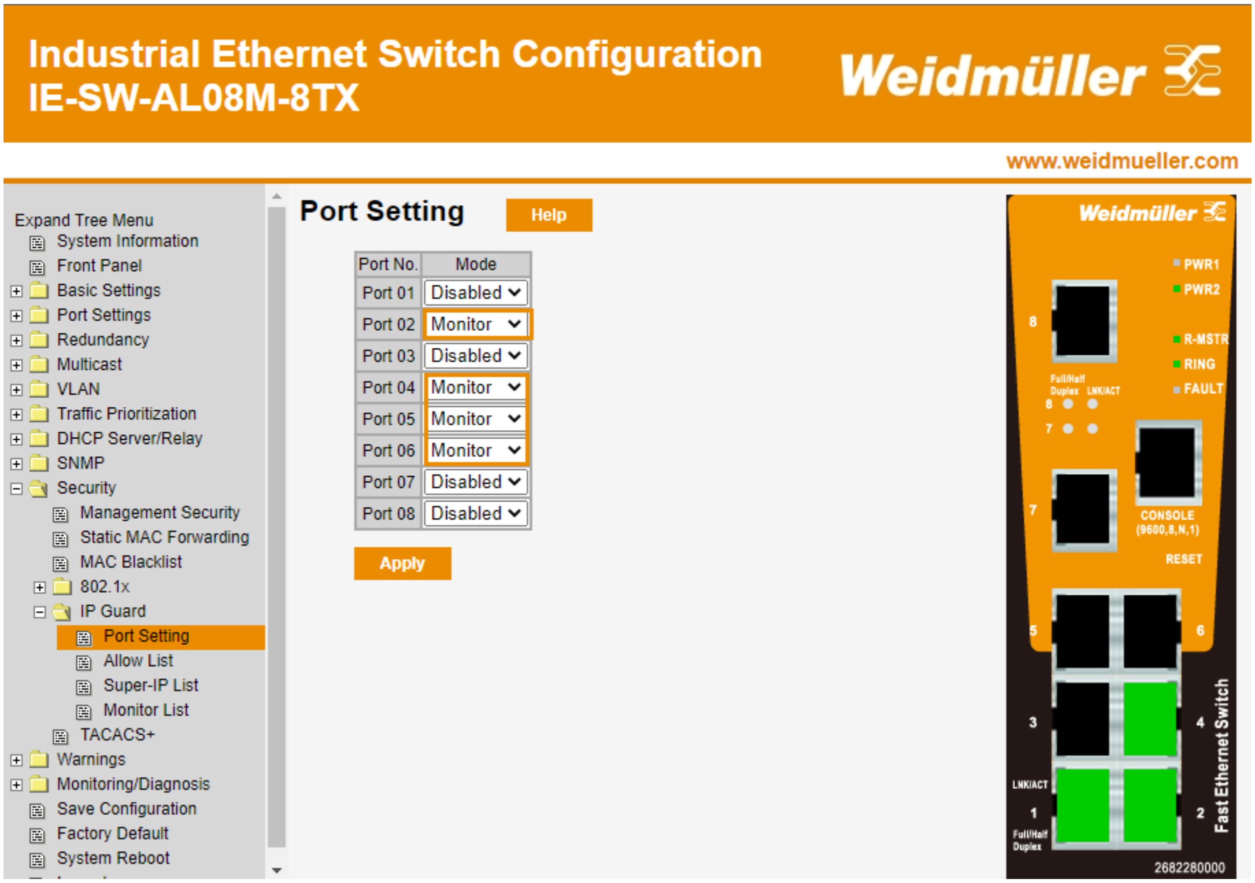
- If we replace any cable of the connected devices and execute the ping commands again we will see that the requests do not arrive when the port and the MAC address static definition do not match(the switch discards the frames)

4.3 Define authorized devices (IP guard)

The option “*Static MAC Forwarding*” described in the previous section is the most recommended one to control/limit the specific devices that can be connected to a switch in small networks because all the MAC addresses have to be introduced manually.
If we have a big network with many devices and we do not want to introduce all the allowed MAC addresses one by one, we can use the IP guard function. This function is quite similar in terms of security results because it also links physical ports of the switch with specific IP/MAC addresses of devices. If we are using the IP guard, we do not need to use the “*Static MAC forwarding*”.

The IP guard function is NOT available in the Lite Managed models (IE-SW-AL05M-5TX of the Training Kit)

As with this function we want to avoid entering the authorized devices manually, our first step has to be to detect all the connected devices of the network. To do so, go to the option “*IP Guard - Port Setting*” of the Security menu, we set the ports with connected devices in “*Monitor*” mode and press the “*Apply*” button.



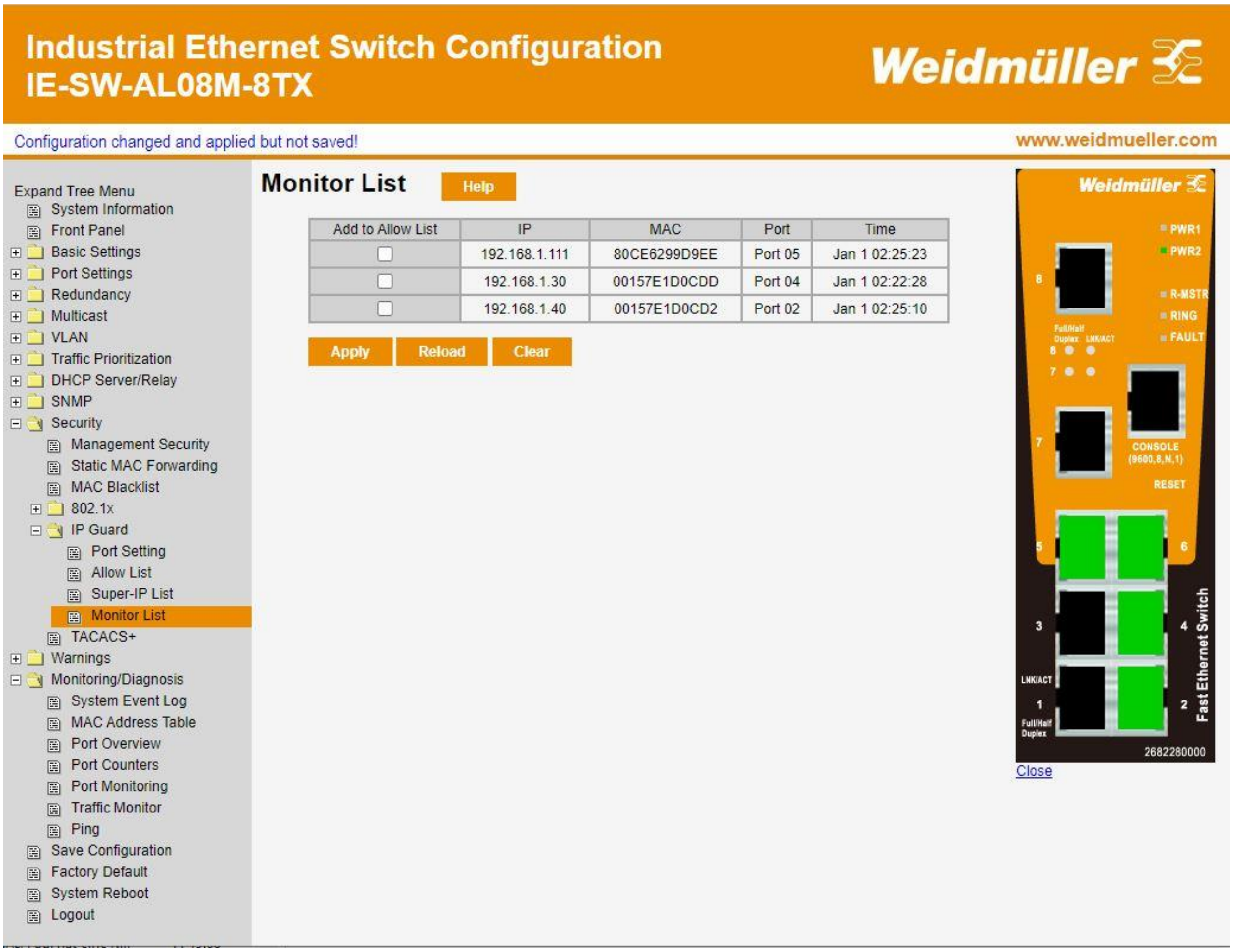
Port Setting

Port No.	Mode
Port 01	Disabled
Port 02	Monitor
Port 03	Disabled
Port 04	Monitor
Port 05	Monitor
Port 06	Monitor
Port 07	Disabled
Port 08	Disabled

Figure 9: Enabling Monitor option for the ports

Clicking the option “*IP- Guard – Monitor List*” shows an automatically generated table with the connected devices for each port.

The IP guard function is monitoring IP traffic so it may take time to display the complete list of devices of the network in the “*Monitor List*”. Generating IP traffic between devices may speed up this process of detecting all the connected devices (ex: switch as NTP server and connected devices as SNTP clients).



Industrial Ethernet Switch Configuration
IE-SW-AL08M-8TX

Configuration changed and applied but not saved!

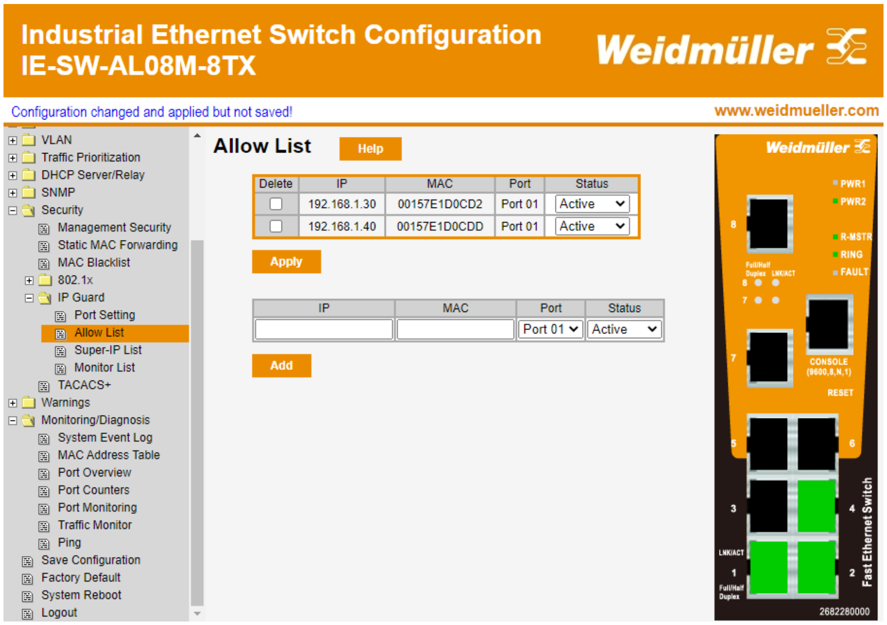
Monitor List

Add to Allow List	IP	MAC	Port	Time
□	192.168.1.111	80CE6299D9EE	Port 05	Jan 1 02:25:23
□	192.168.1.30	00157E1D0CDD	Port 04	Jan 1 02:22:28
□	192.168.1.40	00157E1D0CD2	Port 02	Jan 1 02:25:10

Figure 10: Monitoring list

The devices displayed in the Monitor List can be directly included in the Allow List by just clicking the checkbox and then pressing the button “*Apply*”.

After this action is done, the devices are not shown any longer in the Monitor List and we can see them in the option “*IP Guard – Allow List*”. The option “*Allow List*” also makes it possible to manually add any device to the list if you know its IP - and MAC-Address.



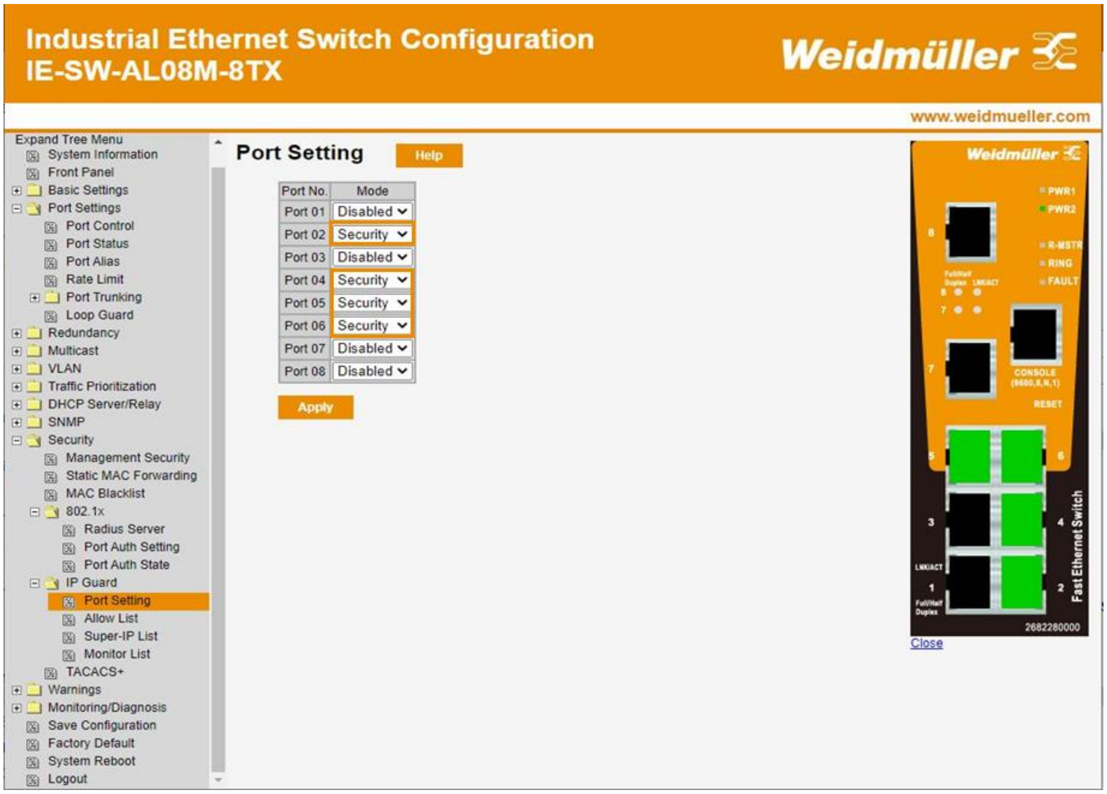
Allow List

Delete	IP	MAC	Port	Status
☐	192.168.1.30	00157E1D0CD2	Port 01	Active
☐	192.168.1.40	00157E1D0CDD	Port 01	Active

IP	MAC	Port	Status
		Port 01	Active

Figure 11: Allowed List

Once we have the Allow List table according to our preferences with all the known/authorized devices in the expected ports, we will go to the option "IP Guard - Port Setting" again. From there set the ports with connected devices to "Security" mode and then click on "Apply".



Port Setting

Port No.	Mode
Port 01	Disabled
Port 02	Security
Port 03	Disabled
Port 04	Security
Port 05	Security
Port 06	Security
Port 07	Disabled
Port 08	Disabled

Figure 12: Changing port Settings from Monitoring to Security

Now we can confirm that our network is really robust in terms of security.

- Executing ping commands from the switch or from the end devices we will see that all are perfectly received according to the Allow List table
- If we replace any cable of the connected devices and execute the ping commands again, we will see that the pings are not received when there is no match between the port and the IP/MAC address according to the table

4.4 External port authentication (IEEE 802.1X standard and RADIUS)

IEEE (Institute of Electrical and Electronics Engineering) 802.1X is a standard to control the port access of a LAN and requires three main elements:

- Supplicant: End device (client) connected to the switch that wants to access the Local Area Network
- Authentication server: The server that performs the authentication of the supplicant. In our case, it is a RADIUS (Remote Authentication Dial-In User Service) server (most common one for IEEE 802.1X). The customer has to take care of this
- Authenticator: The switch takes this role and is the device between the supplicant and the authentication server

Any supplicant (device) will have access to the network through the switch only after the successful authentication of that device in the RADIUS server. More information can be found in the user manual of the Advanced Line switches.

This 802.1X authentication will usually only be used on customer’s demand and mainly requires the setting of the RADIUS server in the switch (Menu “*802.1x*”).

The IEEE 802.1X authentication is NOT available in the Lite Managed models (IE-SW-AL05M-5TX of the Training Kit)

5 Security in accessing the Switch’s Management

The Advanced Line switches can be managed via web browser, the Simple Network Management Protocol (SNMP) or Command Line Interface (CLI).

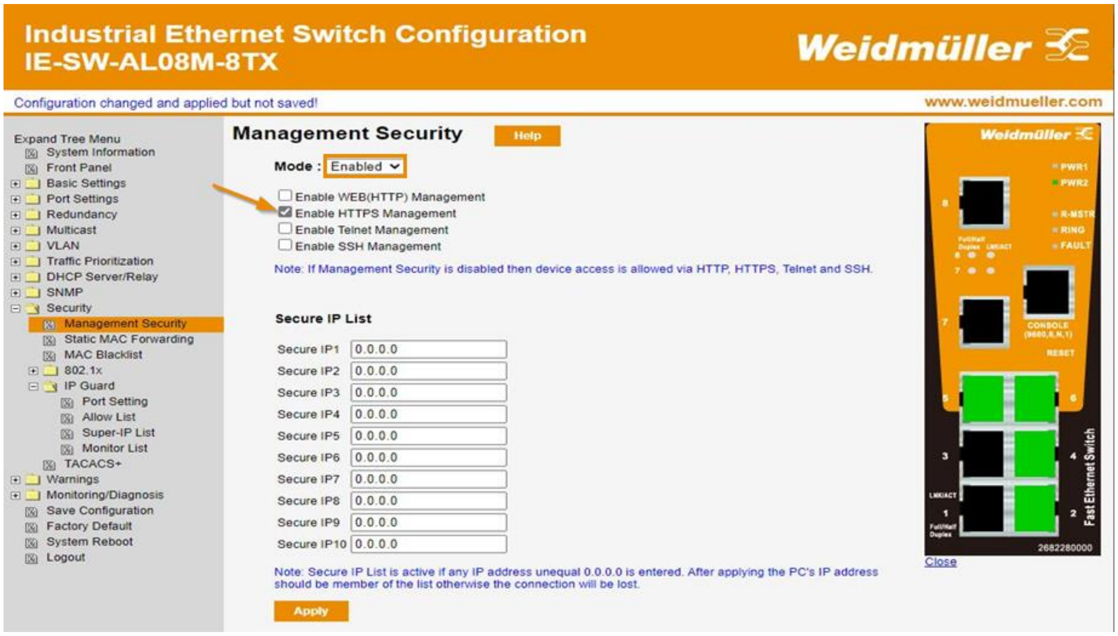
In this chapter we will focus on security for access through web browser or Command Line Interface. SNMP can be easily enabled or disabled from the “*SNMP*” menu and in terms of security, it is always recommended to use SNMPv3 as it provides user authentications security measurements.

➡ The security options to control access to the Switch’s management are available in both IE-SW-AL05M-5TX (Lite Managed) and IE-SW-AL08M-8TX (Fast Ethernet) models of the Training Kit. However, it has to be considered that the Lite Managed models don’t have serial port so the access to CLI can only be made through Telnet or SSH (not through Console).

5.1 Authorized access method

We can easily program that only secure access to the switch is permitted (https for web browser and SSH for Command Line Interface). Moreover, we can also define a list of authorized IP addresses for the management computer.

If we want to block the possibility of access to the switch using any non-secure protocol like “*HTTP*”, we have to go to the option “*Management Security*” of the Security menu. Once we enable the mode of Management Security, we can check or uncheck the allowed access methods to the Ethernet switch. By checking only “*Enable HTTPS Management*” and pressing the button “*Apply*” we will ensure that the access to the switch is only possible through the web server (not CLI) and only with a secure https connection.



Industrial Ethernet Switch Configuration
IE-SW-AL08M-8TX

Configuration changed and applied but not saved!

Management Security

Mode : Enabled

- ☐ Enable WEB(HTTP) Management
- ☑ Enable HTTPS Management
- ☐ Enable Telnet Management
- ☐ Enable SSH Management

Note: If Management Security is disabled then device access is allowed via HTTP, HTTPS, Telnet and SSH.

Secure IP List

Secure IP1	0.0.0.0
Secure IP2	0.0.0.0
Secure IP3	0.0.0.0
Secure IP4	0.0.0.0
Secure IP5	0.0.0.0
Secure IP6	0.0.0.0
Secure IP7	0.0.0.0
Secure IP8	0.0.0.0
Secure IP9	0.0.0.0
Secure IP10	0.0.0.0

Note: Secure IP List is active if any IP address unequal 0.0.0.0 is entered. After applying the PC's IP address should be member of the list otherwise the connection will be lost.

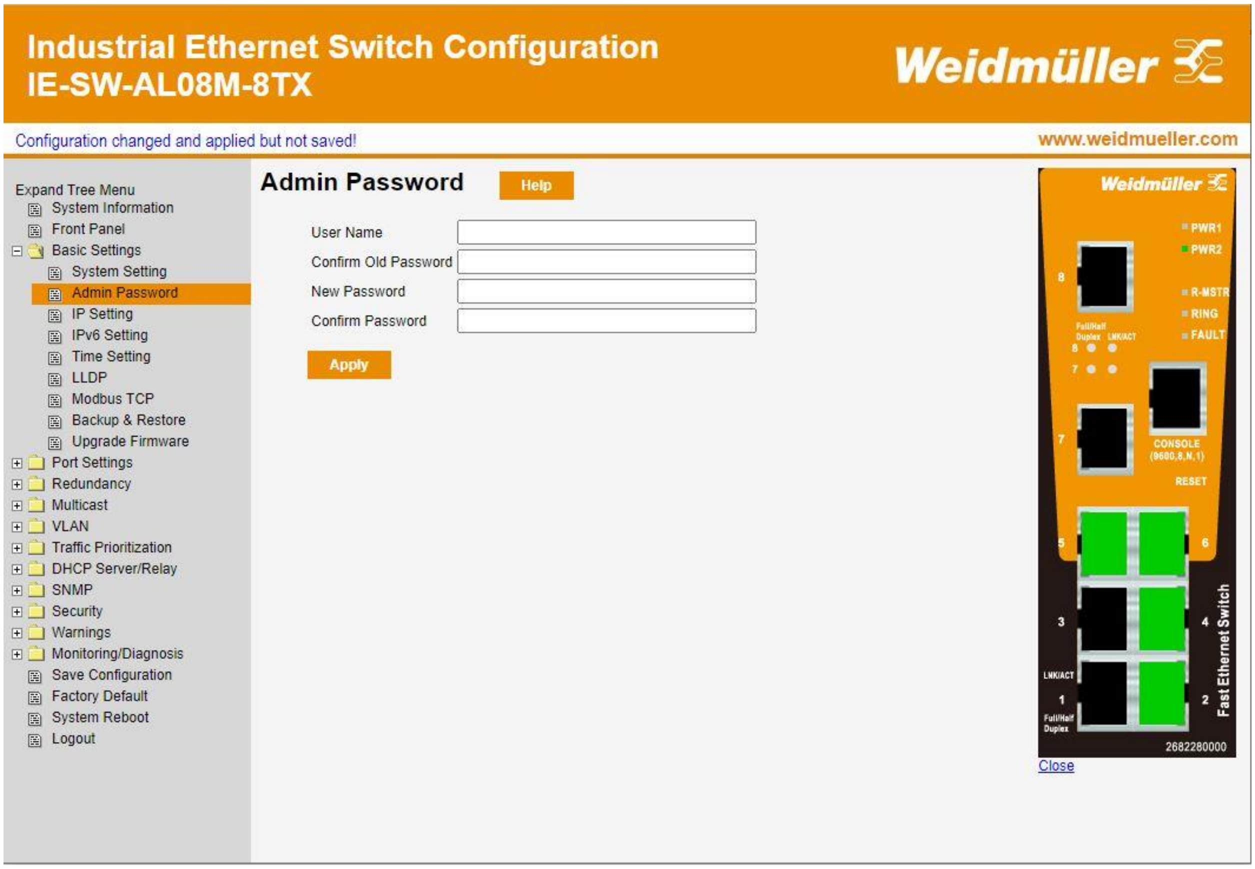
Figure 13: Enable HTTPS Management

In fact, after clicking Apply we can no longer access the switch if we previously used a standard http connection.
Afterwards we should close the web browser, open it again and check that just typing the switch's IP address in the Address or URL field of the browser is not working anymore (we receive a message that is not possible to access to the site).

To access the web interface, enter "***https://<Switch's IP address>***" in the address field and press "*Enter*". A warning message will pop out to warn us that the security certificate was issued by a company they have not chosen to trust.
As we (and the customer) know that the certificate is issued by Weidmüller, we can select "***Continue to this website*"** and we will access the switch's web interface secured via HTTPS.

5.2 Access through TACACS+

The switch has a login and password that is locally stored. By default, the login is "admin" and the password is "Detmold" as stated in Application Note 01 and in the manual, but both parameters should be changed in the option "*Admin Password*" of the "*Basic Settings*" menu as seen below.



Industrial Ethernet Switch Configuration
IE-SW-AL08M-8TX

Configuration changed and applied but not saved!

Admin Password

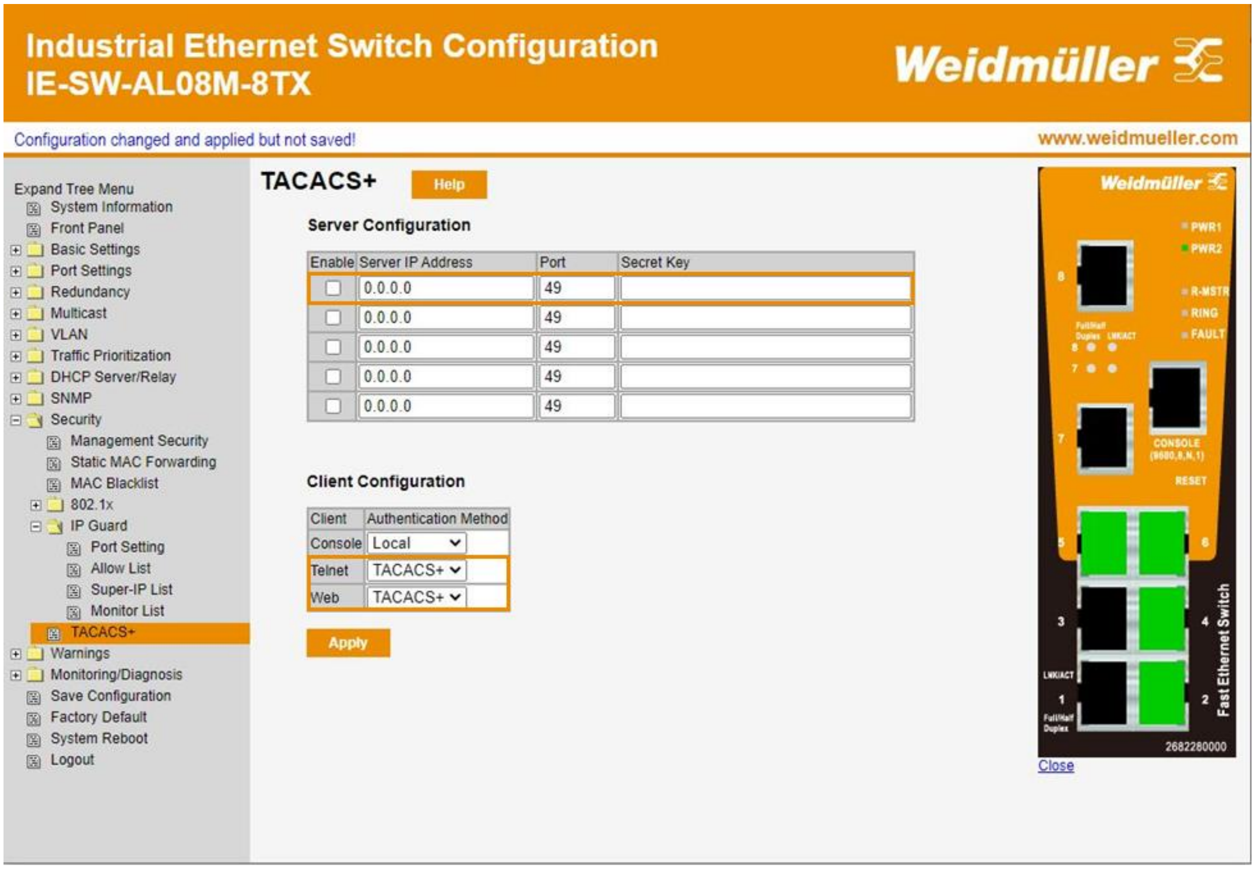
User Name
Confirm Old Password
New Password
Confirm Password

Figure 14: Changing Password

But what happens if a customer wants to have multiple user accounts and wants to provide different privileges for different users or track all changes made by the users?

This can be achieved through an external AAA (Authentication, Authorization, Accounting) server of type TACACS+ (Terminal Access Controller Access Control System). The switch will match all access requests from a client with the AAA server and will permit or deny access depending on information provided by the AAA server.

In the switch we need to define if we want the authentication method to be local or by a TACACS+ server. In case of TACACS+, its main parameters have to be entered in the configuration shown below. Note, that if you want to use a AAA server, the server has to be hosted and managed by yourself.
Afterwards, the main parameters of the AAA server would need to be entered into the switch. This includes for example the IP address, the port and the secret key. For ack-up purposes, up to five different TACACS+ server can be configured in the switch.



Configuration changed and applied but not saved!

TACACS+

Server Configuration

Enable	Server IP Address	Port	Secret Key
☐	0.0.0.0	49	
☐	0.0.0.0	49	
☐	0.0.0.0	49	
☐	0.0.0.0	49	
☐	0.0.0.0	49	

Client Configuration

Client	Authentication Method
Console	Local
Telnet	TACACS+
Web	TACACS+

Figure 15: Distributing rights for different user

6 Additional security features in Full Gigabit switches

As it has been indicated in section 2, the Full Gigabit switches of the Advanced Line have more security features than the switches that can be found on the Training Kit.

The most differentiating additional features are:

- **Creation of different users with different profiles locally:** The switches available on the Training Kit can only have one local user/password. It means, if the customer wants to have different login/password for users and/or different privileges it is mandatory to use an external authentication TACACS+ server. The Full Gigabit models provide the possibility to create several different users with different privileges in the local database of the switch.

- **Access Control Lists:** The switches available in the Training Kit can limit access to the network based on MAC and IP address. However, it is not possible to analyze the frames and block access based on it as Firewalls are usually doing. The Access Control List is available in the Full Gigabit models to allow the user to deny or permit frames based on specific Ethernet / ARP / IP / TCP / UDP parameters.

7 Results

In this Application Note we have learned how to disable unused ports, restrict the access via MAC- and IP addresses and also how to restrict access with external port authentication.
Moreover, we learned how to restrict access to the switch to accesses secured via https, how to use multiple users each with different rights with the help of a TACACS+ Server and explained the main differences between the Weidmueller switch models.

8 List of Figures