Atop Technologies, Inc.

Industrial Managed Ethernet Switch

User Manual

V0.1

April 18th, 2022

Series covered by this manual:
EH3408ls, EH3408lu, EH3408s, EH3408u,

*** The user interface on these products may be slightly different from the one shown on this user manual**

This PDF Document contains internal hyperlinks for ease of navigation.
For example, click on any item listed in the Table of Contents to go to that page.

Published by:

Atop Technologies, Inc.

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Chupei City, Hsinchu County
Taiwan, R.O.C.

Tel: +886-3-550-8137
Fax: +886-3-550-8131
www.atoponline.com

Important Announcement

Disclaimer

We have checked the contents of this manual for agreement with the hardware and the software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual is reviewed regularly and any necessary corrections will be included in subsequent editions.
Suggestions for improvement are welcome. All other product's names referenced herein are registered trademarks of their respective companies.

Preface

This manual contains some advanced network management knowledge, instructions, examples, guidelines, and general theories. The contents are designed to help users manage the switch and use its software, a background in general theory is a must, when reading it. Please refer to the Glossary for technical terms and abbreviations.

Who Should Use This User Manual

This manual is to be used by qualified network personnel or support technicians who are familiar with network operations, and might be useful for system programmers or network planners as well. This manual also provides helpful and handy information for first time users. For any related problems, please contact your local distributor. If they are unable to assist you, please redirect your inquiries to www.atoponline.com .

Warranty Period

Atop technology provides a limited 5-year warranty for managed Ethernet switches.

Documentation Control

Author:	**Saowanee Saewong**
Revision:	**0.1**
Revision History:	**Initial**
Creation Date:	**17 December 2021**
Last Revision Date:	**17 April 2022**
Product Reference:	**Industrial Lite-managed Switch**
Document Status:	**Released**

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Introduction to Industrial Managed Switch

Atop's EH (Ethernet Switching Hub) 3408 series are product lines of cost-effective switch for industrial networking where simple managing is required. This lite-managed switch provides key features that most users need without those unnecessary features. The device's easy web configuration includes functions like SNMP, warning realy-out, Syslog and a user-friendly web GUI, which is especially useful when creating a compatible network for industry 4.0 automation equipment, setting up Quality of Service (QoS) and Virtual Local Area Network (VLAN) to run industrial protocols such as Profinet and Ethernet/IP. Furthermore, multiple account levels allow optimal management with different users accessing different operations.

All these features are packed in a slim and sturdy enclosure that fits in cabinets with limited space, while protecting against environmental hazards according to CE, FCC and UL standards. Two operation ranges are available for your choice: -10 C to +60 C for regular climates and -40 C to +75 C for extreme ones. Cyber protection is not overlooked either. The EH3408 series supports security features based on the IEC62443-4-2 standard. An EH3408 switch comes with either USB or Micro-SD card support so that device configurations can be automatically backed up on a regular basis. In the unlikely event of device failure, simply transfer the USB or SD card to a new device to restore all original configurations.

Note:
Throughout the manual, the symbol * indicates that more detailed information of the subject will be provided at the end of this book or as a footnote.

1.2 Software Features

Atop's industrial lite-managed switches come with a wide range of network protocols and software features. These protocols and software features allow the network administrator to implement security and reliability into their network. These features enable Atop's switches to be used in safety applications, and factory and process automation. The followings are the list of protocols and software features.

- **User Interfaces**
  - **Web browser**
  - **Telnet Console**
  - **Serial Console**
- **Dynamic Host Configuration Protocol (DHCP) Server/Relay/Client with Option 66/67**
- **Time Synchronization**
  - **Network Time Protocol (NTP) Server/Client**
  - **Simplified Network Time Protocol (SNTP)**
- **Quality of Service (QoS) Traffic Regulation**
- **Simple Network Management Protocol (SNMP) v1/v2/v3 (with MD5 Authentication and DES encryption)**
- **Spanning Tree Protocol (STP)/Rapid Spanning Tree Protocol (RSTP**
- **Virtual Local Area Network (VLAN)**
- **IEEE 802.1x / Extensible Authentication Protocol (EAP) / Remote Authentication Dial-In User Service (RADIUS) / Terminal Access Controller Access-Control System (TACACS+)**
- **Alarm System (with E-mail Notification or Relay Output)**

2 Configuring with a Web Browser

Chapter 2 explains how to access the industrial lite-managed switch for the first time. There are three ways to configure this Ethernet Switch:

1. **Web browser**
2. **Telnet console**
3. **Serial console**

The web browser and the telnet console methods allow users to access the switch over the Internet or the Ethernet LAN, while the serial console method requires a serial cable connection between the console and the switch. There are only a few differences among these three methods. Users are recommended to use the web browser method to configure the system because of its user-friendly interface.

2.1 Web-based Management Basics

Users can access the managed switch easily using their web browsers (Internet Explorer 8 or 11, Firefox 44, Chrome 48 or later versions are recommended). We will proceed to use a web browser to introduce the managed switch's functions.

2.1.1 Default Factory Settings

Below is a list of default factory settings. This information will be used during the login process. Make sure that the computer accessing the switch has an IP address in the same subnet and the subnet mask is the same.

IP Address: 10.0.50.1
Subnet Mask: 255.255.0.0
Default Gateway: 0.0.0.0
User Name: admin
Password: default

2.1.2 Login Process and Main Window Interface

Before users can access the configuration, they have to log in. This can simply be done in three steps.

1. **Launch a web browser.**
2. **Type in the switch's IP address (e.g. http://10.0.50.1), as shown in Figure 2.1).**

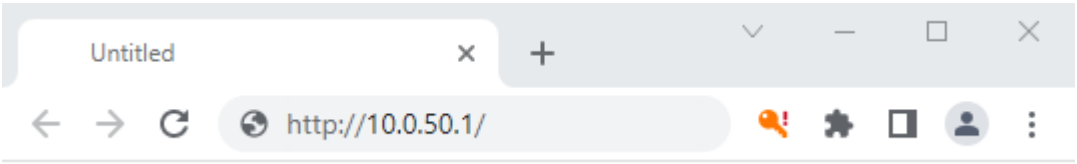


Figure 2.1 IP Address for Web-based Setting

3. **A login prompt will be shown as in Figure 2.2. You can enter the default user name and password given in previous page. Then, click the Login button to login to the web interface.**

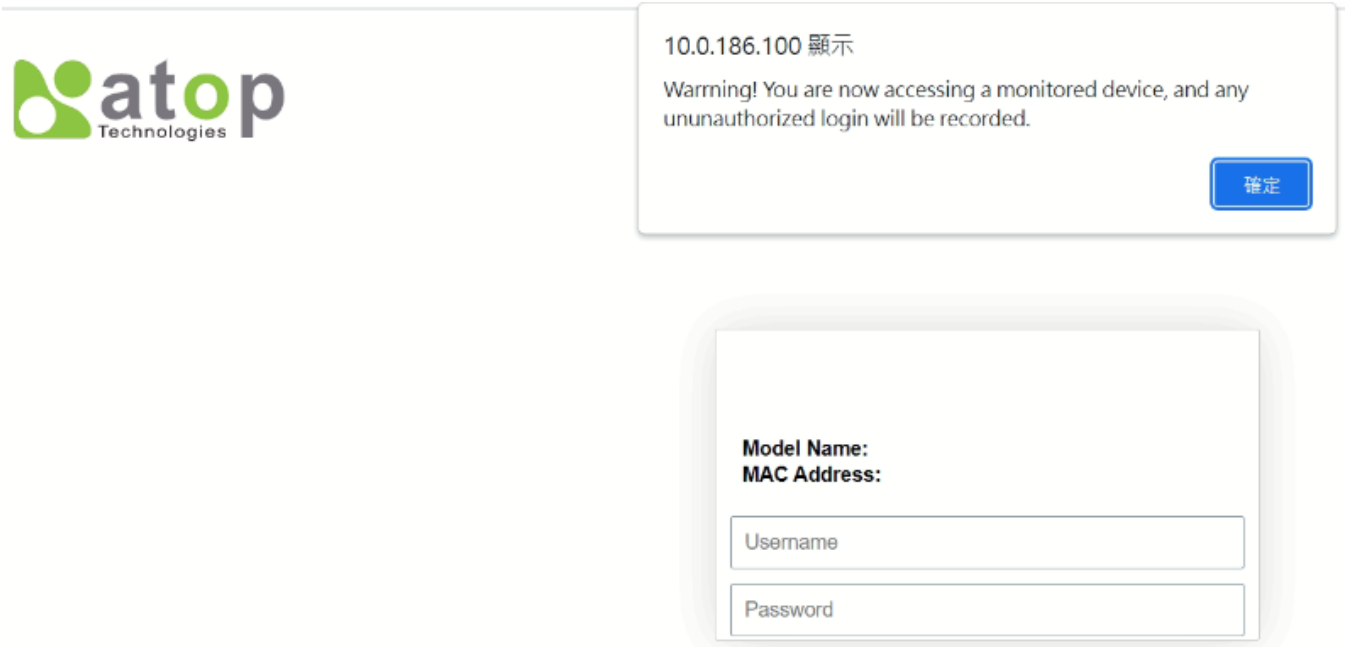


Figure 2.2 Login Prompt

After the login process, the main interface will show up as shown in Figure 2.3. Under the Atop Technologies' Logo, there are basic information about the device which are Model Name, Kernel Version, Firmware Version, Serial Number (SerialNum) and MAC Address. The main configuration menu of the EH3408 series is listed as the group of green circular icons called function bar under the basic information of the device. Each configuration web page can be accessed by clicking on corresponding circular icon of the function bar. The user can move the pointer of the mouse on top of particular circular icon to see the tooltip that indicates the name of the icon.

Figure 2.3 Default Web Interface for EH3408-SD

The function bar on the top of the web GUI is shown in Figure 2.4. There are 8 functions in the bar from the left side to the right side which are functions to manage Information, Configuration, Diaganostic, Security, RSTP, Management, Maintetance, and Logout. Note that there is a picture of the front panel of the EH3408 device on the left side of the screen under the function bar. This front panel of the manage switch display the LEDs of power, fault, port link status, etc. Note that in this case the Port 4 is highlighted in green, indicating that the port is being connected. Detailed explanations of each function icon will be addressed later as necessary.

Figure 2.4 Function Bar on Top of Web GUI

2.2 Information

To help users become familiar with the device, the Information function icon denoted by question mark provides important details of the managed switch. This is also the main welcome screen once the user has logged in. The details make it easier to identify different switches connected to the network. The information web page is separated into three boxes or features called Information, Connection and Log as shown in Figure 2.5. Each feature usually includes a gear icon next to the feature's name. This gear for particular feature can be used to bring up a pop-up window for managing configuration of that particular feature.

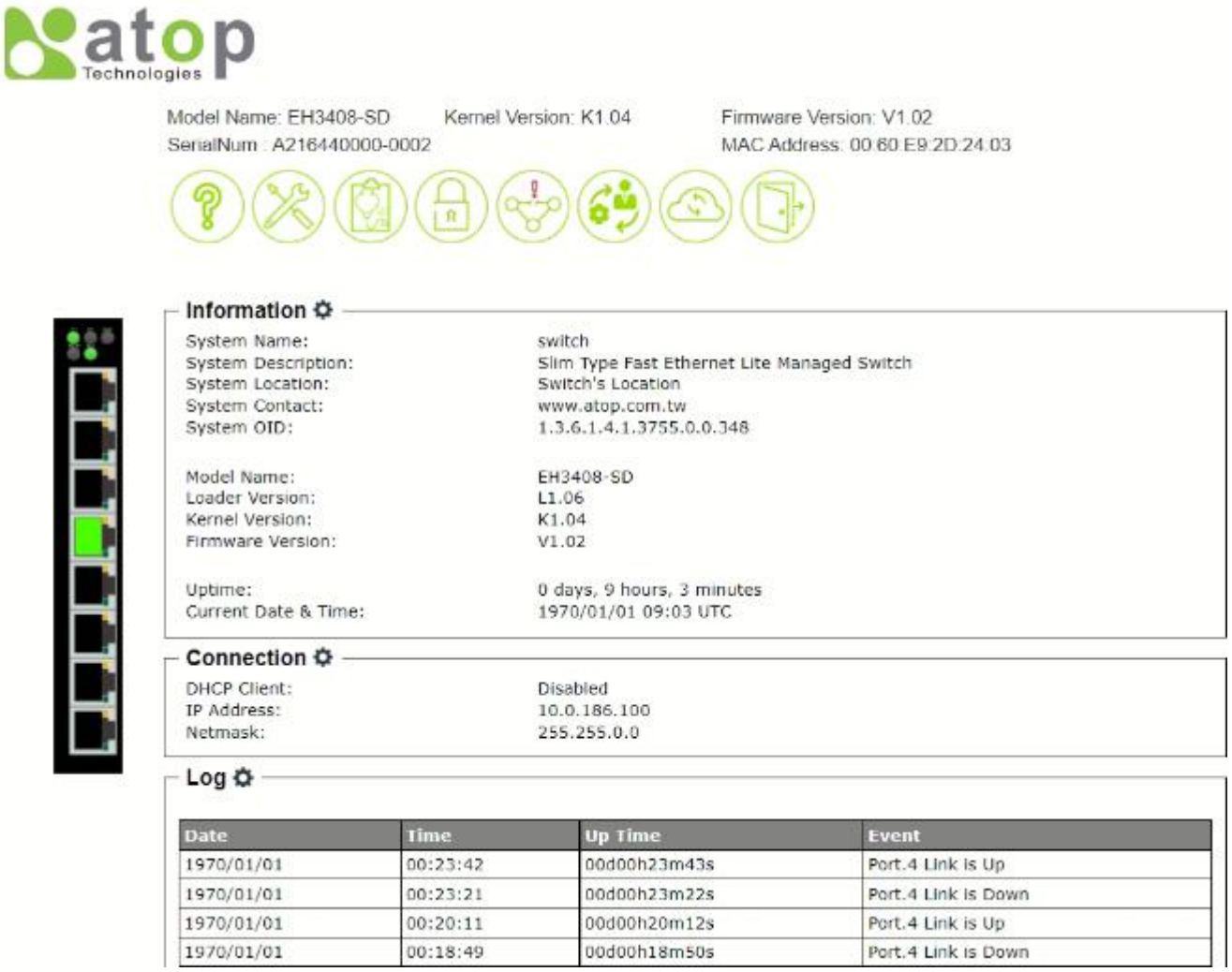


Figure 2.5 Information Function

2.2.1 Information feature

This feature provides basic system information of Atop's industrial managed switch. The user can check the device description which includes System Name, System Description, System Location, System Contact, and System OID as shown in Figure 2.6. Additionally, the Model Name, Loader Version, Kernel Version, and Firmware Version are listed. Note that Atop's firmware generally consists of kernel version and firmware version. At the bottom of this section, the Uptime and the Current Date & Time of the device are displayed. Table 2.1 summarizes the description of each basic information.

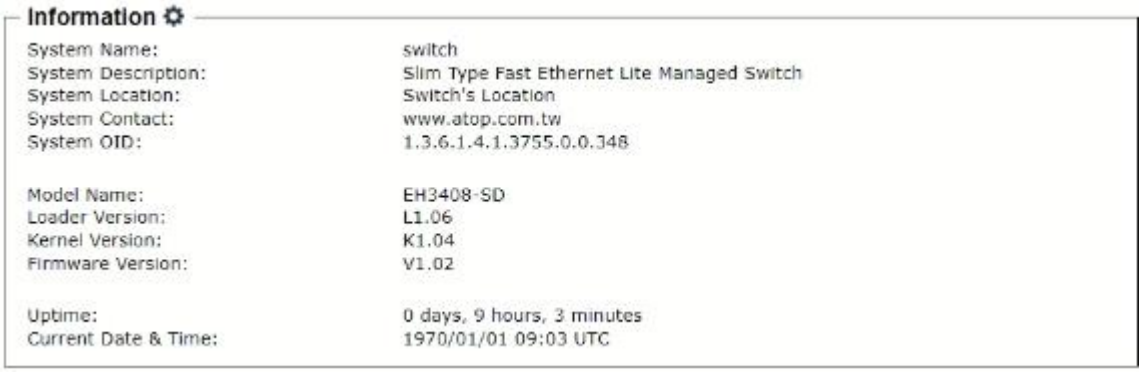


Figure 2.6 Information Feature

Table 2.1 Descriptions of the information features

Label	Description	Factory Default
System Name	**Specifies a particular role or application of different switches. The name entered here will also be shown in Atop's Device Management Utility. Max. 63 Char.**	**(Model name)**
System Description	**Detailed description of the unit. Max. 63 Characters.**	**Managed Switch + (Model name)**
System Location	**Location of the switch. Max. 63 Characters.**	**Switch Location**
System Contact	**Provides contact information for maintenance. Enter the name of whom to contact in case a problem occurs. Max. 63 Characters.**	**www.atop.com.tw**
System OID	**System's SNMP object identification (OID) number**	**-**
Model name	**The device's complete model name**	**(Model name)**
Loader Version	**The bootloader version of the device**	**-**
Kernel Version	**The current kernel version of the device**	**-**
Firmware Version	**The current firmware version of the device**	**-**
Uptime	**The duration of time since the device was started in days, hours, and minutes**	**-**
Current Date & Time	**The current date and time of the device**	**-**

To change or configure fields under the Information feature, the user can click on the gear icon to bring up a pop-up window called System Setting as shown in Figure 2.7. On this window, the user can configure System Name, System Description, System Location and System Contact. After you finished, clicking on the Save Changes button to save any changes or clicking on the Save Changes and Apply button to save and apply the setting.

Remark: The management pages provide two ways to save the changes of the configuration: Save Changes and Save Changes and Apply buttons. The former button will only save the new setting whole the latter button will save and then apply the setting so that it will be in effect immediately.

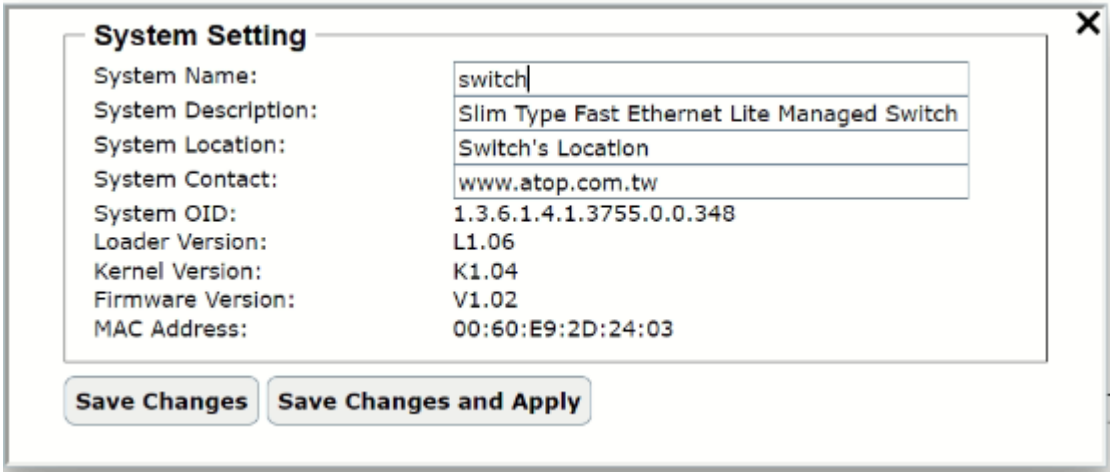


Figure 2.7 System Setting Management Pop-up Window

2.2.2 Connection feature

The Connection feature displays the current setting of the network configuration of the manage switch which are the status of DHCP Client, the IP Address, and the sub-Netmask as shown in Figure 2.8. To change network configuration, the user can click on the gear icon to bring up the IP Network Setting pop-up window as shown in Figure 2.9. The user can choose to enable or disable the Dynamic Host Configuration Protocol (DHCP) on the device as the DHCP client by selecting the corresponding drop-down list. If the DHCP Client is enabled, the manage switch will obtain the IP address configuration from another server in the network. If the DHCP Client is disabled, the user will have to enter the IPv4 Address, Subnet Mask, Gateway IP, DNS Servers 1 and DNS Servers 2. After you finished, clicking on the Save Changes button to save any changes or clicking on the Save Changes and Apply button to save and apply the setting. Table 2.2 summarizes the device information setting descriptions and corresponding default factory settings.

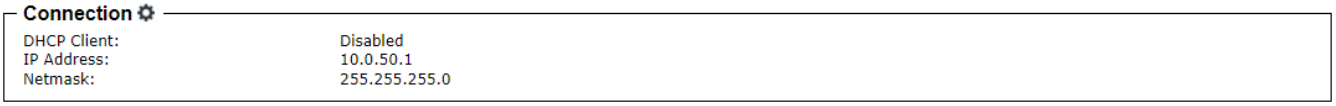


Figure 2.8 Connection Feature

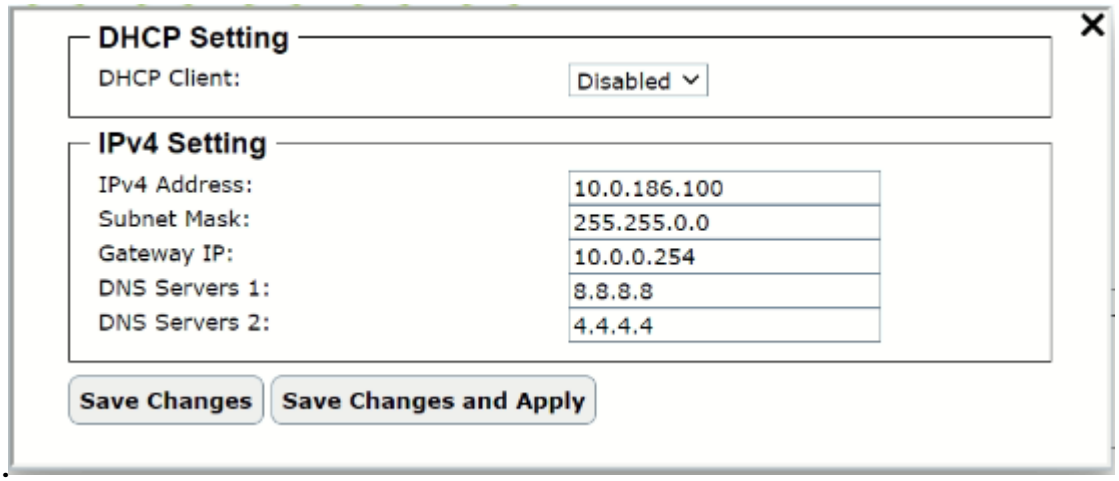


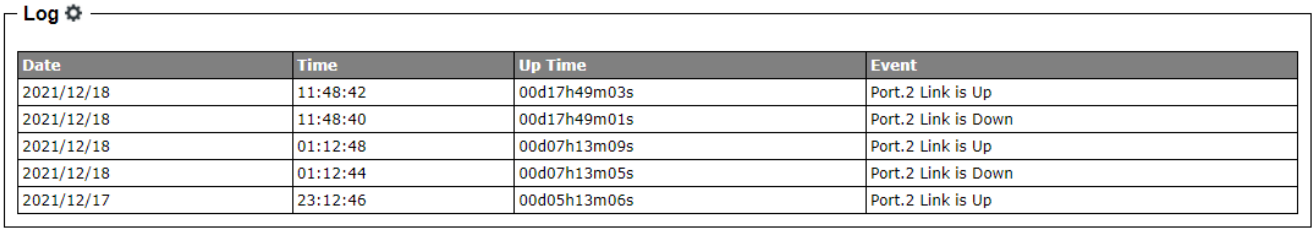
Figure 2.9 IP Network Setting Pop-up Window

Table 2.2 Description of IP Network Settings

Label	Description	Factory Default
DHCP Client	By selecting Enabled, an IP address and related fields will be automatically assigned. Note the fields below will be grey out. Otherwise, users can select Disabled and continue to set up the static IP address and related fields manually.	Disabled
IPv4 Address	The current IPv4 address of the device. Users can set a new static IP address for the device.	10.0.50.1
Subnet Mask	Display current Subnet Mask or set a new subnet mask	255.255.0.0
Gateway IP	Show current Gateway IP address or user can set a new one	0.0.0.0
DNS Server 1	Show current primary DNS IP address to be used by your network or user can set a new one	0.0.0.0
DNS Server 2	Show current secondary DNS IP address to be used by your network or user can set a new one	0.0.0.0

2.2.3 System Log feature

The Log feature at the buttom of the Information function shows a table of at least 5 system logs as shown in Figure 2.10. Each log entry includes Date, Time, Up Time, and Event description. Note that the log entries are sorted by date and time. Table 2.3 provides explanation of each column in the Log table.


Log

Date	Time	Up Time	Event
2021/12/18	11:48:42	00d17h49m03s	Port.2 Link is Up
2021/12/18	11:48:40	00d17h49m01s	Port.2 Link is Down
2021/12/18	01:12:48	00d07h13m09s	Port.2 Link is Up
2021/12/18	01:12:44	00d07h13m05s	Port.2 Link is Down
2021/12/17	23:12:46	00d05h13m06s	Port.2 Link is Up

Figure 2.10 Log Feature

Table 2.3 Description of Log Entry

Label	Description
Date	Indicate the system date of the occurred event
Time	Indicate the time stamp that this event occurred
Up Time	Indicate how long the system (managed switch) has been up since this event occurred
Event	Details description of this event

If the user would like to configure the System Log Setting, the user can click on the gear icon to bring up a System Log Setting pop-up window as shown in Figure 2.11. On this window, the user can enable or disable sending log to a log server. If the user enables the Log to Server option by choosing from the pull-down menu, the user will have to specify the Log's Server IP Address and Server Service Port in the next two fields. After you finished, clicking on the Save Changes button to save any changes or clicking on the Save Changes and Apply button to save and apply the setting.

Figure 2.11 System Log Setting Pop-up Window

Table 2.4 Description of System Log Setting Pop-up Window

Label	Description	Factory Default
Log to Server	Enabled: Enable Syslog Server. Disabled: Disable Syslog Server. If enabled, all recorded log events will be sent to the remote System Log server.	Disable
Server IP Address	Set the IP address of Syslog server	0.0.0.0
Server Service Port	Set the service port number of System Log server. Range from Port 1 to Port 65535.	514

2.3 Configuration

The Configuration or System Setting function is the second icon from the left. It is the circular icon with the pictures of wrench and screw driver. There are three features under the Configuration or System Setting function which are IP Setting, System Time, and Port Status as shown in Figure 2.12.

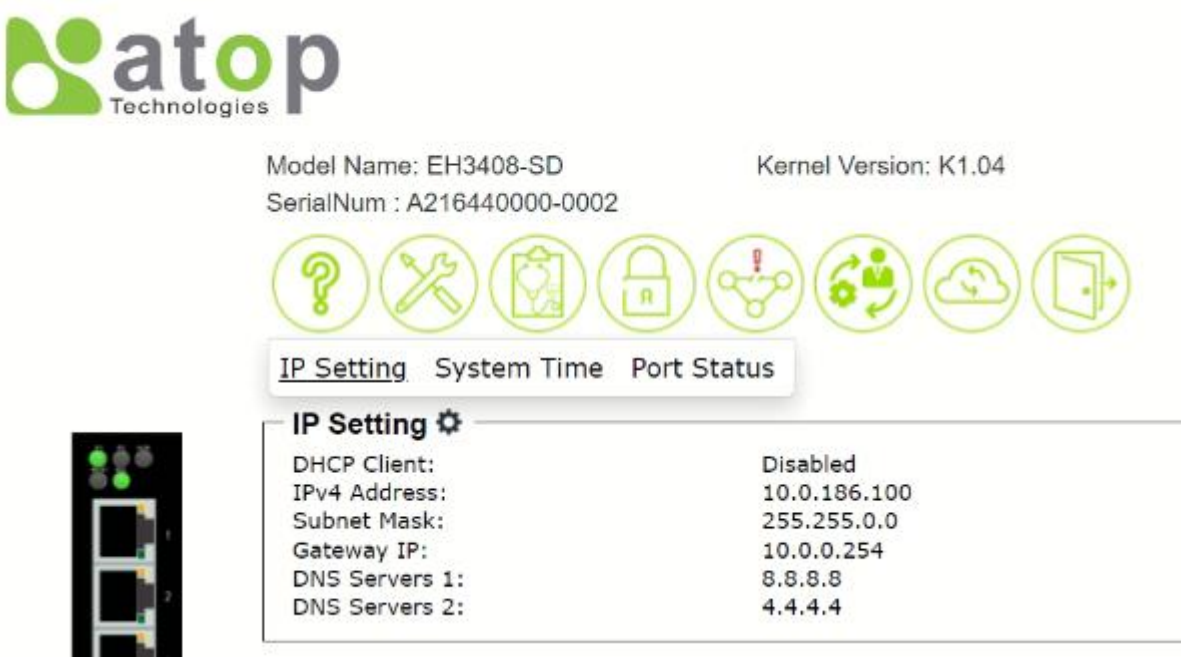


Figure 2.12 System Setting or Configuration Function

2.3.1 IP Setting feature

The **IP Setting** feature summarizes the current IP configuration of the manage switch. This web page as shown in Figure 2.13 displays information such as **DHCP Client**, **IPv4 Address**, **Subnet Mask**, **Gateway IP**, **DNS Servers 1**, and **DNS Servers 2**. By clicking on the gear icon next to the IP Setting title, the user can bring up the IP Setting pop-up window as shown in Figure 2.14. Table 2.5 summarizes each field in the IP Setting pop-up window. **After you finished, clicking on the Save Changes button to save any changes or clicking on the Save Changes and Apply button to save and apply the setting.**

Figure 2.13 IP Setting Feature

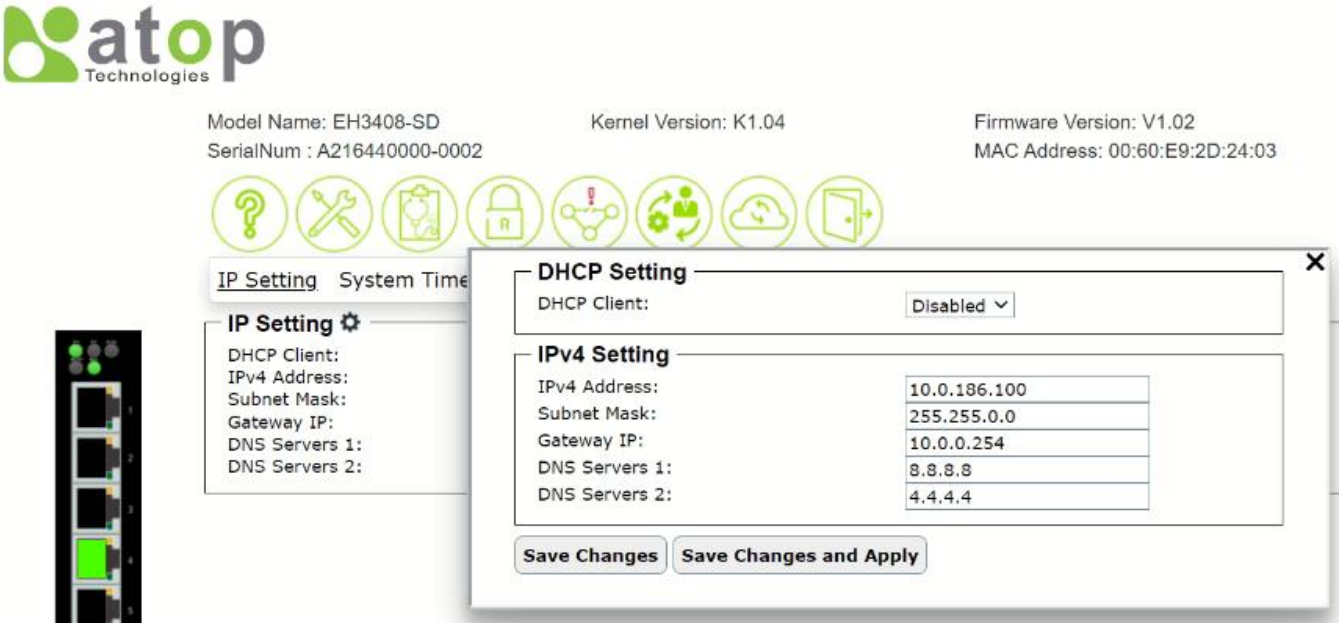


Figure 2.14 IP Setting Pop-up Window

Table 2.5 Description of IP Setting Pop-up Window

Label	Description	Factory Default
DHCP Client	By selecting Enabled, an IP address and related fields will be automatically assigned. Note the fields below will be grey out. Otherwise, users can select Disabled and continue to set up the static IP address and related fields manually.	Disabled
IPv4 Address	The current IPv4 address of the device. Users can set a new static IP address for the device.	10.0.50.1
Subnet Mask	Display current Subnet Mask or set a new subnet mask	255.255.0.0
Gateway IP	Show current Gateway IP address or user can set a new one	0.0.0.0
DNS Server 1	Show current primary DNS IP address to be used by your network or user can set a new one	0.0.0.0
DNS Server 2	Show current secondary DNS IP address to be used by your network or user can set a new one	0.0.0.0

2.3.2 System Time feature

The second feature under the system setting function is the System Time feature as shown in Figure 2.15. Atop's industrial managed switch has internal calendar (date) and clock (or system time) which can be set manually or automatically. This web page shows the configuration of System Time and Simple Network Time Protocol (SNTP). The first line in the figure indicates the Current Date & Time. The next line shows the current Time Zone. Then, the Mode option indicates the current mode of system time setting. This could be manual or automatic. The next three fields are NTP Server IP, SNTP Server IP, and NTP Server Setting. Finally, the last four lines on this web page provides information about the daylight time saving status, which are Daylight Saving State, Start Date, End Date, and Offset.

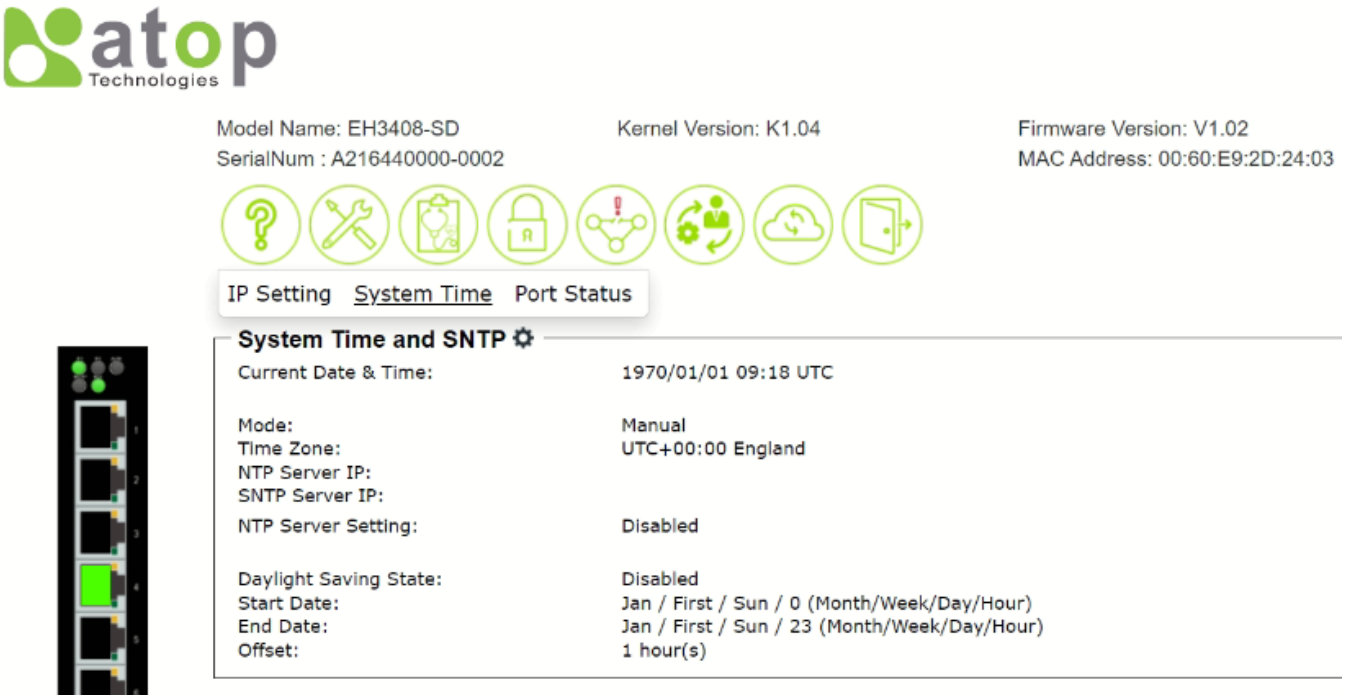


Figure 2.15 System Time Feature

To configure system time and SNTP, the user can click on the gear icon in Figure 2.15. This will bring up the System Time and SNTP pop-up window as shown in Figure 2.16. The users have options to configure Current Date & Time manually by choosing the pull-down menu for Mode to Manual. In manual mode as shown in Figure 2.16, the user can enter the Date and Time in the formats of YYYY:MM:DD and hh:mm:ss.

For automatically date and time setting, the users can enable Simple Network Time Protocol (SNTP) by selecting the pull-down manu for Mode as Automatic. Next, the user can select the Time Zone from the drop-down list. Then, the users must enter the NTP Server 1, NTP Server 2, and NTP Server 3 which will be used as the reference servers to synchronize date and time to. Next, the SNTP Server IP's address can be specified.

The managed switch can become a network time protocol server for the local devices by enabling NTP Server Setting option. The user can either enable or disable this option.

Finaly, the user has an option to enable or disable the Daylight Saving State. If the manage switch is deployed in a region where daylight saving time is practiced (see note below for explanation), please check the Enable option for Daylight Saving State. Then, the users will have to enter the Start Date, End Date, and Offset in hour(s). After you finished, clicking on the Save Changes button to save any changes or clicking on the Save Changes and Apply button to save and apply the setting. Table 2.6 **summarizes the description of fields in System Time and SNTP pop-up window.**

***Note:**

- Daylight Saving Time: In certain regions (e.g. US), local time is adjusted during the summer season in order to provide an extra hour of daylight in the afternoon, and one hour is usually shifted forward or backward.

- SNTP: Simple Network Time Protocol is used to synchronize the computer systems' clocks with a standard NTP server. Examples of two NTP servers are *time.nist.gov* and *time-A.timefreq.bldrdoc.gov*.

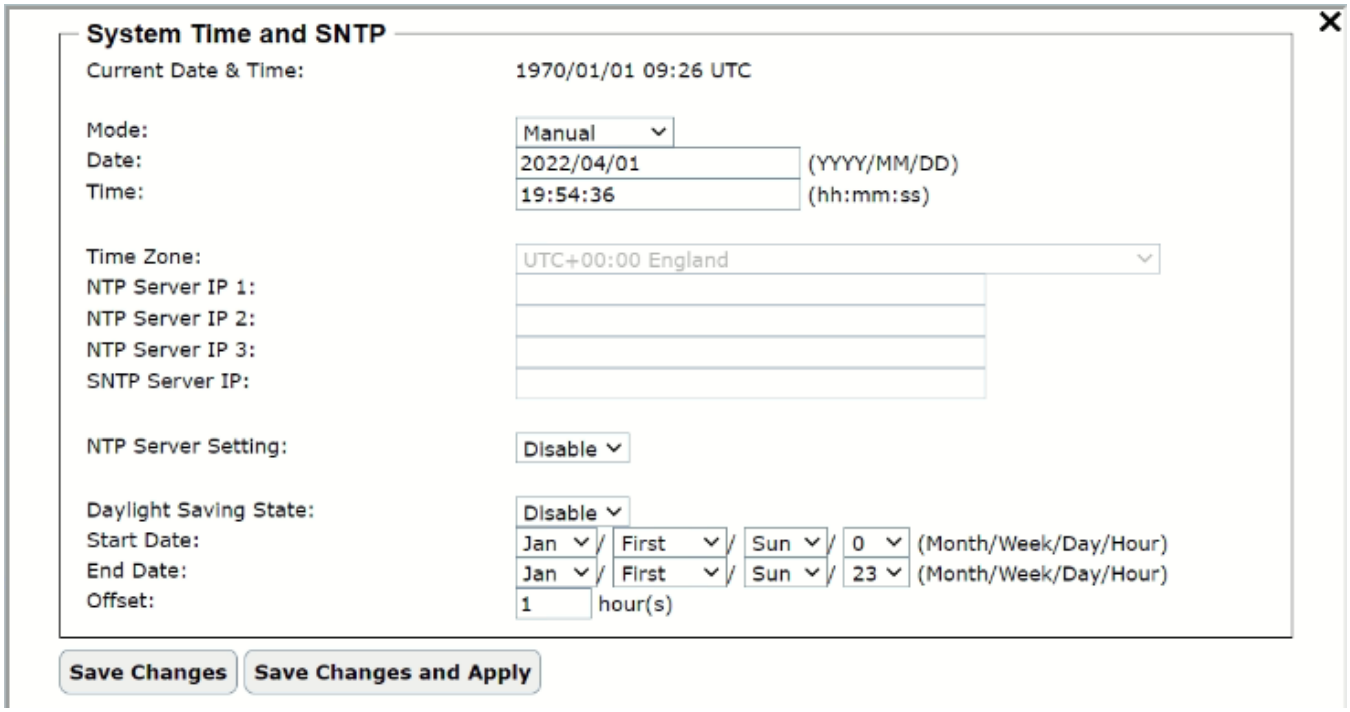


Figure 2.16 System Time and SNTP Pop-up Window

Table 2.6 Description of System Time and SNTP Pop-up Window

Label	Description	Factory Default
Current Date & Time	Display the current date and time on the manage switch	None
Mode	This option can be set as Manual or Automatic date and time setting	Manual
Date	Allows local date configuration in YYYY/MM/DD format	None
Time	Allows local time configuration in local hh:mm:ss format	None
Time Zone	The user can choose the current local time from the drop-down list.	(UTC+00:00) England
Daylight Saving	Enable or disable Daylight Saving Time function	Unchecked
NTP Server IP 1	Sets the first IP or Domain address of NTP Server.	time.nist.gov
NTP Server IP 2	Sets the second IP or Domain address of NTP Server. Switch will locate the 2nd NTP Server if the 1st NTP Server fails to connect.	Time-A.timefreq.bldrdoc.gov
NTP Server IP 3	Sets the third IP or Domain address of NTP Server. Switch will locate the 3rd NTP Server if the 1st and 2nd NTP Servers fail to connect.	
SNTP Server IP	Sets the IP or Domain address of SNTP Server.	
NTP Server Setting	This option can enable or disable network time protocol (NTP) daemon inside the managed switch which allows other devices in the network to synchronize their clock with this managed switch using NTP.	Disable

Label	Description	Factory Default
Daylight Saving State	This option allows the user to enable or disable Daylight Saving on the switch	Disable
Start Date	Define the start date of daylight saving	NULL
End Date	Define the end date of daylight saving	NULL
Offset	Decide how many hours to be shifted forward/backward when daylight saving time begins and ends. See note below.	0

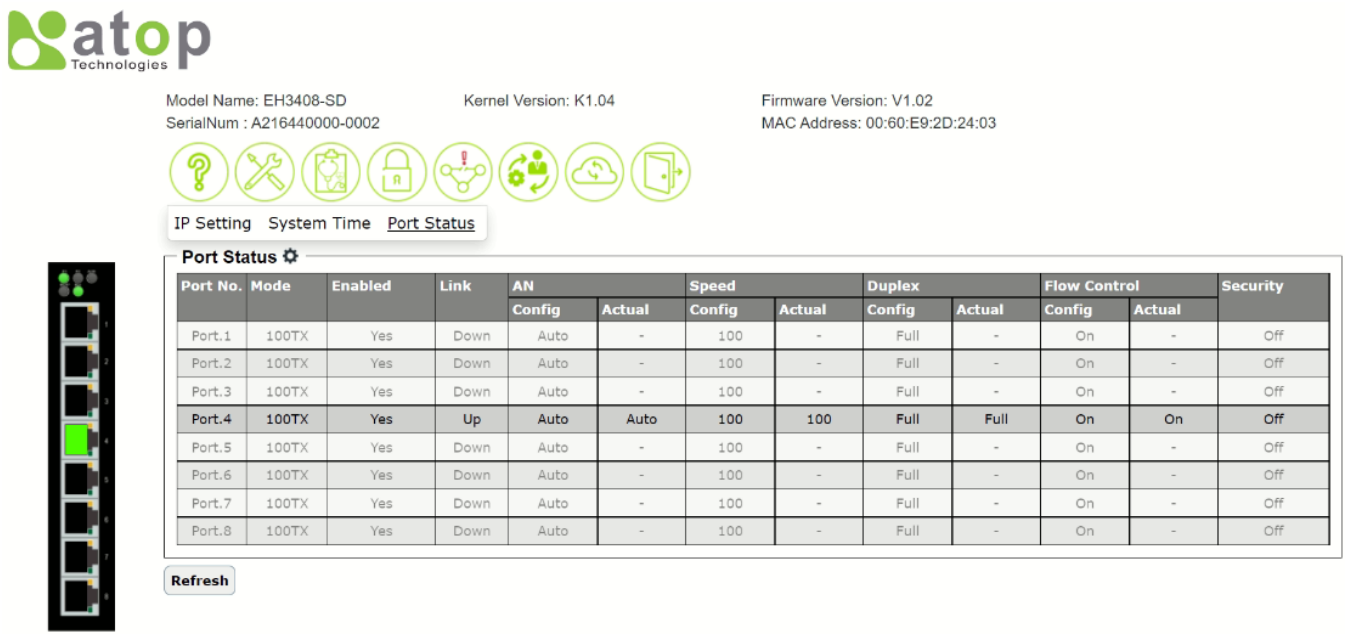
2.3.3 Port Status feature

The third feature under the system setting function is the Port Status feature as shown Figure 2.17. The overview of port status on the managed switch can be viewed in this webpage. Each entry in the table of the port status shows information related to a port on the managed switch which are Port No., Mode, Enabled, Link, AN-Config/Actual, Speed-Config/Actual, Duplex-Config/Actual, Flow Control-Config/Actual, and Security. Note that the last column reports the security status whether it is turned on or off on each port, which can be either static security or 802.1x. To check the latest status of all port, click the Refresh button at the bottom of the webpage.

The header in each column and its possible values of the ports's status are listed here:

- **Port No. (Port 1 to Port 8)**
- **Mode (Copper (C) or Fiber (F))**
- **Enable (Yes or No)**
- **Link (Up or Down)**
- **AN or Auto Negotiation (Auto or Force)**
- **Speed (unit: Mbps)**
- **Duplex (Full or Half)**
- **Flow Control (On or Off)**
- **Security (On or Off): Either static security or 802.1x port security is turned on or off.**

Note: Config column means the configuration on the device while Actaul column refers to the current status or operation of the port.



Port No.	Mode	Enabled	Link	AN		Speed		Duplex		Flow Control		Security
				Config	Actual	Config	Actual	Config	Actual	Config	Actual	
Port.1	100TX	Yes	Down	Auto	-	100	-	Full	-	On	-	Off
Port.2	100TX	Yes	Down	Auto	-	100	-	Full	-	On	-	Off
Port.3	100TX	Yes	Down	Auto	-	100	-	Full	-	On	-	Off
Port.4	100TX	Yes	Up	Auto	Auto	100	100	Full	Full	On	On	Off
Port.5	100TX	Yes	Down	Auto	-	100	-	Full	-	On	-	Off
Port.6	100TX	Yes	Down	Auto	-	100	-	Full	-	On	-	Off
Port.7	100TX	Yes	Down	Auto	-	100	-	Full	-	On	-	Off
Port.8	100TX	Yes	Down	Auto	-	100	-	Full	-	On	-	Off

Figure 2.17 Port Status Feature

If the user would like to configure the status of the port, the user can click on the gear icon to bring up the Port Control pop-up window as shown in Figure 2.18. For each port, the users can control the state of each port by selecting the State to Enable or Disable from the drop-down selection box. Next, under the Speed/Duplex column the user can configure the speed and duplexing setting of the port, which can be either AutoNegotiation or Force. When selecting the Force negotiation, the port's speed and duplexing will be locked to the settings configured by the users. On the other hand, the AutoNegotiation will allow the switch to determine the actual speed and duplexing for that port. Each port can set the Flow Control mechanism to either On or Off on the eighth column. This flow control will be useful to avoid packet loss when there is a network congestion. However, the Flow Control setting is Off by default. After you finished, clicking on the Save Changes button to save any changes or clicking on the Save Changes and Apply button to save and apply the setting. Table 2.7 summarizes the description of fields in Port Control pop-up window.

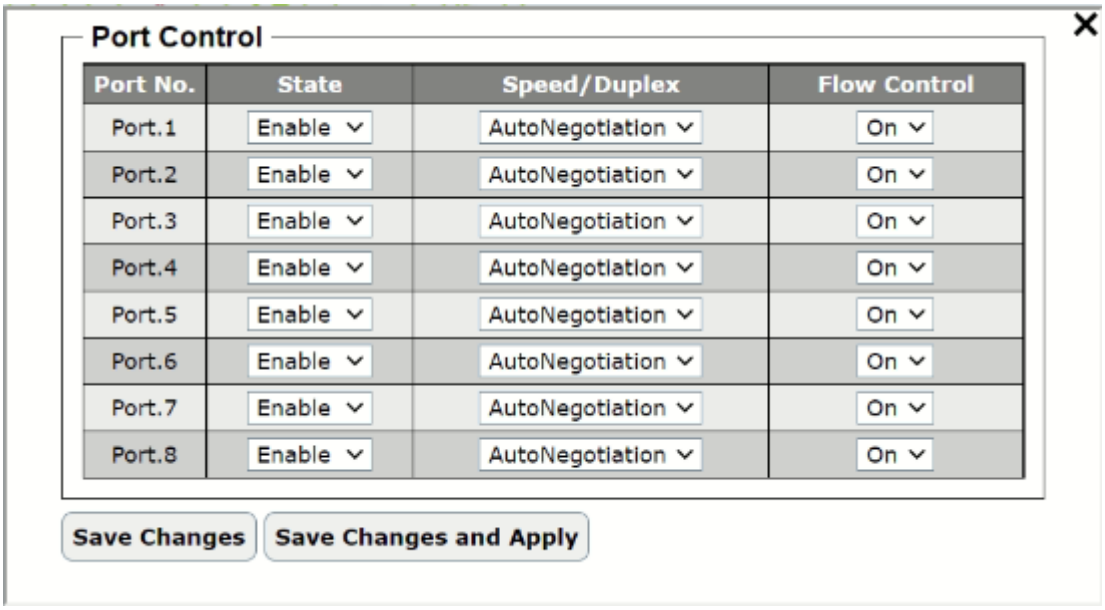


Figure 2.18 Port Control Pop-up Window

Table 2.7 Description of Port Control Pop-up Window

Label	Description	Factory Default
Port No.	Port number on the managed switch.	-
State	Check the box to allow data to be transmitted and received through this port	All ports are enabled
Speed/Duplex	Choose from either Force or AutoNegotiation.	Auto-negotiation is enabled to all ports.
Flow Control	Either on or off. The Flow Control mechanism can be enabled (On) to avoid packet loss when congestion occurs.	On

2.4 Diagnostic

The Diagnostic function allows the user to check the operation of the managed switch through the following features: System Log, Rmon History, Port Statistics, LLDP, Warning/Alarm, and Log Event. The Diagnostic function is the third circular icon with stethoscope picture on top of a medical chart. Figure 2.19 illustrates the list of features under the Diagnostic function.

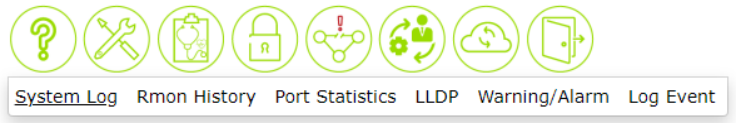


Figure 2.19 Diagnostic Function on Menu Bar

2.4.1 System Log feature

The System Log feature under the Diagnostic function contains two sections: System Log Setting and System Log as shown in Figure 2.20. In the upper section, the System Log Setting summarizes the current configuration of system log. To configure the system log, the user can click on the gear icon next to the System Log Setting title to bring up the System Log Setting pop-up window as shown in Figure 2.21. Note that this pop-up window is the same feature as described in Log feature under the Information function in Section 2.2.3.

In the lower section of the web page, a table of system log is displayed. Each log entry includes Date, Time, Up Time, and Event description. Note that the log entries are sorted by date and time. Table 2.3 in Section 2.2.3 provides explanation of each column in the System Log table. The user can choose how many log entries to be displayed in the table by selecting the number (20, 50, or 100) from the Show's drop-down list. Additionally, the user can find relevant log entries through the Search box on the top left of the table. Under each column, the user can filter the log entries based in Date, Time, Up Time, and Event. The user can also click on the Refresh button to obtain the latest log entries from the managed switch.

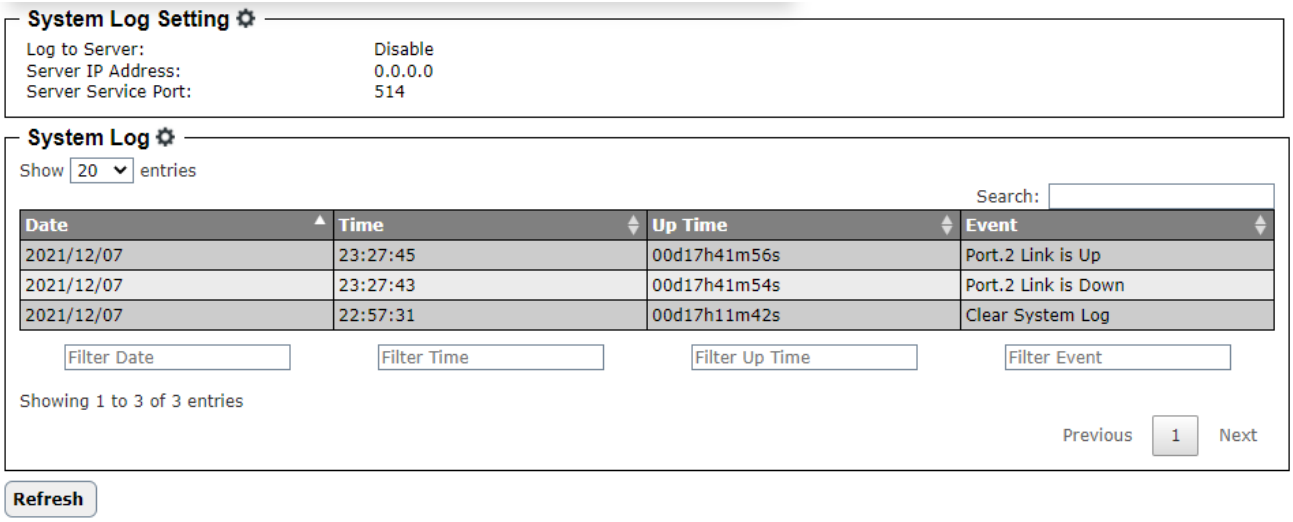


Figure 2.20 System Log Feature

Figure 2.21 System Log Setting Pop-up Window

To clear the table of system log, the user can click on the gear icon of the System Log title to bring up the System Log Clear pop-up window as shown in Figure 2.22. By clicking on the Clear System Log button on this pop-up window, the user can clear all log enries.

Figure 2.22 System Log Clear Pop-up Window

2.4.2 Rmon History feature

The Rmon History feature under the Diagnostic function contains a remote network monitoring (RMON) information in a form of table as shown in Figure 2.23. Each entry summarizes the counts of Drop, Octets, Packets, Broadcast, Multicast, CRCAlignError, Undersize, Oversize, Fragments, Jabber, Collisions, Utilization for each port. At the bottom of the table, the user can check the box in front of Auto Refresh to enable the automatic refresh of the information in the table and also can specify the duration of each refresh in the text box which is in unit of seconds. The user can also click the Refresh button to obtain the latest information.

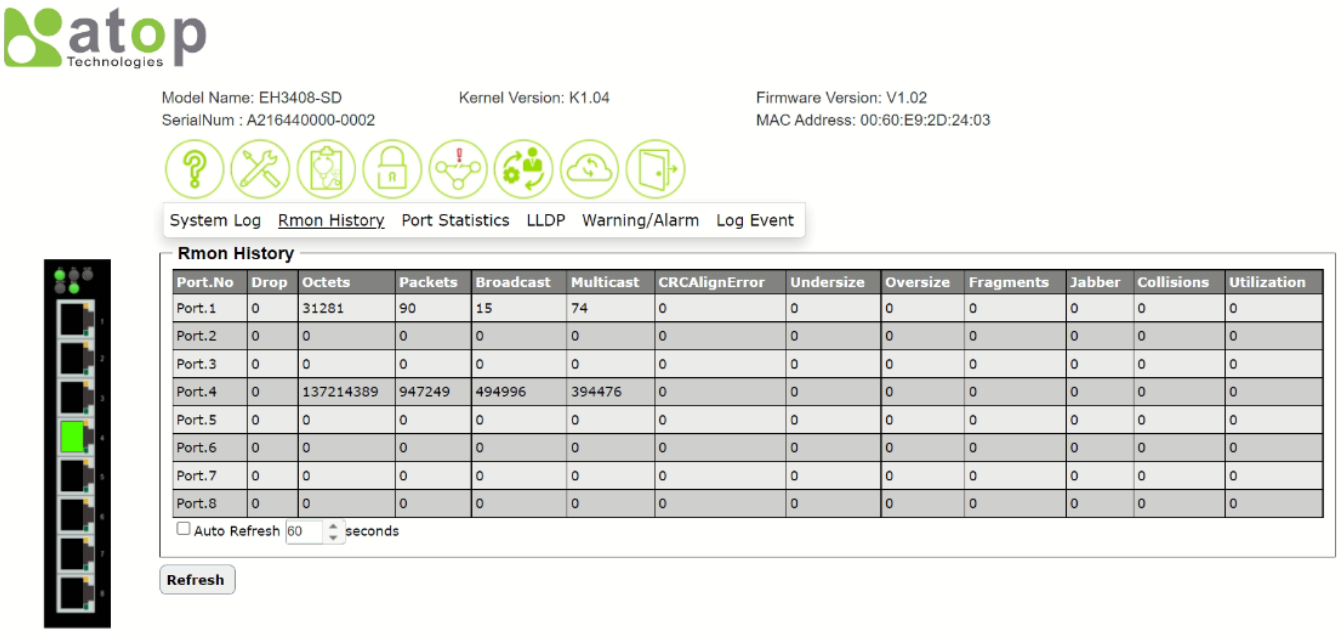


Figure 2.23 Rmon History Feature

2.4.3 Port Statistics feature

The Port Statistics feature under Diagnostic function provides overview information of link status and frame's statistics for each port on the managed switch. Port Overview table as shown in Figure 2.24 displays the counts of OK and Error of transmitting (TX) and receiving (RX) frames. It also indicates the status of each port whether it is enabled or disable and whether the link is up or down. At the bottom of the table, the user can check the box in front of Auto Refresh to enable the automatic refresh of the information in the table and also can specify the duration of each refresh in the text box which is in unit of seconds. The user can also click the Refresh button to obtain the latest information. If the user cleck the Clear button, the statistics information will be cleared from the table.

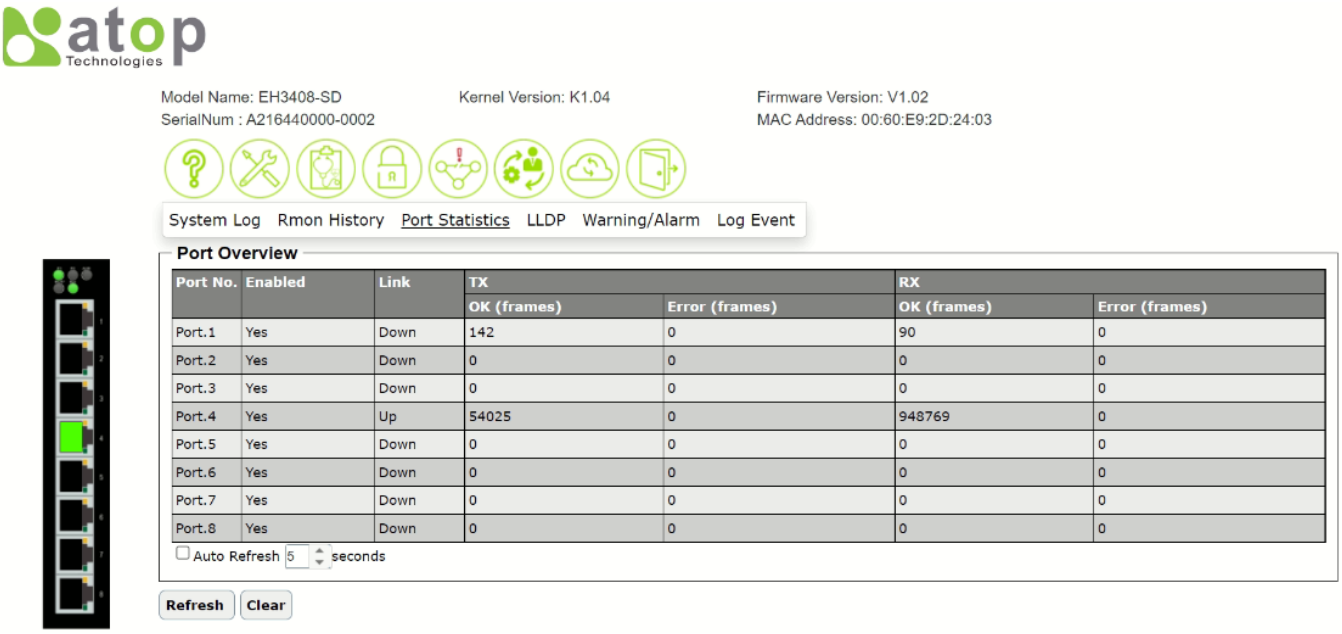


Figure 2.24 Port Statistics (Overview) Feature

2.4.4 LLDP feature

Link Layer Discovery Protocol (LLDP) is an IEEE802.1ab standard OSI layer-2 protocol. LLDP allows Ethernet network devices to advertise details about themselves, such as device configuration, capabilities and identification. The advertise packets are periodically sent to directly connected devices on the network that are also using LLDP or so called its neighbors. LLDP is a "one hop" unidirectional protocol in an advertising mode.

LLDP information can only be sent to and received by devices, no solicit information or state changes between nodes. The device has a choice to turn on and off sending and receiving function independently. Advertised information is not forward on to other devices on the network. LLDP is designed to be managed with SNMP. Applications that use this protocol include topology discovery, inventory management, emergency services, VLAN assignment, and inline power supply.

LLDP feature under Diagnostic function contains LLDP Neighbor Info Table as shown in Figure 2.25. This webpage allows the user to view the LLDP's neighbor information of the managed switch. The Neighbor Information table contains Port ID, Chassis ID, Remote Port ID, Port Description, System Name, System Description, and Management Address on each Port of the managed switch. The user can choose how many entries to be displayed in the table by selecting the number from the Show's drop-down list. Additionally, the user can find relevant log entries through the Search box on the top left of the table. The users can also click on the Refresh button to get the latest Neighbor Information table. Table 2.8 summarizes the description of each column in LLDP neighbor info table.

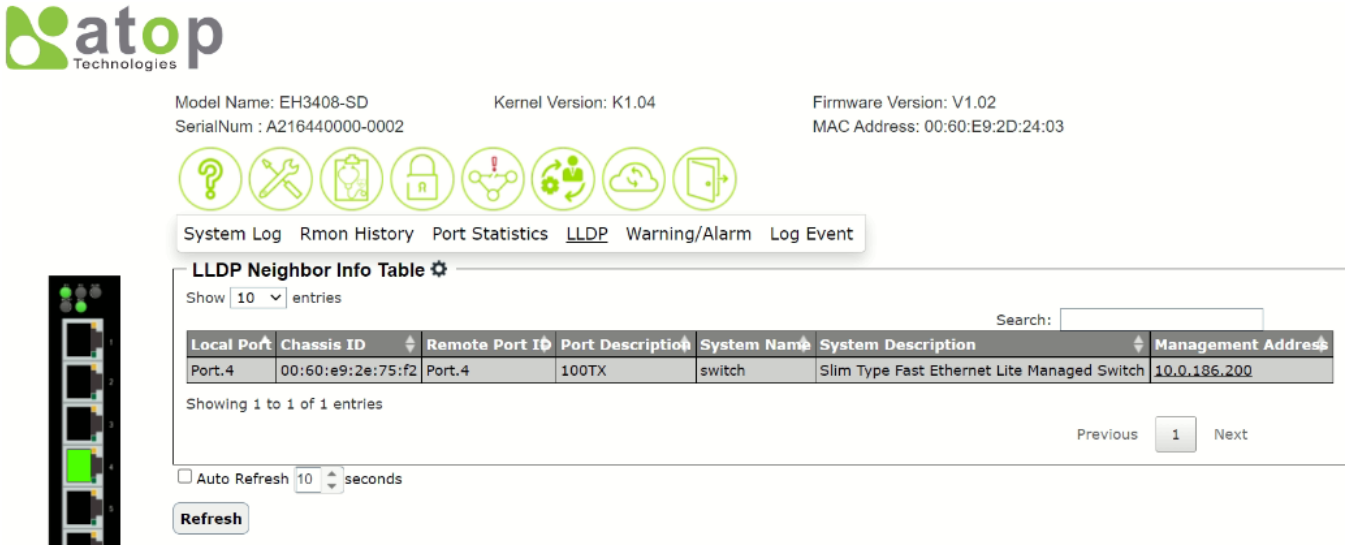


Figure 2.25 LLDP Feature

Table 2.8 Description of Columns in LLDP Neighbor Info Table

Label	Description
Local Port	Indicates particular port number of the switch.
Chassis ID	Indicates the identity of the neighbor of this particular port.
Remote Port ID	Indicates the port number of this Neighbor.
Port Description	Shows a textual description of the neighbor port.
System Name	Indicates the device name/hostname of the Neighbor.
System Description	Shows a more detailed description of the neighbor's device.
Management Address	Indicates neighbor's management IP address.

To configure LLDP protocol, the user can click the gear icon next to the LLDP Neighbor Info Table title. This will bring up the LLDP Setting pop-up window as shown in Figure 2.26. On this window, the user has options for enabling or disabling the LLDP Protocol, as well as setting LLDP transmission parameters which are Tx Interval and Tx Time-To-Live (TTL). After you finished, clicking on the Save Changes button to save any changes or clicking on the Save Changes and Apply button to save and apply the setting. Table 2.9 describes the LLDP Setting parameters which are transmit interval and transmit time-to-live of the LLDP advertisement packets.

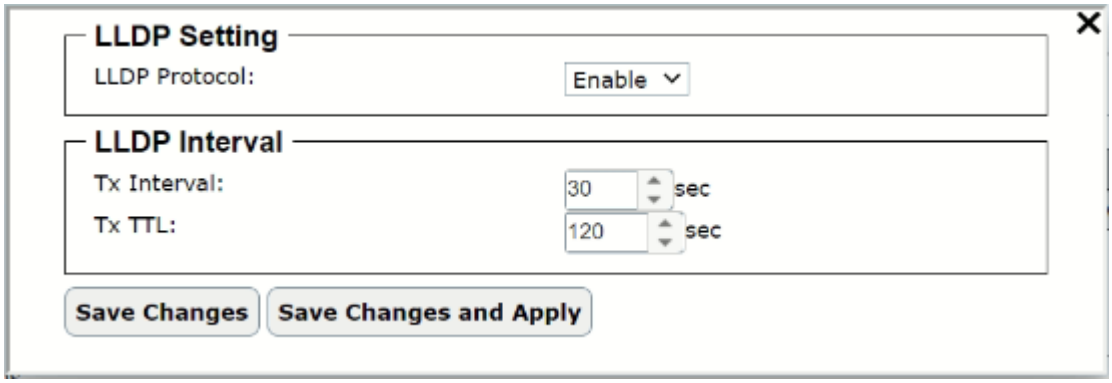


Figure 2.26 LLDP Setting Pop-up Window

Table 2.9 Description of LLDP Protocol Setting Pop-up Window

Label	Description	Factory Default
LLDP	Choose to either enable or disable LLDP.	Enabled
Tx Interval	Set the transmit interval of LLDP messages. Range from 5 to 65535 seconds.	30
TxTTL	*Tx Time-To-Live*. Amount of time to keep neighbors' information. The recommend TTL value is 4 times of *Tx Interval*. The information is only removed when the timer is expired. Range from 5 to 65535 seconds.	120

2.4.5 Warning/Alarm feature

For EH3408 series of lite-managed switch, there are two types of Warning or Alarm: Link Status Alarms and Power Status Alarms as shown in Figure 2.27. The Link Status Alarms are related to the activities of particular port(s). Power Status Alarms keep track of power status of the switch based on the available input connectors. For link status and power status alarms, there are two possible notification methods via Relay and Alarm LED. The table of Link Status Alarms shows the settings of notifications on Relay and Alarm LED for each port. The table of Power Status Alarms also shows the settings of notifications on Relay and Alarm LED for each power input connector.

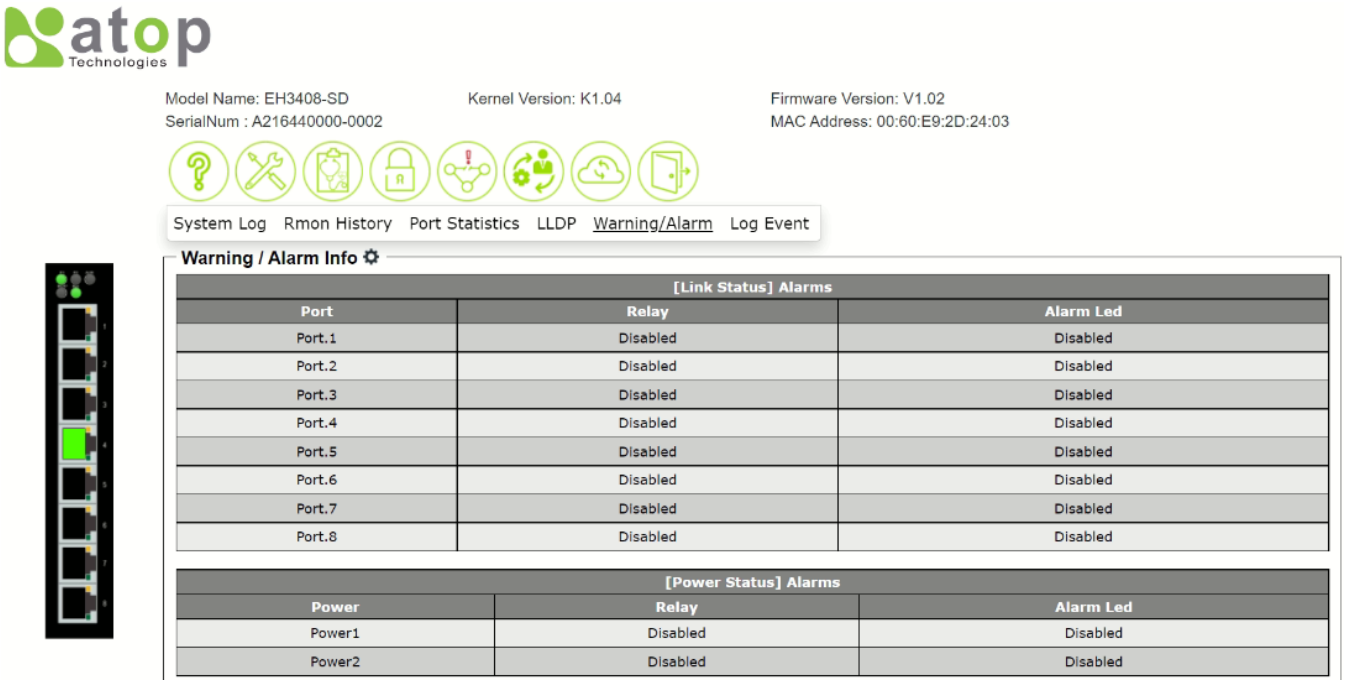


Figure 2.27 Warning/Alarm Feature

To setup the Warning/Alarm, the user can click on the gear icon to bring up Warning/Alarm Setting pop-up window as shown in Figure 2.28. Then, the user can independently enable or disable warning or alarm on each port and/or power input connector. After you finished, clicking on the Save Changes button to save any changes or clicking on the Save Changes and Apply button to save and apply the setting.

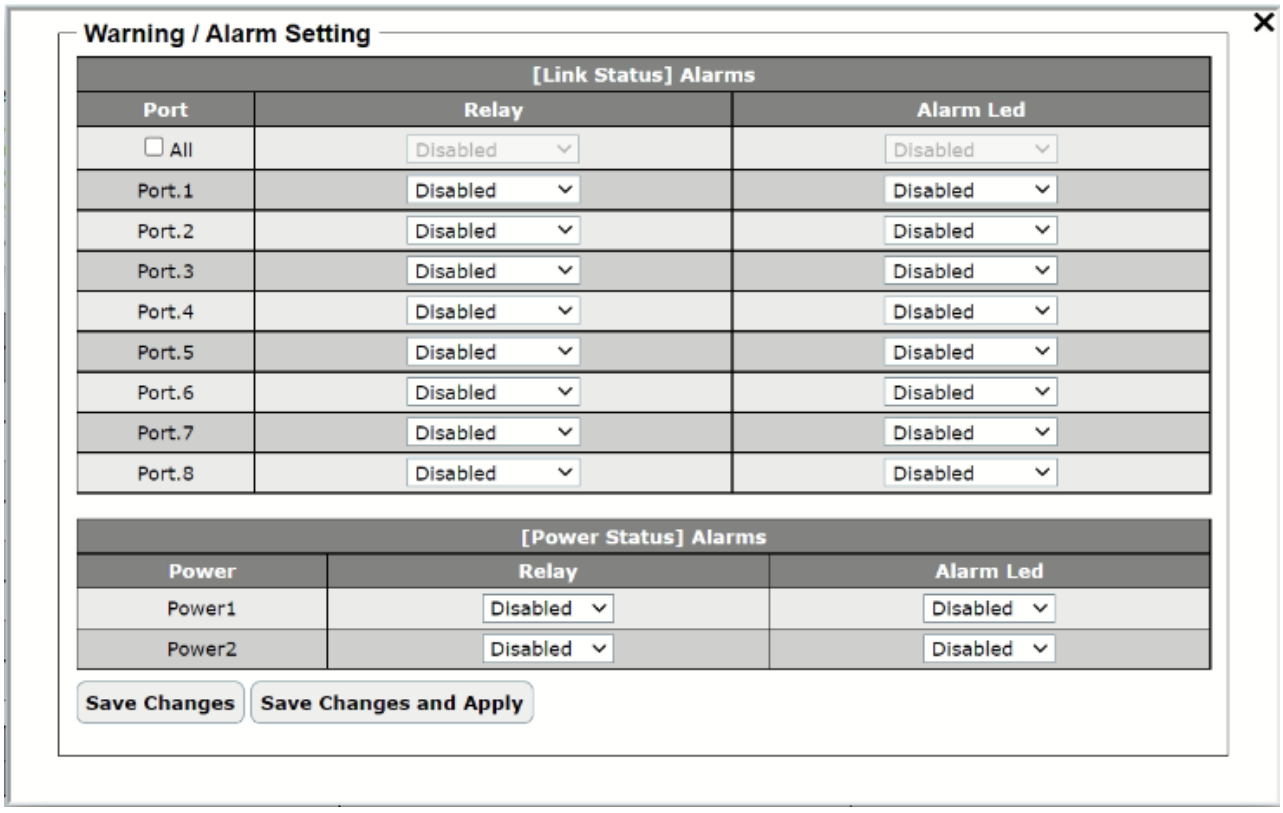


Figure 2.28 Warning/Alarm Setting Pop-up Window

2.4.6 Log Event feature

The Log Event feature under the Diagnostic function is shown in Figure 2.29. This web page displays SYSLOG status of the following events: System Restart, SNMP Authentication Failure, and status of each port.

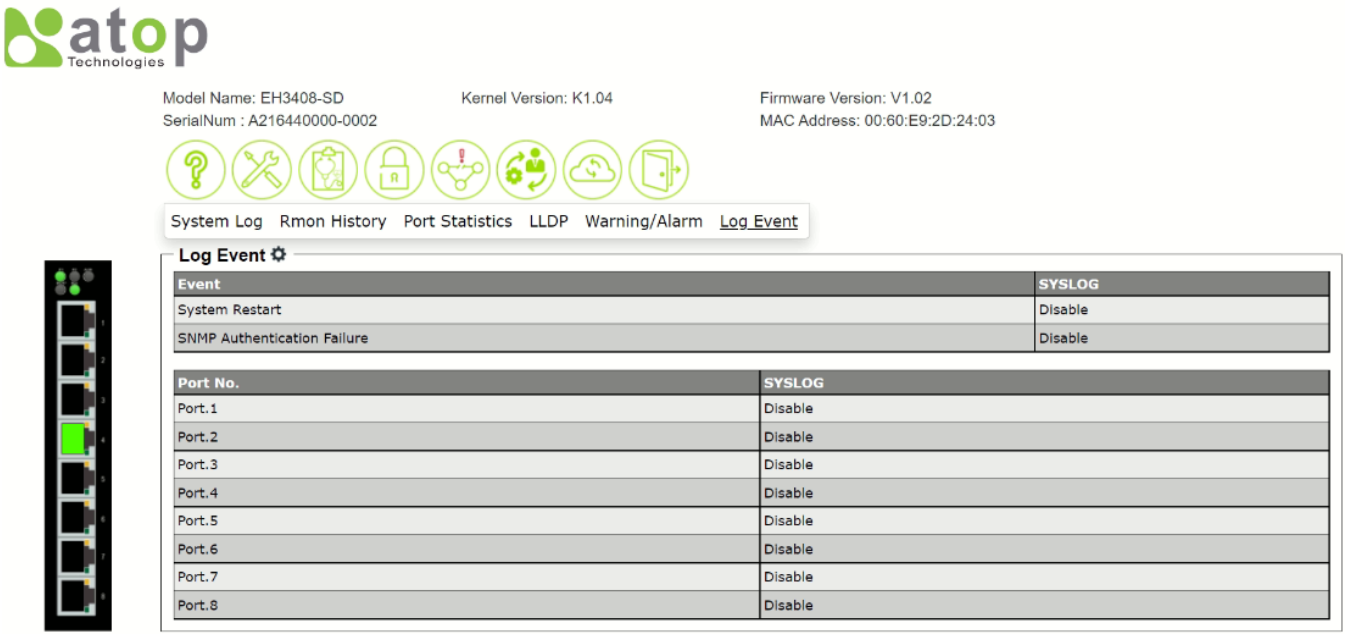


Figure 2.29 Log Event Feature

To configure the SYSLOG event and SYSLOG status for each port, the user can click on the gear icon to bring up the Log Event pop-up window. The System Restart and SNMP Authentication Failure event boxes can be checked to enable or uncheck to disable. The SYSLOG of each port status can be set to Disable, Link Up, Link Down or Link Up & Down as shown in Figure 2.31.

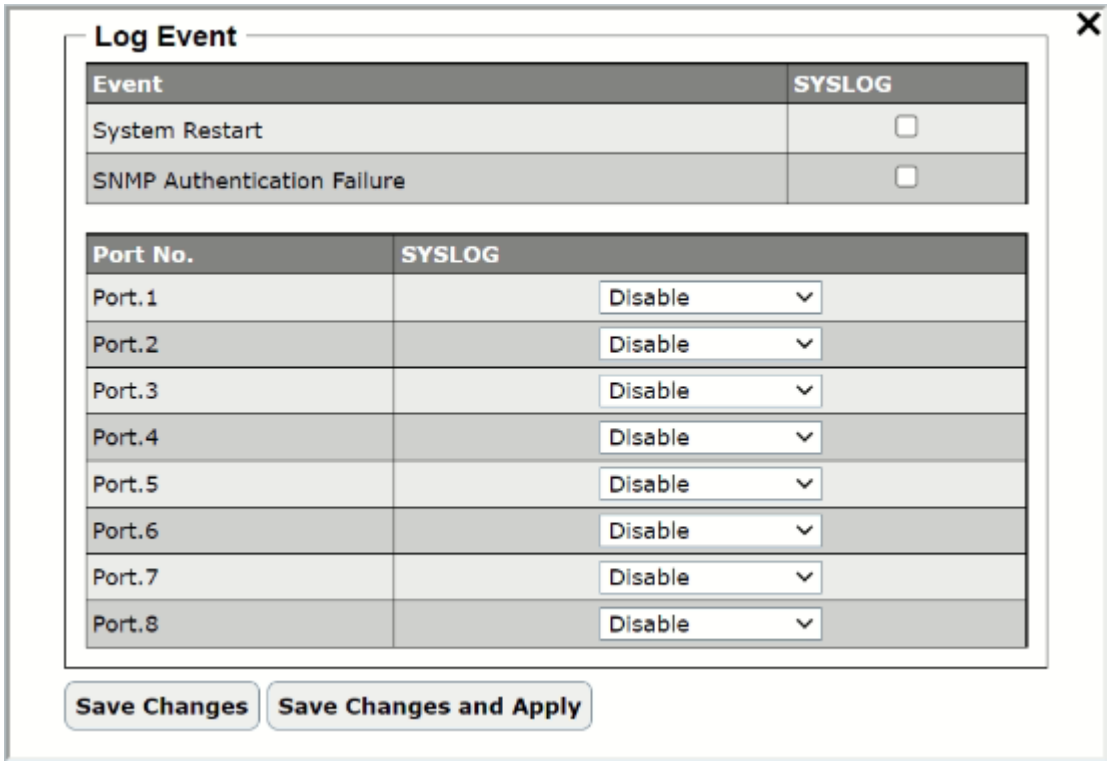


Figure 2.30 Log Event Setting Pop-up Window

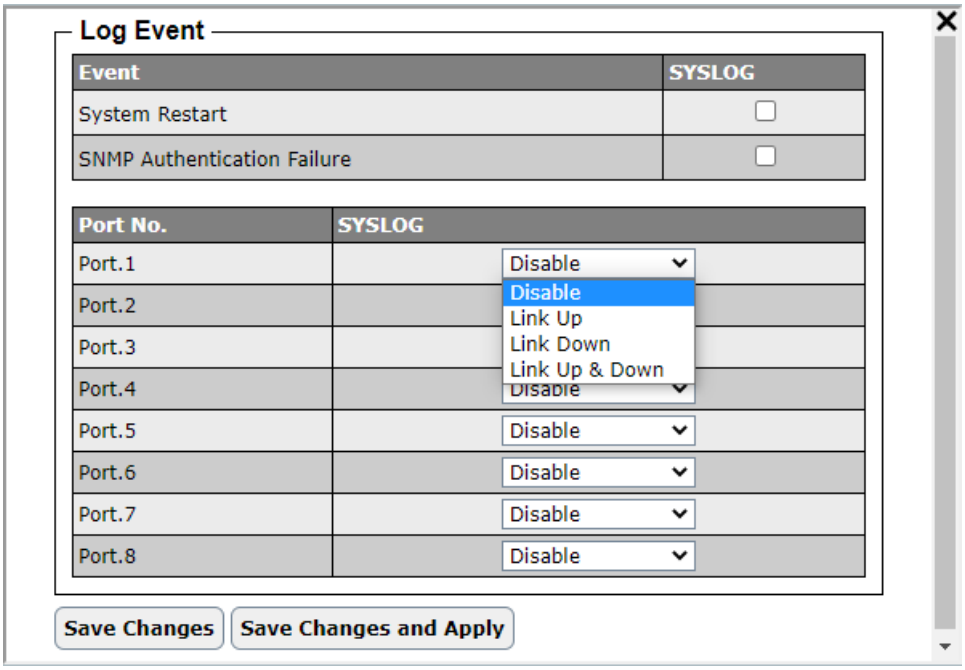


Figure 2.31 SYSLOG Event Drop-down Selection

2.5 Security

The Security function for EH3408 series lite-managed switch includes Strom Control and VLAN Table features as shown in the menu bar in Figure 2.32. The Security function is the fourth circular icon on the menu bar with the lock picture.

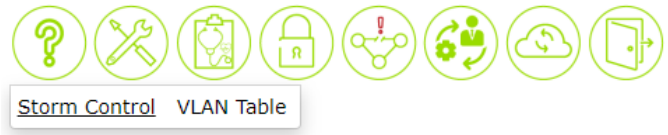


Figure 2.32 Security Function

2.5.1 Storm Control feature

Storm control prevents traffic on a LAN from being disrupted by ingress traffic of broadcast, multicast, and destination lookup failure (DLF) on a port. Figure 2.33 shows the Strom Control feature under the Security function. On this web page, there are two sections: Storm Control Threshold and Storm Control Information. The Storm Control Threshold indicates the current setting of the threshold (ranging from 0 to 255500 packet per second (pps)) while the Storm Control Information summarizes the current settings for different types of traffic in each port in a table format. The Strom Control feature in EH3408 series lite-managed switch can prevent three types of ingress traffic on a LAN which are DLF (Destination Lookup Failure), Multicast and Broadcast.

Type of Storm Packets:

- **DLF: Destination Lookup Failure. The switch will always look for a destination MAC address in its MAC Table first. In case that a MAC address cannot be found in the MAC Table, which means DLF occurs, the switch will forward the packets to all ports that are in the same LAN.**
- **Multicast: This type of transmission sends messages from one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive it. Network devices that support multicast send only one copy of the information across the network until the delivery path that reaches group members diverges. At these**

diverging points, multicast packets will be copied and forwarded. This method helps reducing high traffic volumes due to large number of destinations, using network bandwidth efficiently.

- Broadcast: Messages are sent to all devices in the network.

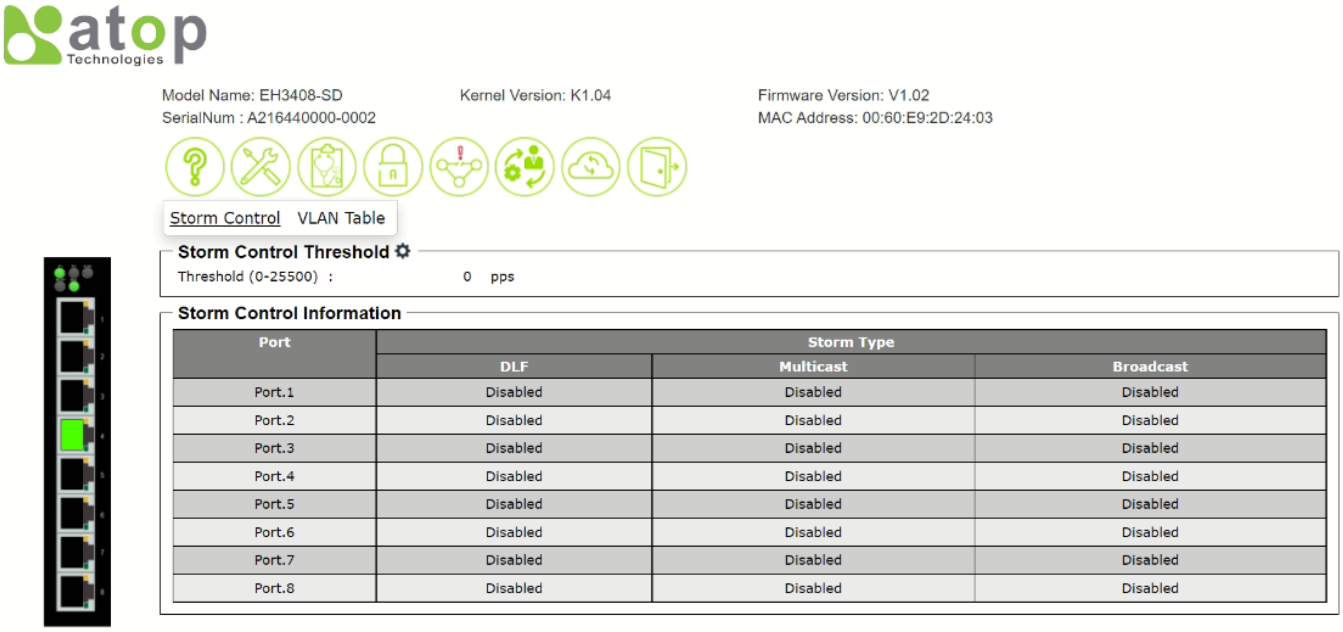


Figure 2.33 Storm Control Feature

To configure the Storm Control feature, the user can click on the gear icon to bring up a pop-up window as shown in Figure 2.34. On this window, the user can set the Threshold value from 0 to 25500 pps. The users can enable or disable setting of any Storm Control Type on all ports at the same time by clicking on the box in front of the All line. The storm control setting can also be independently control on each port by selecting Enabled or Disabled from the drop-down selection under each column. After you finished, clicking on the Save Changes button to save any changes or clicking on the Save Changes and Apply button to save and apply the setting.

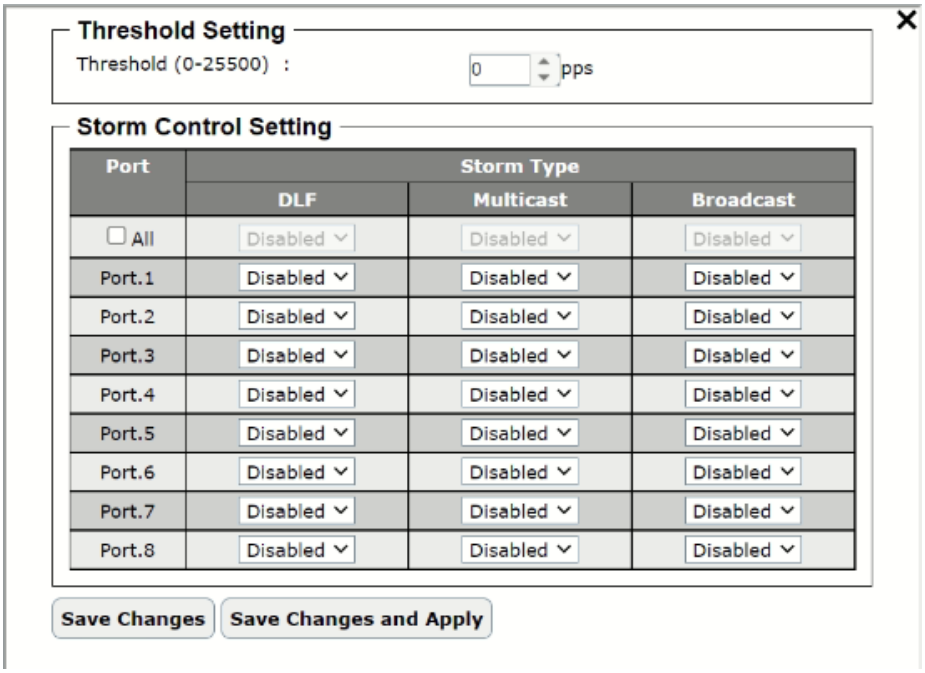


Figure 2.34 Storm Control Setting Pop-up Window

2.5.2 VLAN Table feature

The VLAN Table feature under Security function displays the current 802.1Q VLAN table which lists all the VLANs that are added/modified to the managed switch. The VLAN Table consists of three columns: VLAN ID, Untagged Ports, and Tagged Ports as shown in Figure 2.35. The number of VLAN entries can be selected to Show 10, 25, 50, or 100 entries from the drop-down selection.

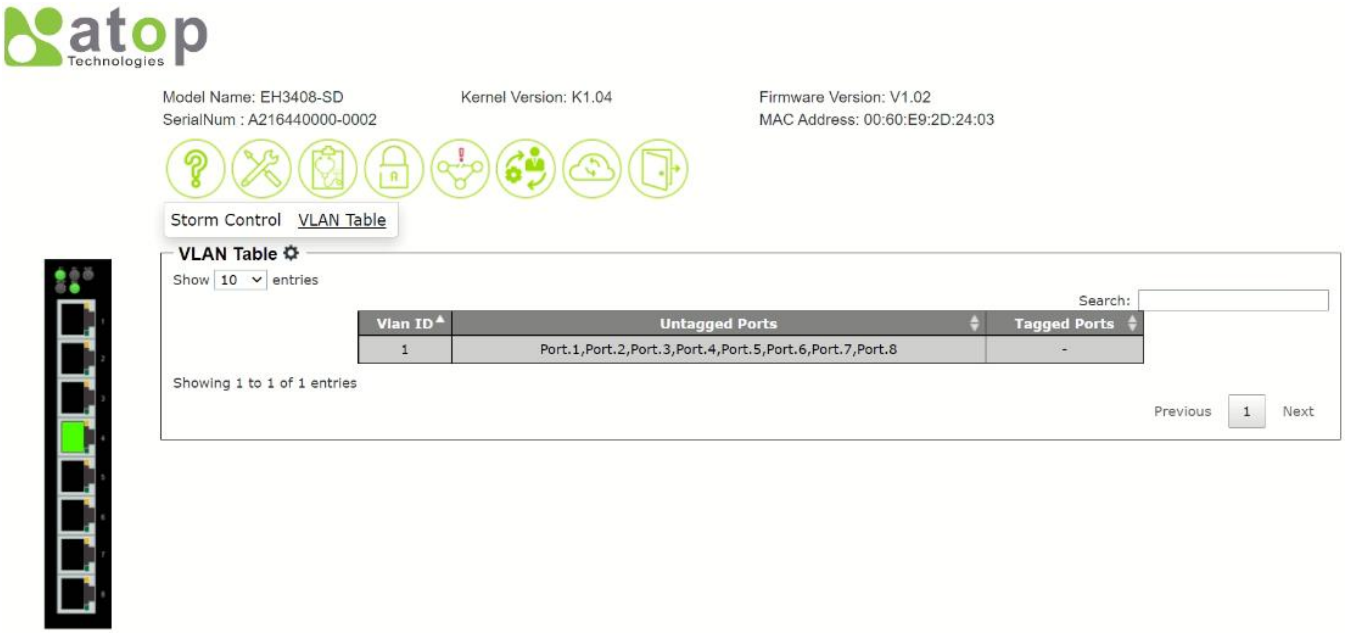


Figure 2.35 VLAN Table Feature

To configure the VLAN, the user can click on the gear icon to bring up the VLAN Setting pop-up window as shown in Figure 2.36. On this pop-up window, VLAN Mode Setting, Management VLAN, and 802.1Q VLAN Setting can be managed. The VLAN Mode Setting can be set to 802.1Q or Disable. Next, the Management VLAN (ID) can be set to the value from 1 to 4094. Next, the 802.1Q VLAN Setting is a table that allows independent setting of each port. The user can select the Link Type as either Access or 1QTrunk. The PVID can be set to the value from 1 to 4094. Finally, Untagged and Tagged VLAN can be set to a range of VLAN ID from 1 to 4094.

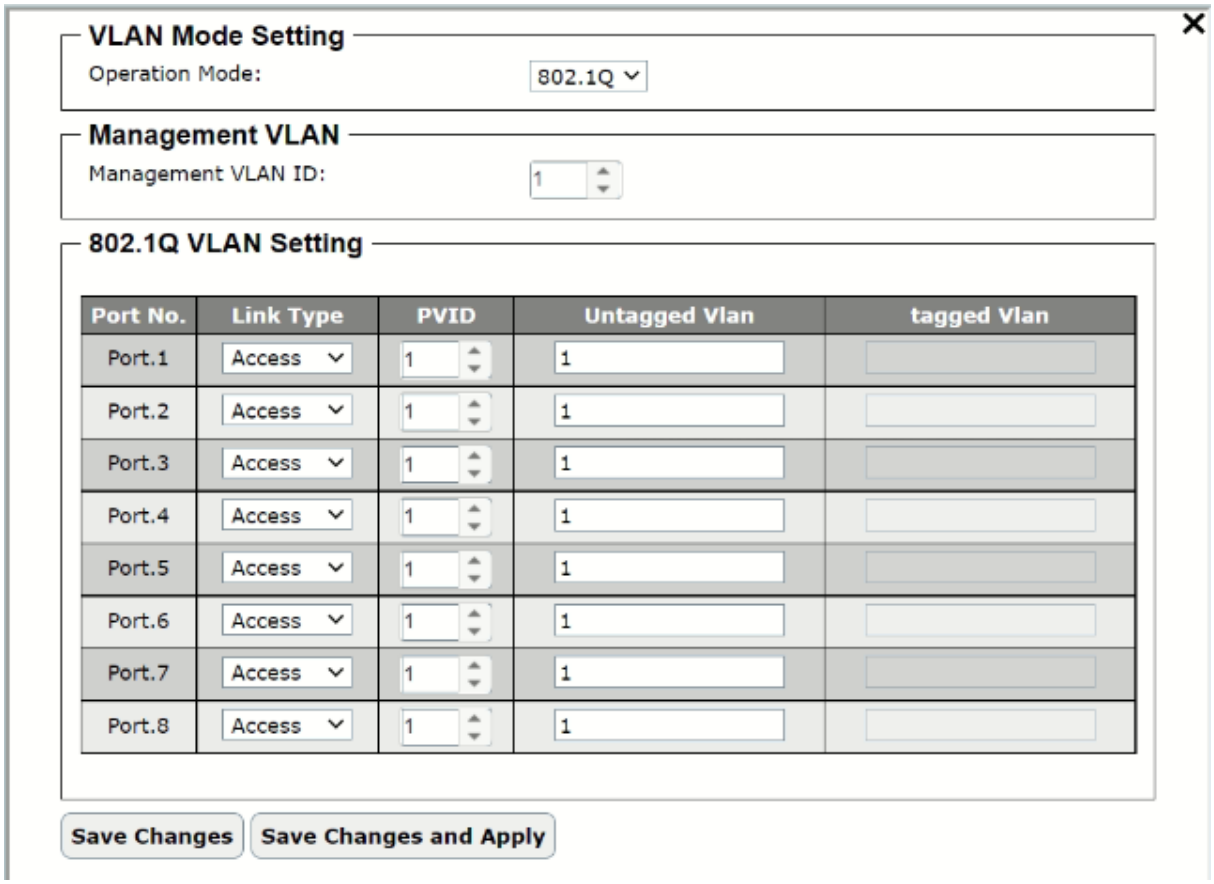


Figure 2.36 VLAN Setting Pop-up Window

2.6 RSTP

The RSTP or Rapid Spanning Tree Protocol function/feature is the fifth circular icon on the menu bar. It is the icon with a simple ring network topology. Typicall, the Spanning Tree Protocol (STP) provides a function to prevent switching loops and broadcast radiation at the OSI layer 2. A switching loop occurs in a network when there are multiple connections or redundant paths between two network switches or at least two ports are connected on both sides of the two network switches. The switching loop can create a broadcast radiation, which is the accumulation of broadcast and multicast traffics in a computer network. As broadcast and multicast messages are forwarded by bridges/switches to every port, the bridges/switches will repeatedly rebroadcast the broadcast messages, and this accumulation of traffic can flood the network. STP creates a spanning tree topology and disables those links of the network that are not part of the spanning tree, which leaves only a single active path between two nodes. This function can avoid flooding and increase network efficiency. Therefore, Atop's managed switches deploy spanning tree as a tool when the users set up connection or port redundancy or fault-tolerance in their network.

RSTP (Rapid Spanning Tree Protocol), IEEE 802.1W, is supported in Atop's EH3408 series lite-managed switches. It is an evolution of the STP, but it is still backwards compatible with standard STP. RSTP has the advantage over the STP. When there is a topology change such as link failure in the network, the RSTP will converge significantly faster to a new spanning tree topology. RSTP improves convergence on point-to-point links by reducing the Max-Age time to 3 times Hello interval, removing the STP listening state, and exchanging a handshake between two switches to quickly transition the port to forwarding state.

Figure 2.37 shows the web page of RSTP feature which includes Root Bridge Information, Bridge Setting, and Port Information. The Root Bridge Information lists information of the root, which are the Root Bridge ID, Root Priority, Root Port, Root Path Cost, Root Max Age Time, Root Hello Time, and Root Forward Delay Time. Next, the Bridge Setting shows current bridge setting which are Bridge ID, Priority, Max Age Time, Hello Time, and Forward Delay Time. Finally, the Port Information shows current setting and status of each port on the switch. Table 2.10 summarizes the description of parameters of the Root Bridge Information.

Root Bridge Information

Root Bridge ID:	00:60:E9:2D:23:FE
Root Priority:	32768
Root Port:	This bridge is Root.
Root Path Cost:	0
Root Max Age Time:	20
Root Hello Time:	2
Root Forward Delay Time:	15

Bridge Setting

Bridge ID:	00:60:E9:2D:23:FE
Priority:	32768
Max Age Time:	20
Hello Time:	2
Forward Delay Time:	15

Port Information

Port	Enable	Priority	Path Cost	OperP2P	OperEdge	Role	State
Port.1	Enable	128	200000	no	yes	Disabled	discarding
Port.2	Enable	128	200000	yes	yes	Designated	forwarding
Port.3	Enable	128	200000	no	yes	Disabled	discarding
Port.4	Enable	128	200000	no	yes	Disabled	discarding
Port.5	Enable	128	200000	no	yes	Disabled	discarding
Port.6	Enable	128	200000	no	yes	Disabled	discarding
Port.7	Enable	128	200000	no	yes	Disabled	discarding
Port.8	Enable	128	200000	no	yes	Disabled	discarding

Figure 2.37 RSTP Feature

Table 2.10 Description of Root Bridge Information

Label	Description
Root Bridge ID	MAC address of the root of the spanning tree
Root Priority	Root's priority value: the switch with highest priority has the lowest priority value and it will be elected as the root of the spanning tree.
Root Port	Indicate the status of the root such as "This bridge is root"
Root Path Cost	Root's path cost is calculated from the data rate of the switch's port.
Root Max Age Time	Root's maximum age is the maximum amount of time that the switch will maintain protocol information received on a link.
Root Hello Time	Root's hello time which is the time interval for RSTP to send out a hello message to the neighboring nodes to detect any change in the topology.
Root Forward Delay	Root's forward delay is the duration that the switch will be in learning and listening states before a link begins forwarding.

To configure RSTP, the user can click on the gear icon of the Bridge Setting to bring up the RSTP Setting pop-up window as shown in Figure 2.38. There are three sections on this window: RSTP Setting, Bridge Setting, and Port Setting. First, the user can select to enable the RSTP Mode. Then, the user can continue to adjust the parameters of the bridge under the Bridge Setting section. The Priority can be set to the value from 0 to 61440. The Max Age Time can be set to value from 6 to 40. The Hello Time is fixed to 2. The Forward Delay Time can be set to value from 4 to 30. Finally, the Port Setting section contains the table with the list of ports on the managed switch. Each port can be Enable or Disable. The Priority of the port can be set to a value from 0 to 240. The Path Cost can be set to 0 for Auto or other value from 1 to 200000000. The P2P can be selected from True, False, or Auto. The Edge can either be True or False. After you finished, clicking on the Save Changes button to save any changes or clicking on the Save Changes and Apply button to save and apply the setting.

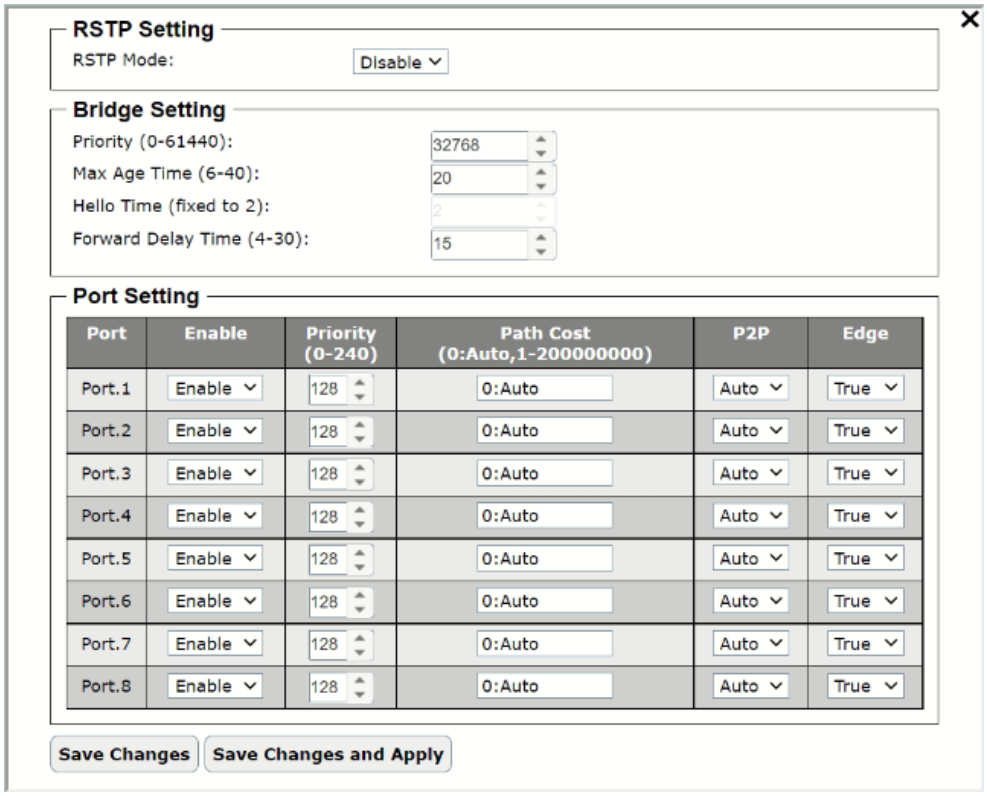


Figure 2.38 RSTP Setting Pop-up Window

2.7 Management

The Management function is the sixth circular icon on the menu bar. It is the icon with gear and person. The Management function has three features which are Account, HTTPS, and SNMP as shown in Figure 2.39. These features allow the user to manage the accounts, enable secure HTTP for web interface, and set up the SNMP protocol.

Figure 2.39 Management Function

2.7.1 Account feature

The Account feature is shown in Figure 2.40 with a list of account or user on the managed switch. It is presented in a format of table with two columns: Username and Permission. To add or delete an account or user, the user can click on the gear icon to bring up the Account Setting pop-up window as shown in Figure 2.41. For each new user, please enter the User Name, Password, Confirm Password and select the Permission Level then click the Add User button. To remove a user from the lsit, entering all information then click the Delete User button.

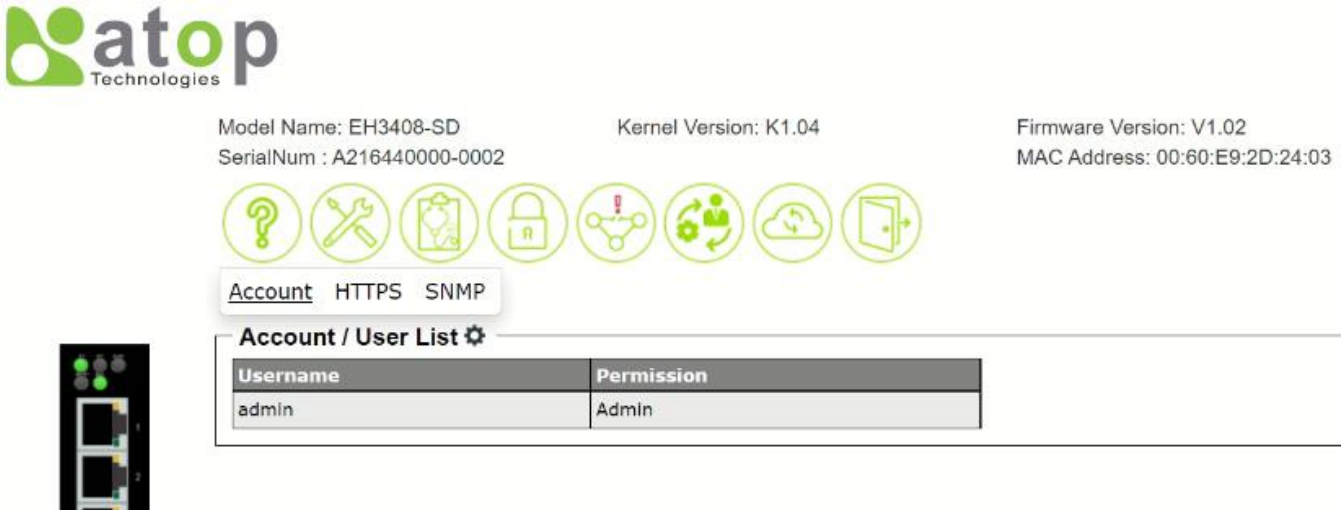


Figure 2.40 Accout Feature

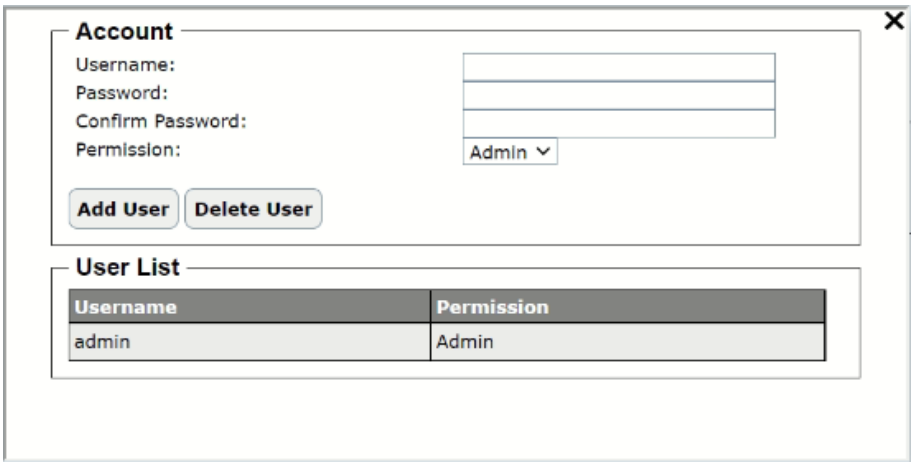


Figure 2.41 Accout/User List Pop-up Window

2.7.2 HTTPS feature

The HTTPS or HyperText Transfer Protocol Secure feature is another feature under the Management function. This page presents the current setting of HTTPS for the managed switch's web interface as shown in Figure 2.42. To enable the HTTPS, the user can click on the gear icon to bring up the HTTPS Setting pop-up window as shown in Figure 2.43. Next checking the Enabled box to redirect web interface access to HTTPS protocol. After you finished, clicking on the Save Changes button to save any changes or clicking on the Save Changes and Apply button to save and apply the setting.

Figure 2.42 HTTPS Feature

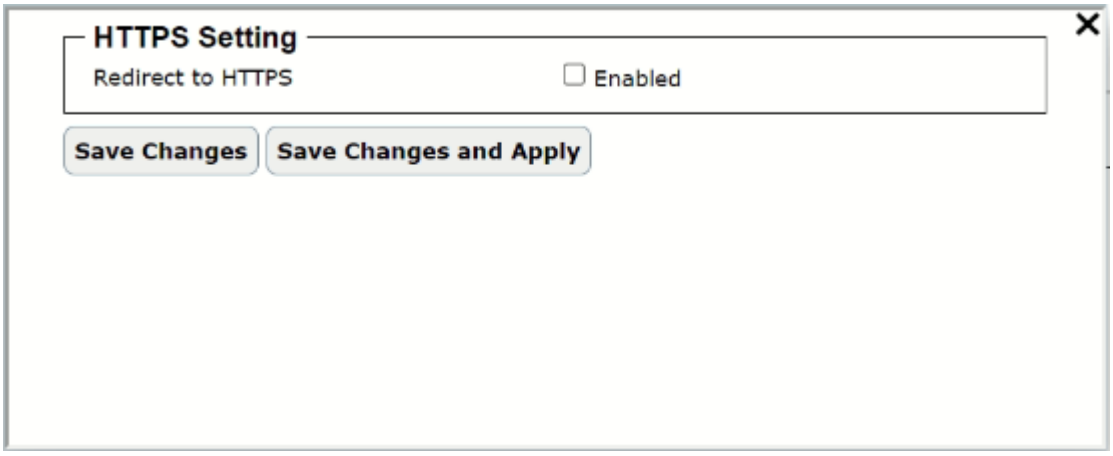


Figure 2.43 HTTPS Setting Pop-up Window

2.7.3 SNMP feature

Simple Network Management Protocol (SNMP) is a protocol for managing devices on IP networks. It exposes management data in the form of variables on the managed systems which describe the system configuration. These variables can then be queried or defined by the users. The SNMP is used by network management system or third-party software to monitor devices such as managed switches in a network to retrieve network status information and to configure network parameters. The Atop's managed switch support SNMP and can be configured through this feature under the Management function.

Figure 2.44 shows the SNMP feature' s web page. It consists of four sections: SNMP Mode Setting, SNMP v1/v2c Agent Setting, SMPT v1/v2c Trap Setting and SNMP v3 Configuration. The current version of SNMP configured to run on the switch can be viewed behind the SNMP Mode Setting. The SNMP Agent Version can be set to either SNMP v1/v2c or SNMP v3. Note that depending on the SNMP Agent Version selection some of the sections will be

active while another section will be grey out. For example, when SNMP Agetn Version is set to SNMP v1/v2c, SNMP v1/v2c Agent Setting and SNMP v1/v2c Trap Setting will be available to configure as shown in Figure 2.44.

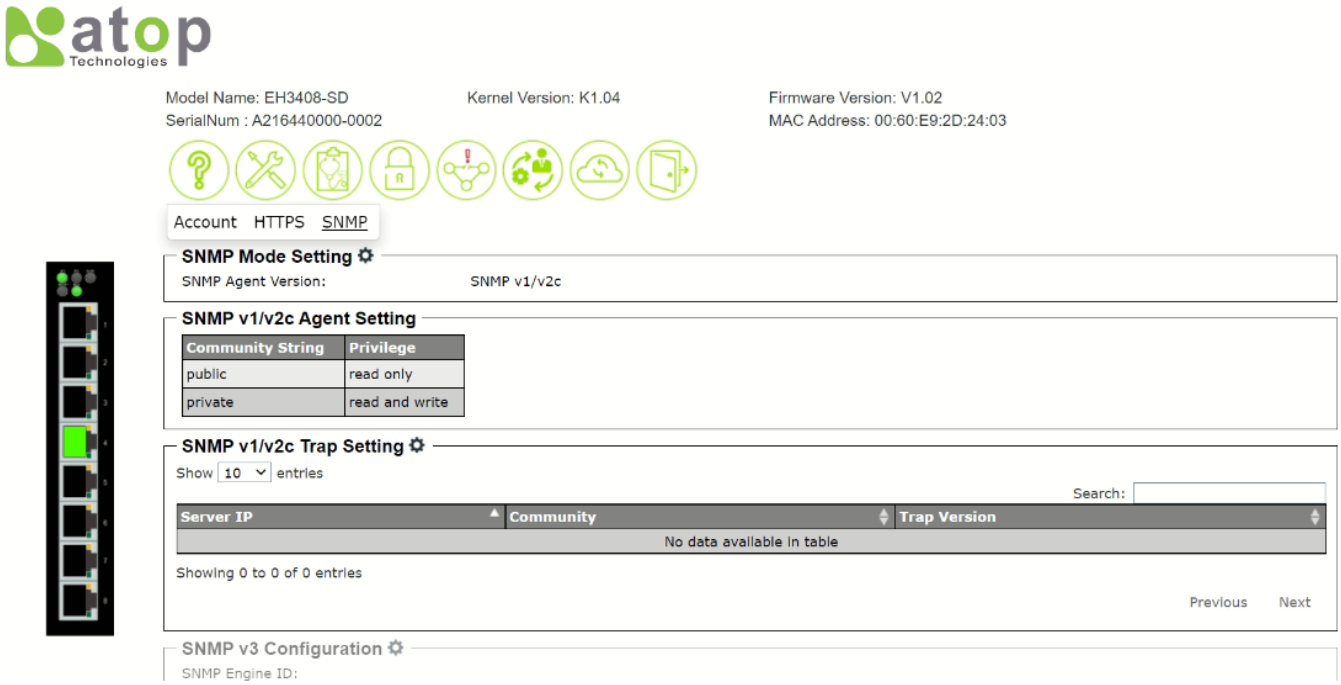


Figure 2.44 SNMP Feature

To select the SNMP Agent Version, the user can click on the gear icon next to the SNMP Mode Setting to bring up the pop-up window as shown in Figure 2.45. When the SNMP v1/v2c is selected, the Community String and Privilege of each Community String can be managed as shown in the figure. After you finished, clicking on the Save Changes button to save any changes or clicking on the Save Changes and Apply button to save and apply the setting.

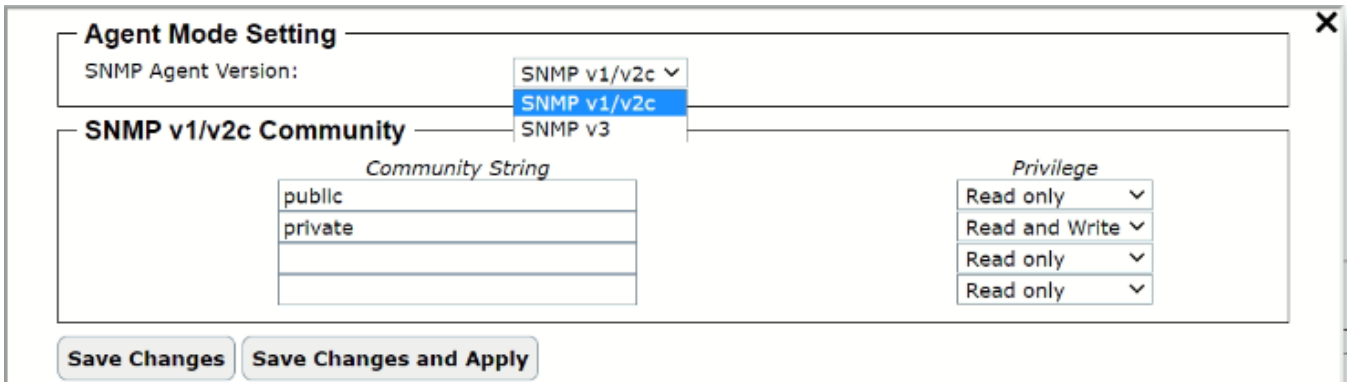


Figure 2.45 SNMP Agent Mode and SNMP v1/v2c Community Management

While SNMP Agent Version is set as SNMP v1/v2c, the SNMP v1/v2c Trap Setting section is active. The user can configure Trap Server by clicking on the gear icon next to the SNMP v1/v2c Trap Setting. A pop-up window as shown in can be used to manage the trap server by adding Trap Server IP and Community, and selectinv of Trap Version. After filled in and selecting all fields, the user can click Add button to add an entry into SNMP v1/v2c Community table shown in the lower part of the pop-up window. The user can also delete an entry from the SNMP v1/v2 Community table by selecting an entry and then clicking on the Remove button.

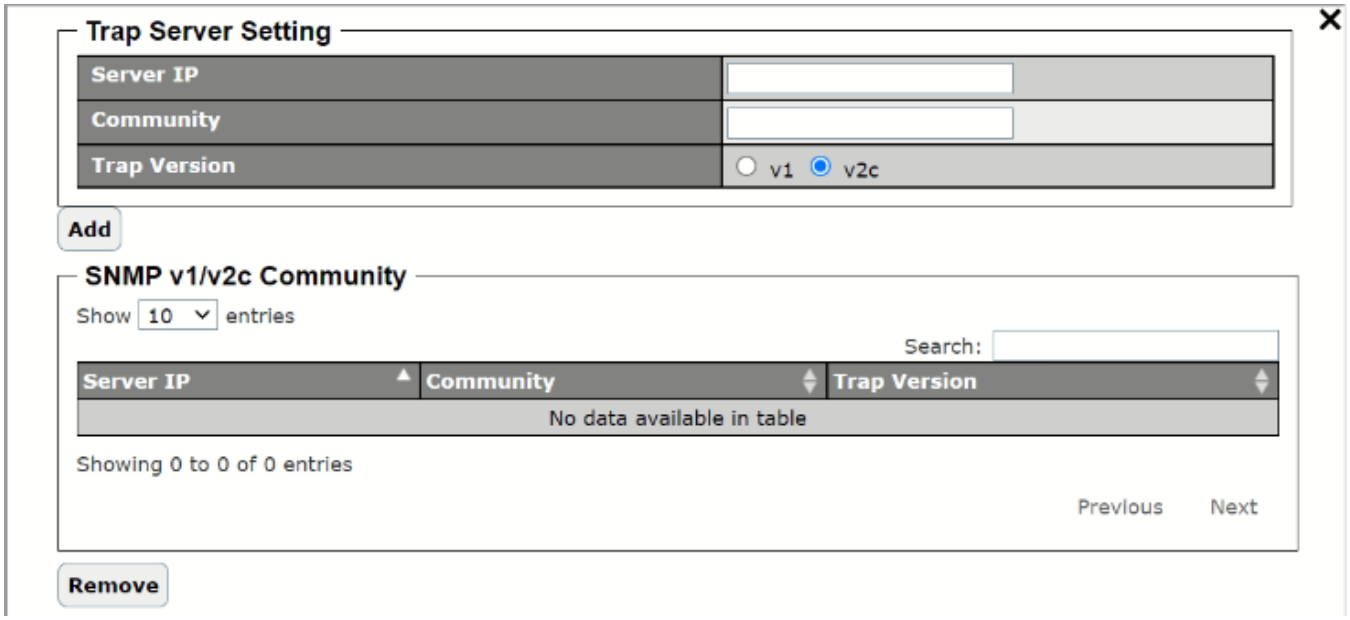


Figure 2.46 SNMP v1/v2c Trap Management

If SNMP Agent Version is set to SNMP v3, the SNMP v3 Configuration and SNMP v3 Trap sections will become active as shown in Figure 2.47. This web page provides detailed setup of SNMP v3 Configuration and SNMP v3 Trap Server.

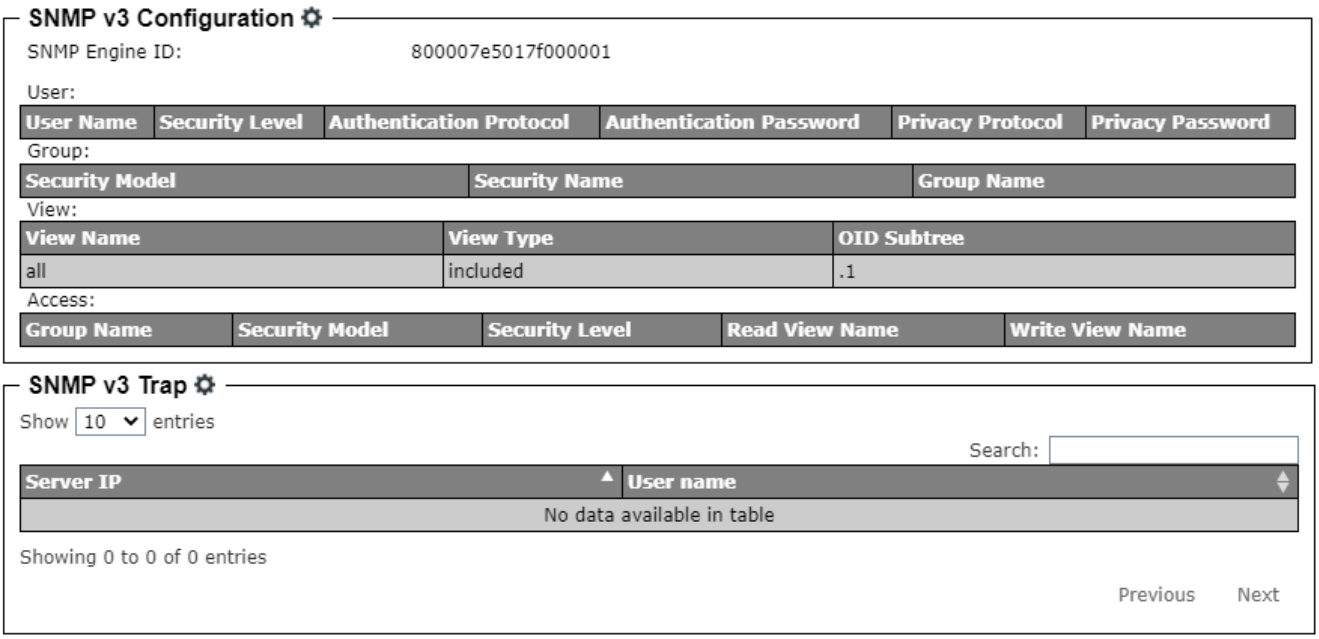


Figure 2.47 SNMP v3 Feature

To configure SNMP v3, the user can click the gear icon next to the SNMP v3 Configuration to bring up the pop-up window as shown in Figure 2.48. On this window, there are four sections: SNMP v3 User Configuration, SNMP v3 Group Configuration, SNMP v3 View Configuration, and SNMP v3 Access Configuration. Under the SNMP v3 User Configuration, the user can add new SNMP's user by filling new User Name and set Security Level, Authentication Protocol, Authentication Password, Privacy Protocol and Privacy Password. After finished entering all information, click Add button to add the new SNMP's user. Note that you can delete existing user by clicking on Delete button in front of that particular User Name. SNMP v3 Group, View, and Access can also be configured in the same manner

as described for SNMP v3 User Configuration. After you finished, clicking on the Save Changes button to save any changes or clicking on the Save Changes and Apply button to save and apply the setting.

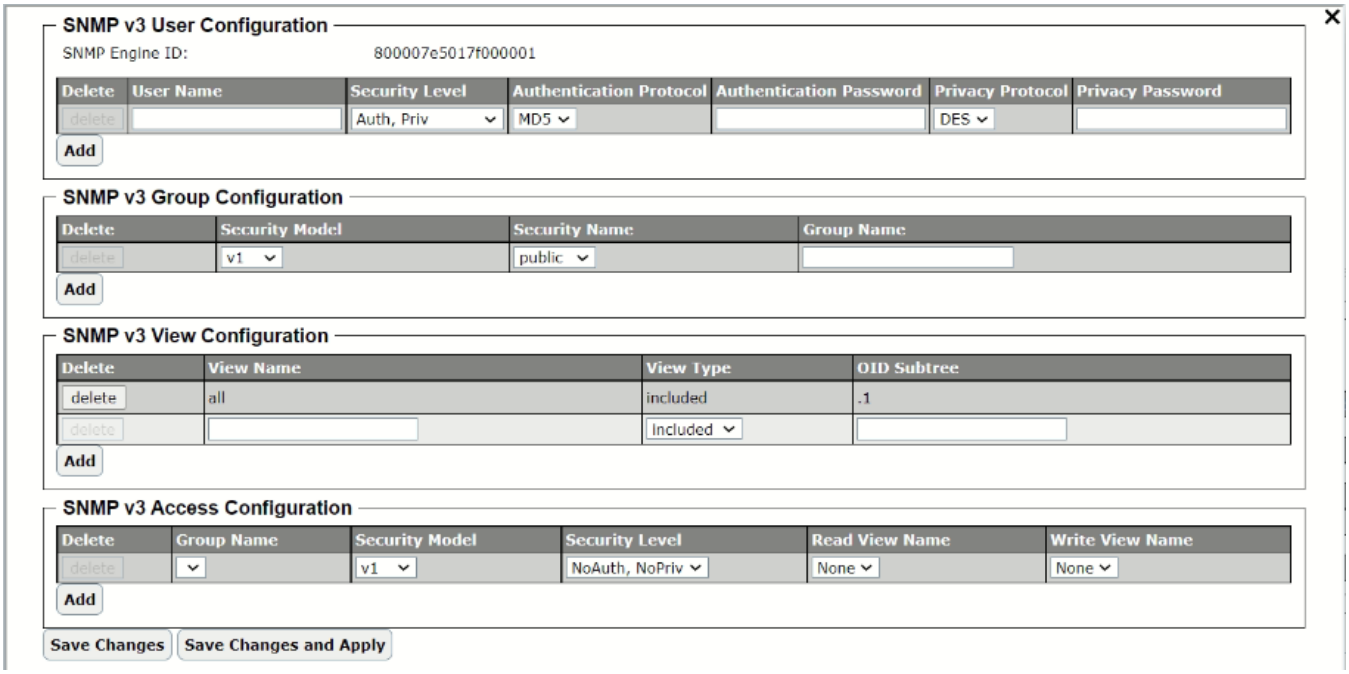


Figure 2.48 SNMP v3 Configuration Pop-up Window

To configure SNMP v3 Trap Server, the user can click the gear icon next to the SNMP v3 Trap in Figure 2.47 to bring up another pop-up window as shown in Figure 2.49. On this window, the user can set the SNMP v3 Trap Server IP address and choose the User name previously configured in SNMP v3 User Configuration. After clicking on Add button, the new entry will be added to the SNMP v3 Trap List shown in the lower part of the window. You can delete an entry from SNMP v3 Trap List by selecting that particular entry and clicking on the Remove button.

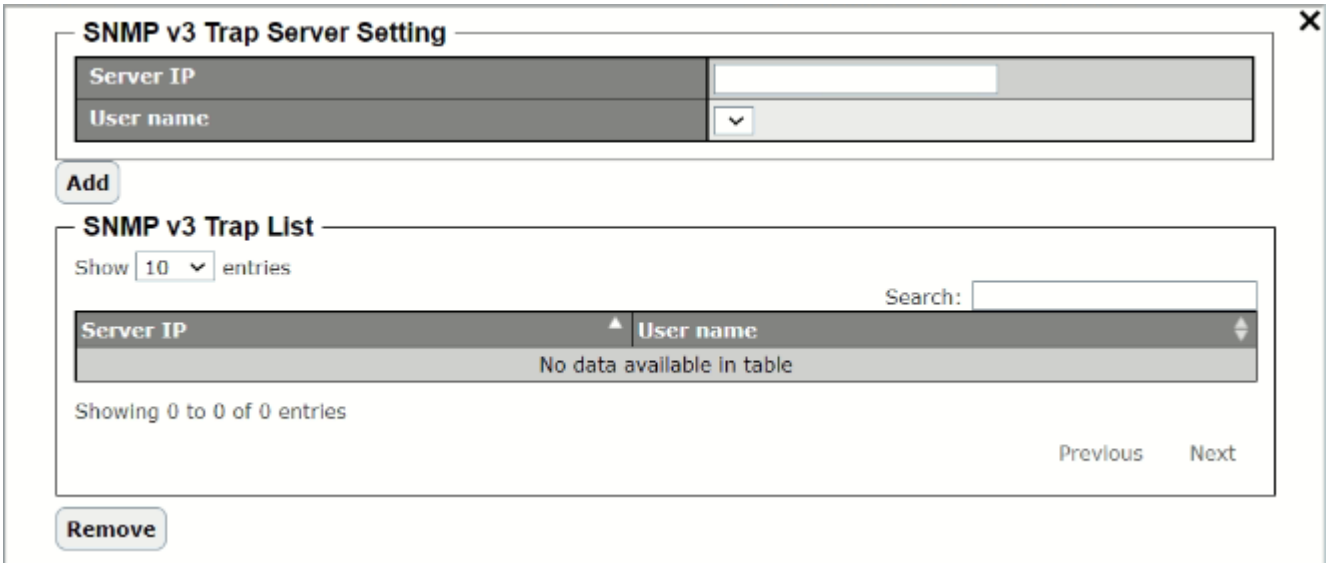


Figure 2.49 SNMP v3 Trap Server Setting Pop-up Window

2.8 Maintenance

The Maintenace function is the seventh circular icon on the menu bar. It is the circular icon with a cloud picture. This function contains important features that allow the user to maintain the operation of the EH3408 series lite-managed switch. The Mainteance function includes the following features as shown in Figure 2.50: Firmware, Backup/Restore, Backup/Restore (storage device), Factory Default, Reboot, and Apply All.

Figure 2.50 Maintenace Function

2.8.1 Firmware feature

The firmware feature under the Maintenace function shows two information about the managed switch: firmware and image bank. The user can check the current boot Loader Version, Kernel Virsion, and Firmware Version under the Upgrade Firmware section. On the Select Image Bank section, there are information related to Image Banks. The EH3408 device has two or dual image banks. One of the image banks is set as Current Image Bank or is the one currently applied to the switch. The other image bank is the backup. If the user upgrades a firmware to the switch, the new firmware image will be updated to the backup bank. When the upgrade progress completed, the device will reboot. After rebooting, the upgraded bank will be applied. The originally applied image bank before rebooting will become the backup image bank.

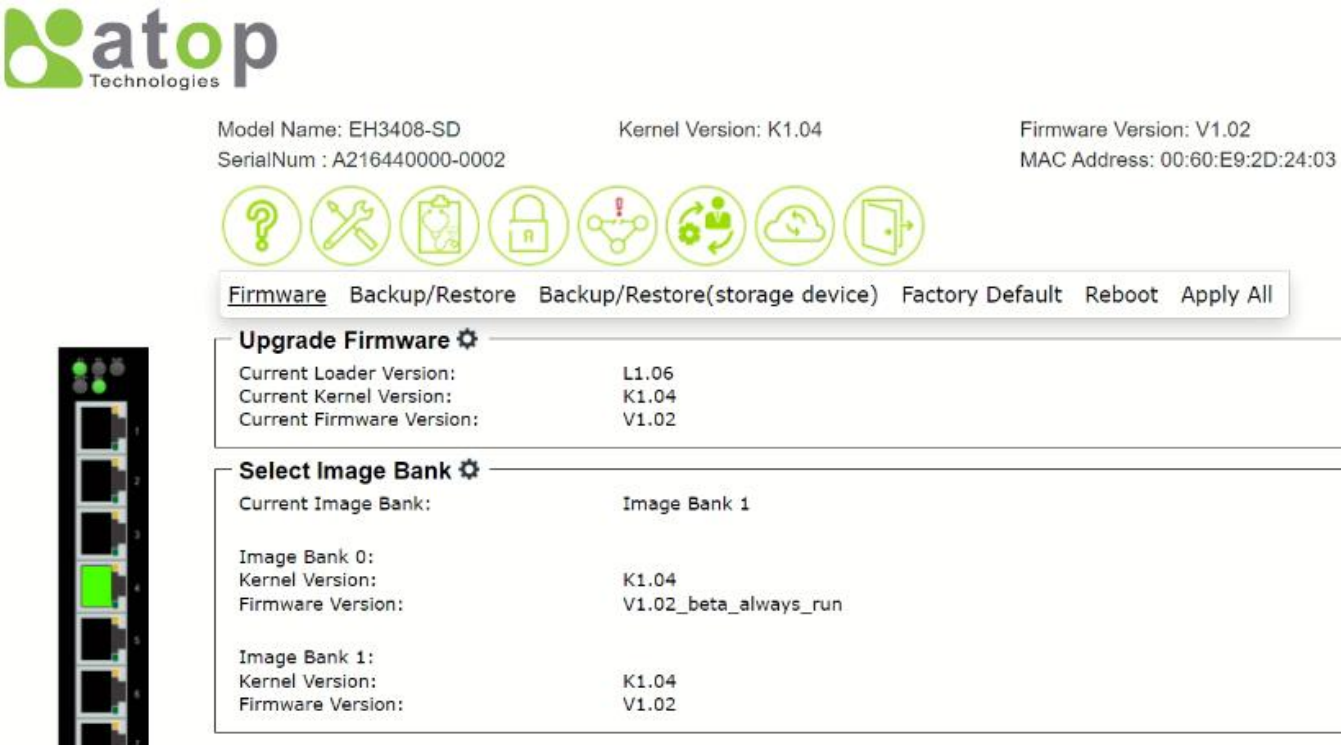


Figure 2.51 Firmware Feature

In the process of traditional firmware update and during firmware upgrade progress on a device, the system might suffer from unpredictable disconnection or interruption of power supply. This may lead to unrecoverable damage on the device and it will have to be sent for repair. With dual image banks in EH3408 series, even though the system

suffered from unpredictable disconnection or electricity outage during the period of firmware update, the system can still recover and operate properly on the original firmware version or on the new firmware version that user have updated. That is EH3408 series equipped with dual image banks comes with this hardware design for Firmware Update Protection.

To upgrade the firmware, the user can click on the gear icon next to the Upgrade Firmware. This will bring up the Upgrade Firmware pop-up window as shown in Figure 2.52. The users can download a new firmware from Atop's website and save it in a local computer. Then, the user can choose a local firmware file from a file chooser by clicking on Browse… button next to the Select Firmware File option. Note that a valid firmware typically has a ".bin" extension. The user can check the box in front of Attempt to Preserve Settings option if the user would like to keep the current configuration after the firmware is upgraded. To start the upgrading process, the user can click on the Upgrade Now button.

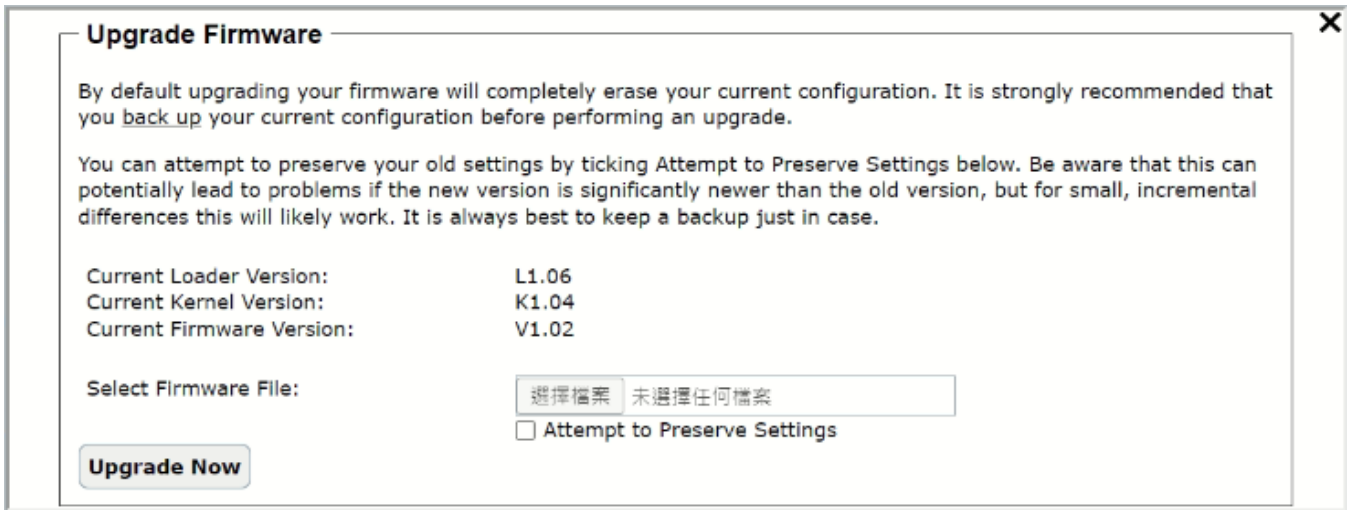


Figure 2.52 Upgrade Firmware Pop-up Window

To select the current Image Bank, the user can click on the gear icon next to the Select Image Bank to bring up the pop-up window as shown in Figure 2.53. When you selected the desired Image Bank by clicking on the radio button in front of the Image Bank 0 or 1, then clicking on the Reboot Now button to apply the selection.

Figure 2.53 Select Image Bank Pop-up Window

2.8.2 Backup/Restore feature

The Backup/Restore feature under the Maintenace function as shown in Figure 2.54 supports the backup and restore of managed switch's configuration.

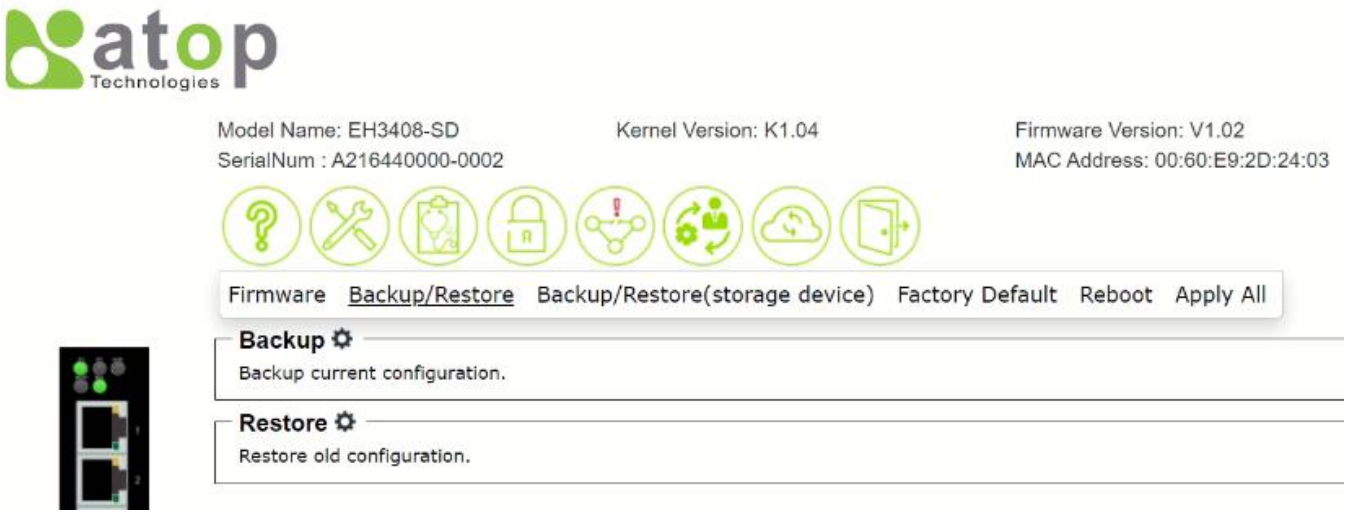


Figure 2.54 Backup/Restore Feature

To create a backup of configuration, the user can click on the gear icon next to the Backup to bring up the pop-up window as shown in Figure 2.55. After clicking on the Get Backup Now button, a backup configuration file will be download and save on your local device. This backup configuration file then can be used to restore the configuration of the managed switch in the future.

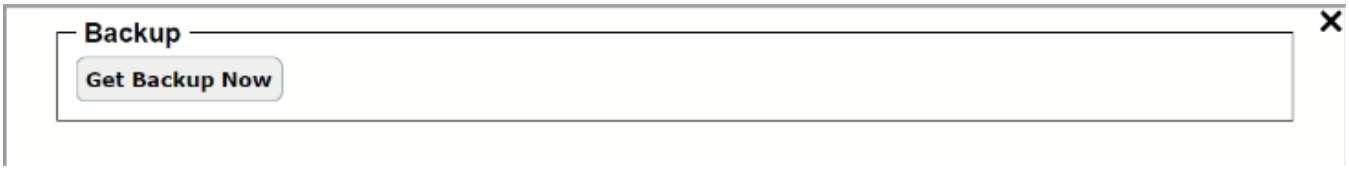


Figure 2.55 Backup Pop-up Window

To restore a configuration file, the user can click on the gear icon next to the Restore to bring up the pop-up window as shown in Figure 2.56. Next, the user can choose a configuration file from your local computer by clicking on Browse... button. Additionally, the user can enable or disable the Keep username & password and Keep IP options to preserve the setting of username and password and to preserve the setting of IP address of the switch after configuration is restored, respectively. To start the restoration process, clicking on the Restore Configuration Now button.

Figure 2.56 Restore Pop-up Window

2.8.3 Backup/Restore (storage device) feature

The Backup/Restore (storage device) feature under the Maintenance function is an alternative feature that allows the user to backup or restore configuration file to or from the storage device inside the EH3408 chasis. Note that Backup/Restore feature in previous subsection download or load the configuration file to and from the local host computer. The storage device can be a Micro-SD card (for EH3408ls and EH3408s) or USB storage device (EH3408lu and EH3408u) attached to the EH3408 device. The supported formats of the storate device are FAT32 and exFAT.

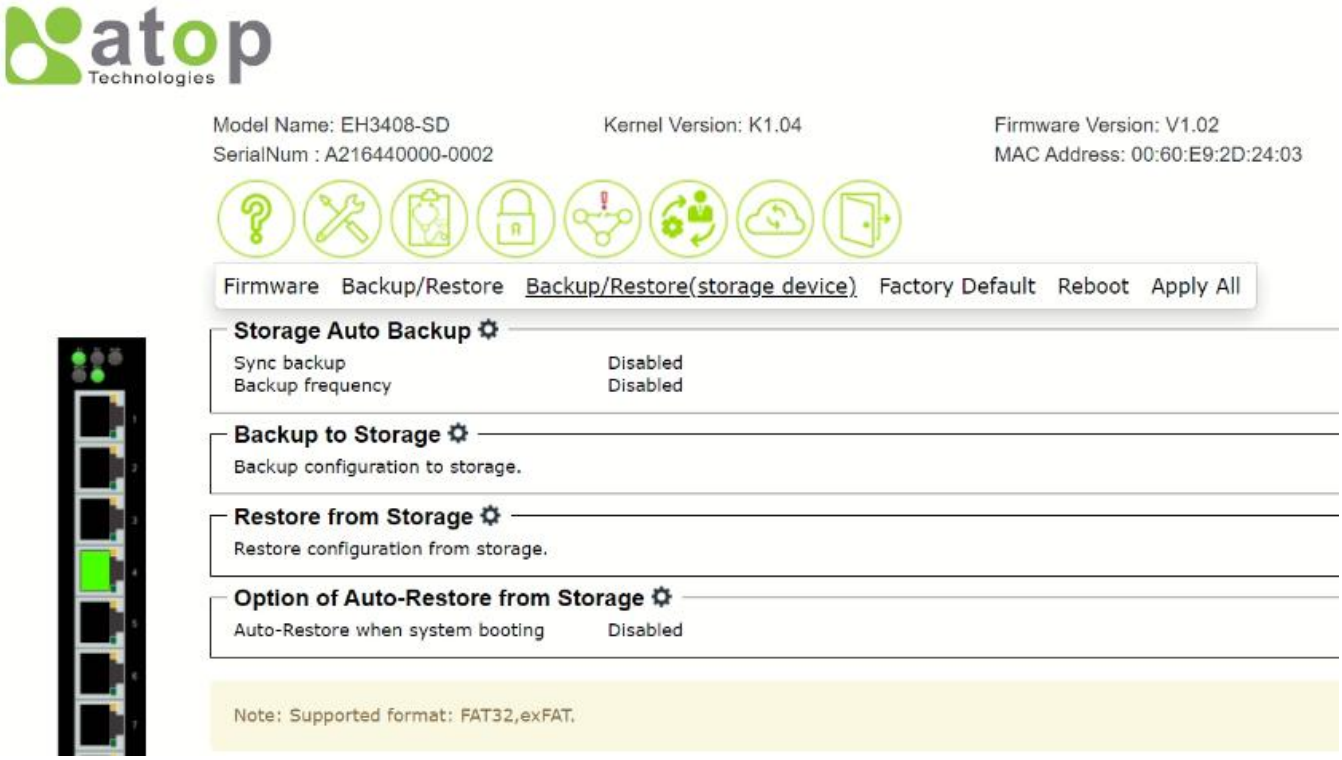


Figure 2.57 Backup/Restore (storage device)

To setup the automatic backup, the user can click the gear icon next to the Storage Auto Backup to bring up the pop-up window as shown in Figure 2.58 for EH3408lu and EH3408u or as shown in Figure 2.59 for EH3408ls and EH3408s. There are two options on this window which are Sync backup and Backup frequency. After finished setting the options, click on the Save button.

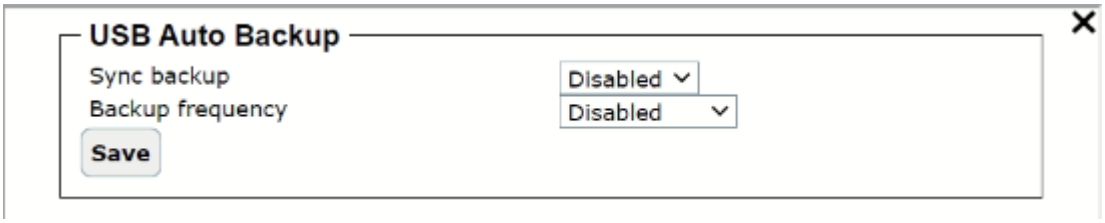


Figure 2.58 USB Auto Backup Pop-up Window for EH3408lu and EH3408u

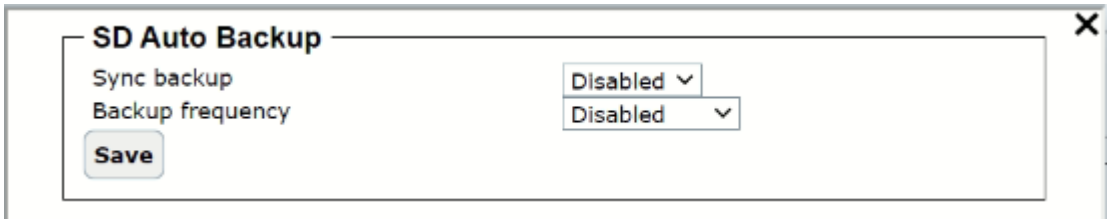


Figure 2.59 SD Auto Backup Pop-up Window for EH3408ls and EH3408s

To start backup the configuration file to the storage device, the user can click on the gear icon next to Backup to Storage. This will bring up the pop-up window as shown in Figure 2.60 and in Figure 2.61 for the managed switch with USB storage device and with Micro-SD storage device, respectively. To check the status of either USB or Micro-SD device, press the Read Device button. To back up the configuration to the storage device, click on the Get Backup Now button.

Figure 2.60 Backup to USB Storage Device Pop-up Window for EH3408lu and EH3408u

Figure 2.61 Backup to Micro-SD Storage Device Pop-up Window for EH3408ls and EH3408s

To restore a configuration file from storage device, the user can click on the gear icon next to Restore from Storage to bring up the pop-up window as shown in Figure 2.62 for EH3408lu and EH3408u or as shown in Figure 2.63 for EH3408ls and EH3408s. To check the status of either USB or Micro-SD device, press the Read Device button. Then, the user can choose a restore file from the Select a restore file option. The user also has two additional options to enable or disable the Keep username & password and Keep IP. These optons can preserve the current setting on the username, password and IP address of the managed switch after the restoration of the configuration file. To restore the configuration from the storage device, click on the Restore Configuration Now button.

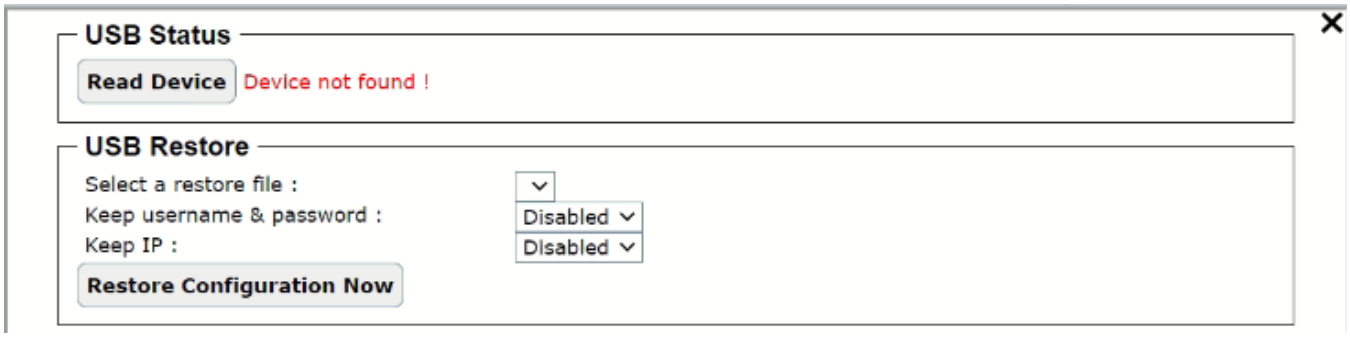


Figure 2.62 Restore from USB Storage Device Pop-up Window for EH3408lu and EH3408u

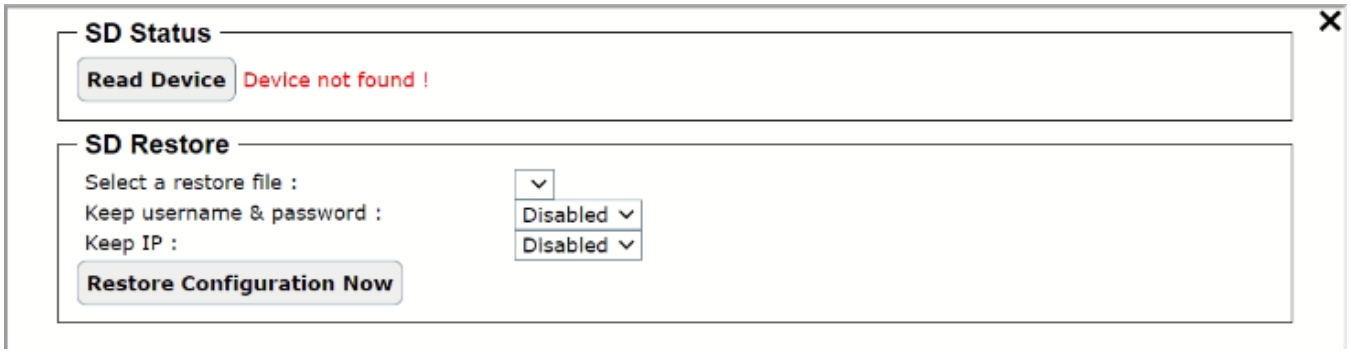


Figure 2.63 Restore from Micro-SD Storage Device Pop-up Window for EH3408ls and EH3408s

To set the automatic restore of the configuration file from storage device while the managed switch is booting, the user can click on the gear icon next to Option of Auto-Restore from Storage. This will bring up the pop-up window as shown in Figure 2.64 for EH3408lu and EH3408u or as shown in Figure 2.65 for EH3408ls and EH3408s. On this window, the user can select Disabled or Enabled the Option from the drop-down selection and then click Save button.

Figure 2.64 Option of Auto-Restore from USB Pop-up Window for EH3408lu and EH3408u

Figure 2.65 Option of Auto-Restore from Micro-SD Pop-up Window for EH3408ls and EH3408s

2.8.4 Factory Default feature

The Factory Default feature under the Maintenace function allows the user to reset the device to the original or factory default configuration. The Factory Default web page is shown in Figure 2.66. To perform the factory default setting, the user can click on the gear icon next to the Factory Default to bring up the pop-up window as shown in

Figure 2.67. Then, clicking on the Restore Default Configuration Now button to restore the configuration of the device to the factory default setting.

Figure 2.66 Factory Default Feature

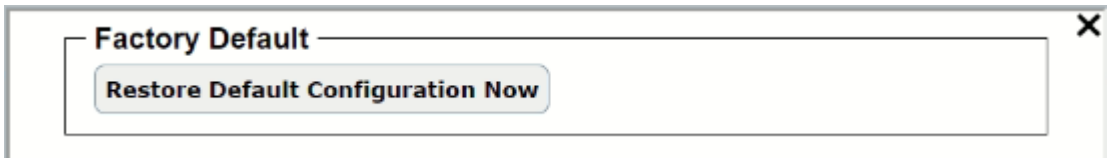


Figure 2.67 Factory Default Pop-up Window

2.8.5 Reboot feature

The Reboot feature under the Maintenance function supports the rebooting of the managed switch through the web GUI. The Reboot feature is shown in Figure 2.68. To reboot the device, clicking on the gear icon next to Reboot to bring up the pop-up window as shown in Figure 2.69. Then, clicking on the Reboot Now button to reboot the device.

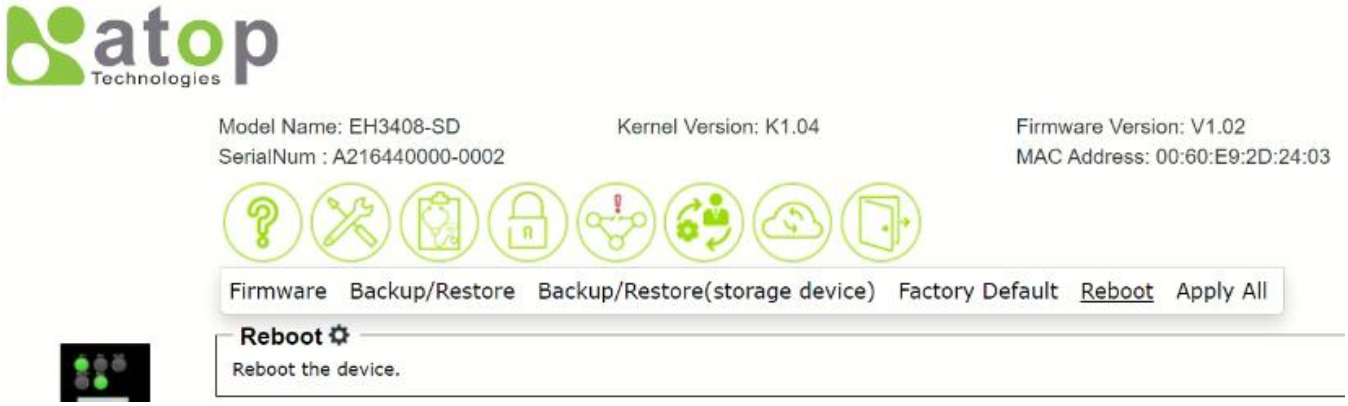


Figure 2.68 Reboot Feature

Figure 2.69 Reboot Pop-up Window

2.8.6 Apply All feature

The Apply All feature under the Maintenance function as shown in Figure 2.70 enables that all saved configuration of the device will be applied after issuing this command. To issue the Apply All command, clicking on the gear icon next to the Apply All to bring up the pop-up window as shown in Figure 2.71. After clicking on the Apply All button, the system wil apply all saved configuration to the device.

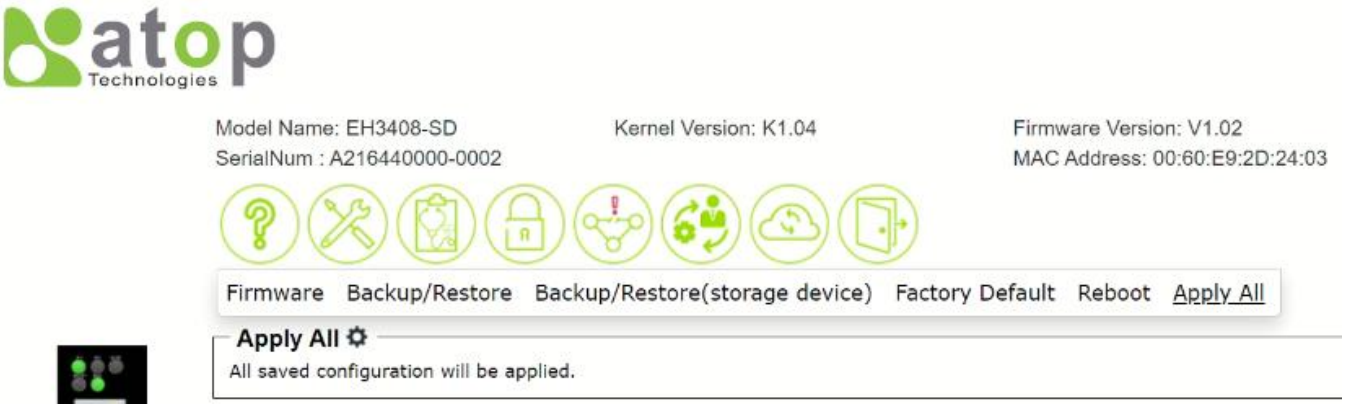


Figure 2.70 Apply All Feature

Figure 2.71 Apply All Pop-up Window

2.9 Logout

To logout of the managed switch, the user can click on the Logout icon which is the last circular icon with an opened door as shown in Figure 2.72. After clicked on the icon, the user will be returned to the login page as shown in Figure 2.2.

Figure 2.72 Logout Feature

Atop Technologies, Inc.

www.atoponline.com

TAIWAN HEADQUARTER and INTERNATIONAL SALES:

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Chupei City, Hsinchu County
Taiwan, R.O.C.
Tel: +**886-3-550-8137**
Fax: +**886-3-550-8131**
sales@atop.com.tw

ATOP CHINA BRANCH:

3F, 75th, No. 1066 Building,
Qingzhou North Road,
Shanghai, China
Tel: +86-21-64956231