Atop Technologies, Inc.

AW5601 Series
Industrial Access Point

User Manual

V1.0

7th March 2024

*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
sales@atop.com.tw
www.atoponline.com

Technical Support Contact Information

www.atoponline.com/request-support

Asia & Australia
Jopson Li
Tel: +886-918-694-073
eMail: jopsonli@atop.com.tw

China
Sam Xia
Tel: +86-21-649562-31
eMail: sales@atop.com.tw

Europe
Alessio Longhini
Tel: +39-348-26-28-727
eMail: alessio@atop.com.tw

Germany
Mattel Tabarelli de Fatis
Tel: +886-919-209-290
eMail: matteo.tabarelli@atop.com.tw

India & SAARC
Prashant Mishra
Tel: +91-80-492-06308
eMail: prasant.m@atop.com.tw

Indonesia
Anisah Ambarwati
Tel: +62-896-761-93026
eMail: anisah@atop.com.tw

Italy
Mattel Tabarelli de Fatis
Tel: +886-919-209-290
eMail: matteo.tabarelli@atop.com.tw

Japan
Keiichi Sagami
Tel: +090-2284-9632
eMail: sakagami@atop.com.tw

Latin America
Jopson Li
Tel: +886-918-694-073
eMail: jopsonli@atop.com.tw

Middle East & Africa
Prashant Mishra
Tel: +91-80-492-06308
eMail: prasant.m@atop.com.tw

Russia & CIS
Timur Dautov
Tel: +7-985-855-1056
eMail: timur@atop.com.tw

Taiwan
Tony Lin
Tel: +886-968-386876
eMail: tonylin@atop.com.tw

USA & Canada
Prashant Mishra
Tel: +91-80-492-06308
eMail: prasant.m@atop.com.tw

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 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 you 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. For any related problems, please contact your local distributor. If they are unable to assist you, please redirect your inquiries to www.atoponline.com.

Documentation Control

Author:	Non-switch Team
Revision:	1.0
Revision History:	Feature/Title Update
Creation Date:	20 November 2023
Last Revision Date:	7 March 2024
Document Status:	Released

Table of Contents

List of Figures

List of Tables

1 Introduction

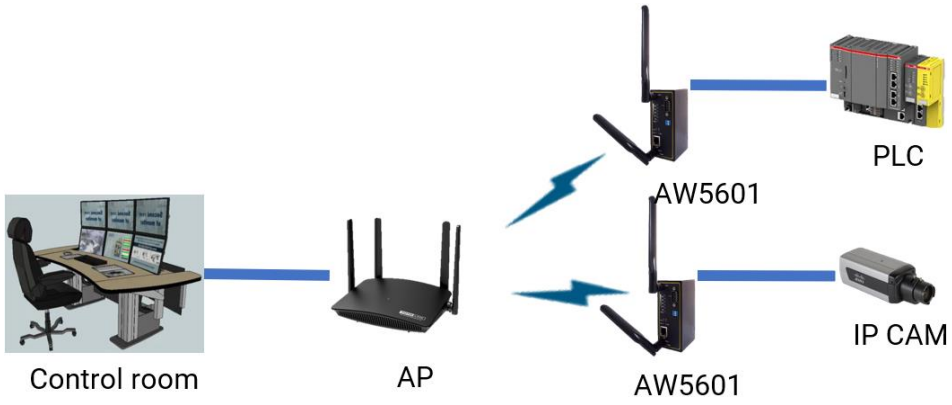
1.1 *Overview*

Atop's AW5601 series are the product line of wireless product for applications in harsh environment. It is robust enough to operate at temperatures ranging from -20°C to 70°C. The ease of installation makes it attractive because it utilizes a DIN-Rail for fixing itself to virtually any surface in workplace. Reliability is a key factor of AW5601 when wireless solution is needed. The small dimension of AW5601 casing is also ideal for small space while it can still provide real-time control and exceptional networking performance.

The AW5601 is designed to provide wireless connectivity to clients and mobile stations or other ATOP's industrial networking products creating a complete solution for your industrial wireless networking. It can be operated as an access point (AP), a wireless distribution system (WDS) bridge, and an AP client. The AW5601 supports IEEE 802.11 a/b/g/n/ac wireless connectivity standards.

As an example, user can connect serial devices to ATOP's Wireless Serial Device Server (e.g. SW55XX series) and then connect the serial device server with the AW5601 Industrial Wireless Access Point. Therefore, this configuration allows the serial devices to be access over a wireless local area network (WLAN). Another example is depicted in Figure 1 where the AW5601 is operated in AP client mode and associated with another WLAN AP called AP1. In this example, the personal computer (PC) and the IP camera which are connected to ATOP's industrial Managed Ethernet Switch (e.g. EH/EHG/EMG/RHG Series) can be wirelessly connected the control room on the other side of the network.

Figure 1. An Application of Industrial Wireless Access Point in WLAN.



1.2 *Product Features*

AW5601 Platform

- 1 x RJ45 for 10/100/1000Mbps BaseT LAN
- Different operating modes and topology options (AP mode, WDS mode, and Client mode)
- Supporting of the most popular wireless local area network standards IEEE 802.11a/b/g/n/ac
- Industrial EMC protection, -20ºC~70ºC wide-range temperature operation
- Rugged metal case with a wall or DIN-Rail mount
- PoE PD support for flexible deployment
- Power supply input supporting 12~48VDC
- Flash-Roaming with less than 50ms latency
- PROFINET transparent mode support
- Easy configuration through embedded web server interface or ATOP's Windows®-based configuration utility program called **Device Management Utility®**
- Firmware upgradable through embedded web server interface or ATOP's **Device Management Utility®**

2 Getting Started

This chapter explains how to access the AW5601 for the first time.

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 *Default Factory Settings*

Below is the list of default factory settings. This information will be used during the login process. Make sure that the computer accessing the AW5601 has an IP address in the same subnet and the subnet mask is the same.

AW5601 default network parameters are listed in the table below.

Table 1. Network Interfaces Default Settings

IP Address	Subnet Mask	Default Gateway
10.0.50.200	255.255.0.0	0.0.0.0

Its Web GUI login default Username and password are listed in the table below. Please pay attention that username and password are case sensitive.

Table 2. Login Default Settings

Login Parameter	**Default Values**
Username	admin
Password	default

2.1.1 The Reset Button

If you forget the password or cannot access the Web Configurator of the device, you can use the RESET button to restore the factory default configuration file. This means you will lose all of your configurations after the resetting. The password will also be reset to the factory default setting (see the device label), and the LAN IP address will be "192.168.1.1". To reset the device, follow these steps:

1. Make sure the POWER LED is on (not blinking).
2. Press the "Reset" button on the panel from the same side of the terminal bolck for **5** seconds to restore the factory default settings. When the Wi-Fi and Ethernet LED begin to blink, the device is starting to restore its factory default setting.

3.

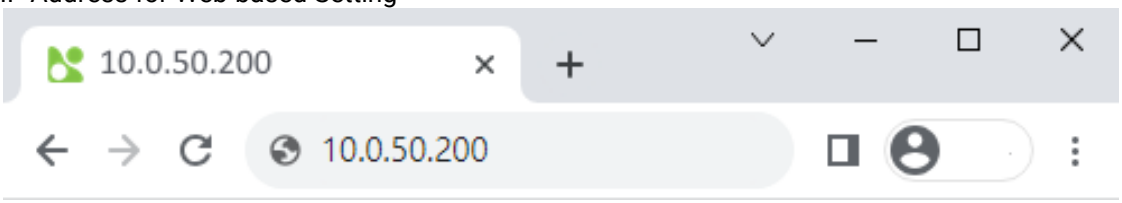
2.2 *Login Process and Main Window Interface*

2.2.1 Login Process

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

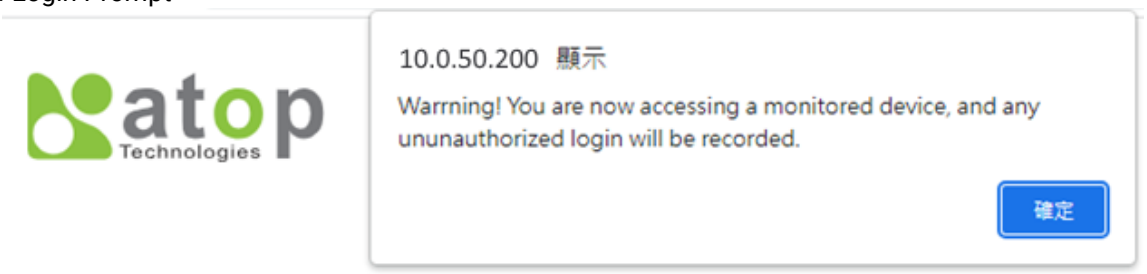
1. Launch a web browser.
2. Type in the device's IP address (e.g. http://10.0.50.200), as shown in Figure 2.

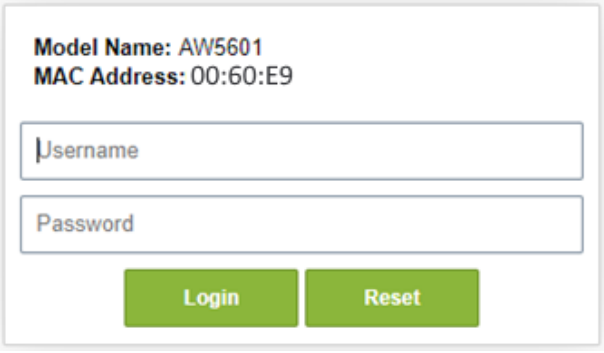
Figure 2. IP Address for Web-based Setting



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

Figure 3. Login Prompt





After the login process, the main interface will show up as shown in Figure 4. 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 AW5601 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 4. Default Web Interface for AW5601

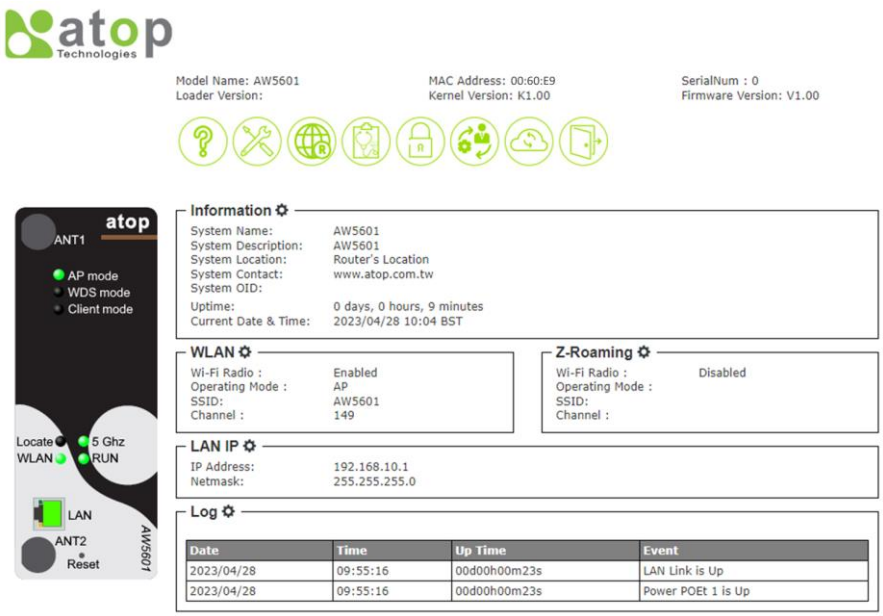


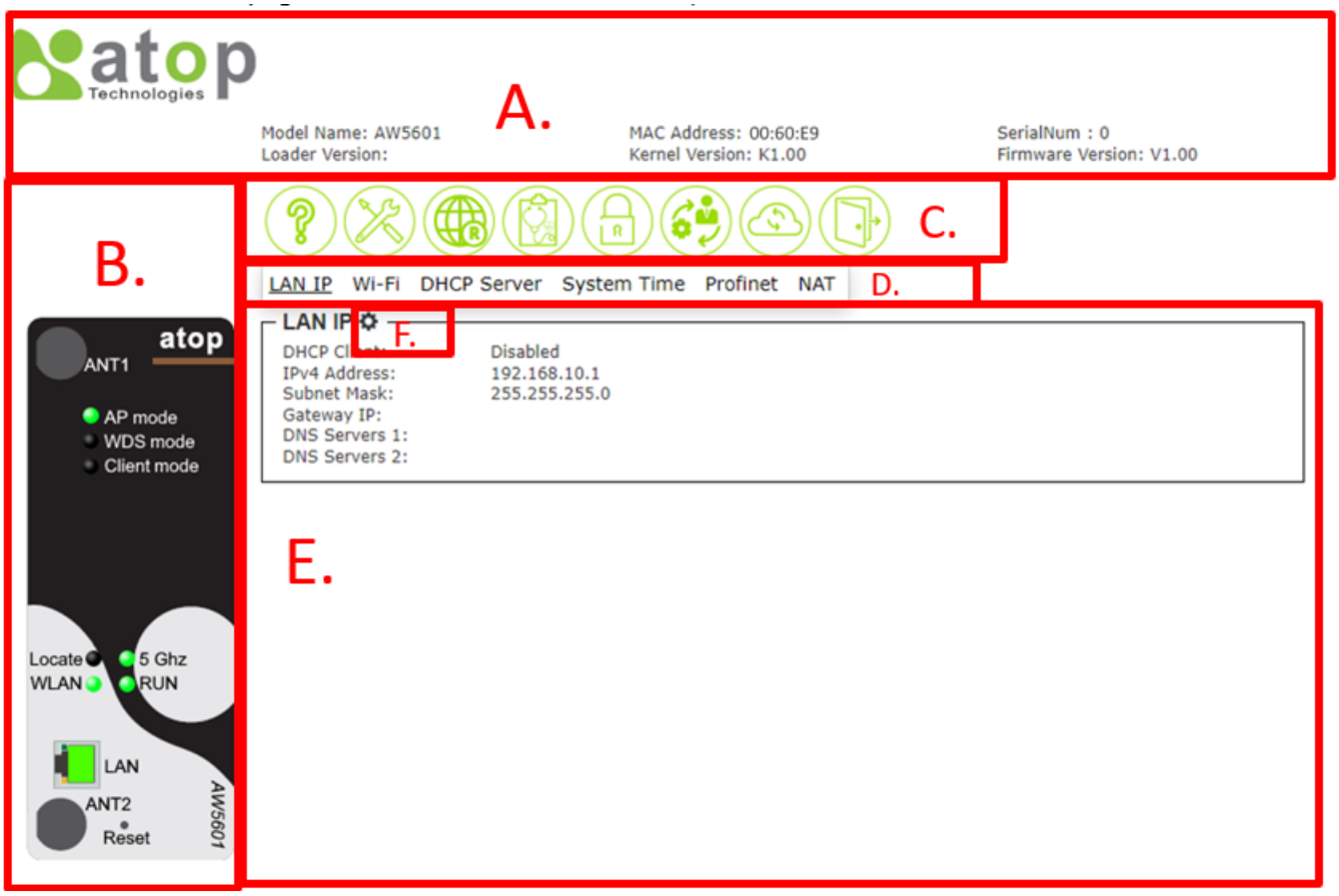
Figure 5. Function Bar on Top of Web GUI

The function bar on the top of the web GUI is shown in Figure 5. Function Bar on Top of Web GUI. There are 8 functions in the bar from the left side to the right side which are functions to manage Information, Configuration, Flash-Roaming, Diagnostic, Security, Management, Maintenance, and Logout. Note that there is a picture of the front panel of the AW5601 device on the left side of the screen under the function bar. This front panel of the manage switch display the LEDs of power, Wi-Fi mode, port link status, etc. Note that in this case the LAN port is highlighted in green, indicating that the port is being connected. Detailed explanations of each function icon will be addressed later as necessary.

2.2.2 Main Window Interface

The main web page is divided into several sections, and these sections will be introduced below.

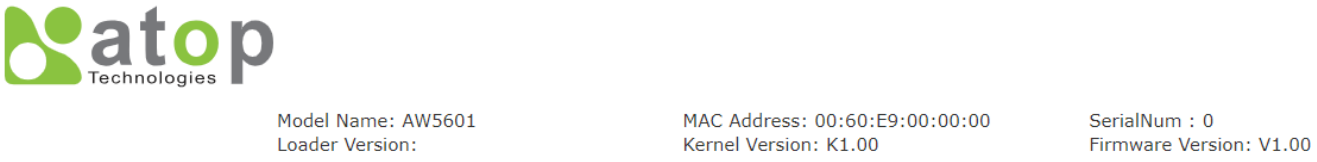
Figure 6. Main Window Interface



A. Banner with device Information

It displays ATOP's LOGO, and shows Model Name, Kernel Version, Firmware Version, Serial Number (SerialNum) and MAC Address.

Figure 7. Logo and banner Information



B. Panel Information

It displays the LEDs of power, Wi-Fi mode, 5 GHz, WLAN, Locate, and LAN port link status.

Figure 8. Panel Information

C. Function Bar.

All main function buttons display here.

Figure 9. Function Bar on Top of Web GUI

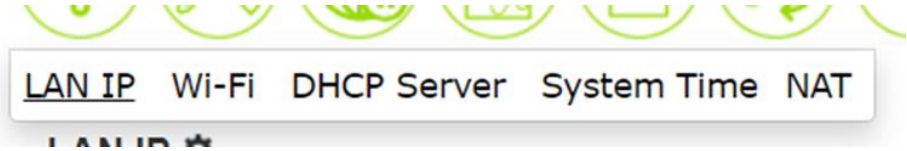
Table 3. Descriptions of the Function Bar

Button	Name	Description
	Information	Default webpage while login into device. It includes Device information, Wi-Fi, Syslog functions.
	Configuration	It includes LAN IP, Wi-Fi, DHCP server, System time, NAT functions.
	Roaming	It includes Flash-Roaming function.
	Diagnostic	It includes Syslog, SMTP, Ping, Locate LED functions.
	Security	It includes Firewall and Filtering functions.
	Management	It includes Account, HTTPS/Telnet/SSH, SNMP functions.
	Maintenance	It includes Firmware Upgrade, Configure Backup and Restore, Factory Default, Reboot functions.
	Logout	It will close current connection, and return to login page.

D. Sub function button.

If main function bar has sub functions, the sub functions display here.

Figure 10. Sub Function Button



E. Main display section.

Current operation function display section.

F. Gear button.

Click gear button will open a configuration frame to pop-up configuration window.

Figure 11. Gear Button

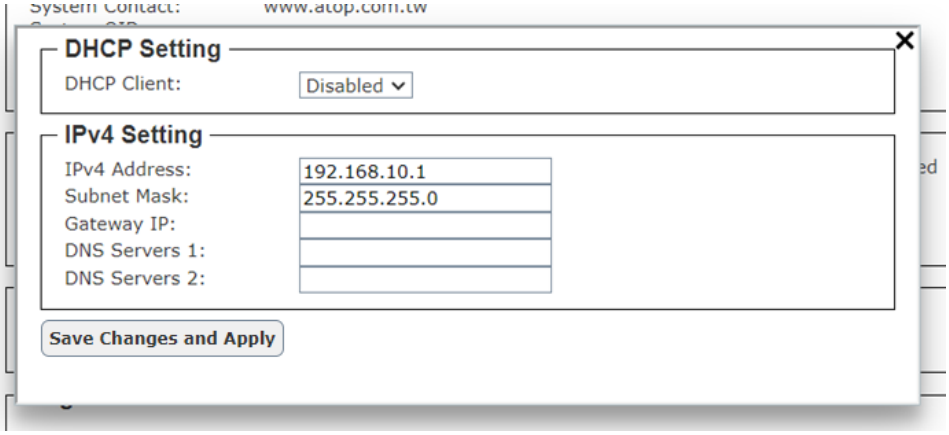
Explaining the functionality of the pop-up window associated with the gear icon:

Figure 12. Pop-up Window

G. Configuration window.

It displays configurations for function.

Figure 13. Configuration Window



H. Close button.

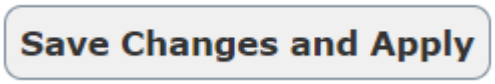
It displays on right-top in configuration frame, and it can close configuration frame.

Figure 14. Close Window Button

I. Save Changes and Apply button.

“Save Changes and Apply” button will save and apply the settings.

Figure 15. Save Changes and Apply Button.



3 Main Menu

This is the main welcome screen once the user has logged in. The details make it easier to identify different access points connected to the network. The information web page is separated into five boxes or features called **Information**, **WLAN**, **Flash-Roaming**, **LAN IP** and **Log** as shown in Figure 16. . 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 16. Main Menu

Information

System Name:	AW5601
System Description:	AW5601
System Location:	Router's Location
System Contact:	www.atop.com.tw
System OID:	
Uptime:	8 days, 1 hours, 36 minutes
Current Date & Time:	2023/05/06 11:31 BST

WLAN

Wi-Fi Radio :	Enabled
Operating Mode :	Client
SSID:	AW5601
Channel :	
IP Address:	192.168.10.1
Netmask:	255.255.255.0

Flash-Roaming

Wi-Fi Radio :	Enabled
Operating Mode :	AP
SSID:	flash-roaming
Channel :	36

LAN IP

IP Address:	192.168.10.1
Netmask:	255.255.255.0

Log

Date	Time	Up Time	Event
2023/04/30	09:59:31	02d00h04m37s	LAN Link is Up
2023/04/30	09:59:29	02d00h04m35s	LAN Link is Down
2023/04/30	09:59:27	02d00h04m33s	LAN Link is Up
2023/04/30	09:59:25	02d00h04m31s	LAN Link is Down
2023/04/28	09:55:16	00d00h00m23s	LAN Link is Up

3.1 *Information Feature*

This feature provides basic system information of Atop's industrial access point. The user can check the device description which includes System Name, System Description, System Location, System Contact, and System OID as shown in Figure 17. At the bottom of this section, the Uptime and the Current Date & Time of the device are displayed. Table 4 summarizes the description of each basic information.

Figure 17. Information Function

Information

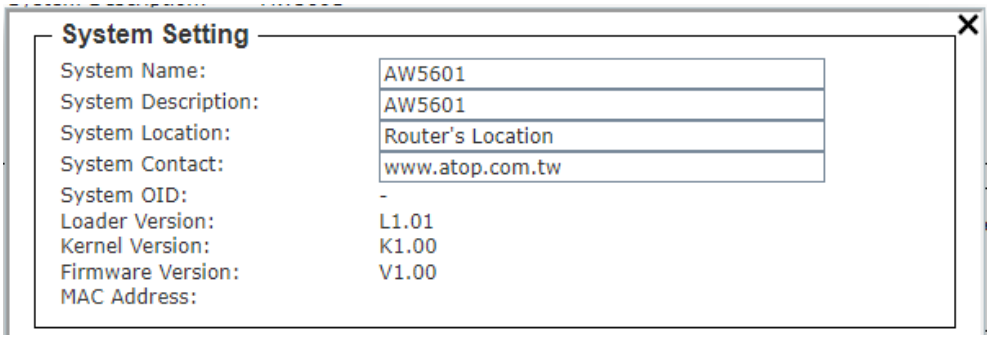
System Name:	AW5601
System Description:	AW5601
System Location:	Router's Location
System Contact:	www.atop.com.tw
System OID:	
Uptime:	8 days, 1 hours, 36 minutes
Current Date & Time:	2023/05/06 11:31 BST

Table 4. 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 Characters.	(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) numbers.	-
Model name	The device's complete model name.	AW5601
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 18 On this window, the user can configure System Name, System Description, System Location and System Contact. After you finished, clicking on the **Save Changes and Apply** button to save and apply the settings.

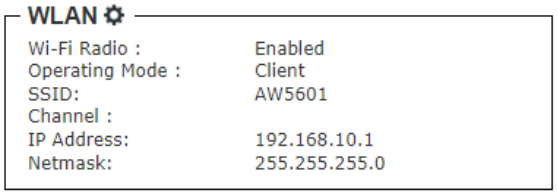
Figure 18. System Setting Pop-up Window



3.2 *WLAN Feature*

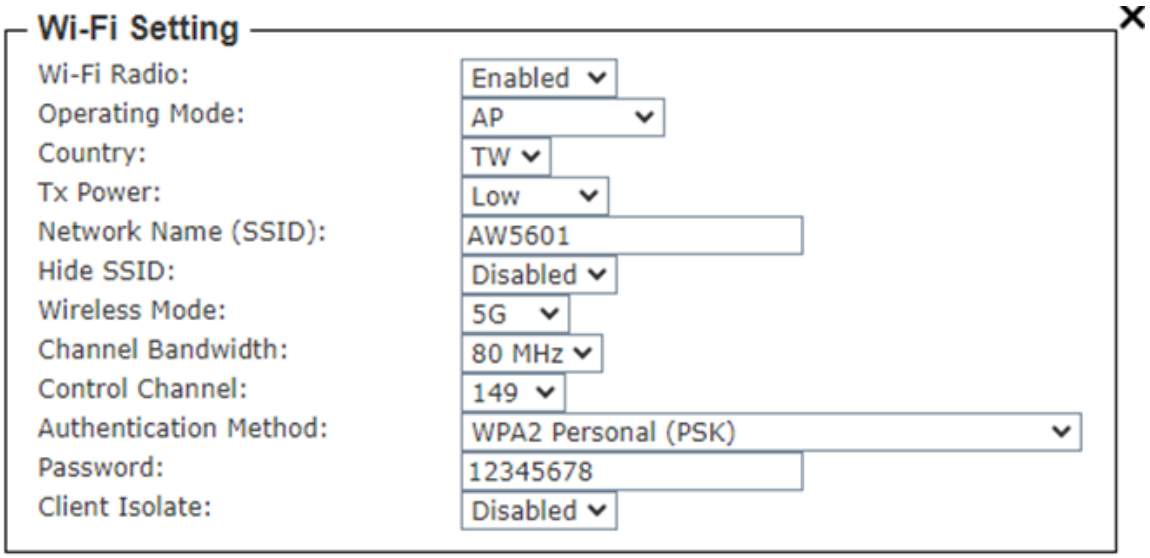
The WLAN feature displays the current setting of the Wi-Fi network configuration of the access point which are the status of Wi-Fi Radio, Operating Mode, SSID, Channel, IP Address, and Sub-Netmask as shown in Figure 19. To change WLAN configuration, the user can click on the gear icon to bring up the Wi-Fi Setting pop-up window as shown in Figure 20. The user can choose to enable or disable the Wi-Fi Radio on the device, and choose AP or Client mode as the Operating Mode by selecting the corresponding drop-down list. After you finished, clicking on **the Save Changes and Apply** button to save and apply the settings.

Figure 19. WLAN feature



To change or configure fields under the WLAN feature, the user can click on the gear icon to bring up a pop-up window called Wi-Fi Setting as shown in Figure 24. On this window, the user can configure Wi-Fi Radio, Operating Mode, Country, Tx Power, Network Name (SSID), Hide SSID, Wireless Mode, Channel Bandwidth, Control Channel, Authentication Method, Password, and Client Isolate. After you finished, clicking on the **Save Changes and Apply** button to save and apply the settings.

Figure 20. Wi-Fi Setting Pop-up Window



3.3 *Flash-Roaming Feature*

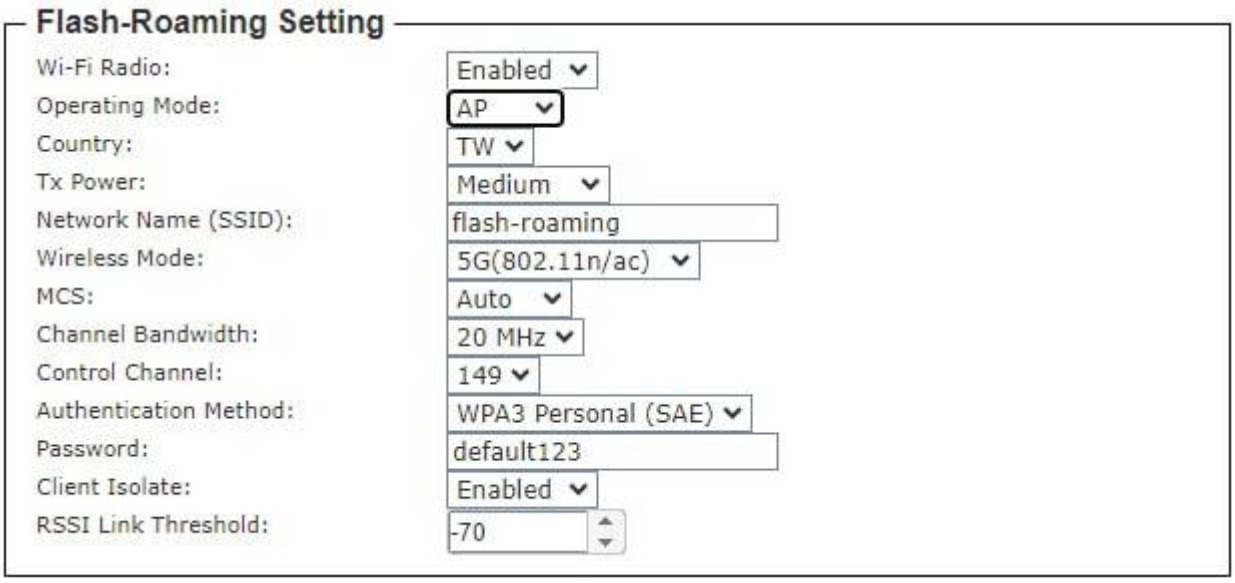
The Flash-Roaming feature displays the current setting of the Wi-Fi configuration of the access point which are the status of Flash-Roaming's Wi-Fi Radio, Operating Mode, SSD, and Channel as shown in Figure 21.
This roaming feature allows mobile devices to smoothly switch between different locations within the wireless network without experiencing interruptions in connectivity

Figure 21. Flash-Roaming Feature

To change or configure fields under the Flash-Roaming feature, the user can click on the gear icon to bring up a pop-up window called Flash-Roaming Setting as shown in Figure 22. On this window, the user can configure Wi-Fi Radio, Operating Mode, Country, Tx Power, Network Name (SSID), Hide SSID, Wireless Mode, Channel Bandwidth, Control Channel, Authentication Method, Password, Client Isolate,

and RSSI Link Threshold. After you finished, clicking on the **Save Changes and Apply** button to save and apply the settings.

Figure 22. Flash-Roaming Setting Pop-up Window



3.4 *LAN IP Feature*

The LAN IP feature displays the current setting of the network configuration of the access point which are the status of IP Address, and Sub-Netmask as shown in Figure 23. 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 24. 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 and Apply button to **save and apply** the settings.

Figure 23. LAN IP Feature

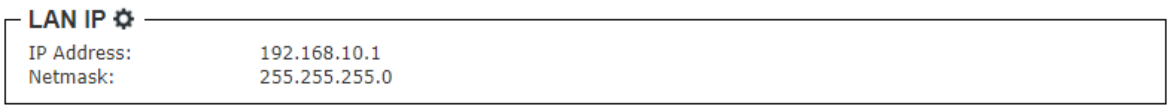
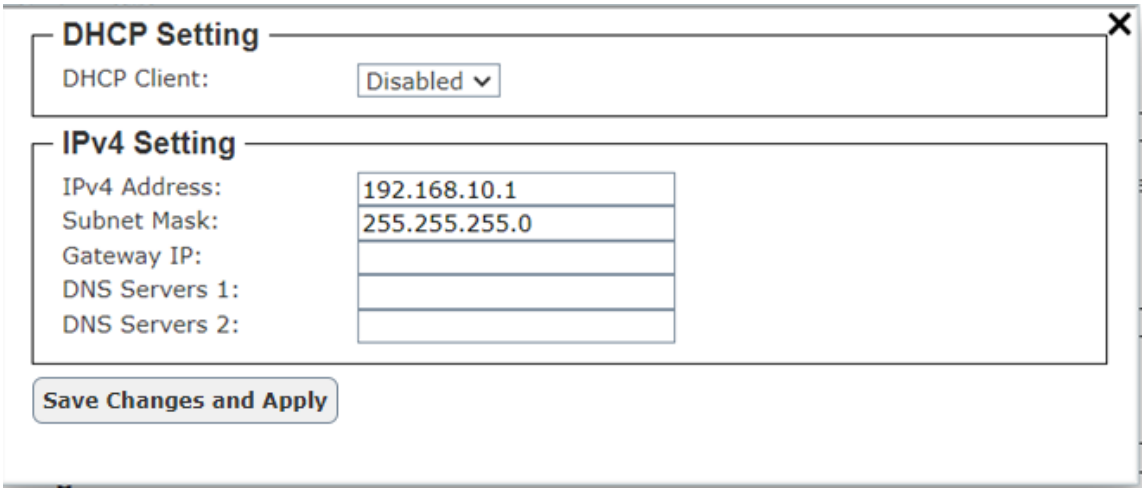


Figure 24. IP Network Setting Pop-up Window



3.5 *System Log Feature*

The Log feature at the bottom of the Information function shows a table of at least 5 system logs as shown in Figure 25. Each log entry includes Date, Time, Up Time, and Event description. Note that the log entries are sorted by date and time. Table 5 provides explanation of each column in the Log table.

Figure 25. Log Feature

Log

Date	Time	Up Time	Event
2023/04/30	09:59:31	02d00h04m37s	LAN Link is Up
2023/04/30	09:59:29	02d00h04m35s	LAN Link is Down
2023/04/30	09:59:27	02d00h04m33s	LAN Link is Up
2023/04/30	09:59:25	02d00h04m31s	LAN Link is Down
2023/04/28	09:55:16	00d00h00m23s	LAN Link is Up

Table 5. 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 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 26. 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 and Apply** button to save and apply the settings.

Figure 26. System Log Setting Pop-up Window

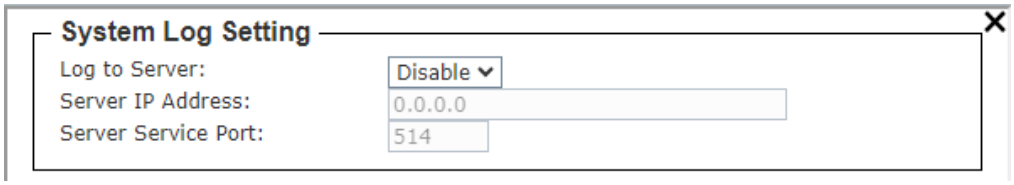


Table 6. Description of System Log Setting Pop-up Entry

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

4 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 five features under the Configuration or System Setting function which are **LAN IP, Wi-Fi, DHCP Server, System Time** and **NAT** as shown Figure 27.

Figure 27. Configuration Function on Menu Bar

4.1 *LAN IP Feature*

The LAN IP feature summarizes the current IP configuration of the manage switch. This web page as shown in Figure 28 displays information such as DHCP Client, IPv4 Address, Subnet Mask, Gateway IP, DNS Server 1, and DNS Server 2. By clicking on the gear icon next to the LAN IP title, the user can bring up the LAN IP Setting pop-up window as shown in Figure 29. Table 7 summarizes each field in the IP Setting pop-up window. After you finished, clicking on the **Save Changes and Apply** button to **save and apply** the settings

Figure 28. LAN IP Feature

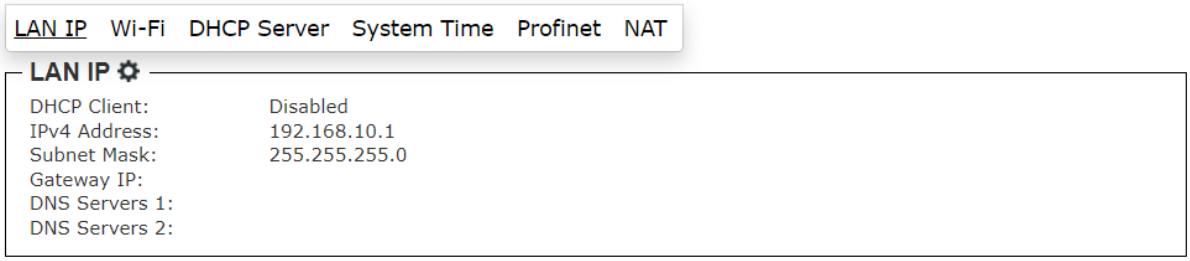


Figure 29. IP Network Setting Pop-up Window

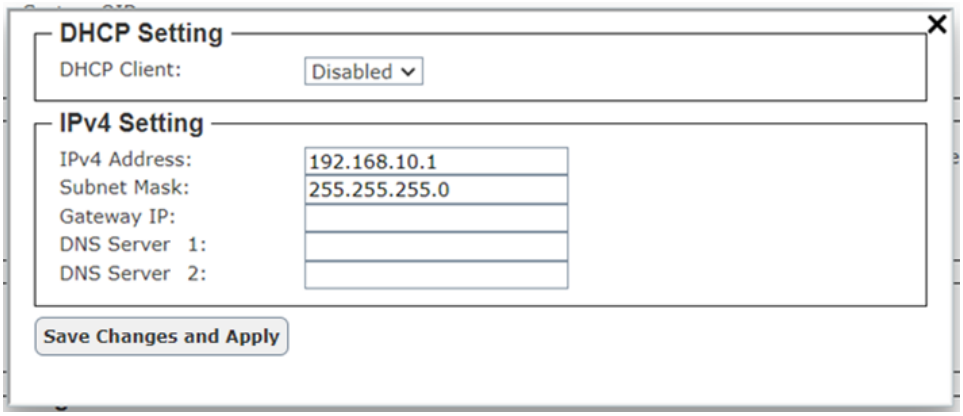


Table 7. Description of IP Network Settings

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	empty
DNS Server 1	Show current primary DNS IP address to be used by your network or user can set a new one	empty
DNS Server 2	Show current secondary DNS IP address to be used by your network or user can set a new one	empty

4.2 *Wi-Fi Feature*

Packet forwarding behavior table in different Wi-Fi modes. Here is an example: If you are using Wi-Fi mode (AP/Client) with NAT, this mode does not support the delivery of PN packets and L2 packets, but supports the delivery of L3 packets.

Table 8. Description of Wi-Fi mode with packet forwarding

Wi-Fi Mode & NAT \ Type of packet delivery		PN Packet	L2 Packet	L3 Packet
AP/Client	NAT	No	No	Yes
AP/Client	Non-NAT	No	No	Yes
WDS-AP/Client/Hybrid	Non-NAT	No	Yes**(*2)**	Yes

Flash-Roaming AP/Client	NAT	Yes(***1**)	No	Yes
Flash-Roaming AP/Client	Non-NAT	Yes	Yes	Yes

Yes: It means that this type of packet can be delivered.
No: It means that this type of packet cannot be delivered.

(*1): If you are using **Flash-Roaming AP/Client** in Wi-Fi mode and want transparent PROFINET packets when NAT is enabled, you need to manually enable **PROFINET Transparent** on the WEB. (Section 4.3)

(*2): WDS mode does not support the transmission of VLAN tagged packets. If you want to transmit VLAN tagged packets, it is recommended to use **Flash-Roaming** mode.

4.2.1 Wi-Fi AP Mode / Client Mode

Access Point's AP mode is used to connect to wireless clients (wireless adapter cards) such as laptops, desktops, and PDAs. Wireless clients can only communicate to AP in Access Point mode.

Access Point's Client mode allows the Access Point to become a wireless client to another AP. In essence the AP has now become a wireless adapter card. You would use this mode to allow an AP to communicate with another AP.

Note: Not all Access Points support AP Client mode. If the mode is supported it will operate only with devices of the same series. Wireless cards will not communicate with access points in AP Client/ Wireless Client mode.

There is a topology for AP/Client mode is looks like below, as shown in Figure 30. We set AP1 as AP mode as shown in Figure 31 and AP2 as Client mode as shown in Figure 32.

Figure 30. Wi-Fi AP Mode / Client Mode Topology

Figure 31. Wi-Fi AP Mode for AP1 Setting

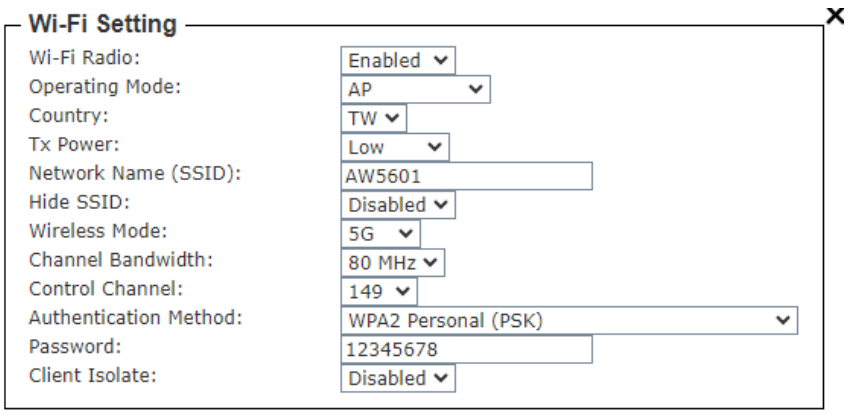


Figure 32. Wi-Fi Client Mode for AP2 Setting

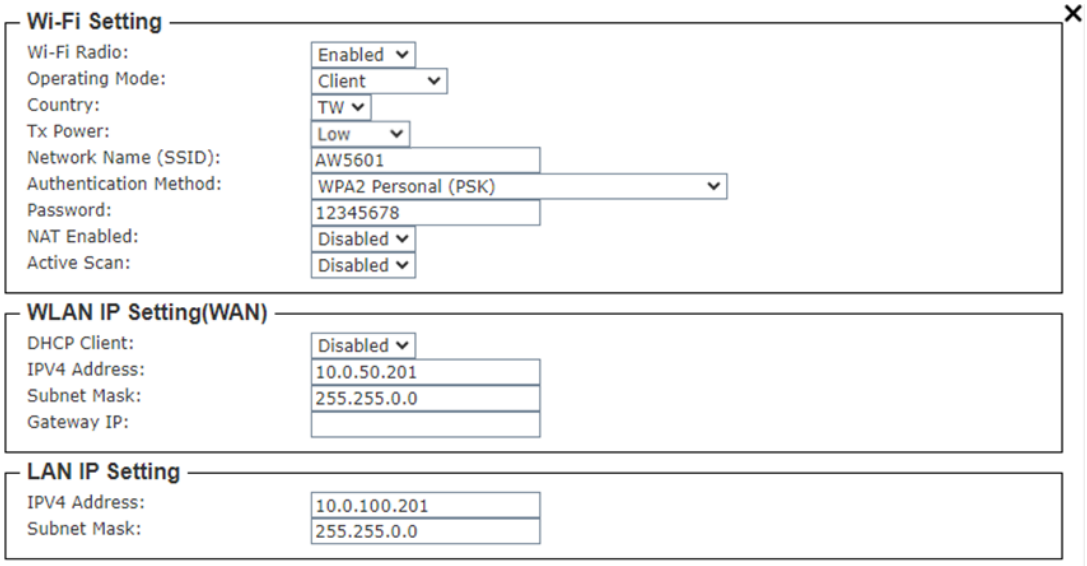


Table 9. Wi-Fi AP / Client Mode Setting Table

	AP1	AP2
DHCP server	Disabled	
Wi-Fi Radio	Enabled	
Operating Mode	AP	Client
WLAN IP Setting	N/A	10.0.50.201
LAN IP Setting	10.0.50.200	10.0.100.201
Network Name (SSID)	AW5601	
NAT Enabled	N/A	Disabled

Table 10. Wi-Fi AP / Client Mode's Devices IP Address Setting Table

	Device1	Device2
IP Address	10.0.50.1	10.0.100.2

4.2.2 Wi-Fi WDS-AP / Client / Hybrid Mode (Non-NAT)

Wireless distribution system (WDS) expands a wireless network through multiple access points. A wireless base station connects to the Internet, can have wired and wireless clients, and sends its wireless signal to an access point that works as a wireless repeater. A wireless repeater can also have wired and wireless clients, but connects to the Internet through the wireless base station.

WDS-AP: Enabling Access Point (AP) in this mode will become the root node of the entire wireless network. It can establish connections with APs in WDS Station mode (leaf nodes) using either Point-to-Point (P2P) or Point-to-Multi-Point (P2MP) tree topology to link one or multiple local area networks.

WDS-Client: Enabling Access Point (AP) in this mode will become a leaf node of the wireless network, establishing a Point-to-Point connection with the root node.

WDS-Hybrid: To combine WDS-AP and WDS-Client, and have both functionalities, you can set up the device in WDS Bridge mode. In this mode, the device acts as both an Access Point (WDS-AP) and a Client (WDS-Client), allowing it to connect to another Access Point while also accepting connections from other client devices.

Before you set up a wireless network with WDS, both access points must meet the following conditions:

- Use the same SSID, wireless channel, and encryption mode.
- Be on the same LAN IP subnet. That is, all of the access point LAN IP addresses are in the same network.
- All LAN devices (wired and wireless computers) are configured to operate in the same LAN network address range as the access points.

Note: In this mode, currently only the same device can be used for wireless connection

There is a topology for WDS-AP/WDS-Hybrid/WDS-Client mode, looks like below as shown in Figure 33. We set AP1 as WDS-AP mode as shown in Figure 34, set AP2 as WDS-Hybrid mode as shown in Figure 35 and set AP3 as WDS-Client mode as shown in Figure 36.

Figure 33. WDS-AP/Client/Hybrid Mode Topology

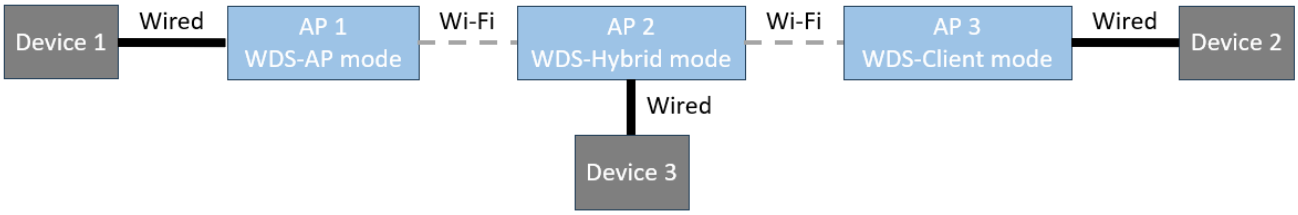


Figure 34. WDS-AP Mode for AP1 Setting

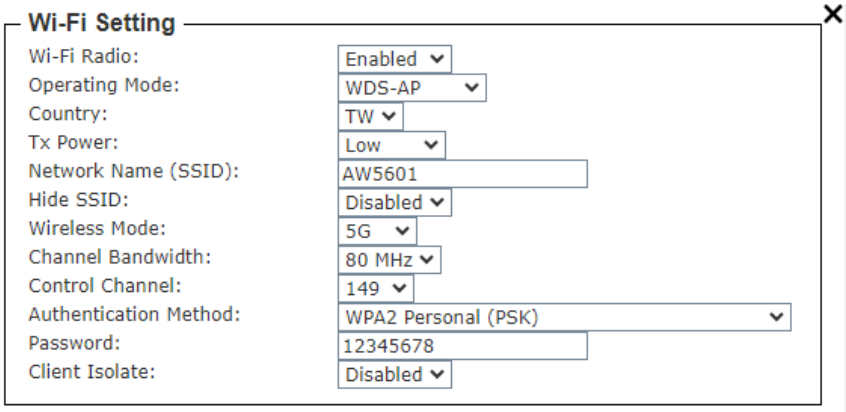


Figure 35. WDS-Hybrid Mode for AP2 Setting

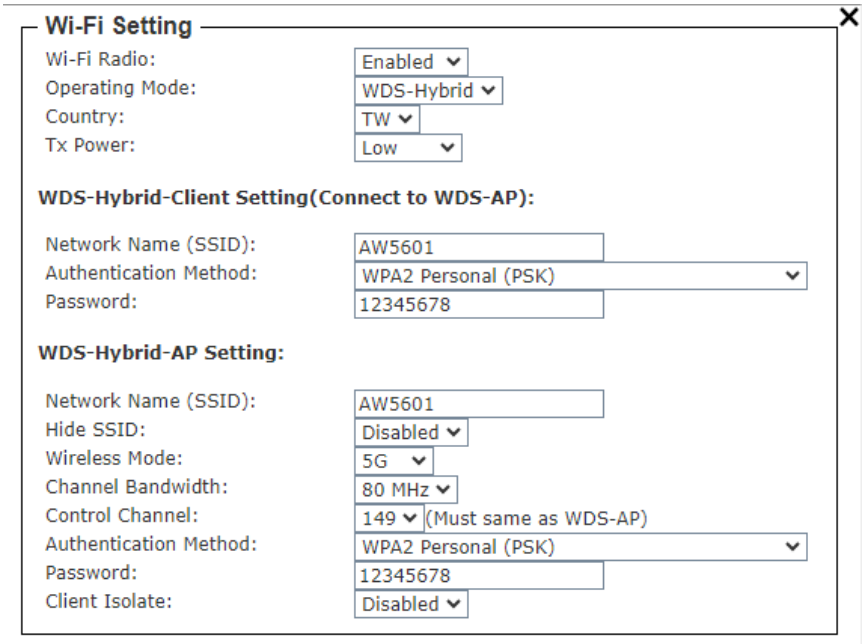


Figure 36. WDS-Client Mode for AP3 setting

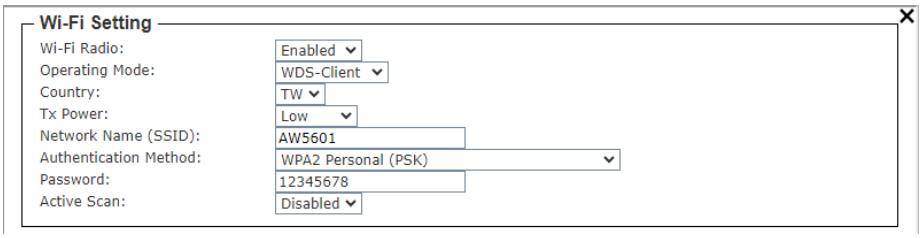


Table 11. WDS-AP/WDS-Hybrid/WDS-Client Mode for APs Setting

	AP1	AP2	AP3
DHCP server	Disabled		
Wi-Fi Radio	Enabled		
Operating Mode	WDS-AP	WDS-Hybrid	WDS-Client
LAN IP Setting	10.0.50.200	10.0.50.201	10.0.50.202
Network Name (SSID)	AW5601		
NAT Enabled	N/A	Disabled	Disabled

4.2.3 Wi-Fi Flash-Roaming AP / Flash-Roaming Client Mode

Wi-Fi Flash-Roaming AP / Flash-Roaming Client: It is similar to WDS-AP / WDS-Client mode but incorporates Roaming behavior. We will introduce Flash-Roaming feature in the Section 4.3.

4.3 *Flash-Roaming Feature*

Roaming, in the context of wireless networks, refers to the ability of mobile devices to automatically switch and maintain connections between different wireless access points. When a wireless device, such as a mobile phone, laptop, or tablet, moves within the coverage area of one wireless network, it may enter the range of another wireless access point. To ensure continuous connectivity, the device performs **"Flash-Roaming"**, which means it automatically switches to the most suitable access point to maintain optimal signal strength and network performance.

This Flash-Roaming feature allows devices to smoothly switch between different locations within the wireless network without experiencing interruptions in connectivity. It is crucial for providing a seamless wireless experience, especially in large areas such as corporate offices, airports, hotels, campus, factories or Automated Guided Vehicle (AGV).

4.3.1 Flash-Roaming AP / Flash-Roaming Client Mode

There is a topology for Flash-Roaming AP / Flash-Roaming Client mode, looks like below, as shown in Figure 37. We set AP1 as Flash-Roaming AP mode as shown in Figure 38, AP2 as Flash-Roaming Client mode as shown in Figure 39.

Figure 37. Flash-Roaming AP / Flash-Roaming Client Topology

Table 12. Flash-Roaming AP / Flash-Roaming Client mode setting

	AP1	AP2
DHCP server	Disabled	
Wi-Fi Radio	Enabled	
Operating Mode	AP	Client
LAN IP Setting	10.0.50.200	10.0.50.201
Network Name (SSID)	flash-roaming	
NAT Enabled	N/A	Disabled

Table 13. Devices IP address setting

	Device1	Device2
LAN IP Setting	10.0.50.1	10.0.50.22

Figure 38. Flash-Roaming AP Mode for AP1 setting

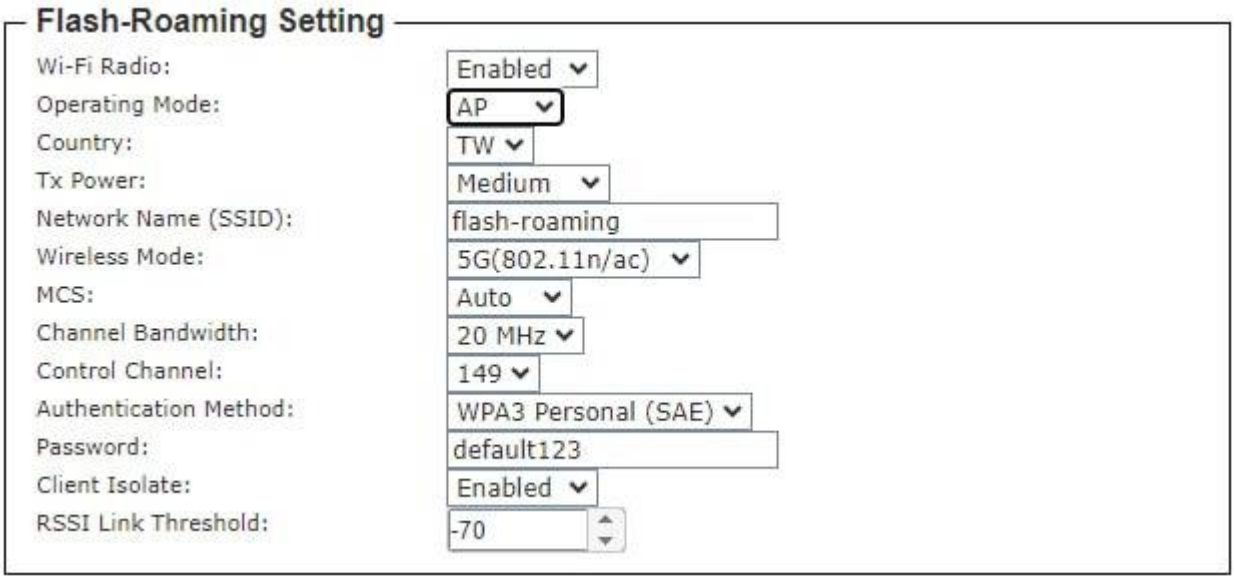


Table 14. Descriptions of the Flash-Roaming AP mode

Label	Description	Default Value
Wi-Fi Radio	This option can turn on or turn off the wireless signal of AW5601 completely	Disabled
Operating Mode	AP mode: Access Point mode, and Client mode.	AP
Country	US: United States (FCC), EU: Europe (ETSI), JP: Japan (MIC), CN: China (CCC), TW: Taiwan (NCC)	TW
TX Power	The transmit power of AW5601 can be reduced to prevent wireless interference with other wireless networks. The higher the power, the higher the transmission distance, but it will also increase the impact on jitter and latency.	Medium
Network Name (SSID)	Network name for WLAN which is assigned by the network administrator.	flash-roaming
Wireless Mode	2.4 GHz: IEEE 802.11g/n, 5 GHz: IEEE 802.11n/ac, or IEEE 802.11a only, or IEEE 802.11n only.	5G (802.11n/ac)
MCS	Modulation Coding Scheme index is a metric based on several parameters of a Wi-Fi connection between two stations. Auto means MCS full range automatic adjustment, Stable, and Stable means locked in some relatively stable range.	Auto
Channel Bandwidth	20 MHz or 40 MHz or 80 MHz	20 MHz
Control Channel	2.4 GHz: channel 1 to 11 or channel 1 to 13 depending on the Regulatory Domain 5 GHz: depending on the Regulatory Domain ● Channel 36, 40, 44, 48 for EU/JP and IEEE 802.11a only, or IEEE 802.11n only, or 802.11n/ac. ● Channel 36, 40, 44, 48, 149, 153, 157, 161, 165 for TW and IEEE 802.11a only, or IEEE 802.11n only, or 802.11n/ac.	5G(802.11n/ac)

	● Channel 36, 40, 44, 48, 149, 153, 157, 161, 165 for US and IEEE 802.11a only, or IEEE 802.11n only, or 802.11n/ac. ● Channel 149, 153, 157, 161, 165 for CN and IEEE 802.11a only, or IEEE 802.11n only, or 802.11n/ac.	
Authentication Method	Mode of authentication for WLAN which can be Open System, WPA3 Personal (SAE)	WPA3 Personal (SAE)
Password	This is a user defined string which must be ASCII format between 8 and 63 characters.	default123
Client Isolate	Creates a firewall between wireless clients connected to this AP. The isolation can be enabled to prevent data traffic flowing between clients to increase client security and to prevent unnecessary traffic between clients.	Enabled
RSSI Link Threshold	RSSI (Received Signal Strength Indicator), minimum connectable signal strength.	-70

Figure 39. Flash-Roaming Client Mode for AP2 Setting

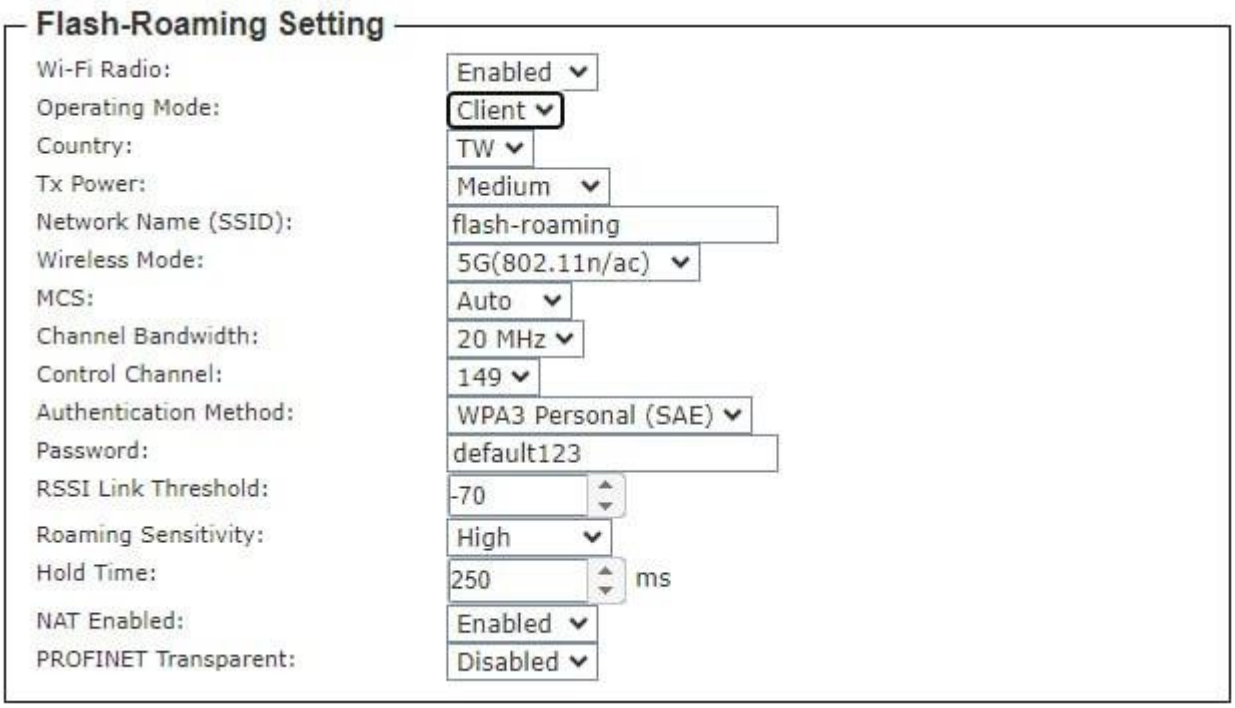


Table 15. Descriptions of the Flash-Roaming Client Mode

Label	Description	Default Value
Wi-Fi Radio	This option can turn on or turn off the wireless signal of AW5601 completely	Disabled
Operating Mode	AP mode: Access Point mode, and Client mode.	AP
Country	US: United States, EU: Europe, JP: Japan, CN: China, TW: Taiwan	EU
TX Power	The transmit power of AW5601 can be reduced to prevent wireless interference with other wireless networks. The higher the power, the higher the transmission distance, but it will also increase the impact on jitter and latency.	Medium
Network Name (SSID)	Network name for WLAN which is assigned by the network administrator.	flash-roaming

Label	Description	Default Value
Wireless Mode	2.4 GHz: IEEE 802.11g/n, 5 GHz: IEEE 802.11n/ac, or IEEE 802.11a only, or IEEE 802.11n only.	5G (802.11n/ac)
MCS	Modulation Coding Scheme index is a metric based on several parameters of a Wi-Fi connection between two stations. Auto means MCS full range automatic adjustment, and Stable means locked in some relatively stable range.	Auto
Channel Bandwidth	20 MHz or 40 MHz or 80 MHz	20 MHz
Control Channel	2.4 GHz: channel 1 to 11 or channel 1 to 13 depending on the Regulatory Domain 5 GHz: depending on the Regulatory Domain ● Channel 36, 40, 44, 48 for EU/JP and IEEE 802.11a only, or IEEE 802.11n only, or 802.11n/ac. ● Channel 36, 40, 44, 48, 149, 153, 157, 161, 165 for TW and IEEE 802.11a only, or IEEE 802.11n only, or 802.11n/ac. ● Channel 36, 40, 44, 48, 149, 153, 157, 161, 165 for US and IEEE 802.11a only, or IEEE 802.11n only, or 802.11n/ac. ● Channel 149, 153, 157, 161, 165 for CN and IEEE 802.11a only, or IEEE 802.11n only, or 802.11n/ac.	36
Authentication Method	Mode of authentication for WLAN which can be Open System, WPA3 Personal (SAE)	WPA3 Personal (SAE)
Password	This is a user defined string which must be ASCII format between 8 and 63 characters.	default123
RSSI Link Threshold	RSSI (Received Signal Strength Indicator), minimum connectable signal strength.	-70
Roaming Sensitivity	Enable this option to allow Flash-Roaming Client mode to scan for available access points in the background to speed up roaming when necessary. Very High or High or Medium or Low or Very Low.	High
Hold Time	The minimum stay time after connecting to the AW5601. When there are multiple AW5601s with similar signal strength around, setting this value appropriately can avoid frequent switching between devices.0 to 2000 ms	250 ms
NAT Enabled	Network Address Translation. Enabled or Disabled.	Enabled
PROFINET Transparent	Enable this option to allow Flash-Roaming Client mode to forward PRIFINET packets.	Disabled

4.3.2 PROFINET Transparent over Flash-Roaming and NAT

If we want to connect AP1 and AP2 by Flash-Roaming under NAT enabled, we have to enable PROFINET transparent to let PROFINET packets transmit between device1 and device2. We set AP1 as Flash-Roaming AP mode as shown in Figure 40, set AP2 as Flash-Roaming Client mode and AP2 enable NAT and PROFINET Transparent as shown in Figure 41.

Table 16. Flash-Roaming AP / Flash-Roaming Client Mode Setting

	AP1	AP2
Operating Mode	AP	Client
LAN IP Setting	10.0.50.200	10.0.50.201
Network Name (SSID)	flash-roaming	
NAT Enabled	N/A	Enabled

PROFINET Transparent	N/A	Enabled

Table 17. Flash-Roaming AP / Flash-Roaming Client Mode's Device IP Address setting

	Device1	**Device2**
LAN IP Setting	10.0.50.1	10.0.50.22

Figure 40. Flash-Roaming AP Mode Setting

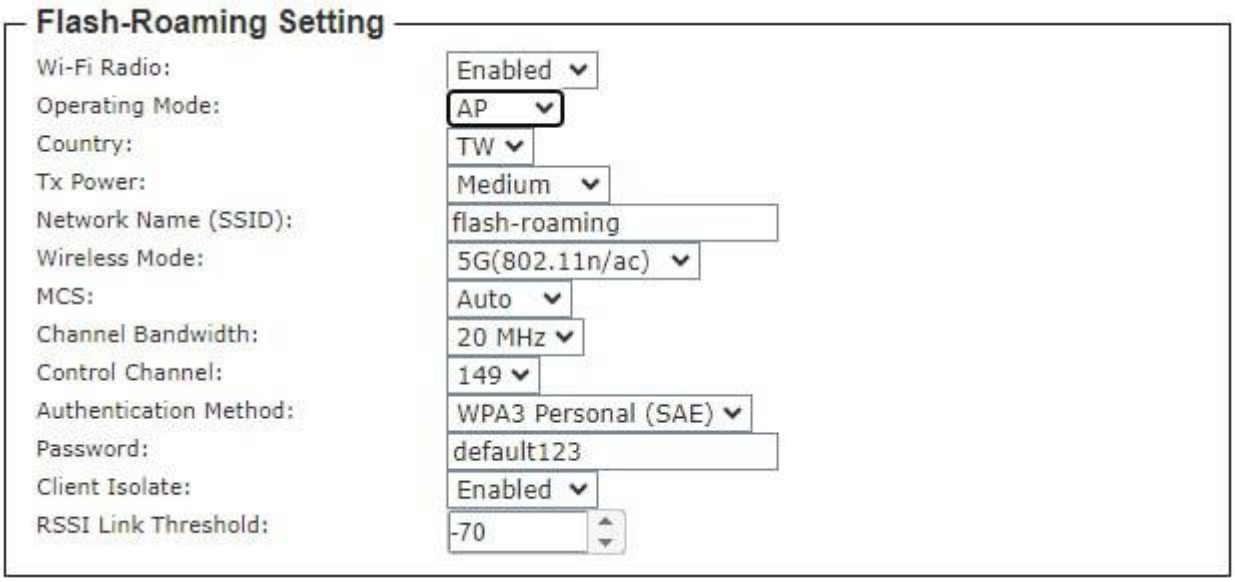
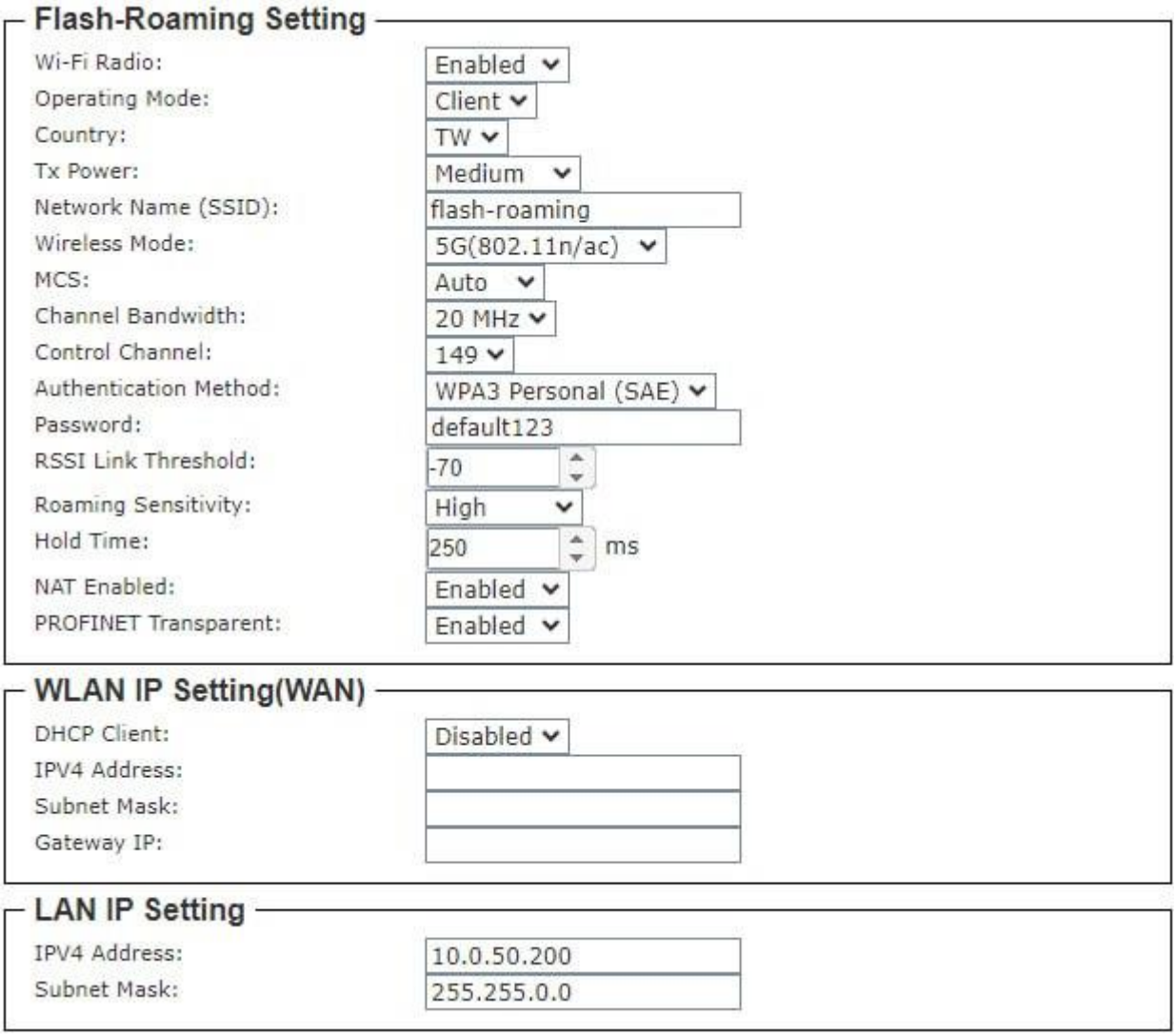


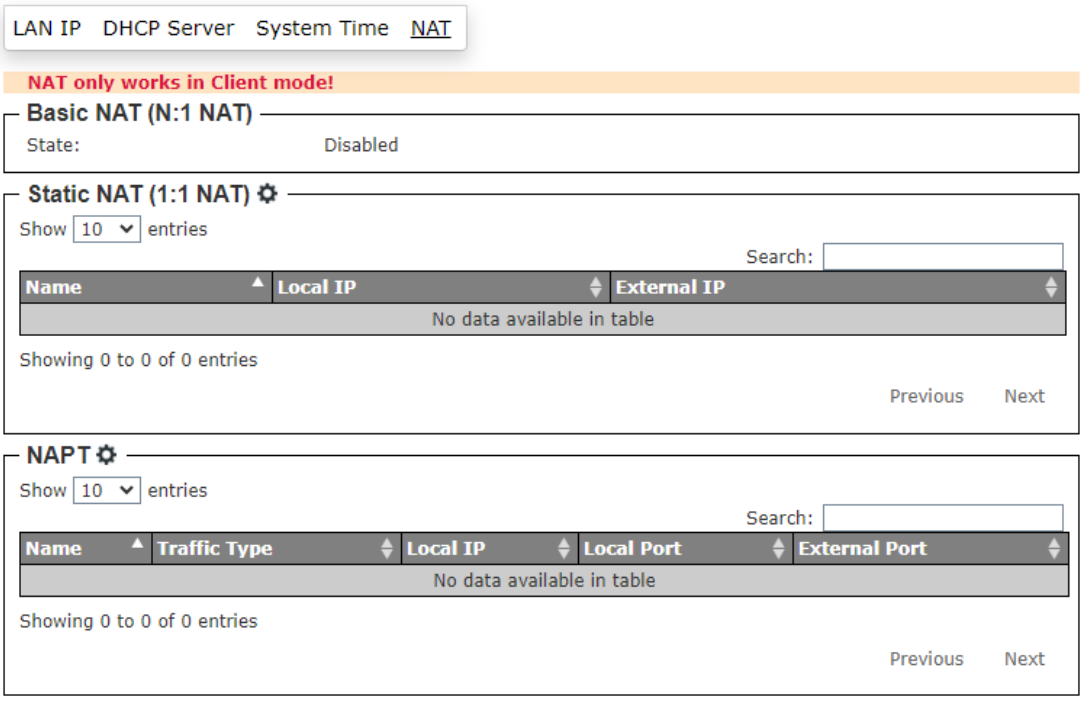
Figure 41. Flash-Roaming Client Mode Setting



4.4 *NAT Feature*

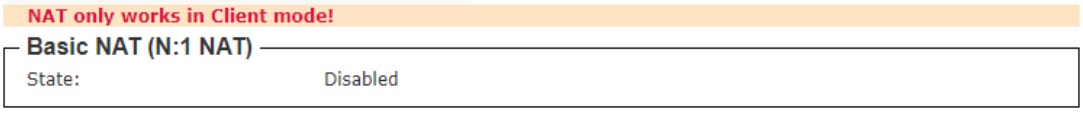
NAT function only works in Wi-Fi client mode, and it is distributed to Basic NAT, Static NAT, and NAPT sub-function.

Figure 42. NAT Feature



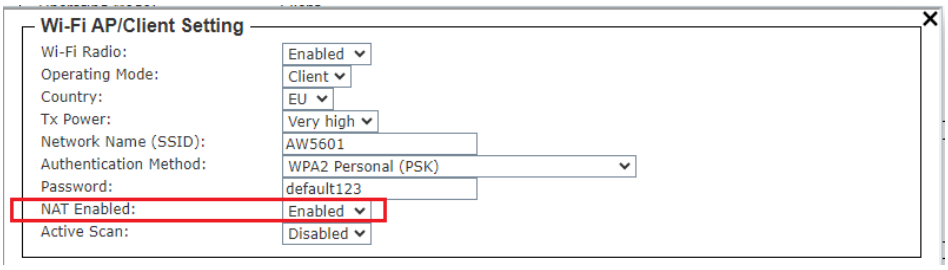
4.4.1 Basic NAT (N:1 NAT)

Figure 43. Basic NAT (N:1 NAT) Feature



Basic NAT can be used to interconnect two IP networks that have incompatible addressing which are WLAN and LAN interfaces in Wi-Fi client mode. If client mode is activated in “Wi-Fi -> AP/Client -> Wi-Fi AP/Client Setting”, “NAT Enabled” will be enabled on this page shown below.

Figure 44. Wi-Fi Client Enable Basic NAT Mode



4.4.2 Static NAT (1:1 NAT)

Static NAT function can map two IP addresses between two network interfaces. In Wi-Fi client mode, it can map an external IP address in WLAN interface to a local IP address in LAN interface. To add a Group Name, a Local IP, and an External IP as shown in Figure 46.

Figure 45. Static NAT (1:1 NAT) Feature

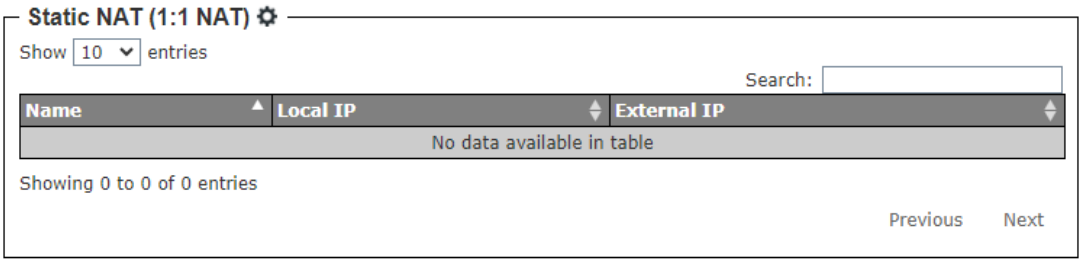
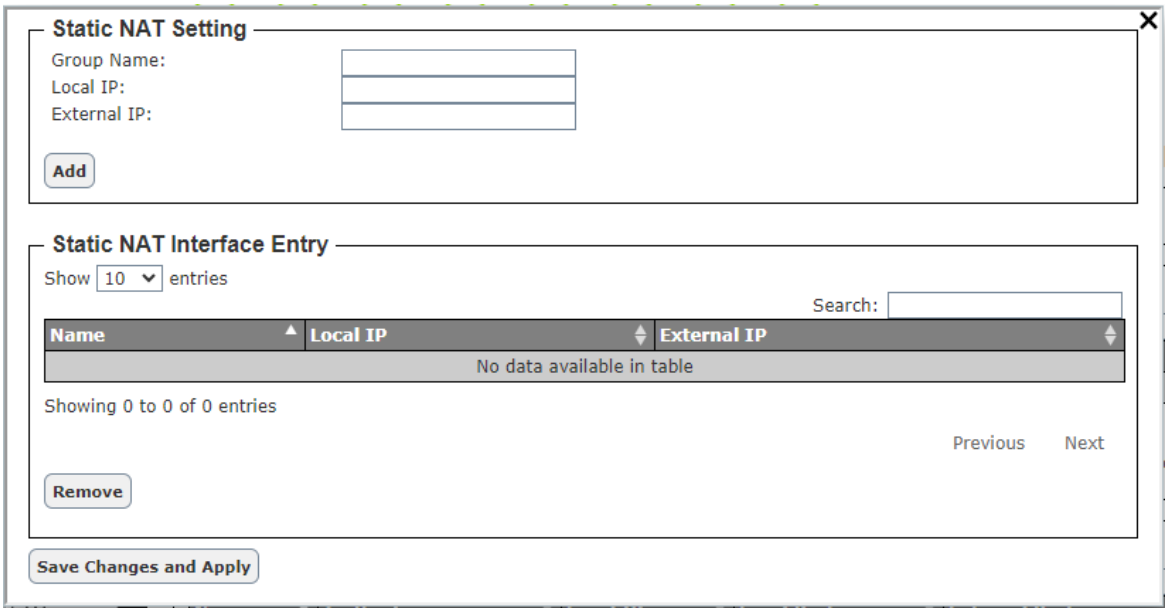


Figure 46. Static NAT Setting Pop-up Window



4.4.3 NAPT

NAPT extends NAT with port translation. NAPT maps the WLAN IP address of Client and an external TCP/UDP port to an IP address and port in local interface. To add a Name, Traffic Type, Local IP, Local Port, and External Port as shown in Figure 48.

Figure 47. NAPT Feature

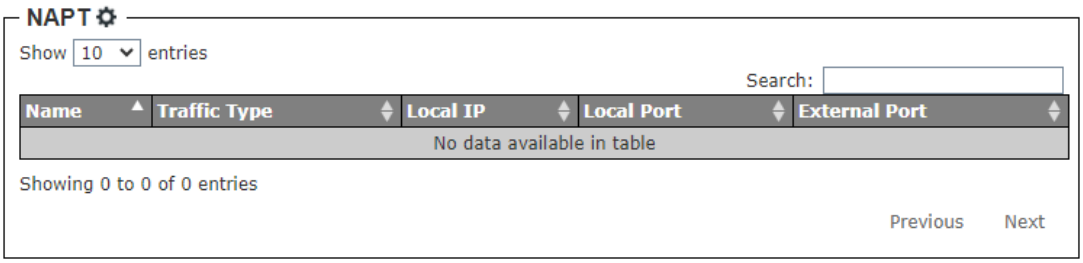
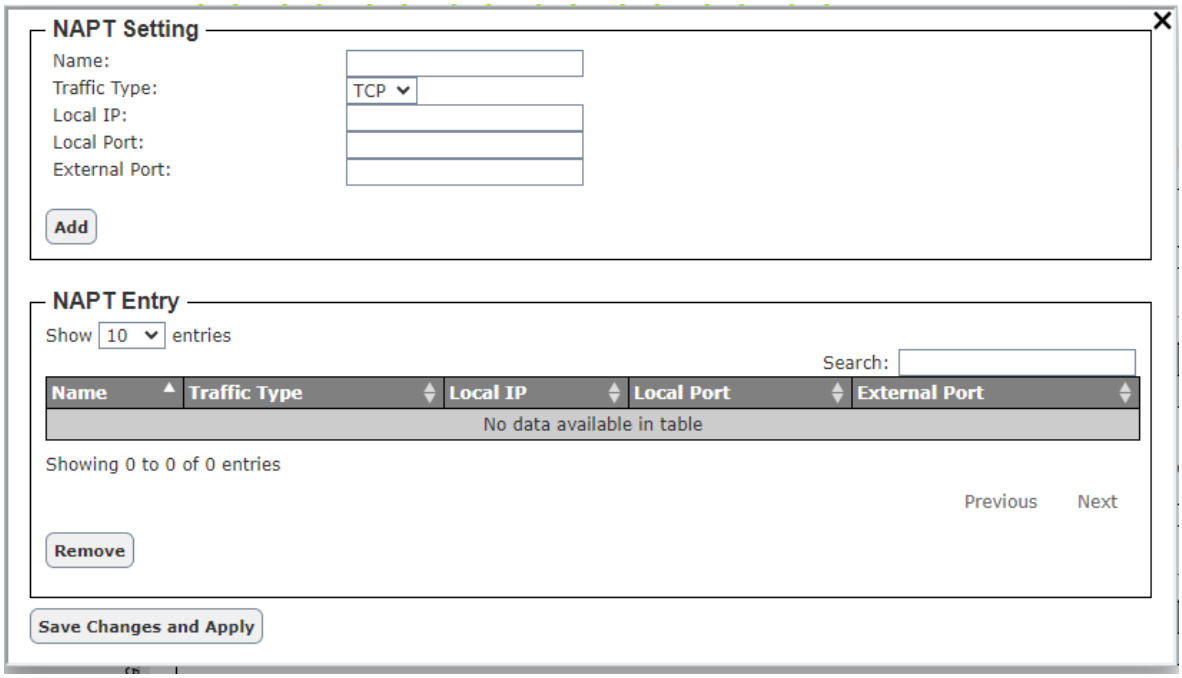


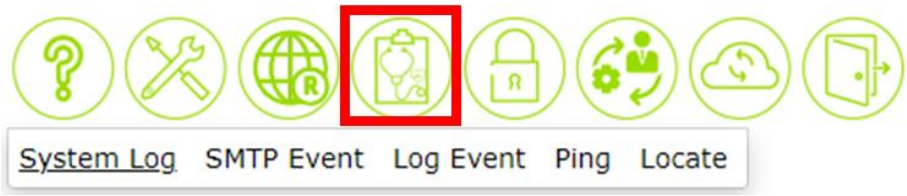
Figure 48. NAPT Setting Pop-up Window



5 Diagnostic

The Diagnostic function allows the user to check the operation of the access point through the following features: **System Log, SMTP Event, Log Event, Ping** and **Locate**. The Diagnostic function is the fourth circular icon with stethoscope picture on top of a medical chart. Figure 49 illustrates the list of features under the Diagnostic function.

Figure 49. Diagnostic Function on Menu Bar



5.1 *System Log Feature*

The System Log feature under the Diagnostic function contains two sections: **System Log Setting** and **System Log** as shown in Figure 50. 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 51. Note that this pop-up window is the same feature as described in Log feature under the Information function in Table 6.

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 5 in Section 3.5 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 access point.

Figure 50. System Log Feature

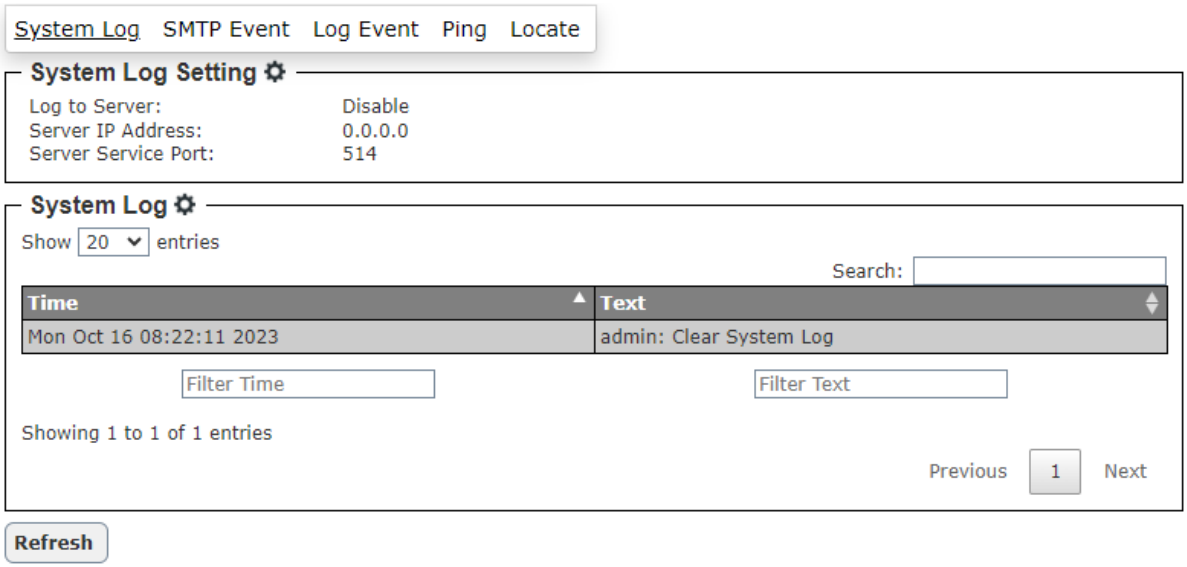
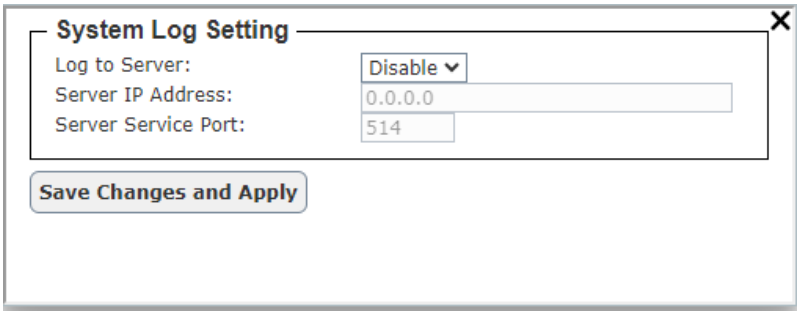
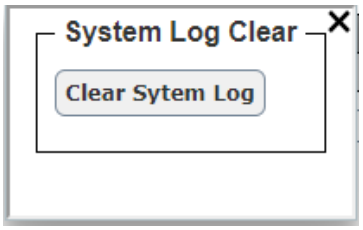


Figure 51. Systm Log Setting Pop-up Window



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 52. By clicking on the Clear System Log button on this pop-up window, the user can clear all log entries.

Figure 52. Systm Log Clear Pop-up Window



5.2 *SMTP Event Feature*

When AW5601 device raises an alert and/or a warning message, it can send an e-mail to an administrator's mailbox. This E-mail Settings web page allows you to set up the AW5601 to be able to send an e-mail.

Figure 53. SMTP Event Feature

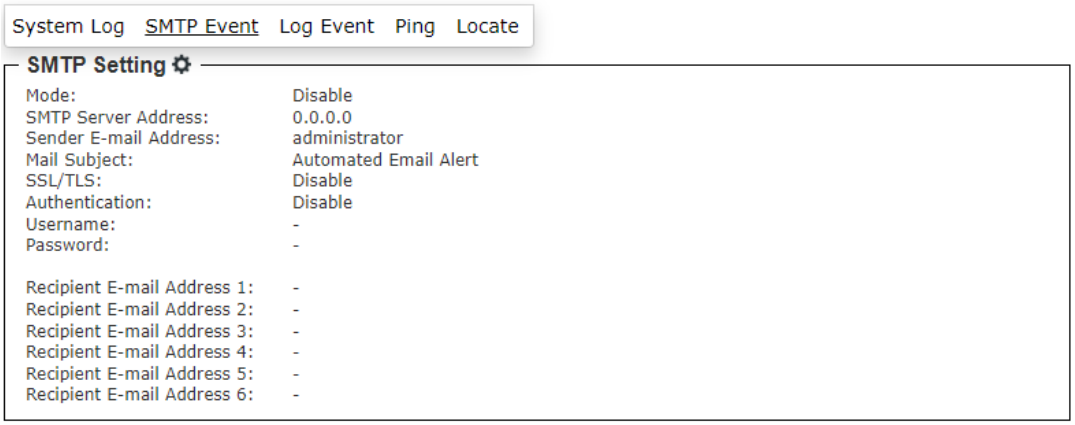
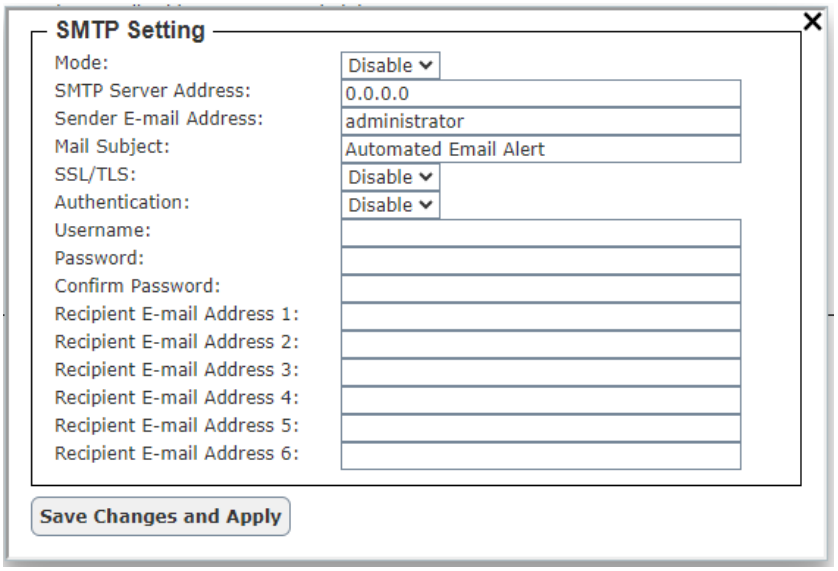


Figure 54. SMTP Event Setting Pop-up Window



5.3 *Log Event Feature*

Figure 55. Log Event Feature

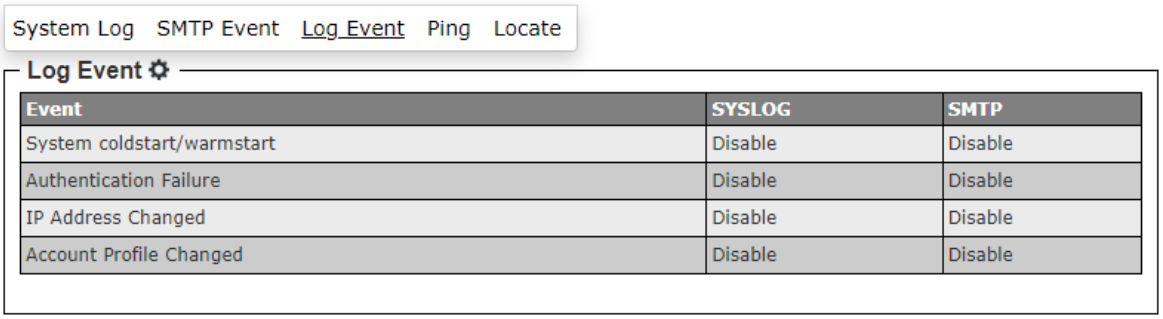
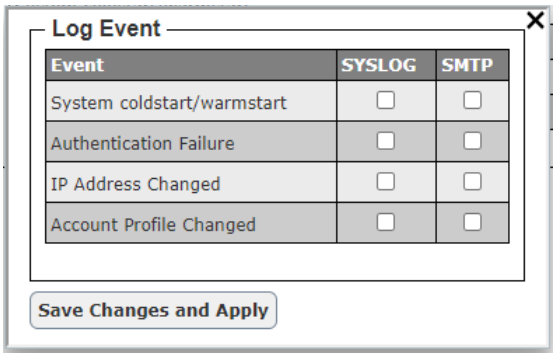


Figure 56. Log Event Pop-up Window



5.4 *Ping Feature*

The Web UI of AW5601 has an interface to call Ping, which is a network diagnostic utility for testing reachability. You can use the Ping function to determine whether AW5601 can reach the gateway or other devices in the network. To use the Ping, enter a destination IP address in the text box and click

Ping button as shown in Figure 57. This process usually takes around 20 seconds. The two figures below represent a successful ping without packet loss from AW5601 to the address 10.0.50.200 and back, and the connecting device at the address 10.0.50.2 is unreachable in which no packets have returned from the transmitted ping packets.

Figure 57. Ping Feature

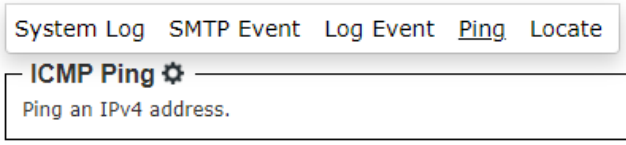


Figure 58. Ping Pop-up Window

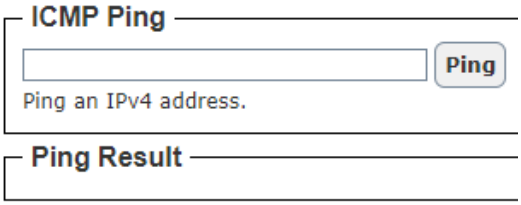


Figure 59. Ping Successful with No Packet Loss

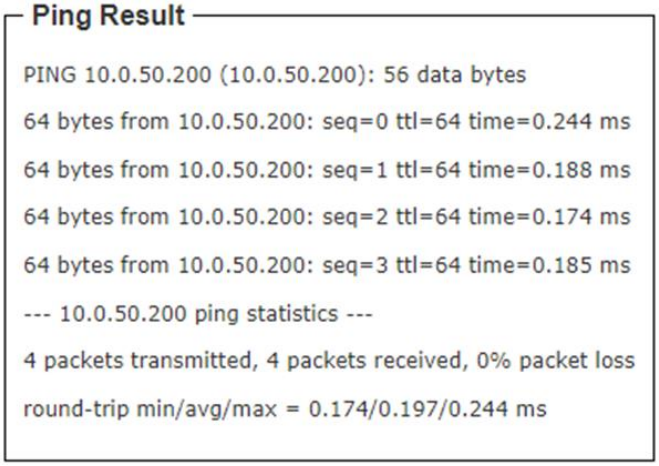
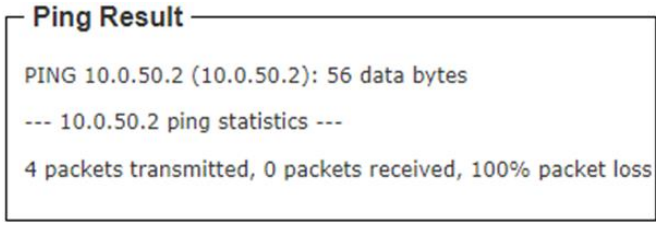


Figure 60. Ping Unsuccessful with 100% Packet Loss



5.5 *Locate Feature*

The Locate function can provide quick positioning in the device group. When the **Turn On** button on the WEB is pressed, the position of the "Locate" light in the Panel on the left side of the WEB UI will turn from black to red, as shown in Figure 63, and at the same time, the "Locate" light on the machine will also light up in red. If you press the **Turn Off** button, the "Locate" light on the panel on the left side of

the WEB UI will turn from red to black, as shown in Figure 64, and the red light of the device entity's Locate will also turn off.

Figure 61. Locate Feature

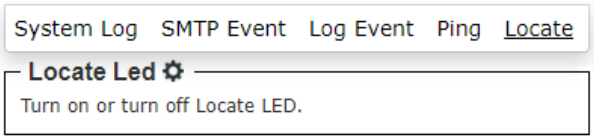
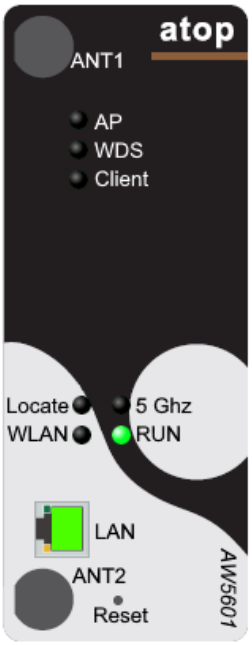


Figure 62. Locate Pop-up Window

Figure 63. Locate Turn-on State on Panel

Figure 64. Locate Turn-off State on Panel



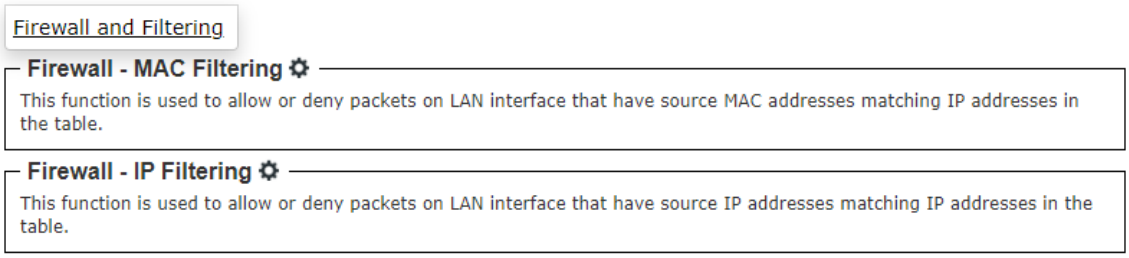
6 Security

Figure 65. Security Function on Menu Bar

The following sections describe how to set up the network firewall and its packet filtering in the AW5601. Available criteria for packet filtering are based on MAC address (wired or wireless) and IP address. These filtering methods provide security by preventing unauthorized or malicious packets from entering your network. Packets will be filtered (or classified) as "allowed packets" or "denied packets".

The "allow packets" mode is often called "whitelisting" and the "deny packets" mode is often called "blacklisting". We strongly recommend that you take extra care in this section, as data that does not meet any of these criteria will be discarded and, if configured incorrectly, may render the AW5601 inaccessible. If the latter occurs, you will need to reset the device back to factory defaults by any of the methods described in Section 8.4.

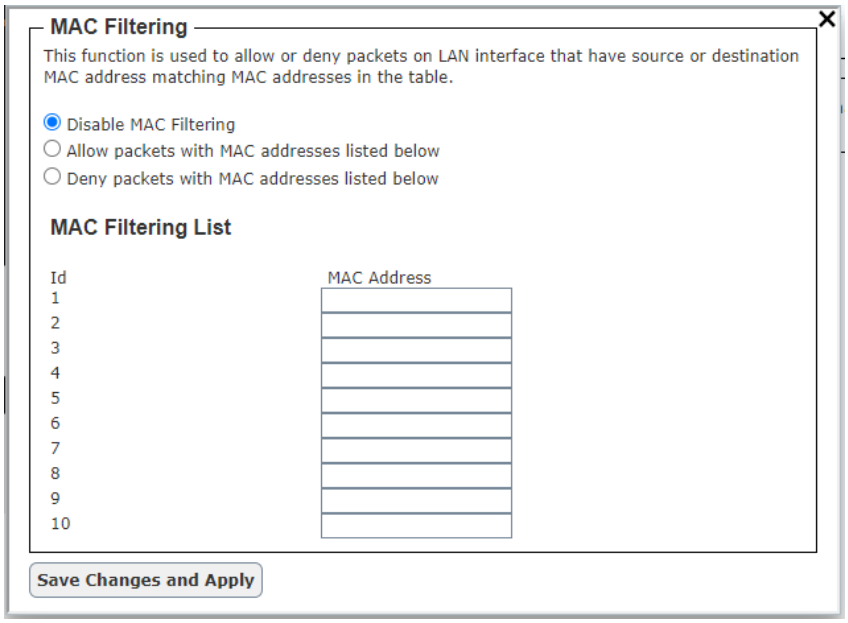
Figure 66. Seurity Feature



6.1 *Firewall - Mac Filtering Feature*

This function helps users to filter packets from the specific MAC address.

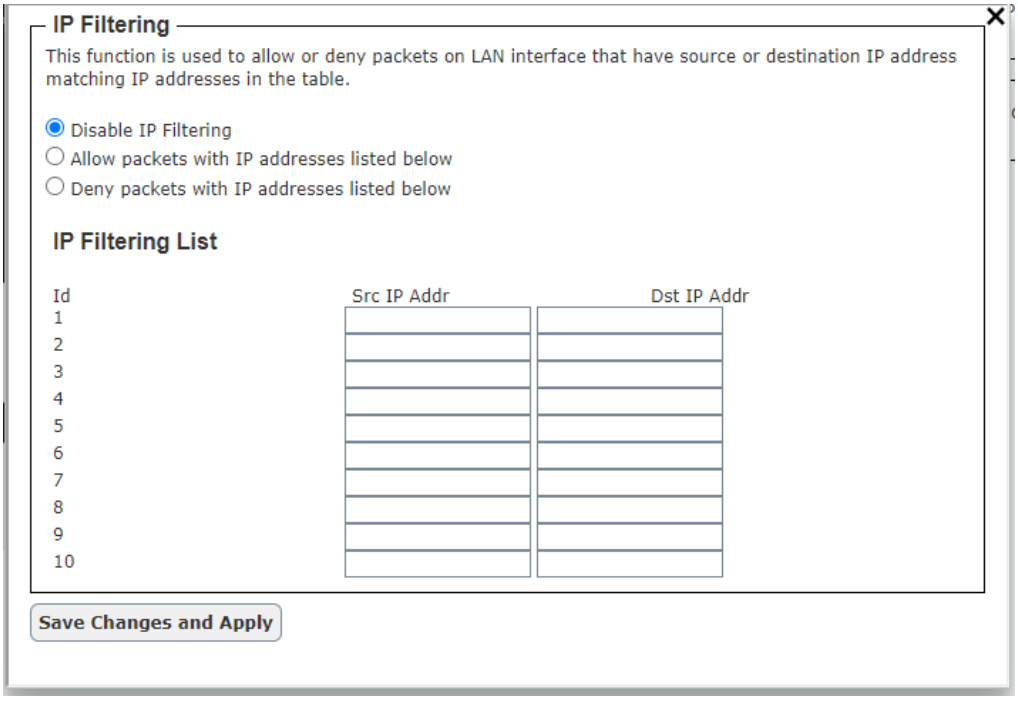
Figure 67. Firewall – Mac Filtering Pop-up Window



6.2 *Firewall - IP Filtering Feature*

This function helps users to filter packets from the specific IP address.

Figure 68. Firewall – IP Filtering Pop-up Window



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/Telnet/SSH**, and **SNMP** as shown in Figure 69. These features allow the user to manage the accounts, enable secure HTTP for web interface, and set up the SNMP protocol.

Figure 69. Management Function on Menu Bar

7.1 *Account Feature*

The Account feature is shown in Figure 70 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 71. 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 list, entering all information then click the **Delete User** button.

Figure 70. Account Feature

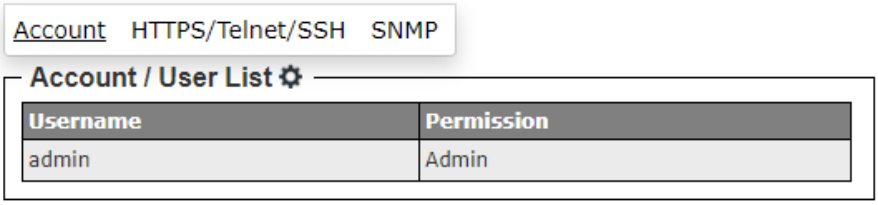
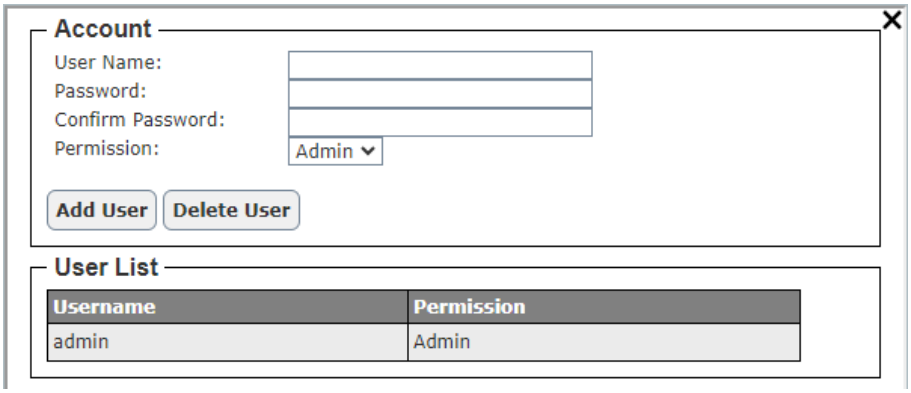


Figure 71. Account Pop-up Window



7.2 *HTTPS/Telnet/SSH Feature*

The HTTPS or Hyper Text 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 72. 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 73. Next checking the Enabled box to redirect web interface access to HTTPS protocol. After you finished, clicking on the **Save Changes and Apply** button to save and apply the settings.

Figure 72. HTTPS/Telnet/SSH Feature

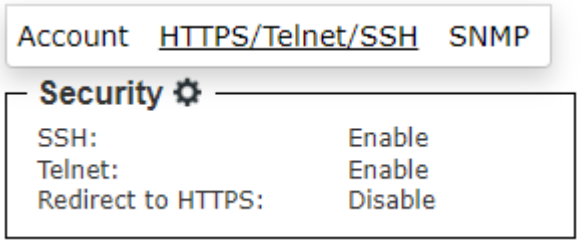
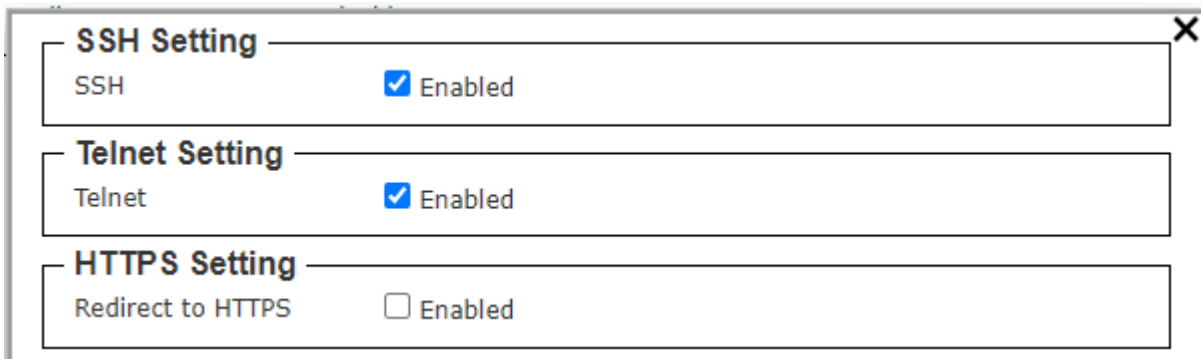


Figure 73. HTTPS/Telnet/SSH Feature Pop-up Window

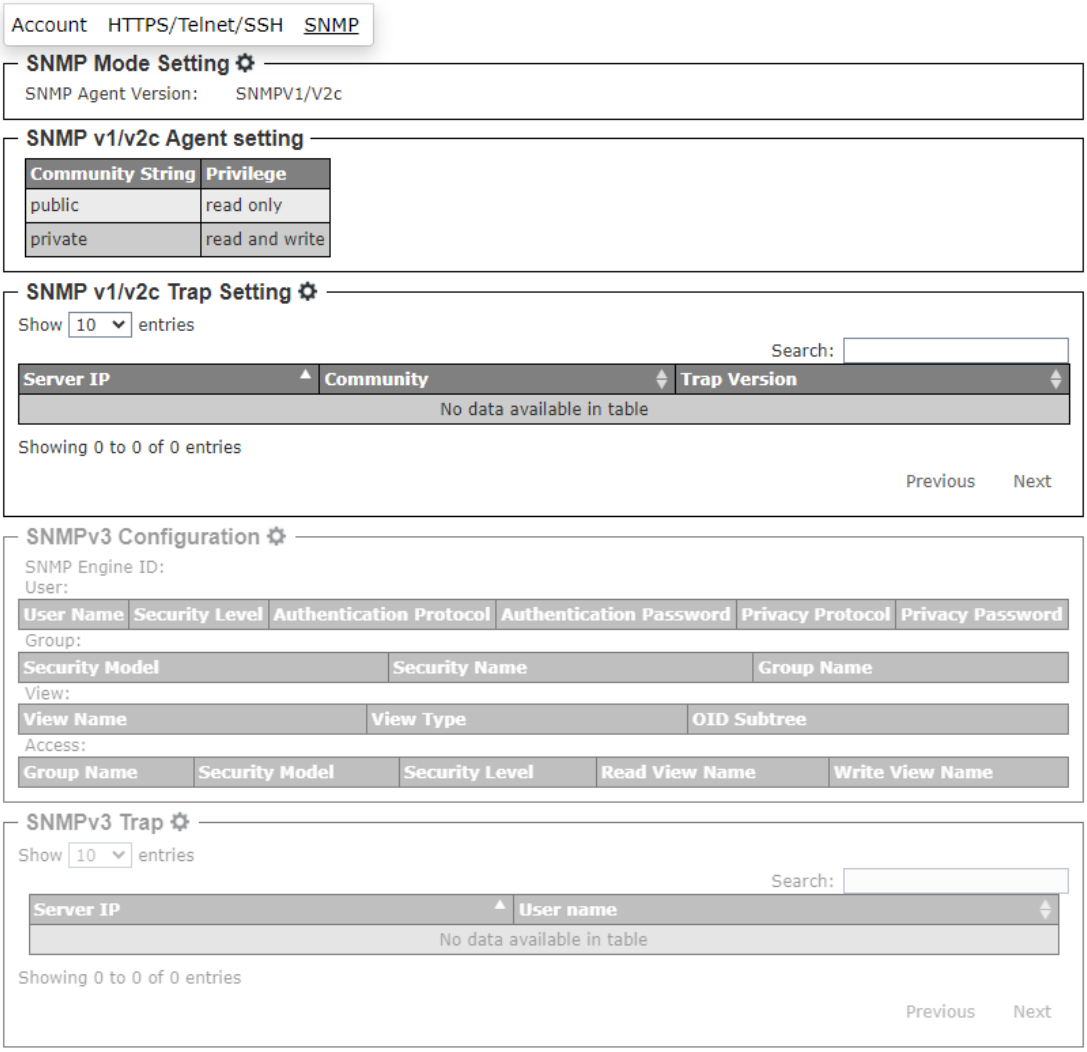


7.3 *SNMP Feature*

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 wireless access point support SNMP and can be configured through this feature under the Management function.

Figure 74 shows the SNMP feature' s web page. It consists of four sections: **SNMP Mode Setting**, **SNMP v1/v2c Agent Setting, SNMP 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 Agent 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 75.

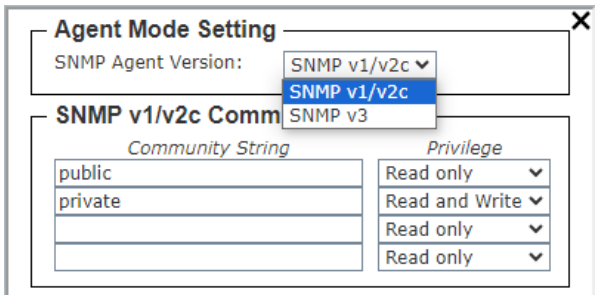
Figure 74. SNMP Feature



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 75. When the SNMP v1/v2c is selected, the

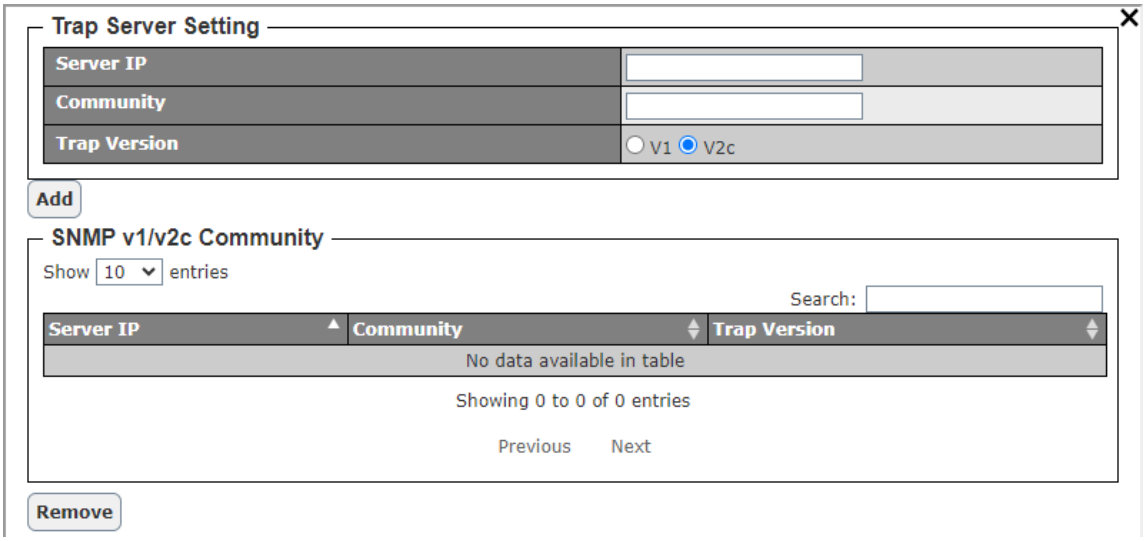
Community String and Privilege of each Community String can be managed as shown in the figure. After you finished, clicking on the **Save Changes and Apply** button to save and apply the settings.

Figure 75. SNMP Agent Mode and SNMP v1/v2c Community Managment



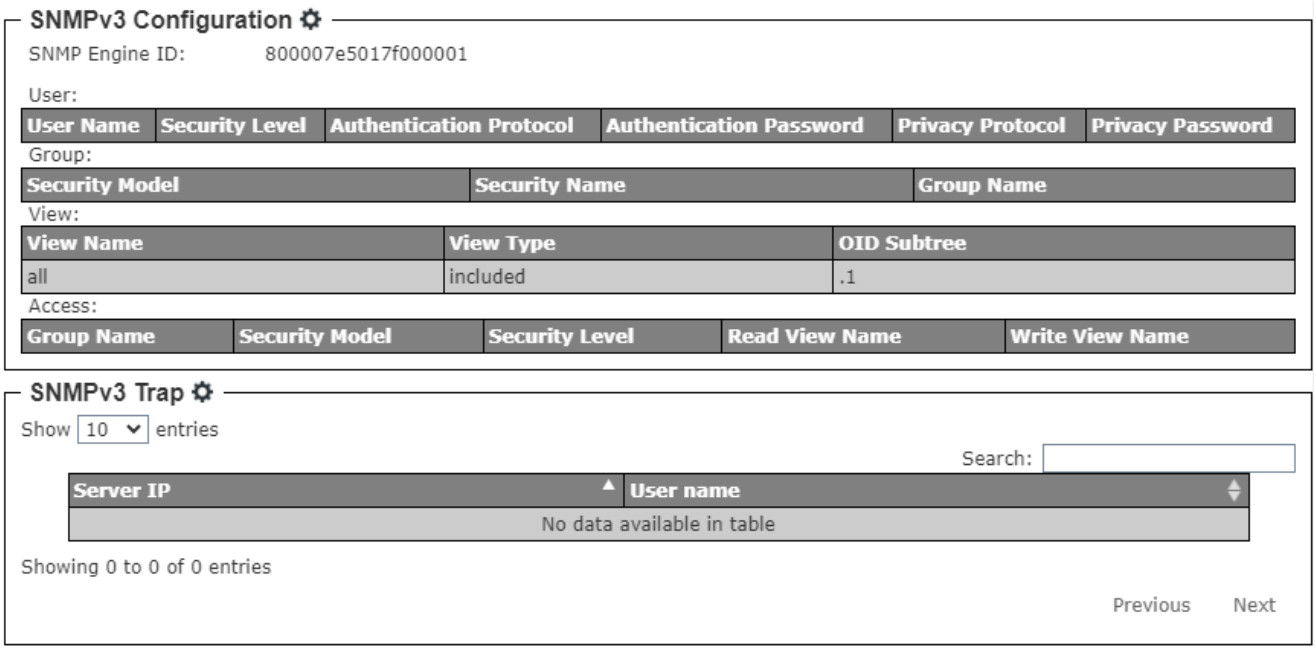
While SNMP Agent Version is set as SNMP v1/v2c, the SNMP v1/v2c Trap Setting section is active. The user can configure Trap Server by clicking on the gear icon next to the SNMP v1/v2c Trap Setting. A pop-up window as shown in can be used to manage the trap server by adding Trap Server IP and Community, and select 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 76. SNMP v1/v2c Trap Management



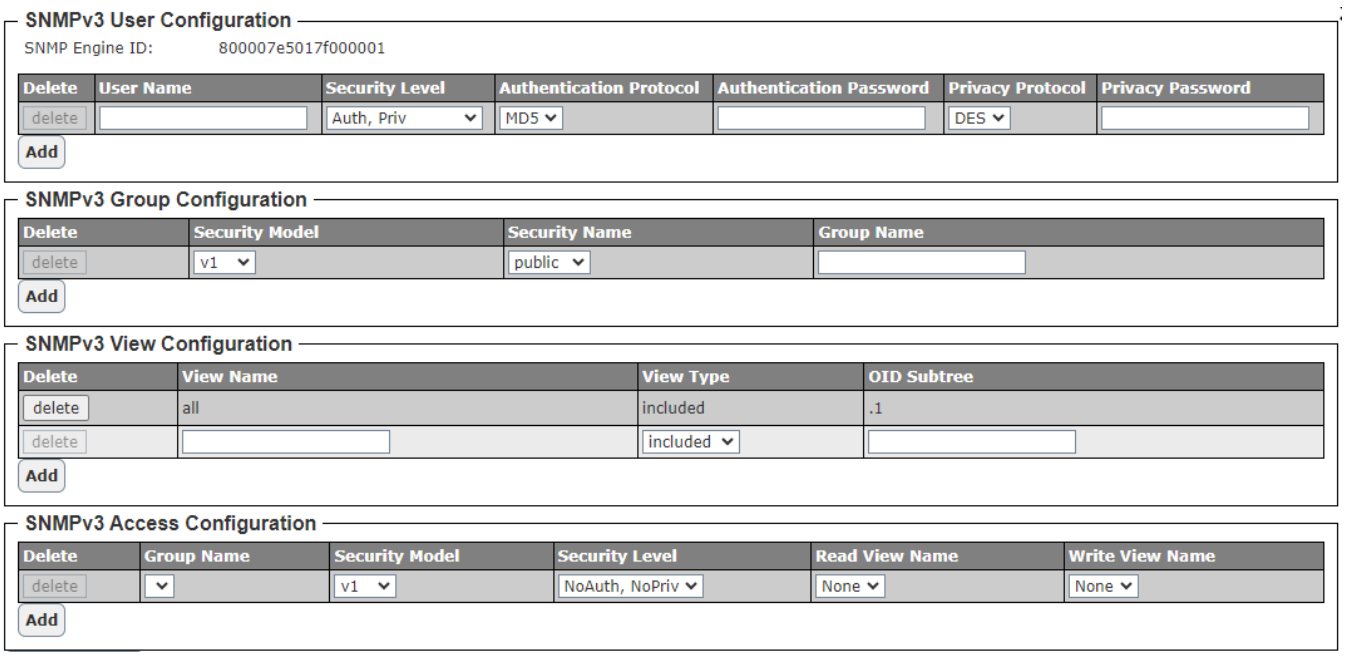
If SNMP Agent Version is set to SNMP v3, the SNMP v3 Configuration and SNMP v3 Trap sections will become active as shown in Figure 77. This web page provides detailed setup of SNMP v3 Configuration and SNMP v3 Trap Server.

Figure 77. SNMP v3 Feature



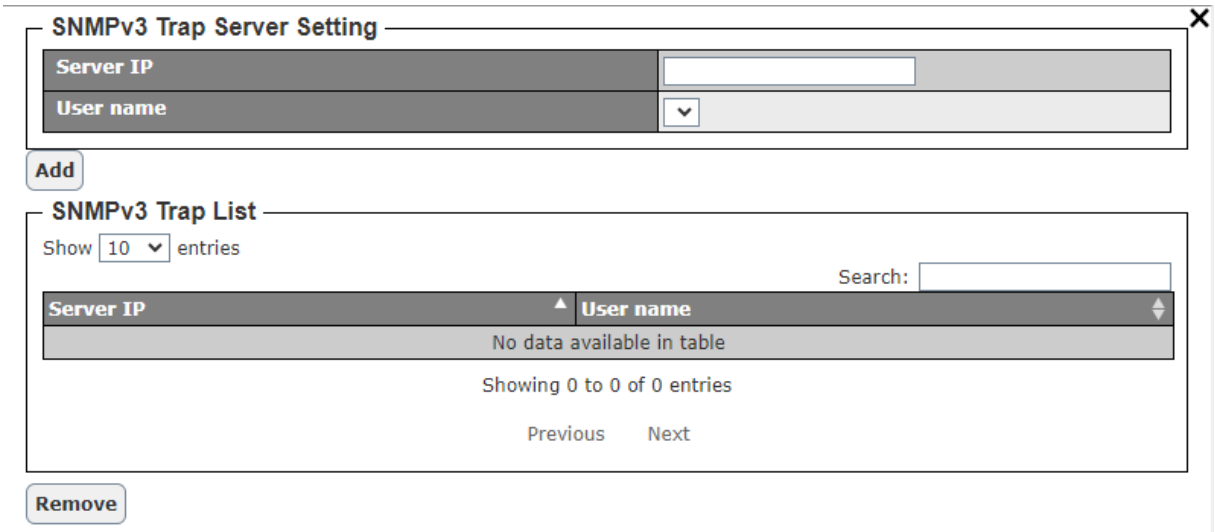
To configure SNMP v3, the user can click the gear icon next to the SNMP v3 Configuration to bring up the pop-up window as shown in Figure 78. On this window, there are four sections: SNMP v3 User Configuration, SNMP v3 Group Configuration, SNMP v3 View Configuration, and SNMP v3 Access Configuration. 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 and Apply** button to save and apply the settings.

Figure 78. 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 77 to bring up another pop-up window as shown in Figure 79. 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.

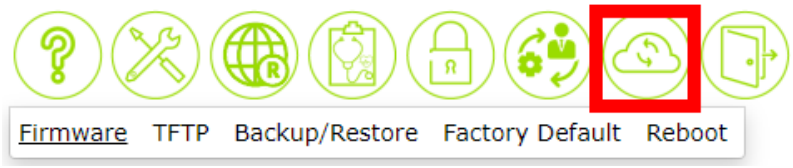
Figure 79. SNMP v3 Trap Server Setting Pop-up Window



8 Maintenance Feature

The Maintenance function is the seventh circular icon on the menu bar. It is the icon with cloud and arrow. The Maintenance function has five features which are **Firmware, TFTP, Backup/Restore, Factory Default**, and **Reboot** as shown in Figure 80. These features allow the user to upgrade firmware, backup/restore configuration, factory default, and reboot device.

Figure 80. Maintenance Function on Menu Bar



8.1 *Firmware Feature*

The firmware feature under the Maintenance function shows about the AP's firmware. The user can check the **Current Loader Version, Kernel Version and Firmware Version** under the Upgrade Firmware section. When the upgrade progress completed, the device will reboot by self.

Figure 81. Firmware Feature

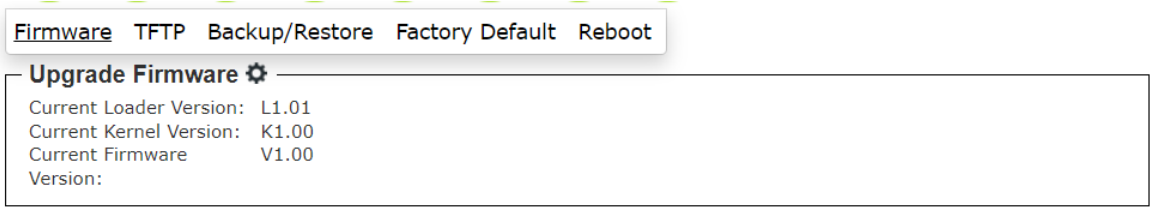


Figure 82. Upgrade Firmware Pop-up Window

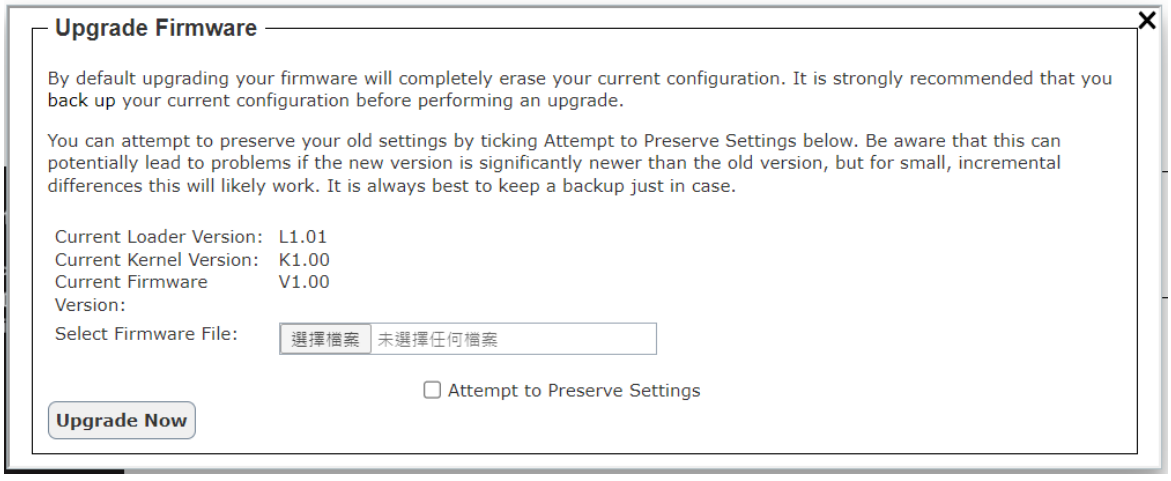
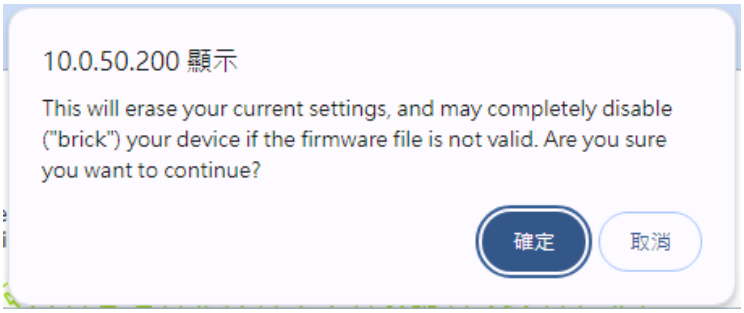


Figure 83. Upgrade Firmware Pop-up Alert Window

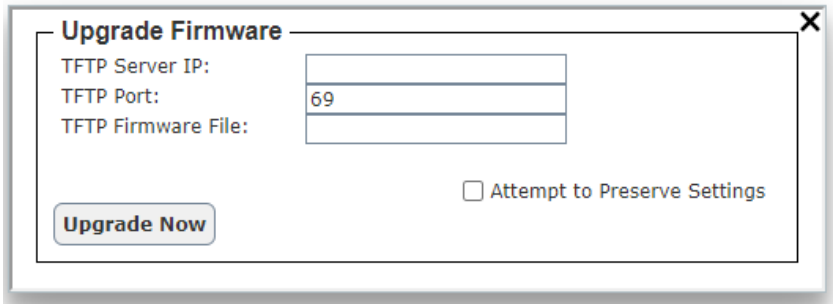


8.2 *TFTP Feature*

TFTP feature under the Maintenance function allows the user to Upgrade Firmware. The user can check **TFTP Server IP, TFTP Port, TFTP Firmware file, and Attempt to Preserve Settings.** After you finished, clicking on the **Upgrade Now** button to upgrade firmware from TFTP protocol.

Figure 84. TFTP Feature

Figure 85. TFTP Pop-up Window



8.3 *Backup / Restore Feature*

The Backup/Restore feature under the Maintenance function is an alternative feature that allows the user to backup or restore configuration file to or from the local host computer inside the AW5601. Note that Backup/Restore feature in previous subsection download or load the configuration file to and from the local host computer. Static Routes

Figure 86. Backup/Restore Feature

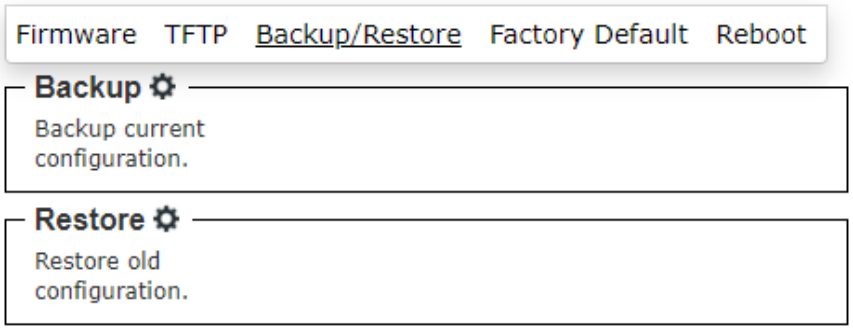


Figure 87. Backup Pop-up Window

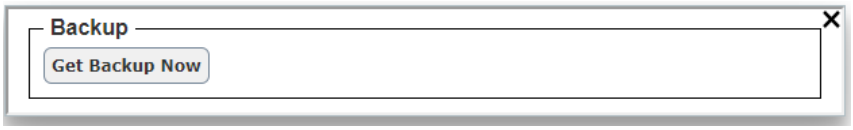


Figure 88. Restore pop-up window

8.4 *Factory Default Feature*

The Factory Default feature under the Maintenance function allows the user to reset the device to the original or factory default configuration. The Factory Default web page is shown in Figure 89. 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 90. Then, clicking on the **Restore Default Configuration Now** button to restore the configuration of the device to the factory default setting.

Figure 89. Factory Default Feature

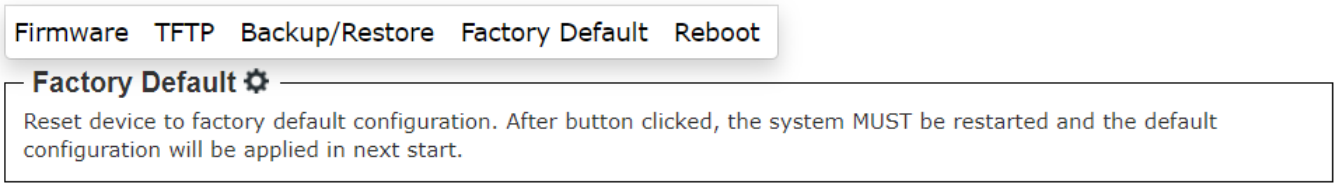
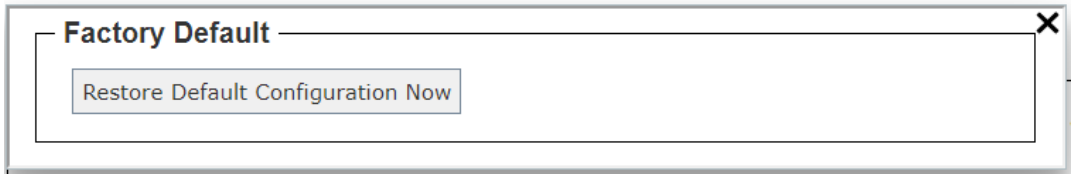


Figure 90. Factory Default Pop-up Window



The AW5601 Industrial Wireless Access Point is equipped with one LAN interface and its network default setting is summarized in Table 18. Upon arrival, it will be set to work as AP mode. Its factory default parameters are listed in Table 19.

Table 18. Network Default Setting

Interface	Device IP	Subnet Mask	Gateway IP	DNS
LAN	10.0.50.200	255.255.0.0	0.0.0.0	0.0.0.0

Table 19. Wireless Factory Default Setting

Mode	AP mode	WDS	Flash-Roaming	Client mode
Wi-Fi Radio	Disabled			Enabled
Operating Mode	AP	WDS-AP/Client/Hybrid	AP	Client
Country	TW			
Tx Power	Medium			
Network Name (SSID)	AW5601		flash-roaming	N/A
Hide SSID	Disabled		N/A	N/A
Wireless Mode	5G(802.11n/ac)			
Channel Bandwidth	20 MHz			
Control Channel	36			
Authentication Method	WPA2 Personal (PSK)		WPA3 Personal (SAE)	WPA2 Personal (PSK)
Password	12345678		Default123	12345678
Client Isolate	Disabled		Enabled	N/A
NAT Enabled	N/A	N/A	Enabled	
Active Scan			N/A	Disabled
WLAN IP Setting (WAN)				

Mode	AP mode	WDS	Flash-Roaming	Client mode
DHCP Client	N/A		Disabled	
IPV4 Address			Empty	
Subnet Mask			Empty	
Gateway IP			Empty	
LAN IP Setting (WAN)				
IPV4 Address	N/A		10.0.50.200	
Subnet Mask			255.255.0.0	
Flash-Roaming Setting				
MCS	N/A		Auto	N/A
RSSI Link Threshold			-70	
Roaming Sensitivity			High	
Hole Time			250 ms	
PROFINET Transparent			Disabled	

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 91. To reboot the device, clicking on the gear icon next to Reboot to bring up the pop-up window as shown in Figure 92. Then, clicking on the **Reboot Now** button to reboot the device.

Figure 91. Reboot Feature

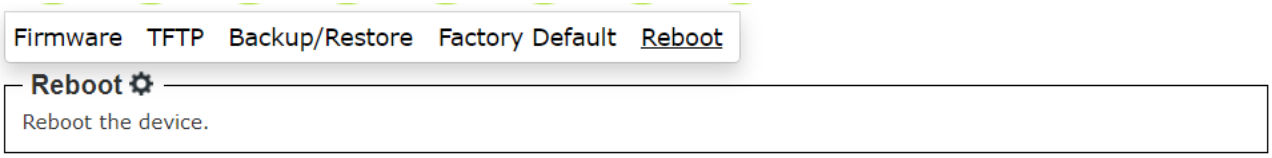
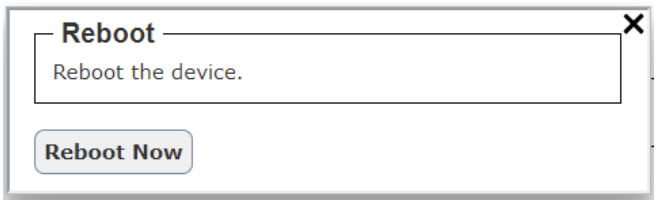


Figure 92. Reboot Pop-up Window



9 Logout

To logout of the AW5601, the user can click on the **Logout** icon which is the last circular icon with an opened door as shown in Figure 93. After clicked on the icon, the user will be returned to the login page as shown in Figure 3.

Figure 93. Logout Function on Menu Bar

10 Specifications

10.1 *Hardware Specification*

Table 20. Hardware Specification

System	
CPU	ARM Cortex A53 Dual Core 1GHz
Flash Memory	*32MB*
RAM	*DDR3L 512MB*
Network	
Ethernet Interface	1x10/100/1000 LAN Connector: RJ45(802.3at PoE PD; optional)
Wireless Interface	802.11a/g/n/ac 2T2R MIMO
Wi-Fi Security	WPA/WPA2/WPA3 PSK/Enterprise
LED Indicator	
LED indication	AP/WDS/Client Mode Location 5GHz WLAN RUN RJ45 Speed Link/ACK
Power Requirement	
Input	Single 12~48 VDC 3-pin terminal block connector
Mechanical	
Dimensions (W x H x D)	145 x 120 x 46 mm
Enclosure	IP30 protection, metal housing
Environmental	
Temperature	Operations -30°C ~ 70°C
	Storage -40°C ~ 85°C
Relative Humidity	5% ~ 95%, 55°C Non-condensing

10.2 *AW5601 Device Pin Assignments for WAN/LAN Port*

RJ45 connectors for 10/100/1000Base-T(X) Ethernet

Figure 94. WAN/LAN Port on RJ45 with Pin Numbering of AW5601 Device

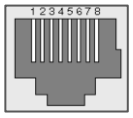


Table 21. Assignment for RJ-45 Connector of AW5601 Device

10/100/1000Base-T(x)								
Pin#	1	2	3	4	5	6	7	8
Signal	Tx+	Tx-	Rx+	-	-	Rx-	-	-
1000Base-T								
Pin#	1	2	3	4	5	6	7	8
Signal	BI_DA+	BI_DA-	BI_DB+	BI_DC+	BI_DC+	BI_DB-	BI_DD+	BI_DD-

It is strongly recommended for you to set the Network Parameters through **Device Management Utility©** first. Other device-specific configurations can later be carried out via Atop's user-friendly Web-Interface.

11 Glossary

- AP – Access Point
- APN – Access Point Name
- AS – Autonomous System
- BIRD – Bird Internet Routing Daemon
- BSSID – Basic Service Set Identifiers
- CAP – Central Acccess Point
- CIDR – Classless Inter-Domain Routing
- DHCP – Dynamic Host Configuration Protocol
- DDNS – Dynamic Domain Name Service
- DNS –Domain Name Service
- FQDN – Fully Qualified Domain Name
- IP – Internet Protocol
- IP Address – Internet Protocol Address
- IGP – Interior Gateway Protocol
- ISP – Internet Service Provider
- LAN – Local Area Network
- LSR – Link State Routing
- LTE – Long Term Evolution
- MTU - Maximum Transmission Unit
- MU-MIMO – Multi-user Multiple-Input Multiple-Output
- NAT – Network Address Translation
- NTP – Network Time Protocol
- OSPF – Open Shortest Path First
- PPPoE – Point-to-Point Protocol over Ethernet
- QMI – Qualcomm MSM Interface
- RSSI - Received Signal Strength Indicatior
- SIM – Subscriber Identity Module
- SMS – Short Message Service
- SNR – Signal to Noise Ratio
- SSID – Service Set Identifier
- SSL – Secure Sockets Layer
- STP – Spanning Tree Protocol
- TLS – Transport Layer Security
- VPN – Virtual Private Network
- WAN – Wide Area Network

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