



AW5601/AW5601-IC Industrial AP Router

Device Setup
Architectural overview
AW5601

User Manual

V1.0
11th July 2024

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.

- [General Description](#)
 - [User Guide](#)
-

Published by:**ATOP Technologies, Inc.**

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

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

Important Announcement

The information contained in this document is the property of ATOP technologies, Inc., and is supplied for the sole purpose of operation and maintenance of Atop Technologies, Inc., products.

No part of this publication is to be used for any other purposes, and it is not to be reproduced, copied, disclosed, transmitted, stored in a retrieval system, or translated into any human or computer language, in any form, by any means, in whole or in part, without the prior explicit written consent of ATOP Technologies, Inc.,

Offenders will be held liable for damages and prosecution.

All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

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.

Documentation Control

Author:	Shawn Lee
Revision:	1.1
Revision History:	Feature/Title Update
Creation Date:	20 November 2023
Last Revision Date:	16 August 2024
Reviewer	Shawn Lee
Product Reference:	AW5601/AW5601-IC Industrial AP Router Family
Document Status:	Released

Table of Contents

1	Introduction	8
1.1	Overview.....	8
1.2	Software Features	9
2	Getting Started	10
2.1	Default Factory Settings	10
	The Reset Button.....	10
2.2	Login Process and Main Window Interface	10
	Login Process.....	10
	Main Window Interface	12
3	Main Menu	17
3.1	Information Feature.....	17
3.2	AP/Client Feature	19
3.3	Industrial Communication Feature.....	19
3.4	LAN IP Feature.....	20
3.5	WDS Feature	21
3.6	Log Feature.....	21
4	Configuration	23
4.1	LAN IP Feature.....	24
4.2	DHCP Server Feature.....	25
4.3	System Time and SNTP Feature	27
4.4	NAT Feature.....	29
	Basic NAT (N:1 NAT).....	29
	Static NAT (1:1 NAT).....	30
	NAPT (Network Address Port Translation)	31
4.5	Bridge Feature	32
5	Wi-Fi	33
5.1	AP/Client Mode Feature.....	34
	AP / Client Mode	34
5.2	WDS Mode Feature.....	35
	WDS-AP / Client / Hybrid Mode (Non-NAT)	35
5.3	Industrial Communication	38
	Industrial Communication AP / Industrial Communication Client Mode.....	38
	PROFINET Transparent over Industrial Communication mode and NAT	41
6	Diagnostic	43
6.1	System Log	43
6.2	SMTP Event	44
6.3	LLDP	45
6.4	Log Event	46
6.5	Ping	47
6.6	Locate	48
7	Security	49
7.1	Firewall - MAC (Wired / Wireless) Filtering	50
7.2	Firewall – IP Filtering.....	50
8	Management	52

8.1	Account Feature	52
8.2	HTTPS/Telnet/SSH Feature	53
8.3	SNMP Feature.....	54
9	Maintenance Feature	58
9.1	Firmware Feature	58
9.2	TFTP Feature	59
9.3	Backup / Restore Feature	60
9.4	Factory Default Settings	61
9.5	Reboot Feature	64
10	Logout.....	65
11	Specifications	65
11.1	Hardware Specification.....	65
11.2	AW5601 Device Pin Assignments for WAN/LAN Port	66
12	Glossary.....	67

List of Figures

Figure 1.1 An Application of Industrial Wireless Access Point in WLAN.....	8
Figure 2.1. IP Address for the Web-based Setting	11
Figure 2.2. Login Prompt	11
Figure 2.3. Default Web Interface for AW5601	11
Figure 2.4. Function Bar on Top of Web GUI	12
Figure 2.5. Main Window Interface	12
Figure 2.6. Logo and Banner Information	13
Figure 2.7. Panel Information	13
Figure 2.8. Function Bar on Top of Web GUI	13
Figure 2.9. Sub-Function Button.....	14
Figure 2.10. Pop-up Window.....	15
Figure 2.11. Configuration Window.....	15
Figure 2.12. Save Changes and Apply Button	16
Figure 3.1. Main Menu	17
Figure 3.6.1. Log Feature.....	21
Figure 3.6.2. System Log Setting Pop-up Window	22
Figure 4.1.1. Configuration Function	23
Figure 4.1.2. LAN IP Feature.....	24
Figure 4.1.3. IP Network Setting Pop-up Window	24
Figure 5.1. Configuration Function.....	33
Figure 6.1. Diagnostic Function on the Menu Bar	43
Figure 6.1.4. System Log Clear Pop-up Window	44
Figure 6.5.3. Ping Successful with No Packet Loss.....	48
Figure 7.1. Security Function on Menu Bar.....	49
Figure 8.1. Management Function on the Menu Bar.....	52
Figure 9.1. Maintenance Function on the Menu Bar	58
Figure 9.11. Reboot Feature	64
Figure 9.12. Reboot Pop-up Window.....	64
Figure 10.1. Logout Function on Menu Bar	65
Figure 11.1. WAN/LAN Port on RJ45 with Pin Numbering of AW5601 Device	66

List of Tables

Table 2-1 Default Settings of the Network Interfaces.....	10
Table 2-2. Login Default Settings	10
Table 2-3. Descriptions of the Function Bar	14
Table 3-1. Descriptions of the Information Features	18
Table 3-3. Description of System Log Setting Pop-up Entry.....	22
Table 4-1. Description of IP Network Settings	24
Table 5-2. Description of Wi-Fi mode with packet forwarding	33
Table 5-3. AP/Client Mode Setting.....	35
Table 5-4. IP Address Settings for Devices in AP/Client Mode.....	35
Table 5-5. WDS-AP/WDS-Hybrid/WDS-Client Mode for APs Setting	37
Table 5-6. Industrial Communication AP / Industrial Communication Client Mode Setting	38
Table 5-7. Devices IP Address Setting	38
Table 5-8. Descriptions of the Industrial Communication AP Mode.....	39
Table 5-9. Descriptions of the Industrial Communication Client Mode.....	40
Table 5-10. Industrial Communication AP / Industrial Communication Client Mode Setting	41
Table 5-11. Industrial Communication AP / Client Mode's Device IP Address Setting	41
Table 9-1. Network Default Setting	62
Table 9-2. Wireless Factory Default Setting	63
Table 11-1. Hardware Specification.....	65
Table 11-2. Assignment for RJ-45 Connector of AW5601 Device	66

1 Introduction

1.1 Overview

Atop's AW5601 Series is a line of wireless products designed for applications in harsh environments. 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 practically any surface in the workplace. Reliability is a key factor for choosing the AW5601 when a wireless solution is needed. The small size of the AW5601 casing is also ideal for small spaces while providing 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 network. It can be operated as an access point (AP), a wireless distribution system (WDS) bridge, or an AP client. For example, a user can connect serial devices to an Atop's Wireless Serial Device Server (e.g., SW55XX series) and then connect the serial device server to the AW5601 Industrial Wireless Access Point. This configuration allows the serial devices to be accessed over a wireless local area network (WLAN). Note that the AW5601 follows the IEEE 802.11 a/b/g/n/ac wireless connectivity standards.

Figure 1.1 shows another example where the AW5601 operates in AP client mode and associates with another WLAN AP called AP1. In this example, the personal computer (PC) and the IP camera connected to Atop's industrial Managed Ethernet Switch (e.g., EH/EHG/EMG/RHG Series) can be wirelessly connected to the control room on the other side of the network.

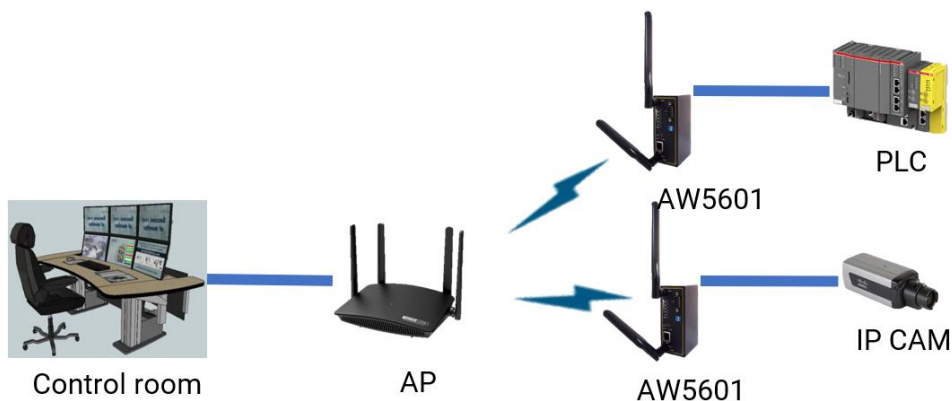


Figure 1.1 An Application of Industrial Wireless Access Point in WLAN

1.2 Software Features

AW5601 Platform

- 1x RJ45 for 10/100/1000 Mbps Base-T LAN
- Supports different operating modes and topology options (AP mode, WDS mode, and Client mode)
- Supports the most popular wireless local area network standards: IEEE 802.11a/b/g/n/ac
- Industrial EMC protection, wide-range temperature operation: -30°C to 70°C
- Rugged metal case with wall-mounted or DIN-rail mounted capability
- Supports PoE PD for flexible deployment
- Power supply input supporting 12 to 48 VDC
- Industrial Communication mode with less than 50 ms latency
- Supports PROFINET transparent mode
- Easy configuration through the embedded web server interface or Atop's Windows®-based configuration utility program, **Device Management Utility®**
- Firmware upgradeable through the embedded web server interface or Atop's **Device Management Utility®**

2 Getting Started

This chapter describes how to access the AW5601 for the first time. Users can easily access the industrial AP router using any of their web browsers. Internet Explorer 8 or 11, Firefox 44, Chrome 48, or later versions are recommended. Next, we will introduce the industrial AP router's functions using a web browser.

2.1 Default Factory Settings

Below is a list of the default factory settings. This information will be used during the first login process or after the device is reset to the factory default setting. Users can change these settings later. However, users should make sure that the computer accessing the AW5601 has an IP address within the same subnet and subnet mask as the AW5601.

The default network parameters of AW5601 are listed in the table below.

Table 2-1 Default Settings of the Network Interfaces

IP Address	Subnet Mask	Default Gateway
10.0.50.200	255.255.0.0	10.0.50.1

The default username and password for the web GUI login are listed in the table below. Please be aware that usernames and passwords are case-sensitive when entering them.

Table 2-2. Login Default Settings

Login Parameter	Default Values
Username	admin
Password	default

The Reset Button

If you forget the password or cannot access the device's web configuration, you can use the RESET button to restore to the factory default settings. The current configuration will be lost after resetting. The password will be reset to the factory default setting (see the device label), and the LAN IP address will be "10.0.50.200". To reset the device, follow these steps:

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

2.2 Login Process and Main Window Interface

Login Process

Before accessing the web configuration, users must log in. This can simply be done in three steps.

1. Launch a web browser.
2. Type in the device's IP address on the device (e.g. <http://10.0.50.200>), as shown in Figure 2.1.

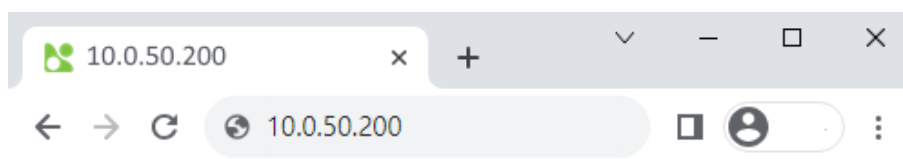


Figure 2.1. IP Address for the Web-based Setting

- The login prompt will be shown as in Figure 2.2. You can enter the default username and password displayed on the previous page, and then click the Login button.



Figure 2.2. Login Prompt

After the login process, the main web interface launches as shown in Figure 2.3. Directly below the Atop logo, some basic device information is listed including model name, loader version, kernel version, firmware version, serial number (SerialNum), and MAC address. Beneath these basic information, the main configuration menus for the AW5601 appear as a group of green, circular icons called the function bar. Users can access each configuration web page by clicking on the corresponding circular icon in the function bar. Moving the mouse's pointer over a particular icon will display a tooltip indicating its name.

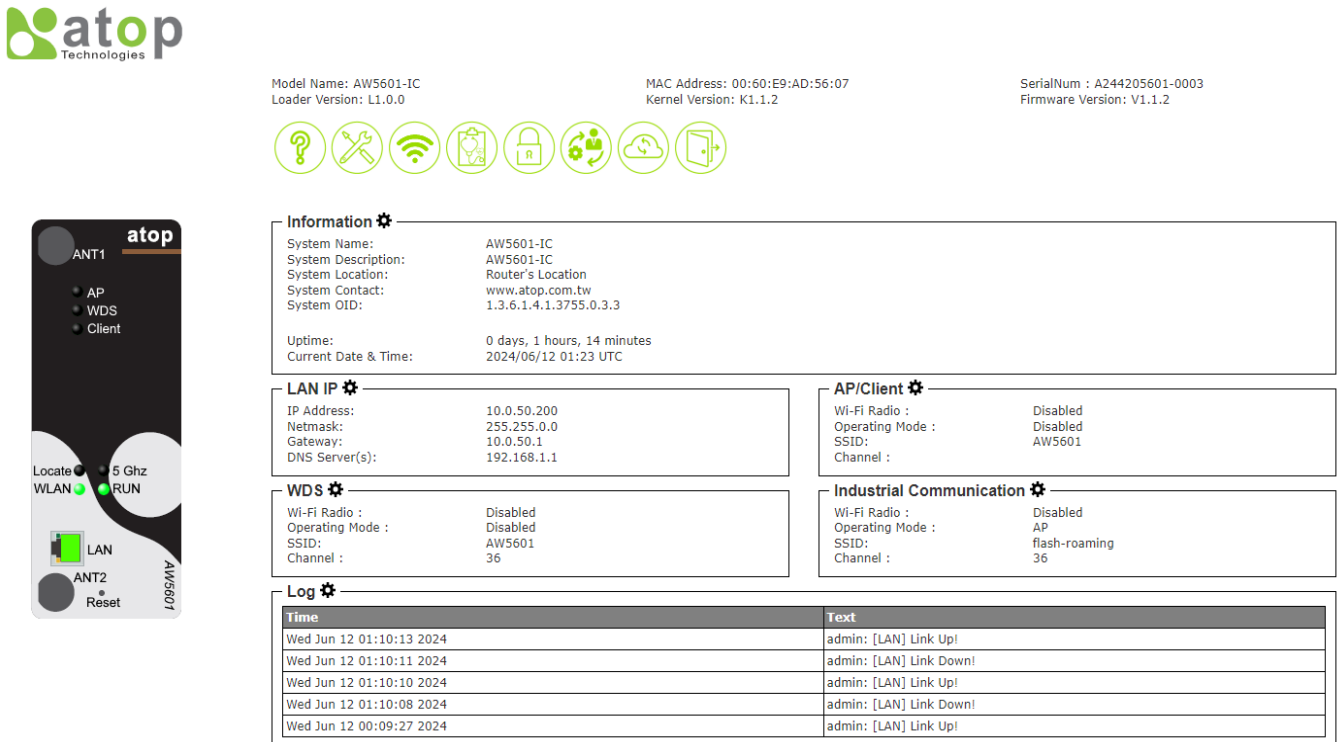


Figure 2.3. Default Web Interface for AW5601



Figure 2.4. Function Bar on Top of Web GUI

The function bar at the top of the web GUI is shown in Figure 2.4. It contains eight functions arranged from left to right: Information, Configuration, Wi-Fi, Diagnostics, Security, Management, Maintenance, and Logout.

For your convenience, the front panel of the AW5601 device is depicted on the left side of the screen and below the function bar. An example of front panel is shown in Figure 2.3. It displays the power LEDs, Wi-Fi mode, port link status, and so on. In this example, the LAN port is highlighted in green which indicates that the port is connected. Detailed explanations of each icon will be provided later.

Main Window Interface

Upon logging in, the main web page launches and displays several sections as shown in Figure 2.5. These sections, which are labelled as A through F, will be introduced as followings.

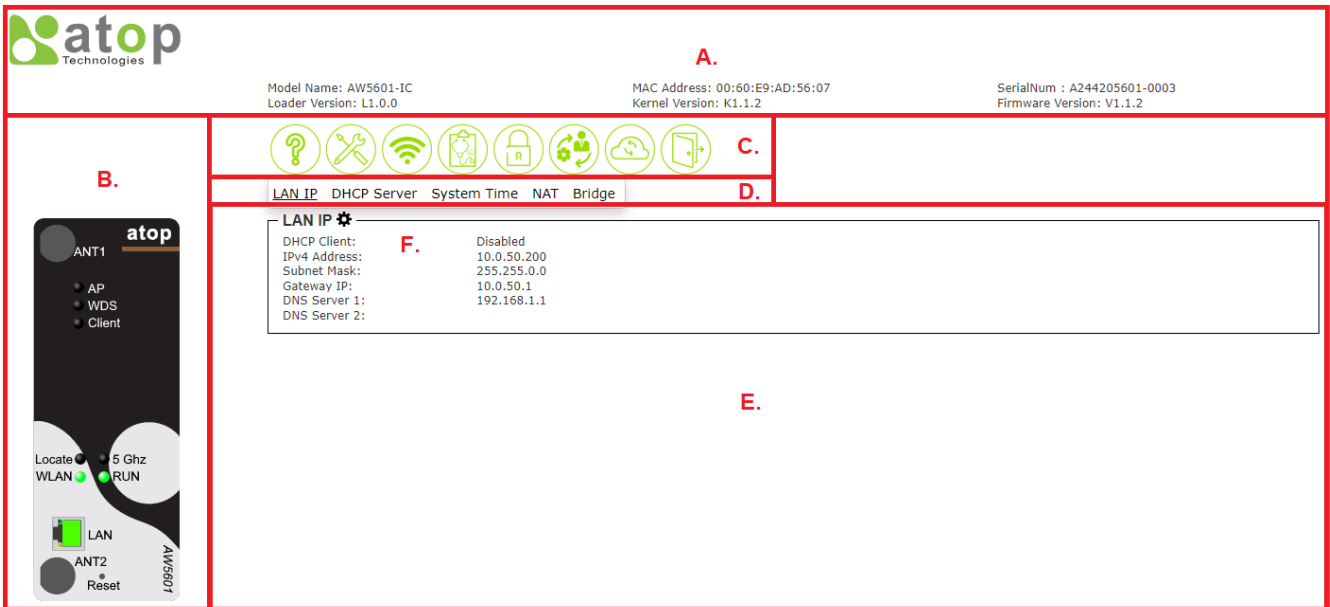


Figure 2.5. Main Window Interface

A. Banner with the Device Information

This section is located at the top of the web page. It displays the Atop logo and information about the device which are Model Name, Kernel Version, Firmware Version, Serial Number (SerialNum), MAC Address.



Model Name: AW5601-1C
Loader Version: L1.0.0

MAC Address: 00:60:E9:AD:56:07
Kernel Version: K1.1.2

SerialNum : A244205601-0003
Firmware Version: V1.1.2

Figure 2.6. Logo and Banner Information

B. Panel Information

Section B is located on the left side of the web page as shown in the figure below. It displays the power LEDs, Wi-Fi mode (including 5 GHz), WLAN, Locate function, and LAN port link status.



Figure 2.7. Panel Information









C. Function Bar

Function Bar is located right under Section A where all basic information is displayed. There are eight main function buttons in the function bar which are displayed in the circular icon shape as shown in the figure below. From left to right, the managed functions of these buttons are Information, Configuration, Wi-Fi, Diagnostic, Security, Management, Maintenance, and Logout.



Figure 2.8. Function Bar on Top of Web GUI

Table 2-3. Descriptions of the Function Bar

Button	Name	Description
	Information	After clicking this button, it will revert back to the default web page when first logging into the device. It includes device information, Wi-Fi, and Syslog functions.
	Configuration	User can configure the following device's settings through this web page including LAN IP, Wi-Fi, DHCP server, System time, and NAT functions.
	Wi-Fi	After clicking this button, user can view the Wi-fi function.
	Diagnostic	After clicking this button, the diagnostic page will be launched which will include Syslog, SMTP, Ping, and locate LED functions.
	Security	Security settings which include firewall and filtering functions can be configured through this button.
	Management	Functions for management include Account, HTTPS/Telnet/SSH, and SNMP functions.
	Maintenance	User can set the maintenance functions through this button which includes Firmware Upgrade, Configure Backup and Restore, Factory Default, and Reboot.
	Logout	After clicking this button, the current connection with the device will be shut down. The existing web page will be closed. The user will be returned to the login webpage.

D. Sub Function Button.

To view sub-functions of each icon in the main function bar, the user can simply hover the mouse's pointer over it. Figure 2.9 shows an example of the sub-functions of the configuration icon on the function bar.

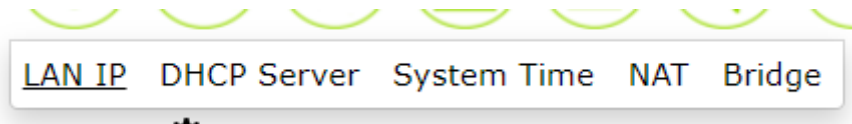



Figure 2.9. Sub-Function Button

E. Main display section

Section E shows the current operation function.

F. Gear button.

Section F is the area that displays details of a highlighted sub-function. In Section F, if a user clicks the gear button , it will pop-up a configuration window as shown in Figure 2.10. Each functionality within the pop-up window will be explained in Section G, H, and I.



Model Name: AW5601-1C MAC Address: 00:60:E9:AD:56:07 SerialNum : A244205601-0003
Loader Version: L1.0.0 Kernel Version: K1.1.2 Firmware Version: V1.1.2



LAN IP DHCP Server System Time NAT Bridge



LAN IP ⚙️

DHCP Client:	Disabled
IPv4 Address:	10.0.50.200
Subnet Mask:	255.255.0.0
Gateway IP:	10.0.50.1
DNS Server 1:	192.168.1.1
DNS Server 2:	

DHCP Setting H | X

DHCP Client:

IPv4 Setting

IPv4 Address:	<input type="text" value="10.0.50.200"/>
Subnet Mask:	<input type="text" value="255.255.0.0"/>
Gateway IP:	<input type="text" value="10.0.50.1"/>
DNS Server 1:	<input type="text" value="192.168.1.1"/>
DNS Server 2:	<input type="text"/>

G.

I.

Figure 2.10. Pop-up Window

G. Configuration Window

In Section G, user can configure each sub-function within it. Figure 2.11 shows the configuration window of LAN IP subfunction which includes DHCP Setting and IPv4 Setting.

DHCP Setting X


DHCP Client:

IPv4 Setting

IPv4 Address:	<input type="text" value="10.0.50.200"/>
Subnet Mask:	<input type="text" value="255.255.0.0"/>
Gateway IP:	<input type="text" value="10.0.50.1"/>
DNS Server 1:	<input type="text" value="192.168.1.1"/>
DNS Server 2:	<input type="text"/>

Figure 2.11. Configuration Window

H. Close button

Section H displays the close button  on the sub-function's configuration window, which is located on the upper right of the window. When clicking this button, the configuration pop-up window will be closed.

I. Save Changes and Apply Button

Section I displays "Save Changes and Apply" button which is located at the bottom left of the configuration pop-up window. After clicking this button, the configuration will be saved and applied.

A rectangular button with rounded corners, a light blue background, and a thin grey border. The text "Save Changes and Apply" is centered on the button in a bold, black, sans-serif font.

Figure 2.12. Save Changes and Apply Button

3 Main Menu

This is the main welcome screen after the user logged in. The detailed information provided here allows users to easily identify different access points connected to the network.

The information on the web page is separated into five boxes/features: Information, LAN IP, WDS, AP/Client, Industrial Communication and Log as shown in Figure 3.1. Each feature has a gear icon next to its name. By clicking this gear icon for any specific feature, a pop-up window will appear for managing the configuration of that feature.

The following subsections will describe the settings within each feature in detail.



Information ⚙️

System Name:	AW5601-IC
System Description:	AW5601-IC
System Location:	Router's Location
System Contact:	www.atop.com.tw
System OID:	1.3.6.1.4.1.3755.0.3.3
Uptime:	0 days, 2 hours, 13 minutes
Current Date & Time:	2024/06/12 02:22 UTC

LAN IP ⚙️

IP Address:	10.0.50.200
Netmask:	255.255.0.0
Gateway:	10.0.50.1
DNS Server(s):	192.168.1.1

AP/Client ⚙️

Wi-Fi Radio :	Disabled
Operating Mode :	Disabled
SSID:	AW5601
Channel :	

WDS ⚙️

Wi-Fi Radio :	Disabled
Operating Mode :	Disabled
SSID:	AW5601
Channel :	36

Industrial Communication ⚙️

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

Log ⚙️

Time	Text
Wed Jun 12 01:54:17 2024	admin: [LAN] Link Up!
Wed Jun 12 01:54:15 2024	admin: [LAN] Link Down!
Wed Jun 12 01:54:14 2024	admin: [LAN] Link Up!
Wed Jun 12 01:54:12 2024	admin: [LAN] Link Down!
Wed Jun 12 01:53:42 2024	admin: [LAN] Link Up!

Figure 3.1. Main Menu

3.1 Information Feature

This feature displays basic system information of Atop's industrial access point router. Here, users can check the device description including System Name, System Description, System Location, System Contact, and System OID, as shown in Figure 3.. The Uptime and the Current Date & Time of the device are displayed in the last two rows of this feature. Table 3-1 summarizes the description of each basic information.

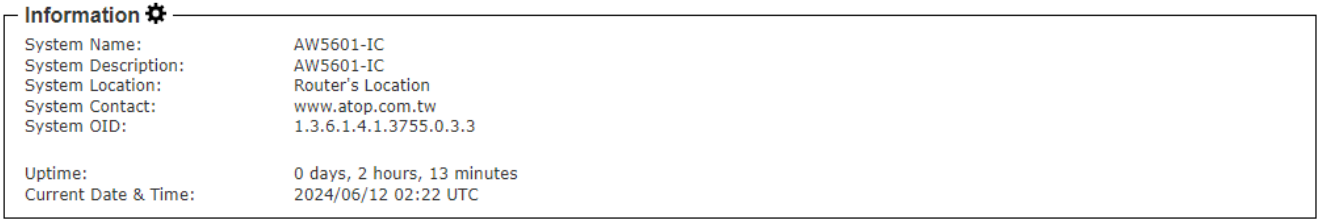


Figure 3.1.1. Information Function

Table 3-1. Descriptions of the Information Features

Label	Description	Factory Default
System Name	This field specifies the particular role or application of different devices. The name entered here will also be displayed in Atop's Device Management Utility. This field has a maximum character limit of 63.	(Model name)
System Description	This field specifies the detailed description of the device. This field has a maximum character limit of 63.	Industrial AP router + (Model name)
System Location	This field indicates location of the switch. It supports up to 63 Characters.	Switch Location
System Contact	This field provides contact information for maintenance. Enter name of whom to contact in case a problem occurs. This field has a maximum character limit of 63.	www.atop.com.tw
System OID	System's SNMP object identification (OID) number	-
Uptime	The duration 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, users can click on the gear icon to bring up a pop-up window called "System Settings" as shown in Figure 3.. In this window, users can configure the System Name, System Description, System Location, and System Contact. After finishing, click the "Save Changes and Apply" button to save and apply the changes to the settings.

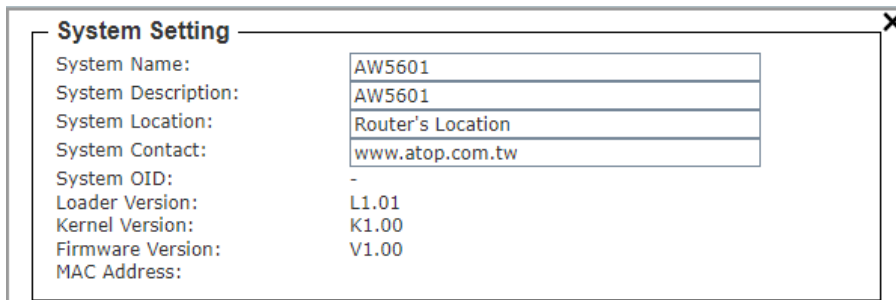


Figure 3.1.2. System Setting Pop-up Window

3.2 AP/Client Feature

In the AP/Client feature, the current Wi-Fi network configuration of the access point is displayed. This includes the status of Wi-Fi Radio, Operating Mode, SSID, Channel as shown in Figure 3.. To edit the AP/Client configuration, users can click on the gear icon to bring up the AP/Client Settings pop-up window as shown in Figure 3..

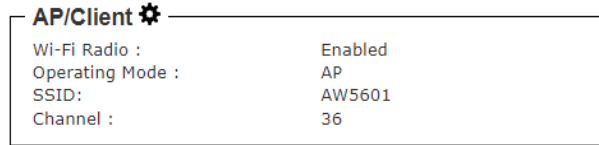


Figure 3.2.1. AP/Client Feature

In the AP/Client Settings pop-up window, users can configure the following twelve submenus: Wi-Fi Radio, Operating Mode, Country, Tx Power, Network Name (SSID), Hide SSID, Wireless Mode, Channel Bandwidth, Control Channel, Authentication Method, Password, 802.11r and Client Isolate. Then, by selecting the corresponding drop-down lists, users can choose to enable or disable the Wi-Fi Radio on the device and choose AP or Client mode as the Operating Mode. After finishing, clicking the **“Save Changes and Apply”** button will save and apply the changes to the settings.

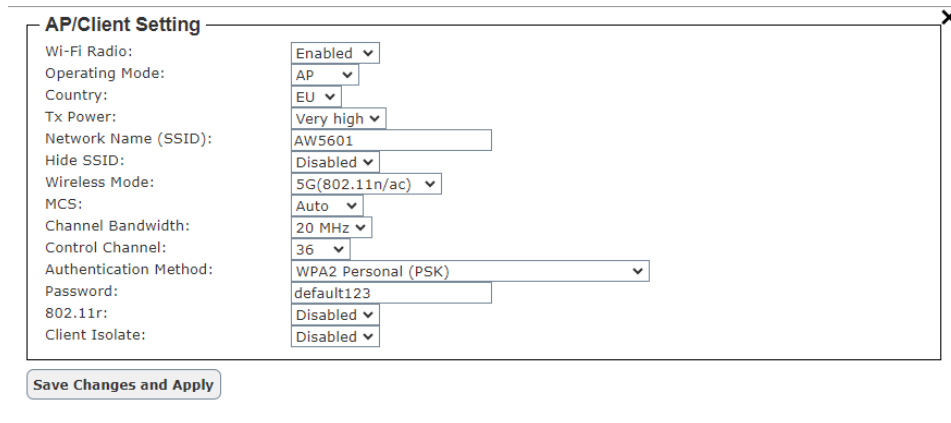


Figure 3.2.2. AP/Client Setting Pop-up Window

3.3 Industrial Communication Feature

The Industrial Communication feature displays the current Wi-Fi settings including the status of Industrial Communication 's Wi-Fi Radio, Operating Mode, Tx Power, Country, Network Name (SSID), Wireless Mode, MCS, Channel Bandwidth, Control Channel, Authentication Method, Client Isolate and RSSITHRESHOLD, as shown in Figure 3.. This Industrial Communication feature allows mobile devices to smoothly switch between different locations within the wireless network without experiencing any interruptions in connectivity.



Figure 3.3.1. Industrial Communication Feature

To edit fields under the Industrial Communication feature, users can click on the gear icon to bring up a pop-up window called "Industrial Communication Setting" as shown in Figure 3.3.2. In this window, users can configure the following thirteen submenus: Wi-Fi Radio, Operating Mode, Country, Tx Power, Network Name (SSID), Wireless Mode, Channel Bandwidth, Control Channel, Authentication Method, Password, Client Isolate, and RSSI Link Threshold. After finishing, clicking the **"Save Changes and Apply"** button will save and apply the settings.

Industrial Communication Setting	
Wi-Fi Radio:	Enabled
Operating Mode:	AP
Country:	EU
Tx Power:	Medium
Network Name (SSID):	flash-roaming
Wireless Mode:	5G(802.11n/ac)
MCS:	Auto
Channel Bandwidth:	20 MHz
Control Channel:	36
Authentication Method:	WPA3 Personal (SAE)
Password:	default123
Client Isolate:	Enabled
RSSI Link Threshold:	-70

Figure 3.3.2. Industrial Communication Setting Pop-up Window

3.4 LAN IP Feature

The LAN IP feature displays the current network configuration including the IP address , Netmask, Gateway and DNS Server(s) as shown in Figure 3.4.1Figure 4.1. To change the network configuration, click the gear icon to open the IP Network Setting pop-up window as shown in Figure 3.. You can then enable or disable DHCP using the drop-down list. When DHCP is enabled, the device will obtain its IP address configuration from another server on the network. If DHCP is disabled, you will need to enter the IPv4 address, subnet mask, gateway IP, and primary and secondary DNS servers. Once you are finished, click the **"Save Changes and Apply"** button to save and apply the settings.

LAN IP	
IP Address:	10.0.50.200
Netmask:	255.255.0.0
Gateway:	10.0.50.1
DNS Server(s):	192.168.1.1

Figure 3.4.1. LAN IP Feature

DHCP Setting

DHCP Client: Disabled

IPv4 Setting

IPv4 Address: 10.0.50.200

Subnet Mask: 255.255.0.0

Gateway IP: 10.0.50.1

DNS Server 1: 192.168.1.1

DNS Server 2:

Save Changes and Apply

Figure 3.4.2. LAN IP Network Setting Pop-up Window

3.5 WDS Feature

In the WDS feature, the current Wi-Fi network configuration of the access point is displayed. This includes the status of Wi-Fi Radio, Operating Mode, SSID, Channel as shown in Figure 3.. To edit the WDS configuration, users can click on the gear icon to bring up the WDS Settings pop-up window as shown in Figure 3..

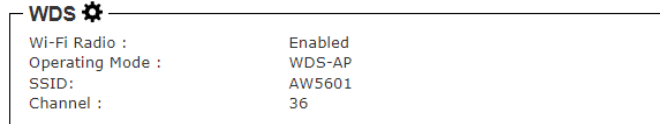


Figure 3.5.1. WDS Feature

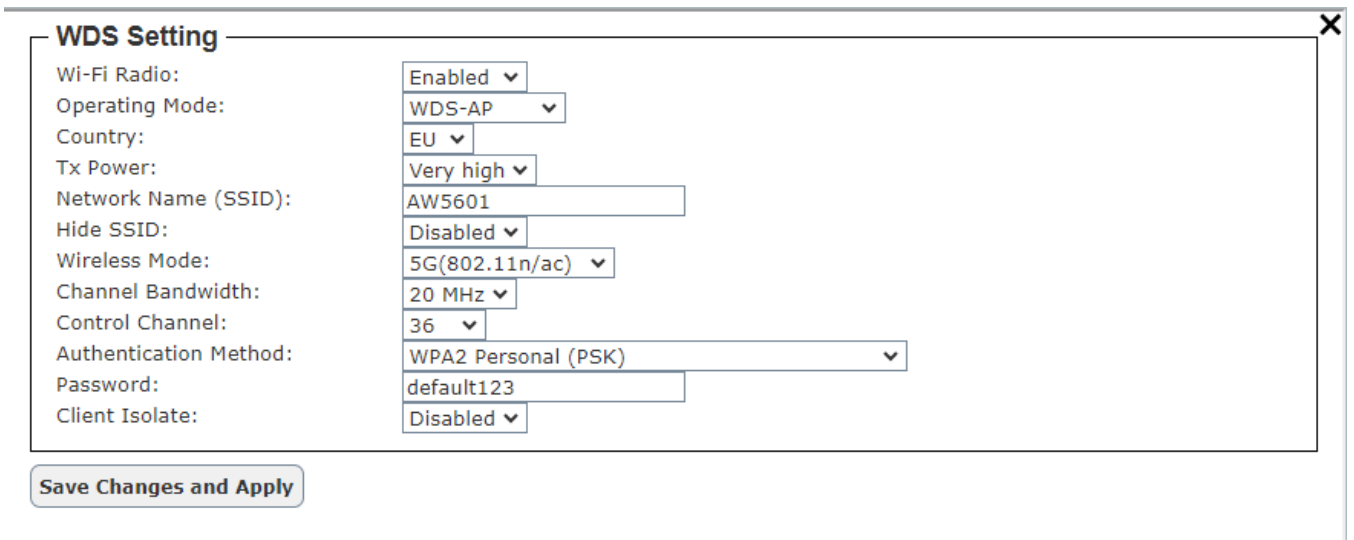


Figure 3.5.2. WDS Setting Pop-up Window

3.6 Log Feature

The Log feature at the bottom of the Information function displays a table of at least five system logs as shown in Figure 3.2. Each log entry includes the fields of Time and Text. Note that the log entries are sorted by date and time. Table 3-Table 3- provides an explanation of each column in the Log table.

Log ⚙️	
Time	Text
Wed Jun 12 04:30:18 2024	admin: [LAN] Link Up!
Wed Jun 12 04:30:16 2024	admin: [LAN] Link Down!
Wed Jun 12 04:30:15 2024	admin: [LAN] Link Up!
Wed Jun 12 04:30:13 2024	admin: [LAN] Link Down!
Wed Jun 12 01:54:17 2024	admin: [LAN] Link Up!

Figure 3.2. Log Feature

Table 3-2. Description of Log Entry

Label	Description
Time	Indicate the time stamp that this event is occurred

Text	Detailed description of this event
-------------	------------------------------------

To configure the System Log Setting, the user can click on the gear icon to bring up the System Log Setting pop-up window as shown in Figure 3.3. This window allows users to enable or disable sending logs to a log server. If the user enables the "Log to Server" option by choosing from the pull-down menu, he/she will then need to specify the Log Server IP Address and Server Service Port in the next two fields. Once finished, clicking the **"Save Changes and Apply"** button will save and apply the settings. Table 3-2 provides an explanation of each column in the System Log setting pop-up entry.

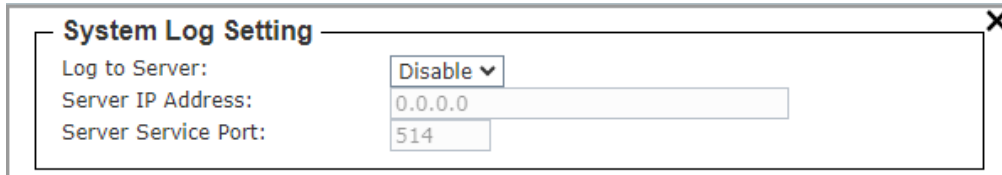


Figure 3.3. System Log Setting Pop-up Window

Table 3-2. 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 an IP address of Syslog server	0.0.0.0
Server Service Port	Set the service port number of System Log server, ranging from Port 1 to 65535.	514

4 Configuration

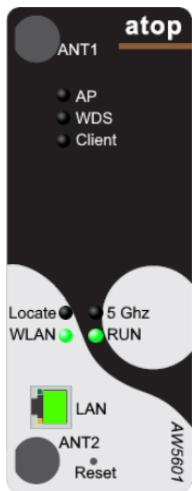
The **Configuration** or **System Settings** function is the second icon from the left. It is the circular icon with a wrench and a screwdriver. This function includes five features: **LAN IP**, **DHCP Server**, **System Time**, **NAT** and **Bridge** as shown in Figure 4.1



Model Name: AW5601-IC
Loader Version: L1.0.0

MAC Address: 00:60:E9:AD:56:07
Kernel Version: K1.1.2

SerialNum : A244205601-0003
Firmware Version: V1.1.2



LAN IP ⚙️

DHCP Client: Disabled
IPv4 Address: 10.0.50.200
Subnet Mask:
Gateway IP:
DNS Server 1:
DNS Server 2:

DHCP Setting [X]

DHCP Client:

IPv4 Setting

IPv4 Address:	<input type="text" value="10.0.50.200"/>
Subnet Mask:	<input type="text" value="255.255.0.0"/>
Gateway IP:	<input type="text" value="10.0.50.1"/>
DNS Server 1:	<input type="text" value="192.168.1.1"/>
DNS Server 2:	<input type="text"/>

Figure 4.1.1. Configuration Function

4.1 LAN IP Feature

The LAN IP feature summarizes the current IP configuration of the industrial AP router. This web page, as shown in Figure 4.1.2, 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 4.1.3. Table 4-1 summarizes each field in the IP Setting pop-up window. After you have finished, clicking on the "Save Changes and Apply" button to save and apply the settings.

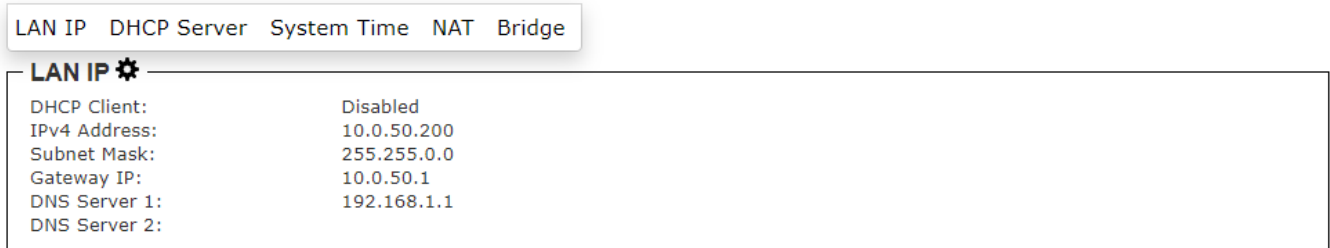


Figure 4.1.2. LAN IP Feature

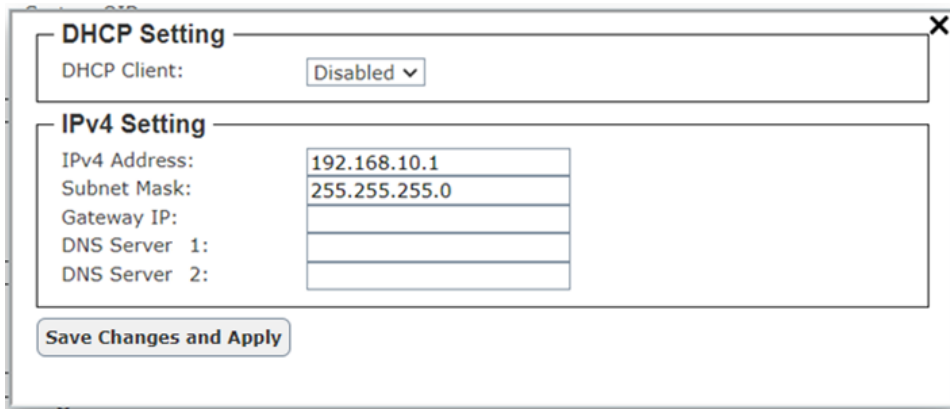


Figure 4.1.3. IP Network Setting Pop-up Window

Table 4-1. Description of IP Network Settings

Label	Description	Factory Default
DHCP Client	Selecting "Enabled" will automatically assign an IP address and related fields. These fields will then be grayed out. Otherwise, users can choose "Disabled" and manually configure the static IP address and related fields.	Disabled
IPv4 Address	Display the current IPv4 address of the device. Users can also set a new static IP address for the device.	10.0.50.200
Subnet Mask	Display the current Subnet Mask. Users can also set a new subnet mask.	255.255.0.0
Gateway IP	The current Gateway IP address is shown. A new one can also be set by the user.	10.0.50.1
DNS Server 1	This displays the current primary DNS IP address used by your network. You can also set a new one.	192.168.1.1
DNS Server 2	There are two ways to configure the secondary DNS IP address for your network: 1) You can view the current address being used, or 2) you can set a new one.	empty

4.2 DHCP Server Feature

DHCP (Dynamic Host Configuration Protocol) Server could assign IP addresses to each client automatically, AW5601 can serve as the DHCP Server to statically or dynamically assign an IP address to any network device. This web page, as shown in Figure 4.2.1.

To enable such functionality, check LAN DHCP Server Enabled to enable the DHCP Server in AW5601. as shown in Figure 4.2.2.

Next proceed to fill in the IP Address Range part which includes the "Start" IP Address and "End" IP Address. Then fill in the Custom DNS servers 1, Custom DNS servers 2.

Next the "Lease Time" is the duration in hours that an assigned IP Address will belong to that device. Once this Lease Time expired, the IP address will be recycled.

A maximum of 8784 hours is set by default.

You could also assign a static IP address to a network device using the Static Connection part.

This means that the network device would always get the same Static IP Address from the DHCP server.

To statically assign an IP address, fill in Host Name, MAC, IP Address and then then click Add button in last of line.as shown in Figure 4.2.3.

After you have finished, clicking on the "Save Changes and Apply" button to save and apply the settings.

LAN IP DHCP Server System Time NAT Bridge

DHCP Server Settings ⚙

LAN DHCP Server Enabled: Disabled
 Start: 10.0.50.100
 End: 10.0.50.109
 Lease Time: 1 (hours)
 Custom DNS servers 1: 8.8.8.8
 Custom DNS servers 2: 8.8.4.4
 Assigned Static IP Addresses:

Figure 4.2.1. DHCP Server Feature

DHCP

LAN DHCP Server Enabled

DHCP range:

Start: 10.0.50. 100

End: 10.0.50. 109

Custom DNS servers 1: 8.8.8.8

Custom DNS servers 2: 8.8.4.4

Lease Time: 1 (hours)

Static IPs

Add Static IP Address:

Host Name	MAC	IP	
(Optional)	Eg. aa:bb:cc:dd:ee:ff	Eg. 10.0.50.xx	Add

Select Hostname/MAC From Currently Connected Hosts ▾

Assigned Static IP Addresses:

Save Changes and Apply

Figure 4.2.2 DHCP Setting Pop-up Window

Static IPs

Add Static IP Address:

Host Name	MAC	IP	
<input type="text" value="(Optional)"/>	<input type="text" value="Eg. aa:bb:cc:dd:ee:ff"/>	<input type="text" value="Eg. 10.0.50.xx"/>	<input type="button" value="Add"/>

Select Hostname/MAC From Currently Connected Hosts ▾

Assigned Static IP Addresses:

Host Name	MAC	IP		
AW5601	00:60:e9:11:22:33	10.0.50.201	<input type="button" value="Edit"/>	<input type="button" value="Remove"/>

Figure 4.2.3 DHCP Static IP setting

4.3 System Time and SNTP Feature

Date and time can be set manually or using Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) to automatically synchronize date and time of AW5601 with a Time Server.

This web page, as shown in Figure 4.3.1.

By clicking on the gear icon next to the System Time and SNTP title, the user could bring up the System Time and SNTP Setting pop-up window as shown in Figure 4.3.2.

Table 4-3 summarizes each field in the System Time and SNTP Setting pop-up window. After you have finished, clicking on the "Save Changes and Apply" button to save and apply the settings.

LAN IP	DHCP Server	System Time	NAT	Bridge
System Time and SNTP ⚙️				
Current Date & Time:	2024/06/17 05:53 BST			
Mode:	Manual			
Time Zone:	UTC+00:00 England			
NTP Server IP:				
SNTP Server IP:				
NTP Server Setting:	Disabled			

Figure 4.3.1. System Time and SNTP Feature

System Time and SNTP

Current Date & Time: 2024/06/17 06:05 BST

Mode:

Date: (YYYY/MM/DD)

Time: (hh:mm:ss)

Time Zone:

NTP Server IP 1:

NTP Server IP 2:

NTP Server IP 3:

SNTP Server IP:

NTP Server Setting:

Save Changes and Apply

Figure 4.3.2. System Time and SNTP Pop-up Window

Table 4-3. Description of System Time Settings

Label	Description	Factory Default
Mode	Mode selection(Manual/NTP Client/ SNTP Client).	Manual
Date	Format (year/month/day).	(YYYY/MM/DD)
Time	Format (hours/minutes/seconds).	(hh:mm:ss)
Time Zone	It is the standard unit of time used in different parts of the planet in order to harmonize global time.	UTC+00:00 England
NTP Server IP1	The IP address or hostname of the first NTP server (the DNS server must be configured correctly for the hostname entered).	empty
NTP Server IP2	The IP address or hostname of the second NTP server (the hostname entered must be properly configured for the DNS server).	empty
NTP Server IP3	IP address or hostname of the third NTP server (the hostname entered must be properly configured as a DNS server).	empty
SNTP Server IP	IP address of the SNTP server.	empty
NTP Server Setting	NTP server setting enable or disable.	Disable

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.

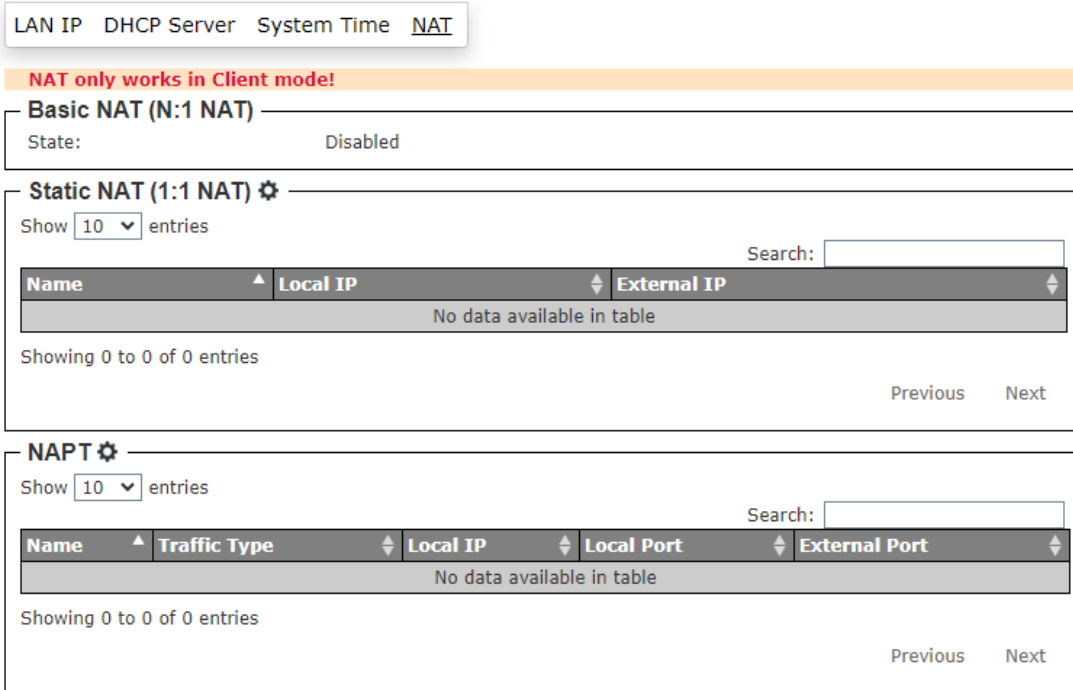


Figure 4.4.1. NAT Feature

Basic NAT (N:1 NAT)

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.

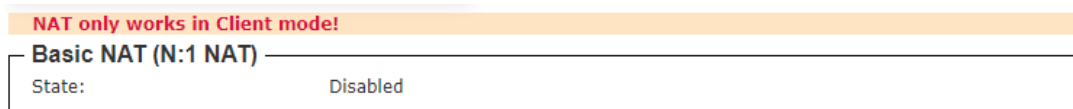


Figure 4.4.1.1. Basic NAT (N:1 NAT) Feature

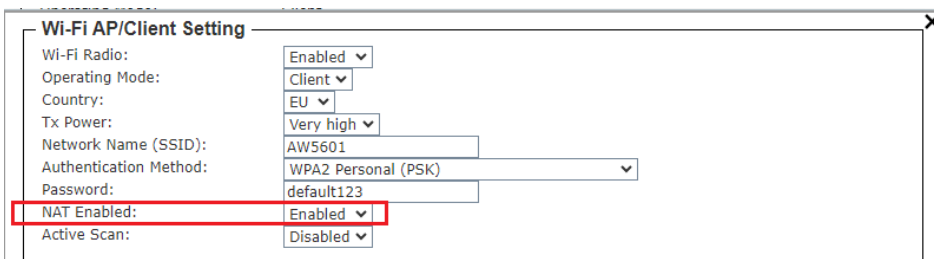


Figure 4.4.1.2. Wi-Fi Client Enable Basic NAT Mode

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 .



Figure 4.4.2.1. Static NAT (1:1 NAT) Feature

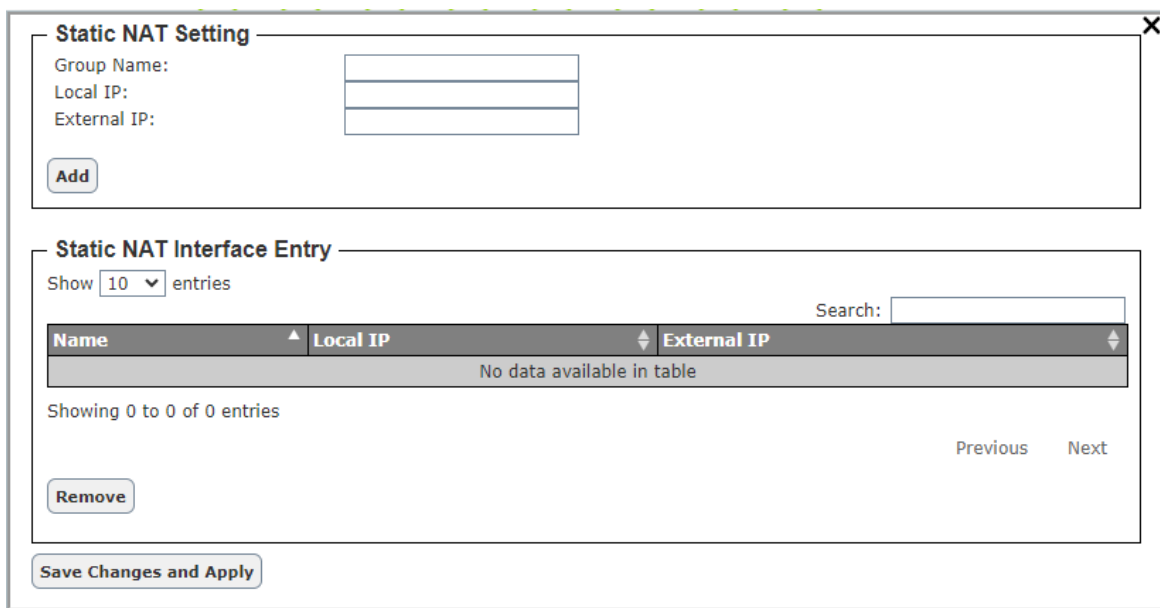


Figure 4.4.2.2. Static NAT Setting Pop-up Window

NAPT (Network Address Port Translation)

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 4.4.3.2.

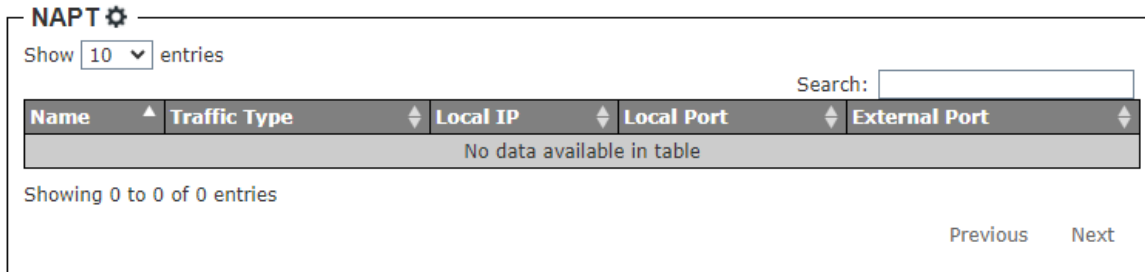


Figure 4.4.3.1 NAPT Feature

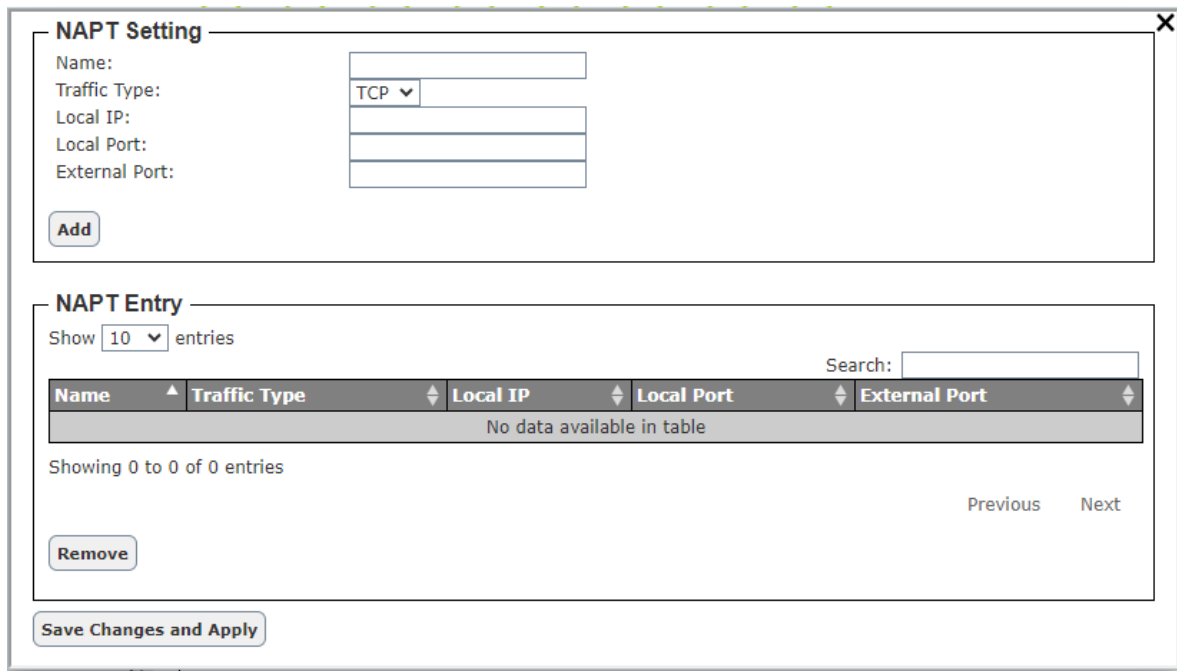
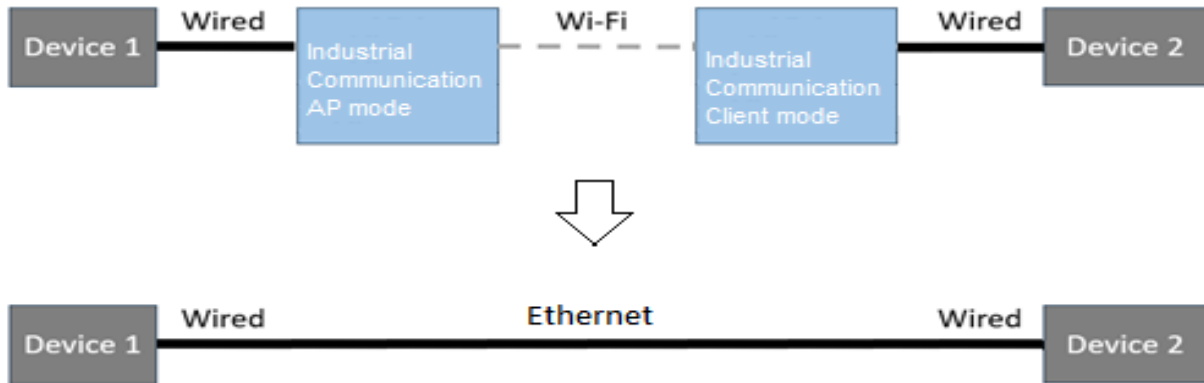


Figure 4.4.3.2 NAPT Setting Pop-up Window

4.5 Bridge Feature

Forward LLDP packets from Ethernet to Wireless and from Wireless to Ethernet. This web page, as shown in Figure 4.5.1.

If LLDP is disabled and LLDP Forwarding is enabled, LLDP packets can be forwarded between the Ethernet and Wireless interfaces. In the former scenario, it will be just like end device A is neighbor to end device B if we have applied these settings of LLDP. (As shown in the picture below)



To enable such functionality, select Enabled selection to enable the LLDP forwarding in AW5601. as shown in Figure 4.5.2.

After you have finished, clicking on the "Save Changes and Apply" button to save and apply the settings.



Figure 4.5.1. Bridge Feature



Figure 4.5.2 Bridge Setting Pop-up Window

5 Wi-Fi

The **Wi-Fi** function is the third icon from the left. It is the circular icon with a wrench and a screwdriver. This function includes five features: **AP/Client**, **WDS** and **Industrial Communication** shown in Figure 4.1 Figure 4.1.

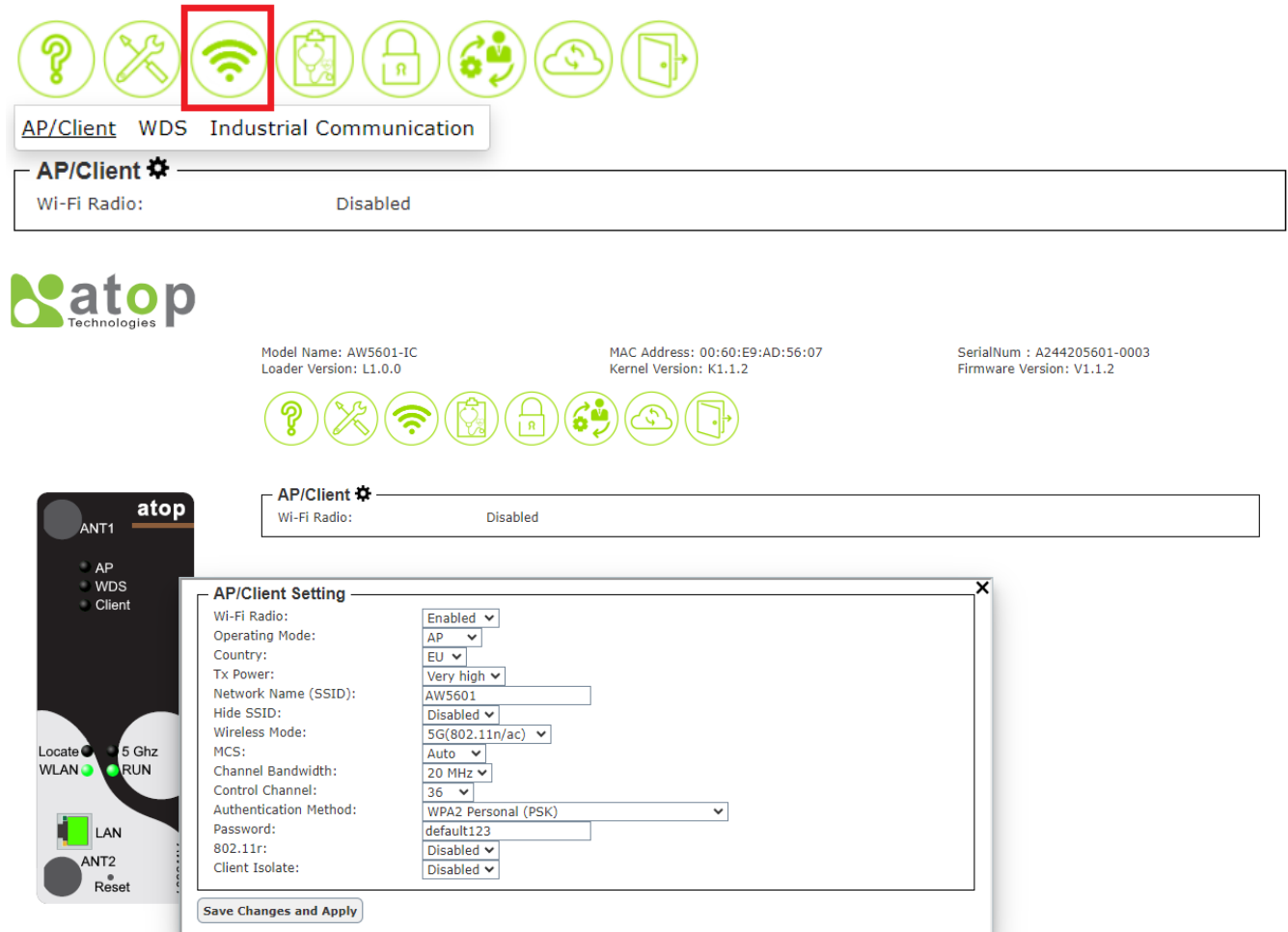


Figure 5.1. Configuration Function

Packet forwarding behaviors are summarized in Table 5-1 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 it supports the delivery of L3 packets.

Table 5-1. 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
Industrial Communication AP/Client	NAT	Yes(*1)	No	Yes
Industrial Communication 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 **Industrial Communication 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 **Industrial Communication** mode.

5.1 AP/Client Mode Feature

AP / Client Mode

An Access Point's (AP) primary mode is Access Point mode. In this mode, the AP acts as a central hub which connects wireless clients (devices with wireless adapter cards) such as laptops, desktops, and PDAs to a wired network. Wireless clients can only communicate with the AP in Access Point mode.

Client mode allows an Access Point to become a wireless client itself. Then it can connect to another AP. Essentially, the AP acts like a wireless adapter card in this mode. You would use Client mode to extend the reach of your wireless network by connecting an AP to a distant main AP.

Note that not all Access Points support Client mode. Even if supported, it might only work with devices from the same manufacturer or series. In Client mode, wireless clients cannot communicate directly with the Access Point.

A typical network topology for AP/Client mode is shown in Figure . In this setup, AP1 is configured in Access Point mode (Figure 5.), while AP2 operates in Client mode (Figure 5.).



Figure 5.1.1. AP Mode/Client Mode Topology

Wi-Fi Setting ✕

Wi-Fi Radio:	Enabled ▾
Operating Mode:	AP ▾
Country:	TW ▾
Tx Power:	Low ▾
Network Name (SSID):	AW5601
Hide SSID:	Disabled ▾
Wireless Mode:	5G ▾
Channel Bandwidth:	80 MHz ▾
Control Channel:	149 ▾
Authentication Method:	WPA2 Personal (PSK) ▾
Password:	12345678
Client Isolate:	Disabled ▾

Figure 5.1.2. AP Mode for AP1 Setting

Wi-Fi Setting

Wi-Fi Radio:

Operating Mode:

Country:

Tx Power:

Network Name (SSID):

Authentication Method:

Password:

NAT Enabled:

Active Scan:

WLAN IP Setting(WAN)

DHCP Client:

IPv4 Address:

Subnet Mask:

Gateway IP:

LAN IP Setting

IPv4 Address:

Subnet Mask:

Figure 5.1.3. Client Mode for AP2 Setting

Table 5-2. AP/Client Mode Setting

	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 5-3. IP Address Settings for Devices in AP/Client Mode

	Device1	Device2
IP Address	10.0.50.1	10.0.100.2

5.2 WDS Mode Feature

WDS-AP / Client / Hybrid Mode (Non-NAT)

Wireless distribution system (WDS) expands a wireless network through multiple access points. The wireless base station acts as the internet gateway. It 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 it connects to the Internet through the wireless base station.

WDS-AP: When enabled in WDS-AP mode, the access point becomes the root node of the entire wireless network. It can establish connections with access points 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. Thus, it establishes 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). This allows it to connect to another Access Point while it also can accept 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 an example of topology for WDS-AP/WDS-Hybrid/WDS-Client mode as shown in Figure 5.. We set AP1 as WDS-AP mode as shown in Figure 5., set AP2 as WDS-Hybrid mode as shown in Figure 5., and set AP3 as WDS-Client mode as shown in Figure 5.. All AP Settings are summarized in Table 5-4.

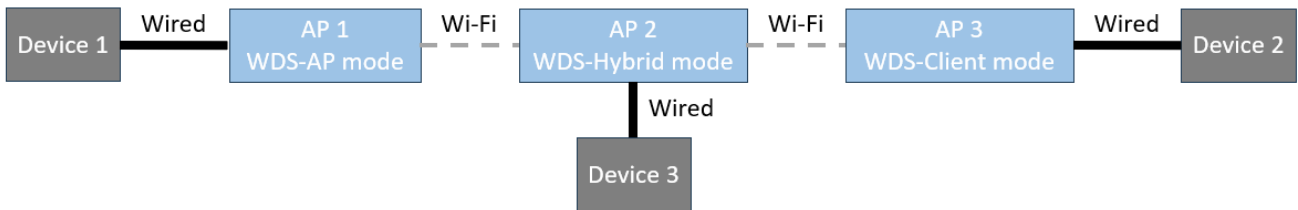


Figure 5.2.1.1. WDS-AP/Client/Hybrid Mode Topology

Wi-Fi Setting X

Wi-Fi Radio:	Enabled ▾
Operating Mode:	WDS-AP ▾
Country:	TW ▾
Tx Power:	Low ▾
Network Name (SSID):	AW5601
Hide SSID:	Disabled ▾
Wireless Mode:	5G ▾
Channel Bandwidth:	80 MHz ▾
Control Channel:	149 ▾
Authentication Method:	WPA2 Personal (PSK) ▾
Password:	12345678
Client Isolate:	Disabled ▾

Figure 5.2.1.2. WDS-AP Mode for AP1 Setting

Wi-Fi Setting ✕

Wi-Fi Radio: Enabled ▾

Operating Mode: WDS-Hybrid ▾

Country: TW ▾

Tx Power: Low ▾

WDS-Hybrid-Client Setting(Connect to WDS-AP):

Network Name (SSID): AW5601

Authentication Method: WPA2 Personal (PSK) ▾

Password: 12345678

WDS-Hybrid-AP Setting:

Network Name (SSID): AW5601

Hide SSID: Disabled ▾

Wireless Mode: 5G ▾

Channel Bandwidth: 80 MHz ▾

Control Channel: 149 ▾ (Must same as WDS-AP)

Authentication Method: WPA2 Personal (PSK) ▾

Password: 12345678

Client Isolate: Disabled ▾

Figure 5.2.1.3. WDS-Hybrid Mode for AP2 Setting

Wi-Fi Setting ✕

Wi-Fi Radio: Enabled ▾

Operating Mode: WDS-Client ▾

Country: TW ▾

Tx Power: Low ▾

Network Name (SSID): AW5601

Authentication Method: WPA2 Personal (PSK) ▾

Password: 12345678

Active Scan: Disabled ▾

Figure 5.2.1.4. WDS-Client Mode for AP3 setting

Table 5-4. 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

5.3 Industrial Communication

Industrial Communication mode, 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 "Industrial Communication mode" which means it automatically switches to the most suitable access point to maintain optimal signal strength and network performance.

This Industrial Communication mode feature allows devices such as Automated Guided Vehicles (AGVs) 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, and factories.

For bridging, this mode requires the use of devices of the same model that inherently support L2, VLAN tags, Profinet packets, etc. Additionally, it provides extra support for Profinet transparent under NAT.

Industrial Communication AP/ Industrial Communication Client mode is similar to WDS-AP/WDS-Client mode, but it incorporates roaming behaviour.

Industrial Communication AP / Industrial Communication Client Mode

There is an example of topology for Industrial Communication AP and Industrial Communication Client modes illustrated in Figure 5.. In this topology, we configure AP1 in Industrial Communication AP mode (as shown in Figure 5..1.) and AP2 in Industrial Communication Client mode (as shown in Figure 5.1.2.).



Figure 5.3.1. Industrial Communication AP / Industrial Communication Client Topology

Table 5-5. Industrial Communication AP / Industrial Communication 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 5-6. Devices IP Address Setting

	Device1	Device2
LAN IP Setting	10.0.50.1	10.0.50.22

Industrial Communication Setting

Wi-Fi Radio:

Operating Mode:

Country:

Tx Power:

Network Name (SSID):

Wireless Mode:

MCS:

Channel Bandwidth:

Control Channel:

Authentication Method:

Password:

Client Isolate:

RSSI Link Threshold:

Figure 5.3.1.1. Industrial Communication AP Mode for AP1 setting

Table 5-7. Descriptions of the Industrial Communication AP Mode

Label	Description	Default Value
Wi-Fi Radio	This option can turn on or turn off the wireless signal of AW5601.	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	This field displays the transmission’s power. To prevent wireless interference with other networks, the transmit power of the AW5601 can be reduced. While higher power increases transmission distance, it also negatively impacts jitter and latency.	Medium
Network Name (SSID)	This field displays the WLAN network name, 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	The Modulation Coding Scheme (MCS) index is a metric based on several parameters of a Wi-Fi connection between two stations. Two options are available: Auto and Stable. Auto enables full-range automatic adjustment of the MCS index, while Stable locks it in a 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 <ul style="list-style-type: none"> ● 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. 	5G(802.11n/ac)
Authentication Method	Modes of authentication for WLANs include Open System and 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	When this option is enabled, it 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	Minimum connectable signal strength is measured in RSSI (Received Signal Strength Indicator)	-70

Industrial Communication Setting

Wi-Fi Radio:

Operating Mode:

Country:

Tx Power:

Network Name (SSID):

Wireless Mode:

MCS:

Channel Bandwidth:

Control Channel:

Authentication Method:

Password:

RSSI Link Threshold:

Roaming Sensitivity:

Hold Time: ms

NAT and WLAN/LAN IP Setting

NAT Enabled:

Figure 5.3.1.2. Industrial Communication Client Mode for AP2 Setting

Table 5-8. Descriptions of the Industrial Communication Client Mode

Label	Description	Default Value
Wi-Fi Radio	This option can turn on or turn off the wireless signal of AW5601.	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	This field displays the transmission’s power. To prevent wireless interference with other networks, the transmit power of the AW5601 can be reduced. While higher power increases transmission distance, it also negatively impacts jitter and latency.	Medium
Network Name (SSID)	This field displays the WLAN network name, 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	The Modulation Coding Scheme (MCS) index is a metric based on several parameters of a Wi-Fi connection between two stations. Two options are available: Auto and Stable. Auto enables full-range automatic adjustment of the MCS index, while Stable locks it in a stable range	Auto
Channel Bandwidth	20 MHz or 40 MHz or 80 MHz	20 MHz

Label	Description	Default Value
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 <ul style="list-style-type: none"> ● 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	Modes of authentication for WLANs include Open System and 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	Minimum connectable signal strength is measured in RSSI (Received Signal Strength Indicator)	-70
Roaming Sensitivity	Enable this option to allow Industrial Communication Client mode to scan for available access points in the background to speed up roaming when necessary. Choose from the following roaming aggressiveness levels: Very High, High, Medium, Low, or Very Low.	High
Hold Time	The minimum stay time specifies the duration a device will remain connected to the AW5601 after initially associating with it. When multiple AW5601s with similar signal strengths are present, setting this value appropriately can help avoid frequent switching between devices. The valid range for this setting is 0 to 2000 milliseconds (ms).	250 ms

PROFINET Transparent over Industrial Communication mode and NAT

To connect AP1 and AP2 by Industrial Communication mode under NAT enabled conditions, you need to enable PROFINET transparent mode to allow PROFINET packets to transmit between device1 and device2. Users should set AP1 to Industrial Communication AP mode (as shown in Figure 5.Figure 5.) and set AP2 to Industrial Communication Client mode with NAT and PROFINET Transparent enabled (as shown in Figure 5.).

Table 5-9. Industrial Communication AP / Industrial Communication 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 5-10. Industrial Communication AP / Client Mode's Device IP Address Setting

	Device1	Device2
LAN IP Setting	10.0.50.1	10.0.50.22

Industrial Communication Setting

Wi-Fi Radio:	Enabled ▾
Operating Mode:	AP ▾
Country:	EU ▾
Tx Power:	Medium ▾
Network Name (SSID):	flash-roaming
Wireless Mode:	5G(802.11n/ac) ▾
MCS:	Auto ▾
Channel Bandwidth:	20 MHz ▾
Control Channel:	36 ▾
Authentication Method:	WPA3 Personal (SAE) ▾
Password:	default123
Client Isolate:	Enabled ▾
RSSI Link Threshold:	-70 ▾

Figure 5.3.2.1. Industrial Communication AP Mode Setting

Industrial Communication Setting

Wi-Fi Radio:	Enabled ▾
Operating Mode:	Client ▾
Country:	EU ▾
Tx Power:	Medium ▾
Network Name (SSID):	flash-roaming
Wireless Mode:	5G(802.11n/ac) ▾
MCS:	Auto ▾
Channel Bandwidth:	20 MHz ▾
Control Channel:	36 ▾
Authentication Method:	WPA3 Personal (SAE) ▾
Password:	default123
RSSI Link Threshold:	-70 ▾
Roaming Sensitivity:	High ▾
Hold Time:	250 ▾ ms

NAT and WLAN/LAN IP Setting

NAT Enabled:	Enabled ▾
PROFINET Transparent:	Enabled ▾
WLAN DHCP Client:	Disabled ▾
WLAN IPV4 Address:	
WLAN Subnet Mask:	
WLAN Gateway IP:	
LAN IPV4 Address:	10.0.50.200
LAN Subnet Mask:	255.255.0.0

Figure 5.3.2.2. Industrial Communication Client Mode Setting

6 Diagnostic

The Diagnostic function allows users to check the operation of the access point. It provides several features to assist the users with System Log, SMTP Event, Log Event, Ping, and Locate. The Diagnostic function is represented by the fourth circular icon with a stethoscope on top of a medical chart. Figure 6.1 illustrates the list of features available under the Diagnostic function.



Figure 6.1. Diagnostic Function on the Menu Bar

6.1 System Log

The System Log feature under the Diagnostic function contains two sections: **System Log Setting** and **System Log** as shown in Figure 6.1.1. The upper section labelled System Log Setting summarizes the current configuration of the system log. To configure the log, users can click the gear icon next to the title to bring up the System Log Setting pop-up window as shown in Figure 6.. Note that this pop-up window provides the same functionality as described in the Log feature under the Information function as summarized in Table 3-2.

In the lower section of the web page, there is a table that displays system logs. Each log entry includes the description of Date, Time, Up Time, and Event. The entries are sorted by date and time. Table 3-Table 3- in Section 3.5 explains each column in the System Log table. Users can choose how many entries to display per page (20, 50, or 100) from the "Show ... entries" drop-down list. Additionally, users can find relevant entries through the Search box located at the top left of the table. Users can filter entries based on Date, Time, Uptime, and Event by clicking under each column header. Finally, clicking the Refresh button retrieves the latest entries from the access point.

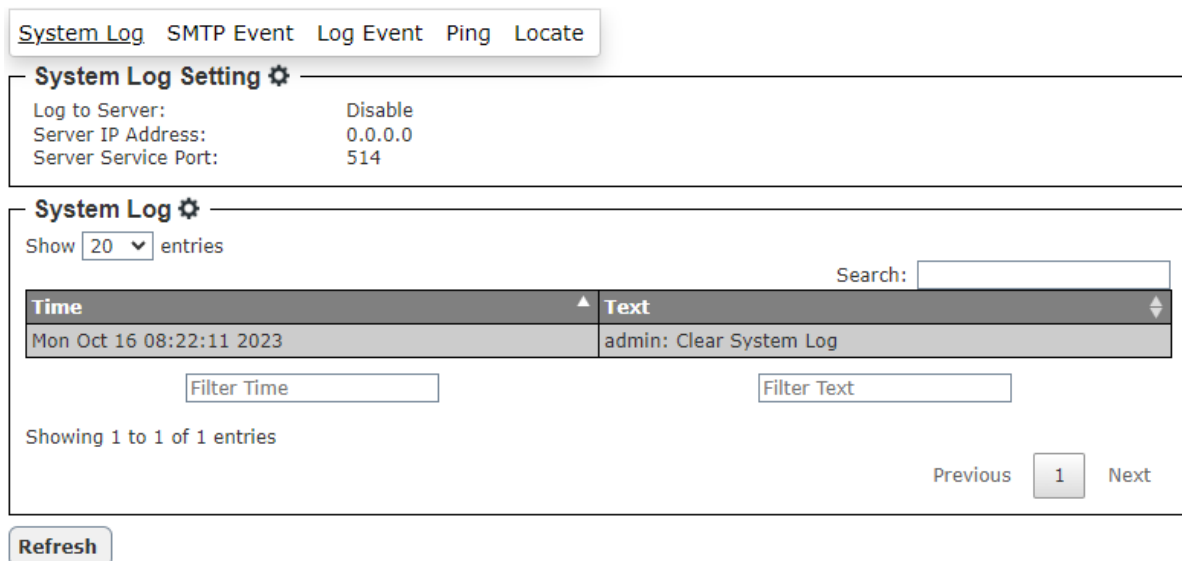


Figure 6.1.1. System Log Feature

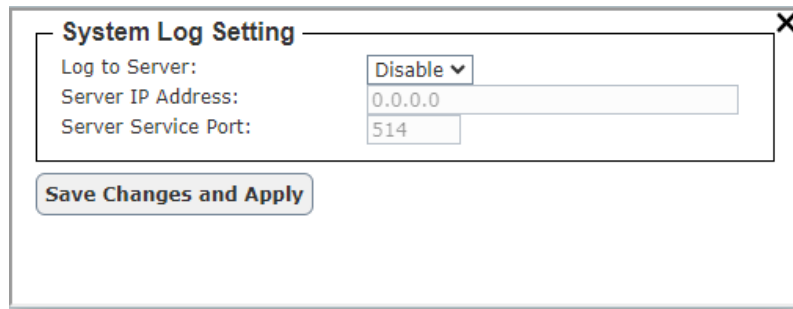


Figure 6.1.2. System Log Setting Pop-up Window

To clear the system log, the user can click the gear icon next to the "System Log" title. This will bring up the "System Log Clear" pop-up window as shown in Figure 6.1.2. System Log Clear Pop-up Window. Clicking the "Clear System Log" button in this window will erase all log entries.

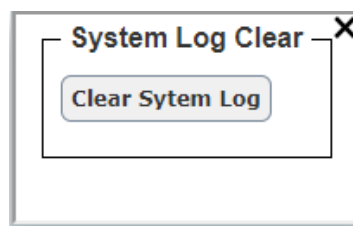


Figure 6.1.2. System Log Clear Pop-up Window

6.2 SMTP Event

The SMTP event feature under the Diagnostic function contains an SMTP settings submenu. This feature allows users to configure email alerts for various events related to the access point as shown in Figure 6. The following list explains each option of the SMTP settings and their default values:

- **Mode:** This is set to "Disabled" by default, indicating email alerts are currently off. Users can enable them by selecting "Enabled".
- **SMTP Server Address:** This field shows the address of the outgoing mail server used to send alerts. The value would depend on your email provider (e.g., smtp.atop.com for Atop). The default value is 0.0.0.0.
- **Sender Email Address:** This specifies the email address that will appear as the sender of the alerts. The value is administrator by default.
- **Mail Subject:** This allows you to customize the subject line of the email alerts. The default might be generic (e.g., "Automated Email Alert") or blank.
- **SSL/TLS:** This setting determines whether a secure connection is used for sending emails. The default could be "Disabled" or "Enabled" depending on the security configuration of your email server.
- **Authentication:** This specifies if authentication is required to access the SMTP server. Defaults could be "None," "Plain Text," or another option depending on email provider's requirements.
- **Username:** If authentication is enabled, this field would be used to enter the username for user's email account. It would likely be blank by default.
- **Password:** Similar to username, this field would require user's email account password if authentication is enabled. It would also be blank by default for security reasons.
- **Recipient Email Address:** This specifies the email address(es) where the alerts will be sent. The default might be blank. This field is used for entering the desired recipient(s)'s email address.

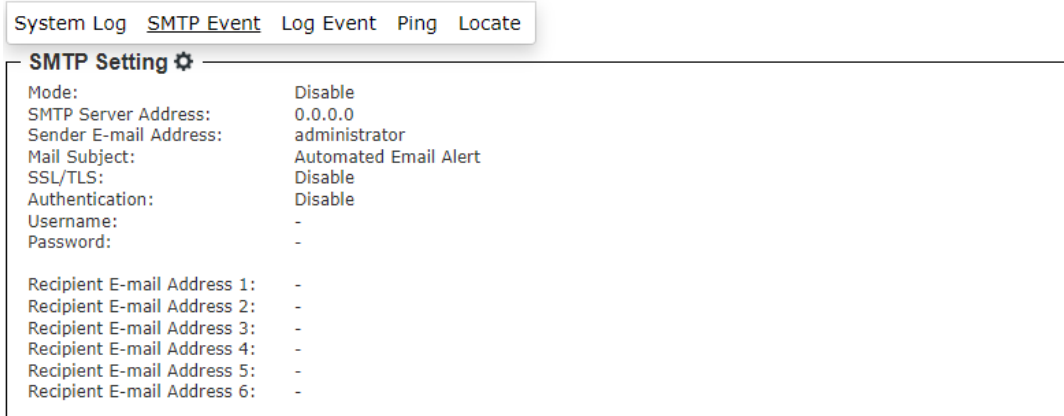


Figure 6.2.1. SMTP Event Feature

Once you have finished entering information, click **“Save Changes and Apply”** to save your settings.

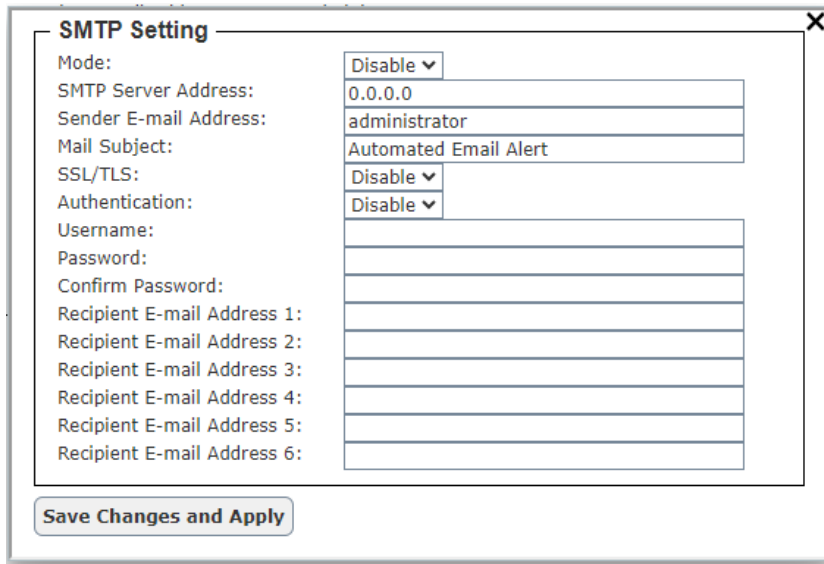


Figure 6.2.2. SMTP Event Setting Pop-up Window

6.3 LLDP

LLDP: Link Layer Discovery Protocol is a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities, and neighbors on a local area network based on IEEE 802 technology, principally wired Ethernet.

The LLDP default setting of AW5601 is enabled on Ethernet.

The LLDP feature as shown in Figure 6.1.1.

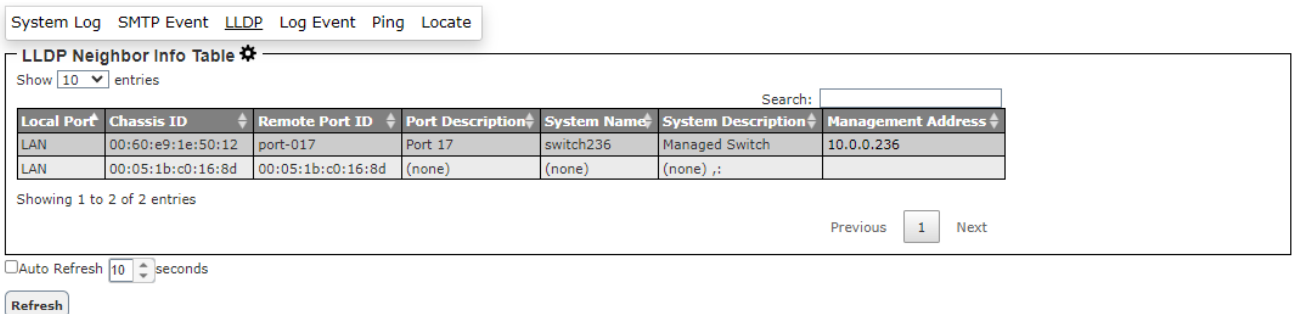


Figure 6.3.1. LLDP Neighbor Feature

In the LLDP setting of AW5601, supported interfaces as LAN, WLAN, LAN & WLAN, and LLDP disable. Once you have finished, click **“Save Changes and Apply”** to save your settings.

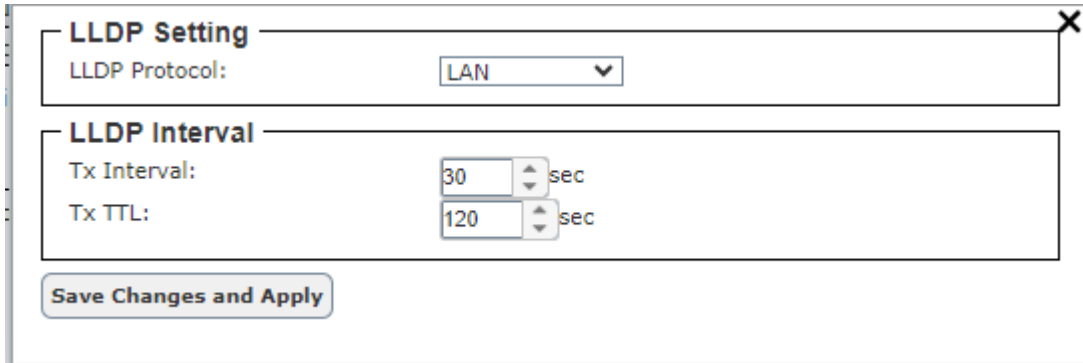


Figure 6.3.2. LLDP Setting Pop-up Window

6.4 Log Event

The Log event feature under the Diagnostic function allows users to view log events that have occurred on the AW5601 access point as shown in Figure 6.. These events are displayed in a table format. The table displays various system events and the corresponding logging options for Syslog and SMTP. By default, all logging events are disabled. This means that these events are not recorded in the system log or sent via SMTP notification.

Users can customize the logging behavior for each event by enabling or disabling the corresponding checkboxes under the Syslog and SMTP columns. To set these behaviors, users can click on the gear icon next to the Log Event title. This will bring up the Log Event pop-up window as shown in Figure 6.. A checked box indicates that the event will be logged or included in the SMTP notification.

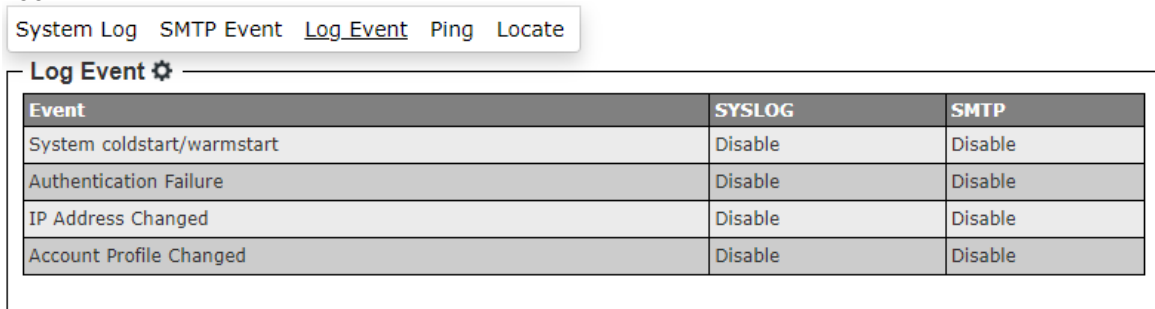


Figure 6.4.1. Log Event Feature

Once you have finished, click **“Save Changes and Apply”** to save your settings.

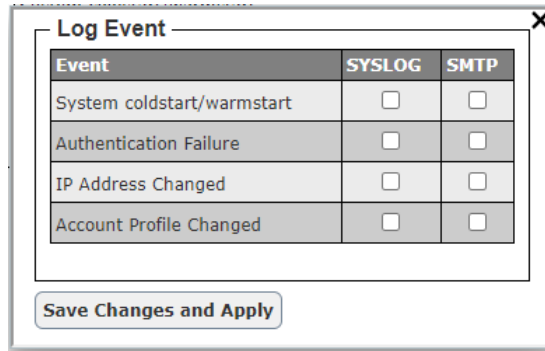


Figure 6.4.2. Log Event Pop-up Window

6.5 Ping

The AW5601 web interface provides an interface to call Ping utility which is a network diagnostic utility used to test network reachability. Users can use the Ping function to check if the AW5601 can reach the gateway or other devices on the network. To use Ping, user must enter a destination IP address in the text box and click the "Ping" button as shown in Figure 6.5.1. This process typically takes around 20 seconds.

The two figures below represent different scenarios:

- A successful ping: No packet loss is shown from AW5601 to the address 10.0.50.200 and back.
- An unreachable device: No packets return from the transmitted ping packets sent to the address 10.0.50.2.

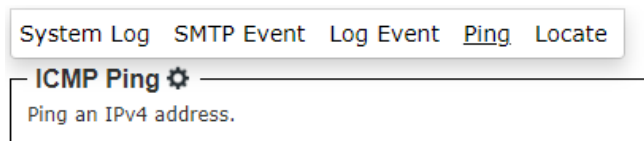


Figure 6.5.1. Ping Feature

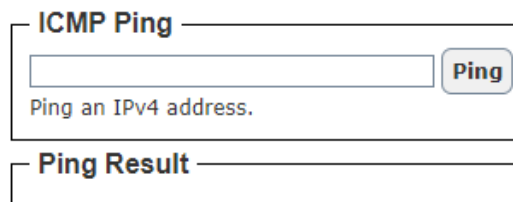


Figure 6.5.2. Ping Pop-up Window

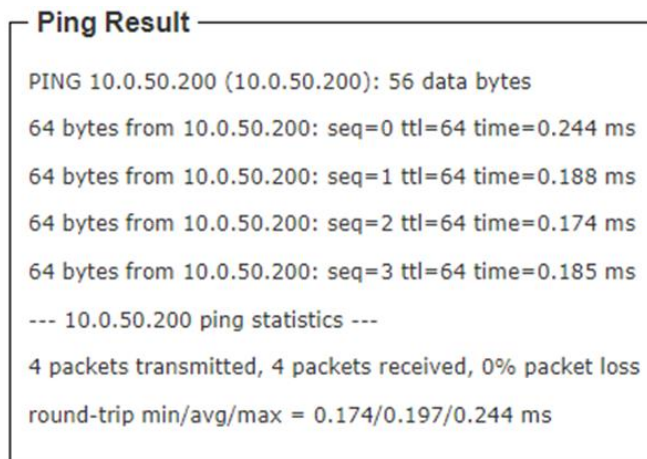


Figure 6.3. Ping Successful with No Packet Loss

```
Ping Result  
PING 10.0.50.2 (10.0.50.2): 56 data bytes  
--- 10.0.50.2 ping statistics ---  
4 packets transmitted, 0 packets received, 100% packet loss
```

Figure 6.5.4. Ping Unsuccessful with 100% Packet Loss

6.6 Locate

The Locate function can provide quick positioning for devices in the group. When the **Turn On** button on the WEB is pressed, the "Locate" light in the front panel on the left side of the WEB UI will turn from black to red as shown in Figure 6.. Simultaneously, the "Locate" light on the actual device will also illuminate red. Pressing the **Turn Off** button will turn the "Locate" light on the front panel on the left side of the WEB UI from red back to black as shown in Figure 6.6.2. The red light on the device's Locate function will also turn off.

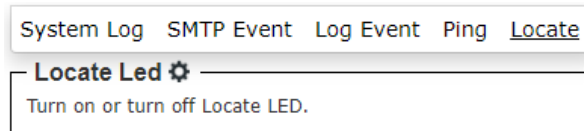


Figure 6.6.1. Locate Feature

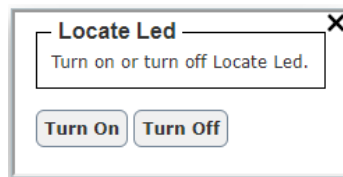


Figure 6.6.2. Locate Pop-up Window



Figure 6.6.3. Locate Turn-on State on Panel



Figure 6.6.4. Locate Turn-off State on Panel

7 Security



Figure 7.1. 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 include MAC address (wired / wireless) and IP address. This packet filtering functionality enhances security by preventing unauthorized or malicious packets from entering your network. Packets will be filtered (or classified) as "allowed packets" or "denied packets".

"Allow packets" mode, also known as "whitelisting," permits specified traffic. Conversely, "deny packets" mode, or "blacklisting," blocks specified traffic. Extreme caution is advised in this section as data that does not meet any of

these criteria will be discarded. Incorrect configuration could prevent access to the AW5601. If the latter occurs, you will need to reset the device back to factory defaults by following any of the methods described in Section 9.4 (Factory Default settings).

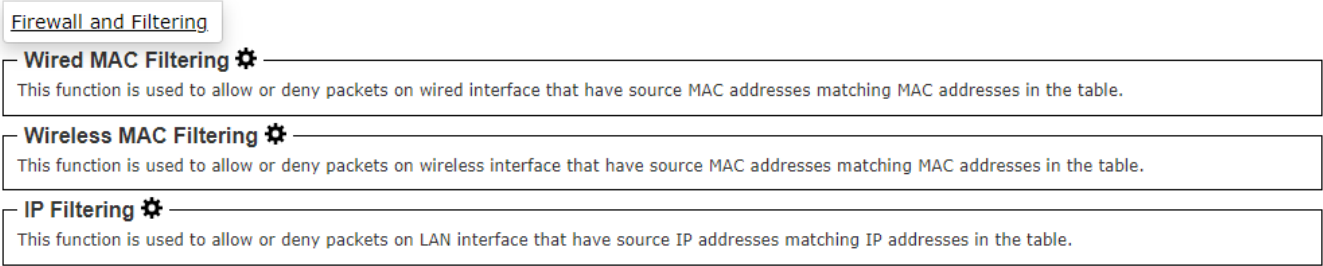


Figure 7.1.1. Security Feature

7.1 Firewall - MAC (Wired / Wireless) Filtering

The MAC Filtering feature under the Security function allows you to control which devices can access your wireless network by specifying a list of allowed or denied MAC addresses as shown in Figure 7.2. A MAC address is a unique identifier assigned to each network device. By default, MAC filtering is disabled. This means that any device with a compatible wireless adapter can connect to your network.

To create a MAC filtering rule, user can follow these steps:

- Click the radio button next to either Allow packets with MAC addresses listed below or Deny packets with MAC addresses listed below, depending on whether you want to restrict access to specific devices or allow all devices except for those listed.
- In the MAC Address field, enter the MAC address of the device that you want to allow or deny access to. You can add multiple MAC addresses by separating them with commas.

Click the Save Changes and Apply button to save your changes.

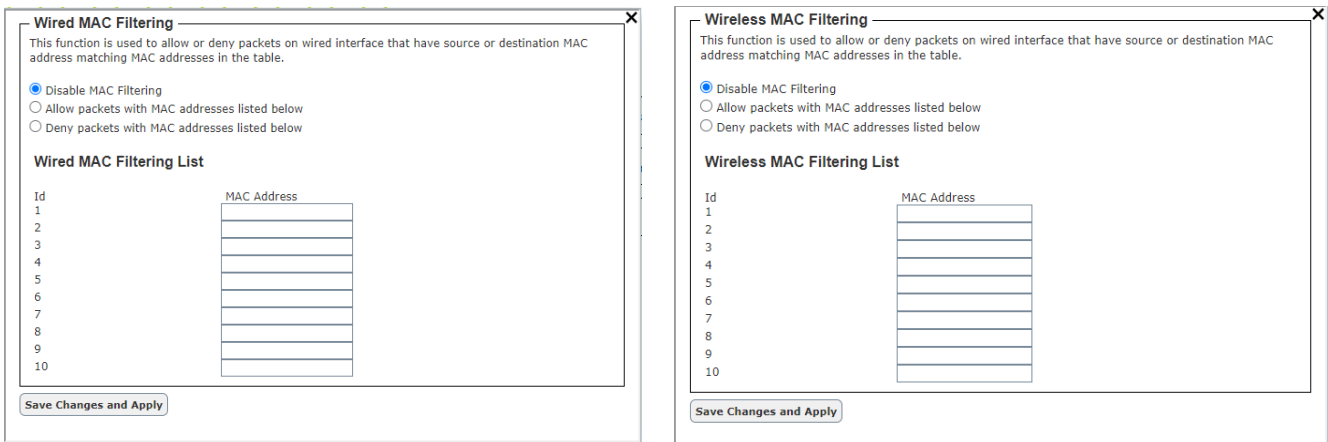


Figure 7.1. 2.Firewall – MAC (wired / wireless) Filtering Pop-up Window

7.2 Firewall – IP Filtering

The Firewall – IP Filtering feature under the Security function allows you to control incoming and outgoing traffic on your network by specifying rules that allow or deny packets based on their source and destination IP addresses as shown in Figure 7.. By default, IP filtering is disabled. This means that all traffic is allowed on your network.

To create an IP filtering rule, user can follow these steps:

- Click the radio button next to either Allow packets with IP addresses listed below or Deny packets with IP addresses listed below, depending on whether you want to allow or deny traffic from specific IP addresses.
- In the Src IP Addr field, enter the source IP address or subnet that you want to allow or deny traffic from. You can use an asterisk (*) as a wildcard to match any IP address.
- In the Dst IP Addr field, enter the destination IP address or subnet that you want to allow or deny traffic to. You can use an asterisk (*) as a wildcard to match any IP address.

Click the Save Changes and Apply button to save your changes.

IP Filtering

This function is used to allow or deny packets on LAN interface that have source or destination IP address matching IP addresses in the table.

Disable IP Filtering
 Allow packets with IP addresses listed below
 Deny packets with IP addresses listed below

IP Filtering List

Id	Src IP Addr	Dst IP Addr
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Save Changes and Apply

Figure 7.2.1. Firewall – IP Filtering Pop-up Window

8 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 8.1. These features allow the user to manage the accounts, enable secure HTTP for web interface, and set up the SNMP protocol.



Figure 8.1. Management Function on the Menu Bar

8.1 Account Feature

The Account feature is shown in Figure 8.1.. It displays a list of accounts or users on the industrial AP router. This information is presented in a table format with two columns: Username and Permission. To add or delete an account or user, you can click the gear icon. This will bring up the Account Setting pop-up window as shown in Figure 8.. To add a user, you must enter the Username, Password, and Confirm Password. Then, select the Permission Level for the user and click the Add User button. To remove a user from the list, you can select the user and click the Delete User button.

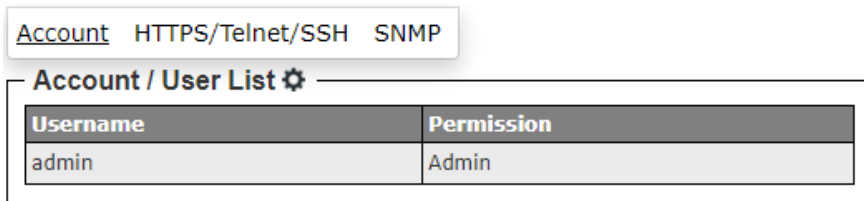


Figure 8.1.1. Account Feature

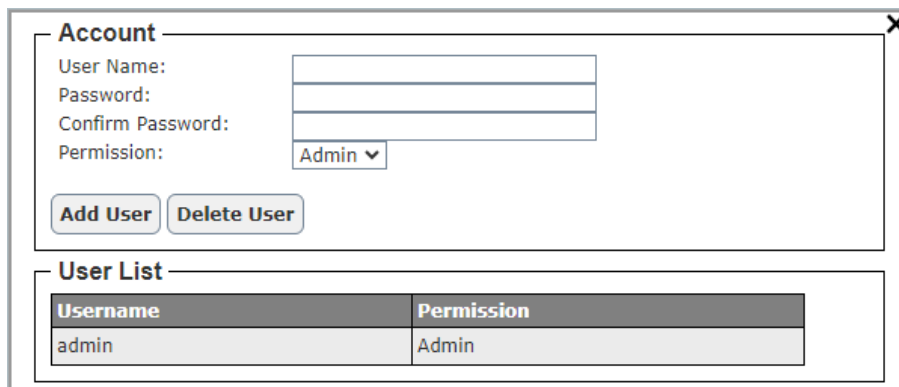


Figure 8.1.2. Account Pop-up Window

8.2 HTTPS/Telnet/SSH Feature

The HTTPS (Hyper Text Transfer Protocol Secure) feature is another option under the Management function. This web page presents the current setting of HTTPS for the industrial AP router’s web interface as shown in Figure 8.. To enable HTTPS, the user can click on the gear icon to bring up the HTTPS Setting pop-up window as shown in Figure 8.. Next, check the Enabled box to redirect web interface access to HTTPS. After you have finished, click on the **Save Changes and Apply** button to save and apply the settings.



Figure 8.2.1. HTTPS/Telnet/SSH Feature

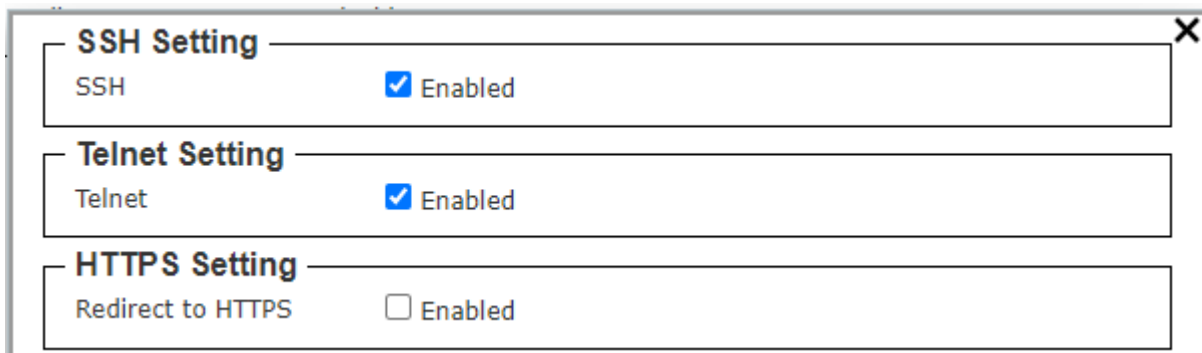


Figure 8.2.2. HTTPS/Telnet/SSH Feature Pop-up Window

8.3 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 set by users. The SNMP is used by network management systems or third-party software to monitor devices on a network such as industrial AP routers. SNMP retrieves network status information and can also be used to configure network parameters. Atop's wireless access points support SNMP and can be configured through this feature under the Management function.

Figure 8. 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 on the industrial AP router can be viewed under the SNMP Mode Setting. The SNMP Agent Version can be set to either SNMP v1/v2c or SNMP v3. Note that depending on the selected SNMP Agent Version, some sections will be active while others will be greyed out. For example, when SNMP Agent Version is set to SNMP v1/v2c, only the SNMP v1/v2c Agent Setting and SNMP v1/v2c Trap Setting sections will be available for configuration as shown in Figure 8..

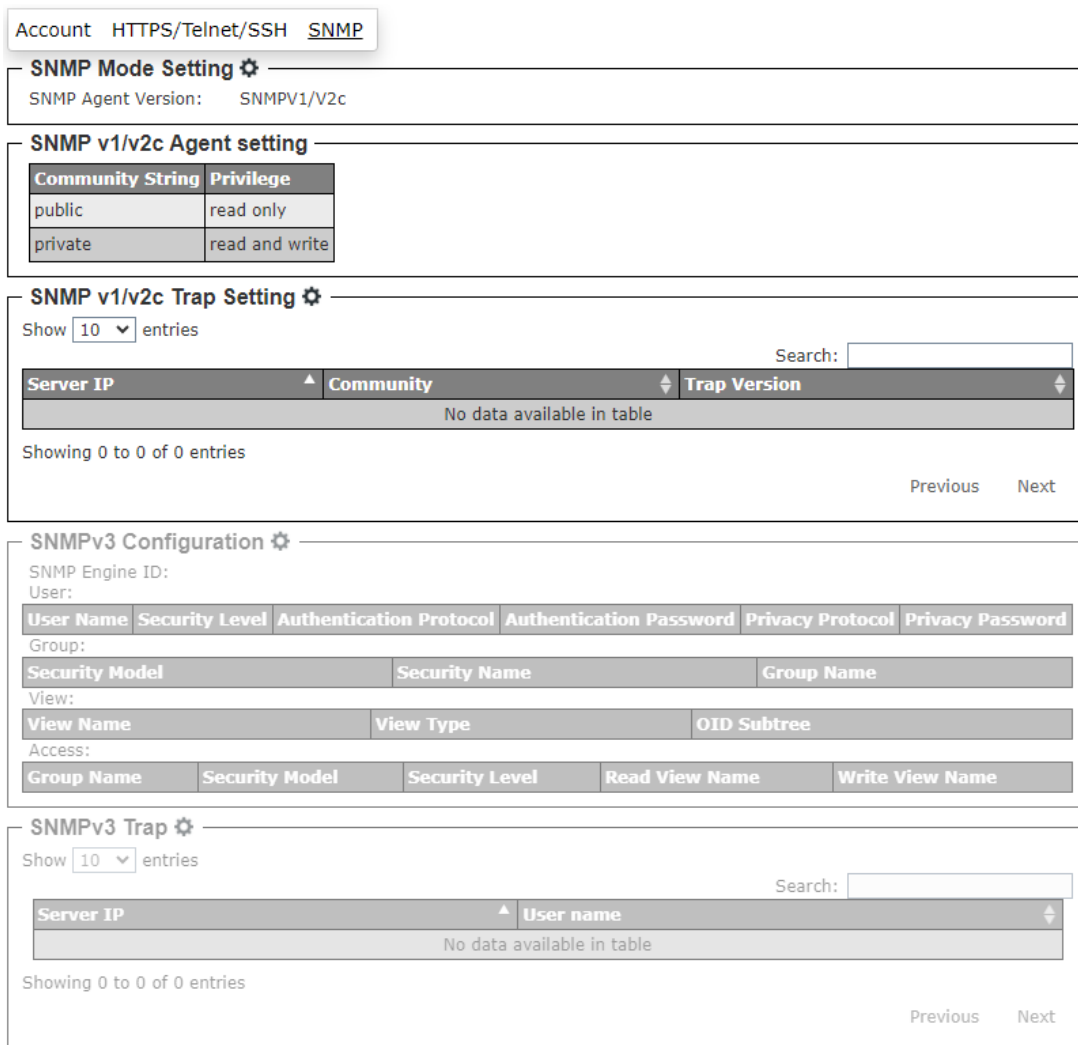


Figure 8.3.1. SNMP Feature

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 8. When SNMP v1 or v2c is selected, the community string and privilege of each community string can be managed as shown in the figure. After you have finished, click the **Save Changes and Apply** button to save and apply the settings.

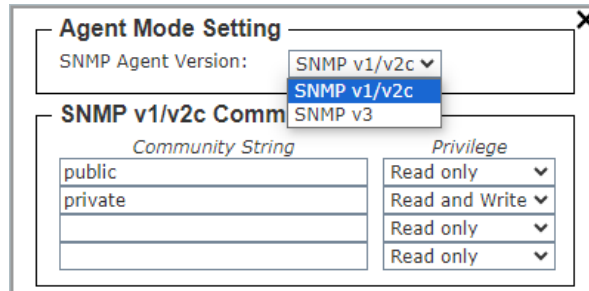


Figure 8.3.2. SNMP Agent Mode and SNMP v1/v2c Community Management

Although the SNMP Agent Version is set to SNMPv1/v2c, the SNMP v1/v2c Trap Setting section remains active. Users can configure the Trap Server by clicking the gear icon next to the SNMP v1/v2c Trap Setting. A pop-up window appears as shown in Figure 8., which allows users to manage the trap server. This includes adding the Trap Server IP address, Community string, and selecting the Trap Version. After filling in and selecting all fields, users can click the "Add" button to create an entry in the SNMP v1/v2c Community table displayed at the bottom of the pop-up window. Users can also delete an entry from the SNMP v1/v2c Community table by selecting it and then clicking the "Remove" button.

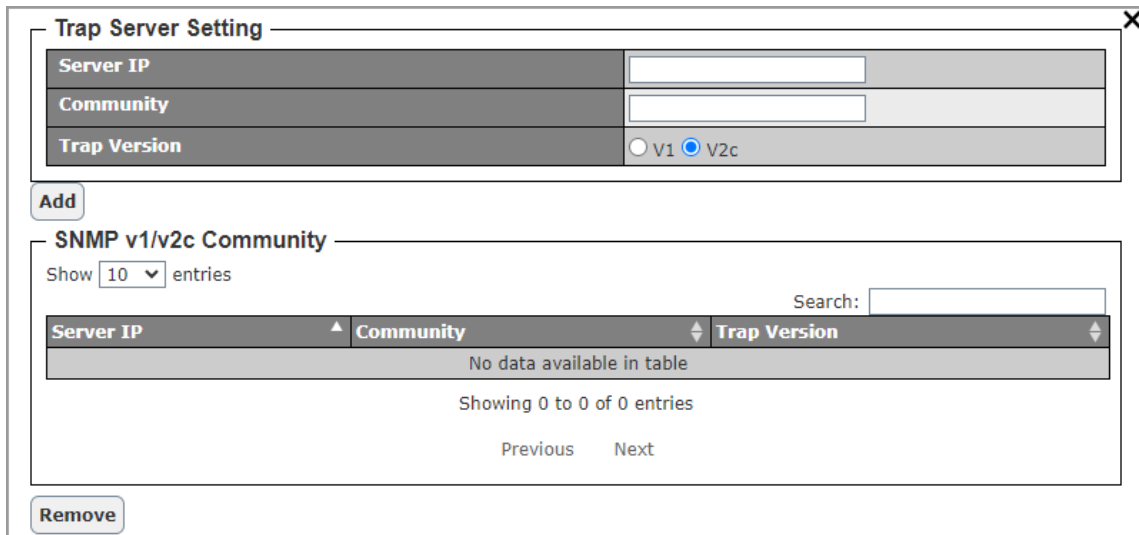


Figure 8.3.3. SNMP v1/v2c Trap Management

If the SNMP agent version is set to SNMPv3, the SNMPv3 Configuration and SNMPv3 Trap sections will become active as shown in Figure 8. This web page provides detailed setup for SNMPv3 Configuration and SNMPv3 Trap Server.

SNMPv3 Configuration ⚙

SNMP Engine ID: 800007e5017f000001

User:

User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Group:					
Security Model	Security Name	Group Name			

View:

View Name	View Type	OID Subtree
all	included	.1

Access:

Group Name	Security Model	Security Level	Read View Name	Write View Name

SNMPv3 Trap ⚙

Show entries

Search:

Server IP	User name
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

Figure 8.3.4. 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 8.. This window is divided into four sections: SNMPv3 User Configuration, SNMPv3 Group Configuration, SNMPv3 View Configuration, and SNMPv3 Access Configuration. Under the SNMP v3 User Configuration, the user can add a new SNMP user by entering a new User Name and setting the Security Level, Authentication Protocol, Authentication Password, Privacy Protocol, and Privacy Password. Once all the information is entered, click the **Add** button to add the new SNMP user. Note that existing users can be deleted by clicking the **Delete** button in front of the specific User Name. SNMP v3 Group, View, and Access can also be configured in the same manner as described for SNMP v3 User Configuration. After finishing, click the **"Save Changes and Apply"** button to save and apply the settings.

SNMPv3 User Configuration

SNMP Engine ID: 800007e5017f000001

Delete	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="button" value="delete"/>	<input type="text"/>	Auth, Priv	MDS	<input type="text"/>	DES	<input type="text"/>

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
<input type="button" value="delete"/>	v1	public	<input type="text"/>

SNMPv3 View Configuration

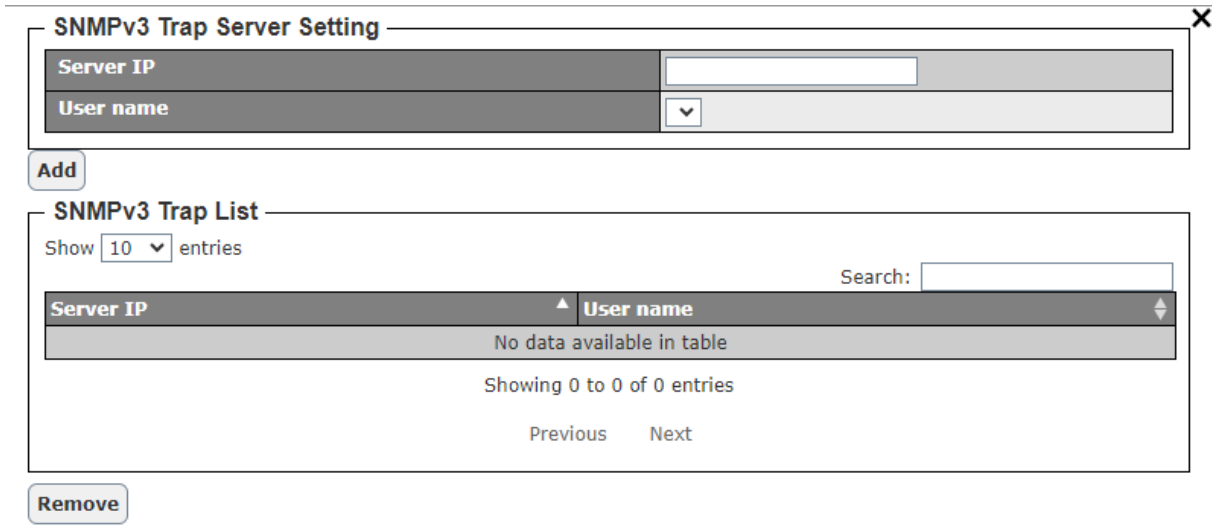
Delete	View Name	View Type	OID Subtree
<input type="button" value="delete"/>	all	included	.1
<input type="button" value="delete"/>	<input type="text"/>	included	<input type="text"/>

SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="button" value="delete"/>	<input type="text"/>	v1	NoAuth, NoPriv	None	None

Figure 8.3.5. SNMP v3 Configuration Pop-up Window

To configure an SNMP v3 Trap Server, the user can click the gear icon next to the "SNMP v3 Trap" in Figure 8.. This action will open another pop-up window as shown in Figure 8.Figure 8.. In this window, you can set the IP address for the SNMP v3 Trap Server and choose a username previously configured in SNMP v3 User Configuration. Clicking the "Add" button adds the new entry to the SNMP v3 Trap List displayed below. To delete an entry from the SNMP v3 Trap List, select the desired entry and click the "Remove" button.



The image shows a pop-up window titled "SNMPv3 Trap Server Setting" with a close button (X) in the top right corner. The window is divided into two main sections. The top section, "SNMPv3 Trap Server Setting", contains two input fields: "Server IP" with a text box and "User name" with a dropdown menu. Below these fields is an "Add" button. The bottom section, "SNMPv3 Trap List", features a "Show 10 entries" dropdown, a "Search:" text box, and a table. The table has two columns: "Server IP" and "User name". The table is currently empty, displaying the message "No data available in table" and "Showing 0 to 0 of 0 entries". Below the table are "Previous" and "Next" navigation buttons. At the bottom left of the window is a "Remove" button.

Figure 8.3.6. SNMP v3 Trap Server Setting Pop-up Window

9 Maintenance Feature

The Maintenance function of the web-based management interface allows you to perform various tasks to keep your access point running smoothly. These tasks as shown in Figure 9.1 include:

- **Firmware Updates:** This menu is used to update the firmware on your access point. Firmware updates can contain new features, bug fixes, and security patches.
- **TFTP:** This menu allows you to configure Trivial File Transfer Protocol (TFTP) settings for your access point. TFTP is a simple file transfer protocol that can be used to transfer firmware updates and other files to and from your access point.
- **Backup/Restore:** This menu allows you to back up and restore the configuration of your access point. This can be useful if you need to reset your access point to factory defaults or if you want to migrate your configuration to a new access point.
- **Factory Default:** This menu allows you to reset your access point to its factory default settings. This will erase all your configuration settings and return the access point to its original state.
- **Reboot:** This menu allows you to reboot your access point. Rebooting can sometimes help to resolve minor issues with the access point.

The following sections of this manual will provide detailed instructions on how to use each of these features.



Figure 9.1. Maintenance Function on the Menu Bar

9.1 Firmware Feature

The firmware feature in Figure 9. under the Maintenance function shows information about the AP’s firmware. The user can check the **Current Loader Version, Kernel Version and Firmware Version** under the Upgrade Firmware menu. To upgrade the firmware, the user can click on the gear icon next to the Upgrade Firmware title. The Upgrade Firmware pop-up window will show up as shown in Figure 9.1. The user can choose a firmware file and click **Upgrade Now** button to start the process. When the upgrade progress is completed, the device will reboot by itself.

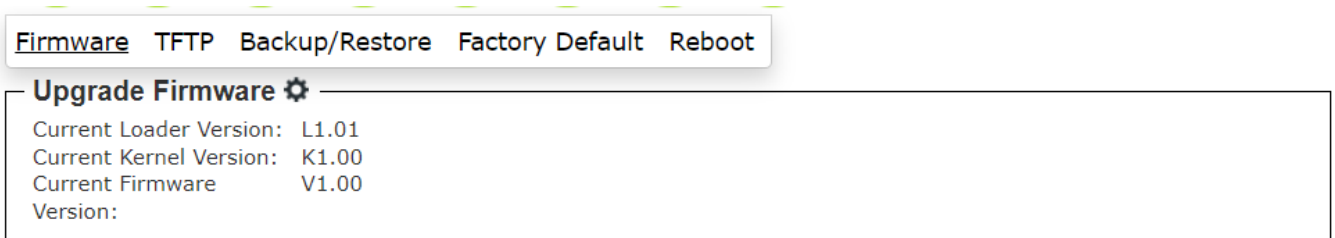


Figure 9.1.1. Firmware Feature

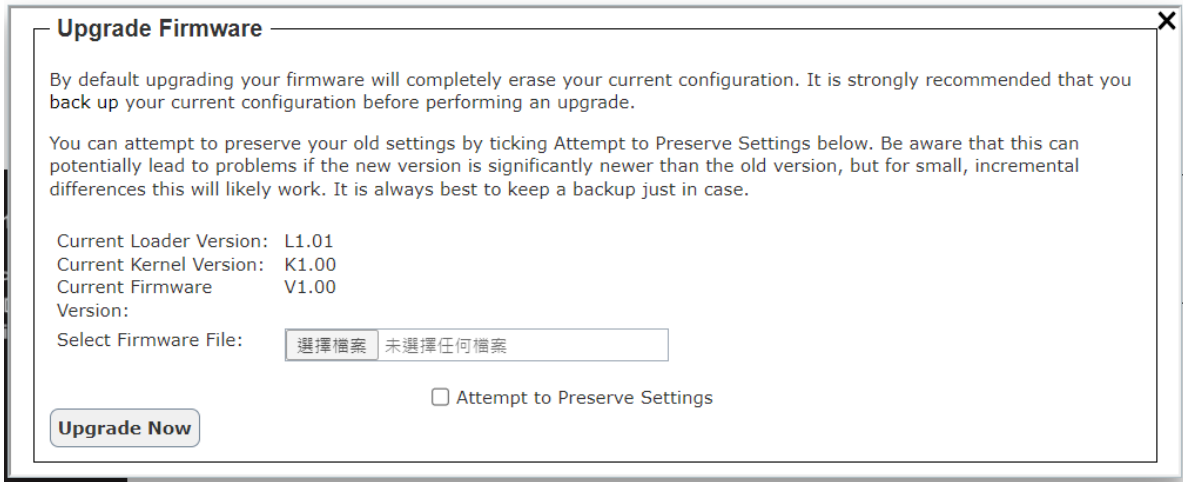


Figure 9.1.2. Upgrade Firmware Pop-up Window

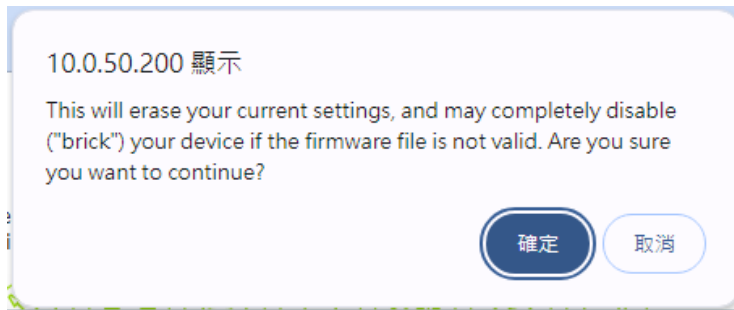


Figure 9.1.3. Upgrade Firmware Pop-up Alert Window

9.2 TFTP Feature

The TFTP feature under the Maintenance function allows users to upgrade the firmware through a TFTP server. After clicking on the gear icon next to the Upgrade Firmware title as shown in Figure 9., a pop-up window will be presented as shown in Figure 9.. Users can set the following options: **TFTP server IP**, **TFTP port**, **TFTP firmware file**, and **attempt to preserve settings** before proceeding with this method of firmware update. After finishing, clicking the "Upgrade Now" button initiates the firmware upgrade using the TFTP protocol.

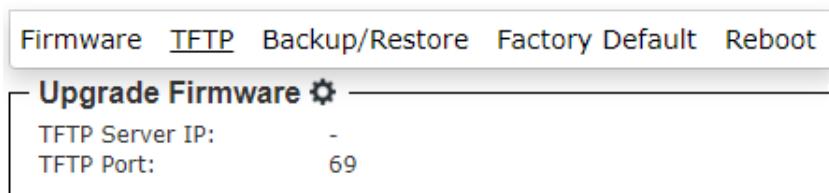


Figure 9.2.1. TFTP Feature

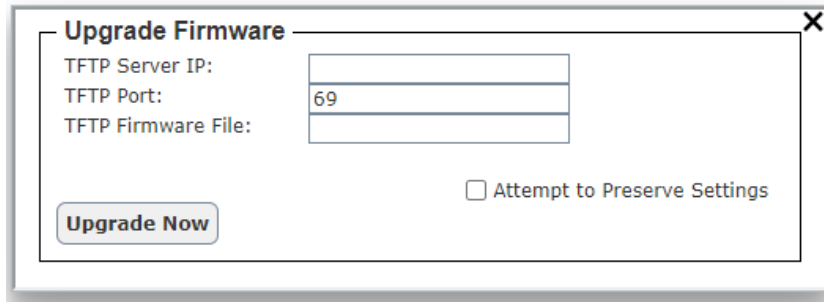


Figure 9.2.2. TFTP Pop-up Window

9.3 Backup / Restore Feature

The Backup/Restore feature within the Maintenance function offers another maintenance option for users. It allows them to back up or restore configuration files directly to or from their local host computer which is located within the same network as AW5601 device. To start backing up current configuration of the device, the user can click on the gear icon next to the Backup title, this will bring up the Backup pop-up window as shown in Figure 9.. The user can click the Get Backup Now button to start downloading the backup configuration file from the device to the user’s local host computer. To restore a configuration file from the user’s local host computer, the user can click on the gear icon next to the Restore title. This will bring up the Restore pup-up window as shown in Figure 9.. The user must specified the configuration file on your local host computer first and can enable or disable the options for Keep username & password and Keep IP. To start the restoration process, the user can click the Restore Configuration Now button.

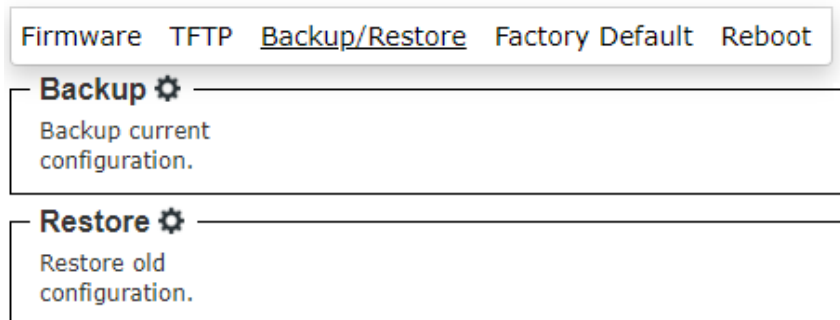


Figure 9.3.1. Backup/Restore Feature

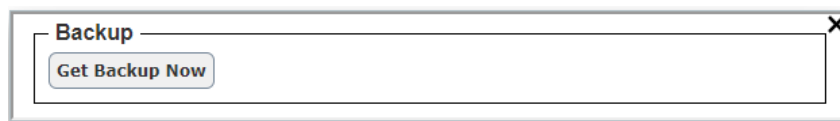


Figure 9.3.2. Backup Pop-up Window



Figure 9.3.3. Restore Pop-up Window

9.4 Factory Default Settings

The Factory Default feature under the Maintenance function allows the user to reset the device to its original or factory default configuration. The Factory Default web page is shown in Figure 9.. To perform a factory reset, the user can click on the gear icon next to "Factory Default" to bring up the pop-up window, as shown in

Figure 9.

Figure 9.. Then, clicking on the "Restore Default Configuration Now" button to restore the device to its factory default settings.

Firmware TFTP Backup/Restore Factory Default Reboot

Factory Default

Reset device to factory default configuration. After button clicked, the system MUST be restarted and the default configuration will be applied in next start.

Figure 9.4.1. Factory Default Feature

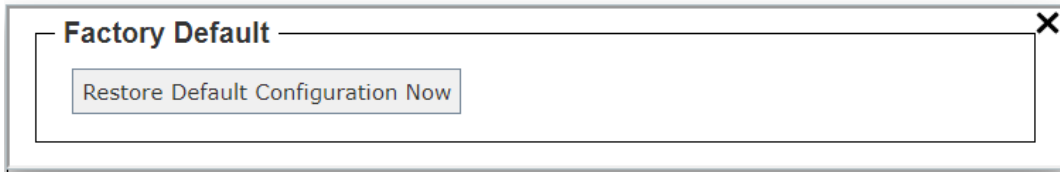


Figure 9.4.2. Factory Default Pop-up Window

The AW5601 Industrial Wireless Access Point comes equipped with one LAN interface. Its default network settings are summarized in Table 9-1Table 9-1. Upon arrival, it will be configured to operate in AP mode. The factory default parameters are listed in

Table 9-2.

Table 9-1. Network Default Setting

Interface	Device IP	Subnet Mask	Gateway IP	DNS
LAN	10.0.50.200	255.255.0.0	10.0.50.1	0.0.0.0

Table 9-2. Wireless Factory Default Setting

Mode	AP mode	WDS	Industrial Communication	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	N/A	N/A	Disabled
WLAN IP Setting (WAN)				
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	
Industrial Communication Setting				
MCS	N/A		Auto	N/A
RSSI Link Threshold			-70	
Roaming Sensitivity			High	
Hole Time			250 ms	
PROFINET Transparent			Disabled	

9.5 Reboot Feature

The Reboot feature under the Maintenance function allows you to reboot the industrial AP router through the web GUI. The Reboot feature is shown in

Figure 9.2. To reboot the device, the user can click the gear icon next to Reboot to open the pop-up window as shown in

Figure 9.3

Figure 9.2. Then, click the **Reboot Now** button to reboot the device.

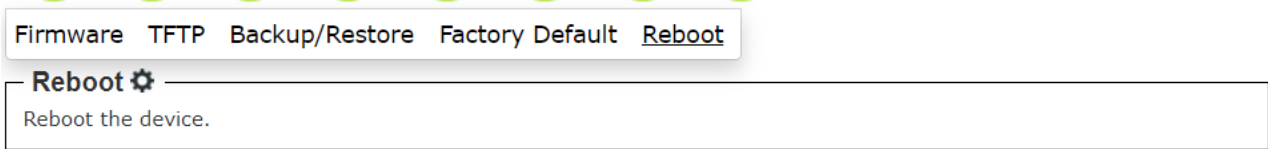


Figure 9.2. Reboot Feature

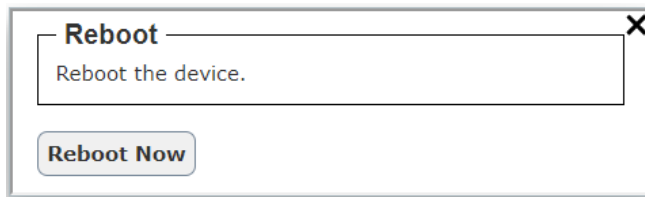


Figure 9.3. Reboot Pop-up Window

10 Logout

To logout of the AW5601, the user can click on the **Logout** icon which is the last circular icon with an open door as shown in Figure 10.1. After clicking on the icon, the user will be returned to the login page as shown in Figure 2.2.



Figure 10.1. Logout Function on Menu Bar

11 Specifications

11.1 Hardware Specification

Table 11-1. Hardware Specification

System	
CPU	Marvell 88F3720
Flash Memory	32MB x1 WSONB
RAM	512MB DDR3
Network	
Ethernet Interface	1x10/100/1000 LAN Connector: RJ45
Wireless Interface	802.11ac, 802.11a, 802.11n, 802.11 b/g MU-MIMO access point
Wi-Fi Security	TKIP, WPA3-PSK, WPA2-PSK, AES, 802.1x(RADIUS)
LED Indicator	
LED indication	AP mode x1 WDS mode x 1 Client mode x 1 5GHz x1 Locate x1 WLAN x1 LAN x1 RUN x1
Power Requirement	

Input	Single 12~48 VDC 3-pin terminal block connector
Mechanical	
Dimensions (W x H x D)	47 x 110 x 90 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

11.2 AW5601 Device Pin Assignments for WAN/LAN Port

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

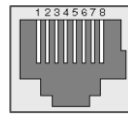


Figure 11.1. WAN/LAN Port on RJ45 with Pin Numbering of AW5601 Device

Table 11-2. 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 that you set the Network Parameters through **the Device Management Utility**© first. This will ensure a proper connection. Other device-specific configurations can then be carried out via Atop's user-friendly web interface.

12 Glossary

- AP – Access Point
- APN – Access Point Name
- AS – Autonomous System
- BIRD – Bird Internet Routing Daemon
- BSSID – Basic Service Set Identifiers
- CAP – Central Access 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 Indicator
- 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
www.atop.com.tw

TAIWAN HEADQUARTERS

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

ATOP INDIA OFFICE & GLOBAL INQUIRIES

Prashant Mishra
No. 3M-217, East of NGEF Layout, Kasturi Nagar,
Bengaluru- 560043, Karnataka, India
Tel: +91-80-492-06308
E-mail: prashant.m@atop.com.tw

ATOP CHINA BRANCH

Sam Xia
3F, 75th, No. 1066 Building,
Qingzhou North Road,
Shanghai, China
Tel: +86-21-64956231
E-mail: info@atop.com.tw

ATOP INDONESIA OFFICE

Anisah Ambarwati
Wisma Slipi, Kav. 12 Lt. 3 Unit 308
Jl. Let. Jend. S. Parman 11480 - Indonesia
Tel: +6221-5326171
E-mail: anisah@atop.com.tw

ATOP JAPAN OFFICE

易傑 Takashi Eki
東京都千代田区丸の内 1-1-3
日本生命丸の内ガーデンタワー3F
Tel: +81-3-4530-3390
E-mail: eki@atop.com.tw

ATOP COLOMBIA OFFICE

Brenda Solano Sarmiento
Calle 35 No. 19 - 41 - Oficina 315 Torre Norte,
Bucaramanga, Santander, Colombia
Tel: +57 322 848 9815
E-mail: brenda.solano@atop.com.tw

ATOP VIETNAM CONTACT

Jenny Duong
Tel: +84 93 275 18 52
E-mail: jenny.duong@atop.com.tw

ATOP NORTH AMERICA CONTACT

Sam Leong
Tel: +1 323 315 0484
E-mail: samleong@atop.com.tw

ATOP EUROPE CONTACT

Timur Dautov
Tel: +48 690 261 220
E-mail: timur@atop.com.tw