

Atop Technologies, Inc.

# AW5601 Series Industrial Access Point

# **User Manual**

V1.0 7<sup>th</sup> March 2024

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

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

# Published by:

### Atop Technologies, Inc.

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

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

# **Technical Support Contact Information**

www.atoponline.com/request-support

#### Asia & Australia

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

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

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

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

USA & Canada Prashant Mishra Tel: +91-80-492-06308 eMail: prasant.m@atop.com.tw <u>China</u> Sam Xia Tel: +86-21-649562-31 eMail: <u>sales@atop.com.tw</u>

#### India & SAARC

Prashant Mishra Tel: +91-80-492-06308 eMail: <u>prasant.m@atop.com.tw</u>

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

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

Alessio Longhini Tel: +39-348-26-28-727 eMail: <u>alessio@atop.com.tw</u>

Indonesia

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

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

Taiwan Tony Lin Tel: +886-968-386876 eMail: tonylin@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 names referenced herein are registered trademarks of their respective companies.

# Preface

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

# Who Should Use This User Manual

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

# **Documentation Control**

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

# **Table of Contents**

1	Intr	oduction	9
	1.1	Overview	9
	1.2	Product Features	
2	Get	ting Started	11
	2.1	Default Factory Settings	
		2.1.1 The Reset Button	
	2.2	Login Process and Main Window Interface	
		2.2.1 Login Process	
~		2.2.2 Main Window Interface	
3	Ма	in Menu	
	3.1	Information Feature	
	3.2	WLAN Feature	
	3.3	Flash-Roaming Feature	
	3.4 3.5	LAN IP Feature	
4		System Log Feature	
4	CO	nfiguration	
	4.1	LAN IP Feature	
	4.2	Wi-Fi Feature	-
		4.2.1 Wi-Fi AP Mode / Client Mode	
		4.2.2 Wi-Fi WDS-AP / Client / Hybrid Mode (Non-NAT)	
	4.3	4.2.3 Wi-Fi Flash-Roaming AP / Flash-Roaming Client Mode Flash-Roaming Feature	
	4.3	4.3.1 Flash-Roaming AP / Flash-Roaming Client Mode	
		4.3.2 PROFINET Transparent over Flash-Roaming and NAT	
	4.4	NAT Feature	
		4.4.1 Basic NAT (N:1 NAT)	
		4.4.2 Static NAT (1:1 NAT)	
		4.4.3 NAPT	
5	Dia	gnostic	39
	5.1	System Log Feature	40
	5.2	SMTP Event Feature	41
	5.3	Log Event Feature	
	5.4	Ping Feature	
_	5.5	Locate Feature	
6	Sec	curity	46
	6.1	Firewall - Mac Filtering Feature	47
	6.2	Firewall - IP Filtering Feature	
7	Ma	nagement	48
	7.1	Account Feature	
	7.2	HTTPS/Telnet/SSH Feature	
	7.3	SNMP Feature	50
8	Ma	intenance Feature	54
	8.1	Firmware Feature	
	8.2	TFTP Feature	55

	8.3	Backup / Restore Feature	55
	8.4	Factory Default Feature	57
	8.5	Factory Default Feature Reboot Feature	58
9	Log	jout	. 59
10	Spe	ecifications	60
		Hardware Specification AW5601 Device Pin Assignments for WAN/LAN Port	
11	Glo	ssary	62

Figure 1. An Application of Industrial Wireless Access Point in WLAN.	
Figure 2. IP Address for Web-based Setting	
Figure 3. Login Prompt	
Figure 4. Default Web Interface for AW5601	
Figure 5. Function Bar on Top of Web GUI	
Figure 6. Main Window Interface	
Figure 7. Logo and banner Information	
Figure 8. Panel Information	
Figure 9. Function Bar on Top of Web GUI	
Figure 10. Sub Function Button	
Figure 11. Gear Button	
Figure 12. Pop-up Window	
Figure 13. Configuration Window	
Figure 14. Close Window Button	
Figure 15. Save Changes and Apply Button	
Figure 16. Main Menu	
Figure 17. Information Function	
Figure 18. System Setting Pop-up Window	
Figure 19. WLAN feature	
Figure 20. Wi-Fi Setting Pop-up Window	
Figure 21. Flash-Roaming Feature	
Figure 22. Flash-Roaming Setting Pop-up Window	
Figure 23. LAN IP Feature	
Figure 24. IP Network Setting Pop-up Window	
Figure 25. Log Feature	
Figure 26. System Log Setting Pop-up Window	
Figure 27. Configuration Function on Menu Bar	
Figure 28. LAN IP Feature	
Figure 29. IP Network Setting Pop-up Window	
Figure 30. Wi-Fi AP Mode / Client Mode Topology	
Figure 31. Wi-Fi AP Mode for AP1 Setting	
Figure 32. Wi-Fi Client Mode for AP2 Setting	
Figure 33. WDS-AP/Client/Hybrid Mode Topology	
Figure 34. WDS-AP Mode for AP1 Setting	
Figure 35. WDS-Hybrid Mode for AP2 Setting	
Figure 36. WDS-Client Mode for AP3 setting	
Figure 37. Flash-Roaming AP / Flash-Roaming Client Topology	
Figure 38. Flash-Roaming AP Mode for AP1 setting	
Figure 39. Flash-Roaming Client Mode for AP2 Setting	
Figure 40. Flash-Roaming AP Mode Setting	
Figure 41. Flash-Roaming Client Mode Setting	
Figure 42. NAT Feature	
Figure 43. Basic NAT (N:1 NAT) Feature	
Figure 44. Wi-Fi Client Enable Basic NAT Mode	
Figure 45. Static NAT (1:1 NAT) Feature	
Figure 46. Static NAT Setting Pop-up Window	
Figure 47. NAPT Feature	
Figure 48. NAPT Setting Pop-up Window	
Figure 49. Diagnostic Function on Menu Bar	
Figure 50. System Log Feature	
Figure 51. Systm Log Setting Pop-up Window	
Figure 52. Systm Log Clear Pop-up Window	
Figure 53. SMTP Event Feature	
Figure 54. SMTP Event Setting Pop-up Window	
Figure 55. Log Event Feature	. 42

Figure 56. Log Event Pop-up Window	
Figure 57. Ping Feature	
Figure 58. Ping Pop-up Window	
Figure 59. Ping Successful with No Packet Loss	
Figure 60. Ping Unsuccessful with 100% Packet Loss	
Figure 61. Locate Feature	
Figure 62. Locate Pop-up Window	
Figure 63. Locate Turn-on State on Panel	44
Figure 64. Locate Turn-off State on Panel	45
Figure 65. Security Function on Menu Bar	
Figure 66. Seurity Feature	
Figure 67. Firewall – Mac Filtering Pop-up Window	
Figure 68. Firewall – IP Filtering Pop-up Window	
Figure 69. Management Function on Menu Bar	
Figure 70. Account Feature	
Figure 71. Account Pop-up Window	
Figure 72. HTTPS/Telnet/SSH Feature	
Figure 73. HTTPS/Telnet/SSH Feature Pop-up Window	
Figure 74. SNMP Feature	50
Figure 75. SNMP Agent Mode and SNMP v1/v2c Community Managment	51
Figure 76. SNMP v1/v2c Trap Management	51
Figure 77. SNMP v3 Feature	52
Figure 78. SNMP v3 Configuration Pop-up Window	52
Figure 79. SNMP v3 Trap Server Setting Pop-up Window	53
Figure 80. Maintenance Function on Menu Bar	54
Figure 81. Firmware Feature	54
Figure 82. Upgrade Firmware Pop-up Window	54
Figure 83. Upgrade Firmware Pop-up Alert Window	55
Figure 84. TFTP Feature	55
Figure 85. TFTP Pop-up Window	
Figure 86. Backup/Restore Feature	56
Figure 87. Backup Pop-up Window	56
Figure 88. Restore pop-up window	56
Figure 89. Factory Default Feature	57
Figure 90. Factory Default Pop-up Window	
Figure 91. Reboot Feature	
Figure 92. Reboot Pop-up Window	
Figure 93. Logout Function on Menu Bar	
Figure 94. WAN/LAN Port on RJ45 with Pin Numbering of AW5601 Device	

# List of Tables

Table 1. Network Interfaces Default Settings	
Table 2. Login Default Settings	
Table 3. Descriptions of the Function Bar	
Table 4. Descriptions of the Information Features	
Table 5. Description of Log Entry	
Table 6. Description of System Log Setting Pop-up Entry	
Table 7. Description of IP Network Settings	
Table 8. Description of Wi-Fi mode with packet forwarding	
Table 9. Wi-Fi AP / Client Mode Setting Table	
Table 10. Wi-Fi AP / Client Mode's Devices IP Address Setting Table	
Table 11. WDS-AP/WDS-Hybrid/WDS-Client Mode for APs Setting	
Table 12. Flash-Roaming AP / Flash-Roaming Client mode setting	
Table 13. Devices IP address setting	
Table 14. Descriptions of the Flash-Roaming AP mode	
Table 15. Descriptions of the Flash-Roaming Client Mode	
Table 16. Flash-Roaming AP / Flash-Roaming Client Mode Setting	
Table 17. Flash-Roaming AP / Flash-Roaming Client Mode's Device IP Address setting	
Table 18. Network Default Setting	57
Table 19. Wireless Factory Default Setting	57
Table 20. Hardware Specification	60
Table 21. Assignment for RJ-45 Connector of AW5601 Device	61

# 1 Introduction

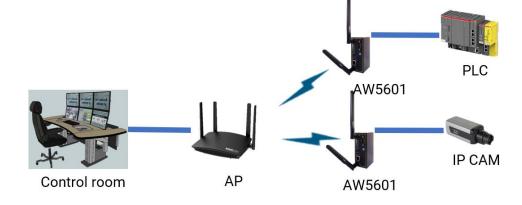
## 1.1 Overview

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

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

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

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



# 1.2 Product Features

#### AW5601 Platform

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

# 2 Getting Started

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

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

### 2.1 Default Factory Settings

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

AW5601 default network parameters are listed in the table below.

#### Table 1. Network Interfaces Default Settings

IP Address	Subnet Mask	Default Gateway
10.0.50.200	255.255.0.0	0.0.0.0

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

#### Table 2. Login Default Settings

Login Parameter	Default Values
Username	admin
Password	default

#### 2.1.1 The Reset Button

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

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

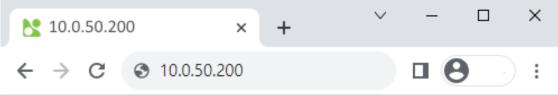
3.

# 2.2 Login Process and Main Window Interface

#### 2.2.1 Login Process

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

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



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

Figure 3. Login Prompt

Technologies P	10.0.50.200 顯示 Warrning! You are now accessing a monitored device, and any ununauthorized login will be recorded. 確定
Model Name: AW56	01

1	 	
Username	 	
Password		

After the login process, the main interface will show up as shown in Figure 4. Under the Atop Technologies' Logo, there are basic information about the device which are Model Name, Kernel Version, Firmware Version, Serial Number (SerialNum) and MAC Address. The main configuration menu of the AW5601 is listed as the group of green circular icons called function bar under the basic information of the device. Each configuration web page can be accessed by clicking on corresponding circular icon of the function bar. The user can move the pointer of the mouse on top of particular circular icon to see the tooltip that indicates the name of the icon.

#### Figure 4. Default Web Interface for AW5601

	)				
	Model Name: AW5601 Loader Version:		C Address: 00:60: rnel Version: K1.0		SerialNum : 0 Firmware Version: V1.00
	?>		69@		
	Information O				
ANT1 atop ANT1 AP mode WDS mode	System Name: System Description: System Location: System Contact: System OID:	AW5601 AW5601 Router's Location www.atop.com.tw			
Client mode	Uptime: 0 days, 0 hours, 9 minutes Current Date & Time: 2023/04/28 10:04 BST				
	WLAN &			- Z-Roaming	¢
	Wi-Fi Radio : Operating Mode : SSID: Channel :	Enabled AP AW5601 149		Wi-Fi Radio : Operating Mod SSID: Channel :	Disabled le :
Locate	LAN IP &				
WLAN .	IP Address: Netmask:	192.168.10.1 255.255.255.0			
LAN	– Log 🌣 –––––				
ANT2 Reset	Date	Time	Up Time		Event
Reset 9	2023/04/28	09:55:16	00d00h00m23s		LAN Link is Up
	2023/04/28	09:55:16	00d00h00m23s		Power POEt 1 is Up

Figure 5. Function Bar on Top of Web GUI



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

### 2.2.2 Main Window Interface

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

Figure 6. Main Window Interface

technologies	Model Name: AW5601 Loader Version:	MAC Address: 00:60:E9 Kernel Version: K1.00	SerialNum : 0 Firmware Version: V1.00
B. ANT1 atop	DHCP CI		
<ul> <li>AP mode</li> <li>WDS mode</li> <li>Client mode</li> </ul>	Subnet Mask: 255.255.2 Gateway IP: DNS Servers 1: DNS Servers 2:	255.0	
Locate 5 Ghz WLAN RUN LAN ANT2 Reset 801			

A. Banner with device Information

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

Figure 7. Logo and banner Information



Model Name: AW5601 Loader Version: MAC Address: 00:60:E9:00:00:00 Kernel Version: K1.00 SerialNum : 0 Firmware Version: V1.00

V1.0

B. Panel Information

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

Figure 8. Panel Information



C. Function Bar.

All main function buttons display here.

Figure 9. Function Bar on Top of Web GUI



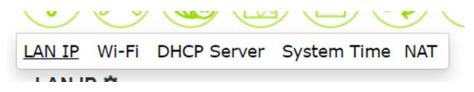
Table 3. Descriptions of the Function Bar

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

D. Sub function button.

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

Figure 10. Sub Function Button



E. Main display section.

Current operation function display section.

F. Gear button.

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

Figure 11. Gear Button

Ø

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

Figure 12. Pop-up Window

atop	)		
	Model Name: AW5601 Loader Version:	MAC Address: 00:60:E9 Kernel Version: K1.00	SerialNum : 0 Firmware Version: V1.00
	Image: Wi-Fi         DHCP Ser	ver System Time Profinet NAT	
ANT1 ANT1 AP mode WDS mode Client mode	DHCP Setting DHCP Client: IPv4 Setting IPv4 Address: Subnet Mask: Gateway IP: DNS Servers 1: DNS Servers 2:	Disabled V	H.
Locate C 5 Ghz WLAN CRUN LAN ANT2 Reset	Save Changes and Apply	Í.	

G. Configuration window.

It displays configurations for function.

Figure 13. Configuration Window

system contact:	www.atop.com.tw	
DHCP Setting — DHCP Client:	Disabled 🗸	×
- IPv4 Setting		
IPv4 Address:	192.168.10.1	
Subnet Mask:	255.255.255.0	
Gateway IP:		
DNS Servers 1:		
DNS Servers 2:		

H. Close button.

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

Figure 14. Close Window Button

V1.0

I. Save Changes and Apply button.

"Save Changes and Apply" button will save and apply the settings.

Figure 15. Save Changes and Apply Button.



# 3 Main Menu

This is the main welcome screen once the user has logged in. The details make it easier to identify different access points connected to the network. The information web page is separated into five boxes or features called **Information**, **WLAN**, **Flash-Roaming**, **LAN IP** and **Log** as shown in Figure 16. . Each feature usually includes a gear icon next to the feature's name. This gear for particular feature can be used to bring up a pop-up window for managing configuration of that particular feature.

#### Figure 16. Main Menu

Information 🌣					
System Name: System Description: System Location: System Contact: System OID:	AW5601 AW5601 Router's Location www.atop.com.tw				
Uptime: Current Date & Time:	8 days, 1 hours, 36 r 2023/05/06 11:31 B				
WLAN Ø			- Flash-Roa	ming 🗘 —	
Wi-Fi Radio : Operating Mode : SSID: Channel :	Enabled Client AW5601		Wi-Fi Radio Operating M SSID: Channel :		Enabled AP flash-roaming 36
IP Address: Netmask:	192.168.10.1 255.255.255.0				
LAN IP &					
IP Address: Netmask:	192.168.10.1 255.255.255.0				
Log 🌣 —					
Date	Time	Up Time		Event	
2023/04/30	09:59:31	02d00h04n	n37s	LAN Link is	Up
2023/04/30	09:59:29	02d00h04n	135s	LAN Link is	Down
2023/04/30	09:59:27	02d00h04n	n33s	LAN Link is	Up
2023/04/30	09:59:25	02d00h04n	n31s	LAN Link is	Down

# 3.1 Information Feature

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

#### Figure 17. Information Function

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

Table 4. Descriptions of the	e Information Features
------------------------------	------------------------

Label	Description	Factory Default
System Name	Specifies a particular role or application of different switches. The name entered here will also be shown in Atop's Device Management Utility. Max. 63 Characters.	(Model name)
System Description	Detailed description of the unit. Max. 63 Characters.	Managed Switch + (Model name)
System Location	Location of the switch. Max. 63 Characters.	Switch Location
System Contact	Provides contact information for maintenance. Enter the name of whom to contact in case a problem occurs. Max. 63 Characters.	www.atop.com.tw
System OID	System's SNMP object identification (OID) numbers.	-
Model name	The device's complete model name.	AW5601
Loader Version	The bootloader version of the device.	-
Kernel Version	The current kernel version of the device.	-
Firmware Version	The current firmware version of the device.	-
Uptime	The duration of time since the device was started in days, hours, and minutes.	-
<b>Current Date &amp; Time</b>	The current date and time of the device.	-

To change or configure fields under the Information feature, the user can click on the gear icon to bring up a pop-up window called System Setting as shown in Figure 18 On this window, the user can configure System Name, System Description, System Location and System Contact. After you finished, clicking on the **Save Changes and Apply** button to save and apply the settings.

Figure 18. System Setting Pop-up Window

System Setting ——		
System Name:	AW5601	
System Description:	AW5601	
System Location:	Router's Location	
System Contact:	www.atop.com.tw	
System OID:	-	
Loader Version:	L1.01	
Kernel Version:	K1.00	
Firmware Version: MAC Address:	V1.00	

### 3.2 WLAN Feature

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

#### Figure 19. WLAN feature

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

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

#### Figure 20. Wi-Fi Setting Pop-up Window

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 🗸	

#### 3.3 Flash-Roaming Feature

The Flash-Roaming feature displays the current setting of the Wi-Fi configuration of the access point which are the status of Flash-Roaming's Wi-Fi Radio, Operating Mode, SSD, and Channel as shown in Figure 21.

This roaming feature allows mobile devices to smoothly switch between different locations within the wireless network without experiencing interruptions in connectivity

#### Figure 21. Flash-Roaming Feature

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

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

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

Figure 22. Flash-Roaming Setting Pop-up Window

Flash-Roaming Setting	g
Wi-Fi Radio:	Enabled 🗸
Operating Mode:	AP V
Country:	TW 🗸
Tx Power:	Medium 🖌
Network Name (SSID):	flash-roaming
Wireless Mode:	5G(802.11n/ac) 🗸
MCS:	Auto 🗸
Channel Bandwidth:	20 MHz 🗸
Control Channel:	149 🗸
Authentication Method:	WPA3 Personal (SAE) 🗸
Password:	default123
Client Isolate:	Enabled 🗸
RSSI Link Threshold:	-70

# 3.4 LAN IP Feature

The LAN IP feature displays the current setting of the network configuration of the access point which are the status of IP Address, and Sub-Netmask as shown in Figure 23. To change network configuration, the user can click on the gear icon to bring up the IP Network Setting pop-up window as shown in Figure 24. The user can choose to enable or disable the Dynamic Host Configuration Protocol (DHCP) on the device as the DHCP client by selecting the corresponding drop-down list. If the DHCP Client is enabled, the manage switch will obtain the IP address configuration from another server in the network. If the DHCP Client is disabled, the user will have to enter the IPv4 Address, Subnet Mask, Gateway IP, DNS Servers 1 and DNS Servers 2. After you finished, clicking on the Save Changes and Apply button to **save and apply** the settings.

#### Figure 23. LAN IP Feature

LAN IP 🌣		
IP Address:	192.168.10.1	
Netmask:	255.255.255.0	

Figure 24.	IP Network	Setting Po	op-up Window
------------	------------	------------	--------------

- DHCP Setting —		
DHCP Client:	Disabled V	
- IPv4 Setting		
IPv4 Address:	192.168.10.1	
Subnet Mask:	255.255.255.0	
Gateway IP:		
DNS Servers 1:		
DNS Servers 2:		

### 3.5 System Log Feature

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

#### Figure 25. Log Feature

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

#### Table 5. Description of Log Entry

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

If the user would like to configure the System Log Setting, the user can click on the gear icon to bring up a System Log Setting pop-up window as shown in Figure 26. On this window, the user can enable or disable sending log to a log server. If the user enables the Log to Server option by choosing from the pull-down menu, the user will have to specify the Log's Server IP Address and Server Service Port in the next two fields. After you finished, clicking on the **Save Changes and Apply** button to save and apply the settings.

#### Figure 26. System Log Setting Pop-up Window

- System Log Setting -		>
Log to Server:	Disable 🗸	
Server IP Address:	0.0.0	
Server Service Port:	514	

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

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

# 4 Configuration

The Configuration or System Setting function is the second icon from the left. It is the circular icon with the pictures of wrench and screw driver. There are five features under the Configuration or System Setting function which are **LAN IP**, **Wi-Fi**, **DHCP Server**, **System Time** and **NAT** as shown Figure 27.

#### Figure 27. Configuration Function on Menu Bar



### 4.1 LAN IP Feature

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

#### Figure 28. LAN IP Feature

LAN IP Wi-Fi	DHCP Server System Ti	me Profinet NAT
LAN IP 🌣 —		
DHCP Client: IPv4 Address: Subnet Mask: Gateway IP: DNS Servers 1: DNS Servers 2:	Disabled 192.168.10.1 255.255.255.0	

Figure 29. IP Network Setting Pop-up Window

- DHCP Setting —		
DHCP Client:	Disabled V	
- IPv4 Setting —		
IPv4 Address:	192.168.10.1	
Subnet Mask:	255.255.255.0	
Gateway IP:		
DNS Server 1:		
DNS Server 2:		

Table 7. Description of IP Network Settings

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

#### 4.2 Wi-Fi Feature

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

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

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

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

Yes: It means that this type of packet can be delivered.

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

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

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

#### 4.2.1 Wi-Fi AP Mode / Client Mode

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

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

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

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

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



#### Figure 31. Wi-Fi AP Mode for AP1 Setting

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 32. Wi-Fi Client Mode for AP2 Setting

Wi-Fi Setting		,
Wi-Fi Radio:	Enabled 🗸	
Operating Mode:	Client 🗸	
Country:	TW 🗸	
Tx Power:	Low 🗸	
Network Name (SSID):	AW5601	
Authentication Method:	WPA2 Personal (PSK)	
Password:	12345678	
NAT Enabled:	Disabled 🗸	
Active Scan:	Disabled 🗸	
- WLAN IP Setting(WAN	)	
DHCP Client:	Disabled 🗸	
IPV4 Address:	10.0.50.201	
Subnet Mask:	255.255.0.0	
Gateway IP:		
LAN IP Setting		
IPV4 Address:	10.0.100.201	
Subnet Mask:	255.255.0.0	

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

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

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

	Device1	Device2
IP Address	10.0.50.1	10.0.100.2

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

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

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

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

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

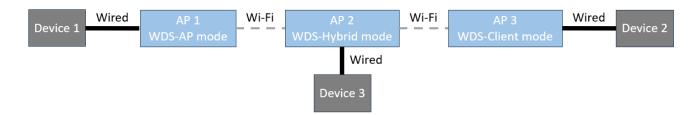
Before you set up a wireless network with WDS, both access points must meet the following conditions:

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

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

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

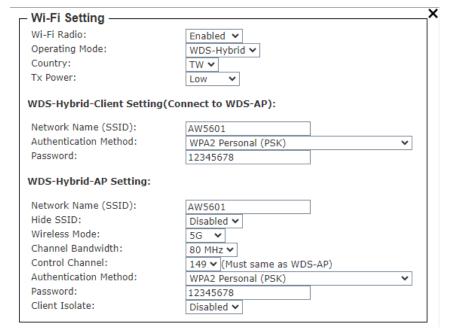
### Figure 33. WDS-AP/Client/Hybrid Mode Topology



#### Figure 34. WDS-AP Mode for AP1 Setting

Wi-Fi Setting		
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 35. WDS-Hybrid Mode for AP2 Setting



#### Figure 36. WDS-Client Mode for AP3 setting

-Fi Radio:	Enabled 🗸	
perating Mode:	WDS-Client V	
Country:	TW 🗸	
'x Power:	Low 🗸	
letwork Name (SSID):	AW5601	
uthentication Method:	WPA2 Personal (PSK)	~
assword:	12345678	
active Scan:	Disabled 🗸	

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

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

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

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

# 4.3 Flash-Roaming Feature

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

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

### 4.3.1 Flash-Roaming AP / Flash-Roaming Client Mode

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

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



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

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

### Table 13. Devices IP address setting

	Device1	Device2
LAN IP Setting	10.0.50.1	10.0.50.22

# Figure 38. Flash-Roaming AP Mode for AP1 setting

<ul> <li>Flash-Roaming Setting</li> </ul>	) <u> </u>
Wi-Fi Radio:	Enabled 🗸
Operating Mode:	AP V
Country:	TW 🗸
Tx Power:	Medium 💙
Network Name (SSID):	flash-roaming
Wireless Mode:	5G(802.11n/ac) 🗸
MCS:	Auto 🗸
Channel Bandwidth:	20 MHz 🗸
Control Channel:	149 🗸
Authentication Method:	WPA3 Personal (SAE) 🗸
Password:	default123
Client Isolate:	Enabled 🗸
RSSI Link Threshold:	-70

# Table 14. Descriptions of the Flash-Roaming AP mode

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

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

### Figure 39. Flash-Roaming Client Mode for AP2 Setting

Wi-Fi Radio:	Enabled 🗸
Operating Mode:	Client V
Country:	TW V
Tx Power:	Medium 🗸
Network Name (SSID):	flash-roaming
Wireless Mode:	5G(802.11n/ac) 🗸
MCS:	Auto 🗸
Channel Bandwidth:	20 MHz 🗸
Control Channel:	149 🗸
Authentication Method:	WPA3 Personal (SAE) 🗸
Password:	default123
RSSI Link Threshold:	-70
Roaming Sensitivity:	High V
Hold Time:	250 🗢 ms
NAT Enabled:	Enabled V
PROFINET Transparent:	Disabled V

Table 15. Descriptions of the Flash-Roaming Client Mode

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

Label	Description	Default Value
Wireless Mode	2.4 GHz: IEEE 802.11g/n,	5G (802.11n/ac)
	5 GHz: IEEE 802.11n/ac, or IEEE 802.11a only, or IEEE	
	802.11n only.	•
MCS	Modulation Coding Scheme index is a metric based on	Auto
	several parameters of a Wi-Fi connection between two	
	stations. Auto means MCS full range automatic adjustment,	
	and Stable means locked in some relatively stable range.	
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	36
	the Regulatory Domain	
	5 GHz: depending on the Regulatory Domain	
	• Channel 36, 40, 44, 48 for EU/JP and IEEE 802.11a	
	only, or IEEE 802.11n only, or 802.11n/ac.	
	• Channel 36, 40, 44, 48, 149, 153, 157, 161, 165 for TW	
	and IEEE 802.11a only, or IEEE 802.11n only, or	
	802.11n/ac.	
	<ul> <li>Channel 36, 40, 44, 48, 149, 153, 157, 161, 165 for US</li> </ul>	
	and IEEE 802.11a only, or IEEE 802.11n only, or	
	802.11n/ac.	
	<ul> <li>Channel 149, 153, 157, 161, 165 for CN and IEEE 802.11a only, or IEEE 802.11n only, or 802.11n/ac.</li> </ul>	
Authentication Method	Mode of authentication for WLAN which can be Open	WPA3 Personal
Authentication Method	System, WPA3 Personal (SAE)	(SAE)
Password	This is a user defined string which must be ASCII format	default123
Fassword	between 8 and 63 characters.	uerault125
RSSI Link Threshold	RSSI (Received Signal Strength Indicator), minimum	-70
	connectable signal strength.	,0
Roaming Sensitivity	Enable this option to allow Flash-Roaming Client mode to	High
	scan for available access points in the background to speed	. iigii
	up roaming when necessary.	
	Very High or High or Medium or Low or Very Low.	
Hold Time	The minimum stay time after connecting to the AW5601.	250 ms
	When there are multiple AW5601s with similar signal	
	strength around, setting this value appropriately can avoid	
	frequent switching between devices.0 to 2000 ms	
NAT Enabled	Network Address Translation. Enabled or Disabled.	Enabled
PROFINET Transparent	Enable this option to allow Flash-Roaming Client mode to	Disabled
•	forward PRIFINET packets.	

# 4.3.2 PROFINET Transparent over Flash-Roaming and NAT

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

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

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

PROFINET Transparent N/A Enabled

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

	Device1	Device2
LAN IP Setting	10.0.50.1	10.0.50.22

#### Figure 40. Flash-Roaming AP Mode Setting

<ul> <li>Flash-Roaming Setting</li> </ul>	g
Wi-Fi Radio:	Enabled 🗸
Operating Mode:	AP V
Country:	TW 🗸
Tx Power:	Medium 🗸
Network Name (SSID):	flash-roaming
Wireless Mode:	5G(802.11n/ac) 🗸
MCS:	Auto 🖌
Channel Bandwidth:	20 MHz 🗸
Control Channel:	149 🗸
Authentication Method:	WPA3 Personal (SAE) 🗸
Password:	default123
Client Isolate:	Enabled 🗸
RSSI Link Threshold:	-70

# Figure 41. Flash-Roaming Client Mode Setting

g		
Enabled V		
Client 🗸		
TW 🗸		
Medium 🗸		
flash-roaming		
5G(802.11n/ac) 🗸		
Auto 🗸		
20 MHz 🗸		
149 🗸		
WPA3 Personal (SAE) 🗸		
default123		
-70		
High V		
250 🗢 ms		
Enabled V		
Enabled V		
)		
Disabled V		
10.0.50.200		
255.255.0.0		

# 4.4 NAT Feature

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

#### Figure 42. NAT Feature

LAN IP	DHCP Server	System Time	NAT							
NAT or	nly works in Clie	ent mode!								
- Basic	NAT (N:1 NAT	) ————								
State:		Disabled								
- Static	NAT (1:1 NAT	) ¢ —								
	0 v entries									
							Search:			
Name		▲ Local IP			\$	External IP				\$
			No	data ava	ilable in t	table				
Showing	0 to 0 of 0 entrie	es								
									Previous	Next
	¢									
Show 1	0 🗙 entries									
							Search:			
Name	Traffic Ty	/pe 🌲	Local	IP	🔶 Loc	al Port	🔶 Ex	terna	l Port	\$
			No	data ava	ailable in t	table				
Showing	0 to 0 of 0 entrie	es								
									Previous	Next

## 4.4.1 Basic NAT (N:1 NAT)

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

NAT only works in	Client mode!	
- Basic NAT (N:1 N	IAT)	
State:	Disabled	

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

Figure 44. Wi-Fi Client Enable Basic NAT Mode

Wi-Fi Radio:	Enabled 💙
Operating Mode:	Client 🗸
Country:	EU 🗸
Tx Power:	Very high 🗸
Network Name (SSID):	AW5601
Authentication Method:	WPA2 Personal (PSK) V
Password:	default123
NAT Enabled:	Enabled 🖌
Active Scan:	Disabled 🗸

## 4.4.2 Static NAT (1:1 NAT)

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

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

Show 10 v entries	¢				
			Search	h:	
Name '	Local IP	\$	External IP		\$
		No data available in	table		
Showing 0 to 0 of 0 entries	3				
				Previous	Next

## Figure 46. Static NAT Setting Pop-up Window

Static NAT Setting ——						×
Group Name:						
Local IP:						
External IP:						
Add						
─ Static NAT Interface En	try					
Show 10 🗸 entries						
				Search:		
Name 🔺	Local IP	4	External IP			\$
	No	o data available in	table			
-						
Showing 0 to 0 of 0 entries						
Showing 0 to 0 of 0 entries					Previous	Next
Showing 0 to 0 of 0 entries					Previous	Next

## 4.4.3 NAPT

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

## Figure 47. NAPT Feature

Show 10	✓ entries			Search:	
Name	Traffic Type	🜲 Local IP	🜲 Local Port	🜲 External Port	\$
		No data ava	ailable in table		
Showing 0 t	o 0 of 0 entries				
				Previous	Next

Figure 48. NAPT Setting Pop-up Window

NADT Soffing				×
NAPT Setting				
Name:				
Traffic Type:	TCP 🗸			
Local IP:				
Local Port:				
External Port:				
Add				
Inde				
- NAPT Entry				
Show 10 V entries				
			Search:	
Name 🔺 Traffic Type	🔶 Local IP	Local Port	External Port	
Name Trainc Type			* External Port	<b>•</b>
	No data	a available in table		
Showing 0 to 0 of 0 entries				
			Previous	Next
			Previous	Next
Remove				
Save Changes and Apply				
(16				

# 5 Diagnostic

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

Figure 49. Diagnostic Function on Menu Bar



## 5.1 System Log Feature

The System Log feature under the Diagnostic function contains two sections: **System Log Setting** and **System Log** as shown in Figure 50. In the upper section, the System Log Setting summarizes the current configuration of system log. To configure the system log, the user can click on the gear icon next to the System Log Setting title to bring up the System Log Setting pop-up window as shown in Figure 51. Note that this pop-up window is the same feature as described in Log feature under the Information function in Table 6.

In the lower section of the web page, a table of system log is displayed. Each log entry includes Date, Time, Up Time, and Event description. Note that the log entries are sorted by date and time. Table 5 in Section 3.5 provides explanation of each column in the System Log table. The user can choose how many log entries to be displayed in the table by selecting the number (20, 50 or 100) from the Show's drop-down list. Additionally, the user can find relevant log entries through the Search box on the top left of the table. Under each column, the user can filter the log entries based in Date, Time, Up Time, and Event. The user can also click on the Refresh button to obtain the latest log entries from the access point.

Figure	50.	System	Log	Feature
			9	

System Log	SMTP Event	Log Event	Ping	Locate		
- System Lo	g Setting 🌣					
Log to Server Server IP Ado Server Servic	dress:	Disable 0.0.0.0 514				
- System Lo	g 🗘 ———					
Show 20 🗸	entries				Search:	
Time				<b></b>	Text	\$
Mon Oct 16 0	8:22:11 2023				admin: Clear System Log	
	Filter Time		]		Filter Text	
Showing 1 to	1 of 1 entries					
					Previo	ous 1 Next
Refresh						

Figure 51. Systm Log Setting Pop-up Window

Server IP Address: 0.0.0.0	0.0.0.0 514			
	514			
Server Service Port: 514				
ave Changes and Apply	r			

To clear the table of system log, the user can click on the gear icon of the System Log title to bring up the System Log Clear pop-up window as shown in Figure 52. By clicking on the Clear System Log button on this pop-up window, the user can clear all log entries.

Figure 52. Systm Log Clear Pop-up Window

System Log Clear 🚽	٢
Clear Sytem Log	

## 5.2 SMTP Event Feature

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

Figure 53. SMTP Event Feature

System Log	SMTP Event	Log Event	Ping	Locate
- SMTP Sett	tting 🌣 ———			
Mode: SMTP Server Sender E-ma Mail Subject: SSL/TLS: Authenticatio Username: Password:	ail Address: t:	Disable 0.0.0.0 administrat Automated Disable Disable -		Alert
Recipient E-n Recipient E-n Recipient E-n Recipient E-n	mail Address 1: mail Address 2: mail Address 3: mail Address 4: mail Address 5: mail Address 6:	-		

- SMTP Setting	×
Mode:	Disable 🗸
SMTP Server Address:	0.0.0.0
Sender E-mail Address:	administrator
Mail Subject:	Automated Email Alert
SSL/TLS:	Disable 🗸
Authentication:	Disable 🗸
Username:	
Password:	
Confirm Password:	
Recipient E-mail Address 1:	
Recipient E-mail Address 2:	
Recipient E-mail Address 3:	
Recipient E-mail Address 4:	
Recipient E-mail Address 5:	
Recipient E-mail Address 6:	
Save Changes and Apply	

## 5.3 Log Event Feature

## Figure 55. Log Event Feature

system Log SMTP Event Log Event Ping Locate		
Log Event 🌣		
Event	SYSLOG	SMTP
System coldstart/warmstart	Disable	Disable
Authentication Failure	Disable	Disable
IP Address Changed	Disable	Disable
Account Profile Changed	Disable	Disable

## Figure 56. Log Event Pop-up Window

Event	SYSLOG	SMTP
System coldstart/warmstart		
Authentication Failure		
IP Address Changed		
Account Profile Changed		

## 5.4 Ping Feature

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

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

Figure 57. Ping Feature

System Log	SMTP Event	Log Event	<u>Ping</u>	Locate	
- ICMP Ping	¢				
Ping an IPv4 a	address.				

Figure 58. Ping Pop-up Window

ICMP Ping	Ping
Ping an IPv4 address.	
Ping Result	

## Figure 59. Ping Successful with No Packet Loss

Ping Result
• • • • • • • • • • • • • • • • • • • •
PING 10.0.50.200 (10.0.50.200): 56 data bytes
64 bytes from 10.0.50.200: seq=0 ttl=64 time=0.244 ms
64 bytes from 10.0.50.200: seq=1 ttl=64 time=0.188 ms
64 bytes from 10.0.50.200: seq=2 ttl=64 time=0.174 ms
64 bytes from 10.0.50.200: seq=3 ttl=64 time=0.185 ms
10.0.50.200 ping statistics
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.174/0.197/0.244 ms

Figure 60. Ping Unsuccessful with 100% 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

## 5.5 Locate Feature

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

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

Figure 61. Locate Feature

System Log	SMTP Event	Log Event	Ping	<u>Locate</u>
Turn on or turn	n off Locate LED			

Figure 62. Locate Pop-up Window

Locate Led	×
Turn on or turn off Locate Led.	
Turn On Turn Off	

Figure 63. Locate Turn-on State on Panel



## Figure 64. Locate Turn-off State on Panel



# 6 Security

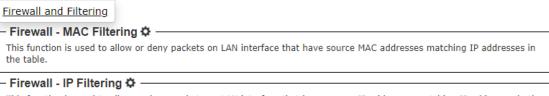
Figure 65. Security Function on Menu Bar



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

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

## Figure 66. Seurity Feature



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

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

Figure 67. Firewall – Mac Filtering Pop-up Window

MAC Filtering —	
	llow or deny packets on LAN interface that have source or destination IAC addresses in the table.
Disable MAC Filtering	
○ Allow packets with MA	C addresses listed below
$\bigcirc$ Deny packets with MA	C addresses listed below
MAC Filtering List	
Id	MAC Address
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
Save Changes and Appl	v

## 6.2 Firewall - IP Filtering Feature

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

Figure 68. Firewall – IP Filtering Pop-up Window

- IP Filtering	<b>_</b> ×'				
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.					
<ul> <li>Disable IP Filtering</li> <li>Allow packets with IP addresses listed below</li> <li>Deny packets with IP addresses listed below</li> </ul>	-				
IP Filtering List					
Id     Src IP Addr     Dst IP Addr       1					
Save Changes and Apply					

# 7 Management

The Management function is the sixth circular icon on the menu bar. It is the icon with gear and person. The Management function has three features which are **Account**, **HTTPS/Telnet/SSH**, and **SNMP** as shown in Figure 69. These features allow the user to manage the accounts, enable secure HTTP for web interface, and set up the SNMP protocol.

Figure 69. Management Function on Menu Bar



## 7.1 Account Feature

The Account feature is shown in Figure 70 with a list of account or user on the managed switch. It is presented in a format of table with two columns: Username and Permission. To add or delete an account or user, the user can click on the gear icon to bring up the Account Setting pop-up window as shown in Figure 71. For each new user, please enter the User Name, Password, Confirm Password and select the Permission Level then click the **Add User** button. To remove a user from the list, entering all information then click the **Delete User** button.

Figure 70. Account Feature

## Figure 71. Account Pop-up Window

- Account				×
User Name:			]	
Password:				
Confirm Password:				
Permission:	Admin 🗸			
Add User Delete Use	r			
User List				
Username		Permission		
admin		Admin		

## 7.2 HTTPS/Telnet/SSH Feature

The HTTPS or Hyper Text Transfer Protocol Secure feature is another feature under the Management function. This page presents the current setting of HTTPS for the managed switch's web interface as shown in Figure 72. To enable the HTTPS, the user can click on the gear icon to bring up the HTTPS Setting pop-up window as shown in Figure 73. Next checking the Enabled box to redirect web interface access to HTTPS protocol. After you finished, clicking on the **Save Changes and Apply** button to save and apply the settings.

## Figure 72. HTTPS/Telnet/SSH Feature

Account	HTTPS/Tel	SNMP	
- Securit	y 🌣 ——		
SSH: Telnet: Redirect	to HTTPS:	Enable Enable Disable	

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

SSH Setting	✓ Enabled	×
Telnet Setting — Telnet	Enabled	
- HTTPS Setting - Redirect to HTTPS	Enabled	

## 7.3 SNMP Feature

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

Figure 74 shows the SNMP feature's web page. It consists of four sections: **SNMP Mode Setting**, **SNMP v1/v2c Trap Setting** and **SNMP v3 Configuration**. The current version of SNMP configured to run on the switch can be viewed behind the SNMP Mode Setting. The SNMP Agent Version can be set to either SNMP v1/v2c or SNMP v3. Note that depending on the SNMP Agent Version selection some of the sections will be active while another section will be grey out. For example, when SNMP Agent Version is set to SNMP v1/v2c, SNMP v1/v2c Agent Setting and SNMP v1/v2c Trap Setting will be available to configure as shown in Figure 75.

## Figure 74. SNMP Feature

Account HTTPS/Telnet/SSH <u>SNMP</u>	
SNMP Mode Setting 🌣	
SNMP Agent Version: SNMPV1/V2c	
SNMP v1/v2c Agent setting	
Community String Privilege public read only	
private read and write	
SNMP v1/v2c Trap Setting 🌣	
Show 10 🗸 entries	
	Search:
Server IP Community	Trap Version 🔶
No data available in table	
Showing 0 to 0 of 0 entries	
	Previous Next
SNMPv3 Configuration 🌣	
SNMP Engine ID:	
SNMP Engine ID: User:	ssword Privacy Protocol Privacy Password
SNMP Engine ID:	ssword Privacy Protocol Privacy Password
SNMP Engine ID:         User:         User Name         Security Level         Authentication         Group:         Security Model	ssword Privacy Protocol Privacy Password Group Name
SNMP Engine ID: User: User Name Security Level Authentication Protocol Authentication Par Group: Security Model Security Name View:	Group Name
SNMP Engine ID: User: User Name Security Level Authentication Protocol Authentication Par Group: Security Model Security Name View: View Name View Type	
SNMP Engine ID: User: User Name Security Level Authentication Protocol Authentication Par Group: Security Model Security Name View: View Name View Type Access:	Group Name
SNMP Engine ID: User: User Name Security Level Authentication Protocol Authentication Par Group: Security Model Security Name View: View Name View Type Access:	Group Name OID Subtree
SNMP Engine ID: User: User Name Security Level Authentication Protocol Authentication Par Group: Security Model Security Name View: View Name View Type Access: Group Name Security Model Security Level Read V	Group Name OID Subtree
SNMP Engine ID: User: User Name Security Level Authentication Protocol Authentication Par Group: Security Model Security Name View: View Name View Type Access: Group Name Security Model Security Level Read V SNMPv3 Trap \$	Group Name OID Subtree
SNMP Engine ID: User: User Name Security Level Authentication Protocol Authentication Par Group: Security Model Security Name View: View Name View Type Access: Group Name Security Model Security Level Read V SNMPv3 Trap \$	Group Name OID Subtree iew Name Write View Name
SNMP Engine ID:         User:         User Name         Security Model         Security Model         View:         View Name         Access:         Group Name         Show 10 ✓ entries	Group Name OID Subtree iew Name Write View Name
SNMP Engine ID: User: User Name Security Level Authentication Protocol Authentication Par Group: Security Model Security Name View: View Name Access: Group Name Security Model Security Level Read V SNMPv3 Trap ↔ Show 10 ✓ entries Server IP ▲ User name	Group Name OID Subtree iew Name Write View Name
SNMP Engine ID: User: User Name Security Level Authentication Protocol Authentication Par Group: Security Model Security Name View: View Name View Type Access: Group Name Security Model Security Level Read V SNMPv3 Trap Show 10 v entries Server IP User name No data available in table	Group Name OID Subtree iew Name Write View Name

To select the SNMP Agent Version, the user can click on the gear icon next to the SNMP Mode Setting to bring up the pop-up window as shown in Figure 75. When the SNMP v1/v2c is selected, the

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

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

- Agent Mode Setting				
SNMP Agent Version:	SNMP v1	/v2c 🗸		
	SNMP v1	/v2c		
<ul> <li>SNMP v1/v2c Comm</li> </ul>	SNMP v3			
Community Strir	ng	P	rivilege	
public		Read	only	~
private		Read a	and Wri	te 🗸
		Read	only	~
		Read	only	~

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

Figure 76. SNMP v1/v2c Trap Management

<ul> <li>Trap Server Setting</li> </ul>				
Server IP				
Community				
Trap Version		○ V1 <b>○</b> V2c		
Add				
SNMP v1/v2c Comn	nunity			
Show 10 💙 entries			_	
			Search:	
Server IP	Community	🔶 Tra	p Version	+
	No data ava	ilable in table		
	Showing 0 to	0 of 0 entries		
	Davis	s Next		
	Previous			

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

## Figure 77. SNMP v3 Feature

SNMPv3 Configuration Structure					
SNMP Engine ID: 800007e5017f000001					
User:					
User Name Security Level Authenticat	tion Protocol	Authentication Passwo	ord Privacy Pro	otocol Privacy P	assword
Group:					
Security Model	Security Nan	ne	Group Na	ame	
View:					
View Name	View Type		OID Subtree		
	included		.1		
Access: Group Name Security Model	Security Lev	vel Read View	Namo	Write View Name	
Group Name Security Model	Security Lev	keau view	Name	write view Name	
- SNMPv3 Trap 🌣					
Show 10 V entries					
			Sear	ch:	
Server IP	4	User name			\$
	a available in table				
Showing 0 to 0 of 0 entries					
Showing o to o or o entries					
				Previous	s Next

To configure SNMP v3, the user can click the gear icon next to the SNMP v3 Configuration to bring up the pop-up window as shown in Figure 78. On this window, there are four sections: SNMP v3 User Configuration, SNMP v3 Group Configuration, SNMP v3 View Configuration, and SNMP v3 Access Configuration. Under the SNMP v3 User Configuration, the user can add new SNMP's user by filling new User Name and set Security Level, Authentication Protocol, Authentication Password, Privacy Protocol and Privacy Password. After finished entering all information, click **Add** button to add the new SNMP's user. Note that you can delete existing user by clicking on **Delete** button in front of that particular User Name. SNMP v3 Group, View, and Access can also be configured in the same manner as described for SNMP v3 User Configuration. After you finished, clicking on the **Save Changes and Apply** button to save and apply the settings.

#### SNMPv3 User Configuration SNMP Engine ID: 800007e5017f000001 User Na ecurity Le Auth ~ Auth, Priv MD5 V DES ¥ Add SNMPv3 Group Configuration curity Mode ecurity Na Group Nam public 🗸 v1 ~ Add SNMPv3 View Configuration

## Figure 78. SNMP v3 Configuration Pop-up Window

	Delete	View Name	View Type	OID Subtree	
	delete	all	included	.1	
	delete		included 🗸		
	Add				

#### - SNMPv3 Access Configuration -

Delete Group Name Security Model S		Security Level	Read View Name	Write View Name		
	delete	~	v1 ¥	NoAuth, NoPriv 🗸	None 🗸	None 🗸
	Add					

To configure SNMP v3 Trap Server, the user can click the gear icon next to the SNMP v3 Trap in Figure 77 to bring up another pop-up window as shown in Figure 79. On this window, the user can set the SNMP v3 Trap Server IP address and choose the User name previously configured in SNMP v3 User Configuration. After clicking on **Add** button, the new entry will be added to the SNMP v3 Trap List shown in the lower part of the window. You can delete an entry from SNMP v3 Trap List by selecting that particular entry and clicking on the **Remove** button.

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

SNMPv3 Trap Server Setting	
Server IP	
User name	▼
Add	
SNMPv3 Trap List	
Show 10 🗸 entries	
	Search:
Server IP 🔺 User n	name 🔶
No data available	e in table
Showing 0 to 0 of	f 0 entries
Previous	Next
Remove	

# 8 Maintenance Feature

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

Figure 80. Maintenance Function on Menu Bar



8.1 Firmware Feature

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

#### Figure 81. Firmware Feature

<u>Firmware</u>	TFTP	Backup/Restore	Factory Default	Reboot
– Upgrade	Firmv	vare 🌣 ———		
	ernel Ver	rsion: L1.01 rsion: K1.00 V1.00		

Figure 82. Upgrade Firmware Pop-up Window

Upgrade Firmware	×
By default upgrading your firmware will completely erase your current configuration. It is strongly recommended that you back up your current configuration before performing an upgrade.	
You can attempt to preserve your old settings by ticking Attempt to Preserve Settings below. Be aware that this can potentially lead to problems if the new version is significantly newer than the old version, but for small, incremental differences this will likely work. It is always best to keep a backup just in case.	
Current Loader Version: L1.01 Current Kernel Version: K1.00	
Current Firmware V1.00 Version:	
Select Firmware File: 選擇檔案 未選擇任何檔案	
Attempt to Preserve Settings	
Upgrade Now	



## 8.2 TFTP Feature

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

Figure 84. TFTP Feature

	Firmware	<u>TFTP</u>	Backup/Restore	Factory Default	Reboot
Upgrade Firmware 🌣 ———————————————————————————————————					
TFTP Server IP: TFTP Port:		- 69			

#### Figure 85. TFTP Pop-up Window

Upgrade Firmware -		<
TFTP Server IP:		
TFTP Port:	69	
TFTP Firmware File:		
Upgrade Now	Attempt to Preserve Settings	

## 8.3 Backup / Restore Feature

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

## Figure 86. Backup/Restore Feature

Firmware	TFTP	Backup/Restore	Factory Default	Reboot						
Backup	– Backup 🌣 –									
-	Backup current configuration.									
- Restore	¢ —									
Restore ol configurati										

## Figure 87. Backup Pop-up Window

Backup —	×
Get Backup Now	

## Figure 88. Restore pop-up window

Select a restore file :	選擇檔案 未選擇任何檔案
Keep username & password :	Disabled 🗸
Keep IP :	Disabled 🗸

## 8.4 Factory Default Feature

The Factory Default feature under the Maintenance function allows the user to reset the device to the original or factory default configuration. The Factory Default web page is shown in Figure 89. To perform the factory default setting, the user can click on the gear icon next to the Factory Default to bring up the pop-up window as shown in Figure 90. Then, clicking on the **Restore Default Configuration Now** button to restore the configuration of the device to the factory default setting.

## Figure 89. Factory Default Feature

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 90. Factory Default Pop-up Window



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

## Table 18. Network Default Setting

Interface Device IP		Subnet Mask	Gateway IP	DNS	
LAN	10.0.50.200	255.255.0.0	0.0.0.0	0.0.00	

## Table 19. Wireless Factory Default Setting

Mode	AP mode	WDS	Flash-Roaming	Client mode
Wi-Fi Radio		Disabled		Enabled
Operating Mode	AP	WDS-AP/Client/Hybrid	AP	Client
Country		TW		
Tx Power		Medium	า	
Network Name	A	W5601	flash-roaming	N/A
(SSID)				
Hide SSID	D	isabled	N/A	
Wireless Mode		N/A		
Channel Bandwidth		20 MHz		N/A
Control Channel		36		
Authentication	WPA2 P	ersonal (PSK)	WPA3 Personal	WPA2 Personal
Method			(SAE)	(PSK)
Password	12	2345678	Default123	12345678
Client Isolate	D	isabled	Enabled	N/A
NAT Enabled	N/A	N/A	En	abled
Active Scan	IN/A	IN/A IN/A		Disabled
WLAN IP Setting (WA	N)			

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

## 8.5 Reboot Feature

The Reboot feature under the Maintenance function supports the rebooting of the managed switch through the web GUI. The Reboot feature is shown in Figure 91. To reboot the device, clicking on the gear icon next to Reboot to bring up the pop-up window as shown in Figure 92. Then, clicking on the **Reboot Now** button to reboot the device.

## Figure 91. Reboot Feature

Firmware	TFTP	Backup/Restore	Factory Default	Reboot
- <b>Reboot</b>				

Figure 92. Reboot Pop-up Window

	- <b>Reboot</b> Reboot the device.	×
(	Reboot Now	

# 9 Logout

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

Figure 93. Logout Function on Menu Bar



# **10 Specifications**

## 10.1 Hardware Specification

Table 20. Hardware Specification

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

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

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

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



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

	10/100/1000Base-T(x)									
Pin#	1	2	3	4	5	6	7	8		
Signal	Tx+	Tx-	Rx+	-	-	Rx-	-	-		
			10	00Base-T						
Pin#	Pin# 1 2 3 4 5 6 7 8									
Signal	BI_DA+	BI_DA-	BI_DB+	BI_DC+	BI_DC+	BI_DB-	BI_DD+	BI_DD-		

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

# **11 Glossary**

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



# Atop Technologies, Inc.

www.atoponline.com

# TAIWAN HEADQUARTER and INTERNATIONAL SALES:

## ATOP CHINA BRANCH:

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

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