



User Manual

TESS AIRTMS S807

Users Guide

1. Product Overview	4
1.1 Product Specification	5
1.2 LED operation	6
2. Basic configuration	7
2.1 Console Interface	7
2.2 Basic Configuration (PC)	8
2.3 Basic Setting (Controlled AP)	10
2.4 Basic Setting (Standalone AP)	11
2.4.1 Status Info	11
2.4.2 Network Management	19
3. Advanced Configuration	27
3.1 2.4GHz Radio Config	27
3.1.1 Advanced Radio Config	27
3.1.2 WLAN Config	28
3.1.3 WPS Config	29
3.1.4 Wireless Client MGMT	30
3.1.5 Rate Limit	30
3.1.6 WMM Config	31
3.1.7 MAC filtering Config	33
3.1.8 Networking Mode for SSID	34
3.2 5GHz Radio Config	35
3.2.1 Advanced Radio Config	36
3.2.2 WLAN Config	38
3.2.3 WPS Config	38
3.2.4 Wireless Client MGMT	38
3.2.5 Rate Limit	38
3.2.6 WMM Config	38
3.2.7 MAC filtering Config	38
3.2.8 Networking Mode for SSID	38
3.3 6GHz Radio Config	38
3.3.1 Advanced Radio Config	38
3.3.2 WLAN Config	39
3.4 Easy Mesh	42
3.4.1 Step 1 Mode Selection	42
3.4.2 Step 2 WTP Config	43
3.4.3 Step 3 SOS Config	43
3.4.4 Step 4 Network Config	44
3.4.5 Step 5 Advanced Config	44
3.4.6 Step 6 FrontHaul Config	45

3.4.7 Step 7 BackHaul Config	46
3.5 LACP	46
3.6 WTP Config	47
3.7 Ethernet Config	47
3.7.1 Ethernet Port Config	48
3.8 Traffic MGMT	48
3.8.1 Port Forwarding	49
3.8.2 DMZ Config	49
3.9 Stateful Firewall	51
3.10 System MGMT	52
3.10.2 Log Config	53
3.10.3 Account Config	54
3.10.4 image Upgrade	55
3.10.5 initialization	56
3.10.6 Reset system	56
4. Regulatory Compliance	68
4.1 Federal Communications Commission	68
4.2 Innovation, Science and Economic Development Canada	69
5. USA Representative	70

1. Product Overview

The S807 are a high-end dual-band, dual-concurrent Wi-Fi 7 WIPS that supports 1 spatial streams in triple bands, the 5GHz, 2.4GHz and 6GHz band, channel bandwidths up to 160MHz, and 1024-QAM modulation. The S807 are designed to deliver high performance access for mobile and IoT devices in environments where device density is high.

With OFDMA and MU-MIMO capabilities, efficiently manages up to 1024 client connections with increased capacity, improved coverage and performance in ultra-high dense environments such as healthcare facilities, universities, conference centers, arenas, and stadiums. Furthermore, multi-gigabit Ethernet ensures the backhaul is not a bottleneck for full use of available Wi-Fi capacity.

The S807 uses 802.11be features to simultaneously serve multiple clients and prioritize different types of traffic, which increases the data rates for both individual applications, devices and the overall network.

The S807 supports WiFi Enhanced Open™ which provides confidentiality for over-the-air communications with OWE (Opportunistic Wireless Encryption) & SAE (Simultaneous Authentication of Equals) in open networks such as coffee shops and restaurants, as well as airports, hotels and sports arenas and Easy Connect™ for IoT connection.



1.1 Product Specification

Item	Specification
Radio	2.4GHz & 5GHz & 6GHz
Spatial stream	2 (1T2R)
WiFi Standard	2.4GHz: 802.11b/g/n/ax/be 5GHz: 802.11a/ac/n/ax/be 6GHz: 802.11ax/be
WAN1(PoE)	10Gbps base-T with POE+
WAN2 or LAN2	-
LAN1	1Gbps base-T auto MDI/MDI-X
USB	1* USB 3.0 Host Port for AUX
Console	RS-232C for management, RJ-45
LED	• Power - Green ON : Power ON - Green ON/OFF(1 sec) : Normal operation - Green Blink: Connecting to MGMT server • WAN (Green ON : Link/Connected) • LAN (Green ON : Link/Connected) • 2.4G (Green ON : Active) • 5G (Green ON : Active) • 6G (Green ON : Active)
Dimensions	235(H) x 235(W) x 45(D)mm
Weight (Device)	1300g
Operating Temp.	0~55℃
Operating RH	5~90%
Rated Power	802.3at/bt PoE or DC12V/4A AC-DC Adaptor (DC-038 Type)
Consumption	30W(Avg.), 40W(Max.)

1.2 LED operation

The S807 model is equipped with six status LEDs (Power, WAN, LAN, 2.4G, 5G, 6G) that allow users to determine the operational status of the access point, such as during boot-up or controller connection. All LEDs are of a single color — green.

LED	Operation	Description
POWER	ON	Power is on and the system is in normal service state
	Blinks (1 sec)	During boot / IP assignment / Attempting to connect to the controller
	Flashing	AP Check in progress
WAN	ON	Port connected (1G, 2.5G, or 5Gbps Link)
	OFF	Port not connected
LAN	ON	PC connected (10/100/1000Mbps Link)
	OFF	Port not connected
2.4G	ON	2GHz wireless is active
	OFF	2GHz wireless is inactive
5G	ON	5GHz wireless is active
	OFF	5GHz wireless is inactive
6G	ON	6GHz wireless is active
	OFF	6GHz wireless is inactive

2. Basic configuration

2.1 Console Interface

The pin arrangement of S807 console port is as follows.

9pin EIA-232(console)		Connects to		RJ-45(DVW-602/604)	
Pin	Signal		Pin		Signal
1	NC(Not Connected)		1		NC(Not Connected)
2	TXD		2		NC
3	RXD		3		TXD
4	NC		4		NC
5	GND		5		GND
6	NC		6		RXD
7	NC		7		NC
8	NC		8		NC
9	NC				

[Pin out of a console port]

After connecting a console cable, you can initially set up basic configurations such as IP and Voice. These are detail properties of a console connection.

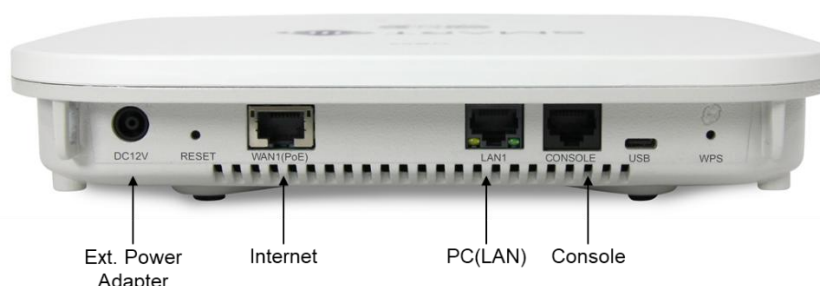
```
> Baud Rate           : 115200
> Byte Size           : 8
> Parity               : None
> Stop Bits           : 1
> Hardware Flow Control : None
> Software Flow Control : None
> RS485 Mode          : Off
```

※ Note : The console port of AP won't give you the prompt for security when you connect to it. You have to enter the specific password for getting the prompt. So it will be used for debugging only.

2.2 Basic Configuration (PC)

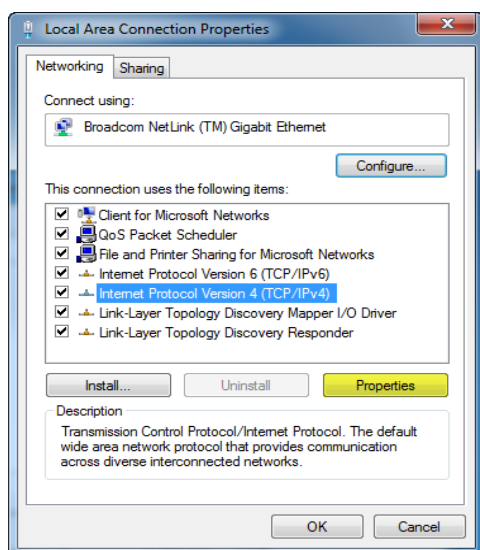
The basic configuration of the PC must be completed before installing and setting up the wireless AP. Since the wireless AP operates in NAT mode by default, the PC will be assigned a private IP address when connected to the LAN port, allowing access to the AP's web interface via HTTP using its private IP address.

As shown in the diagram below, connect the PC to the LAN port on the back of the wireless AP.

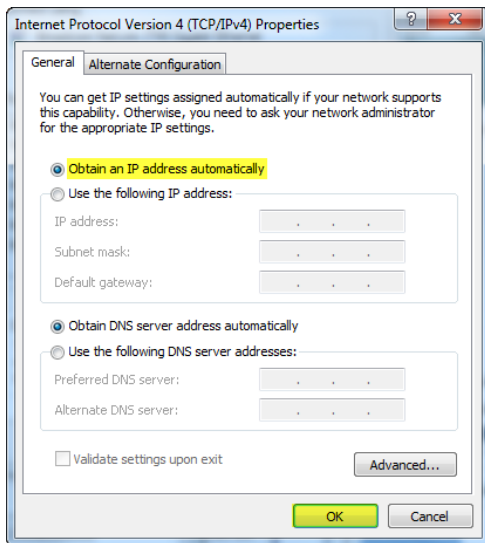


- 1) The network settings of the connected PC can be configured as shown below. The instructions are based on Windows 10

In Windows of your PC(notebook), go to Start -> Control Panel and press Network Connection. Once the Network Connection window is displayed, double-click Local Area Connection and press Attributes in the Local Area Connection State window



- 1) As shown in the figure on the right, select Internet Protocol (TCP/IP) and press Attributes.



As shown in the figure on the left, select “obtain an IP address automatically”.

Once the above process is complete, the PC(notebook) will be assigned a private IP address of 192.168.1.2~254 range.

2.3 Basic Setting (Controlled AP)

Before installing the controlled wireless AP, you must first complete basic settings, such as setting the IP address.

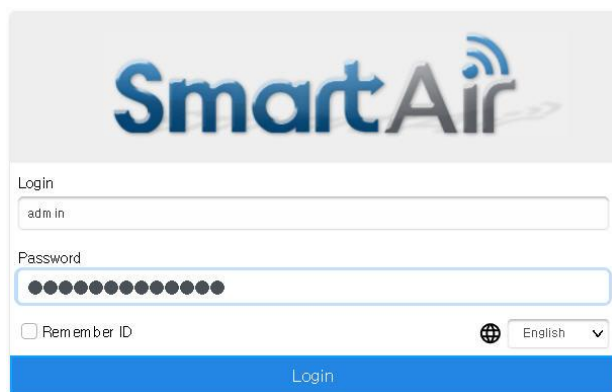
As shown in the figure below, connect your PC(notebook) with the LAN port on the backside of the Wireless AP.

- 1) Start the web browser and enter `http://192.168.1.1:88/login` into the address field.



- ※ **Note :** The wireless AP can operate in NAT or Bridge Mode for wireless interfaces. In NAT mode, a wireless client will be received the IP address from DHCP server of AP. In bridge mode, a wireless client will be received it from the DHCP server of network and AP will pass through all DHCP messages. However, this corresponds to the wireless side and the LAN port is fixed with 192.168.1.1.

The user password is set to “**tr2-ovePlwr?=uwo**” by default. Enter the password and press the login button.



- ※ **Caution:** Continuous use of basic passwords can pose a security risk. Change your passwords frequently and manage them carefully
- ※ **Caution:** If you initializes AP(factory default), the operation mode of AP will be changed to the controlled mode.

- 2) Once you have access, the Wireless AP status window is displayed.

Status Info

System Info

Wired/Wireless Info

Client Info

Log Info

System Info

Model/Manufacturer	DVW-604X/Davolink
S/W Version	7.0.2
Date/Time	May 6 15:08:00 2020
Running Time	0 Day(s) 0 Hour(s) 1 Minute(s) 33 Second(s) Elapsed
Memory Usage	31%
CPU Usage	5Sec:3% / 1Min:0% / 10Min:0%
MAC address	00:03:7F:BA:DB:AD

Firmware Image

Bank selection

Bank0 Bank1

3) In WTP Setting, enter the AP controller IP address and AP name.

WTP Config

WTP Config

Operation Mode	☒ Controlled ☐ Standalone
AP Name	DAVOLINK-00:03:7f:ba:db:ad
IP Address of Controller	172.17.122.139
CAPWAP State	Run

Apply

※ Note : The setting menu on web UI of AP are different for standalone and controlled type.

※ Note : On CAPWAP state, “Run” indicates that the AP has been normally registered into controller. You must complete other settings on the controller.

2.4 Basic Setting (Standalone AP)

2.4.1 Status Info

After successful log-in, the status information of AP like system, firmware, IP address of WAN and LAN port will be shown.

1) System Info

Status Info▲

▪ System Info

▪ AP Scan

▪ Wired/Wireless Info

▪ Client Info

▪ Log Info

System Info

Model/Manufacturer	DVW-624X/Davolink
S/W Version	9.1.6
Date/Time	Jan 4 13:32:06 2024
Running Time	0 Day(s) 2 Hour(s) 39 Minute(s) 27 Second(s) Elapsed
Memmory Usage	16%
CPU Usage	5Sec:23% / 1Min:7% / 10Min:6%
MAC address	00:08:52:FD:54:40
Serial Number	DVW624IA20CBL00085

System Info will give you the information about model name, software version, running time after rebooting, memory usage, etc.

Firmware Image

Bank selection	Bank0 Bank1
bank0	ImageVersion : 9.0.30 ImageBuildTime : 2023-02-13 16:43:01
bank1	ImageVersion : 9.0.36 ImageBuildTime : 2023-06-13 16:09:37

Apply

The AP have two different firmware version in separated two area(bank) of flash memory. You can choose the bank you want.

WAN Configuration Info

Interface	WAN
IP Allocation	DHCP
IP Address	172.17.111.65
Subnet Mask	255.255.254.0
Default. GW	172.17.111.254
1st DNS	168.126.63.1
2nd DNS	168.126.63.2

The IP address which is configured or assigned will be displayed.

2) Wired/Wireless Info

- System Info
- [Wired/Wireless Info](#)
- Client Info
- Log Info
- AP Scan

Wired State Info

Operation State				Configuration State			
Port	Link	Speed	Duplex	Auto Nego.	Speed	Duplex	Pause
LAN	O	1G	Full	Enable	-	-	Disable
WAN1	O	1G	Full	Enable	-	-	Disable
WAN2	-	-	-	Enable	-	-	Disable

Wired State Info shows the current link state and speed of ethernet interfaces.

Wireless State Info

SSID Name	SSID State	Authentication	Wireless Protocol
smartair_5G_0	Enable	WPA-PSK	11a/n/ac/ax
smartair_5G_1	Disable	WPA-PSK	11a/n/ac/ax
smartair_5G_2	Disable	WPA-PSK	11a/n/ac/ax
smartair_5G_3	Disable	WPA-PSK	11a/n/ac/ax
smartair_5G_4	Disable	WPA-PSK	11a/n/ac/ax
smartair_5G_5	Disable	WPA-PSK	11a/n/ac/ax
smartair_5G_6	Disable	WPA-PSK	11a/n/ac/ax
smartair_5G_7	Disable	WPA-PSK	11a/n/ac/ax
smartair_5G_8	Disable	WPA-PSK	11a/n/ac/ax
smartair_5G_9	Disable	WPA-PSK	11a/n/ac/ax
smartair_5G_10	Disable	WPA-PSK	11a/n/ac/ax
smartair_5G_11	Disable	WPA-PSK	11a/n/ac/ax
smartair_5G_12	Disable	WPA-PSK	11a/n/ac/ax
smartair_5G_13	Disable	WPA-PSK	11a/n/ac/ax
smartair_5G_14	Disable	WPA-PSK	11a/n/ac/ax
smartair_5G_15	Disable	WPA-PSK	11a/n/ac/ax

smartair_2G_0	Enable	WPA-PSK	11b/g/n/ax
smartair_2G_1	Disable	WPA-PSK	11b/g/n/ax
smartair_2G_2	Disable	WPA-PSK	11b/g/n/ax
smartair_2G_3	Disable	WPA-PSK	11b/g/n/ax
smartair_2G_4	Disable	WPA-PSK	11b/g/n/ax
smartair_2G_5	Disable	WPA-PSK	11b/g/n/ax
smartair_2G_6	Disable	WPA-PSK	11b/g/n/ax
smartair_2G_7	Disable	WPA-PSK	11b/g/n/ax
smartair_2G_8	Disable	WPA-PSK	11b/g/n/ax
smartair_2G_9	Disable	WPA-PSK	11b/g/n/ax
smartair_2G_10	Disable	WPA-PSK	11b/g/n/ax
smartair_2G_11	Disable	WPA-PSK	11b/g/n/ax
smartair_2G_12	Disable	WPA-PSK	11b/g/n/ax
smartair_2G_13	Disable	WPA-PSK	11b/g/n/ax
smartair_2G_14	Disable	WPA-PSK	11b/g/n/ax
smartair_2G_15	Disable	WPA-PSK	11b/g/n/ax

smartair_6G_0	Enable	OWE	11axa
smartair_6G_1	Enable	WPA-PSK	11axa
smartair_6G_2	Disable	WPA-PSK	11axa
smartair_6G_3	Disable	OWE	11axa
smartair_6G_4	Disable	OWE	11axa
smartair_6G_5	Disable	OWE	11axa
smartair_6G_6	Disable	OWE	11axa
smartair_6G_7	Disable	OWE	11axa
smartair_6G_8	Disable	OWE	11axa
smartair_6G_9	Disable	OWE	11axa
smartair_6G_10	Disable	OWE	11axa
smartair_6G_11	Disable	OWE	11axa
smartair_6G_12	Disable	OWE	11axa
smartair_6G_13	Disable	OWE	11axa
smartair_6G_14	Disable	OWE	11axa
smartair_6G_15	Disable	OWE	11axa

Wireless State Info shows 16 SSID names per frequency, the status of activation, and the authentication mode set.

3) Client Info

The information of clients on Ethernet or wireless interface will be displayed.

- System Info
- Wired/Wireless Info
- [Client Info](#)
- Log Info
- AP Scan

Wired Client Info

MAC Address	IP Address	Port Info	Ping Test	Result
0e:a9:0f:87:b8:0a	192.168.1.183	Smartair_5G_davolink	PING	
00:0e:c6:8e:71:0d	192.168.1.248	LAN1	PING	

Wireless Client Info

SSID Name	MAC Address	Channel	RSSI	Rate	Tx packets	Tx Bytes	Rx packets	Rx Bytes	Elapsed Time	MU Stream	MU Group ID
Smartair_5G_davolink	0e:a9:0f:87:b8:0a	157	-36	1201	134	27947	179	28103	0h 0m 6s	0	0

[Refresh](#)

4) Log Info

- System Info
- Wired/Wireless Info
- Client Info
- [Log Info](#)
- AP Scan

The logs will be stored in volatile memory (DRAM) firstly, and then stored in non-volatile memory (NAND flash). These logs can be downloaded to your local computer.

It shows the SSID name, channel number used, signal strength, BSSID, and radio mode that are searched by detecting other Wi-Fi signals around the AP. It shows the 2.4 GHz and 5 GHz frequency bands separately as shown in the following figure.

Note : NBSS(Number of BSS networks)

2.4GHz AP Scan						
Channel	Wlan Name	Signalstrength	Channel Load	BSSID	Mode	NBSS
6		-24	99	06:08:52:fd:63:d0	11AXG_HE20	11
1	smartair_2G_0	-25	99	06:29:d5:4b:5b:00	11AXG_HE20	17
6	U+Net0894_5G	-25	99	06:08:52:fd:63:e2	11AXG_HE20	11
11		-27	94	06:29:d5:73:42:90	11AXG_HE20	15
7	Bob_FD6328	-27	88	06:08:52:fd:63:28	11AXG_HE20	6
1	U+Net0814	-27	99	14:4d:67:ee:08:16	11AXG_HE20	17

5GHz AP Scan						
Channel	Wlan Name	Signalstrength	Channel Load	BSSID	Mode	NBSS
157		-28	16	0a:08:52:fd:63:2c	11AXA_HE80	18
157	Bob_FD6328	-29	16	0a:08:52:fd:63:28	11AXA_HE80	18
157	U+Net0894_5G	-31	16	0a:08:52:fd:63:e2	11AXA_HE80	18
157		-32	16	0a:08:52:fd:63:3c	11AXA_HE80	18
157	Bob_FD6338	-32	16	0a:08:52:fd:63:38	11AXA_HE80	18
157		-34	16	1a:4d:67:ee:08:97	11AXA_HE80	18

6GHz AP Scan						
Channel	Wlan Name	Signalstrength	Channel Load	BSSID	Mode	NBSS
53		-36	3	0e:08:52:fd:62:20	11AXA_HE160	8
53	Kevin_FD63D0	-36	3	0e:08:52:fd:62:22	11AXA_HE160	8
53		-39	3	0e:08:52:fd:63:d0	11AXA_HE160	8
53	Kevin_FD63D0	-39	3	0e:08:52:fd:63:d2	11AXA_HE160	8
165	DAVO_DVW624_WIFI0_6G	-46	1	0e:29:d5:5e:86:f0	11AXA_HE80	1
53		-75	3	0e:29:d5:73:3f:a0	11AXA_HE160	8
85		-75	1	0e:29:d5:73:ea:c0	11AXA_HE160	4
53	hu chao 5a	-75	3	0e:29:d5:73:3f:a0	11AXA_HE160	8

Search

2.4.2 Network Management

Network Management

- Network Config
- Multi Nat Config
- Internet Connection Config
- Airtime Fairness Config
- LAN IP & DHCP Config
- Smart Power Config
- VLAN Config

In this page, you can configure the IP address, operation mode, VLAN mode for Ethernet interface like WAN and LAN.

1) Network Config

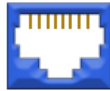
Network Config

Networking Mode
NAT

Save

For three Ethernet interfaces, the default config is NAT mode. As shown below, WAN1 port is for uplink and PoE, WAN2 port is also for uplink, LAN port is for PC.

NAT



WAN1



LAN

The combination for S807 as below can be configured.

Configuration mode	WAN1(PoE)	WAN2	LAN
NAT	WAN(PoE)	WAN	LAN
Bridge	WAN(PoE)	WAN	WAN
NAT(WAN1, LAN2)	WAN(PoE)	LAN	LAN
NAT(LACP)	WAN(PoE)	WAN(LACP)	LAN
NAT(PoE)	PoE Only	WAN	LAN
NAT(Failover)	WAN(PoE)	WAN	LAN
Bridge(LACP)	WAN(PoE)	WAN(LACP)	WAN
Bridge(PoE)	PoE Only	WAN	WAN

※ LACP : Link Aggregation Control Protocol.

※ NAT(Failover) : When WAN1 port is disconnected from internet, for uplink connection, AP will failover to WAN2 port.

2) Internet Connection Config

You can configure IP address allocation mode and DNS server address of the uplink port which connect to internet.

- Network Config
- Internet Connection Config
- LAN IP & DHCP Config
- VLAN Config
- Multi Nat Config
- Airtime Fairness Config
- Smart Power Config

Internet Connection Config

IP Config	☒ DHCP ☐ Static IP
DNS Config	☒ Auto ☐ Manual

Save

The following screen shows IP address information allocated or configured.

Assigned IP Info

IP Address	172.17.111.72		
Subnet Mask	255.255.254.0	1st DNS	168.126.63.1
Gateway	172.17.111.254	2nd DNS	168.126.63.2

3) LAN IP & DHCP Config

Network Config

Multi Nat Config

Internet Connection Config

Airtime Fairness Config

LAN IP & DHCP Config

Smart Power Config

VLAN Config

LAN IP & DHCP Config

IP Address	192 . 168 . 1 . 1
Subnet Mask	255 . 255 . 255 . 0
DHCP Server	☒ Enable ☐ Disable
DHCP IP 사용범위	192 . 168 . 1 . 2 ~ 192 . 168 . 1 . 254 Range) x.x.1.1 ~ x.x.1.254
Leased Time	3600 (sec)

Save

The LAN IP address is set to 192.168.1.1 by default. it is changeable, and the DHCP server function is also set to "Active" by default.

IPv6 Passthrough Config

☐ Enable ☒ Disable

Save

If you use the IPv6 feature behind NAT, you can enable the pass-through option.

4) VLAN Config

- Network Config
- Internet Connection Config
- LAN IP & DHCP Config
- [VLAN Config](#)
- Multi Nat Config
- Airtime Fairness Config
- Smart Power Config

You can set the VLAN on WAN(Uplink) network side. If you select "Active" for the VLAN mode, you can set the VLAN ID and priority.

VLAN Config

VLAN Operation ☒ Enable ☐ Disable

WAN VLAN ID

WAN VLAN Priority ▼

Save

5) Multi Nat config

- Network Config
- Internet Connection Config
- LAN IP & DHCP Config
- [VLAN Config](#)
- [Multi Nat Config](#)
- Airtime Fairness Config
- Smart Power Config

Multi Nat Config

Multi Nat	-- None -- ▼		
Name	multinat		
IP Address	192 168 3 1	IP Check	
Subnet Mask	255 255 255 0		
DHCP Action	☒ Enable ☐ Disable		
Start IP Address	192 168 3 2		
End IP Address	192 168 3 253		
Gateway	192 168 3 1		
Dns Server1	168 126 63 1		
Dns Server2	168 126 63 2		
Leased Time	3600 (sec)		

Add

Multi NAT is the function to configure and allocate the additional multiple range for the IP addresses by adding an IP address range assign to the wired or wireless clients which are connected.

When you configure multiple SSIDs, you can choose “multinat1” on “2.4GHz Radio Config->Networking Mode for SSID” or “5GHz Radio Config->Networking Mode for SSID” menu for multi NAT feature to assign addresses in different IP address range to each SSID.

Networking Mode for SSID

VAP	SSID Name	Mode	Vlan Tag ID	Vlan Priority	Multi Nat
vap10	smartair_5G_Wifi7_Davolink	NAT	0	0	multinat1
vap11	smartair_5G_1	NAT	0	0	LAN
vap12	smartair_5G_2	NAT	0	0	LAN
vap13	smartair_5G_3	NAT	0	0	LAN
vap14	smartair_5G_4	NAT	0	0	LAN
vap15	smartair_5G_5	NAT	0	0	LAN
vap16	smartair_5G_6	NAT	0	0	LAN
vap17	smartair_5G_7	NAT	0	0	LAN
vap18	smartair_5G_8	NAT	0	0	LAN
vap19	smartair_5G_9	NAT	0	0	LAN
vap110	smartair_5G_10	NAT	0	0	LAN
vap111	smartair_5G_11	NAT	0	0	LAN
vap112	smartair_5G_12	NAT	0	0	LAN
vap113	smartair_5G_13	NAT	0	0	LAN
vap114	smartair_5G_14	NAT	0	0	LAN
vap115	smartair_5G_15	NAT	0	0	LAN

Save

6) Airtime Fairness Config

- Network Config
- Internet Connection Config
- LAN IP & DHCP Config
- VLAN Config
- Multi Nat Config
- **Airtime Fairness Config**
- Smart Power Config

Airtime Fairness function is a function that gives all associated wireless clients an opportunity to occupy radio resources evenly because a specific client may monopolize radio resources when multiple wireless clients are connected and traffic is loaded at the same time. However, the transmission opportunity is given with an algorithm to provide the maximum performance of the entire wireless client in consideration of the difference in performance of the wireless client itself, the connected wireless mode, and the strength of the wireless signal. Airtime fairness function is activated to allocate equal transmission resources to connected wireless clients. In addition, strict queues can be used to provide fixed speed and performance to wireless clients.

Airtime Fairness

Airtime Fairness	☒ Enable ☐ Disable
Strict Queue	☐ Enable ☒ Disable

Save

Airtime Fairness MAC Config

MAC Address	11:22:33:44:55:66 ☐ Select for current associated clients,Ex) 11:22:33:44:55:66	
Airtime Percentage	50 (0 ~ 100%)	

Selection	MAC Address	Percentage (0~100%)
☐	11:22:33:44:55:66	50%

AddDelete

Airtime fairness function can provide the wireless resource to the selected client by configuring specific client as above.

7) Smart Power Config

Network Config
 Internet Connection Config
 LAN IP & DHCP Config
 VLAN Config

Multi Nat Config
 Airtime Fairness Config
 Smart Power Config

Smart Power function provides the ability to detect ambient interference signals at each operation cycle for each radio frequency and automatically increase or decrease the transmission output power.

Smart Power Config

Radio	5G 
Mode	☐ Enable ☒ Disable
Check Interval	1800 60 ~ 86400
Tx Auto Mode	☒ Enable ☐ Disable
RSSI	Low : -65 Mid : -75 High : -99 
OBSS	Low : 80 Mid : 50 High : 0 

Save

3. Advanced Configuration

3.1 2.4GHz Radio Config

2.4GHz Radio Config ▲

3.1.1 Advanced Radio Config

■ Advanced Radio Config

■ WLAN Config

■ WPS Config

■ Wireless Client MGMT

■ Rate Limit

■ WMM Config

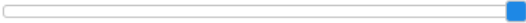
■ MAC filtering Config

■ Networking Mode for SSID

Current Channel/Bandwidth1/20MHz

It shows the Channel number and frequency bandwidth currently in service as above. The channel bandwidth in the 2.4 GHz frequency band is 20 MHz by default due to heavy interference. Using a 40 MHz channel bandwidth can result in performance degradation by severe interference.

Advanced Radio Config

Wireless Action	☒ Enable ☐ Disable
Wireless protocol	☐ b ☐ g ☐ n ☐ ax ☐ b/g/n/ax ☐ b/g/n ☐ g/n/ax ☐ g/n ☐ n/ax ☐ b/g ☒ b/g/n/ax/be
Channel Bandwidth	☒ 20MHz ☐ 40MHz
SideBand	☒ Upper ☐ Lower
Channel Selection Mode	☐ Auto ☒ Auto(Select) ☐ Manual
Preferred Channels	☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☒ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☒ 11 ☐ 12 ☐ 13
Tx Power	23 dbm 
Tx Rate	auto ▼
Beacon Interval	100 ms
Preamble	☐ Short ☒ Long
Guard Interval	☒ Short ☐ Long
AMPDU	☒ Enable ☐ Disable
Fragmentation Threshold	2346 (range : 256~2546)
DTIM	3 (range : 1~255)
LDPC	☒ Enable ☐ Disable
TxBF	☐ Enable ☒ Disable
DL MU-MIMO	☐ Enable ☒ Disable
UL MU-MIMO	☐ Enable ☒ Disable
DL OFDMA	☐ Enable ☒ Disable
UL OFDMA	☐ Enable ☒ Disable
TWT	☐ Enable ☒ Disable
256QAM	☒ Enable ☐ Disable
Channel Width Management	☐ Enable ☒ Disable

Save

3.1.2 WLAN Config

- Advanced Radio Config
- WLAN Config
- WPS Config
- Wireless Client MGMT
- Rate Limit
- WMM Config
- MAC filtering Config
- Networking Mode for SSID

You can configure SSID name, authentication method, encryption mode, password, etc. WPA3 authentication method is supported and if WPA is selected, it means using 802.1X or WPA Enterprise method, so the RADIUS server-related settings menu will be displayed.

WLAN Config

VAP Mode	vap00 (smartair_2G_Wifi7_Davolink)		
WLAN	☒ Enable ☐ Disable		
Enabled SSID	smartair_2G_Wifi7_Davolink	☐ Hide SSID	
Password		☐ Show password Password must be at least 10 characters and not more than 63 characters.	
Password Format	☒ passphrase ☐ hex		
Broadcast Key Update	0 sec	☐ Use	
MLO Config	☐ Enable ☒ Disable		
Authentication	☐ None ☐ WEP ☐ WPA ☒ WPA-PSK		
WPA Mode	☐ WPA ☐ WPA2 ☒ WPA&WPA2 ☐ WPA3 ☐ WPA2&WPA3		
Encryption Type	☐ TKIP ☐ AES ☒ TKIP&AES		
STA Auth	☐ Enable ☒ Disable		
STA Auth Type	☒ External		
Max Station	512	1 ~ 512	
Block device communication in wireless LAN	☐ Enable ☒ Disable		
Block device communication between wireless LAN	☐ Enable ☒ Disable		
Block device access managemet WEB from wireless LAN	☐ Enable ☒ Disable		

Save

If you select WPA-PSK for authentication and WPA2&WPA3 for WPA mode as in the above figure, you only need to enter the password. Encryption algorithms support AES.

3.1.3 WPS Config

▪ Advanced Radio Config

▪ Rate Limit

▪ WLAN Config

▪ WMM Config

▪ WPS Config

▪ MAC filtering Config

▪ Wireless Client MGMT

▪ Networking Mode for SSID

Wi-Fi Protected Setup (WPS) is designed to provide easy connectivity for general users who are not familiar with wireless access and wireless security, and many recent APs do not support it due to security vulnerabilities, but only older versions of Android support it for smartphones.

If you connect your smartphone using the WPS method, you must first check whether your smartphone supports the WPS method.

Caution : If you press the "Reset to Unconfigured" button in the figure below, the authentication method for the SSID regardless of pre-configuration will be changed to PSK and the password will also be changed to the default value.

WPS Config

WLAN Selection	☐ None ☐ WLAN <button>Save</button>
WPS State	Unconfigured <button>Reset to Unconfigured</button>
PBC Button	Start PBC

Current Key Info		
Authentication	Encryption	Key
-	-	-

3.1.4 Wireless Client MGMT

- Advanced Radio Config
- WLAN Config
- WPS Config
- Wireless Client MGMT
- Rate Limit
- WMM Config
- MAC filtering Config
- Networking Mode for SSID

It shows the wireless clients connected at 2.4 GHz frequency. You can also be forced to disconnect from the radio by selecting a specific client from the displayed clients and pressing the "Cancel" button.

Wireless Client MGMT									
Wlan Name	Access ID	MAC Address	IP Address	Authentication	Tx bytes	Rx bytes	Elapsed time	Access Control	
smartair_2G_Davolink	--	B2:45:21:58:03:4F(ch:1)	192.168.1.119	WPA-PSK	183308	90510	0h 9m 55s	Cancel	

3.1.5 Rate Limit

- Advanced Radio Config
- WLAN Config
- WPS Config
- Wireless Client MGMT
- [Rate Limit](#)
- WMM Config
- MAC filtering Config
- Networking Mode for SSID

You can set the speed limit for upload/download for a specific client or SSID.

Rate Limit Config

SSID Name	smartair_2G_Wifi7_Davolink ▼ Refresh
Rate limit Type	☐ Disable ☒ Per Client ☐ Per SSID
Download limit	10000 kbps
Upload limit	10000 kbps
MAC Address	11:22:33:44:55:66
Description	

Selection	MAC List	Description
☐	11:22:33:44:55:66	

Delete

Add

Save

You can also add or delete MAC addresses for setting per-client speed limits.

3.1.6 WMM Config

- Advanced Radio Config
- WLAN Config
- WPS Config
- Wireless Client MGMT
- Rate Limit
- [WMM Config](#)
- MAC filtering Config
- Networking Mode for SSID

It is possible to set up WMM related items as below. However, unless it is a special case, please maintain the default value.

WMM				
단말	AC_BE	AC_BK	AC_VI	AC_VO
CWmin (0~15)	4	4	3	2
CWmax (0~15)	10	10	4	3
AIFS (0~15)	3	7	2	1
TxopLimit (0~8192)	0	0	3008	1504

CWmin(Minimum contention window size) : The initial upper limit of the length of the CW. The AC will wait for a random time between 0 and CWMin before attempting to transmit. Higher priority AC with higher priority is assigned a shorter CWMin.

CWmax(Maximum contention window size) : The upper limit of the CW. If a collision occurs, the AC doubles the size of the CW, up to the CWMax, and attempts to transmit again. The CWMax must be larger than the CWMin.

ECWmin(Exponent form of CWmin) specifies the minimum backoff time, and ECWmax(Exponent form of CWmax) specifies the maximum backoff time. Together, they determine the average backoff time. Large ECWmin and ECWmax values mean a long average backoff time for the STA and a low STA priority.

AIFS number : Arbitration Interframe Spacing Number. The DIFS(Distributed Inter-Frame Space) has a fixed value. WMM provides different DIFS values for different AC(access categories)s. A large AIFSN value means that the STA must wait for a long time and has a low priority.

TxopLimit : Transmission Opportunity Limit (TXOPLimit). After preempting a channel, the STA can occupy the channel within the period of TXOPLimit. A large TXOPLimit value means that the STA can occupy the channel for a long time. If the TXOPLimit value is 0, the STA can only send one data frame every time it preempts a channel.

Qos Category

Category	AC_BE	AC_BK	AC_VI	AC_VO
Category 0	☒	☐	☐	☐
Category 1	☐	☒	☐	☐
Category 2	☐	☒	☐	☐
Category 3	☒	☐	☐	☐
Category 4	☐	☐	☒	☐
Category 5	☐	☐	☒	☐
Category 6	☐	☐	☐	☒
Category 7	☐	☐	☐	☒

Save

3.1.7 MAC filtering Config

- Advanced Radio Config
- WLAN Config
- WPS Config
- Wireless Client MGMT
- Rate Limit
- WMM Config
- **MAC filtering Config**
- Networking Mode for SSID

Select the SSID for wireless MAC filtering first, then either blacklist or whitelist. If Blacklist is selected, wireless terminals with all configured MAC addresses will be denied access. In addition, if Whitelist is selected, only wireless terminals with configured MAC addresses will be allowed access.

MAC filtering Selection

VAP	SSID Name	Local Mode		
vap00	smartair_2G_Wifi7_Davolink	☒ Disable	☐ Black List	☐ White List
vap01	smartair_2G_1	☒ Disable	☐ Black List	☐ White List
vap02	smartair_2G_2	☒ Disable	☐ Black List	☐ White List
vap03	smartair_2G_3	☒ Disable	☐ Black List	☐ White List
vap04	smartair_2G_4	☒ Disable	☐ Black List	☐ White List
vap05	smartair_2G_5	☒ Disable	☐ Black List	☐ White List
vap06	smartair_2G_6	☒ Disable	☐ Black List	☐ White List
vap07	smartair_2G_7	☒ Disable	☐ Black List	☐ White List
vap08	smartair_2G_8	☒ Disable	☐ Black List	☐ White List
vap09	smartair_2G_9	☒ Disable	☐ Black List	☐ White List
vap010	smartair_2G_10	☒ Disable	☐ Black List	☐ White List
vap011	smartair_2G_11	☒ Disable	☐ Black List	☐ White List
vap012	smartair_2G_12	☒ Disable	☐ Black List	☐ White List
vap013	smartair_2G_13	☒ Disable	☐ Black List	☐ White List
vap014	smartair_2G_14	☒ Disable	☐ Black List	☐ White List
vap015	smartair_2G_15	☒ Disable	☐ Black List	☐ White List

Save

Add or delete the MAC address of the wireless terminal as follows.

MAC filtering Config

Filtering SSID ☒ vap10

Allowed MAC Addr 11:11:22:22:33:33

Selection

MAC List

☐

11:11:22:22:33:33

Delete

Add

Save

3.1.8 Networking Mode for SSID

- Advanced Radio Config
- WLAN Config
- WPS Config
- Wireless Client MGMT
- Rate Limit
- WMM Config
- MAC filtering Config
- [Networking Mode for SSID](#)

For each configured wireless SSID, it can be set to operate in NAT or Bridge or VLAN mode. If it is set to NAT, the wireless client to be connected will be assigned a private IP address from the AP. In Bridge mode, the wireless client which is connected will be assigned an IP address from the DHCP server at the network side.

VAP	SSID Name	Mode	Vlan Tag ID	Vlan Priority	Multi Nat
vap00	smartair_2G_Wifi7_Davolink	NAT ▼	0	0 ▼	LAN ▼
vap01	smartair_2G_1	NAT ▼	0	0 ▼	LAN ▼
vap02	smartair_2G_2	NAT ▼	0	0 ▼	LAN ▼
vap03	smartair_2G_3	NAT ▼	0	0 ▼	LAN ▼
vap04	smartair_2G_4	NAT ▼	0	0 ▼	LAN ▼
vap05	smartair_2G_5	NAT ▼	0	0 ▼	LAN ▼
vap06	smartair_2G_6	NAT ▼	0	0 ▼	LAN ▼
vap07	smartair_2G_7	NAT ▼	0	0 ▼	LAN ▼
vap08	smartair_2G_8	NAT ▼	0	0 ▼	LAN ▼
vap09	smartair_2G_9	NAT ▼	0	0 ▼	LAN ▼
vap010	smartair_2G_10	NAT ▼	0	0 ▼	LAN ▼
vap011	smartair_2G_11	NAT ▼	0	0 ▼	LAN ▼
vap012	smartair_2G_12	NAT ▼	0	0 ▼	LAN ▼
vap013	smartair_2G_13	NAT ▼	0	0 ▼	LAN ▼
vap014	smartair_2G_14	NAT ▼	0	0 ▼	LAN ▼
vap015	smartair_2G_15	NAT ▼	0	0 ▼	LAN ▼

Save

3.2 5GHz Radio Config

5GHz Radio Config

3.2.1 Advanced Radio Config

- [Advanced Radio Config](#)
- WLAN Config
- WPS Config
- Wireless Client MGMT
- Rate Limit
- WMM Config
- MAC filtering Config
- Networking Mode for SSID

It shows the channel number and frequency bandwidth currently in use, the advanced and detailed 5 GHz radio setting options.

Current Channel/Bandwidth	40/80MHz
----------------------------------	----------

TWT (Target Wake Time) is a function that is included in the 802.11ax (Wifi6) standard and introduced, and the wakeup cycle can be adjusted to minimize the battery consumption of the device when accommodating the WiFi IoT devices.

Advanced Radio Config

Wireless Action	☒ Enable ☐ Disable
Wireless protocol	☐ a ☐ n ☐ ac ☐ ax ☐ a/n/ac/ax ☐ a/n/ac ☐ n/ac/ax ☐ n/ac ☐ a/n ☐ ac/ax ☒ a/n/ac/ax/be
Channel Bandwidth	☐ 20MHz ☐ 40MHz ☒ 80MHz ☐ 160MHz
SideBand	☒ Upper ☐ Lower
Channel Selection Mode	☐ Auto ☒ Auto(Select) ☐ Manual
Preferred Channels	☒ 36 ☒ 40 ☒ 44 ☒ 48 ☐ 52 ☐ 56 ☐ 60 ☐ 64 ☐ 100 ☐ 104 ☐ 108 ☐ 112 ☐ 116 ☐ 120 ☐ 124 ☐ 128 ☐ 132 ☐ 136 ☐ 140 ☐ 144 ☒ 149 ☒ 153 ☒ 157 ☒ 161
Tx Power	23 dbm <input type="range"/>
Tx Rate	auto ▼
Beacon Interval	100 ms
Preamble	☐ Short ☒ Long
Guard Interval	☒ Short ☐ Long
AMPDU	☒ Enable ☐ Disable
Fragmentation Threshold	2346 (range : 256~2346)
DTIM	3 (range : 1~255)
LDPC	☒ Enable ☐ Disable
TxBF	☐ Enable ☒ Disable
DL MU-MIMO	☐ Enable ☒ Disable
UL MU-MIMO	☐ Enable ☒ Disable
DL OFDMA	☐ Enable ☒ Disable
UL OFDMA	☐ Enable ☒ Disable
TWT	☐ Enable ☒ Disable
Channel Width Management	☐ Enable ☒ Disable
DFS	☒ Enable ☐ Disable

Save

- 3.2.2 WLAN Config
- 3.2.3 WPS Config
- 3.2.4 Wireless Client MGMT
- 3.2.5 Rate Limit
- 3.2.6 WMM Config
- 3.2.7 MAC filtering Config
- 3.2.8 Networking Mode for SSID

The above items are set in the same way as a previous paragraph, 2.4 GHz Radio Config.

3.3 6GHz Radio Config

6GHz Radio Config

3.3.1 Advanced Radio Config

Advanced Radio Config

WLAN Config

Wireless Client MGMT

Rate Limit

WMM Config

MAC filtering Config

Networking Mode for SSID

It shows the channel number and frequency bandwidth currently in use, the advanced and detailed 6 GHz radio setting options.

Current Channel/Bandwidth

165/80MHz

The default setting for channel selection mode is Auto (Select) and one of the selected channels shown in preferred channels is selected and applied. If you select the manual option, you can set the channel number.

Advanced Radio Config

Wireless Action	☒ Enable ☐ Disable
Wireless protocol	☐ ax ☒ ax/be
Channel Bandwidth	☐ 20MHz ☐ 40MHz ☐ 80MHz ☒ 160MHz ☐ 320MHz
SideBand	☒ Upper ☐ Lower
Channel Selection Mode	☐ Auto ☒ Auto(Select) ☐ Manual
Preferred Channels	☐ 1 ☒ 5 ☐ 9 ☐ 13 ☐ 17 ☒ 21 ☐ 25 ☐ 29 ☐ 33 ☒ 37 ☐ 41 ☐ 45 ☐ 49 ☒ 53 ☐ 57 ☐ 61 ☐ 65 ☒ 69 ☐ 73 ☐ 77 ☐ 81 ☒ 85 ☐ 89 ☐ 93 ☐ 97 ☒ 101 ☐ 105 ☐ 109 ☐ 113 ☒ 117 ☐ 121 ☐ 125 ☐ 129 ☒ 133 ☐ 137 ☐ 141 ☐ 145 ☒ 149 ☐ 153 ☐ 157 ☐ 161 ☒ 165 ☐ 169 ☐ 173 ☐ 177 ☒ 181 ☐ 185 ☐ 189 ☐ 193 ☒ 197 ☐ 201 ☐ 205 ☐ 209 ☒ 213 ☐ 217 ☐ 221
Tx Power	18 dbm 
Tx Rate	auto ▼
Beacon Interval	100 ms
Preamble	☐ Short ☒ Long
Guard Interval	☒ Short ☐ Long
AMPDU	☒ Enable ☐ Disable
Fragmentation Threshold	2346 (range : 256~2346)
DTIM	3 (range : 1~255)
LDPC	☒ Enable ☐ Disable
TxBF	☐ Enable ☒ Disable
DL MU-MIMO	☐ Enable ☒ Disable
UL MU-MIMO	☐ Enable ☒ Disable
DL OFDMA	☐ Enable ☒ Disable
UL OFDMA	☐ Enable ☒ Disable
TWT	☐ Enable ☒ Disable
Channel Width Management	☒ Enable ☐ Disable

Save

3.3.2 WLAN Config

- Advanced Radio Config
- [WLAN Config](#)
- Wireless Client MGMT
- Rate Limit
- WMM Config
- MAC filtering Config
- Networking Mode for SSID

Set SSID name, authentication method, encryption mode, password, etc. WPA3 authentication method is supported and if WPA is selected, it means using 802.1X or WPA Enterprise method, so the RADIUS server-related settings menu will be displayed.

WLAN Config	
VAP Mode	vap20 (smartair_6G_Wifi7_Davolink)
WLAN	☒ Enable ☐ Disable
SSID to be changed	smartair_6G_Wifi7_Davolink ☐ Hide SSID
MLO Config	☐ Enable ☒ Disable
Authentication	☒ None ☐ WPA ☐ WPA-PSK
Mode	☒ OWE
STA Auth	☐ Enable ☒ Disable
STA Auth Type	☒ External
Max Station	512 1 ~ 512
Block device communication in wireless LAN	☐ Enable ☒ Disable
Block device communication between wireless LAN	☐ Enable ☒ Disable
Block device access managemet WEB from wireless LAN	☐ Enable ☒ Disable
Beacon Protection	☐ Enable ☒ Disable

Save

WLAN Config

VAP Mode	vap20 (smartair_6G_Wifi7_Davolink)	
WLAN	☒ Enable ☐ Disable	
SSID to be changed	smartair_6G_Wifi7_Davolink	☐ Hide SSID
Password	••••••••	☐ Show password Password must be at least 10 characters and not more than 63 characters.
Password Format	☒ passphrase	
Broadcast Key Update	0 sec	☐ Use
MLO Config	☐ Enable ☒ Disable	
Authentication	☐ None ☐ WPA ☒ WPA-PSK	
WPA Mode	☒ WPA3	
Encryption Type	☒ AES	
STA Auth	☐ Enable ☒ Disable	
STA Auth Type	☒ External	
Max Station	512	1 ~ 512
Block device communication in wireless LAN	☐ Enable ☒ Disable	
Block device communication between wireless LAN	☐ Enable ☒ Disable	
Block device access managemet WEB from wireless LAN	☐ Enable ☒ Disable	
Beacon Protection	☐ Enable ☒ Disable	

Save

Unlike the 2.4 GHz and 5 GHz settings, the OWE(Opportunistic Wireless Encryption) option is added to the WLAN Config menu for 6 GHz frequency and set to active to enhance security in the open environment. In addition, for 6 GHz frequency, only WPA3 security method will be used regardless of authentication methods (NONE, PSK, 802.1X).

3.3.3 Wireless Client MGMT

3.3.4 Rate Limit

3.3.5 WMM Config

3.3.6 MAC filtering Config

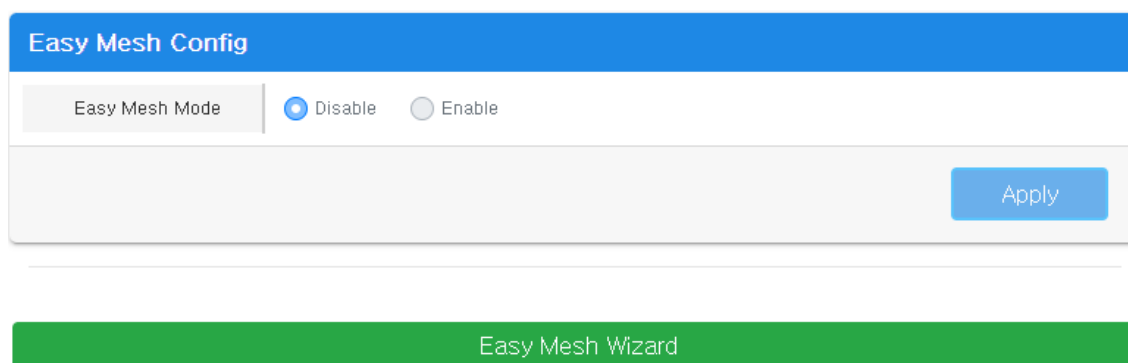
3.3.7 Networking Mode for SSID

The above items are set in the same way as a previous paragraph, 2.4 GHz Radio Config.

3.4 Easy Mesh

Easy Mesh

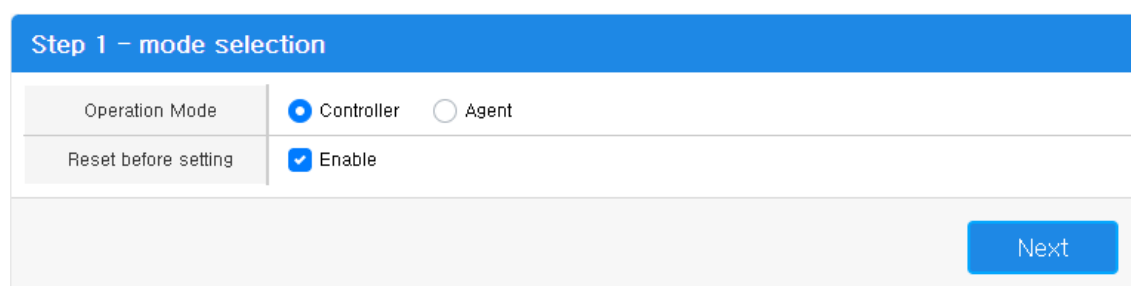
Easy Mesh function allows you to extend your wireless coverage by connecting wireless links without a wired cable connection. This function can be used indoors and outdoors. As shown in the figure below, you cannot basically select active or inactive, and a wizard function is provided to help you set it up step by step.



The image shows two UI elements. The top one is a blue header bar labeled "Easy Mesh Config". Below it is a white box with a tab labeled "Easy Mesh Mode". To the right of the tab are two radio buttons: "Disable" (which is selected) and "Enable". At the bottom right of this box is a blue "Apply" button. Below this is a green button labeled "Easy Mesh Wizard".

3.4.1 Step 1 Mode Selection

Press the "Easy Mesh Wizard" button in the figure above to display the Step 1 setup window below.



The image shows a window titled "Step 1 - mode selection". It has a blue header bar. Below the header is a white box with two sections. The first section is labeled "Operation Mode" and has two radio buttons: "Controller" (selected) and "Agent". The second section is labeled "Reset before setting" and has a checked checkbox next to the word "Enable". At the bottom right of the window is a blue "Next" button.

You can select "Controller" or "Agent" in Step 1. The controller must be the AP to which the wired Ethernet is connected among the APs that make up the mesh network. The remaining APs that need to be connected to the controller or other agents wirelessly are selected and configured as agents.

Note : "Reset before setting" option must be enabled. If set through Easy Mesh wizard, SSID, authentication method, password, etc. will be reset, which may cause problems due to previous settings.

3.4.2 Step 2 WTP Config

Step 2 WTP Config sets AP mode. S807/602i can be configured for Easy Mesh network regardless of controlled AP or standalone AP. However, if AP is controlled mode, Easy Mesh network setting must be done by controller, so if controller is selected in Step 1, only standalone can be selected in Step 2-WTP Config. Also, if Agent is selected in Step 1, both Controlled mode and Standalone mode can be selected and set in Step 2-WTP Config.

Step 2 – WTP Config

Operation Mode	☐ Controlled ☒ Standalone
AP Name	SmartAir_Mesh_controller

[Previous](#) [Next](#)

3.4.3 Step 3 SOS Config

Step 3 – SOS Config

SOS Config	☐ Disable ☐ 2GHz ☐ 5GHz ☒ 2.4GHz + 5GHz
SSID Name	SmartAir_Mesh_controller_SOS ☐ Hide SSID
Authentication	☐ None ☐ WEP ☒ WPA-PSK
WPA Mode	☐ WPA ☐ WPA2 ☐ WPA&WPA2 ☐ WPA3 ☒ WPA2&WPA3
Encryption Type	☒ AES
Password Format	☒ passphrase ☐ hex
Password	•••••••• ☐ Show password The password must be at least 10 characters long.
SOS TimeOut	300 (180 ~ 65535)
Mode	☐ Always ☒ In case of WAN link disconnection

[Previous](#) [Next](#)

Step 3 SOS Config sets up the SOS function. The SOS function allows wireless connection to the SOS SSID when a wired connection is not possible to the AP. After accessing/logging in the management screen, you can check the status of the AP service and change the configuration. You can select and set when the SOS SSID is activated in two ways: WAN link disconnection or always as shown above.

3.4.4 Step 4 Network Config

Step 4 – Network Config

Networking Mode	Bridge
Wireless Protocol	Bridge
VLAN Trunk	☒ Enable ☐ Disable
WAN VLAN	☒ Enable ☐ Disable
WAN VLAN ID	100
WAN VLAN Priority	0
IP Config	☒ DHCP ☐ Static IP
DNS Config	☒ Auto ☐ Manual

Pervious

Next

Step 4 sets the network operation mode for wired ports and wireless links. Typically, set to bridge.

VLAN Trunk : Provides VLAN Trunk functionality when an AP WAN port is connected to a trunk port on an Ethernet switch. It forwards a number of VLAN information and packets delivered from a VLAN Trunk port on an Ethernet switch to the other side over a wireless link.

WAN VLAN : Set when the AP WAN port is connected to an access port that uses VLAN tagging on the Ethernet switch.

3.4.5 Step 5 Advanced Config

Step 5 – Advanced Config

Allow ieee1905 over ethernet	☐ Enable
LACP forward	☐ Enable

Pervious

Next

Step 5 sets up detailed options.

The "Allowieee1905 over ethernet" option handles mesh connection packets from the wired port when enabled.

The "LACP forward" option, when enabled, allows the LACP function to be supported for two radio links, such as wired LACP functionality.

Note : The LACP forward function is restricted to use by both connected switches; it is recommended to maintain the disable function for the two options.

3.4.6 Step 6 FrontHaul Config

Step 6 – FrontHaul Config

Selection	SSID	Key	Authentication	Encryption Type
☒	vap10/vap00 Smartair_5G_davolink	123456789a	WPA2&WPA3-PSK ▼	AES ▼
☐	vap11/vap01 smartair_5G_1	123456789a	WPA&WPA2-PSK ▼	TKIP&AES ▼
☐	vap12/vap02 smartair_5G_2	123456789a	WPA&WPA2-PSK ▼	TKIP&AES ▼
☐	vap13/vap03 smartair_5G_3	123456789a	WPA&WPA2-PSK ▼	TKIP&AES ▼
☐	vap14/vap04 smartair_5G_4	123456789a	WPA&WPA2-PSK ▼	TKIP&AES ▼
☐	vap15/vap05 smartair_5G_5	123456789a	WPA&WPA2-PSK ▼	TKIP&AES ▼
☐	vap16/vap06 smartair_5G_6	123456789a	WPA&WPA2-PSK ▼	TKIP&AES ▼
☐	vap17/vap07 smartair_5G_7	123456789a	WPA&WPA2-PSK ▼	TKIP&AES ▼
☐	vap18/vap08 smartair_5G_8	123456789a	WPA&WPA2-PSK ▼	TKIP&AES ▼
☐	vap19/vap09 smartair_5G_9	123456789a	WPA&WPA2-PSK ▼	TKIP&AES ▼
☐	vap110/vap010 smartair_5G_10	123456789a	WPA&WPA2-PSK ▼	TKIP&AES ▼
☐	vap111/vap011 smartair_5G_11	123456789a	WPA&WPA2-PSK ▼	TKIP&AES ▼

Previous
Next

Step 6 In FrontHaul Config, select the SSID for the Front Haul service and set the SSID name. You can also enter a key (password) to set the PSK method for wireless access.

3.4.7 Step 7 BackHaul Config

Step 7 – BackHaul Config

SSID	Key	Encryption
vap112/vap012 smartair_5G_mesh_backhaul	123456789a	WPA3-PSK AES

Previous

Apply

Select the SSID for the Front Haul service and press the "Next" button to display the 7-Step Back Haul settings. When the setup is complete, press the "Apply" button to apply the setup.

After pressing the "Apply" button, the Easy Mesh Mode displays the "Enable" status and the operation mode.

Easy Mesh Config

Easy Mesh Mode ☐ Disable ☒ Enable (Controller)

Apply

WPS Button

When the wireless mesh link is established, the agent APs and wireless clients are displayed as shown below.

EasyMesh AP & Station Info

This AP is no connected AP & Stations.

Refresh

3.5 LACP

LACP

Note : The LACP menu is intended to implement and set up wired LACP capabilities over two wireless links by connecting four APs (2 Controllers and 2 Agents) to the same Ethernet switch on both sides. It is not commonly used as a feature for application in special cases.

LACP Config

LACP Mode

☒ Disable ☐ Enable ☐ Debug Mode

Apply

3.6 WTP Config

WTP Config

It can be used as standalone mode and controlled(controller-based) mode, and can be changed when selected and set from the menu below.

WTP Config

Operation Mode

☐ Controlled ☒ Standalone

AP Name

SmartAir

Save

WTP Config

Operation Mode

☒ Controlled ☐ Standalone

Provisioning only

☐ Enable ☒ Disable

AP Name

SmartAir

IP Address of Controller

10.255.255.250

CAPWAP State

Save

3.7 Ethernet Config

Ethernet Config

3.7.1 Ethernet Port Config

Ethernet Port Config

	WAN1	LAN
Port		
Link	0	0
Speed	1G	1G
Duplex	Full	Full
Port Config	Auto nego	Auto nego
Pause Config	Active	Deactive
Pause mode	Receive	None
Prefer	Slave	Slave

Save

It can be set up for each of the three Ethernet ports. It can be set up related to the Pause frame transmission/reception processing function that can affect service during interworking with L2 switch. Ethernet ports can support up to 5 Gbps, so if a Pause frame which is sent from a low-speed (1 Gbps or lower) port is not processed, problems such as slowing down can occur.

Port Reset

LAN	WAN2	WAN1

Reset

You can select and reset each individual port or all ports in the figure above.

3.8 Traffic MGMT

Traffic Management

It provides the following router capabilities.

3.8.1 Port Forwarding

▪ Port Forwarding Config

▪ DMZ Config

▪ Port statistics info

When used in NAT mode, if a PC or server program connected to a LAN port uses a specific UDP/TCP port, it cannot receive packets from the Internet because it uses a private IP address. To resolve the issue, you must use Port Forwarding function to ensure that the service is functional. You must know the port information that a particular program running on your PC or server uses.

Port Forwarding Config

Source IP Address	210.123.245.230		
Source Port	4000	~	5000
External Port	8000	~	9000
Internal IP Address	192.168.1.210		
Internal Port	12000	~	13000
Protocol	TCP ▼		
Description			

Selection	Source IP Address	Source Port	External Port	Internal IP Address	Internal Port	Protocol	Description
☐	210.123.245.230	4000:5000	8000:9000	192.168.1.210	12000:13000	TCP	

Delete

AddSave

3.8.2 DMZ Config

▪ Port Forwarding Config

▪ DMZ Config

▪ Port statistics info

DMZ Config

DMZ Config

☐ Disable
☒ DMZ

DMZ Host IP addr

192.168.1.210

Save

DMZ functionality can be used as if PC or Server system behind NAT is connected to the Internet without the use of the port forwarding function. The default setting is "Disable" and you can enter the IP address of it, if you select "DMZ" button.

Exceptional Port

Exceptional Port

TCP

Selection	Protocol	Port Number
No Entries.		

Delete

Add

After DMZ configuration, you can also set exceptional ports.

3.8.3 Port statistics info

Port Forwarding Config

DMZ Config

Port statistics info

Port statistics info

Port	Rx Bytes	Rx UniPkts	Rx MultiPkts	Rx BroadPkts	Rx Errors	Tx Bytes	Tx UniPkts	Tx MultiPkts	Tx BroadPkts	Tx Errors
LAN1	57941219	405317	11621	5797	0	1672258863	1346191	1176	1372	0
WAN	1956184820	1324007	729234	837325	0	58113385	391342	1568	62	0
WAN2	0	0	0	0	0	0	0	0	0	0

Delete

It shows the statistics for each wired Ethernet port as shown above. Pressing the "Delete" button will initialize the statistics to Zero.

3.9 Stateful Firewall

Stateful firewall ▲

3.9.1 Security Config

• Security Config

▪ Access List Config

It provides stateful firewall functionality. So it provides protection against attacks such as TCP sync, ICMP/SYN flooding, IP spoofing, wireless spoofing, Ping of Death, and TCP port scan, etc.

Security Config

TCP SYN Attack	☒ Enable ☐ Disable
Allowable SYN count	INPUT 1000 /sec
ICMP Flood	☒ Enable ☐ Disable
Allowable ICMP count	EchoRequest 100 /sec
Response of trace route	☐ Enable ☒ Disable
Response of broadcast ping	☐ Enable ☒ Disable
SYN Flooding	☒ Enable ☐ Disable
IP Spoofing	☐ Enable ☒ Disable
Ping of Death	☒ Enable ☐ Disable
TCP Port Scan	☒ Enable ☐ Disable
Wireless ARP Spoofing	☐ Enable ☒ Disable
Blocking Worm virus	☐ Enable ☒ Disable

Save

- ✓ TCP SYN Attack, Allowable SYN count : configure the allowable number of SYN packets per second (default value is 1,000). Drops when exceeded
- ✓ ICMP Flood, Allowable ICMP count : configure the allowable number of ICMP packets per second (default value is 100). Drops when exceeded
- ✓ Trace route : No response when receiving trace route packets (enable)
- ✓ Broadcast ping : No response when receiving Broadcast ping packets (enable)
- ✓ SYN Flooding : Faster recovery of internal resources (such as memory) by reducing timeout for sessions waiting for ACK messages after SYN-ACK transmission

- ✓ IP Spoofing : Detects packets with distorted source IP address and blocks transmission (enable)
- ✓ Ping of Death : No response to ICMP echo request (enable)
- ✓ TCP port scan : No response to port scan (enable)
- ✓ ARP Spoofing : Not allow any MAC address changes due to an attack that changes the MAC address of the Default Gateway IP address to the attacker's MAC address (enable)
- ✓ Blocking Worm Virus : Blocks known worm virus traffic types

Provides defense against each of the above attack types.

3.9.2 Access List Config

Security Config
Access List Config

Access List Config

Source IP Address	~
Source Port	~
Destination IP Address	~
Destination Port	~
Protocol	TCP ▼
Permit / Deny	Permit ▼

Selection	Number	Source IP Address	Source Port	Destination IP Address	Destination Port	Protocol	Permit / Deny
No Entries.							

Delete
Add
Save

By analyzing a specific source/destination IP address and port number for each protocol type, you can allow or block transmitted packets. This function allows you to set up connection ACLs.

3.10 System MGMT

System Management ▲

3.10.1 NTP/Timezone Config

- [NTP/Timezone Config](#)
- Initialization
- IP Detective Config
- Snapshot
- Log Config
- Reset system
- DNS Cache Config
- Account Config
- Remote Access Control
- Smart Tunnel Config
- Image Upgrade
- Iperf Test
- SNMP Config

NTP/Timezone Config

1st NTP Server	time.ktiphone.co.kr
2nd NTP Server	time.kriss.re.kr
Update Interval	720 min
Timezone config	(GMT+09:00)Seoul ▼

Save

You can enter the information of the NTP server to receive the time information. Also, if it is installed overseas, if you set the timezone in your area, it will be applied as the local time.

Synchronization

The latest sync time Dec/05/2023 PM17:45:46

Synchronization

Time synchronization basically takes place by receiving time information from the NTP server every 12 hours. If you press the "Synchronization" button, it immediately requests time information from the NTP server to synchronize time.

3.10.2 Log Config

- NTP/Timezone Config
- [Log Config](#)
- Account Config
- Image Upgrade
- Initialization
- Reset system
- Remote Access Control
- Iperf Test
- IP Detective Config
- DNS Cache Config
- Smart Tunnel Config
- SNMP Config
- Snapshot

Logs that occur during AP operations are stored by default in internal DRAM & flash memory on the AP. In order to collect and manage logs for all APs from the log server, the IP address of the remote log server is set and the logs are sent to the server.

Log Config	
Save to memory	☒ Enable ☐ Disable
Save to Flash	☒ Enable ☐ Disable
Send to Remote Server	☐ Enable ☒ Disable
	IP address of Remote Server
	Logging level 7 (Level : 1 ~ 7)
Logging of admin login	☐ Enable ☒ Disable
Save	

3.10.3 Account Config

▪ NTP/Timezone Config	▪ Log Config	▪ Account Config	▪ Image Upgrade
▪ Initialization	▪ Reset system	▪ Remote Access Control	▪ Iperf Test
▪ IP Detective Config	▪ DNS Cache Config	▪ Smart Tunnel Config	▪ SNMP Config
▪ Snapshot			

Access accounts can be added, and for security purposes, the login password must be set to at least 10 digits by combining alphabets, numbers, and special characters.

Account Config

User ID	
User ID to be changed	
Current password	
New password	 Password must be at least 10 characters in combination of English characters and numbers.
Confirm New password	

[Apply](#) [Cancel](#)

3.10.4 image Upgrade

- NTP/Timezone Config
- Log Config
- Account Config
- **Image Upgrade**
- Initialization
- Reset system
- Remote Access Control
- Iperf Test
- IP Detective Config
- DNS Cache Config
- Smart Tunnel Config
- SNMP Config
- Snapshot

It supports four upgrade methods.

- ① Upgrade by USB : Plug the firmware file into the USB port on the back of the AP in the USB memory where the firmware file is stored, enter the firmware file name on the upgrade screen, and then click the "Upgrade" button to upgrade.
- ② ① Upgrade by TFTP : Run the TFTP server on a PC connected to an external Ethernet and enter the IP address, ID, password and filename on the upgrade screen, then click the "Upgrade" button to upgrade.
- ③ Upgrade by FTP : Run the FTP server on a PC connected to an external Ethernet and enter the IP address and filename on the upgrade screen, then click the "Upgrade" button to upgrade.
- ④ Upgrade in local : You can upgrade by selecting the firmware stored on the PC that you accessed the AP's management screen and pressing the "Upgrade" button.

Image Upgrade

Upgrade by USB	File name		Upgrade
Upgrade by TFTP	Server IP Addr		
	File name		Upgrade
Upgrade by FTP	Server IP Addr		
	ID		
	Password		
	File name		Upgrade
Upgrade in local	File name		Find Upgrade

3.10.5 initialization

- NTP/Timezone Config
- Log Config
- Account Config
- Image Upgrade
- **Initialization**
- Reset system
- Remote Access Control
- Iperf Test
- IP Detective Config
- DNS Cache Config
- Smart Tunnel Config
- SNMP Config
- Snapshot

It can be restored and initialized to factory default settings.

Caution : If it is initialized, it will be changed to controlled mode and the setting will be initialized, so it must be changed to standalone mode and configure again.

Initialization

Initialization (Factory default)	Restore Factory	Reset with network setting
Restore setting	Back Up	Find Restore
System Name		

3.10.6 Reset system

- NTP/Timezone Config
- Log Config
- Account Config
- Image Upgrade
- Initialization
- [Reset system](#)
- Remote Access Control
- Iperf Test
- IP Detective Config
- DNS Cache Config
- Smart Tunnel Config
- SNMP Config
- Snapshot

You can restart the AP manually.

And it provides automatic soft reset function at periodically scheduled times.

Reset system

Reset system

Automatic/periodic reset(This feature does not work while the user is in use)

Periodic Reset

☐ Enable ☒ Disable

Save

3.10.7 Remote Access Control

- NTP/Timezone Config
- Log Config
- Account Config
- Image Upgrade
- Initialization
- Reset system
- [Remote Access Control](#)
- Iperf Test
- IP Detective Config
- DNS Cache Config
- Smart Tunnel Config
- SNMP Config
- Snapshot

You can access and manage the LAN port by connecting it, but for remote management, you must select “enable” and apply for Web server option the remote management item on the screen above. The default web access port is 88 and can be changed.

Remote Access Control	
Web server	☒ Enable ☐ Disable
Server	☒ HTTP ☐ HTTPS
Port	88 ☒ Enable remote access
Save	

For security purposes, ssh server are disabled by default. If “Enable” is selected, the server port and session timeout option are displayed and can be set and changed.

SSH Config	
SSH Server	☒ Enable ☐ Disable
Server Port	6022 (1 ~ 65535) ☒ Enable remote access
Session Timeout	600 (300 ~ 3600)
Save	

3.10.8 iperf Test

▪ NTP/Timezone Config	▪ Log Config	▪ Account Config	▪ Image Upgrade
▪ Initialization	▪ Reset system	▪ Remote Access Control	▪ Iperf Test
▪ IP Detective Config	▪ DNS Cache Config	▪ Smart Tunnel Config	▪ SNMP Config
▪ Snapshot			

This function is provided to first test and determine whether there is an abnormality in the wired network when a wireless client connects to the AP and experiences a slowdown problem. To use this function, first install and run an iperf server such as a PC. After that, you can test the wired network between the iperf client (AP) and the iperf server by entering the command option as follows.

Iperf Test

Iperf command

-c 220.120.246.214

Connecting to host 220.120.246.214, port 5201

[4] local 172.17.111.72 port 48380 connected to 220.120.246.214 port 5201

[ID]	Interval	Transfer	Bandwidth	Retr	Cwnd
-------	----------	----------	-----------	------	------

[4]	0.00-1.00 sec	11.3 MBytes	95.0 Mb/s	0	67.9 KBytes
------	---------------	-------------	-----------	---	-------------

[4]	1.00-2.00 sec	11.1 MBytes	93.5 Mb/s	0	67.9 KBytes
------	---------------	-------------	-----------	---	-------------

[4]	2.00-3.00 sec	11.2 MBytes	94.0 Mb/s	0	67.9 KBytes
------	---------------	-------------	-----------	---	-------------

[4]	3.00-4.00 sec	11.1 MBytes	93.3 Mb/s	0	67.9 KBytes
------	---------------	-------------	-----------	---	-------------

[4]	4.00-5.00 sec	11.3 MBytes	94.8 Mb/s	0	67.9 KBytes
------	---------------	-------------	-----------	---	-------------

[4]	5.00-6.00 sec	11.1 MBytes	93.5 Mb/s	0	67.9 KBytes
------	---------------	-------------	-----------	---	-------------

[4]	6.00-7.00 sec	11.1 MBytes	93.5 Mb/s	0	67.9 KBytes
------	---------------	-------------	-----------	---	-------------

[4]	7.00-8.00 sec	11.3 MBytes	94.8 Mb/s	0	67.9 KBytes
------	---------------	-------------	-----------	---	-------------

[4]	8.00-9.00 sec	11.1 MBytes	93.5 Mb/s	0	67.9 KBytes
------	---------------	-------------	-----------	---	-------------

[4]	9.00-10.00 sec	11.2 MBytes	94.0 Mb/s	0	67.9 KBytes
------	----------------	-------------	-----------	---	-------------

[ID]	Interval	Transfer	Bandwidth	Retr
-------	----------	----------	-----------	------

[4]	0.00-10.00 sec	112 MBytes	94.0 Mb/s	0	sender
------	----------------	------------	-----------	---	--------

[4]	0.00-10.00 sec	112 MBytes	94.0 Mb/s	0	receiver
------	----------------	------------	-----------	---	----------

Cancel

Start

3.10.9 IP Detective Config

- NTP/Timezone Config
- Initialization
- IP Detective Config
- Snapshot
- Log Config
- Reset system
- DNS Cache Config
- Account Config
- Remote Access Control
- Smart Tunnel Config
- Image Upgrade
- Iperf Test
- SNMP Config

This feature is intended to leave a history of access in the log when a wireless client user accesses, pings, etc. to a specific preset IP address.

IP Detective Config

IP Detective Mode

☒ Enable ☐ Disable

Address

Add

ex) 1.1.1.1

Selection	IP List
☐	8.8.8.8
☐	183.111.138.165
☐	23.207.177.231

Delete

Save

When a wireless client user pings or connects to the pre-configured IP address, it is stored in the log as follows. It is saved as a log once on the first attempt and not on the next attempt.

Logs in Flash

Time	Description
5a:d0 0000 _____	set_login_proc()[0352] : ID admin HTTP login successfully from 192.168.1.248 +
5a:d0 0000 _____	ip_detect_msg_print()[0363] : IP_detective: [IP-8.8.8.8,STA-0ea90f87b80a] started! +
8:0a 0000 _____	sm_WPA_PTK_PTKINITDONE_Enter()[3903] : pairwise key handshake completed (RSN) +
8:0a 0000 kern<-hapd	handle_assoc()[5036] : -----> send. assoc resp : resp(0) +
8:0a 0000 kern->hapd	handle_assoc()[4564] : -----> recv. assoc : radio(wifi0) wlanid(0) reassoc(0) rs
8:0a 0000 kern->hapd	wpa_supplicant_event()[2696] : -----> recv. EVENT_HELLO event. rssi(-71) +
8:0a 0000 kern->hapd	handle_auth()[2448] : -----> recv. auth : radio(wifi0) wlanid(0) auth_alg(3) statu
8:0a 0000 kern->hapd	handle_auth()[2448] : -----> recv. auth : radio(wifi0) wlanid(0) auth_alg(3) statu
8:0a 0000 kern->hapd	handle_auth()[2448] : -----> recv. auth : radio(wifi0) wlanid(0) auth_alg(3) statu
5a:d0 0000 _____	set_login_proc()[0352] : ID admin HTTP login successfully from 192.168.1.248 +
5a:d0 0000 _____	set_login_proc()[0352] : ID admin HTTP login successfully from 192.168.1.248 +
5a:d0 0000 _____	set_login_proc()[0352] : ID admin HTTP login successfully from 192.168.1.248 +
5a:d0 0000 _____	set_login_proc()[0352] : ID admin HTTP login successfully from 192.168.1.248 +
5a:d0 0000 _____	received wpa_ie [173 17 111 73] 1 1

[Download](#)

3.10.10 DNS Cache Config

- NTP/Timezone Config
- Initialization
- IP Detective Config
- Snapshot
- Log Config
- Reset system
- **DNS Cache Config**
- Account Config
- Remote Access Control
- Smart Tunnel Config
- Image Upgrade
- Iperf Test
- SNMP Config

This feature is intended to collect the access/visit history of the user/wireless client about which Internet URL the wireless client has accessed/visited. Access/visit URL information can be collected with DNS Query/Response message analysis, and URLs (e.g., com, net, kr, etc.) must be configured.

DNS Cache Config

VAP	vap00 (5g 0) ▼		
DNS Cache Mode	☒ Enable ☐ Disable		
DNS Cache Alive Time	60 sec (60 ~ 3600)		
Rule	Rule Back ▼	URL	Num 2 Add

Act	Rule	URL	Num
	back	com	3
	back	net	3

<< < 1 > >>

Back : Collects and sends only the last 2 digits of the access URL

Filter : Do not collect DNS queries containing configured URLs.

Drop : Blocks DNS queries containing configured URLs

The collected access logs are not stored in the AP's internal storage space and can be sent by setting up a syslog server as shown below.



DNS Cache Log Config

Log Server1	Address	172.17.110.243	Port	514
Log Server2	Address	172.17.110.244	Port	514

Save

3.10.11 Smart Tunnel Config

- NTP/Timezone Config
- Initialization
- IP Detective Config
- Snapshot
- Log Config
- Reset system
- DNS Cache Config
- Account Config
- Remote Access Control
- **Smart Tunnel Config**
- Image Upgrade
- Iperf Test
- SNMP Config

It is a function for remote connection (HTTP, ssh) from a smart tunnel server (Smartair controller) to a wireless AP inside the firewall or using an intranet/private network. Of course, the port used for tunnel connection in the firewall must be open to connect. If a smart tunnel is connected, it will be displayed on the smart tunnel server and access is possible.

SmartTunnel	
SmartTunnel 모드	☒ Enable ☐ Disable
Remote IP	0.0.0.0
Remote Port	1194
AP Name	SmartAir
Save	

3.10.12 SNMP Config

- NTP/Timezone Config
- Initialization
- IP Detective Config
- Snapshot
- Log Config
- Reset system
- DNS Cache Config
- Account Config
- Remote Access Control
- Smart Tunnel Config
- Image Upgrade
- Iperf Test
- [SNMP Config](#)

It supports all SNMP versions, SNMP v1/2/3 and can be set as follows.

To use SNMP v3, you must configure user accounts, authentication algorithms (MD5 or SHA), passwords, and privacy algorithms (DES).



SNMP Config

SNMP	☐ Enable ☒ Disable
SNMP V1	☐ Enable ☒ Disable
SNMP V2	☐ Enable ☒ Disable
SNMP V3	☒ Enable ☐ Disable
User	
Auth Alg	MD5 v
Auth Password	
Private Alg	None v
SNMP Trap	☒ Enable ☐ Disable
Version	V3 v
User	
Auth Alg	None v
Server IP/Domain 1	
Server IP/Domain 2	
Server IP/Domain 3	
ACL Policy	None v
ACL Server	IP : Netmask : Add Delete

Selection

ACL Server

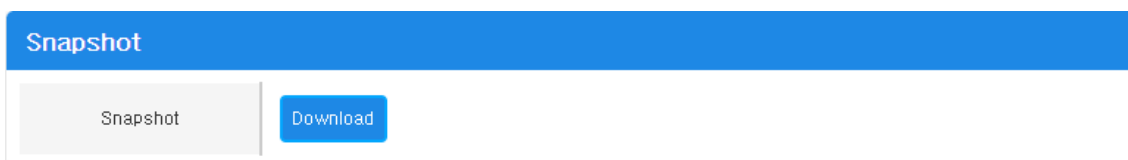
☐ 0.0.0.0/0

Save

3.10.13 Snapshot

- NTP/Timezone Config
- Initialization
- IP Detective Config
- **Snapshot**
- Log Config
- Reset system
- DNS Cache Config
- Account Config
- Remote Access Control
- Smart Tunnel Config
- Image Upgrade
- Iperf Test
- SNMP Config

If you click the "Download" button, you can download it to your connected PC, including all current configuration, current running processes, and logs. The downloaded snapshot file will help you determine the cause of the problem.



The text file is created and downloaded with a file name such as "snapshot_ DVW-624X_000852fd5440_20240104_114055.txt".

DVW-624X: Model name

000852fd5440 : MAC address of AP

20240104 : File creation date

114055 : File creation time

4. Regulatory Compliance

4.1 Federal Communications Commission

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

- FCC regulations restrict the operation of this device to indoor use only.
- The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet.
- Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

4.2 Innovation, Science and Economic Development Canada

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

- (1) This device may not cause interference.
- (2) This device must accept any interference, including interference that may cause undesired operation of the device

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : 1) L'appareil ne doit pas produire de brouillage; 2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

- IC regulations restrict the operation of this device to indoor use only.
- The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet.
- Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Toute modification non expressément approuvée par la partie responsable de la conformité peut annuler le droit d'utilisation de cet équipement. Cet émetteur ne doit pas être installé à proximité d'une autre antenne ou d'un autre émetteur, ni fonctionner conjointement avec ceux-ci.

- La réglementation de la IC limite l'utilisation de cet appareil à un usage intérieur uniquement.

- L'utilisation de cet appareil est interdite sur les plateformes pétrolières, dans les véhicules (voitures, trains, bateaux) et les aéronefs, à l'exception des gros porteurs volant à plus de 3 000 mètres d'altitude.
- L'utilisation d'émetteurs dans la bande 5,925-7,125 GHz est interdite pour le contrôle ou la communication avec des systèmes d'aéronefs sans pilote.

Operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

DFS (Dynamic Frequency Selection) products that operate in the bands 5250- 5350 MHz, 5470-5600MHz, and 5650-5725MHz.

La bande 5150-5250 MHz est réservée uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Les produits utilisant la technique d'atténuation DFS (sélection dynamique des fréquences) sur les bandes 5250- 5350 MHz, 5470-5600MHz et 5650-5725MHz.

5. USA Representative

Firm Name		CN Number	
Street			
City		Contact Name	
State/Province		Job Title	
Post Code		Email	
Country	USA	Telephone	