

HIRSCHMANN IT

A **BELDEN** BRAND

DAP User Manual

User manual
Release 1.24

Technical Support
<http://www.belden.com>

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2025, Belden Singapore Pte Ltd

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Belden according to the best of the company's knowledge. Belden reserves the right to change the contents of this document without prior notice. Belden can give no guarantee in respect of the correctness or accuracy of the information in this document.

Belden can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann IT product site (www.belden.com).

Safety agreement

Safety location

By default, device should be placed in certain location that is safe, stable and reliable; all physical operators should be authorized; the operation CLI scripts should be properly kept, updated and reviewed.

Safety channel

Hirschmann IT devices support multiple managing methods, including SSH, HTTP/HTTPS. All un-encrypted management protocols are not recommended. We highly recommend that our user only use SSH and HTTPs as the way to operate the devices, in order to ensure all management traffic is encrypted.

Safety storage

The login credentials, device configuration and status data should be kept in an appropriate place and be updated regularly and this information can only be accessed and managed by authorized people.

Table of Contents

SAFETY AGREEMENT	3
1 INTRODUCTION	9
1.1 REVISION HISTORY	9
1.2 OVERVIEW	10
1.3 DOCUMENT CONVENTIONS	10
2 INTRODUCTION FOR DAP WORK MODE	12
2.1 CLUSTER MODE	12
2.2 DAC MODE	13
BWO MODE	13
3 CLUSTER DEPLOYMENT SAMPLE	15
3.1 TOPOLOGY	15
3.2 DESCRIPTIONS FOR THE SCENARIO	17
4 SETUP WIZARD	19
4.1 ACCESS DAP CLUSTER VIA WEB BROWSER	19
4.1.1 PREREQUISITES FOR SETTING UP AND ACCESSING DAP CLUSTER	19
4.1.2 THE IP ADDRESS OF DAP	20
4.1.3 ACCESS DAP WEB GUI IN INITIALIZATION STATE	20
4.2 USING THE DAP SETUP WIZARD.....	24
5 DAP CLUSTER WEB GUI	29
5.1 DASHBOARD OVERVIEW	29
5.2 WLAN	30
5.3 AP	31

5.4 CLIENT.....	35
5.5 MONITORING.....	38
5.6 SYSTEM.....	43
5.7 WIRELESS.....	43
5.8 ACCESS.....	44
IOT.....	44
5.9 MORE.....	44
6 WLAN CONFIGURATION	47
6.1 TWO WAYS TO CREATE A NEW WLAN	47
6.2 WLAN TYPE INTRODUCTION	49
6.3 KEY WORDS SPECIFICATION FOR WLAN.....	52
6.4 MODIFY WLAN CONFIGURATION	69
6.5 DELETE YOUR WLAN.....	70
6.6 WMM CONFIGURATION	71
7 DAP MANAGEMENT	72
7.1 CHECK DETAILED INFORMATION.....	73
7.2 MODIFY AP NAME AND LOCATION.....	73
7.3 ADD A NEW AP TO CLUSTER	74
7.4 REMOVE AN AP FROM THE CLUSTER.....	75
7.5 ALLOW AN AP TO JOIN THE CLUSTER.....	77
7.6 REPLACE A CURRENT AP IN CLUSTER	77
7.7 MODIFY IP ADDRESS	78
CONVERT FROM CLUSTER MODE TO DAC/BWO MODE	79

7.8 CHECK CURRENT CONFIGURATION.....	81
7.9 REBOOT DAP.....	81
7.10 CLEAR CONFIGURATION.....	83
7.11 BACKUP AND RESTORE CONFIGURATION.....	84
7.12 UPGRADE AP FIRMWARE.....	84
7.13.1 UPGRADE ALL DAPS.....	85
7.13.2 UPGRADE SINGLE AP.....	88
7.13 LOCATE OR TURN ON/OFF LED.....	89
7.14 AP ADVANCED CONFIGURATION.....	89
7.15 AP WORKS AS GATEWAY.....	104
7.16.1 CONFIGURE DHCP SERVER.....	104
7.16.2 CONFIGURE DNS SERVER.....	105
7.16.3 NAT CONFIGURATION.....	105
8 SYSTEM MANAGEMENT.....	109
8.1 CLUSTER INFO MANAGEMENT.....	109
8.2 MANAGE YOUR ACCOUNTS.....	111
8.2.1 MANAGE YOUR WEB GUI ACCOUNTS.....	111
8.2.2 MANAGE YOUR CLI ACCOUNT.....	112
8.3 CERTIFICATE MANAGEMENT.....	113
8.4 SERVICES MANAGEMENT.....	114
8.5 SYSTEM TIME CONFIGURATION.....	115
8.6 CONFIGURING SYSLOG.....	116
8.7 CONFIGURING SNMP.....	119

8.7.1	CONFIGURING SNMPV2	119
8.7.2	CONFIGURING SNMPV3	120
9	WIRELESS MANAGEMENT.....	121
9.1	RF CONFIGURATION	122
9.1.1	MODIFY AP TRANSMISSION POWER AND CHANNEL	125
9.1.2	CONFIGURE CHANNEL WIDTH TO 160MHZ.....	126
9.1.3	TURN ON/OFF A SPECIFIC AP RADIO.....	127
9.2	WIDS/WIPS	128
9.3	PERFORMANCE OPTIMIZATION	133
10	ACCESS.....	137
10.1	AUTHENTICATION WINDOW	137
10.2	LOGIN CAPTIVE PORTAL	139
10.3	ACCOUNT & ACCESS CODE MANAGEMENT	141
10.4	CUSTOMIZE PORTAL PAGE	144
10.5	CLIENT BLOCKLIST BASED ON WIRELESS ACCESS	145
10.6	CLIENT ALLOWLIST BASED ON CAPTIVE PORTAL	146
10.7	WALLED GARDEN	147
10.8	MULTICAST CONTROL	148
10.9	ACL.....	150
11	IOT.....	152
11.1	ADVERTISE MODE	152
11.1.1	IBEACON	153
11.1.2	EDYUID	154

11.1.3 EDYURL	155
11.2 SCANNER MODE	156
11.3 ADVERTISE & SCANNER MODE.....	158
12 SUPPORT TOOLS	159
12.1 TOOLS	159
12.2 PMD.....	165
13 DEPLOYMENT LARGE SCALE OF DAPS.....	166
14 CONFIGURE AP IF DHCP SERVER UNREACHABLE	167
15 GLOSSARY	168

1 Introduction

1.1 Revision History

Version	Date	Description
1.23	May-2022	
1.24	Dec-2025	

1.2 Overview

The high-performance DAP series featuring enhanced WLAN technology with RF radio dynamic adjustment, distributed control Wi-Fi architecture, secure network admission control with unified access, this making the DAP is ideal for enterprises of all sizes demanding a simple, secure and scalable wireless solution.

Deliver enterprise-grade Wi-Fi to high-density client environments in offices, hospitals, schools, retail stores and warehouses, achieve the highest speeds and best performance for your network services and applications.

This user manual describes all features supported by the DAP under 'CLUSTER' mode and provides instructions and examples for configuration of DAP. It is designed for network administrators who are responsible for configuring and maintaining the Wi-Fi network. It assumes the reader is familiar with Layer2 and Layer3 networks and basic 802.11 protocols and related technologies.

The manual covers an introduction to the DAP and configuration samples. The examples describe the general steps of setting up a Wi-Fi network based on several typical deployment scenarios. It is useful for those new to the DAP configuration and those already familiar with the software wanting to know more about certain functions.

1.3 Document Conventions

The following conventions are used throughout this manual to emphasize important concepts:



Note

It indicates helpful suggestions, pertinent information, and important things to remember.



It indicates a risk of damage to your hardware or loss of data or some incorrect or improper operation that should be avoided.

2 Introduction for DAP Work Mode

2.1 Cluster Mode

DAP can realize self-management function through distributed autonomous networking mode, by default, are running in “cluster mode” which provides simplified plug-and-play deployment. The access point cluster is an autonomous system that consists of DAPs and a virtual manager, the DAPs with the same cluster ID will form a cluster and it will select the Primary Virtual Manager (PVM) and Secondary Virtual Manager (SVM) based on AP model and MAC address.

The cluster will select the DAP which has the highest priority as the PVM and the AP which has the second highest priority as the SVM, in case of DAPs has the same priority, the AP with higher MAC address will select as the PVM. Each cluster has a management IP address that is a virtual IP and will be assigned to the PVM.

When the PVM fails to respond due to an unexpected error or issues (for example, in case of a network issue or PVM had power down due to some unexpected condition), the SVM will automatically upgrade to act as the PVM, this can realize the redundancy on management level and there will be no interruption or service disturbance to member APs or any of the wireless users.

One DAP cluster supports up to 255 DAPs. The access point cluster architecture ensures simplified and quick deployment. Once the first DAP is configured using the configuration wizard, the remaining DAPs in the same layer2 network which has the same “Cluster ID” will come up automatically with an updated configuration. This ensures the whole network is up and functional within a few minutes, by default the “Cluster ID” is 100.

To configure the DAP out-of-box, connect the DAP to the network and powered by POE or power adapter, and ensure the DAP can retrieve an IP address from the network. When the LED on DAP would be in “Green Blinking” state, a SSID named with “mywifi-xx:xx” (xx:xx is the last 2 characters of the DAP MAC address) will be able to detected and connected. After associated with this WLAN SSID, the DAP web

based management page would be able to be reached via below default

URL:<http://find.dragonflyap.com:8080/> or <https://find.dragonflyap.com>. After login with the default account (user: Administrator / Password: admin), the “configuration wizard” would be displayed on web page configuration, user may follow the wizard to configure the DAP.

The PVM/SVM election rules are as following:

- PVM/SVM election priority: DAP640/DAP645/DAP646/DAP647 > DAP620
- Among the DAPs with same priority, the one with highest MAC address will be selected as PVM, the second highest MAC address DAP will be selected as SVM.
- If a higher priority DAP joins an existed DAP cluster, it will take over the PVM role. For example, a DAP640 will become PVM after it joins an existed pure DAP620 cluster, and the previous PVM will change to SVM or member in the DAP cluster.

2.2 DAC Mode

DAP can also working on DAC mode which means DAP can be centrally managed by a management platform to easily deployed on a large network. An Ethernet port with routable connectivity to the DAC or a self-enclosed network is used for deploying a Wireless Network. A DAP can be installed at a single site or deployed across multiple geographically dispersed locations, please refer to DAC User Manual for more detailed information.

BWO Mode

DAP can also working on BWO mode which means DAP can be centrally managed by a management platform to easily deployed on a large network. An Ethernet port with routable connectivity to the BWO or a self-enclosed network is used for deploying a Wireless Network. A DAP can be installed at a single site or deployed across multiple

geographically dispersed locations, please refer to BWO User Manual for more detailed information.

3 Cluster Deployment Sample

This chapter describes a typical wireless network topology of cluster mode and the network units in the scenario includes DAP, switch, router and related servers of applications, which also the configuration sample for this user manual.

3.1 Topology

Following are the brief topology for a typical cluster scenario for your reference, there is no DAC/BWO deployed in this scenario; all DAPs worked on the “Cluster” mode and realize self-management function.

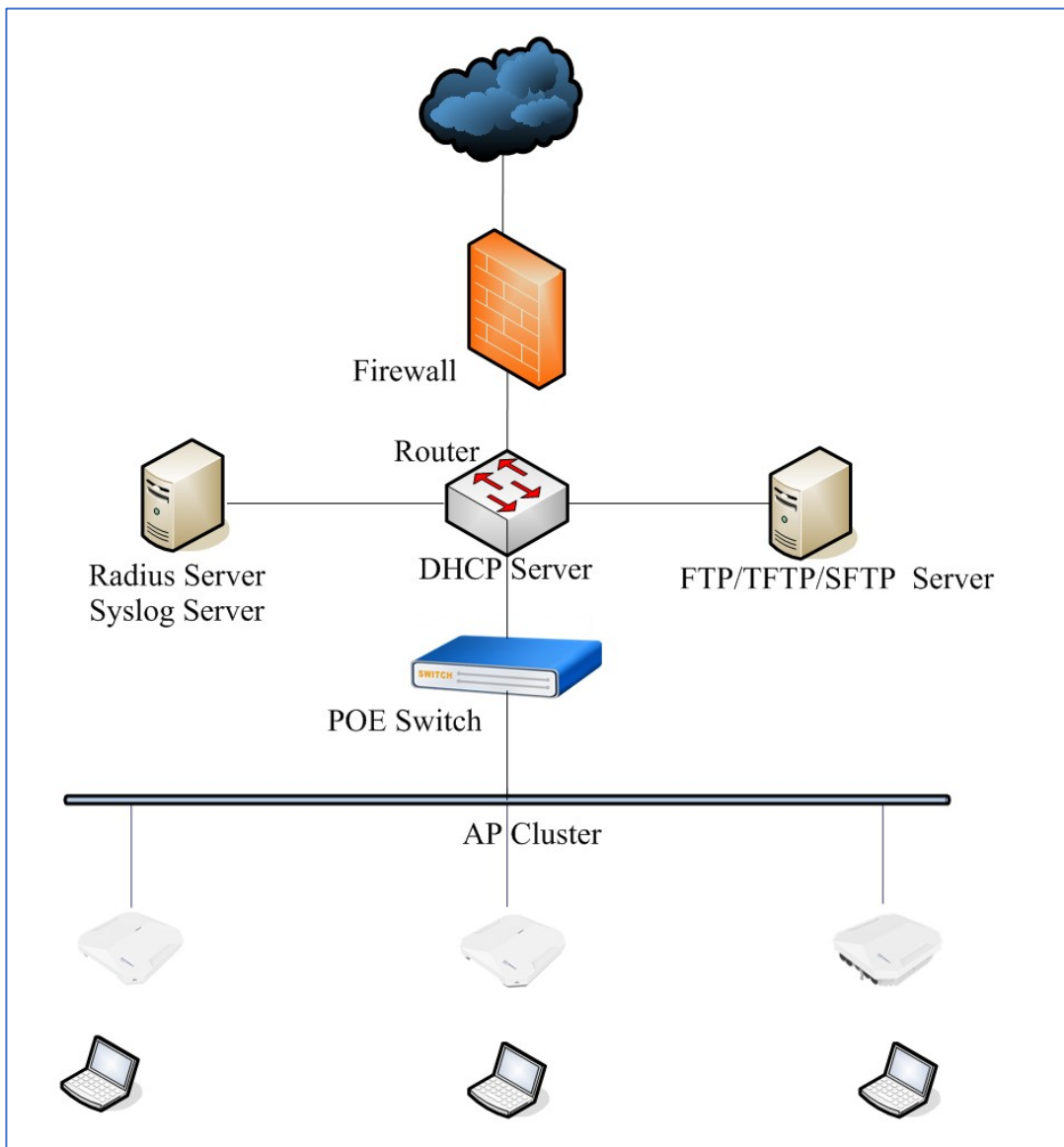


Figure3-1-1 Topology

3.2 Descriptions for the scenario

There are three DAPs in one cluster. All these three DAPs connected to a standard PoE switch and all APs belongs to the same management VLAN, the PoE switch connects to the core router which provides DHCP service to all DAPs and the wireless stations. The PVM in the cluster will be responsible for an internal portal server, configuration synchronizing, AP and client management & monitoring. ALL DAPs usage and client connections are visible in the UI dashboard.

All three APs broadcast three SSIDs:

- My-wifi-test, a SSID with PSK encryption type.
- My-wifi-portal, a SSID with OPEN+Portal authentication.
- My-wifi-1x, a SSID with 802.1x authentication type.

The SSID “My-wifi-test” is designed for a PSK SSID which means a Protected Network for users. Suitable for setting up a Personal network that requires a PSK/Passphrase, this is a typically used for commonplace.

The SSID “My-wifi-portal” is designed for the guests. It uses a captive portal authentication and a portal page will pop up when wireless station browsing any website. Guests can access the network only after inputting the access code or user name and password provided by the network administrator. The popped up page can be customized to follow the customer’s requirement.

The SSID “My-wifi-1x” is used for the company staff, for security, this WLAN will use 802.1x authentication methods, anyone who tries connecting to this WLAN will be requested to input the user name and password registered in an internal RADIUS server.

The related servers also deployed in this scenario:

- **Radius Server:** Used for 802.1x authentication for an Enterprise SSID, it could be a windows Server or other type of Radius server.

- **Syslog Server:** Used as a remote syslog server for receiving syslog generated by DAP which described in Chapter [8.6 Configuring Syslog](#)
- **TFTP Server:** Used for recording the client connection information (Client Behavior Tracking), AP log collection, Post Mortem Dump (PMD) ,DAP firmware upgrading and uploading wireless capture.
- **SFTP Server:** Used for DAP firmware upgrading and recording the client connection information (Client Behavior Tracking).

4 Setup Wizard

Initializing wizard page is loaded by connecting to the pre-defined SSID accessing the URL <http://find.dragonflyap.com:8080/>, in this chapter, it mainly introduces how to access DAP cluster and complete the basic configuration when using DAP according to the wizard for the first time.

4.1 Access DAP cluster via web browser

Each DAP supports up to three simultaneous GUI connections. The GUI is accessible through a standard web browser from a remote management console or workstation. The GUI includes configuration wizards that guide you to change administrator password and complete basic WLAN configuration. In addition to the wizards, the GUI includes a dashboard monitoring feature that provides visibility into your wireless network's performance and usage.

This allows you to easily locate and diagnose WLAN issues. For details on the GUI dashboard, see [5.1 Dashboard Overview](#)

4.1.1 Prerequisites for setting up and accessing DAP cluster

- Connect all DAPs to switch and power up.
- All the DAPs should be in the same subnet and reachable for each one.
- Ensure that a DHCP server is present and accessible in the network. The DAP cluster uses an external DHCP server for IP address management of the access points and the wireless clients.
- Ensure that a DNS server is available in the network, which helps to parse the web URL used to access the DAP.

- It is recommended that your configuring terminal should have a compatible operating system and browser.

Recommended OS	Recommended Browser
Window 10	Google Chrome 132 and later
Window 11	Google Chrome 132 and later
MAC OS Monterey 12.0	

Table4-1-1-1 Recommended OS and Browser



Note

- *The process of connecting to a single DAP through web is same as connecting to DAP cluster.*
- *It is recommended to connect only one DAP at a time to the network and complete the configuration, then plug in other DAPs one by one to synchronize the configurations.*

4.1.2 The IP address of DAP

DAP supports manage its IP address by the following 3 ways :

- DAP will use the IP address 192.168.1.254 by default if there is no DHCP server in the network.
- DAP can be configured a static IP address manually.
- DAP supports obtain an IP address from a DHCP server.

4.1.3 Access DAP web GUI in initialization state

In the default factory state, the DAP will create a pre-defined SSID on 2.4G band to provide wireless access and manage the DAP through the web page. Follow the configuration wizard to complete the initial configuration of the DAP:

- Connect to SSID which named “mywifi-xx:xx” on 2.4G radio (Note: xx:xx is the last 2 characters of the PVM MAC address), shown as Figure4-3-1.

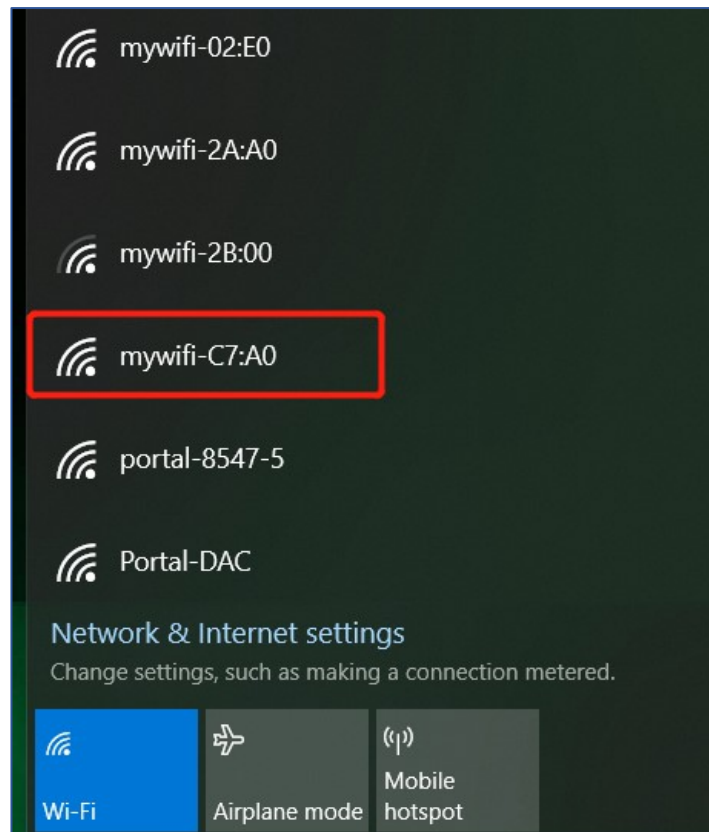


Figure4-1-3-1 Connect to default SSID

- Login to the DAP cluster web management system by http or https using the default password “admin”

For example: http login shown in Figure4-1-3-2 and https login shown in Figure4-1-3-

3

<http://find.dragonflyap.com:8080/>

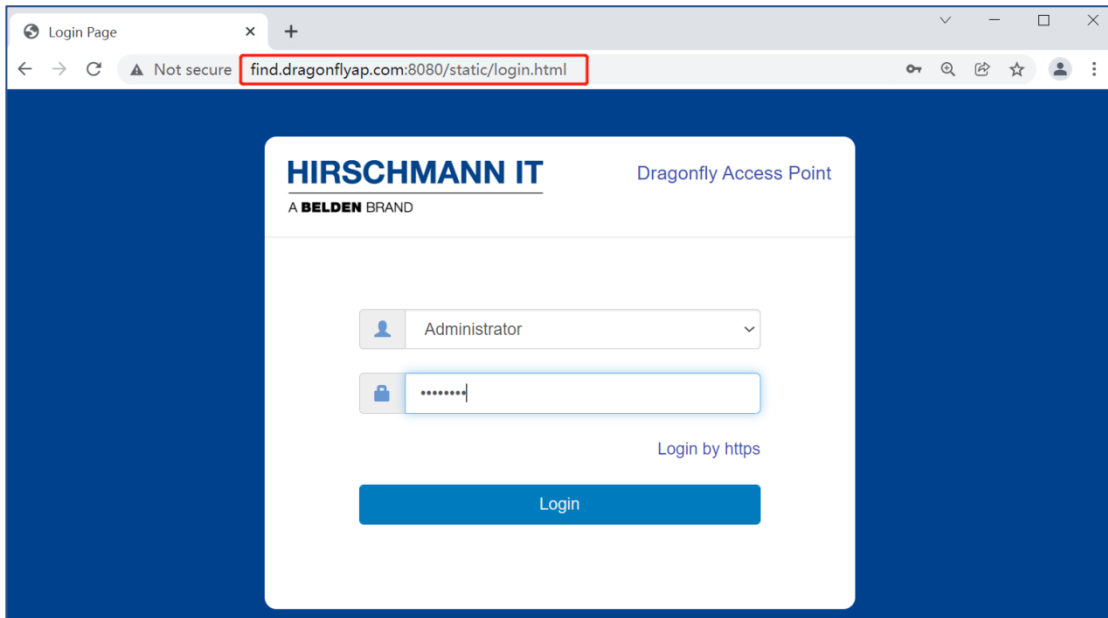


Figure4-1-3-2 Login by http

<https://find.dragonflyap.com>

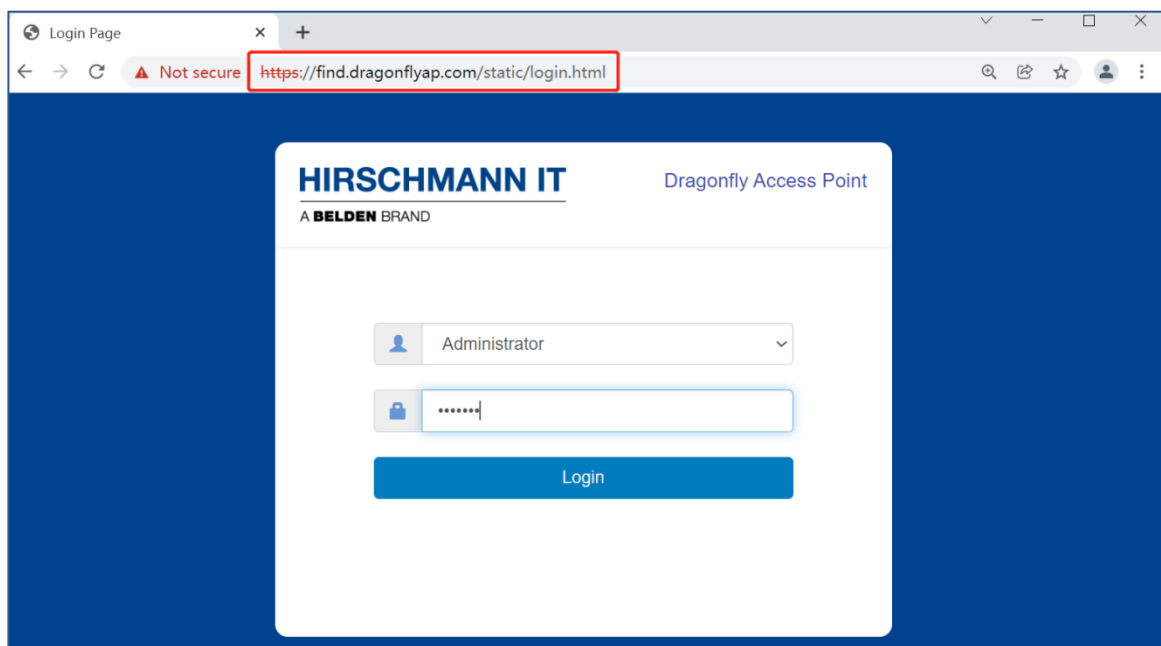


Figure4-1-3-3 Login by https



Note

A digital certificate was required when login by https mode for more secure communication between DAP and the browser. A CA root needs to be downloaded from the DAP and installed into the trust store of the browser used. The certificate installation procedure varies from operating system and browser combinations, you can download the root certificate file from DAP shown as below Figure4-1-3-4:

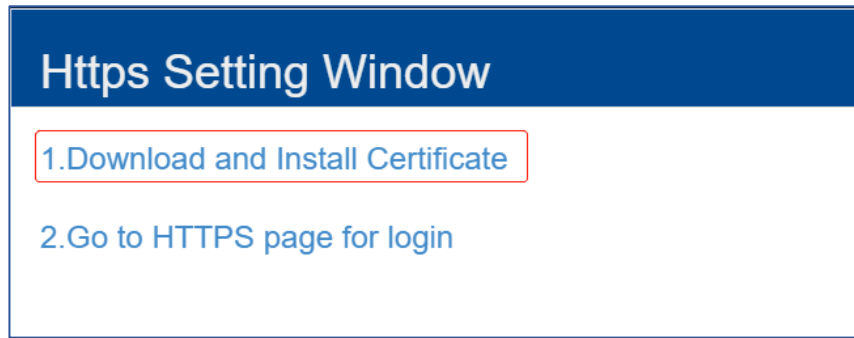


Figure4-1-3-4 Download a Certificate

If there is no DNS server in the network, you can connect to the DAP cluster directly by using the IP address of any DAP in the cluster, for example:

<http://172.16.10.169:8080> (172.16.10.169 was the IP address of DAP)

<https://172.16.10.169> (172.16.10.169 was the IP address of DAP), shown in Figure4-1-3-5

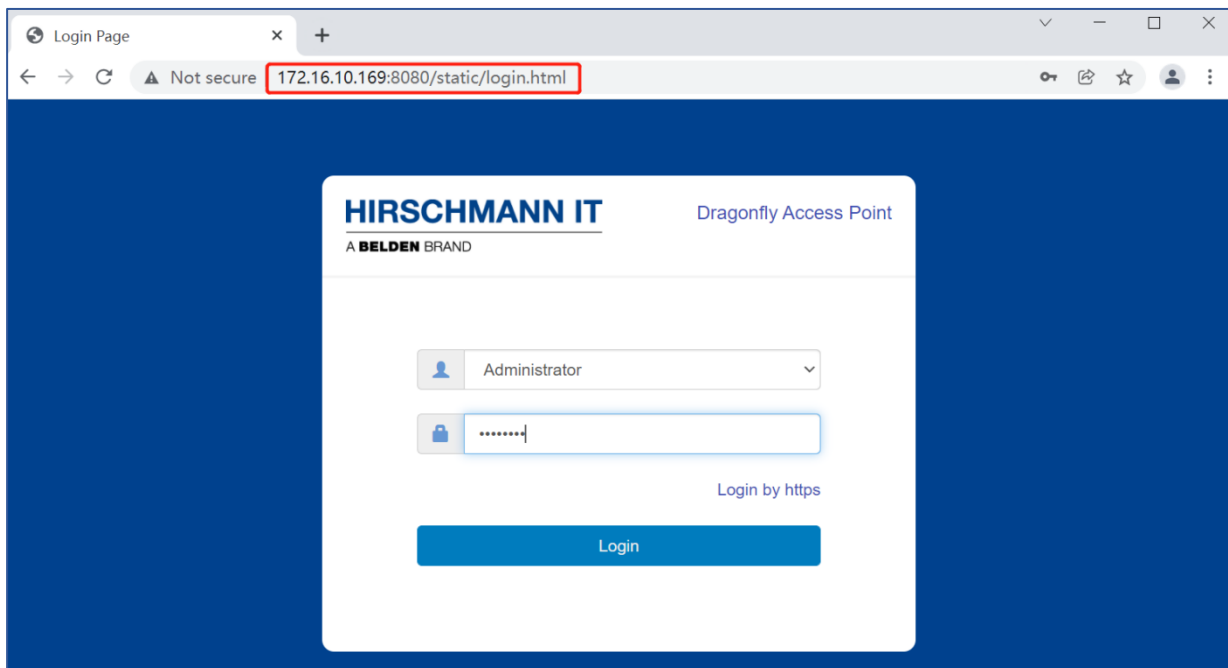


Figure4-1-3-5 Login by using IP address

The IP address of DAP can be seen by using command "ifconfig br-wan" shown in Figure4-1-3-6.

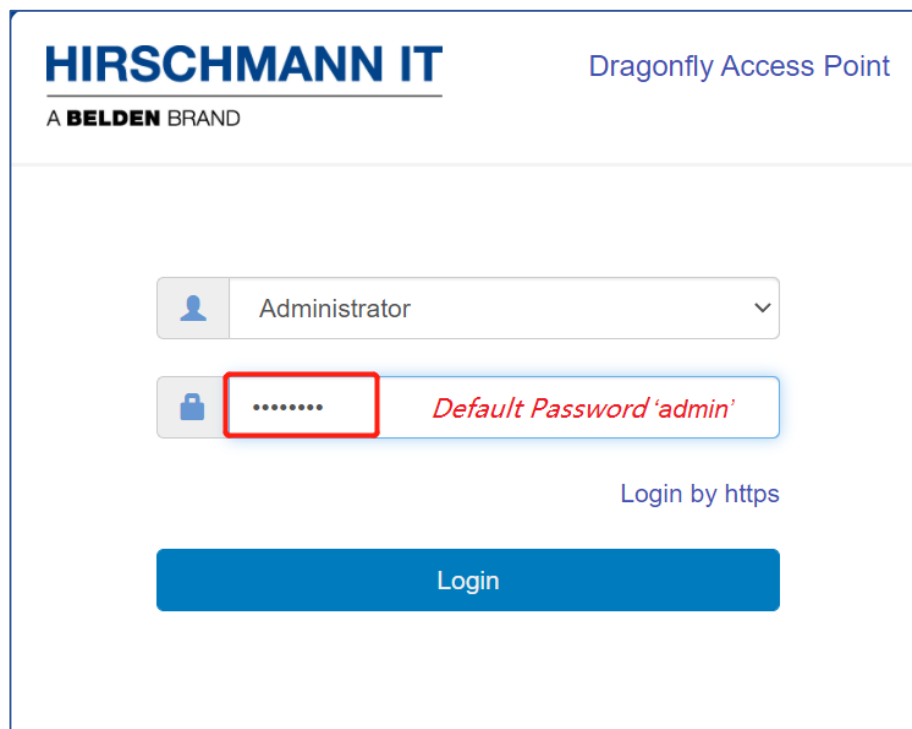
```
support@My-AP:~$ ifconfig br-wan
br-wan  Link encap:Ethernet  HWaddr 94:AE:E3:FF:C0:70
        inet addr:172.16.10.169  Bcast:172.16.10.255  Mask:255.255.255.0
        inet6 addr: fe80::96ae:e3ff:feff:c070/64  Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:48239  errors:0  dropped:0  overruns:0  frame:0
        TX packets:49865  errors:0  dropped:0  overruns:0  carrier:0
        collisions:0  txqueuelen:1000
        RX bytes:6365560 (6.0 MiB)  TX bytes:19186865 (18.2 MiB)

support@My-AP:~$ █
```

Figure4-1-3-6 Check DAP IP address

4.2 Using the DAP setup wizard

Login with the Administrator account and the default password “admin” shown in Figure4-2-1, the Setup Wizard will be loaded to start your configuration; following are the Initialization Wizards:

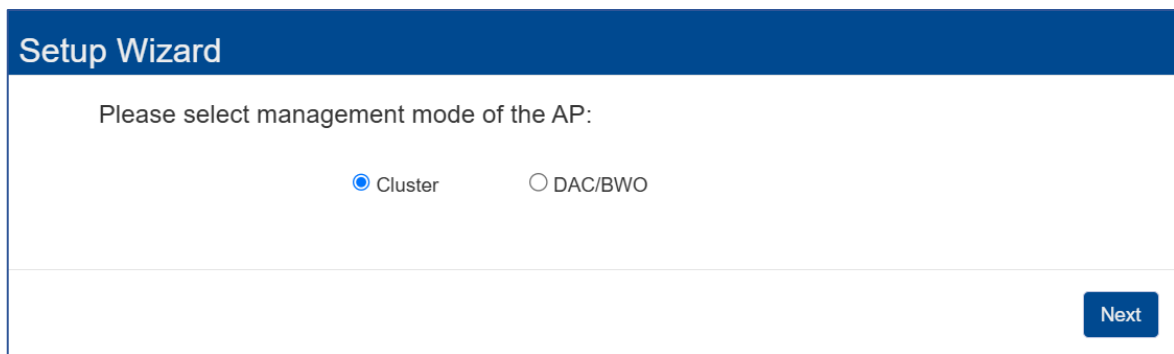


The screenshot displays the login interface for a Hirschmann IT Dragonfly Access Point. At the top left is the Hirschmann IT logo, and at the top right is the text 'Dragonfly Access Point'. Below the logo, it says 'A BELDEN BRAND'. The main area contains a login form with a user selection dropdown set to 'Administrator', a password field with a red box around the masked characters and a red note 'Default Password 'admin'', and a 'Login by https' link. A blue 'Login' button is positioned below the form.

Figure4-2-1 Login with Administrator

- **Select the AP work mode**, there are two work modes for DAP shown as Figure4-2-2:

- **Cluster**—A self-management and autonomous mode, no additional controller are required, a virtual manager will be elected from DAPs which called PVM
- **DAC**—Under this mode, all DAPs will register to a management platform which named DAC (Dragonfly Access Controller), and all the configurations and policies will performed by DAC, Please refer to the **DAC User Manual** for detailed configurations under this mode.
- **BWO**—Under this mode, all DAPs will register to a management platform which named BWO (Belden Wireless Orchestration), and all the configurations and policies will performed by BWO, Please refer to the **BWO User Manual** for detailed configurations under this mode.



The screenshot shows a 'Setup Wizard' window with a blue header. Below the header, the text reads 'Please select management mode of the AP:'. There are two radio button options: 'Cluster' (which is selected, indicated by a blue dot) and 'DAC/BWO' (which is unselected, indicated by a grey dot). At the bottom right of the form, there is a blue button labeled 'Next'.

Figure4-2-2 Select AP work mode

- **Step1/3, Change your administrator password**, please note that the new login password can be set to “admin” which is the default one, shown in Figure4-2-3

Setup Wizard

Step 1/3 Change your administrator password

Password:

Confirm:

[Back](#) [Next](#)

Figure4-2-3 Change your administrator password

- **Step2/3, Choose your Country or Region and Time Zone**, shown in Figure4-2-4

Setup Wizard

Step 2/3 Choose your Country or Region

Country/Region:

Time Zone:

[Back](#) [Next](#)

Figure4-2-4 Choose your Country or Region

- **Step3/3, Create New WLAN**, you can click 6 WLAN Configuration for details, please note that the default SSID named "mywifi-xx:xx" will be deleted automatically when the new SSID created successfully, illustrated in Figure4-2-5.

Setup Wizard

Step 3/3 Create New WLAN

WLAN Name:

Band: 2.4GHz 5GHz

Security Level:

Key Management:

PMF:

Password Format:

Password:

Confirm:

Figure4-2-5 Create New WLAN

- After we finished the Setup Wizard, DAP will reboot automatically and convert to the new work mode named Cluster mode and load the new configurations, a Notice will be popup shown as Figure4-2-6.

Notice

The setup wizard has completed. You can create more WLANs and perform other configurations in main page.

Since you have switched the AP's operating mode, the device is restarting, when the device is restarted, Please connect to the WLAN **My-wifi-test**. and login to the main page with your new administrator password.

Figure4-2-6 popup notice for DAP rebooting

After the DAP reboot, please connect to the new SSID you created and login with the new password and continue the other configurations if needed, after you login the web

GUI, you will see the default SSID had deleted and new SSID displayed in the WLAN window, shown in Figure4-2-7

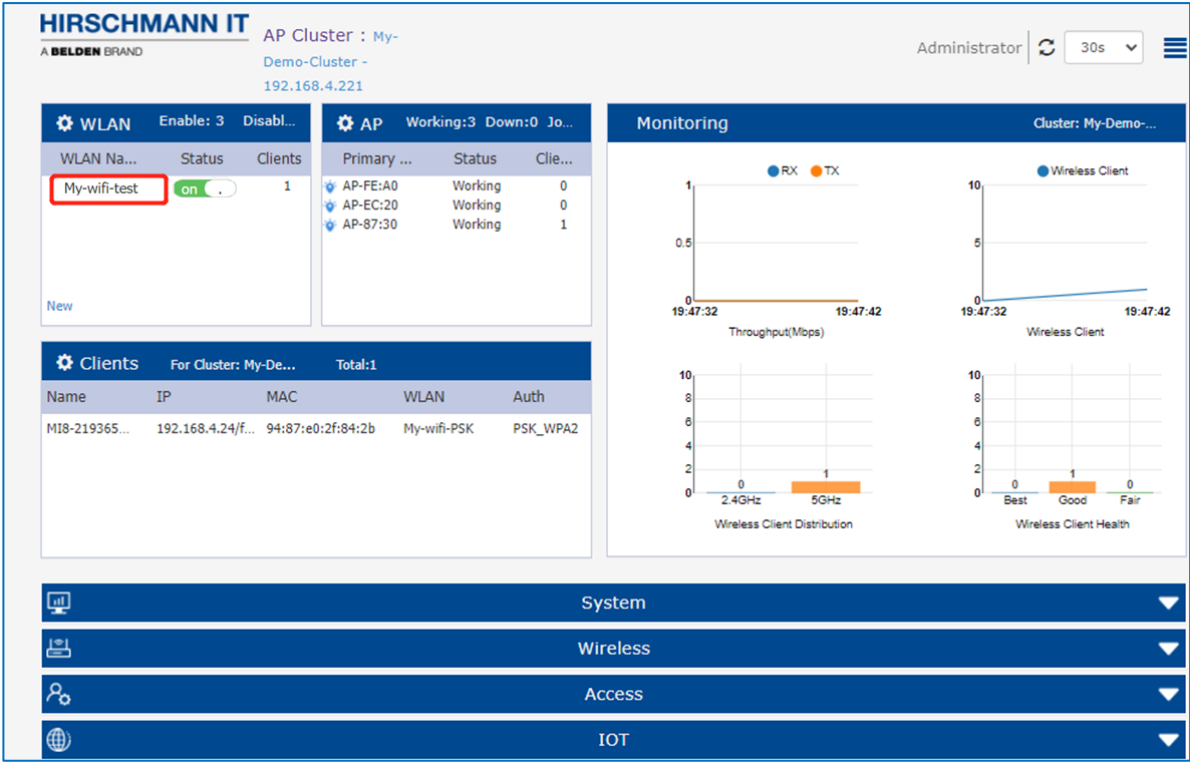


Figure4-2-7 Login the AP Cluster

5 DAP Cluster Web GUI

This chapter has a briefly introduction for the dashboard and each configuration window on DAP Web UI, for more detailed information for separated function, please refer to related chapter accordingly.

5.1 Dashboard overview

The DAP provides a visualized dashboard for DAP and client monitoring and configuration. As illustrated in below screen shot Figure 5-1-1 Dashboard overview, on the top of the window, you can see the cluster information, current logged in user, refresh button ,refresh cycle and “More”, the dashboard is split into sub-windows for **WLAN**, **AP**, **Client** , **Monitoring**, **System**, **Wireless** and **Access**. You can briefly check the WLAN, AP or Clients in the dashboard or click the framework of each window to see the detailed information.

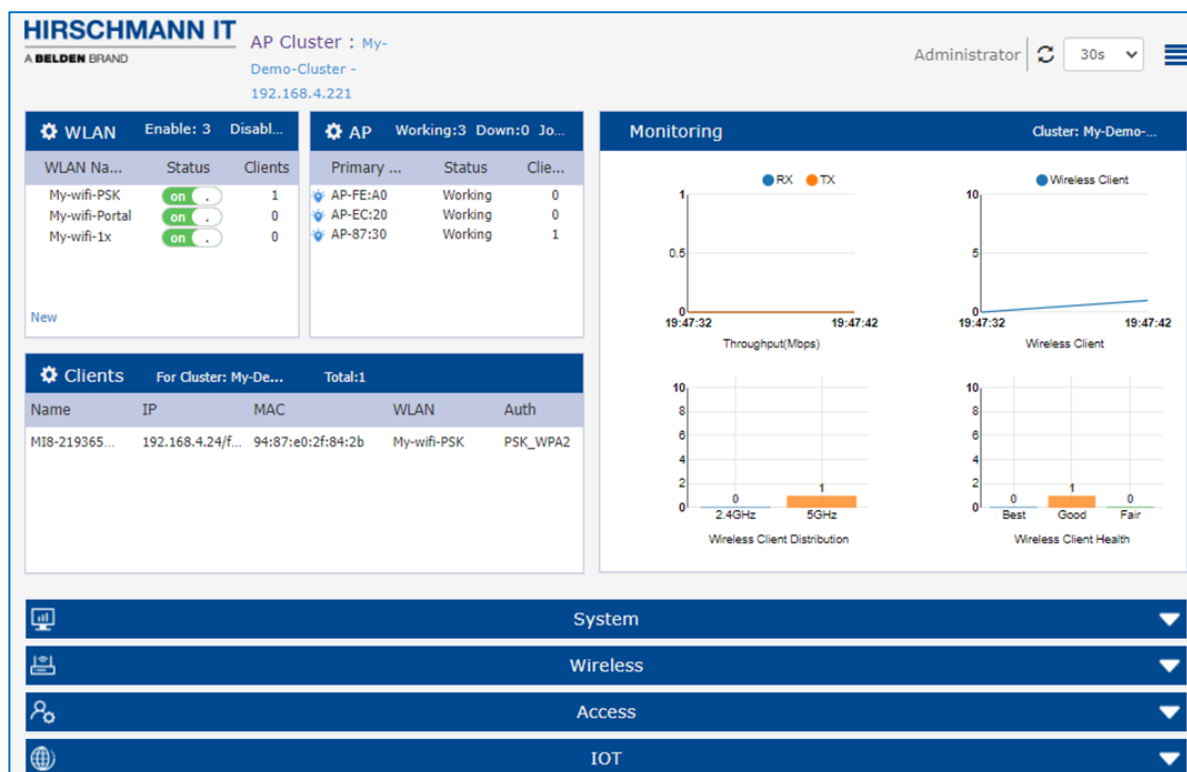


Figure 5-1-1 Dashboard overview

5.2 WLAN

The WLAN configuration window is integrated with all WLAN related monitoring and operation tasks. There are two modes for the WLAN window, WLAN window illustrated in Figure5-2-1 and WLAN Configuration window illustrated in Figure 5-2-2. You can easily launch the WLAN configuration window from WLAN window by clicking the WLAN window frame.

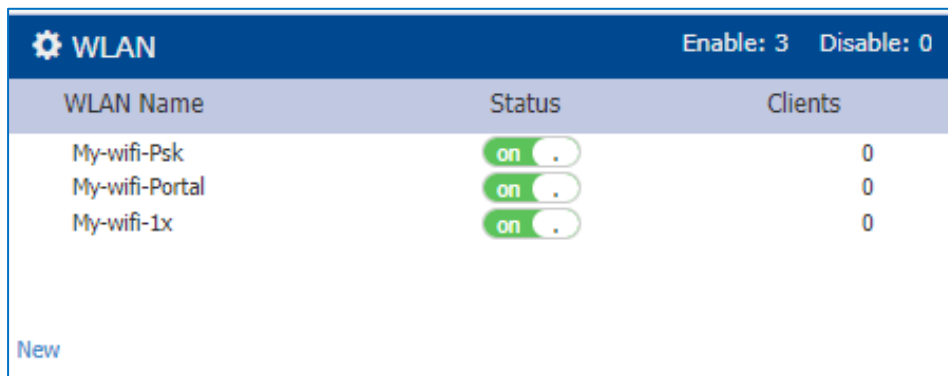


Figure 5-2-1 WLAN Window

Parameter	Specification
WLAN Name	Label or name of WLAN, which is composed by 0-9, a-z or other string.
Status	Indicates the WLAN state
	<input checked="" type="checkbox"/> indicates that WLAN is in broadcast state, while
	<input type="checkbox"/> indicates WLAN is not in broadcast state.
Clients	The number of users connected to the WLAN.
New	Launch the WLAN creation window.

Table 5-2-1 Key words specification in WLAN Window

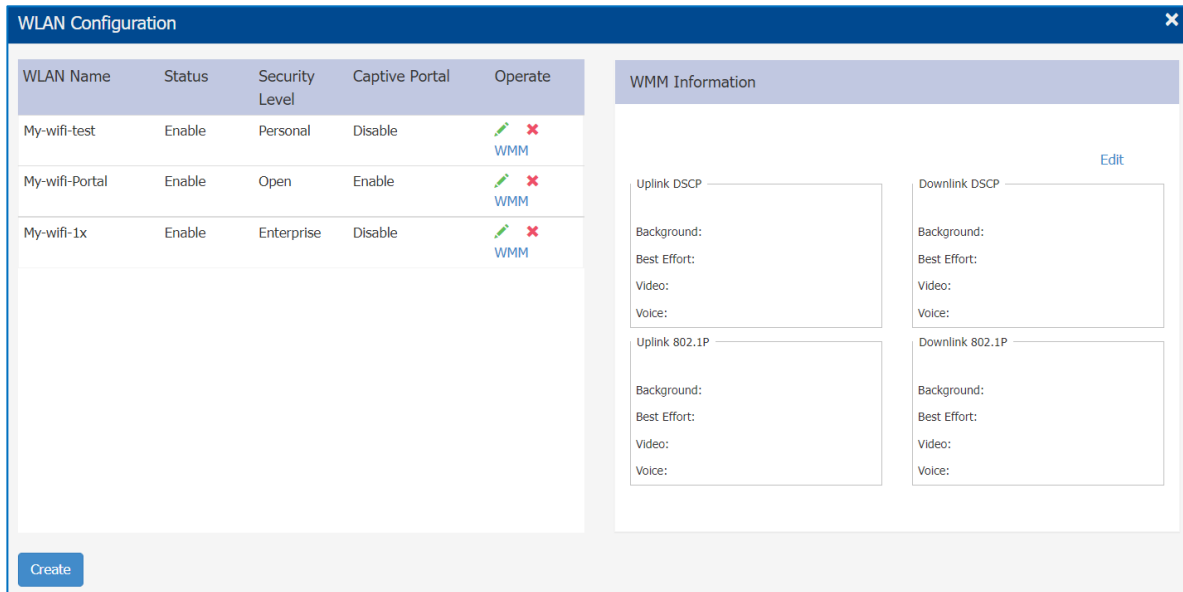


Figure 5-2-2 WLAN Configuration Window

WLAN Name	Label or name of WLAN.
Status	Indicates the WLAN state, ' Enable ' indicates that WLAN is in broadcast state, while " Disable " indicates WLAN is not in broadcast state.
Security Level	Security Level of WLAN, from high to low is Enterprise>Personal>Open .
Captive Portal	Indicates whether the WLAN is using captive portal authentication. ' Enable ' means the WLAN is configured with captive portal authentication, while ' Disable ' means the WLAN is without captive portal authentication.
Operate	Operation for the WLAN which includes ' Modify your WLAN ', ' Delete your WLAN ' and ' Modify WMM '
Create	Create a new WLAN

Table 5-2-2 Key words specification in WLAN Configuration Window



Note

The label below displays the number of enabled or disabled WLANs.

WLAN

Enable: 3 Disable: 0

5.3 AP

AP Window is integrated with all DAPs and cluster related monitoring and configuration functions. Similar to the WLAN Window, there are two modes for AP

Window, Simplified window illustrated in Figure 5-3-1 and AP Configuration window illustrated in Figure 5-3-2. You can easily launch the Advanced Mode from Simplified Mode by clicking the AP Window Frame.

AP Working:3 Down:0 Joining:0		
Primary Name	Status	Clients
AP-FE:A0	Working	0
AP-87:30	Working	0
AP-EC:20	Working	0

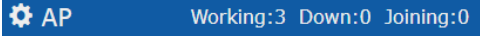
Figure 5-3-1 AP Window

Parameter	Specification
Primary Name	AP MAC Address.
Status	Connection statuses of AP, there are three indications for AP status: Working, Down and Joining.
Clients	The total number of users currently connected to AP.

Table 5-1-1 Key words specification in AP Window



DAP has three status indications when connecting to cluster, they are ‘working’ which indicates that DAP(s) has connected to the PVM successfully and is working normally, ‘Down’ indicates that DAP(s) is disconnected from the cluster, and ‘Joining’ indicates that DAP(s) is requesting to join the cluster but hasn’t completed yet. The Label in AP Window indicates the number of APs in each status.



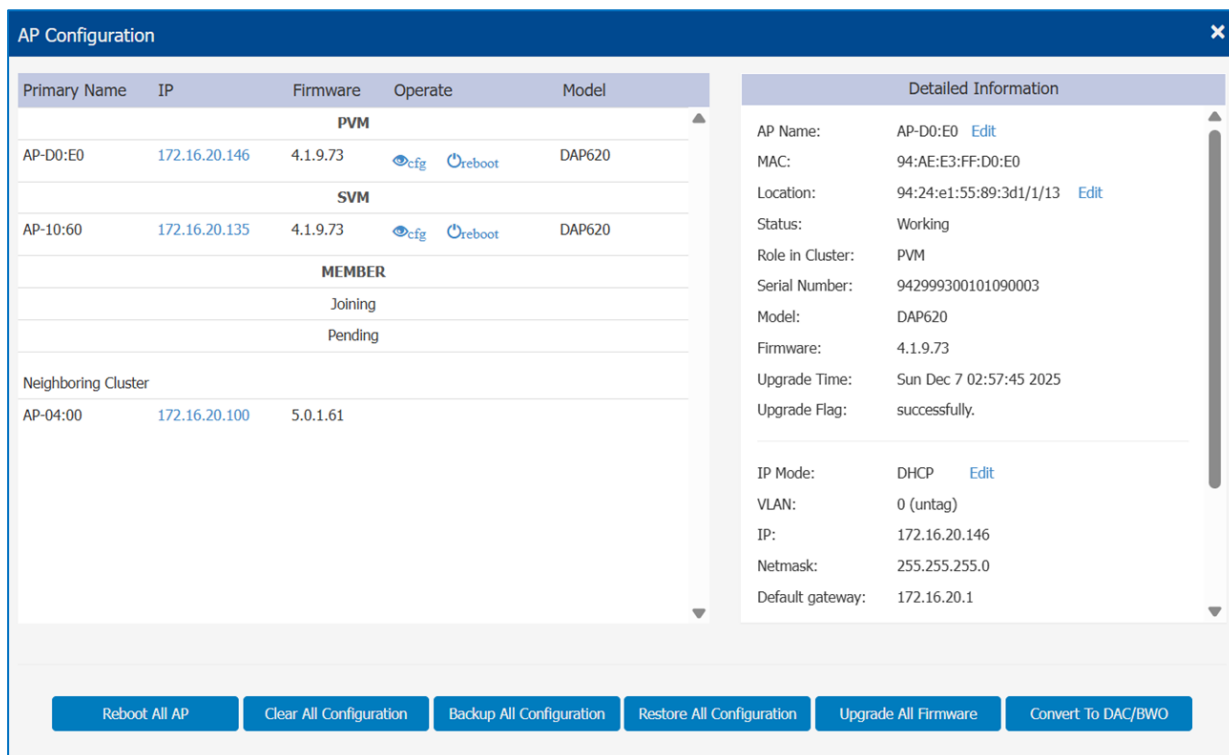




Figure 5-3-2 AP Configuration Window

Parameter	Specification
Primary Name	Name of the DAP.
IP	IP address of the DAP.
Firmware	Firmware version of the DAP.
Operate	There are two optional operations for the DAP: Checking the detailed configuration on the DAP Execute to reboot the DAP.
PVM	Primary Virtual Management in the DAP cluster.
SVM	Secondary Virtual Controller in the DAP cluster.
MEMBER	Other member DAPs in the cluster except PVM/SVM.
Joining	DAPs in joining state, needs to be authorized to join the cluster.
Pending	DAPs in pending state, needs to upgrade the software to join the cluster.
Neighboring cluster	Neighboring DAP clusters with different cluster ID.
	Checking the detailed configuration on the DAP.
	Execute to reboot the DAP.
Reboot All AP	Reboot all the DAPs in the cluster.
Clear All Configuration	Restore factory settings for all the DAPs in the cluster.
Backup All Configuration	Backup the configuration of DAP cluster.

Restore All Configuration	Restore the configuration for DAP cluster.
Upgrade All Firmware	Update the firmware for all the DAPs in the cluster.
Convert To DAC/BWO	Convert all the APs in the cluster to be managed through DAC/BWO. Once configured, DAP will reboot and register to DAC/BWO. Management Server – DAC/BWO address to which DAP register. DHCP Option – Obtain the DAC/BWO address through DHCP option 138 or option 43 during AP booting up state. Static – Configure a static DAC/BWO to which AP will register after rebooting.
Detailed Information	Detailed information for the selected DAP.
AP Name	Name of DAP.
Location	Location of DAP.
Status	Connection status of DAP, there are three indications for AP status: Working, Down and Joining.
Kick Off	Remove the DAP from the cluster. When a DAP is removed from the cluster, it changes into Joining state until the administrator permits it to join the cluster again.
Role in cluster	AP role in the cluster, including PVM, SVM and MEMBER.
Update to PVM	Upgrade the member or SVM to be the PVM of the AP cluster.
Serial Number	Serial Number of the DAP selected.
Model	Product Model of the DAP selected.
Upgrade Time	Last firmware upgrade time.
Upgrade Flag	Flag of last time firmware upgrade. Success means the firmware was upgraded successfully on the Upgrade Time, Failed means the firmware wasn't upgraded successfully on the Upgrade Time.
IP Mode	The way by which the AP attains its IP address, dynamically assigned from DHCP server or static IP configured manually. Only IPv4 static address can be configured for AP.
IP	IPv4/IPv6 address of the DAP selected.
Netmask	Netmask of the IPv4 address of the DAP selected.
Default Gateway	Default Gateway of the DAP selected.
DNS	DNS server in the network.
AP Mode	<ul style="list-style-type: none"> Cluster – DAP working in cluster mode. DAC/BWO – Change the DAP to be managed and configured through DAC/BWO. You need to specify the DAC/BWO IP address when changing to DAC/BWO mode. DHCP Option – Obtain the DAC/BWO address through DHCP option 138 or option 43 during DAP booting up state. Static – Configure a static DAC/BWO IP address to which AP will register after rebooting.

Table 5-3-2 Key words specification in AP Configuration Window

5.4 Client

Client Window displays all the connected clients. Similar to the WLAN Window, there are two modes for Client Window, Simplified window illustrated in Figure 5-4-1 and Client information window illustrated in Figure 5-4-2. You can launch the Client information window from Simplified window by clicking the Clients Window frame.


 Clients For Cluster: AP-Cluster Total:3				
Name	IP	MAC	WLAN	Auth
MS-KAWGSNR...	192.168.8.53/fe...	00:15:00:65:4a:70	My-wifi-test	PSK_WPA2
Lakers0326	192.168.8.33/24...	c0:3c:59:70:3d:c5	My-wifi-test	PSK_WPA2
iPhone-2	192.168.8.4/240...	dc:0c:5c:dd:59:c9	My-wifi-test	PSK_WPA2

Figure 5-4-1 Clients Window-Simplified Mode

In the Clients Information window, click '✖' of client entry will kick off the specific client from AP, and click '🚫' will kick off the client and add it to the blacklist.

Parameter	Specification
For Cluster:[Cluster Name]	Clients connected to the Cluster.
For WLAN:[WLAN Name]	Clients connected to the specified WLAN in the Cluster.
For AP:[AP_MAC]	Clients connected to the specified AP in the Cluster.
Name	User name or host name of the client. For 802.1X or captive portal authentication through username & password, username is populated in the field. For client authentication without username (Open/PSK/Captive portal through terms and conditions check only), hostname is populated in the field. DAP obtains client hostname from client DHCP packets. For some cases of client DHCP packets not being carried, hostname cannot be obtained, and the Name field could be empty.
IPv4	IPv4 address of the client.
IPv6	IPv6 address of the client.
MAC	MAC address of the client.
WLAN	WLAN to which the client connected.
Auth	Authentication type: Open, Portal (Captive portal), PSK (Personal), 802.1X (Enterprise).



Table 5-4-1 Key words specification in Clients Window

Clients Information

Q
✕

Name	IP	MAC	WLAN	Access Point			Client Detail	
MS-KAWGSNR...	192.168.8.53/fe80...	00:15:00:65:4a:70	My-wifi-test	AP-C0:70	✕	🗑️	Name:	MS-KAWGSNRXDJDC
Lakers0326	192.168.8.33/240...	c0:3c:59:70:3d:c5	My-wifi-test	AP-C0:70	✕	🗑️	IPv4:	192.168.8.53
iPhone-2	192.168.8.4/2409...	dc:0c:5c:dd:59:c9	My-wifi-test	AP-C0:70	✕	🗑️	IPv6:	fe80::285f:5e03:3110:2427
							MAC:	00:15:00:65:4a:70
							WLAN:	My-wifi-test
							Access Point:	AP-C0:70 (94:ae:e3:ff:c0:70)
							AP Name:	AP-C0:70
							Auth:	PSK_WPA2
							Attached Band:	5G
							Online Time:	35 s
							RSSI:	-47dBm
							Working Mode:	11NA_HT40
							PHY Rx rate:	300.00Mbps
							PHY Tx rate:	300.00Mbps
							Rx rate:	0.00Mbps

Figure 5-4-2 Clients Information Window

Parameter	Specification
User Name	User Name of the client.
IP	IPv4 address of the client.
MAC	MAC address of the client.
WLAN	WLAN to which the client connected.
Access Point	Access point to which the client connected.
	Force the client to disconnect the wireless network.
	Remove the client from the wireless network and put it within the blocklist. If removed, the client can be displayed and operated in the blocklist window.
AP Name	Name of Access Point that the client connected.
Auth	Authentication type: Open, Portal (Captive Portal), PSK (Personal), 802.1X (Enterprise).
Attached Band	The radio band through which the client attaching to AP, 2.4GHz or 5GHz.
Online Time	Time when the client attached to the wireless network.
Session Time	Time when the client has passed the captive portal authentication, only for captive portal clients.
RSSI	Received Signal Strength Indication of the client, Value 0~99.
Working Mode	Wireless working mode of the client.
PHY Rx rate	Physical receiving rate of the client.
PHY Tx rate	Physical sending rate of the client.
Rx rate	Packet receiving rate of the client.
Tx rate	Packet sending rate of the client.
Download	Total download data size since the client connected to the wireless network.
Upload	Total upload data size since the client connected to the wireless network.
Device type	Device type of the client.
OS Type	Operating system type of the client.
Rx Error	The number of error packets received by the client. Interference is the most major cause of packet error. Another cause of packet error is the mismatch of broadcast power levels (Tx Power). If an AP and client device are communicating at much different broadcast strengths, then this can cause packet error.
Tx Retry	The number of retry packets sent by the client. The Retry indicates packets that had to be re-sent because they were corrupted upon arriving at the proper destination.

Roaming History	<p>Showing roaming history between SSID/AP/Band for the client, total 32 roaming records can be displayed and will be separated by connection sessions.</p> <ul style="list-style-type: none"> • Connection Session – A session represent a period which starting from associating to the wireless network and ending by disassociating. Roaming records are distributed within sessions. • The connection sessions are arranged based to time sequence. The latest session will be positioned on the top of roaming history display. • The Offline status represent the connection session has ended. The Online status represent an ongoing session and the client is not disassociated.
------------------------	---

Table 5-4-2 Key words specification in Clients Information Window

5.5 Monitoring

The monitoring window displays the utilization of the wireless network, including statistics of traffic throughput and client working state.

The monitoring window can monitor from four different aspects: cluster based, WLAN based, AP based and client based, illustrated in Figure 5-5-1, Figure 5-5-2, Figure 5-5-3 and Figure 5-5-4.

The cluster monitoring is the default display; you can select to monitor certain WLAN/AP/client from the WLAN Window/AP Window/Client Window on left side of the Dashboard.

The monitoring window is automatically refreshed every 30 seconds by default, and the data refresh cycle can be set to 30s /60s /120s.



Figure 5-5-1 Monitoring Window - AP Cluster

Parameter	Specification
RX	Total receiving rate of the AP Cluster.
TX	Total sending rate of the AP Cluster.
Client	The number of clients connected to the AP Cluster.
Client Band	The working band distribution of clients connected to the AP Cluster, including number of clients working on 2.4GHz band and number of clients working on 5GHz band.
Client Health	The wireless connection quality between client and DAP, it is judged by the signals of client, and classified as below: <ul style="list-style-type: none"> Best— Number of clients whose signal strength is more than 30. Good— Number of clients whose signal strength is between 15 ~30. Fair—Number of clients whose signal strength is less than 15.

Table 5-5-1 Key words specification in AP Cluster Monitoring Window



Figure 5-5-2 Monitoring Window – WLAN

Parameter	Specification
RX	Total receiving rate of the WLAN.
TX	Total sending rate of the WLAN.
Client	The number of clients connected to the WLAN.
Client Band	The working band distribution of clients connected to the WLAN, including number of clients working on 2.4GHz band and number of clients working on 5GHz band.
Client Health	<p>The wireless connection quality between client and DAP, it is judged by the signals of client, and classified as below:</p> <ul style="list-style-type: none"> • Best— Number of clients which signal strength is more than 30. • Good— Number of clients which signal strength is between 15 ~30. • Fair—Number of clients which signal strength is less than 15.

Table 5-5-2 Key words specification in WLAN Monitoring Window

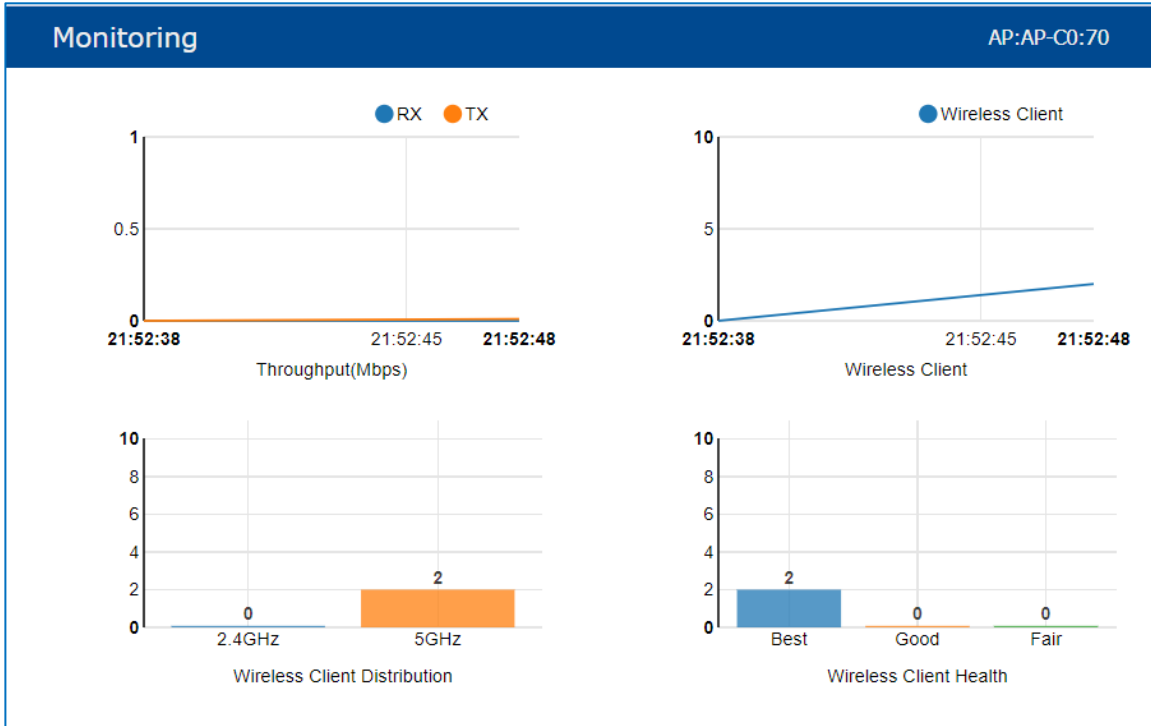


Figure 5-5-3 Monitoring Window – AP

Parameter	Specification
RX	Total receiving rate of the AP.
TX	Total sending rate of the AP.
Client	The number of clients connected to the AP.
Client Band	The working band distribution of clients connected to the AP, including number of clients working on 2.4GHz band and number of clients working on 5GHz band.
Client Health	The wireless connection quality between client and DAP, it is judged by the signals of client, and classified as below: Best— Number of clients which signal strength is more than 30. Good— Number of clients which signal strength is between 15 ~30. Fair—Number of clients which signal strength is less than 15.

Table 5-5-3 Key words specification in AP Monitoring Window

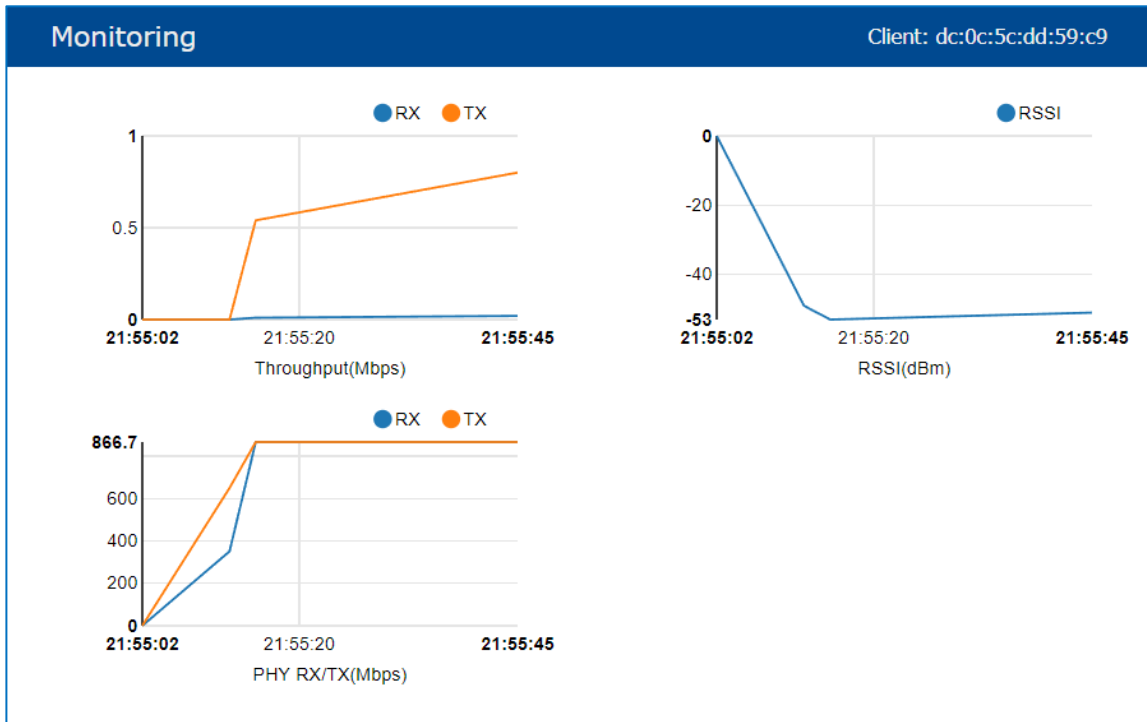


Figure 5-5-4 Monitoring Window – Client

Parameter	Specification
RX	Receiving rate of the client.
TX	Sending rate of the client.
RSSI	Received Signal Strength Indication of the client
PHY RX	Physical receiving rate of the client.
PHY TX	Physical sending rate of the client.

Table 5-5-4 Key words specification in Client Monitoring Window

5.6 System

The System window was divided into three windows in System Page: General window, System Time window and Syslog window, illustrated in Figure 5-6-1 System page.

The screenshot shows the 'System' configuration page with three main sections:

- General:** Cluster ID: 301, Cluster Name: My-Cluster, Cluster Location: My_Location, Cluster Manage IP: 172.16.10.234, Cluster Manage Netmask: 255.255.255.0, User - Viewer: Disabled, User - GuestOperator: Disabled, Certificate - Web Server: default.
- System Time:** Date and Time: Tue Jan 11 2022 09:19:51, Daylight-Saving Time: off, Time Zone: (UTC+08:00)Kuala-Lumpur,Singapore, NTP Server List: (empty), NTP Server: IP Address (v4|v6) [Add].
- Syslog & SNMP:** Syslog and SNMP tabs. Syslog table:

Title	Level	Source
DNS servers are unreach...	CRIT	172.16.10.169
DNS servers are unreach...	CRIT	172.16.10.169
DNS servers are unreach...	CRIT	172.16.10.169
DNS servers are unreach...	CRIT	172.16.10.169

Log Level: Ap-Debug: Notice, System: Error.

Figure 5-6-1 System page

5.7 Wireless

The Wireless Window focuses on advanced wireless functions, including three windows: RF (Radio Frequency), wIDS/wIPS, and Performance Optimization, illustrated in Figure 5-7-1 Wireless Window.

The screenshot shows the 'Wireless' configuration page with three main sections:

- RF:** 2.4GHz selected, 5GHz unselected. 2.4GHz Channel Distribution pie chart showing CH1, CH6, and CH11.
- wIDS/wIPS:** Rogue Suppress: on, Dynamic Blocklist: on, Wireless Attack Detection: on. Unknown AP bar chart showing Interfering AP and Rogue AP with MAC addresses.
- Performance Optimization:** Background Scanning: on. Scanning Interval: 0 min, 20 sec. Scanning Duration: 50ms. Band Steering: on, Force 5G: [], Exclude. Load Balance: on. RSSI Threshold: 2.4G: 0, 5G: 0.

Figure 5-7-1 Wireless Window

5.8 Access

The Access page is divided into three windows: Authentication window, Blocklist & Allowlist window, ACL window, illustrated in Figure 5-8-1.

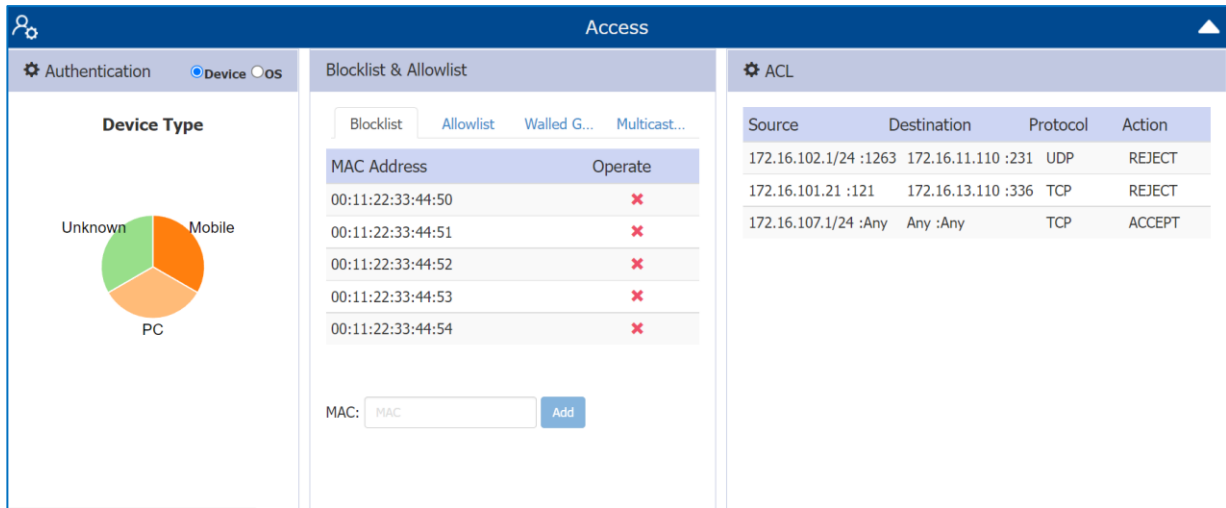


Figure 5-8-1 Access Page

IoT

The IoT window was divided into two windows: Bluetooth configuration page and Detailed Information page, illustrated in Figure 5-9-1.

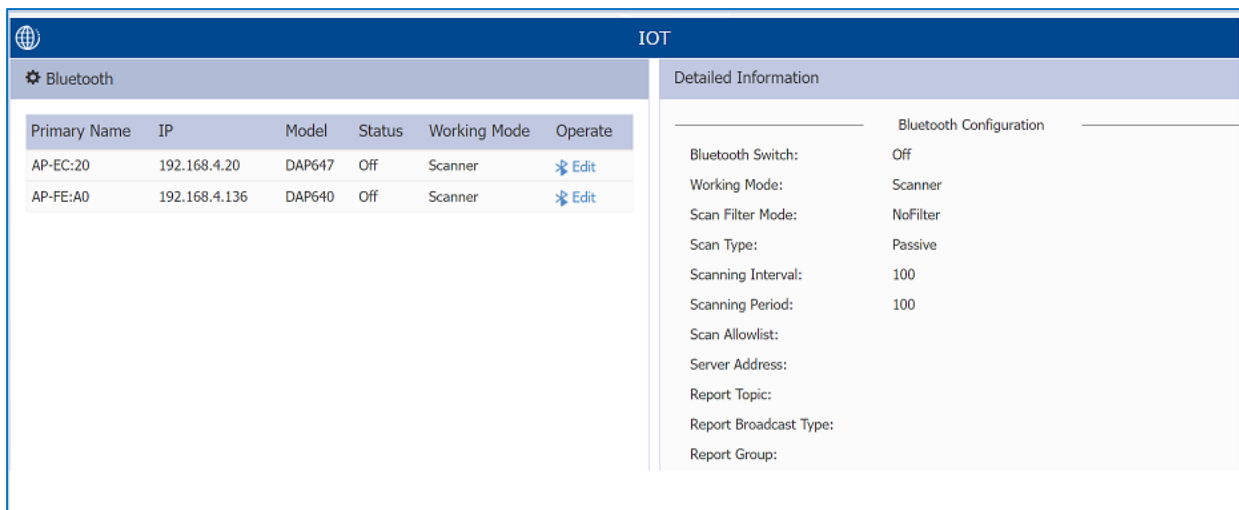


Figure 5-9-1 IoT Page

5.9 More

Some additional information can be seen by click “More” tab on the right corner shown in Figure 5-10-1.

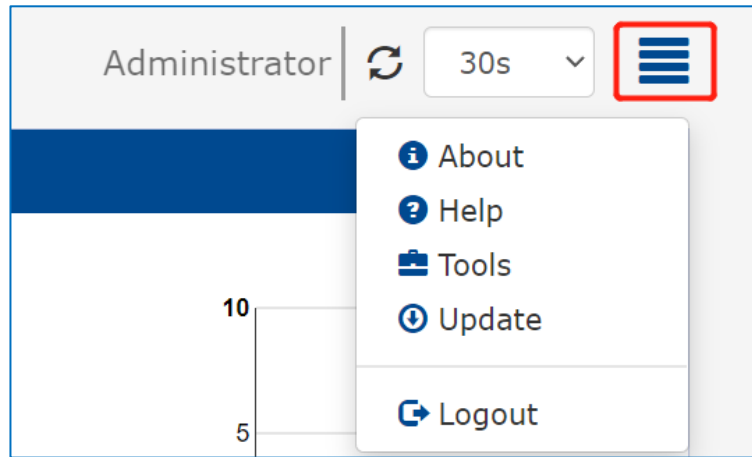


Figure5-10-1 More information about DAP

- ✓ **About:** Basic information of DAP cluster, such as software version, Country/Region, etc. shown in Figure5-10-2



Figure5-10-2 About

- ✓ **Help:** Related help information will be displayed when mouse moved to the title bar, shown in Figure5-10-3.

HIRSCHMANN IT
A **BELDEN** BRAND

AP Cluster : My-Demo-
Cluster - 172.16.10.234
My_Location

WLAN			AP			
WLAN Name	Status	Clients	Primary	Working:1	Down:0	Joining:0
My-wifi-test	<input checked="" type="checkbox"/>	1	AP-C037			1

Click on each row in AP list to see the monitoring and client information of this AP in the corresponding display area, you can also see the details of each AP by clicking the title.

Clients				
For Cluster: My-Demo-Clu...				
Name	IP	MAC	WLAN	Auth
Lakers0326	172.16.10.102/fe80...	c0:3c:59:70:3d:c5	My-wifi-test	PSK_WPA2

Figure5-10-3 Online help

- ✓ **Tools:** Some basic troubleshooting tools integrated in DAP; please refer to 11 Support Tools for details.
- ✓ **Update:** Upgrades DAP if new version detected.
- ✓ **Logout:** Logout current User.

6 WLAN Configuration

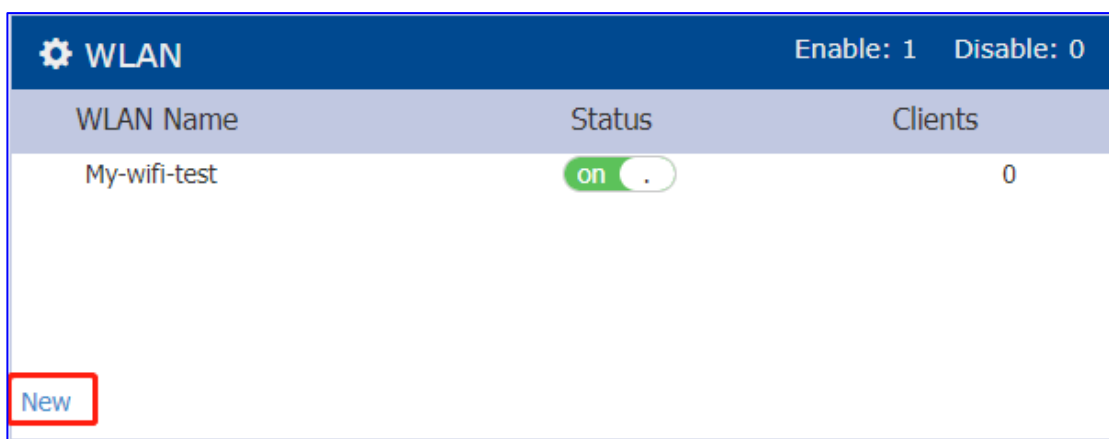
Configuring WLAN should be the first step when setting up your Wi-Fi network. This section contains the following topics:

- [Two ways to create a new WLAN](#)
- [Introduction to WLAN with different authentication modes](#)
- [Key words specification for WLAN](#)
- [Modify WLAN Configuration](#)
- [Delete Your WLAN](#)
- [WMM Configuration](#)

6.1 Two ways to create a new WLAN

There are 2 ways to create a new WLAN in cluster mode show as below:

- Create a new WLAN by clicking hyperlink “New” in the WLAN Simplified mode of main page, See in Figure6-1-1 and Figure6-1-2:



WLAN Enable: 1 Disable: 0		
WLAN Name	Status	Clients
My-wifi-test	<input checked="" type="checkbox"/>	0

[New](#)

Figure6-1-1 WLAN Simplified Mode

Create New WLAN [X]

WLAN Name:

Security Level: ▼

Key Management: ▼

PMF: ▼

Password Format: ▼

Password:

Confirm:

Figure6-1-2 Create New WLAN Window

- Create a new WLAN by clicking “Create” button in the WLAN Configuration Window, shown in Figure6-1-3:

WLAN Configuration [X]

WLAN Name	Status	Security Level	Captive Portal	Operate
My-wifi-test	Enable	Personal	Disable	<input type="checkbox"/> <input type="checkbox"/> WMM

Create New WLAN

WLAN Name: (1-32 chars)

Security Level: ▼

Key Management: ▼

PMF: ▼

Password Format: ▼

Password:

Confirm:

Inactivity Timeout Status: off

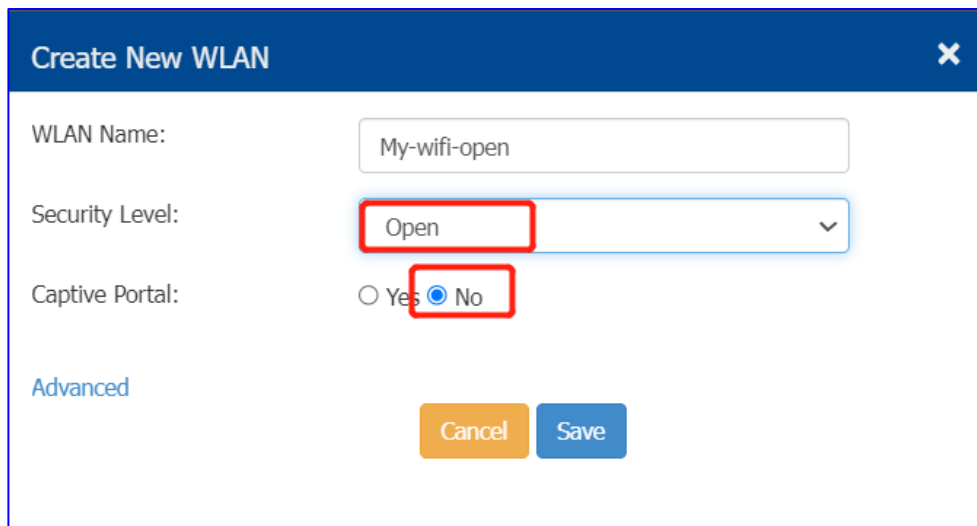
Create

Figure6-1-3 Create New WLAN in WLAN Configuration window

6.2 WLAN type introduction

There are 4 types of WLAN supported by DAP in cluster mode:

Open : There is no Authentication or encryption method for this kind of wireless network, the data frame of wireless clients will be transmitted as plain text transmit mode over the air, shown in Figure6-2-1

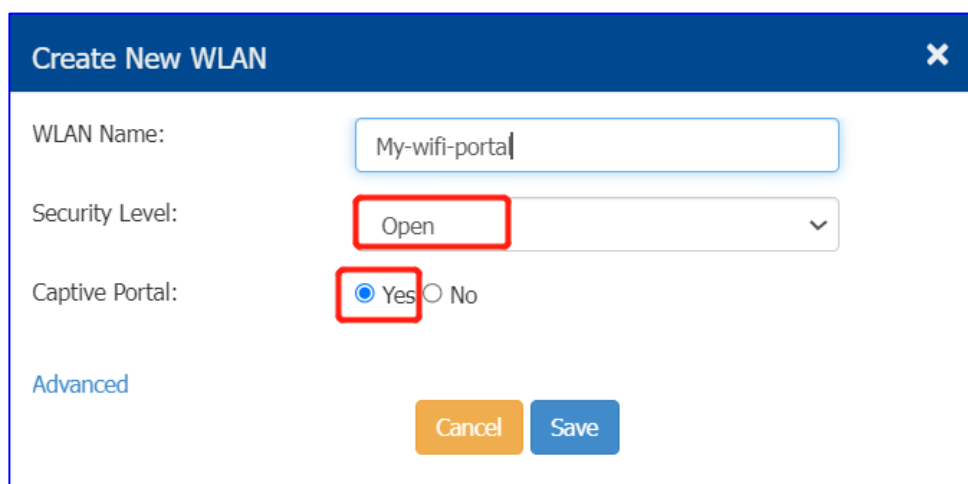


The screenshot shows a 'Create New WLAN' dialog box with the following fields and options:

- WLAN Name: My-wifi-open
- Security Level: Open (highlighted with a red box)
- Captive Portal: Yes No (highlighted with a red box)
- Advanced (link)
- Buttons: Cancel (orange), Save (blue)

Figure6-2-1 Create an Open WLAN

Open with Portal authentication : As shown in Figure6-2-2, Captive portals are only used in an Open WLAN where the users are shown a welcome message informing them of the conditions of access and access the network only after logging in, shown in Figure6-2-3. Captive portal authentication are usually used for a guest user , please refer to [10.1 Login methods for the captive portal authentication](#) for details.



The screenshot shows a 'Create New WLAN' dialog box with the following fields and options:

- WLAN Name: My-wifi-portal
- Security Level: Open (highlighted with a red box)
- Captive Portal: Yes No (highlighted with a red box)
- Advanced (link)
- Buttons: Cancel (orange), Save (blue)

Figure6-2-2 Create a portal WLAN

Figure6-2-3 Portal log in page

Personal: Also referred to as PSK (pre-shared key) mode, this is designed for home and small office networks and doesn't require an authentication server. Each wireless network device encrypts the network traffic using a 256 bit key. This key may be entered either as a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters. Personal mode is available with WPA, WPA2 and WPA3 or combinations, illustrated in Figure6-2-4

The screenshot shows the 'Create New WLAN' configuration window. The 'WLAN Name' is 'My-wifi-PSK'. The 'Security Level' is set to 'Personal'. The 'Key Management' dropdown menu is open, showing options: 'Static WEP', 'WPA2 Personal', 'WPA3 Personal', 'Both (WPA2 & WPA)', and 'Both (WPA3 & WPA2)'. The 'Both (WPA2 & WPA)' option is selected. The 'PMF' field is empty. The 'Password Format' field is empty. The 'Password' and 'Confirm' fields are masked with dots.

Figure6-2-4 Create a Personal WLAN

Enterprise: Namely 802.1x authentication, this is designed for enterprise networks and requires a RADIUS authentication server. This requires a more complicated setup, but provides additional security (e.g. protection against dictionary attacks on short passwords). Various kinds of the Extensible Authentication Protocol (EAP) are used for authentication. Enterprise mode is available with Both (WPA2 & WPA), WPA2 and WPA3, illustrated in Figure6-2-5.

The screenshot shows the 'Create New WLAN' configuration window. The 'WLAN Name' is 'My-wifi-enterprise'. The 'Security Level' is set to 'Enterprise'. The 'Key Management' dropdown menu is open, showing options: 'WPA2 Enterprise', 'WPA2 Enterprise', 'WPA3 Enterprise', and 'Both (WPA2 & WPA)'. The 'WPA2 Enterprise' option is selected. The 'PMF' field is empty. The 'AuthServer' is '172.16.12.113'. The 'AuthPort' is '1812'. The 'AuthSecret' field is masked with dots.

**Note**

WPA uses 802.1X authentication which is one of the Extensible Authentication Protocol (EAP) types available today. 802.1X is a port-based network access control method for wired, as well as wireless, networks. It was adopted as a standard by the IEEE in August of 2001. EAP handles the presentation of users' credentials, in the form of digital certificates (already widely used in Internet security), unique usernames and passwords, smart cards, secure IDs, or any other identity credential that the IT administrator is comfortable deploying. WPA allows flexibility in both the type of credentials that are used and in the selection of an EAP type.

6.3 Key words specification for WLAN

Regarding different scenario on end customer, different configurable WLAN parameters can be set for special requirement, below are the key word specification in Create new WLAN /Modify WLAN Window for your reference:

PMF: DAP supports the IEEE802.11w standard, also known as Protected Management Frames (PMF). The PMF function increases the security by providing data confidentiality of management frames. PMF is applicable for WPA2 and WPA3 encryption method, illustrated in Figure6-3-1.

- **Disable**: Disables 802.11w PMF protection for WLAN, it is "**Disabled**" by default.
- **Optional**: Both 802.11w PMF capable clients and 802.11w PMF non-capable clients can connect the SSID.
- **Required**: Clients only support 802.11w PMF can connect to the SSID.

**Note**

For WPA3 Enterprise authentication, if the CNSA is selected, PMF is set to 'required' which means only PMF capable client can connect.

The screenshot shows the 'Edit WLAN Information' configuration page. The fields are as follows:

- WLAN Name: My-wifi-test (1-32 chars)
- Security Level: Personal
- Key Management: Both (WPA2 & WI)
- PMF: Disabled (selected and highlighted in blue)
- Password Format: Optional
- Password: [Redacted]
- Confirm: [Redacted]
- Inactivity Timeout Status: off

Figure6-3-1 PMF settings for WLAN

Inactivity Timeout Status: Specify the inactivity timeout interval configuration status. The clients will be disconnected from the wireless network for a specific duration that not transmitting any packets. If Inactivity Timeout Status is enabled, the configured Inactivity Timeout Interval will be used to disconnect inactivity client, illustrated in Figure6-3-2.

Inactivity Timeout Interval: Specify the inactivity timeout internal, the default value is set to 600 seconds and can be configured from 60 seconds to 12000 seconds, illustrated in Figure6-3-2.

The screenshot shows the 'Edit WLAN Information' configuration interface. It includes the following fields and options:

- Password:** A text input field with masked characters (dots).
- Confirm:** A text input field with masked characters (dots).
- Inactivity Timeout Status:** A toggle switch currently set to 'on', highlighted with a red box.
- Inactivity Timeout Interval:** A text input field containing the value '600', highlighted with a red box. To its right, the range '(60-12000)s' is indicated.
- Enable:** Radio buttons for 'Yes' (selected) and 'No'.
- Hidden:** Radio buttons for 'Yes' and 'No' (selected).

Figure6-3-2 Inactivity Timeout Configuration

Enable: Specify the WLAN state, 'Yes' means that WLAN is in broadcast state, while 'No' means WLAN will not applied to APs and not in broadcast state, illustrated in Figure6-3-3.

Hidden: Specify visibility of the WLAN, 'Yes' means that the "SSID" parameter will not include in the beacon frame and WLAN is invisible to wireless clients, while 'No' means WLAN is invisible, illustrated in Figure6-3-3;

Create New WLAN

Password:

Confirm:

Inactivity Timeout Status: on off

Inactivity Timeout Interval: (60-12000)s

Enable: Yes No

Hidden: Yes No

Multicast: Yes No

ARP Proxy: Yes No

Band: 2.4GHz 5GHz

Figure6-3-3 Enable and Hidden WLAN

Multicast: This feature allows DAPs to convert multicast streams into unicast streams over the wireless network based on the IGMP snooping table. Enabling Multicast to Unicast (for up to 6 clients) can enhance the quality and reliability of video streams, while preserving the bandwidth available to the non-video services, illustrated in Figure6-3-4.

Create New WLAN

Inactivity Timeout Status:	<input type="checkbox"/> on <input checked="" type="checkbox"/> off	
Inactivity Timeout Interval:	<input type="text" value="600"/>	(60-12000)s
Enable:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Hidden:	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Multicast:	<input type="radio"/> Yes <input checked="" type="radio"/> No	
ARP Proxy:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Band:	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz	
Scope Type:	<input checked="" type="radio"/> All <input type="radio"/> Group	
WLAN Access Timer:	<input type="checkbox"/> on <input checked="" type="checkbox"/> off	
MaxClients Per Band:	<input type="text" value="64"/>	(1-256)

Figure6-3-4 Multicast configuration

ARP Proxy: If enabled, when the ARP request to a client connected to DAP, DAP will reply to clients' ARP request instead of forwarding, this will reduce the ARP forwarding in the air and improve the wireless performance, illustrated in Figure6-3-5.



Note

The DAP does not act as an ARP proxy for gratuitous ARP. When a client obtains an IP address from DHCP or IP release / renewal, the client will send gratuitous ARP packets, DAP will not respond to this special ARP packet and broadcast it normally.

Create New WLAN

Inactivity Timeout Status: off

Inactivity Timeout Interval: (60-12000)s

Enable: Yes No

Hidden: Yes No

Multicast: Yes No

ARP Proxy: Yes No

Band: 2.4GHz 5GHz

Scope Type: All Group

WLAN Access Timer: off

MaxClients Per Band: (1-256)

Figure6-3-5 ARP Proxy configuration

Band: Select a value to specify the band at which the network transmits radio signals. You can set the band to 2.4 GHz, 5 GHz, or both of them. The All option is selected by default, illustrated in Figure6-3-6

Create New WLAN

Inactivity Timeout Status: off

Inactivity Timeout Interval: (60-12000)s

Enable: Yes No

Hidden: Yes No

Multicast: Yes No

ARP Proxy: Yes No

Band: 2.4GHz 5GHz

Scope Type: All Group

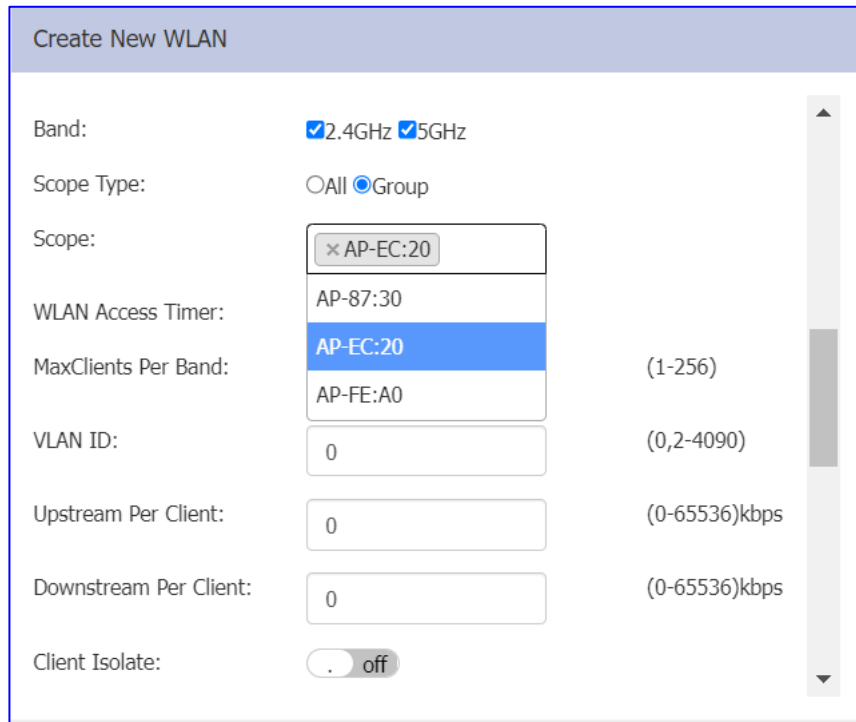
WLAN Access Timer: off

MaxClients Per Band: (1-256)

Figure6-3-6 Band Configuration

Scope Type: Specify the scope of APs in the cluster which will create the WLAN, shown in Figure6-3-7

- All – All DAPs in the cluster will create the WLAN.
- Cluster – Select the DAPs which will create the WLAN. The DAP which MAC address is in the cluster will be valid for the WLAN.



The screenshot shows the 'Create New WLAN' configuration page. The 'Scope Type' is set to 'Group'. The 'Scope' dropdown menu is open, showing a list of APs: 'AP-EC:20' (selected), 'AP-87:30', 'AP-EC:20', and 'AP-FE:A0'. Other settings include 'Band' (2.4GHz and 5GHz checked), 'WLAN Access Timer' (0), 'MaxClients Per Band' (0), 'VLAN ID' (0), 'Upstream Per Client' (0), 'Downstream Per Client' (0), and 'Client Isolate' (off).

Figure6-3-7 Scope Type configuration

WLAN Access Timer: Specify the WLAN working period, in which only SSID broadcasts. If NOT configured (it is Disabled by default), the SSID will always broadcast if the WLAN is activated, illustrated in Figure6-3-8, after a WLAN timer configured, there will be icon of timer displayed in front of the WLAN which shown in Figure6-3-9.



Please make sure the system time and time zone configured correctly before you using this feature.
WLAN may not work as expected if the DAP system time and time zone not correct.

Note

- Access Days – Specify the days for broadcasting SSID per week.
- Operational Hours – Specify the time of the day in which broadcasting SSID.

- Start Time – Time to enable the WLAN
- End Time – Time to disable the WLAN

Figure6-3-8 WLAN Access Timer configuration

HIRSCHMANN IT A **BELDEN** BRAND

AP Cluster : My-Demo-
Cluster - 172.16.10.234
My_Location

WLAN			AP		
WLAN Name	Status	Clients	Primary Name	Status	Clients
My-wifi-test	<input checked="" type="checkbox"/>	1	AP-C0:70	Working	1
My-wifi-test-102	<input checked="" type="checkbox"/>	0			

WLAN: Enable: 2 Disable: 0 | AP: Working: 1 Down: 0 Joining: 0

New

Figure6-3-9 WLAN Access Timer indication

VLAN ID: Identifier of the VLAN to which the WLAN mapping, it is traffic VLAN for wireless clients, illustrated in Figure6-3-10, if WLAN-VLAN binding configured, the related bridge interface will be created on AP and handling the relative traffic

forwarding, you can check the VLAN configuration by using command 'brctl show' illustrate in Figure6-3-11.

The screenshot shows a 'Create New WLAN' configuration window. The 'VLAN ID' field is highlighted with a red box and contains the value '102'. Other fields include WLAN Access (on), Access Days (Mon-Fri), Operational Hours (on), Start Time (08:00), End Time (18:59), MaxClients Per Band (64), Upstream Per Client (0), and Downstream Per Client (0).

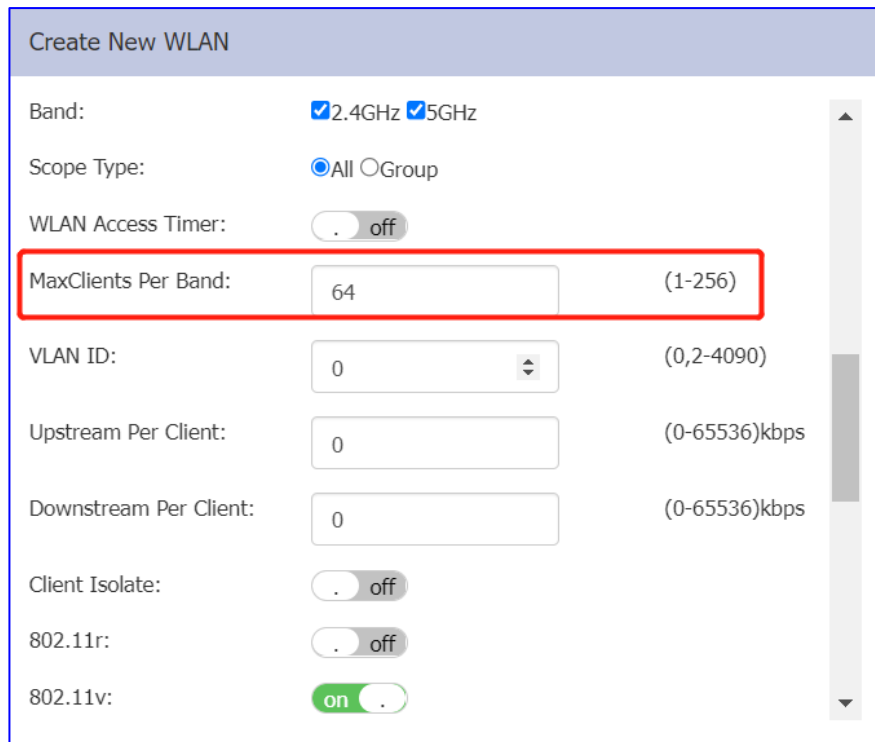
Figure6-3-10 VLAN Configuration

```
support@AP-C0:70:~$
support@AP-C0:70:~$
support@AP-C0:70:~$ brctl show
bridge name      bridge id          STP enabled      interfaces
br-vlan102       7fff.94aee3ffc070 no                ath002
                  eth102
                  eth0-102
                  eth1-102
br-vlan103       7fff.94aee3ffc070 no                ath003
                  ath103
                  eth0-103
                  eth1-103
br-wan           7fff.94aee3ffc070 no                ath001
                  ath101
                  eth0
                  eth1
support@AP-C0:70:~$
support@AP-C0:70:~$
```

Figure6-3-11 Checking VLAN Configuration by using command

MaxClients Per Band: Specify the maximum number of clients that can be configured for each BSSID on a WLAN. You can specify a value within the range of 1 to 256. The default value is 64, when the clients connect to AP reach this specific

number, the authentication request from new client will ignored by DAP and cannot connect to the SSID successfully, illustrated in Figure6-3-12.



Create New WLAN		
Band:	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz	
Scope Type:	<input checked="" type="radio"/> All <input type="radio"/> Group	
WLAN Access Timer:	<input type="checkbox"/> off	
MaxClients Per Band:	<input type="text" value="64"/>	(1-256)
VLAN ID:	<input type="text" value="0"/>	(0,2-4090)
Upstream Per Client:	<input type="text" value="0"/>	(0-65536)kbps
Downstream Per Client:	<input type="text" value="0"/>	(0-65536)kbps
Client Isolate:	<input type="checkbox"/> off	
802.11r:	<input type="checkbox"/> off	
802.11v:	<input checked="" type="checkbox"/> on	

Figure6-3-12 MaxClient Per Band Configuration

Upstream Per Client: Specify the maximum upstream bandwidth limitation for each wireless client, illustrated in Figure6-3-13.

Downstream Per Client: Specify the maximum downstream bandwidth limitation for each wireless client, illustrated in Figure6-3-13.

WLAN Access Timer: off

MaxClients Per Band: (1-256)

VLAN ID: (0,2-4090)

Upstream Per Client: (0-65536)kbps

Downstream Per Client: (0-65536)kbps

Client Isolate: off

802.11r: off

802.11v: on

802.11k: on

UAPSD: on

Figure6-3-13 Clients traffic limitation Configuration

Client Isolate: Not permit the clients attached to the same WLAN to communicate with each other; they can only communicate with upstream gateway, illustrated in Figure6-3-14.

Upstream Per Client: (0-65536)kbps

Downstream Per Client: (0-65536)kbps

Client Isolate: off

802.11r: off

802.11v: on

802.11k: on

UAPSD: on

2.4G Client Rate Control: off

Figure6-3-14 Client Isolate

802.11r: Select to enable IEEE 802.11r (Fast BSS Transition). The Fast BSS Transition mechanism minimizes the delay when a client transitions from one BSS to another within the same cluster, illustrated in Figure6-3-15.

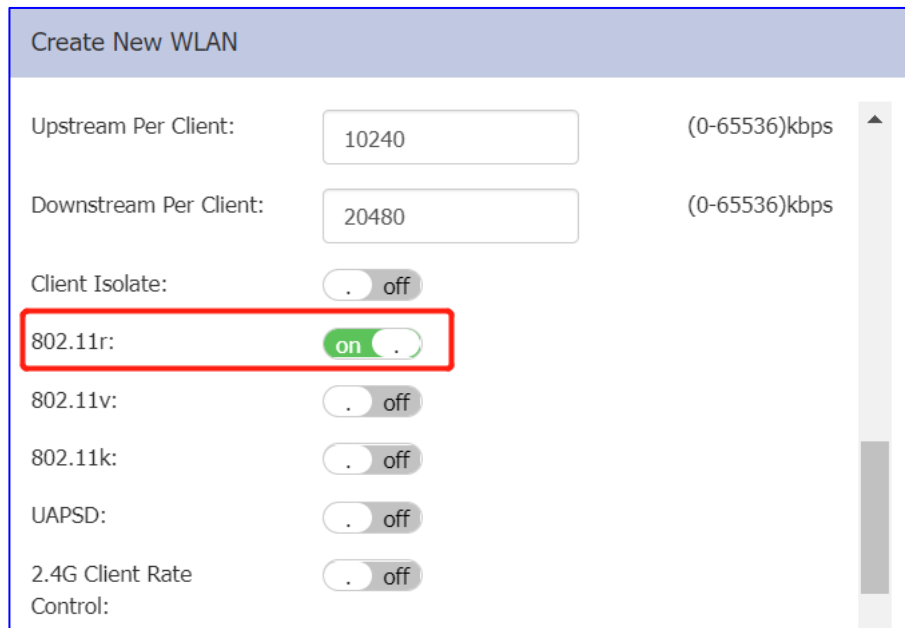


Figure6-3-15 11r Configuration

802.11k/v: Enables/Disables 802.11k/v, they are enabled by default., 802.11k/11v is working together with “Roaming RSSI Threshold”, which is a way for roaming optimization, while it mainly relies on the client behavior during the roaming, illustrated in Figure6-3-16.

- When enabling 802.11k/11v on the SSID, “Roaming RSSI Threshold” is the trigger of 802.11k/11v message exchanges between AP and Clients.
- When DAP detects the SNR value of device is lower than “Roaming RSSI Threshold”, 802.11k event will be sent to this device. If it’s an 802.11k compliant device, it will respond to DAP with a packet which contains the RF scanned information from this device.
- Based on the data received, DAP will calculate from the Wi-Fi driver to check what would be the best BSSID for this device to roam, and then send the best SSID information to this device with 802.11v event.

- Finally, the device will choose if it's going to roam or not. If roams, still the device will choose if it takes the BSSID from DAP's recommendation in 802.11v event, or some other BSSID to roam, which cannot be managed from AP side.

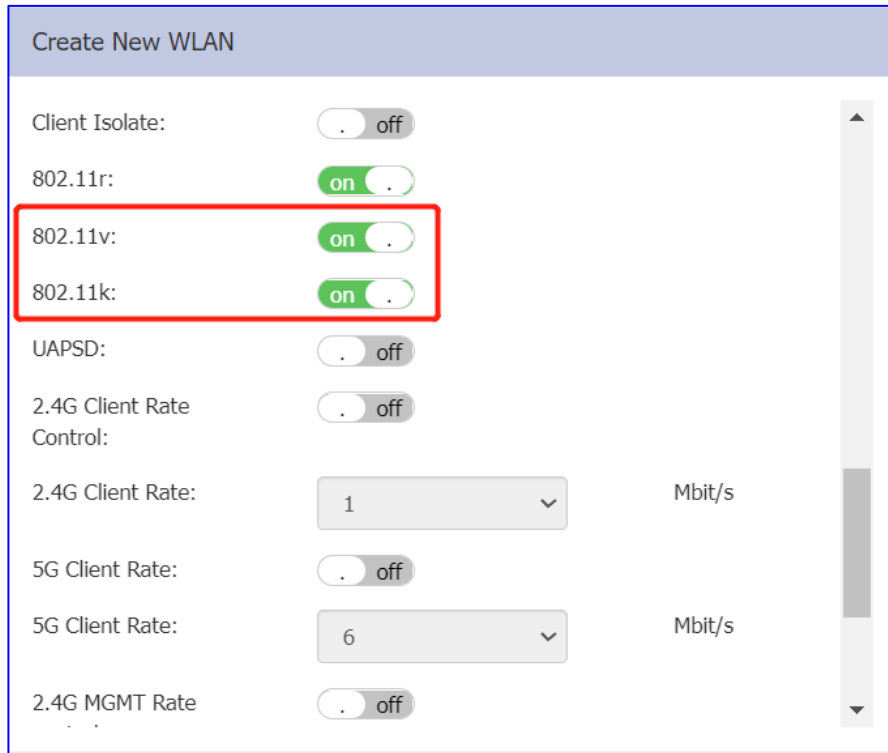


Figure6-3-16 802.11k/v Configuration

OKC: If OKC is enabled, a cached pairwise master key (PMK) will be used when the client roams to a new AP. This allows faster roaming of clients without the need for a complete 802.1x authentication procedure, it is only supported in Enterprise mode and disabled by default, illustrated in Figure6-3-17.

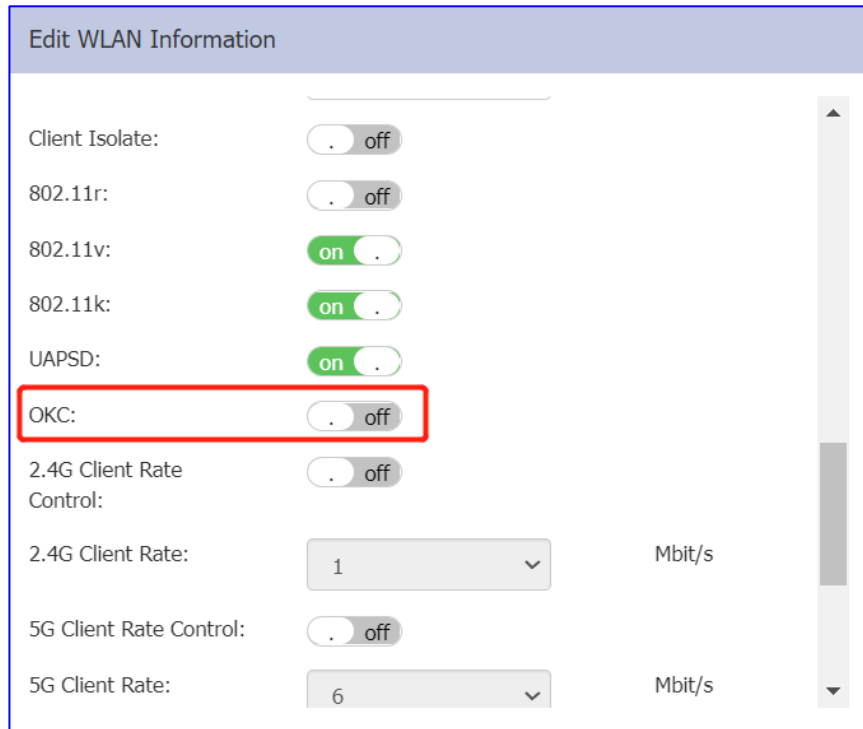


Figure6-3-17 OKC Configuration

UAPSD: Unscheduled automatic power save delivery (U-APSD) is a QoS facility that is defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending the battery life, this feature reduces the latency of traffic flow that is delivered over the wireless media. U-APSD does not require the client to poll each individual packet that is buffered at the access point; it allows delivery of multiple downlink packets by sending a single uplink trigger packet, shown in Figure6-3-18

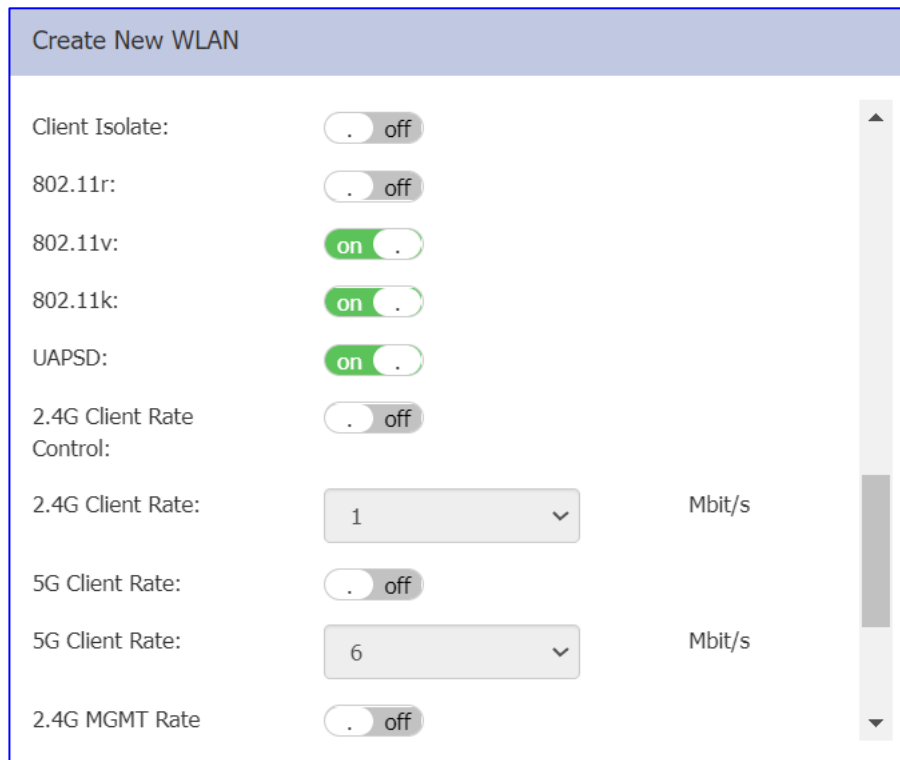


Figure6-3-18 UAPSD Configuration

2.4G Client Rate Control: Enables/Disables 2.4G band accessing control based on client data rate, it is disabled by default, shown in Figure6-3-19.

2.4G Client Rate: 2.4G band client with lower data speed will not be allowed to access, recommended value 12, shown in Figure6-3-19.

5G Client Rate Control: Enables/Disables 5G band accessing control based on client data rate, it is disabled by default, shown in Figure6-3-19.

5G Client Rate: 5G band client with lower data speed will not be allowed to access, recommended value 24, shown in Figure6-3-19.

The screenshot shows the 'Create New WLAN' configuration interface. It features several sections for rate control:

- 2.4G Client Rate Control:** A toggle switch is turned 'on'. Below it, a dropdown menu is set to '12' Mbit/s.
- 5G Client Rate:** A toggle switch is turned 'on'. Below it, a dropdown menu is set to '24' Mbit/s.
- 2.4G MGMT Rate control:** A toggle switch is turned 'on'. Below it, a dropdown menu is set to '6' Mbit/s.
- 5G MGMT Rate control:** A toggle switch is turned 'on'. Below it, a dropdown menu is set to '12' Mbit/s.

At the bottom of the form, there are two buttons: 'Cancel' (orange) and 'Save' (blue). A vertical scrollbar is visible on the right side of the configuration area.

Figure6-3-19 Client Rate configuration

2.4G MGMT Rate Control: Enables/Disables 2.4G band wireless management frame rate control, it is disabled by default, shown in Figure6-3-20.

2.4G MGMT Rate: 2.4G band wireless management frame transmit rate, higher value means less coverage, lower value means larger coverage, shown in Figure6-3-20.

5G MGMT Rate Control: Enables/Disables 5G band wireless management frame rate control, it is disabled by default, shown in Figure6-3-20.

5G MGMT Rate: 5G band wireless management frame transmit rate, higher value means less coverage, lower value means larger coverage, shown in Figure6-3-20.

Create New WLAN

2.4G Client Rate Control: on

2.4G Client Rate: Mbit/s

5G Client Rate: on

5G Client Rate: Mbit/s

2.4G MGMT Rate control: on

2.4G MGMT Rate: Mbit/s

5G MGMT Rate control: on

5G MGMT Rate: Mbit/s

Figure6-3-20 Management Rate configuration

DTIM Interval: Delivery Traffic Indication Map Interval, default value is 1; the higher value, the better the terminal's power saving, but the higher the multicast delay. Conversely, lower values result in worse power saving but lower multicast delay, shown in Figure6-3-21.

Create New WLAN

5G Client Rate: Mbit/s

2.4G MGMT Rate control: off

2.4G MGMT Rate: Mbit/s

5G MGMT Rate control: off

5G MGMT Rate: Mbit/s

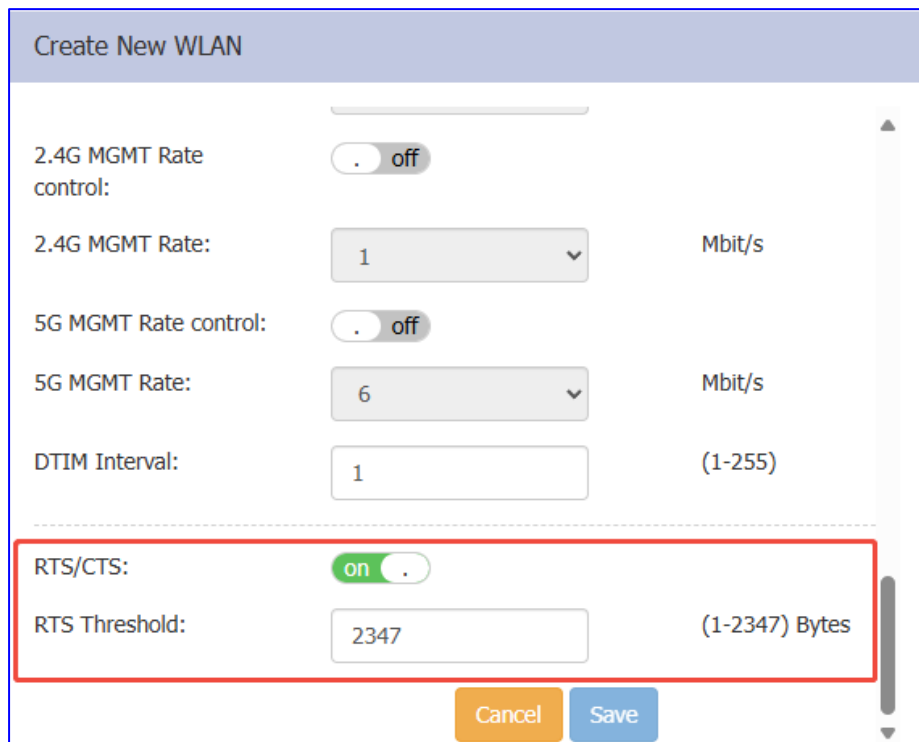
DTIM Interval: (1-255)

RTS/CTS: off

Figure6-3-21 DTIM Interval configuration

RTS/CTS: Enables/Disables RTS/CTS frame transmission, it is disabled by default. Enabling it can better resolve the conflicts caused by hidden nodes. shown in Figure6-3-22.

RTS Threshold: Threshold for sending RTS frames, default value is 2347, shown in Figure6-3-22.



The screenshot displays the 'Create New WLAN' configuration window. It features several settings:

- 2.4G MGMT Rate control:** A toggle switch set to 'off'.
- 2.4G MGMT Rate:** A dropdown menu set to '1' Mbit/s.
- 5G MGMT Rate control:** A toggle switch set to 'off'.
- 5G MGMT Rate:** A dropdown menu set to '6' Mbit/s.
- DTIM Interval:** A text input field set to '1' (range 1-255).
- RTS/CTS:** A toggle switch set to 'on', highlighted with a red box.
- RTS Threshold:** A text input field set to '2347' (range 1-2347) Bytes, also highlighted with a red box.

At the bottom of the window, there are 'Cancel' and 'Save' buttons.

Figure6-3-22 RTS/CTS configuration

6.4 Modify WLAN Configuration

In WLAN Configuration window, you can modify the WLAN by clicking the '✎' button, all the configurable WLAN parameters will be displayed on the right side of WLAN Configuration window, Click '**Cancel**' button to cancel the modification or click '**Save**' button to save the configuration, shown in Figure6-4-1.

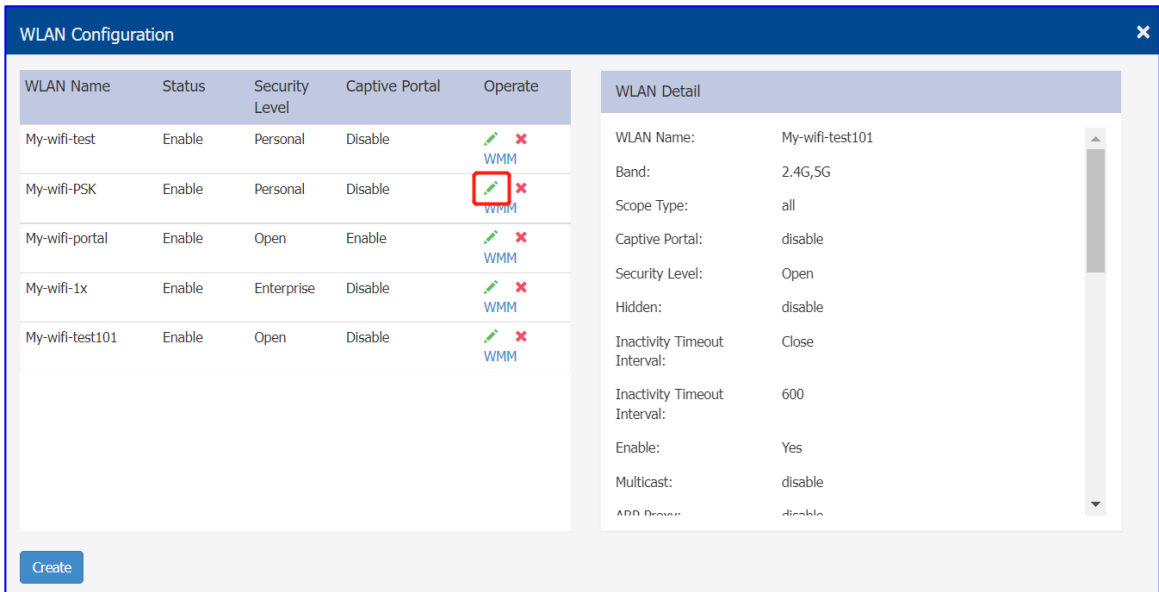


Figure6-4-1 Modify WLAN Configuration

6.5 Delete your WLAN

In WLAN Configuration window, you can delete a WLAN by clicking the ‘✖’ button as required, shown in Figure6-5-1;

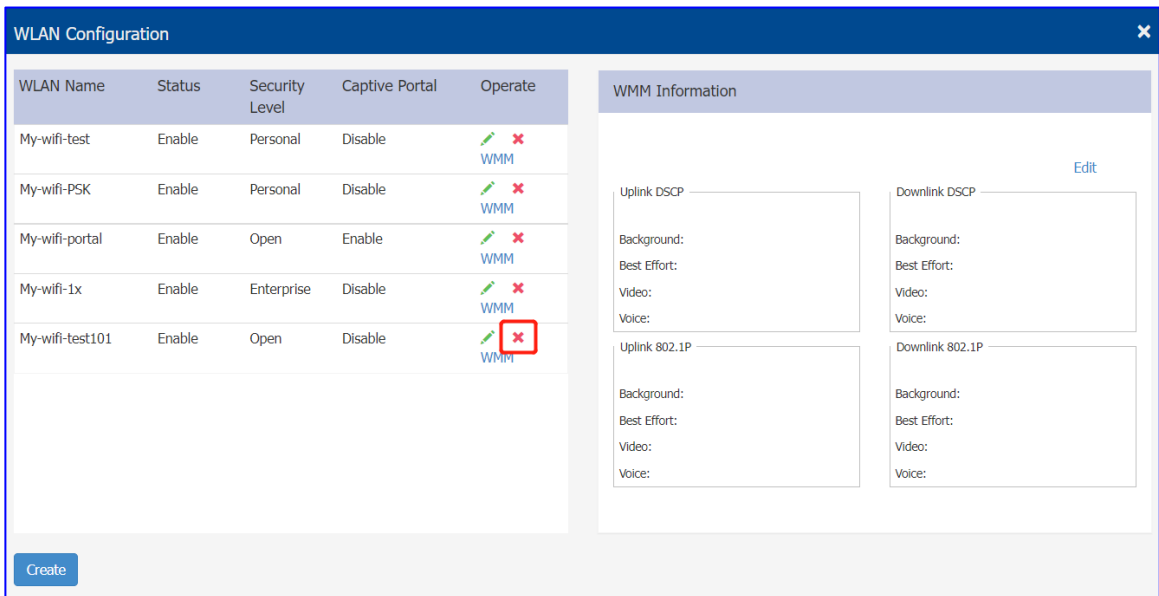
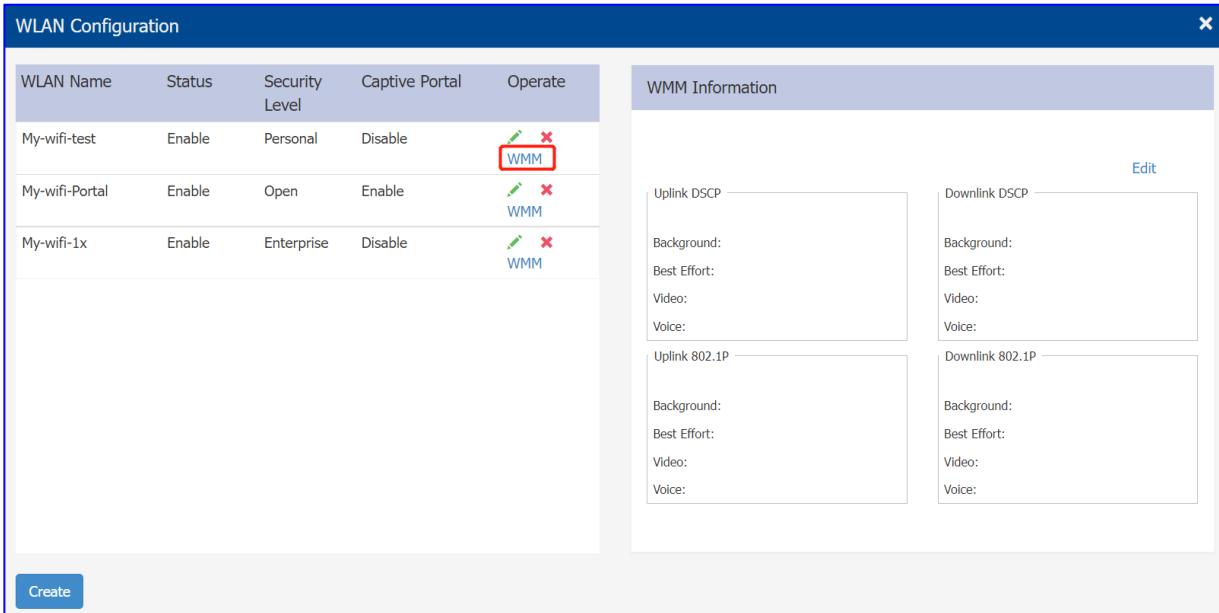


Figure6-5-1 Delete a WLAN

6.6 WMM Configuration

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic Quality of Service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to four Access Categories (AC): voice (AC_VO), video (AC_VI), best effort (AC_BE), and background (AC_BK). It is suitable for well-defined applications that require QoS, such as Voice over IP (VoIP) on Wi-Fi phones.

WMM based on each SSID, different SSID has its own rules, you can edit the mapping relationship between DSCP/802.1p values and WMM priorities for a WLAN on DAP, shown in Figure6-6-1.



The screenshot displays the 'WLAN Configuration' interface. On the left, a table lists WLANs with columns for Name, Status, Security Level, Captive Portal, and Operate. The 'My-wifi-test' WLAN is highlighted, and its 'Operate' column contains a 'WMM' button. On the right, the 'WMM Information' panel is visible, featuring an 'Edit' link and four configuration sections: Uplink DSCP, Downlink DSCP, Uplink 802.1P, and Downlink 802.1P. Each section includes input fields for Background, Best Effort, Video, and Voice. A 'Create' button is located at the bottom left of the interface.




WLAN Name	Status	Security Level	Captive Portal	Operate
My-wifi-test	Enable	Personal	Disable	
My-wifi-Portal	Enable	Open	Enable	
My-wifi-1x	Enable	Enterprise	Disable	

Figure6-6-1 WMM Configuration

7 DAP Management

This chapter describes how to configure and manage DAPs in the cluster. The DAP cluster solution is a controller-less based architecture. The DAPs can establish an autonomous cluster, in which there are three types of AP roles, Primary Virtual Management (PVM), Secondary Virtual Management (SVM) and MEMBER. This chapter describes how to manage the cluster and how to check, backup, restore AP configuration and upgrade firmware via Web GUI.

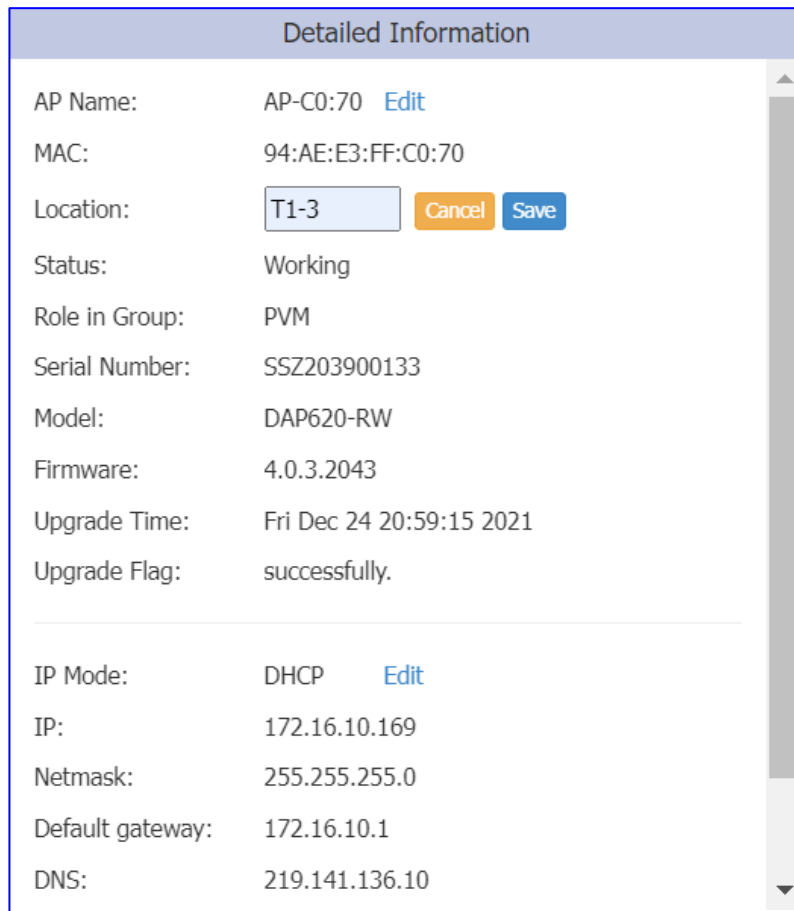
DAP Management procedures described in this chapter includes:

- [Check Detailed Information](#)
- [Modify AP Name and Location](#)
- [Add a New AP to Cluster](#)
- [Remove an AP from the Cluster](#)
- [Allow an AP to Join the Cluster](#)
- [Replace a Current AP in Cluster](#)
- [Modify IP Address](#)
- [Convert from Cluster Mode to DAC/BWO Mode](#)
- [Check current configuration](#)
- [Reboot DAP](#)
- [Clear Configuration](#)
- [Backup and Restore Configuration](#)
- [Upgrade AP Firmware](#)
- [Locate or turn on/off LED](#)
- [AP Advanced Configuration](#)

- [AP works as Gateway](#)

7.1 Check Detailed Information

The DAP detailed information will be displayed by click the related AP item, by default, the detailed information of PVM will be displayed in the right window of DAP configuration page if no DAP selected, The AP Name, Location, IP Mode and AP Mode also can be set in this page, illustrated in Figure7-1-1

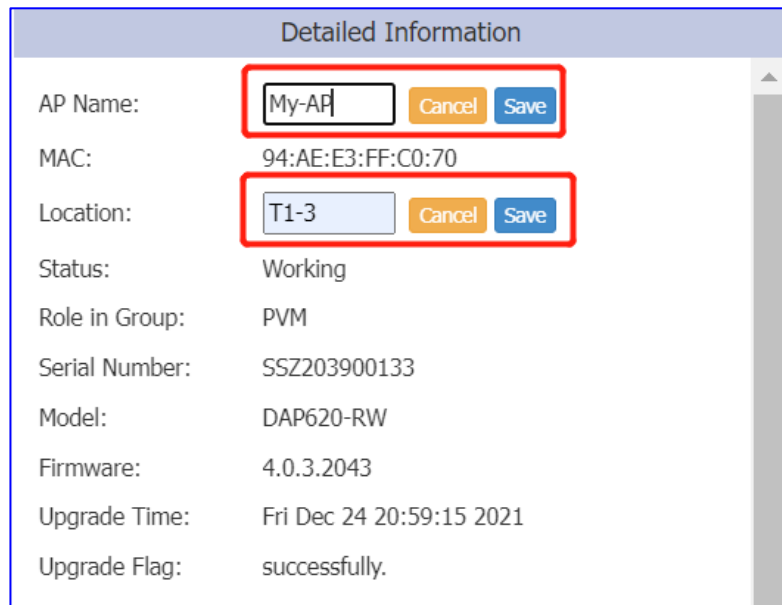


Detailed Information	
AP Name:	AP-C0:70 Edit
MAC:	94:AE:E3:FF:C0:70
Location:	<input type="text" value="T1-3"/> Cancel Save
Status:	Working
Role in Group:	PVM
Serial Number:	SSZ203900133
Model:	DAP620-RW
Firmware:	4.0.3.2043
Upgrade Time:	Fri Dec 24 20:59:15 2021
Upgrade Flag:	successfully.
<hr/>	
IP Mode:	DHCP Edit
IP:	172.16.10.169
Netmask:	255.255.255.0
Default gateway:	172.16.10.1
DNS:	219.141.136.10

Figure7-1-1 DAP Detailed Information

7.2 Modify AP Name and Location

Click on “Edit” to modify the **AP Name** and **Location**, and then enter a name and location information to identify the specific AP, illustrated in Figure7-2-1. By default, the DAP is named with the last two bytes of its MAC address, for example, AP-C0:70.



Detailed Information	
AP Name:	<input type="text" value="My-AP"/> <input type="button" value="Cancel"/> <input type="button" value="Save"/>
MAC:	94:AE:E3:FF:C0:70
Location:	<input type="text" value="T1-3"/> <input type="button" value="Cancel"/> <input type="button" value="Save"/>
Status:	Working
Role in Group:	PVM
Serial Number:	SSZ203900133
Model:	DAP620-RW
Firmware:	4.0.3.2043
Upgrade Time:	Fri Dec 24 20:59:15 2021
Upgrade Flag:	successfully.

Figure7-2-1 Modify AP Name and AP Location

7.3 Add a New AP to Cluster

To add a new AP to the Cluster, please ensure that the PVM is not in the 'Down' state and the new AP has the same "Cluster ID" with PVM. If the PVM is down, please upgrade the SVM to be the PVM before plugging in the new AP.

There are 2 ways to check the "Cluster ID" information:

- Login the AP and find the "Cluster ID" in System window, illustrated in Figure7-3-1:

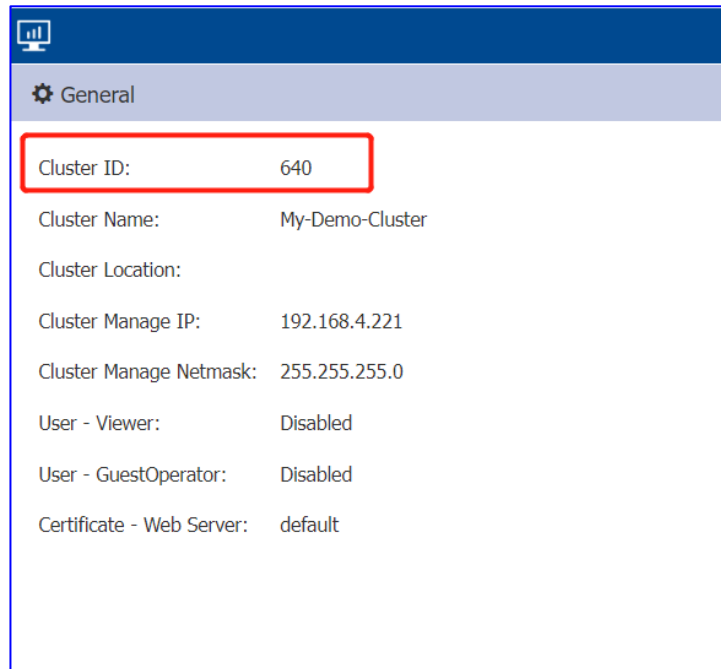


Figure7-3-1 Checking Cluster ID in Web GUI

- Checking the Cluster ID information in CLI, illustrated in Figure7-3-2:

```

support@AP-87:30:~$
support@AP-87:30:~$ cat /var/config/cluster.conf
{
    "cluster":{
        "cluster_id":"640",
        "cluster_name":"My-Demo-Cluster",
        "cluster_priority":"0",
        "cluster_vip":"192.168.4.221",
        "cluster_netmask":"255.255.255.0",
        "cluster_vip6":"::"
    }
}
support@AP-87:30:~$

```

Figure7-3-2 Checking Cluster ID in CLI

7.4 Remove an AP from the Cluster

An AP can be removed from the AP Cluster list (PVM/SVM/MEMBER) when it selected and clicking “kick off” button, illustrated in Figure7-4-1.

Then the AP enters the Cluster blacklist, if it is not disconnected from the network it will move to the 'Joining' state, illustrated in Figure7-4-2, and without authorization is not permitted to be a member of Cluster again.

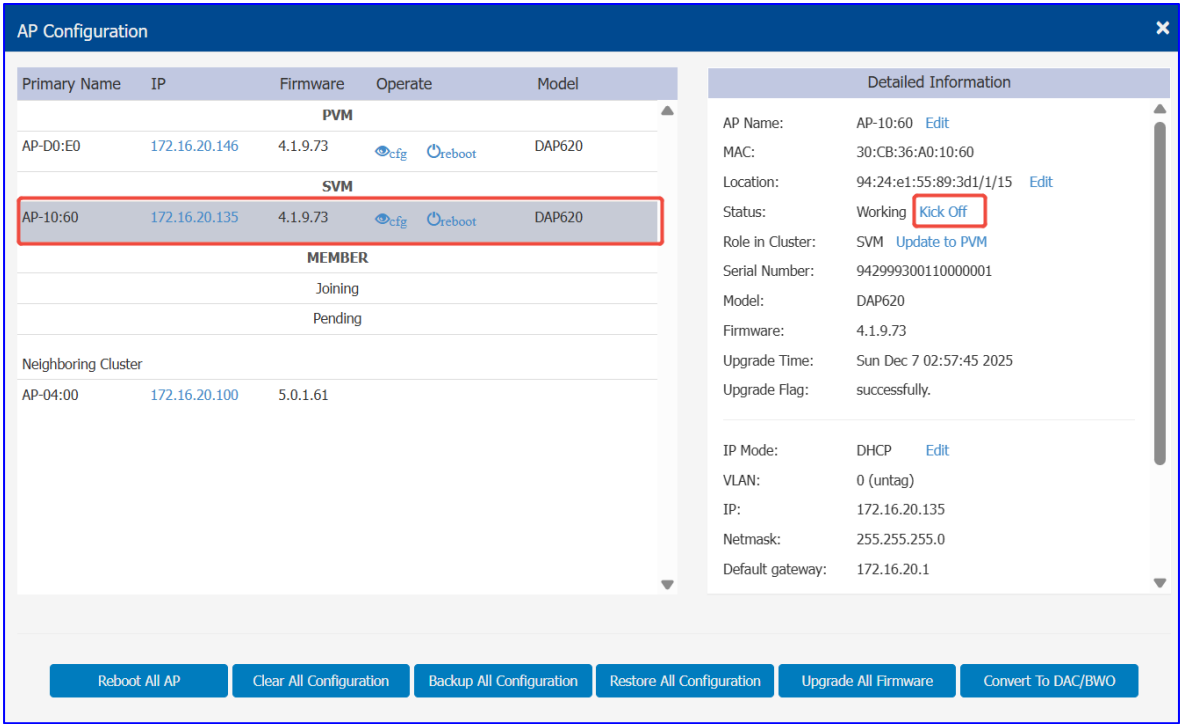


Figure7-4-1 kick off an AP in Cluster

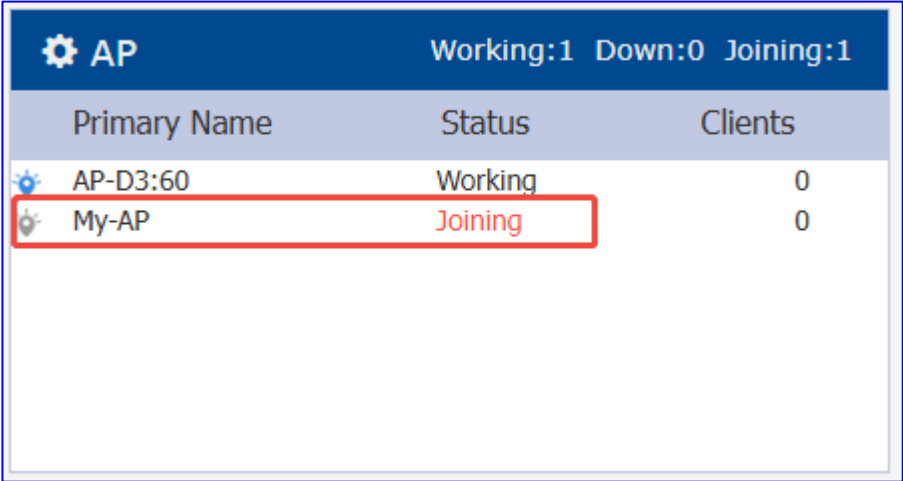


Figure7-4-2 AP in "Joining" state after kicked off

7.5 Allow an AP to Join the Cluster

In the displayed AP Configuration screen, an AP in 'Joining' state is in the Cluster block list; the 'Accept' operation and corresponding "Cluster ID" lets it re-join the cluster and removes it from the cluster block list, illustrated in Figure7-5-1.

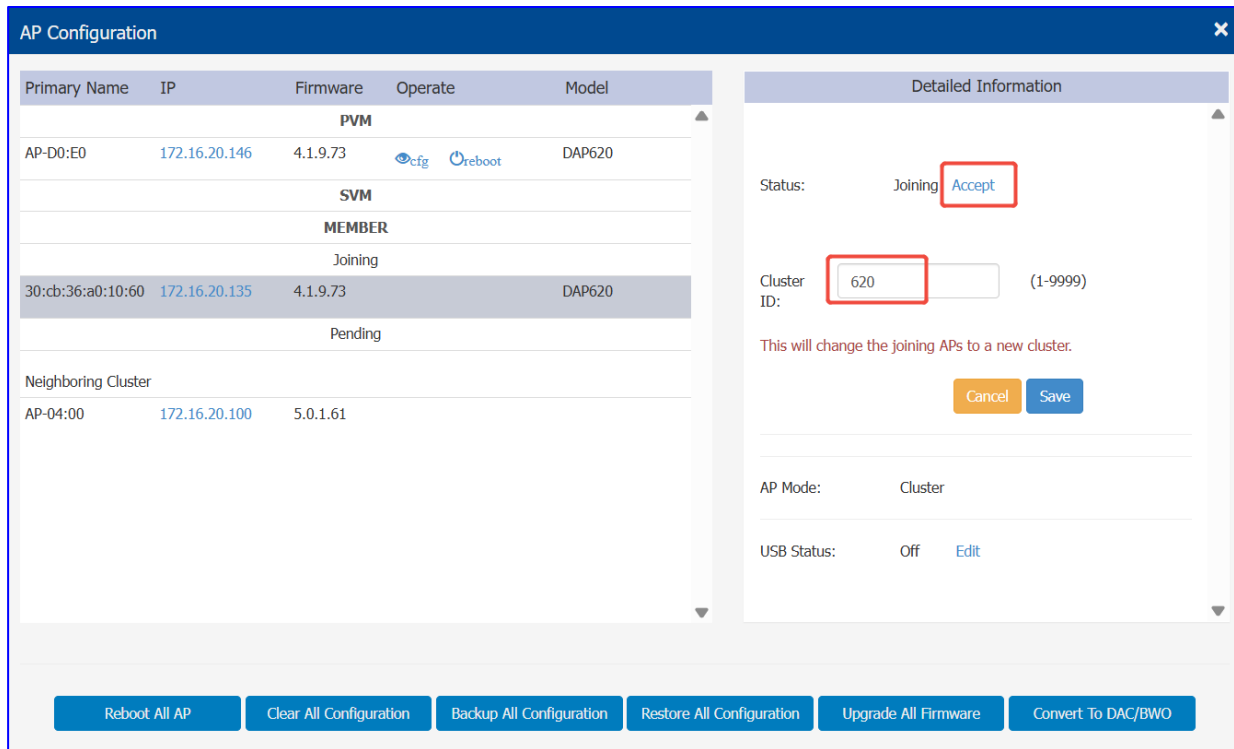


Figure7-5-1 Accept an AP Re-join Cluster

7.6 Replace a Current AP in Cluster

There are 2 cases of replacing the AP in Cluster:

- To replace the current PVM:

Upgrade the SVM to the PVM before disconnecting the old PVM. Then replace the old PVM with a new DAP.

- To replace the SVM or a MEMBER of the Cluster:

Disconnect and replace the SVM or MEMBER directly with a new DAP, users on other DAPs will not be affected.

7.7 Modify IP Address

DAP supports both static IP address and a dynamic IP addresses obtained from DHCP Server, DHCP mode was used by default, Click “Edit” to modify the IP address show as Figure7-7-1 and Figure7-7-2.

Detailed Information	
AP Name:	My-AP Edit
MAC:	30:CB:36:A0:10:60
Location:	T1_3 Edit
Status:	Working
Role in Cluster:	PVM
Serial Number:	942999300110000001
Model:	DAP620
Firmware:	4.1.9.65
Upgrade Time:	Thu Oct 1 13:44:23 2025
Upgrade Flag:	successfully.
<hr/>	
IP Mode:	DHCP Edit
IP:	192.168.20.62
Netmask:	255.255.254.0
Default gateway:	192.168.21.254
DNS:	192.168.10.31

Figure7-7-1 Edit AP IP Mode

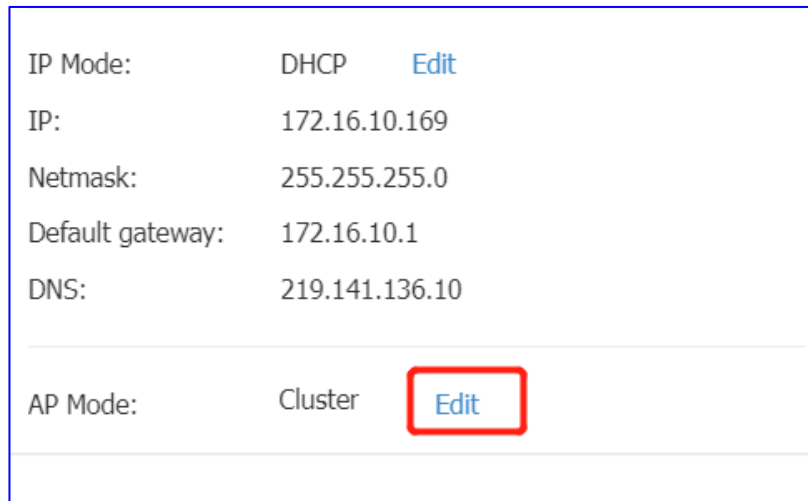
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static	Cancel	Save
IP:	<input type="text" value="192.168.8.41"/>		
Netmask:	<input type="text" value="255.255.255.0"/>		
Default gateway:	<input type="text" value="192.168.8.1"/>		
DNS:	<input type="text" value="192.168.8.1"/>		

Convert from Cluster Mode to DAC/BWO Mode

DAP can be converted to DAC/BWO mode on web GUI from cluster mode:

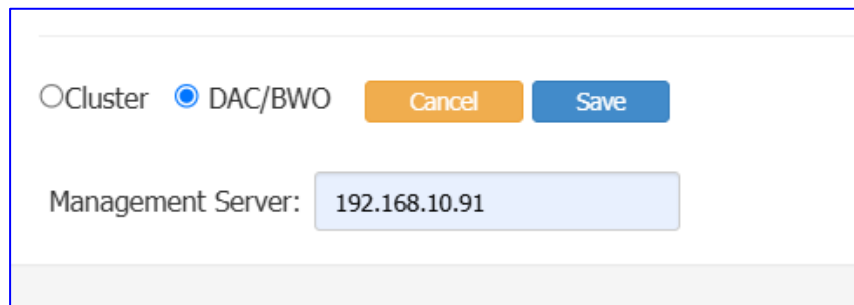
- **Convert single AP to DAC/BWO mode:**

Click “Edit” on DAP detailed information page—>select “DAC/BWO”—> input the DAC or BWO IP address and save configuration, after a required of AP reboot, the specific single DAP in the cluster will convert to the DAC/BWO mode, illustrated in Figure7-8-1 and Figure7-8-2.



IP Mode:	DHCP	Edit
IP:	172.16.10.169	
Netmask:	255.255.255.0	
Default gateway:	172.16.10.1	
DNS:	219.141.136.10	
<hr/>		
AP Mode:	Cluster	Edit

Figure7-8-1 Edit AP Mode



Cluster
 DAC/BWO
 [Cancel](#)
[Save](#)

Management Server:

Figure7-8-2 Configure DAC/BWO Mode

- **Convert all DAPs in the Cluster to DAC/BWO mode:**

Click **“Convert To DAC/BWO”** in the bottom right-hand corner of AP Configuration page ,input the DAC/BWO IP address and save configuration ,after a required of DAP reboot ,all the DAPs in the cluster will convert to the DAC/BWO mode, illustrated in Figure7-8-3 and Figure7-8-4.

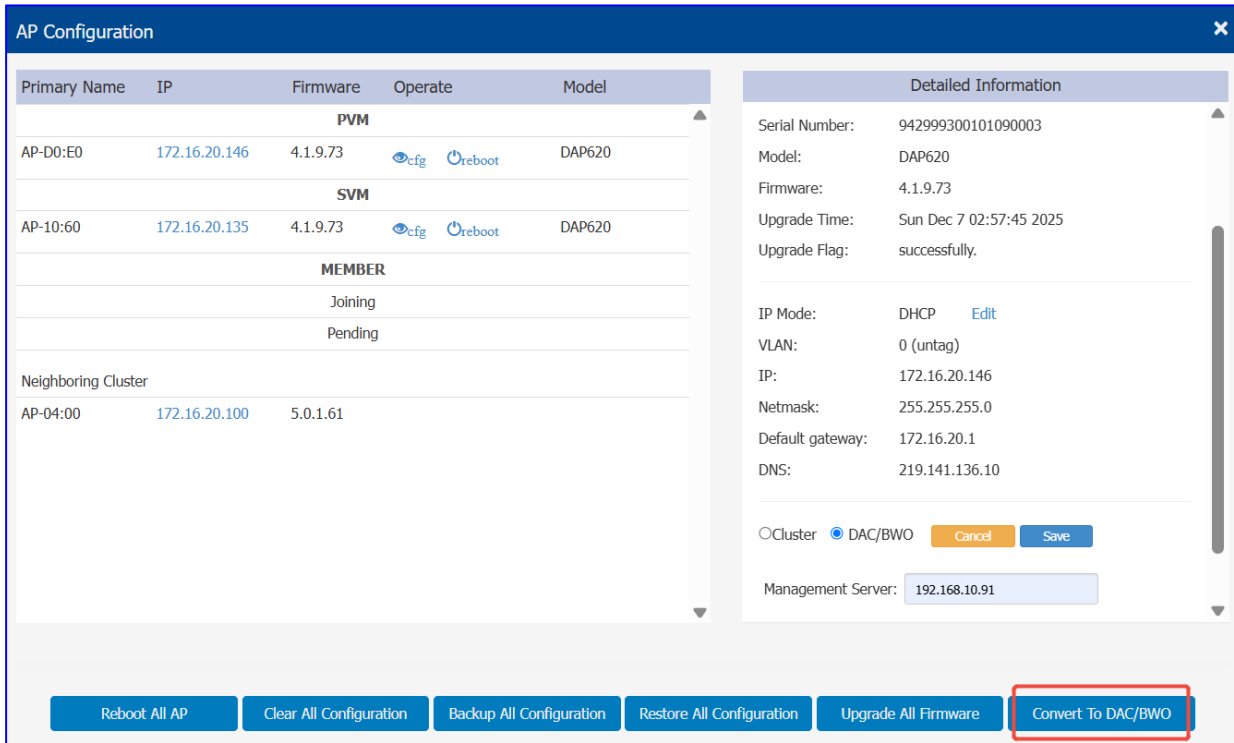


Figure7-8-3 Convert To DAC/BWO

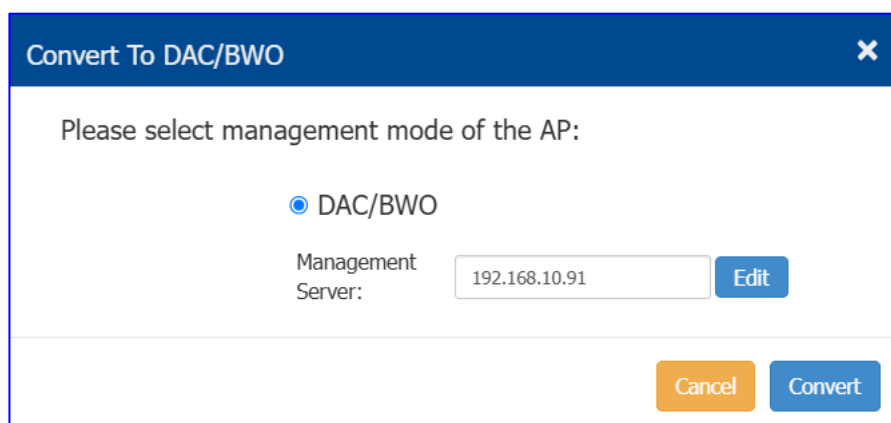



Figure7-8-4 Configure DAC/BWO Mode



Note

All the configuration under cluster mode will be cleared after DAP convert to DAC/BWO mode. DAP will get new configuration from DAC/BWO.

7.8 Check current configuration

Click  to check the configuration in the AP Configuration window, illustrated in Figure7-9-1:

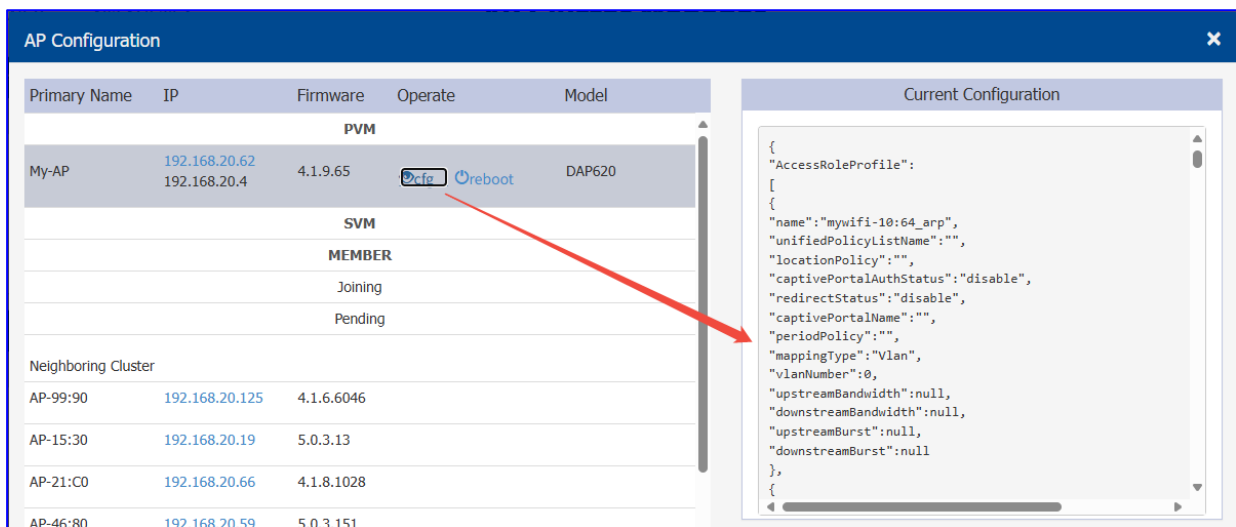



Figure7-9-1 Check AP Current Configuration

7.9 Reboot DAP

The DAP can be rebooted manually base on the actual requirement:

- **Reboot one single DAP in the cluster**

Click  of the AP item in the AP Configuration window, the specific AP will be reboot as required, shown in Figure7-10-1.

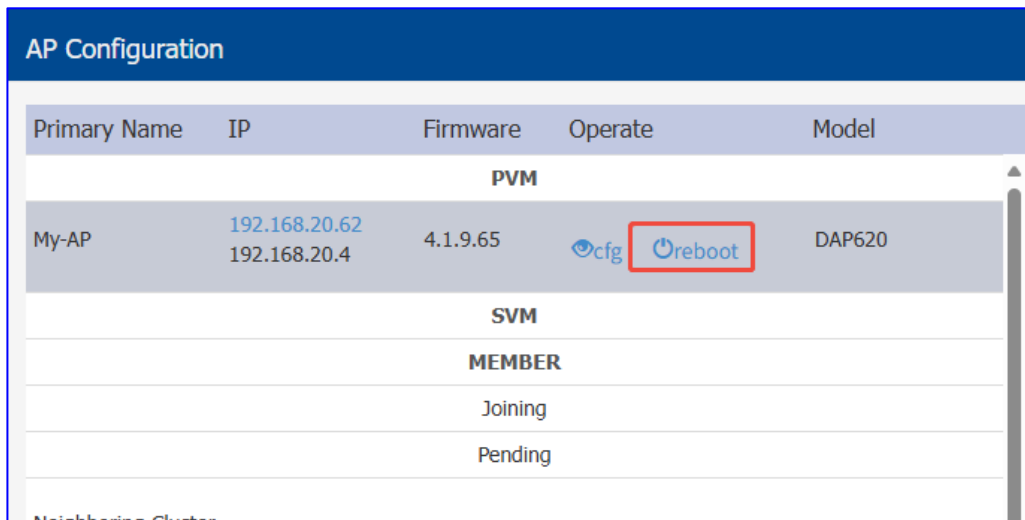


Figure7-10-1 Reboot an AP in Cluster

- **Reboot All DAPs in the cluster**

Click “Reboot All AP” button in the bottom of left-hand corner of AP Configuration window, all the APs in the cluster will be rebooted as required, shown in Figure7-10-2:

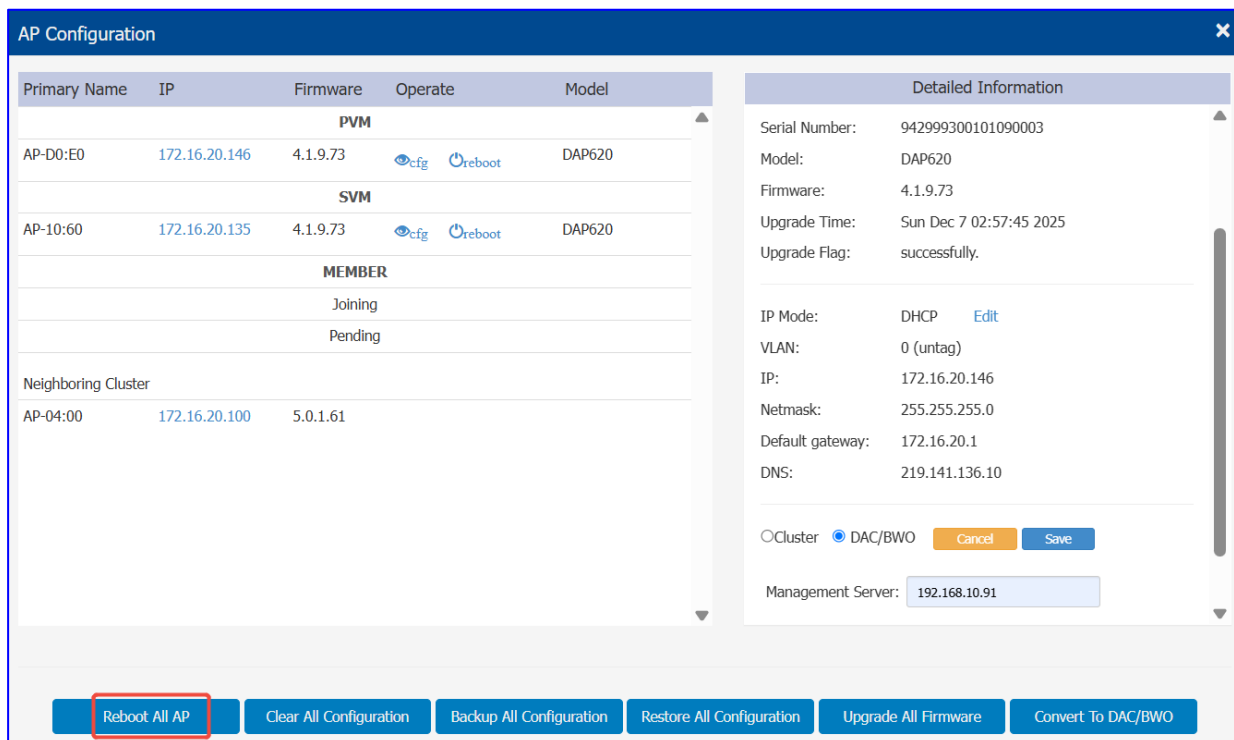
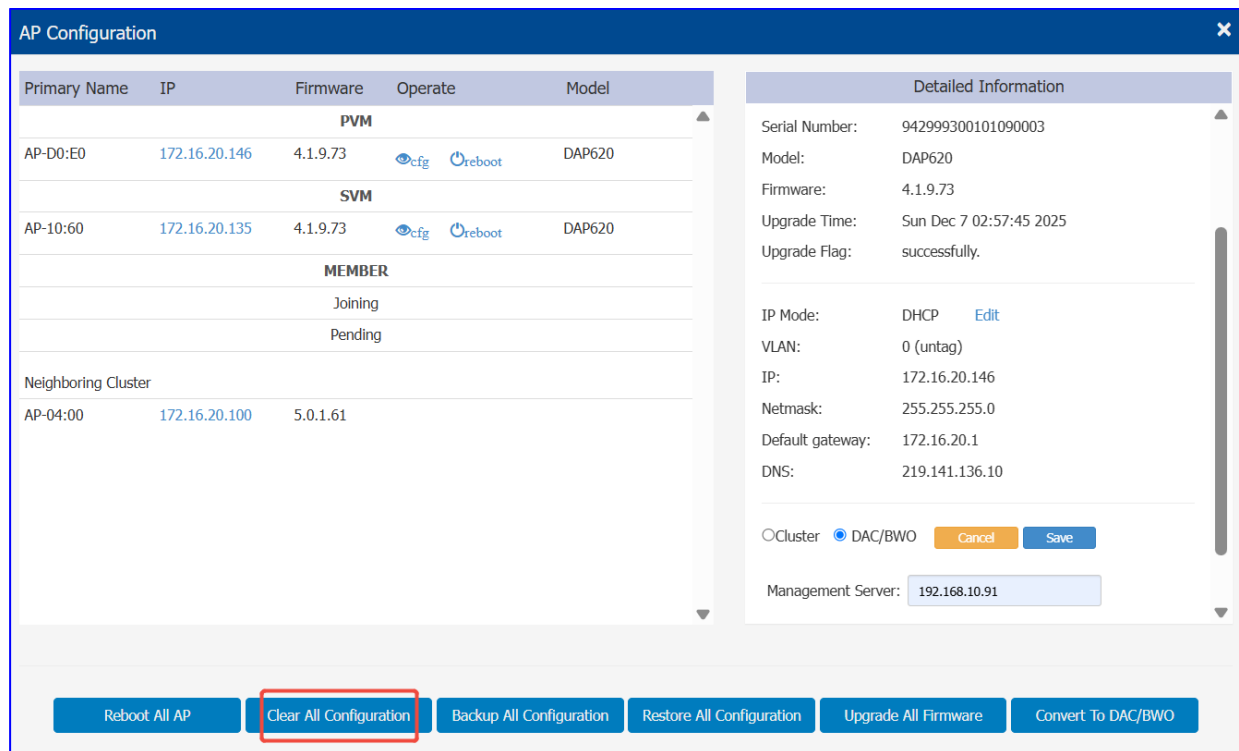


Figure7-10-2 Reboot All APs in the Cluster

7.10 Clear Configuration

In case of some situation, below methods can help to clear AP configuration and make the AP back to 'factory settings':

Click "Clear All Configuration" button in AP Configuration window, shown in Figure7-11-1.



The screenshot shows the 'AP Configuration' window. It features a table with columns: Primary Name, IP, Firmware, Operate, and Model. The table is divided into sections: PVM, SVM, MEMBER, and Neighboring Cluster. The PVM section contains one entry: AP-D0:E0 with IP 172.16.20.146, Firmware 4.1.9.73, and Model DAP620. The SVM section contains one entry: AP-10:60 with IP 172.16.20.135, Firmware 4.1.9.73, and Model DAP620. The MEMBER section has 'Joining' and 'Pending' entries. The Neighboring Cluster section contains one entry: AP-04:00 with IP 172.16.20.100 and Firmware 5.0.1.61. To the right of the table is a 'Detailed Information' panel showing fields for Serial Number, Model, Firmware, Upgrade Time, Upgrade Flag, IP Mode, VLAN, IP, Netmask, Default gateway, and DNS. At the bottom of the window, there are several buttons: 'Reboot All AP', 'Clear All Configuration' (highlighted with a red box), 'Backup All Configuration', 'Restore All Configuration', 'Upgrade All Firmware', and 'Convert To DAC/BWO'.

Figure7-11-1 Clear All Configuration

below more two ways also can make DAP back to 'factory settings':



Note

- Long pressing the "reset" button for at least 6 seconds
- Command "ssudo firstboot" and "ssudo reboot" input via Console or SSH connection under 'support' account (default password :support\aos2016)

7.11 Backup and Restore Configuration

In the AP Configuration window, you can backup and restore the cluster configuration, shown in Figure7-12-1.

- The configuration file can be downloaded by clicking **“Backup All Configuration”** button in the bottom of the AP Configuration window, The AP configuration file was named as “pub-config.tar”.
- The configuration file also can be uploaded to the DAP cluster by clicking **“Restore All Configuration”** button in the bottom of the AP Configuration window.

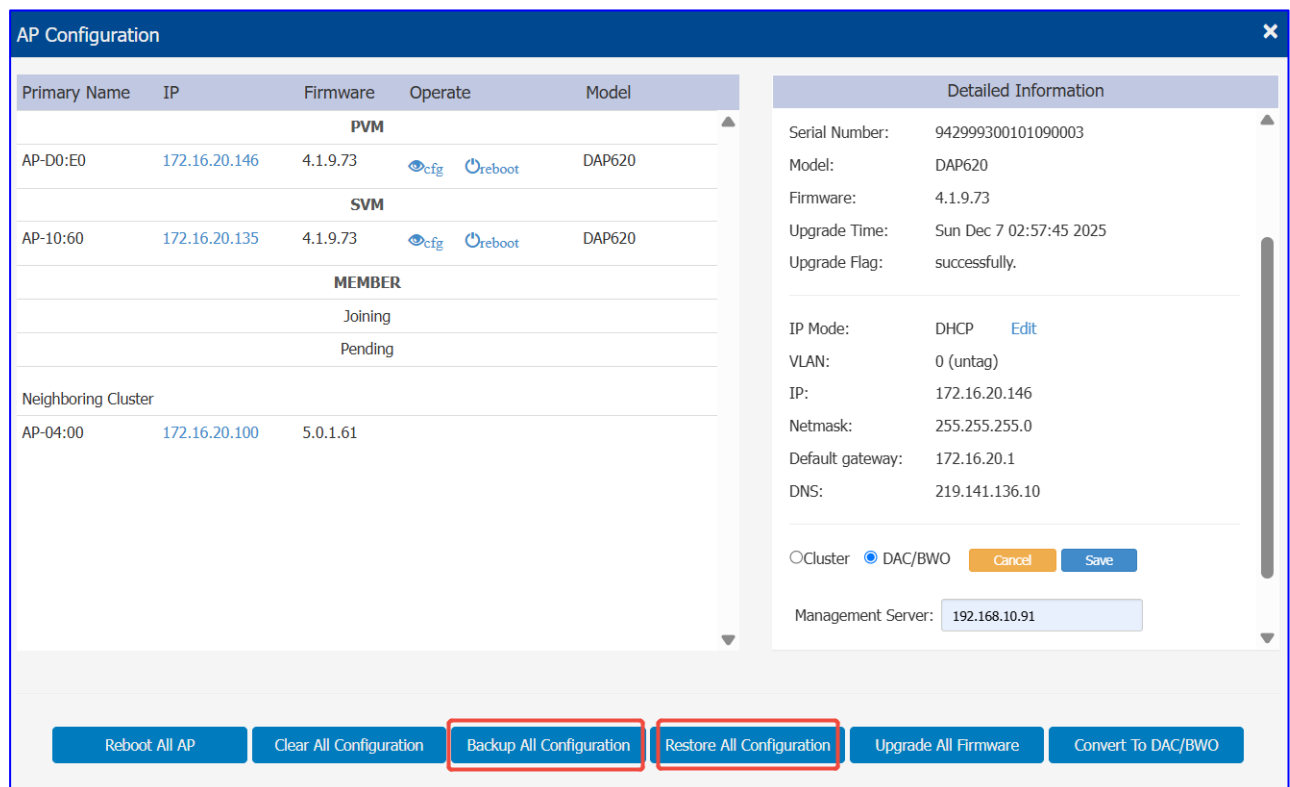


Figure7-12-1 Backup and Restore AP configuration

7.12 Upgrade AP Firmware

Before upgrading the DAP you should prepare the firmware file to be upgraded. You can download the firmware file from <https://hirschmann-it->

support.belden.com/en/downloads/dragonfly-wireless and save it in the local disk of the PC you are using to connect to the DAP or save the firmware file in a remote TFTP or SFTP server.

Click the “Upgrade all Firmware” button in the AP Configuration window, the Multi-mode Upgrade page will be popped up, illustrated in Figure7-13-1.

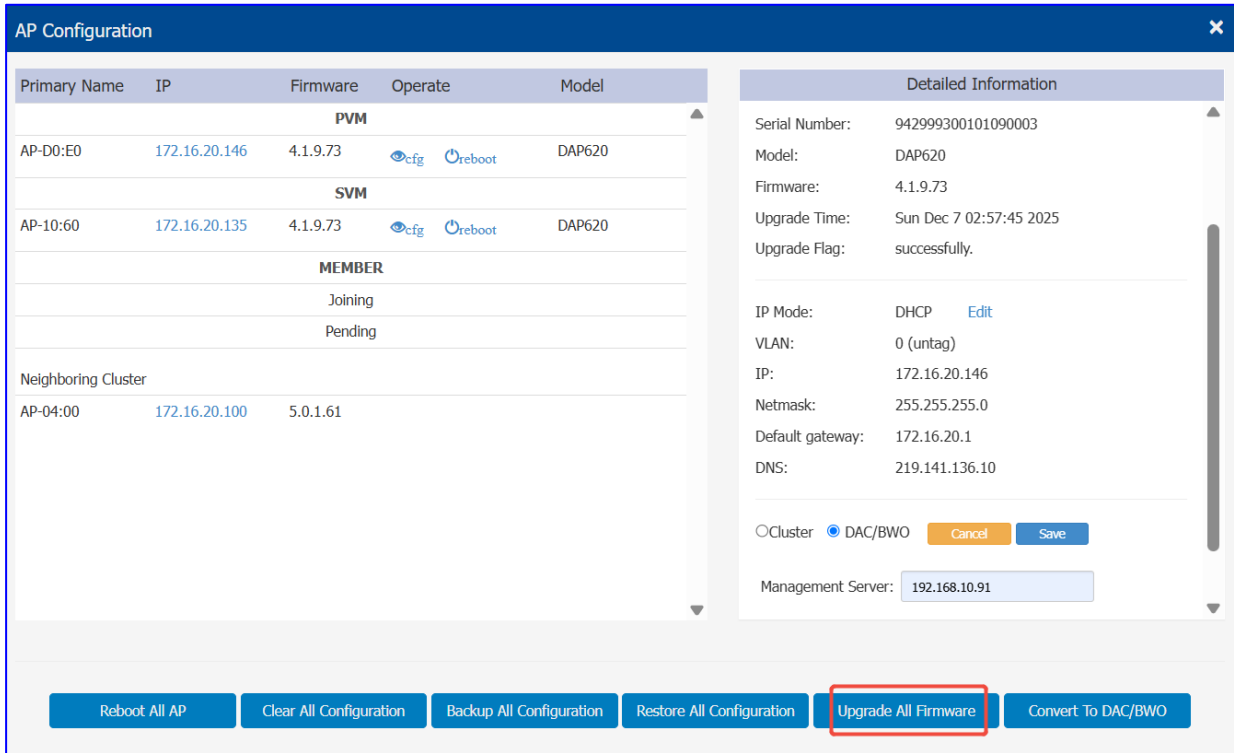


Figure7-13-1 Go to AP upgrade page

7.13.1 Upgrade all DAPs

To upload separate DAP firmware for each DAP model and upgrade, please select the related DAP firmware file according the AP model to be upgraded in Multi-model Upgrade page; you can upgrade multiple models of APs at the same time, shown in Figure7-13-1-1. Generally, it takes approximately five minutes to upgrade the AP firmware.

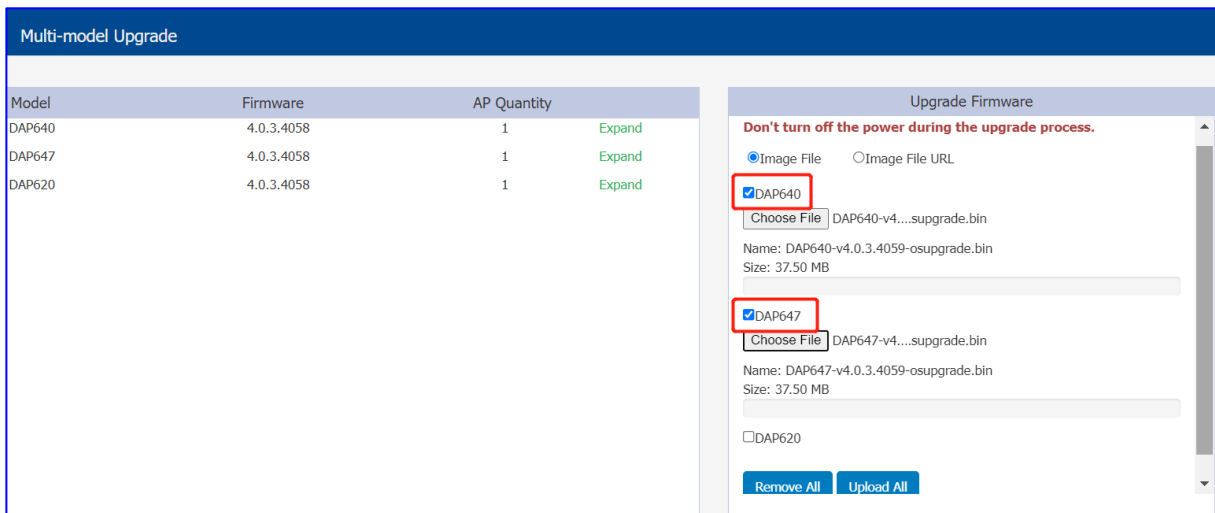


Figure7-13-1-1 Upgrade All Firmware

There are three ways to upload AP firmware:

- Please select "Image File" option and upload the firmware from local image file and click "Upload All" button to perform the upgrade operation, you can also cancel the upgrade operation by clicking "Remove All" button, shown in Figure7-13-1-2:

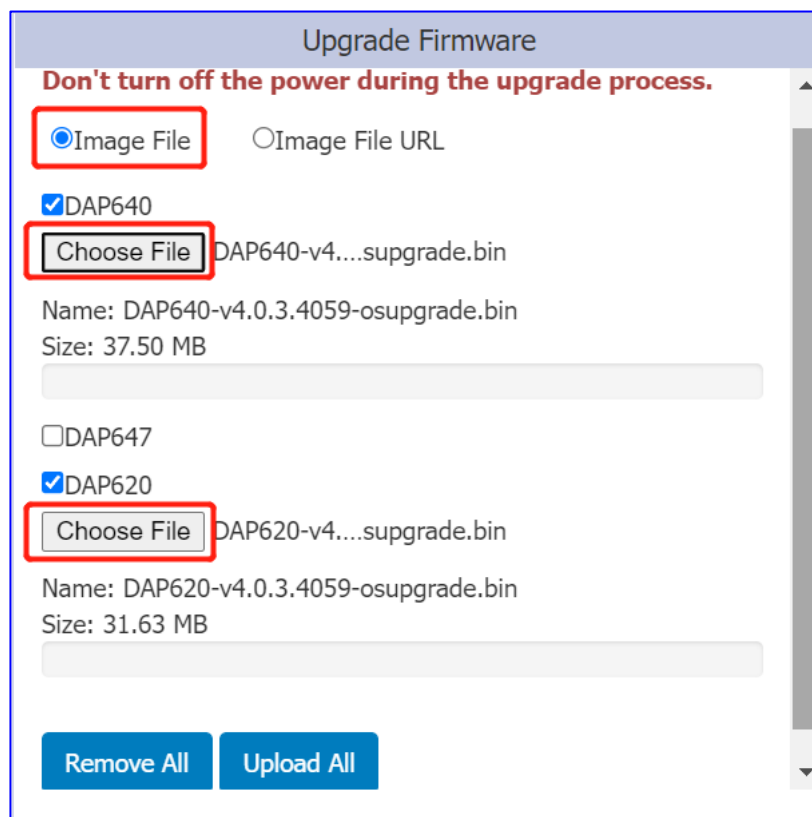


Figure7-13-1-2 Upload firmware from local file

- Upload the AP firmware by using SFTP, please select “Image File URL” option and input the specified URL with SFTP Server IP address, credentials and firmware file name, click “Upload To All” button to perform the upgrade operation shown in Figure7-13-1-3:


The screenshot shows the 'Upgrade Firmware' interface. At the top, it says 'Upgrade Firmware'. Below that, a warning: 'Don't turn off the power during the upgrade process.' There are two radio buttons: 'Image File' (unselected) and 'Image File URL' (selected). Below this, there are three rows for different AP models: DAP640, DAP647, and DAP620. Each row has a text input field containing an SFTP URL: 'SFTP://admin:test1234@192.168.62.137/DAP640-v4.0.3.', 'SFTP://admin:test1234@192.168.62.137/DAP647-v4.0.3.', and 'SFTP://admin:test1234@192.168.62.137/DAP620-v4.0.3.' respectively. Below these fields, there are two lines of text: '(TFTP://ip[[ipv6]/file.bin)' and '(SFTP://UserName:Password@ip[[ipv6]/file.bin)'. At the bottom, there is a blue button labeled 'Upload To All'.

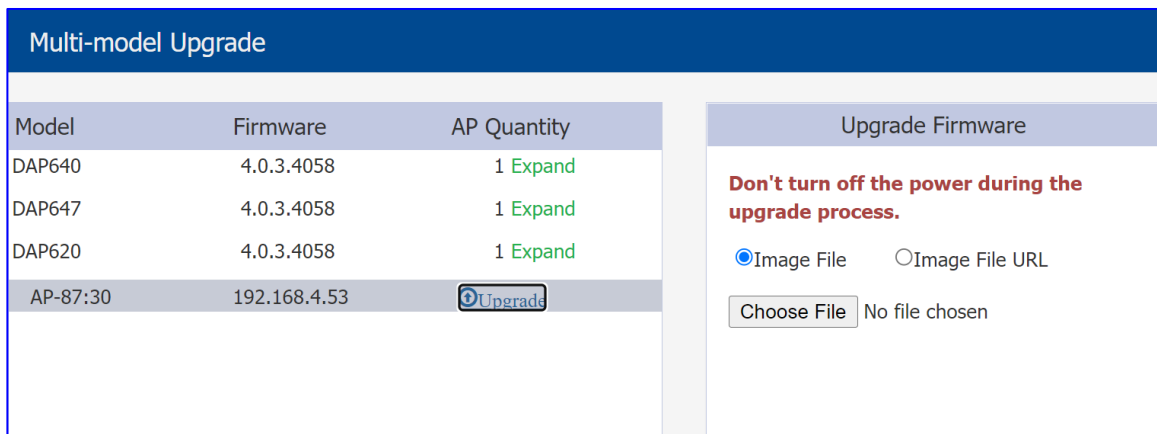
Figure7-13-1-3 Upload AP firmware by using SFTP


- Upload the AP firmware by using TFTP, please input the specified URL with TFTP Server IP address and firmware file name, then click “Upload To All” button to perform the upgrade operation shown in Figure7-13-1-4:

The screenshot shows the 'Upgrade Firmware' interface. At the top, it says 'Upgrade Firmware'. Below that, a warning: 'Don't turn off the power during the upgrade process.' There are two radio buttons: 'Image File' (unselected) and 'Image File URL' (selected). Below this, there are three rows for different AP models: DAP640, DAP647, and DAP620. Each row has a text input field containing a TFTP URL: 'TFTP://192.168.62.137/DAP640-v4.0.3.4059-osupgrade.b', 'TFTP://192.168.62.137/DAP647-v4.0.3.4059-osupgrade.b', and 'TFTP://192.168.62.137/DAP620-v4.0.3.4059-osupgrade.b' respectively. Below these fields, there are two lines of text: '(TFTP://ip[[ipv6]/file.bin)' and '(SFTP://UserName:Password@ip[[ipv6]/file.bin)'. At the bottom, there is a blue button labeled 'Upload To All'.

7.13.2 Upgrade single AP

Select the DAP to be upgraded from the AP list in the right hand of the Multi-model Upgrade page, click  Upgrade and upload firmware for designate DAP, illustrated in Figure 7-13-2-1, and you can also upgrade one single DAP via AP Advanced Configuration page which described in Chapter [7.15.6 System management](#).



Model	Firmware	AP Quantity
DAP640	4.0.3.4058	1 Expand
DAP647	4.0.3.4058	1 Expand
DAP620	4.0.3.4058	1 Expand
AP-87:30	192.168.4.53	 Upgrade

Upgrade Firmware

Don't turn off the power during the upgrade process.

Image File Image File URL

No file chosen

Figure7-13-2-1 Upgrade All Firmware



Don't turn off the power during the upgrade process!




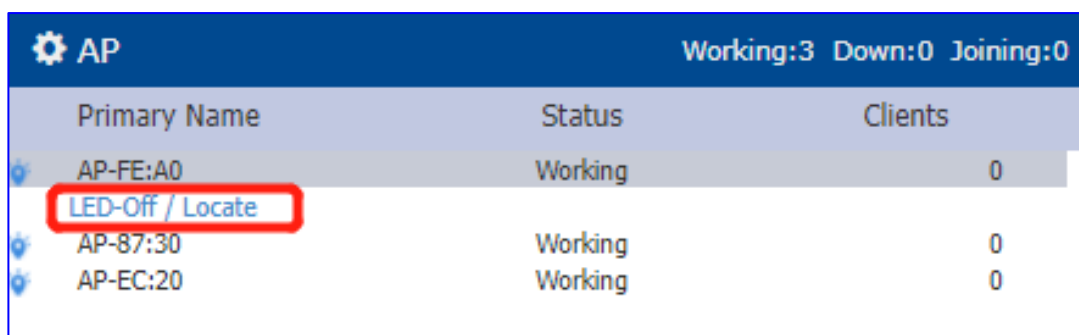
Note

In order to make sure you're running the latest software, we strongly recommend clearing the browsing data in your browser after the software upgrade, including:

- Cookies
- Cache

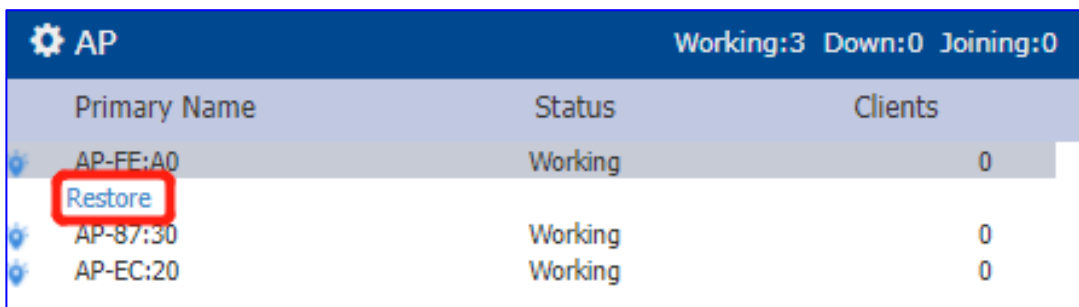
7.13 Locate or turn on/off LED

- Click  in AP Window of Dashboard to launch 'LED-Off/Locate' buttons, shown in Figure7-14-1.
- Click 'LED-Off' to turn off the LED light.
- Click "Locate" to locate AP, in this state, the '**Restore**' label appears and the LED on DAP blinks with red, blue and green color, shown in Figure7-14-2.
- Click "Restore" to return to the normal state.



AP Working:3 Down:0 Joining:0		
Primary Name	Status	Clients
AP-FE:A0	Working	0
LED-Off / Locate		
AP-87:30	Working	0
AP-EC:20	Working	0

Figure7-14-1 Locate or turn on/off LED



AP Working:3 Down:0 Joining:0		
Primary Name	Status	Clients
AP-FE:A0	Working	0
Restore		
AP-87:30	Working	0
AP-EC:20	Working	0

Figure7-14-2 Restore LED to default state

7.14 AP Advanced Configuration

In the AP Configuration page, you can click the IP address of the item to open a specific AP advanced configuration page from the AP list, illustrated in Figure7-15-1







AP Configuration					
Primary Name	IP	Firmware	Operate		Model
PVM					
AP-FE:A0	192.168.4.52 192.168.4.221	4.0.3.2043	 cfg	 reboot	DAP640
SVM					
AP-87:30	192.168.4.53	4.0.3.2043	 cfg	 reboot	DAP620
MEMBER					
AP-EC:20	192.168.4.31	4.0.3.2043	 cfg	 reboot	DAP647

Figure7-15-1 Access to AP UI

7.15.1 AP advanced configuration page overview

AP advanced configuration page is a dedicated web interface to monitor and configure single DAP in the cluster, while cluster web management system is focus on configuration base on cluster level as well as monitoring, illustrated in Figure7-15-1-1.

In AP advanced configuration page, you can:

- Learn the WLANs status, connecting clients on the DAP.
- Configure DHCP/DNS/NAT services on the DAP.
- Configure wireless Mesh/Bridge feature for the DAP.
- Maintenance – Upgrade/Reset/Reboot the DAP.
- RF environment monitoring & scanning.
- Neighbor AP presentation & configuration.

HIRSCHMANN IT
A BELDEN BRAND

Administrator

AP					WLAN			
MAC	IP	Status	Clients	Work Mode	WLAN Name	Status	Type	Clients
94:AE:E3:FF:C0...	172.16.10.169	CLUSTER	1	AP	My-wifi-test	enable	Personal	1
					My-wifi-PSK	enable	Personal	0
					My-wifi-portal	enable	Open	0
					My-wifi-1x	enable	Enterprise	0
					My-wifi-test101	enable	Open	0

Clients					RF				
For AP: 94:AE:E3:FF:...					Total:1				
Name	IP	MAC	WLAN	Auth	Channel	Status	Power	Clients	
	172.16.10.102/fe8	c0:3c:59:70:3d:c5	My-wifi-test	PSK_WPA2	2.4G	11	enable	17	
					5G_all	52	enable	21	

- System
- Network
- Service
- Neighbor AP
- RF Environment

Figure7-15-1-1 AP advanced configuration page

7.15.2 AP information and work mode configuration

The AP information window indicate the basic information for specific DAP, such as AP MAC ,AP IP address, Status, number of associated clients and current Work Mode, illustrated in Figure7-15-2-1.

AP				
MAC	IP	Status	Clients	Work Mode
94:AE:E3:FF:C0:70	172.16.10.169	CLUSTER	1	AP

Figure7-15-2-1 AP information window

Specific DAP can be configured to work on Bridge mode or Router mode, click hyperlink 'AP' in AP information window to load the Mode Configuration page, a reboot is required if change DAP work mode, it is AP mode by default, illustrated in Figure7-15-2-2 and 7-15-2-3.

AP				
MAC	IP	Status	Clients	Work Mode
94:AE:E3:FF:C0:70	172.16.10.169	CLUSTER	1	AP

Figure7-15-2-2 AP Mode Configuration Entry

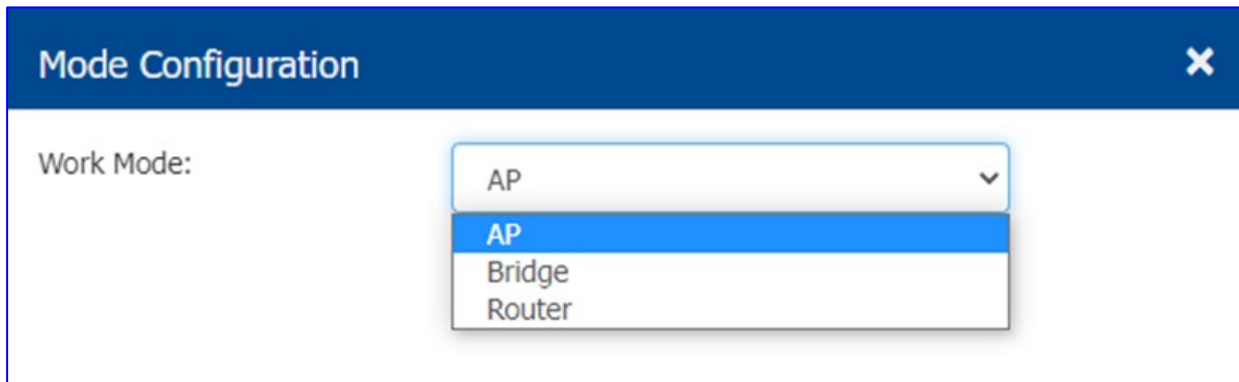


Figure7-15-2-3 AP Mode Configuration

Configure DAP works on Bridge Mode:

A point-to-point wireless bridge is used to connect LAN(s) which in different buildings through the wireless interface, illustrated in Figure7-15-2-4.

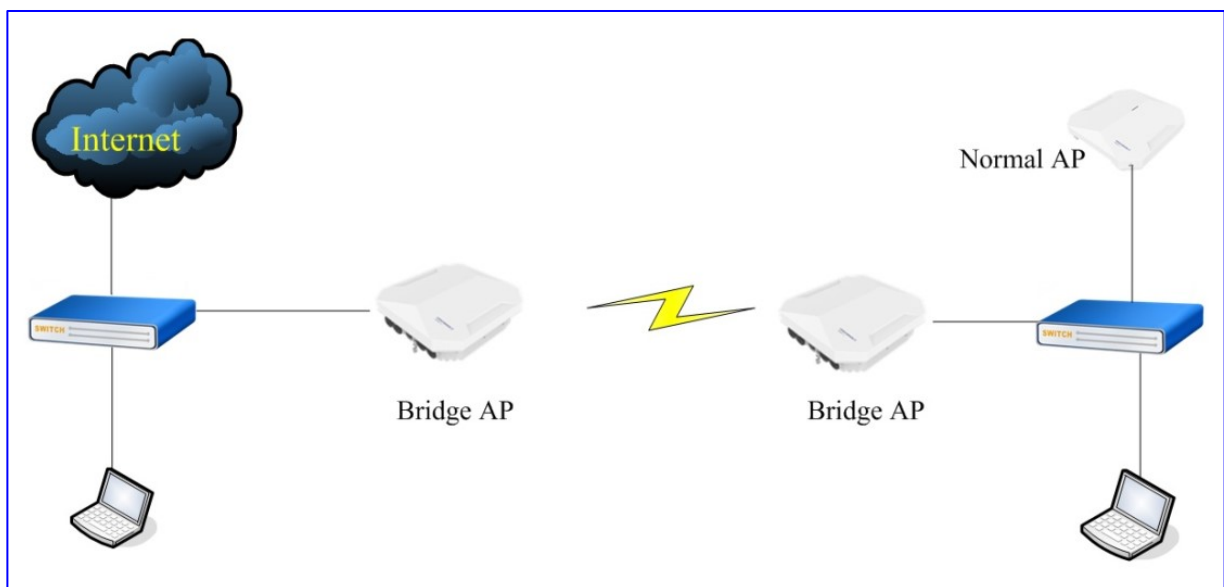


Figure7-15-2-4 Bridge Topology

In Bridge mode, DAP will only broadcast a bridge SSID configured and not accept wireless client connection except Bridge AP, illustrated in Figure7-15-2-5.

Figure7-15-2-5 AP Bridge Configuration

- **Work Mode** – DAP working mode, bridge mode, AP mode or Router mode.
- **SSID** – WLAN used to setup wireless bridge connection.
- **Band** – Wireless bridge working frequency.
- **Root** – Specify the root node of the wireless bridge.
- **Passphrase** – Password of the WLAN used to setup wireless bridge connection.
- **Confirm** – Re-enter the password to confirm.

Configure AP works on Router Mode

DAP can be set worked as a Router, in this mode AP will also work as a DHCP server and provide IP address for clients. DAP supports to manage its IP address of uplink interface (WAN) by DHCP, Static or PPPoE, illustrated in Figure7-15-2-6.

Figure7-15-2-6 Configure wan IP

The detailed network configuration can be seen and modified in AP Networks configuration window in Network page, you can modify the wan interface and default (LAN) interface, illustrated in Figure7-15-2-7

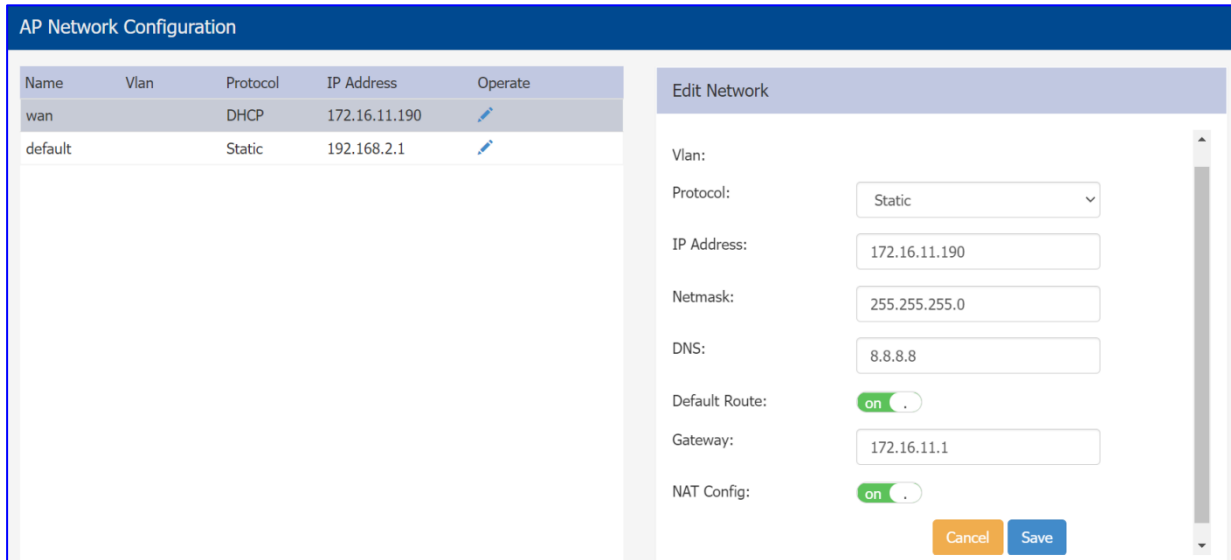


Figure7-15-2-7 Modify AP Network Configuration

7.15.3 WLAN information

The WLAN information window indicates the basic information of SSIDs on specific DAP, such as WLAN Name, Status, encryption type and number of client associated to the WLAN. In this window, all the information is just for your reference and not configurable, illustrated in Figure7-15-3-1.

WLAN			
WLAN Name	Status	Type	Clients
My-wifi-test	enable	Personal	1
My-wifi-Portal	enable	Open	0
My-wifi-1x	enable	Enterprise	0

Figure7-15-3-1 WLAN information overview

7.15.4 Clients information

The Clients information window indicates the basic information of clients on specific DAP, such as User Name for portal authentication, IP address, WLAN, encryption type. In this window, all the information just for your reference and not configurable, illustrated in Figure7-15-4-1.

Clients				
For AP: 34:E7:0B:09:C0:70				
Total:2				
User Name	IP	MAC	WLAN	Auth
	192.168.8.4/fe80::1852:435	dc:0c:5c:dd:59:c9	My-wifi-test	PSK_WPA2
	192.168.8.33/2409:8a00:18	c0:3c:59:70:3d:c5	My-wifi-test	PSK_WPA2

Figure7-15-4-1 Clients information overview

7.15.5 RF information

The RF information window indicates the basic information of radio, such as the current worked channel, current work state, the transmit power of each radio and number of client associated to the radio. In this window, all the information just for your reference and not configurable, illustrated in Figure7-15-5-1

RF				
	Channel	Status	Power	Clients
2.4G	1	enable	20	0
5G_all	149	enable	21	2

Figure7-15-5-1 RF information overview

7.15.6 System management

In this page, you can see the syslog information related the specific AP and you can also perform the DAP upgrading, illustrated in Figure7-15-6-1, please refer to [8.6 Syslog](#) and [7.13 Upgrade All Firmware](#) for details.

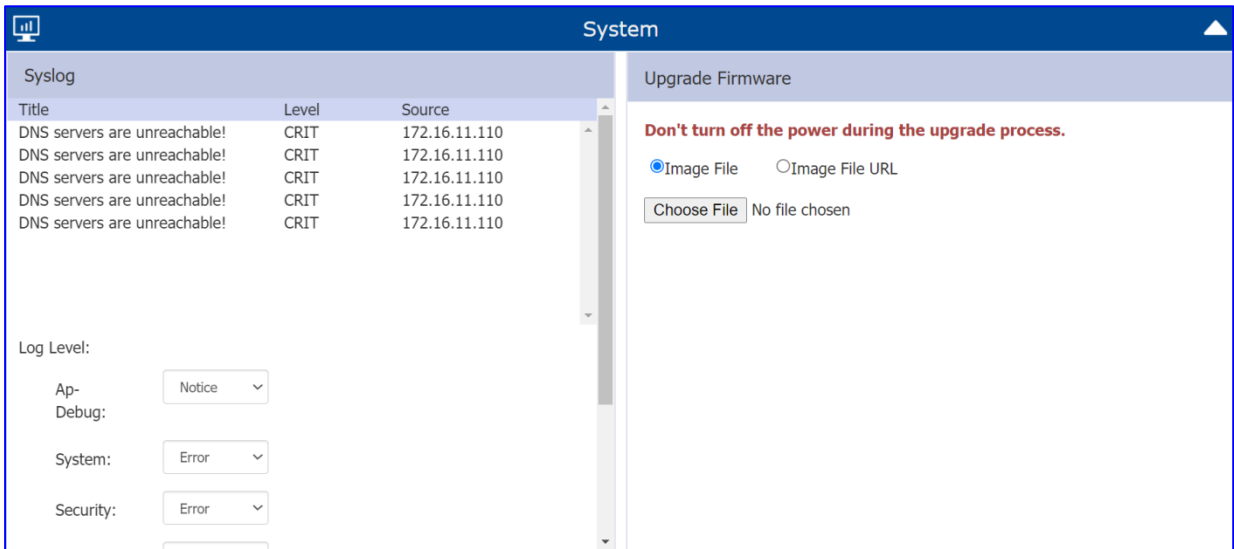


Figure7-15-6-1 System management on AP UI

7.15.7 AP Interface

Navigate: advanced configuration page -> Network -> AP Interface -> AP Interface Configuration, illustrated in Figure7-15-7-1 and 7-15-7-2

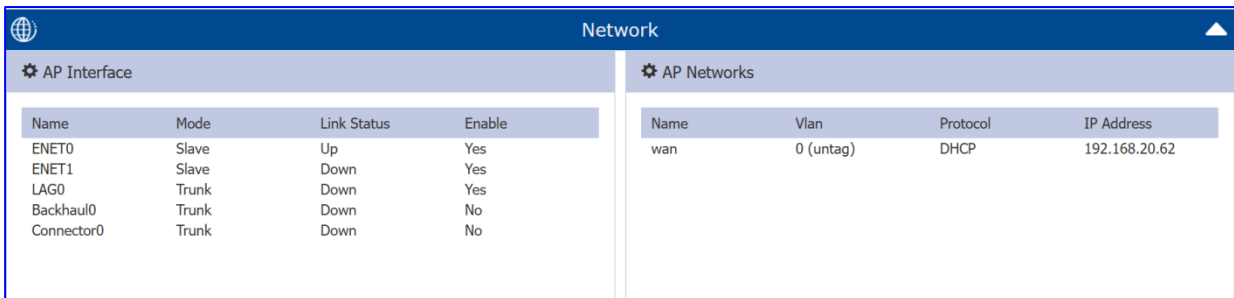


Figure7-15-7-1 AP Interface window



AP Interface Configuration						
Name	Speed(MB)	Model	Link Status	Enable	Operate	
Eth0	1000	Trunk	Up	Yes		
Eth1	0	Trunk	Down	Yes		
LAG0	0	Trunk	Down	No		
Backhaul0	0	Trunk	Down	No		
Connector0	0	Trunk	Down	No		

Figure7-15-7-2 AP Interface Configuration

Interface Description:

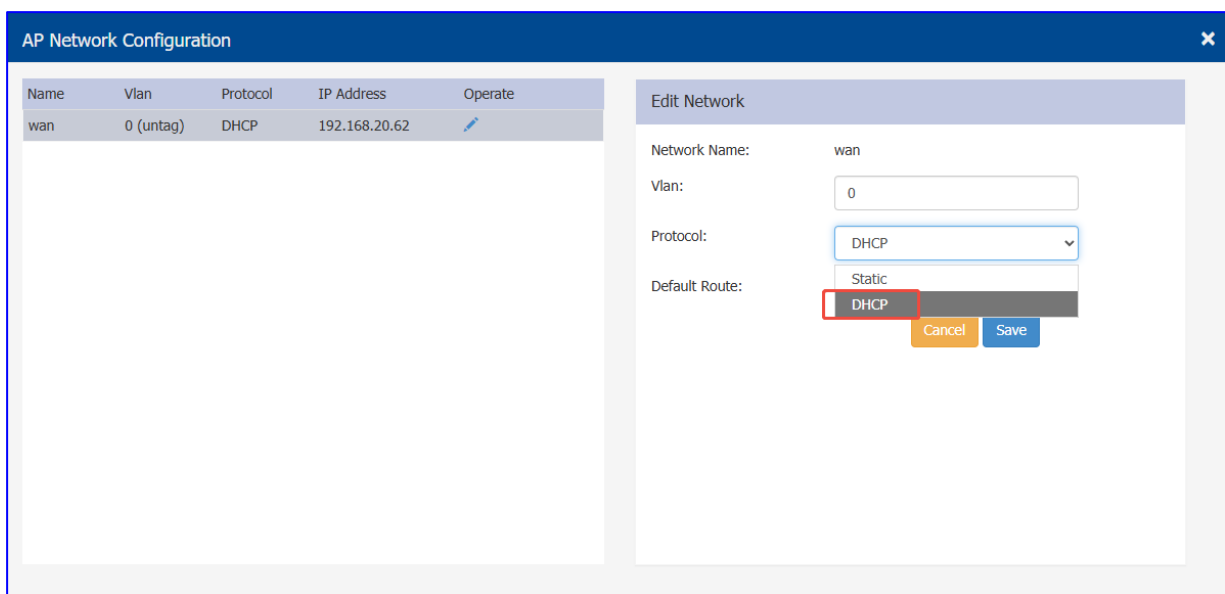
- **Eth0/Eth1**– Uplink interface of AP (Wired interface).
- **LAG0**–Uplink interface of the AP(Link Aggregation interface)
- **Backhaul1** – Downlink interface of the Mesh/Bridge link.
- **Connector1** – Uplink interface of the Mesh/Bridge link.

For each AP interface

- **Speed** – Link speed of the AP interface.
- **Mode** – VLAN access mode or WLAN trunk mode.
- **Link Status** – Up/down.
- **Enable** – Indicate whether the AP interface is enabled or disabled.
- **Operate** – Can be applied to Backhaul1 or Connector1 interface for wireless mesh/bridge configuring.

7.15.8 AP Network

The WAN or VLAN interfaces are configurable for DAP required by some specific network scenario, Navigate: advanced configuration page -> Network -> AP Networks, illustrated in Figure7-15-8-1



- **Network Name** – Name of the network. There are 2 types of network on AP: VLAN networks mapping to WLAN (SSID); WAN networking mapping to AP uplink port.
- **VLAN** – VLAN ID mapping to specific WLAN (SSID).
- **Protocol** – IP address allocation for the network interface. IP address of a network interface is usually set as the gateway of the devices connecting the network.
 - **DHCP** - the interface IP address is obtained from an outside DHCP server.
 - **Static** – Indicates the interface IP address of the network is manually set.
- **Operate** – Edit the AP network.
- **IP Address** – Interface IP address of the network.
- **Netmask** - Netmask of the network.
- **DNS** – DNS server for the network.
- **Default Route** – Indicate whether the interface of the network is default route of the AP. By default, WAN interface in the default route of the AP.

7.15.9 MESH configuration

The Belden mesh solution is an effective way to expand wireless network coverage for enterprise environments without any wires. Using mesh, you can bridge multiple Ethernets LANs or you can extend your wireless coverage (Wireless backhauling). As traffic traverses across mesh APs, the mesh network automatically reconfigures around broken or blocked paths. This self-healing feature provides increased reliability and redundancy: the network continues to operate if an AP stops functioning or a connection fails, illustrated in Figure7-15-9-1.

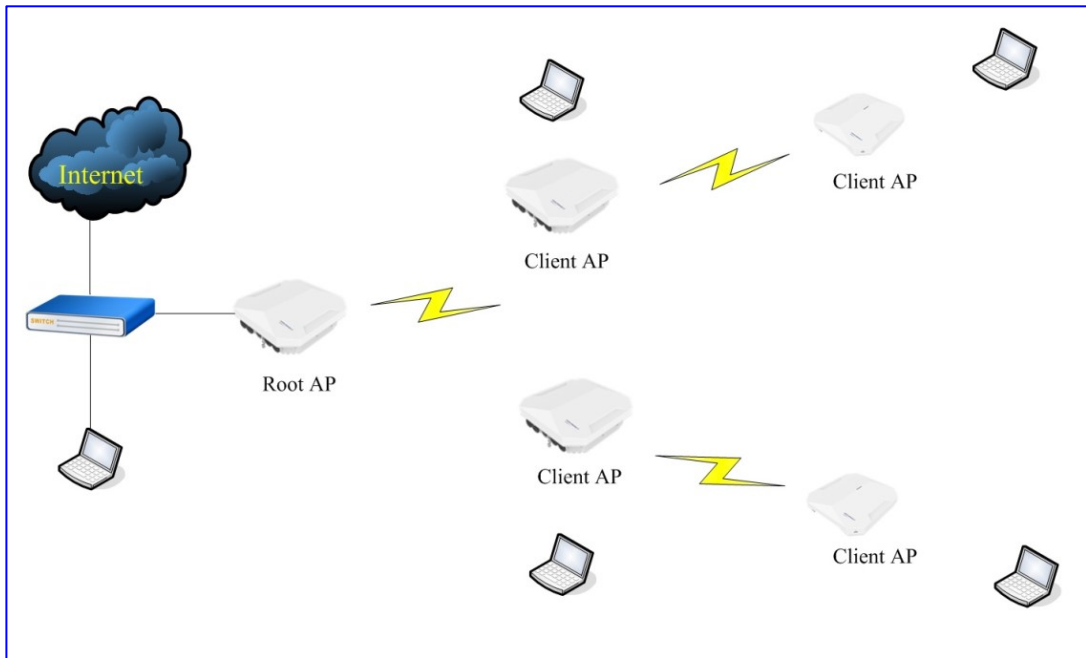





Figure7-15-9-1 MESH Topology

To expand your wireless coverage without bridging Ethernet LAN segments, you can use Mesh services configured as wireless backhaul. In this deployment scenario, the AP provides network access for wireless clients and establishes a mesh path to the mesh root, which uses its wired interface to connect to the switch.

Configure your mesh networks, please go to AP UI-> “Network”->“AP Interface”, find the interface named “Backhaul0” and click  to configure your mesh network, illustrated in Figure7-15-9-2

AP Interface Configuration
✕

Name	Speed(MB)	Model	Link Status	Enable	Operate
Eth0	100	Trunk	Up	Yes	
Eth1	0	Trunk	Down	Yes	
LAG0	0	Trunk	Down	No	
Backhaul0	0	Trunk	Down	No	
Connector0	0	Trunk	Down	No	

Edit Interface

Enable: Yes No

Type: Mesh

SSID:

Root: Yes No

Band: 2.4G 5G

Passphrase:

Confirm:

Cancel
Save

Figure7-15-9-2 AP Interface Configuration

- ✓ **Enable**: Enable/disable the wireless mesh on DAP
- ✓ **SSID**: SSID for mesh connection
- ✓ **Band**: The working band for mesh connection. All the mesh connection from root node to client node shall be in the same band.
- ✓ **Root**: Specify the root node of the wireless mesh chain
- ✓ **Passphrase**: Password of the WLAN used to setup wireless mesh connection

7.15.10 Static Neighbor AP Configuration

Neighbor AP is the candidate to which clients connecting to current AP might roam. There two types of neighbor AP – Auto Neighbor AP as well as Static Neighbor AP. Auto Neighbor AP is discovered through wireless scanning automatically, while Static Neighbor AP is manually added in case of some special deployment scenarios, illustrated in Figure7-15-10-1.

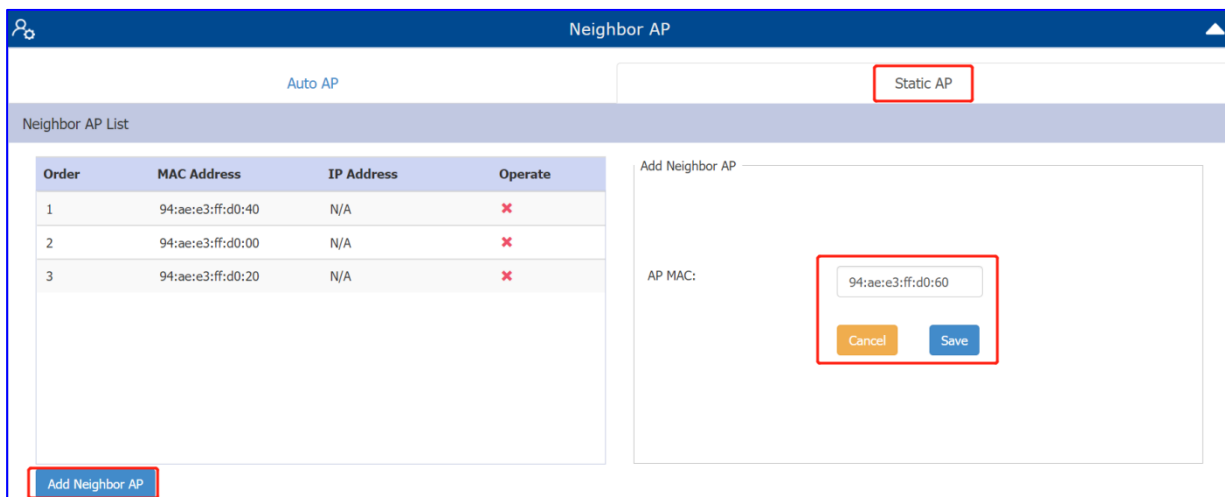


Figure7-15-10-1 Configure Static Neighbor AP

- **Order** – Item number of the neighbor AP.
- **MAC Address** – MAC address of the neighbor AP.

- **IP Address** – IP address of the neighbor AP.
- **Operate** – Remove the neighbor AP, it only applicable for static neighbor APs.

7.15.11 RF Environment

The RF Environment is used to view Scanning Mode data for DAPs. Wireless networks operate in environments with RF devices that can interfere with network communications. APs can examine the RF environment in which the Wi-Fi network is operating, identify interference, and classify its sources. An analysis of the results can then be used to quickly isolate issues with packet transmission, channel quality, and traffic congestion caused by contention with other devices operating in the same channel.

The scanning band can be selected for 2.4G radio or 5G radio and the scanning date includes the channel utilization and the SSIDs in the RF environment, the detailed channel information can be seen when mouse move to the related channel and the detailed SSID information will be shown when click the relevant item, illustrated in Figure7-15-11-1.

There are two types of AP Scanning Mode:

- **One Time** – The scanning mode will last for 5 minutes duration and then return to normal AP mode in which wireless clients can associate.
- **Always** – The scanning mode is always active and wireless client is not allowed to associate if the AP is powered on.



Note

To view Scanning Mode data for an AP, the AP must be in "Scanning Mode". When an AP is in Scanning Mode, it will not response the clients' connection. When the scanning mode is terminated automatically (One Time mode or Always mode), AP will return to normal AP mode and clients are allowed to connect.

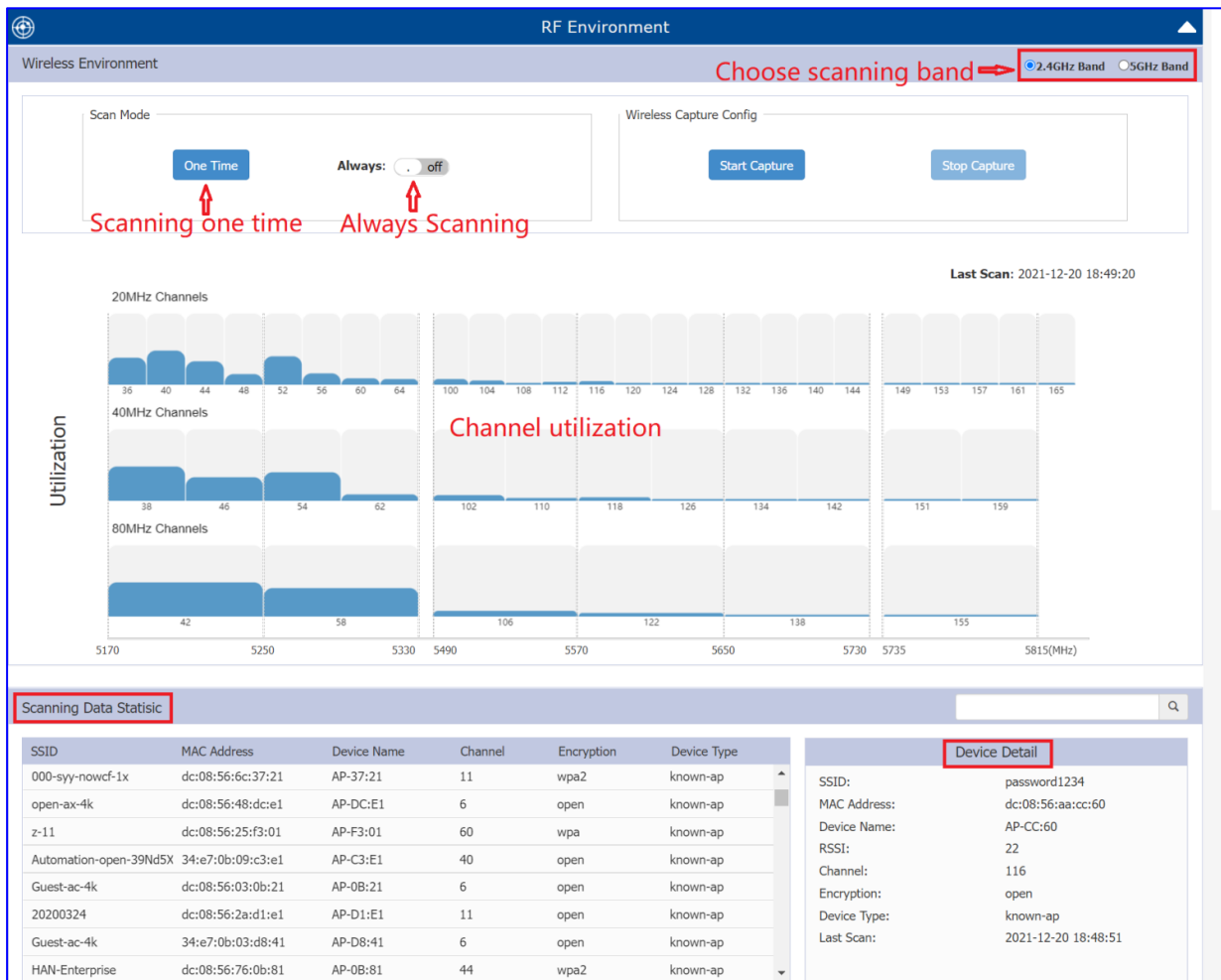


Figure7-15-11-1 RF Environment

7.15.12 Wireless Capture

AP can work on capture mode and support wireless packets capture, in this mode, all clients on this AP will be disconnected and wireless scanning will be stopped during packet capture period. Packet capture will be completed automatically when reaches its threshold (5minutes/10MB) or it can be stopped manually in any time, please refer to the following steps for the capture on DAP:

Step1- Please login AP UI page and go to RF Environment→ Wireless Capture Config→Start Capture, shown as Figure7-15-12-1

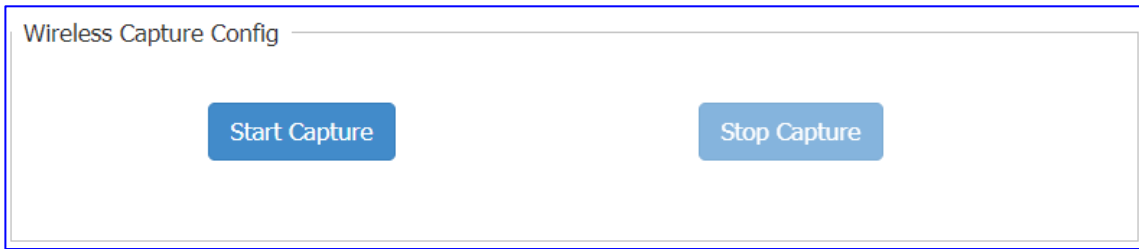


Figure7-15-12-1 Wireless Capture Config

Step2-Please select the corresponding filters to capture, shown as Figure7-15-12-2.

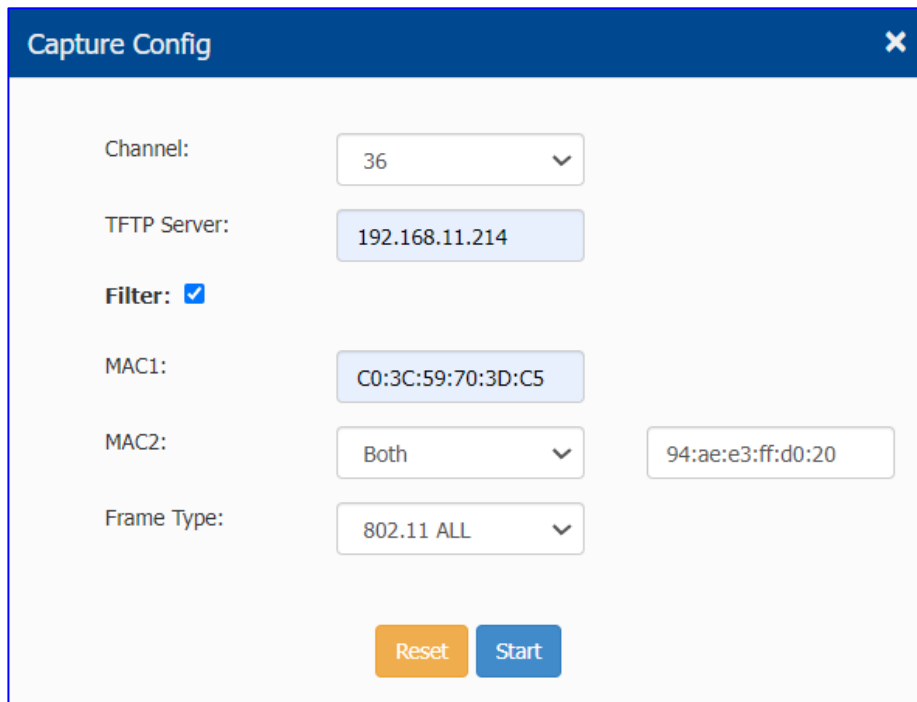
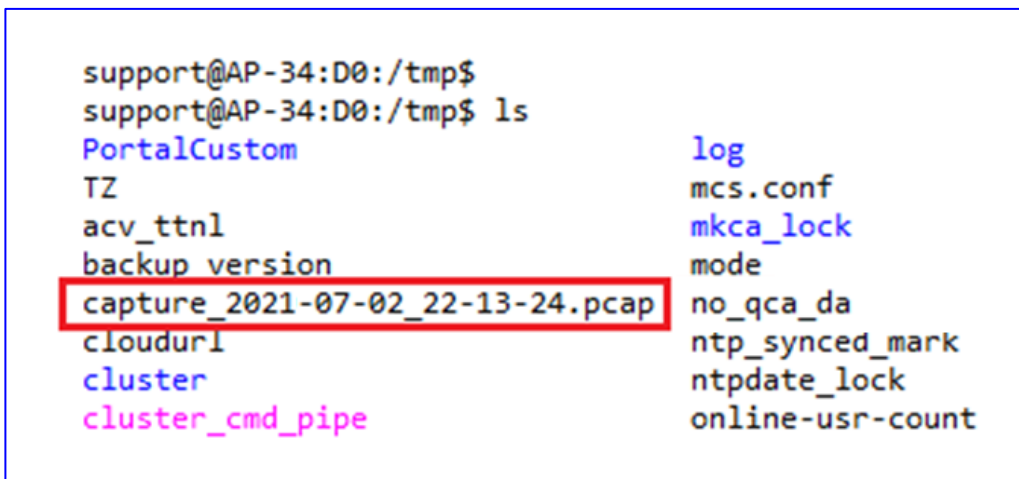


Figure7-15-12-2 Capture Filter Config

After click "Start" AP will stored packet file under /tmp folder temporarily and delete it automatically after it uploaded to TFTP server, illustrated in Figure7-15-12-3.



7.15 AP works as Gateway

7.16.1 Configure DHCP Server

For an AP cluster in the same Layer 2 network, you can setup DHCP server on a specific AP in the cluster. Navigate: AP advanced configuration page -> Service -> DHCP, shown in Figure7-16-1-1

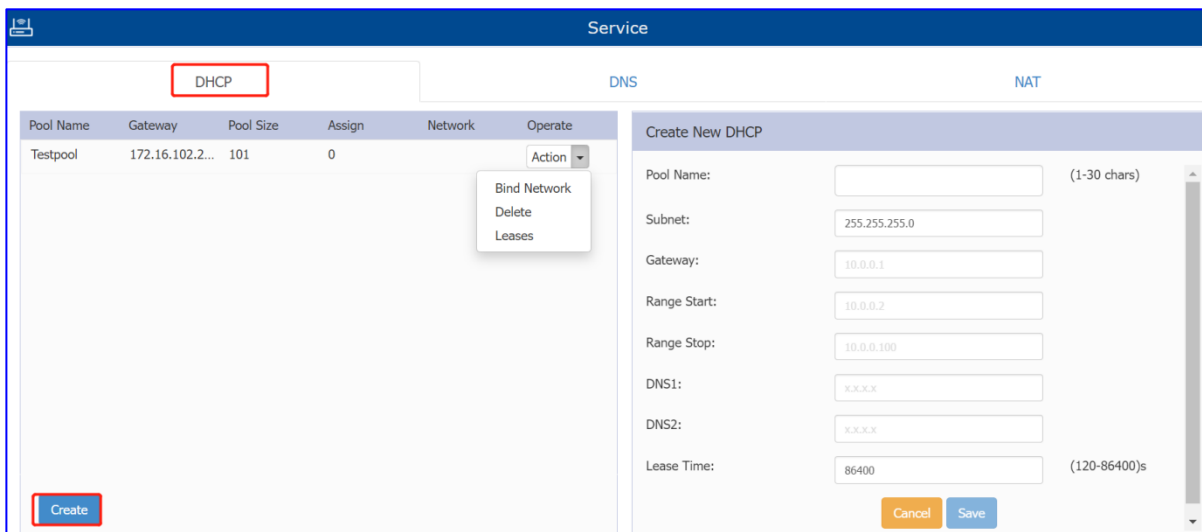
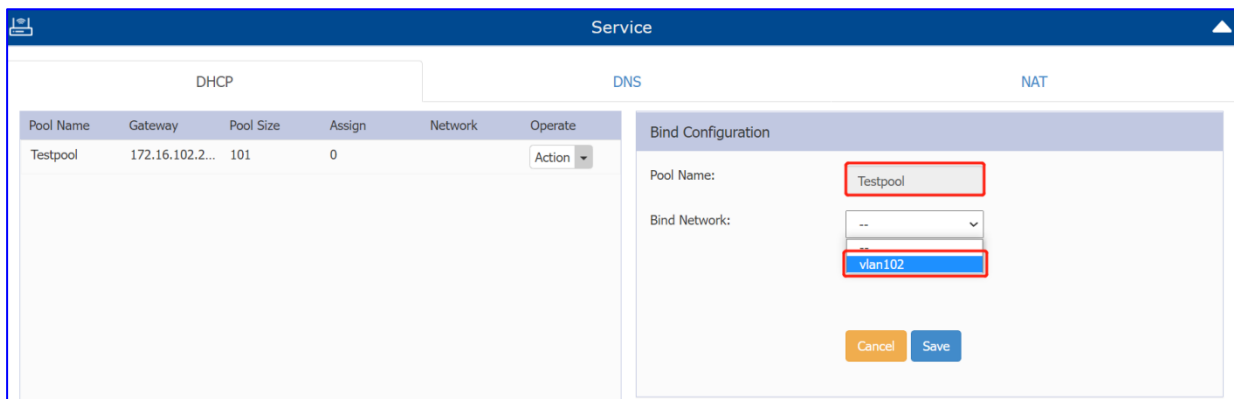


Figure7-16-1-1 Configure DHCP Server

After you create a DHCP pool, you should bind the DHCP pool to specific Network and take effect, illustrated in Figure7-16-1-2. Before binding, you need to configure the Network basic parameters in the 'AP UI -> Network -> AP Networks window'. Only Network with static IP (as gateway) can be bound to a DHCP pool.



Action for DHCP pool:

- **Bind Network** – Bind the DHCP pool to specific Network.
- **Delete** – Delete the DHCP pool.
- **Leases** – Display the IP addresses which have been allocated to devices.

7.16.2 Configure DNS Server

Cache Size – Specify the size for the DNS cache, up to 1000 entries can be set and default value is 150 entries, Navigate: advanced configuration page -> Service -> DNS, illustrated in Figure7-16-2-1

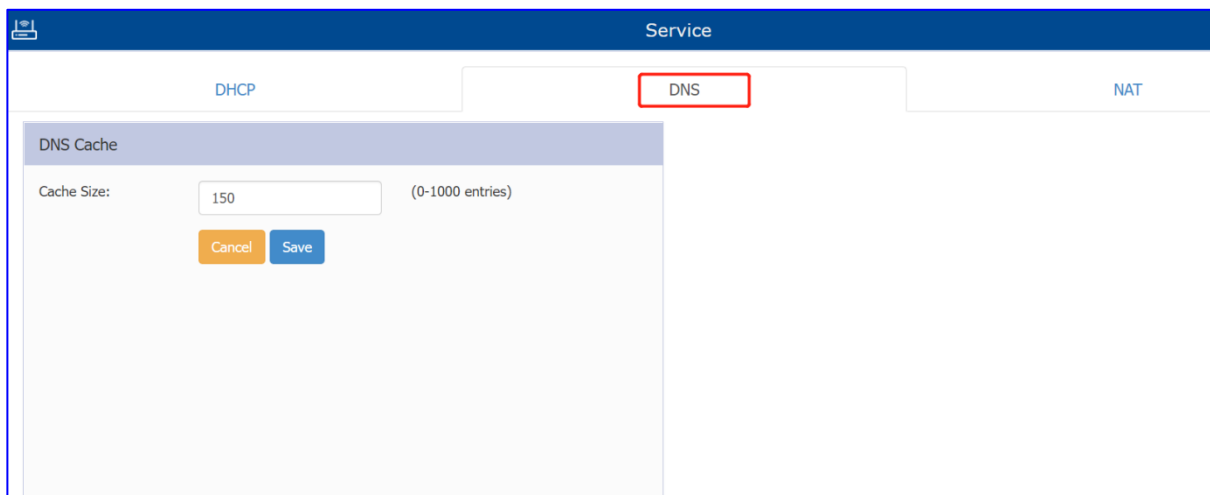


Figure7-16-2-1 DNS Cache setting

7.16.3 NAT Configuration

NAT is the process of modifying network address information when packets pass through a routing device. The routing device acts as an agent between the public (the Internet) and the private (local network), which allows translation of private network IP addresses to a public address space.

DAP supports the NAT mechanism to allow a routing device to use the translation tables for mapping the private addresses into a single IP address. When packets are sent from this address, they appear to originate from the routing device. Similarly, if packets are sent to the private IP address, the destination address is translated as per the information stored in the translation tables of the routing device.

Both Source NAT and Destination NAT supported by DAP, Navigate: advanced configuration page -> Service -> DNS.

Source NAT can be utilized to translate the internal IP addresses to single external IP address while visiting Internet, by saving public IP address, configure Source NAT by clicking the window frame of Source NAT, illustrated in Figure7-16-3-1.

- **Name** – Name of the Source NAT rule.
- **Source IP** – Mapping source IP address of the NAT rule, single IP or segment.
- **Destination IP** – Mapping destination IP address of the NAT rule, single IP or segment.
- **Source Port** – Mapping source port of the NAT rule.
- **Destination Port** – Mapping destination port of the NAT rule.
- **Protocol Type** – Network protocol to which the NAT rule is applied.
- **Output Interface** – Specify the outbound interface of the NAT rule.
- **Translation** – Use Masquerade, indicates the internal IP addresses will be translated to the interface IP address (gateway) of the network.

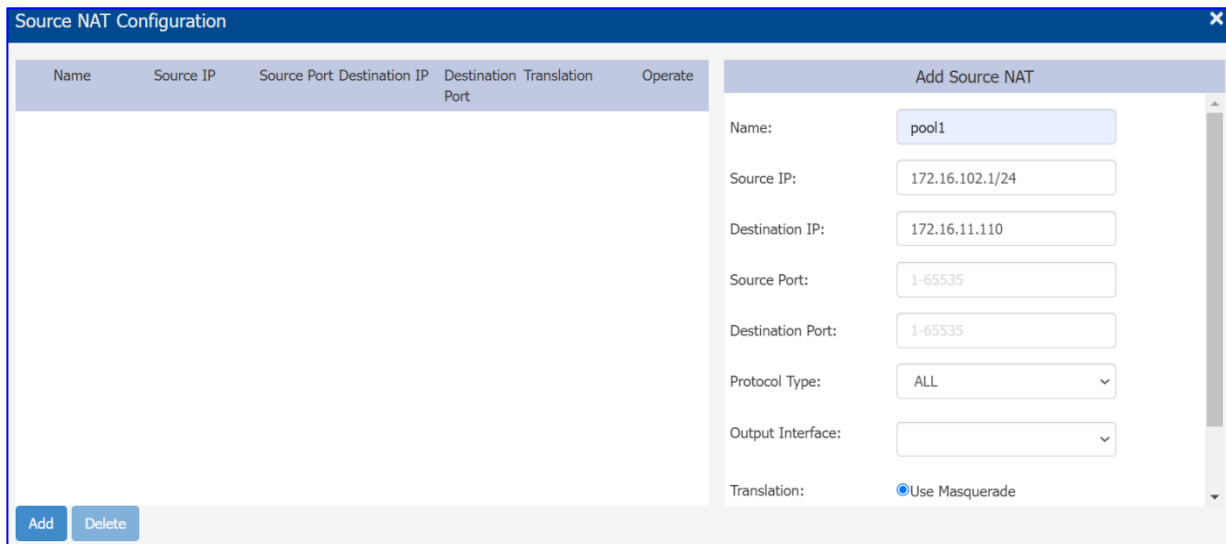


Figure7-16-3-1 Configure Source NAT

Destination NAT can be utilized to realize visiting specific server in the internal network from internet, configure Destination NAT by clicking the window frame of Destination NAT, illustrated in Figure7-16-3-2.

- **Name** – Name of the destination NAT rule.
- **Source IP** - Mapping source IP address of the NAT rule, single IP or segment.
- **Destination IP** - Mapping source port of the NAT rule.
- **Source Port** – Mapping source port of the NAT rule.
- **Destination Port** – Mapping destination port of the NAT rule.
- **Protocol Type** - Network protocol to which the NAT rule is applied.
- **Input Interface** - Specify the inbound interface of the NAT rule.
- **Translation**
 - **IP** – IP address to which the external IP address will be translated
 - **Port** - Port to which the external IP address will be translated

Destination NAT Configuration

Name	Source IP	Source Port	Destination IP	Destination Port	Translation	Operate
(Empty table body)						

Add
Delete

Add Destination NAT

Source Port:

Destination Port:

Protocol Type: ▼

Input Interface: ▼

*Translation: Specify Network Addr

IP:

Port:

Cancel
Save

Figure7-16-3-2 Configure Destination NAT

8 System Management

The System window focuses on the basic settings of the DAP cluster, including: DAP cluster attributes, system management accounts, system time and syslog.

This chapter contains the following topics:

- [Cluster Info Management](#)
- [Manage your Accounts](#)
- [Certificate Management](#)
- [Services Management](#)
- [System Time Configuration](#)
- [Configuring Syslog](#)
- [Configuring SNMP](#)

8.1 Cluster Info Management

To configure or modify the cluster attributes, please launch the window 'System->General Configuration', as shown in Figure8-1-1. DAP Cluster Information will be displayed at the top of the Dashboard, as shown in Figure8-1-2.

A management IP can be set manually by the administrator in Cluster Info Management sheet, the management IP address is used to management DAP cluster which is a virtual IP and will be assigned to the PVM and can be access from both wireless and wired side

Parameter	Specification
Cluster Name	Name of the DAP Cluster.
Location	Location of the DAP Cluster.
Cluster Management IP	A virtual IP address for DAP Cluster management

Cluster Management Netmask	Netmask of Cluster Management IP.
Cluster Management IPv6	A virtual IPv6 address for DAP Cluster management.
Cluster ID	Identification of the DAP Cluster, the default Cluster ID is 100.

Table8-1-1 DAP Cluster Parameters Specification

Figure8-1-1 AP Cluster configuration

Figure 8-1-2 AP Cluster Information



Note

AP of a Cluster usually obtains its IP address dynamically from a DHCP server, and it is difficult to keep the same assigned IP address for the AP. So managing the AP Cluster by the AP's dynamic IP address can be difficult. The Cluster Management IP is a static IP address configured for the AP Cluster web management, and you can manage the AP Cluster via accessing the URL: <http://IP:8080> by wired or wireless. The Management IP is configured on the PVM of the AP Cluster, and you have to make sure the Management IP on the PVM is routable from your configuring terminal (browser). A recommended method is to choose an idle IP address from the AP Cluster domain to configure as a Management IP.

8.2 Manage your Accounts

8.2.1 Manage your Web GUI accounts

There are three accounts can login to the Web GUI with different privileges: Administrator, Viewer, and Guest Manager which has different authority show as below:

- **Administrator:** Administrator account has the highest privilege and allows configuring and viewing the whole system.
- **Viewer:** Viewer account allows checking configuration and monitoring of WLAN operations.
- **Guest Manager:** ONLY has the privilege to edit the guest portal users.

Each account can be logged in at the same time, when a same account logged in; the previous session will be terminated. By default, only the Administrator account is enabled; Viewer and Guest Manager account are disabled.

In the Account Management tab, you can enable/disable the Viewer and Guest Manager account; change the password for Administrator, Viewer and Guest Manager, illustrated in Figure8-2-1-1

General Configuration

Cluster Info Management Account Management Certificate Management Service Management

Administrator

Password: (4-16 chars)

Confirm:

Viewer Enable Disable

Password: (4-16 chars)

Confirm:

Guest Manager Enable Disable

Password: (4-16 chars)

Confirm:

Tip: In order to ensure user security, please set the different password.

Figure8-2-1-1 Account Management

8.2.2 Manage your CLI account

There are two accounts can login to the DAP command line interface with different privileges: **support** and **root**. Administrator can change the login password for those command line accounts. The root password is a string held by the customer only and is used to generate real root access credential by DAP, illustrated in Figure8-2-2-1.

General Configuration

Cluster Info Management Account Management Certificate Management Service Management

Tip: In order to ensure user security, please set the different password.

Cancel Save

Support Account

Password: (4-16 chars)

Confirm:

Cancel Save

Root Account

Password: (4-16 chars)

Confirm:

Cancel Save

**Note**

For security, the administrator should change the CLI root, and support passwords before use.

8.3 Certificate Management

DAP support below two types of build-in certificates; administrator of customer can customize their own certificate base on specific requirement:

- **Internal Web Server** – The certificate is utilized to setup the secure connection between web browser and AP web server for https management. By default, there is a build-in CA certificate generated by Belden with the domain 'find.dragonflyap.com'. User can use open SSL to generate his/her own CA certificate and replace the default one (User needs to use domain 'find.dragonflyap.com' for your own certificate because the login URL cannot be changed).
- **Internal Portal Server** – The certificate is utilized to setup the secure connection between captive portal page and the AP web server for protecting the user login credentials being stolen. User can define its own captive login URL and replace the certificate accordingly.

Navigate: Dashboard → System Window → General Configuration page –>Certificate sheet, illustrated in Figure8-3-1.

Figure8-3-1 Certificate management

8.4 Services Management

As shown in Figure8-4-1, DAP support below services which can enable or disable separately base on requirement of the real scenario, both of them are disabled by default:

IPV6 L3 Forwarding: Layer 3 IPv6 traffic forwarding between clients and other network elements if the IPv6 Service is enabled

IGMP Snooping: The administrative status of the IGMP Snooping function on the AP.

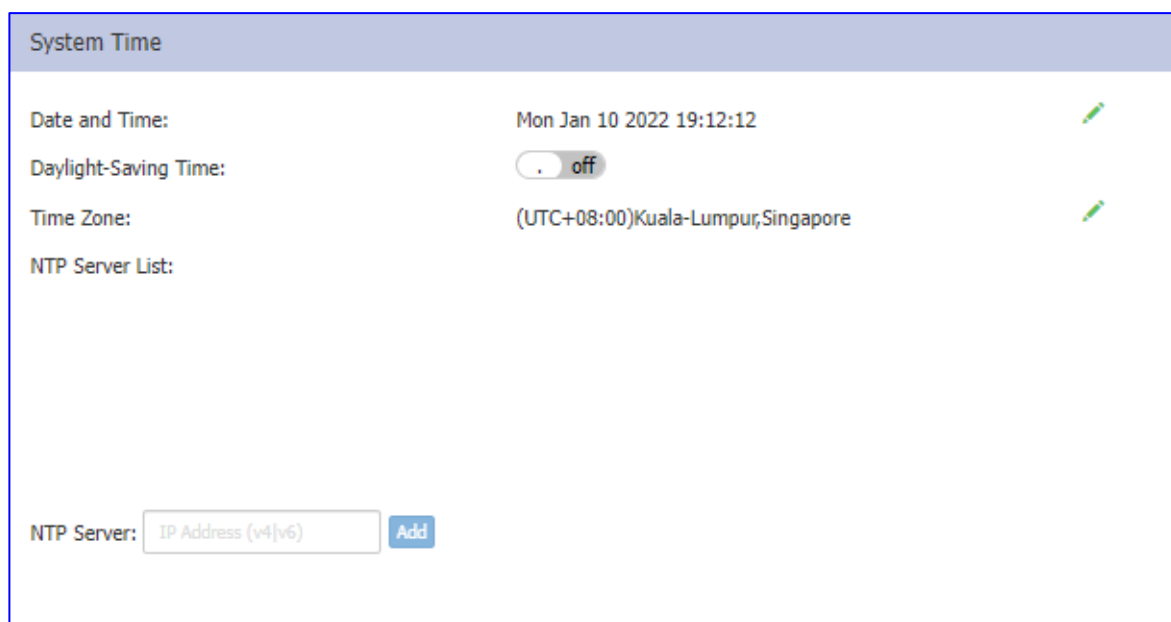
Figure8-4-1 Service management

8.5 System Time Configuration

It is important to ensure the system time is correct; this is because proper communication between network elements and syslog for troubleshooting are based on the correct time.

Navigate: System – System Time

NTP (RFC 1305 - Network Time Protocol) is a networking protocol for time synchronization between the elements across the network. If you have a private NTP server in your network, please configure it and prioritize it to the top of the NTP Server List, If you don't have a private NTP server in your network, it is suggested to add your favorite NTP server and prioritize it to the top of the NTP Server List, or use the default NTP servers in the system, illustrated in Figure8-5-1, If configured, APs in the cluster synchronize the time with NTP sever in 15-minute intervals.



The screenshot displays the 'System Time' configuration interface. It includes the following elements:

- Date and Time:** Mon Jan 10 2022 19:12:12
- Daylight-Saving Time:** A toggle switch set to 'off'.
- Time Zone:** (UTC+08:00)Kuala-Lumpur,Singapore
- NTP Server List:** A section for adding NTP servers, featuring an input field labeled 'IP Address (v4|v6)' and an 'Add' button.

Figure8-5-1 System time configuration

You can also specify the **Time Zone** and daylight-saving time of the DAP cluster to coordinate with the local time. The daylight-saving time is automatically enabled on supporting time zone. Please note that in order to ensure time synchronization, it is recommended to check the reachability before adding an NTP server. If the NTP server is not configured or is unreachable, an AP reboot may lead to variation in time.

8.6 Configuring Syslog

Syslog is a standard for message logging. Syslog is used for system management and security auditing as well as general informational, analysis, and debugging messages.

Navigate: System – Syslog & SNMP – Syslog

APs in cluster generate logs following the standard of Syslog; you can view logs and configure corresponding attributes in the Syslog Window.

Upper part of the Syslog Window displays error level Syslog generated by DAPs in the cluster.

- **Title** is the content of the log message.
- **Level** is the severity of the log message.
- **Source** is the generator's IP address of the log message.

When you move the mouse cursor to certain row of log message, the generating time of the log displays, illustrated in Figure8-6-1.

Syslog & SNMP

Syslog
SNMP

Title	Level	Source
DNS servers are unreachable!	CRIT	172.16.11.110
DNS servers are unreachable!	CRIT	172.16.11.110
DNS servers are unreachable!	CRIT	172.16.11.110
DNS servers are unreachable!	CRIT	172.16.11.110
DNS servers are unreachable!	CRIT	172.16.11.110
DNS servers are unreachable!	CRIT	172.16.11.110

Log Level:

Ap-Debug: ▼

System: ▼

Security: ▼

Wireless: ▼

Network: ▼

User: ▼

Log Remote: off

Log File: ▼

Figure8-6-1 Syslog Configuration

Log Level:

Setting of Syslog message severity. If certain level is specified, the DAP cluster will generate Syslog messages including all lower levels. That is, if Syslog messages are separated by individual severity, a Warning level entry will also be included in Notice, Info and Debug processing. Notice is the default level of Syslog setting, and the system generates logs including levels of Notice, Warning, Error, Critical, Alert and Emergency. User can specify separate log level for different facilities (System, Security, Wireless, Network and User):

- AP Debug - Detailed log about the AP device
- System - Log about AP configuration and system status
- Security – Log about network security
- Wireless – Log about wireless RF
- Network – Log about network change
- User - Log about client

Log Remote:

Settings of the remote log server. If configured and enabled, besides storage in local file, Syslog messages of all APs in cluster can be sent to and stored in the server once generated.

Log File:

Download the log file on a selected DAP in the cluster to your configuring machine. Syslog messages are stored in a local file when generated. For one DAP, up to 1MB size of syslog messages can be saved in the local log file. The log file is FIFO; new syslog messages will replace the old ones if the size exceeds 1MB.



Note

Syslog is divided into eight levels, and lowest level 0 is Emergency severity while highest level 7 is Debug severity. Definition of Syslog severity as follow:

Level Value	Severity	Keyword	Description
0	Emergency	EMERG	System is unusable
1	Alert	ALERT	Should be corrected immediately
2	Critical	CRIT	Critical conditions
3	Error	ERR	Error conditions
4	Warning	WARNING	May indicate that an error will occur if action is not taken
5	Notice	NOTICE	Events that are unusual, but not error conditions
6	Info	INFO	Normal operational messages that require no action
7	Debug/All	DEBUG	Information useful to developers for debugging

8.7 Configuring SNMP

SNMP was supported in cluster mode; Administrator can monitor DAP status in the cluster through traditional network management platform. In the current build, only SNMPv2 and SNMPv3 was supported and SNMPv1 are not supported by DAP.

Related parameters can be configured on Syslog&SNMP window by clicking **System** frame.

8.7.1 Configuring SNMPv2

Select snmp version 2, illustrated in Figure8-7-1:

The screenshot shows the 'Syslog & SNMP' configuration window. The 'SNMP' tab is selected. The 'SNMP Agent' is turned on. The 'Version' is set to 'v2c'. The 'Community' is set to 'public'. The 'SNMP Trap' is also turned on. The 'Version' for traps is 'v2c'. The 'Trap Server' is '127.0.0.1'. The 'Community' for traps is 'public'. The 'Trap List' contains 'apColdBoot'. At the bottom are 'Cancel' and 'Save' buttons.

Parameter	Value
SNMP Agent	on
Version	v2c
Community	public
SNMP Trap	on
Version	v2c
Trap Server	127.0.0.1
Community	public
Trap List	apColdBoot

Figure8-7-1 SNMPv2 Configuration

- **SNMP Agent** – Enable/Disable the SNMP agent on DAP. Network management platform can fetch information from DAP through SNMP protocol.
- **Version** – Select SNMP version v2c or v3.
- **Community** – The credential used to communicate between DAPs and network management platform.
- **SNMP Trap** – Enable/Disable DAP to send trap to network management platform.
- **Trap Server** – Network management platform to which DAP send SNMP traps.
- **Trap List** – Specify the trap items needs to be sent to network management platform.

8.7.2 Configuring SNMPv3

Select snmp version 3, illustrated in Figure8-7-2:

Figure8-7-2 SNMPv3 Configuration

- **Username** – SNMP server uniquely identifies users.
- **Passphrase** – Authentication password, length 8-16 bytes. The SHA authentication protocol is currently used by default.

9 Wireless Management

The Wireless page focuses on advanced wireless functions, including three windows: RF (Radio Frequency), Wireless Intrusion Detection System/Wireless Intrusion Prevention System (wIDS/wIPS), and wireless performance optimization, illustrated in Figure9-1 Wireless Page.

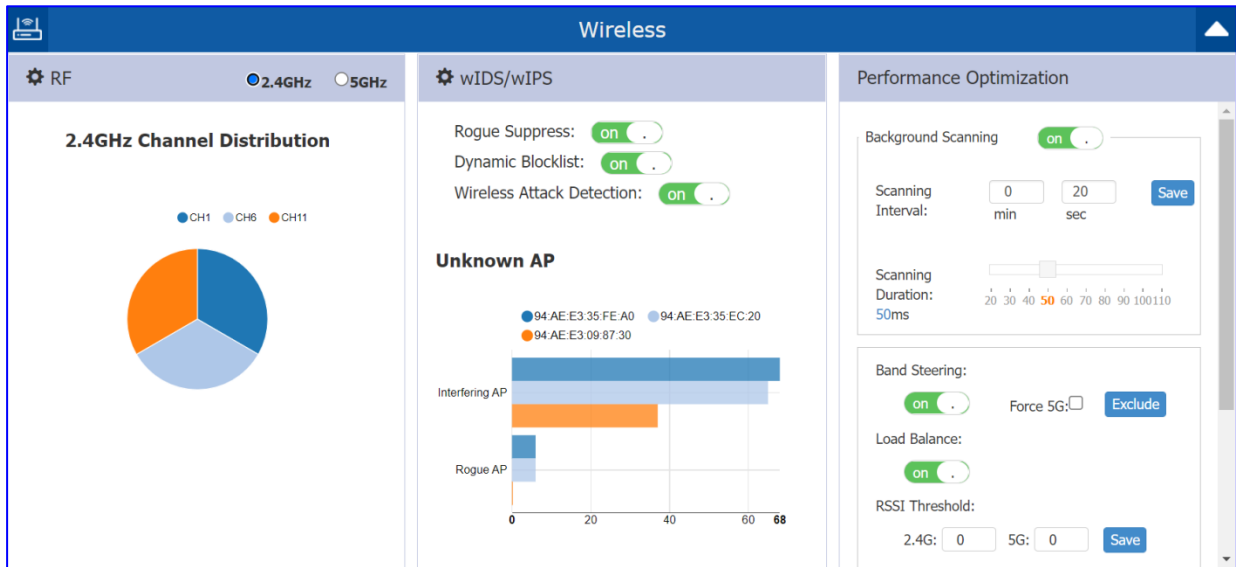


Figure9-1 Wireless Page

This chapter mainly presents the following three functions:

- [RF Configuration](#)
- [wIDS/wIPS](#)
- [Performance Optimization](#)

9.1 RF Configuration

Radio Frequency (RF) window is for monitoring the wireless utilization and configuring wireless attributes like channel and transmitting power.

There are two modes for RF Window, Simplified Mode illustrated in Figure 9-1-1 and Advanced Mode illustrated in Figure 9-1-2; you can launch the Advanced Mode from Simplified Mode by clicking the RF Window Frame.

Simplified mode displays the monitoring information of channel distribution, can be selected on 2.4G band or 5G band. Channels are separated by different colors, when you move the mouse cursor to the colored section of the pie chart; it displays the clients connected to the AP cluster through 2.4G band or 5G band.

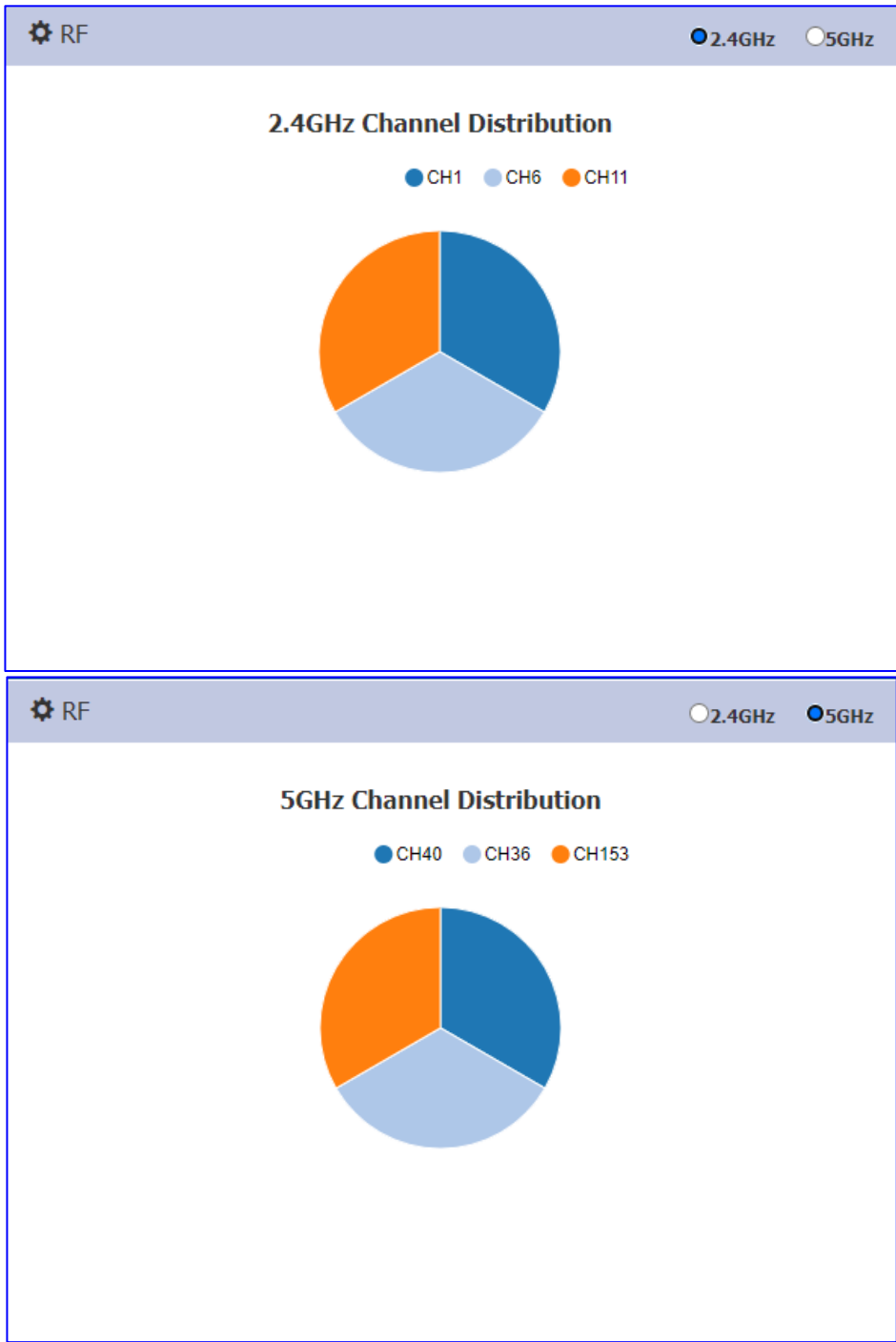


Figure 9-1-1: RF Window

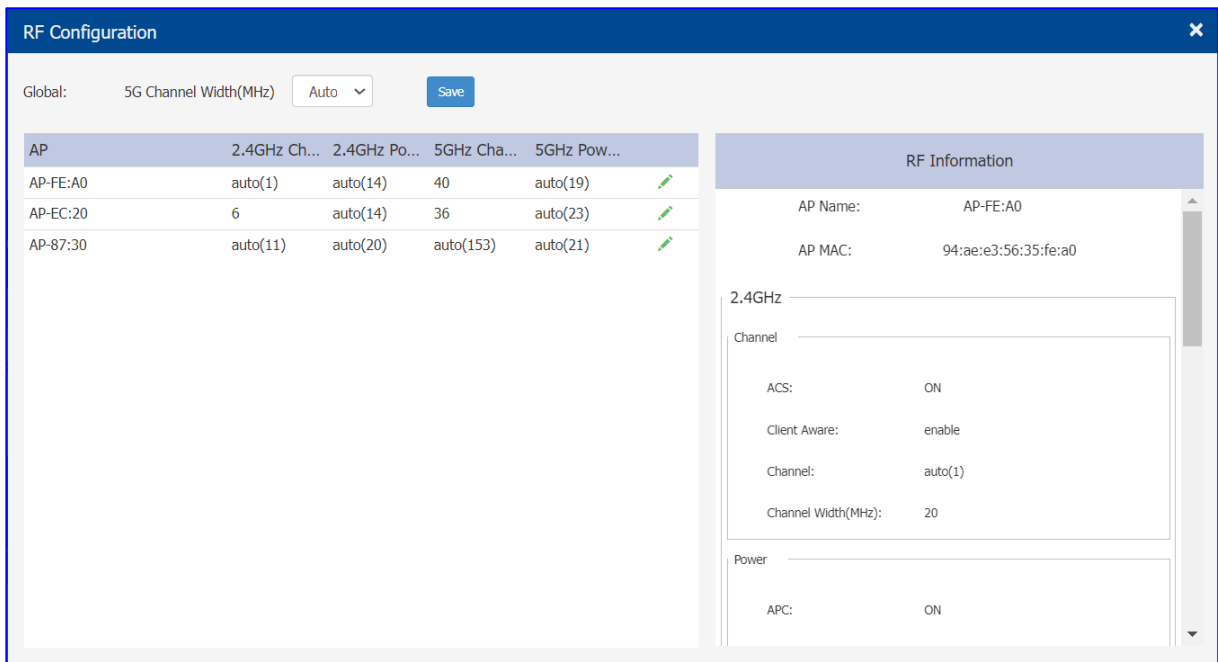


Figure 9-1-2: RF Configuration Window

The left side of the RF Configuration window displays the list of working channels and transmitting power of all DAPs in the cluster. When you pick an AP from the list, its detailed RF information is displayed on the right side of the window. The global configuration can be used to change 5GHz channel width for all DAPs in the cluster for efficiency or you can change the channel width for specific DAP by individually editing it, shown in Figure9-1-3. The private configuration based on individual DAP will take effect if both global setting and private configuration exist.

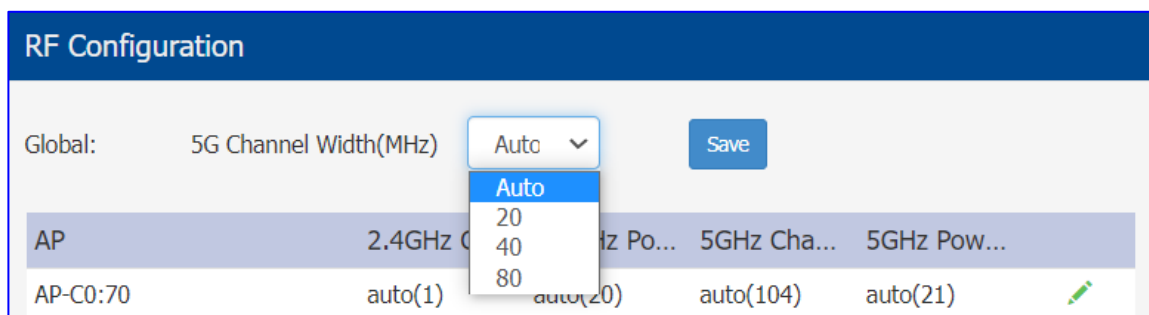


Figure 9-1-3: Global 5G Channel Width Configuration



Note

Regarding the channel width for 160MHz, it cannot be configured in global configuration; it is a private configuration due to some restrictions such as the supported AP model, scope of supported channel and power supply.

9.1.1 Modify AP Transmission Power and Channel

You can modify the transmission power and working channel for the DAP in the RF Configuration Window, shown in Figure9-1-1-1, by default, the working channel and transmitting power are automatically managed by Dynamic Radio Management (DRM) technology. If you want to set the channel and power values for an AP manually, you need to disable the Automatic Channel Selection (ACS) and Automatic Power Control (APC); in manual mode the AP transmits power can be adjusted in 1 dB increments.

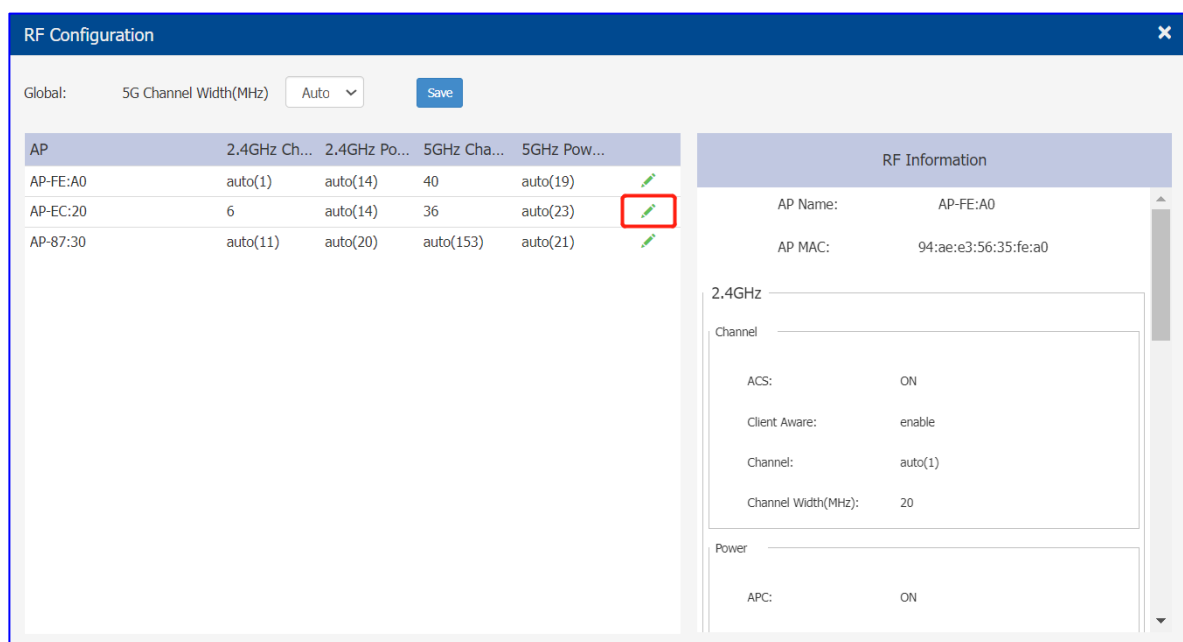


Figure9-1-1-1 RF Configuration

You can specify the channels list/power range applicable for auto selection, which can reduce the risk of low power transmitting or DFS channel conflict, shown in Figure9-1-1-2.

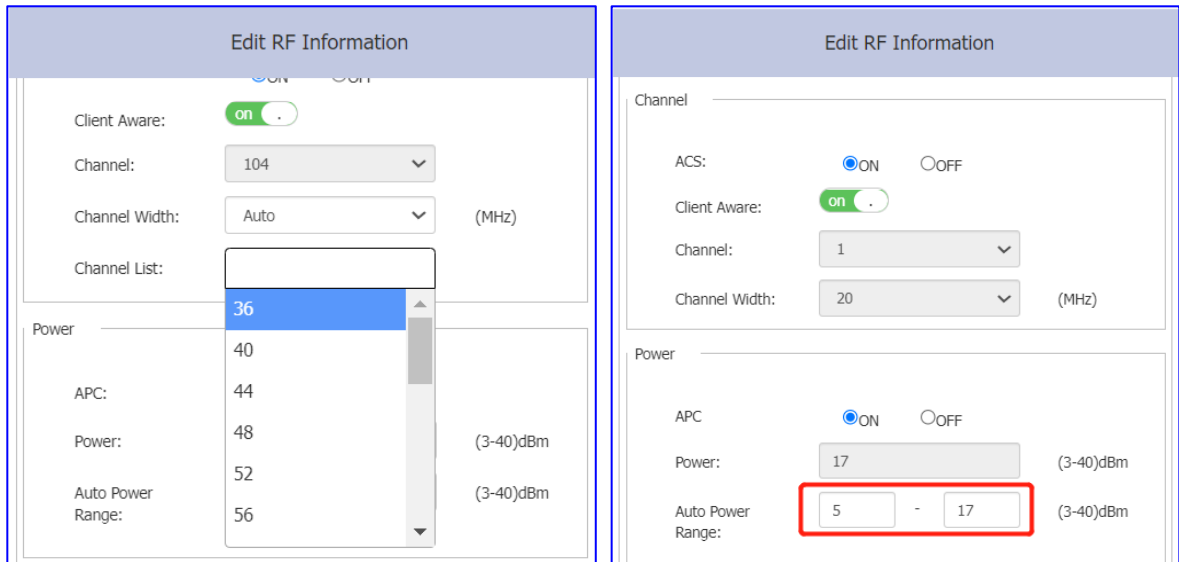


Figure 9-1-1-2 Specify channel list and power range

Key word specification in RF Configuration Window

Parameter	Specification
Client Aware	When enabled, Auto Channel Selection does not change channels for DAPs with connected clients, except for high-priority events such as RADAR detected. If "Client Aware" is Disabled, the DAP may change to a more optimal channel, which may temporarily disrupt current client traffic.
Short GI	Enable/Disable Short Guard Interval. In IEEE 802.11 OFDM-based communications, Guard Interval is used to ensure that distinct transmissions occur between the successive data symbols transmitted by a device. The standard symbol Guard Interval used in 802.11 OFDM is 800 nanoseconds in duration. To increase data rates, the 802.11 standard added optional support for a 400 nanoseconds guard interval (Short Guard Interval). This would provide approximately an 11% increase in data rates. However, using the Short Guard Interval will result in higher packet error rates when the delay spread of the RF channel exceeds the Short Guard Interval, or if timing synchronization between the transmitter and receiver is not precise. By Default, Short Guard Interval is enabled on the wireless radio. If the multipath effect is too serious (too many metals or other reflecting materials), disabling Short Guard Interval is recommended.
High Efficiency	Enable/Disable 802.11ax high efficiency wireless functionality. When disabled, the HE mode capable AP will downgrade to VHT (Very High Throughput) mode.

Table9-1-1-1 Key word specification in RF Configuration Window

9.1.2 Configure channel width to 160MHz

Channel width of 160MHz can be set in private configuration for DAP which supported, shown in Figure9-1-2-1, it has some restrictions show as below:

- 160MHz not supported on DAP620.
- 160MHz only supported on 5G radio with channel range 36-64,100-128.
- 160MHz only supported when AP powered by DC power injector or POE+(or higher)
- Only static 160MHz channel width is supported, Auto Channel Selection will not use 160MHz channels

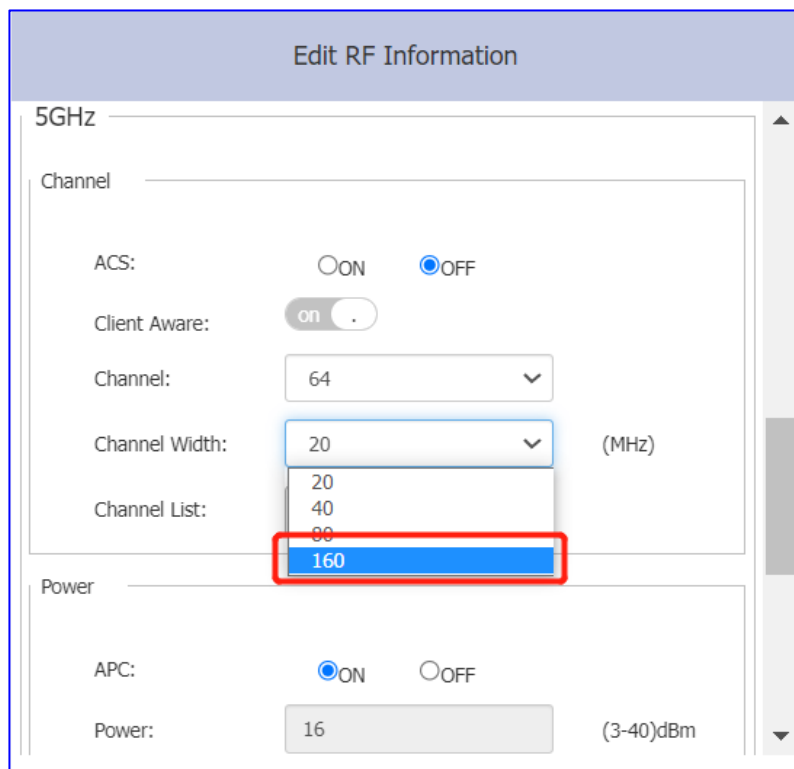


Figure 9-1-2-1 Configure channel width to 160MHz

9.1.3 Turn ON/OFF a specific AP Radio

You can turn OFF specific wireless radios for DAPs in the cluster to reduce the radio emissions or for other purpose with Radio ON/OFF button, shown in Figure9-1-3-1.

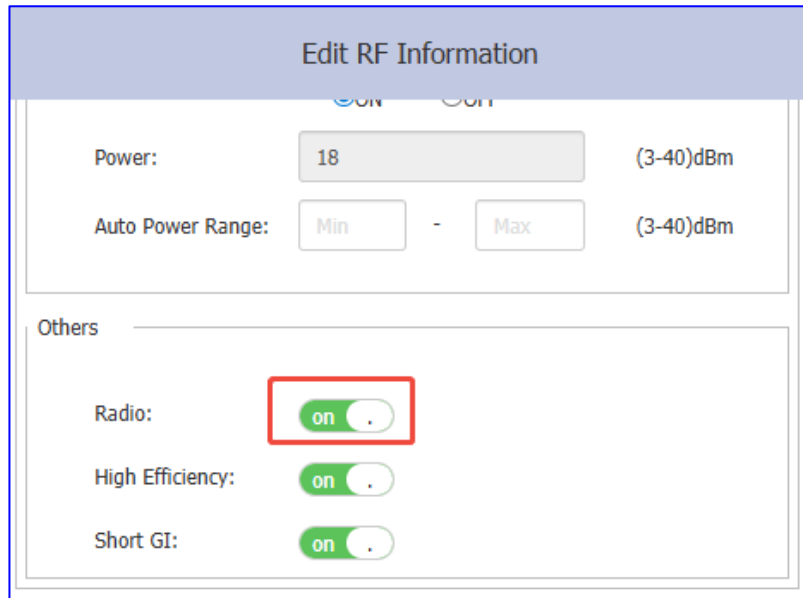


Figure9-1-3-1 Turn ON/OFF Radio

9.2 wIDS/wIPS

DAP provides the basic wIDS/wIPS functions under cluster mode, to achieve more advanced functions required, it is recommended to use DAC/BWO mode and purchase relevant licenses.

WIPS (Wireless Intrusion Prevention System) is a layer 2 protocol detection and protection function developed for 802.11 protocol. WIPs detects wireless behaviors or devices that threaten network security, interfere with network services and affect network performance through channel monitoring, analysis and processing, and provides countermeasures against invading wireless devices to provide a complete set of security solutions for wireless networks.

WIDS (Wireless Intrusion Detection System) can detect malicious user attacking and intrusions early, and protect enterprise networks and users from unauthorized devices on wireless networks. WIDS can monitor the wireless network without reducing the network performance and provide real-time prevention against various attacks.

Rogue Suppress: DAP supports preventing the connections of the client attached on Rogue AP by sending a de-authentication frame with client's MAC address to the

Rogue AP; this can disconnect the client whom already connected to the Rogue AP. If a known AP is confirmed as non-interference or a legal AP, you can click "trust" in the list to set the AP as a "friendly AP", shown in Figure9-2-1; it is disabled by default, shown in Figure9-2-2.

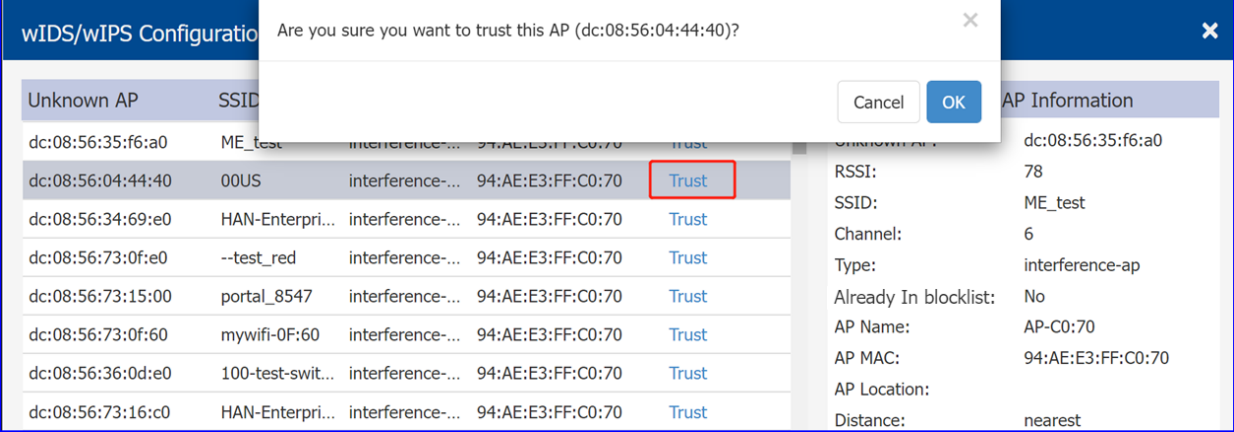


Figure9-2-1 Trust AP

Dynamic Blocklist: If enabled, all the ad-hoc devices found will be added to the AP Blocklist automatically, which prevents the ad-hoc device from changing its role to act as a client and access to AP wireless network. By default, the ad-hoc device is not added to the Blocklist automatically, shown in Figure9-2-2

Wireless Attack Detection: If enabled, DAP will detect multiple attacks originating from foreign APs, it is disabled by default, shown in Figure9-2-2.

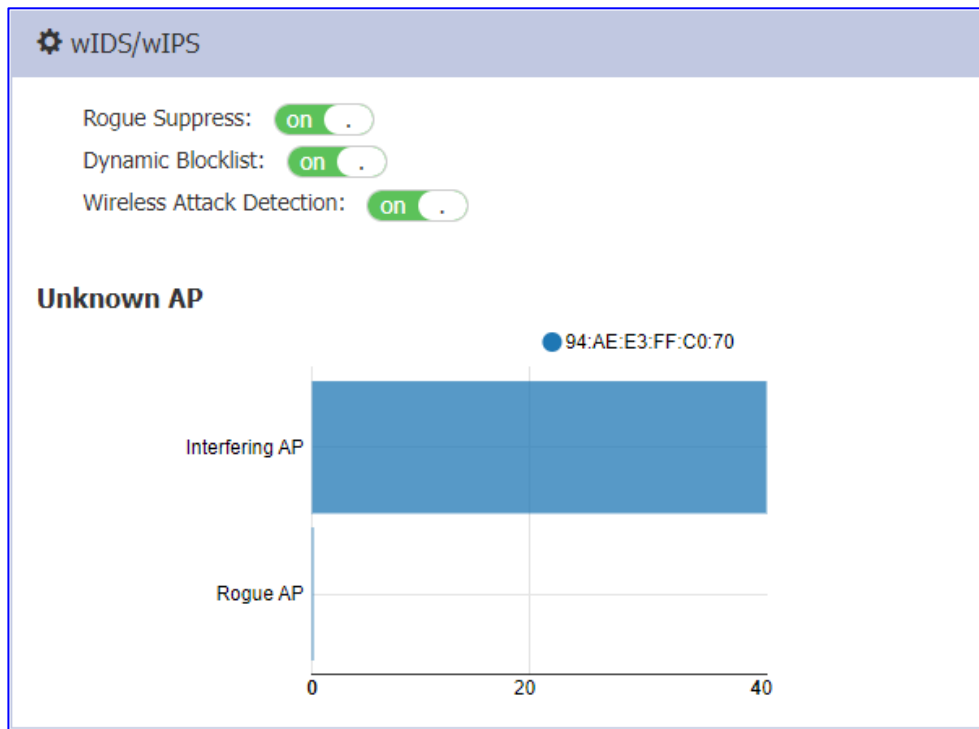


Figure9-2-2 wIDS/wIPS Window

Rogue AP: An unauthorized AP plugged into the wired side of the network or a foreign interfering AP broadcasting the same SSID with the DAP cluster. A Rogue AP is considered a security threat to the DAP cluster.

Interfering AP: An AP seen in the wireless environment but not connected to the wired network. The interfering AP can provide RF interference potentially; however, it is not considered a direct security threat, because it is not connected to the wired network.

Allowlist: Both interfering APs and Rogue APs are foreign unknown APs which can be found by background scanning and listed in the unknown AP list. However, some foreign APs found are trusted APs, those are not suitable for being classified as interfering APs or Rogue APs. To avoid this confusion, you can add the trusted MAC address or MAC-OUI to the AP Allowlist, illustrated in Figure9-2-3. If a foreign AP MAC address is added to the Allowlist, it will not be displayed in the unknown AP list.

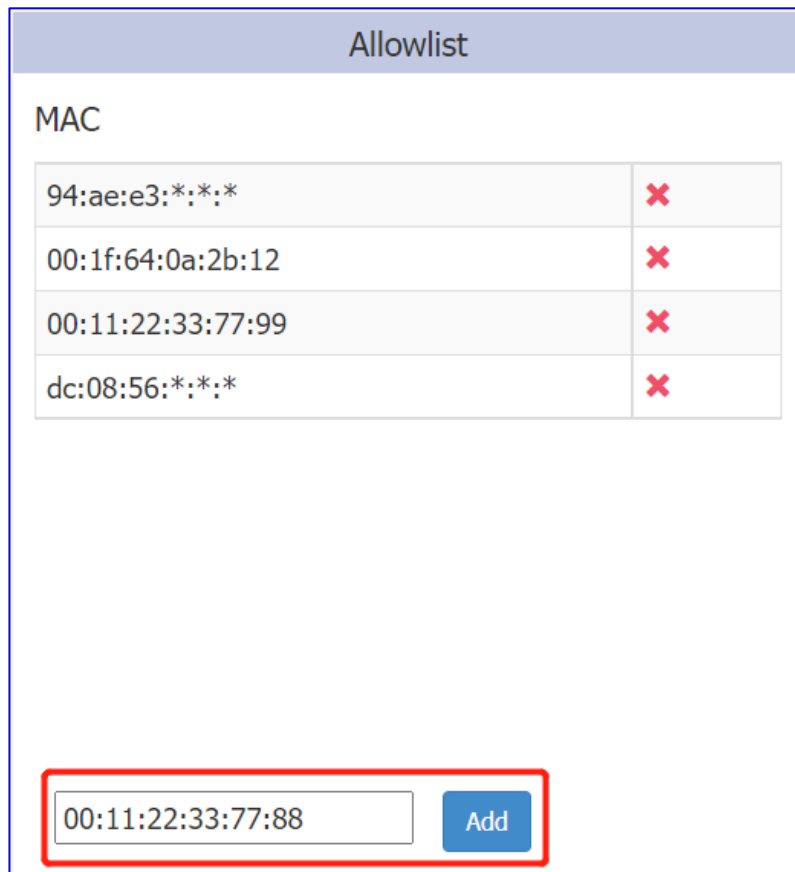


Figure9-2-3 AP Allowlist tab

You can see the lists information for the interfering APs and Rogue APs in wIDS/wIPS Configuration page after you click the wIDS/wIPS window frame, and you can also see the detailed information of interfering APs and Rogue APs, such as the RSSI, Channel, Encryption Type..., illustrated in Figure9-2-4.

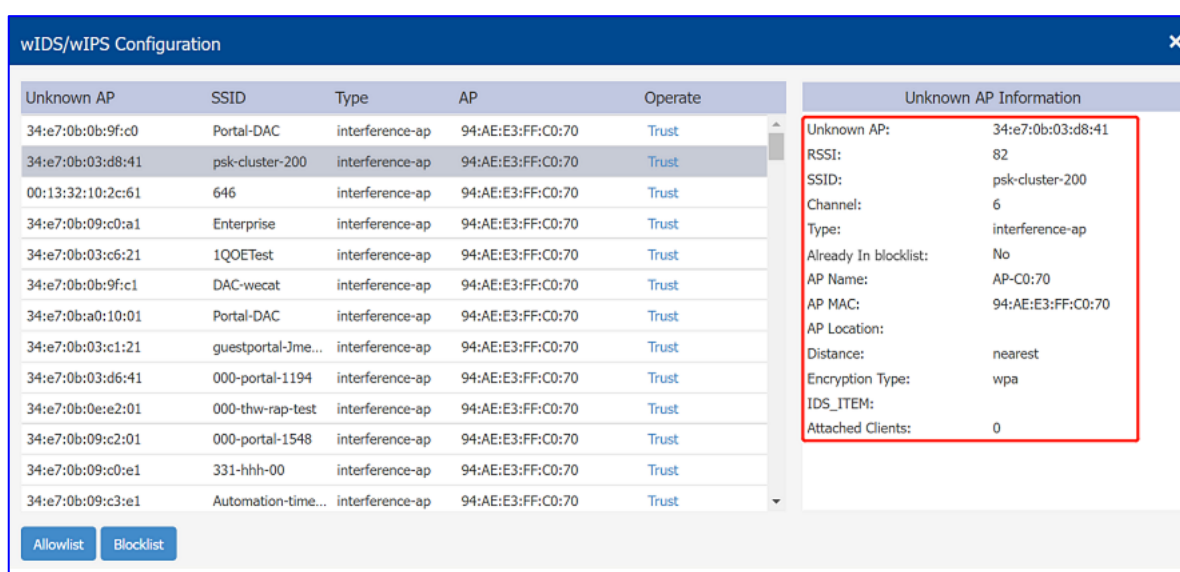


Figure9-2-4 wIDS/wIPS Configuration Window

Blocklist: Only Rogue APs can be added to the Blocklist. If a Rogue AP is added to the Blocklist, it cannot change its role to act as a client and access to the DAP wireless network, illustrated in Figure9-2-5

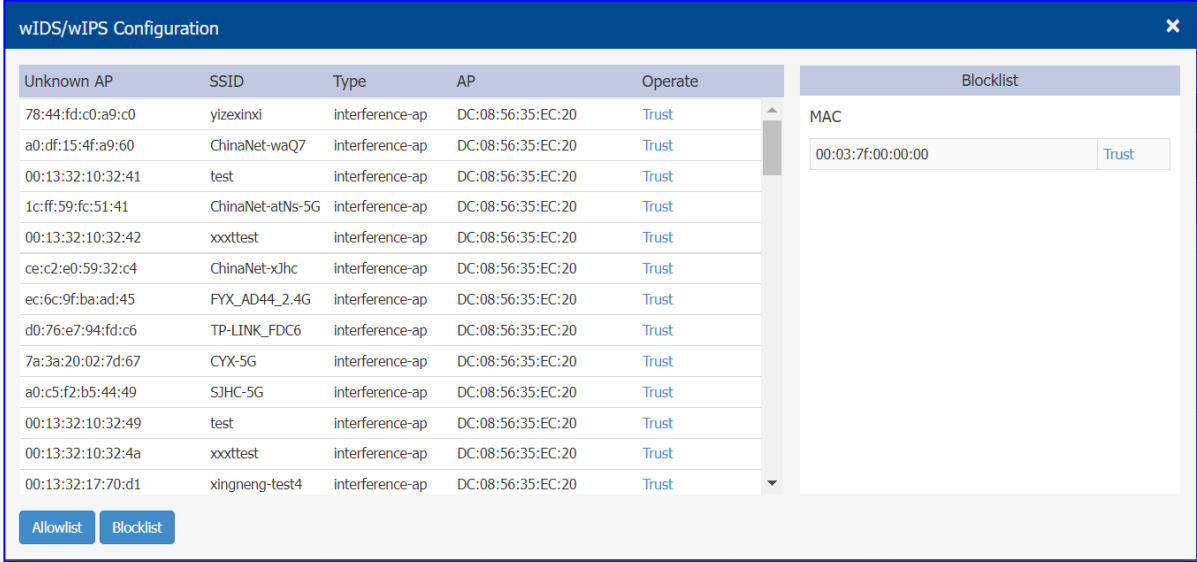


Figure9-2-5 AP Blocklist

Parameter	Specification
Unknown AP	MAC address of the unknown AP detected in the nearby.
SSID	SSID broadcasting by the unknown AP.
Type	Classified result of the unknown AP, can be interfering AP or Rogue AP.
RSSI	Received Signal Strength Indication of the unknown AP.
Channel	Working channel of the unknown AP.
Already In Blocklist	Flag of ad-hoc device, depends on the “Dynamic Blocklist” switch. If on, the ad-hoc devices will be automatically added to the Blocklist and the flag is true (Yes); If off or the unknown AP in list is not an ad-hoc device, the flag is false (No).
AP/AP Name	Name of detecting AP in the Cluster.
AP MAC	MAC of detecting AP in the Cluster.
AP Location	Location of detecting AP in the Cluster.
Distance	Distance between unknown AP and the detecting AP in the Cluster, it is measured by RSSI of the unknown AP: <ul style="list-style-type: none"> • Nearest – RSSI>(-20dBm); • Near – (-45dBm)<RSSI< (-20dBm); • Far - (-70dBm) <RSSI<(-45dBm);

	<ul style="list-style-type: none"> • Farthest - RSSI<(-70dBm);
Encryption Type	The encryption type of the SSID being broadcast by the unknown AP.
Attached Clients	The number of clients attached to the unknown AP, and MAC of each client.
Operate	Operation to trust the foreign AP and delete it from the unknown AP list. If the foreign AP is trusted, its MAC address will be added to the Allowlist.
Allowlist	Allowlist of foreign APs. Those not considered as security threat to the DAP network, you can add the trusted MAC address into Allowlist manually, see more in Figure 4-30.
Blocklist	Blocklist of foreign APs. Those classified as Rogue APs and pretending to act as a client to access the DAP network. If Dynamic Blocklist: <input checked="" type="checkbox"/> and there are detected ad-hoc devices, all of them will be added to the Blocklist automatically. You can remove a foreign AP from the Blocklist by the Trust operation.

Table9-2-1 Key words specification in WIDS/WIPS Configuration Window



- *Background scanning should be enabled as required by WIPS/WIDS function*
- *It is recommended the background scanning interval less than 1 minutes for better detecting efficiency*

9.3 Performance Optimization

Wireless performance optimization is useful to enhance the quality of wireless service for users. The performance optimization includes Background Scanning, Band Steering, Load Balance, RSSI Threshold, Roaming RSSI, Voice and Video Awareness, and Airtime Fairness, illustrated in Figure 9-3-1:

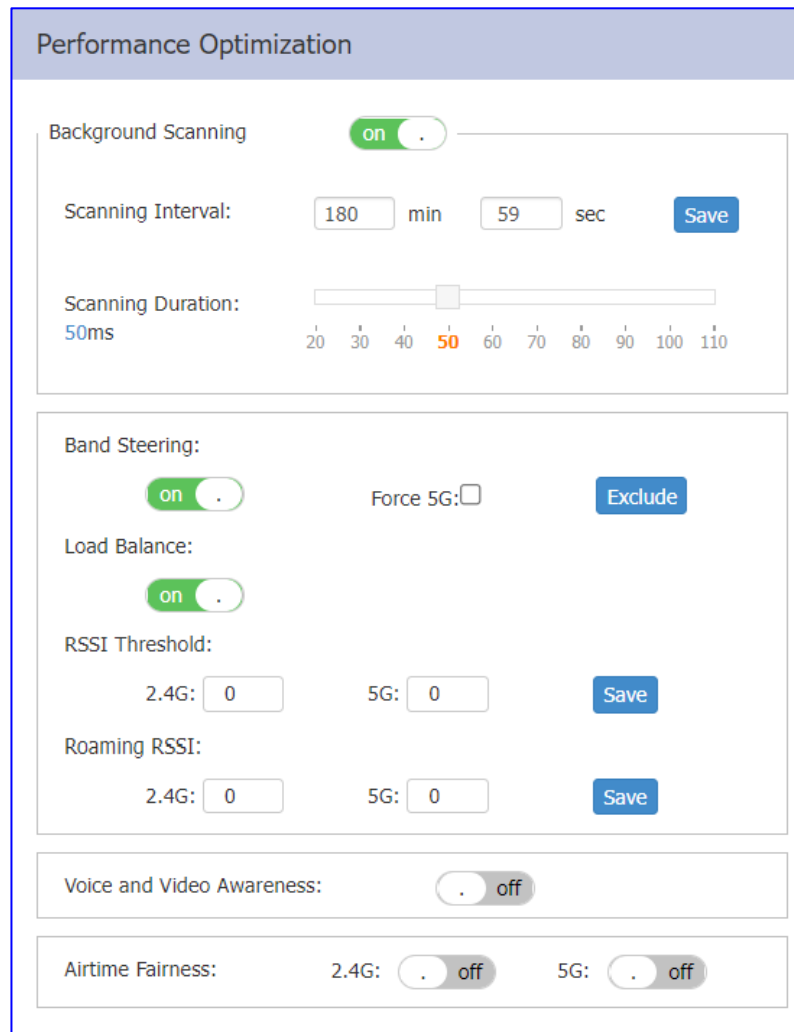


Figure 9-3-1 Wireless Optimization Window

Background Scanning:

Wireless networks operate in environments with electrical and radio frequency devices that can interfere with network communications. Microwave ovens, cordless phones, and even adjacent Wi-Fi networks are all potential sources of continuous or intermittent interference. The background scanning is able to examine the radio frequency (RF) environment in which the Wi-Fi network is operating, identify interference and classify its sources.

Background scanning is the basis for some advanced features such as: WIDS/WIPS, APC etc. When it's turned OFF, the foreign AP detection and Rogue suppression will stop and the DRM will drop its precision. By default, background scanning is enabled.

The scanning interval of Background Scanning can be configured from 5 seconds to 180 minutes according to deployment requirement. For highly sensitive packet delay

use case, it is recommended to set interval from default 20-second setting. If the interval is longer than 1 minute, WIPS feature accuracy will be impacted.



There are two wireless interfaces reserved in DAP620 for background scanning which named "athscan0" for 2.4G channels and "athscan1" for 5G channels, these two interfaces perform background scanning based on the settings of "Performance Optimization". For DAP640\DAP645\DAP646\DAP647, there is a dedicate scanning radio named "athmon2", it performs the background scanning both on 2.4G channels and 5G channels.

Band Steering:

Band steering supports **Prefer 5G** and **Force 5G**.

Prefer 5G: It assigns the dual band clients to the 5 GHz band prior to the 2.4G band. Thus can reduce co-channel interference and increase available bandwidth for clients, because there are more available channels on 5 GHz band. By default, band steering is enabled. When Band Steering is enabled and Force 5G is NOT selected, AP is working in Prefer 5G mode. The prefer-5GHz-band-steering is based on channel utilization and client density. When the 5G band is busy and connecting too many clients, a new client will be guided to connect to free 2.4G band.

Force 5G: DAP forces dual band clients to connect to the 5 GHz band. Dual band clients are not allowed to connect 2.4G radio. Those clients only supporting 2.4G band are permitted to connect to 2.4G radio. When Band Steering is enabled and Force 5G is selected, DAP is working in Force 5G mode.

Exclude: Excludes the clients from Band Steering. For example, user can exclude some special dual band terminals from Band Steering and DAP will let those terminals choose wireless band to connect freely.

Load Balance:

The principle of this is to provide fair distribution of clients among neighboring APs. Based on the client density, channel utilization on associated DAPs, and associating

clients RSSI value, it is steered from a busy DAP to an idle DAP. The thresholds for client density is 10, channel utilization is 70% for 2.4G and 70% for 5G. Load Balance is enabled by default.

RSSI Threshold:

Wireless access control, "RSSI threshold" only works during the client's association procedure ,if the client's SNR value is lower than "RSSI Threshold" ,AP will not response to the client, it does not effected by 802.11kv enabled or not, client with lower RSSI value than threshold is forbidden to access. By default, RSSI threshold is disabled (0). RSSI threshold can be applied to 2.4G band or 5G band separately. RSSI threshold is recommended to be deployed in high density scenario.

Roaming RSSI:

Wireless access control, client with lower RSSI value than setting is forced to roaming. By default, roaming RSSI is disabled (0). Roaming RSSI can be applied to 2.4G band or 5G band separately. "Roaming RSSI" is working together with 802.11k and 802.11v.

Voice and Video Awareness:

Background scanning needs to be aware of existing traffic on the DAP, if there is an ongoing voice/video service, scanning should not be performed to ensure uninterrupted traffic; and allows resuming scanning when there is no active voice/video traffic. Voice and Video Awareness feature is disabled by default.

Airtime Fairness:

All clients share the wireless transition time slice equally, even with traditional low speed clients present. Airtime fairness is disabled by default.

10Access

The Access Window focuses on user access management including: Authentication, Blocklist & Allowlist and ACL.

This chapter contains the following topics:

- [Authentication Window](#)
- [Three methods to Login Captive Portal](#)
- [Account & Access Code Management](#)
- [Customize Portal Page](#)
- [Client Blocklist based on wireless access](#)
- [Client Allowlist based on captive portal](#)
- [Walled Garden](#)
- [Multicast Control](#)
- [ACL](#)

10.1 Authentication Window

There are two modes for Access & Authentication Window, Simplified Authentication window illustrated in Figure10-1-1 and Authentication Configuration Window illustrated in Figure10-1-2. You can launch the Authentication Configuration Window from Simplified Mode by clicking the Authentication Window Frame.

Simplified Authentication Window displays the statistics information of the users' device and operating system, when you move the mouse cursor to certain sector of the pie chart, the number of related Device or OS will be displayed.

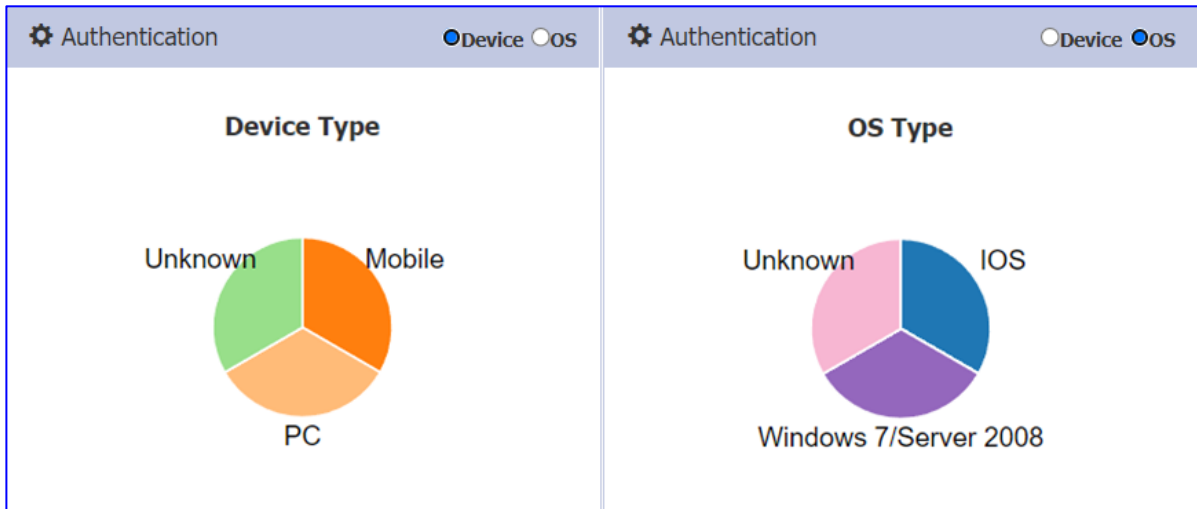


Figure 10-1-1 Authentication Window

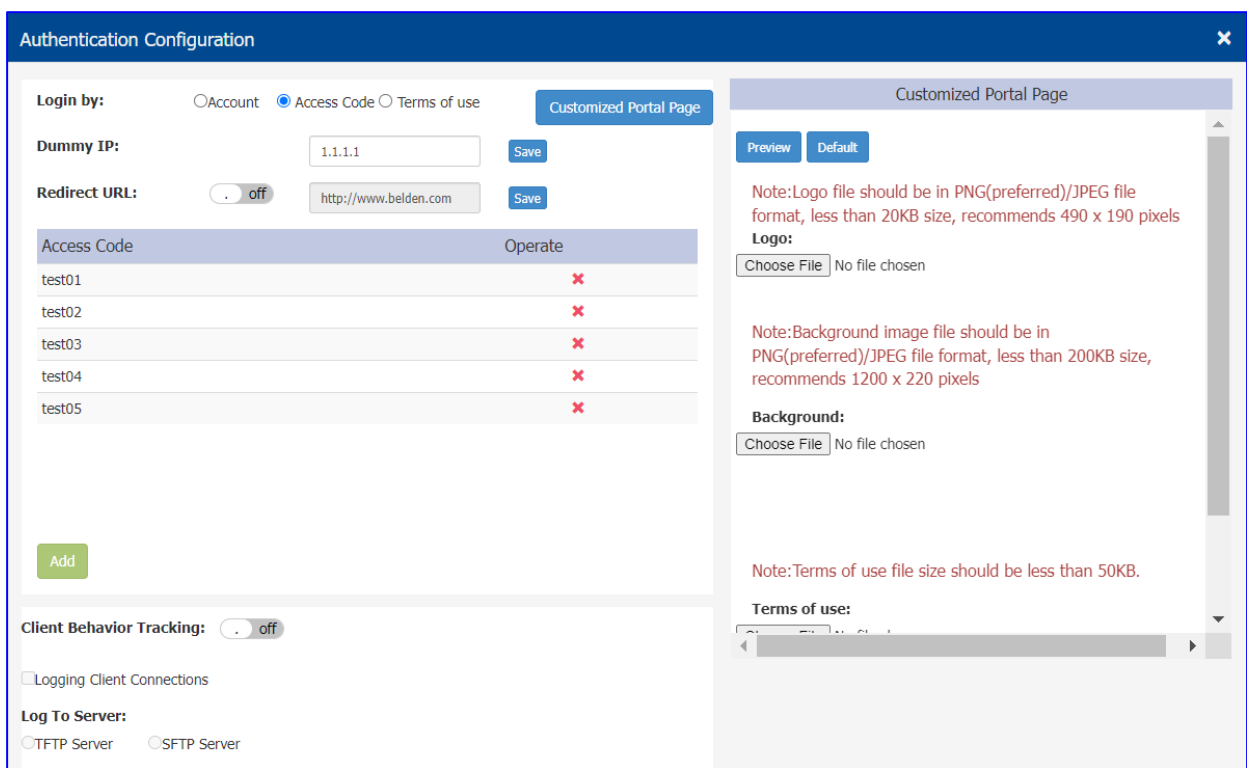


Figure 10-1-2 Authentication Configuration Window

Key words specification in Authentication Window :

Base on different requirement for customer, some other different configurable parameters can be set for special requirement, below are the key word specification in Authentication Configuration Window for your reference:

Dummy IP: IP address of captive portal FQDN

Client Behavior Tracking: Enable logging user behavior to a SFTP server or TFTP server. Connection information of all users including online and offline will be recorded

Logging Client Connections:

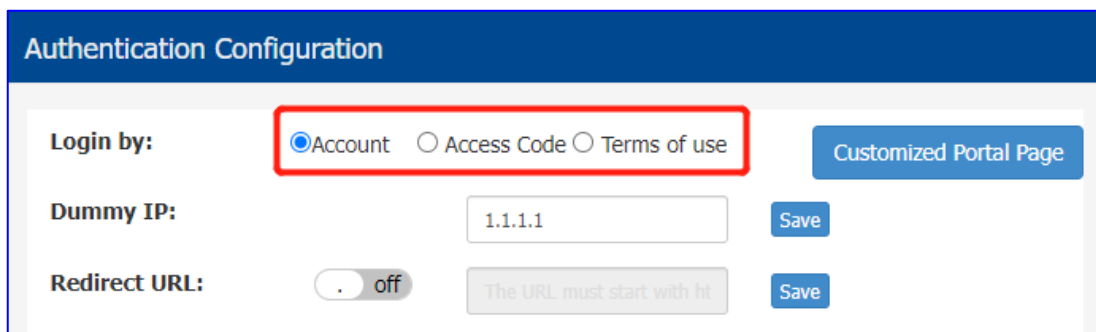
- HTTP/HTTPS – Record the HTTP/HTTPS web session of wireless clients
- ALL – Record the all the session including HTTP(s)/TCP/UDP of wireless clients

Log To Server:

- TFTP Server – Record the client connection information to a specific TFTP server by uploading log files
- SFTP Server – Record the client connection information to a specific SFTP server by uploading log files

10.2 Login Captive Portal

There are three login methods for the captive portal authentication for a Portal WLAN, **Account**, **Access Code** and **Terms of use**, it is Account by default which illustrated in Figure10-2-1, please refer to [6.2 Introduction to WLAN with different security modes](#) for how to create a Captive Portal WLAN.




The screenshot shows the 'Authentication Configuration' interface. The 'Login by' section has three radio buttons: 'Account' (selected), 'Access Code', and 'Terms of use'. The 'Dummy IP' field contains '1.1.1.1'. The 'Redirect URL' section has a toggle switch set to 'off' and a text box with the placeholder 'The URL must start with ht'. There are 'Save' buttons for the 'Dummy IP' and 'Redirect URL' fields, and a 'Customized Portal Page' button.

Figure10-2-1 Choose your login method

Login by Account: If **Account** selected, the username and password are required when user login, the related account should be created by Administrator or Guest Manager, illustrated in Figure10-2-2.

HIRSCHMANN IT
A BELDEN BRAND



Please login to the network using your username and password.

Username:

Password:


I accept the [terms of use](#)

Contact a staff member if you are experiencing difficulty logging in.

Figure10-2-2 login by Username and Password

Login by Access Code: An Access Code is required when user login, the related Access Code should be created by Administrator or Guest Manager, illustrated in Figure10-2-3.

HIRSCHMANN IT
A BELDEN BRAND



Please login to the network using your access code.

Access Code:

I accept the [terms of use](#)

Contact a staff member if you are experiencing difficulty logging in.

Figure10-2-3 login by Access Code

Login by Terms of use: No account or access code required and login to the network only by accepting terms, illustrated in Figure10-2-4.

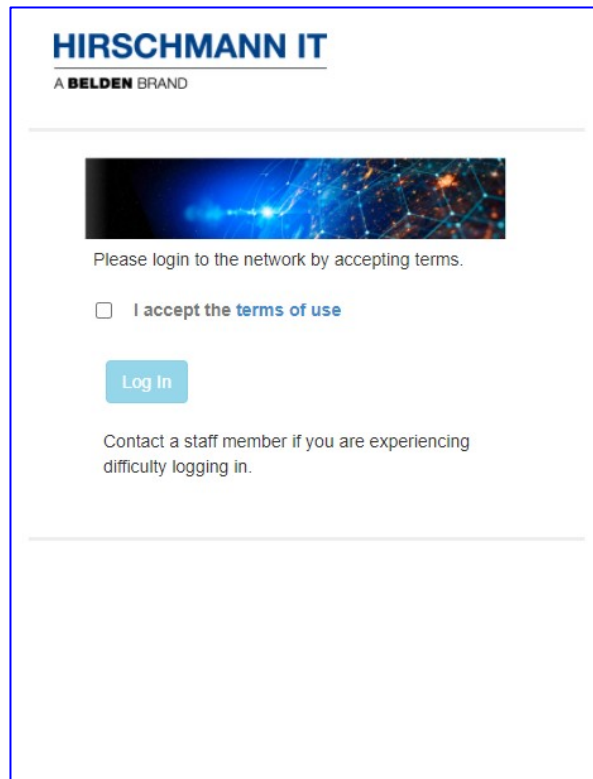


Figure10-2-4 login by Terms of use

10.3 Account & Access Code Management

If you have selected login by Account or Access Code for the captive portal authentication, it ONLY supports users in the local user database. It does not support connecting to an external authentication server. You can add Accounts or Access Codes to the local user database.

Add an Account: When 'Account' option selected as the login method, click '**Add**' button in authentication window and in the left side of authentication configuration page, you will see the parameters needed for creating an Account, the fields with * are required mandatory, and you will see the detailed information for an account in the left side of the window when you click one account, illustrated in Figure10-3-1 and Figure 10.3.2.

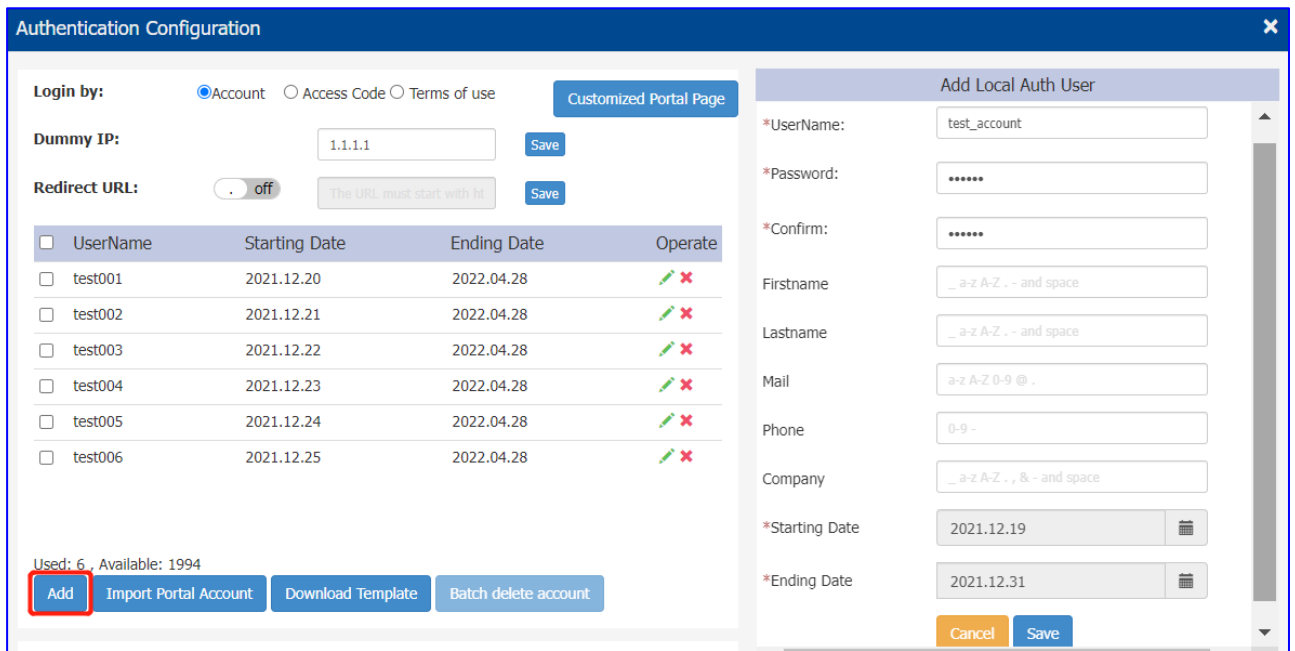


Figure10-3-1 Create an account

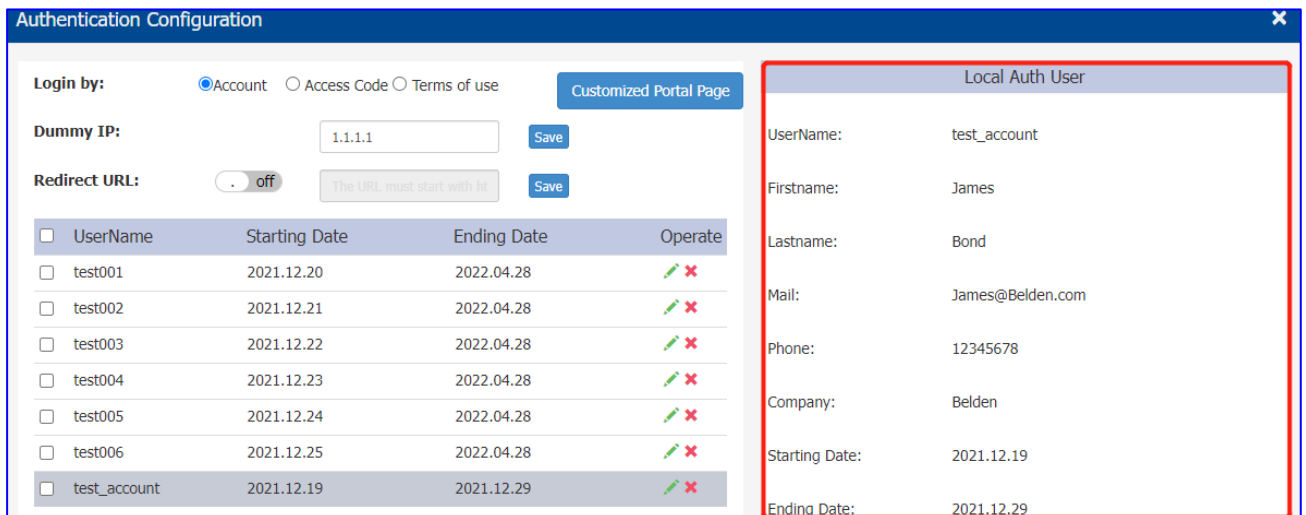


Figure10-3-2 Account detailed information

Import Portal Account: For the batch creation for the accounts, DAP also support import Portal Account from a local CSV file which modified by customer from the downloaded template, illustrated in Figure10-3-3.

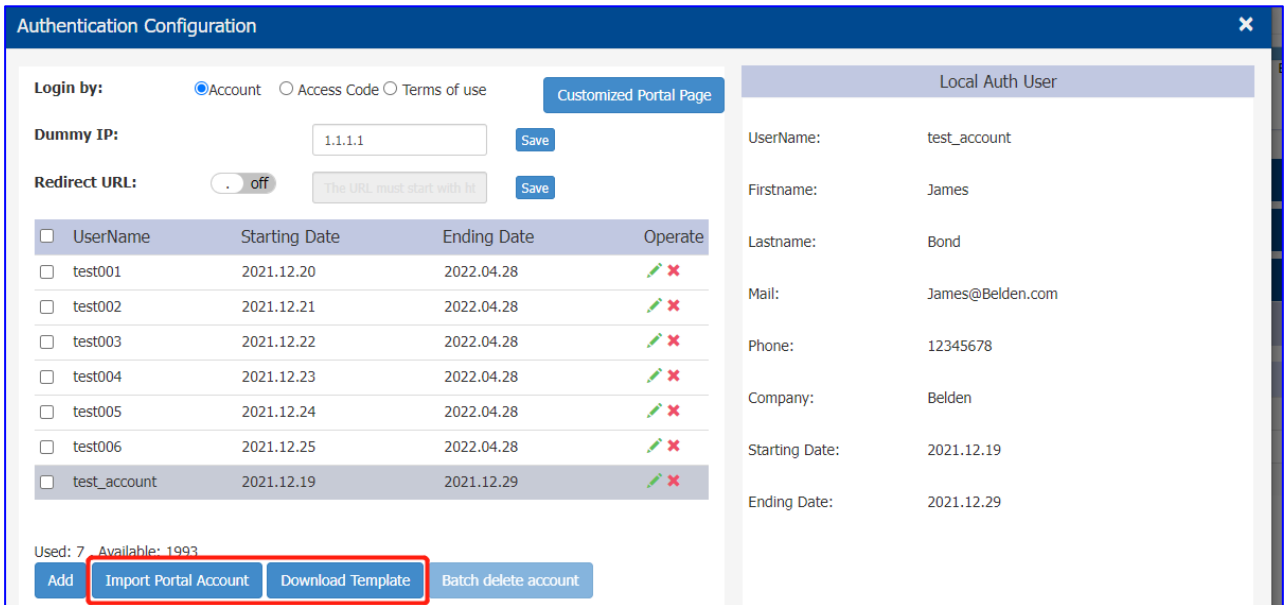


Figure10-3-3 Import Portal Account

Modify or Delete Account(s): Click ‘’ to modify an account, and specific account can be deleted by clicking ‘’, and batch account deletion also supported when multiple accounts selected and click ‘Batch delete account’ button, illustrated in Figure 10-3-4.

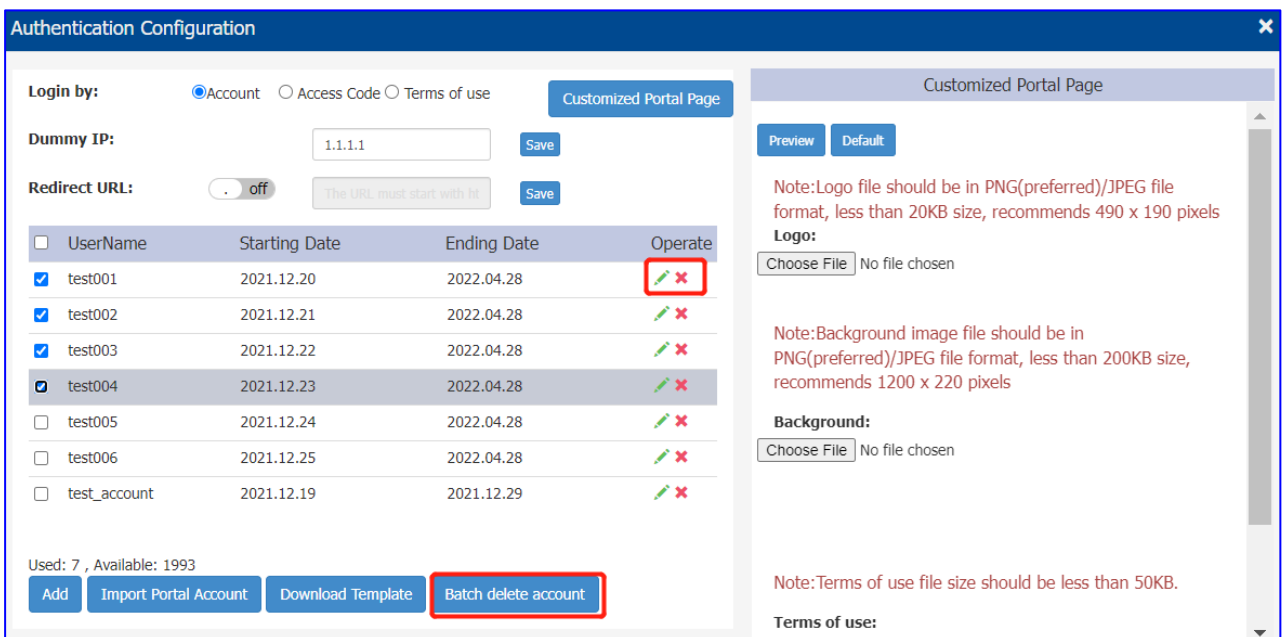


Figure10-3-4 Modify or Delete Account(s)

Create or delete an Access Code: When ‘Access Code’ option selected as the login method, Click ‘Add’ button in authentication window and in the left side of

authentication configuration page, you can add an Access Code for user, and the related Access Code will be deleted by clicking '✘', illustrated in Figure10-3-4.



Note

Single user Account or Access Code can be used by multiple devices simultaneously; there are no limits to the number of devices a captive portal user account can connect to the network.

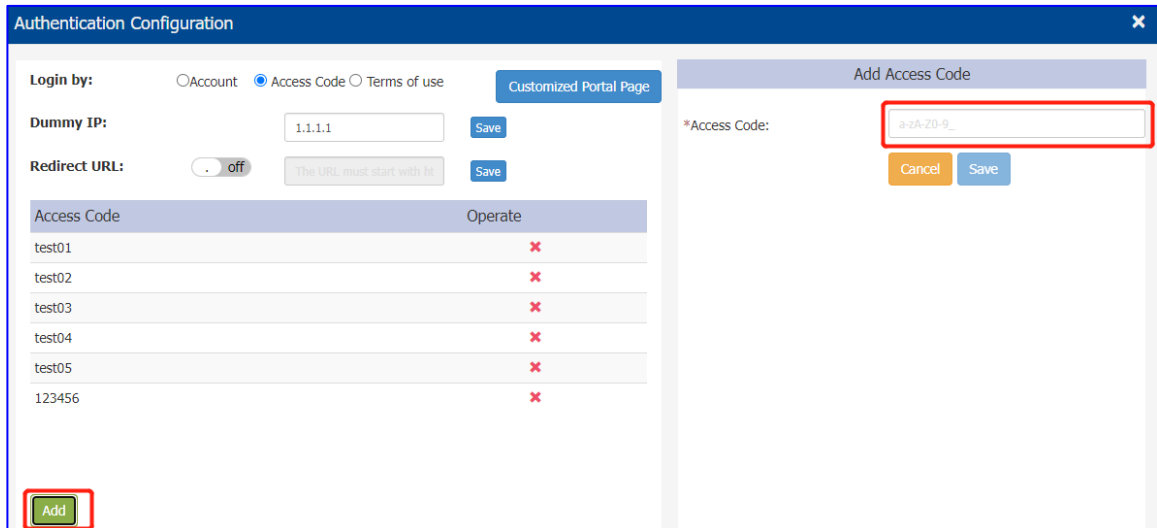


Figure10-3-4 Create an Access Code

10.4 Customize Portal Page

The Portal page can be customized base on the requirement of customer, the logo, background and Terms of use can be modified by customer, illustrated in Figure10-4-1.

Navigate: Dashboard->Access Page->Authentication Window-Authentication Configuration Window->Customized Portal Page.

- Upload the related file according the notes.
- Click the 'Preview' button to view the final demonstration of the customized portal page
- Click 'default' button will return to the default portal page.

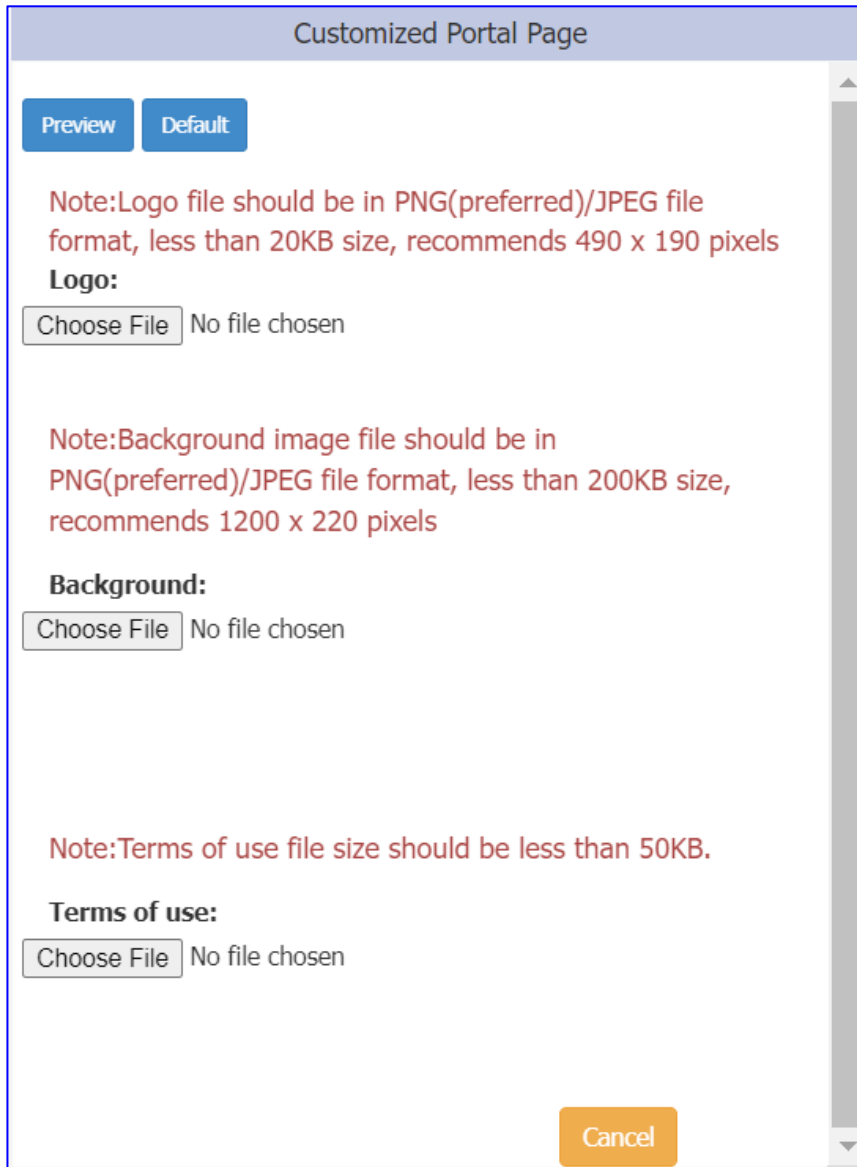


Figure10-4-1 Customize Portal Page

10.5 Client Blocklist based on wireless access

Blocklist focus on the basic access control mechanism for users connecting to SSID based on the client level; those clients on the Blocklist are denied associating to the DAP, once a client is in the Blocklist, it cannot connect to any WLAN of any security level (Enterprise/Personal/Open). You can add/delete the Blocklist based on client's MAC address, illustrated in Figure10-5-1.

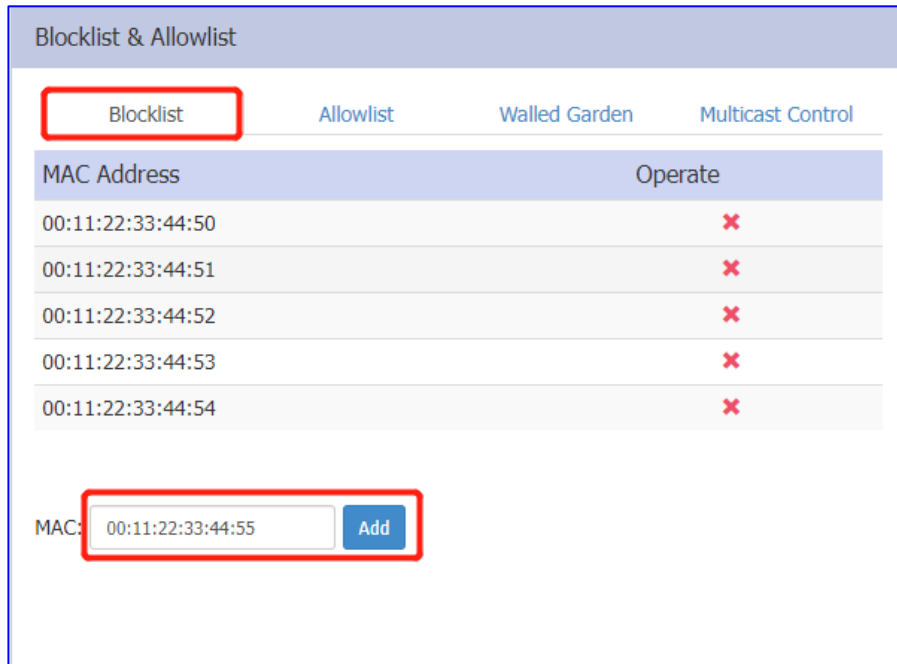


Figure10-5-1 Blocklist configuration

10.6 Client Allowlist based on captive portal

The Allowlist is applied to captive portal authentication ONLY. Those clients on the Allowlist are permitted to access the network resources without a captive portal authentication. You can manually add/remove client(s) to/from the Allowlist for captive portal authentication by MAC address, illustrated in Figure10-6-1. The Allowlist does not support Enterprise/Personal WLANs. This means that the clients in the Allowlist are not allowed to access Enterprise/Personal WLANs without using correct credentials.

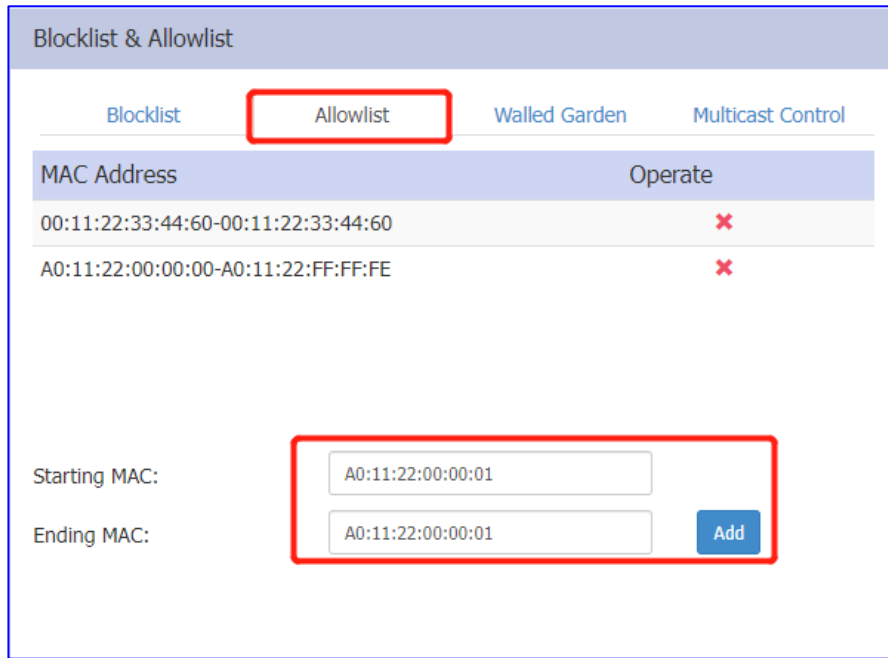


Figure10-6-1 Allowlist configuration

10.7 Walled Garden

The Walled Garden is a control mechanism over network resources; it restricts access to non-approved applications or contents. The Walled Garden is applied for Captive Portal authentication ONLY. The client can access the network resources listed in the Walled Garden before passing a Captive Portal authentication. You can add/remove allowed domain(s) or IP(s) to/from the walled garden, illustrated in Figure10-7-1 and Figure10-7-2.

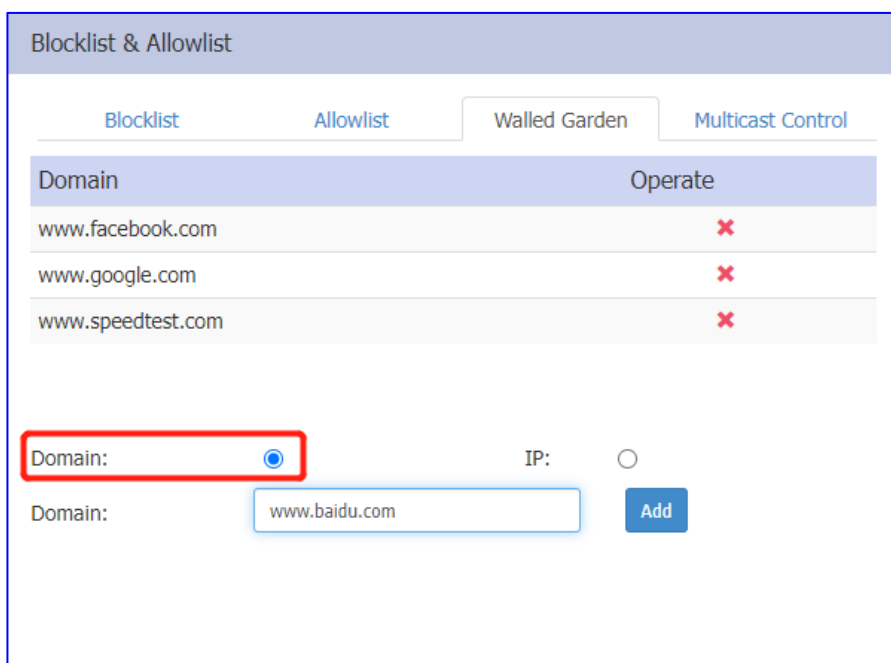


Figure10-7-1 Walled Garden configuration for domain

The screenshot shows a configuration window titled "Blocklist & Allowlist" with four tabs: "Blocklist", "Allowlist", "Walled Garden", and "Multicast Control". The "Walled Garden" tab is active. Below the tabs is a table with two columns: "IP" and "Operate". The table contains four rows of IP address ranges, each with a red "X" in the "Operate" column. Below the table are radio buttons for "Domain:" (unselected) and "IP:" (selected). There are two input fields for "Starting IP:" and "Ending IP:", both with placeholder text "IP Address (v4 | v6)". An "Add" button is located to the right of the "Ending IP:" field.

IP	Operate
172.16.188.130-172.16.188.135	✘
192.168.199.20-192.168.199.20	✘
10.1.1.100-10.1.1.100	✘
172.16.10.220-172.16.10.220	✘

Domain: IP:

Starting IP:

Ending IP:

Figure10-7-1 Walled Garden configuration for IP Address

10.8 Multicast Control

The Multicast Control targets on the mDNS multicast traffic forwarding from wired network (switch ports) towards DAP. When enabled, only traffic from the configured multicast source in the Allowlist can be forwarded by DAP to the clients connecting to it. Maximum 8 items of multicast Allowlist are supported. When Multicast Allowlist is disabled, the mDNS multicast traffic is forwarding without conditions, illustrated in Figure10-8-1

Blocklist & Allowlist

Blocklist Allowlist Walled Garden **Multicast Control**

Multicast Allowlist: on

Multicast Type	Destination IP	Source MAC	Operate
mDNS	224.0.0.251	c0:3c:59:70:3d:c5	✘
mDNS	224.0.0.251	c0:3c:59:70:3d:c6	✘
mDNS	224.0.0.251	c0:3c:59:70:3d:c7	✘

Multicast Type:

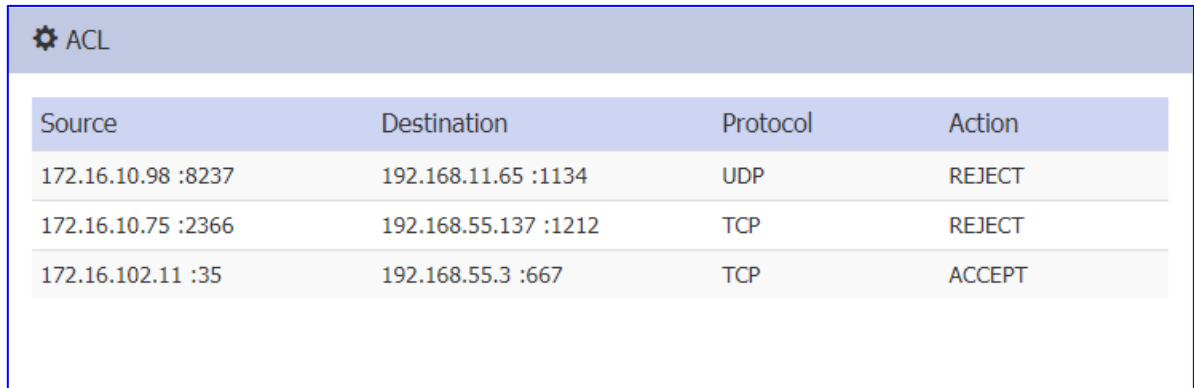
Destination IP:

Source MAC:

Figure10-8-1 Multicast Control

10.9 ACL

There are two modes for ACL Window, Simplified window which only list the ACL entries illustrated in Figure10-9-1 and ACL Configuration window illustrated in Figure10-9-2; you can launch the ACL Configuration window from Simplified window by clicking the ACL Window Frame.

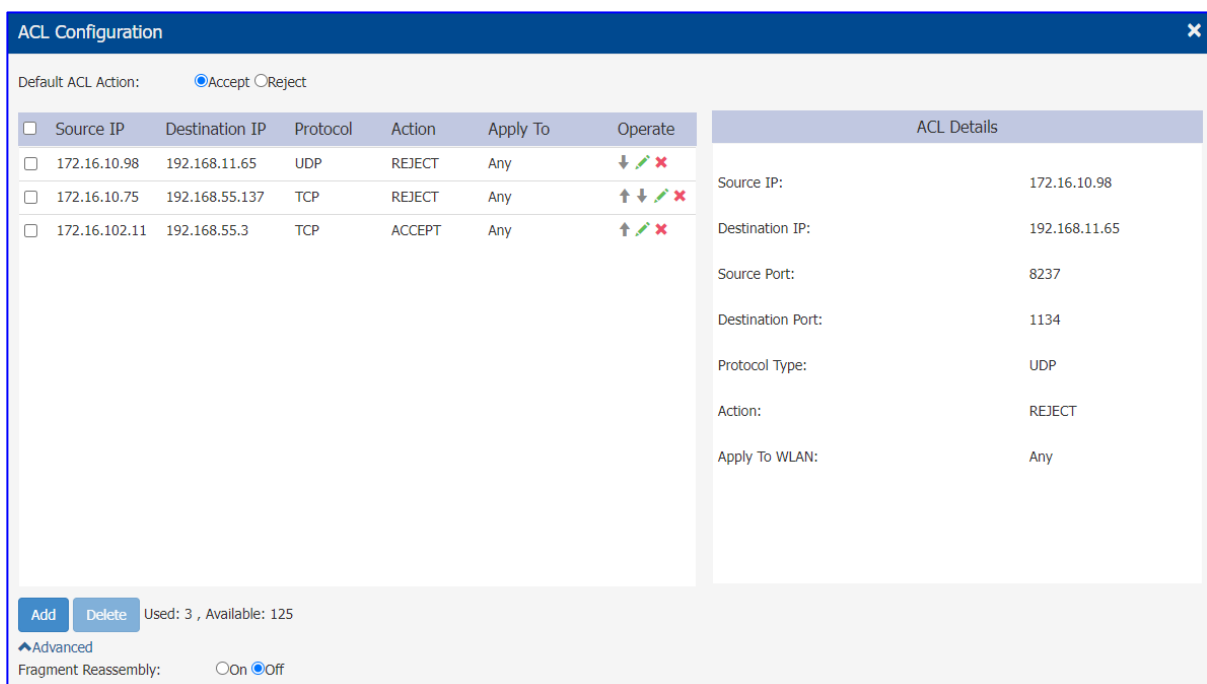


The image shows a simplified ACL window with a table of three rules. The table has columns for Source, Destination, Protocol, and Action. The rules are as follows:

Source	Destination	Protocol	Action
172.16.10.98 :8237	192.168.11.65 :1134	UDP	REJECT
172.16.10.75 :2366	192.168.55.137 :1212	TCP	REJECT
172.16.102.11 :35	192.168.55.3 :667	TCP	ACCEPT

Figure10-10-1 Simplified ACL Window

Up to 128 rules supported by DAP, you can create L3 ACLs using wildcard entries for both IP address and TCP/UDP/ICMP ports. The ACL rules created in the list are applied sequentially, based on the precedence of top-to-bottom, by default, traffic is allowed to pass if no ACL rules are matched (Default ACL action is 'Accept'), illustrated in Figure10-9-2.



The image shows the ACL Configuration window. At the top, it says "ACL Configuration" with a close button. Below that, it shows "Default ACL Action: Accept Reject". There is a table with columns: Source IP, Destination IP, Protocol, Action, Apply To, and Operate. The table contains three rules. To the right of the table is an "ACL Details" section showing the configuration for the selected rule. At the bottom, there are "Add" and "Delete" buttons, and a status bar showing "Used: 3, Available: 125". There is also an "Advanced" section with "Fragment Reassembly: On Off".

Source IP	Destination IP	Protocol	Action	Apply To	Operate	ACL Details
<input type="checkbox"/> 172.16.10.98	192.168.11.65	UDP	REJECT	Any	↓ ↕ ↗ ✖	Source IP: 172.16.10.98
<input type="checkbox"/> 172.16.10.75	192.168.55.137	TCP	REJECT	Any	↑ ↓ ↕ ↗ ✖	Destination IP: 192.168.11.65
<input type="checkbox"/> 172.16.102.11	192.168.55.3	TCP	ACCEPT	Any	↑ ↕ ↗ ✖	Source Port: 8237

Destination Port: 1134
Protocol Type: UDP
Action: REJECT
Apply To WLAN: Any

Used: 3, Available: 125
Fragment Reassembly: On Off

Figure10-9-2 ACL Configuration Window

Parameter	Specifications
Source IP	The source IP address.
Destination IP	The destination IP address.
Source Port	Source UDP or TCP port.
Destination Port	Destination UDP or TCP port.
Protocol Type	There are three options for IP Protocol, TCP, UDP or ICMP.
Action	ACCEPT or REJECT
Apply To WLAN	Indicate the range which the ACL rule takes effect for wireless connection, specific SSID or any SSID.

Table10-9-1 ACL Parameter Specification

11IoT

DAP with BLE function can be deployed in a specific position, and be used as a Bluetooth beacon, announcing Bluetooth signal in a regular time and also be used as a Bluetooth signal scanner, scanning the Bluetooth signal in a regular time and reporting to the required server.

BLE feature is disabled by default, you can set global Bluetooth configuration for all the DAPs in the list or select a specific DAP for private Bluetooth configuration, the private Bluetooth configuration takes precedence over global configuration. It includes three types of working mode:

- **Advertise Mode** - Enable the BLE advertising function for the Device. If enabled, the Device will broadcast BLE packets.
- **Scanner Mode** - Enable the Bluetooth beacon scanning function for the AP.
- **Advertise & Scanner Mode** - Enable Bluetooth beacon scanning and BLE advertising function

The IoT window was divided into two windows: Bluetooth configuration page and Detailed Information page, in Bluetooth configuration page all the DAPs supported Bluetooth will be shown in the list; in the Detailed Information page, the detailed configuration will show when single DAP selected.

11.1 Advertise mode

There are three advertising protocols which are:

- **iBeacon** - Apple iBeacon format
- **Edyuid** - Google Eddystone format. A unique static ID with a 10-byte Namespace component and a 6-byte Instance component.
- **Edyurl** - Google Eddystone format. A compressed URL that, once parsed and decompressed, is directly usable by the client.

Below are the general configurations in Advertise mode:

- **Broadcast Power** - The transmit power used to broadcast BLE packets.
(Range = - 20 - 10, Default = 4)
- **Broadcast Frequency** - The time circle during which the BLE packets will be broadcast, in milliseconds. (Range = 20 - 9,000,000, Default = 200)
- **Broadcast channel** - The transmit channel used to broadcast BLE packets.

11.1.1 iBeacon

UUID, Major and Minor value can be edited in the BG Configuration window. Shown in Figure11-1-1.

Major and Minor values are advertised actually based on the BLE MAC of the AP by default although they display 65535 by default.

The Major value is got by converting the seventh and eighth bits of BLE MAC to the decimal value, and the Minor value is got by converting to the decimal value from the last four bits of BLE MAC.

The image shows a 'BG Configuration' window with the following settings:

- Bluetooth Switch: on
- Working Mode: Advertise
- Transmit Power: 4 (0-19)dbm
- Transmit Frequency: 100 (20-10485)ms
- Transmit Channel: Channel 37 Channel 38 Channel 39
- Beacon Mode: iBeacon
- UUID: 01020304-1a2b-3c4d-5e6f-12
- Major: 65535 (0-65535)
- Minor: 65535 (0-65535)

Buttons: Cancel, Save

Figure11-1-1 Configure iBeacon mode

11.1.2 Edyuid

Namespace and Instance value can be edited in the BG Configuration window, Shown in Figure11-1-2.

- **Namespace** - 20 characters containing 0-9, a-f.
- **Instance ID** - 12 characters containing 0-9, a-f.

The image shows a 'BG Configuration' dialog box with a blue header and a close button (X) in the top right corner. The dialog contains the following settings:

- Bluetooth Switch: on
- Working Mode:
- Transmit Power: (0-19)dbm
- Transmit Frequency: (20-10485)ms
- Transmit Channel: Channel 37 Channel 38 Channel 39
- Beacon Mode:
- Namespace:
- Instance:

At the bottom of the dialog are two buttons: 'Cancel' (orange) and 'Save' (blue). A vertical scrollbar is visible on the right side of the dialog.

Figure11-1-2 Configure Edyuid mode

11.1.3 Edyurl

Plain URL which will be compressed can be edited in the BG Configuration window. Shown in Figure11-1-3.

The image shows a 'BG Configuration' dialog box with the following settings:

- Bluetooth Switch: on
- Working Mode: Advertise
- Transmit Power: 4 (0-19)dbm
- Transmit Frequency: 100 (20-10485)ms
- Transmit Channel: Channel 37 Channel 38 Channel 39
- Beacon Mode: Edyurl
- Plain url: https://github.com/

Buttons: Cancel, Save

Figure11-1-3 Configure Edyurl mode

11.2 Scanner mode

The engine server should be configured including below parameters:

- **Scan Filter** - enable/disable scan filter
- **Scan Type**
 - **Passive Scanning** - Passive Scanning
 - **Active Scanning** - Active Scanning
- **Scan Interval** - The Bluetooth scanning interval for AP, in milliseconds. (Range = 4 -10240, Default = 100)
- **Scanning Period** - Duration of each scan, in milliseconds. (Range = 4 - 10240)

Service Config:

- **Report Data Type** - Bluetooth Data

- **Server Address** – Server Host/Port that receive data from AP.
- **Report Topic** – The topic which send message to MQTT broker.
- **Report Broadcast Type:**
 - **iBeacon** - iBeacon is a protocol developed by Apple, it can be used to determine the device's physical location, track customers, or trigger a location-based action on the device.
 - **Edyuid** - Google Eddysone format. A unique static ID with a 10-byte Namespace component and a 6-byte Instance component.
 - **Edyurl** - Google Eddysone format. A compressed URL that, once parsed and decompressed, is directly usable by the client.
 - **S1** – A type of customize beacon format
- **Report Group** - Group ID of device.
- **Username** - Username to connect MQTT broker.
- **Login Key** - Secret key to connect MQTT broker.
- **Bluetooth Data Report Interval** - reporting interval of Bluetooth message.(Range 1~20).
- **Map Building ID** – Map Building ID.

BG Configuration
✕

Bluetooth Switch: on

Working Mode:

Scan Filter Mode: Filter No Filter

Scan Type: Active Passive

Scanning Interval: (4-10240)ms

Scanning Period: (4-10240)ms

Scan Allowlist: + ✕

Service Config

Report Data Type: Bluetooth Data

Server Address:

Report Topic:

Report Broadcast Type:

Report Group:

Username:

Login Key:

Bluetooth Data Report Interval: (1-20)s

Map Building ID:

Figure11-2-1 Scanner mode

11.3 Advertise & Scanner mode

Both Bluetooth beacon scanning and BLE advertising functions are enabled in this mode, please refer to Chapter [11.1 Advertise mode](#) and [11.2 Scanner mode](#) for details.

12 Support tools

12.1 Tools

Tools are several commands integrated in DAP for diagnosing and troubleshooting. The commands are applied to a single DAP in the cluster. You can select an AP from the cluster and execute a command to discover the running information of the DAP, such as system health, wireless health and reboot reason, illustrated in Figure12-1-1 and Figure12-1-2.

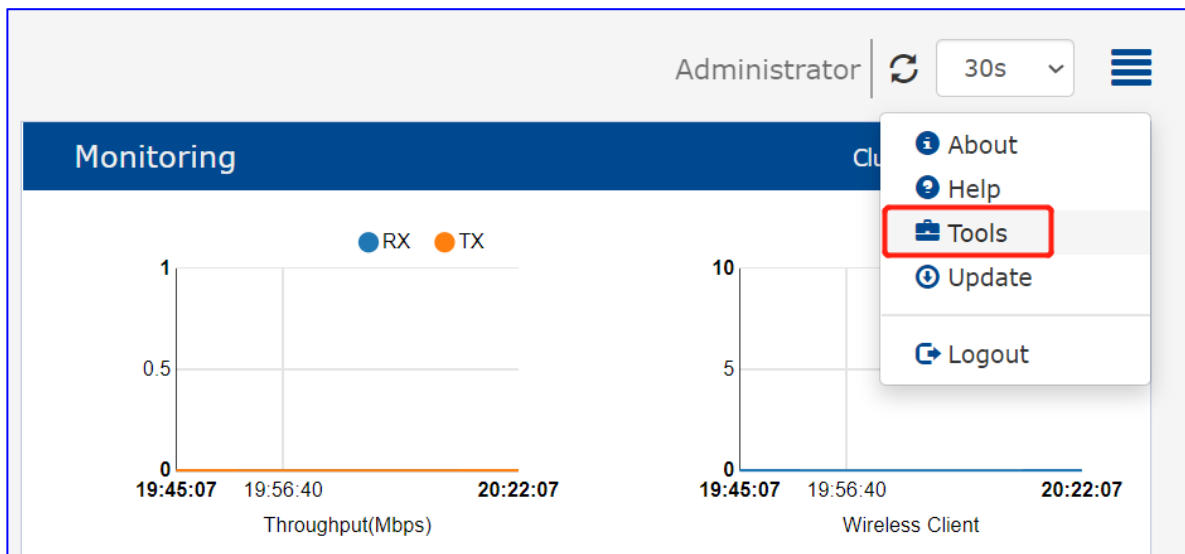


Figure12-1-1 Entry of Tools

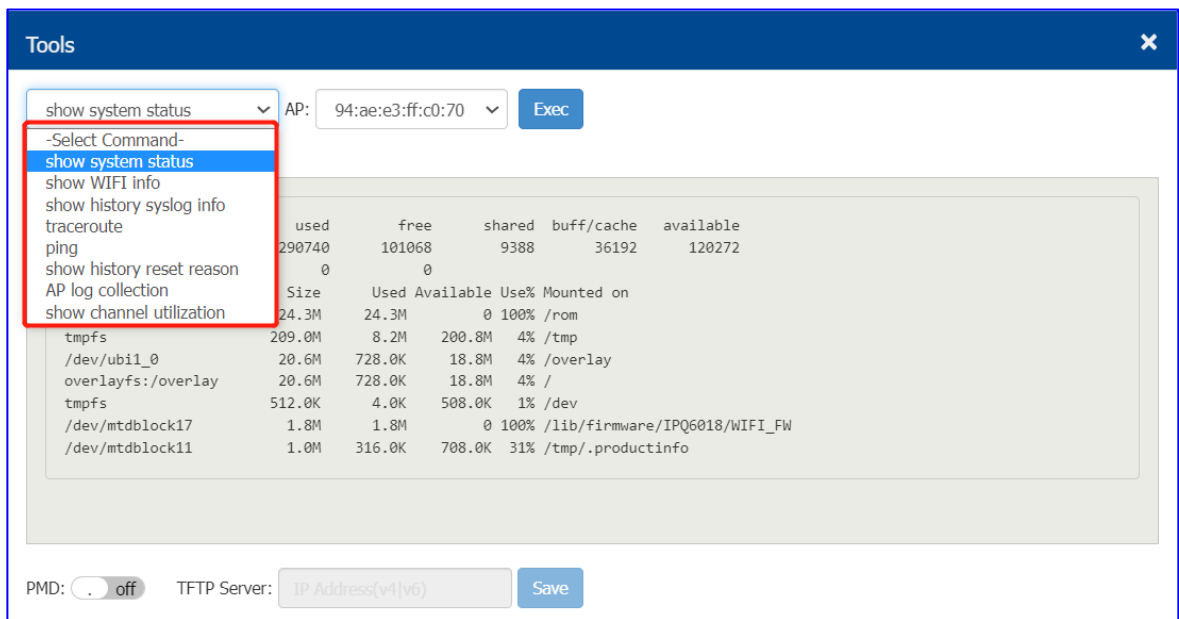


Figure12-1-2 Troubleshooting Tools

- **show system status:** Show system CPU and memory usage information of specified DAP, illustrated in Figure12-1-3.

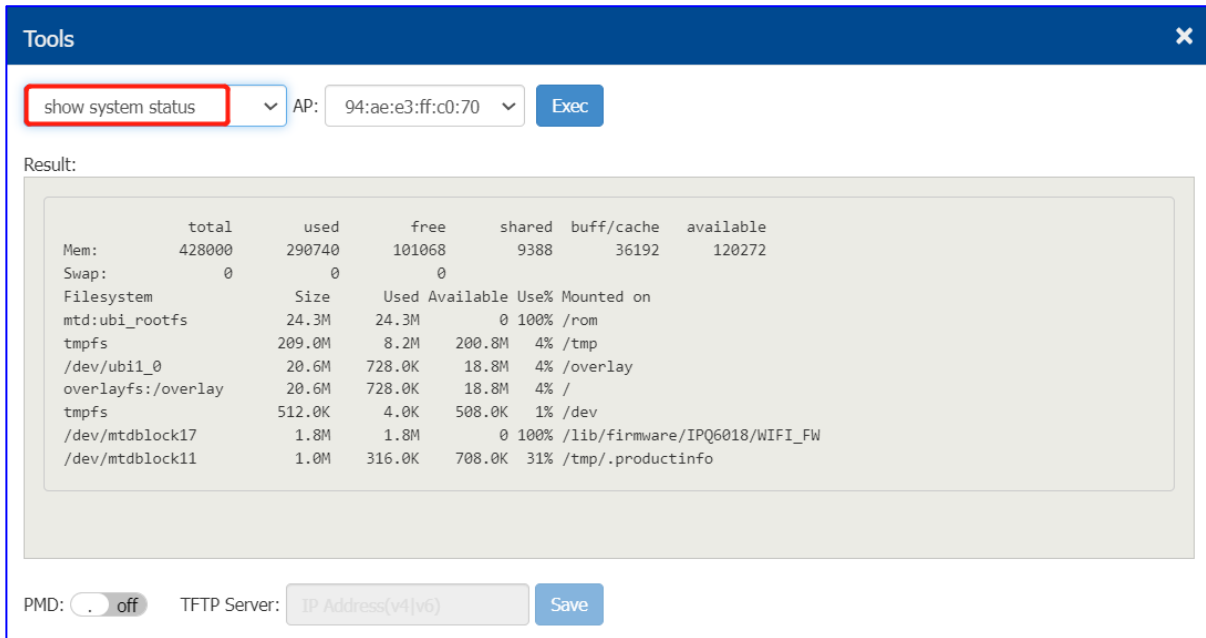


Figure12-1-3 show system status

- **show WIFI info:** Show wireless interface information of specified DAP(illustrated in Figure12-1-4) which includes:
 - Output information of commands 'iwconfig' and 'wlanconfig', for example the DAP working channel; transmit power, BSSID, etc.
 - PHY information of client, for example the MAC address and RSSI, etc.

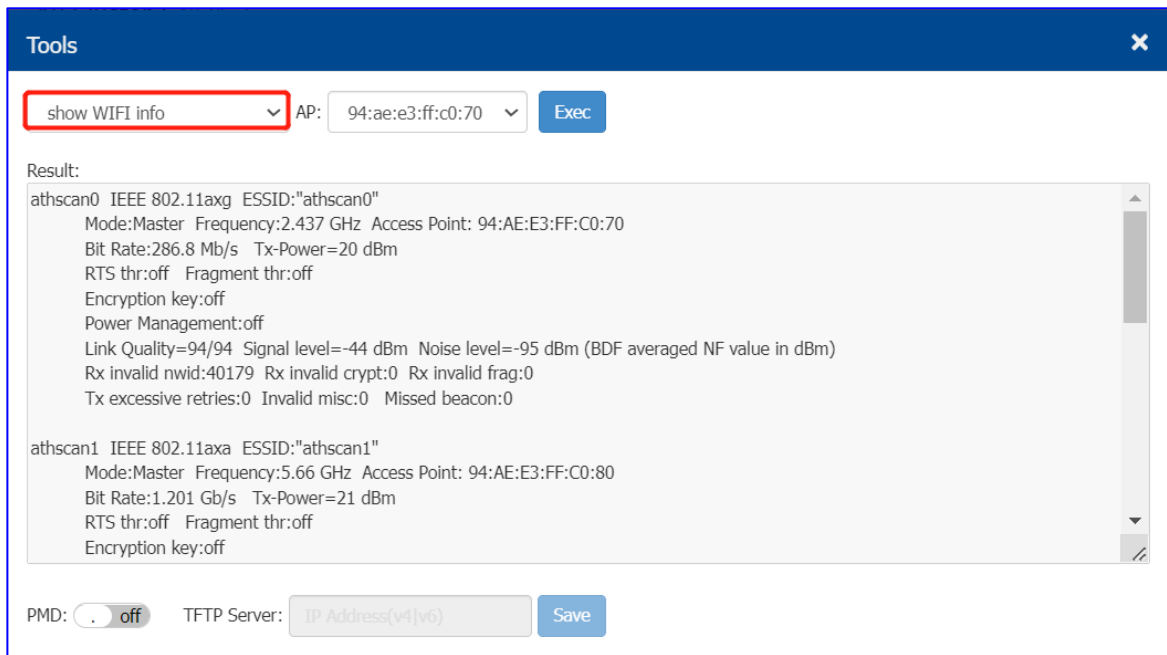


Figure12-1-4 show WIFI info

- **show history syslog info:** Show historic Syslog messages generated in last time system running (Before this time system up) of specified DAP, illustrated in Figure12-1-5.

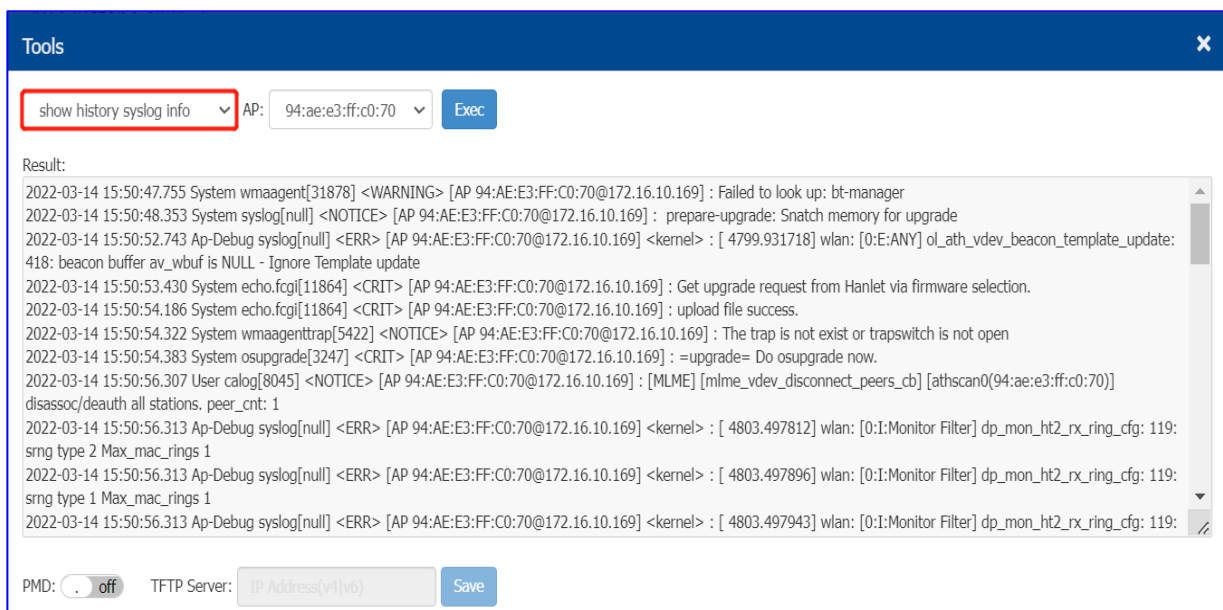


Figure12-1-5 show history syslog info

- **traceroute:** Traceroute from specified DAP to another host in the network, illustrated in Figure12-1-6.

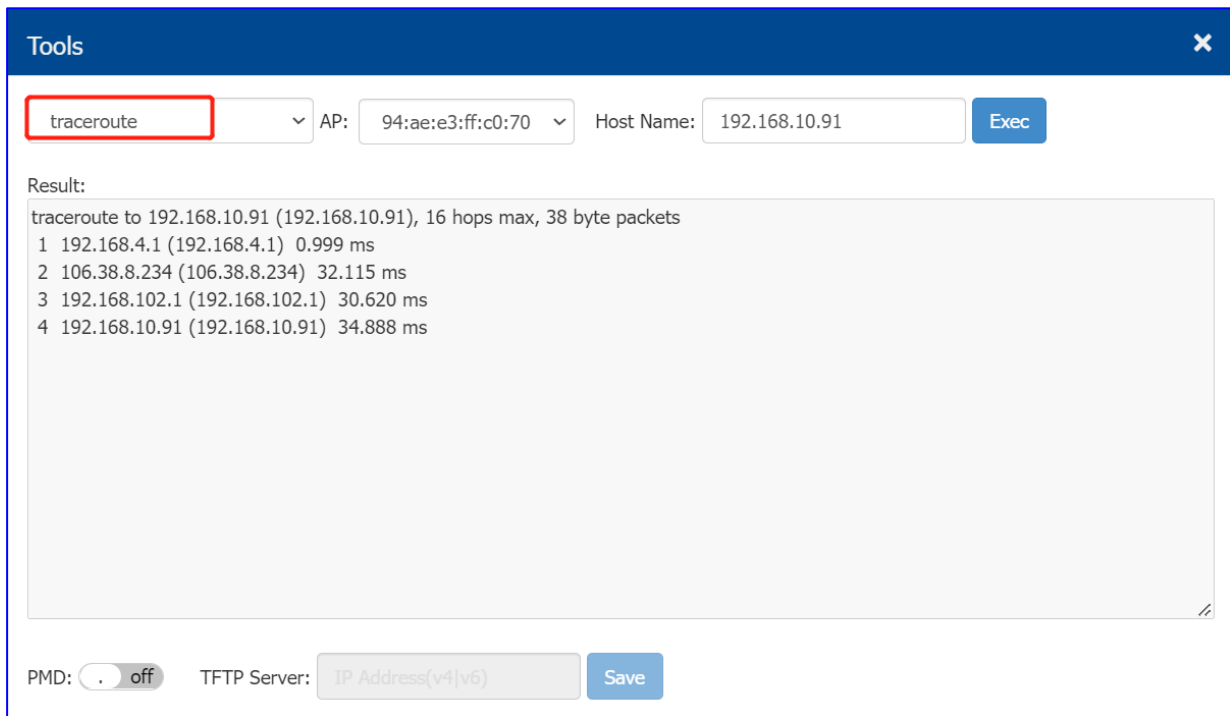


Figure12-1-6 traceroute

- **ping**: Ping operation from specified DAP to another host in the network, illustrated in Figure12-1-7

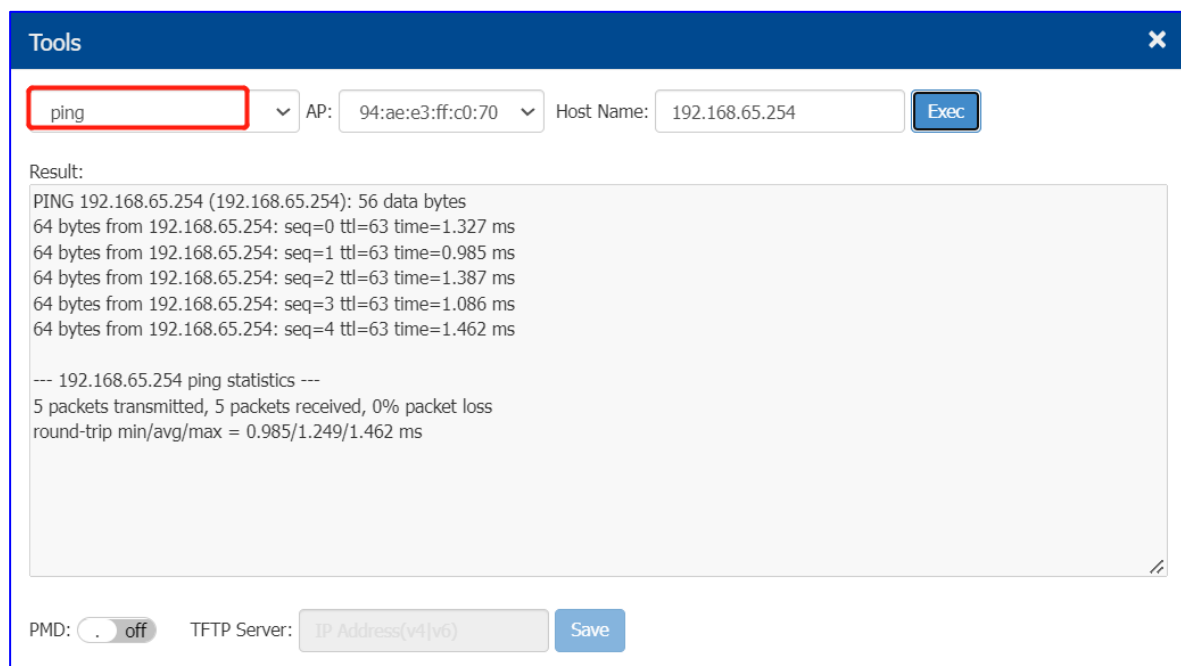


Figure12-1-7 ping testing on specific DAP

- **show history reset reason:** Show latest 10 reboot records of specified DAP which includes reboot time, reboot reason; it's the same output for command `reset_record get` under CLI mode, illustrated in Figure12-1-8.

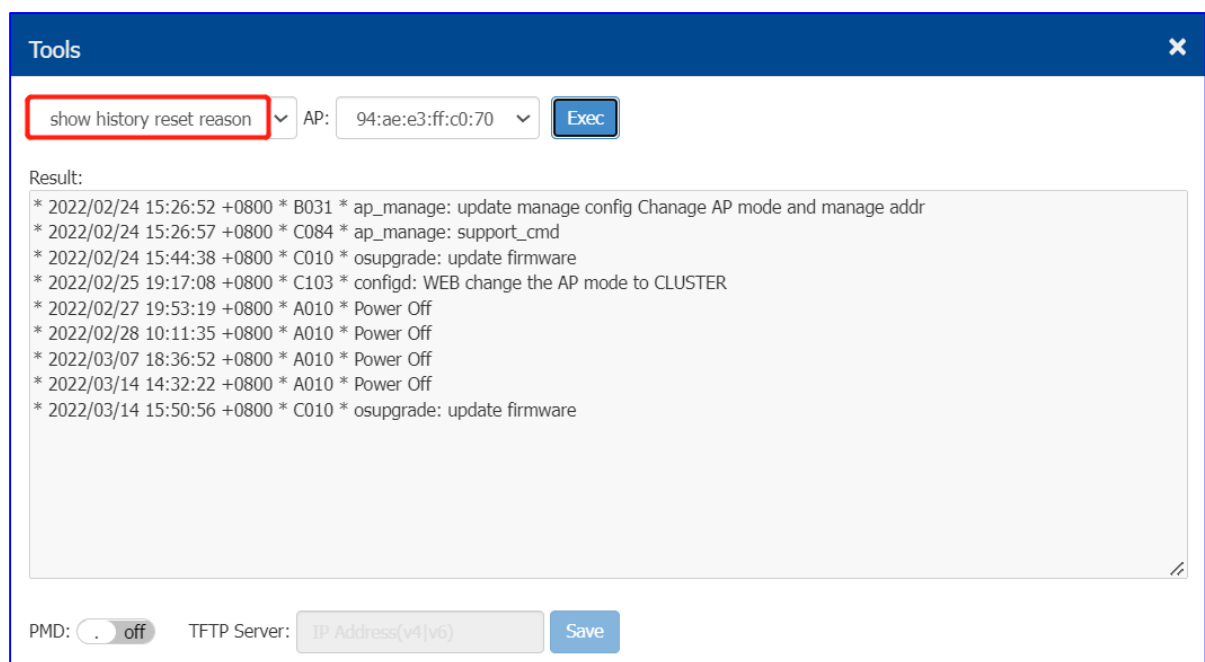


Figure12-1-8 show history reset reason

- **AP log collection:** Collect AP log files for troubleshooting and download by TFTP/HTTP, illustrated in Figure12-1-9.

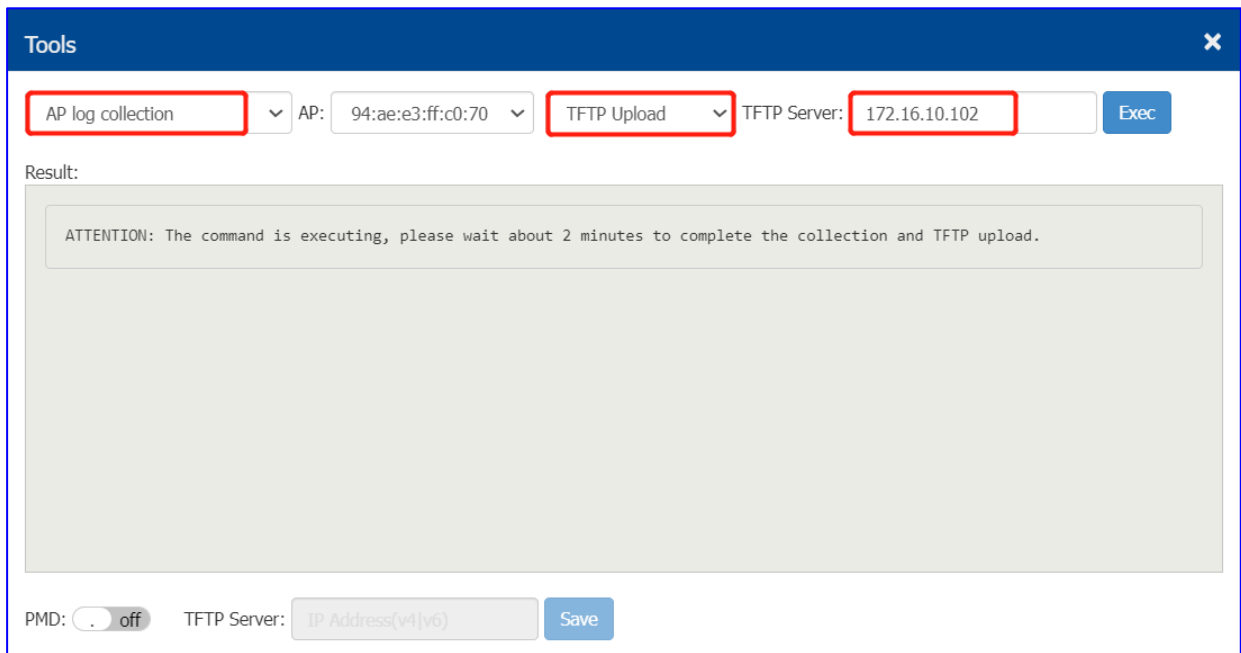


Figure12-1-9 AP log collection by TFTP

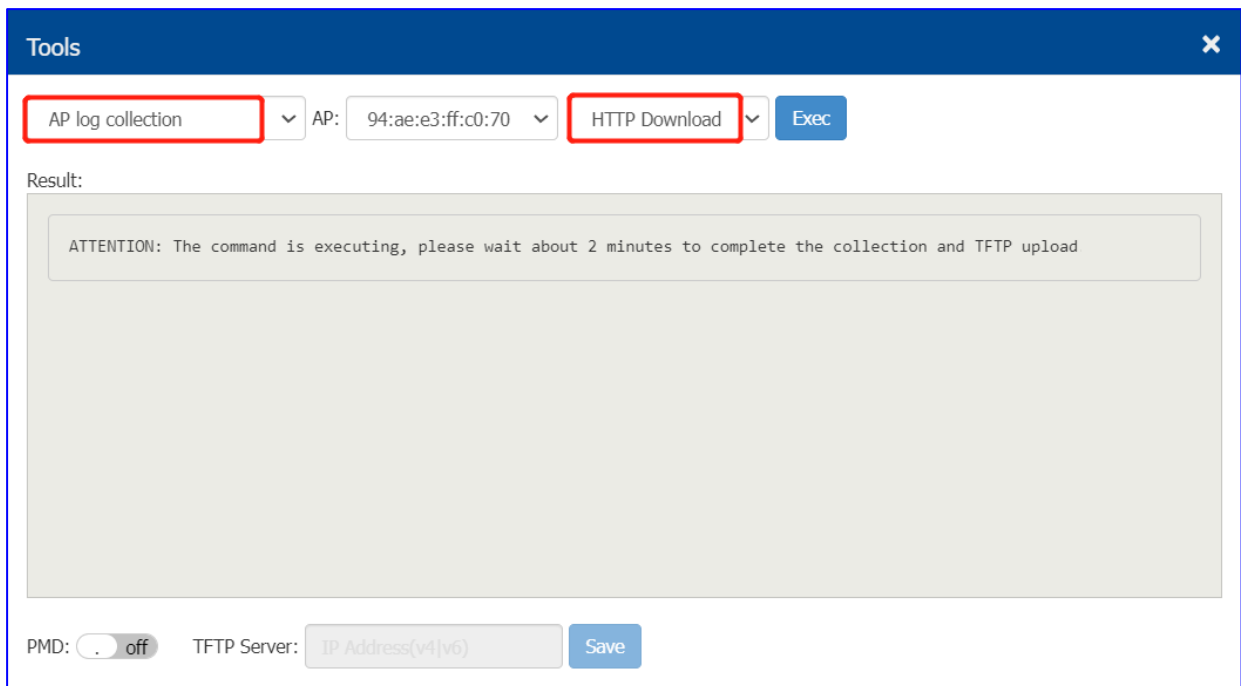


Figure12-1-9 AP log collection by HTTP

- **show channel utilization**: Display current 2.4G/5G band channel utilization detected by the AP, illustrated in Figure12-1-10.

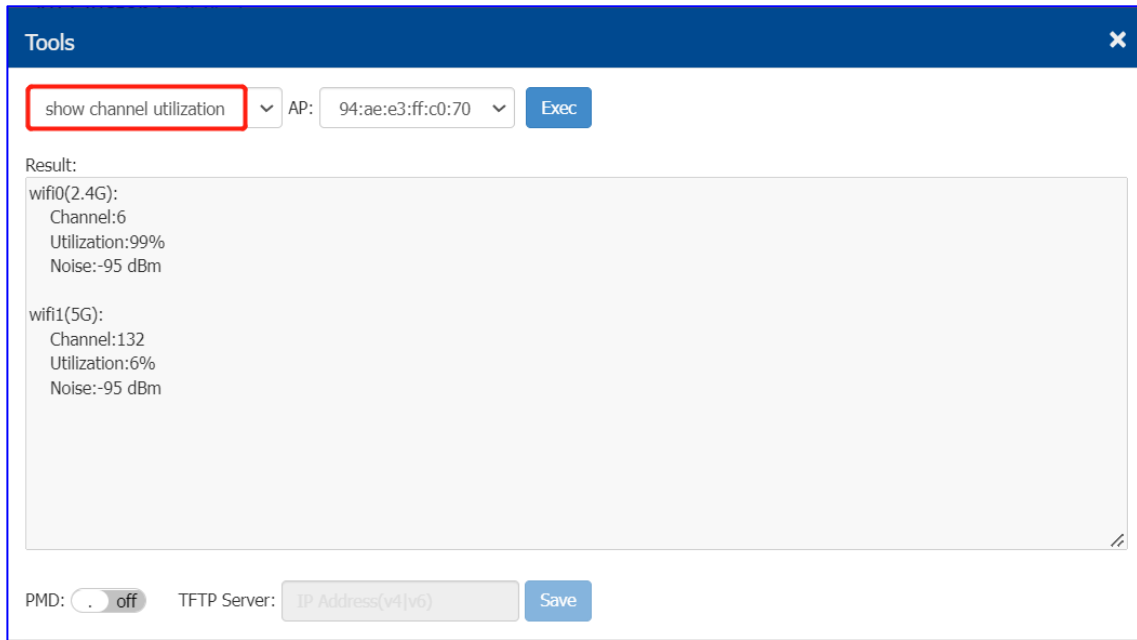


Figure12-1-10 show channel utilization

12.2 PMD

Post Mortem Dump (PMD) is a troubleshooting method helping to identify root cause of a core dump and exception pointers after a fatal crash. If PMD is enabled and configured, the DAP will send PMD files to a specific TFTP server immediately when there is key process crashing on the DAP. By default, PMD files sending to external TFTP server is disabled, shown in Figure12-2-1.

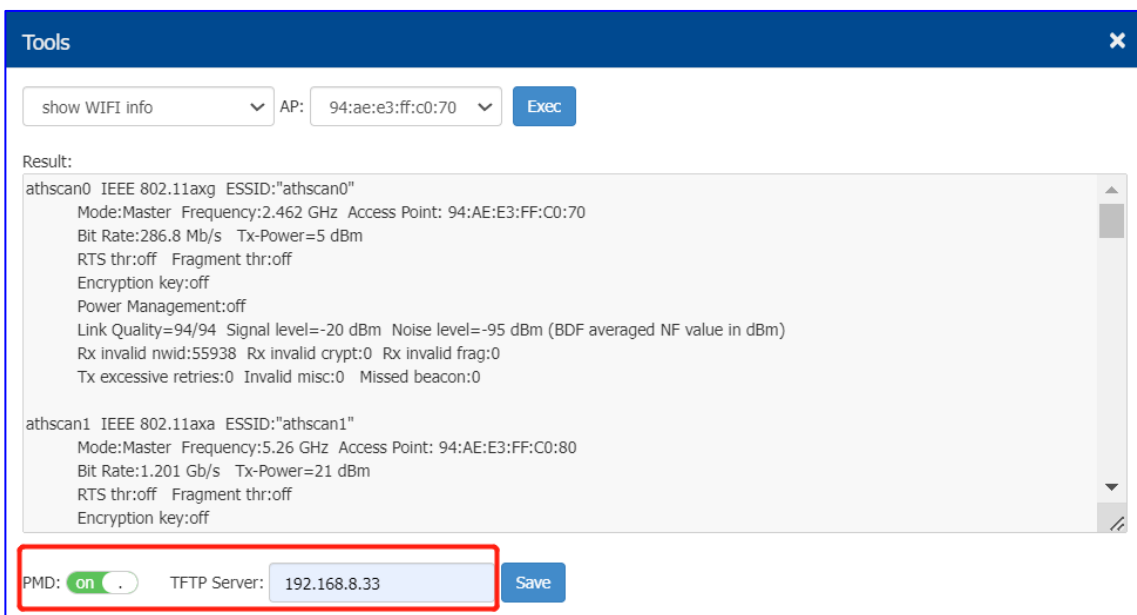


Figure12-2-1 PMD Configuration

13 Deployment large scale of DAPs

If you have more DAPs than a cluster specification (255), you can setup more than one AP cluster to provide Wi-Fi service.

There are three methods to setup more than one AP cluster in the network:

Method one: Divide the APs into different subnets by changing the default VLAN of the switch ports to which the DAPs connect; for example: subnet-A uses default VLAN 100 while subnet-B uses default VLAN 200 and subnet-C uses default VLAN 300.

Method two: Setup up different Cluster IDs for each AP Cluster respectively. Perform the following steps:

- Select the DAPs which you want to work in Cluster-A, plug in to the switch to build the first AP Cluster;
- Browse to the Cluster-A management interface and change its Cluster ID. (For example: change the Cluster ID from 100 to 101), see in General Window.
- Repeat the above process to setup Cluster B/C/etc.

Method three: Deploy DAP with DAC and scale up to 4000 AP in one network.

14 Configure AP if DHCP Server unreachable

Case one: If the DAPs reboot and the DHCP server are not accessible, all the DAPs return to the system default IP which is 192.168.1.254. This means there is duplicate IPs in the broadcast domain. All the APs work separately as the PVM and broadcast the same WLANs. In this case, it is highly recommended to fix the DHCP server in the network and let the wireless service recover.

Case two: If you want to configure a single DAP without a DHCP server, please perform the following steps:

- Connect the DAP (default IP address is 192.168.1.254) to your configuring terminal (laptop for example) directly with an Ethernet cable.
- Specify a static IP address and a DNS server for the network card of your laptop, for example: IP Address for 192.168.1.100; Subnet Mask for 255.255.255.0; Default Gateway for 192.168.1.254 and DNS server for 192.168.1.254.
- Browse <http://192.168.1.254:8080> to configure the DAP.

15 Glossary

ACL	Access Control List
ACS	Automatic Channel Selection
APC	Automatic Power Control
ARP	Address Resolution Protocol
BLE	Bluetooth Low Energy
BSSID	Basic Service Set Identifier
CLI	Command-Line Interface
DAC	Dragonfly Access Controller: DAC is a simple, easy to deploy turnkey WLAN solution consisting of one or more DAPs
BWO	Belden Wireless Orchestration: BWO is a simple, easy to deploy turnkey WLAN solution consisting of one or more DAPs
DAP	Dragonfly Access Point: Enhanced WLAN technology with RF radio dynamic adjustment, distributed control Wi-Fi architecture, secure network admission control with unified access
DCM	Dynamic Client Management
DNS	Domain Name System
DRM	Dynamic Radio Management: automatically manage DAP working channel and transmitting power
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Services Code Point
ESSID	Extended Service Set Identifier

FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
IDS	Intrusion Detection System
IG	Installation Guide
IGMP	Internet Group Management Protocol
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MIMO	Multiple-Input Multiple-Output
MTU	Maximum Transmission Unit
MU-MIMO	Multi-User Multiple-Input Multiple-Out
NAT	Network Address Translation
NTP	Network Time Protocol
OKC	Opportunistic Key Caching
PMD	Post Mortem Dump
PMF	Protected Management Frames
POE	Power over Ethernet
PPPOE	Point-to-Point Protocol over Ethernet
PVM	Primary Virtual Manager: the virtual manager selected from DAPs according to the defined priority will be responsible for an internal portal server, AP and client management and monitoring
QoS	Quality of Service
QSG	Quick Start Guide
RF	Radio Frequency

RSSI	Received Signal Strength Indicator
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
SVM	Secondary Virtual Manager: the second highest priority in the cluster. When the PVM fails to respond due to an unexpected error or issues, the SVM will automatically upgrade to act as the PVM
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
WBM	Web Based Management
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multimedia (WMM)
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
UUID	Universally Unique Identifier

