HIRSCHMANN IT

A BELDEN BRAND

User Manual

Configuration

Dragonfly Access Point

DAP847-XXA

Technical support
https://hirschmann-it-support.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 to anyone.

© 2023-2024 Belden Singapore Pte Ltd

Manual 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 manual.

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

You may get the latest version of this manual on the Internet at: https://catalog.belden.com.

Revision History

Version	Date	Description
1.0	2023.12	First draft, based on Web GUI 4.1.6.21
1.2	2024.08	Based on Web GUI version 4.1.6.43 Add the following parameters to section 6.3 WLAN Parameters Introduction: DTIM Interval, RTS/CTS, RTS Threshold. Update section 9.1.3 Configure DAP847-XXA antenna.

Contents

Revision History **3**
Contents **4**
Safety instructions **8**
About this manual **9**
About DAP **10**
Key **11**
1 Introduction **12**
1.1 Overview 12
2 DAP847-XXA work mode **13**
2.1 Cluster mode 13
2.1.1 Selection of PVM and SVM in Cluster 13
2.1.2 DAP847-XXA unpacking settings 14
2.2 DAC mode 15
3 Cluster deployment example **16**
3.1 Topology 16
3.2 Scenario description 17
3.2.1 DAPs SSIDs in Cluster 17
3.2.2 Deployed Servers 18
4 Setup wizard **19**
4.1 Access the DAP cluster by web browser 19
4.1.1 Prerequisites 19
4.1.2 DAP847-XXA IP address 20
4.1.3 Access DAP847-XXA web GUI in initialization state 21
4.2 Using the DAP847-XXA setup wizard 24
4.2.1 DAP Initialization 24
5 DAP cluster web GUI **28**
5.1 Dashboard overview 29
5.2 WLAN 30
5.3 AP 32
5.4 Clients 35
5.5 Monitoring 39
5.5.1 Cluster-based Monitoring 40
5.5.2 WLAN-based Monitoring 41
5.5.3 AP-based Monitoring 42

5.5.4 Clients-based Monitoring 43
5.6 System 44
5.7 Wireless 45
5.8 Access 46
5.9 More 47
6 WLAN 49
6.1 Create a WLAN in two ways 50
6.2 WLAN security types 52
6.2.1 Security type Open 52
6.2.2 Security type Portal 52
6.2.3 Security type Personal 53
6.2.4 Security type Enterprise 55
6.3 WLAN parameter description 57
6.4 Modify WLAN configuration 75
6.5 Delete a WLAN 76
6.6 WMM configuration 77
7 DAP847-XXA Management 79
7.1 Check detailed information 80
7.2 Modify the DAP847-XXA name and location 81
7.3 Add a new DAP847-XXA to a cluster 82
7.4 Remove a DAP847-XXA from a cluster 84
7.5 Allow a DAP847-XXA to join a cluster 86
7.6 Replace an DAP847-XXA in a cluster 87
7.7 Modify DAP847-XXA IP address 88
7.8 Convert DAP847-XXA to DAC mode 89
7.9 Check DAP847-XXA current configuration 91
7.10 Reboot the DAP847-XXA 92
7.11 Clear all configuration 94
7.12 Backup and restore configuration 95
7.13 Upgrade the DAP847-XXA firmware 96
7.13.1 Upgrade all DAP847-XXA in cluster 96
7.13.2 Upgrade the single DAP847-XXA 99
7.14 Configure the LED 100
7.15 DAP847-XXA advanced configuration 101
7.15.1 AP advanced configuration window overview 102
7.15.2 AP status monitoring and working mode configuration 103
7.15.3 WLAN information 106
7.15.4 Clients information 106
7.15.5 RF information 106

7.15.6 System management 107
7.15.7 DAP847-XXA Interface configuration 107
7.15.8 DAP847-XXA network 109
7.15.9 Mesh configuration 111
7.15.10 Static neighbor AP configuration 113
7.15.11 RF environment 113
7.15.12 Wireless capture 115
7.16 Configure DAP847-XXA network service 117
7.16.1 Configure a DHCP server 117
7.16.2 Configure a DNS server 119
7.16.3 NAT configuration 119
8 System management 122
8.1 Cluster info management 123
8.2 Accounts management 125
8.2.1 Manage web GUI accounts 125
8.2.2 Manage CLI accounts 126
8.3 Certificate management 127
8.4 Services management 128
8.5 System time configuration 129
8.6 Syslog configuration 131
8.7 SNMP configuration 133
8.7.1 Configure SNMPv2c 134
8.7.2 Configure SNMPv3 136
9 Wireless management 138
9.1 RF configuration 139
9.1.1 Modify DAP847-XXA transmit power and channel 141
9.1.2 Configure channel width 143
9.1.3 Configure DAP847-XXA Antennas 144
9.1.4 Turn on/off DAP847-XXA radio 145
9.2 wIDS/wIPS 147
9.3 Performance Optimization 153
10 Access 157
10.1 Authentication 158
10.2 Login captive portal 161
10.3 Account and access code management 164
10.4 Customize portal page 167
10.5 Client blocklist for wireless access 168
10.6 Client allowlist for captive portal 169

10.7 Walled garden 170
10.8 Multicast control 171
10.9 ACL 172
11 IoT 174
12 Tools 175
12.1 Tools 175
12.2 PMD 181
13 Deployment large scale of DAP847-XXA devices 182
14 Configure the AP without DHCP server 183
15 Glossary 184
A Further support 186

Safety instructions

Security channel

Hirschmann IT devices support multiple management methods, including SSH, HTTP, and HTTPS. All un-encrypted management protocols are not recommended. Hirschmann IT recommends using SSH and HTTPS to operate the devices to help ensure management traffic is encrypted.

Security storage

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

About this manual

This user manual contains the reference information you need to operate the device for the first time. It will guide you step by step from the startup operation to complete the configuration of each function.

About DAP

The DAP847-XXA series is a next-generation enterprise wireless access point specifically designed for industrial wireless coverage scenarios. The DAP847-XXA series supports enhanced WLAN technologies, including RF Radio Dynamic Adjustments (RDA), distributed control Wi-Fi architecture, and network admission control through unified access. With simple configuration and maintenance operations, it provides secure and scalable wireless solutions for industrial applications, making it an ideal choice for various industrial scenarios.

DAP847-XXA can provide enterprise-grade Wi-Fi solutions for high-density environments such as offices, hospitals, schools, retail stores, and warehouses, enabling high-speed and high-performance network services and applications.

Furthermore, DAP847-XXA also supports establishing wireless connections with DAP847-XXC series wireless access clients, serving as a channel for vehicle-to-ground data communication in railway deployment scenarios, enabling real-time transmission of railway control signals and related data.

Key

The symbols used in this manual have the following meanings:

▶	Listing
☐	Work step
■	Subheading
Note:	A note emphasizes a significant fact or draws your attention to a dependency.

1 Introduction

1.1 Overview

The manual describes the features of the DAP847-XXA in **“CLUSTER”** mode. It provides instructions and examples for the DAP847-XXA configurations. It is designed for network administrators who configure and maintain the Wi-Fi network. It assumes that the reader is familiar with Layer 2 and Layer 3 networks, basic IEEE 802.11 protocols, and related technologies.

The manual covers an introduction to the DAP847-XXA and configuration examples. The examples describe the general steps to set up a Wi-Fi network based on several typical deployment scenarios. It is useful for readers who are new to the DAP847-XXA configurations or familiar with the software but want to know more about functions.

2 DAP847-XXA work mode

2.1 Cluster mode

DAP847-XXA can realize self-management functions through a distributed autonomous network mode. By default, it runs in **“Cluster mode”**, **which** provides simplified plug-and-play deployment. The cluster is an autonomous system that consists of DAP847-XXA devices and a virtual manager. The DAP847-XXA devices are capable of automatic discovery, automatic forming of a network, and self-management.

2.1.1 Selection of PVM and SVM in Cluster

The DAP847-XXA devices configured with the same cluster ID can form a cluster. Meanwhile, DAP847-XXA can also form a cluster with DAP6XX series devices. The cluster selects the Primary Virtual Manager (PVM) and the Secondary Virtual Manager (SVM) by the AP model and the MAC address.

The selection rules for the PVM or SVM selection are as follows:

- Based on the model of the DAP, the cluster will select the device with the highest priority as the PVM. Generally, the selection priority of the PVM or the SVM: DAP640/DAP645/DAP646/DAP647/DAP847-XXA > DAP620.
- Among the DAPs with the same priority, the DAP with the highest MAC address will be selected as the PVM and the one with the second-highest MAC address will be selected as the SVM.
- If a higher-priority DAP joins a DAP cluster, it will take over the PVM role. For example, a DAP847 will become the PVM after it joins a DAP620 cluster, and the previous PVM will be changed to the SVM or a member in the DAP cluster.
- When the PVM is unable to run due to an unexpected error or detected issues (for example, a network outage or the PVM losing power due to an unexpected condition), the SVM automatically upgrades to be the PVM. This enables redundancy at the management level without interruption or service disturbance to DAP847-XXA devices or any wireless users.

One DAP847-XXA cluster supports up to 255 DAP847-XXA devices. The cluster architecture ensures the DAP847-XXA with simplified and quick

deployment. Once you have configured the first DAP847-XXA using the configuration wizard, the remaining DAP847-XXA devices with the same **“Cluster ID”** in the same layer 2 network will automatically join the cluster and obtain configuration information from the PVM. This ensures that the whole network starts working within a few minutes. By default, the **“Cluster ID”** is 100.

2.1.2 DAP847-XXA unpacking settings

To set up the DAP847-XXA out of the box:

- ☐ Connect the DAP847-XXA to the network.
- ☐ Power it by a Power over Ethernet (PoE) or a power adapter.
- ☐ Ensure that the DAP847-XXA can obtain an IP address from the network.

When the LED on the DAP847-XXA is in a **“Green Blinking”** state, it can be detected, and then the user can connect to an SSID named **“mywifi-xx:xx”** (xx:xx is the last 2 characters of the DAP847-XXA MAC address).

After associating with the WLAN SSID, you can access the DAP847-XXA web-based management window by visiting the following default URLs:

- ► http://find.dap.com:8080
- ► https://find.dap.com

After you log in with the default account (username is “**Administrator**” and the password is “**admin**”), you can set up the DAP847-XXA by the **“Setup Wizard”**.

2.2 DAC mode

When the DAP847-XXA works in DAC mode, all DAP847-XXA devices can be centrally managed by a management platform to easily deploy large networks. It supports Layer 3 networking, so you can deploy a single site or across multiple sites with separated locations as long as it can be routable to the DAC.

For detailed information, refer to the DAC User Manual.

3 Cluster deployment example

This chapter mainly describes the typical wireless network topology in Cluster mode, including wireless networks and wired networks. The network components in the scenario include a DAP847-XXA, a switch, a router, and related application servers.

3.1 Topology

Figure 1 is the brief topology for a typical cluster scenario for your reference. No DAC management platform is deployed in this scenario. All the DAP847-XXA devices work in **"Cluster"** mode to realize the self-management function.

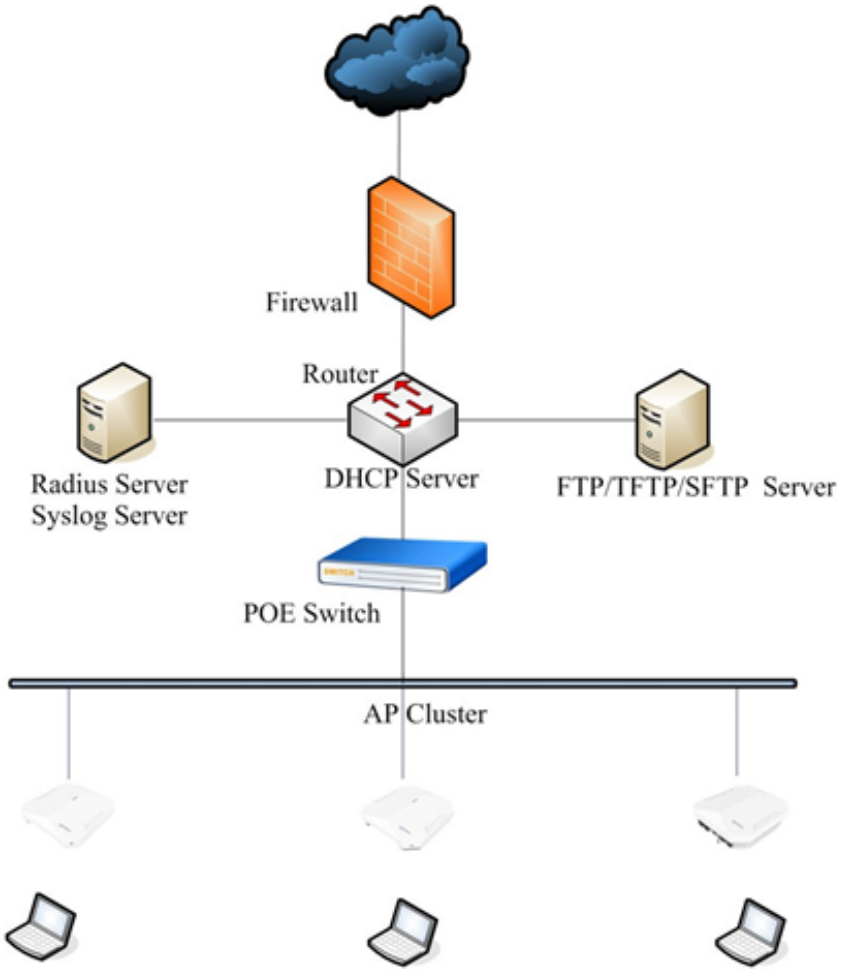


Figure 1: Topology

3.2 Scenario description

The topology in Figure 1 works as follows:

- There are 3 DAP847-XXA devices in a cluster. The 3 DAP847-XXA devices connect to a standard PoE switch that supports the IEEE 802.3at standard, and all the DAP847-XXA devices belong to the same management VLAN.
- The PoE switch is uplink connected to the core router, which provides the Dynamic Host Configuration Protocol (DHCP) service to the DAP847-XXA devices, wireless client devices and configuration terminals.
- The PVM in the cluster is responsible for managing and monitoring DAP847-XXA, synchronization of configuration, and synchronization of client information. Meanwhile, the PVM is also a built-in portal server in Portal scenarios.

Only indoor operation is allowed when used in the band 5150 … 5250 MHz, including installations inside road vehicles, trains, and aircraft. Outdoor operation is limited. If used outdoors, DAP847-XXA cannot be attached to a fixed installation or to the external body of road vehicles, a fixed infrastructure, or a fixed outdoor antenna. The use by unmanned aircraft systems (UAS) is limited to within the 5170 … 5250 MHz band.

Only indoor operation is allowed when used in the band 5250 … 5350 MHz, such as inside buildings. Installations in road vehicles, trains and aircraft are not permitted. Outdoor use is not permitted.

3.2.1 DAPs SSIDs in Cluster

The 3 DAPs in the cluster are configured with the following 3 SSIDs:

- **My-wifi-test**

  The SSID **“My-wifi-test”** is designed for a PSK SSID, which is mainly used in scenarios that require simple and fast secure connections, such as home networks, small office networks, etc. It can provide basic security protection without complex configuration and management.

- **My-wifi-portal**

  The SSID **“My-wifi-portal”** is designed for guests who need portal authentication. It is usually used in public places such as hotels, airports, shopping malls, etc. Guests can access the network by connecting to the

portal SSID, accessing a dedicated portal page, and then entering an access code or credentials. Portal WLAN can also be used within an enterprise to provide secure Internet access for temporarily visiting customers, partners, or suppliers.

- **My-wifi-1x**

  This WLAN uses the IEEE 802.1x authentication methods. The company staff and security use the SSID **"My-wifi-1x"**. The username and password are stored inan internal RADIUS server. Users need to enter the username and password or certificates to connect to the WLAN. This authentication method has higher security than the previous two SSIDs.

3.2.2 Deployed Servers

The related servers deployed in the scenario in Figure 1:

- **RADIUS Server**: It is used for IEEE 802.1x authentication for an Enterprise SSID. it could be a windows server or other types of RADIUS server.
- **Syslog Server**: It is used for receiving syslog generated by DAP847-XXA devices, see "Syslog configuration" on page 131.
- **TFTP Server**: It is mainly used for DAP847-XXA snapshot log collection, software upgrade, and Post Mortem Dump (PMD) file collection.
- **SFTP Server**: It is used for software upgrade of DAP847-XXA and recording of client connection information (Client Behavior Tracking).

4 Setup wizard

The predefined SSID connects to the initial wizard window by accessing the URL http://find.dap.com:8080/ or https://find.dap.com/. This chapter mainly introduces how to access the DAP cluster and complete the basic configuration according to the wizard when using DAP847-XXA for the first time.

4.1 Access the DAP cluster by web browser

Each DAP847-XXA supports logging in to the DAP847-XXA Cluster Manager with 3 different accounts. The GUI can be accessed through a web browser on your PC.

The GUI includes a configuration wizard that guides you through changing the administrator password and completing basic WLAN configuration.

In addition to the wizard, the GUI provides a dashboard monitoring function. This Dashboard is a central panel that graphically displays key metrics, network performance data, and wireless client information of DAP847-XXA. It allows users to track, analyze, and monitor the operational status of DAP847-XXA in an intuitive manner, thereby gaining a better understanding of its key metrics.

To identify and diagnose WLAN issues in the GUI dashboard, see “Dashboard overview” on page 29.

4.1.1 Prerequisites

Before setting up DAP847-XXA, the following prerequisites must be met:

- The DAP847-XXA devices are connected to the switch and powered up.
- The DAP847-XXA devices are in the same subnet and can be reachable (The switch has not enabled the port isolation function.).
- A DHCP server is accessible in the network. The DAP847-XXA cluster uses an external DHCP server for IP address management of the APs and the wireless clients.
- A DNS server is available in the network, which helps to parse the web URLs to access the DAP847-XXA devices.

Hirschmann IT recommends that your configuring terminal is compatible with the following Operating System (OS) and browser.

Recommended OS	Recommended browser
Windows 8	Google Chrome 115 and higher.
Windows 10 Windows 11	Mozilla Firefox 113 and higher.
MAC OS X 10.10	Microsoft Edge 115 and higher.
MAC OS X 10.11	

Table 1: Recommended OS and browser

Note: The process of connecting to a single DAP847-XXA through the web browser is the same as connecting to a DAP847-XXA cluster.

Hirschmann IT recommends connecting only 1 DAP847-XXA to the network at a time and completing the configuration, then connecting the other DAP847-XXA devices one by one to synchronize the configurations.

4.1.2 DAP847-XXA IP address

DAP847-XXA supports IP address management in the following ways:

- By default, if no DHCP server is available in the network, the DAP847-XXA uses the IP address 192.168.1.254.
- DAP847-XXA supports manual configuration of a static IP address.
- DAP847-XXA obtains an IP address from a DHCP server.

  If there is a DHCP server in the network, DAP847-XXA supports obtaining an IP address dynamically from the DHCP server. You can check the assigned address in the DHCP server, or query through the ARP table entries of the uplink switch, or use the "`ipconfig br-wan`" command via a serial connection to view the IP address of DAP847-XXA, see Figure 2.

```
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:~$
```

Figure 2 Check IP address by CLI

4.1.3 Access DAP847-XXA web GUI in initialization state

In the default factory settings, the DAP847-XXA has been pre-defined as a 2.4 GHz brand SSID to provide wireless access and management through the web page. Follow the configuration wizard to complete the initial configuration:

- ☐ Connect to a 2.4 GHz brand SSID named **"mywifi-xx:xx"**, see Figure 3.

  Note: "xx:xx" is the last 2 characters of the PVM MAC address.

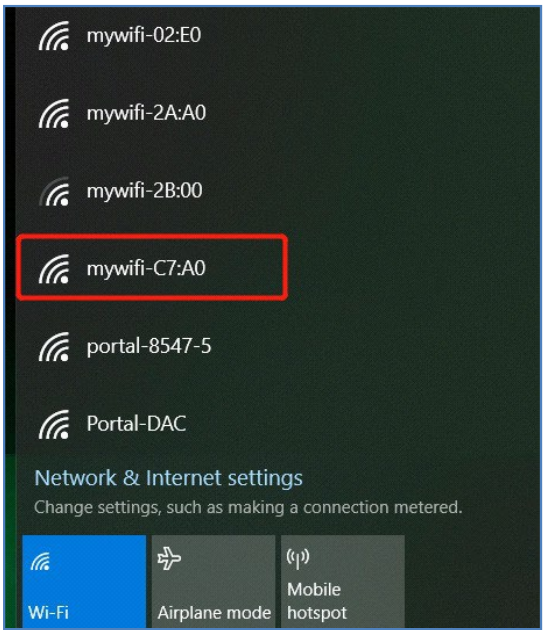


Figure 3: Connect to the default SSID

- ☐ Log in to the DAP847-XXA Cluster Manager through http or https. The factory default login password is **"admin"**.
  - ► Login with http by http://find.dap.com:8080/. The IP address of DAP847-XXA IP is 72.16.102.109, see Figure 4.

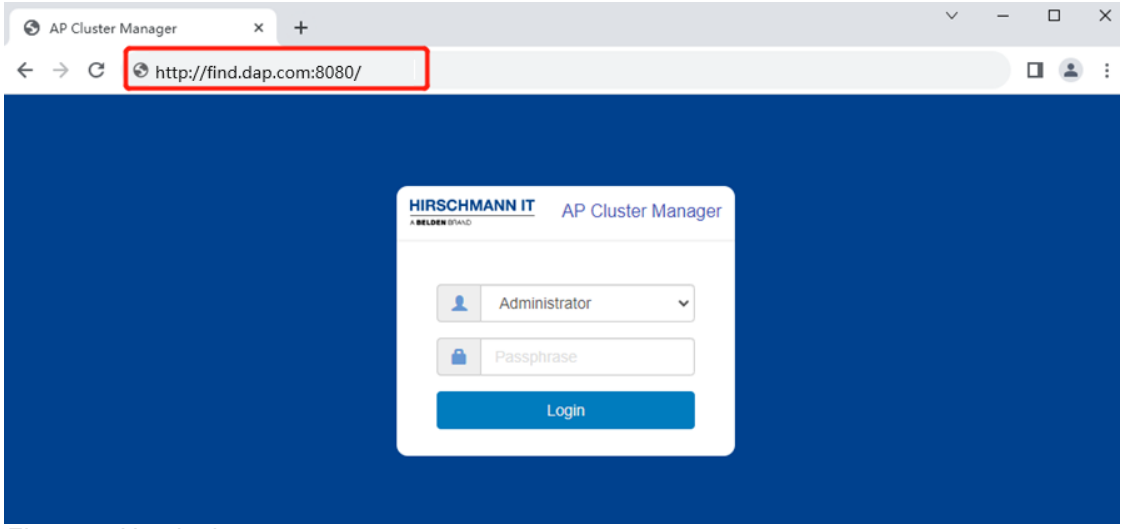


Figure 4: Http login

- Login with http by https://find.dap.com. The IP address of DAP847-XXA IP is 172.16.102.109, see Figure 5.

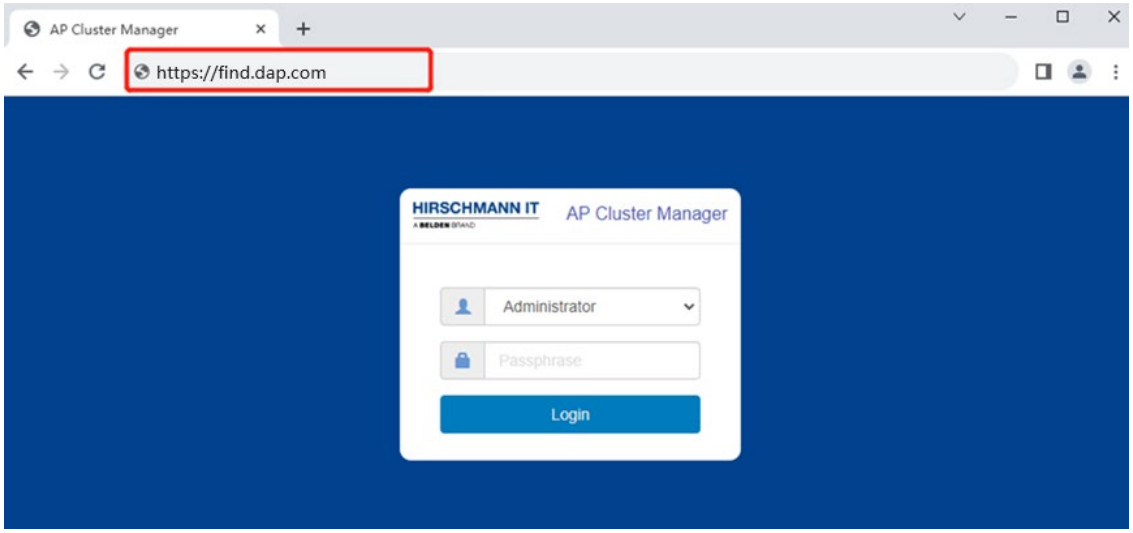


Figure 5: Https login

Note: A digital certificate needs to be installed by https login for secure communication between the DAP847-XXA and the browser. The certificate installation procedure varies from the OS and browser combinations. You can download the CA root certificate file from DAP847-XXA, see Figure 6.

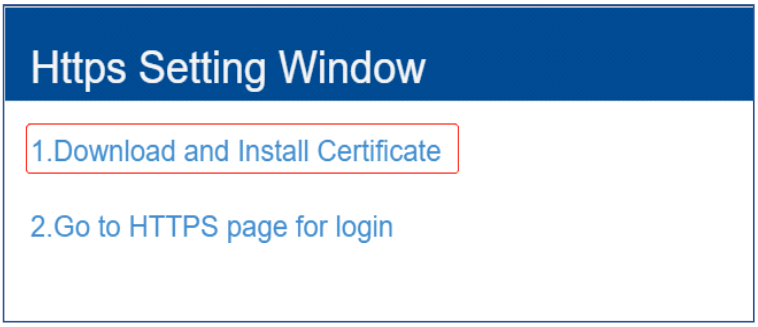


Figure 6: Download and Install Certificate

If no DNS server is available in the network, you can connect directly to the DAP847-XXA cluster using the IP address of any DAP847-XXA in the cluster. If you log in using the IP address of a non-PVM device, you will automatically jump to the PVM login page. See Figure 7.

For example:

- http://172.16.10.169:8080 (DAP847-XXA IP address is 172.16.10.169)
- https://172.16.10.169 (DAP847-XXA IP address is 172.16.10.169)

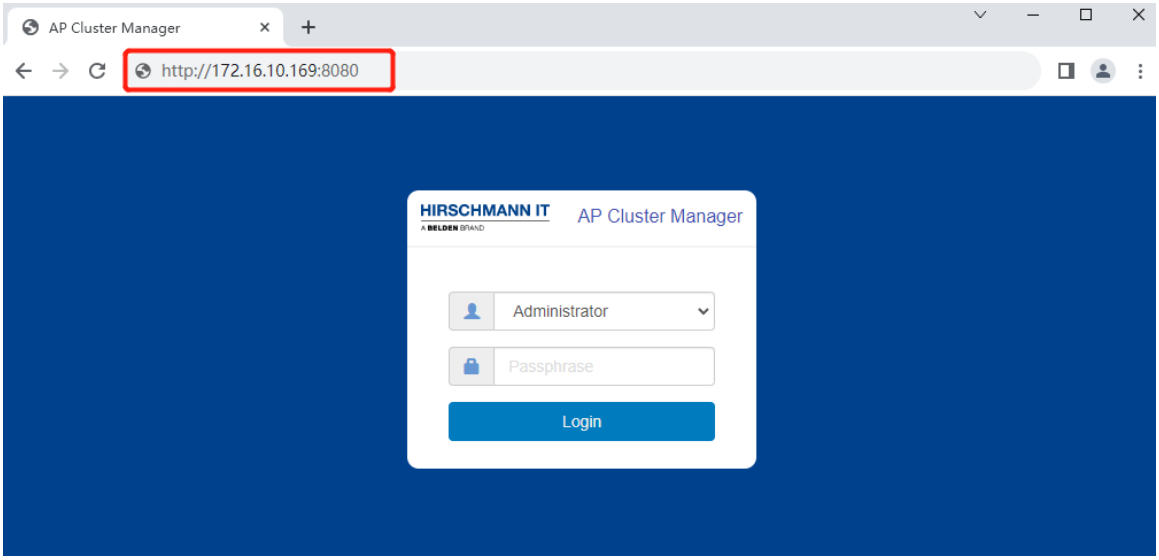


Figure 7: Log in using the IP address

If you do not know the current DAP847-XXA IP address, you can use the command "`ifconfig br-wan`" to check the IP address, see DAP847-XXA IP address on page 20.

4.2 Using the DAP847-XXA setup wizard

You can log in with the user name **“Administrator”** and the default password **“admin”**. When logging in for the first time, the initial configuration is completed through the configuration wizard.

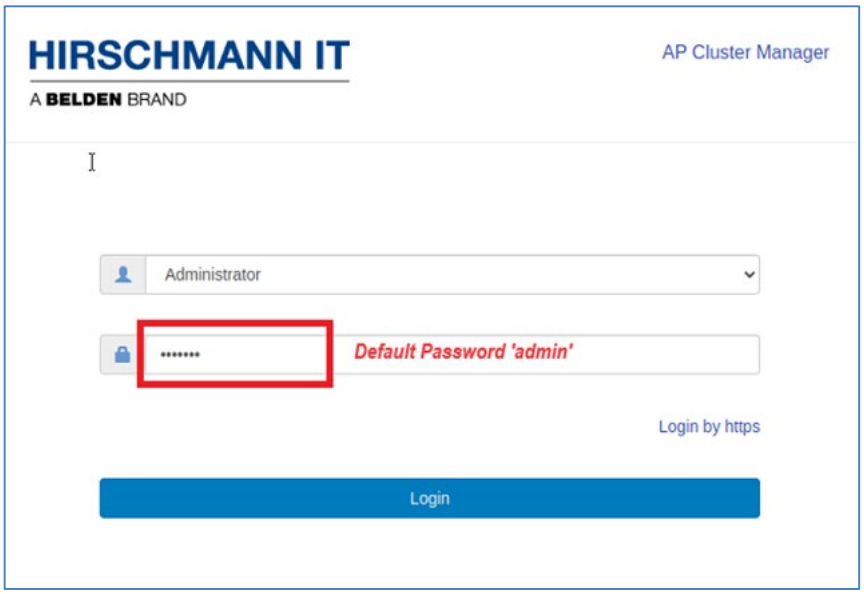


Figure 8: Log in with administrator

4.2.1 DAP Initialization

Configure the DAP847-XXA by the Setup Wizards:

☐ Select one of the following DAP847-XXA work modes.

- **Cluster mode:**

  The DAP847-XXA is in self-management and autonomous mode and an additional controller is not needed. A virtual manager named PVM will be selected from the DAP847-XXA devices.

- **DAC mode:**

  The DAP847-XXA is managed by a management platform named DAC. DAC will perform the configurations and policies.

  For detailed configuration in this mode, refer to the DAC User Manual.

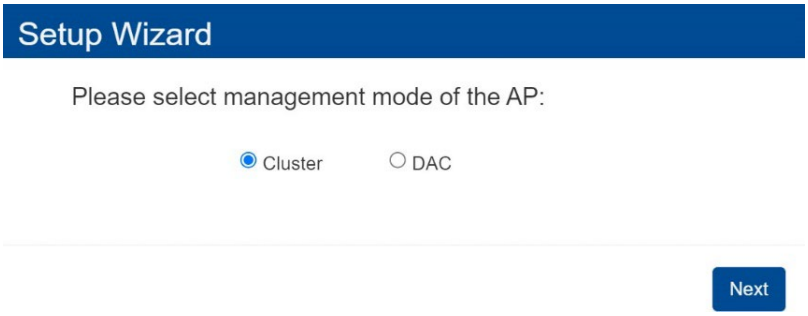


Figure 9: Select the AP work mode

☐ Welcome window of the DAP847-XXA Cluster Manager.

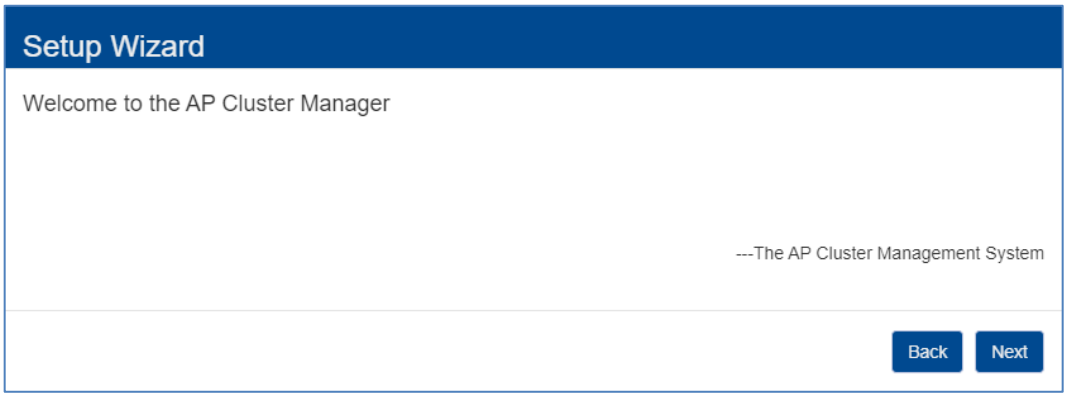


Figure 10: Welcome window of the DAP847-XXA Cluster Manager

☐ Change your administrator password.

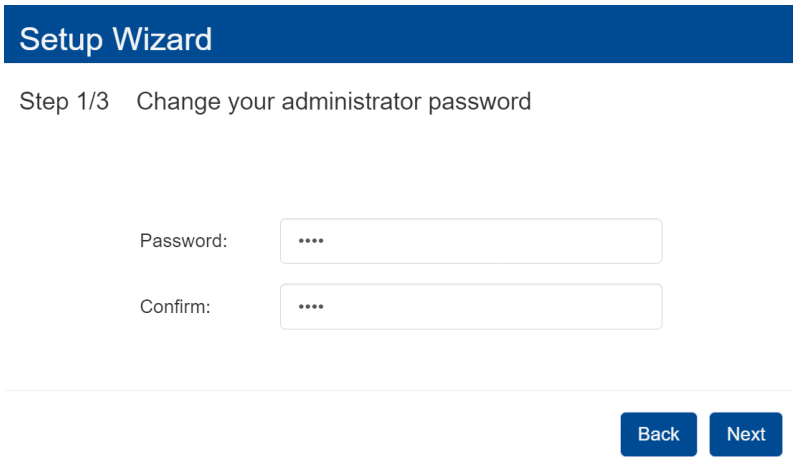


Figure 11: Change your administrator password

☐ Choose your "**Country/Region**" and "**Time Zone**".

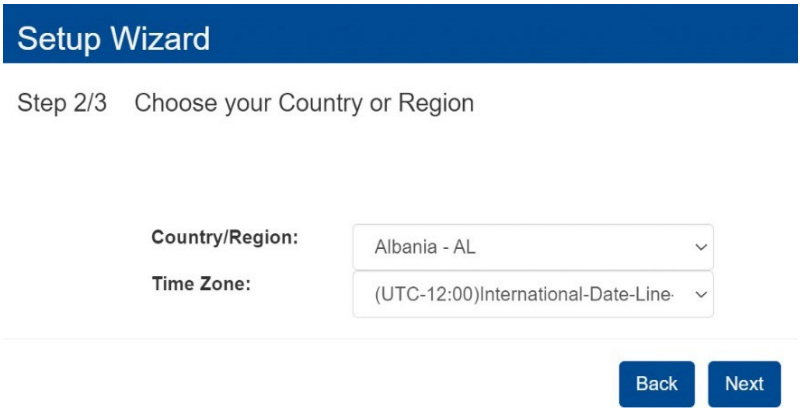


Figure 12: Choose your country/region and time zone

☐ Create a new WLAN. See "WLAN" on page 49.

Note: The default SSID named **"mywifi-xx:xx"** will be deleted automatically after a new SSID is created.

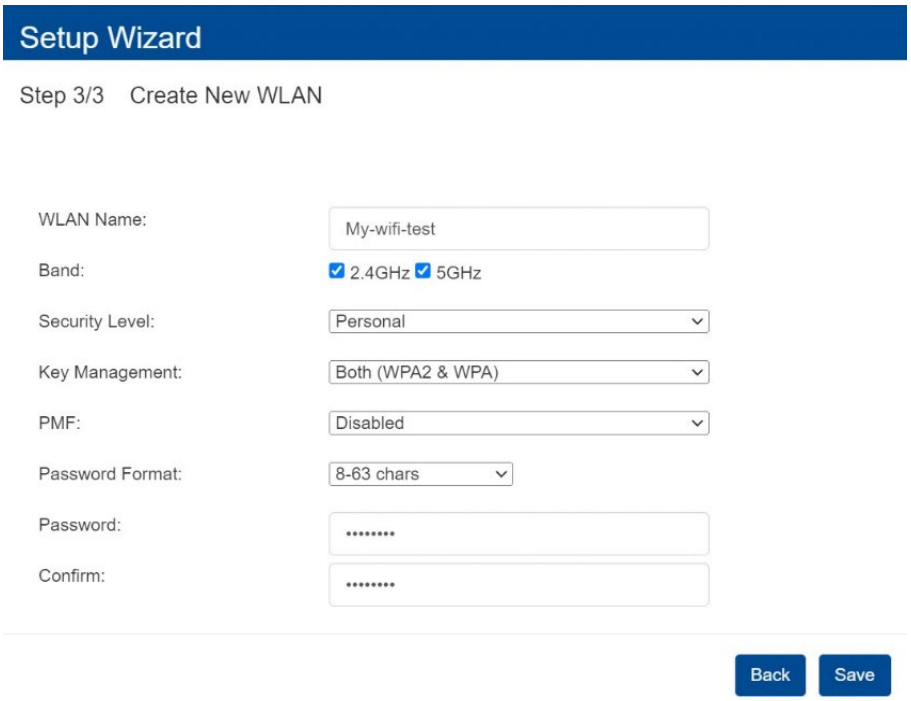


Figure 13: Create a new WLAN

After finishing the Setup Wizard, the DAP847-XXA automatically reboots and switches to the new working mode. At the same time, a **"Notice"** window pops up.

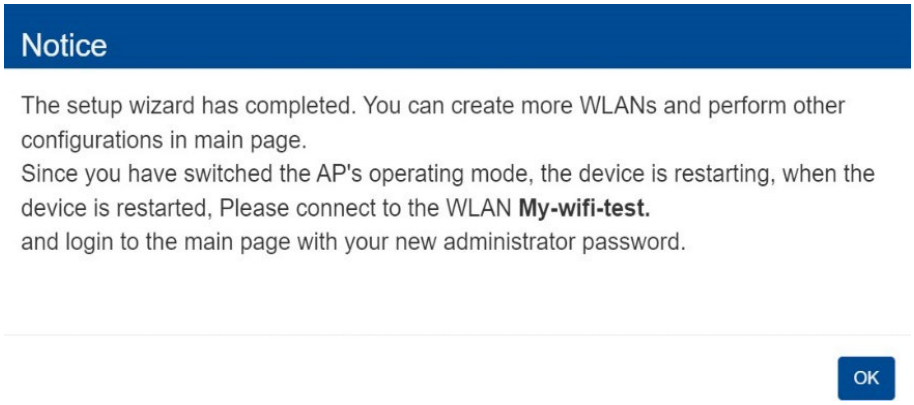


Figure 14: Pop up notice for DAP847-XXA rebooting

After the DAP847-XXA reboot, connect to the new SSID. Log in with the new password and continue with other configurations as needed. After you log in to the web GUI, you will see the default SSID has been deleted and a new SSID is displayed in the WLAN window.

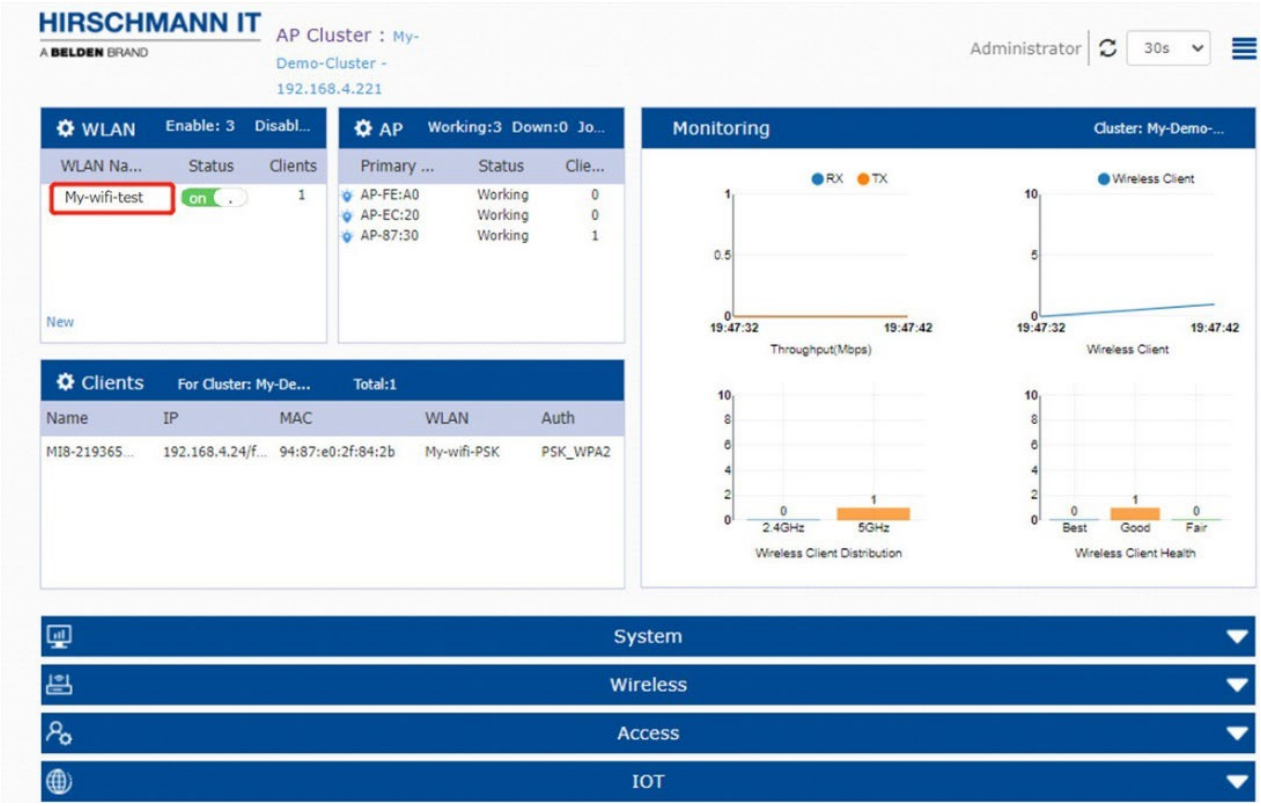


Figure 15: Log in the DAP847-XXA cluster

5 DAP cluster web GUI

This chapter briefly introduces the dashboard and configuration windows on the DAP847-XXA Web GUI. For detailed information on separate functions, refer to the related chapter accordingly.

This section contains the following topics:

- Dashboard overview
- WLAN
- AP
- Clients
- Monitoring
- System
- Wireless
- Access
- More

5.1 Dashboard overview

The DAP847-XXA provides a dashboard window to display the current operating status and configuration information.

Figure 16: Dashboard overview

Figure 16 illustrates the Dashboard overview. On the top of the window, you can see the cluster information, the current login user, the refresh button, the refresh cycle, and more.

The dashboard window is divided into **WLAN**, **AP**, **Monitoring**, **Clients**, **System**, **Wireless**, **Access**, and **IOT** sub-windows. You can briefly check the detailed information by clicking each window.

5.2 WLAN

The WLAN window contains WLAN-related monitoring and operations. There are 2 modes for the WLAN window. Click the WLAN window to launch the WLAN Configuration window.

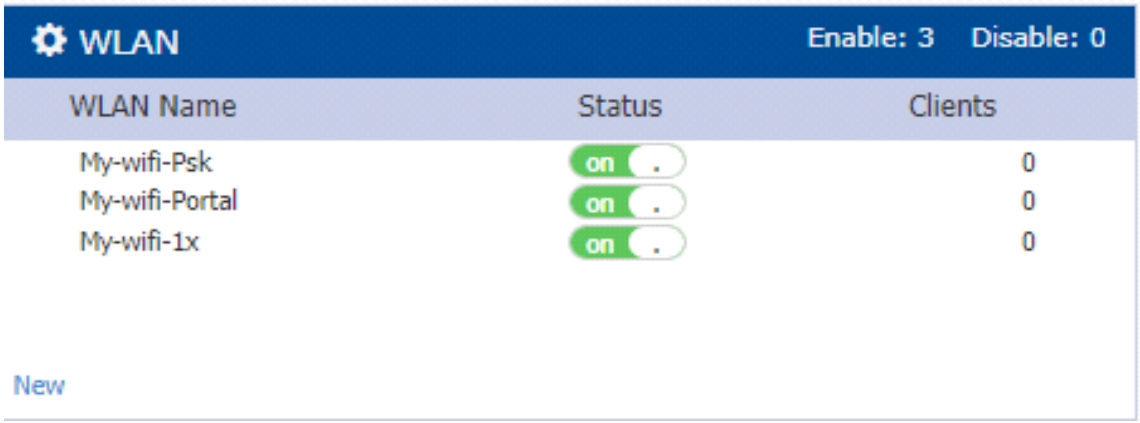


Figure 17: WLAN window

The key parameters are described as follows:

Parameter	Description
WLAN Name	Labels or WLAN names, which are composed by 0 … 9, a … z, or other strings
Status	Indicates the WLAN state: . off indicates that WLAN is not in broadcast state. on . indicates WLAN is in broadcast state.
Clients	The number of users connected to the WLAN
New	Launches the WLAN creation window.

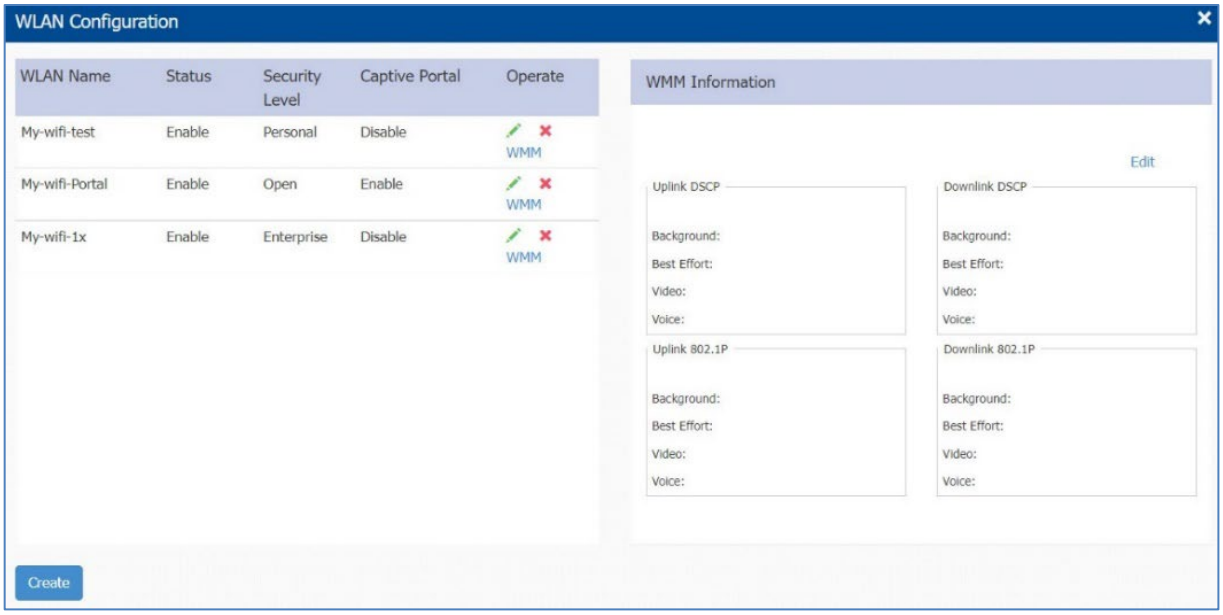


Figure 18: WLAN configuration window

The key parameters are described as follows:

Parameter	Description
WLAN Name	The name of the WLAN, which are composed by 0 … 9, a … z, or other strings
Status	Indicates the WLAN state: ▶ **"Enable"**: The WLAN is in the broadcast state. ▶ **"Disable"**: The WLAN is not in the broadcast state.
Security Level	Indicates the security level of WLANs, from high to low: **Enterprise>Personal>Open**.
Captive Portal	Indicates whether the WLAN is using the captive portal authentication: ▶ **"Enable"**: The WLAN is configured with captive portal authentication. ▶ **"Disable"**: means the WLAN is not configured with captive portal authentication.
Operate	Operates the WLANs including **"Modifying your WLAN"**, **"Deleting your WLAN"**, and **"Modifying Wi-Fi Multimedia (WMM)"**.
Create	Creates a new WLAN.

Note: The label below shows the number of enabled or disabled WLANs.

5.3 AP

The AP Window contains the DAP847-XXA's cluster-related monitoring and configuration functions. There are 2 modes for the AP window. Click the AP window frame from the basic mode to the AP Configuration mode.

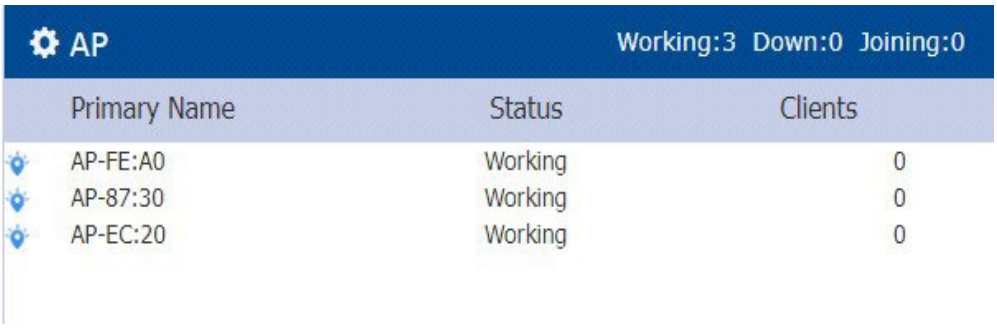
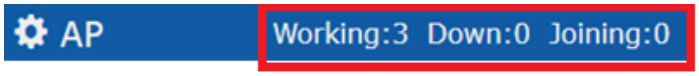


Figure 19: AP window

The key parameters are described as follows:

Parameters	Description
Primary Name	Shows the name of the DAP847-XXA. The name format is AP-XX:XX, where XX:XX represents the last two bytes of the AP MAC address.
Status	Indicates the connection status of the DAP847-XXA: ▶ Working: The DAP847-XXA has connected to the PVM and it is working normally. ▶ Down: The DAP847-XXA disconnected from the cluster. ▶ Joining: The DAP847-XXA is joining the cluster.
Clients	Indicates the number of current users connected to the DAP847-XXA devices.

Note: The Label in the AP window indicates the number of Aps in each status.



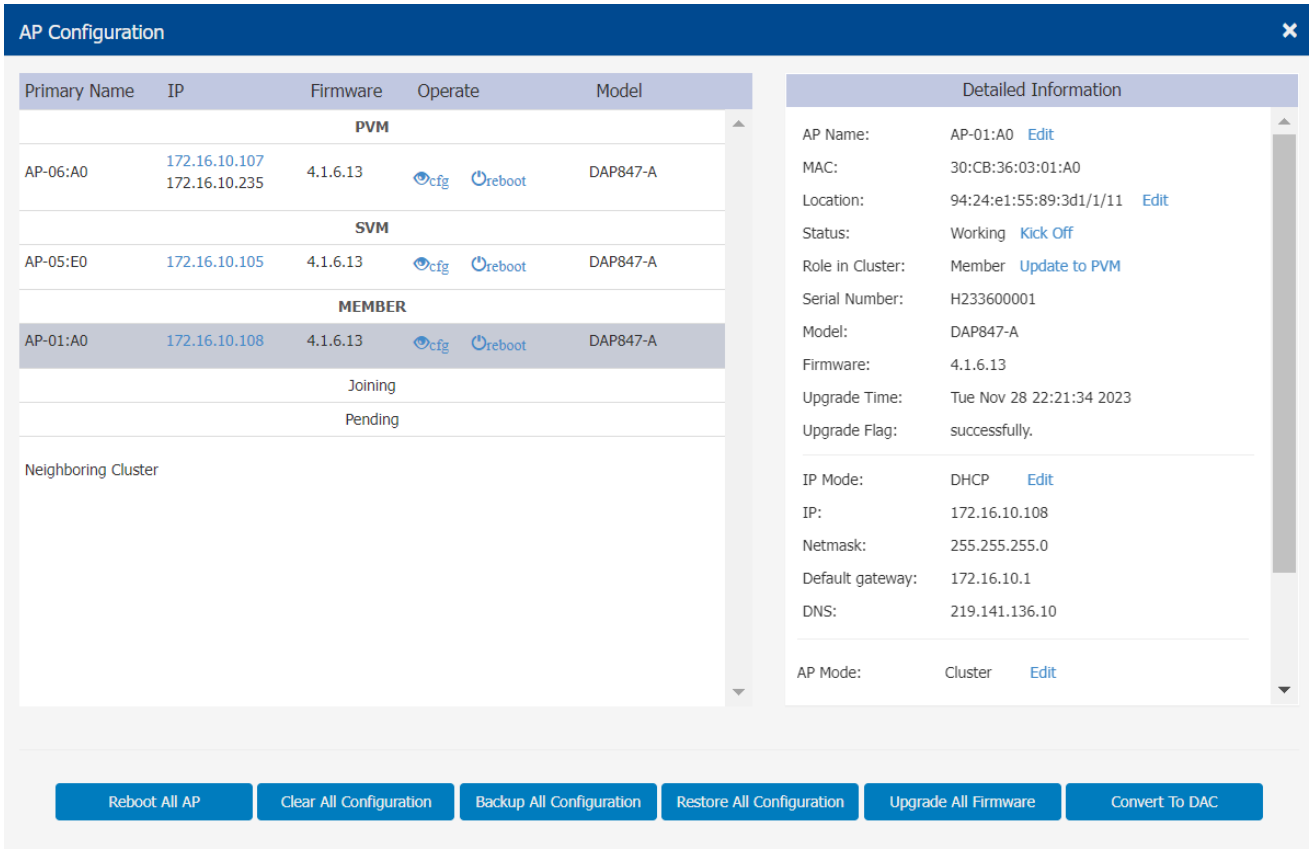


Figure 20: AP configuration window

The key parameters are described as follows:

Parameter	Description
Primary Name	Name of the DAP847-XXA.
IP	The IP address of the DAP847-XXA.
Firmware	The firmware version of the DAP847-XXA.
Operate	There are 2 optional operations for the DAP847-XXA: ▶ cfg: Checks the detailed configuration of the DAP847-XXA. ▶ reboot: Executes to reboot the DAP847-XXA.
Model	The model of the DAP847-XXA.
PVM	The DAP847-XXA is the PVM of the cluster.
SVM	The DAP847-XXA is the SVM of the cluster.
MEMBER	The DAP847-XXA is the member of the cluster.
Joining	In the joining state, the DAP847-XXA needs the authorization to join the cluster.
Pending	In a pending state, the DAP847-XXA needs to upgrade the software to join the cluster.
Neighboring Cluster	The neighboring DAP847-XXA clusters with different cluster ID.
Reboot All AP	Reboots all the DAP847-XXA devices in the cluster.

Parameter	Description
Clear All Configuration	Restores the factory settings for all the DAP847-XXA devices in the cluster.
Backup All Configuration	Backups the configuration of the DAP cluster, a configuration file named "`pub-config.tar`" will be downloaded to the local host.
Restore All Configuration	To restore the previously backed up configuration file, please note that the filename must be "`pub-config.tar`".
Upgrade All Firmware	Updates the firmware for all the DAP847-XXA devices in the cluster.
Convert To DAC	Switch DAP847-XXA from cluster working mode to DAC working mode. Once configured, DAP847-XXA will reboot and register with the DAC. ► **Management Server**: DAC IP address.
Detailed Information	Detailed information for the selected DAP847-XXA: ► AP name: The name of the selected DAP847-XXA ► MAC: The MAC address of the selected DAP847-XXA ► Location: The location of the selected DAP847-XXA ► Status: The status of the selected DAP847-XXA ► Role in Cluster: The role of the selected AP in the cluster ► Serial Number: The serial number of the selected DAP847-XXA ► Model: The product model number of the selected DAP847-XXA ► Firmware: The firmware version of the selected DAP847-XXA ► Upgrade Time: The last upgrade time of the selected DAP847-XXA ► Upgrade Flag: The result of the last upgrade ► IP Mode: The way that the selected DAP847-XXA obtains the IP address ► IP: The IP address of the selected DAP847-XXA ► Netmask: The IPv4 address netmask of the selected DAP847-XXA ► Default gateway: The default gateway of the selected DAP847-XXA ► DNS: The DNS server
Kick Off	Removes the DAP847-XXA from the cluster. When a DAP847-XXA is removed from the cluster, it changes into a Joining state until the administrator allows it to join the cluster again.
Update to PVM	The member or the SVM of the DAP847-XXA cluster can be upgraded to the PVM.
AP Mode	► **Cluster**: The DAP is working in the cluster mode. ► **DAC**: Configures and manages the DAP847-XXA through the DAC. You need to specify the DAC IP address when you change the mode of the DAP847-XXA to the DAC mode.

5.4 Clients

The Clients window displays the connected clients. Like the WLAN window, there are 2 modes for the Client window: basic mode and client information mode. Click the Clients window frame to launch the client information mode from the basic mode.

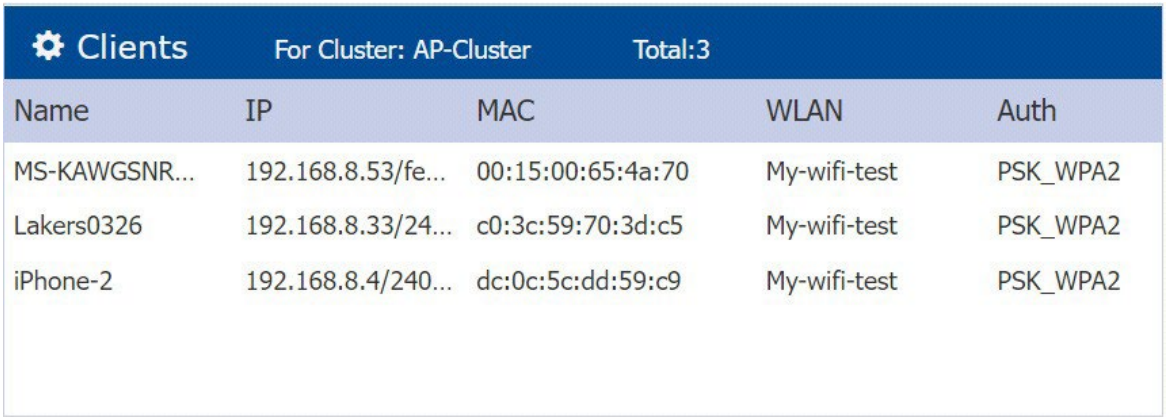


Figure 21: Clients window - basic mode

The key parameters are described as follows:

Parameter	Description
For Cluster: [*ClusterName*]	Clients connected to the cluster
For WLAN: [*WLANName*]	Clients connected to the specified WLAN in the cluster
For AP: [*AP_MAC*]	Clients connected to the specified DAP847-XXA in the cluster.
Name	The user name or host name of the client. For clients who log in with a user name, the user name is shown in the field. For clients who log in without a user name, the host name is shown in the field. The name field may be empty if the host name cannot be obtained.
IP	The IP address of the client, including IPv4 address and IPv6 address.
MAC	The MAC address of the client
WLAN	The WLAN to which the client connected
Auth	The authentication type of the clients: Open, Portal (Captive portal), PSK (Personal), and IEEE 802.1X (Enterprise).

In the **Clients Information** window, click "✖" of the client entry to remove the specific client from DAP847-XXA, and click "🗑" to remove the client and add it to the blocklist.

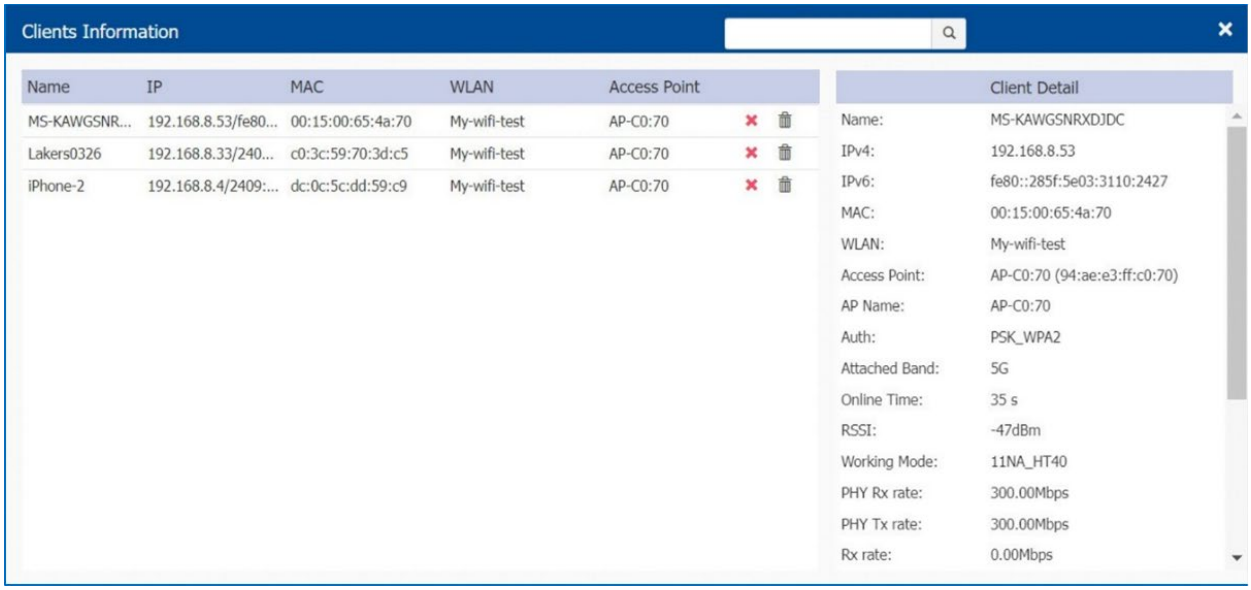


Figure 22: Clients information window

The key parameters of **Client Information** are described as follows:

Parameter	Description
Name	The user name of the client
IP	The IP address of the client
MAC	The MAC address of the client
WLAN	WLAN to which the client connected
Access Point	The name of DAP847-XXA to which the client is connected
✖	Disconnects the client from the wireless network.
🗑	Removes the client from the wireless network and put it on the blocklist. If a client is added to the blacklist, you can view and modify it in the **Access** -> **Blocklist & Allowlist window**.

Client Detail	
Name:	iPhone-2
IPv4:	172.16.10.109
IPv6:	fe80::84e:1082:bc25:1a14
MAC:	dc:0c:5c:dd:59:c9
WLAN:	My-wifi-test
Access Point:	AP-06:A0 (30:cb:36:03:06:a0)
AP Name:	AP-06:A0
Auth:	PSK_WPA3
Attached Band:	5G
Online Time:	7 m 33 s
RSSI:	-78dBm
Working Mode:	11AC_VHT20
PHY Rx rate:	130.00Mbps
PHY Tx rate:	144.40Mbps
Rx rate:	0.00Mbps
Tx rate:	0.00Mbps
Download:	43MB
Upload:	3MB
Device Type:	Mobile
OS Type:	iOS
Rx Error:	0
Tx Retry:	0
Roaming History	

Figure 23: Client Detail Window

The key parameters of **Client Detail** are described as follows:

Parameter	Description
Name	Name of the selected client.
IPv4	The IPv4 address of the client.
IPv6	The IPv6 address of the client.
MAC	The MAC address of the client.
WLAN	The WLAN which the client is associated with.
Access Point	The device name (MAC address) of the DAP847-XXA that the client is associated with.
AP Name	The device name of the DAP847-XXA that the client is associated with.

Parameter	Description
Auth	The authentication type of the client: Open, Portal (Captive Portal), PSK (Personal), IEEE 802.1X (Enterprise)
Attached Band	The radio band through which the client attaches to AP, 2.4 GHz or 5GHz
Online Time	The online connection duration of the client
RSSI	The Received Signal Strength Indication (RSSI) of the client. The value is 0~99.
Working Mode	The wireless working mode of the client
PHY Rx rate	Physical receiving rate of the client, unit: Mbps
PHY Tx rate	Physical sending rate of the client, unit: Mbps
Rx rate	Packet receiving rate of the client, unit: Mbps
Tx rate	Packet sending rate of the client, unit: Mbps
Download	The amount of data downloaded by the client since the last connection
Upload	The amount of data uploaded by the client since the last connection
Device type	The device type of the client
OS Type	The operating system type of the client
Rx Error	Shows the number of detected error packets received by the client, caused by interference or mismatch of broadcast power levels.
Tx Retry	Shows the number of retry packets sent by the client. The retry packets indicate re-sent packets because they were corrupted upon arriving at the proper destination.
Roaming History	Shows roaming history between SSID/AP/Band for the client. A total of 32 roaming records can be displayed and will be separated by connection sessions. Connection Session: A session represents a period that starts by associating with the wireless network and ending by disassociating.Roaming records are distributed within sessions. The connection sessions are arranged based on a time sequence. The latest session will be positioned on the top of the roaming history display. The Offline status represents the connection session has ended. TheOnline status represents an ongoing session, and the client is not disassociated.

5.5 Monitoring

The **Monitoring** window displays the utilization of the wireless network. It includes statistics of traffic throughput and client working state. The monitoring window shows 4 different aspects of data: cluster-based, WLAN-based, AP-based, and client-based.

Cluster-based monitoring is the default display:

- Switch to statistics of the WLAN by selecting a WLAN in the WLAN window.
- Switch to statistics of a specific DAP847-XXA by selecting a DAP847-XXA in the AP window.
- Switch to statistics of a specific client by selecting a client in the Client window.

By default, the refresh cycle of the **Monitoring** window is 30 seconds, and it can be set to 60 seconds or 120 seconds.

5.5.1 Cluster-based Monitoring

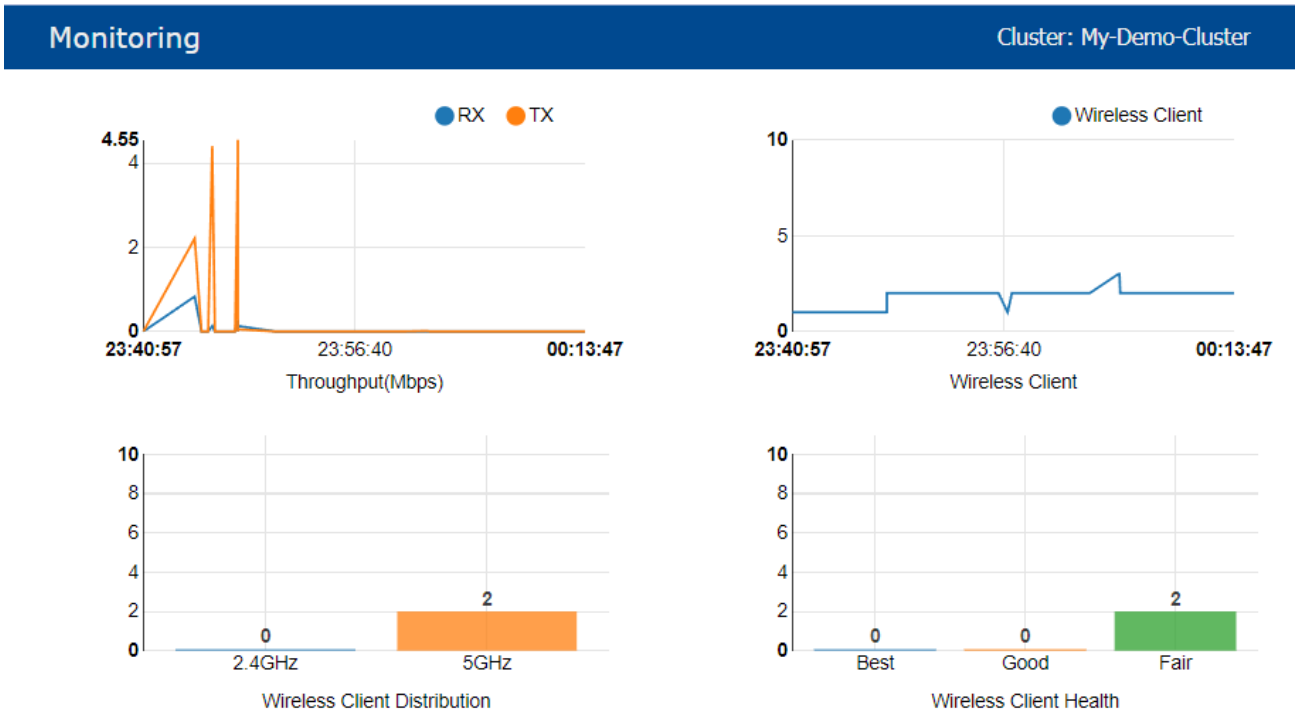


Figure 24: Monitoring window - cluster-based

The key parameters are described as follows:

Parameter	Description
RX	The average received data rate (throughput) of all DAP847-XXA devices in the cluster, unit: Mbps.
TX	The average transmission data rate (throughput) of all DAP847-XXA devices in the cluster, unit: Mbps.
Wireless Client	The number of clients connected to the DAP847-XXA cluster
Wireless Client Distribution	The working band distribution of clients connected to the DAP847-XXA cluster,including the number of clients working on the 2.4 GHz band and the number of clients working on the 5 GHz band
Wireless Client Health	The wireless connection quality between the client and the DAP847-XXA is judged by the signal strength of the client, and it is classified into the following grades: ▶ Best: Number of clients whose signal strength greater than or equal to 30. ▶ Good: Number of clients whose signal strength is between 15 and 30. ▶ Fair: Number of clients whose signal strength is less than or equal to 15.

5.5.2 WLAN-based Monitoring

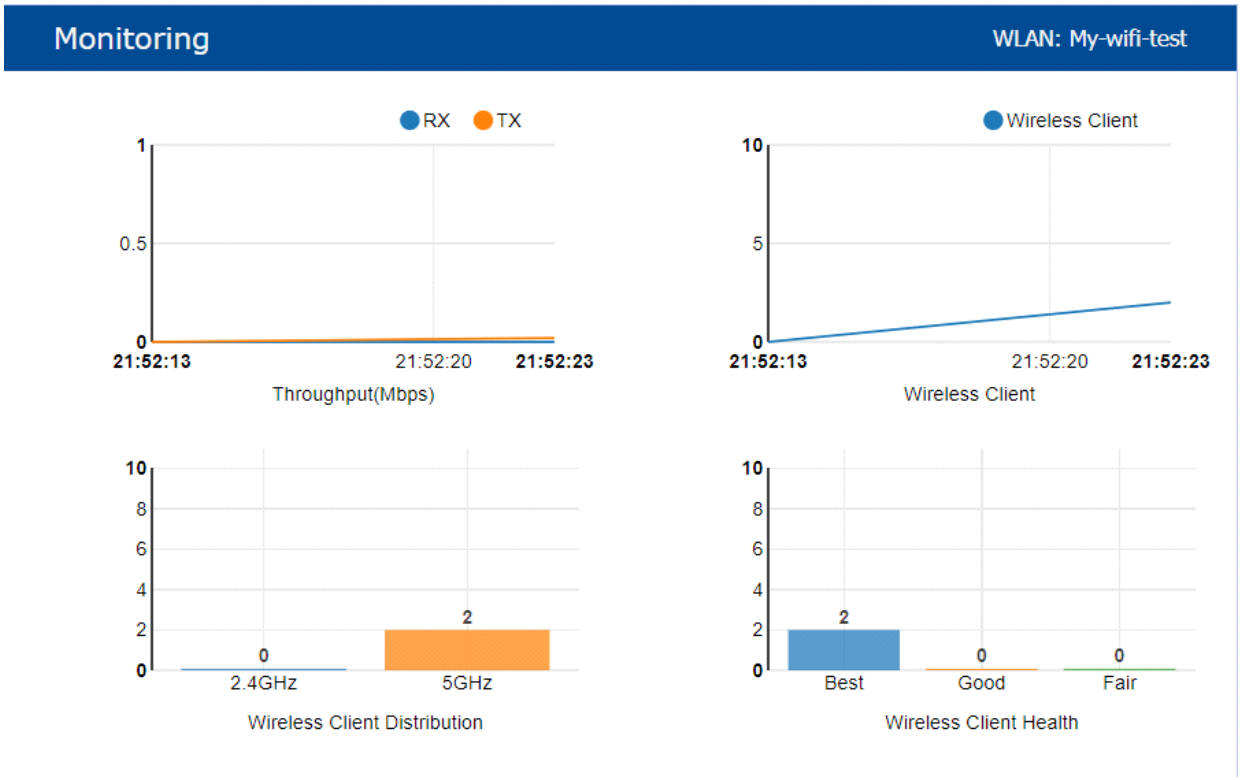


Figure 25: Monitoring window – WLAN-based

The key parameters are described as follows:

Parameter	Description
RX	The average received data rate (throughput) of this WLAN, unit: Mbps.
TX	The average transmission data rate (throughput) of this WLAN, unit: Mbps.
Wireless Client	The number of clients connected to the WLAN.
Wireless Client Distribution	The working band distribution of clients connected to the WLAN, including the number of clients working on the 2.4 GHz band and the number of clients working on the 5 GHz band.
Wireless Client Health	The wireless connection quality between the client and DAP847-XXA is judged bythe signal strength of the client, and it is classified into the following grades: ▶ Best: Number of clients whose signal strength greater than or equal to 30. ▶ Good: Number of clients whose signal strength is between 15 and 30. ▶ Fair: Number of clients whose signal strength is less than or equal to 15.

5.5.3 AP-based Monitoring

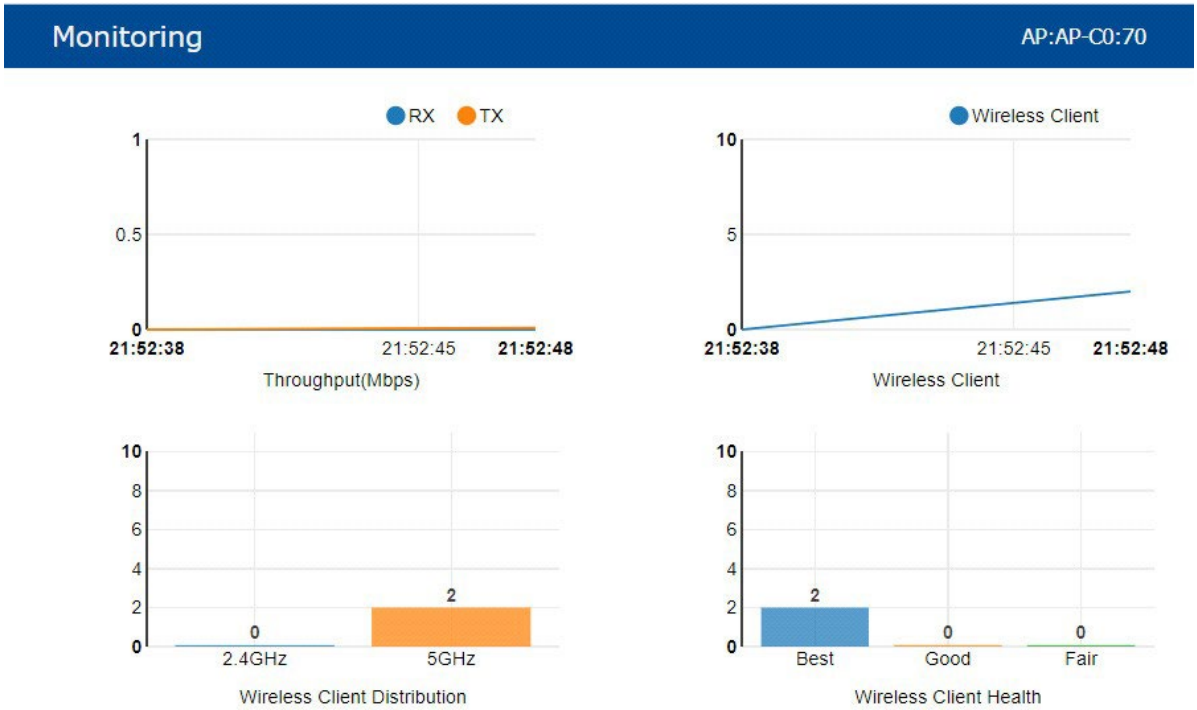


Figure 26: Monitoring window – AP-based

The key parameters are described as follows:

Parameter	Description
RX	The average received data rate (throughput) of this AP, unit: Mbps
TX	The average transmission data rate (throughput) of this AP, unit: Mbps
Wireless Client	The number of clients connected to the AP
Wireless Client Distribution	The working band distribution of clients connected to the AP, including the number of clients working on the 2.4 GHz band and the number of clients working on the 5 GHz band
Wireless Client Health	The wireless connection quality between the client and DAP is judged by the signal strength of the client, and it is classified into the following grades: ▶ Best: Number of clients whose signal strength greater than or equal to 30. ▶ Good: Number of clients whose signal strength is between 15 and 30. ▶ Fair: Number of clients whose signal strength is less than or equal to 15.

5.5.4 Clients-based Monitoring

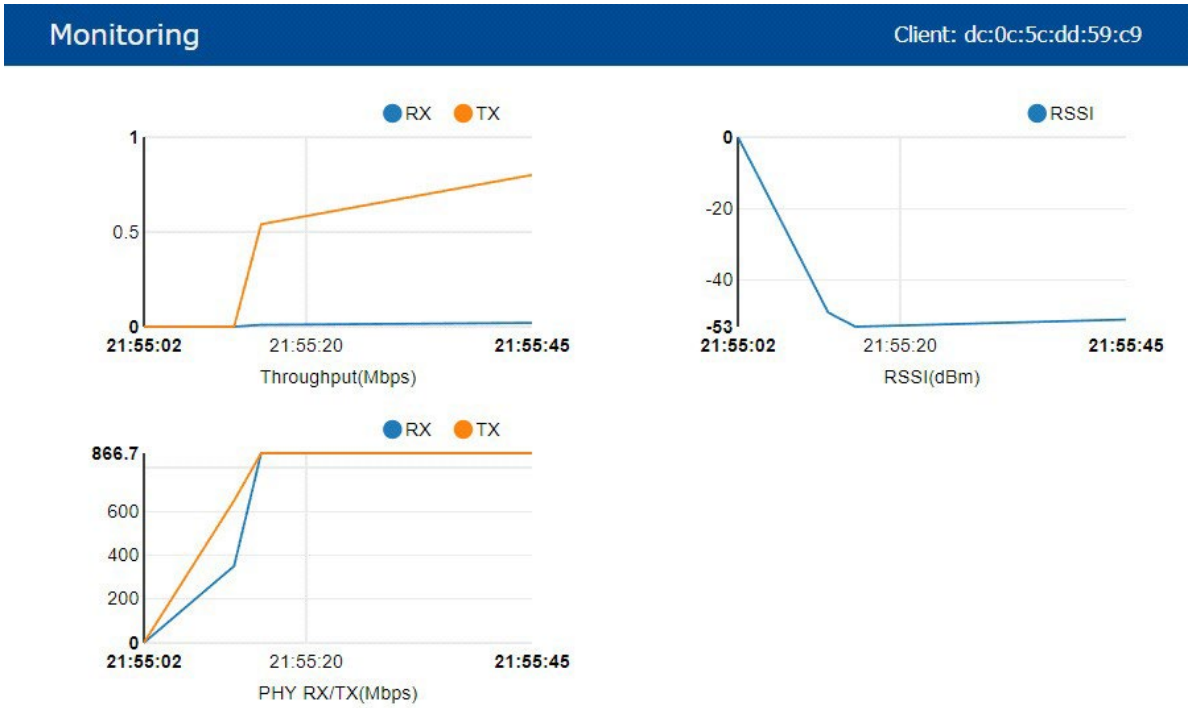


Figure 27: Monitoring window - clients-based

The key parameters are described as follows:

Parameter	Description
RX	The receiving rate of the client, unit: Mbps
TX	The sending rate of the client, unit: Mbps
RSSI	The Received Signal Strength Indication (RSSI) of the client
PHY RX	The physical receiving rate of the client, unit: Mbps
PHY TX	The physical sending rate of the client, unit: Mbps

5.6 System

The System window shows 3 blocks of information: **General, System Time**, and **Syslog & SNMP**. For details, see “System management” on page 122.

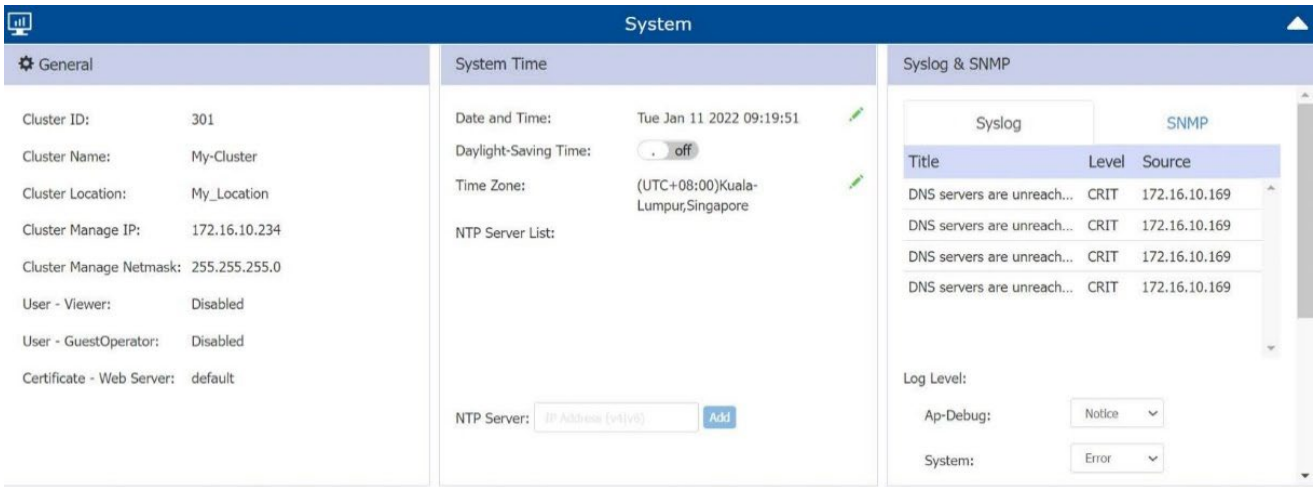


Figure 28: System window

5.7 Wireless

The Wireless window shows 3 blocks of information: Radio Frequency (RF), wIDS/wIPS, and Performance Optimization.

For details, see “Wireless management” on page 138.

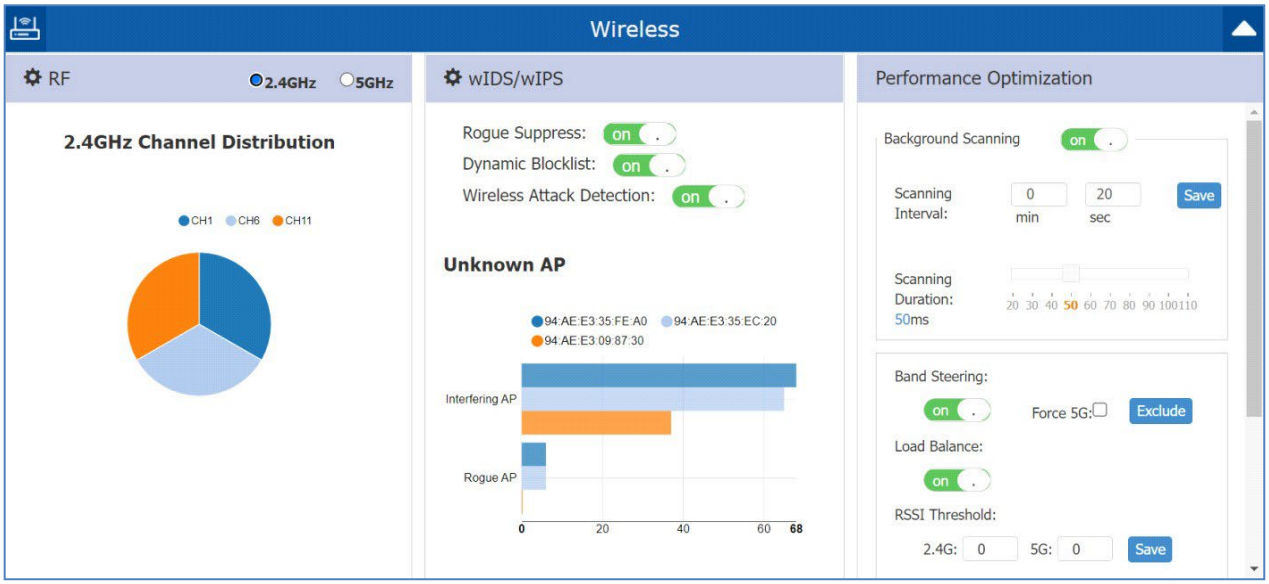


Figure 29: Wireless window

5.8 Access

The Access window shows 3 blocks of information: The **Authentication** window, **Blocklist & Allowlist** window, and the **ACL** window.

For more information about **Access**, see “Access” on page 157.

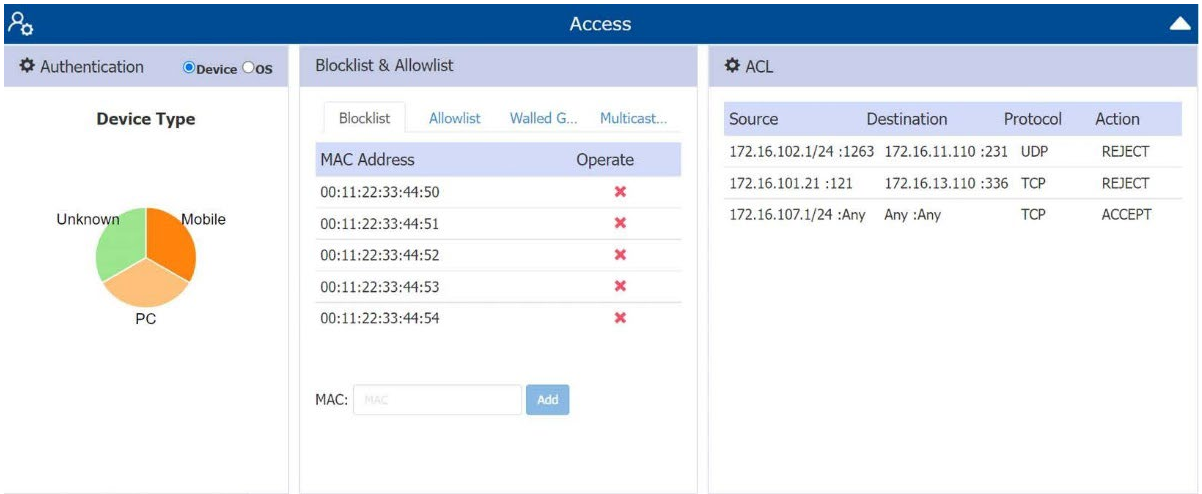


Figure 30: Access page

5.9 More

For more information about DAP847-XXA, click the More tab in the right-top corner.

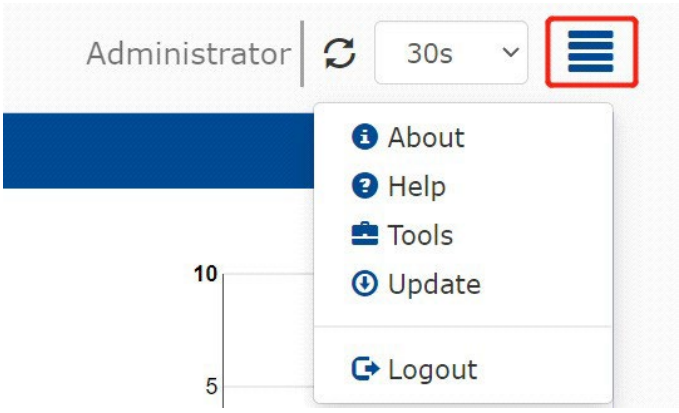


Figure 31: More information about DAP847-XXA

- **About**: Basic information of DAP847-XXA cluster, such as software version, Country/Region, etc.

Figure 32: About page

- **Help:** Displays the information in the tooltip when you hover the mouse pointer over the title bar.

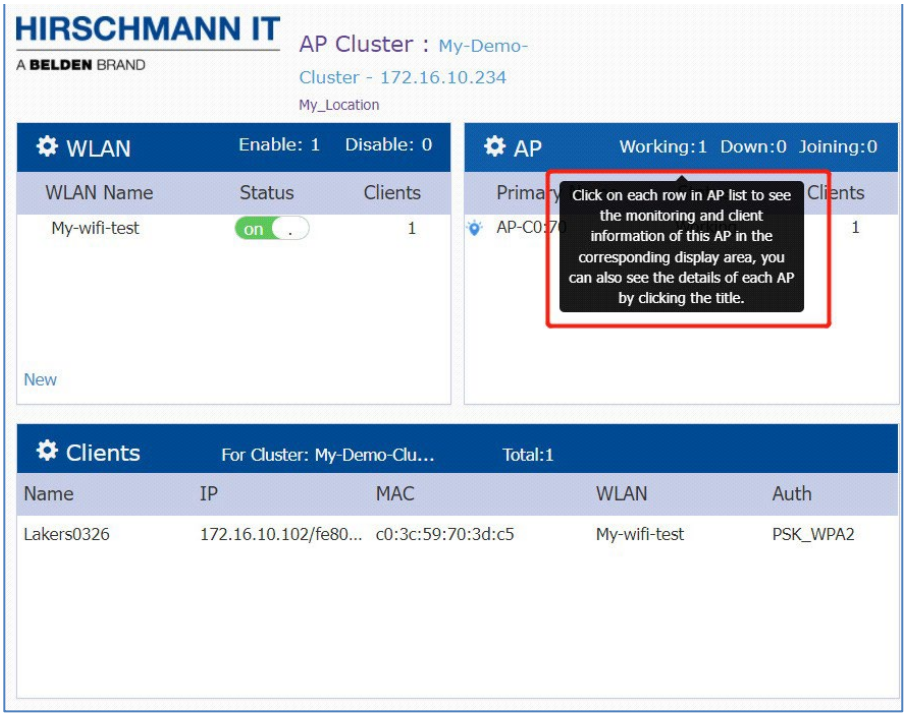


Figure 33: Online help

- **Tools:** Some basic troubleshooting tools integrated in the DAP847-XXA. See“Tools” on page 175.
- **Update:** Upgrades the DAP847-XXA if new version is detected.
- **Logout:** Logs out the current user.

6 WLAN

Configuring WLAN is the first step when you set up your Wi-Fi network. This section contains the following topics:

- Create a WLAN in two ways
- WLAN types
- WLAN parameter description
- Modify WLAN configuration
- Delete a WLAN
- WMM configuration

6.1 Create a WLAN in two ways

Create a WLAN in the cluster mode in the following two ways:

- ☐ Create a WLAN by clicking **"New"** in the WLAN basic mode in the WLAN window.

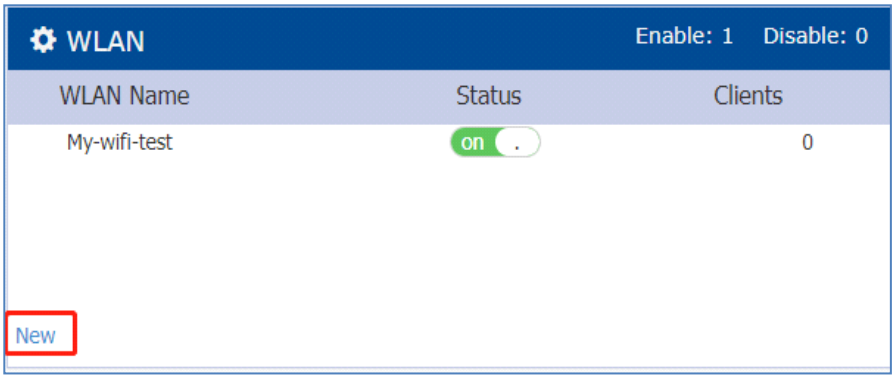


Figure 34: WLAN basic mode

On the pop-up "**Create New WLAN"** window, complete the WLAN configuration.

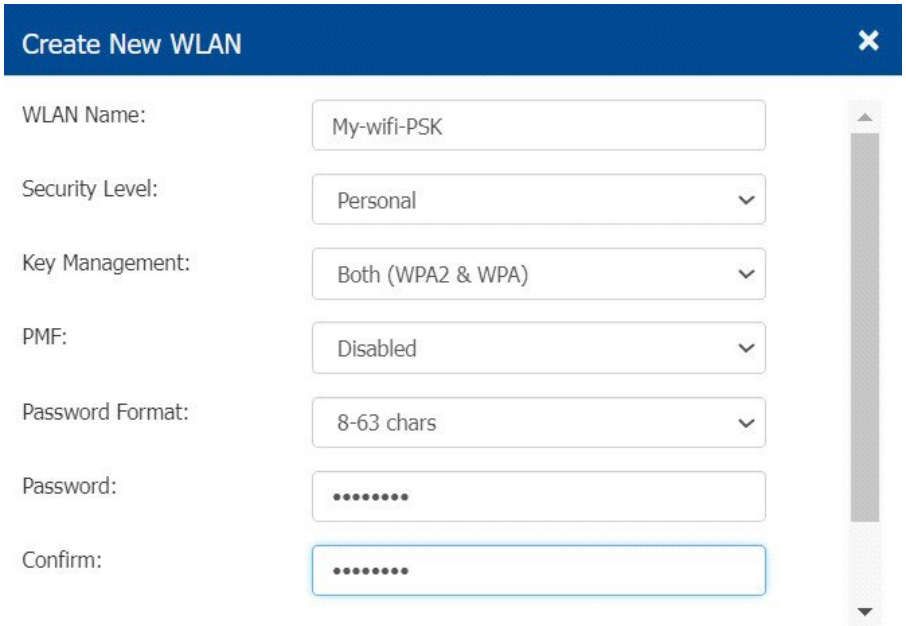


Figure 35: Create New WLAN window

- ☐ On **WLAN Configuration** page, click "**Create**" and finish the configuration on the right window.

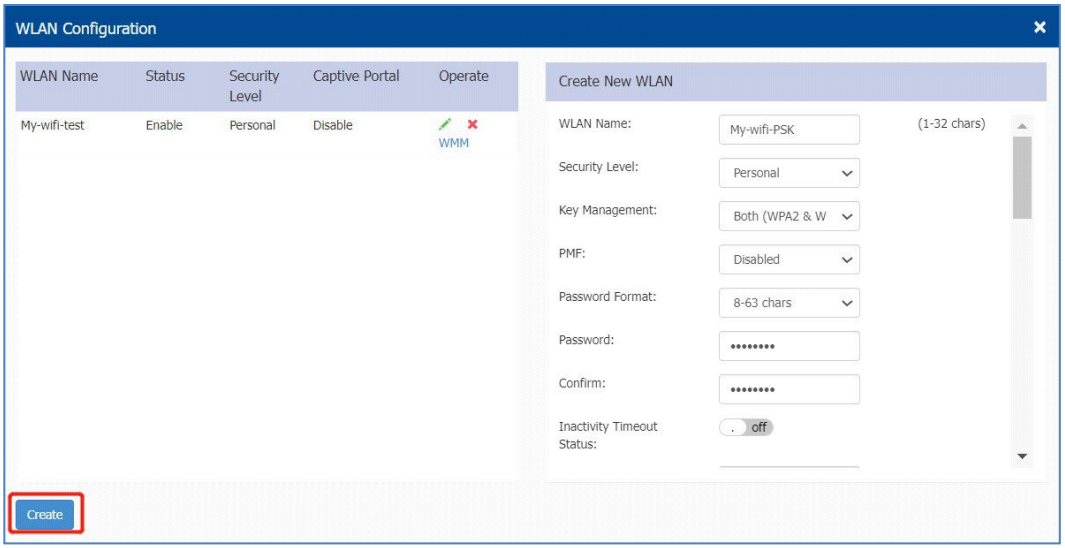


Figure 36: Create new WLAN in WLAN configuration window

6.2 WLAN security types

The DAP847-XXA supports 4 types of WLAN in the cluster mode:

- Open
- Portal
- Personal
- Enterprise

6.2.1 Security type Open

The **Open** type means no authentication or encryption. The data frame of wireless clients is transmitted as plain text.

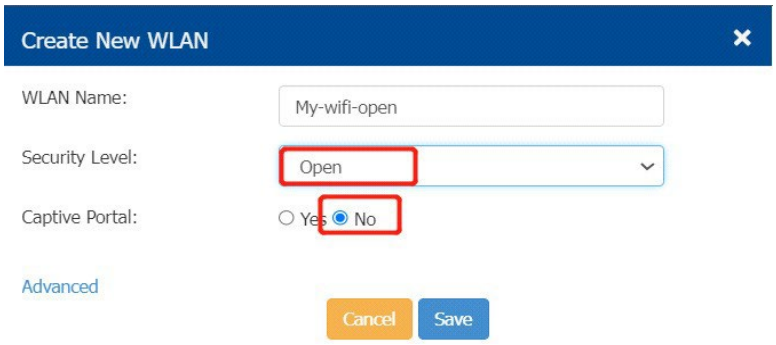


Figure 37: Create an open WLAN

6.2.2 Security type Portal

Configure **Open** in **"**Security Level" and select "**Yes**" for **"Captive Portal"** in the **Create New WLAN** window. Users connect to the network by a portal window with the access code needed. See "Login captive portal" on page 161.

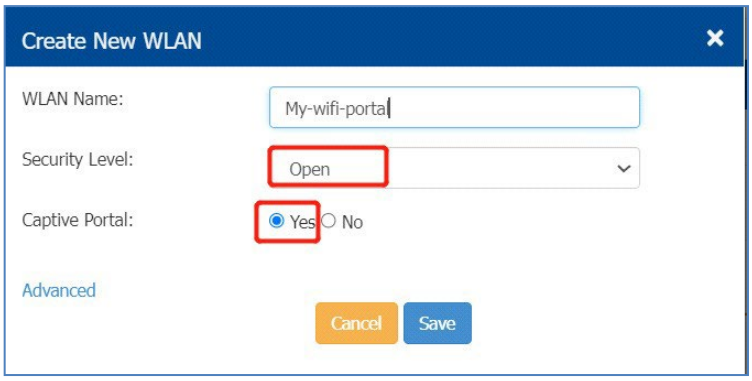


Figure 38: Create a portal WLAN

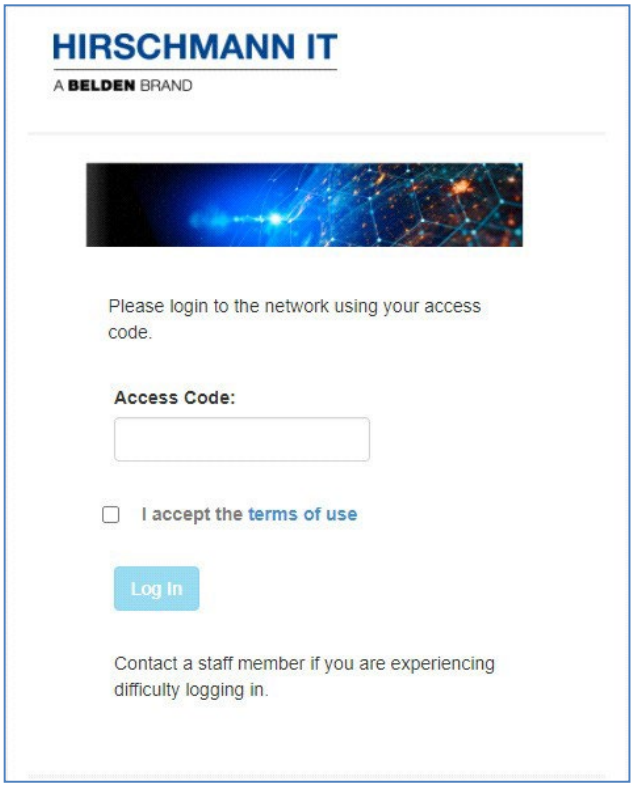


Figure 39: Portal login window

6.2.3 Security type Personal

The **Personal** type refers to PSK (Pre-Shared Key) mode and supports 5 security modes: Static WEP, WPA2, WPA3, WPA2 & WPA, and WPA3 & WPA2. It is an authentication mode designed for home or small business networks. In this mode, each wireless user needs to enter a preconfigured key to access the network, and no authentication server is required.

WPA, WPA2, and WPA3 use dynamic keys to encrypt data packets. Each wireless network device encrypts the network traffic using a 256-bit key. The key usually consists of 8 to 63 ASCII characters. The **Personal** type supports the following ways of key management:

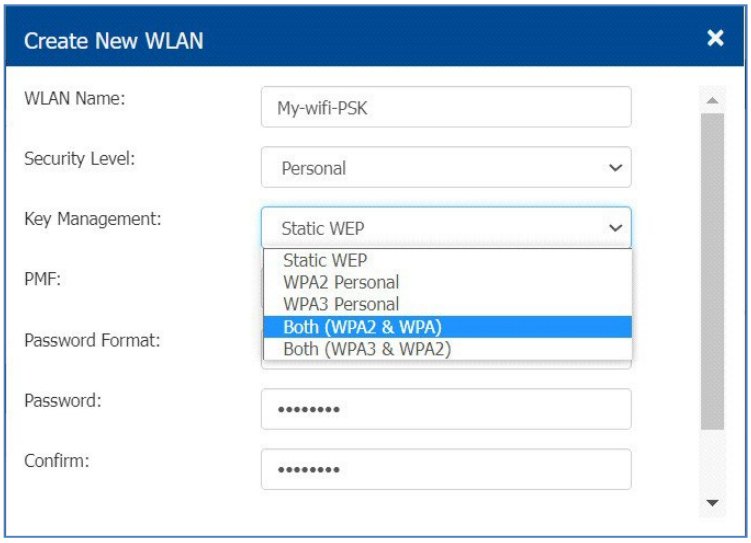


Figure 40: Create a Personal WLAN

- **Static WEP:** Encrypts and decrypts all communications with the same key, so it is called Static WEP. Static WEP encrypts packets using a static key pair, which can be 128 or 256 bits long, depending on the configuration chosen by the network administrator. Compared with WPA, WPA2, and WPA3-Personal, Static WEP uses a weaker encryption algorithm that can be easily cracked. Therefore, Static WEP encryption is not recommended in some wireless networks that require a high security level.
- **WPA2 Personal:** Personal mode of the WPA2 encryption protocol which uses cipher-based encryption. It is mainly designed to meet the needs of home and small company networks that cannot afford the cost and complexity of IEEE 802.1X authentication servers. WPA2 encrypts packets with a dynamic key, and each wireless network device encrypts the traffic using a 256-bit key, which is typically made up of 8 to 63 ASCII characters. In addition, WPA2 supports the four-handshake process, in which the client and the AP shake hands 4 times during the connection to enhance security.
- **WPA3 Personal:** It is the successor to WPA2 (WiFi Protected Access version 2), released by the Wi-Fi Alliance in 2018. WPA3-Personal utilizes a stronger secure encryption algorithm that can withstand dictionary attacks. It can withstand dictionary attacks by using password-based authentication and a secure authentication method SAE (Simultaneous Authentication of Equals). WPA3-Personal is more difficult to crack than the previous encryption algorithms used in TKIP (Temporal Key Integrity Protocol) and WPA2, thus enhancing the security of data transmission.

  WPA, WPA2, and WPA3 use dynamic encryption of packets. Each wireless

network device encrypts network traffic using a 256-bit key, which typically consists of 8 to 63 ASCII characters. In this mode, each wireless user is required to enter the same pre-configured key to access the network. The key typically consists of 8 to 63 ASCII characters.

- Both (WPA2 & WPA): Supports both WPA and WPA2.
- Both (WPA3 & WPA2): Supports both WPA2 and WPA3.

6.2.4 Security type Enterprise

Enterprise type is IEEE 802.1x authentication. It is an encryption method built on the IEEE 802.1X authentication framework that requires users to authenticate with personal certificates or usernames and passwords. It encrypts data transmissions using the AES encryption algorithm to provide a higher security level. Enterprise mode provides stronger security and more flexible deployment options than Personal authentication mode. It supports various types of EAPs (Extensible Authentication Protocols) for secure deployment of wireless networks in enterprises and public places.

It is designed for enterprise networks and a RADIUS authentication server is needed. It requires a complicated setup but provides additional security (e.g. protection against unauthorized access on short passwords). Various kinds of Extensible Authentication Protocols (EAP) are used for authentication. Enterprise mode is applicable for WPA2 & WPA combination, WPA2, and WPA3.

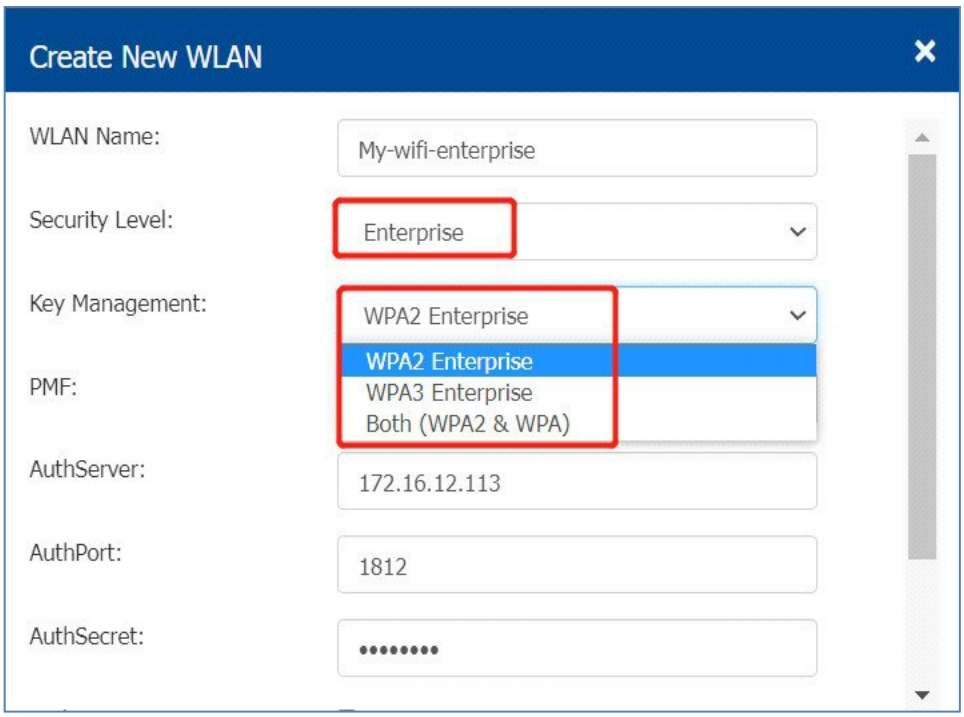


Figure 41:Create an enterprise type WLAN

- **WPA2-Enterprise:** WPA2-Enterprise is an authentication method for WPA2 which is mainly used for enterprise wireless networks for a higher security level. 4 handshakes are required between the client and the AP to establish a secure connection in this mode.
- **WPA3-Enterprise:** WPA3-Enterprise is designed specifically for enterprise-level users and scenarios that require a higher security protection, such as financial institutions, governments and enterprises, and can provide higher level of security than WPA2-Enterprise.
- **WPA3-Enterprise:** WPA3-Enterprise adds WPA3-Enterprise 192bit to WPA2-Enterprise as a more secure optional. This mode uses the 192-bit Suite-B security suite, enhancing password defense by increasing the key length to 192 bits from the 128-bit key length of WPA2-Enterprise. This means that even with a relatively simple password, it can effectively resist attacks such as offline brute force dictionary attacks, providing a higher level of protection for network users.

  In addition to the 192-bit encryption, WPA3-Enterprise has other security performance enhancements. For example, it uses WPS2 (Wi-Fi Protected Setup version 2) technology during handshake, which makes it less vulnerable to attacks like KRACK. It also places strict limits on the number of times a user can guess a password to prevent security risks like password cracking. WPA3-Enterprise also has the Easy Connect function, which simplifies the pairing process of smart home devices, and supports Enhanced Open to make device connections more secure and convenient. These features give WPA3-Enterprise greater capability in securing the network.
- **Both (WPA2 & WPA):** Both WPA and WPA2 are supported.

6.3 WLAN parameter description

Regarding different scenarios on the end customers, different configurable WLAN parameters are used for specific requirements. The parameter description in the Create New WLAN or Edit WLAN Information window is as follows.

- **PMF**

  DAP847-XXA supports the IEEE 802.11w standard, also known as PMF (Protected Management Frames). The PMF enhances the security of the DAP by providing data confidentiality of management frames. It is applicable to WPA2 and WPA3 encryption methods. In WLAN networks, management frames that are not encrypted can lead to security issues such as hackers stealing information in the management frame from communication between APs and users, and hackers impersonating APs or users to send fake requests to bring legitimate users offline. The PMF feature protects the management frames and a robust set of management frames against forgery and replay attacks.

  The PMF feature has two modes: the non-mandatory mode and the mandatory mode. In the non-mandatory mode, the terminal can access DAP847-XXA no matter it supports PMF or not. But DAP847-XXA only protects management frames of the terminals that support PMF. In the mandatory mode, DAP847-XXA only allows access from terminals that support PMF.

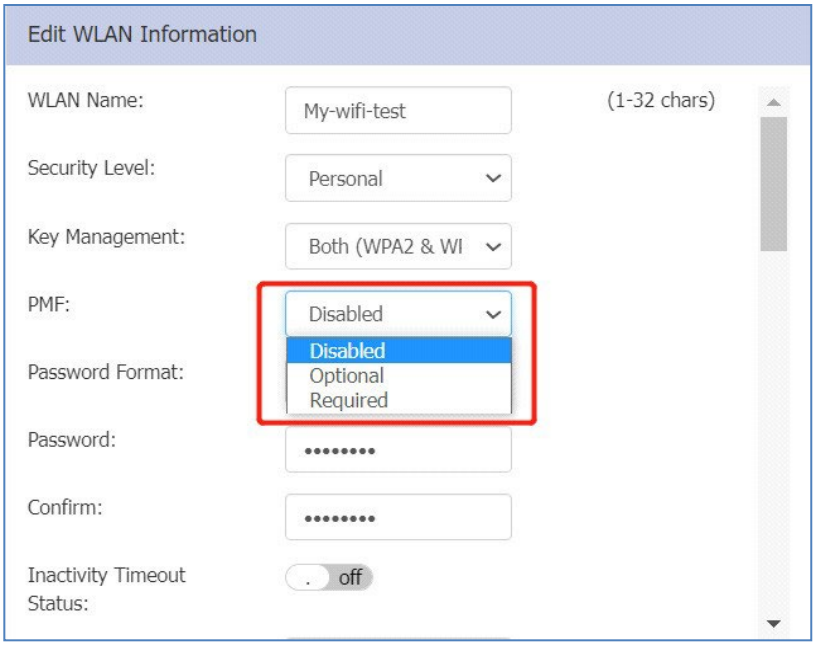


Figure 42: PMF settings for WLAN

Parameter	Description
Disable	Disables IEEE 802.11w PMF protection for WLAN. It is disabled by default.
Optional	Both IEEE 802.11w PMF capable clients and IEEE 802.11w PMF non-capable clients can connect to the SSID.
Required	Clients only support IEEE 802.11w PMF and can connect to the SSID.

Note: For WPA3 Enterprise authentication, PMF is forcefully set to **"Required"**. This means that only PMF-capable clients can be connected.

Inactivity Timeout

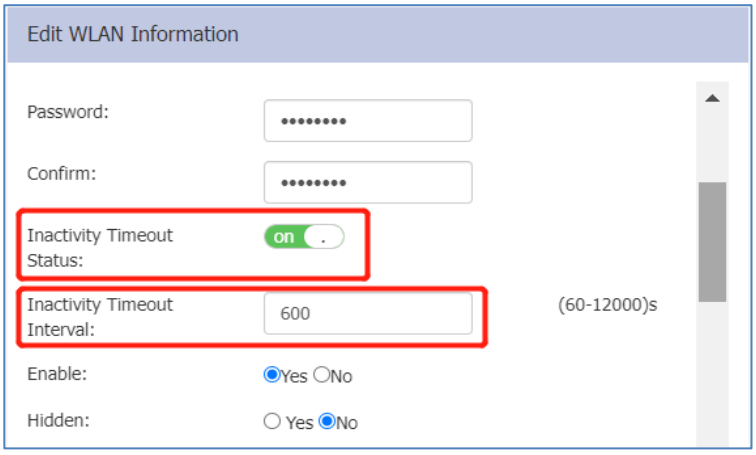


Figure 43: Inactivity timeout configuration

Parameter	Description
Inactivity Timeout Status	Specifies the inactivity timeout configuration status. This status is usually related to the activity status of the connected end device. Within a specific interval, if the end device does not communicate with the DAP847-XXA device, the DAP847-XXA device will consider the device to be in an inactive state. In this state, the connection of the wireless client device will be disconnected to save network resources.
Inactivity Timeout Interval	Specifies the inactivity timeout interval. The default value is 600 seconds and can be configured from 60 seconds to 12000 seconds.

Enable/Hidden

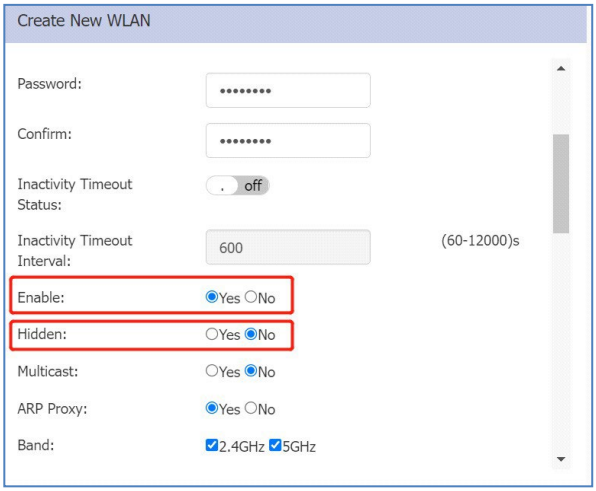


Figure 44: Enable and hidden WLAN

Parameter	Description
Enable	Specifies the WLAN state. Select **"Yes"** to broadcast the WLAN, while select **"No"** means WLAN is not applicable and not in the broadcast state.
Hidden	Specifies whether the WLAN is visible for the clients or not. For security reasons, some users can choose to hide the SSID so that the wireless network will not be searched and need to manually set the SSID to enter the corresponding network. Select **"Yes"** to ensure the WLAN is invisible to wireless clients, while select **"No"** to ensure it is visible.

One point to note is that while hiding the SSID improves the security level of the network, it also affects the accessibility of the network. Because once a wireless network is hidden, other devices cannot discover and connect to that network unless they already know the name and password of the network.

Multicast

That is, multicast to unicast. In wireless networks, multicast messages use the lowest rate to send broadcast messages, which consume relatively more air interface resources, thus affecting the performance and applications of the entire wireless network. Moreover, multicast messages are not confirmed at layer 2, which causes serious packet loss and affects video quality. After the multicast-to-unicast function is enabled, DAP847-XXA maintains multicast to unicast tables, by listening to the multicast report messages and leaving messages. When DAP847-XXA sends a multicast packet to the client, it converts the multicast data packet into a unicast data packet

according to the multicast-to-unicast table, thereby improving the efficiency of multicast data stream transmission.

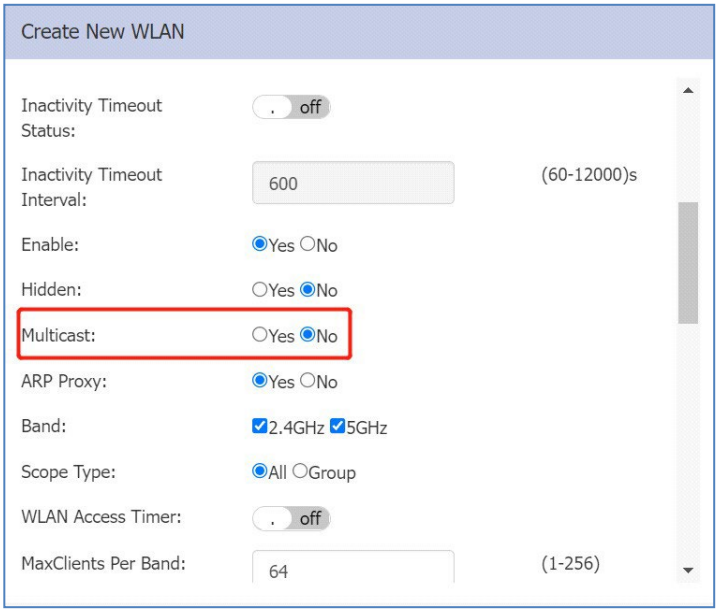


Figure 45: Multicast configuration

In addition, after the multicast-to-unicast adaptive function is turned on, when the air interface performance bottleneck occurs, DAP847-XXA automatically switches the multicast group with the smallest number of terminals to multicast mode. When the air interface performance has been improving for a period of time, DAP847-XXA automatically switches the multicast group with the largest number of terminals to unicast mode, ensuring that air interface performance is automatically adjusted without manual intervention and improving the overall wireless user experience.

ARP Proxy

ARP Proxy is a network technology commonly used in WLAN to solve the mapping problem of IP address and MAC address. If there is an ARP request from the wired side to the wireless client, DAP847-XXA responds to the request on behalf of the wireless client. Instead of forwarding ARP requests directly to the client, the purpose of this operation is to reduce the forwarding of ARP messages on the air interface to improve wireless performance.

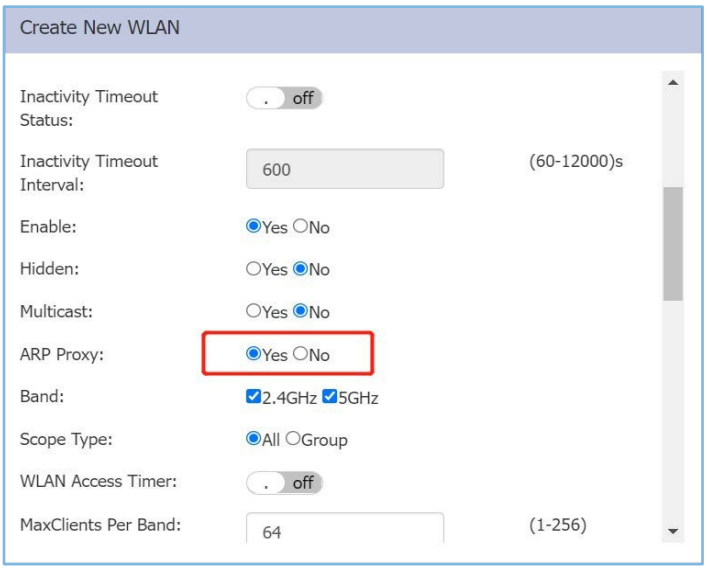


Figure 46: ARP proxy configuration

Note: The DAP847-XXA does not act as an ARP proxy for a gratuitous ARP. When a client obtains an IP address from the DHCP or DHCP release/renewal, it sends gratuitous ARP packets. DAP847-XXA does not respond to this special ARP packet, and broadcasts it normally.

- **Band:** Selects 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. By default, both options are selected.

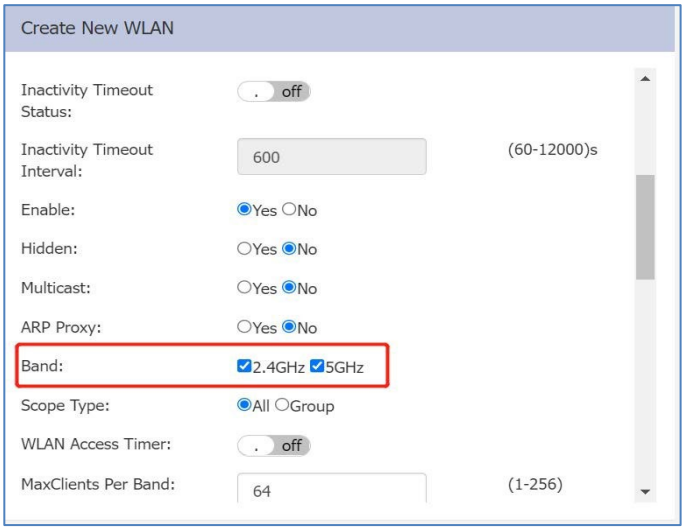


Figure 47: Band configuration

Scope Type

Specifies the scope of the DAP847-XXA devices in the cluster that can create the WLAN, that is, which DAP847-XXA devices will broadcast this WLAN.

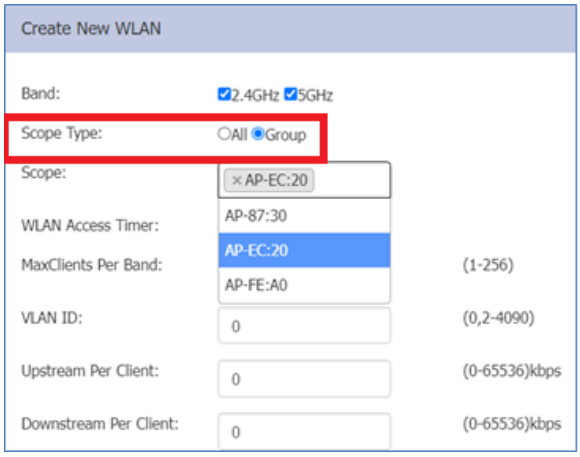


Figure 48: Scope type configuration

Parameter	Description
All	The WLAN configuration will be delivered to all the DAP847-XXA devices in the cluster.
Group	The WLAN configuration will be delivered to the selected DAP847-XXA group in the cluster.

WLAN Access Timer

Specifies the WLAN working period, during which DAP847-XXA only enables the WLAN. By default, the WLAN Access Timer is disabled. If it is disabled, the SSID will broadcast the activated WLAN, as shown in Figure 49. After it is configured, a timer icon displays before the WLAN, as shown in Figure 50.

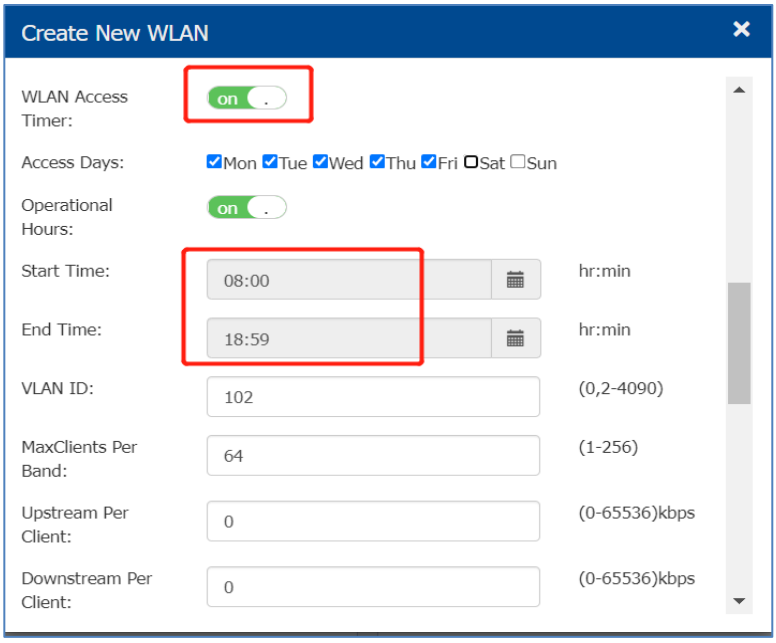


Figure 49: WLAN access timer configuration

Parameter	Description
Access Days	Activates or deactivates the days for broadcasting SSID per week.
Operational Hours	Enables or disables the time of the day in which broadcasting SSID.
Start Time	Specifies time to enable the WLAN.
End Time	Specifies time to disable the WLAN.

Note: Ensure that the system time and time zone are configured correctly before you configure the parameter. WLAN may not work as expected if the system time and time zone are not correct.

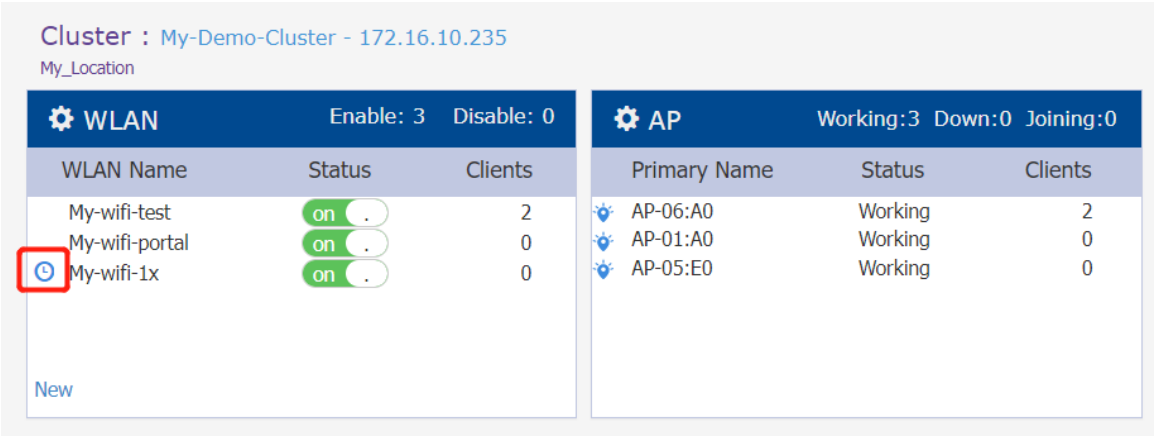


Figure 50: WLAN access timer indication

- **VLAN ID:** The VLAN identifier to which the WLAN is mapping is the traffic VLAN for wireless clients. If the WLAN-VLAN binding is configured, the DAP847-XXA will create a related bridge interface and handle relative traffic forwarding.

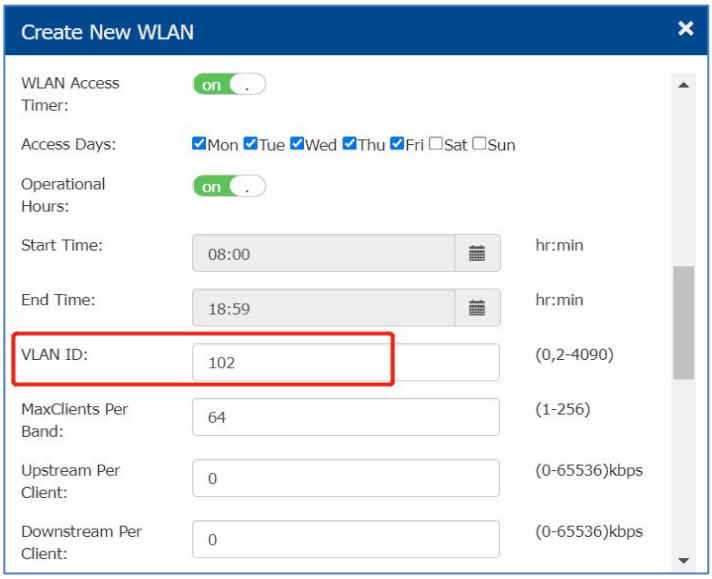


Figure 51: VLAN configuration

You can use the command "`brctl show`" to check the 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
                                                                ath102
                                                                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:~$
```

Figure 52: Checking VLAN configuration using command

- **MaxClients Per Band:** Specifies the maximum number of clients that can be configured for each BSSID on a WLAN. You can specify a value from 1 to 256. The default value is 64. When clients connected to the AP reach a maximum number, the DAP847-XXA ignores the authentication request from the new client and cannot connect to the SSID.

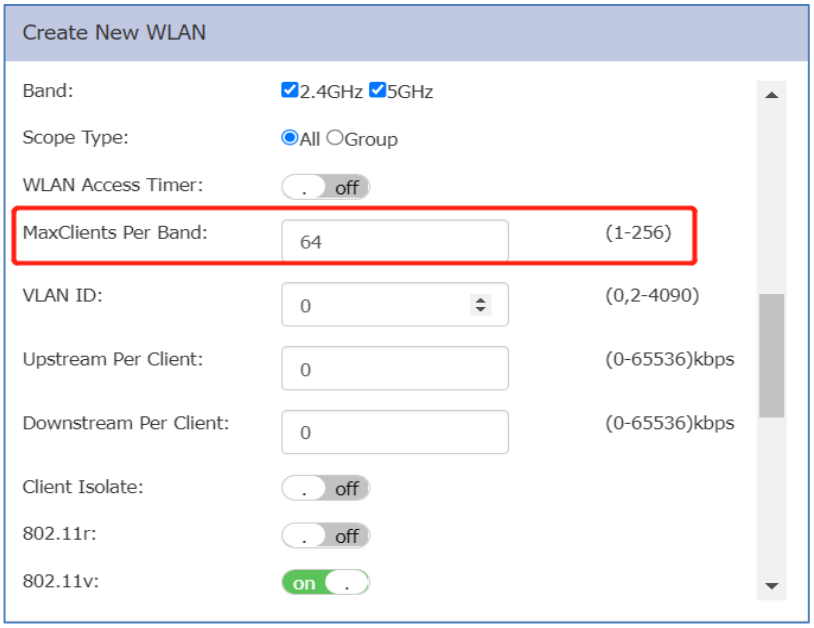


Figure 53: MaxClients per band configuration

- **Upstream Per Client:** Indicates the maximum uplink bandwidth of the configured wireless client, in kbps, and the configurable range is 0 … 65536, where 0 indicates that no client traffic speed limit is configured.
- **Downstream Per Client:** Indicates the maximum downlink bandwidth of the configured wireless client, in kbps, and the configurable range is 0 … 65536, where 0 indicates that no client traffic speed limit is configured.

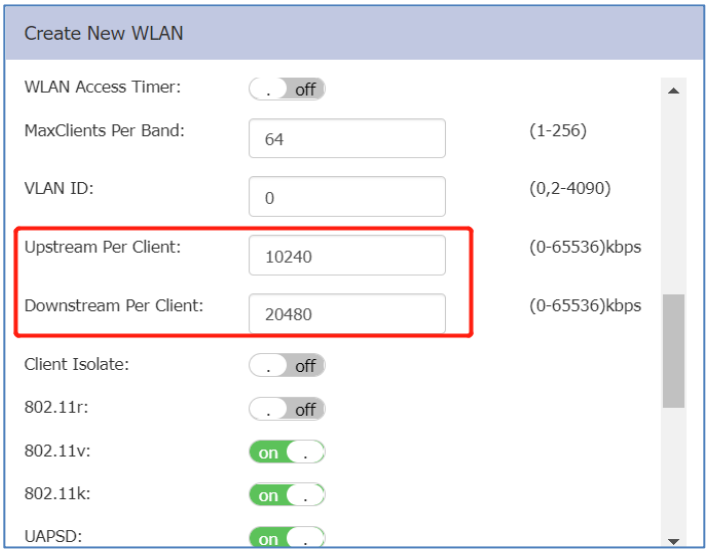


Figure 54: Clients traffic limitation configuration

- **Client Isolate:** Clients attached to the same WLAN are not allowed to communicate with each other. The clients can only communicate with the upstream gateway.

Figure 55: Client isolate

- **802.11r**

Enables Fast BSS Transition mechanism to minimize the delay when a client transits from one BSS to another in the same cluster.

Enabling Fast BSS Transition mechanism minimizes the delay when a client transitions from one BSS to another within the same Group. The IEEE 802.11r protocol proposes a three-layer key structure and computation method, while the traditional RSN (Robust Security Network, a wireless network security standard) has a two-layer key structure. RSN obtains GTK and PTK using the PMK shared by the authenticator (DAP847-XXA) and the applicant (wireless client). IEEE 802.11r, on the other hand, divides the key management into three layers: PMK_ R0, PMK_R1, and PTK. The computation of PMK_R0 and PMK_R1 is specific to IEEE 80211r. In addition, the IEEE 802.11r protocol reduces the time required for authentication during roaming, which helps support applications for real-time services such as voice service.

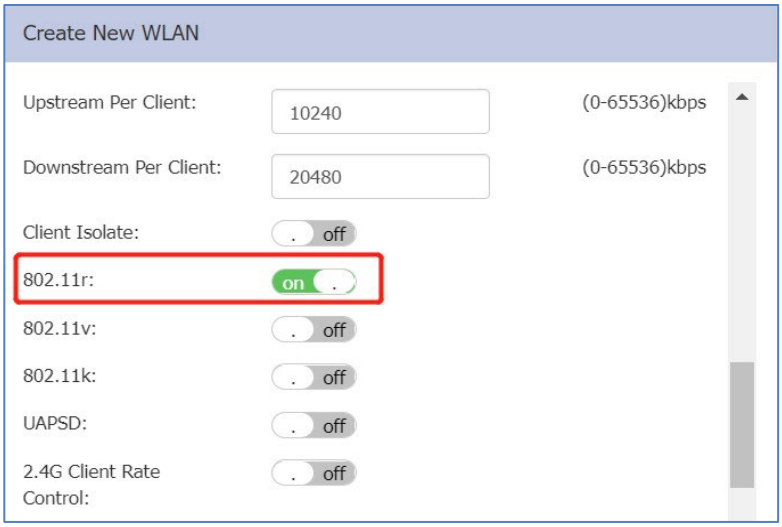


Figure 56: 802.11r configuration

- **802.11k/v:** By default, IEEE 802.11k or IEEE 802.11v are enabled. They both work together with “Roaming RSSI Threshold”. In practical applications, IEEE 802.11k/v can optimize the roaming performance and security of mobile devices in WLAN networks. The roaming optimization mainly depends on the client’s behavior during the roaming.

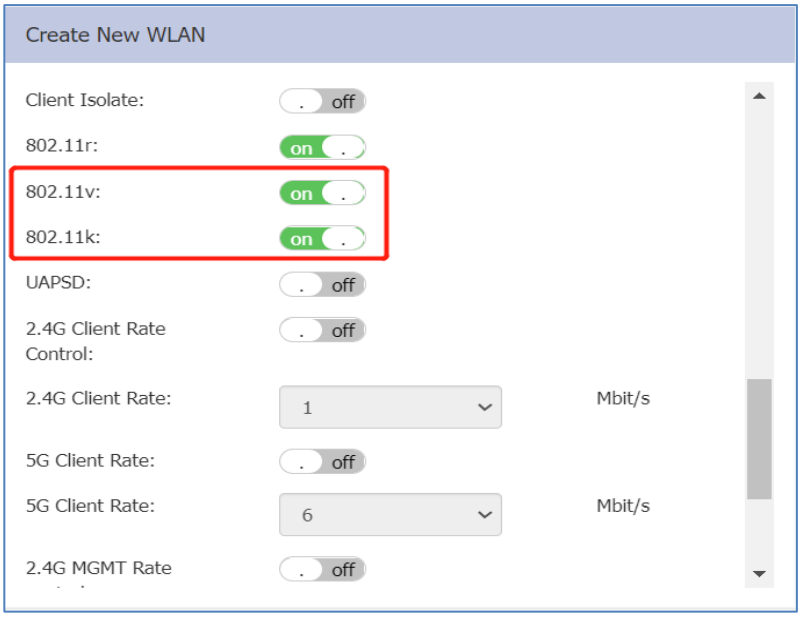


Figure 57: 802.11k/v configuration

  - When IEEE 802.11k or IEEE 802.11v is enabled on the SSID, “Roaming RSSI Threshold” is the trigger for IEEE 802.11k or IEEE 802.11v message exchanges between the DAP847-XXA and clients.

- When the DAP847-XXA detects that the SNR value of the device is lower than the “Roaming RSSI Threshold”, it sends an IEEE 802.11k event to this device. If the device is an IEEE 802.11k compliant device, it will respond to the DAP847-XXA with a packet that contains the RF scanned information from this device.
- Based on the data received, the DAP847-XXA will calculate what would be the best possible BSSID for this device to roam, and then send the best possible SSID information to this device with the IEEE 802.11v event.
- Finally, the device will choose whether to roam or not. If the device roams, it will decide if it takes the BSSID from the DAP847-XXA in the IEEE 802.11v event or another BSSID to roam that the AP cannot manage.

OKC

Enables OKC to use a cached Pairwise Master Key (PMK) when the client roams to a new AP. This ensures clients roam faster and eliminates the need for a complete IEEE 802.1x authentication procedure.

OKC mainly addresses the network latency and performance issues caused by frequent IEEE 802.1X authentication during fast roaming. It enables faster connection between devices and new APs during roaming by caching PMKs between devices. When a wireless client (Station) connects to a new AP and the AP supports OKC, STA calculates a new PMK and stores it in the PMKSA Cache based on the SSID of the AP and the PMKs that have been cached before. In the next connection, the STA can directly use this cached PMK without needing another IEEE 802.1X authentication.

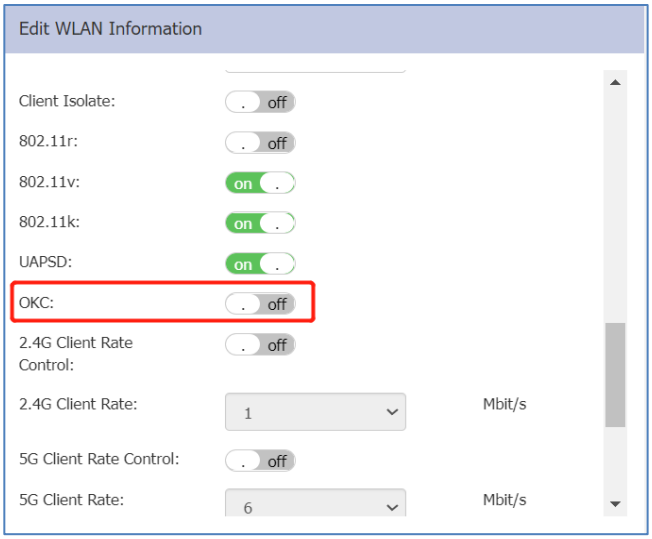


Figure 58: OKC configuration

- **UAPSD**: Unscheduled Automatic Power Save Delivery (UAPSD) defines the Quality of Service (QoS) facility in IEEE 802.11e that extends the battery life of mobile clients. Additionally, it reduces the latency of traffic flow delivered over wireless media, while extending the battery life. UAPSD does not need the client to poll each individual packet buffered at the DAP847-XXA. It ensures the delivery of multiple downlink packets by sending a single uplink trigger packet.

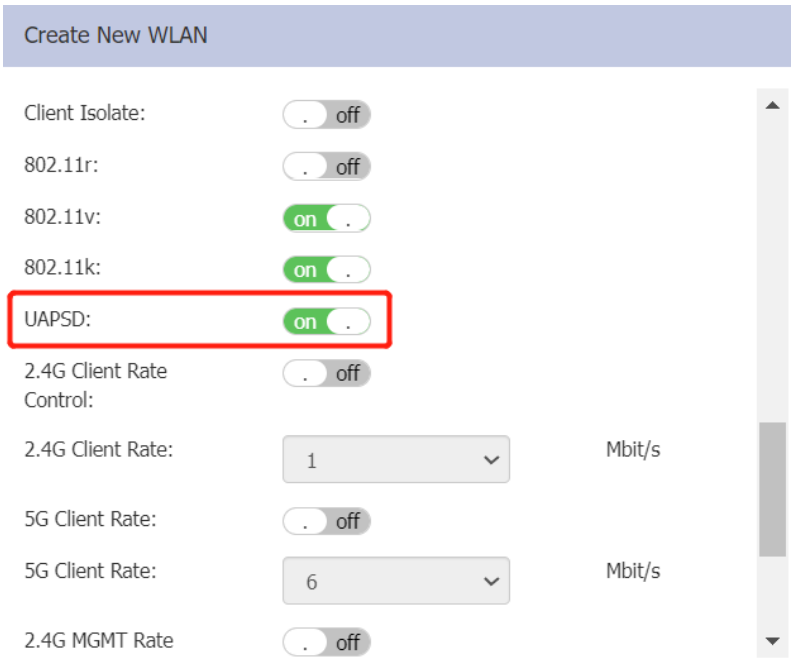


Figure 59: UAPSD configuration

- **2.4G Client Rate Control**: Enables or disables the 2.4 GHz band access control based on the client data rate as shown in Figure 60. It is disabled by default.
- **2.4G Client Rate**: 2.4 GHz band clients with lower data speed will not be allowed to access. The recommended value is 12 Mbit/s, as shown in Figure 60. The main purpose of data frame rate control is to optimize the performance and stability of WLAN. If the sending rate of management frames is too low, it may cause excessive interference and congestion, affecting WLAN performance and stability.
- **5G Client Rate Control**: Enables or disables the 5 GHz band access control based on the client data rate, as shown in Figure 60. It is disabled by default.
- **5G Client Rate**: 5 GHz band clients with lower data speed will not be allowed to access the DAP847-XXA. The recommended value is 24 Mbit/s, as shown in Figure 60. The main purpose of data frame rate control is to optimize the performance and stability of WLAN. If the sending rate of management frames is too low, it may cause excessive interference and congestion, affecting WLAN performance and stability.

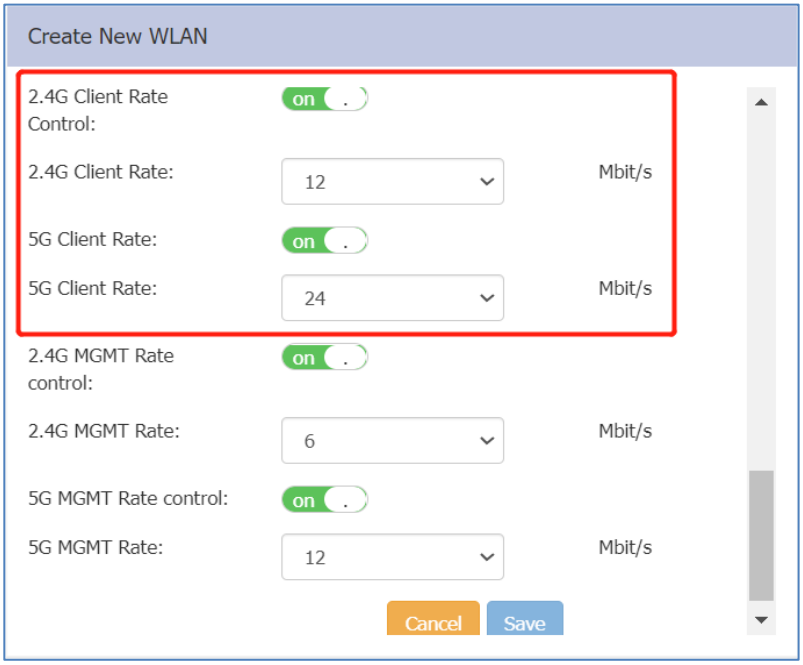


Figure 60: Client rate configuration

- **2.4G MGMT Rate Control**: Enables or disables the 2.4 GHz band wireless management frame rate control, as shown in Figure 61. It is disabled by default.

- **2.4G MGMT Rate**: The transmit rate of the 2.4 GHz band wireless management frame is shown in Figure 61. A higher value means less coverage, and a lower value means larger coverage. The main purpose of managing frame rate control is to optimize WLAN performance and stability. If the sending rate of management frames is too low, it may cause excessive interference and congestion, affecting WLAN performance and stability.

- **5G MGMT Rate Control**: Enables or disables the 5 GHz band wireless management frame rate control, as shown in Figure 61. It is disabledby default.

- **5G MGMT Rate**: The transmit rate of the 5 GHz band wireless management frame is shown in Figure 61. A higher value means less coverage, and a lower value means larger coverage. The main purpose of managing frame rate control is to optimize WLAN performance and stability. If the sending rate of management frames is too low, it may cause excessive interference and congestion, affecting WLAN performance and stability.

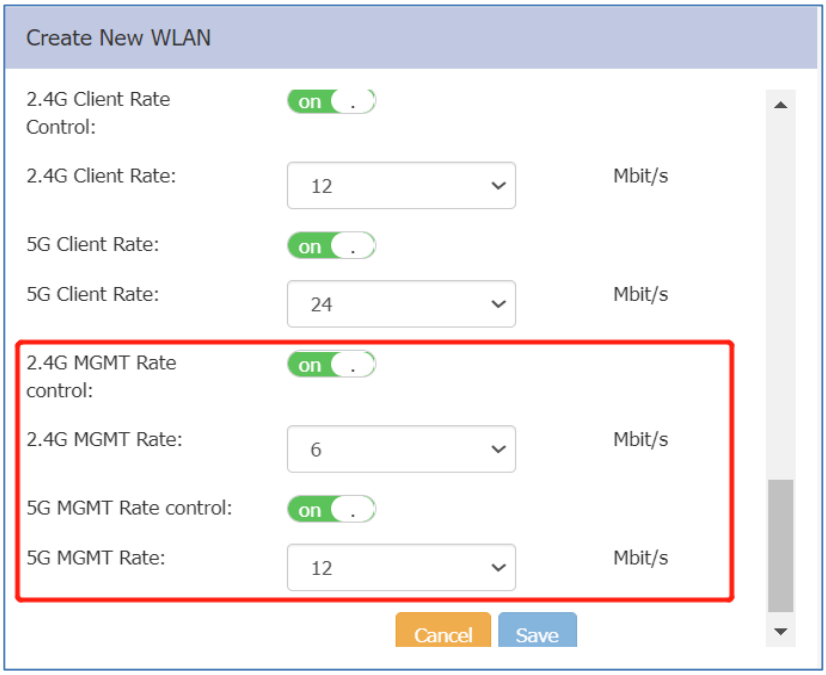


Figure 61: Management rate configuration

- **DTIM Interval:** The time interval at which the DAP847-XXA sends a DTIM (Delivery Traffic Indication Message) to notify wireless clients when data is available for reception. This prevents client devices from remaining unnecessarily awake when no data needs to be received. Increasing the DTIM Interval can conserve battery life of terminal devices more effectively, but it will increase the access point's buffer usage and introduce transmission delays. Therefore, the DTIM interval should be correctly set according to the actual usage scenario. By default, the DTIM interval parameter is set to 1, as shown in Figure 62.

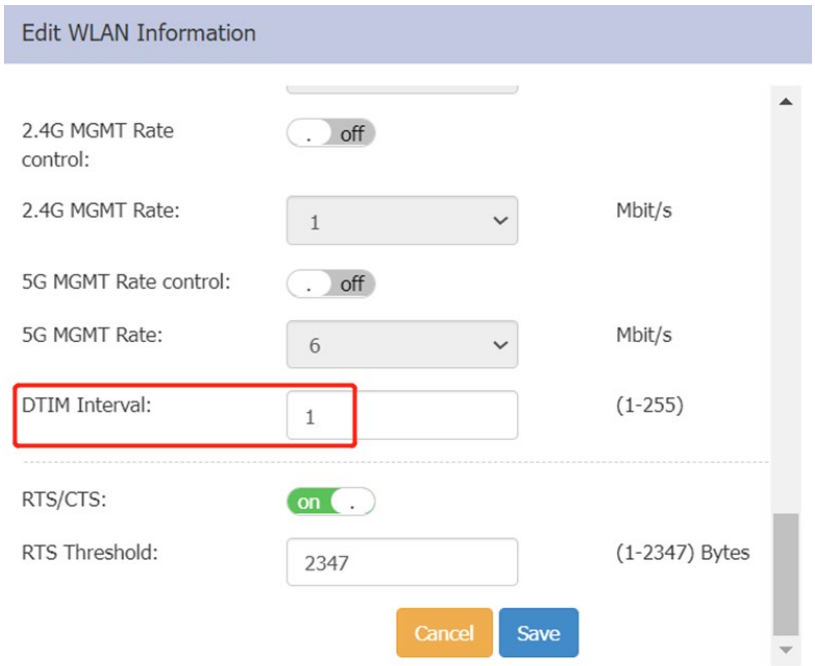


Figure 62 DTIM Interval configuration

- **RTS/CTS:** When enabled, the DAP847-XXA will send RTS (Request to Send) and CTS (Clear to Send) frames. This helps identify hidden nodes within the network, thereby reducing packet collisions caused by hidden nodes. Such collisions can lead to increased packet retransmissions or packet loss. Refer to Figure 63 for specific configuration.

- **RTS Threshold:** The configurable range for this parameter is 1 … 2347 bytes. By default, this feature is disabled. When the DAP847-XXA needs to send a data packet exceeding this threshold, it first sends an RTS signal to notify the receiver, as a precaution against signal collisions. Refer to Figure 63 for specific configuration.

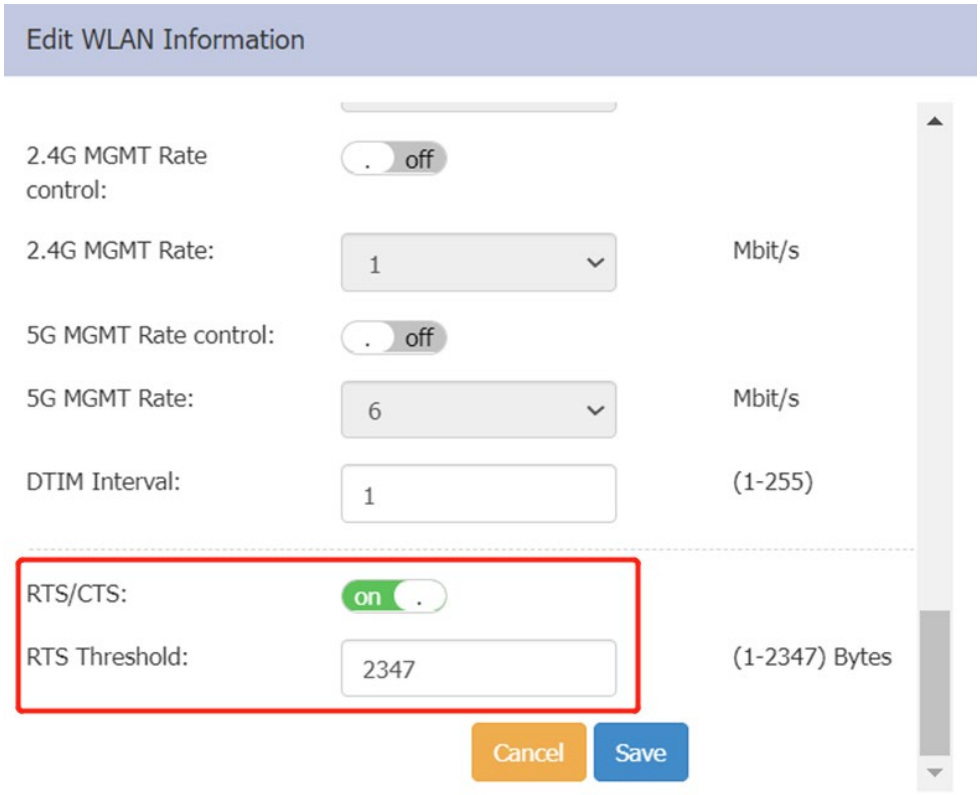


Figure 63 RTS/CTS Configuration

6.4 Modify WLAN configuration

In the WLAN Configuration window, you can modify the WLAN settings by clicking the "✎" button. The configurable WLAN parameters are shown on the right side of the WLAN Configuration window.

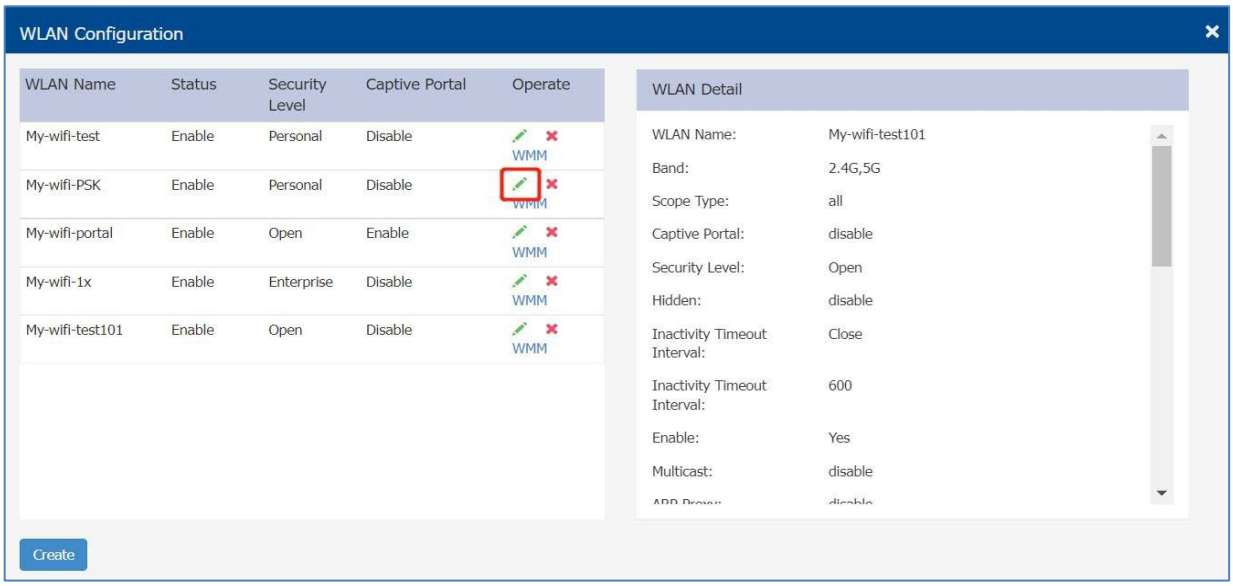


Figure 64: Modify WLAN configuration

- ☐ To cancel the modification, click the **"Cancel"** button.
- ☐ To save the modification, click the **"Save"** button.

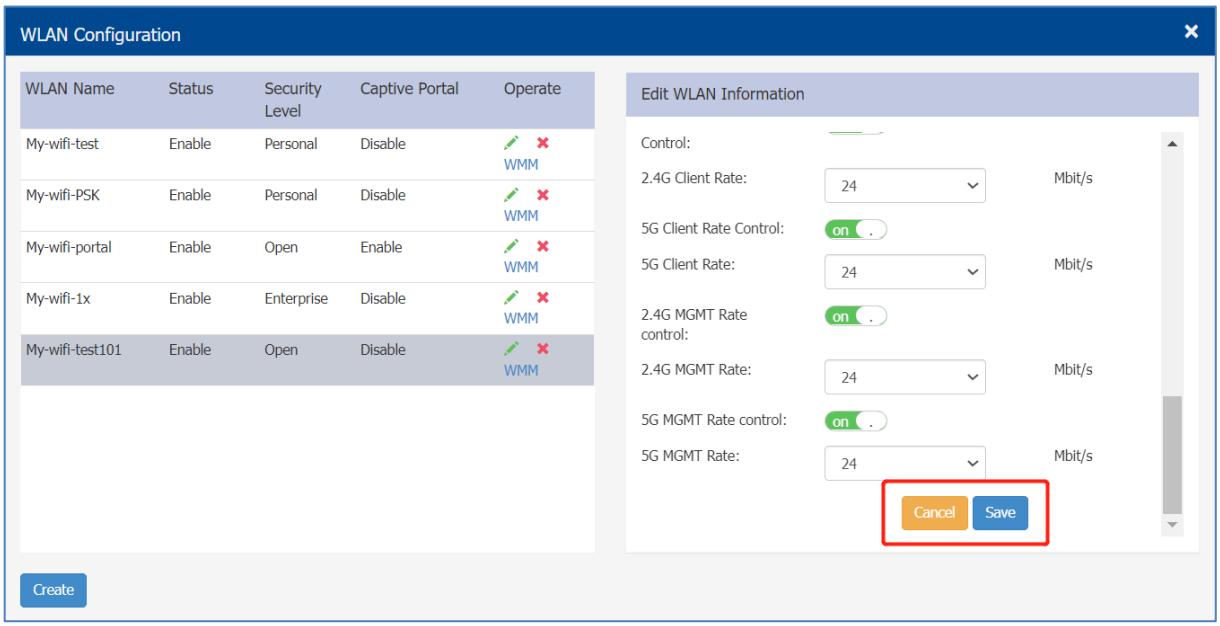


Figure 65: Update the configuration

6.5 Delete a WLAN

In the WLAN Configuration window, click the "✖" button to delete a WLAN.

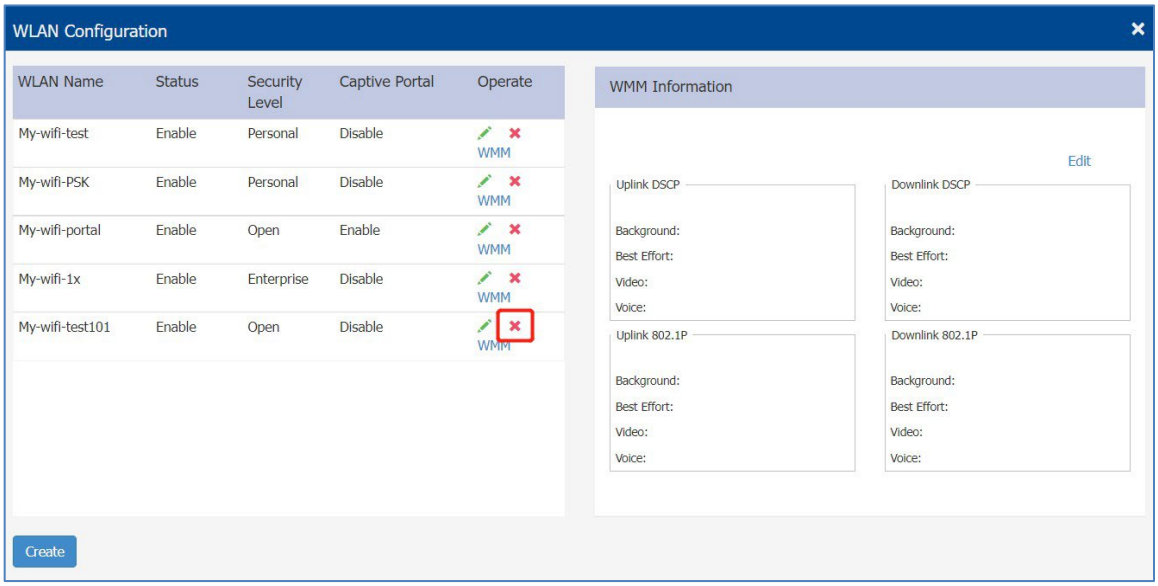


Figure 66: Delete WLAN configuration

6.6 WMM configuration

The WMM (Wi-Fi Multimedia) is a Wi-Fi alliance interoperability certification based on the IEEE 802.11e standard. It provides the basic QoS features for IEEE 802.11 networks. It is suitable for well-defined applications that require QoS, such as Voice over IP (VoIP) on Wi-Fi phones. WMM ensures smooth transmission of high-bandwidth applications such as voice, video, and gaming without network congestion. WMM prioritizes traffic and data transmission according to 4 Access Categories (AC): voice (AC_VO), video (AC_VI), best effort (AC_BE), and background (AC_BK):

- **Background:** Used for transmitting background data such as email, web browsing, etc. The priority is the lowest.
- **Video:** Used for transmitting video streams, such as online movies or video conferences. The priority is higher than Background.
- **Voice:** Used for transmitting video streams, such as VoIP calls or voice calls. The priority is higher than Background.
- **Best Effort:** Used for transmitting all other data, such as files, online games, etc. The priority is the highest.

WMM classifies and marks data by using WMM markers to prioritize it before sending it to the network. At the receiving end, WMM markers are used to identify the priority of the packet so that it can be delivered correctly to the appropriate applications.

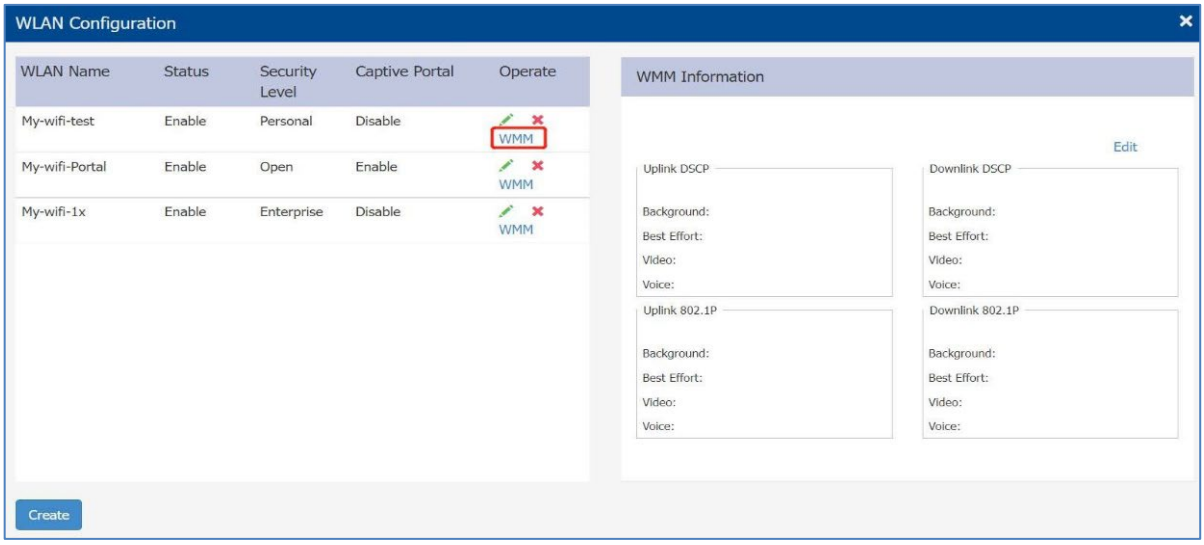


Figure 67: WMM Configuration

Each WLAN can configure WMM rules. For the WLAN on DAP847-XXA, you can modify the values of DSCP and IEEE 802.1p, and the mapping relationship among priorities.

7 DAP847-XXA Management

This chapter describes how to configure and manage DAP847-XXA devices in the cluster, and how to check, back up, restore AP configurations, and upgrade firmware via Web GUI. The DAP847-XXA cluster solution is a controller-less-based architecture.

The DAP847-XXA can establish an autonomous cluster, in which there are 3 types of AP roles: PVM, SVM, and MEMBER. This chapter describes how to manage the cluster and DAP847-XXA Management procedures described in this chapter include the following:

- Check detailed information
- Modify the DAP847-XXA name and location
- Add a new DAP847-XXA to a cluster
- Remove a DAP847-XXA from a cluster
- Allow a DAP847-XXA to join a cluster
- Replace an DAP847-XXA in a cluster
- Modify DAP847-XXA IP address
- Convert DAP847-XXA to DAC mode
- Check DAP847-XXA current configuration
- Reboot the DAP847-XXA
- Clear all configuration
- Backup and restore configuration
- Upgrade the DAP847-XXA firmware
- Configure the LED
- DAP847-XXA advanced configuration
- Configure DAP847-XXA network service

7.1 Check detailed information

You can view the detailed DAP information in the right window of the DAP847-XXA configuration page by clicking the related DAP item. You can modify the **AP Name** and **Location** by clicking “Edit” on this page.

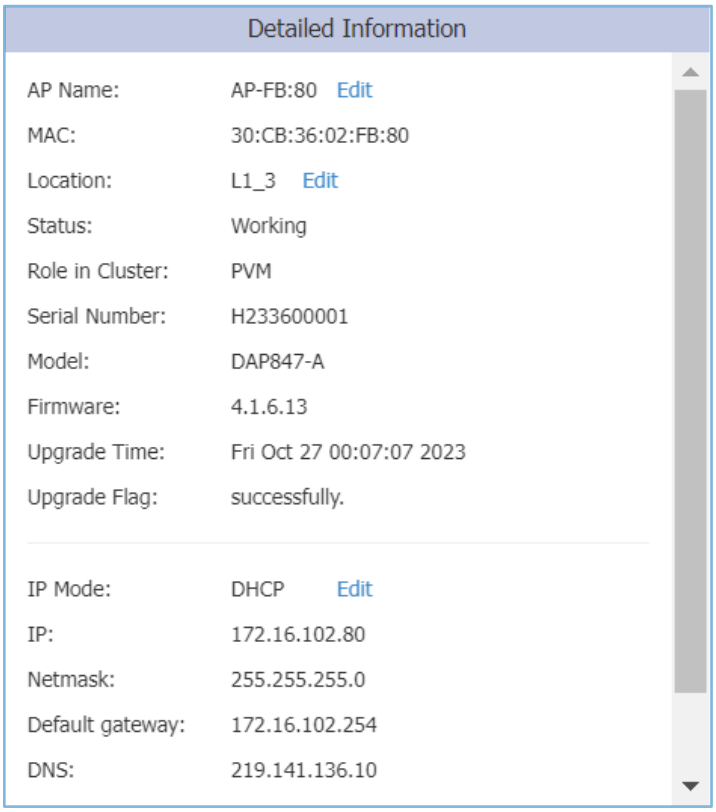


Figure 68: DAP847-XXA detailed information

7.2 Modify the DAP847-XXA name and location

- ☐ Click the "**Edit**" icon to modify the AP name and location.
- ☐ Enter the **"AP Name"** or **"Location"** field to identify the specific DAP847-XXA. By default, the DAP847-XXA is named with the "AP-" character and the last 2 bytes of its MAC address, for example, AP-DB:80.

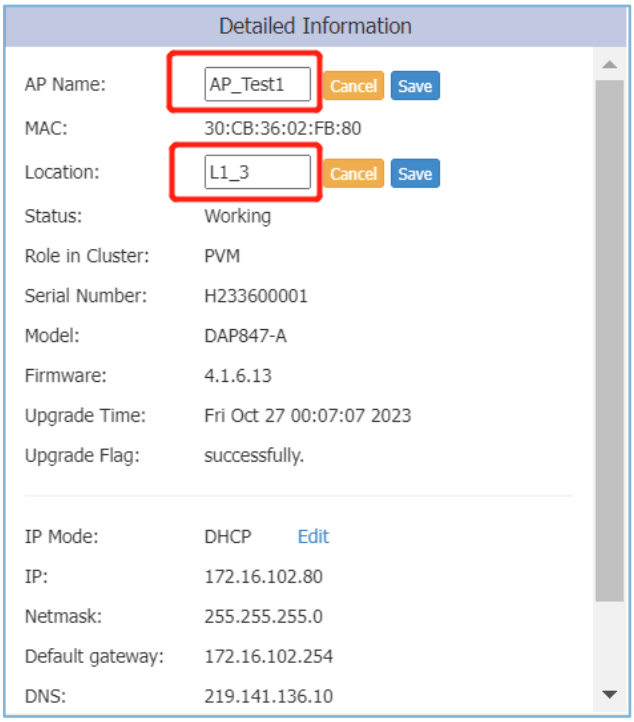


Figure 69: Modify name and location

7.3 Add a new DAP847-XXA to a cluster

Prerequisite

Before adding a new DAP847-XXA to a cluster, ensure the following:

- The PVM is in normal working condition.
- Newly added DAP847-XXA should use the cluster ID same as the cluster.

Note: If you want to add a new DAP847-XXA to the cluster, connect the AP to the same Layer 2 network as the cluster. Meanwhile, ensure that the AP can communicate with other APs, meaning there is no isolation between the AP and the APs in the cluster.

If the PVM cannot be operated, please upgrade the SVM to the PVM before adding a new DAP847-XXA.

Check the **"Cluster ID"** information in the following 2 ways:

- Log in to the DAP847-XXA and check the **"Cluster ID"** in the System window.

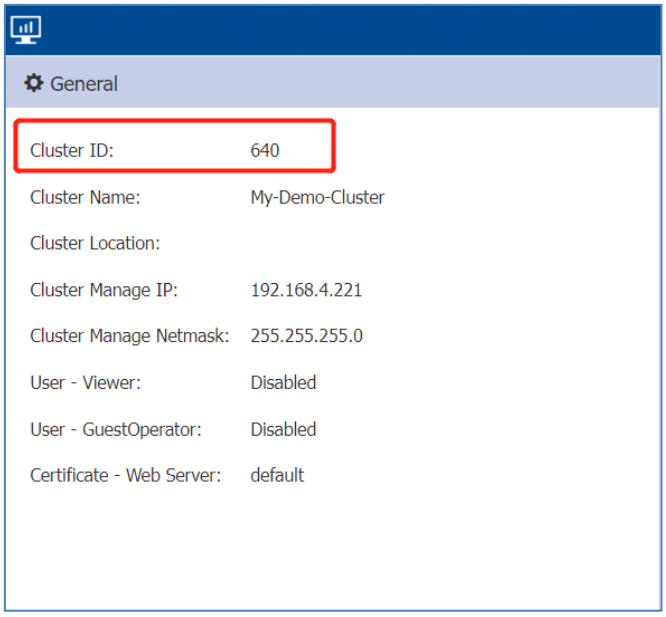


Figure 70: Check Cluster ID via GUI

- Check the Cluster ID information using the CLI.

```
support@AP_Test1:~$
support@AP_Test1:~$
support@AP_Test1:~$ cat /var/config/cluster.conf
{
        "cluster":{
                "cluster_id":"1869",
                "cluster_name":"AP-Group",
                "cluster_priority":"0"
        }
}
support@AP_Test1:~$
support@AP_Test1:~$
support@AP_Test1:~$
```

Figure 71: Check Cluster ID using the CLI

7.4 Remove a DAP847-XXA from a cluster

- ☐ Select a DAP847-XXA to be removed from the AP cluster list (PVM, SVM, or MEMBER).
- ☐ Click the **"Kick Off"** button. the DAP847-XXA will be dropped into the cluster blocklist.

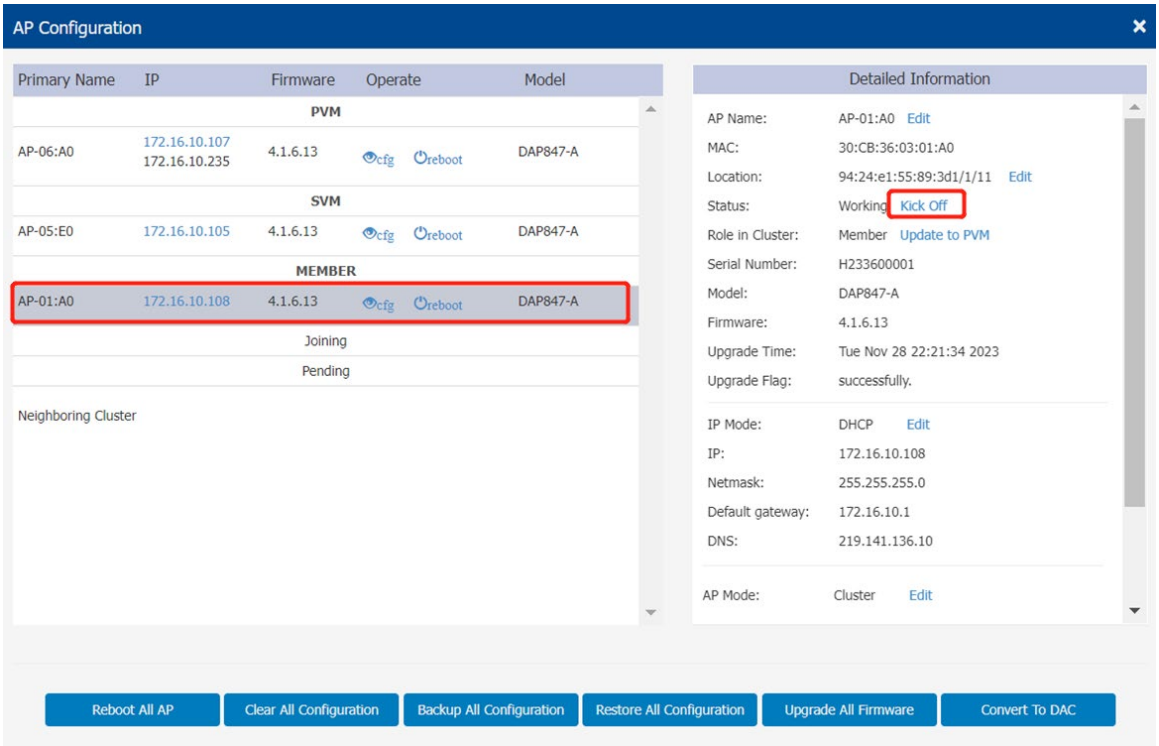


Figure 72: Kick off an DAP847-XXA in the cluster

If the DAP847-XXA is connected to the network, the status of the DAP847-XXA will switch from the "**Working**" state to the **"Joining"** state. Without the administrator's authorization, the DAP847-XXA device is not allowed to join the cluster again and become a member of the cluster.

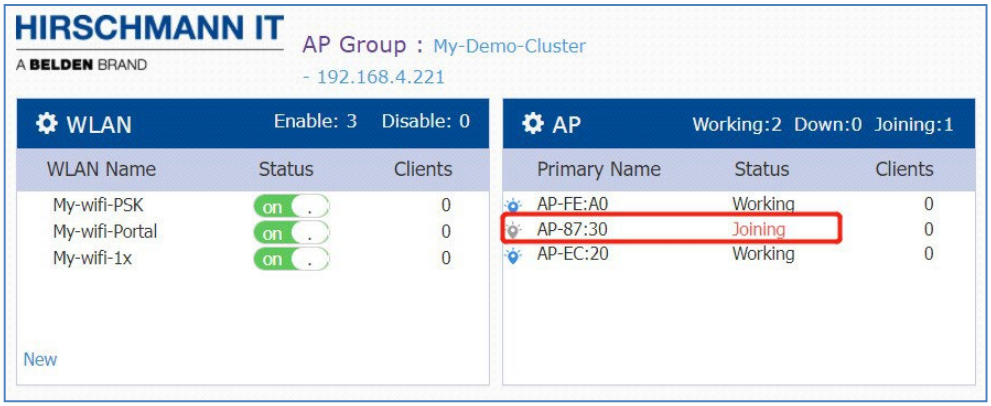


Figure 73: DAP847-XXA in "Joining" state after kicked off

7.5 Allow a DAP847-XXA to join a cluster

If a DAP847-XXA in the “**Joining**” state is in the cluster block list, clicking the “**Accept**” button and the corresponding “**Cluster ID**” will allow the DAP847-XXA to rejoin the cluster and remove it from the cluster blocklist.

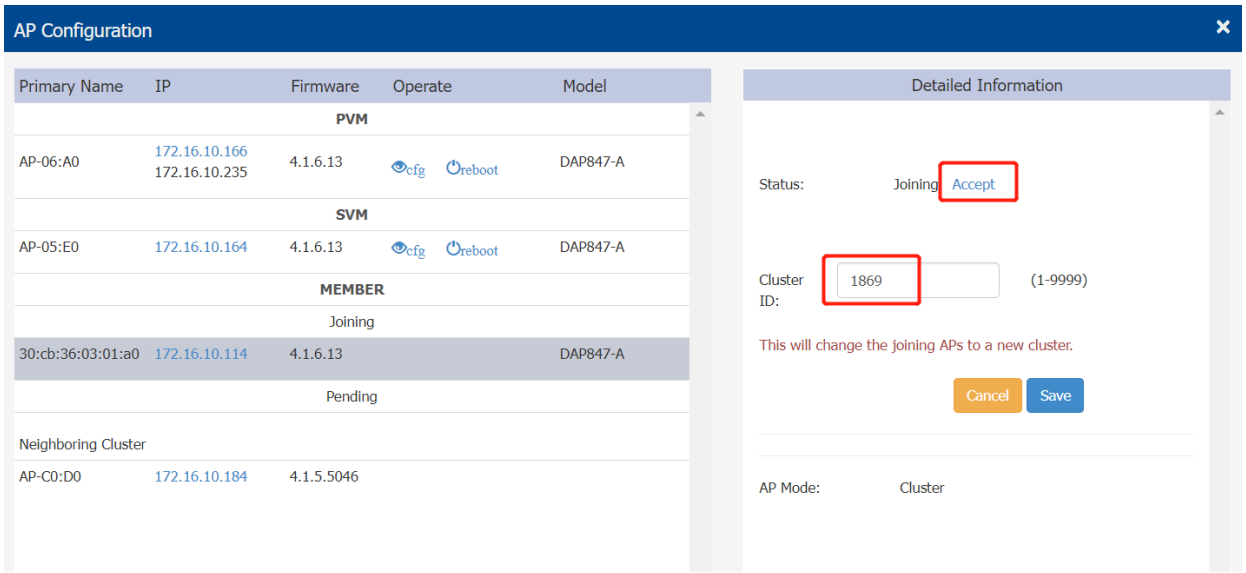


Figure 74: Allow DAP847-XXA to rejoin the cluster

7.6 Replace an DAP847-XXA in a cluster

Replace a DAP847-XXA in the cluster in the following cases:

- **Replace the current PVM:**

  Upgrade the SVM to the PVM before disconnecting the former PVM. Then replace the former PVM with a new DAP847-XXA.

- **Replace the SVM or a MEMBER of the cluster:**

  Disconnect and replace the SVM or MEMBER directly with a new DAP847-XXA.

7.7 Modify DAP847-XXA IP address

DAP847-XXA supports obtaining an IP address from a DHCP server and also supports configuring a static IP address. By default, the IP mode is DHCP.

- ☐ Click the **"Edit"** button to modify the IP mode. See Figure 75 and Figure 76.

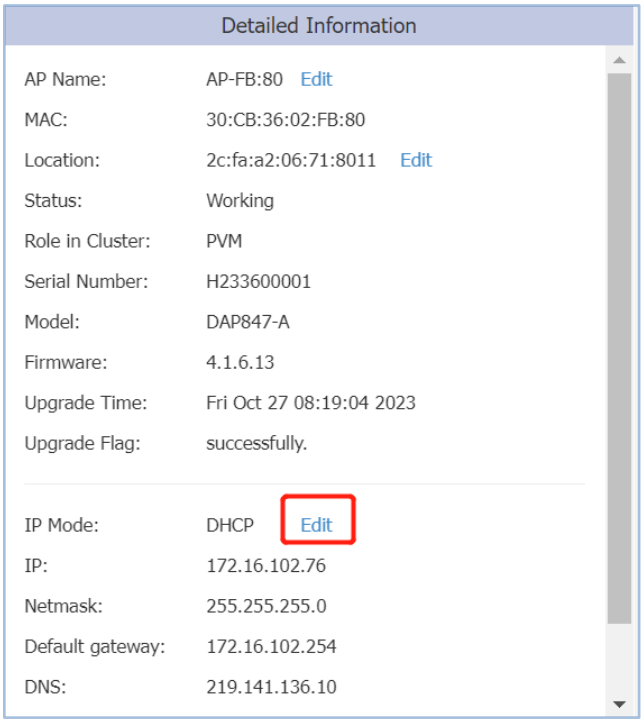


Figure 75: Edit DAP847-XXA IP mode

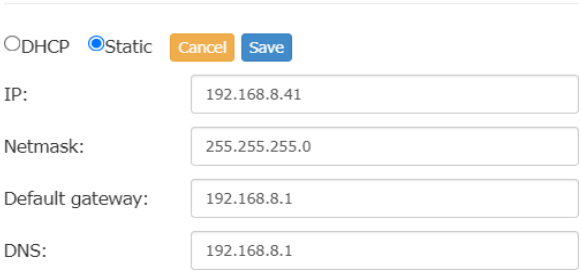


Figure 76: Modify DAP847-XXA IP address

7.8 Convert DAP847-XXA to DAC mode

According to actual requirements, DAP847-XXA can convert from cluster mode to DAC mode on the web GUI.

Convert a single DAP847-XXA to the DAC mode:

- Select a DAP847-XXA on "**AP Configuration**" page. Click the "**Edit**" button on the detailed information page.

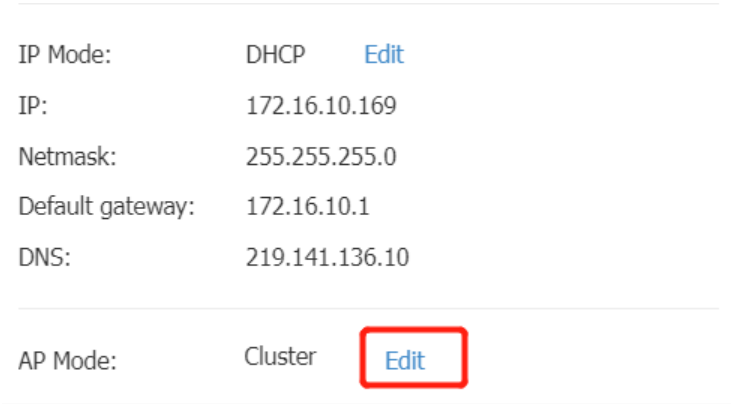


Figure 77: Edit AP mode

- Select the "**DAC**" option.

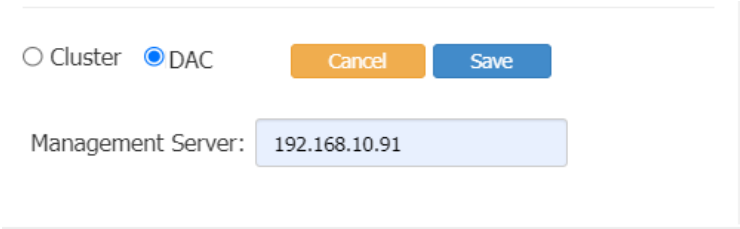


Figure 78: Configure DAC mode

- Enter the DAC IP address and save the configuration.

After the DAP847-XXA reboots, the specific single DAP847-XXA in the cluster switches to the DAC mode.

Convert all DAP847-XXA devices in the cluster to the DAC mode:

- Click the **"Convert To DAC"** at the bottom of the right-hand corner on the AP Configuration page.

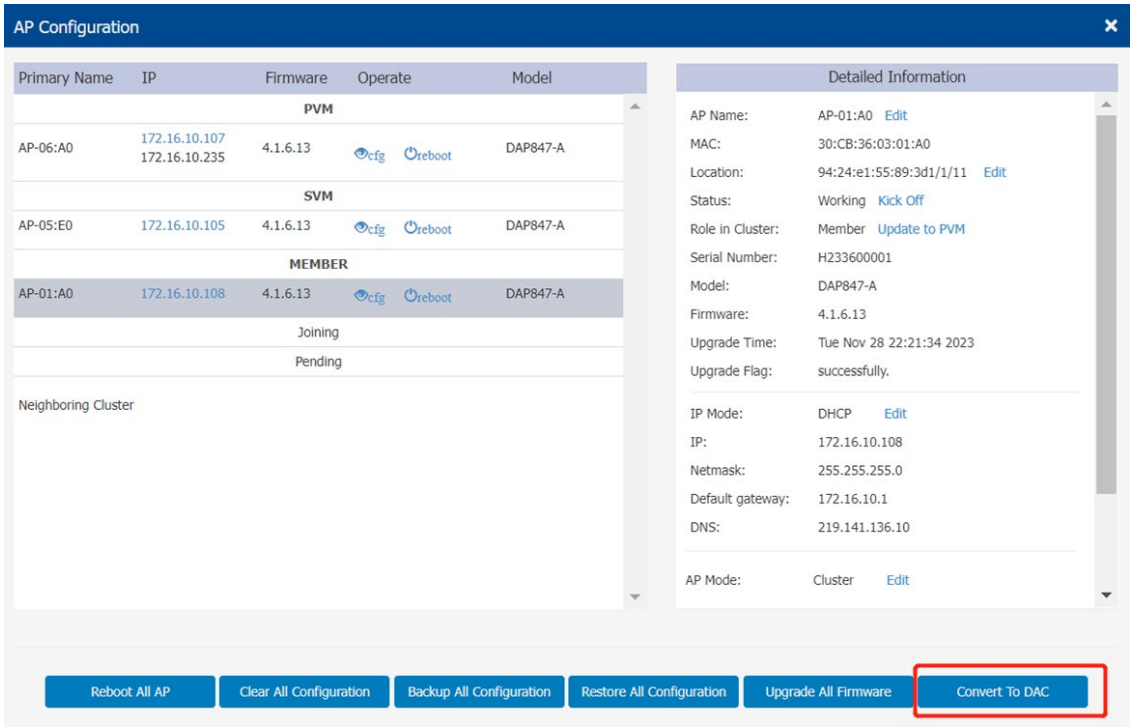


Figure 79: Convert to DAC

☐ Enter the DAC IP address and save the configuration.

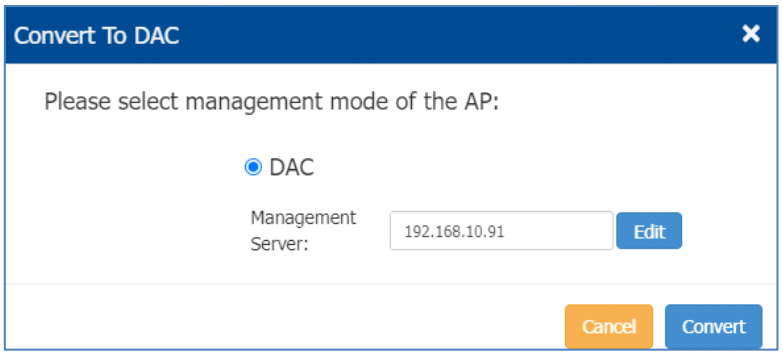


Figure 80: Configure DAC mode

After the DAP847-XXA reboots, every DAP847-XXA in the cluster switches into the DAC mode.

Note: After the DAP switches to the DAC mode, the configuration under the cluster mode gets cleared. The DAP847-XXA will get a new configuration from DAC.

7.9 Check DAP847-XXA current configuration

In the DAP847-XXA list, click cfg and you can view the current configuration information of DAP847-XXA as shown in Figure 81.

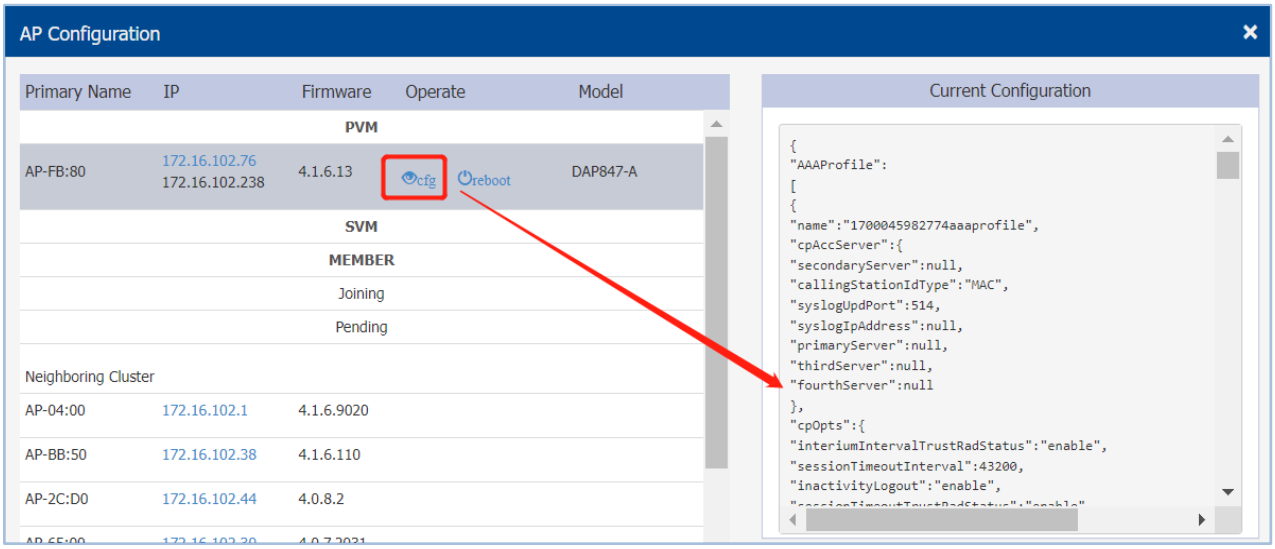


Figure 81: Check DAP847-XXA current configuration

7.10 Reboot the DAP847-XXA

DAP847-XXA supports manual reboot by your actual requirements.

Reboot a single DAP847-XXA in the cluster

- Select one DAP847-XXA, and click reboot to reboot it in the AP Configuration window.

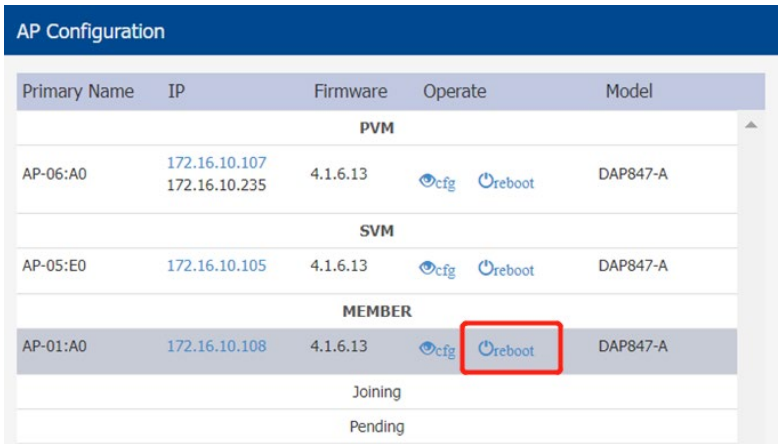


Figure 82: Reboot an AP in Cluster

Reboot all DAP847-XXA devices in the cluster

- Click the **"Reboot All AP"** button at the bottom left-hand corner of the AP Configuration window. All the DAP847-XXA devices in the cluster will reboot.

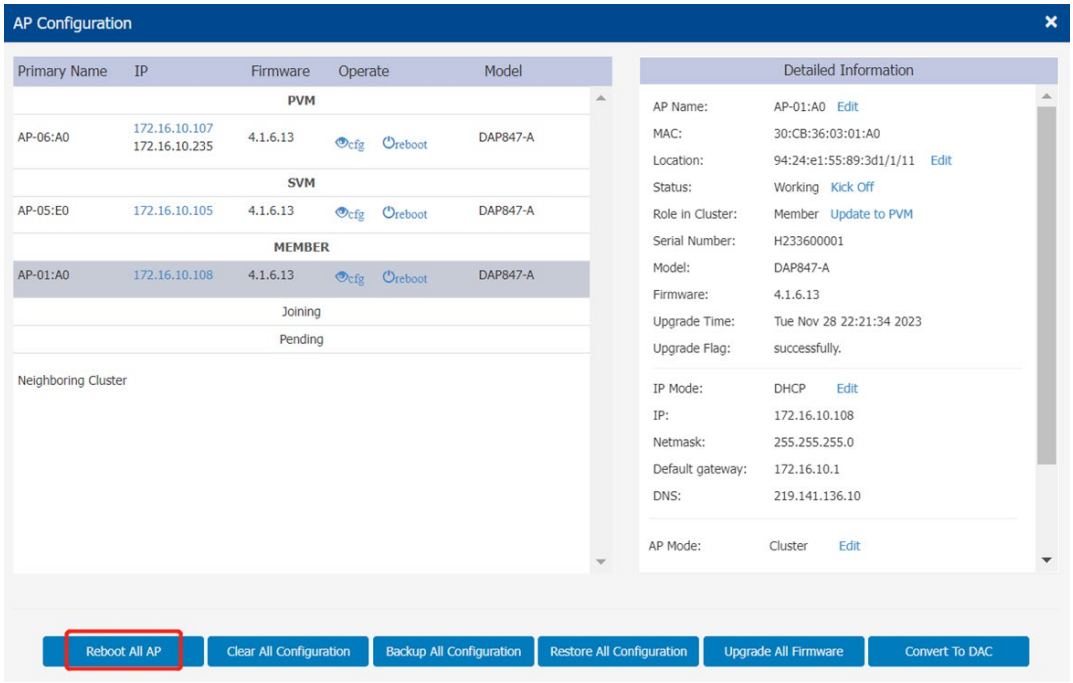


Figure 83: Reboot all DAP847-XXA devices in the Cluster

7.11 Clear all configuration

Click the **“Clear All Configuration”** button in the AP Configuration window to clear the configuration of all DAP847-XXA devices and restore it to the **“factory setting”**.

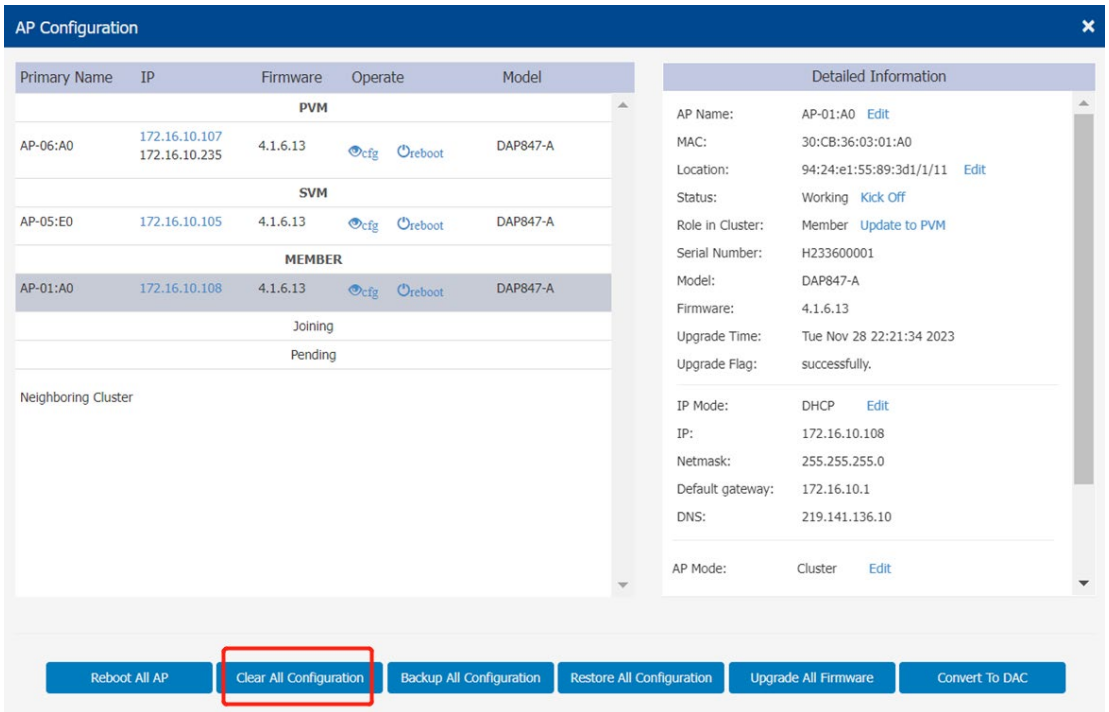


Figure 84: Clear all configuration

Note: In addition, there are the following two ways to restore DAP847-XXA to “factory settings”:

- Long press the **“reset”** button for at least 6 seconds.
- In CLI mode, enter commands **“**`ssudo firstboot`**”** and **“**`ssudo reboot`**”** to restore to “factory settings” (default account/password: support\Belden996!@#).

7.12 Backup and restore configuration

In the AP Configuration window, you can back up and restore the cluster configuration.

- ☐ Click the **"Backup All Configuration"** button at the bottom of the AP Configuration window to download the configuration file. The default name of the configuration file is "`pub-config.tar`".
- ☐ Click the **"Restore All Configuration"** button at the bottom of the AP Configuration window to restore the configuration file. The default name of the configuration file is "`pub-config.tar`".

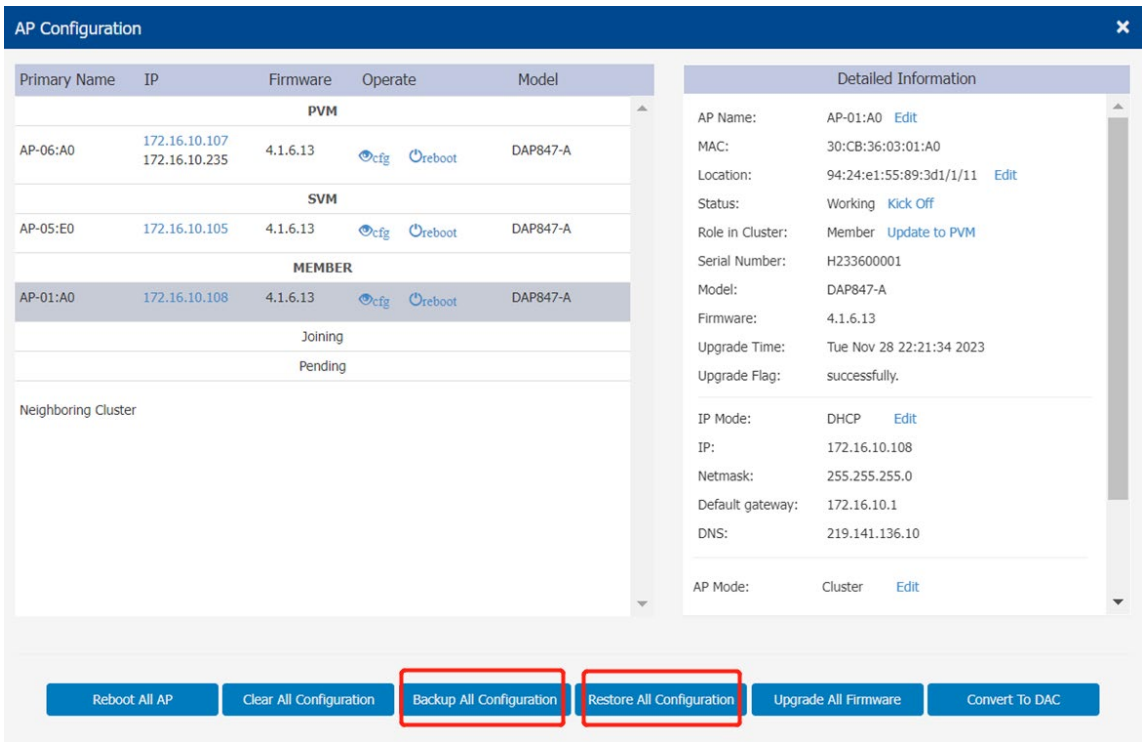


Figure 85: Backup and restore configurations

7.13 Upgrade the DAP847-XXA firmware

Before upgrading the DAP847-XXA firmware, download the firmware file from https://catalog.belden.com. Save the firmware file to your local disk of the PC you are using to connect the DAP847-XXA or to a remote TFTP or SFTP server.

- ☐ Click the **"Upgrade All Firmware"** button in the AP Configuration window and the Upgrade window will pop up.

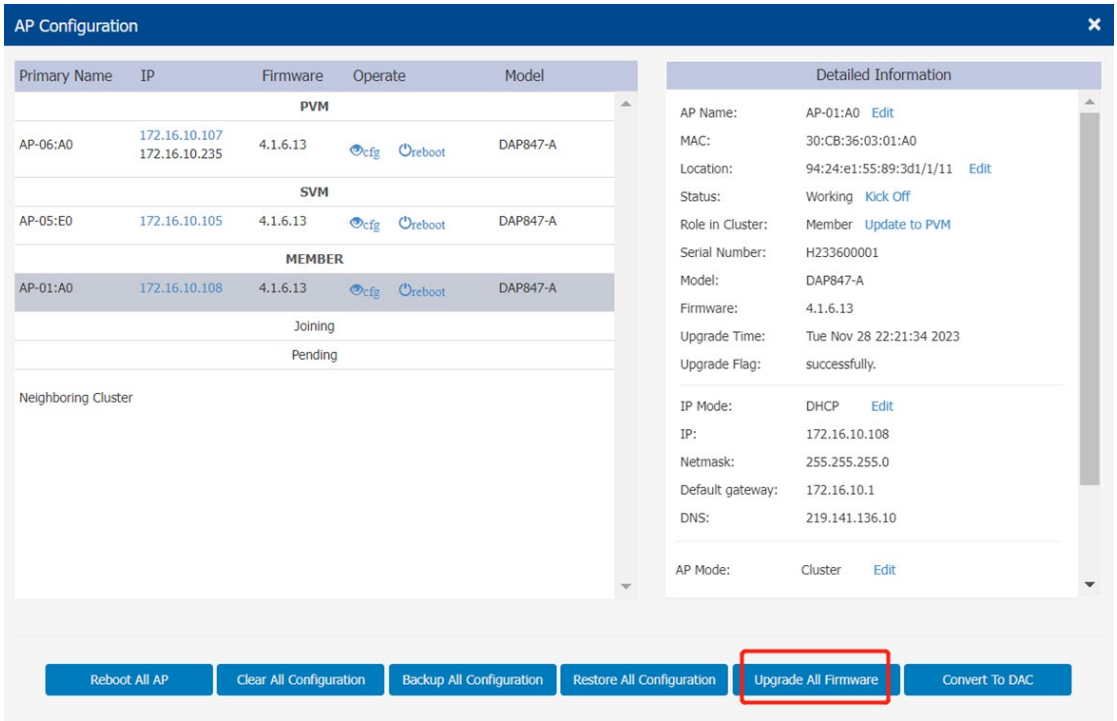


Figure 86: Go to DAP847-XXA upgrade window

7.13.1 Upgrade all DAP847-XXA in cluster

If you need to upgrade the DAP847-XXA firmware of different models, such as in a mixed network of DAP847-XXA and DAP6XX series, select the related DAP firmware file according to the AP models on the **Multi-model Upgrade** page. Multiple models of DAP devices can be upgraded at the same time.

Note: Generally, it takes about 5 minutes to upgrade the AP firmware.

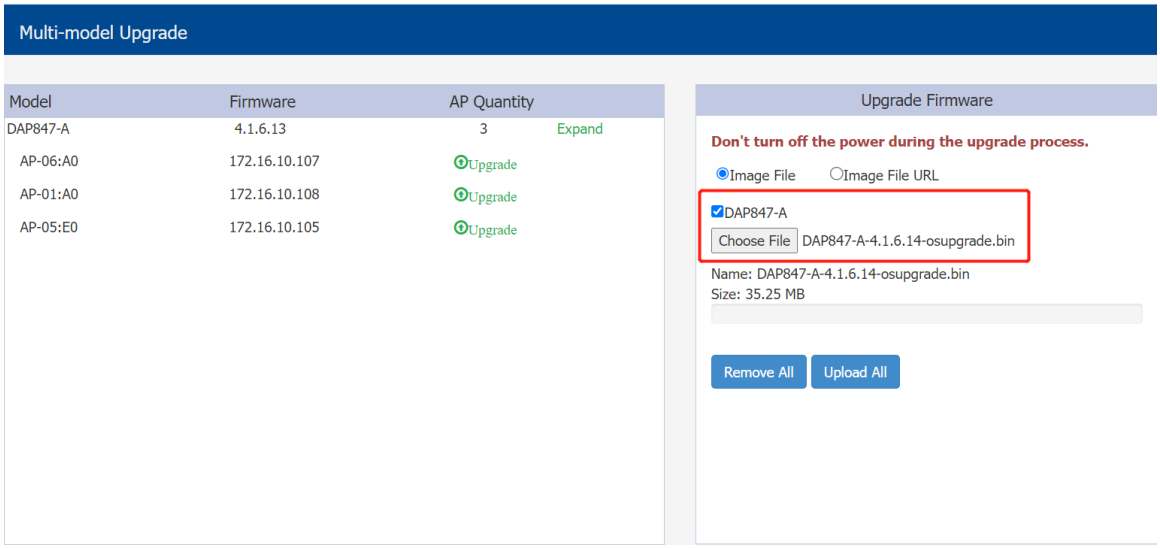


Figure 87: Upgrade all firmware

Upload the DAP847-XXA firmware in the following 3 ways:

- **Upload from local file:** Selects the **"Image File"** option and upload the firmware from the local file. Click the **"Upload All"** button to perform the upload and upgrade. Click the **"Remove All"** button to cancel the upgrade.

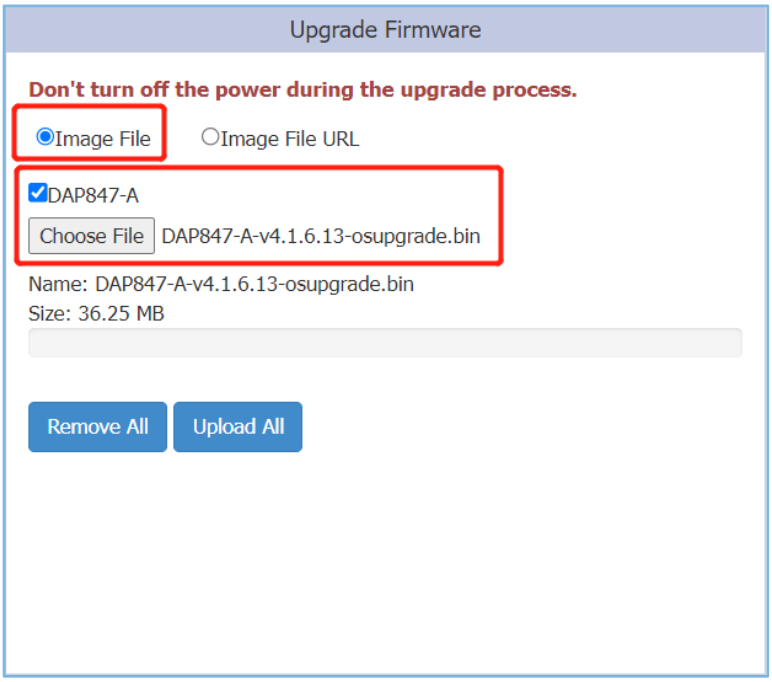


Figure 88: Upload firmware from local file

- **SFTP**: Uploads the AP firmware by using SFTP and select the **"Image File URL"** option. Enter the specified URL with the SFTP server IP

address, credentials, and firmware file name. Click the **“Upload To All”** button to perform the upload and upgrade.

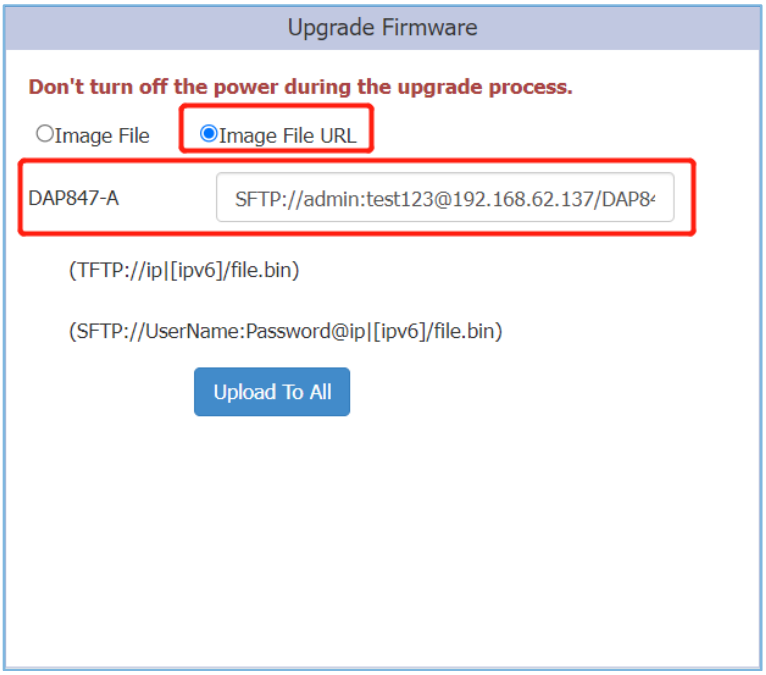


Figure 89: Upload DAP847-XXA firmware by using SFTP

- **TFTP**: Uploads the AP firmware by using TFTP and enter the specified URL with the TFTP server IP address, and firmware file name. Click **“Upload To All”** button to perform the upload and upgrade.

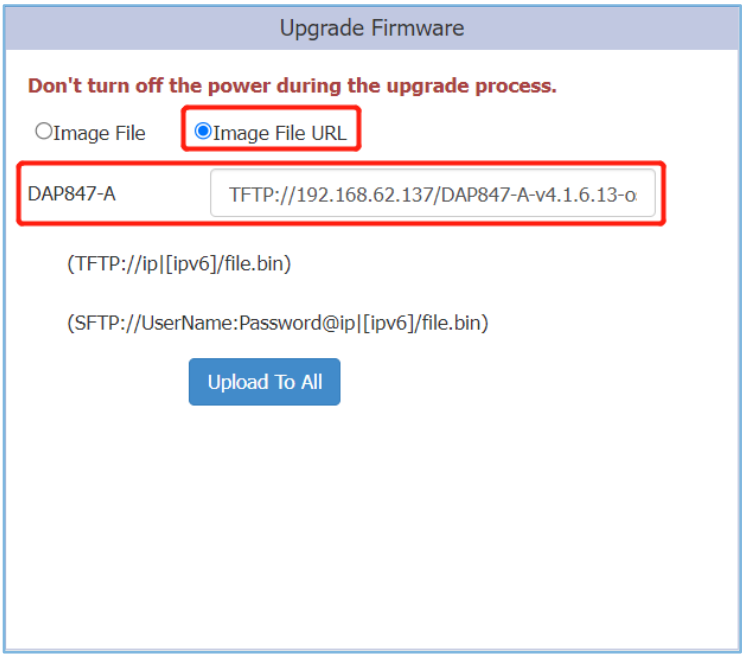


Figure 90: Upload DAP847-XXA firmware by using TFTP

7.13.2 Upgrade the single DAP847-XXA

To upgrade the single DAP847-XXA, select the DAP847-XXA from the AP list on the Multi-model Upgrade page. Click Upgrade and upload firmware file for the selected DAP847-XXA.

Upload the single DAP847-XXA firmware in the following 3 ways:

- Upload local file
- SFTP
- TFTP

You can also upgrade one single DAP847-XXA via the AP Advanced Configuration page. See “System management” on page 107.

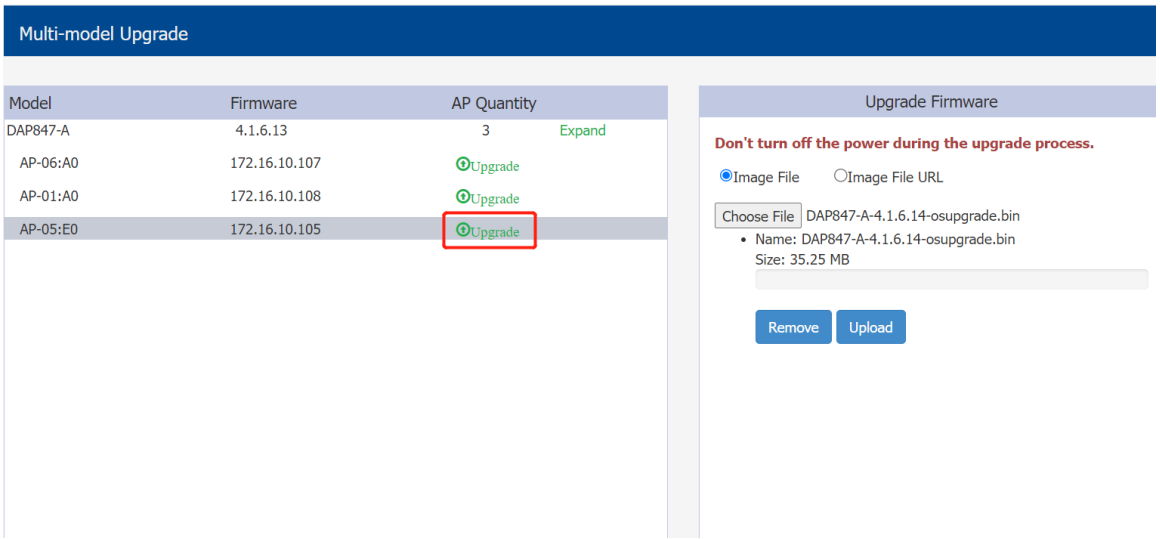


Figure 91: Upgrade the single DAP847-XXA in the cluster

Note: Don’t turn off the power during the upgrade process. To ensure the best use of the new software version, Hirschmann IT recommends clearing the history data in your browser after the software upgrade, including Cookies and Caches.

7.14 Configure the LED

- ☐ Click in the AP Window to launch the **“LED-Off/Locate”** button, see Figure 92.
- ☐ Click **“LED-Off”** to turn off the LED light.
- ☐ Click **“Locate”** to locate the AP in this state. The **“Restore”** label appears, and the LED on the DAP blinks in red, blue, and green alternately.

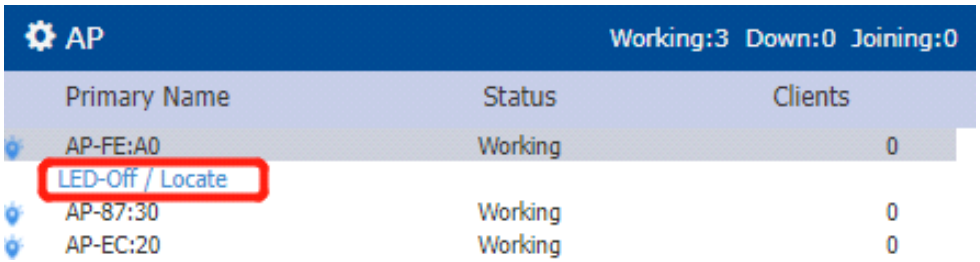


Figure 92: Locate or turn on/off LED

- ☐ Click **“Restore”** to return to the default state, see Figure 93.

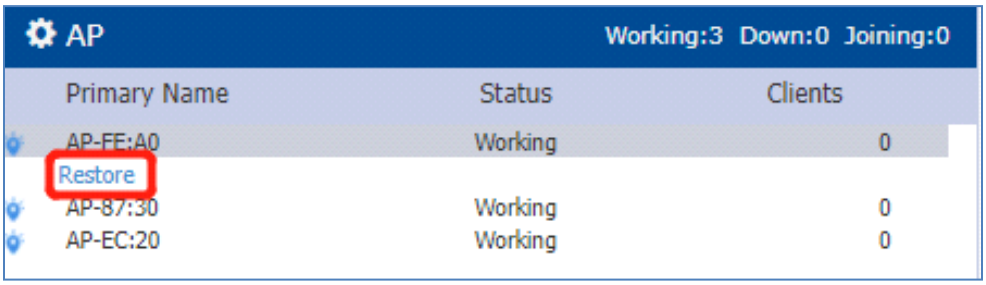


Figure 93: Restore LED to default state

7.15 DAP847-XXA advanced configuration

You can access the AP Configuration window by clicking the IP address from the AP list, see Figure 94.

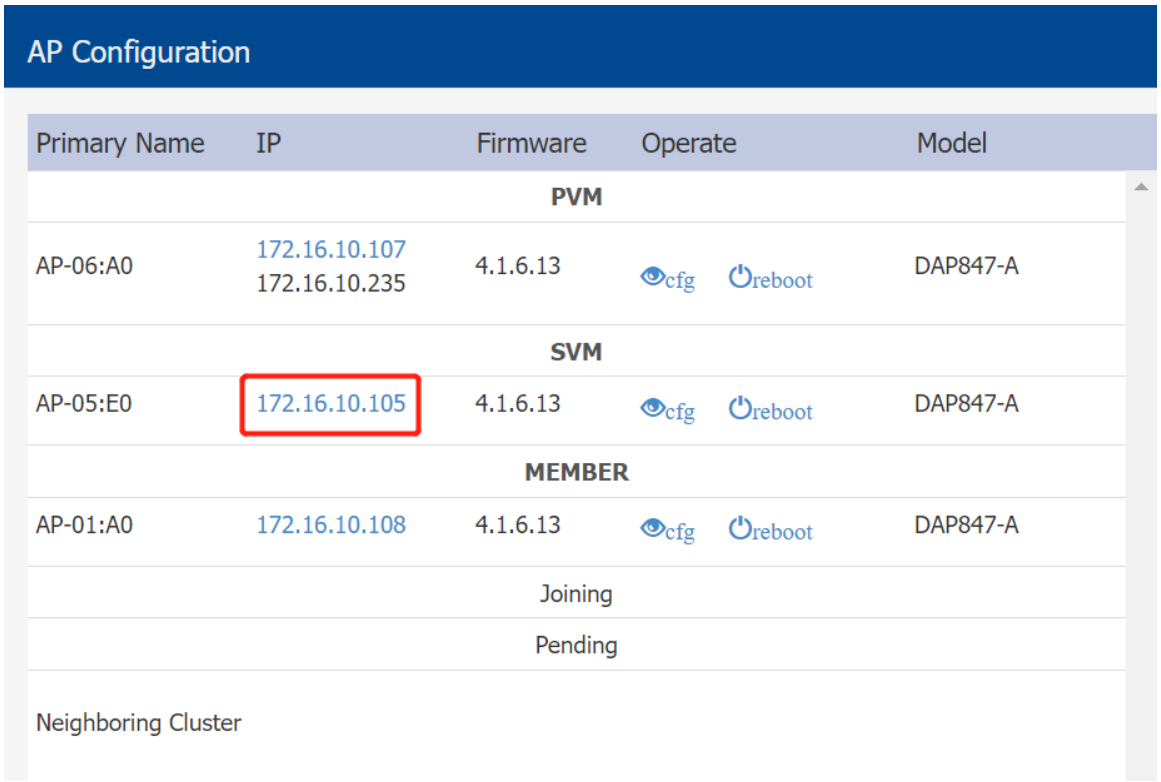


Figure 94: Advanced DAP847-XXA configuration

7.15.1 AP advanced configuration window overview

DAP847-XXA Advanced Configuration window is a dedicated web interface to monitor and configure a single DAP in the cluster, while the cluster web management system is used for configuration based on the cluster level as well as monitoring, see Figure 95. On the AP advanced configuration page, you can:

- Check the WLAN status by connecting clients on the DAP847-XXA.
- Configure DHCP/DNS/NAT services on the DAP847-XXA.
- Configure the wireless Mesh/Bridge feature for the DAP847-XXA.
- Upgrade, reset, or reboot the DAP847-XXA.
- Monitor and scan the RF environment.
- Configure and show the Neighbor DAP847-XXA devices.

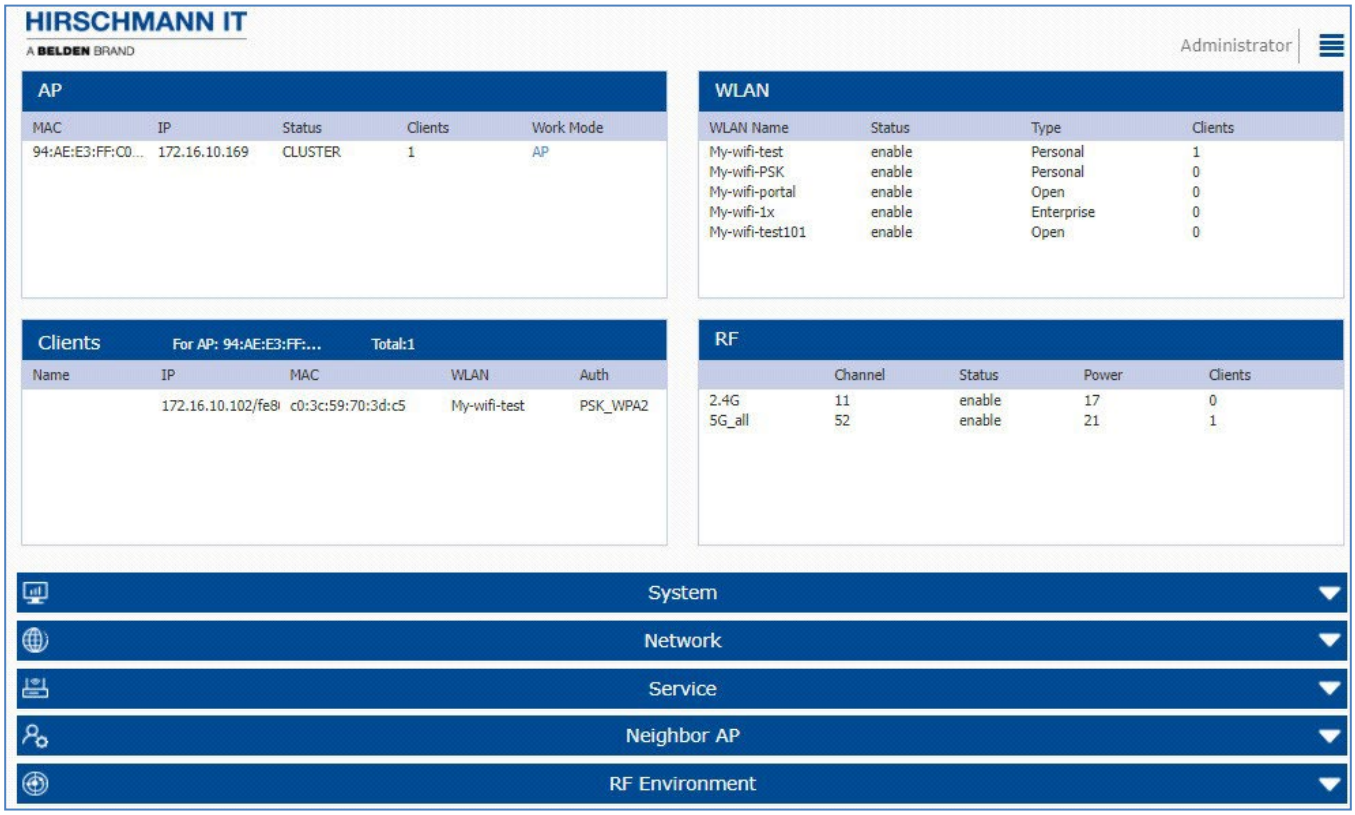
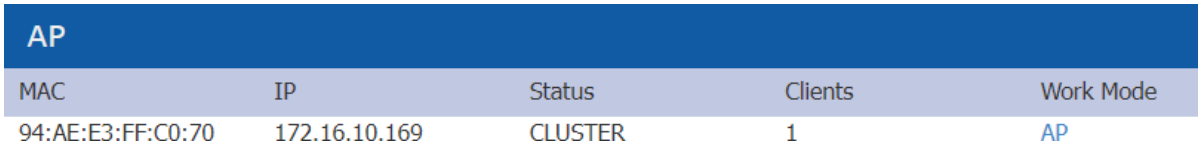


Figure 95: AP advanced configuration page

7.15.2 AP status monitoring and working mode configuration

The AP information window shows the basic information for a specific DAP847-XXA, such as MAC, IP address, Status, number of associated Clients and Work Mode.



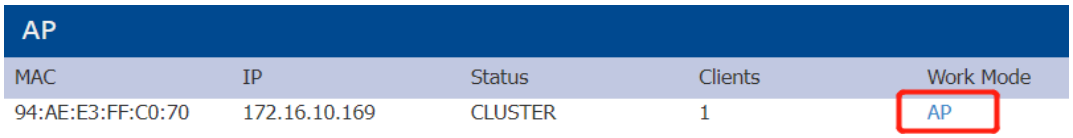
AP

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

Figure 96: AP information window

To load the Mode Configuration page:

- ☐ Click on the hyperlink **"AP"** in the AP information window.



AP

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

Figure 97: AP mode configuration entry

- ☐ Change work mode in **Mode Configuration** page.

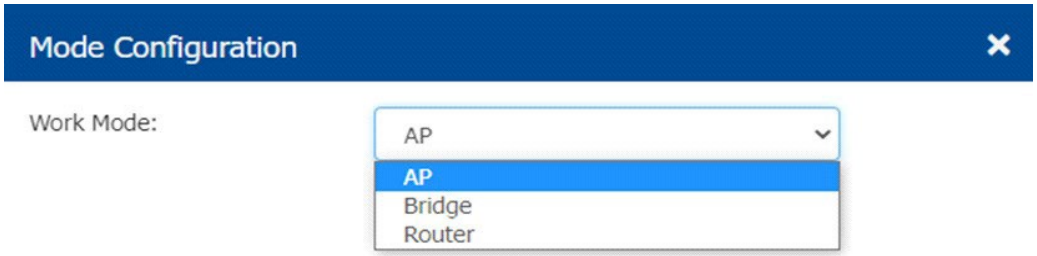


Figure 98: AP mode configuration

- ☐ Reboot is needed to change the DAP847-XXA work mode. By default, the device is in the AP mode.

You can configure a specific DAP847-XXA to work in Bridge mode or Router mode.

■ Configure DAP847-XXA works in bridge mode

The bridge mode of DAP847-XXA is a type of network connection. It allows establishing bridges between DAP847-XXA devices for connections between two or more networks. In bridge mode, a DAP847-XXA can connect another DAP847-XXA to extend network coverage or connect different networks.

Note: All DAP847-XXA devices in bridge mode need to be in the same IP segment and need to use the same channel and encryption method.

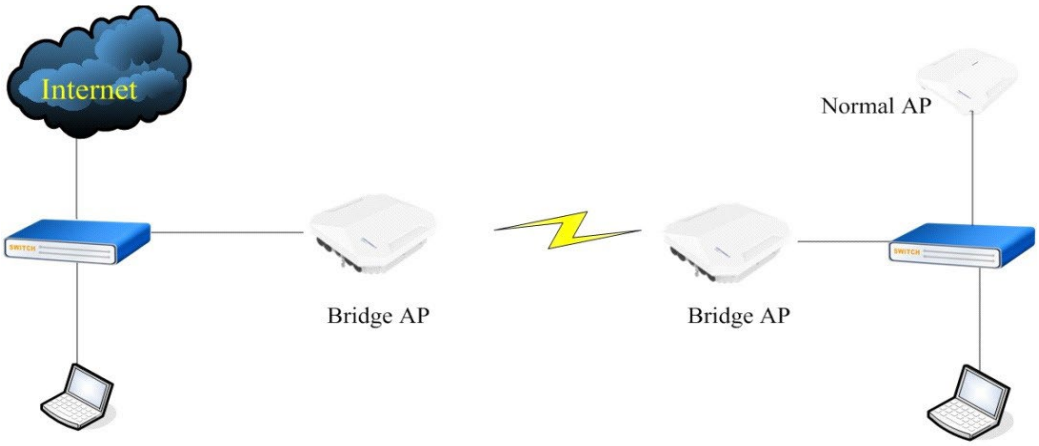


Figure 99: Bridge topology

In the Bridge mode, DAP847-XXA will only broadcast a bridge SSID and will not accept wireless client connection, except for the Bridge AP. See Figure 100.

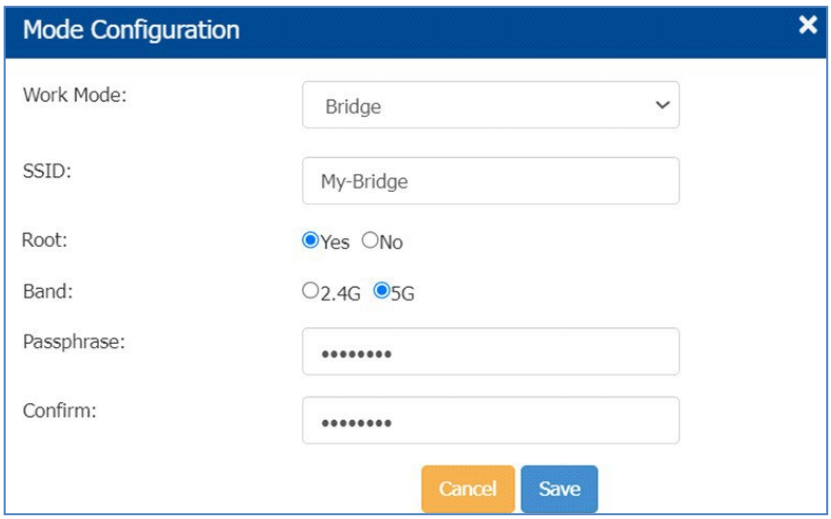


Figure 100: Bridge configuration

Parameter	Description
Work Mode	DAP847-XXA working mode, including Bridge mode, AP mode, and Router mode.
SSID	Configures the SSID used for Bridge connection. The SSID needs to be consistent with the SSID name configured on the peer device.
Root	Specifies the root node of the wireless bridge.
Band	Wireless bridge working frequency, 2.4G or 5G.
Passphrase	Password of the WLAN used to set up wireless bridge connection
Confirm	Re-enters the password to confirm.

Configure DAP847-XXA works in router mode

In the router mode, DAP847-XXA will work as a DHCP server and provide an IP address for clients. DAP847-XXA supports managing the IP address of an uplink interface (WAN) by DHCP, Static, or PPPOE.

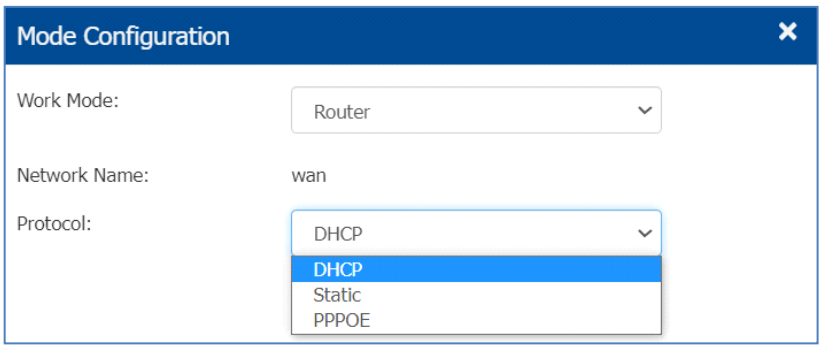


Figure 101: Configure WAN IP

The detailed network configuration can be viewed and modified on the **AP Network Configuration** page. You can modify the configuration of the WAN interface and default interface (LAN) interface, IP address, DNS, Gateway, and so on.

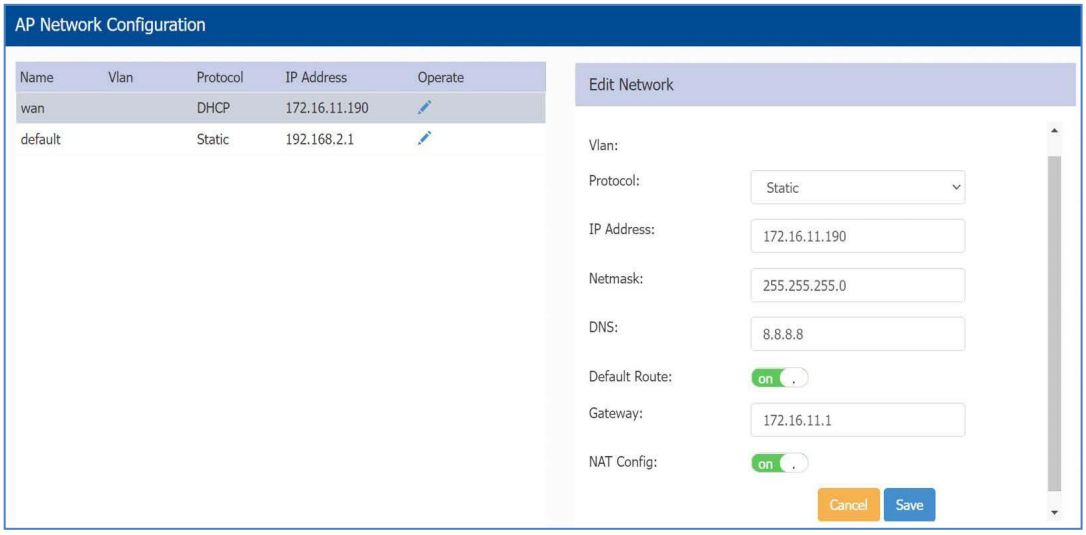


Figure 102: Modify DAP847-XXA network configuration

7.15.3 WLAN information

The WLAN information window shows the basic information about SSID on a specific DAP847-XXA, such as WLAN Name, Status, encryption type, and the number of clients associated with the WLAN. The information in this window is only for view and cannot be configured.

WLAN

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

Figure 103: WLAN information overview

7.15.4 Clients information

The Clients information window shows the basic information about clients on a specific DAP847-XXA, such as User Name for portal authentication, IP address, MAC, WLAN, and encryption type. The information in this window is only for view and cannot be configured.

Clients For AP: 34:E7:0B:09:C0:70 Total:2

User Name	IP	MAC	WLAN	Auth
	192.168.8.4/fe80::1852:43	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

Figure 104: Clients information overview

7.15.5 RF information

The RF information window shows the basic information about the radio,such as the channel, the work status, the transmit powerof each radio, and the number of clients associated to the radio. The information in this window is only for your view and cannot be configured.

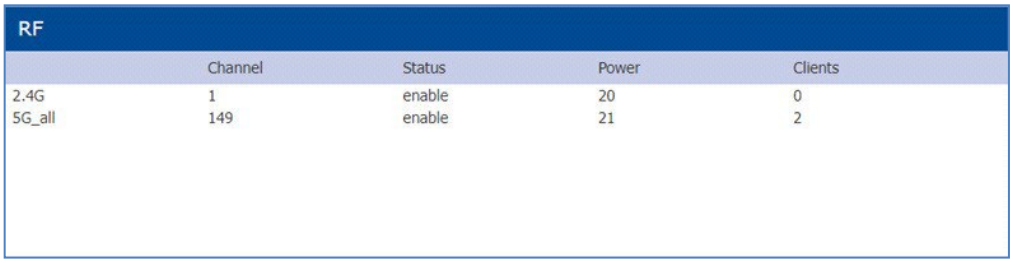


Figure 105: RF information overview

7.15.6 System management

On this page, you can view the syslog information related to the specific DAP847-XXA. You can also perform the DAP847-XXA upgrade, see Figure 106.

See “Syslog configuration” on page 131 and “Upgrade the DAP847-XXA firmware” on page 96.

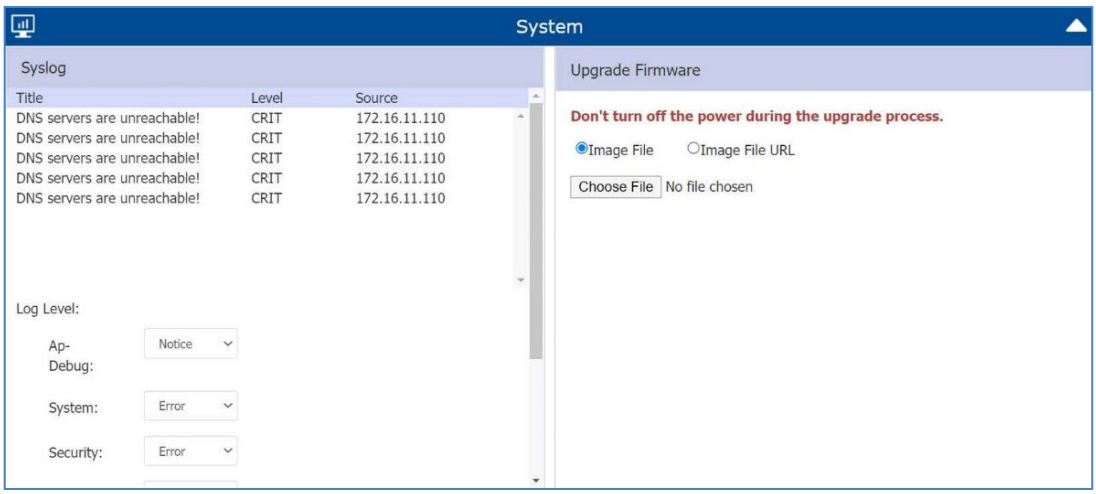


Figure 106: System management on AP UI

7.15.7 DAP847-XXA Interface configuration

In the interface configuration of DAP847-XXA, you can view the detailed information of each interface of DAP847-XXA. At the same time, in the interface configuration, you can connect the DAP847-XXC to DAP847-XXA by configuring the Mesh wireless network connection.

To complete the interface configuration of DAP847-XXA, follow the path to complete the configuration: **AP Advanced Configuration → Network → AP Interface** →AP Interface Configuration.

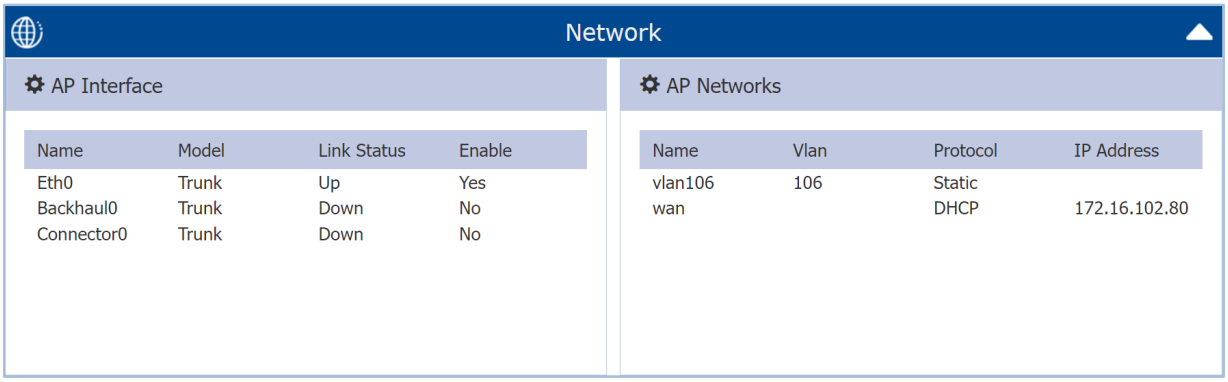


Figure 107: DAP847-XXA interface window

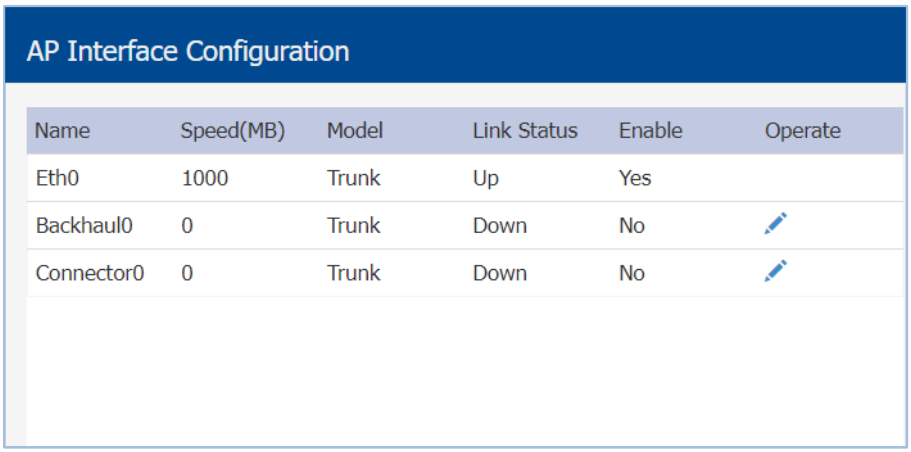


Figure 108: AP interface configuration

Parameter	Description
Eth0	Wired interface to connect switches and other equipment.
Backhaul0	The downlink interface of the Mesh/Bridge link.
Connector0	The uplink interface of the Mesh/Bridge link.
Speed	Link speed of the AP interface
Model	VLAN access mode or WLAN trunk mode.
Link Status	Up or down.
Enable	Indicates whether the AP interface is enabled or disabled.
Operate	Applied to Backhaul0 or Connector0 interface for wireless mesh/bridge configuration.

7.15.8 DAP847-XXA network

According to different scenarios and network configuration requirements, relevant parameters can be configured for the WAN interface and VLAN interface of DAP847-XXA, including VLAN, DHCP or Static IP, etc. You can complete the configuration by following the path:

AP Advanced Configuration → Network → AP Network Configuration.

Note: When creating or editing WLAN, if VLAN configuration is mapped, DAP847-XXA creates a VLAN interface, see Figure 51.

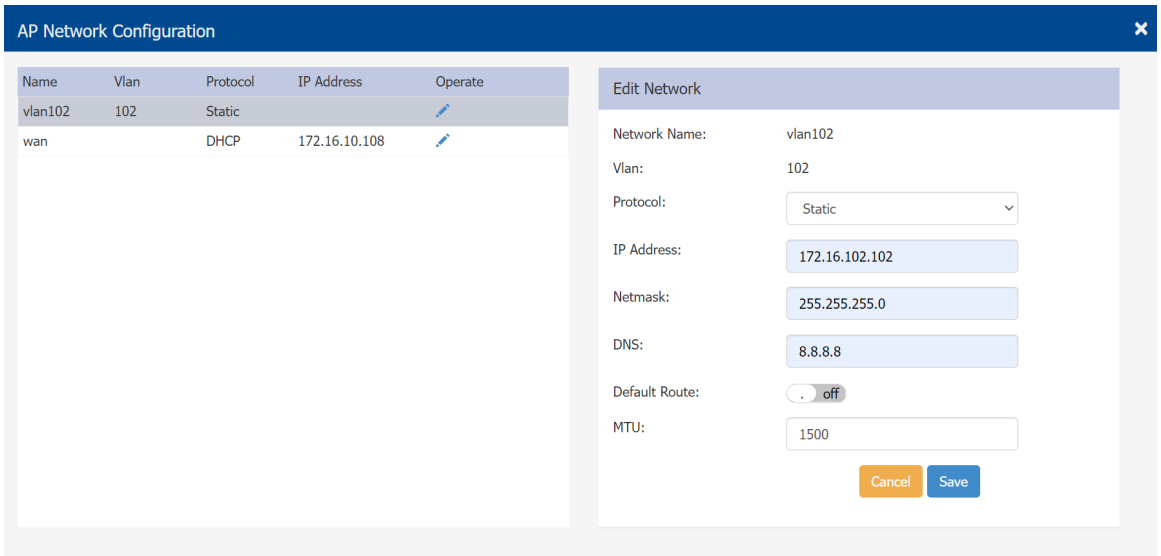


Figure 109: Network configuration

The key parameters are described as follows:

Parameter	Description
Name	The name of the network interface. There are 2 types of network interfaces: ▶ VLAN networks mapping to WLAN (SSID) ▶ WAN networks mapping to the DAP uplink port.
VLAN	VLAN ID mapping to a specific WLAN (SSID) or VLAN ID mapped to a WLAN interface.
Protocol	Protocol for IP address allocation for the network interface. The IP address of a network interface is set as the gateway for the devices connecting to the network. ▶ DHCP: The interface IP address is obtained from an outside DHCP server.

Parameter	Description
	► Static: The interface IP address of the network is manually set.
IP Address	The IP address of the network.
Operate	Edits the DAP847-XXA network.

The key parameters of editing network are described as follows:

Parameter	Description
Network Name	The network interface name to be edited
Vlan	VLAN ID mapping to a specific WLAN (SSID) or VLAN ID mapped to a WLAN interface.
Protocol	Protocol for IP address allocation for the network interface, including: ► DHCP: The interface IP address is obtained from an outside DHCP server. ► Static: The interface IP address of the network is manually set.
IP Address	The IP address of the network interface.
Netmask	Netmask of the network.
DNS	DNS server for the network.
Default Route	Shows whether the interface of the network is the default route of the AP. By default, the WAN interface is the default route of the AP.
MTU	The MTU value of the network interface.

7.15.9 Mesh configuration

The Belden mesh solution is an effective way to expand wireless network coverage for enterprise environments without any wires.

This solution can also be used in mobile scenarios such as in rail transit. DAP847-XXA supports connecting downlink DAP-XXC devices to provide channels for train to ground communication, enabling real-time transmission of railway controlling signals and related data.

You can bridge multiple Ethernet LANs or extend your wireless coverage (Wireless back hauling) by mesh. As traffic traverses across mesh APs, the mesh network automatically reconfigures around broken or blocked paths. The self-healing feature increases the reliability and redundancy of the DAP847-XXA. The network continues to run if a DAP847-XXA stops working or disconnects from the network, see Figure 110.

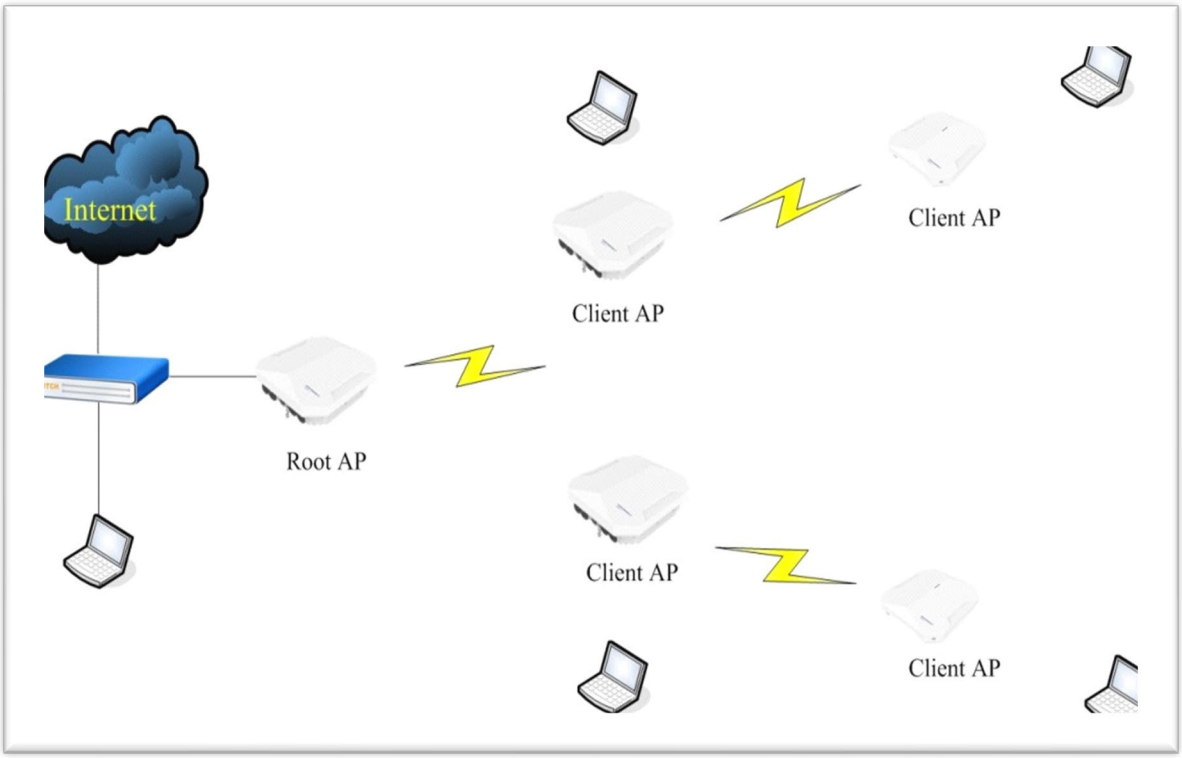


Figure 110: MESH topology

To expand your wireless coverage without bridging Ethernet LAN segments,you can use Mesh services configured as a wireless backhaul. In this scenario, the DAP847-XXA provides network access for wireless clients and establishes a mesh path to the mesh root, which uses wired interface to connect with the switch.

To configure your mesh networks, navigate to **AP Advanced Configuration → Network → AP Interface**.

- ☐ Click "✎" of the **"Backhaul0"** interface to configure your mesh network, see Figure 111.

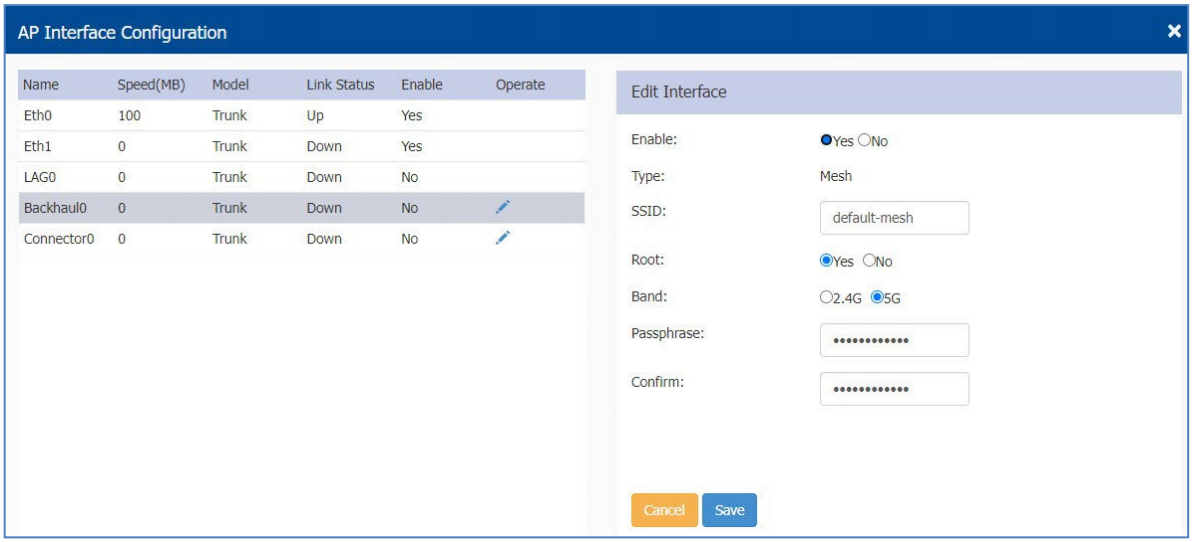


Figure 111: AP interface configuration

Parameter	Description
Enable	Selects **Yes** to enable or select **No** to disable the wireless mesh on DAP847-XXA.
SSID	SSID for mesh connection.
Root	Specifies the root node of the wireless mesh chain.
Band	The working band for mesh connection. The bands of the mesh connections from the root node to the client node are the same.
Passphrase	Password of the WLAN to set up wireless mesh connection.
Confirm	Re-enters the password to confirm.

7.15.10 Static neighbor AP configuration

The neighbor AP is the candidate to which clients connecting to the current DAP847-XXA might roam.

There are 2 types of neighbor APs:

- **Auto Neighbor AP**: Discovered through wireless scanning automatically.
- **Static Neighbor AP**: Manually added in case of some special deployment scenarios.

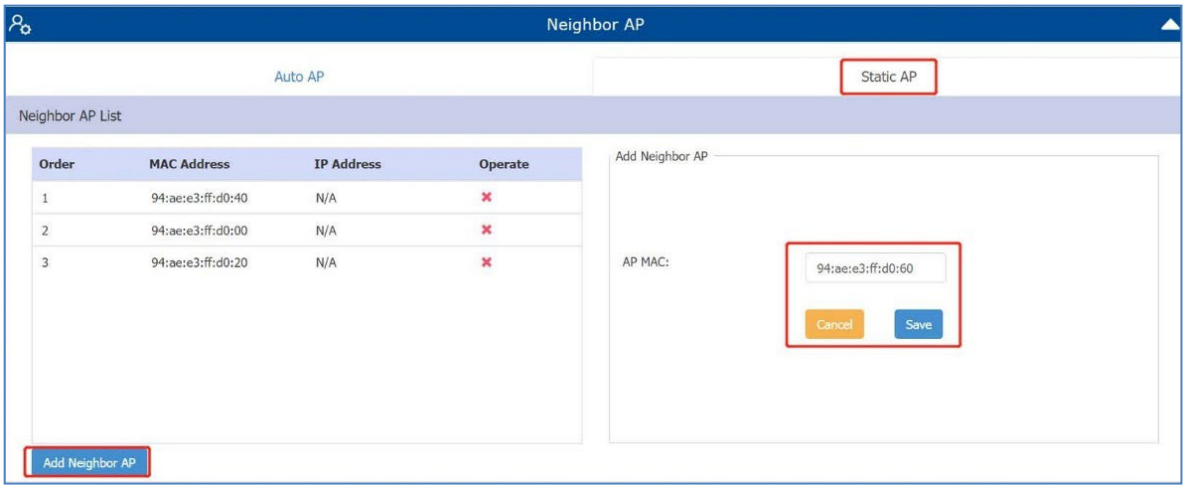


Figure 112: Configure static neighbor AP

Parameter	Description
Order	Item number of the neighbor APs.
MAC Address	MAC address of the neighbor APs.
IP Address	IP address of the neighbor APs.
Operate	Removes the neighbor APs. It is only applicable for Static Neighbor APs.

7.15.11 RF environment

The RF Environment window is used to view the DAP847-XXA data in different scanning modes. Wireless networks run in environments with RF devices that can interfere with network communications.

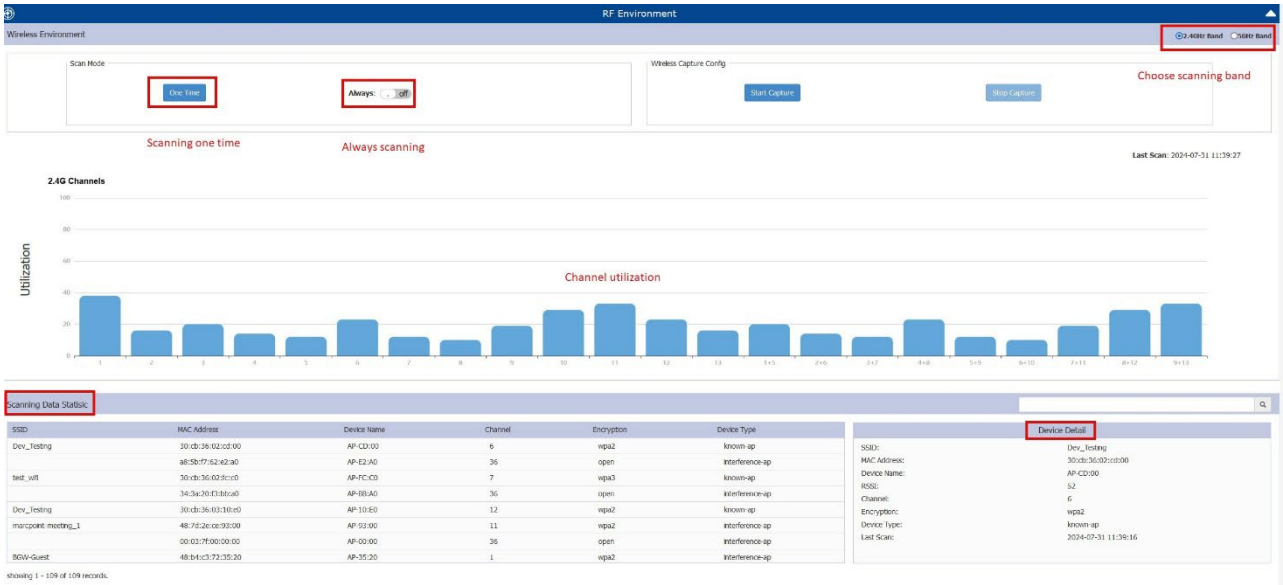
DAP847-XXA can detect the RF environment in which the Wi-Fi network is working, identify interference, and classify its sources. An analysis of the results can be used to quickly isolate detected issues with packet transmission, channel quality, and traffic congestion caused by contention with other devices working in the same channel.

The scanning band can be selected for 2.4 GHz or 5 GHz. The scanning data includes the channel utilization and the SSID in the RF environment. If you move your mouse to a channel, then you can view the detailed information of the channel. If you click the relevant item, then you can view the detailed SSID information, see Figure 113.

You could select the following types of scanning mode:

- **One Time:** The scanning mode will last for 5 minutes and then return to normal AP mode in which wireless clients associate.
- **Always:** The scanning mode is active, and the wireless client is not allowed to associate if the DAP847-XXA is powered on.

Note: To view the Scanning Mode data of a DAP847-XXA, ensure that the DAP847-XXA is in **"Scanning Mode"**. When the DAP847-XXA is in scanning mode, it does not respond to the clients' connection request. When the scanning mode (One Time mode or Always mode) is terminated automatically, the DAP847-XXA will return to the normal AP mode and the clients are allowed to connect.



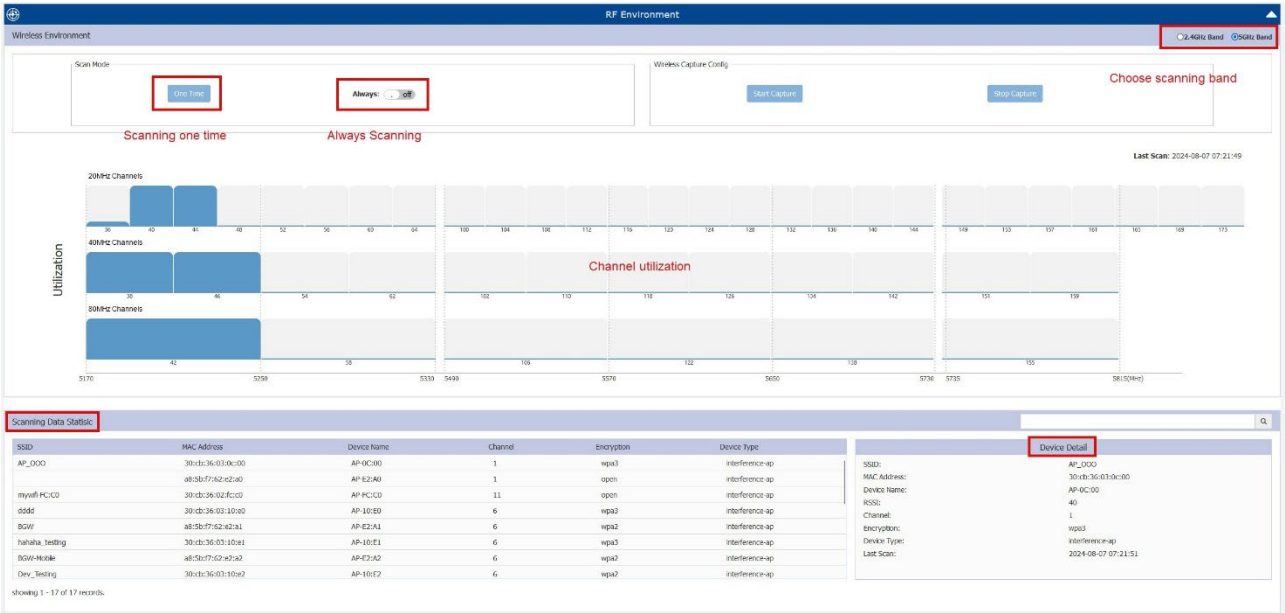


Figure 113: RF environment

7.15.12 Wireless capture

DAP847-XXA supports wireless packet capture mode. In this mode, the clients disconnect with the DAP847-XXA and stop wireless scanning during the packet capture.

When the threshold for packet capture is 5 minutes/10 MB, it will complete automatically, or it can stop manually at any time.

Refer to the following steps for the capture on the DAP847-XXA:

- ☐ Log in to the **AP Advanced Configuration** and navigate to **RF Environment → WirelessCapture Config → Start Capture**, see Figure 114.

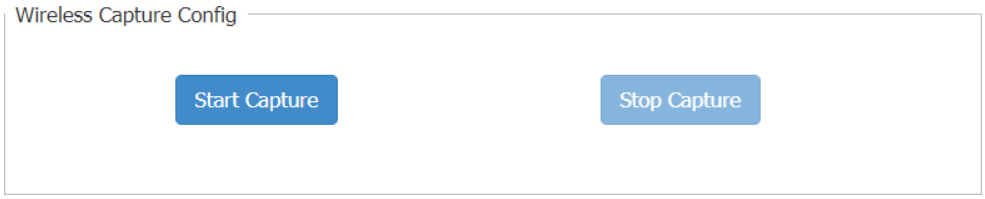


Figure 114: Wireless capture config

- ☐ Select the corresponding filters to capture.

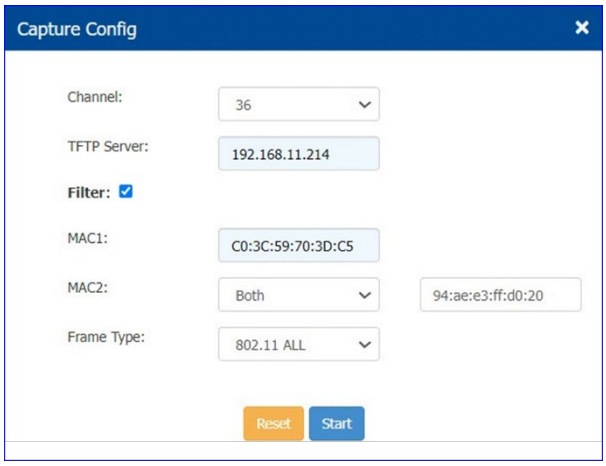


Figure 115: Capture filter config

- Click **"Start"** button. The DAP847-XXA will store the packet file to the /tmp folder temporarily and delete it automatically after it is uploaded to the TFTP server.

```
support@AP-34:D0:/tmp$
support@AP-34:D0:/tmp$ ls
PortalCustom                        log
TZ                                  mcs.conf
acv_ttnl                            mkca_lock
backup_version                      mode
capture_2021-07-02_22-13-24.pcap    no_qca_da
cloudurl                            ntp_synced_mark
cluster                             ntpdate_lock
cluster_cmd_pipe                    online-usr-count
```

Figure 116: Capture file example

7.16 Configure DAP847-XXA network service

7.16.1 Configure a DHCP server

On special occasions when there is no DHCP server or DAP847-XXA running in router mode, you can set up a DHCP server on a specific AP in the cluster.

Follow the path to finish the configuration: **AP advanced configuration** window → **Service** → **DHCP**, see Figure 117.

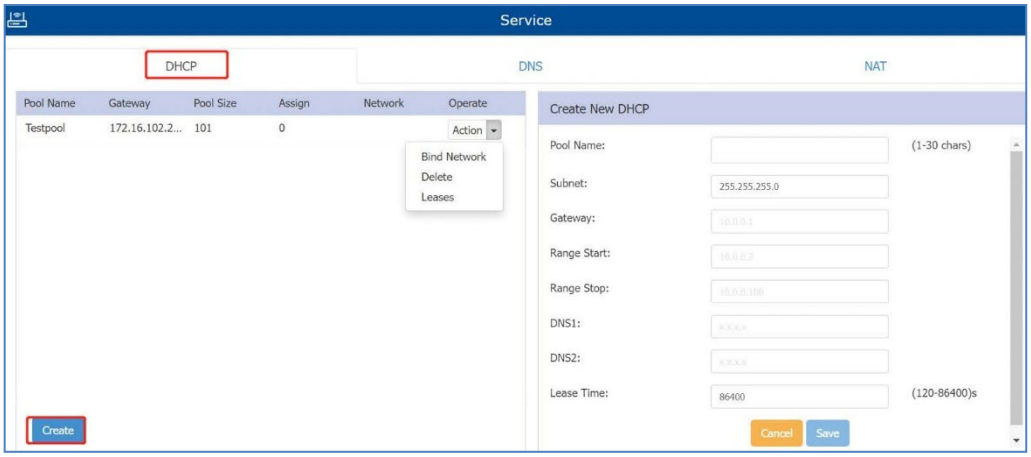


Figure 117: Configure DHCP server

After creating a DHCP pool, you must bind the DHCP pool to a specific network, see Figure 119. Before binding, you need to configure the network basic parameters in the **AP UI** → **Network** → **AP Networks Configuration**.

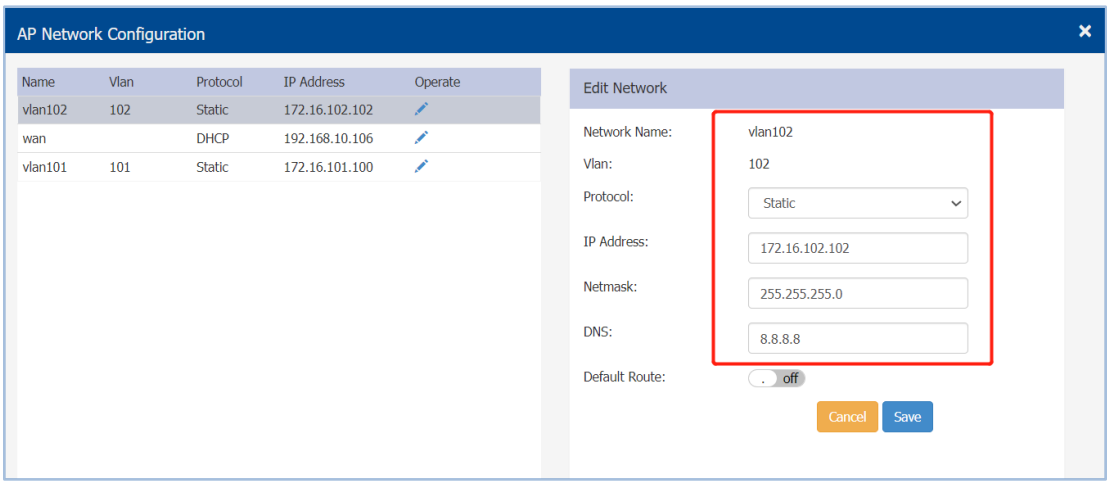


Figure 118: AP network configuration

Note: DHCP pool can only bind to the network interface with static IP.

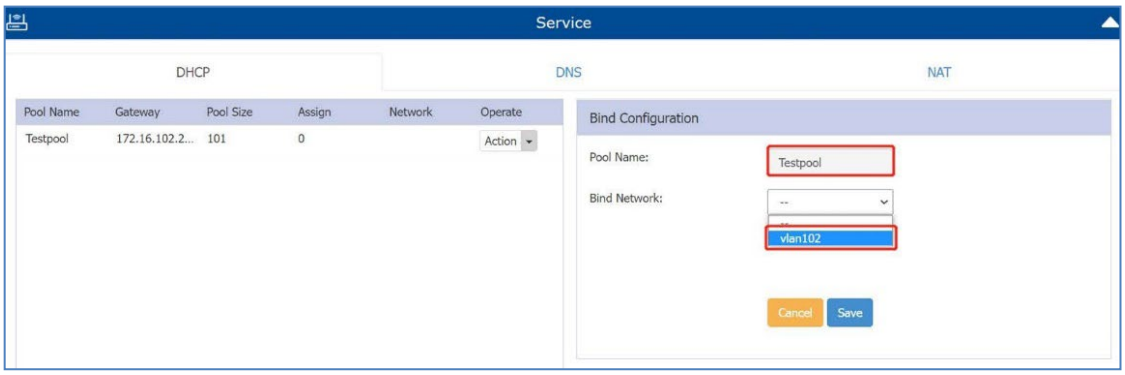


Figure 119: Bind DHCP pool to network interface

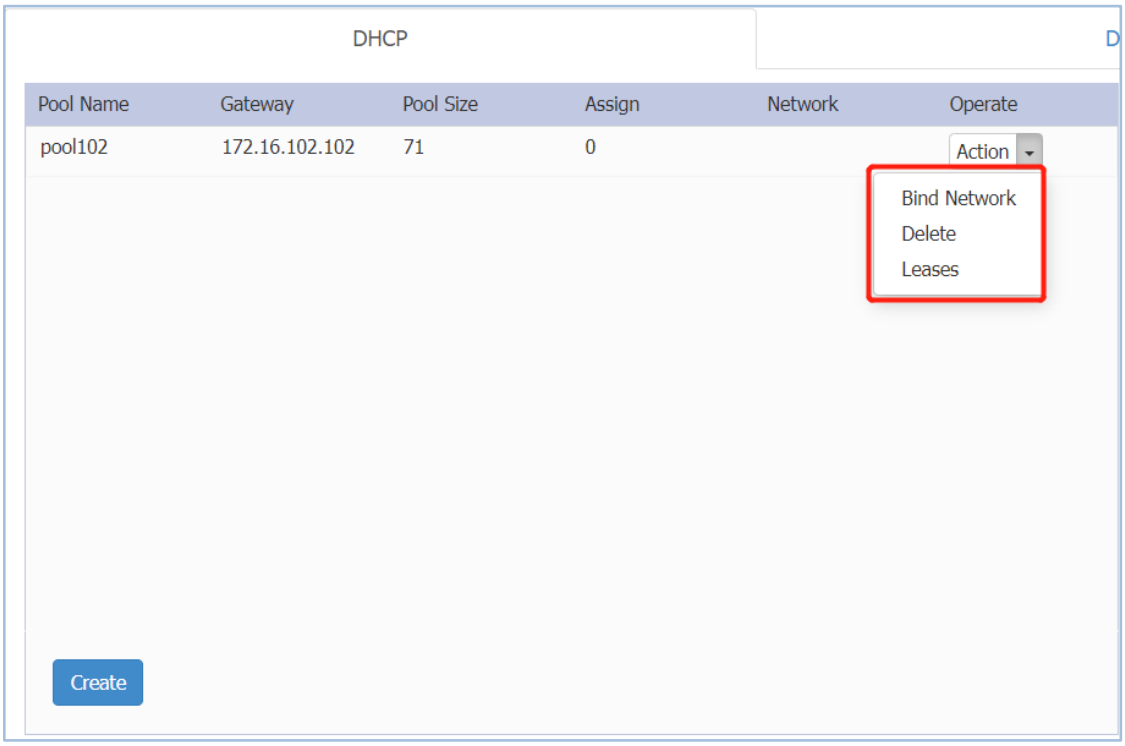


Figure 120: DHCP pool

Parameter	Description
Bind Network	Binds the DHCP pool to a specific network interface.
Delete	Deletes the DHCP pool.
Leases	Shows the IP addresses assigned to devices.

7.16.2 Configure a DNS server

DNS (Domain Name System) Cache stores DNS query results in DAP847-XXA. This caching method reduces the number of requests to DNS servers, thus enhancing the web browsing speed of clients and reducing traffic in the network.

When a client tries to connect to a domain name (such as www.belden.com), it first resolves the domain name to the corresponding IP address with a DNS query. The query process involves sending a request to a DNS server and waiting for the response. If the result of the domain name has been queried before and is still valid, the result can be used directly without sending another query request to the DNS server.

Configuration path: **AP Advanced Configuration → Service → DNS**.

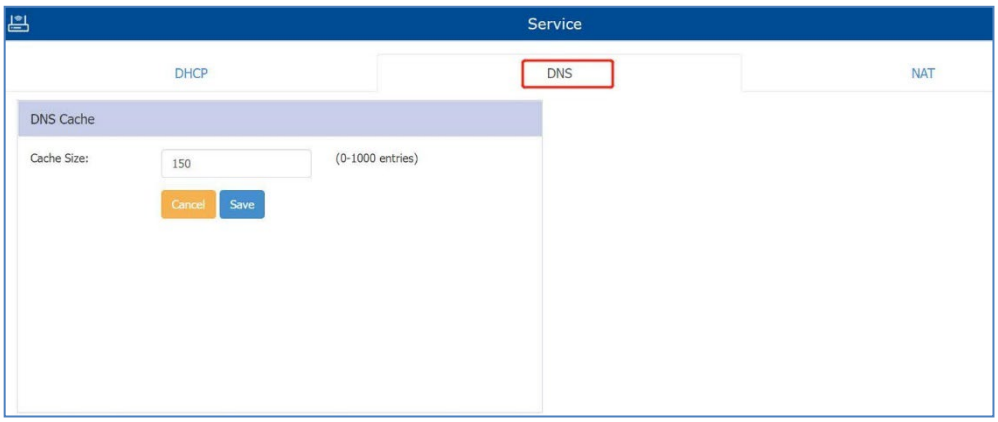


Figure 121: DNS Cache setting

Parameter	Description
Cache Size	Specifies the size for the DNS cache, and it can be set up to 1000 entries.The default value is 150 entries.

7.16.3 NAT configuration

NAT is the process of modifying network address when packets pass through a routing device. The routing device works as an agent between the public network (the internet) and the private network (local network), which ensures the translation of private network IP addresses into a public address space.

NAT converts intranet addresses and port numbers into legitimate public ones to create sessions with hosts in the public network. Hosts outside of NAT cannot actively communicate with hosts inside of NAT. Hosts inside of NAT that need active communication have to communicate with an IP in the public network. DAP 847-XXA is responsible for establishing a mapping relation for

data transmission.

The function of NAT not only solves the problem of insufficient IP addresses, but also effectively avoids intrusion from outside the network, hides and protects computers inside the network. Static NAT cannot save public network addresses but can hide the internal networks.

DAP847-XXA supports both Source NAT and Destination NAT.

Configuration path: **AP Advanced Configuration → Service → NAT**.

Source NAT

Use Source NAT to translate the internal IP addresses to a single external IP address when visiting the internet. You can configure Source NAT by saving the public IP addresses and clicking the window frame of Source NAT, see Figure 122.

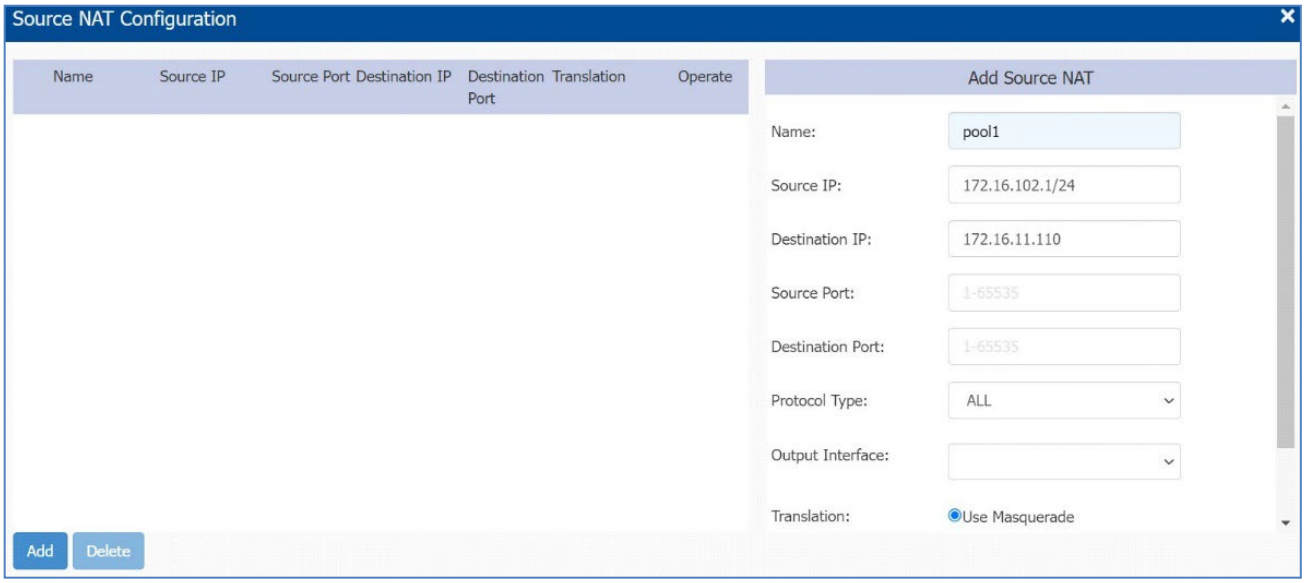


Figure 122: Configure source NAT

Parameter	Description
Name	Name of the Source NAT rule.
Source IP	Mapping source IP address of the NAT rule, single IP, or segment.
Destination IP	Mapping the destination IP address of the NAT rule, single IP, or segment.
Source Port	Mapping source port of the NAT rule.
Destination Port	Mapping the destination port of the NAT rule.
Protocol Type	Network protocol to which the NAT rule is applied.
Output Interface	Specifies the outbound interface of the NAT rule.
Translation	Use Masquerade to translate the internal IP address to the interface IP address

	(gateway) of the network.

Destination NAT

Use Destination NAT to realize visiting specific servers in the internal network from the internet. You can configure Destination NAT by clicking the window frame of Destination NAT, see Figure 123.

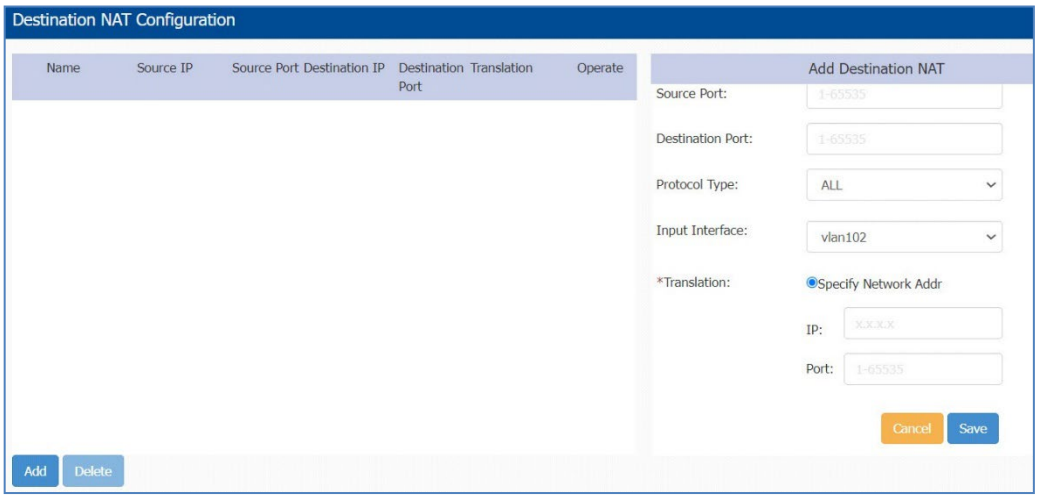


Figure 123: Configure destination NAT

Parameter	Description
Name	Name of the destination NAT rule.
Source IP	Mapping the source IP address of the NAT rule, single IP, or segment.
Source Port	Mapping the source port of the NAT rule.
Destination IP	Mapping the NAT destination address, which can be a single IP or an IP segment.
Destination Port	Mapping the destination port of the NAT rule.
Protocol Type	Network protocol to which the NAT rule is applied.
Input Interface	Specifies the inbound interface of the NAT rule.
Translation	▶ IP: Maps the external IP address to an internal address. ▶ Port: The internal port to which the external IP address will be mapped.

8 System management

The System window mainly displays the basic information of the current DAP847-XXA cluster, including DAP847-XXA cluster attributes, system management accounts, system time, and syslog. You can also query and modify the configuration of the DAP847-XXA system information.

This chapter contains the following topics:

- Cluster info management
- Accounts management
- Certificate management
- Services management
- System time configuration
- Syslog configuration
- SNMP configuration

8.1 Cluster info management

Navigate to **System → General Configuration** to configure or modify the cluster attributes, such as Cluster Name and Location.

The administrator can manually set the management IP address in the Cluster Info Management tab. The management IP address is used to manage the DAP cluster, which is a virtual IP. It is assigned to the PVM and can be accessed from both the wireless and wired sides.

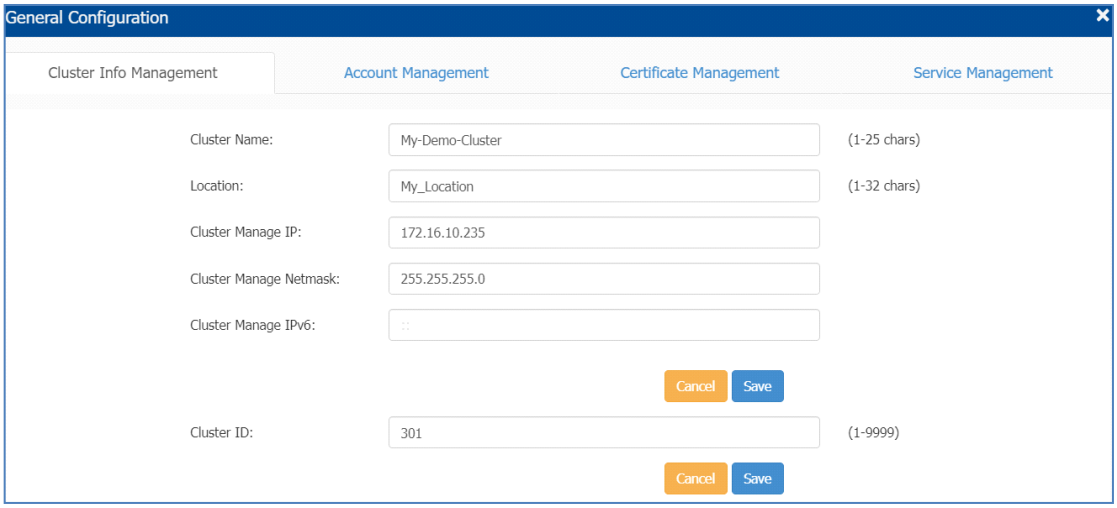


Figure 124: Cluster info management

Parameter	Description
Cluster Name	The name of the DAP847-XXA cluster
Location	The location of the DAP847-XXA cluster
Cluster Manage IP	A virtual IP address for DAP847-XXA cluster management
Cluster Manage Netmask	The netmask of DAP847-XXA cluster management IP
Cluster Manage IPv6	A virtual IPv6 address for DAP847-XXA cluster management
Cluster ID	Identification of the DAP847-XXA cluster, the default cluster ID is 100.

The DAP847-XXA Cluster Information displays at the top of the Dashboard.

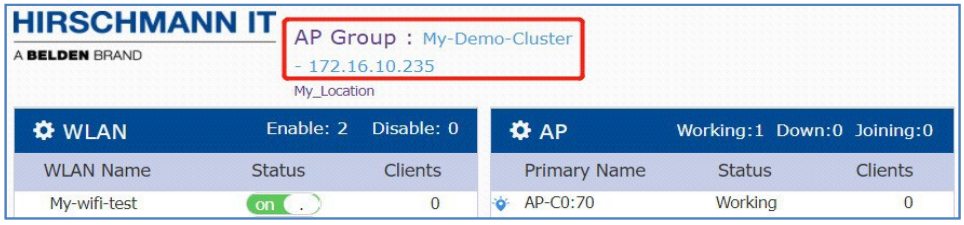


Figure 125: Cluster information

Note: The **Cluster Manage IP** is a static IP address configured for the DAP847-XXA cluster web management. You can manage the DAP847-XXA cluster by accessing the URL: http://IP:8080 or https://IP by wired or wireless network.

The management IP is configured on the PVM of the DAP847-XXA Cluster. Ensure that the Management IP on the PVM is routable from your configuring terminal (browser). Hirschmann IT recommends that you choose an idle IP address from the DAP847-XXA cluster domain to configure it as a management IP address.

8.2 Accounts management

8.2.1 Manage web GUI accounts

You can log in to the web GUI using three different types of accounts with different privileges:

- **Administrator**: The administrator account has the highest privilege. You can view and modify system configurations, including enabling or disabling Viewer users, deleting configurations, and restoring DAP847-XXA to factory settings.
- **Viewer:** You can view the configurations and monitor the WLAN operations with the viewer account
- **Guest Manager**: You can only edit and view the guest portal users with the guest manager account.

You can log in to multiple accounts at the same time. When the same account is logged in, the previous session is terminated. By default, only the **Administrator account** is enabled, and the **Viewer** and **Guest Manager** accounts are disabled.

In the **Account Management** tab, you can enable or disable the **Viewer** and **Guest Manager** accounts, and change the password for **Administrator**, **Viewer**, and **Guest Manager**, see Figure 126.

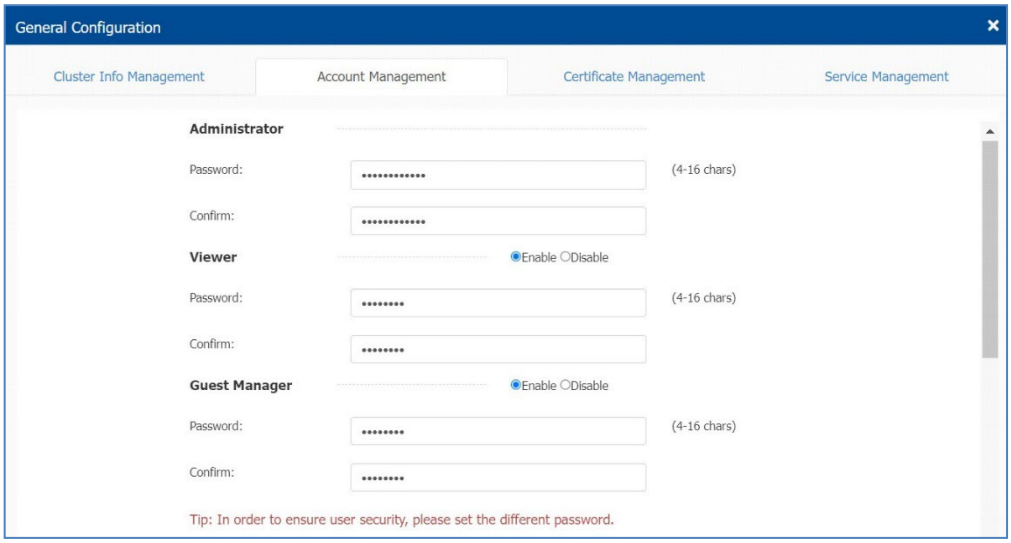


Figure 126: Account management

8.2.2 Manage CLI accounts

You can log in to the DAP847-XXA CLI using different accounts with different privileges: **Support** and **Root**. Administrator can change the login password for the CLI accounts. The root password is a string held by the customer only. The string is used to generate the root access credential by DAP847-XXA, see Figure 127.

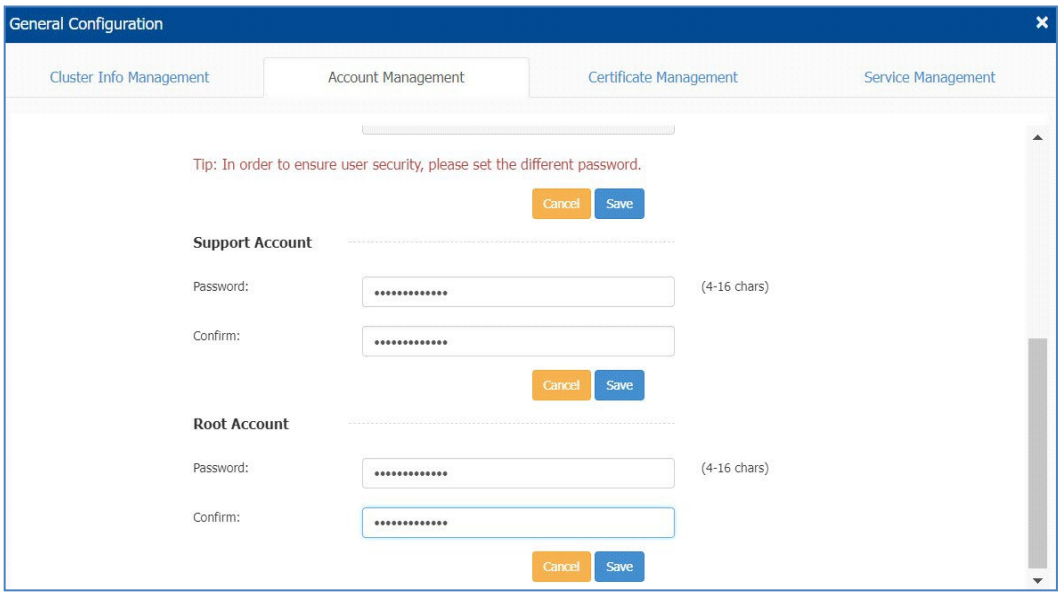


Figure 127: CLI account management

Note: For security reasons, Hirschmann IT recommends that administrators change the root and support user passwords before using DAP847-XXA.

8.3 Certificate management

DAP847-XXA supports 2 types of built-in certificates. The administrator can customize the certificate based on specific requirements:

- **Internal Web Server:** The certificate is used to establish the secure connection between the web browser and the DAP847-XXA web server for https management. By default, a built-in CA certificate is generated by Belden with the domain **"find.dap.com"**. Users need to use open SSL to generate a CA certificate and replace the default one (User needs to use the domain **"find.dap.com"** for their own certificate because the login URL cannot be changed).
- **Internal Portal Server:** The certificate is used to establish the secure connection between the captive portal window and the DAP847-XXA web server to protect the user login credentials from being stolen. Users can define the Portal login URL and replace the certificate accordingly.

Configuration path: **System→ General Configuration → Certificate Management**.

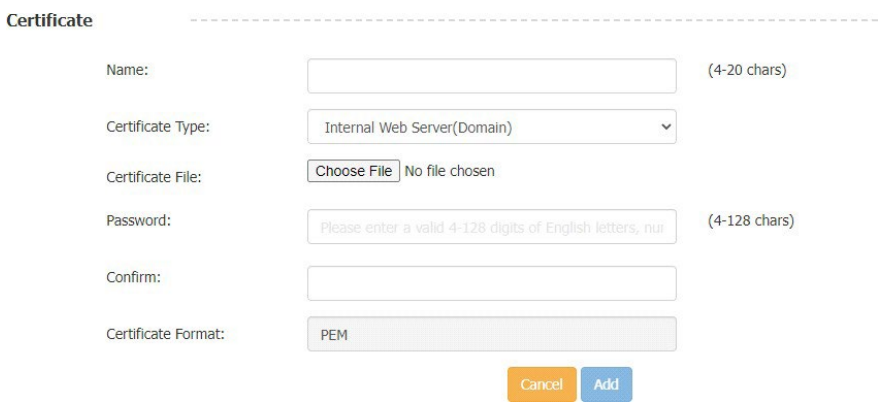


Figure 128: Certificate management

8.4 Services management

DAP847-XXA supports the following services which can be enabled or disabled separately based on your requirements, see Figure 129. By default, both of the following services are disabled.

- **IPV6 L3 Forwarding**: If the IPv6 service is enabled, Layer 3 IPv6 traffic forwarding between the client and other network devices.
- **IGMP Snooping**: The management status of the IGMP Snooping function on DAP847-XXA is a multicast constraint mechanism running on layer 2 devices and is used to manage and control multicast groups.

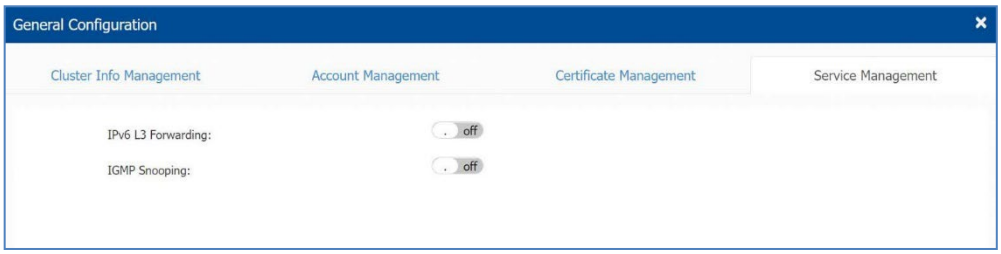


Figure 129: Service management

8.5 System time configuration

It is essential to have the correct system time for DAP847-XXA. It can record communications with other network devices, and system logs, especially for troubleshooting, which all depends on the correct system time.

Administrator can navigate to **System → System Time** to configure the system time.

NTP (RFC 1305 - Network Time Protocol) is a network protocol used to synchronize the time between the elements in the network. The main function of NTP is to provide precise time synchronization services that synchronize computer systems in seconds. It uses NTP to transmit time information and calculate the best time by comparing time information from different clock sources. NTP synchronizes computer systems in a network using high-precision clocks such as GPS, atomic clocks, etc., and provides precise time synchronization. NTP can be used globally and supports a variety of network protocols such as UDP, TCP, etc.

If you have a dedicated NTP server in your network, configure and prioritize it to the top of the NTP server list. Or if you don't have a dedicated one, add an available NTP server and prioritize it to the top of the NTP server list.

Once the NTP server is configured, the DAP847-XXA in the cluster synchronizes system time with the NTP server every 15 minutes.

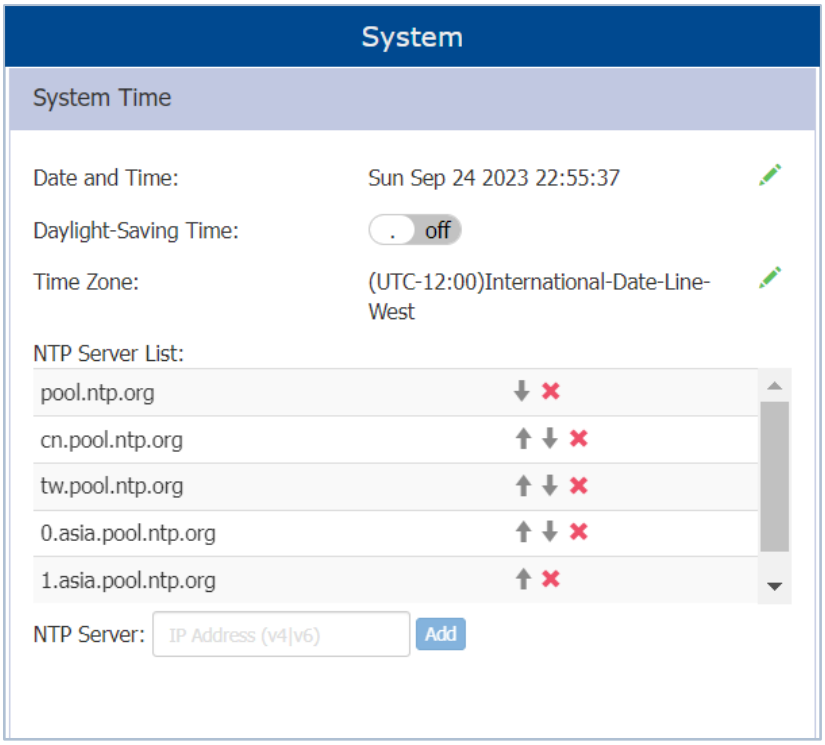


Figure 130: System time configuration with Daylight-Saving Time off

You can also specify the **“Daylight-Saving Time”** and **“Time Zone”** of the DAP847-XXA cluster to coordinate with the local time. “**Daylight-Saving Time”** is automatically enabled in the supporting time zone. See Figure 131.

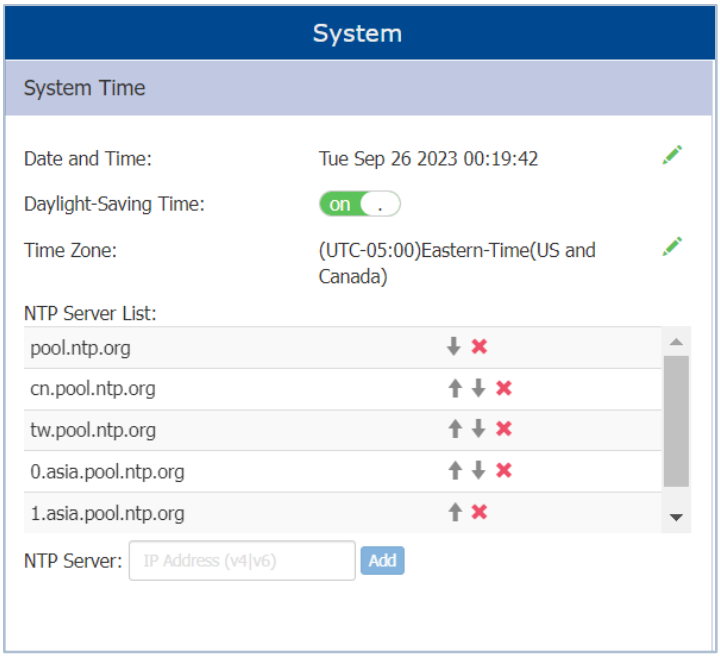


Figure 131: System Time Configuration with Daylight-Saving Time on

Note: Hirschmann IT recommends checking the reachability before you add an NTP server for time synchronization. If the NTP server is not configured or unreachable, rebooting the DAP847-XXA will cause a time change.

8.6 Syslog configuration

Syslog is a standard protocol for system logs, usually used to record system and application log information. It is widely used in network devices, operating systems, and applications to collect, record, and transmit log data for system management and troubleshooting.

Syslog transmits logs using the UDP protocol. The default port is usually 514. Syslog supports multiple message formats and priorities. It can also filter and selectively log according to its importance and message types.

Through Syslog, administrators can monitor system status in real-time, track the running status of applications, discover security events and conduct audits, etc.

Navigate to **System** → **Syslog & SNMP** → **Syslog** to view system logs.

Logs of the DAP847-XXA follow the standard of Syslog. You can view logs and configure corresponding attributes on the Syslog page. The upper part of the Syslog window displays the **"Error"** generated by the DAP847-XXA cluster and the Syslog information above this level.

- **Title**: The content of the log message.
- **Level**: The severity of the log message.
- **Source**: IP address of DAP847-XXA that generates logs.

When you hover your mouse cursor over a certain row of log messages, the log generation time will be displayed, see Figure 132.

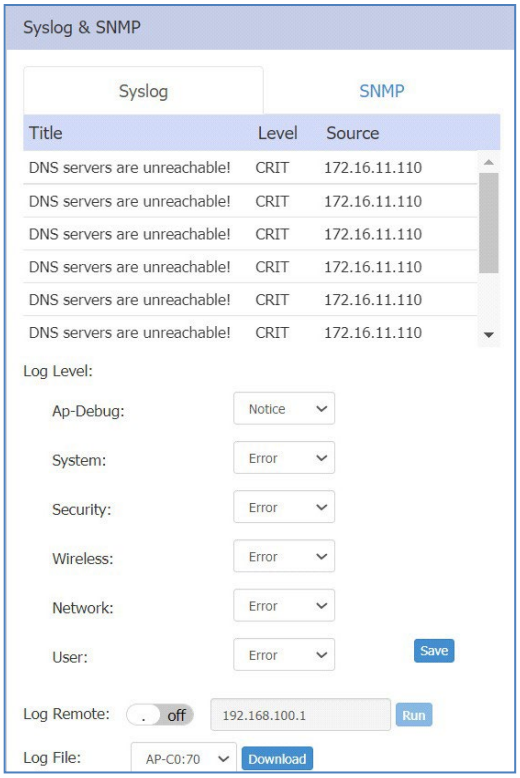


Figure 132: Syslog configuration

Log level

The log level is the severity setting of the Syslog message. If a level is specified, the DAP847-XXA cluster will generate Syslog messages for that level and higher level. This means:

- If Syslog messages are configured according to different severities, Warning level entries will also be included in entries of Notice, Info, and Debug levels.
- Notice is the default level of the Syslog, and the system generates logs including levels of Notice, Warning, Error, Critical, Alert, and Emergency.

Users can specify different log levels for different modules.

Parameter	Description
AP-Debug	Detailed log about the DAP847-XXA.
System	AP configuration and system status log.
Security	Network security log.
Wireless	Wireless RF log.
Network	Network state change log.
User	User log.

Log remote

DAP847-XXA supports configuring a remote log server for receiving and storing Syslog messages sent by DAP847-XXA.

Note: Syslog is divided into 8 levels, and the highest level 0 is Emergency severity while the lowest level 7 is Debug severity. Syslog severity is defined as follows:

Level	Severity	Keywords	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

Table 13: Syslog severity definition

8.7 SNMP configuration

SNMP (Simple Network Management Protocol) is a standard protocol of network management. It is used to manage and monitor network devices in a network system to ensure its reliability and stability.

SNMP defines ways of communication between the Network Managing Station (NMS) and the SNMP agent. NMS is an administrator computer used to manage and monitor a network. The agent is an application program that runs on a DAP847-XXA to collect the status and performance of the device and send it to NMS.

There are 3 versions of SNMP, SNMPv1, SNMPv2c, and SNMPv3.

- SNMPv1 is the earliest version providing basic network management functions but is less secure.
- SNMPv2c is an improved version of SNMPv1 and adds community concept and improves security.
- SNMPv3 introduces User-based Security Model (USM), which facilitates a higher level of security.

Currently, DAP847-XXA supports SNMPv2c and SNMPv3. SNMPv1 is not supported by DAP847-XXA due to its low security.

SNMP Trap is a notification protocol used to generate notifications on managed devices to inform the network management system (NMS) of specific events or errors without having to wait for the NMS to poll again.

For configuration of related parameters, navigate to **System → Syslog & SNMP →SNMP**.

8.7.1 Configure SNMPv2c

You can configure the following parameters for SNMPv2c:

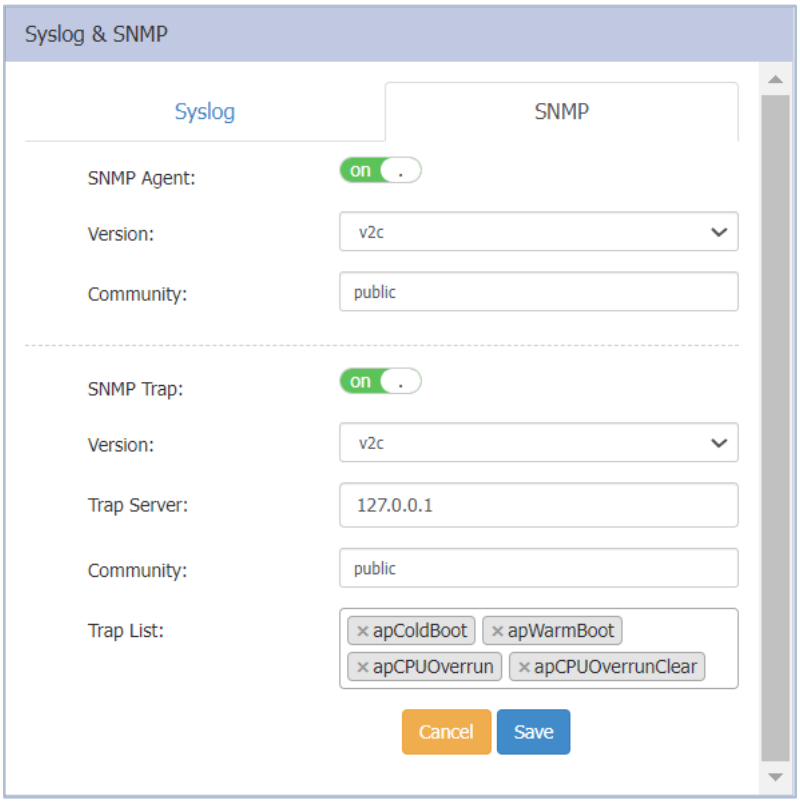


Figure 133: SNMPv2c configuration

The key parameters are described as follows:

Configure SNMPv2c Agent

Parameter	Description
SNMP Agent	Enables or disables the SNMP Agent on DAP847-XXA.
Version	Selects the required SNMP version of v2c.

Parameter	Description
Community	The credential used to communicate between SNMP Agent and the network management system (NMS). The value needs to be the same for DAP847-XXA and NMS to communicate.

Configure SNMPv2c Trap

Parameter	Description
SNMP Trap	Enables or disables DAP847-XXA to send a trap to the network management system (NMS).
Version	Selects the required SNMP trap version of v2c.
Trap Server	Network management system (NMS) that receives SNMPv2c trap.
Trap List	Specifies the type of trap to send.

8.7.2 Configure SNMPv3

You can configure the following parameters for SNMPv3:

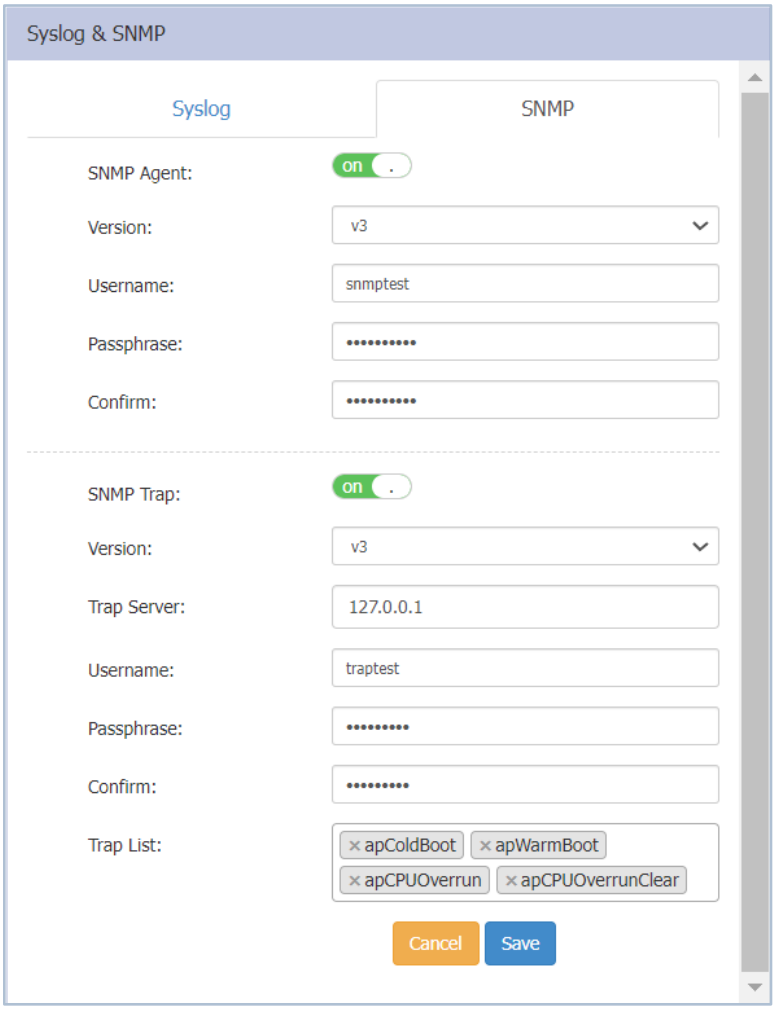


Figure 134: SNMPv3 configuration

The key parameters are described as follows:

Configure SNMPv3 Agent

Parameter	Description
SNMP Agent	Enables or disables the SNMP Agent on DAP847-XXA. The network management platform can fetch information from DAP847-XXA through the SNMP protocol.
Version	Selects the required SNMP version of v3.
Username	Identifies and authenticates users of SNMP management systems.
Passphrase	Passphrase used to authenticate SNMPv3. The authentication password must contain at least 8 characters except space.
Confirm	Confirms the password.

Configure SNMPv3 Trap

Parameter	Description
SNMP Trap	Enables or disables DAP847-XXA to send a trap to the network management system (NMS).
Version	Selects the required SNMP trap version of v3.
Trap Server	Network management system (NMS) that receives SNMPv3 trap.
Username	Indicates the username sending the trap.
Passphrase	Passphrase used to authenticate SNMPv3. The authentication password must contain at least 8 characters except space.
Confirm	Confirms the password.
Trap List	Specifies the type of trap to send.

9 Wireless management

The Wireless window is used to display wireless statistics and configuration of DAP847-XXA, as well as advanced functions related to the Radio level: RF, wIDS/wIPS (Wireless Intrusion Detection System/Wireless Intrusion Prevention System), and Performance Optimization.

Figure 135: Wireless page

This chapter includes the following 3 topics:

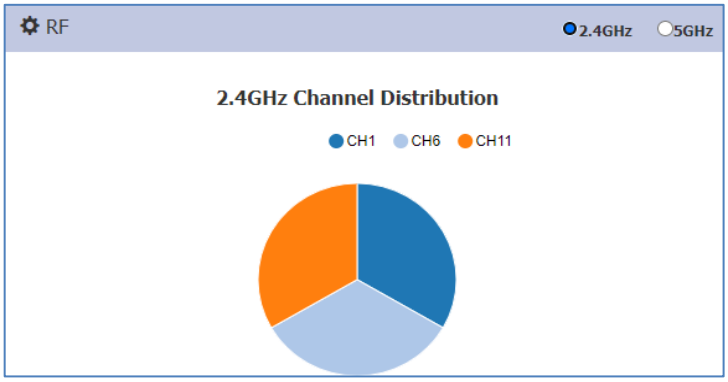
- RF configuration
- wIDS/wIPS
- Performance Optimization

9.1 RF configuration

The RF window is used to monitor the wireless utilization and configure wireless attributes, such as channel, Short GI, and transmitting power.

There are 2 modes for the RF window: Basic Mode and Advanced Mode. Click the RF window to switch to the Advanced Mode from the Basic Mode. In Advanced Mode, global RF configuration can be set for DAP847-XXA clusters. RF configuration for each DAP847-XXA can also be set as needed.

The Basic Mode shows the monitoring information of channel distribution of 2.4 GHz or 5 GHz band. Different colors are used for different channels. When you hang the mouse cursor over the section of the pie chart, it shows the clients connected to the AP cluster of the bands 2.4 GHz or 5 GHz.



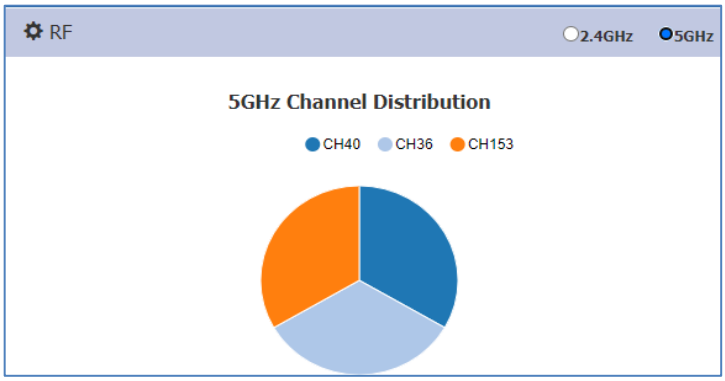


Figure 136: RF configuration

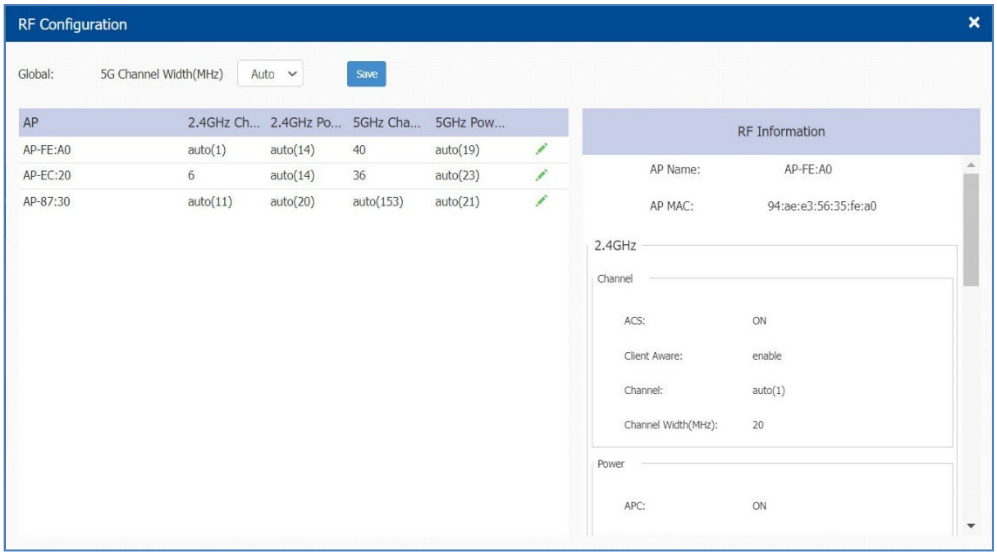


Figure 137: RF configuration window

The RF Configuration window shows the working channel list and transmit power of the DAP847-XXA in the cluster. When you select a DAP847-XXA on the list, it shows the detailed RF information in the column on the right-hand side, including channel, power, channel width, etc.

The global configuration can be used to change the 5 GHz channel width for any DAP847-XXA devices in the cluster, see Figure 138. You can also change the channel width for a specific DAP847-XXA by individually editing it, see Figure 142.

The individual configuration for a DAP847-XXA will take effect if both global and individual configurations exist.

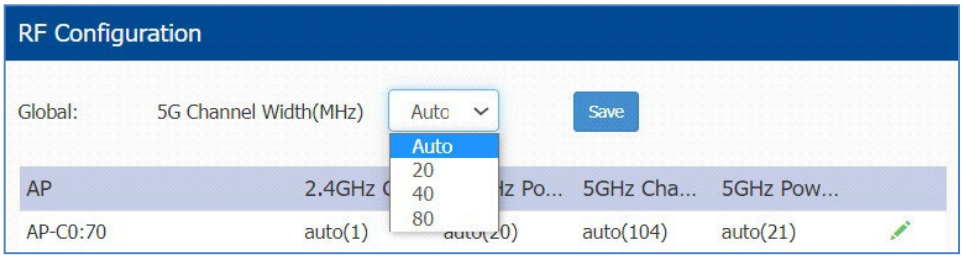


Figure 138: Global 5G channel width configuration

Note: The channel width for 160 MHz cannot be configured globally. Due to restrictions such as the supported AP model, scope of supported channel and power supply, it needs to be set individually.

9.1.1 Modify DAP847-XXA transmit power and channel

You can modify the transmit power and working channel for the DAP847-XXA in the RF Configuration window, see Figure 139. By default, the working channel and transmit power are automatically managed by Dynamic Radio Management (DRM) technology to dynamically manage and optimize the performance of the wireless system. It improves the efficiency and reliability of wireless systems by monitoring the wireless environment and system load in real-time and making decisions based on this information.

If you want to modify the values of the working channel and transmit power on a DAP847-XXA 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.

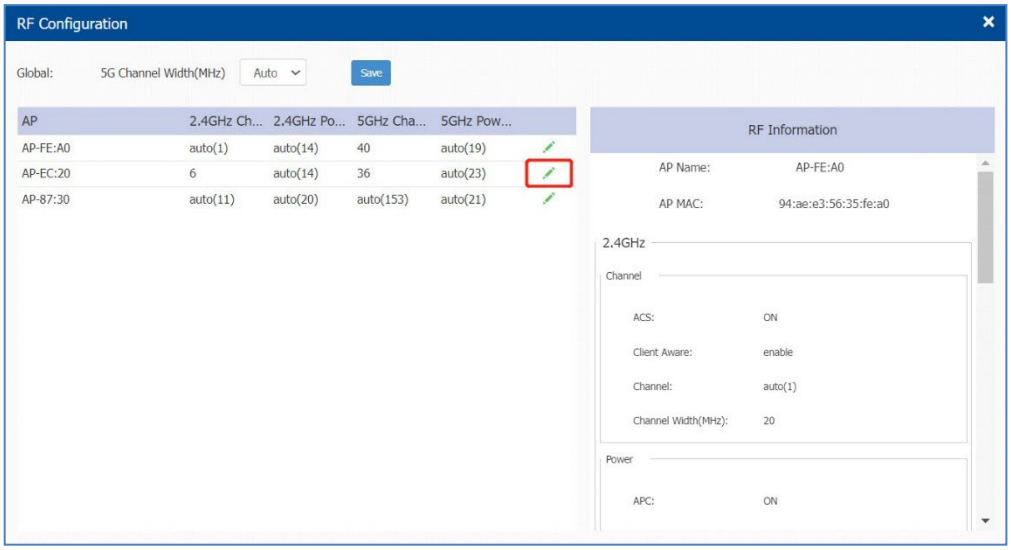


Figure 139: RF Configuration

To reduce the potential risk of low power transmitting or DFS channel conflict, specify the channel list or the auto power range. This can improve performance for specific scenarios, see Figure 140.

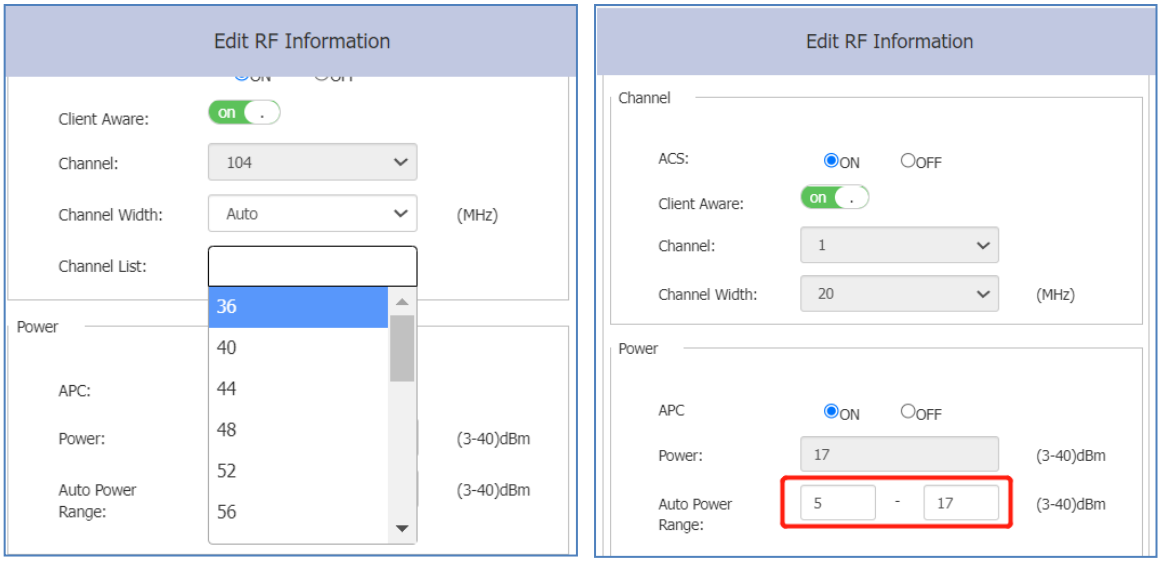


Figure 140: Specify channel list and auto power range

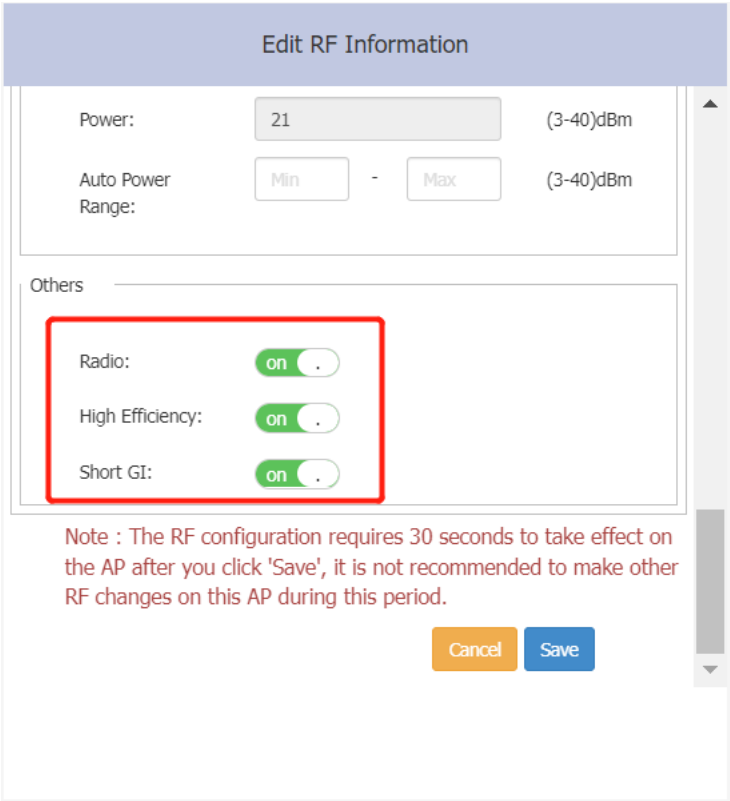


Figure 141: RF information – Others

Parameter description in RF Configuration window

Parameter	Description
Client Aware	If **"Client Aware"** is enabled, Auto Channel Selection does not change channels for DAP847-XXA devices with connected clients, except for high-priority events such as RADAR detected. If it is disabled, the DAP847-XXA may change to a more optimal channel, which may temporarily disrupt current client traffic.
Radio	Enables or disables Radio, and it can be configured for 2.4 GHz and 5 GHz respectively.
Short GI	Enables or disables the Short Guard Interval. In IEEE 802.11 OFDM based communications, the guard interval is used to verify that distinct transmissions are occurred between the successive data symbols which is transmitted by a device. The standard symbol guard interval used in IEEE 802.11 OFDM is 800 nanoseconds in duration. To increase data rates, the IEEE 802.11n 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 detection 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 GI" is enabled on the wireless radio. If the multipath effect is too serious (too many metals or other reflecting materials), it is recommended to disable the Short Guard Interval.
High Efficiency	Enables or disables the IEEE 802.11ax function. When it is disabled, the DAP847-XXA is switched to IEEE 802.11ac to avoid possible compatibility issue with some older IEEE 802.11ac devices.

Table 14: Parameter description in RF Configuration window

9.1.2 Configure channel width

DAP847-XXA supports 20 MHz, 40 MHz, 80 MHz, and 160 MHz channel width and it can be set individually in RF information, see Figure 142.

Note: 160 MHz has the following limitations:

- 160 MHz is only supported on 5 GHz radio with channel range 36 … 64, and 100 … 128.
- 160 MHz is only supported when AP is powered by a DC power injector or POE+ (or higher).
- Only static 160 MHz channel width is supported. Auto channelselection does not use 160 MHz channels.

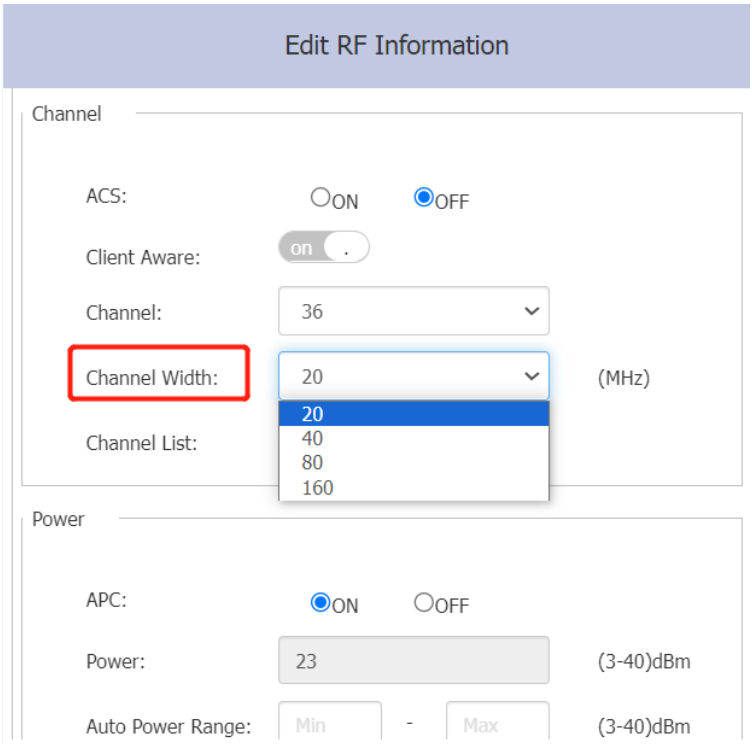


Figure 142: Configure channel width to 160 MHz

9.1.3 Configure DAP847-XXA Antennas

On the RF Configuration page, you can configure the gain of the DAP847-XXA antennas and the MIMO mode on the 5G Radio, as shown in Figure 143.

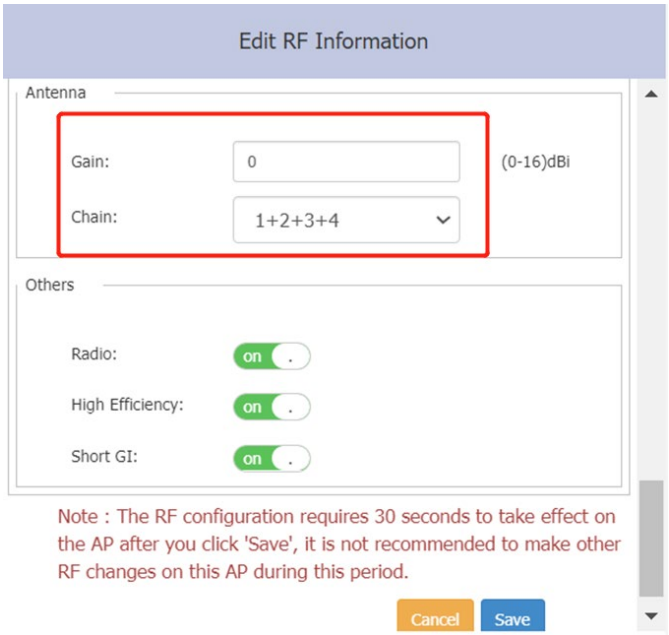


Figure 143 DAP847-XXA Antenna Configuration

Configure Antennas

Parameter	Description
Gain	Specifies the gain value of the external antenna.
Chain	Indicates the MIMO mode of the DAP847-XXA. The configuration of the external antennas is as follow:
	1 represents MIMO mode 1x1, corresponding to antenna interface ANT1
	2 represents MIMO mode 1x1, corresponding to antenna interface ANT2
	3 represents MIMO mode 1x1, corresponding to antenna interface ANT3
	4 represents MIMO mode 1x1, corresponding to antenna interface ANT4
	1+2 represents MIMO mode 2x2, corresponding to antenna interfaces ANT1+ANT2
	1+4 represents MIMO mode 2x2, corresponding to antenna interfaces ANT1+ANT4
	1+2+3 represents MIMO mode 3x3, corresponding to antenna interfaces ANT1+ANT2+ANT3
	1+2+3+4 represents MIMO mode 4x4, corresponding to antenna interfaces ANT1+ANT2+ANT3+ANT4

9.1.4 Turn on/off DAP847-XXA radio

You can turn off the 2.4 GHz or 5 GHz wireless radio module of the DAP847-XXA device in the cluster by clicking the Radio on/off button to reduce the radio emissions or for other purposes, see Figure 144.

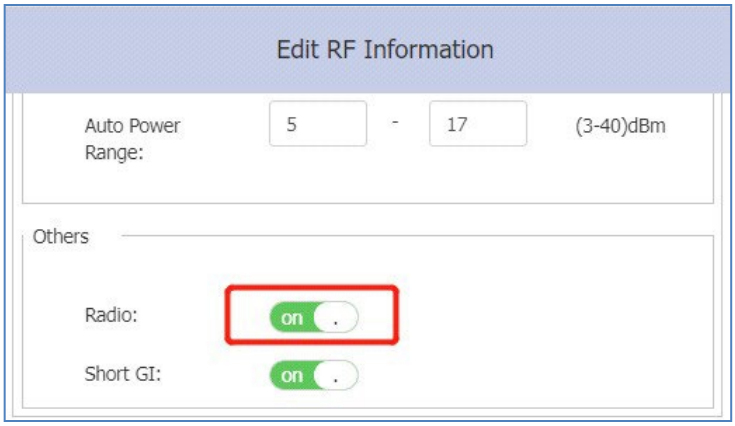


Figure 144: Turn on/off radio

9.2 wIDS/wIPS

DAP847-XXA provides the basic wIDS/wIPS functions in the Cluster mode. Hirschmann IT recommends using the DAC mode and purchasing relevant licenses for advanced functions.

- **wIPS**: wIPS (Wireless Intrusion Prevention System) is a system for detecting and defending against security threats in wireless networks. It monitors and analyzes transmission data from wireless networks in real time, detects and blocks malicious attacks and unauthorized access against wireless networks. wIPS is a layer 2 protocol detection and protection function developed for the IEEE 802.11 protocol. The wIPS detects wireless behaviors or devices that threaten network security, interfere with network services, and affect network performance through channel monitoring, analysis, and processing. It provides countermeasures against invading wireless devices and a complete set of security solutions for wireless networks.
- **wIDS:** wIDS (Wireless Intrusion Detection System) is a system used to detect possible security threats in a wireless network. It detects any unauthorized access, malicious attacks or unusual behavior by analyzing the transmission data of the wireless network. Unlike wIPS, which focuses on detecting potential threats, wIDS focuses more on defending and stopping those threats. wIDS can detect malicious users' unauthorized access and intrusions early. It also protects enterprise networks and users from unauthorized devices on wireless networks. wIDS can monitor the wireless network without reducing network performance and provides real-time prevention against various unauthorized accesses.
- **Rogue Suppress:** DAP847-XXA supports preventing the connections between clients and rogue APs by sending a de-authentication frame with the client's MAC address to the rogue AP. It can disconnect the clients, which are already connected to the rogue AP. If a known AP is confirmed as non-interfering or a legal AP, you can click **"Trust"** on the list, see Figure 145, and add the AP to the Allowlist. By default, this function is disabled, see Figure 146.

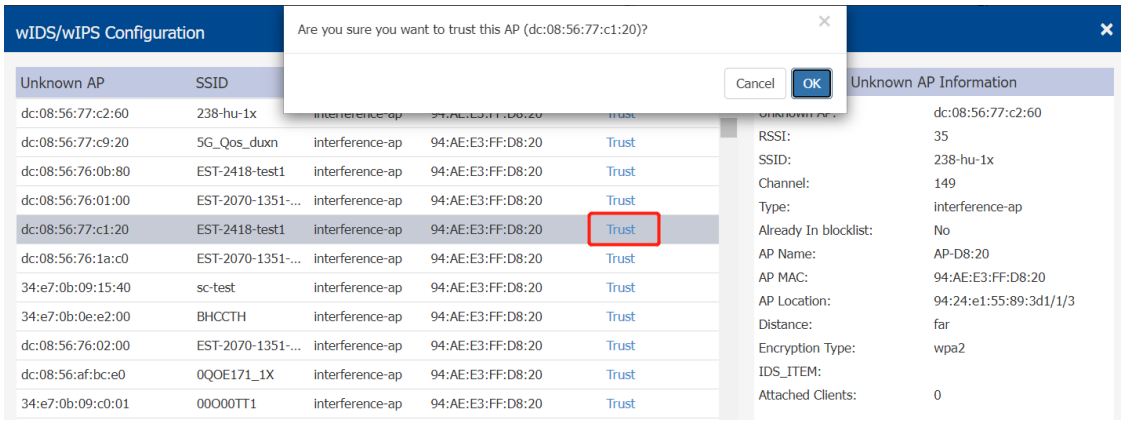


Figure 145: Trust AP

- **Dynamic Blocklist:** If the Dynamic Blocklist is enabled, the detected ad-hoc devices will be added to the DAP847-XXA blocklist automatically. This prevents the ad-hoc devices from changing their role to a client and gaining access to the DAP847-XXA wireless network. By default, the ad-hoc device is not added to the blocklist automatically, see Figure 149.
- **Wireless Attack Detection:** If the Wireless Attack Detection is enabled, the DAP847-XXA will detect unauthorized accesses originating from foreign APs. By default, it is disabled, see Figure 146.

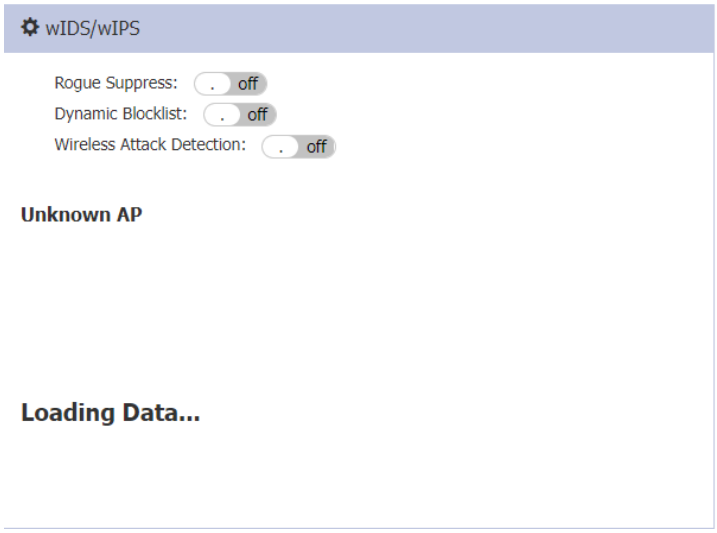


Figure 146: wIDS/wIPS window

- **Rogue AP:** Rogue APs are unauthorized wireless APs usually built by employees without authorization to provide wireless access. Since these APs are not formally authorized, they can pose a threat to an organization's

network security. Rogue APs can be exploited by malicious attackers for sensitive information, cyberattacks, etc. For example, an unauthorized AP plugged into the wired side of the network or a foreign interfering AP broadcasting the same SSID with the DAP847-XXA cluster. A rogue AP is considered as a security threat to the DAP847-XXA cluster.

- **Interfering AP:** An AP seen in the wireless environment but not connected to the wired network. The interfering AP potentially provides RF interference. However, it is not considered as 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 detected by Background Scanning and listed on the unknown AP list. However, some detected foreign APs are trusted APs, and they 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, see Figure 147. If a foreign AP MAC address is added to the Allowlist, then it will not be shown in the unknown AP list.

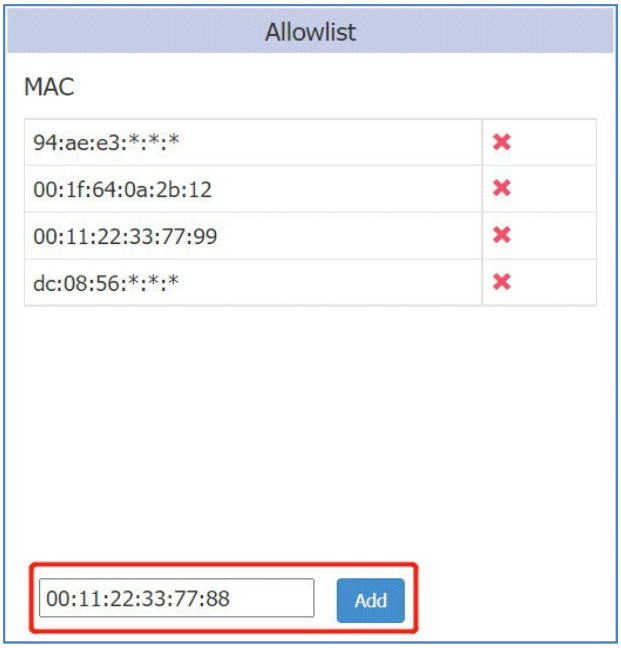


Figure 147: AP allowlist tab

After clicking the wIDS/wIPS window, you can see the list of information for the interfering APs and rogue APs on the wIDS/wIPS Configuration page, including further details on Interfering APs and Rogue APs, such as RSSI, Channel, and Encryption Type, as shown in Figure 148.

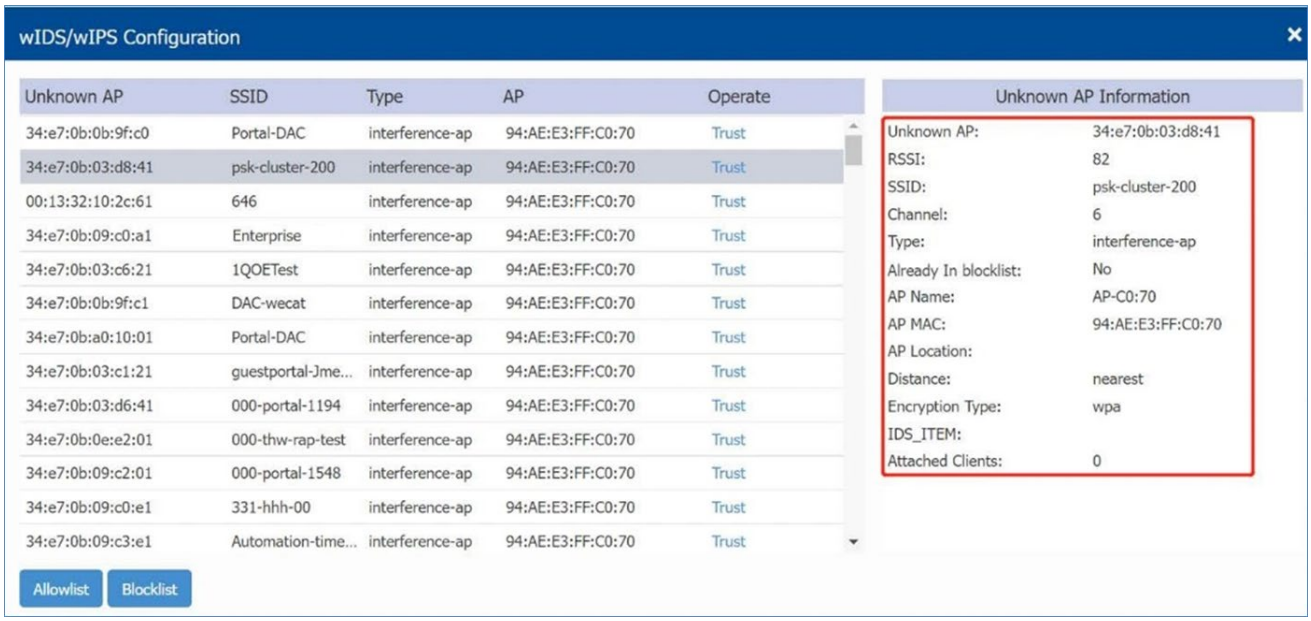


Figure 148: wIDS/wIPS Configuration window

Parameter	Description
Unknown AP	The MAC address of the unknown AP
SSID	SSID broadcasted by the unknown AP
Type	The classified result of the unknown AP (interfering AP or rogue AP)
RSSI	The RSSI of the unknown AP
Channel	The working channel of the unknown AP
Already In Blocklist	The flag of ad-hoc devices, depending on whether the **"Dynamic Blocklist"** is on. If it is on, the ad-hoc devices will be automatically added to the Blocklist, and the flag is true (Yes). If it is off or the unknown AP in list is not an ad-hoc device, the flag is false (No).
AP Name	The name of the DAP847-XXA in the cluster that detects the unknown AP
AP MAC	The MAC address of the DAP847-XXA in the cluster that detects the unknown AP
AP Location	The location of the DAP847-XXA in the cluster that detects the unknown AP
Distance	The distance between the unknown AP and the detecting DAP847-XXA in the cluster. It is measured by RSSI of the unknown AP: ▶ Nearest – RSSI≥(-20 dBm) ▶ Near – (-45 dBm) ≤RSSI<(-20 dBm) ▶ Far - (-70 dBm)<RSSI<(-45 dBm) ▶ Farthest - RSSI≤(-70 dBm)
Encryption Type	The encryption type of the SSID broadcasted by the unknown AP.

Parameter	Description
IDS_ITEM	Specific behavior or an event identified and flagged by the wIDS system that is a potential wireless network security threat or risk, such as: ▶ AP Spoofing ▶ Broadcast De-authentication ▶ Broadcast Disassociation ▶ Ad-hoc Network Using Valid SSID ▶ Long SSID ▶ AP Impersonation ▶ Ad-hoc Network ▶ WDS-Wireless Bridge ▶ Null Probe Response ▶ Invalid Address Combination ▶ De-authentication Reason Code Invalid ▶ Disassociation-Reason Code Invalid ▶ Valid Client Mis-associaton ▶ Omerta Attack ▶ Unencrypted Valid Clients ▶ IEEE 802.11n 40 MHz Intolerance Setting ▶ Active IEEE 802.11n Greenfiled-Mode ▶ DHCP Client ID ▶ DHCP Conflict ▶ DHCP Name Change ▶ Channel Change ▶ Invalid-MAC OUI ▶ Valid SSID Misuse ▶ Malformed Frame-Assoc Request ▶ Frequent Certification
Attached Clients	The number of clients attached to the unknown AP, and MAC of each client.

▶ **Blocklist:** Blocklist can add only Rogue APs. If a Rogue AP is added to the Blocklist, it cannot change its role to act as a client and access the DAP847-XXA wireless network, see Figure 149.

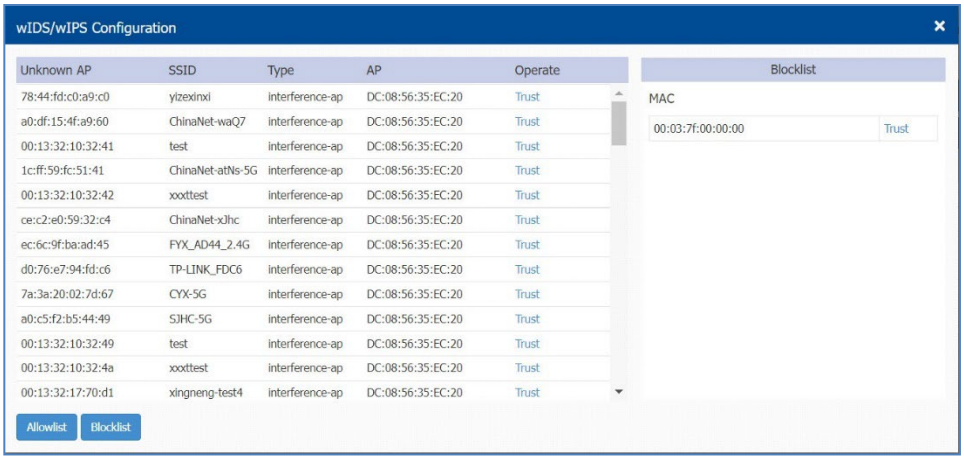


Figure 149: Add to blocklist

Parameter	Description
Operate	The operation of trusting an external AP and removing it from the unknown AP list. If the external AP is trusted, its MAC address will be added to the Allowlist.
Allowlist	List of external APs which is not considered as security threat to the DAP847-XXA. You can add the trusted MAC address into the Allowlist manually.
Blocklist	The Blocklist of foreign APs classified as rogue APs and pretending as a client to access the DAP847-XXA. If the Blocklist is on and ad-hoc devices are detected, all of them will be automatically added to the Blocklist. You can remove a foreign AP from the Blocklist by the Trust operation.

Note: Background Scanning needs to be enabled for wIDS/wIPS function. Hirschmann IT recommends setting the Background Scanning interval to less than 1 minute in scenarios that require a higher level of security for better detection efficiency and performance.

9.3 Performance Optimization

Wireless Performance Optimization is used to improve 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 functions, see Figure 150.

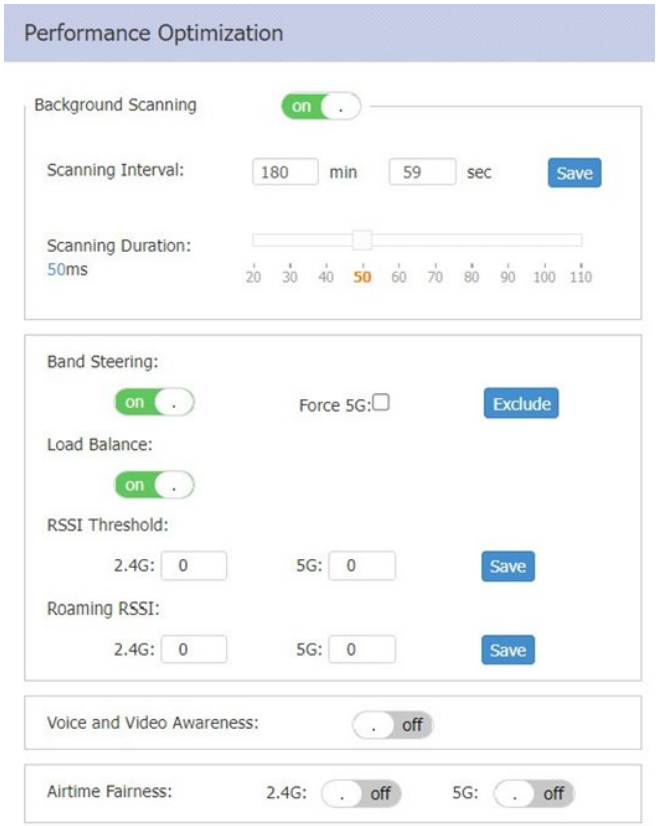


Figure 150: Wireless optimization window

- **Background Scanning**: Wireless networks operate in environments where electrical and radio frequency devices may be present and interfere with network communications. Microwave ovens, cordless phones, and even adjacent Wi-Fi networks are all potential sources of continuous or intermittent interference. Background Scanning is used to examine the RF environment in which the Wi-Fi network is working, identify interference and classify its sources.

  Background Scanning is the basis for some advanced features such as wIDS/wIPS, APC, etc. When it is turned off, the external AP detection and rogue suppression stops, and the precision of DRM reduces. By default, Background Scanning is enabled.

The interval of Background Scanning can be configured from 5 seconds to 180 minutes according to deployment requirements. For highly sensitive packet delay cases, the default value of 20 seconds is recommended as the interval. If the interval is longer than 1 minute, it will impact the accuracy of the wIPS feature.

Note: A dedicated scanning radio named **"athmon2"** is reserved for DAP847-XXA for the background scanning for both 2.4 GHz channels and 5 GHz channels.

- **Band Steering:** Band steering supports two cases: Prefer 5G and Force 5G.
  - **Prefer 5G:** It prioritizes assigning the dual-band clients to the 5 GHz bands compared to the 2.4 GHz band. This can reduce co-channel interference and increase available bandwidth for clients because there are more available channels on the 5 GHz band. By default, the Band Steering is enabled. When Band Steering is enabled and Force 5G is disabled, DAP847-XXA is working in the Prefer 5G mode.

    Prefer 5 GHz is based on channel utilization and client density. When the 5 GHz band is busy and connected with too many clients, a new client will connect to the 2.4 GHz frequency band where the channel is relatively idle.
  - **Force 5G:** DAP847-XXA forces dual-band clients to connect to the 5 GHz frequency band. After turning on this function, wireless clients in dual-band working mode are not allowed to connect to 2.4 GHz frequency band. The clients who only support 2.4 GHz are allowed to connect to the 2.4 GHz frequency band. When Band Steering is enabled and Force 5G is selected, DAP847-XXA works in the Force 5G mode.
- **Exclude**: It excludes the dual-band clients from the Band Steering. DAP847-XXA allows them to choose a wireless band freely. Users can add a MAC address of the terminal or MAC OUI to exclude specific terminals from the Band Steering.
- **Load Balance:** It is a network optimization technology that can balance load among DAP847-XXA devices, ensure the performance of each device and ensure enough bandwidth for wireless clients.

  It provides a fair distribution of clients among neighboring DAP847-XXA devices. Based on the client density, channel utilization and client's RSSI

value on associated DAP847-XXA devices, wireless clients are steered from a busy device to an idle one. The threshold for the client density is 10, and the channel utilization is 70% for both 2.4 GHz and 5 GHz. Load Balanceis enabled by default.

- **RSSI Threshold:** It is used for wireless access control. **“RSSI threshold”** only works during the association procedure of the clients. If the RSSI value of the clients is lower than the **“RSSI threshold”**, DAP847-XXA will not respond to the clients. It is not affected whether IEEE 802.11kv is enabled or not. Clients with a lower RSSI value than the threshold are unauthorized to access. By default, RSSI threshold is disabled (0). RSSI threshold can be applied to the 2.4 GHz band or 5 GHz band separately. Hirschmann IT recommends deploying the RSSI threshold in high-density scenarios, RSSI range of 25 … 35.
- **Roaming RSSI:** When it is enabled, it forces the clients with a lower RSSI value to roam. Roaming RSSI is mainly used along with IEEE 802.11k and IEEE 802.11v to control and guide the roaming process for wireless clients.
  - When IEEE 802.11k and IEEE 802.11v are enabled on WLAN, “Roaming RSSI Threshold” triggers message exchange of IEEE 802.11k and IEEE 802.11v between the DAP847-XXA and the wireless client.
  - When the DAP847-XXA detects the RSSI value of a wireless client lower than the “Roaming RSSIThreshold”, it sends an IEEE 802.11k event to that client. If that client supports IEEE 802.11k, it will respond to DAP847-XXA with a packet containing the RF scan information from the client.
  - Based on received data, DAP847-XXA calculates the best BSSID for roaming of the client, and sends to that wireless client the best SSID message through the IEEE 802.11v event.
  - That wireless client decides whether to roam. If it roams, it decides either to obtain a target BSSID from the IEEE 802.11v event sent by the DAP847-XXA, or another BSSID outside the recommended range of the DAP847-XXA to roam.

  By default, roaming RSSI is disabled (0). Roaming RSSI can be applied to the 2.4 GHz band or 5 GHz band separately.
- **Voice and Video Awareness:** Background Scanning enables awareness of existing traffic types on the DAP847-XXA. If there is an ongoing voice or video

service, Background Scanning stops to ensure traffic with higher priority is uninterrupted. It resumes Background Scanning when there is no active voice or video traffic. This feature is disabled by default.

- **Airtime Fairness:** DAP847-XXA distributes the wireless transition time slice equally, even with traditional low-speed clients that only support IEEE 802.11a, IEEE 802.11g, or IEEE 802.11n are present. It can effectively balance the load of wireless APs and ensure that each client can get a fair allocation of bandwidth, improving the performance and availability of the entire wireless network. Airtime fairness is disabled by default.

10 Access

The Access window includes function configurations of authentication and access control. It is mainly used for user access management, including Authentication, Blocklist, Allowlist, and ACL.

This chapter contains the following topics:

- Authentication
- Login captive portal
- Account and access code management
- Customize portal page
- Client blocklist for wireless access
- Client allowlist for captive portal
- Walled garden
- Multicast control
- ACL

10.1 Authentication

There are two modes of the Authentication window:

- Authentication window
- Authentication Configuration window. Click the Authentication window to switch to the Authentication Configuration window.

The Authentication window shows the statistics about wireless clients and the Operating System (OS), see Figure 151. When you hang the mouse cursor over a certain pie-chart sector, it shows the number of relevant devices, see Figure 152.

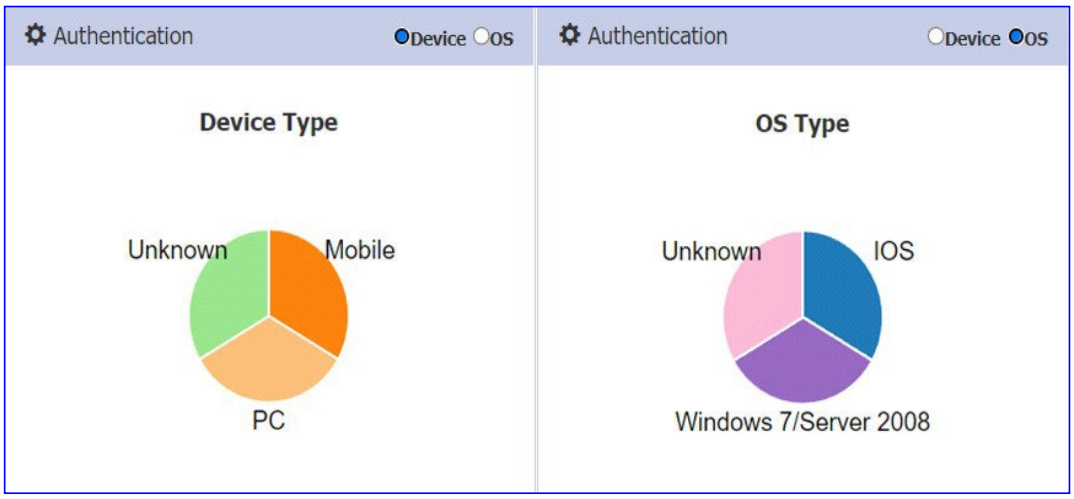


Figure 151: Authentication window

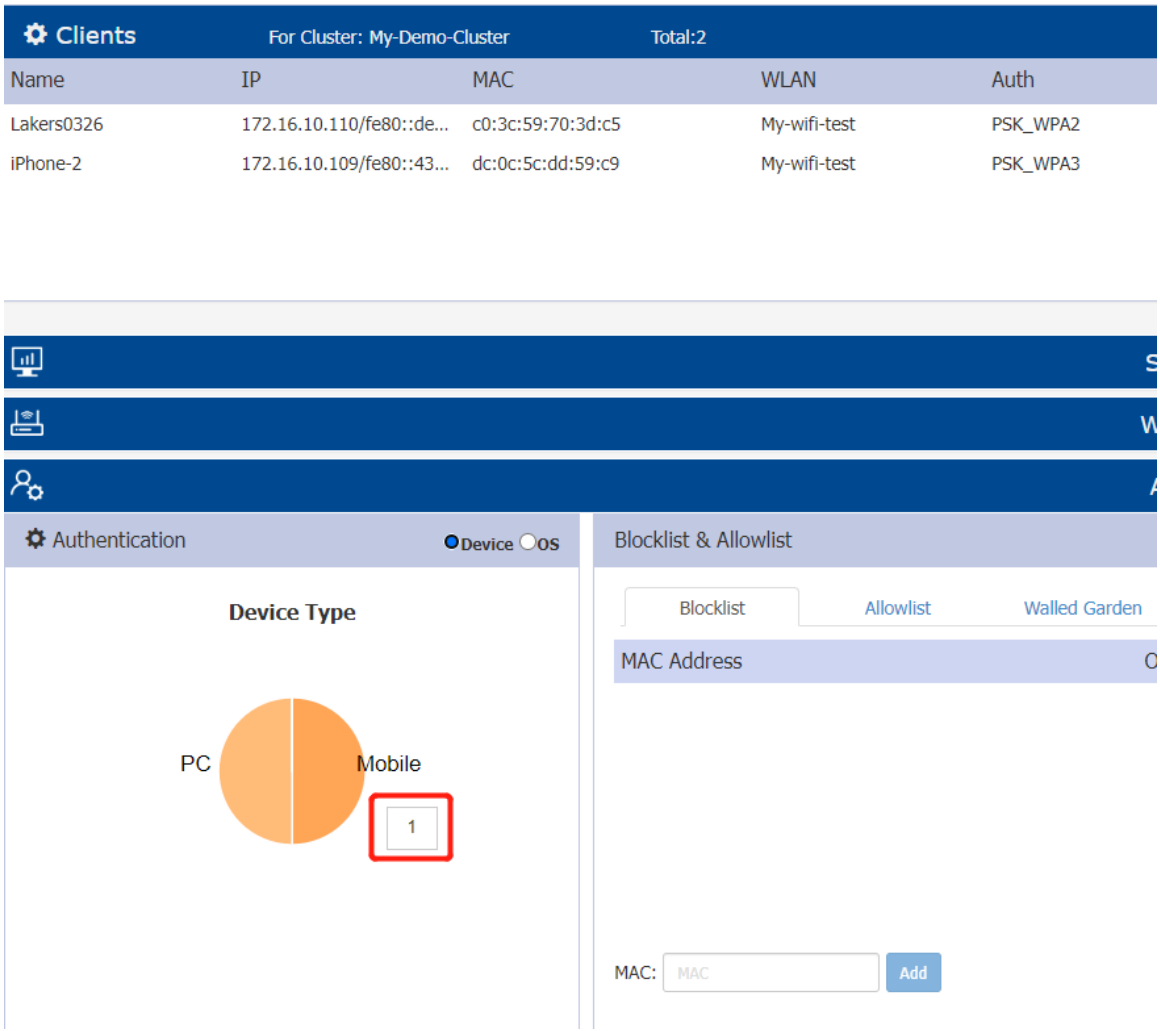


Figure 152: Device Type

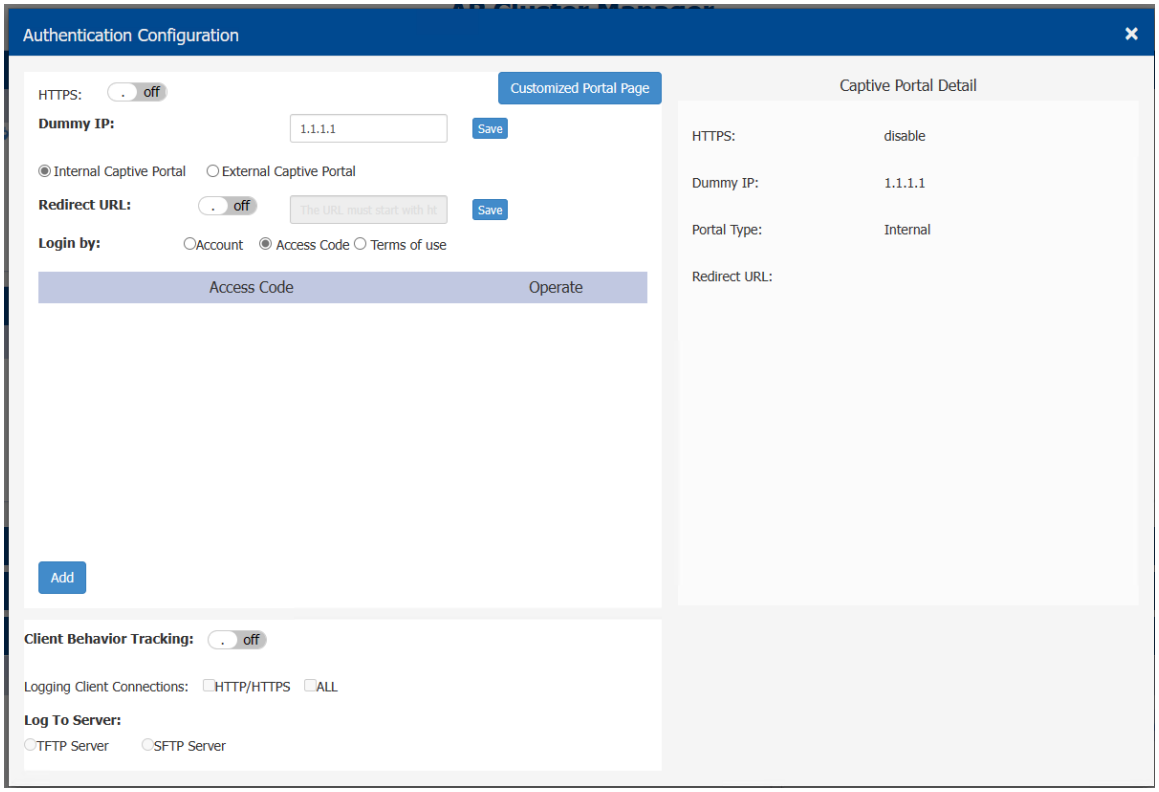


Figure 153: Authentication configuration window

You can configure other parameters required for Portal authentication according to the needs of actual business scenarios. The parameter description in the Authentication Configuration window is as follows:

Parameters	Description
Login by	Portal login authentication method: Account, Access Code and Terms of use.
Dummy IP	The IP address of the captive portal FQDN, the default is 1.1.1.1.
Client Behavior Tracking	Tracks client behavior and sends users' URL access records through SFTP or TFTP.
Logging Client Connections	▶ **HTTP/HTTPS:** Records the HTTP/HTTPS web session of wireless clients. ▶ **ALL:** Records the HTTP/TCP/UDP sessions of wireless clients.
Log to Server	▶ **TFTP Server:** Uploads log files of client connection information to a specific TFTP server. ▶ **SFTP Server:** Uploads log files of client connection information to a specific SFTP server.

10.2 Login captive portal

There are 3 login methods for the captive portal authentication for a portal WLAN, **Account**, **Access Code**, and **Terms of use**. Account is used by default, see Figure 154. To create a Captive Portal WLAN, see “WLAN security types” on page 52.

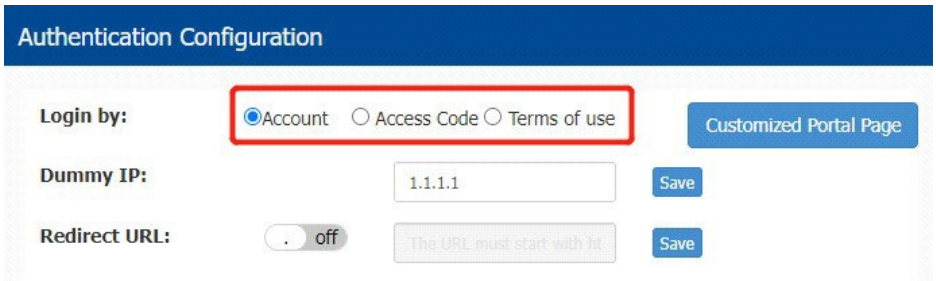


Figure 154: Choose your login method

Log in by Account:

- ☐ Select **“Account”** as the login method.
- ☐ Create a Captive Portal authentication account by Administrator or Guest Manager.
- ☐ When the wireless client is connected to WLAN, enter the **“Username”** and **“Password”** in the Portal authentication pop-up page.

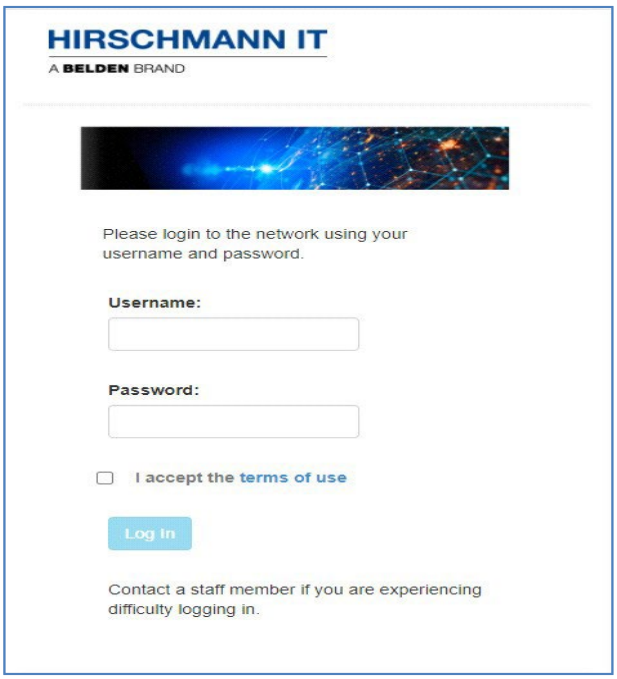


Figure 155: Login by username and password

Login by Access Code:

- ☐ Select **“Access Code”** as the login method.
- ☐ Create the **“Access code”** by Administrator or Guest Manager.
- ☐ When the wireless client is connected to WLAN, enter the **“Access code”** in the Portal authentication pop-up page.

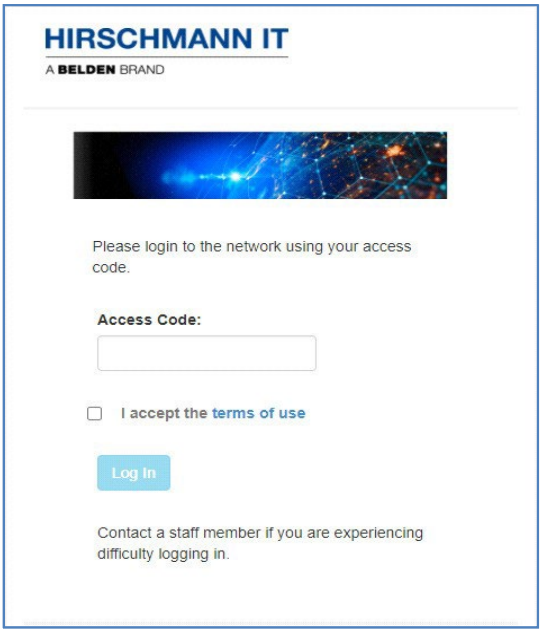


Figure 156: Login by access code

Login by Terms of use

- ☐ Select **“terms of use”** as the login method.
- ☐ When the wireless client is connected to WLAN, select the **“I accept the terms of use”** in the Portal authentication pop-up page.

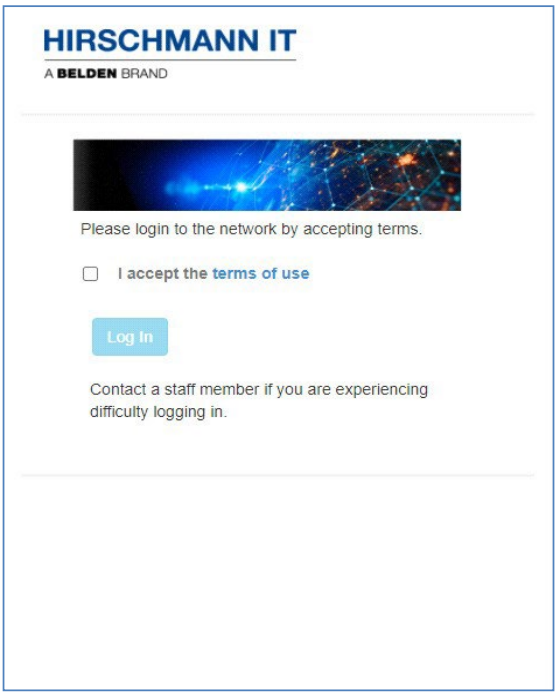


Figure 157: Login by terms of use

10.3 Account and access code management

Only users in the local user database support logging in by Account or Access Code for the captive portal authentication. External authentication servers are not supported (for example Windows server as a RADIUS server). You can add Account or Access Code to the local user database.

Add an account

- ☐ Select **“Account”** as the login method.
- ☐ Click **“Add”** button on the Authentication Configuration page.
- ☐ Fill in user information in **“Add Local Auth User”** on the right-hand side. The fields with **“*”** are mandatory, see Figure 158.

To view the detailed information of a user, click the account shown on the left side of the window, the details are shown in “Local Auth User” on the right, see Figure 159.

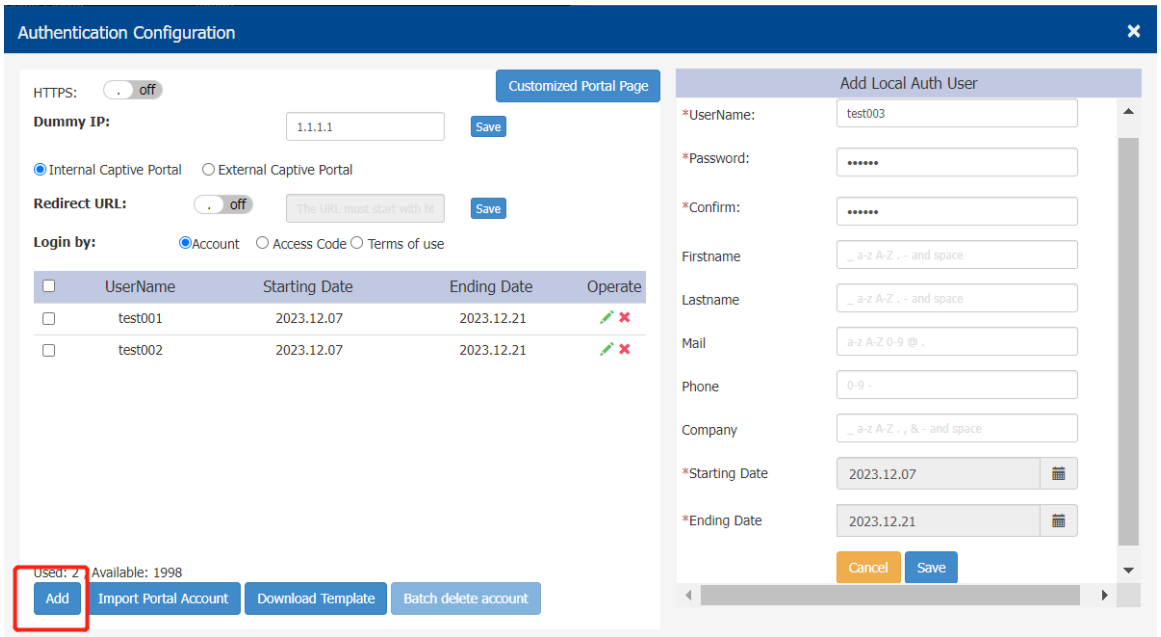


Figure 158: Add an account

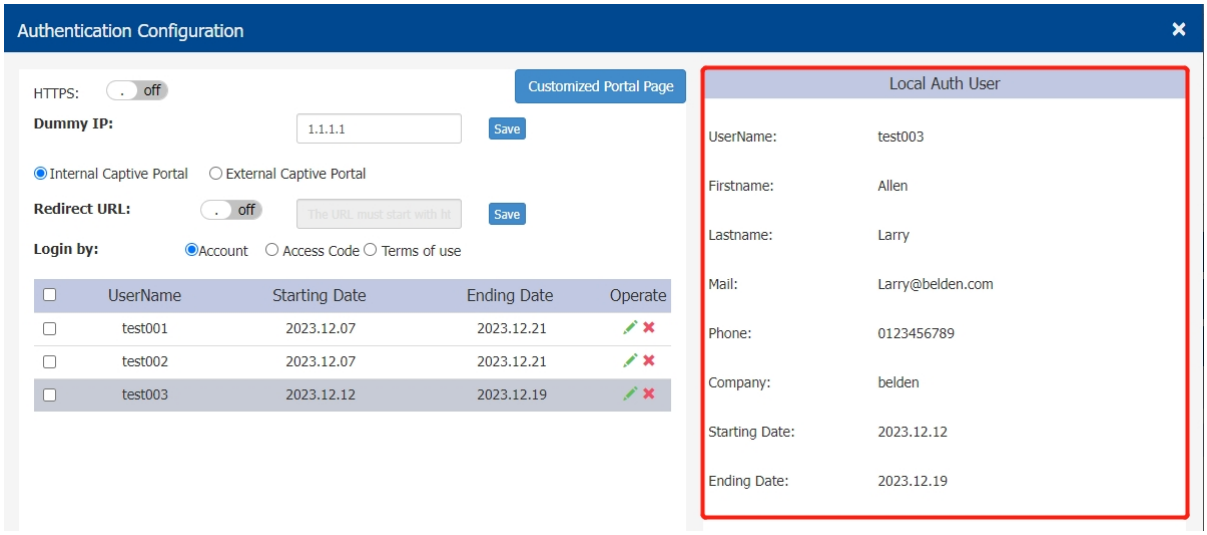


Figure 159: Account detailed information

Batch Import portal accounts

DAP847-XXA supports import accounts from a local CSV file. You can modify the local CSV file from the downloaded template to create a batch of accounts.

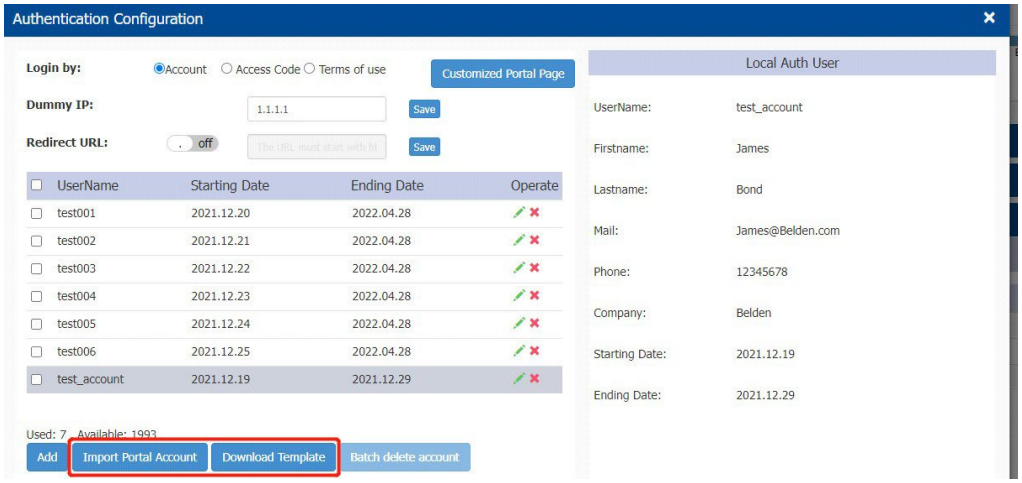


Figure 160: Batch import portal accounts

Modify or delete account(s):

- ☐ Click "✎" to modify an account.
- ☐ Click "✖" to delete an account.
- ☐ To delete multiple accounts, select the accounts and click the **"Batch delete account"** button, see Figure 161.

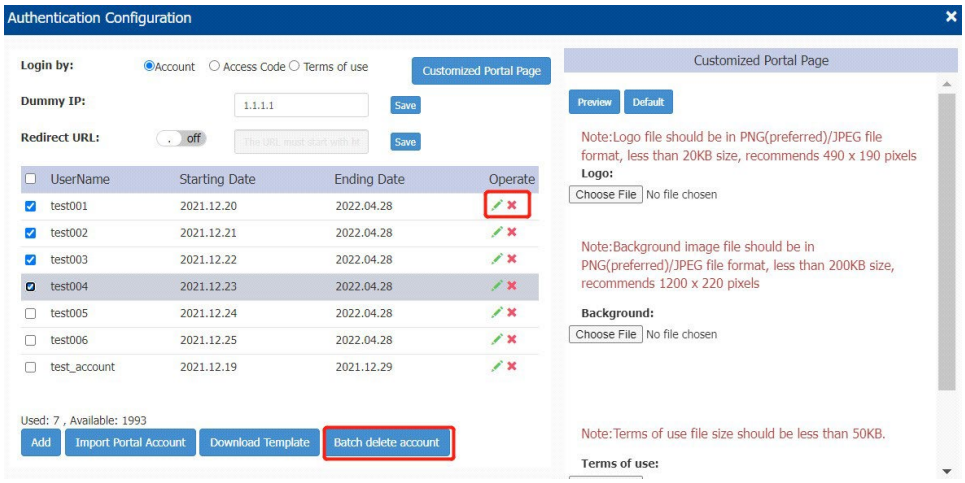


Figure 161: Modify or delete account(s)

■ Create or delete an Access Code:

- ☐ Select the **"Access Code"** as the login method.
- ☐ Add an Access Code by clicking **"Add"** button on the Authentication Configuration page.
- ☐ Click **"✖"** button to delete an Access Code, see Figure 162.

Note: A single Account or an Access Code can be used by multiple devices simultaneously. There are no limits to the number of devices that a captive portal user account or an access code can connect to the network.

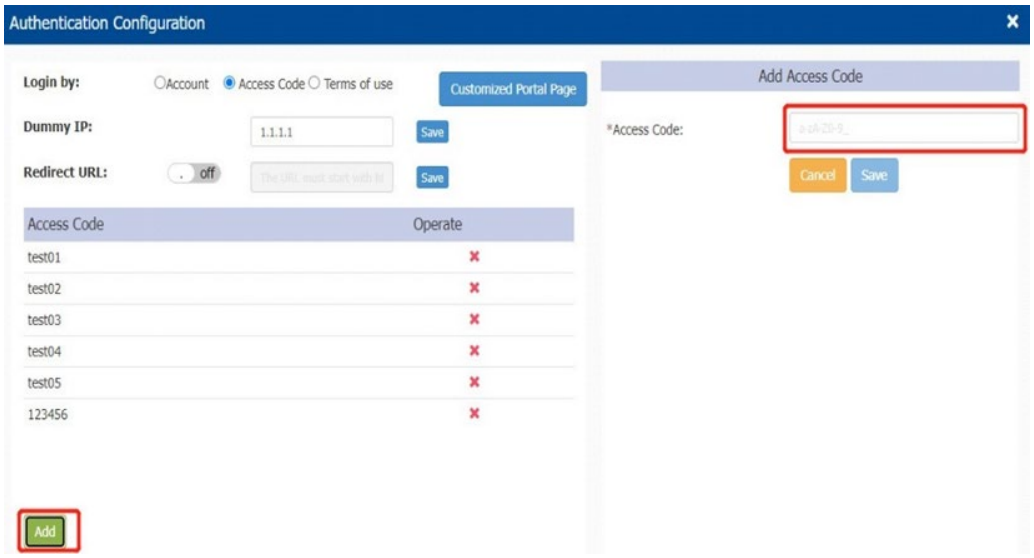


Figure 162: Create an access code

10.4 Customize portal page

Users can customize the portal page by specific design and requirements, including the logo, the background, and the terms of use, see Figure 163.

Configuration path: **Dashboard → Access Page → Authentication → Authentication Configuration → Customized Portal Page**.

- ☐ Upload the logo, background image and terms of use according to the requirements mentioned in notes.
- ☐ Click the **"Preview"** button to preview the customized Portal Page.
- ☐ Click the **"Default"** button to cancel changes and return to the default portal page.

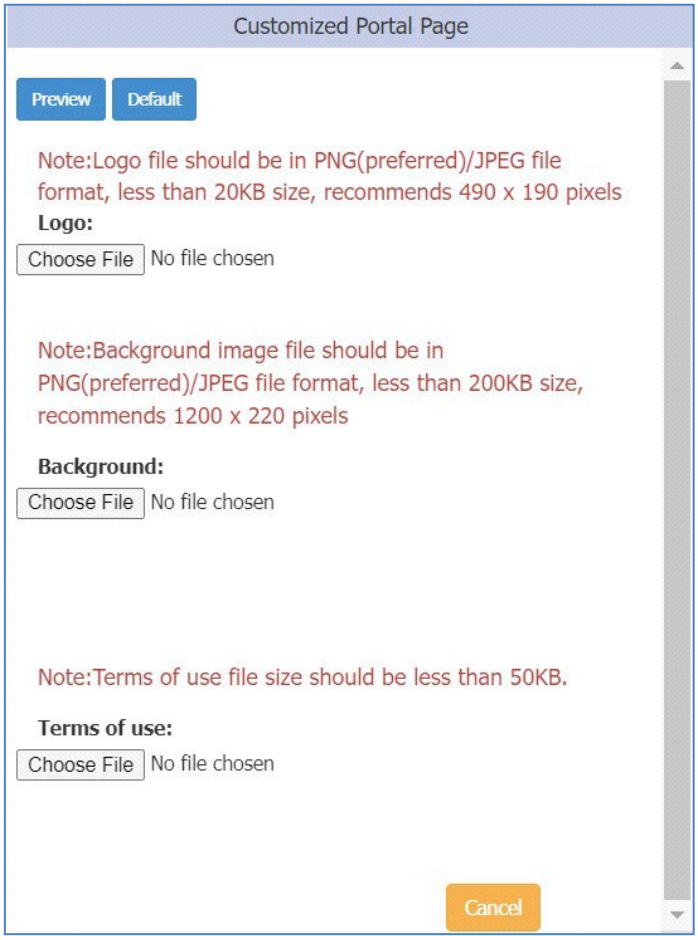


Figure 163: Customize portal page

10.5 Client blocklist for wireless access

The blocklist of DAP847-XXA is used for access control of wireless users. Blocklist records the MAC address of wireless devices that the DAP847-XXA clusters are restricted to connect. When the MAC address is added to the blocklist, the device cannot connect to the Wi-Fi of the DAP847-XXA cluster. Blocklist can help administrators control which devices are not allowed to connect to the wireless network for security.

To delete the device from Blocklist, enter the Blocklist configuration window and find the MAC address for the device. Click the "✖" button.

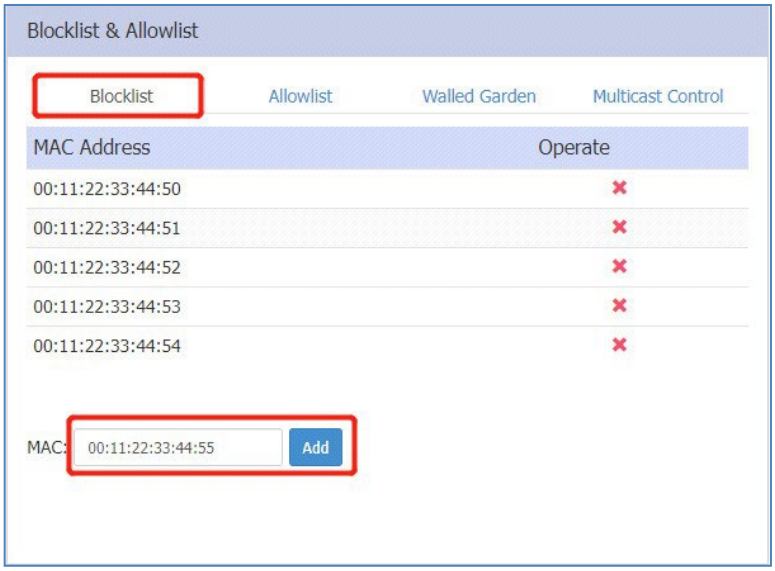


Figure 164: Blocklist configuration

10.6 Client allowlist for captive portal

The clients on the allowlist are permitted to access the network resources without a captive portal authentication. You can manually add or remove the MAC address of clients from the allowlist for captive portal authentication. Please note that allowlist applies only in captive portal authentication. The clients in the allowlist are not allowed to access Enterprise/Personal WLANs without correct credentials.

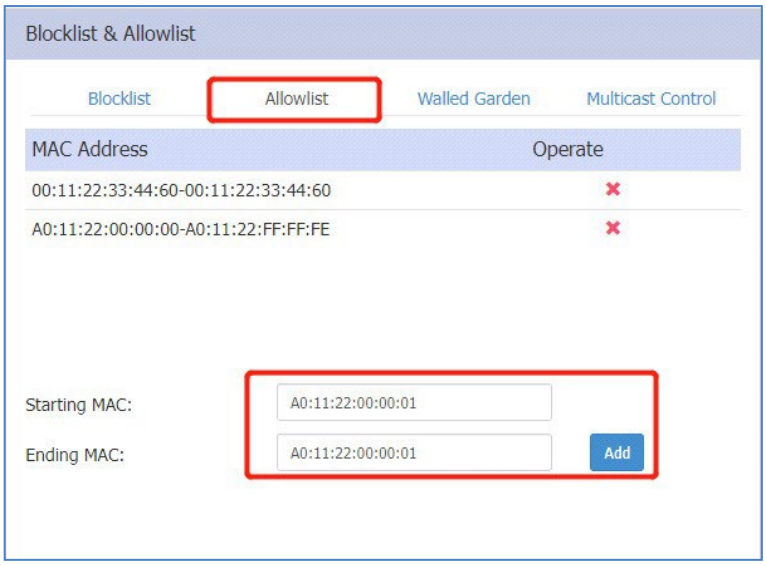


Figure 165: Allowlist configuration

10.7 Walled garden

The Walled Garden is a control mechanism over network resources, and it restricts the access to non-approved applications or contents. The Walled Garden is only applied for Captive Portal authentication. The clients can access the network resources listed in the Walled Garden before passing a Captive Portal authentication. You can add or remove the domains or IP addresses from the Walled Garden.

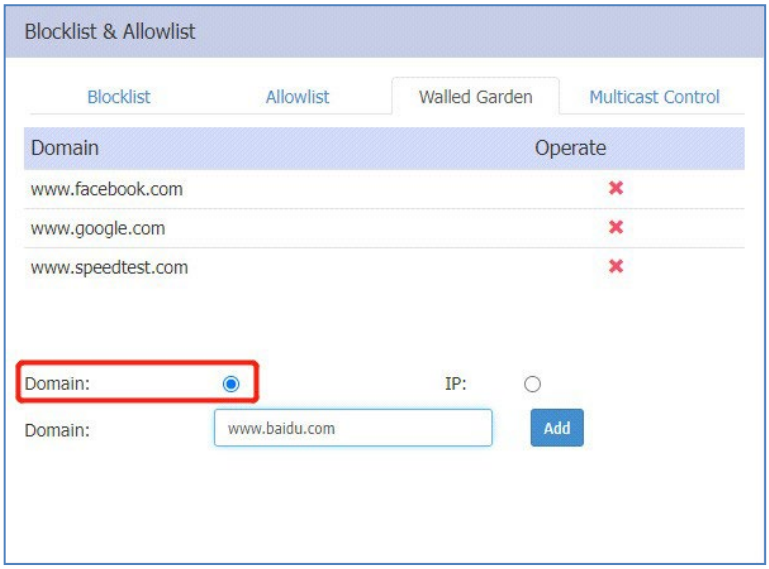


Figure 166: Walled Garden configuration for domain

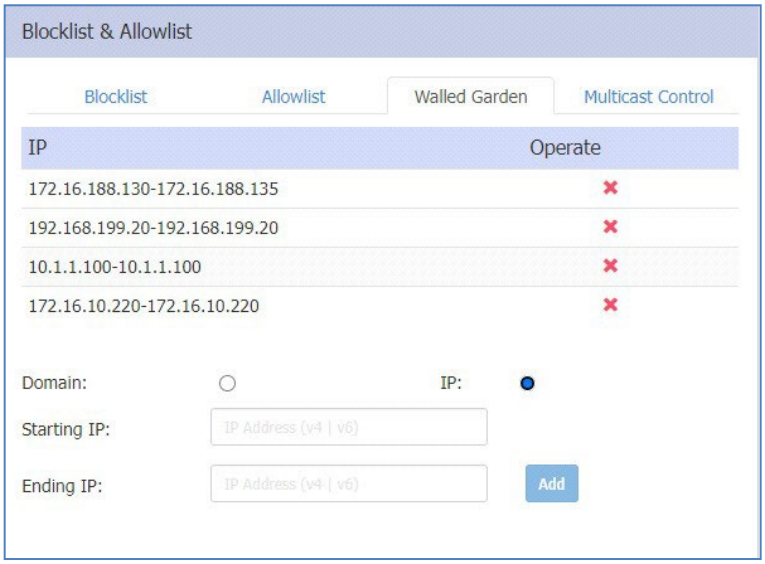


Figure 167: Walled Garden configuration for IP address

10.8 Multicast control

The Multicast Control is used for the mDNS multicast traffic forwarding from the wired network (switch ports) towards the DAP847-XXA. When it is enabled, only traffic from the configured multicast source in the allowlist can be forwarded by the DAP847-XXA to the clients. A maximum 8 items are supported in the multicast allowlist. When it is disabled, the mDNS multicast traffic is forwarded without conditions.

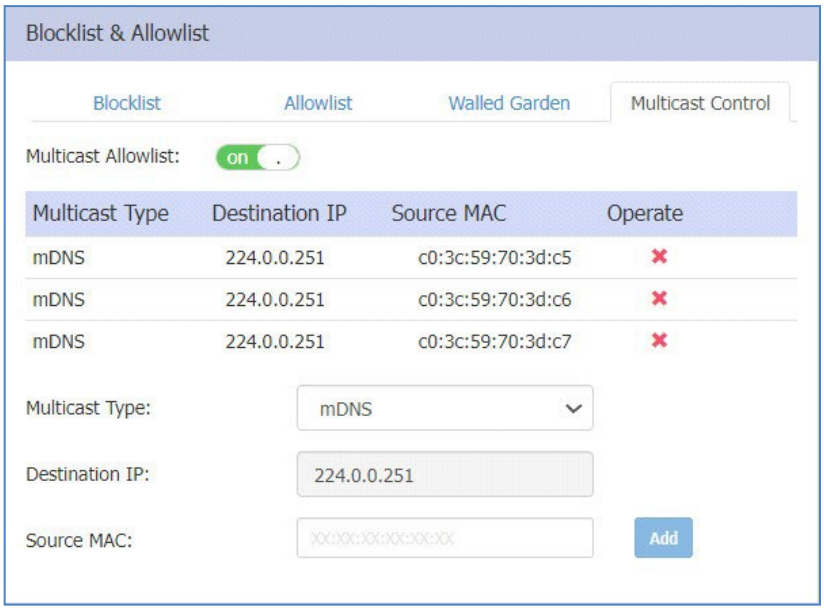


Figure 168: Multicast control

10.9 ACL

There are 2 modes for the ACL window, Basic window and ACL Configuration window. See Figure 169 and Figure 170.

Click the ACL window frame to switch to the ACL Configuration window from the Basic window.

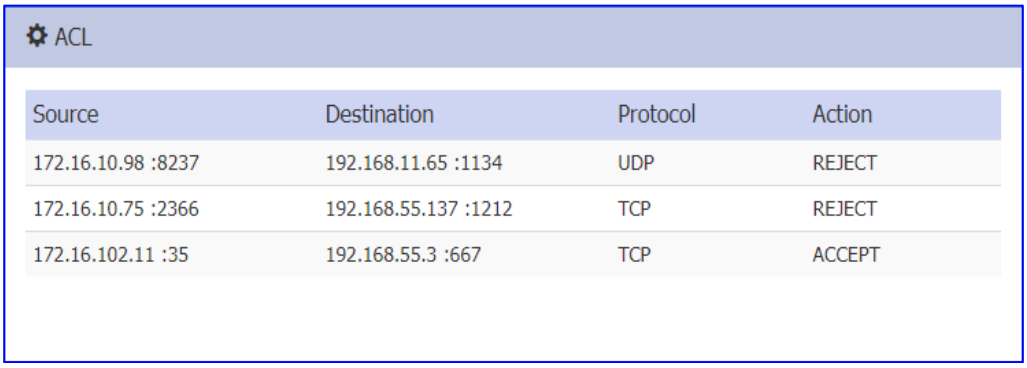


Figure 169: Basic ACL window

DAP847-XXA supports up to 128 rules. You can create L3 ACLs using IP address protocols and port numbers. The ACL rules created in the list are applied from top to bottom. Traffic is allowed to pass if no ACL rules are matched (The default ACL action is **"Accept"**), see Figure 170.

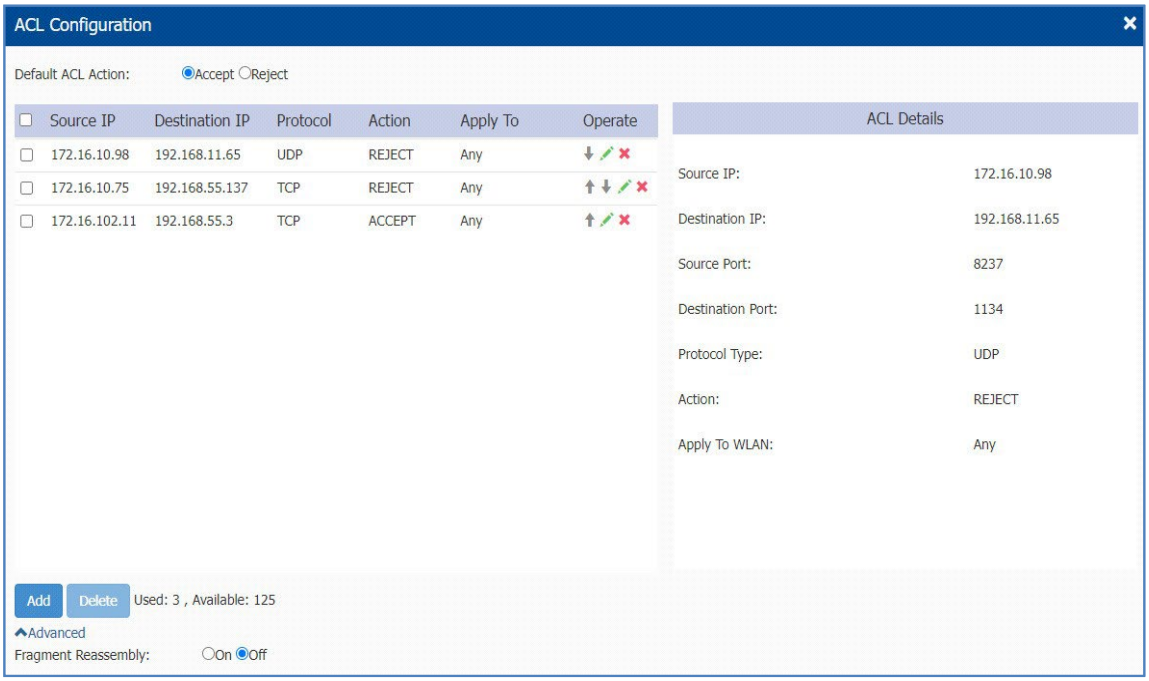


Figure 170: ACL configuration window

Parameter	Description
Source IP	The source IP address
Destination IP	The destination IP address
Source Port	The source UDP or TCP port
Destination Port	The destination UDP or TCP port
Protocol Type	ALL, TCP, UDP, ICMP, or ICMPv6
Action	ACCEPT or REJECT
Apply To WLAN	The range which the ACL rule takes effect, specific SSID or any SSID

11 IoT

DAP847-XXA does not support IoT functions. However, when DAP847-XXA and other devices that support IoT (such as DAP640) are in a cluster, IoT can be configured. For details, see User Manual: DAP Family.

12 Tools

12.1 Tools

Tools are integrated commands of the DAP847-XXA used for day-to-day diagnosing and troubleshooting. The commands are executed in the DAP847-XXA. Network administrators can view the running information by these tools, such as system status, Wi-Fi information, and reboot reason, etc.

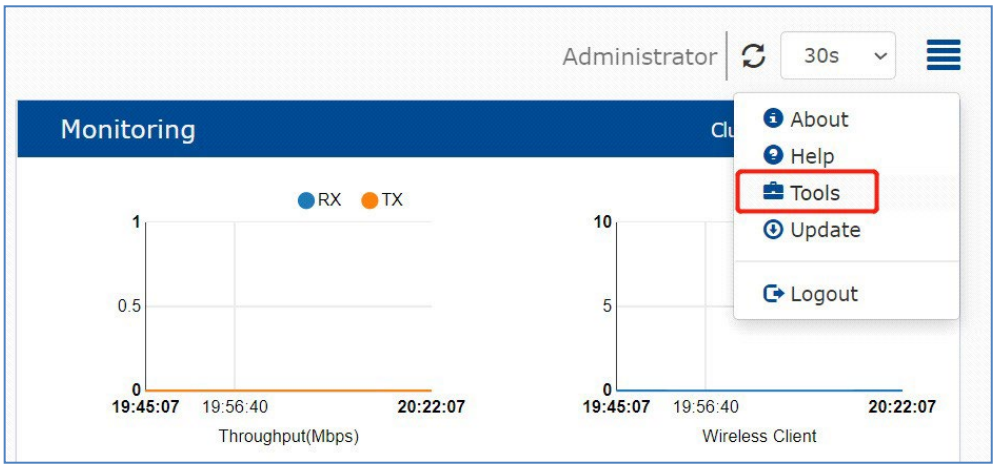


Figure 171: Entry of tools

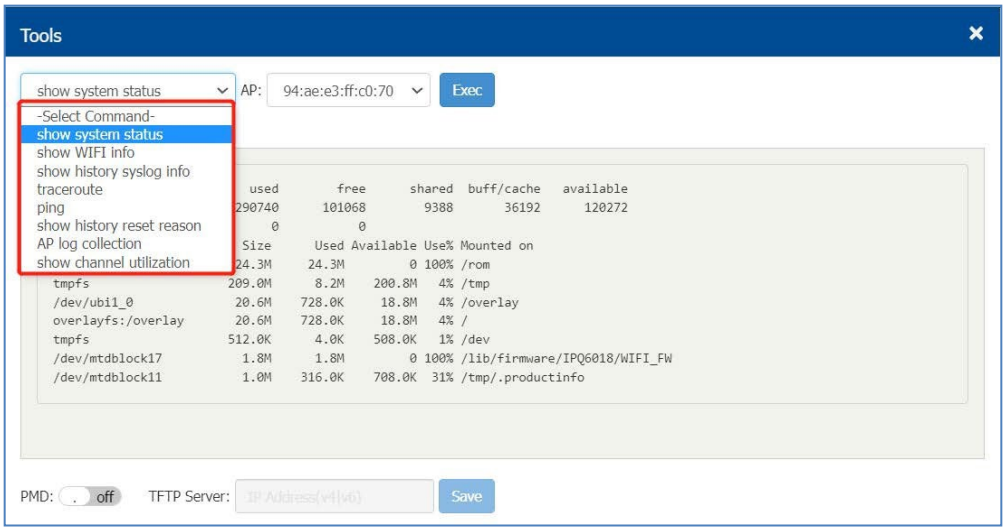


Figure 172: Troubleshooting tools

- **show system status:** Shows the system memory usage information for a DAP847-XXA.

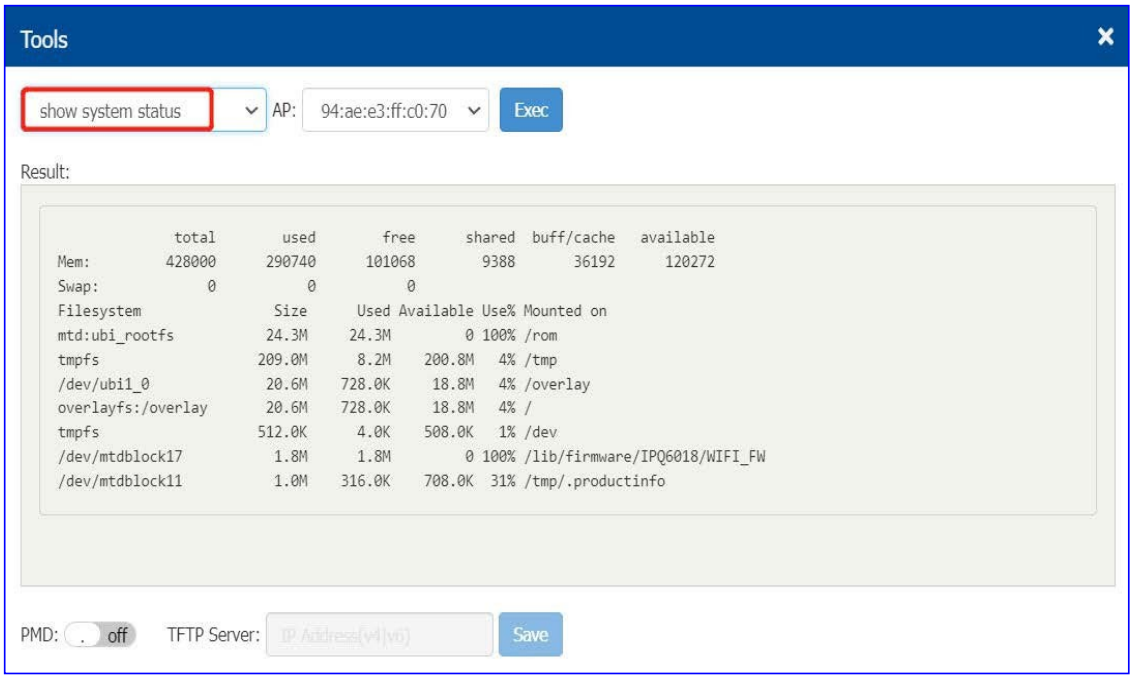


Figure 173: Show system status

- **show WIFI info:** Shows the wireless interface status for a DAP847-XXA.

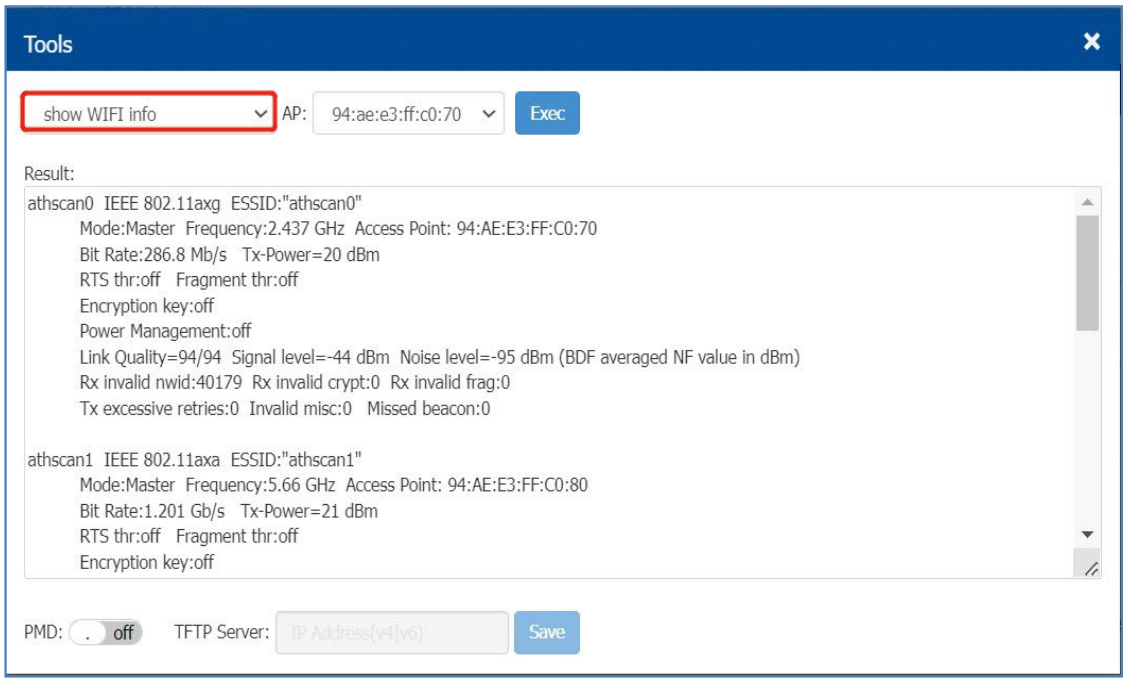


Figure 174: Show WIFI info

- **show history syslog info**: Shows the historic syslog messages generated for a specified DAP847-XXA during the last run of the system.

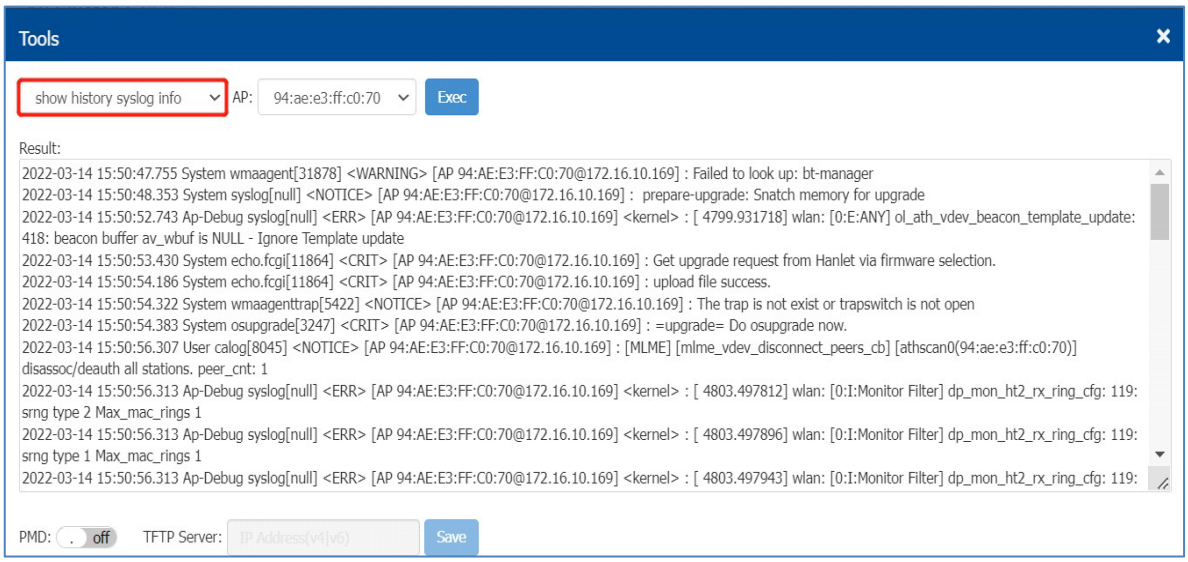


Figure 175: show history syslog info

- **traceroute:** Built-in tool of DAP847-XXA used to check route information in the network, see Figure 176.

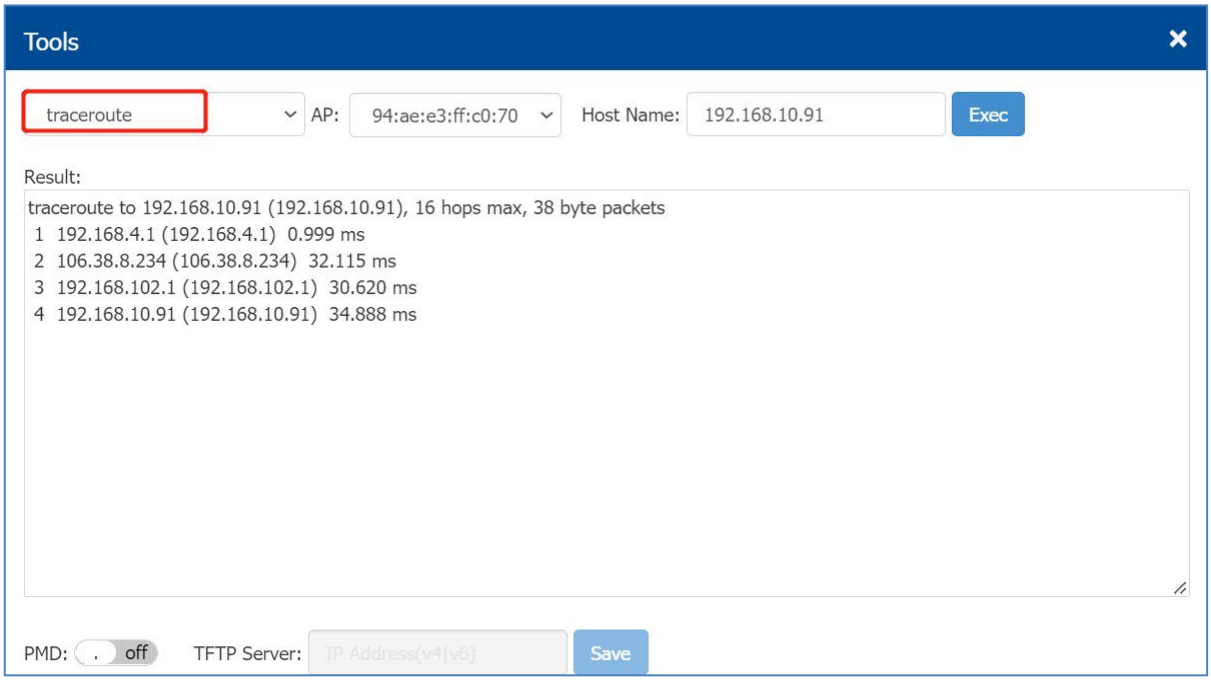


Figure 176: traceroute

- **ping**: Ping operations from a specified DAP847-XXA to another host in the network.

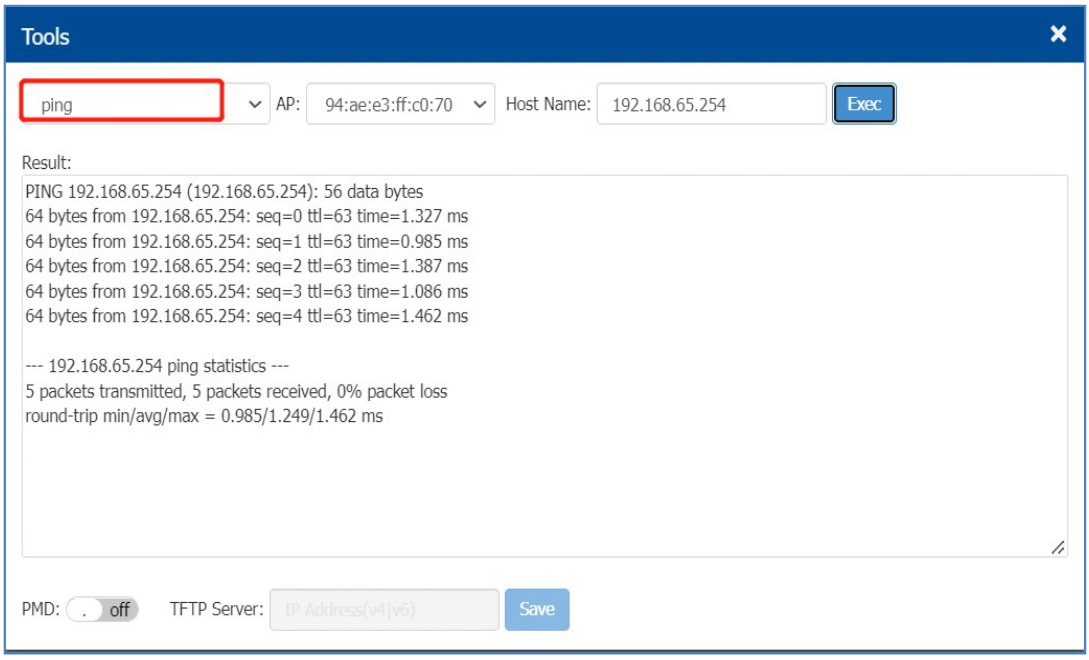


Figure 177: Ping testing on specific DAP

- **show history reset reason**: Shows the latest 10 reboot records of a specified DAP847-XXA. Output is the same as the command `reset_record get`, see Figure 178.

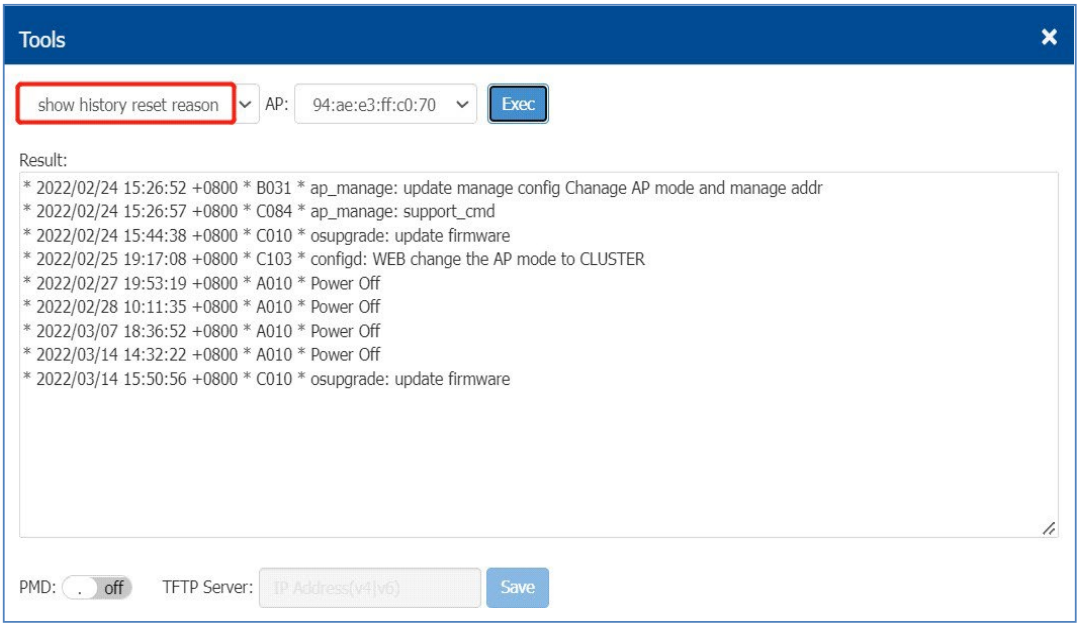


Figure 178: show history reset reason

- **AP log collection**: Collects log files of the DAP847-XXA for troubleshooting. Files can be downloaded using TFTP and HTTP, see Figure 179 and Figure 180.

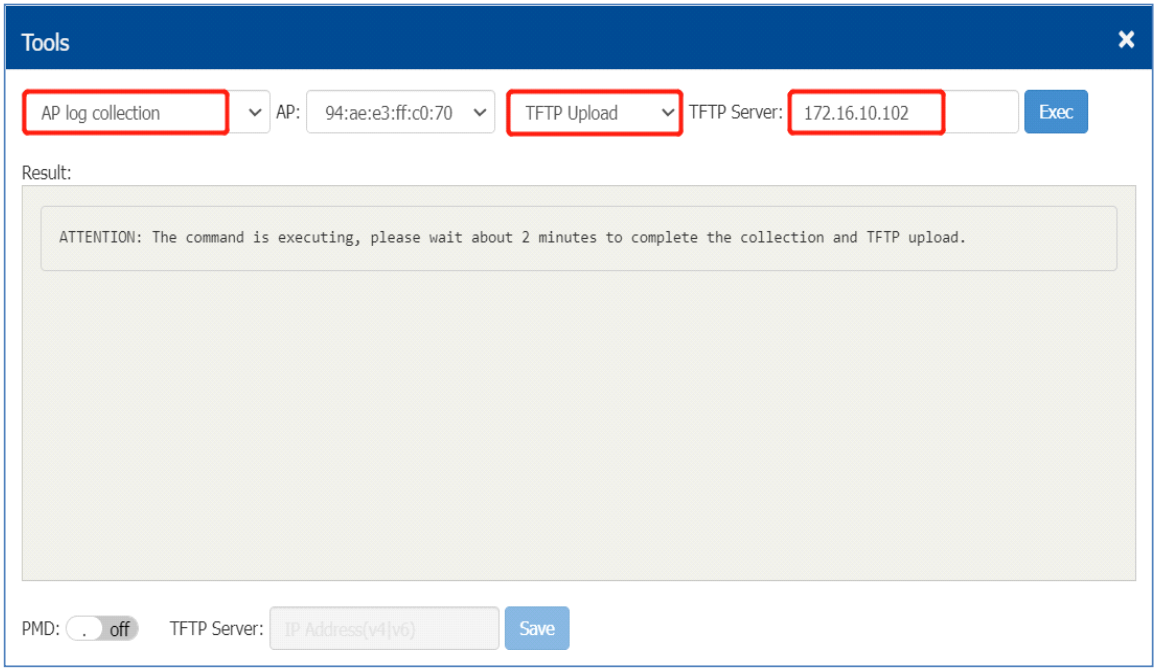


Figure 179: AP log collection by TFTP

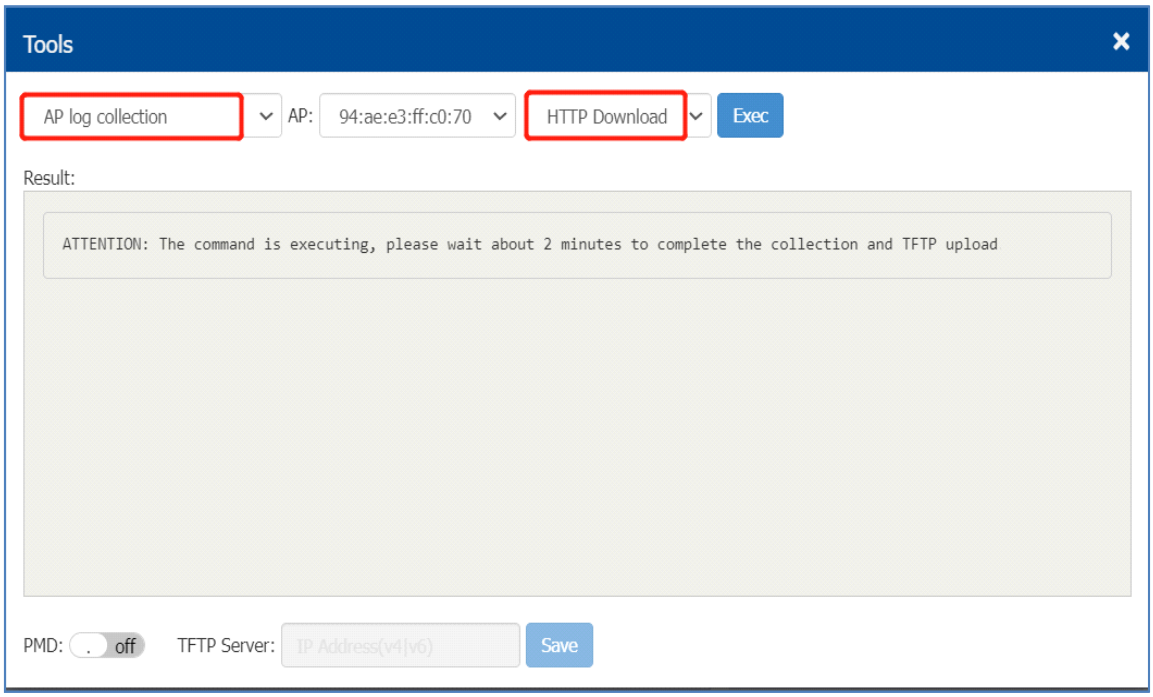


Figure 180: AP log collection by HTTP

- **show channel utilization**: Shows the channel utilization of 2.4 GHz and 5 GHz band, see Figure 181.

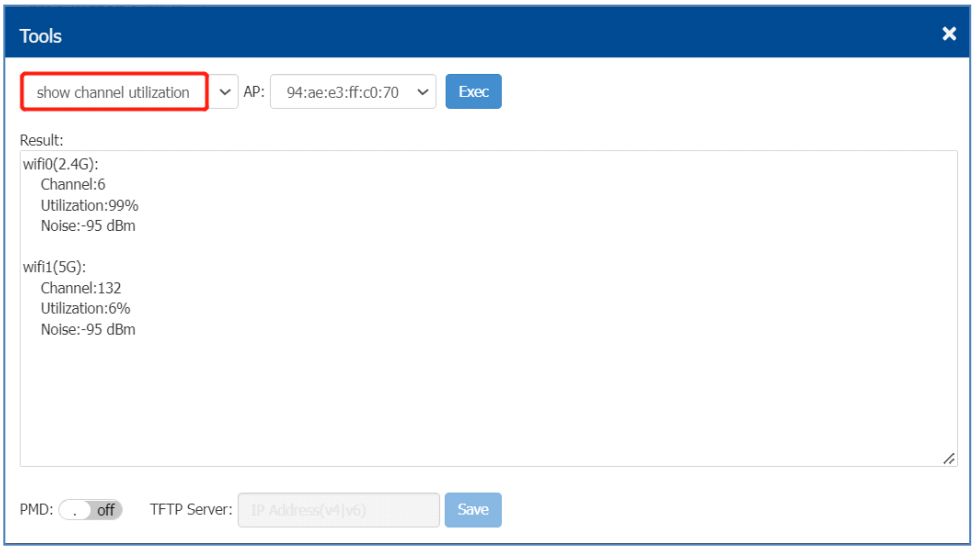


Figure 181: Show channel utilization

12.2 PMD

Post Mortem Dump (PMD) is a troubleshooting tool. When a crash or an error occurs, it saves information including the memory content, register status, and stack information, and uploads them to the server through TFTP for future analysis and debugging. If PMD is enabled and configured, the DAP847-XXA sends PMD files to a specific TFTP server immediately when there is a key process crashing on the DAP847-XXA. By default, the PMD function is disabled.

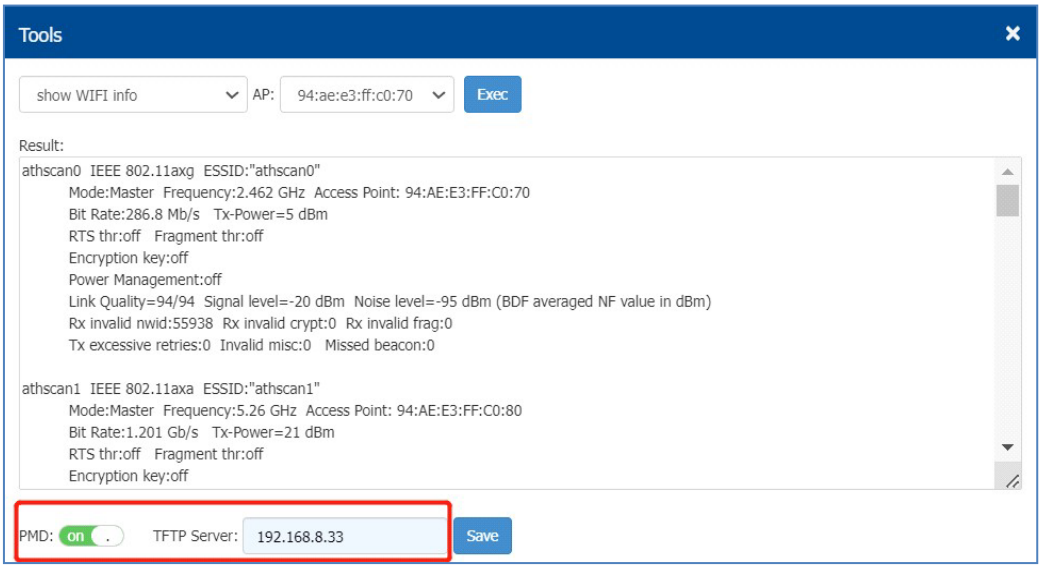


Figure 182: PMD configuration

13 Deployment large scale of DAP847-XXA devices

If you have DAP847-XXA devices more than the maximum specification of a cluster (255), you can set up 2 or more clusters for deployment to flexibly expand the customer's business applications.

You can deploy multiple clusters through the following 3 methods:

Method 1: Devide subnets

Divide the DAP847-XXA devices into different subnets by changing the default VLAN of the switch ports to which the DAP847-XXA devices connect.

For example, the subnet-A uses default VLAN 100, the subnet-B uses default VLAN 200, and the subnet-C uses default VLAN 300.

Method 2: Set different cluster IDs

Setting up different cluster IDs for each DAP847-XXA cluster can also divide different clusters, even if all the DAP847-XXA devices are in the same subnet.

- ☐ Select the DAP847-XXA devices for Cluster-A and plug into the switch to build the first AP cluster.
- ☐ Browse the Cluster-A by management IP and change the cluster ID.(For example: change the cluster ID from the default value 100 to 101).
- ☐ Repeat the above steps to set up Cluster-B, Cluster-C, etc.

Method 3: Deploy in DAC mode

Deploy DAP847-XXA devices in DAC mode which supports scaling up to 4000 DAP847-XXA devices in one network. For details, see DAC User Manual.

14 Configure the AP without DHCP server

This section describes the configuration of the DAP847-XXA in 2 scenarios without a DHCP server.

Case 1: DAP847-XXA cannot connect to a DHCP server

If the DAP847-XXA in the cluster cannot connect to the DHCP server in the network after startup, the system default IP address (192.168.1.254) is used.

When there are multiple DAP847-XXA devices in a network, there may be duplicate IPs in the network. The DAP847-XXA devices work separately from the cluster and broadcast the same WLAN. In this case, Hirschmann IT recommends fixing the DHCP server in the network.

Case 2: Configure the DAP847-XXA without a DHCP server in the network

If you want to configure a single DAP847-XXA without a DHCP server in the network, perform the following steps:

- ☐ Connect the DAP847-XXA (the default IP address is 192.168.1.254) to your configuring terminal (for example, laptop or PC) directly.
- ☐ Specify a static IP address and a DNS server for the network card of your laptop (or PC). For example, specify the IP Address as 192.168.1.100, the subnet mask as 255.255.255.0, the default gateway as 192.168.1.254, and the DNS server as 192.168.1.254.g
- ☐ Browse http://192.168.1.254:8080 for AP Cluster Manager for further configuration needed.

Note: To configure multiple DAP847-XXA devices in a cluster, configure different IP addresses for DAP847-XXA devices.

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
CTS	Clear To Send
DAC	Dragonfly Access Controller
DAP	Dragonfly Access Point
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
DTIM	Delivery Traffic Indication Message
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
QoS	Quality of Service
QSG	Quick Start Guide
RF	Radio Frequency
RSSI	Received Signal Strength Indicator
RTS	Request To Send
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
SVM	Secondary Virtual Manager: The second highest priority in the cluster. When the PVM is inoperable 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

A Further support

Technical questions

For technical questions, please contact any Hirschmann IT dealer in yourarea or Hirschmann IT directly.

A list of local telephone numbers and email addresses for technical support directly from Hirschmann IT is available at

https://hirschmann-it-support.belden.com

This site also includes a free of charge knowledge base and a software download section.