HIRSCHMANN IT

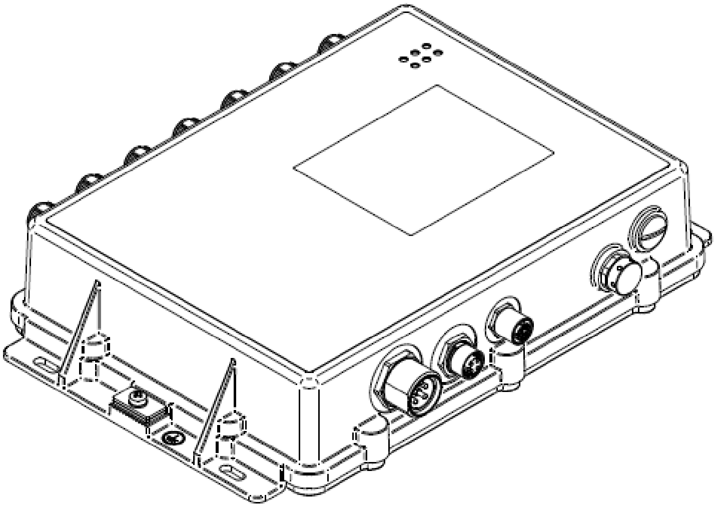
A BELDEN BRAND

User Manual

Configuration

Dragonfly Access Point Client

DAP847-XXC



User Manual DAP847-XXC
Release 1.2 08/2024

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.

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.

User Manual DAP847-XXC
Release 1.2 08/2024

Revision History

Version	Date	Description
1.0	Dec-2023	First version, based on Web GUI 4.1.6.115.
1.2	Aug-2024	Based on Web GUI version 4.1.6.142, add the following parameters to section 7.1.2 Wireless Network Configuration DAP847-XXC on DAP847-XXC: RSSI Healthy Check, 11R, Roaming Aggressiveness, RTS/CTS, RTS Threshold.

Contents

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.

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 draws your attention

1 Introduction

1.1 Overview

As a new generation of enterprise-level wireless access clients, the DAP847-XXC series is suitable for industrial Wi-Fi 6 equipment in the railway deployment scenario. It supports an uplink connection to the DAP847-XXA series to achieve a real-time transmission of the railway control signals and related monitoring data of applications.

According to the different deployment scenarios and requirements, the DAP847-XXC supports dual-band operation at 2.4 GHz and 5 GHz radios. It supports the configuration of antenna gain and flexible configuration of antenna MIMO, which ensuring stable and efficient roaming performance between the train and the DAP847-XXA under high-speed running conditions.

This user manual describes the features supported by the DAP847-XXC in the railway deployment scenario of connecting the DAP847-XXA series. It provides instructions and examples for the configuration of DAP847-XXC. It is designed for network administrators who are responsible for configuring and maintaining the Wi-Fi network. It assumes the reader is familiar with Layer 2 and Layer 3 networks and basic IEEE 802.11 protocols and related technologies.

The examples describe the general steps of setting up a Wi-Fi network based on the typical deployment scenarios. It is useful for those new to the DAP847-XXC configuration and those already familiar with the software wanting to know more about certain functions.

2 DAP847-XXC deployment sample

This chapter mainly introduces a typical network topology structure including wireless networks in the rail transit scenario. This scenario includes:

- DAP847-XXC
- DAP847-XXA
- Switch
- Router
- Related application servers

2.1 Topology

Figure 1 illustrates the brief topology for a typical scenario for your reference. There is a DAP847-XXA deployed in this scenario and a DAP847-XXC connected to DAP847-XXA via 5 GHz channel.

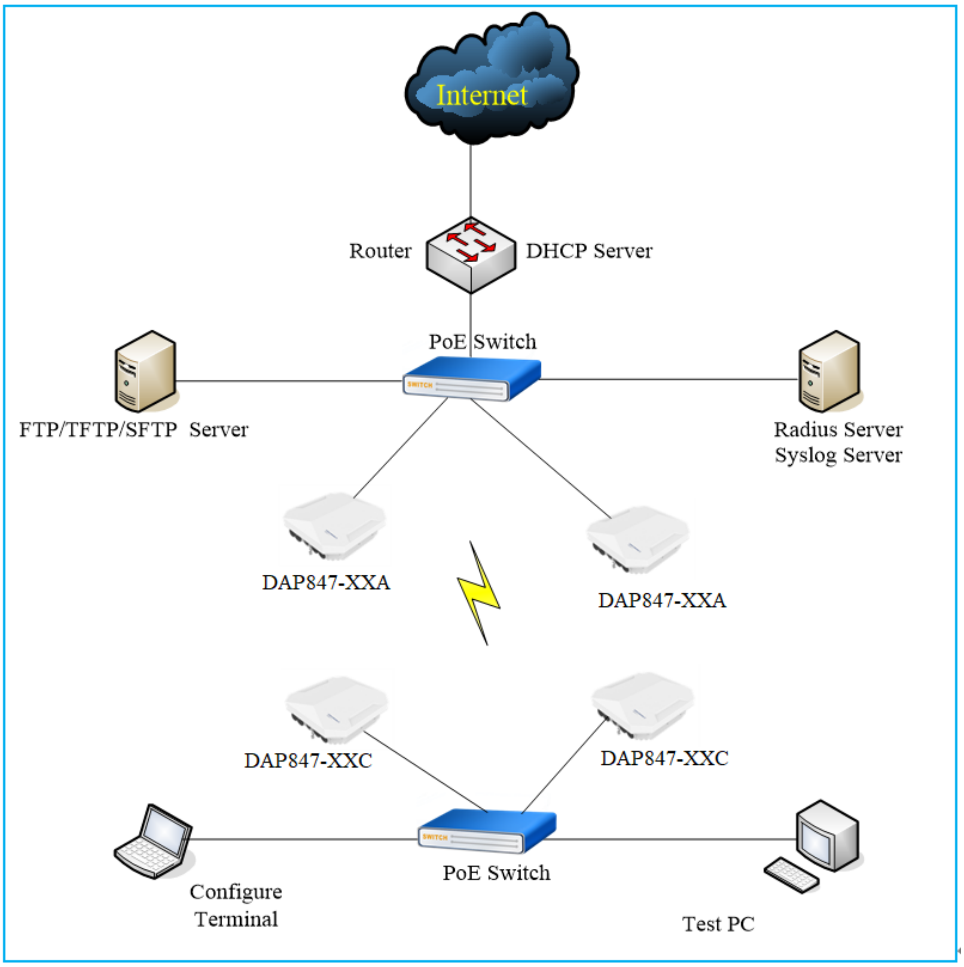


Figure 1: Topology

2.2 Descriptions for the scenario

There are 2 DAP847-XXAs and 2 DAP847-XXCs in this cluster. DAP847-XXCs connect to the DAP847-XXAs via 5 GHz channel. The DAP847-XXAs and DAP847-XXCs are respectively connected to 2 PoE switches supporting the IEEE 802.3 standard.

A router provides DHCP service to all DAPs and the terminal. A MESH interface with SSID named “TestSSID” is configured on the DAP847-XXA. The DAP847-XXC is configured with the same SSID and connected to DAP847-XXA as a wireless client.

The related servers are also deployed in this scenario:

- **Radius Server**: Used for IEEE 802.1x authentication for an Enterprise SSID, it may be a windows Server or other type of RADIUS server.
- **Syslog Server**: Used as a remote syslog server for receiving syslog generated by DAP847-XXC which is described in Chapter Syslog on page 38.
- **TFTP Server**: Used for DAP847-XXC snapshot collection and DAP847-XXC firmware upgrading.
- **SFTP Server**: Used for DAP firmware upgrading.

3 Setup wizard

Initializing wizard window is displayed when you first log in to DAP847-XXC. In this chapter, it mainly introduces how to access DAP847-XXC and complete the basic configuration when using DAP847-XXC according to the wizard for the first time.

3.1 Access DAP847-XXC Onboard Client Manager via web browser

DAP847-XXC supports remote connection to DAP847-XXC Web GUI through a web browser. The GUI includes the configuration wizards to guide you to change administrator password and complete basic configuration.

Recommended OS	Recommended Browser
Windows 8	Google Chrome 115 and later
Windows 10 Windows 11	Mozilla Firefox 113 and later
MAC OS X 10.10	Microsoft Edge 115 and later
MAC OS X 10.11	

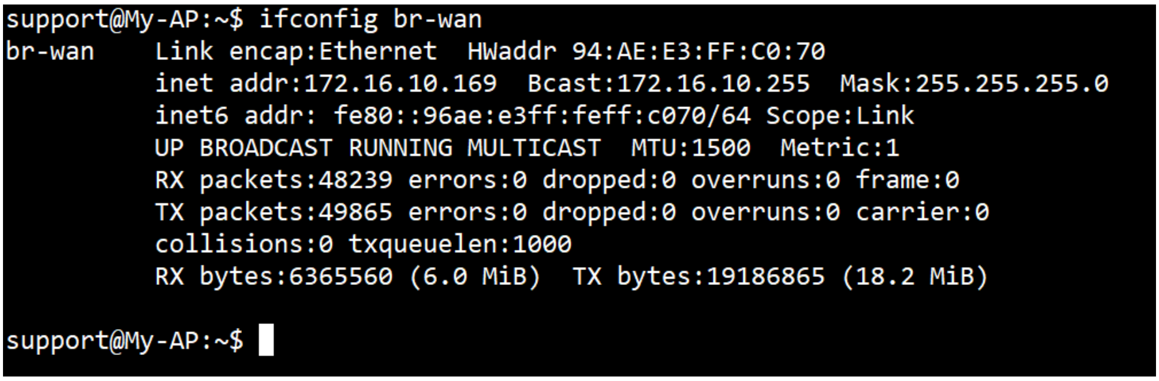
Table 1: Recommended operating system and browser

Note: Hirschmann IT recommends to access the DAP847-XXC Onboard Client Manager web window in Chrome browser for the best possible user experience.

3.1.1 DAP847-XXC IP address

The DAP847-XXC supports obtaining and managing the IP address in the following 3 ways:

- By default, if there is no DHCP server on the network, the DAP847-XXC uses the IP address 192.168.1.254.
- A static IP address can be manually configured to the DAP847-XXC.
- If there is a DHCP server, the DAP847-XXC can obtain an IP address from a DHCP server. You can check the IP address by following methods:
  - Check the IP address on the DHCP server.
  - Check the IP address on the ARP table of the uplink switch.
  - When checking the IP address on a console access, use the command `ifconfig br-wan` on DAP847-XXC, 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:~$ █
```

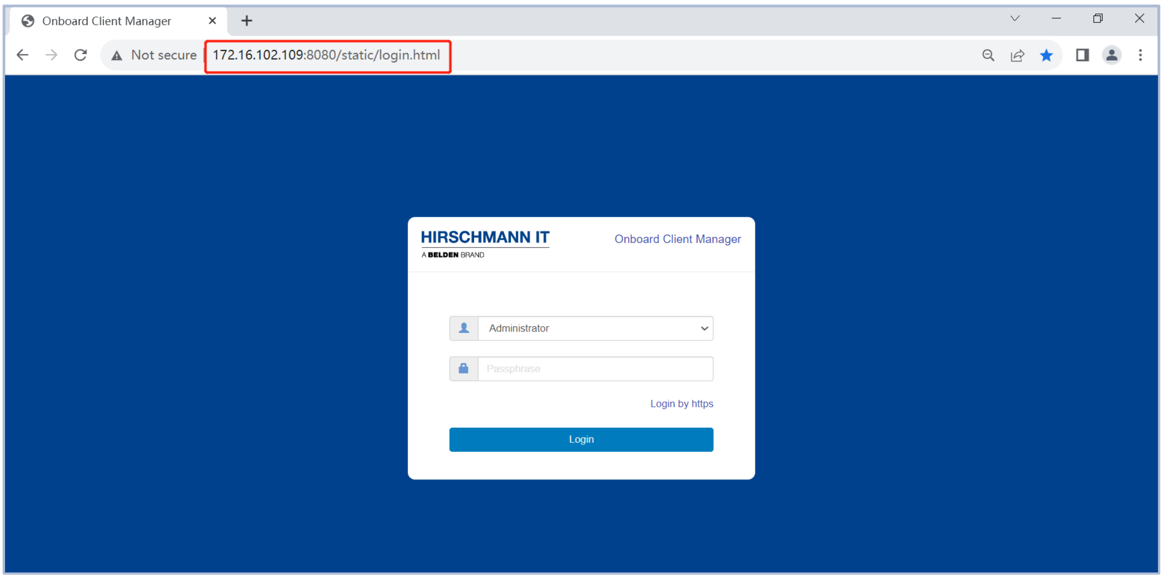
Figure 2: Check DAP IP address

3.1.2 Access DAP847-XXC web GUI in initialization state

Open your browser on your workstation and log in to the DAP847-XXC onboard manager by http or https using the default password “**admin**”.

For example:

- Log in with http by http://172.16.102.109:8080 in Figure 3. The DAP847-XXC IP address is 172.16.102.109.



Not secure 172.16.102.109:8080/static/login.html

Administrator

Figure 3: Log in http

- Log in with https by https://172.16.102.109 in Figure 4. The DAP847-XXC IP address is 172.16.102.109.

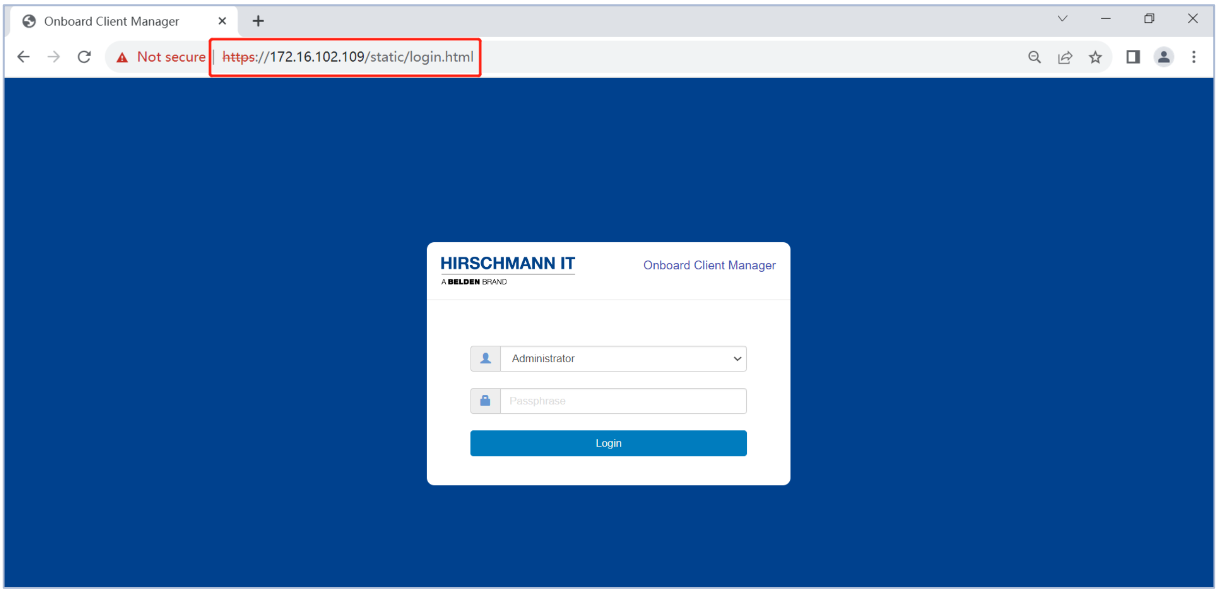
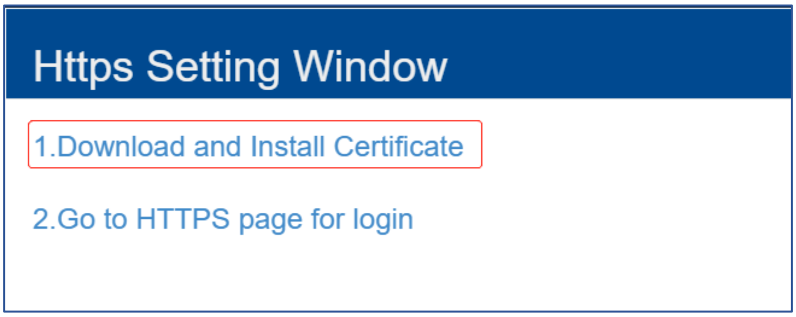


Figure 4: Login with https

Note: A digital certificate is required when you log in by **https** mode for more secure communication between DAP847-XXC and the browser.

Download the CA root from the DAP847-XXC and install it into the trust store of the used browser. The certificate installation procedure varies from the operating system and browser combinations, see Figure 5.


Https Setting Window

1.Download and Install Certificate

2.Go to HTTPS page for login

Figure 5: Download a certificate

3.2 Using DAP847-XXC setup wizard

You can log in with the Administrator account and the default password “admin”. The configuration step starts by loading the **Setup Wizard**.

- □ Log in to Setup Wizard.

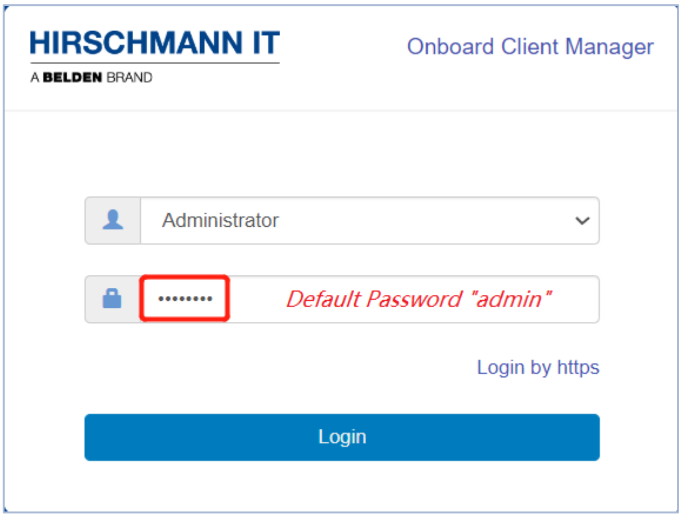
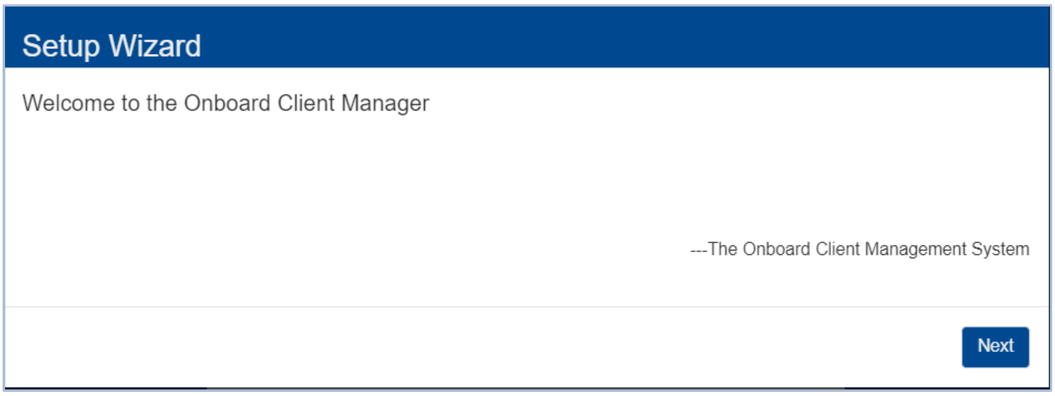


Figure 6: Login with Administrator

- □ A popup Setup Wizard in initial state.



Setup Wizard

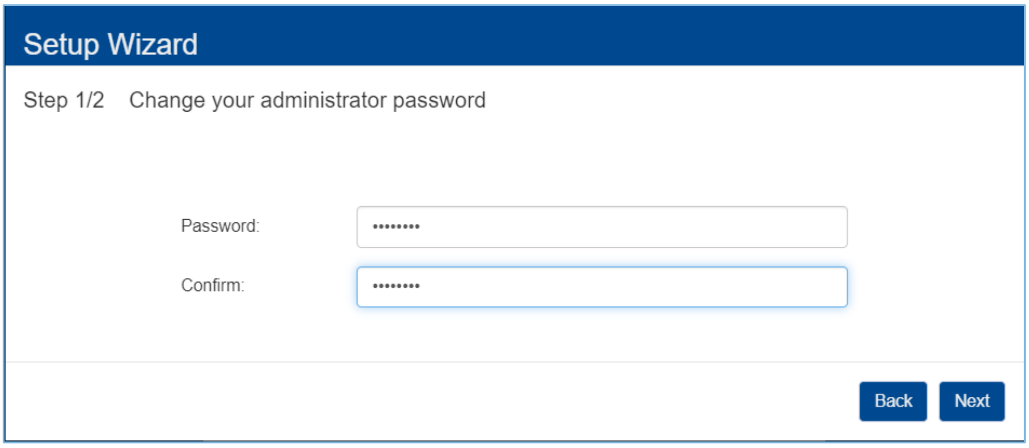
Welcome to the Onboard Client Manager

---The Onboard Client Management System

Figure 7: DAP847-XXC onboard manager

- □ Change your administrator password.

  Note: You can set the new login password to the default value “admin”.



Setup Wizard

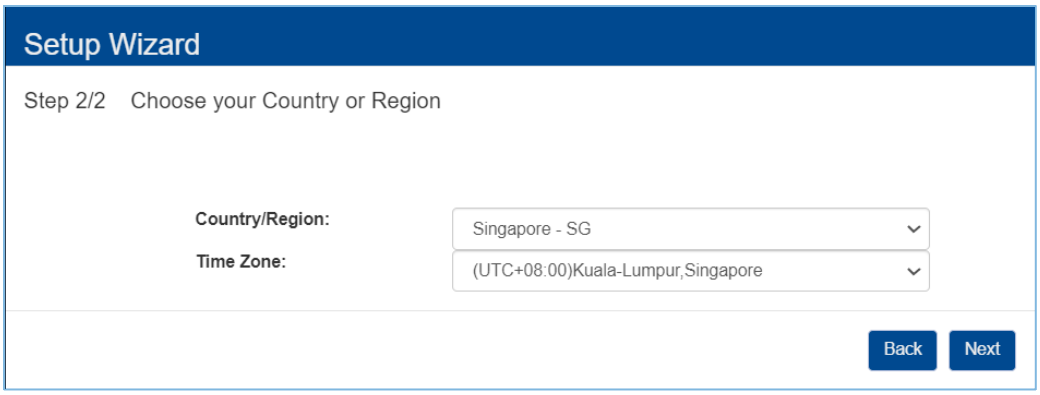
Step 1/2 Change your administrator password

Password: ••••••••

Confirm: ••••••••

Figure 8: Change your administrator password

- ☐ Choose your “Country/Region” and “Time Zone”.



Setup Wizard

Step 2/2 Choose your Country or Region

Country/Region: Singapore - SG

Time Zone: (UTC+08:00)Kuala-Lumpur,Singapore

Figure 9: Choose your country or region

When you finish the setup, the current login is terminated, and a re-login is required. You can log in with the new password and continue the other configuration steps if needed.

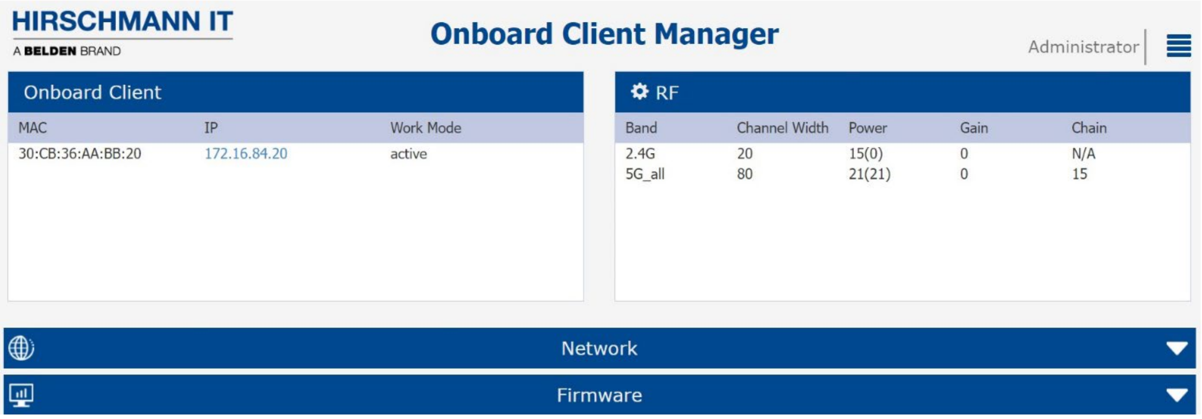
4 DAP847-XXC Onboard Client Manager Web GUI

This chapter briefly introduces the dashboard and each configuration window on the DAP847-XXC Web UI. For detailed information on separate functions, refer to the related chapter accordingly.

This section contains the following topics:

4.1 Dashboard overview

The DAP847-XXC provides a visualized dashboard for running state and configuration.



Onboard Client

MAC	IP	Work Mode
30:CB:36:AA:BB:20	172.16.84.20	active

RF

Band	Channel Width	Power	Gain	Chain
2.4G	20	15(0)	0	N/A
5G_all	80	21(21)	0	15

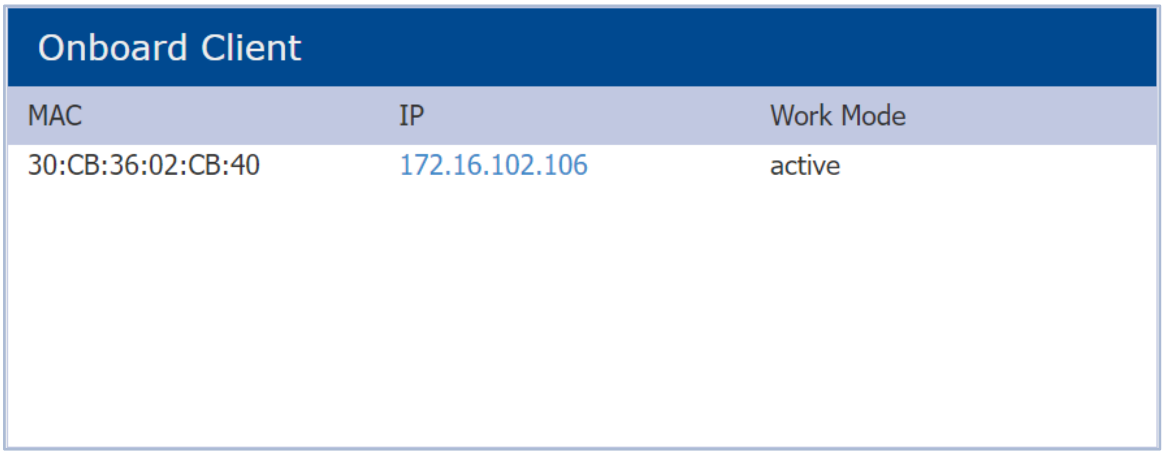
Figure 10*: Dashboard overview*

In Figure 10, on the top of the window, you can see the currently logged-in user and the more information icon.

The dashboard splits into sub-windows for **Onboard Client**, **RF**, **Network** and **Firmware**. You can briefly check the Onboard Client, RF in the dashboard, or click the framework of each window to see the detailed information.

4.2 Onboard client

The Onboard Client window shows brief information for DAP847-XXC, including its MAC address, IP address, and work mode. You can launch into the DAP847-XXC system configuration window by clicking its IP address.



Onboard Client

MAC	IP	Work Mode
30:CB:36:02:CB:40	172.16.102.106	active

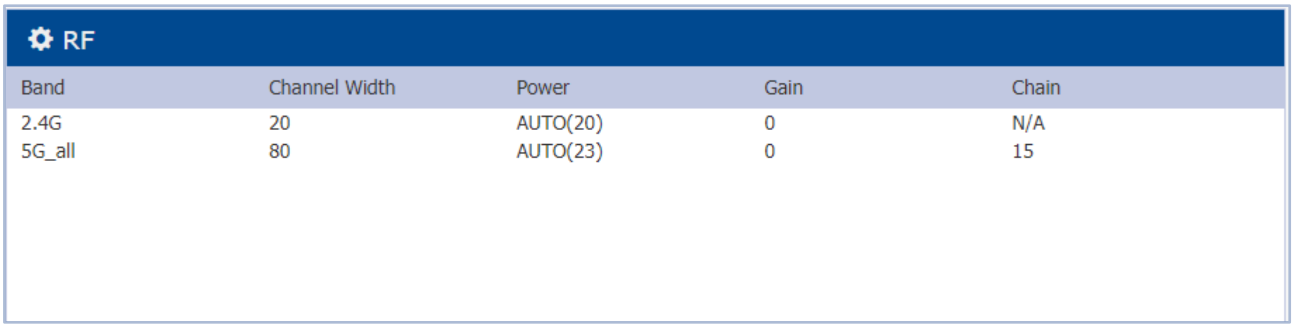
Figure 11: Onboard Client window

The key parameters are described as follows:

Parameter	Specification
MAC	The MAC address of the DAP847-XXC.
IP	The IP address of the DAP847-XXC.
Work Mode	The work mode of the DAP847-XXC: **Active:** The DAP847-XXC is working. **Standby:** The DAP847-XXC is on standby.

4.3 RF

The RF information window indicates the basic information about the radio, such as the current worked channel width, the transmit power, the **Gain,** and the **Chain** of each radio.



RF

Band	Channel Width	Power	Gain	Chain
2.4G	20	AUTO(20)	0	N/A
5G_all	80	AUTO(23)	0	15

Figure 12: RF information overview

The key parameters are described as follows:

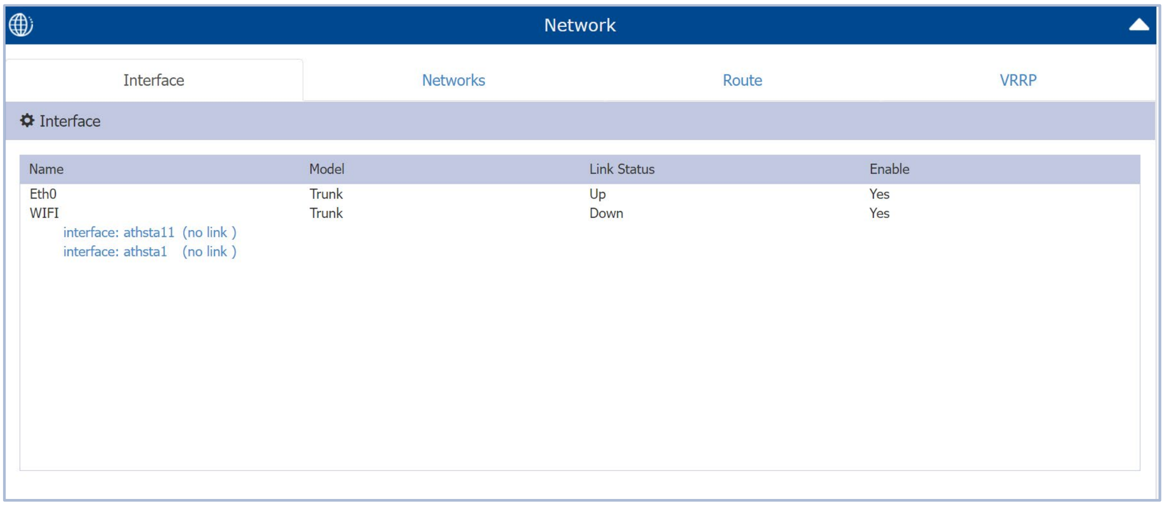
Parameter	**Specification**
Band	The radio band of DAP847-XXC, 2.4 GHz or 5 GHz.
Channel Width	The current channel width set on DAP847-XXC on 2.4 GHz and 5 GHz band.
Power	The current transmit power and Automatic Power Control (APC) state on specific radio, it indicates that transmission EIRP setting on the radio.
Gain	Specifies the gain value for the external antenna.
Chain	Indicates that the external antenna MIMO mode on DAP847-XXC.

4.4 Network

The **Network** window divides into 4 function frames:

- Interface
- Networks
- Route
- VRRP

For more details, see “Network configuration” on page 47.

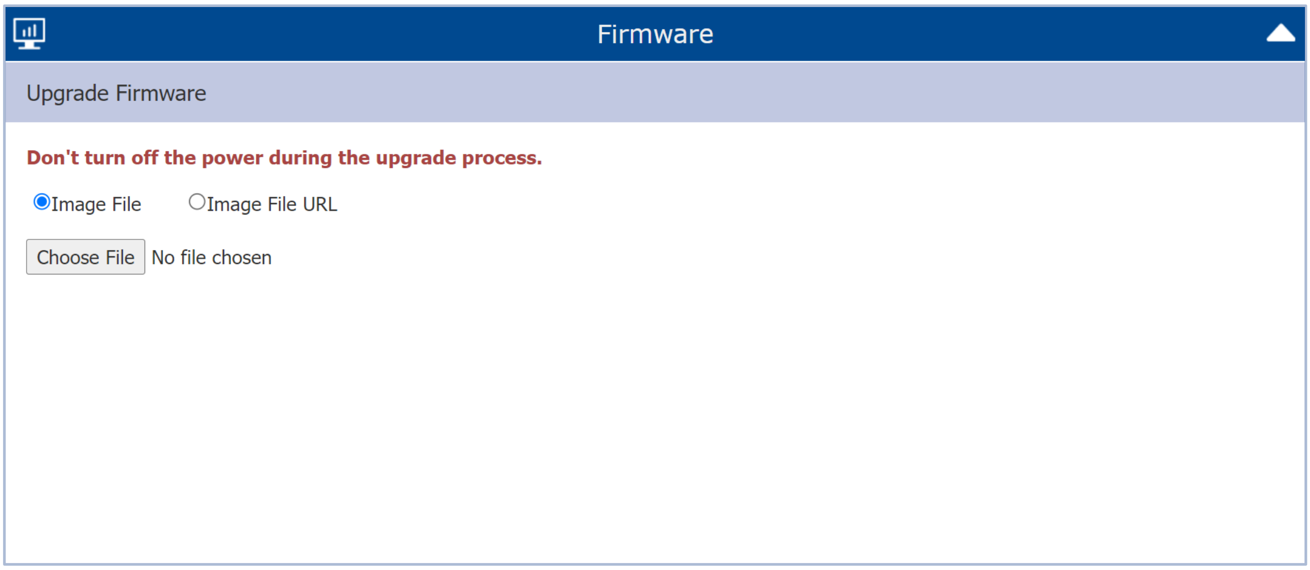


Name	Model	Link Status	Enable
Eth0	Trunk	Up	Yes
WIFI	Trunk	Down	Yes
interface: athsta11 (no link)			
interface: athsta1 (no link)			

Figure 13: Network page

4.5 Firmware

On **Firmware** page, you can perform the upgrading to manage the DAP847-XXC version, see Figure 14 and “Upgrade Firmware” on page 67.



Upgrade Firmware

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

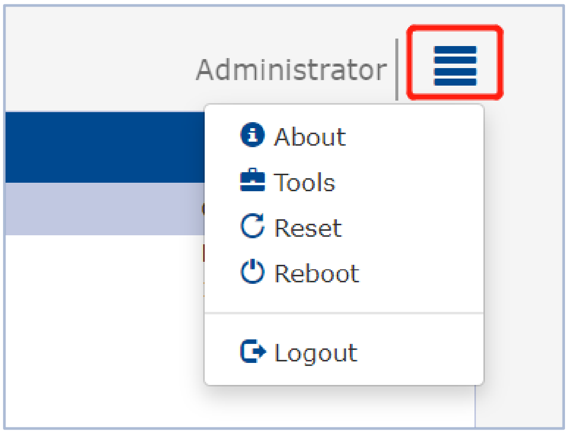
● Image File ○ Image File URL

No file chosen

Figure 14: Firmware page

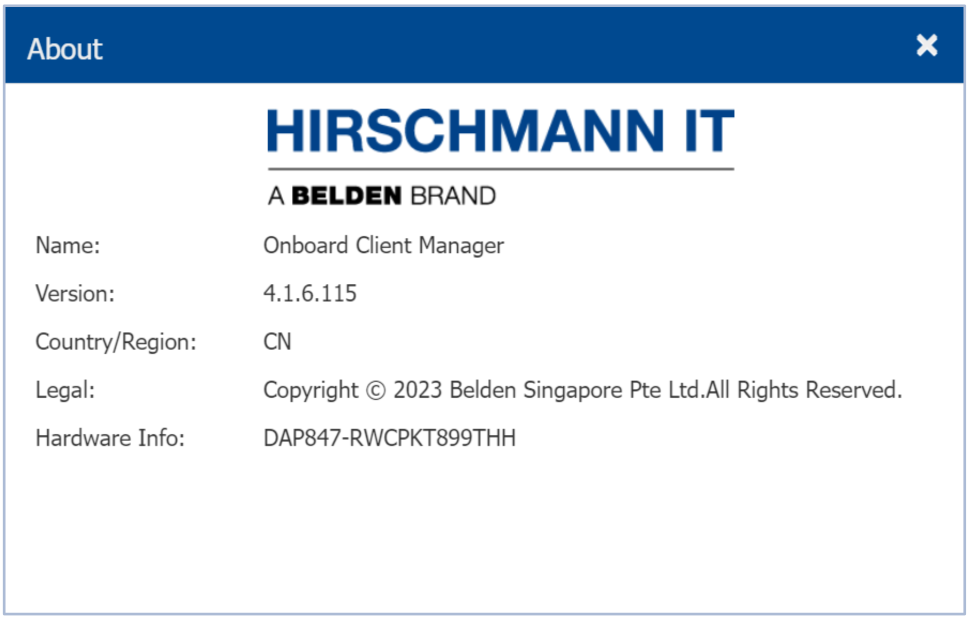
4.6 Other information

For additional information about the DAP847-XXC, such as **About**, **Tools**, click the ☰ tab located in the right-top corner.



- Figure 15: More information about DAP847-XXC**About**:

  Basic information of the DAP847-XXC cluster, such as software **name** and software **version**, **Country/Region**, etc.



About ✖

HIRSCHMANN IT
A BELDEN BRAND

Name: Onboard Client Manager
Version: 4.1.6.115
Country/Region: CN
Legal: Copyright © 2023 Belden Singapore Pte Ltd.All Rights Reserved.
Hardware Info: DAP847-RWCPKT899THH

Figure 16: About page

- **Tools:** Some basic troubleshooting tools integrated in DAP847-XXC; See “Tools” on page 69.
- **Reset:** Sets the DAP847-XXC back to the **Factory setting**.
- **Reboot:** Reboots DAP847-XXC.

- **Logout:** Logouts current User.

5 DAP847-XXC cluster management

This chapter describes how to configure and manage DAP847-XXC in the cluster.

The DAP847-XXC cluster solution is a controller-less-based architecture. The DAP847-XXC can establish an autonomous cluster, in which there are 3 types of Client roles: Primary Virtual Management (PVM), Secondary Virtual Management (SVM), and MEMBER.

This chapter describes how to manage the cluster and how to check and clear configuration, upgrade firmware, and perform system configurations via Web GUI, including system time configuration, syslog configuration, and SNMP configuration.

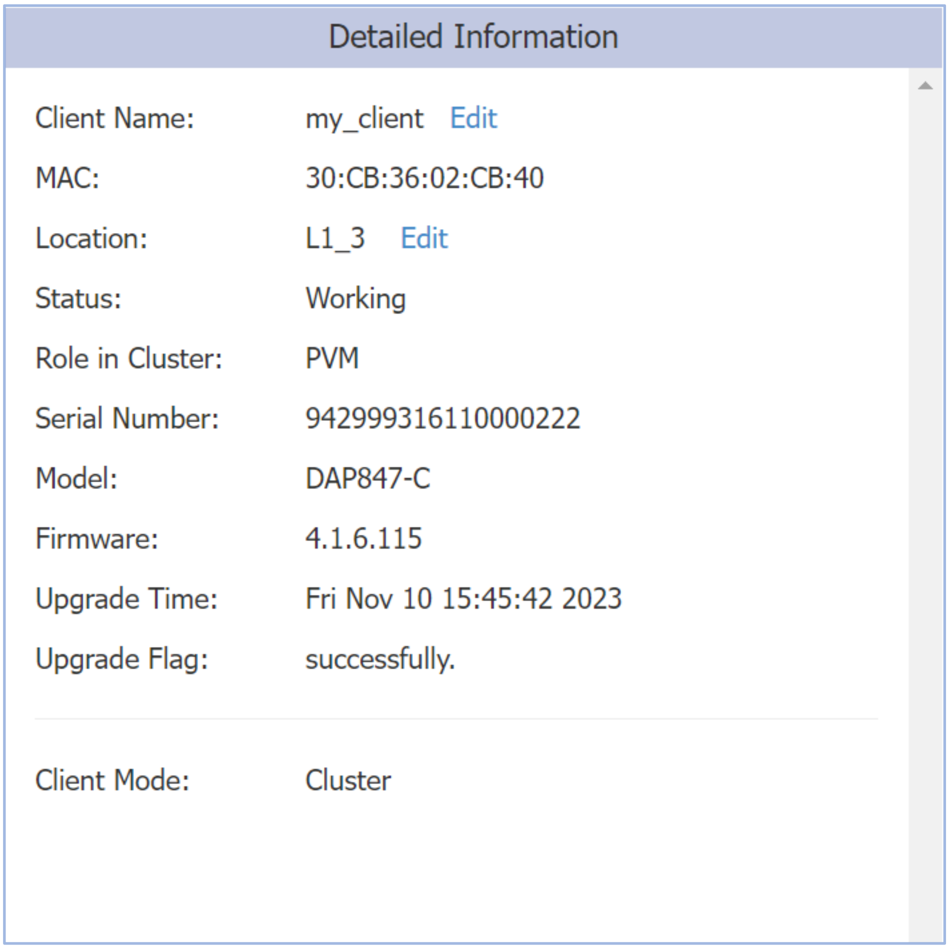
You can launch into the DAP847-XXC cluster management window by clicking the IP address in Onboard Client window.

This chapter contains the following topics:

- Check detailed information of DAP847-XXC
- Modify DAP847-XXC name and location
- Check DAP847-XXC current configuration
- Reboot DAP847-XXC
- Clear configuration
- Upgrade all firmware
- Cluster info management
- Accounts management
- System time configuration
- Syslog configuration
- SNMP configuration

5.1 Check detailed information of DAP847-XXC

You can view the detailed DAP847-XXC information displayed in the right window of the DAP847-XXC configuration window by clicking the related Client item. You can modify the **Client Name** and **Location** on this window by clicking **Edit**.



Detailed Information

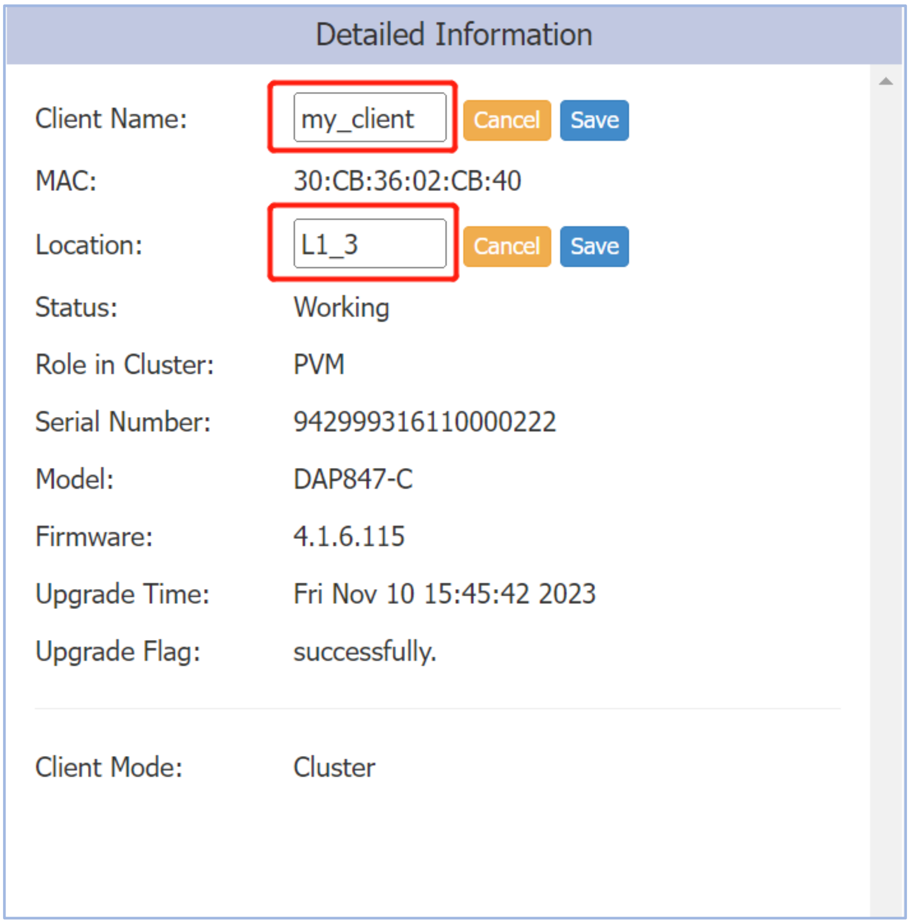
Client Name:	my_client Edit
MAC:	30:CB:36:02:CB:40
Location:	L1_3 Edit
Status:	Working
Role in Cluster:	PVM
Serial Number:	942999316110000222
Model:	DAP847-C
Firmware:	4.1.6.115
Upgrade Time:	Fri Nov 10 15:45:42 2023
Upgrade Flag:	successfully.
Client Mode:	Cluster

Figure 17 DAP847-XXC detailed information

5.2 Modify DAP847-XXC name and location

☐ Click the “**Edit**” icon, enter the “**Client Name**” and “**Location**” field to identify the specific DAP847-XXC.

In the default setting, the DAP847-XXC is named with the last 2 bytes of its MAC address, for example, AP-CB:40.



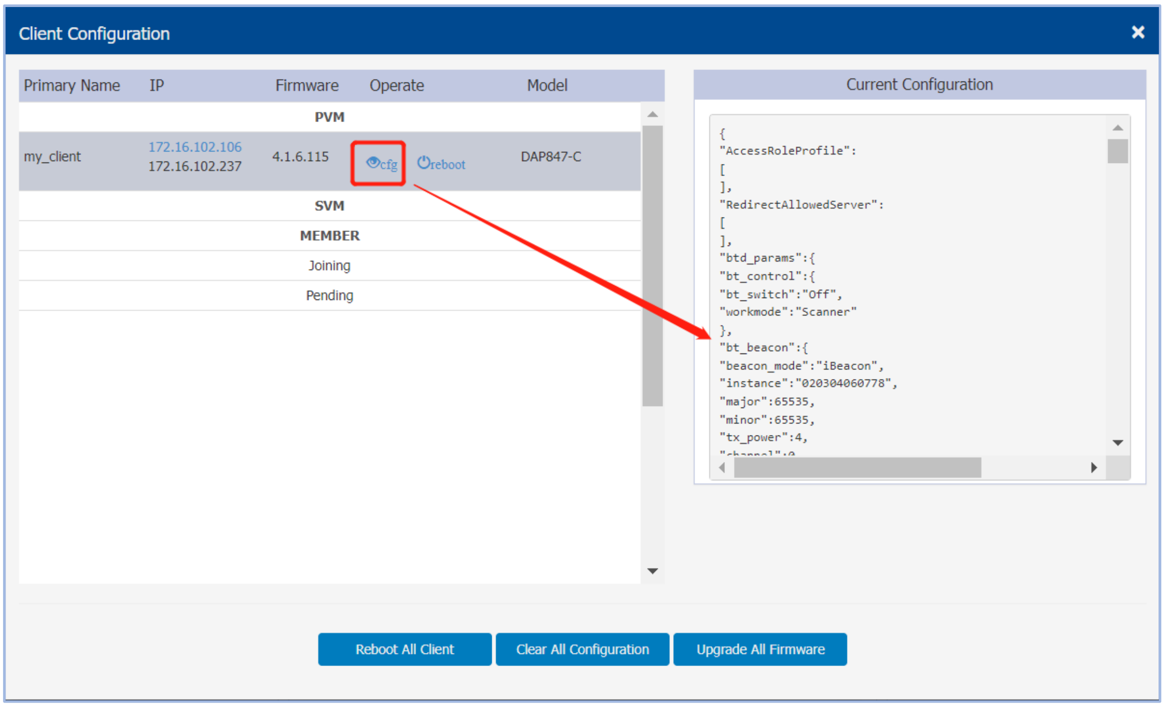
Detailed Information

Client Name:	my_client
MAC:	30:CB:36:02:CB:40
Location:	L1_3
Status:	Working
Role in Cluster:	PVM
Serial Number:	942999316110000222
Model:	DAP847-C
Firmware:	4.1.6.115
Upgrade Time:	Fri Nov 10 15:45:42 2023
Upgrade Flag:	successfully.
Client Mode:	Cluster

Figure 18: Modify DAP847-XXC name and location

5.3 Check DAP847-XXC current configuration

In the Client Configuration list, click 👁cfg to check the current configuration details on the right window, see Figure 19.



Client Configuration

Primary Name	IP	Firmware	Operate	Model
		PVM		
my_client	172.16.102.106 172.16.102.237	4.1.6.115	👁cfg ⏻reboot	DAP847-C
		SVM		
		MEMBER		
		Joining		
		Pending		

Current Configuration

```
{
"AccessRoleProfile":
[
],
"RedirectAllowedServer":
[
],
"btd_params":{
"bt_control":{
"bt_switch":"Off",
"workmode":"Scanner"
},
"bt_beacon":{
"beacon_mode":"iBeacon",
"instance":"020304060778",
"major":65535,
"minor":65535,
"tx_power":4,
"channel":0
```

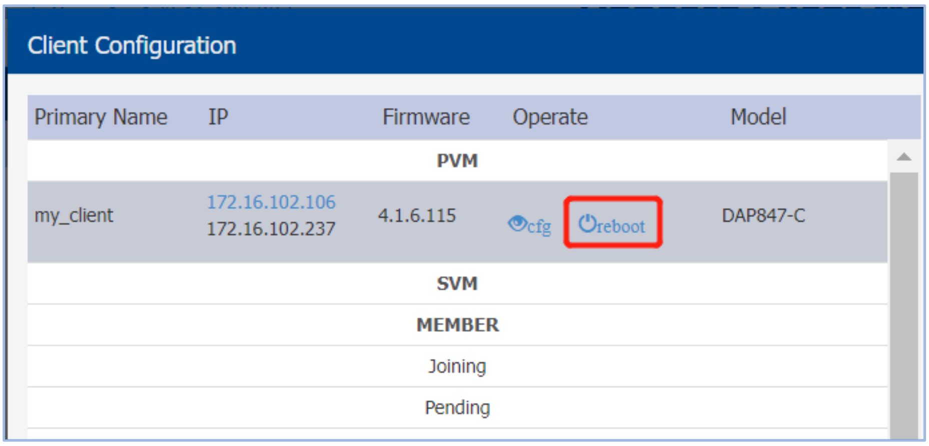
Figure 19: Check DAP847-XXC current configuration

5.4 Reboot DAP847-XXC

You can manually reboot DAP847-XXC based on the actual requirement.

■ Reboot one single DAP847-XXC in the cluster

□ Click ⏻reboot to reboot the specific DAP847-XXC in the Client Configuration window.

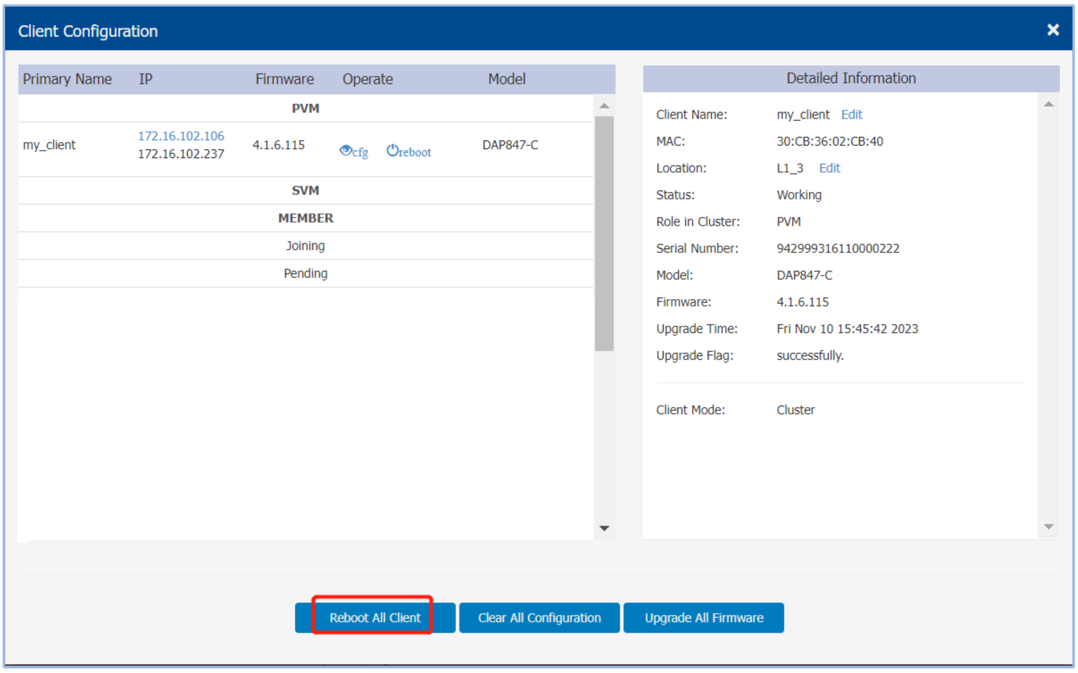


Primary Name	IP	Firmware	Operate	Model
		PVM		
my_client	172.16.102.106 172.16.102.237	4.1.6.115	cfg ⏻reboot	DAP847-C
		SVM		
		MEMBER		
		Joining		
		Pending		

Figure 20: Reboot a DAP847-XXC in the cluster

■ Reboot All DAP847-XXC in the cluster

□ Click the “**Reboot All Client**” button at the bottom left-hand corner of the Client Configuration window. All DAP847-XXCs in the cluster will be rebooted.



Primary Name	IP	Firmware	Operate	Model
		PVM		
my_client	172.16.102.106 172.16.102.237	4.1.6.115	cfg ⏻reboot	DAP847-C
		SVM		
		MEMBER		
		Joining		
		Pending		

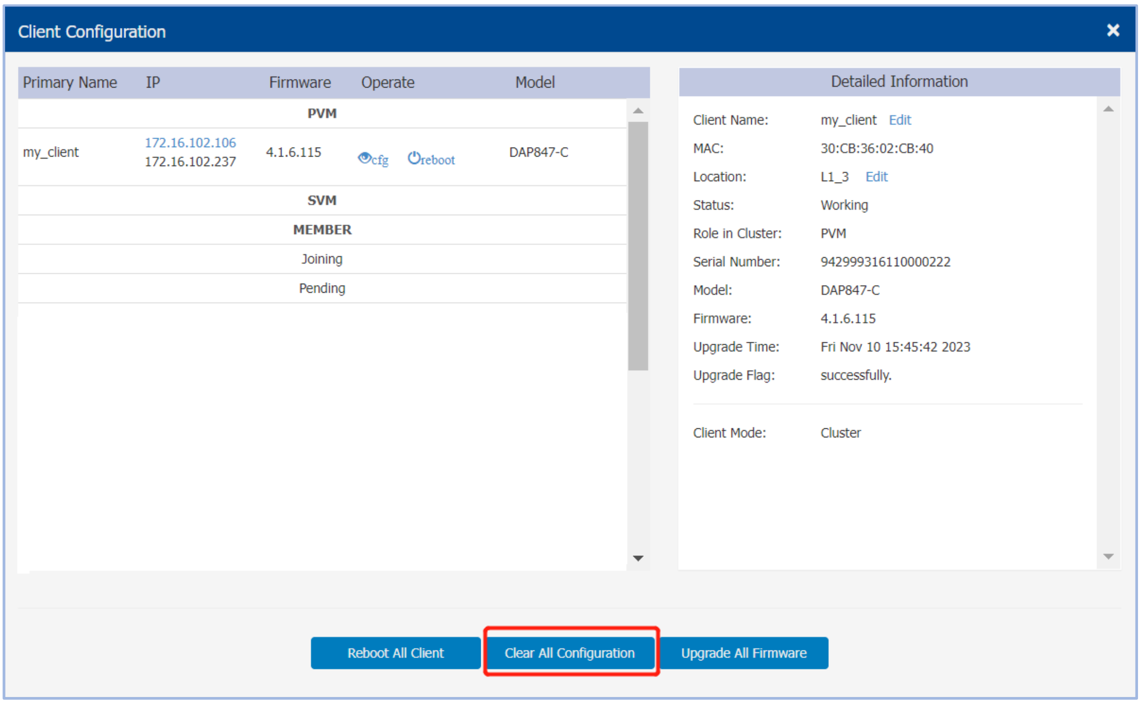
Detailed Information

Client Name:	my_client Edit
MAC:	30:CB:36:02:CB:40
Location:	L1_3 Edit
Status:	Working
Role in Cluster:	PVM
Serial Number:	942999316110000222
Model:	DAP847-C
Firmware:	4.1.6.115
Upgrade Time:	Fri Nov 10 15:45:42 2023
Upgrade Flag:	successfully.
Client Mode:	Cluster

Figure 21: Reboot all DAP847-XXC in the cluster

5.5 Clear configuration

□ Click the “**Clear All Configuration**” button in the Client Configuration window to clear the configurations of all the DAP847-XXCs in the cluster and make the DAP847-XXCs back to the “**factory setting**”.



Client Configuration

Primary Name	IP	Firmware	Operate	Model
		PVM		
my_client	172.16.102.106 172.16.102.237	4.1.6.115	cfg reboot	DAP847-C
		SVM		
		MEMBER		
		Joining		
		Pending		

Detailed Information

Client Name:	my_client Edit
MAC:	30:CB:36:02:CB:40
Location:	L1_3 Edit
Status:	Working
Role in Cluster:	PVM
Serial Number:	942999316110000222
Model:	DAP847-C
Firmware:	4.1.6.115
Upgrade Time:	Fri Nov 10 15:45:42 2023
Upgrade Flag:	successfully.
Client Mode:	Cluster

Figure 22: Clear all configuration

Note: Below are 3 more ways to restore DAP847-XXC to “**factory settings**”:

- Long press the “**reset**” button for at least 6 seconds.
- In Console or SSH connection under “**support**” account:

  □ Type the command `ssudo firstboot`.

  □ Type the command `ssudo reboot`.

  After reboot, the system recovers to “**factory settings**”. The default username is **support**. The default password is **Belden996!@#**.

- Click the ☰ tab in the right-top corner of dashboard and choose "**Reset**" option in the list.

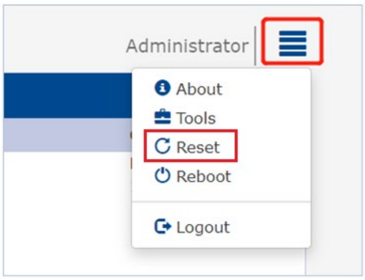


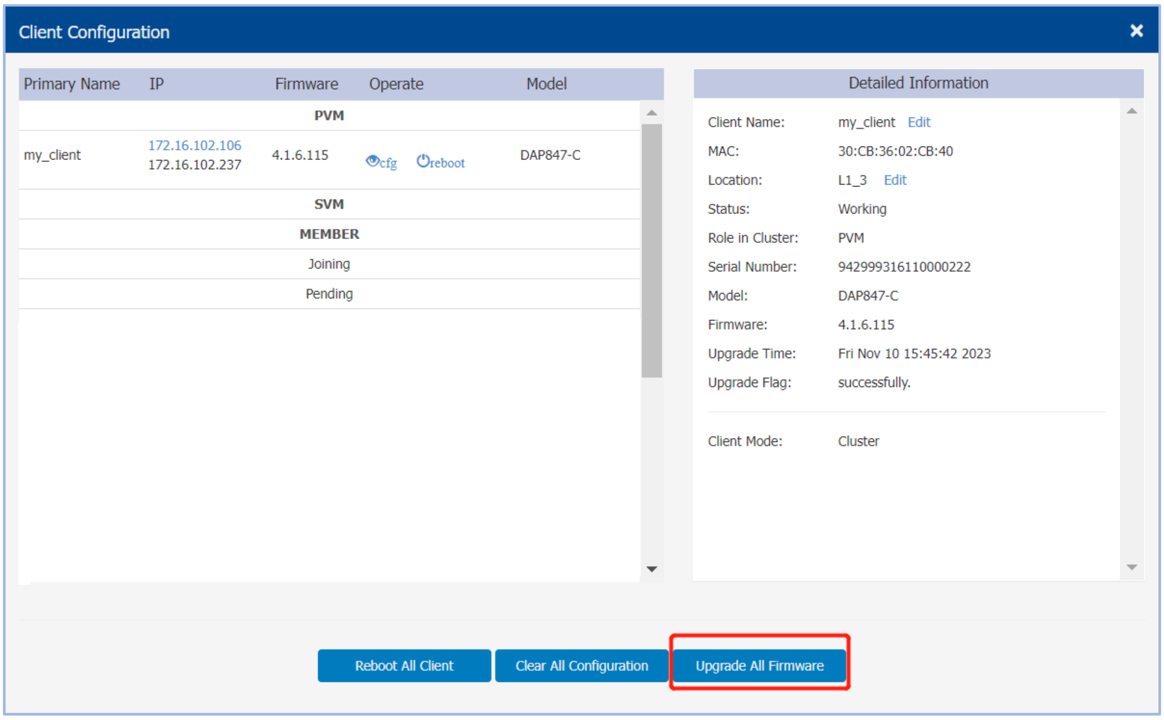
Figure 23: Reset DAP847-XXC

5.6 Upgrade all firmware

Before upgrading the DAP847-XXC, you need to prepare the firmware file for upload.

You can download the firmware file from https://catalog.belden.com. Save the firmware file to the local disk of the PC that is being used to connect the DAP847-XXC or to a remote TFTP or SFTP server.

- □ Click the "**Upgrade All Firmware**" button in the Client Configuration window and the DAP847-XXC Upgrade window will pop up.



Client Configuration

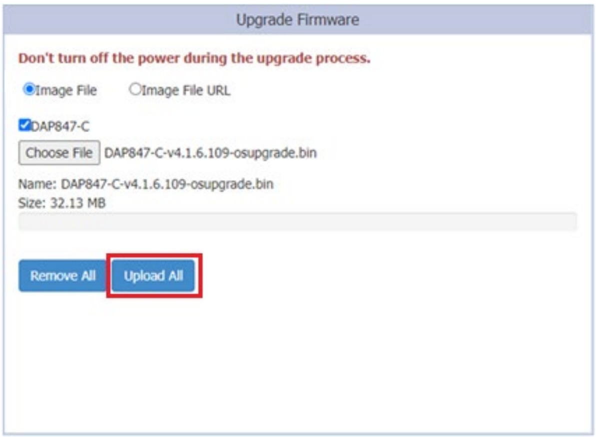
Primary Name	IP	Firmware	Operate	Model
PVM				
my_client	172.16.102.106 172.16.102.237	4.1.6.115	cfg reboot	DAP847-C
SVM				
MEMBER				
Joining				
Pending				

Detailed Information

Client Name:	my_client Edit
MAC:	30:CB:36:02:CB:40
Location:	L1_3 Edit
Status:	Working
Role in Cluster:	PVM
Serial Number:	942999316110000222
Model:	DAP847-C
Firmware:	4.1.6.115
Upgrade Time:	Fri Nov 10 15:45:42 2023
Upgrade Flag:	successfully.
Client Mode:	Cluster

Figure 24: Go to client upgrade window

- □ Select the firmware version to be upgraded, and click "**Upload All**" to upload the firmware file.



Upgrade Firmware

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

● Image File ○ Image File URL

☑ DAP847-C

Choose File DAP847-C-v4.1.6.109-osupgrade.bin

Name: DAP847-C-v4.1.6.109-osupgrade.bin
Size: 32.13 MB

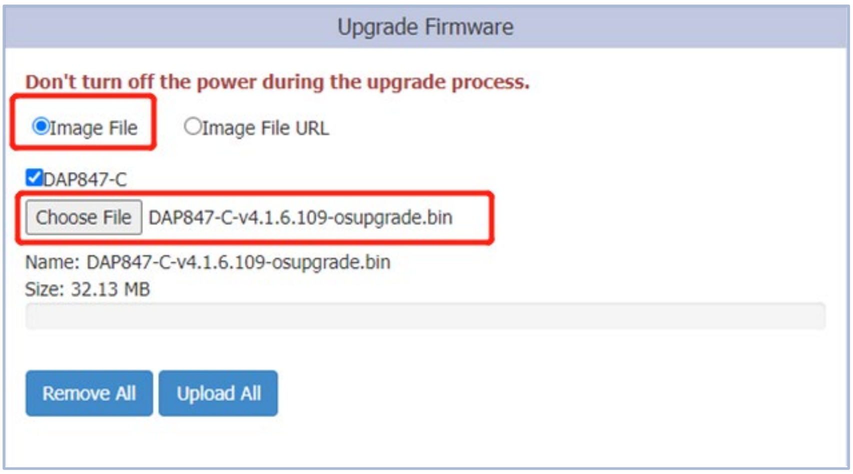
Figure 25: Upgrade DAP847-XXC

Note: It takes 5 minutes to upgrade the client firmware.

There are 3 ways to upload DAP847-XXC firmware:

▶ Upload local file

- □ Select the "**Image File**" option and click "**Choose File**" to upload the firmware from the local image file.
- □ Click the "**Upload All**" button to perform the upgrade operation.
- □ Click the "**Remove All**" button to cancel the upgrade operation.



Upgrade Firmware

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

● Image File ○ Image File URL

☑ DAP847-C

Choose File DAP847-C-v4.1.6.109-osupgrade.bin

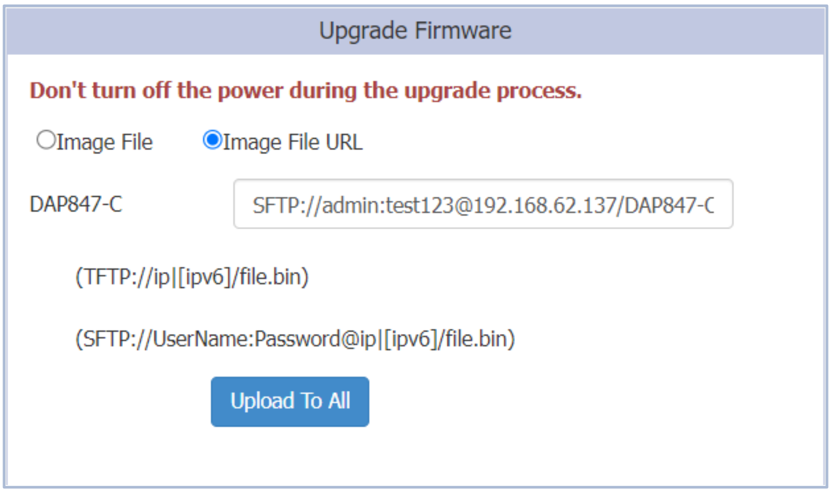
Name: DAP847-C-v4.1.6.109-osupgrade.bin

Size: 32.13 MB

Figure 26: Upload firmware from local file

▶ SFTP

- □ 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 upgrade operation.



Upgrade Firmware

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

○ Image File ● Image File URL

DAP847-C SFTP://admin:test123@192.168.62.137/DAP847-C

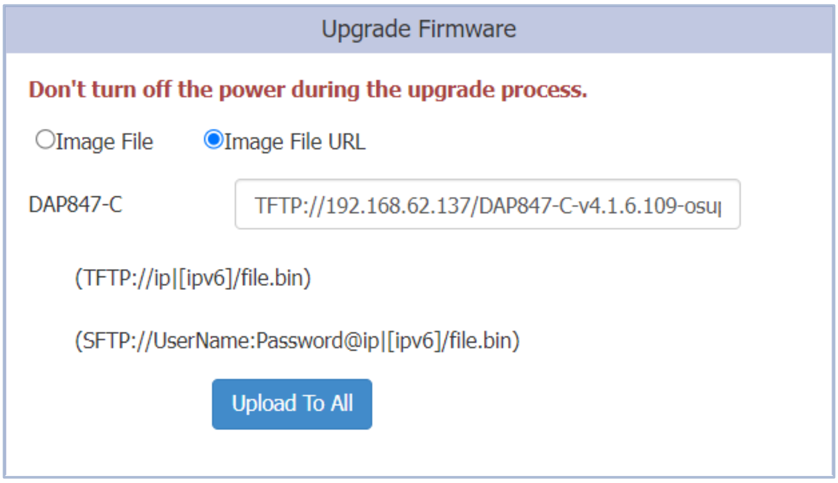
(TFTP://ip|[ipv6]/file.bin)

(SFTP://UserName:Password@ip|[ipv6]/file.bin)

Figure 27: Upload AP firmware by using SFTP

▶ TFTP

- □ Upload the DAP847-XXC firmware by using TFTP.
- □ Enter the specified URL with the TFTP Server IP address and firmware file name.
- □ Click “**Upload To All**” button to perform the upgrade operation.



Upgrade Firmware

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

○Image File ●Image File URL

DAP847-C TFTP://192.168.62.137/DAP847-C-v4.1.6.109-osu|

(TFTP://ip|[ipv6]/file.bin)

(SFTP://UserName:Password@ip|[ipv6]/file.bin)

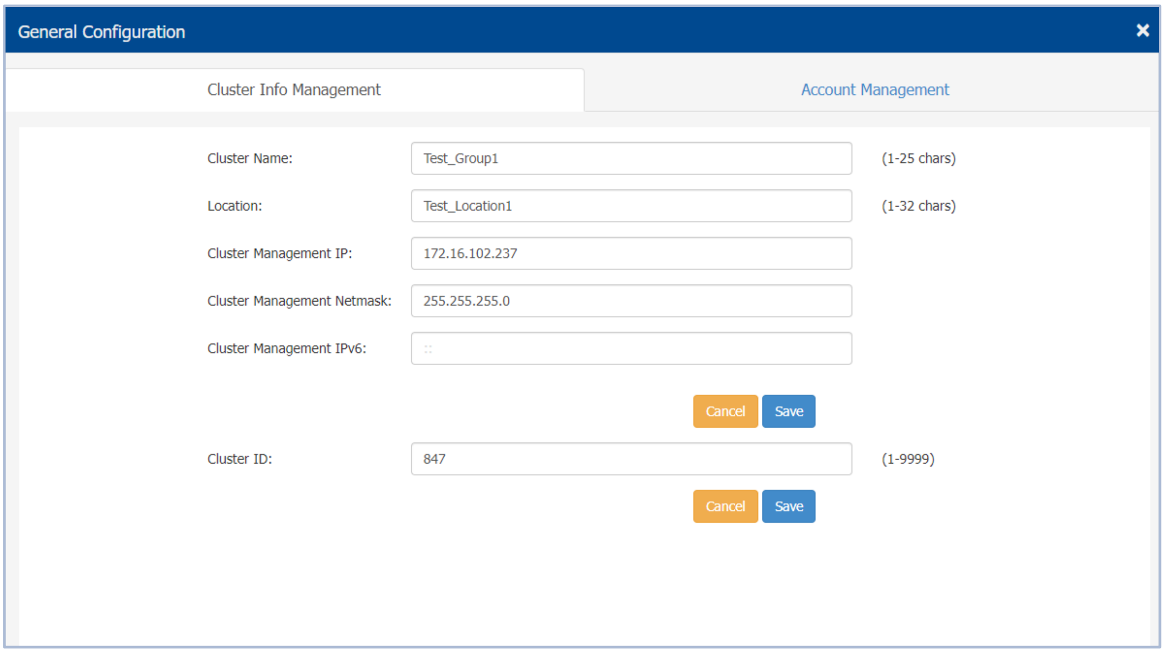
Figure 28: Upload client firmware by using TFTP

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 Cache.

5.7 Cluster info management

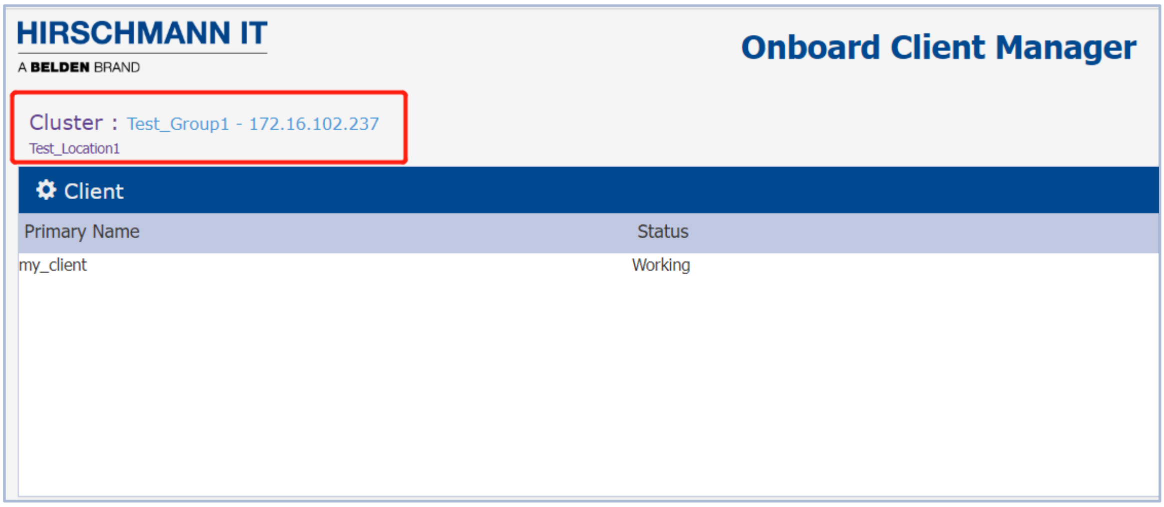
Navigate to the window **System** → **General Configuration** to configure or modify the cluster attributes. The DAP847-XXC Cluster Information displays at the top of the Dashboard, such as **Cluster Name** and **Cluster Management IP**.

In the **Cluster Info Management** tab, the administrator can manually set the management IP address, which is a virtual IP assigned to the PVM to manage the DAP847-XXC cluster.



Cluster Name:	Test_Group1	(1-25 chars)
Location:	Test_Location1	(1-32 chars)
Cluster Management IP:	172.16.102.237	
Cluster Management Netmask:	255.255.255.0	
Cluster Management IPv6:	::	
Cluster ID:	847	(1-9999)

Figure 29: Cluster configuration



Cluster : Test_Group1 - 172.16.102.237
Test_Location1

Primary Name	Status
my_client	Working

Figure 30: Cluster information

The key parameters are described as follows:

Parameter	Specification
Cluster Name	Name of the DAP847-XXC Cluster.
Location	Location of the DAP847-XXC Cluster.
Cluster Management IP	A virtual IP address for DAP847-XXC Cluster management
Cluster Management Netmask	Netmask of Cluster Management IP.
Cluster Management IPv6	A virtual IPv6 address for DAP847-XXC Cluster management.
Cluster ID	Identification of the DAP847-XXC Cluster, the default Cluster ID is 30000.

5.8 Accounts management

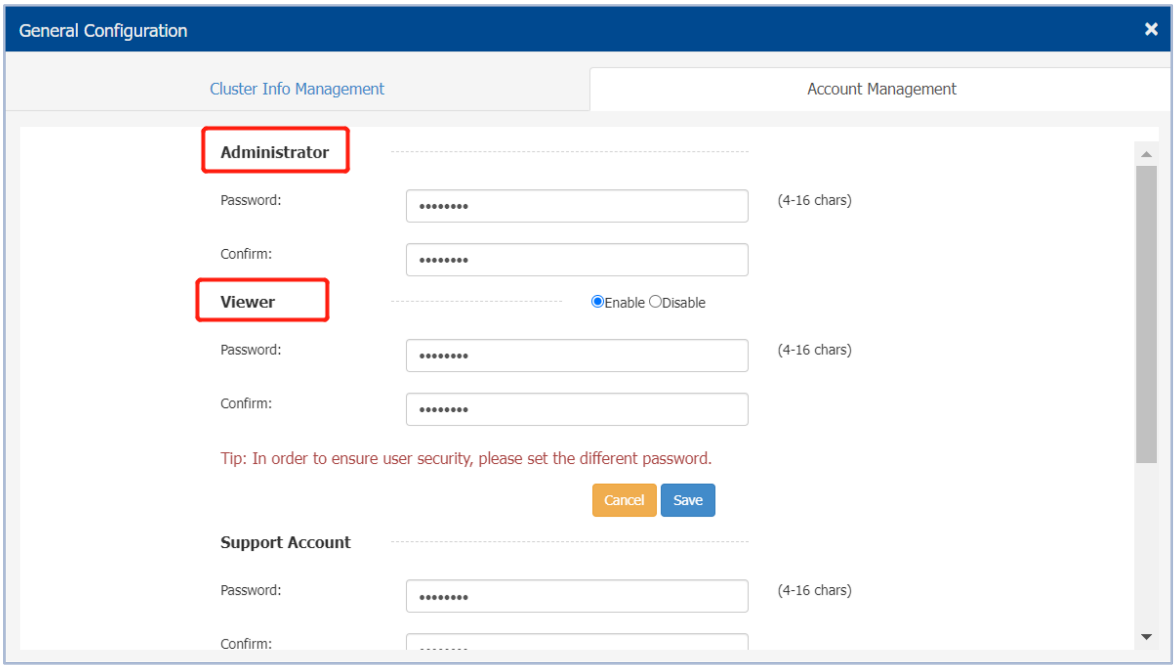
5.8.1 Manage web GUI accounts

There are 2 accounts that can log in to the Web GUI with different privileges:

- **Administrator:** The administrator account has the highest privilege. It can view and modify the system configurations, such as enabling and disabling Viewer accounts, deleting configuration, and resetting DAP847-XXC to "**factory setting**".
- **Viewer:** The viewer account only has permission to view the DAP847-XXC configuration.

You can log in to each account at the same time. When the same account is logged in, the previous session is terminated. In the default setting, only the Administrator account is enabled, the Viewer account is disabled.

In the **Account Management** tab, you can enable or disable the Viewer account, and change the password for Administrator and Viewer.



General Configuration

Cluster Info Management | Account Management

Administrator

Password: •••••••• (4-16 chars)

Confirm: ••••••••

Viewer ● Enable ○ Disable

Password: •••••••• (4-16 chars)

Confirm: ••••••••

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

Support Account

Password: •••••••• (4-16 chars)

Confirm: ••••••••

Figure 31: Account management

5.8.2 Manage CLI account

Support Account and **Root Account** can log in to the DAP847-XXC CLI with different privileges.

Administrator can change the login password for those command line accounts. The root password is a string held by the customer only and used to generate the real root access credential by DAP847-XXC.

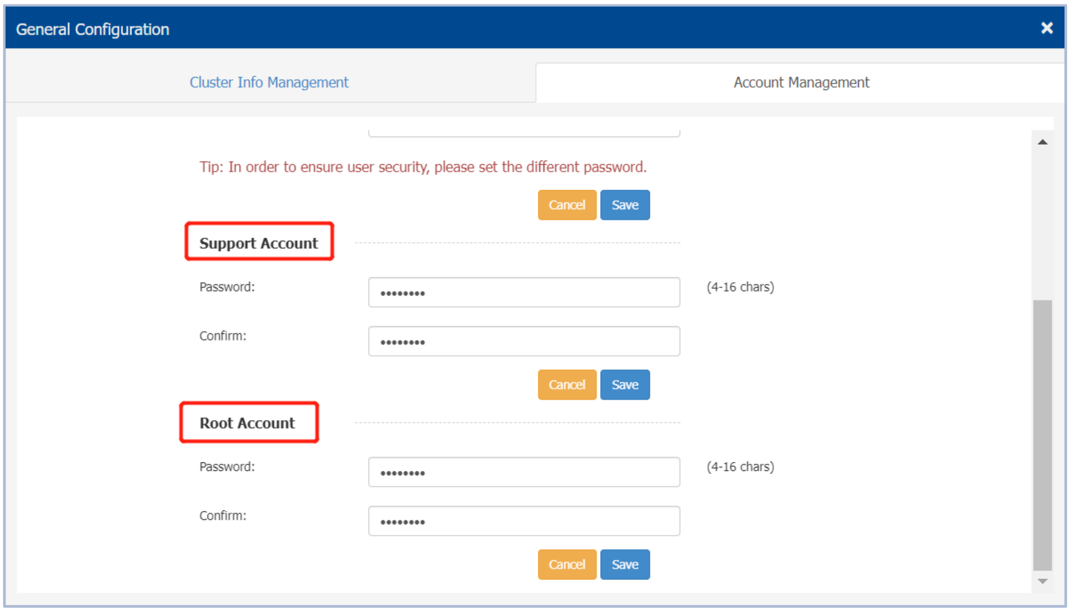


Figure 32: CLI account management

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

5.9 System time configuration

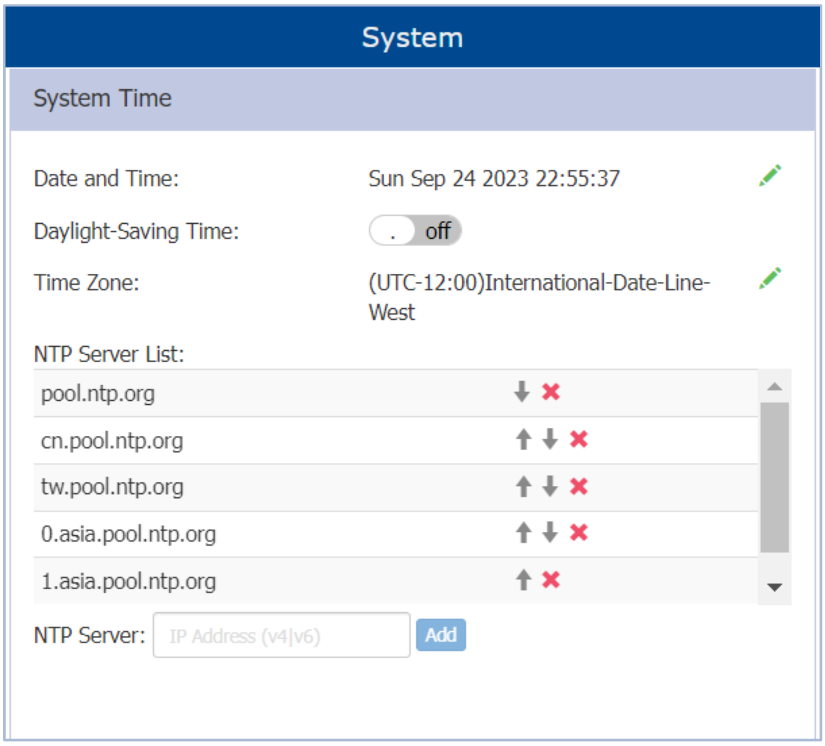
It is essential to have the correct system time for DAP847-XXC. It can record communications with other network devices, and system logs, especially for troubleshooting, which all depends on the correct system time.

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

NTP (RFC 1305 - Network Time Protocol) is a networking 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-XXC in the cluster synchronizes system time with the NTP server every 15 minutes.



System

System Time

Date and Time: Sun Sep 24 2023 22:55:37

Daylight-Saving Time: off

Time Zone: (UTC-12:00)International-Date-Line-West

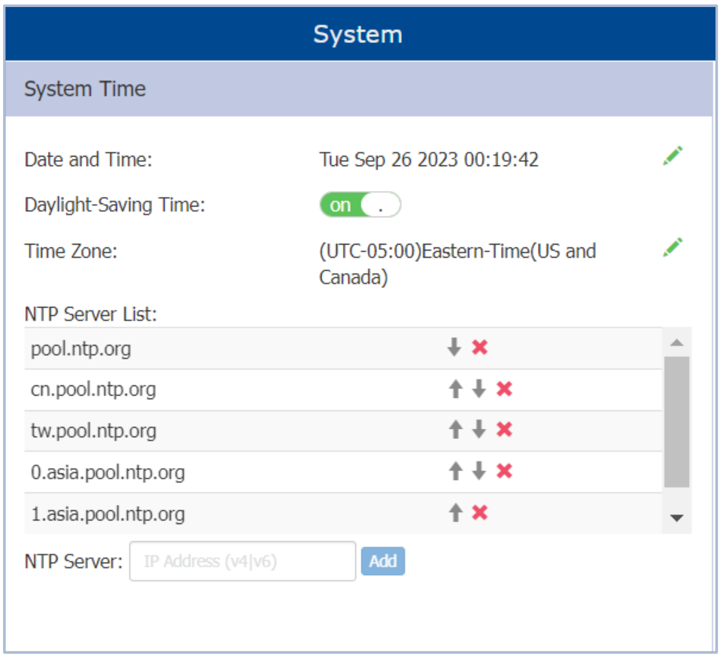
NTP Server List:

- pool.ntp.org
- cn.pool.ntp.org
- tw.pool.ntp.org
- 0.asia.pool.ntp.org
- 1.asia.pool.ntp.org

NTP Server: IP Address (v4|v6)

Figure 33: System time configuration with Daylight-Saving Time off

You can also specify the “**Daylight-Saving Time**” and “**Time Zone**” of the DAP847-XXC cluster to coordinate with the local time. “**Daylight-Saving Time”** is automatically enabled in the supporting time zone. See Figure 34.



System Time

Date and Time: Tue Sep 26 2023 00:19:42

Daylight-Saving Time: on

Time Zone: (UTC-05:00)Eastern-Time(US and Canada)

NTP Server List:

pool.ntp.org	↓ ✖
cn.pool.ntp.org	↑ ↓ ✖
tw.pool.ntp.org	↑ ↓ ✖
0.asia.pool.ntp.org	↑ ↓ ✖
1.asia.pool.ntp.org	↑ ✖

NTP Server: IP Address (v4|v6) Add

Figure 34: System Time Configuration with Daylight-Saving Time on

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

5.10 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 based on the importance and message types.

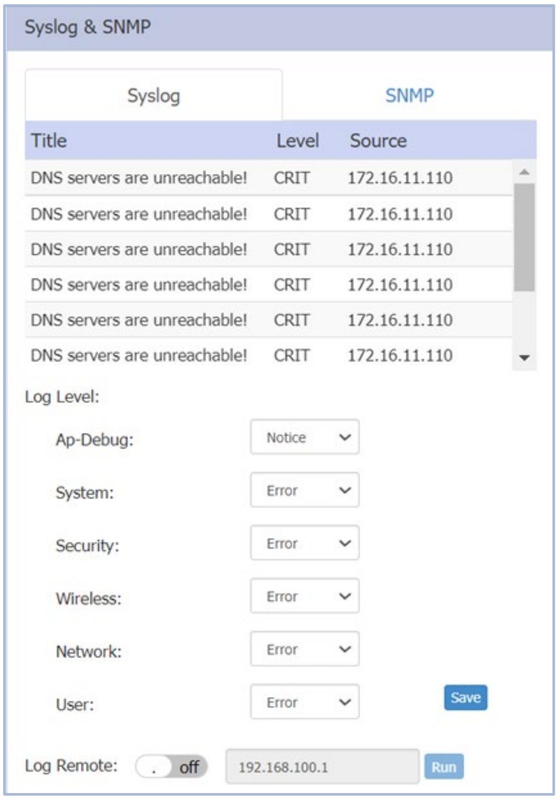
Through Syslog, administrators can monitor system status in real-time, track the running status of applications, discover security events, and conduct audits, etc.

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

Logs of the DAP847-XXC 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-XXC 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-XXC 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 35.



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

Log Level:

Ap-Debug:	Notice
System:	Error
Security:	Error
Wireless:	Error
Network:	Error
User:	Error

Log Remote: off 192.168.100.1

Figure 35: Syslog configuration

■ Log level

The log level is the severity setting of the Syslog message. If a level is specified, the DAP847-XXC 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 separate 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-XXC supports configuring a remote log server for receiving and storing Syslog messages sent by DAP847-XXC.

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

Level Value	Severity	Keyword	Description
0	Emergency	EMERG	System is unusable
1	Alert	ALERT	Should be corrected immediately
2	Critical	CRIT	Critical conditions
3	Error	ERR	Error conditions

Level Value	Severity	Keyword	Description
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 5: Syslog severity definition

5.11 SNMP configuration

SNMP (Simple Network Management Protocol) is a standard protocol for 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-XXC 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 with the concept of community and enhanced security.
- SNMPv3 introduces a User-based Security Model (USM), which facilitates a higher level of security.

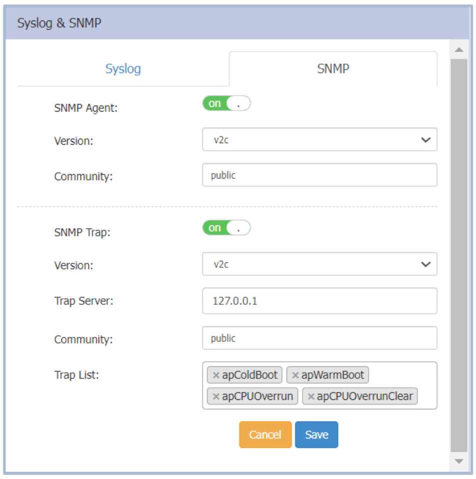
Currently, DAP847-XXC supports SNMPv2c and SNMPv3. SNMPv1 is not supported by DAP847-XXC due to its low security.

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**.

5.11.1 Configure SNMPv2c

You can configure the following parameters for SNMPv2c:



SNMP Agent: on

Version: v2c

Community: public

SNMP Trap: on

Version: v2c

Trap Server: 127.0.0.1

Community: public

Trap List: × apColdBoot × apWarmBoot × apCPUOverrun × apCPUOverrunClear

Figure 36: SNMPv2c configuration

The key parameters are described as follows:

Configure SNMPv2c Agent

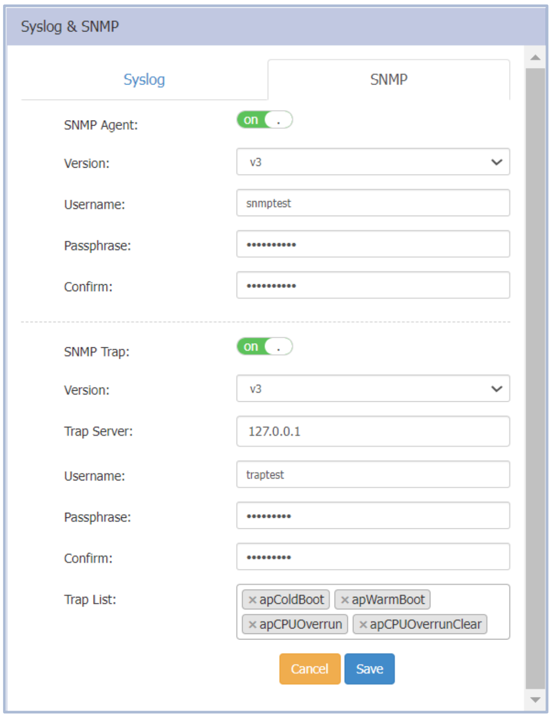
Parameter	Description
SNMP Agent	Enables or disables the SNMP Agent on DAP847-XXC.
Version	Selects the required SNMP version of v2c.
Community	The credential used to communicate between SNMP Agent and the network management system (NMS). The value needs to be the same for DAP847-XXC and NMS to communicate.

Configure SNMPv2c Trap

Parameter	Description
SNMP Trap	Enables or disables DAP847-XXC 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.

5.11.2 Configure SNMPv3

You can configure the following parameters for SNMPv3:



SNMP Agent: on

Version: v3

Username: snmptest

Passphrase: ••••••••••

Confirm: ••••••••••

SNMP Trap: on

Version: v3

Trap Server: 127.0.0.1

Username: traptest

Passphrase: •••••••••

Confirm: •••••••••

Trap List: × apColdBoot × apWarmBoot × apCPUOverrun × apCPUOverrunClear

Figure 37: SNMPv3 configuration

The key parameters are described as follows:

Configure SNMPv3 Agent

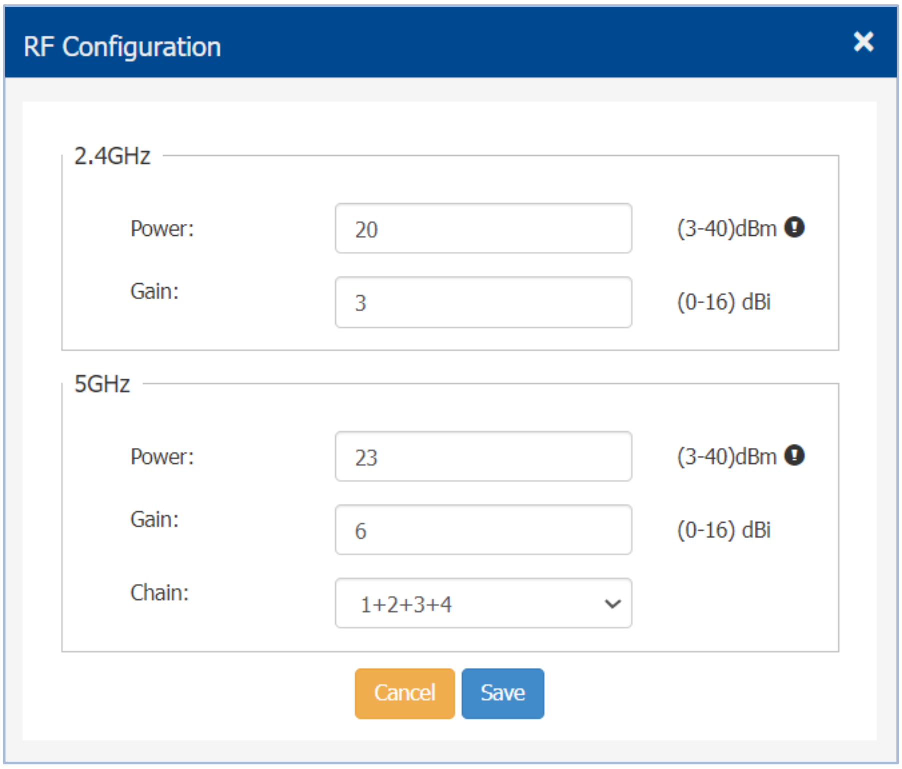
Parameter	Description
SNMP Agent	Enables or disables the SNMP Agent on DAP847-XXC. The network management platform can fetch information from DAP847-XXC through the SNMP protocol.
Version	Selects the required SNMP version of v3.
Username	Identifies and authenticates users of SNMP management systems.
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-XXC 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.

6 RF configuration

You can modify the transmission power and External Antenna Gain for the DAP847-XXC in the RF Configuration Window. The transmit power was set manually by default. In manual mode, the DAP847-XXC transmitted power can be adjusted in 1 dB increments.



RF Configuration

2.4GHz

Power: 20 (3-40)dBm

Gain: 3 (0-16) dBi

5GHz

Power: 23 (3-40)dBm

Gain: 6 (0-16) dBi

Chain: 1+2+3+4

Figure 38: RF configuration window

The key parameters are described as follows:

Parameter	Specification
Channel Width	Configures the channel width. Channel width is used to control how broad the signal is for transferring data. By increasing the channel width, you can increase the speed and throughput. However, larger channel width brings more unstable transmission in crowded areas with a lot of frequency noise and interference. The channel width support is different between 2.4 GHz and 5 GHz. ▶ 2.4GHz – 20 MHz / 40 MHz ▶ 5GHz – 20 MHz / 40 MHz / 80 MHz Note that some high-frequency channels (e.g., 165) do not support 40 MHz / 80 MHz. If an AP is using these channels, a Channel Width of

Parameter	Specification
	40 MHz / 80 MHz will not be available.
Power	Specifies the transmit power on specific radio, it indicates that transmission EIRP setting on the radio includes the External Antenna Gain.
Gain	Specifies the gain value for the external antenna.
Chain	Indicates that the external antenna MIMO mode on DAP847-XXC ▶ 1 means that MIMO mode is 1x1, corresponds to ANT1 ▶ 2 means that MIMO mode is 1x1, corresponds to ANT2 ▶ 3 means that MIMO mode is 1x1, corresponds to ANT3 ▶ 4 means that MIMO mode is 1x1, corresponds to ANT4 ▶ 1+2 means that MIMO mode is 2x2, corresponds to ANT1+ANT2 ▶ 1+4 means that MIMO mode is 2x2, corresponds to ANT1+ANT4 ▶ 1+2+3 means that MIMO mode is 3X3, corresponds to ANT1+ANT2+ANT3 ▶ 1+2+3+4 means that MIMO mode is 4X4, correspond to ANT1+ANT2+ANT3+ANT4

7 Network configuration

The Network Window focuses on the DAP847-XXC network configuration.

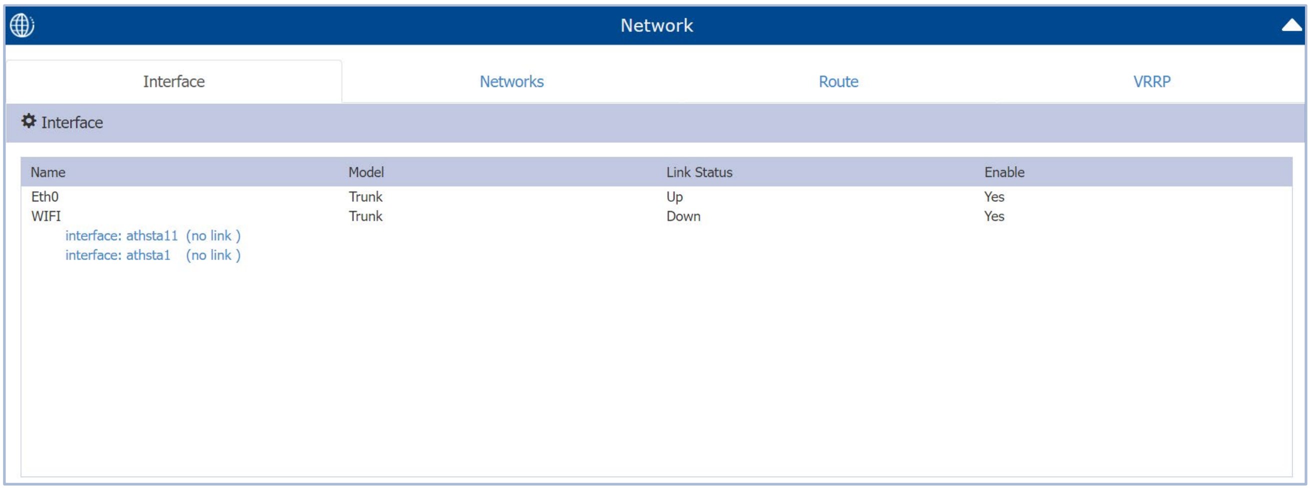
This chapter contains the following topics:

7.1 Interface configuration

You can check the DAP847-XXC interfaces details in interface configuration window and manage DAP847-XXC wireless connection to DAP847-XXA.

For configuration of the DAP847-XXC interface, navigate to **Web UI** → **Network** → **Interface** → **Interface Configuration**.

7.1.1 Interface overview

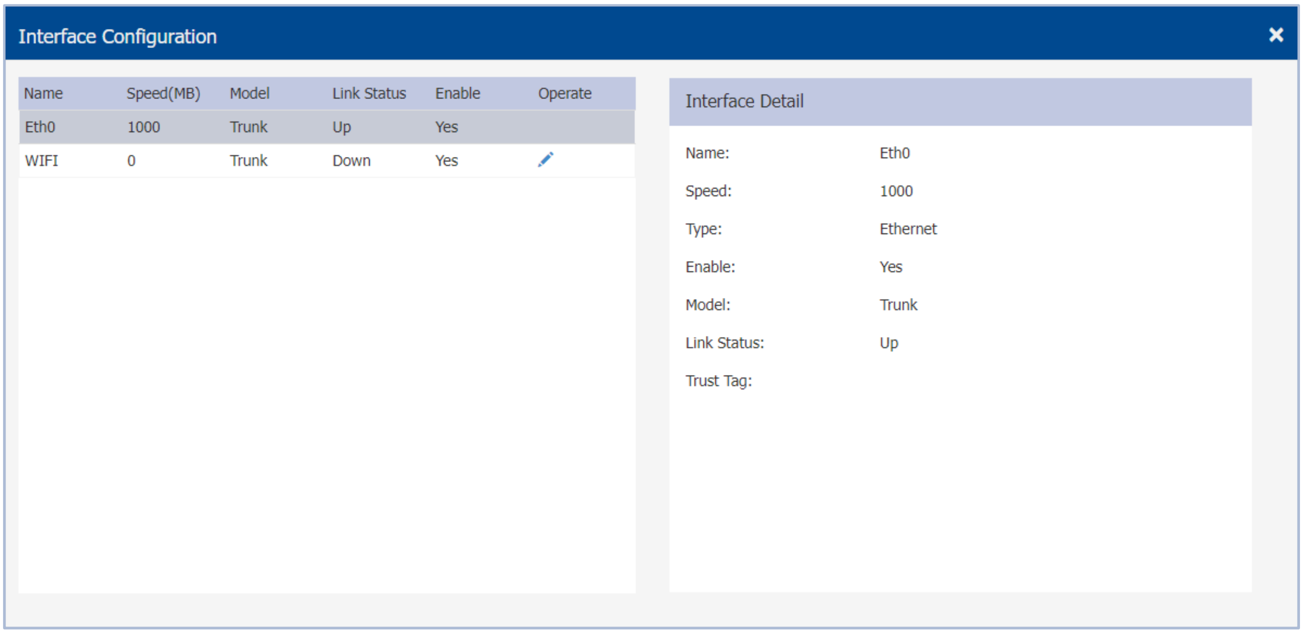


Name	Model	Link Status	Enable
Eth0	Trunk	Up	Yes
WIFI	Trunk	Down	Yes
interface: athsta11 (no link)			
interface: athsta1 (no link)			

Figure 39: DAP847-XXC interface window

The key parameters are described as follows:

Parameter	Specification
Eth0	The downlink interface of DAP847-XXC (Wired interface).
WIFI	The uplink interface of DAP847-XXC, to connect with DAP847-XXA (Wireless interface).



Name	Speed(MB)	Model	Link Status	Enable	Operate
Eth0	1000	Trunk	Up	Yes	
WIFI	0	Trunk	Down	Yes	✎

Interface Detail

Name: Eth0
Speed: 1000
Type: Ethernet
Enable: Yes
Model: Trunk
Link Status: Up
Trust Tag:

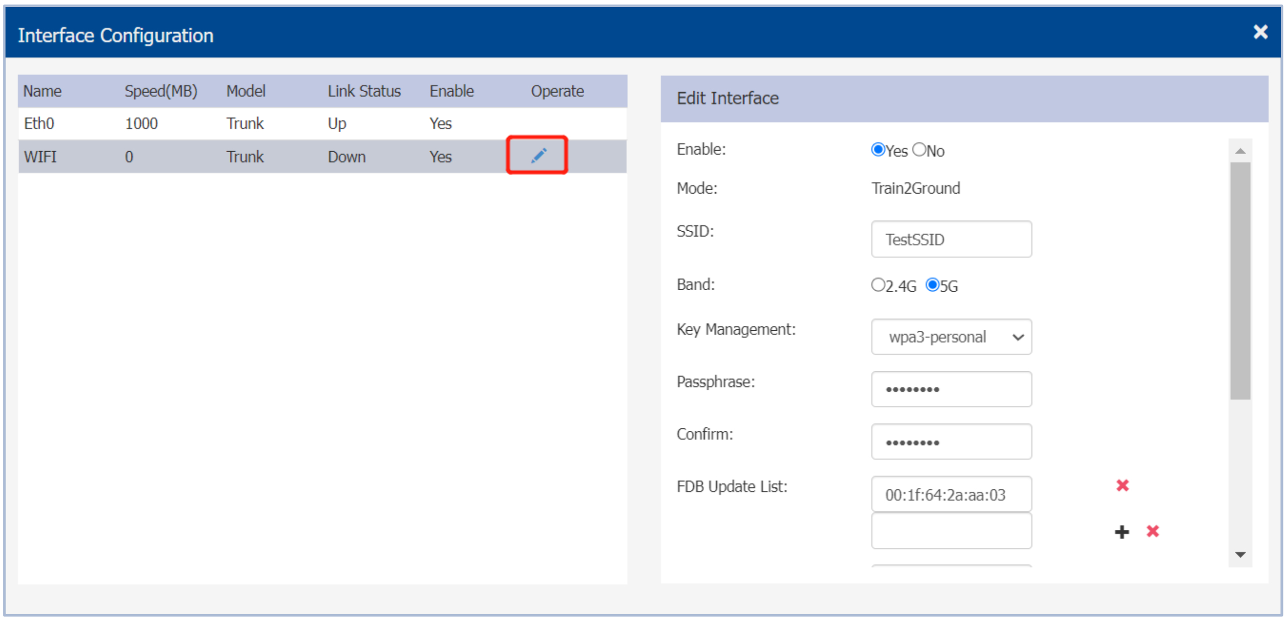
Figure 40: DAP847-XXC interface configuration

The key parameters for each client are described as follows:

Parameter	Specification
Speed	Link speed of the client interface.
Type	Port type. The port type of Eth0 is Ethernet. The port type of Wi-Fi is Mesh.
Enable	Displays whether the client interface is enabled or disabled.
Model	VLAN access mode or VLAN trunk mode.
Link Status	Up or down.
Operate	Applied to WIFI interface for wireless configuration.

7.1.2 Wireless network configuration on DAP847-XXC

In the Interface Configuration window, find the interface named “**WIFI**” and click ✎ to configure your wireless network. See configurations of the DAP847-XXA for wireless connection between DAP847-XXC and DAP847-XXA.



Interface Configuration

Name	Speed(MB)	Model	Link Status	Enable	Operate
Eth0	1000	Trunk	Up	Yes	
WIFI	0	Trunk	Down	Yes	

Edit Interface

Enable: ● Yes ○ No

Mode: Train2Ground

SSID: TestSSID

Band: ○ 2.4G ● 5G

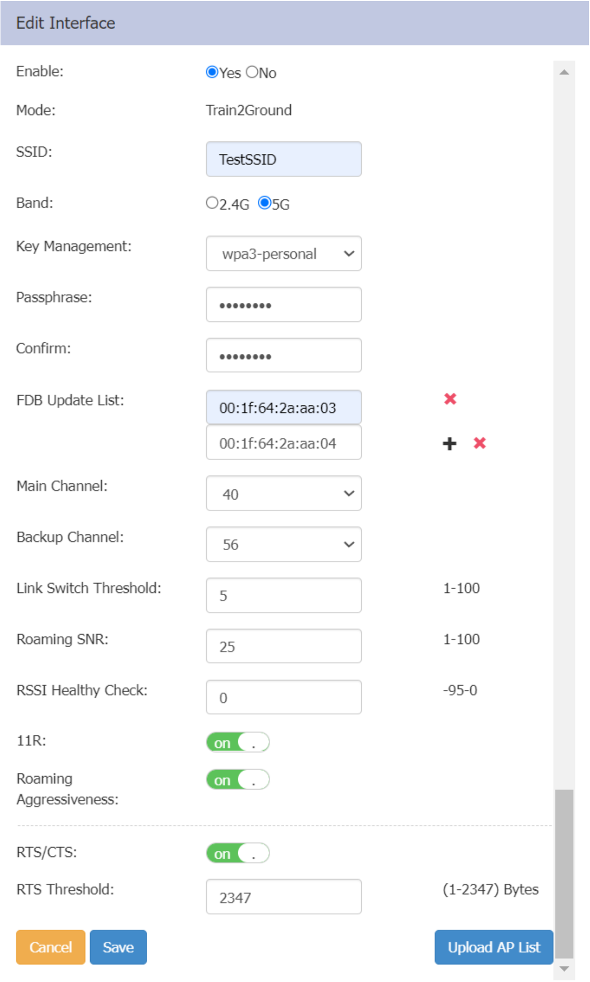
Key Management: wpa3-personal

Passphrase: ••••••••

Confirm: ••••••••

FDB Update List: 00:1f:64:2a:aa:03

Figure 41: Edit WIFI interface



Edit Interface

Enable: ● Yes ○ No

Mode: Train2Ground

SSID: TestSSID

Band: ○ 2.4G ● 5G

Key Management: wpa3-personal

Passphrase: ••••••••

Confirm: ••••••••

FDB Update List: 00:1f:64:2a:aa:03
00:1f:64:2a:aa:04

Main Channel: 40

Backup Channel: 56

Link Switch Threshold: 5 1-100

Roaming SNR: 25 1-100

RSSI Healthy Check: 0 -95-0

11R: on

Roaming Aggressiveness: on

RTS/CTS: on

RTS Threshold: 2347 (1-2347) Bytes

Figure 42: WIFI interface configuration

The key parameters are described as follows:

Parameter	Specification
Enable	Enables or disables the wireless interface on DAP847-XXC.
Mode	Train2Ground.
SSID	SSID for wireless connection to DAP847-XXA. Needs to be the same as the SSID configured in DAP847-XXA.
Band	The working band for wireless connection, 2.4G or 5G.
Key Management	The security level defined on DAP847-XXC, for more information, see Chapter 7.1.3 Key Management.
Passphrase	Password used to set up wireless connection.
FDB Update List	A MAC address list for some specific silence device connected to DAP847-XXC. When DAP847-XXC connects to a new DAP847-XXA, the DAP847-XXC will send RARP packets to DAP847-XXA on behalf of silence device to notify the switch to update the FDB list.
Main Channel	The preferred working channel on DAP847-XXC.
Backup Channel	The backup working channel on DAP847-XXC. If there is no target SSID scanned on Main Channel, DAP847-XXC will switch to Backup Channel.
Link Switch Threshold	DAP847-XXC has 2 wireless connections at the same time, Active and Standby. When the detected signal of Standby is greater than that of Active, and the difference exceeds the threshold, signal switching occurs. Standby is switched to Active, and the original Active becomes Standby.
Roaming SNR	Indicates the minimum signal strength supported by DAP847-XXC for wireless connections. If DAP847-XXC detects that the signal strength of DAP847-XXA is less than the value, it will no longer connect to this DAP847-XXA .
RSSI Healthy Check	This function works in conjunction with SNMP Trap. When the signal strength detected by the Scan radio falls below the set threshold, it triggers the cpeScanAbnormal Trap.
11R	Enables or disables 802.11r, which is disabled by default. Enabling the 11R function minimizes the delay when the DAP847-XXC switches from one BSS to another.
Roaming Aggressiveness	Enables or disables roaming aggressiveness, which is disabled by default. When enabled, if the Active link becomes a Standby link, and the DAP847-XXC detects a new BSS signal three times in a row with increasing strength and an SNR higher than the set Roaming SNR, the DAP847-XXC will proactively roam to the new node.
RTS/CTS	Enables or disables RTS/CTS, which is disabled by default. When enabled, the DAP847-XXC sends RTS/CTS frames to identify hidden nodes, reducing packet collisions, increased

Parameter	Specification
	retransmissions, or packet loss caused by hidden nodes
RTS Threshold	The range for the RTS threshold is 1 … 2347 bytes. The default value is 2347 bytes. When the data packet sent by the DAP847-XXC exceeds this threshold, the device first sends an RTS signal to notify the other party, preventing signal collisions.

7.1.3 Key management

There are 4 options for the Key Management methods:

- Both (wpa & wpa2)
- wpa3 personal
- wpa2-enterprise
- wpa3 enterprise

■ Both (wpa & wpa2)

This is a pre-shared key mode, both WPA and WPA2 are supported. Pre-shared key mode is an authentication model designed for home or small enterprise networks. The pre-shared key mode means the wireless connection is protected by a key and doesn't require an authentication server. Each wireless network device encrypts the network traffic using a 256-bit key. This key will be entered as a passphrase of 8 to 63 printable ASCII characters.

■ wpa3-personal

WPA3-Personal is a successor of WPA2 (Wi-Fi Protected Access version 2). WPA3-Personal adopts a stronger security encryption algorithm to resist dictionary attacks.

WPA3 provides a new key exchange protocol that uses a secure method Simultaneous Authentication of Equals (SAE) with password-based authentication that is resistant to dictionary attacks. Compared to the previous TKIP (Temporal Key Integrity Protocol) and encryption algorithm used in WPA2, WPA3-Personal provides stronger security in data transmission. In this mode, the key is entered as a passphrase of 8 to 63 printable ASCII characters.

■ wpa2-enterprise

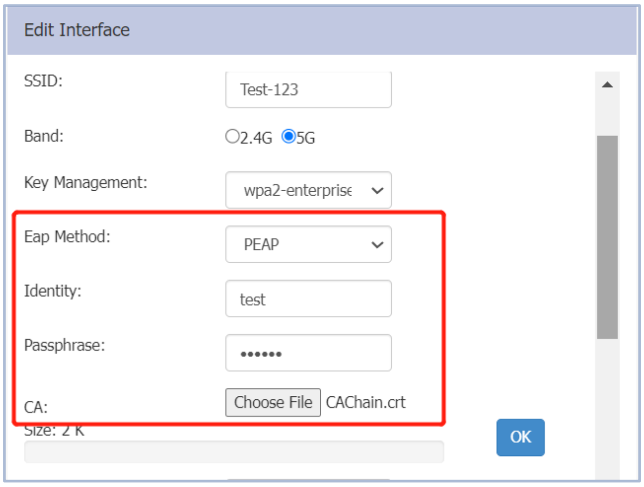
WPA2-Enterprise is an authentication method for WPA2, also known as IEEE 802.1x authentication. It is an encryption method built on the IEEE 802.1X authentication framework that requires users to authenticate with a personal certificate or username and password. It encrypts data transmissions using AES encryption algorithm to provide a higher security level. Compared to WPA2-Personal, WPA2-Enterprise provides stronger security and more flexible deployment options.

Namely, IEEE 802.1x authentication is designed for enterprise and public networks and requires a RADIUS authentication server. Enterprise is more secure than personal. This requires a complicated setup but provides additional security (e.g., protection against dictionary unauthorized access on short passwords). Various kinds of Extensible Authentication Protocols (EAP) are used for authentication.

There are 3 types of EAP methods supported in this mode:

- **PEAP**: The PEAP (Protected Extensible Authentication Protocol), also known as Protected EAP, is a protocol that encapsulates EAP within a potentially encrypted and authenticated TLS tunnel. It uses Transport Layer Security (TLS) for secure communication and authentication.

  PEAP provides a higher security level than the traditional EAP protocol, because PEAP creates a secure communication tunnel between client and server for transmitting usernames, passwords, and other authentication information. If PEAP is used, the user identity, passphrase, and a CA certificate are required and must be configured correctly.



Edit Interface

SSID: Test-123

Band: ○2.4G ●5G

Key Management: wpa2-enterprise

Eap Method: PEAP

Identity: test

Passphrase: ••••••

CA: Choose File CAChain.crt

Size: 2 K

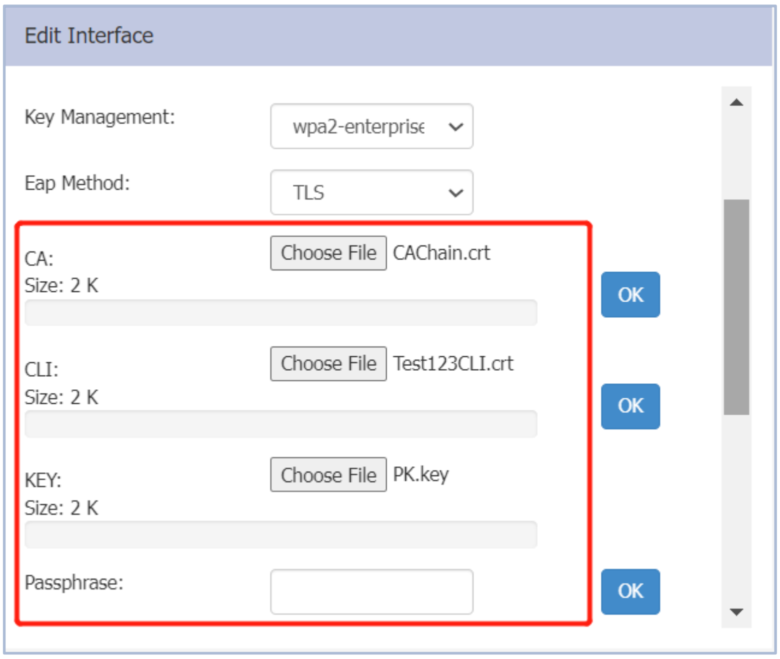
Figure 43: EAP-PEAP configuration

The key parameters are described as follows:

Parameter	Specification
Identity	Identity represents the credentials provided by DAP847-XXC for authentication.
Passphrase	The password used for authentication.
CA	A digital certificate issued by a trusted organization Certificate Authority (CA).

- **TLS**: TLS is Transport Layer Security and is a standardized version of SSL. EAP-TLS is a secure EAP authentication method that uses the TLS protocol to encrypt and authenticate communication between clients and servers.

  If TLS is used, the CA certificate, the client certificate, the KEY (Public key certificate), and the passphrase are required and must be configured correctly.



Edit Interface

Key Management: wpa2-enterprise

Eap Method: TLS

CA: Choose File CAChain.crt
Size: 2 K

CLI: Choose File Test123CLI.crt
Size: 2 K

KEY: Choose File PK.key
Size: 2 K

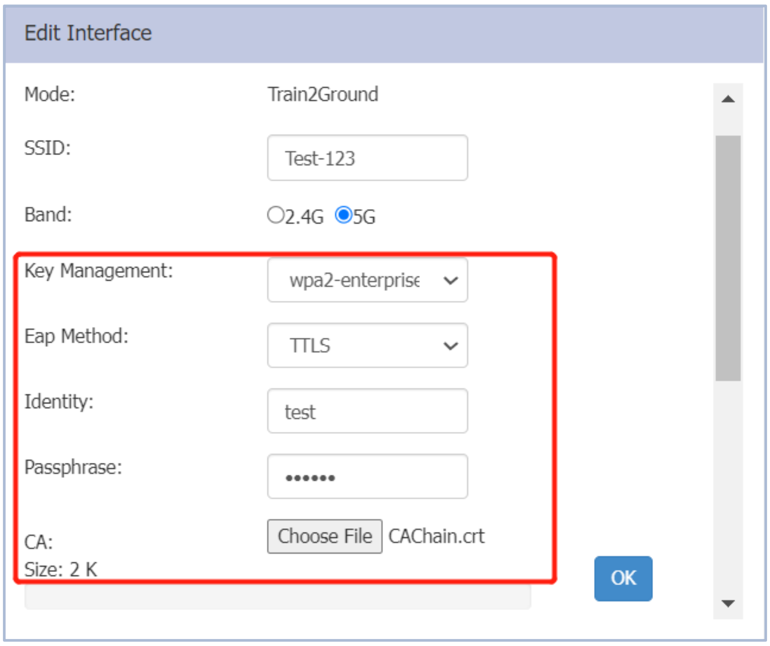
Passphrase:

Figure 44: EAP-TLS configuration

The key parameters are described as follows:

Parameter	Specification
CA	A digital certificate issued by a trusted organization Certificate Authority (CA).
CLI	Client certificate which is a self-signed certificate, or a certificate issued by a trusted CA.
KEY	Public key certificate.
Passphrase	The password used for authentication.

- **TTLS:** Tunneled Transport Layer Security is an extension of the EAP-TLS mechanism. EAP-TTLS is different from EAP-TLS because it does away with the EAP-TLS requirement of a supplicant-side certificate. Only the authentication server component requires a digital certificate. If TTLS used, the user identity, passphrase, and a CA certificate are required and should be configured correctly.



Edit Interface

Mode: Train2Ground

SSID: Test-123

Band: ○2.4G ●5G

Key Management: wpa2-enterprise

Eap Method: TTLS

Identity: test

Passphrase: ••••••

CA: Choose File CAChain.crt

Size: 2 K

Figure 45: EAP-TTLS configuration

The key parameters are described as follows:

Parameter	Specification
Identity	Identity represents the credentials provided by DAP847-XXC for authentication.
Passphrase	The password used for authentication.
CA	A digital certificate issued by a trusted organization Certificate Authority (CA).

■ wpa3-enterprise

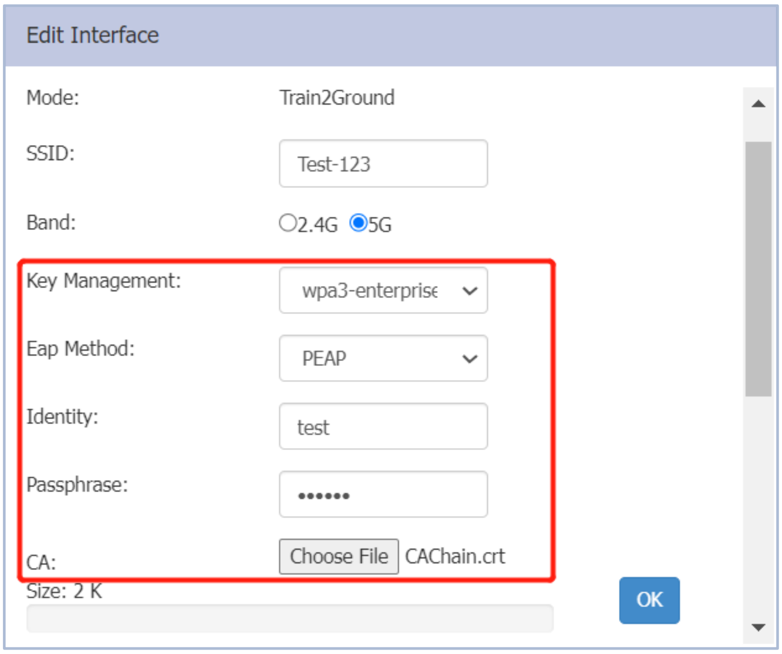
WPA3-Enterprise is designed specifically for enterprise-level users and scenarios that require a higher security protection, such as financial institutions, governments, and enterprises, and can provide a higher level of security than WPA2-Enterprise.

WPA3-Enterprise adds WPA3-Enterprise 192-bit to WPA2-Enterprise as a more secure option. 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 features Easy Connect, which simplifies pairing smart home devices, and features Enhanced Open, to make device connections more secure and convenient. These features give WPA3-Enterprise greater capability in securing the network.

There are 3 types of EAP methods supported in this mode:

- **PEAP:** The PEAP (Protected Extensible Authentication Protocol), also known as Protected EAP, is a protocol that encapsulates EAP within a potentially encrypted and authenticated TLS tunnel. PEAP provides a higher security level than the traditional EAP protocol, because PEAP creates a secure communication tunnel between client and server for transmitting usernames, passwords, and other authentication information. PEAP is one of the most used EAP types supported by WPA3. If PEAP is used, the user identity, passphrase, and a CA certificate are required and should be configured correctly.


Edit Interface

Mode: Train2Ground

SSID: Test-123

Band: ○2.4G ●5G

Key Management: wpa3-enterprise

Eap Method: PEAP

Identity: test

Passphrase: ••••••

CA: Choose File CAChain.crt

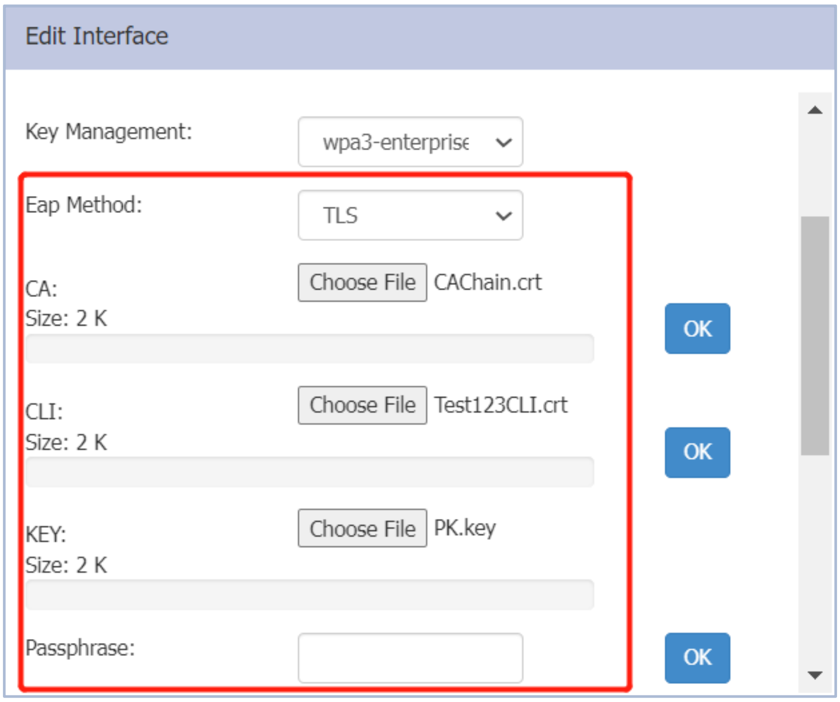
Size: 2 K

Figure 46: EAP-PEAP configuration

The key parameters are described as follows:

Parameter	**Specification**
Identity	Identity represents the credentials provided by DAP847-XXC for authentication.
Passphrase	The password used for authentication.
CA	A digital certificate issued by a trusted organization Certificate Authority (CA).

- **TLS**: When using EAP-TLS for authentication in WPA3, users need to provide a certificate which can be a self-signed certificate or a certificate issued by a trusted CA. EAP-TLS in WPA3 supports multiple cipher suites, including AES-GCM-256, SHA384, etc. It can provide powerful encryption and authentication functions, ensuring the security of user connections. If TLS used, the CA certificate, the client certificate, the KEY (Public key certificate) and the passphrase are required and should be configured correctly.



Edit Interface

Key Management: wpa3-enterprise

Eap Method: TLS

CA: Size: 2 K — Choose File CAChain.crt

CLI: Size: 2 K — Choose File Test123CLI.crt

KEY: Size: 2 K — Choose File PK.key

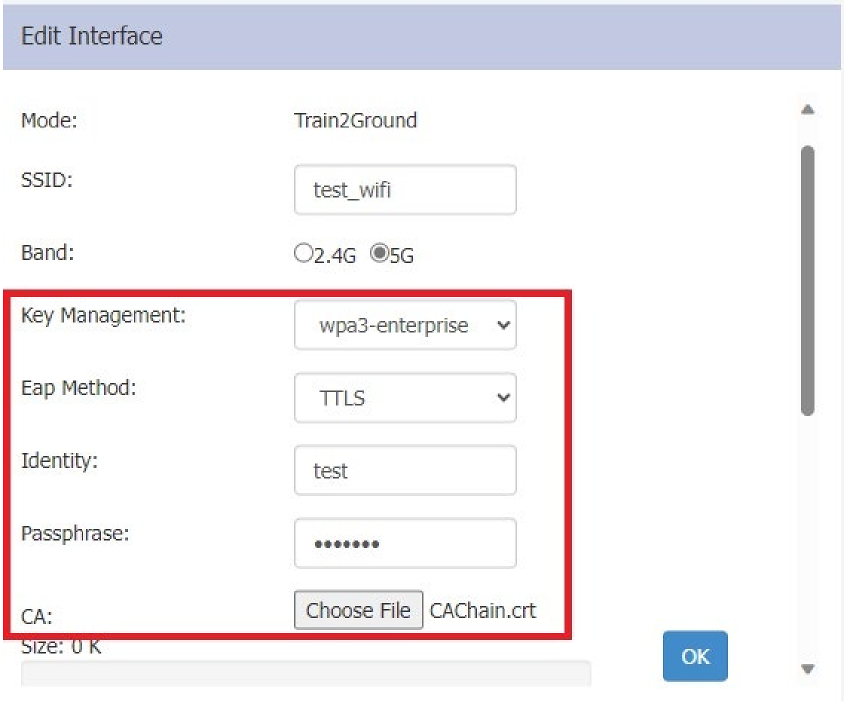
Passphrase:

Figure 47: EAP-TLS configuration

The key parameters are described as follows:

Parameter	Specification
CA	A digital certificate issued by a trusted organization Certificate Authority (CA).
CLI	Client certificate which is a self-signed certificate, or a certificate issued by a trusted CA.
KEY	Public key certificate.
Passphrase	The password used for authentication.

- **TTLS**: The WPA3 Enterprise supports the cipher suite used by EAP-TTLS, providing the best compatibility and security. Tunneled Transport Layer Security is an extension of the EAP-TLS mechanism. EAP-TTLS is different from EAP-TLS because it does away with the EAP-TLS requirement of a supplicant-side certificate. Only the authentication server component requires a digital certificate. If TTLS is used, the user identity, passphrase and a CA certificate are required and should be configured correctly.



Edit Interface

Mode: Train2Ground

SSID: test_wifi

Band: ○2.4G ●5G

Key Management: wpa3-enterprise

Eap Method: TTLS

Identity: test

Passphrase: •••••••

CA: Choose File CAChain.crt

Size: 0 K

Figure 48: EAP-TTLS configuration

The key parameters are described as follows:

Parameter	Specification
Identity	Identity represents the credentials provided by DAP847-XXC for authentication.
Passphrase	The password used for authentication.
CA	A digital certificate issued by a trusted organization Certificate Authority (CA).

Note:

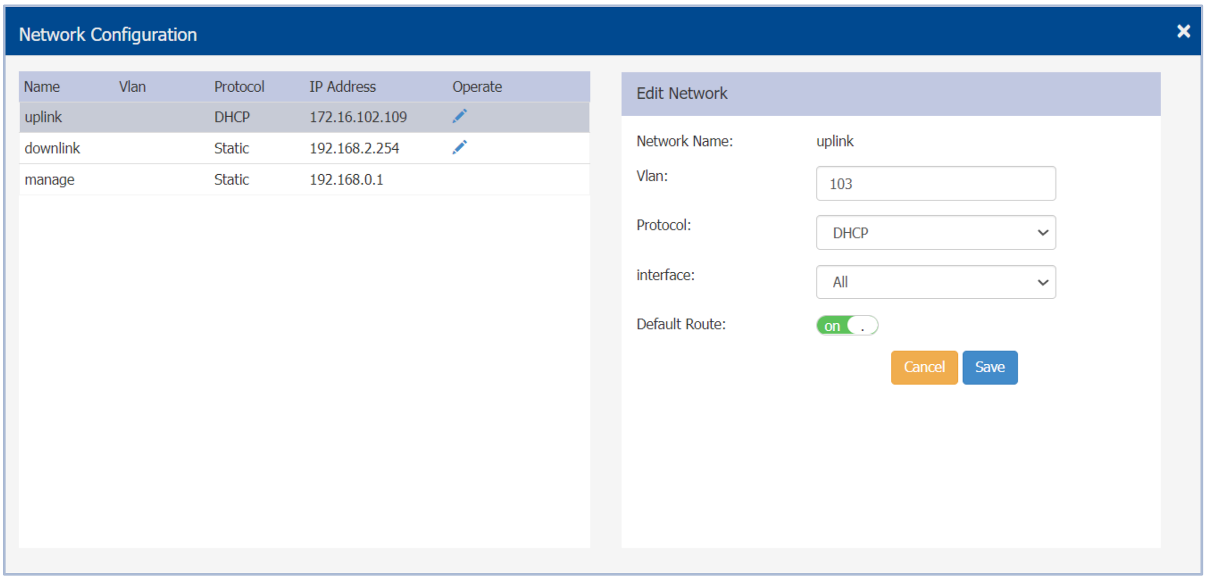
To use EAP-TLS authentication function, the system time of the DAP847-XXC must be consistent with the validity period of the CA certificate.

7.2 Network configuration

Parameters for the uplink interface of DAP847-XXC can be configured for different scenarios and network configuration requirements, including VLAN, DHCP, and Static IP.

For the configuration, navigate to **Network → Networks**.

- Click ✏ to configure the uplink port and obtain the IP address from an outside DHCP server.



Network Configuration

Name	Vlan	Protocol	IP Address	Operate
uplink		DHCP	172.16.102.109	✏
downlink		Static	192.168.2.254	✏
manage		Static	192.168.0.1	

Edit Network

Network Name: uplink

Vlan: 103

Protocol: DHCP

interface: All

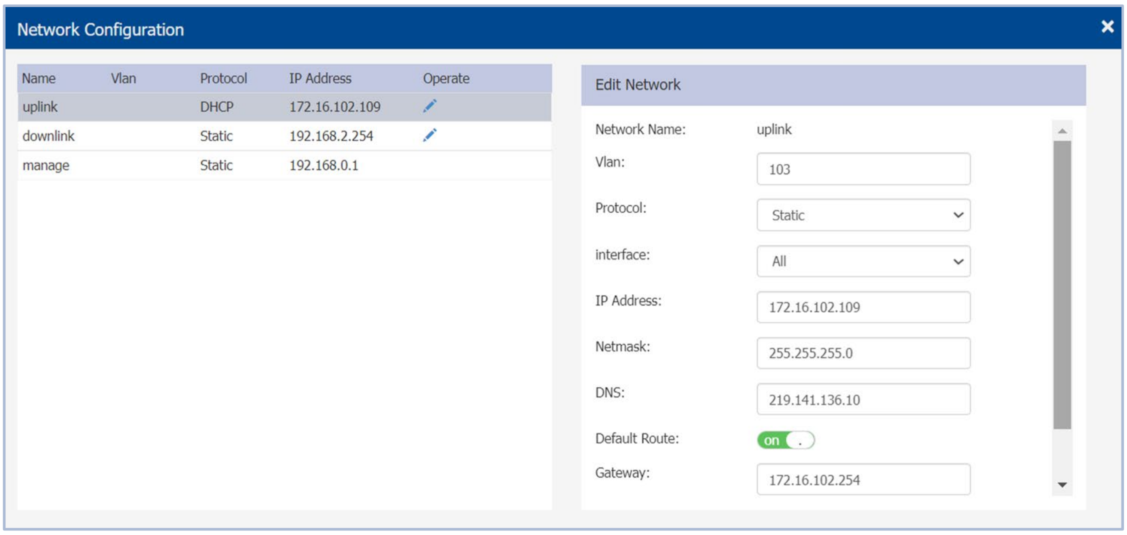
Default Route: on

Figure 49: Network configuration

The key parameters are described as follows:

Parameter	Specification
Network Name	The name of the network.
VLAN	VLAN ID mapping to the network.
Protocol	IP address allocation for the network interface, DHCP in this case.
Interface	Selects interface uplink, All or athsta1+athsta11.
Default Route	Configures whether the interface of the network is the default route of the DAP847-XXC. By default, the uplink interface is the default route of the DAP847-XXC.

▶ Configure a static IP address.



Network Configuration

Name	Vlan	Protocol	IP Address	Operate
uplink		DHCP	172.16.102.109	✎
downlink		Static	192.168.2.254	✎
manage		Static	192.168.0.1	

Edit Network

Network Name: uplink

Vlan: 103

Protocol: Static

interface: All

IP Address: 172.16.102.109

Netmask: 255.255.255.0

DNS: 219.141.136.10

Default Route: on

Gateway: 172.16.102.254

Figure 50: Network configuration - Static IP address configuration

The key parameters are described as follows:

Parameter	Specification
Network Name	The name of the network.
VLAN	VLAN ID mapping to the network
Protocol	IP address allocation for the network interface, Static in this case.
Interface	Selects interface uplink, All or athsta1+athsta11.
IP Address	Interface IP address of the network.
Netmask	Netmask of the network.
DNS	DNS server for the network.
Default Route	Configures whether the interface of the network is the default route of the DAP847-XXC. By default, the uplink interface is the default route of the DAP847-XXC.
Gateway	Gateway of the network.

Note:

When DAP847-XXC is configured with a Tagged VLAN in MESH mode, the corresponding trackside DAP with MESH-enabled WLAN cannot bind any VLAN to it. This is to avoid issues caused by multiple VLAN tags when processing packets received over the wireless interface.

When DAP847-XXC is configured with a Tagged VLAN in MESH mode, the VLAN configured in the regular WLAN of the corresponding trackside DAP must not overlap with the Tagged VLAN configured in the onboard AP. This is to prevent VLAN tag conflicts and ensure correct transmission and processing of network packets.

For example, if DAP847-XXC is configured with Tagged VLAN 104 in MESH mode, the regular WLAN configuration in the corresponding trackside AP must not use VLAN 104.

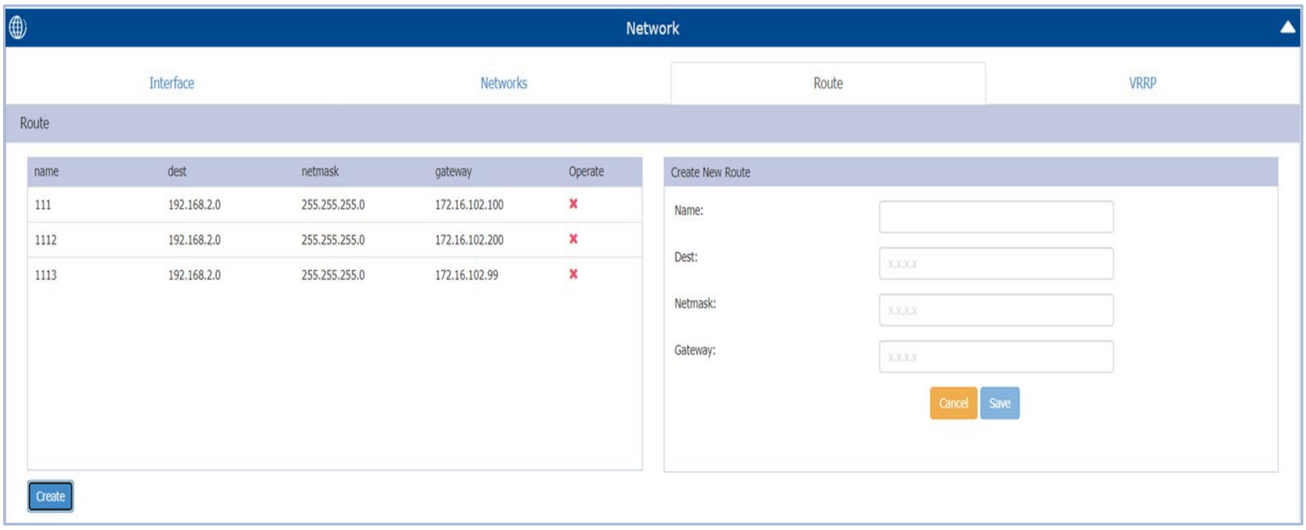
7.3 Route configuration

The routing function of a router enables transmitting packets from one node to another, even when the two nodes are not directly connected. The core of the routing function is the routing table, which consists of a series of routing entries. Each entry contains information such as the destination network address, next-hop address, and output port.

Note: The routing functions described in this chapter are ONLY applicable when DAP847-XXC is in "**Station**" mode.

DAP847-XXC currently supports only configuring static routes, and does not support dynamic routes such as OSPF or RIP.

Route configuration can be applied only when DAP847-XXC works in **Station** mode. You can create a maximum of 128 route items as required.



name	dest	netmask	gateway	Operate
111	192.168.2.0	255.255.255.0	172.16.102.100	✗
1112	192.168.2.0	255.255.255.0	172.16.102.200	✗
1113	192.168.2.0	255.255.255.0	172.16.102.99	✗

Create New Route

Name:

Dest: x.x.x.x

Netmask: x.x.x.x

Gateway: x.x.x.x

Figure 51: Route configuration

The key parameters are described as follows:

Parameter	Specification
Name	Name of the route item.
Dest	Identifies the destination address or network of the IP packet.
Netmask	Netmask is a 32-bit mask matched to the destination network.
Gateway	Indicates the next-hop address for the packet.
Operate	Deletes the specific route item.

7.4 VRRP configuration

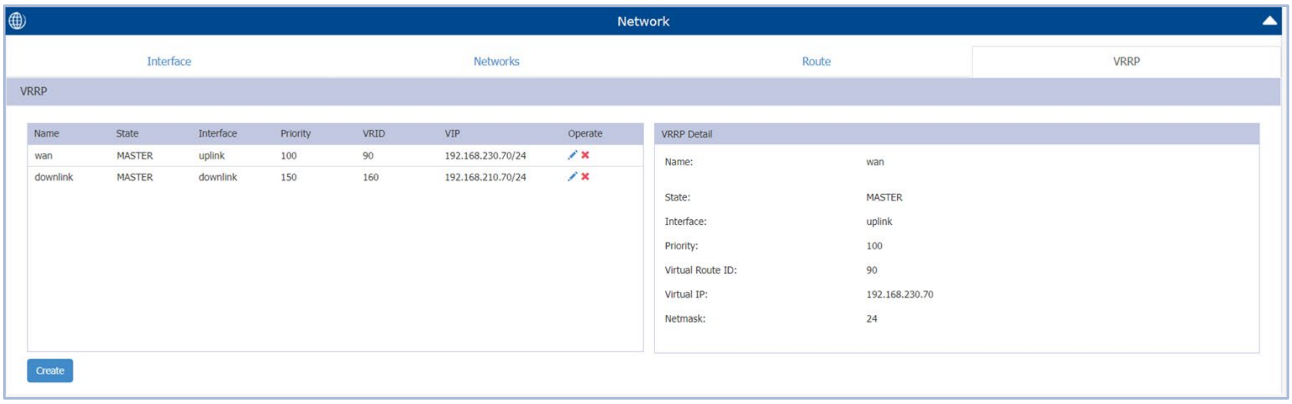
VRRP (Virtual Router Redundancy Protocol) is a network protocol that creates a virtual router within a local area network (LAN) to improve network reliability and availability.

In a traditional network environment, when the primary router fails or does not work properly, the terminal connected to that router cannot access the external network. With the VRRP protocol, however, multiple routers in the LAN can form a virtual router to ensure a backup router takes over in time when the primary router fails. This ensures the continuity and stability of the network connection.

Note: The VRRP function described in this section is only applicable when DAP847-XXC is in "**Station**" mode.

Normally, the virtual router is selected from the 2 DAP847-XXCs in the same cluster using VRRP protocol. The router with the highest priority becomes the MASTER virtual router and is responsible for handling all routing requests from terminals. If the MASTER router fails, another backup router takes over and becomes the new MASTER.

Normally, the network administrator needs to configure the uplink and downlink VRRP profiles for each DAP847-XXC to create uplink and downlink virtual routers.



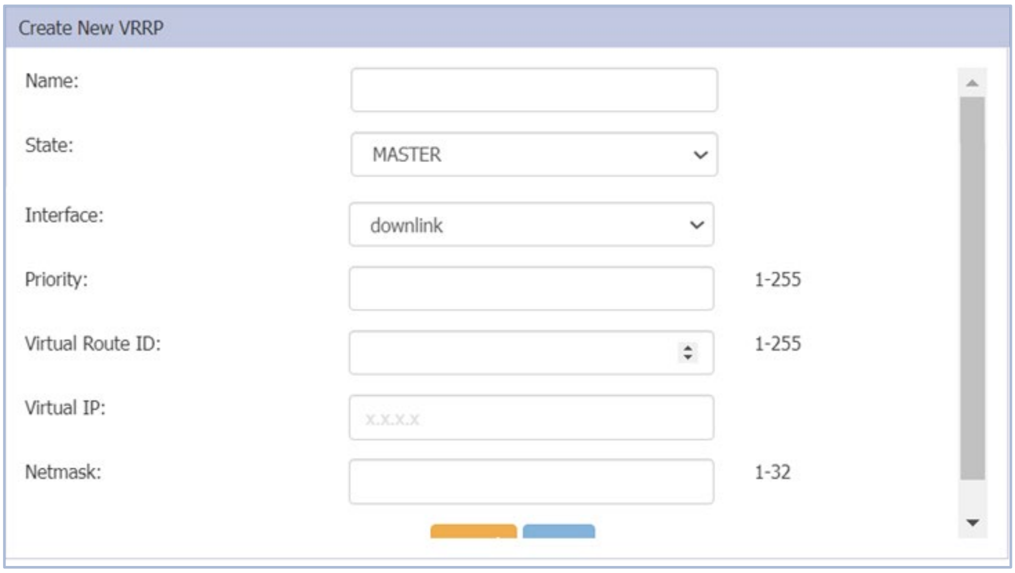
VRRP

Name	State	Interface	Priority	VRID	VIP	Operate
wan	MASTER	uplink	100	90	192.168.230.70/24	✎ ✖
downlink	MASTER	downlink	150	160	192.168.210.70/24	✎ ✖

VRRP Detail

Name:	wan
State:	MASTER
Interface:	uplink
Priority:	100
Virtual Route ID:	90
Virtual IP:	192.168.230.70
Netmask:	24

Figure 52: VRRP configuration



Create New VRRP

Name:		
State:	MASTER	
Interface:	downlink	
Priority:		1-255
Virtual Route ID:		1-255
Virtual IP:	x.x.x.x	
Netmask:		1-32

Figure 53: Create VRRP configuration file

The key parameters are described as follows:

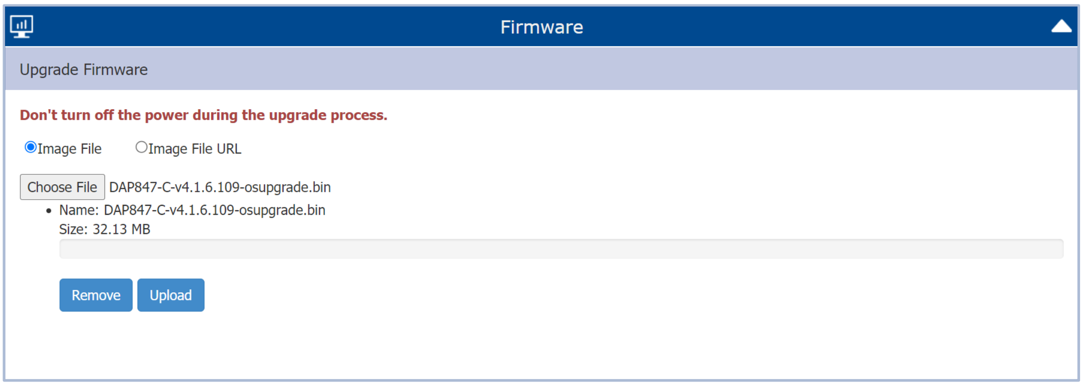
Parameter	Specification
Name	Name of the VRRP Profile
State	Role configured in VRRP for the DAP847-XXC: ▶ MASTER: DAP847-XXC is set as the main router with higher priority. ▶ BACKUP: DAP847-XXC is set as backup router with lower priority than the master router.
Interface	Used to create interface for the virtual router, Uplink interface or Downlink interface.
Priority	Priority of DAP847-XXC in VRRP Greater the value, higher the priority.
Virtual Route ID	ID of the virtual router The virtual router can only be created between DAP847-XXCs that have the same Virtual Route ID.
Virtual IP	Virtual IP address of the virtual router.
Netmask	Subnet mask of the virtual router.

8 Upgrade firmware

Before upgrading the DAP847-XXC, you need to prepare the firmware file for upload. You can download the firmware file from https://catalog.belden.com. Save the firmware file to the local disk of the PC you are using to connect the DAP847-XXC or to a remote TFTP or SFTP server.

There are 3 ways to upload DAP847-XXC firmware:

- Upload local file
  - □ Select “**Image File**” option and upload the firmware from the local image file.
  - □ Click “**Upload**” button to perform the upgrade operation.
  - □ Click “**Remove**” button to cancel the upgrade operation.



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

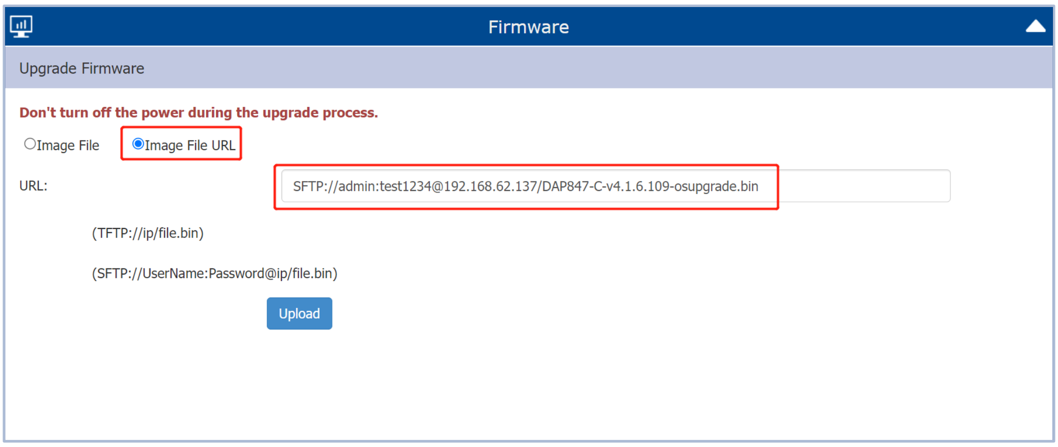
● Image File ○ Image File URL

Choose File DAP847-C-v4.1.6.109-osupgrade.bin

- Name: DAP847-C-v4.1.6.109-osupgrade.bin
  Size: 32.13 MB

Figure 54: Upload firmware from local file

- SFTP Server
  - □ Select “**Image File URL**” option.
  - □ Enter the specified URL with the SFTP Server IP address, credentials, and firmware file name.
  - □ Click “**Upload**” button to perform the upgrade operation.



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

○ Image File ● Image File URL

URL: SFTP://admin:test1234@192.168.62.137/DAP847-C-v4.1.6.109-osupgrade.bin

(TFTP://ip/file.bin)

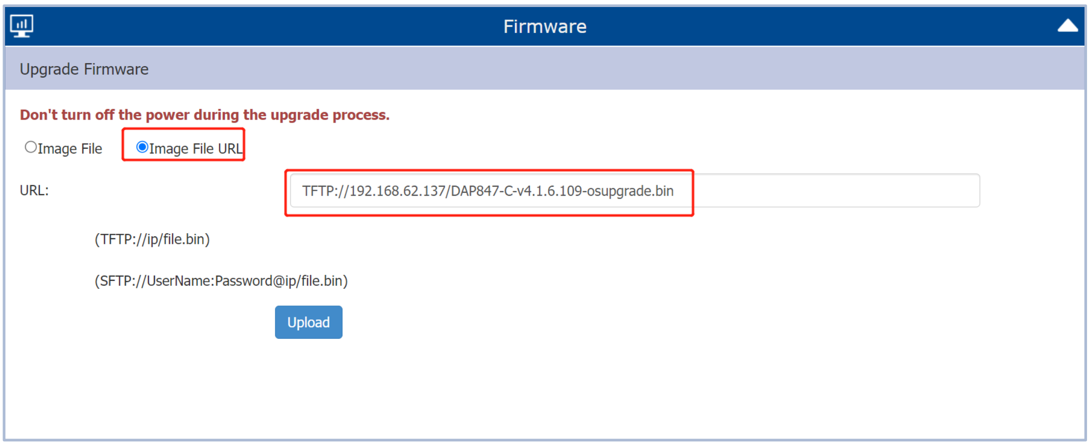
(SFTP://UserName:Password@ip/file.bin)

Figure 55: Upload AP firmware by using SFTP

▶ TFTP Server

☐ Enter the specified URL with the TFTP Server IP address, and firmware file name.

☐ Click "**Upload**" button to perform the upgrade operation.



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

○Image File ●Image File URL

URL: TFTP://192.168.62.137/DAP847-C-v4.1.6.109-osupgrade.bin

(TFTP://ip/file.bin)

(SFTP://UserName:Password@ip/file.bin)

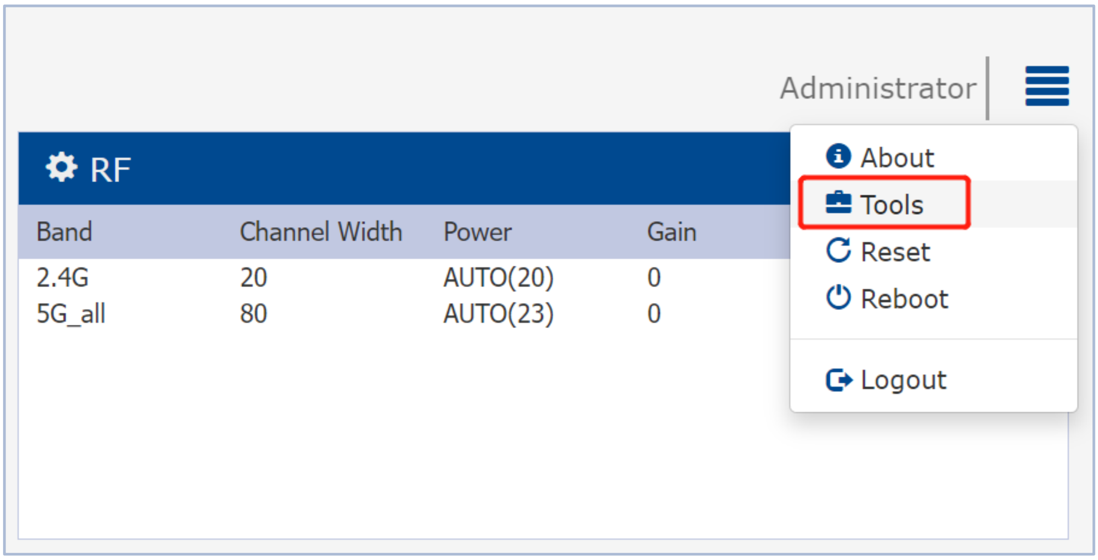
Figure 56: Upload AP firmware by using TFTP

Note: It takes 5 minutes to upgrade the DAP847-XXC firmware.

9 Tools

Tools are DAP847-XXC integrated commands which are used for diagnosing and troubleshooting.

The commands are applied to a single DAP847-XXC in the cluster. You can execute a command to discover the running information on the DAP847-XXC, such as system status, Wi-Fi information, and reboot reason.



Band	Channel Width	Power	Gain
2.4G	20	AUTO(20)	0
5G_all	80	AUTO(23)	0

Figure 57: Entry of Tools

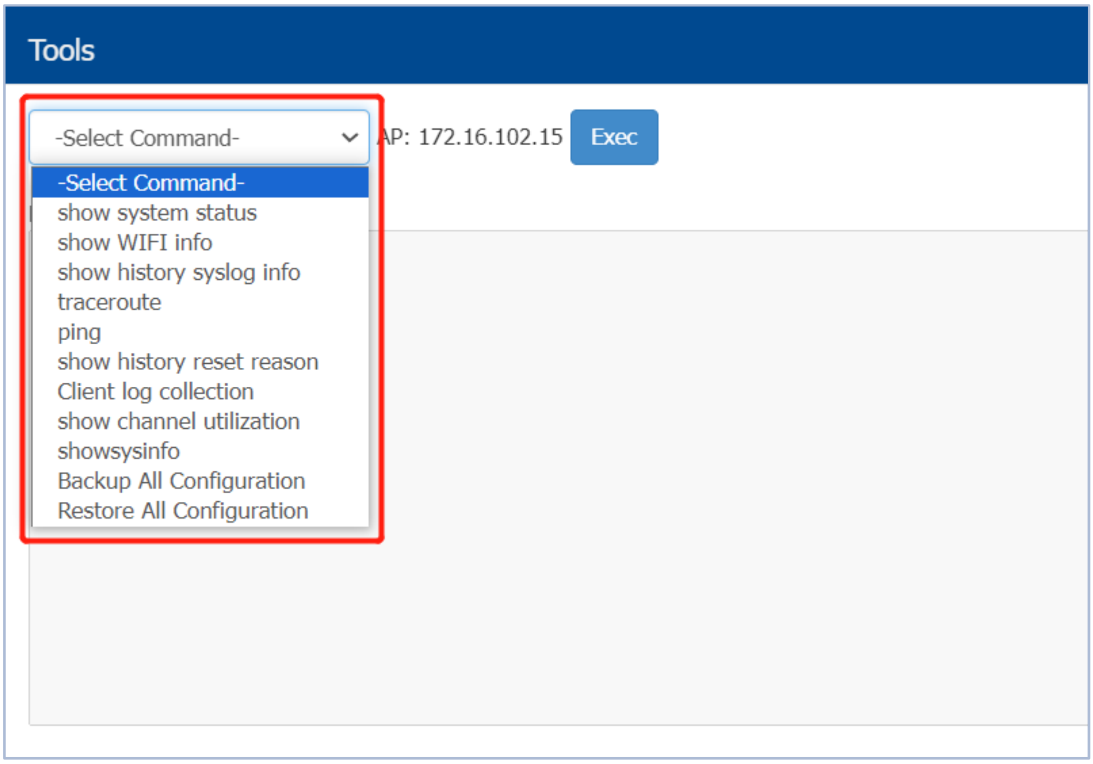
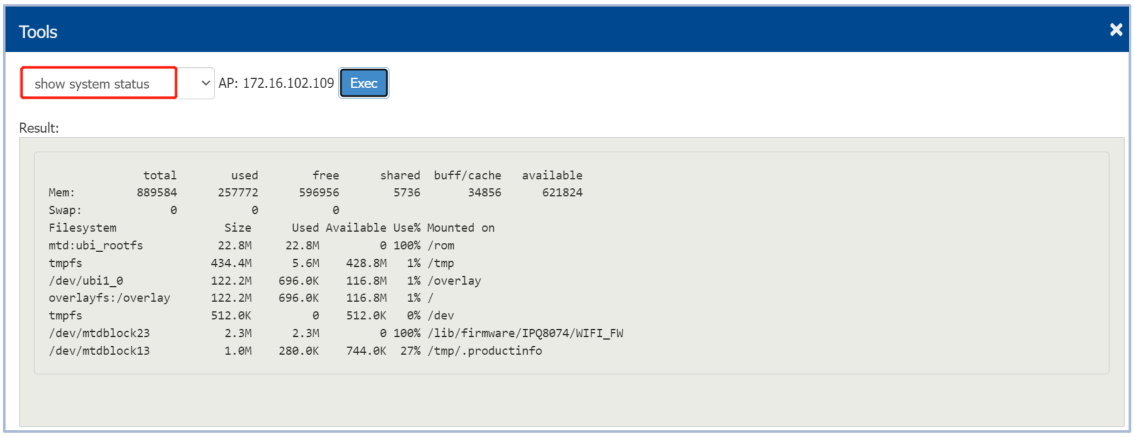


Figure 58: Troubleshooting Tools

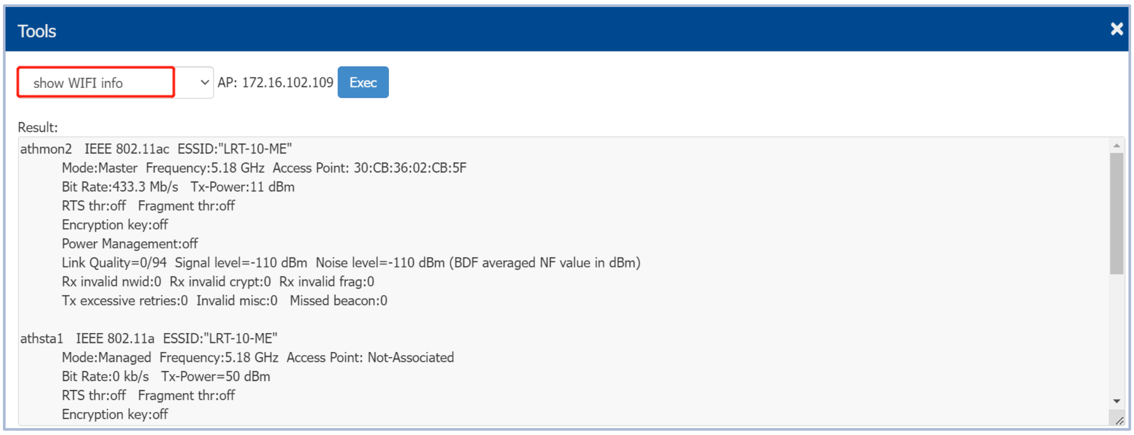
- **show system status**: Displays system memory usage information for the specified DAP847-XXC.



```
              total        used        free      shared  buff/cache   available
Mem:         889584      257772      596956        5736       34856      621824
Swap:             0           0           0
Filesystem                Size      Used Available Use% Mounted on
mtd:ubi_rootfs           22.8M     22.8M         0 100% /rom
tmpfs                   434.4M      5.6M    428.8M   1% /tmp
/dev/ubi1_0             122.2M    696.0K    116.8M   1% /overlay
overlayfs:/overlay      122.2M    696.0K    116.8M   1% /
tmpfs                   512.0K         0    512.0K   0% /dev
/dev/mtdblock23           2.3M      2.3M         0 100% /lib/firmware/IPQ8074/WIFI_FW
/dev/mtdblock13           1.0M    280.0K    744.0K  27% /tmp/.productinfo
```

Figure 59: show system status

- **show WIFI info:** Displays wireless interface information.

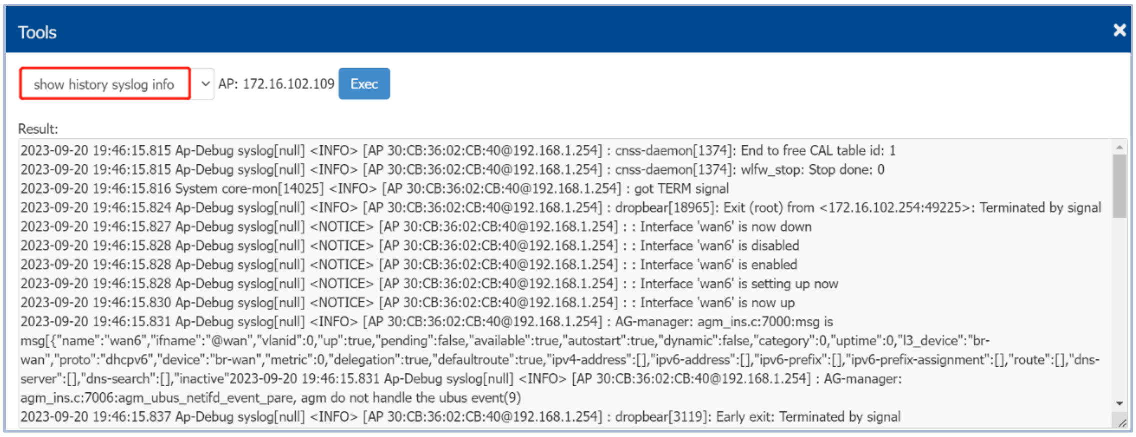


```
athmon2   IEEE 802.11ac  ESSID:"LRT-10-ME"
          Mode:Master  Frequency:5.18 GHz  Access Point: 30:CB:36:02:CB:5F
          Bit Rate:433.3 Mb/s   Tx-Power:11 dBm
          RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/94  Signal level=-110 dBm  Noise level=-110 dBm (BDF averaged NF value in dBm)
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

athsta1   IEEE 802.11a  ESSID:"LRT-10-ME"
          Mode:Managed  Frequency:5.18 GHz  Access Point: Not-Associated
          Bit Rate:0 kb/s   Tx-Power=50 dBm
          RTS thr:off   Fragment thr:off
          Encryption key:off
```

Figure 60: show WIFI info

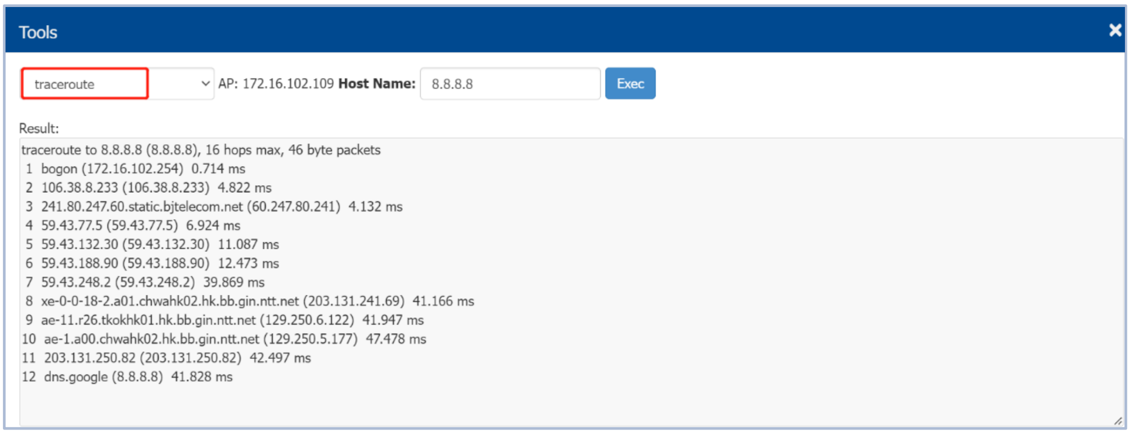
- **show history syslog info:** Displays historic Syslog messages generated in the last time the system ran (Before this time system up) for the specified DAP847-XXC.



```
2023-09-20 19:46:15.815 Ap-Debug syslog[null] <INFO> [AP 30:CB:36:02:CB:40@192.168.1.254] : cnss-daemon[1374]: End to free CAL table id: 1
2023-09-20 19:46:15.815 Ap-Debug syslog[null] <INFO> [AP 30:CB:36:02:CB:40@192.168.1.254] : cnss-daemon[1374]: wlfw_stop: Stop done: 0
2023-09-20 19:46:15.816 System core-mon[14025] <INFO> [AP 30:CB:36:02:CB:40@192.168.1.254] : got TERM signal
2023-09-20 19:46:15.824 Ap-Debug syslog[null] <INFO> [AP 30:CB:36:02:CB:40@192.168.1.254] : dropbear[18965]: Exit (root) from <172.16.102.254:49225>: Terminated by signal
2023-09-20 19:46:15.827 Ap-Debug syslog[null] <NOTICE> [AP 30:CB:36:02:CB:40@192.168.1.254] : : Interface 'wan6' is now down
2023-09-20 19:46:15.828 Ap-Debug syslog[null] <NOTICE> [AP 30:CB:36:02:CB:40@192.168.1.254] : : Interface 'wan6' is disabled
2023-09-20 19:46:15.828 Ap-Debug syslog[null] <NOTICE> [AP 30:CB:36:02:CB:40@192.168.1.254] : : Interface 'wan6' is enabled
2023-09-20 19:46:15.828 Ap-Debug syslog[null] <NOTICE> [AP 30:CB:36:02:CB:40@192.168.1.254] : : Interface 'wan6' is setting up now
2023-09-20 19:46:15.830 Ap-Debug syslog[null] <NOTICE> [AP 30:CB:36:02:CB:40@192.168.1.254] : : Interface 'wan6' is now up
2023-09-20 19:46:15.831 Ap-Debug syslog[null] <INFO> [AP 30:CB:36:02:CB:40@192.168.1.254] : AG-manager: agm_ins.c:7000:msg is
msg[{"name":"wan6","ifname":"@wan","vlanid":0,"up":true,"pending":false,"available":true,"autostart":true,"dynamic":false,"category":0,"uptime":0,"l3_device":"br-
wan","proto":"dhcpv6","device":"br-wan","metric":0,"delegation":true,"defaultroute":true,"ipv4-address":[],"ipv6-address":[],"ipv6-prefix":[],"ipv6-prefix-assignment":[],"route":[],"dns-
server":[],"dns-search":[],"inactive"2023-09-20 19:46:15.831 Ap-Debug syslog[null] <INFO> [AP 30:CB:36:02:CB:40@192.168.1.254] : AG-manager:
agm_ins.c:7006:agm_ubus_netifd_event_pare, agm do not handle the ubus event(9)
2023-09-20 19:46:15.837 Ap-Debug syslog[null] <INFO> [AP 30:CB:36:02:CB:40@192.168.1.254] : dropbear[3119]: Early exit: Terminated by signal
```

Figure 61: show history syslog info

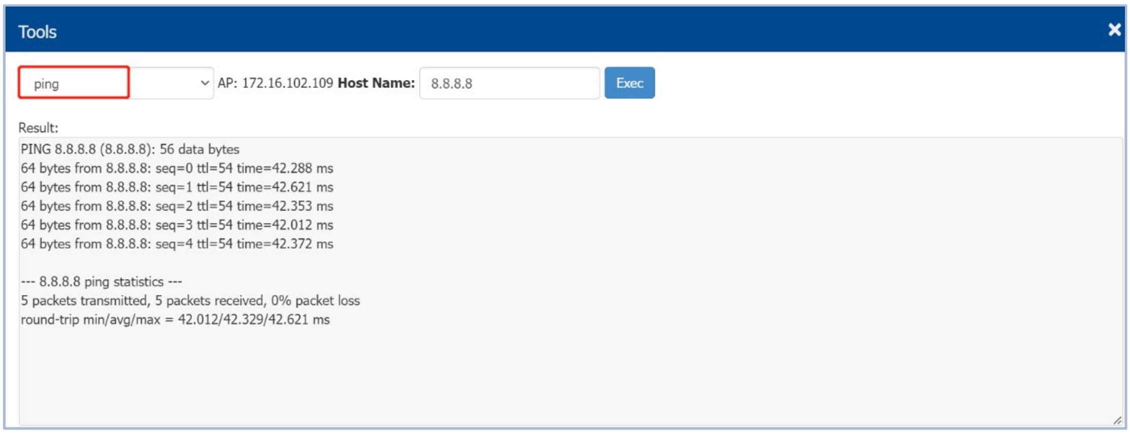
- **traceroute:** A built-in traceroute tool in DAP847-XXC which is used to check the routing information in the network.



```
traceroute to 8.8.8.8 (8.8.8.8), 16 hops max, 46 byte packets
 1  bogon (172.16.102.254)  0.714 ms
 2  106.38.8.233 (106.38.8.233)  4.822 ms
 3  241.80.247.60.static.bjtelecom.net (60.247.80.241)  4.132 ms
 4  59.43.77.5 (59.43.77.5)  6.924 ms
 5  59.43.132.30 (59.43.132.30)  11.087 ms
 6  59.43.188.90 (59.43.188.90)  12.473 ms
 7  59.43.248.2 (59.43.248.2)  39.869 ms
 8  xe-0-0-18-2.a01.chwahk02.hk.bb.gin.ntt.net (203.131.241.69)  41.166 ms
 9  ae-11.r26.tkokhk01.hk.bb.gin.ntt.net (129.250.6.122)  41.947 ms
10  ae-1.a00.chwahk02.hk.bb.gin.ntt.net (129.250.5.177)  47.478 ms
11  203.131.250.82 (203.131.250.82)  42.497 ms
12  dns.google (8.8.8.8)  41.828 ms
```

Figure 62: traceroute

- **ping:** Ping operation from DAP847-XXC to another host in the network.

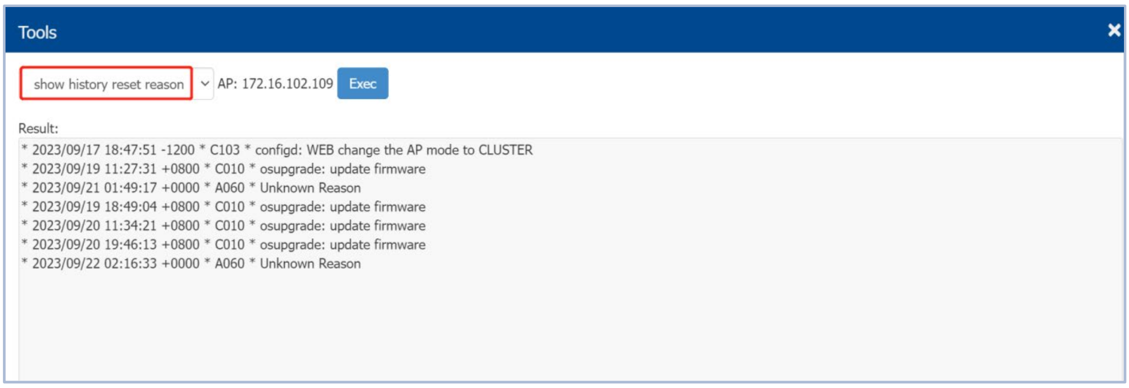


```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=54 time=42.288 ms
64 bytes from 8.8.8.8: seq=1 ttl=54 time=42.621 ms
64 bytes from 8.8.8.8: seq=2 ttl=54 time=42.353 ms
64 bytes from 8.8.8.8: seq=3 ttl=54 time=42.012 ms
64 bytes from 8.8.8.8: seq=4 ttl=54 time=42.372 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 42.012/42.329/42.621 ms
```

Figure 63: ping testing on DAP847-XXC

- **show history reset reason:** Shows latest 10 reboot records of DAP847-XXC which includes reboot time, reboot reason. It is the same output for command `reset_record get` under CLI mode.



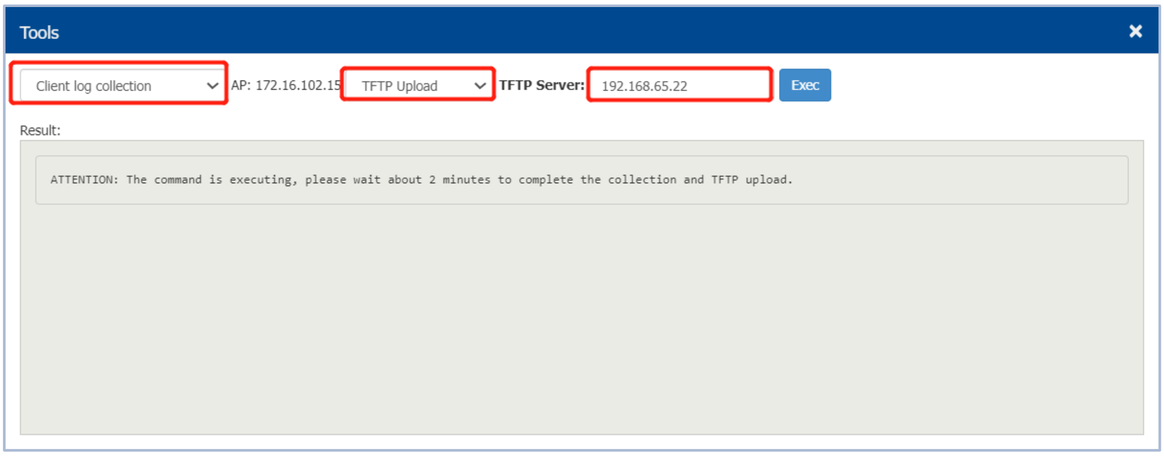
show history reset reason AP: 172.16.102.109

Result:

```
* 2023/09/17 18:47:51 -1200 * C103 * configd: WEB change the AP mode to CLUSTER
* 2023/09/19 11:27:31 +0800 * C010 * osupgrade: update firmware
* 2023/09/21 01:49:17 +0000 * A060 * Unknown Reason
* 2023/09/19 18:49:04 +0800 * C010 * osupgrade: update firmware
* 2023/09/20 11:34:21 +0800 * C010 * osupgrade: update firmware
* 2023/09/20 19:46:13 +0800 * C010 * osupgrade: update firmware
* 2023/09/22 02:16:33 +0000 * A060 * Unknown Reason
```

Figure 64: show history reset reason

- **Client log collection:** Collection of DAP847-XXC log files for troubleshooting and download by TFTP/HTTP.

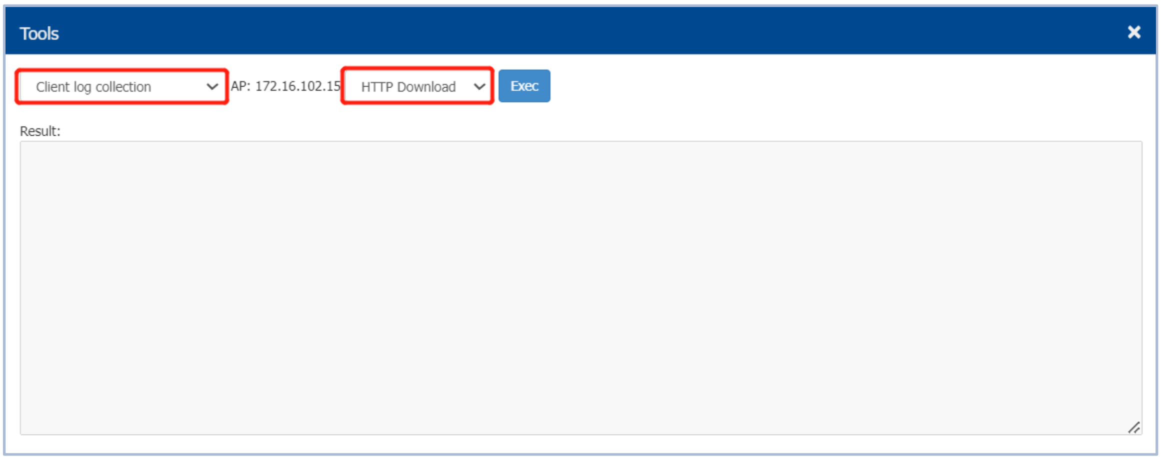


Client log collection AP: 172.16.102.15 TFTP Upload **TFTP Server:** 192.168.65.22

Result:

```
ATTENTION: The command is executing, please wait about 2 minutes to complete the collection and TFTP upload.
```

Figure 65: Client log collection by TFTP

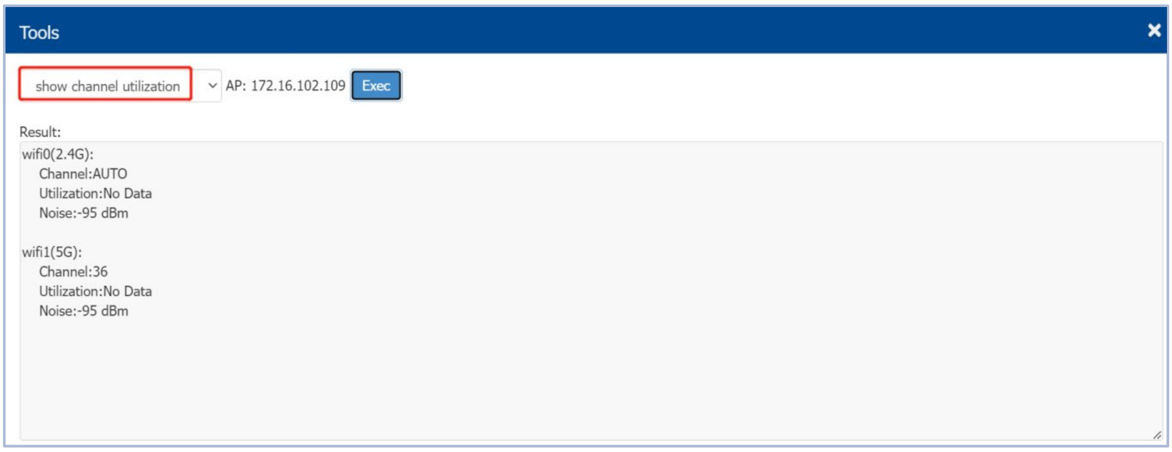


Client log collection AP: 172.16.102.15 HTTP Download

Result:

Figure 66: Client log collection by HTTP

- **show channel utilization:** Displays current 2.4G/5G band channel utilization.

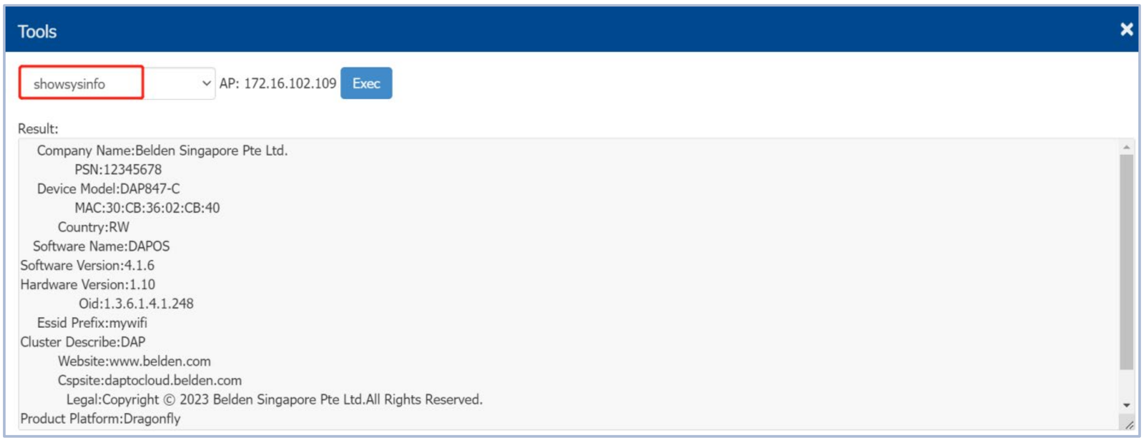


```
Result:
wifi0(2.4G):
   Channel:AUTO
   Utilization:No Data
   Noise:-95 dBm

wifi1(5G):
   Channel:36
   Utilization:No Data
   Noise:-95 dBm
```

Figure 67 show channel utilization

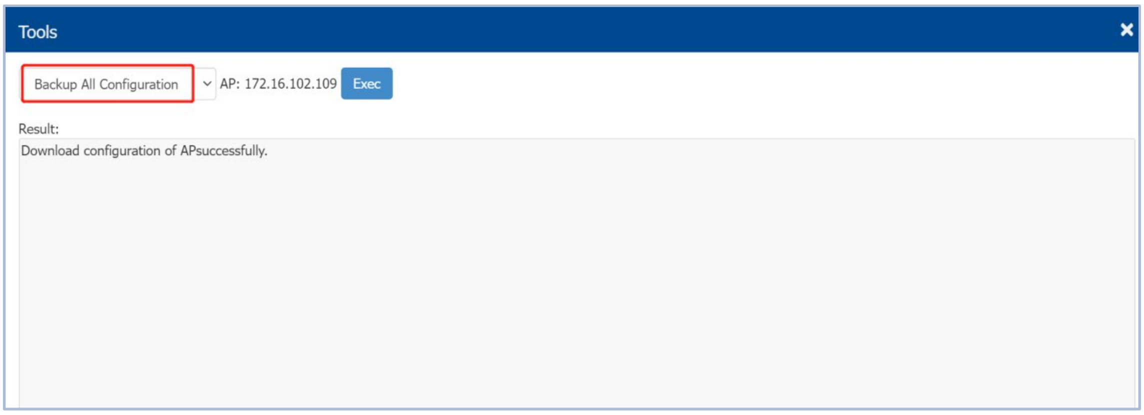
- **showsysinfo:** Displays basic information of DAP847-XXC, such as device model, MAC address, PSN and software version, etc.



```
Result:
   Company Name:Belden Singapore Pte Ltd.
          PSN:12345678
   Device Model:DAP847-C
          MAC:30:CB:36:02:CB:40
       Country:RW
  Software Name:DAPOS
Software Version:4.1.6
Hardware Version:1.10
          Oid:1.3.6.1.4.1.248
   Essid Prefix:mywifi
Cluster Describe:DAP
       Website:www.belden.com
       Cspsite:daptocloud.belden.com
         Legal:Copyright © 2023 Belden Singapore Pte Ltd.All Rights Reserved.
Product Platform:Dragonfly
```

Figure 68: show channel utilization

- **Backup All Configuration:** Backups and downloads the current configuration file of DAP847-XXC. The name of the configuration file is `pub-config.tar`.

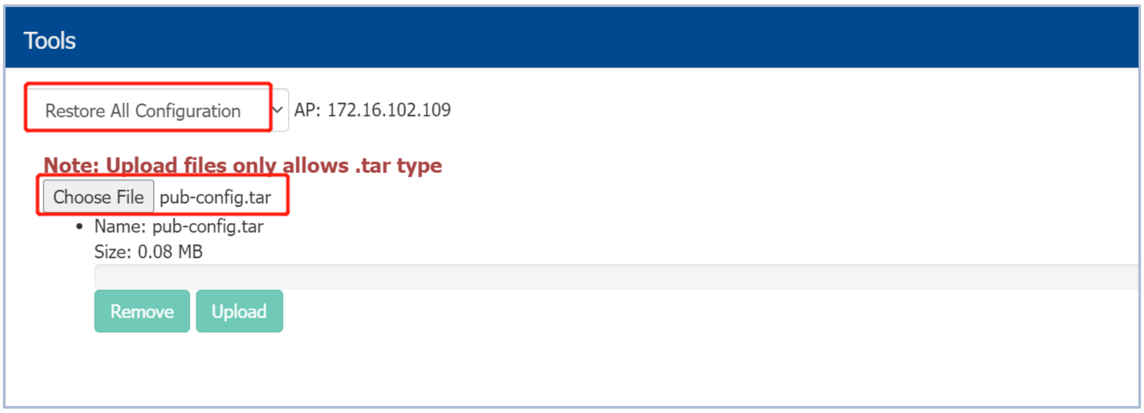


Result:

Download configuration of APsuccessfully.

Figure 69: Backup All Configuration

- **Restore All Configuration:** Restores the configuration file.



Note: Upload files only allows .tar type

pub-config.tar

- Name: pub-config.tar
  Size: 0.08 MB

Figure 70: Restore All Configuration

10 Glossary

A	
APC	Automatic Power Control
ARP	Address Resolution Protocol
C	
CA	Certificate Authority
CLI	Command-Line Interface
CPU	Central Processing Unit
CTS	Clear To Send
D	
DAC	Dragonfly Access Controller: DAC is a simple, easy to deploy turnkey WLAN solution consisting of one or more DAPs
DAP	Dragonfly Access Point: Enhanced WLAN technology with RF radio dynamic adjustment, distributed control Wi-Fi architecture, secure network admission control with unified access
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
E	
EAP	Extensible Authentication Protocol
F	
FDB	Forward Data-Base
G	
GCM	Galois/Counter Mode
GUI	Graphical User Interface
H	
HTTP	Hypertext Transfer Protocol

HTTPS	Hypertext Transfer Protocol Secure
I	
IP	Internet Protocol
M	
MAC	Media Access Control
MIMO	Multiple-Input Multiple-Output
N	
NTP	Network Time Protocol
P	
PC	Personal Computer
PEAP	Protected EAP
PoE	Power over Ethernet
PVM	Primary Virtual Manager: the virtual manager selected from DAP847-XXCs according to the defined priority will be responsible for DAP847-XXC management and monitoring
R	
RARP	Reverse Address Resolution Protocol
RF	Radio Frequency
RSSI	Received Signal Strength Indicator
RTS	Request To Send
S	
SAE	Simultaneous Authentication of Equals
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SSID	Service Set Identifier

SVM	Secondary Virtual Manager: the second highest priority in the cluster. When the PVM fails to respond due to an unexpected error or issues, the SVM will automatically upgrade to act as the PVM
T	
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
U	
URL	Uniform Resource Locator
V	
VLAN	Virtual Local Area Network
W	
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3

A Further support

Technical questions

For technical questions, please contact any Hirschmann IT dealer in your area 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.

HIRSCHMANN IT

A BELDEN BRAND