

HIRSCHMANN IT

A **BELDEN** BRAND

用户配置手册

Dragonfly Access Point

DAP847-XXA

即使没有明确说明，本手册中的受版权保护的商标名也不应被认为这些名称从商标和商品名称保护法的意义上说是免费的、因此可供任何人自由使用的。

© 2023-2024 Belden Singapore Pte Ltd

手册和软件均受版权保护。保留所有权利。严禁将全部或部分内容复制、复印、翻译、转换成任何电子媒体或机器可扫描的形式，但您因为自用而制作软件备份的情况除外。

本文描述的性能特征只有协议双方在签署合同时明确同意才具约束力。本文由**Belden**就能力所及而制作。**Belden**保留更改本文内容的权利，恕不另行通知。**Belden**不保证本文中信息的正确性或准确性。

对于因使用网络组件或相关操作软件而导致的损害，**Belden**不承担任何责任。此外，本文参考了许可合同中规定的使用条件。

您可登录Hirschmann IT产品网站获取本手册的最新版本：

<https://catalog.belden.com>

版本记录

版本	日期	描述
1.0	2023.12	第一版，基于Web GUI版本4.1.6.21。
1.2	2024.08	基于Web GUI版本4.1.6.43。 增加以下参数至章节6.3 WLAN的相关参数介绍： DTIM Interval, RTS/CTS, RTS Threshold。 更新章节9.1.3 配置DAP847-XXA天线。

目录

版本记录	3
目录	4
安全指南	8
关于本手册	9
关于 DAP	10
符号含义	11
1 简介	12
1.1 概述	12
2 DAP847-XXA工作模式介绍	13
2.1 Cluster集群模式	13
2.1.1 Cluster中PVM和SVM选择	13
2.1.2 DAP847-XXA开箱设置	14
2.2 DAC模式	15
3 DAP集群部署示例	16
3.1 拓扑结构	16
3.2 场景描述	17
3.2.1 集群中DAP的SSIDs	17
3.2.2 部署服务器	19
4 设置向导	20
4.1 通过Web浏览器访问DAP847-XXA Cluster Manager	20
4.1.1 预置条件	20
4.1.2 DAP847-XXA IP地址	21
4.1.3 在初始状态下访问DAP847-XXA的Web GUI	22
4.2 使用DAP847-XXA设置向导	25
4.2.1 DAP的初始化配置	26
5 DAP847-XXA Cluster Manager用户界面	30
5.1 Dashboard页面简介	31
5.2 WLAN页面	32
5.3 AP页面	34

5.4	Clients页面.....	37
5.5	Monitoring页面.....	41
5.5.1	基于集群的监控.....	42
5.5.2	基于WLAN的监控.....	43
5.5.3	基于AP的监控.....	44
5.5.4	基于客户端的监控.....	45
5.6	System页面.....	46
5.7	Wireless页面.....	47
5.8	Access页面.....	48
5.9	DAP847-XXA的其它信息.....	49
6	WLAN配置.....	51
6.1	创建WLAN的两种方式.....	52
6.2	WLAN的安全类型.....	54
6.2.1	安全类型Open.....	54
6.2.2	安全类型Portal.....	54
6.2.3	安全类型Personal.....	55
6.2.4	安全类型Enterprise.....	57
6.3	WLAN的相关参数介绍.....	59
6.4	修改WLAN的配置.....	75
6.5	删除WLAN.....	76
6.6	WMM配置.....	77
7	管理DAP847-XXA.....	78
7.1	查看DAP847-XXA详细信息.....	79
7.2	修改DAP847-XXA的名称和位置信息.....	80
7.3	添加DAP847-XXA到集群.....	81
7.4	删除集群中DAP847-XXA.....	83
7.5	允许DAP847-XXA加入集群.....	85
7.6	替换DAP847-XXA.....	86
7.7	修改DAP847-XXA的IP地址.....	87
7.8	切换DAP847-XXA为DAC模式.....	88
7.9	查看DAP847-XXA的当前配置.....	90
7.10	重启DAP847-XXA.....	91
7.11	恢复出厂配置.....	92

7.12	DAP847-XXA的配置备份和恢复	93
7.13	DAP847-XXA固件升级	94
7.13.1	升级集群中所有DAP847-XXA	94
7.13.2	升级集群中单台DAP847-XXA	97
7.14	DAP847-XXA的LED指示灯配置	99
7.15	DAP847-XXA高级配置	100
7.15.1	DAP847-XXA高级配置页面简介	100
7.15.2	AP状态监控和工作模式配置	101
7.15.3	WLAN信息	105
7.15.4	Clients信息	105
7.15.5	RF信息	105
7.15.6	系统管理	106
7.15.7	DAP847-XXA接口配置	106
7.15.8	DAP847-XXA网络配置	108
7.15.9	Mesh配置	109
7.15.10	Neighbor AP配置	112
7.15.11	RF environment监控	113
7.15.12	无线抓包功能	114
7.16	配置DAP847-XXA的网络服务	116
7.16.1	配置DHCP服务	116
7.16.2	配置DNS服务	118
7.16.3	NAT配置	119
8	系统管理	122
8.1	管理集群信息	123
8.2	账户管理	125
8.2.1	管理Web GUI账户	125
8.2.2	管理CLI账户	126
8.3	证书管理	127
8.4	系统服务配置	128
8.5	配置系统时间	129
8.6	配置Syslog系统日志	131
8.7	配置SNMP	134
8.7.1	配置SNMPv2c	135

8.7.2	配置SNMPv3.....	136
9	无线管理.....	138
9.1	RF配置.....	139
9.1.1	修改DAP847-XXA的功率和信道.....	141
9.1.2	配置信道带宽.....	144
9.1.3	配置DAP847-XXA天线.....	145
9.1.4	开启/关闭DAP847-XXA的无线射频.....	146
9.2	wIDS/wIPS.....	147
9.3	无线性能优化.....	153
10	Access页面.....	156
10.1	认证.....	157
10.2	Portal认证.....	160
10.3	账号和Access Code管理.....	163
10.4	定制化Portal页面.....	166
10.5	无线客户端黑名单.....	167
10.6	Portal认证白名单.....	168
10.7	Portal开放区域.....	169
10.8	组播控制.....	170
10.9	ACL.....	171
11	IoT.....	173
12	DAP847-XXA内部集成工具.....	174
12.1	Tools.....	174
12.2	PMD.....	180
13	部署大规模DAP847-XXA网络系统.....	181
14	无DHCP服务器场景.....	182
15	术语表.....	183
A	更多支持.....	185

安全指南

■ 安全通道

Hirschmann IT设备支持多种管理方式，包括SSH，HTTP，和HTTPS。不推荐任何未加密的管理协议。Hirschmann IT建议使用SSH和HTTPS操作设备，以确保对管理流量进行加密。

■ 安全储存

妥善保存并定期更新登录凭证、设备配置和状态数据。这些信息仅供授权人员访问和管理。

关于本手册

该用户手册包含了您初次操作设备所需要的参考信息，本用户手册将会从初始化状态开始引导您一步一步的完成各项功能的配置操作。

关于 DAP

作为新一代企业级无线接入点，DAP847-XXA系列是专门为工业级无线覆盖场景设计的Wi-Fi 6设备。DAP847-XXA系列支持增强型WLAN技术，包括RF无线电动态调整（RDA）、分布式控制Wi-Fi架构以及通过统一接入进行网络准入控制；配置及维护操作简单，可以提供安全和可扩展无线解决方案的工业应用场景，这使其成为各种规模的工业场景的理想选择。

DAP847-XXA可为高密环境（例如办公室、医院、学校、零售店和仓库）提供企业级Wi-Fi解决方案，以实现高速、性能卓越的网络服务和应用。

同时DAP847-XXA也支持下行与DAP847-XXC系列无线接入客户端建立无线连接，为轨道交通部署场景提供车地数据通信的通道，实现铁路控制信号及相关数据的实时传输。

符号含义

本手册中使用的符号具有以下含义：

▶	分项列表
□	工作步骤
■	副标题
注意	强调一项重要事实或引起相关性重视的一则提示。

1 简介

1.1 概述

本文档主要描述了DAP847-XXA在“CLUSTER”模式下所支持的功能、配置方法、和配置步骤等，并且提供了DAP847-XXA的配置说明和配置示例，适用对二、三层网络数据转发和基本的IEEE 802.11协议有一定了解的网络管理员和无线网络维护人员。

本手册包括DAP847-XXA和配置示例的描述，其中的示例描述了基于典型部署场景配置Wi-Fi网络的常规方法。对于初次配置DAP847-XXA的用户或者对DAP847-XXA产品和软件有一定了解但希望有更深入了解的用户有一定的帮助。

2 DAP847-XXA工作模式介绍

2.1 Cluster集群模式

DAP847-XXA可以通过分布式自组网模式实现自主管理功能，在缺省情况下，DAP847-XXA运行在“集群模式”，该模式基于无控制器架构，提供了即插即用的极简化部署方案，是一个由DAP847-XXA和虚拟管理器组成的自治系统。DAP847-XXA设备间能够完成自动发现，自动组网，和自我管理。

2.1.1 Cluster中PVM和SVM选择

配置了相同集群ID的DAP847-XXA之间能够组成一个集群，同时DAP847-XXA与DAP6XX系列也能够组成一个集群。通过DAP的型号和MAC地址区分优先级选择 Primary Virtual Management（PVM）和 Secondary Virtual Management（SVM）。

PVM或SVM的选举规则如下：

- ▶ 根据DAP的型号在集群中会选择一个优先级最高的设备作为PVM。一般是DAP640/DAP645/DAP646/DAP647/DAP847-XXA 的优先级大于DAP620。
- ▶ 在具有相同优先级的DAP中，具有最高MAC地址的DAP将被选为PVM，具有第二高MAC地址的DAP将被选为SVM。
- ▶ 如果具有更高优先级的DAP加入DAP集群，它将接管PVM角色。例如，DAP847加入DAP620集群后将成为PVM，之前的PVM将变为SVM或DAP集群中的成员。每个集群都可以配置一个管理IP地址，该IP地址是分配给PVM设备的一个虚拟的IP地址。
- ▶ 当PVM因出现意外错误或检测到出现异常问题（例如，网络中断或PVM因意外情况断电）而无法运行时，SVM设备会自动升级为PVM。这能够保证在集群的管理层面能够实现冗余，不会导致DAP847-XXA的业务出现中断或影响无线用户的服务。

一个DAP847-XXA集群支持多达255个DAP847-XXA设备，集群的架构能够确保DAP847-XXA简单快速的完成部署。一旦您使用配置向导配置了第一个DAP847-XXA设备，在同一个二层网络中使用相同“**集群ID**”的其它DAP847-XXA设备将自动加入集群并从PVM获取配置信息，这能够确保整个无线网络在几分钟内完成快速部署。默认情况下，DAP847-XXA使用的“**集群ID**”为100。

2.1.2 DAP847-XXA开箱设置

要设置DAP847-XXA开箱即用：

- 将DAP847-XXA连接到网络中的交换机.
- 通过以太网供电（PoE）或电源适配器为其供电.
- 确保DAP847-XXA可以从网络中的DHCP服务器获取到IP地址。

当 DAP847-XXA 上的 LED 处于“绿色闪烁”状态时，将可以扫描并且能够连接到一个在2.4 GHz信道上名为“mywifi-xx:xx”的 SSID（xx:xx 是 DAP847-XXA MAC 地址的最后 2 个字节）。

当配置终端关联到这个SSID 后，便可以通过以下默认 URL 来访问DAP847-XXA的Web管理页面：

- ▶ <http://find.dap.com:8080>
- ▶ <https://find.dap.com>

使用默认帐户登录后（用户名为“Administrator”，密码为“admin”），您可以通过“配置向导”来配置DAP847-XXA了。

2.2 DAC模式

当DAP847-XXA工作在DAC模式时，所有的DAP847-XXA设备可以由管理平台进行集中管理，以便于轻松部署大型网络。部署DAC模式，支持DAP847-XXA与DAC的三层组网，只需要保证DAP847-XXA与DAC之间网络可达即可。您可以在单个区域安装部署，也可以在多个地理分散的位置部署DAP847-XXA。

有关详细信息，请参考[DAC用户手册](#)。

3 DAP集群部署示例

本章节主要介绍了集群模式下的典型无线网络拓扑结构，包括了无线网络和有线网络在内。该场景中包括了DAP847-XXA、交换机、路由器和相关的应用服务器等网络设备。

3.1 拓扑结构

图 1是一个典型集群部署场景的简要拓扑结构，用来为该手册中介绍的功能提供参考。在此场景中没有部署DAC管理平台。所有的DAP847-XXA以“集群”的模式工作，以实现自主管理功能。

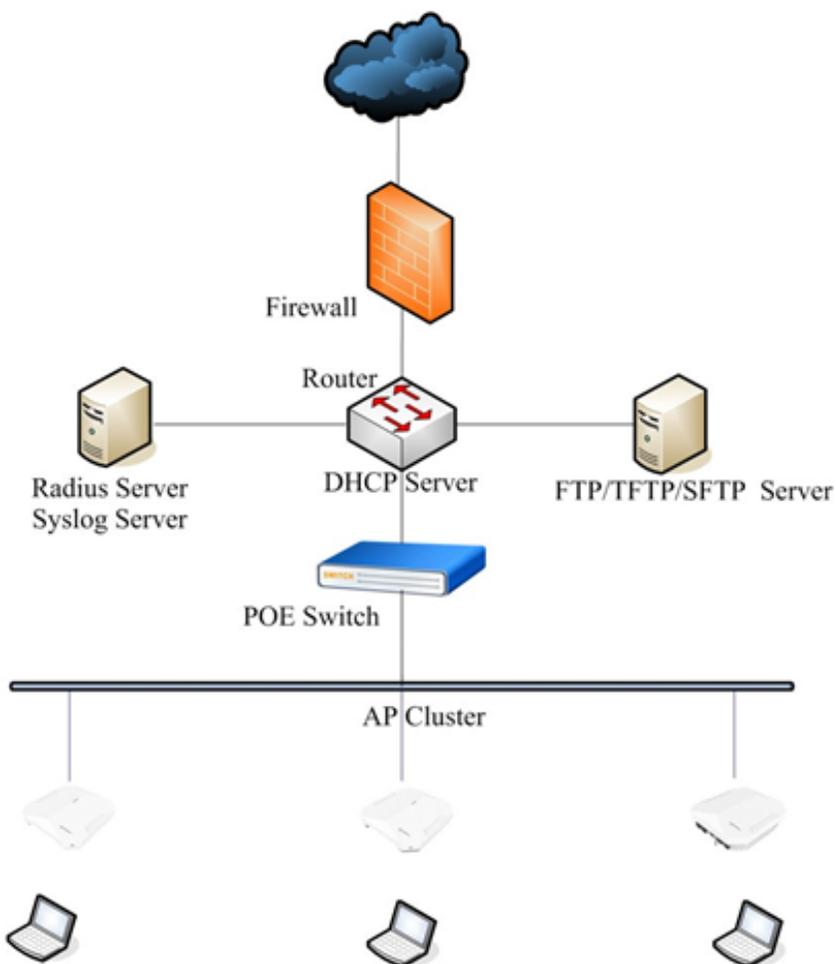


图 1: 网络拓扑图

3.2 场景描述

图 1 网络拓扑工作模式如下：

- ▶ 集群有3个DAP847-XXA，都连接到一台支持IEEE 802.3at标准的PoE交换机，所有DAP847-XXA都属于同一个VLAN。
- ▶ PoE交换机上行连接到核心路由器，该路由器为DAP847-XXA和无线客户端设备以及配置终端提供Dynamic Host Configuration Protocol (DHCP) 服务。
- ▶ 集群中的PVM负责DAP847-XXA的管理和监控、配置的不同步以及客户端信息的同步；同时，对于Portal使用场景，PVM也是一个内置的portal服务器。

在5150 ... 5250 MHz频段使用时，只允许在室内操作，包括安装在公路车辆、火车和飞机内。室外操作的场景有限。如果在室外使用，DAP847-XXA不能连接到固定装置、公路车辆的车身外部、固定基础设施或固定室外天线上。仅限在5170 ... 5250 MHz频段内使用无人机系统（UAS）。

在5250 ... 5350 MHz频段内使用时，只允许在室内操作，如建筑物内。不允许在公路车辆、火车和飞机上安装。不允许在室外使用。

3.2.1 集群中DAP的SSIDs

集群中的3台DAP配置如下3个SSID：

■ My-wifi-test

这是一个预共享密钥的模式SSID，主要用于需要简单和快速安全连接的场景，例如家庭网络、小型办公室网络等，可以在不需要复杂的设置和管理的情况下提供基本的安全保护。

■ My-wifi-portal

这是配置了portal认证的SSID，为访客场景设计的，通常用于酒店、机场、购物中心等公共场所，为访客提供临时的互联网接入。访客通过连接到portal SSID，访问一个专门的门户页面，然后输入访问代码或凭据，以获取互联网接入权限。portal WLAN还可以用于企业内部，为临时来访的客户、合作伙伴或供应商提供安全的互联网接入。

■ My-wifi-1x

此WLAN使用IEEE 802.1x认证方式。公司员工和安全人员可以使用SSID“**My-wifi-1x**”。用户名和密码存储在内部RAIUS服务器中。用户需要输入用户名和密码或使用证书才能连接到WLAN。该认证方式较前两种SSID具有更高的安全性。

3.2.2 部署服务器

在图 1场景中，部署的相关服务器有：

- ▶ **RADIUS Server:** 用于IEEE 802.1x认证，可以是一个 Windows Server 或者是一台其它类型的RADIUS server。
- ▶ **Syslog Server:** 作为远程系统日志服务器，用于接收查看DAP847-XXA生成的系统日志，请参考第131页“配置Syslog系统日志”。
- ▶ **TFTP Server:** 主要用于DAP847-XXA的snapshot log收集、软件升级以及Post Mortem Dump (PMD)文件的收集等。
- ▶ **SFTP Server:** 主要用于DAP847-XXA的软件升级和客户端连接信息的记录（客户端行为追踪）。

4 设置向导

用户通过连接预定义的SSID并访问默认的URL <http://find.dap.com:8080/> 或 <https://find.dap.com/> 即可以连接到初始化配置向导页面。本章节主要介绍用户在初次使用DAP847-XXA时如何访问DAP集群管理页面并根据配置向导完成基本的参数配置。

4.1 通过Web浏览器访问DAP847-XXA Cluster Manager

每个DAP847-XXA支持3个不同的账号同时登陆DAP847-XXA Cluster Manager，通过PC上的Web浏览器访问GUI。

该GUI包括一个设置向导，可以指导您更改管理员密码并完成基本的WLAN配置。

GUI中还提供了Dashboard监控功能，该Dashboard是一个以图形化方式展示DAP847-XXA的关键指标、网络性能数据和无线客户端信息的中心面板。它允许用户以直观的方式跟踪、分析和监控DAP847-XXA的运行状态，从而更好地理解DAP847-XXA的关键指标。

如需在 **GUI Dashboard** 中识别和诊断 WLAN 的相关问题，请参阅文档第31页的“[Dashboard页面简介](#)”。

4.1.1 预置条件

要设置DAP847-XXA，请确保以下条件均被满足：

- ▶ 首先将DAP847-XXA设备连接到交换机并接通电源。
- ▶ 保证所有的DAP847-XXA设备在相同的子网里并且能够相互通信（交换机未开启端口隔离功能）。
- ▶ 网络中有可用的 DHCP 服务器为DAP847-XXA和无线客户端分配IP地址。
- ▶ 网络中有可用的DNS 服务器，能够解析访问DAP847-XXA的URL信息。

根据使用经验和测试经验，我们建议配置终端能够支持如下操作系统 (OS) 和浏览器。

建议操作系统	建议浏览器
Windows 8	Google Chrome 115 及更高版本
Windows 10 Windows 11	Mozilla Firefox 113及更高版本
MAC OS X 10.10	Microsoft Edge 115及更高版本
MAC OS X 10.11	

表 1: 推荐的操作系统和浏览器版本

注意: 通过Web浏览器连接单个DAP847-XXA的过程与连接到DAP847-XXA集群的过程是相同的。我们建议初次配置时先只连接1台DAP847-XXA设备到网络并完成初始配置, 然后再逐台连接其他的DAP847-XXA同步集群的配置。

4.1.2 DAP847-XXA IP地址

可以通过如下三种方式获取和管理DAP847-XXA的IP地址:

- ▶ 默认状态下, 如果网络中没有DHCP服务器, DAP847-XXA将会使用192.168.1.254作为其默认的管理地址。
- ▶ DAP847-XXA支持手动配置一个静态的IP地址。
- ▶ 如果网络中存在DHCP服务器, DAP847-XXA支持从DHCP服务器动态获取IP地址。您可以通过在DHCP中查看已分配的地址, 也可以通过上行交换机的ARP表项来查询, 或者通过串口连接的方式使用“ifconfig br-wan”命令查看DAP847-XXA的IP地址, 见图 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:~$ █
```

图 2: 使用CLI查看DAP847-XXA的IP地址

4.1.3 在初始状态下访问DAP847-XXA的Web GUI

在默认出厂设置中，在DAP847-XXA内部预置了一个2.4 GHz频段的SSID，可以通过无线接入并通过Web GUI进行管理。您可根据配置向导完成初始化的配置：

- 在无线控制端上搜索并连接到一个在2.4 GHz频段一个名为“mywifi-xx:xx”的SSID，如图3所示。

注意：“xx:xx”是PVM MAC地址的最后两个字节。

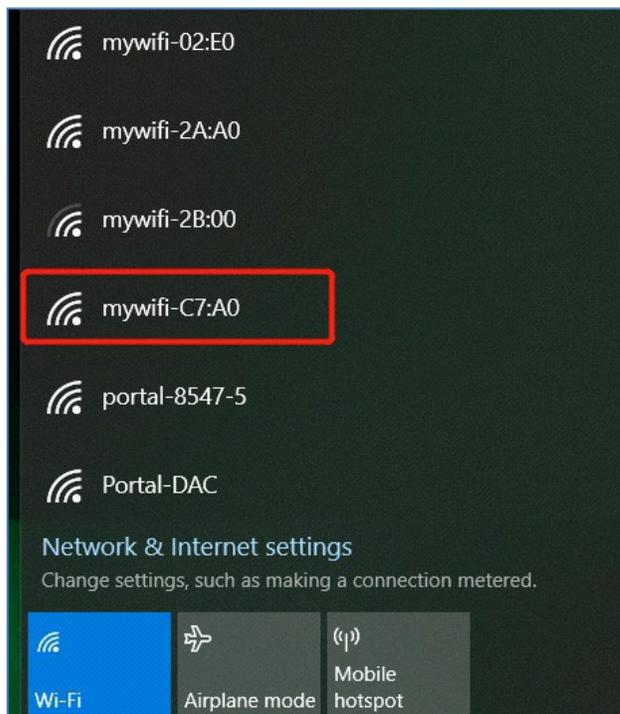


图3：连接到默认的SSID

- 通过http或https的方式登陆AP Cluster Manager，出厂状态下的登录密码为“admin”。
 - ▶ 通过http登录，输入<http://find.dap.com:8080/>。DAP847-XXA IP地址是172.16.102.109，参考图4。

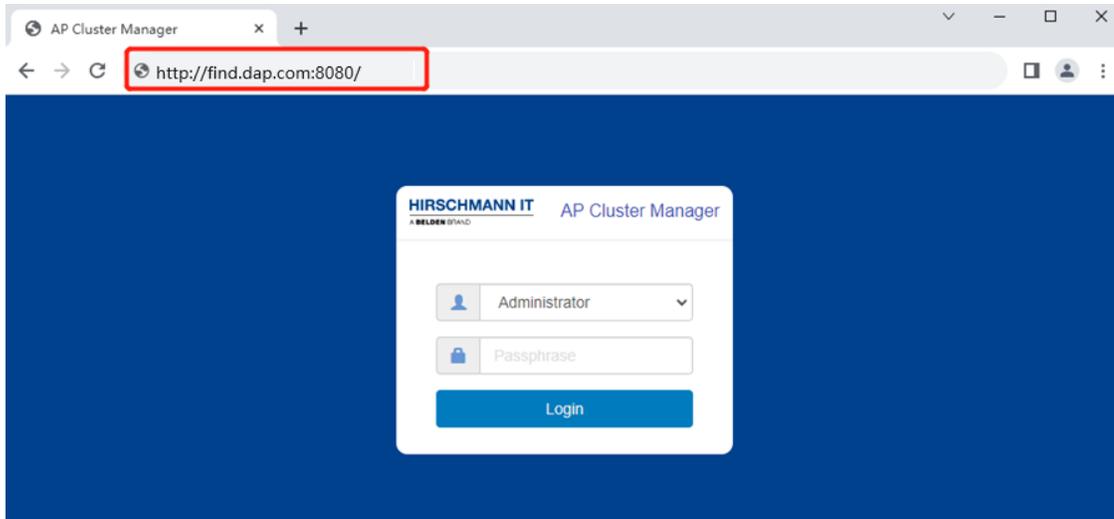


图 4: HTTP 登陆

- ▶ 通过https登录，输入<https://find.dap.com>。DAP847-XXC IP地址是172.16.102.109，参考图 5。

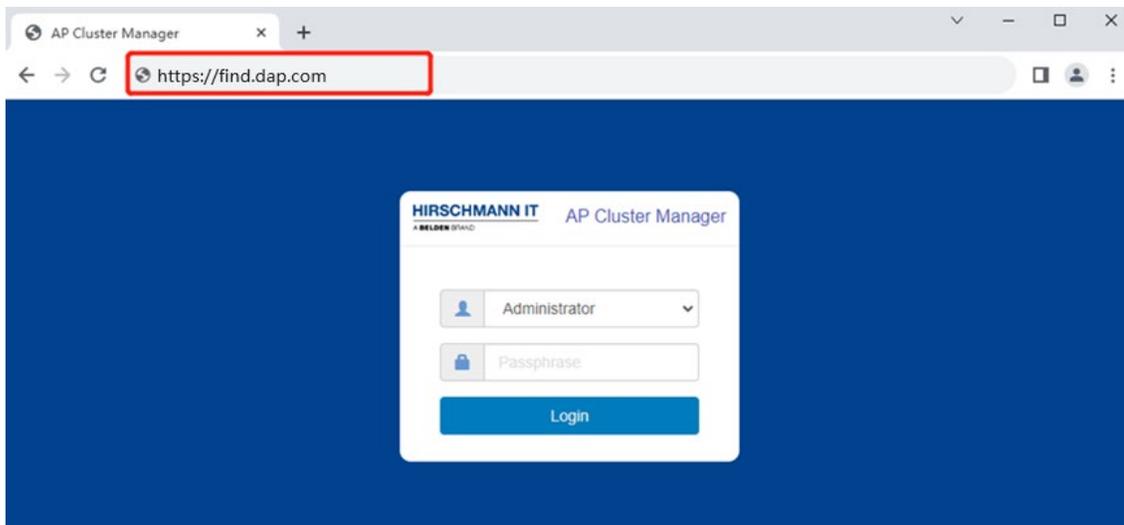


图 5: HTTPS 登陆

注意：为保证DAP847-XXA和浏览器之间进行更安全的通信，通过https模式登录时需要使用数字证书。首先需要从DAP847-XXA下载CA根证书，并将其安装到浏览器中。证书安装过程因操作系统和浏览器组合而异。请参考图 6。

Https Setting Window

1. Download and Install Certificate

2. Go to HTTPS page for login

图 6: 下载并安装证书

如果在网络中没有可用的DNS服务器，则可以使用集群中任意一台DAP847-XXA的IP地址登陆到DAP847-XXA集群。如果使用非PVM设备的IP地址登陆，则会自动跳转到PVM的登陆页面，请参考图 7。

例如：

- ▶ <http://172.16.10.169:8080>（172.16.10.169是DAP847-XXA的IP地址）
- ▶ <https://172.16.10.169>（172.16.10.169是DAP847-XXA的IP地址）

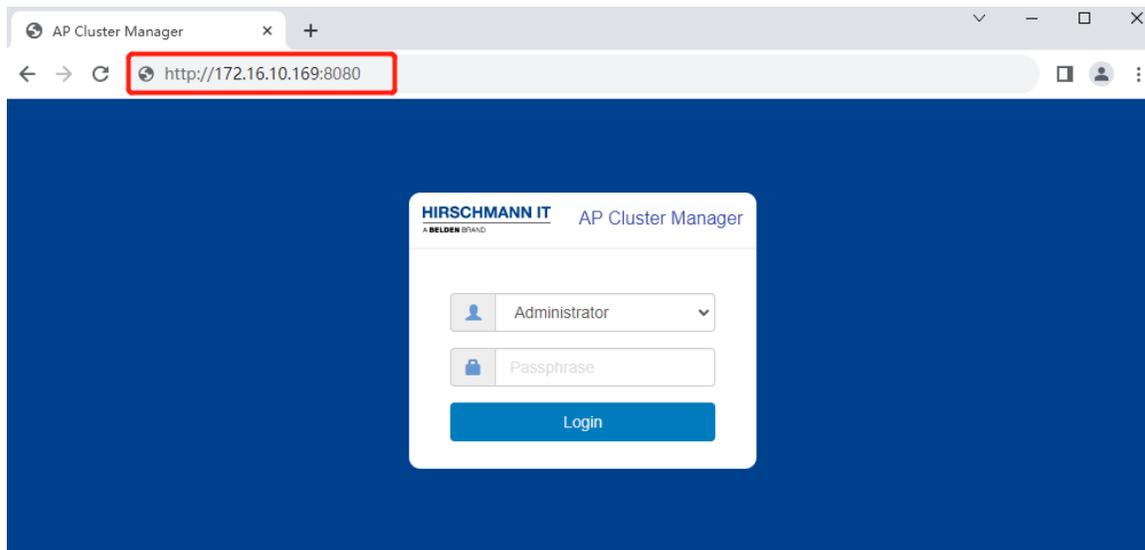
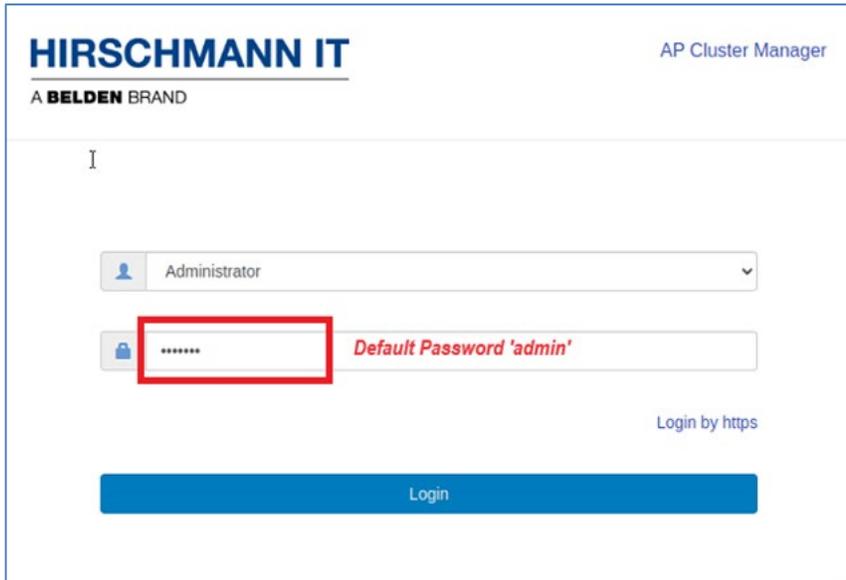


图 7: 使用IP地址登陆

如果您不知道DAP847-XXA当前的IP地址，可以使用命令行`ifconfig br-wan`查看DAP847-XXA使用的IP地址，见第21页的“DAP847-XXA IP地址”。

4.2 使用DAP847-XXA设置向导

请使用默认的**Administrator**帐户登陆，初始化默认密码为“**admin**”。初次登陆时，将会通过配置向导来完成初始的配置。



The screenshot displays the login interface for the Hirschmann IT AP Cluster Manager. At the top left, the logo 'HIRSCHMANN IT' is shown with the tagline 'A BELDEN BRAND'. The top right corner identifies the application as 'AP Cluster Manager'. The main content area features a user selection dropdown menu currently set to 'Administrator'. Below this is a password input field, which is highlighted with a red rectangular box. To the right of the password field, a red text prompt reads 'Default Password 'admin''. Below the password field, there is a link for 'Login by https' and a prominent blue 'Login' button.

图 8: 以Administrator登陆

4.2.1 DAP的初始化配置

按照设置向导的步骤完成DAP的初始化配置：

- 选择DAP847-XXA的工作模式。
 - ▶ **集群模式：**通过分布式自组网络模式实现自主管理，无需额外的控制器，会从集群中选举出来一台DAP847-XXA作为虚拟控制器。
 - ▶ **DAC模式：**DAP847-XXA设备可以由DAC管理平台进行集中管理，由DAC完成配置和策略的下发，关于DAC模式的详细信息请参考[DAC用户手册](#)。

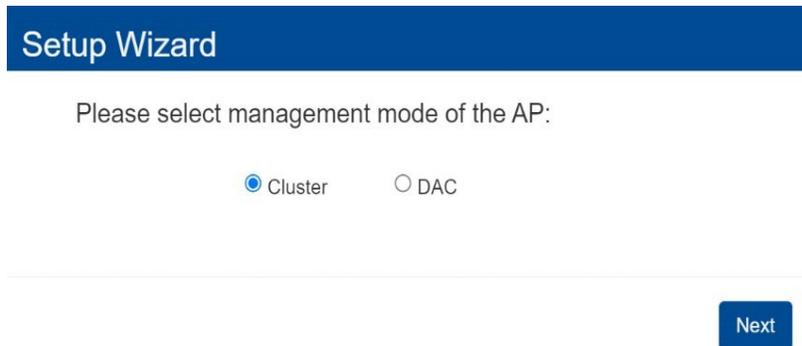


图9：选择工作模式

- DAP847-XXA Cluster Manager欢迎页面。

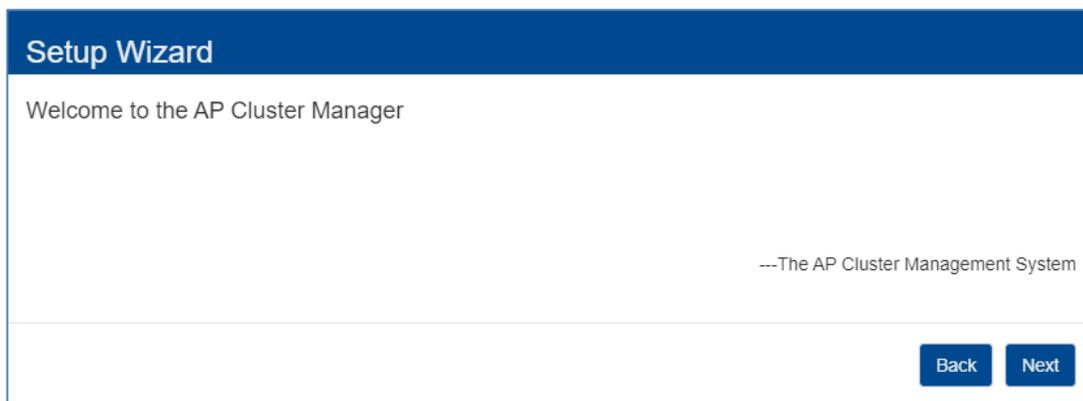


图10：DAP847-XXA Cluster Manager欢迎页面

- 修改administrator的登陆密码。

Setup Wizard

Step 1/3 Change your administrator password

Password:

Confirm:

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

图 11: 修改管理员账户密码

- 选择 **“Country/Region”** 和 **“Time Zone”**。

Setup Wizard

Step 2/3 Choose your Country or Region

Country/Region:

Time Zone:

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

图 12: 选择 Country/Region 和 Time Zone

- 创建一个新的WLAN，参考第32页的 [“WLAN页面”](#)。

注意：创建新的SSID后，默认的名称为 **“mywifi-xx:xx”** 的SSID将会被删除。

Setup Wizard

Step 3/3 Create New WLAN

WLAN Name:	<input type="text" value="My-wifi-test"/>
Band:	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz
Security Level:	<input type="text" value="Personal"/>
Key Management:	<input type="text" value="Both (WPA2 & WPA)"/>
PMF:	<input type="text" value="Disabled"/>
Password Format:	<input type="text" value="8-63 chars"/>
Password:	<input type="password" value="....."/>
Confirm:	<input type="password" value="....."/>

图 13: 创建一个新的 WLAN

在完成设置向导后，DAP847-XXA会自动重新启动并切换到新的工作模式并给出如下提示信息。

Notice

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

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

图 14: DAP847-XXA 切换模式并重新启动

当DAP847-XXA重新启动后，您便能够连接到新的SSID上。您可以使用新密码登录，并根据需要继续完成其他功能的配置。当您登录到Web GUI后，您将看到默认SSID已被删除，新的SSID显示在WLAN页面中。

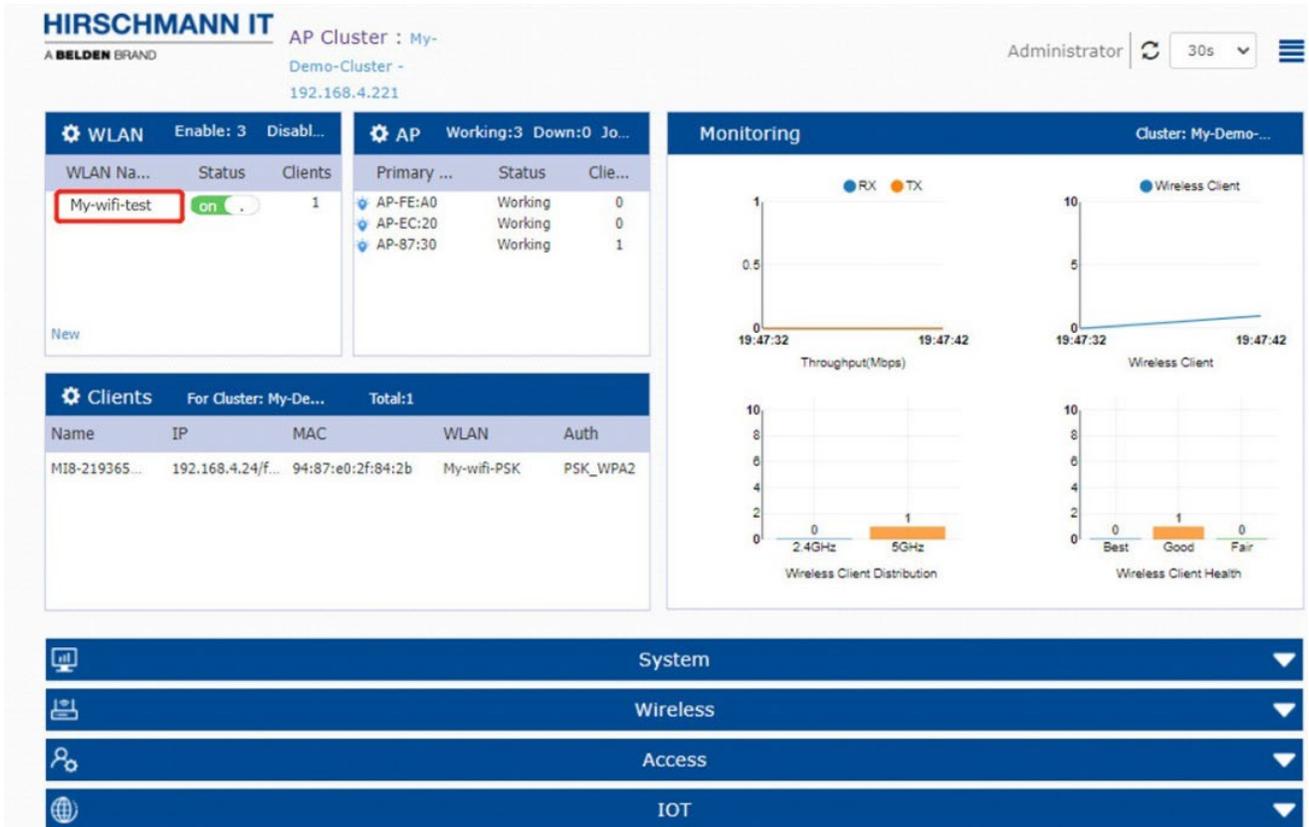


图 15: 重新登陆DAP847-XXA Cluster Manager

5 DAP847-XXA Cluster Manager用户界面

在本章节中主要介绍了DAP847-XXA Web UI上的Dashboard以及每个单独的配置页面。关于具体的配置内容和详细信息，请参考对应章节中的详细描述。

本章节主要包含如下内容：

- ▶ [Dashboard](#)页面简介
- ▶ [WLAN](#)页面
- ▶ [AP](#)页面
- ▶ [Clients](#)页面
- ▶ [Monitoring](#)页面
- ▶ [System](#)页面
- ▶ [Wireless](#)页面
- ▶ [Access](#)页面
- ▶ [DAP847-XXA](#)的其它信息

5.1 Dashboard页面简介

DAP847-XXA提供了一个Dashboard页面，用来展示当前的运行状态和配置信息。

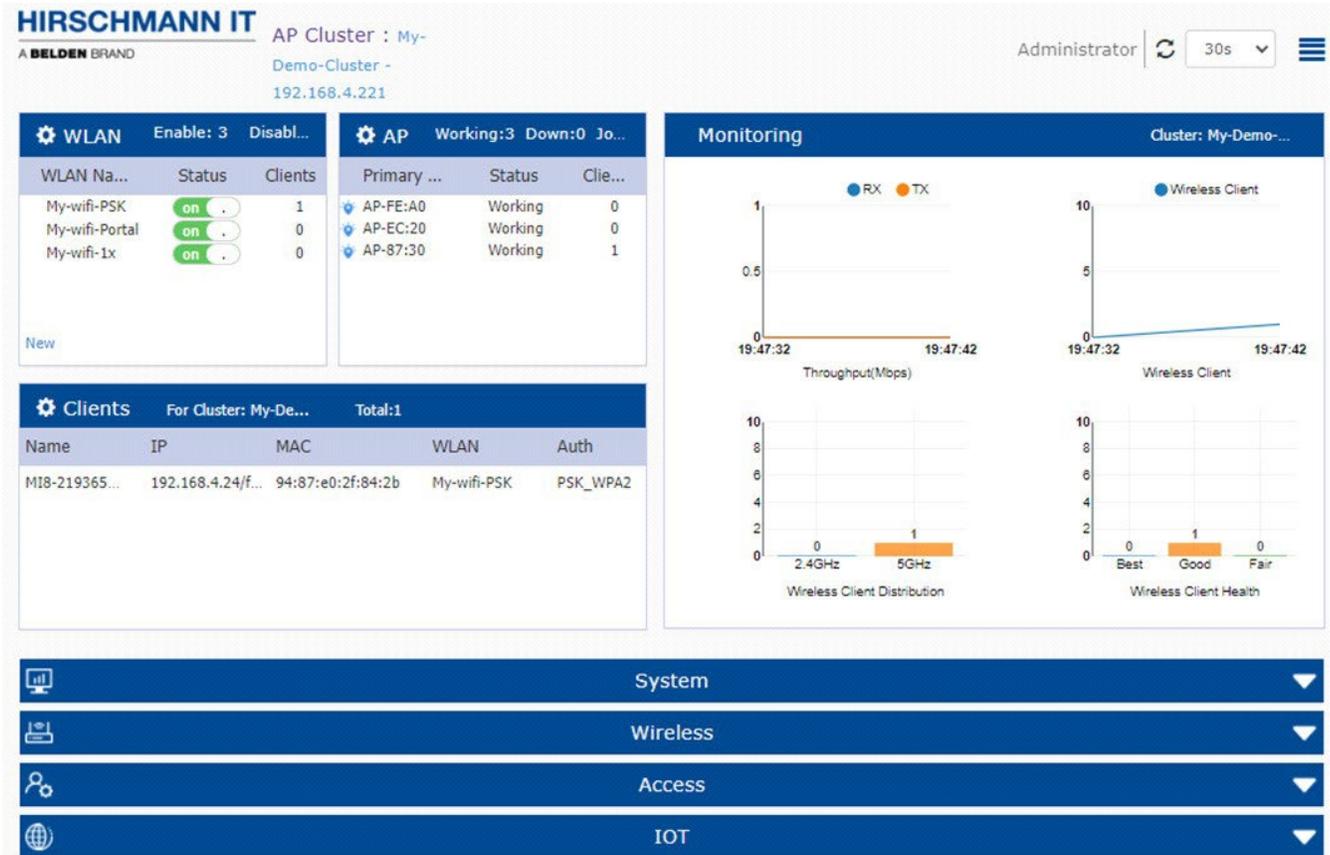


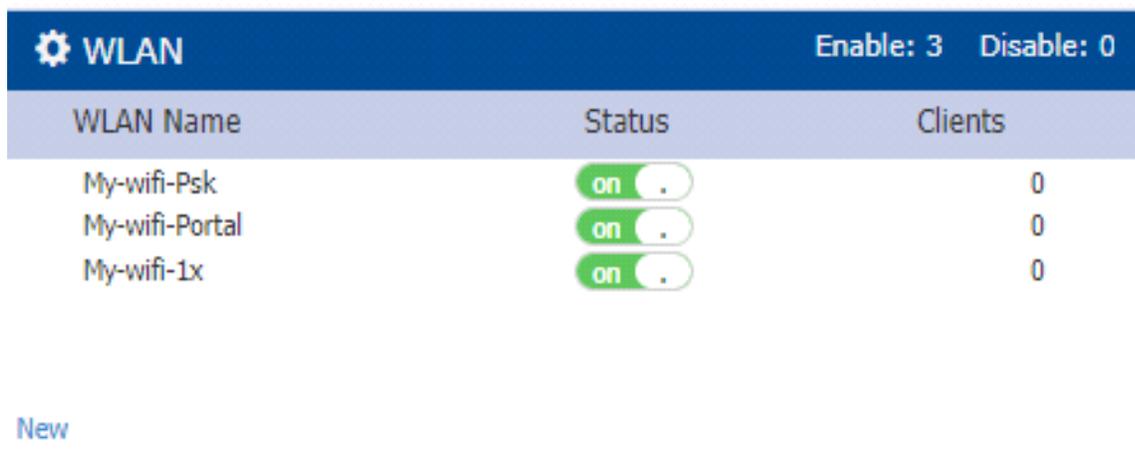
图 16: DAP847-XXA 主页面

如图 16 所示，在页面顶端，可以看到集群信息、当前登录用户、刷新按钮以及刷新周期等。

Dashboard 页面分为 **WLAN**、**AP**、**Monitoring**、**Clients**、**System**、**Wireless**、**Access** 和 **IOT** 等几个子页面，可以点击每个页面查看详细的信息。

5.2 WLAN页面

WLAN页面包含了与WLAN相关的状态监控信息和和配置操作。WLAN页面有两种模式，基本模式和WLAN配置模式，单击**WLAN**页面以进入WLAN配置页面。



WLAN		Enable: 3	Disable: 0
WLAN Name	Status	Clients	
My-wifi-Psk	<input checked="" type="checkbox"/>	0	
My-wifi-Portal	<input checked="" type="checkbox"/>	0	
My-wifi-1x	<input checked="" type="checkbox"/>	0	

New

图 17: WLAN 页面

关键参数描述如下：

参数	描述
WLAN Name	WLAN名称，即SSID名称，由0 ... 9、a ... z或其他字符串组成。
Status	标识 WLAN 的状态： <input type="checkbox"/> off 表示该WLAN未启用。 <input checked="" type="checkbox"/> on 表示该WLAN已启用。
Clients	该WLAN下连接的无线用户数量。
New	进入WLAN创建页面。

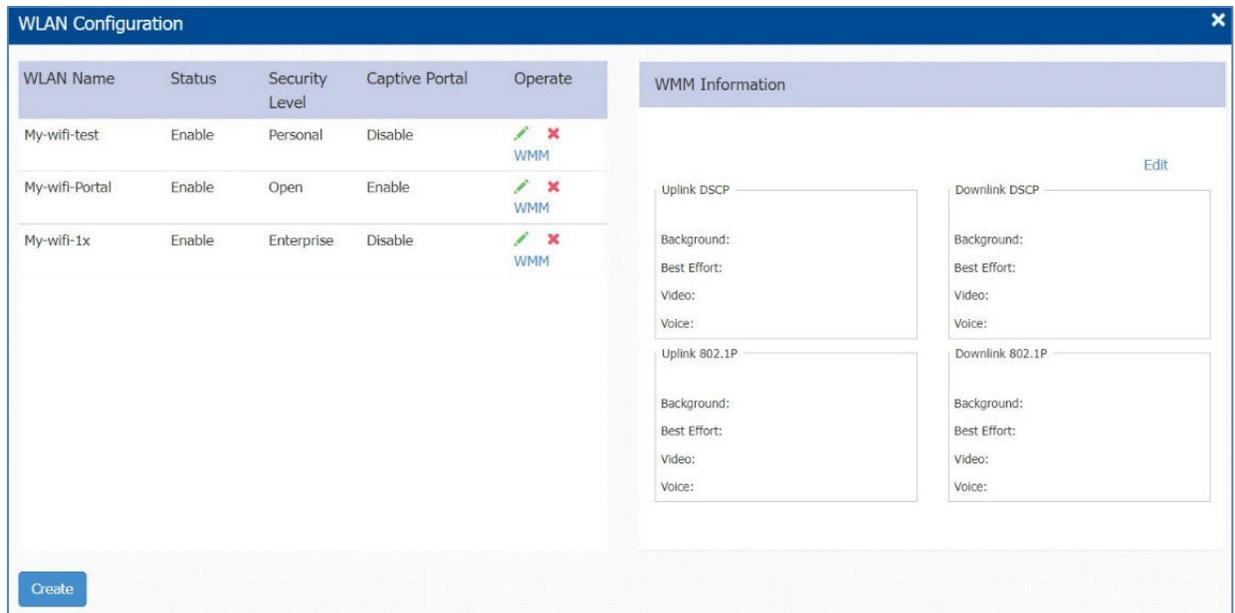


图 18: WLAN Configuration 页面

关键参数描述如下:

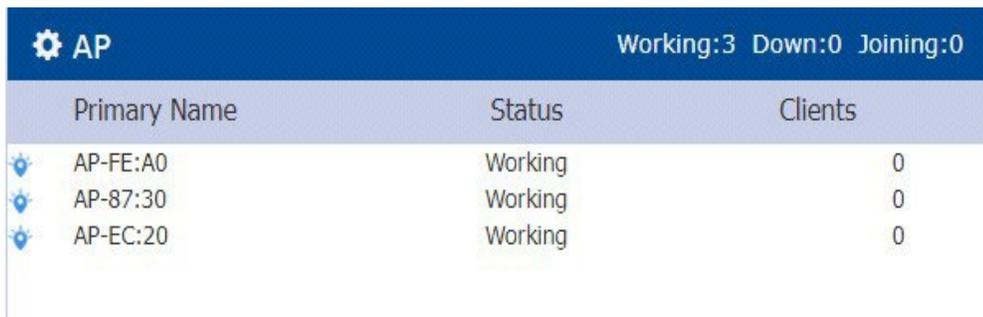
参数	描述
WLAN Name	WLAN名称, 即SSID名称, 由0 ... 9、a ... z或其他字符串组成。
Status	标识WLAN的状态: <ul style="list-style-type: none"> ▶ “Enable”: 表示该WLAN已启用。 ▶ “Disable”: 表示该WLAN未启用。
Security Level	表示WLAN的安全级别, 按照安全级别由高到低的顺序, 分别为: Enterprise>Personal>Open 。
Captive Portal	表示该WLAN是否开启了Portal身份验证: <ul style="list-style-type: none"> ▶ “Enable”: 表示该WLAN启用了Portal身份验证。 ▶ “Disable”: 表示该WLAN未启用Portal身份验证。
Operate	配置操作WLAN, 包括 “Modifying your WLAN” 、 “Deleting your WLAN” 和 “Modifying Wi-Fi Multimedia (WMM)” 。
Create	创建一个新的WLAN。

注意: 如下标签显示启用或禁用状态的WLAN的数量。



5.3 AP页面

AP页面包含了DAP847-XXA的基本信息，包括MAC地址和工作状态等，AP页面有两种模式，单击AP页面标题栏，可以从基本模式切换到AP Configuration模式。



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

图 19: AP 页面

关键参数描述如下：

参数	描述
Primary Name	显示DAP847-XXA的名称，默认格式为AP-XX:XX，其中XX:XX为AP MAC最后两个字节。
Status	表示DAP847-XXA的连接状态： ▶ Working : 表示该DAP847-XXA已连接到PVM，工作正常。 ▶ Down : 表示该DAP847-XXA已断开与集群的连接。 ▶ Joining : 表示该DAP847-XXA正在加入集群。
Clients	表示该WLAN下连接的无线用户的数量。

注意：AP页面中的标签显示了每种状态下的AP数量。



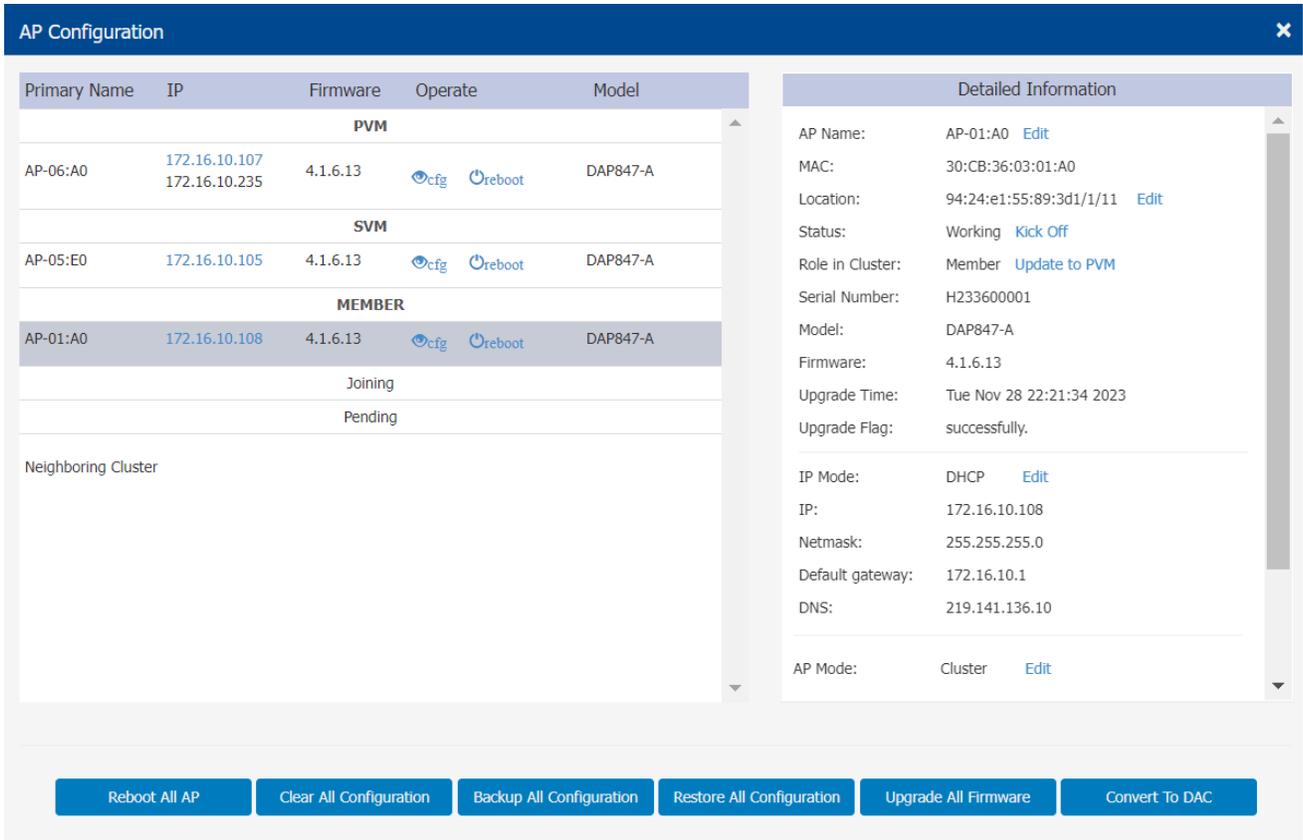


图 20: AP Configuration 页面

关键参数描述如下:

参数	描述
Primary Name	DAP847-XXA名称。
IP	DAP847-XXA的IP地址。
Firmware	DAP847-XXA的软件版本。
Operate	DAP847-XXA有两种可选操作： cfg : 查看该DAP847-XXA的详细配置信息。 reboot : 重启该DAP847-XXA。
Model	DAP847-XXA的型号。
PVM	表示该DAP847-XXA在集群中是PVM。
SVM	表示该DAP847-XXA在集群中是SVM。
MEMBER	表示该DAP847-XXA在集群中是普通成员。
Joining	处于Joining状态下的 DAP847-XXA，需要授权才能加入集群。
Pending	处于Pending状态下的DAP847-XXA，需要升级软件才能加入集群。
Neighboring Cluster	具有不同集群ID的相邻DAP847-XXA集群。

参数	描述
Reboot All AP	重启集群中所有DAP847-XXA设备。
Clear All Configuration	清除所有配置，将集群中所有设备恢复出厂设置。
Backup All Configuration	备份DAP集群的配置，一个名为“pub-config.tar”的配置文件将会下载到本地主机。
Restore All Configuration	恢复之前备份的配置文件，请注意这个文件名必须为“pub-config.tar”。
Upgrade All Firmware	为集群中所有的DAP847-XXA设备升固件。
Convert To DAC	将DAP847-XXA由集群工作模式切换到DAC工作模式，一旦执行该操作，DAP847-XXA将会重启并注册到DAC中，由DAC集中管理。 Management Server: DAC的IP地址。
Detailed Information	<p>所选DAP847-XXA的详细信息：</p> <ul style="list-style-type: none"> ▶ AP Name: 该DAP847-XXA的名称 ▶ MAC: 该 DAP847-XXA的MAC地址 ▶ Location: 该DAP847-XXA的位置信息 ▶ Status: 该DAP847-XXA的状态 ▶ Role in Cluster: 群集中所选DAP847-XXA的角色 ▶ Serial Number: 该DAP847-XXA的序列号（SN）。 ▶ Model: 该DAP847-XXA的产品型号 ▶ Firmware: 该DAP847-XXA的固件版本 ▶ Upgrade Time: 该DAP847-XXA上次升级时间 ▶ Upgrade Flag: 该DAP847-XXA上次升级的结果 ▶ IP Mode: 该DAP847-XXA获取IP地址的方式 ▶ IP: 该DAP847-XXA的IP地址 ▶ Netmask: 该DAP847-XXA的IPv4地址网络掩码 ▶ Default gateway: 该DAP847-XXA的默认网关 ▶ DNS: DNS服务器
Kick Off	从集群中删除指定DAP847-XXA，该设备从集群中删除后，将会变为“Joining”状态，直到管理员允许它再次加入该集群。
Update to PVM	集群中的SVM成员设备可以升级成为PVM。
AP Mode	<ul style="list-style-type: none"> ▶ Cluster: DAP在集群模式下工作。 ▶ DAC: 通过DAC平台集中管理DAP。如需将DAP847-XXA的模式更改为DAC模式时，需要指定DAC的IP地址。

5.4 Clients页面

Clients页面显示了当前连接的客户端信息。与WLAN页面一样，客户端页面有两种模式：基本模式和客户端详细信息模式。单击“**Clients**”页面的标题栏，可以从基本模式进入到客户端详细信息模式。

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

图 21: Clients 页面 - 基本模式

关键参数描述如下：

参数	描述
For Cluster: [Cluster Name]	整个集群中连接的客户端信息。
For WLAN: [WLAN Name]	基于指定WLAN统计的客户端信息。
For AP: [AP_MAC]	基于指定的DAP847-XXA统计的客户端信息。
Name	客户端的用户名或主机名。对于使用用户名登录的客户端，该用户名将显示在该字段中。对于不使用用户名登录的客户端，则显示为主机名。如果无法获取主机名，则该Name字段可能显示为空。
IP	客户端的IP地址，包括IPv4地址和IPv6地址。
MAC	客户端的MAC地址。
WLAN	客户端所连接的WLAN名称。
Auth	客户端的认证类型：OPEN、Portal (Captive portal)、PSK (Personal)或802.1x (Enterprise)。

在“**Clients Information**”页面中，选择并点击客户端条目的“**x**”按钮，可以断开客户端与DAP847-XXA的无线连接；如果选择点击“**⌵**”按钮，则会断开客

户端的连接并将该客户端加入到黑名单列表中。

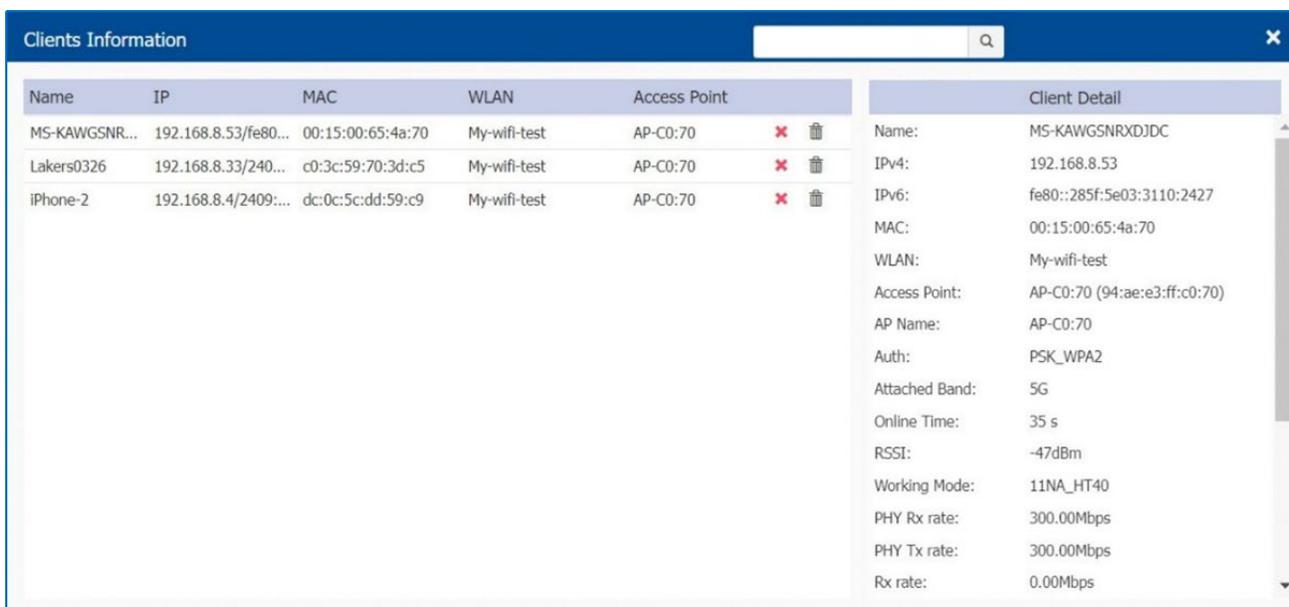


图 22: Clients information 页面

■ Client Information 参数描述如下:

参数	描述
Name	客户端的用户名。
IP	客户端的IP地址。
MAC	客户端的MAC地址。
WLAN	客户端所关联的WLAN。
Access Point	客户端所关联的DAP847-XXA设备名称。
	断开该客户端的无线连接。
	断开客户端的连接并将该客户端加入到黑名单列表中，如果客户端被加入到黑名单列表，您可以在 Access→Blocklist & Allowlist 页面中进行查看和修改。

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 +	

图 23: Client Detail 页面

■ Client Detail 参数描述如下:

参数	描述
Name	客户端名称。
IPv4	客户端的IPv4地址。
IPv6	客户端的IPv6地址。
MAC	客户端的MAC地址。
WLAN	客户端所关联的WLAN。
Access Point	客户端所关联的DAP847-XXA设备名称（MAC地址）。
AP Name	客户端所关联的DAP847-XXA设备名称。
Auth	客户端的身份验证类型：包括Open、Portal（Captive Portal）、PSK（Personal）、802.1x（Enterprise）。

参数	描述
Attached Band	客户端连接的射频信息，2.4 GHz或5 GHz。
Online Time	客户端的在线连接时长。
RSSI	客户端的接收信号强度（RSSI），范围为0 ... 99。
Working Mode	客户端的无线模式。
PHY Rx rate	客户端的物理层接收速率，单位为Mbps。
PHY Tx rate	客户端的物理层发送速率，单位为Mbps。
Rx rate	客户端的网络层接收速率，单位为Mbps。
Tx rate	客户端的网络层发送速率，单位为Mbps。
Download	客户端自最近一次连接来所下载的数据量。
Upload	客户端自最近一次连接来所上传的数据量。
Device type	客户端的设备类型。
OS Type	客户端的操作系统类型。
Rx Error	表示客户端检测接收到的错误数据包的数量，这些错误数据包可能是由于干扰或信号强度不匹配导致的。
Tx Retry	表示客户端发送的重试数据包数，重试数据包表示重新发送的数据包，有可能是由于干扰等原因该数据帧在到达接收端时已经损坏。
Roaming History	<p>显示客户端在SSID/AP/Band之间的漫游的历史信息，最多可以显示32条漫游记录，按照连接会话进行区分。</p> <p>Connection Session: 表示从与无线网络关联开始到解除关联的时间。漫游记录也会分布在Session中。</p> <p>连接会话是基于时间顺序来显示的，最新的会话将位于漫游历史信息顶部。</p> <p>Offline状态表示该连接已经结束。Online状态表示该目前处于在线状态。</p>

5.5 Monitoring页面

“**Monitoring**”页面主要显示了无线网络的使用情况，包括无线网络流量和客户端状态的统计信息。监控页面显示了4个方面的数据统计，分别是基于集群、基于WLAN、基于AP和基于客户端的数据。

默认状态下呈现的是基于群集的数据统计：

- 在 **WLAN** 页面中选择一个 **WLAN**，切换为该 **WLAN** 的数据统计
- 在 **AP** 页面中选择一个 **DAP847-XXA**，切换为该 **DAP847-XXA** 的数据统计
- 在 **Client** 页面中选择一个客户端，切换为该 **Client** 的数据统计

默认情况下，“**Monitoring**”页面的刷新周期为30秒，并可以设置为60秒或120秒。

5.5.1 基于集群的监控

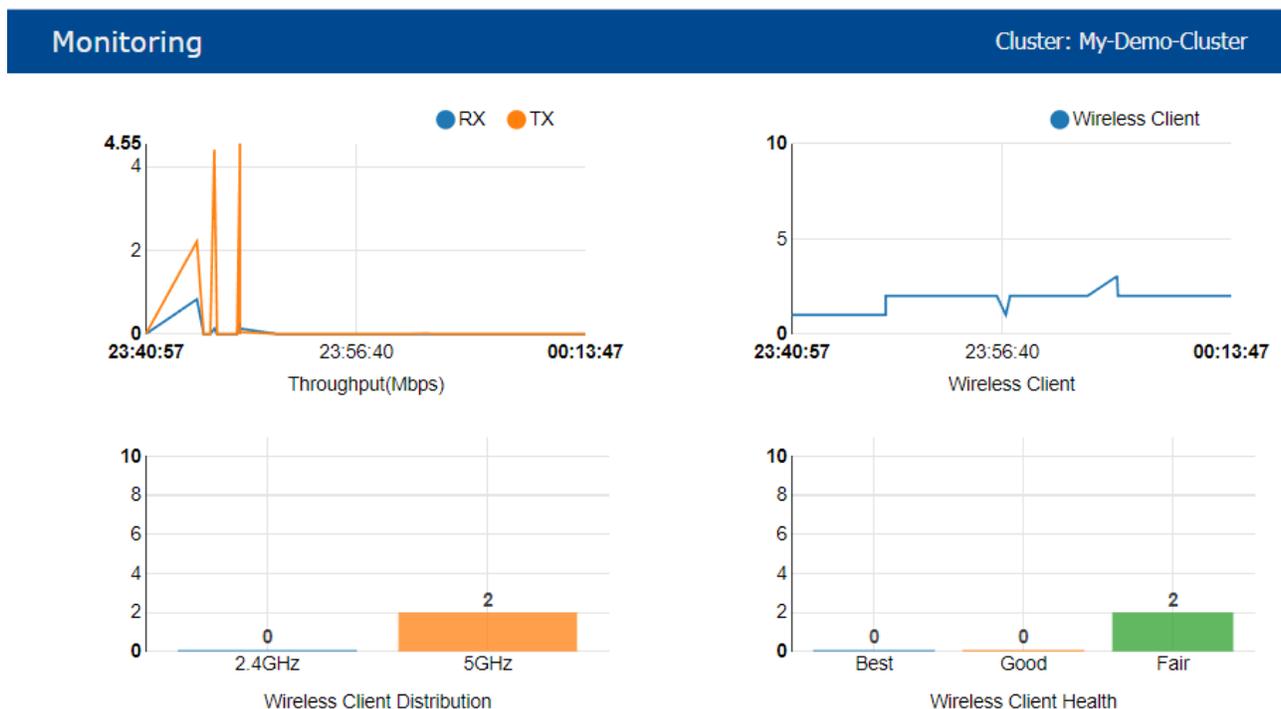


图 24: Cluster Monitoring 页面

关键参数描述如下:

参数	描述
RX	表示集群中所有DAP847-XXA的平均接收的数据速率（吞吐量），单位为Mbps。
TX	表示集群中所有DAP847-XXA的平均发送的数据速率（吞吐量），单位为Mbps。
Wireless Client	表示集群中所有无线客户端的总数。
Wireless Client Distribution	表示连接到DAP847-XXA集群的无线客户端所属的频段分布，包括关联在2.4 GHz频段的客户端数量和关联在5 GHz频段的客户数量。
Wireless Client Health	根据客户端的信号强度来评估客户端和DAP847-XXA之间的无线链路质量，分为以下三个级别： <ul style="list-style-type: none"> ►Best: 信号强度超过30的客户端数量（含）。 ►Good: 信号强度在15到30之间的客户端数量。 ►Fair: 信号强度小于15（含）的客户数量。

5.5.2 基于WLAN的监控

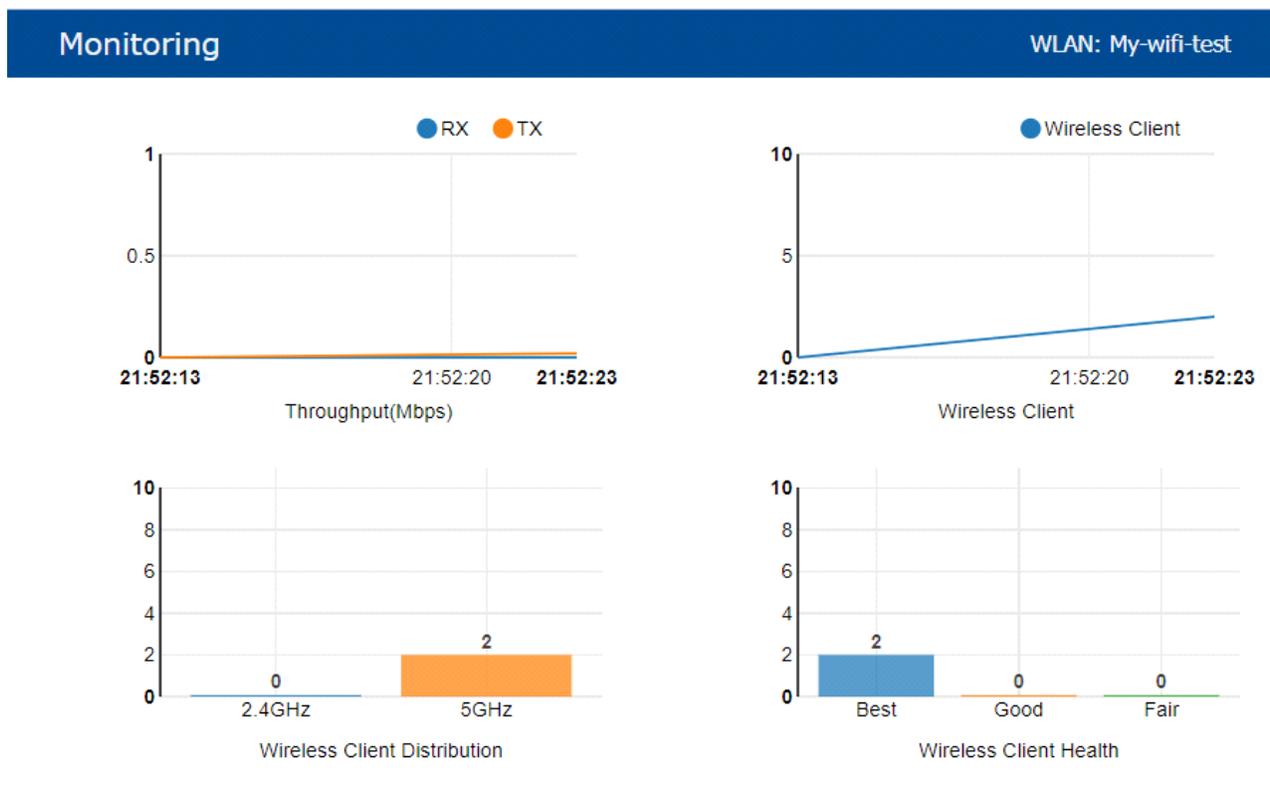


图 25: WLAN Monitoring 页面

关键参数描述如下:

参数	描述
RX	表示该WLAN下的平均接收的数据速率（吞吐量），单位为Mbps。
TX	表示该WLAN下的平均发送的数据速率（吞吐量），单位为Mbps。
Wireless Client	表示该WLAN下所有无线客户端的总数。
Wireless Client Distribution	表示连接到该WLAN的无线客户端所属的频段分布，包括关联在2.4 GHz频段的客户端数量和关联在5 GHz频段的客户端数量。
Wireless Client Health	<p>在该WLAN下，按照客户端的信号强度来评估客户端和DAP847-XXA之间的无线链路质量，分为以下三个级别：</p> <ul style="list-style-type: none"> ▶Best: 信号强度超过30的客户端数量（含）。 ▶Good: 信号强度在15到30之间的客户端数量。 ▶Fair: 信号强度小于15（含）的客户端数量。

5.5.3 基于AP的监控



图 26: AP Monitoring 页面

关键参数描述如下:

参数	描述
RX	表示该AP的平均接收的数据速率（吞吐量），单位为Mbps。
TX	表示该AP的平均发送的数据速率（吞吐量），单位为Mbps。
Wireless Client	表示该AP下所有无线客户端的总数。
Wireless Client Distribution	表示连接到该DAP847-XXA下的无线客户端所属的频段的分布，包括关联在2.4 GHz频段的客户端数量和关联在5 GHz频段的客户端的数量。
Wireless Client Health	在该下，按照客户端的信号强度来评估客户端和DAP之间的无线链路质量，分为以下三个级别： ▶Best: 信号强度超过30的客户端数量（含）。 ▶Good: 信号强度在15到30之间的客户端数量。 ▶Fair: 信号强度小于15（含）的客户端数量。

5.5.4 基于客户端的监控



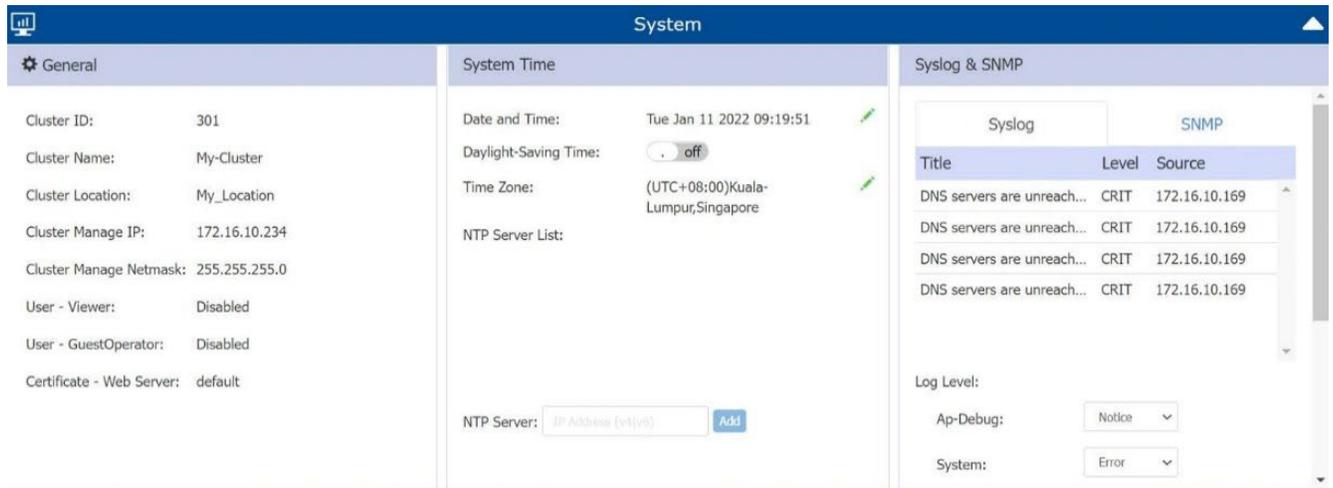
图 27: Client Monitoring 页面

关键参数描述如下:

参数	描述
RX	客户端的网络层接收速率，单位为Mbps。
TX	客户端的网络层发送速率，单位为Mbps。
RSSI	客户端接收信号强度。
PHY RX	客户端的物理层接收速率，单位为Mbps。
PHY TX	客户端的物理层发送速率，单位为Mbps。

5.6 System页面

System页面包含如下三个内容板块：**General**、**System Time**和**Syslog & SNMP**。有关System的详细介绍请参考第122页的“系统管理”。



The screenshot displays the 'System' configuration page, divided into three main sections: General, System Time, and Syslog & SNMP.

- General:** Contains fields for Cluster ID (301), Cluster Name (My-Cluster), Cluster Location (My_Location), Cluster Manage IP (172.16.10.234), Cluster Manage Netmask (255.255.255.0), User - Viewer (Disabled), User - GuestOperator (Disabled), and Certificate - Web Server (default).
- System Time:** Shows Date and Time (Tue Jan 11 2022 09:19:51), Daylight-Saving Time (off), Time Zone ((UTC+08:00)Kuala-Lumpur,Singapore), and an NTP Server List. An NTP Server field with a placeholder 'IP Address (v4/v6)' and an 'Add' button is visible at the bottom.
- Syslog & SNMP:** Features a 'Syslog' tab and an 'SNMP' tab. Below the tabs is a table with columns 'Title', 'Level', and 'Source'. The table contains four entries: 'DNS servers are unreach...', 'CRIT', and '172.16.10.169'. Below the table, there are 'Log Level' settings for 'Ap-Debug' (set to Notice) and 'System' (set to Error).

图 28: System页面

5.7 Wireless页面

Wireless页面包含如下3个内容板块：Radio Frequency (RF)、wIDS/wIPS和Performance Optimization，有关Wireless的详细介绍请参考第138页的“无线管理”。

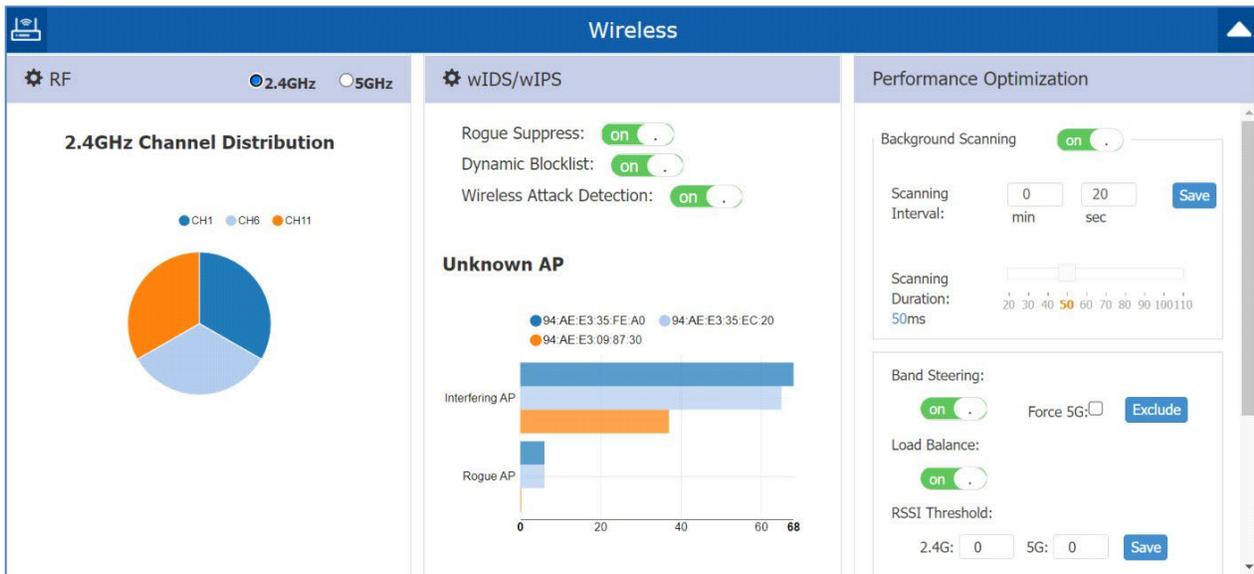


图 29: Wireless页面

5.8 Access页面

Access页面包括如下3个内容板块：**Authentication**、**Blocklist & Allowlist**和**ACL**。

有关Access的详细介绍，请参考第156页的“Access页面”。

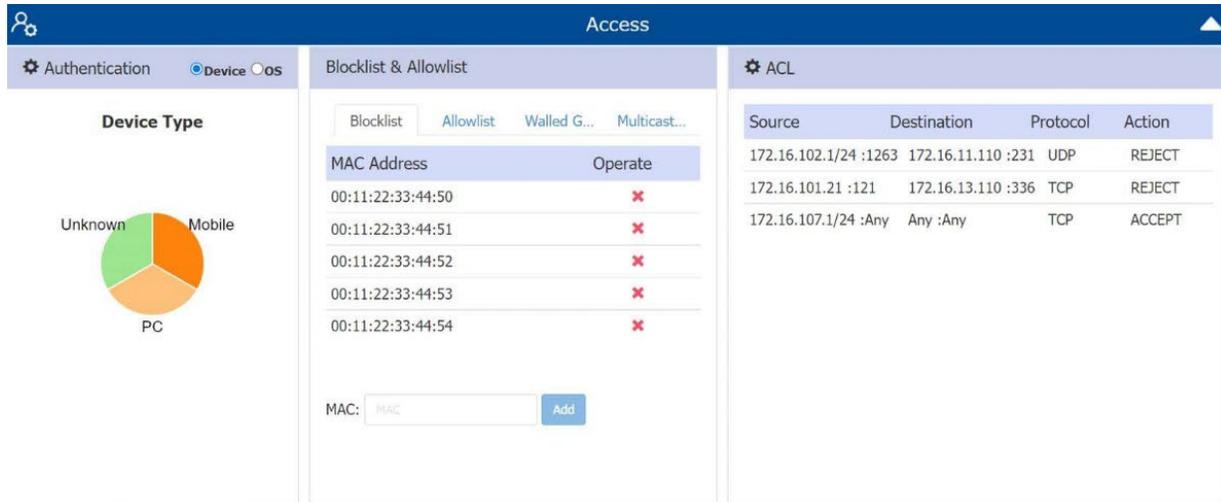


图 30: Access页面

5.9 DAP847-XXA的其它信息

有关DAP847-XXA的其他信息，如About, Tools等，请通过单击右上角的“More”来查看。

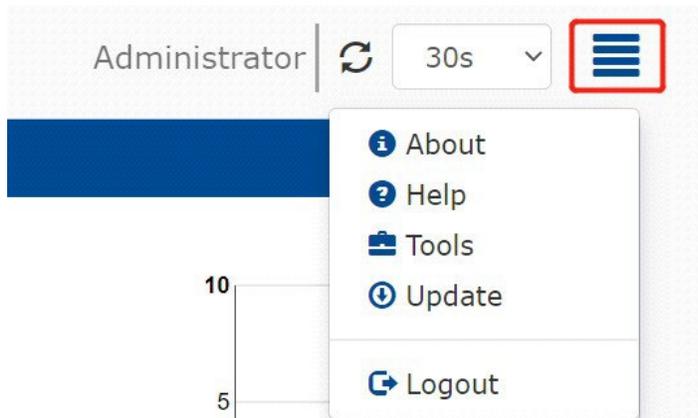


图 31: DAP847-XXA的其它信息

- ▶ **About:** 包含了DAP847-XXA的一些基本信息，如软件名称和软件版本、国家/地区等信息。



图 32: About 页面

- ▶ **Help:** 将鼠标指针停留在标题栏上时，将会给出对应的提示信息，可以帮助您更好的理解相关功能和操作。

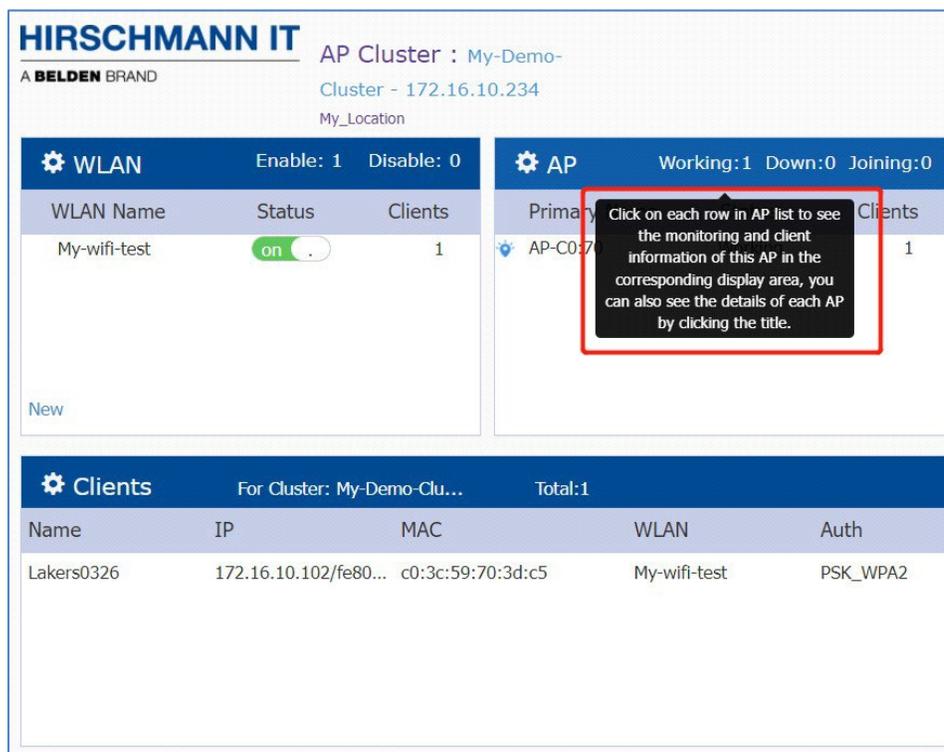


图 33: Online help

- ▶ **Tools:** DAP847-XXA中集成的一些基础的故障排查工具，详细信息请参考第174页的“DAP847-XXA内部集成工具”。
- ▶ **Update:** 如果检测到有新的版本，将会进行系统版本升级操作。
- ▶ **Logout:** 退出当前的用户登录。

6 WLAN配置

如果要配置一个Wi-Fi网络，配置WLAN通常是第一步操作，本章节主要介绍WLAN的相关配置操作，包括如下几个方面：

- ▶ 创建WLAN的两种方式
- ▶ WLAN的安全类型
- ▶ WLAN的相关参数介绍
- ▶ 修改WLAN的配置
- ▶ 删除WLAN
- ▶ WMM配置

6.1 创建WLAN的两种方式

集群模式下创建WLAN，有如下两种方式：

- 在WLAN的基本模式下，即主页面的WLAN页面，点击“New”。

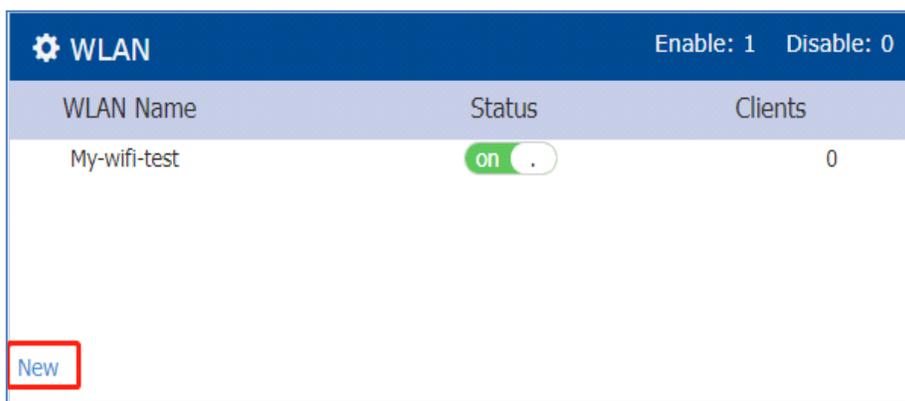
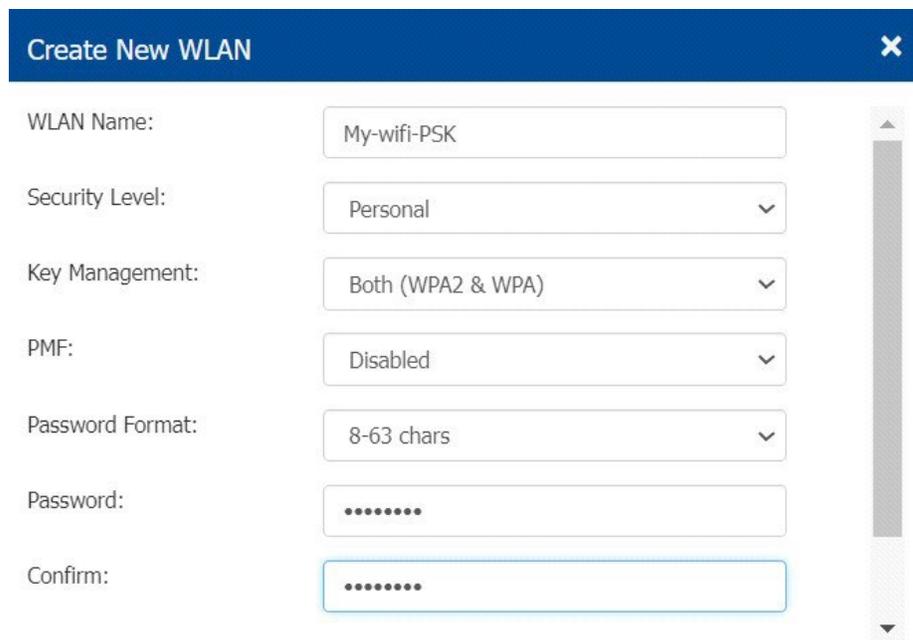


图 34: WLAN 基本模式

在弹出的“Create New WLAN”页面完成WLAN的配置。



The screenshot shows the 'Create New WLAN' configuration page. The title bar at the top is blue with the text 'Create New WLAN' and a close button (X). The page contains several configuration fields:

- WLAN Name: My-wifi-PSK
- Security Level: Personal (dropdown menu)
- Key Management: Both (WPA2 & WPA) (dropdown menu)
- PMF: Disabled (dropdown menu)
- Password Format: 8-63 chars (dropdown menu)
- Password: [masked with dots]
- Confirm: [masked with dots]

A vertical scrollbar is visible on the right side of the form.

图 35: Create New WLAN 页面

- 在**WLAN Configuration**页面，点击“**Create**”按钮，在右侧页面中完成WLAN的配置。

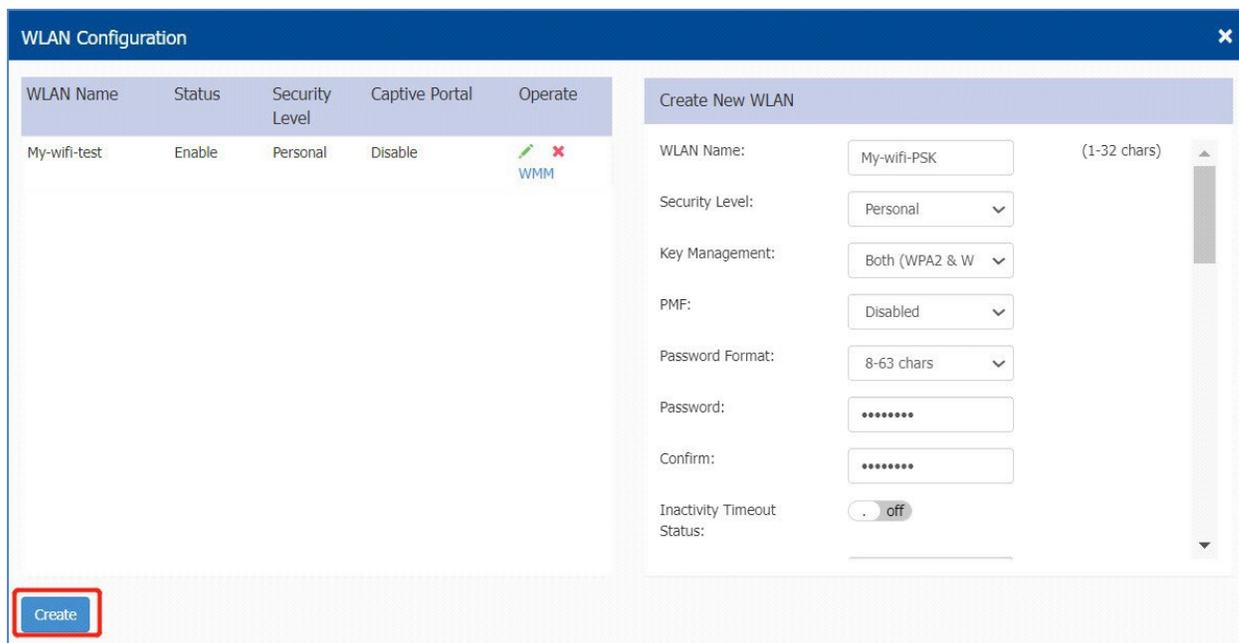


图 36: 在 WLAN Configuration 页面中创建 WLAN

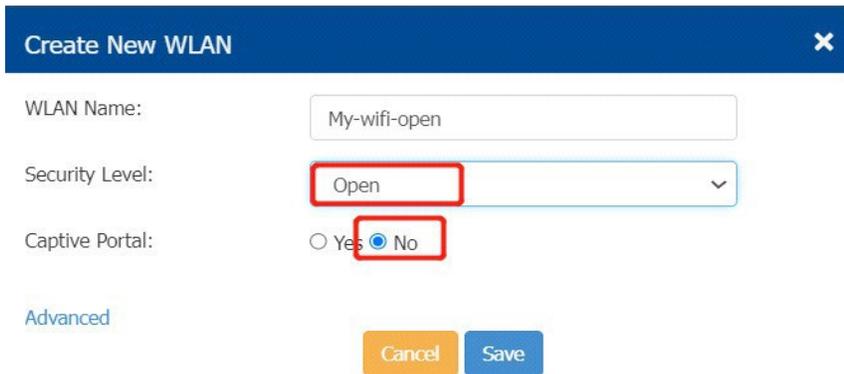
6.2 WLAN的安全类型

在集群模式下，DAP847-XXA支持如下4种安全类型的WLAN：

- ▶ Open
- ▶ Portal
- ▶ Personal
- ▶ Enterprise

6.2.1 安全类型Open

Open类型，即无身份验证或加密，无线客户端的数据以明文的形式传输。



The image shows a configuration window titled "Create New WLAN". It has a blue header bar with a close button (X). Below the header, there are three main configuration fields: "WLAN Name" with a text input containing "My-wifi-open"; "Security Level" with a dropdown menu showing "Open" (highlighted with a red box); and "Captive Portal" with two radio buttons, "Yes" and "No", where "No" is selected (highlighted with a red box). Below these fields is a link labeled "Advanced". At the bottom of the dialog are two buttons: "Cancel" (orange) and "Save" (blue).

图 37：创建一个Open类型的WLAN

6.2.2 安全类型Portal

在” **Create New WLAN** ” 页面，配置 “ **Security Level** ” 为 **Open** ，并将 “ **Captive Portal** ” 选择为 “ **Yes** ” ，则会创建一个**Portal**认证方式的WLAN。用户需要完成Portal认证后才能访问网络资源，参考第160页的 “ **Portal认证** ” 。

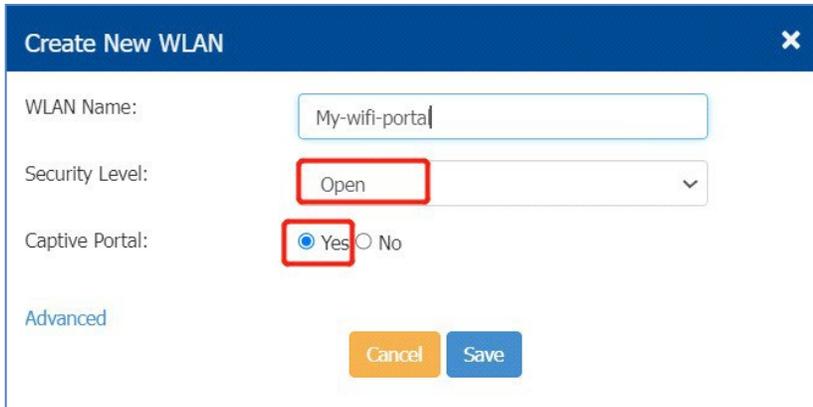


图 38: 创建一个 Portal 认证类型的 WLAN

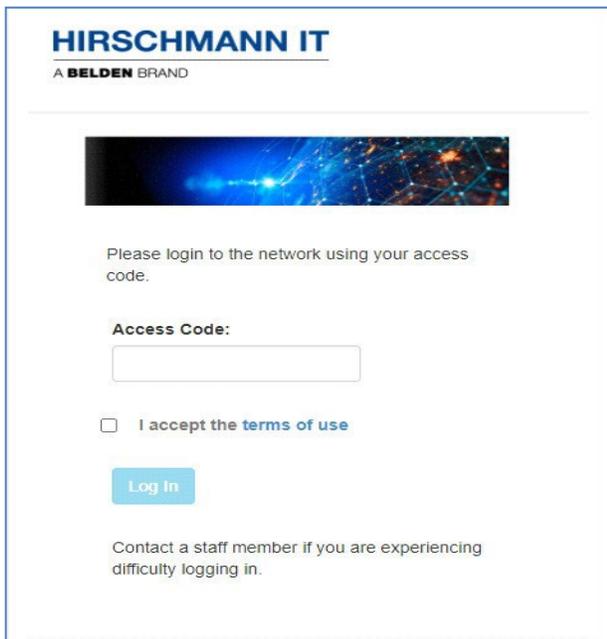


图 39: Portal 登陆页面

6.2.3 安全类型 Personal

Personal模式即PSK模式，是一种预共享密钥的模式，支持Static WEP、WPA2、WPA3、WPA2 & WPA、WPA3 & WPA2五种模式，预共享密钥模式是一种针对家庭或小型公司网络设计的认证模式。在这种模式下，每一个无线用户都需要输入预先配置好的密钥才能接入网络，不需要身份验证服务器。

WPA、WPA2、WPA3采用动态密加密数据包，每个无线网络设备使用256位密钥对网络流量进行加密，该密钥通常由8到63个ASCII字符组成。在**Personal**模式下，支持如下几种密钥管理方式：

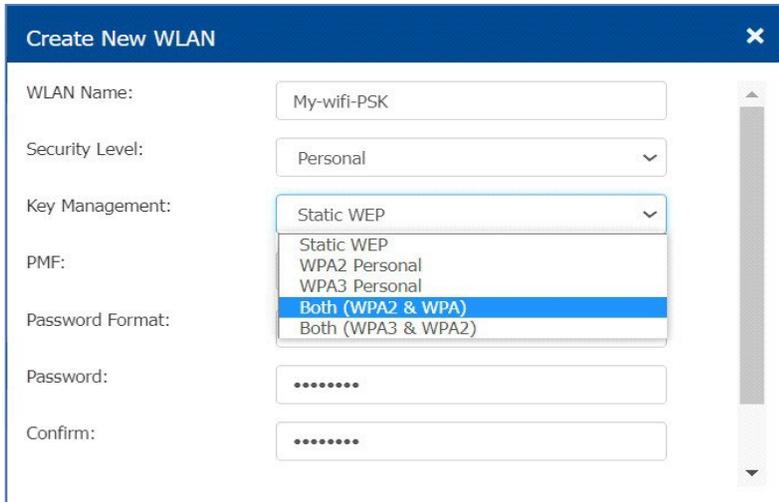


图 40: 创建 Personal 类型的 WLAN

- ▶ **Static WEP:** 使用相同的密钥对所有通信进行加密和解密，因此称为 Static WEP，Static WEP使用静态密钥对加密数据包，密钥可以是128位或256位长，取决于网络管理员选择的配置；与WPA/WPA2/WPA3-Personal不同，Static WEP使用较弱的加密算法，容易被破解。因此，在一些对安全性要求较高的无线网络中，不建议使用Static WEP加密。
- ▶ **WPA2 Personal:** 使用基于密码的加密技术，属于WPA2加密协议的个人模式，主要设计用于满足那些无法承担IEEE 802.1X验证服务器成本和复杂度的家庭和小型公司网络的需求，WPA2采用动态密钥加密数据包，每个无线网络设备使用256位密钥对网络流量进行加密，该密钥通常由8到63个ASCII字符组成。此外，WPA2还支持“四次握手”的过程，在此过程中，客户端和接入点在连接期间进行四次握手以增强安全性。
- ▶ **WPA3 Personal:** 是WPA2（WiFi Protected Access version 2）的后续版本，由Wi-Fi联盟于2018年发布。WPA3-Personal采用了更强大的安全加密算法，能够抵御字典攻击。它使用了一种安全的认证方式SAE（Simultaneous Authentication of Equals）和基于密码的身份验证并可以抵御字典攻击。相比之前的TKIP（Temporal Key Integrity Protocol）和WPA2使用的加密算法，WPA3-Personal更难被破解，从而提高了数据传输的安全性。

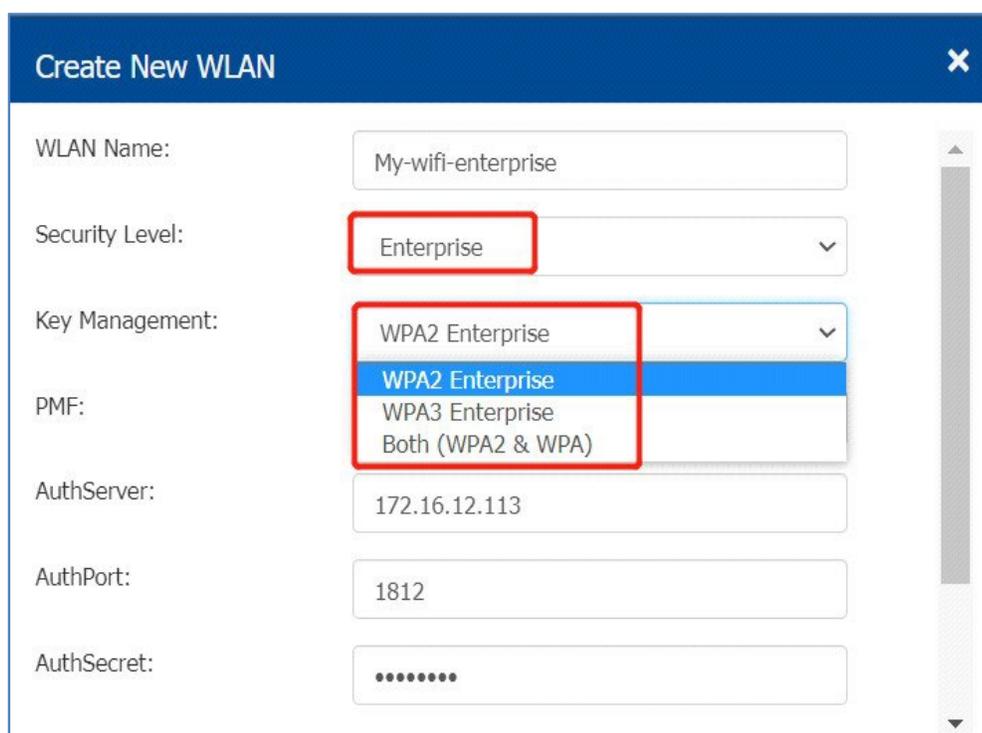
WPA、WPA2、WPA3采用动态密加密数据包，每个无线网络设备使用256位密钥对网络流量进行加密，该密钥通常由8到63个ASCII字符组成，在该模式下，每个无线用户都需要输入预先配置好的相同密钥才能接入网络，该密钥通常由8到63个ASCII字符组成。

- ▶ **Both (WPA2 & WPA):** 同时支持WPA和WPA2两种安全标准。
- ▶ **Both (WPA3 & WPA2):** 同时支持WPA2和WPA3两种安全标准。

6.2.4 安全类型Enterprise

Enterprise也称为IEEE 802.1x认证，它是建立在IEEE 802.1X认证框架上的一种加密方式，要求用户使用个人证书或用户名/密码进行身份验证，并使用AES加密算法进行数据传输加密，以提供更高级别的安全性。相比**Personal**的认证模式，**Enterprise**模式提供了更强大的安全性和更灵活的部署选项。它支持各种类型的EAP（Extensible Authentication Protocols），适用于企业和公共场所的无线网络的安全部署。

Enterprise模式需要RADIUS身份验证服务器进行验证。虽然与**Personal**相比，这些设置要更复杂一些，但它们有助于提供额外的安全性，如防止短密码的字典未经授权访问等。**Enterprise**模式下，支持WPA、WPA2、WPA3三种安全标准或采取组合的方式：



The screenshot shows a 'Create New WLAN' configuration window. The 'WLAN Name' field contains 'My-wifi-enterprise'. The 'Security Level' dropdown menu is set to 'Enterprise'. The 'Key Management' dropdown menu is open, showing three options: 'WPA2 Enterprise' (which is selected and highlighted in blue), 'WPA3 Enterprise', and 'Both (WPA2 & WPA)'. The 'AuthServer' field contains '172.16.12.113', the 'AuthPort' field contains '1812', and the 'AuthSecret' field is masked with dots. A red box highlights the 'Enterprise' dropdown and the 'Key Management' dropdown menu.

图 41：创建一个 Enterprise 类型的 WLAN

- ▶ **WPA2-Enterprise:** WPA2-Enterprise是WPA2的一种认证方式，主要用于企业无线网络中，以提供高级别的安全性，在这种模式下，客户端和接入点之间需要进行四次握手以建立安全连接。
- ▶ **WPA3-Enterprise:** WPA3-Enterprise是专门为需要更高安全保护的企业级用户和场景设计的，如金融机构、政府和企业等，可以提供比WPA2 Enterprise更高级别的安全性。
- ▶ **WPA3-Enterprise:** 在WPA2-Enterprise的基础上增加了一种更加安全的可选模式，名为WPA3-Enterprise 192bit。该模式使用192位的Suite-B安全套件，相较于WPA2-Enterprise的128位密钥长度，密钥长度增加至192位，进一步提升了密码防御强度。这意味着即使密码设置的相对简单，也能有效抵抗离线暴力字典攻击等攻击手段，为网络用户提供更高级别的安全性保护。

除了上述的192位加密功能之外，WPA3-Enterprise还具有其他加强安全性能的特点。例如在握手过程中使用了WPS2（Wi-Fi Protected Setup version 2）技术，这使得它不易受到像KRACK这样的攻击。它还对用户猜测密码的次数进行了严格限制，以防止密码破解等安全风险。此外WPA3-Enterprise还具备Easy Connect功能，简化了智能家居设备的配对过程，并支持Enhanced Open，以使设备的连接更加安全便捷。这些特点使得WPA3-Enterprise在保护网络安全方面具有更高级别的能力。

- ▶ **Both (WPA2 & WPA):** 同时支持WPA和WPA2两种安全标准。

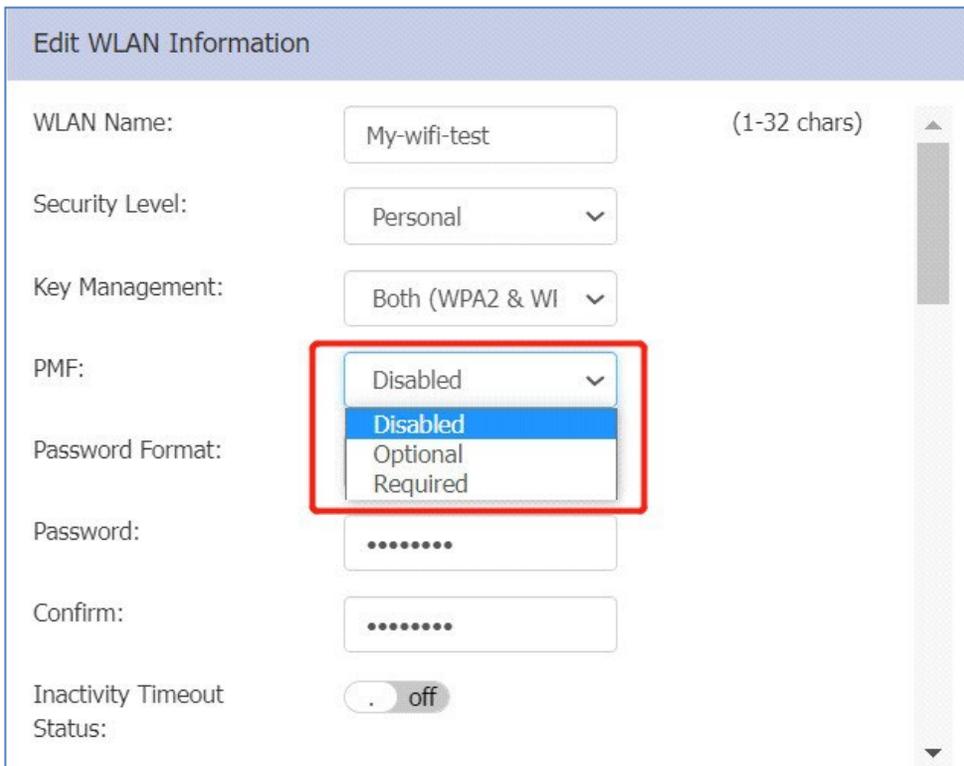
6.3 WLAN的相关参数介绍

对于不同客户的使用场景以及特定的客户需求，可以在WLAN中配置不同的参数。当创建一个新的WLAN或编辑一个已经存在的WLAN时，请根据以下介绍来配置参数。

► PMF

DAP847-XXA设备支持IEEE802.11w标准，也称为PMF(Protected Management Frames)。PMF通过提供管理帧的数据加密来增强DAP的安全性，适用于WPA2和WPA3加密方式。在WLAN网络中，管理帧不加密可能导致安全问题，如黑客窃取AP和用户之间通信的管理帧信息，以及黑客仿冒AP或用户发送虚假请求，使合法用户下线。PMF功能保护了管理帧和一组稳健的管理帧，防止伪造和重放攻击。

PMF功能有两种模式：非强制方式和强制方式。在非强制方式下，无论终端是否支持PMF，都可以接入DAP847-XXA，DAP847-XXA仅对支持PMF的终端的管理帧进行加密保护。在强制方式下，DAP847-XXA只允许支持PMF的终端接入。



The image shows a configuration interface titled "Edit WLAN Information". It contains several fields for configuring a WLAN:

- WLAN Name: My-wifi-test (1-32 chars)
- Security Level: Personal
- Key Management: Both (WPA2 & WI)
- PMF: Disabled (highlighted in blue, circled in red)
- Password Format: (dropdown menu with options Disabled, Optional, Required)
- Password: (masked with dots)
- Confirm: (masked with dots)
- Inactivity Timeout Status: off

图 42: WLAN 中 PMF 的配置

参数	描述
Disable	禁用WLAN的IEEE 802.11w PMF功能，缺省为Disable状态。
Optional	支持IEEE 802.11w PMF的客户端和不支持IEEE 802.11w PMOF的客户端都可以连接到WLAN。
Required	只有支持IEEE 802.11w PMF的客户端才能够连接到WLAN。

注意：对于WPA3 Enterprise企业身份验证，PMF会强制设置为“Required”，这意味着只有具有PMF功能的客户端才能连接。

► Inactivity Timeout



图 43: Inactivity timeout 配置

参数	描述
Inactivity Timeout Status	指不活动超时状态。这个状态通常与连接的终端设备的活动状态有关。在特定的间隔内，如果终端设备没有与DAP847-XXA设备进行任何通信，那么DAP847-XXA设备就会认为该设备处于不活动的状态。在该状态下，无线客户端设备的连接会被断开，以节省网络资源。
Inactivity Timeout Interval	不活动超时间隔。缺省值为600秒，可配置的范围为60秒到12000秒。

► Enable/Hidden

The screenshot shows the 'Create New WLAN' configuration interface. It includes fields for Password, Confirm, Inactivity Timeout Status (set to 'off'), and Inactivity Timeout Interval (set to 600). The 'Enable' option is selected as 'Yes' and the 'Hidden' option is selected as 'No'. Other options include Multicast (set to 'No'), ARP Proxy (set to 'Yes'), and Band (checked for 2.4GHz and 5GHz).

图 44： 开启或隐藏 WLAN

参数	描述
Enable	表示是否使能该WLAN。选择“ Yes ”代表该WLAN处于使能状态，而选择“ No ”则表示 WLAN目前未使能状态。
Hidden	表示是否将该WLAN设置为“Hidden”状态，即指定WLAN对客户端是否可见。出于安全考虑，有些用户可以选择隐藏SSID，这样无线网络就不会被搜索到，需要手动设置SSID才能进入相应的网络。选择“ Yes ”代表WLAN对无线客户端不可见，而选择“ No ”表示客户能够扫描到该WLAN。

需要注意的一点，隐藏SSID虽然可以提高网络的安全性，但也会影响到网络的可访问性，因为一旦无线网络被隐藏，其他设备就无法发现并连接该网络，除非它们已经知道该网络的名称和密码。

► Multicast

即组播转单播，在无线网络中，组播报文会使用最低速率发送广播报文，这会相对较多地消耗信道空口资源，从而影响到整个无线网络性能和应用。而且，组播报文在2层并没有得到确认，会导致丢包严重，影响视频质量，开启组播转单播功能后，DAP847-XXA通过侦听用户上报的组播报告报文和离开报文来维护组播转单播表项。当DAP847-XXA向客户端发送组播报文时，根据组播转单播表项，将组播数据报文转换为单播数据报文，从而提高组播数据流传输效率。

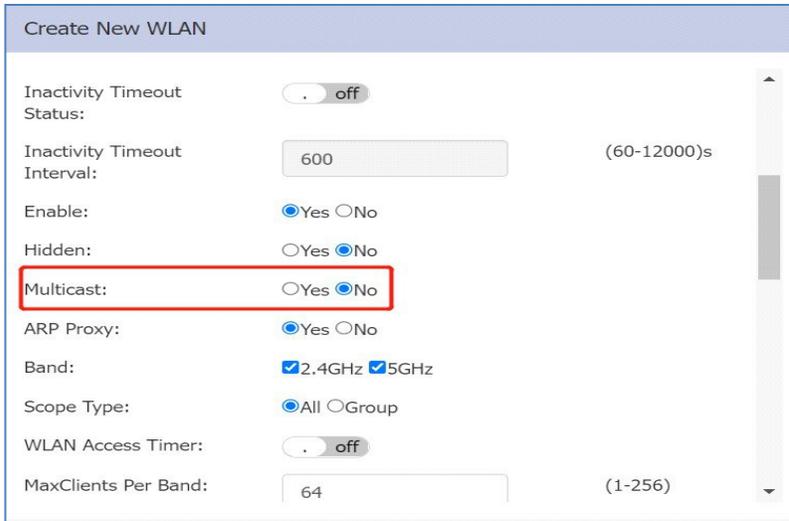


图 45: Multicast 配置

此外，开启组播转单播自适应功能后，当组播转单播出现空口性能瓶颈时，**DAP847-XXA**自动将终端数最少的组播组切换为组播模式，当空口性能改善持续一段时间后，**DAP847-XXA**自动将终端数最多的组播组切换为单播模式，从而保证在不需要人工干预的情况下，自动调整空口性能，提升整体无线用户体验。

- ▶ **ARP Proxy:** ARP Proxy 是一种 WLAN 中常用的网络技术，用于帮助解决 IP 地址和 MAC 地址的映射问题，如果有来自于有线侧发给无线客户端的 ARP 请求，**DAP847-XXA** 将会代表无线客户端响应该 ARP 请求，而不是直接转发给客户端，这要操作的目的是减少在空口中 ARP 报文的转发以此来提高无线性能。

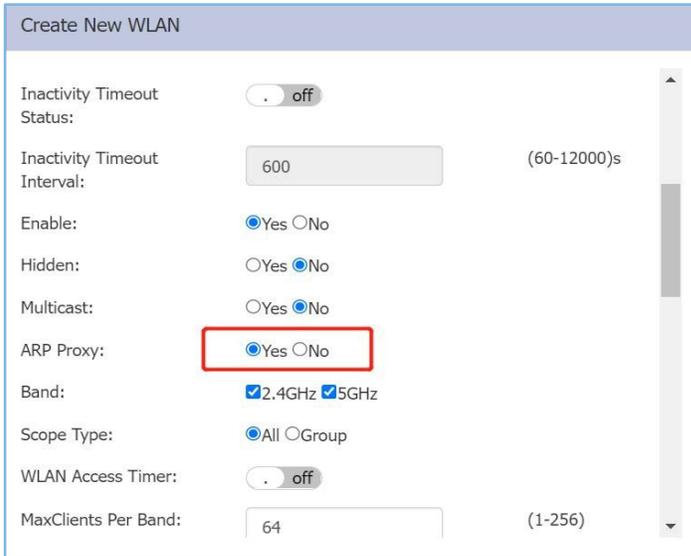


图 46: ARP proxy 配置

注意： DAP847-XXA不充当免费ARP的ARP代理。如当客户端通过DHCP或DHCP release中获得IP地址时，将发送免费的ARP数据包，此时DAP847-XXA不会对这个特殊的ARP数据包做出响应并正常广播。

- ▶ **Band:** 该 WLAN 的工作频段，可以将频段设置为 2.4 GHz、5 GHz 或同时支持这两个频段。默认情况下是同时 2.4 GHz 和 5 GHz 这两个频段。

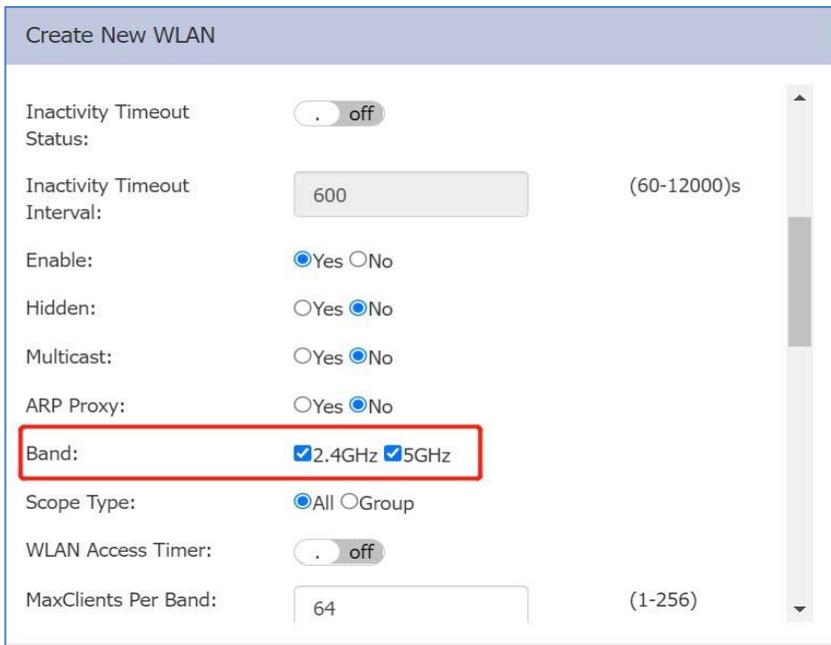


图 47: Band 配置

- **Scope Type:** Scope Type 用来指定该 WLAN 在集群中的 DAP847-XXA 上应用的范围，即哪些 DAP847-XXA 设备会广播这个 WLAN。

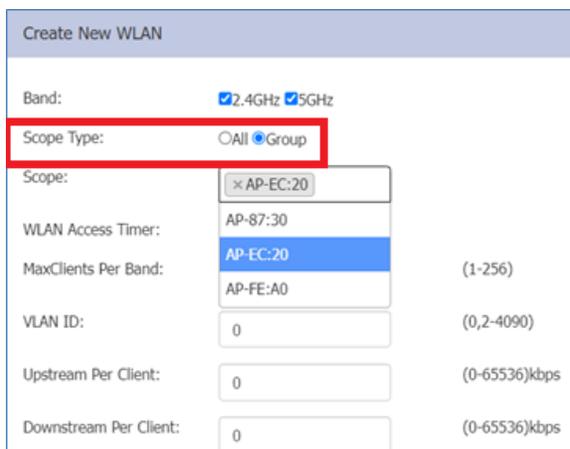


图 48: Scope Type 和 Scope 配置

参数	描述
All	该WLAN的配置将下发到集群中所有DAP847-XXA上。
Group	该WLAN的配置会下发到集群里选定的DAP847-XXA组中。

► WLAN Access Timer

指定WLAN的工作周期，DAP847-XXA仅在此期间内启用该WLAN。默认情况下，WLAN Access Timer处于“Off”状态。如果是“Off”状态，DAP847-XXA将一直释放该WLAN信号，如图 49所示。如果是“On”状态，在该WLAN之前会显示一个计时器图标，如图 50所示。

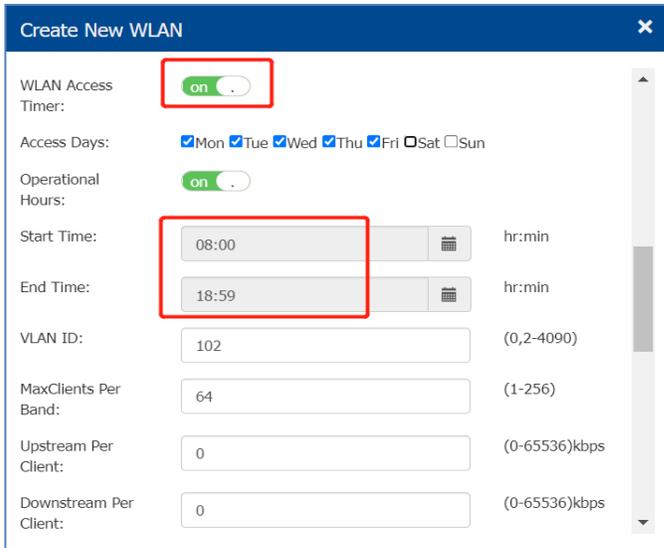


图 49: WLAN access timer 配置

参数	描述
Access Days	在一周内指定的某几天会启用或禁用该WLAN。
Operational Hours	在每天内启用或禁用WLAN的时间。
Start Time	启用WLAN的时间。
End Time	禁用WLAN的时间。

注意： 在配置参数之前，请正确配置系统时间和时区，如果系统时间和时区不正确，可能会导致WLAN无法在预期的时间内工作。

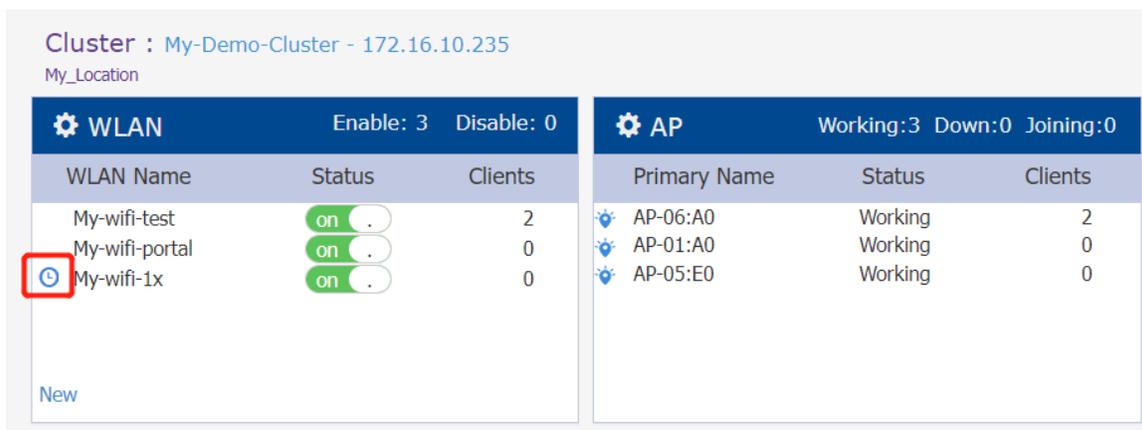


图 50: WLAN Access Timer 标识

- ▶ **VLAN ID:** 表示该 WLAN 将用户的业务流量映射到对应的 VLAN，如果配置了 WLAN-VLAN 绑定，则会在 DAP847-XXA 中创建对应的网桥接口处理用户的流量转发。

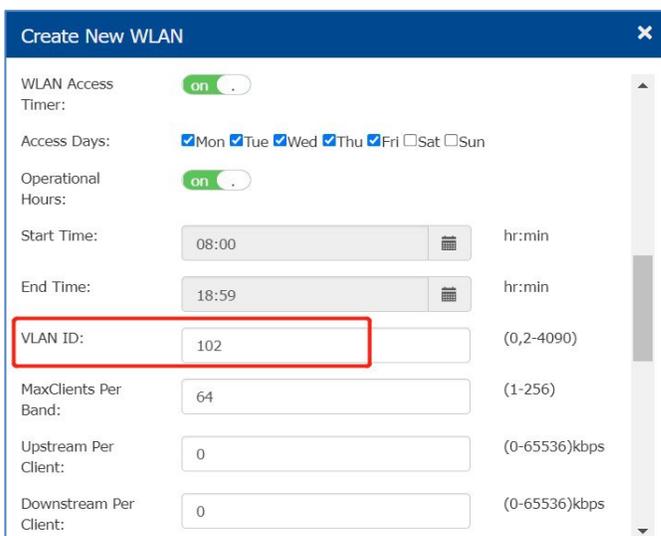


图 51: VLAN ID 配置

您可以在CLI下使用命令“brctl show”来检查VLAN的配置。

```
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:~$
```

图 52: 在 CLI 下检查 VLAN 的配置

- ▶ **MaxClients Per Band:** 指定可以为该 WLAN 上的每个 BSSID 配置的最大允许连接的客户端数量。根据实际使用的需要，可配置的范围为 1 到 256，其默认值为 64。当连接到 AP 的客户端达到最大数量时，DAP847-XXA 将忽略来自新客户端的身份验证请求，新的客户端将无法连接到该 WLAN。

The screenshot shows the 'Create New WLAN' configuration interface. The 'MaxClients Per Band' field is highlighted with a red box and contains the value '64'. Other visible settings include: Band (2.4GHz and 5GHz checked), Scope Type (All selected), WLAN Access Timer (off), VLAN ID (0), Upstream Per Client (0), Downstream Per Client (0), Client Isolate (off), 802.11r (off), and 802.11v (on).

图 53: MaxClients per band 配置

- ▶ **Upstream Per Client:** 表示配置的无线客户端的最大上行带宽，单位为 kbps，可配置的范围为 0 ... 65536，其中 0 代表未配置客户端流量限速。
- ▶ **Downstream Per Client:** 表示配置的无线客户端的最大下行带宽，单位为 kbps，可配置的范围为 0 ... 65536，其中 0 代表未配置客户端流量限速。

The screenshot shows the 'Create New WLAN' configuration interface with 'Upstream Per Client' and 'Downstream Per Client' fields highlighted by a red box. The 'Upstream Per Client' field is set to '10240' and the 'Downstream Per Client' field is set to '20480'. Other visible settings include: WLAN Access Timer (off), MaxClients Per Band (64), VLAN ID (0), Client Isolate (off), 802.11r (off), 802.11v (on), 802.11k (on), and UAPSD (on).

图 54: Clients 流量限速配置

- **Client Isolate:** 客户端隔离功能，指连接到同一个 WLAN 的客户端不允许相互通信，客户端只能与上行网关通信。

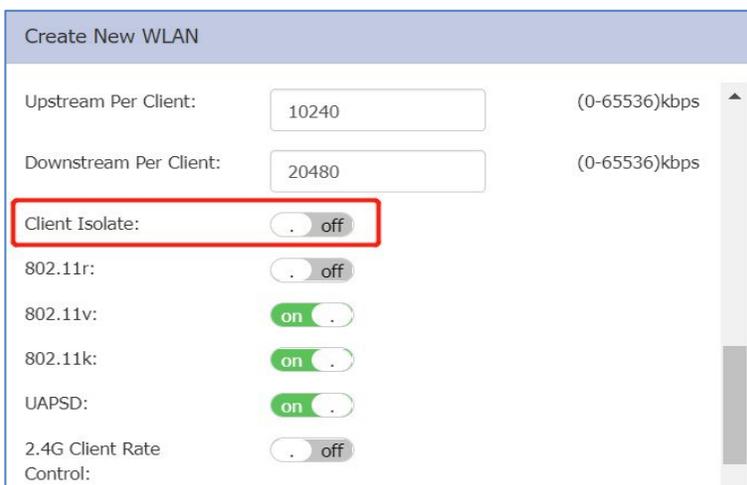


图 55: Client isolate 配置

- **802.11r:** 启用“快速 BSS 转换”机制，以最大限度地减少客户端从同一集群中的一个 BSS 转换到另一 BSS 时的延迟。在 IEEE 802.11r 协议中，提出了三层密钥的结构和计算方法，而传统的 RSN（无线网络安全标准）则是两层密钥结构。RSN 通过认证者（DAP847-XXA）和申请者（无线客户端）共享的 PMK 进行展开，获得组临时密钥(GTK)和 PTK。IEEE 802.11r 则将密钥管理分为三层，三层密钥分别为 PMK_R0，PMK_R1，PTK。PMK_R0 和 PMK_R1 的计算是 IEEE 80211r 特有的。此外，IEEE 802.11r 协议还着眼于减少漫游时认证所需的时间，这将有助于支持语音等实时业务的应用。



图 56: 802.11r 配置

- ▶ **802.11k/v:** DAP847-XXA 在默认情况下，IEEE 802.11k 和 IEEE 802.11v 都处于启用状态。两者都与“Roaming RSSIThreshold”协同工作，在实际应用中，IEEE 802.11k/v 可以优化移动设备在 WLAN 网络中的漫游性能和安全性。漫游优化主要取决于客户端在漫游过程中的行为。

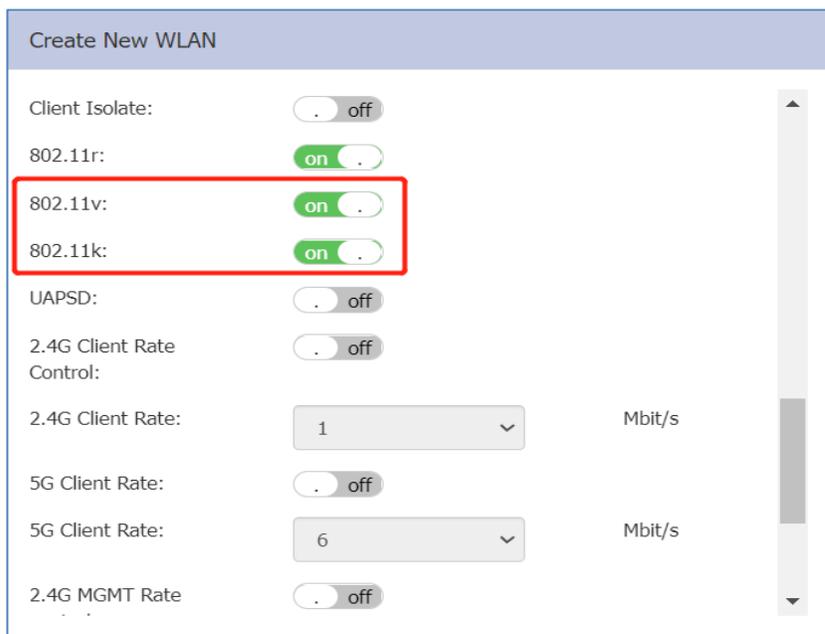


图 57: 802.11k/v 配置

- ▶ 当在WLAN上启用IEEE 802.11k和IEEE 802.11v功能时，“Roaming RSSI Threshold”将触发DAP847-XXA和无线客户端之间的IEEE 802.11k和IEEE 802.11v消息交换。
- ▶ 当DAP847-XXA检测到无线客户端设备的SNR值低于“Roaming RSSI Threshold”时，它会向该无线客户端设备发送一个IEEE 802.11k事件。如果该设备是支持IEEE 802.11k的设备，则该设备将使用包含来自该设备的RF扫描信息的数据包来响应DAP847-XXA。
- ▶ 基于接收到的数据，DAP847-XXA将会计算该设备漫游的最佳BSSID，然后通过IEEE 802.11v事件向该无线客户端设备发送最佳SSID信息。
- ▶ 最后，该无线客户端设备将选择是否进行漫游。如果设备漫游，它将选择是在DAP847-XXA发送的IEEE 802.11v事件中获取一个目标BSSID，还是选择在DAP847-XXA推荐范围外的另一个BSSID进行漫游。

- ▶ **OKC:** OKC（Opportunistic Key Caching）功能是一种加密技术，它允许无线设备在连接到一个新的 AP 时，使用之前已经缓存的 PMK（Pairwise Master Key）来进行连接，而不需要再次进行完整的 IEEE 802.1X 认证。

OKC 主要是为了解决在快速漫游（Roaming）过程中，由于需要频繁地进行 IEEE 802.1X 认证而导致的网络延迟和性能问题。它通过在设备之间缓存 PMK，使得设备在漫游时能够更快地连接到新的 AP。当无线客户端（Station）连接到一个新的 AP 时，如果该 AP 支持 OKC 功能，STA 会根据之前已经缓存的 PMK 和 AP 的 SSID 等信息，计算出一个新的 PMK 并存储在 PMKSA Cache 中。这样，下一次连接时，STA 就可以直接使用这个缓存的 PMK 来进行连接，而不需要再次进行 IEEE 802.1X 认证。

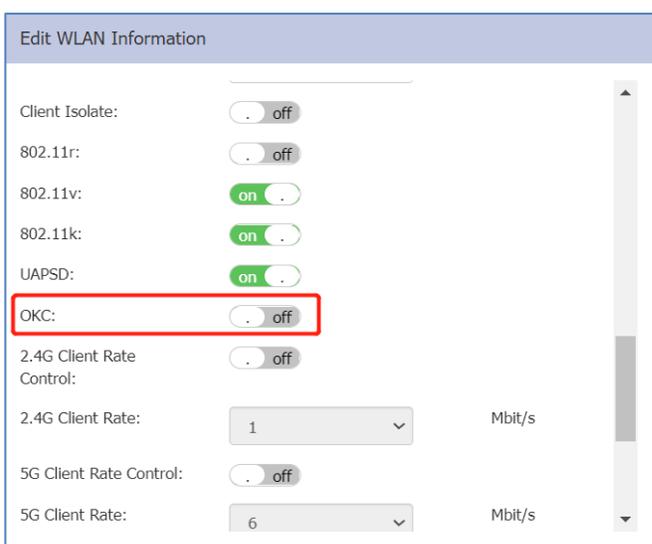


图 58: OKC 配置

- ▶ **UAPSD:** Unscheduled Automatic Power Save Delivery（UAPSD）定义了 IEEE 802.11e 中的服务质量（QoS），是一种 Wi-Fi 节能服务，它用于管理 Wi-Fi 设备的电源。这种节能服务能够延长 Wi-Fi 设备的电池寿命,此外，还降低了通过无线媒体传输的流量的延迟。UAPSD 不需要客户端去轮询在 DAP847-XXA 缓冲的每个数据包,它通过发送单个上行链路触发数据包来确保多个下行链路数据包的传递。

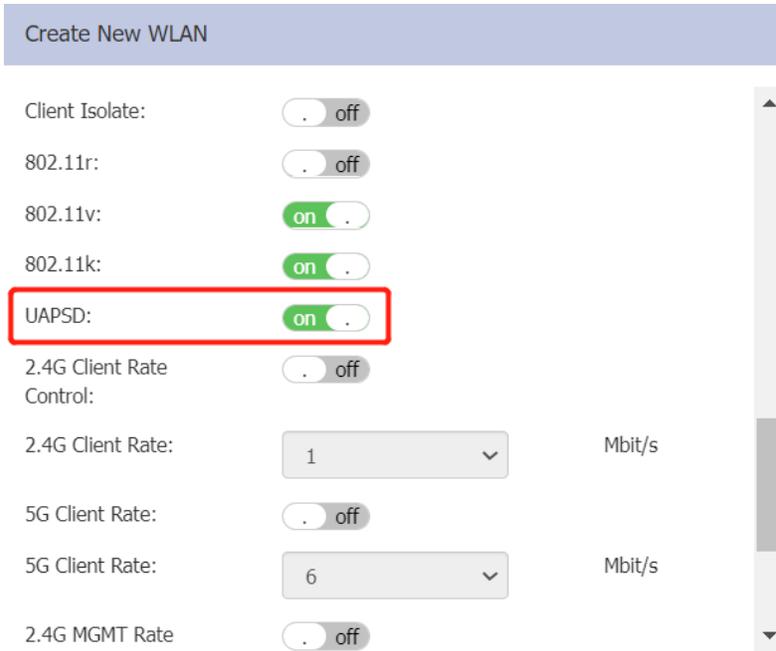


图 59: UAPSD 配置

- ▶ **2.4G Client Rate Control:** 根据客户端数据速率启用或禁用 2.4 GHz 频段访问控制，如图 60 所示。默认状态为 Off。
- ▶ **2.4G Client Rate:** 数据速度较低的 2.4 GHz 频段客户端将不允许访问 DAP847-XXA。推荐值为 12Mbit/s，如图 60 所示。数据帧速率控制的主要目的是优化 WLAN 的性能和稳定性。如果管理帧的发送速率过低，可能会导致过多的干扰和拥塞，从而影响 WLAN 的性能和稳定性。
- ▶ **5G Client Rate Control:** 根据客户端数据速率启用或禁用 5 GHz 频段访问控制，如图 60 所示。默认状态为 Off。
- ▶ **5G Client Rate:** 数据速度较低的 5 GHz 频段客户端将不允许访问 DAP847-XXA。推荐值为 24Mbit/s，如图 60 所示。数据帧速率控制的主要目的是优化 WLAN 的性能和稳定性。如果管理帧的发送速率过低，可能会导致过多的干扰和拥塞，从而影响 WLAN 的性能和稳定性。

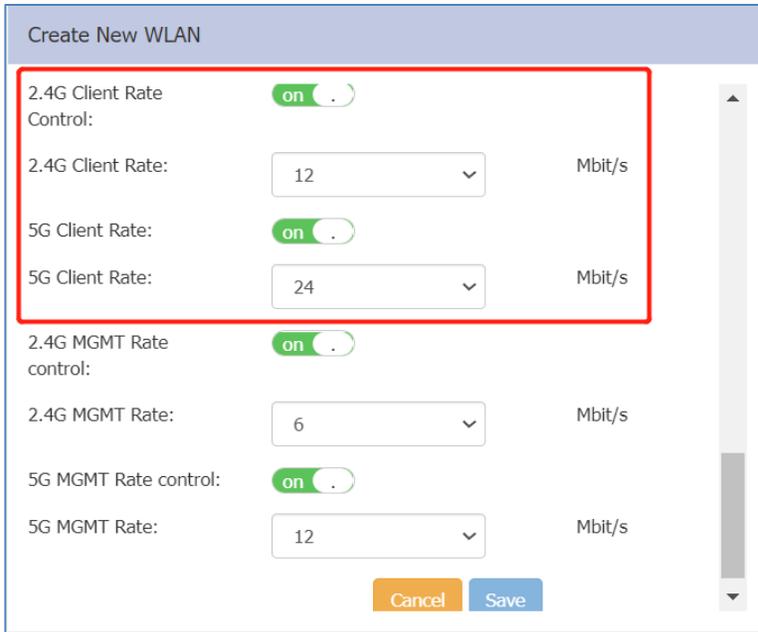


图 60: Client Rate 配置

- ▶ **2.4G MGMT Rate Control:** 启用或禁用 2.4 GHz 频段无线管理帧速率控制，如图 61 所示。默认情况下，它处于 Off 状态。
- ▶ **2.4G MGMT Rate:** 2.4 GHz 频段无线管理帧的传输速率，如图 61 所示，值越高，代表覆盖范围越小，值越低，代表覆盖范围越大。管理帧速率控制的主要目的是优化 WLAN 的性能和稳定性。如果管理帧的发送速率过低，可能会导致过多的干扰和拥塞，从而影响 WLAN 的性能和稳定性。
- ▶ **5G MGMT Rate Control:** 启用或禁用 5 GHz 频段无线管理帧速率控制，如图 61 所示，默认情况下，该功能处于 Off 状态。
- ▶ **5G MGMT Rate:** 5 GHz 频段无线管理帧的传输速率，如图 61 所示，值越高，代表覆盖范围越小，值越低，代表覆盖范围越大。管理帧速率控制的主要目的是优化 WLAN 的性能和稳定性。如果管理帧的发送速率过低，可能会导致过多的干扰和拥塞，从而影响 WLAN 的性能和稳定性。

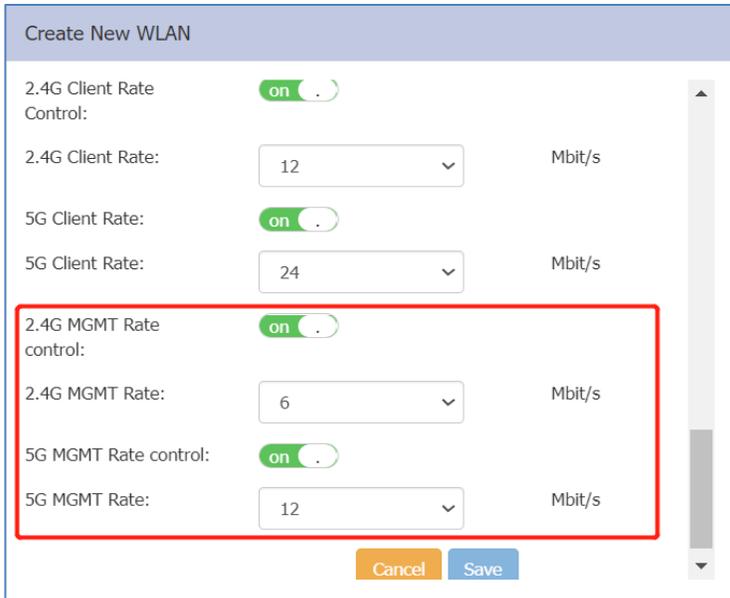


图 61: 修改 2.4 GHz/5 HzG 的 Management Rate

- ▶ **DTIM Interval:** DAP847-XXA 发送 DTIM (Delivery Traffic Indication Message) 的时间间隔，用于通知无线客户端何时需要接收数据，以避免客户端设备在无数据接收时保持不必要的唤醒状态。增加 DTIM Interval 能够更有效地节省终端设备的电量，但会增加接入点的缓存占用和引入一定的传输延迟。因此，DTIM 间隔的配置应根据实际使用场景进行正确设置。在默认情况下，DTIM 周期参数为 1，如图 62 所示。

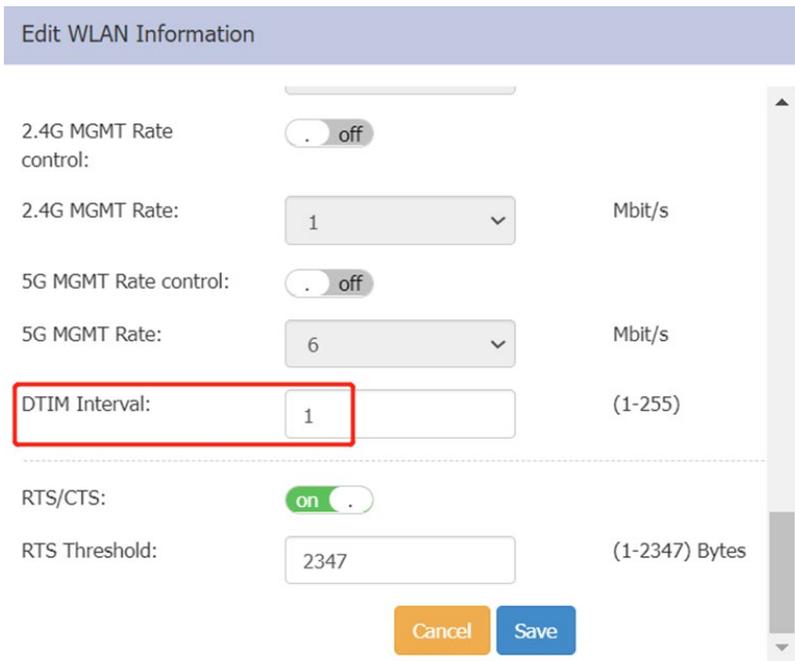


图 62: 修改 DTIM Interval

- ▶ **RTS/CTS:**用此功能后，DAP847-XXA 将发送 RTS（Request to Send，请求发送）和 CTS（Clear to Send，允许发送）帧。这有助于发现网络中的隐藏节点，从而减少因隐藏节点造成的发包冲突，这类冲突可能会导致数据包重传次数增加或数据包丢失。具体配置参考图 63。
- ▶ **RTS Threshold:** 该参数的可设置范围为 1 ... 2347 Bytes。默认情况下，此功能是关闭的。当 DAP847-XXA 需要发送一个超过该阈值的数据包时，它会首先发送一个 RTS 信号以通知接收方，这样做是为了预防信号冲突。具体配置参考图 63。

The screenshot shows the 'Edit WLAN Information' configuration interface. It includes several settings: '2.4G MGMT Rate control' (off), '2.4G MGMT Rate' (1 Mbit/s), '5G MGMT Rate control' (off), '5G MGMT Rate' (6 Mbit/s), and 'DTIM Interval' (1 (1-255)). The 'RTS/CTS' setting is highlighted with a red box and is currently 'on'. Below it, the 'RTS Threshold' is set to '2347' Bytes. At the bottom, there are 'Cancel' and 'Save' buttons.

图 63: RTS/CTS 配置

6.4 修改WLAN的配置

在**WLAN Configuration**页面中，您可以通过单击“”按钮来修改WLAN的配置。该WLAN的详细参数将显示在WLAN配置页面的右侧。

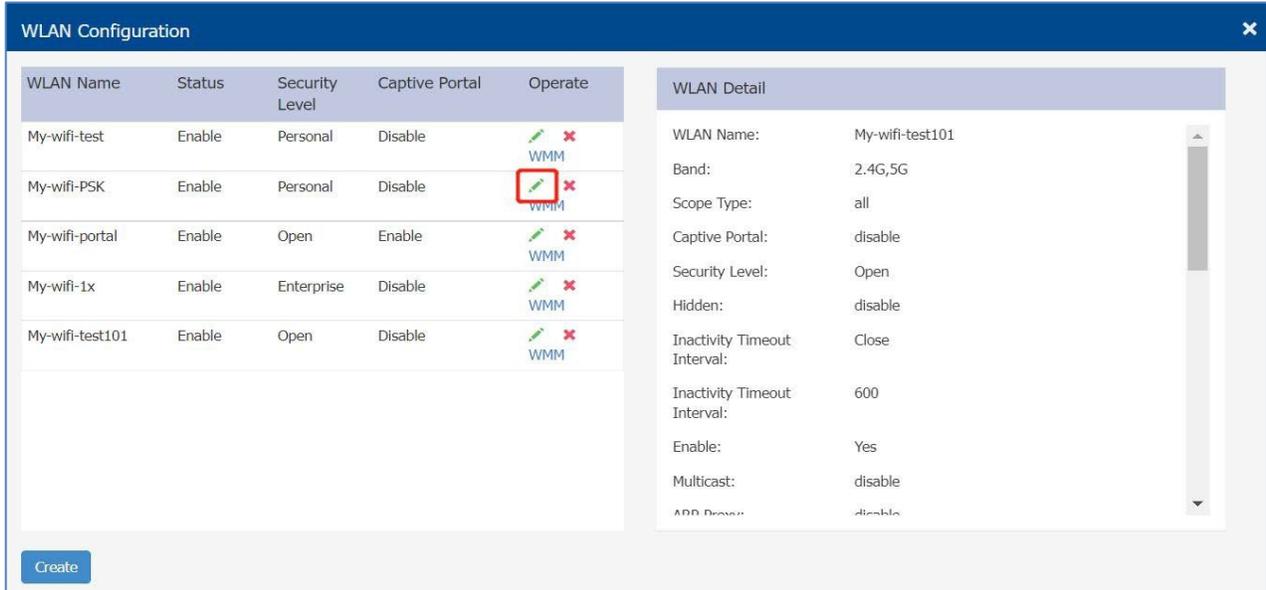


图 64：修改 WLAN 配置

- 单击“**Cancel**”按钮取消对该配置的修改。
- 单击“**Save**”按钮来保存配置修改。

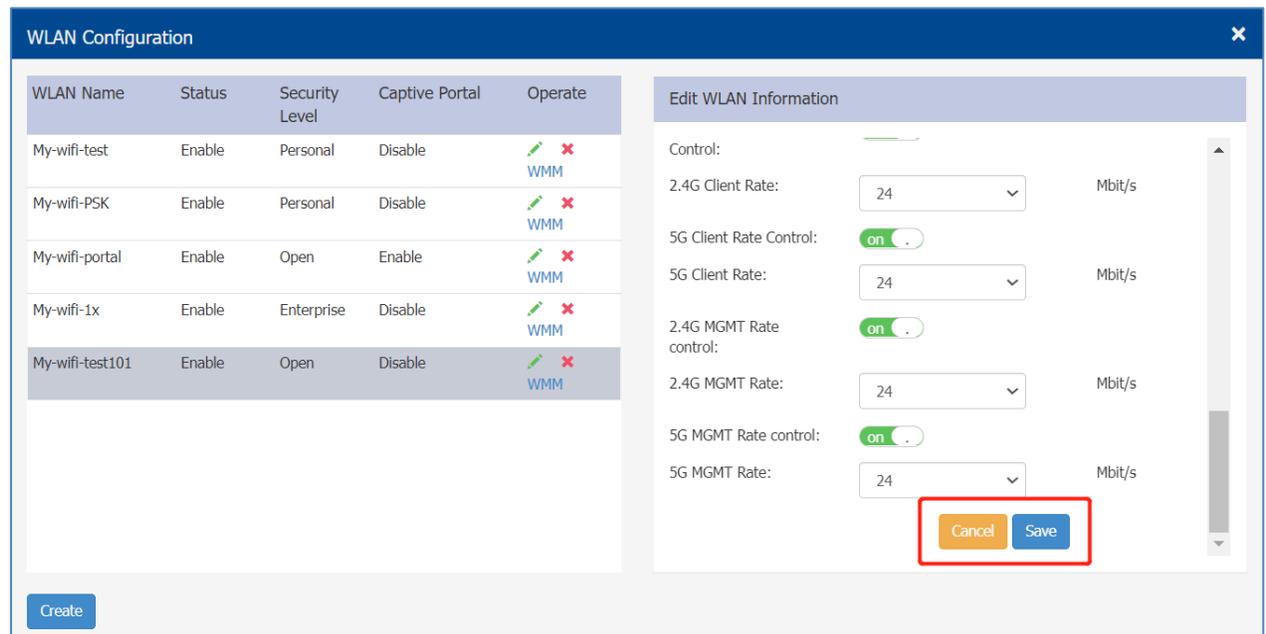


图 65：保存或取消 WLAN 的配置修改

6.5 删除WLAN

在WLAN Configuration页面，单击WLAN后的“x”按钮，可以将对应的WLAN删除。如下图所示。

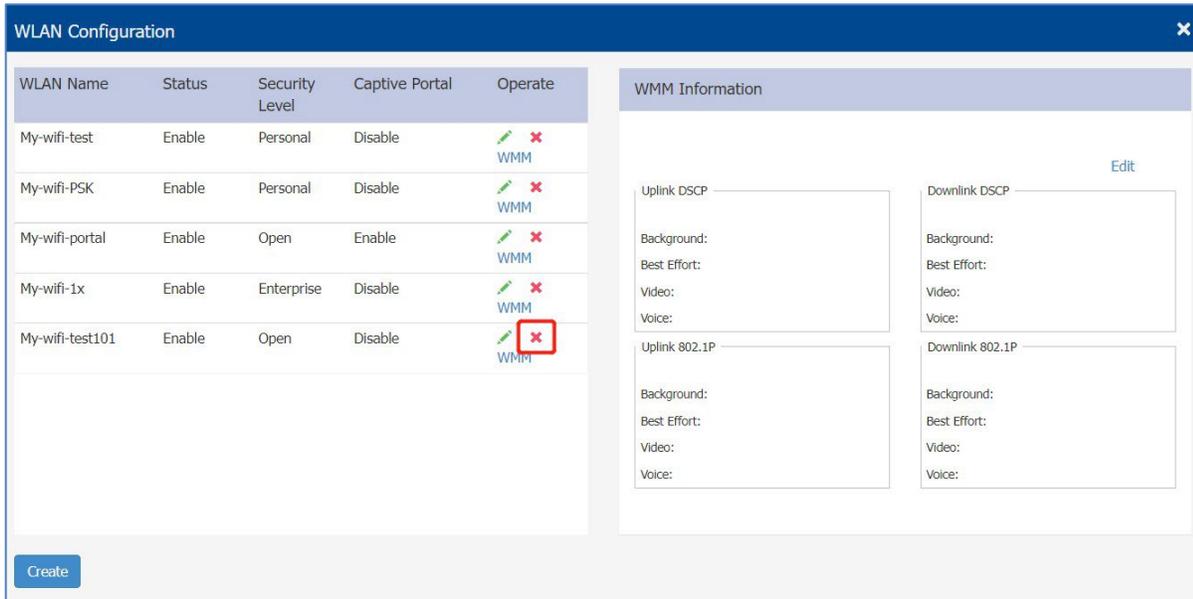


图 66: 删除 WLAN

6.6 WMM配置

WMM（Wi-Fi Multimedia）是基于IEEE 802.11e标准的Wi-Fi联盟互操作性认证，是一种在Wi-Fi网络中实现QoS（Quality of Service）的技术。它能够为数据传输提供不同的优先级，以确保音频、视频和游戏等高带宽应用能够流畅地传输，而不会受到网络拥塞的影响。WMM支持四种不同的AC（Access Category）：

- ▶ **背景类别（Background）**：用于传输后台数据，如电子邮件、网页浏览等，优先级最低。
- ▶ **视频类别（Video）**：用于传输视频流，如在线电影或视频会议等，优先级较高。
- ▶ **语音类别（Voice）**：用于传输音频流，如VoIP电话或语音聊天等，优先级较高。
- ▶ **最佳类别（Best Effort）**：用于传输所有其他数据，如文件传输、网络游戏等，优先级最高。

WMM通过使用WMM标记对数据进行分类和标记，以便在发送到网络之前对其进行优先级排序。在接收端，WMM标记被用来识别数据包的优先级，以便正确地将其传递给相应的应用程序。

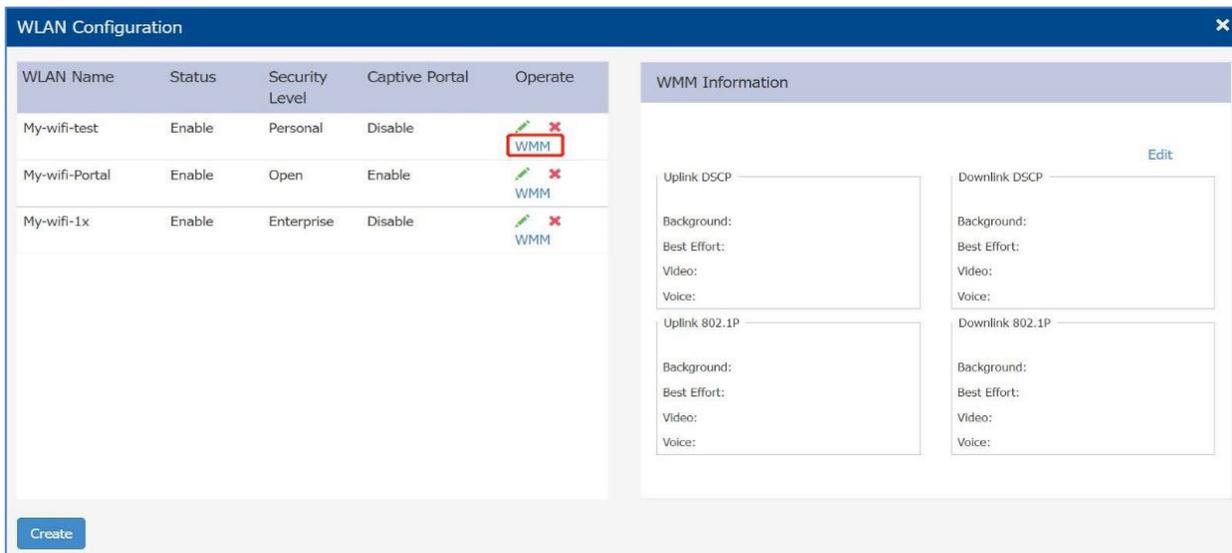


图 67：WMM配置

每个WLAN都可以配置WMM的规则，对于DAP847-XXA上的WLAN，您可以修改DSCP和IEEE 802.1p值以及WMM优先级之间的映射关系。

7 管理DAP847-XXA

本章主要介绍如何在集群中配置和管理DAP847-XXA，以及如何通过Web GUI检查、备份、恢复DAP847的配置以及升级固件等。DAP847-XXA集群解决方案是一种基于无控制器的体系结构。

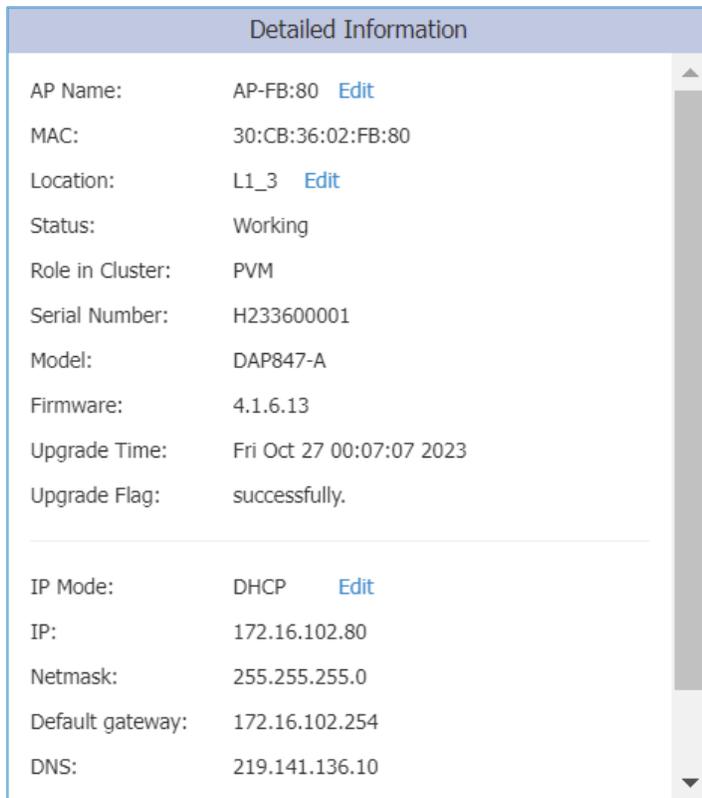
DAP847-XXA之间可以建立一个自治集群，其中有三种类型的角色：PVM、SVM和MEMBER。

本章所描述的DAP847-XXA系统管理主要包括以下内容：

- ▶ [查看DAP847-XXA的详细信息](#)
- ▶ [修改DAP847-XXA的名称和位置信息](#)
- ▶ [添加DAP847-XXA到集群](#)
- ▶ [删除集群中DAP847-XXA](#)
- ▶ [允许DAP847-XXA加入集群](#)
- ▶ [替换DAP847-XXA](#)
- ▶ [修改DAP847-XXA的IP地址](#)
- ▶ [将DAP847-XXA切换为DAC模式](#)
- ▶ [查看DAP847-XXA的当前配置](#)
- ▶ [重启DAP847-XXA](#)
- ▶ [恢复出厂配置](#)
- ▶ [DAP847-XXA的配置备份和恢复](#)
- ▶ [DAP847-XXA固件升级](#)
- ▶ [DAP847-XXA的LED指示灯配置](#)
- ▶ [DAP847-XXA高级配置](#)
- ▶ [配置DAP847-XXA的网络服务](#)

7.1 查看DAP847-XXA详细信息

通过点击列表中的指定的DAP847-XXA设备，在右侧的**Detailed Information**页面中，您可以查看DAP847-XXA的详细信息。您可以在该页面中点击“**Edit**”来修改“**AP Name**”和“**Location**”。

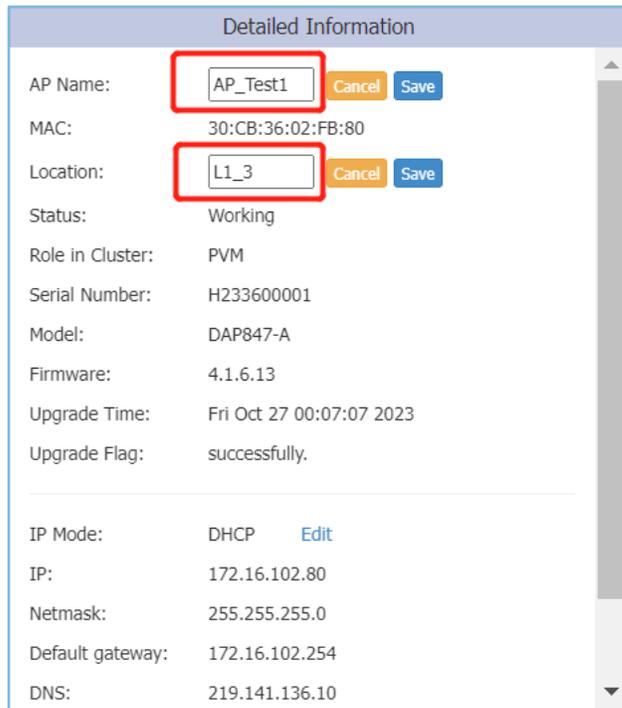


Detailed Information	
AP Name:	AP-FB:80 Edit
MAC:	30:CB:36:02:FB:80
Location:	L1_3 Edit
Status:	Working
Role in Cluster:	PVM
Serial Number:	H233600001
Model:	DAP847-A
Firmware:	4.1.6.13
Upgrade Time:	Fri Oct 27 00:07:07 2023
Upgrade Flag:	successfully.
<hr/>	
IP Mode:	DHCP Edit
IP:	172.16.102.80
Netmask:	255.255.255.0
Default gateway:	172.16.102.254
DNS:	219.141.136.10

图 68: DAP847-XXA 的详细信息

7.2 修改DAP847-XXA的名称和位置信息

- 点击“**Edit**”，修改**AP Name**和**Location**。
- 输入“**AP Name**”和“**Location**”字段以标记特定DAP847-XXA。缺省状态下，DAP847-XXA以“AP”加上其MAC地址的最后2个字节命名，例如AP-FB:80，如下图所示。



Detailed Information	
AP Name:	AP_Test1 Cancel Save
MAC:	30:CB:36:02:FB:80
Location:	L1_3 Cancel Save
Status:	Working
Role in Cluster:	PVM
Serial Number:	H233600001
Model:	DAP847-A
Firmware:	4.1.6.13
Upgrade Time:	Fri Oct 27 00:07:07 2023
Upgrade Flag:	successfully.
<hr/>	
IP Mode:	DHCP Edit
IP:	172.16.102.80
Netmask:	255.255.255.0
Default gateway:	172.16.102.254
DNS:	219.141.136.10

图 69：修改 DAP847-XXA 的 Name 和 Location 信息

7.3 添加DAP847-XXA到集群

■ 操作前的准备工作

在将新DAP847-XXA添加到集群之前，请注意检查以下事项：

- ▶ PVM是正常工作状态。
- ▶ 新添加的DAP847-XXA应使用与集群相同的集群ID。

注意：如果要将一台新的DAP添加到集群，只需要将该AP接入到与cluster同属二层网络即可，同时请确保该AP与其它AP间能够相互通信，即与cluster中的AP间没有隔离。

如果无法对PVM完成操作，请在添加新的DAP847-XXA到集群之前将SVM升级到PVM。

关于集群ID的信息，您可以通过以下两种方式来查看：

- ▶ 登录DAP847-XXA并在System页面中检查“**Cluster ID**”（集群ID）。

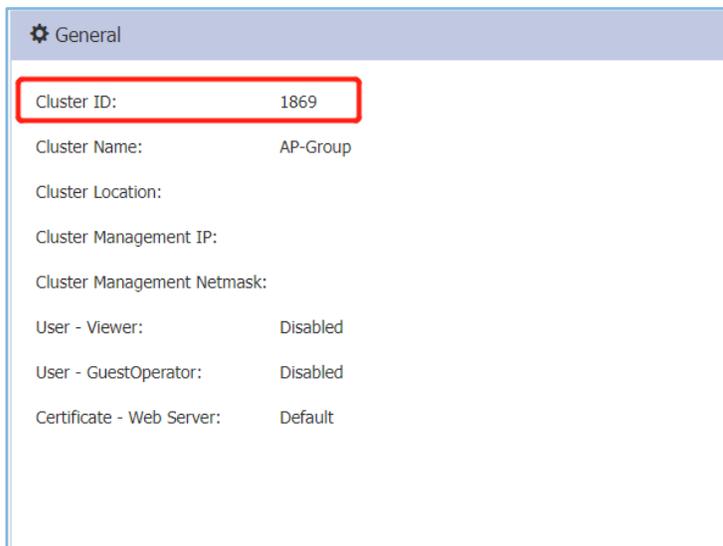


图 70：通过 Web 页面查看集群 ID

- ▶ 通过CLI来查看**Cluster ID**。

```
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:~$ █
```

图 71: 在 CLI 下查看集群 ID

7.4 删除集群中DAP847-XXA

在集群中删除一个DAP847-XXA:

- 从AP集群列表中选择要删除的DAP847-XXA（可以是PVM、SVM或MEMBER）。
- 单击“**Kick Off**”按钮，则选中的DAP847-XXA将被加入到集群的Block列表中。

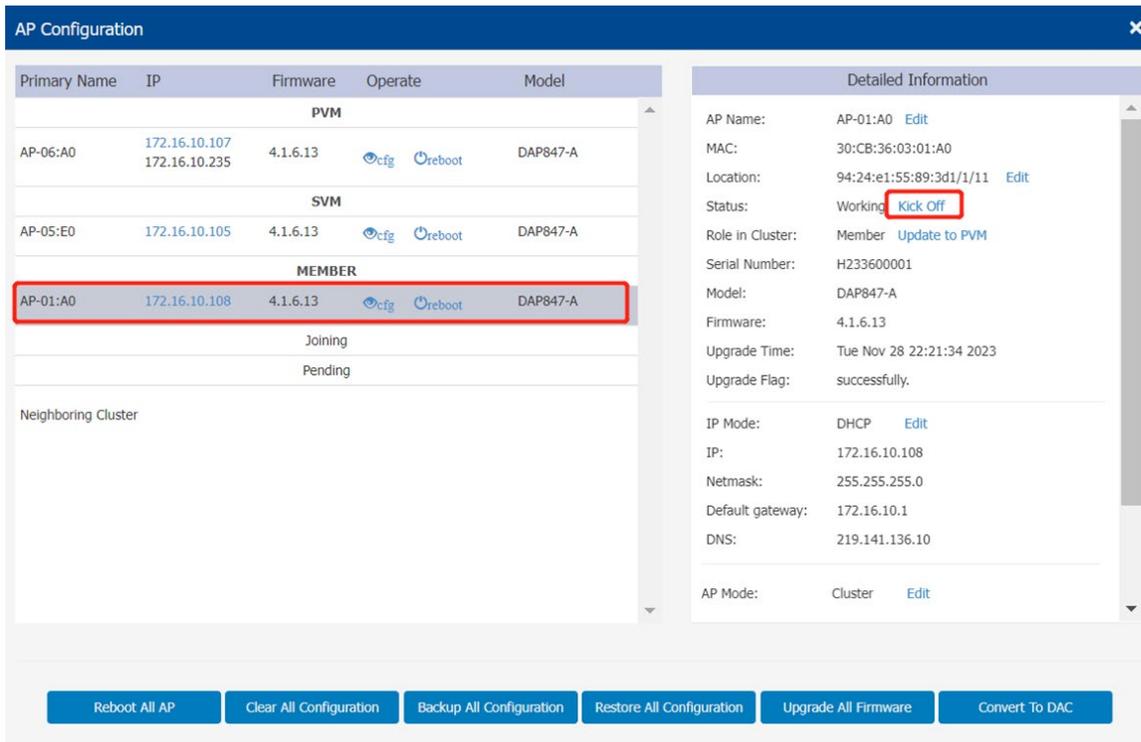


图 72: 在集群中删除 DAP847-XXA

如果该DAP847-XXA已经连接到网络，则其状态将从“**Working**”状态切换到“**Joining**”状态。如果没有经过管理员的授权，则该DAP847-XXA设备不允许再次加入此集群成为集群的成员。

HIRSCHMANN IT AP Group : My-Demo-Cluster
 A **BELDEN** BRAND - 192.168.4.221

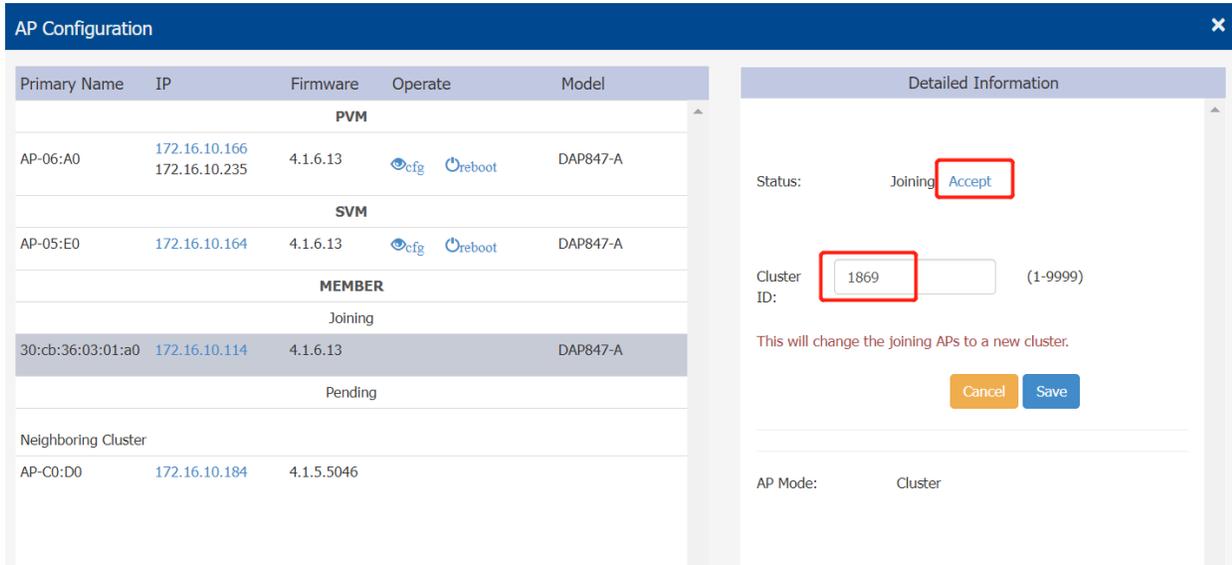
WLAN			AP		
WLAN Name	Status	Clients	Primary Name	Status	Clients
My-wifi-PSK	on <input type="checkbox"/>	0	AP-FE:A0	Working	0
My-wifi-Portal	on <input type="checkbox"/>	0	AP-87:30	Joining	0
My-wifi-1x	on <input type="checkbox"/>	0	AP-EC:20	Working	0

New

图 73: DAP847-XXA 在被删除后进入 “Joining” 状态

7.5 允许DAP847-XXA加入集群

如果处于“Joining”状态的DAP847-XXA在集群的Block列表中，单击“Accept”（接受）按钮和相应的“Cluster ID”（集群ID）能够让该DAP847-XXA重新加入集群并且从集群的Block列表中删除。



The screenshot displays the 'AP Configuration' window. On the left is a table with columns: Primary Name, IP, Firmware, Operate, and Model. The table is divided into sections: PVM, SVM, MEMBER, and Neighboring Cluster. The 'Joining' section is highlighted, showing an AP with MAC address 30:cb:36:03:01:a0 and IP 172.16.10.114. On the right is the 'Detailed Information' panel for this AP, showing its status as 'Joining' with an 'Accept' button. Below this, the 'Cluster ID' is set to 1869, with a note that this will change the joining APs to a new cluster. 'Cancel' and 'Save' buttons are at the bottom of the panel.

Primary Name	IP	Firmware	Operate	Model
PVM				
AP-06:A0	172.16.10.166 172.16.10.235	4.1.6.13		DAP847-A
SVM				
AP-05:E0	172.16.10.164	4.1.6.13		DAP847-A
MEMBER				
Joining				
30:cb:36:03:01:a0	172.16.10.114	4.1.6.13		DAP847-A
Pending				
Neighboring Cluster				
AP-C0:D0	172.16.10.184	4.1.5.5046		

图 74：允许DAP847-XXA重新加入到集群

7.6 替换DAP847-XXA

替换集群中的DAP847-XXA，涉及到如下两个场景：

- ▶ **替换当前的PVM设备**

在断开前一个PVM之前，将SVM升级到PVM。然后用新的DAP替换以前的PVM。

- ▶ **替换SVM或集群中的一个MEMBER**

断开SVM或MEMBER的连接，直接用新的DAP847-XXA完成替换。

7.7 修改DAP847-XXA的IP地址

DAP847-XXA支持从DHCP服务器获取IP地址，同时也支持配置一个静态的IP地址。缺省情况下，IP模式为DHCP。

□ 可以单击“**Edit**”按钮修改IP模式，如图75、图76所示。

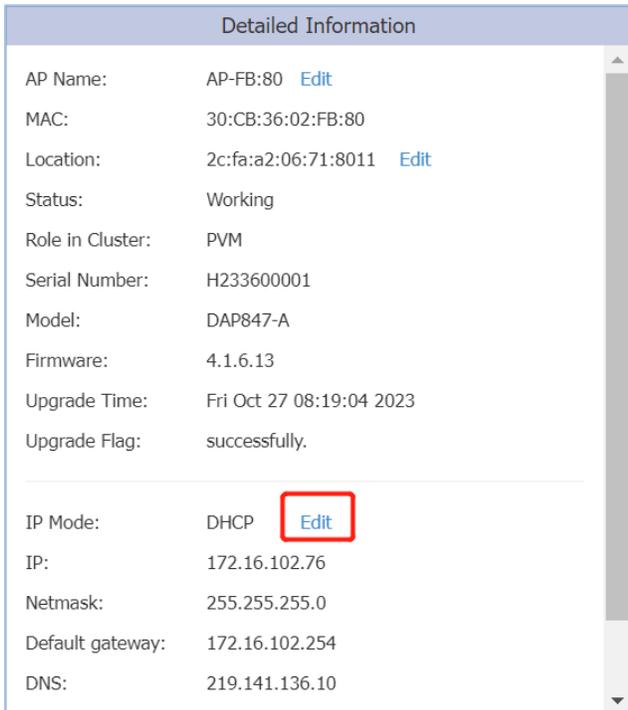


图75: 修改DAP847-XXA的IP模式

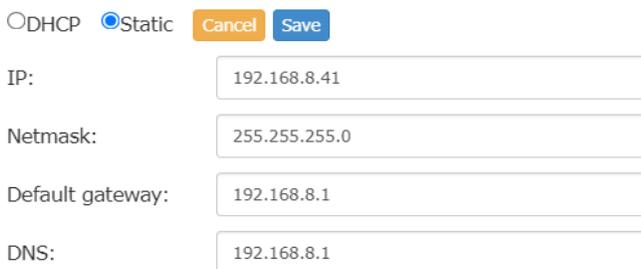


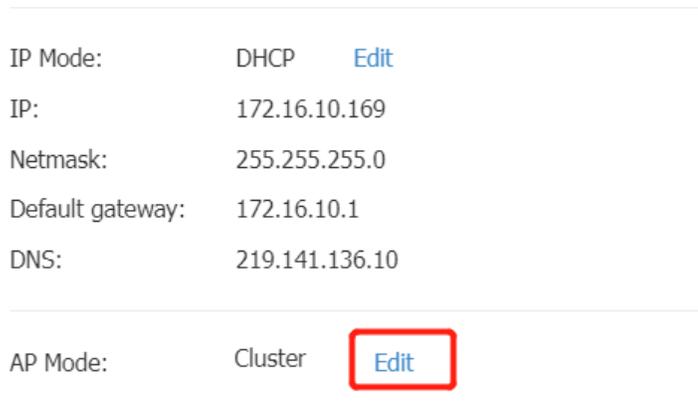
图76: 修改DAP847-XXA的IP地址

7.8 切换DAP847-XXA为DAC模式

根据实际使用场景的需要，DAP847-XXA可以在Web GUI上从集群模式切换为DAC的工作模式。

■ 切换集群中的单台 DAP847-XXA 到 DAC 模式

- 在“**AP Configuration**”页面，选择一台将要切换为DAC模式的DAP847-XXA，在右侧的“**Detailed information**”页面上点击AP Mode后的“**Edit**”按钮。



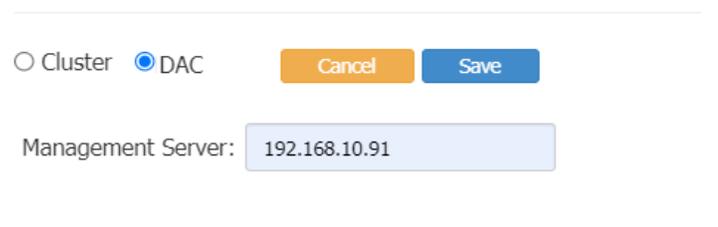
The screenshot shows the 'Detailed information' section of the AP Configuration page. It lists the following settings:

IP Mode:	DHCP	Edit
IP:	172.16.10.169	
Netmask:	255.255.255.0	
Default gateway:	172.16.10.1	
DNS:	219.141.136.10	

Below these settings, the 'AP Mode' is set to 'Cluster', and the 'Edit' button is highlighted with a red box.

图 77: 修改 AP Mode

- 选择“**DAC**”选项。



The screenshot shows a dialog box for configuring the DAC mode. It has two radio buttons: 'Cluster' (unselected) and 'DAC' (selected). There are 'Cancel' and 'Save' buttons. Below the radio buttons, there is a 'Management Server' field with the IP address '192.168.10.91' entered.

图 78: 配置 DAC 模式

- 输入DAC的IP地址，并保存配置。

在DAP847-XXA重启后，将会切换为DAC模式并按照指定的IP地址完成注册。

■ 切换集群中的所有 DAP847-XXA 到 DAC 模式

- 单击AP Configuration页面右下角的“Convert To DAC”。

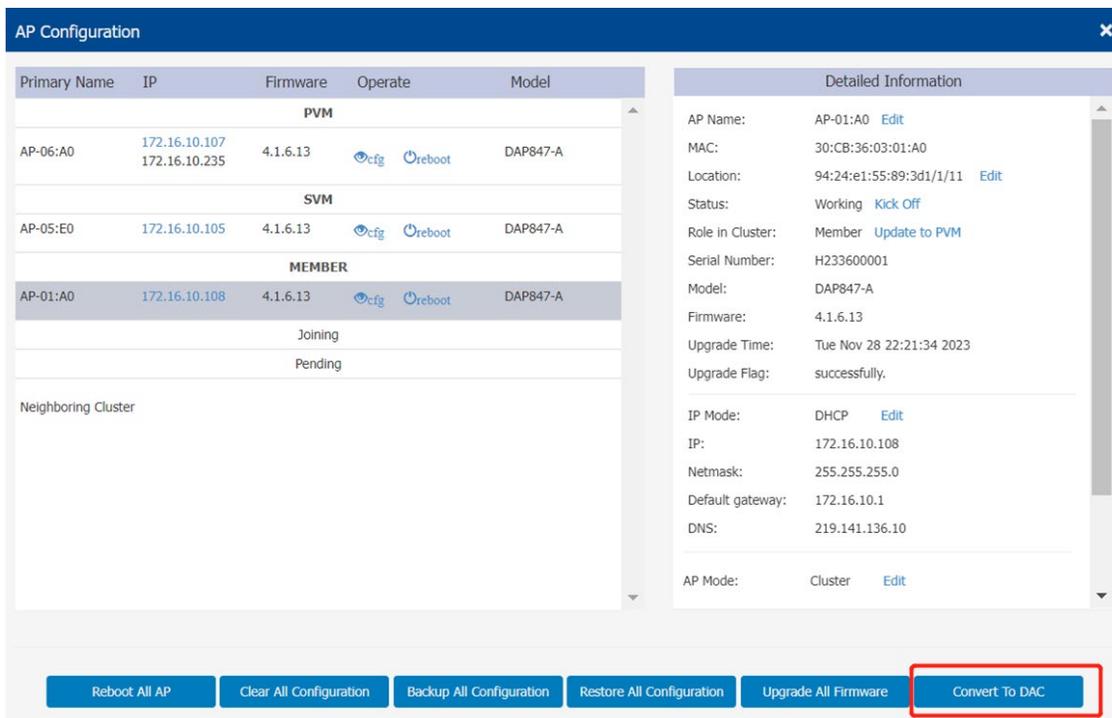


图 79: 切换为 DAC 模式

- 输入DAC的IP地址，并保存配置。

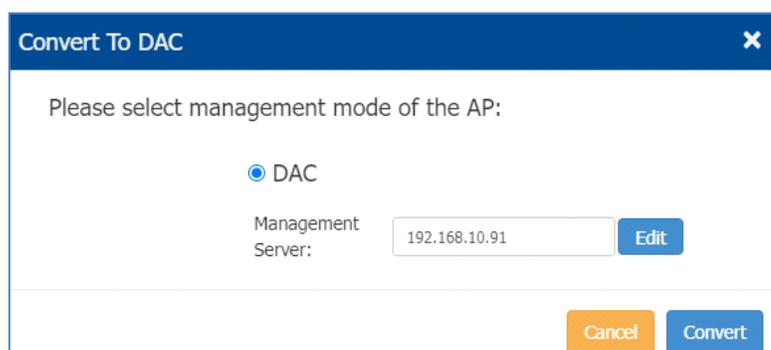


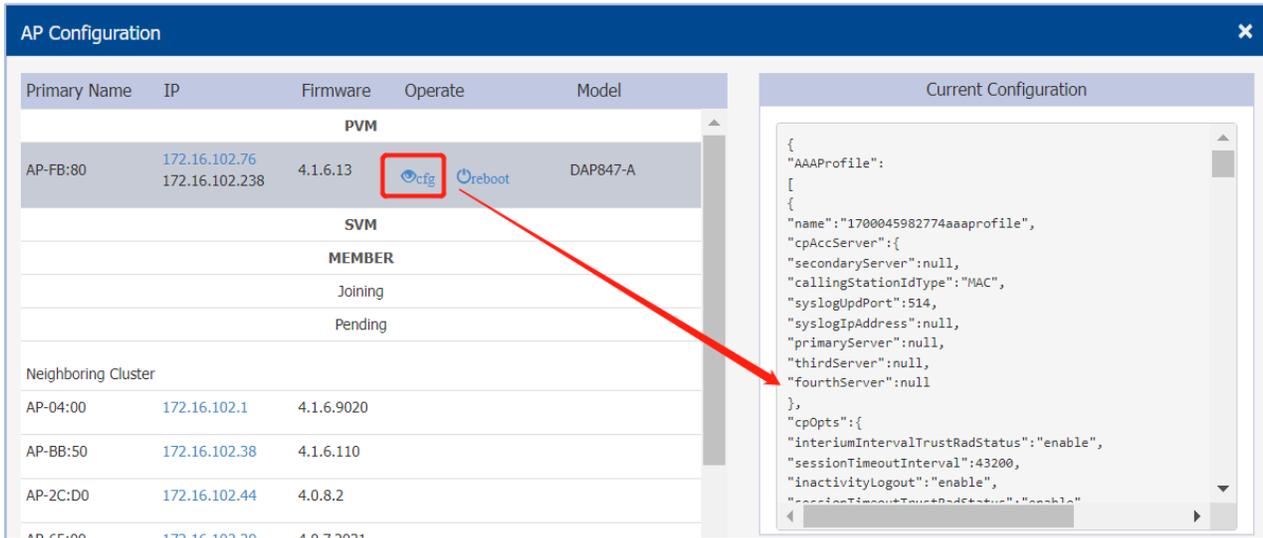
图 80: 配置 DAC 模式

在DAP847-XXA重启后，将会切换为DAC模式并按照指定的IP地址完成注册。

注意：当DAP847-XXA切换到DAC模式后，在集群模式下的配置将被清除。DAP847-XXA将从DAC获取新的配置。

7.9 查看DAP847-XXA的当前配置

在DAP847-XXA列表中，点击“cfg”图标，在右侧的Current Configuration页面中，可以查看DAP847-XXA当前的详细配置信息，如下图所示。



The screenshot displays the 'AP Configuration' window. On the left, a table lists APs under different categories: PVM, SVM, MEMBER, and Neighboring Cluster. The 'AP-FB:80' entry is highlighted, and a red box around its 'Operate' column contains a 'cfg' icon. A red arrow points from this icon to the 'Current Configuration' panel on the right, which shows a JSON configuration for the selected AP.

Primary Name	IP	Firmware	Operate	Model
PVM				
AP-FB:80	172.16.102.76 172.16.102.238	4.1.6.13	 	DAP847-A
SVM				
MEMBER				
			Joining	
			Pending	
Neighboring Cluster				
AP-04:00	172.16.102.1	4.1.6.9020		
AP-BB:50	172.16.102.38	4.1.6.110		
AP-2C:D0	172.16.102.44	4.0.8.2		
AP-6E:00	172.16.102.20	4.0.7.2021		

```
{
  "AAAPProfile":
  [
    {
      "name": "1700045982774aaaprofile",
      "cpAccServer": {
        "secondaryServer": null,
        "callingStationIdType": "MAC",
        "syslogUpdPort": 514,
        "syslogIpAddress": null,
        "primaryServer": null,
        "thirdServer": null,
        "fourthServer": null
      },
      "cpOpts": {
        "interiumIntervalTrustRadStatus": "enable",
        "sessionTimeoutInterval": 43200,
        "inactivityLogout": "enable",
        "sessionTimeoutTrustRadStatus": "enable"
      }
    }
  ]
}
```

图 81：查看 DAP847-XXA 的配置信息

7.10 重启DAP847-XXA

根据需要，您可以对DAP847-XXA执行重启的操作。

■ 重启集群中的一台 DAP847-XXA

- 选择一台DAP847-XXA，点击“reboot”来完成重启，如下图所示。

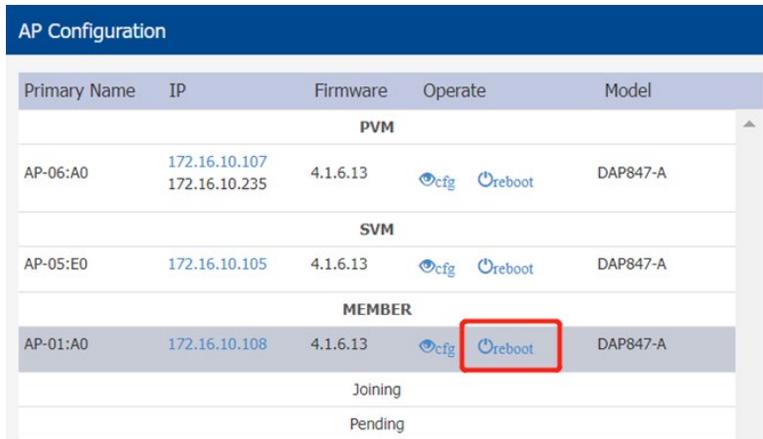


图 82：重启指定的DAP847-XXA 设备

■ 重启集群中所有 DAP847-XXA

- 点击页面底部的“**Reboot All AP**”按钮可以将所有的DAP847-XXA执行重启操作，如下图所示。

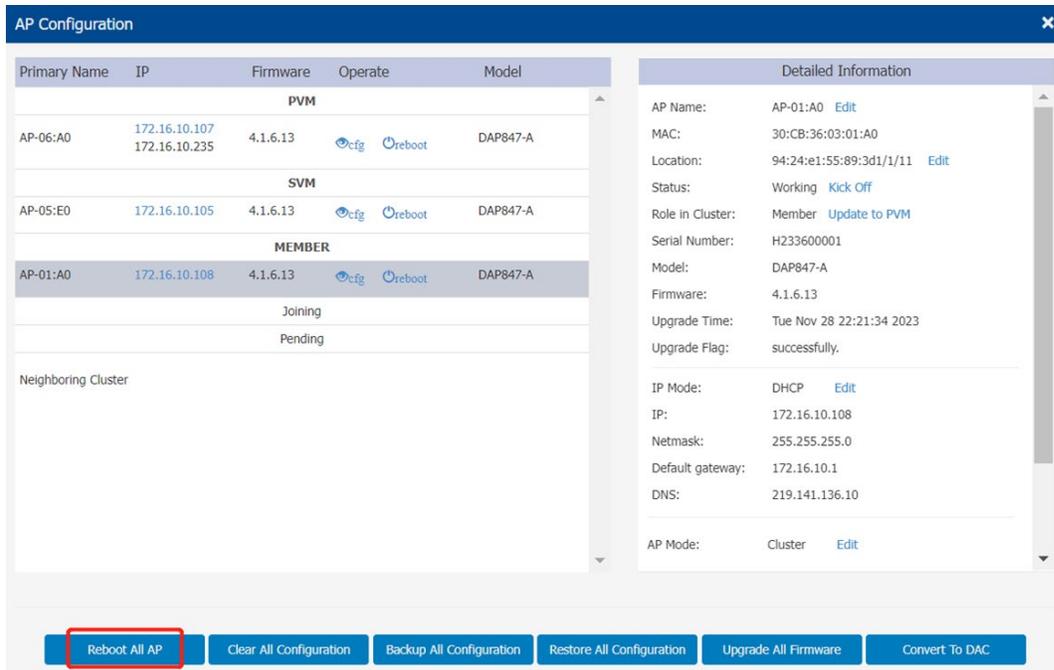


图 83：重启指定的DAP847-XXA 设备

7.11 恢复出厂配置

在AP Configuration页面的底部，点击“**Clear All Configuration**”按钮，可以将所有的DAP847-XXA配置清除并恢复到出厂配置。

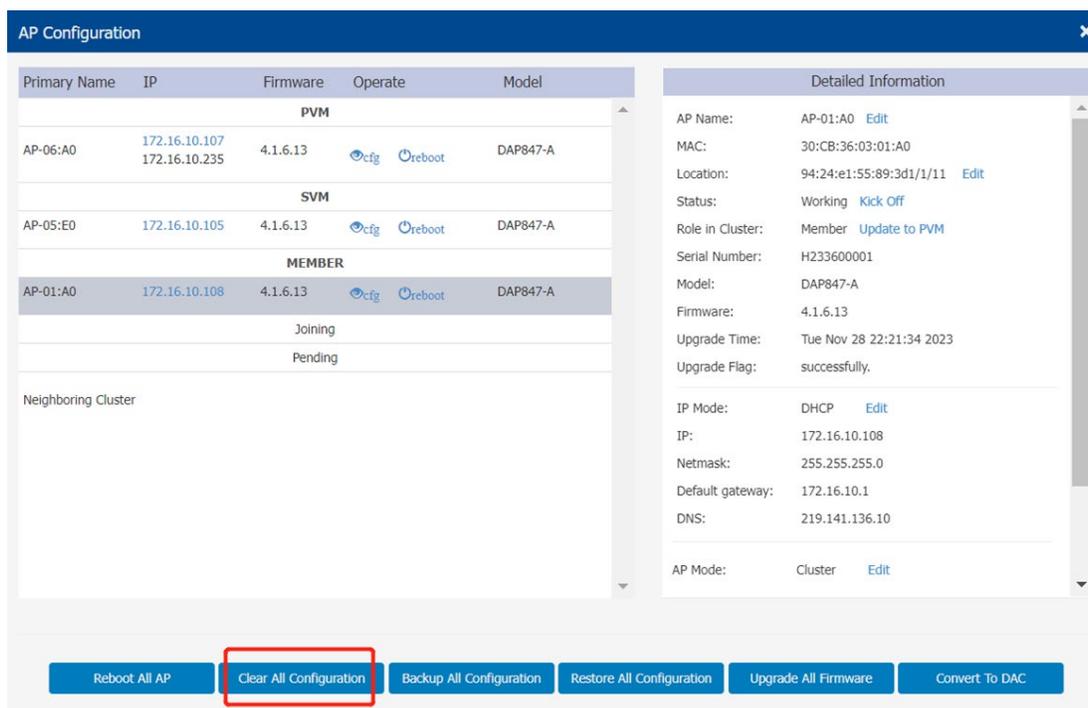


图 84: 清除所有配置

注意: 另外还有如下2种方式可以将DAP847-XXA恢复为“出厂设置”:

- ▶ 长按设备上的“**Reset**”按钮超过6秒钟。
- ▶ 在CLI模式下，使用命令“**ssudo firstboot**”和“**ssudo reboot**”来恢复“出厂设置”（默认帐户为：**support**，默认密码为：**Belden996!@#**）。

7.12 DAP847-XXA的配置备份和恢复

在AP Configuration页面, 您可以根据实际业务的需要备份和恢复集群的配置。

- ❑ 单击AP Configuration底部的“**Backup All Configuration**”按钮下载备份当前集群的配置文件, 该配置文件的默认名称是“pub-config.tar”
- ❑ 单击AP Configuration底部的“**Restore All Configuration**”按钮以恢复之前备份的配置文件, 请注意这个文件名必须为“pub-config.tar”。

The screenshot displays the 'AP Configuration' interface. It features a table with columns for Primary Name, IP, Firmware, Operate, and Model. The table is divided into sections: PVM, SVM, and MEMBER. The MEMBER section is currently selected, showing AP-01:A0 with IP 172.16.10.108 and firmware 4.1.6.13. To the right, a 'Detailed Information' panel provides specific details for the selected AP, including its name, MAC, location, status, role, serial number, model, firmware, upgrade time, and IP mode. At the bottom of the interface, there are several action buttons: 'Reboot All AP', 'Clear All Configuration', 'Backup All Configuration', 'Restore All Configuration', 'Upgrade All Firmware', and 'Convert To DAC'. The 'Backup All Configuration' and 'Restore All Configuration' buttons are highlighted with red boxes.

Primary Name	IP	Firmware	Operate	Model
PVM				
AP-06:A0	172.16.10.107 172.16.10.235	4.1.6.13		DAP847-A
SVM				
AP-05:E0	172.16.10.105	4.1.6.13		DAP847-A
MEMBER				
AP-01:A0	172.16.10.108	4.1.6.13		DAP847-A
			Joining	
			Pending	
Neighboring Cluster				

Detailed Information:

AP Name: AP-01:A0 [Edit](#)
MAC: 30:CB:36:03:01:A0
Location: 94:24:e1:55:89:3d1/1/11 [Edit](#)
Status: Working [Kick Off](#)
Role in Cluster: Member [Update to PVM](#)
Serial Number: H233600001
Model: DAP847-A
Firmware: 4.1.6.13
Upgrade Time: Tue Nov 28 22:21:34 2023
Upgrade Flag: successfully.

IP Mode: DHCP [Edit](#)
IP: 172.16.10.108
Netmask: 255.255.255.0
Default gateway: 172.16.10.1
DNS: 219.141.136.10
AP Mode: Cluster [Edit](#)

Buttons: Reboot All AP, Clear All Configuration, Backup All Configuration, Restore All Configuration, Upgrade All Firmware, Convert To DAC

图 85: 配置备份和恢复

7.13 DAP847-XXA固件升级

在升级DAP847-XXA之前，请先准备要升级版本文件。

您可以从链接<https://catalog.belden.com>中下载版本文件，并将版本文件保存到用于连接DAP847-XXA的本地电脑或是远程TFTP、SFTP服务器上。

- 点击“**AP Configuration**”页面中的“**Upgrade All Firmware**”按钮，将会弹出DAP847-XXA的升级页面，如下图所示。

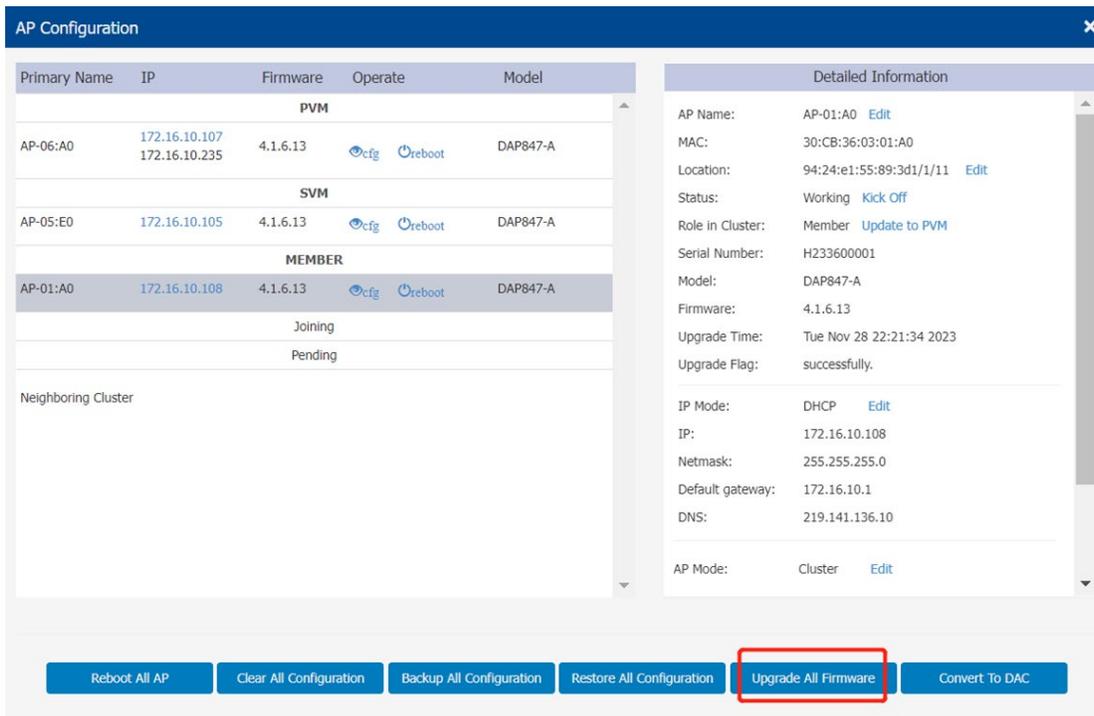


图 86: 跳转到 DAP847-XXA 升级页面

7.13.1 升级集群中所有DAP847-XXA

如果您需要升级不同型号的DAP固件，如DAP847-XXA和DAP6XX系列混合组网时，请根据**Multi-model Upgrade**页面上的AP型号选择相关DAP固件文件，多个型号的DAP设备可以同时进行升级。

注意：通常情况下，整个升级过程将会持续大概5分钟。

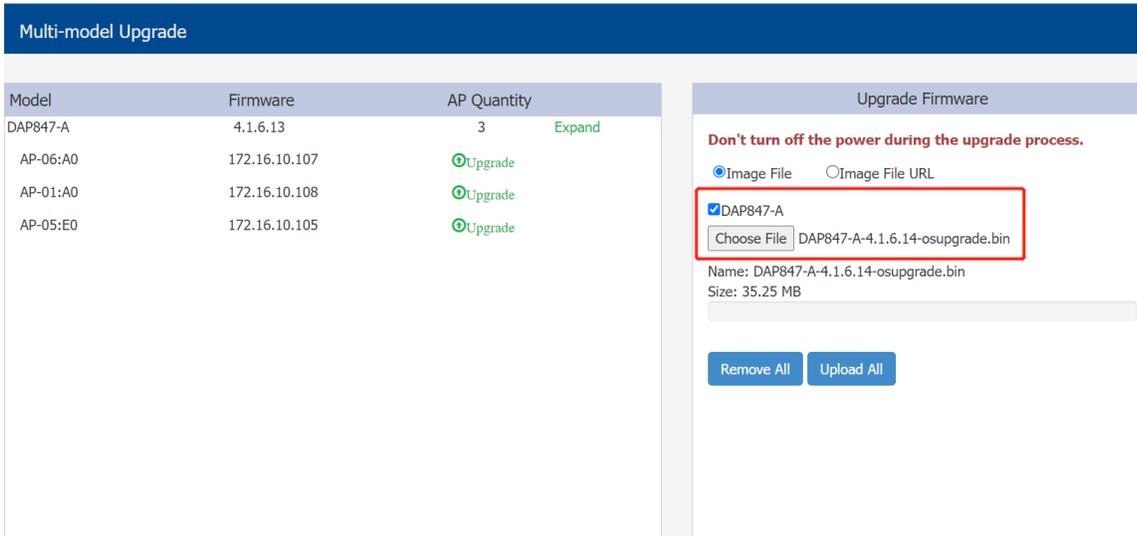


图 87: DAP847-XXA 升级页面

DAP847-XXA支持如下三种上传版本文件的方式:

- ▶ **本地文件上传:** 选择“Image File”选项，点击“Choose File”按钮从本地上传版本文件，单击“Upload All”按钮执行版本文件的上传和升级操作。如果想要取消本次升级，可单击“Remove All”按钮，如下图所示。

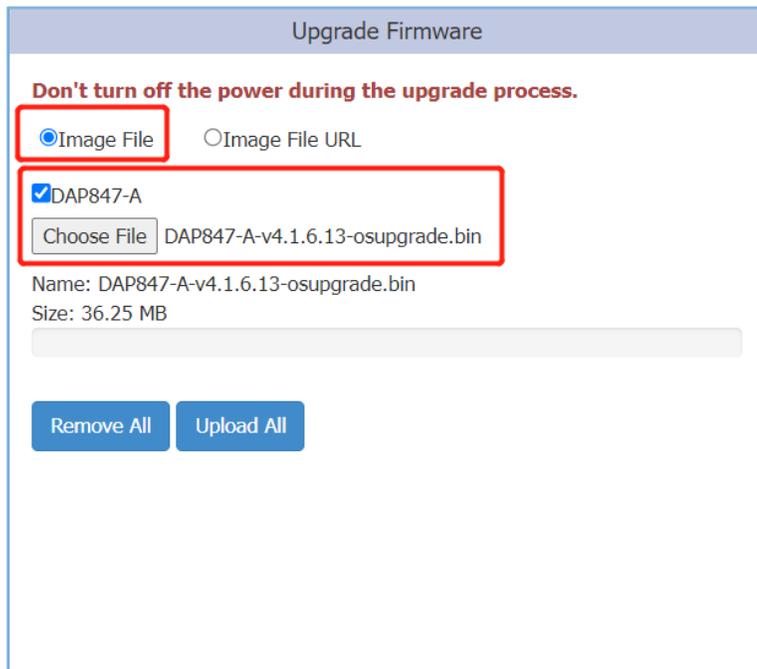


图 88: 上传本地升级文件

- ▶ **SFTP:** 通过SFTP的方式上传版本文件，选择“**Image File URL**”选项，在URL中输入SFTP服务器IP地址、用户名、密码以及版本文件名，单击“**Upload To All**”按钮执行上传和升级的操作，如下图所示。

Upgrade Firmware

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

Image File Image File URL

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

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

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

Upload To All

图 89: SFTP 方式上传升级文件

- ▶ **TFTP:** 通过TFTP的方式上传版本文件，选择“**Image File URL**”选项。在URL中输入TFTP服务器IP地址及版本文件名。单击“**Upload To All**”按钮执行上传和升级的操作，如下图所示。

Upgrade Firmware

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

Image File Image File URL

DAP847-A TFTP://192.168.62.137/DAP847-A-v4.1.6.13-o

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

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

Upload To All

图 90: TFTP 方式上传升级文件

7.13.2 升级集群中单台DAP847-XXA

DAP847-XXA集群同样支持为集群中的单台DAP847-XXA设备进行升级，您可以从**Multi-model Upgrade**页面的AP列表中选择要升级的设备。单击“**Upgrade**”并上传所选DAP847-XXA的固件文件。升级单台设备，支持的三种文件上传方式：

- ▶ 本地文件上传
- ▶ SFTP
- ▶ TFTP

当然，您也可以通过AP Advanced Configuration页面升级一台DAP847-XXA。参见第106页的“系统管理”。

Multi-model Upgrade

Model	Firmware	AP Quantity	
DAP847-A	4.1.6.13	3	Expand
AP-06:A0	172.16.10.107	 Upgrade	
AP-01:A0	172.16.10.108	 Upgrade	
AP-05:E0	172.16.10.105	 Upgrade	

Upgrade Firmware

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

Image File Image File URL

Choose File DAP847-A-4.1.6.14-osupgrade.bin

- Name: DAP847-A-4.1.6.14-osupgrade.bin
- Size: 35.25 MB

图 91：升级集群中的单台 DAP847-XXA

注意：为了避免异常状况的发生，请在升级过程中不要关闭电源。同时为确保新的软件版本达到最好的使用效果，建议在软件升级后清除浏览器中保存的历史数据，包括Cookies和Cache。

7.14 DAP847-XXA的LED指示灯配置

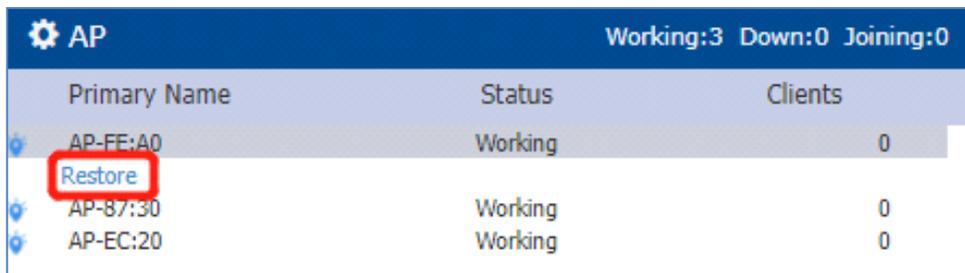
- 在AP页面中单击“”后可以启动“LED-Off/Locate”按钮，见图 92。
- 点击“**LED-Off**”可以关闭DAP847-XXA的 LED指示灯。
- 点击“**Locate**”以定位处于此状态的AP，出现“**Restore**”标签，DAP上的LED以红色、蓝色和绿色交替闪烁。



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

图 92: Locate 或 开启/关闭LED

- 点击“**Restore**”按钮恢复缺省状态，参考图 93。

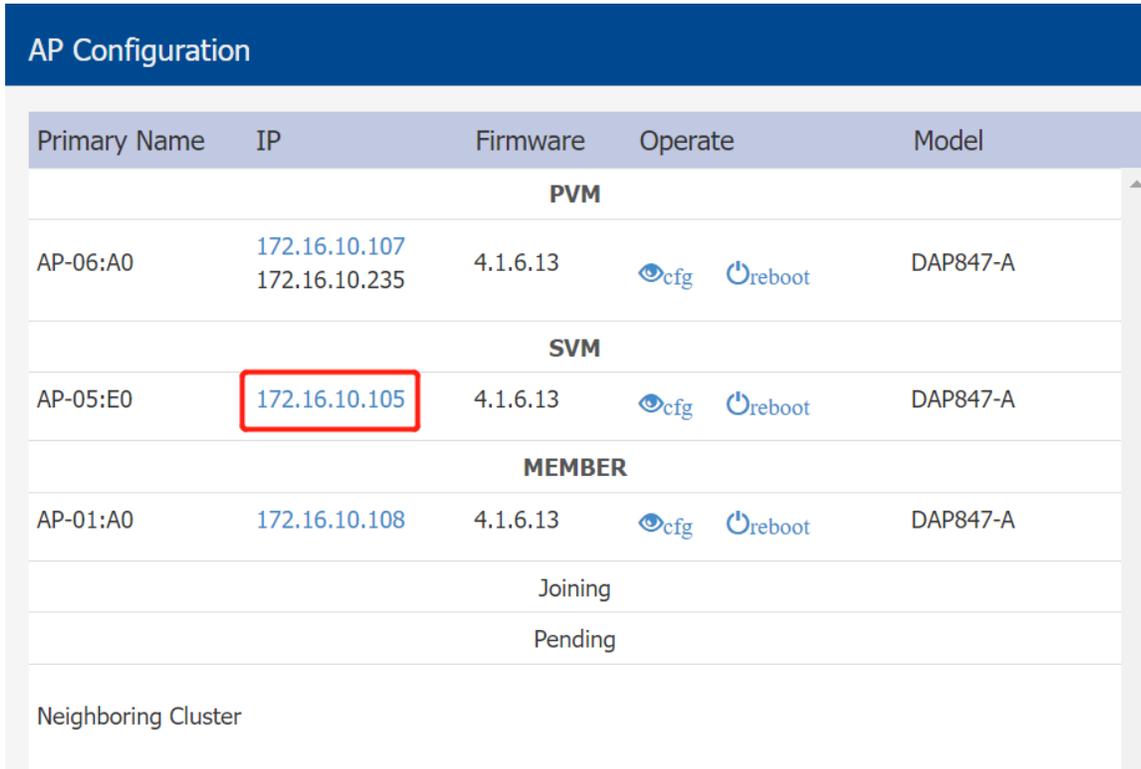


AP		Working:3	Down:0	Joining:0
Primary Name	Status	Clients		
AP-FE:A0	Working	0		
Restore				
AP-87:30	Working	0		
AP-EC:20	Working	0		

图 93: 恢复LED为缺省状态

7.15 DAP847-XXA高级配置

您可以通过单击DAP847-XXA列表中的IP地址来访问DAP847-XXA的高级配置页面。参考图 94。



Primary Name	IP	Firmware	Operate	Model
PVM				
AP-06:A0	172.16.10.107 172.16.10.235	4.1.6.13	 	DAP847-A
SVM				
AP-05:E0	172.16.10.105	4.1.6.13	 	DAP847-A
MEMBER				
AP-01:A0	172.16.10.108	4.1.6.13	 	DAP847-A
Joining				
Pending				
Neighboring Cluster				

图 94: DAP847-XXA 高级配置

7.15.1 DAP847-XXA高级配置页面简介

DAP847-XXA的高级配置页面是一个专用的web界面，用于监控和配置集群中的单台DAP847-XXA设备并完成私有配置，而集群web管理系统是用于基于集群全局的配置和监控，参考图 95。在DAP847-XXA的高级配置页面中，您可以完成如下操作：

- ▶ 通过连接到DAP847-XXA上的客户端来检查WLAN状态。
- ▶ 在DAP847-XXA上配置DHCP/DNS/NAT服务。
- ▶ 为DAP847-XXA配置无线Mesh功能。
- ▶ 升级、重置或重启DAP847-XXA。
- ▶ 监测和扫描RF环境。
- ▶ 配置及邻居DAP的显示。

HIRSCHMANN IT				
A BELDEN BRAND				Administrator
AP				
MAC	IP	Status	Clients	Work Mode
94:AE:E3:FF:C0:70	172.16.10.169	CLUSTER	1	AP
WLAN				
WLAN Name	Status	Type	Clients	
My-wifi-test	enable	Personal	1	
My-wifi-PSK	enable	Personal	0	
My-wifi-portal	enable	Open	0	
My-wifi-1x	enable	Enterprise	0	
My-wifi-test101	enable	Open	0	
Clients				
For AP: 94:AE:E3:FF:...		Total:1		
Name	IP	MAC	WLAN	Auth
	172.16.10.102/fe8	c0:3c:59:70:3d:c5	My-wifi-test	PSK_WPA2
RF				
	Channel	Status	Power	Clients
2.4G	11	enable	17	0
5G_all	52	enable	21	1
System				
Network				
Service				
Neighbor AP				
RF Environment				

图 95: AP 高级配置页面

7.15.2 AP状态监控和工作模式配置

AP基本信息页面主要显示了DAP847-XXA的基本信息，包括MAC地址、IP地址、状态、关联客户端数量和工作模式。

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

图 96: AP 基本信息页面

如要进入AP模式配置页面：

- 请单击AP基本信息页面中的“AP”超链接。

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

图 97: 点击超链接进入工作模式配置页面

- 在弹出的“**Mode Configuration**”页面更改工作模式。

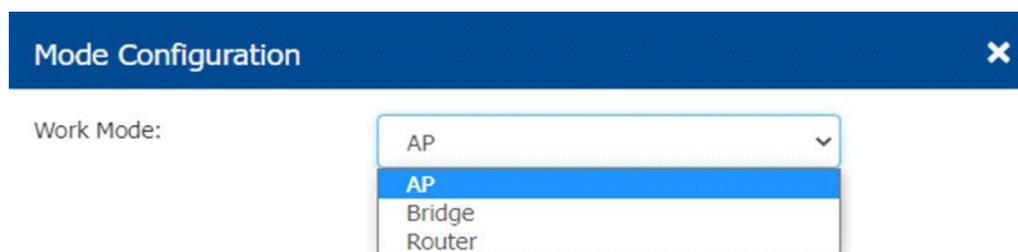


图 98: AP 工作模式配置

- 修改模式后 DAP847-XXA 将会重新启动使配置生效。在默认情况下，DAP847-XXA 工作于 AP 模式。

根据使用场景的需要，您可以将指定的 DAP847-XXA 设备配置在 Bridge 模式或 Router 模式下工作。

■ 配置 DAP847-XXA 为 Bridge 模式

DAP847-XXA 的 Bridge 模式是一种网络连接模式，它允许 DAP847-XXA 之间建立桥接以实现两个或多个网络之间的连接，在 Bridge 模式下，DAP847-XXA 可以与另一个 DAP847-XXA 进行连接，从而扩展网络范围或连接不同的网络。

需要注意的是，Bridge 模式下的 DAP847-XXA 必须处于相同的 IP 网段，并且必须使用相同的信道和加密方式进行连接。

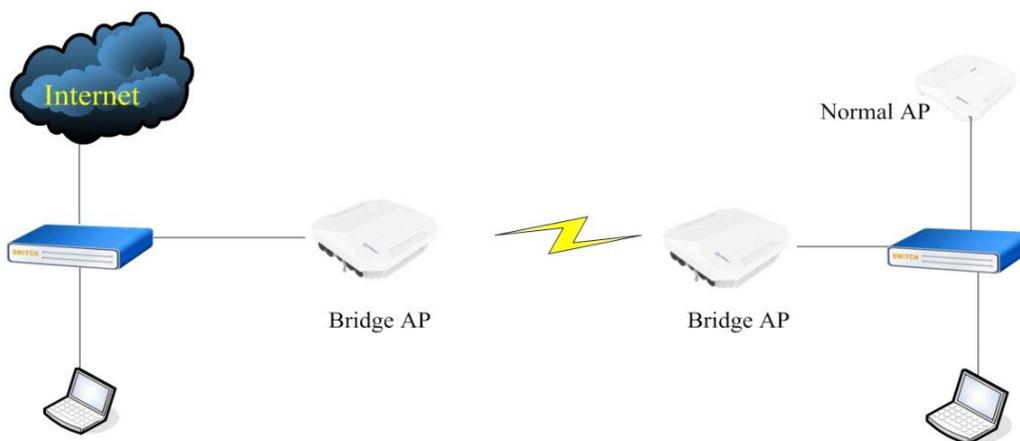


图 99: Bridge 模式拓扑图

在Bridge模式下，DAP847-XXA只广播用于bridge连接的SSID，除了接受bridge AP的连接外，不接受其它无线客户端连接，参考图 100。

图 100: Bridge 模式配置

关键参数描述如下：

参数	描述
Work Mode	DAP847-XXA的工作模式，包括Bridge模式, AP模式以及,Router模式缺省状态下为AP模式。
SSID	配置用来进行Bridge连接的SSID，该SSID需要与对端设备中配置的SSID名称一致。
Root	指定该DAP847-XXA是否为根节点。
Band	用于Bridge连接的频段，2.4G或5G。
Passphrase	用于设置无线连接的密码。
Confirm	确认密码。

■ 配置 DAP847-XXA 工作在 Router 模式

在Router模式下，DAP847-XXA将成为一个DHCP服务器为无线客户端分配IP地址。DAP847-XXA支持通过DHCP、静态IP或PPPOE管理上行链路接口（WAN）的IP地址。

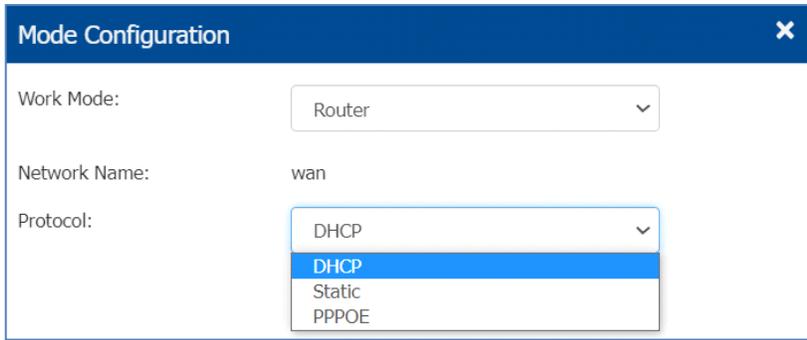


图 101: 配置 WAN 接口的 IP 地址模式

您可以在**AP Network Configuration**页面中查看和修改详细的网络配置，在该页面，您可以修改WAN接口和默认接口（LAN）接口的配置，IP地址，DNS，Gateway等。

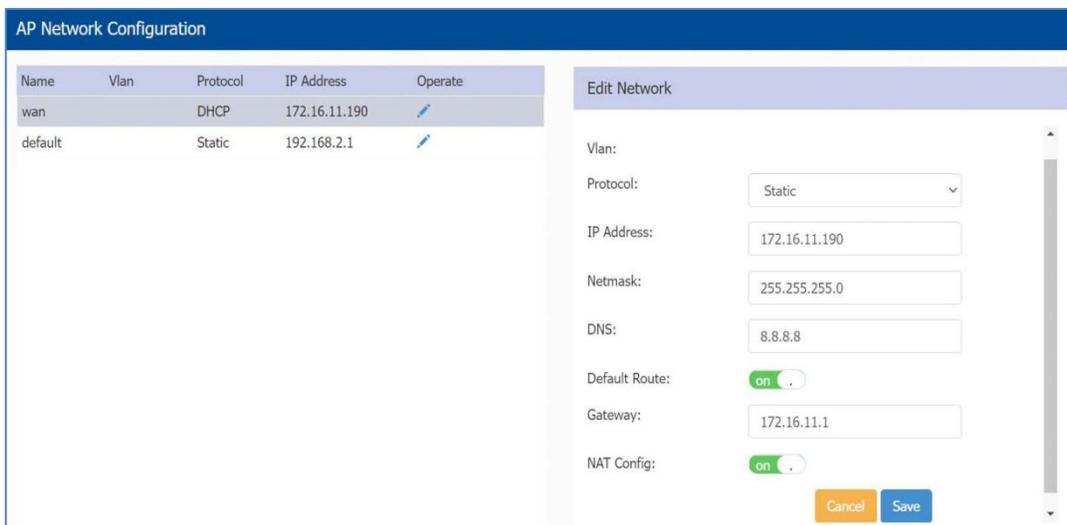


图 102: 修改 DAP847-XXA 的网络配置

7.15.3 WLAN信息

WLAN信息页面显示了当前DAP847-XXA上WLAN的基本信息，例如WLAN Name、状态、加密类型以及关联到WLAN的无线客户端数量。该页面中的信息仅能够查看，不能对其进行配置。

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

图 103: WLAN 基本信息

7.15.4 Clients信息

“Clients”页面显示了当前DAP847-XXA上关联的客户端的基本信息，例如客户端的IP地址、MAC地址、客户端所关联的WLAN和加密类型以及Captive portal认证用户的用户名。该页面中的信息仅能够查看，不能对其进行配置。

Clients				
For AP: 34:E7:08:09: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

图 104: Clients 信息页面

7.15.5 RF信息

RF页面显示的是有关当前DAP847-XXA设备上RF的基本信息，通过该页面，您可以了解到当前DAP847-XXA设备的RF信道、工作状态、每个RF的发射功率以及与RF相关的客户端数量。该页面中的信息仅能够查看，不能对其进行配置。

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

图 105: RF 页面

7.15.6 系统管理

在System页面上，您可以查看与当前DAP847-XXA设备相关的系统日志信息。您也可以在该页面中对DAP847-XXA进行升级。请参考图 106。

参考第131页的“配置Syslog系统日志”和第94页的“升级集群中所有DAP847-XXA”。

图 106: AP UI 中的系统管理

7.15.7 DAP847-XXA接口配置

在DAP847-XXA的接口配置中，您可以查看到DAP847-XXA每个接口的详细信息。同时，在接口配置中，您可以通过配置Mesh无线网络连接将DAP847-XXC连接到DAP847-XXA。

如需完成DAP847-XXA的接口配置，请按照如下路径完成配置**AP Advanced Configuration → Network → AP Interface → AP Interface Configuration**。

AP Interface				AP Networks			
Name	Model	Link Status	Enable	Name	Vlan	Protocol	IP Address
Eth0	Trunk	Up	Yes	vlan106	106	Static	
Backhaul0	Trunk	Down	No	wan		DHCP	172.16.102.80
Connector0	Trunk	Down	No				

图 107: DAP847-XXA 接口状态

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

图 108: AP 接口配置

关键参数描述如下:

参数	描述
Eth0	有线接口，连接交换机等设备。
Backhaul0	Mesh/Bridge链路的下行接口。
Connector0	Mesh/Bridge链路的上行接口。
Speed	接口的链路传输速率。
Model	VLAN access 模式或 VLAN trunk 模式。
Link Status	Up或down。
Enable	显示接口是否是启用状态。
Operate	操作状态，是否可以接口进行配置操作，只有对Backhaul0和Connector0接口才能完成配置操作。

7.15.8 DAP847-XXA网络配置

根据不同的使用场景和网络配置的要求，可以针对DAP847-XXA的WAN接口和VLAN接口完成相关参数的配置，包括VLAN，DHCP或Static IP等。您可以按照如下路径完成配置：

AP Advanced Configuration → Network → AP Network Configuration。

注意：在创建或编辑WLAN时，如果绑定了VLAN的配置，DAP847-XXA中会相应的创建VLAN接口，参考图 51。

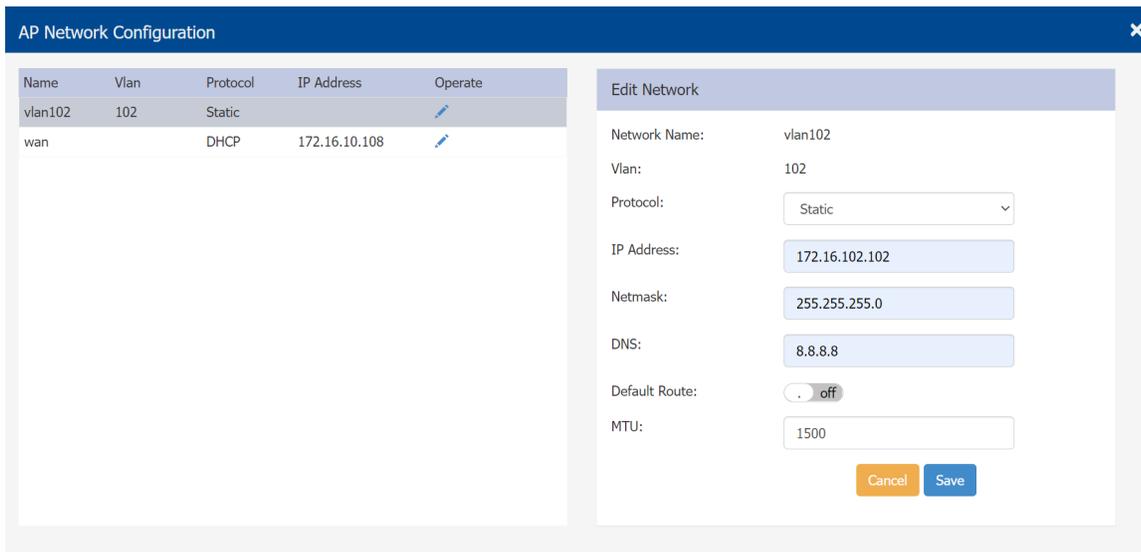


图 109：网络配置

关键参数描述如下：

参数	描述
Name	网络接口名称， DAP847-XXA 上有如下两种网络接口类型： <ul style="list-style-type: none">▶ 绑定到 WLAN 的 VLAN 接口类型 VLAN networks mapping to WLAN (SSID)▶ 绑定到 DAP847-XXA 上行接口的 WAN 接口类型。
VLAN	VLAN ID，关联到对应的 WLAN(SSID)或 WLAN 接口映射的 VLAN ID。
Protocol	网络接口的 IP 地址分配方式，包含如下两种： <ul style="list-style-type: none">▶ DHCP：接口的 IP 地址是从 DHCP 服务器获取的。▶ Static：接口的 IP 地址是手动设置的。
IP Address	网络接口的 IP 地址。

Operate	修改 DAP847-XXA 的网络配置。
---------	----------------------

编辑AP网络参数描述如下：

参数	描述
Network Name	待编辑的网络接口名称。
Vlan	关联到对应的 WLAN(SSID)或 WAN 接口映射的 VLAN ID。
Protocol	网络接口的 IP 地址分配方式，包含如下两种： <ul style="list-style-type: none"> ▶ DHCP: 接口的 IP 地址是从 DHCP 服务器获取的。 ▶ Static: 接口的 IP 地址是手动设置的。
IP Address	网络接口的 IP 地址。
Netmask	网络的子网掩码。
DNS	网络的 DNS 服务器。
Default Route	显示网络接口是否为 AP 的默认路由。默认情况下，WAN 接口是 AP 的默认路由。
MTU	网络接口的 MTU 值。

7.15.9 Mesh配置

Belden的Mesh解决方案是一种高效、可靠的方式，可以在没有铺设线缆或不方便布线的情况下来扩充无线网络覆盖范围。

Belden的Mesh解决方案也可以用于某些移动场景，如在轨道交通的使用场景，DAP847-XXA支持与下行DAP-XXC设备的连接，提供车地数据通信的通道，实现铁路控制信号及相关数据的实时传输。

通过DAP847-XXA的Mesh功能，您可以桥接多个以太网局域网或通过Mesh扩展无线覆盖范围（无线回传）。当流量穿过Mesh网络时，Mesh会自动重新配置断开或阻塞的路径。这种自愈的功能提高了DAP847-XXA的可靠性和冗余性。如果某个DAP847-XXA停止工作或与网络断开连接，则Mesh网络仍能够继续工作。参考图 110。

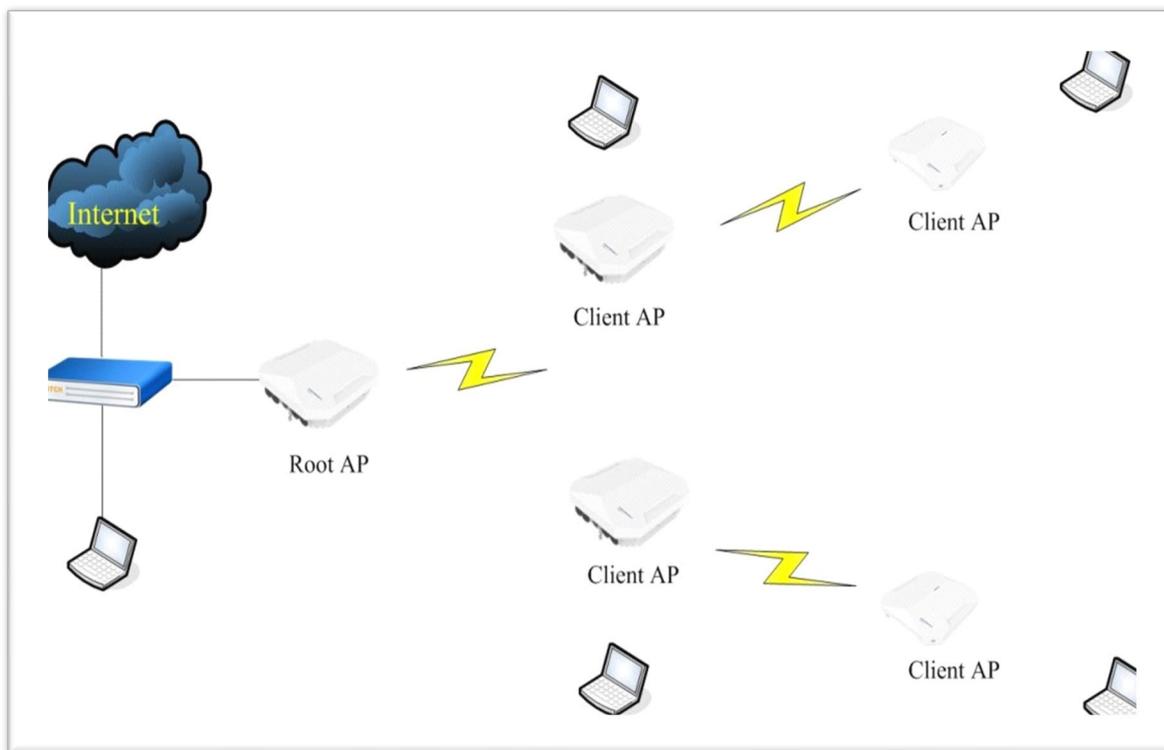


图 110: MESH 拓扑图

在不需要桥接以太网局域网的情况下扩大无线覆盖范围，您可以将DAP847-XXA配置为无线回传的Mesh模式。在这种情况下，DAP847-XXA同时也能够为无线客户端提供网络接入服务，将用户的数据经由root设备转到有线网络。

您可以按照如下路径完成配置：

AP Advanced Configuration → Network → AP Interface

- 点击“**Backhaul0**”接口的“”来配置您的Mesh网络，参考图 111。

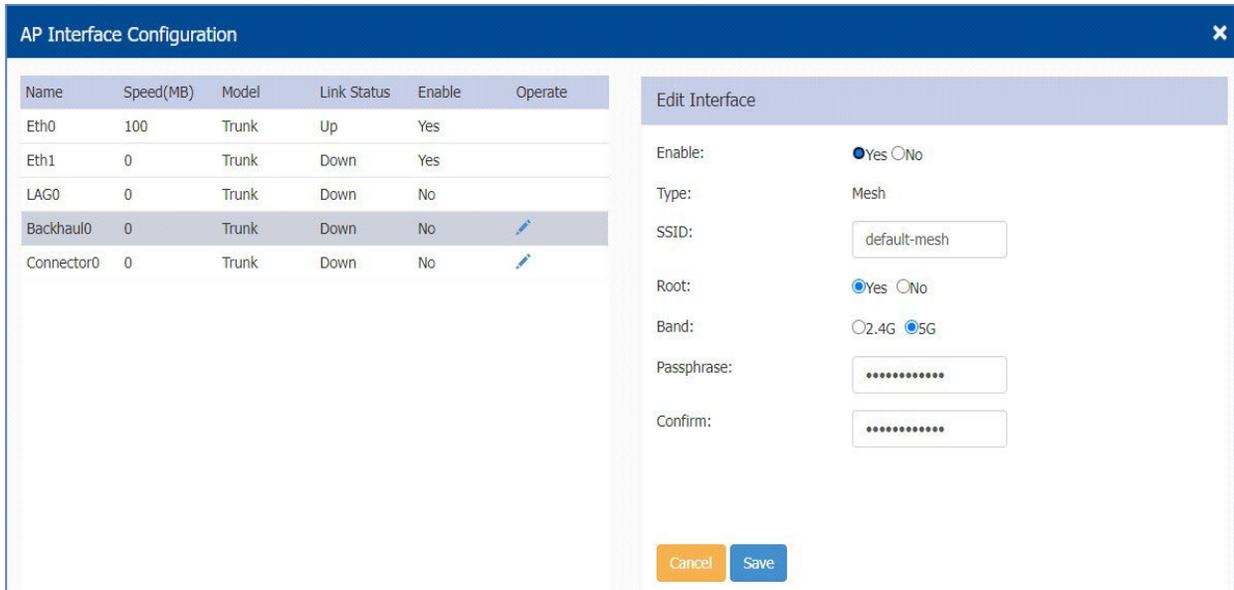


图 111: AP interface configuration 页面

关键参数描述如下:

参数	描述
Enable	选择 “Yes” 启用或选择 “No” 禁用 DAP847-XXA 上的 Mesh 功能。
SSID	Mesh 连接的 SSID。
Root	指定 Mesh 网络的根节点。
Band	用于 Mesh 连接的频段，从 Mesh 根节点到 Mesh Client 节点应使用相同的频段。
Passphrase	WLAN 的密码，用于设置 Mesh 连接。
Confirm	重新输入密码进行确认。

7.15.10 Neighbor AP配置

Neighbor AP是指与当前DAP847-XXA部署位置邻近的其它DAP847-XXA设备，也是连接到当前DAP847-XXA的客户端可能漫游的目标设备。

目前DAP847-XXA上有两种类型的**Neighbor AP**：

- ▶ **Auto Neighbor AP**：通过无线扫描自动发现的。
- ▶ **Static Neighbor AP**：静态邻居AP是在某些特殊部署场景下手动添加的。

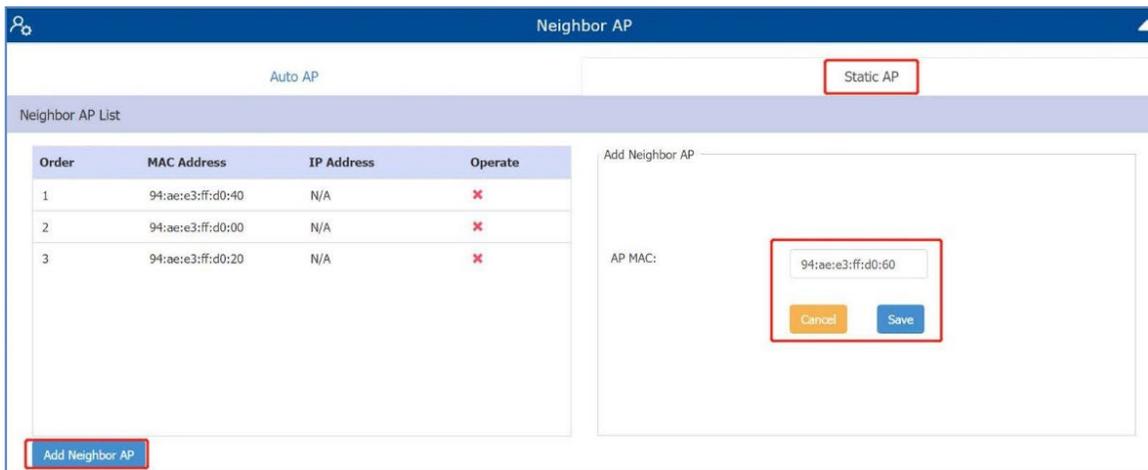


图 112: 配置 Static neighbor AP

关键参数描述如下：

参数	描述
Order	Neighbor AP 的编号。
MAC Address	Neighbor AP 的 MAC 地址。
IP Address	Neighbor AP 的 IP 地址。
Operate	删除 Neighbor AP，只适用于对 StaticNeighbor AP 进行该操作。

7.15.11 RF environment监控

RF Environment页面用于监控不同模式下的DAP847-XXA的无线扫描数据。无线网络运行过程中，可能会遇到其它一些RF设备产生的干扰，从而影响无线通信的质量。

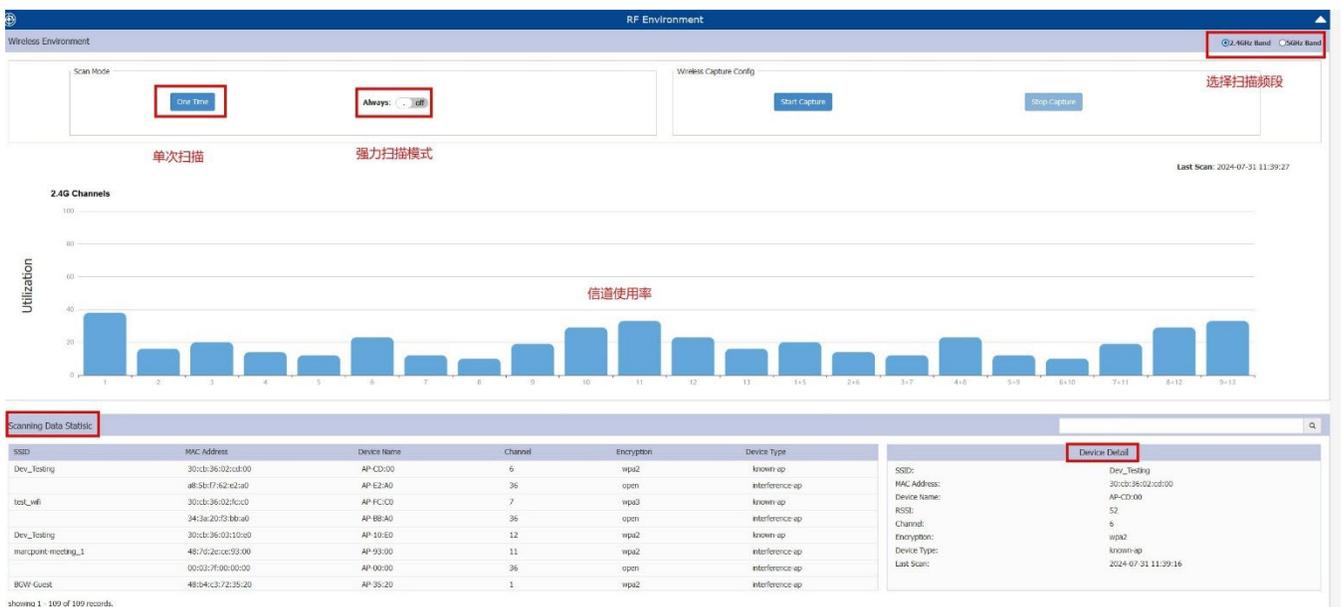
DAP847-XXA可以检测Wi-Fi网络的RF环境，识别干扰，并对其来源进行分类。这个分析结果可用于快速隔离检测到的数据传输以及信道质量的问题，同时也能够检测出在同一信道中工作的其他设备的抢占引起的流量拥塞问题。

扫描频段可以选择为2.4 GHz或5 GHz，扫描的数据包括RF环境中的信道利用率和SSID信息等。如果您将鼠标移动到某个信道上，便可以查看该信道的详细信息，如果单击相关条目，则可以查看详细的SSID信息，参考图 113。

DAP847-XXA提供了如下两种扫描模式：

- ▶ **One Time:** 单次扫描，扫描将持续5分钟，然后返回到正常模式，即AP模式。
- ▶ **Always:** 扫描模式始终处于激活状态，也可以称为强力扫描模式，在该模式下不允许无线客户端关联。

注意：要查看DAP847-XXA的扫描模式数据，请确保该DAP847-XXA处于“扫描模式”。在扫描模式下，DAP847-XXA将不会响应客户端的连接请求。当扫描模式（One Time mode或 Always mode）自动终止时，DAP847-XXA将返回到正常的AP模式，允许客户端连接。



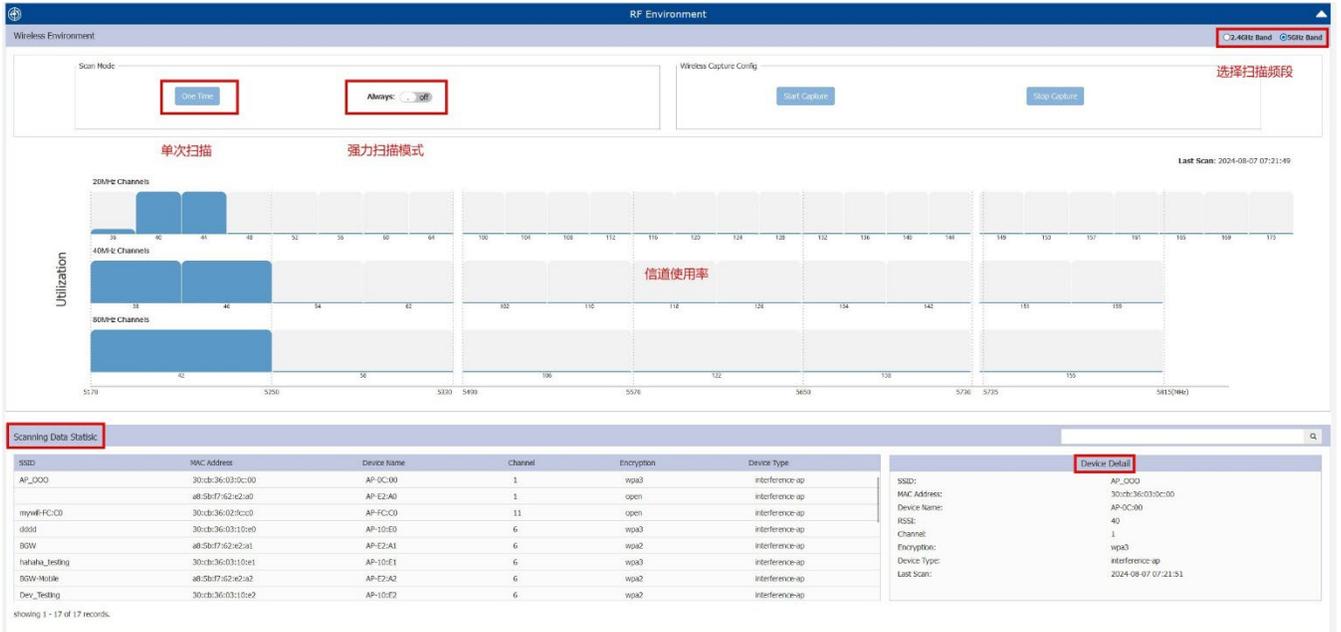


图 113: RF environment 页面

7.15.12 无线抓包功能

DAP847-XXA支持无线抓包模式，在这种模式下，DAP847-XXA将会断开与无线客户端的连接，同时在抓包期间停止无线扫描。

当抓包时间达到5分钟或抓包文件达到10MB时，抓包将会自动停止。在抓包过程中也可以随时手动停止抓包。

在DAP847-XXA上完成无线抓包，请参考如下步骤：

- 登陆**AP Advanced Configuration**页面→**RF Environment**→**WirelessCapture Config**→**Start Capture**，参考图 114。

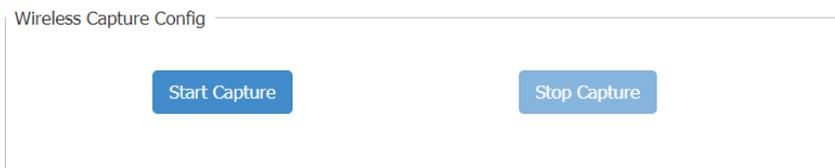


图 114: 无线抓包配置

- 根据实际需要选择合适的过滤条件。

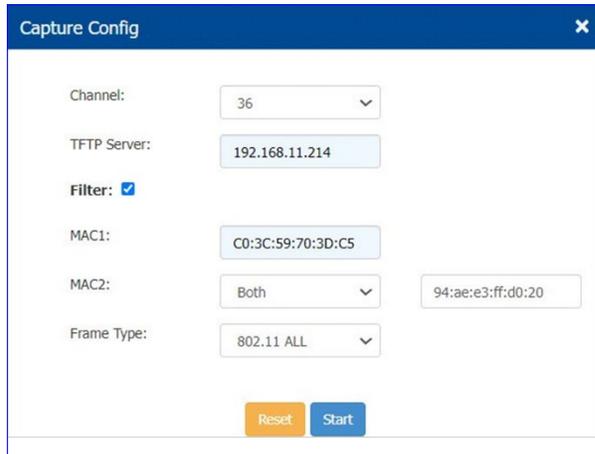


图 115: 抓包过滤条件

- 单击“**Start**”按钮开始抓包，DAP847-XXA将数据包文件临时存储在/tmp文件夹中，并在上传到TFTP服务器后自动删除。

```
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
```

图 116: 抓包文件存储示例

7.16 配置DAP847-XXA的网络服务

7.16.1 配置DHCP服务

在一些特殊的使用场景，如网络中没有DHCP服务器或DAP847-XXA工作在路由模式时，您可以设置DAP847-XXA上的DHCP功能，使其提供DHCP服务。

请按照如下路径完成配置：**AP advanced configuration page** → **Service** → **DHCP**，参考图 117。

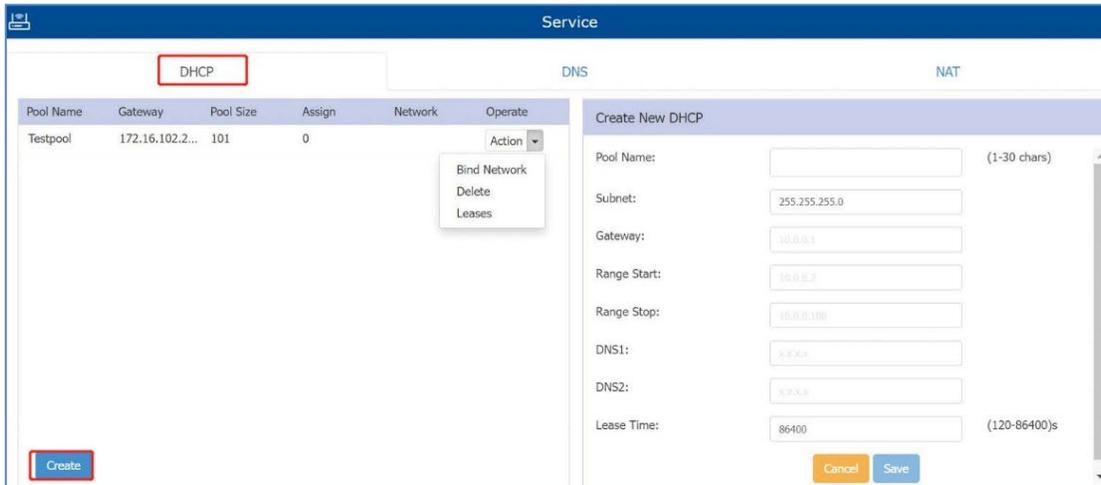


图 117: 配置 DHCP 服务

在创建一个DHCP地址池后，必须将DHCP地址池绑定到一个指定的网络，如图 118所示。绑定地址池之前，您需要在**AP UI** → **Network** → **AP Networks Configuration**中完成对应接口的配置：

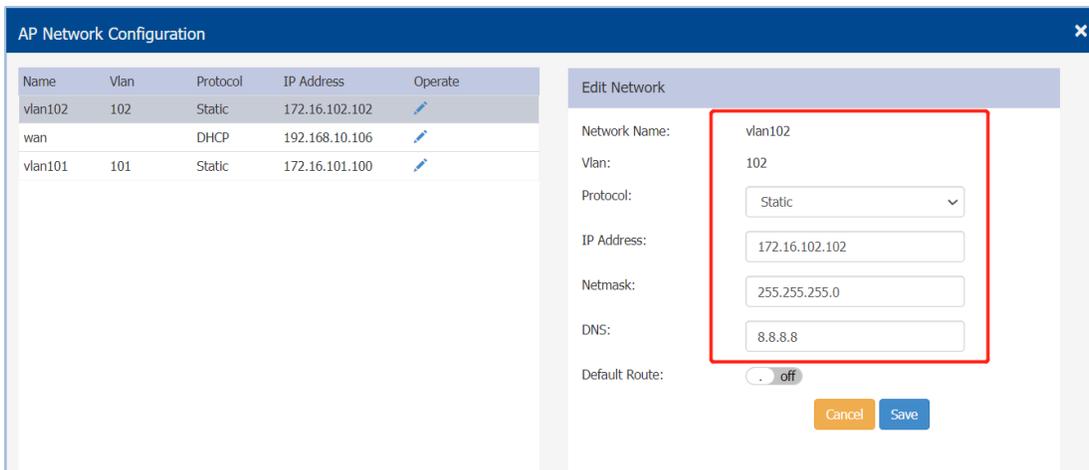


图 118: 网络接口配置

注意： DHCP地址池只能绑定到配置了静态IP的网络接口上。

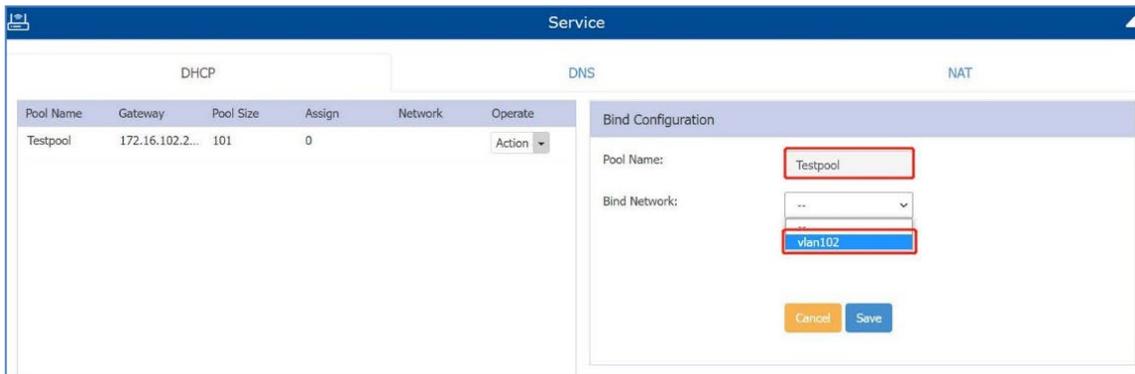


图 119：将 DHCP 地址池绑定到对应接口上

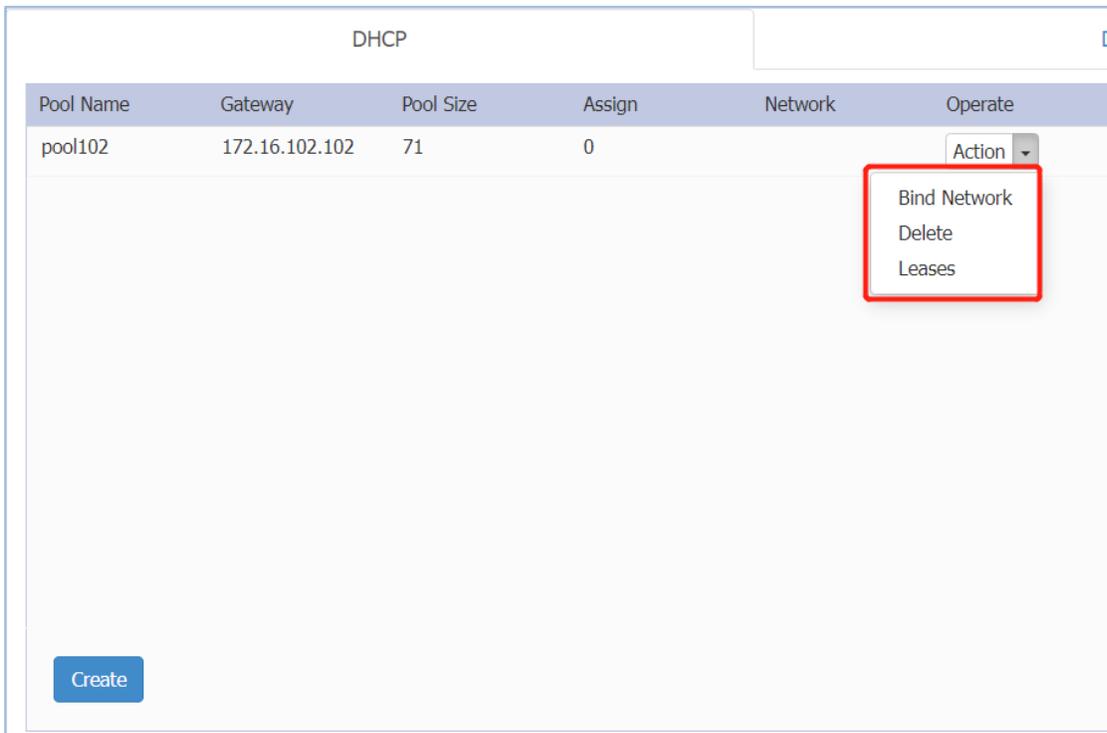


图 120：DHCP 地址池操作

关键参数描述如下：

参数	描述
Bind Network	绑定 DHCP 地址池到指定的网络接口。
Delete	删除 DHCP 地址池。
Leases	显示 IP 地址的分配情况。

7.16.2 配置DNS服务

DNS Cache，也称为DNS高速缓存，可以在DAP847-XXA设备中存储DNS（域名系统）查询结果，这种缓存的方式可以减少对DNS服务器的请求次数，从而加快客户端网络浏览速度，并减少网络流量。

当一台客户端尝试连接到一个域名（例如www.belden.com）时，它会首先通过DNS查询将这个域名解析为对应的IP地址。这个查询过程需要向DNS服务器发送请求并等待其响应。如果这个域名解析的结果在之前已经查询过，并且目前结果仍然有效，那么就可以直接使用这个结果，而不需要再次向DNS服务器发送查询请求。

配置路径：**AP Advanced Configuration** → **Service** → **DNS**。

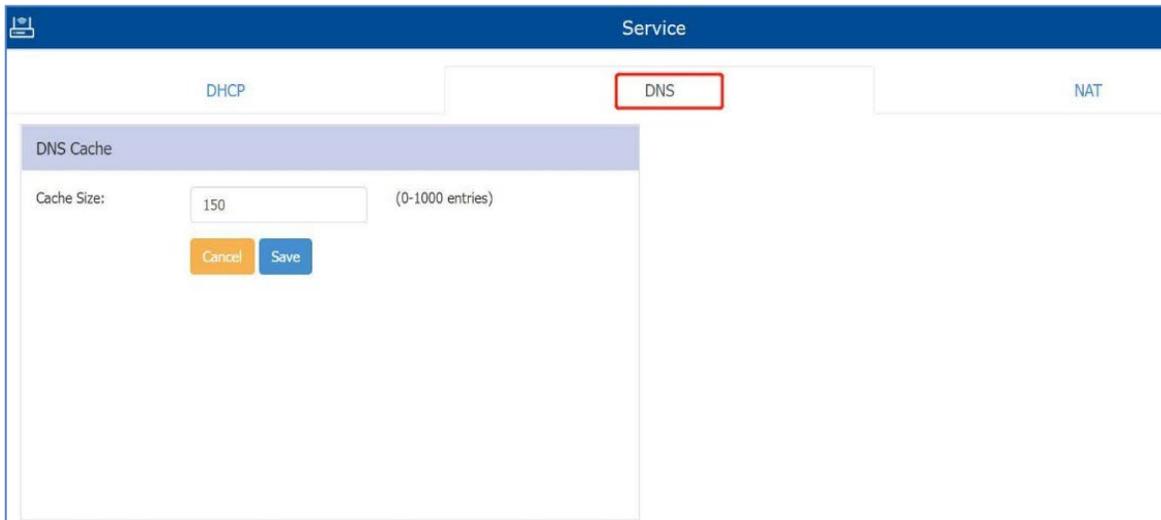


图 121: DNS 缓存配置

关键参数描述如下：

参数	描述
Cache Size	指定 DNS 缓存的数量，在 DAP847-XXA 中，最多可以设置为 1000（条），缺省值为 150（条）。

7.16.3 NAT配置

NAT（Network Address Translation）是DAP847-XXA上采用的一种网络地址转换技术，用于实现在专用网络（私网）和公共网络（公网）之间的互访。而DAP847-XXA则作为专用网络和公共网络的代理。

NAT的工作原理是将内网地址和端口号转换成合法的公网地址和端口号，建立一个会话，与公网主机进行通信。NAT外部的主机无法主动与位于NAT内部的主机通信。NAT内部主机想要通信，必须主动和公网的一个IP通信，DAP847-XXA负责建立一个映射关系，从而实现数据的转发。

NAT的功能不仅解决了IP地址不足的问题，而且还能有效的避免来自网络外部的入侵，隐藏并保护网络内部的计算机。静态NAT不能节约公网地址，但可以起到隐藏内部网络的作用。

DAP847-XXA同时支持源NAT（Source NAT）和目标NAT（Destination NAT）。

配置路径：AP Advanced Configuration → Service → NAT。

■ Source NAT

在客户端访问互联网时，使用Source NAT配置可将内部多个IP地址转换为单个外部的IP地址，您可以用这个方式节省公共IP地址。配置Source NAT，请单击Source NAT的标题栏，并在弹出的Source NAT Configuration页面中完成配置，参考图 122。

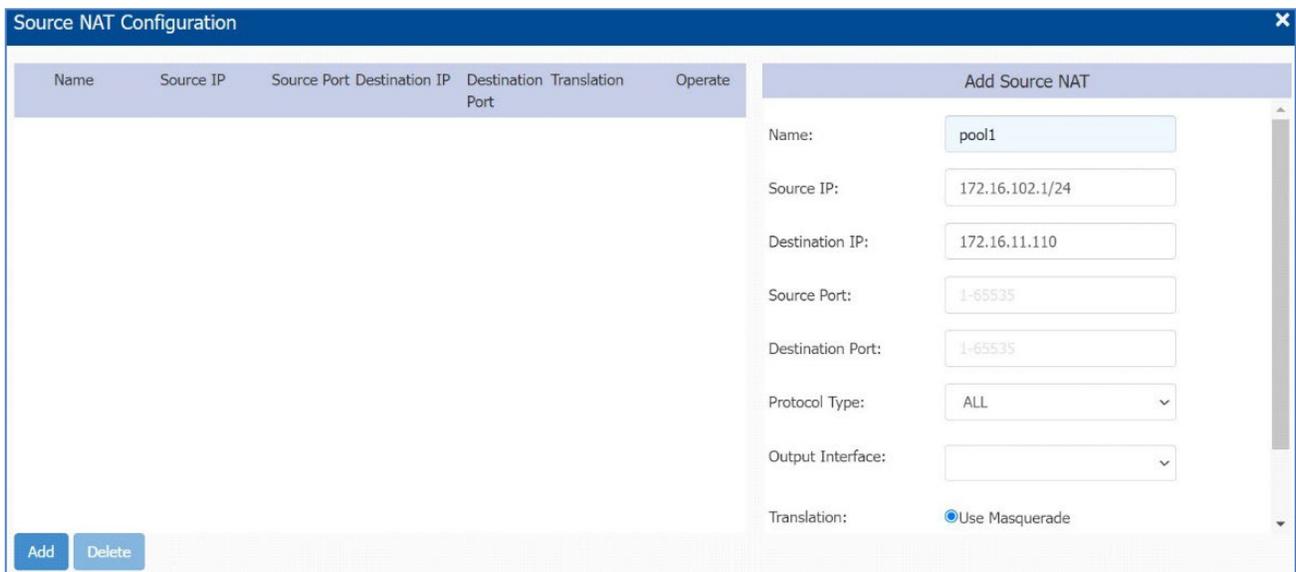


图 122：配置 Source NAT

关键参数描述如下：

参数	描述
Name	Source NAT 规则名称。
Source IP	映射 NAT 源地址，可以是单个 IP 或一个 IP 段。
Destination IP	映射 NAT 目的地址，可以是单个 IP 或一个 IP 段。
Source Port	映射 NAT 规则的源端口。
Destination Port	映射 NAT 规则的目的端口。
Protocol Type	映射 NAT 规则的协议类型。
Output Interface	指定 NAT 规则的外部接口。
Translation	使用 Masquerade 将内部 IP 地址转换为网络的接口 IP 地址（网关）。

■ Destination NAT

目标地址转换，用于将内部服务器的IP地址发布到外部网络，使得外部网络的主机可以访问内部服务器的特定服务。您可以通过单击Destination NAT的标题栏来配置Destination NAT，参考图 123。

The screenshot displays the 'Destination NAT Configuration' window. On the left, there is a table with the following columns: Name, Source IP, Source Port, Destination IP, Destination Port, Translation, and Operate. The table is currently empty. To the right of the table is a configuration panel titled 'Add Destination NAT'. This panel contains several input fields and a radio button: 'Source Port' (text input with '1-65535'), 'Destination Port' (text input with '1-65535'), 'Protocol Type' (dropdown menu with 'ALL'), 'Input Interface' (dropdown menu with 'vlan102'), and '*Translation' (radio button selected for 'Specify Network Addr', with sub-fields for 'IP' (text input with 'x.x.x.x') and 'Port' (text input with '1-65535')). At the bottom of the configuration panel are 'Cancel' and 'Save' buttons. At the bottom left of the main window are 'Add' and 'Delete' buttons.

图 123: 配置 Destination NAT

关键参数描述如下：

参数	描述
Name	Destination NAT 规则名称。
Source IP	映射 NAT 源地址，可以是单个 IP 或一个 IP 段。
Source Port	映射 NAT 规则的源端口。
Destination IP	映射 NAT 目的地址，可以是单个 IP 或一个 IP 段。
Destination Port	映射 NAT 规则的目的端口。
Protocol Type	映射 NAT 规则的协议类型。
Input Interface	指定 NAT 规则的内部接口。
Translation	<ul style="list-style-type: none">▶ IP: 将外部 IP 地址映射成内部的一个地址。▶ Port: 外部 IP 地址将被映射到的内部端口。

8 系统管理

System页面主要展示了当前DAP847-XXA集群的基本信息，包括DAP集群属性、系统管理帐户、系统时间和系统日志，您也可以对DAP847-XXA的系统信息进行配置的查询和修改。

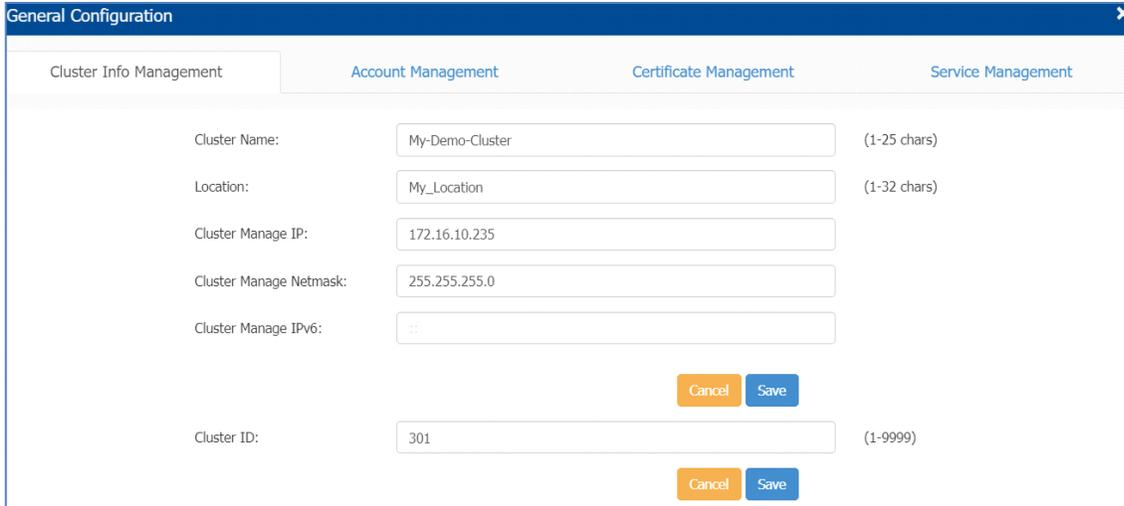
本章节主要包含以下内容：

- ▶ [管理集群信息](#)
- ▶ [账户管理](#)
- ▶ [证书管理](#)
- ▶ [系统服务配置](#)
- ▶ [配置系统时间](#)
- ▶ [配置Syslog系统日志](#)

8.1 管理集群信息

如果要修改DAP847-XXA集群的相关配置，如Cluster Name， Location信息等，可以进入**System**→ **General Configuration**配置页面进行配置或修改群集属性。

管理员可以手动给Cluster设置一个Cluster Management IP地址，这个Cluster Management IP地址用于管理DAP-XXA集群，是分配给PVM的一个虚拟的IP地址。



The screenshot shows the 'General Configuration' window with the 'Cluster Info Management' tab selected. It contains the following fields and values:

- Cluster Name: My-Demo-Cluster (1-25 chars)
- Location: My_Location (1-32 chars)
- Cluster Manage IP: 172.16.10.235
- Cluster Manage Netmask: 255.255.255.0
- Cluster Manage IPv6: ::
- Cluster ID: 301 (1-9999)

Each field has a 'Cancel' button (orange) and a 'Save' button (blue) to its right.

图 124: 集群信息管理

关键参数描述如下:

参数	描述
Cluster Name	DAP847-XXA 集群的名称。
Location	DAP847-XXA 集群的位置。
Cluster Management IP	DAP847-XXA 集群管理的虚拟 IP 地址。
Cluster Management Netmask	DAP847-XXA 集群管理 IP 的子网掩码。
Cluster Management IPv6	DAP847-XXA 集群管理的虚拟 IPv6 地址。
Cluster ID	DAP847-XXA 集群的标识，默认集群 ID 为 100。

The DAP847-XXA集群信息将会显示在页面顶部，如下图所示。

WLAN			AP		
WLAN Name	Status	Clients	Primary Name	Status	Clients
My-wifi-test	on	0	AP-C0:70	Working	0

图 125: 集群信息展示

注意: Cluster Management IP是为DAP847-XXA Cluster Manager配置的一个静态IP地址。您可以通过有线网络或无线网络访问以下URL来管理群集：
<http://IP:8080>或<https://IP>。

Cluster Management IP配置在AP集群的PVM上的IP地址。请确保PVM上的管理IP可从配置终端（浏览器）是路由可达的。为了避免地址冲突，建议您从DAP847-XXA集群中选择一个空闲的IP地址，并将其配置为管理IP地址。

8.2 账户管理

8.2.1 管理Web GUI账户

DAP847-XXA中内置有3个具有不同权限的账户，可以通过这些账户登录到AP Cluster Manager:

- ▶ **Administrator:** Administrator账户具有最高权限，能够查看并修改系统的配置，包括启用或禁用Viewer用户、删除配置以及将DAP847-XXA恢复出厂状态等。
- ▶ **Viewer:** Viewer 账户只有查看DAP847-XXA集群配置的权限。
- ▶ **Guest Manager:** 使用Guest Manager账户登陆，只有编辑和查看Guest Portal账户的权限。

这3个账户可以同时登录DAP847-XXA集群。但当同一个账户重复登录时，前一个登录的会话会被强制终止。在缺省状态下，仅有Administrator账户是启用的，Viewer账户和Guest Manager账户是禁用状态

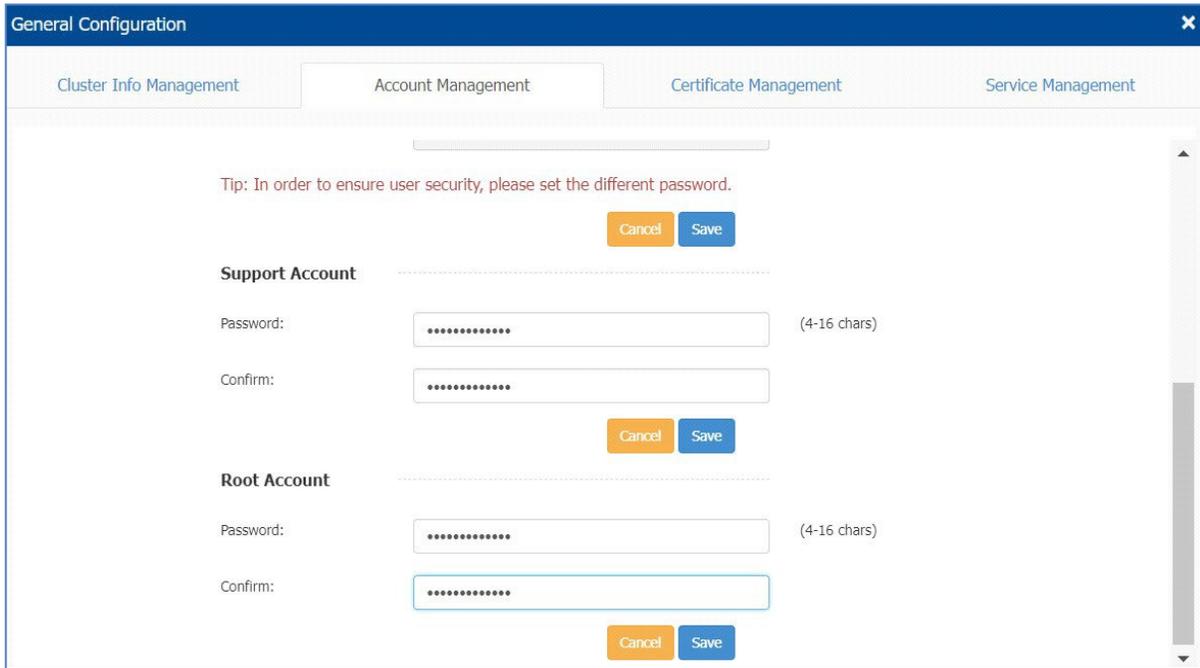
在“**Account Management**”的配置中，您可以选择启用或禁用Viewer帐户，并可以更改Administrator和Viewer的密码，参考图 126。

The screenshot displays the 'General Configuration' window with the 'Account Management' tab selected. It shows the configuration for three user accounts: Administrator, Viewer, and Guest Manager. Each account has a 'Password' field and a 'Confirm' field, both masked with dots and labeled '(4-16 chars)'. The Viewer and Guest Manager accounts also have radio buttons for 'Enable' (selected) and 'Disable'. A tip at the bottom states: 'Tip: In order to ensure user security, please set the different password.'

图 126: 账户管理

8.2.2 管理CLI账户

DAP847-XXA中同样内置了两个CLI用户，可以使用不同的权限登录DAP847-XXA命令行界面：**support**用户和**root**用户。Administrator可以更改这两个CLI用户的登录密码，其中root密码是一个仅由客户持有的一串字符，这一串字符用于DAP847-XXA生成真正的root访问凭据，参考图 127。



The screenshot shows a web interface titled "General Configuration" with a close button (X) in the top right corner. Below the title bar are four tabs: "Cluster Info Management", "Account Management" (which is selected), "Certificate Management", and "Service Management".

Under the "Account Management" tab, there is a tip: "Tip: In order to ensure user security, please set the different password." Below the tip are "Cancel" and "Save" buttons.

The "Support Account" section contains two password fields: "Password:" and "Confirm:". The "Password:" field has a "(4-16 chars)" label to its right. Below these fields are "Cancel" and "Save" buttons.

The "Root Account" section also contains two password fields: "Password:" and "Confirm:". The "Password:" field has a "(4-16 chars)" label to its right. Below these fields are "Cancel" and "Save" buttons.

图 127: CLI 账户管理

注意：为了安全起见，建议管理员在使用DAP847-XXA前先修改root用户和support用户密码。

8.3 证书管理

DAP847-XXA支持如下2种类型的内置证书，系统管理员可以根据客户要求使用自定义证书：

- ▶ **内置Web服务器：**该证书用于在web浏览器和DAP847-XXA Web服务器之间建立安全连接，进行https访问管理。默认情况下，Belden会生成一个内置的CA证书，其域为“find.dap.com”。用户需要使用Open SSL来生成CA证书并替换默认证书（由于登录URL无法更改，因此用户需要使用域“find.dap.com”作为自己的证书）。
- ▶ **内置Portal Server：**该证书用于在portal页面和DAP847-XXA Web服务器之间建立安全连接，以帮助保护用户登录信息不被窃取。用户可以定义Portal登录URL并相应地替换证书。

配置路径：**System**→**General Configuration** → **Certificate Management**

The screenshot shows a web interface for adding a certificate. The form is titled "Certificate" and is separated from the rest of the page by a dashed line. It contains the following fields and controls:

- Name:** A text input field with a placeholder and a label "(4-20 chars)".
- Certificate Type:** A dropdown menu currently showing "Internal Web Server(Domain)".
- Certificate File:** A file selection control with a "Choose File" button and the text "No file chosen".
- Password:** A text input field with a placeholder "Please enter a valid 4-128 digits of English letters, num" and a label "(4-128 chars)".
- Confirm:** A text input field for password confirmation.
- Certificate Format:** A dropdown menu currently showing "PEM".

At the bottom of the form, there are two buttons: "Cancel" (orange) and "Add" (blue).

图 128：证书管理

8.4 系统服务配置

DAP847-XXA支持以下2种服务类型，这些服务可以根据您的需求单独启用或禁用，参考图 129。默认情况下，以下两项服务都处于禁用状态。

- ▶ **IPv6 L3 Forwarding:** 如果启用了IPv6服务，则在客户端和其他网络设备之间进行3层IPv6数据转发
- ▶ **IGMP Snooping:** DAP847-XXA上IGMP Snooping功能的管理状态，是运行在二层设备上的组播约束机制，用于管理和控制组播组。

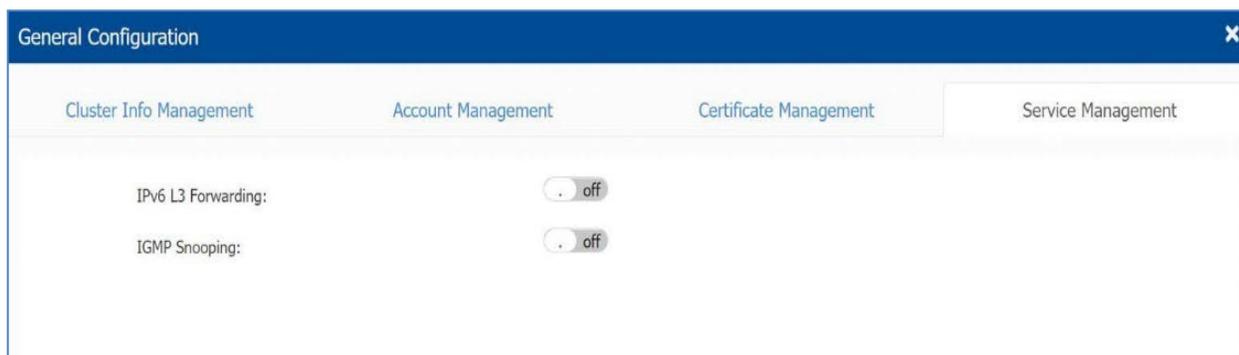


图 129: 系统服务配置

8.5 配置系统时间

正确的系统时间对于DAP847-XXA的运行是非常重要的，DAP847-XXA和其它网络设备的通信以及系统日志等，特别是对于故障排除，都依赖于一个准确的系统时间。

管理员可以在**System → System Time**页面完成系统时间的配置。

NTP（RFC 1305-Network Time Protocol）是一种用于在网络上的设备之间进行时间同步的网络协议。NTP的主要功能是提供精确的时间同步服务，使得计算机系统能够以秒为单位进行同步。它使用网络时间协议（Time Protocol）来传输时间信息，并通过比较来自不同时钟源的时间信息来计算出最佳的时间。NTP通过使用GPS、原子钟等高精度时钟来同步网络中的计算机系统，并提供了精确的时间同步。它可以在全球范围内使用，并支持多种网络协议，如UDP、TCP等。

如果您的网络中有一个专用NTP服务器，则建议将其配置为最高优先级，排列到NTP服务器列表的顶部。如果您的网络中没有专用NTP服务器，可以根据实际情况配置一个可用的NTP服务器，并设置为最高优先级。

配置后，群集中的DAP847-XXA将会每15分钟与NTP服务器同步一次时间。

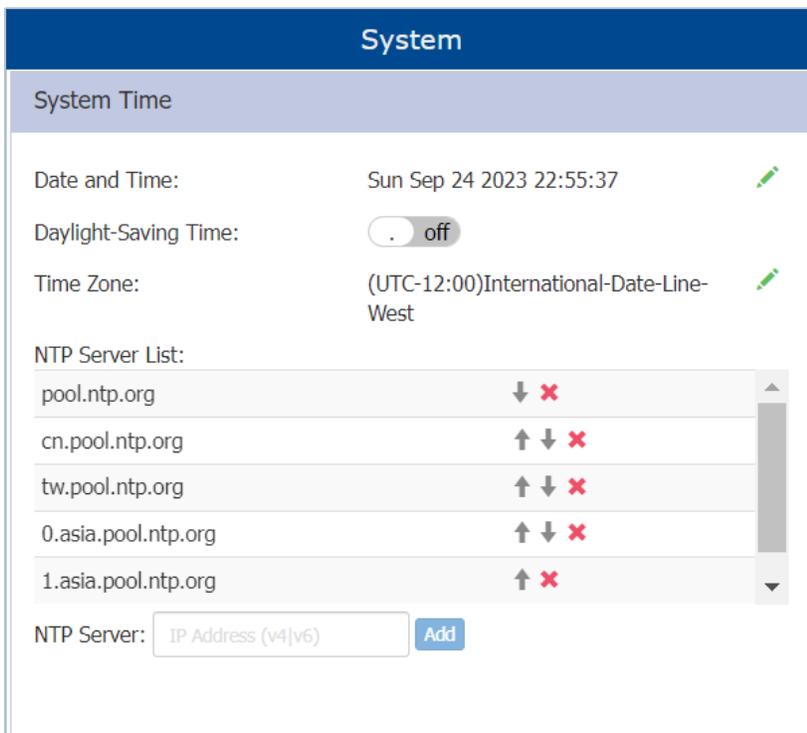


图 130: 配置系统时间

根据需要，用户还可以指定DAP847-XXA的“**Daylight-Saving time**”和“**Time**

Zone”，更准确的设置当地的时间，在支持**Daylight-Saving time**的时区中会自动启用夏令时，见图 131。

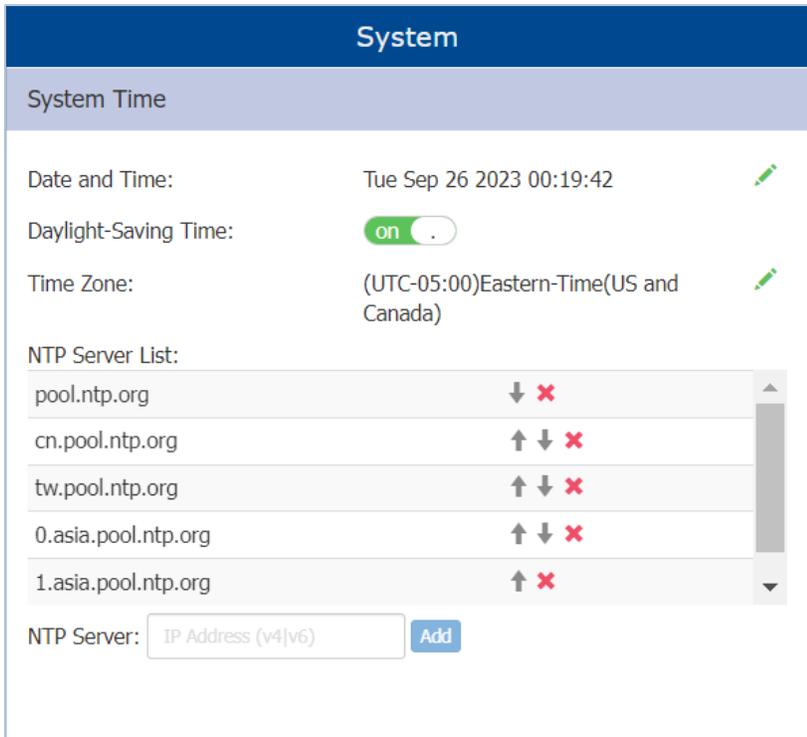


图 131：开启夏令时

注意：建议在添加NTP服务器之前，先检查NTP服务器是否可用，以确保时间能够正确同步。如果没有正确配置NTP服务器或NTP服务器不可达，则DAP847-XXA重启后可能会导致使用错误的时间。

8.6 配置Syslog系统日志

Syslog是一种用于系统日志的标准协议，通常用于记录系统和应用程序的日志信息。它被广泛用于网络设备、操作系统和应用程序中，用于收集、记录和传输日志数据，以便进行系统管理和故障排除。

Syslog使用UDP协议传输日志信息，通常默认使用端口**514**。它支持多种消息格式和优先级，可以根据消息的重要性和类型进行过滤和选择性地记录。

通过**Syslog**，管理员可以实时监控系统状态、跟踪应用程序的运行情况、发现安全事件并进行审计等。

通过**System**→**Syslog & SNMP**→**Syslog**页面查看日志。

DAP847-XXA的日志符合**Syslog**协议标准，可以在**Syslog**页面查看日志和配置相应的属性，**Syslog**页面上部会显示DAP847-XXA集群生成的“**Error**”及此级别以上的**Syslog**日志信息。

- ▶ **Title:** 日志消息的内容。
- ▶ **Level:** 日志消息的严重程度
- ▶ **Source:** 生成日志消息的DAP847-XXA的IP地址。

当您将光标移动到日志消息的某一行时，会显示出该日志的生成时间。

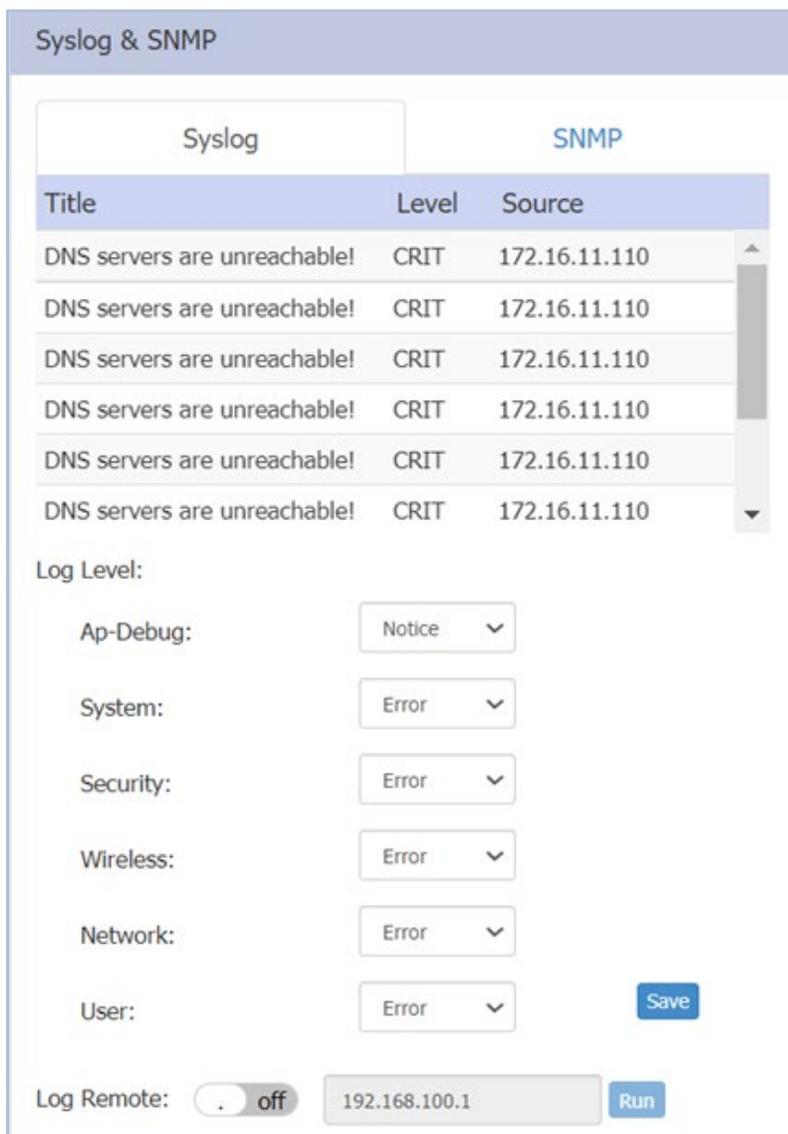


图 132: Syslog 配置

■ Log level

Log level 设置 Syslog 日志消息严重程度。

如果指定了某个级别，则 DAP847-XXA 将生成包括该级别及其以上所有级别的 Syslog 日志消息。也就意味着：

- ▶ 如果 Syslog 消息是按不同的严重程度配置的话，那么在 Notice、Info 和 Debug 级别的日志中也将包含 Warning 级别的日志。
- ▶ Syslog 设置的默认级别为 Notice，系统生成的日志包括 Notice、Warning、Error、Critical、Alert 和 Emergency 这几种级别。

用户可以对不同的模块分别指定不同的日志级别。

参数	描述
AP-Debug	有关DAP847-XXA设备的详细日志。
System	有关DAP847-XXA配置和系统状态的日志。
Security	有关网络安全的日志。
Wireless	有关无线RF的日志。
Network	有关网络状态变化的日志。
User	有关用户的日志。

■ Log remote

DAP847-XXA支持设置远程日志服务器用来接收并存储DAP847-XXA发送的Syslog日志消息。

注意： Syslog分为8个级别，最高级别0为Emergency，最低级别7为Debug/All。Syslog严重级别的定义如下：

级别	严重程度	关键词	描述
0	Emergency	EMERG	系统不可用
1	Alert	ALERT	应立即进行修正
2	Critical	CRIT	严重
3	Error	ERR	错误
4	Warning	WARNING	警告
5	Notice	NOTICE	通知
6	Info	INFO	信息类消息
7	Debug/All	DEBUG	调试类消息

表 13: Syslog 严重级别定义

8.7 配置SNMP

SNMP（Simple Network Management Protocol）是一种用于网络管理的标准协议，它用于在计算机网络系统中管理和监控网络设备的配置和运行状态等信息，以确保网络的可靠性并保持稳定的性能。

SNMP协议定义了Network Management System（网络管理系统NMS）和代理（Agent）之间的通信方式，网络管理系统（NMS）是用于管理和监控网络的管理员计算机，而Agent是运行在DAP847-XXA设备上的应用程序，用于收集设备的状态和性能信息并将其发送到NMS。

SNMP有三个版本，分别是SNMPv1，SNMPv2c和SNMPv3。

- ▶ SNMPv1是最早的版本，提供了基本的网络管理功能，但不太安全。
- ▶ SNMPv2c是SNMPv1的改进版本，增加了共同体概念（community concept），提高了安全性。
- ▶ SNMPv3则引入了基于用户的安全模型（USM），提供了更高级别的安全性，

目前DAP847-XXA支持SNMPv2c和SNMPv3两个版本，由于SNMPv1较低的安全性，目前的版本中已不再支持。

SNMP Trap是一种通知协议，用于在受管理的设备上产生主动通知，告知网络管理系统（NMS）发生了特定事件或错误，而无需等待网络管理系统（NMS）的再次轮询。

SNMP的相关参数可以在**System → Syslog&SNMP → SNMP**页面中进行配置。

8.7.1 配置SNMPv2c

如果选择SNMPv2c版本，需要配置如下参数：

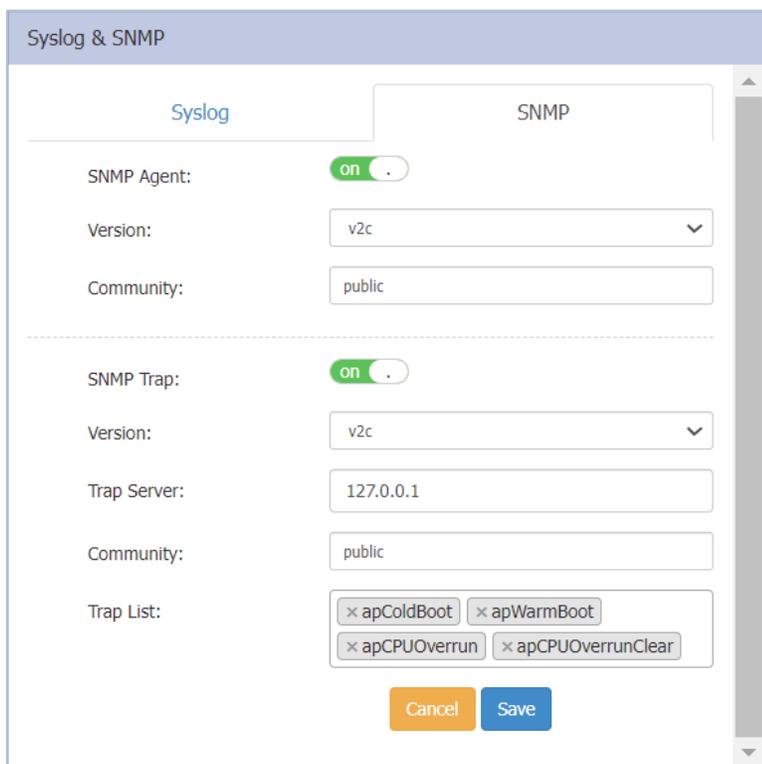


图 133: NMPv2c 配置

■ 配置 SNMPv2c Agent

参数	描述
SNMP Agent	启用或禁用DAP847-XXA上的SNMP代理。
Version	选择SNMP版本v2c。
Community	SNMP Agent代理和网络管理系统（NMS）之间用于通信的凭据，双方的community值必须完全一致，否则将无法进行正常的通信。

■ 配置 SNMPv2c Trap

参数	描述
SNMP Trap	启用或禁用DAP847-XXA向网络管理系统 (NMS)发送Trap。
Version	选择SNMP版本v2c。
Trap Server	接收 SNMPv2c trap的网络管理系统（NMS）。
Trap List	指定要发送的Trap类型。

8.7.2 配置SNMPv3

如果选择SNMPv3版本，需要配置如下参数：

The screenshot shows the 'Syslog & SNMP' configuration window. The 'SNMP' tab is selected. Under 'SNMP Agent', the 'SNMP Agent' toggle is turned on, 'Version' is set to v3, 'Username' is 'snmpstest', and there are two masked 'Passphrase' fields. Under 'SNMP Trap', the 'SNMP Trap' toggle is turned on, 'Version' is set to v3, 'Trap Server' is '127.0.0.1', 'Username' is 'trapstest', and there are two masked 'Passphrase' fields. The 'Trap List' section includes checkboxes for 'apColdBoot', 'apWarmBoot', 'apCPUOverrun', and 'apCPUOverrunClear'. 'Cancel' and 'Save' buttons are at the bottom.

图 134: SNMPv3 配置

■ 配置 SNMPv3 Agent:

参数	描述
SNMP Agent	启用或禁用DAP847-XXA上的SNMP代理。
Version	选择SNMP版本v3。
Username	标识和认证SNMP管理系统的用户。
Passphrase	用于对SNMPv3进行身份验证的密码，该密码必须至少包含8个字符（空格除外）。
Confirm	确认密码。

■ 配置 SNMPv3 Trap

参数	描述
SNMP Trap	启用或禁用DAP847-XXA向网络管理系统(NMS)发送Trap。
Version	选择SNMP版本v3。
Trap Server	接收 SNMPv3 trap的网络管理系统(NMS)。
Username	标识和认证SNMP管理系统的用户。
Passphrase	用于对SNMPv3进行身份验证的密码，该密码必须至少包含8个字符（空格除外）。
Confirm	确认密码。
Trap List	指定要发送的Trap类型。

9 无线管理

Wireless页面用于展示DAP847-XXA无线的统计信息和配置信息，以及Radio层面相关的高级功能：如RF、wIDS/wIPS（无线入侵检测系统/无线入侵预防系统）和无线性能优化。



图 135: Wireless 页面

本章节主要包含如下3个方面的内容：

- ▶ RF配置
- ▶ wIDS/wIPS
- ▶ 无线性能优化

9.1 RF配置

RF页面用于监控无线信道的使用情况以及常用的RF相关功能的配置，如信道、发射功率和Short GI的配置等。

RF页面有两种模式：基本模式和高级模式。单击RF页面的标题栏，可以从基本模式进入到高级配置模式，在该模式下，您可以对DAP847-XXA集群做全局RF配置，也可以根据需求分别针对每台DAP847-XXA单独进行RF的配置。

在基本模式下，只展示2.4 GHz和5 GHz频段的信道分布监控信息，使用不同的颜色表示不同的信道。当您将光标移动至饼图上时，将会显示连接到2.4 GHz或5 GHz频段的客户端的统计信息。

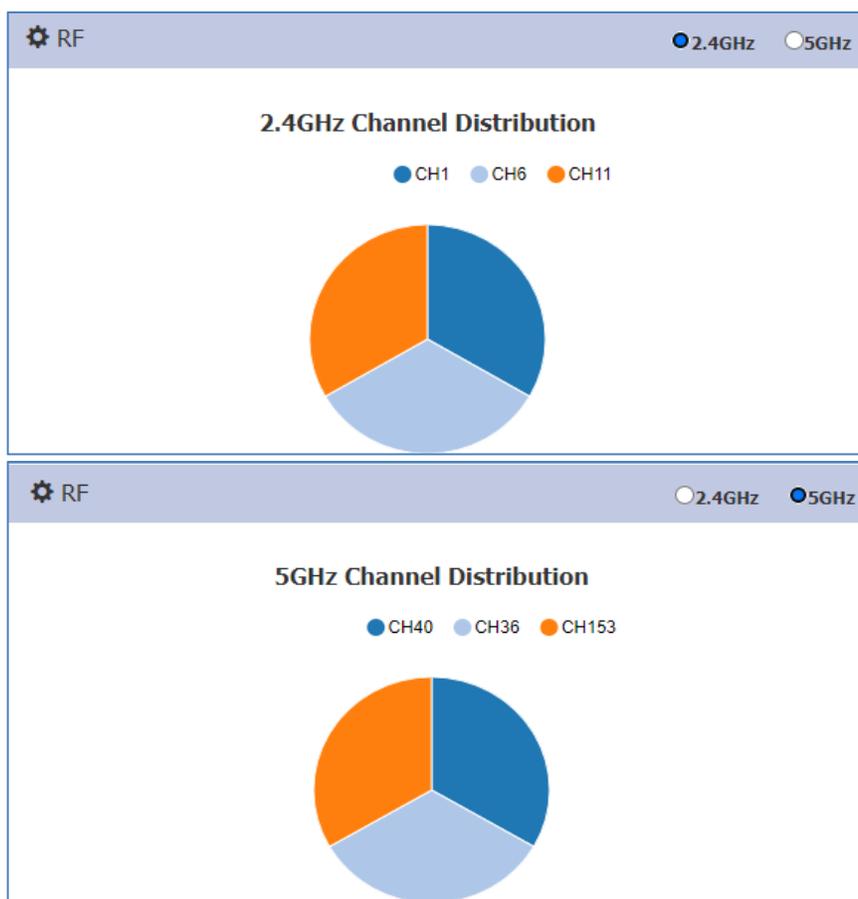


图 136: RF 配置

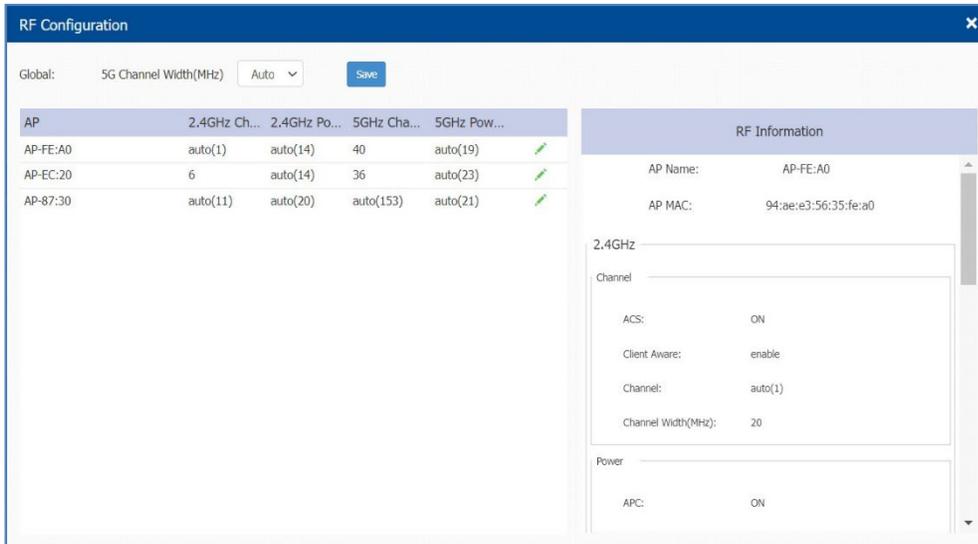


图 137: RF Configuration 页面

RF配置页面显示了集群中DAP847-XXA的信道列表和发射功率，当在列表中选择 一个DAP847-XXA时，会在右侧信息栏中显示其详细的RF信息，包括信道，功率， 信道带宽等。

全局配置可用于更改集群中DAP847-XXA在5 GHz信道的带宽配置，参考图 138， 您也可以选择指定的设备单独更改其信道宽度，参考图 142。

如果同时存在全局设置和私有配置，则最终生效的是DAP847-XXA的私有配置。

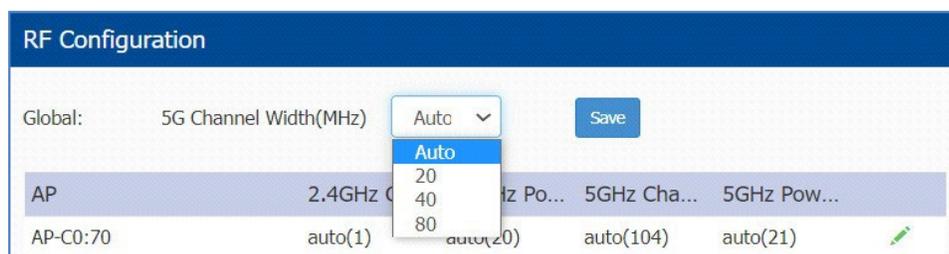


图 138: 全局 5 GHz 信道带宽配置

注意：关于160MHz的信道宽度，由于受支持的DAP型号、信道范围及供电模式等 限制，只支持私有配置。不支持在全局配置。

9.1.1 修改DAP847-XXA的功率和信道

在RF配置页面中，您可以修改DAP847-XXA的传输功率和工作信道，参考图 139。默认情况下，工作信道和发射功率由Dynamic Radio Management（DRM）自动管理，用于动态地管理和优化无线系统的性能。它通过实时监测无线环境和系统的负载，以及根据这些信息做出决策，来提高无线系统的效率和可靠性。

如果要手动设置DAP847-XXA的工作信道和传输功率值，需要禁用自动信道选择（ACS）和自动功率控制（APC）。在手动模式下，AP发射功率可以以1dB的步长进行调整。

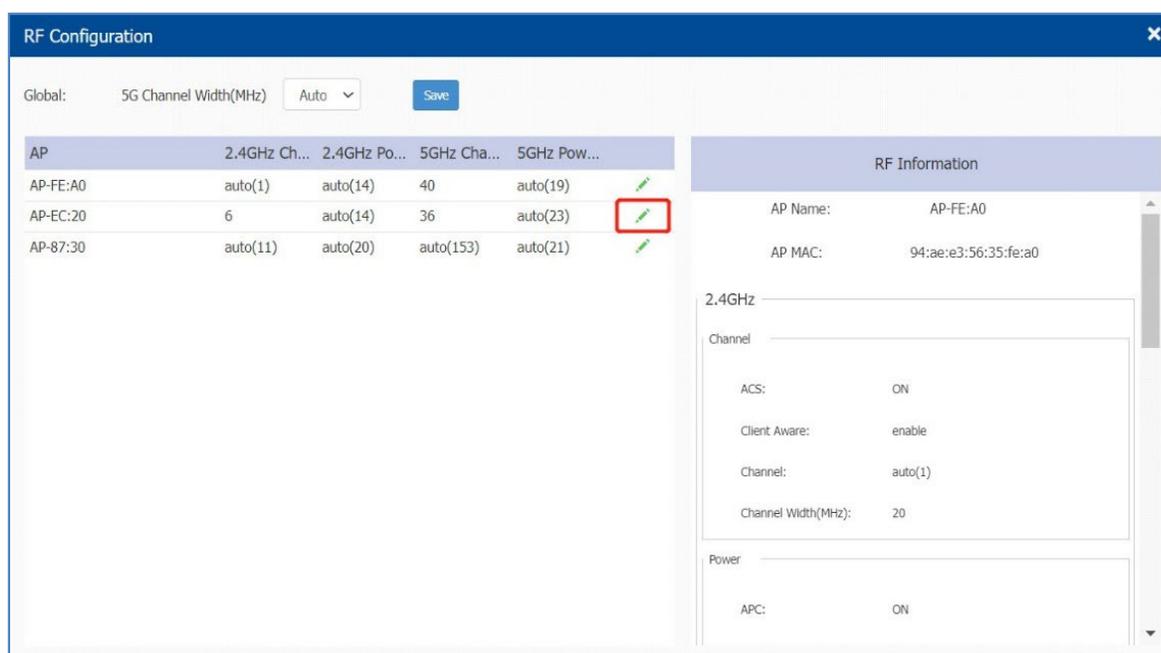


图 139: RF 配置

为了最大程度减少低功率或DFS信道冲突存在的潜在风险，您也可以对DAP847-XXA指定信道列表或设置一个自动功率选择的范围，这样可以有针对性的对一些特殊场景进行优化，参考图 140。

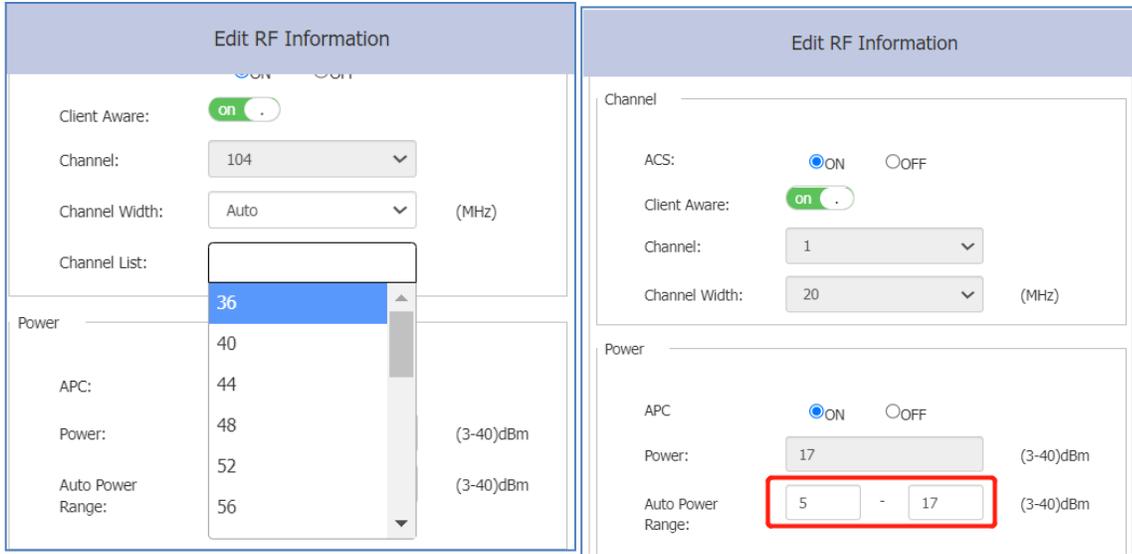


图 140: 设置 Channel List 和 Auto Power Range

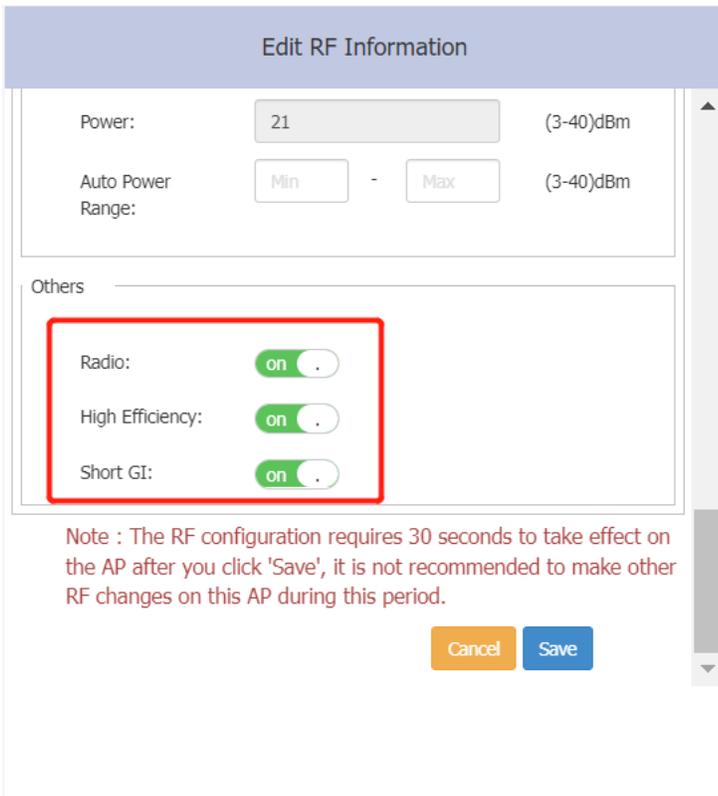


图 141: 其他 RF 配置

■ RF Configuration 页面的配置参数介绍

参数	描述
Client Aware	如果开启了“ Client Aware ”功能，当有无线客户端连接的情况下，即使符合条件，DAP847-XXA也不会切换其工作信道，除非检测到RADAR等高优先级事件。如果禁用该功能，DAP847-XXA可能会切换为更优的信道，不过这有可能会暂时中断当前客户端业务。
Radio	开启或关闭Radio，可针对2.4 GHz和5 GHz频段分别配置。
Short GI	启用/禁用Short Guard Interval。在基于IEEE 802.11 OFDM的无线通信中，Guard Interval（GI）用于确保在设备发送的连续数据符号之间发生不同的传输。IEEE 802.11 OFDM中使用的标准的信号GI是800纳秒。为了提高数据速率，IEEE 802.11标准增加了对400纳秒GI的可选支持，这可以使数据传输速率提高约11%。然而，当RF信道的延迟超过短GI时，或者当发射机和接收机之间的定时同步不精确时，使用Short Guard Interval将导致更高的错误率。默认情况下，短GI在无线电台上处于启用状态。如果多径效应太严重（金属或其他反射材料太多），则建议关闭“Short Guard Interval”功能。
High Efficiency	开启或关闭802.11ax模式。当关闭该模式，则DAP847-XXA将从IEEE 802.11ax模式切换到IEEE 802.11ac模式。该操作的主要目的是解决部分老旧的IEEE 802.11ac终端可能出现的与DAP847-XXA兼容性的问题。

9.1.2 配置信道带宽

DAP847-XXA支持20 MHz、40 MHz、80 MHz和160 MHz信道带宽，您可以在DAP847-XXA的私有RF配置中设置信道带宽，参考图 142。

注意：关于160 MHz信道带宽有以下一些限制：

- ▶ 160 MHz仅在信道范围为36至64和100至128的5 GHz无线电上受支持。
- ▶ 只有当AP由电源适配器或POE+（或更高）供电模式时，才支持160MHz。
- ▶ 仅支持静态160 MHz信道宽度。自动频道选择将不使用160 MHz频道。

The screenshot displays the 'Edit RF Information' configuration interface. It is divided into two main sections: 'Channel' and 'Power'.
In the 'Channel' section:
- 'ACS' is set to OFF.
- 'Client Aware' is set to on.
- 'Channel' is set to 36.
- 'Channel Width' is set to 20, with a dropdown menu open showing options 20, 40, 80, and 160. The '20' option is highlighted in blue.
- 'Channel List' is empty.
In the 'Power' section:
- 'APC' is set to ON.
- 'Power' is set to 23 (3-40)dBm.
- 'Auto Power Range' is set to Min - Max (3-40)dBm.

图 142: 配置 160 MHz 信道带宽

9.1.3 配置DAP847-XXA天线

在射频配置页面中，您可以配置DAP847-XXA天线的增益和5G Radio上的MIMO模式，如图 143所示：

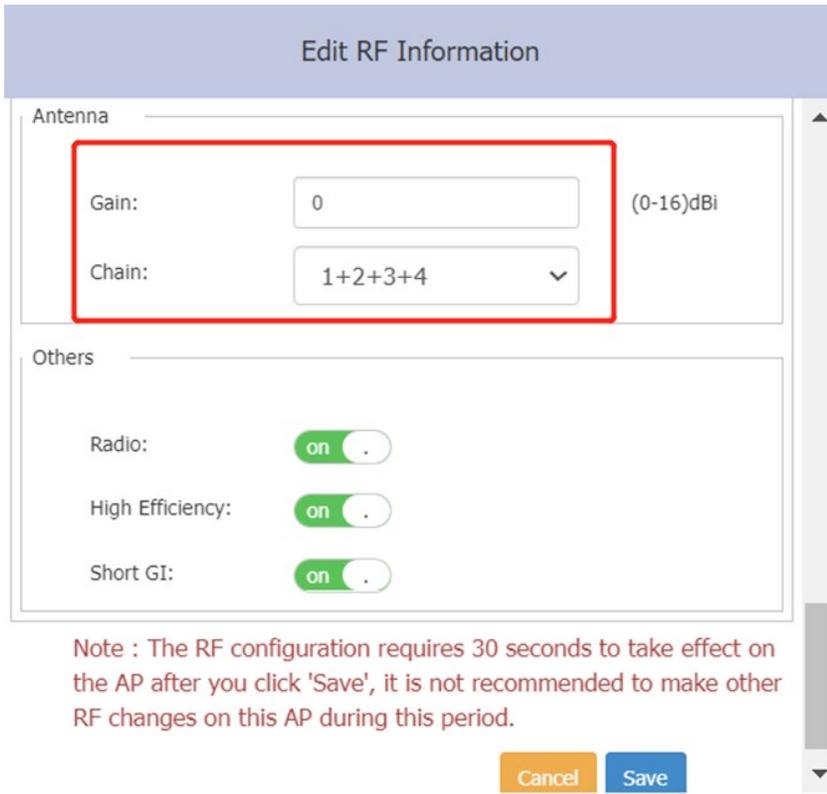


图 143: DAP847-XXA 天线配置

参数	描述
Gain	指定外部天线的增益值。
Chain	表示DAP847-XXA的MIMO模式，即外部天线的配置： <ul style="list-style-type: none">• 1 代表 MIMO 模式为 1x1, 对应的天线接口为 ANT1• 2 代表 MIMO 模式为 1x1, 对应的天线接口为 ANT2• 3 代表 MIMO 模式为 1x1, 对应的天线接口为 ANT3• 4 代表 MIMO 模式为 1x1, 对应的天线接口为 ANT4• 1+2 代表 MIMO 模式为 2x2, 对应的天线接口为 ANT1+ANT2• 1+4 代表 MIMO 模式为 2x2, 对应的天线接口为 ANT1+ANT4• 1+2+3 代表 MIMO 模式为 3X3, 对应的天线接口为 ANT1+ANT2+ANT3• 1+2+3+4 代表 MIMO 模式为 4X4, 对应的天线接口为 ANT1+ANT2+ANT3+ANT4

9.1.4 开启/关闭DAP847-XXA的无线射频

您可以通过单击Radio on/off按钮来关闭集群中DAP847-XXA设备的2.4 GHz或5 GHz无线射频模块。以减少无线干扰或用于其他目的，请参考图 144。

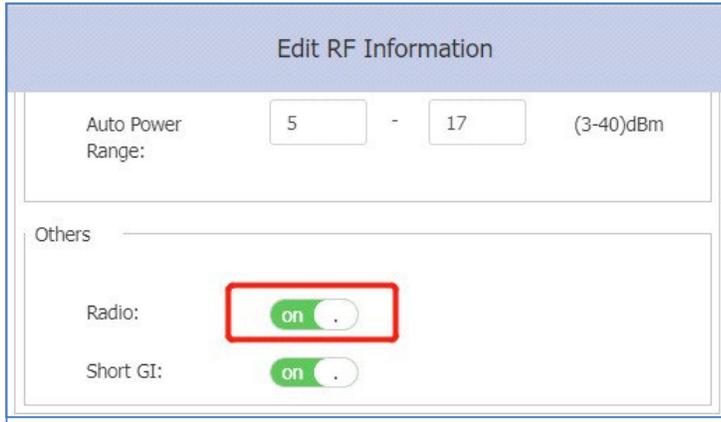


图 144： 开启或关闭无线射频模块

9.2 wIDS/wIPS

DAP847-XXA在集群模式下能够提供基本的wIDS/wIPS功能，如果需要使用其更多高级功能，建议使用DAC模式并购买相应的License。

- ▶ **wIPS: Wireless Intrusion Prevention System**，无线入侵防御系统，是一种用于检测和防御无线网络中的安全威胁的系统。它能够实时监测和分析无线网络的传输数据，并检测和阻止针对无线网络的恶意攻击和未经授权的访问。wIPS是为 IEEE 802.11 协议开发的第二层协议检测和保护功能。wIPS 通过信道监控、分析和处理来检测威胁网络安全、干扰网络服务和影响网络性能的无线行为或设备。它提供了针对入侵无线设备的对策和一套完整的无线网络安全解决方案。
- ▶ **wIDS: Wireless Intrusion Detection System**，无线入侵检测系统，是一种用于检测无线网络中可能存在的安全威胁的系统。它通过分析无线网络的传输数据来检测任何未经授权的访问、恶意攻击或异常行为。与 wIPS（无线入侵防御系统）不同，wIDS 侧重于检测潜在的威胁，而 wIPS 则更注重防御和阻止这些威胁。wIDS 可以在早期检测恶意用户未经授权的访问和入侵。它还保护企业网络 and 用户免受无线网络上未经授权的设备的攻击。wIDS 可以在不降低网络性能的情况下监控无线网络，并对各种未经授权的访问提供实时预防。
- ▶ **Rogue Suppress: DAP847-XXA 支持通过向 Rogue AP 发送带有客户端 MAC 地址的 de-authentication 帧来阻止客户端连接到 Rogue AP。由此可以断开已经连接到 Rogue AP 的客户端的连接。如果一个已知的 AP 设备被确认为非干扰 AP 或合法 AP，您可以点击列表中的“Trust”，如图 145 所示，将该 AP 添加到 Allowlist 中。默认情况下，该功能为 Disable 状态，参考图 146。**

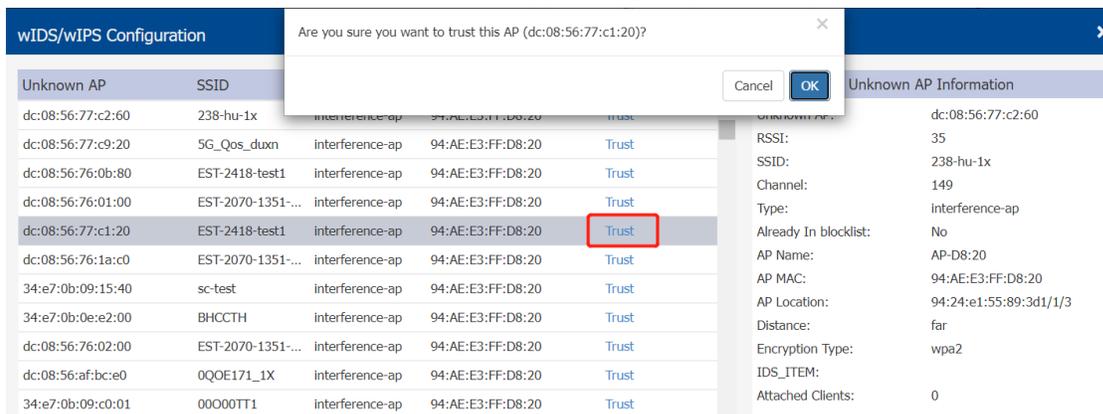


图 145: Trust AP

- ▶ **Dynamic Blocklist:** 如果启用了 Dynamic Blocklist 功能，则检测到的 ad-hoc 设备将会自动添加到 DAP847-XXA 的 Dynamic Blocklist 中。这能够防止 ad-hoc 设备将其角色改变为客户端并获得对 DAP847-XXA 无线网络的访问。默认情况下 ad-hoc 设备不会自动添加到 Dynamic Blocklist 中，参考图 149。
- ▶ **Wireless Attack Detection:** 如果启用了 Wireless Attack Detection，DAP847-XXA 将检测来自外部 AP 的未经授权的访问，缺省情况为关闭状态，参考图 146。

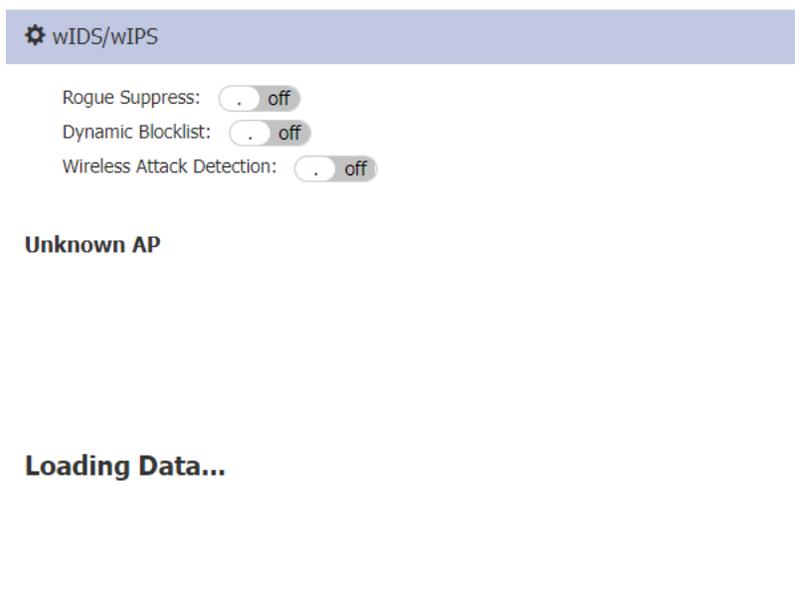


图 146: wIDS/wIPS 页面

- ▶ **Rogue AP:** Rogue AP 是指未经授权的无线访问点（AP），通常由员工未经授权搭建，以提供无线互联网访问。由于这些 AP 未经过正式授权，因此它们可能会对企业的网络安全造成威胁。Rogue AP 可能会被恶意攻击者利用，以窃取敏感信息、进行网络攻击等。如一台插入网络有线侧的未经授权的 AP，或者是与 DAP847 集群广播相同 SSID 的外部干扰 AP，Rogue AP 通常被认为是 DAP847 集群的安全威胁。
- ▶ **Interfering AP:** 在无线环境中能够看到但未连接到有线网络的 AP。干扰 AP 潜在地提供 RF 干扰。然而，它不被视为直接的安全威胁，因为它没有连接到有线网络。
- ▶ **Allowlist:** Rogue AP 和 Interfering AP 都是来自外部的未知 AP，可以通过后台扫描检测到并列在未知 AP 列表上。然而，一些检测到的外来接入点是受信

任的接入点，它们不适合被归类为 **Rogue AP** 或 **Interfering AP**。为了避免这种误判的情况，您可以将受信任的 **MAC** 地址或 **MAC-OUI** 添加到 **AP Allowlist** 中，如图 147 所示。如果将外部 **AP MAC** 地址添加到 **Allowlist**，则它将不会显示在未知 **AP** 列表中。

Allowlist	
MAC	
94:ae:e3:*:*:*	✘
00:1f:64:0a:2b:12	✘
00:11:22:33:77:99	✘
dc:08:56:*:*:*	✘

图 147: AP Allowlist

单击 **wIDS/wIPS** 页面的标题栏，您将在 **wIDS/wIPS Configuration** 页面上看到 **Interfering AP** 和 **Rogue APs** 的信息列表，以及有关 **Interfering AP** 和 **Rogue APs** 的更多详细信息，如 **RSSI**、信道和加密类型等，参考图 148。

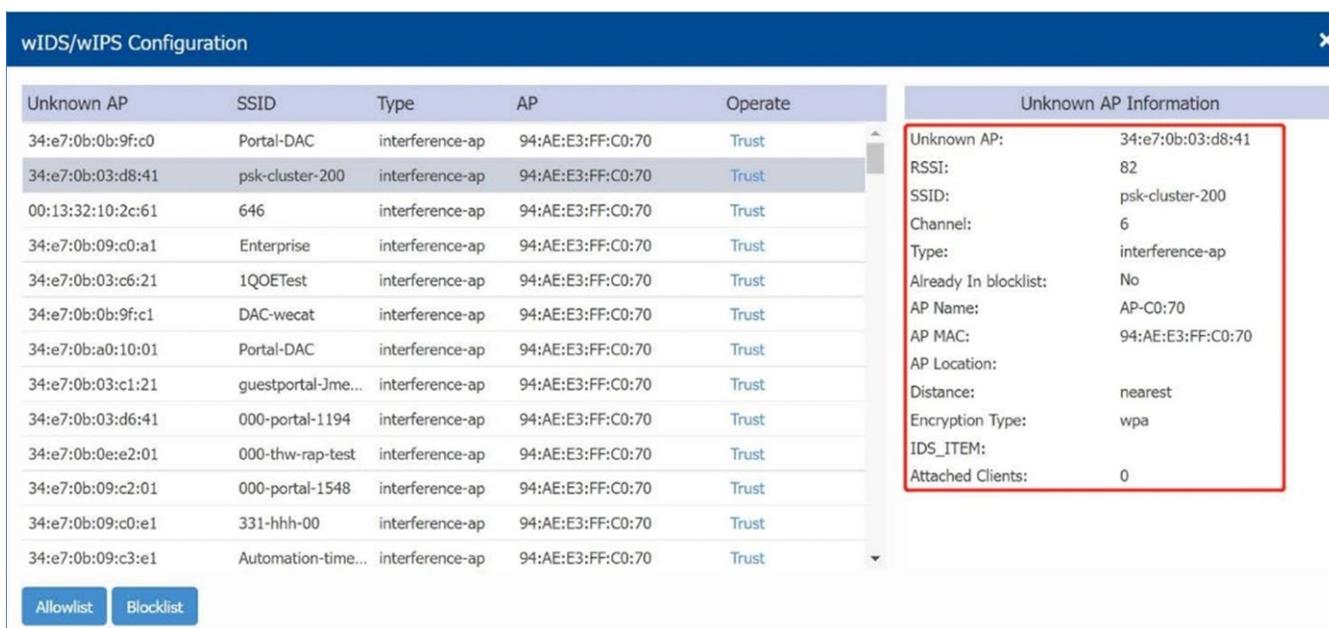


图 148: wIDS/wIPS Configuration 页面

参数	描述
Unknown AP	未知AP的MAC地址。
SSID	未知AP广播的SSID名称。
Type	未知AP（干扰AP或流氓AP）的分类结果。
RSSI	未知AP的RSSI。
Channel	未知AP的工作信道。
Already In Blocklist	ad-hoc设备的标记，取决于“ Dynamic Blocklist ”是否启用。如果启用，则ad-hoc设备将自动添加到阻止列表中，并且标志为true。如果它处于off状态，或者列表中的未知AP不是ad-hoc设备，则标志为（否）。
AP Name	群集中检测到该未知AP的DAP847-XXA设备的名称。
AP MAC	群集中检测到该未知AP的DAP847-XXA设备的MAC地址。
AP Location	群集中检测到该未知AP的DAP847-XXA设备的地址。
Distance	集群中未知AP和检测DAP847-XXA之间的距离，该距离通过未知AP的RSSI计算得出： Nearest - $RSSI \geq (-20 \text{ dBm})$ Near - $(-45 \text{ dBm}) \leq RSSI < (-20 \text{ dBm})$ Far - $(-70 \text{ dBm}) < RSSI < (-45 \text{ dBm})$ Farthest - $RSSI \leq (-70 \text{ dBm})$
Encryption Type	未知AP的SSID的加密方式。
IDS_ITEM	代表一个被wIDS系统识别并标记的特定行为或事件，这些行为或事件可能表明了一个潜在的无线网络安全风险或威胁，如识别出：

参数	描述
	<ul style="list-style-type: none"> ▶ AP仿冒攻击 ▶ 广播解除认证 ▶ 广播解除关联 ▶ 使用有效SSID的Adhoc网络 ▶ 长SSID ▶ AP扮演者攻击 ▶ Adhoc网络 ▶ 无线桥接 ▶ 空探测响应 ▶ 无效地址组合 ▶ 无效原因代码取消认证 ▶ 无效原因代码解除关联 ▶ 有效客户端误关联 ▶ Omerta攻击 ▶ 未加密的有效客户端 ▶ 802.11n 40MHz不耐受设置 ▶ 活动的802.11n Greenfield模式 ▶ DHCP客户端ID ▶ DHCP冲突 Conflict ▶ DHCP名称更改 Name Change ▶ 信道更改 ▶ 无效MAC OUI ▶ 有效SSID误用 ▶ 畸形帧关联请求请求 ▶ 频繁证书
Attached Clients	连接到未知AP的客户端数量，以及每个客户端的MAC地址。

- ▶ **Blocklist:** Blocklist 只可以添加 Rogue AP。如果一个 Rogue AP 被添加到阻止列表中，它就不能改变其角色来充当客户端并访问 DAP847-XXA 无线网络，参考图 149。

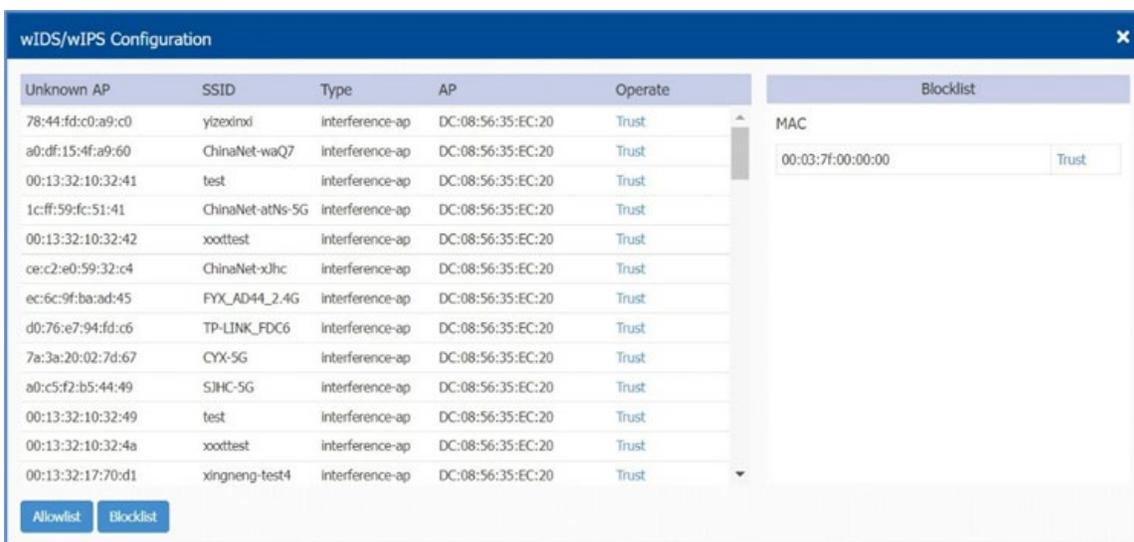


图 149: 添加 Blocklist

参数	描述
Operate	Trust外部AP并将其从未知AP列表中删除的操作。如果对外部AP执行Trust操作，则其MAC地址将被添加到Allowlist中。
Allowlist	认为对DAP847-XXA没有安全威胁的外部AP列表，您可以手动将受信任的MAC地址添加到Allowlist中。
Blocklist	被归类为rogue AP以及仿冒客户端连接DAP847-XXA的外部AP的黑名单列表。如果黑名单功能打开并且检测到特定设备，则这些设备都将自动添加到黑名单列表中。您可以通过“Trust”操作从黑名单列表中删除指定的AP。

注意：如果要使用wIDS/wIPS功能，需要开启背景扫描功能，在一些对安全性要求较高的使用场景，为了提高检测效率和检测性能，建议将背景扫描间隔设置为小于1分钟。

9.3 无线性能优化

无线性能优化用于提高用户的无线服务质量。无线性能优化包括Background Scanning、Band Steering、Load Balance、RSSI Threshold、Roaming RSSI、Voice and Video Awareness以及Airtime Fairness等功能，参考图 150。

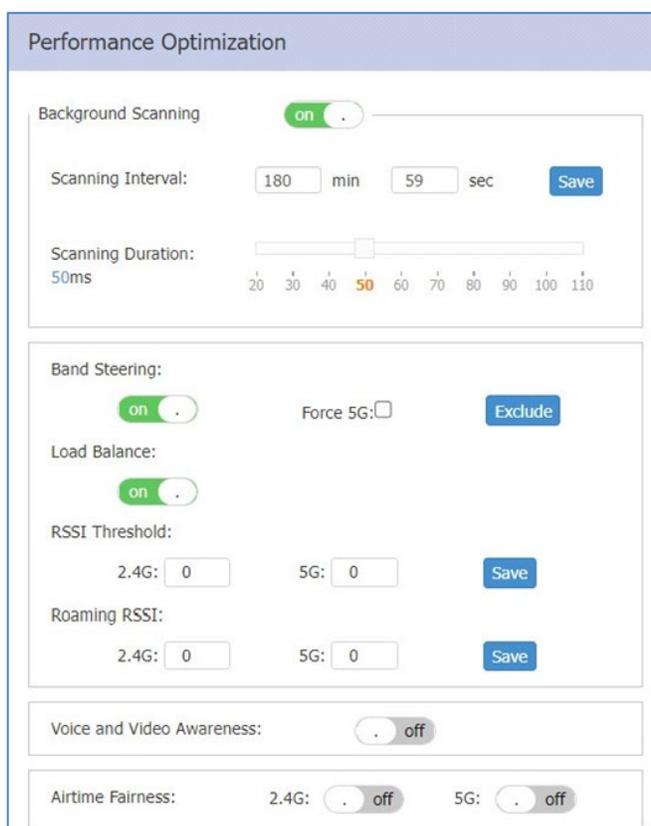


图 150: 无线性能优化配置

- ▶ **Background Scanning:** 无线网络在可能存在干扰网络通信的电气和射频设备的环境中工作。如微波炉、无绳电话，甚至相邻的 Wi-Fi 网络都可能是存在持续性或间歇性干扰的潜在来源。Background Scanning 用于检测 Wi-Fi 网络工作的射频环境，识别干扰并对其来源进行分类。

Background Scanning 是一些高级功能的基础，如 wIDS/wIPS、APC 等。当该功能关闭时，外部 AP 检测和流氓抑制将会停止，DRM 将降低其精度。默认情况下，“背景扫描”处于启用状态。

背景扫描的间隔可以根据部署要求进行配置，配置的范围为 5 秒到 180 分钟。对于高度敏感的数据包延迟情况，建议使用默认值 20 秒作为扫描间隔，如果间隔超过 1 分钟，将会影响到 wIPS 功能的准确性。

注意：为 DAP847-XXA 中预留了一个名为“athmon2”的专用扫描接口，用于完成 2.4 GHz 信道和 5 GHz 信道的背景扫描。

- ▶ **Band Steering:** Band steering 分为 Prefer 5G 和 Force 5G 两种场景。
 - **Prefer 5G:** 相对于 2.4 GHz 频段，如果 DAP847-XXA 探测到连接的无线客户端支持 2.4 GHz / 5 GHz 双频模式，它优先将该客户端引导至 5 GHz 频段上，这样能够减少同信道干扰并能够增加客户端的可用带宽，是因为 5 GHz 频段上有更多可用的信道。默认情况下，Band steering 处于启用状态，当启用 Band steering 且 Force 5G 为关闭状态时，DAP847-XXA 将在 Prefer 5G 模式下工作。

Prefer 5G 基于信道利用率和客户端的数量，当 5 GHz 频段的信道利用率升高并且连接较多客户端时，新的客户端将会连接到信道相对空闲的 2.4 GHz 频段。
 - **Force 5G:** 强制双频工作的无线客户端连接到 5 GHz 频段。打开该功能后，双频工作模式的无线客户端不允许连接到 DAP847-XXA 的 2.4 GHz 频段，只支持 2.4 GHz 频段的客户端才被允许连接到 2.4 GHz 频段。当开启 Band steering 并选择 Force 5G 时，则 DAP847-XXA 在强制 5G 模式下工作。
- ▶ **Exclude:** 将指定的双频客户端排除在 Band Steering 之外，DAP 允许他们自由选择无线频带，在这里您可以添加一个终端的 MAC 地址，或者添加 MAC OUI，将特定类型的终端排除在 Band Steering 之外。
- ▶ **Load Balance:** 是 DAP847-XXA 上的一种网络优化技术，它能够平衡 DAP847-XXA 之间的负载，确保每个设备都能发挥最佳性能，使无线客户端能够获得足够的带宽。

Load Balance 提供了无线客户端在相邻 DAP847-XXA 之间的公平分配，基于客户端的密度、DAP847-XXA 上的信道利用率以及关联客户端的 RSSI 值等信息，主要的目的是将无线客户端从相对繁忙的设备上引导到空闲的设备。根据软件中的设定，客户端密度的阈值为 10，2.4 GHz 和 5 GHz 的信道利用率均为 70%。默认情况下 Load Balance 为开启状态。

- ▶ **RSSI Threshold:** 用于无线接入控制，“RSSI threshold”仅在无线客户端的关联过程中起作用。如果无线客户端的 RSSI 值低于“RSSI threshold”，DAP847-XXA 将不会对客户端做出响应。是否配置该参数与 IEEE 802.11k

功能不受影响。RSSI 值低于阈值的无线客户端不允许接入无线网络。默认情况下，该功能为禁用状态（0），“RSSI threshold”可以分别应用于 2.4 GHz 频段或 5 GHz 频段。通常情况下，建议在高密部署场景中配置“RSSI threshold”，RSSI 配置范围为 25 ... 35。

- ▶ **Roaming RSSI:** 如果配置了 Roaming RSSI，将会强制 RSSI 值较低的无线客户端进行漫游。Roaming RSSI 主要与 IEEE 802.11k 和 IEEE 802.11v 功能配合使用。控制和引导无线客户端的漫游过程。
 - 当在 WLAN 上启用 IEEE 802.11k 和 IEEE 802.11v 功能时，“Roaming RSSI Threshold”将触发 DAP847-XXA 和无线客户端之间的 IEEE 802.11k 和 IEEE 802.11 v 消息交换。
 - 当 DAP847-XXA 检测到无线客户端设备的 RSSI 值低于“Roaming RSSI Threshold”时，它会向该无线客户端设备发送一个 IEEE 802.11k 事件，支持 IEEE 802.11k 的无线客户端设备将使用包含来自该设备的 RF 扫描信息的数据包来响应 DAP847-XXA。
 - 基于接收到的数据，DAP847-XXA 将会计算该设备漫游的最佳 BSSID，然后通过 IEEE 802.11v 事件向该无线客户端设备发送最佳 SSID 信息。
 - 最后，该无线客户端设备将选择是否进行漫游。如果设备漫游，它将选择是在 DAP847-XXA 发送的 IEEE 802.11v 事件中获取一个目标 BSSID，或是选择在 DAP847-XXA 推荐范围外的另一个 BSSID 进行漫游。

默认情况下，Roaming RSSI 为禁用状态（0）。Roaming RSSI 可以单独应用于 2.4 GHz 频段或 5 GHz 频段。

- ▶ **Voice and Video Awareness:** 语音和视频感知。Background Scanning 能够感知到 DAP847-XXA 上数据业务的流量类型，如果当前正在进行语音或视频业务，则 Background Scanning 将会停止工作以确保高优先级的业务流量不会被中断。当检测到没有语音或视频流量时，将重新开启 Background Scanning。默认情况下，Voice and Video Awareness 功能处于禁用状态。
- ▶ **Airtime Fairness:** 时间公平，即使网络中存在传统的低速率客户端，如仅支持 IEEE 802.11a、IEEE 802.11g 或 IEEE 802.11n 的无线客户端，DAP847-XXA 也将会平均分配无线客户端的传输时隙，Airtime Fairness 可以有效地平衡无线接入点的负载，并确保每个客户端都能获得公平的带宽分配，通过这种方式提高整个无线网络的性能和可用性。缺省情况下 Airtime Fairness 是关闭的。

10 Access页面

Access页面包含了认证和访问控制相关的功能配置，主要用于用户访问管理，包括认证、无线客户端黑名单、Portal认证白名单和ACL等。

本章节主要包含如下内容：

- ▶ 认证
- ▶ Portal认证
- ▶ 账号和Access Code管理
- ▶ 定制化Portal页面
- ▶ 无线客户端黑名单
- ▶ Portal认证白名单
- ▶ Portal开放区域
- ▶ 组播控制
- ▶ ACL

10.1 认证

Authentication 页面有两种模式：

- ▶ Authentication 统计面板。
- ▶ Authentication Configuration 页面。单击 Authentication 页面标题栏可以进入 Authentication Configuration 页面。

Authentication 面板显示有关无线客户端的类型和操作系统（OS）的统计信息，见图 151。当光标移动至某个饼图上时，将能够显示相关设备的数量，见图 152。

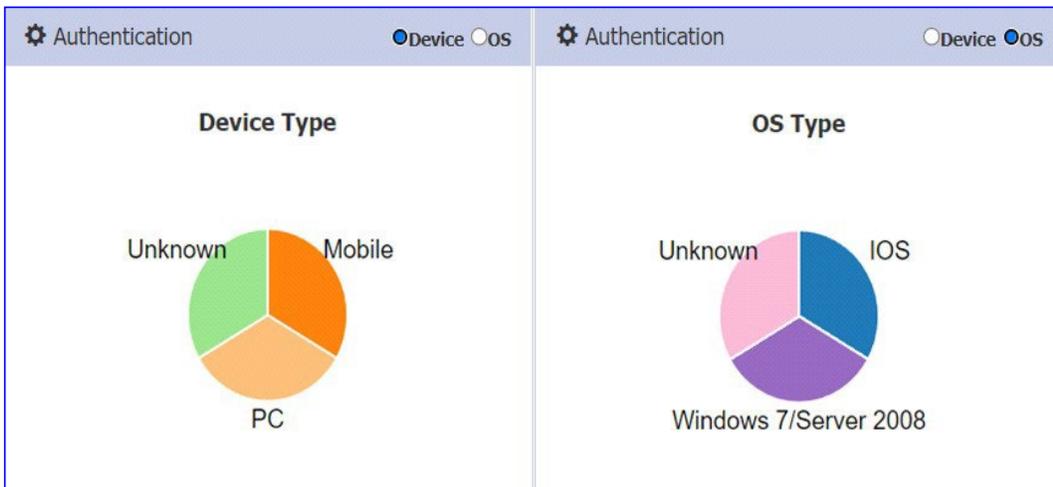


图 151: Authentication 统计面板

Clients				
		For Cluster: My-Demo-Cluster	Total:2	
Name	IP	MAC	WLAN	Auth
Lakers0326	172.16.10.110/fe80::de...	c0:3c:59:70:3d:c5	My-wifi-test	PSK_WPA2
iPhone-2	172.16.10.109/fe80::43...	dc:0c:5c:dd:59:c9	My-wifi-test	PSK_WPA3

🏠 Authentication
● Device ○ OS

Device Type



PC



Mobile

1

Blocklist & Allowlist

Blocklist
Allowlist
Walled Garden

MAC Address

MAC: Add

图 152: Device 类型

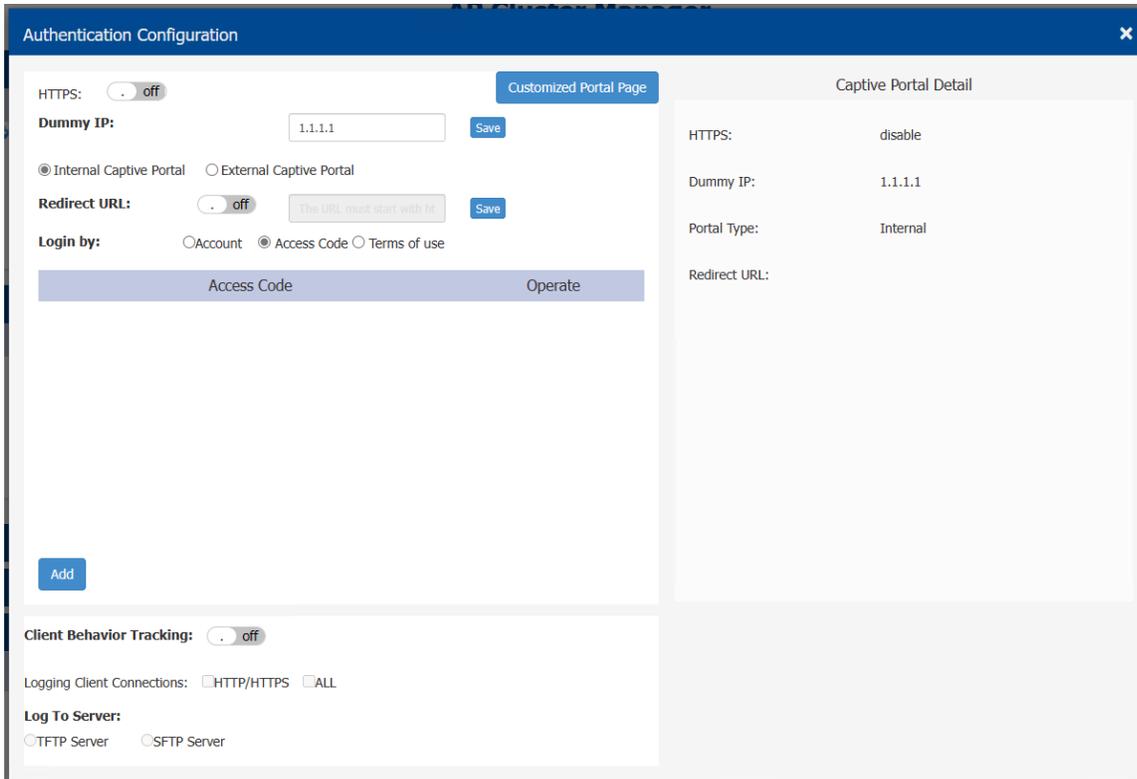


图 153: Authentication Configuration 页面

您可以根据实际业务场景的需要完成Portal认证所需其它参数的配置。
“Authentication Configuration” 页面中的相关参数描述如下：

参数	描述
Login by	Portal 认证登陆方式，包括 Account，Access Code 和 Terms of use 三种。
Dummy IP	Captive Portal 门户 FQDN 的 IP 地址，默认地址为 1.1.1.1。
Client Behavior Tracking	客户端行为跟踪，通过 SFTP 或 TFTP 的方式发送用户的 URL 访问记录。详见参数 Log to Server。
Logging Client Connections	<ul style="list-style-type: none"> ▶ HTTP/HTTPS: 记录无线客户端的 HTTP/HTTPS web 会话。 ▶ ALL: 记录无线客户端的 HTTP/TCP/UDP 会话。
Log to Server	<ul style="list-style-type: none"> ▶ TFTP Server: 通过日志文件的方式将客户端连接信息记录上传到指定的 TFTP 服务器。 ▶ SFTP Server: 通过日志文件的方式将客户端连接信息记录上传到指定的 SFTP 服务器。

10.2 Portal认证

对于Captive Portal认证类型的WLAN，有以下3种登录方式：**Account**，**Access Code**和**Terms of use**，缺省情况下为**Account**登录方式，请参考图 154。关于创建Captive Portal类型WLAN的步骤，请参阅第54页的“WLAN的安全类型”。

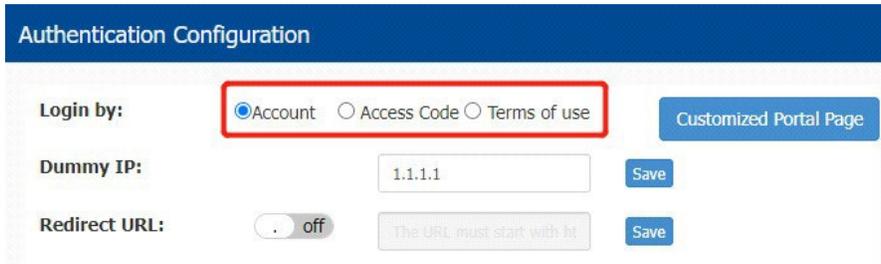


图 154: 选择登录方式

■ 使用用户名和密码方式登陆

- 选择“**Account**”登陆方式。
- 创建Captive Portal认证账户（由Administrator或Guest Manager创建）。
- 无线客户端在连接WLAN后，在弹出的Portal认证页面中输入“**Username**”和“**Password**”，并勾选“**I accept the terms of use**”后完成登陆认证。

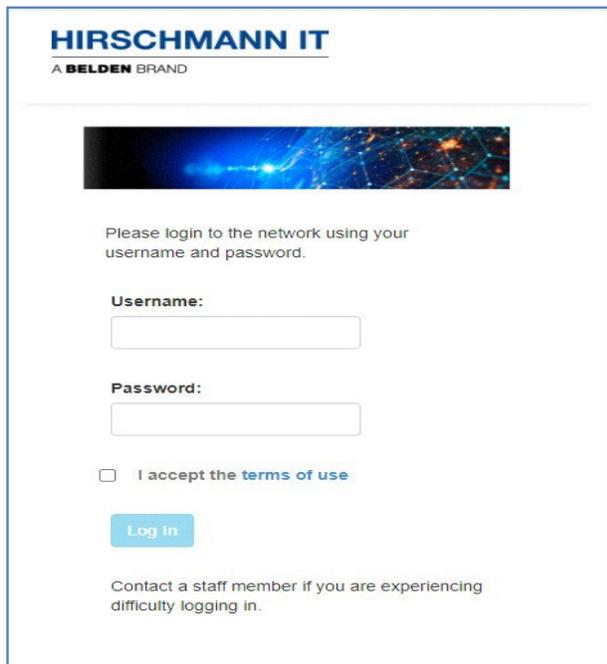


图 155: 使用用户名和密码方式登陆

■ 使用 **Access Code** 方式登陆

- 选择 “**Access Code**” 登陆方式。
- 创建**Access Code**（由Administrator或Guest Manager创建）。
- 无线客户端在连接WLAN后，在弹出的Portal认证页面中输入 “**Access Code**”，并勾选 “**I accept the terms of use**” 后完成登陆认证。

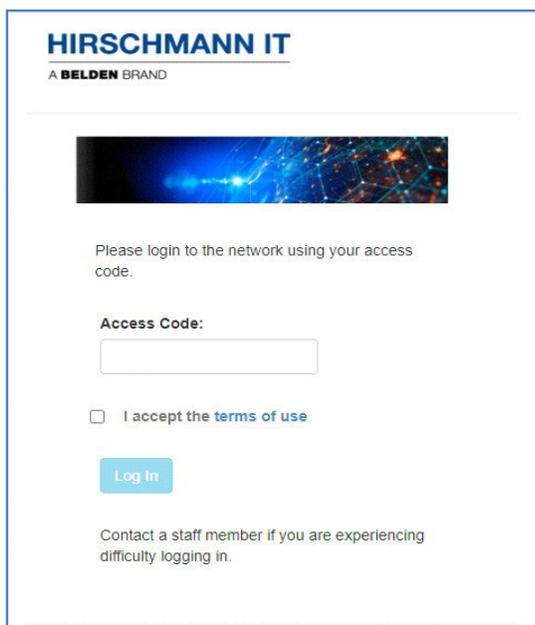


图 156: 使用 Access Code 登陆

■ 使用 **Terms of use** 方式登录

- 选择 “**Terms of use**” 的登陆方式。
- 无线客户端在连接WLAN后，在弹出的Portal认证页面中勾选 “**I accept the terms of use**” 即可登陆。

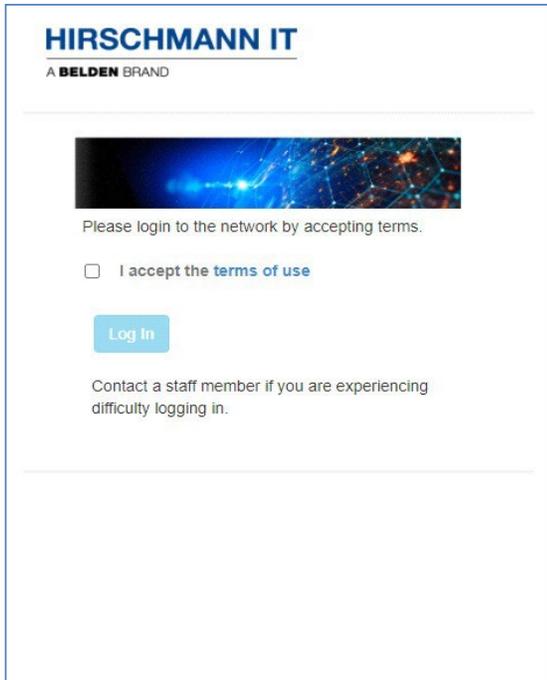


图 157: Terms of use 登陆

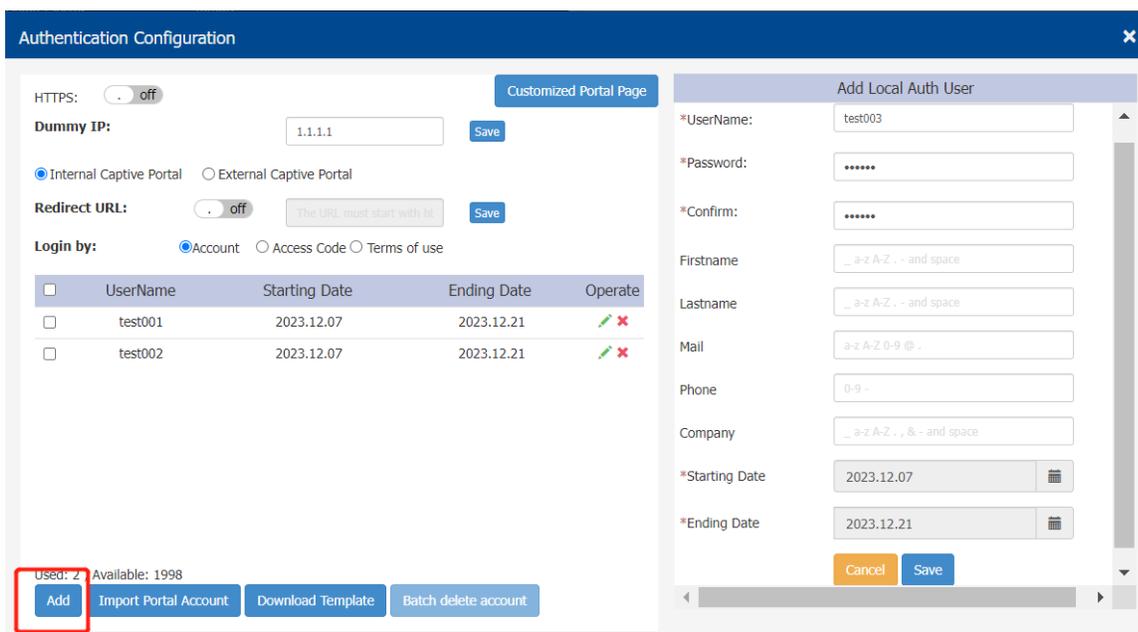
10.3 账号和Access Code管理

对于用户账户或Access Code登录方式，目前DAP847-XXA中仅支持本地用户数据库中的用户，不支持外部身份验证服务器（如Windows server做为一个Radius服务器）。您可以将Account或Access Code添加到本地用户数据库中。

■ 创建一个新的账户

- 选择“**Account**”登陆认证方式。
- 点击Authentication Configuration页左下方的“**Add**”按钮。
- 在右侧的“Add Local Auth User”页面中填写用户信息。其中带“*”的字段是必填字段，请参考图 158。

要查看某一个用户的详细信息，请单击页面左侧对应的帐户，在右侧的“Local Auth User”页面将会显示该用户的详细信息，参考图 159。



The screenshot displays the 'Authentication Configuration' interface. On the left, there are settings for HTTPS (off), Dummy IP (1.1.1.1), Captive Portal (Internal selected), Redirect URL (off), and Login by (Account selected). A table lists existing users: test001 and test002, both with starting dates of 2023.12.07 and ending dates of 2023.12.21. At the bottom left, the 'Add' button is highlighted with a red box. On the right, the 'Add Local Auth User' form is visible, with fields for *UserName (test003), *Password, *Confirm, Firstname, Lastname, Mail, Phone, Company, *Starting Date (2023.12.07), and *Ending Date (2023.12.21). The 'Add' button is highlighted with a red box.

图 158: 创建一个新账户

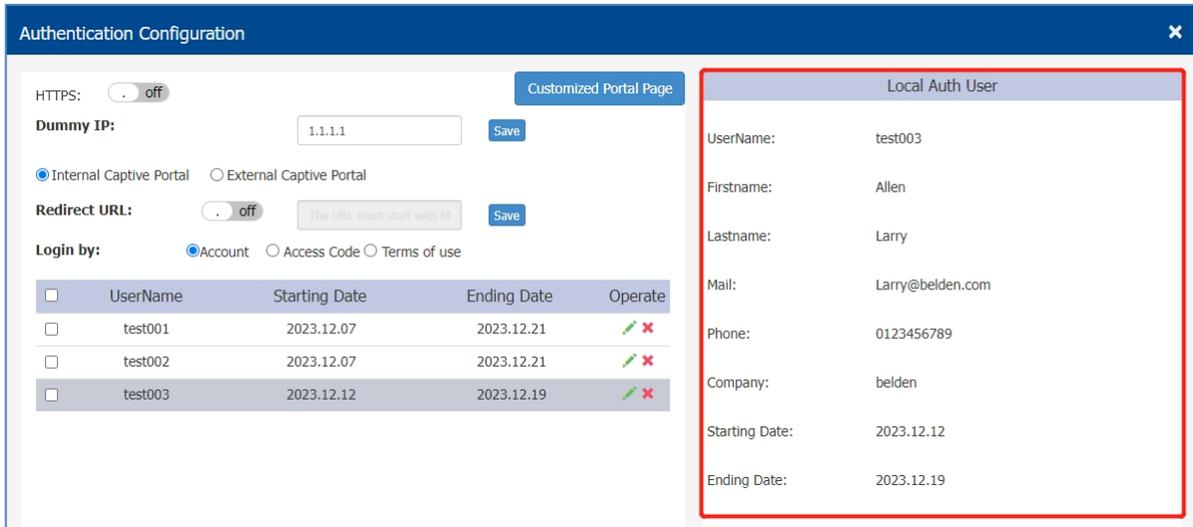


图 159: 账户详细信息

■ 批量导入 Portal 账户

DAP847-XXA支持从本地CSV文件批量导入帐户。您可以从下载的模板中修改本地CSV文件，这样可以批量创建Portal账户。

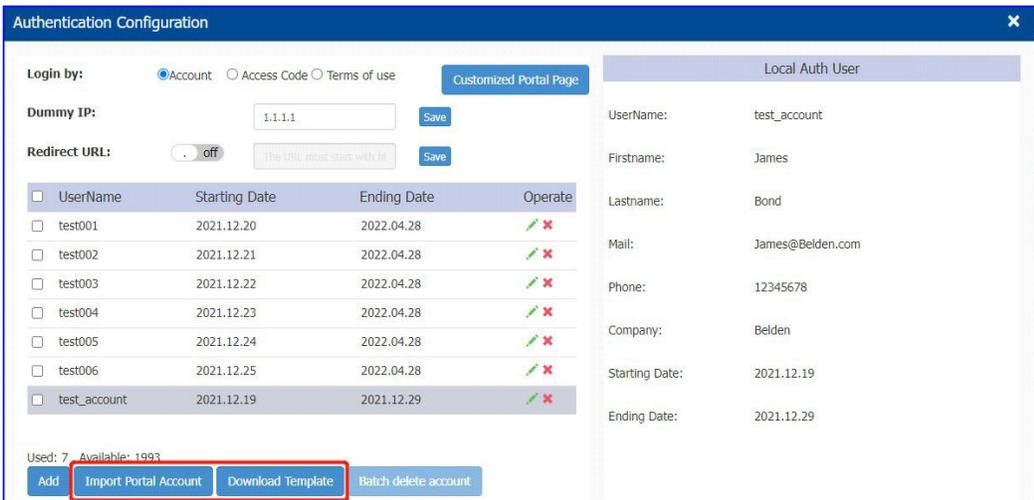


图 160: 批量导入 Portal 账户

■ 修改或删除账户

- 点击“”修改一个账户。
- 点击“”删除一个账户。
- 要删除多个帐户，请选择帐户并单击“**Batch delete account**”按钮，如图 161所示。

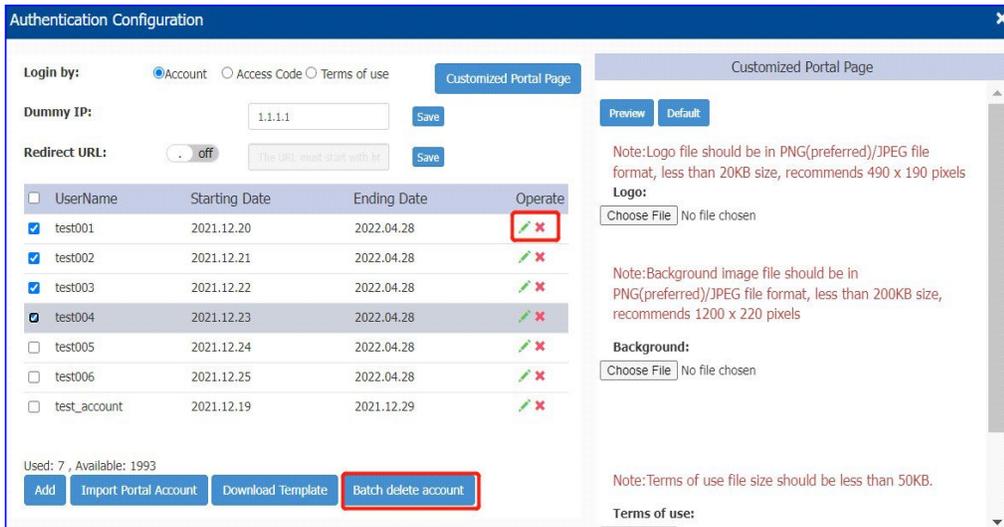


图 161: 修改或删除账户

■ 创建或删除 “Access Code”

- 选择 “Access Code” 登陆方式。
- 点击 Authentication Configuration 页面左下方的 “Add” 按钮创建一个 Access Code。
- 点击 “✘” 按钮删除一个 Access Code，参考图 162。

注意：对于Captive Portal认证，每个用户帐户或Access Code对可以连接到网络的设备数量没有限制，对多个设备可以同时使用一个帐户或Access Code。

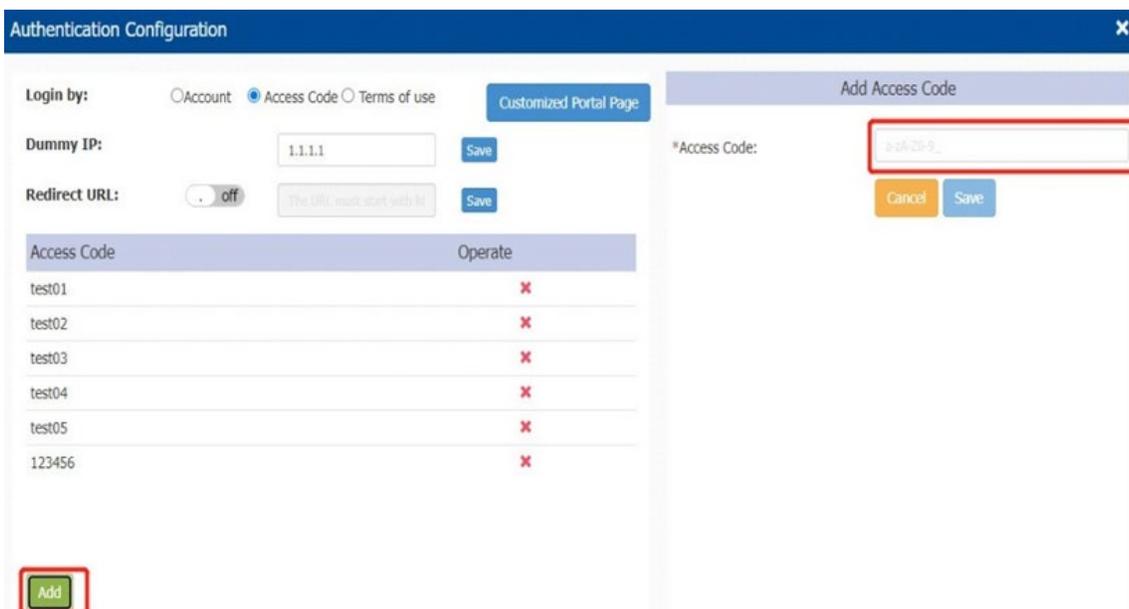


图 162: 创建一个 Access code

10.4 定制化Portal页面

为满足客户的个性化需求，提高用户体验和客户的竞争力，您可以根据客户的具体需求和风格对Portal页面进行设计，包括背景图案，logo以及使用条款等，参考图 163。

配置路径：**Dashboard → Access Page → Authentication → Authentication Configuration → Customized Portal Page**

- 按照提示的要求上传logo、背景图案和使用条款。
- 点击“**Preview**”按钮可以预览定制化Captive Portal页面。
- 点击“**Default**”按钮可以撤销定制化的修改内容恢复为系统默认的Captive Portal页面。

Customized Portal Page

Preview Default

Note: Logo file should be in PNG(preferred)/JPEG file format, less than 20KB size, recommends 490 x 190 pixels

Logo:

Choose File No file chosen

Note: Background image file should be in PNG(preferred)/JPEG file format, less than 200KB size, recommends 1200 x 220 pixels

Background:

Choose File No file chosen

Note: Terms of use file size should be less than 50KB.

Terms of use:

Choose File No file chosen

Cancel

图 163: 定制化 Captive Portal 页面

10.5 无线客户端黑名单

Blocklist是指DAP847-XXA的黑名单列表，用于无线用户的访问控制，其中记录了被DAP847-XXA集群禁止连接的无线设备的MAC地址。在黑名单中添加了无线设备的MAC地址后，该设备将无法连接到DAP847-XXA集群的Wi-Fi网络。该Blocklist功能可以帮助管理员控制哪些设备不可以连接到无线网络，以保护网络安全。

如果需要从黑名单中删除设备，可以进入Blocklist配置页面，找到对应设备的MAC地址，然后点击后面的“✘按钮”将其删除。

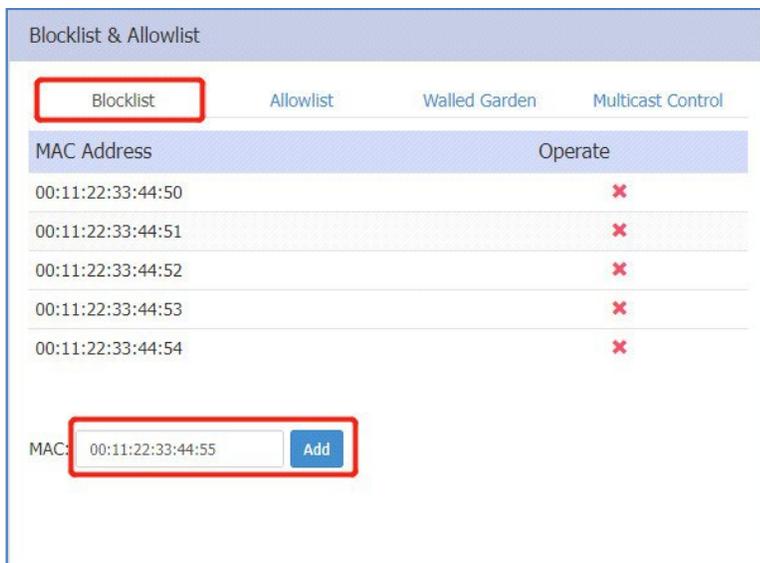


图 164: Blocklist 配置

10.6 Portal认证白名单

Allowlist中的无线客户端可以不需要经过Portal认证直接访问网络资源，您可以手动添加无线客户端设备的MAC地址或从Allowlist中删除无线客户端设备的MAC地址。请注意Allowlist仅适用于Captive Portal身份验证的场景，Allowlist中的客户端不允许在没有正确凭据的情况下访问Enterprise以及Personal类型的WLAN。

MAC Address	Operate
00:11:22:33:44:60-00:11:22:33:44:60	✘
A0:11:22:00:00:00-A0:11:22:FF:FF:FE	✘

Starting MAC:

Ending MAC:

图 165: Allowlist 配置

10.7 Portal开放区域

Walled Garden(Portal开放区域) 是一种对网络资源的控制机制，它用于限制对未经批准的应用程序或内容的访问。Walled Garden仅适用于Captive Portal认证，在通过Captive Portal身份验证之前，客户端可以访问Walled Garden中列出的网络资源的内容，您可以在Walled Garden中添加或删除域名或IP地址形式的网络资源。

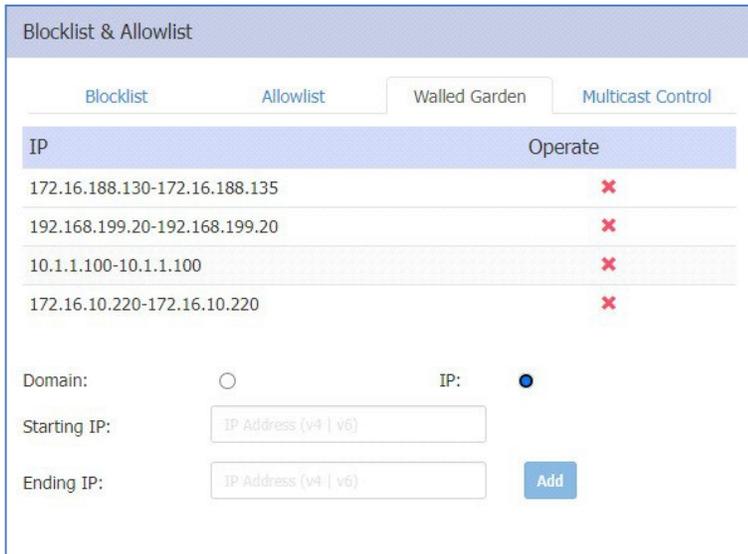


图 166: IP 地址格式的Walled Garden 配置



图 167: 域名格式的Walled Garden 配置

10.8 组播控制

组播控制用于从有线网络（交换机端口）向DAP847-XXA转发mDNS组播流量。启用该功能后，DAP847-XXA只能将来自源地址为allowlist中配置的地址的组播数据转发到客户端。Multicast Allowlist中最多支持配置8条组播流。当组播控制禁用时，DAP847-XXA将无差别转发mDNS流量。

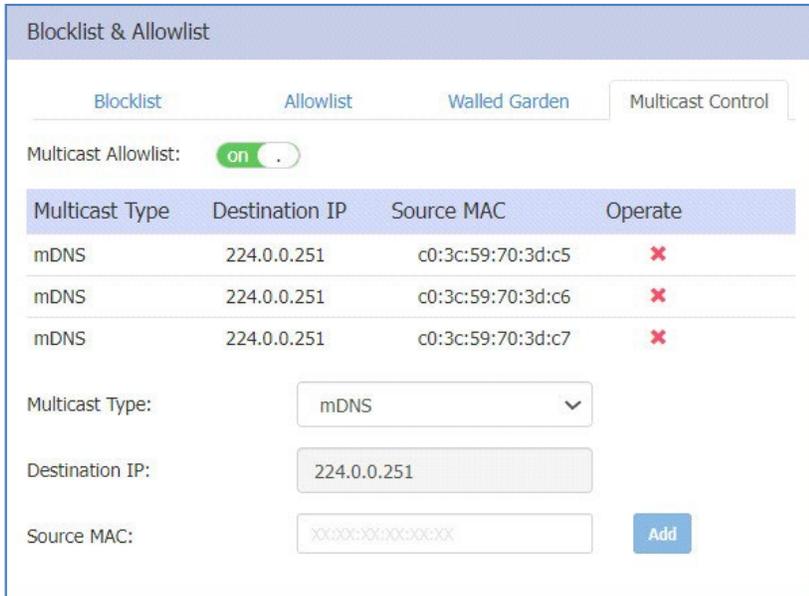
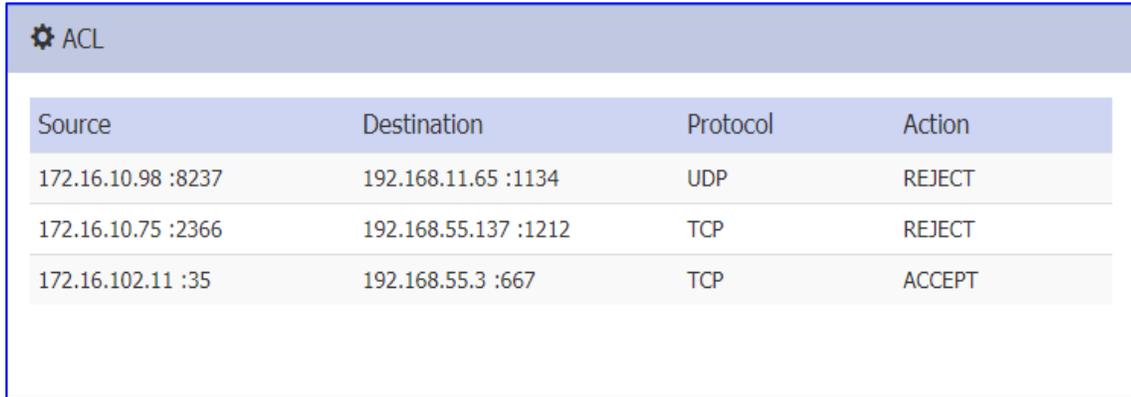


图 168：组播控制

10.9 ACL

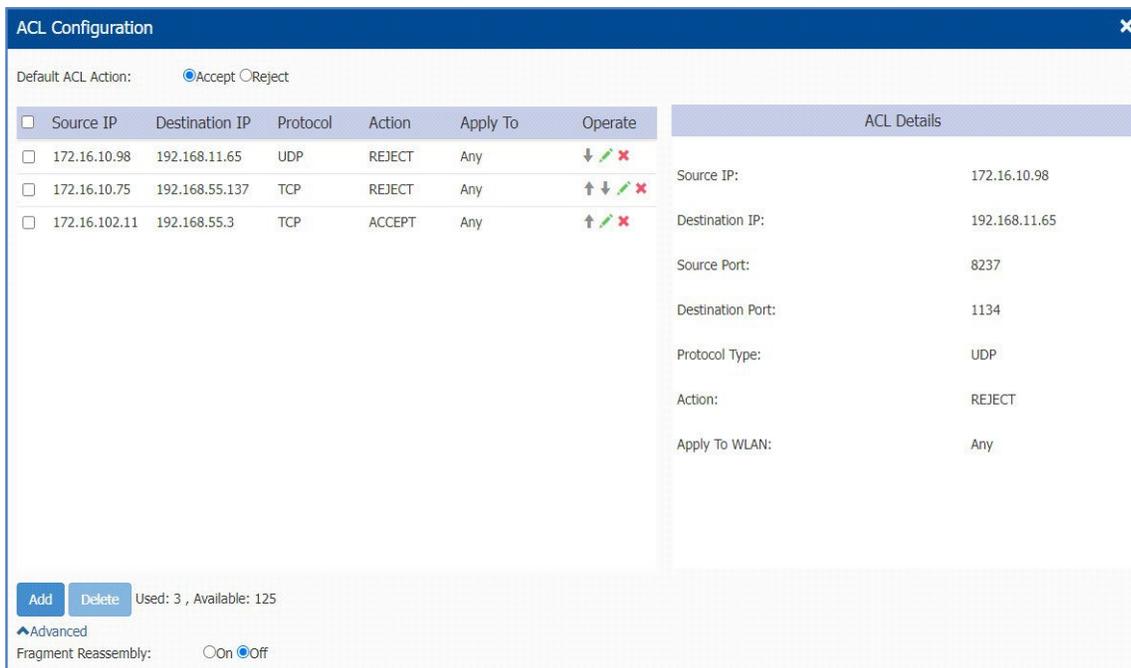
ACL页面有两种模式，ACL基本模式和ACL配置模式。参考图 169 和图 170。单击ACL页面的标题栏，可以从ACL的基本模式进入到ACL配置模式。



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

图 169: ACL 基本模式

DAP847-XXA最多支持128条规则，您可以使用IP地址、协议及端口号等内容创建L3 ACL。列表中创建的ACL规则将根据由上到下的优先级顺序生效，如果最终没有匹配的ACL规则，则允许该流量通过（默认ACL操作为“Accept”），参考图 170。



ACL Configuration

Default ACL Action: Accept Reject

<input type="checkbox"/>	Source IP	Destination IP	Protocol	Action	Apply To	Operate	ACL Details
<input type="checkbox"/>	172.16.10.98	192.168.11.65	UDP	REJECT	Any	↓ ↕ ↗ ✖	Source IP: 172.16.10.98
<input type="checkbox"/>	172.16.10.75	192.168.55.137	TCP	REJECT	Any	↑ ↓ ↕ ↗ ✖	Destination IP: 192.168.11.65
<input type="checkbox"/>	172.16.102.11	192.168.55.3	TCP	ACCEPT	Any	↑ ↕ ↗ ✖	Source Port: 8237
							Destination Port: 1134
							Protocol Type: UDP
							Action: REJECT
							Apply To WLAN: Any

Add Delete Used: 3, Available: 125

Fragment Reassembly: On Off

图 170: ACL 配置页面

参数	描述
Source IP	源IP地址。
Destination IP	目的IP地址。
Source Port	TCP或UDP协议报文的源端口。
Destination Port	TCP或UDP协议报文的端口。
Protocol Type	ALL、TCP、UDP、ICMP或ICMPv6。
Action	ACCEPT或REJECT。
Apply To WLAN	ACL规则的应用范围，特定SSID或任何SSID。

11 IoT

DAP847-XXA不支持IoT功能，但如果DAP847-XXA与其它支持IoT功能的设备（如DAP640）组成集群时，仍可以完成IoT的配置，详细信息请参考[DAP系列用户手册](#)。

12 DAP847-XXA内部集成工具

12.1 Tools

Tools是DAP847-XXA内部集成的一些常用的Debug命令，用于日常的诊断和故障排查。这些命令在DAP847-XXA中执行，通过这些工具，网络管理员能够查看DAP847-XXA上的运行信息，例如系统状态、Wi-Fi信息和重启原因等。

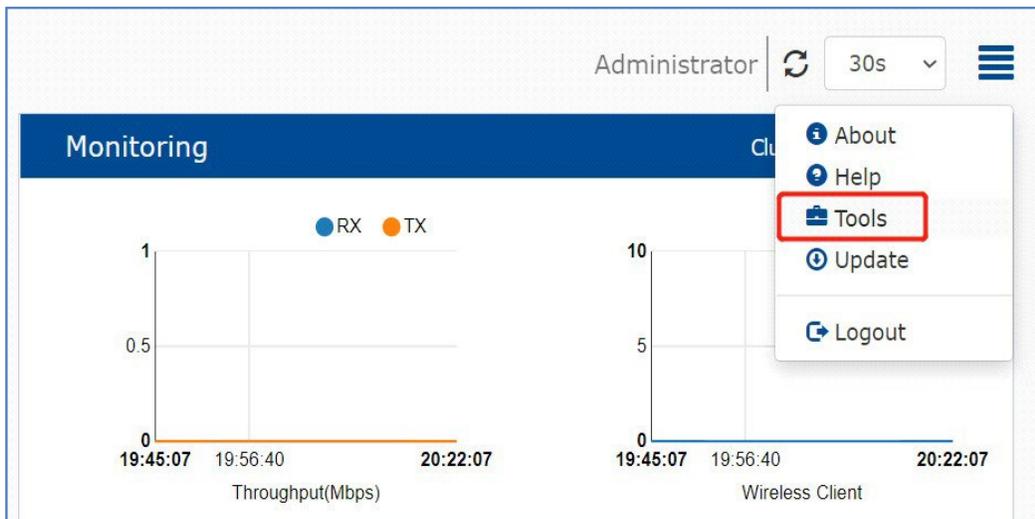


图 171: 进入 Tools 页面

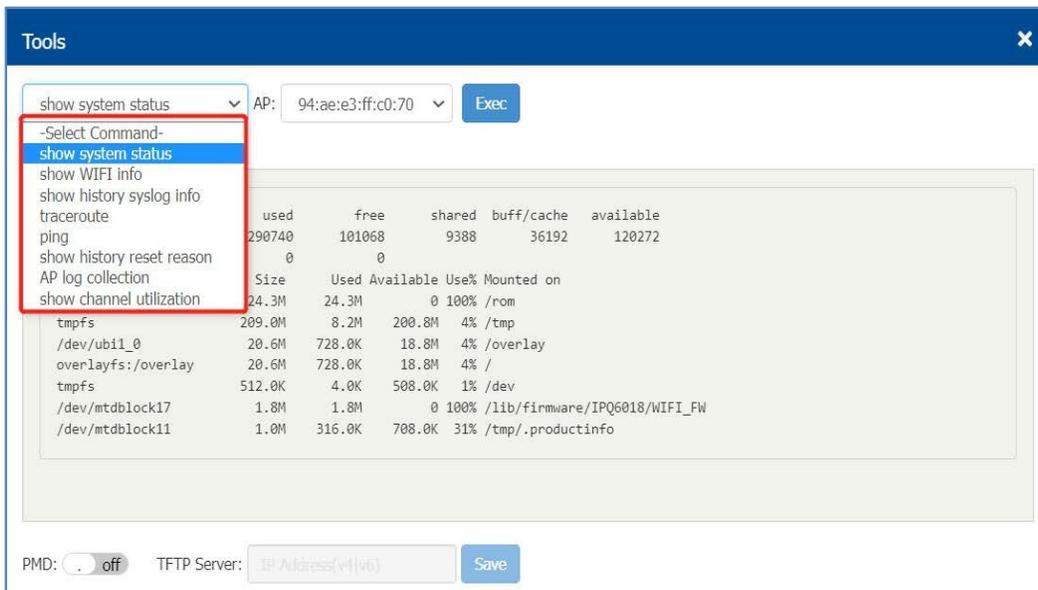


图 172: DAP847-XXA 集成的工具

- ▶ **show system status:** 显示 DAP847-XXA 的内存的使用情况。

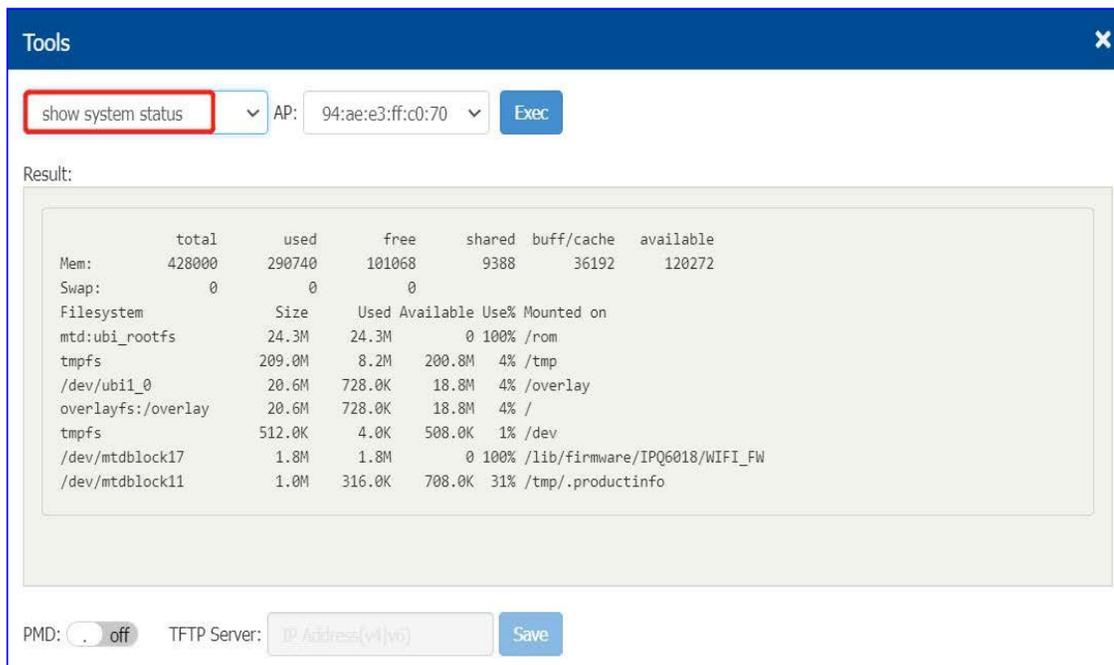


图 173: 显示系统状态

- ▶ **show WIFI info:** 显示 DAP847-XXA 无线接口的状态信息。

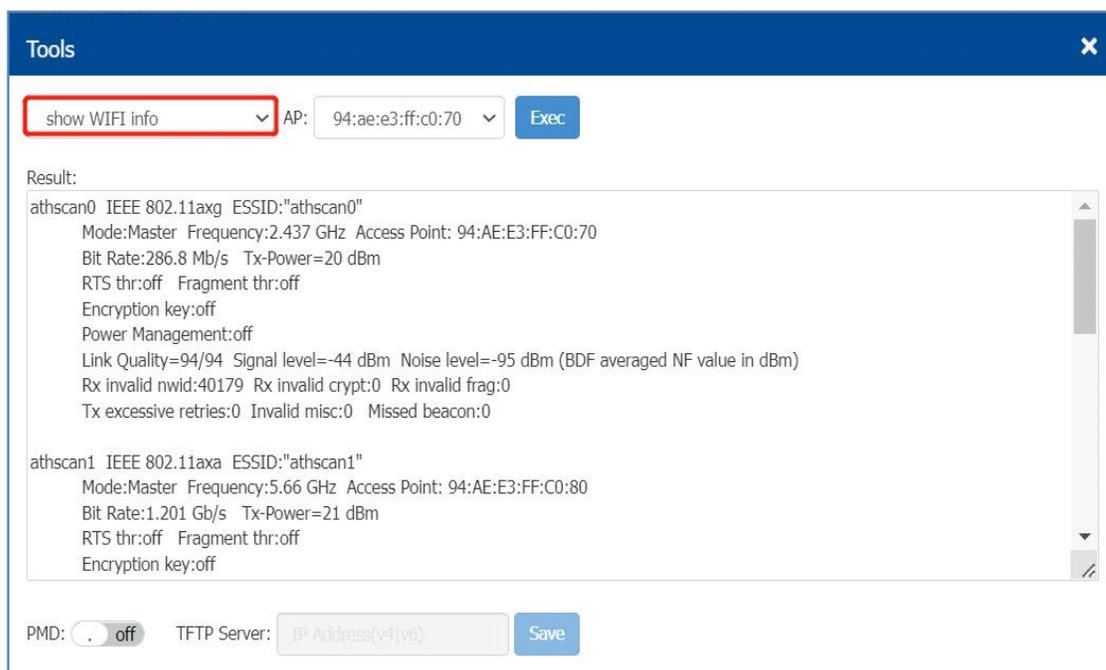


图 174: 显示 WIFI 信息

- ▶ **show history syslog info:** 显示指定 DAP847-XXA 最近一次运行期间（系统启动之前）生成的历史 Syslog 日志消息。

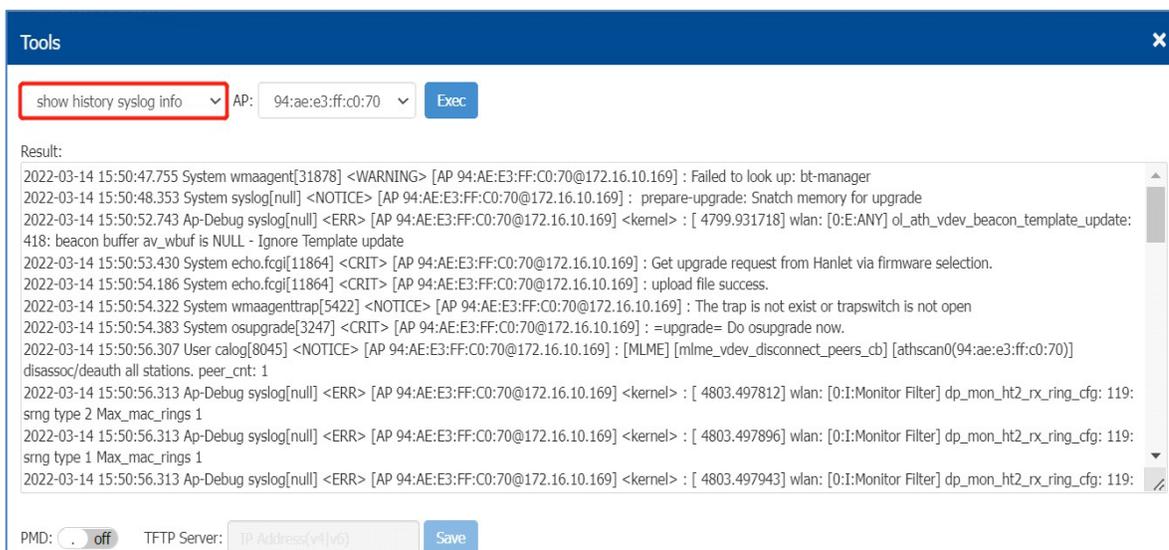


图 175: 显示历史 Syslog 日志消息

- ▶ **traceroute:** DAP847-XXA 内置的 traceroute 工具，用于检查网络中的路由信息，参考图 170。

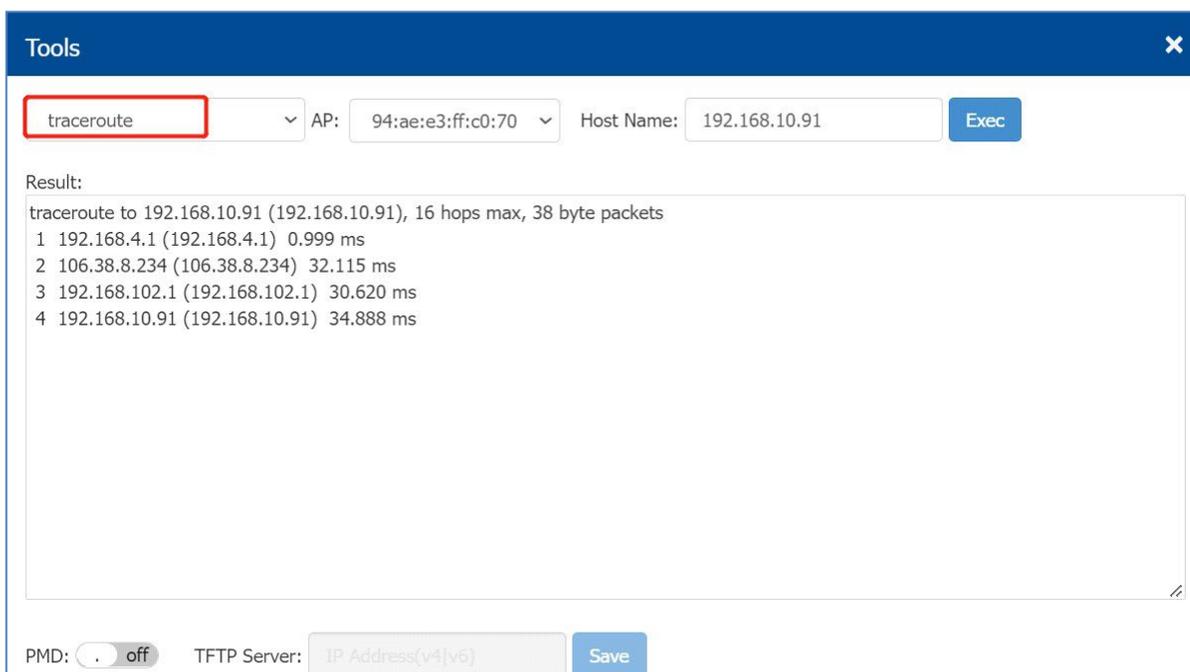


图 176: Traceroute

- ▶ **ping:** 可以在 DAP847-XXA 中 ping 网络中其它主机。

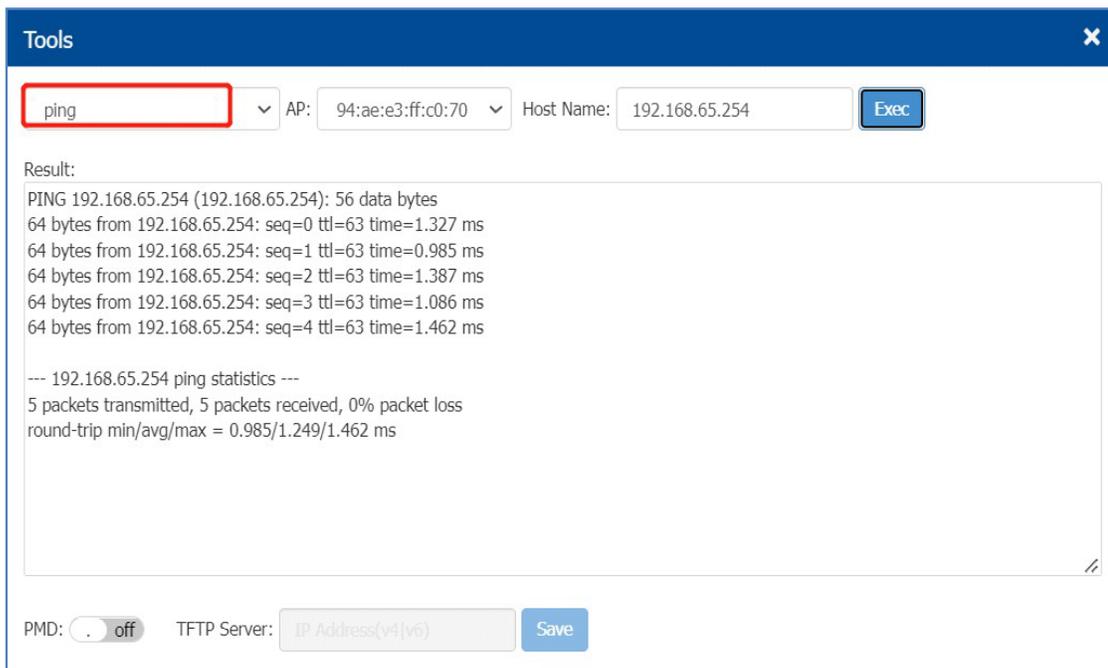


图 177: 在 DAP847-XXA 上进行 ping 测试

- ▶ **show history reset reason:** 显示 DAP847-XXA 最近 10 次重启的记录信息，与命令行 `reset_record get` 返回的结果一致，参考图 178。

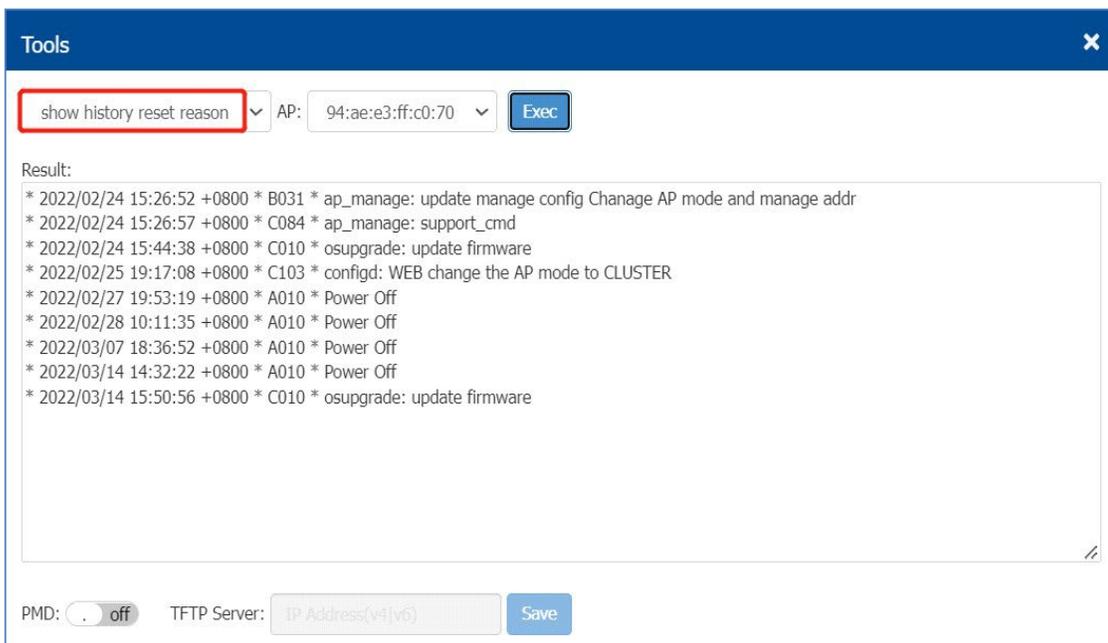


图 178: 显示历史重启原因

- ▶ **AP log collection:** 收集 DAP847-XXA 的 log 文件，支持通过 TFTP 及 HTTP 的方式下载，参考图 179 和图 180。

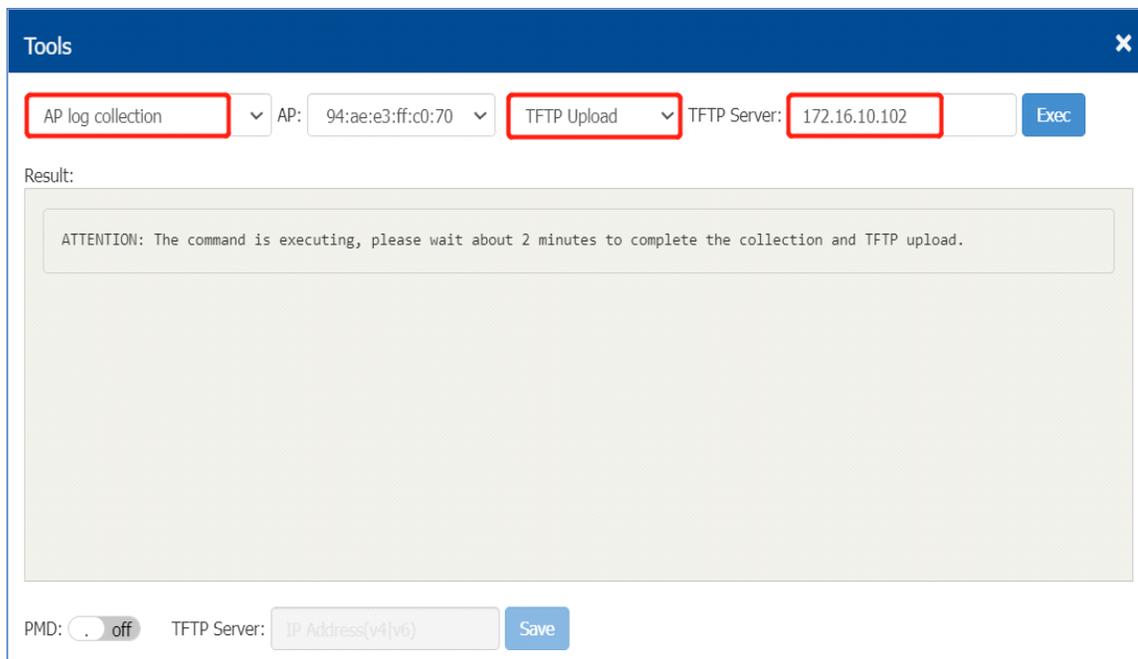


图 179: 使用 TFTP 收集日志

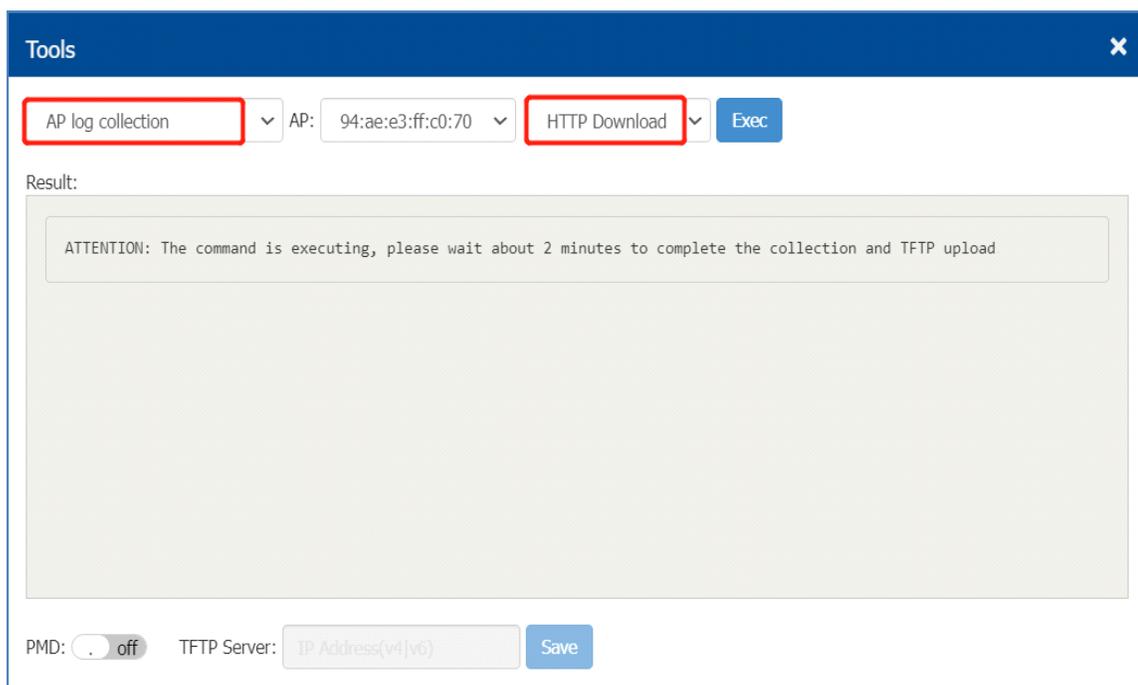


图 180: 使用 HTTP 收集日志

- ▶ **show channel utilization:** 显示 2.4G 及 5G 信道的利用率，参考图 181。

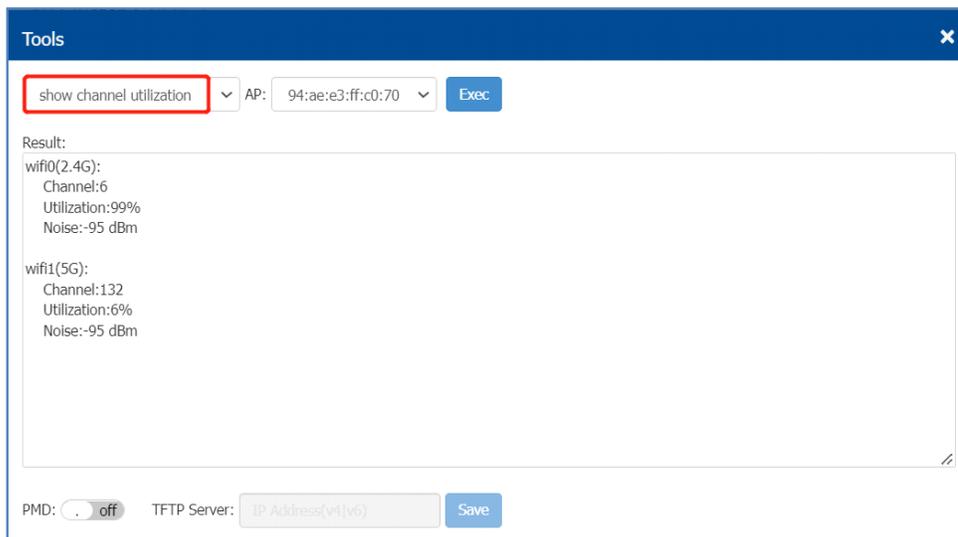


图 181: 显示信道利用率

12.2 PMD

Post Mortem Dump (PMD) 是DAP847-XXA支持的一种故障排查工具，在应用程序崩溃或发生错误时，可以将应用程序当时的内存内容、寄存器状态、堆栈信息等保存下来并通过TFTP的方式上传至服务器，以便于后续进行分析和调试。如果启用并配置了PMD，则当DAP847-XXA上出现关键进程崩溃时，DAP847-XXA将立即向指定的TFTP服务器发送PMD文件。默认情况下，PMD功能处于禁用状态。

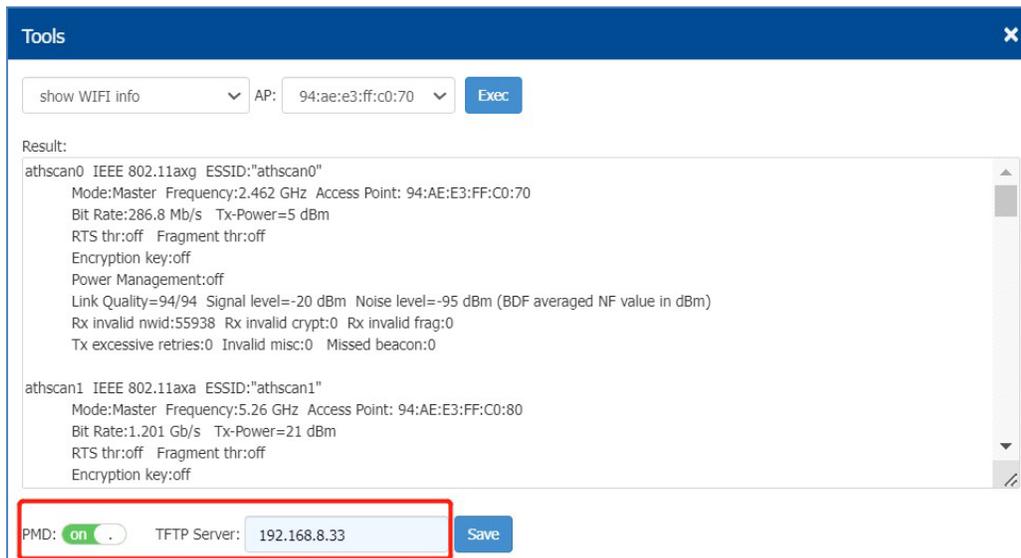


图 182: PMD 配置

13 部署大规模DAP847-XXA网络系统

对于一些大规模的部署场景，如果您的DAP847-XXA的数量超过集群定位的最大规格（255），则可以设置2个或多个集群的方式来进行部署，灵活扩展客户的业务应用。

您可以通过如下3种方案部署多个集群的场景：

■ 方案 1：划分子网

通过划分DAP847-XXA所连接交换机端口的默认VLAN，将DAP847-XXA划分为不同的子网，例如，子网A使用默认VLAN 100，子网B使用默认VLAN 200，子网C使用默认VLAN 300。

■ 方案 2：设置不同集群 ID

为每个DAP847-XXA群集设置不同的集群ID，即使将DAP847-XXA部署在同一个子网里，也能够通过集群ID来隔离不同的集群。

- 将DAP847-XXA插入交换机并组建第一个集群-A。
- 登陆集群-A后修改该集群的集群ID。(如将集群ID由默认的100更改为101)。
- 重复以上步骤完成集群-B和集群-C的配置。

■ 方案 3：部署 DAC 模式

将DAP847-XXA部署为DAC模式，该模式下能够支持多达4000台DAP847-XXA的集中管理，详细操作步骤，请参考[DAC用户手册](#)。

14 无DHCP服务器场景

本章节介绍两种无DHCP服务器的场景下，DAP847-XXA的配置方法。

■ 场景 1：DA847-XXA 无法连接到 DHCP 服务器

如果集群中的DAP847-XXA在启动后无法连接到网络中的DHCP服务器，则将会使用系统默认的IP地址（192.168.1.254）。

如果网络中有多台DAP847-XXA设备，可能会导致该网络中存在重复的IP地址，这种情况下DAP847-XXA将会与PVM分离各自组成一个集群，并且广播相同的WLAN。在这种情况下，建议修复网络中的DHCP服务器。

■ 场景 2：网络无 DHCP 服务器下配置 DAP847-XXA

如果在网络中没有DHCP服务器的情况下需要配置一台DAP847-XXA，可以按照如下步骤完成配置：

- 将DAP847-XXA（默认IP地址为192.168.1.254）直接连接到您的配置终端（例如，笔记本电脑或PC机）。
- 将笔记本电脑（或PC机）的网卡配置一个静态IP地址和DNS服务器。例如，将IP地址配置为192.168.1.100，子网掩码配置为255.255.255.0，默认网关配置为192.168.1.254，DNS服务器配置为192.168.1.254。
- 在浏览器输入<http://192.168.1.254:8080>访问AP Cluster Manager，根据客户需要完成后续的配置。

注意：如果需要配置多台DAP847-XXA组成一个集群，只需将DAP847-XXA配置不同的IP地址即可。

15 术语表

ACL	Access Control List	访问控制列表
ACS	Automatic Channel Selection	自动信道选择
APC	Automatic Power Control	自动功率控制
ARP	Address Resolution Protocol	地址解析协议
BLE	Bluetooth Low Energy	蓝牙低功耗
BSSID	Basic Service Set Identifier	基本服务集标识符
CLI	Command-Line Interface	命令行界面
CTS	Clear To Send	允许发送
DAC	Dragonfly Access Controller	Dragonfly 无线控制器
DAP	Dragonfly Access Point	Dragonfly 无线接入点
DCM	Dynamic Client Management	动态客户端管理
DNS	Domain Name System	域名系统
DRM	Dynamic Radio Management: Automatically manage DAP working channel and transmitting power	动态无线电管理：用于自动管理 DAP 的工作信道和传输功率。
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DSCP	Differentiated Services Code Point	差分服务代码点
DTIM	Delivery Traffic Indication Message	传输流量指示消息
ESSID	Extended Service Set Identifier	扩展服务集标识符
FQDN	Fully Qualified Domain Name	完全限定域名
GUI	Graphical User Interface	图形用户界面
IDS	Intrusion Detection System	入侵检测系统
IG	Installation Guide	安装指南
IGMP	Internet Group Management Protocol	互联网组管理协议
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
MAC	Media Access Control	以太网地址
MIMO	Multiple-Input Multiple-Output	多输入多输出
MTU	Maximum Transmission Unit	最大传输单元
MU-MIMO	Multi-User Multiple-Input Multiple-Out	多用户多输入多输出
NAT	Network Address Translation	网络地址转换
NTP	Network Time Protocol	网络时间协议
OKC	Opportunistic Key Caching	机会性密钥缓存

PMD	Post Mortem Dump	事后转储
PMF	Protected Management Frames	保护管理帧
POE	Power over Ethernet	以太网供电
PPPOE	Point-to-Point Protocol over Ethernet	以太网上的点对点协议
PVM	Primary Virtual Manager	主虚拟管理器
QoS	Quality of Service	服务质量
QSG	Quick Start Guide	快速入门指南
RF	Radio Frequency	射频
RSSI	Received Signal Strength Indicator	接收信号强度指示器
RTS	Request To Send	请求发送
SNMP	Simple Network Management Protocol	简单网络管理协议
SSID	Service Set Identifier	服务集标识符
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	次要虚拟管理器：在集群中具有第二高优先级。当 PVM 由于意外错误或问题无法响应时，SVM 将自动升级为 PVM 的角色。
TCP	Transmission Control Protocol	传输控制协议
TLS	Transport Layer Security	传输层安全协议
UDP	User Datagram Protocol	用户数据报协议
VLAN	Virtual Local Area Network	虚拟局域网
WBM	Web Based Management	基于 Web 的管理
WIDS	Wireless Intrusion Detection System	无线入侵检测系统
WIPS	Wireless Intrusion Prevention System	无线入侵防御系统
WLAN	Wireless Local Area Network	无线局域网
WMM	Wi-Fi Multimedia (WMM)	Wi-Fi 多媒体
WPA	Wi-Fi Protected Access	Wi-Fi 保护接入
WPA2	Wi-Fi Protected Access 2	Wi-Fi 保护接入 2
UUID	Universally Unique Identifier	通用唯一标识符

A 更多支持

技术问题

如有技术问题，请直接联系当地的Hirschmann IT经销商或Belden。

Hirschmann IT直接技术支持的当地电话号码和电子邮箱列表，请访问：

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

该网站中还包括免费提供的知识库和软件下载版块。

HIRSCHMANN IT

A **BELDEN** BRAND