HIRSCHMANN IT

A BELDEN BRAND

用户配置手册

DAP849-WIFI

DAP849-WIFI 用户手册
版本 1.1 01/2026

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

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。

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	2025.12	第一版
1.1	2026.01	1. 更新 WLAN 配置的 Enterprise 安全类型。 2. 更新 SNMP 配置版本为 v2c 时的团体名方法。

目录

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。本用户手册适用于 4.1.7.72 及以上版本。

关于 DAP

作为新一代企业级无线接入点，DAP849 系列是专门为工业级无线覆盖场景设计的 Wi-Fi 6 设备。DAP849 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。

DAP849 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 DAP849 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 DAP849 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 DAP849 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 DAP849 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 DAP849 的用户或者对 DAP849 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 DAP849 工作模式介绍

2.1 Cluster 集群模式

DAP849 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，DAP849 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 DAP849 和虚拟管理器组成的自治系统。DAP849 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 DAP849 之间能够组成一个集群，同时 DAP849 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/DAP849 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，DAP849 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 DAP849 的业务出现中断或影响无线用户的服务。

一个 DAP849 集群支持多达 255 个 DAP849 设备，集群的架构能够确保 DAP849 简单快速的完成部署。一旦您使用配置向导配置了第一个 DAP849 设备，在同一个二层网络中使用相同“**集群 ID**”的其它 DAP849 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，DAP849 使用的“**集群 ID**”为 100。

2.1.2 DAP849 开箱设置

要设置 DAP849 开箱即用：

- ☐ 将 DAP849 连接到网络中的交换机.
- ☐ 通过电源适配器为其供电.
- ☐ 确保 DAP849 可以从网络中的 DHCP 服务器获取到 IP 地址。

当 DAP849 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 DAP849 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 DAP849 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 DAP849 了。

2.2 DAC 模式

当 DAP849 工作在 DAC 模式时，所有的 DAP849 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 DAP849 与 DAC 的三层组网，只需要保证 DAP849 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 DAP849。

有关详细信息，请参阅 DAC 用户手册。

2.3 BWO 模式

当 DAP849 工作在 BWO 模式时，所有的 DAP849 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 BWO 模式，支持 DAP849 与 BWO 的三层组网，只需要保证 DAP849 与 BWO 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 DAP849。

有关详细信息，请参阅 BWO 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 DAP849、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 或 BWO 管理平台。所有的 DAP849 以“集群”的模式工作，以实现自主管理功能。

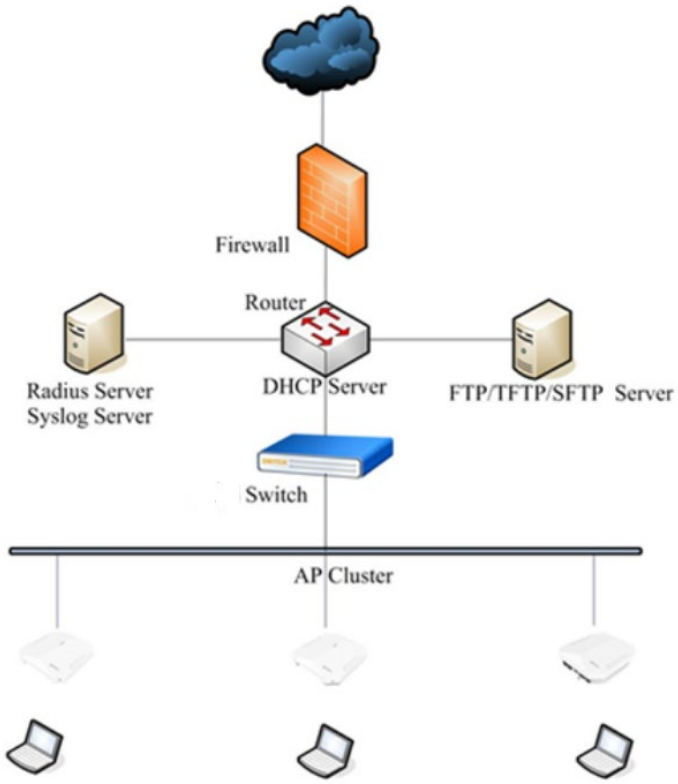


图 1：网络拓扑图

3.2 场景描述

图 1 网络拓扑工作模式如下：

- 集群有 3 个 DAP849，都连接到一台交换机，所有 DAP849 都属于同一个 VLAN。
- 交换机上行连接到核心路由器，该路由器为 DAP849 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 DAP849 的管理和监控、配置的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，DAP849 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的 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 RADUIS server。
- **Syslog Server**：作为远程系统日志服务器，用于接收查看 DAP849 生成的系统日志，请参阅第 131 页的“配置 Syslog 系统日志”。
- **TFTP Server**：主要用于 DAP849 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 DAP849 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 DAP849 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 DAP849 Cluster Manager

每个 DAP849 支持 3 个不同的账号同时登陆 DAP849 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 DAP849 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 DAP849 的运行状态，从而更好地理解 DAP849 的关键指标。

如需在 **GUI Dashboard** 中识别和诊断 WLAN 的相关问题，请参阅第 32 页的“Dashboard 页面简介”。

4.1.1 预置条件

要设置 DAP849，请确保以下条件均被满足：

- 首先将 DAP849 设备连接到交换机并接通电源。
- 保证所有的 DAP849 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 DAP849 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 DAP849 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 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 DAP849 的过程与连接到 DAP849 集群的过程是相同的。我们建议初次配置时先只连接 1 台 DAP849 设备到网络并完成初始配置，然后再逐台连接其他的 DAP849 同步集群的配置。

4.1.2 DAP849 IP 地址

可以通过如下三种方式获取和管理 DAP849 的 IP 地址：

- 默认状态下，如果网络中没有 DHCP 服务器，DAP849 将会使用 192.168.1.254 作为其默认的管理地址。
- DAP849 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，DAP849 支持从 DHCP 服务器动态获取 IP 地址。您可以通过在 DHCP 中查看已分配置的地址，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 DAP849 的 IP 地址, 见图 2。

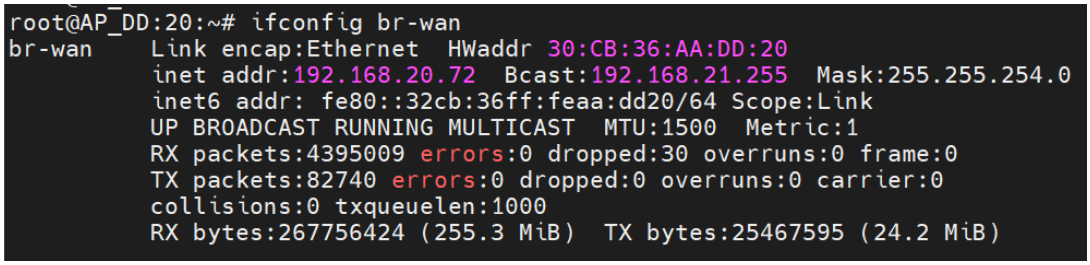


图 2：使用 CLI 查看 DAP849 的 IP 地址

4.1.3 在初始状态下访问 DAP849 的 Web GUI

在默认出厂设置中，在 DAP849 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。

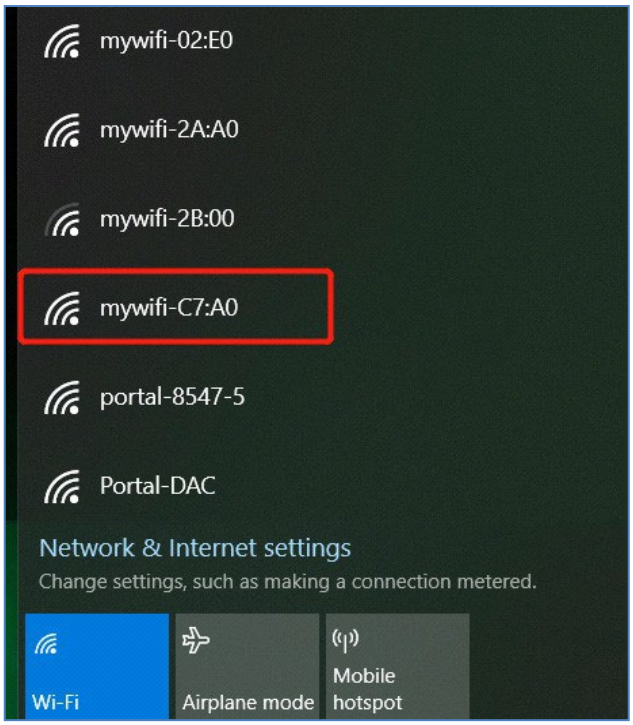


图 3：连接到默认的 SSID

☐ 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/。参考图 4。

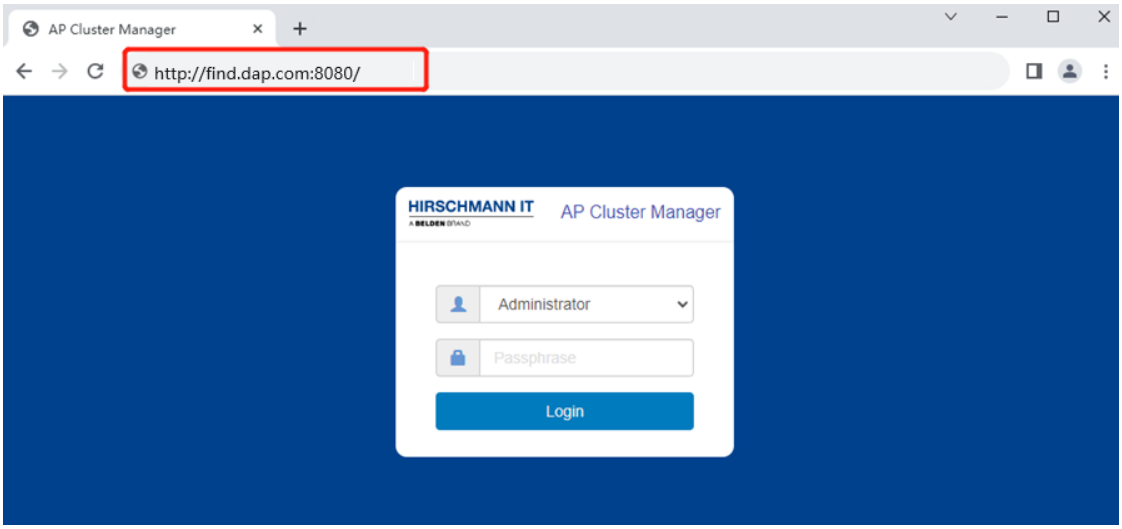


图 4：HTTP 登陆

► 通过 https 登录，输入 https://find.dap.com。参考图 5。

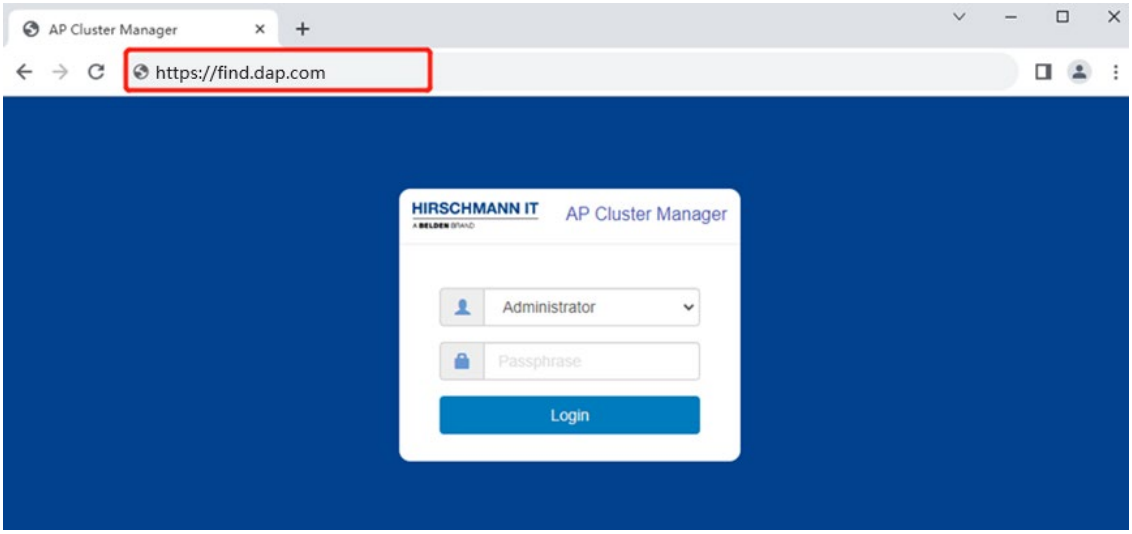


图 5：HTTPS 登陆

注意：为保证DAP849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 DAP849 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。

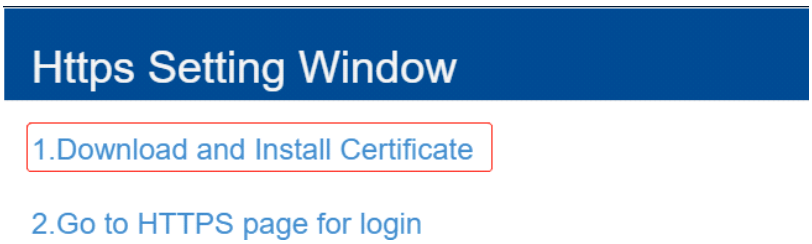


图 6：下载并安装证书

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 DAP849 的 IP 地址登陆到 DAP849 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 DAP849 的 IP 地址）
- https://172.16.10.169 （172.16.10.169 是 DAP849 的 IP 地址）

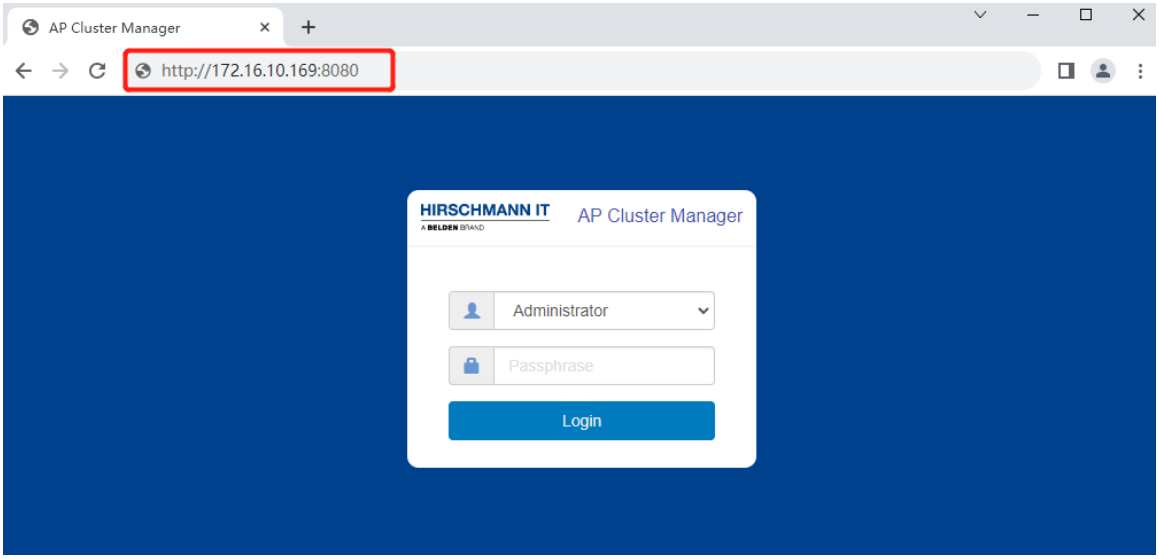


图 7：使用 IP 地址登陆

如果您不知道 DAP849 当前的 IP 地址，可以使用命令行 `ifconfig br-wan` 查看 DAP849 使用的 IP 地址，见第 22 页的“DAP849 IP 地址”。

4.2 使用 DAP849 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。

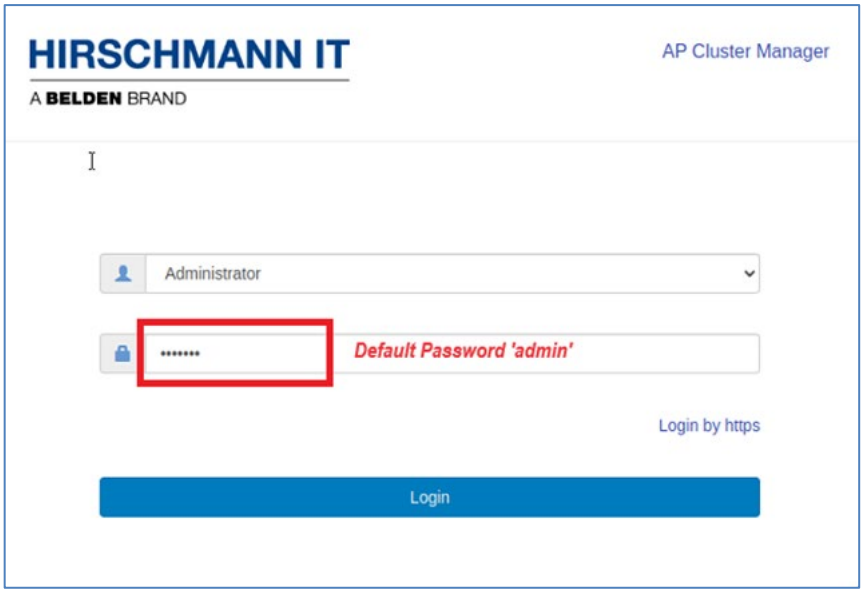


图 8：以 Administrator 登陆

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 DAP849 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 DAP849 作为虚拟控制器。
- **DAC 模式：**DAP849 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阅 DAC 用户手册。
- **BWO 模式：**DAP849 设备可以由 BWO 管理平台进行集中管理，由 BWO 完成配置和策略的下发，关于 BWO 模式的详细信息请参阅 BWO 用户手册。

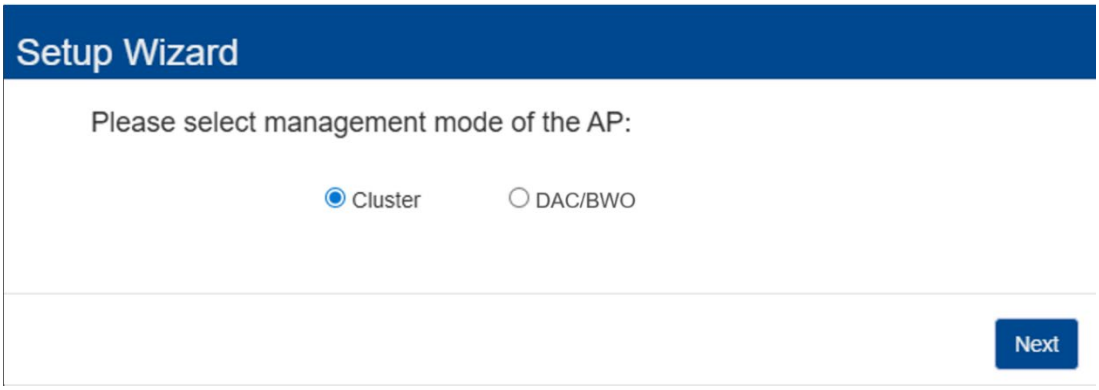


图 9：选择工作模式

☐ DAP849 Cluster Manager 欢迎页面。

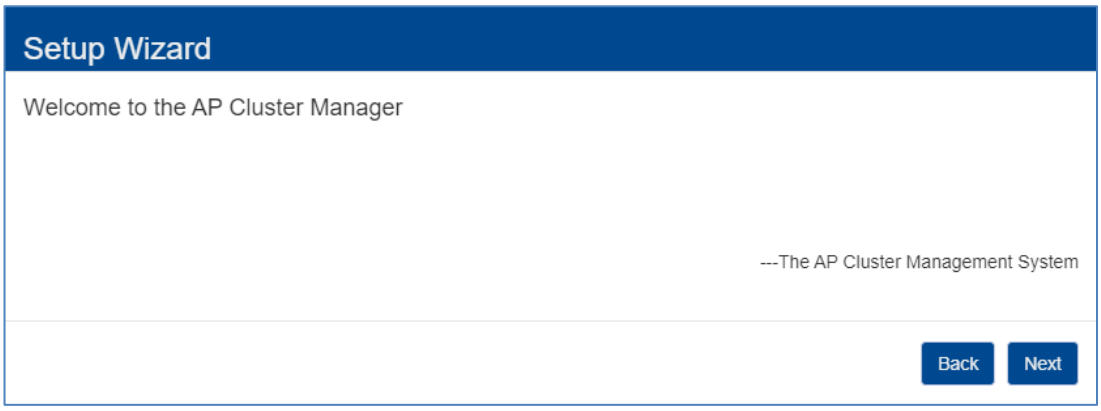


图 10：DAP849 Cluster Manager 欢迎页面

☐ 修改 administrator 的登陆密码。

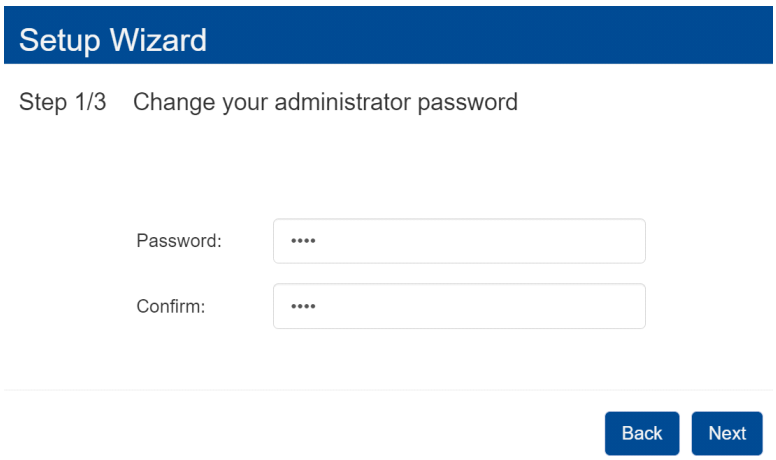


图 11：修改管理员账户密码

☐ 选择“Country/Region”和“Time Zone”。

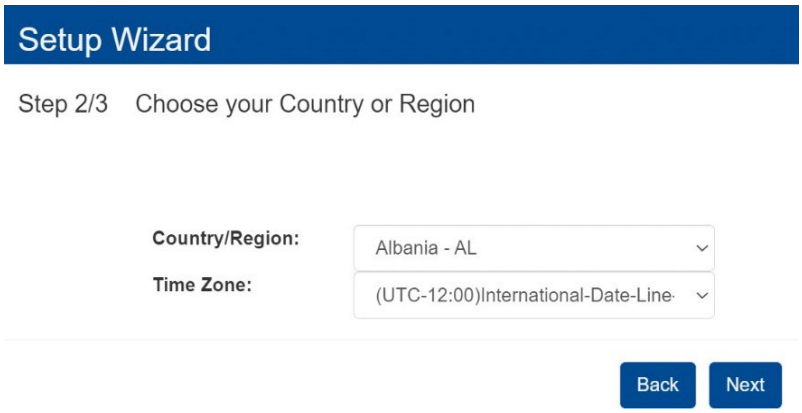


图 12：选择 Country/Region 和 Time Zone

☐ 创建一个新的 WLAN，请参阅第 33 页的“WLAN 页面”。

注意：创建新的 SSID 后，默认名为“mywifi-xx:xx”的 SSID 将会被删除。

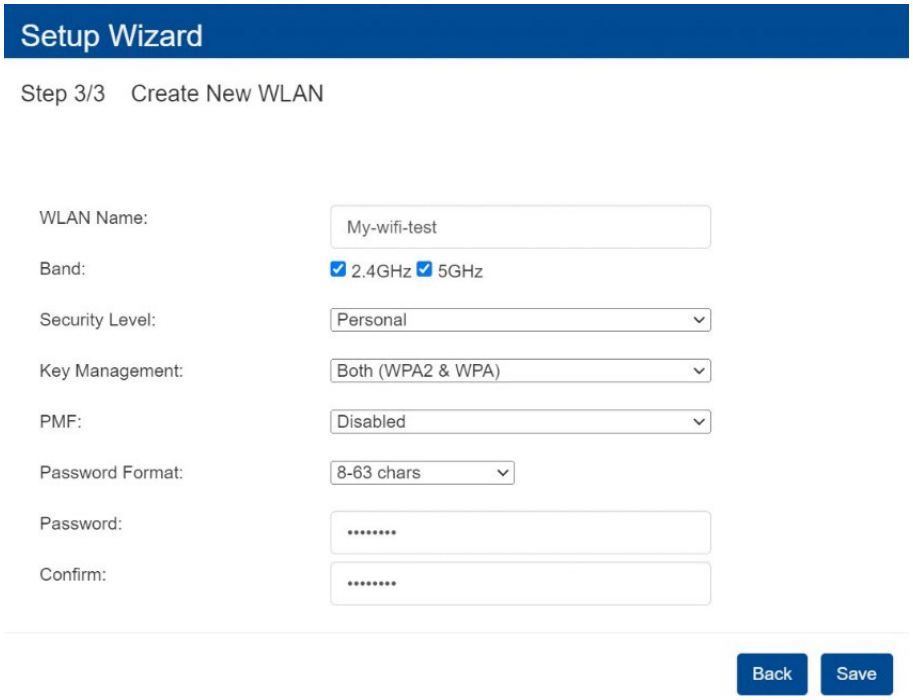


图 13：创建一个新的 WLAN

在完成设置向导后，DAP849 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。

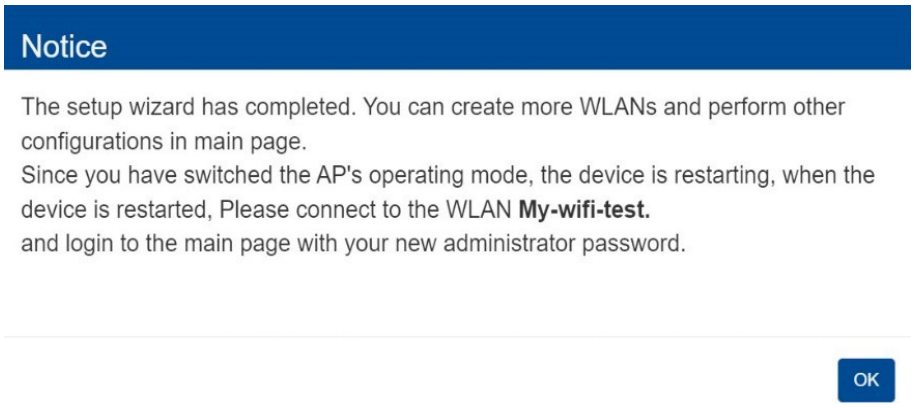


图 14：DAP849 切换模式并重新启动

当 DAP849 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。

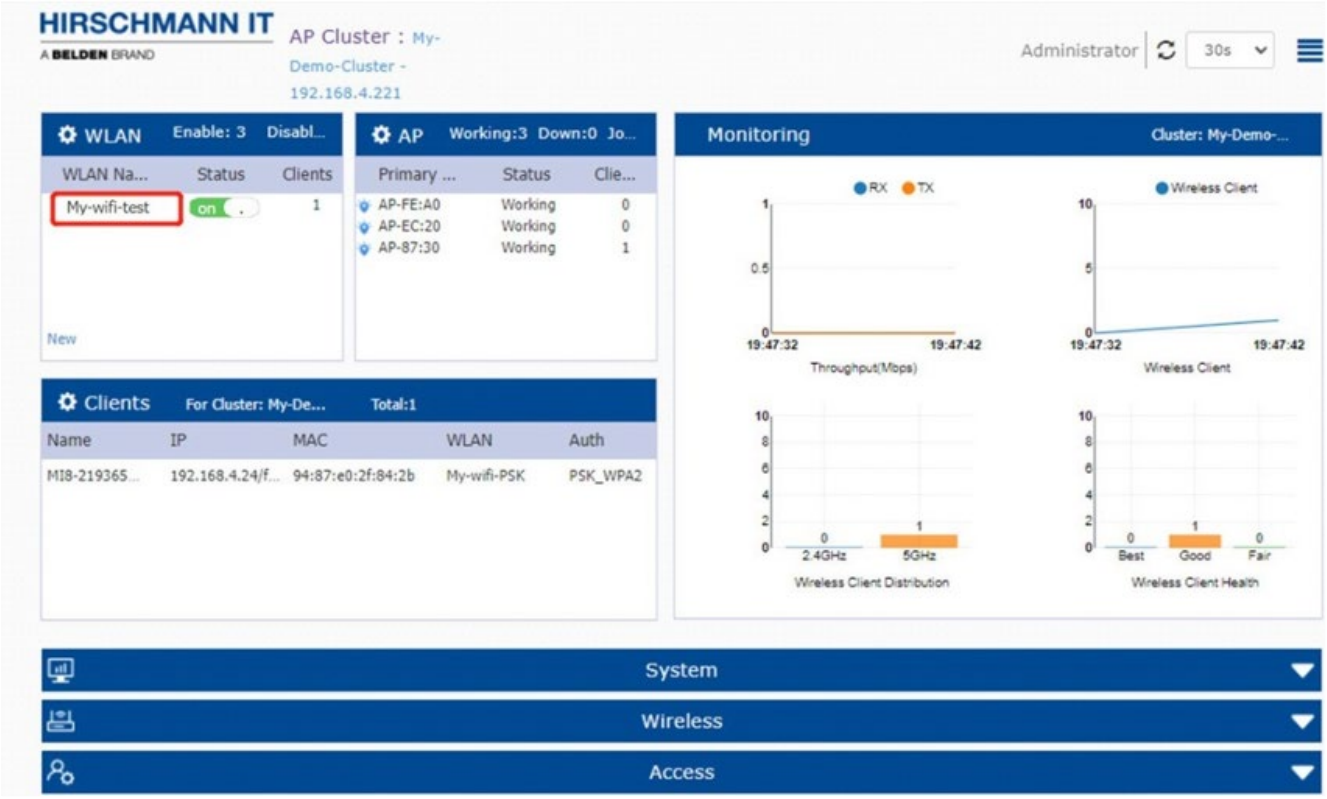


图 15：重新登陆 DAP849 Cluster Manager

5 DAP849 Cluster Manager 用户界面

在本章节中主要介绍了 DAP849 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
- DAP849 的其它信息

5.1 Dashboard 页面简介

DAP849 提供了一个 Dashboard 页面，用来展示当前的运行状态和配置信息。

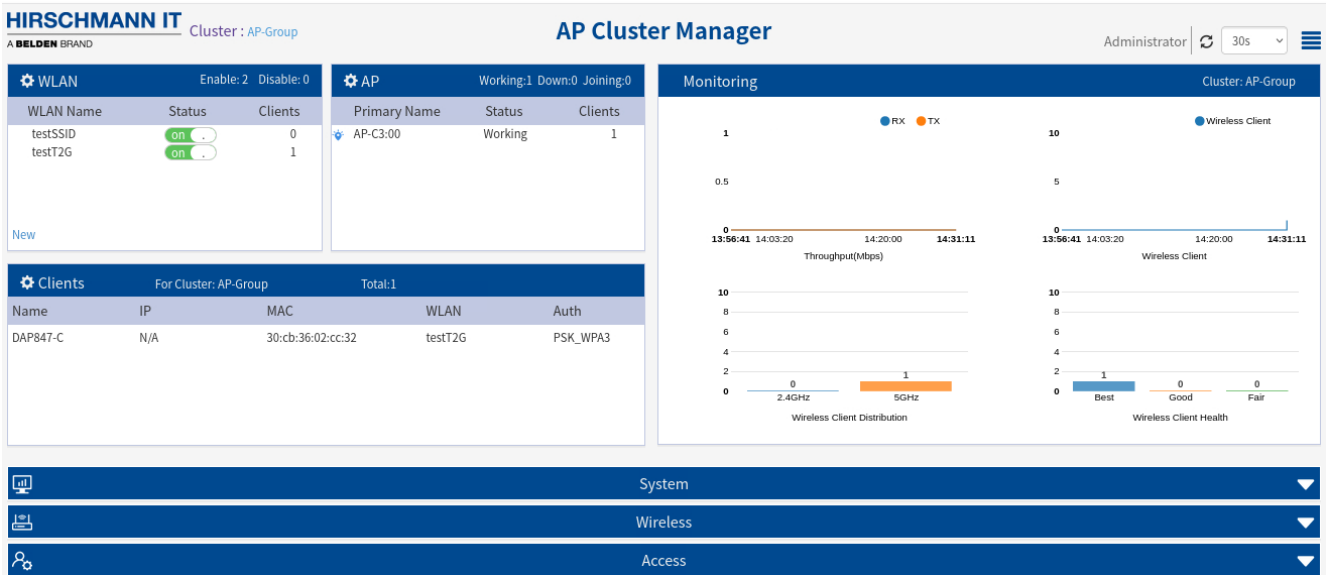


图 16：DAP849 主页面

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** 和 **Access** 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。

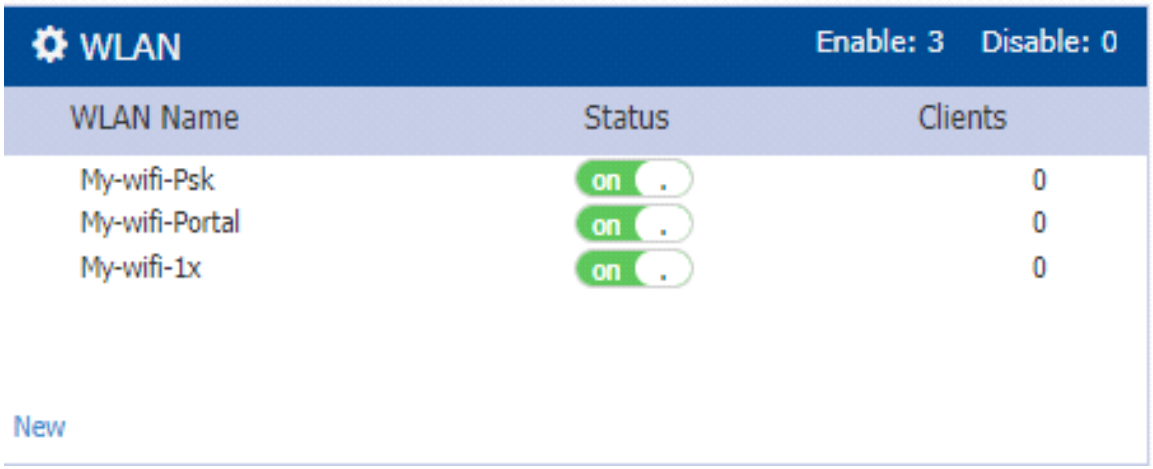


图 17：WLAN 页面

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： off 表示该 WLAN 未启用。 on on on on on on on on on on on on on 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。

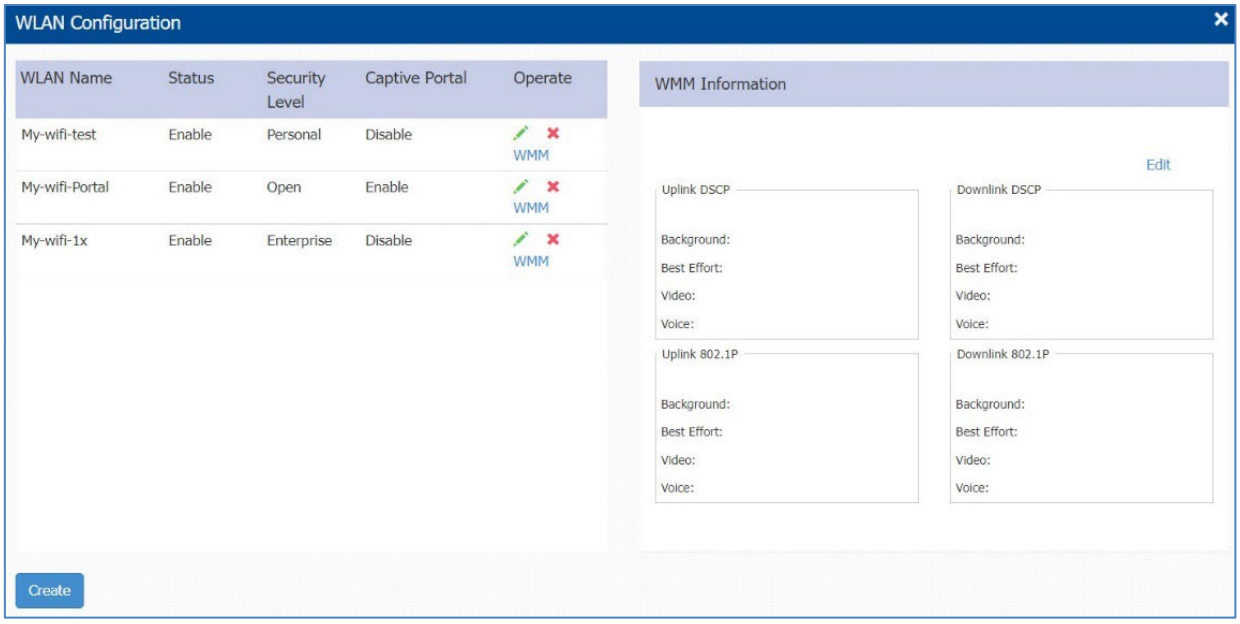


图 18：WLAN Configuration 页面

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： ▶ **“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： ▶ **“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 DAP849 的基本信息，包括 AP Primary Name 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。

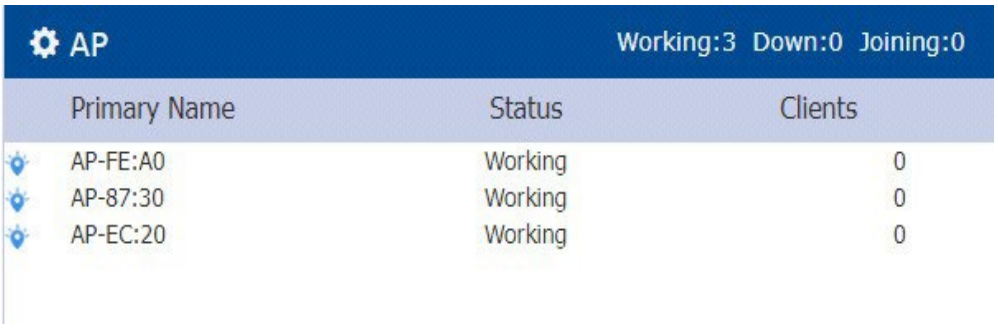
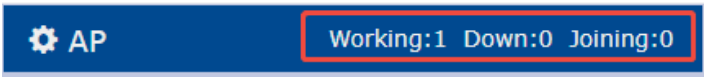


图 19：AP 页面

关键参数描述如下：

参数	描述
Primary Name	显示 DAP849 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 DAP849 的连接状态： ▶**Working**：表示该 DAP849 已连接到 PVM，工作正常。 ▶**Down**：表示该 DAP849 已断开与集群的连接。 ▶**Joining**：表示该 DAP849 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。



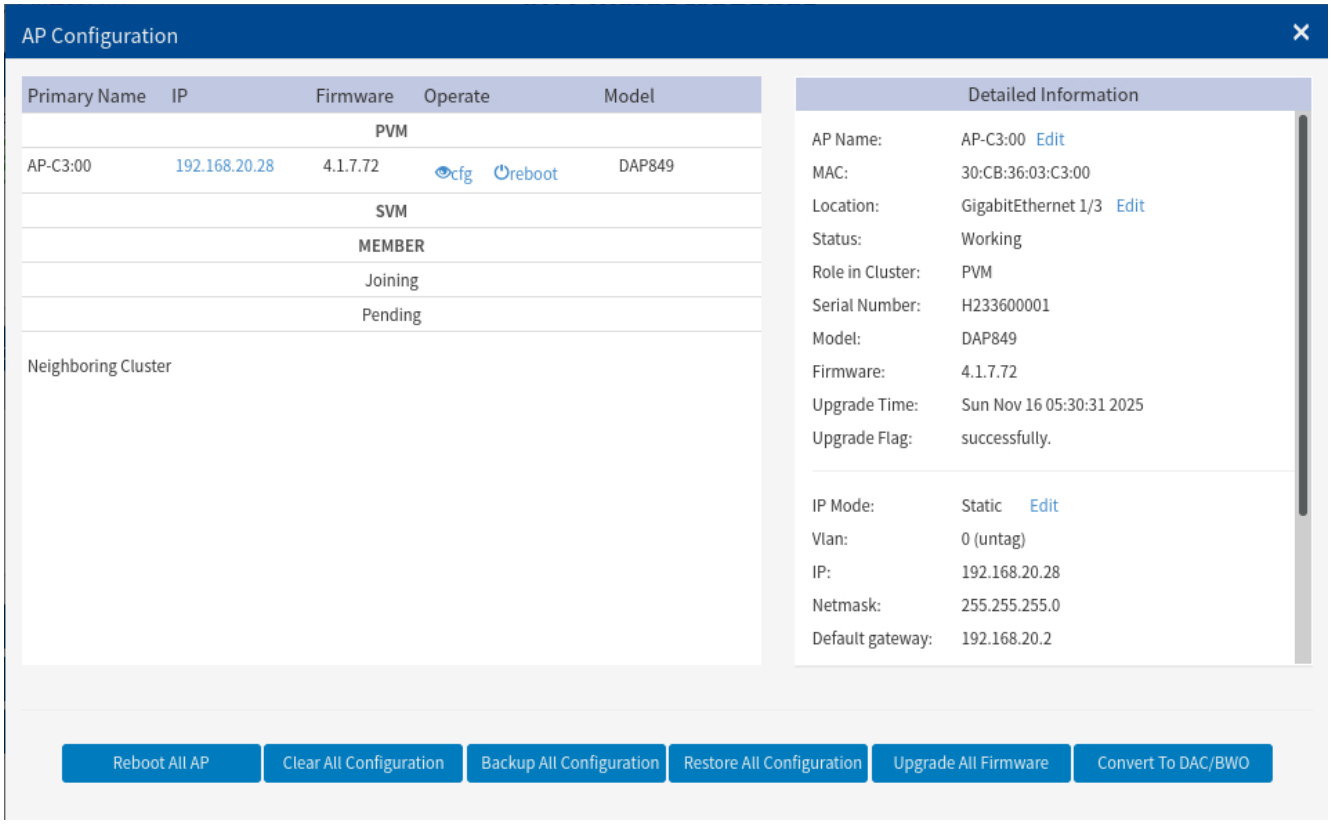


图 20：AP Configuration 页面

关键参数描述如下：

参数	描述
Primary Name	DAP849 名称。
IP	DAP849 的 IP 地址。
Firmware	DAP849 的软件版本。
Operate	DAP849 有两种可选操作： **cfg**：查看该 DAP849 的详细配置信息。 **reboot**：重启该 DAP849。
Model	DAP849 的型号。
PVM	表示该 DAP849 在集群中是 PVM。
SVM	表示该 DAP849 在集群中是 SVM。
MEMBER	表示该 DAP849 在集群中是普通成员。
Joining	处于 Joining 状态下的 DAP849，需要授权才能加入集群。
Pending	处于 Pending 状态下的 DAP849，需要升级软件才能加入集群。
Neighboring Cluster	具有不同集群 ID 的相邻 DAP849 集群。
Reboot All AP	重启集群中所有 DAP849 设备。

参数	描述
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 DAP849 设备升 WIFI 固件。
Convert To DAC/BWO	将 DAP849 由集群工作模式切换到 DAC 或 BWO 工作模式，一旦执行该操作，DAP849 将会重启并注册到 DAC 或 BWO 中，由 DAC 或 BWO 集中管理。 **Management Server**：DAC 或 BWO 的 IP 地址。
Detailed Information	所选 DAP849 的详细信息： ► AP Name：该 DAP849 的名称 ► MAC：该 DAP849 的 MAC 地址 ► Location：该 DAP849 的位置信息 ► Status：该 DAP849 的状态 ► Role in Cluster：群集中所选 DAP849 的角色 ► Serial Number：该 DAP849 的序列号（SN）。 ► Model：该 DAP849 的产品型号 ► Firmware：该 DAP849 的固件版本 ► Upgrade Time：该 DAP849 上次升级时间 ► Upgrade Flag：该 DAP849 上次升级的结果 ► IP Mode：该 DAP849 获取 IP 地址的方式 ► IP：该 DAP849 的 IP 地址 ► Netmask：该 DAP849 的 IPv4 地址网络掩码 ► Default gateway：该 DAP849 的默认网关 ► DNS：DNS 服务器
Kick Off	从集群中删除指定 DAP849，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	► **Cluster**：DAP 在集群模式下工作。 ► **DAC/BWO**：通过 DAC 或 BWO 平台集中管理 DAP。如需将 DAP849 的模式更改为 DAC/BWO 模式时，需要指定 DAC 或 BWO 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。

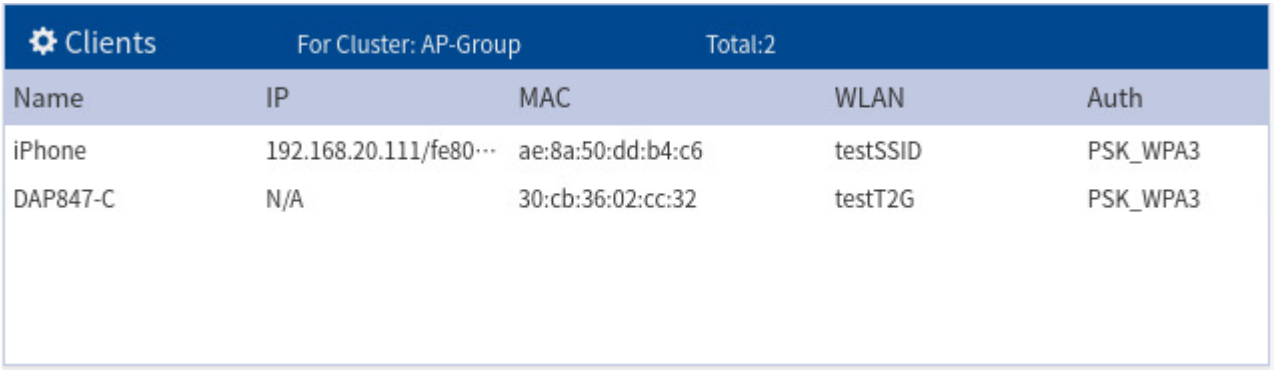


图 21：Clients 页面 – 基本模式

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 DAP849 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“✖”按钮，可以断开客户端与 DAP849 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。

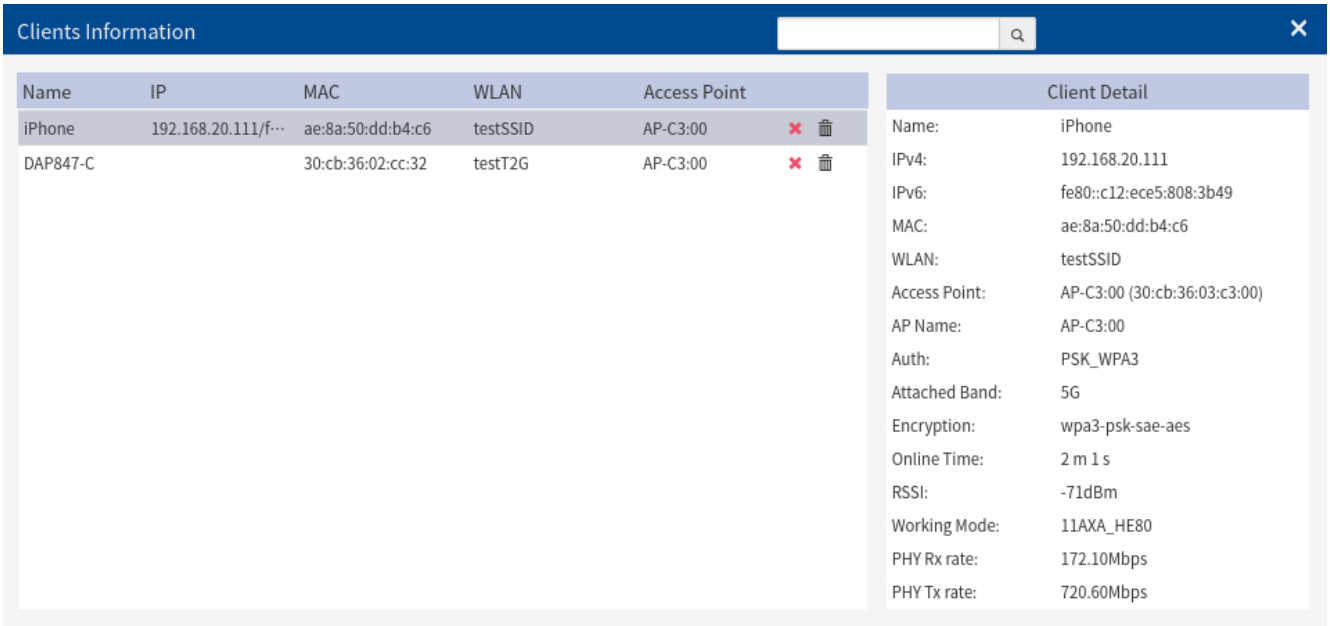


图 22：Clients information 页面

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 DAP849 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。

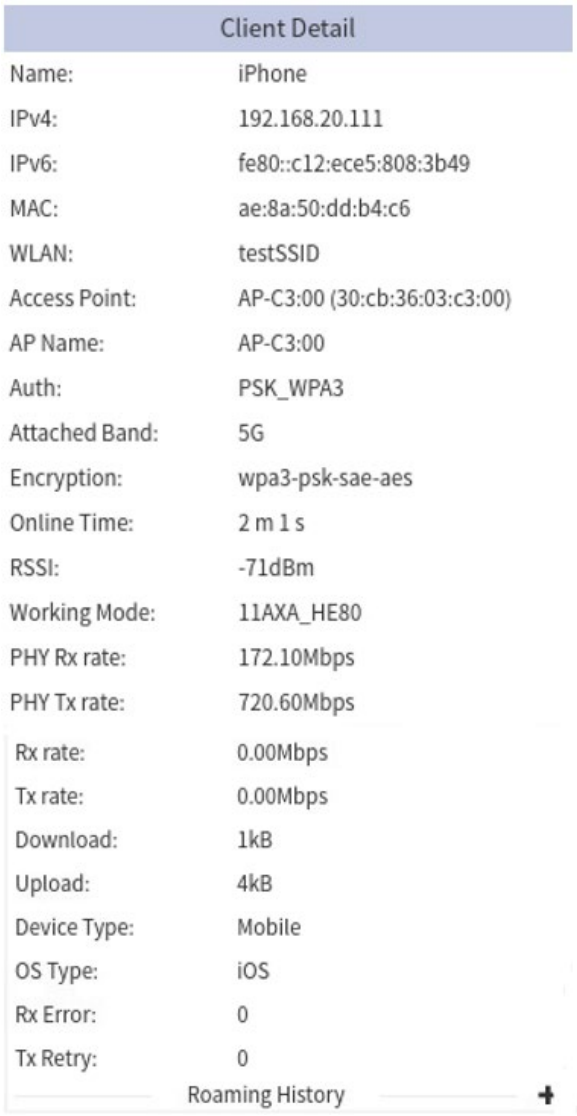


图 23：Client Detail 页面

■ 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 DAP849 设备名称（MAC 地址）。
AP Name	客户端所关联的 DAP849 设备名称。
Auth	客户端的身份验证类型：包括 Open、Portal（Captive Portal）、PSK

参数	描述
	（Personal）、802.1x（Enterprise）。
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-95~0dBm。
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	客户端的网络层接收速率，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	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。 **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。 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的顶部。 **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。

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 DAP849，切换为该 DAP849 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

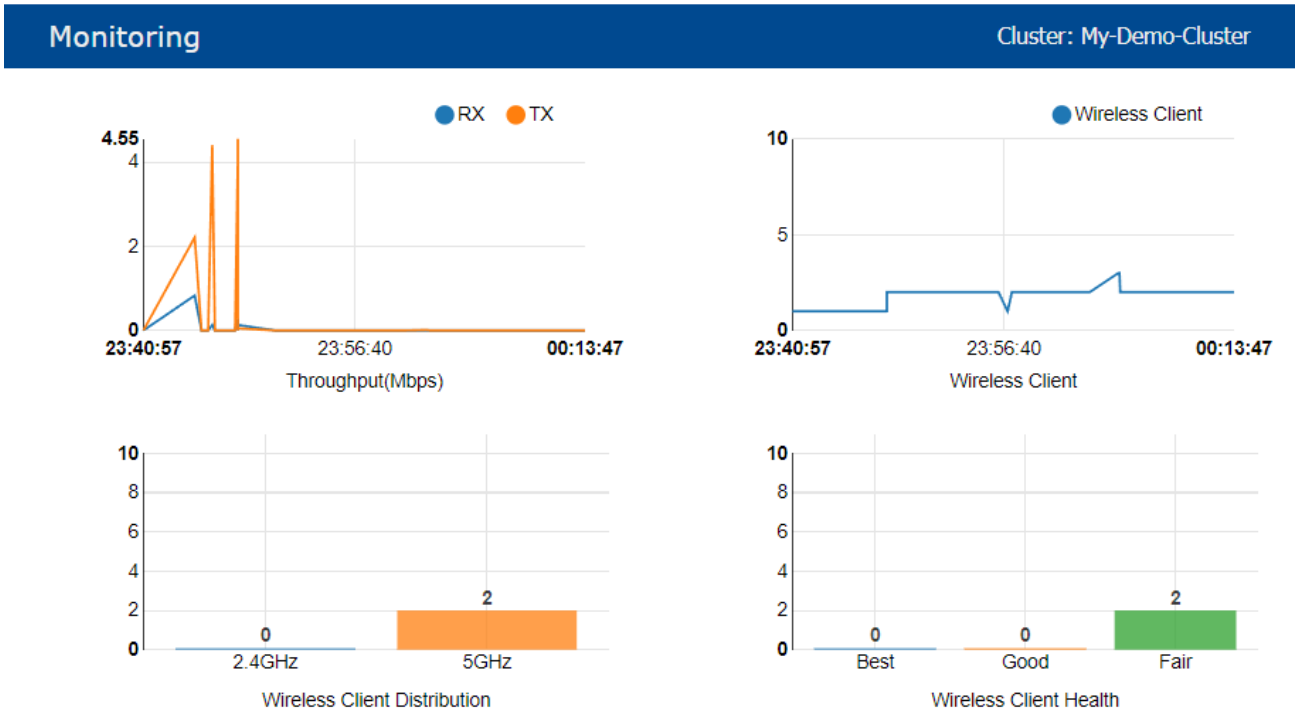


图 24：Cluster Monitoring 页面

关键参数描述如下：

参数	描述
RX	表示集群中所有 DAP849 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 DAP849 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 DAP849 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	根据客户端的信噪比 SNR 来评估客户端和 DAP849 之间的无线链路质量，分为以下三个级别： ▶Best：SNR 超过 30 的客户端数量（含）。 ▶Good：SNR 在 15 到 30 之间的客户端数量。 ▶Fair：SNR 小于 15（含）的客户数量。

5.5.2 基于 WLAN 的监控

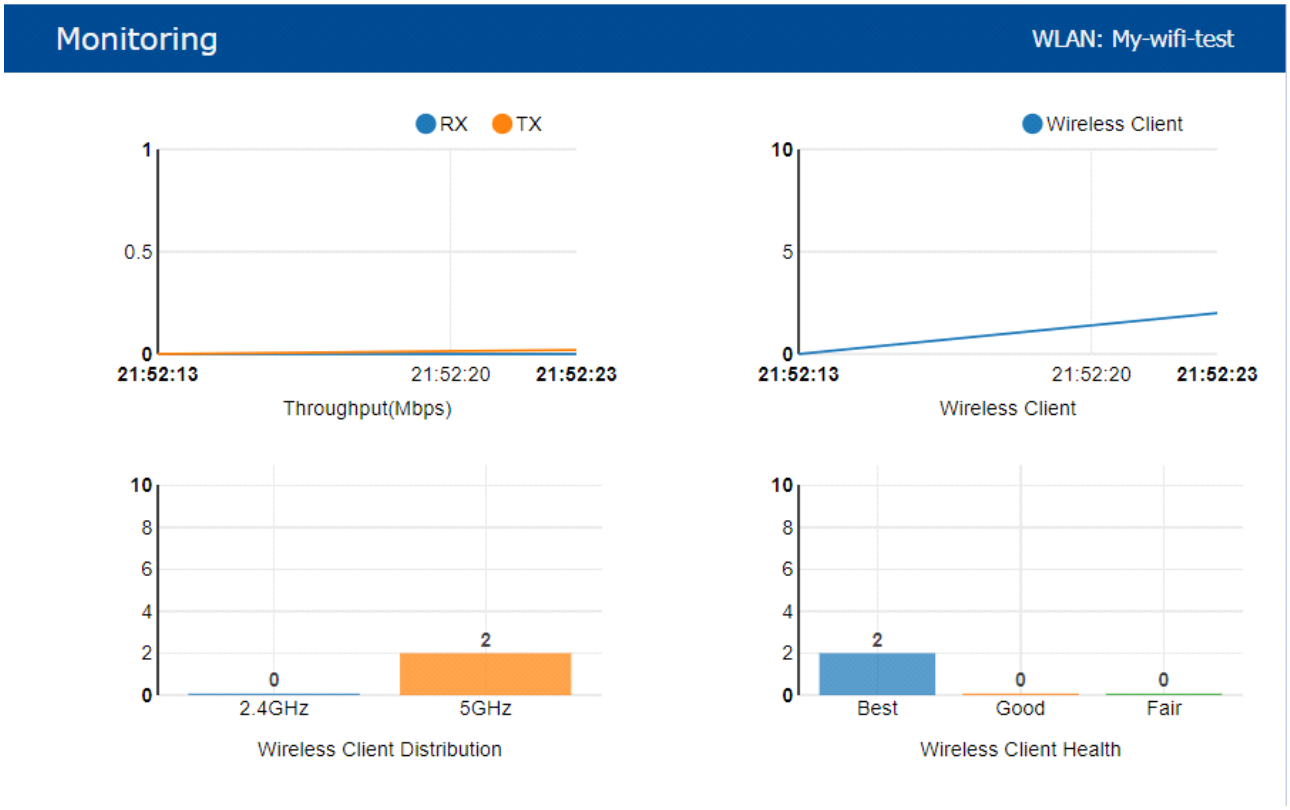


图 25：WLAN Monitoring 页面

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	在该 WLAN 下，按照客户端的信噪比 SNR 来评估客户端和 DAP849 之间的无线链路质量，分为以下三个级别： ▶Best：SNR 超过 30 的客户端数量（含）。 ▶Good：SNR 在 15 到 30 之间的客户端数量。 ▶Fair：SNR 小于 15（含）的客户数量。

5.5.3 基于 AP 的监控

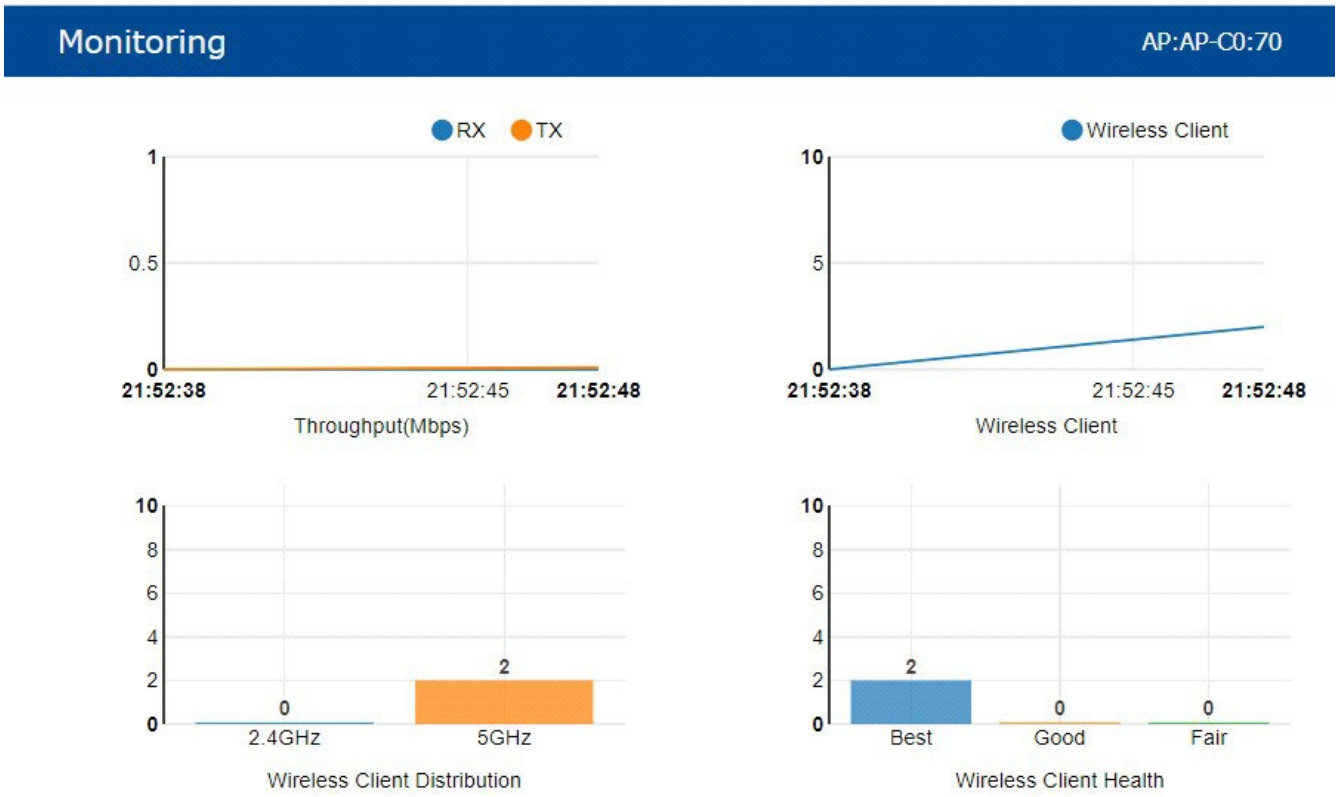


图 26：AP Monitoring 页面

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 DAP849 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，按照客户端的信噪比 SNR 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：SNR 超过 30 的客户端数量（含）。 ▶Good：SNR 在 15 到 30 之间的客户端数量。 ▶Fair：SNR 小于 15（含）的客户数量。

5.5.4 基于客户端的监控

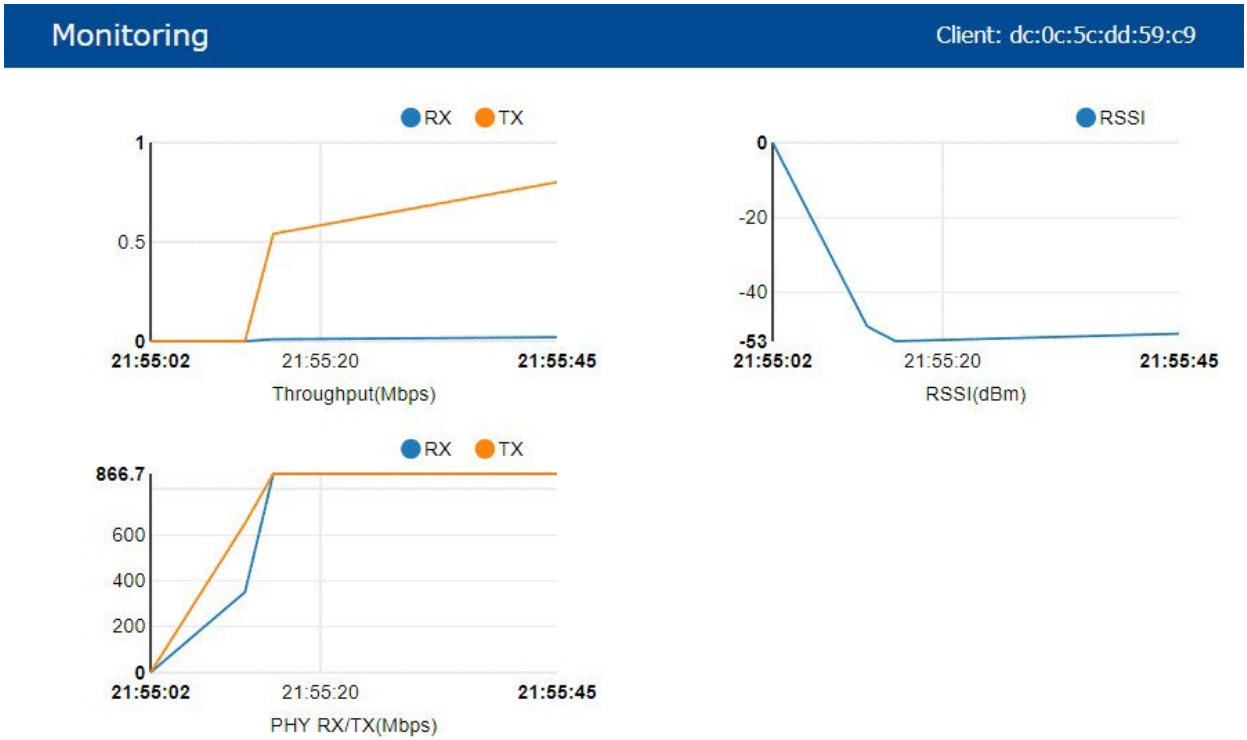


图 27：Client Monitoring 页面

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 的详细介绍请参阅第 122 页的“系统管理”。

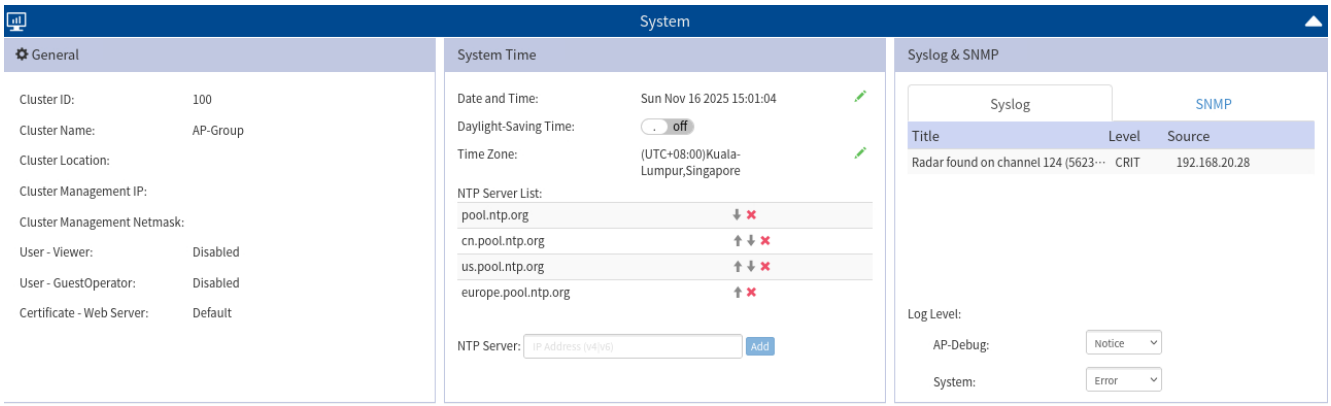


图 28：System 页面

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 的详细介绍请参阅第 138 页的“无线管理”。

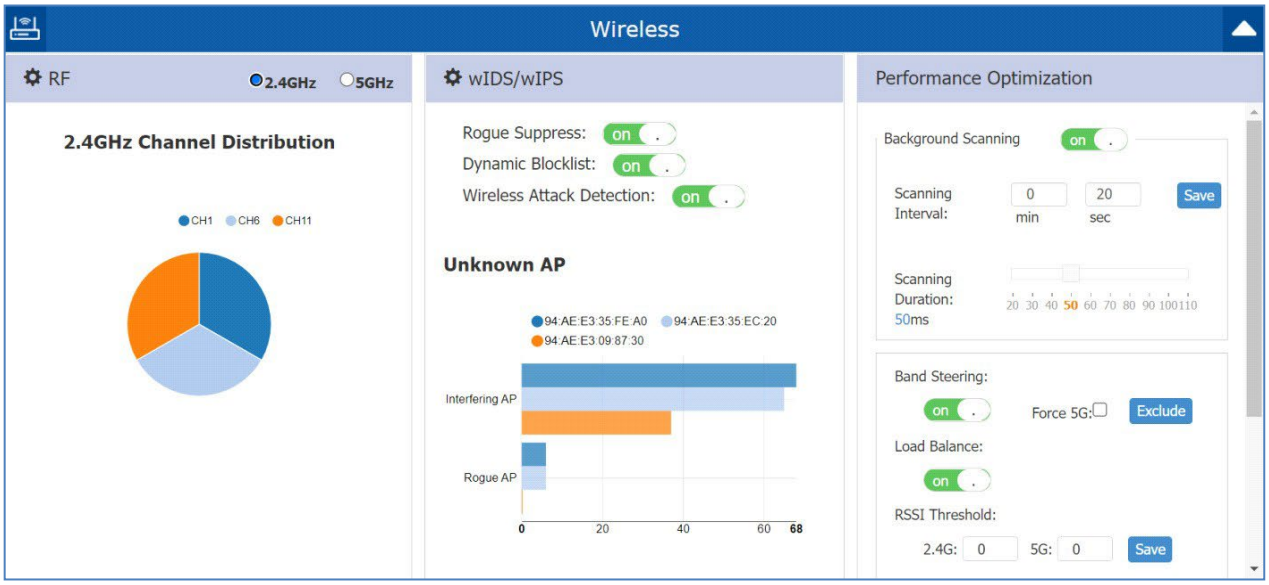


图 29：Wireless 页面

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，请参阅第 157 页的“Access 页面”。

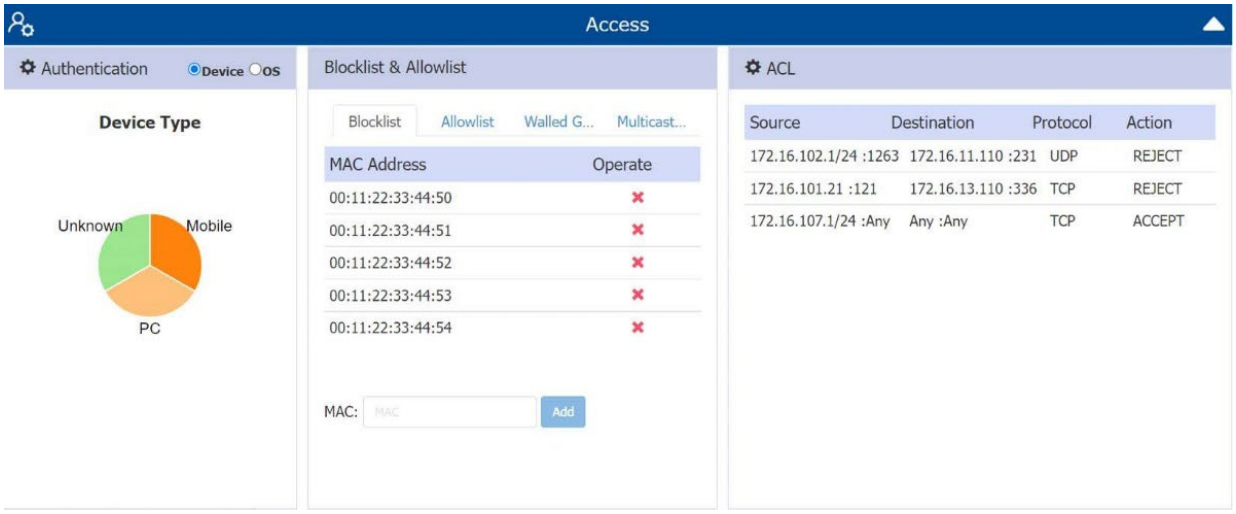


图 30：Access 页面

5.9 DAP849 的其它信息

有关 DAP849 的其他信息，如 About, Tools 等，请通过单击右上角的“**More**”来查看。

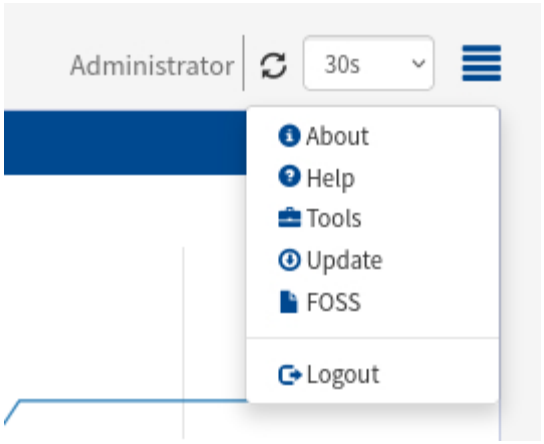


图 31：DAP849 的其他信息

- **About**：包含了 DAP849 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。

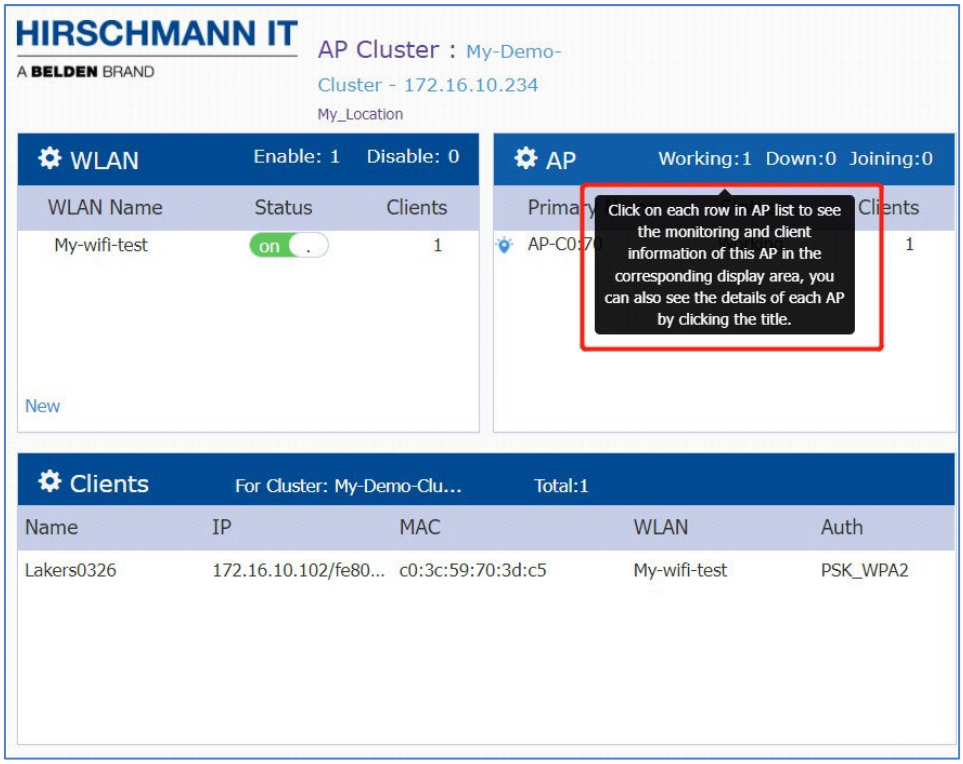


图 33：Online help

- **Tools**：DAP849 中集成的一些基础的故障排查工具，详细信息请参阅第 177 页的“DAP849 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。
- **FOSS**：免费的开源软件。
- **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**”。

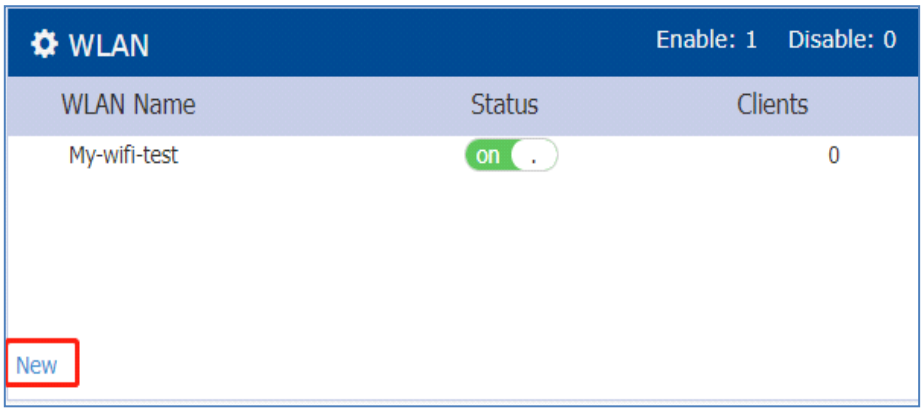


图 34：WLAN 基本模式

在弹出的“**Create New WLAN**”页面完成 WLAN 的配置。

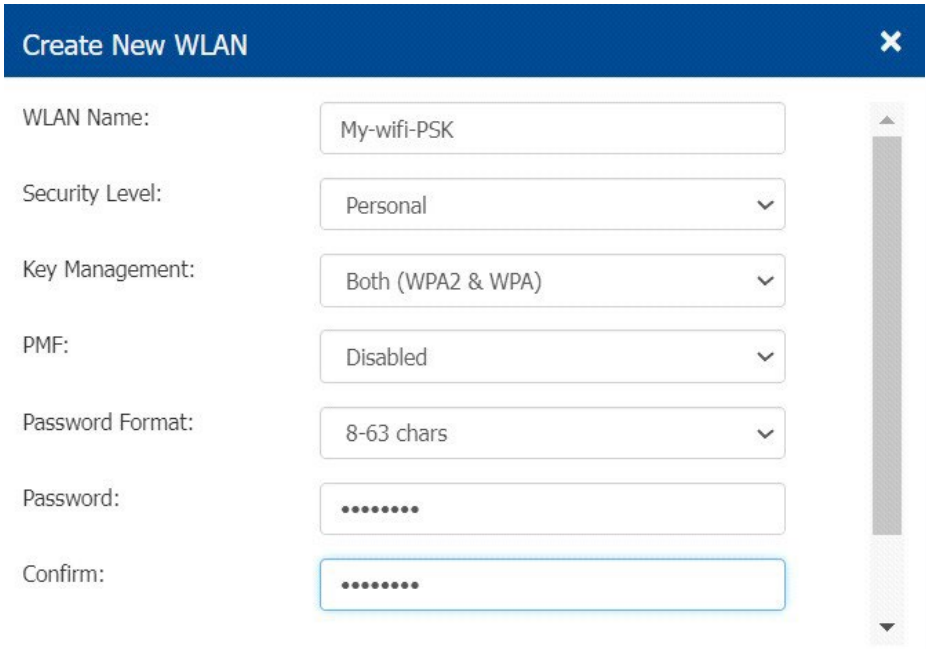


图 35：Create New WLAN 页面

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

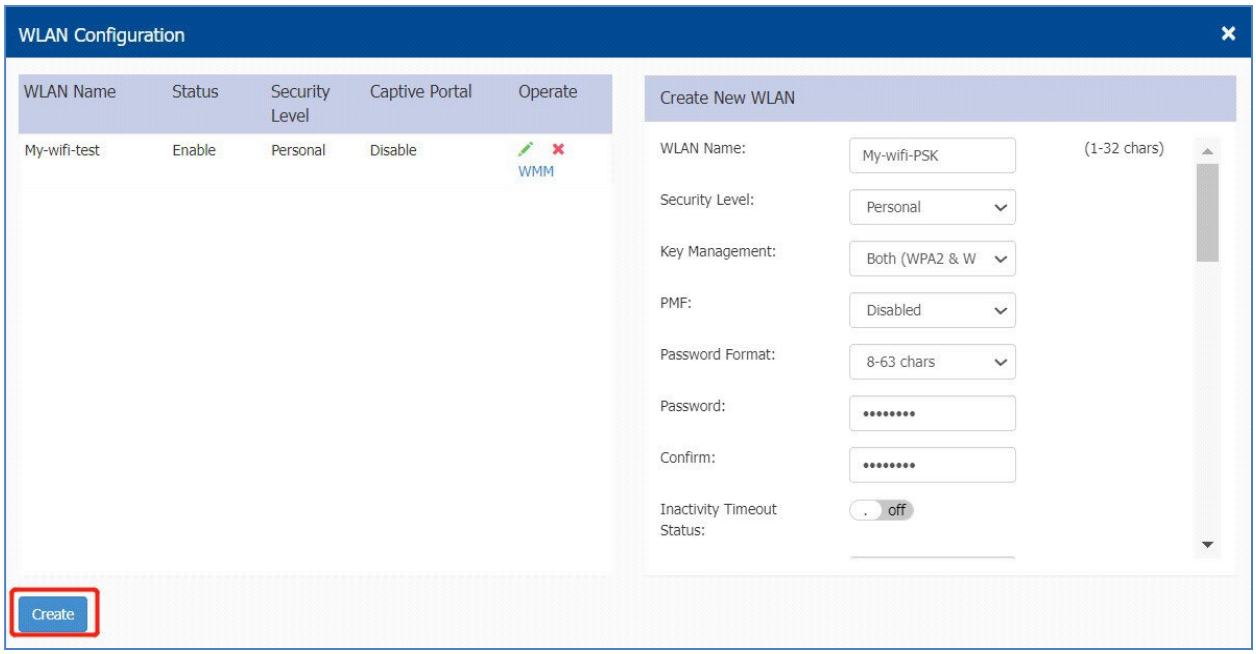


图 36：在 WLAN Configuration 页面中创建 WLAN

6.2 WLAN 的安全类型

在集群模式下，DAP849 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。

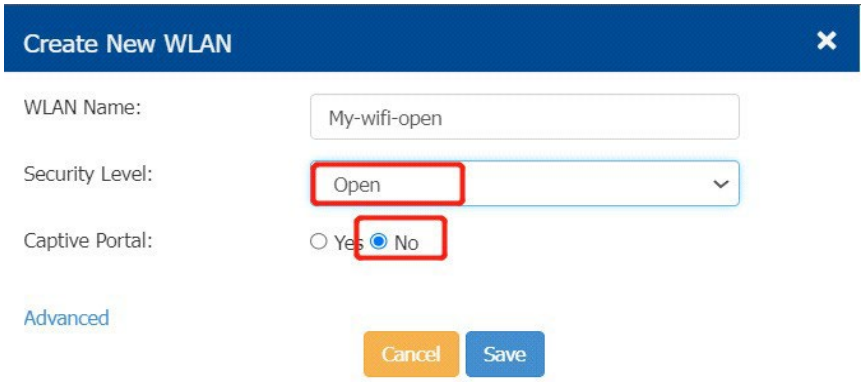


图 37：创建一个 Open 类型的 WLAN

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，请参阅第 161 页的“Portal 认证”。

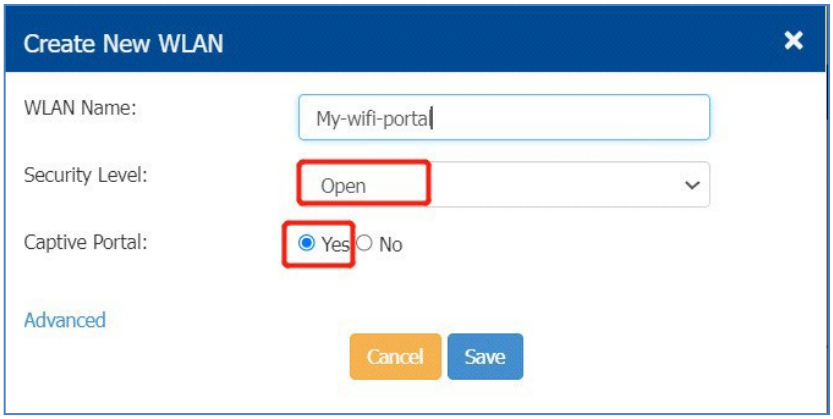


图 38：创建一个 Portal 认证类型的 WLAN

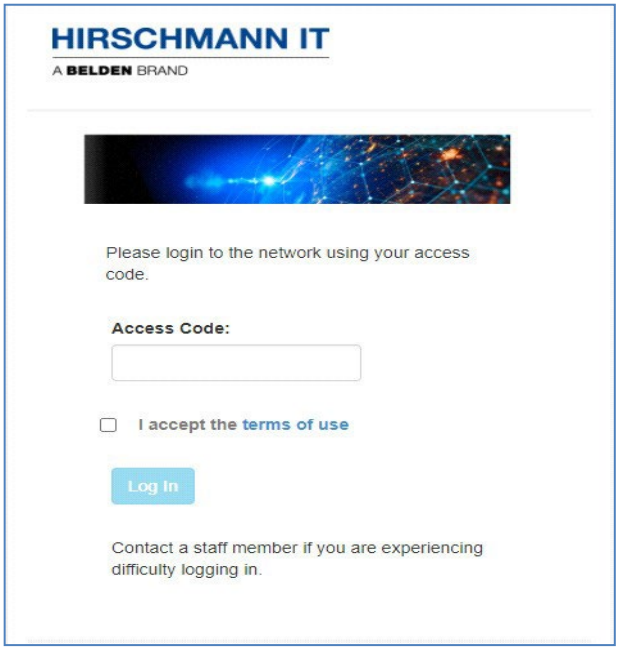


图 39：Portal 登陆页面

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：

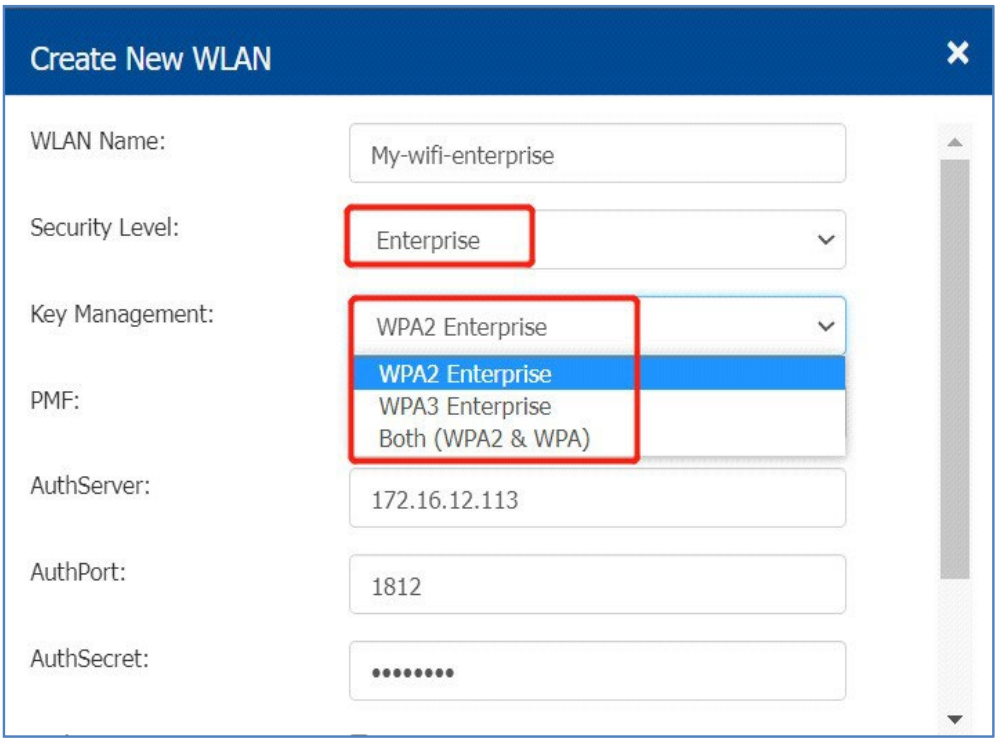


图 41：创建一个 Enterprise 类型的 WLAN

- **WPA2-Enterprise**：WPA2-Enterprise 是 WPA2 的一种认证方式，主要被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。通过动态协商密钥和随机数生成机制，彻底消除了离线字典攻击的风险。WPA3-Enterprise 强制启用 PMF（Protected Management Frames），通过加密和签名保护信标帧、认证帧等管理类数据，有效抵御 KRACK 攻击和去认证洪水攻击。

图 42：CNSA Suite

CNSA Suite (Commercial National Security Algorithm Suite)，在 WPA3-Enterprise 的基础上增加了一种更加安全的可选模式。CNSA Suite 引入 了 192 位加密强度的 Suite-B 安全套件，采用了 AES-256 加密算法和 GCMP-256 认证协议。相较于 WPA2-Enterprise 的 128 位加密，密钥空间扩大了 2^64 倍，显著提升了抵御暴力破解攻击的能力，为网络用户提供更高级别的安全性保护。

- 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**

  DAP849 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 DAP849，DAP849 仅对支持 PMF 的终端的管理帧进行加密保护。在强制方式下，DAP849 只允许支持 PMF 的终端接入。

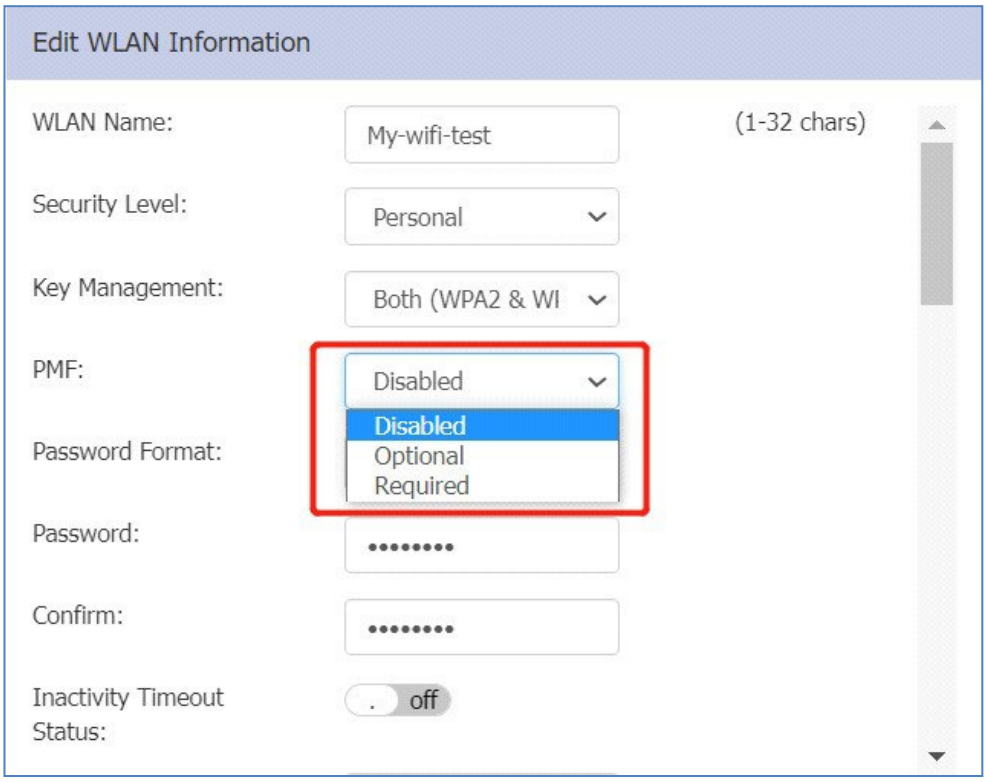


图 43：WLAN 中 PMF 的配置

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 PMF 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

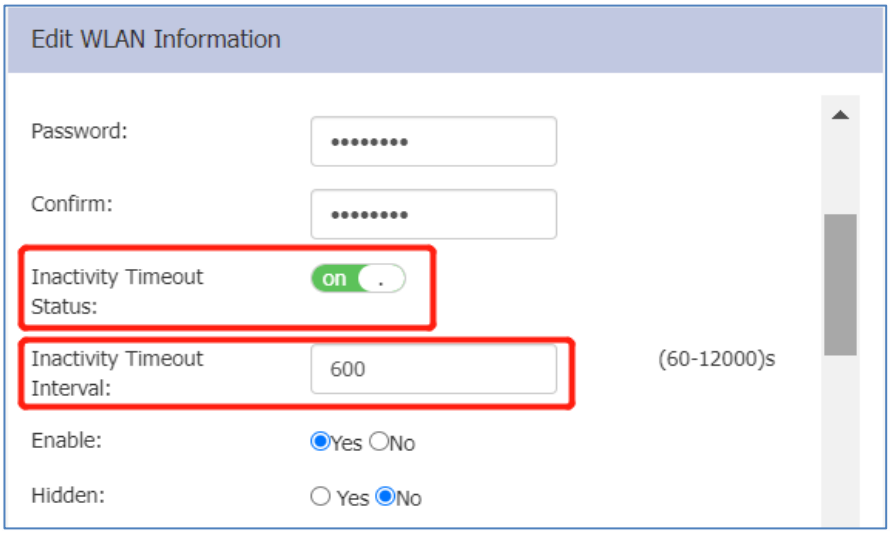


图 44：Inactivity timeout 配置

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 DAP849 设备进行任何通信，那么 DAP849 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

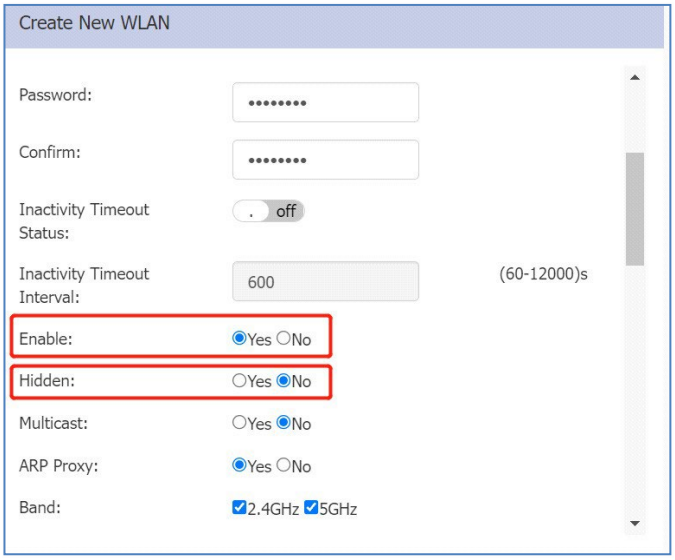


图 45：开启或隐藏 WLAN

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，DAP849 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 DAP849 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。

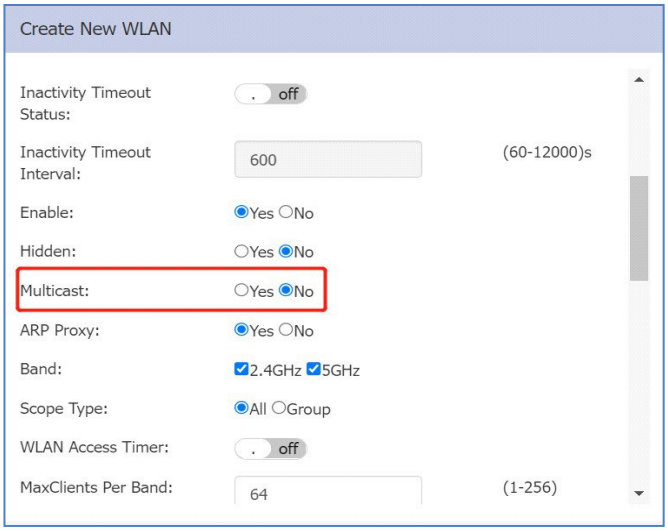


图 46：Multicast 配置

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，DAP849 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，DAP849 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，DAP849 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，这样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。

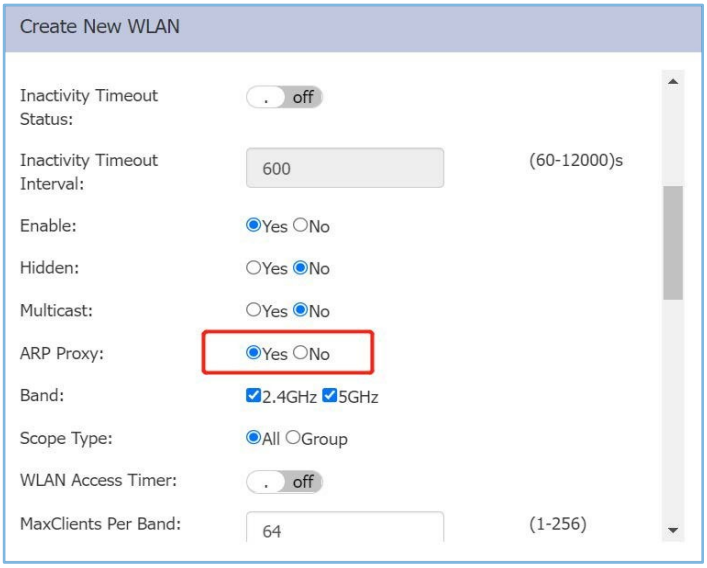


图 47：ARP proxy 配置

注意：DAP849 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 DAP849 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。

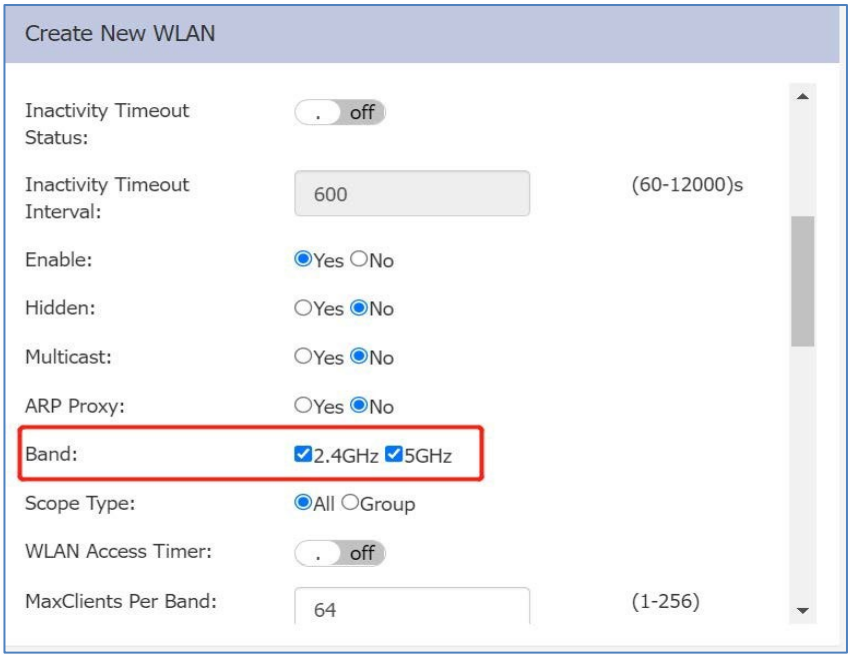


图 48：Band 配置

- **Train2Ground：**Train2Ground 用于 DAP847-XXC 关联，默认关闭，开启后只能用于 DAP847-XXC 连接，同时 ARP Proxy 和 Client Isolate 失效。仅支持 WPA2-Enterprise、WPA3-Enterprise、WPA3 Personal 和 WPA&WPA2 Personal 加密方式。

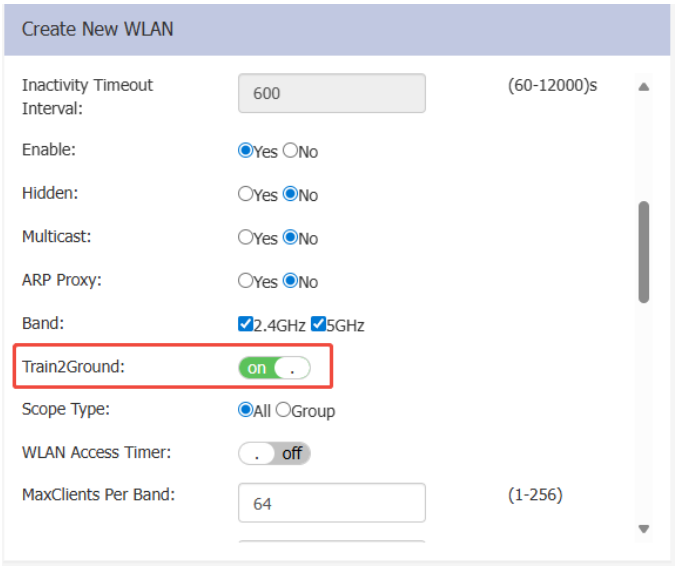


图 49：Train2Ground 配置

- **Scope Type**：Scope Type 用来指定该 WLAN 在集群中的 DAP849 上应用的范围，即哪些 DAP849 设备会广播这个 WLAN。

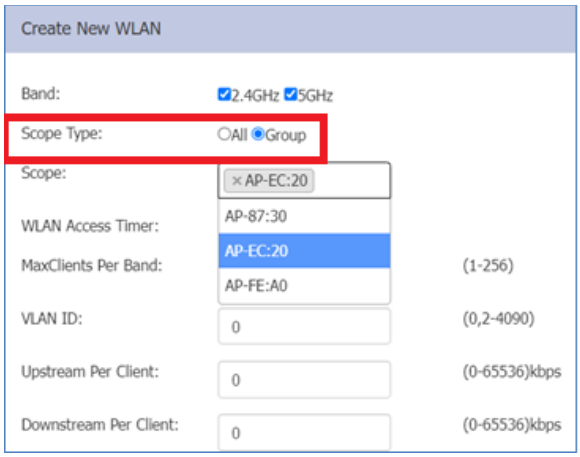


图 50：Scope Type 和 Scope 配置

参数	描述
All	该 WLAN 的配置将下发到集群中所有 DAP849 上。
Group	该 WLAN 的配置会下发到集群里选定的 DAP849 组中。

▶ WLAN Access Timer

指定 WLAN 的工作周期，DAP849 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，DAP849 将一直释放该 WLAN 信号，如图 51 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 52 所示。

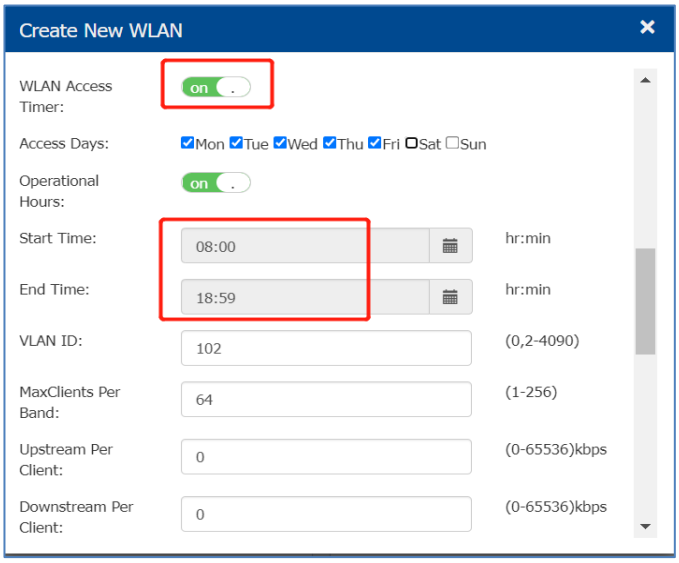


图 51：WLAN access timer 配置

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。

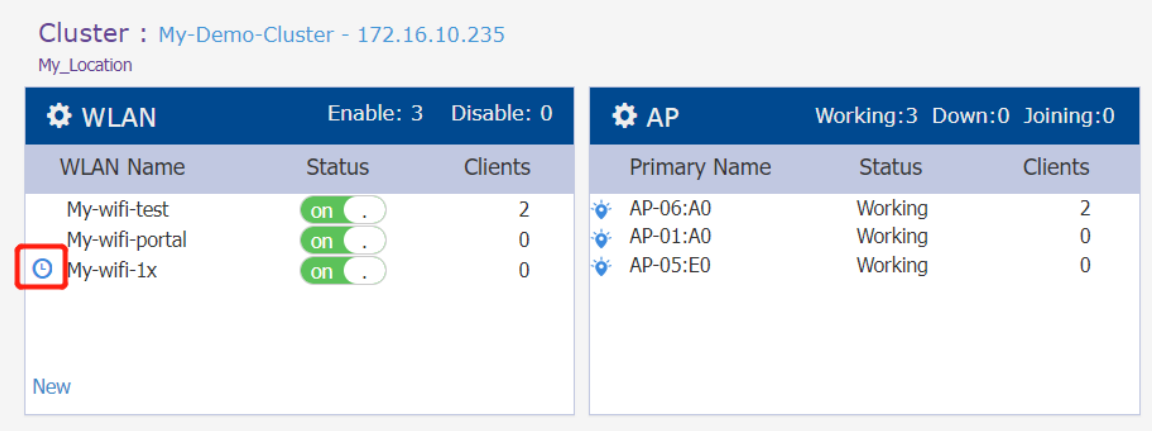


图 52：WLAN Access Timer 标识

- **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 DAP849 中创建对应的网桥接口处理用户的流量转发。

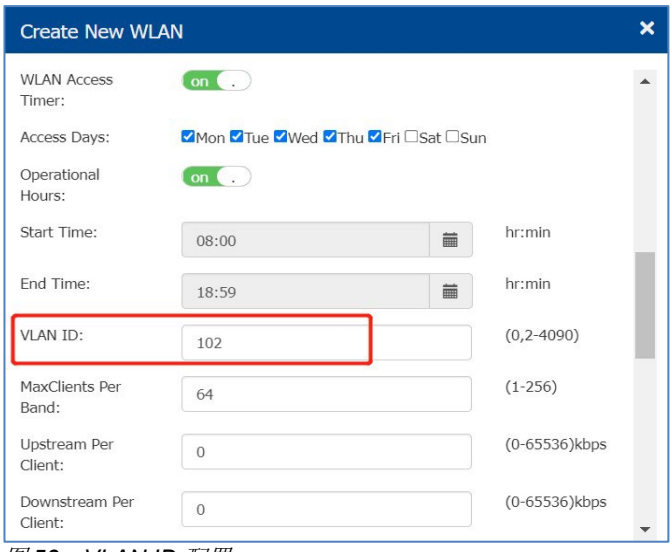


图 53：VLAN ID 配置

您可以在 CLI 下使用命令“brctl show”来检查 VLAN 的配置。

图 54：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，DAP849 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。

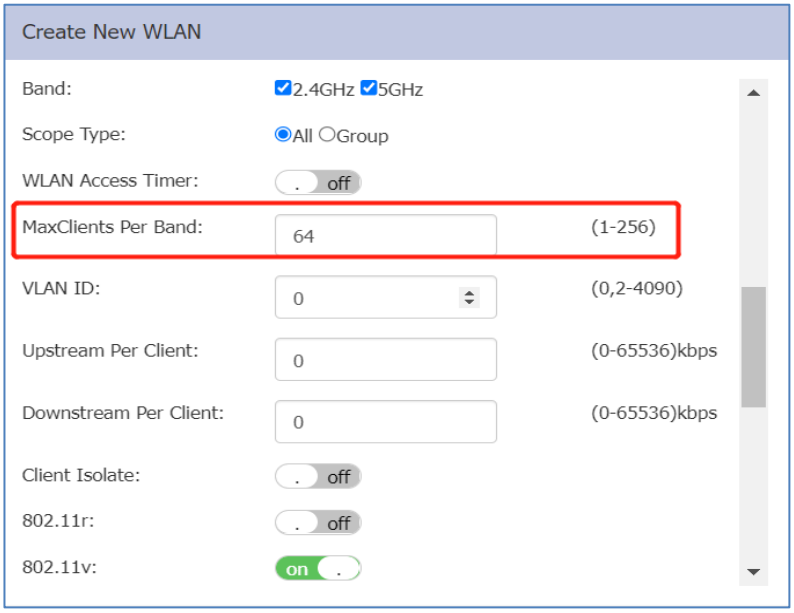


图 55：MaxClients per band 配置

- **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。

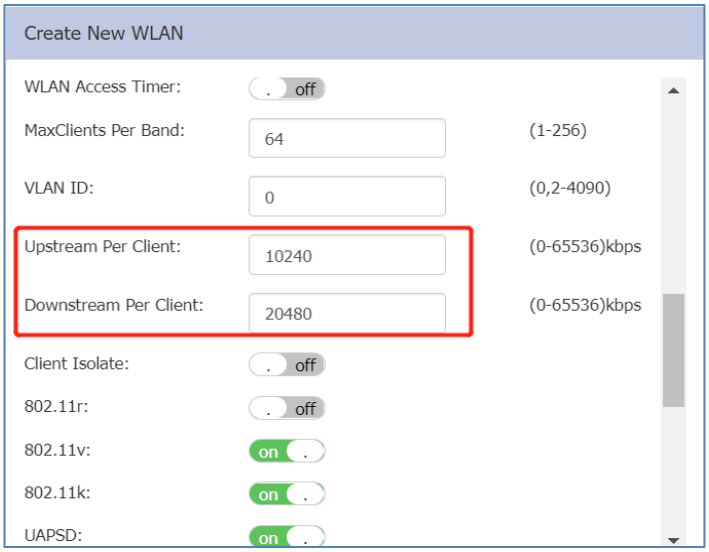


图 56：Clients 流量限速配置

- **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 57：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（DAP849）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 58：802.11r 配置

- **802.11k/v**：DAP849 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。

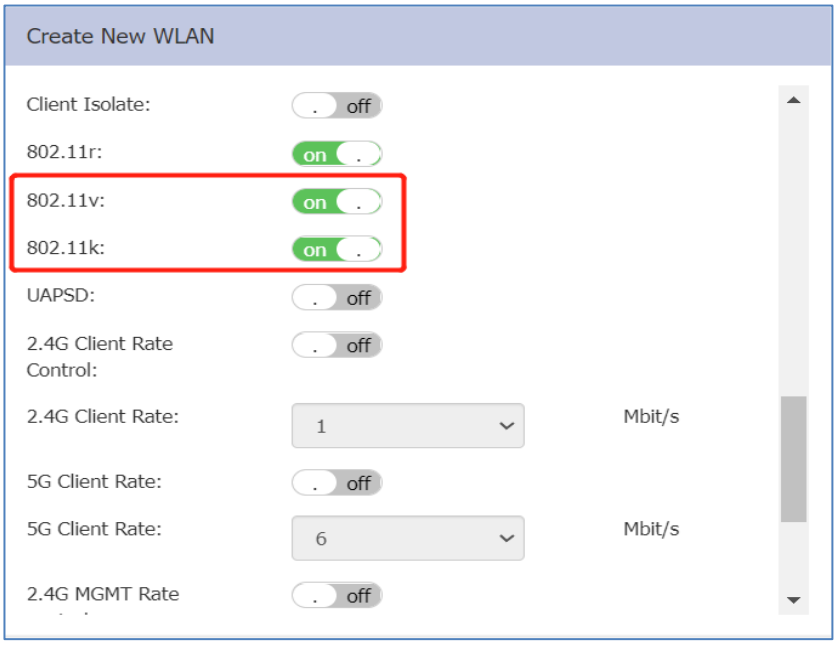


图 59：802.11k/v 配置

- 当在 WLAN 上启用 IEEE 802.11k 和 IEEE 802.11v 功能时，“Roaming

RSSIThreshold”将触发 DAP849 和无线客户端之间的 IEEE 802.11k 和 IEEE 802.11v 消息交换。

- 当 DAP849 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 DAP849。
- 基于接收到的数据，DAP849 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 DAP849 发送的 IEEE 802.11v 事件中获取一个目标 BSSID，还是选择在 DAP849 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。

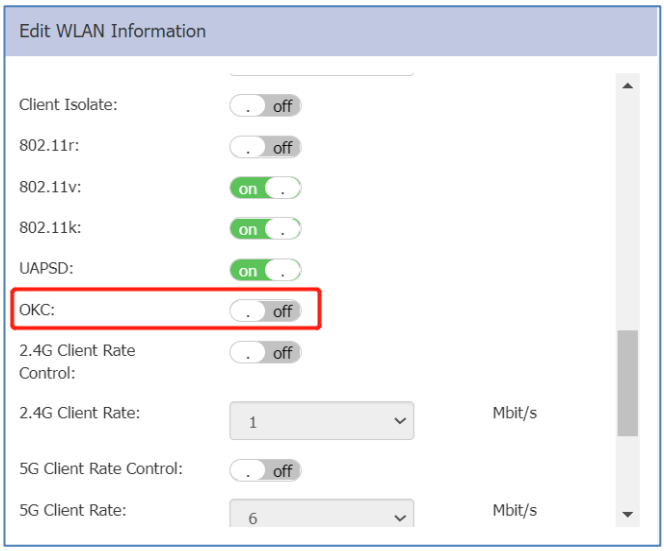


图 60：OKC 配置

- **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 DAP849 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。

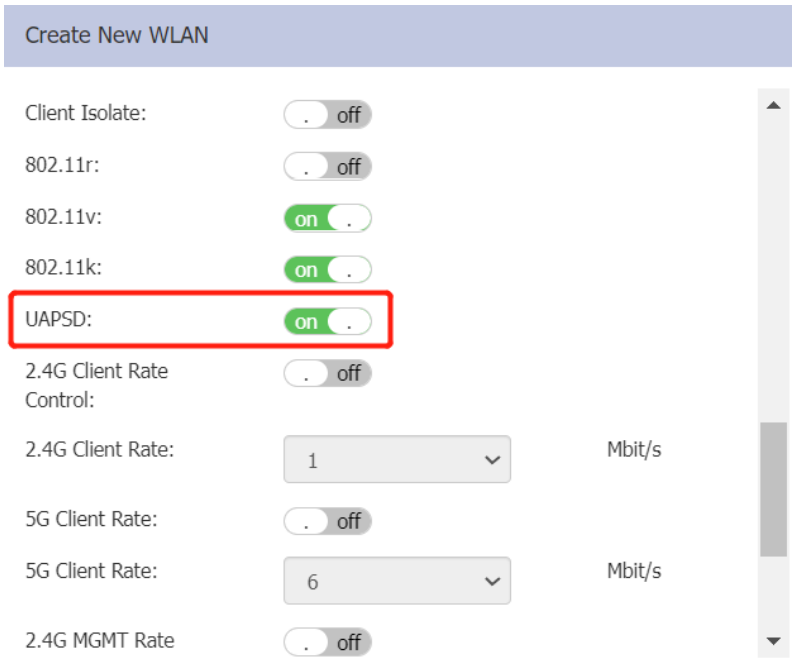


图 61：UAPSD 配置

- **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 62 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 DAP849。推荐值为 12Mbit/s，如图 62 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。如果数据帧的发送速率过低，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 62 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 DAP849。推荐值为 24Mbit/s，如图 62 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。如果数据帧的发送速率过低，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。

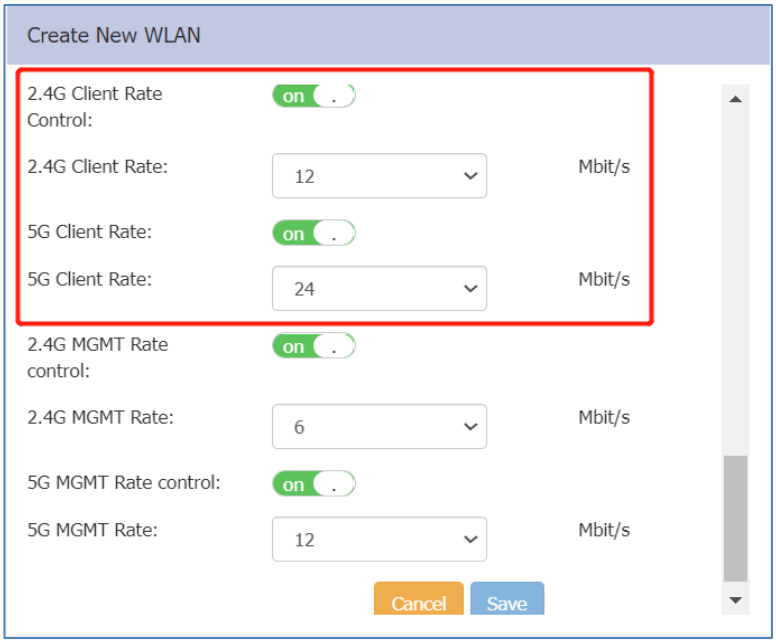


图 62：Client Rate 配置

- **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 63 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 63 所示，值越高，代表覆盖范围越小，值越低，代表覆盖范围越大，推荐值为 1Mbit/s。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 63 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 63 所示，值越高，代表覆盖范围越小，值越低，代表覆盖范围越大，推荐值为 6Mbit/s。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。

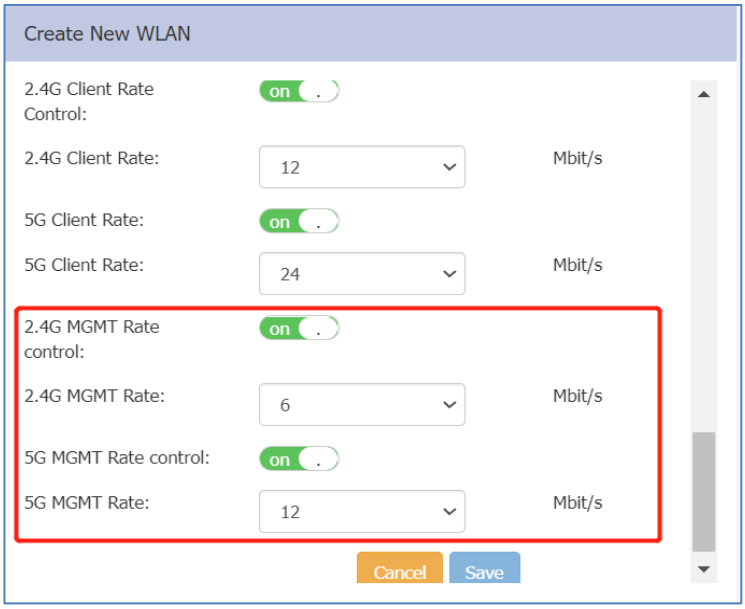


图 63：修改 2.4 GHz/5GHz 的 Management Rate

- **DTIM Interval:** DAP849 发送 DTIM (Delivery Traffic Indication Message) 的 beacon 间隔，用于告知无线客户端何时有数据需要接收，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 可让终端节电效果更好，但会占用接入点更多的缓存以及产生传输延迟，该参数需要根据实际使用场景正确的配置。缺省情况下，DTIM 周期参数为 1。如图 64 所示。

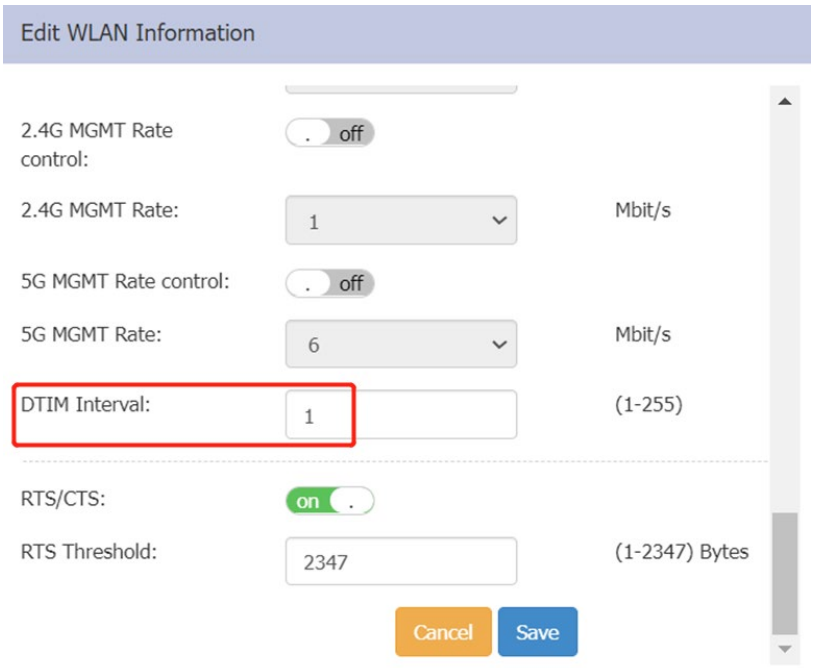


图 64：修改 DTIM Interval

- **RTS/CTS**：开启该功能，DAP849 将会发送 RTS/CTS 帧用于发现隐藏节点，

减少因隐藏节点出现发包冲突导致重传增加或者报文丢失，如图 65 所示。

- **RTS Threshold**: RTS threshold 的范围是 1-2347 Bytes，默认情况下是关闭状态，当 DAP849 要发送一个超过该门限值的数据包时，就会先发送 RTS 信号通知对方以防信号冲突，如图 65 所示。

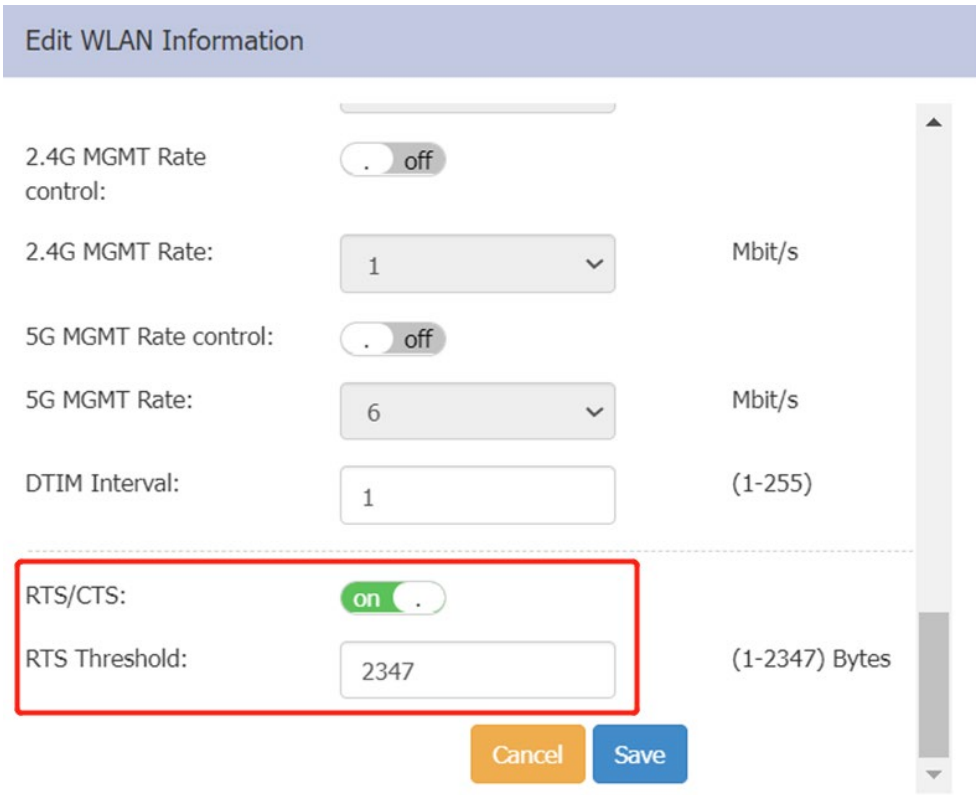


图 65: RTS/CTS 配置

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。

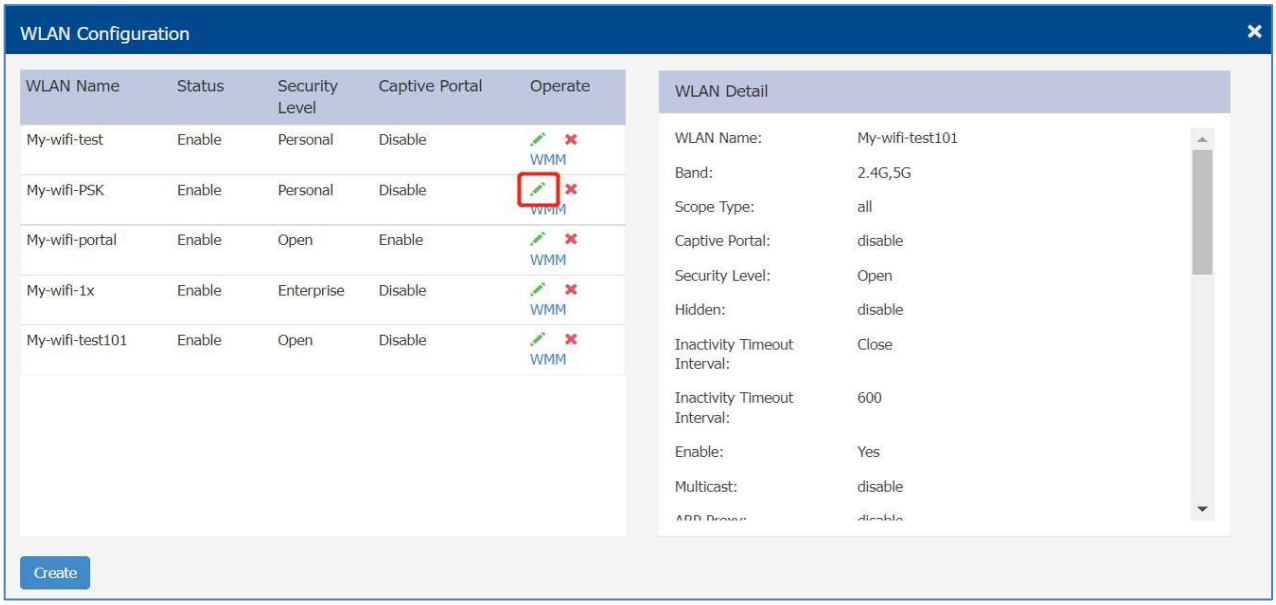


图 66：修改 WLAN 配置

- ☐ 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。

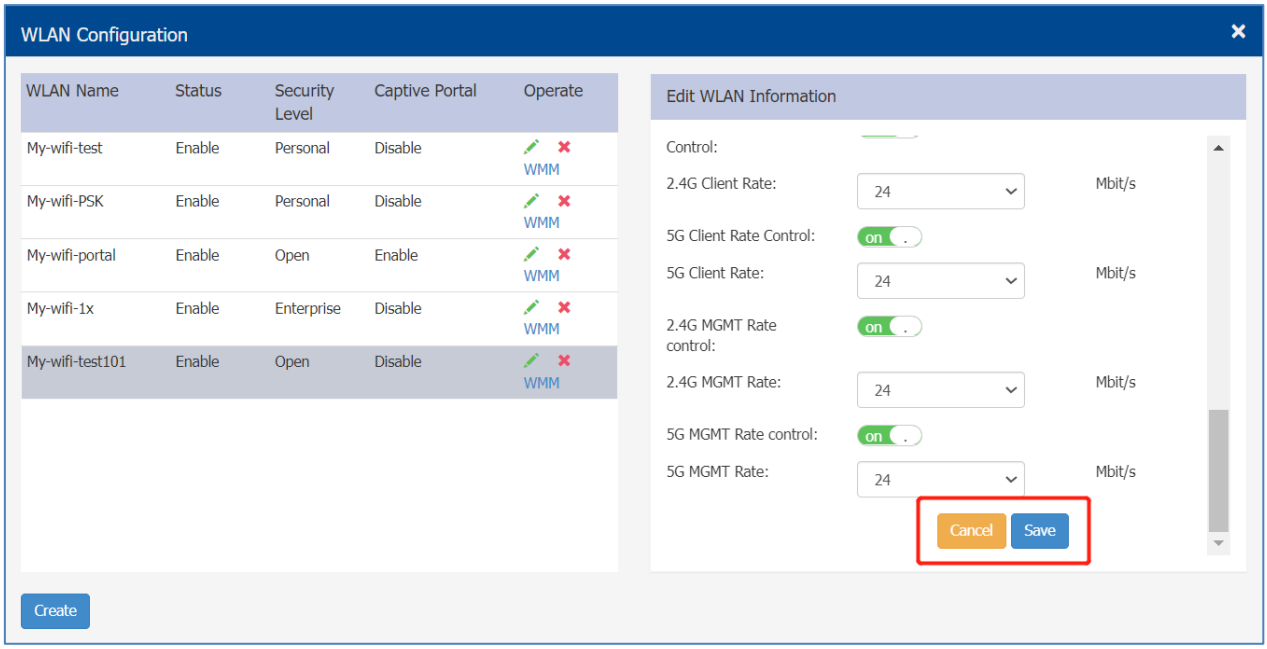


图 67：保存或取消 WLAN 的配置修改

6.5 删除 WLAN

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

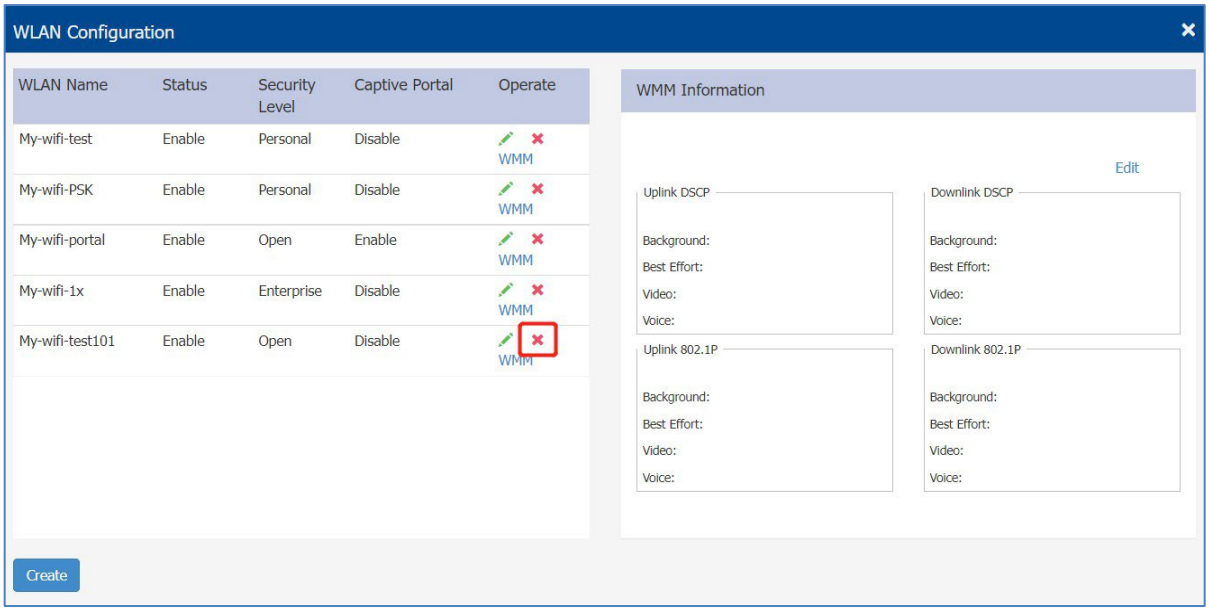


图 68：删除 WLAN

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。
- **尽力而为类别（Best Effort）**：用于传输所有其他数据，如文件传输、网络游戏等，优先级较低。
- **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，WMM 与 DSCP 和 802.1P 优先级的默认映射关系如图 69 所示。

默认映射			
WMM	TID	DSCP	802.1P
BK	1,2	8 ~ 23	1,2
BE	0,3	0~7, 24~31	0,3
VI	4,5	32 ~ 47	4,5
VO	6,7	48 ~ 63	6,7

图 69：WMM 默认映射

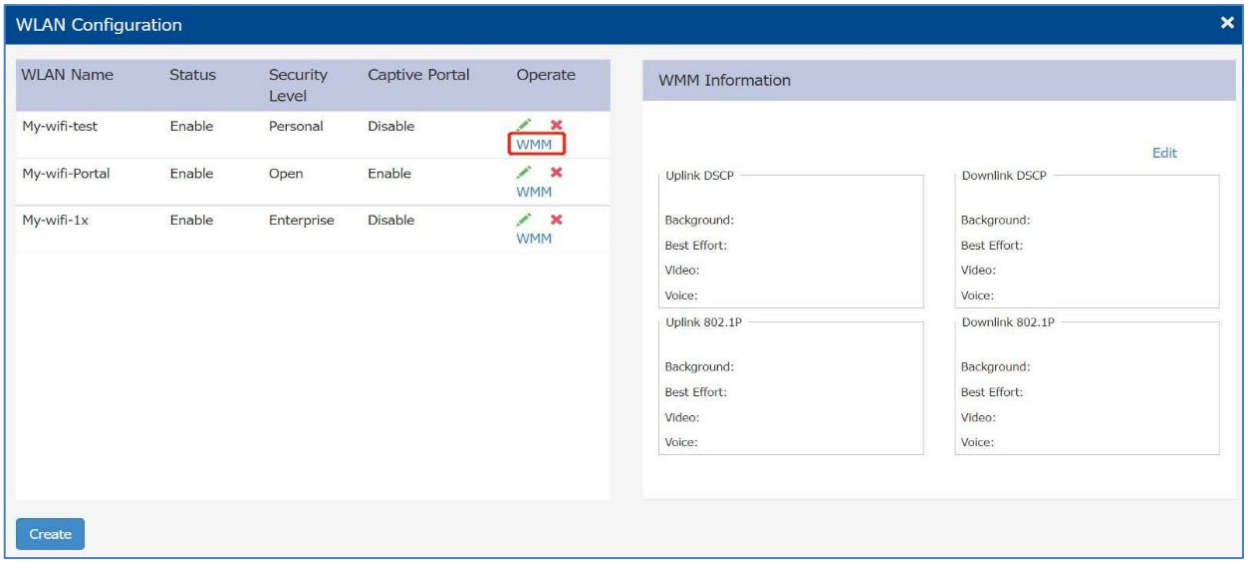


图 70：WMM 配置

每个 WLAN 都可以配置 WMM 的规则，对于 DAP849 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。没有配置的优先级根据默认映射关系进行映射。当 DSCP 与 802.1P 映射为不同的 WMM 优先级时，以 WMM 优先级高的为准。

7 管理 DAP849

本章主要介绍如何在集群中配置和管理 DAP849，以及如何通过 Web GUI 检查、备份、恢复 DAP849 的配置以及升级固件等。DAP849 集群解决方案是一种基于无控制器的体系结构。

DAP849 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 DAP849 系统管理主要包括以下内容：

- 查看 DAP849 的详细信息
- 修改 DAP849 的名称和位置信息
- 添加 DAP849 到集群
- 删除集群中
- 允许 DAP849 加入集群
- 替换
- 修改 DAP849 的 IP 地址
- 将 DAP849 切换为 DAC/BWO 模式
- 查看 DAP849 的当前配置
- 重启 DAP849
- 恢复出厂配置
- DAP849 的配置备份和恢复
- DAP849 WIFI 固件升级
- DAP849 的 LED 指示灯配置
- DAP849 高级配置
- 配置 DAP849 的网络服务

7.1 查看 DAP849 详细信息

通过点击列表中的指定的 DAP849 设备，在右侧的 **Detailed Information** 页面中，您可以查看 DAP849 的详细信息。您可以在该页面中点击“**Edit**”来修改“**AP Name**”和“**Location**”。

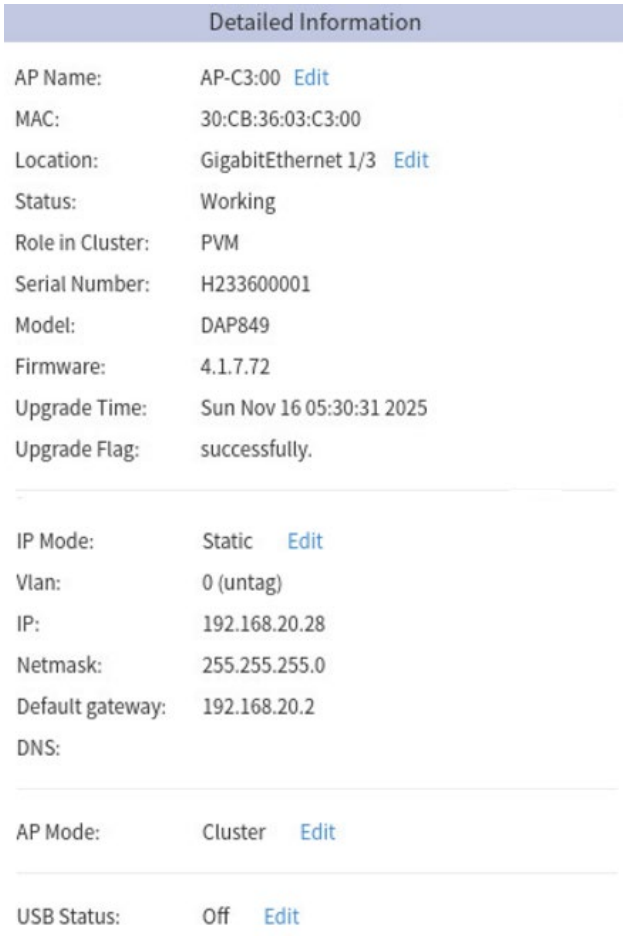


图 71：DAP849 的详细信息

7.2 修改 DAP849 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 DAP849。缺省状态下，DAP849 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。

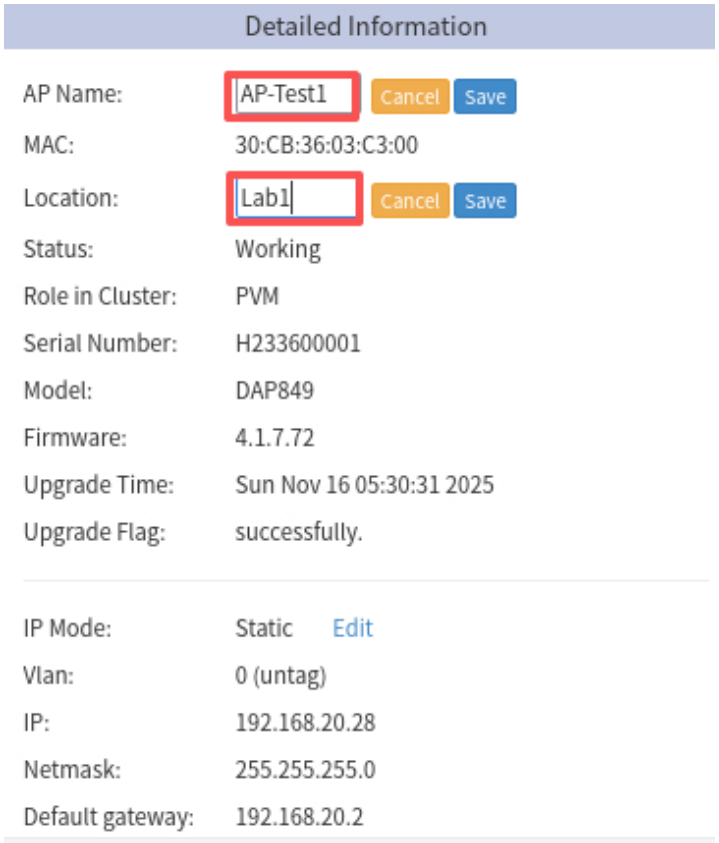


图 72：修改 DAP849 的 Name 和 Location 信息

7.3 添加 DAP849 到集群

■ 操作前的准备工作

在将新 DAP849 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 DAP849 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 DAP849 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 DAP849 并在 System 页面中检查“**Cluster ID**”（集群 ID）。

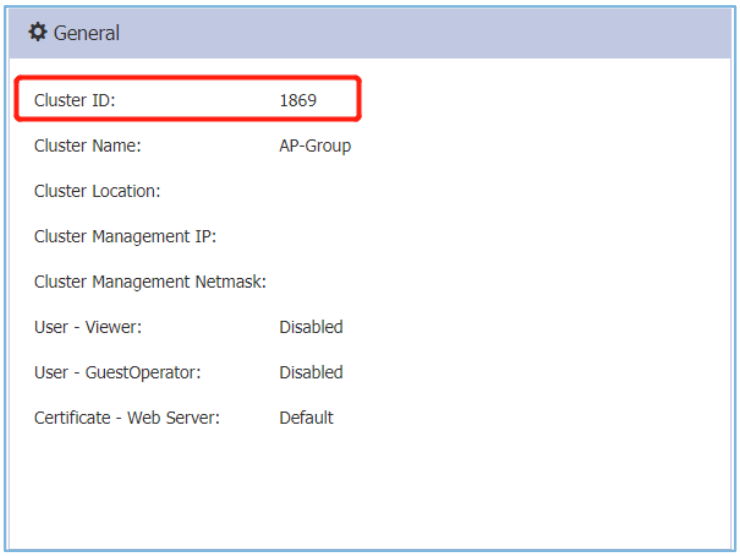


图 73：通过 Web 页面查看集群 ID

- ► 通过 CLI 来查看 Cluster ID。

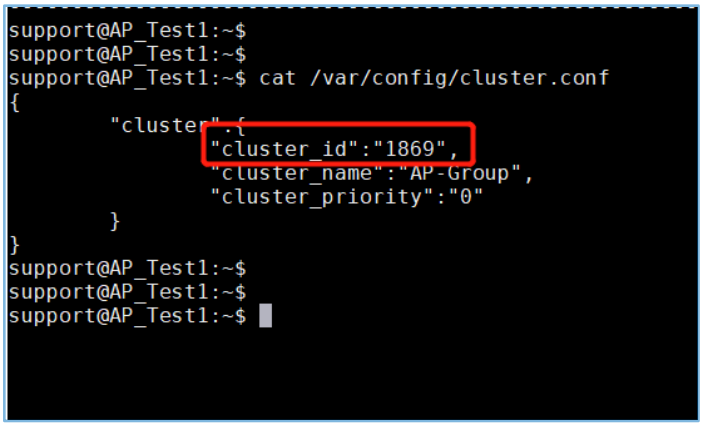


图 74：在 CLI 下查看集群 ID

7.4 删除集群中 DAP849

在集群中删除一个 DAP849：

- ☐ 从 AP 集群列表中选择要删除的 DAP849（可以是 PVM、SVM 或 MEMBER）。
- ☐ 单击“**Kick Off**”按钮，则选中的 DAP849 将被加入到集群的 Block 列表中。

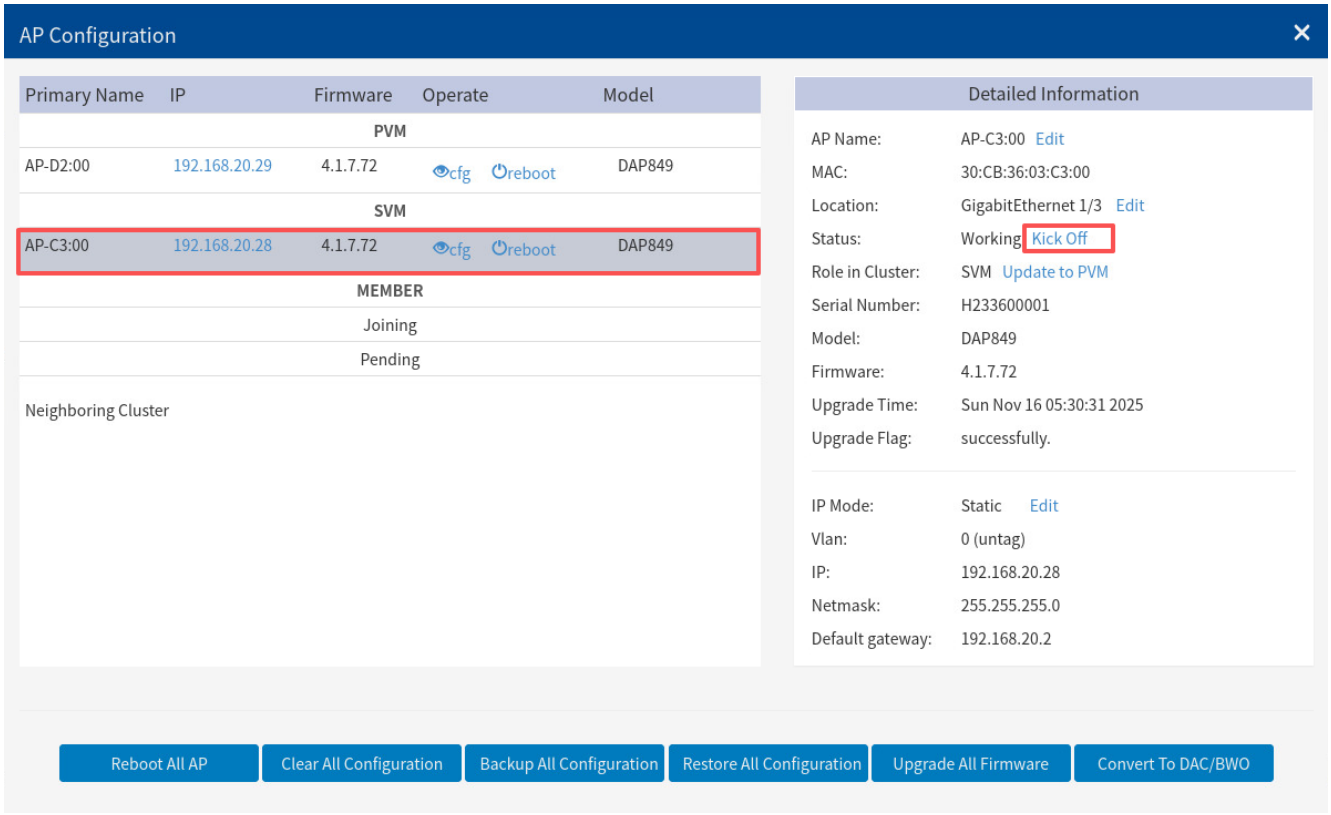


图 75：在集群中删除 DAP849

如果该 DAP849 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 DAP849 设备不允许再次加入此集群成为集群的成员。

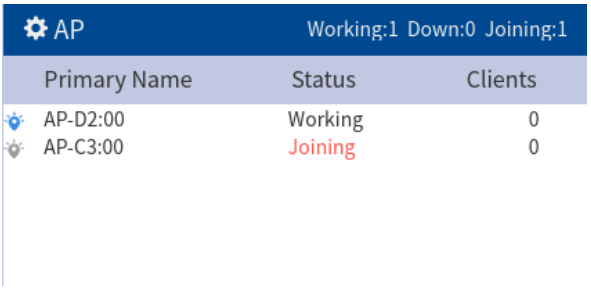


图 76：DAP849 在被删除后进入 “Joining” 状态

7.5 允许 DAP849 加入集群

如果处于**“Joining”**状态的 DAP849 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 DAP849 重新加入集群并且从集群的 Block 列表中删除。

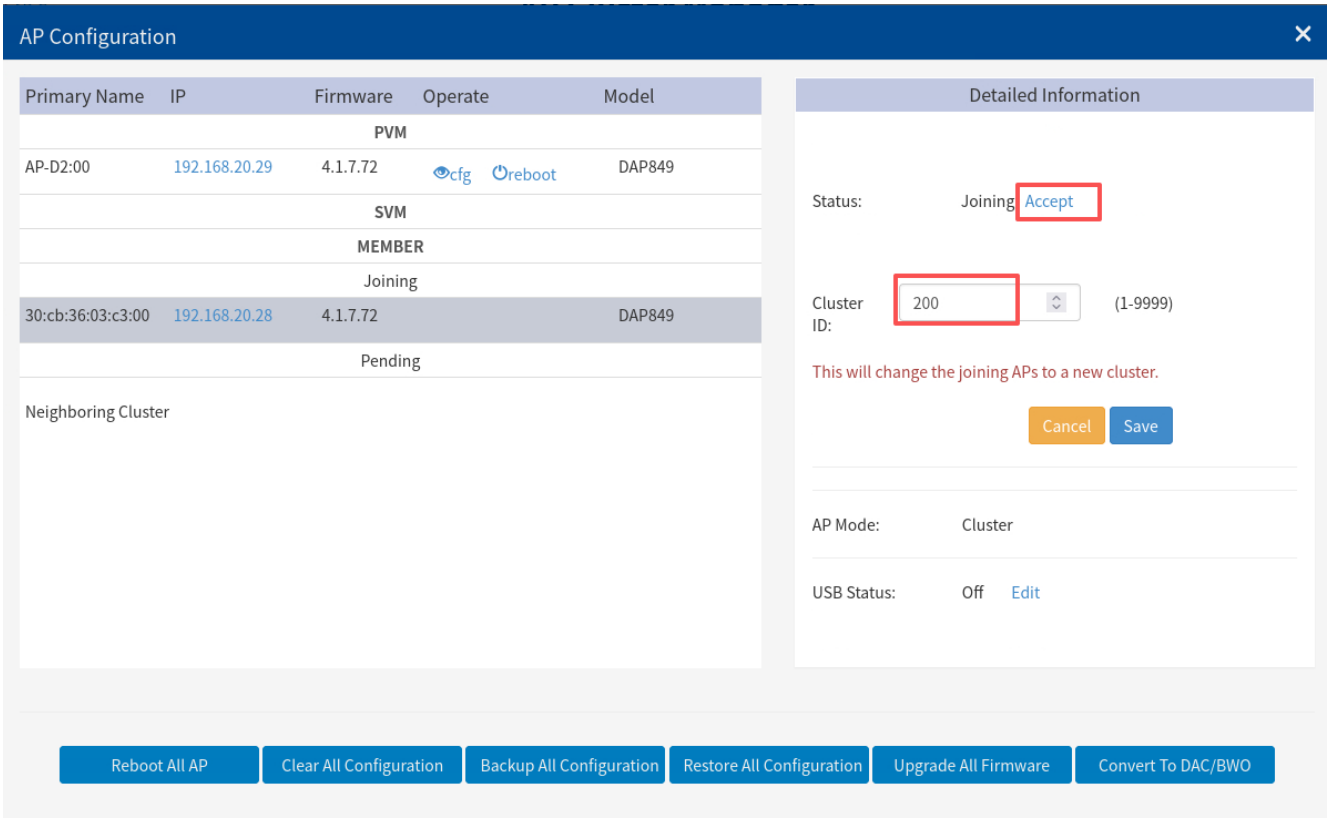


图 77：允许 DAP849 重新加入到集群

7.6 替换 DAP849

替换集群中的 DAP849，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 DAP849 完成替换。

7.7 修改 DAP849 的 IP 地址

DAP849 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 78、图 79 所示。

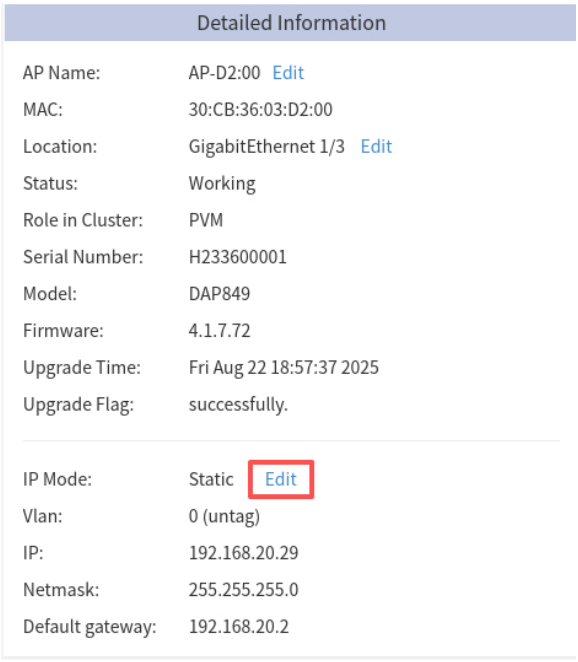


图 78：修改 DAP849 的 IP 模式

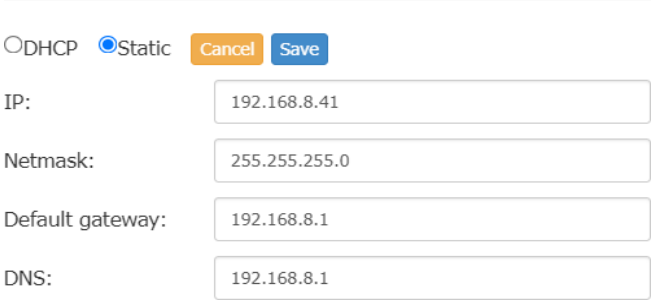


图 79：修改 DAP849 的 IP 地址

7.8 切换 DAP849 为 DAC 或 BWO 模式

根据实际使用场景的需要，DAP849 可以在 Web GUI 上从集群模式切换为 DAC 或 BWO 的工作模式。

■ **切换集群中的单台 DAP849 到 DAC 或 BWO 模式**

☐ 在“**AP Configuration**”页面，选择一台将要切换为 DAC 或 BWO 模式的 DAP849，在右侧的“**Detailed information**”页面上点击 AP Mode 后的**“Edit”**按钮。

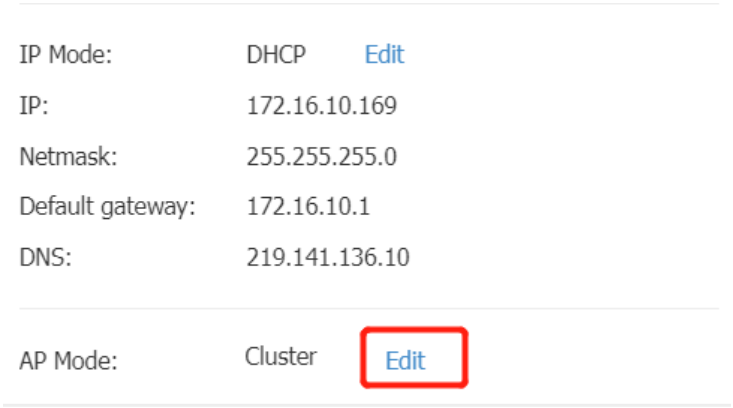


图 80：修改 AP Mode

☐ 选择“**DAC/BWO**”选项。

图 81：配置 DAC 或 BWO 模式

☐ 输入 DAC 或 BWO 的 IP 地址，并保存配置。

在 DAP849 重启后，将会切换为 DAC 或 BWO 模式并按照指定的 IP 地址完成注册。

■ 切换集群中的所有 DAP849 到 DAC 或 BWO 模式

☐ 单击 AP Configuration 页面右下角的“**Convert To DAC/BWO**”。

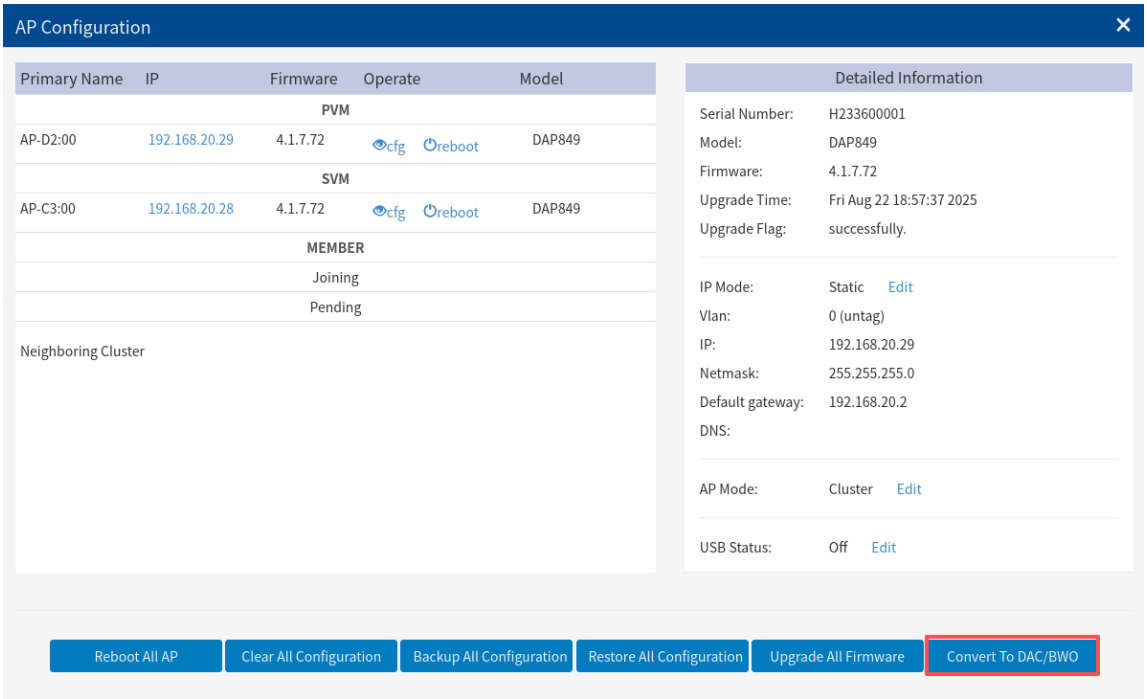


图 82：切换为 DAC 或 BWO 模式

☐ 输入 DAC 或 BWO 的 IP 地址，并保存配置。

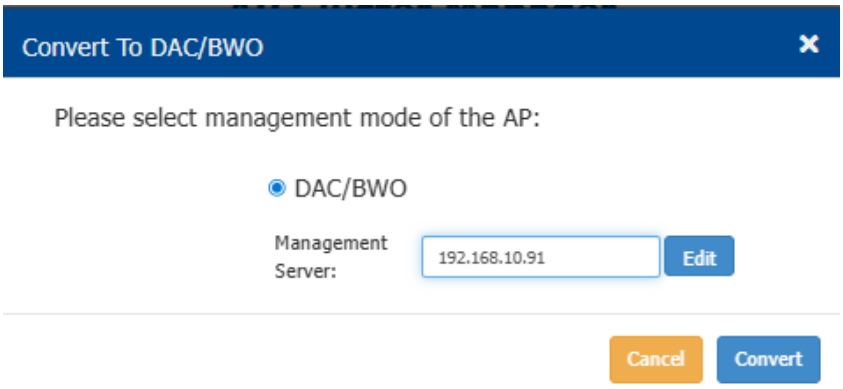


图 83：配置 DAC 或 BWO 模式

在 DAP849 重启后，将会切换为 DAC 或 BWO 模式并按照指定的 IP 地址完成注册。

注意：当 DAP849 切换到 DAC 或 BWO 模式后，在集群模式下的配置将被清除。DAP849 将从 DAC 或 BWO 获取新的配置。

7.9 查看 DAP849 的当前配置

在 DAP849 列表中，点击“ cfg ”图标，在右侧的 Current Configuration 页面中，可以查看 DAP849 当前的详细配置信息，如下图所示。

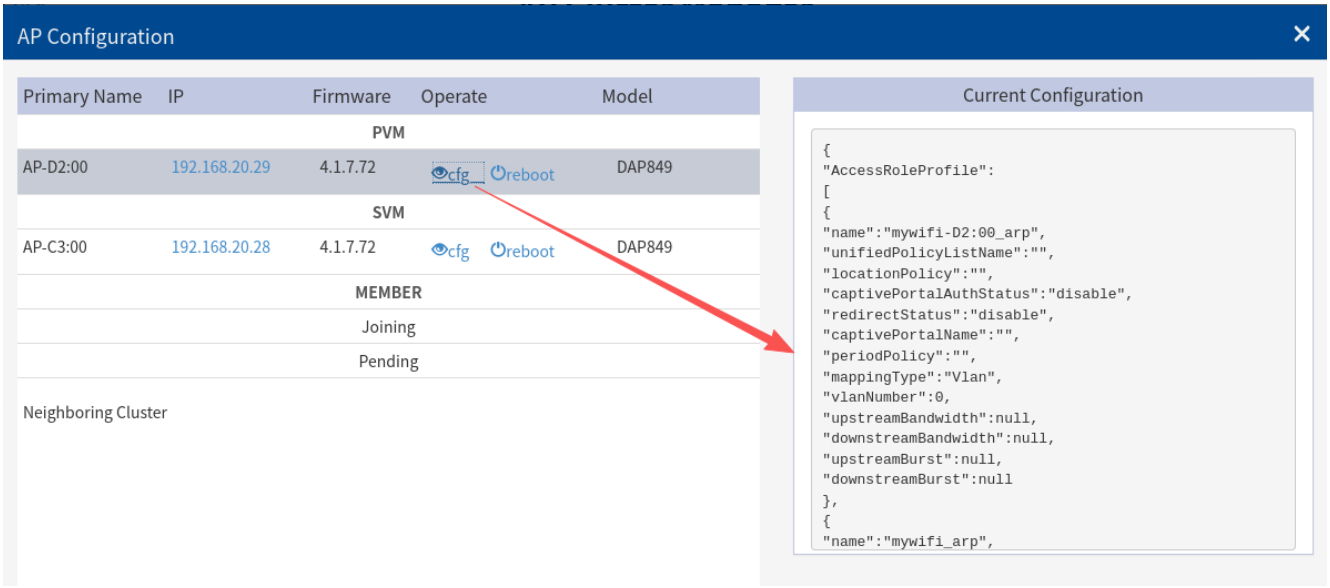


图 84：查看 DAP849 的配置信息

7.10 重启 DAP849

根据需要，您可以对 DAP849 执行重启的操作。

■ 重启集群中的一台 DAP849

☐ 选择一台 DAP849，点击“ reboot ”来完成重启，如下图所示。

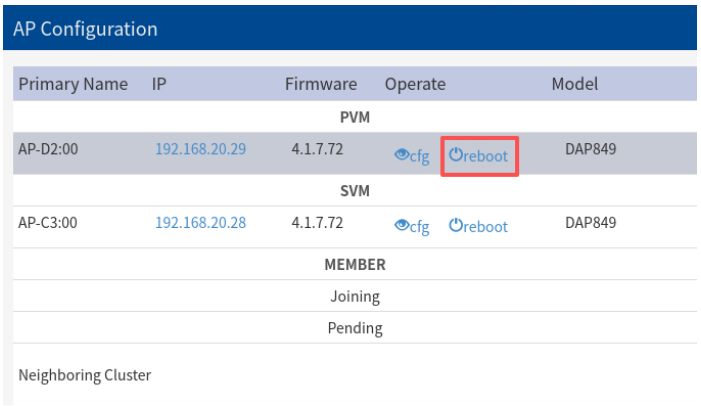


图 85：重启指定的 DAP849 设备

■ 重启集群中所有 DAP849

☐ 点击页面底部的“**Reboot All AP**”按钮可以将所有的 DAP849 执行重启操作，如下图所示。

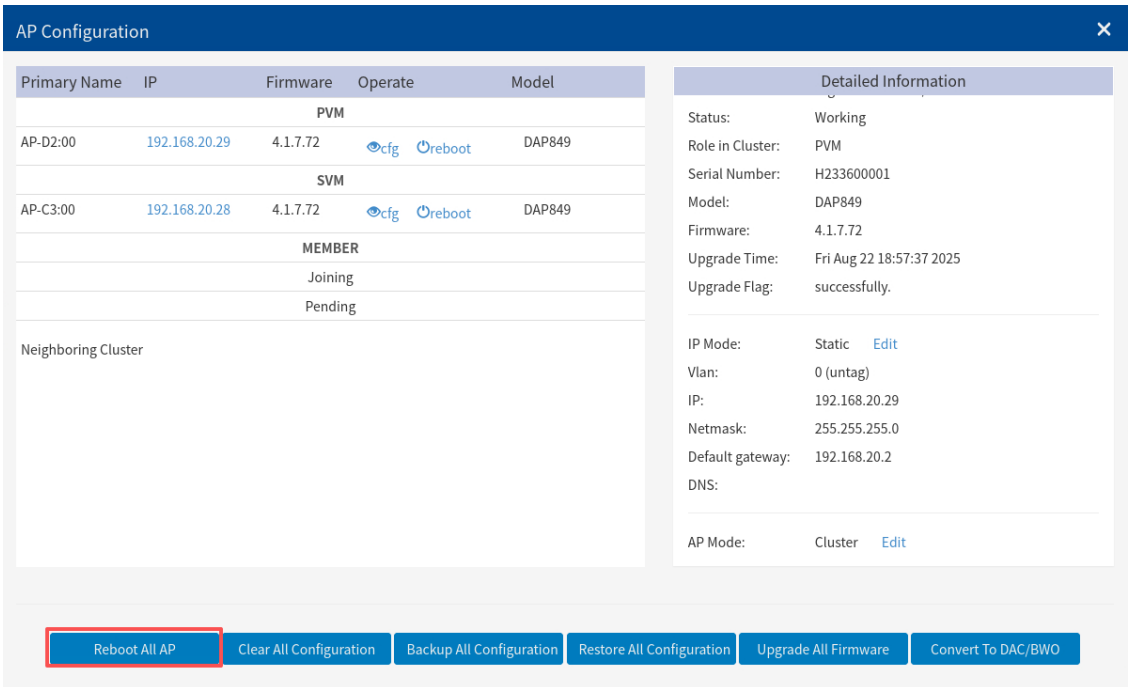


图 86：重启所有的 DAP849 设备

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 DAP849 配置清除并恢复到出厂配置。

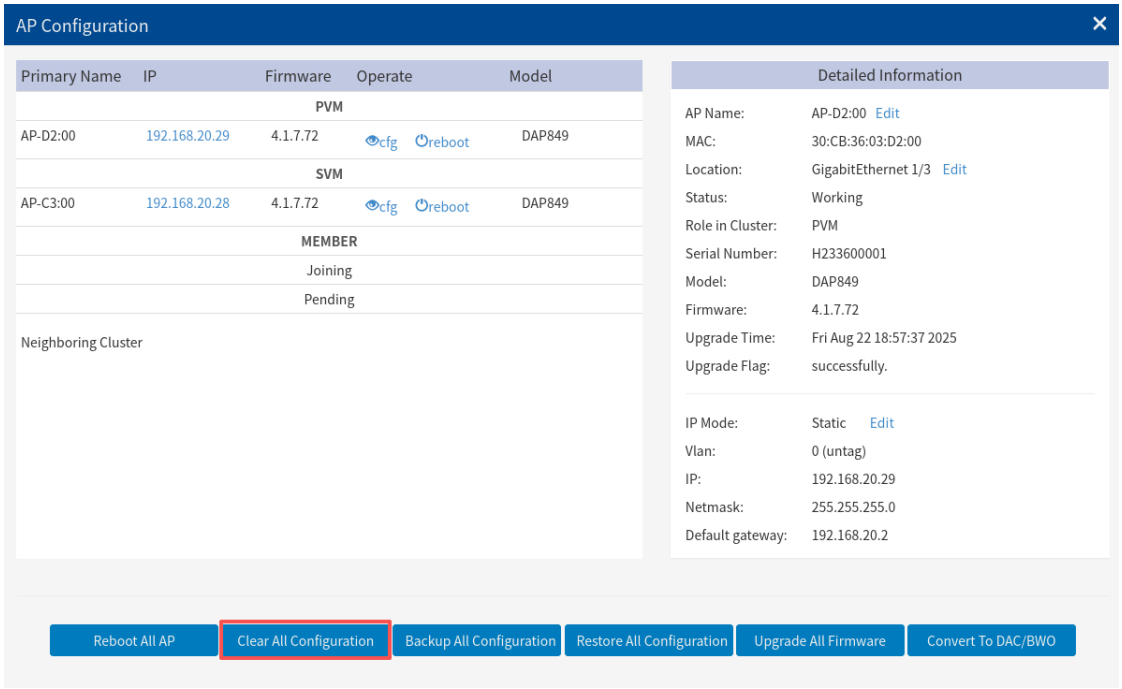


图 87：清除所有配置

注意：另外还有如下方式可以将 DAP849 恢复为“出厂设置”：

- 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 DAP849 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”

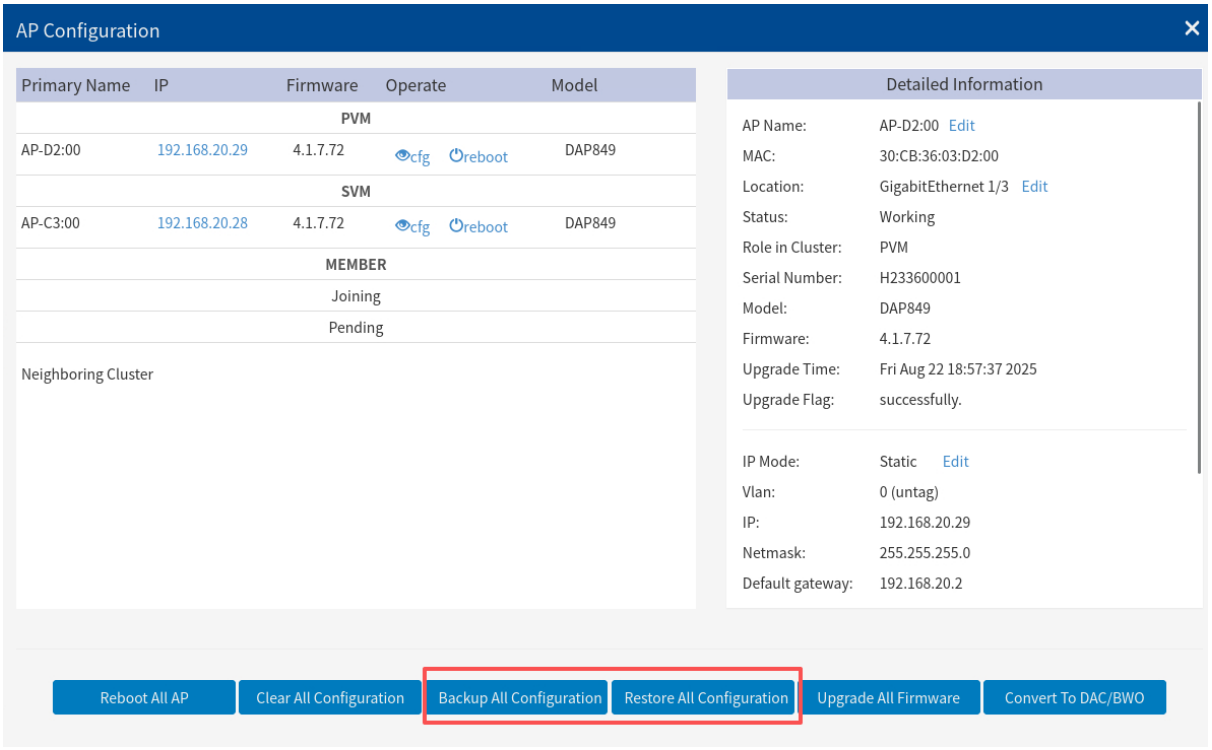


图 88：配置备份和恢复

7.13 DAP849 固件升级

在升级 DAP849 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 DAP849 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 DAP849 的升级页面，如下图所示。

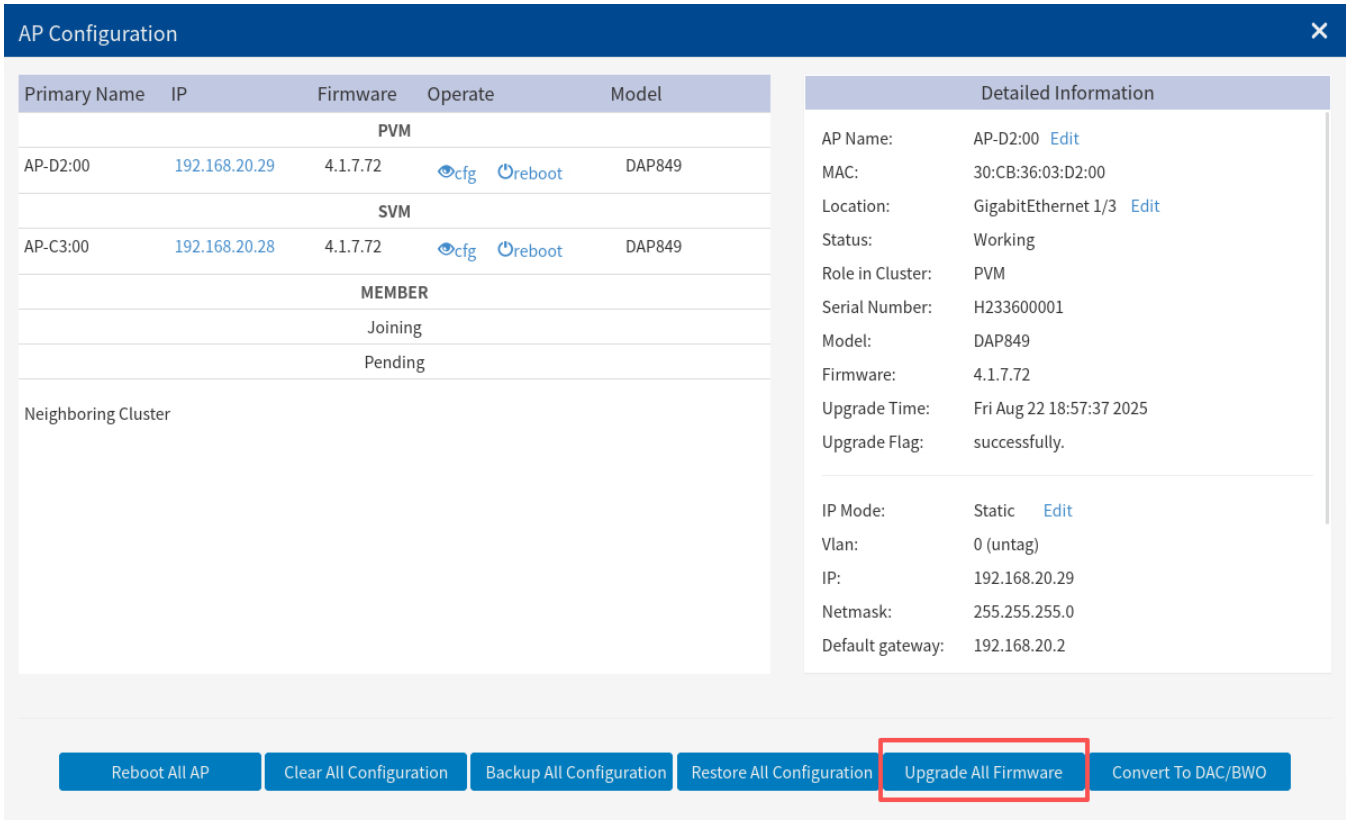


图 89：跳转到 DAP849 升级页面

7.13.1 升级集群中所有 DAP849

如果您需要升级不同型号的 DAP 固件，如 DAP849 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。

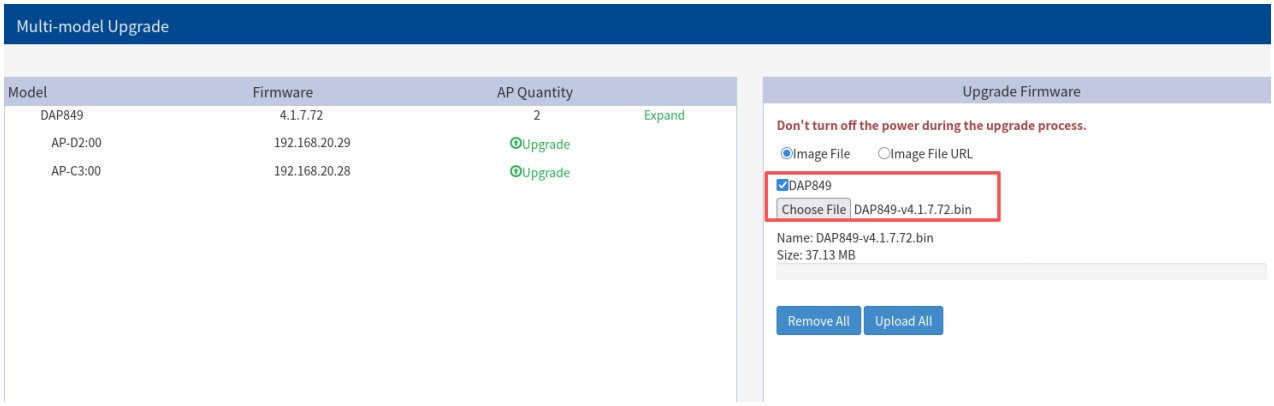


图 90：DAP849 升级页面

DAP849 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，可点单击“**Remove All**”按钮，如下图所示。

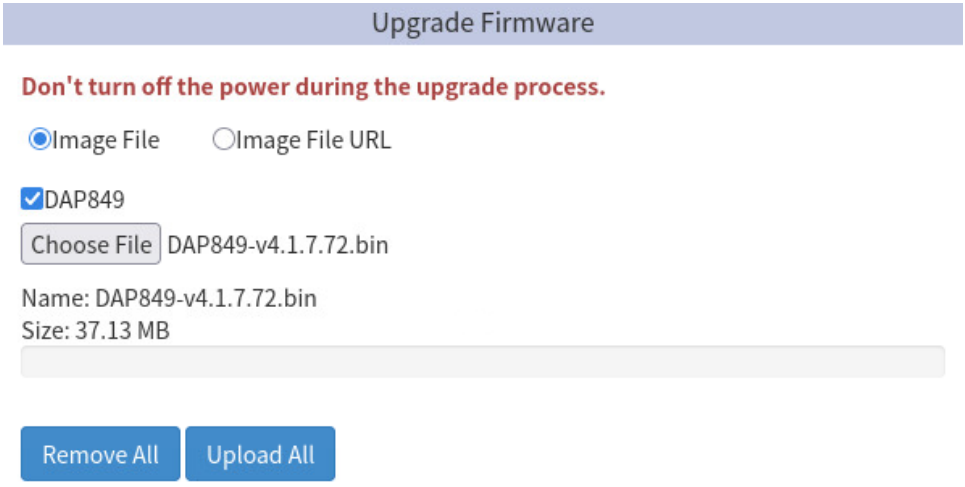


图 91：上传本地升级文件

- **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。

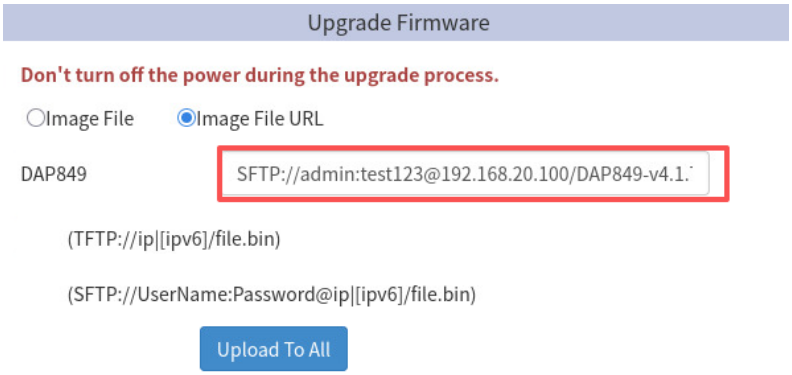


图 92：SFTP 方式上传升级文件

- **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。

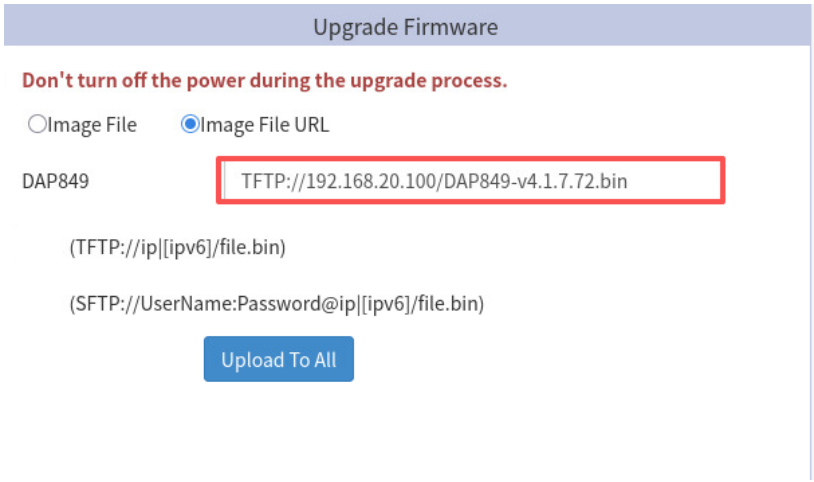


图 93：TFTP 方式上传升级文件

7.13.2 升级集群中单台 DAP849

DAP849 集群同样支持为集群中的单台 DAP849 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 DAP849 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 DAP849。请参阅第 106 页的“系统管理”。

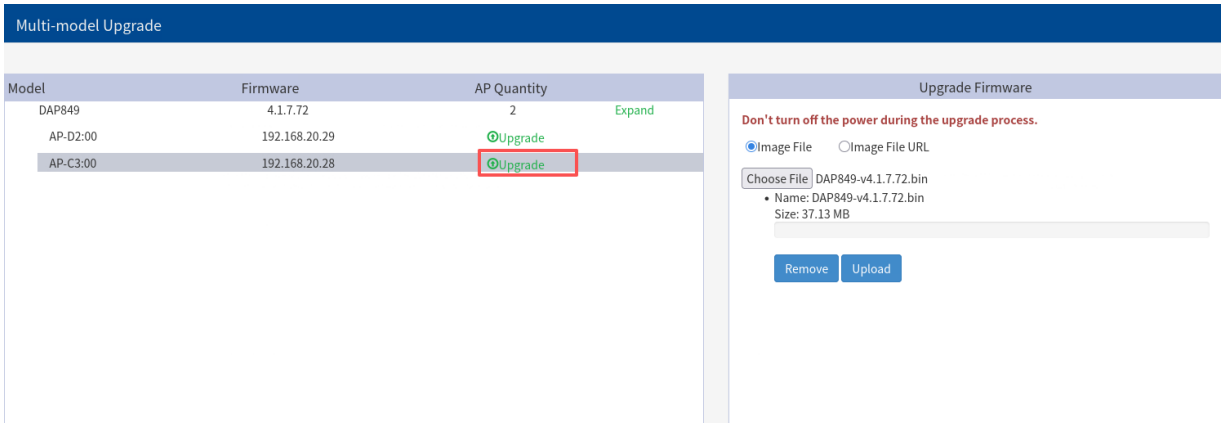


图 94：升级集群中的单台 DAP849

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 DAP849 的 WIFI LED 指示灯配置

- 在 AP 页面中单击“”后可以启动“**LED-Off**”按钮，见图 95。
- 点击“**LED-Off**”可以关闭 DAP849 的 WIFI LED 指示灯。

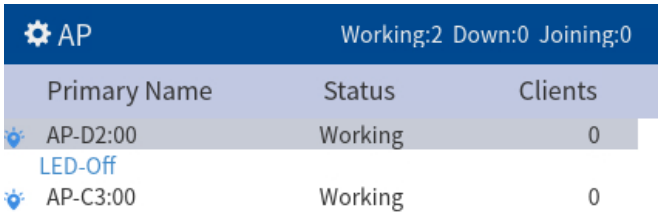


图 95：关闭 LED

- 点击“**LED-On**”按钮恢复开启状态，参考图 96。

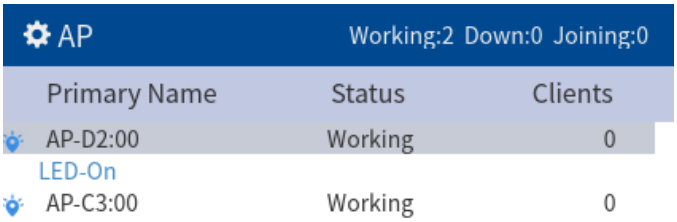


图 96：恢复 LED 为开启状态

7.15 DAP849 高级配置

您可以通过单击 DAP849 列表中的 IP 地址来访问 DAP849 的高级配置页面。参考图 97。

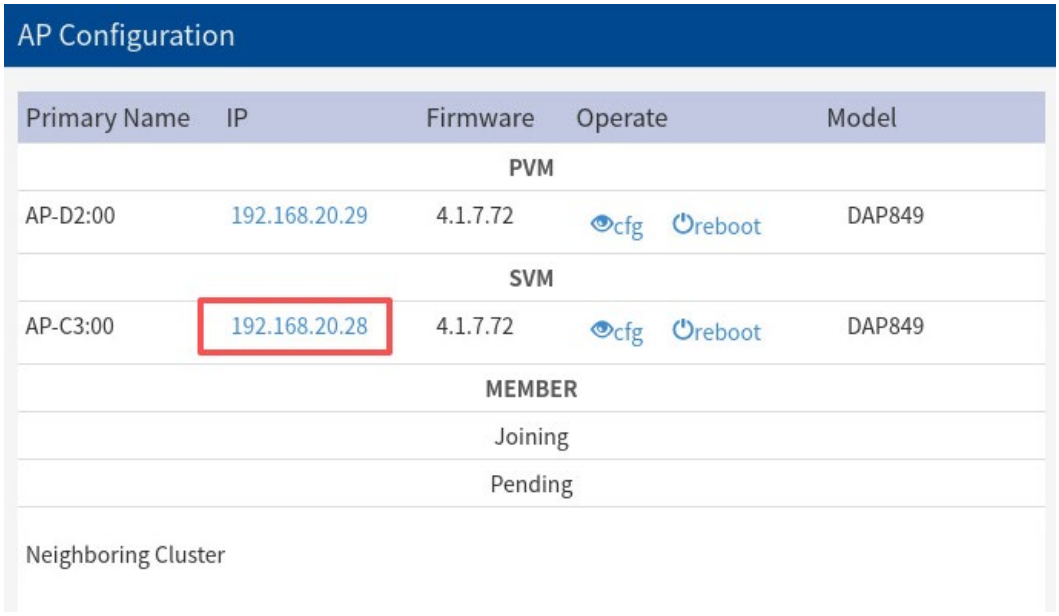


图 97：DAP849 高级配置

7.15.1 DAP849 高级配置页面简介

DAP849 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 DAP849 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 98。在 DAP849 的高级配置页面中，您可以完成如下操作：

- 通过连接到 DAP849 上的客户端来检查 WLAN 状态。
- 在 DAP849 上配置 DHCP/DNS/NAT 服务。
- 为 DAP849 配置无线 Mesh 功能。
- 升级、重置或重启 DAP849。
- 监测和扫描 RF 环境。
- 配置及邻居 DAP 的显示。

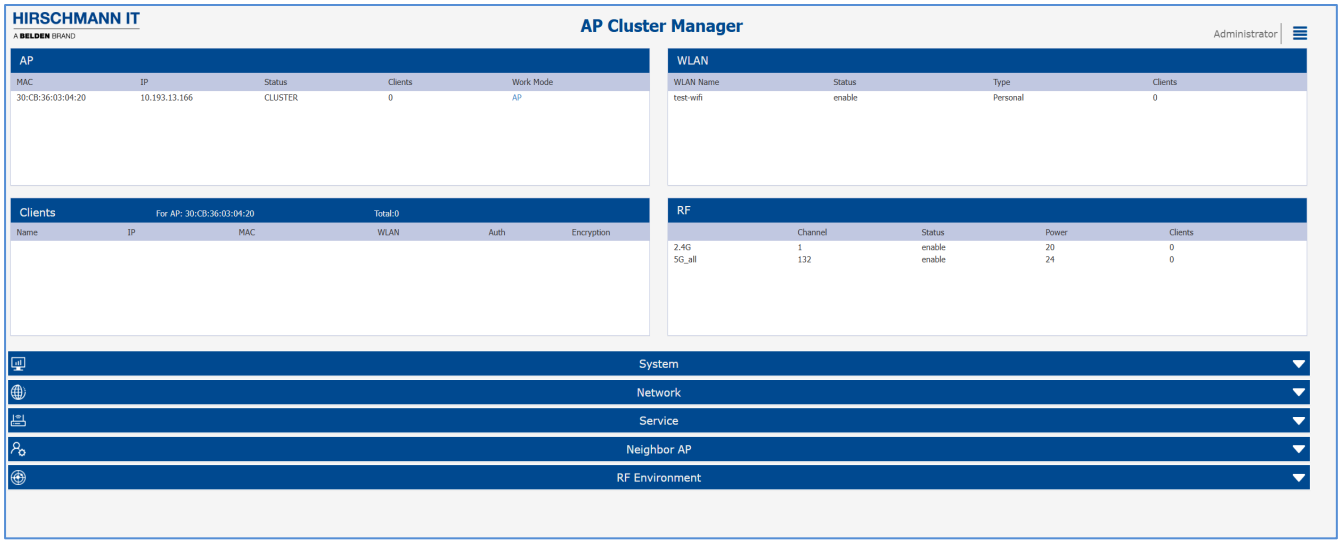


图 98：AP 高级配置页面

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 DAP849 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。

图 99：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。

图 100：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。

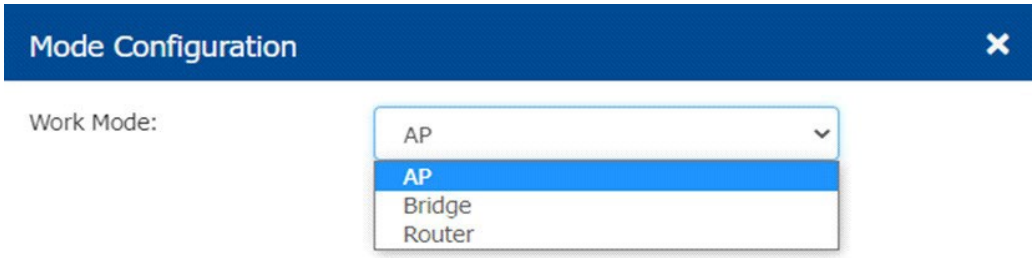


图 101：AP 工作模式配置

- 修改模式后 DAP849 将会重新启动使配置生效。在默认情况下，DAP849 工作于 AP 模式。

根据使用场景的需要，您可以将指定的 DAP849 设备配置在 Bridge 模式或 Router 模式下工作。

配置 DAP849 为 Bridge 模式

DAP849 的 Bridge 模式是一种网络连接模式，它允许 DAP849 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，DAP849 可以与另一个 DAP849 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 DAP849 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。

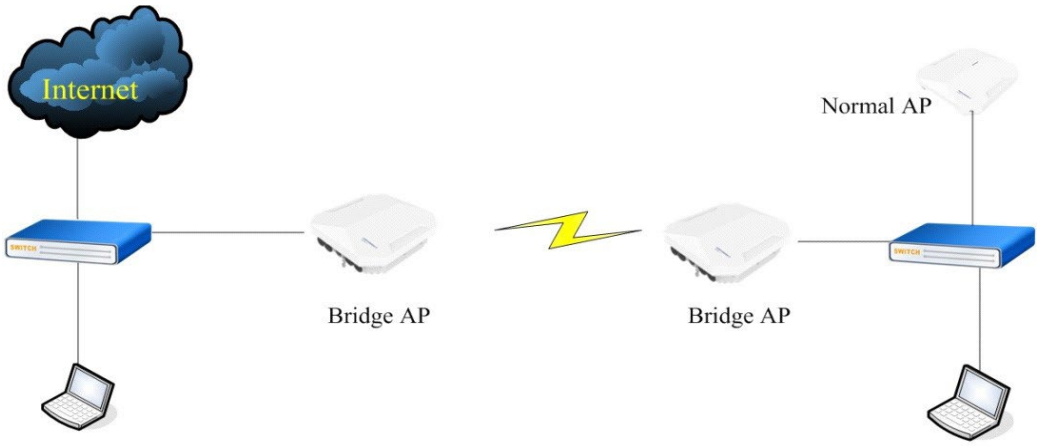


图 102：Bridge 模式拓扑图

在 Bridge 模式下，DAP849 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 103。

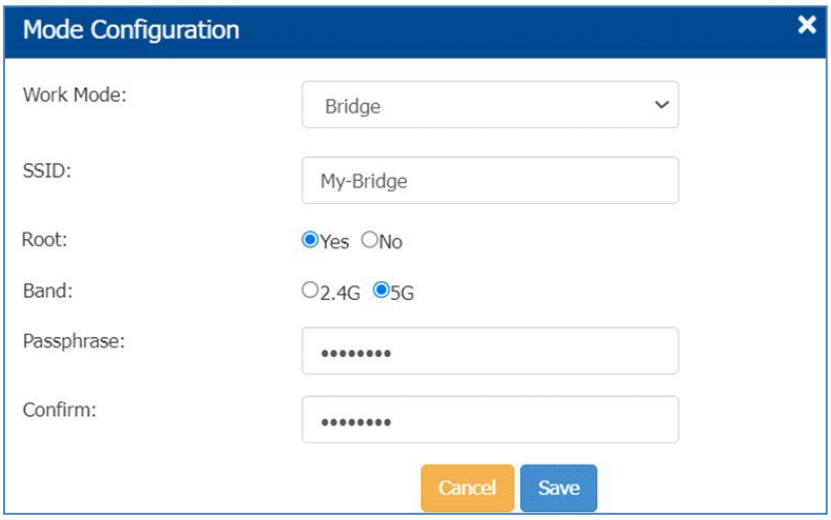


图 103：Bridge 模式配置

关键参数描述如下：

参数	描述
Work Mode	DAP849 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 DAP849 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 DAP849 工作在 Router 模式

在 Router 模式下，DAP849 将成为一个 DHCP 服务器为无线客户端分配 IP 地址。DAP849 支持通过 DHCP、静态 IP 或 PPPOE 管理上行链路接口（WAN）的 IP 地址。

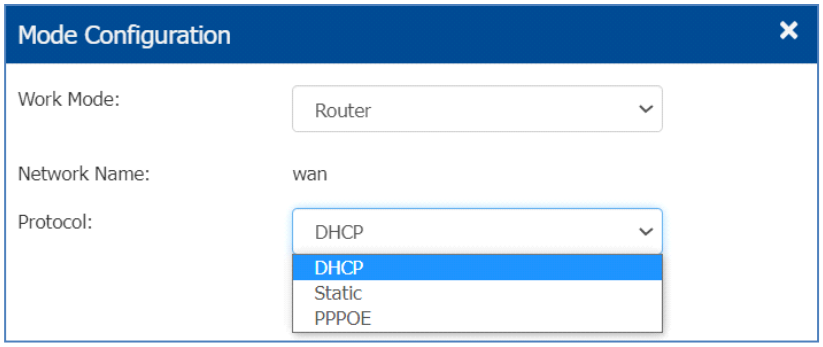


图 104：配置 Router 模式

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。

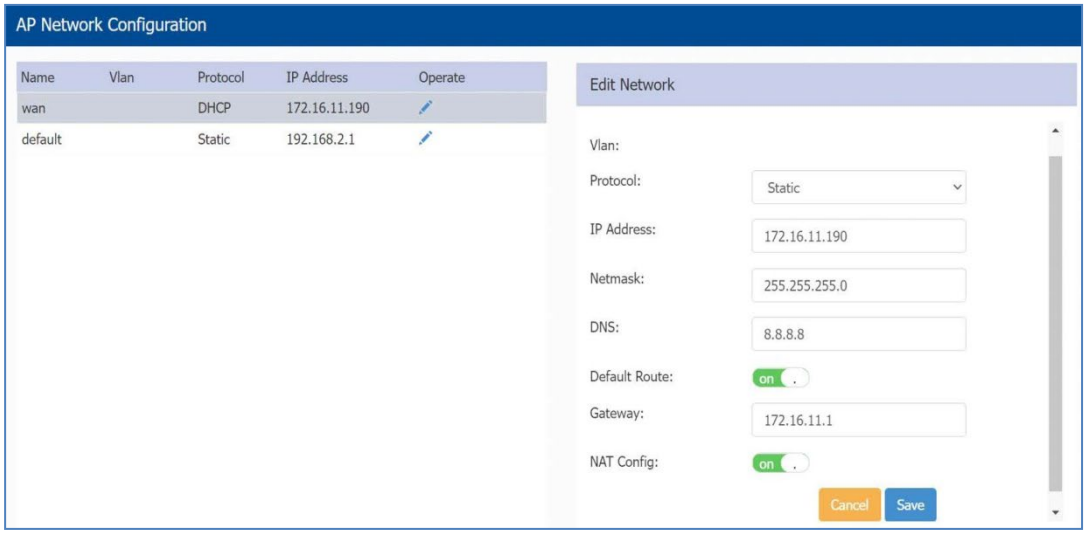
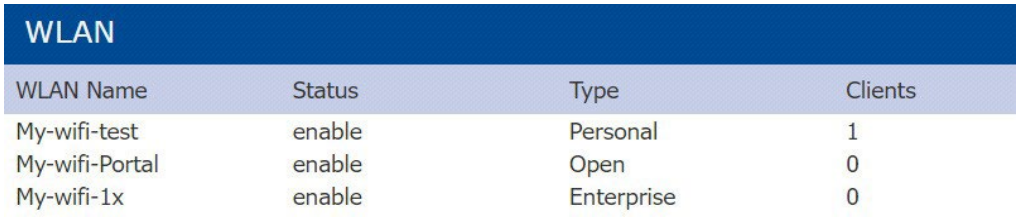


图 105：修改 DAP849 的网络配置

7.15.3 WLAN 信息

WLAN 信息页面显示了当前 DAP849 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。



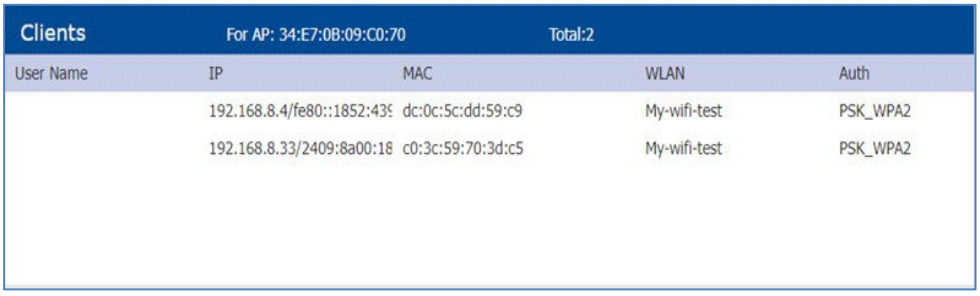
WLAN

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

图 106：WLAN 基本信息

7.15.4 Clients 信息

“**Clients**”页面显示了当前 DAP849 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:E7:0B:09:C0:70 Total:2

User Name	IP	MAC	WLAN	Auth
	192.168.8.4/fe80::1852:43	dc:0c:5c:dd:59:c9	My-wifi-test	PSK_WPA2
	192.168.8.33/2409:8a00:18	c0:3c:59:70:3d:c5	My-wifi-test	PSK_WPA2

图 107：Clients 信息页面

7.15.5 RF 信息

RF 页面显示的是有关当前 DAP849 设备上 RF 的基本信息，通过该页面，您可以了解到当前 DAP849 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。

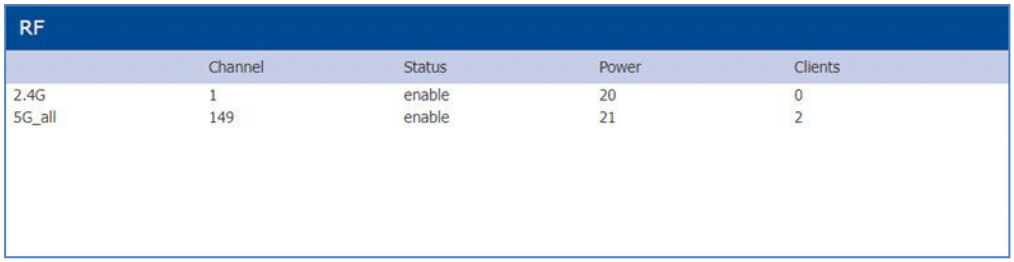


图 108：RF 页面

7.15.6 系统管理

在 System 页面上，您可以查看与当前 DAP849 设备相关的系统日志信息。您也可以在该页面中对 DAP849 进行升级。请参考图 109。

详细信息请参阅第 131 页的“配置 Syslog 系统日志”和第 95 页的“升级集群中所有”。

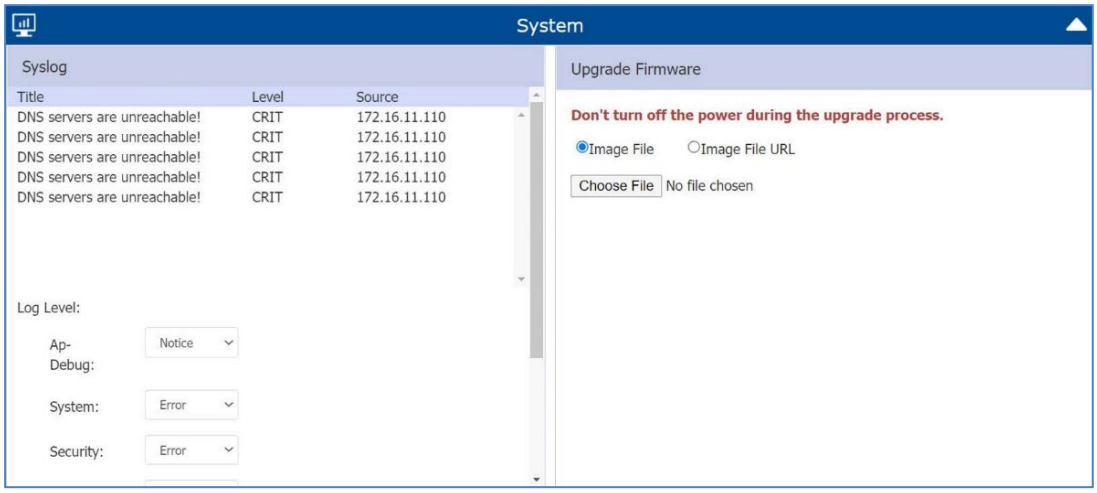


图 109：AP UI 中的系统管理

7.15.7 DAP849 接口配置

在 DAP849 的接口配置中，您可以查看到 DAP849 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 DAP849。

如需完成 DAP849 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**。

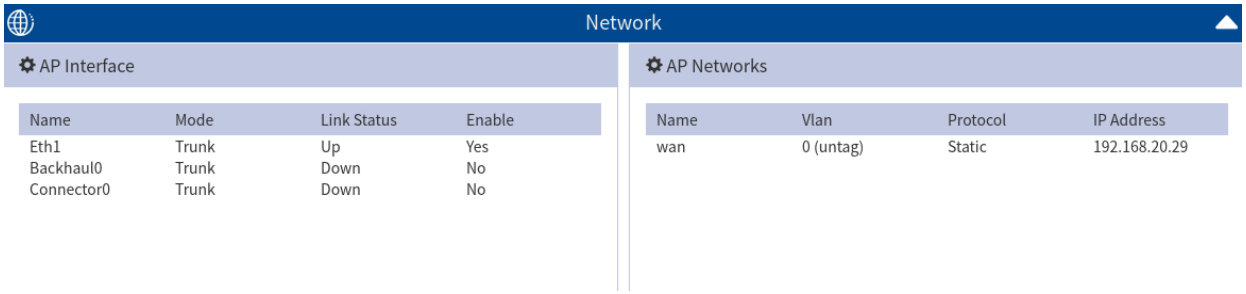


图 110：DAP849 接口状态

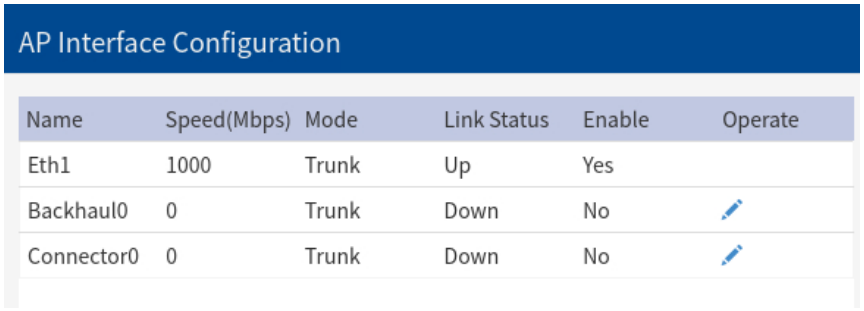


图 111：AP 接口配置

关键参数描述如下：

参数	描述
Eth1	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 DAP849 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 DAP849 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，DAP849 中会相应的创建 VLAN 接口，参考图 53。

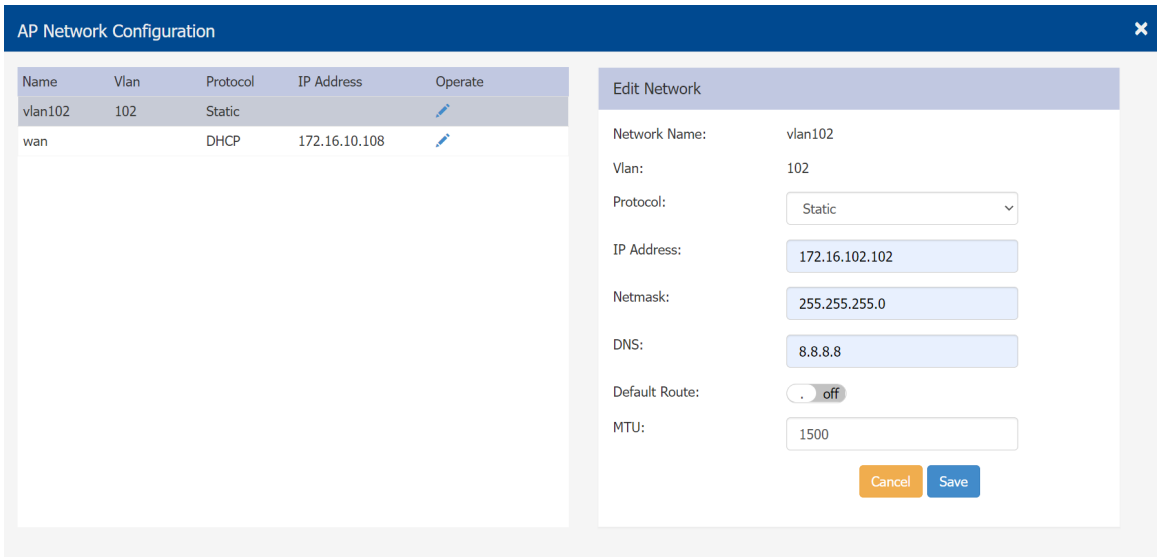


图 112：网络配置

关键参数描述如下：

参数	描述
Name	**网络接口名称，DAP849 上有如下两种网络接口类型：** ▶ 绑定到 WLAN 的 VLAN 接口类型 VLAN networks mapping to WLAN (SSID) ▶ 绑定到 DAP849 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： ▶ **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 DAP849 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： ► **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，DAP849 支持与下行 DAP847-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 DAP849 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 DAP849 的可靠性和冗余性。如果某个 DAP849 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 113。

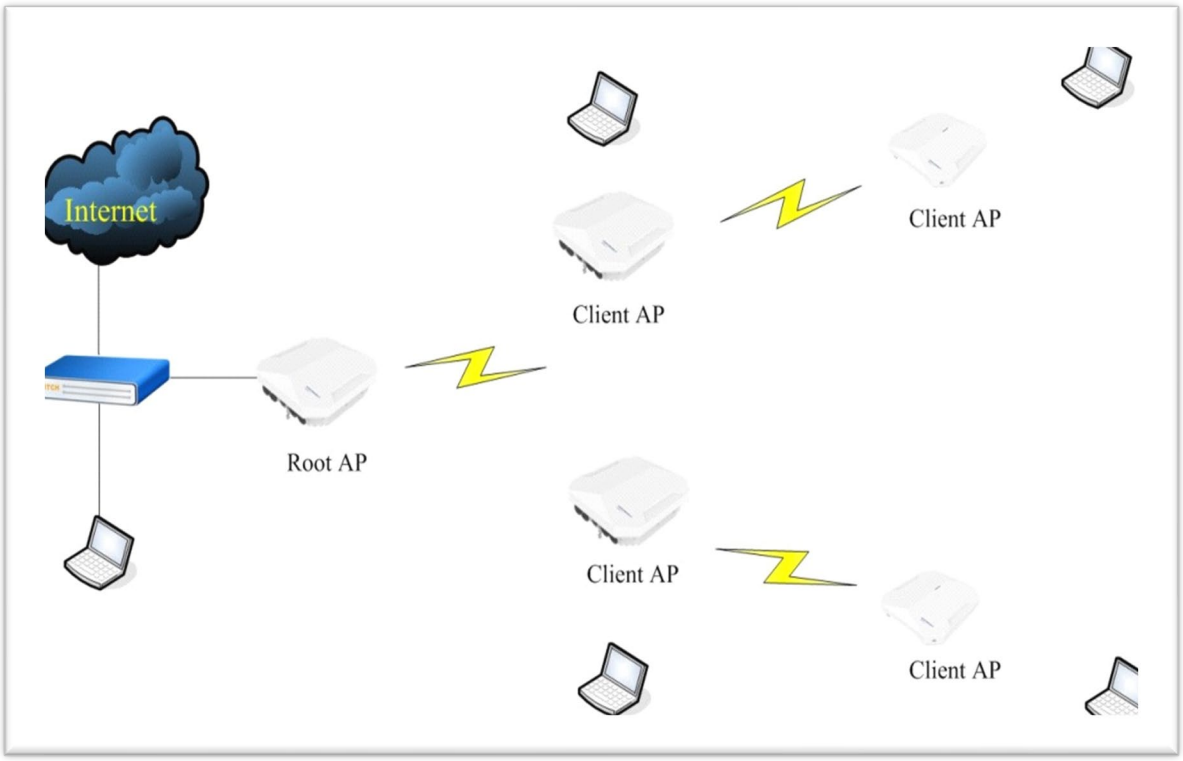


图 113：MESH 拓扑图

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 DAP849 配置为无线回传的 Mesh 模式。在这种情况下，DAP849 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 114。

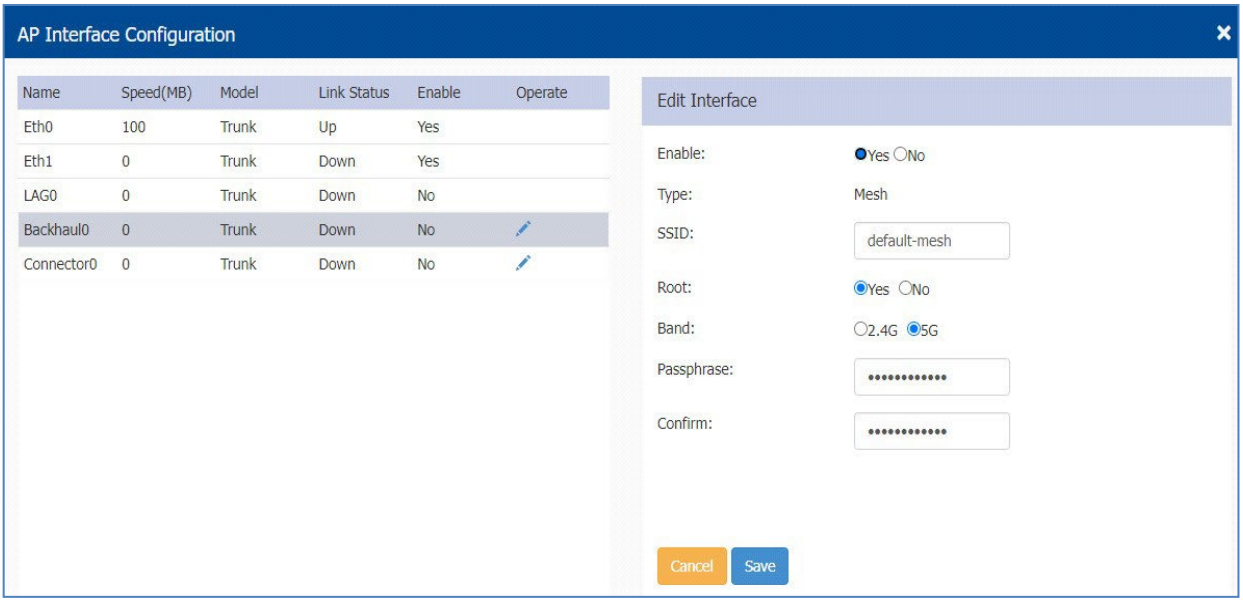


图 114：AP interface configuration 页面

关键参数描述如下：

参数	描述
Enable	选择“Yes”启用或选择“No”禁用 DAP849 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 DAP849 部署位置邻近的其它 DAP849 设备，也是连接到当前 DAP849 的客户端可能漫游的目标设备。

目前 DAP849 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。

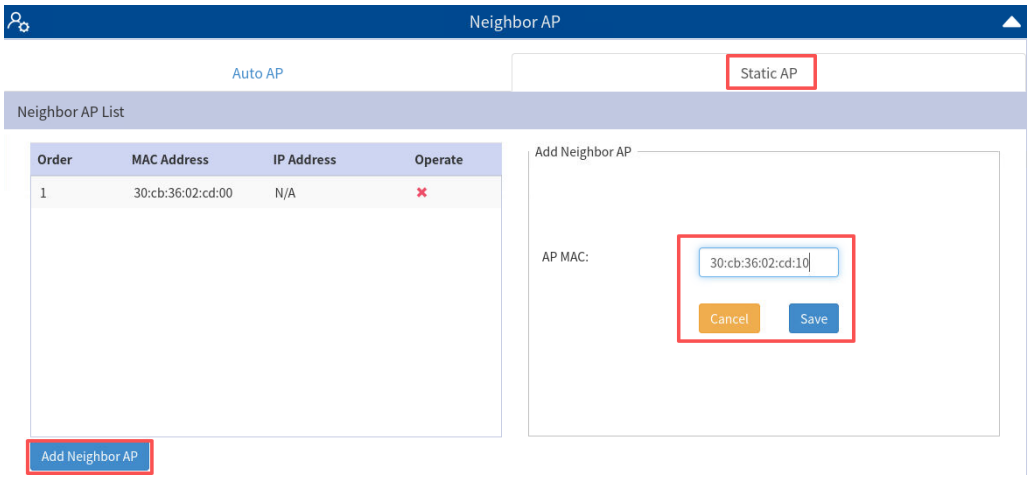


图 115：配置 Static neighbor AP

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 DAP849 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。

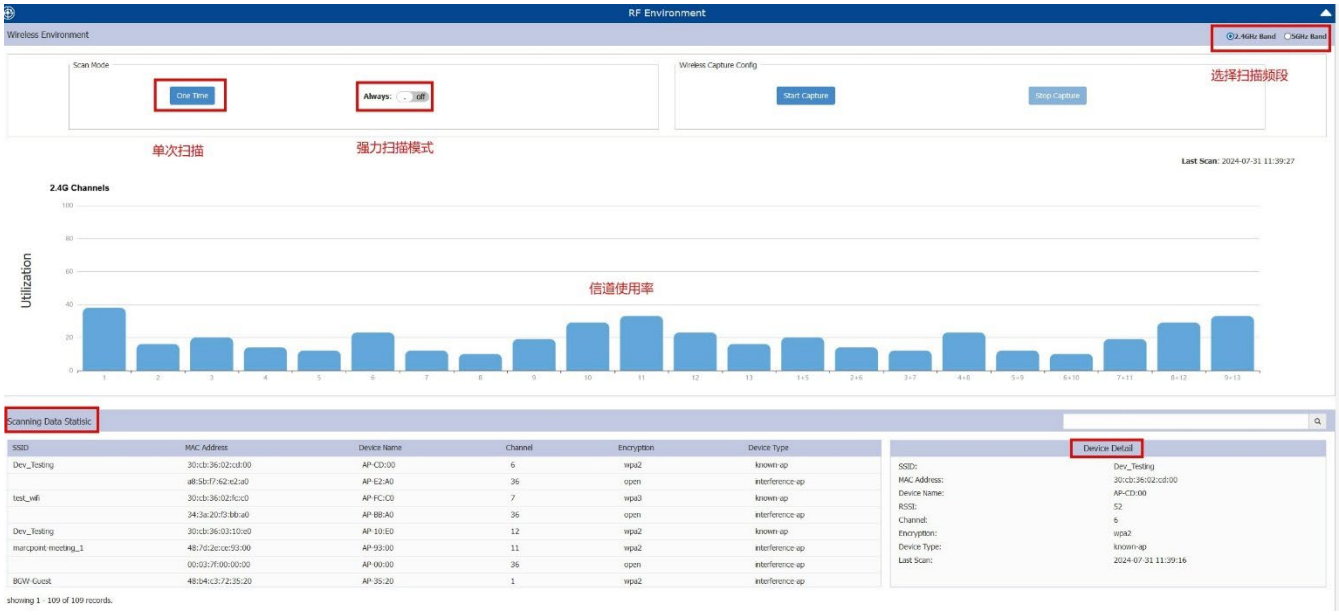
DAP849 可以检测 Wi-Fi 网络的 RF 环境，识别干扰，并对其来源进行分类。这个分析结果可用于快速隔离检测到的数据传输以及信道质量的问题，同时也能够检测出在同一信道中工作的其他设备的抢占引起的流量拥塞问题。

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 116。

DAP849 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 DAP849 的扫描模式数据，请确保该 DAP849 处于“**扫描模式**”。在扫描模式下，DAP849 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，DAP849 将返回到正常的 AP 模式，允许客户端连接。



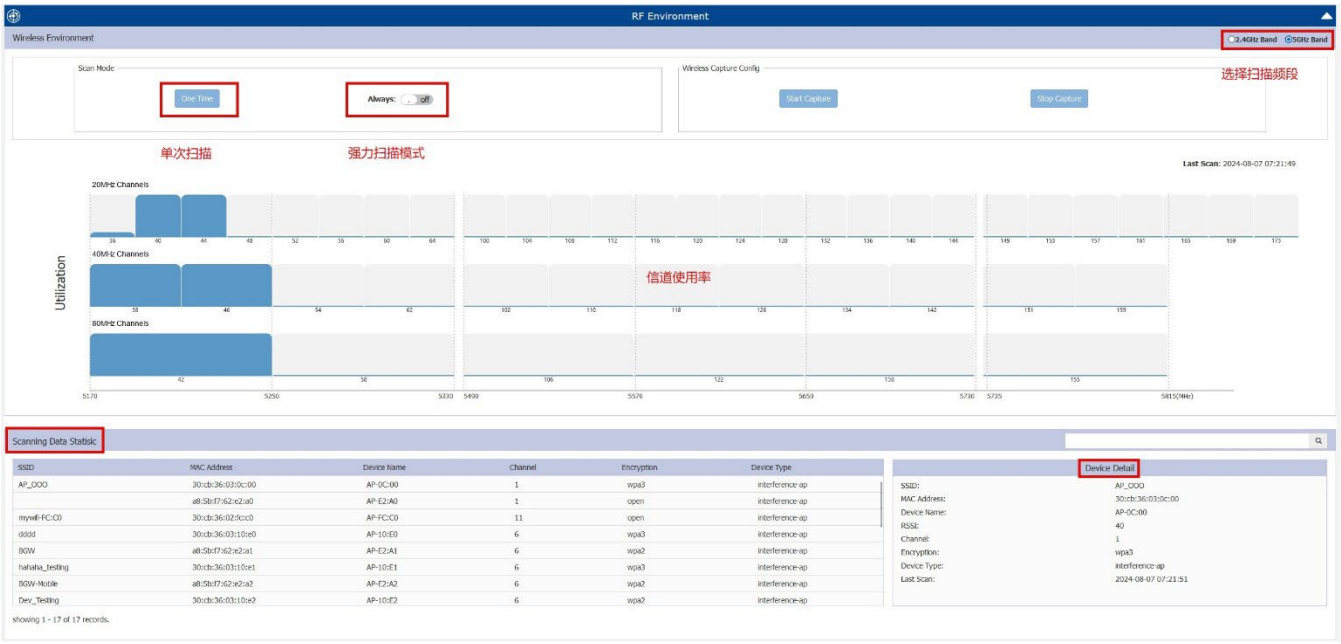


图 116：RF environment 页面

7.15.12 无线抓包功能

DAP849 支持无线抓包模式，在这种模式下，DAP849 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 10 MB 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 DAP849 上完成无线抓包，请参考如下步骤：

☐ 登陆 AP Advanced Configuration 页面→RF Environment→Wireless Capture Config→Start Capture, 参考图 117。

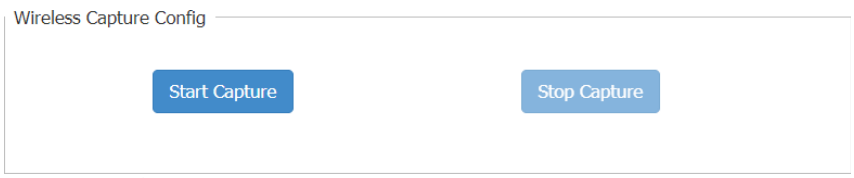


图 117：无线抓包配置

☐ 根据实际需要选择合适的过滤条件。

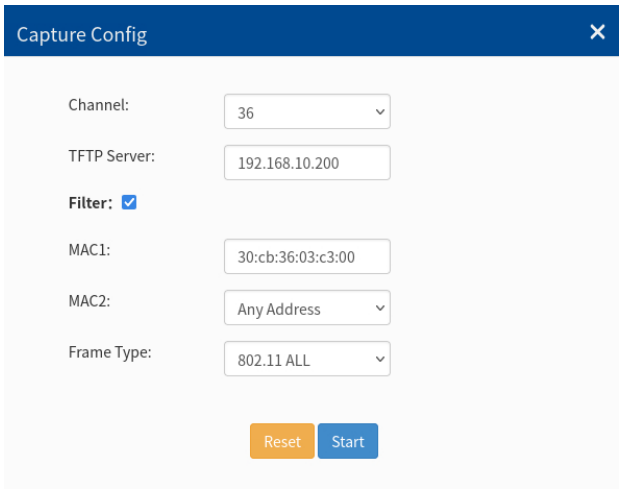


图 118：抓包过滤条件

- 单击“**Start**”按钮开始抓包，DAP849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。

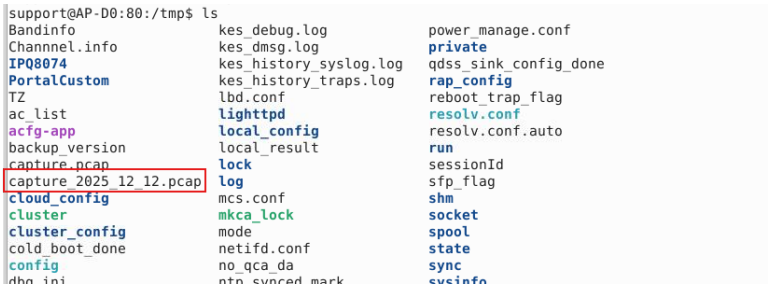


图 119：抓包文件存储示例

7.16 配置 DAP849 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 DAP849 工作在路由模式时，您可以设置 DAP849 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 120。

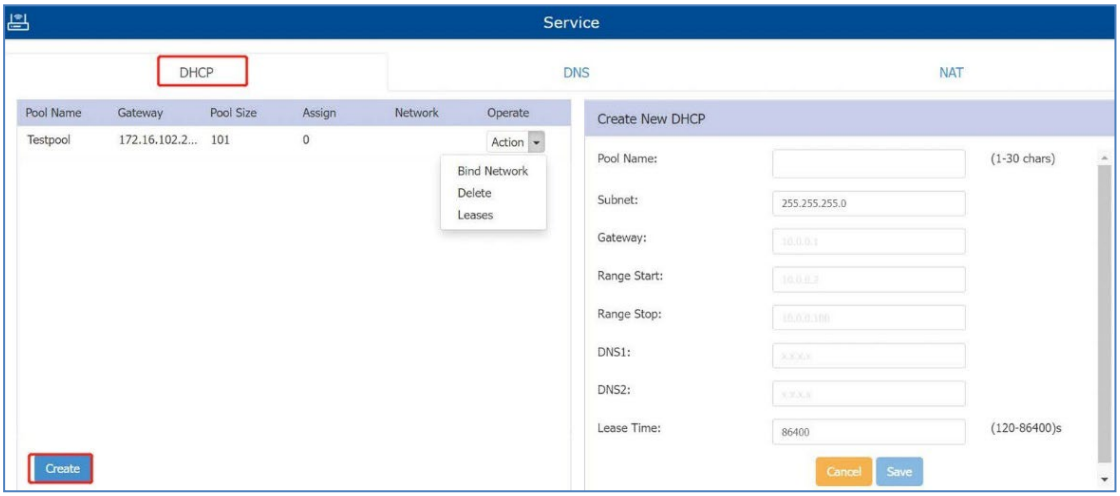


图 120：配置 DHCP 服务

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 121 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：

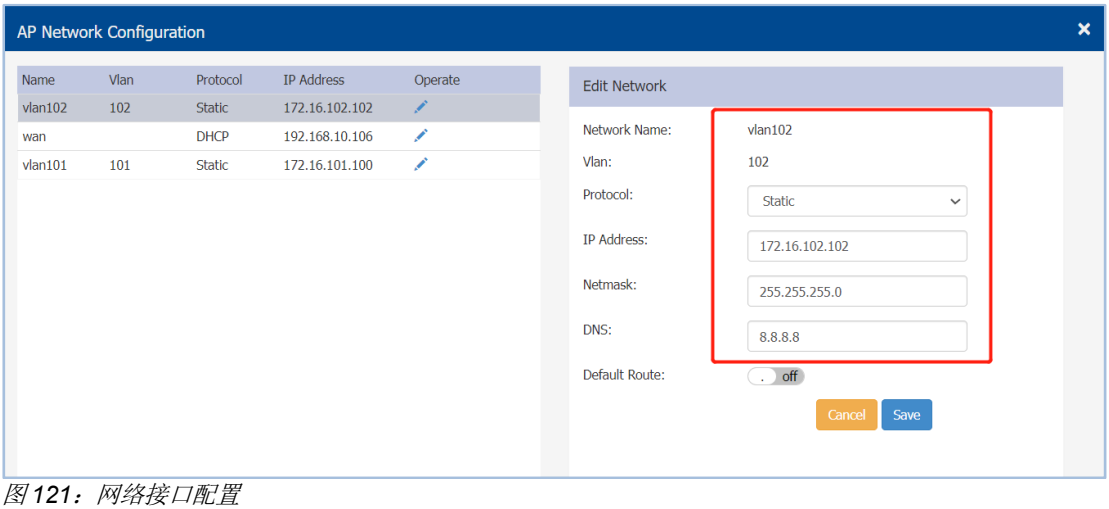


图 121：网络接口配置

注意：DHCP 地址池只能绑定到配置了静态 IP 的网络接口上。

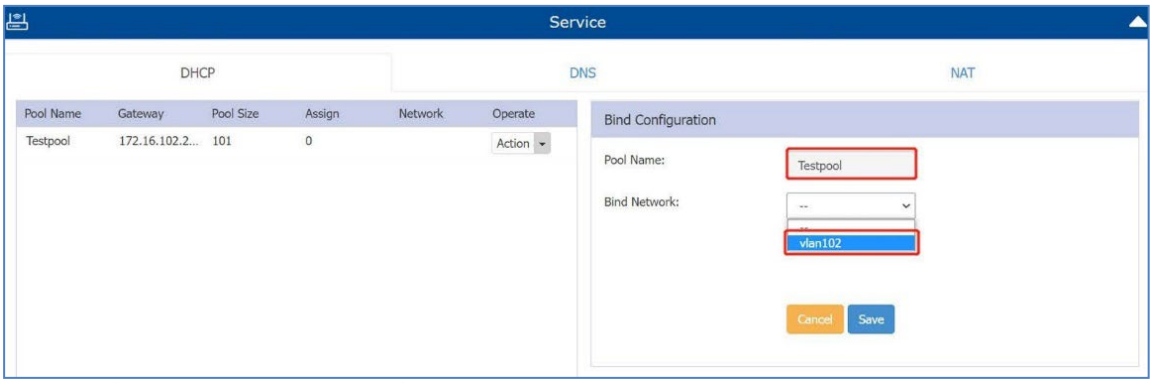


图 122：将 DHCP 地址池绑定到对应接口上

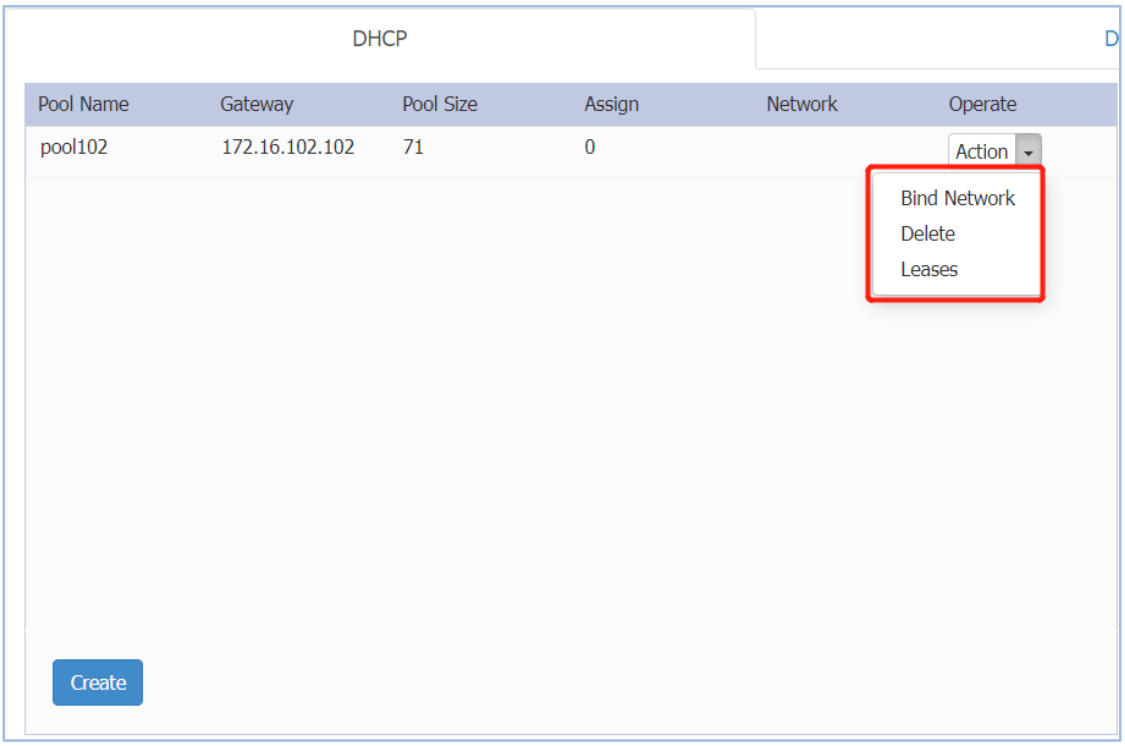


图 123：DHCP 地址池操作

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 DAP849 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**。

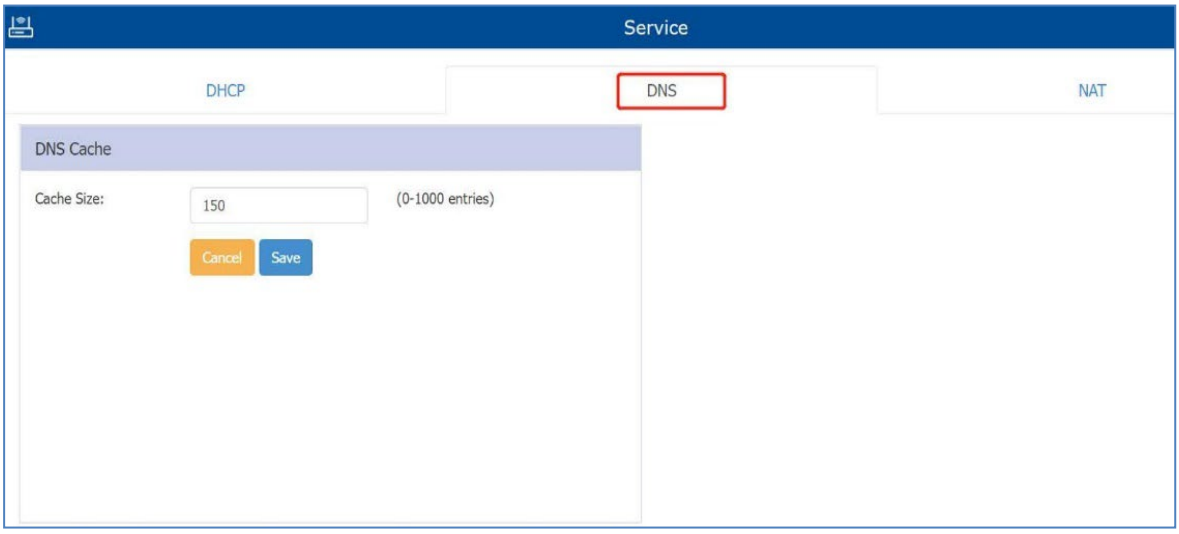


图 124：DNS 缓存配置

关键参数描述如下：

参数	描述
Cache Size	指定 DNS 缓存的数量，在 DAP849 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 DAP849 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 DAP849 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，DAP849 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。

DAP849 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 125。

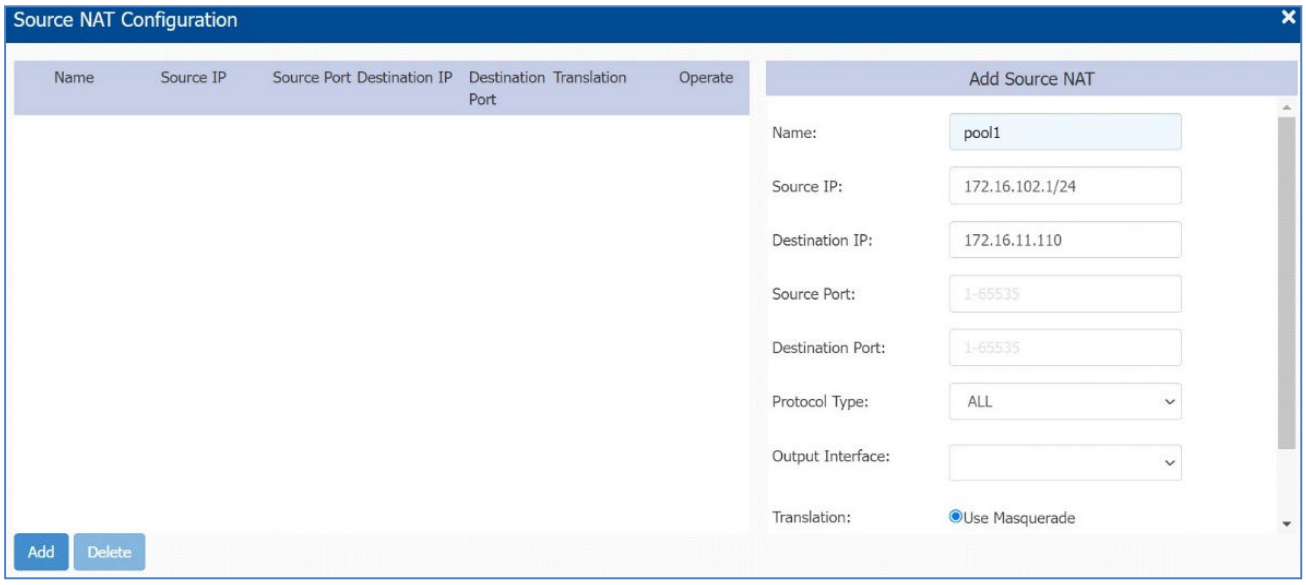


图 125：配置 Source NAT

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 126。

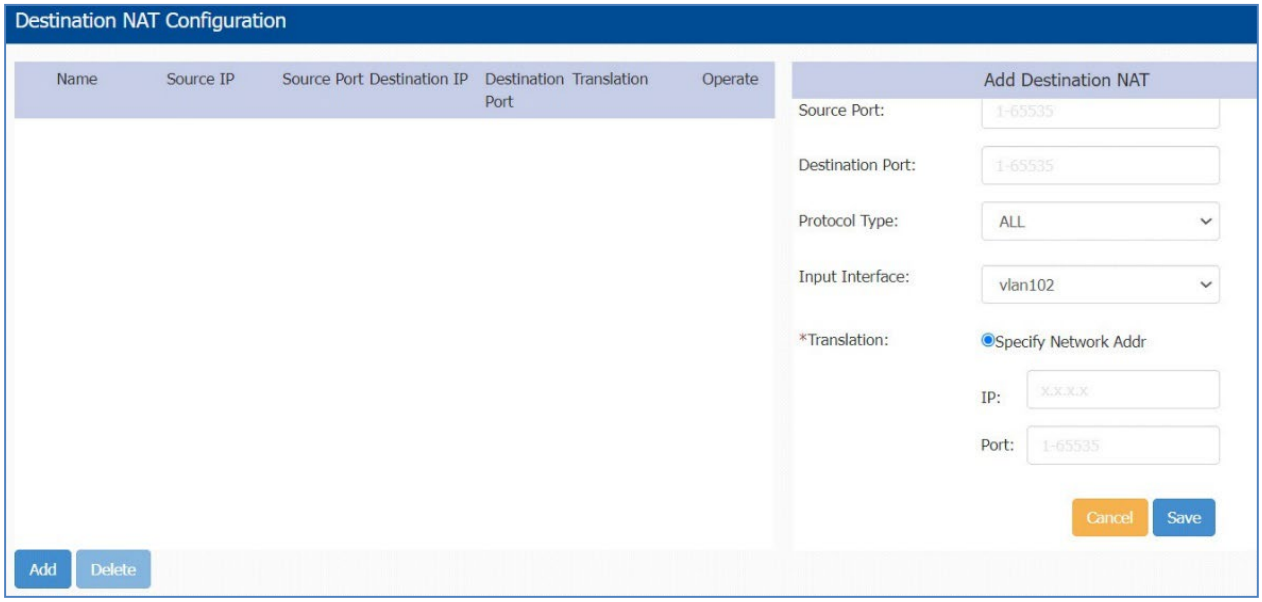


图 126：配置 Destination NAT

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	► **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 DAP849 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 DAP849 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
- 配置 SNMP

8.1 管理集群信息

如果要修改 DAP849 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。

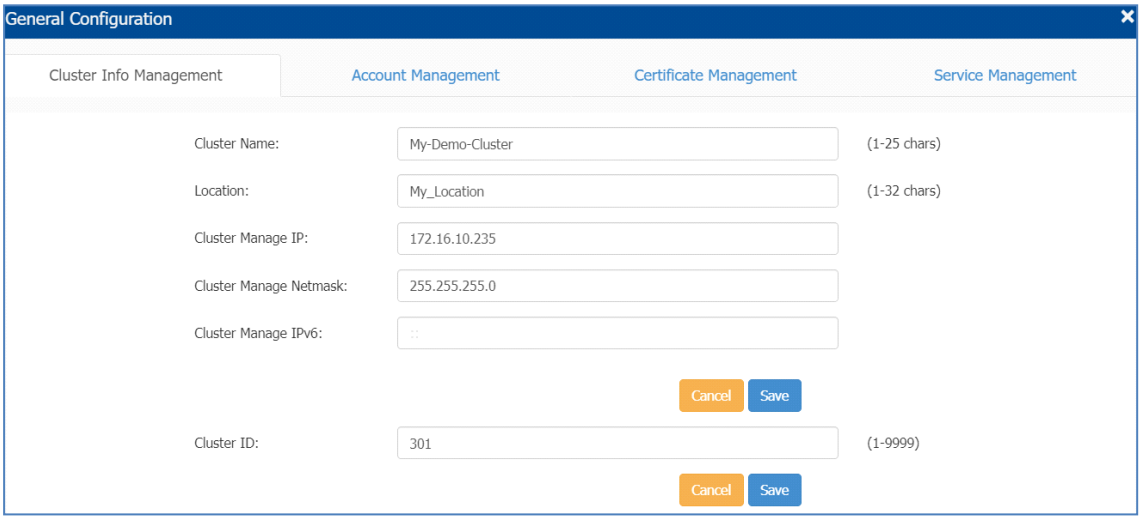


图 127：集群信息管理

关键参数描述如下：

参数	描述
Cluster Name	DAP849 集群的名称。
Location	DAP849 集群的位置。
Cluster Management IP	DAP849 集群管理的虚拟 IP 地址。
Cluster Management Netmask	DAP849 集群管理 IP 的子网掩码。
Cluster Management IPv6	DAP849 集群管理的虚拟 IPv6 地址。
Cluster ID	DAP849 集群的标识，默认集群 ID 为 100。

The DAP849 集群信息将会显示在页面顶部，如下图所示。

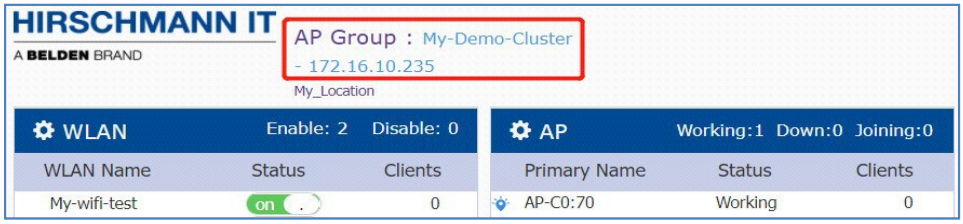


图 128：集群信息展示

注意：Cluster Management IP 是为 DAP849 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 DAP849 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

DAP849 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 DAP849 恢复出厂状态等。
- **Viewer**：Viewer 账户只有查看 DAP849 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 DAP849 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 129。

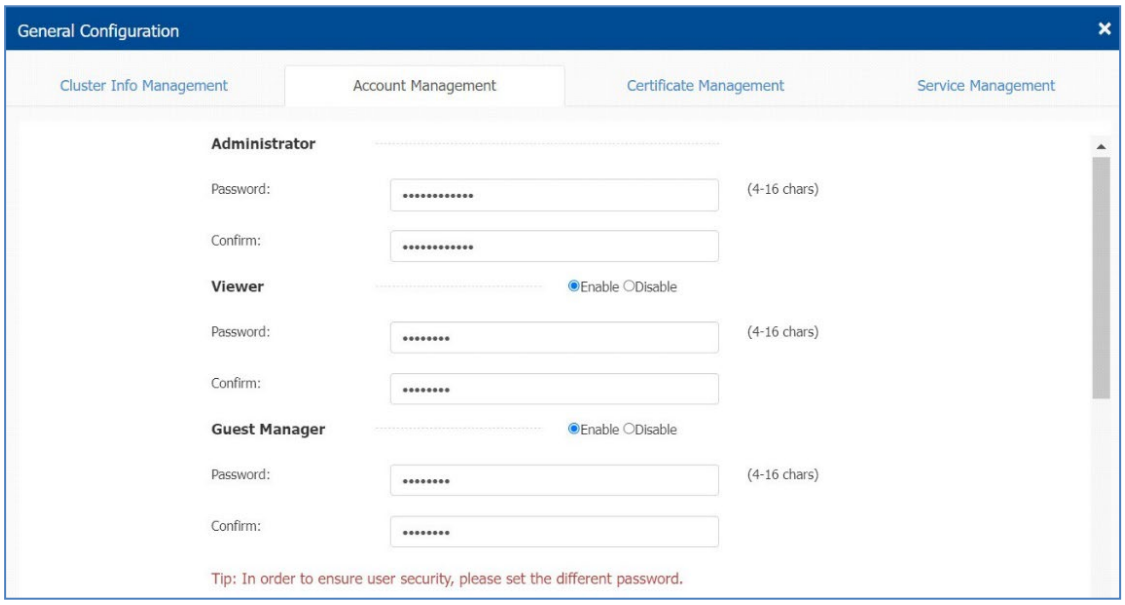


图 129：账户管理

8.2.2 管理 CLI 账户

DAP849 中同样内置了两个 CLI 用户，可以使用不同的权限登录 DAP849 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 DAP849 生成真正的 root 访问凭据，参考图 130。

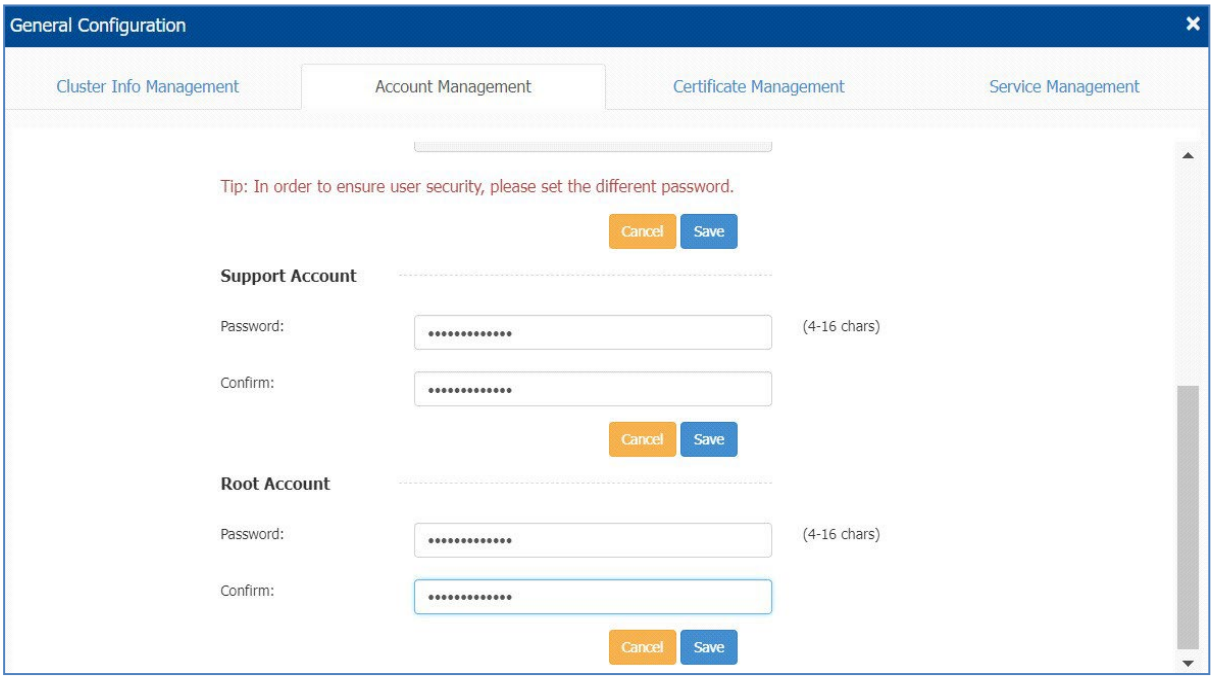


图 130：CLI 账户管理

注意：为了安全起见，建议管理员在使用 DAP849 前先修改 root 用户和 support 用户密码。

8.3 证书管理

DAP849 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 DAP849 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 DAP849 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**

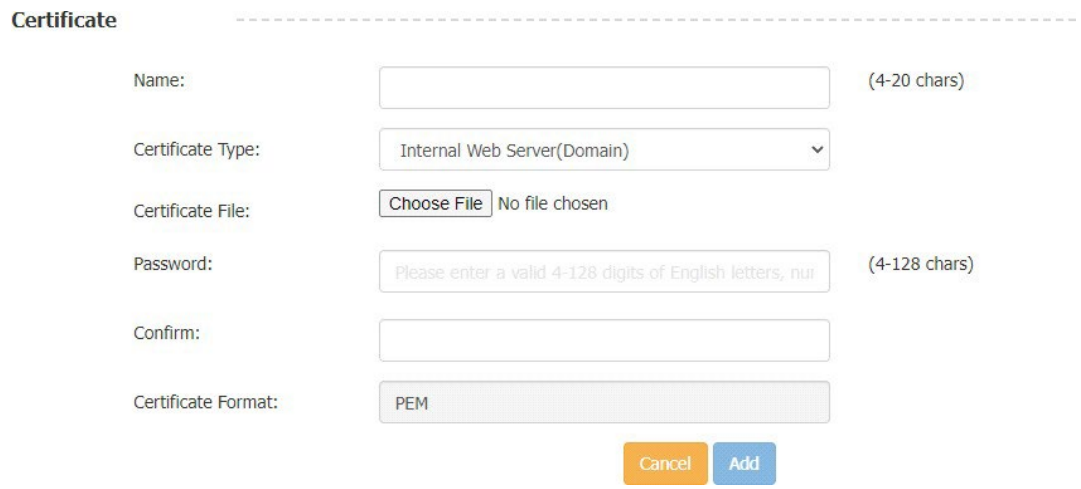


图 131：证书管理

8.4 系统服务配置

DAP849 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 132。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**：DAP849 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。

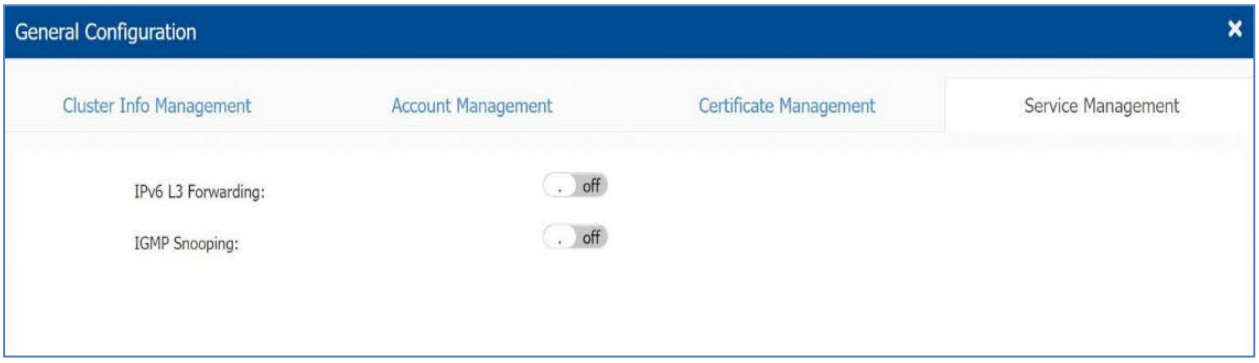


图 132：系统服务配置

8.5 配置系统时间

正确的系统时间对于 DAP849 的运行是非常重要的，DAP849 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 DAP849 将会每 15 分钟与 NTP 服务器同步一次时间。

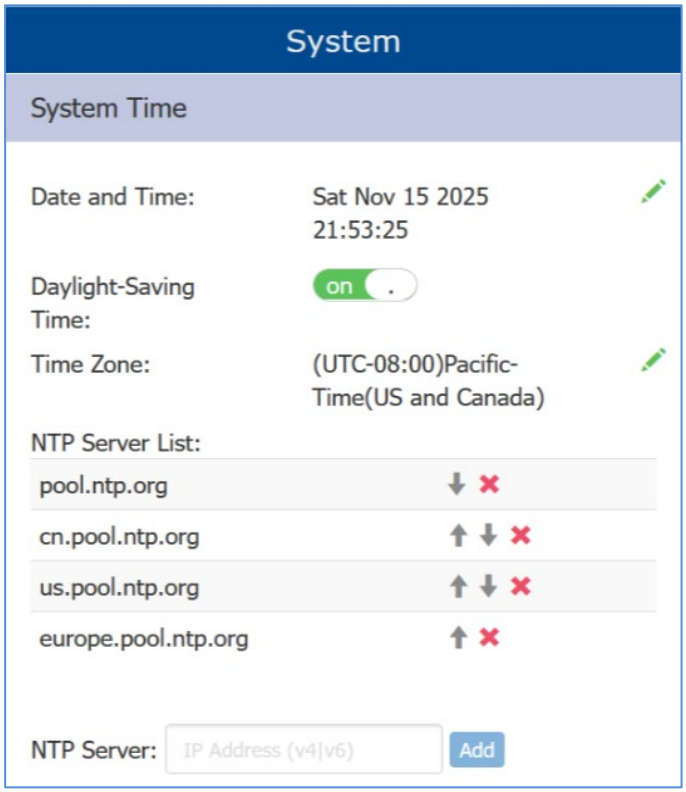


图 133：配置系统时间

根据需要，用户还可以指定 DAP849 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 134。

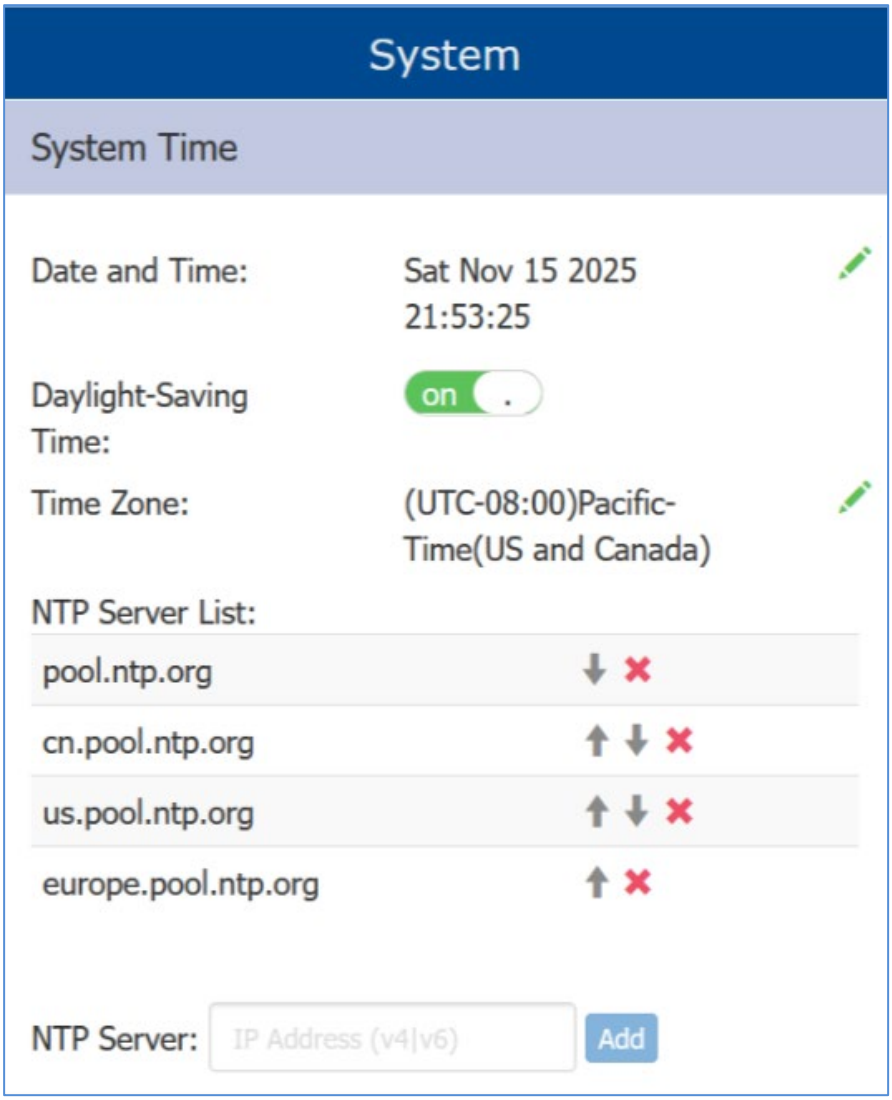


图 134：开启夏令时

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 DAP849 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。

DAP849 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 DAP849 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 DAP849 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。

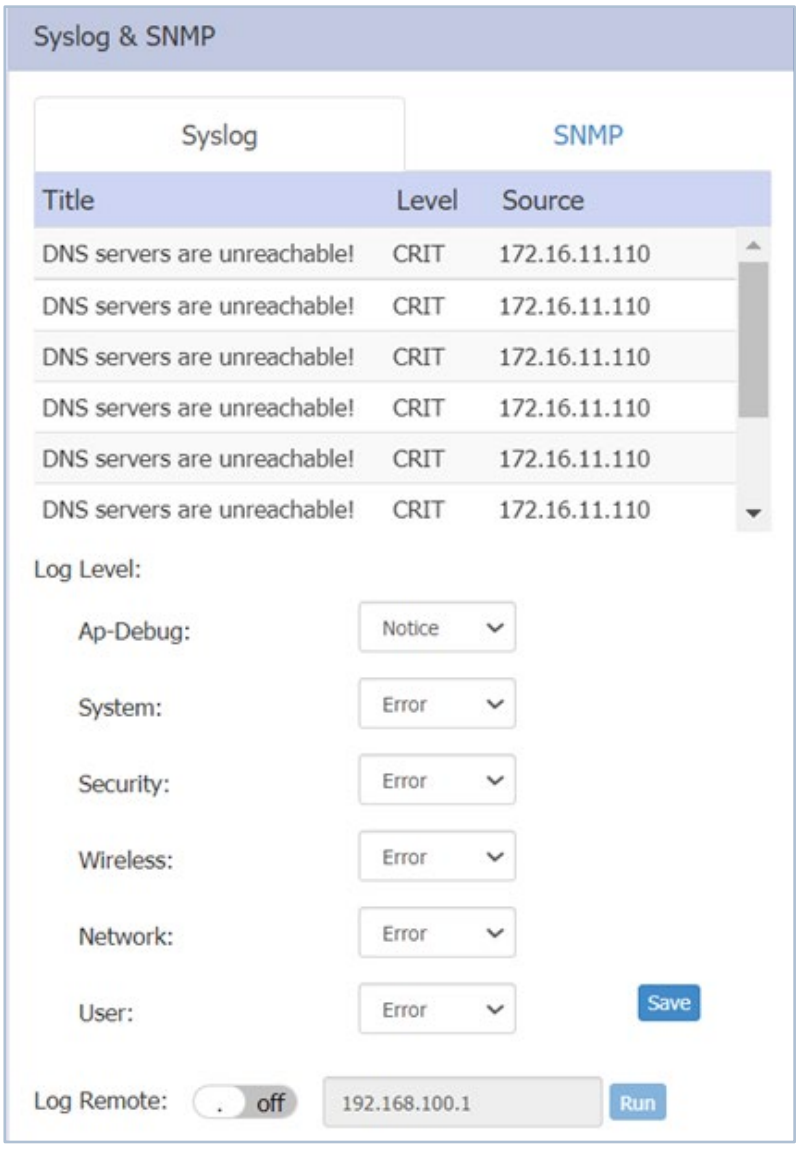


图 135：Syslog 配置

■ 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 DAP849 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 DAP849 设备的详细日志。
System	有关 DAP849 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

DAP849 支持设置远程日志服务器用来接收并存储 DAP849 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 2：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 DAP849 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。
  当 SNMP 版本选择为“**v2c**”时，在“**Community**”字段填入团体名。
  创建时，默认的团体名为“public”，建议修改为其他团体名。
- 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 DAP849 WIFI 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：

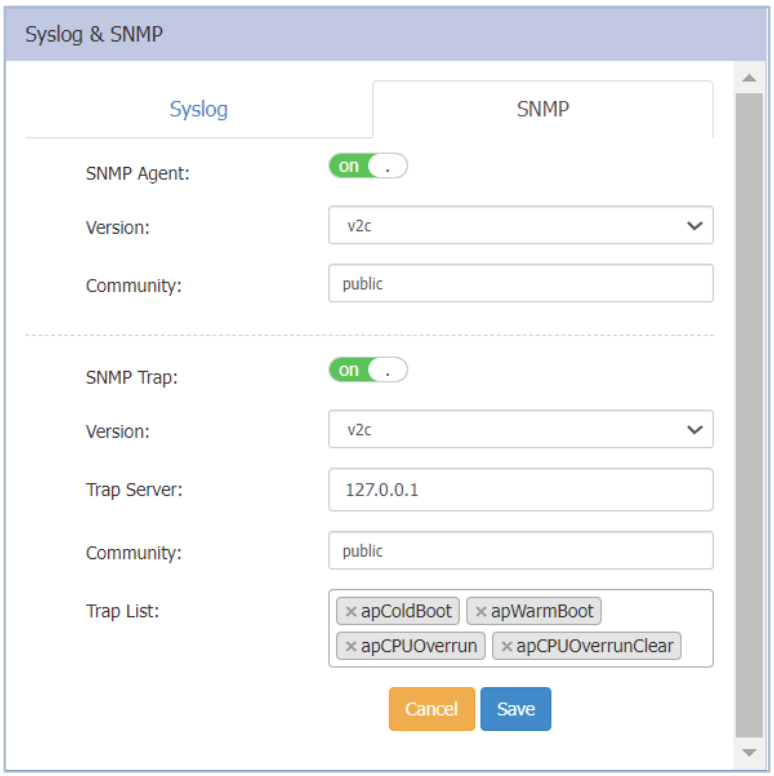


图 136：SNMPv2c 配置

配置 SNMPv2c Agent

参数	描述
SNMP Agent	启用或禁用 DAP849 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 DAP849 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（仅支持 SHA-AES 加密），需要配置如下参数：

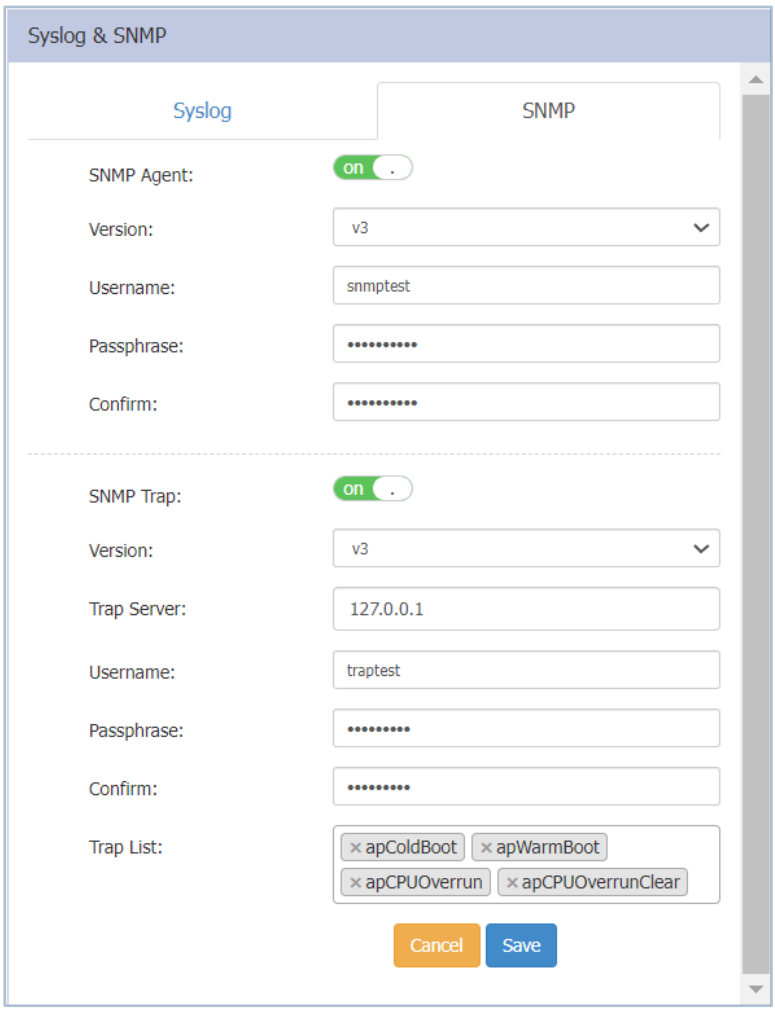


图 137：SNMPv3 配置

配置 SNMPv3 Agent:

参数	描述
SNMP Agent	启用或禁用 DAP849 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 DAP849 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。

注意：针对 apColdBoot，因设备硬件之间的差异性，建议断电 20 秒左右来触发该 trap。

9 无线管理

Wireless 页面用于展示 DAP849 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 138：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 DAP849 集群做全局 RF 配置，也可以根据需求分别针对每台 DAP849 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。

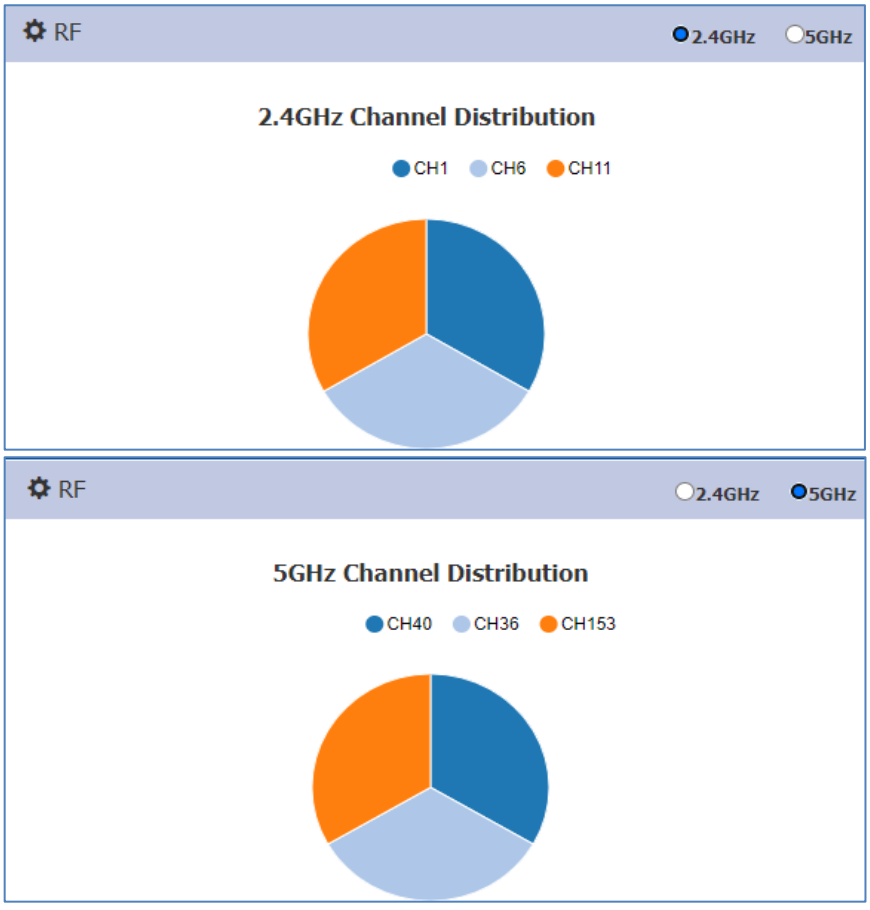


图 139：RF 配置

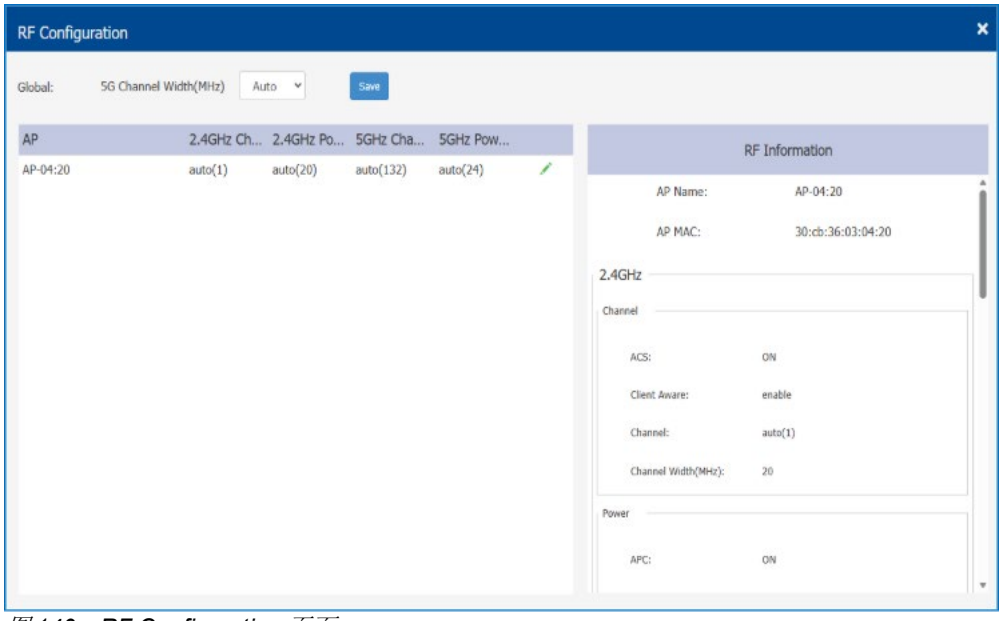


图 140：RF Configuration 页面

RF 配置页面显示了集群中 DAP849 的信道列表和发射功率，当在列表中选择一个 DAP849 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 DAP849 在 5 GHz 信道的带宽配置，参考图 141，您也可以选择指定的设备单独更改其信道宽度，参考图 146。

如果同时存在全局设置和私有配置，则最终生效的是 DAP849 的私有配置。

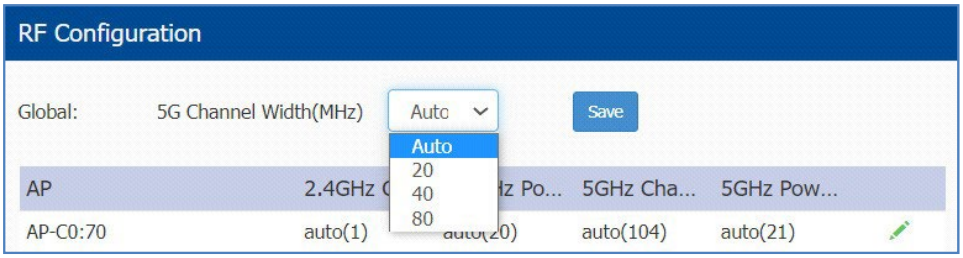


图 141：全局 5 GHz 信道带宽配置

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 DAP849 的功率和信道

在 RF 配置页面中，您可以修改 DAP849 的传输功率和工作信道，参考图 142。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 DAP849 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。

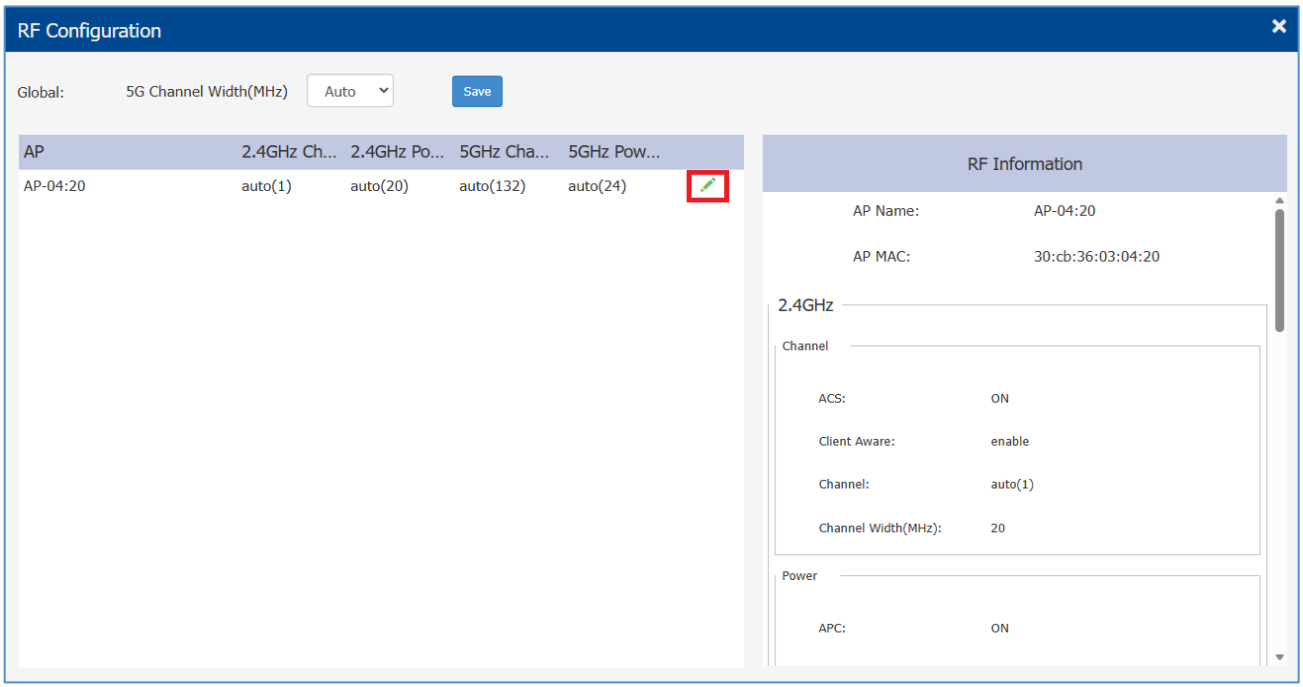


图 142：RF 配置

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 DAP849 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 143。

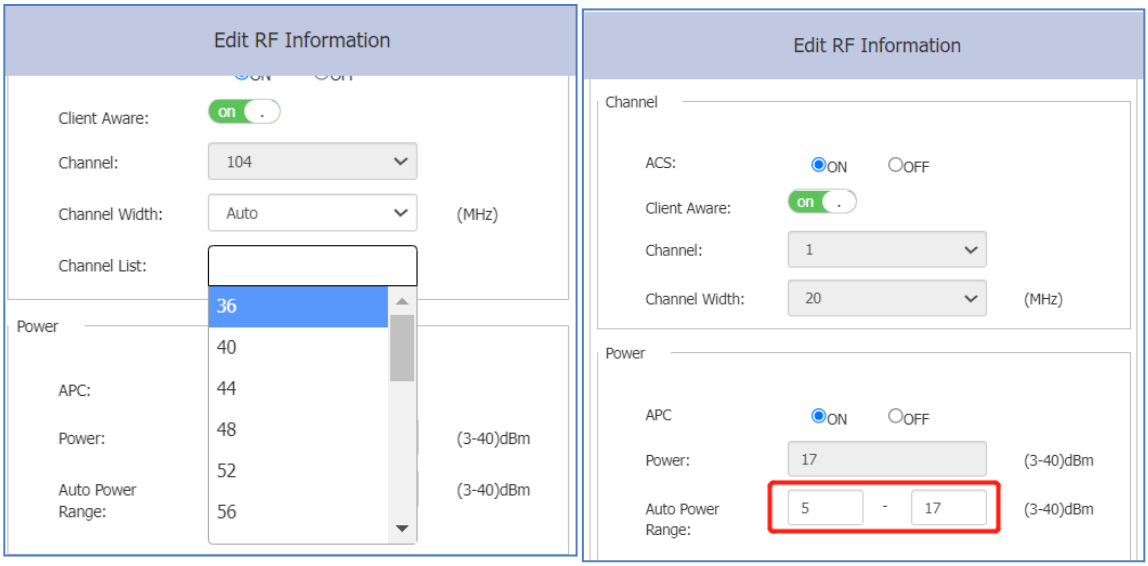


图 143：设置 Channel List 和 Auto Power Range

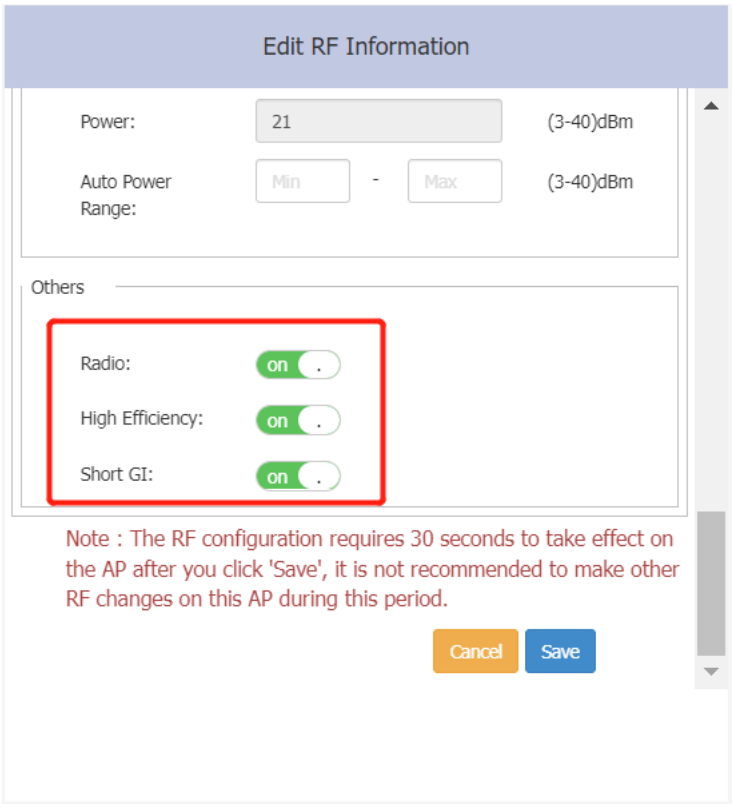


图 144：其他 RF 配置

■ 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，DAP849 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，DAP849 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 DAP849 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 DAP849 兼容性的问题。

9.1.2 DAP849 特定 DFS 信道配置

DAP849 在固定工作信道的情况下支持开启特定 DFS 信道跳转功能，参考图 145。当工作在 DFS 信道下，检测到雷达信号后跳转到 Radar Nest CH 进行避让，若该信道处于不可用状态则随机跳转其它信道。

特定 DFS 信道跳转功能关闭的情况下检测到雷达后默认进行随机信道跳转避让。若跳转后的信道为 DFS 信道，则信道 up 时间为 1 分钟或者 10 分钟；若跳转后的信道为非 DFS 信道，则信道 up 时间在 1s 内。

如果配置的频宽高于 20 MHz，不建议选择该频宽内的信道作为特定跳转信道，此情况下会触发随机跳转，失去了该特性的意义。

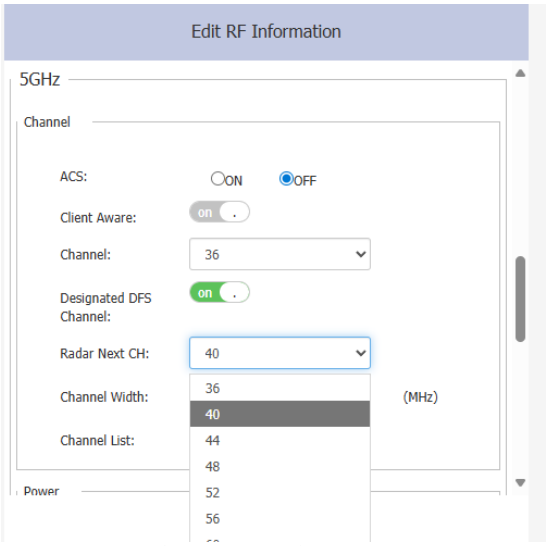


图 145：设置特定 DFS 信道

9.1.3 配置信道带宽

DAP849 支持 20 MHz、40 MHz、80 MHz 和 160 MHz 信道带宽，您可以在 DAP849 的私有 RF 配置中设置信道带宽，参考图 146。

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。
- 仅支持固定信道下配置 160 MHz 信道宽度。自动信道选择将不使用 160 MHz 频宽。
- 仅支持 MIMO 为 4x4 情况下使用 160 MHz 频宽。

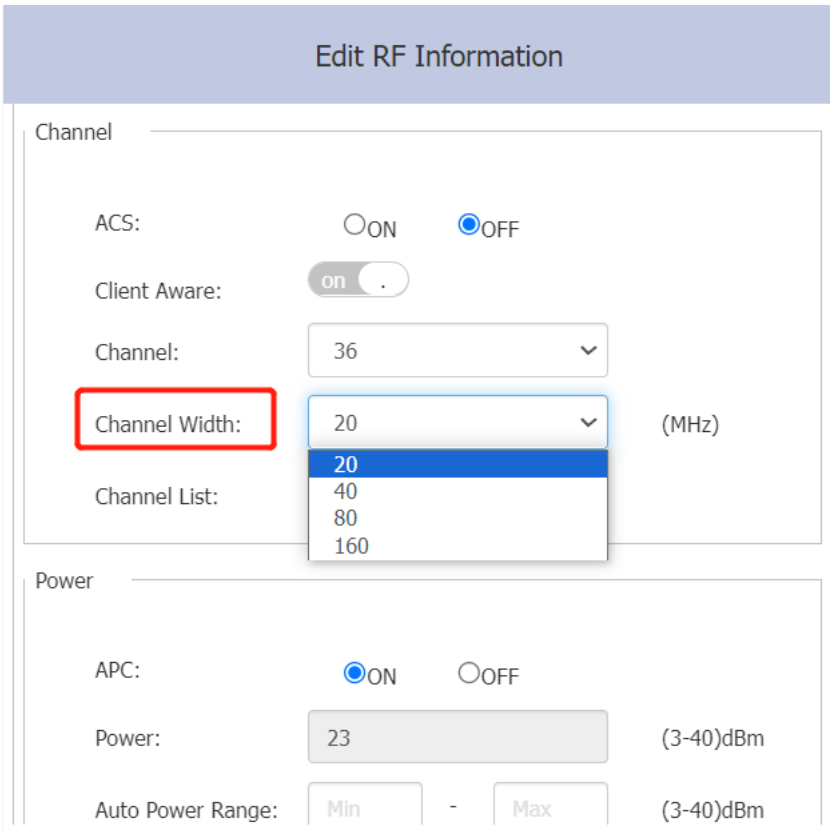


图 146：配置信道带宽

9.1.4 配置 DAP849 天线

在射频配置页面中，您可以配置 DAP849 天线的增益和 5G Radio 上的 MIMO 模式，如图 147 所示：

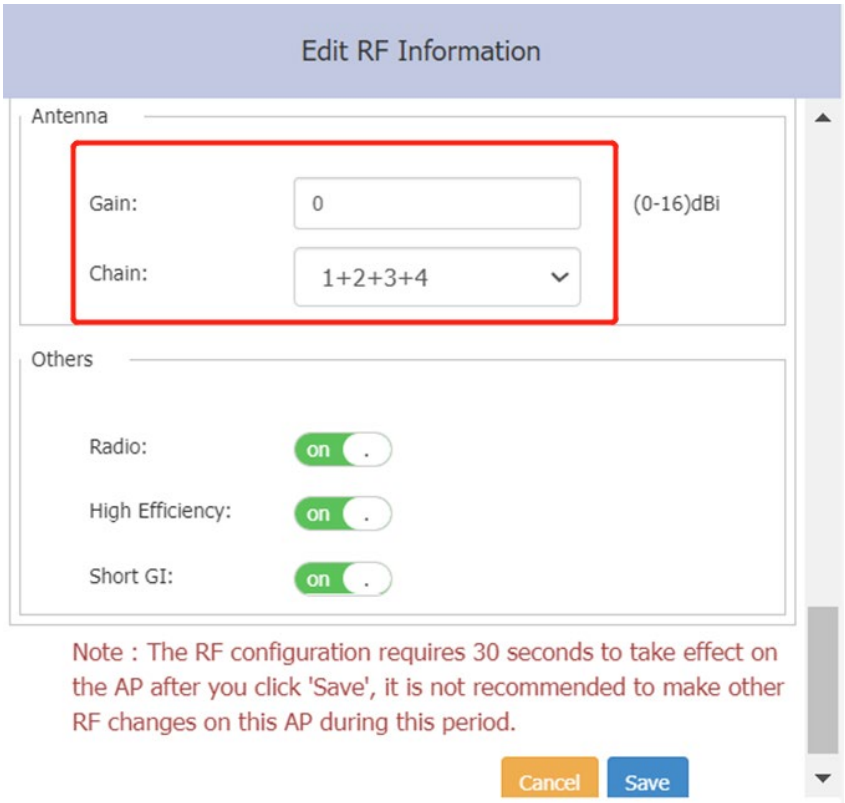


图 147：DAP849 天线配置

参数	描述
Gain	指定外部天线的增益值。
Chain	表示 DAP849 的 MIMO 模式，即外部天线的配置： • 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

9.1.5 开启/关闭 DAP849 的无线射频

您可以通过单击 Radio on/off 按钮来关闭集群中 DAP849 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 148。

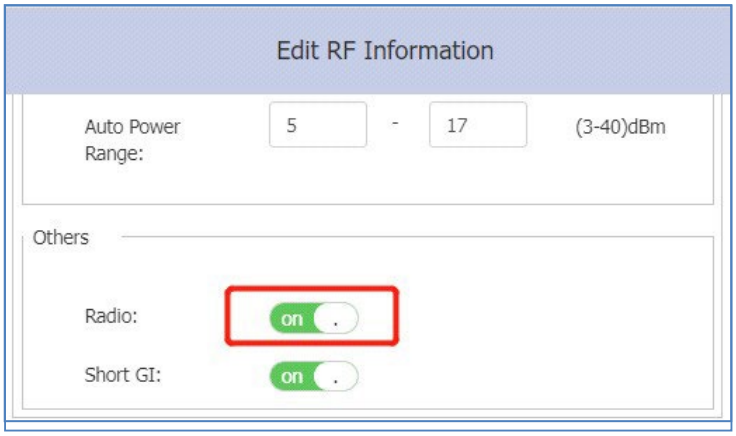


图 148：开启或关闭无线射频模块

9.2 wIDS/wIPS

DAP849 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 或 BWO 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。它还保护企业网络和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**：DAP849 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 149 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 150。

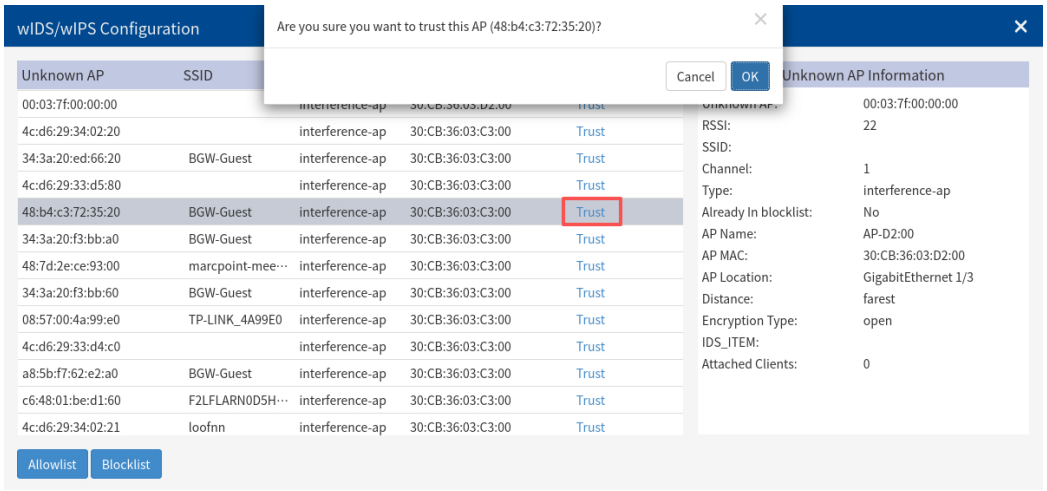


图 149：Trust AP

- **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 DAP849 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 DAP849 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 153。
- **Wireless Attack Detection：**如果启用了 Wireless Attack Detection，DAP849 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 150。

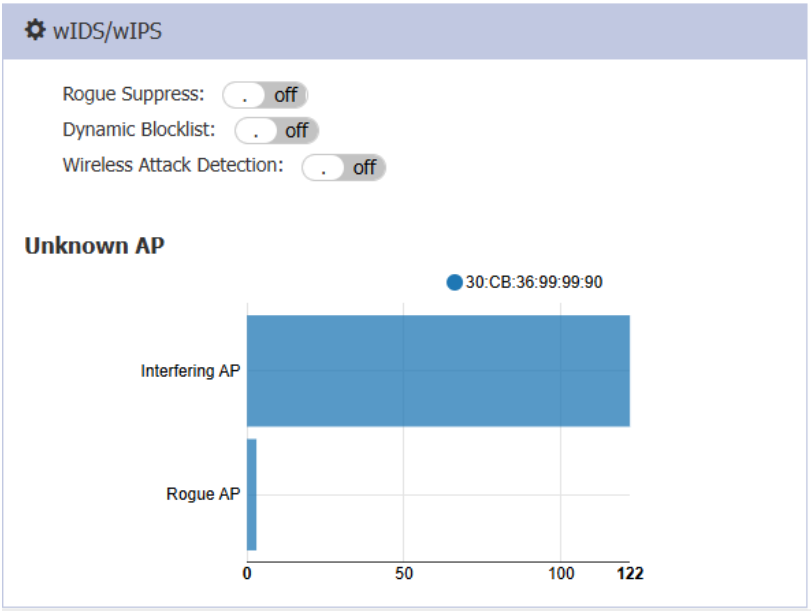


图 150：wIDS/wIPS 页面

- **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 DAP849 集群广播相同 SSID 的外部干扰 AP，Rogue AP 通常被认为是 DAP849 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 151 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。

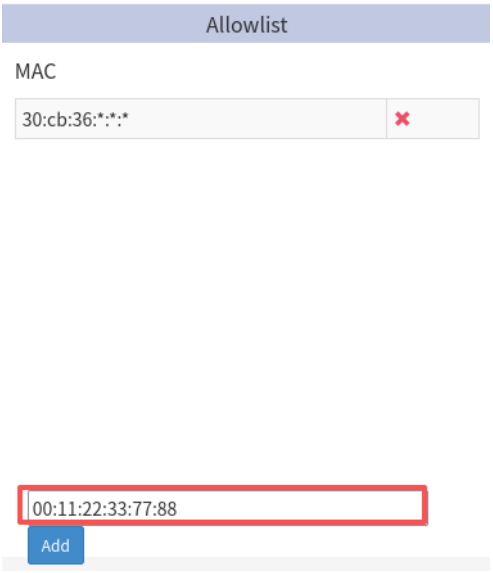


图 151：AP Allowlist

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 152。

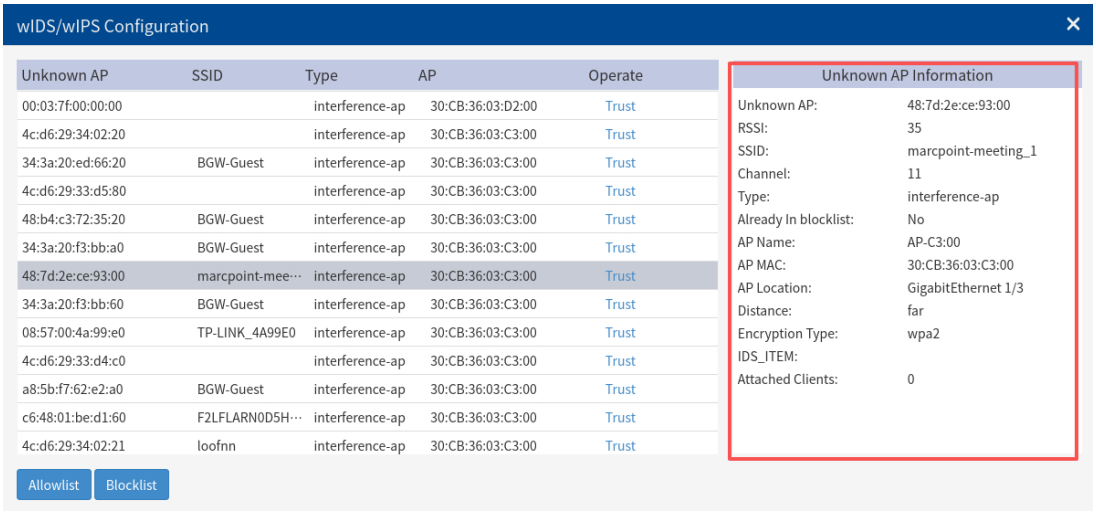


图 152：wIDS/wIPS Configuration 页面

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 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 DAP849 设备的名称。
AP MAC	群集中检测到该未知 AP 的 DAP849 设备的 MAC 地址。
AP Location	群集中检测到该未知 AP 的 DAP849 设备的地址。
Distance	集群中未知 AP 和检测 DAP849 之间的距离，该距离通过未知 AP 的 RSSI 计算得出： Nearest：RSSI≥(-20 dBm) Near：(-45 dBm)≤RSSI<(-20 dBm) Far：(-70 dBm)<RSSI<(-45 dBm) Farthest：RSSI≤(-70 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威胁或风险，如识别出： ► 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

参数	描述
	▶ 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 DAP849 无线网络，参考图 153。

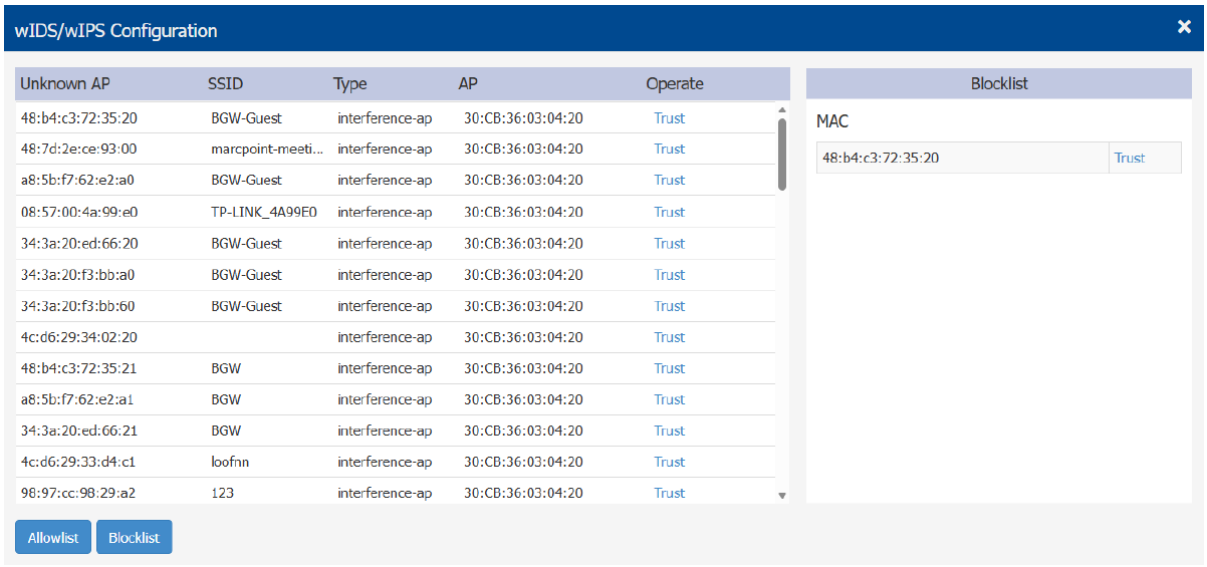


图 153：添加 Blocklist

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 DAP849 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 DAP849 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 154。

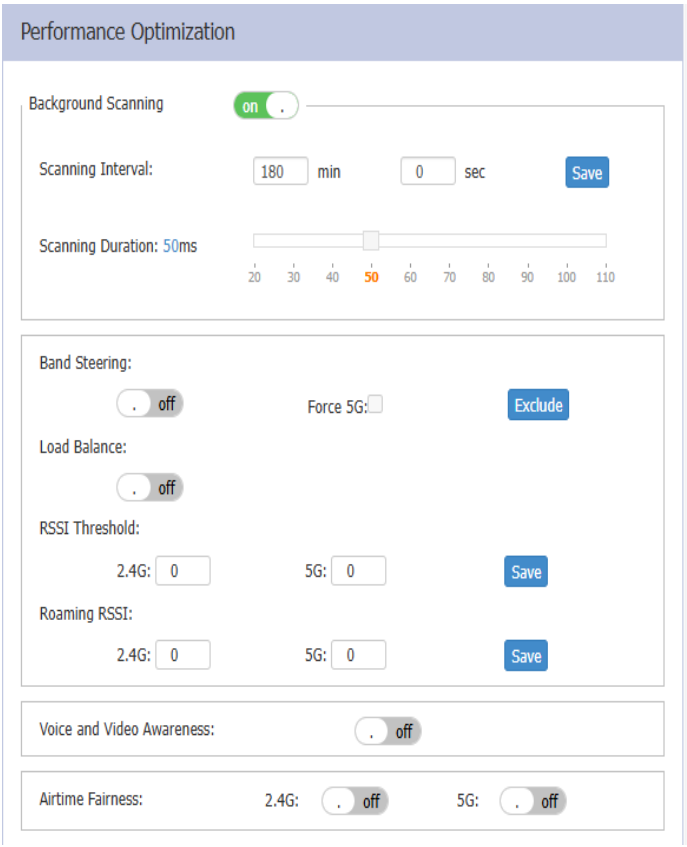


图 154：无线性能优化配置

- **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。

背景扫描时长可以根据部署要求进行配置，配置的范围为 20 到 110ms。该参数会影响 WLAN 的性能。对于 DAP849，有专用扫描接口，该参数失效。

注意：为DAP849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 DAP849 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，DAP849 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 DAP849 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 DAP849 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 DAP849 上的一种网络优化技术，它能够平衡 DAP849 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 DAP849 之间的公平分配，基于客户端的密度、DAP849 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”，DAP849 将不会对客户端做出响应。是否配置该参数与 IEEE 802.11kv 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 0-100。

- **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 DAP849 和无线客户端之间的 IEEE 802.11k 和 IEEE 802.11 v 消息交换。
  - 当 DAP849 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 DAP849。
  - 基于接收到的数据，DAP849 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 DAP849 发送的 IEEE 802.11v 事件中获取一个目标 BSSID，或是选择在 DAP849 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 DAP849 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，DAP849 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 155。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 156。

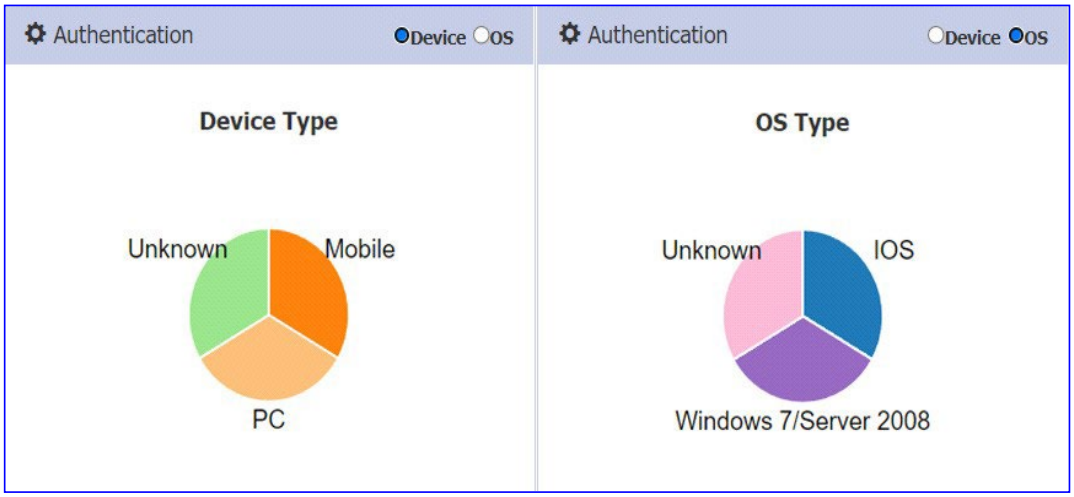


图 155：Authentication 统计面板

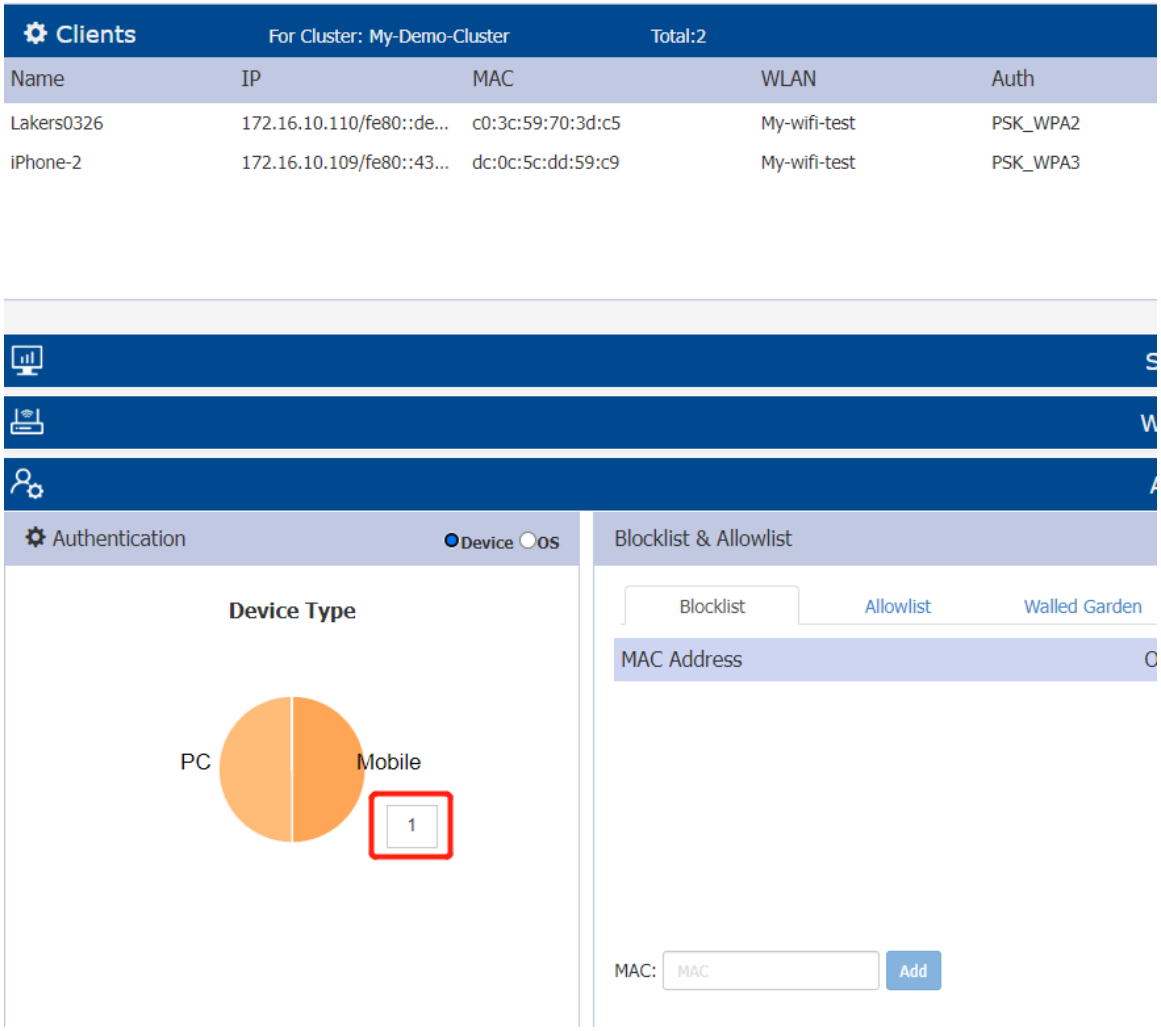


图 156：Device 类型

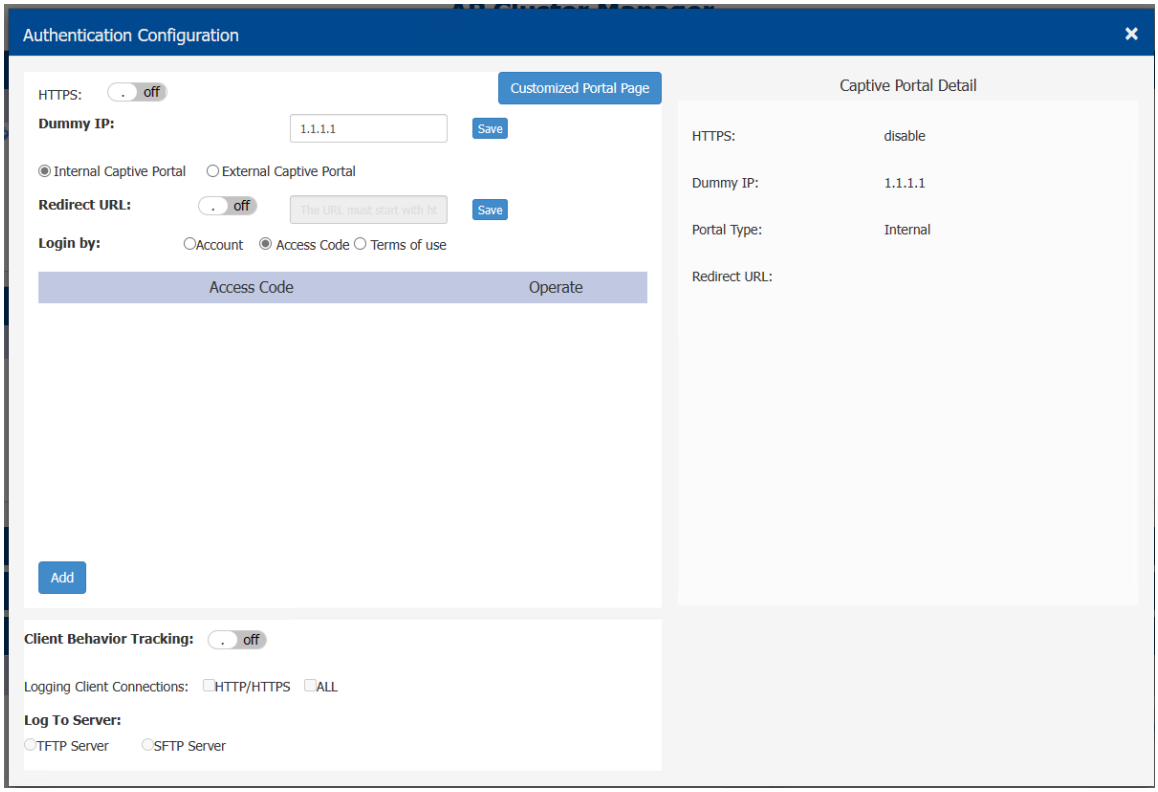


图 157：Authentication Configuration 页面

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	▶ **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	▶ **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 158。关于创建 Captive Portal 类型 WLAN 的步骤，请参阅第 55 页的“WLAN 的安全类型”。

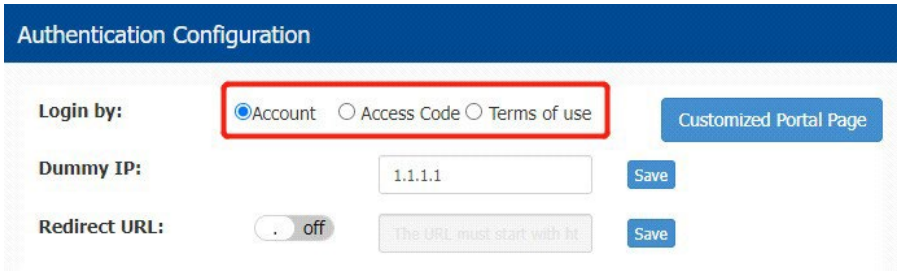


图 158：选择登录方式

■ 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。

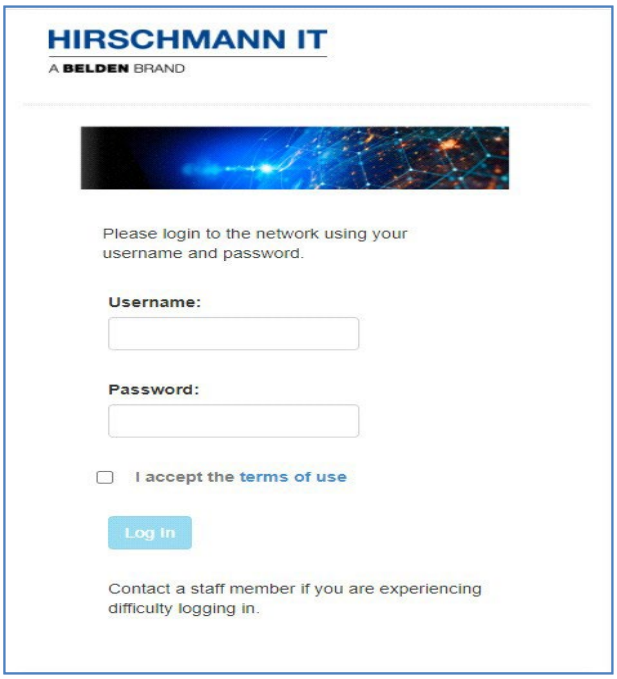


图 159：使用用户名和密码方式登陆

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。

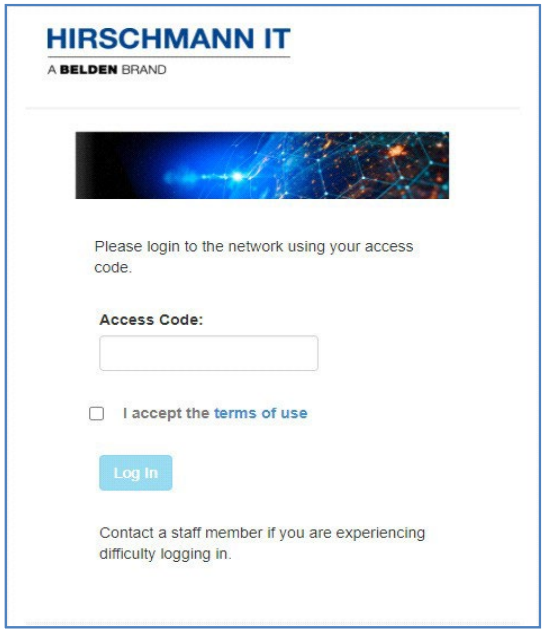


图 160：使用 Access Code 登陆

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。

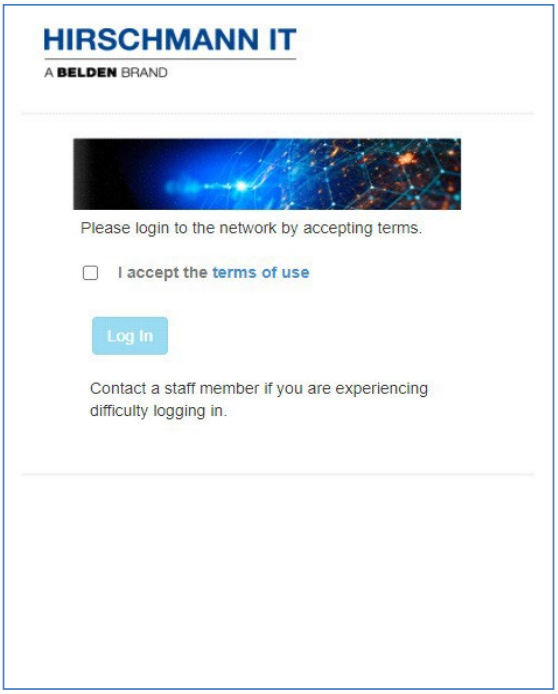


图 161：Terms of use 登陆

10.3 账号和 Access Code 管理

对于用户账户或 Access Code 登录方式，目前 DAP849 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 162。

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 163。

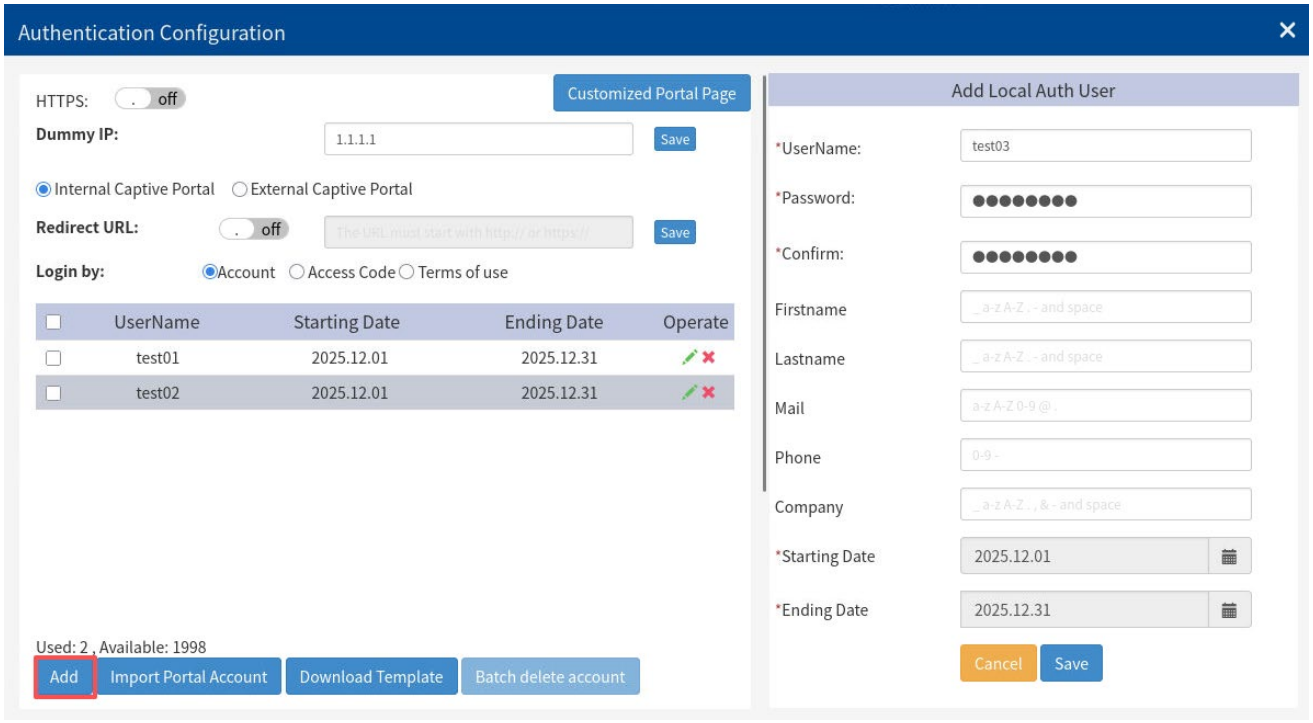


图 162：创建一个新账户

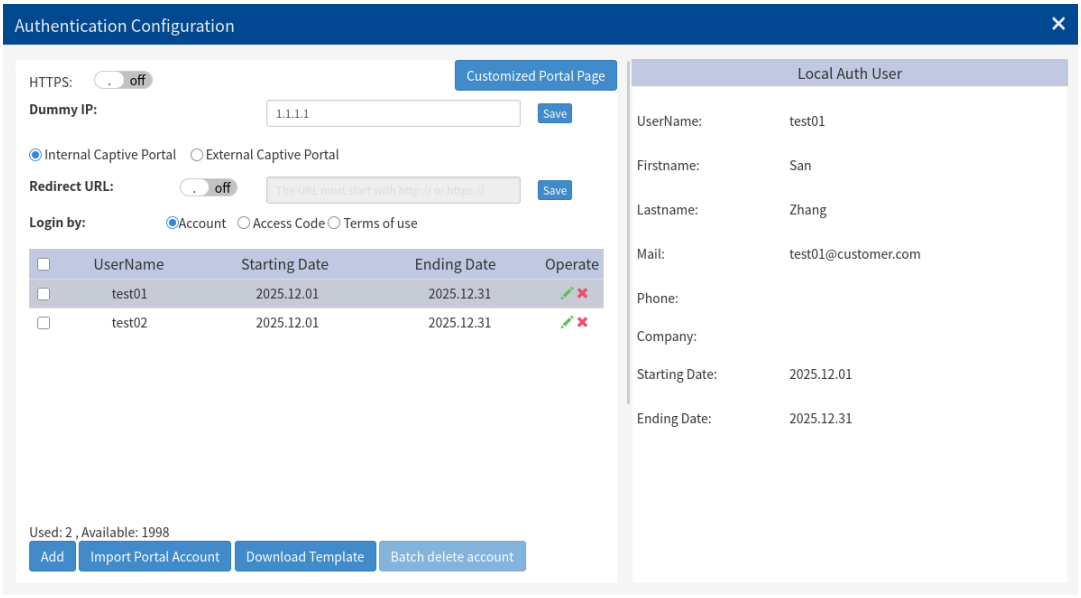


图 163：账户详细信息

■ 批量导入 Portal 账户

DAP849 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。

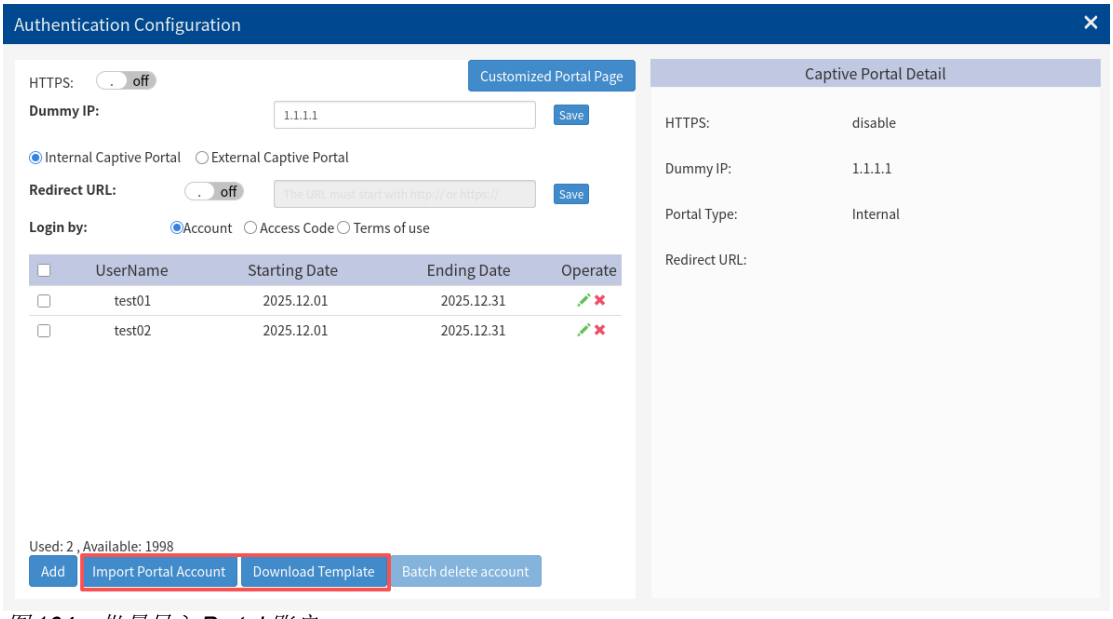


图 164：批量导入 Portal 账户

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 165 所示。

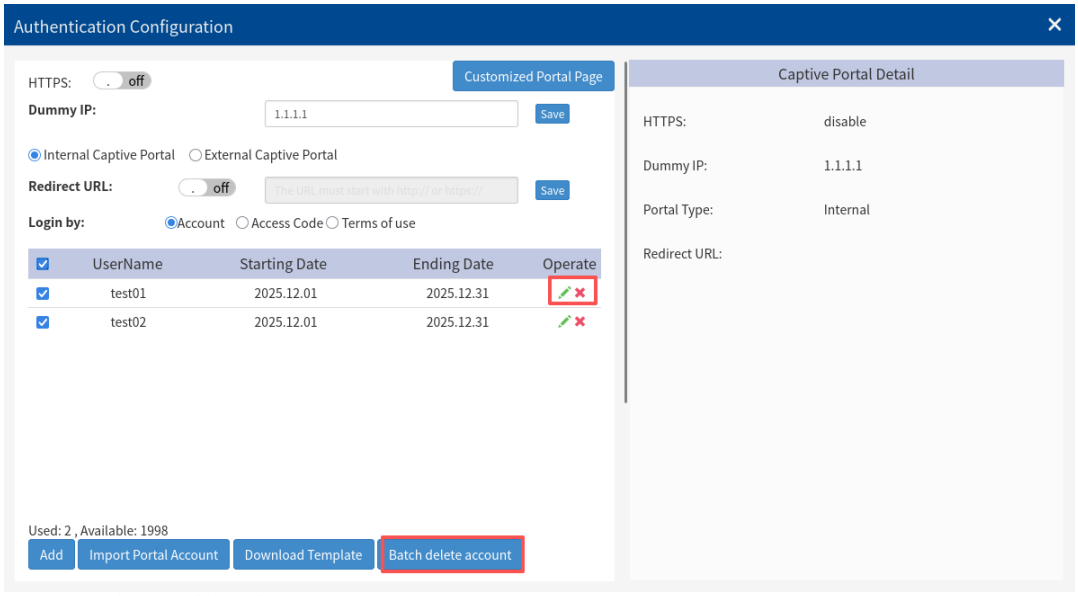


图 165：修改或删除账户

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“✖”按键删除一个 Access Code，参考图 166。

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账户或 Access Code。

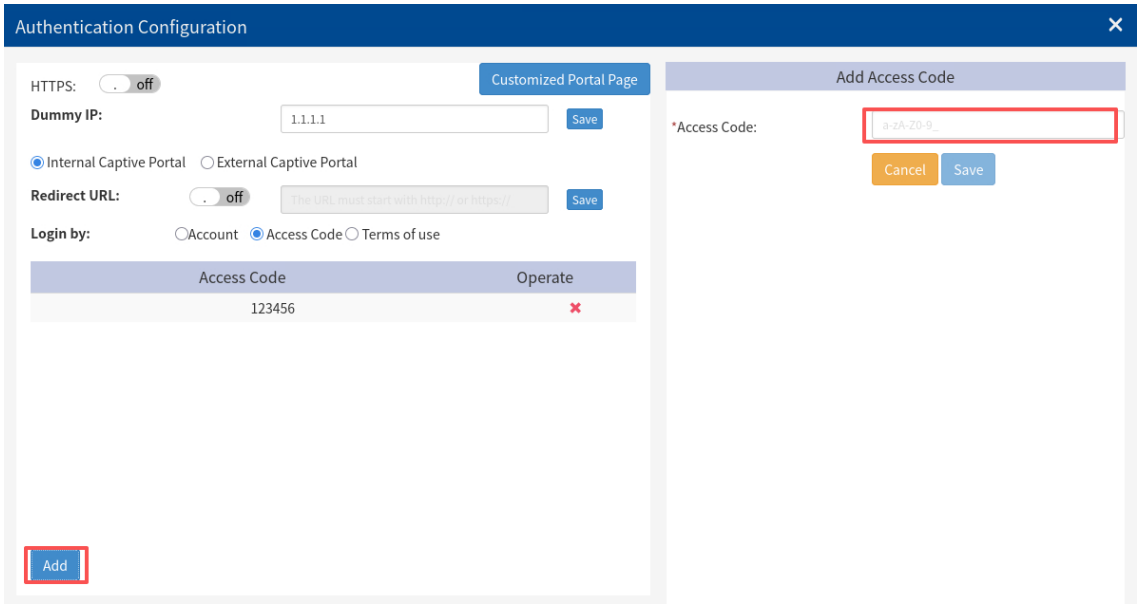


图 166：创建一个 Access code

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 167。

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。

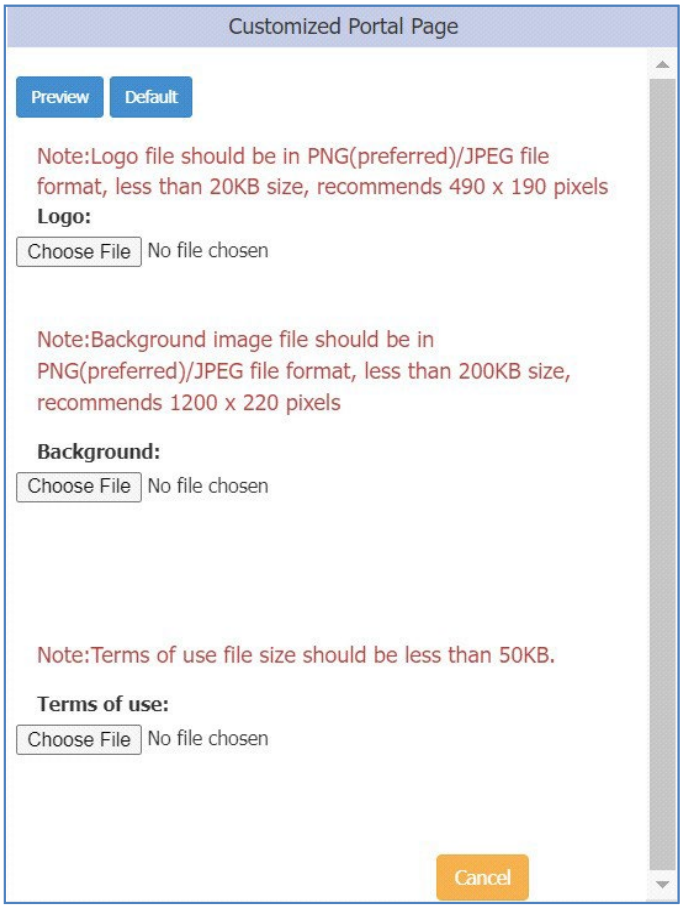


图 167：定制化 Captive Portal 页面

10.5 无线客户端黑名单

Blocklist 是指 DAP849 的黑名单列表，用于无线用户的访问控制，其中记录了被 DAP849 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 DAP849 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。

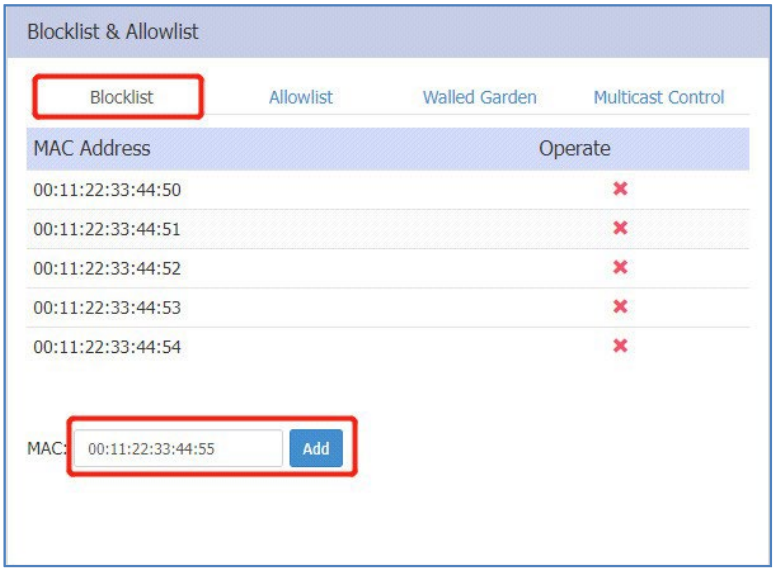


图 168：Blocklist 配置

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。

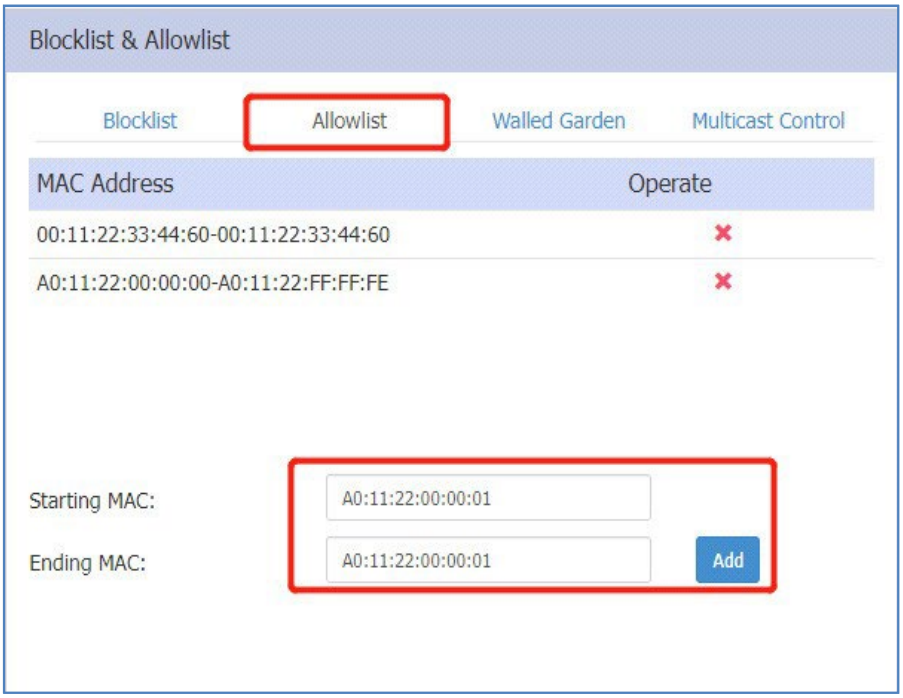


图 169：Allowlist 配置

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。

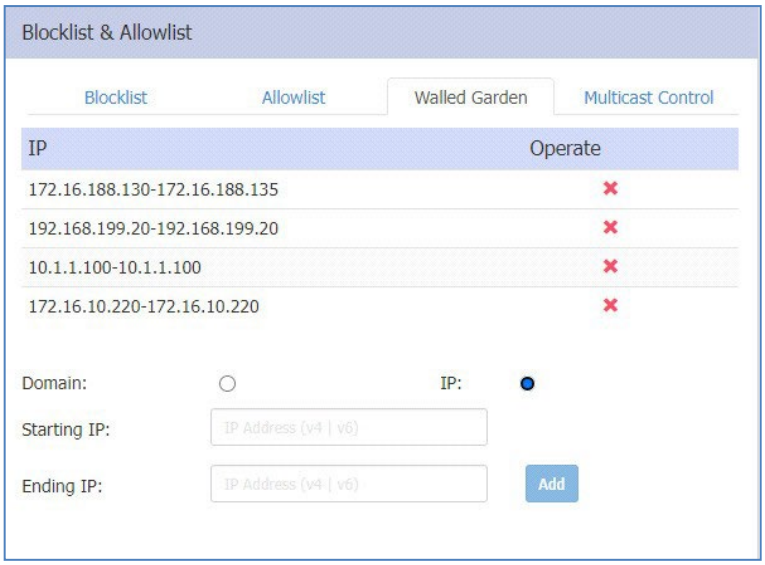


图 170：IP 地址格式的 Walled Garden 配置

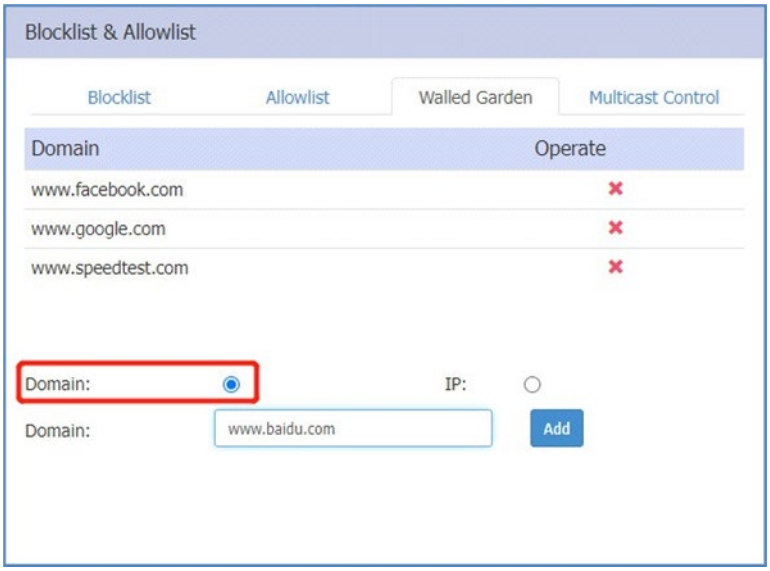


图 171：域名格式的 Walled Garden 配置

10.8 组播控制

组播控制用于从有线网络（交换机端口）向 DAP849 转发 mDNS 组播流量。启用该功能后，DAP849 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，DAP849 将无差别转发 mDNS 流量。

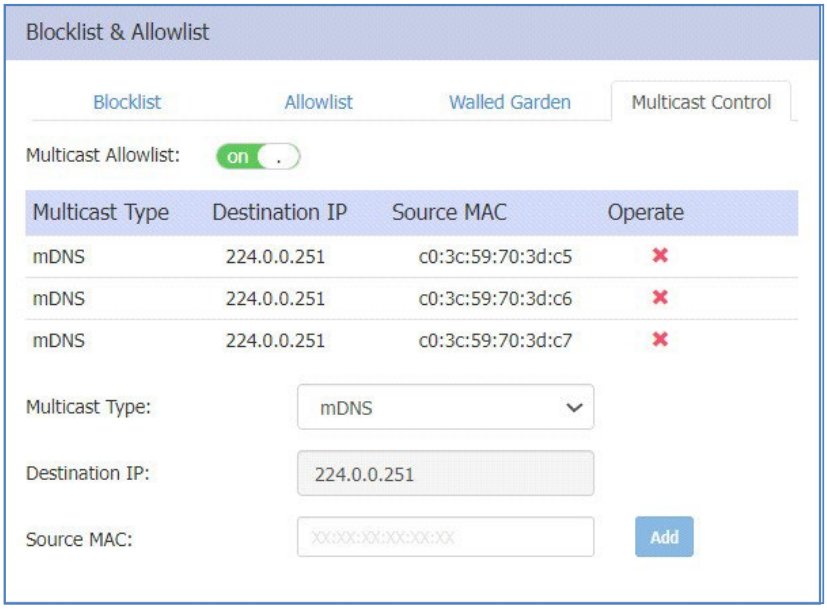


图 172：组播控制

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 173 和图 174。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。

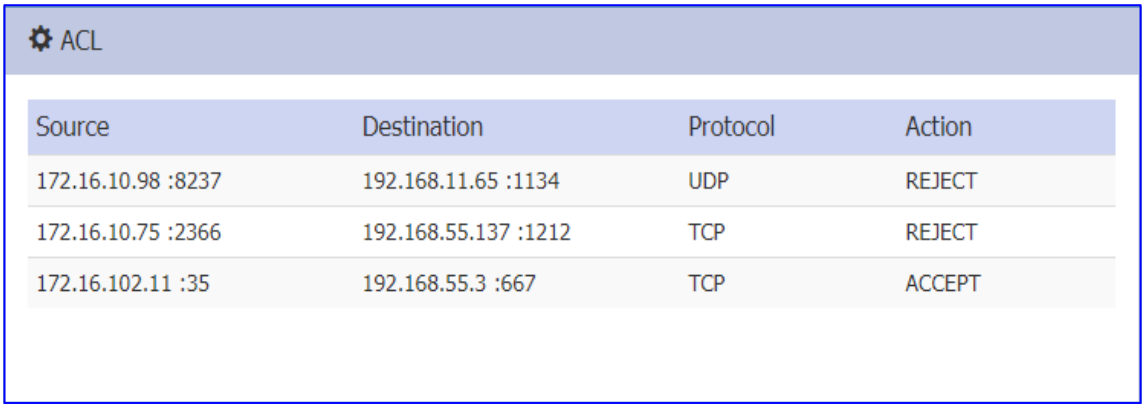


图 173：ACL 基本模式

DAP849 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 174。

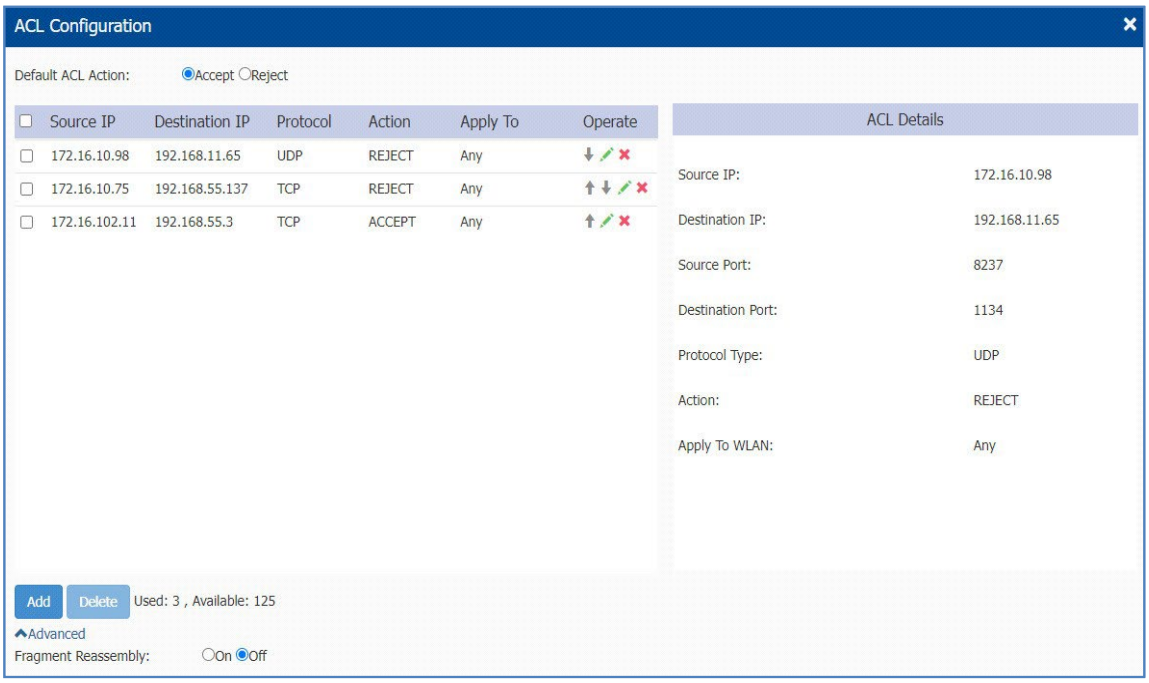


图 174：ACL 配置页面

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 协议报文的目的端口。
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

DAP849 不支持 IoT 功能，但如果 DAP849 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，详细信息请参阅 DAP 系列用户手册。

12 DAP849 内部集成工具

12.1 Tools

Tools 是 DAP849 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 DAP849 中执行，通过这些工具，网络管理员能够查看 DAP849 上的运行信息，例如系统状态、Wi-Fi 信息和重启原因等。

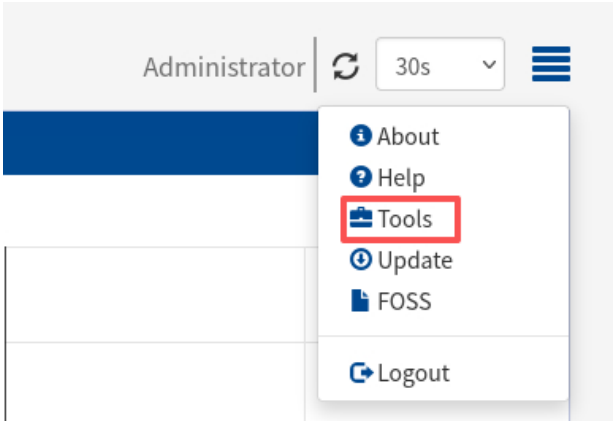


图 175：进入 Tools 页面

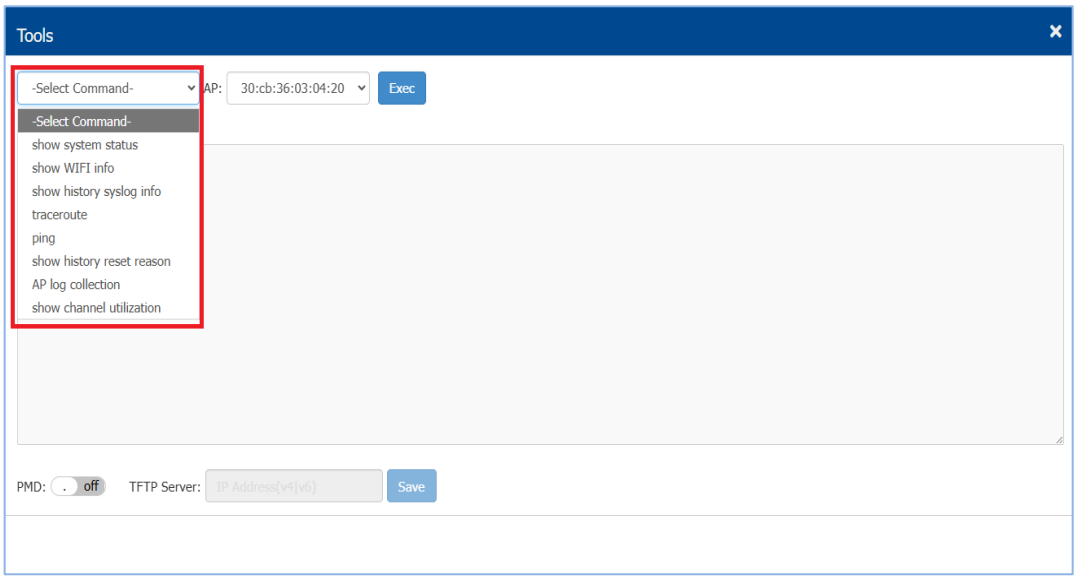


图 176：DAP849 集成的工具

- **show system status：**显示 DAP849 的内存的使用情况。

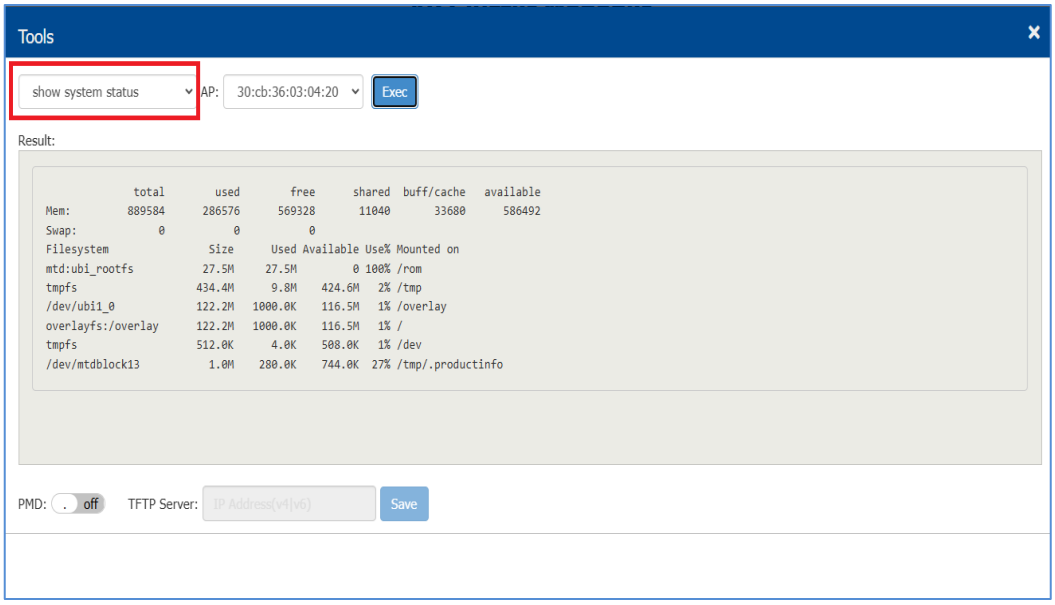


图 177：显示系统状态

- **show WIFI info**：显示 DAP849 无线接口的状态信息。

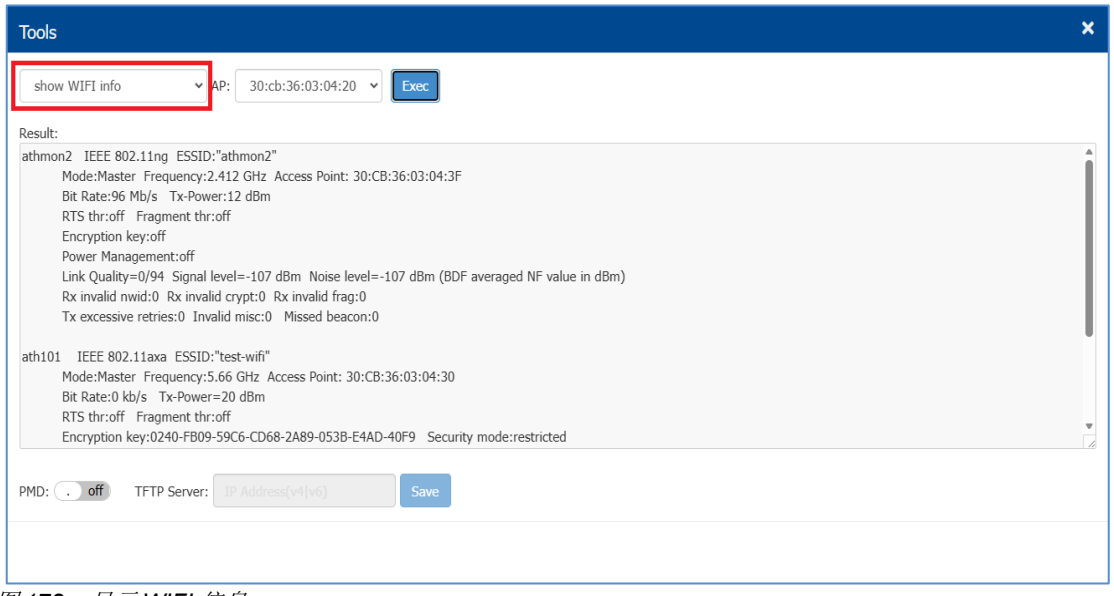


图 178：显示 WIFI 信息

- **show history syslog info**：显示指定 DAP849 最近一次运行期间（系统启动之前）生成的历史 Syslog 日志消息。

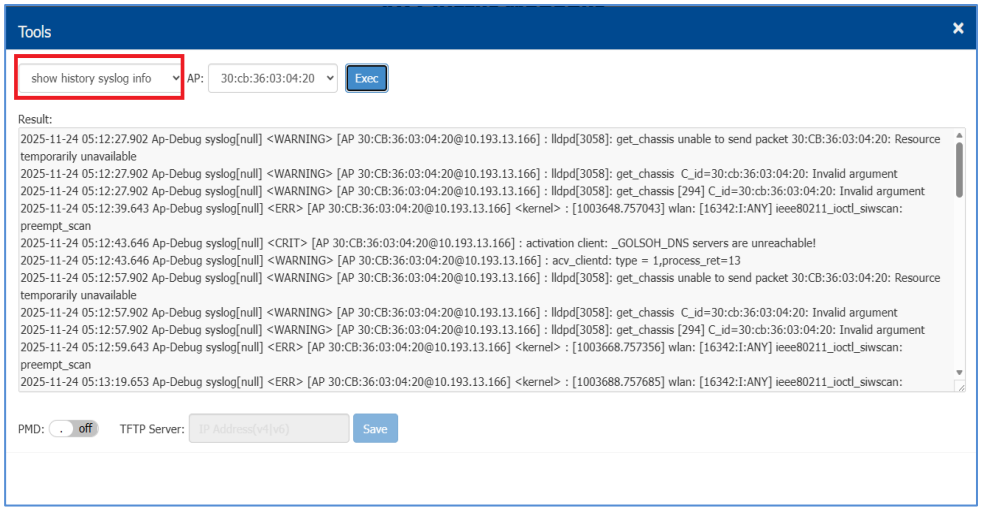


图 179：显示历史 Syslog 日志消息

- **traceroute**：DAP849 内置的 traceroute 工具，用于检查网络中的路由信息，参考图 180。

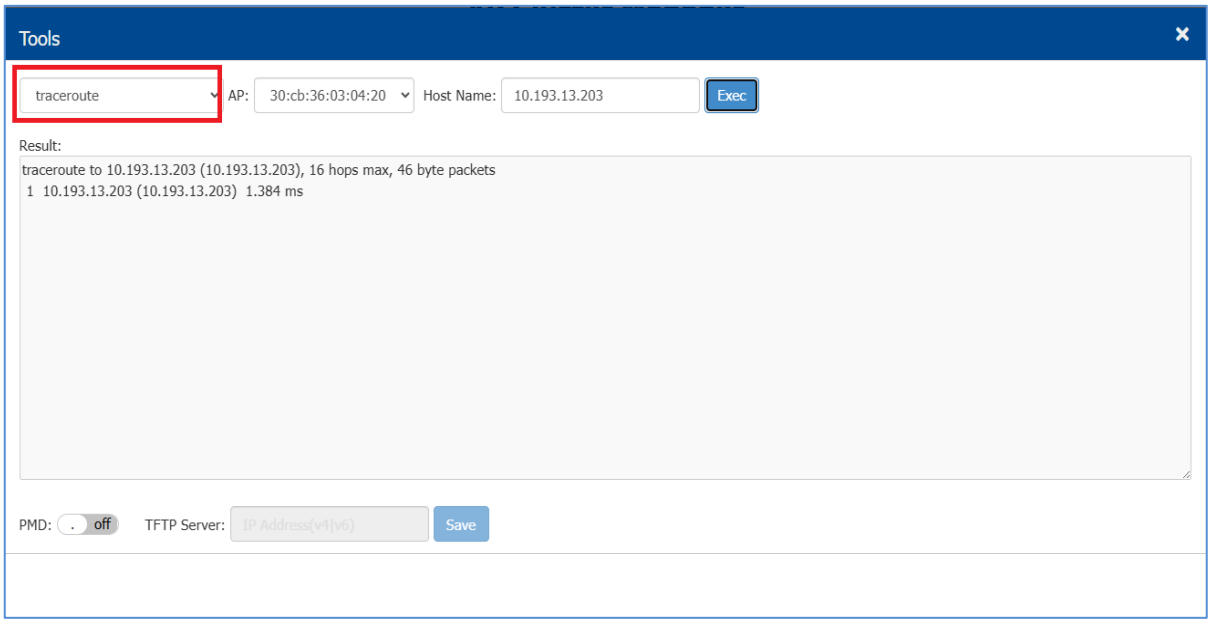


图 180：Traceroute

- **ping**：可以在 DAP849 中 ping 网络中其它主机。

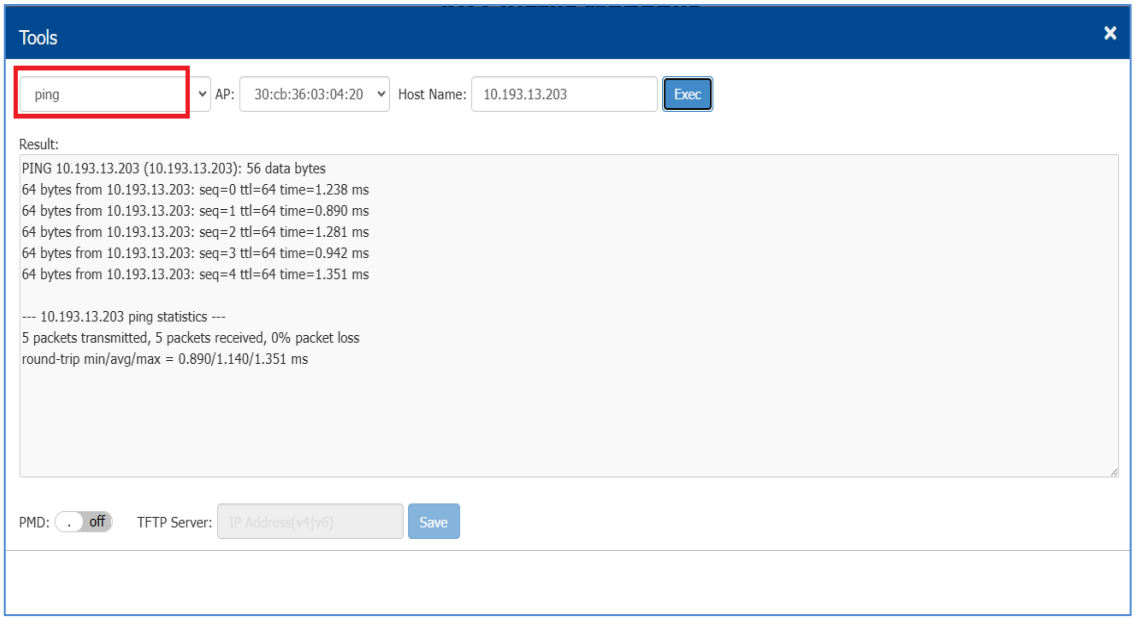


图 181：在 DAP849 上进行 ping 测试

- **show history reset reason**：显示 DAP849 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 182。

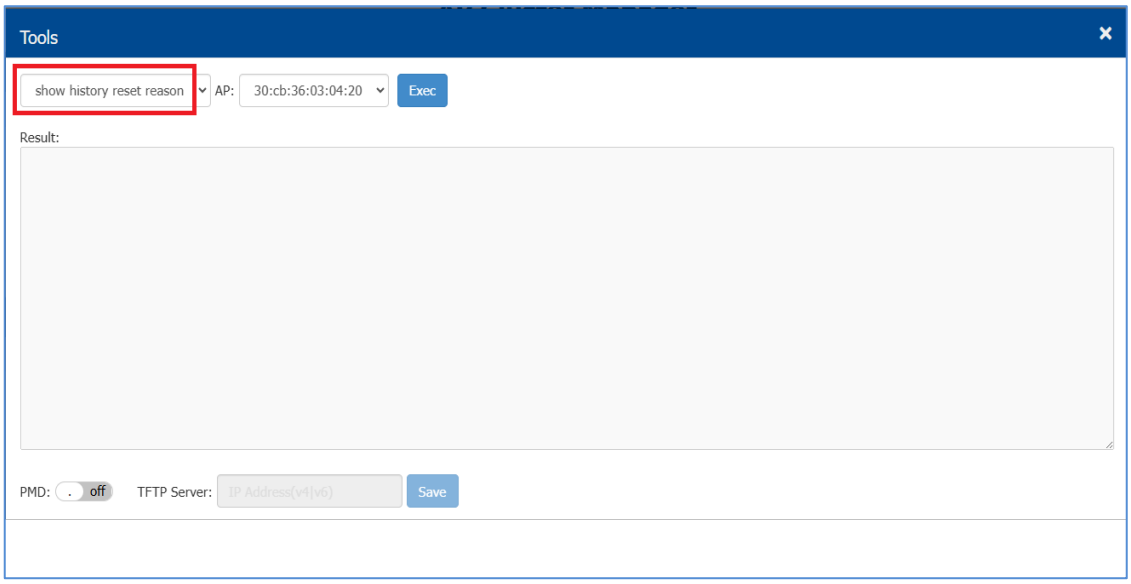


图 182：显示历史重启原因

- **AP log collection**：收集 DAP849 的 log 文件，支持通过 TFTP 及 HTTP 的方式下载，参考图 183 和图 184。

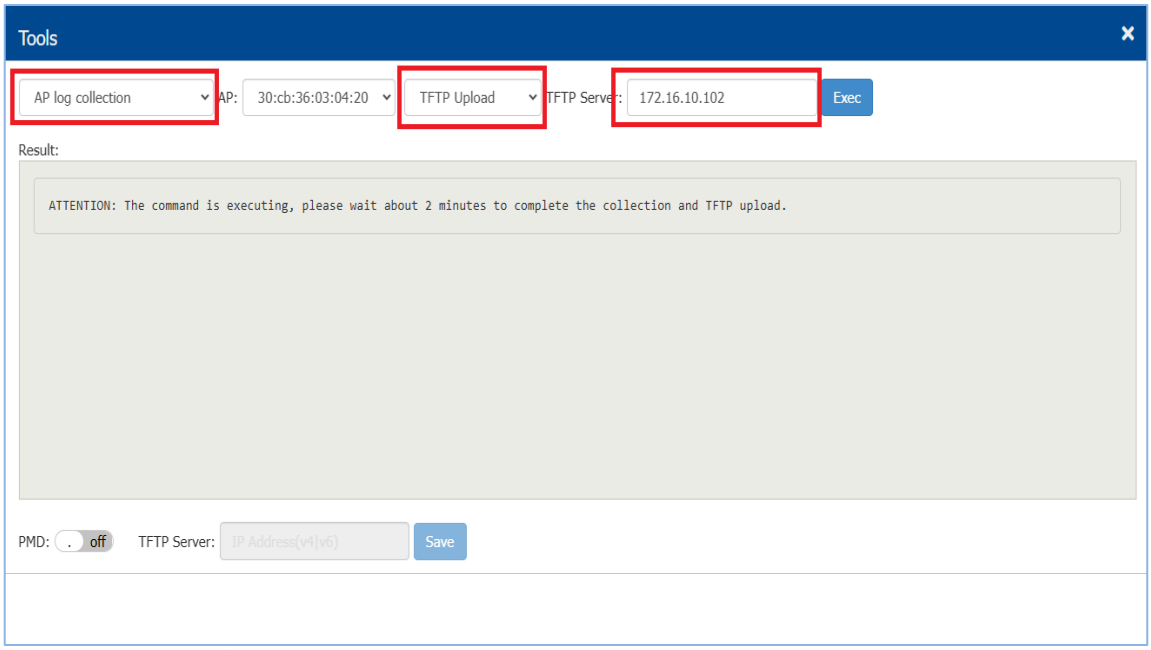


图 183：使用 TFTP 收集日志

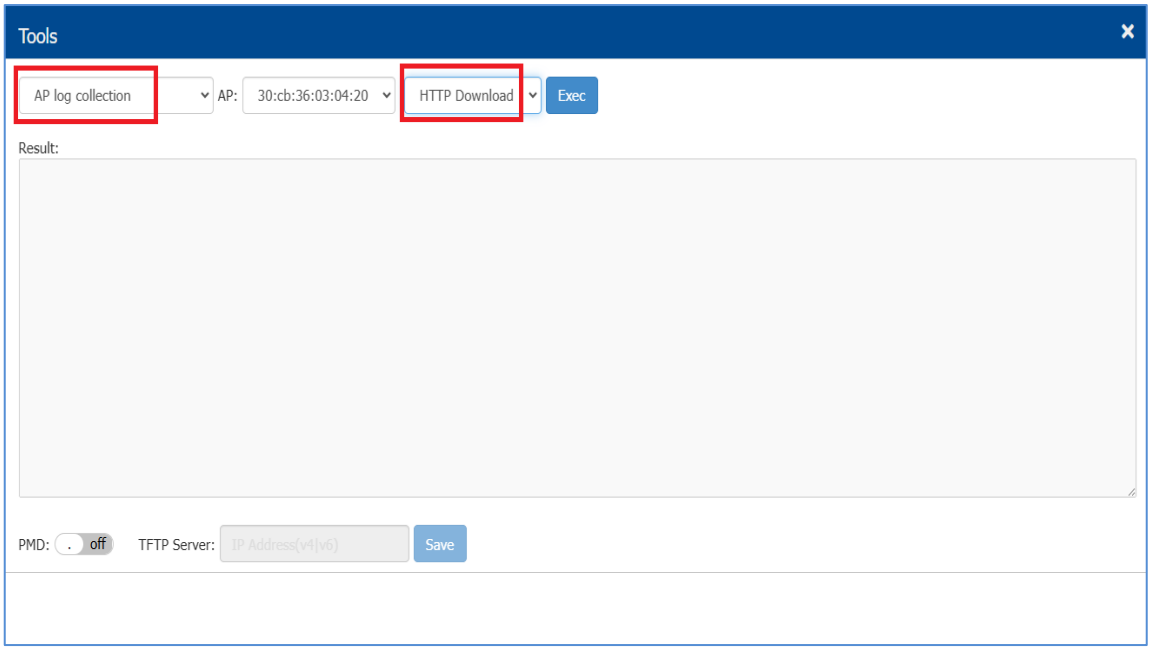


图 184：使用 HTTP 收集日志

- **show channel utilization**：显示 2.4G 及 5G 信道的利用率，参考图 185。

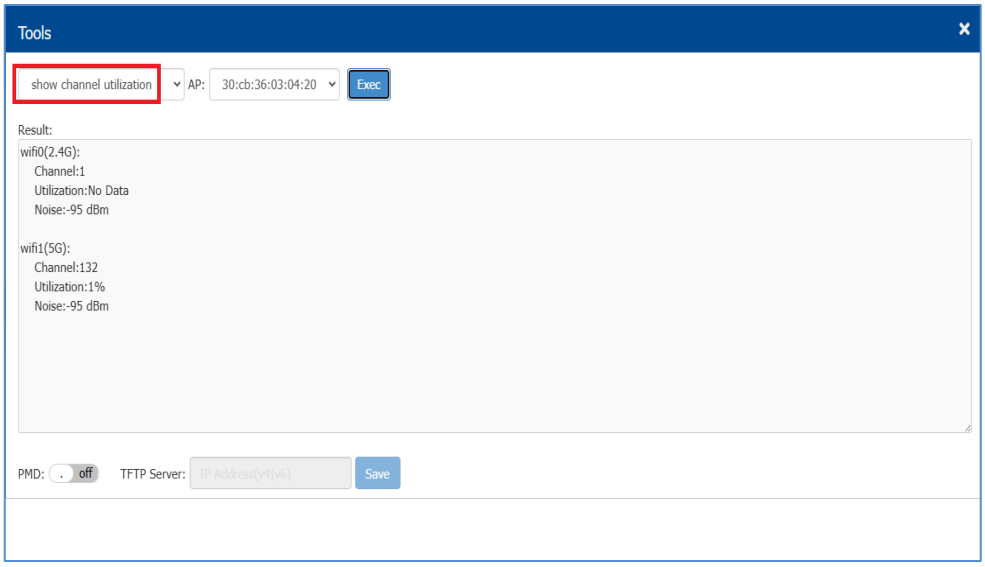


图 185：显示信道利用率

12.2 PMD

Post Mortem Dump（PMD）是 DAP849 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 DAP849 上出现关键进程崩溃时，DAP849 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。

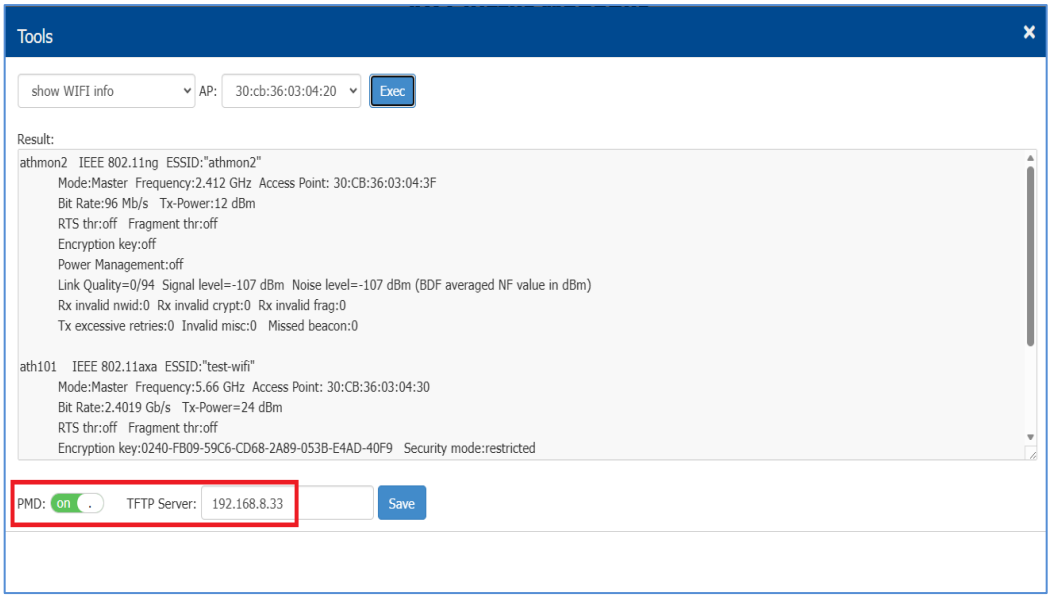


图 186：PMD 配置

13 部署大规模 DAP849 网络系统

对于一些大规模的部署场景，如果您的 DAP849 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 DAP849 所连接交换机端口的默认 VLAN，将 DAP849 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 DAP849 群集设置不同的集群 ID，即使将 DAP849 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 DAP849 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 或 BWO 模式

将 DAP849 部署为 DAC 或 BWO 模式，该模式下能够支持多达 4000 台 DAP849 的集中管理，详细操作步骤，请参阅《DAC 用户手册》或《BWO 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，DAP849 的配置方法。

■ 场景 1：DAP849 无法连接到 DHCP 服务器

如果集群中的 DAP849 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 DAP849 设备，可能会导致该网络中存在重复的 IP 地址，这种情况下 DAP849 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 DAP849

如果在网络中没有 DHCP 服务器的情况下需要配置一台 DAP849，可以按照如下步骤完成配置：

- ☐ 将 DAP849（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 DAP849 组成一个集群，只需将 DAP849 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
BWO	Belden Wireless Orchestration	Belden 无线编排器
CLI	Command-Line Interface	命令行界面
CTS	Clear To Send	清除发送
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	延迟传输指示消息
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