HIRSCHMANN IT

A BELDEN BRAND

用户配置手册

Dragonfly Access Controller（无线控制器）

修改历史

版本	日期	描述
	08/2023	增加功能：SNMP 和天线配置

您可登录Hirschmann IT产品网站https://catalog.belden.com获取本手册的最新版本。

目录

安全指南

安全位置

设备需放置在安全、稳定、可靠的地方。物理运营商必须获得授权。操作CLI脚本应妥善保管、更新和审查。

安全通道

Hirschmann IT设备支持多种管理方式，包括SSH，HTTP，和HTTPS。不推荐使用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

本“配置”用户手册为您提供了开始操作设备所需要的信息。本手册会逐步引导您，从首次启动操作到在用户操作环境中进行基本设置。
本“配置”用户手册适用于 DAC 1.1.5.6005 及更高版本。

关于DAC

DAC 是一种简单易用的即插即用无线局域网控制软件，用于管理 DAP。部署无线网络可以使用路由跨网段连接或通过局域网连接。DAP 可以安装在一个独立 Site（站点），或分别部署在多个分散的地理位置。
DAC UI 提供一个基于 Web 的标准界面，用于配置和监控 Wi-Fi 网络。DAC UI 可以通过以下浏览器从远程管理控制台或工作站访问：

- ► Microsoft Internet Explorer 11或更高版本
- ► Apple Safari 6.0或更高版本
- ► Google Chrome 23.0.1271.95或更高版本
- ► Mozilla Firefox 17.0或更高版本

如果使用不支持的浏览器打开 DAC UI，系统会弹出一则警告信息，并列出推荐使用的浏览器列表。用户也可点击登录页面的继续登录链接进行登录。

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
Link	交叉引用链接
注：	强调一项重要事实或引起相关性重视的一则提示。

1 DAC 设置

本章介绍如何在DAC上注册DAP。本章包含下列主题：

- ► 系统要求
- ► DAC安装
- ► DAC升级
- ► 在DAC上注册DAP

1.1 系统要求

DAC运行在虚拟机（VM）里，所需资源的要求如下表所示：

AP/客户端	配置	硬盘
50 个 AP+1000 个客户端	4 核 CPU+16GB 内存+1TB 硬盘	读：1.7Gbit/s 写：134Mbit/s
256 个 AP+5000 个客户端	8 核 CPU+16GB 内存+1TB 硬盘	
500 个 AP+10000 个客户端	12 核 CPU+32GB 内存+1TB 硬盘	
1000 个 AP+20000 个客户端	24 核 CPU+32GB 内存+1TB 硬盘	

表 1：配置要求

具体系统要求，请参阅DAC安装指南第2.1章“在虚拟机上安装”。

1.2 DAC 安装

具体安装过程，请参阅 DAC 安装指南。安装完成后，可登录 DAC。默认账户名称是 admin，默认密码是 Admin@01。首次登录时，安全考虑建议修改默认密码。

1.3 DAC 升级

具体升级过程，请参阅DAC安装指南第4章“安装”。

1.4 在 DAC 上注册 DAP

当DAP连接到有线网络时，DAP需在DAC上进行注册，以便由DAC进行管理。有两种方法可以在DAC上注册DAP：

- ► 通过DHCP选项发现DAC
- ► 从DAP网站配置DAC IP地址

1.4.1 通过 DHCP 选项发现 DAC

如果AP从DHCP服务器接收到Option 43，Sub-Option 1，AP将启动并连接到DAC进行管理。配置DHCP服务器时，Option 43和Sub-Option 1（01:0C:31:39:32:2E:31:36:38:2E:32:32:2E:31）表示192.168.22.1。

01	**0C**	**31**	**39**	**32**	**2E**	**31**	**36**	**38**	**2E**	**32**	**32**	**2E**	**31**
Sub-Option 1	IP 地址长度，0C=12	1	9	2	.	1	6	8	.	2	2	.	1

表 2：DHCP 服务器配置

1.4.2 从 DAP 网站配置 DAC IP 地址

在DAP设置向导中，您可选择DAP的管理模式：集群或DAC。选择DAC，即可设置DAC IP地址。
有关更多信息，请参考DAP用户手册设置向导章节。

2 DAC 入门指南

本章是DAC的基本概述，包含下列主题：

- ► 使用默认帐户admin登录
- ► 使用向导开始
- ► 网络结构
- ► 账户管理
- ► 管理员权限

2.1 使用默认帐户 admin 登录

登录DAC设备。默认账户名称是**admin**，默认密码是**Admin@01**。首次登录时，建议修改默认密码。

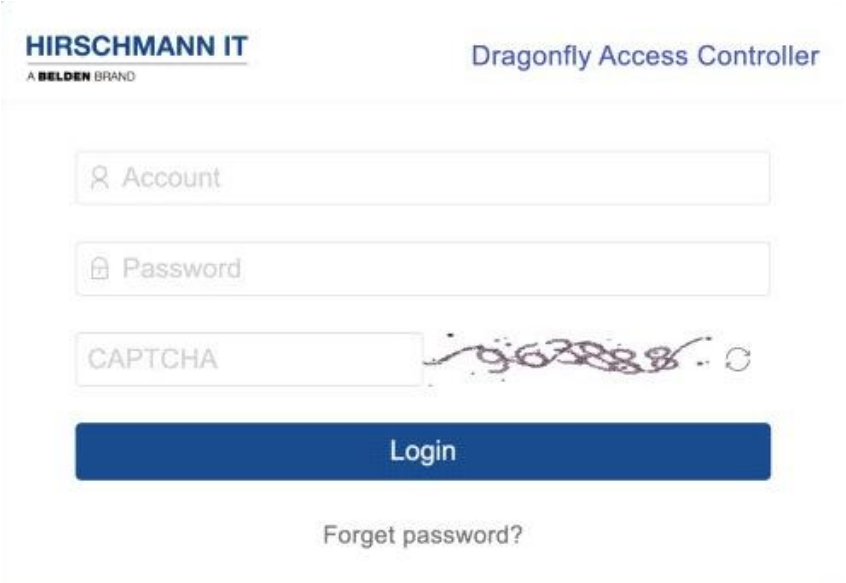


图 1：DAC 登录

2.1.1 修改 admin 账户的默认密码

使用admin账户登录DAC。点击导航栏的人像图标，点击“**Personal setting**”，进入“**Personal settings**”页面，然后点击“**Change password**”。

打开“**Change password**”对话框后，可修改您的密码。

- ► Old password：当前使用的密码。
- ► New password：填入新密码。
- ► Confirm Password：再次填入新密码。

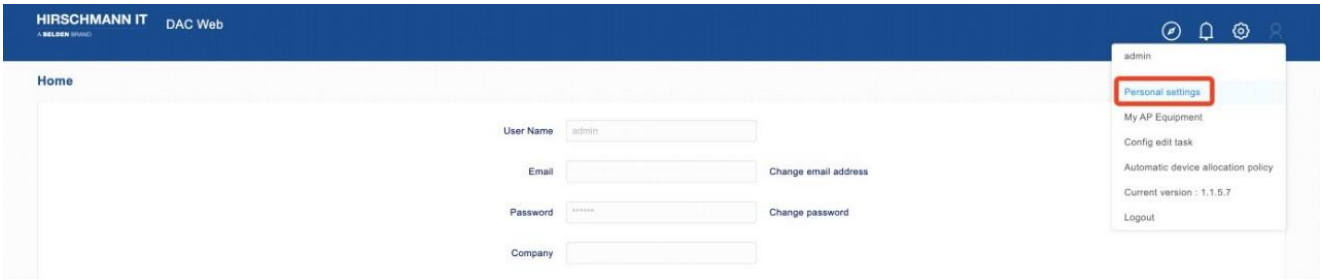


图 2：修改密码

2.2 使用向导开始

首次使用 **admin** 账户登录 DAC 时，系统会要求通过向导进行配置。您可选择“**yes**”进入向导程序或选择“**cancel**”跳过向导程序。您也可点击导航栏的 **wizard** ⊘ 图标进入向导程序。在向导程序中，完成下列步骤：

2.2.1 搭建无线网络架构

根据您公司的组织架构，搭建无线网络结构。
DAC为网络架构管理提供三层式结构。

- ► Site（必选）
- ► Group（可选）
- ► Corporate（可选）

Site 是最基础的结构，提供最丰富的网络配置。同时，您可以将部分 DAP 从 Site 分配给 Group。Group 不仅沿用了 Site 大部分的配置，而且提供一些特殊配置的功能。将 Site 添加到 Corporate 可以帮助管理 Site 和分配统一的权限。您可以根据业务需要，将 Site 映射到园区大楼。也可以将 Site 映射到公司办公网络，用 Group 为特定部门（如安全性要求更高的财务办公室）提供安全隔离的特殊配置。

更多细节，请参考网络结构。

- ■ **创建Site（必选）**

DAC定义客户应首先创建一个Site。Site是配置中的一个分发单元，是一个组织结构概念，比Group大但比Corporate小。在Site上创建的无线配置直接对Site下的AP生效，并分发到其所属的每个Group中的AP。首先，需要创建客户自己的Site，如果有组织结构划分需求，则可以在现有Site上继续创建Group。

- ■ **创建一个Group（可选）**

Group是无线配置分配的最小单位。Group需要一个能满足用户需求的主Site结构。根据设计，Group可以拥有自己的无线配置，并继承主Site的无线配置，具有很高的灵活性。

■ **创建一个Corporate（可选）**

Corporate是最大的单位。当客户的实际组织结构覆盖多个Site时，通过Corporate的概念可以实现对多个Site的统一管理。

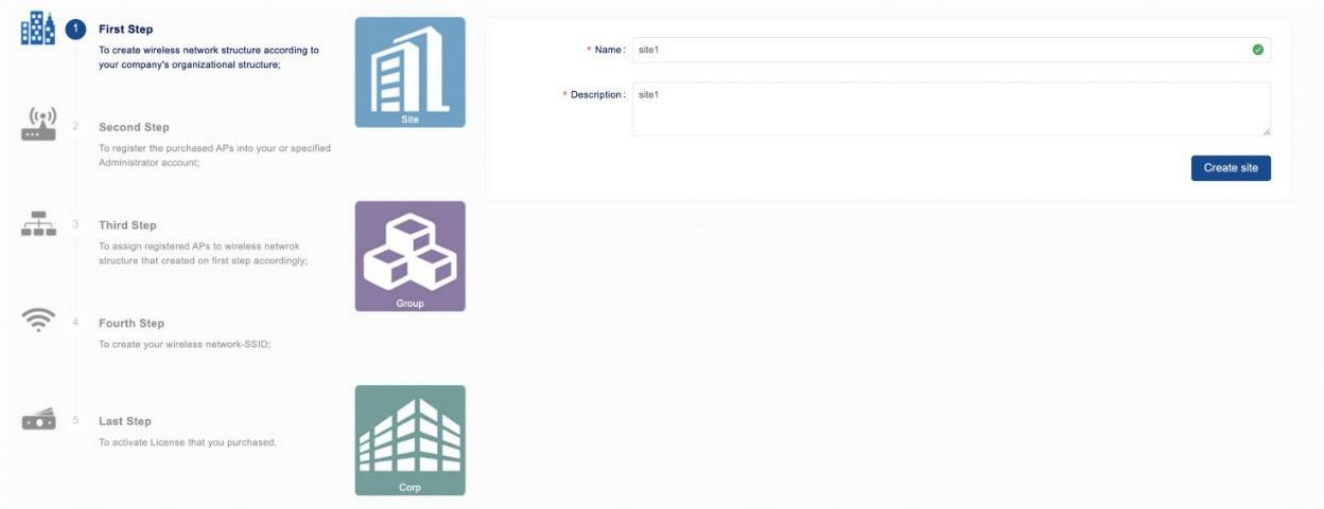


图3：第一步向导配置

2.2.2 注册 AP

将已购买的AP注册到您或指定的管理员帐户中。
这一步不是必需的。在DAC上首次注册DAP时，会自动绑定到管理员账户。

☐ 在账户下，选择要注册的AP。
☐ 填入AP的“**MAC**”和“**SN**”将其添加到帐户中。

注意：AP和DAC网络可以相互通信。此外，我们还提供更便捷的功能，如“自动录入具有相同网关的AP”和“集群添加”。其中，“集群添加”的功能是建立在“自动录入具有相同网关的AP”的基础上的。

■ **自动录入具有相同网关的AP**

当客户在自己的网络上批量部署AP无线网络时，位于默认网关后面的AP设备可以使用此功能。此功能可以一次完成批量录入，并在录入框下显示AP列表。

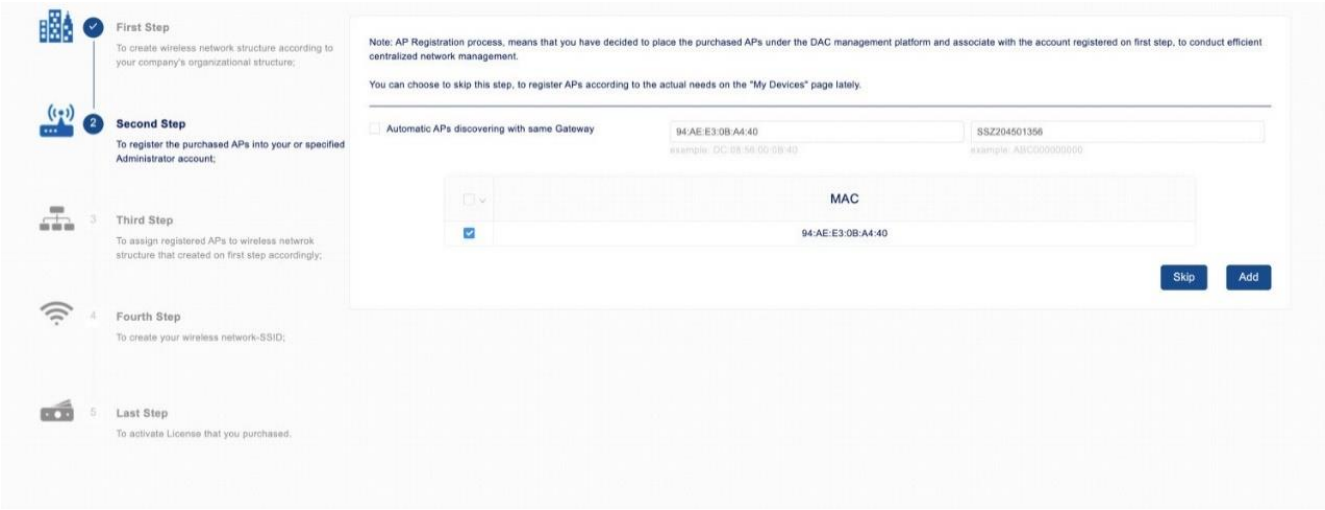


图 4：第二部向导配置

2.2.3 分配已注册的 AP

根据第一步创建的无线网络结构，将已注册的AP分配到相应的位置。

- ☐ 在设置向导的第三步中，为Site或者Site下的Group选择AP设备。
- ☐ 点击“**Next step**”按钮。

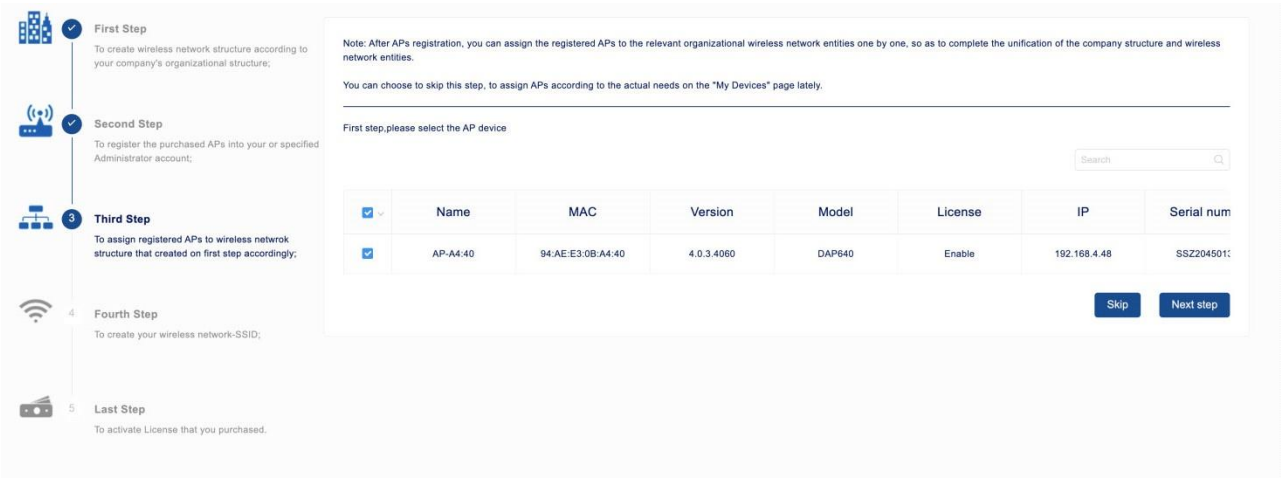


图 5：第三步向导配置

- ☐ 选择“**Site**”或“**Group**”来分配AP。

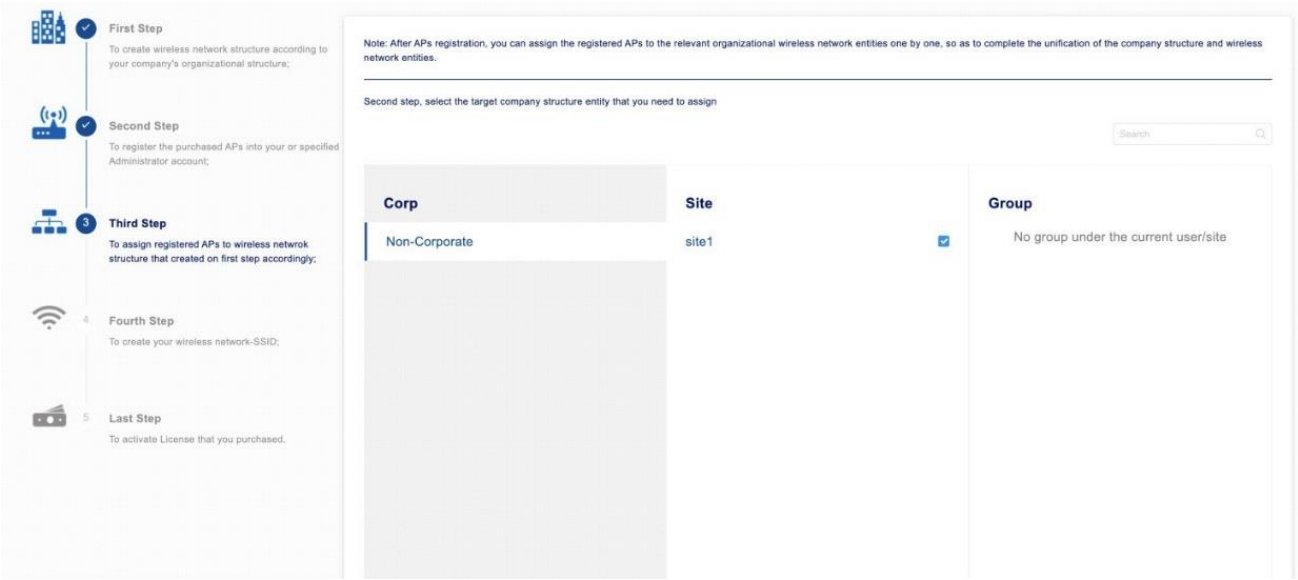


图 6：选择要分配 AP 的 Site

2.2.4 创建 WLAN

基于Site或Group创建WLAN。您需要选择Site或Group来创建WLAN。请参阅第95页的“WLAN”。

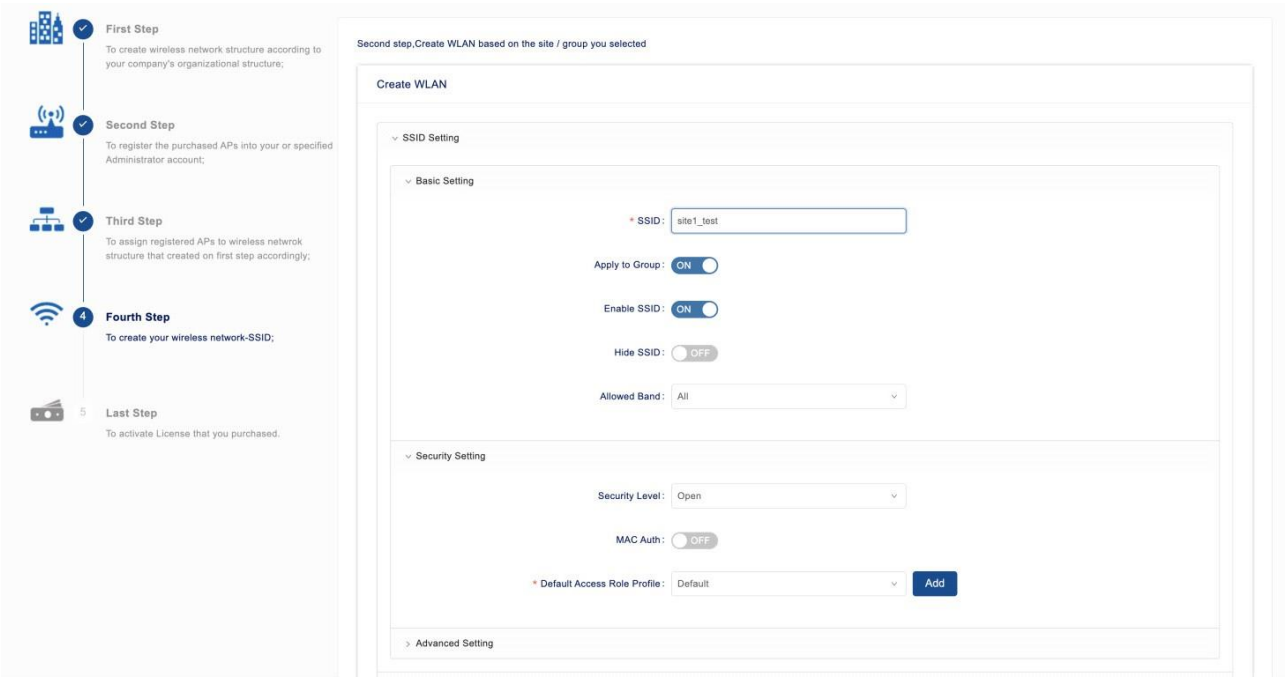


图 7：第四步向导配置

2.2.5 激活购买的许可证

设置向导的最后一步是激活许可证。

☐ 填入许可证代码并点击“**Activate**”按钮，启用许可证。

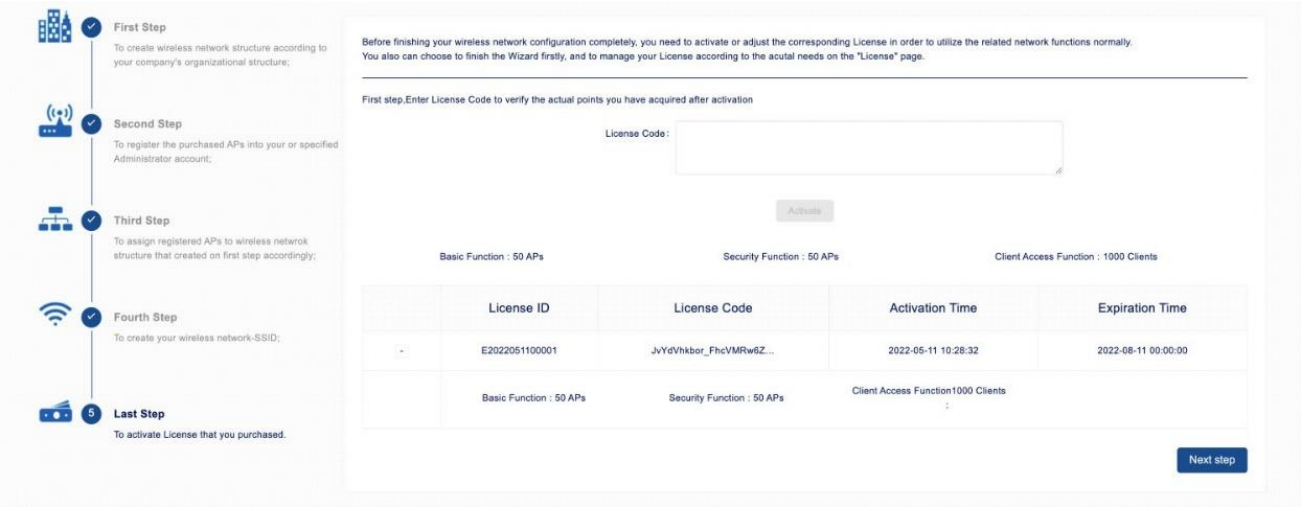


图8：最后一步向导配置

2.3 网络结构

企业的内部组织通常不是完全扁平的，而是分为不同的区域或子网。对于拥有许多分支机构或连锁店的企业来说，需要进行独立管理网络。此外，需要将不同权限的管理员分配给各分支机构或商店，以便进行网络维护。DAC为解决这些情况提供了机制。

DAC通过Corporate（可选）、Site（必选）和Group（可选）级别的关系来管理企业网络结构。在向导中，我们已经建立了相应的网络结构。本节介绍如何从用户仪表盘创建相应的管理对象。

只有“**admin**”账户可以创建和维护这些网络结构。

- ► **Site**：Site是提供最丰富网络配置的基本结构。
- ► **Group**：Group从属于Site，只能由Site创建。Group不仅沿用了Site大部分的配置，而且具备特殊配置的能力。
- ► **Corporate**：Corporate是一组Site。将Site添加到Corporate可以帮助您管理Site并分配统一的权限。

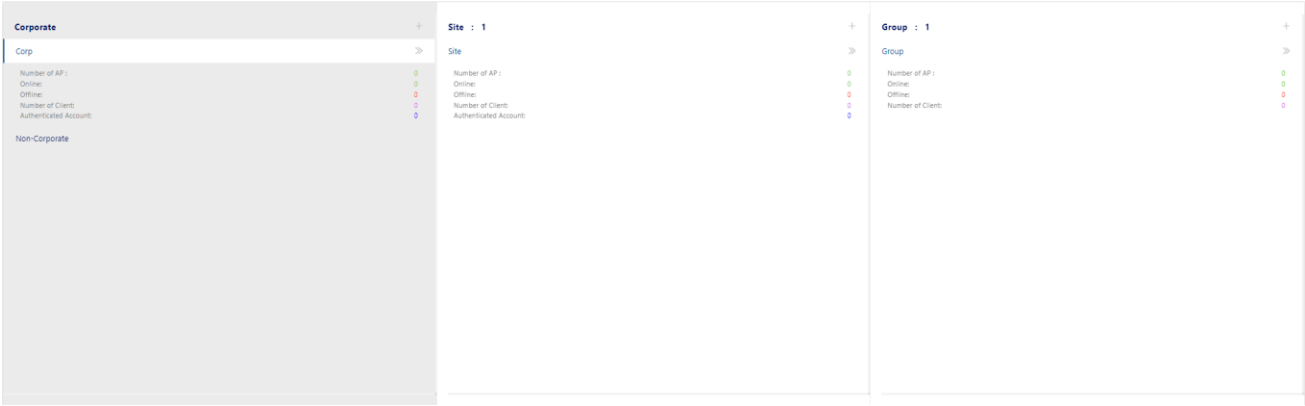


图 9：网络结构

2.3.1 创建新的 Site

☐ 在用户仪表盘页面上，点击“**Site**”选项卡上的“**+**”图标，打开“**Create Site**”窗口。

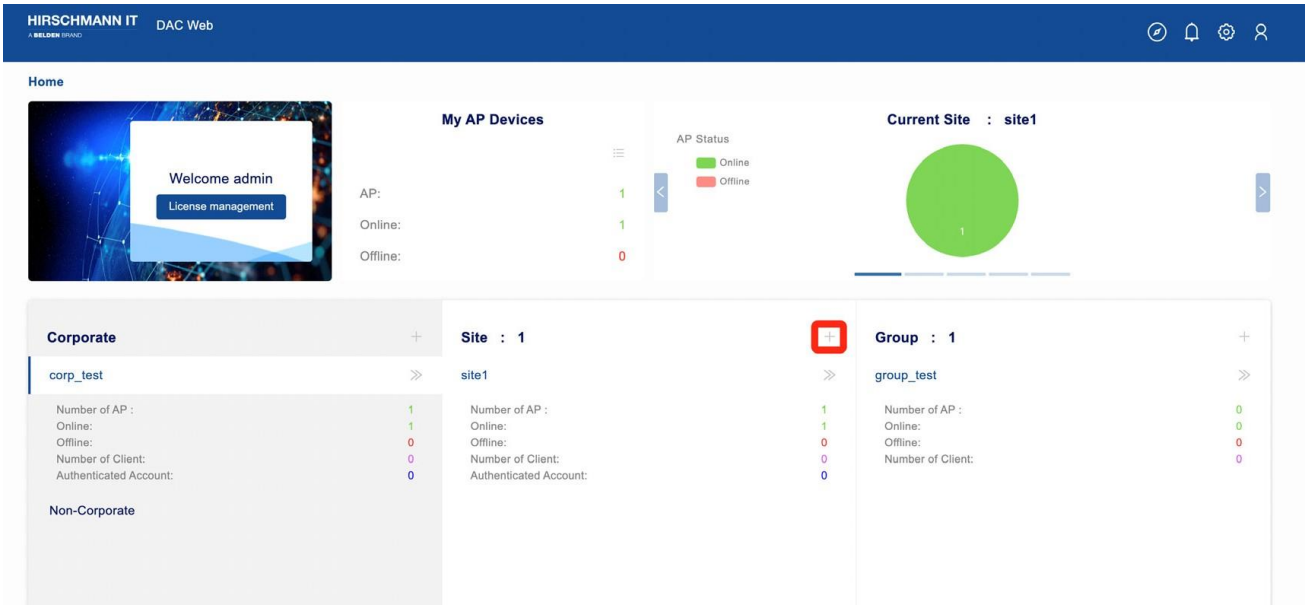


图 10：创建新站点

- 填入“**Name**”和“**Description**”字段。
- 点击“**Save**”应用设置。您可以在用户仪表盘的“Site”选项卡上看到新创建的Site。

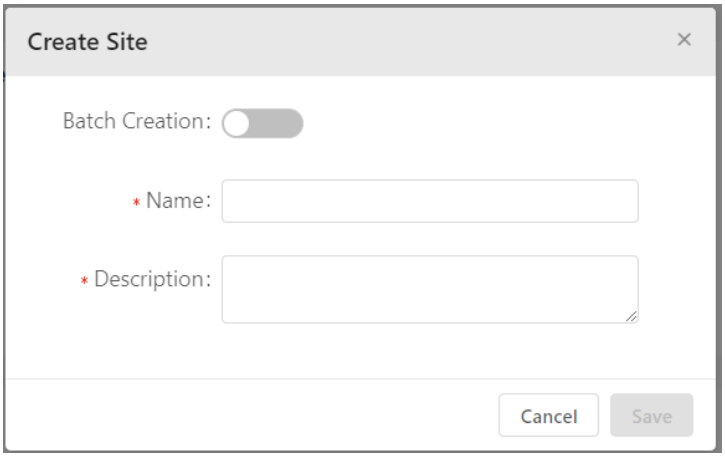


图 11：Create Site 窗口

- 如果要批量创建Site，请启用“**Batch Creation**”开关。
- 填写需要创建的Site数量，最多64个。

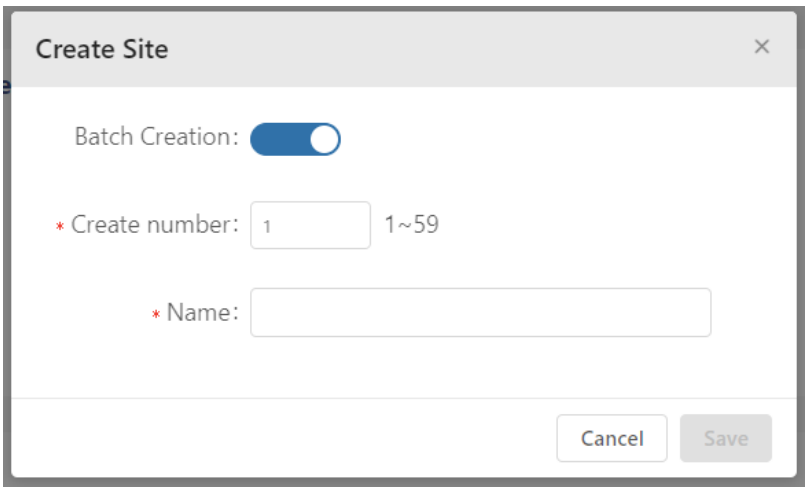


图 12：批量创建 Site 窗口

注意：每个用户最多可以创建64个Site。如果您已经有其他Site，则批量创建的Site总数为64减去已创建的Site数。

2.3.2 创建新的 Group

- ☐ 在用户仪表盘页面上，选择要添加Group的Site。
- ☐ 在“**Group**”选项卡上点击“**+**”图标。

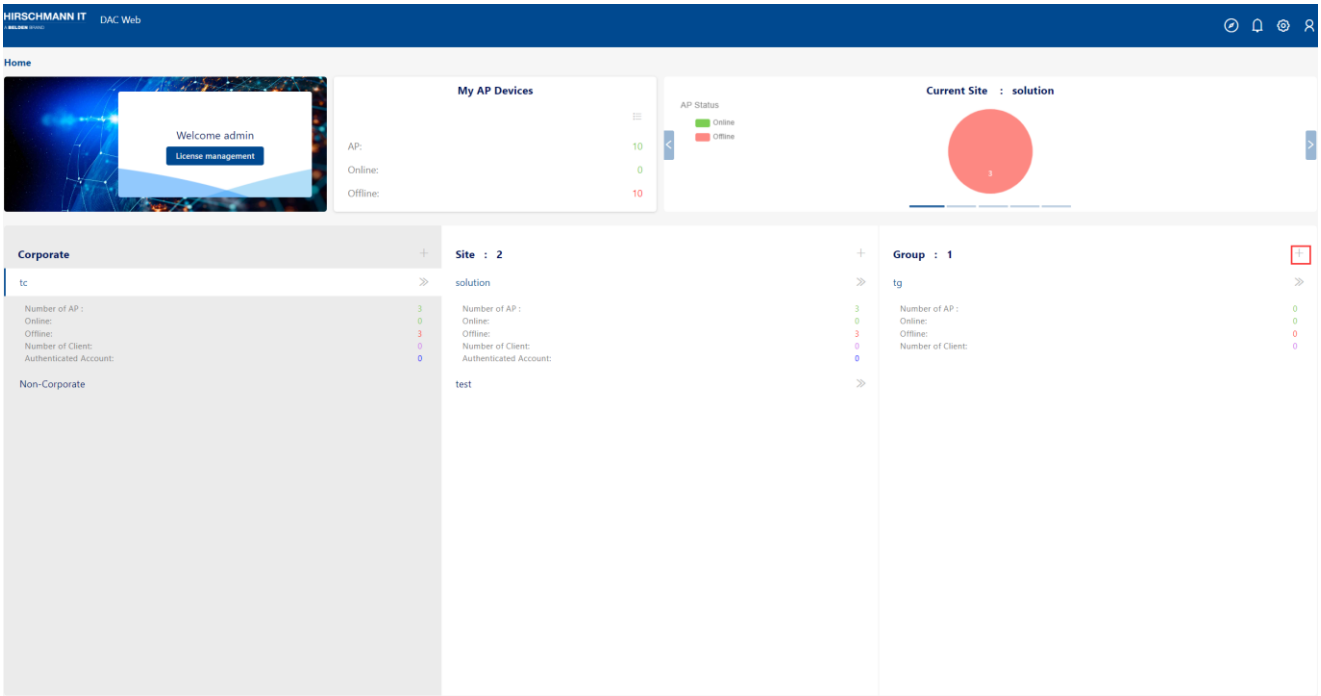


图 13：创建新的 Group

- ☐ 点击“**Add Group**”，打开“**Create Group**”窗口。
- ☐ 填入“**Name**”和“**Description**”字段。
- ☐ 点击“**Save**”应用设置。您可以在用户仪表板的“**Group**”选项卡上看到新创建的Group。

图 14：Create Group 窗口

2.3.3 创建新的 Corporate

- ☐ 在用户仪表盘页面上，点击“**Corporate**”选项卡上的“**+**”图标，打开“**Create Corporate**”窗口。

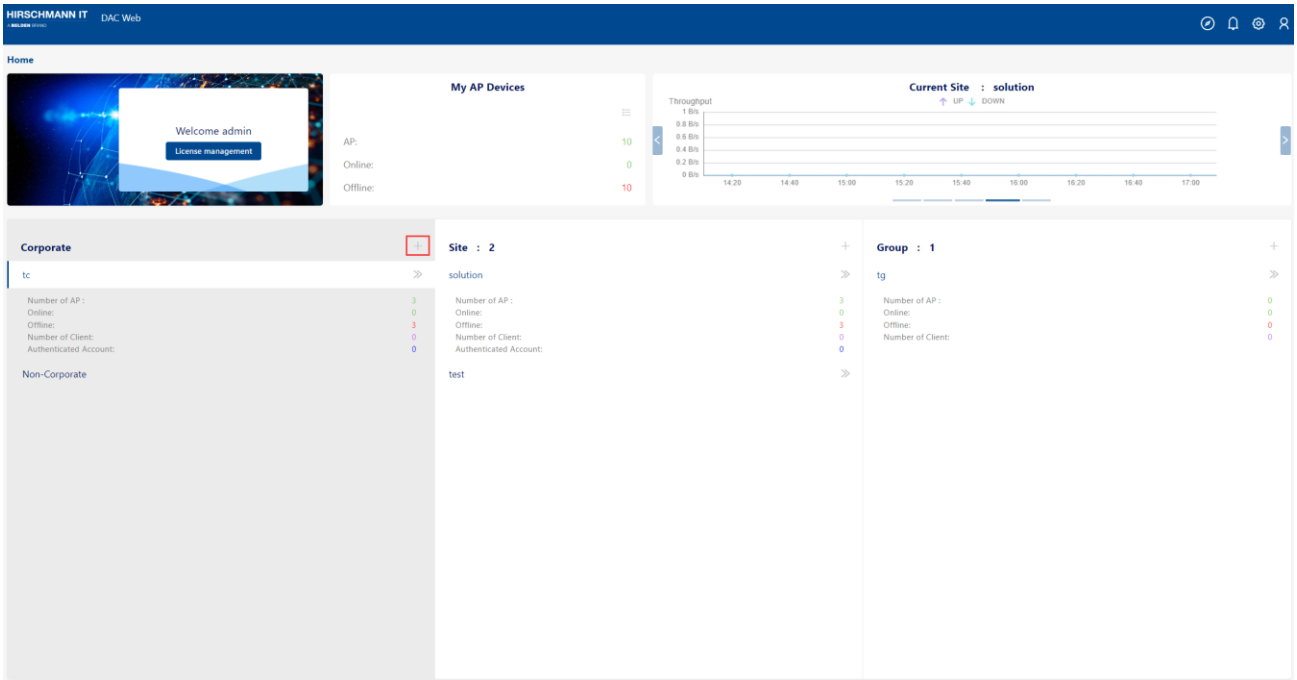


图 15：创建新的 Corporate

- ☐ 填入“**Name**”和“**Description**”字段。
- ☐ 点击“**Save**”应用设置。您可以在用户仪表盘的“**Corporate**”选项卡中看到新创建的Corporate。

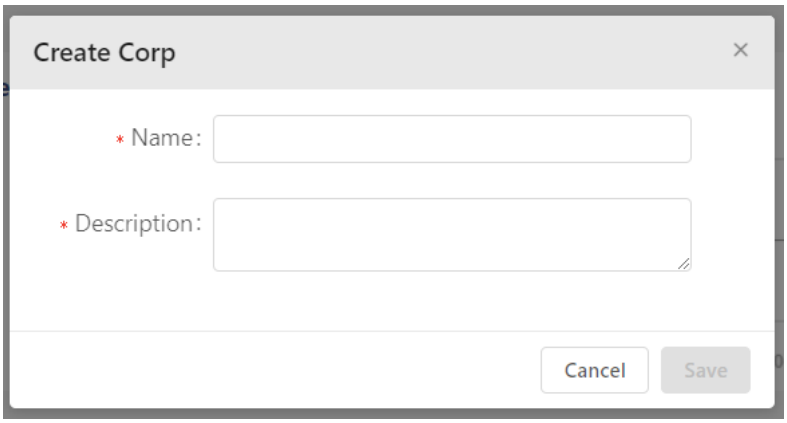


图 16：Create Corp 窗口

2.3.4 将 Site 添加到 Corporate

一个Site只能加入一个Corporate。如果一个Site已经加入了一个Corporate，应先将它退出。

- ☐ 在Site视图中打开“**Setting**”选项卡。
- ☐ 点击“**Join Corp**”，打开“**Corp information**”窗口。

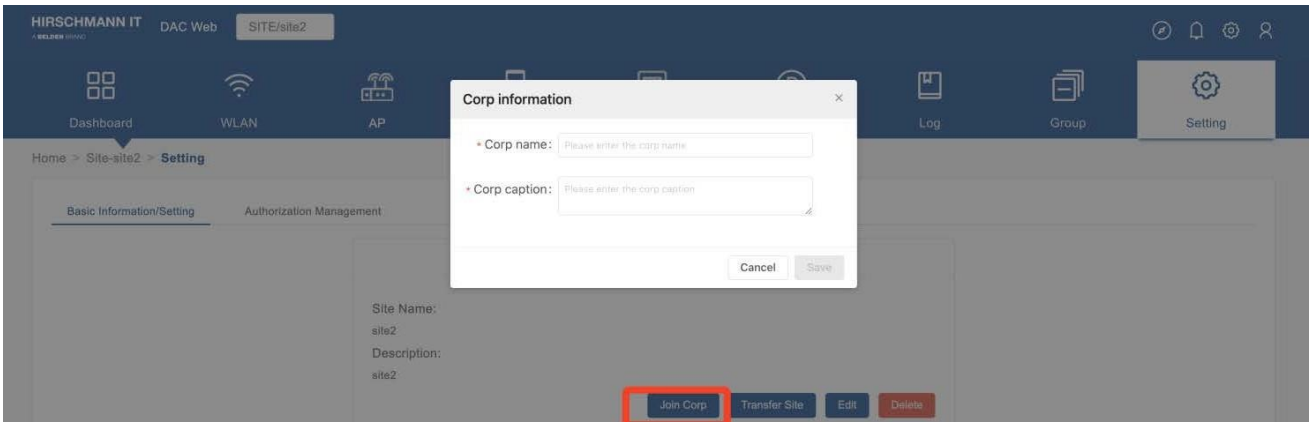


图 17：Corp 信息窗口

- ☐ 填入“**Corp name**”和“**Corp caption**”字段。请确保该Corp已存在。
- ☐ 单击“**Save**”按钮。如果加入成功，则Site的“**Setting**”视图中“**Corp Operation**”窗口打开，加入状态显示为“**InProgress**”。

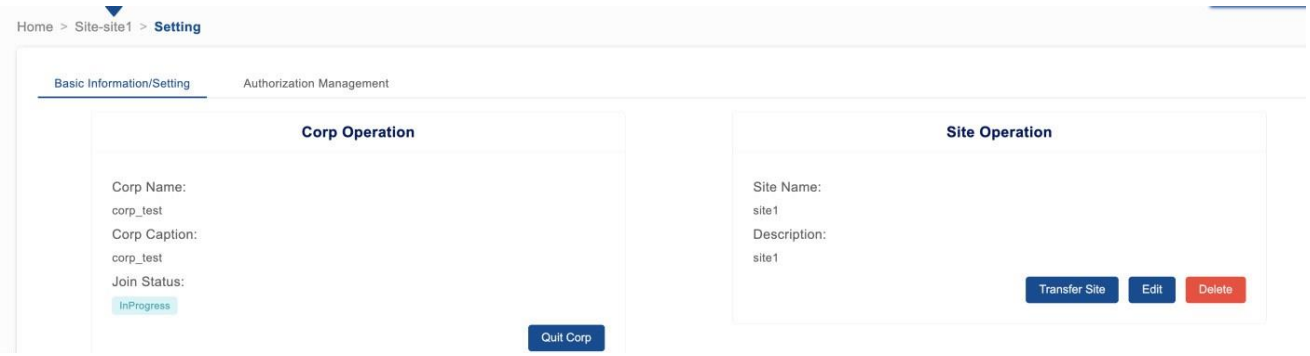


图 18：Corp 和 Site 的操作窗口

- 切换到“**Corp dashboard**”页面。“**Monitoring Panel**”弹出加入请求。
- 点击“**Accept**”同意加入请求，或点击“**Reject**”拒绝加入请求。

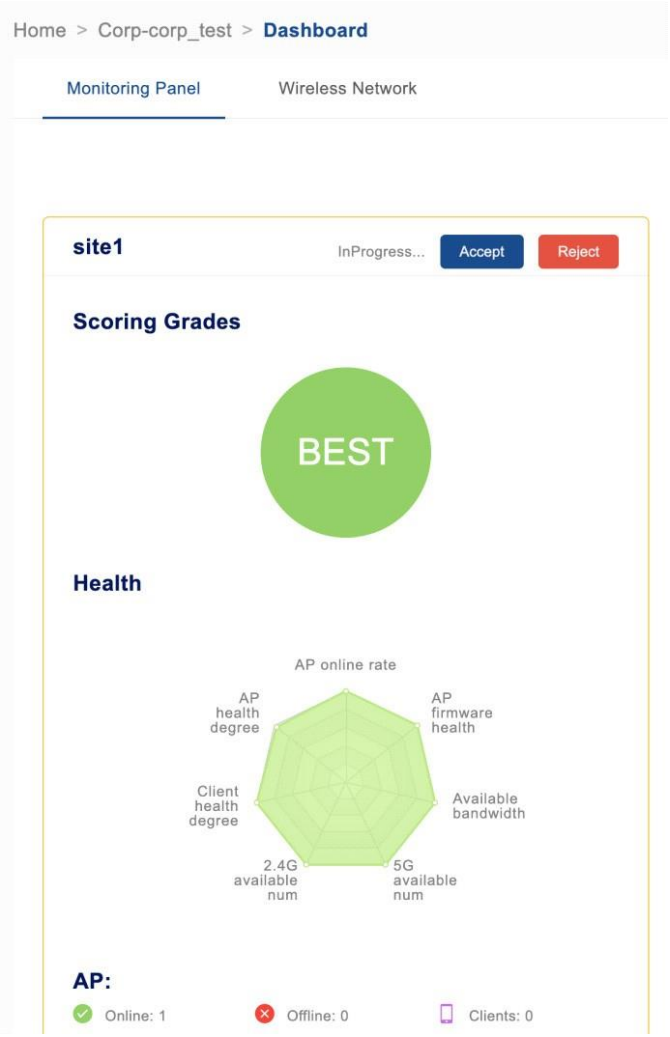


图 19：Corp 操作窗口

2.4 账户管理

DAC是一个多租户系统，可进行丰富和灵活的授权控制。作为网络管理员，您通常可以使用默认帐户“**admin**”来管理您的无线网络。但在某些情况下，您需要创建新账户并为其分配授权，以实现更灵活的网络管理。

DAC可通过“**admin**”账户发送邀请邮件来引导其他管理员完成账户注册。
为了启用DAC的帐户创建和其他功能的电子邮件通知（这些功能需要系统向外部发送电子邮件），您首先需要添加至少一个可用于从DAC发送电子邮件的SMTP服务器。

2.4.1 添加 SMTP 服务器

- ☐ 使用默认帐户“**admin**”登录。
- ☐ 在导航栏上点击“**System Configuration**”。
- ☐ 点击“**SMTP (Email) Configuration**”选项卡进入SMTP邮箱列表页面。
- ☐ 点击“**+**”图标添加SMTP服务器。

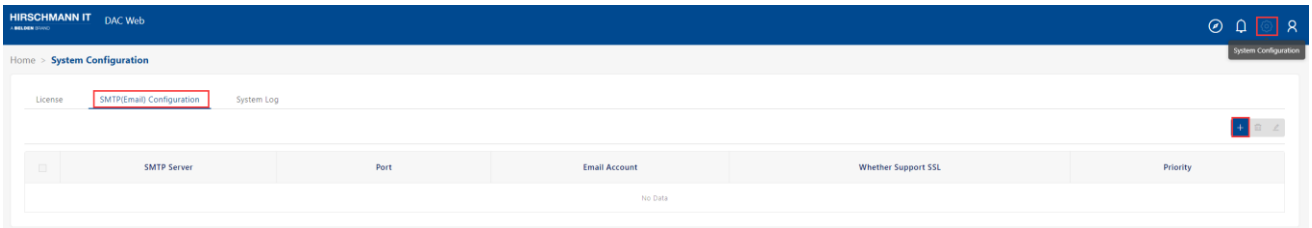


图 20：SMTP 配置

- ☐ 在添加SMTP邮箱服务器对话框中，填入以下字段：
  - ► **SMTP Server**：SMTP服务器的域名。
  - ► **Priority**：SMTP邮件服务器的优先级。最多可添加10个SMTP邮件服务器。值越低，优先级越高。如果工作邮箱由于检测到故障而无法发送邮件，则系统会尝试从优先级较低的工作邮箱发送邮件。
  - ► **Port**：SMTP服务器的端口。
  - ► **Email Account**：用于发送邮件的电子邮件帐户。
  - ► **Email Password**：邮箱密码。
  - ► **Whether Support SSL**：是否支持SSL。
    - - **Support**：使用SSL连接邮件服务器。

- **Not Support**：不支持SSL的邮件服务器，将正常连接。

► **Test Email**：用于接收测试邮件的电子邮件地址。

☐ 点击“**Email Server Test**”按钮。

DAC将发送一封测试邮件验证功能。只有在成功发送测试邮件后，“**Save**”按钮才可用。

☐ 点击“**Save**”保存工作邮箱。

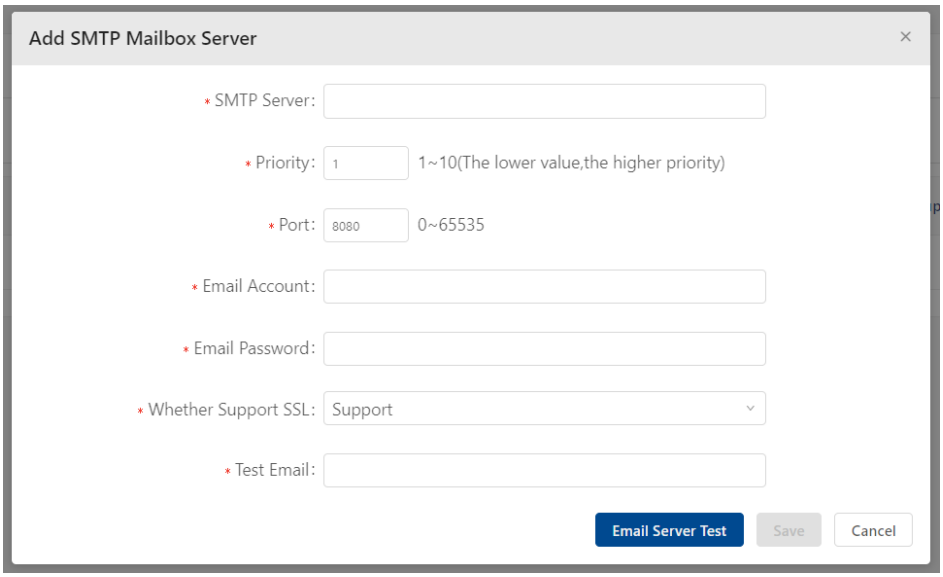


图 21：Add SMTP Mailbox Server 窗口

2.4.2 创建账户

账户创建需要通过**admin**账户的邀请完成，并且账户的授权将同时完成。

■ **发起电子邮件邀请**

☐ 在**Site**视图中打开“**Setting**”页面，然后点击“**Authorization management**”选项卡。

☐ 点击“**+**”图标，打开“**Add Administrator**”窗口。

☐ 填入要注册的帐户的“**User name/Email**”。

☐ 从下拉列表中选择一个“**Character**”定义新账户的角色。

☐ 点击“**Save**”。

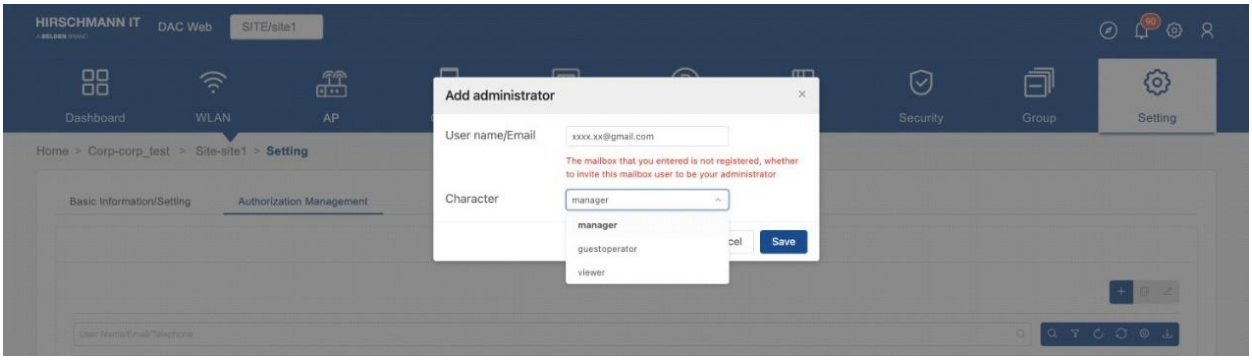


图 22：发起电子邮件邀请

■ 创建账户

☐ 登录到配置的邮箱。

☐ 点击注册链接，进入“**Invitation Registration**”页面。

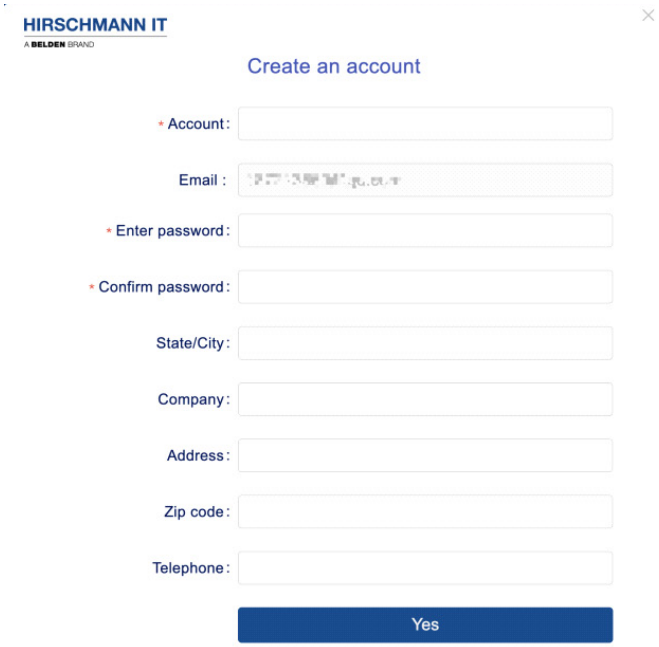


图 23：创建账户

☐ 填入以下字段创建帐户：

- ► **Account：**账户。
- ► **Email：**用于登录的电子邮件。
- ► **Enter Password：**用于登录的密码。
- ► **Confirm Password：**确认密码。

- ▶ **State/City**：省/城市。
- ▶ **Company**：公司名称。
- ▶ **Address**：公司地址。
- ▶ **Zip code**：公司邮政编码。
- ▶ **Telephone**：电话号码。

2.4.3 修改密码

登录设备后，可以修改密码。

☐ 点击导航栏上的人像图标。

☐ 点击“**Personal settings**”，打开“**Personal setting**”页面。

☐ 点击“**Change password**”，打开“**Change password**”对话框。

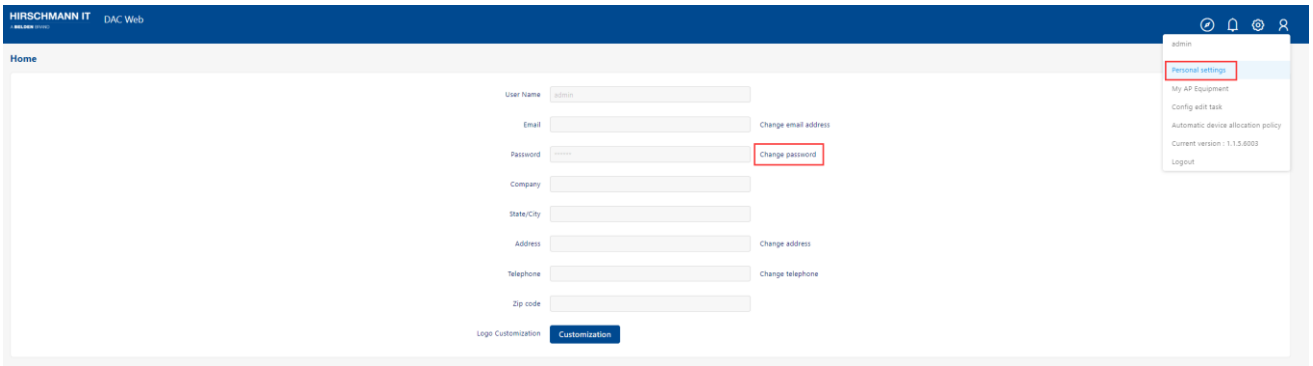


图 24：Personal settings

☐ 填入以下字段修改密码：

- ▶ **Old password**：当前使用的密码。
- ▶ **New password**：想要设置的新密码。
- ▶ **Confirm Password**：再次填入新密码。

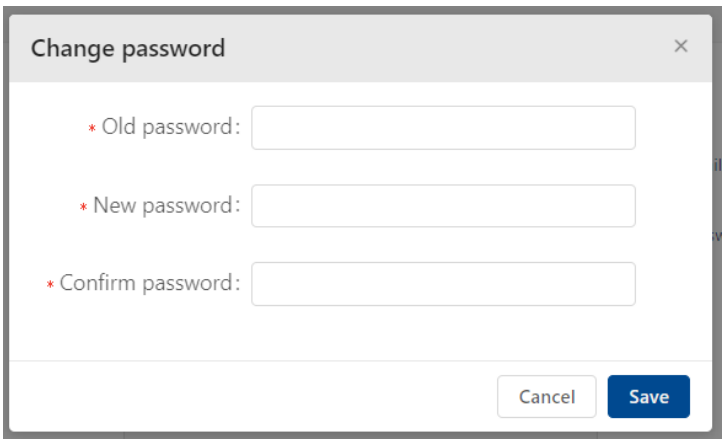


图 25：Change password 窗口

2.4.4 忘记密码

如果忘记了密码，可以选择恢复账户。

☐ 在登录页面上点击“**Forgot password**”链接，打开“**Recover your account**”页面。

☐ 填入以下字段恢复账号：

- ► **Email/Account**：填入您的电子邮件或账号。
- ► **Verification code**：填入正确的电子邮件或帐户后，点击“**Get Code**”。您会在电子邮件中收到一个验证码。
- ► **New password**：填入想要设置的新密码。
- ► **Confirm password**：确认新密码。

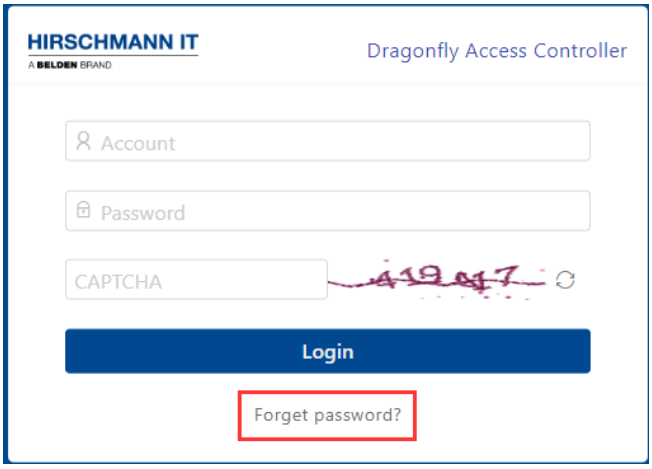


图 26：Forget password 按钮

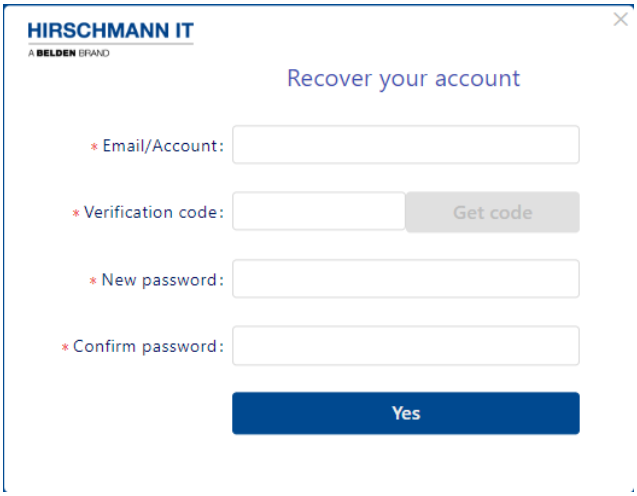


图 27：Recover your account 窗口

2.5 管理员权限

“**admin**”账户是DAC的主用户，它是AP设备、许可证和网络结构的所有者。其他用户只能通过“**admin**”账户的电子邮件邀请进行注册，成为网络的管理员。

DAC管理员可以分为以下几类：

角色	权限	访问级别
Admin	Owner	► 网络的所有者，拥有所有 AP 设备和许可证。 ► 创建网络结构并将 AP 分配给 Site。可使用管理和监控功能。 ► 可邀请其他用户，基于网络组织结构，对网络进行管理和监控。
其他用户	Manager	► 网络管理者，而不是设备和许可证的所有者。 ► 可使用管理和监控功能。
	Viewer	► 网络的观察者，而不是网络的管理者。 ► 具有监控功能的特权，但没有网络管理和配置功能的特权。
	Guest Operator	► 网络访客的管理员，而不是整个网络的管理员，也不是设备和许可证的所有者。 ► 具有网络访客管理功能。

表 3：DAC 管理员

■ admin

► “admin”账户拥有网络，包括AP设备和许可证。

► “admin”账户可以创建新的网络结构（Site、Group和Corporate）、将AP分配给除Corporate外的网络结构，也可以为其他账号分配Site和Group的管理权限。

► “admin”账户具有管理和监控功能的特权。

► “admin”账户可以发起邀请，让其他人注册账户。只有收到邀请的电子邮件地址才能在DAC上注册账户。

► “admin”账户可以邀请其他用户注册账户，并为不同的Site授予他们不同的权限。

■ Manager

如果用户在一个Site上拥有manager权限，则该用户可以使用Site的管理和监控功能。

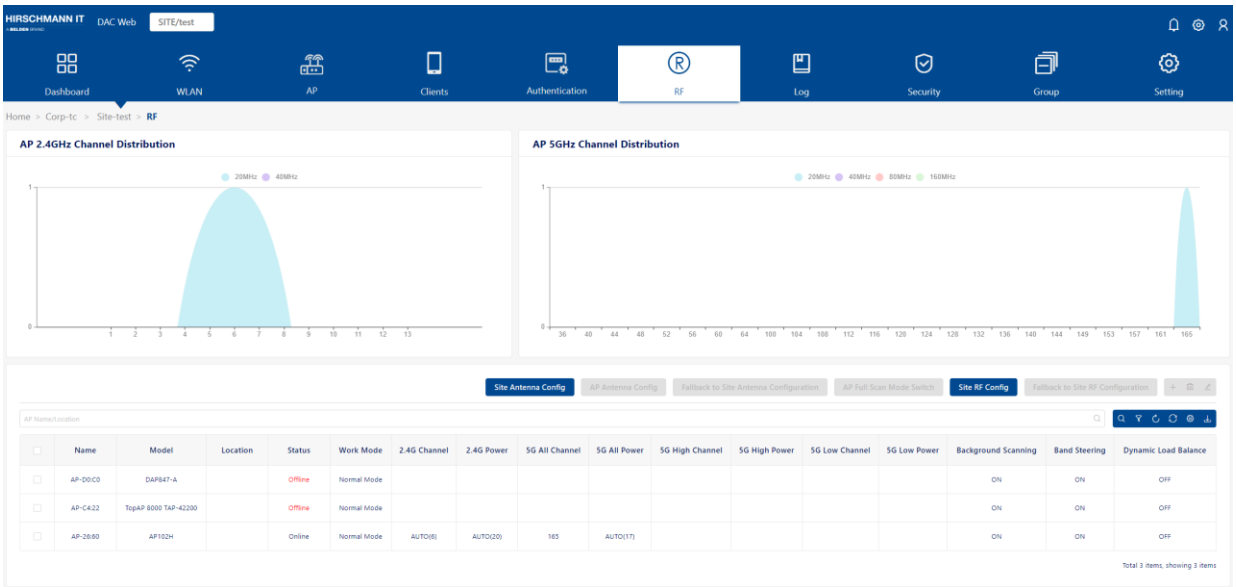


图 28：Manager 权限的 RF 页面

■ Viewer

如果用户在一个Site上拥有viewer权限，则该用户可以查看Site配置并监控Site的运行状态，但是不能添加或修改Site的配置。

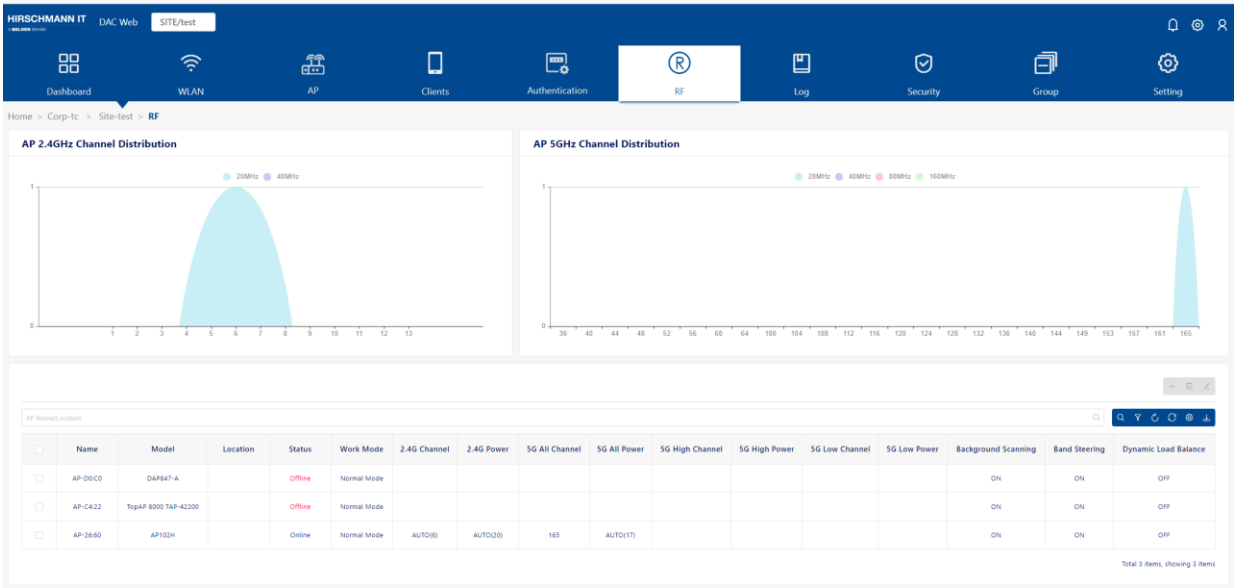


图 29：Viewer 权限的 RF 页面

■ **Guest operator**

如果用户在一个Site拥有guest operator权限，则该用户管理该Site的访客账户。

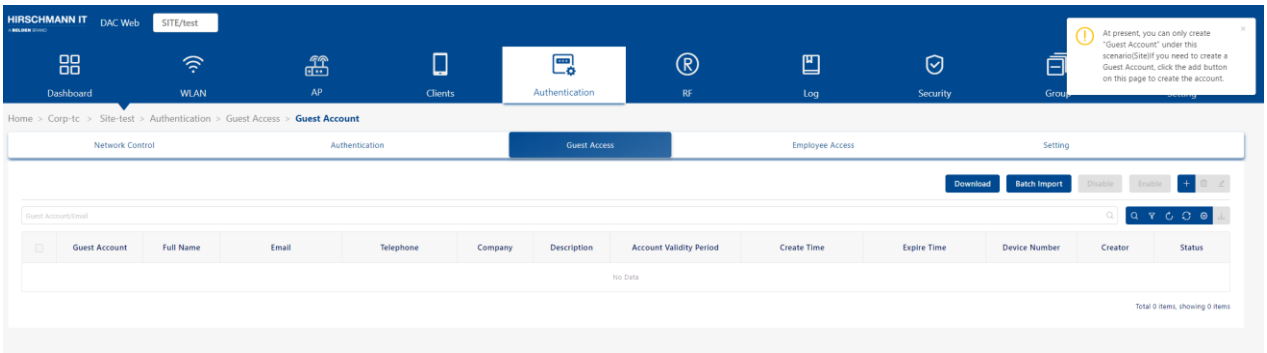


图 30：Guest operator 权限管理页面

2.5.1 添加 Site 管理员

- ☐ 在Site的“**Setting**”页面上，点击“**Authorization Management**”选项卡。
- ☐ 点击“**+**”图标，打开“**Add administrator**”窗口。
- ☐ 填入“**User name/Email**”字段。填入的用户名应存在。
- ☐ 从下拉列表中选择“**Character**”。您还可以邀请新用户来管理当前Site。请参阅第38页的“创建账户”。
- ☐ 点击“**Save**”完成授权。

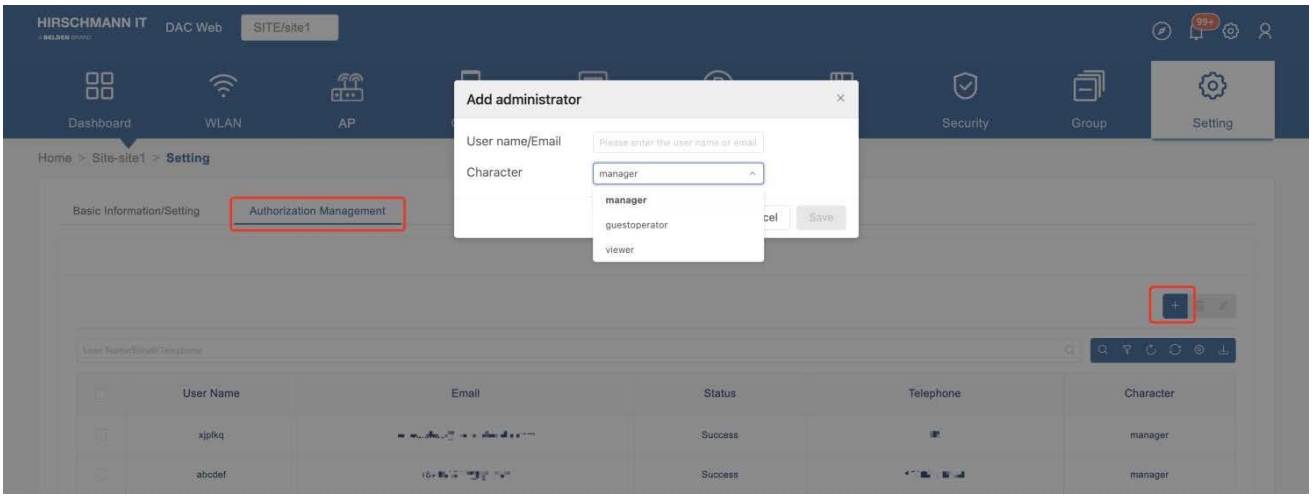


图 31：添加 Site 管理员

2.5.2 删除 Site 管理员

- ☐ 从“Authorization Management”中选择要从列表中删除的用户。
- ☐ 单击“**Delete**”图标。
- ☐ 在确认提示上单击“**Yes**”。

3 DAC 用户界面介绍

本章介绍DAC的用户界面的基本操作，包含下列主题：

- ► 条幅工具
- ► 配置/显示器图标
- ► 使用图表
- ► 用户主页
- ► Site视图
- ► Group视图

3.1 条幅工具

条幅工具	
	向导 点击可快速进入向导模式，配置相关的网络结构及其相应的许可证激活。
	注意 点击查看用户级别相应的消息通知
	系统配置 点击可填入许可证、SMTP（电子邮件）配置和系统日志。
	常用信息 点击可快速访问个人配置和部分功能。

表 4：条幅工具

► 向导

- 点击可快速进入向导模式，配置相关的网络结构及其相应的许可证激活。请参阅第26页的“使用向导开始”。

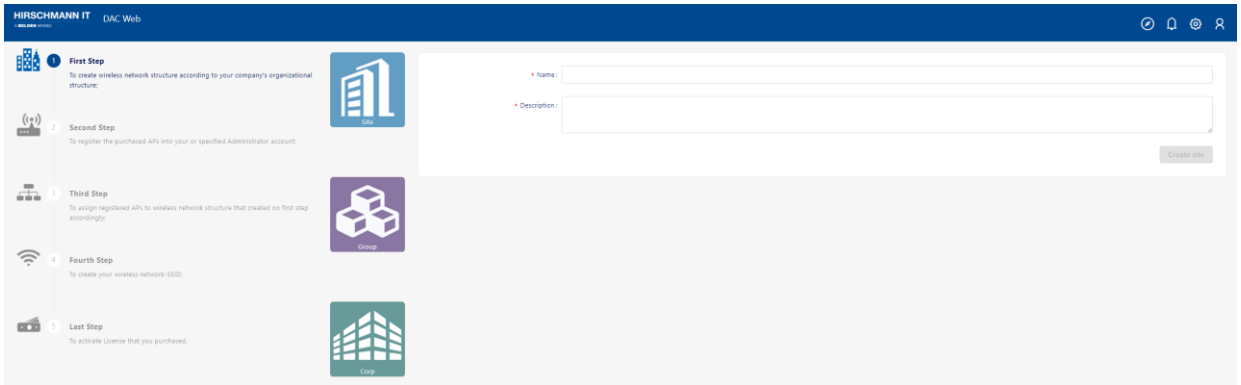


图 32：向导

► 通知

- 点击查看用户级别相应的消息通知。
- **Message**：根据账户维度显示消息通知。
- **Message Setting**：配置是否接收相关消息或发送电子邮件通知消息选项。

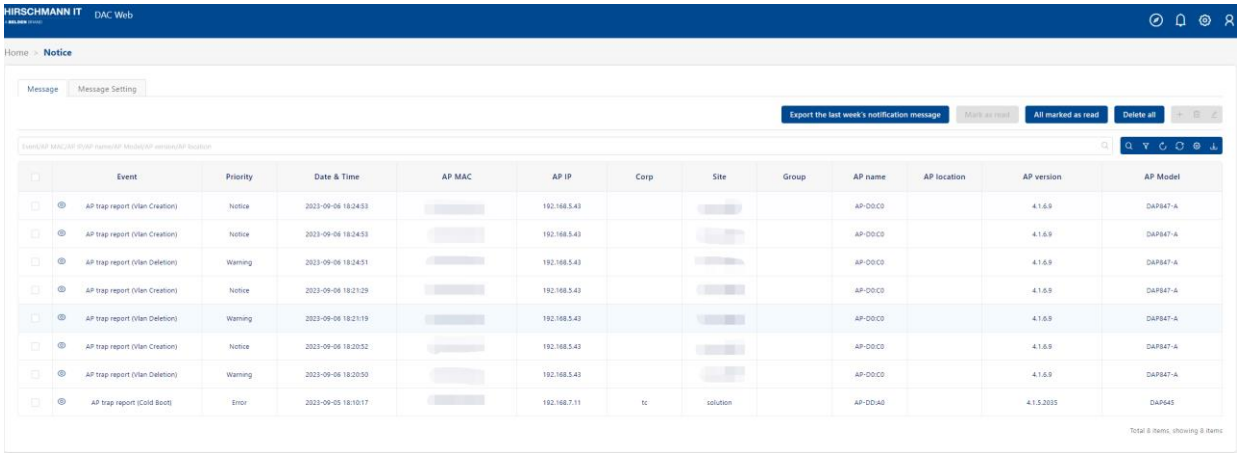


图 33：通知

注：如果配置了相关消息，只有在打开Site的日志模块后才会生成相应的消息信息。如果Site的日志模块未打开，则不会生成基于Site的消息信息。

► 系统配置

- 可以在此处填入许可证、SMTP（电子邮件）配置和系统日志。

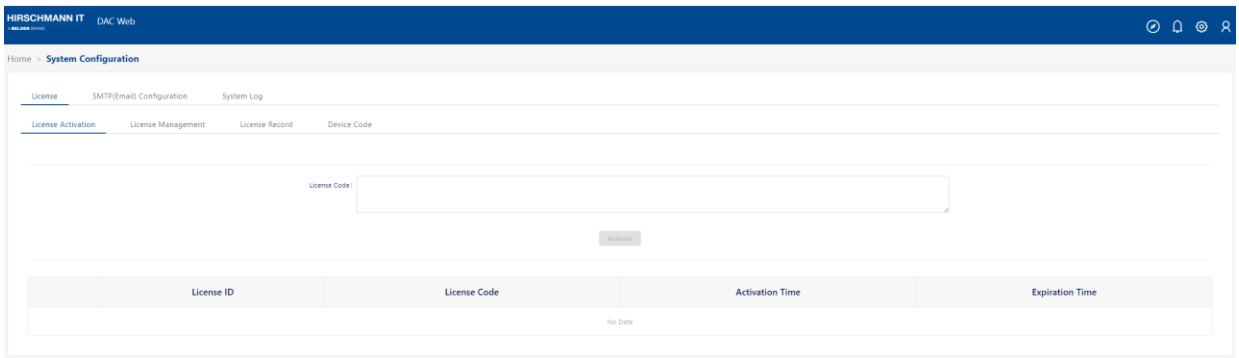


图 34：System Configuration 页面

► 常用信息

- **Personal settings：**点击进入个人信息修改页面。可以修改电子邮件、密码、地址和电话号码。
- **My AP Equipment：**点击进入我的设备页面。
- **Config edit task：**点击查看当前用户下的配置任务列表。您可以在此页面上取消或删除配置任务。
- **Automatic device allocation policy：**配置子网和Site的绑定策略。相

应的Site会自动分配AP。

- **Current version：** 点击查看DAC发布说明。
- **Logout：** 点击注销当前账户。

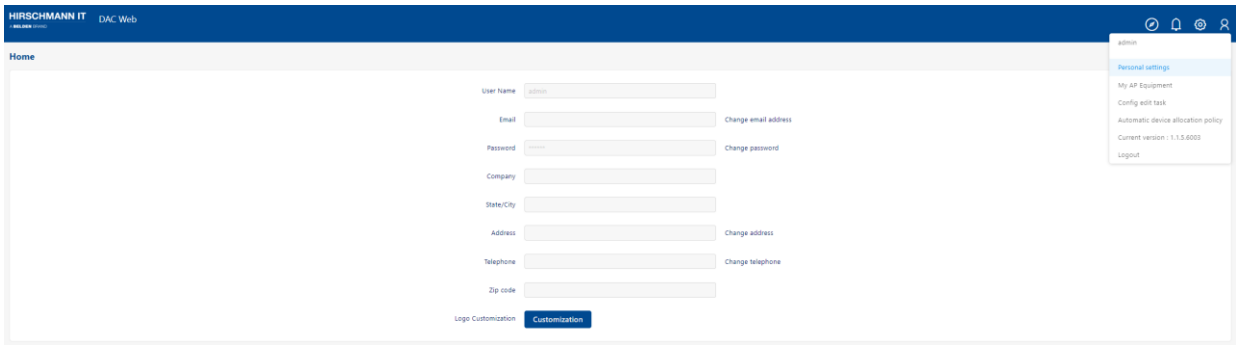


图 35：常用信息

3.2 配置/显示器图标

DAC提供与配置/显示界面交互的标准工具。这些图标/按钮包括：

配置图标/按钮	
+	**添加** 点击“**Add**”图标，在配置界面创建新条目。
	编辑 在配置界面选择条目，点击“**Edit**”，即可编辑现有条目。
	删除 选择条目并点击“**Delete**”图标，即可删除该条目。
	向导 点击可快速进入向导模式，配置相关的网络结构及其相应的许可证激活。
	注意 点击查看用户级别相应的消息通知。
	系统配置 点击可填入许可证、SMTP（电子邮件）配置和系统日志。
	常用信息 点击可快速访问个人配置和部分功能。
	帮助 点击“**help**”按钮加载相应的提示信息。

表格图标/按钮	
	搜索 点击“**Search**”按钮并在“Search...”字段中填入搜索条件，即可显示表中的特定条目。
	过滤器 用户可以设置表格的相应过滤字段以显示特定数据。
	重置 在对表格进行过滤筛选后，点击“**Reset**”按钮可返回到原始显示状态。
	刷新 “**Refresh**”按钮会加载应用程序表格、图表或列表的最新数据。
	设置 用于配置在表格中显示的列标题。 点击“**Settings**”按钮，选择您想要显示的列标题。
	导出为 CSV 文件 点击“**CSV**”按钮将表格视图中显示的信息下载为 CSV（电子表格）文件。

表格图标/按钮	
	排序 列表视图中显示的信息可以通过点击“**Sort**”按钮按字母顺序进行升序或降序排序。您还可以在表格视图中点击任何表格列顶部的上/下箭头，根据所选列对数据进行升序或降序排序。

表 5：配置/显示图标

3.3 使用图表

DAC中的信息主要以表格形式呈现。DAC中的表格有一些常见的功能/行为。每个区域的一般功能如下所述。可在Configuration/Display图标处获取每个按钮的详细信息。

图 36：DAC 信息表格

- **Configuration Options：**用于创建、编辑和删除条目（例如，创建、编辑和删除WLAN）。可在Configuration/Display图标处获取每个按钮的详细信息。
- **Display Options：**用于将表格显示从表格视图更改为列表视图，设置要显示的列，并刷新表格中的数据。可在Configuration/Display图标处获取每个按钮的详细信息。
- **Sort：**点击列顶部的箭头，根据该列的升序或降序对表格进行排序。
- **Set Lines to Display/Page in the List：**使用页面右下角的下拉列表设置列表中显示的行数。

3.4 用户主页

用户主页包括Corporate、Site、Group、设备列表、许可证和其他信息。

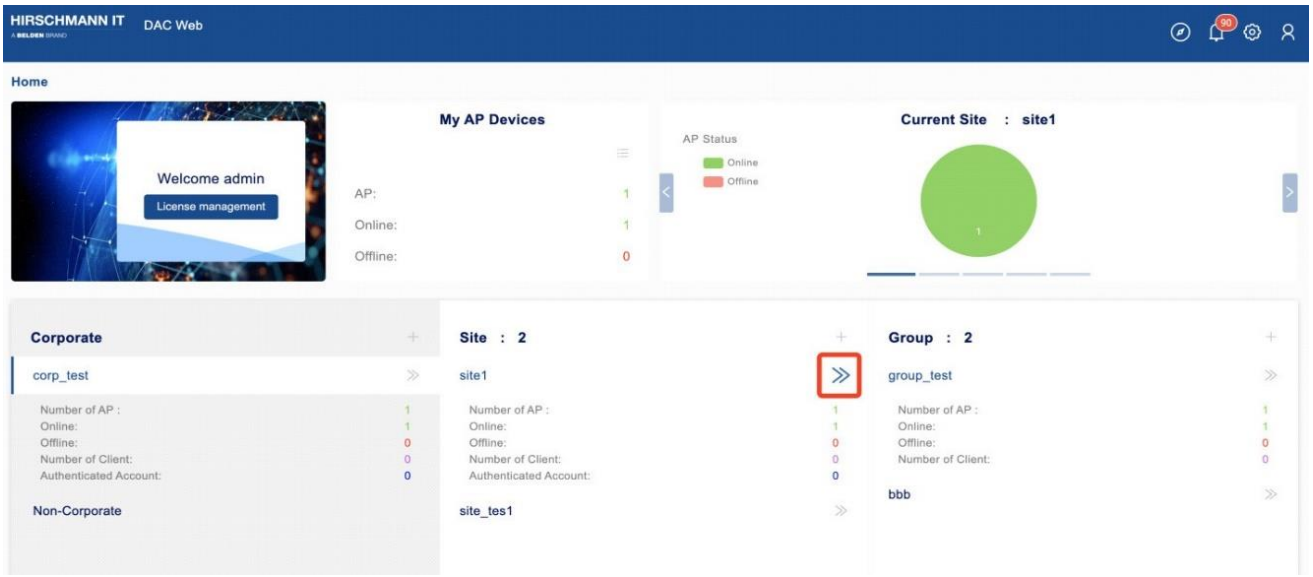


图 37：用户主页

3.4.1 首页

► **欢迎信息和许可证管理：**

登录后，客户账户会显示在此面板上。同时，该面板的选项卡还提供了“**License management**”功能的入口。

图 38：License management 功能

► **我的AP设备：**

用于监控AP的总数、在线AP的数量和离线AP的数量。点击列表图标快速进入我的设备界面。

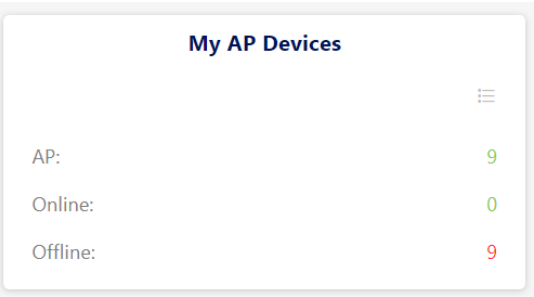


图 39：My AP Devices 界面

▶ **当前Site：**

- **AP Status：**AP状态的饼图（在线或离线数量）。

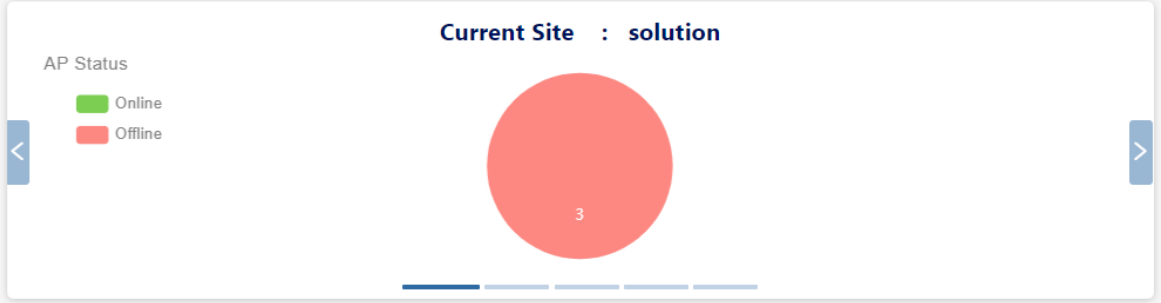


图 40：当前 Site - AP Status

- **AP Model：**AP设备的型号和数量。

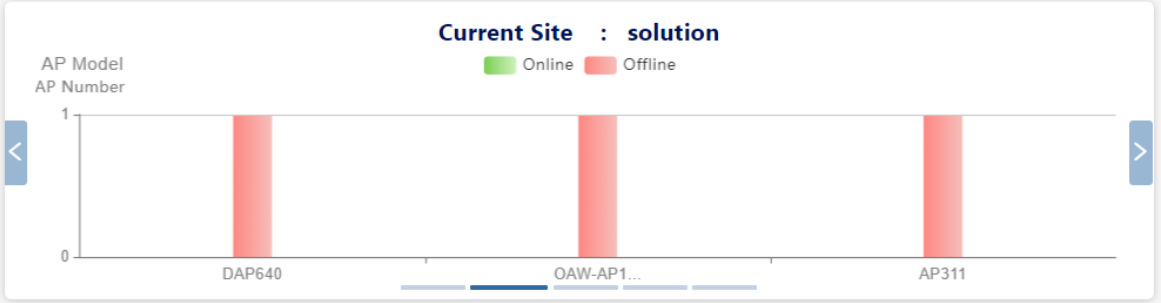


图 41：当前 Site - AP Model 和 AP Number

- **Client Number：**客户端统计。

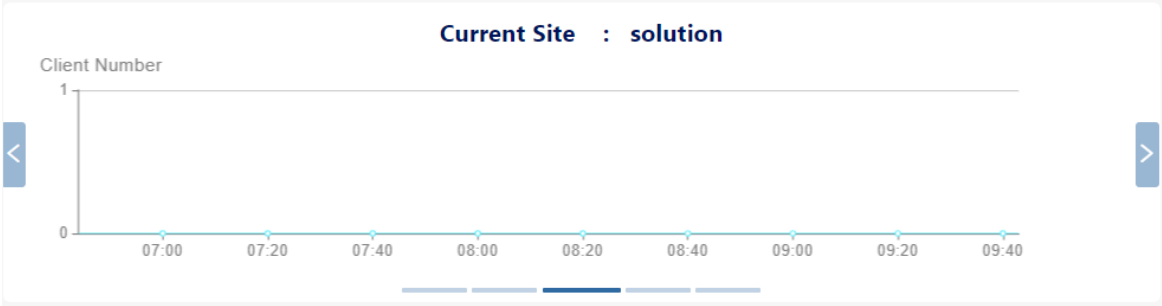


图 42：当前 Site - Client Number

- **Throughput：**带宽的折线图。

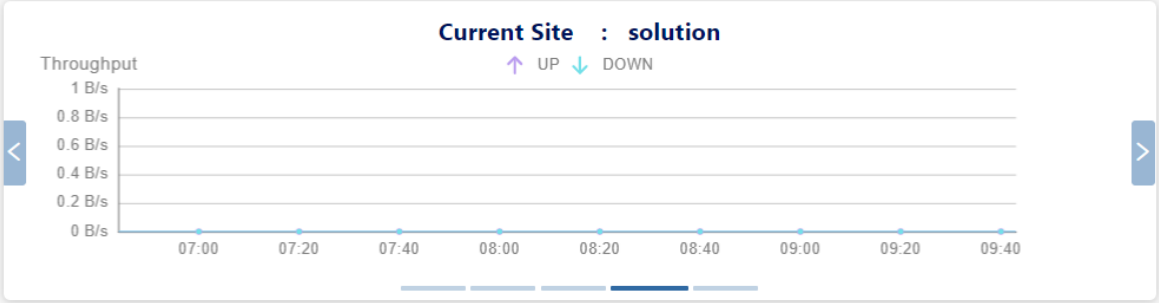


图 43：当前 Site - Throughput

- **Total Traffic：**流量柱状图。

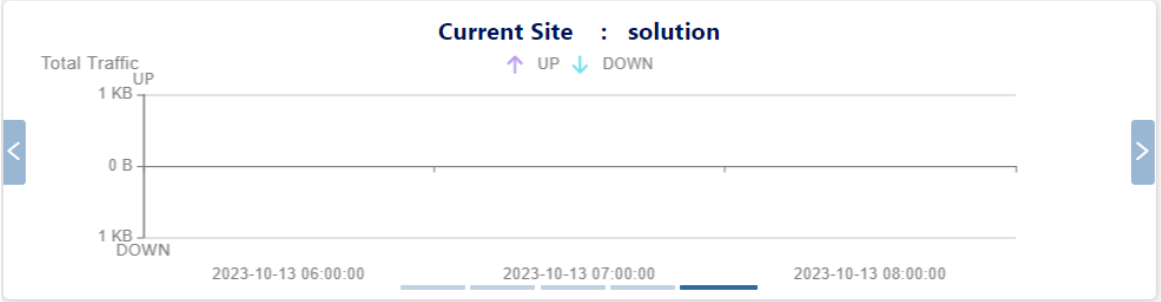


图 44：当前 Site - Total Traffic

► **网络结构**

客户网络结构面板分为：

- **Corporate**
- **Site**
- **Group**

三层网络结构在设计中采用了渐进显示的方法。如果客户拥有多个Corporate或Site，则在单击“Corporate”或“Site”时将显示相应的Site或Group。

图 45：网络结构

3.4.2 我的设备

在主页上**My AP Devices**面板上，点击☰图标进入我的设备界面。

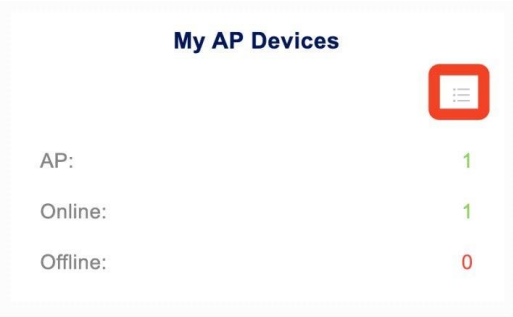


图 46：我的设备面板

在“My Device”界面上，顶部突出位置显示着“**count of online APs (green number)**”和“**count of offline APs (red number)**”。

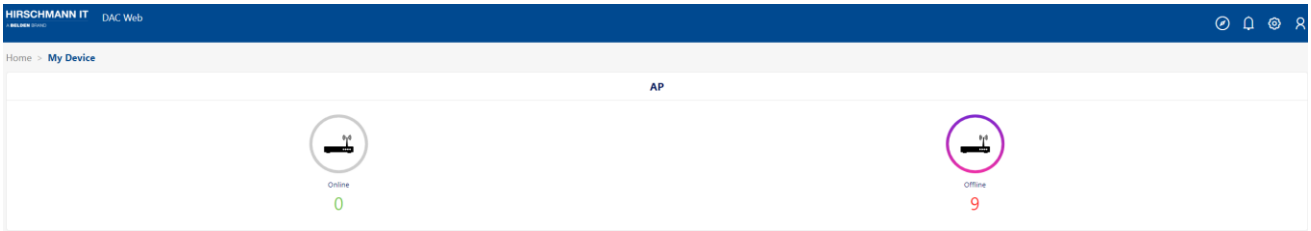


图 47：My Device 界面

3.4.3 AP 设备

AP设备列出您管理的所有AP设备。您可以选择显示Owner权限设备或管理员权限设备。

- **Name**：AP设备名称。
  您可以更改AP的名称，以便快速地找到。也可点击进入AP详细视图。
- **Site**：AP所属的Site。您可点击进入Site视图。
- **Group**：AP被分配到的Group。您可点击进入Group视图。
- **Corp**：AP所属的Corp。
- **MAC**：AP的MAC地址。
- **Firmware**：AP的固件版本。
- **Model**：AP的硬件类型。
- **License**：AP的许可证状态，可以启用或禁用。如果许可证被禁用，则AP不会广播SSID。
- **IP**：AP的IP地址。
- **Serial Number**：AP的序列号。
- **Status**：AP的状态，在线或离线。
- **Client Number**：当前连接到AP上的客户端数量。
- **Permission**：当前用户管理AP的权限。
- **Location**：AP设备的位置。
- **2.4G Channel**：用于DAP的2.4G频段。
- **5G High Channel**：DAP使用5G高频段。
- **5G Low Channel**：DAP使用5G低频段。

► **5G All Channel**：用于DAP的5G全频段。

► **Online Duration**：DAP连接到DAC的持续时长。

► **Last Offline Time**：DAP最近一次与DAC断开的时间。

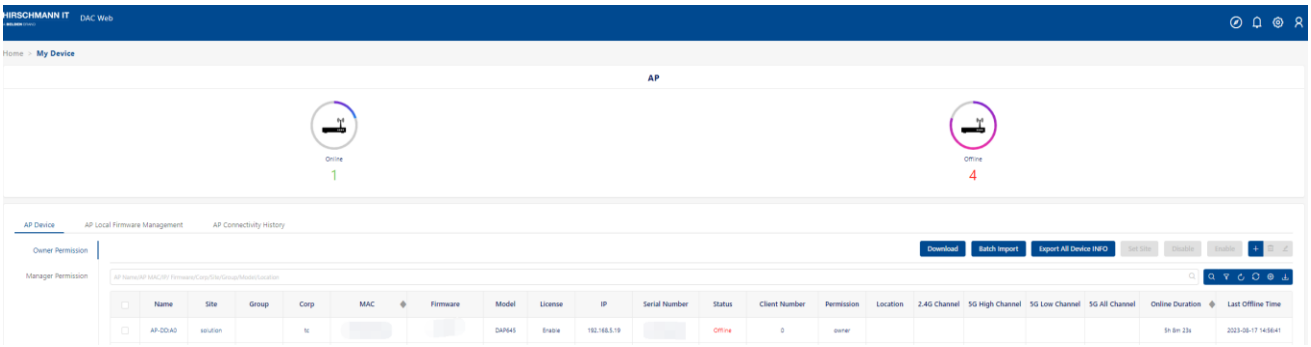


图 48：AP Device 列表

3.4.4 将 DAP 分配给 Site 或 Group

- ☐ 切换到**Home→My Device**页面。**点击“AP Device”**选项卡。
- ☐ 选择要分配给Site或Group的AP。
- ☐ 单击“**Set Site**”按钮。然后在确认提示上点击“**Yes**”按钮，打开“**Set Site**”界面。
- ☐ 从下拉列表中选择一个Site，点击“**Next step**”按钮。
- ☐ 选择一个Group，若不设置Group，则点击“**Next step**”按钮。
- ☐ 点击“**Save**”确认信息。

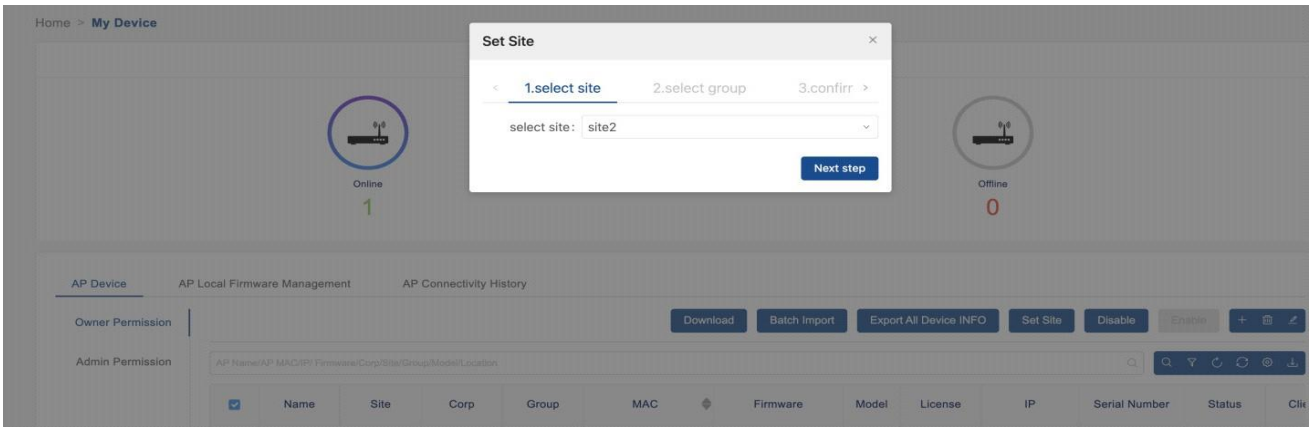


图 49：Set Site 界面

3.4.5 AP 本地固件管理

- ☐ 切换到**Home→My Device**页面，然后点击“**AP Local Firmware Management**”选项卡，管理本地AP固件。
  通常情况下，DAC 会从云端下载 AP 的固件。然而，在某些情况下，我们需要从 DAC 管理页面导入 DAP 的固件。导入的固件是一个压缩包，您可以从供应商那里获取到。
- ☐ 点击“**+**”图标，打开“Upload”窗口。
- ☐ 点击“Upload”按钮，选择从供应商获取的AP固件包。上传的文件出现在列表中。
  - ► **Firmware Version**：DAP固件的版本。
  - ► **Firmware Description**：DAP固件描述。
  - ► **Upload Time**：上传固件所需时间。

然后，您可以在Site视图的AP设备列表页面上升级AP设备的固件。请参阅第115页的“升级固件”。

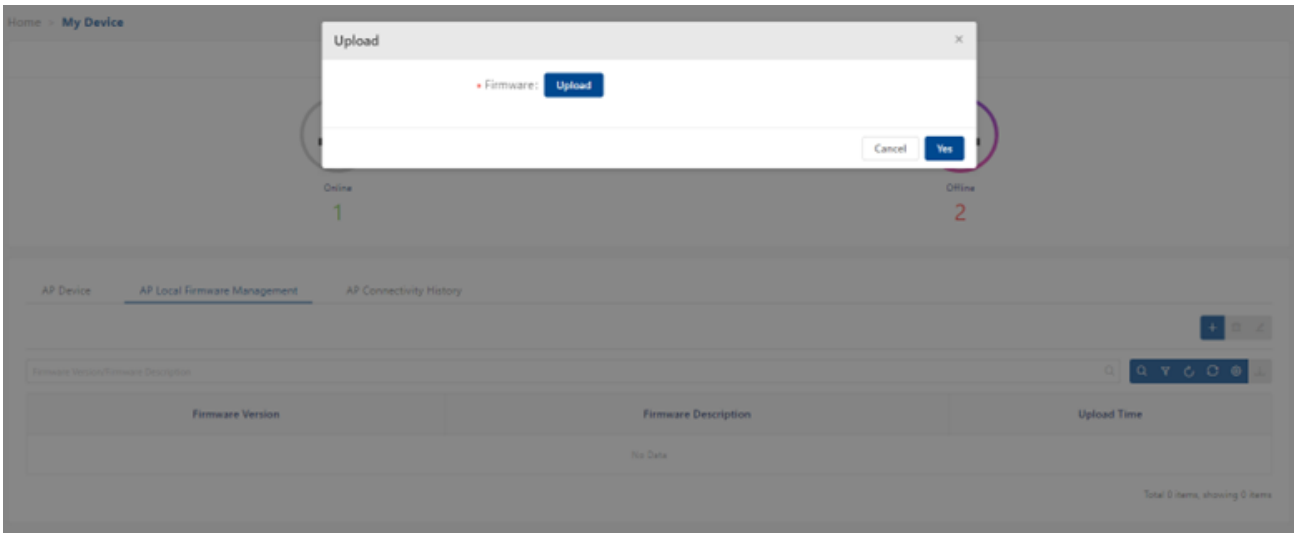


图 50：AP 本地固件管理

3.4.6 AP 连接历史

AP连接历史包括AP连接记录和断开记录。

- ► **MAC**：AP设备的MAC地址。
- ► **Name**：AP设备的名称。

► **MQTT Connected Time**：AP设备的MQTT连接时间。

► **MQTT Disconnected Time**：AP设备的MQTT断开时间。

► **MQTT Connected Duration**：AP设备的MQTT连接持续时间。

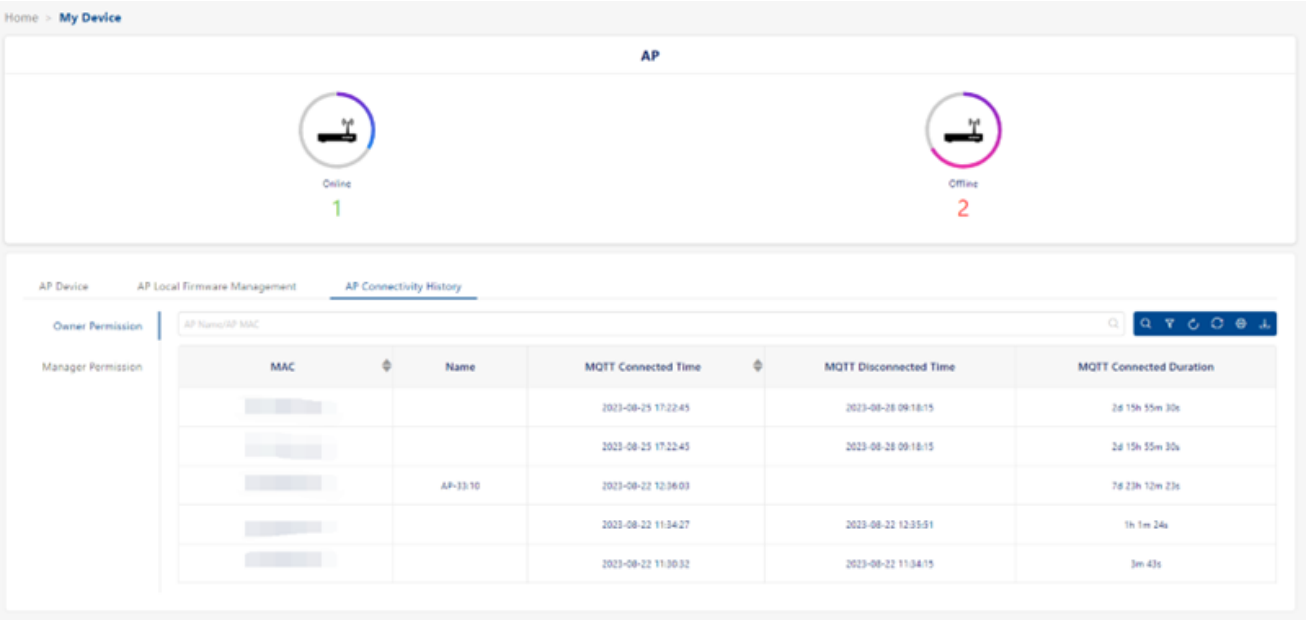


图 51：AP 连接历史

3.5 Site 视图

在主页上点击“Site”，查看Site信息。

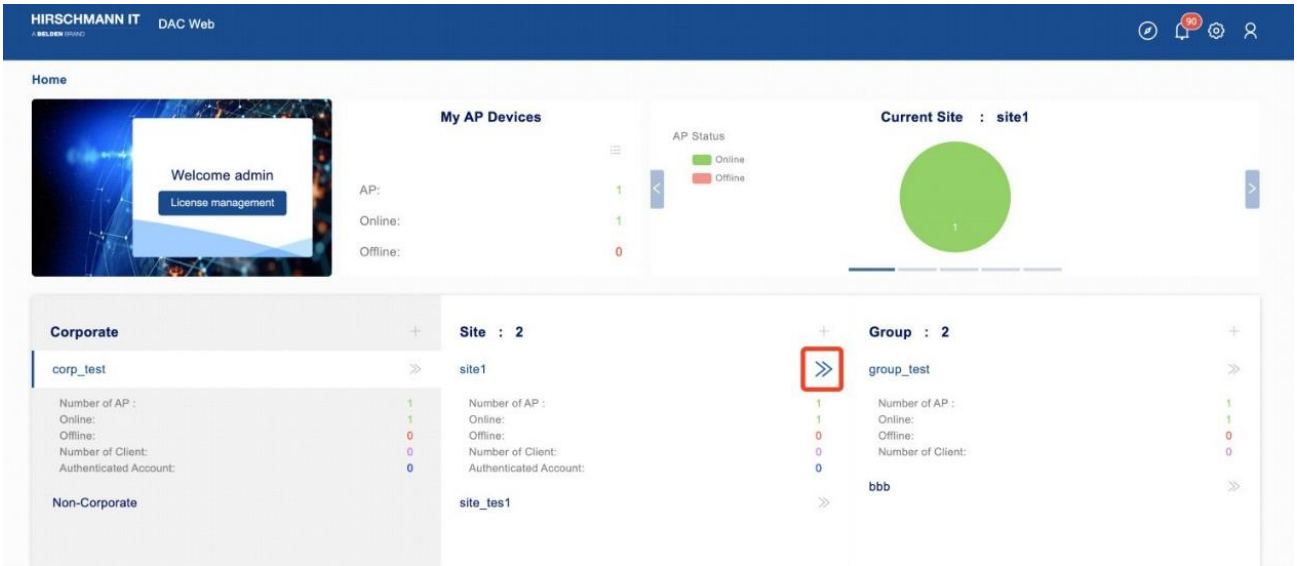


图 52：主页

在Site视图中，您可以看到Dashboard、WLAN、AP、Clients、Authentication、RF、Log、Security、Group和Setting选项卡。

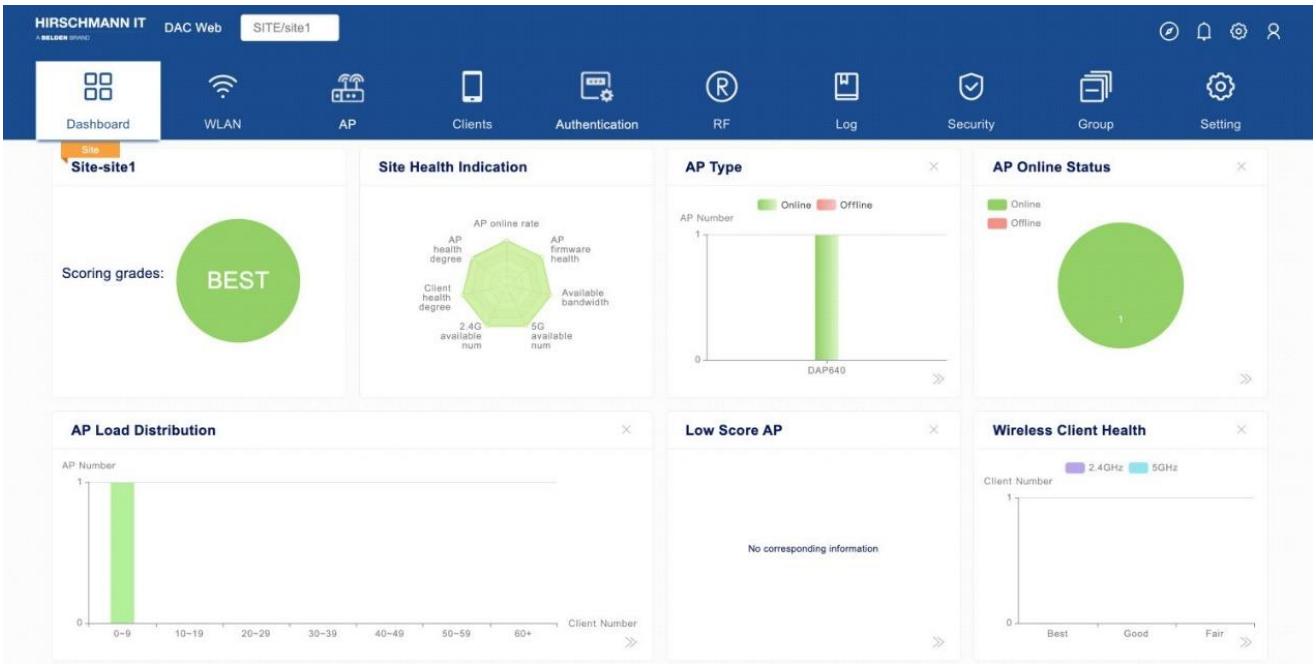


图 53：Site 视图页面

3.5.1 仪表盘

► **Today's data：**显示实时终端的当前数量，当天的历史终端数量和流量，过去8天内每天计算的用户峰值数量，累计用户数量，上行流量统计和下行流量统计。

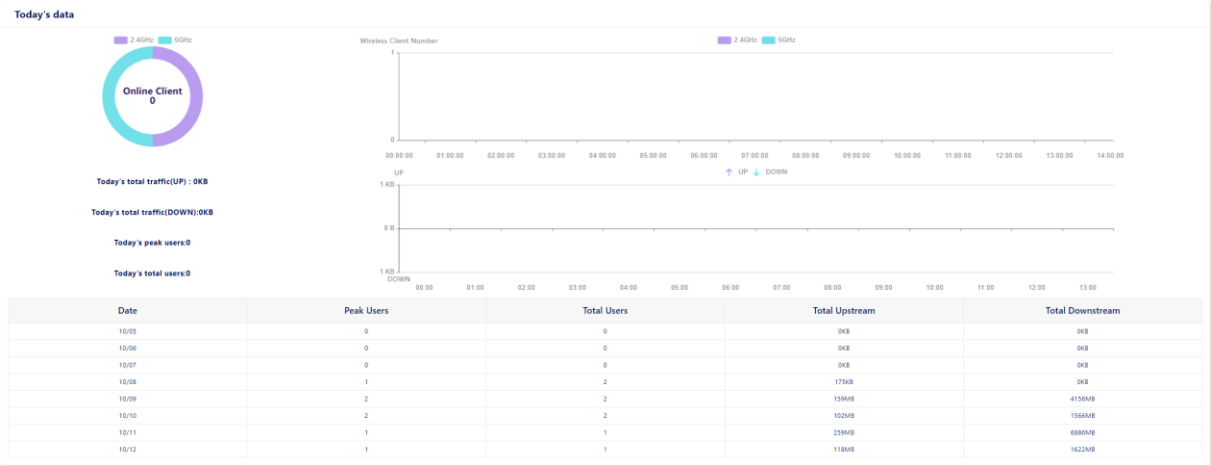


图 54：Site 仪表盘 - Today's data

► **Scoring grades：**显示当前Site健康水平（最佳、良好、一般或N/A）。

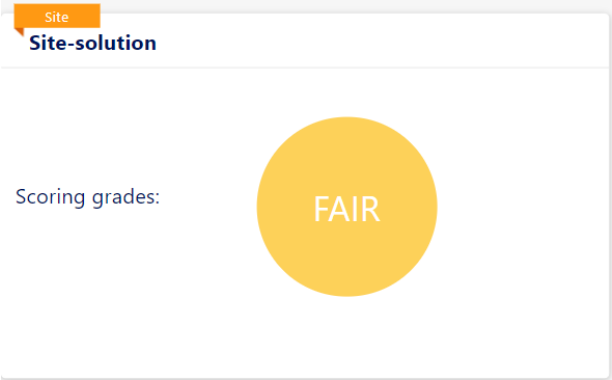


图 55：Site 仪表盘 - Scoring grades

► **Site Health Indication：**显示当前领域所有AP、终端或带宽维度的具体健康水平详情。健康水平分三等：最好、较好和一般。

- **AP online rate：**由Site中在线AP占所有AP的百分比决定。
  最好：占比>80%；较好：60%<占比<80%；一般：占比<60%
- **AP firmware health：**
  最好：Site中所有AP均为最新版本。
  较好：Site中所有AP版本相同但不是最新版本。

一般：Site中AP的版本不同。

- **Available bandwidth**：由Site中每个AP的平均可用带宽与总带宽之比决定。
  最好：占比>80%；较好：60%<占比<80%；一般：占比<60%
- **5G available num**：由Site中在线AP在5G频段的平均客户端数量决定。
  最好：平均值<8；较好：8<平均值<16；一般：平均值>16
- **2.4G available num**：由Site中在线AP在2.4G频段的平均客户端数量决定。
  最好：平均值<8；较好：8<平均值<16；一般：平均值>16
- **Client health degree**：由Site中健康客户端与所有客户端之比决定。
  最好：占比>80%；较好：60%<占比<80%；一般：占比<60%
  注意：客户端是否健康由其RSSI决定。
- **AP health degree**：由Site中在线AP平均CPU使用率决定。
  最好：平均值<20%；较好：20%<平均值<40%；一般：平均值>40%

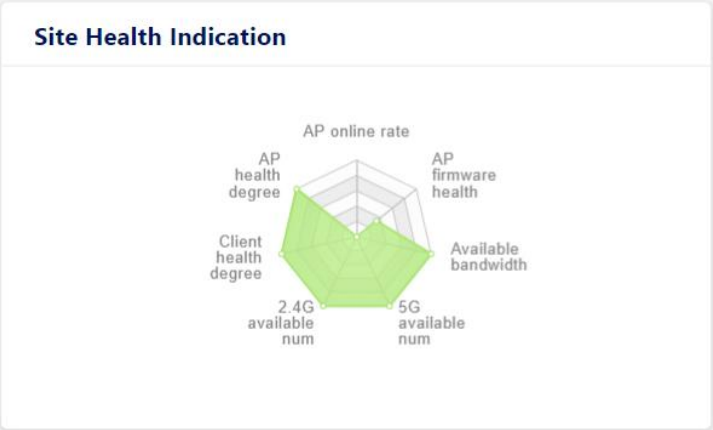


图 56：Site 仪表盘 - Site Health Indication

► **AP Type**：AP的具体型号和在“Site”中该型号数量的柱状图。横轴表示AP型号，纵轴表示相应型号的数量。

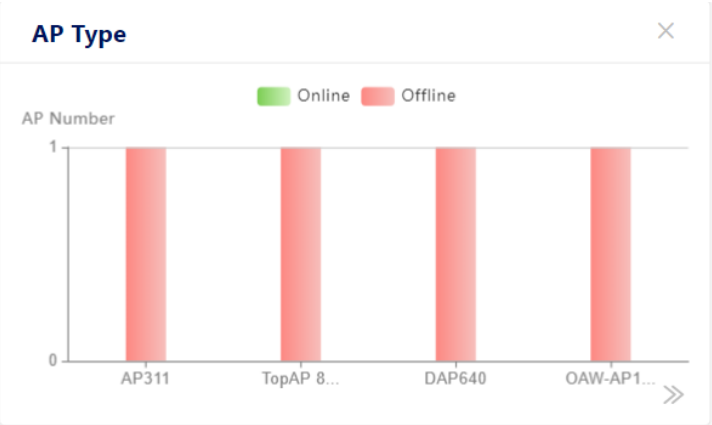


图 57：Site 仪表盘 - AP Type

► **AP Online Status：**显示AP在线和离线的饼图百分比。

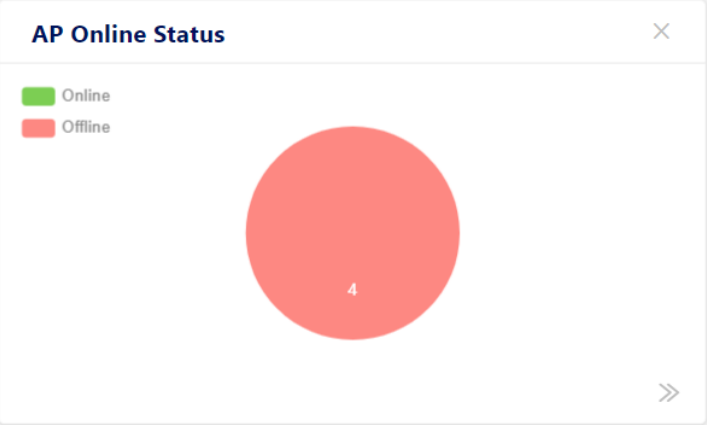


图 58：Site 仪表盘 - AP Online Status

► **AP Load Distribution：**AP中的负载平衡。表示不同AP连接的终端数量的条形统计图。

- 横轴表示连接的终端的数量，分7个参考范围：0-9、10-19、20-29、30-39、40-49、50-59、60+。
- 纵轴表示对应连接终端数量的AP的数量。

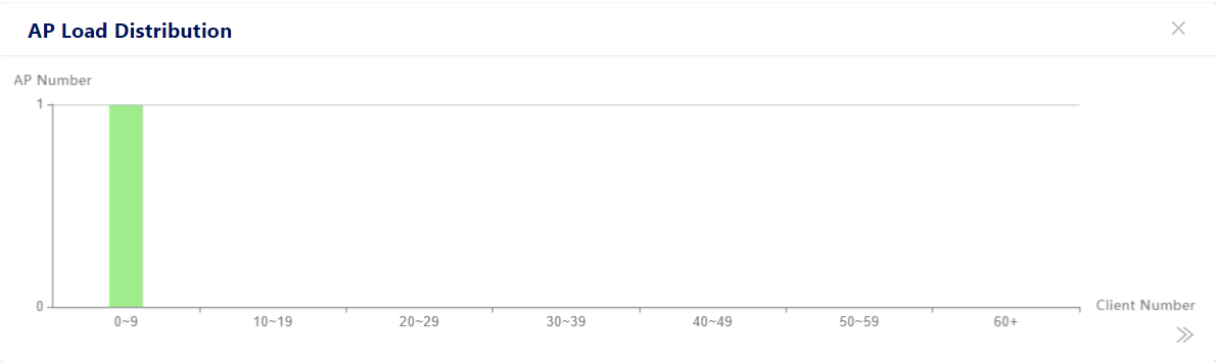


图 59：Site 仪表盘 - AP Load Distribution

► **Low Score AP**：提供一个得分低于阈值标准的AP列表。提醒客户关注AP的具体操作状态和版本信息。低分区AP选项卡中的AP列表是动态的。如果AP指标不符合阈值要求，则在选项卡中显示该AP。

客户可以直接点击，进入设备菜单（一级菜单）查看具体情况。但如果AP指标恢复达到阈值要求，AP会自动从选项卡中消失。

AP阈值指标从以下5个方面进行评判：

- AP CPU利用率
- AP内存利用率
- AP闪存利用率
- 终端接入数量
- AP已使用的带宽

► **Group List**：显示Site下的Group列表。

- **Group Name**：Site包含的所有Group的名称。您可点击Group名称进入Group视图。
- **AP Number**：Group中的AP数量。
- **Client Number**：Group中的客户端数量。
- **SSID Number**：在Group中创建的SSID数量。

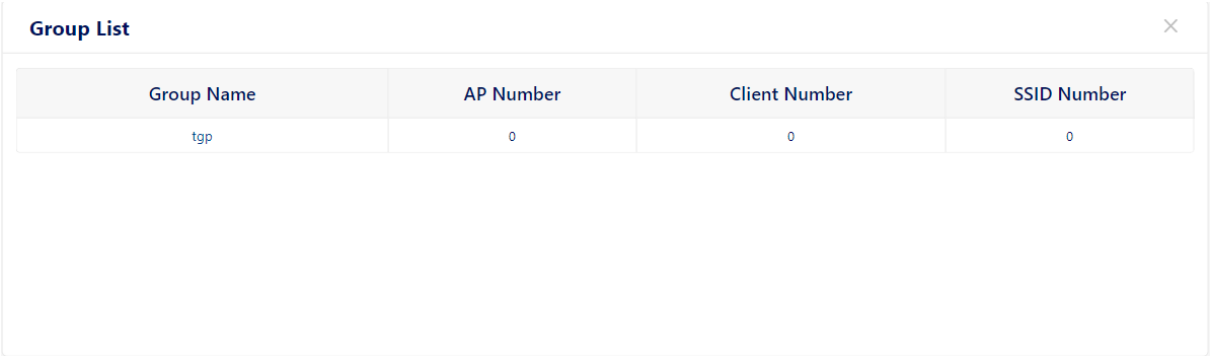


图 60：Site 仪表盘 - Group List

► **WLAN List：显示Site上的SSID列表。**

- **SSID：**无线网络的SSID名称。
- **Client Number：**与SSID关联的客户端数量。
- **From(Site/Group)：**Site或Group，表示SSID是从该Site或Group创建的。
- **Security：**无线安全级别，可以是Open、Personal或Enterprise。

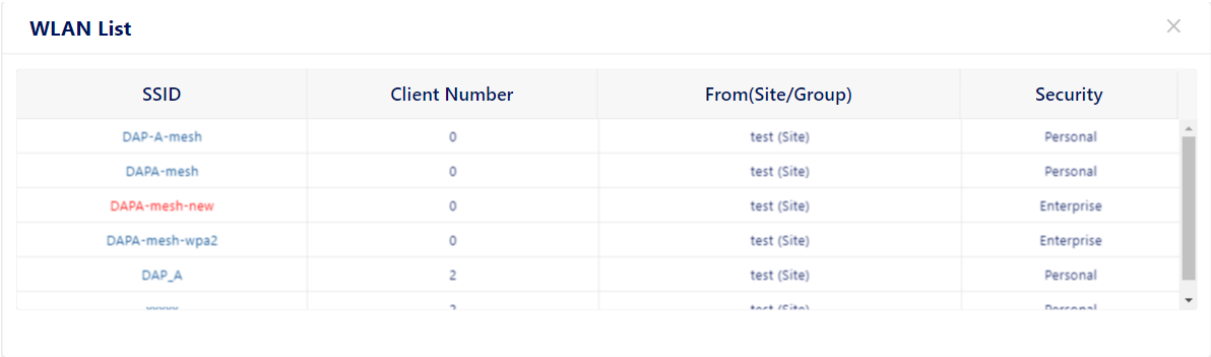


图 61：Site 仪表盘 - WLAN List

► **Wireless Client Health：**在终端健康选项卡中，根据终端信号传输到AP的信号强度（RSSI为接收信号强度指示），提供了3个级别的接入健康状况：

- 符合最佳RSSI阈值的终端归类为“best”水平。
- 符合良好RSSI阈值的终端归类为“good”水平。
- 符合一般RSSI阈值的终端归类为“fair”水平。

同时，我们使用颜色来区分终端的接入频段。

图 62：Site 仪表盘 - Wireless Client Health

► **Client Type：**当前接入终端的硬件类型包括计算机、移动设备和其他设备。

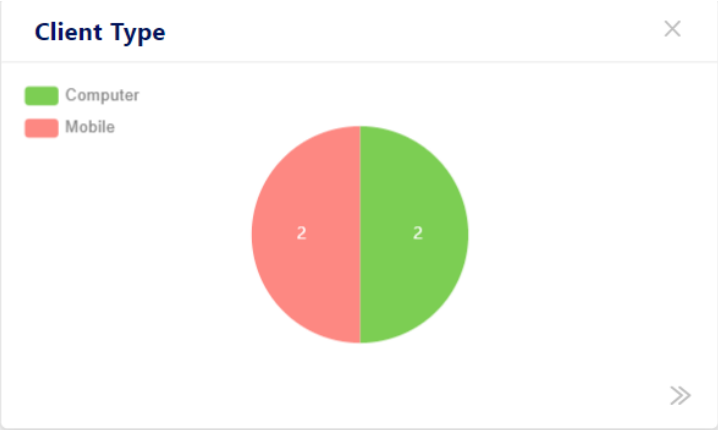


图 63：Site 仪表盘 - Client Type

► **Operating System：**接入终端的操作系统类型以饼图的形式直观呈现。

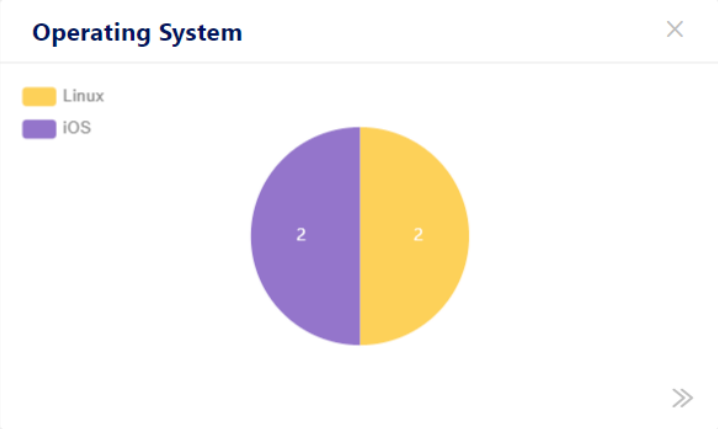


图 64：Site 仪表盘 - Operating System

► **Current Intrusive AP：** 以饼图形式展示干扰AP和Rogue AP的比例。

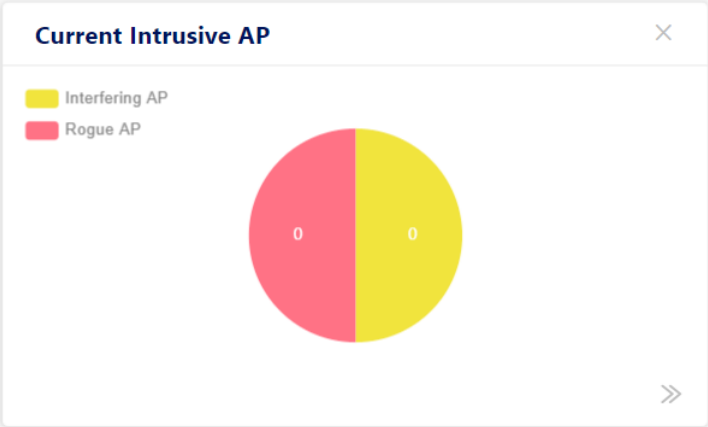


图 65：Site 仪表盘 - Current Intrusive AP

► **Current Intrusive Client：** 以饼图形式展示干扰客户端和Rogue客户端的比例。

图 66：Site 仪表盘 - Current Intrusive Client

► **Historical statistics：** 可从下拉列表中选择一个时间段。

- **Client Number：** 客户端数量的折线图。
- **Throughput：** Site的吞吐量折线图。
- **Traffic：** 流量柱状图。

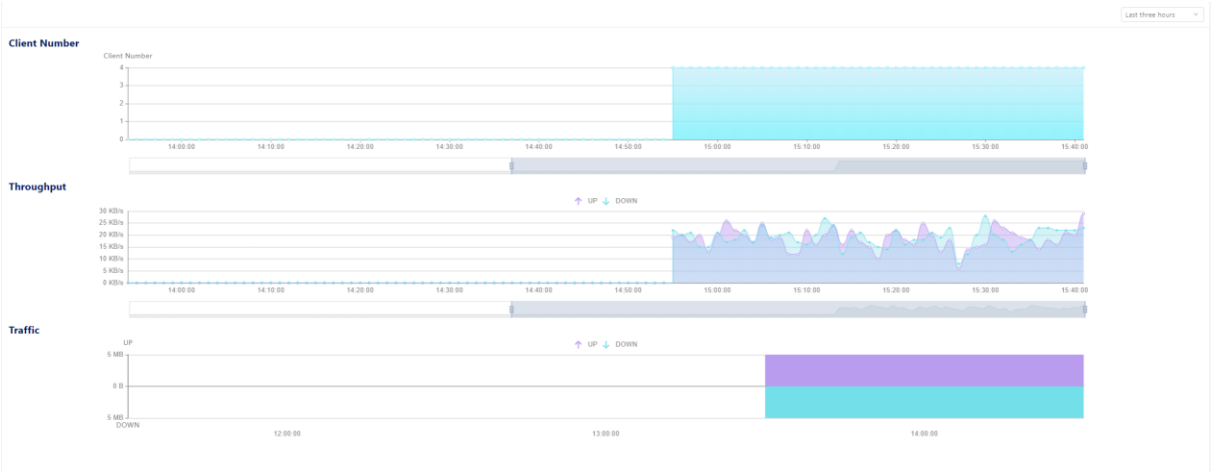


图 67：Site 仪表盘 - Historial statistics

3.5.2 WLAN

创建、修改和删除Site的SSID。请参阅第91页的“WLAN”。

3.5.3 AP

AP设备的管理和监控。管理包括AP名称修改、版本管理、NTP服务管理等。监控包括系统日志的记录，AP的系统日志服务，以及AP单元中的关键指标。请参见第110页的“AP”。

3.5.4 客户端

终端管理和监控。管理包括对具有异常行为的终端进行黑名单处理。监控包括终端类型统计、操作系统类型统计以及网络连接的终端各种参数的查询。请参见第133页的“客户端”。

3.5.5 身份验证

创建、修改和删除身份验证和其他相关策略配置。请参阅第141页的“身份验证”。

3.5.6 RF

显示AP RF配置。根据Site设置RF配置。根据单个AP设置RF配置（优先级高于

Site配置）。请参见第204页的“RF”。

3.5.7 日志

系统日志或设备日志。请参见第216页的“日志”。

3.5.8 安全

配置Rogue AP策略和无线攻击检测策略。无线攻击检测策略包括AP攻击检测策略、终端攻击检测策略和黑名单策略。
统计非法AP记录，包括干扰AP、Rogue AP、攻击AP和无效AP。干扰终端记录的统计包括与干扰AP关联的终端，与Rogue AP关联的终端，终端攻击检测到的终端，以及进入黑名单的终端。提供攻击排名统计数据。请参见第223页的“安全”。

3.5.9 Group

从属于该Site的Group入口。您可以查看该Site上所有Group，每个Group都显示在一张卡片上。

- **Scoring Grades**：显示Group健康水平（最佳、良好、一般或N/A）。
- **Health**：显示当前区域所有AP、终端和带宽维度的具体健康级别详情。
- **AP**：在线和离线数量。

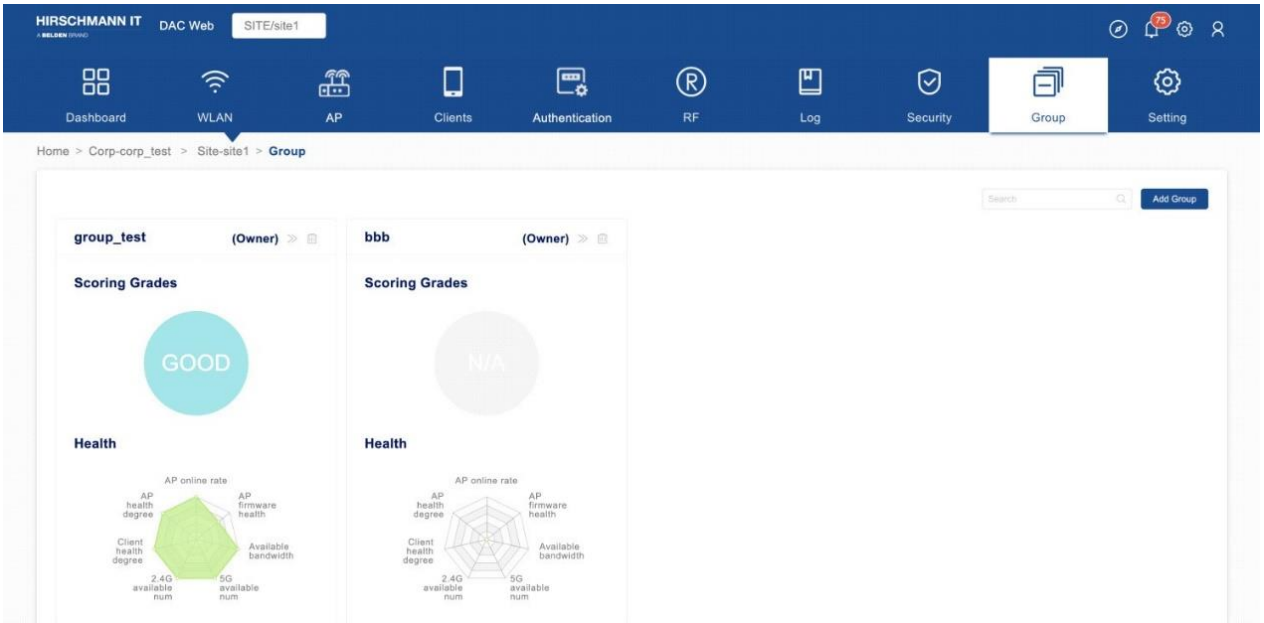


图 68：Group 窗口

■ 创建一个Group

☐ 点击“**Add Group**”按钮，打开“**Create Group**”窗口。
☐ 填入“**Name**”和“**Description**”字段。
☐ 点击“**Save**”保存Group。您可以在Group页面上看到新添加的Group。

■ 删除一个Group

☐ 点击Group卡片上的“**Delete**”图标。
☐ 在确认提示上单击“**Yes**”。

3.5.10 设置

Site设置。

■ 基本信息/设置

▶ **Corp Operation**：在将Site分配给Corporate后显示。

- **Quit Corp**：将当前Site从Corporate中移除。

▶ **Site Operation**：

- **Transfer Site**：将Site的Owner权限转移给其他用户。
- **Edit**：修改Site的“**Name**”或“**Description**”。
- **Delete**：删除Site。
- **Join Corporate**：使用此功能将Site分配给Corporate。

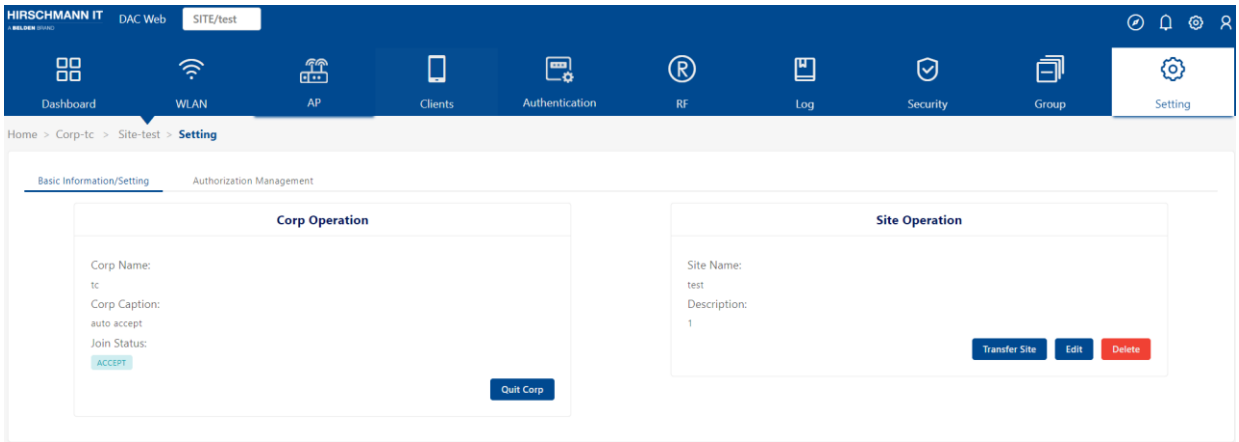


图 69：Site Setting 窗口

■ 授权管理

您可以添加其他用户来管理Site。仅限Site的Owner查看该功能。

▶ 管理员列表

- **User Name：**用户名。
- **Email：**电子邮件。
- **Status：**成功/失败。
- **Telephone：**用户的电话号码。
- **Character：**角色可以是Manager、Viewer或Guest Operator。

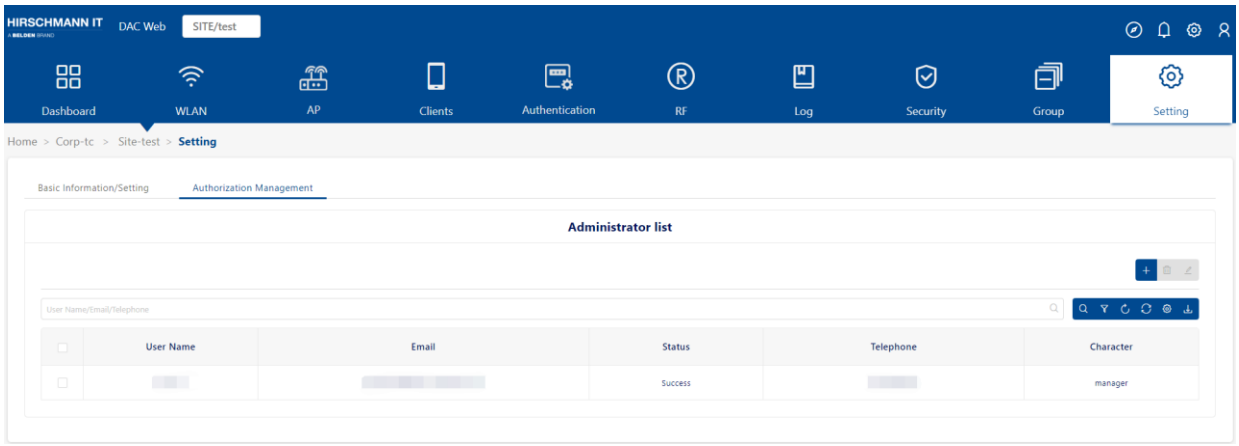


图 70：Authorization Management 窗口

■ 添加管理员

☐ 点击“**+**”图标，打开“**Add administrator**”窗口。

☐ 填入您要添加的“**User name**”或“**Email**”。

☐ 从下拉列表中选择“**Character**”（Manager、Viewer、或者Guest Operator）。

☐ 点击“**Save**”应用设置。

如果用户账户不存在，可以使用目标用户的电子邮件邮请注册。接收到注册邀请邮件后，目标用户可以注册账户。注册的帐户具有当前Site的相应权限。请参阅第38页的“创建账户”。

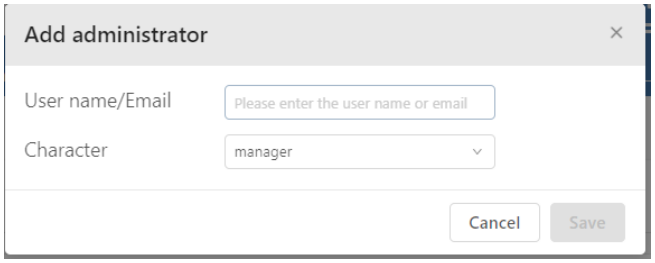


图 71：Add Administrator 窗口

■ 删除管理员

- ☐ 选择您要删除的管理员。
- ☐ 单击“**Delete**”图标。
- ☐ 在确认提示上单击“**Yes**”。

3.6 Group 视图

3.6.1 仪表盘

► **Today's data：**显示实时终端的当前数量，当天的历史终端数量和流量，过去8天内每天计算的用户峰值数量，累计用户数量，上行流量统计和下行流量统计。

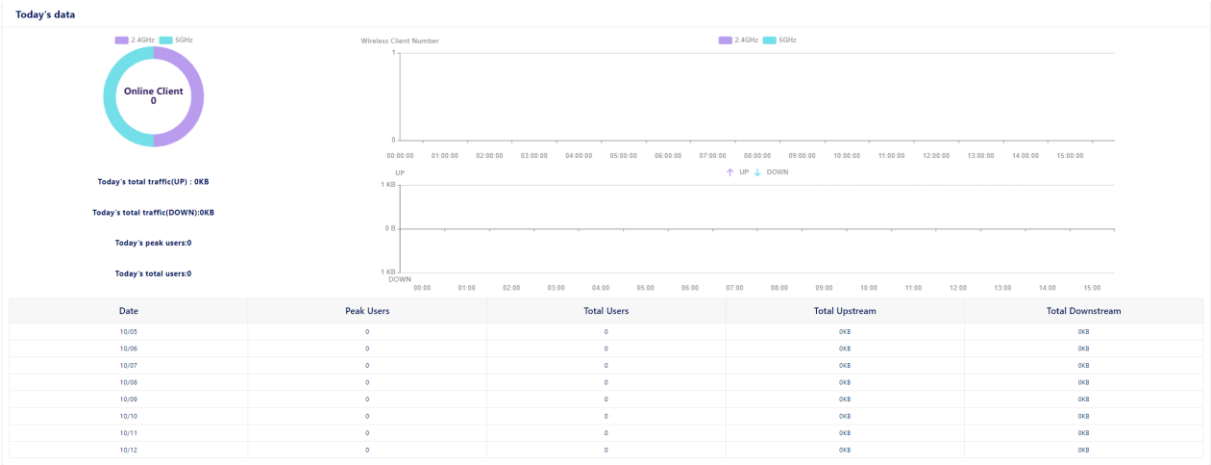


图 72：Group 仪表盘 - Today's data

► **Scoring grades：**显示当前Group健康水平（最佳、良好、一般或N/A）。

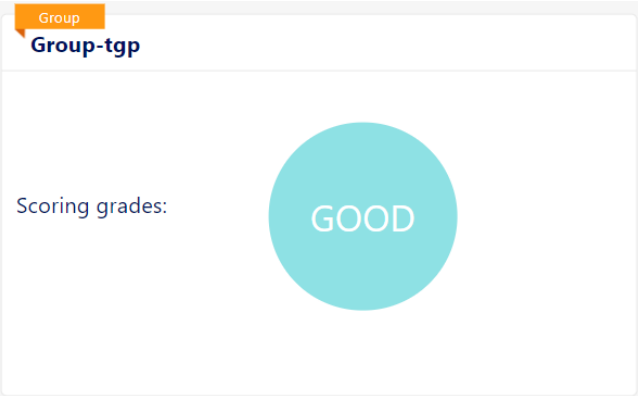


图 73：Group 仪表盘 - Scoring grades

► **Group Health Indication：**显示当前区域所有AP、终端或带宽维度的具体健康水平详情。健康水平分三等：最好、较好和一般。

- **AP online rate：**由Group中在线AP占所有AP的百分比决定。
  最好：占比>80%；较好：60%<占比<80%；一般：占比<60%
- **AP firmware health：**

最好：Group中所有AP均为最新版本。

较好：Group中所有AP版本相同但不是最新版本。

一般：Group中AP的版本不同。

- **Available bandwidth**：由Group中每个AP的平均可用带宽与总带宽之比决定。

  最好：占比>80%；较好：60%<占比<80%；一般：占比<60%

- **5G available num**：由Group中在线AP在5G频段的平均客户端数量决定。

  最好：平均值<8；较好：8<平均值<16；一般：平均值>16

- **2.4G available num**：由Group中在线AP在2.4G频段的平均客户端数量决定。

  最好：平均值<8；较好：8<平均值<16；一般：平均值>16

- **Client health degree**：由Group中健康客户端与所有客户端之比决定。

  最好：占比>80%；较好：60%<占比<80%；一般：占比<60%

  注意：客户端是否健康由其RSSI决定。

- **AP health degree**：由Group中在线AP平均CPU使用率决定。

  最好：平均值<20%；较好：20%<平均值<40%；一般：平均值>40%

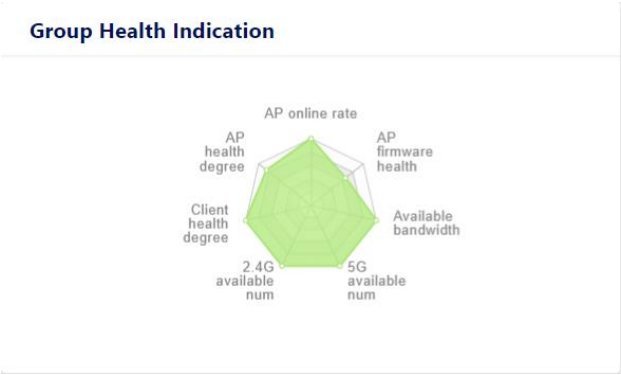


图 74：Group 仪表盘 - Group Health Indication

► **AP Type**：AP的具体型号和在**“Site”**中该型号数量的柱状图。横轴表示AP模型，纵轴表示相应模型的数量。

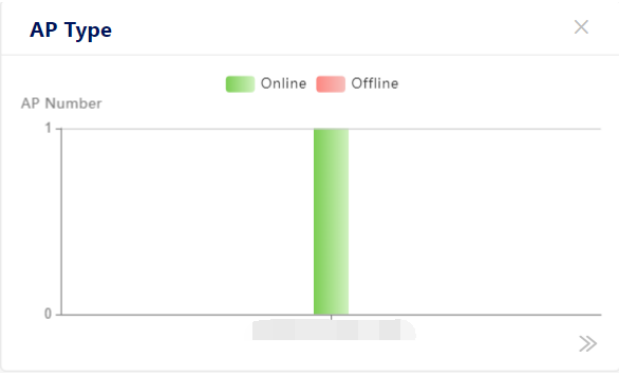


图 75：Group 仪表盘 - AP Type

► **AP Online Status：**AP在线和离线的饼图百分比。

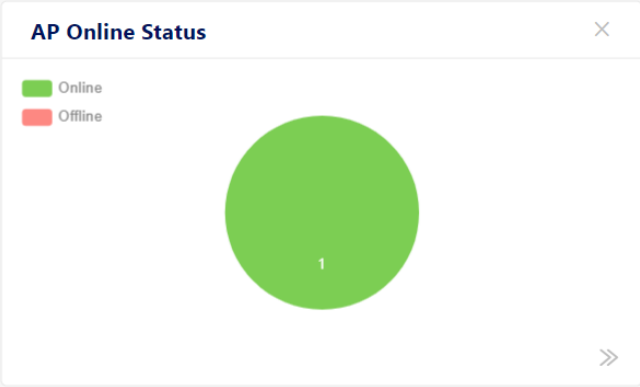


图 76：Group 仪表盘 - AP Online Status

► **AP Load Distribution：**AP中的负载均衡。

在水平轴上，我们提供了7个参考值，表示连接的终端数量，它们是：0-9、10-19、20-29、30-39、40-49、50-59、60+。纵轴是AP的数量。

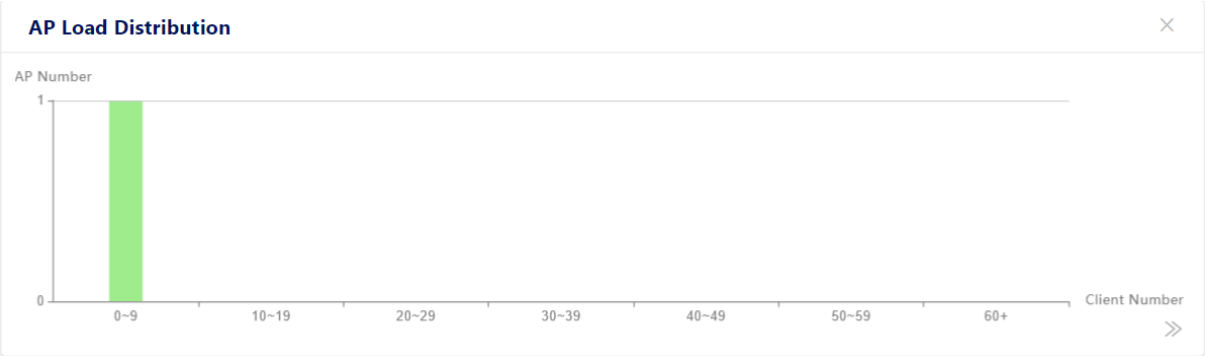


图 77：Group 仪表盘 - AP Load Distribution

► **Low Score AP：**提供一个得分低于阈值标准的AP列表。提醒客户关注AP的具体操作状态和版本信息。

低分区AP选项卡中的AP列表是动态的。如果AP指标不符合阈值要求，则显示在该选项卡中。客户可以直接点击，进入设备菜单（一级菜单）查看具体情况。但如果AP指标恢复达到阈值要求，AP会自动从选项卡中消失。

AP阈值指标从以下5个方面进行评判：

- AP CPU利用率
- AP内存利用率
- AP闪存利用率
- 终端访问次数
- AP使用的带宽

► **WLAN List**：显示Site上的SSID列表。

- **SSID**：无线网络的SSID名称。
- **Client Number**：与SSID关联的客户端数量。
- **From(Site/Group)**：Site或Group，表示SSID是从该Site或Group创建的。
- **Security**：无线安全级别，可以是Open、Personal或Enterprise。

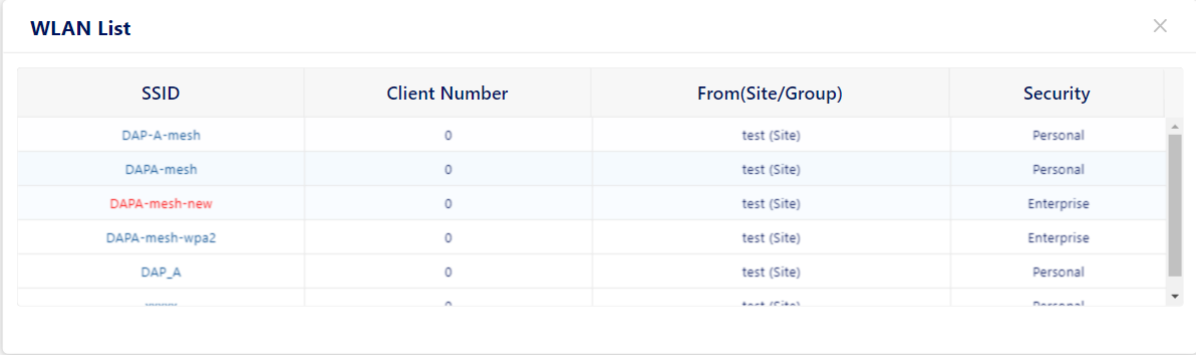


图 78：Group 仪表盘 - WLAN List

► **Wireless Client Health**：

在终端健康选项卡中，根据终端信号上行到AP的信号强度（RSSI为接收信号强度指示），提供了3个级别的接入健康：

- 满足最佳RSSI阈值的终端归类为“best”级别。
- 满足良好RSSI阈值的终端归类为“good”水平。
- 满足一般RSSI阈值的终端归类为“fair”水平。

同时，我们使用颜色来区分终端的接入频段。

图 79：Group 仪表盘 - Wireless Client Health

► **Client Type：**当前的访问终端硬件类型包括计算机、移动设备和其他设备。

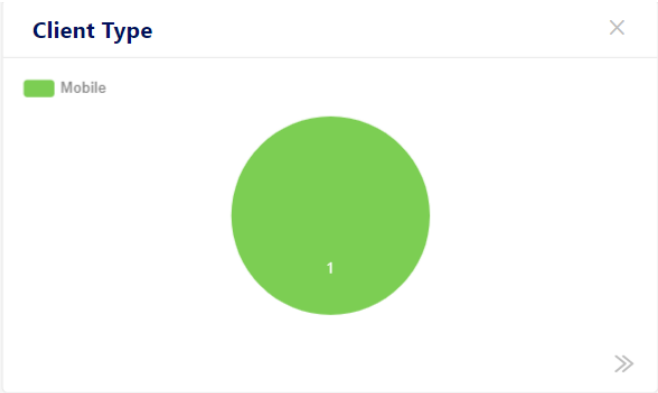


图 80：Group 仪表盘 - Client Type

► **Operating System：**访问终端的操作系统类型以饼图的形式直观呈现。

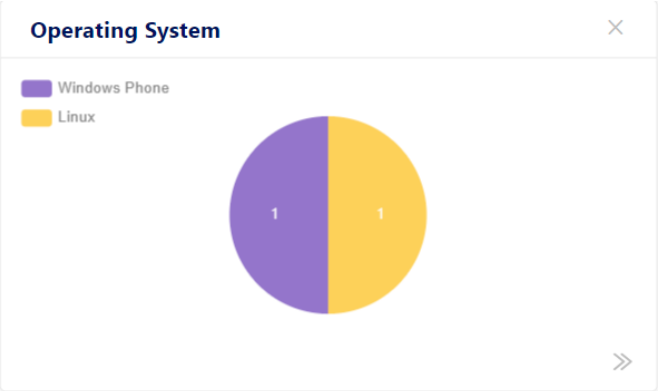


图 81：Group 仪表盘 - Operating System

► **Current Intrusive AP：**以饼图形式展示干扰AP和Rogue AP的比例。

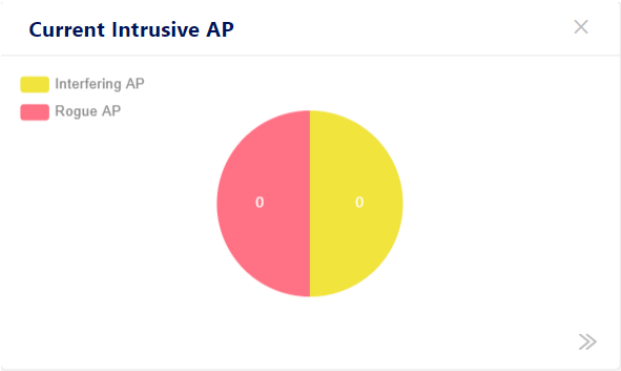


图 82：Group 仪表盘 - Current Intrusive AP

► **Current Intrusive Client：** 以饼图形式展示干扰客户端和Rogue客户端的比例。

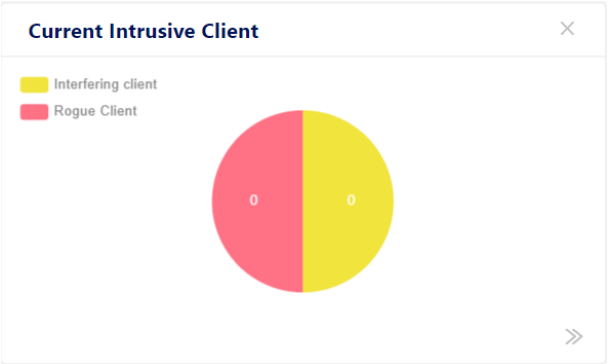


图 83：Group 仪表盘 - Current Intrusive Client

► **Historical statistics：** 可从下拉列表中选择一个时间段。

- **Client Number：** 客户端数量的折线图。
- **Throughput：** Site的吞吐量折线图。
- **Traffic：** 流量柱状图。

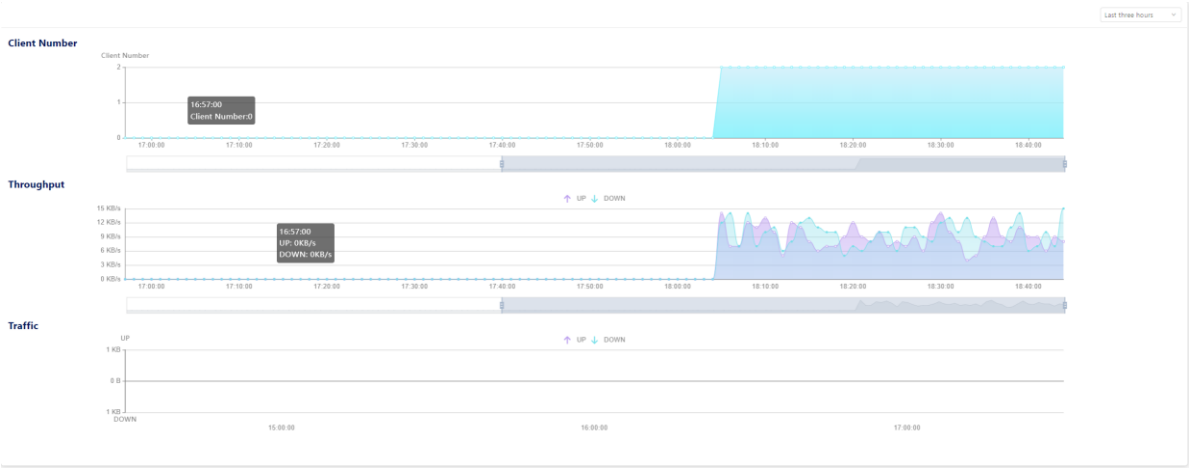


图 84：Group 仪表盘 - Historical statistics

3.6.2 WLAN

创建、修改和删除Group的无线网络。请参阅第91页的“WLAN”。

3.6.3 AP

对Group中AP设备的监控。监控包括系统日志的记录，AP的系统日志服务，以及AP单元中的关键指标。请参见第110页的“AP”。

3.6.4 客户端

终端管理和监控。管理包括对具有异常行为的终端进行黑名单处理。监控包括终端类型统计、操作系统类型统计以及附加到网络的终端的各种参数的统计和查询。请参见第133页的“客户端”。

3.6.5 身份验证

创建、修改和删除身份验证和其他相关策略配置。请参阅第141页的“身份验证”。

3.6.6 RF

显示AP RF配置。在Group的RF页面上，您只能查看RF的配置，无法修改。请参见第204页的“RF”。

3.6.7 日志

系统日志或设备日志。请参见第216页的“日志”。

3.6.8 安全

可以在此页面上查看AP记录、客户记录和黑名单。若想配置流氓AP策略和无线攻击检测策略，切换到“**Site**”的“**Security**”视图。请参见第223页的“安全”。

3.6.9 设置

Group设置。

■ 基本信息/设置

▶ **Group Operation**

- **Edit：** 更改Group名称或描述。
- **Delete：** 删除Group。

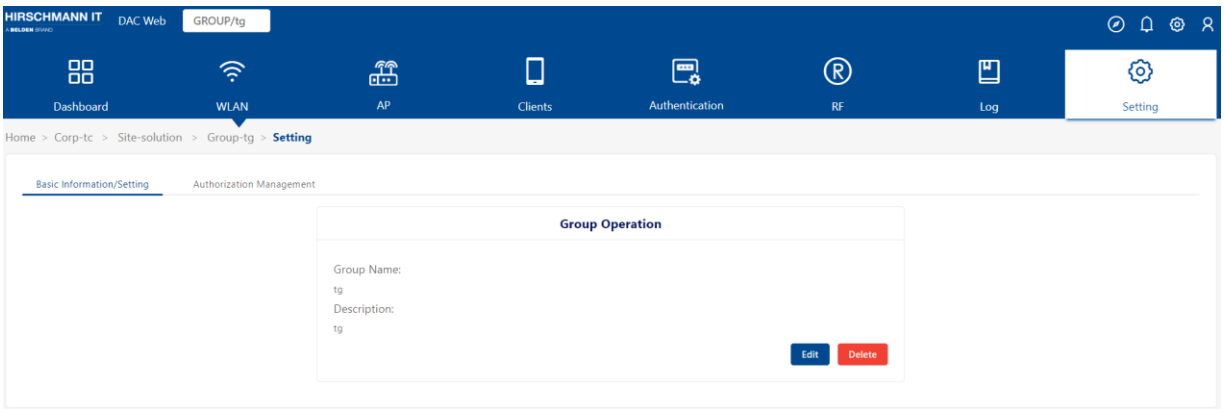


图 85：Basic Information/Setting 界面

■ 授权管理

您可以添加其他用户来管理Group。仅限Group的Owner查看此功能。

▶ **Administrator list**

- **User Name：** 用户名
- **Email：** 电子邮件
- **Status：** 成功/失败
- **Telephone：** 用户的电话号码
- **Character：** 角色可以是Manager或者Viewer

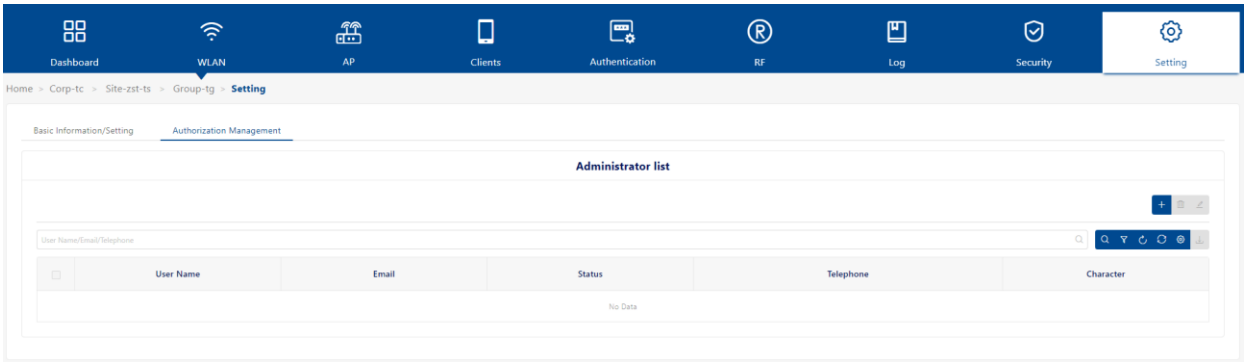


图 86：Authorization Management 界面

■ 添加管理员

- ☐ 点击“**+**”图标，打开“**Add administrator**”窗口。
- ☐ 填入您要添加的“**User name**”或“**Email**”。
- ☐ 从下拉列表中选择“**Character**”（Manager或Viewer）。
- ☐ 点击“**Save**”应用设置。

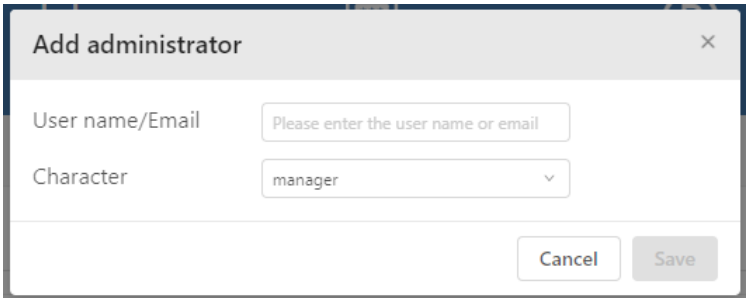


图 87：Add Administrator 窗口

■ 删除管理员

- ☐ 选择您要删除的管理员。
- ☐ 单击“Delete”图标。
- ☐ 在确认提示上单击“Yes”。

4 许可证

目前，DAC有两种许可证：

- **基本许可证**

  包括基本功能（创建WLAN、终端显示、统计等）和客户端访问功能。基本功能基于AP的总数进行授权。客户端访问功能基于认证终端的总数进行授权。

- **安全许可证**

  无线安全包括WIDS和WIPS。安全许可证基于AP数量进行授权。

您可以购买的许可证如下：

型号	零件号	零件名称	描述
基本许可证	942999321	DAC-50	许可证支持 50 个 AP 和 1000 个客户端许可证的软件 DAC 平台
	942999322	DAC-256	许可证支持 256 个 AP 和 5000 个客户端的软件 DAC 平台
	942999323	DAC-500	许可证支持 500 个 AP 和 10000 个客户端的软件 DAC 平台
	942999324	DAC-1000	许可证支持 1000 个 AP 和 20000 个客户端的软件 DAC 平台
安全许可证	942999327	DAC-Sec-50	安全功能许可证支持 50 个 AP 的软件 DAC 平台
	942999328	DAC-Sec-256	安全功能许可证支持 256 个 AP 的软件 DAC 平台
	942999329	DAC-Sec-500	安全功能许可证支持 500 个 AP 的软件 DAC 平台
	942999330	DAC-Sec-1000	安全功能许可证支持 1000 个 AP 的软件 DAC 平台

表 6：许可证型号

许可证以许可证代码形式为载体。根据客户实际购买的AP产品，将其分发给客户。客户可以在Web GUI上激活许可证码，并随时从Web GUI上观察其消耗计数。

在用户“Home”页面上点击“License management”按钮，打开“License”界面。

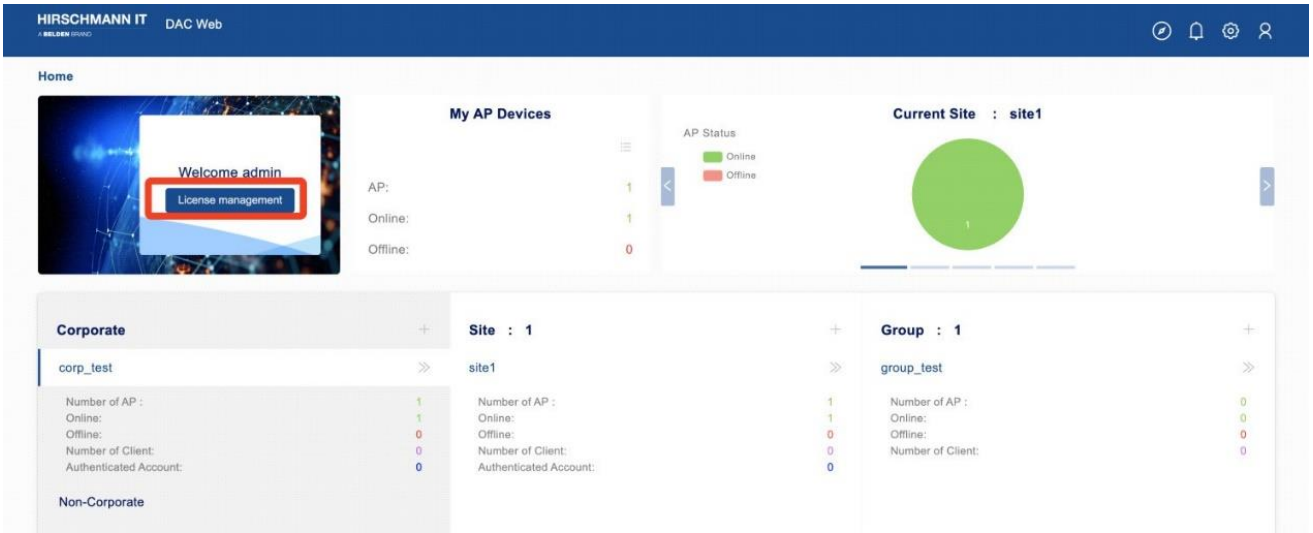


图 88：主页

本章包含下列主题：

- ▶ 许可证激活
- ▶ 许可证管理
- ▶ 许可证记录
- ▶ 设备编码

4.1 许可证激活

使用“**License Activation**”页面激活许可证代码。

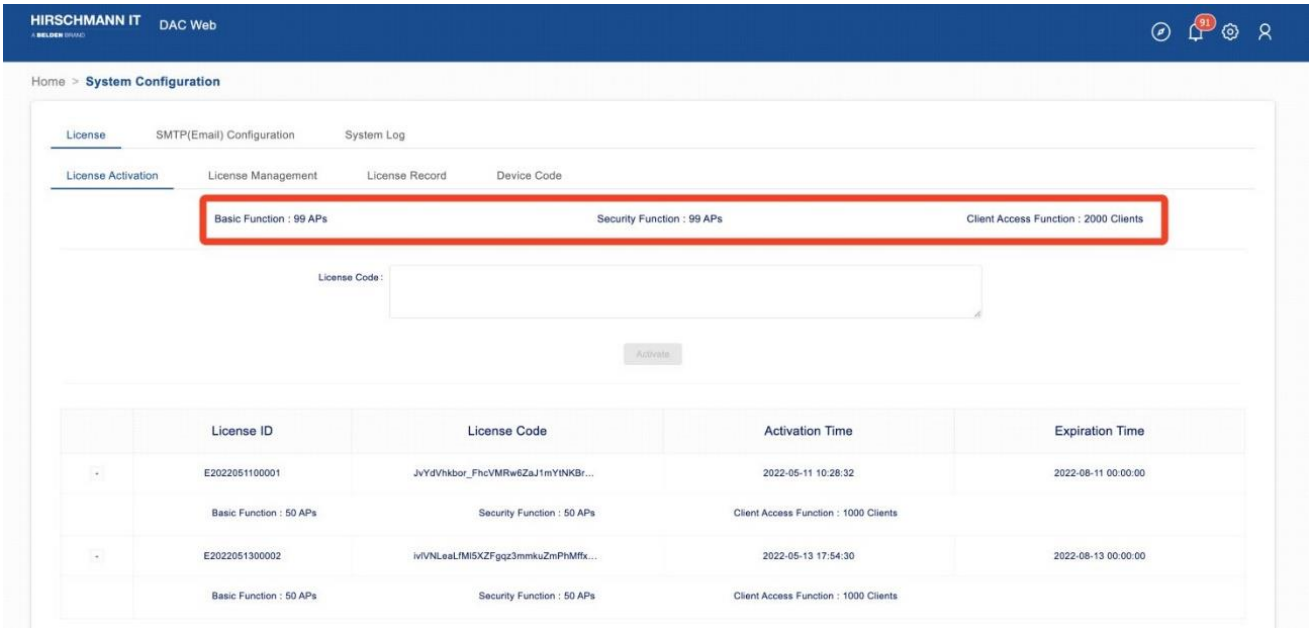


图 89：许可证激活页面

- ☐ 将从供应商处获得的“**License code**”填入到输入框中。
- ☐ 点击“**Activate**”按钮，打开“**License Code**”窗口。详细信息包括每个功能的点数。
  - ► Basic Function：基础AP功能，包括WLAN，RF，数据报告等。如图 89所示，基础功能可用的最大AP数为99。
  - ► Security Function：安全功能，包括黑名单、wIDS/wIPS。如图 89所示，安全功能可用的最大AP数为99。
  - ► Client Access Function：如图 89所示，最多可接入2000个客户端。
- ☐ 在详细信息窗口点击“**Activation**”按钮，启用许可证。然后，新激活的许可证将出现在已激活许可证列表中。

如果您已激活多个许可证，则可以查看每个许可证的实际激活功能和功能数量。同时，您可以看到基本功能的剩余AP数量，可以认证的终端的剩余数量，以及安全功能的剩余AP数量。

已激活许可证列表：

- **License ID**：许可证ID。
- **License Code**：许可证代码。
- **Activation Time**：激活此许可证的时间。
- **Expiration Time**：到失效日期后，许可证中的设备数量将不可用。

官方许可证购买的失效日期为2099-12-31。试用许可证的失效时间为试用申请日期起3个月。

4.2 许可证管理

在此页面上，可以管理和分配您的许可证。

- ☐ 选择相应的Site并点击功能开关。
- ☐ 点击“**Yes**”按钮，确认并启用该功能。

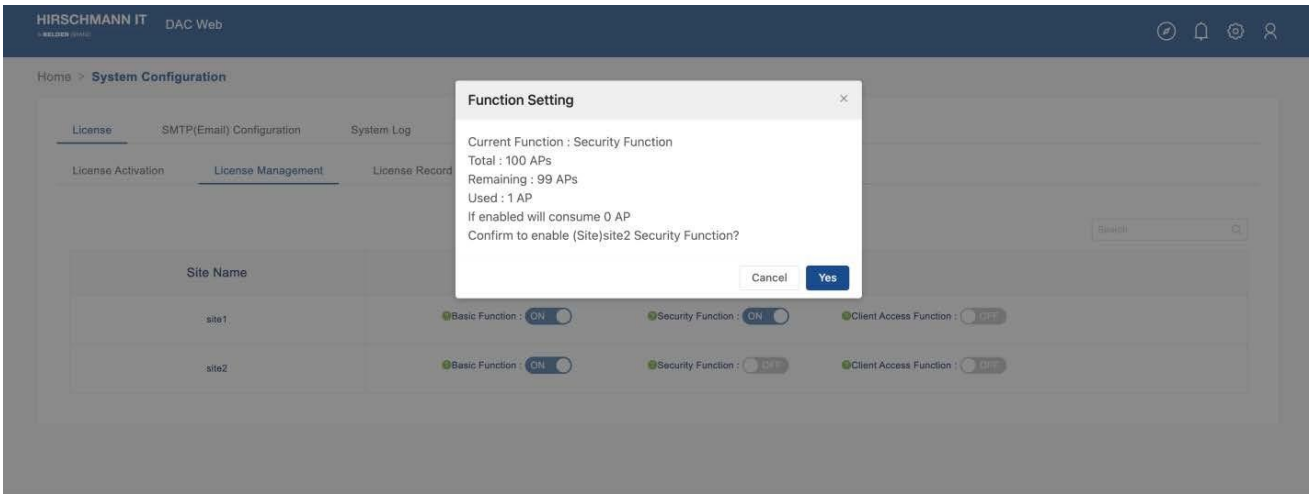


图 90：DAC 许可证管理

在所有Site中，可以启用基本功能的AP总数小于或等于未过期的基本功能许可证的总数。在所有Site中，可以启用安全功能的AP总数小于或等于未过期的安全功能许可证的总数。在所有Site中，可以进行认证的访问客户端总数小于或等于未过期的客户端访问功能的总数。

4.3 许可证记录

根据功能，许可证记录会显示每个Site中每个功能的使用情况，以及当前账户的剩余或过期数量。您可以从下拉列表中选择要显示的功能。

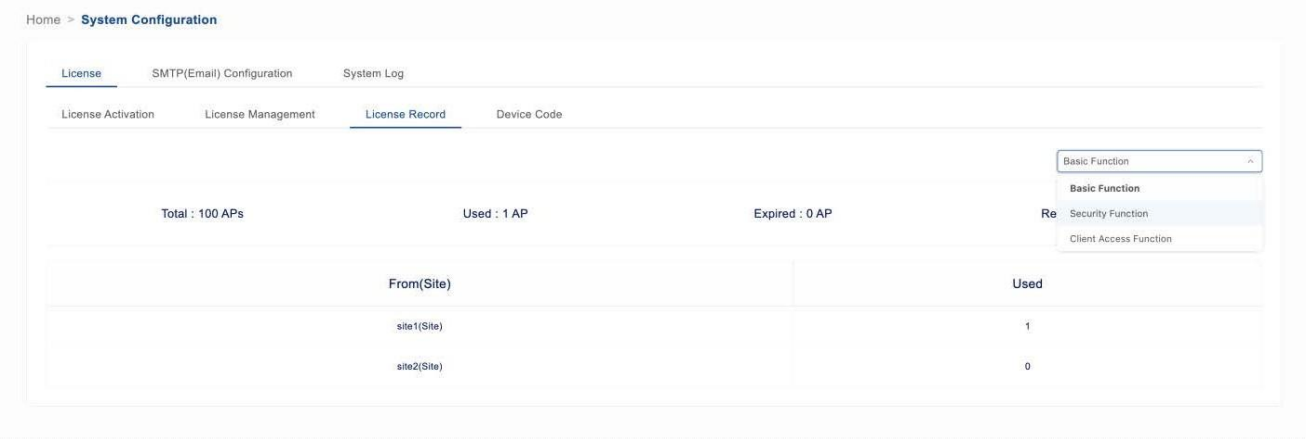


图 91：DAC 许可证记录

4.4 设备编码

DAC设备编码就是DAC的指纹。申请许可证时，您需要向供应商提供设备编码。供应商生成一个许可证代码，该代码只能根据设备编码应用于当前设备。

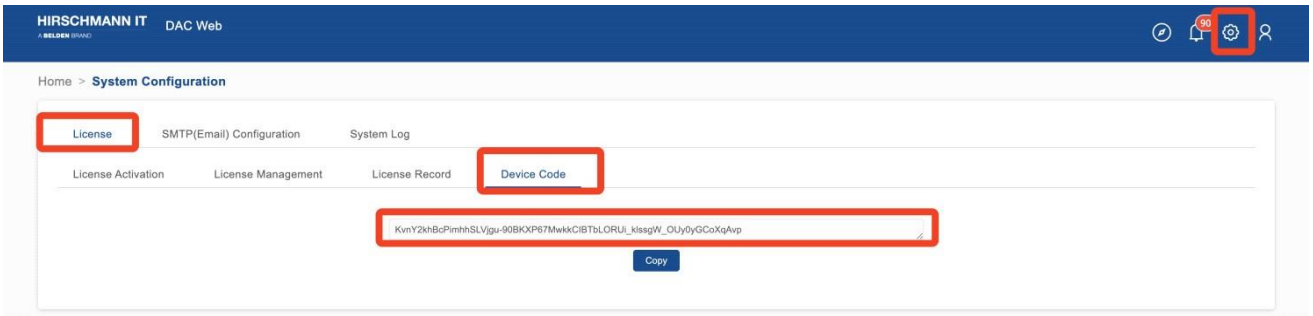


图 92：DAC 设备编码

5 WLAN

本节介绍了无线接入的基本原理，还描述了如何创建或修改WLAN。可在“Site”或“Group”视图中配置WLAN。

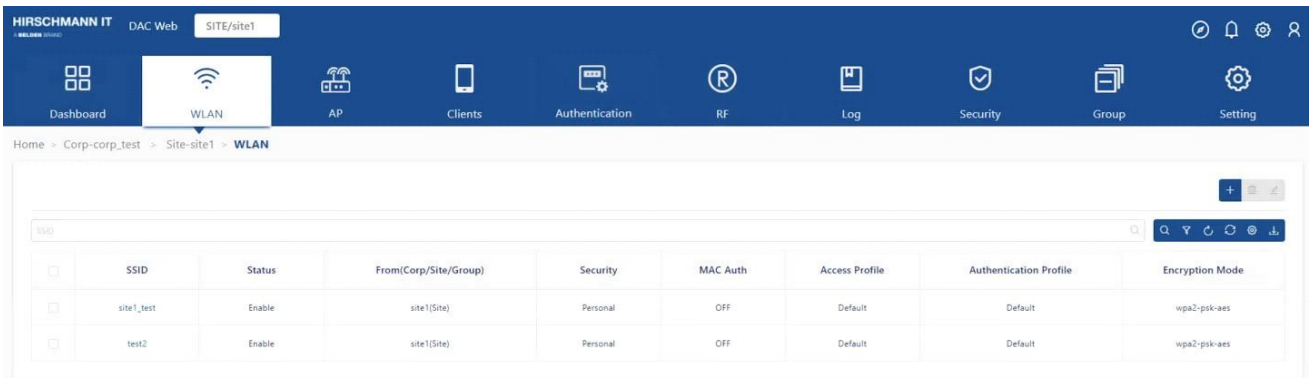


图 93：WLAN 页面

在启动过程中，无线客户端会搜索来自最近的DAP的无线电信号或信标帧。在定位到DAP后，客户端和DAP之间进行以下交互：

- **WLAN Access Authentication**：当无线客户端尝试连接DAP时，DAP需要对客户端进行相应的身份验证。身份验证方法取决于WLAN安全级别和MAC身份验证状态。
- **WLAN Connection**：WLAN接入认证成功后，客户端与DAP建立连接。
- **Network Access (Captive Portal) Authentication**：客户端连接DAP后，可根据需要进一步发起强制登录页身份验证。这一步并非必需步骤。

本章包含下列主题：

5.1 安全级别

- ► **Open**：没有任何安全配置的Wi-Fi。
- ► **Personal**：密钥保护Wi-Fi。DAP通过验证口令来对客户端进行身份验证。
- ► **Enterprise**：认证服务器通过802.1x认证对连接客户端进行身份验证。

5.2 MAC 身份验证

MAC身份验证是根据设备的物理介质访问控制（MAC）地址进行身份验证。MAC身份验证虽然不是最安全和可扩展的方法，但它为身份验证设备隐含地提供了额外的安全层级。通常，基于MAC的认证用于对特定设备进行认证并允许其访问网络，同时拒绝其他设备的访问。

5.3 创建 WLAN

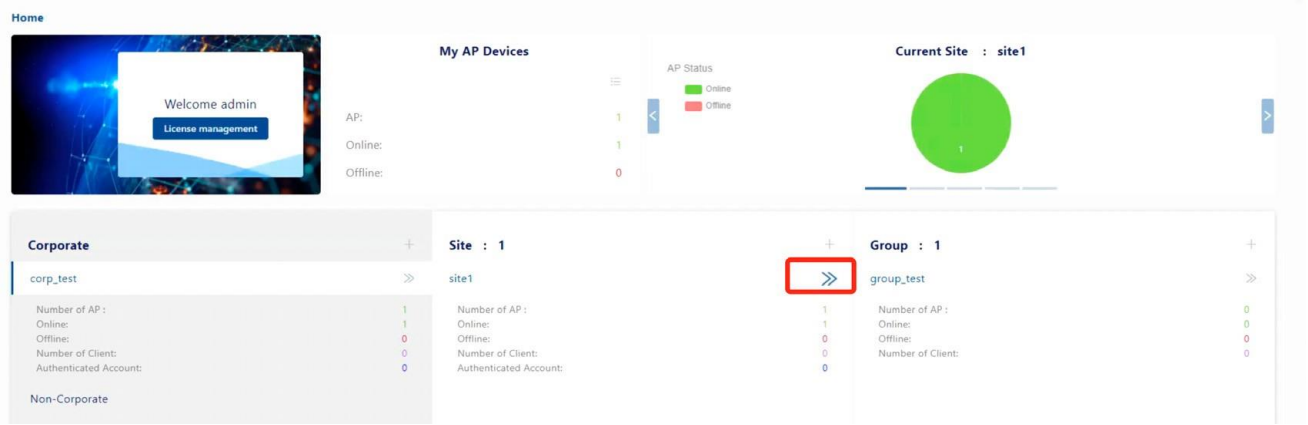


图 94：Home page

- 点击“**>>**”图标进入“**Site**”视图。
- 点击“**WLAN**”选项卡进入“**WLAN**”列表页面。

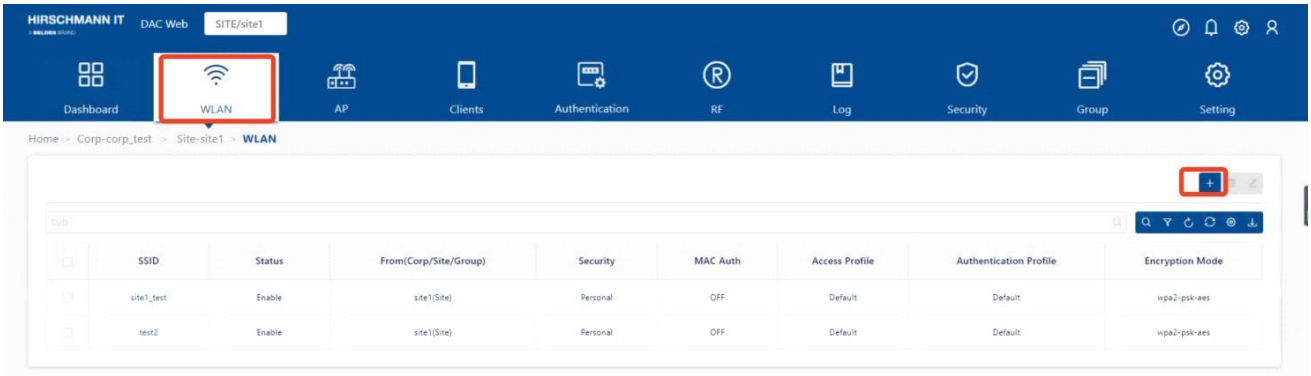


图 95：WLAN 列表

- 在“Site”或“Group”视图的WLAN选项卡上，点击WLAN列表表头上的“**+**”图标，打开“**Create WLAN**”窗口。

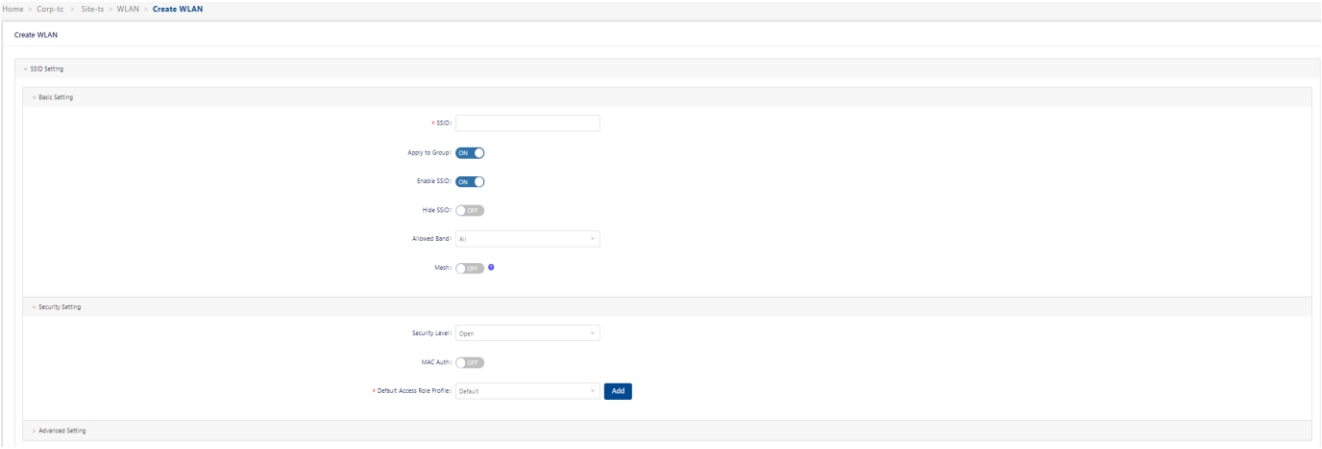


图 96：WLAN 窗口

5.3.1 SSID 设置

■ **Basic setting**

► **SSID**：用户配置的唯一标识无线网络的名称（最多32个字符）。如果SSID包含空格，则必须用引号括起来。

► **Apply to Group**：启用或禁用分配给该Group的WLAN。

► **Enable SSID**：启用或禁用SSID。

► **Hide SSID**：启用或禁用信标帧中的SSID。默认值为禁用。

注意：隐藏SSID对提高安全性几乎没有帮助。

► **Allowed Band**：服务中可用的频段：

- 2.4G Hz
- 5G Hz
- All，包含5G Hz和2.4G Hz（默认值）

► **Mesh**：为基于Mesh的车地链路快速切换启用或禁用SSID。启用Mesh后，只能选择WPA2_PSK_AES、WPA3_SAE_AES、WPA2_AES或WPA3_AES加密模式。仅在DAP847-A上生效。

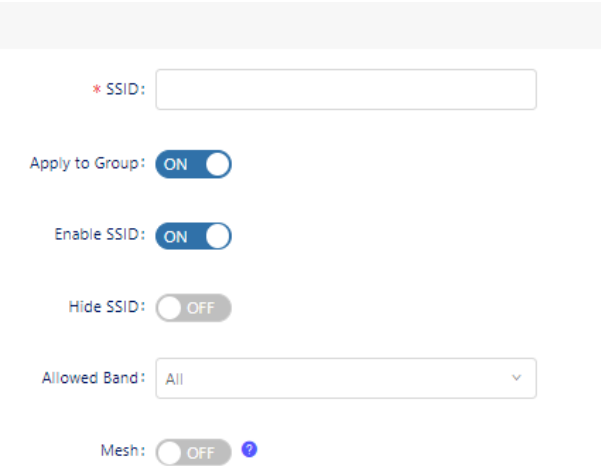


图 97：WLAN 基本设置

■ Security setting

- ► **Security Level：**选择WLAN服务的安全级别。
- ► **Open：**未加密的Wi-Fi。
  要为客户端分配角色，可配置默认角色或启用MAC身份验证。
- ► **MAC Auth：**启用或禁用MAC身份认证。
- ► **Authentication Profile：**
  - **Default：**简单快捷的配置方法。
    选择Default可以为当前的SSID选择访客或员工的Web Portal身份验证，或者为Company Device设置访问SSID。
  - **Customization：**需要手动创建访问策略、认证策略，访客接入策略或员工接入策略。请参阅第141页的“身份验证”。
- ► **Customization Page：**选择用于Web门户验证的模板页面，并根据需要进行自定义。只能在身份验证类型设置为“Guest”或“Employee”时才可设置。

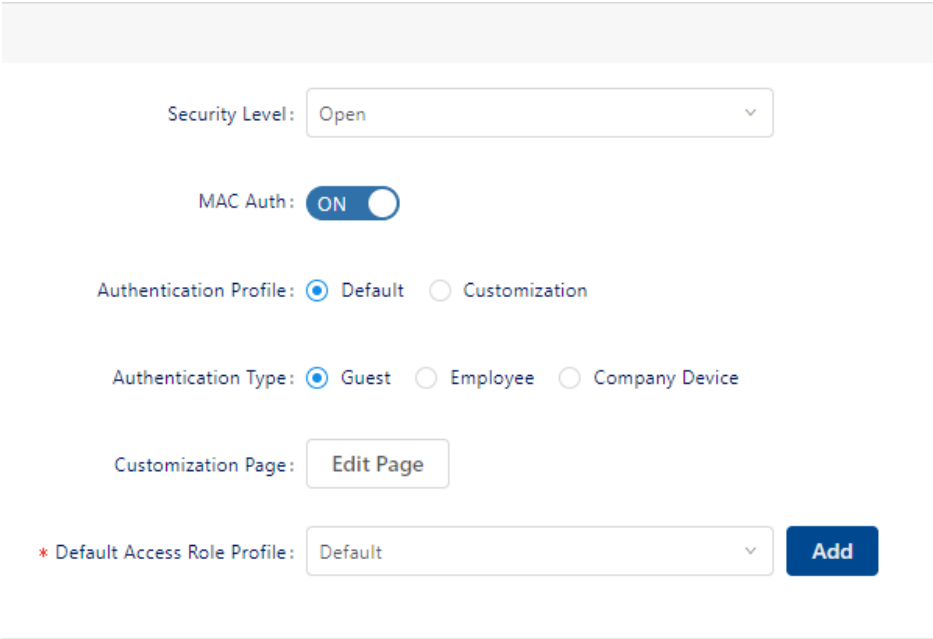


图 98：安全设置-“Open”安全级别

- **Personal**：通过密钥保护Wi-Fi。
- **Encryption Mode**：从下拉列表中选择一种加密模式，然后填入密码。
  - **WPA_PSK_AES**：使用预共享密钥进行AES加密的WPA。
  - **WPA_PSK_AES_TKIP**：使用预共享密钥进行TKIP和AES混合加密的WPA。
  - **WPA2_PSK_TKIP**：使用预共享密钥进行TKIP加密的WPA2。
  - **WPA2_PSK_AES**：使用预共享密钥进行AES加密的WPA2。
  - **WPA3_SAE_AES**：使用预共享密钥进行AES加密的WPA3，仅允许WPA3兼容客户端访问。
  - **WPA3_PSK_SAE_AES**：WPA3和WPA2混合模式，允许WPA3和WPA2兼容客户端访问。
- **PMF-Protected Management Frames**：配置是否接受来自支持特定安全级别或加密类型的受保护管理帧的客户端连接（企业：WPA2_AES/WPA3_AES256/WPA3AES，个人：WPA2_PSK_AES/WPA3_SAE_AES/WPA3_PSK_SAE_AES）。
  - **Disabled**：禁用受保护管理帧要求。WPA3加密需要启用受保护的管理帧，无法禁用。WPA3加密的字段不可配置。
  - **Optional**：允许来自支持受保护管理帧和不支持受保护管理帧的客户端的连接。
  - **Required**：仅允许来自支持受保护管理帧的客户端的连接。

- **Enter Password**：终端连接ESSID的密码。
- **Confirm Password**：再次输入密码。
- **Device Specific PSK**：设备特定PSK比传统PSK具备更高的安全性。如果在无线网络上启用了设备特定PSK，且设备已配置了设备特定PSK，则AAA服务器会为该设备发送用于MAC身份验证的Radius接入接受响应，并根据设备的MAC地址来发送该设备的特定预共享密钥。这意味着每个设备都会有一个不同的密钥。您可以在Company device页面上为特定的MAC地址设置设备特定PSK。
  - **Disabled**：禁用设备特定PSK。
  - **Prefer Device Specific PSK**：AAA服务器始终使用首选设备特定PSK。如果AAA服务器随Radius接入接受响应一起发送**“AES-CBC-128”**属性，则将使用此值。如果AAA服务器没有发送**“AES-CBC-128”**属性，则将使用在SSID中配置的密钥。
  - **Force Device Specific PSK**：返回“AES-CBC-128”属性的值，无论其是否存在。设备特定PSK无法与外部RADIUS服务器配合使用。该设备在Company device页面上已配置了设备特定PSK。
- **Authentication Profile**：
  - **Default**：简单快捷的配置方法。
    选择Default只可以为Company Device设置访问SSID。
  - **Customization**：需要手动创建访问策略、认证策略，访客接入策略或员工接入策略。请参阅第141页的“身份验证”。

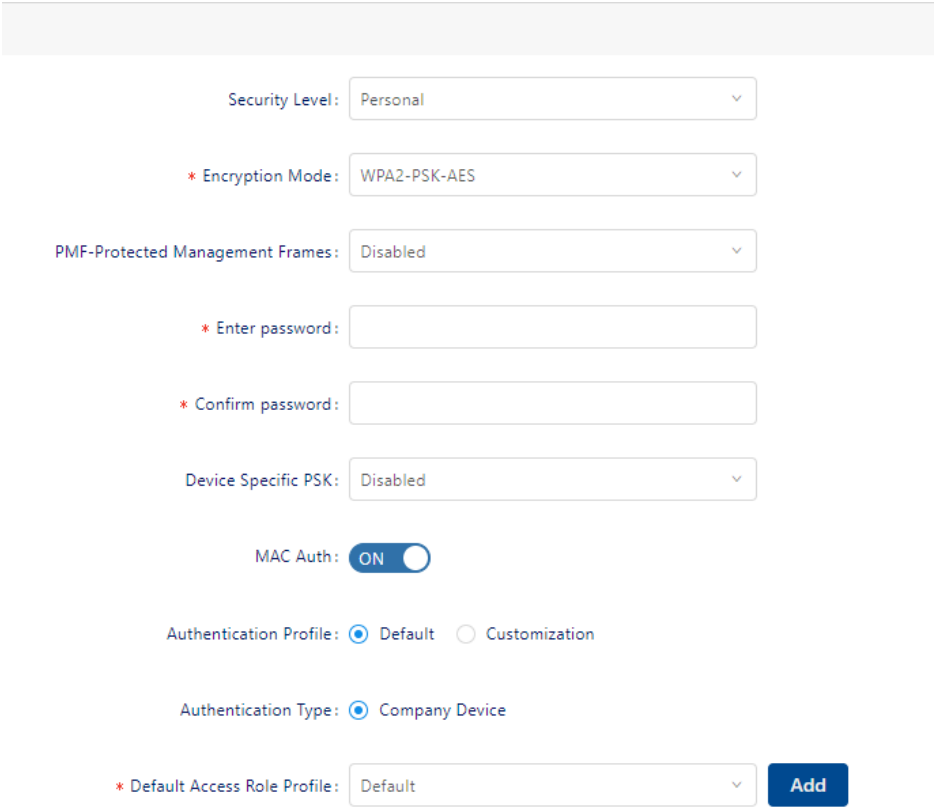


图 99：安全设置-“Personal”安全级别

- **Enterprise**：认证服务器通过802.1x认证对连接客户端进行身份验证。
- **Encryption Mode**：从下拉列表中选择一种加密类型。
  - **DYNAMIC_WEP**：具有动态密钥的WEP。
  - **WPA_TKIP**：使用802.1X进行TKIP加密和有动态密钥的WPA。
  - **WPA2_TKIP**：使用802.1X进行TKIP加密和有动态密钥的WPA2。
  - **WPA2_AES**：使用802.1X进行AES加密和有动态密钥的WPA2。
  - **WPA3_AES256**：使用802.1X进行CNSA（Suite B）加密的WPA3。
    注意：当将WPA3_AES256加密应用到不支持它的AP时，加密将自动回退到WPA2_AES。
  - **WPA3_AES**：使用802.1X进行AES加密和有动态密钥的WPA3。
- **Default Access Role Profile**：选择默认访问角色配置文件，如果其他角色分配方法无法分配角色给客户端，将应用该默认配置文件。请参阅第147页的“访问角色配置文件”。
- **Authentication Profile**：
  - **Default**：简单快捷的配置方法。

选择Default则可以为当前的SSID选择访客或员工的Web Portal身份验证，或者为Company Device设置访问SSID。

- **Customization**：需要手动创建访问策略、认证策略，访客接入策略或员工接入策略。请参阅第141页的“身份验证”。
- **MAC Auth**：启用或禁用MAC身份认证。只有当**Authentication Profile**选择**Customization**时适用。

► **Authentication Source**：只能在认证配置文件设置为默认时设置。

- **Local Database**：此SSID用于访客接入。
- **External LDAP/AD**：此SSID用于员工权限。
- **External Radius**：为公司拥有的设备设置此SSID，可分配给员工进行日常使用（例如打印机、IP电话、笔记本电脑、平板电脑）。它基于MAC身份验证。可以在Authentication→Setting→Company Device中添加公司设备MAC。请参阅第184页的“公司设备”。

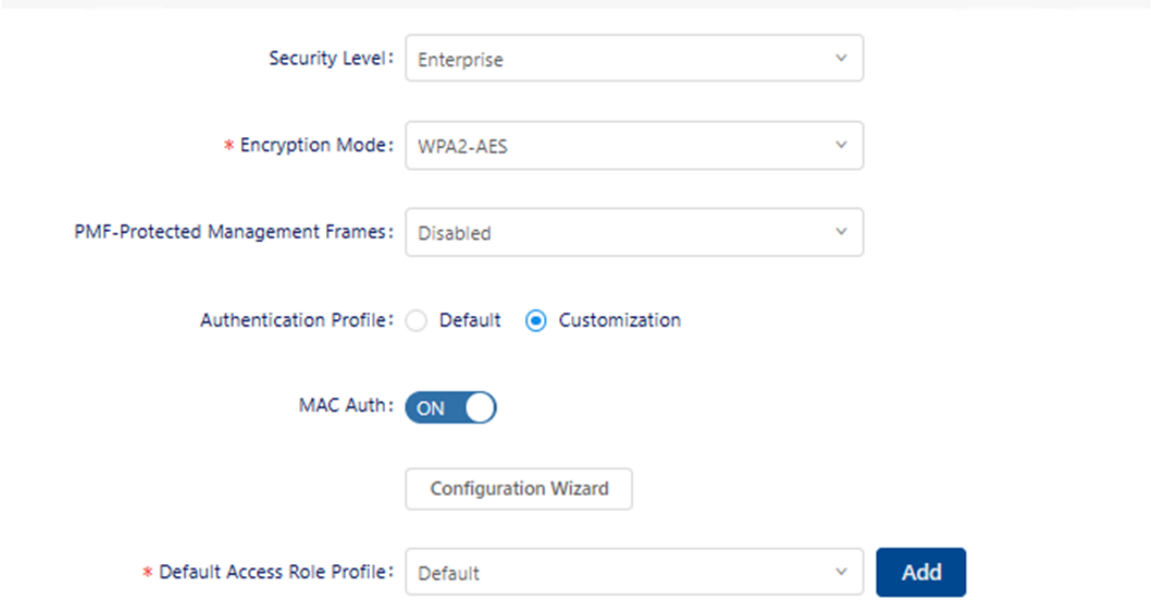


图 100：安全设置-“Enterprise”安全级别

■ Advance setting

► **Maximum clients allowed of single AP of this WLAN**：单个AP和单个频段下允许的最大客户端数量。当前AP的当前SSID下的最大终端数量（可选值：1..256，默认值：64）

- **WLAN Timing**：通过时间控制WLAN广播SSID。打开开关后，将看到更多的子选项。
  - **WLAN Work Cycle**：
    - **Daily**：WLAN每天广播此SSID。
    - **Weekday**：WLAN每个工作日广播此SSID。
    - **Weekend**：WLAN每个周末广播此SSID。
  - **Custom WLAN work schedule**：启用或禁用配置特殊的时间范围。
  - **WLAN work schedule**：选择时间范围。
- **802.11r**：启用或禁用IEEE 802.11r（快速基本服务集转换）。快速基本服务集（BSS）转换机制可最大限度地减少客户端从同一分组内的一个BSS过渡到另一个BSS时的延迟。
- **User Access Limit of 802.11b/g**：仅允许客户端以802.11b/g模式连接。（偶尔用于调试）
- **L3 Roaming**：启用或禁用第3层漫游。
  - 第3层漫游允许客户端在接入点之间移动，并连接到新的IP子网和VLAN。
- **Client Isolation**：启用或禁用客户端隔离。
  - 如果启用，则会阻止同一AP中SSID上的客户端之间的流量。客户端流量只能流向路由器。（默认：禁用）
- **802.11k**：启用或禁用802.11k。
  802.11k协议使AP和客户端能够动态测量可用的无线资源。当启用802.11k时，AP和客户端会互相发送邻居报告、信标报告和链路测量报告。
- **802.11v**：启用或禁用802.11v。
  - 802.11v标准定义了无线网络管理增强和BSS转换管理的机制。它允许客户端设备交换有关网络拓扑和射频环境的信息。BSS转换管理机制使得DAP可以要求语音客户端转换到特定的AP，或者由于网络负载均衡或BSS终止而向客户端建议一组首选AP。它还帮助客户端在漫游时识别最佳的AP进行转换。
- **2.4G Data Frame Rate**：数据速度较低的2.4G频段客户端将无法获得访问权限。推荐值为12。
- **2.4G Manage Frame Rate**：2.4G频段无线管理帧的传输速率。较高的值意味着覆盖范围较小，较低的值意味着覆盖范围较大。
- **5G Data Frame Rate**：数据速度较低的5G频段客户端将无法访问。推荐值为24。

► **5G Manage Frame Rate**：5G频段无线管理帧传输速率。较高的值意味着覆盖范围较小，较低的值意味着较大的覆盖范围较大。

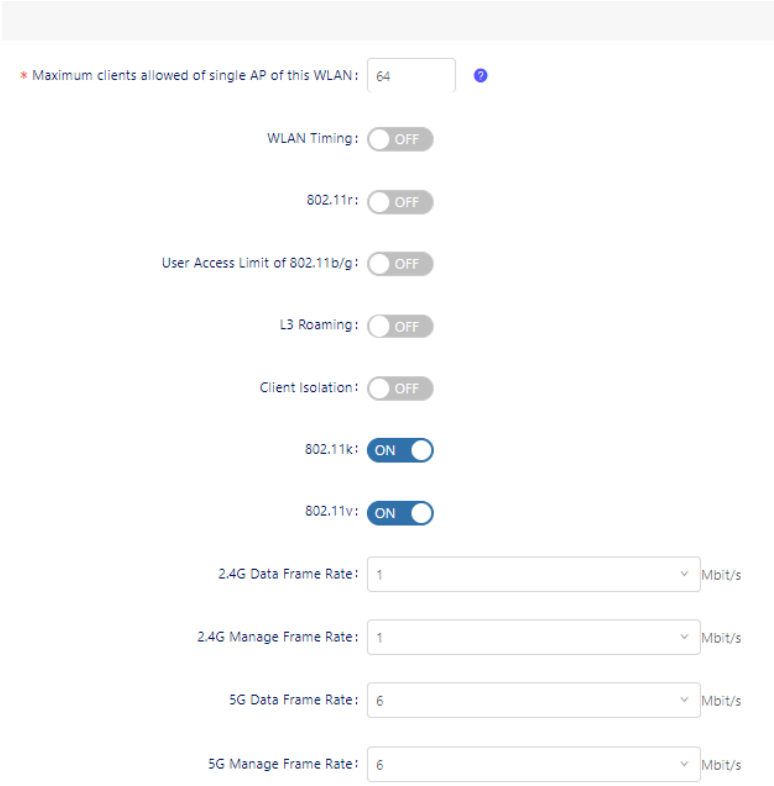


图 101：高级设置

5.3.2 QoS 设置

按照以下详细说明，对配置文件的无线QoS设置进行配置。

■ **Bandwidth contract**

► **Upstream Bandwidth**：从客户端到AP的最大流量带宽。

► **Downstream Bandwidth**：从AP到客户端的最大流量带宽。

► **Upstream Burst**：从客户端到AP的流量所使用的最大流量桶大小。流量桶大小决定了在最大带宽速率上可以突发多少流量。

► **Downstream Burst**：用于从AP到客户端的流量所使用的最大桶大小。流量桶大小决定了在最大带宽速率上可以突发多少流量。

图 102：带宽协议

■ 802.1p mapping setting

用于配置Wi-Fi多媒体（WMM）接入类别和802.1p优先级之间的上行和下行映射机制。上行流量只能映射到一个值。下行流量可以映射到多个值。字段使用默认值填充。

- ☐ 要修改默认上行链路值，请在字段中填入新值。
- ☐ 要修改默认下行链路值，请在字段中填入新值。
- ☐ 要删除一个值，请点击该值旁边的“**x**”。

► **Enable**：如果启用，则信任流量的原始802.11p映射。（默认值：禁用）

► **Background**：将WMM后台映射到802.1p值。

- **Uplink**：映射上行链路流量（从AP到WAN网络）。（可选值：0..7，默认值：1）
- **Downlink**：映射下行链路流量（从WAN网络到AP）。（可选值：0..7，默认值：1，2）

► **Best Effort**：将WMM最佳努力模式映射到802.1p值。

- **Uplink**：映射上行流量（从AP到WAN网络）。（可选值：0..7，默认值：0）
- **Downlink**：映射下行流量（从WAN网络到AP）。（可选值：0..7，默认值：0，3）

► **Video**：将WMM视频映射到802.1p值。

- **Uplink**：映射上行流量（从AP到WAN网络）。（可选值：0..7，默认

值：4）

- **Downlink**：映射下行流量（从WAN网络到AP）。（可选值：0..7，默认值：4，5）

► **Voice**：将WMM语音映射到802.1p值。

- **Uplink**：映射上行流量（从AP到WAN网络）。（可选值：0..7，默认值：6）
- **Downlink**：映射下行流量（从WAN网络到AP）。（可选值：0..7，默认值：6，7）

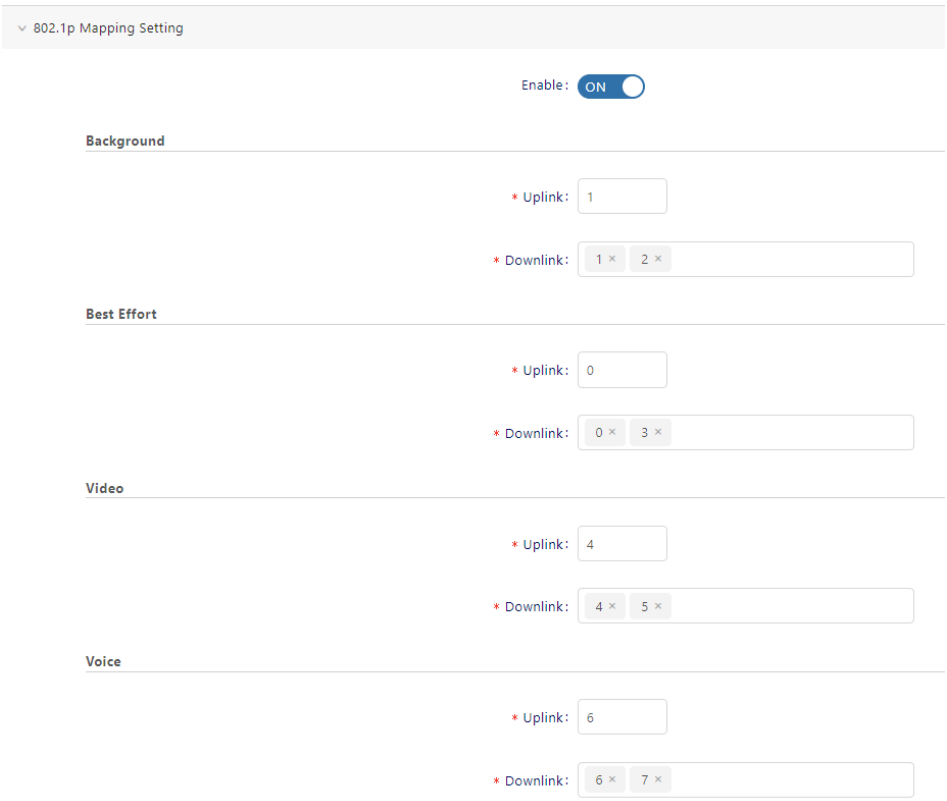


图 103：802.1p 映射设置

■ DSCP mapping settings

用于配置Wi-Fi多媒体（WMM）接入类别和DSCP优先级之间的上行和下行映射机制。上行流量只能映射到一个值。下行流量可以映射到多个值。字段使用默认值填充。

☐ 要修改默认上行链路值，请在字段中填入新值。
☐ 要修改默认下行链路值，请在字段中填入新值。

☐ 要删除一个值，请点击该值旁边的**“x”**。

► **Enable**：如果启用，则信任流量的原始DSCP映射。（默认值：禁用）

► **Background**：将WMM后台映射到DSCP值。

- **Uplink**：映射上行流量（从AP到WAN网络）。（可选值：0..63，默认值：10）
- **Downlink**：映射下行流量（从WAN网络到AP）。（可选值：0..63，默认值：2，10）

► **Best Effort**：将WMM最佳努力模式映射到DSCP值。

- **Uplink**：映射上行流量（从AP到WAN网络）。（可选值：0..63，默认值：0）
- **Downlink**：映射下行流量（从WAN网络到AP）。（可选值：0..63，默认值：0，18）

► **Video**：将WMM视频映射到DSCP值。

- **Uplink**：映射上行流量（从AP到WAN网络）。（可选值：0..63，默认值：40）
- **Downlink**：映射下行流量（从WAN网络到AP）。（可选值：0..63，默认值：24，36，40）

► **Voice**：将WMM语音映射到DSCP值。

- **Uplink**：映射上行流量（从AP到WAN网络）。（可选值：0..63，默认值：46）
- **Downlink**：映射下行流量（从WAN网络到AP）。（可选值：0..63，默认值：46，48，56）

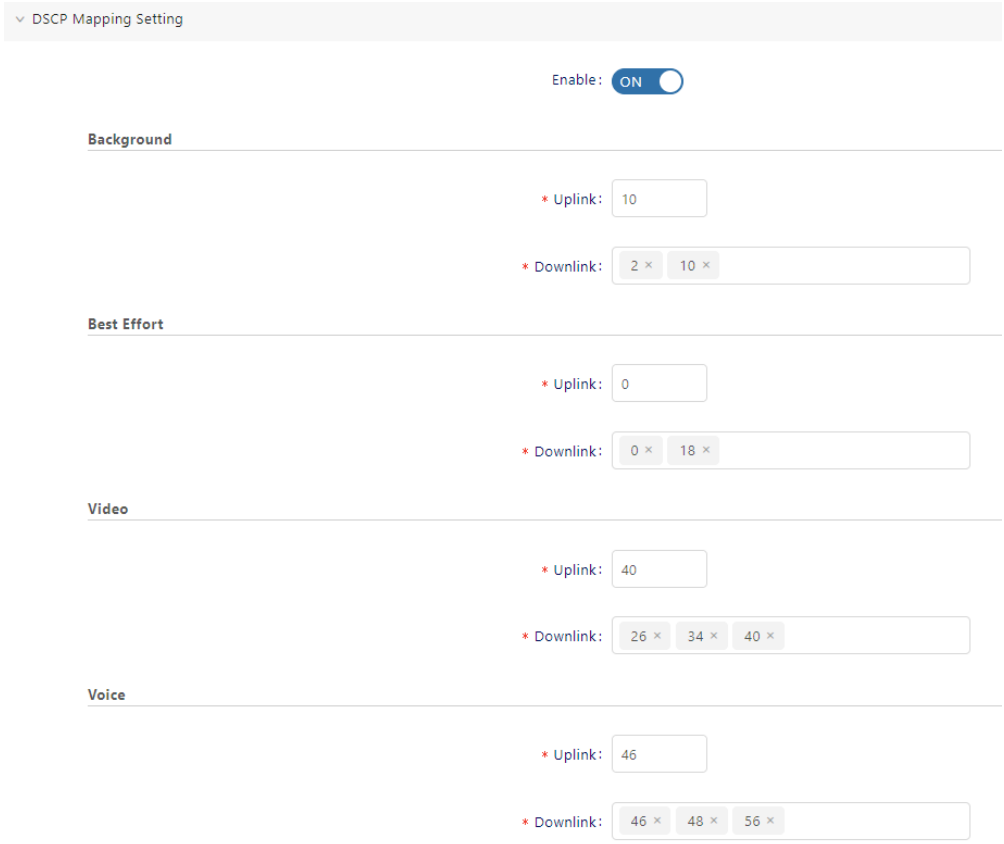


图 104：DSCP 映射设置

5.3.3 广播/组播优化设置

- **Broadcast Key Rotation**：启用或禁用广播密钥轮换功能。如果启用，则广播密钥在每个间隔后轮换。
- **Broadcast Key Rotation Time Interval**：轮换广播密钥的间隔以分钟为单位（可选值：1..1440，默认值：15）。
- **Broadcast Filter All**：启用或禁用广播过滤。如果启用，则除了DHCP和地址解析协议（ARP）帧之外，所有广播帧都会被丢弃。
- **Broadcast Filter ARP**：启用或禁用ARP的广播过滤。如果启用，则AP充当**“ARP代理”**。如果ARP请求数据包请求客户端的MAC地址，并且AP知道客户端的MAC和IP地址，则AP会响应ARP请求，但不会将ARP请求（广播）转发到所有广播域。这减少了ARP广播数据包的转发，显著提高了网络性能。

  注意：AP不会作为Gratuitous ARP数据包的ARP代理。当站点从DHCP获取IP地址或释放/更新IP时，它将发送Gratuitous ARP数据包。AP不响应此类特殊ARP数据包，而是正常广播。

- **Multicast Optimization**：启用或禁用组播流量速率优化。
- **Multicast Based Channel Utilization**：基于信道利用率优化百分比来配置组播。（可选值：0..100，默认值默认值：90）
- **Number of Clients**：配置组播优化的阈值。这是高吞吐量的最大客户端数量。

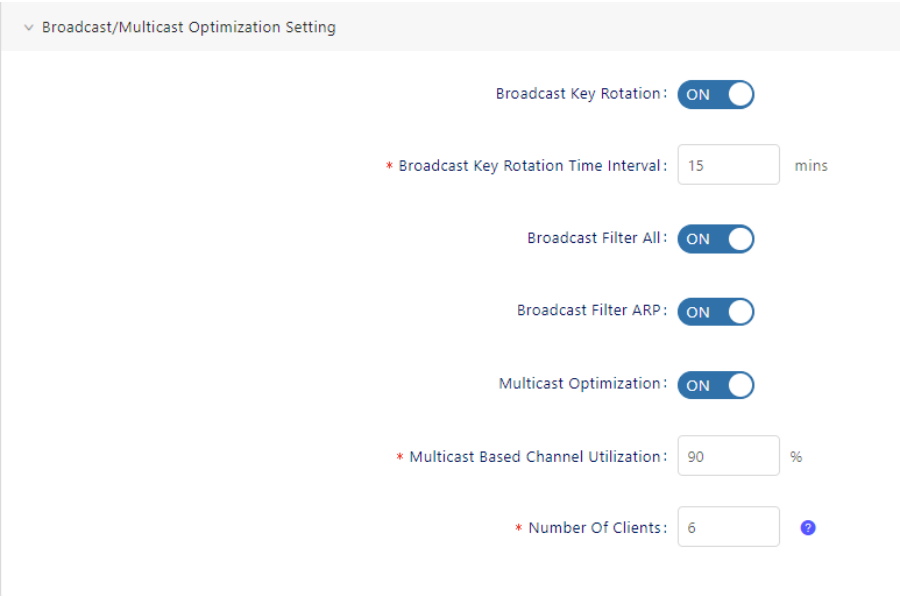


图 105：广播/组播优化设置

5.4 编辑 WLAN

- ☐ 从WLAN列表中选择WLAN。
- ☐ 点击**Edit**图标，打开“**Edit WLAN**”界面。
- ☐ 编辑需要更改的字段。
- ☐ 点击“**Effect Now**”按钮将更改保存到服务器。

5.5 删除 WLAN

- ☐ 从WLAN列表中选择WLAN。
- ☐ 点击“**Delete**”图标。
- ☐ 在确认提示上单击“**Yes**”。将从服务器上删除配置文件。

6 AP

AP界面显示分配给Site的所有DAP的信息，可用于配置AP的NTP，更新AP的固件，重启AP，设置AP的LED模式，并对AP执行特定操作（例如，打开设备的Web UI以管理单个AP，执行一些操作，如ping或trace）。

☐ 点击**“>>”**图标进入**“Site”**视图。

图 106：主页

☐ 点击**“AP”**图标，将显示**“AP”**界面。

本章包含下列主题：

- ► 设备列表
- ► 配置AP
- ► 配置蓝牙
- ► 报告配置
- ► 操作工具
- ► 从AP执行操作
- ► 设备连接记录

6.1 设备列表

此列表显示Site上的所有AP设备，可以根据AP的基本功能（无线WLAN和蓝牙Bluetooth）对设备进行筛选。

- **All Devices**：该表显示了Site上的所有设备。
- **Devices with WLAN**：该表显示具有WLAN功能的设备。只有当Site上的设备有WLAN功能时显示。
- **Devices with Bluetooth**：该表显示具有蓝牙功能的设备。只有当Site上的设备有蓝牙功能时显示。
- **MAC**：设备的MAC地址。
- **Name**：设备名称。
- **Group**：设备所属的Group。
- **Firmware**：设备的固件版本。
- **Model**：设备的型号（例如，DAP640）。
- **License**：设备的许可证状态。如果禁用，则DAC不会将配置发送到DAP。所以，DAP不广播SSID。
- **IP**：设备的IP地址。
- **Status**：AP状态，可以是在线或离线。
- **Client Number**：当前按设备计算的客户端数量。由于数据报告间隔，与AP上实际客户端数量相比，计数会有所延迟。
- **Working Mode**：
  - **Normal Mode**：AP为无线客户端提供服务。
  - **Full Scan Mode**：在此模式下，AP下的所有无线电将不会广播SSID。
- **Location**：设备的位置。
- **Online Duration**：AP在线持续时间。
- **Last Offline Time**：设备最后一次断开连接的时间。

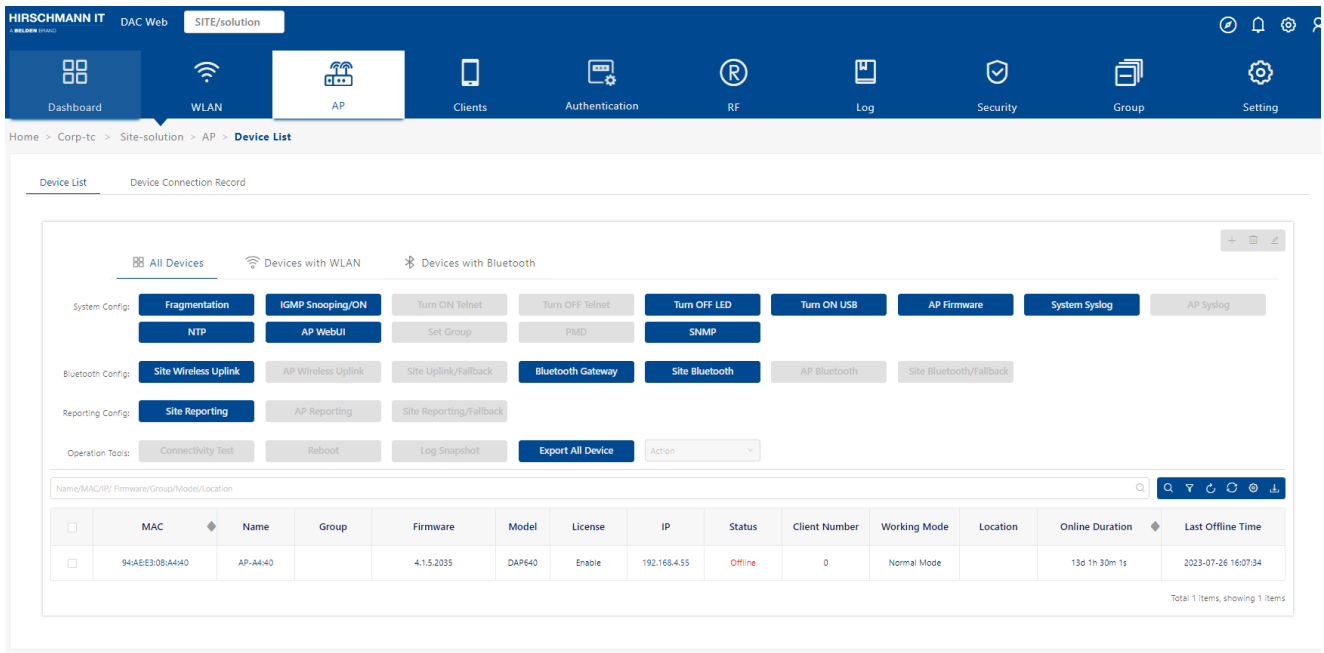

HIRSCHMANN IT
DAC Web
SITE/solution
Dashboard
WLAN
AP
Clients
Authentication
RF
Log
Security
Group
Setting
Home > Corp-tc > Site-solution > AP > Device List
Device List
Device Connection Record
All Devices
Devices with WLAN
Devices with Bluetooth
System Config:
Fragmentation
IGMP Snooping/ON
Turn ON Telnet
Turn OFF Telnet
Turn OFF LED
Turn ON USB
AP Firmware
System Syslog
AP Syslog
NTP
AP WebUI
Set Group
PMD
SNMP
Bluetooth Config:
Site Wireless Uplink
AP Wireless Uplink
Site Uplink/Fallback
Bluetooth Gateway
Site Bluetooth
AP Bluetooth
Site Bluetooth/Fallback
Reporting Config:
Site Reporting
AP Reporting
Site Reporting/Fallback
Operation Tools:
Connectivity Test
Reboot
Log Snapshot
Export All Device
Action
Name/MAC/IP/ Firmware/Group/Model/Location
MAC
Name
Group
Firmware
Model
License
IP
Status
Client Number
Working Mode
Location
Online Duration
Last Offline Time
94:AE:E3:08:A4:40
AP-A4:40
4.1.5.2035
DAP640
Enable
192.168.4.55
Offline
0
Normal Mode
13d 1h 30m 1s
2023-07-26 16:07:34
Total 1 items, showing 1 items

图 107：设备列表窗口

6.2 配置 AP

6.2.1 数据报分段

启用 UDP 数据包分段转发优化以避免设备负载过大。默认关闭。

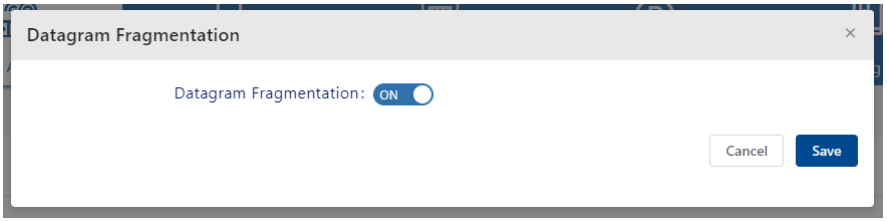


图 108：数据报分段

6.2.2 打开/关闭 IGMP Snooping

Internet 组管理协议（IGMP）是 IPv4 网络上主机和相邻路由器用于建立组播组成员资格的通信协议。IGMP 是 IP 组播的一个重要组成部分。IGMP 允许网络只向提出请求的主机发送组播信息。

IGMP Snooping 是监听 Internet 组管理协议（IGMP）网络流量的过程，目的是控制 IP 组播的传输。具有 IGMP Snooping 功能的网络交换机会监听主机和路由器之间的 IGMP 对话，并维护一个映射表，记录哪些链路需要哪些 IP 组播传输，以过滤掉不需要组播的链路，从而节省这些链接上的带宽。

- ☐ 点击**“IGMP Snooping/ON”**按钮以启用**“IGMP Snooping”**功能。
- ☐ 再次点击**“IGMP Snooping/ON”**按钮以禁用**“IGMP Snooping”**功能。

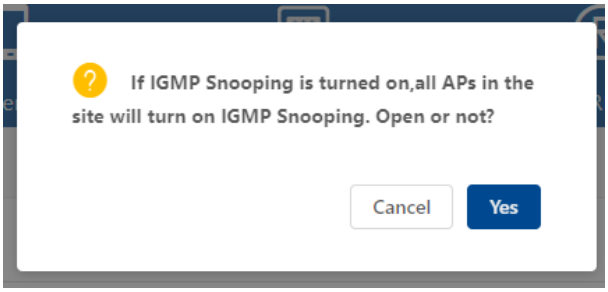


图 109：打开 IGMP Snooping

6.2.3 打开/关闭 Telnet

- ☐ 选择要启用Telnet的AP。
- ☐ 点击**“Turn On Telnet”**按钮。
- ☐ 在确认提示上单击**“Yes”**。将打开所选AP的Telnet功能。
- ☐ 无论当前Site中哪个AP的Telnet被启用，都会出现**“Turn Off Telnet”**按钮。点击**“Turn Off Telnet”**按钮后，当前Site中所有AP的Telnet都将被禁用。

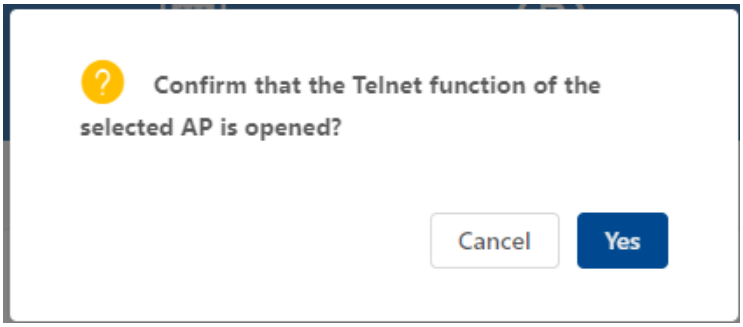


图 110：打开 Telnet

6.2.4 打开/关闭 LED

- ☐ 点击**“Turn On LED”**按钮打开LED灯。此设置对当前Site上的所有AP都有效。
- ☐ 点击**“Turn Off LED”**按钮关闭当前Site中所有AP的LED灯。

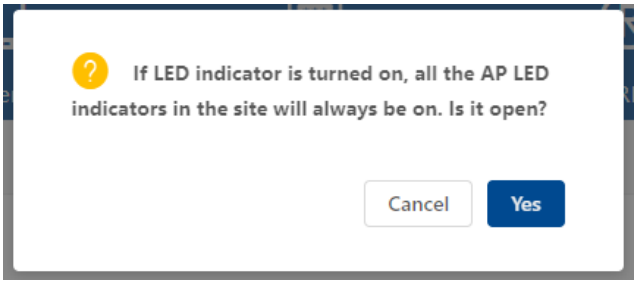


图 111：打开 LED

6.2.5 打开/关闭 USB

- ☐ 点击**“Turn On/Off USB”**按钮以启用或禁用设备上的USB端口。

此设置对当前Site上的设备都有效。此功能仅适用于具有USB接口的设备。

注：当电源供应不足时，设备上的USB接口可能无法打开。

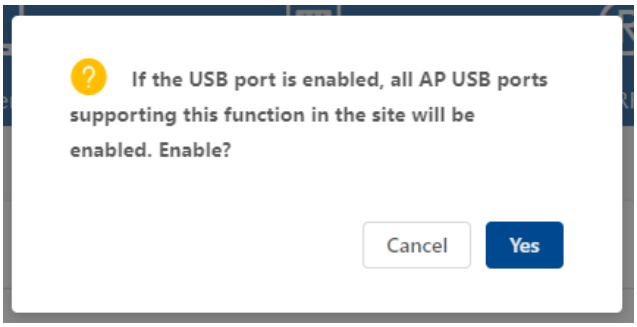


图 112：打开 USB

6.2.6 升级固件

- ☐ 点击“**AP Firmware**”按钮，打开“**AP Firmware**”窗口。
- ☐ 配置固件升级策略，可选择“**Smart Upgrade**”或“**Customization Upgrade**”。只能选择其中一种策略进行固件升级。

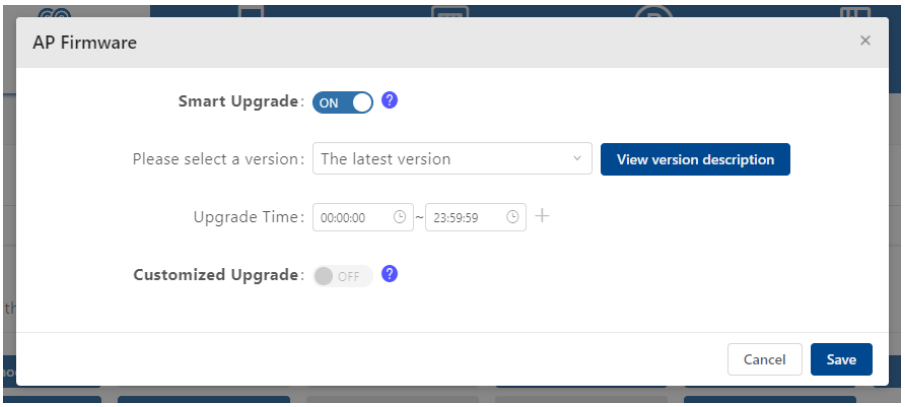


图 113：固件窗口

通常情况下，当DAC可以访问云端时，DAC会同步可用的DAP固件映像文件。如果您的部署环境不允许DAC访问云端，那么需从供应商处获取DAP固件并手动上传固件到DAC。请参阅第60页的“AP本地固件管理”。然后选择“**Smart Upgrade**”或“**Customization Upgrade**”，DAP将从DAC下载所需的固件进行升级。

- **Smart Upgrade**：您应该选择一个固件版本，并设置设备升级的时间段。通常情况下，应该选择最新版本，这意味着DAC将每天尝试从云端同步最新版本。根据智能升级的规则，它将自动根据用户的配置完成AP的固件升级。如果不确定选择哪个版本，可以联系供应商。一旦到达设置的升级时间段，当前Site中的所有设备将自动进行检查并升级至用户选择的版本。在同一时间，将有20个DAP执行版本下载和升级操作，其他设备则处于等待状态。如果升级时间段结束时，当前站点的设备未完成升级，则处于升级状态的设备将继续升级，而等待升级的设备将暂停升级，直到下一个允许升级的时间段到来。您可以在升级时间段列表中添加一天中的多个时间段，以避免使用设备。
- **Customization Upgrade**：自定义升级任务将仅在设定的时间点进行更新。设备升级后,任务会自动清除（仅一次）。如果设备升级失败，则需要手动执行下一次升级。这是与**Smart Upgrade**的主要区别。

6.2.7 配置设备系统日志

为了方便定位设备问题，需要将设备日志上传到指定的日志服务器。

☐ 点击**“System Syslog”**按钮设置当前 Site 下所有 AP 报告日志的地址，或者选中单个 AP 并点击**“AP Syslog”**按钮设置所选 AP 报告日志的地址。

- **Remote Log Switch**：打开或关闭记录设备日志到远程syslog服务器。
- **Remote Log Server Config**：默认表示记录到DAC中。自定义表示记录到手动设置的地方。
- **Remote Log Server**：远程syslog服务器地址。
- **Log Level**：发送的日志级别。

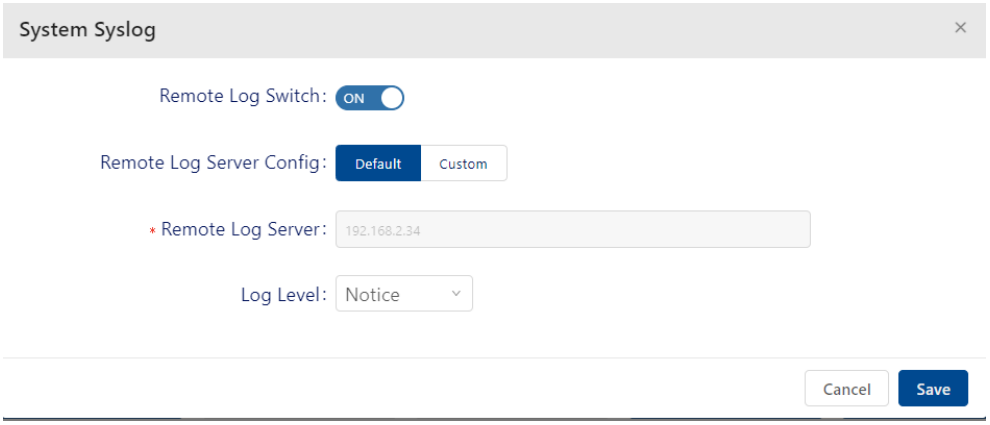


图 114：系统 Syslog

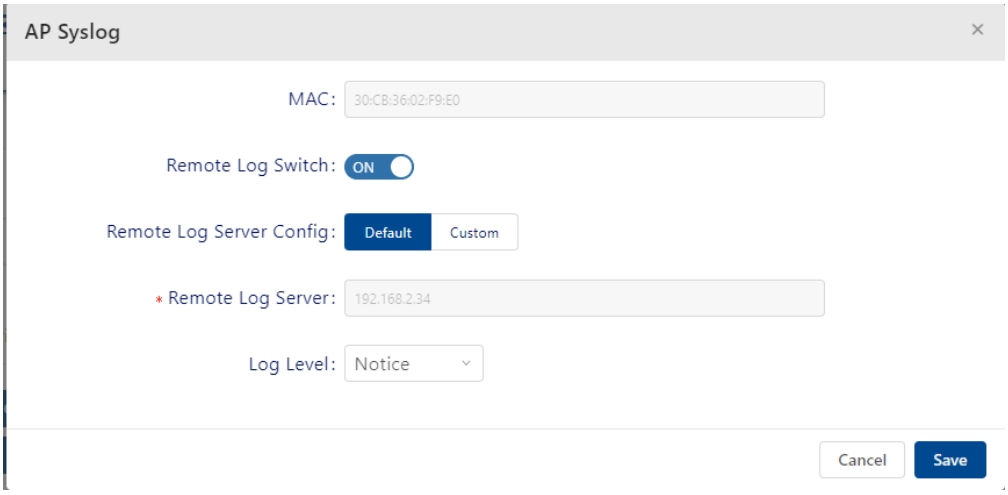


图 115：AP Syslog

6.2.8 配置设备的 NTP

网络时间协议（NTP）是一种网络协议，用于通过分组交换、可变延迟数据网络实现计算机系统之间的时钟同步。

- 单击**“NTP”**按钮，打开**“NTP Config”**窗口。
  - **Time Zone：**从下拉列表中选择一个时区。
  - **NTP Server：**输入**“NTP Server address”**。点击**“Add”**按钮将设备添加到NTP服务器列表中。DAC内置了一个NTP服务器。默认情况下，它会将此NTP服务器发送给当前Site的设备，以保持DAP和DAC之间的时间同步。
  - **NTP Server List：**当前已添加的NTP服务器列表。
- 点击**“Save”**按钮保存配置，并将这些配置应用于本Site上的设备。目前支持的版本是NTPv4。

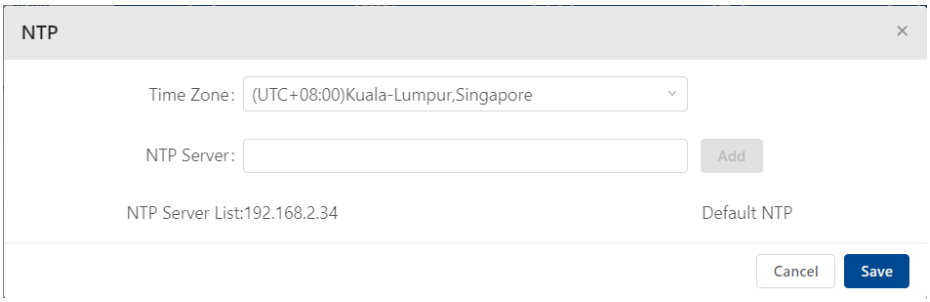


图 116：NTP

6.2.9 访问 AP Web UI

对于一些维护操作，需要直接访问 AP 设备的 Web UI 界面。

- ☐ 点击“**AP WebUI**”按钮，打开“**AP WebUI**”模块窗口。
  - ► **AP Page**：打开或关闭AP WebUI。
  - ► **Login Name**：登录名必须为“**administrator**”。
  - ► **Password**：管理员的密码。可使用此密码登录AP WebUI。
  - ► **Confirm password**：确认新密码。
- ☐ 点击**Save**按钮保存配置。
- ☐ 在设备列表中，点击“**IP Address**”以访问AP的WebUI。
- ☐ 输入“**Password**”登录到AP WebUI页面。

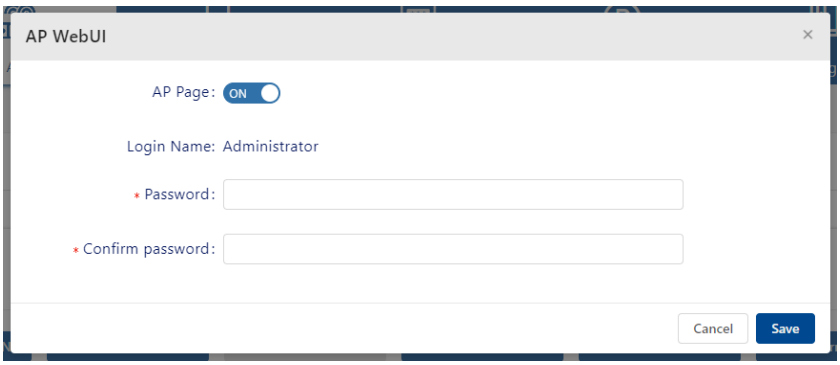


图 117：AP Web UI

6.2.10 分配 AP 到 Group

- ☐ 从设备列表中选择AP。
- ☐ 点击“**Set Group**”按钮，打开“**Set Group**”窗口。
- ☐ 从下拉列表中选择一个Group。
- ☐ 点击“**Next step**”按钮，信息确认视图打开。
- ☐ 点击“**Save**”按钮。然后，选择的AP将被分配到该Group。

如果要将AP分配到一个新Group，则应创建一个新Group。请参阅第33页的“创建新的Group”。

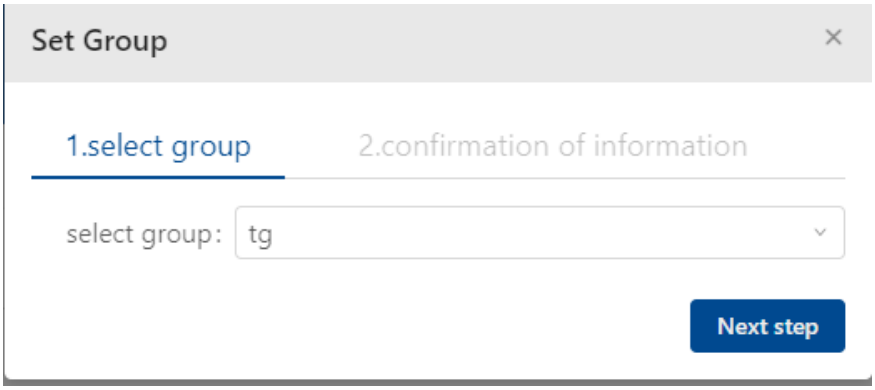


图 118：分配 AP 到 Group

6.2.11 配置 PMD

PMD是一种故障排除方法，有助于确定致命崩溃后内核转储和异常指针的根本原因。

如果启用并配置了PMD，当DAP上的关键进程崩溃时，DAP将立即向特定TFTP服务器发送PMD文件。默认情况下，禁用将PMD文件发送到到外部TFTP服务器。

- ☐ 从AP列表中选择要收集PMD文件的AP。
- ☐ 点击**“PMD”**按钮，打开**“PMD”**窗口。
- ☐ 打开**“Switch”**。
- ☐ 填入**“Server address”**，该地址是TFTP服务器地址。
- ☐ 点击**“Save”**按钮保存配置。

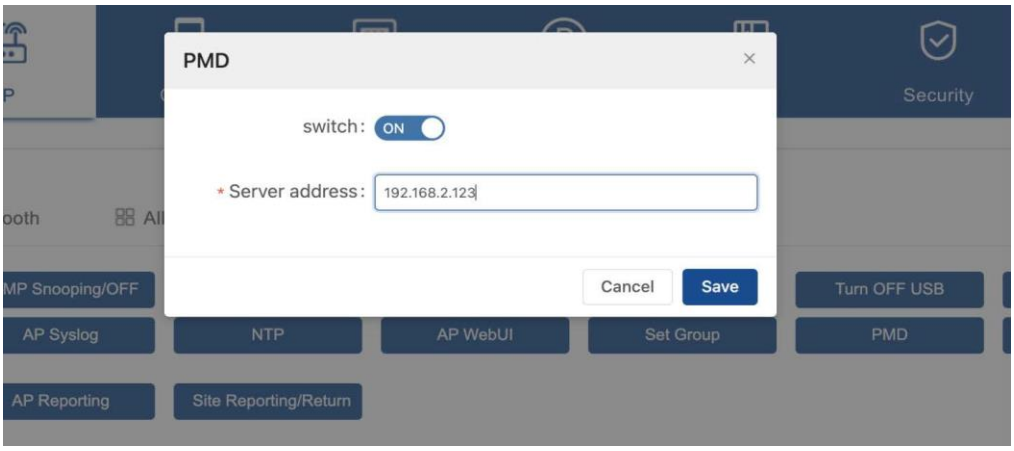


图 119：PMD 窗口

6.2.12 SNMP

SNMP是一种应用层协议，用于记录、存储和共享网络中支持SNMP的设备的信息，以便深入了解设备的工作情况。SNMP陷阱是代理向管理器发送的信息，会在预设事件发生时发送。

- ☐ SNMP配置在站点内的所有AP上生效。
- ☐ 点击“**SNMP**”按钮，打开“**Edit SNMP**”窗口。
  - ► **SNMP**：打开/关闭SNMP配置。
  - ► **Version**：SNMP的版本。支持V2c和V3。
  - ► **Community**：用于访问AP统计信息的社区字符串。
  - ► **Trap**：打开/关闭SNMP陷阱配置。
  - ► **Trap Server**：SNMP陷阱主机的IP地址。
  - ► **Username**：主机连接代理时使用的用户名。当Version设为V3时需要填入。
  - ► **Enter Password**：主机连接代理时用户使用的密码。当Version设为V3时需要填入。
  - ► **Confirm Password**：再次输入密码检查是否一致。当Version设为V3时需要填入。
  - ► **Trap List**：SNMP代理发送的事件类型。

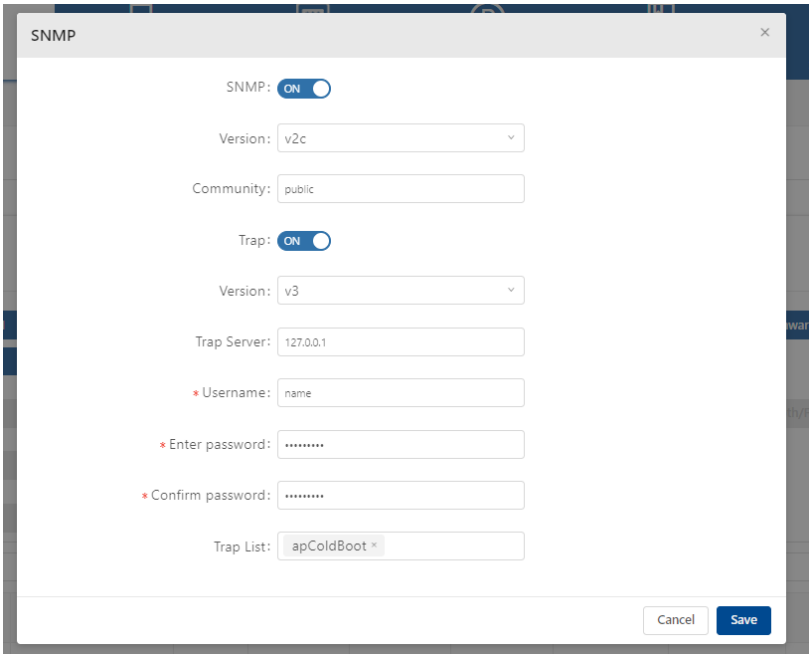


图 120：SNMP 窗口

6.3 配置蓝牙

6.3.1 蓝牙设置

可以配置整个Site蓝牙，或选择特定的AP进行私有蓝牙配置。AP的私有蓝牙配置优先于Site的整体配置。

- ☐ 选择AP。
- ☐ 点击“**Site Bluetooth/Fallback**”按钮以清除AP的独立蓝牙配置。这些AP将重用Site的蓝牙配置。
- ☐ 点击“**Site Bluetooth**”按钮，打开“**Bluetooth Configuration**”模块窗口或选择AP。
- ☐ 点击“**AP Bluetooth**”按钮，打开“**AP Bluetooth Configuration"**模块窗口。
  - ► **Bluetooth**：关闭蓝牙。如果打开，则Site中的所有蓝牙设备或所选设备都会打开蓝牙功能。
  - ► **Work Mode**：
    - **Scanner Mode**：启用“**Bluetooth beacon scanning**”功能。
    - **Advertise Mode**：启用“**BLE advertising**”功能。如果启用，则设备广播BLE数据包。
    - **Advertise & Scanner Mode**：同时启用“**Bluetooth beacon scanning**”和“**BLE advertising**”功能。

■ 扫描模式的详细信息

- ► **Scan Type**：
  - **Passive Scanning**：被动扫描。
  - **Active Scanning**：主动扫描。
- ► **Scan Interval**：AP的蓝牙扫描间隔，以毫秒为单位。（可选值：4..10240，默认值：100）
- ► **Scan Window**：每次扫描的持续时间，以毫秒为单位。（可选值：4..10240）
- ► **Scan Filter**：启用或禁用扫描过滤器。

■ 广播模式的详细信息

- ► **Broadcast Power**：用于广播BLE数据包的发射功率。（可选值：-20..-10，默认值：4）
- ► **Broadcast Frequency**：BLE数据包广播的时间周期，以毫秒为单位。（可选值：20..9,000,000，默认值：200）
- ► **Broadcast Channel**：用于广播BLE数据包的发射通道。
- ► **Beacon Mode**：指定用于定义广播BLE信标格式的BLE协议。
  - **iBeacon**：苹果iBeacon格式。
  - **Edyuid**：谷歌Eddystone格式。
    具有10字节命名空间组件和6字节实例组件的唯一静态ID。
    - **Namespace**：包含0-9、a-f的20个字符。
    - **Instance ID**：包含0-9，a-f的12个字符。
- ► **Edyurl**：谷歌Eddystone格式。压缩后的URL，一经解析和解压缩，客户端即可直接使用。
- ► **Plain_URL**：将被压缩的普通URL。

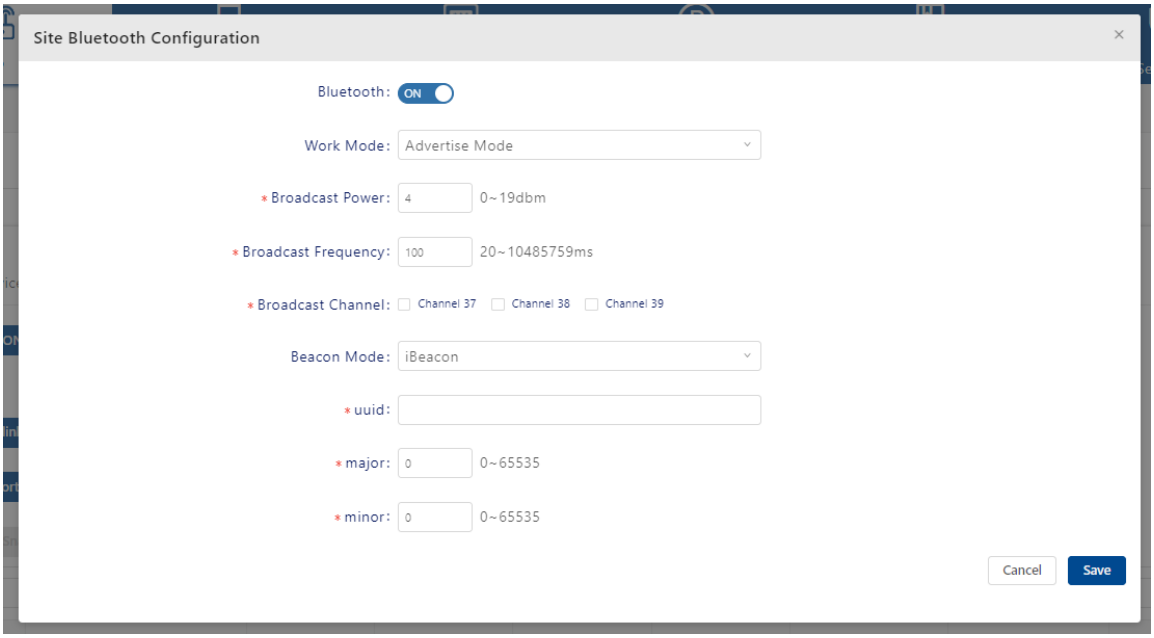


图 121：Site 蓝牙设置

6.3.2 配置蓝牙 WLAN 上行链路

有些设备包括WLAN和蓝牙模块。WLAN模块可以作为客户端连接到网络，用作设备管理或数据链路以完成设备注册、蓝牙信息报告等。

- ☐ 点击**“Site Wireless Uplink”**按钮，打开**“Site Bluetooth Wireless Uplink Configuration”**窗口。或者点击**“AP Wireless Uplink”**按钮，打开**“Bluetooth Wireless Uplink Configuration”**窗口。
- ☐ 点击**“Save”**按钮将配置应用于Site的蓝牙设备。
  - ► **Wireless Uplink：**开启/关闭WLAN上行链路。
  - ► **Mode：**Station（无法更改）。
  - ► **SSID：**将要连接的蓝牙设备的SSID。
  - ► **Security Level：**此蓝牙设备将连接的SSID的安全级别。可以是Open或Personal。
  - ► **Password：**当安全级别为Personal时，应设置密码。

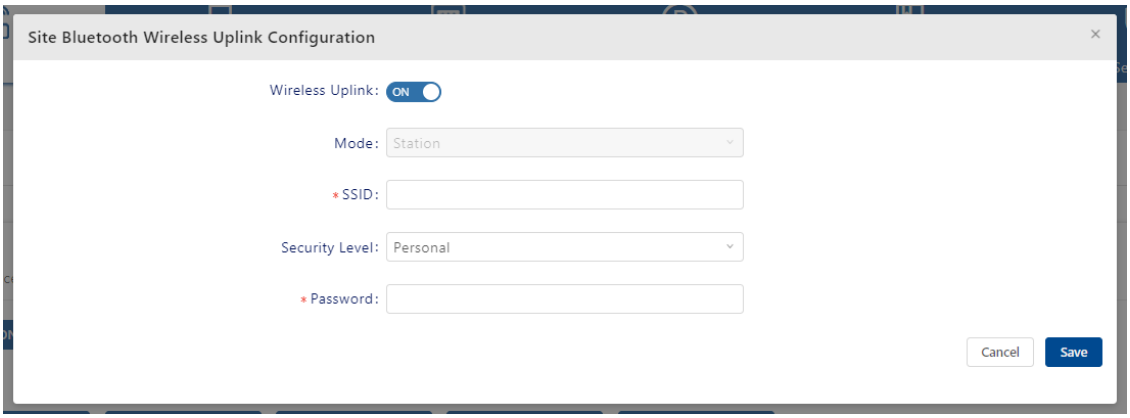


图 122：Site 蓝牙上行链路设置

6.4 报告配置

报告配置功能用于设置AP通过MQTT代理向第三方系统报告终端列表、RSSI等信息。第三方系统可以基于这些信息开发一些新的应用，比如室内定位等。

- ☐ 点击“**Site Reporting**”按钮，设置所有设备报告信息。
- ☐ 选择设备并点击“**AP Reporting**”按钮，设置选定设备报告信息。
  - ► **Service Switch**：启用或禁用Service Switch服务。
  - ► **Data Type**：选择蓝牙数据、Wi-Fi数据或两者都选。
  - ► **Advertise Address**：一对多广播地址。
  - ► **Bluetooth Topic**：使用Bluetooth Topic向MQTT代理发送消息。
  - ► **Advertise Type**：
    - **iBeacon**：苹果开发的iBeacon协议。该协议确定设备的物理位置，跟踪用户或在设备上触发基于位置的操作。
    - **Edyuid**：谷歌Eddystone格式。
      - 具有10字节命名空间组件和6字节实例组件的唯一静态ID。
    - **Edyurl**：谷歌Eddystone格式。压缩后的URL，一经解析和解压缩，客户端即可直接使用。
    - **Other**：其他广告类型。
  - ► **Group ID**：设备的Group ID。
  - ► **Access Key**：连接到MQTT代理的访问密钥。
  - ► **Secret Key**：连接到MQTT代理的密钥。
  - ► **Bluetooth Reporting Interval**：蓝牙消息的报告间隔（可选值：1..20）。
  - ► **Wifi Reporting Interval**：Wi-Fi消息的报告间隔（可选值：1..20）。
  - ► **Building ID**：建筑物ID。

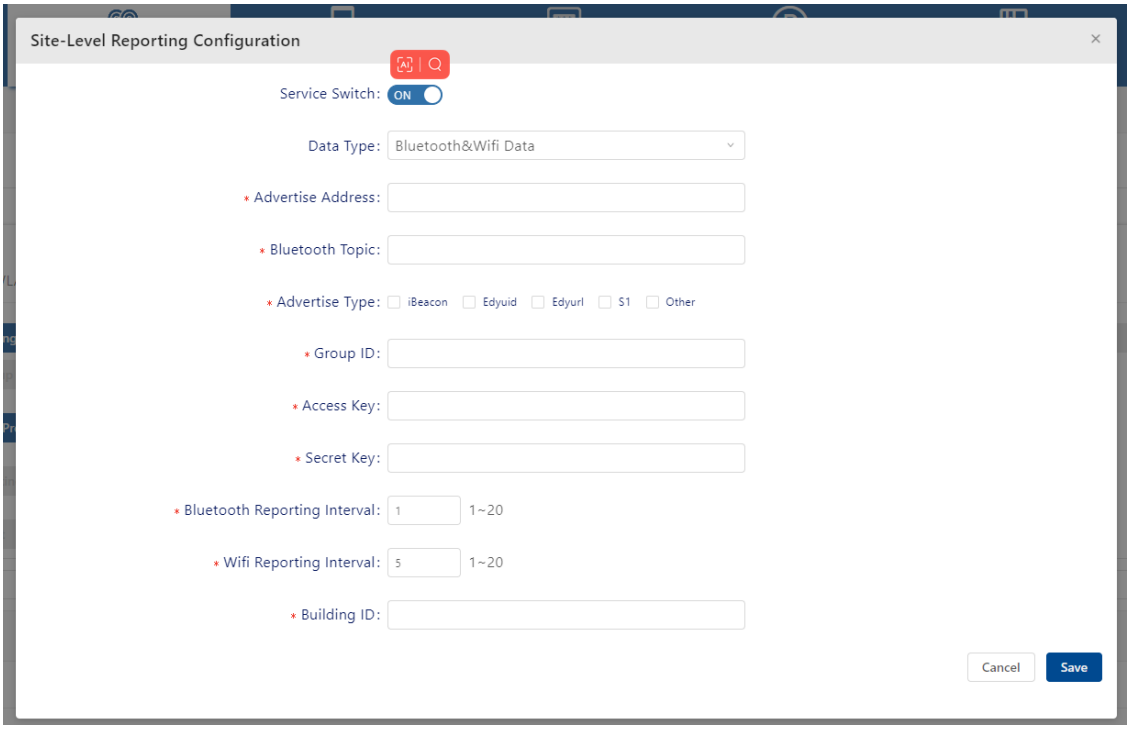


图 123：Site 报告配置

6.5 操作工具

操作工具提供一组小工具，方便用户进行简单的操作和维护操作。

6.5.1 连通性测试

测试所选设备是否可以通过ping命令从DAC访问。

- ☐ 选择一个或多个AP（不超过10个）。
- ☐ 单击“**Connectivity Testing**”按钮。“**Connectivity Testing**”对话框将在几秒钟内出现，带一个包含Ping结果的表格。
  - ► **AP MAC**：AP MAC地址。
  - ► **AP name**：AP的名称。
  - ► **AP IP**：AP的IP地址。
  - ► **AP status**：AP状态，在线或离线。
  - ► **Send number**：发出的ping包数量。
  - ► **Receiving number**：接收到的包数量。
  - ► **Package loss rate**：丢包率。
  - ► **Average latency**：平均延迟。
  - ► **Connectivity status**：网络连接状态，“最优”或“异常”。

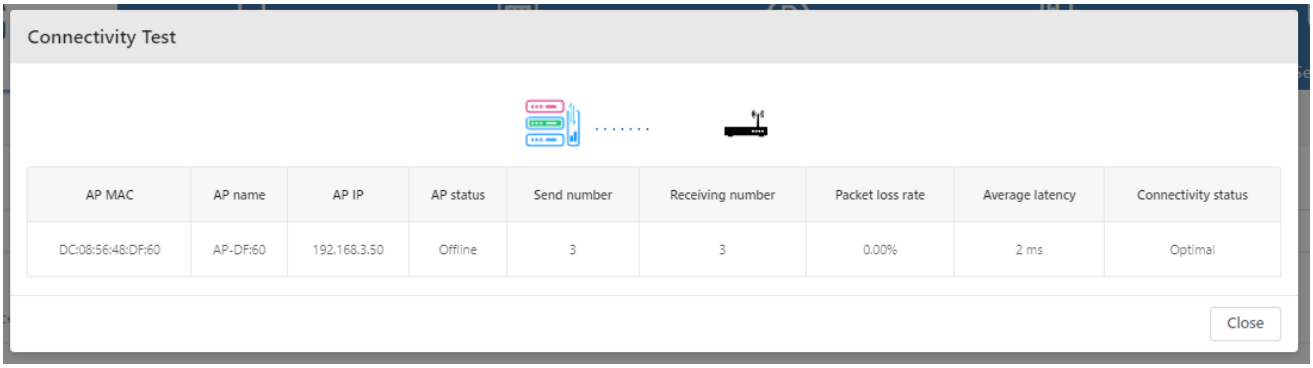


图 124：连通性测试

6.5.2 重启设备

- ☐ 选择要手动重启的设备。
- ☐ 点击“**Reboot**”按钮。

当设备重新启动后，它会重新连接到DAC。然后，将DAC上的最新配置下载到

AP。如果AP无法连接到DAC，则AP会使用最新保存的本地配置重新启动。

6.5.3 日志快照

有时候需要从设备中收集一些信息，以便于研发发现问题。

- ☐ 选择一个设备。
- ☐ 单击**“Log Snapshot”**按钮。

需要等待片刻，让设备将快照日志文件上传到DAC。在文件上传期间，需要保持在当前页面。文件传输完成后，浏览器会自动开始下载文件。

6.5.4 导出所有设备的信息

点击**“Export All Device”**按钮，可以从Site导出所有设备的信息。可以在下载文件窗口更改导出文件名，文件类型为xlsx，可使用Microsoft Office Excel打开。

MAC	Name	Group	Version	Model	License	IP	Status	Clients Number	Work Pattern	Position	Onlene Time
[redacted]	AP-33:10		[redacted]	[redacted]	Enable	192.168.5.2	Online	0	Normal Mode		3days4hours48minutes15seconds
[redacted]	AP-C4:23		[redacted]	[redacted]	Enable	192.172.6.42	Online	0	Normal Mode		19days13hours47minutes42seconds
[redacted]	AP-C4:22		[redacted]	[redacted]	Enable	192.172.6.41	Online	0	Normal Mode		19days13hours47minutes42seconds

图 125：导出的所有设备列表

6.6 从 AP 执行操作

在设备上执行特定命令并返回命令的输出。可以从下拉列表中执行操作。

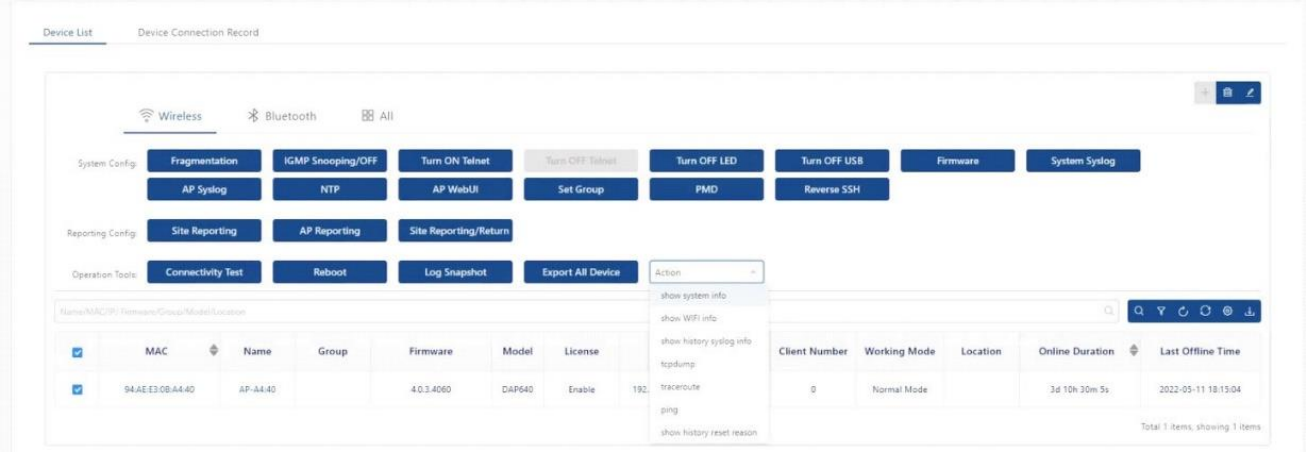


图 126：操作下拉菜单

6.6.1 Show system info

此操作会显示有关设备的系统信息，例如设备上的内存使用情况和文件系统的使用情况。

图 127：Show system info

6.6.2 Show WIFI info

显示指定DAP的无线接口信息，包括：

- ► “iwconfig”和“wlanconfig”命令的输出信息。例如，DAP的工作通道、发射功率、BSSID等。
- ► 客户端的PHY信息。例如，MAC地址，RSSI等。

图 128：Show WIFI info

6.6.3 Show history syslog info

显示指定DAP上次系统运行（本次系统启动前）以来生成的历史syslog消息。

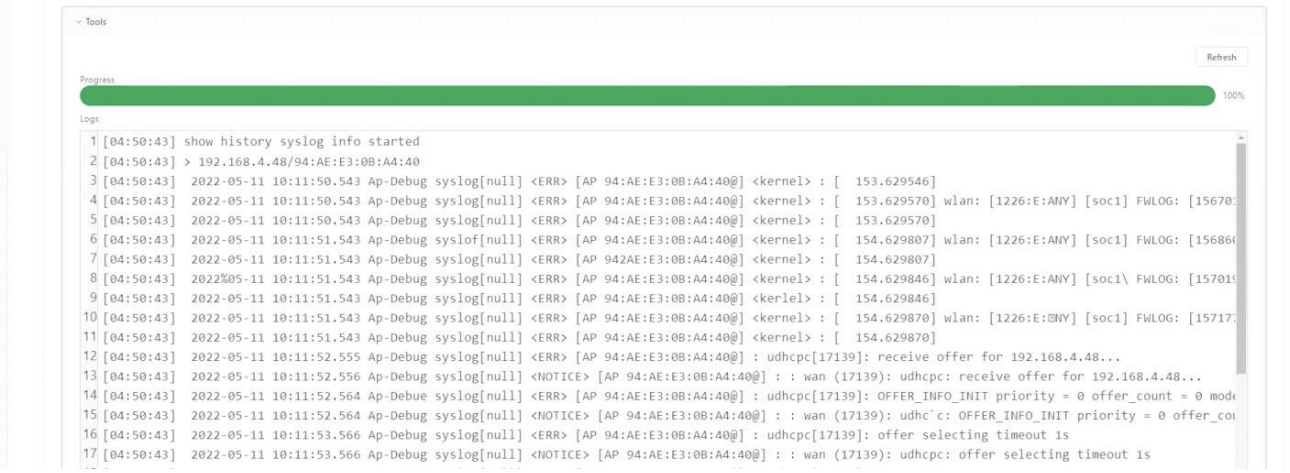


图 129：Show history syslog info

6.6.4 Tcpdump

可以使用“tcpdump”操作在设备上捕获数据包。

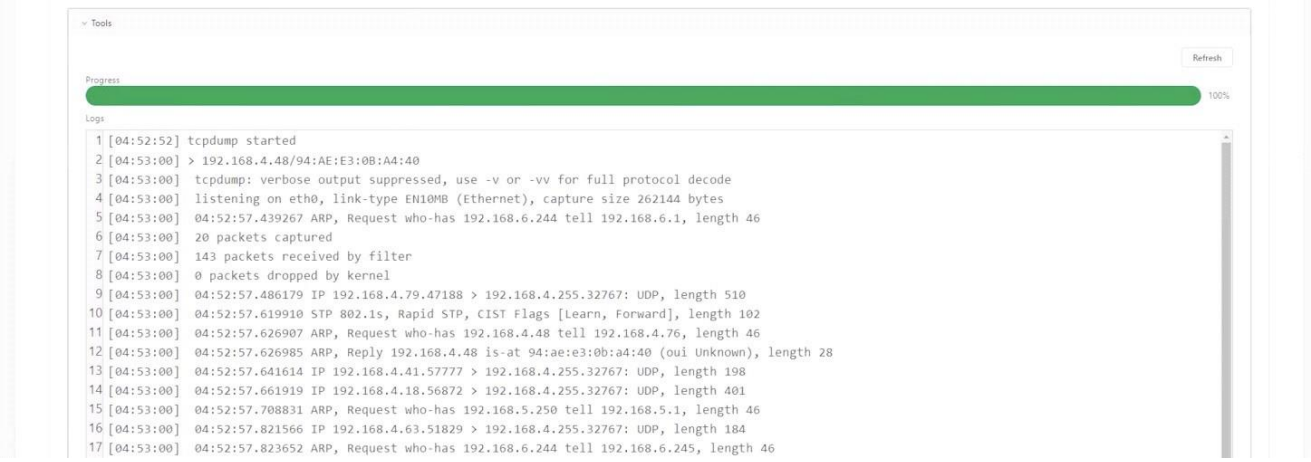


图 130：Tcpdump

6.6.5 Traceroute

从指定的DAP到网络中的另一个主机的Traceroute操作。

图 131：Traceroute

6.6.6 Ping

从指定的DAP到网络中的另一台主机的ping操作。

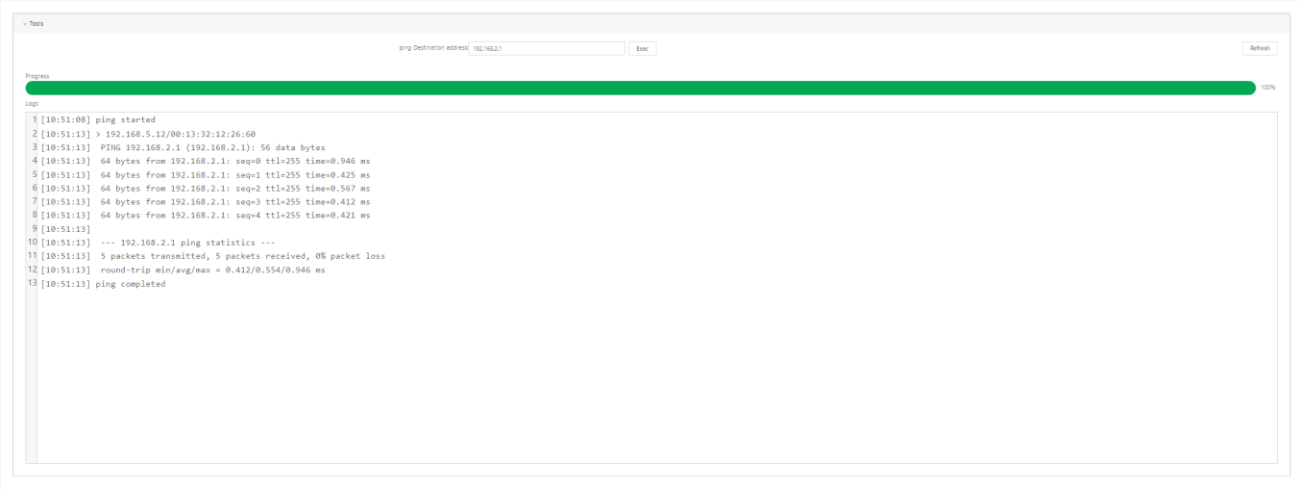


图 132：Ping 命令

6.6.7 Show history reset reason

显示指定DAP的最新10条重启记录，包括重启时间和重启原因。这与在DAP CLI模式下的reset_record命令的输出相同。

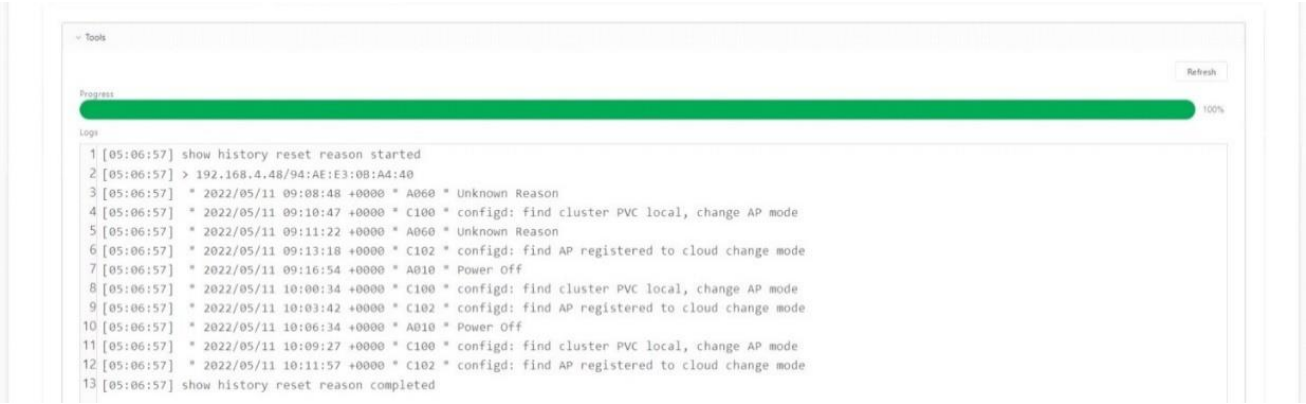


图 133：Show history reset reason 命令

6.7 设备连接记录

该列表包含设备的连接历史记录。当设备连接到DAC时，会生成一条记录。在断开设备时，MQTT更新断开时间。

- **MAC**：设备的MAC地址。
- **Name**：设备的名称。
- **MQTT Connected Time**：连接时间的最新更新记录。
- **MQTT Disconnected Time**：连接的MQTT断开时间。
- **MQTT Connected Duration**：连接的MQTT连接持续时间。

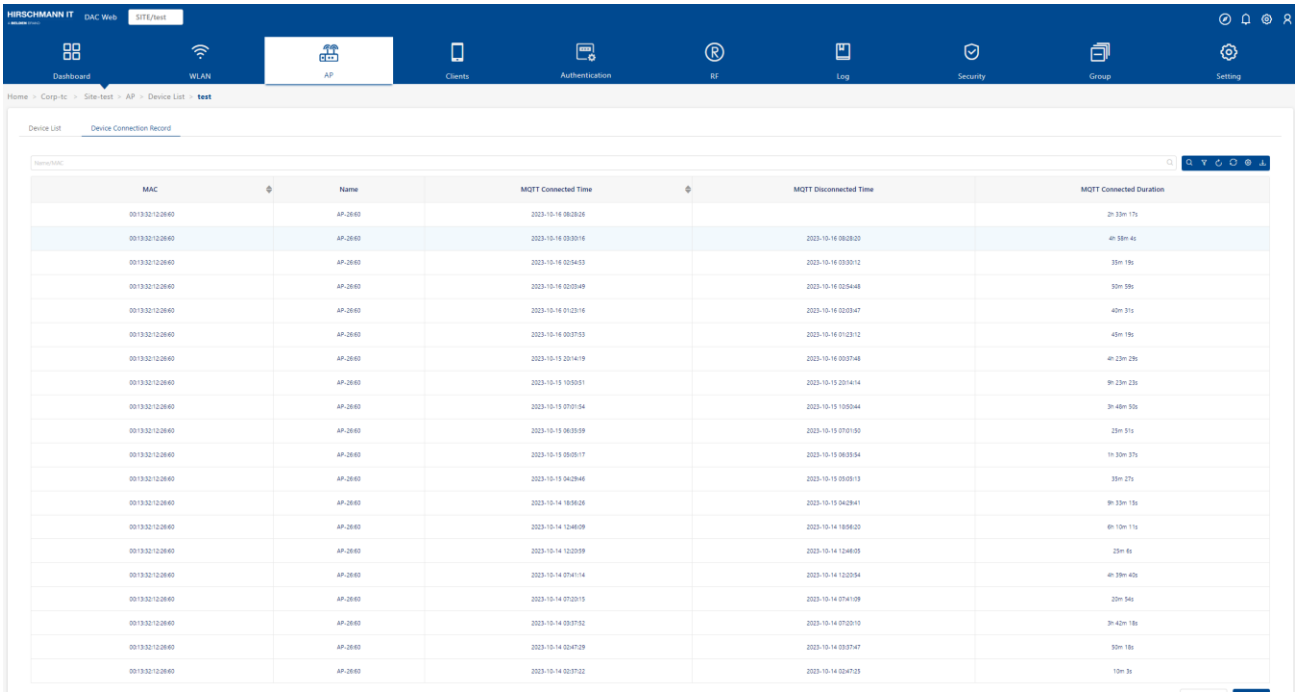


图 134：设备连接记录

7 客户端

客户端页面显示连接到当前Site的客户端。

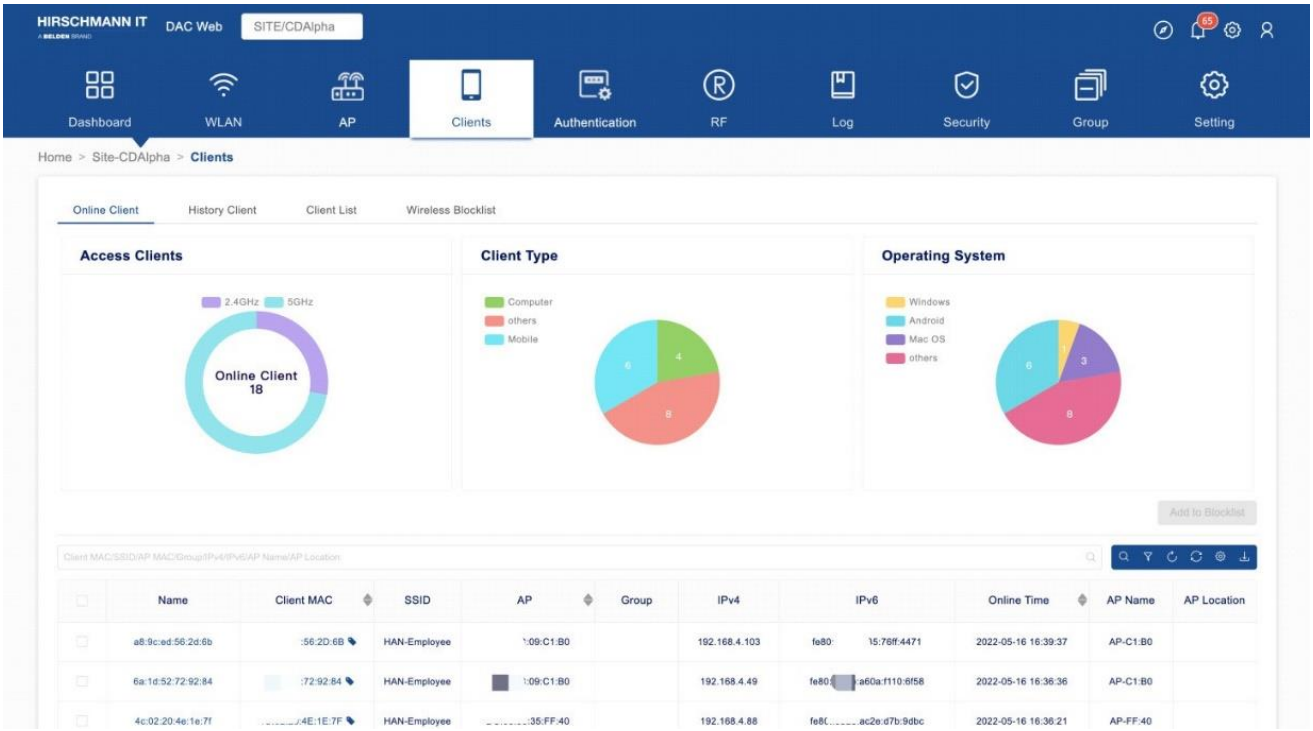


图 135：客户端页面

本章包含下列主题：

- ► 在线客户端
- ► 历史客户端
- ► 客户端列表
- ► 无线黑名单

7.1 在线客户端

该模块显示当前在线客户端列表。图 136中3个饼图显示了不同维度上客户端的分布情况。

- **Access Clients：**显示不同频段客户端的饼图（2.4G或5G）。
- **Client Type：**显示客户端类型的饼图，包括计算机、移动设备和其他设备。
- **Operating System：**显示客户端操作系统的饼图。

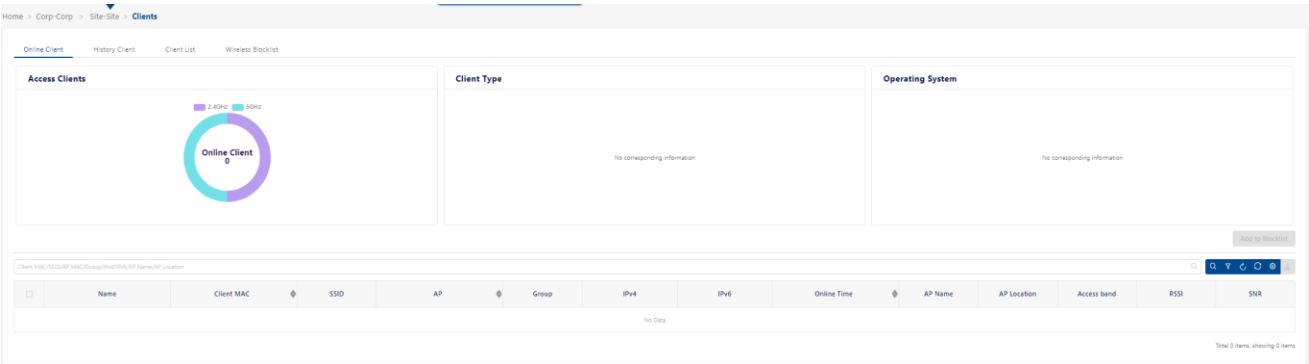


图 136：在线客户端

■ 客户端名单

列表显示在当前Site连接到AP的客户端。由于AP数据报告存在一定的时间间隔，因此这里的数据更新会有一定的延迟。

- **Name：**客户端名称。
- **Client MAC：**客户端的MAC地址。
- **SSID：**客户端所关联的SSID。
- **AP：**客户端关联的AP的MAC地址。
- **Group：**客户端所关联的AP的Group。
- **IPv4：**客户端的IPv4地址。
- **IPv6：**客户端的IPv6地址。
- **Online Time：**客户端与无线网络连接的时间。
- **AP Location：**AP设备的位置。
- **Access Band：**客户端连接到AP的无线电频段（2.4G Hz或5G Hz）。用

户需要点击“⚙”按钮手动添加该数据。

- **RSSI**：客户端的接收信号强度指示器（可选值：0..99）。用户需要点击“⚙”按钮手动添加该数据。
- **SNR**：信噪比。用户需要点击“⚙”按钮手动添加该数据。

客户端的MAC地址旁边有一个书签。点击书签可查看终端的更多详细信息。

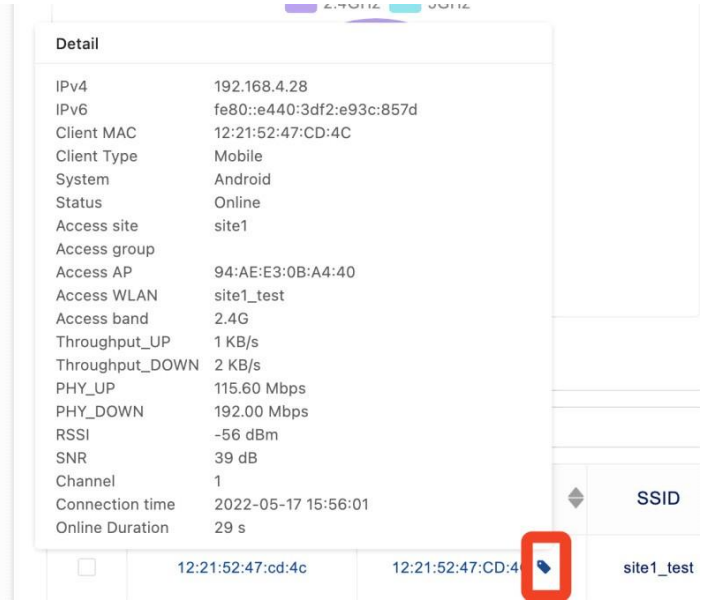


图 137：在线客户端信息

- **Client Type**：客户端设备类型，包括PC、移动设备和其他设备类型。
- **System**：客户端的操作系统。
- **Throughput_UP**：客户端发送数据包的速率。客户端发送数据包并收集流量统计数据。
- **Throughput_DOWN**：客户端接收数据包的速率。客户端接收数据包并收集流量统计数据。
- **PHY_UP**：客户端在物理层发送数据的速率。客户端发送数据包并收集流量统计数据。
- **PHY_DOWN**：客户端在物理层接收数据的速率。客户端接收数据包并收集流量统计数据。
- **Channel**：客户端的工作信道。

7.1.1 从在线客户端中添加客户端到黑名单

- ☐ 从客户端列表中选择要阻止的客户端。
- ☐ 点击**“Add to Blocklist”**按钮。
- ☐ 在确认提示窗口设置**“Expiry Time”**。
- ☐ 点击**“Save”**。

客户将无法再访问网络。它们会显示在无线黑名单界面上。

7.2 历史客户端

历史客户端表显示过去的连接记录。

- **Client MAC**：客户端的MAC地址。
- **SSID**：客户端所关联的SSID。
- **AP**：客户端关联的AP的MAC地址。
- **Group**：客户端所关联的AP的Group。
- **IPv4**：客户端的IPv4地址。
- **IPv6**：客户端的IPv6地址。
- **Online Time**：客户端与无线网络关联的时间。
- **Offline Time**：客户端与无线网络断开连接的时间。

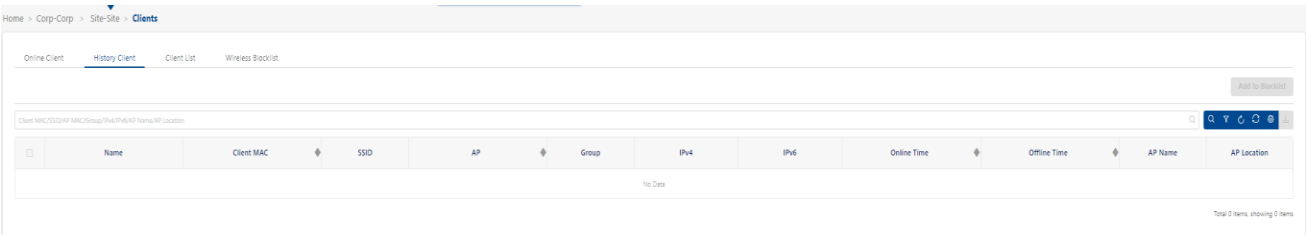


图 138：历史客户端

7.3 客户端列表

记录了所有连接到Site的客户端的连接总数和最后连接时间。

- **Name**：客户端名称。默认是客户端的MAC地址。

  为了方便地找到终端，可以对其进行修改。

  选择一个客户端，点击“**Edit**”图标，进入“**Name**”字段，然后点击“**Save**”按钮。
- **Client MAC**：客户端的MAC地址。
- **Connecting Times**：客户端的连接次数。
- **Last Connection**：客户端上次访问Site的时间。
- **Group**：客户端最后访问Site的Group。

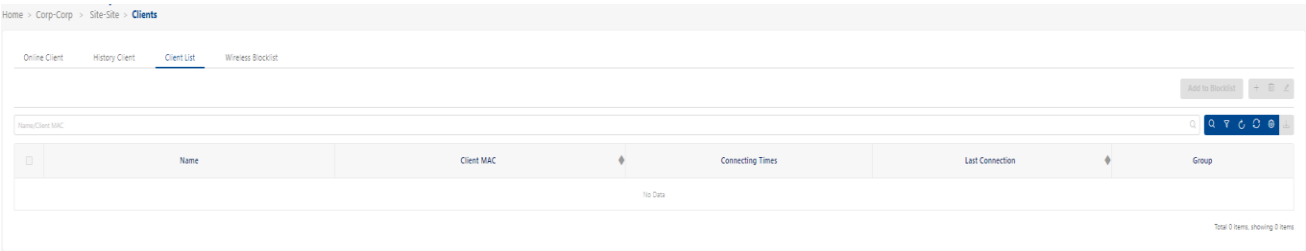


图 139：客户端列表

7.4 无线黑名单

黑名单专注于基于客户端级别的用户连接到SSID的基本访问控制机制。在黑名单上的客户端将被拒绝与DAP关联。一旦客户端被列入黑名单，它将无法连接到任何安全级别的WLAN（Enterprise，Personal或Open）。您可以根据客户端的MAC地址添加或删除黑名单。

无线黑名单界面显示在该Site被阻止的所有客户端的有关信息。您还可以将客户端手动添加到黑名单中。

- **Client MAC：**黑名单中的客户端的MAC地址。
- **Type：**将客户端添加到黑名单的原因。
  - **Manual：**由用户手动添加到黑名单。
  - **Auto：**由WIPS策略动态添加到黑名单。
- **Start Time：**阻止开始的时间。
  - 在此期间，客户端无法访问无线网络。
- **Expiry Time：**阻止到期的时间。
  - 阻止到期时间过后，客户端即可访问无线网络。
- **From(Site/Group)：**记录添加来源，从Site或Group添加的记录。

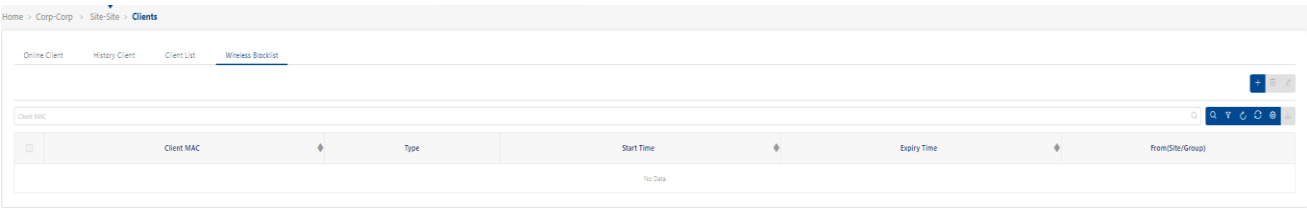


图 140：无线黑名单

7.4.1 手动添加客户端到黑名单

- ☐ 点击“**+**”图标，打开“**Add to Blocklist**”窗口。
- ☐ 输入客户端MAC地址。
- ☐ 点击“**Save**”按钮。

重复以上步骤添加其他客户端。您应该为客户端设置一个到期时间，则在到期时间之前，客户端无法连接到Site的SSID。

7.4.2 从黑名单中删除客户端

- ☐ 从列表中选择一个设备。
- ☐ 点击“**Delete**”图标。
- ☐ 在确认提示上单击“**Yes**”。

8 身份验证

DAC 内置了 AAA 服务器。根据 WLAN 配置，DAP 向 DAC 发送身份验证请求，该请求可采用 802.1x 身份验证、MAC 身份验证或其他身份验证方法。
本章包含下列主题：

8.1 身份验证概念

■ **802.1X身份验证**

IEEE 802.1X 是一种基于端口的网络接入控制（PNAC）的 IEEE 标准，属于 IEEE 802.1 组的网络协议之一，为要连接到 LAN 或 WLAN 的设备提供了身份验证机制。

802.1X 是电气和电子工程师学会（IEEE）制定的标准，为 WLANs 提供了认证框架。在身份验证过程中，802.1X 使用可扩展认证协议（EAP）进行消息交换。在 802.1X 框架内，适用于无线网络的身份验证协议包括 EAP 传输层安全性（EAP-TLS）、受保护的 EAP（PEAP）和 EAP 隧道化 TLS（EAP-TTLS）。这些协议允许网络对客户端进行身份验证，同时也允许客户端对网络进行身份验证。802.1x 认证由下列 3 个组件组成：

- **Client**：要访问网络的设备。
- **Authenticator**：身份验证器，网络的门卫，允许或拒绝客户端访问。无线控制器可充当身份验证器，负责在认证服务器和客户端之间的传递信息。
  注意：身份验证服务器和客户端之间的EAP类型必须保持一致，并且对无线控制器透明。
- **Authentication Server**：身份验证服务器，提供身份验证所需的信息数据库，并告知验证器是否拒绝或允许客户端访问。802.1X身份验证服务器通常是符合EAP标准的RADIUS服务器，可以对用户（通过密码或证书）或客户端计算机进行认证。

在我们的系统中，DAP 充当身份验证器，DAC 充当身份验证服务器。DAC 可以使用不同的数据源进行用户身份验证。

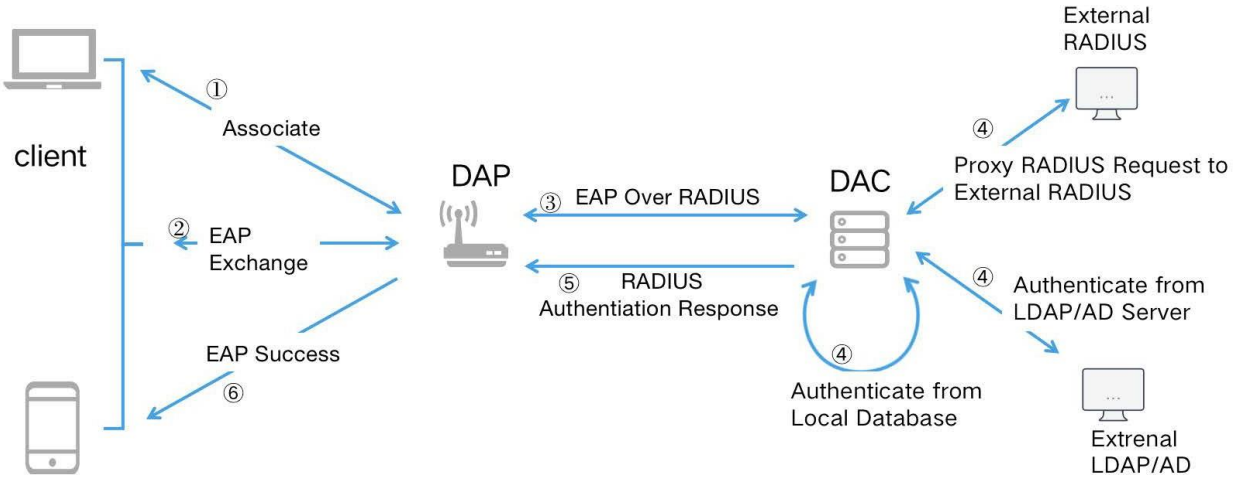


图 141：802.1X 身份验证过程

图 141展示了我们系统中802.1x身份验证过程的基本流程。

1 客户端发起无线关联。

2 客户端与DAP开始EAP交互，这是一个涉及到多条消息的握手过程。

3 DAP通过RADIUS协议将相应的EAP消息转发给DAC。

4 DAC（基于不同的配置）使用不同的数据源来验证用户。

5 DAC通过RADIUS协议将EAP认证结果返回给DAP。

6 DAP将EAP身份验证结果返回给客户端。

■ MAC身份验证

MAC身份验证是根据设备的物理介质访问控制（MAC）地址进行身份验证。设备的MAC地址将用作RADIUS访问请求中的用户名和密码。MAC身份验证是Web身份验证的必要预处理。

当无线终端访问DAP时，DAP将启动MAC身份验证。RADIUS访问请求将经过**访问策略**的规则匹配，并进入相应的**身份验证策略**进行处理。如果**身份验证策略**配置为**访客/员工接入策略**，MAC地址在之前已通过门户进行了身份验证，相应的账户已绑定且绑定未过期，则认证模块将直接返回认证成功，并将相应的访问角色返回给AP。如果MAC之前没有经过门户认证，或者之前绑定的记录已过期，那么配置在**认证策略**中的**访客/员工接入策略**的门户URL将发送给终端。在终端打开改页面后，输入**“User name”**和**“Password”**完成门户认证过程。如果认证成功，则根据策略保存MAC身份验证绑定记录。

■ Web门户身份验证

Web门户身份验证是通过Web页面获取用户凭据，并通过RADIUS服务器进行身份验证的机制。如果身份验证成功，则RADIUS服务器返回一个应用于用户设备流量的**访问角色**。DAC实现支持Web门户机制。

Web门户身份验证是**访问角色配置文件**的一个可配置选项，用于在用户被分配到配置文件之后（初始MAC身份验证之后）进行认证。这种类型的身份验证不会更改用户设备的访问角色配置。相反，Web门户提供了一个二级身份验证，用于将新的访问角色应用于用户。

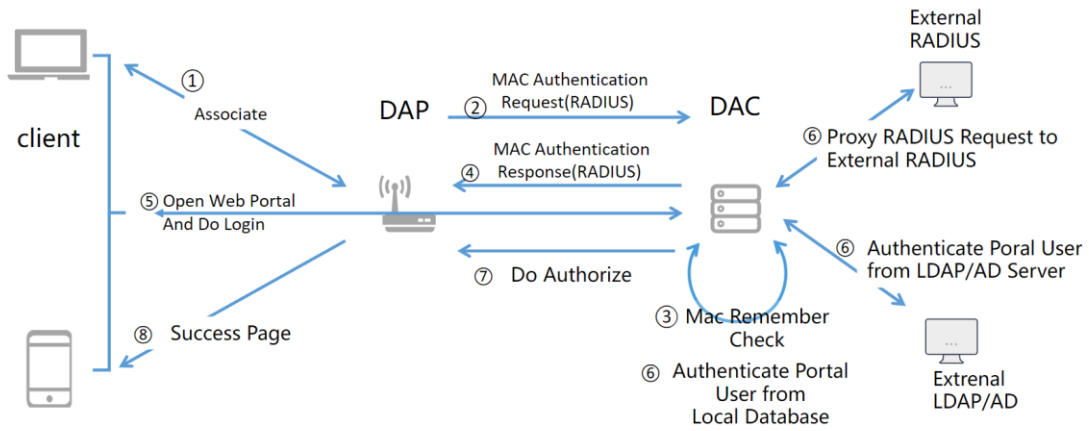


图 142：Web 门户身份验证过程

图 142展示了系统中Web门户认证的基本流程。

1 客户端发起无线关联。

2 DAP通过RADIUS协议启动MAC身份验证。

3 DAC执行记住检查（检查客户端MAC地址绑定的账号是否有效）

4 DAC把记住检查结果回复给DAP。如果客户有未过期的记住检查记录，则DAP将直接授权客户，而不会将其重定向到Web门户。否则，根据配置，DAC将向DAP返回相应的Web门户，并且DAP将通过HTTP 302把客户端的HTTP请求重定向到Web门户页面。

5 客户端浏览器打开Web门户页面，输入用户名和密码，并发起登录请求。直接提交给DAC。

6 DAC根据不同的配置使用不同的数据源来验证用户。

7 DAC根据认证结果将客户端的授权信息（访问角色配置文件）发送给DAP。

8 身份验证结果将显示在客户端浏览器网页上。

访问角色

每个无线客户端在访问或认证时都会被分配一个**访问角色**。终端**访问角色**分配可以直接从WLAN获取，也可以根据认证过程中的策略进行分配，还可以在认证账户上进行设置。有关详细信息，请参阅第147页的“访问角色配置文件”。

访问策略

RADIUS数据包包含一些用户或终端相关属性。当认证模块接收到RADIUS数据包时，**访问策略**将匹配相应规则并使用相应的**认证策略**进行认证。有关详细信息，请参阅第161页的“访问策略”。

身份验证策略

身份验证策略定义了MAC认证或802.1x认证的相关策略参数，包括身份验证源、**访问角色**、是否启用Web认证等其他属性。选择不同的身份验证源时，Web身份验证的选择有一些限制。请参阅第163页的“身份验证策略”。

访客接入策略

为访客定义网络身份验证策略。您可以点击**“Edit Page”**来自定义网页。请参阅第242页的“强制登录页”和第170页的“访客接入策略”。

员工接入策略

为员工定义Web身份验证策略。请参阅第178页的“员工接入策略”。

身份验证源

用于身份验证的数据源。您可在身份验证策略和访客/员工接入策略看到此配置。此选项可以有以下值：

- **None**：只能在**身份验证策略**中选择。如果选择此**身份验证源**作为身份验证策略，那么在此阶段仅执行记住验证，并不能用于802.1x身份验证。
- **Local Database**：本地身份验证数据库。可用于**身份验证策略**或**访客/员工接入策略**。对于802.1x身份验证，您需要在**Authentication→Employee Access→Employee Access Strategy**中添加员工帐户，并且这些帐户也可用于**员工接入策略**中的Web门户身份验证。对于**访客接入策略**中的Web门户身份验证，只能选择本地数据库作为**身份验证源**。
- **External LDAP/AD**：使用外部LDAP/AD作为**身份验证源**。可用于**身份验证策略**或**员工接入策略**。可以在**Authentication→Setting→LDAP/AD Configuration**中完成参数设置。请参阅第185页的“LDAP/AD配置”。
- **External Radius**：使用外部RADIUS作为**身份验证源**。可用于**身份验证**

策略或**员工接入策略**。您可以在**Authentication→Setting→External Radius**中添加外部RADIUS。

已记住的设备

可用于简化**Web门户身份验证**的过程。通过**Web门户身份验证**后，终端的MAC地址和帐户与授权**访问角色配置文件**之间的绑定关系将被记录下来。当终端在有效期内再次访问无线网络时，无需再次进行**Web门户身份验证**。

下图为**访问策略**、**认证策略**、**访客接入策略**和**员工接入策略**之间的关系。

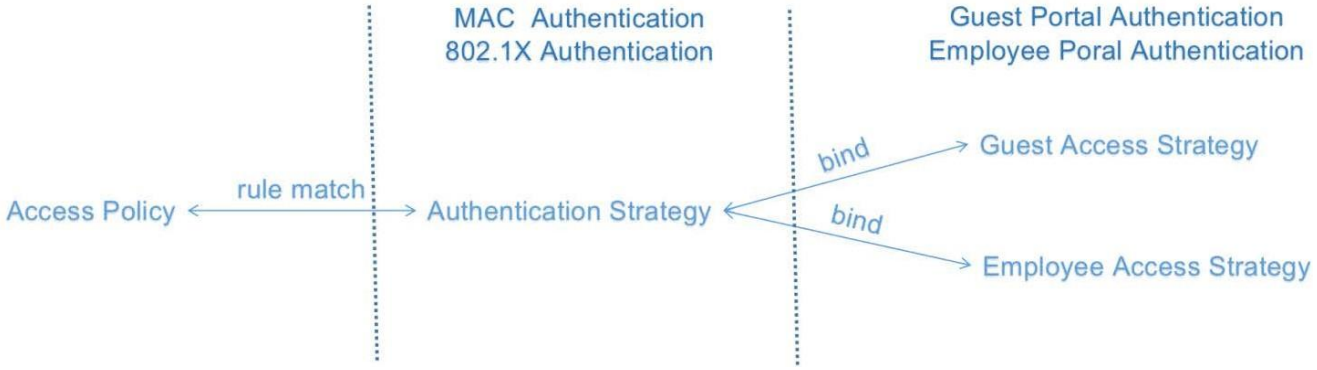


图 143：访问策略与各策略之间的关系

总的来说，终端访问可能需要2个身份验证步骤，即MAC身份验证或802.1X身份验证，以及Web身份验证。

身份验证策略用于定义MAC身份验证或802.1X身份验证。身份验证结果决定是否需要进行后续的网络身份验证。**访客接入策略**或**员工接入策略**是Web身份验证的配置。

8.2 网络控制

网络控制用于控制用户的在线行为，由访问角色配置文件、位置策略、时间策略、策略和策略列表组成。

8.2.1 访问角色配置文件

访问角色配置界面显示所有已配置的访问角色配置文件，并用于创建、编辑和删除访问角色配置文件。访问角色配置文件包含分配给该配置文件的用户的各种属性（例如，VLAN或带宽控制）。访问角色配置文件被视为与无线网络上的每个客户端相关联的用户角色。

■ 创建访问角色配置文件

☐ 点击**“+”**图标。
☐ 填入**“Profile Name”**并参考以下描述配置文件。
☐ 点击**“Save”**按钮。

策略和策略列表
可以使用现有的策略列表来配置访问角色配置文件，策略列表中的一组规则将应用于通过无线设备传输的流量。每个配置文件只允许使用一个策略列表，但多个配置文件可以使用同一个策略列表。

☐ 从下拉列表中为配置文件选择策略列表。
☐ 点击**“Add”**链接创建新的策略列表。

位置策略
☐ 从下拉列表中选择**“Location Policy”**。

时间策略
☐ 从下拉列表中选择一个**“Period Policy”**。

带宽控制设置
► **Upstream Bandwidth：**分配给配置文件的UNP（User Network Profile）端口上入口流量的最大带宽限制。如果最大入口带宽值设置为**“0”**，则所有入口流量不受限制。

- **Downstream Bandwidth**：分配给配置文件的UNP端口上出口流量的最大带宽限制。如果最大出口带宽值设置为**“0”**，则UNP端口上允许所有出口流量。
- **Upstream Burst**：分配给配置文件的UNP端口上流量的最大入口深度值。该值决定了超过最大入口带宽速率的流量突发量。最大入口深度值与最大入口带宽参数一起配置。
- **Downstream Burst**：分配给配置文件的UNP端口流量的最大出口深度值。该值决定了超过最大出口带宽速率的流量突发量。最大出口深度值与最大出口带宽参数一起配置。

VLAN和VLAN池

您可以为访问角色配置文件设置单个VLAN或多个VLAN（作为VLAN池）。对于单个VLAN类型，可以将VLAN ID设置为**“0”**，意味着将访问角色配置文件映射到未标记的流量。

注意：可以通过输入多个VLAN来选择一个VLAN池。

可以输入一个VLAN的可选值（例如，10..20），或单个VLAN（21、23、25），或两者都输入（10..20、21、23、25）。

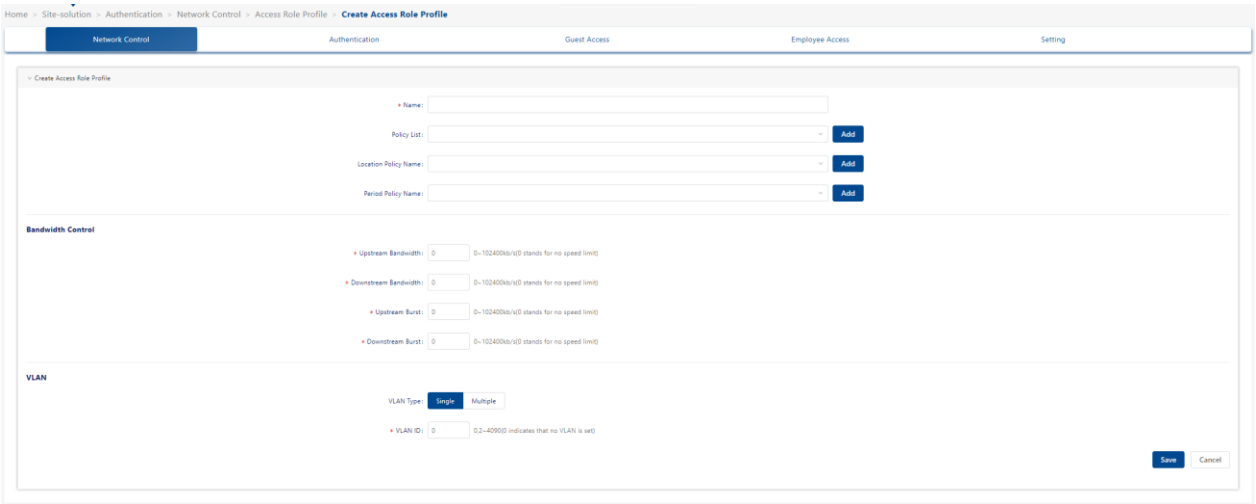


图 144：创建访问角色配置文件

■ 编辑访问角色配置文件

☐ 从访问角色配置文件列表中选择配置文件。

☐ 点击“Edit”图标。打开**“Edit Access Role Profile”**界面。

☐ 参考上述描述编辑字段。
☐ 点击“**Save**”按钮将更改保存到服务器。
注意：无法编辑访问角色配置文件名称。

■ **删除访问角色配置文件**

☐ 在“**Access Role Profile**”界面中选择配置文件。
☐ 点击“**Delete**”图标。
☐ 在确认提示上单击“**Yes**”。此操作将从服务器上删除配置文件。

8.2.2 策略

策略界面应用程序显示已配置的策略，用于创建、编辑、删除和查看策略。策略是可以应用于DAP的QoS策略。策略使用向导创建，向导会指导您完成创建策略所需的每个步骤。

■ **创建策略**

向导会引导您完成创建策略所需的每个步骤。要创建策略，请点击“**+**”图标。然后，向导会引导您完成以下界面：

► **Config：**基本策略配置（例如，策略名称，优先级）。
► **Set Condition：**指定在流量允许通过之前必须满足的条件。
► **Set Action：**指定流量的参数。
► **Validity Period：**指定策略生效的时间段。
► **Confirm：**在创建策略之前，请查看策略详细信息。

配置

策略界面用于配置基本策略参数。

完成所有参数配置后，请点击界面底部的“**Next**”按钮，以进入下一步。

► **Name：**策略名称。
► **Precedence：**策略的优先级。在默认设置中，优先级字段预先填充为未使用的最低优先级值（可选值：0..65535）。

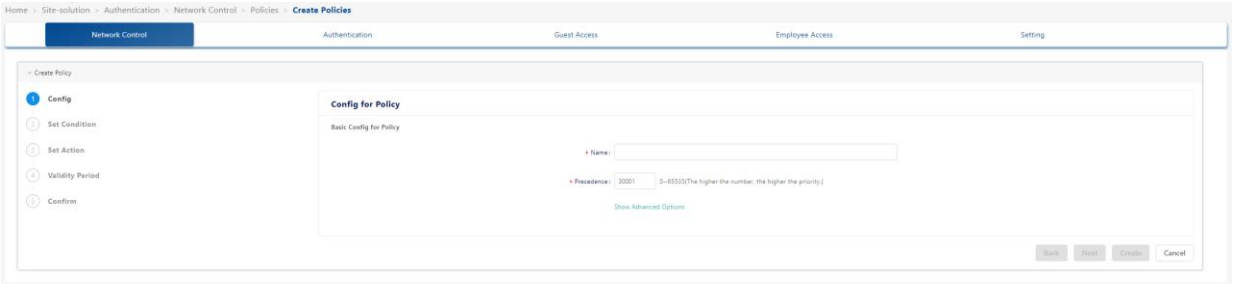


图 145：策略的基本配置

设置条件

“Policies Set Condition”界面包含一个条件列表，可以为策略配置条件（例如，MAC条件，IP条件）。创建条件时，配置的条件必须为真，才允许流量流动。

- ☐ 单击条件以显示条件的配置选项。（再次点击条件可隐藏配置选项。）
- ☐ 完成所有条件的参数设置后，请点击界面底部的**“Next”**按钮，以进入下一步。
- ☐ 点击**“Back”**按钮返回**“Config”**界面。

每个条件的简要描述如下。点击每个条件的超链接以获取详细的配置说明。

- ► **L2 MACs**：创建一个条件，将策略应用于源MAC地址/源MAC地址组的流量，或目的MAC地址/目的MAC地址组的流量。
- ► **L3 IPs**：创建一个条件，将策略应用于源IP地址/源IP地址组的流量，或目的IP地址/目的IP地址组的流量。

  注意：任何IP地址都可以进行掩码处理。
- ► **L3 DSCP/TOS**：创建一个条件，将策略应用于具有DSCP（区分服务代码点）字节或IP TOS（IP服务类型）字节中具有指定值的流量。DSCP和IP TOS是用于在帧的IP头部中传递QoS信息的机制。
- ► **L4 Services**：创建一个条件，将策略应用于在2个TCP或UDP端口之间流动的流量，或将策略应用于从TCP或UDP端口发起的所有流量，或将策略应用于流向TCP或UDP端口的所有流量。还可以使用现有的服务或服务Group创建条件。

L2 MACs

MAC条件将策略应用于从MAC地址/组流出的流量和流向MAC地址/组的流量。

注意：当流量经过路由器时，Layer 2条件（指定MAC地址的条件）会**“丢失”**。因此，当流量的传输跳数超过1个路由器跳数时，建议使用其他类型的条件（例如Layer 3条件，指定IP地址）。

- ☐ 通过选择适用的复选框，选择要配置的参数。
- ☐ 单击**Single**以配置单个MAC地址，或单击**Group**以配置MAC Group。
- ☐ 输入MAC地址或从下拉列表中选择一个MAC Group。（还也可以点击**“Add”**图标，进入Group应用程序并创建一个新的MAC Group。）
- ► **Source MAC Address/MAC Group：**配置源MAC地址/Group条件可将策略限制为仅适用于从该MAC地址/Group流出的流量。如果未选择此选项，则不会处理源MAC地址/Group的流量。
- ► **Destination MAC Address/MAC Group：**配置目标MAC地址/Group条件可将策略限制为仅适用于流向该MAC地址/Group的流量。如果未选择此选项，则不会处理目的地MAC地址/Group的流量。

L3 IPs

IP条件将策略应用于源自或流向IP地址/IP地址组的流量。任何IP地址都可以进行掩码处理。

- ☐ 通过选择适用的复选框来选择您想要配置的参数。
- ☐ 对于源IP地址/目标IP地址，请单击**“Single”**以配置单个IP地址，或单击**“Group”**以配置IP地址组。
- ☐ 输入**“IP Address”**或从下拉列表中选择一个Group IP Address。（也可点击**“+”**图标，进入Group应用程序并创建一个新的Group IP Address。）
- ► **Source IP Address/Group IP Address：**配置源IP地址/IP地址组条件可将策略限制为仅适用于从此IP地址或子网掩码/IP地址组流出的流量。如果未选择此选项，则不会处理源IP地址或子网掩码/IP地址组的流量。
- ► **Destination IP Address/Group IP Address：**配置目标IP地址/IP地址组条件可将策略限制为仅适用于流向该IP地址/IP地址组的流量。如

果未选择此选项，则不会处理目标IP地址或子网掩码/IP地址组的流量。

L3 DSCP/TOS

DSCP/TOS条件将策略应用于DSCP（区分服务代码点）字节或TOS（服务类型）字节中具有指定值的传入流量。DSCP和TOS都是用于在帧的IP头部传递QoS信息的机制。DSCP和TOS是互斥的，可以使用DSCP或TOS，但不能同时使用两者。点击适用的按钮（DSCP或TOS），然后输入一个值。

- **DSCP**：定义了每个网络设备对帧的QoS处理，这被称为逐跳行为。如果使用DSCP，则可以将帧的IP头部中的DSCP值定义为0..63范围内的任何值。包含此值的流量将与此条件匹配。
- **TOS**：TOS值创建了一个条件，将策略应用于帧的IP头部中具有指定TOS值的流量。输入0-7之间的任意值，指定TOS字节中与此条件匹配的优先级字段的值，值为7具有最高优先级，值为0具有最低优先级。

L4 Services

服务条件将策略应用于源自/流向2个TCP或UDP端口的服务协议流量（TCP或UDP），或者应用于源自/流向TCP或UDP服务或服务组的流量。选择要配置的服务条件类型，然后根据以下描述配置参数。

- **Protocol Only**：选择TCP或UDP，仅为服务协议创建条件。
- **Port(s)**：要为特定的服务端口配置条件，请从下拉列表中选择**源端口**和目标端口，以指定所选服务的特定端口。也可以点击**“Add”**图标创建新的服务端口。
- **Service**：从下拉列表中选择一个服务。也可以点击**“Add”**图标创建新的服务。
- **Group**：从下拉列表中选择一个Service Group。也可以点击**“Add”**图标创建一个新的Service Group。

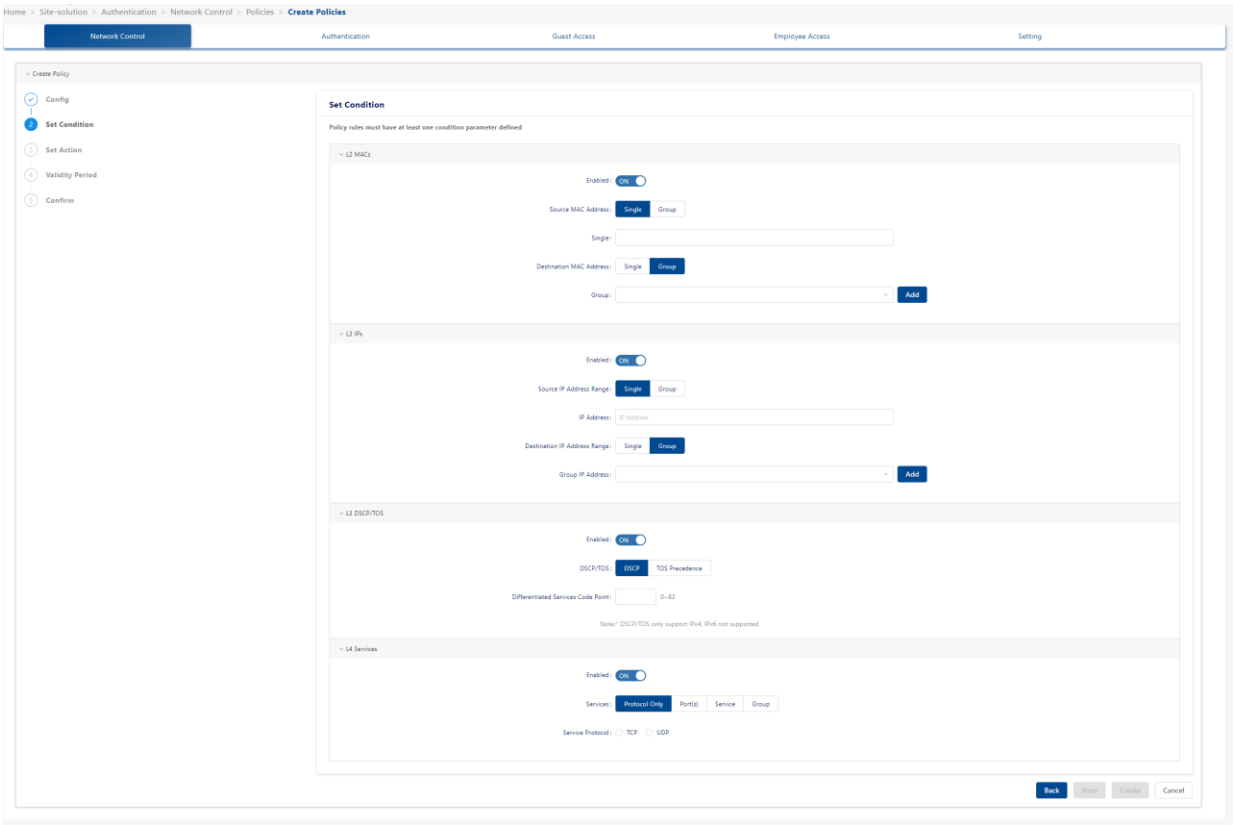


图 146：设置条件

设置操作

策略设置操作界面列出了可为策略配置的一系列操作选项（如 QoS，TCM）。策略操作可让您指定流量在流动时所接收到的处理方式。这包括流量将接收的优先级，其最小和最大输出速率，以及在流出交换机时帧头部中指定位的设置值。当策略条件指定的条件为真时，流量将按照策略操作所指定的方式进行流动。

- ☐ 当您完成所有操作的参数设置后，点击界面底部的**“Next”**按钮或点击界面左侧的**“Validity Period”**以进入下一步。
- ☐ 点击**“Back”**按钮返回。

每个操作的简要描述如下。点击每个操作的超链接以获取详细的配置说明。

- ► **QoS：** 设置操作以指定对符合配置策略条件的流量施加的QoS操作。当策略指定的条件为真时，流量将按照策略操作所指定的方式流动。
  QoS适用于无线设备的会话类型。
- ► **TCM：** 创建一个操作，以指定对符合配置策略条件的流量施加三色标记（TCM）的操作。TCM通过限制交换机接口上发送或接收流量的速率，

为网络流量的监管提供了一种管控机制。TCM根据用户配置的数据包速率和突发大小对流量进行计量，并根据流量是否符合配置的速率将计量的数据包**“marks”**为绿色、黄色或红色。这个**“color marking”**决定了发生拥塞时数据包的优先级。无线设备不支持TCM，应用于这些设备时会被忽略。

QoS

QoS策略操作选项可指定对符合配置策略条件的流量施加的QoS操作。当策略指定的条件为真时，流量将按照策略操作所指定的方式流动。

- **Behavior**：将操作设置为Accept或Drop，对符合配置条件的流量进行处理。
- **Priority**：指定符合配置条件的流量将获得的QoS优先级。
- **Max Output Rate**：指定端口能够保证传输的流量的最大速率，以kilobits每秒为单位。如果没有其他流量存在，则输出将限制为此处指定的速率。
- **802.1p Priority Level**：如果希望传出的数据包带有802.1p优先级级别标记，则将802.1p优先级级别字段设置为0到7之间的任何值，以指定传出的流量所需的802.1p优先级。值为7表示最高优先级，值为0表示最低优先级。

  注意：对于配置了802.1q的端口，此值用于802.1q头部，并指示帧的传出优先级。

  当一个帧从队列中取出准备进行传输时，它会被分配给队列的优先级，并映射到传出的802.1p优先级。此优先级与VLAN Group ID结合，创建用于传输的802.1p/q头部。

  注意：如果流量符合策略条件的规定，但是传出端口不支持802.1p标记，则策略操作将失败。此参数不支持AOS无线设备，应用于这些设备时将被忽略。
- **DSCP/TOS**：启用或禁用DSCP/TOS优先级。RFC 791对TOS字节进行了定义。这个字节包含2个字段。优先级字段是高三位（位0-2），用于指示帧的优先级。服务类型字段（位3-6）定义了帧的吞吐量、延迟、可靠性或成本。然而，在实践中这些位并未使用。如果启用**TOS Precedence radio**，则将相关字段设置为0..7之间的任何值，以指定在从交换机出口时将插入到TOS字节的优先级字段中的值。值为7具有最高优先级，值为0具有最低优先级。

注意：可以启用DSCP或TOS Precedence radio来指定要使用的机制（如果有的话）在帧的IP头部中传递QoS信息。DSCP和TOS是互斥的，可以使用DSCP或TOS，但不能同时使用。此参数不支持AOS无线设备，应用于这些设备时将被忽略。

TCM

TCM策略操作选项允许您指定在满足配置的策略条件的流量上施加的三色标记（TCM）操作。TCM通过限制交换机接口上发送或接收流量的速率，为网络流量的监管提供了一种管控机制。

TCM根据用户配置的数据包速率和突发大小对流量进行计量，并根据流量是否符合配置的速率将计量的数据包**“marks”**为绿色、黄色或红色。这个**“color marking”**决定了发生拥塞时数据包的优先级。AOS无线设备不支持TCM，应用于这些设备时会被忽略。

- **Committed Information Rate：**端口上所有进入流量的保证带宽，以每秒比特为单位。（256~65535 kbit/s）
- **Peak Information Rate：**端口上所有进入流量的峰值带宽，以每秒比特为单位。（256~65535 kbit/s）

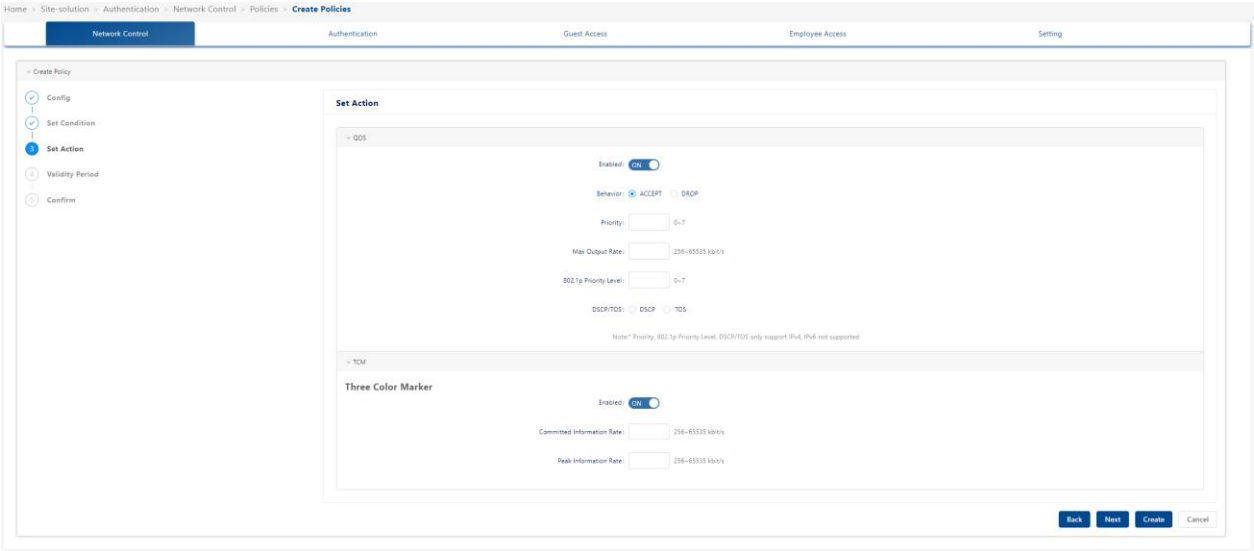


图147：设置操作

有效期

通过策略有效期界面，可以为策略添加有效期，指定策略激活和执行的时间段。从有效期下拉列表中选择一个有效期：

- **AllTheTime**：该策略将在全年每天24小时内都生效和执行。
- **Weekdays**：该策略将在每个工作日（星期一至星期五）的全天24小时内生效和执行。
- **Weekends**：该策略将在每周的非工作日（星期六和星期日）的全天24小时内生效和执行。
- **WorkingDay**：该策略将在每个工作日（星期一至星期五）的上午9:00至下午5:00的时段生效和执行。
- **Custom**：选择通过指定具体日期、月份和时间来创建自定义有效期。

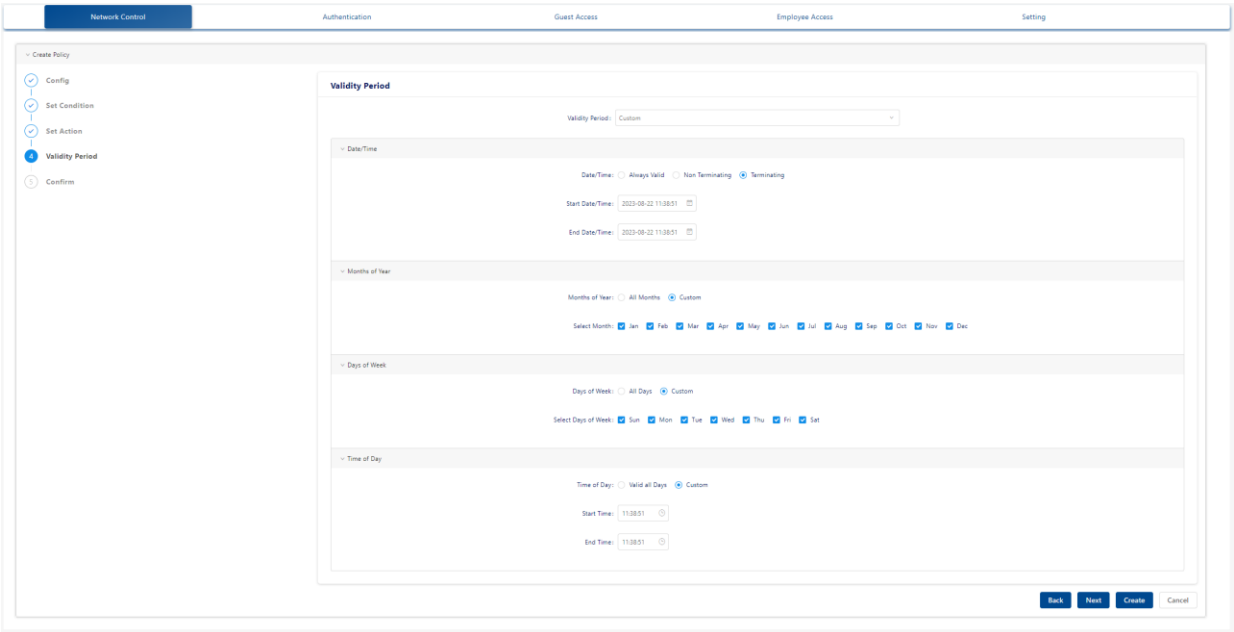


图 148：策略有效期

☐ 完成所有参数配置后，请点击界面底部的“**Next**”按钮，以进入下一步。
☐ 如有必要，点击“**Back**”按钮返回。

注意：预设有效期，**AllTheTime**是默认值。在配置IP条件或服务条件时，可以配置一个有效期。如果未指定IP或服务条件，则配置的期限不适用于无线控制器。

■ 编辑策略

☐ 在Existing Policies Table中选择要编辑的策略。
☐ 点击“**Edit**”图标。使用向导进行编辑。

■ **删除策略**

☐ 在Existing Unified Policies Table中选择要删除的策略。
☐ 点击**“Delete”**图标。
☐ 在确认提示上单击**“Yes”**。

8.2.3 策略列表

策略列表界面显示所有已配置的策略列表，包括每个列表中包含的策略，并用于创建、编辑、删除、查看和应用策略列表。策略列表是一组将策略分组并分配给设备作为一个组的策略。策略列表可以应用于DAP，策略列表必须作为访问角色配置文件的一部分应用。

■ **创建一个策略列表**

☐ 单击**“+”**图标，打开Create Policy List Wizard窗口。

☐ 按照以下描述完成配置。

☐ 单击**“Add”**按钮。

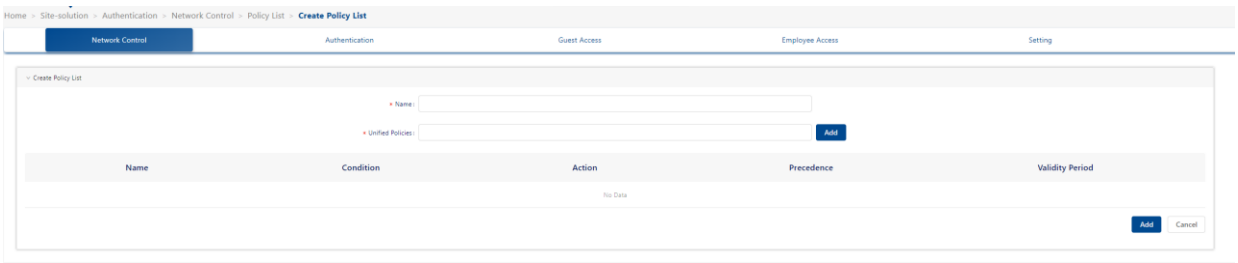


图 149：策略列表

策略列表配置

☐ 输入策略列表的名称。
☐ 从**Unified Policies**下拉列表中选择要包含在列表中的策略。当前配置的所有统一策略都会出现在列表中。
☐ 点击**“Add”**按钮，打开**“Create policy”**窗口。
☐ 创建一个新的策略，添加到列表中。
☐ 当您从下拉列表中选择一个策略时，该策略将显示在下方的表格中，在表

中可查看策略列表配置。

- ☐ 点击“**Add**”按钮。新的策略列表出现在界面上。

■ **编辑策略列表**

可以编辑策略列表中包含的策略，或编辑列表中任何策略的优先级。

- ☐ 选择一个Unified Policy List。
- ☐ 点击“**Edit**”图标，打开“**Edit Policy List**”窗口。
- ☐ 点击“**Add Unified Policies**”下拉列表。当前配置的所有统一策略都会出现在列表中。
- ☐ 点击“**Add**”图标，打开“**Create Policy**”窗口。创建一个新的策略添加到列表中。
- ☐ 点击“**Edit**”按钮以编辑统一策略。更新的策略列表显示在界面上。

■ **删除策略列表**

- ☐ 选择要删掉的一个或多个列表。
- ☐ 点击“**Delete**”图标。
- ☐ 在确认提示上单击“**Yes**”。

注意：不能删除与访问角色配置文件关联的策略列表。如果要删除，必须先从相关的访问角色配置文件中删除该列表。

8.2.4 位置策略

位置策略界面显示所有已配置的位置策略，并用于创建、编辑和删除位置策。位置策略定义了设备可以访问网络的特定位置。该策略与访问角色配置文件相关联，适用于访问角色配置文件中分类的设备。

■ **创建位置策略**

- ☐ 点击“**+**”图标。
- ☐ 按照以下描述填写字段。
- ☐ 点击“**Save**”按钮。
  - ► **Name：**用户配置的位置策略名称。
  - ► **AP Location：**设备可以访问网络的AP的配置位置。

► **AP Name**：设备可以访问网络的AP的配置名称。

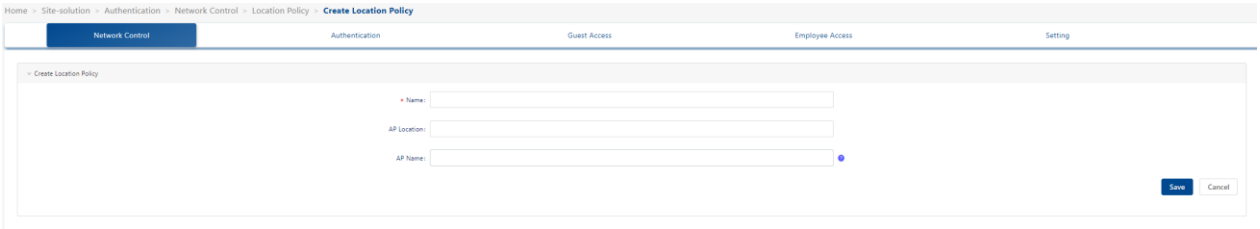


图 150：位置策略

■ **编辑位置策略**

☐ 在位置策略列表中选择策略。
☐ 点击“**Edit**”图标，打开“**Edit Location Policy**”窗口。
☐ 按照上述描述编辑字段。
☐ 点击“**Save**”按钮以保存更改。
注意：无法编辑配置文件名称。

■ **删除位置策略**

☐ 在位置策略列表中选择策略。
☐ 点击“**Delete**”图标。
☐ 在确认提示上单击“**Yes**”。

8.2.5 时间策略

时间策略界面显示所有已配置的时间策略，用于创建、编辑和删除时间策略。时间策略规定了设备可以访问网络的天数和次数。该策略与访问角色配置文件相关联，适用于访问角色配置文件中分类的设备。

■ **创建时间策略**

☐ 点击“**+**”图标。
☐ 按照以下描述填写字段。
☐ 点击“**Save**”按钮。

► **Name**：用户配置的时间策略名称。
► **Date/Time**：单击Days/Months、Date/Time和Time of Day滑块，配置设

备可以访问网络的时间。

- **Start Time**：Access Role Profile中Period Policy的生效时间。
- **End Time**：Access Role Profile中Period Policy的失效时间。
- **Timezone**：选择适用于时间策略的时区。

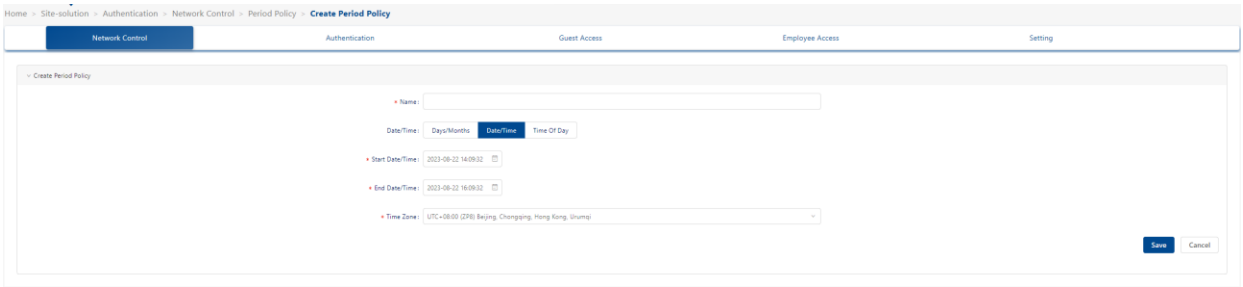


图 151：时间策略

■ 编辑时间策略

☐ 从时间策略列表中选择一个策略。

☐ 点击“**Edit**”图标，打开“**Edit Period Policy**”窗口。

☐ 按照上述描述编辑字段。

☐ 点击“**Save**”按钮以保存更改。

注意：无法编辑配置文件名称。

■ 删除时间策略

☐ 从时间策略列表中选择一个策略。

☐ 点击“**Delete**”图标。

☐ 在确认提示上单击“**Yes**”。

8.3 身份验证

身份验证模块用于配置用户访问策略。

8.3.1 仪表盘

仪表盘由4个图表组成。

Authentication Result Statistic：图 152展示了身份验证的结果（成功/失败）。认证方法包括MAC、802.1x和强制登录页。客户类型包括员工、公司设备、未知和访客。时区包括由几个不同的时区。

剩下的3个图表显示标签中描述的内容，分别是“Top 10 AP with Authentication Request”、“Top 10 AP with Authentication Failure”和“Top 10 Reason of Authentication Failure”。

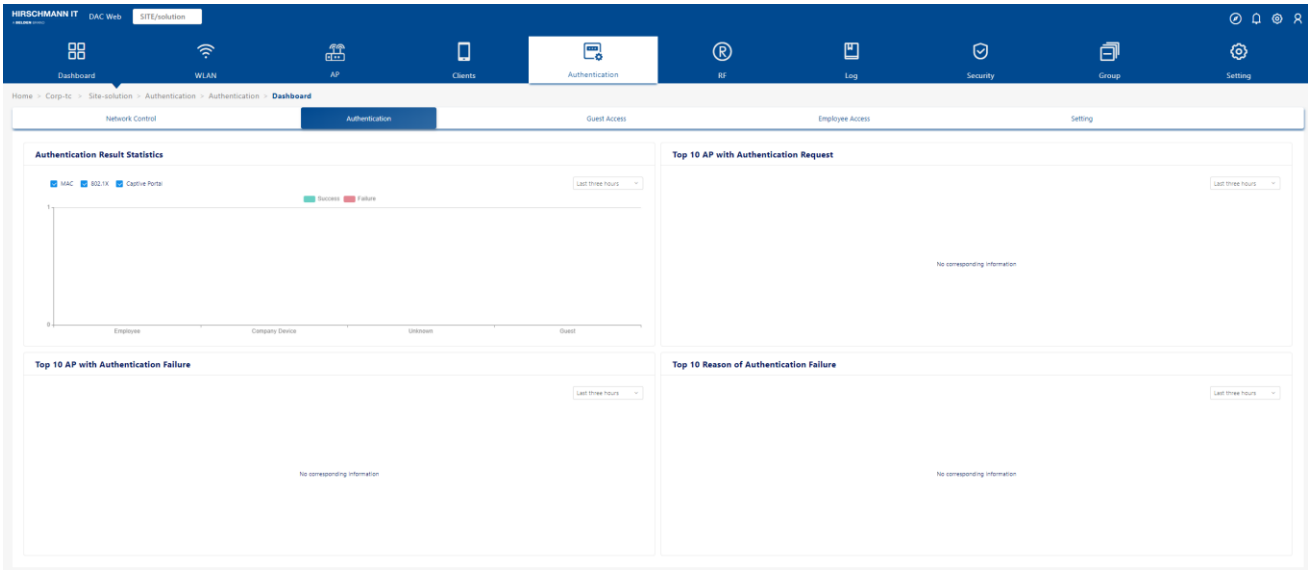


图 152：身份验证 Dashboard

8.3.2 访问策略

身份验证访问策略用于定义身份验证策略的映射条件。通过访问策略配置，可以将**身份验证策略**应用于不同的用户组，这些用户组可以根据SSID或其他属性进行划分。**访问策略**界面显示所有已配置的访问策略，并用于创建、编辑和删除访问策略。

- **Name：**用户配置的策略名称。

► **Priority**：访问策略优先级。

请求身份验证的用户可能匹配多个访问策略，优先级最高的策略将在身份验证后生效。（可选值：1..99，1代表最高优先级，99代表最低优先级）

► **Mapping Condition**：对于添加到策略的条件的描述说明。

► **Authentication Strategy**：在匹配访问策略时，使用的身份验证策略。

■ 创建访问策略

☐ 点击“**+**”图标，打开“**Create Access Policy**”窗口。

☐ 输入下列字段。

☐ 点击“**Save**”按钮。

► **Name**：用户配置的策略名称。

► **Priority**：访问策略优先级。

请求身份验证的用户可能匹配多个访问策略，优先级最高的策略将在身份验证后生效。（可选值：1..99，1代表最高优先级，99代表最低优先级）

► **Mapping Condition**：选择一个属性然后选择或输入一个值。

► **Authentication Type**：

- **802.1X**：802.1X身份验证。
- **MAC**：MAC身份验证。

► **Network Type**：

- **Wireless**：无线网络。

► **SSID**：选择Site的无线网络SSID。

► **AP IP**：输入AP IP地址或从下拉列表中选择AP IP地址。

► **AP Name**：输入AP名称或从下拉列表中选择AP名称。

► **User Mac**：输入用户MAC地址。

► **Authentication Strategy**：在匹配访问策略时，使用的身份验证策略。

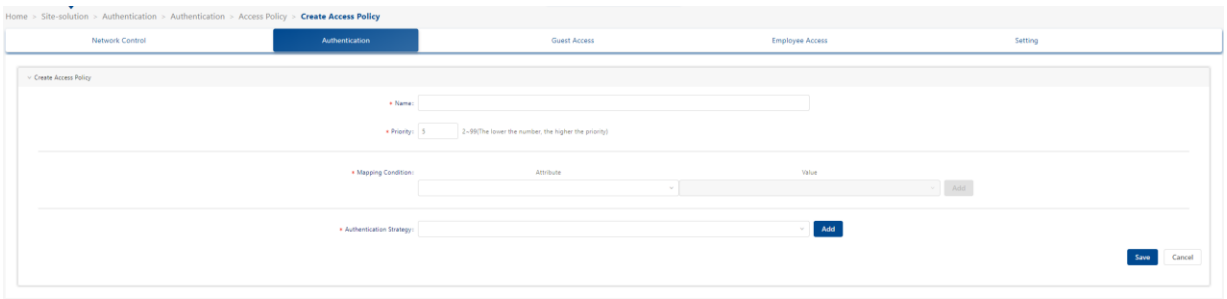


图 153：访问策略

■ **编辑访问策略**

☐ 从访问策略列表中选择一个策略。
☐ 点击**“Edit”**图标。
☐ 如上所述编辑字段。
☐ 点击**“Save”**按钮。
注意：无法编辑策略名。

■ **删除访问策略**

☐ 从访问策略列表中选择一个策略。
☐ 点击**“Delete”**图标。
☐ 在确认提示上单击**“Yes”**。

8.3.3 身份验证策略

身份验证策略用于设置用户配置文件源和登录方法（网页或非网页）以进行身份验证，以及通过身份验证后网络属性的应用。

身份验证策略界面显示所有已配置的身份验证策略，并用于创建、编辑和删除身份验证策略。

■ **创建身份验证策略**

☐ 点击**“+”**图标，打开**“Create Authentication Strategy”**界面。
☐ 输入下列字段。
☐ 点击**“Save”**按钮。

通用

- **Strategy Name**：身份验证策略名称。
- **Authentication Source**：指定用户配置文件的来源（帐户或密码）。用户配置文件可以保存在不同的服务器上，并且需要指定，以便认证能够获取用户配置文件进行身份验证。
  - **None**：针对“**None**”进行身份验证。仅支持MAC身份验证，需要强制登录页身份验证。不支持802.1x身份验证。在这种情况下，用户首先需要通过强制登录页认证（认证方法可以是帐号+密码或访问码），用户的MAC地址将被存储，用户将完成MAC认证。对于访客用户，设备将显示在**Authentication→Guest Access→Guest Device→Remembered Device**。对于员工用户，设备将显示在**Authentication→Employee Access→Employee Device→Remembered Device**。
  - **Local Database**：针对本地数据库中的用户配置文件进行身份验证。在认证之前，必须创建员工或访客用户。在Authentication→Employee Access→Employee Account界面上创建员工用户。在Authentication→Guest Access→Guest Account界面上创建访客用户。
  - **External LDAP/AD**：针对外部LDAP/AD服务器中的用户配置文件进行身份验证。在Authentication→Setting→LDAP/AD Configuration界面上配置服务器。
  - **External Radius**：针对外部RADIUS服务器中的用户配置文件进行身份验证。在Authentication→Setting→External Radius界面上配置服务器。

Web重定向执行策略

- **Web Authentication**：指定是否需要网页重定向，以及在身份验证期间将使用哪个网页登录页面。
  - **Guest**：在身份验证时，重定向到访客登录页面。
  - **Employee**：在身份验证时，重定向到员工登录页面。
- **Access Strategy**：为每个用户组指定访问策略。
  - **Guest Access Strategy**：指定访客用户的访问策略。
  - **Employee Access Strategy**：指定员工用户的访问策略。

网络执行策略

- **Default Access Role Profile**：绑定到员工帐户的访问角色配置文件。
- **Default Policy List**：身份验证策略的默认访问策略。

- **Session Timeout Status**：如果设置为OFF，则用户会话永不超时。
- **Session Timeout Interval**：会话超时间隔是允许用户连接在会话结束或提示之前的最大连续连接秒数。如果未配置，则会使用设备的默认会话超时策略。（可选值：2000..86400，默认值：43200）
- **Account External Radius**：是否将记帐消息转发到外部RADIUS服务器。
- **Accounting Interim Interval**：RADIUS记帐的间隔，以秒为单位。如果未配置，则使用设备的默认记账策略。（可选值：60..1200，默认值：600）

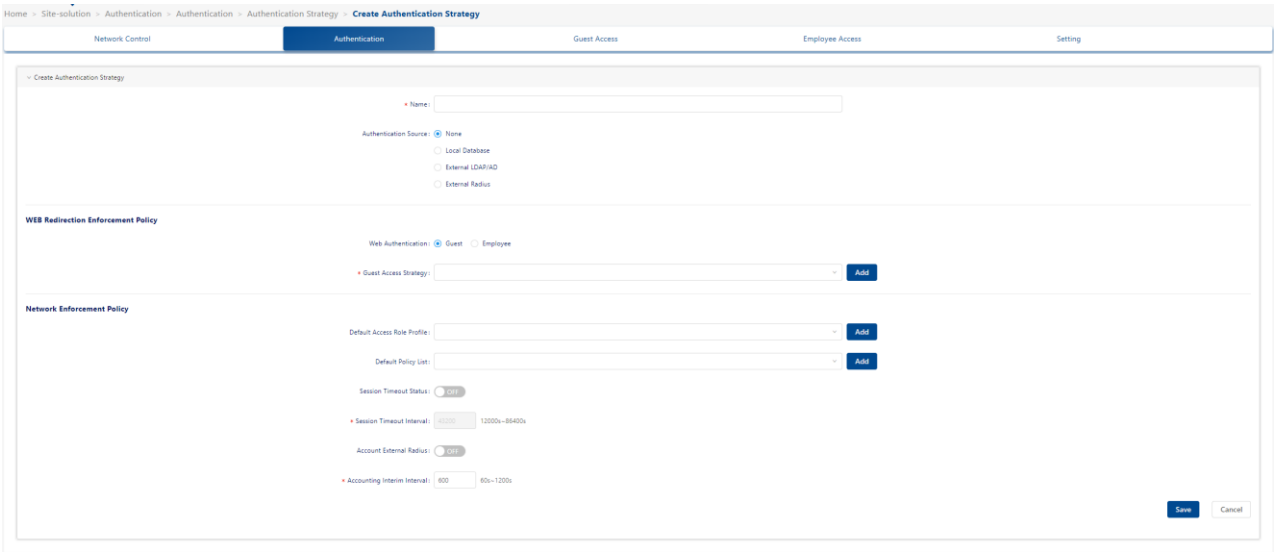


图 154：身份验证策略

8.3.4 LDAP 的角色映射

LDAP/AD的身份验证角色映射功能可根据用户属性创建映射规则，基于用户属性为不同的子用户组分配不同的访问角色配置文件和策略列表。LDAP/AD的角色映射界面显示所有已配置的映射，并用于创建、编辑和删除映射。

角色映射列表显示所有已配置映射的信息。

- **Name**：用户为映射规则配置的名称。
- **Default Access Role Profile**：匹配角色映射规则后应用于用户的访问角色配置文件。
- **Priority**：角色映射规则的优先级。
- **LDAP/AD Attributes Condition**：为策略配置的映射条件。

- **Default Policy List**：匹配角色映射规则后应用于用户的策略列表。

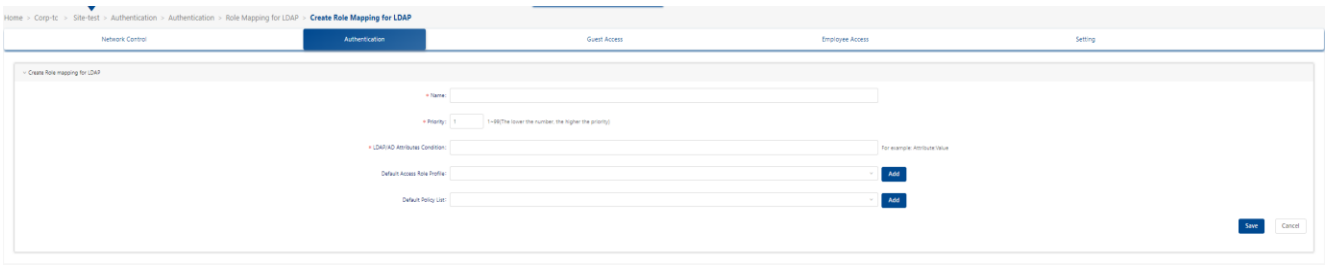


图 155：: LDAP 的角色映射

请求LDAP/AD身份验证的用户可能匹配多个角色映射规则，其中优先级最高的一个角色映射规则将在身份验证后生效。（可选值：1..99，1是最高优先级，99是最低优先级）。

■ 为LDAP创建角色映射

- **Name**：用户为映射规则配置的名称。
- **Default Access Role Profile**：匹配角色映射规则后应用于用户的访问角色配置文件。
- **Priority**：角色映射规则的优先级。请求LDAP/AD身份验证的用户可能匹配多个角色映射规则，其中优先级最高的一个角色映射规则将在身份验证后生效。（可选值：1..99，1是最高优先级，99是最低优先级）。
- **LDAP/AD Attribute Condition**：用于引用LDAP/AD帐户的属性和值对。
  - **Attribute**：用作角色映射规则键的LDAP/AD属性。
  - **Value**：角色映射规则值。
- **Default Policy List**：匹配角色映射规则后应用于用户的策略列表。

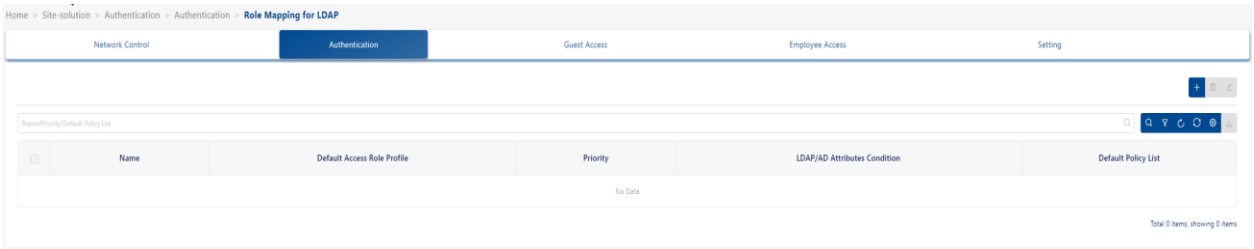


图 156：LDAP 的角色映射

■ **编辑映射**

☐ 从角色映射列表中选择一个映射。
☐ 点击**“Edit”**图标。
☐ 如上所述编辑字段。
☐ 点击**“Save”**按钮。

注意：无法编辑映射名称。

■ **删除映射**

☐ 从角色映射列表中选择一个映射。
☐ 点击**“Delete”**图标。
☐ 在确认提示上单击**“Yes”**。

8.3.5 身份验证记录

验证记录界面显示了所有通过验证的设备的验证信息。验证记录列表提供基本信息。

► **Account：**要进行身份验证的用户的用户名。

- **MAC Authentication：**账户名称是用户设备的MAC地址。
- **802.1X Authentication：**账户名是员工用户的用户名。
- **Captive Portal Authentication：**账户名是访客用户或员工用户的用户名。

► **Device IPv4：**用户请求身份验证的客户端设备的IPv4地址。

注意：只有在发送或接收RADIUS记帐报文时已知IP地址，才会显示IP地址。对于MAC身份验证，记账开始报文通常不包含客户端IP地址。

► **Device IPv6：**用户请求身份验证的客户端设备的IPv6地址。

注意：只有在发送或接收RADIUS记账报文时已知IP地址，才会显示IP地址。对于MAC身份验证，记账开始报文通常不包含客户端IP地址。

► **Device MAC：**用户设备请求认证的MAC地址。

► **Account Type：**请求身份验证用户所属的组：

- Guest
- Employee

- Unknown（无需强制登录页的MAC身份验证）

- **Session Start：**用户通过身份验证并创建连接会话的时间。
- **Acct Status Type：**记账状态。
- **Acct Interim Interval：**此特定会话的每次临时更新之间的间隔秒数，以秒为单位。
- **Session Timeout：**指定会话终止前提供的最长服务秒数。
- **Session ID：**会话ID可方便地在日志文件中匹配开始记录和停止记录。给定会话的开始和停止记录必须具有相同的会话ID。
- **Access Device MAC：**用户设备所连接的NAS的MAC地址。
- **Access Device Name：**用户设备所连接的NAS的系统名称。
- **Association SSID：**由DAP广播的无线服务。用户设备连接到此SSID（仅适用于无线）。
- **Auth Resource：**用于身份验证的用户配置文件数据库，包括None、本地数据库、LDAP/AD和外部RADIUS服务器。参考身份验证策略定义。
- **Expire Time：**账户过期时间。
- **Framed MTU：**为用户配置的最大传输单位。固定值=1400。
- **NAS IP：**NAS的IP地址。
- **NAS Port：**对用户进行身份验证的NAS的物理端口号。对于AP来说，它是无线电索引号。
- **Network Type：**只能是无线网络。
- **Service Type：**此属性指示用户请求或提供的服务类型。可以在Access-Request和Access-Accept数据包中使用。NAS不必实施所有这些服务类型，并且必须将未知或不受支持的服务类型视为已收到Access-Reject。
- **Access Device Location：**用户设备所连接的DAP的位置。

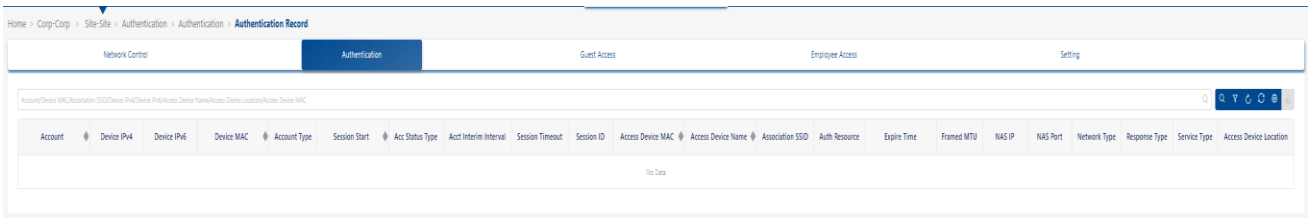


图157：身份验证记录

8.3.6 门户访问记录

身份验证门户访问记录界面上显示了DAC上所有已通过身份验证的设备的强制登录页信息。门户访问记录列表提供以下基本信息。

- **User Name**：请求身份验证的设备的用户名。
- **User MAC**：用户设备请求强制登录页身份验证的MAC地址。
- **AP MAC**：AP MAC地址。
- **ESSID**：门户用户关联的ESSID。
- **Connection Time**：门户用户的登录时间。
- **Offline Time**：门户用户的注销或超时时间。
- **Status**：用户身份验证请求的结果。
  - **Online**：强制登录页身份验证已被接受。
  - **Reject**：强制登录页身份验证已被拒绝。
  - **Empty Value**：强制门户身份验证未激活。
- **Portal Type**：强制登录页用途（Employee或Guest）。
- **AP Name**：用户连接的AP的名称。
- **AP Location**：用户所连接的AP的位置。

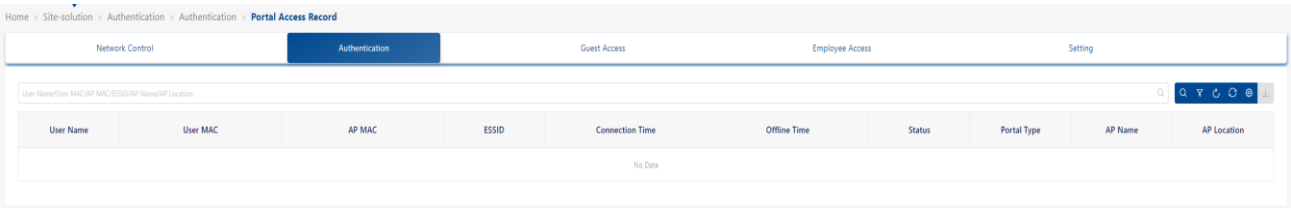


图 158：门户访问记录

8.4 访客接入

访客接入用于管理访问网络的访客用户。访客接入服务基于强制登录页身份验证，它由仪表盘、访客接入策略、访客帐户和访客设备组成。

8.4.1 仪表盘

仪表盘由以下4个部分组成：

- **Guest Account and Device Statistics**：计算不同类型的账户数量（新创建的账户、在线的访客账户、总访客账户）或设备数量（总访客设备）。
- **Guest Device Browser**：浏览器类型的饼图（Chrome、IE等）。
- **Guest Device Category**：设备类别的饼图（电脑、移动设备等）。
- **Guest Account Creation Mode**：账户创建模式的饼图。

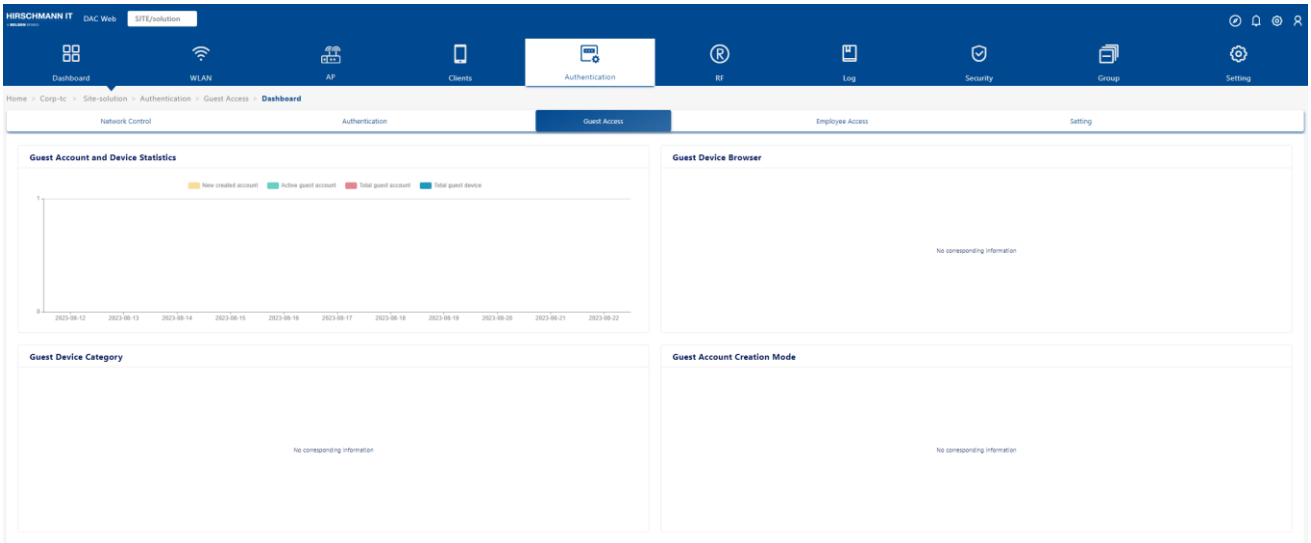


图 159：访客接入仪表盘

8.4.2 访客接入策略

访客接入策略界面用于配置访客用户的访问属性。该界面用于创建、编辑和删除访客接入策略，可以编辑预配置的默认访客接入策略，或者创建新的访客接入策略。

- **Name**：访客接入策略的名称。

- **Authentication Resource**：本地数据库。
- **Account Validity Period**：账户有效期。
- **Device Validity Period**：设备MAC身份验证的有效期。
- **Max Device per Account**：限制同时使用此访客账户的设备数量。
- **Fixed Access Role Profile**：通过身份验证后，分配给访客帐户的访问角色配置文件。
- **Fixed Policy List**：通过身份验证后，分配给访客用户的策略列表。

■ 创建访客接入策略

☐ 点击“**+**”图标并根据以下描述填写字段。

☐ 点击“**Save**”按钮。

通用

配置重定向和身份验证属性。

- **Name**：访客策略名称。
- **Authentication Resource**：访客用户配置文件数据库，即本地数据库。访客用户帐户可以在Authentication Profile→Guest Access→Guest Account界面上添加。

■ 注册策略

- **Account Validity Period**：访客账户的有效期。（可选值：1..180天，默认值：90天）。
- **Device Validity Unit**：设备有效期的分类器。可选择单位为天或分钟。
- **Device Validity Period**：用户设备的有效期。（可选值：1..365天，默认值：1天）。认证成功后，它会记住设备的MAC地址。将首先进行MAC地址检查，允许设备在有效期内无需重新认证，可直接访问。
- **Max Device per Account**：单个帐户可以访问网络的最大设备数量。（可选值：1..10，默认值：1）。

门户

- **Custom Portal Page**：可以在门户认证时编辑页面类型和页面样式。请参阅第242页的“强制登录页”。

门户身份验证后执行

- **Fixed Access Role Profile**：授权后分配给访客设备的访问角色配置文件。
- **Fixed Policy List**：在访客设备获得授权后分配的策略列表。
- **Session Timeout Status**：启用或禁用会话超时。
- **Session Timeout Interval**：会话超时间隔是在终止会话或提示之前允许用户连续连接的最大秒数。如果未配置，则设备的默认会话超时策略生效。（可选值：12000..86400，默认值：43200）
- **Account Interim-interval Status**：启用或禁用记账间隔。
- **Accounting Interim Interval**：RADIUS记帐的间隔，以秒为单位。（可选值：60..1200，默认值：600）

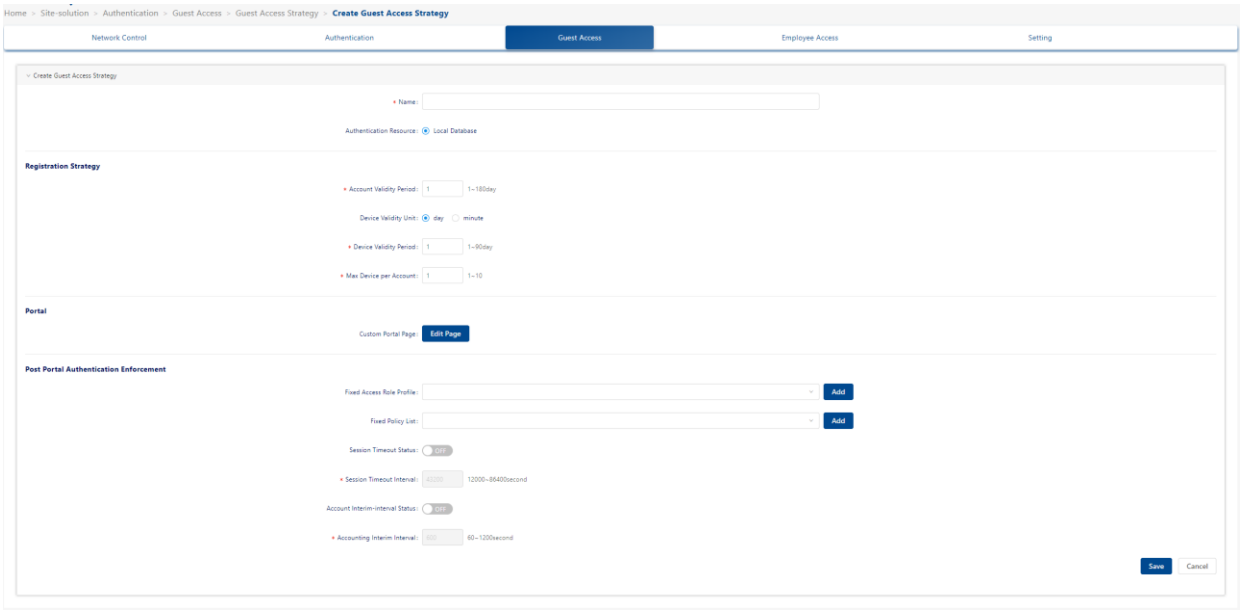


图 160：访客接入策略

■ 编辑访客接入策略

☐ 从访客接入策略列表中选择策略。

☐ 点击 **“Edit”** 图标。

☐ 根据上述说明编辑任何字段。

☐ 点击 **“Save”** 按钮。

注意：无法编辑策略名称。

■ **删除访客接入策略**

☐ 从访客接入策略列表中选择一个或多个策略。
☐ 点击**“Delete”**图标。
☐ 在确认提示上单击**“Yes”**。
注意：无法删除默认的访客接入策略。

8.4.3 访客账户

访客账户用于管理访客账户集。

☐ 您可以通过点击**“+”**图标添加项目。或者可以下载账户模板。
☐ 输入访客账户。
☐ 点击**“Batch Import”**按钮以批量导入账户。
☐ 点击**“Enable/Disable”**按钮以启用或禁用访客账户。

■ **创建访客账户：**

访客可通过账户或访问码进行访问。访问码是一种特殊类型账户，通过内部标签区分。登录时，用户使用访问码的门户模板，只需要输入访问码，无需输入密码。

☐ 点击**“Add”**图标，开**“Create Guest Account”**窗口。
☐ 输入下列字段。
☐ 点击**“Save”**按钮。创建账户后，账户将自动启用。
☐ 要禁用帐户，请选择该帐户，然后点击界面顶部的**“Disable”**图标。

访客输入账户：

► **Guest Account Name：**账户标识符（例如，访客的姓名）。
► **Password：**账户的密码。
► **Confirm Password：**重新输入以确认账户密码。
► **Full Name：**访客用户的全名。
► **Company：**公司名称。
► **Account Valid Period：**访客账户的的有效期长度。（可选值：1..180天，默认值：90天）。
► **Telephone：**访客用户的电话号码。

- ► **Email**：访客用户的电子邮件地址。
- ► **Description**：账户的说明。

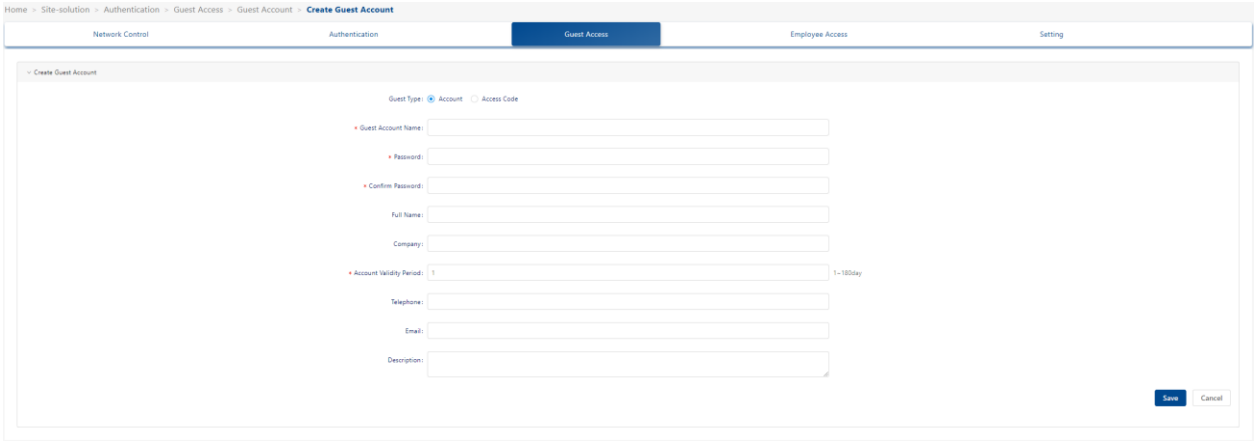


图 161：访客帐户 - “帐户”

访客输入访问码：

- ► **Access Code**：访问码。
- ► **Account Validity Period**：访客账户的有效期长度。（可选值：1..180天，默认值：90天）。
- ► **Description**：访问码的说明。

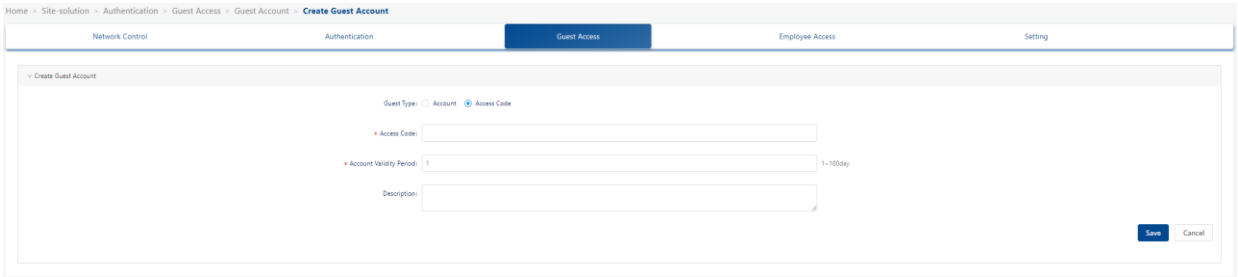


图 162：访客帐户 – “访问码”

■ 编辑访客账户/访问码

☐ 从访客账户列表中选择一个访客账户。
☐ 点击 **“Edit”** 图标。
☐ 参考如上所述描述，编辑字段。
☐ 点击 **“Save”** 按钮。

注意：无法编辑账户名。

■ **删除访客账户/访问码**

☐ 从访客账户列表中选择一个访客账户。

☐ 点击“**Delete**”图标。

☐ 在确认提示上单击“**Yes**”。

8.4.4 访客设备

访客设备由以下2个设备列表组成：

- ► 在线设备列表
- ► 已记住的设备列表

■ **在线设备**

在线设备列出了当前在线的设备。

- ► **Account Name**：终端访问网络的账户。
- ► **Device IPv4**：用户请求身份验证的客户端设备的IPv4地址。

  注意：只有在发送或接收RADIUS记账报文时已知IP地址，才会显示IP地址。对于MAC身份验证，记账开始报文通常不包含客户端的IP地址。在接收到下一个记账更新报文后将进行更新。
- ► **Device IPv6**：用户请求身份验证的客户端设备的IPv6地址。

  注意：只有在发送或接收RADIUS记账报文时已知IP地址，才会显示IP地址。对于MAC身份验证，记账开始报文通常不包含客户端的IP地址。
- ► **Device MAC**：设备的MAC地址。
- ► **Session Start**：用户通过身份验证并创建连接会话的时间。
- ► **Acct Status Type**：此记账请求标志用户服务的开始或结束。
- ► **Acct Interim Interval**：该特定会话每次临时更新之间的间隔秒数（以秒为单位）。
- ► **Session Timeout**：会话超时是在终止会话或提示之前允许用户连续连接的最大秒数。
- ► **Session ID**：会话ID可匹配日志文件中的开始记录和停止记录。给定会话的开始记录和停止记录必须具有相同的会话ID。
- ► **Access Device MAC**：与终端关联的设备的MAC地址。

- **Access Device Name**：与终端关联的设备的名称。
- **Association SSID**：终端关联使用的SSID。
- **Auth Resource**：用于身份验证的用户配置文件数据库（例如，None，本地数据库，LDAP/AD，外部RADIUS服务器）。可以参考身份验证策略定义。
- **Expiration Time**：设备的失效时间。
- **Framed MTU**：未通过其他方式（例如PPP）协商时为用户配置的最大传输单元。这是一个固定值1400。
- **NAS IP**：DAP的IP地址。
- **NAS Port**：对用户进行身份验证的NAS的物理端口号。对于AP来说，它是无线电索引号。
- **Network Type**：网络类型。只能是无线网络。
- **Response Type**：响应类型。
- **Service Type**：此属性表示用户请求或提供的服务类型。只能通过登录用户访问。
- **Access Device Location**：与终端关联的设备位置。

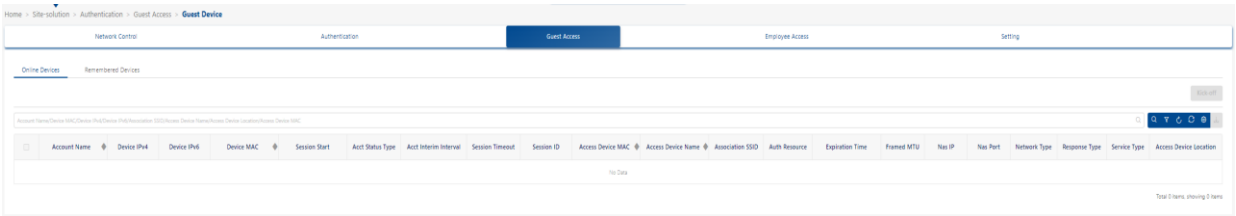


图 163：访客设备

■ 已记住的设备

记录设备列表显示DAC中保存的所有已通过身份验证的GUEST设备，可用于MAC身份验证。

- **Account Name**：已记住的设备的帐户。
- **Device MAC**：已记住的设备的MAC地址。
- **Device Name**：已记住的设备的名称。
- **Device OS**：已记住的设备的操作系统。
- **Expiration Time**：设备的失效时间。

► **First Login Time**：记录首次登录时间。

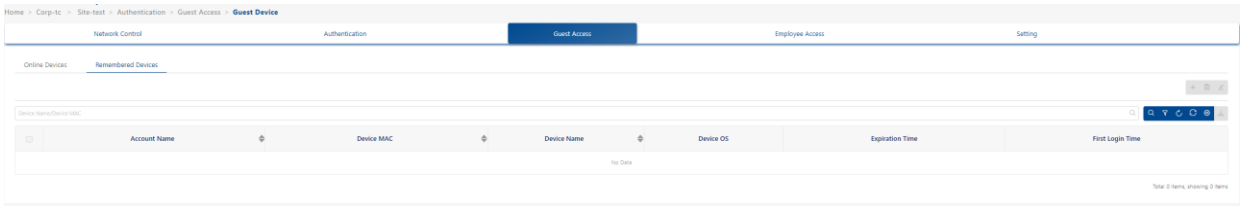


图 164：已记住的设备

8.5 员工接入

员工接入模块用于管理员工接入网络。它由仪表盘、员工接入策略、员工账户和员工设备组成。

8.5.1 仪表盘

仪表盘由以下3个图表组成：

- **Remembered Employee Device：**最近7天记忆设备与在线设备的直方图。
- **Device Category：**设备类别的饼图（计算机、移动设备等）
- **Device Family：**以饼图格式显示按设备系列分类的信息（例如苹果、IBM、华为、小米）。

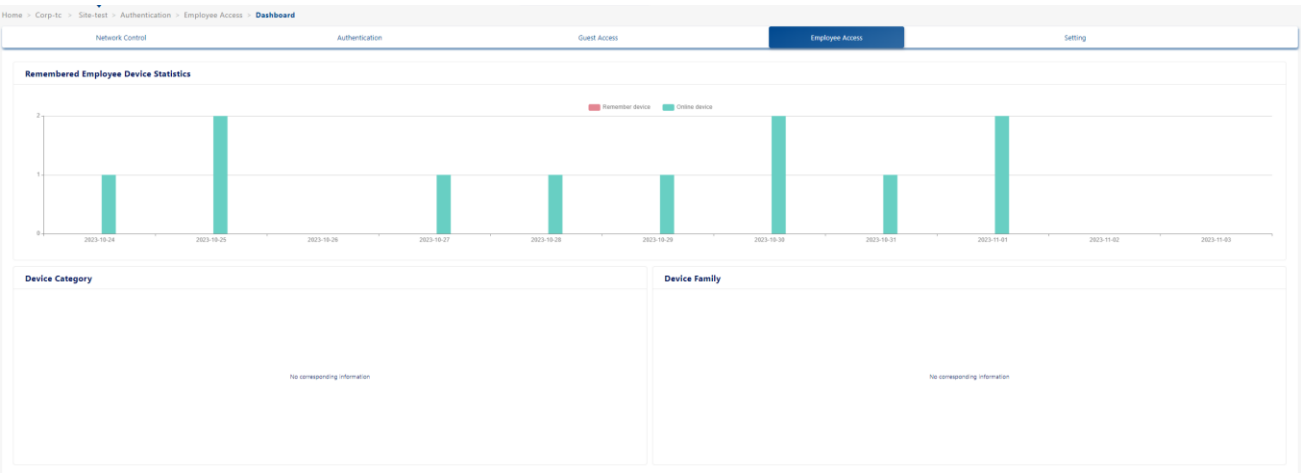


图 165：员工接入仪表盘

8.5.2 员工接入策略

员工策略模块用于配置员工门户策略。它可以配置门户账户身份验证源（包括本地数据库、外部LDAP或AD和外部RADIUS）、账户有效性和设备有效性、在线设备的最大数量、指定访问角色配置文件策略、编辑门户模板等。

- **Name：**员工策略名称。
- **Authentication Source：**指定身份认证数据的来源。

- **Device Validity Period**：访客通过认证后，会有免认证记录。此处指定了免身份验证记录的有效期。
- **Max Device per Account**：可以使用同一账户同时登录的终端数量。
- **Portal Type**：门户页来源，可来自DAC或外部。
- **Customization Portal Page**：可以在门户身份验证时编辑页面类型和页面样式。
- **Fixed Access Role Profile**：当结束身份验证阶段时，分配给终端的访问角色配置文件用来控制终端的网络访问行为。
- **Fixed Policy List**：通过身份验证后，分配给AP的策略列表用于给终端消息设定过程策略。
- **Session Timeout Interval**：指定AP发送会话消息的间隔。
- **Accounting Interim Interval**：指定AP发送记账消息的时间间隔。

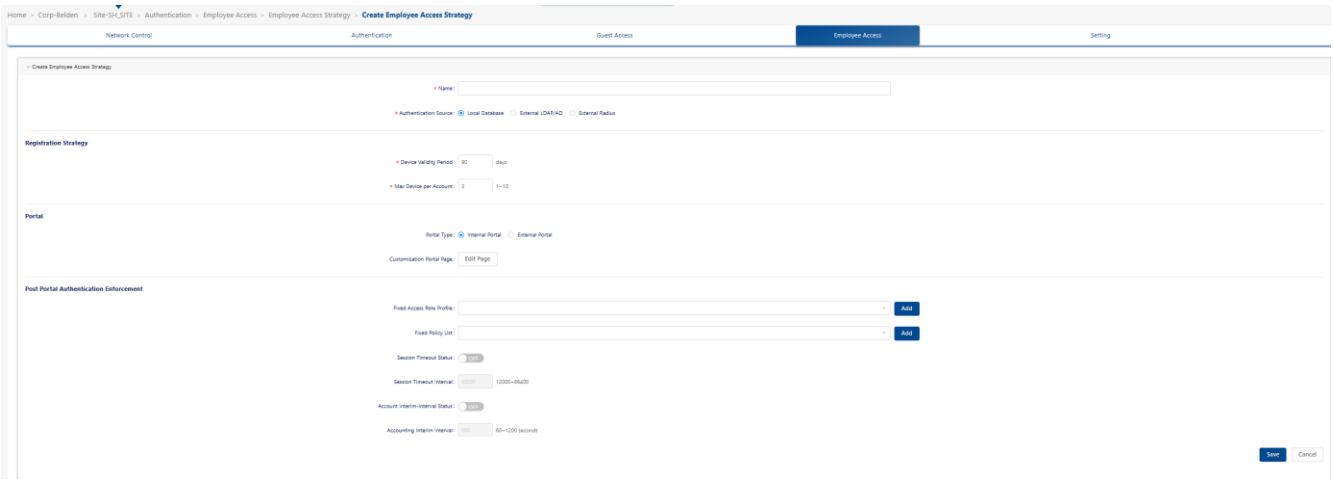


图 166：员工接入策略

8.5.3 员工账户

员工账户用于管理员工终端账户集。

- ☐ 单击“**+**”图标或下载账户模板来添加一个项目。
- ☐ 输入员工账户详细信息。也支持批量导入账号。
- ☐ 单击“**Enable/Disable**”按钮以手动启用或禁用员工账户。

员工账户列表显示有关所有已配置员工账户的信息。

- **Username**：账户的用户名。
- **Full Name**：员工的全名。
- **Email**：电子邮件地址。
- **Telephone**：电话号码。
- **Access Role Profile**：与员工账户绑定的访问角色配置文件。它优先于在身份验证策略中配置的访问角色配置文件。
- **Department**：所属部门。
- **Position**：岗位。
- **Policy List**：与员工账户绑定的策略列表。它优先于在身份验证策略中配置的策略列表。
- **Description**：账户说明。
- **Status**：员工账户为启用或禁用状态。

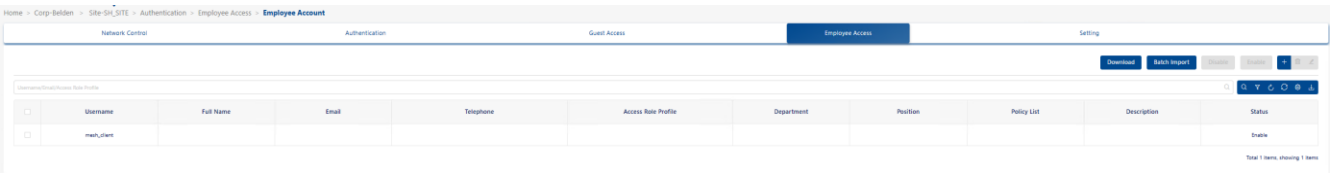


图 167：员工账户

■ 创建员工账户

- **Username**：账户用户名。
- **Password**：账户密码。
- **Repeat Password**：重新输入以确认密码。
- **Telephone**：电话号码。
- **Email**：电子邮件地址。
- **Access Role Profile**：与员工账户绑定的访问角色配置文件。它优先于在身份验证策略中配置的访问角色配置文件。
- **Policy List**：与员工账户绑定的策略列表。它优先于在身份验证策略中配置的策略列表。
- **Full Name**：员工的全名。
- **Department**：所属部门。
- **Position**：岗位。

► **Description**：账户说明。

■ **编辑员工账户**

☐ 在员工账户列表中选择一个员工。
☐ 点击“**Edit**”图标。
☐ 填入上述字段。
☐ 单击“**Save**”按钮。
注意：无法编辑用户名。

■ **删除员工账户**

☐ 在员工账户列表中选择一个员工。
☐ 点击“**Delete**”图标。
☐ 在确认提示上单击“**Yes**”。

8.5.4 员工设备

员工设备包括以下2种类型：

► 在线设备

► 已记住的设备

在线设备列表列出了当前在线的设备。

已记住的设备列出了在设备有效期内下一次访问过程中无需验证的设备。

■ **在线设备**

在线设备列表显示与员工账户关联并已访问网络的设备信息账户。

☐ 在列表中选择一个设备。
☐ 单击“**Kick-off**”按钮，立即将该用户从网络中注销。
☐ 该用户必须再次登录才能连接到网络。

► **Account**：与公司设备关联的员工账户。

► **Device IPv4**：用户请求身份验证的客户端设备的IPv4地址。

注意：只有在发送或接收RADIUS记账报文时已知IP地址，才会显示IP地址。对于MAC身份验证，记账开始报文通常不包含客户端IP地址。

- **Device IPv6**：用户请求身份验证的客户端设备的IPv6地址。

  注意：只有在发送或接收RADIUS记账报文时已知IP地址，才会显示IP地址。对于MAC身份验证，记账开始报文通常不包含客户端IP地址。
- **Device MAC**：设备的MAC地址。
- **Session Start**：用户通过身份验证并创建连接会话的时间。
- **Acct Status Type**：表示此记账请求标记了用户服务的开始还是结束。
- **Acct Interim Interval**：该特定会话的每次临时更新之间的间隔秒数，以秒为单位。
- **Session Timeout**：会话超时是在终止会话或提示之前允许用户连接的最大连续秒数。
- **Session ID**：会话ID可以匹配日志文件中的开始和停止记录。指定会话的开始和停止记录必须具有相同的会话ID。
- **Access Device MAC**：与终端关联设备的MAC地址。
- **Access Device Name**：与终端关联的设备的名称。
- **Association SSID**：终端关联使用的SSID。
- **Auth Resource**：身份验证中使用的用户配置文件数据库（例如，None、本地数据库、LDAP/AD和外部RADIUS服务器）。可以参考身份验证策略定义。
- **Expiration Time**：此设备的失效时间。
- **Framed MTU**：未通过其他方式（例如PPP）协商时为用户配置的最大传输单元。它的固定值为1400。
- **NAS IP**：DAP的IP地址。
- **NAS Port**：对用户进行身份验证的NAS的物理端口号。对于AP来说，它是无线电索引。
- **Network Type**：网络类型。只能是无线网络。
- **Response Type**：响应类型。
- **Service Type**：此属性表示用户请求或提供的服务类型。只能通过登录用户访问。
- **Access Device Location**：与终端关联的设备位置。

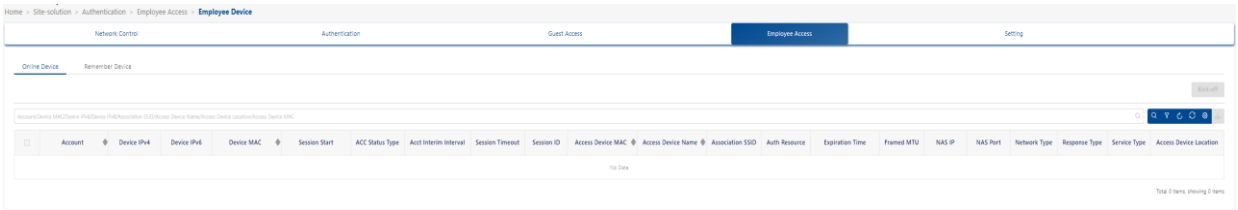


图 168：员工设备 - Online Device

■ 已记住的设备

已记住的设备列出了在下一个访问过程中不会再次进行身份验证的设备。

- ► **Account**：账户。
- ► **Device MAC**：设备的MAC地址。
- ► **Device Name**：设备的名称。
- ► **Device OS**：设备的操作系统。
- ► **Expiration Time**：失效时间。
- ► **First Login Time**：记录的首次登录时间。

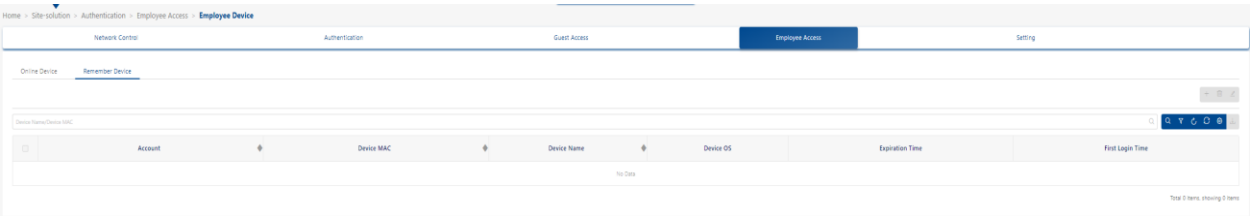


图 169：员工设备 - Remember Device

8.6 设置

设置模块包括以下配置。

8.6.1 公司设备

公司设备用于管理公司的设备组合，例如打印机、网络电话、笔记本电脑和平板电脑。

- ☐ 单击“**+**”图标或下载账户模板以添加一个项目。
- ☐ 使用公司设备填写字段。批量导入账号。可以以.xlsx格式导出所有公司设备。

■ **创建公司设备**

- ► **Device MAC**：公司设备的MAC地址。
- ► **Device Name**：公司设备的系统名称。
- ► **Account**：与公司设备关联的员工账户。
- ► **Device Category**：公司设备的类别（例如，计算机、移动平板电脑）。
- ► **Device Family**：公司设备的生产供应商（例如苹果、华为、IBM）。
- ► **Device OS**：公司设备的操作系统（例如，Linux，Windows，iOS）。
- ► **Device Specific PSK**：如果启用，则必须设置密码和密码有效期。此功能需要与设备特定PSK的WLAN设置配合使用。
- ► **Access Role Profile**：与公司设备绑定的访问角色配置文件。它优先于身份验证策略中配置的ARP。
- ► **Policy List**：与公司设备绑定的策略列表。它优先于身份验证策略中配置的策略列表。

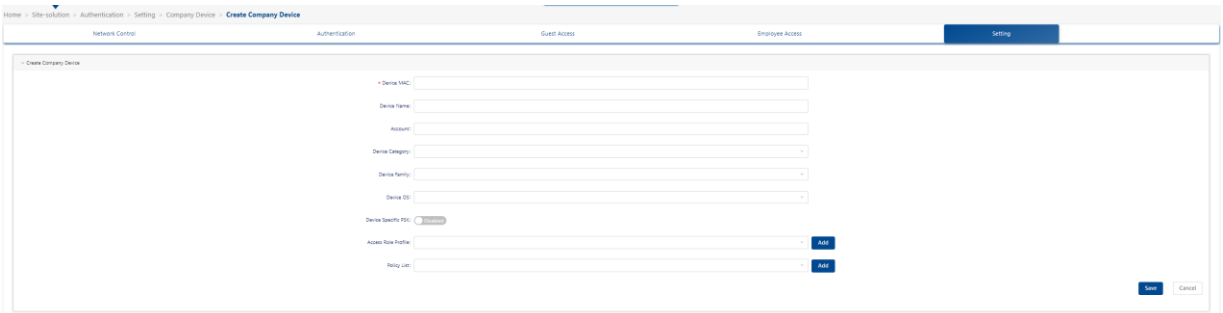


图 170：创建公司设备

■ **删除公司设备**

☐ 选择要删除的公司设备。

☐ 单击“**Delete**”图标。

☐ 在确认提示上单击“**Yes**”。

8.6.2 LDAP/AD 配置

LDAP/AD模块用于配置LDAP或AD源。为策略选择LDAP或AD身份验证时，将使用身份验证源进行身份验证。

点击“Config”按钮进行配置：

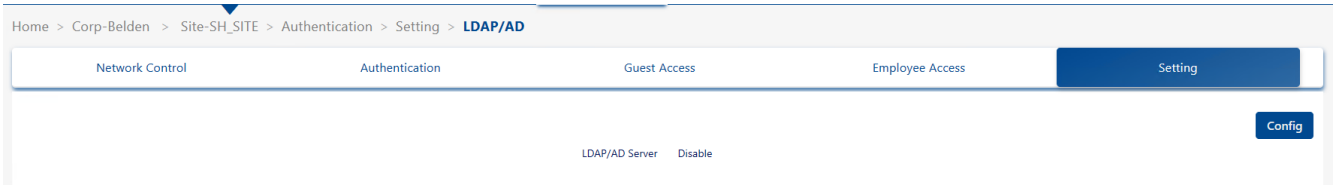


图 171：LDAP/AD 配置

■ **LDAP配置**

- ► **LDAP/AD Server**：启用或禁用LDAP或AD服务器。
- ► **Server Type**：LDAP或AD服务器。
- ► **IP Address**：LDAP服务器的IP地址。
- ► **Port**：LDAP服务器的端口。
- ► **Use TLS Encryption**：是否启用TLS加密。如果将其打开，则应上传证书。
- ► **Certificate**：上传TLS使用的证书。证书应该从外部LDAP服务器获取。
- ► **Admin Name**：用于登录LDAP服务器的管理员账户。（格式：cn=，DC：8-64个字符）
- ► **Admin Password**：用于登录LDAP服务器的管理员密码。（1－32个字符）
- ► **Search Base**：8-64个字符
- ► **Username Attribution**：LDAP条目中表示用于身份验证的用户名的字段。（1-32个字符）

- **Password Attribution**：LDAP条目中表示用于身份验证的密码的字段。（1-32个字符）
- **Object Class**：定义属性的命名集合，并将其分类为必需属性和可选属性集。（1-32个字符）

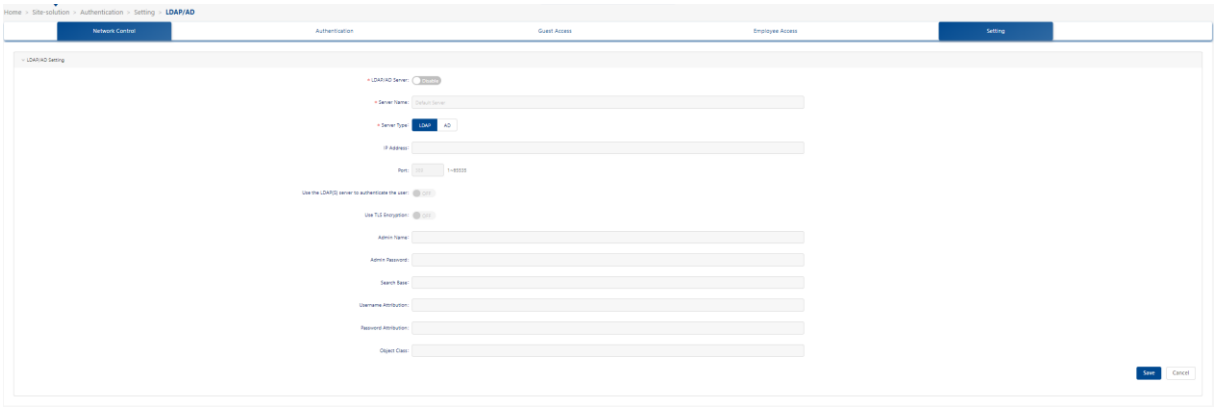


图 172：LDAP/AD 配置 - LDAP 服务器

■ AD配置

- **Workgroup Name**：AD服务器的工作组。
- **Realm**：AD服务器的域。
- **Username**：用于访问AD服务器的用户名。
- **Realm IP**：AD服务器的IP地址。
- **Password**：用于访问AD服务器的密码。
- **AD Port**：用于访问AD服务器的端口。

注意：要加载Windows AD服务器配置，请为Ubuntu系统或VM初始化配置DNS设置。

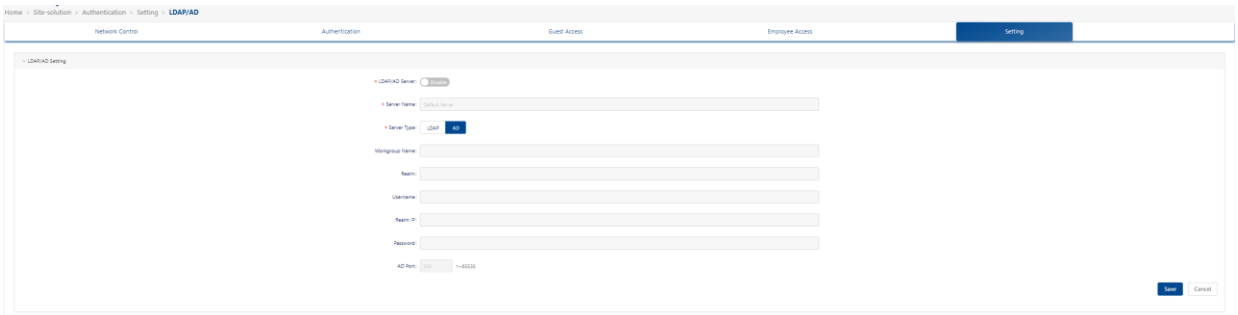


图 173：LDAP/AD 配置 - AD 服务器

8.6.3 外部 RADIUS

外部RADIUS模块用于配置外部RADIUS认证源。为策略选择外部RADIUS身份验证时，将使用身份验证源进行身份验证。

点击“**+**”图标，打开“**External Radius Setting**”窗口。

- **Server Name**：RADIUS服务器的名称。
- **IP Address**：外部RADIUS服务器主机名或IP地址
- **Backup IP Address**：备份外部RADIUS服务器主机名或IP地址。
- **Retries**：当连接超时发生之前，DAC将尝试重新连接到外部RADIUS服务器的次数。如果尝试连接的次数达到上限，仍未连接成功，则认定外部RADIUS服务日无法访问。（可选值：1..3，默认值：3）
- **Timeout**：DAC在超时之前尝试与外部RADIUS服务器建立连接的时间，以秒为单位。（可选值：1..30，默认值：5）
- **Shared Secret**：DAC与外部RADIUS服务器进行通信所使用的共享密钥。（4-64个字符）
- **Confirm Secret**：再次输入以确认共享的密钥。（4－64个字符）
- **Authentication Port**：用于执行身份验证的UDP端口。（可选值：1..65535，默认值：1812）
- **Accounting Port**：用于执行记账的TCP/UDP端口。（可选值：1..65535，默认值：1813）

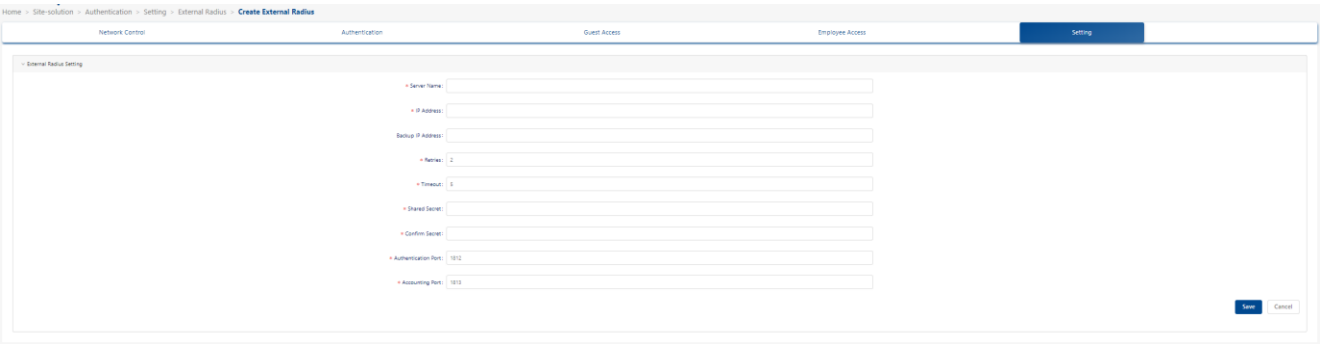


图 174：外部 RADIUS

8.6.4 外部 Portal

DAC支持用户设置员工接入策略中使用的外部portal。

■ **配置外部Portal**

▶ **Name：**外部portal配置的名称，创建后无法修改。

▶ **Portal Page URL：**外部portal的URL。

▶ **Parameter Mapping：**DAC使用的参数映射到外部portal的参数。

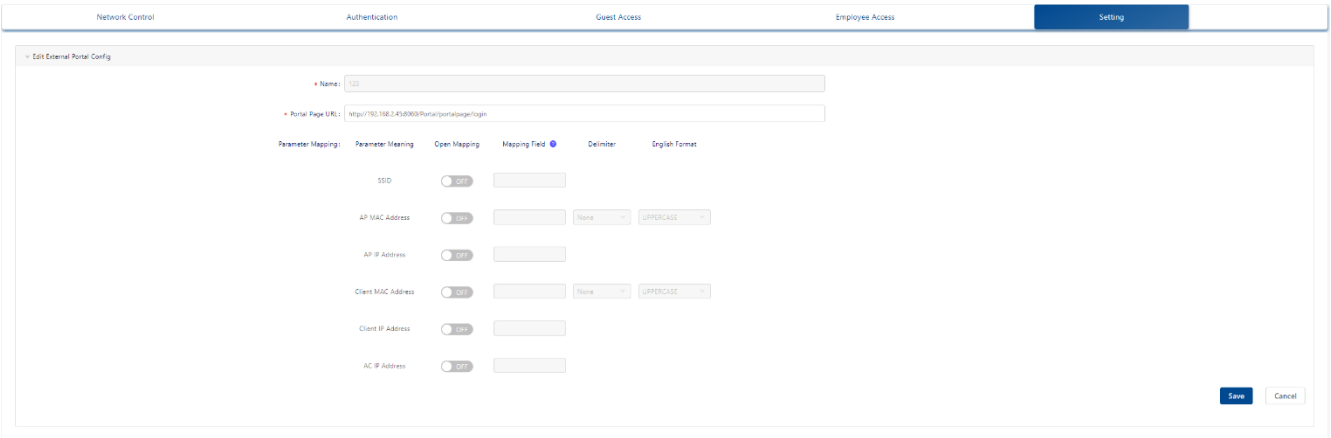


图 175：外部 Portal

8.6.5 允许的 IP

允许的IP是终端在从强制网络门户登录之前可以访问的IP。通常，应将门户网站服务器的IP添加到允许的IP中。

■ **创建允许的IP**

☐ 点击**“+”**图标，打开**“Create Allowed IP”**窗口。

☐ 填入**“Name”**和**“IP Address”**字段。

☐ 单击**“Save”**按钮以保存允许的IP。

▶ **Name：**允许的IP名称。

▶ **IP Address：**设置的IP地址。

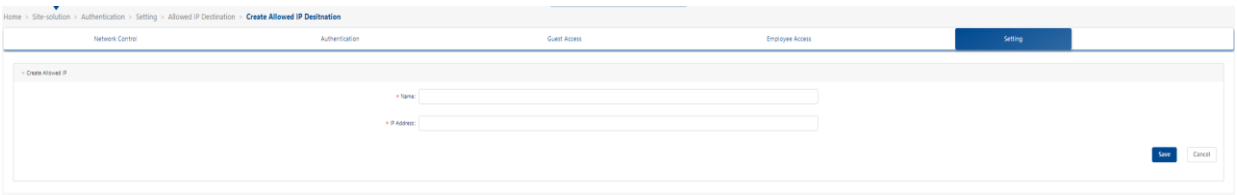


图 176：创建允许的 IP

■ **编辑允许的IP**

☐ 在列表中选择一个允许的IP。
☐ 点击“**Edit**”图标，打开“**Edit Allowed IP**”窗口。
☐ 填入“**IP Address**”字段。
☐ 单击“**Save**”按钮以保存设置。
注：无法更改“**Name**”字段。

■ **删除允许的IP**

☐ 选择要删除的IP条目。
☐ 点击“**Delete**”图标。
☐ 在确认提示上单击“**Yes**”。

8.6.6 MAC 组

MAC组界面显示所有配置的MAC组。该界面用于创建、编辑和删除MAC组，这些组可以用于创建各种策略条件，例如源MAC组条件和目标MAC组条件。

■ **创建MAC组**

☐ 点击“**+**”图标，打开“**Create MAC Group**”窗口。
☐ 为MAC组输入“**Name**”。
☐ 填入“**MAC Address**”。
☐ 点击“**Add**”按钮。
☐ 重复上述操作以添加其他MAC地址。
☐ 单击底部的“**Add**”按钮。该MAC组将显示在MAC组列表中。
注意：必须至少输入一个MAC地址。

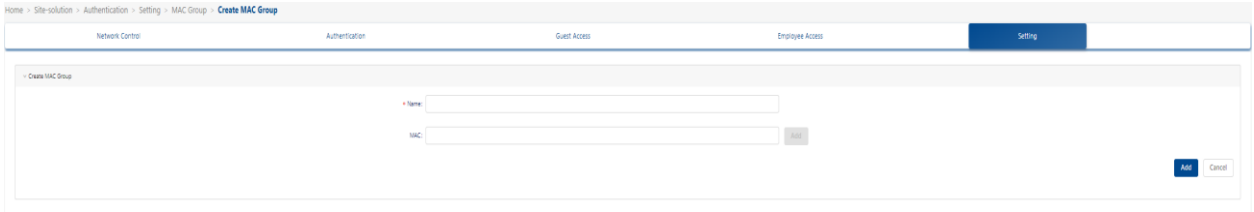


图 177：创建 MAC 组

■ 编辑MAC组

☐ 选择要编辑的MAC组。

☐ 点击**“Edit”**图标，打开**“Edit MAC Group”窗口**。

注意：无法编辑MAC组名。若要编辑MAC组名称，必须删除MAC组并重新创建一个新名称。

将MAC地址添加到组中：

☐ 输入MAC地址

☐ 点击**“Add”**按钮。

☐ 重复上述操作以添加其他MAC地址。

☐ 完成后，单击**“Edit”**按钮。

删除MAC地址：

☐ 单击要删除的MAC地址旁边的**“Delete”**图标。

☐ 重复上述操作以删除其他MAC地址。

☐ 完成后，单击**Edit**按钮。

编辑MAC地址：

☐ 删除MAC地址。

☐ 添加一个新的MAC地址。

■ 删除MAC组

☐ 选中列表中组旁边的复选框。

☐ 点击**“Delete”**图标。

☐ 在确认提示上单击**“Yes”**。

注意：无法删除由策略条件正在使用的MAC组，若要删除这些MAC组，请先将其从策略条件中移除。

8.6.7 IP 组

IP组界面显示所有已配置的IP组。该界面用于创建、编辑和删除网络组。

■ **创建IP组**

☐ 点击**“+”**图标。
☐ 为IP组输入**“Name”**。
☐ 填入**“Subnet IP/Subnet Mask”**字段。
☐ 点击**“Add”**按钮。
☐ 重复上述操作以添加其他子网。
☐ 完成添加子网后，单击底部的**“Add”**按钮。
该IP组将显示在IP组列表中。

注意：必须至少输入一个子网IP或子网掩码。

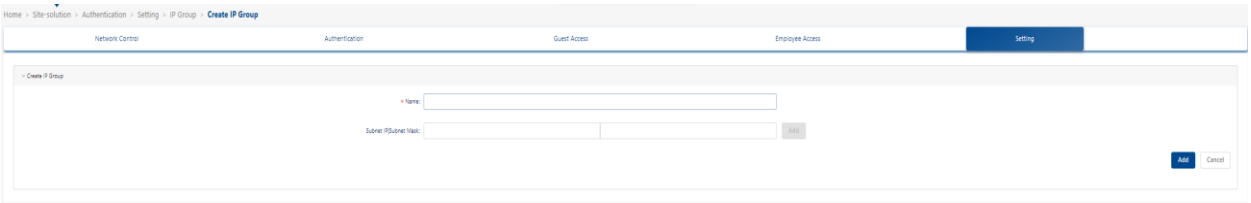


图 178：创建 IP 组

■ **编辑IP组**

☐ 单击要编辑的IP组以查看IP组中的子网。

注意：无法编辑IP组名。若要编辑IP组名称，必须删除IP组并重新创建一个新名称。

将子网地址添加到组中：

☐ 填入**“Subnet IP/Subnet Mask”**字段。
☐ 点击“Add”图标。
☐ 重复上述操作以添加其他子网。
☐ 完成添加子网后，单击**“Edit”**按钮。

删除子网：

- ☐ 单击要删除的子网旁边的“**Delete**”图标。
- ☐ 重复上一步操作以删除子网。
- ☐ 完成后，单击“**Edit**”按钮。

编辑子网：

- ☐ 删除子网。
- ☐ 添加一个新的子网。
- ☐ 完成后，单击“**Edit**”按钮。

■ **删除IP组**

- ☐ 选中列表中组旁边的复选框。
- ☐ 点击“**Delete**”图标。
- ☐ 在确认提示上单击“**Yes**”。

无法删除在策略条件下使用的IP组。若要删除这些IP组，应先将其从策略条件中移除。

8.6.8 服务

服务界面显示所有已配置的服务，这些服务用于创建服务。该界面用于创建、编辑和删除服务。

■ **创建服务**

- ☐ 点击“**+**”图标。
- ☐ 按照以下描述填写字段
- ☐ 点击“**Save**”按钮。
  - ► **Name**：用户配置的服务名称。
  - ► **Protocol**：选择服务的协议。默认情况下，选中TCP并显示TCP端口。选中UDP以显示UDP端口。
  - ► **Service Port**：从下拉列表中选择一个服务端口。如果要创建新的服务端口，请单击“**Service Port**”界面中显示的“**Add**”图标并创建新的服务端口。单击“**Service Port**”屏幕上的“**Save**”按钮时，将返回到创建服

务界面以完成服务的创建。

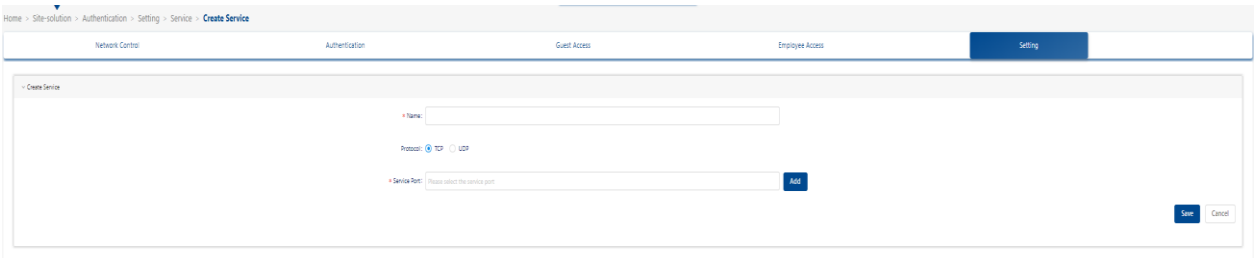


图 179：创建服务

■ **编辑服务**

☐ 单击要编辑的服务。

☐ 点击“**Edit**”图标。

☐ 按照以上描述编辑字段。

☐ 点击“**Save**”按钮。

注意：无法编辑服务名。若要编辑服务的名称，必须删除服务并重新创建一个新服务。

■ **删除服务**

☐ 选中列表中端口旁边的复选框。

☐ 点击“**Delete**”图标。

☐ 在确认提示上单击“**Yes**”。

注意：无法删除策略条件正在使用的服务。若要删除这些服务，请先将其从策略条件中移除。

8.6.9 服务组

服务组界面显示所有已配置的服务组。该界面用于创建、编辑和删除服务组。

■ **创建服务组**

☐ 点击“**+**”图标。

☐ 为服务组输入“**Group Name**”。

☐ 选择一项服务，然后单击“**Save**”按钮。

☐ 单击“**Add**”图标，然后出现“**Service**”。可以创建服务。

☐ 点击“**Save**”图标，打开“**Create Service Group**”窗口。

注意：必须至少输入一个服务。

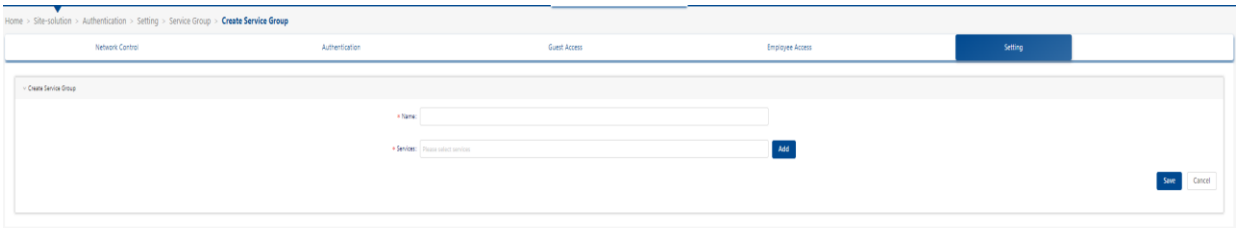


图 180：创建服务组

■ **编辑服务组**

☐ 单击要编辑的服务组。

☐ 单击“**Edit**”图标。

☐ 添加或删除组中的服务。

☐ 单击“**Edit**”按钮。

注意：无法编辑服务组名。若要编辑服务组的名称，必须删除服务组并重新创建一个新服务组。

■ **删除服务组**

☐ 选中列表中组旁边的复选框。

☐ 点击“**Delete**”图标。

☐ 在确认提示上单击“**Yes**”。

注意：无法删除策略条件下使用的服务组。若要删除这些服务组，请先将其从策略条件中移除。

8.6.10 服务端口

服务端口界面显示所有已配置的服务端口，这些端口用于创建服务。默认情况下，选中TCP，显示TCP服务；选中UDP，则显示UDP服务。该界面用于创建、编辑和删除服务端口。

■ **创建一个服务端口**

☐ 点击“**+**”图标。

☐ 按如下所述编辑字段。

☐ 点击“**Save**”按钮。

- ► **Protocol**：TCP或UDP。
- ► **Name**：用户配置的服务端口名称。
- ► **Source Port Range**：输入源端口号或端口号范围（设置范围如22:33）。
- ► **Destination Port Range**：输入目标端口号或端口号范围。

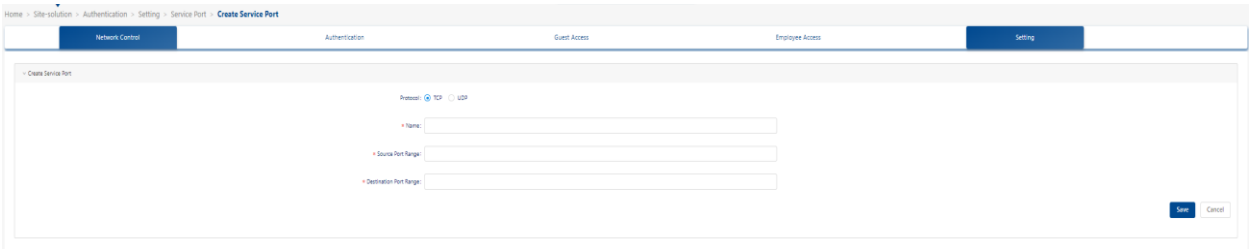


图 181：创建服务端口

■ 编辑服务端口

☐ 单击要编辑的服务端口。

☐ 点击“**Edit**”图标。

☐ 参考上述描述，编辑字段。

☐ 点击“**Save**”按钮。

注意：无法编辑服务端口名称和协议。若要编辑服务端口的名称，必须删除服务端口并重新创建一个新端口。

■ 删除服务端口

☐ 选中列表中端口旁边的复选框。

☐ 点击“**Delete**”图标。

☐ 在确认提示上单击“**Yes**”。

注意：无法删除服务正在使用的服务端口。若要删除这些服务端口，请先将其从服务中移除。

8.7 默认配置和快速入口

所有上述配置都间接绑定到WLAN。为了简化配置，可以在配置WLAN时直接选择默认配置。同时，在配置WLAN时，我们还提供了身份验证配置的快速入口，如下所示：

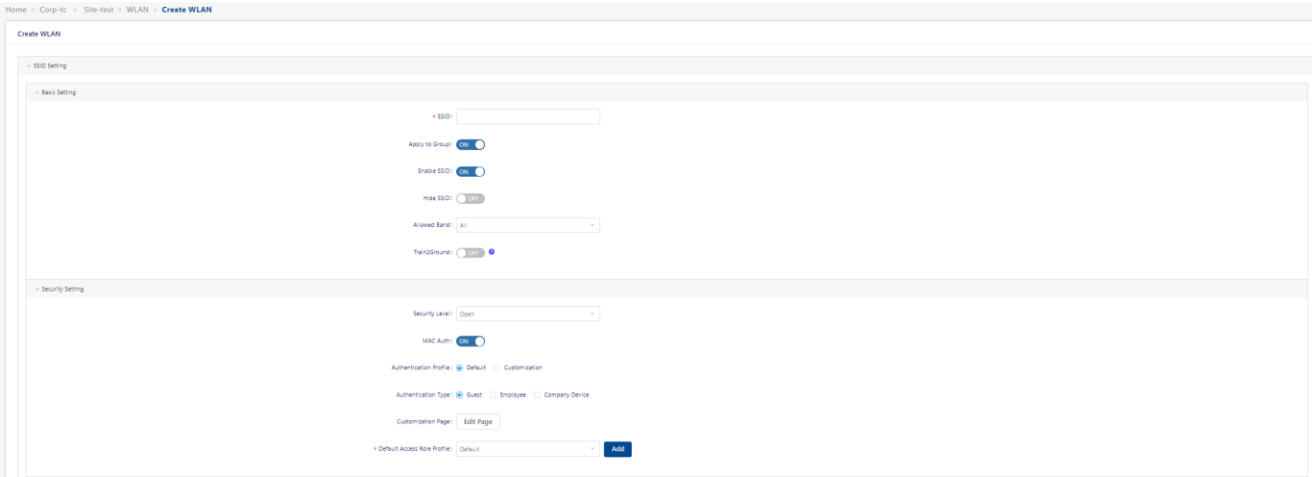


图 182：创建 WLAN

在WLAN配置中，如果选择了**“MAC auth”**，则默认选择一组默认身份验证配置。**自定义**是用户定义身份验证的快捷方式。选择**Customization**后，将出现配置向导按钮。配置与上述模块一致，本节不再赘述。

在身份验证配置中选择**“Default”**时，在后台自动生成一组身份验证配置，用户无法直接查看或编辑这些配置。

默认生成的身份验证配置如下：

- 当选择**“Guest”**作为身份验证类型时，会自动生成身份验证策略，数据源为none。同时，会生成一个访客接入策略，并绑定到身份验证策略。可以在以下Customization Page中自定义门户页面。

  当选择**“Employee”**作为身份验证类型时，会自动生成身份验证策略，数据源为none。同时，将生成一个员工接入策略，并绑定到身份验证策略。可以在以下Customization Page中自定义门户页面。
- 当选择**“Company Device”**作为身份验证类型时，将自动生成一个以本地数据库作为数据源的身份验证策略。
- 最后，它将生成一个以SSID作为映射条件的访问策略，具有最高优先级，并将其与先前提到的身份验证策略绑定。

注意：默认生成的配置绑定到WLAN，用户无法查看。

8.8 用于身份验证的配置实例

在介绍特定配置实例之前，应了解DAC中身份验证的基本概念。请参阅第141页的“身份验证”。

8.8.1 默认配置 802.1X 身份验证

- ☐ 在“**Site**”视图页面上，点击“**WLAN**”项卡以查看WLAN列表。
- ☐ 单击“**+**”按钮，打开“**Create WLAN**”页面。
- ☐ 填入**SSID**字段。
- ☐ 从下拉列表中选择“**Enterprise**”作为安全级别。
- ☐ 选择所需的**加密模式**。请参阅第95页的“SSID设置”。
- ☐ 将身份验证配置文件为**默认**，将自动创建**访问策略**、**身份验证策略**和**员工接入策略**（如果需要的话）。这些策略不可查看。但可以看到有3个身份验证源：**本地数据库**、**外部LDAP/AD**和**外部RADIUS**。这些身份验证源是从默认创建的**身份验证策略**导出的，可简化一些用户配置。
- ☐ 如果选择**本地数据库**身份验证源，则可以在**Authentication→Employee Access→Employee Account**页面添加用户。请参阅第179页的“员工账户”。
- ☐ 如果选择**LDAP/AD**身份验证源，则应在**Authentication→Setting→LDAP/AD Configuration**页面上配置LDAP/AD。请参阅第185页的“LDAP/AD配置”。如果想为通过LDAP认证的终端设置特定的**访问角色配置文件**，可以在**Authentication→Authentication→Role Mapping for LDAP**页面设置相应的映射规则。
- ☐ 如果选择**外部RADIUS**认证源，则可以从下拉列表中选择外部RADIUS服务器。或者点击“**Add**”按钮添加新的外部RADIUS服务器。还可以在**Authentication page→Setting→External Radius**页面中添加新的外部RADIUS服务器。请参阅第188页的“外部RADIUS”。
- ☐ 在**默认访问角色配置文件**中，从下拉列表中选择一个配置文件。或者，可以通过单击旁边的“**Add**”按钮来添加新的访问角色配置文件。请参阅第147页的“访问角色配置文件”。

8.8.2 配置门户验证简单模型

- ☐ 在“**Site**”视图页面上，点击“**WLAN**”选项卡以查看WLAN列表。

- ☐ 单击“**+**”按钮，打开创建WLAN页面。
- ☐ 填入“**SSID**”字段。
- ☐ 从安全级别下拉列表中选择“**Open**”。
- ☐ 将“**Mac Auth**”设置为“**ON**”状态。
- ☐ 在身份验证配置文件中选择“**Default**”。

注意：“Open”安全级别不支持修改身份验证来源，默认使用DAC的本地数据库。

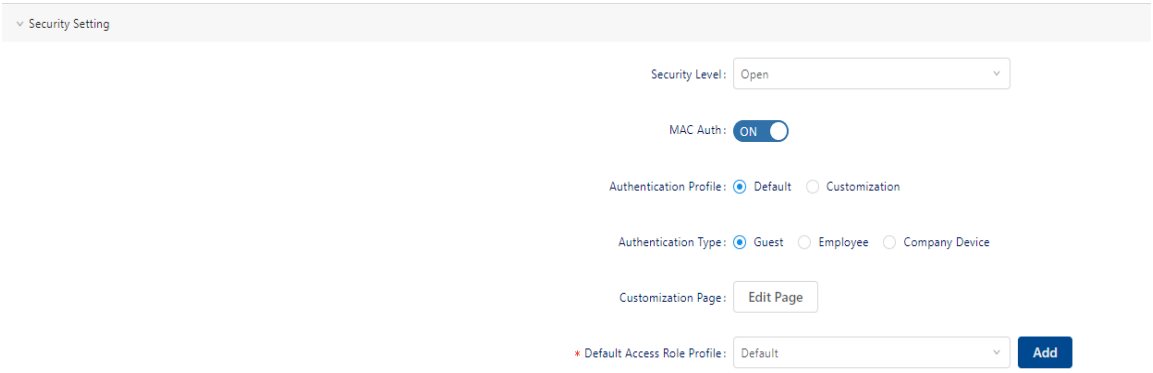


图183：配置门户验证 - WLAN 配置

- ☐ 选择“**Guest**”进行访客身份验证。
  可以在**Authentication→Guest Access→Guest Account**页面中添加访客账户。请参阅第173页的“访客账户”。
- ☐ 为员工身份验证策略选择“**Employee**”。
  可以在**Authentication→Employee Access→Employee Account**页面中添加员工账户。请参阅第179页的“员工账户”。
- ☐ **公司设备**验证类型不适用于门户身份验证。企业中有的的设备没有交互界面，因此无法进行portal认证，但需要连接到无线网络，例如打印机。这些设备可以通过在个人模式或MAC身份验证中输入密码来访问WLAN。可以在**Authentication→Setting→Company Device**页面中添加公司设备的**MAC**地址。请参阅第184页的“公司设备”。

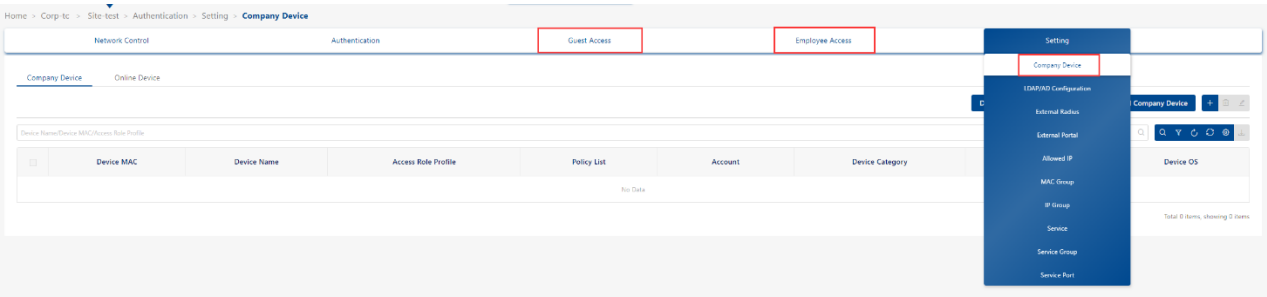


图 184：配置门户验证 - 访客接入、员工接入、公司设备

- 员工或访客账户可单击**“Edit Page”**按钮，打开**“Portal”**页面编辑视图。有关强制登录页的详细信息，请参见第242页的“强制登录页”。
- 在**默认访问角色配置文件**中，从下拉列表中选择一个配置文件或者，可以通过**单击**旁边的**“Add”**按钮来添加新的访问角色配置文件。请参阅第147页的“访问角色配置文件”。

8.8.3 自定义中配置 802.1X 身份验证

- 在**“Site”**视图页面上，点击**“WLAN”**选项卡以查看WLAN列表。
- 单击**“+”**按钮，打开创建WLAN页面。
- 填入**“SSID”**字段。
- 从**“Security Level”**下拉列表中选择**“Enterprise”**。
- 选择所需的**Encryption Mode**。请参阅第95页的“SSID设置”。
- 将身份验证配置文件为**Customization**，这意味着您需要自己创建**访问策略**、**身份验证策略**和**员工接入策略**。
- 将**Mac Auth**设置为**“OFF”**状态。
- 单击**“Effect Now”**以保存WLAN并通过编辑重新进入此页面，然后再继续。否则，无法在下一步中选择SSID。
- 单击**“Configuration Wizard”**按钮。向导将显示在右侧。
  根据第161页的“访问策略”中的信息，需要分别创建一个**访问策略**和**身份验证策略**。在这个向导中，我们将依次创建这些配置文件。由于配置文件中的引用关系，需要在保存**访问策略**之前创建**身份验证策略**。通过这种方式，可以递归地完成这些配置文件的创建。
  另一种操作方式是首先在**Authentication→Authentication→Authentication Strategy**页面创建**身份验证策略**。然后，在**Authentication→Authentication→Access Policy**策略页面中创建一个**访问策略**规则，将

SSID和**身份验证类型**绑定到先前创建的**身份验证策略**。

- ☐ 单击“**Configuration Wizard**”按钮后，首先，单击“**Create Access Policy**”选项卡，然后设置一个“**Name**”。对于当前的802.1X身份验证，建议设置**SSID**和**身份验证类型**的映射条件。在映射条件的**属性**下拉列表中选择**SSID**，并在值的下拉列表中选择刚刚创建的**SSID**。然后，单击**Add**按钮以添加条件。然后在映射条件的属性下拉列表中选择身份验证类型，并选择**802.1X**。然后应该选择一个**身份验证策略**或单击**Add**按钮添加新策略。请参阅第161页的“访问策略”。
- ☐ 其次，如果单击**Add**按钮以添加新的**身份验证策略**，将看到**Create Authentication Strategy**选项卡。应为它设置一个Name。
  - 如果选择**None**作为身份验证源，则表示此**身份验证策略**用于MAC身份验证，应为其选择**访客**或**员工接入策略**。这种配置不适合当前情况。
  - 如果选择**本地数据库**作为身份验证源，则可以在**Authentication→Employee Access→Employee Account**页面添加员工账户。可以看到**Web身份验证**只能设置为**None**，这意味着此**身份验证策略**将用于802.1x身份验证。
  - 如果选择**外部LDAP/AD**作为身份验证源，会发现**Web身份验证**只能设置为**None**，这意味着此身份验证策略将用于802.1x身份验证。应该在**Authentication→Setting→LDAP/AD Configuration**页面上配置**LDAP/AD**。
  - 如果选择**外部RADIUS**作为身份验证源，则应选择一个外部RADIUS或点击**Add**按钮以添加新的外部RADIUS。Web身份验证选择为**None**，这意味着可以将此**身份验证策略**用于802.1X身份验证。请参阅第163页的“身份验证策略”。
- ☐ 第三，可以设置与**网络执行策略**相关的参数。如果设置了**默认访问角色配置文件**，则表示通过**身份验证策略进行身份验证**的终端设备将使用此**访问角色**来授权终端，而不是在WLAN上使用**默认访问角色配置文件**。**默认策略列表**也是一样的。

  如果打开**会话超时状态**，则通过**身份验证策略**的终端将在**会话超时间隔**后自动离线。

  如果打开账户**外部RADIUS**开关，则在使用外部RADIUS时，将在记账间间隔的时间间隔内发送**RADIUS记账中间数据包**。

8.8.4 配置 Web 门户身份验证

- ☐ 在“**Site**”视图页面上，点击“**WLAN**”选项卡以查看WLAN列表。
- ☐ 单击“**+**”按钮，打开“**Create WLAN**”页面。
- ☐ 填入“**SSID**”字段。
- ☐ 从下拉列表中选择“**Open**”作为安全级别。
- ☐ 将“**Mac Auth**”设置为“**ON**”状态。
- ☐ 在身份验证配置文件中选择“**自定义**”，这意味着您需要创建**访问策略**、**身份验证策略和员工接入策略**。
- ☐ 单击“**Effect Now**”以保存WLAN并通过编辑此WLAN重新进入此页面，然后再继续。否则，无法在下一步中选择SSID。
- ☐ 点击“**Configuration Wizard**”按钮，向导将显示在右侧。根据第197页上的图 182中的信息，需要分别创建**访问策略**、**身份验证策略**和**员工接入策略**。在这个向导中，将依次创建这些配置文件。由于配置文件中的引用关系，需要在保存**访问策略**之前创建**身份验证策略**。在保存**身份验证策略**之前，需要创建一个“**员工接入策略**”。通过这种方式，我们递归地完成了这些配置文件的创建。

  另一种操作方式是先在**Authentication→Employee Access→Employee Access Strategy**中创建一个**员工接入策略**，然后在**Authentication→Authentication→Authentication Strategy**页面创建**身份验证策略**，并绑定之前创建的员工接入策略。最后，在**Authentication→Authentication→Access Policy**策略页面中创建一个访问策略规则，将**SSID**和身份**验证类型**绑定到先前创建的身份**验证策略**。
- ☐ 首先，将看到“**Create Access Policy**”选项卡，然后设置一个“**Name**”。对于当前的Web门户身份验证，应该更好地设置**SSID**和**身份验证类型**的映射条件。在映射条件的属性下拉列表中选择“**SSID**”，并在“**Value**”的下拉列表中选择刚刚创建的SSID。然后，单击“**Add**”按钮以添加条件。然后在映射条件的属性下拉列表中选择身份验证类型，并选择“**MAC**”。接下来应该选择一个**身份验证策略**或单击**Add**按钮添加新策略。请参阅第161页的“访问策略”。
- ☐ 其次，如果单击“**Add**”按钮以添加新的身份验证策略，将看到“**Create Authentication Strategy**”选项卡。你应该为它设置一个Name。选择“**None**”作为身份验证源，表示此**身份验证策略**用于MAC身份验证，应该选择“**访客接入策略**”或“**员工接入策略**”或为其添加新策略。在选择访问策略之前，需要先确认选择“Employee”还是“Guest”。请参阅第163页的

“身份验证策略”。

- 第三，如果选择创建**“访客接入策略”**，则可以看到只能使用**本地数据库**作为身份验证源。请参阅第170页的“访客接入策略”。然后，可以设置**固定访问角色配置文件**，该配置文件将在Web门户身份验证后分配给终端。固定**访问角色配置文件**选项不是必须的。如果不设置此选项，终端将使用**身份验证策略中的“默认访问角色配置文件”**。如果在**身份验证策略**中未设置**“默认访问角色配置文件”**，则终端将使用WLAN中设置的**“默认访问角色配置文件”**。如果选择创建**“员工接入策略”**，可以选择**“本地数据库”**，**“外部LDAP/AD”**或**“外部RADIUS”**。
- 第四，可以设置与**网络执行策略**相关的参数。如果设置了**“默认访问角色配置文件”**，则表示通过身份验证**策略进行身份验证**的终端设备将使用此**访问角色**来授权终端，而不使用WLAN的**默认访问角色配置文件**。默认策略列表也是一样的。如果打开**会话超时状态**，则通过**身份验证策略**的终端将在**会话超时间隔**后自动离线。如果打开账户**外部RADIUS**按钮，则在使用外部RADIUS时，将在记账间间隔的时间间隔内发送RADIUS记账中间数据包。

9 RF

RF管理系统确保发射功率和操作频率符合全球监管机构和各个国家的要求。配置文件允许用户根据实际网络环境调整无线参数和功能，以改善无线网络的用户体验。您可以管理特定站点或DAP的RF配置。

本章包含下列主题：

9.1 RF 概述

RF配置选项可以配置为自动模式。DAP将根据周围的信号条件自动设置其相关参数。

图 185里有两个图表显示设备信道的分布。将鼠标放在相应的图表上，即可获取每个信道和带宽的AP编号。

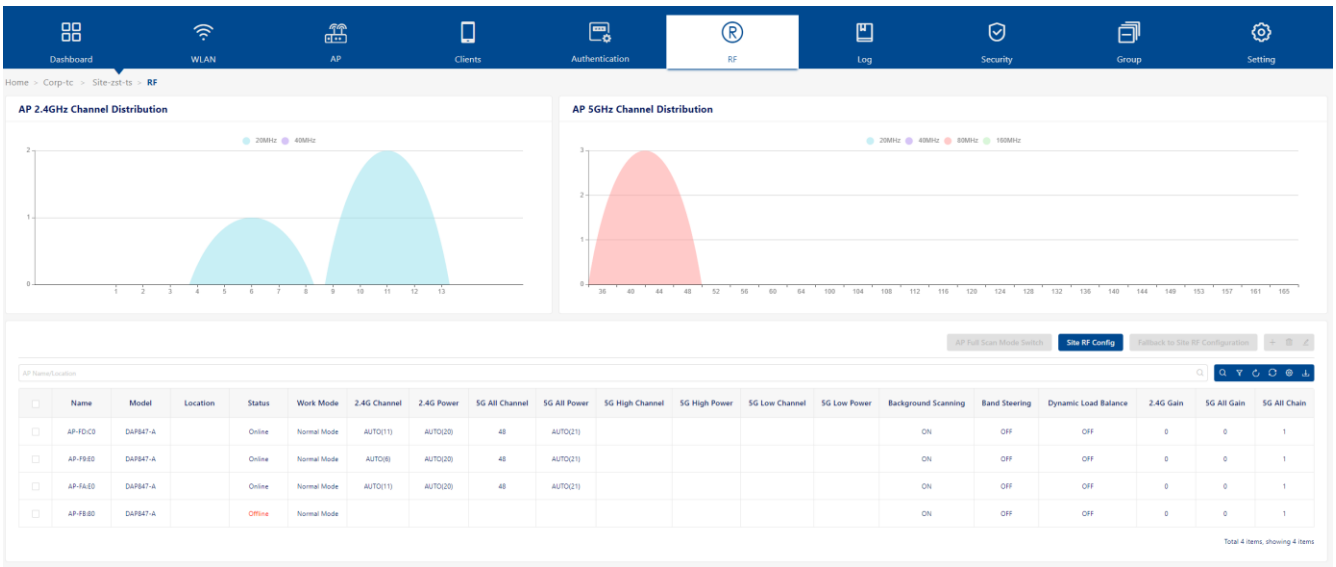


图 185：RF

图表下方是每个AP的详细RF信息列表。可以直接搜索AP名称或使用下拉列表按AP状态或AP模式过滤显示。

- **Name**：AP名称。
- **Model**：AP的型号。
- **Location**：AP的位置。
- **Status**：AP状态，在线或离线。
- **Work Mode**：
  - **Normal Mode**：AP为无线客户端提供服务。
  - **Full Scan Mode**：在此模式下，AP下的所有无线电将不会广播SSID。
- **2.4G Channel**：2.4G频段的信道。
  - 如果配置为Auto模式，则显示AP的实际2.4G信道。
- **2.4G Power**：2.4G频段信道的功率。

- 如果配置为Auto模式，则显示AP的实际2.4G信道功率。

► **5G All Channel**：5G全频段的信道。

- 如果配置为Auto模式，则显示AP的实际5G信道。
- 可选信道会根据不同国家或地区的当地法律而有所不同。

► **5G All Power**：5G全频段信道的功率。

- 如果配置为Auto模式，则显示AP的实际5G信道功率。

► **5G High Channel**：5G高频信道。

- 如果配置为Auto模式，则显示AP的实际5G高频信道。

► **5G High Power**：5G高频信道的功率。

- 如果配置为Auto模式，则显示AP的实际5G高频信道功率。

► **5G Low Channel**：5G低频信道。

- 如果配置为Auto模式，则显示AP的实际5G低频信道。

► **5G Low Power**：5G低频信道的功率。

- 如果配置为Auto模式，则显示AP的实际5G低频信道功率。

► **Background Scanning**：

- 启用或禁用后台扫描。
- 后台扫描用于检查无线网络所处的射频环境，发现邻近的AP，并识别干扰和攻击。
- 后台扫描是一些高级功能的基础，例如WIDS和WIPS。

  如果想使用这些高级功能，请验证**“Background Scanning”**已启用。默认情况下，它处于启用状态。

► **Band Steering**：频段控制状态。默认打开。

- 频段控制根据无线信道的利用率和连接到AP的用户数量来控制双频客户端的行为。
- 它指导客户端访问网络到最佳的5G Hz频段或另一个AP。

► **Dynamic Load Balance**：默认关闭。

- 根据客户端密度、相邻AP上的信道利用率以及关联的客户端RSSI值启用或禁用客户端负载平衡，以在相邻AP之间提供客户端的公平分布。
- 客户端信息（如客户端数量）会在无线网络中进行同步，以便AP了解其邻近AP的负载情况，并决定是否允许客户端访问。

- **2.4G Gain**：2.4G频段AP的天线增益，只支持DAP847-A。
- **5G All Gain**：5G全频段AP的天线增益，只支持DAP847-A。
- **5G All Chain**：5G全频段AP的天线设置，只支持DAP847-A。

9.2 配置 Site RF

点击“**Site RF Config**”按钮，进入RF编辑视图。

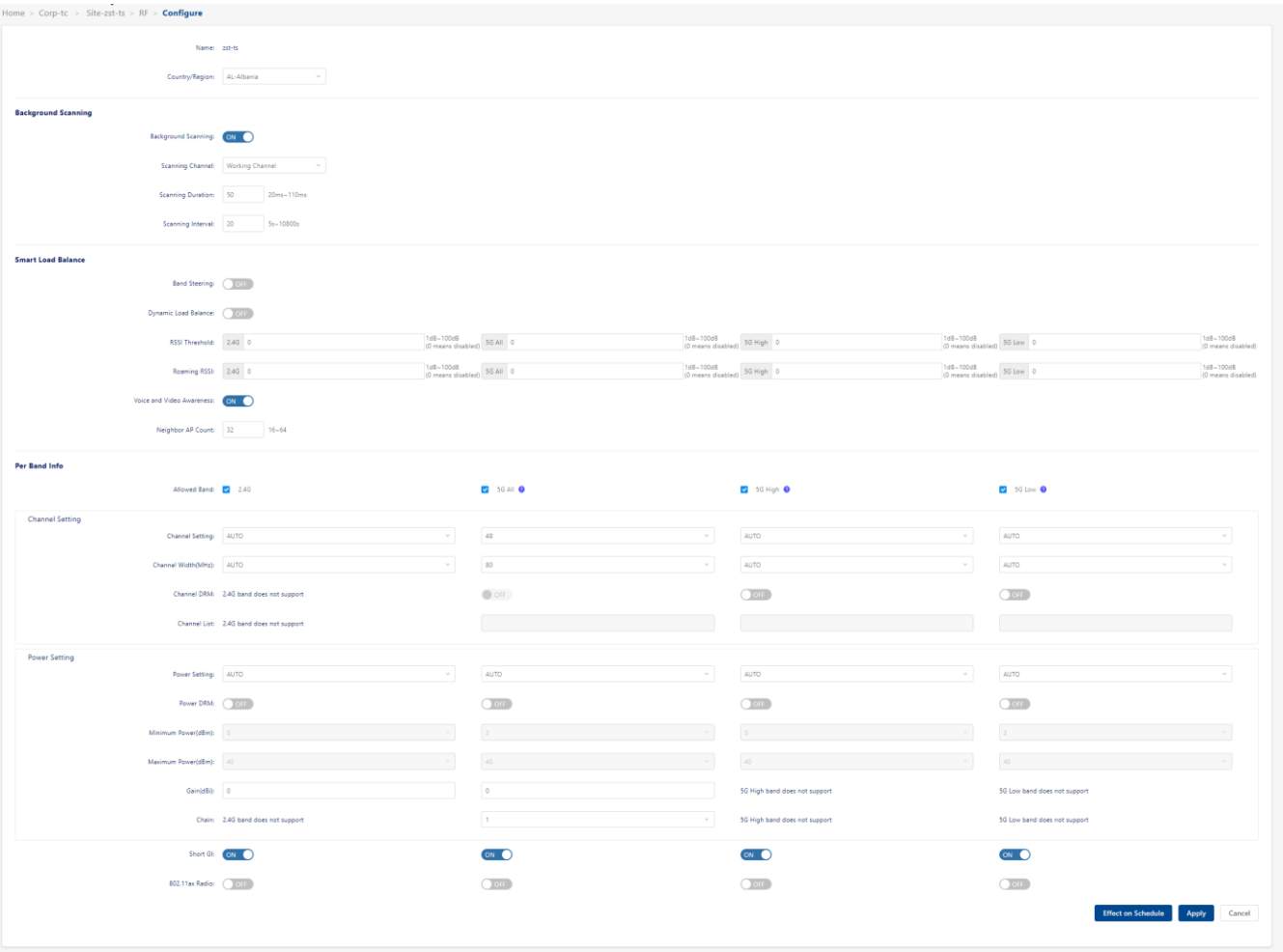


图 186：RF 配置

9.2.1 基本信息

- **Name**：继承自站点名称
- **Country/Region**：
  - 国家或地区是代表国家或附属区域的简短字母地理代码，用于数据处理和通信。
  - 无线发射功率和工作频率（信道）因国家或地区而异。
  - 选择AP所在的国家或地区。

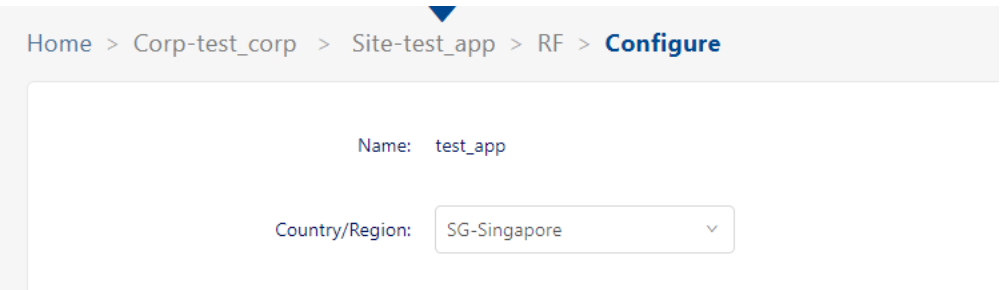


图 187：配置 Site RF - 基本信息

9.2.2 后台扫描

后台扫描用于检查无线网络运行的射频环境，发现邻近的AP，并识别干扰和攻击。后台扫描是一些高级功能的基础，例如MIPS和RDA（ACS/APC）。如果想使用这些高级功能，请确保**“Background Scanning”**已启用。默认情况下，它处于启用状态。

- **Background Scanning：**启用或禁用后台扫描。
- **Scanning Channel：**
  - **工作信道：**AP扫描工作信道。
  - **所有信道：**AP扫描所有信道。
- **Scanning Duration：**后台扫描持续时间，以毫秒为单位给出。（默认值：50）
- **Scanning Interval：**后台扫描间隔，以秒为单位。（默认值：20）

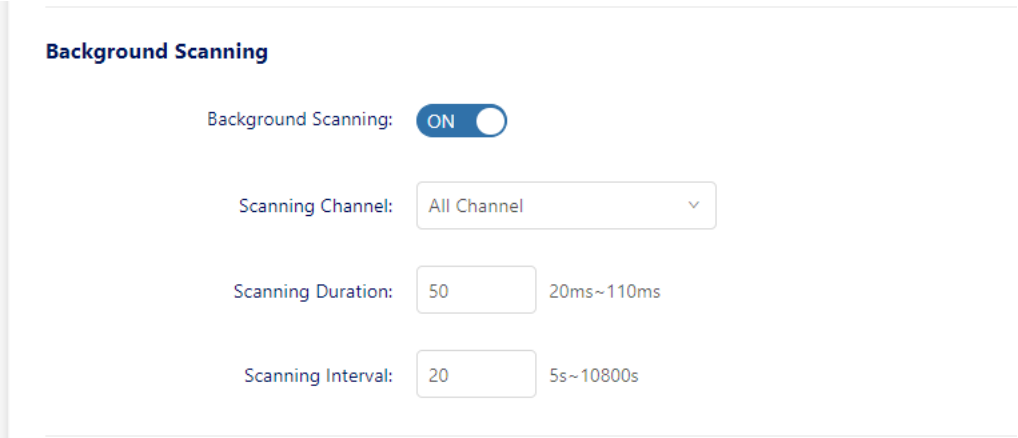


图 188：配置 Site RF - 后台扫描

9.2.3 智能负载均衡

智能负载均衡（SLB）功能改善了访问无线连接时的用户体验。它引导用户的客户端设备连接到空闲无线信道或AP，并拒绝访问信号较弱的AP。

智能负载均衡包括：

- **Band Steering**：启用或禁用频段控制。

  频段控制功能会根据无线信道的利用率和连接到AP的用户数量来控制双频客户端的行为。它将访问网络的客户端引导至最佳AP。

- **Dynamic Load Balance**：在组内的AP之间，或同一无线网络中几个组的AP之间，启用或禁用客户端负载均衡。

  客户端信息（如客户端数量）会在无线网络中进行同步，以便AP确定其邻近AP的负载情况，并决定是否允许客户端访问。

- **RSSI Threshold**：关联RSSI阈值。用于设置阈值，通过禁止具有较弱无线信号的客户端访问网络，以来优化与AP关联时的连接性。如果客户端的RSSI值低于关联的RSSI阈值，则不允许其连接到AP。

  默认情况下，**“RSSI threshold”**处于禁用状态（0）。RSSI阈值可以分别应用于2.4G频段或5G频段。推荐的值是2.4G（5），5G（10）。在高密度场景中建议设置RSSI阈值。

- **Roaming RSSI**：漫游RSSI阈值。

  用于设置阈值，通过禁止具有较弱无线信号（RSSI）的客户端访问网络以优化漫游时的连接性。RSSI值低于漫游RSSI阈值的客户端将被引导漫游到另一个传输信号更好的AP。

  默认情况下，**“Roaming RSSI”**处于禁用状态（0）。漫游RSSI可以分别应用于2.4G频段或5G频段。漫游RSSI与802.11k和802.11v结合使用。当超出阈值时，将通知支持这些协议的客户端漫游到哪个AP。启用802.11k和802.11v时，推荐值为2.4G（10），5G（15）。

- **Voice and Video Awareness**：启用或禁用语音和视频感知。默认为启用。后台扫描必须知道AP上的现有流量。

  如果有正在进行的语音或视频服务，则不应进行扫描以确保流量不中断。如果没有进行的语音或视频会话，则应恢复扫描。

- **Neighbor AP Count**：用于限制一个AP可以连接的相邻AP的数量。（默认值：32）

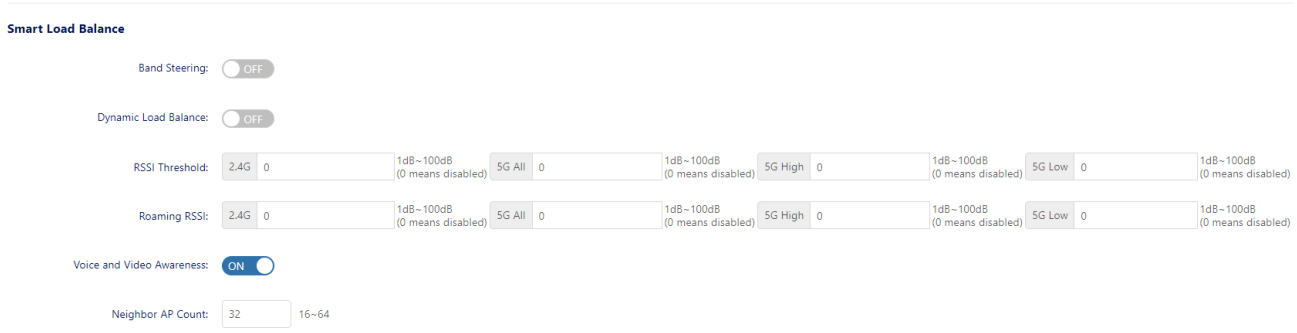


图 189：配置 Site RF - 智能负载均衡

9.2.4 Per band info

配置AP上各个无线电频段，例如无线电的工作信道、发射功率和短保护间隔。

- ► **Allowed Band：**配置AP的工作无线电波段。
  - **2.4G：**激活2.4G频段无线电。
  - **5G All：**激活5G频段无线电。仅适用于双射频AP。
  - **5G High：**激活5.2G频段无线电。仅适用于三射频AP。
  - **5G Low：**激活5.8G频段无线电。仅适用于三射频AP。
- ► **Channel Setting：**配置无线电的工作信道。
  - **Auto：**通过ACS（自动信道选择）动态分配工作信道。
  - **Number：**手动指定信道（允许的频段因国家或地区而异）。
- ► **Channel Width(MHz)：**配置2.4G和5G无线电的信道宽度。
  信道宽度用于控制数据传输的信号宽度。通过增加信道宽度，可以提高无线广播的速度和吞吐量。然而，在频率噪声和干扰较多的拥挤区域，更大的信道宽度会带来更不稳定的传输。2.4G信道宽度支持与5G不同。
  - **2.4G：**20MHz或40MHz
  - **5G All/5G High/5G Low：**20MHz，40MHz，80MHz或160MHz。显示Channel Setting中设置的值。某些高频信道不支持160MHz的信道宽度。例如，只有在36到128之间的信道设置上支持160MHz。
- ► **Channel DRM：**指定DRM的信道范围。在某些地区，可以将特定不需要的频道范围排除在自动频道选择之外，以避免冲突或违法行为。只在2.4G频段上不支持此配置。
- ► **Channel List：**指定DRM可选择的可用信道。只在2.4G频段上不支持此配置。

► **Power Setting**：配置无线电的发射功率。
不同的无线电具有不同的功率范围。

- **Auto**：通过APC动态分配发射功率。
- **Number**：手动指定功率设置（3dBm-40dBm）。

► **Power DRM**：指定DRM的功率范围。默认关闭，如果启用，则可以选择Minimum Power和Maximum Power。

► **Minimum Power(dBm)**：指定DRM功率设置的最小发射功率。这可以防止AP选择低传输功率，从而导致传输质量差。

► **Maximum Power(dBm)**：指定DRM功率设置的最大发射功率。

► **Gain**：可分别为2.4G和5G All设置天线增益，范围：0-16 dBi

► **Chain**：天线配置，只适用于5G，指与MIMO对应的天线界面，可设为如下值：

带宽	MIMO	Chain
20/40/80	1x1	0
		1
		2
		3
	2x2	0+1
		0+3
	3x3	0+1+2
	4x4	0+1+2+3

表 7：DAP847-A 的天线 Chain 和 MIMO

► **Short GI**：启用或禁用短保护间隔。

在基于IEEE 802.11 OFDM的通信中，保护间隔用于验证设备传输的连续数据符号之间是否发生了不同的传输。802.11 OFDM中的标准保护间隔的为800纳秒。为了提高数据速率，802.11n标准增加了400纳秒保护间隔（短保护间隔）的选项。这将提高大约11%的数据速率。但当RF信道延迟超过短保护间隔或收发器时间不同步时，使用段保护间隔会导致更高的数据包检测错误率。默认情况下，无线电上的**“Short GI”**处于禁用状态。

► **802.11ax Radio**：启用或禁用802.11ax（Wi-Fi6）功能。默认启用，如果禁用，则AP可以在802.11ac或更早的协议上工作。

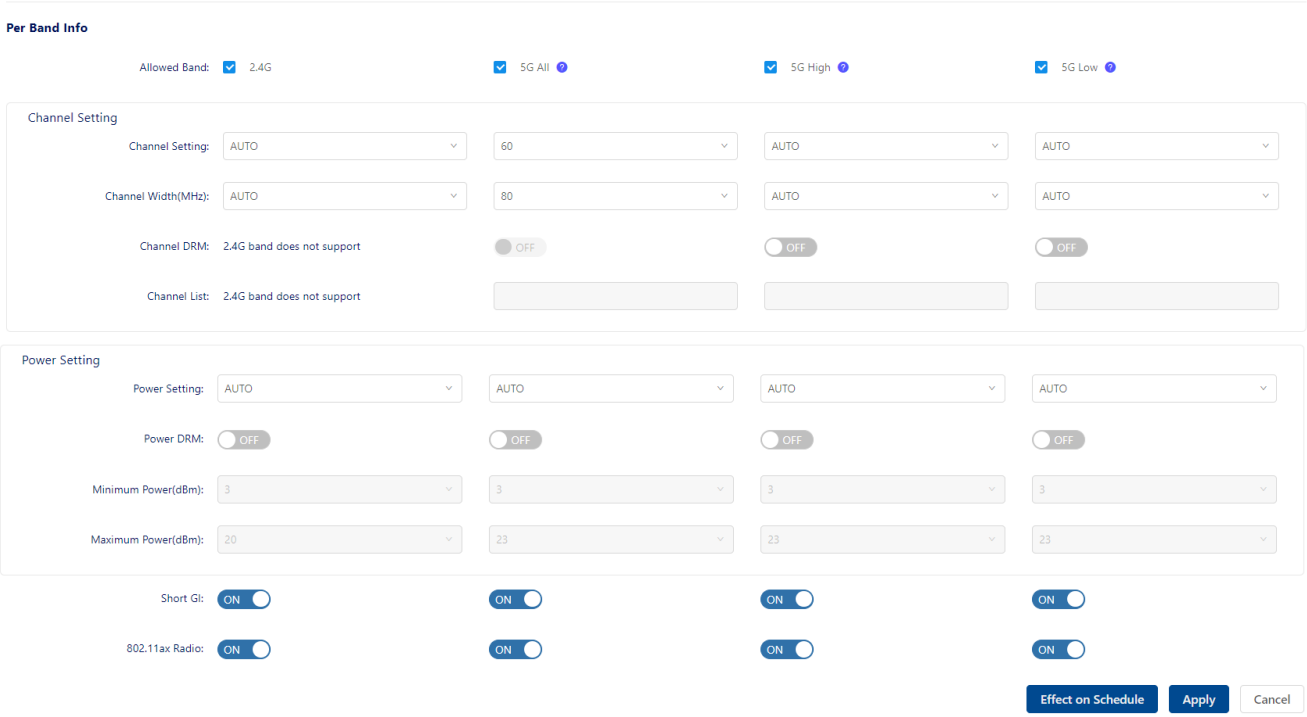


图 190：Per band info

9.3 配置选定 DAP 的 RF

为了给用户提供更好的体验，有时需要调整所选AP的RF配置。在为某个AP配置RF之前，必须先配置相应站点的RF。AP的RF配置优先级高于站点的RF配置。

9.3.1 单个 AP 的 RF 配置

- ☐ 选择单个AP。
- ☐ 单击“ ”图标，进入AP详细信息页面。

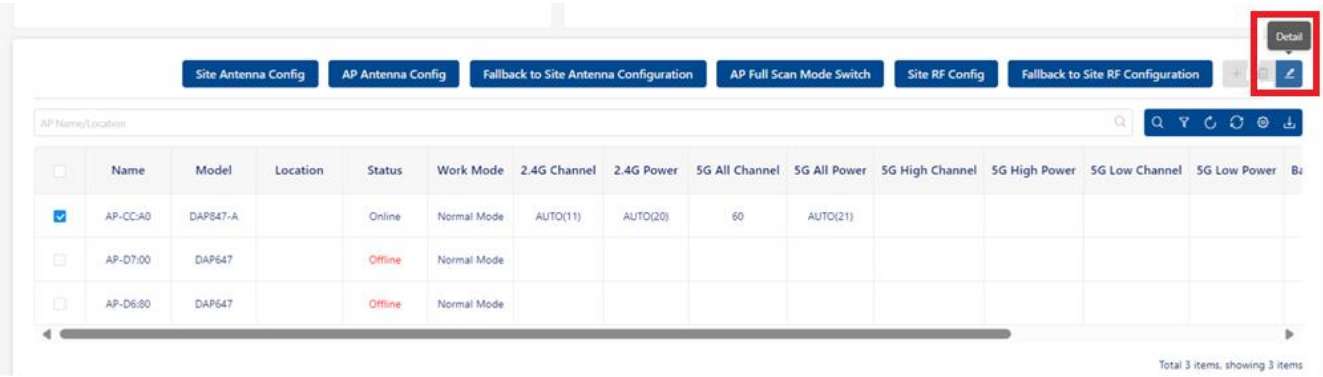


图 191：Detail 图标

- ☐ 点击“**Config**”按钮以配置所选AP的RF。

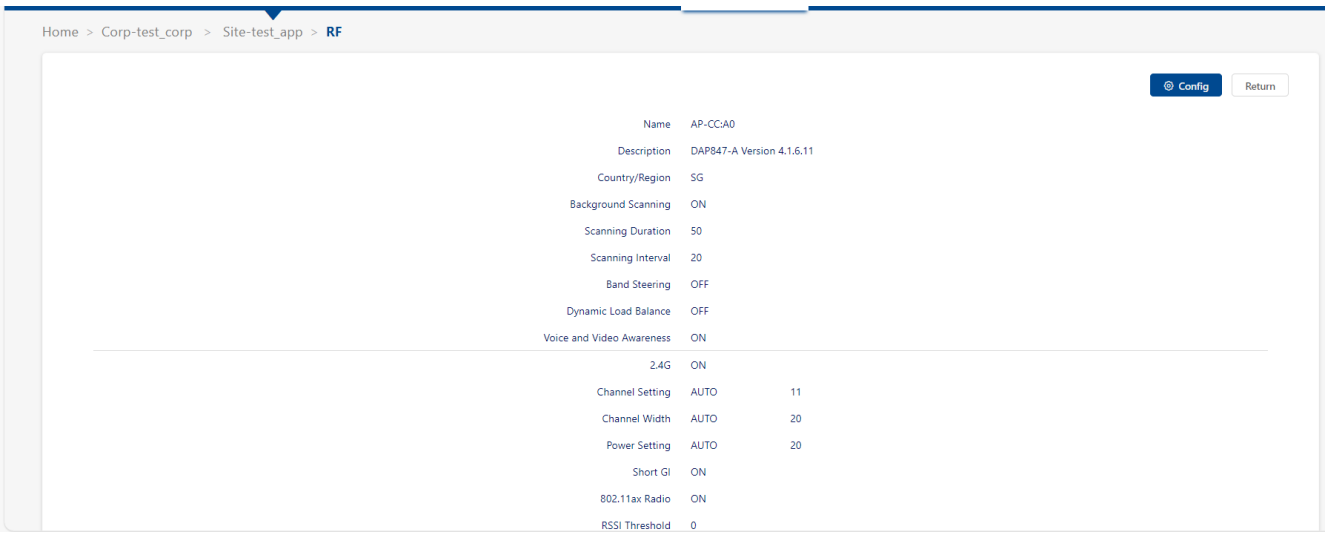


图 192：RF 配置

9.3.2 回退到 Site 的 RF 配置

- ☐ 选择单个或多个AP。
- ☐ 点击“**Fallback to Site RF Configuration**”按钮。
  所选AP的RF配置将被清除并与Site保持一致。

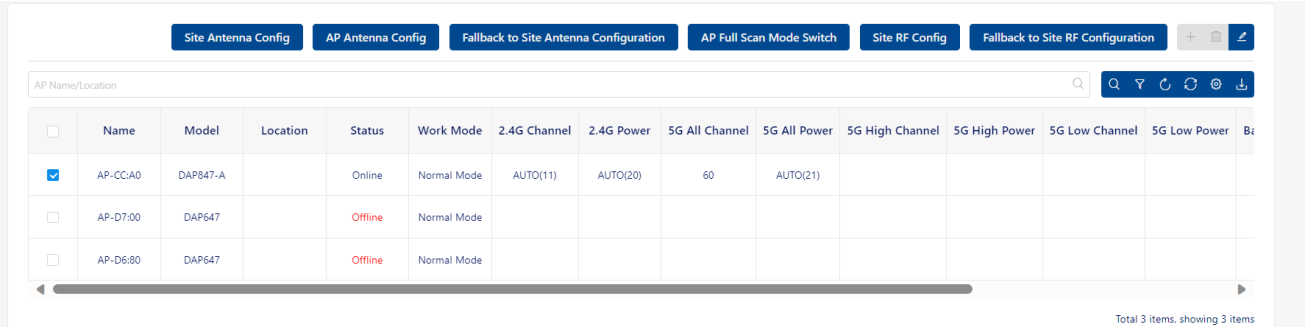


图 193：回退到 Site RF 配置

9.3.3 AP 全扫描模式

- ☐ 选择单个或多个AP。
- ☐ 点击“**AP Full Scan Mode Switch**”按钮，所选的AP将进入全扫描模式。
  全扫描模式下，AP下的所有无线电将不会广播SSID。

注意：启用“**AP Full Scan Mode Switch**”将导致AP关闭当前正在工作的WLAN。与该AP连接的所有终端将离线。

10 日志

日志包含2个主要部分：

- 系统日志
- 设备日志

系统日志包含设备的关键事件和DAC的操作日志。平台从DAP收集日志文件。

DAC提供了良好的运维管理功能，但在某些极端情况下，我们需要获取设备上的详细日志，以便及时进行研发工作和问题定位。

本章包含下列主题：

- 系统日志
- 设备日志

10.1 系统日志

系统日志显示当前日志列表。可以从此列表中搜索特定消息。

10.1.1 日志列表

该列表显示最近的日志。可以按日志类型、日志级别或AP Group筛选日志。

- **Severity：**日志的严重程度。它可以是Emergency、Alert、Critical、Error、Warning、Notice、Informational或Debug。
  - **Emergency：**系统无法使用。
  - **Alert：**必须立即采取行动。
  - **Critical：**严重的情况。
  - **Error：**错误的情况。
  - **Warning：**如果不采取措施，将发生错误。
  - **Notice：**事件不正常但不会导致错误或者故障。
  - **Informational：**正常操作消息，不需要采取任何措施。
  - **Debug：**帮助开发者识别问题的消息。

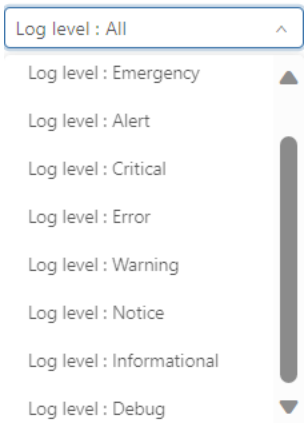


图194：Severity

- **Type：**日志类型。可以是Trap-Hardware，Trap-Upgrade，Trap-Security，Trap-Network，Trap Authentication，Switch Trap-Network或Operator。
  - **Trap-Hardware：**硬件报告信息，主要关注AP的CPU、RAM和闪

存的性能，并监控AP热启动和冷启动的行为。

- **Trap-Upgrade**：固件升级信息，主要包括AP升级的行为。
- **Trap-Security**：无线安全信息，主要包括黑名单的操作信息。
- **Trap-Network**：与网络相关的报告信息，主要包括创建和删除第二层VLAN。
- **Trap-Authentication**：验证信息，包括客户端的验证行为和AP到RADIUS服务器的链路状态。
- **Switch Trap-Network**：网络切换报告。
- **Operator**：DAC的用户操作记录，包括操作者和所执行的操作。

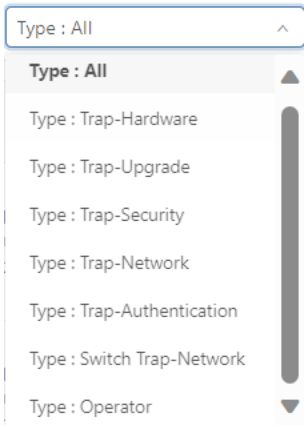


图 195：Type

- **Scene**：日志发生在哪个Corporate、Site或Group。
- **Date & Time**：日志发生的时间和日期。
- **Detail**：日志的详细信息。
- **AP Name**：如果日志是由AP生成的，则此字段显示AP的名称。
- **AP Location**：如果日志由AP生成的，则此字段显示AP的位置。

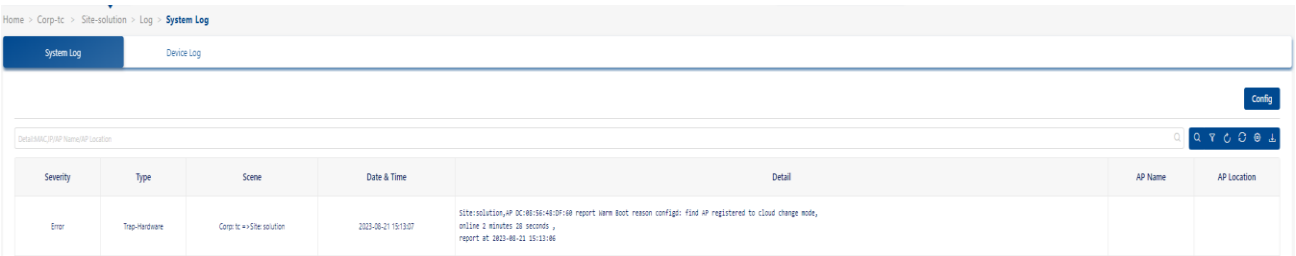


图 196：日志列表

10.1.2 AP 事件日志配置

点击“**Config**”按钮，打开配置页面。当前页面包含设备事件的日志开关或相关参数。可以在此页面上打开关注的设备事件日志。

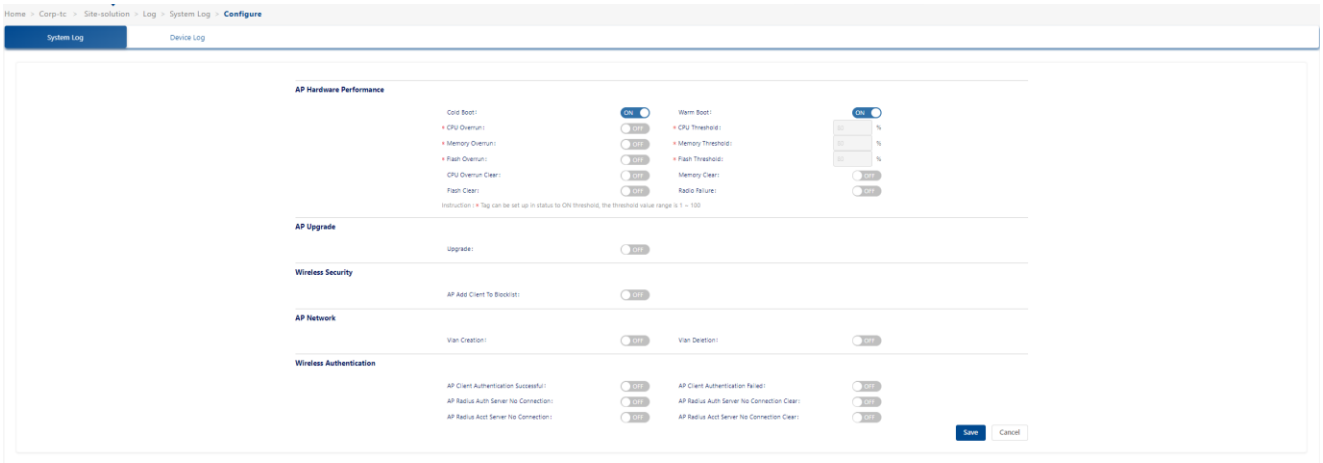


图 197：日志配置

- **AP硬件性能**
  - **Cold Boot：**冷启动是指将AP从关机或无电状态启动，并将其设置为正常工作状态的过程。它也被称为硬启动、冷启动或死启动。
  - **Warm Boot：**热启动（也称为“**软启动**”）是重新启动AP的过程。可与冷启动相对应使用。
  - **CPU Overrun：**当AP CPU负载超过CPU阈值时，会生成此日志。
  - **CPU Threshold：**当AP CPU使用率超过此百分比时，会生成APCPU超载日志。
  - **Memory Overrun：**当AP RAM内存使用超过MEM阈值时，会生成此日志。
  - **Memory Threshold：**当AP内存使用超过此百分比时，会生成AP MEM超载日志。
  - **Flash Overrun：**当AP闪存使用量超过闪存阈值时，会生成此日志。
  - **Flash Threshold：**当AP闪存使用超过此百分比时，会生成AP闪存超载日志。
  - **CPU Overrun Clear：**当AP的CPU使用率从阈值以上水平降低到正常状态时，会生成此日志。

- **Memory Clear**：当AP的RAM内存利用率从阈值以上水平降低到正常状态时，会生成此日志。
- **Flash Clear**：当AP的闪存利用率从阈值以上水平降低到正常状态时，会生成此日志。
- **Radio Failure**：Wi-Fi无法加载。例如，AP的2G芯片损坏导致Wi-Fi释放失败。

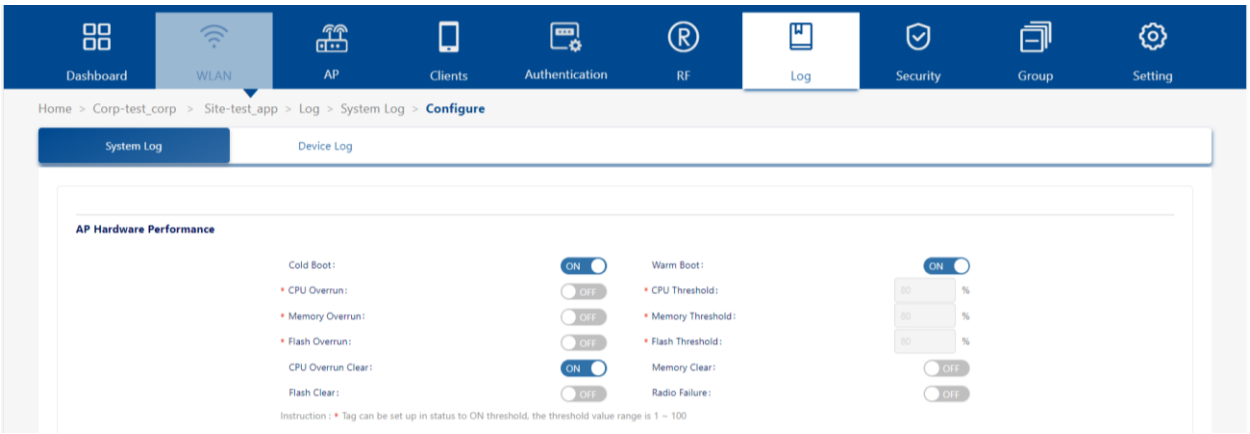


图 198：AP 硬件性能

■ AP升级

- **Upgrade**：AP升级日志。

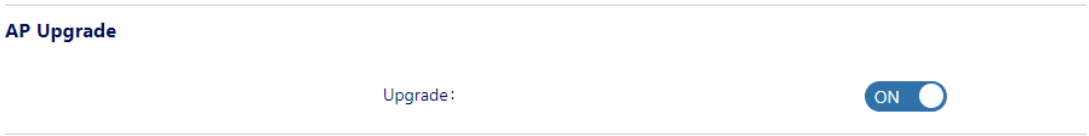


图 199：AP 升级

■ 无线安全

- **AP Add Client to Blocklist**：由WIPS策略动态地或手动将客户端添加到黑名单的日志。

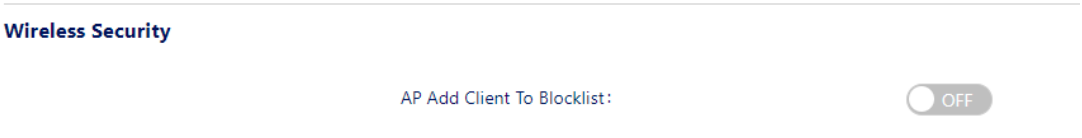


图 200：无线安全

■ **AP网络**

- ► **Vlan Creation**：VLAN创建的日志。
- ► **Vlan Deletion**：VLAN删除的日志。

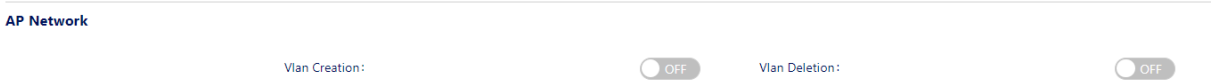


图 201：AP 网络

■ **无线身份验证**

- ► **AP Client Authentication Successful**：客户端认证成功的日志。
- ► **AP Client Authentication Failed**：客户端认证失败的日志。
- ► **AP Radius Auth Server No Connection**：无法连接到认证服务器的日志。
- ► **AP Radius Auth Server No Connection Clear**：认证服务器恢复到可访问状态的日志。
- ► **AP Radius Acct Server No Connection**：无法连接到记账服务器的日志。
- ► **AP Radius Acct Server No Connection Clear**：记账服务器恢复到可访问状态的日志。

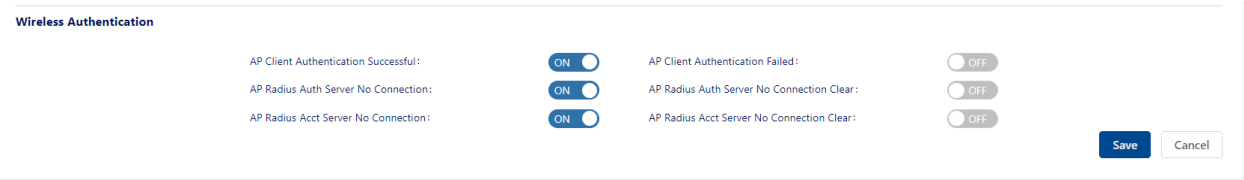


图 202：无线身份验证

10.2 设备日志

AP异常重启后，重新连接到DAC平台，平台将收集AP的日志文件。在设备日志视图中，可以查看收集到的日志列表。

- **File Name：**文件名。
- **AP MAC：**此日志文件的AP MAC地址。
- **AP Name：**此日志文件的AP名称。
- **AP IP：**AP的IP地址。
- **Status：**文件上传状态，成功或失败。
- **Log Generation Time：**此日志文件生成的时间。
- **File Size：**此日志文件的文件大小。

选择一个日志文件，点击**“File Download”**按钮可以下载该文件。

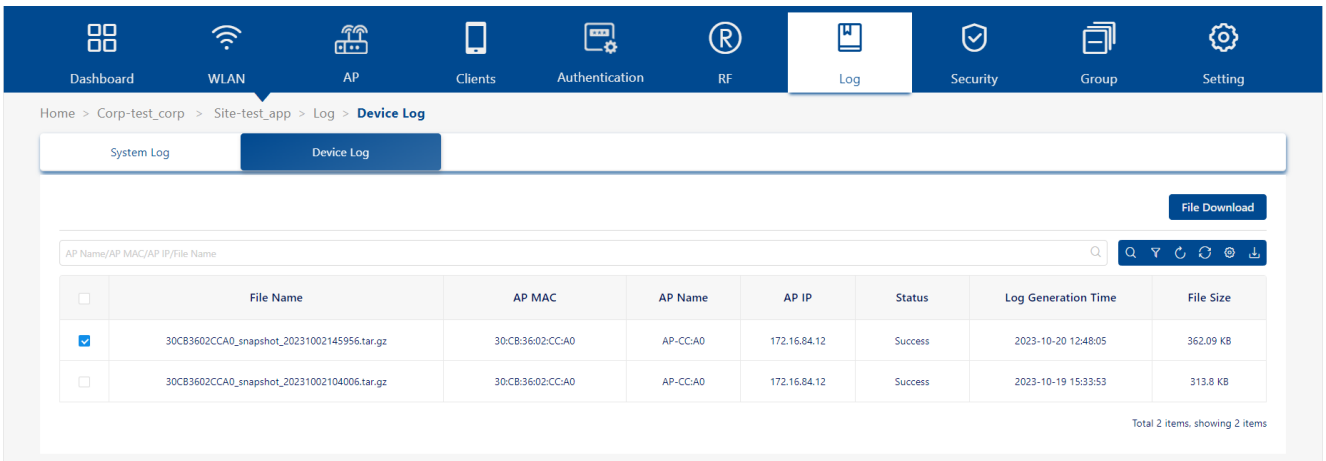


图203：设备日志

11 安全

802.11网络是开放且无边界的，因此容易受到攻击（例如，Rogue AP、未经授权的客户端和DoS攻击）。无线入侵保护系统（WIPS）监控无线电频谱，可检测不安全的接入点和客户端，并采取相应对策减轻外部入侵的影响。WIPS为DAP提供了一个无线网络威胁或入侵的概览，帮助用户建立策略来检测威胁并采取对策。

■ WIDS

DAC提供了全面的安全功能，确保客户的无线网络安全性。该系统根据下列策略和标准识别和检测Rogue AP。

► 检测AP的信号强度阈值何时超过管理员定义的值。

► 检测AP的SSID名称根据系统定义是否有效。

► 通过AP的SSID名称中定义的关键词来检测（关键词由管理员定义）。

► 通过其定义的OUI（MAC地址前六位的组织唯一标识符）来检测AP，请参考黑名单机制。

► 检测已定义的合法OUI，请参考白名单机制。DAC还可以检测一下来自潜在Rogue AP或Rogue客户端的网络攻击行为：

- **AP：**仿冒AP、广播解除认证、广播解除关联、当前基础设施中使用的具有SSID的Ad-hoc网络、无效的长SSID、AP扮演者、Omerta攻击、空探测响应、无效的地址组合、解除认证的无效原因代码、解除关联的无效原因代码。
- **客户端：**有效客户端错误关联、Omerta攻击、未加密的有效客户端、802.11 40MHz带宽不兼容设置、活跃的802.11n Greenfield模式、DHCP客户端ID、DHCP冲突、DHCP名称更改、频繁认证、长SSID（客户端）格式错误。

► **帧：**关联请求、无效的解除认证原因代码、无效的解除关联原因代码。

■ WIPS

DAC与WIDS协同，借助WIPS可实行以下相关的安全策略：

► 安全策略抑制Rogue AP，以减轻破坏性影响，阻止客户端连接到Rogue AP。

- 安全策略抑制Rogue客户端（主动或被动），通过黑名单机制（静态或动态）减轻负面影响。
- 安全策略，通过提供白名单机制来保护合法设备。

主页通过展示2个图表帮助了解当前的整体情况，如图 204。

- **Rogue Client/AP**：Rogue客户端或Rogue AP数量的折线图。
- **Blocklist**：黑名单数量的折线图。

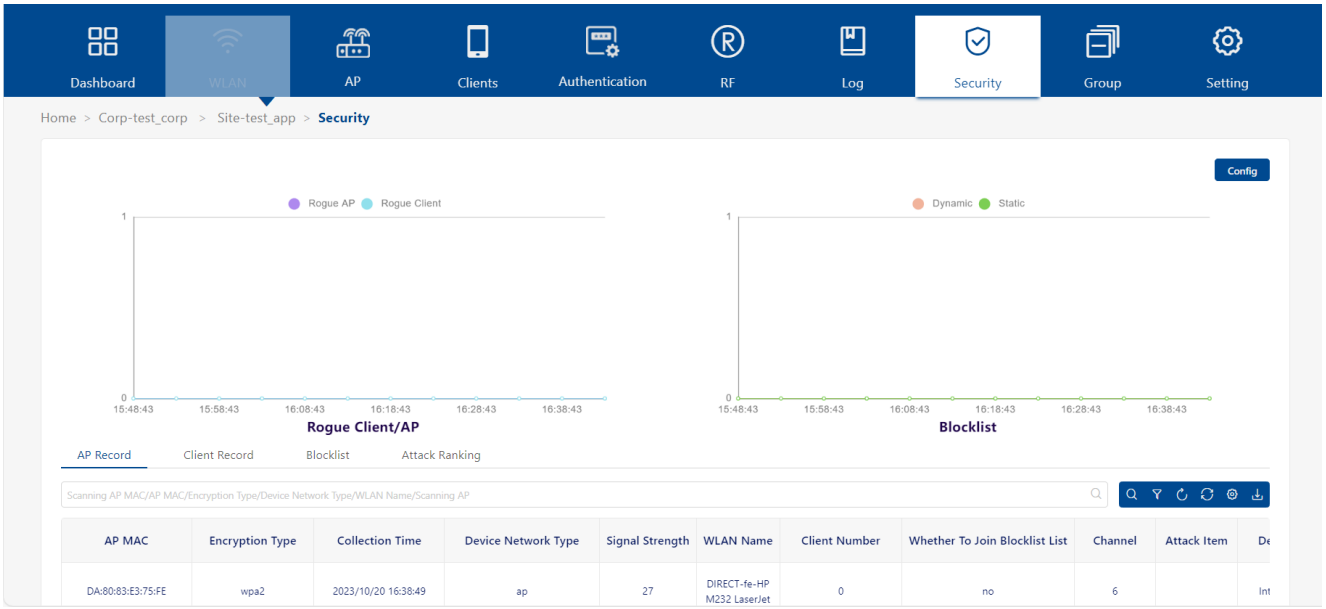


图 204：Security 仪表盘

本章包含下列主题：

- 安全配置
- AP记录
- 客户端记录
- 黑名单
- 攻击排名

11.1 安全配置

安全配置界面用于针对网络上的Rogue AP和无线攻击进行策略配置。当基于策略检测到攻击时，检测到的设备将被禁止接入网络，并显示在**“Rogue AP Record”**或**“Rogue Client Record”**中供审核。

- ☐ 单击**“Config”**按钮。
- ☐ 按照以下描述编辑策略。
- ☐ 点击**“Save”**激活Site无线网络的策略。

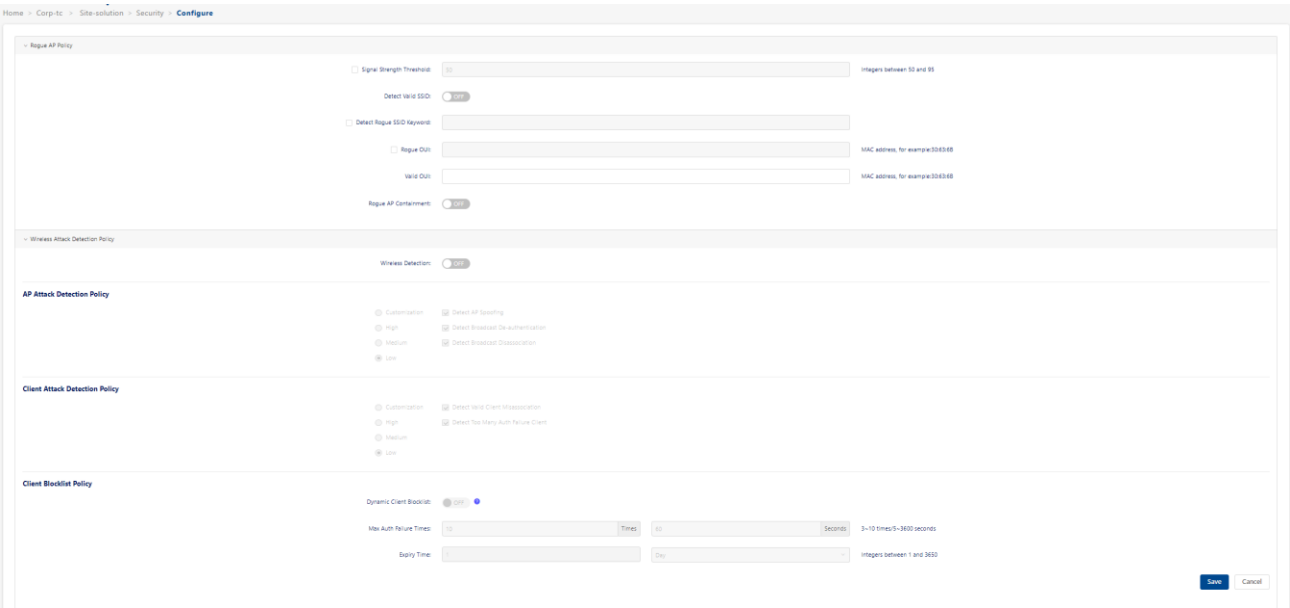


图 205：安全配置

11.1.1 Rogue AP 策略

Rogue AP是连接到网络有线侧的未经授权的AP，被视为对无线网络的安全威胁。干扰AP是指在无线环境中可见，但未连接到有线网络的AP，不被视为直接安全威胁。

然而，一些干扰AP可能会对网络质量产生影响，并干扰有效客户端对网络的访问。通过编辑以下字段配置规则，可将干扰AP划分为Rogue AP。

- ► **Signal Strength Threshold：**如果启用，RSSI大于此设置值的干扰AP将被划分为Rogue AP（可选值：50..95）。默认情况下，RSSI匹配规则为关闭状态。
- ► **Detect Valid SSID：**如果启用，则将广播与DAC网络SSID相同的其他AP

划分为Rogue AP。默认为关闭状态。

- **Detect Rogue SSID Keyword：**如果启用，则广播与用户指定的特征相匹配的SSID的干扰AP将被划分为Rogue AP。匹配条件可以等于或包含配置的关键字的SSID。
- **Rogue OUI：**如果启用，则将与此MAC OUI匹配的干扰AP划分为Rogue AP。
- **Valid OUI：**通过输入AP的MAC OUI，可将被划分的干扰AP或Rogue AP信任为“有效”AP，本质上等同于创建一个供应商“Whitelist”。这些干扰AP就不会被划分为Rogue AP。
- **Rogue AP Containment：**默认禁用，启用时可减少Rogue AP对有效客户端的影响。

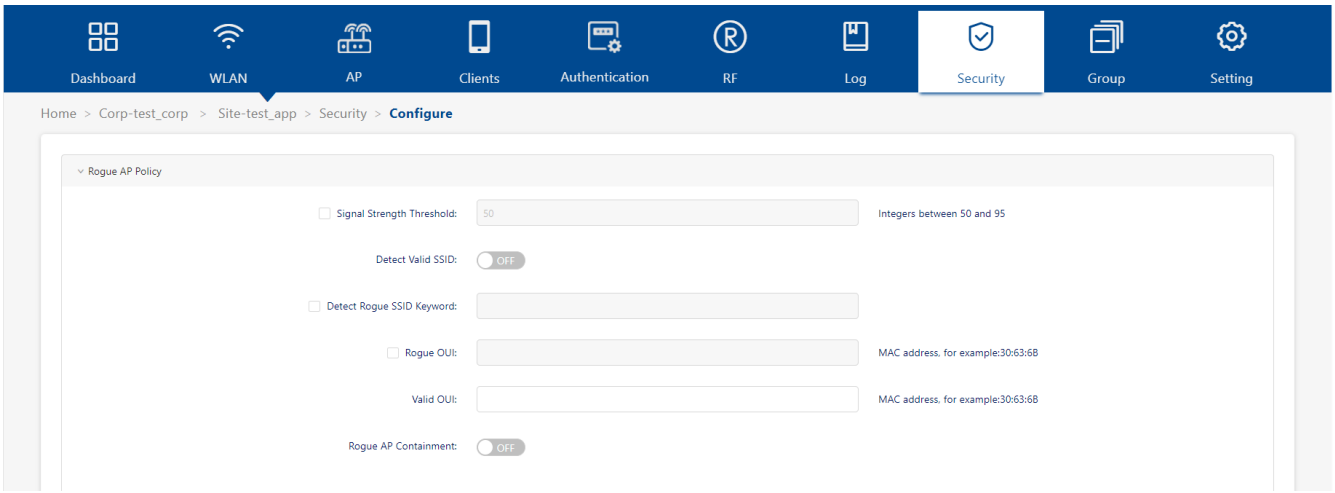


图 206：Rogue AP 策略

11.1.2 无线攻击检测策略

Rogue AP并不是无线网络的唯一威胁。无线攻击检测策略也可以检测其他无线攻击，缓解攻击对AP和客户端的影响。必须启用**无线检测**才能创建无线攻击策略。在配置策略时，每个检测策略可以设置为以下几个级别。选择一个级别时，会显示并选中该级别中包含的所有检测策略。

- **Customization：**仅启用所选择的检测机制。选择此级别时，会显示所有检测机制。可从中选择想要包含在策略中的项目。
- **High：**启用所有适用的检测机制，包括Low和Medium设置的所有选项。

- **Medium**：启用特定的检测机制。包括Low设置中的所有选项。
- **Low**：为默认值。仅启用最关键的检测机制。

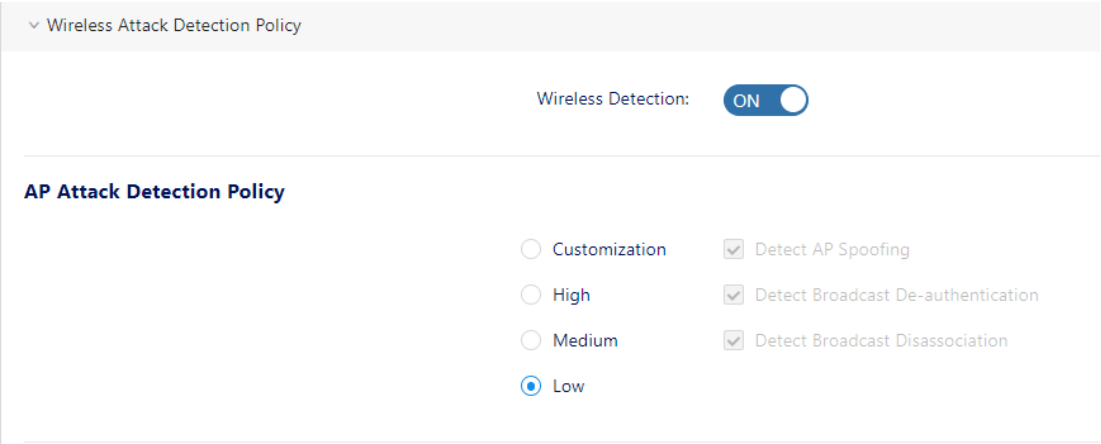


图 207：无线攻击检测策略

下面将对无线攻击策略进行逐个介绍。

■ AP攻击检测策略

AP攻击检测策略可以检测到来自外部AP的多次攻击。根据所选级别，可使用以下检测方法：

- **Detect AP Spoofing**：AP仿冒攻击指入侵者发送伪造的帧，使其看起来像是来自有效的AP的帧。
- **Detect Broadcast De-authentication**：解除认证广播会试图断开范围内的所有客户端。这类攻击不是把伪造的解除认证帧发送到特定的MAC地址，而是发送到一个广播地址。
- **Detect Broadcast Disassociation**：通过向广播地址（FF:FF:FF:FF:FF:FF）发送解除关联帧，入侵者可以使网络上的所有站点断开连接，造成广泛的拒绝服务攻击。
- **Detect Adhoc Network using Valid SSID**：如果一个未经授权的Adhoc网络使用与授权网络相同的SSID，有效的客户端可能会被欺骗连接到错误的网络。如果客户端连接到恶意的adhoc网络，可能会造成安全漏洞或攻击。
- **Detect Long SSID**：此功能可以检测名称超过32个字符的长SSID。
- **Detect AP Impersonation**：AP扮演者攻击会假冒有效AP的BSSID和

ESSID。AP扮演者攻击可用于中间人攻击、试图绕过检测的Rogue AP、或者蜜罐攻击。

- **Detect Omerta Attack**：Omerta是一个802.11 DoS工具，它在收到数据帧时向通道上的所有客户端发送断开连接帧。Omerta攻击的特征是发送具有0x01的原因码的断开连接帧。这个原因码是“**unspecified**”的，在正常情况下不会被使用。
- **Detect Null Probe Response**：空探测响应攻击有可能导致许多802.11网卡的固件崩溃或锁死。在这类攻击中，客户端的探测请求帧由一个包含空SSID的探测响应回答。许多常见的网卡在收到这样的探测响应后会锁定。
- **Detect Invalid Address Combination**：在这类攻击中，入侵者可以使AP将解除认证帧和解除关联帧发送给它的客户端。在源地址字段中使用广播或组播MAC地址都可能导致这类情况发生。
- **Detect Reason Code Invalid of De-authentication**：具有无效原因代码的解除认证数据包会被视为攻击。
- **Detect Reason Code Invalid of Disassociation**：具有无效原因代码的解除关联数据包会被视为攻击。

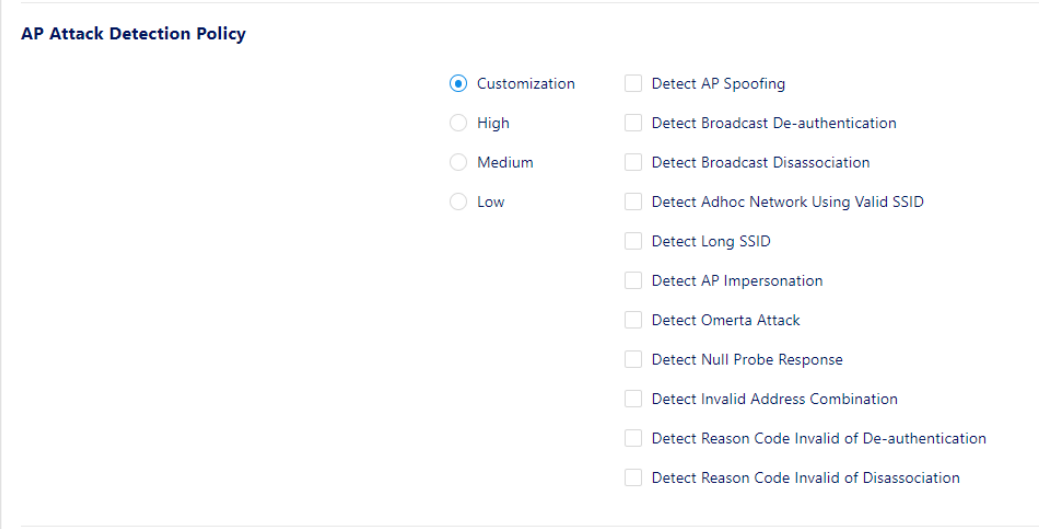


图 208：AP 攻击检测策略

可以快速选择下列相应的级别来完成AP攻击检测策略设置：

- **Low**：
  - 检测AP仿冒

- 检测广播解除认证
- 检测广播解除关联

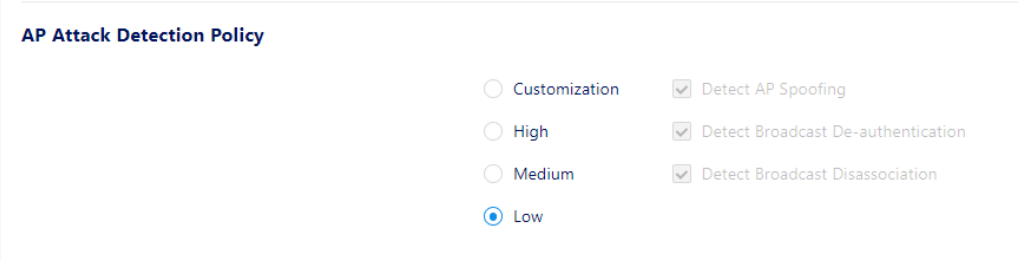


图 209：AP 攻击检测策略 - Low

► **Medium：**

- 检测AP仿冒
- 检测广播解除认证
- 检测广播解除关联
- 使用有效SSID检测Adhoc网络
- 检测长SSID

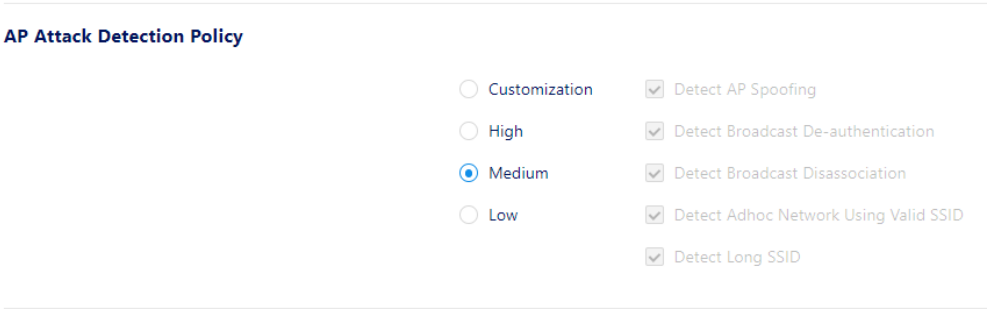


图 210：AP 攻击检测策略 - Medium

► **High：**下列所有项目将都启用

- 检测AP仿冒
- 检测广播解除认证
- 检测广播解除关联
- 使用有效SSID检测Adhoc网络
- 检测长SSID
- 检测AP扮演者

- 检测Omerta攻击
- 检测空探测响应
- 检测无效地址组合
- 检测解除认证无效原因代码
- 检测解除关联无效原因代码

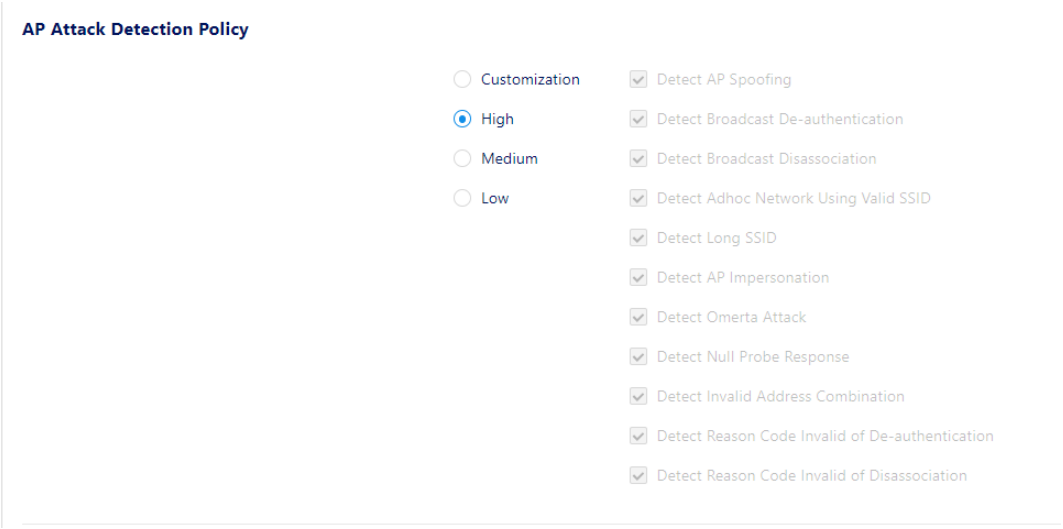


图 211：AP 攻击检测策略 - High

► **Customization：**可以从下列项目中选择关注的攻击检测策略。

- 检测AP仿冒
- 检测广播解除认证
- 检测广播解除关联
- 使用有效SSID检测Adhoc网络
- 检测长SSID
- 检测AP扮演者
- 检测Omerta攻击
- 检测空探测响应
- 检测无效地址组合
- 检测解除认证无效原因代码
- 检测解除关联无效原因代码

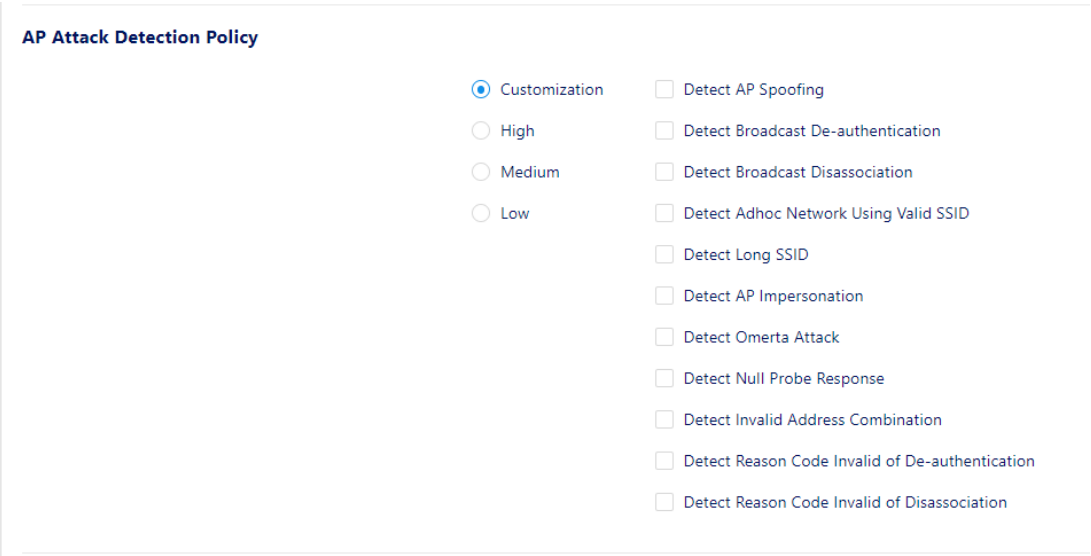


图 212：AP 攻击检测策略 - Customization

■ 客户端攻击检测策略

客户端攻击检测策略可检测来自无线客户端的攻击。根据所选级别，可使用以下检测方法：

► **Detect Valid Client Misassociation**：此功能不会检测攻击，而是监视网络中有效的无线客户端及其关联。有效的客户端错误关联可能对网络安全构成潜在威胁。可监测以下4种误关联类型：

- Valid Client Associated to a Rogue AP：与Rogue AP关联的有效客户端。
- Valid Client Associated to an Interfering AP：与干扰AP关联的有效客户端。
- Valid Client Associated to a Honeypot AP：Honeypot AP是一个无效的AP，但它使用的SSID指定为有效。
- Valid Client in Ad Hoc Connection Mode：已加入Ad hoc网络的有效客户端。

► **Detect Omerta Attack**：Omerta是一个802.11 DoS工具，它在收到数据帧时向通道上的所有客户端发送断开连接帧。Omerta攻击的特征是发送具有0x01的原因码的断开连接帧。这个原因码是“**unspecified**”的，在正常情况下不会被使用。

► **Detect Unencrypted Valid Client**：以未加密模式传输流量的有效客户端存在安全风险。入侵者可以用嗅探器窃听未加密的流量（也称为数据包捕

获工具），并将数据包重新组装成原始消息。

- **Detect 802.11 40MHZ Intolerance Setting**：当客户端对HT能力“禁用位”进行了设置，将其设定为无法使用40MHz BSS，那么AP必须使用较低的数据速率与所有客户端通信。网络管理员通常会注意到网络性能受到了影响，会猜想是否有设备在广告禁用40MHz。
- **Detect Active 802.11n Greenfield Mode**：当802.11设备使用HT操作模式时，它们不能与802.11a/b/g客户端共享相同的信道。它无法与传统设备进行通信，而且使用传输介质的方式也不同，这就会导致冲突、检测到错误和重传。
- **Detect DHCP Client ID**：如果客户端发送的DHCP DISCOVER数据包中的Client-ID标签（标签61）与源MAC地址不匹配，那么可能正在进行DHCP拒绝服务攻击，攻击的目的是耗尽DHCP池。
- **Detect DHCP Conflict**：如果客户端接收到DHCP地址但继续使用不同的IP地址，可能表示这是个配置错误或仿冒的客户端。
- **Detect DHCP Name Change**：DHCP配置协议允许客户端自主选择将主机名放入DHCP Discover数据包中。只有在客户端发生重大变化（例如双启动系统）时，这个值才会更改。因此值的更改通常可能表示存在客户端仿冒或MAC克隆攻击。
- **Detect Too Many Auth Failure Request**：多次试图连接到DAP但未能通过身份验证的客户端为攻击性客户端。
- **Detect Long SSID At Client**：根据客户端发送的数据包，在无线环境中检测长SSID。
- **Detect Malformed Frame-Assoc Request**：一些用于AP的无线驱动程序无法正确解析关联请求帧中包含的SSID信息元素标签。使用空SSID的恶意关联请求可能会在目标设备上触发DoS或潜在的代码执行条件。
- **Detect Reason Code Invalid of De-authentication**：具有无效原因代码的解除认证数据包会视为攻击。
- **Detect Reason Code Invalid of Disassociation**：具有无效原因代码的解除关联数据包会视为攻击。

图 213：客户端攻击检测策略

可以快速选择下列相应的级别来完成客户端攻击检测策略设置：

► **Low：**

- 检测有效的客户端错误关联
- 检测多次身份验证失败客户端

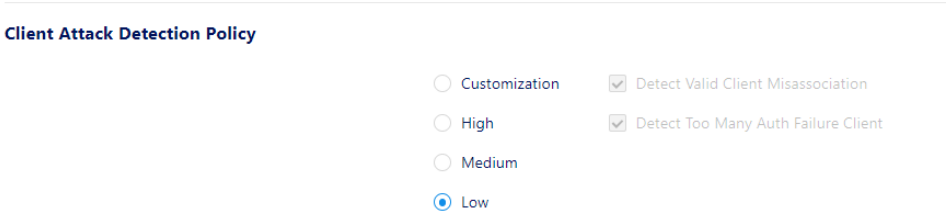


图 214：客户端攻击检测策略 - Low

► **Medium：**

- 检测有效的客户端错误关联
- 检测Omerta攻击
- 检测未加密的有效客户端
- 检测多次身份验证失败客户端
- 在客户端检测长SSID
- 检测到畸形帧关联请求

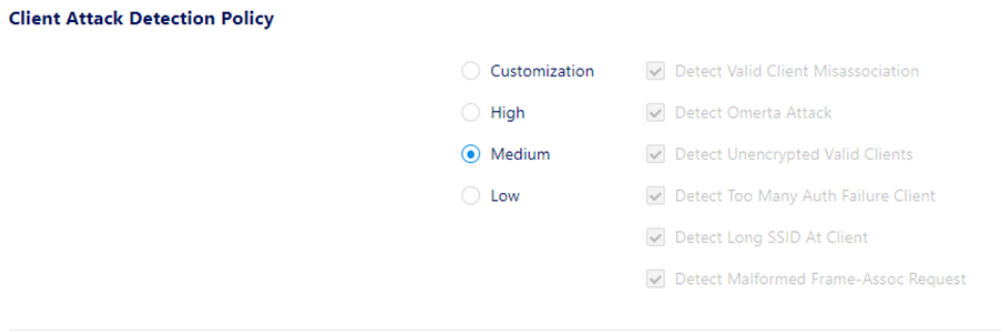


图 215：客户端攻击检测策略 - Medium

► **High：**

- 检测有效的客户端错误关联
- 检测Omerta攻击
- 检测未加密的有效客户端
- 检测802.11 40MHZ不耐受设置
- 检测活动的802.11n Greenfield模式
- 检测DHCP客户端ID
- 检测到DHCP冲突
- 检测DHCP名称更改
- 检测多次身份验证失败客户端
- 在客户端检测长SSID
- 检测到畸形帧关联请求
- 检测解除认证无效原因代码
- 检测解除关联无效原因代码

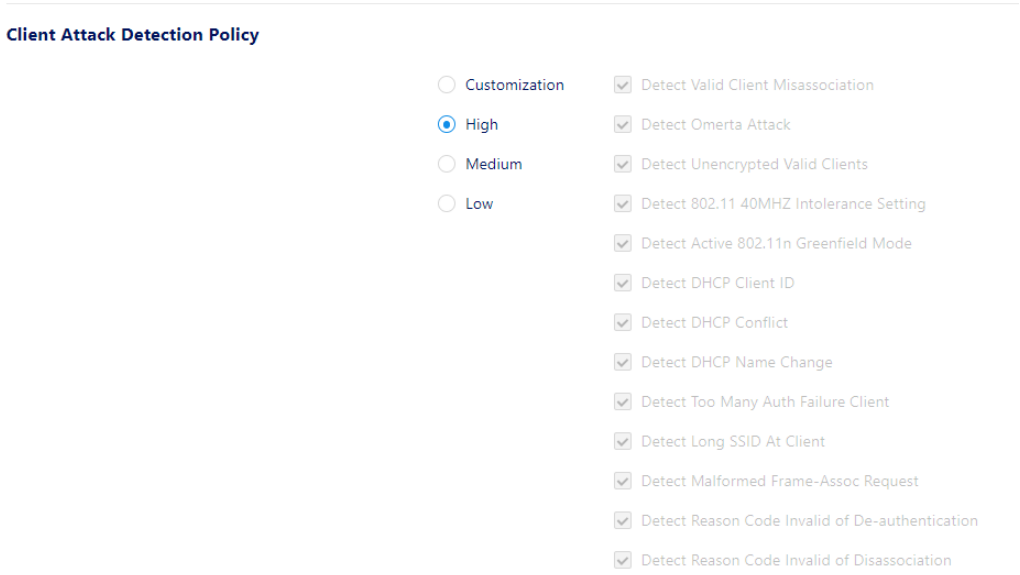


图 216：客户端攻击检测策略 - High

► **Customization：**

可以从下列项目中选择关心的攻击检测策略。

- 检测有效的客户端错误关联
- 检测Omerta攻击
- 检测未加密的有效客户端
- 检测802.11 40MHZ不耐受设置
- 检测活动的802.11n绿野模式
- 检测DHCP客户端ID
- 检测到DHCP冲突
- 检测DHCP名称更改
- 检测多次身份验证失败客户端
- 在客户端检测长SSID
- 检测到畸形帧关联请求
- 检测解除认证无效原因代码
- 检测解除关联无效原因代码

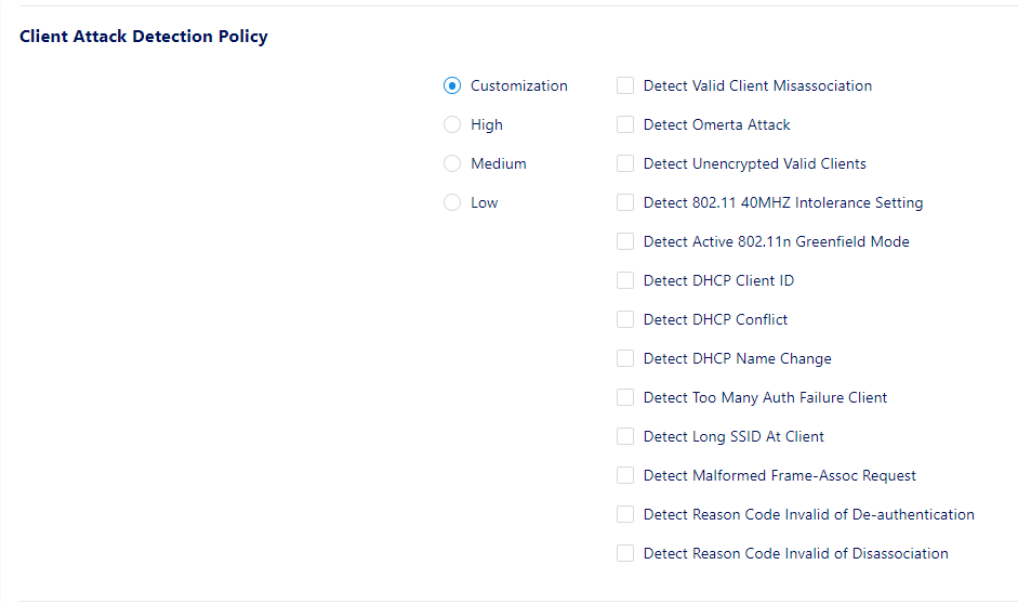


图 217：客户端攻击检测策略 - Customization

■ **客户端黑名单策略**

客户端黑名单有两个来源：用户手动创建或系统动态添加。如果启用了动态客户端黑名单，系统会将WIPS发现的入侵者动态添加到客户端黑名单中，并阻止其与网络关联。

系统会将以下检测到的项目添加到客户端黑名单中：客户端攻击检测列表、临时客户端和与Rogue AP相关联的客户端。

- **Max Auth Failure Times**：身份验证失败次数阈值。
  短时间内，如果客户端多次在关联阶段未能通过身份验证，将被视为攻击并添加到客户端黑名单中。（可选值：3~10次/5~3600秒，默认值：10次/60秒）。
- **Expiry Time**：客户端黑名单的过期时间。一旦过期，客户端将从黑名单中移除，并允许其与有效网络进行关联，直到再次被检测为威胁为止。（可选值：1小时至365天，默认值：1天）。

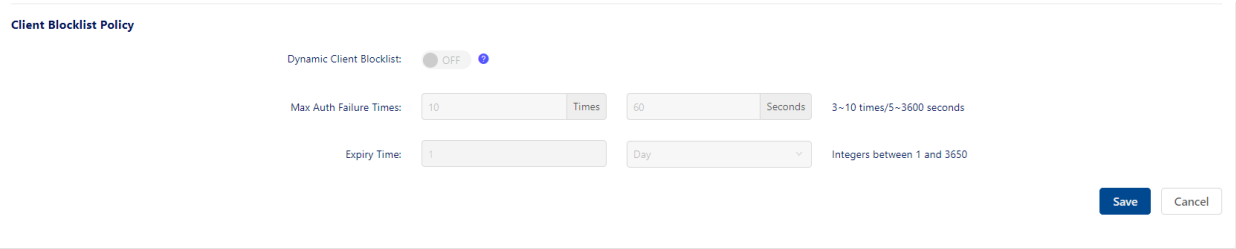


图 218：客户端黑名单策略

11.2 AP 记录

Security→AP Record可显示网络上检测到的AP列表，包括干扰AP、Rogue AP和有效AP。

- ► **AP MAC：**检测到的AP的MAC地址。
- ► **Encryption Type：**WLAN的加密方法。
- ► **Collection Time：**检测到的AP最近出现的时间。
- ► **Device Network Type：**检测到的AP的网络类型。
- ► **Signal Strength：**检测到的AP的RSSI。
- ► **WLAN Name：**AP广播的SSID。
- ► **Client Number：**与检测到的AP相关的客户端数量。
- ► **Whether to Join Blocklist List：**AP是否记入黑名单。
- ► **Channel：**检测到的AP上的无线电频率的工作信道。
- ► **Attack Item：**使用的攻击检测策略（例如，检测有效的站关联错误）
- ► **Device Type：**
  - Rogue AP：MAC地址与恶意OUI匹配的AP为恶意AP。也可通过设置Detect Rogue SSID Keyword判断AP是否为恶意AP。
  - Valid AP：MAC地址与有效OUI匹配的AP为有效AP。
  - Interfering AP：除识别为Rogue AP和Valid AP的AP为干扰AP。
- ► **Scanning AP：**检测Rogue AP、干扰AP和有效AP的AP的MAC地址。

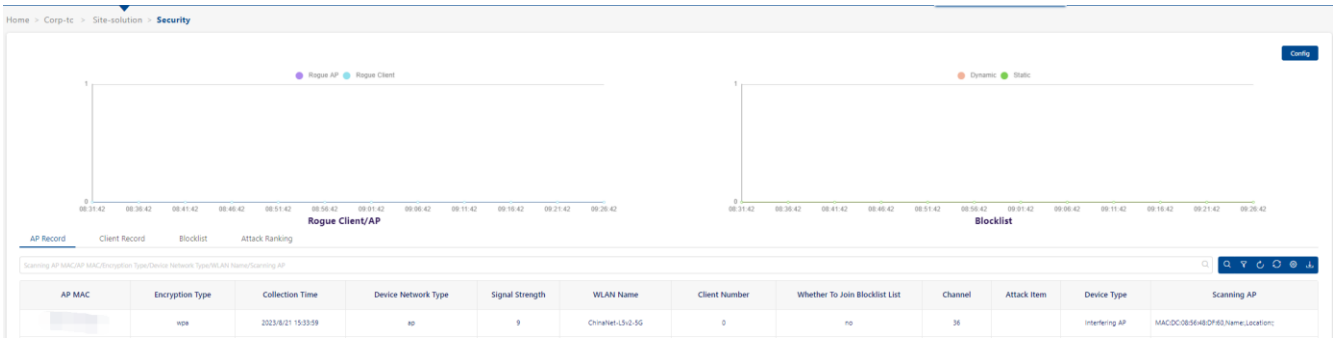


图219：AP 记录界面

11.3 客户端记录

- **Client MAC：**干扰客户端或Rogue客户端的MAC地址。
- **Scanning Client MAC：**扫描客户端MAC地址。
- **Association AP MAC：**与客户端关联的干扰AP或Rogue AP的MAC地址。
- **Attack Item：**使用的攻击检测策略（例如，检测有效的站关联错误）。
- **Collection Time：**最后一次发现Rogue客户端或干扰客户端的时间。
- **Device Network Type：**检测到的客户端的网络类型。
- **Signal Strength：**检测到的客户端的RSSI。
- **Client IP：**检测到的客户端的IP地址。
- **Device Type：**
  - 与Rogue AP相关联的客户端。
  - 与Interfering AP相关联的客户端。

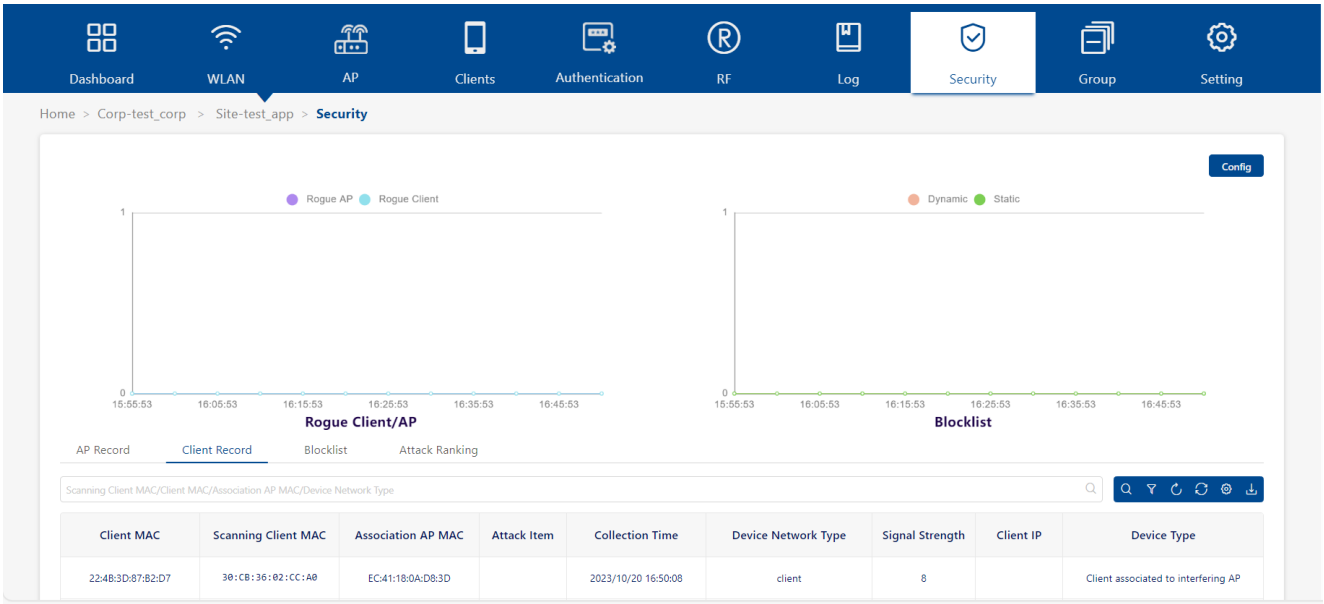


图 220：客户端记录界面

11.4 黑名单

黑名单是一种基于客户端级别的用户连接SSID的基本访问控制机制。列入黑名单的客户端将被拒绝与DAP关联。一旦客户端被列入黑名单，它将无法连接到任何安全级别的WLAN（企业级、个人级或开放级）。可以根据客户端的MAC地址在黑名单中添加和删除客户端。

无线黑名单页面会显示所有被阻止客户端的信息，在这一页面还可将客户端手动添加到黑名单中。

- **Client MAC：**黑名单中的客户端的MAC地址。
- **Type：**客户端被添加到黑名单的方式。
  - **Manual：**由用户添加到黑名单。
  - **Auto：**由WIPS策略动态添加。
- **Start Time：**阻止开始的时间。

  一旦开始，客户端不可访问无线网络。
- **Expiry Time：**黑名单的过期时间。

  到期时间过后，客户端即可访问无线网络。
- **From(Site/Group)：**客户端的Site或Group。

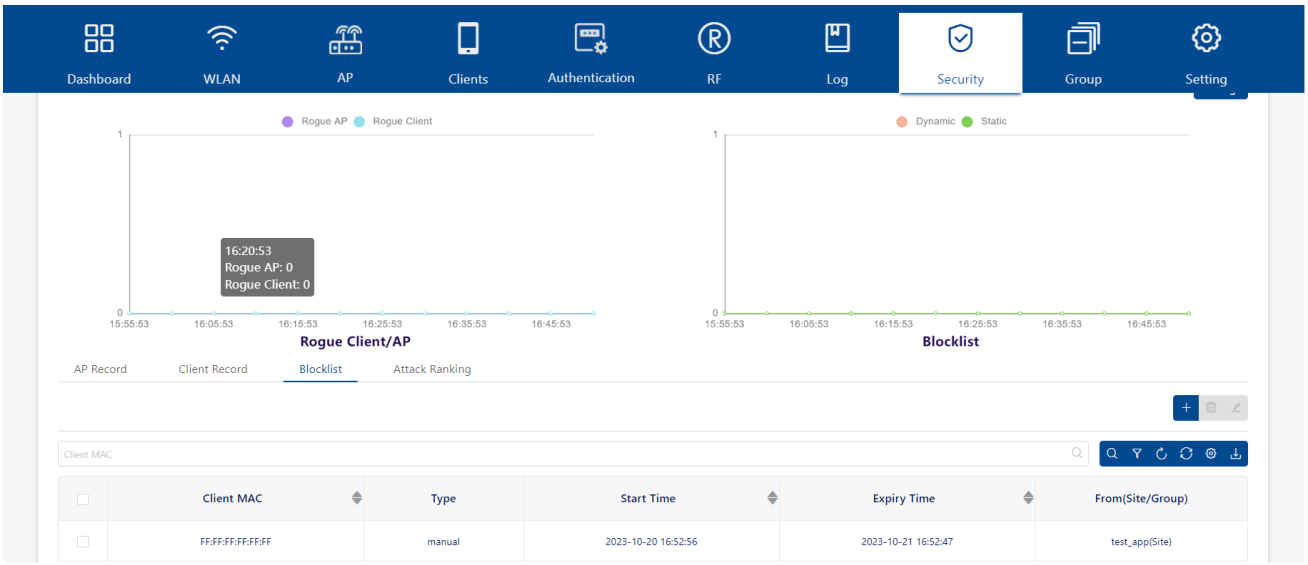


图 221：黑名单界面

11.4.1 将客户端添加到黑名单

- ☐ 点击“**+**”图标，打开“**Add to Blocklist**”窗口。
- ☐ 输入客户端MAC地址。
- ☐ 点击“**Save**”按钮。
- ☐ 如需添加更多客户端，重复以上步骤。

请为客户端设置过期时间。到期后，客户端可以再次连接到此站点的SSID。

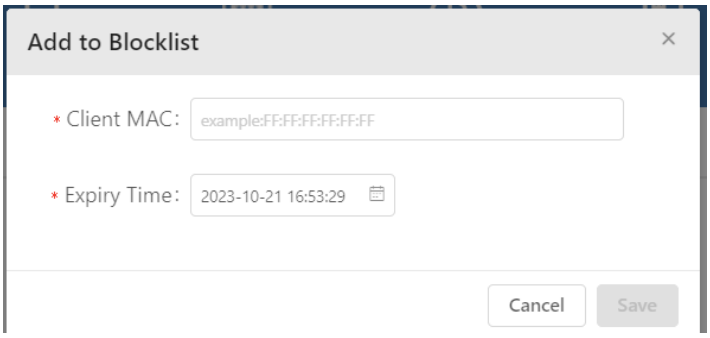


图 222：将客户端添加到黑名单

11.4.2 从黑名单中删除客户端

- ☐ 在列表中选择一个设备。
- ☐ 点击“**Delete**”图标。
- ☐ 在确认提示上单击“**Yes**”。

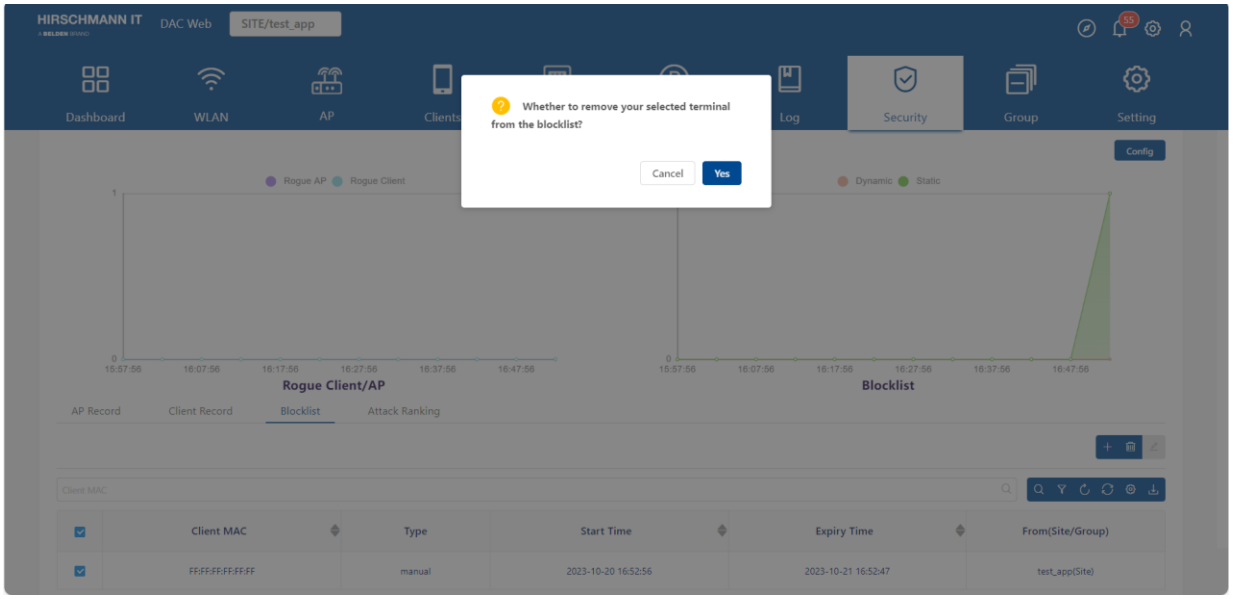


图 223：从黑名单中删除客户端

11.5 攻击排名

计算攻击数量。

- **Attack Item**：使用的攻击检测策略（例如，检测有效的站关联错误）。
- **Attack Times**：攻击项目的数量。

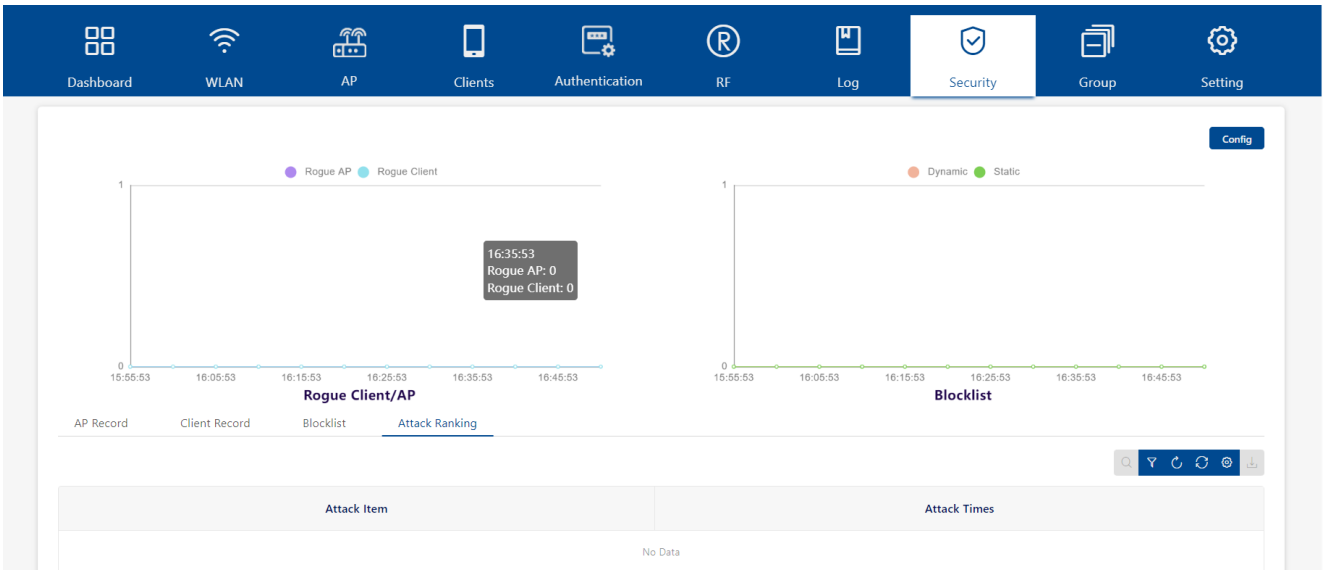


图 224：攻击排名界面

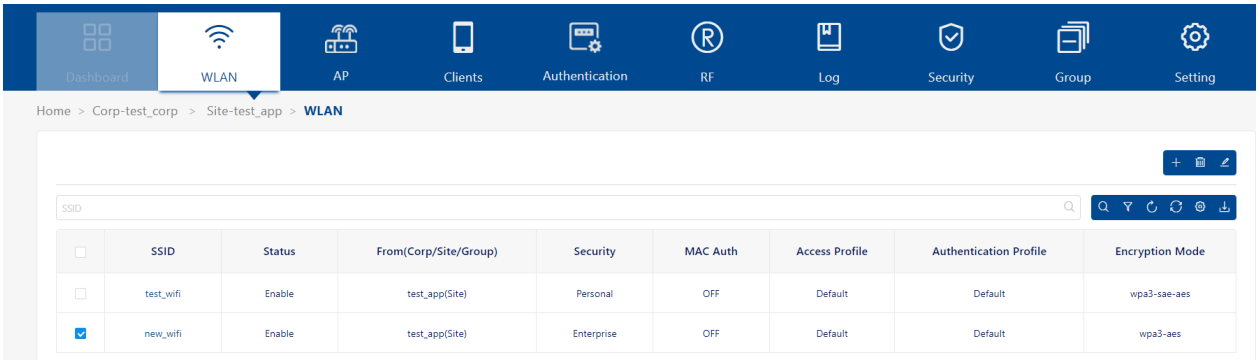
12 强制登录页

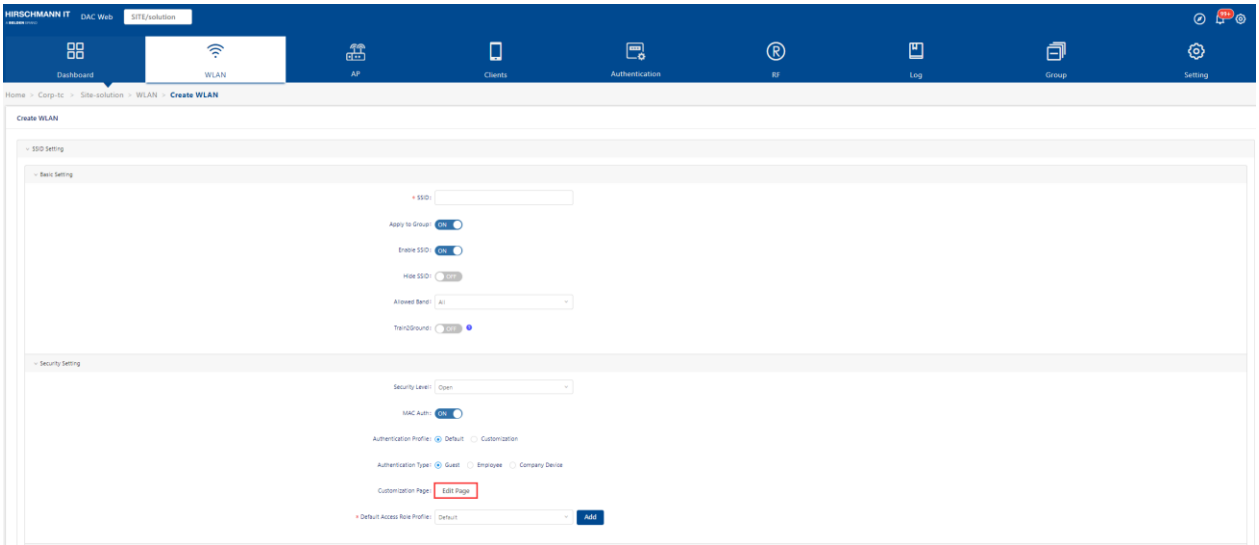
强制登录页身份验证是一种通过网页获取用户凭据，并通过RADIUS服务器对其进行身份验证的机制。如果认证成功，则RADIUS服务器可能会返回适用于用户设备流量的角色（策略列表）。强制登录页提供了一个二级身份验证，用于将一个新的角色（QoS策略列表）应用于用户。员工功能提供了一个外部的、访客强制登录页身份验证机制。

本章包含下列主题：

12.1 进入门户页面编辑器

- 门户页面绑定到访客接入策略或员工接入策略。
- 要使用门户身份验证，请先在WLAN页面启用“**MAC Auth**”并禁用“**Train2Groud**”。
- 如果Authentication Profile选择“**Default**”，可以通过点击“**Edit page**”按钮进入门户编辑器。





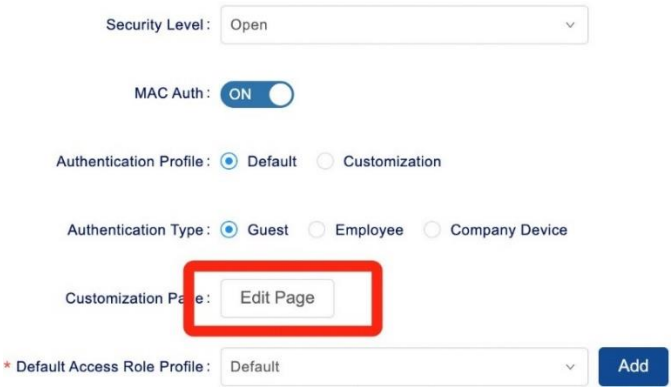


图 225：编辑门户页面

☐ 如果Authentication Profile选择“**Customization**”，可以在访客接入策略或员工接入策略页面中找到门户编辑器的入口。

► 访客接入策略

Authentication→Guest Access→Guest Access Strategy

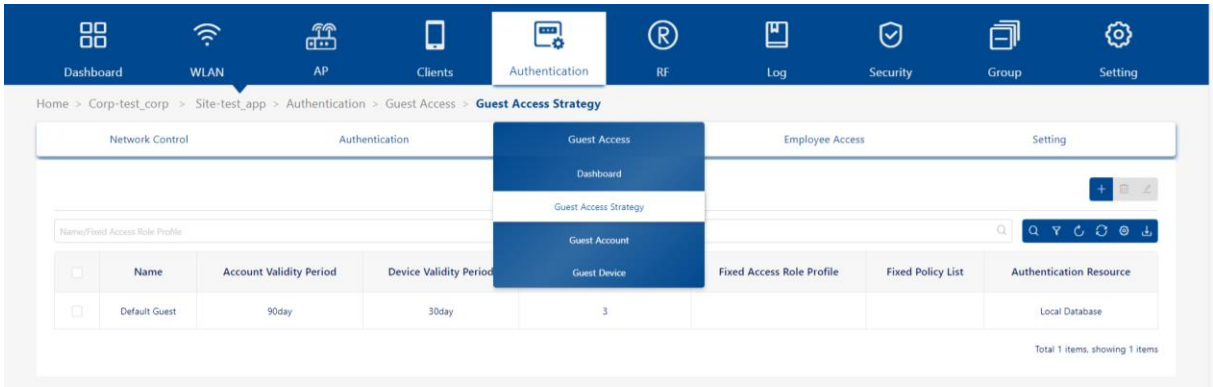


图 226：进入门户页面编辑器 - 访客

► 员工接入策略

Authentication→Employee Access→Employee Access Strategy

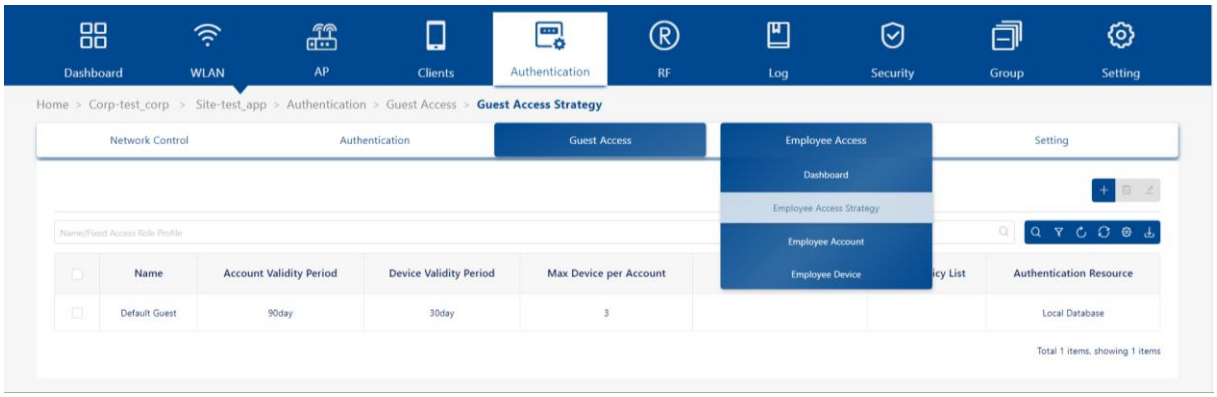


图 227：进入门户页面编辑器 - 员工

12.2 门户编辑器视图

门户定制页面布局如下图所示。门户页面分为以下功能块：

- **Page selector**

  页面选择器一般包括3个HTML页面：index，success和fail。可选择其中一个进行编辑。

- **Page view**

  页面视图可动态显示所选的门户页面。编辑组件属性时，页面视图将实时更新并显示修改结果。

- **Page attributes view**

  页面属性视图可查看HTML组件的设置和属性。

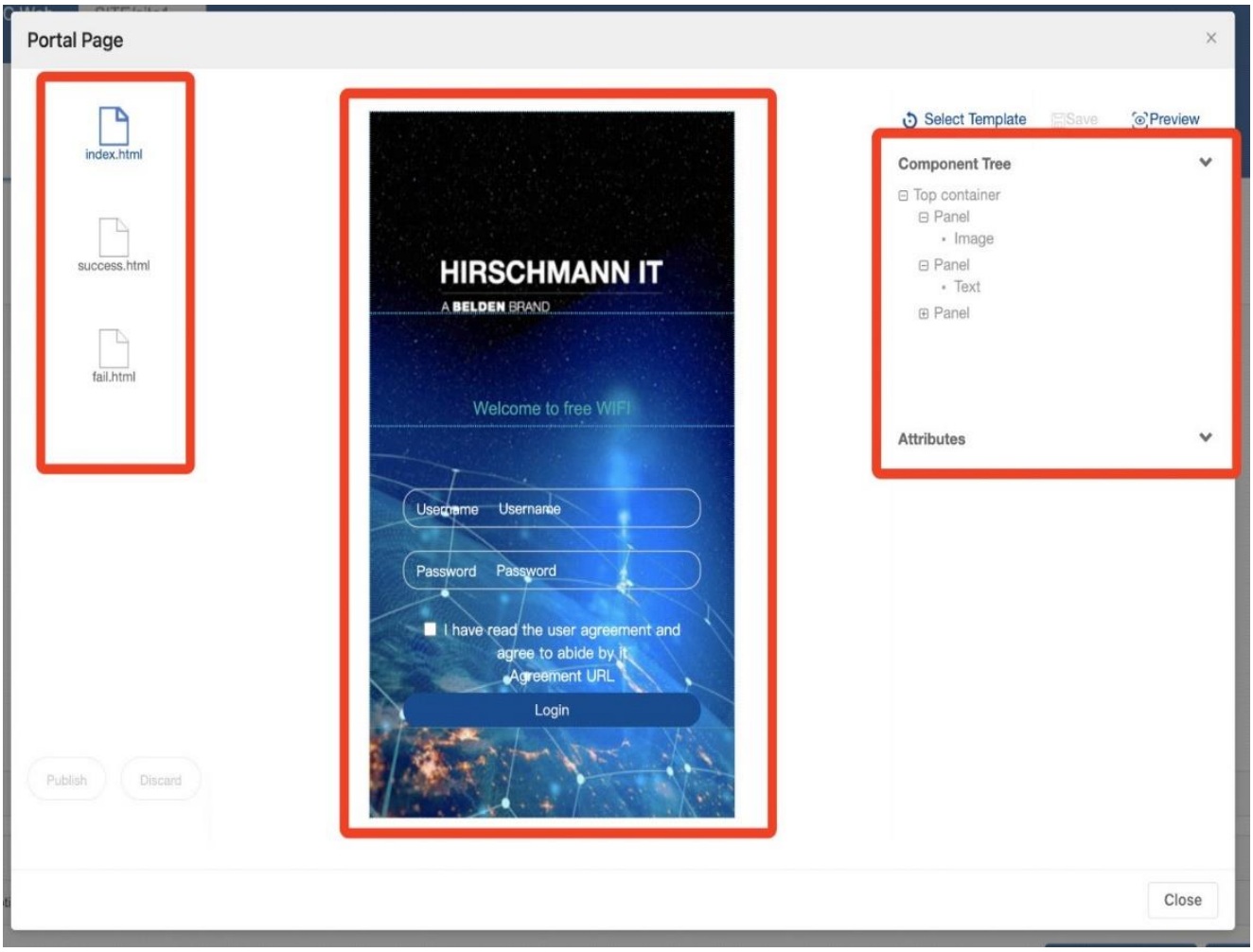


图 228：门户编辑器视图

12.3 选择模板

- ☐ 点击页面属性视图顶部的“**Select Template**”按钮。
- ☐ 在“**Prompt Message**”窗口上，点击“**Confirm**”按钮。

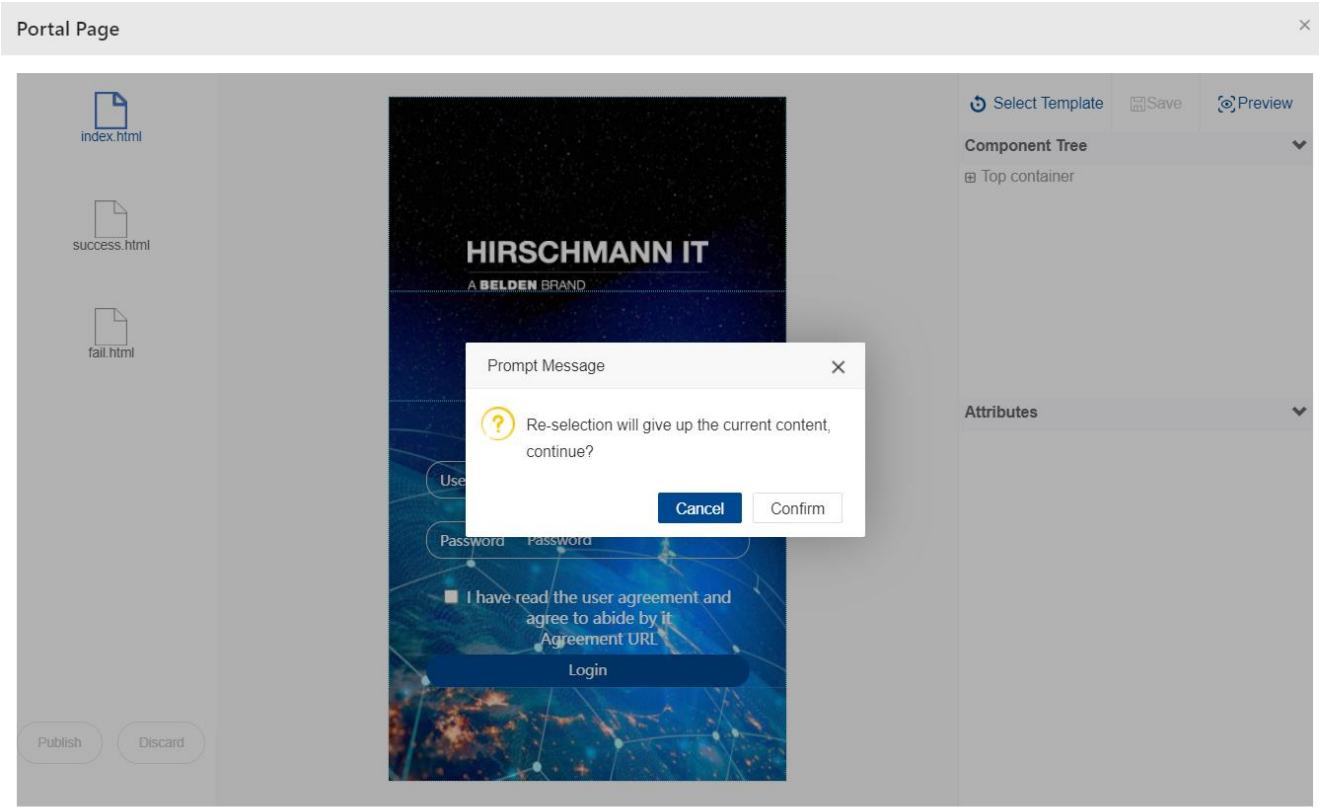


图 229：选择模板

☐ 共有4个模板可供选择：

► **Login by Account**：选择此门户模板，用户可以使用**“Account”**和**“Password”**登录。访客和员工的账户和密码可以在Authentication Profile→Guest Access→Guest Account中，或者Authentication Profile→Employee Access→Employee Account中添加。

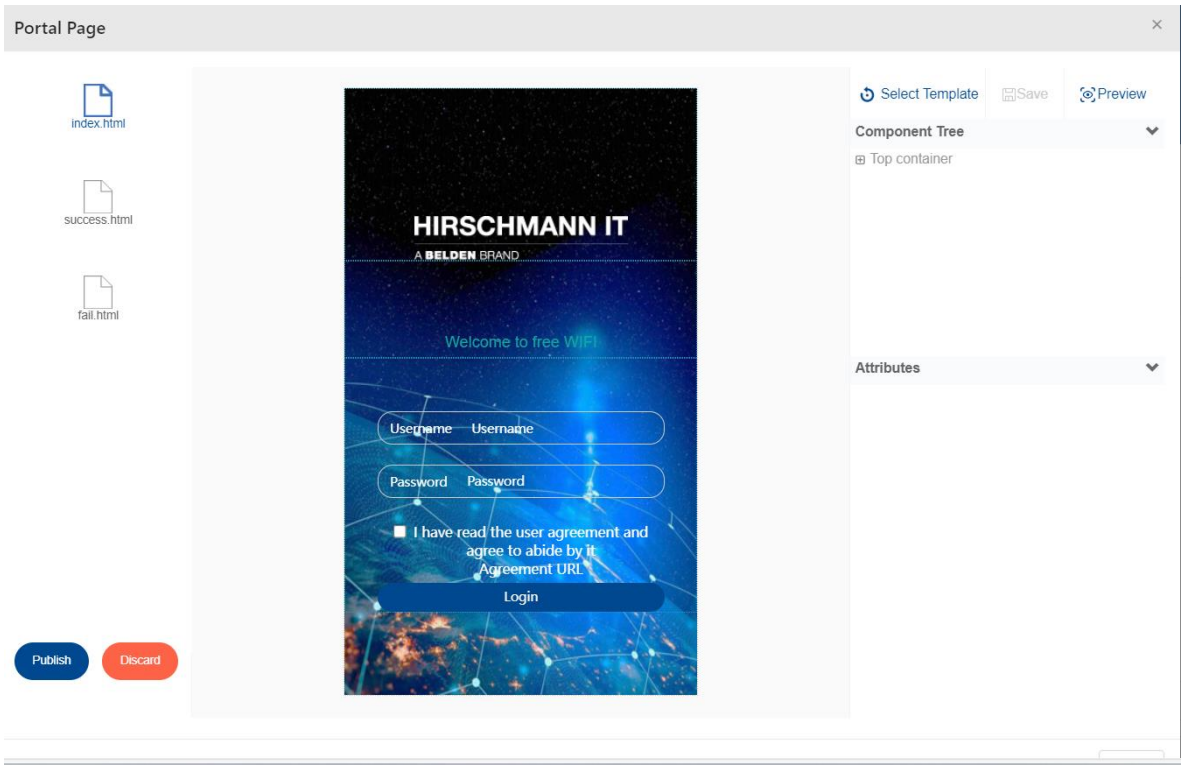


图 230：选择模板 - Login by Account

► **Access Code**：此门户模板用于访客接入。可以在“**Create Guest Account**”页面添加访问码。选择“**Access Code**”作为访客类型。

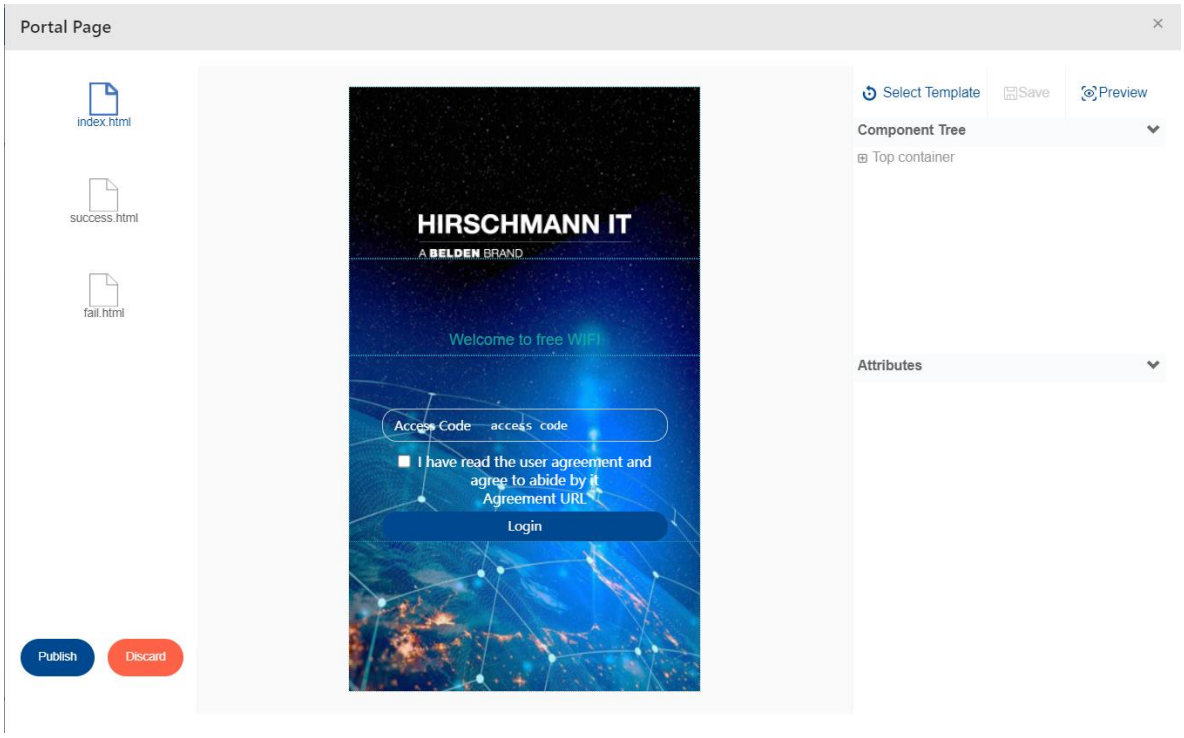


图 231：选择模板 - Access Code

► **Scan QRCode by Employee**：此门户模板用于访客接入。
访客使用此模板关联到WLAN时，将获得一个包含二维码的门户页面。任何员工都可以用用户认证的手机扫描二维码来授权访客。

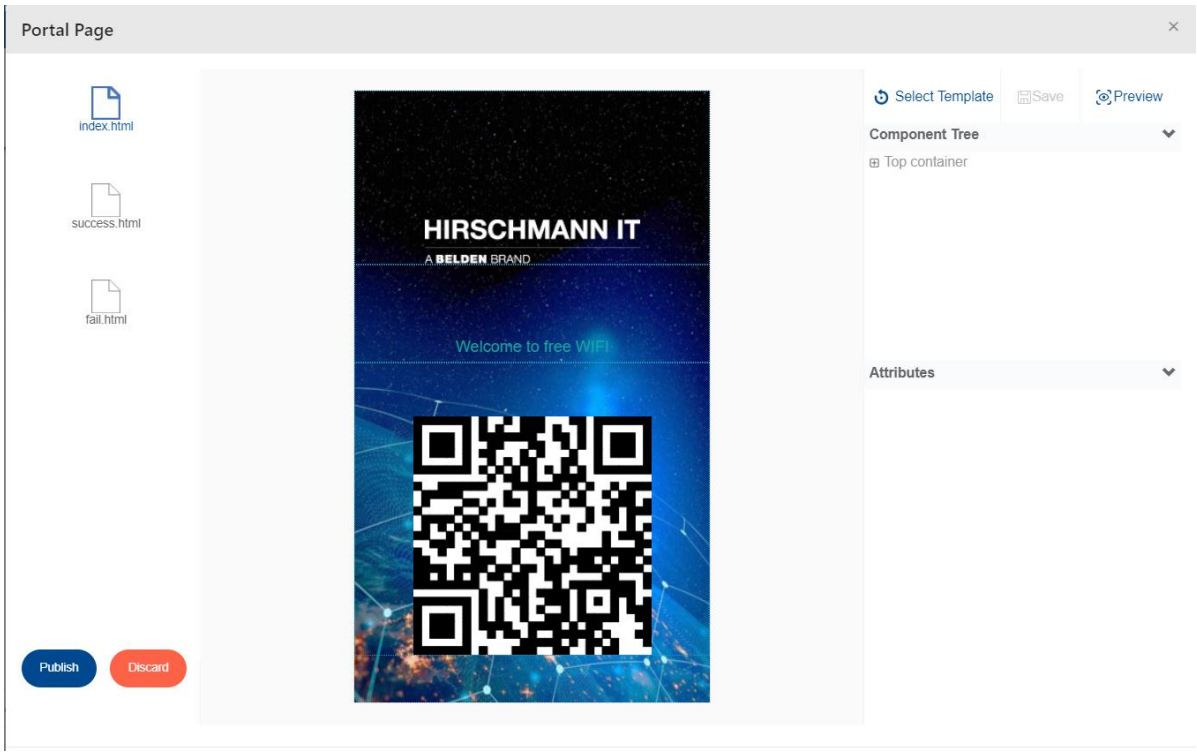


图 232：选择模板 - Scan QRCode by Employee

► **SMS Login**：用户可以使用手机号码登录此门户模板。

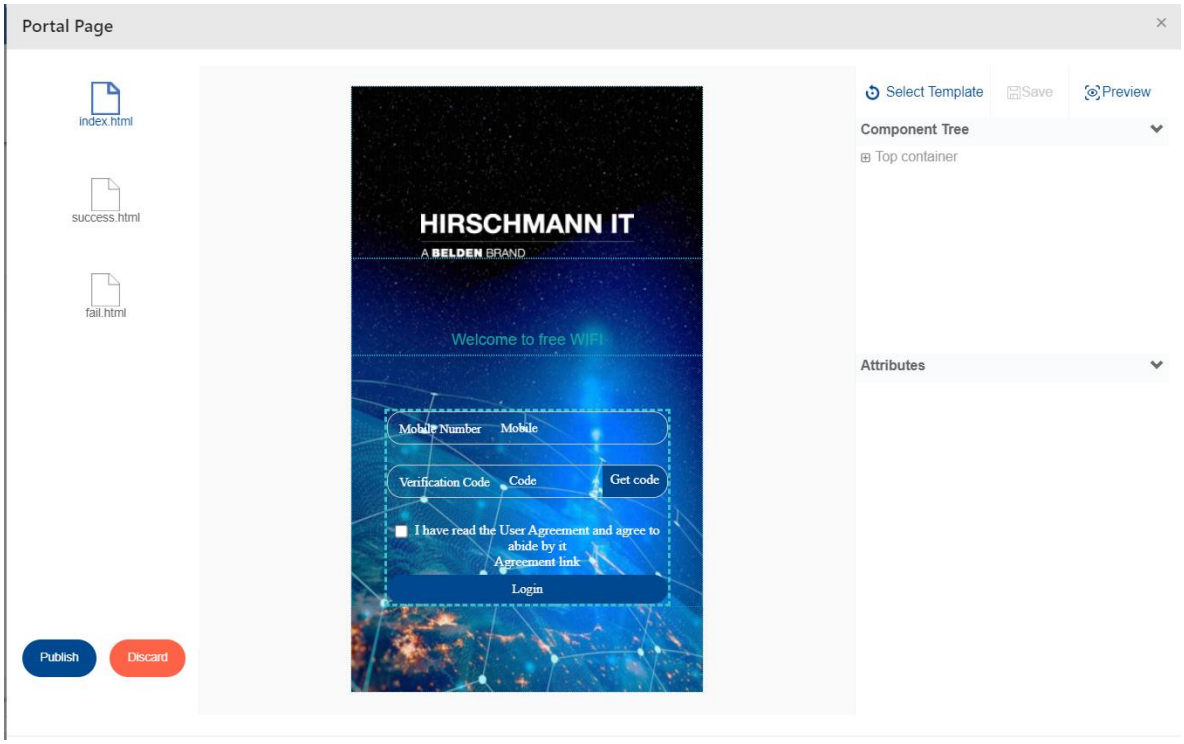


图 233：选择模板 - SMS Login

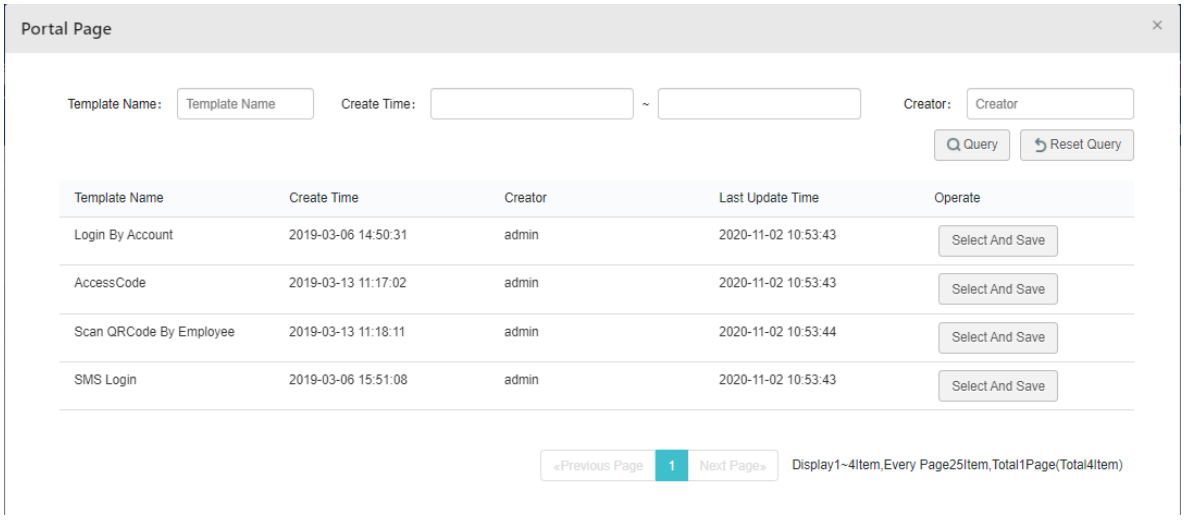


图 234：门户页面

12.4 页面选择器

每个门户模板通常包含3个页面：

- Index
- Success
- Failed

索引页面包含登录表单。用户登录成功，即可看到成功页面。用户登录失败，即可看到失败页面。

点击页面，即可进行编辑。

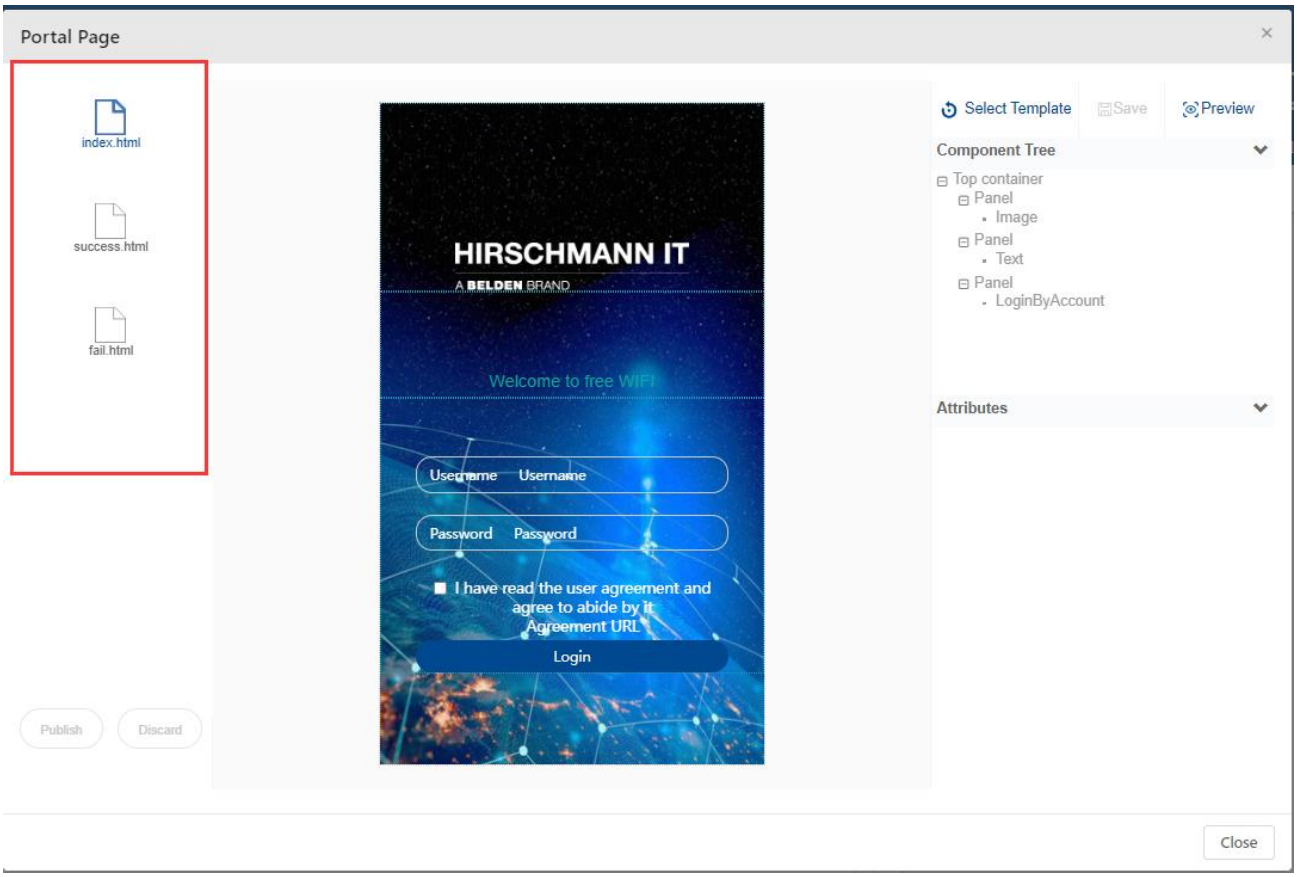


图 235：页面选择器

12.5 页面视图

每个页面包含多个组件。这些组件可以是一张图片、一段文本或者一个表单。可以单击页面元素或从组件树中选择相应组件并进行编辑。页面的显示内容和视觉效果都可进行更改。

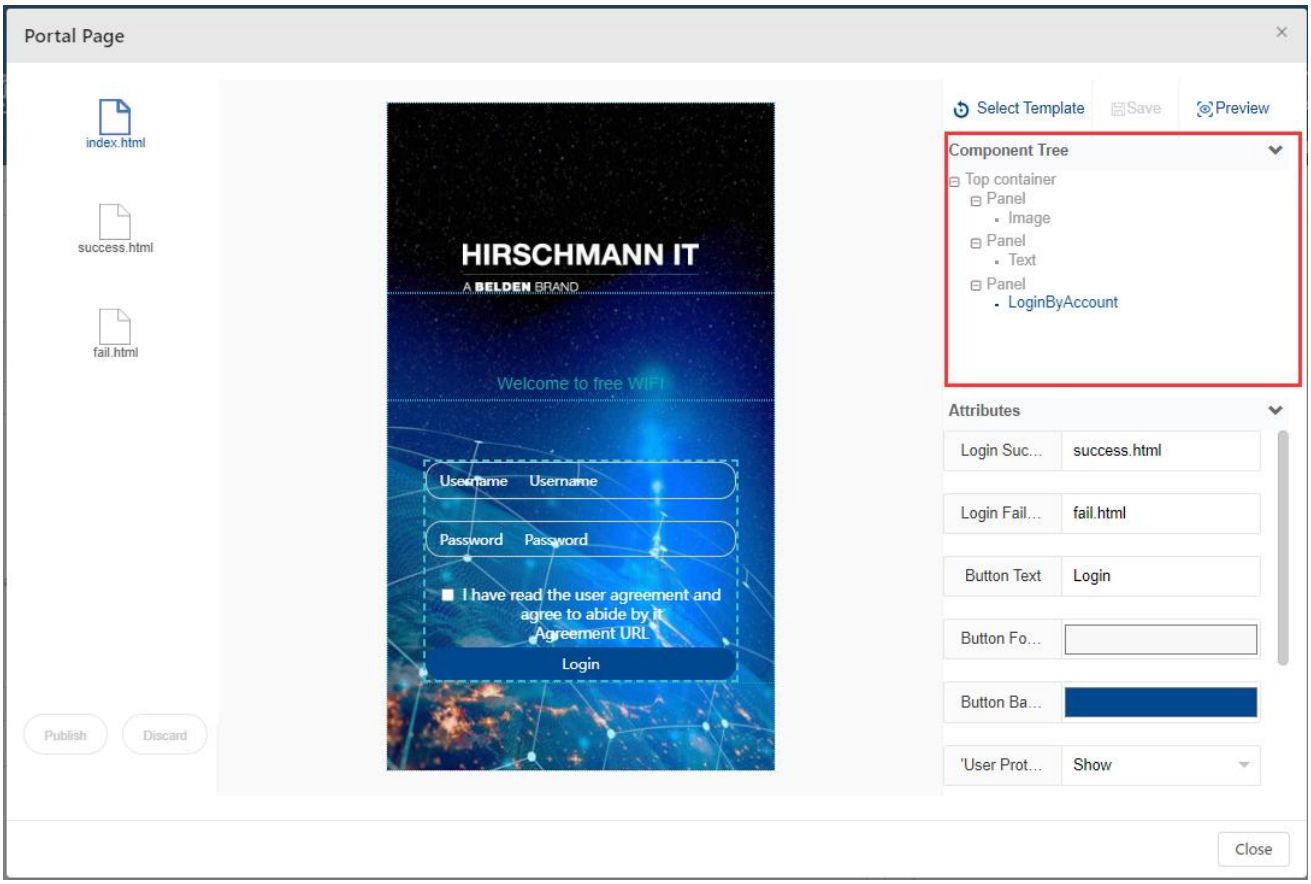


图 236：组件树

12.6 组件属性

每个组件都有若干属性，可以通过修改这些属性来改变页面上显示的内容。

12.6.1 图像组件

下列是图像组件的属性：

- **Image**：可以通过修改这一属性来替换当前图像。
- **Width**：图像的宽度。
- **Height**：图像的高度。如果宽度和高度与原始图像的比例不同，图像将会拉伸变形。
- **Link Address**：超链接，用户点击组件时将打开。如果当前页面在用户登录之前显示，需要验证超链接的IP地址是否在允许的IP范围内。
- **Skip Event**：用户设定的点击图像后跳转的事件。

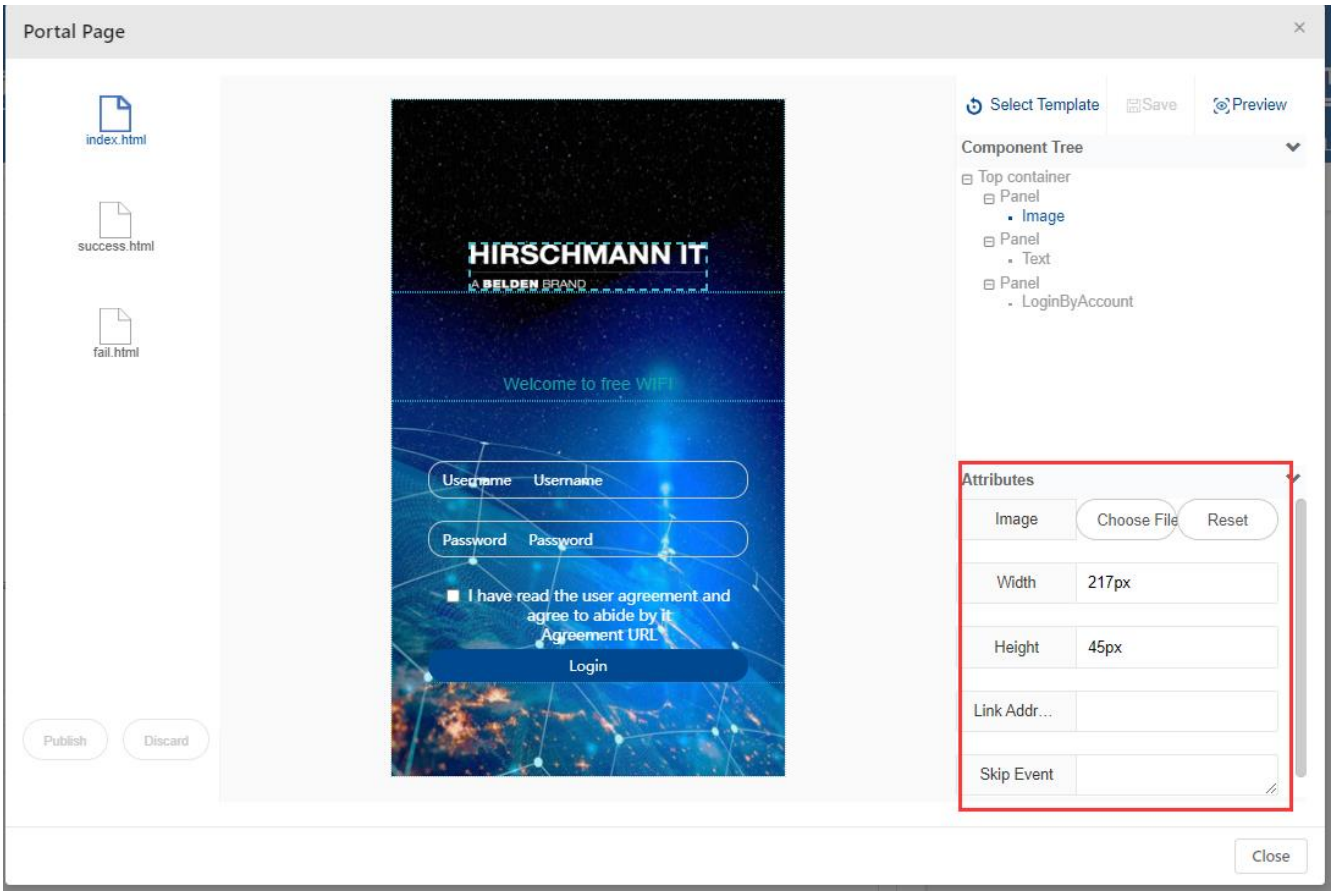


图 237：图像组件属性

12.6.2 文本组件

下列是文本组件的属性：

- **Font Family**：文本的字体类型。
- **Font Size**：文本的字体大小。
- **Content**：文本组件的内容。可以在这里定制个性化信息。
- **Link Address**：点击文本时，URL打开。如果当前页面不是成功页面，则需要验证此URL的IP地址是否在允许的IP范围内。
- **Color**：文本的字体颜色。
- **Action**：点击文本的动作。可选值：none、back或forward。如果配置了链接地址，链接地址在这里会失效。

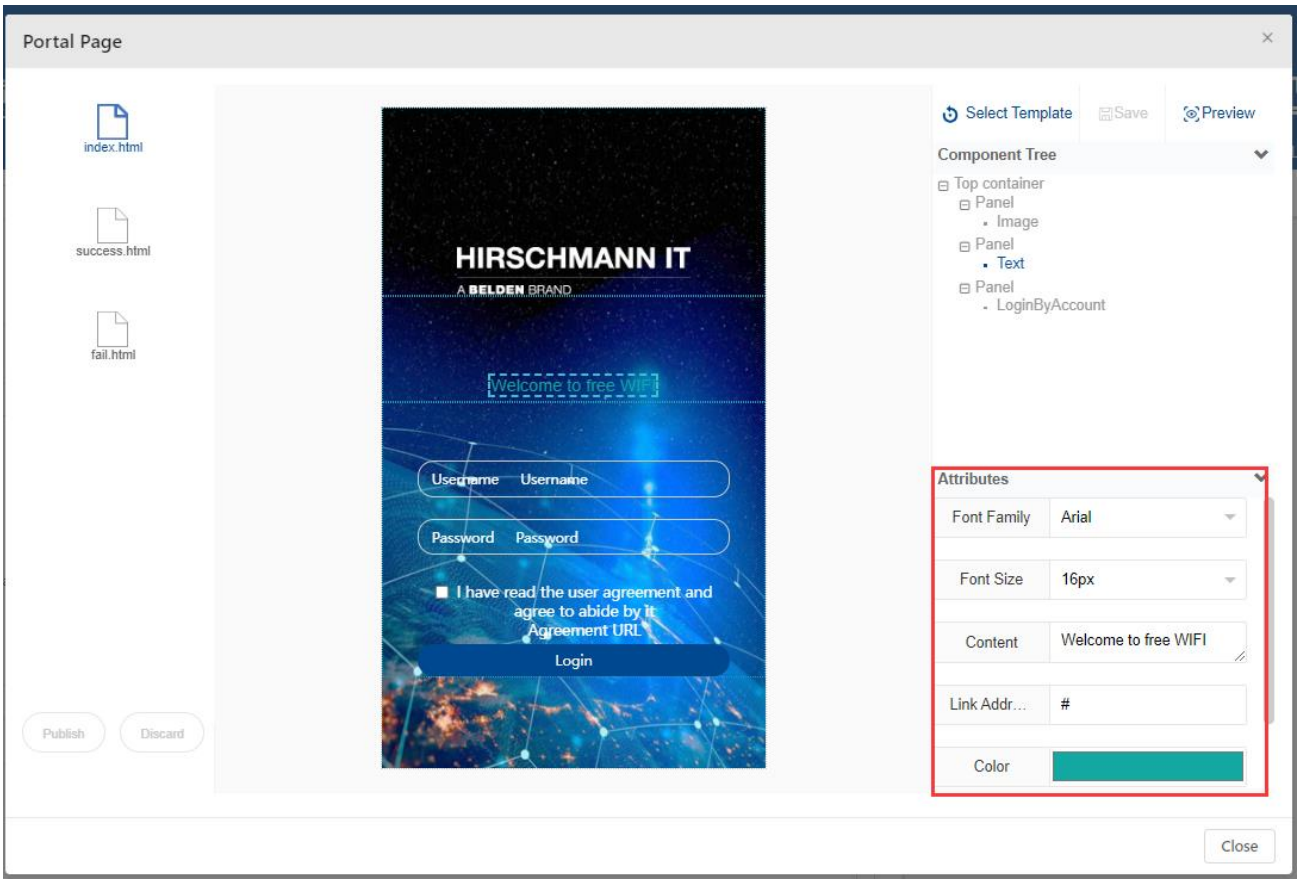


图 238：文本组件属性

12.6.3 表单组件

下列是表单组件的属性：

- **Login Success Redirect URL**：登录成功后重定向到该URL，不再跳转

到模板中的成功页面。可以设置为企业主页或其他推广页面。

- **Login Failed Redirect URL：**登录不成功时，重定向到该URL，不再跳转到模板中的失败页面。需要验证此页面上是否有**“login failure”**的提示。由于用户无法访问网络，需要确保URL所在的IP地址是允许的IP地址。
- **Button Text：**按钮上的文本内容。
- **Button Font Color：**按钮上的文本颜色。
- **Button Background Color：**按钮的颜色。
- **“User Protocol Link” whether or not show：**显示或隐藏用户协议链接文本。
- **“User Protocol Link” Font Color：**用户协议链接文本的字体颜色。
- **“User Protocol Link” whether to add Underline：**显示或隐藏用户协议链接文本上的下划线。
- **Agreement Detail：**用户协议详细信息。
- **Material Width：**仅在员工模板扫描二维码时出现。QR码的宽度可以是像素数或百分比。

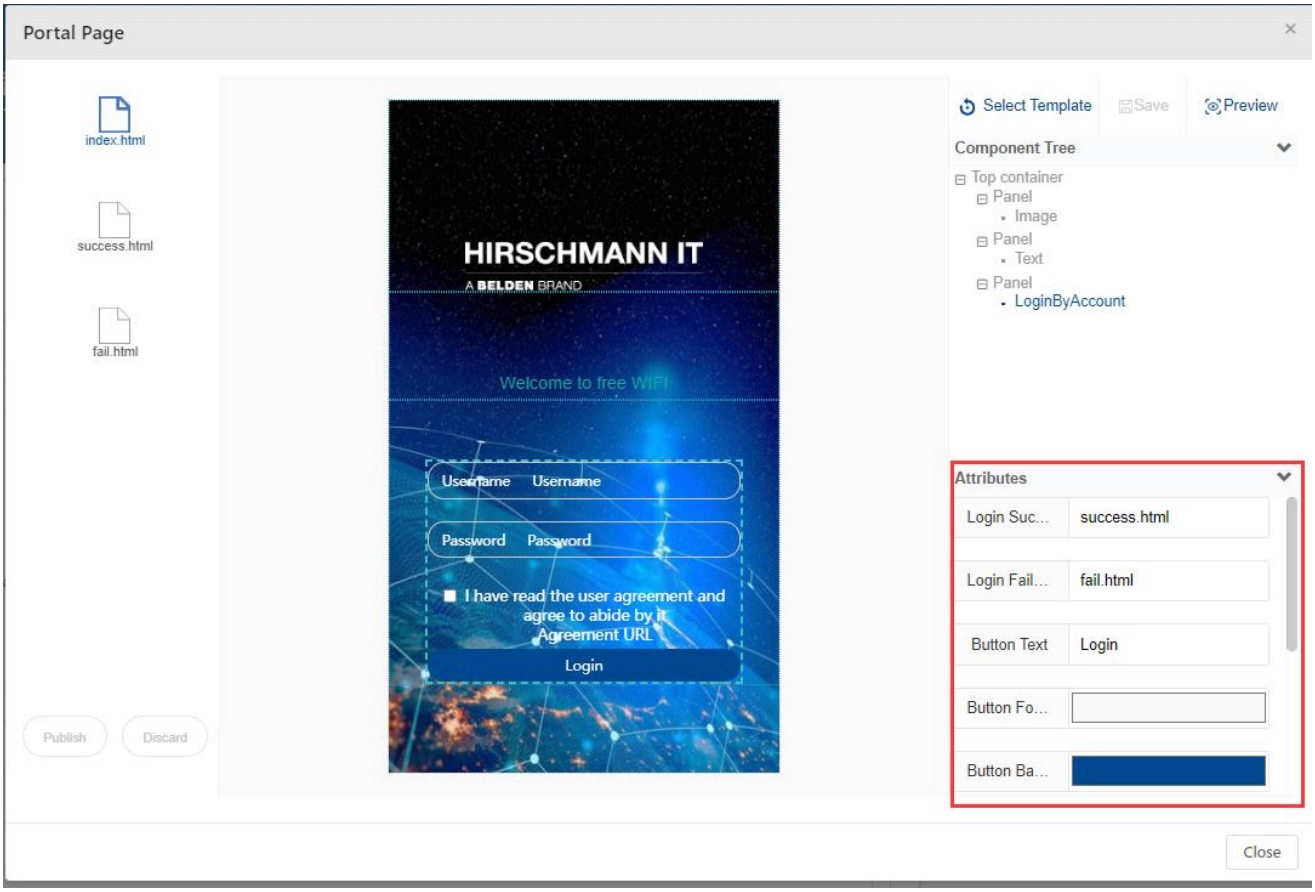


图 239：表单组件属性

13 术语表

13.1 缩写表

A		
AAA	Authentication, authorization, accounting	身份验证、授权、计费
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
B		
BLE	Bluetooth Low Energy	低功耗蓝牙
BSS	Basic Service Set	基本服务集
BSSID	Basic Service Set Identifier	基本服务集标识符
C		
CLI	Command-Line Interface	命令行界面
D		
DAC	Dragonfly Access Controller	Dragonfly 无线控制器
DAP	Dragonfly Access Point	Dragonfly 无线接入点
DCM	Dynamic Client Management	动态客户端管理
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DNS	Domain Name System	域名系统
DRM	Dynamic Radio Management: automatically manages the DAP working channel and transmitting power.	动态无线电管理：自动管理 DAP 工作信道和发射功率。
DSCP	Differentiated Services Code Point	差分服务代码点
E		
EAP	Extensible Authentication Protocol	扩展认证协议
ESSID	Extended Service Set Identifier	扩展服务集标识符
F		
FQDN	Fully Qualified Domain Name	完全限定域名
G		
GUI	Graphical User Interface	图形用户界面
I		
IDS	Intrusion Detection System	入侵检测系统
IG	Installation Guide	安装指南
IGMP	Internet Group Management Protocol	互联网管理协议
L		
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议

M		
MAC	Media Access Control	媒体访问控制
MIMO	Multiple-Input Multiple-Output	多输入多输出
MQTT	Message Queuing Telemetry Transport	消息列队遥测传输
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
N		
NAT	Network Address Translation	网络地址转换
NTP	Network Time Protocol	网络时间协议
O		
OKC	Opportunistic Key Caching	机会性密钥缓存
OUI	Organizationally unique identifier	组织唯一标识符
P		
PHY	Port Physical Layer	端口物理层
PMD	Post Mortem Dump	算后转储
PMF	Protected Management Frames	保护管理帧
PNAC	Port-based Network Access Control	基于端口的网络接入控制
POE	Power over Ethernet	以太网供电
PPPOE	Point-to-Point Protocol over Ethernet	以太网点对点协议
PVM	Primary Virtual Manager: The virtual manager selected from DAPsaccording to the defined priority will be responsible for an internal portal server, AP, and client management and monitoring.	主虚拟管理器：从 DAP 中选择的虚拟管理器 根据定义的优先级，将负责内部门户服务器、AP 和客户端的管理和监控。
Q		
QoS	Quality of Service	服务质量
QSG	Quick Start Guide	快速入门指南
R		
RADIUS	Remote Access Dial-In User Service	远程认证拨入用户服务
RF	Radio Frequency	射频
RSSI	Received Signal Strength Indicator	接收信号强度指示器
S		
SLB	Smart Load Balance	智能负载均衡
SNMP	Simple Network Management Protocol	简单网络管理协议
SNR	Signal-to-noise ratio	信噪比
SSID	Service Set Identifier	服务集标识符
SVM	Secondary Virtual Manager: The second highest priority in the cluster. When the PVM fails to respond due to an unexpected error or issue, the SVM will automatically upgrade to act as the PVM.	次要虚拟管理器：集群中的第二高优先级。当 PVM 因为意外错误或问题无法响应时，SVM 将自动升级为 PVM。

T		
TCM	Three-Color Marking	三色标记
TCP	Transmission Control Protocol	传输控制协议
TLS	Transport Layer Security	传输层安全
U		
UDP	User Datagram Protocol	用户数据报协议
UNP	User Network Profile	用户网络配置文件
V		
VLAN	Virtual Local Area Network	虚拟局域网
W		
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
WPA3	Wi-Fi Protected Access 3	Wi-Fi 保护接入 3

13.2 UI

2.4G available num	2.4G 频段数量
2.4G Channel	2.4G 频段信道
2.4G Data Frame Rate	2.4G 数据帧速率
2.4G Gain	2.4G 天线增益
2.4G Manage Frame Rate	2.4G 管理帧速率
2.4G Power	2.4G 频段功率
5G All Chain	5G 全频段天线设置
5G All Channel	5G 全频段信道
5G All Gain	5G 全频段天线增益
5G All Power	5G 全频段功率
5G All/5G High/5G Low	5G 全频段/5G 高频段/5G 低频段
5G available num	5G 频段数量
5G Data Frame Rate	5G 数据帧速率
5G High Channel	5G 高频段信道
5G High Power	5G 高频信道功率
5G Low Channel	5G 低频段信道
5G Low Power	5G 低频信道功率
5G Manage Frame Rate	5G 管理帧速率
802.1p mapping setting	802.1p 映射设置
802.1p Priority Level	802.1p 优先级级别
802.1X Authentication	802.1X 验证
A	
Accept	同意
Access Band	无线电频段
Access Clients	接入客户端
Access Code	访问码
Access Device Location	接入设备位置
Access Device MAC	接入设备 MAC 地址
Access Device Name	接入设备名称
Access Key	访问密钥
Access Policy	访问策略
Access Role Profile	访问角色配置文件
Access Strategy	访问策略
Account	账户
Account External Radius	外部 RADIUS 服务器
Account Interim-interval Status	记账间隔状态
Account Name	账户名
Account Type	账户类型
Account Valid Period	账户有效期

Account Validity Period	账户有效期
Accounting Interim Interval	记账间隔
Accounting Port	记账端口
Acct Interim Interval	记帐间隔
Acct Status Type	状态类型
Action	动作
Activate	激活
Activation	激活
Activation Time	激活时间
Active Scanning	主动扫描
AD Port	AD 端口
Add	添加
Add Administrator	添加管理员
Add Group	添加群组
Add to Blocklist	添加到黑名单
Add Unified Policies	添加统一策略
Address	地址
Admin	管理员
Admin Name	管理员名称
Admin Password	管理员密码
administrator	管理员
Advance setting	高级设置
Advertise & Scanner Mode	广播和扫描模式
Advertise Address	广播地址
Advertise Mode	广播模式
Advertise Type	广播类型
Agreement Detail	协议详情
Alert	警报
All	全部
All Devices	所有设备
Allowed Band	可用频段
AllTheTime	全天
Antenna Table	天线列表
AP	接入点
AP Add Client to Blocklist	AP 将客户端添加到黑名单
AP Antenna Config	接入点天线配置
AP Bluetooth	AP 蓝牙
AP Bluetooth Configuration	AP 蓝牙配置
AP Client Authentication Failed	AP 客户端身份验证失败
AP Client Authentication Successful	AP 客户端身份验证成功
AP Device	AP 设备

AP Firmware	AP 固件
AP firmware health	AP 硬件健康
AP Full Scan Mode Switch	AP 全面扫描模式开关
AP health degree	AP 健康程度
AP IP	接入点的 IP 地址
AP Load Distribution	AP 负载平衡
AP Local Firmware Management	AP 本地固件管理
AP Location	AP 设备的位置
AP MAC	AP 的 MAC 地址
AP Model	AP 型号
AP Name	AP 的名字
AP Number	AP 数量
AP online rate	AP 在线率
AP Online Status	AP 在线状态
AP Page	AP 网页
AP Radius Acct Server No Connection	AP RADIUS 记账服务器无连接
AP Radius Acct Server No Connection Clear	AP RADIUS 记账服务器无连接清除
AP Radius Auth Server No Connection	AP RADIUS 身份验证服务器无连接
AP Radius Auth Server No Connection Clear	AP RADIUS 身份验证服务器无连接清除
AP Reporting	AP 报告
AP Status	AP 状态
AP Syslog	AP 系统日志
AP Type	AP 型号
AP Wireless Uplink	AP 无线上行
Apply to Group	应用到 Group
Association AP MAC	与客户端关联的 AP 的 MAC 地址
Association SSID	关联 SSID
Attack Item	攻击项目
Attack Times	攻击次数
Attribute	属性
Auth Resource	身份验证源
Authentication	身份验证
Authentication Port	身份验证端口
Authentication Profile	认证配置文件
Authentication Resource	身份验证来源
Authentication Result Statistic	身份验证结果统计
Authentication Server	身份验证服务器
Authentication Source	认证来源
Authentication Strategy	认证策略、身份验证策略

Authentication Type	验证类型
Authenticator	身份验证器
Authorization management	授权管理
Auto	自动
Automatic device allocation policy	自动设备分配策略
Available bandwidth	可用带宽
Average latency	平均延迟
B	
Back	返回
Background	背景流量
Background Scanning	后台扫描
Backup IP Address	备份 IP 地址
Band Steering	频段控制
Bandwidth contract	带宽协议
Basic setting	基本设置
Batch Creation	批量创建
Batch Import	批量导入
Beacon Mode	信标模式
Behavior	行为
best	最好
Best Effort	尽力传输
BLE advertising	蓝牙低功耗广播
Blocklist	黑名单
Bluetooth	蓝牙
Bluetooth beacon scanning	蓝牙信标扫描
Bluetooth Configuration	蓝牙配置
Bluetooth Reporting Interval	蓝牙消息报告间隔
Bluetooth Wireless Uplink Configuration	蓝牙无线上行配置
Broadcast Channel	广播通道
Broadcast Filter All	所有广播过滤
Broadcast Filter ARP	ARP 广播过滤
Broadcast Frequency	广播频率
Broadcast Key Rotation	广播密钥轮换
Broadcast Key Rotation Time Interval	轮换广播密钥的间隔
Broadcast Power	广播功率
Building ID	建筑物 ID
Button Background Color	按钮背景色
Button Font Color	按钮字体颜色
Button Text	按钮文本
C	
cancel	取消

Captive Portal Authentication	强制门户身份验证
Certificate	认证
Chain	天线配置
Change password	修改密码
Channel	信道、工作信道
Channel DRM	DRM 信道
Channel List	信道列表
Channel Setting	信道设置
Channel Width(MHz)	信道宽度
Character	角色
Client	客户端
Client health degree	客户端健康程度
Client IP	客户端 IP 地址
Client Isolation	客户端隔离
Client MAC	客户端的 MAC 地址
Client Number	客户端数量
Client Type	客户端类型
Clients	客户端
Cold Boot	冷启动
Collection Time	收集时间
Color	文本颜色
color marking	颜色标记
Committed Information Rate	承诺信息速率
Common Information	常用信息
Community	社区
Company	公司
Company Device	公司设备
Condition	条件
Config	配置
Config edit task	配置编辑任务
Configuration Options	配置选项
Configuration Wizard	配置向导
Configuration/Display	配置/显示
Confirm	确认
Confirm Password	确认密码
Confirm Secret	确认密钥
Connecting Times	连接次数
Connection Time	连接时间
Connectivity status	连接状态
Connectivity Testing	连通性测试
Content	文本内容

Corp caption	公司说明
Corp dashboard	公司仪表盘
Corp information	公司信息
Corp name	公司名称
Corp Operation	公司操作
Corporate	公司
count of offline APs (red number)	离线 AP 数量（红色数字）
count of online APs (green number)	在线 AP 数量（绿色数字）
Country/Region	国家/地区
CPU Overrun	CPU 溢出
CPU Overrun Clear	CPU 超限清除
CPU Threshold	CPU 阈值
Create Access Policy	创建访问策略
Create Allowed IP	创建允许的 IP
Create Authentication Strategy	创建身份验证策略
Create Corporate	创建公司
Create Group	创建群组
Create Guest Account	创建访客账户
Create MAC Group	创建 MAC 组
Create policy	创建策略
Create Policy List Wizard	创建策略列表向导
Create Service Group	创建服务组
Create Site	创建站点
Create WLAN	创建 WLAN
Critical	严重
Current Intrusive AP	当前入侵 AP
Current Intrusive Client	当前入侵客户端
Current version	当前版本
Custom	自定义
Custom Portal Page	自定义登录页
Custom WLAN work schedule	自定义 WLAN 工作周期
Customization	自定义
Customization Page	自定义页面
Customization Portal Page	自定义门户页面
Customization Upgrade	自定义升级
D	
Daily	每日
Dashboard	仪表盘
Data Type	数据类型
Date & Time	日期和时间
Date/Time	日期/时间

Days/Months	日/月
Debug	排错
Default	默认
Default Access Role Profile	默认访问角色配置文件
Default Policy List	默认策略列表
Delete	删除
Department	部门
Description	描述、说明
Destination IP Address/Group IP Address	目标 IP 地址/IP 地址组
Destination MAC Address/MAC Group	目标 MAC 地址/MAC 地址组
Destination Port Range	目的端口范围
Detail	详细信息
Detect 802.11 40MHZ Intolerance Setting	检测 802.11 40MHZ 不耐受设置
Detect Active 802.11n Greenfield Mode	检测活动的 802.11n Greenfield 模式
Detect Adhoc Networks using Valid SSID	检测使用有效 SSID 的 Adhoc 网络
Detect AP Impersonation	检测 AP 扮演者攻击
Detect AP Spoofing	检测 AP 仿冒攻击
Detect Broadcast De-authentication	检测广播解除认证
Detect Broadcast Disassociation	检测广播解除关联
Detect DHCP Client ID	检测 DHCP 客户端 ID
Detect DHCP Conflict	检测 DHCP 冲突
Detect DHCP Name Change	检测 DHCP 名称更改
Detect Invalid Address Combination	检测无效地址组合
Detect Long SSID	检测长 SSID
Detect Long SSID At Client	在客户端检测长 SSID
Detect Malformed Frame-Assoc Request	检测畸形帧关联请求请求
Detect Null Probe Response	检测空探测响应
Detect Omerta Attack	检测 Omerta 攻击
Detect Reason Code Invalid of De-authentication	检测无效原因代码取消认证
Detect Reason Code Invalid of Disassociation	检测无效原因代码解除关联
Detect Rogue SSID Keyword	检测恶意 SSID 关键字
Detect Too Many Auth Failure Request	检测多次认证错误请求
Detect Unencrypted Valid Client	检测未加密的有效客户端
Detect Valid Client Misassociation	检测有效客户端误关联
Detect Valid SSID	检测有效 SSID
Device Category	设备类别

Device Family	设备系列
Device IPv4	设备的 IPv4 地址
Device IPv6	设备 IPv6 地址
Device MAC	设备 MAC 地址
Device Name	设备名称
Device Network Type	设备网络类型
Device OS	设备操作系统
Device Specific PSK	设备特定预共享密钥
Device Type	设备类型
Device Validity Period	设备有效期
Device Validity Unit	设备有效期单位，分钟或天
Devices with Bluetooth	带蓝牙的设备
Devices with WLAN	带 WLAN 的设备
Disabled	禁用
Display Options	显示选项
Downlink	下行
Downstream Bandwidth	下行带宽
Downstream Burst	下行突发流量
Drop	丢弃
DSCP mapping settings	DSCP 映射设置
Dynamic Load Balance	动态负载均衡
E	
Edit	编辑
Edit Access Role Profile	编辑访问角色配置文件
Edit Allowed IP	编辑允许的 IP
Edit Location Policy	编辑位置策略
Edit MAC Group	编辑 MAC 组
Edit Page	编辑页面
Edit Period Policy	编辑时间策略
Edit Policy List	编辑策略列表
Edit SNMP	编辑 SNMP
Edit WLAN	编辑 WLAN
Effect Now	立即应用
Effective Date	生效日期
Email	电子邮件
Email Account	电子邮件账户
Email Password	电子邮件密码
Email Server Test	电子邮件服务器测试
Email/Account	电子邮件/账户
Emergency	紧急
Employee	员工

Employee Access	员工接入
Employee Access Strategy	员工接入策略
Employee Account	员工账户
Empty Value	空值
Enable	启用
Enable SSID	启用 SSID
Enable/Disable	启用/禁止
Encryption Mode	加密模式
Encryption Type	加密类型
End Time	结束时间
Enter Password	输入密码
Enterprise	企业级别
Error	错误
Existing Policies Table	现有策略表
Existing Unified Policies Table	现有统一策略表
Expiration Time	到期时间
Expire Time	到期时间
Expiry Time	到期时间
Export All Device	导出所有设备的信息
Export to CSV	导出为 CSV 文件
External LADP/AD	外部 LADP/AD
External LDAP/AD	外部 LDAP/AD
External Radius	外部 RADIUS 服务器
F	
fail	失败
Failed	失败
fair	一般
Fallback to Site Antenna Configuration	回退到站点的天线配置
Fallback to Site RF Configuration	回滚到站点射频配置
File Download	文件下载
File Name	文件名
File Size	文件大小
Filter	过滤器
Firmware	固件
Firmware Description	固件描述
Firmware Version	固件版本
First Login Time	首次登录时间
Fixed Access Role Profile	固定访问角色配置文件
Fixed Policy List	固定策略列表
Flash Clear	闪存超限清除
Flash Overrun	闪存溢出

Flash Threshold	闪存阈值
Font Family	字体系列
Font Size	字体大小
Force Device Specific PSK	强制设备特定预共享密钥
Forgot password	忘记密码
forward	前进
Frame	帧
Framed MTU	封装 MTU
From(Site/Group)	来自（站点/群组）
Full Name	全名
Full Scan Mode	全扫描模式
G	
Gain	天线增益
Get Code	获取验证码
good	较好
Group	群组
Group ID	群组 ID
Group IP Address	IP 地址组
Group List	Group 列表
Group Name	Group 名称
Group Operation	Group 操作
Guest	访客
Guest Access	访客接入
Guest Access Strategy	访客接入策略
Guest Account	访客账户
Guest Account and Device Statistics	访客账户和设备数据
Guest Account Creation Mode	访客账户创建模式
Guest Account Name	访客账户名
Guest Device Browser	访客设备浏览器
Guest Device Category	访客设备类别
Guest Operator	访客操作者
H	
Health	健康级别
Height	高度
help	帮助
Hide SSID	隐藏 SSID
High	高级
Historical statistics	历史统计
Home	主页
I	
IGMP Snooping	监听

IGMP Snooping/ON	监听/启用
Ignore Validity Period in defining Policy Condition	在定义策略条件时忽略有效期
Image	图像
index	索引
Informational	消息
InProgress	进行中
Interfering AP	干扰 AP
Invitation Registration	邀请注册
IP Address	IP 地址
IPv4	IPv4 地址
IPv6	IPv6 地址
J	
Join Corp	加入公司
L	
L3 Roaming	L3 漫游
Last Connection	上次访问
Last Offline Time	上次断开时间
LDAP/AD Attribute Condition	LDAP/AD 属性条件
LDAP/AD Configuration	LADP/AD 配置
LDAP/AD Server	LADP/AD 服务器
License	许可证
License Activation	许可证激活
License code	许可证代码
License ID	许可证的 ID
License management	许可证管理
Link Address	链接地址
Local Database	本地数据库
Location	位置
Location Policy	位置策略
Location Policy Screen	位置策略界面
Log	日志
Log Generation Time	日志生成时间
Log Level	日志级别
Log Snapshot	日志快照
Login by Account	按账户登陆
Login Failed Redirect URL	登录失败重定向 URL
login failure	登录失败
Login Name	登录名
Login Success Redirect URL	登录成功重定向 URL
Logout	登出、注销

Low	低级
Low Score AP	低分 AP
M	
MAC	MAC 地址
MAC Auth	MAC 身份验证
MAC Authentication	MAC 验证
MAC Group	MAC 地址组
Manager	管理者
Manual	手动
Mapping Condition	映射条件
marks	标记
Material Width	材料宽度
Max Auth Failure Times	最大身份验证失败次数
Max Device per Account	单个账户允许连接的最大设备数量
Max Output Rate	最大输出速率
Maximum clients allowed of single AP of this WLAN	此 WLAN 单个 AP 允许的最大客户端数量
Maximum Power(dBm)	最大功率
Medium	中级
Memory Clear	内存超限清除
Memory Overrun	内存溢出
Memory Threshold	内存阈值
Message	消息
Message Setting	消息设置
Minimum Power(dBm)	最小功率
Mode	模式
Model	型号
Monitoring Panel	监控面板
MQTT Connected Duration	MQTT 连接持续时间
MQTT Connected Time	MQTT 连接时间
MQTT Disconnected Time	MQTT 断开时间
Multicast Based Channel Utilization	基于信道利用率的组播
Multicast Optimization	组播优化
My AP Devices	我的 AP 设备
My AP Equipment	我的 AP 设备
My Device	我的设备
N	
Name	姓名、名称
NAS IP	NAS IP 地址
NAS Port	NAS 端口
Neighbor AP Count	相邻 AP 数量

Network Access (Captive Portal) Authentication	网络接入（强制登陆页）验证
Network Type	网络类型
New password	新密码
Next	下一步
Next step	下一步
None	无
Normal Mode	正常模式
Not Support	不支持
Notice	注意、通知
NTP Config	NTP 配置
NTP Server	NTP 服务器
NTP Server address	NTP 服务器地址
NTP Server List	NTP 服务器列表
Number of Clients	客户端数量
O	
Object Class	对象类
OFF	关闭
Offline Time	断开连接时间
Old password	旧密码
ON	打开
Online	在线
Online Duration	在线时长
Online Time	在线时间
Open	开放级别
operate	操作、操作信息
Operating System	操作系统
Operation tools	操作工具
Operator	操作者
Optional	允许
Other	其他
Owner	所有者
P	
Package loss rate	丢包率
Page attributes view	页面属性视图
Page selector	页面选择器
Page view	页面视图
Parameter Mapping	参数映射
Passive Scanning	被动扫描
Password	密码
Password Attribution	密码属性

Peak Information Rate	峰值信息速率
Period Policy	时间策略
Permission	权限
Personal	个人级别
Personal settings	个人设置
PHY_DOWN	物理层下行数据的速率
PHY_UP	物理层上行数据的速率
PMF-Protected Management Frames	受保护管理帧
Policies Screen	策略界面
Policies Set Condition	策略设置条件
Policies Validity Period Screen	策略有效期界面
Policy List	策略列表
Policy List Screen	策略列表界面
Port	端口
Port(s)	端口
Portal Page URL	主页 URL
Portal Type	登录页类型
Position	岗位
Power DRM	功率动态无线电管理
Power Setting	功率设置
Precedence	优先级
Prefer Device Specific PSK	首选设备特定共享密钥
Priority	优先级
Profile Name	配置文件名称
Prompt Message	提示消息
Protocol	协议
Protocol Only	仅协议
R	
Radio Failure	无线失败
Realm	域
Realm IP	域的 IP 地址
Reboot	重启
Receiving number	接收数量
Recover your account	恢复您的帐户
Refresh	刷新
Reject	拒绝
Remembered Device	已记住的设备
Remembered Employee Device	已记录的员工设备
Remote Log Server	远程日志服务器
Remote Log Server Config	远程日志服务器配置
Remote Log Switch	远程日志开关

Repeat Password	重新输入密码
Required	仅允许
Reset	重置
Response Type	响应类型
Retries	重试
Roaming RSSI	漫游 RSSI 阈值
Rogue AP	恶意接入点
Rogue AP Containment	阻止恶意接入点
Rogue AP Record	恶意接入点记录
Rogue Client Record	恶意客户端记录
Rogue Client/AP	恶意客户端/接入点
Rogue OUI	恶意 OUI （组织唯一标识）
RSSI Threshold	RSSI 阈值
S	
Save	保存
Scan Filter	扫描过滤器
Scan Interval	扫描间隔
Scan QRCode by Employee	员工扫描二维码
Scan Type	扫描类型
Scan Window	扫描时长
Scanner Mode	扫描模式
Scanning AP	扫描 AP
Scanning Channel	扫描信道
Scanning Client MAC	扫描客户端 MAC
Scanning Duration	扫描持续时间
Scanning Interval	扫描间隔
Scene	场景
Scoring grades	得分
Search	搜索
Search Base	搜索基准
Secret Key	密钥
Security	安全、安全级别
Security Level	安全级别
Security setting	安全设置
Select Template	选择模板
Send number	发出数量
Serial Number	序列号
Server address	服务器地址
Server Name	服务器名称
Server Type	服务器类型
Service	服务

Service Group	服务组
Service Port	服务端口
Service Switch	服务开关
Service Type	服务类型
Session ID	会话 ID
Session Start	会话开始
Session Timeout	会话超时
Session Timeout Interval	会话超时间隔
Session Timeout Status	会话超时状态
Set Action	设置操作
Set Condition	设置条件
Set Lines to Display/Page in the List	设置每页列表要显示的行数
Set Site	设置站点
Setting	设置
Severity	严重等级
Shared Secret	共享密钥
Short GI	短保护间隔
Show Advanced Attribute Selection	显示高级属性选择
Show Basic Attribute Selection	显示基本属性选择
Show history reset reason	显示历史重启原因
Show history syslog info	显示历史日志信息
Show system info	显示系统信息
Show WIFI info	显示 Wi-Fi 信息
Signal Strength	信号强度
Signal Strength Threshold	信号强度阈值
Single	单个
Site	站点
Site Antenna Config	站点天线配置
Site Bluetooth	站点蓝牙
Site Bluetooth Wireless Uplink Configuration	站点蓝牙无线上行配置
Site Bluetooth/Fallback	站点蓝牙/回退
Site Health Indication	站点健康指数
Site Reporting	站点报告
Site RF Configuration	站点射频配置
Site Wireless Uplink	站点无线上行
Skip Event	跳转
Smart Upgrade	智能升级
SMS Login	短信登陆
SMTP (Email) Configuration	SMTP 电子邮件配置
SMTP Server	SMTP 服务器

soft boot	软启动
Sort	排序
Source IP Address/Group IP Address	源 IP 地址/IP 地址组
Source MAC Address/MAC Group	源 MAC 地址/MAC 地址组
Source Port Range	源端口范围
SSID Number	SSID 数量
Start Time	开始时间
State/City	省/城市
Station	工作站
Status	状态
Strategy Name	策略名字
Subnet IP/Subnet Mask	子网 IP/子网掩码
success	成功
Support	支持
Switch	开关
Switch Trap-Network	交换机网络信息
System	系统
System Configuration	系统配置
System Syslog	系统日志
T	
Telephone	电话
Test Email	测试邮件
Throughput	吞吐量
Throughput_DOWN	下行数据包的速率
Throughput_UP	上行数据包的速率
Time of Day	每天的时间
Time Zone	时区
Timeout	超时
Timezone	时区
Today's data	今日数据
Top 10 AP with Authentication Failure	具有身份验证失败的前 10 个 AP
Top 10 AP with Authentication Request	身份验证请求排名前 10 的 AP
Top 10 Reason of Authentication Failure	身份验证失败原因排名前 10
TOS Precedence radio	服务类型优先级
Total Traffic	总流量
Traffic	流量
Transfer Site	转移 Site 权限
Trap	陷阱
Trap List	陷阱列表
Trap Server	陷阱服务器

Trap-Authentication	无线身份验证信息
Trap-Hardware	AP 硬件信息
Trap-Network	AP 网络信息
Trap-Security	无线安全信息
Trap-Upgrade	AP 升级信息
Turn Off LED	关闭 LED
Turn Off Telnet	关闭 Telnet
Turn On LED	打开 LED
Turn On Telnet	打开 Telnet
Turn On/Off USB	打开/关闭 USB
Type	类型
U	
Unified Policies	统一策略
Unified Policy List	统一策略列表
Unknown	未知用户
unspecified	未指定
Upgrade	升级
Uplink	上行
Upload	上传
Upload Time	上传时间
Upstream Bandwidth	上行带宽
Upstream Burst	上行突发流量
Use TLS Encryption	使用 TLS 加密
User Access Limit of 802.11b/g	允许客户端以 802.11b/g 模式连接
User Mac	用户的 MAC 地址
User Name	用户名
User name/Email	用户名/电子邮件
"User Protocol Link" Font Color	“用户协议链接”字体颜色
"User Protocol Link" whether or not show	“用户协议链接”是否显示
"User Protocol Link" whether to add Underline	“用户协议链接”是否加下划线
Username	用户名
Username Attribution	用户名属性
V	
Valid AP	有效 AP
Valid Client Associated to a Honeypot AP	与 Honeypot AP 关联的有效客户端
Valid Client Associated to a Rogue AP	与恶意 AP 程序关联的有效客户端
Valid Client Associated to an Interfering AP	与干扰 AP 关联的有效客户端
Valid Client in Ad Hoc Connection Mode	点对点连接模式下的有效客户端

Valid OUI	有效 OUI （组织唯一标识）
Validity Period	有效期
Value	值
Verification code	验证码
Version	版本
Video	视频服务
Viewer	观察者
Vlan Creation	VLAN 创建
Vlan Deletion	VLAN 删除
Voice	语音服务
Voice and Video Awareness	语音和视频感知
W	
Warm Boot	热启动
Warning	警告
Web Authentication	Web 身份验证
Weekday	每工作日
Weekdays	工作日
Weekend	每休息日
Weekends	周末
Whether Support SSL	是否支持 SSL
Whether to Join Blocklist List	是否加入黑名单
Whitelist	白名单
Width	宽度
Wifi Reporting Interval	Wi-Fi 消息报告间隔
Wireless	无线网络
Wireless Blocklist	无线黑名单
Wireless Client Health	无线客户端健康状况
Wireless Uplink	无线上行链路
wizard	向导
WLAN Access Authentication	WLAN 接入认证
WLAN Connection	WLAN 连接
WLAN List	WLAN 列表
WLAN Name	WLAN 网名称
WLAN Timing	WLAN 时间控制
WLAN Work Cycle	WLAN 工作周期
WLAN work schedule	WLAN 工作周期
Work Mode	工作模式
Workgroup Name	工作组名
Working Mode	工作模式
WorkingDay	工作日
Y	

yes	是
Z	
Zip code	邮政编码

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。