浪潮 IAC 系列 多业务无线控制器

配置手册

浪潮思科网络科技有限公司（以下简称“浪潮思科”）为客户提供全方位的技术支持和服务。直接向浪潮思科购买产品的用户，如果在使用过程中有任何问题，可与浪潮思科各地办事处或用户服务中心联系，也可直接与公司总部联系。

读者如有任何关于浪潮思科产品的问题，或者有意进一步了解公司其他相关产品，可通过下列方式与我们联系：

公司网址：　　http://www.inspur.com/

技术支持热线：　400-691-1766

技术支持邮箱：　inspur_network@inspur.com

技术文档邮箱：　inspur_network@inspur.com

客户投诉热线：　400-691-1766

公司总部地址：　山东省济南市历下区浪潮路 1036 号

邮政编码：　　250000

声　明

由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

修订记录

修订日期	修订版本	修订描述
2021 年 6 月	V1.0	1、全新发布，基于 1.061.48 主线版本
2021 年 9 月	V1.1	1、基于 1.076.10 主线版本； 2、WEB 新增“Easy Portal”菜单，用于“免认证，受限访问”时的终端黑白名单配置； 3、WEB 新增“AP 配置”菜单，用于设置 AP 是否关联受控 AC 及面板 AP 的 LAN 口 VLAN 设置； 4、通过“发现 AP”方式添加 AP 时，可选择直接添加 AP 到指定的 AP 分组中； 5、终端用户列表页面，增加 AP 分组筛选菜单，可根据 AP 分组查看； 6、本地转发时可根据组网需要，配置 DHCP 报文进行本地转发还是集中转发； 7、新增常用认证方式配置介绍 8、支持 LDAP 认证（与 AD 域服务器对接）
2021 年 11 月	V1.1.1	典型配置中增加了内外网隔离配置
2022 年 1 月	V1.1.2	支持智联中心 AP
2022 年 4 月	V1.1.3	新增智联中心 AP 组网示例
2022 年 8 月	V1.1.4	1、新增 WEB 统计信息 2、支持 AC WEB 修改 AP ip 地址 3、支持 Portal 认证无流量下线
2023 年 2 月	V1.1.5	1、增加 MESH、WAPI 内容
2023 年 7 月	V1.1.6	1、部分配置项页面布局调整

目　录

1 前言

本文档系统提供了 Inspur IAC 系列多业务无线控制器 WEB 系统功能配置指导。

本文档适用于负责配置和管理 WLAN 的网络工程师。您应该熟悉以太网基础知识，且具有丰富的网络部署与管理经验。

1.1 产品版本

与本文档相对应的产品版本如下所示。

产品名称	软件版本	适用产品型号
Inspur IAC 系列多业务无线控制器	所有版本	IAC6009、IAC6020-E、IAC6050-E、IAC6070-E、IAC6080-E、IAC6090-E、IAC7000-E

1.2 通用格式约定

格式	说明
宋体	正文采用宋体表示。
黑体	一级标题、二级标题、三级标题、。

1.3 图形界面描述格式约定

格式	描述
【 】	代表菜单或子菜单名称
>	代表 WEB 系统配置路径：如【系统对象】>【地址簿】，表示“系统对象”菜单下的“地址簿”菜单
<>	代表窗口中的选项或按钮名称

2 从这开始

2.1 AC 系统概述

为了方便用户对多业务无线控制器的维护和使用，多业务无线控制器内置一个 Web 服务器，与多业务无线控制器相连的终端（以下均以 PC 为例）可以通过 Web 浏览器访问。同时也支持通过 SSH 及串口方式本地连接进行调试和维护。

- 串口方式连接系统需 PC 与 AC 进行本地串口直连；
- Web 和 SSH 方式连接系统的运行环境如下图所示：

2.2 登陆 AC

使用有线连接的 Web 或 SSH 方式登录设备前，需完成以下任务：

- AC 设备的接入端口已配置 IP 地址(有默认 IP 即可)。
- PC 终端和 AC 设备网络互通。
- 设备正常运行，HTTP 服务和 HTTPS 服务已正确配置。
- PC 终端已安装浏览器软件或已安装 ssh 连接的客户端工具。

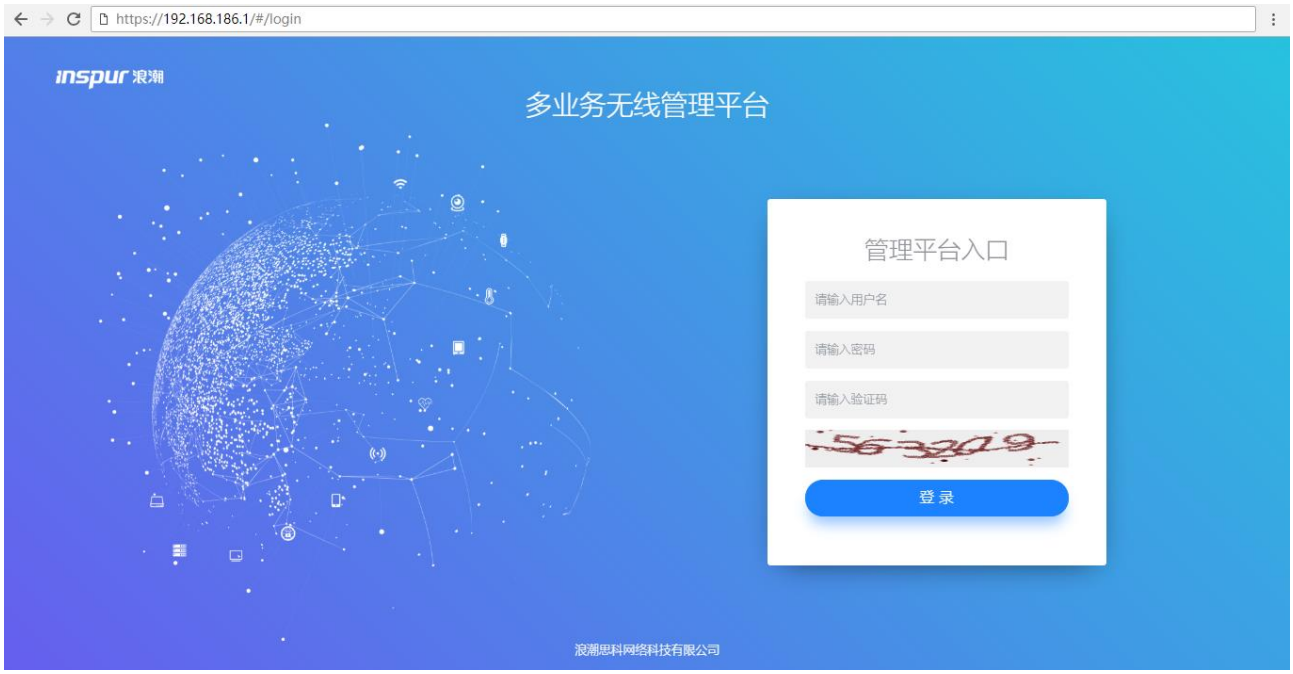
说明：

- IAC6009、IAC6020-E、IAC6050-E、IAC6070-E、IAC6080-E、IAC6090-E、IAC7000-E 出厂时在接口“ **interface vlan1.1** ”（VLAN 1 的接口地址）配置了 IP 地址 192.168.186.1，在所有型号 AC 的物理端口 eth2 及以后的所有电口中缺省已加入 VLAN 1，并默认开启了 DHCP 服务，如 PC 直连时无法获取 IP，则 PC 端需手动配置 192.168.186.0 段的 IP，与 AC 不冲突即可。
- AC 在出厂时已经配置了 SSH 服务，可通过 Shell 工具 SSH 登录至 AC 的命令行。
- 设备在出厂时已经配置了 HTTP 服务和 HTTPS 服务，HTTP 缺省服务端口号为 80，HTTPS 缺省服务端口号为 443。
- 缺省的 Web 和命令行登录账号与密码为 admin/inspur123。

Web 系统的运行环境如下图所示，用户可以使用 PC 通过 Web + 命令行相结合的方式对设备进行管理和配置。

2.2.1登录 AC 的 Web 系统

1、PC 终端打开浏览器软件（以 Google Chrome 为例），在地址栏中输入“http://192.168.186.1”或“https://192.168.186.1”（192.168.186.1 为默认情况下的示例，如有改动，请以实际配置的接入端口 IP 地址为准），按下回车键，显示 Web 系统的登录页面。（**说明：**通过 HTTP 方式登录都会强制跳转到 HTTPS 的登录页面。）如下图所示：



2、输入登录信息。

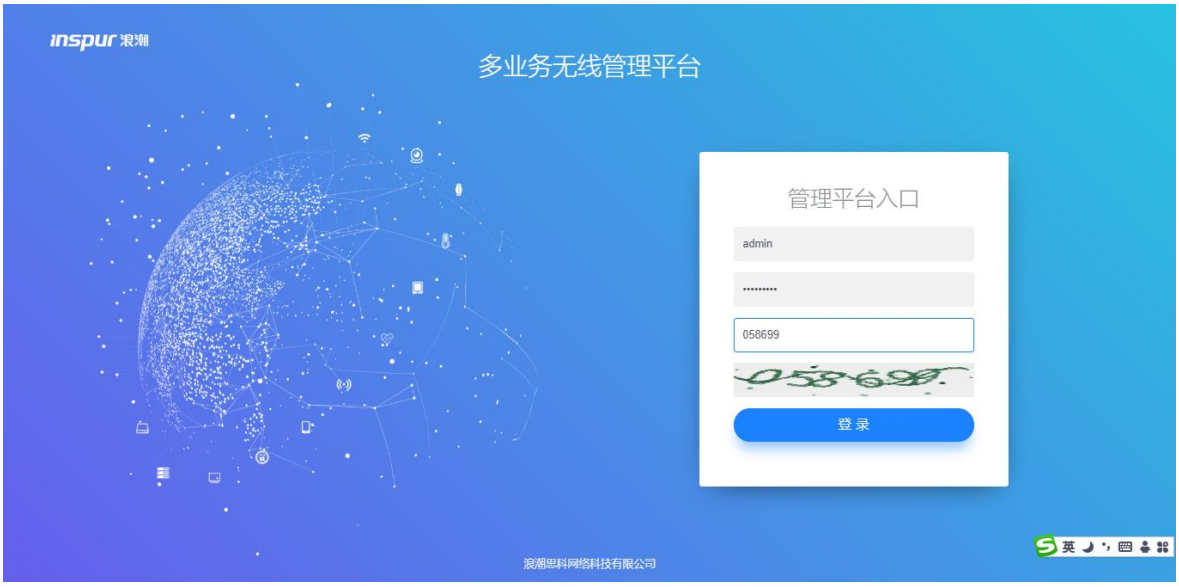
a) 输入登录用户名和密码（默认为：admin/inspur123），以及动态验证码。

b) 单击“登录”，进入操作页面。

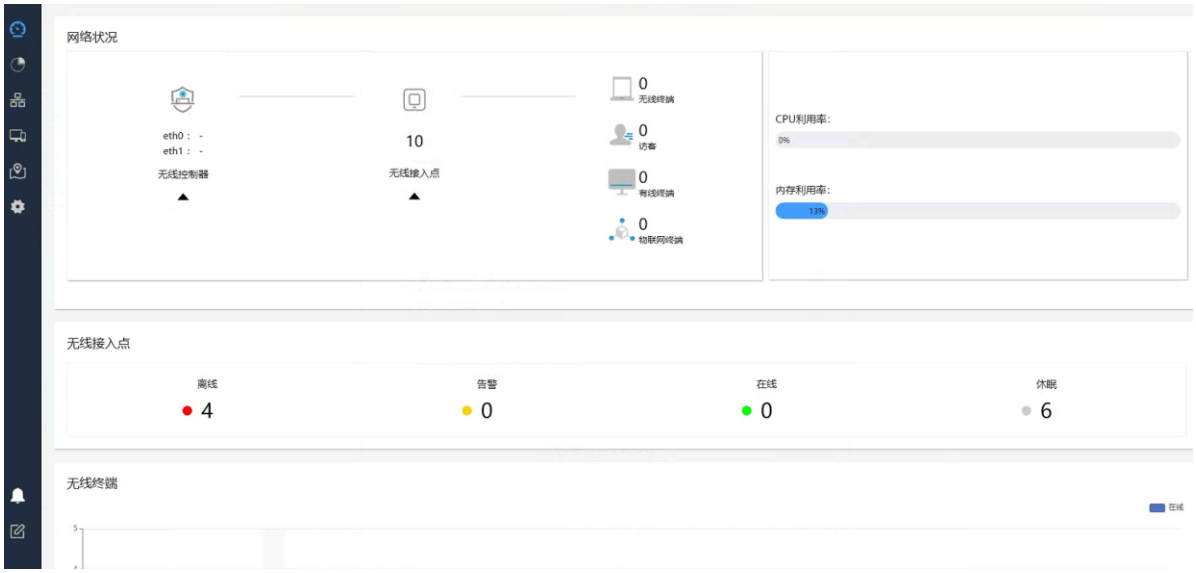
c) 首次登录 Web 系统时，为确保 Web 系统安全性，可先进行密码修改，再退出重新登录。

d) 登录失败时，会提示：“用户名或密码无效”或“验证码错误”，表示输入的用户名或密码或验证码不正确。需核实用户名和密码或刷新验证码然后重新输入。

e) 登录系统过程截图如下所示：



输入登录信息截图



成功登录首页截图

修改账户密码页面截图（成功登录首页→点击右上角<我的账号>按钮）

3、退出当前登录，单击页面右上角的“注销”，重新返回到登录页面。

4、用户登录成功后，在固定时间内未进行任何操作（缺省超时时间为 10 分钟），系统自动注销当前登录，系统会重新返回到登录页面。

2.2.2登录 AC 命令行

2.2.2.1 SSH 登录 AC

1、PC 终端打开支持 SSH 登录的工具软件（这里以 Windows power shell 为例，用户可根据自行习惯进行选择），在 shell 终端输入“ssh admin@192.168.186.1”（192.168.186.1 为默认情况下的示例，如有改动，请以实际配置的接入端口 IP 地址为准），按下回车键，提示输入 admin 账户的密码 inspur123，回车后登录入 AC；登录过程如下所示：

```
Windows PowerShell
版权所有 (C) Microsoft Corporation。保留所有权利。

尝试新的跨平台 PowerShell https://aka.ms/pscore6

PS C:\Users\liangbsh> ssh admin@192.168.186.1
admin@192.168.186.1's password:
 ********************************************************************************
 *     Copyright(c) 2015-2020 Inspur Group Co., Ltd. All rights reserved.       *
 *              Without the owner's prior written consent,                      *
 *        no decompliling or reverse-engineering shall be allowed.              *
 ********************************************************************************

XOS>                                    //新出厂的 AC 系统中 XOS 已调整为 INOP
```

2、AC 命令行下，可根据需要查询不同的命令来查看设备各类状态信息，修改相应配置。

3、用户登录成功后，在固定时间内未进行任何操作（缺省超时时间为 5 分钟），系统自动注销当前登录。需重新进入命令行系统。

2.2.2.2 串口登录 AC

1、打开 PC 上的终端连接工具，例如 SecureCRT，选择对应的 com 口（串口），参数设置如下：

波特率：115200，**数据位**：8，**奇偶校验**：None，**停止位**：1，**流控**：不勾选

2、PC 通过串口线与 AC 前面板 console 口连接后，可看到欢迎信息，如下：

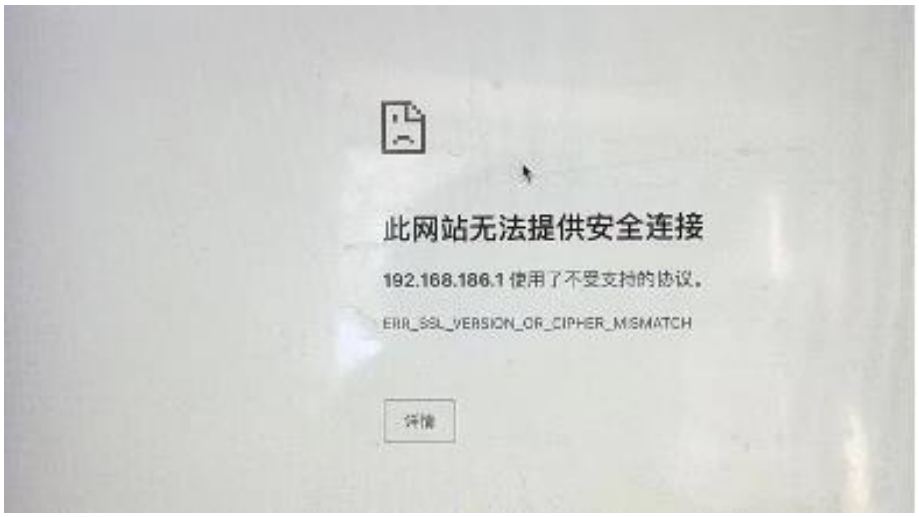
```
login[15310]: root login on 'ttyS0'

*******************************************************************************
*      Copyright(c) 2015-2020 Inspur Group Co., Ltd. All rights reserved.     *
*              Without the owner's prior written consent,                     *
*         no decompliling or reverse-engineering shall be allowed.            *
*******************************************************************************


Please press ENTER
XOS>
```

按照提示按 enter 键后，即可进入系统。

2.3 登录注意事项

2.3.1 使用 AC Web 系统的注意事项

登录 Web 系统建议操作系统为 Windows7.0、Windows10.0。Web 系统可适配市面主流浏览器，推荐使用 Chrome 64.0 以上版本。如遇到下图“此网站无法提供安全连接”的提示，并无法打开 AC Web 界面时，需尽快联系 400 进行指导升级 AC 版本。



2.3.2使用 AC 命令行的注意事项

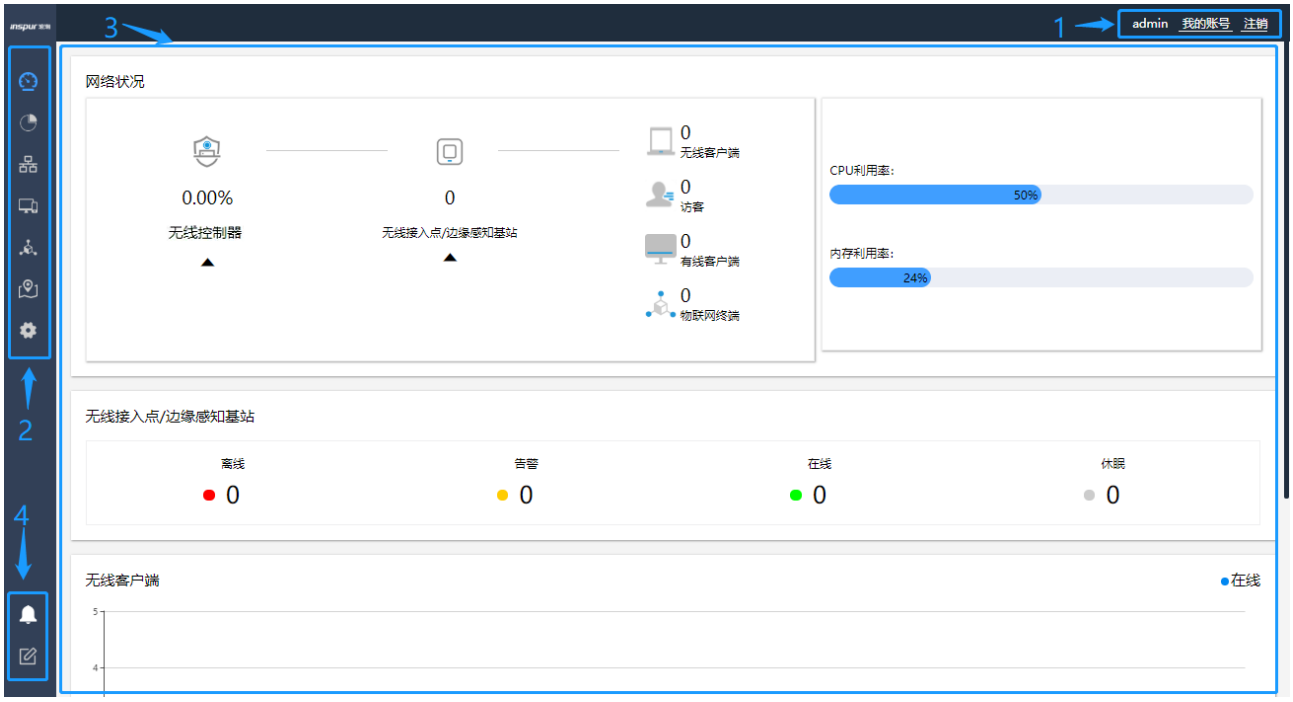
在 Web 系统进行相应功能配置时，需确保命令行中已登录的帐户退出 configure terminal 模式，以保障 Web 配置的顺利下发，否侧可能会出现 Web 已配置，而实际在命令中看不到相应配置内容的情况。

2.4 Web 界面介绍

介绍 Web 界面的主要构成部分与相应的菜单功能。

2.4.1界面区域划分

Web 界面布局，主要包含以下几个区域，如下所示。



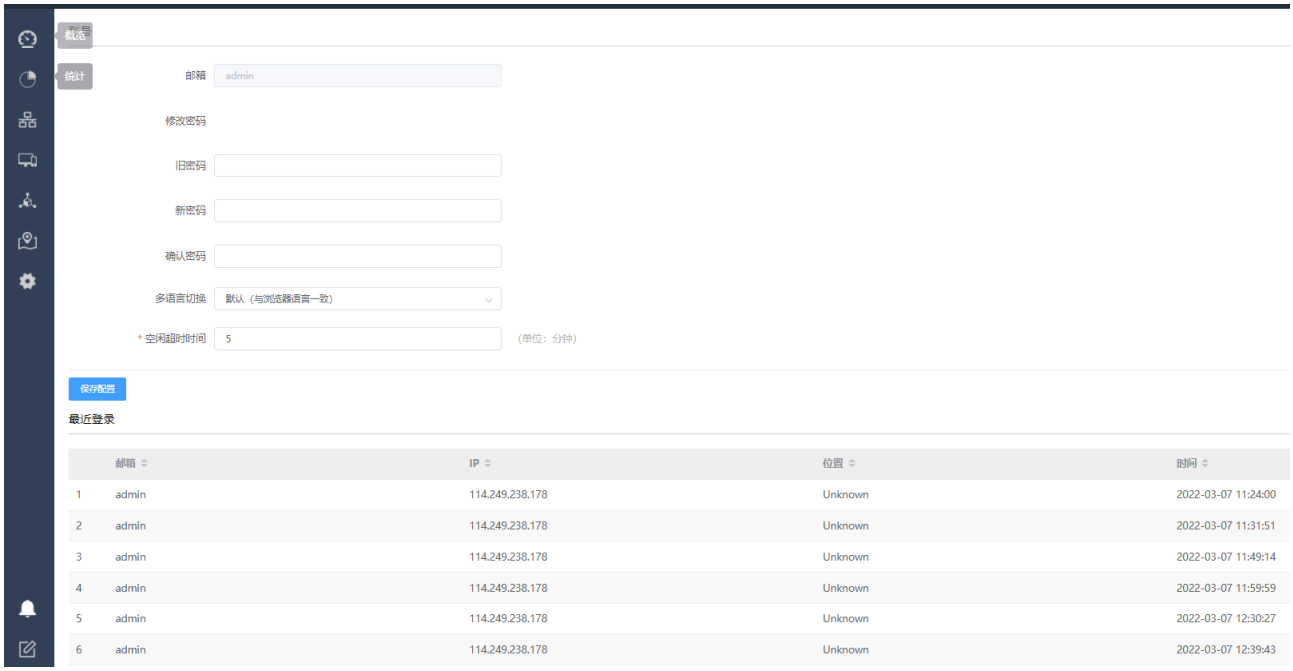
界面区域表：

区域	名称	说明
1	用户登录状态区	用户点击<我的账号>，可快速进行当前登录账号信息修改、账号登录状态查看，点注销可退出登录状态。
2	主要菜单导航	以导航树的模式显示各页签下的具体功能分类。 一级菜单导航位于界面左外侧，二级菜单导航位于界面

		左内侧。
3	功能操作区	用户可在此区域进行具体的功能配置，或者查看功能状态。
4	日志和提示功能区	点日志可查看事件、登录、修改日志，点提示可显示 Web 系统的版本号

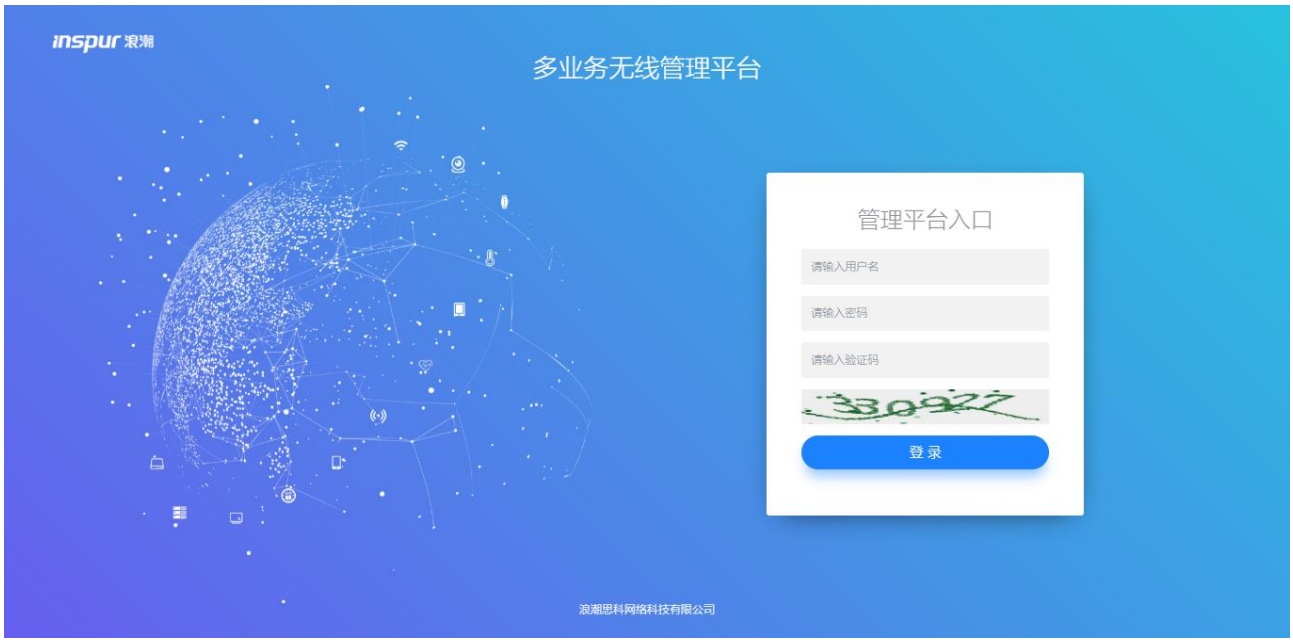
2.4.2 用户登录状态区

1、点击右上角<我的账号>按钮，可查看的信息如下所示：



功能描述：可修改当前账号密码，查看当前账号登录日志，设置空闲超时时间（超时后将退出登录）

2、点击【注销】可返回登录页面，如下所示：

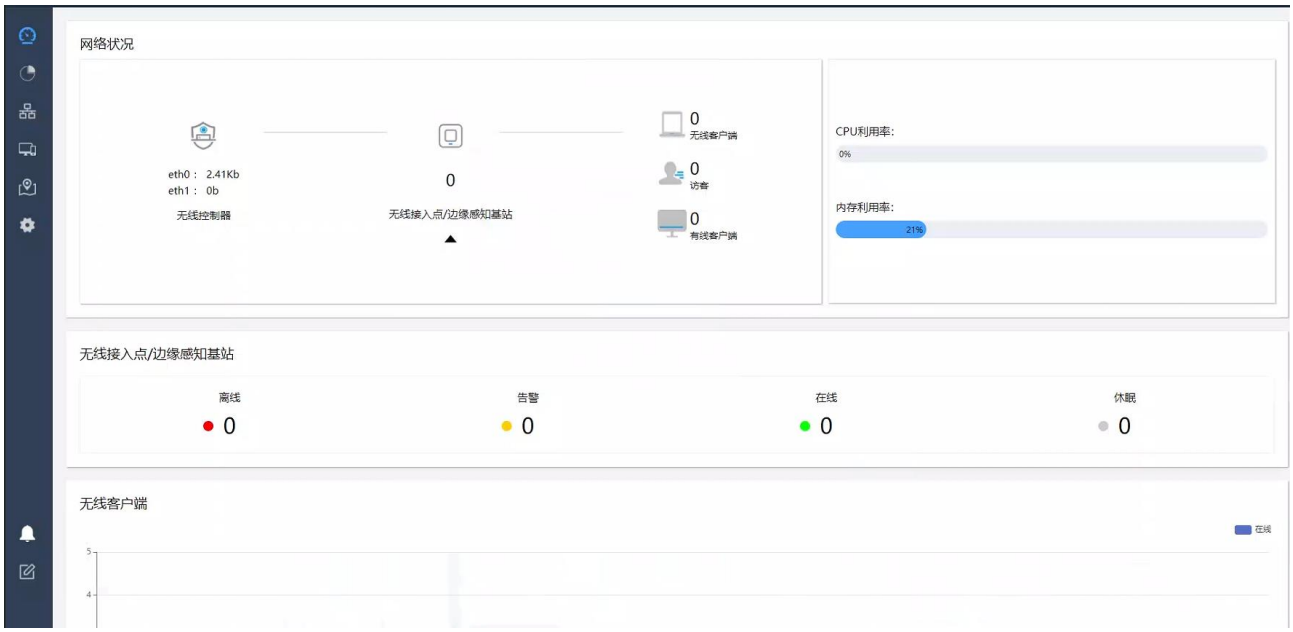


注销后系统将重新返回到用户登录页面。

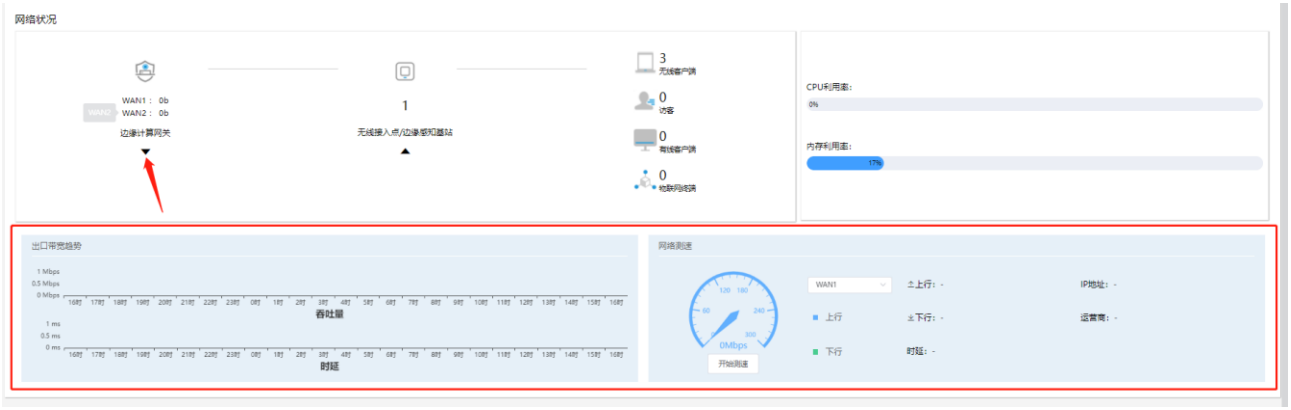
2.4.3 主要菜单导航

2.4.3.1 概览菜单

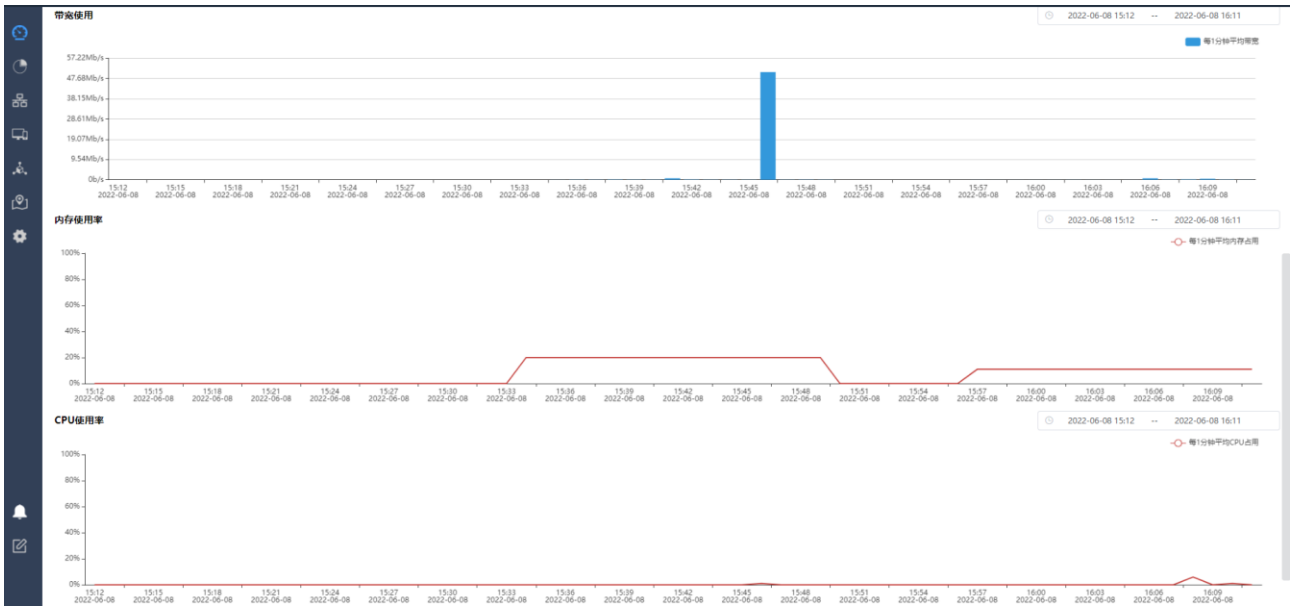
用户成功登录后的系统首页为【概览】菜单，如下图所示：



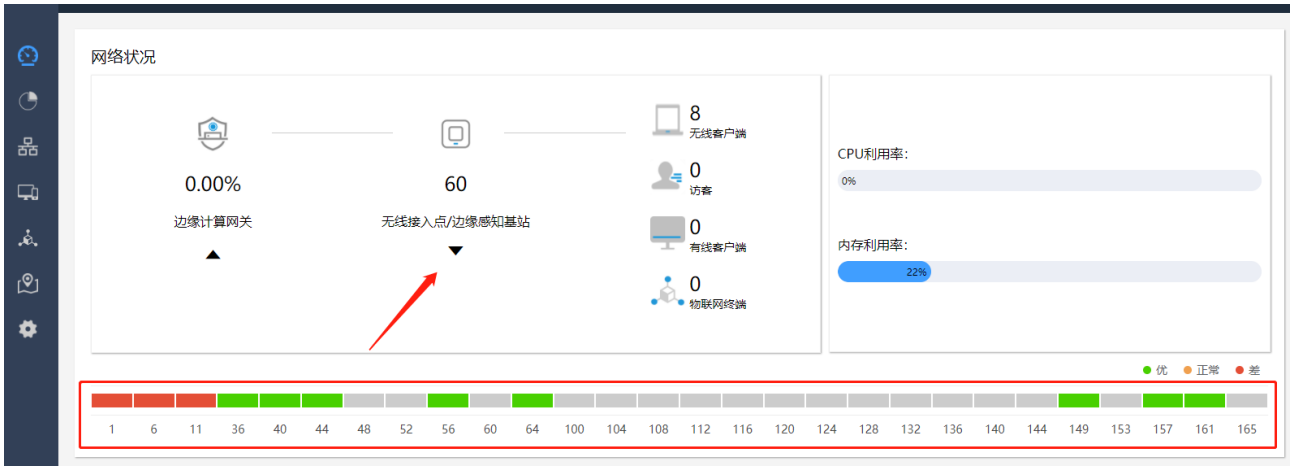
点击“无线控制器”下的三角按钮可查看 WAN 口带宽趋势及 WAN 口测速



通过单击“无线控制器”可进入无线控制器详情页，如下 2 张图所示：



通过单击“无线接入点/边缘感知基站”下的三角按钮可查看信道利用率

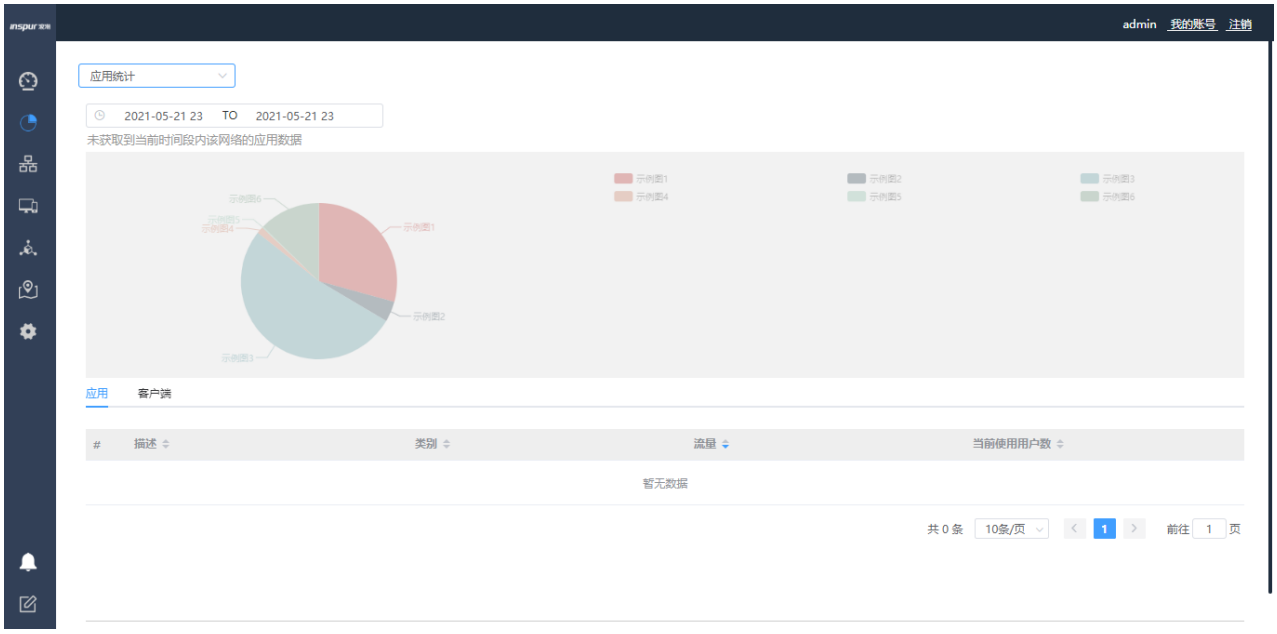


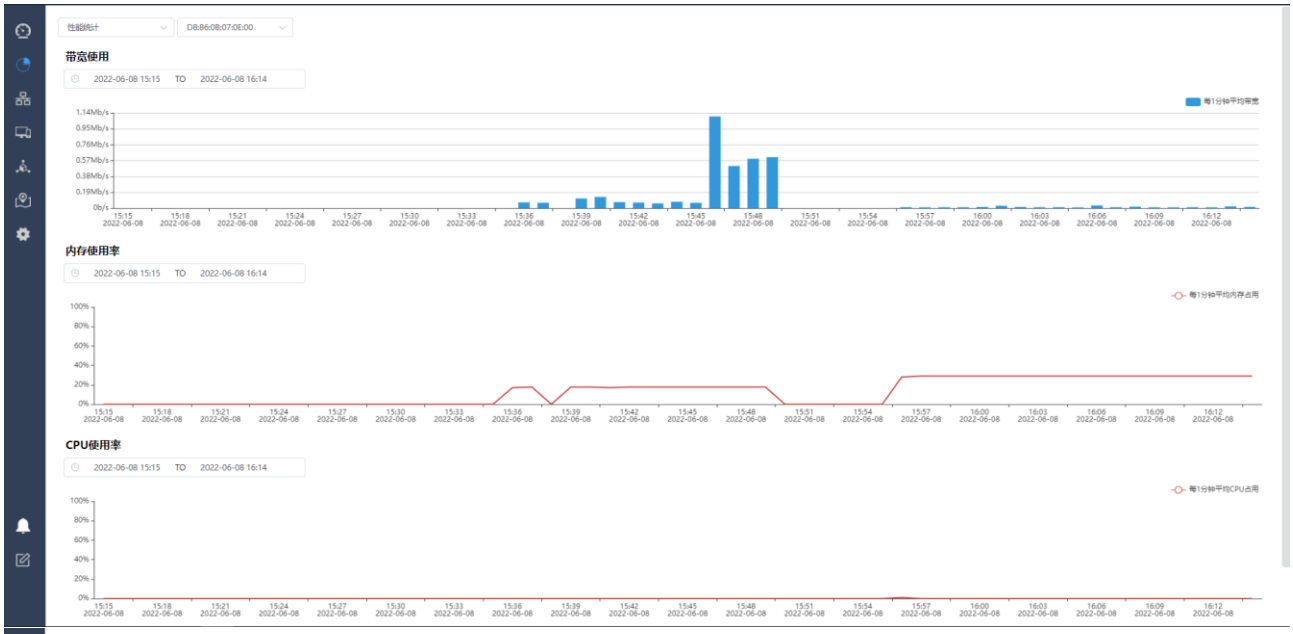
功能描述：通过【概览】菜单可统览系统当前整体状态。包括实时网络流量，CPU、内存利用率，无线接入点/边缘感知基站的状态统计，无线客户端不同时刻在线情况的统计等；

2.4.3.2 统计菜单

点击【统计】菜单，如下图所示：

信道利用率统计图显示当前信道利用率曲线。



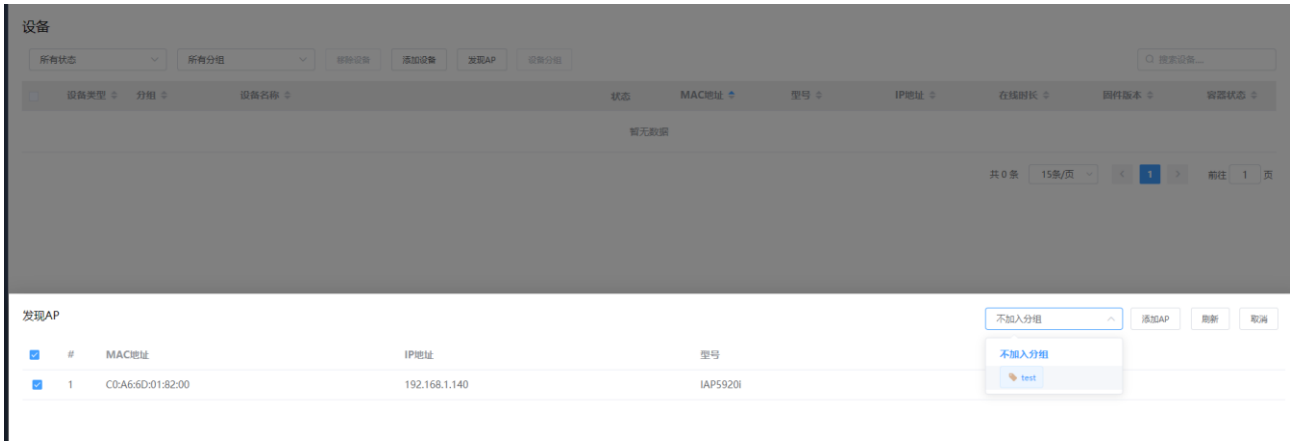


功能描述：通过左上角选项框，可对无线、应用、性能、IDS 等四个维度的相关数据指标进行详细的统计。

具体每个维度统计的具体指标类型可在实际登录时进行细致查看，这里不进行一一赘述。

2.4.3.3 设备菜单

点击【设备】菜单，如下图所示：



功能描述：主要有三项重点功能可在此菜单下进行操作：

1、AP 的添加与删除，在 AP 与 AC 网络连通后，可直接通过<添加设备>功能进行手动添加 AP 设备，或通过<发现 AP>进行自动添加 AP 设备（“发现 AP”方式需要 AC 与 AP 在同一个二层，可选择是否将发现的 AP 加入到分组；智联中心 AP 无法通过发现方式添加，需要在添加设备页面添加，并在智联中心 AP 的 WEB 管理页面手动写入 AC 的 ip 地址或通过 option 43 方式获取 AC 的 ip 地址）；删除 AP 时，可同时选定任意状态的 AP 进行删除操作；

2、AP 的批量升级，上传 AP 升级包后，通过批量选定 AP 进行升级；具体的功能操作将在后续配置示例中进行相应介绍。

3、版本号说明：版本号越大，版本越新。

如：1.029>1.028;

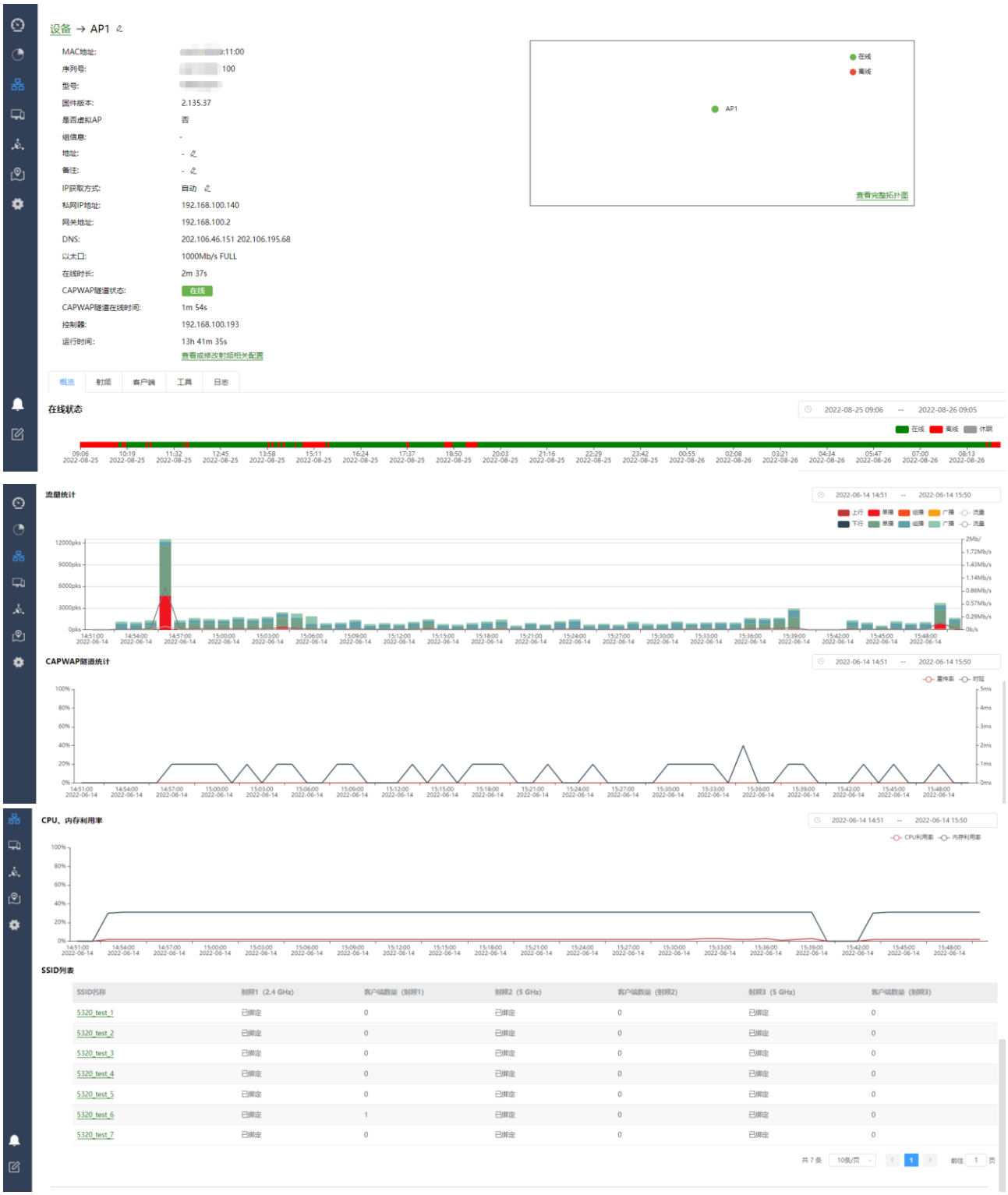
1.029.13>1.029.04;

1.029.13P02>1.029.13

版本名后缀数字前 6 位分别代表年月日，如-210910132923.bin 代表版本发布日期为 21 年 9 月 10 日

4、AP 状态查看，对已添加 AP 列表中，可实时显示 AP 的在线状态，也可通过点击 AP 进入 AP 详情页中查看 AP 的各类详细状态；

AP 的详情页如下：



点击“地址”和“备注“可编辑设备信息”；

点击“IP 获取方式”可配置 AP 的 IP 地址，默认为自动获取地址方式，当“IP 获取方式”选择“静态 IP”时，可为 AP 配置静态 IP。当修改 AP 的 IP 地址后，AP 会短暂离线；

概览页面可查看 AP 在线状态、流量统计、CAPWAP 隧道统计、CPU、内存利用率及 SSID 列表；

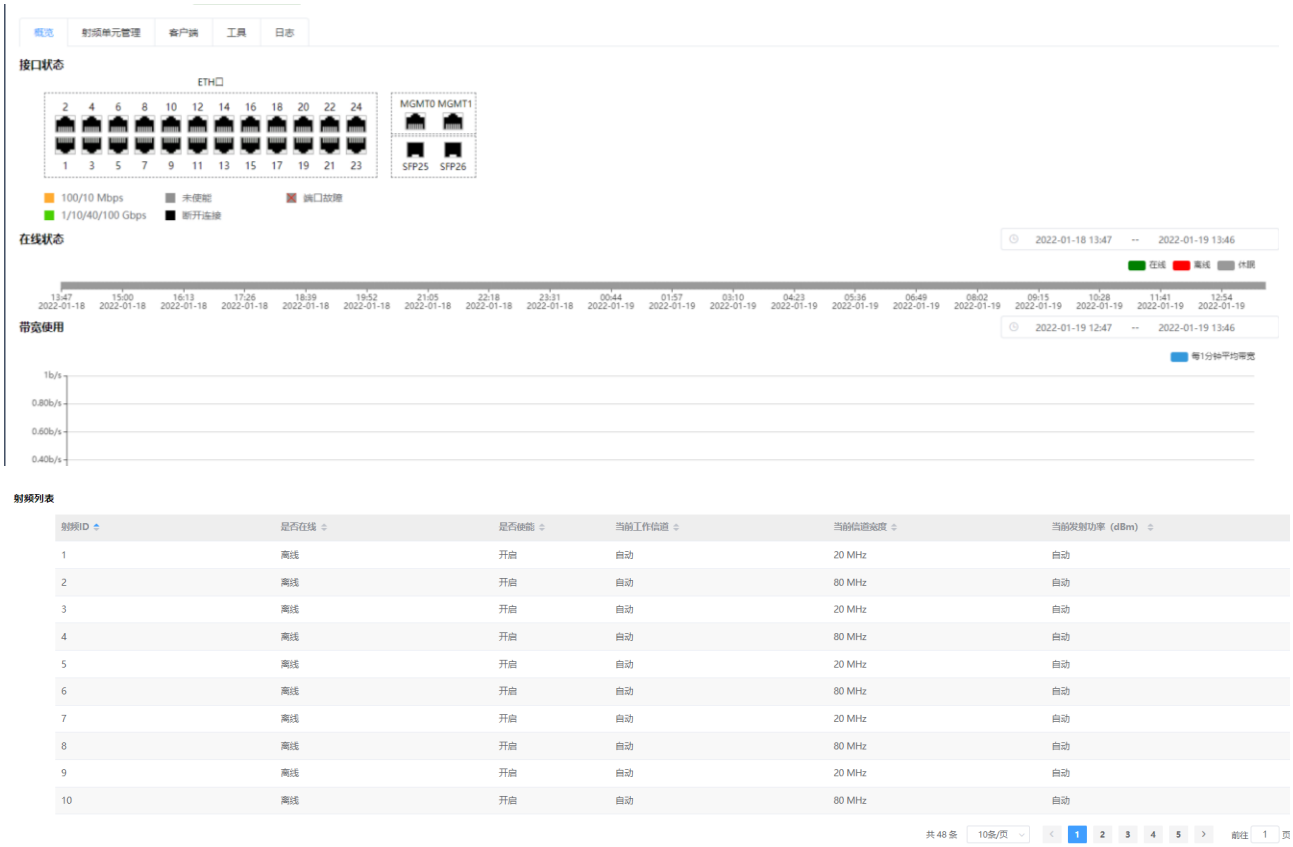
射频页面可查看当前 AP 的射频信息；

客户端页面可查看当前 AP 下关联的客户端信息；

工具页面可进行 ping、重启、远程命令执行等操作；

日志页面可查看当前 AP 日志。

针对智联中心 AP，详情页增加了接口状态和射频单元管理，如下图：

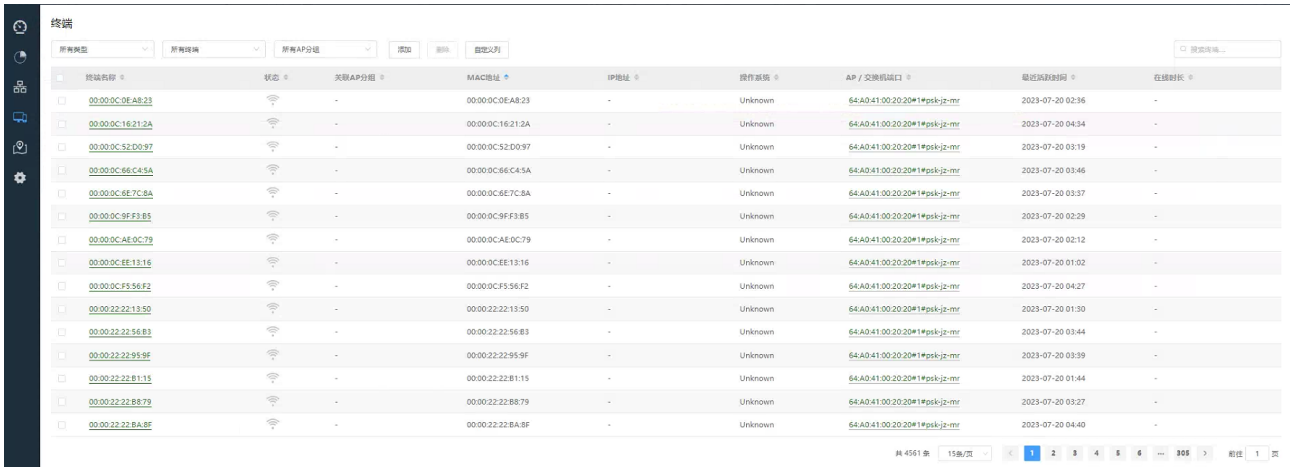


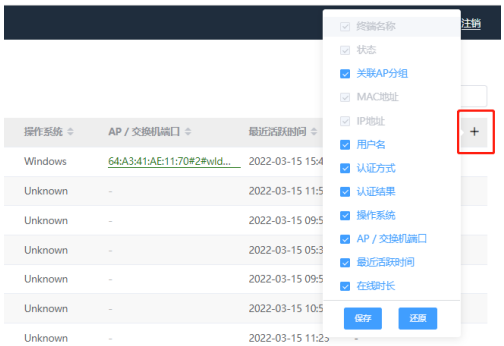
概览页面可查看 AP 接口状态及射频列表；

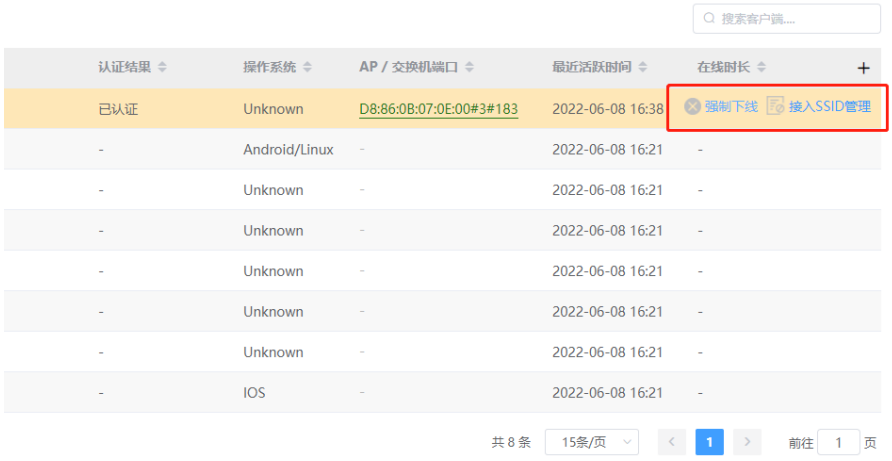
射频单元管理页面可升级对应端口下的智联单元。

2.4.3.4 终端菜单

点击【终端】菜单，如下图所示：







功能描述：所有连接过无线网络的终端设备均可显示在此列表中，能够实时显示终端在线或离线状态；可根据 AP 分组筛选终端，可显示终端关联的 AP 射频单元及 SSID（如 AP/交换机端口列的 64:A3:41:AE:11:70#2#wldapportal，表示终端所关联的 AP MAC 为 64:A3:41:AE:11:70，射频单元为 2，SSID 为 wldapportal），可添加在线终端至黑名单及踢终端下线，客户端列表页支持自定义显示列；

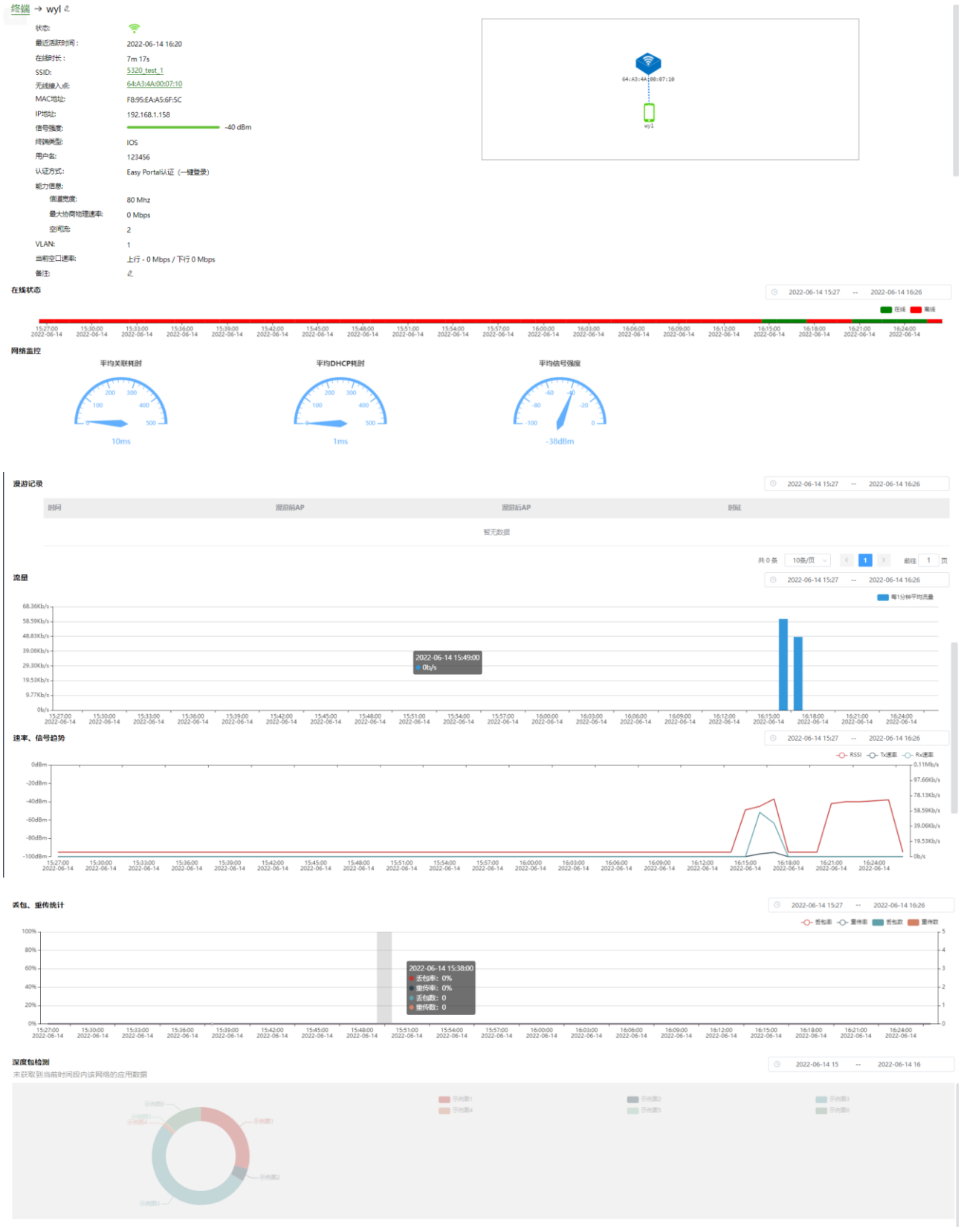
点击右侧的“+”，可自定义要显示的内容；

点击“强制下线”可对选定的无线终端进行强制下线操作；

点击“接入 SSID 管理”可将选定的无线终端加入到 SSID 接入白名单或黑名单。

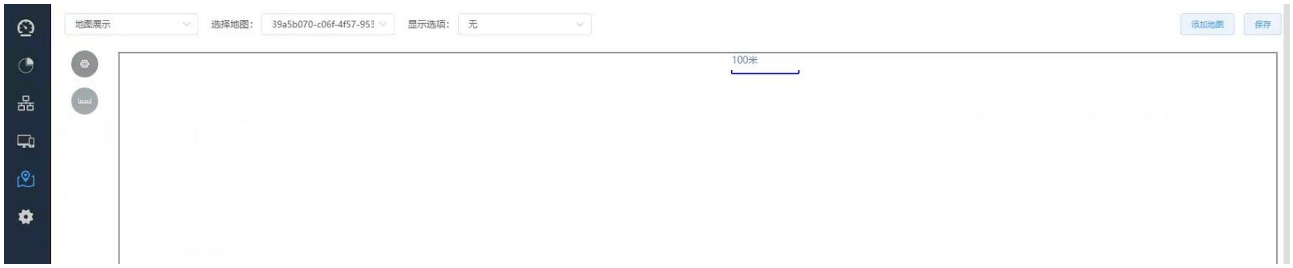
注：“添加”和“删除”按钮仅针对物联网终端设备。

点击【终端】菜单，可进入终端详情页，如下图所示：



2.4.3.5 地图菜单

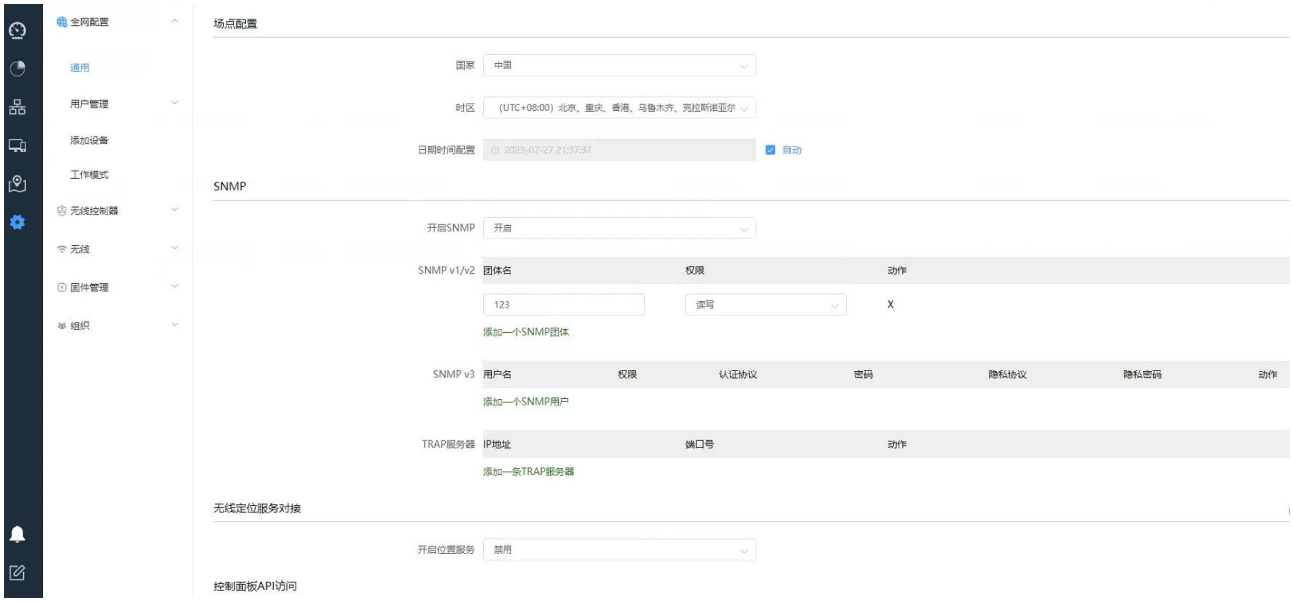
点击【地图】菜单，如下图所示：



功能描述：需深化开发才能完成此功能；

2.4.3.6 设置菜单（业务功能配置菜单）

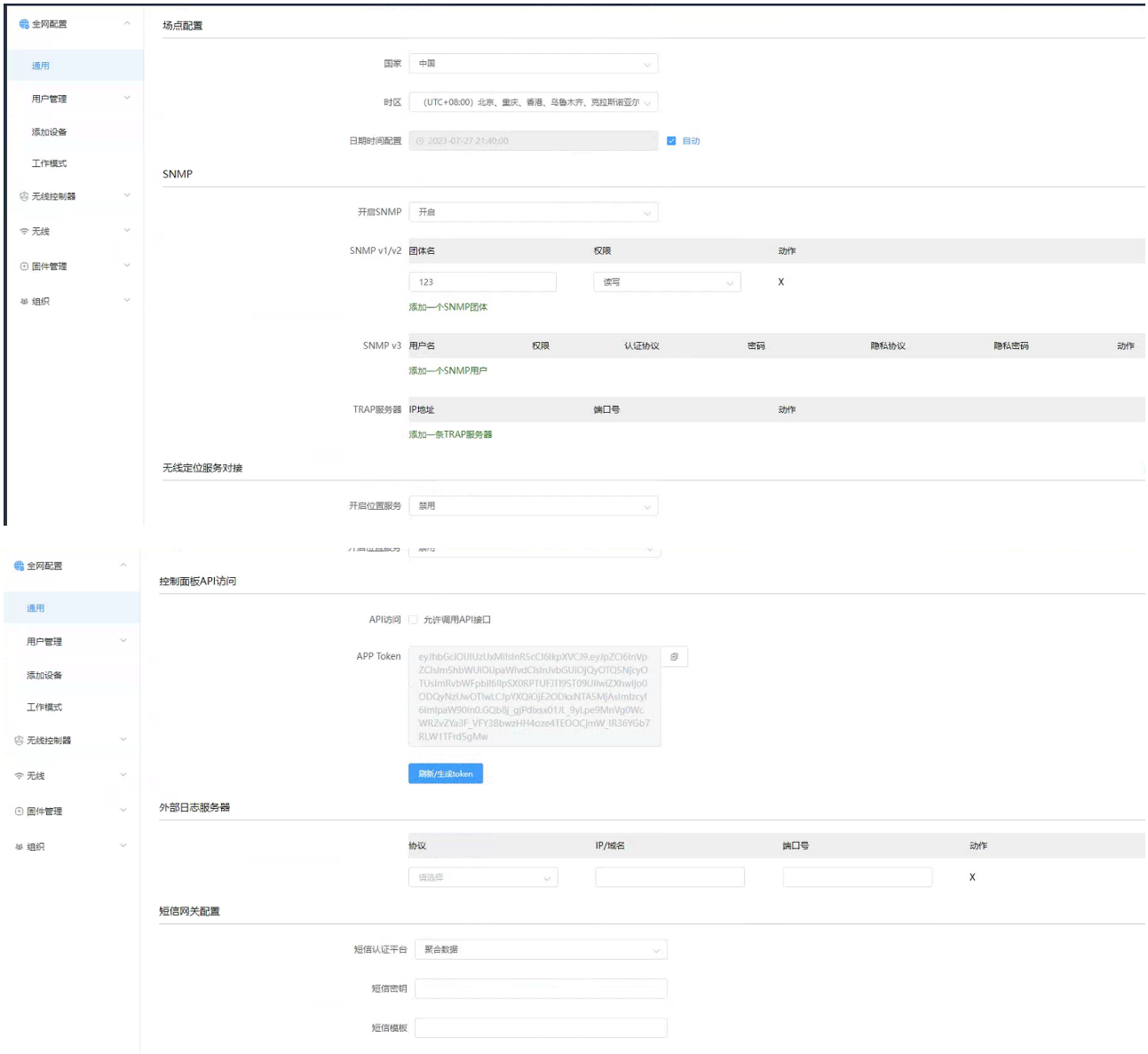
点击【设置】菜单，如下图所示：



功能描述：业务功能的配置几乎都在此菜单中完成，【设置】菜单中包含了有【全网配置】、【无线控制器】、【无线】、【固件管理】、【组织】共五个子菜单。

2.4.3.6.1 全网配置菜单

【通用】菜单-主要功能是 SNMP 以及短信网关等配置，详细内容如下所示：

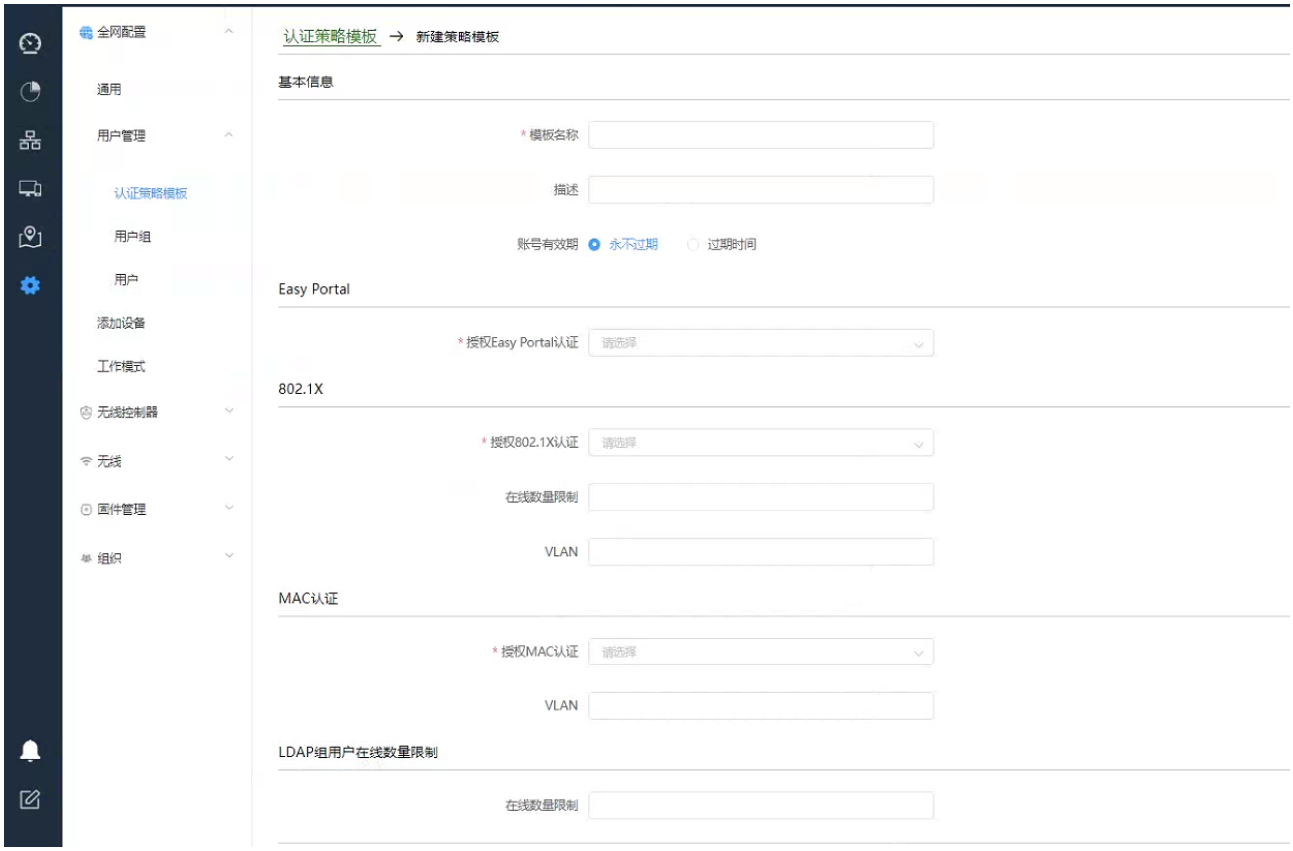


说明：

（1）支持 SNMP v1/v2/v3

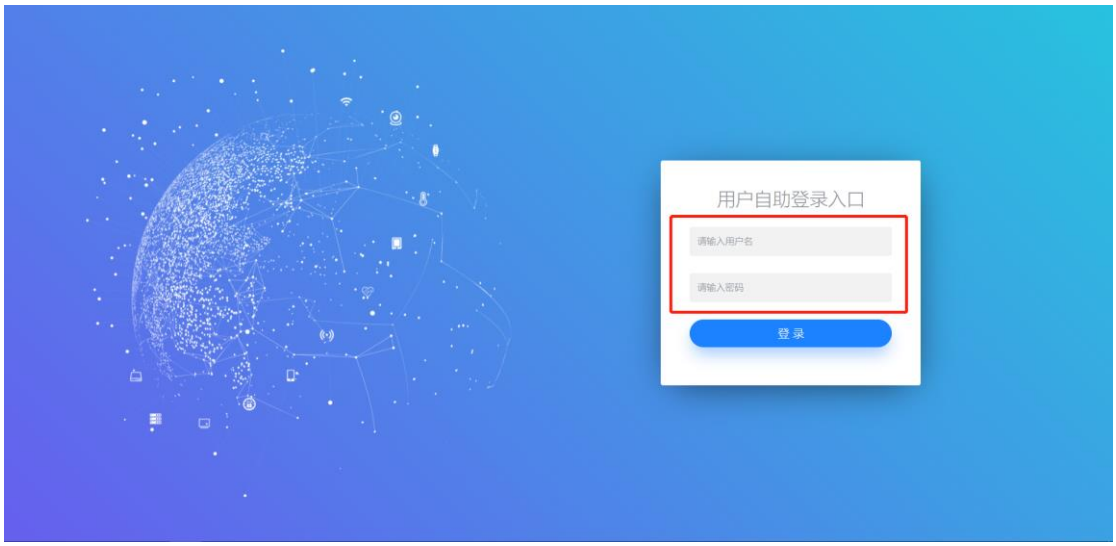
（2）短信认证平台：当前支持聚合数据、亿美软通、企信、移动云 MAS、赛邮·云通信

【用户管理】菜单-主要功能是针对本地 portal、802.1x、mac 认证的用户认证策略模板、用户组、用户的创建及管理，详细配置如下所示：



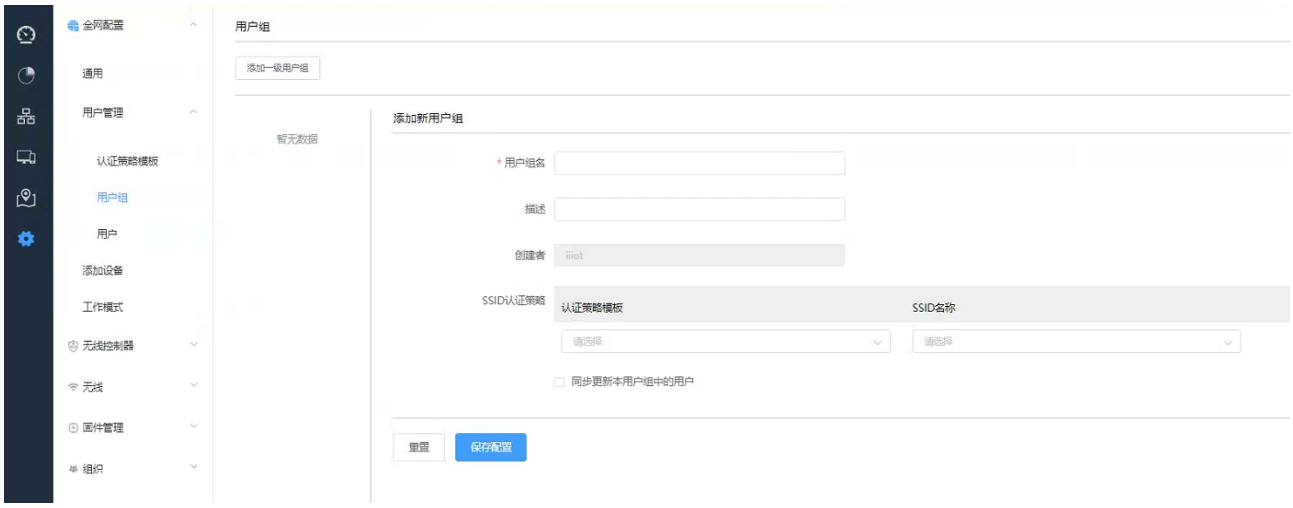
802.1x 认证支持在线数量限制功能，在创建的认证策略模板中，可选择是否授权 Easy Portal、8020.1x、mac 认证，支持 802.1x 认证的用户自主修改账号密码，修改方法：

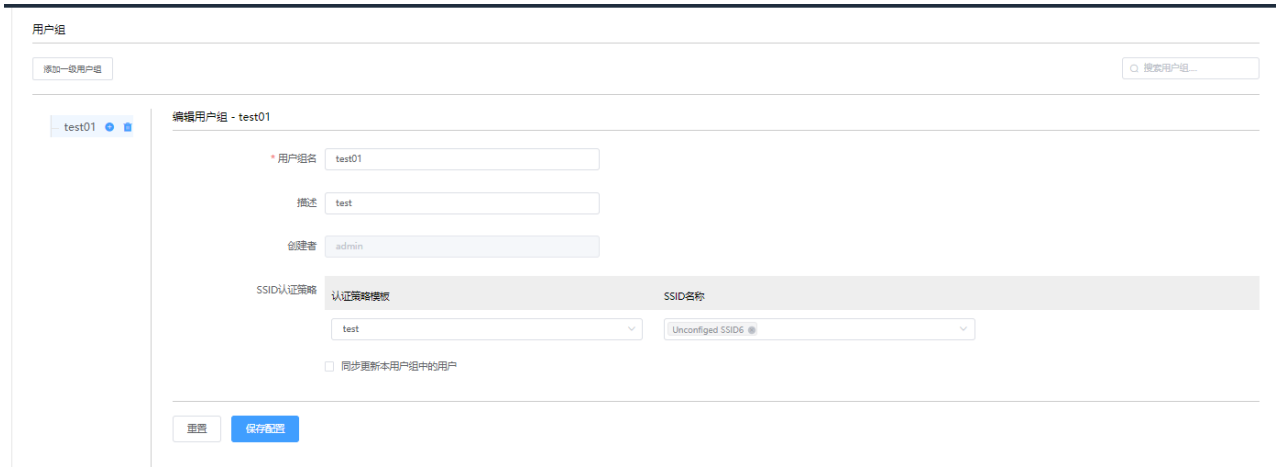
电脑端或手机端浏览器输入地址：http://A.B.C.D/#/localUserLogin?networkname=localhost (A.B.C.D 对应 AC 或云服务器的管理地址；当为云服务器部署时，localhost 改为对应的网络名称，如服务器管理地址为 10.1.6.30，网络名称为 0000，则输入地址为 http://10.1.6.30/#/localUserLogin?networkname=0000)，进入用户自助登录入口，使用个人账号和密码登录，显示如下：



登陆后在输入新密码，点击“保存配置”即可修改成功。

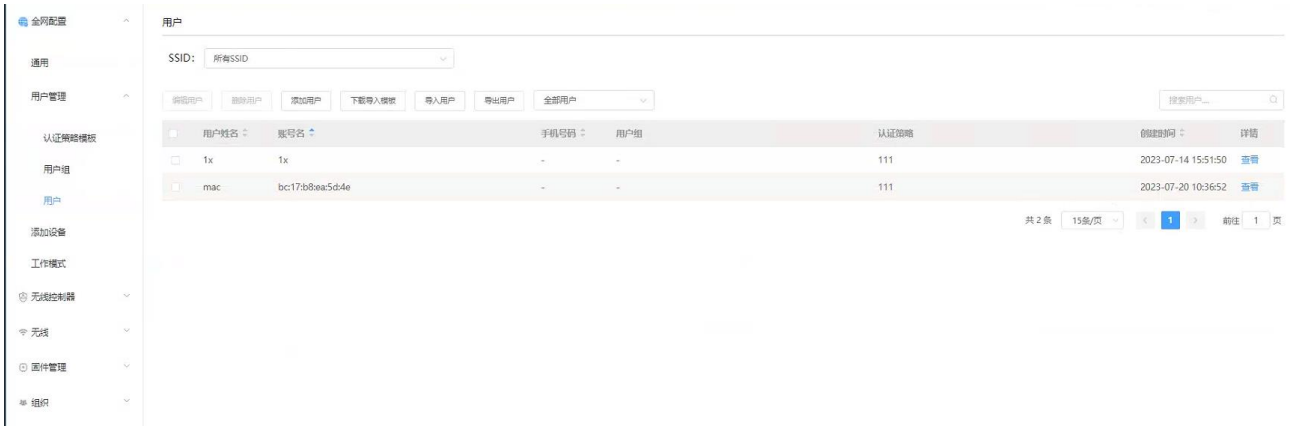
【用户组】页面，可创建用户组，将用户组绑定到认证策略模板及 SSID

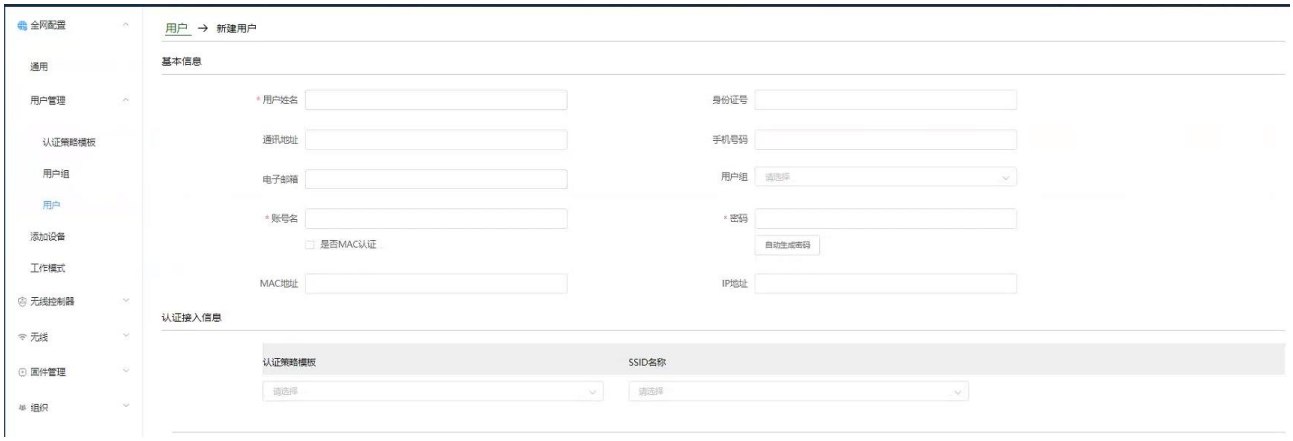




【用户】页面，选择 SSID，可添加单个用户或通过模板批量导入用户

点击<导出用户>可导出当前列表中的所有用户（不包含访客用户，通过访客管理员添加的用户为访客用户）





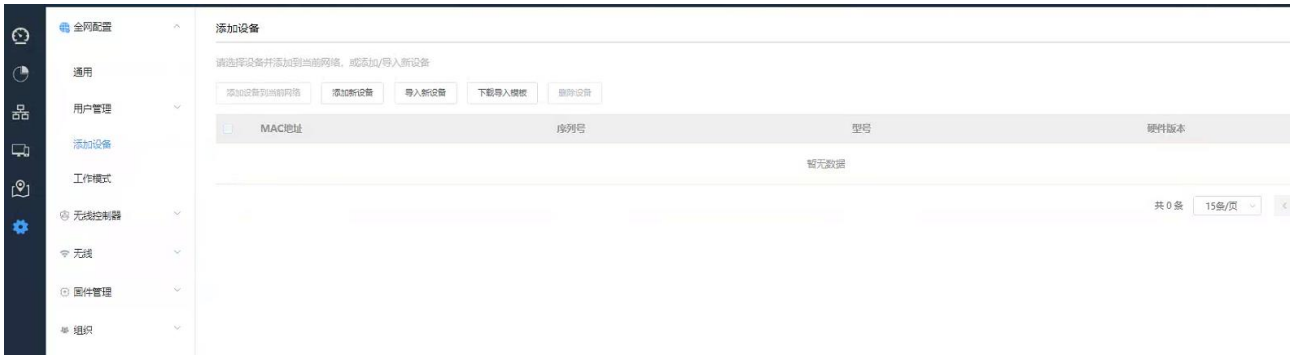
说明：

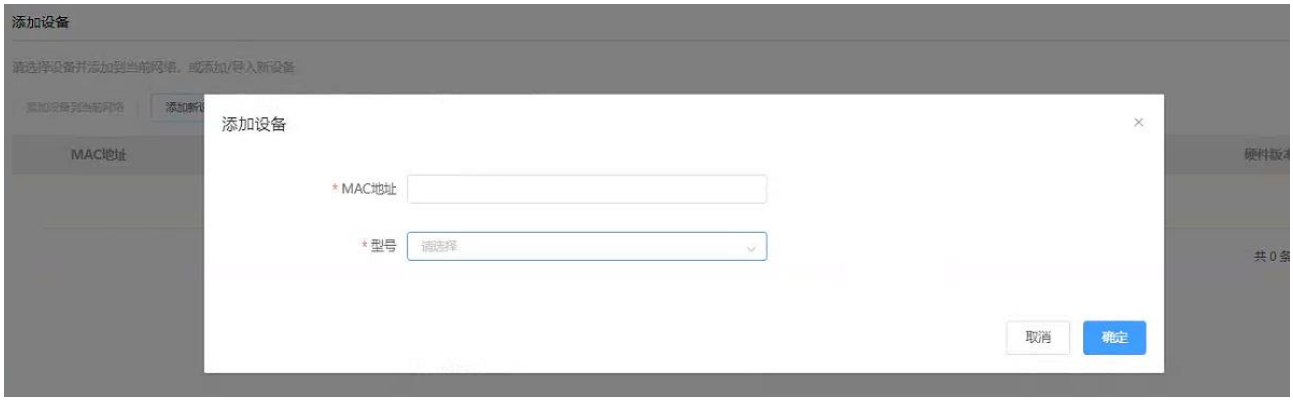
1) 通过模板批量导入用户时，可一次性批量导入 1000 个用户信息，后添加的用户信息会自动追加连接到前面添加的用户信息表面后面，分批导入相互不会覆盖；

2) 通过<添加用户>按扭一个一个添加用户信息时，当勾选“是否 MAC 认证”，用户名格式将变为 mac 用户名格式：xxxx.xxxx.xxxx（字母为小写）；

3) 认证接入信息栏可绑定“认证策略模板”及对应的 SSID；

【添加设备】菜单-主要功能是手动添加/删除 AP、下载批量化导入 AP 的模板、批量导入 AP，也可通过【设备】菜单页面中的<添加设备>按扭进入到【添加设备】菜单页面，详细配置内容如下所示：





单个 AP 增加如上所示，同时也可下载模板，把需添加的 AP 批量化导入 AP 的模板中，支持批量统一对 AP 命名后统再统一导入，示例如下所示：

	A	B	C	D	E
1	MacAddr	Model	Name/设备名称 (3-64 characters/字符)	Address/地址 (6-300 characters/字符)	Notes/备注 (6-300 characters/字符)
2	C0:A6:6D:12:8E:60	IAP5820i-E	09F-AP01		
3	C0:A6:6D:12:D5:00	IAP5820i-E	09F-AP02		
4	C0:A6:6D:12:D6:80	IAP5820i-E	09F-AP03		
5	C0:A6:6D:12:D1:40	IAP5820i-E	09F-AP04		
6	C0:A6:6D:12:CC:80	IAP5820i-E	09F-AP05		
7	C0:A6:6D:12:D4:80	IAP5820i-E	09F-AP06		
8	C0:A6:6D:12:D0:40	IAP5820i-E	09F-AP07		
9	C0:A6:6D:12:CB:60	IAP5820i-E	09F-AP08		
10	C0:A6:6D:12:AB:C0	IAP5820i-E	09F-AP09		
11	C0:A6:6D:12:B2:60	IAP5820i-E	09F-AP10		
12	C0:A6:6D:12:D7:80	IAP5820i-E	09F-AP11		
13	C0:A6:6D:12:AD:C0	IAP5820i-E	09F-AP12		
14	C0:A6:6D:12:AE:E0	IAP5820i-E	09F-AP13		
15	C0:A6:6D:12:90:A0	IAP5820i-E	09F-AP14		
16	C0:A6:6D:12:CD:80	IAP5820i-E	09F-AP15		

【工作模式切换】菜单-主要功能是 AC 切换无线云管理模式功能的配置，详细如下图所示：

网络管理模式配置：默认为本地管理模式，可切换至云管管理模式，云管模式下需要配置云服务器的主机地址。

计算资源配置：默认为无线管理模式。

1、配置为无线管理模式时，CPU 与内存资源优先调度给 AP、终端的接入认证管理，系统侧重于大容量管理，数据走本地转发；

2、配置为数据转发模式时，CPU 与内存资源优先调度给数据转发处理，系统侧重于高转发性能，数据走集

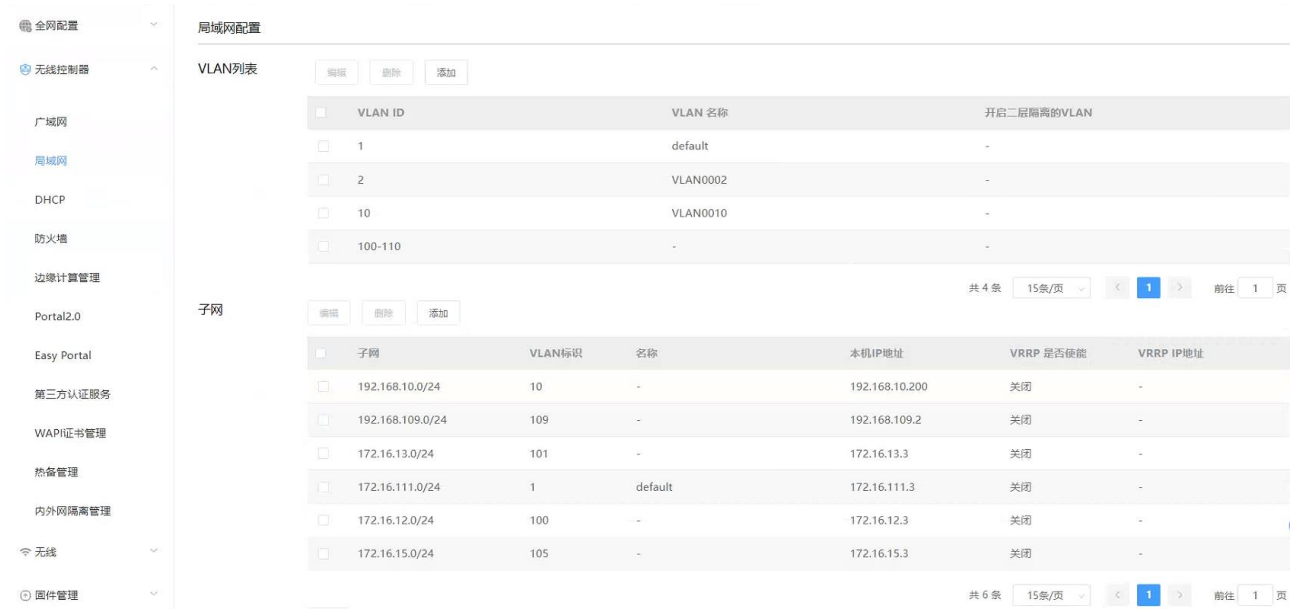
中转发或者设备作为出口网关；

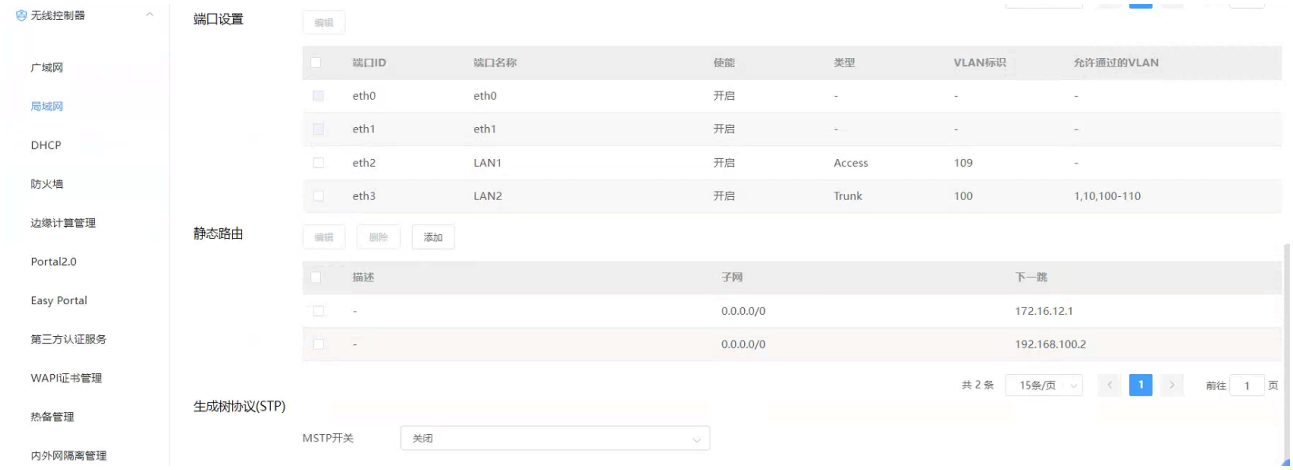
3、配置为 IoT 边缘计算模式时，CPU 与内存资源优先调度给边缘计算处理，系统侧重于物联网边缘业务。

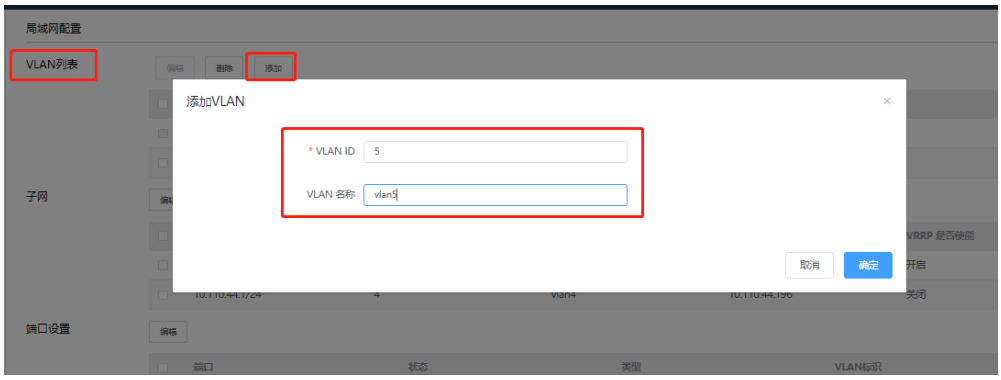
2.4.3.6.2 无线控制器

【广域网】菜单-主要功能是 AC 做网关或切换为云管理模式时进行 WAN 口的 IP 信息、DNS 信息的配置，详见如下图所示：

【局域网】菜单-主要功能是 AC 的 VLAN 创建、VLAN 子网创建、VRRP 功能的开启、上下行网络端口、静态路由、生成树协议等功能的配置，详见如下图所示：





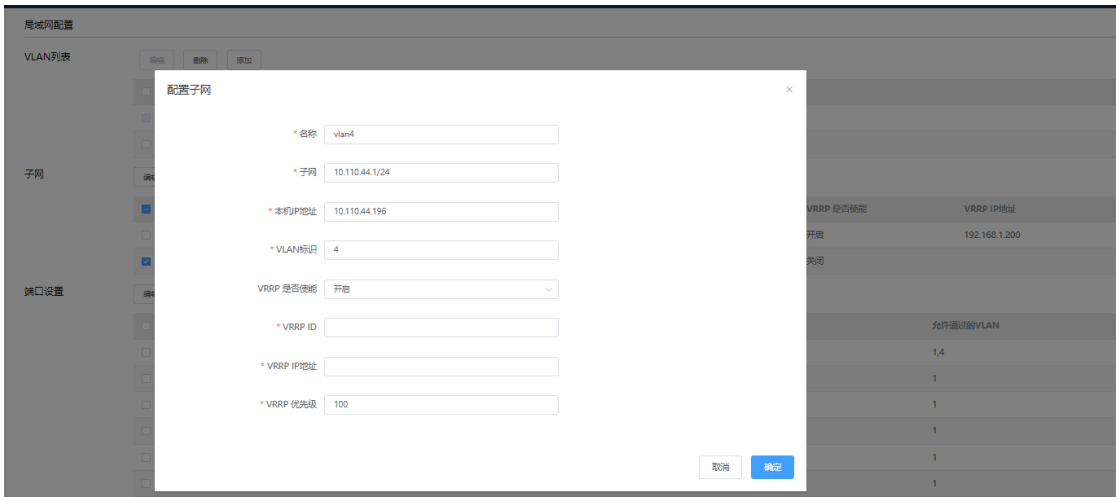


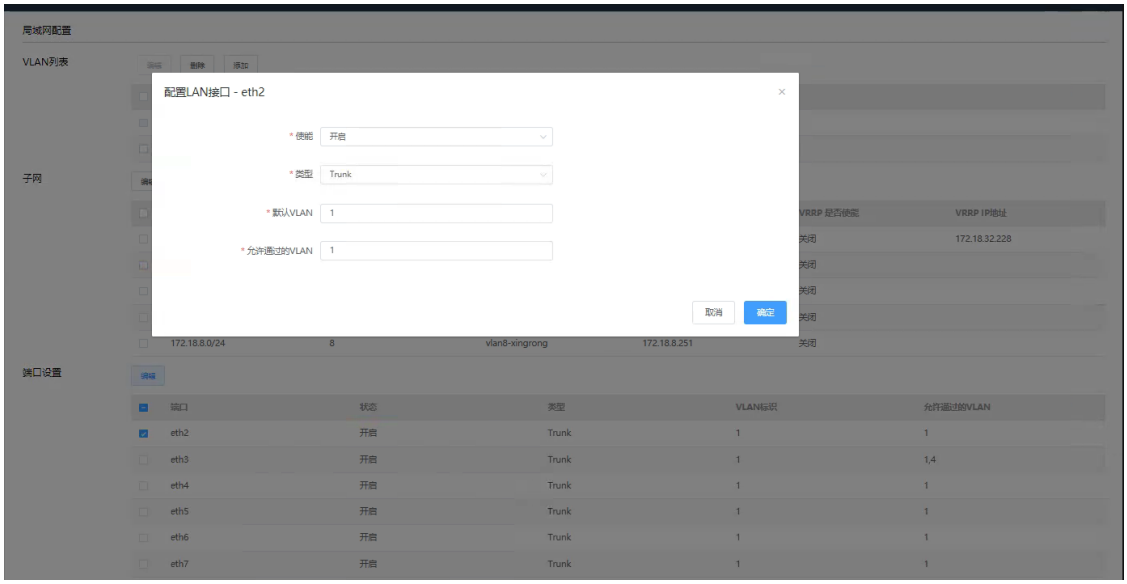
在【VLAN 列表】点击<添加>，可添加 VLAN，VLAN 添加后，在子网模块中可添加该 VLAN 的接口 IP。

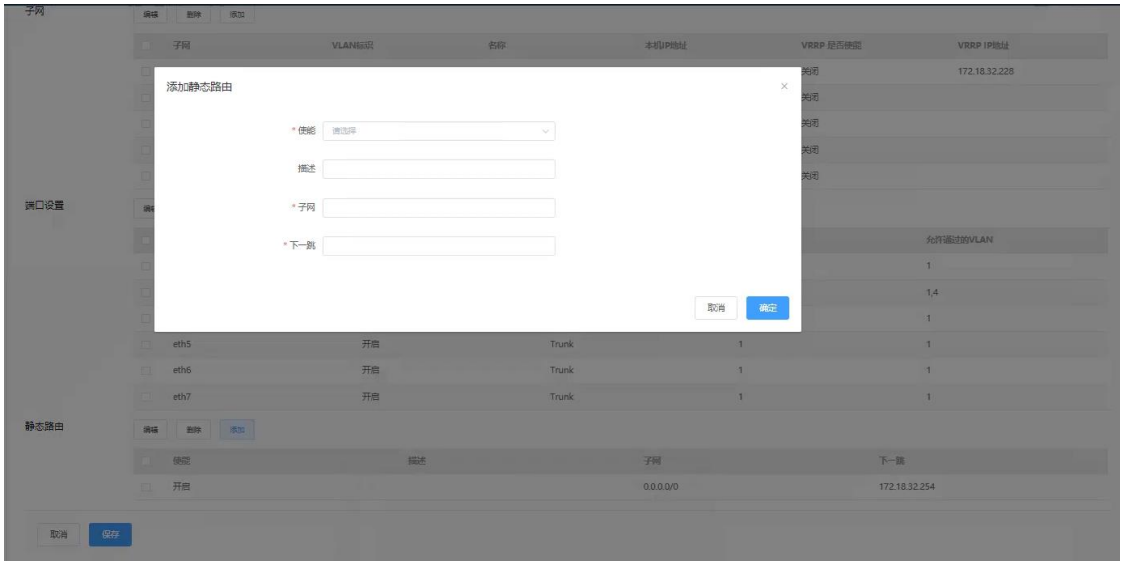
说明：

1） Portal 认证时，需配置相应业务 VLAN 的接口 IP；

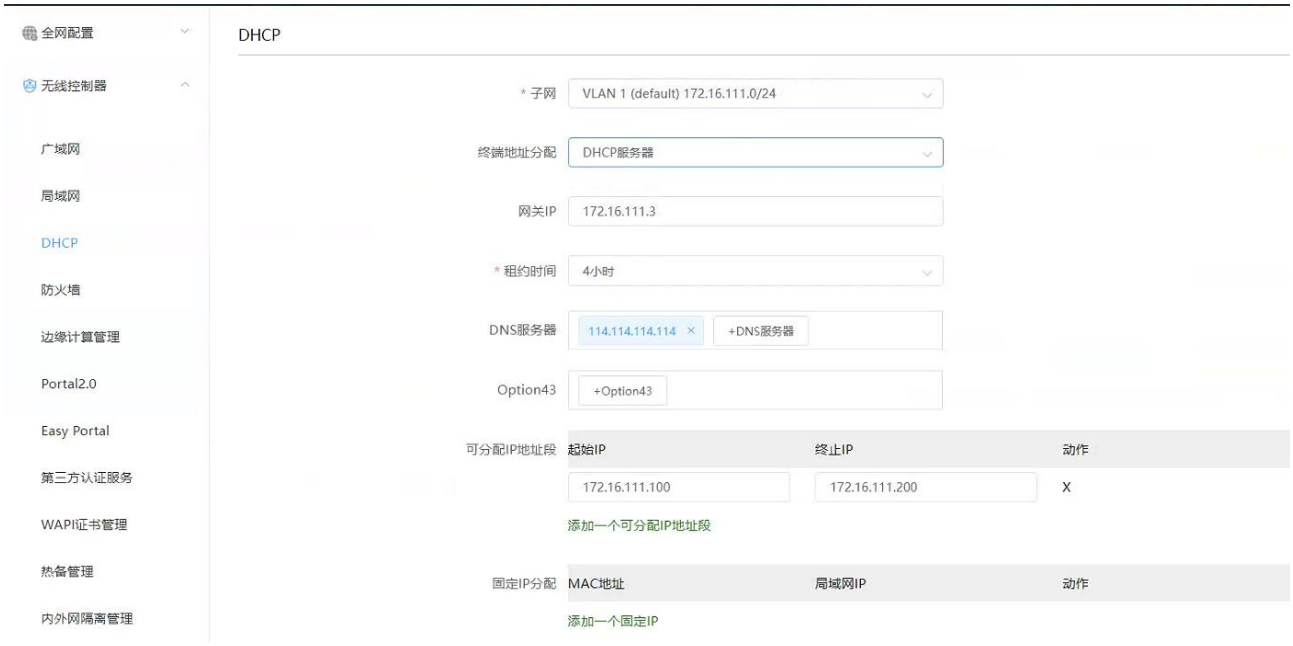
2） 非 Portal 认证时，相应业务 VLAN 的接口 IP 是可配也可不配，业务不受影响；







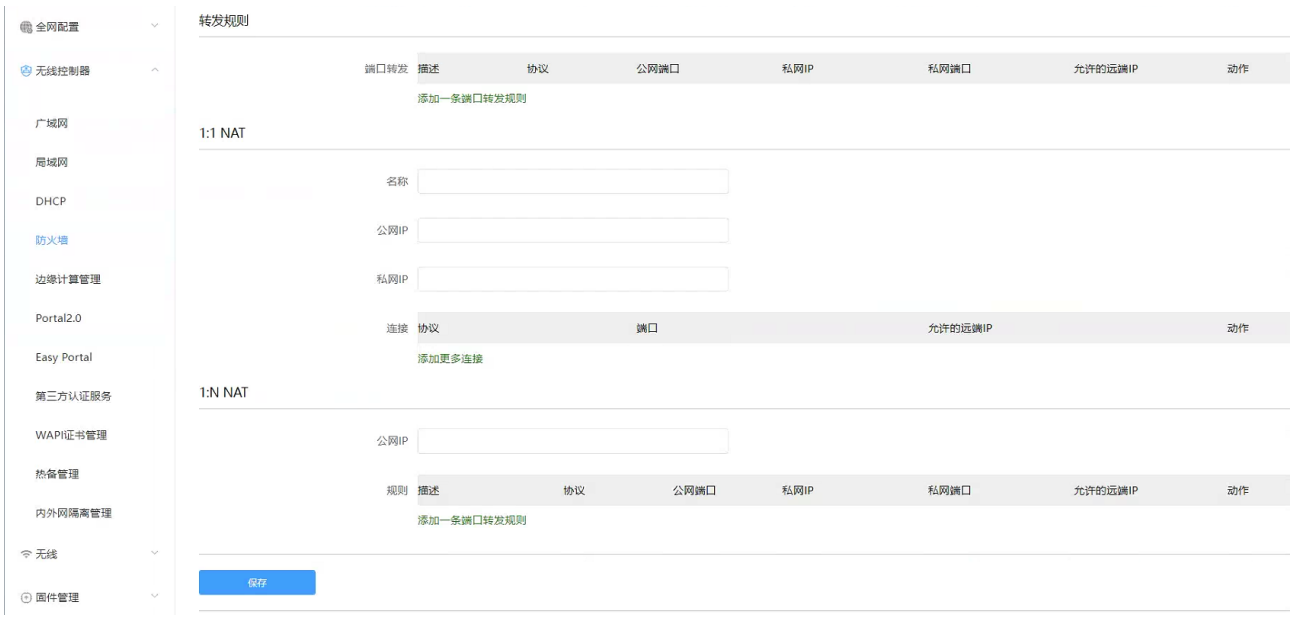
【DHCP】菜单-主要功能是 AC 中 DHCP 服务功能配置，包括开启或关闭 DHCP、网关 IP、租约期限、DNS 服务器、地址池起始与结束地址、固定 IP 与 MAC 绑定等配置，详见如下图所示：



说明：

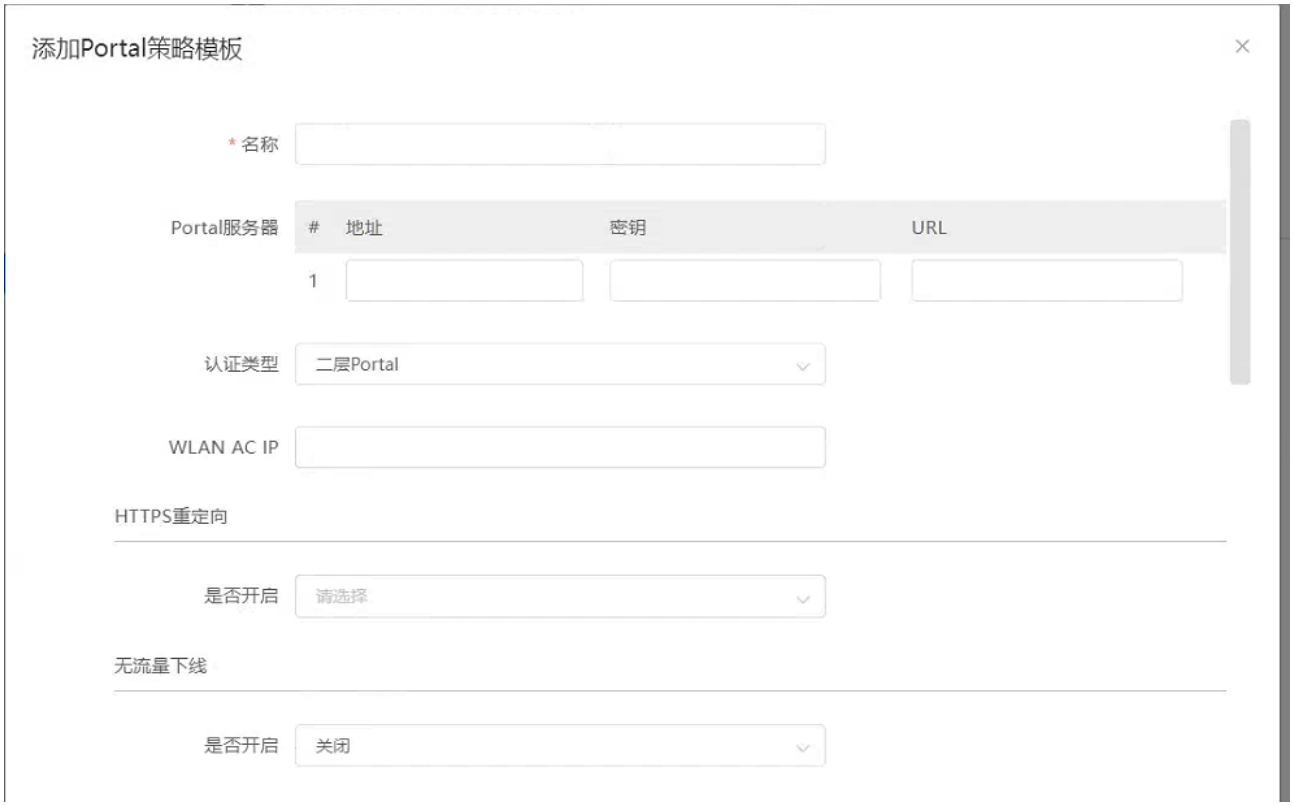
DHCP 服务配置时，需关注 AC 型号，不同型号的 DHCP 服务性能有所不同，具体根据前期规划设计时要求来进行即可。

【防火墙】菜单-主要功能是 AC 作为出口网关时实现简单 ACL 控制、NAT 转换等功能的配置，详见如下图所示：



【边缘计算管理】菜单-主要功能是边缘计算的访问控制功能配置，详见如下图所示：

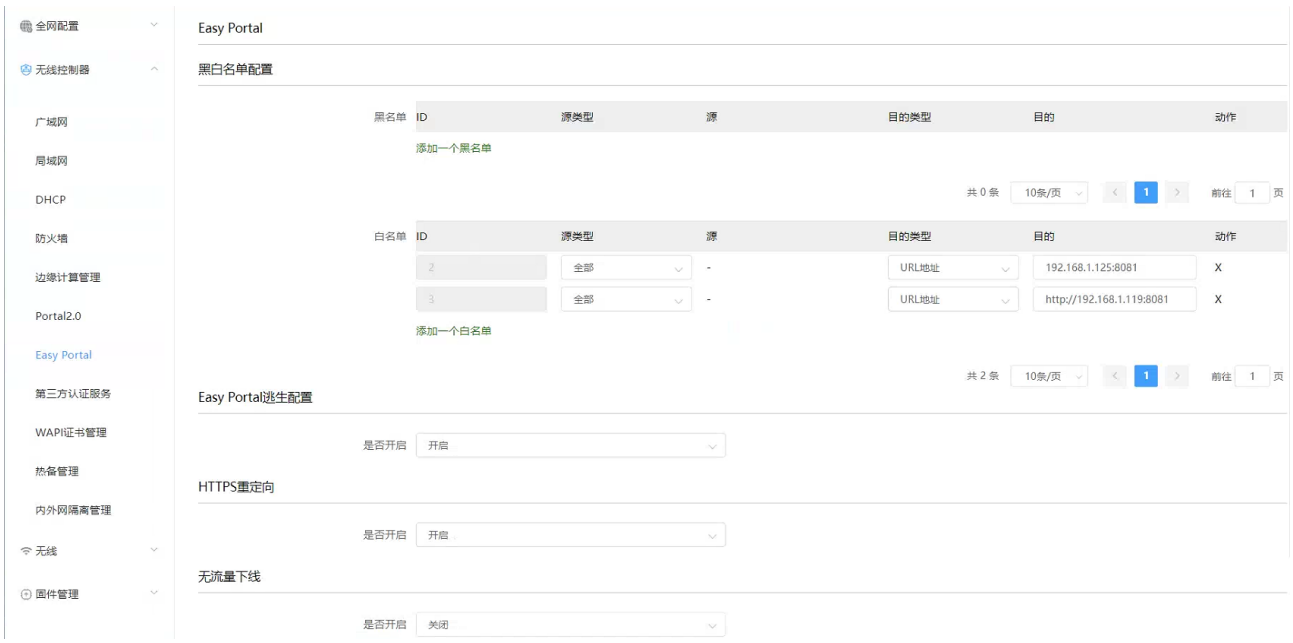
【Portal2.0】菜单-主要功能是 AC 对接第三方 Portal 认证时，在 AC 侧需做的第三方认证平台认证与计费服务信息的配置，详细如下图所示：



点击<添加一个 Portal 策略模板>可以激活 Portal 策略模板配置窗口，可以配置 Portal 服务器名称、Portal 地址、密钥、URL 等功能；

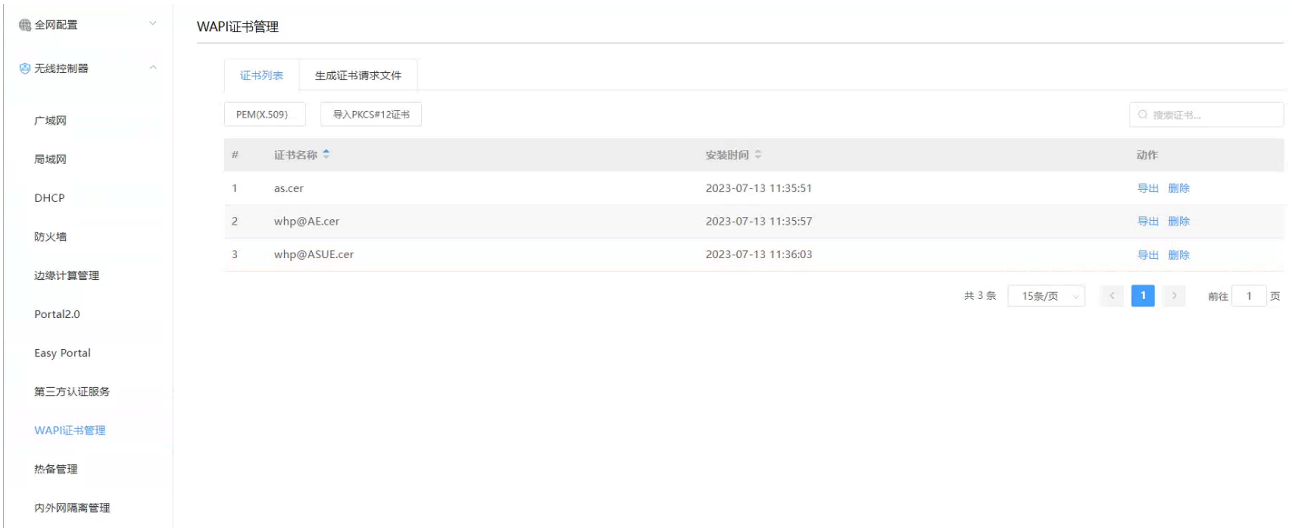
可以选择是否开启开启无流量下线，开启后，终端在流量统计时长内未达到最小流量将下线；

【Easy Portal】菜单-主要功能是对应使用 Easy Portal 认证时，终端的受限访问内容的黑白名单配置。源类型可以为全部、IP 地址、Mac 地址、VLAN，目的类型可以为全部、IP 地址、URL 地址。详细如下图所示：

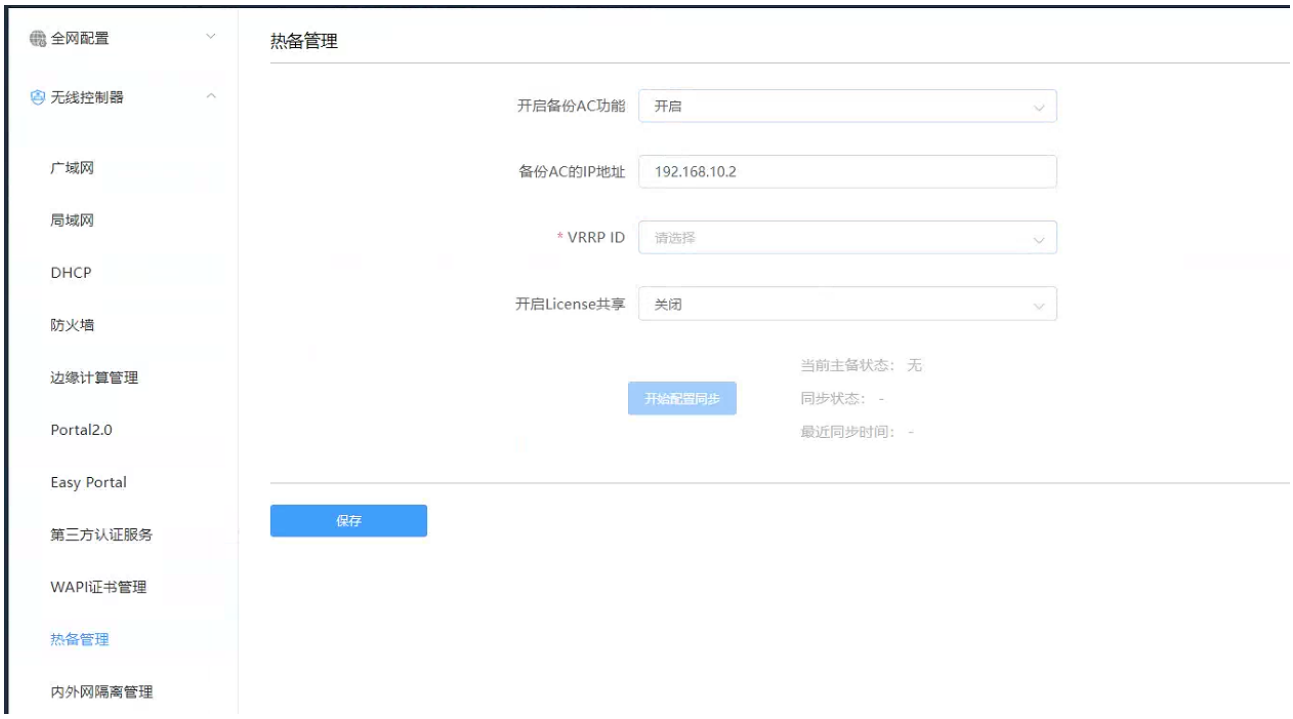


【第三方认证服务】菜单-主要功能是 AC 对接第三方认证服务器时，在 AC 侧需做的第三方认证平台认证与计费服务信息的配置，详细如下图所示：

【WAPI 证书管理】菜单-主要功能是导入 WAPI 证书及生成证书请求文件等，点击“PEM(X.509)”可上传 WAPI 证书



【热备管理】菜单-主要功能是配置热备管理相关配置

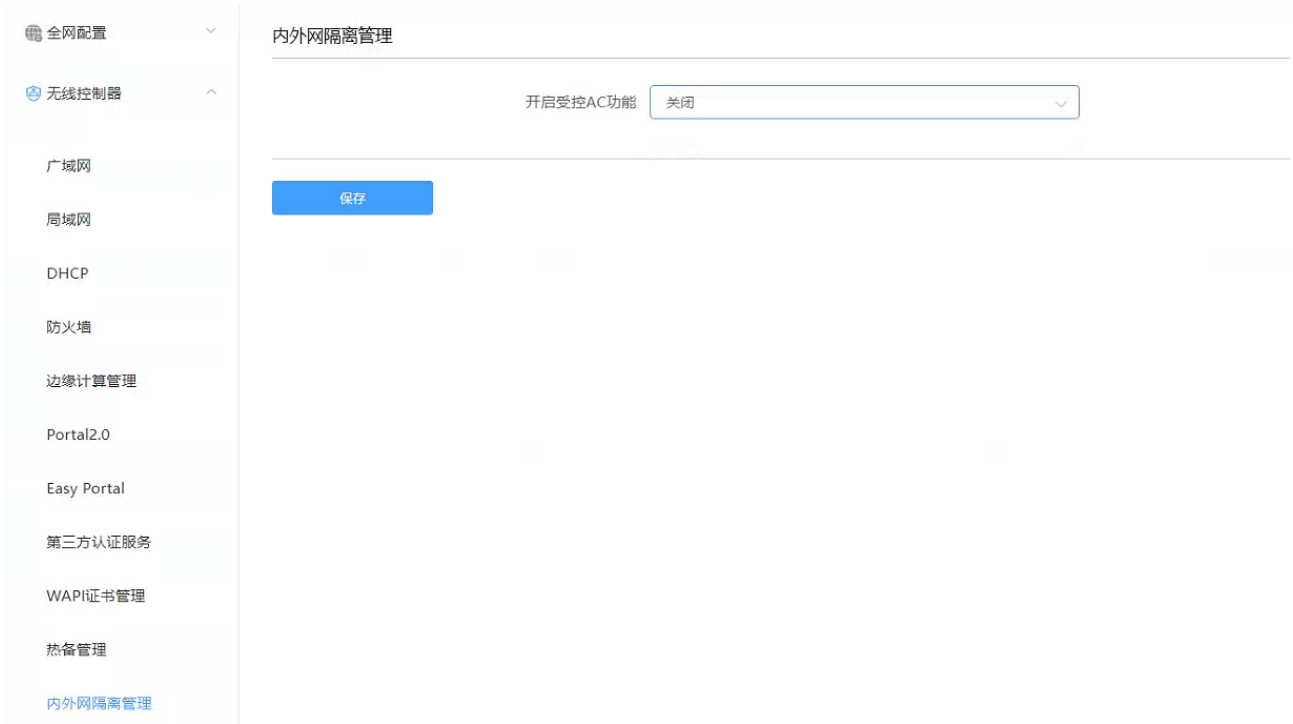


说明：

（1）主备配置同步：主备建立后，登录主 AC，点击<开始配置同步>，可将主 AC 的配置同步到备 AC。

（2）开启 License 共享后，备 AC 可以共享主 AC 的 License（主备 AC 都需要开启），默认是 30 天，主备断开后，30 天内备 AC 可继续使用共享的 License。

【内网网隔离管理】菜单-可开启受控 AC 功能



受控 AC 配置：若开启受控 AC，AP 将能够同时连接主控 AC 和受控 AC，且能够提供互相隔离的网络服务。

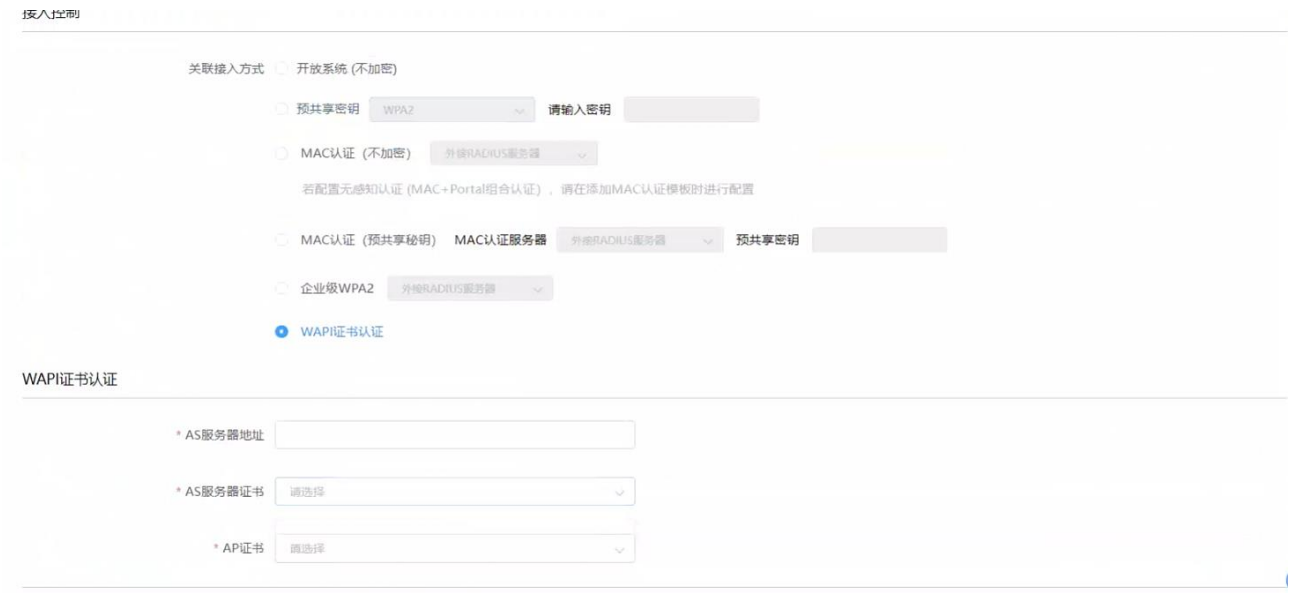
2.4.3.6.3 无线菜单

【无线服务】菜单-主要功能是 SSID 模板的配置，有 SSID 名称、类型、是否开启、接入控制选择（本地或第三方）、本地 Portal 开启及策略选择、本地\集中转发模式、业务 VLAN 指定、二层隔离、用户逃生模式、带宽策略、快速漫游开关、组播优化开关、定时开\关 SSID、AP 的绑定、基于 SSID 的终端黑白名单等功能配置，详见如下图所示：

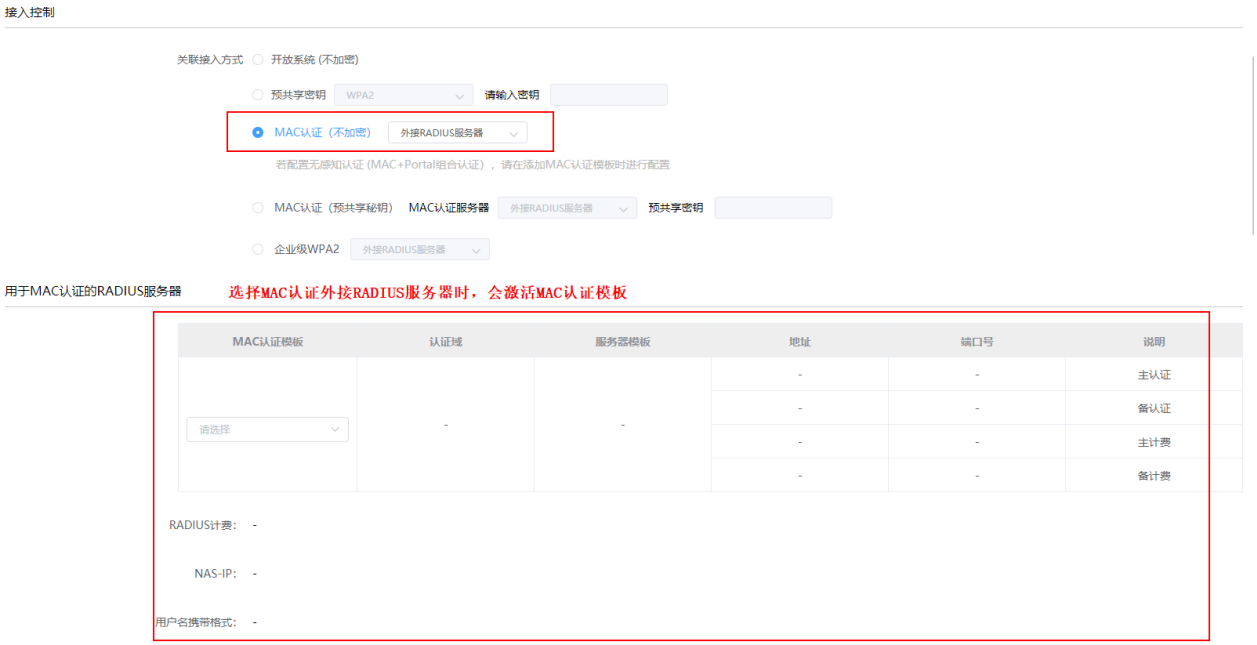
默认有 15 个 SSID 模板，也可再添加，详细的 SSID 模板如下图所示：

默认 SSID 类型为接入业务

预共享密钥可选择 WPA2 和 WAPI，当选择 WAPI 时，可配置 WAPI 加密的 ssid；



当选择 WAPI 证书认证时，会激活 WPAI 认证配置窗口，可配置 AS 服务器的地址和选择 AS 服务器证书及 AP 证书（证书在【边缘计算管理】>【WAPI 证书管理】中上传）



当选择 Easy Portal 中的“免认证，受限访问”时，无线接入用户，无需认证，只限访问受限的网络资源，该资源可以在【设置】>【无线控制器】>【Easy Portal】>【黑白名单配置】中添加黑白名单进行设置

当选择“寻址和流量策略”——“数据转发方式”中的“二层桥接模式”时，可配置 DHCP 转发方式为集中转发模式或本地转发模式。在集中转发模式下，DHCP 报文由 AC 转发，在本地转发模式下，DHCP 报文由 AP 转发。

VALN 标记包含如下 4 个选项：

不使用 VLAN 标记//终端获取 AP 管理 VLAN 的 IP;;

使用预配置 VLAN 标记//配置业务 VLAN

使用基于 IP 的 VLAN 标记//可以添加基于 IP 段与 VLAN 的映射表；

使用基于 MAC 的 VLAN 标记//可以添加基于 MAC 的 VLAN 模板。

选择本地转发时，可配置用户逃生功能，目前支持用户保持在线的逃生模式，此逃生模式下，已在线终端仍接入网络，新用户无法上线。

可以选择是否开启二层隔离，默认为关闭。选择开启后，可以配置基于该 SSID 的二层隔离，连接该 SSID 的无线客户端无法互相访问。

“防火墙”点击“添加一条防火墙规则”可添加防火墙规则。

“服务质量”带宽策略默认为关闭，当选择开启后，可配置基于每 SSID 或每终端的带宽限速。

“漫游”默认关闭三层漫游，三层漫游下拉菜单选择开启，可以开启三层漫游功能；

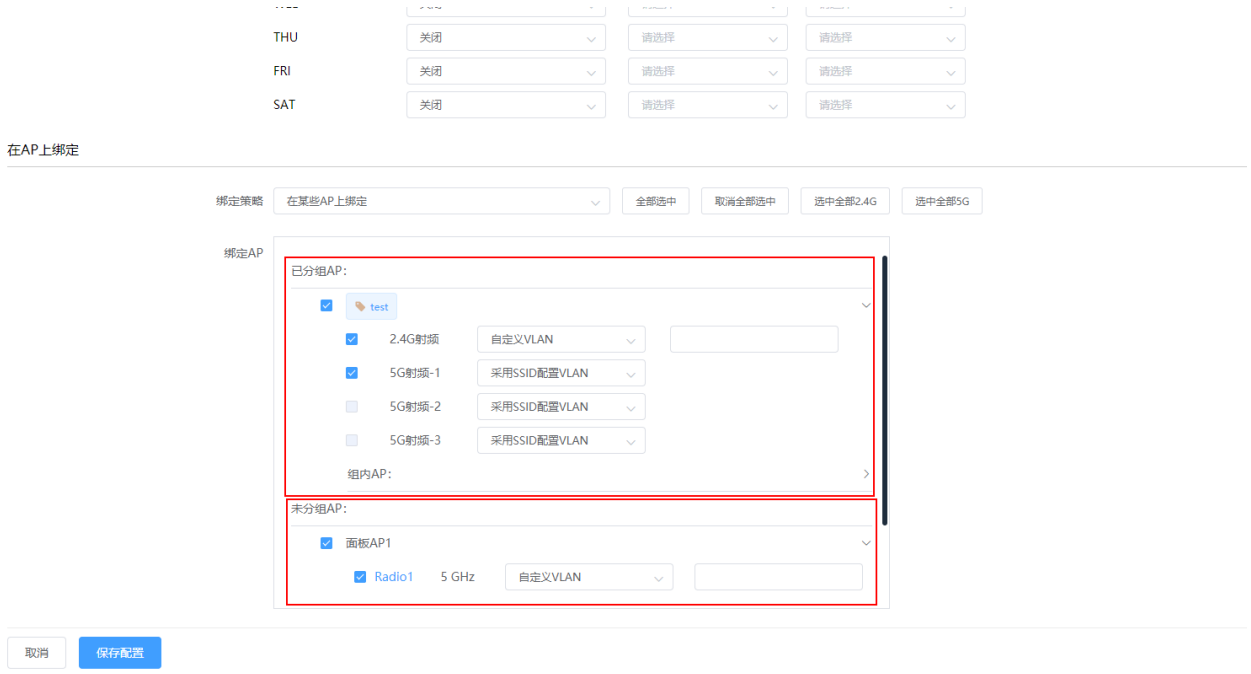
使用三层漫游时，需要注意：

（1）POE 交换机上需要放行本区域的业务 vlan

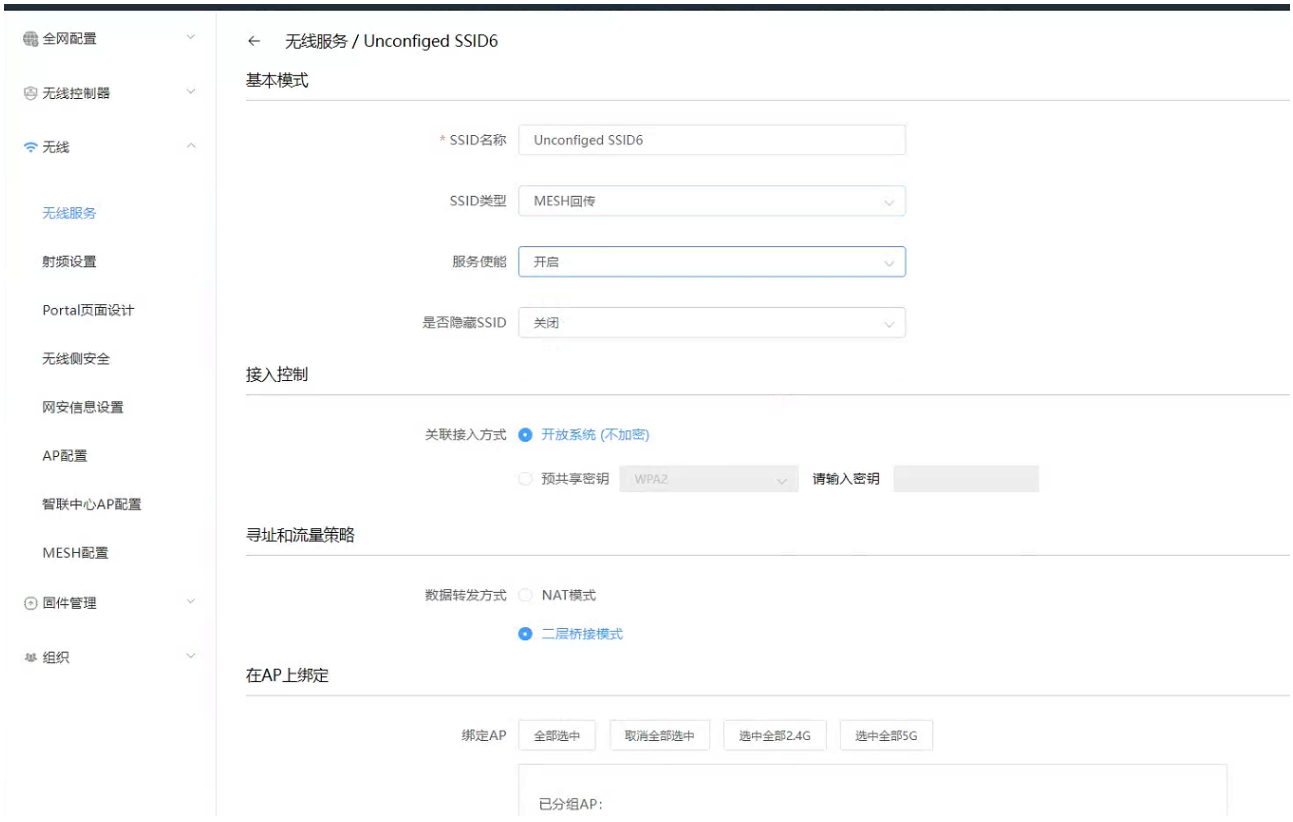
（2）三层漫游会将流量集中到 AC，所以需要在 AC 与核心互联的口放行所有业务 vlan

“接入黑名单管理”和“接入白名单管理”可添加基于 SSID 的终端黑白名单列表，当有终端 mac 加入到白名单列表中后，非白名单的终端将无法接入该 ssid。详见如下图所示：

当选择在某些 AP 上绑定时，可以绑定某个分组或其他未分组的 AP，可以基于 2.4G 射频或 5G 射频自定义 VLAN，将 VLAN 绑定到 AP 的射频上，该 VLAN 优先级高于 SSID 上绑定的 VLAN，详见如下图所示：



MESH 管理 SSID 配置说明：



MESH 功能需配合支持 MESH 的 AP 使用

SSID 类型为终端接入时，可配置普通类型的 ssid 业务；SSID 类型为 MESH 回传时，可配置 MWSH 类型的 ssid 业务。

（1）SSID 类型选择 MESH 回传时

①接入控制可选择关联接入方式为开放系统（不加密）或预共享密钥（WPA2、WEP、WAPI）

②寻址和流量策略可选择 NAT 和二层桥接模式，二层桥接模式时，流量从 MPP 本地转发，选择 NAT 时，激活管理 VLAN 配置窗口，如下图：

管理 VLAN 配置，可配置 MESH 回传 SSID 的管理 vlan 和 MPP LAN 口 IP，连接该 SSID 的 MAP 将获取所该 vlan 网段的 ip（dhcp server 需要在 ac 上配置）

③选择绑定 AP 时，

<1>仅显示 MESH 分组

<2>以分组为单位绑定，可以展开显示组内配置和分组下的 AP

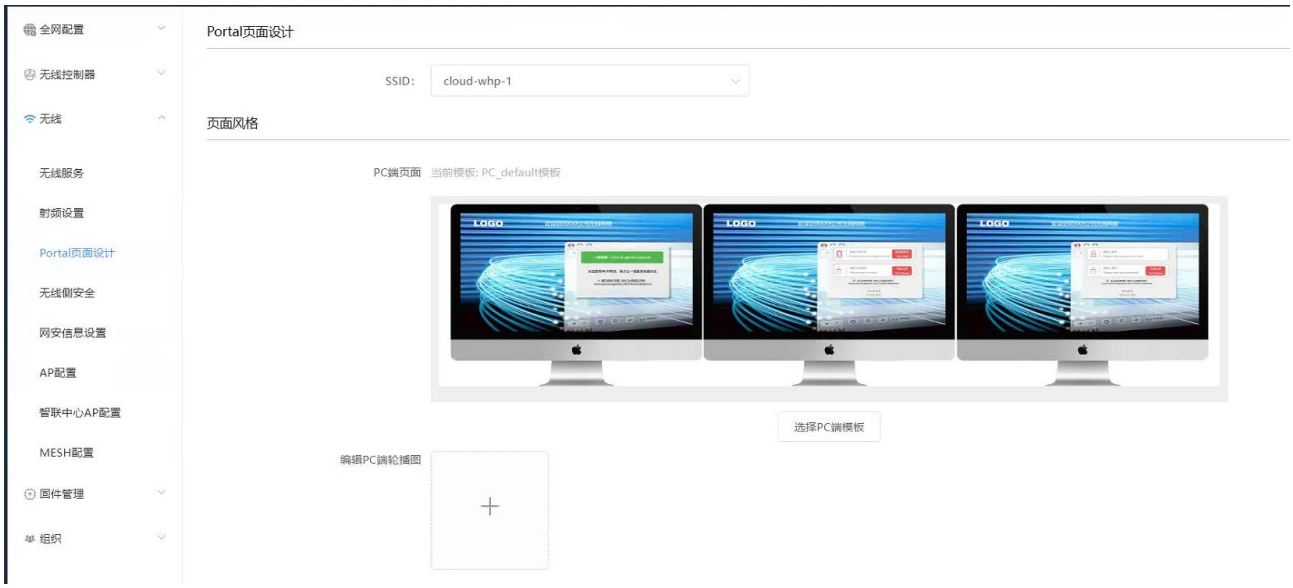
<3>一个 MESH 组只能绑定一个 MESH SSID

<4>一个 MESH SSID 可同时绑定多个 MESH 分组

<5>支持快捷方式全部选中、取消全部选中

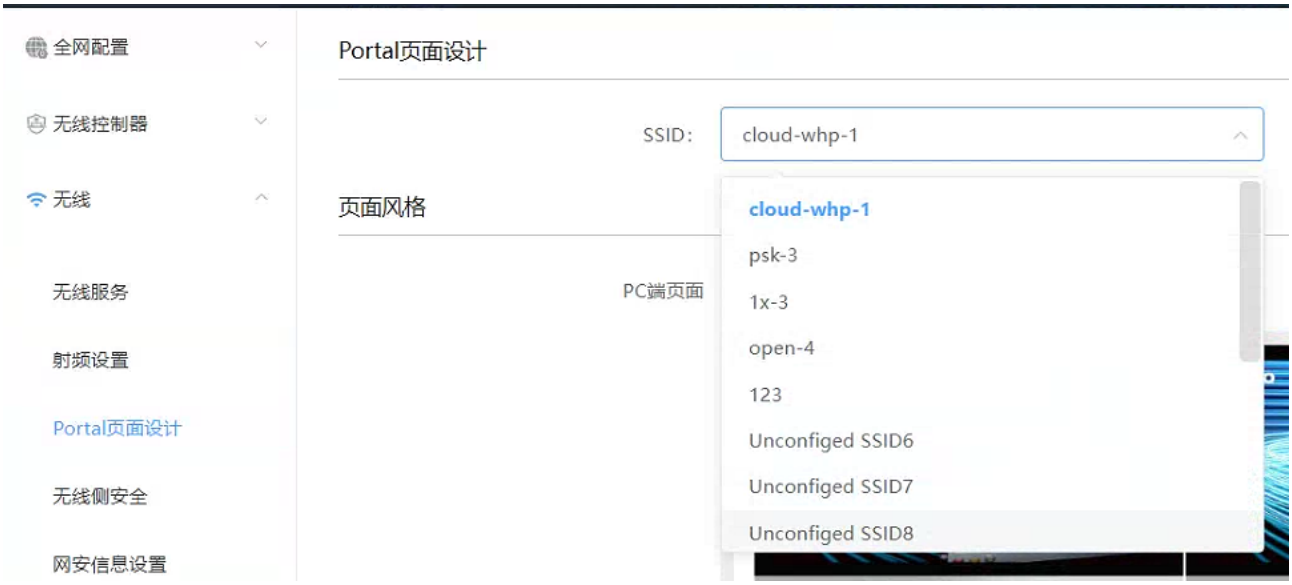
【射频设置】菜单-主要功能是对 AP 的 2.4G/5G 射频的信道、发射功率等功能的配置，详见如下图所示：

【Portal 页面设计】菜单-主要功能是对本地 portal 认证时，重定向页面的风格选择或定制化设计，详见如下图所示：



【Portal 页面设计】

1 在 SSID 下拉框可以选择需要进行 Portal 页面设计的 SSID



【页面风格】

（一）PC 端

1、 PC 端页面

点击<选择 PC 端模板>,可以在弹出页面选择不同模板

2、 编辑 PC 端轮播图

3、 点击<+>，弹出页面点击<新增轮播图>，可添加 png、jpg、jpeg 格式的图片，上传图片大小不能超过 2Mb，图片大小可选择 PC 端常用分辨率，如 1920*1080

4、 PC 端对轮播图的数量无限制，轮询时间无法设置，默认为 5s 一次。

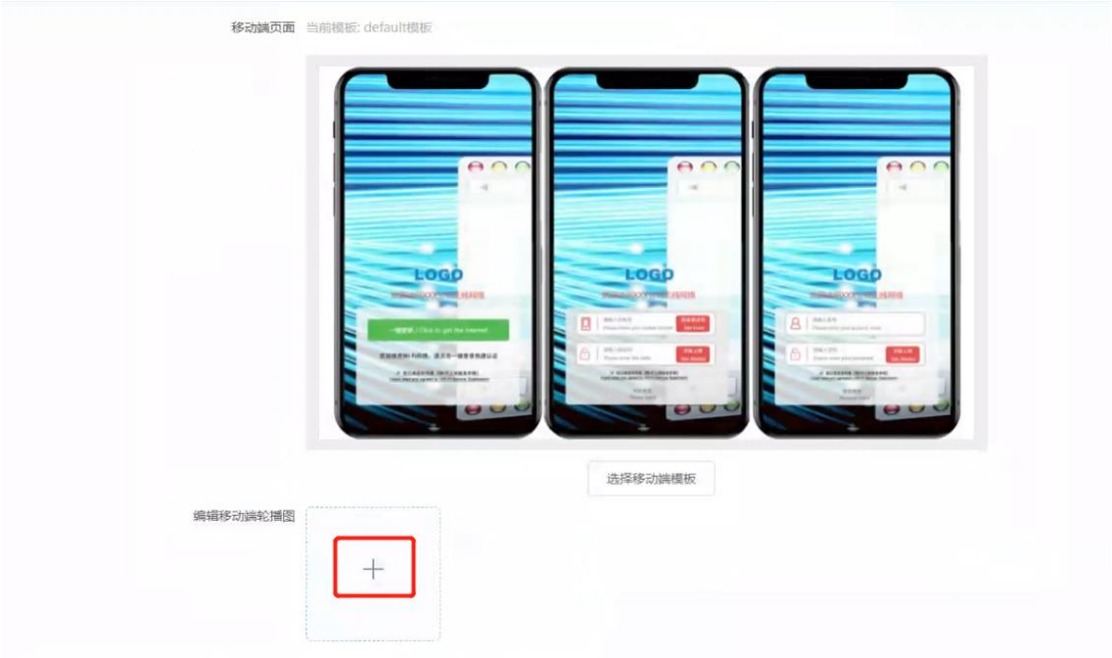
（二）移动端

1、 移动端页面

点击<选择移动端模板>,可以在弹出页面选择不同模板

2、 编辑移动端轮播图

3、 点击<+>，弹出页面点击<新增轮播图>，可添加 png、jpg、jpeg 格式的图片，上传图片大小不能超过 2Mb。因不同终端分辨率不同，可上传图片后根据实际效果进行调整。



4、 移动端对轮播图的数量无限制，轮询时间无法设置，默认为 5s 一次。

【内容定制化】

1、 可设置 PC 端和移动端页面标题内容，长度无限制

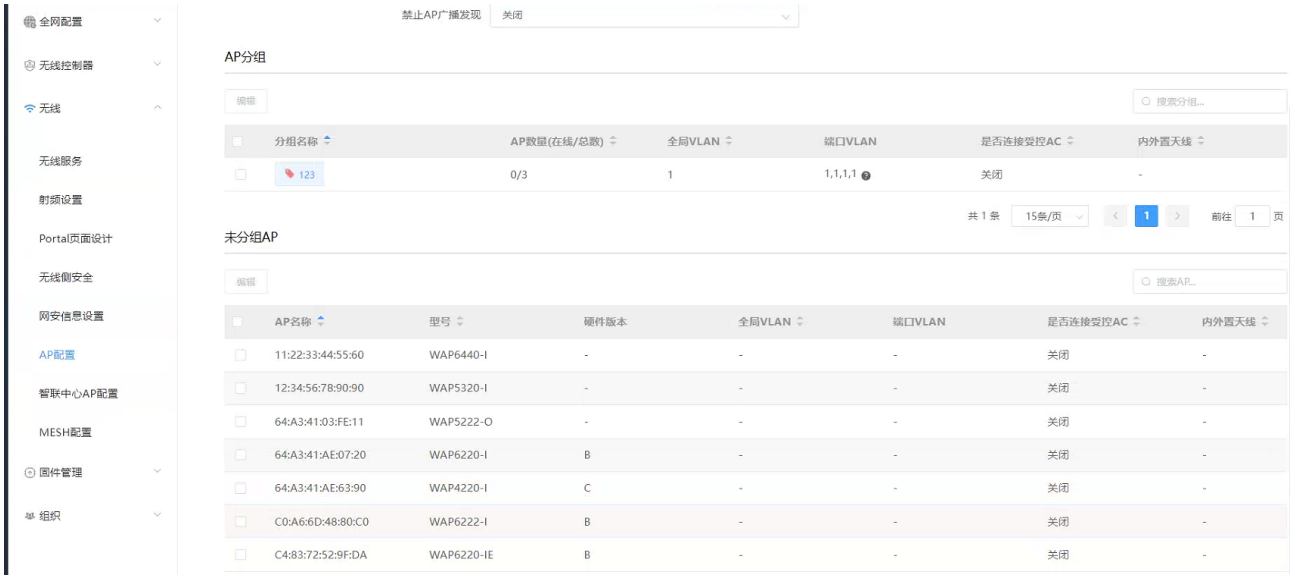
2、 可上传 PC 端和移动端页面 LOGO，支持 png、jpg、jpeg 格式

【跳转行为】

1、 可选择开启或关闭认证前广告，默认为开启，广告展示时间默认为 3s
2、 PC 端页面广告点击<+>可从上传的 PC 端轮播图中选择一张作为页面广告，也可在该页面通过<新增轮播图>上传
3、 移动端页面广告点击<+>可从上传的移动端轮播图中选择一张作为页面广告，也可在该页面通过<新增轮播图>上传
4、 认证成功后跳转 URL 格式必需以 http://或者 https://开头

【无线侧安全】菜单-主要功能是流氓 AP 检测策略、无线侧攻击防御、无线黑名单策略的功能配置，详见如下图所示：

【AP 配置】菜单-主要功能是针对采用内外网隔离的组网方式时，可以选择 AP 是否做内外网隔离以及面板 AP LAN 口的 VLAN 配置，详见如下图所示：



选择 AP 分组或 AP，点击<编辑>可设置 AP 的 VLAN 及选择是否加入受控 AC；

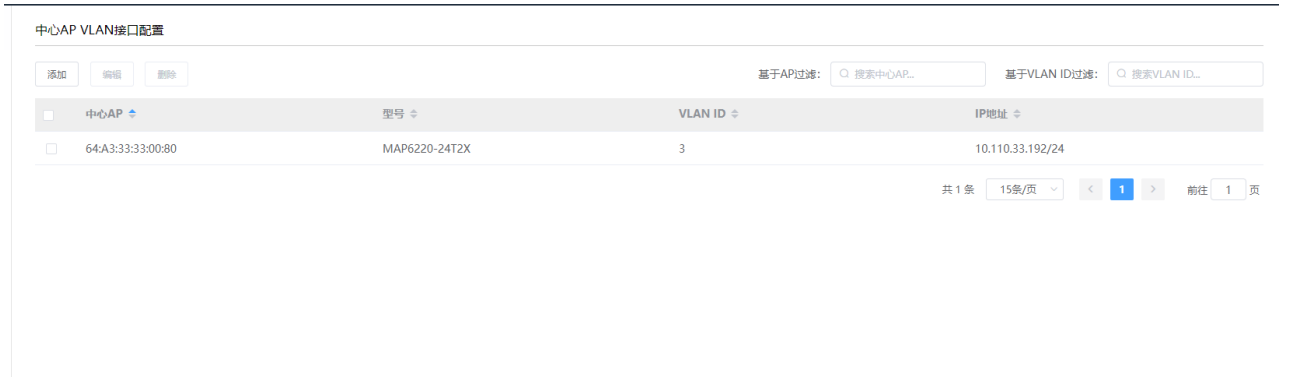
室外 AP 可进行内外置天线切换功能配置；

注:VLAN 配置只对面板 AP 生效,当前支持的面板 AP 型号为:IAP5820w,IAP5820w-L,IAP5820w-S,IAP5920w, IAP5920w V2。

【智联中心 AP 配置】菜单-主要功能是配置智联中心 AP 的 VLAN 接口。

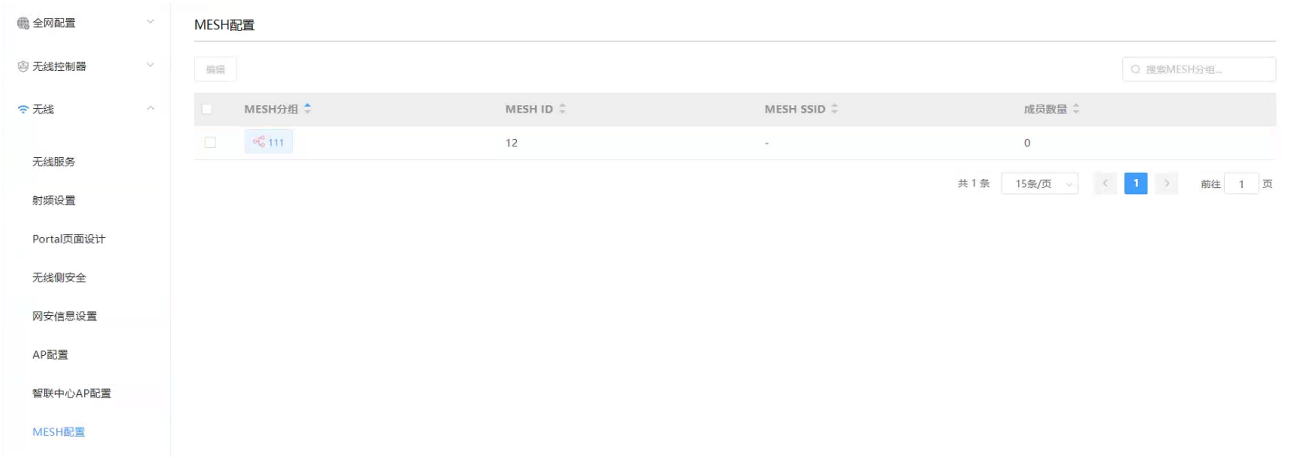
【设置】>【无线】>【AP 配置】【智联中心 AP 配置】进入中心 AP VLAN 接口配置页面，点击<添加>

在弹出的页面，“中心 AP”栏选择要配置的中心 AP，“VLAN ID”栏选择对应的业务 VLAN，“IP 地址栏”配置中心 AP 的 IP 地址及掩码。

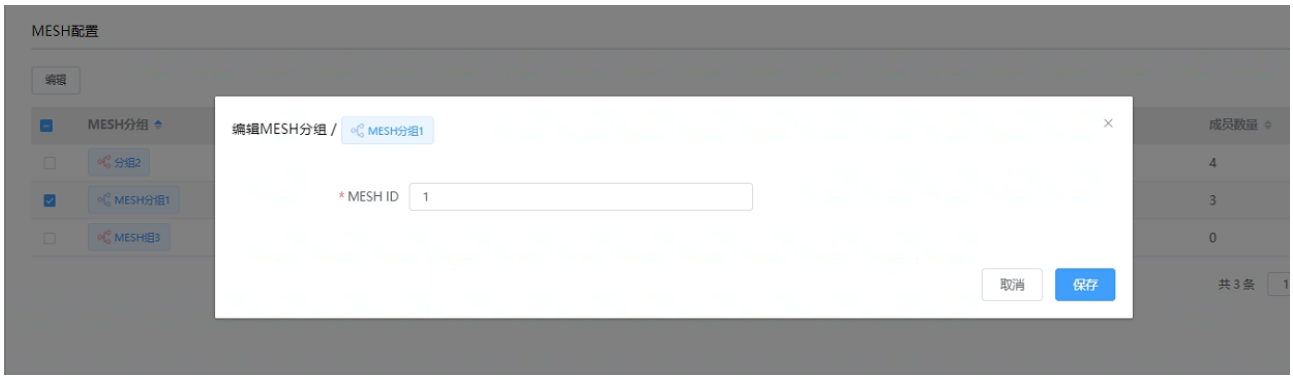


注意：当智联中心 AP 环境下使用 portal 认证时，需要先通过<添加>按钮选择中心 AP 并配置 VLAN 接口，再配置 portal 认证的 ssid。

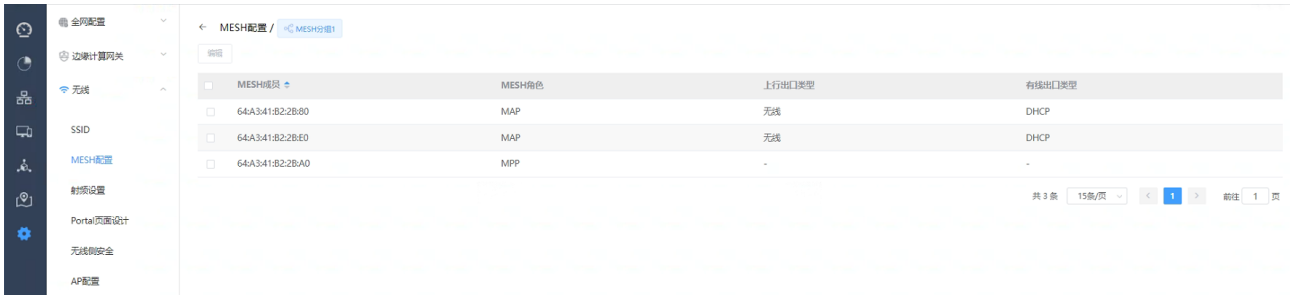
【MESH 配置】菜单-主要功能是对 MESH 分组及 MESH 成员进行配置，详见如下图所示：



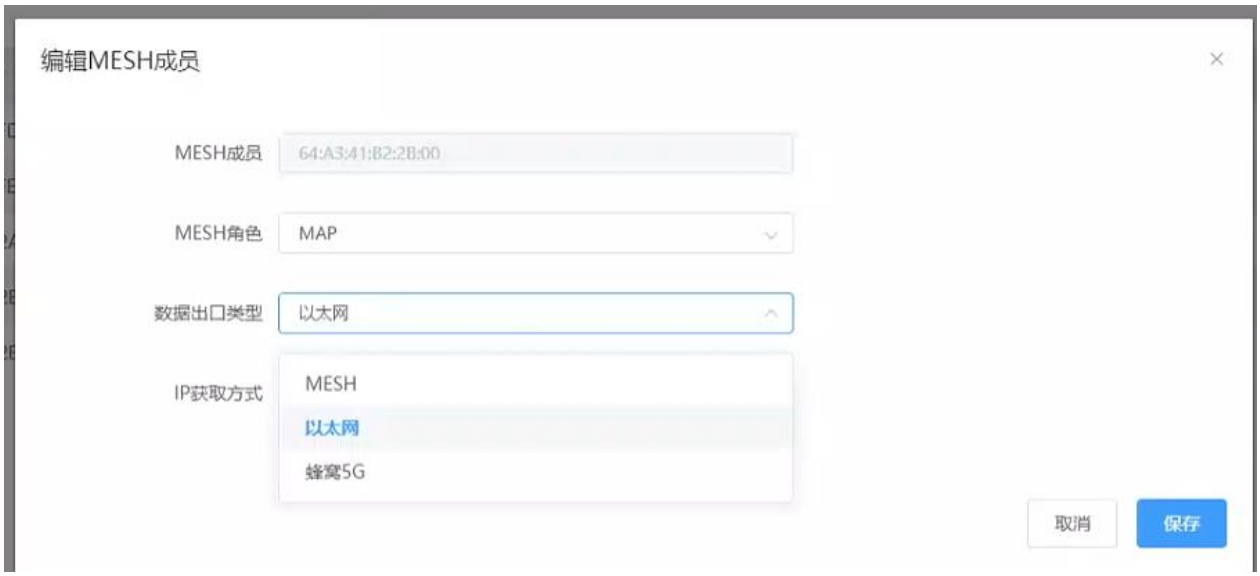
选中 MESH 分组，点击编辑可修改 MESH 分组的 MESH ID



点击某 MESH 分组，可进入该分组的 MESH 配置页面，显示当前分组内的 MESH 成员，成员所属角色、上行出口类型和有线出口类型。

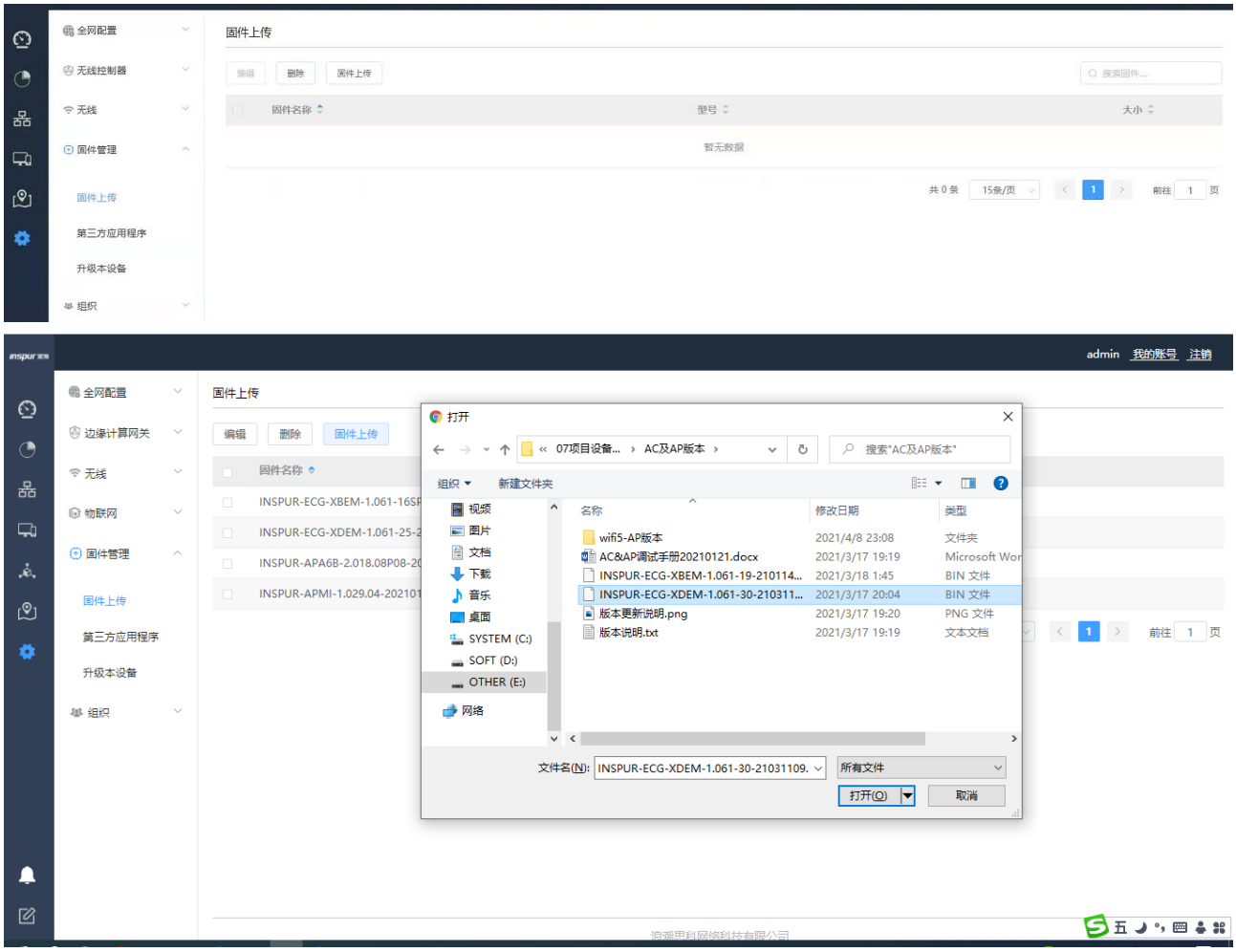


选中成员后点击编辑，可编辑该 MESH 成员，MESH 角色可选中 MAP 或 MPP，当选中 MAP 时，可设置数据出口类型为 MESH、以太网或蜂窝 5G，当为以太网类型时，可选则 IP 获取方式为为 DHCP 或静态地址。



2.4.3.6.4 固件管理菜单

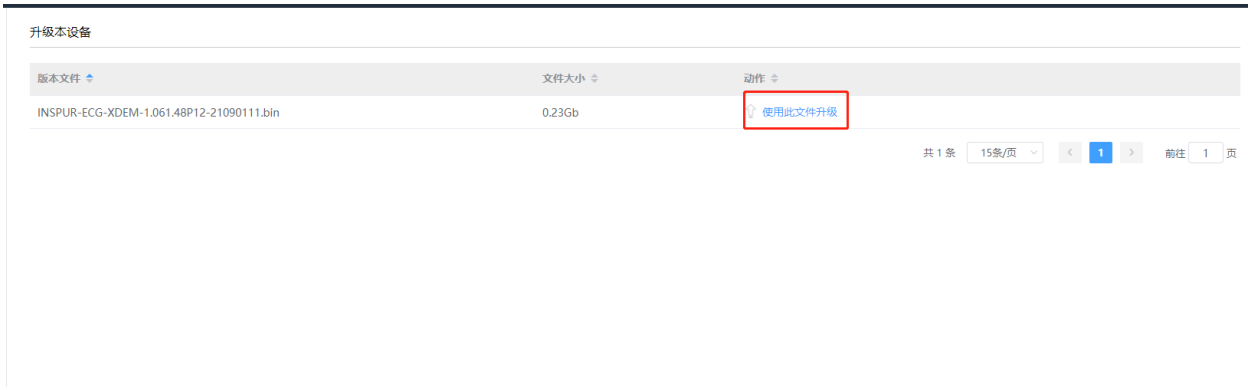
【固件上传】菜单-主要功能是上传 AC、AP 升级包，详见如下图所示：



【第三方应用程序】菜单-功能介绍

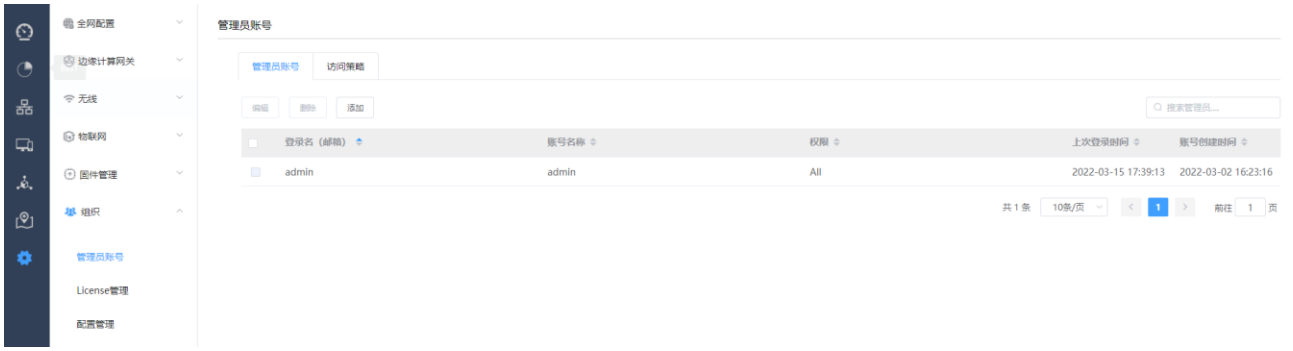
点击<第三方应用程序>按钮，可以上传后缀名为.tar.gz 格式的第三方应用程序文件

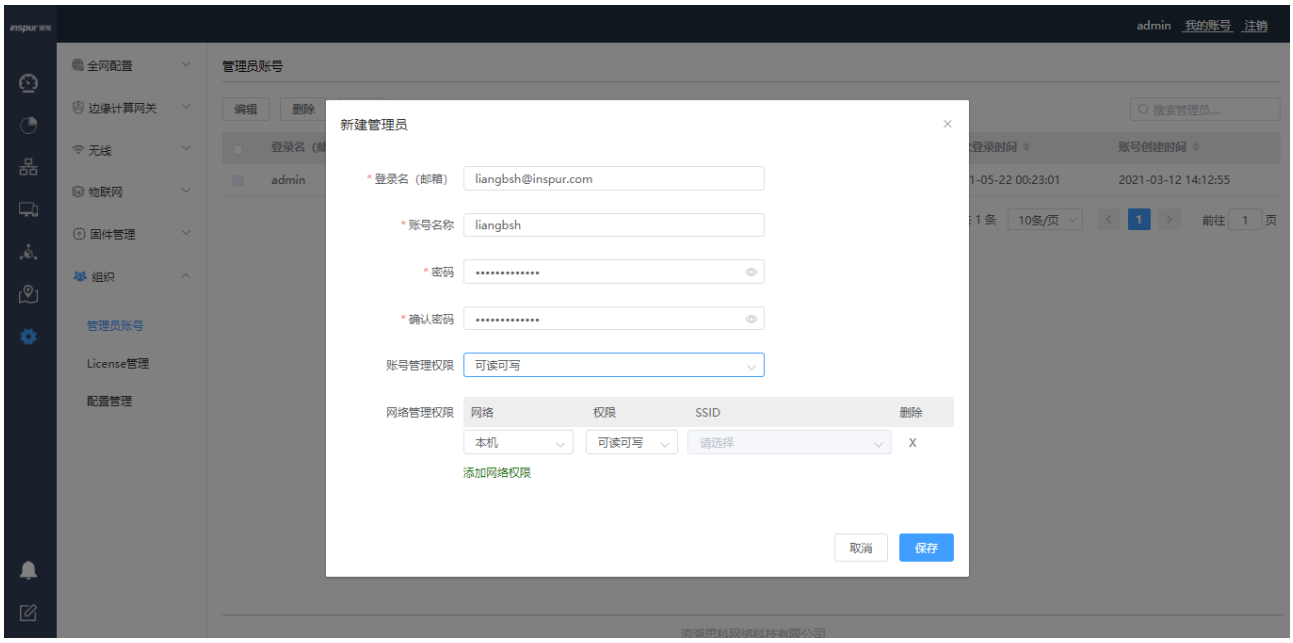
【升级本设备】菜单-主要功能是通过 Web 升级直接 AC 设备的版本，详细如下图所示：



2.4.3.6.5 组织菜单

【管理员账号】菜单-主要功能是创建 Web 登录新账号，与 AC 命令行创建用户功能相互独立，密码需为数字、大小写字母、特殊字符的组合密码，详见如下图所示：





【访问策略】全局设置，针对所有账号，可配置 WEB 登录账号的访问策略，包括最大尝试次数，锁定时间，密码有效期，可访问 IP 地址等。

最大尝试次数：可设置最大尝试次数，可设置范围为 5-10

锁定时间：超过设置的最大尝试次数后，WEB 登录页面会被锁定，可设置范围为 5-60 分钟

密码有效期：可选择 1 天，7 天，30 天，180 天，365 天，永久有效。

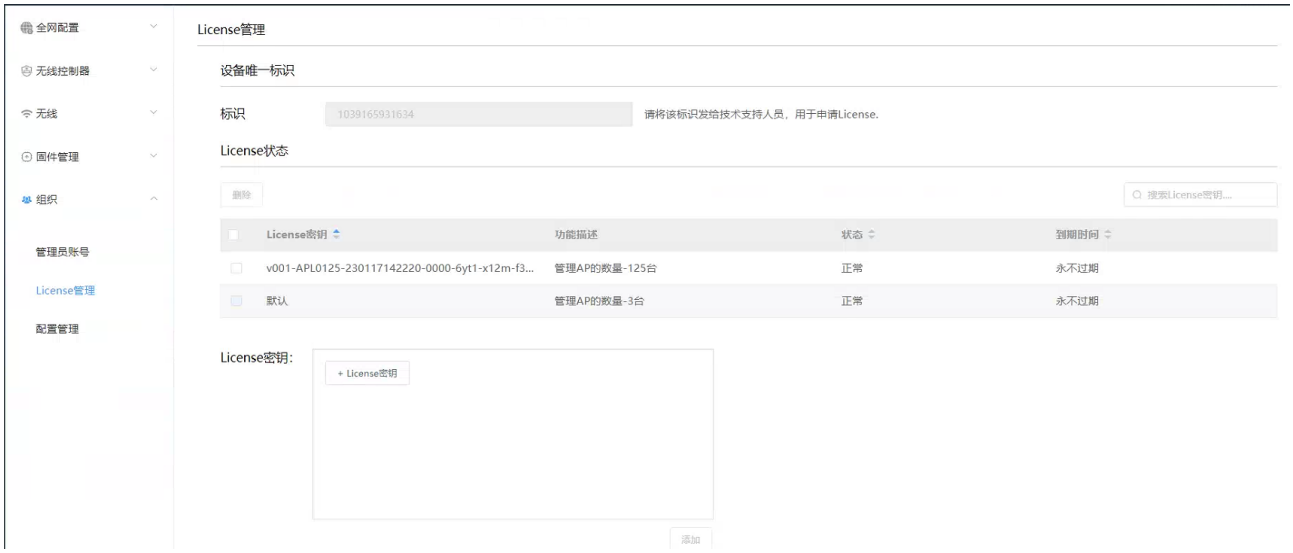
在密码超时前 3 天，开始提示密码即将过期，请及时修改密码。

过期后强制进入密码修改页面，要求用户修改密码，无法进入其他页面；修改保存后，使用新密码可以正常登录 web，正常进入其他 web 功能模块。

可访问 IP 地址：默认为空，不对可访问 ip 进行限制。

配置可访问 IP 地址后，客户端在可访问 ip 地址段内，则可以用账号密码登录 web，客户端地址不在可访问 IP 地址段，提示“设备登录位置异常，登录失败”。

【License 管理】菜单-主要功能是对 AC 进行管理 AP 数据的授权，通过设备唯一标识即 AC 的 device ID，向浪潮网络商务部获取授权，详见如下图所示：



【配置管理】菜单-主要功能是对 AC 业务功能配置进行导入导出，也可进行恢复出厂设置，详见如下图所示：

说明：

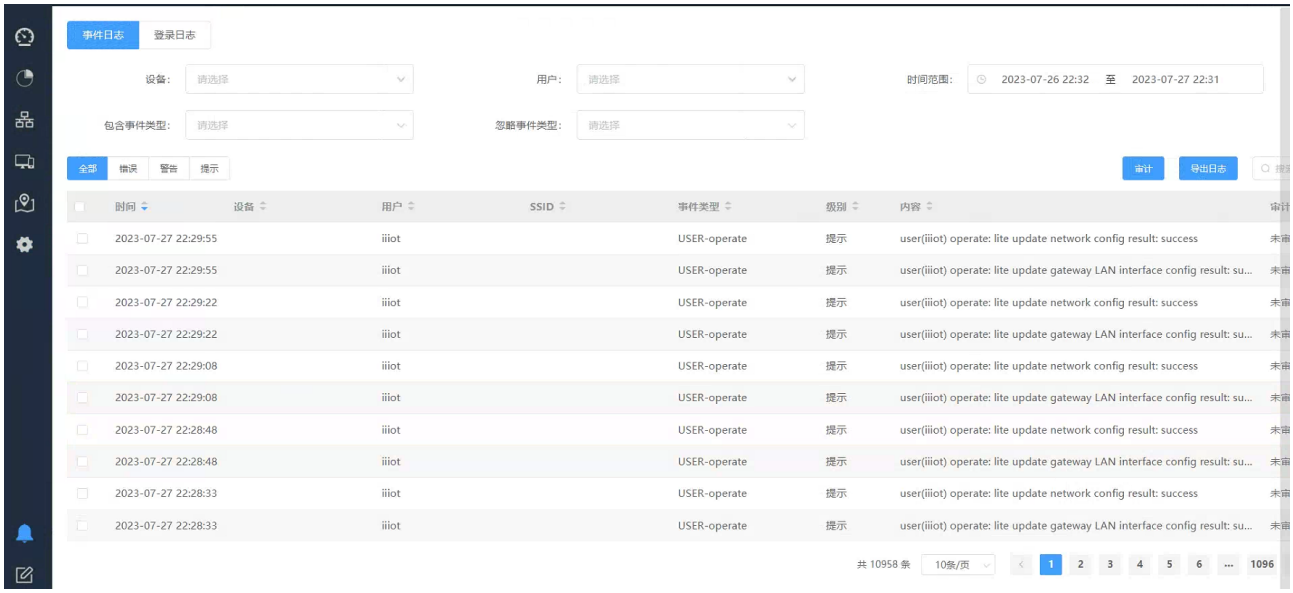
1） 当开局配置时，如遇到设备上有配置记录，建议先做恢复出厂操作，再进行开局的配置。

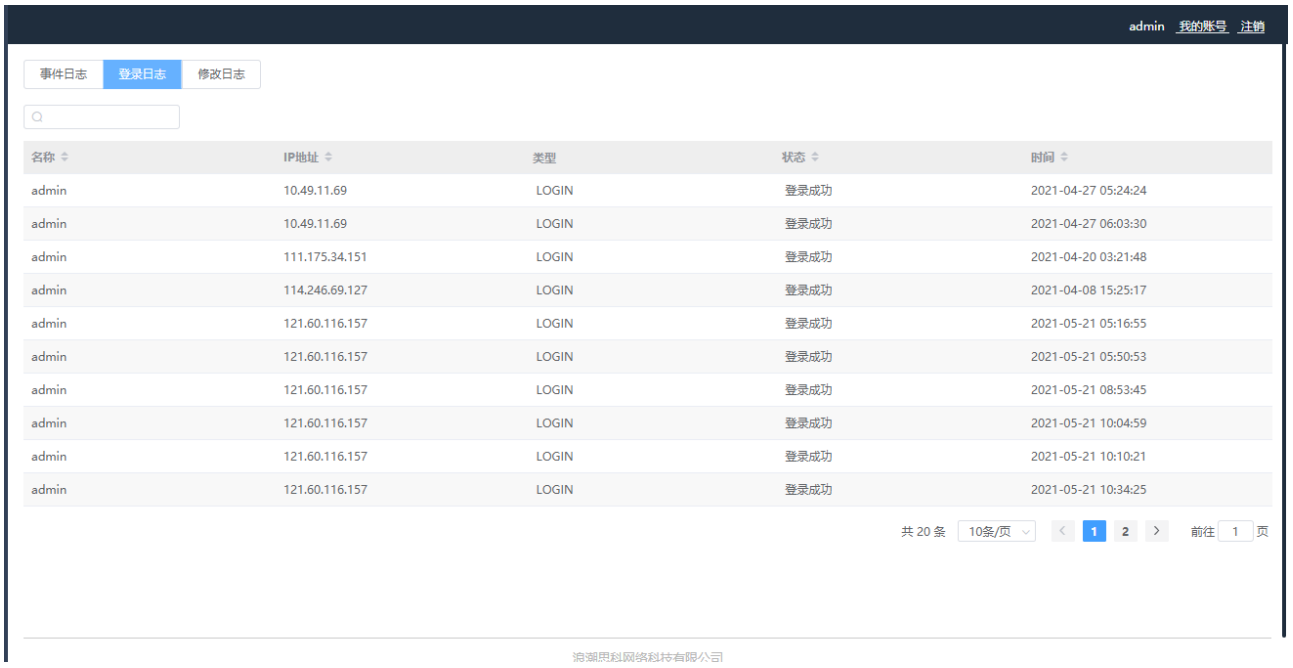
2.4.4 功能操作区

主菜单或子菜单中的功能配置或状态查询都在此区域完成，在每个菜单中进行详细介绍；

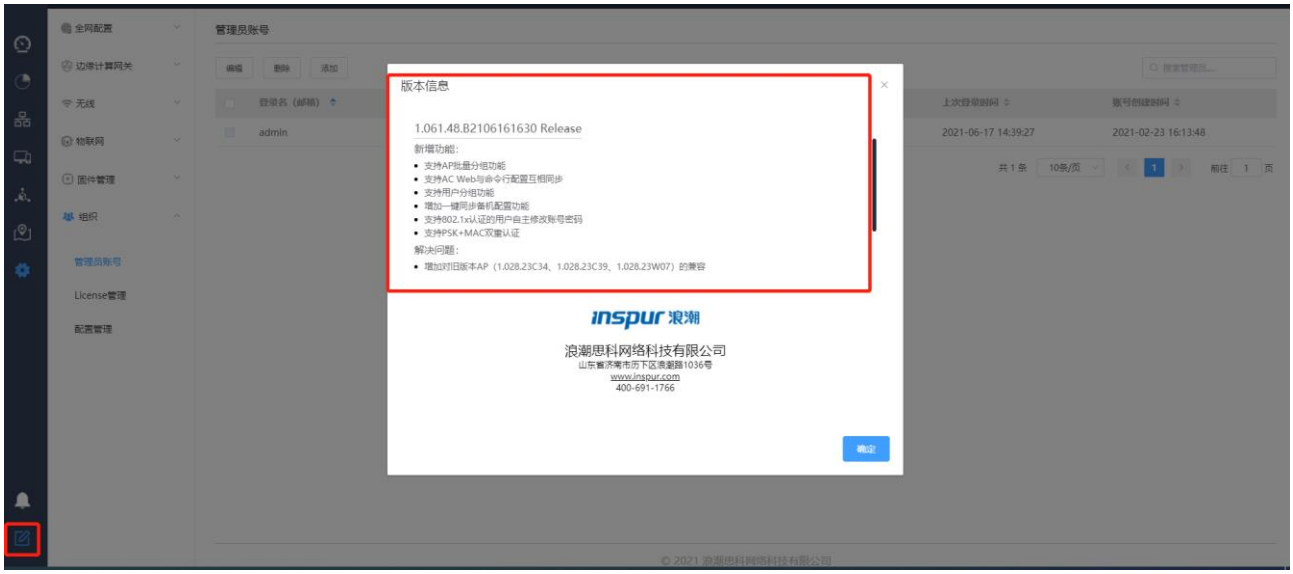
2.4.5 日志和提示功能区

主要分为日志查询和 Web 系统版本查询两个功能，通过<日志>按扭可对系统的事件、登录、修改等日志按不同维度进行查询，如下图所示：





通过<提示>按扭可对 Web 系统的版本进行查询，如下图所示：



2.5 配置命令介绍

2.5.1 基础配置命令

2.5.1.1 获得帮助

使用问号（？）和方向键，可以帮助输入命令：

■ 输入一个问号，获得当前可用的命令列表

XOS>?

■ 输入若干已知字符，紧接着输入问号（无空格），显示当前可用的已知字符开头的命令列表。

XOS>e?

■ 输入命令，紧跟空格和问号，获得命令参数列表

XOS#show ？

■ 按下 up 方向键，可显示前面输入的命令。

2.5.1.2 命令模式

AC 命令行界面可分为多种模式。每种命令模式允许在设备上配置不同的组件，当前可用的命令取决于所处的命令模式。输入问号（？）可以在每种命令模式下显示可用的命令列表。下表列出了常用的命令模式：

操作	进入方式	界面提示符	描述
用户模式	登录	XOS>	
特权模式	在用户模式下输入 enable 命令	XOS#	

全局配置模式	在特权模式下输入 configure terminal 命令	configure terminal	
端口配置模式	在全局配置模式下，输入 interface 命令，例如 interface eth2 可进入 eth2 端口；	XOS(config)#interface eth2 XOS(config-if)#	
进入 vlan 接口	在全局配置模式下，输入 interface 命令，例如 interface vlan1.2 可进入 vlan 2 接口	XOS(config)#interface vlan1.2 XOS(config-if)#	

2.5.1.3 撤销命令

如果想撤销一个命令或恢复为缺省属性，可以在大多数命令前加关键字 no。

例如，no ip dhcp pool

2.5.1.4 保存配置

在特权模式下使用 write 命令可以保存配置。

例如：

```
XOS#write
The current configuration will be written to the device. Are you sure? [Y/N]y
flash:/INSPUR.conf exists, overwrite? [Y/N]:y
Save configuration OK
```

2.5.2 设备管理命令

2.5.2.1 配置 VLAN 接口 IP

配置举例：配置 vlan3 接口 ip 为 192.168.3.1，掩码为 24 位。

```
XOS>enable
XOS# configure terminal      /*在特权模式下进入全局配置模式*/
XOS(config)#interface vlan1.3    /*在全局配置模式下，进入 vlan 3 接口配置模式*/
XOS(config-if)#ip address 192.168.3.1/24     /*在 vlan 3 接口配置模式下，vlan 3 的接口地址*/
```

2.5.2.2 NAT 配置

功能描述

NAT 功能可以根据指定的规则将报文的源地址或目的地址进行替换。这使得用私网地址组建的内网可以通过指定的公网地址访问外网，通过将源地址改为公网 IP 而减少 IP 地址的消耗和减少路由数量。反过来也可以让公网主机访问到私网内的指定主机。

配置 NAT

```
XOS>enable
XOS#configure terminal
XOS(config)#ip nat inside source list 4093 interface vlan1.4093 overload     //配置 NAT 规则
```

2.5.2.3 静态路由配置

功能描述

静态路由允许管理员在设备上配置静态路由信息。若没有特别指定的话，静态路由信息的优先级是除了直连路由外最高的，比动态路由信息具有更高的优先级。在小型网络中，配置静态路由可以为网络提供很好的稳定性。

配置静态路由

静态路由信息可以在配置视图下直接配置，但配置是否生效要根据配置是否满足下一跳 IP 是否在本地网段内和路由优选两个判断条件。此外静态路由配置命令支持为路由配置优先级。涉及以下命令

配置举例：

配置到网关 192.168.1.1 的默认路由。

```
XOS>enable
XOS#configure terminal
XOS(config)#ip route 0.0.0.0/0 192.168.1.1
```

2.5.2.4 端口配置

配置举例：将 eth2 口配置为 trunk 类型，允许通过的 vlan 为 1-9，默认 vlan 为 1。

```
XOS>enable
```

```
XOS#configure terminal
XOS(config)# interface eth2
XOS(config-if)# switchport mode trunk    //端口类型为 trunk
XOS(config-if)# switchport trunk allowed vlan add 1 to 9  //允许通过的 vlan
XOS(config-if)# switchport trunk pvid 1  //默认 vlan
```

2.5.3 WLAN 基本业务配置命令

2.5.3.1 终端在线状态

配置举例：查看所有终端状态

```
XOS>enable
XOS#show wlan client all
Total Number of Clients          : 1
 MacAddr         BSSID           IP              State        Online Time
 ------------------------------------------------------------------------------
 6c6a.7751.f586  1c88.795b.0031  10.110.33.93     Associated     49h33m46s
```

可查看终端的当前在线的终端数量、MAC 地址、所关联的 BSSID、终端的 IP 地址、关联状态、在线时间

2.5.3.2 WLAN 服务模板配置

配置举例：将 WLAN 服务模板 1 配置 ssid 名称为 test，限制 ssid 接入终端数为 50，psk 认证密码为 11111111，二层桥接（本地转发）模式，业务 vlan 为 3，开启 ssid 下行限速 10Mbps，上行限速 5Mbps。

```
XOS>enable
XOS#configure terminal
XOS(config)#wlan service-profile 1        //对应 web 上第一个 ssid
XOS(wlan-service-profile)#max-client-count 50 //限制 ssid 接入终端数（默认为 64）
XOS(wlan-service-profile)#service disable  //配置时应先去掉使能
XOS(wlan-service-profile)#ssid test             //ssid 名称
```

```
XOS(wlan-service-profile)#air-security-policy  wpa2-psk   //关联接入方式为预共享密钥 wpa2-
psk
XOS(wlan-service-profile)#cipher-suite ccmp          //加密类型
XOS(wlan-service-profile)#client-forwarding-mode local-data  //本地转发
XOS(wlan-service-profile)#pre-shared-key pass-phrase 11111111 //密钥
XOS(wlan-service-profile)#vlan-pool 3   //对应 WEB 中寻址和流量策略-VLAN 标记中配置的 VLAN
XOS(wlan-service-profile)#traffic-limit ssid-based inbound 5120   //上行限速 5Mbps ( ssid-
based 为每 ssid 限速 , user-based 为每终端宽带限速 )
XOS(wlan-service-profile)#traffic-limit ssid-based outbound 10240  //下行限速 10Mbps ( ssid-
based 为每 ssid 限速 , user-based 为每终端宽带限速 )
XOS(wlan-service-profile)#service enable //使能
```

2.5.3.3 DHCP 配置

配置举例：地址池名称为 vlan100，子网为 192.168.100.0/24，可分配 IP 地址段为 192.168.100.101-192.168.100.200，默认网关为 192.168.100.1，租约时间为 1 天，DNS 服务器为 114.114.114.114。

```
XOS>enable
XOS#configure terminal
XOS(config)#service dhcp  //开启 DHCP
XOS(config)#ip dhcp pool vlan100  //地址池名称
XOS(dhcp-config)#network 192.168.100.0/24   //子网
XOS(dhcp-config)#range 192.168.100.101 192.168.100.200   //可分配 IP 地址段
XOS(dhcp-config)#default-router 192.168.100.1  //默认网关
XOS(dhcp-config)#lease-time 1 0 0 0  //租约时间
XOS(dhcp-config)#dns-server 114.114.114.114  //DNS 服务器
```

2.5.3.4 射频配置

配置举例：针对型号为 IAP5820i-E、name 为 C0A66D01E500 的 AP，配置 2.4GHz 信道为 6，发射功率为 20dBm，5GHz 信道和发射功率为默认配置

```
XOS>enable

XOS#configure terminal

XOS(config)#wlan ap C0A66D01E500 model iap5820i-e apid 1 //包含 AP 名称、型号、apid

XOS(config)#mac-address c0a6.6d01.e500   //AP mac 地址为 mac-address c0a6.6d01.e500

XOS(wlan-ap)# radio 1 type 80211gn     //radio 1 为 2.4GHz 802.11gn

XOS(wlan-ap-radio)# channel 6       //信道为 6

XOS(wlan-ap-radio)# max-power 20 //发射功率为 20dBm(100mW)

XOS(wlan-ap-radio)# enable  //开启使能

XOS(wlan-ap-radio)# radio 2 type 80211ac    //radio 2 为 5GHz 802.11ac

XOS(wlan-ap-radio)#enable   //开启使能，信道和发射功率为自动
```

2.5.4 AP 管理配置命令

2.5.4.1 查看 AP 在线状态

配置举例：

```
XOS>enable

XOS#show wlan ap all     //可以查看当前 AP 在线状态

NA:Never Assoc NI:No Ip I:Idle  J:Join  ID:Image Download  C:Config
DC:Data Check  R:Running  RS:Reset  M:Master  S:Slave
Running/Total APs                    :0/2
ID   Name              MAC         IP             Model     Time      State
------------------------------------------------------------------------------
1    C0A66D01E500   c0a6.6d01.e500   192.168.1.191     iap5820i-e  1h0m0s      R/M
2    111111111111     1111.1111.1111       0.0.0.0        iap5820i-e  0h0m0s      NA
```

状态说明：

NA:Never Assoc　　//AP 未关联 AC
NI:No Ip　　//无 IP 地址

```
I:Idle                    //空闲状态，当前 AP 为离线状态
J:Join                    //CAPWAP 连接建立状态
ID:Image Download   //版本下载状态
C:Config                 //初始化配置下载状态
DC:Data Check         //数据校验状态
R:Running                //运行状态，表示 AP 与 AC 成功建立 CAPWAP 隧道
RS:Reset                 //不涉及
M:Master                 //主用状态，表示当前 AC 为 AP 的主 AC
S:Slave                  //备用状态，表示当前 AC 为 AP 的备 AC
```

2.5.4.2 重启 AP

配置举例：可以在 AC 的命令行中通过 clear wlan ap [all]|[name]命令重启所有 AP 或具体某个 AP。

```
XOS>enable

XOS#clear wlan ap all    //重启所有 AP

XOS#clear wlan ap name C0A66D01E500   //重启 Name 为 C0A66D01E500 的 AP
```

2.5.5 主备 AC 配置同步（WLAN 部分）

配置方法：登录主 AC，输入 hot-backup sync config 命令进行配置同步。

```
XOS>enable       //进入特权模式

XOS#hot-backup sync config   //下发配置同步操作指令
```

注意：

1、配置同步需要在主 AC 下进行

2、当前支持的配置同步内容：

（1）WLAN 配置同步（使能和关闭、外接 RADIUS 服务器认证方式时 mac 认证模板的增加、删除或修改）

（2）射频配置同步（信道、功率等）

（3）ap 配置同步（AP 的增加与删除）

2.5.1 常用的状态查询命令

1、查看 Device ID

```
XOS#show device id

Device ID:1039165640027
```

2、查看设备型号、MAC、SN 等信息

```
XOS#show device manuinfo
```

3、查看 License 许可数量

```
XOS#show license wlan
```

4、查看接口状态

```
XOS#show interface brief
```

5、查看设备运行状态

```
XOS#start-shell
~ # top  //可查看内存、CPU 使用情况
Mem: 770008K used, 2182620K free, 0K shrd, 2232K buff, 268044K cached
CPU:  0.0% usr  0.3% sys  0.0% nic 98.8% idle  0.0% io  0.3% irq  0.2% sirq
Load average: 0.00 0.00 0.00 1/90 19354
  PID  PPID USER     STAT   VSZ %VSZ CPU %CPU COMMAND
19354 19353 root     R     2564  0.0   0  0.3 top
```

2.5.2 常用的排障命令

1、抓包命令

操作方法：进入 start-shell，通过 tcpdump 命令抓包

示例：tcpdump -i eth2 -w target.pcap

(1)-i eth2 ： 只抓经过接口 eth2 的包

(2)-w target.pcap ： 保存成 pcap 文件，方便用 wireshark 分析

```
~ # tcpdump -i eth2 -w target.pcap
tcpdump: WARNING: eth2: no IPv4 address assigned
tcpdump: listening on eth2, link-type EN10MB (Ethernet), capture size 65535 bytes
^C107 packets captured
107 packets received by filter
0 packets dropped by kernel
```

(3)从 AC 本地取出抓包文件 target.pcap 到电脑本地，步骤如下：

- 第一步，在电脑本地搭建 tftp server，选择与 AC 可连通的本地网卡和文件保存的目录；
- 第二步，从 AC 侧输入收集日志至电脑本地的命令： tftp -pr [文件名] [电脑 IP]

  例如：tftp -pr target.pcap 192.168.1.135 ；

  （注：target.pcap 为 AC 本地需收集的文件名，192.168.1.135 为电脑侧 tftp server IP）

  导出后可通过 wireshark 软件分析抓包文件。

2、debug 日志信息收集

命令：

XOS#debug wlan all　　//开启 wlan 模块的 debug 功能（命令前加 no 可关闭 debug）

XOS#terminal monitor　//输出调试信息

以终端关联 psk 认证的 ssid 的过程为例：

```
XOS#debug wlan all
XOS#terminal monitor
XOS#2021/06/22 10:49:27 informational: WMAC_AC:  Receiving authention frame from station
f8:95:ea:a5:6f:5c.
2021/06/22 10:49:27 informational: WMAC_AC:  New STA
2021/06/22 10:49:27 informational: WMAC_AC:  Authentication OK (Open-System) with bssid
64:a3:41:ae:41:22 .
2021/06/22 10:49:27 errors          : WMAC_AC:  Receiving association request from sta
f8:95:ea:a5:6f:5c
2021/06/22 10:49:27 errors          : WMAC_AC:  Receiving association request from sta
f8:95:ea:a5:6f:5c, seq [0x807f]
2021/06/22 10:49:27 errors        : WMAC_AC:  IEEE 802.11 element parse ignored unknown
element (id=127 elen=8)
2021/06/22 10:49:27 errors        : WMAC_AC:  IEEE 802.11 element parse ignored unknown
element (id=191 elen=12)
2021/06/22 10:49:27 errors       : WMAC_AC:  Unknown vendor specific information element
ignored (vendor OUI 00:17:f2 len=11)
2021/06/22 10:49:27 errors       : WMAC_AC: Unknown Broadcom information element ignored
(type=4 len=5).
2021/06/22 10:49:27 errors       : WMAC_AC:  Unknown vendor specific information element
ignored (vendor OUI 00:10:18 len=9)
2021/06/22 10:49:27 informational: WMAC_AC:  Station association succeed with AID: 1, SSID:
Unconfiged SSID7, BSSID: 64:a3:41:ae:41:22.
2021/06/22 10:49:27 notifications: WMAC_AC:  [IPC] Sending ADD-STATION to AP by CAPWAP with
station MAC f8:95:ea:a5:6f:5c, AID 1 and APID 61 RID 2. assoseq [0x807f]
2021/06/22 10:49:27 informational: WMAC_AC:  STA f8:95:ea:a5:6f:5c - event 1 notification
2021/06/22  10:49:27  informational:  WMAC_AC:  Unauthorizing  port  for  station
f8:95:ea:a5:6f:5c.
2021/06/22 10:49:27 informational: WMAC_AC:  Sending 1/4 msg of 4-Way Handshake.
2021/06/22 10:49:27 informational: WMAC_AC:  Receiving EAPOL-Key frame (2/4 Pairwise) from
stationf8:95:ea:a5:6f:5c.
2021/06/22 10:49:27 notifications: WMAC_AC:  WPA: PTK derivation A1 : 64:a3:41:ae:41:22
A2 : f8:95:ea:a5:6f:5c
2021/06/22 10:49:27 informational: WMAC_AC:  Success to verify key MIC.
2021/06/22 10:49:27 informational: WMAC_AC:  Recving 2/4 msg of 4-Way Handshake
2021/06/22 10:49:27 informational: WMAC_AC:  Sending 3/4 msg of 4-Way Handshake
2021/06/22 10:49:27 informational: WMAC_AC:  STA f8:95:ea:a5:6f:5c - sending 3/4 msg of 4-
Way Handshake
2021/06/22 10:49:27 informational: WMAC_AC:  Receiving EAPOL-Key frame (4/4 Pairwise) from
stationf8:95:ea:a5:6f:5c.
2021/06/22 10:49:27 informational: WMAC_AC:  Updating station key for station f8-95-ea-a5-
6f-5c .
```

```
2021/06/22 10:49:27 notifications: WMAC_AC:  [IPC] Sending ADD-STATION to AP by CAPWAP with station MAC f8:95:ea:a5:6f:5c, AID 1 and APID 61 RID 2. assoseq [0x807f]
2021/06/22 10:49:27 informational: WMAC_AC:  Updateing group key for BSS 64-a3-41-ae-41-22 .
2021/06/22 10:49:27 notifications: WMAC_AC:  Updating WLAN Group key with key index 1.
2021/06/22 10:49:27 notifications: WMAC_AC:  [IPC] Sending UPDATE-WLAN to AP by CAPWAP with ssid Unconfiged SSID7 and APID 61.
2021/06/22 10:49:27 informational: WMAC_AC: AP-STA-CONNECTED f8:95:ea:a5:6f:5c
2021/06/22 10:49:27 informational: WMAC_AC: Authorizing port for station f8:95:ea:a5:6f:5c.
2021/06/22 10:49:27 informational: WMAC_AC:  STA f8:95:ea:a5:6f:5c - Pairwise key handshake completed (RSN)
```

3 开局向导

3.1 无线网络规划

无线项目开局前，与客户确定网络拓扑及网络规划，AC 通常旁挂在核心/汇聚交换机，由 DHCP 服务器提供 AP 及终端的 IP 地址。

配置项	规划说明
管理 VLAN	管理 VLAN 用于设备管理使用，建议和业务 VLAN 分开。
业务 VLAN	终端业务 VLAN，该 VLAN 在 SSID 中配置，可根据不同的业务划分多个不同的业务 VLAN。
AC 的源接口	VLANIF 管理_vlan：x.x.x.x/x（192.168.1.0/24）。 AC 上配置到网关的静态路由。
DHCP 服务器	通常由核心、汇聚、DHCP SERVER 等为 AP 和终端分配 IP 地址。
AP 的 IP 地址池	AP 的管理地址池规划：与 AC 同网段或跨三层（跨三层时需要在 DHCP 中配置 option43 选项）；智联中心 AP 不支持自动发现方式上线，需要在 DHCP 中配置 option43 选项或在智联中心 APWEB 页面手动填写 AC ip 地址。
STA 的 IP 地址池	终端的业务地址池规划，需充分考虑到可能连接的终端数量，预留足够的地址。
AC 接口配置	在 AC 上添加管理 VLAN 和业务 VLAN。 AC 与核心互联口：本地转发时透传管理 VLAN 即可；集中转发时需透传管理 VLAN 和业务 VLAN。

核心/汇聚接口配置	核心到汇聚的下口、汇聚到核心的上行口、汇聚到接入的下行口需透传管理 VLAN 和业务 VLAN。
POE 交换机接口配置	上行口透传管理 VLAN 和业务 VLAN。 下行口透传管理 VLAN 和业务 VLAN，native VLAN（或 pvid）为管理 VLAN。
SSID 规划	一般可分为内部办公、物联终端、运维及访客等几类，可根据不同的场景进行区分。 **要点：** 1、认证接入方式选择：本地 psk、本地 portal、本地 mac+psk、dot.1x、与第三方统一认证平台适配等。 2、转发方式的选择：一般建议选择本地转模式（业务流量不经过 AC），业务需要时才选择集中模式（业务流量经过 AC），一般选择集中转发时，需根据流量大小评估设备性能是否满足要求。 3、根据实际的业务场景对终端带宽进行限定。 4、对 AP 进行合理分组，选择相应的分组，下发匹配的 SSID。

3.2 配置 AP 上线

1、AC 侧局域网配置

路径：【设置】>子菜单【无线控制器】>子菜单【局域网】，进入“局域网配置”页面。

a、根据规划表，创建 AC 的管理 VLAN 及子网 IP、创建业务 VLAN

（注：当使用 Portal 认证方式时，需要为该业务 VLAN 配置子网 IP）

b、配置 AC 与核心/汇聚的互联端口，trunk 模式，透传管理 VLAN（本地转发方式时）

c、配置 AC 到网关的默认路由

2、核心\汇聚交换机配置

a、配置无线管理 VLAN、业务 VLAN 及地址池

b、配置与 AC 互联端口，trunk 模式，透传管理 VLAN

c、配置与 POE 交换机互联端口，trunk 模式，透传管理和业务 VLAN

3、POE 交换机配置

a、配置无线管理 VLAN、业务 VLAN

b、配置与核心\汇聚互联端口，trunk 模式，透传管理和业务 VLAN

c、配置连接 AP 的下行口，trunk 模式，透传管理和业务 VLAN，PVID 或 native vlan 配置为管理 VLAN

4、测试网络连通性

网络配置完成后，检查 AP 是否获取到管理 IP，测试 AP 与 AC 网络连通性

5、导入 AP

可通过模板批量导入 AP，若 AP 出厂版本较老而无法上线，核实 AC 版本是否低于 1.061.48，如低于可直接升级至 1.061.48 或以上版本即可完成 AP 上线，并可对 AP 进行批量升级。

MacAddr 格式为：xx:xx:xx:xx:xx:xx

Model 列的型号与单独添加 AP 时相同

Name/设备名称：3-64 characters/字符

Address/地址：6-300 characters/字符

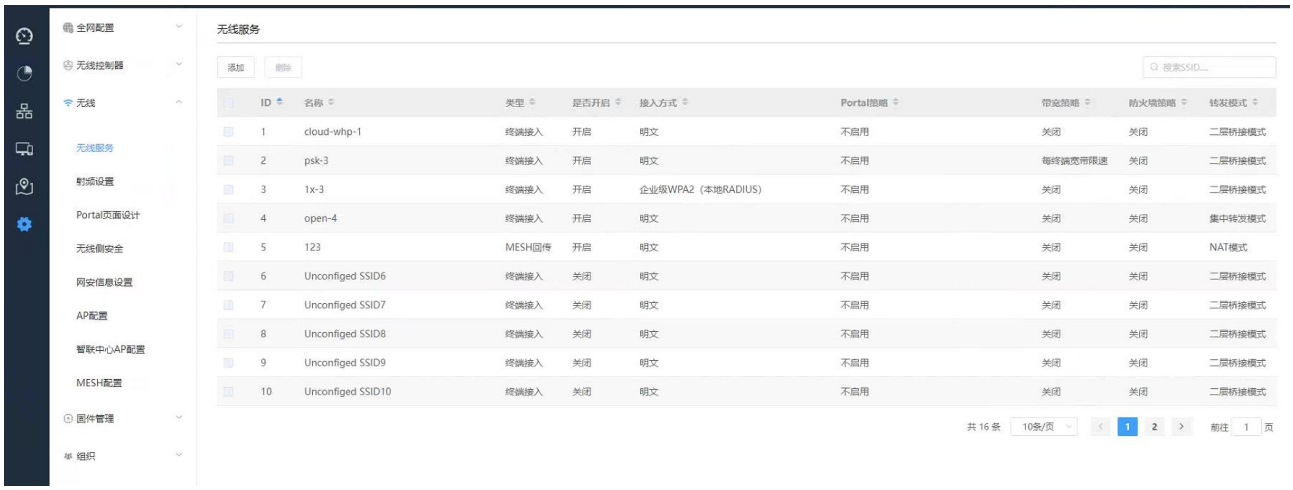
Notes/备注：6-300 characters/字符

AP 模板批量添加时需要注意：MacAddr 及 Model 为必填项，其余为可选项(设备名称建议可在此时统一命名后一并导入，)，导入成功后，会提示“批量导入设备至当前网络成功”，可在设备列表查看导入的设备。

	A	B	C	D	E
1	MacAddr	Model	Name/设备名称 (3-64 characters/字符)	Address/地址 (6-300 characters/字符)	Notes/备注 (6-300 characters/字符)
2	C0:A6:6D:12:8E:60	IAP5820i-E	09F-AP01		
3	C0:A6:6D:12:D5:00	IAP5820i-E	09F-AP02		
4	C0:A6:6D:12:D6:80	IAP5820i-E	09F-AP03		
5	C0:A6:6D:12:D1:40	IAP5820i-E	09F-AP04		
6	C0:A6:6D:12:CC:80	IAP5820i-E	09F-AP05		
7	C0:A6:6D:12:D4:80	IAP5820i-E	09F-AP06		
8	C0:A6:6D:12:D0:40	IAP5820i-E	09F-AP07		
9	C0:A6:6D:12:CB:60	IAP5820i-E	09F-AP08		
10	C0:A6:6D:12:AB:C0	IAP5820i-E	09F-AP09		
11	C0:A6:6D:12:B2:60	IAP5820i-E	09F-AP10		
12	C0:A6:6D:12:D7:80	IAP5820i-E	09F-AP11		
13	C0:A6:6D:12:AD:C0	IAP5820i-E	09F-AP12		
14	C0:A6:6D:12:AE:E0	IAP5820i-E	09F-AP13		
15	C0:A6:6D:12:90:A0	IAP5820i-E	09F-AP14		
16	C0:A6:6D:12:CD:80	IAP5820i-E	09F-AP15		

3.3 SSID 配置

路径：【设置】>子菜单【无线】>子菜单【无线服务】，进入 WLAN 业务配置页面，选择模板配置 SSID



1、认证接入方式选择

根据客户需求创建相应的认证接入方式，常见的认证接入方式有：

（1）预共享密钥，即本地 psk 认证

传统的使用场景

（2）本地 mac 认证

MAC 认证不需要用户安装任何客户端软件。设备在首次检测到用户的 MAC 地址以后，即启动对该用户的认证操作。认证过程中，也不需要用户手动输入用户名或者密码。

需要注意：使用 MAC 认证方式时，要求网络管理员必须明确网络中每个网络终端设备的 MAC 地址，并添加到 AC 中 MAC 认证用户信息的列表中；因此采用 MAC 认证对于网管员来说，其负担是相当重的，而且随着网络设备数量的不断扩大，它的维护工作量也不断加大。

（3）本地 mac+psk 认证

终端认证过程中需要进行本地 mac 和 psk 双重认证。

（4）本地 Portal 认证，包括一键登录、本地账号认证

在进行 Portal 认证方式时，终端会弹出 portal 页面，portal 页面上可以增加图片、url 跳转链接等自定义设置，因此，可以用于需要进行宣传的客户场景。

（5）本地 802.1x 认证

802.1x 认证方式在无线接入设备的射频端口这一级对所接入的无线用户进行认证和控制。连接在射频接口上的无线用户设备如果能通过认证，就可以连接无线网络并访问网络中的资源;如果不能通过认证，则无法连接无线网络和访问网络中的资源。

适用于对更加关注无线安全的场景，如员工内部办公网络等。

（6）对接外部认证：企业微信认证、基于企业微信的二维码访客认证、短信认证、与第三方认证平台对接（城市热点、ISE）、第三方 RADIUS 服务器

2、转发方式选择

（1）一般建议选择本地转发方式（即二层桥接模式，业务流量不经过 AC）

（2）当业务需要时才选择集中转发方式（业务流量经过 AC）。

（3）VALN 标记包含如下 4 个选项：

不使用 VLAN 标记//终端获取 AP 管理 VLAN 的 IP；

使用预配置 VLAN 标记//配置业务 VLAN

使用基于 IP 的 VLAN 标记//可以添加基于 IP 段与 VLAN 的映射表；

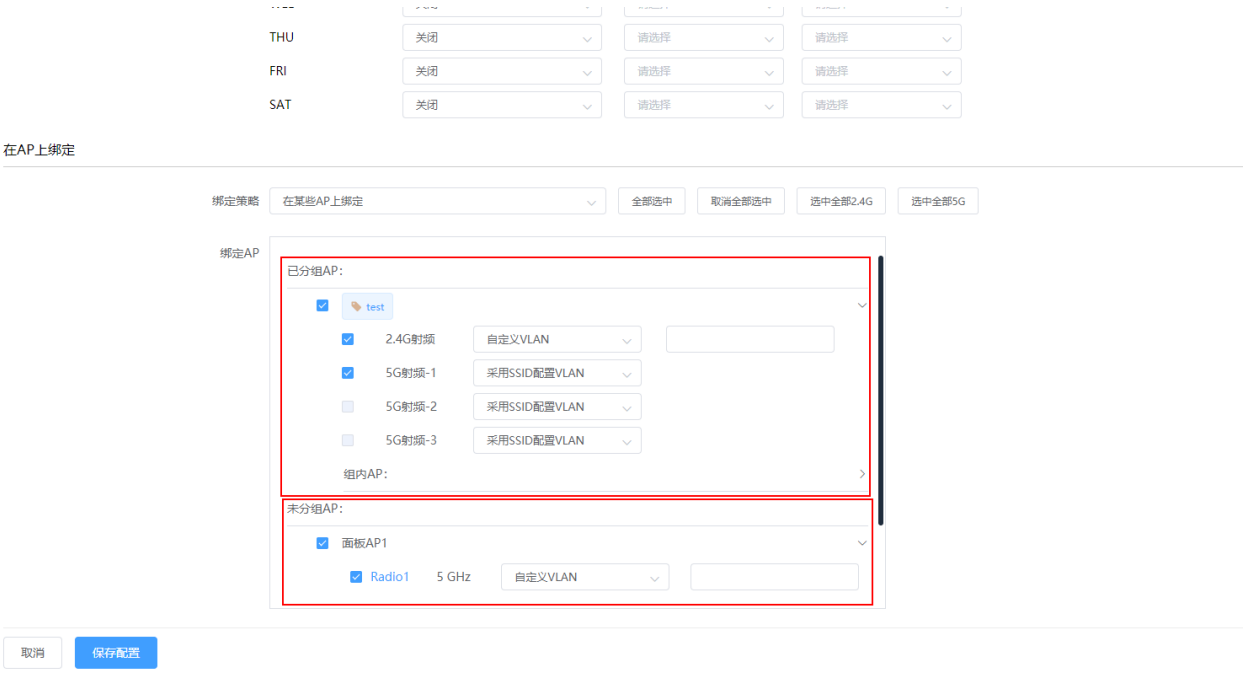
使用基于 MAC 的 VLAN 标记//可以添加基于 MAC 的 VLAN 模板。

（4）DHCP 转发方式：今针对 Portal 认证方式生效，当 DHCP 转发方式为本地转发模式时，DHCP 报文由 AP 转发；为集中转发模式时，DHCP 报文由 AC 转发。DHCP 集中转发一般应用于总部 AC+分支 AP 组网，分支机构的终端通过专线集中到总部获得地址的场景。

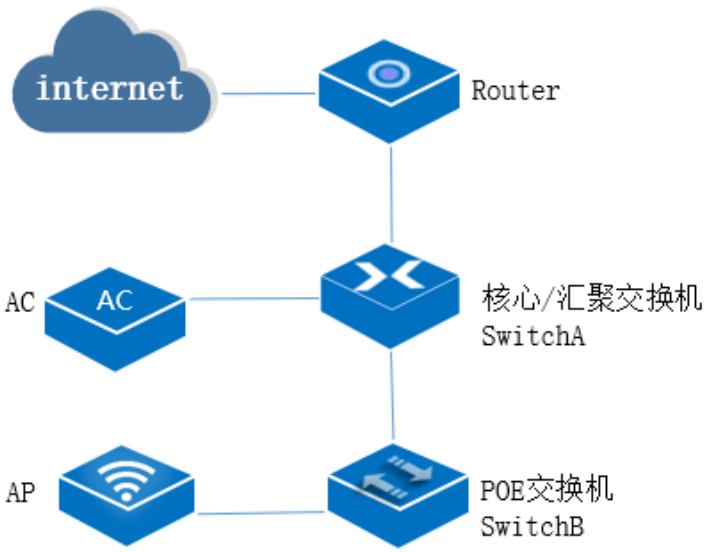
（5）限速配置：“服务质量”带宽策略默认为关闭，当选择开启后，可配置基于每 SSID 或每终端的带宽限速，可根据需求选择是否限速

（6）绑定 AP

当选择在某些 AP 上绑定时，可以绑定某个分组或其他未分组的 AP，可以基于 2.4G 射频或 5G 射频自定义 VLAN，将 VLAN 绑定到 AP 的射频上，该 VLAN 优先级高于 SSID 上绑定的 VLAN，详见如下图所示：



4 配置示例



拓扑示意图

本次配置以上图拓扑为例：

- AC 组网方式：旁挂二层组网。
- DHCP 部署方式：SwitchA 作为 DHCP 服务器为 AP 和 STA 分配 IP 地址。
- 业务数据转发方式：本地转发。

网络规划

配置项	规划数据

管理 VLAN	VLAN100
业务 VLAN	VLAN101
AC 的源接口	VLANIF100：192.168.100.2/24
DHCP 服务器	SwitchA 作为 DHCP 服务器为 AP 和 STA 分配 IP 地址
AP 的 IP 地址池	192.168.100.10～192.168.100.20/24
STA 的 IP 地址池	192.168.101.10～192.168.101.20/24
第三方 RADIUS 服务器参数	IP 地址：192.168.1.11 认证端口号：1812 计费端口号：1813 共享密钥：123456
第三方 LDAP 认证服务器参数	IP 地址：192.168.1.168 **端口号**：389 通用服务器路径：CN=Users,dc=inspur,dc=local 用户标识：windows server 使用 cn 用户名：dcao@inspur.local 密码：12345678
SSID 名称	SSID 名称：test

预置条件：

- 配置 AP、AC 和周边网络设备之间实现网络互通。
- 配置 AC 局域网，创建管理 VLAN 和业务 VLAN
- 配置 AP 在 AC 上线。

4.1 本地 MAC 认证

4.1.1配置 SSID

路径：【设置】>子菜单【无线】>子菜单【无线服务】，进入 WLAN 业务配置页面，选择模板配置 SSID

SSID 名称为：test

使能：开启

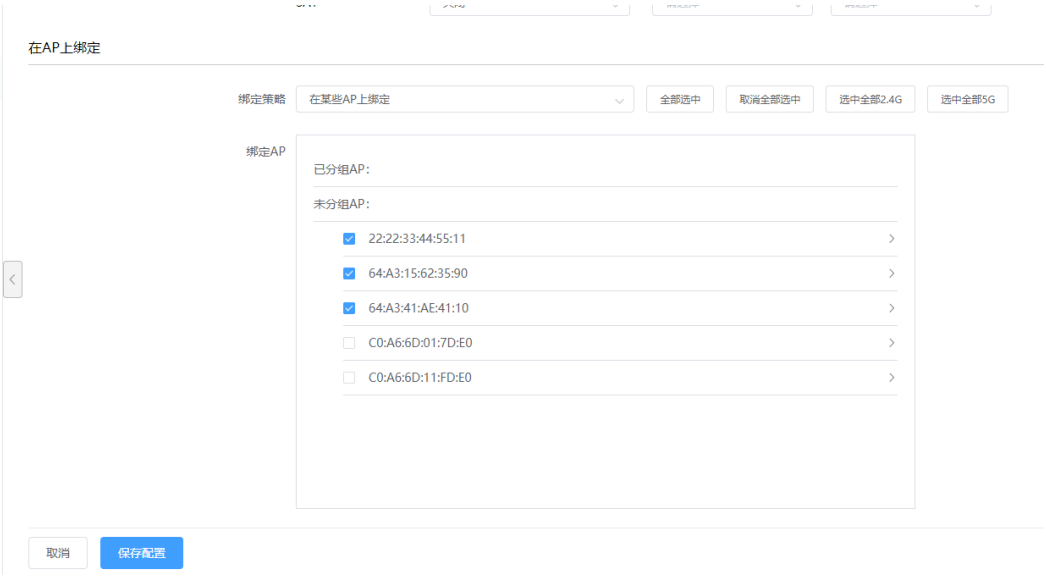
是否隐藏 SSID：广播 SSID

关联接入方式：MAC 认证（不加密）-本地 RADIUS 服务器

数据转发方式：二层桥接模式（本地转发模式）

VLAN 标记：使用预置 VLAN 标记-101

选择要绑定的 AP 并保存



4.1.2MAC 用户配置

✧ 配置认证策略模板：创建授权 MAC 认证的模板，用户组/用户可绑定该模板。

路径:【设置】>子菜单【全网配置】>子菜单【用户管理】>子菜单【认证策略模板】><添加模板>

模板名称：可自定义

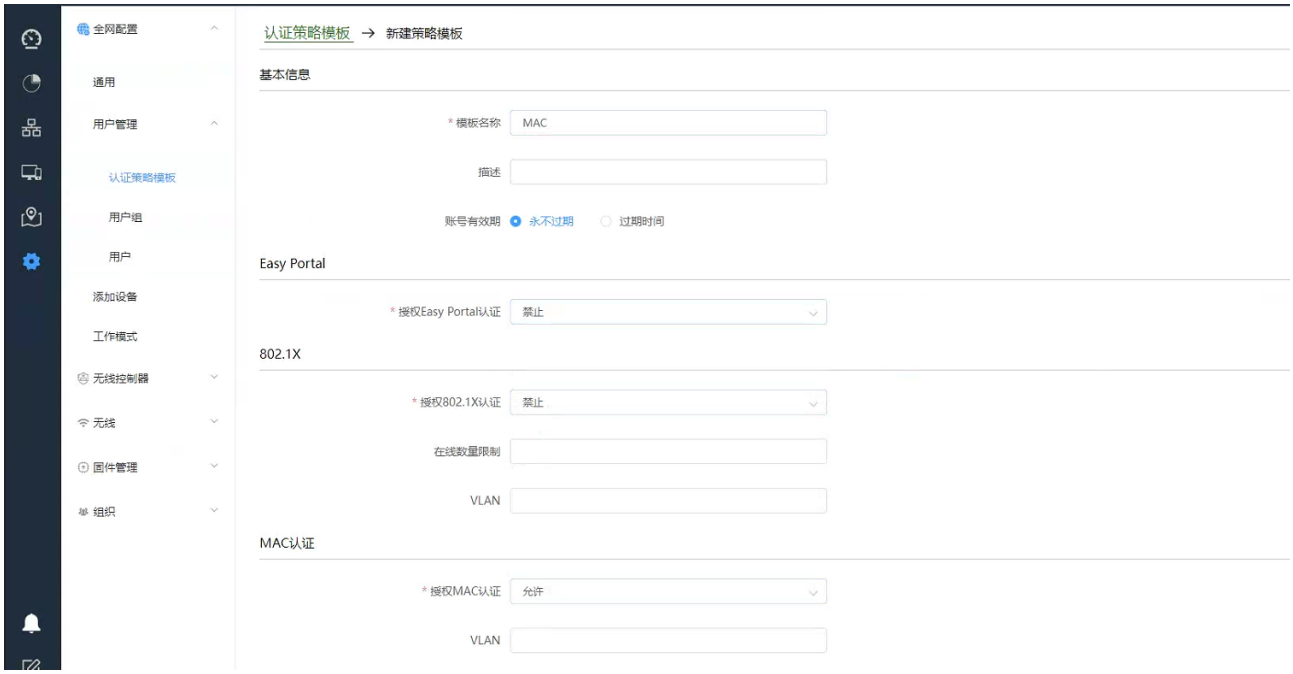
描述：可自定义

账号有效期：可选择永不过期或设置过期时间

Easy Portal 和 802.1X 选择禁止授权

MAC 认证：选择允许并保存

VLAN：优先级高于 SSID 中设置的 VLAN；若为空，则使用 SSID 中配置的 VLAN（本例为空）。



✧ 配置用户组：用户组上可绑定认证策略模板及 SSID

路径：【设置】>子菜单【全网配置】>子菜单【用户管理】>子菜单【用户组】><添加一级用户组>

用户组名：可自定义

描述：可自定义

SSID 认证策略：选择上一步创建的认证策略模板（MAC）及要绑定的 MAC 认证的 SSID（test）

同步更新本用户组中的用户：选中后，会将本用户组中的认证策略模板和绑定的 SSID 同步到该用户组的所有用户。

点击<保存配置生效>

✧ 添加用户：添加 MAC 认证用户

路径：【设置】>子菜单【全网配置】>子菜单【用户管理】>子菜单【用户】

SSID：在 SSID 下拉菜单选择 test 的 SSID

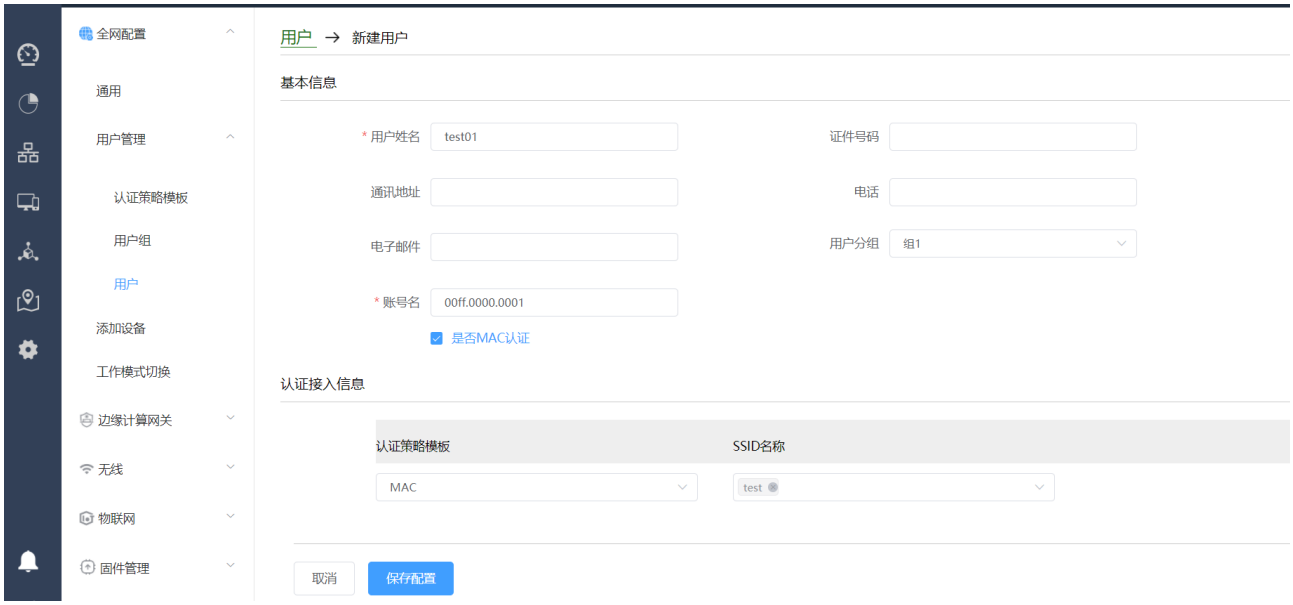
点击<添加用户>可添加单个用户；击<下载模板>，可通过模板批量导入用户

本例点击<添加用户>，弹出如下配置页面：

在用户姓名栏填写用户姓名；

在账号名栏填写终端 MAC 地址（MAC 地址格式为 xxxx.xxxx.xxxx，字母为小写）；

选择用户分组-组 1，认证接入信息会自动变为组 1 中绑定的认证策略模板（MAC）和 SSID（test），点击<保存配置>生效



4.1.3检查配置结果

完成配置后，用户可通过无线终端搜索到 SSID 为 test 的无线网络。

已绑定 MAC 的终端可关联到该无线网络。

未绑定 MAC 的终端无法关联到该无线网络。

4.2 MAC 认证（不加密）-外接 RADIUS 服务器

4.2.1配置第三方认证服务

配置认证域

路径:【设置】>子菜单【无线控制器】>子菜单【第三方认证服务】>【RADIUS 认证服务器配置】点击<新建认证域>

输入认证域“名称”，在 MAC 鉴权接入服务器栏选择“添加一个 Radius 服务器模板”，输入第三方服务器的地址、端口号和密钥，NAS-IP 为设备发送 RADIUS 报文使用的源地址，若未指定源地址，则使用发送 RADIUS 报文的接口地址，用户名携带格式与第三方认证服务器一致，本例选择保留原有域，点击<确定>

选择刚才创建的 Radius 服务器模版并保存配置，完成第三方服务器认证域配置。

4.2.2配置 SSID

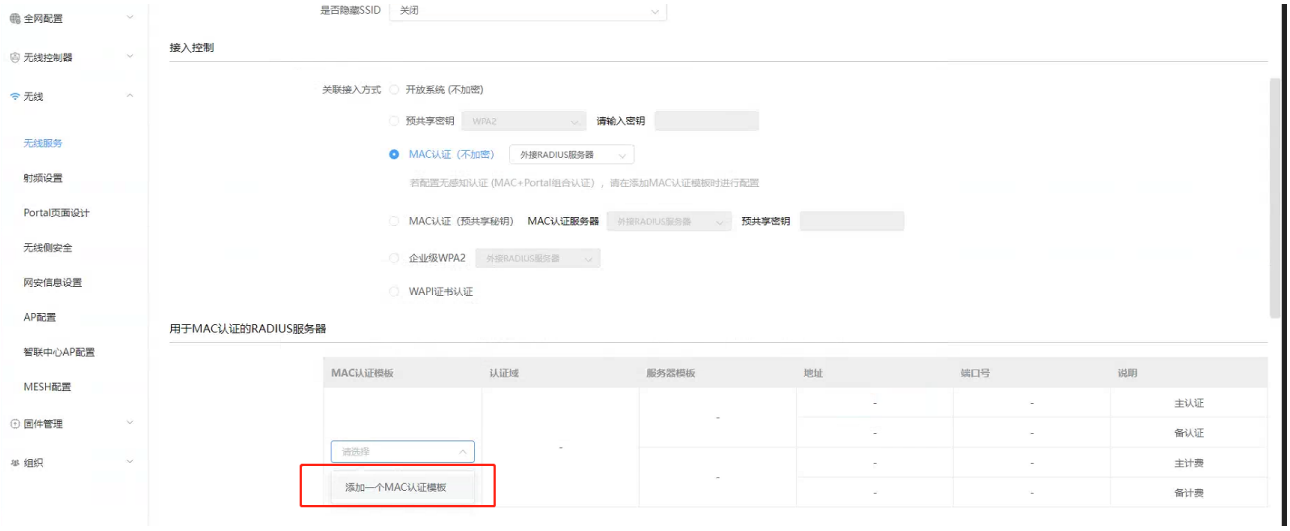
路径：【设置】>子菜单【无线】>子菜单【无线服务】，进入 WLAN 业务配置页面，选择模板配置 SSID

SSID 名称为：test

使能：开启

是否隐藏 SSID：广播 SSID

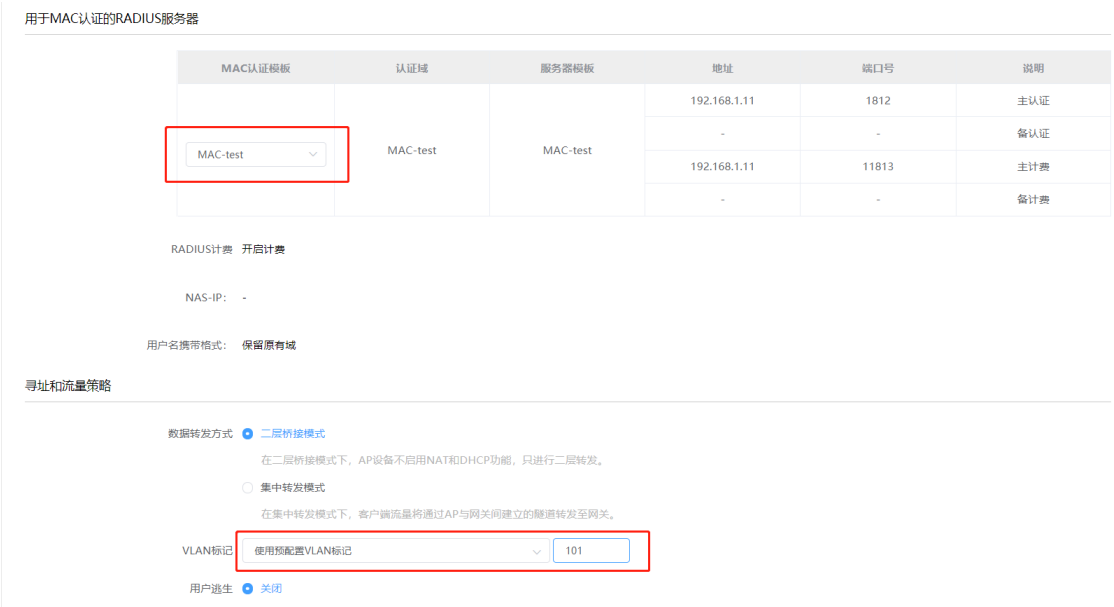
关联接入方式：MAC 认证（不加密）-外接 RADIUS 服务器，在“用于 MAC 认证的 RADIUS 服务器”栏“MAC 认证模板”列选择<添加一个 MAC 认证模板>



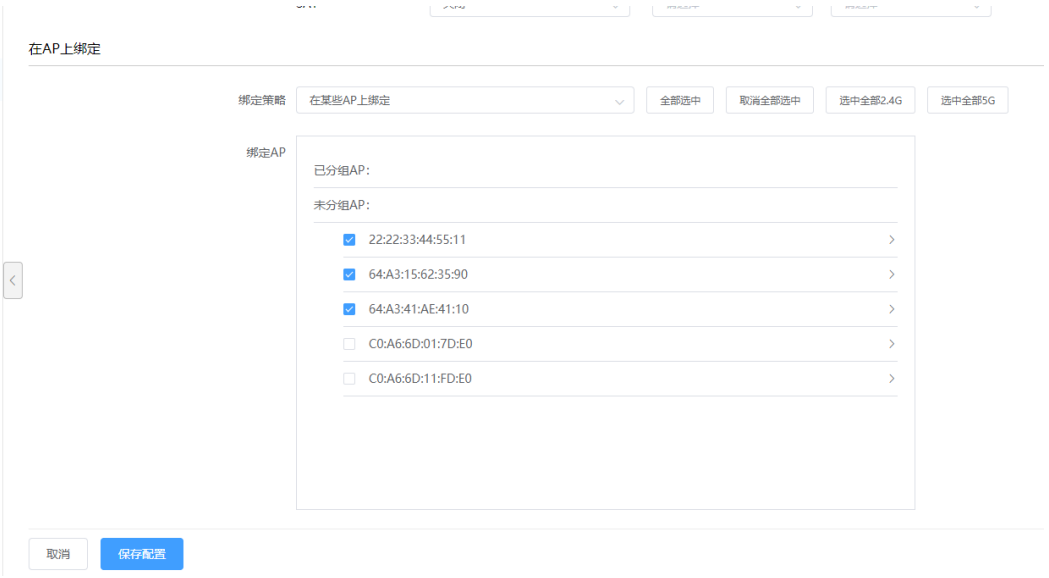
输入模板名称，选择刚才创建的 MAC-test 的 MAC 认证域，点击<确定>

数据转发方式：二层桥接模式

VLAN 标记：使用预置 VLAN 标记-101



选择要绑定的 AP 并保存



4.2.3检查配置结果

完成配置后，用户可通过无线终端搜索到 SSID 为 test 的无线网络。

第三方 RADIUS 服务器上已绑定 MAC 的终端可关联到该无线网络。

第三方 RADIUS 服务器上未绑定 MAC 的终端无法关联到该无线网络。

4.3 MAC 认证（不加密）- LDAP 服务器

4.3.1配置第三方认证服务

1、AC 上 LDAP 参数配置

路径:【设置】>子菜单【无线控制器】>子菜单【第三方认证服务】>【LDAP 认证服务器配置】

主/备服务器：可以是 IP 地址或域名，本例为：192.168.1.168

端口号：默认 389 主备必须相同（freeradius 限制）

通用服务器路径：用户搜索的基本路径，本例为：CN=Users,DC=inspur,DC=local

用户标识：openLDAP 使用 uid，windows server 使用 cn，本例为：cn

分组标识：openLDAP 使用 posixGroup(openldap)，windows server 使用 Group(windows ad)

用户名：管理用户，用户加域名后缀，本例为：dcao@inspur.local

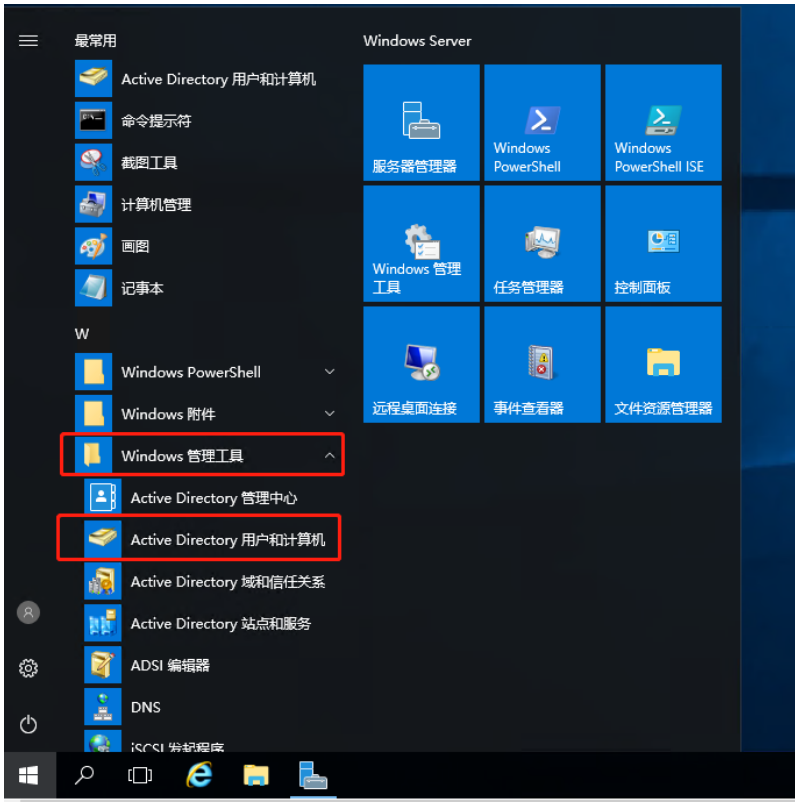
密码：管理用户的密码，本例为：12345678

Windows2000 前域名：可以选择保留原有域名和不携带域名

2、LDAP 相关配置

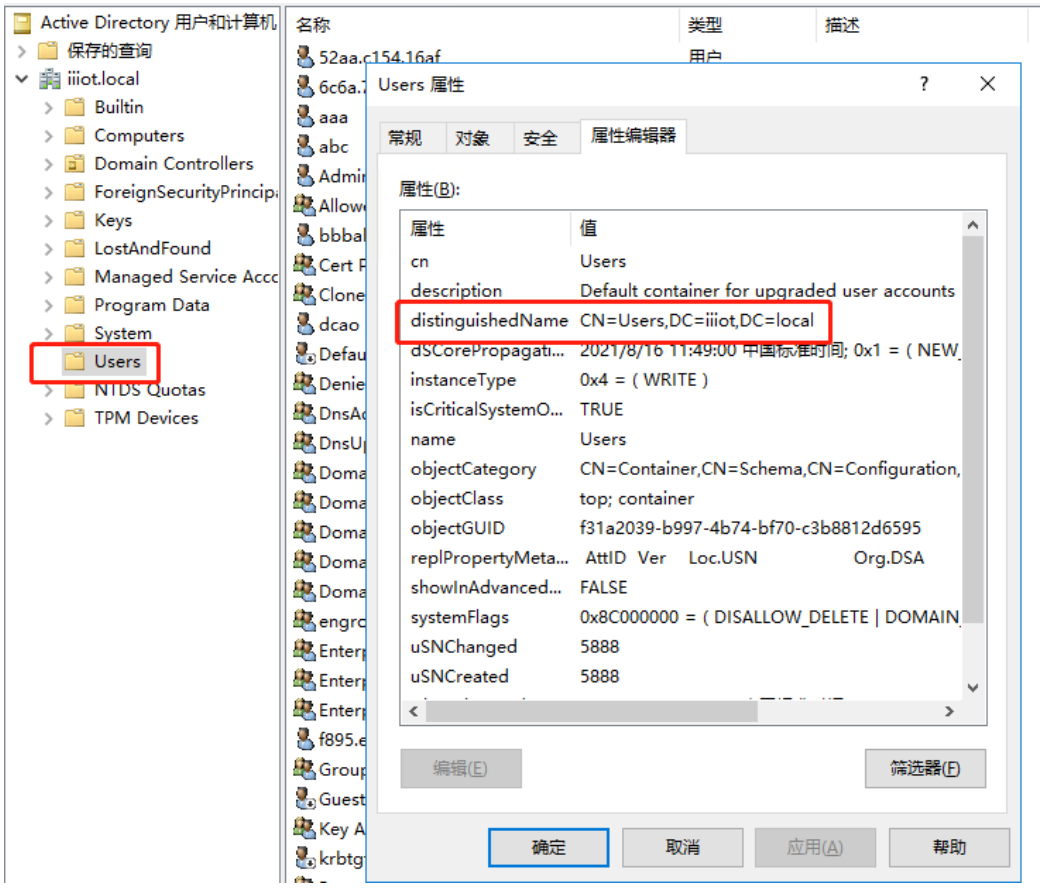
（1）通用服务器路径查看方法：

1） 通过菜单打开 AD 的用户管理



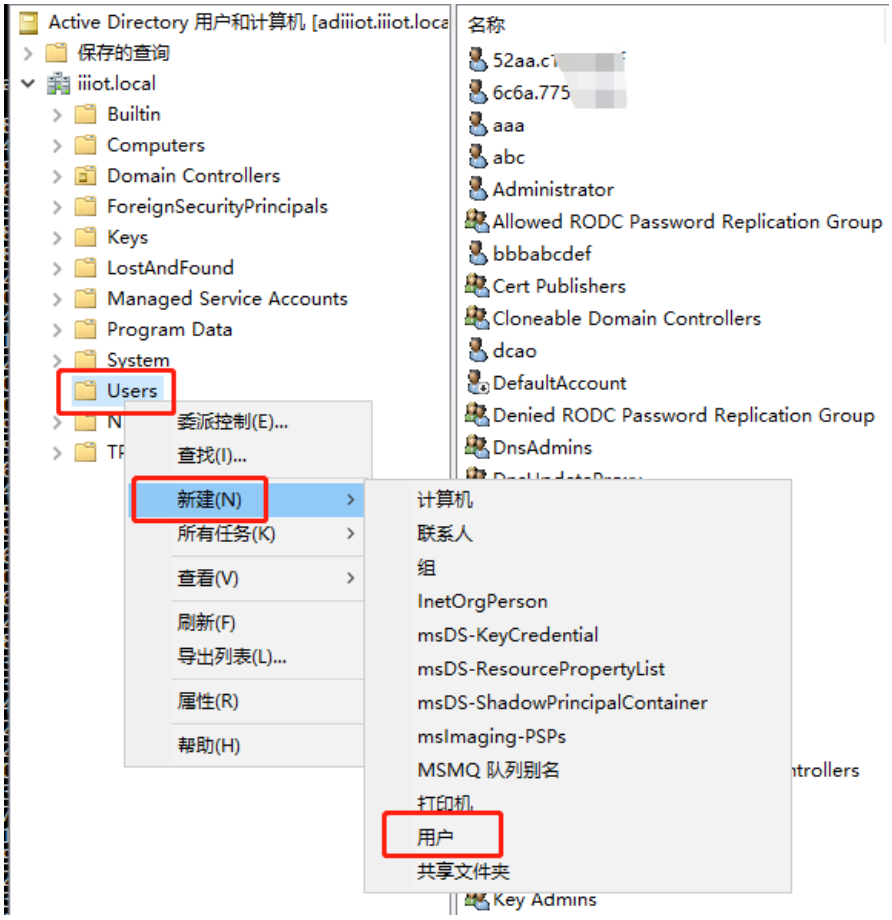
2) 在用户所属组上点击右键，选择属性出现以下对话框，可以看到通用搜索路径。为了提高效率在明确用户组的情况下可以从用户组开始，本例为：CN=Users,DC=inspur,DC=local。

如果不明确用户在哪个组，可以从下一级开始，例如，DC=inspur,DC=local



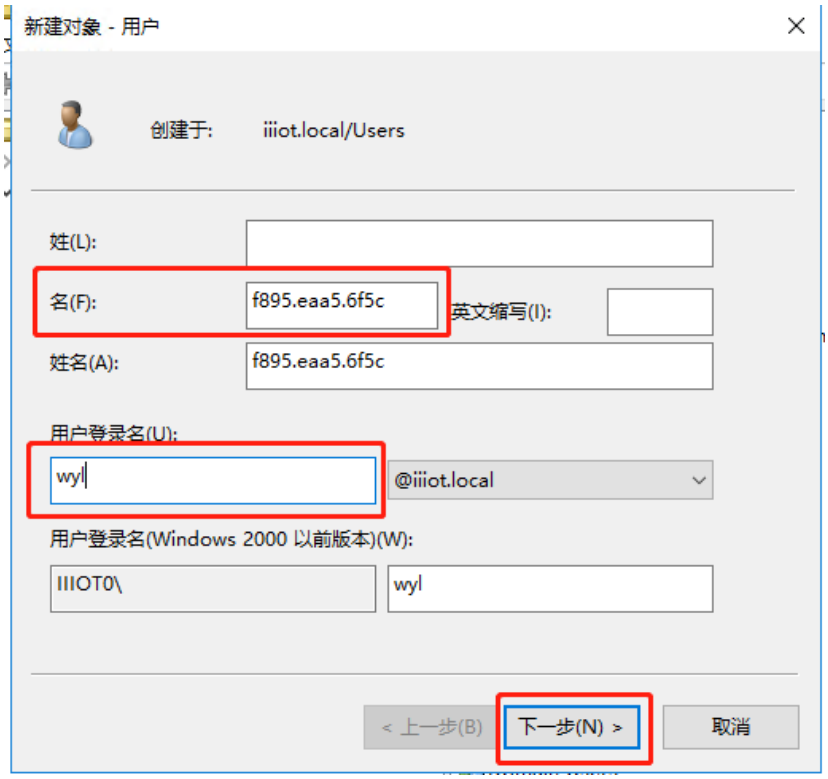
（2）认证用户的添加

1） 在 users 目录上点击右键，新建用户



2） 填写用户信息

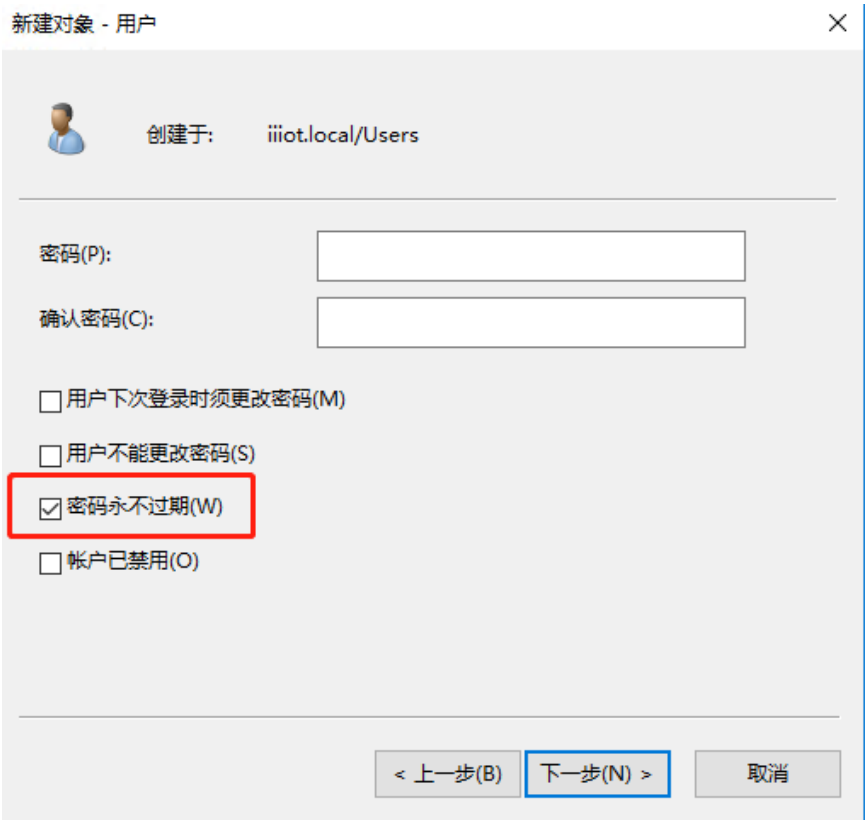
名（F）处填写 MAC 认证的用户名，格式为 xxxx.xxxx.xxxx



3） 选择密码策略为永不过期

MAC 认证的密码格式如下：

密码：f8-95-ea-a5-6f-5c



4.3.2配置 SSID

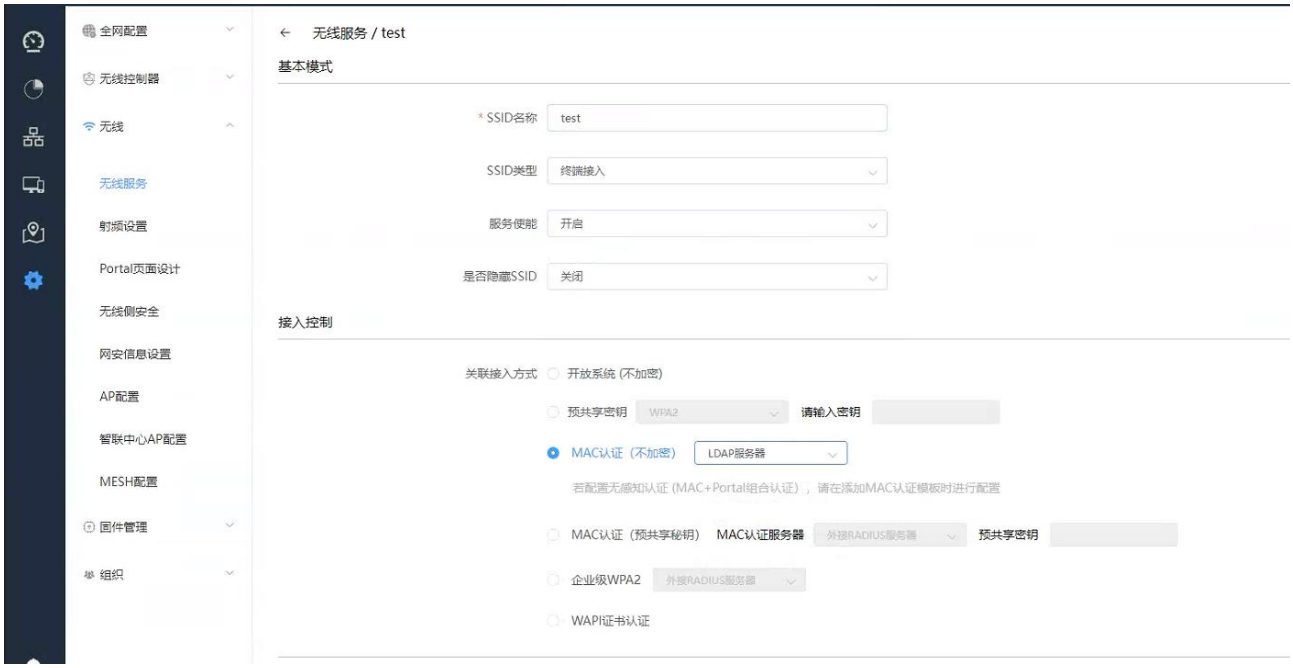
路径：【设置】>子菜单【无线】>子菜单【无线服务】，进入 WLAN 业务配置页面，选择模板配置 SSID

SSID 名称为：test

使能：开启

是否隐藏 SSID：广播 SSID

关联接入方式：MAC 认证（不加密）-LDAP 服务器



数据转发方式：二层桥接模式

VLAN 标记：使用预置 VLAN 标记-101

选择要绑定的 AP 并保存

4.3.3 检查配置结果

完成配置后，用户可通过无线终端搜索到 SSID 为 test 的无线网络。

LDAP 服务器上已添加 MAC 的终端可关联到该无线网络。

LDAP 服务器上未绑定 MAC 的终端无法关联到该无线网络。

4.4 MAC 认证（预共享密钥）

即预共享密钥与 MAC 双重认证，终端在进行认证时，先进行预共享密钥认证，再进行 MAC 认证（其中 MAC 认证支持外接第三方 RADIUS 服务器或使用 AC 内置的本地 RADIUS 服务器）。

4.4.1 配置 SSID

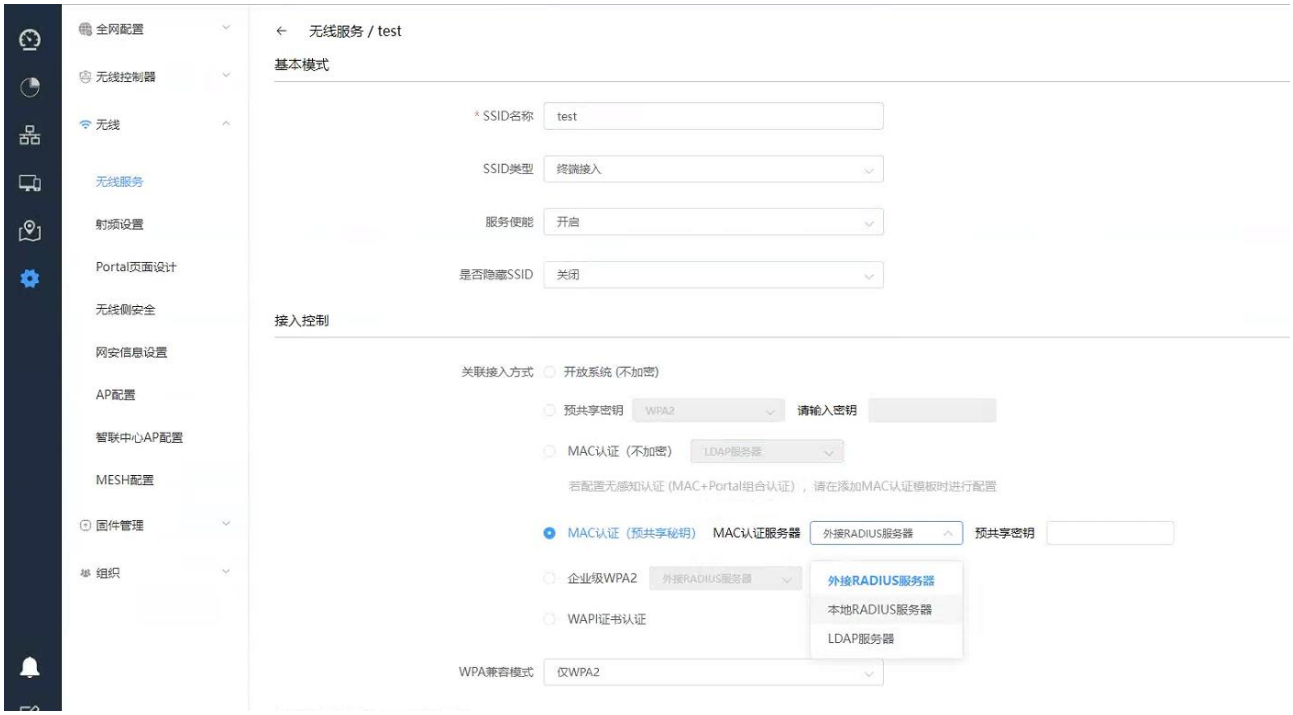
路径:【设置】>子菜单【无线】>子菜单【无线服务】，进入 WLAN 业务配置页面，选择模板配置 SSID

SSID 名称为：test

使能：开启

是否隐藏 SSID：广播 SSID

关联接入方式：MAC 认证（预共享密钥），可选择本地 MAC 认证或外接第三方 MAC 认证服务器，预共享密钥框输入密码。



选择本地 RADIUS 服务器时 SSID 配置及 MAC 用户配置方式参考“本地 MAC 认证”章节

选择外接 RADIUS 服务器时第三方认证服务器配置及 SSID 配置参考“MAC 认证（不加密）-外接 RADIUS 服务器”章节

选择 LDAP 服务器时 LDAP 配置参考“4.3 MAC 认证（不加密）- LDAP 服务器”章节

4.4.2 检查配置结果

完成配置后，用户可通过无线终端搜索到 SSID 为 test 的无线网络。

已绑定 MAC 的终端输入正确的密码后可关联到该无线网络。

未绑定 MAC 的终端即使输入正确的密码页无法关联到该无线网络。

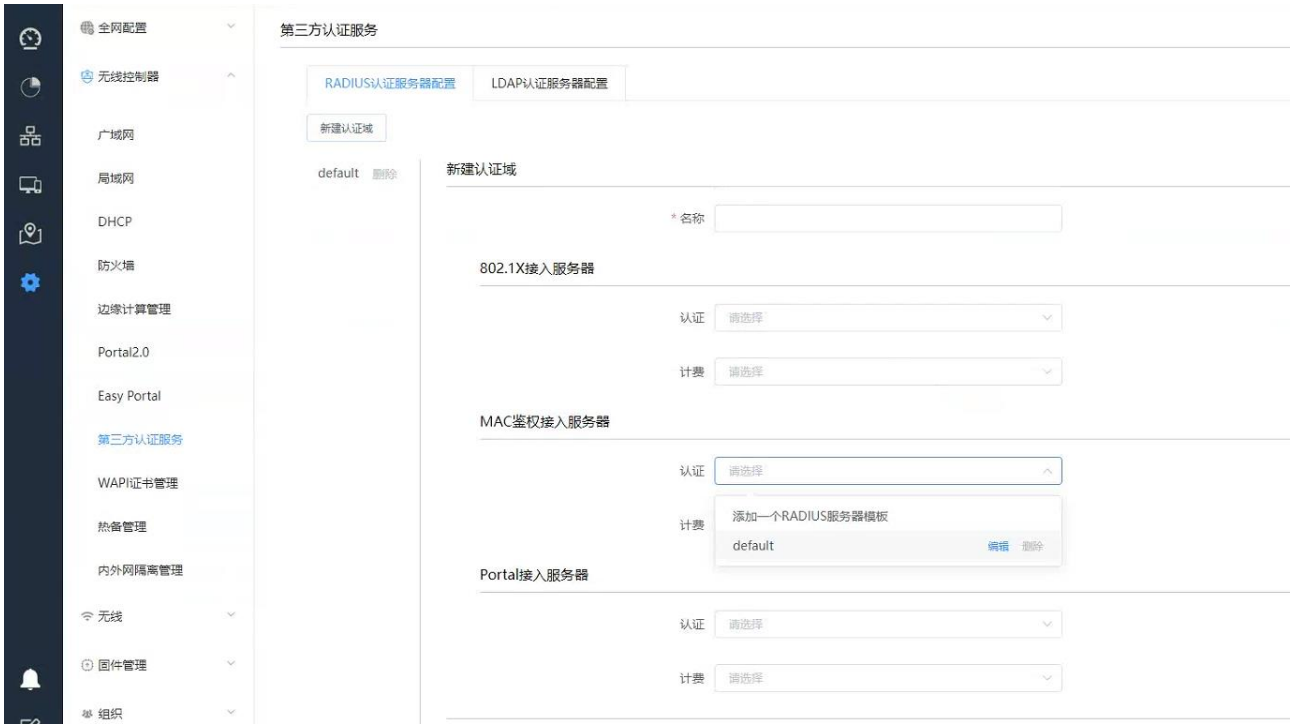
4.5 对接 Cisco ISE 的无感知认证(MAC+Portal 组合认证)

4.5.1 配置第三方认证服务

配置认证域

路径:【设置】>子菜单【无线控制器】>子菜单【第三方认证服务】>点击<新建认证域>

✧ MAC 鉴权接入服务器配置



输入认证域“名称”，在 MAC 鉴权接入服务器栏选择“添加一个 Radius 服务器模板”，输入第三方服务器的地址、端口号和密钥，用户名携带格式与第三方认证服务器一致，本例选择保留原有域，点击<确定>

选择刚才创建的 Radius 服务器模版并保存配置。

注：Cisco ISE 认证服务器上的配置可参考 ISE 相关手册

4.5.2 配置 SSID

路径：【设置】>子菜单【无线】>子菜单【无线服务】，进入 WLAN 业务配置页面，选择模板配置 SSID

SSID 名称为：test

使能：开启

是否隐藏 SSID：广播 SSID

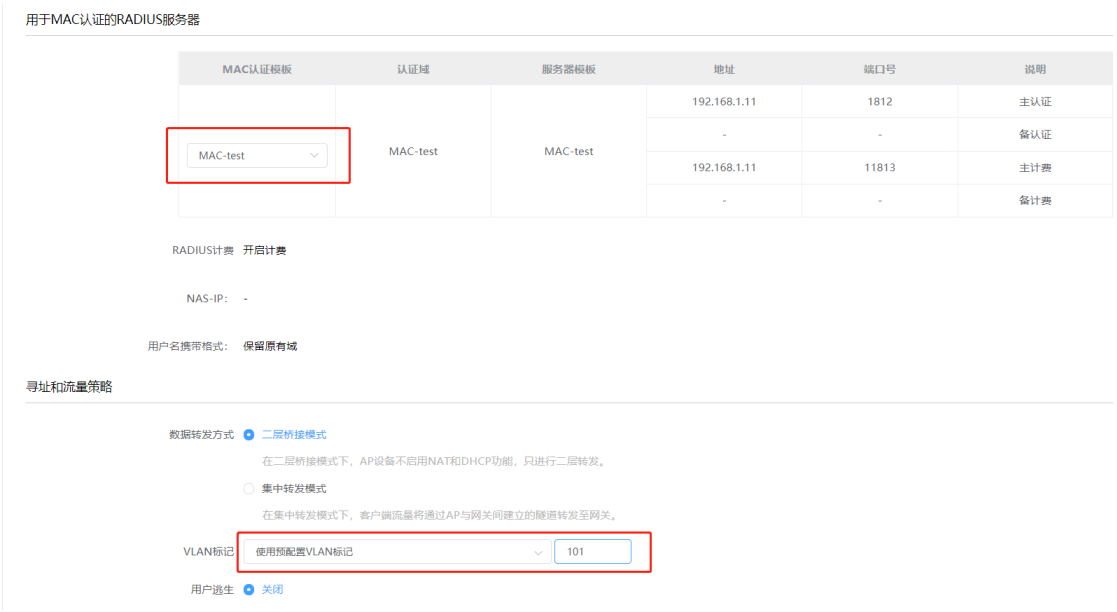
关联接入方式：MAC 认证（不加密）-外接 RADIUS 服务器，在“用于 MAC 认证的 RADIUS 服务器”栏“MAC 认证模板”列选择<添加一个 MAC 认证模板>

输入模板名称，选择刚才创建的 MAC-test 的 MAC 认证域，备选 Portal 认证，选择“Cisco ISE 认证服务器”，在弹出的 Cisco 认证服务器栏，输入认证服务器 ip 地址并点击<确定>。

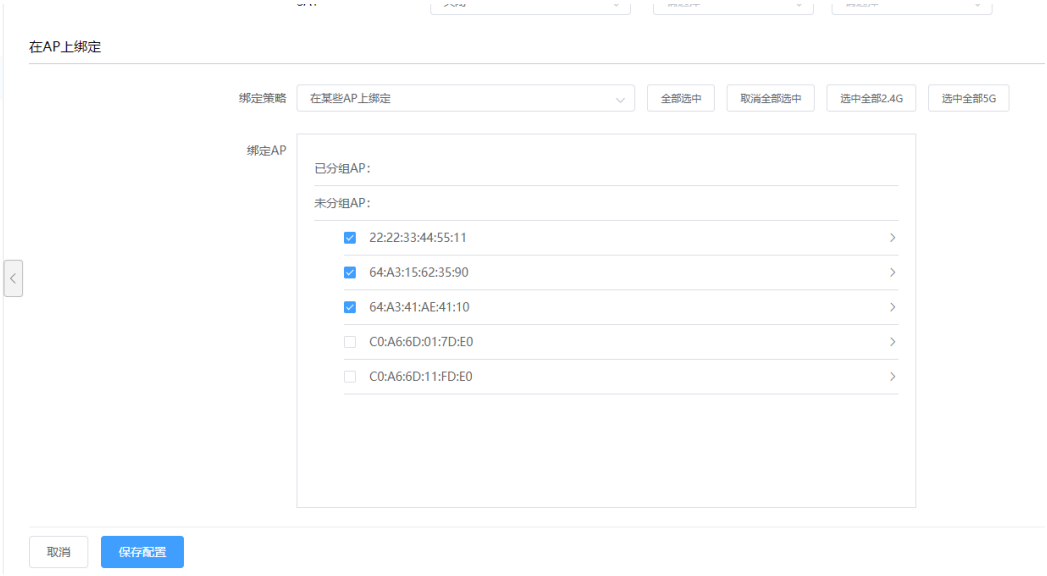
需注意：配置备选 Portal 认证时，先进行 MAC 认证，若认证失败，则转为 Portal 认证；若认证成功，则跳过 Portal 认证，直接允许终端接入；

数据转发方式：二层桥接模式

VLAN 标记：使用预置 VLAN 标记-101



选择要绑定的 AP 并保存



4.5.3 检查配置结果

完成配置后，用户可通过无线终端搜索到 SSID 为 test 的无线网络。

终端第一次认证时，用户从 ssid 上线，因服务器没有添加该 mac 认证用户，所以第一次认证失败，失败后进入 Portal 认证流程，开始 web 认证，web 认证成功后，开始正常上网。

无感知认证时，先进行 MAC 认证，若认证失败，则转为 Portal 认证；若认证成功，则跳过 Portal 认证，直接允许终端接入。

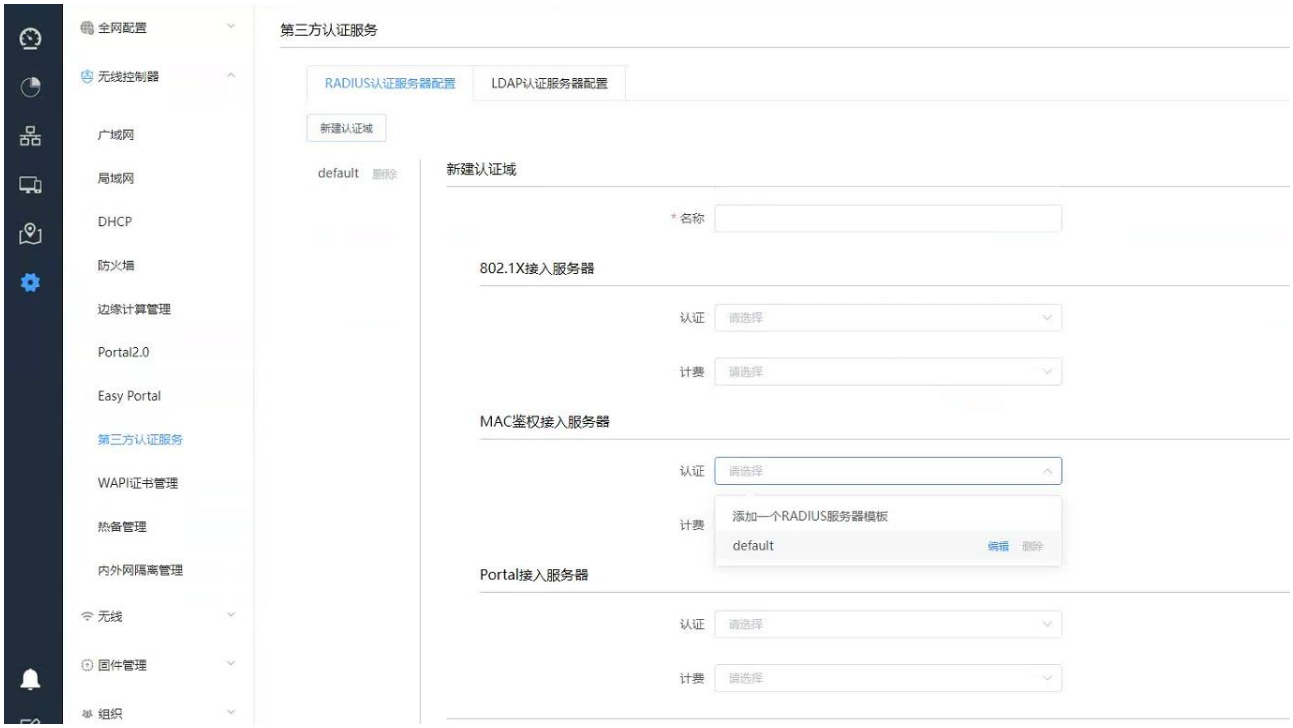
4.6 对接城市热点的无感知认证(MAC+Portal 组合认证)

4.6.1 配置第三方认证服务

配置认证域

路径:【设置】>子菜单【无线控制器】>子菜单【第三方认证服务】>点击<新建认证域>

✧ MAC 鉴权接入服务器配置

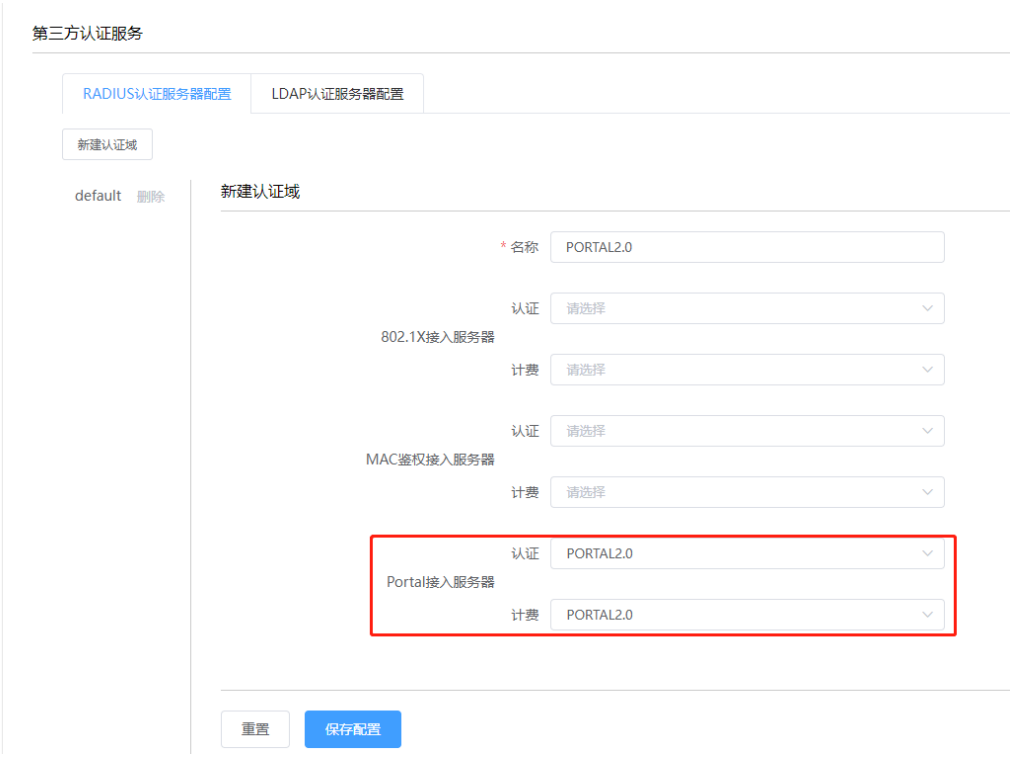


输入认证域“名称”，在 MAC 鉴权接入服务器栏选择“添加一个 Radius 服务器模板”,输入第三方服务器的地址、端口号和密钥，用户名携带格式与第三方认证服务器一致,本例选择保留原有域,点击<确定>

选择刚才创建的 Radius 服务器模版并保存配置。

✧ Portal 接入服务器配置

输入认证域“名称”，在 Portal 接入服务器栏选择“添加一个 Radius 服务器模板”，输入第三方服务器的地址、端口号和密钥，用户名携带格式与第三方认证服务器一致，本例选择保留原有域，点击<确定>



选择刚才创建的 Radius 服务器模版并保存配置。

注：点服务器上的配置可城市热点相关手册。

4.6.2 配置 SSID

路径：【设置】>子菜单【无线】>子菜单【无线服务】，进入 WLAN 业务配置页面，选择模板配置 SSID

SSID 名称为：test

使能：开启

是否隐藏 SSID：广播 SSID

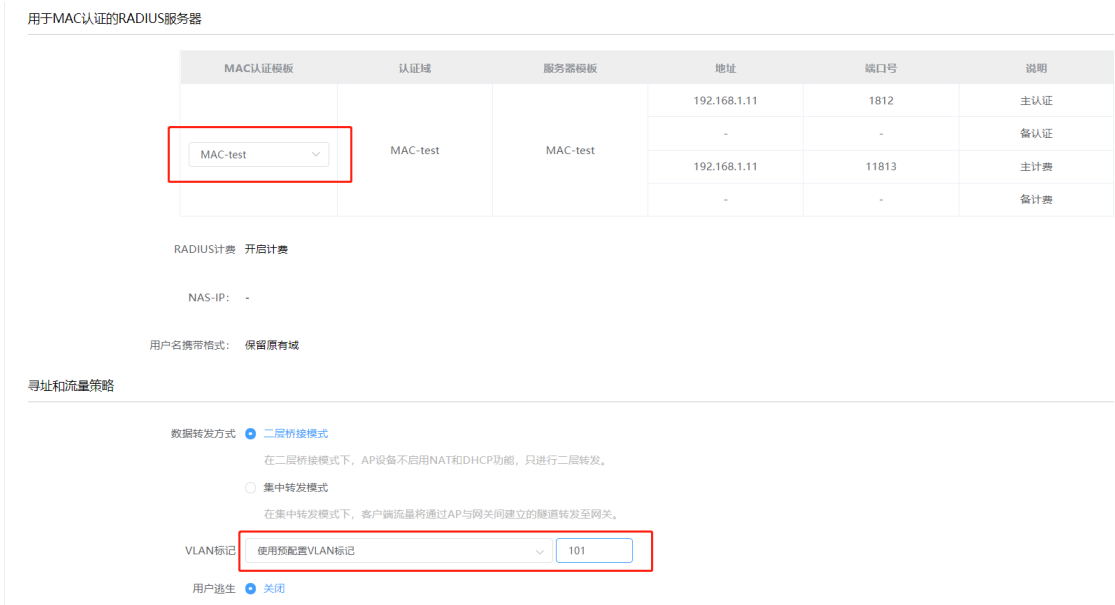
关联接入方式：MAC 认证（不加密）-外接 RADIUS 服务器，在“用于 MAC 认证的 RADIUS 服务器”栏“MAC 认证模板”列选择<添加一个 MAC 认证模板>

输入模板名称，选择刚才创建的 MAC-test 的 MAC 认证域，备选 Portal 认证，选择“城市热点认证服务器”并点击<确定>。

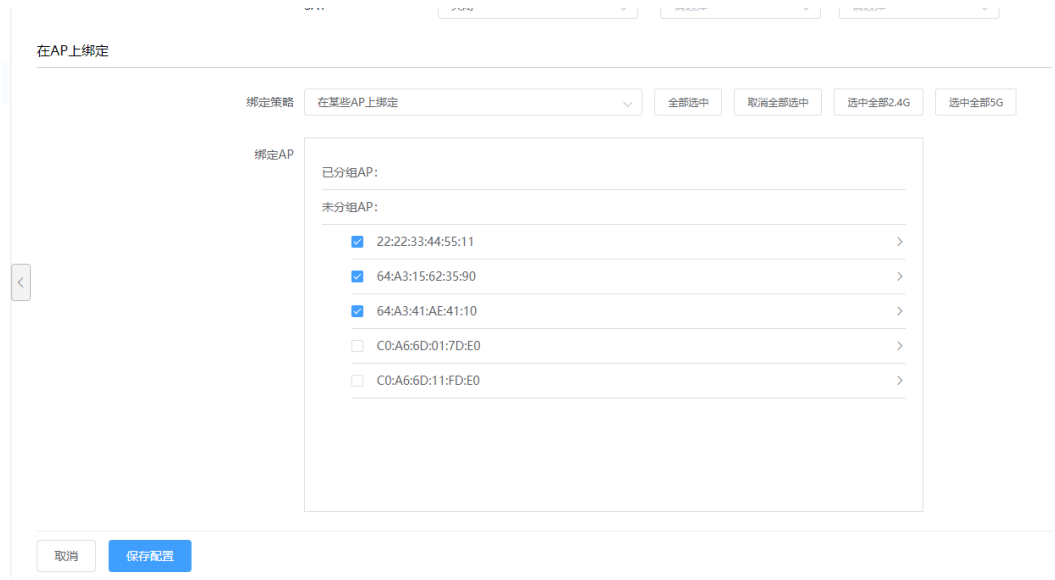
选择“城市热点认证服务器”方式时，Portal 采用 Portal 2.0 协议，需要在【设置】>【无线控制器】>【Portal 2.0】页，在 SSID 对应的 VLAN 下配置相关参数。

数据转发方式：二层桥接模式

VLAN 标记：使用预置 VLAN 标记-101



选择要绑定的 AP 并保存



✧ Portal 2.0 配置

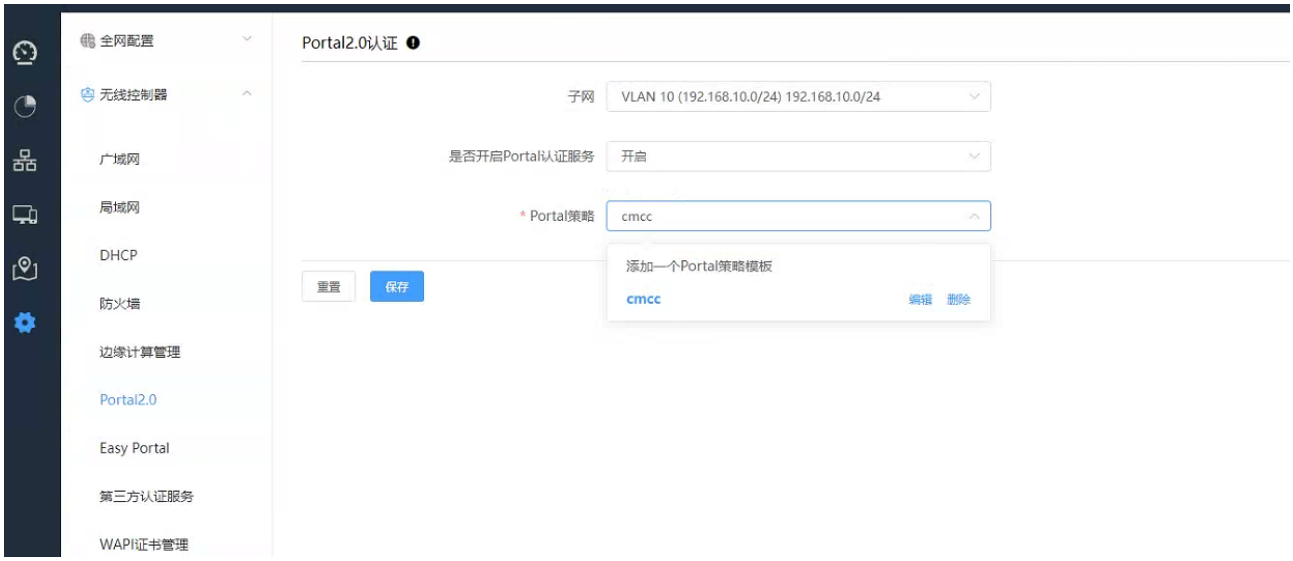
路径:【设置】>子菜单【无线控制器】>子菜单【Portal 2.0】

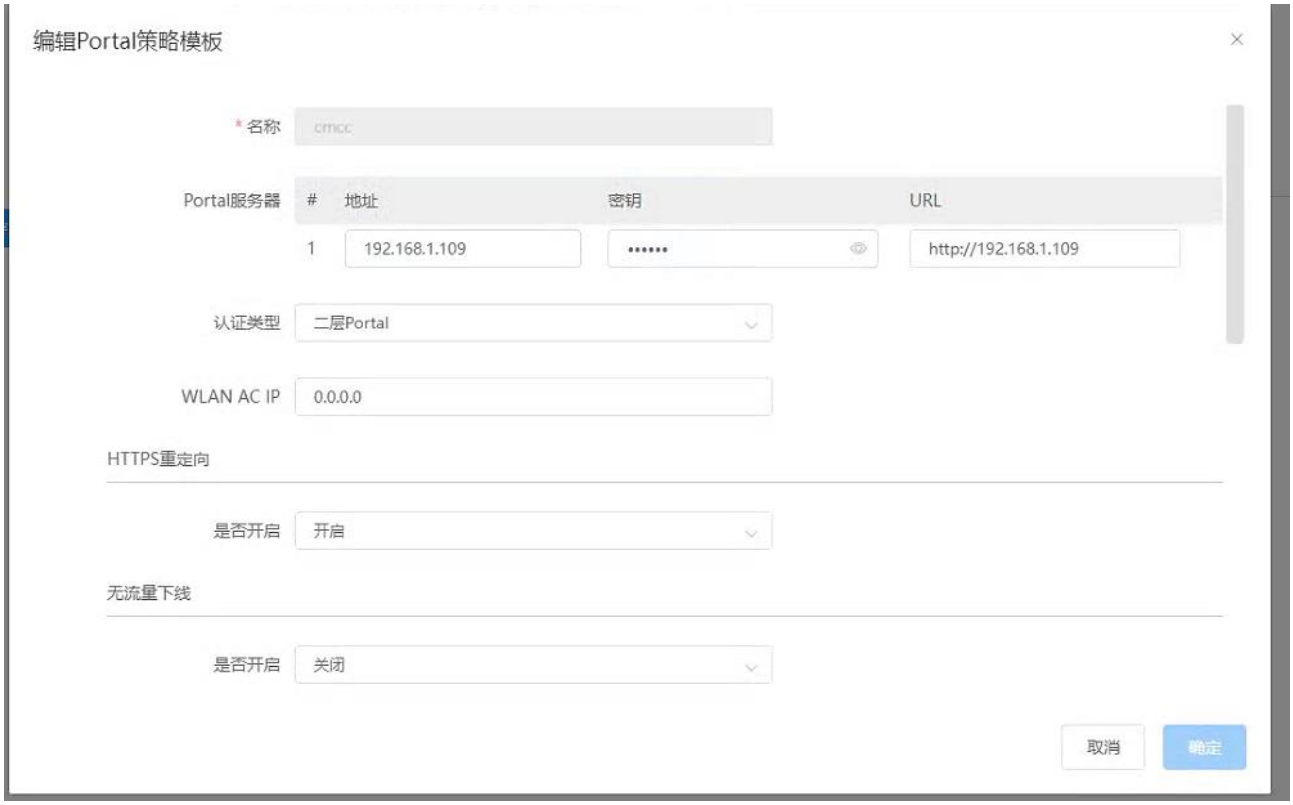
选择 SSID 对应的 VLAN 子网

是否开启 Portal 认证服务选择开启

Portal 服务器设置地址、密钥、URL 等相关参数，认证类型选择二层 Portal，WLAN AC IP 为 AC 的 portal 服务器到 AC 的可达的目的 ip

用于 Portal2.0 认证的 RADIUS 服务器选择上面创建的 PORTAL2.0 的认证域并保存。





4.6.3 检查配置结果

完成配置后，用户可通过无线终端搜索到 SSID 为 test 的无线网络。

终端第一次认证时，用户从 ssid 上线，因服务器没有添加该 mac 认证用户，所以第一次认证失败，失败后进入 Portal 认证流程，开始 web 认证，web 认证成功后，开始正常上网。

无感知认证时，先进行 MAC 认证，若认证失败，则转为 Portal 认证；若认证成功，则跳过 Portal 认证，直接允许终端接入。

4.7 企业级 WPA2 认证（本地 RADIUS 服务器）

4.7.1 配置 SSID

路径：【设置】>子菜单【无线】>子菜单【无线服务】，进入 WLAN 业务配置页面，选择模板配置 SSID

SSID 名称为：test

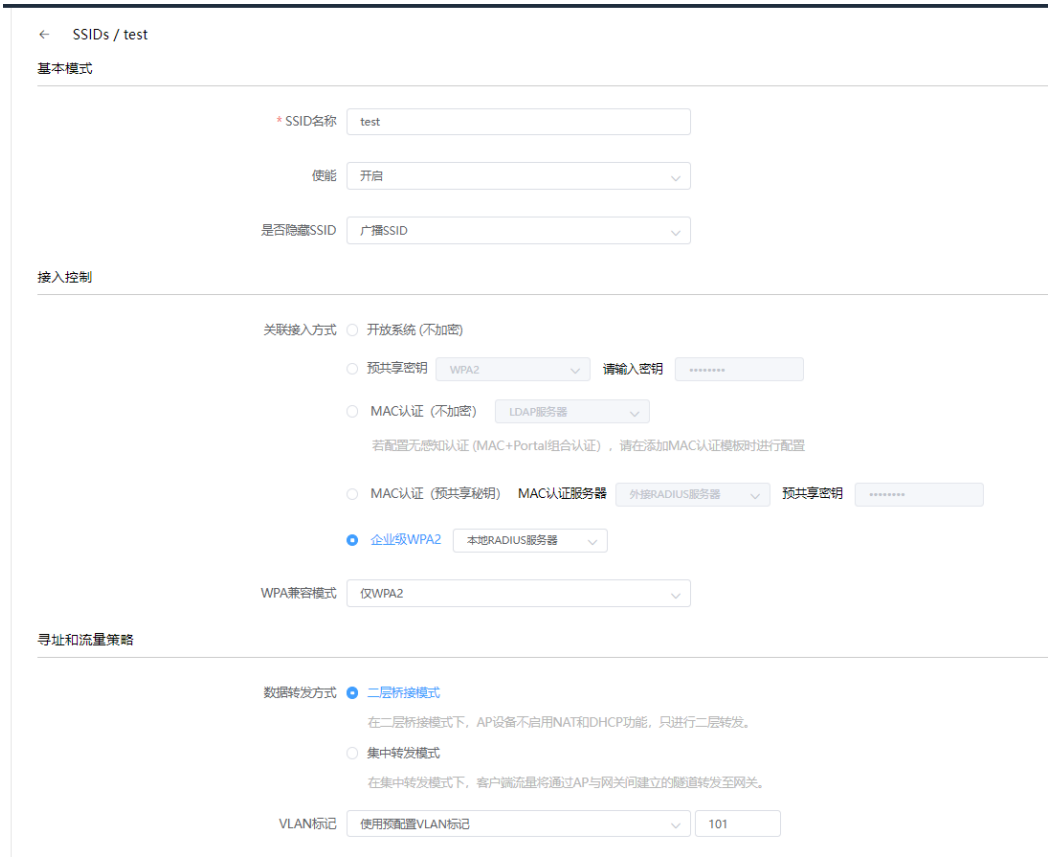
使能：开启

是否隐藏 SSID：广播 SSID

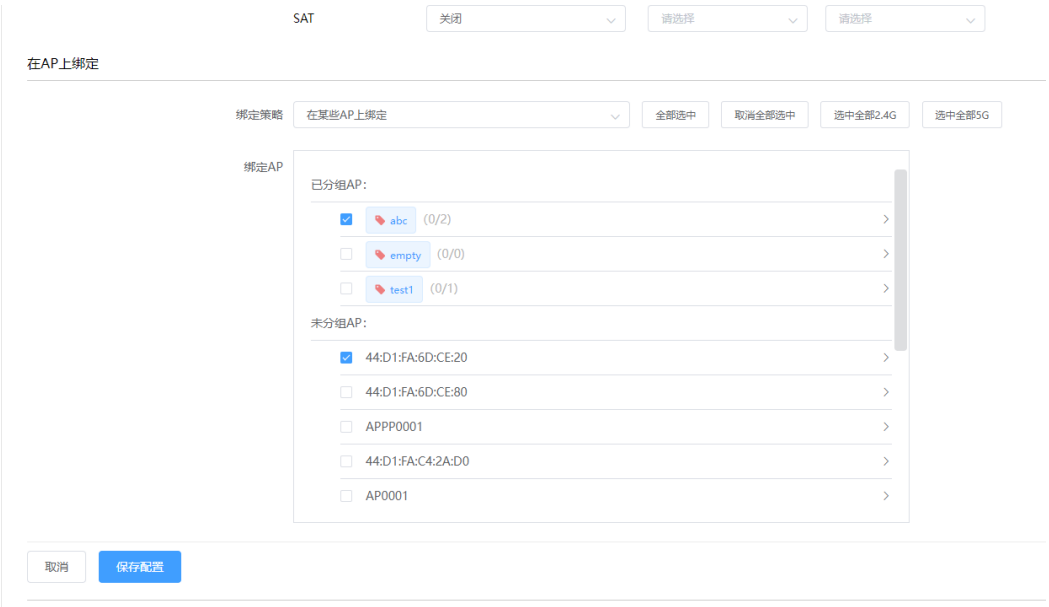
关联接入方式：企业级 WPA2-本地 RADIUS 服务器

数据转发方式：二层桥接模式

VLAN 标记：使用预置 VLAN 标记-101



选择要绑定的 AP 并保存



4.7.2 802.1x 用户配置

✧ 配置认证策略模板：创建授权 802.1x 认证的模板，用户组/用户可绑定该模板。

路径：【设置】>子菜单【全网配置】>子菜单【用户管理】>子菜单【认证策略模板】><添加模板>

模板名称：可自定义

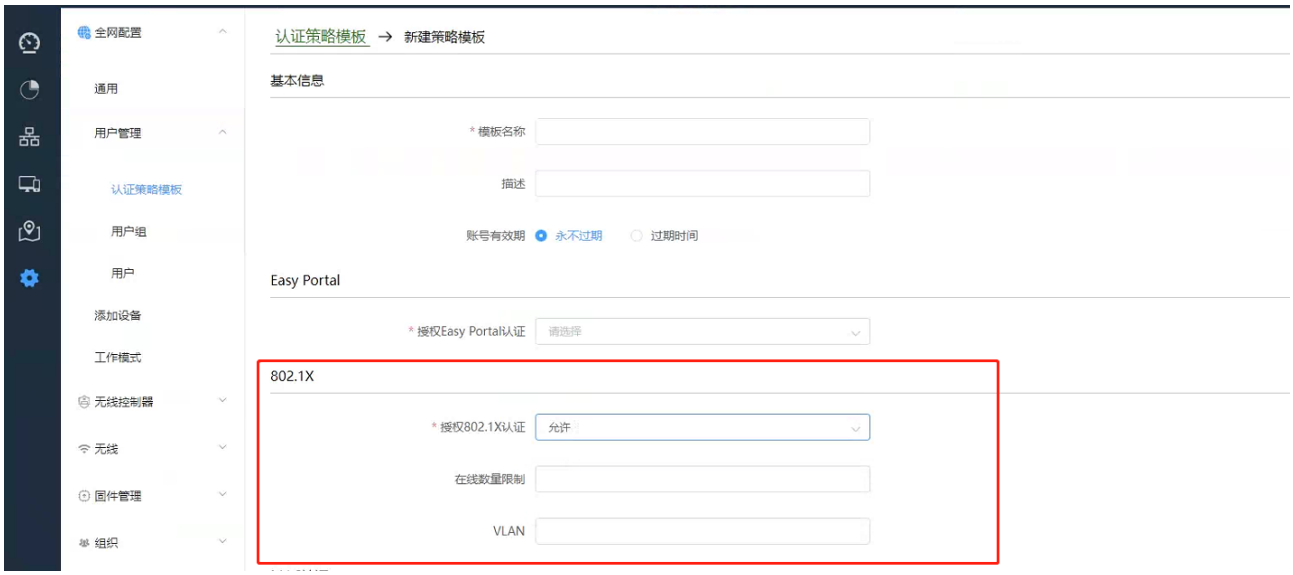
描述：可自定义

账号有效期：可选择永不过期或设置过期时间

Easy Portal 和 MAC 认证选择禁止授权

802.1X：选择允许

VLAN：优先级高于 SSID 中设置的 VLAN；若为空，则使用 SSID 中配置的 VLAN（本例为空）。



✧ 配置用户组：用户组上可绑定认证策略模板及 SSID

路径：【设置】>子菜单【全网配置】>子菜单【用户管理】>子菜单【用户组】><添加一级用户组>

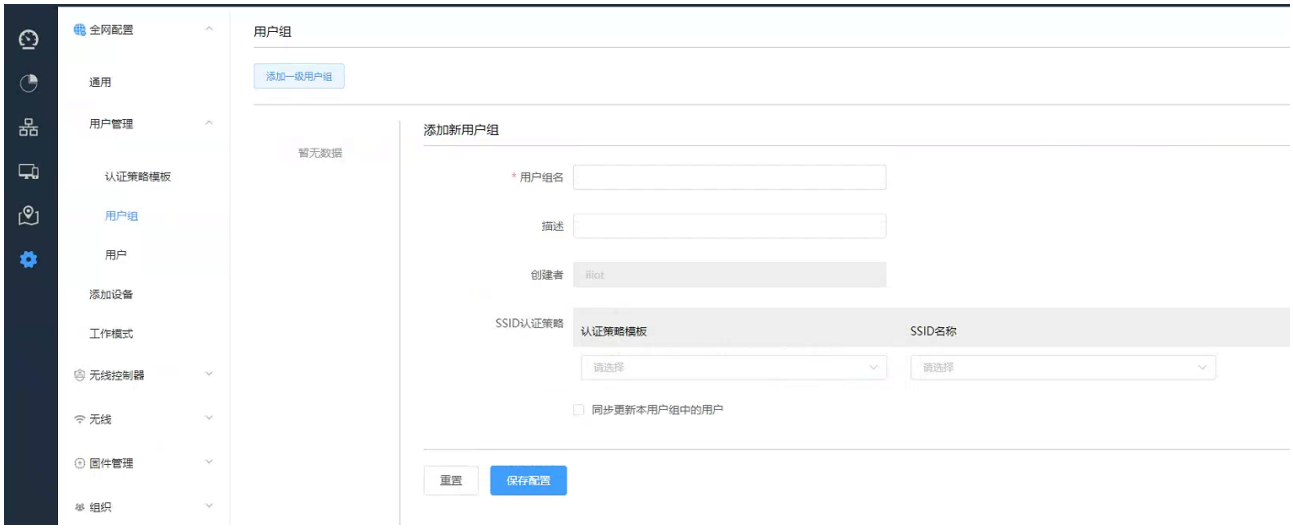
用户组名：可自定义

描述：可自定义

SSID 认证策略：选择上一步创建的认证策略模板（802.1x）及要绑定的 802.1x 认证的 SSID（test）

同步更新本用户组中的用户：选中后，会将本用户组中的认证策略模板和绑定的 SSID 同步到该用户组的所有用户。

点击<保存配置生效>

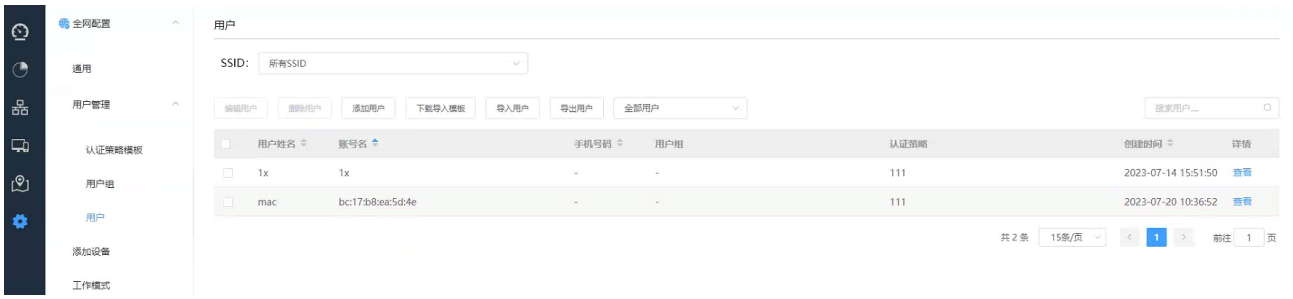


✧ 添加用户：添加 802.1x 认证用户

路径：【设置】>子菜单【全网配置】>子菜单【用户管理】>子菜单【用户】

SSID：在 SSID 下拉菜单选择 test 的 SSID

点击<添加用户>可添加单个用户；击<下载模板>，可通过模板批量导入用户

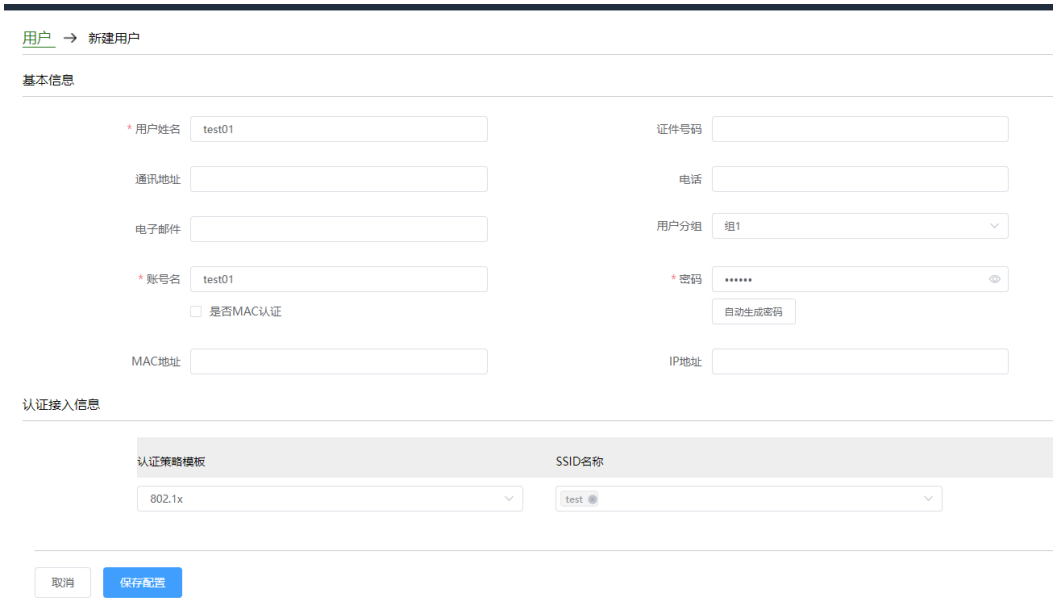


本例点击<添加用户>，弹出如下配置页面：

设置用户姓名、账号名和密码；

账号名栏填写账号名称；

选择用户分组-组 1，认证接入信息会自动变为组 1 中绑定的认证策略模板（802.1x）和 SSID（test），点击<保存配置>生效



4.7.3检查配置结果

完成配置后，用户可通过无线终端搜索到 SSID 为 test 的无线网络。

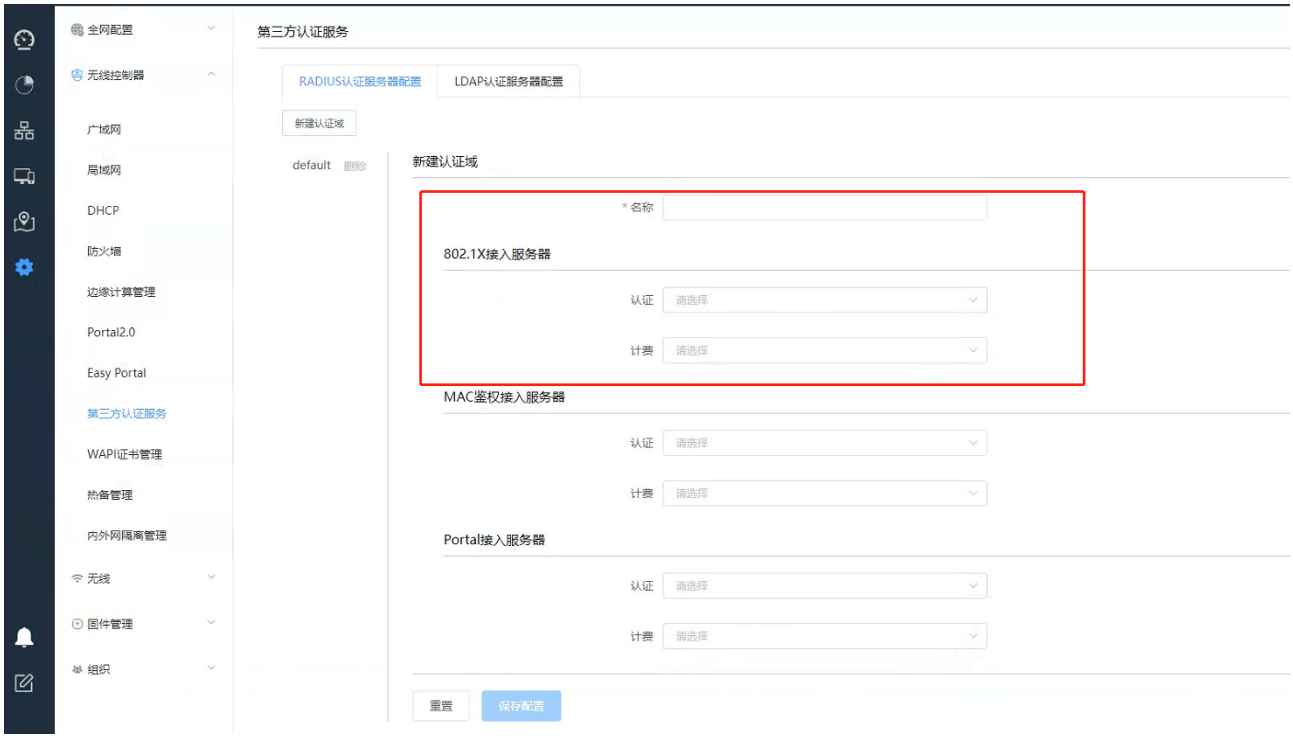
通过设置的 802.1x 账号密码可关联到该无线网络。

4.8 企业级 WPA2 认证（外接 RADIUS 服务器）

4.8.1配置第三方认证服务

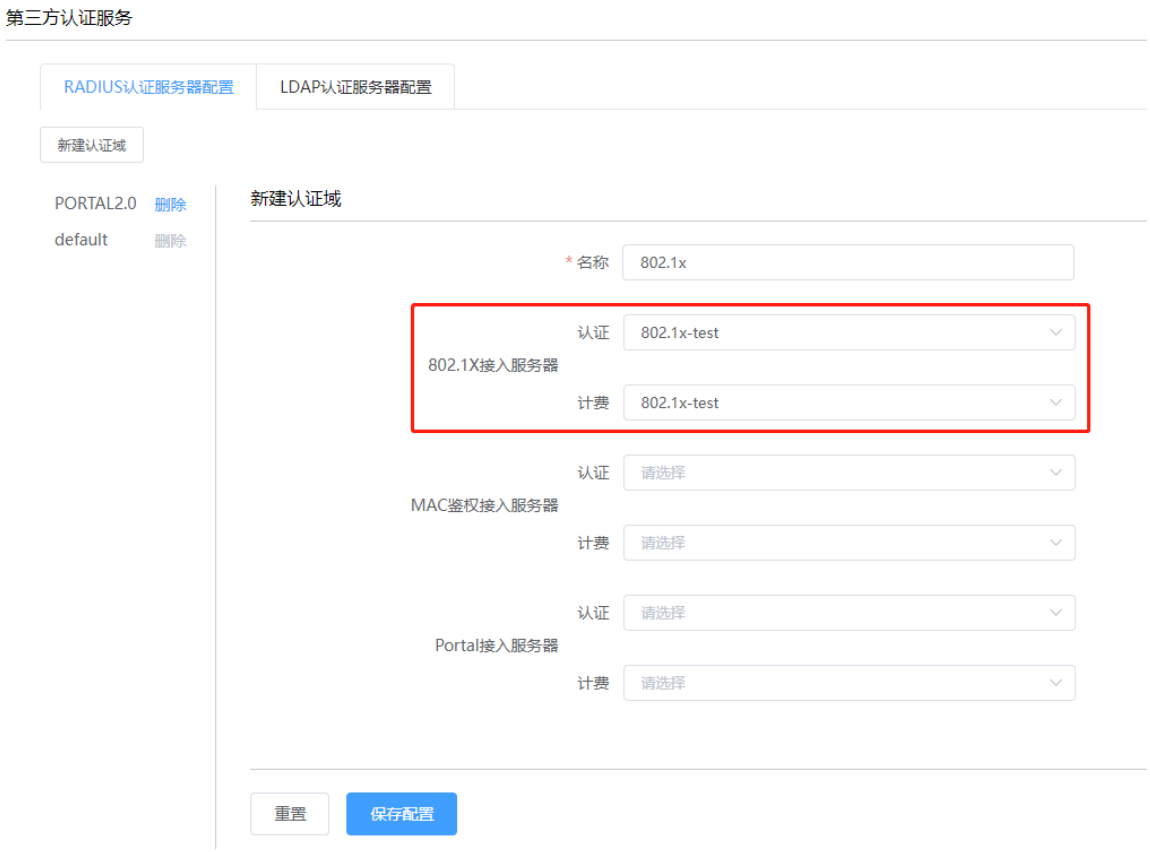
配置认证域

路径:【设置】>子菜单【无线控制器】>子菜单【第三方认证服务】>点击<新建认证域>



输入认证域“名称”，802.1X 接入服务器栏选择“添加一个 Radius 服务器模板”，输入第三方服务器的地址、端口号和密钥，用户名携带格式与第三方认证服务器一致，本例选择保留原有域，点击<确定>

选择刚才创建的 Radius 服务器模版并保存配置，完成第三方服务器认证域配置。



4.8.2配置 SSID

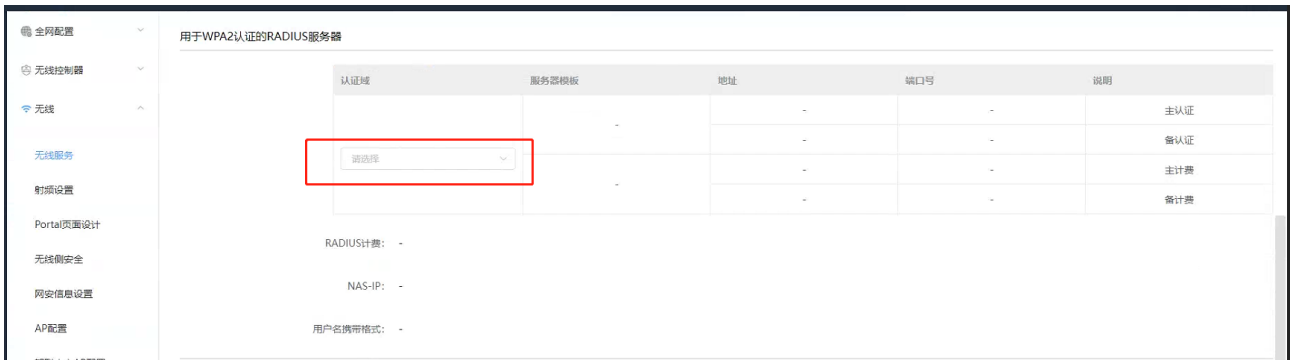
路径：【设置】>子菜单【无线】>子菜单【无线服务】，进入 WLAN 业务配置页面，选择模板配置 SSID

SSID 名称为：test

使能：开启

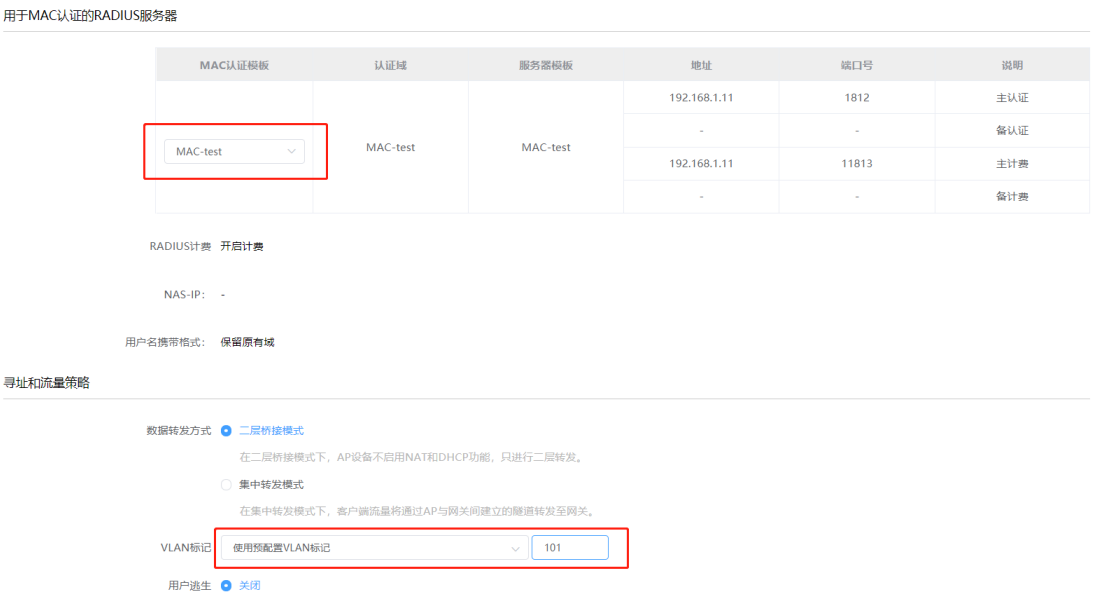
是否隐藏 SSID：广播 SSID

关联接入方式：企业级 WPA2（外接 RADIUS 服务器），在“用于 WPA2 认证的 RADIUS 服务器”栏“认证域”列选择刚才创建的 802.1x 的认证域。

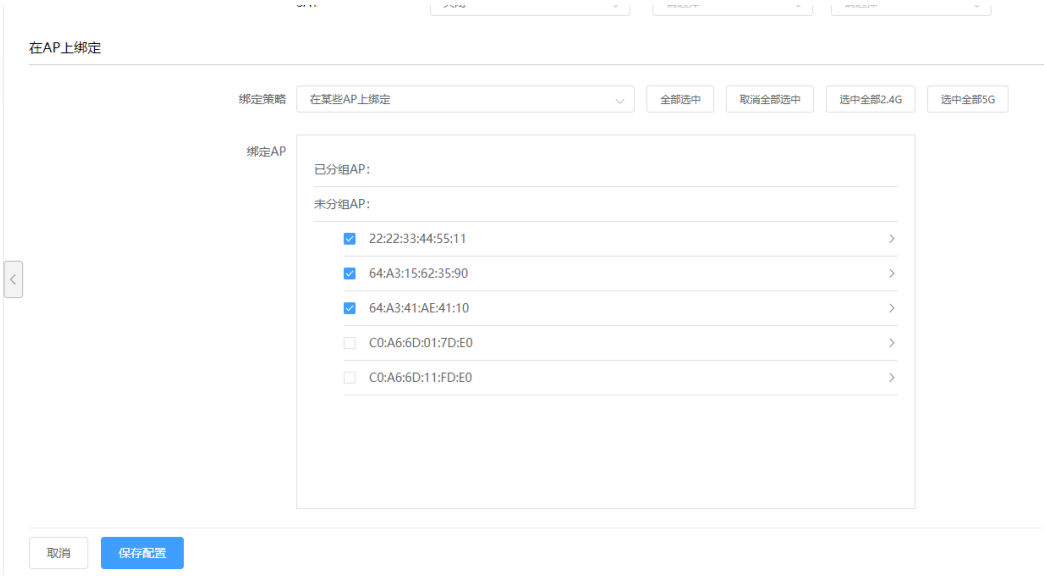


数据转发方式：二层桥接模式

VLAN 标记：使用预置 VLAN 标记-101



选择要绑定的 AP 并保存



4.8.3 检查配置结果

完成配置后，用户可通过无线终端搜索到 SSID 为 test 的无线网络。

通过第三方服务器提供的 802.1x 账号密码可关联到该无线网络。

4.9 企业级 WPA2 认证（LDAP 服务器）

4.9.1 配置第三方认证服务

AC 上 LDAP 参数配置

路径：【设置】>子菜单【无线控制器】>子菜单【第三方认证服务】>【LDAP 认证服务器配置】

主/备服务器：可以是 IP 地址或域名，本例为：192.168.1.168

端口号：默认 389 主备必须相同（freeradius 限制）

通用服务器路径：用户搜索的基本路径，本例为：CN=Users,DC=inspur,DC=local

用户标识：openLDAP 使用 uid，windows server 使用 cn，本例为：cn

分组标识：openLDAP 使用 posixGroup(openldap)，windows server 使用 Group(windows ad)

用户名：管理用户，用户加域名后缀，本例为：dcao@inspur.local

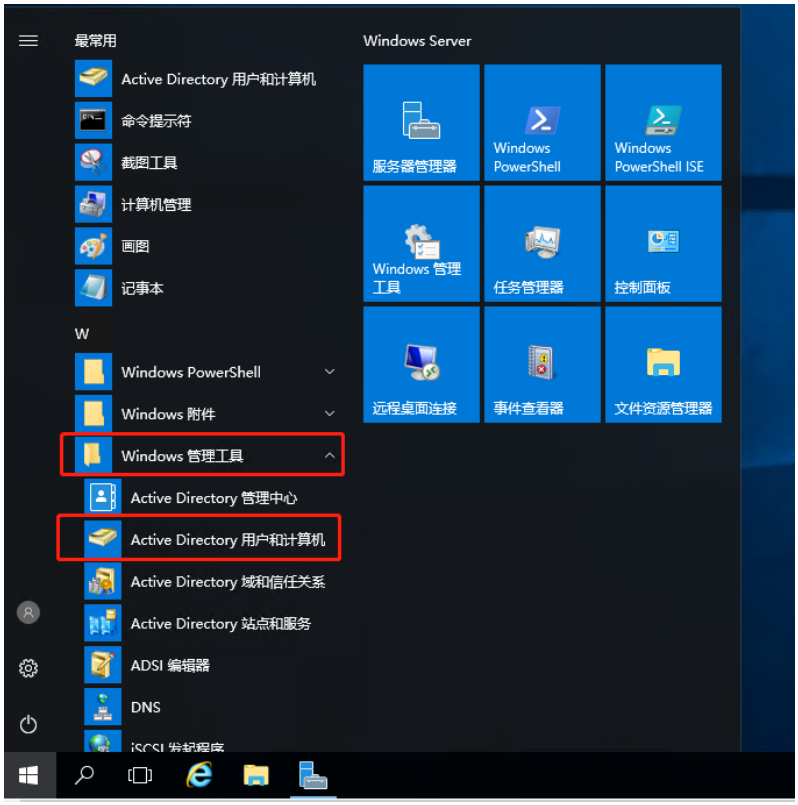
密码：管理用户的密码，本例为：12345678

Windows2000 前域名：可以选择保留原有域名和不携带域名

2、LDAP 相关配置

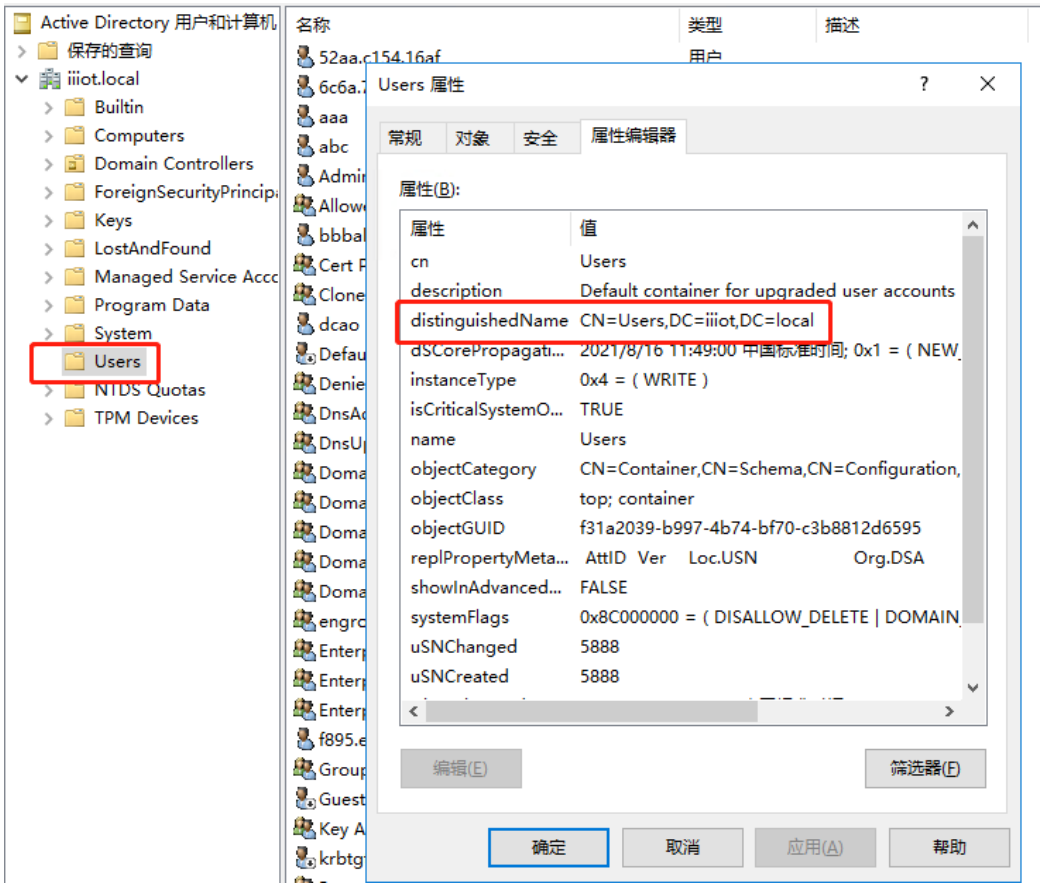
（1）通用服务器路径查看方法：

1） 通过菜单打开 AD 的用户管理



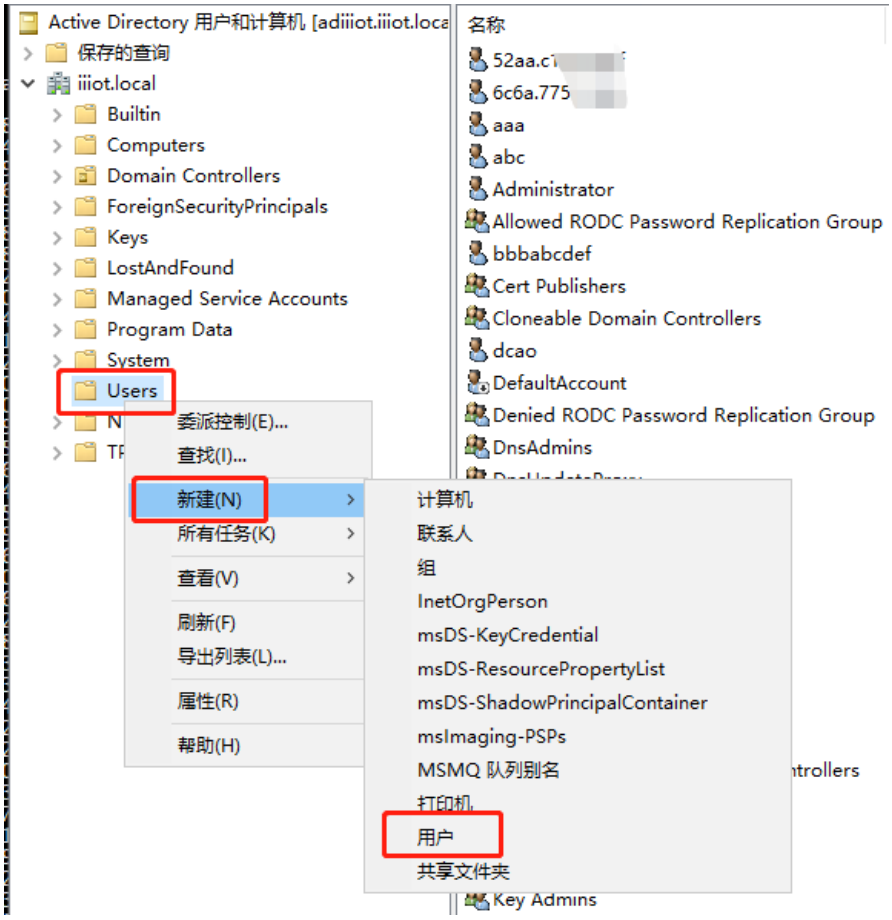
2) 在用户所属组上点击右键，选择属性出现以下对话框，可以看到通用搜索路径。为了提高效率在明确用户组的情况下可以从用户组开始，本例为：CN=Users,dc=inspur,dc=local。

如果不明确用户在哪个组，可以从下一级开始，例如，dc=inspur,dc=local



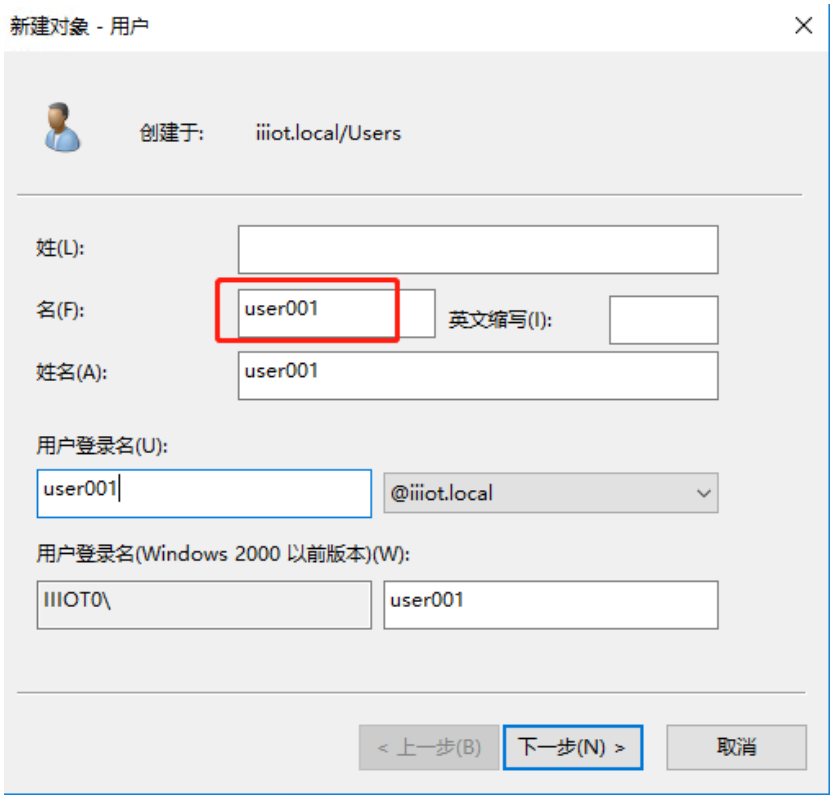
（2）认证用户的添加

1） 在 users 目录上点击右键，新建用户



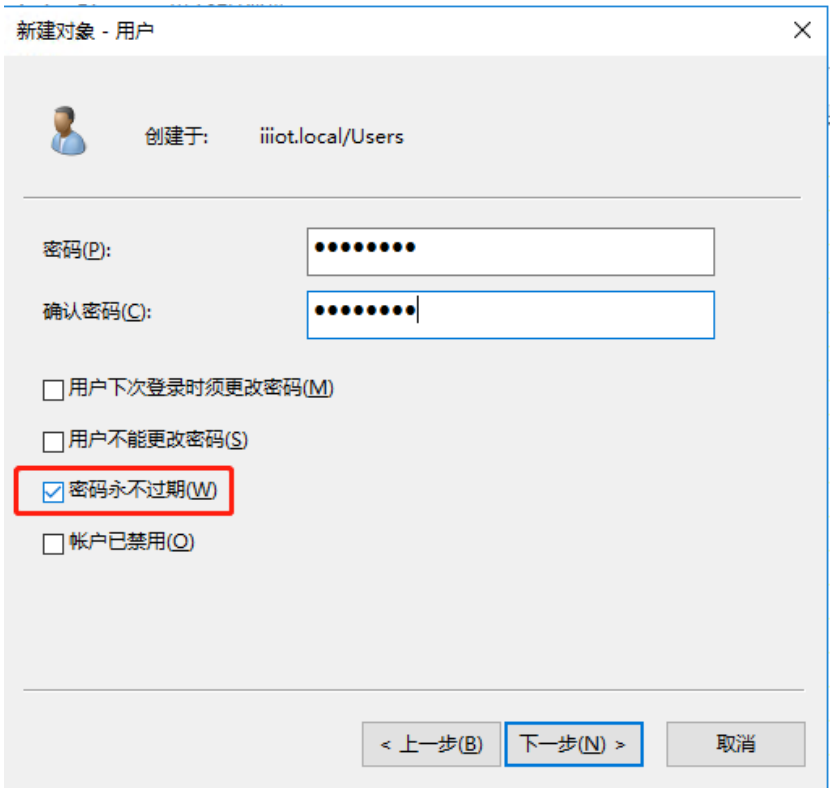
2） 填写用户信息

名（F）处填写 LDAP 认证的用户名

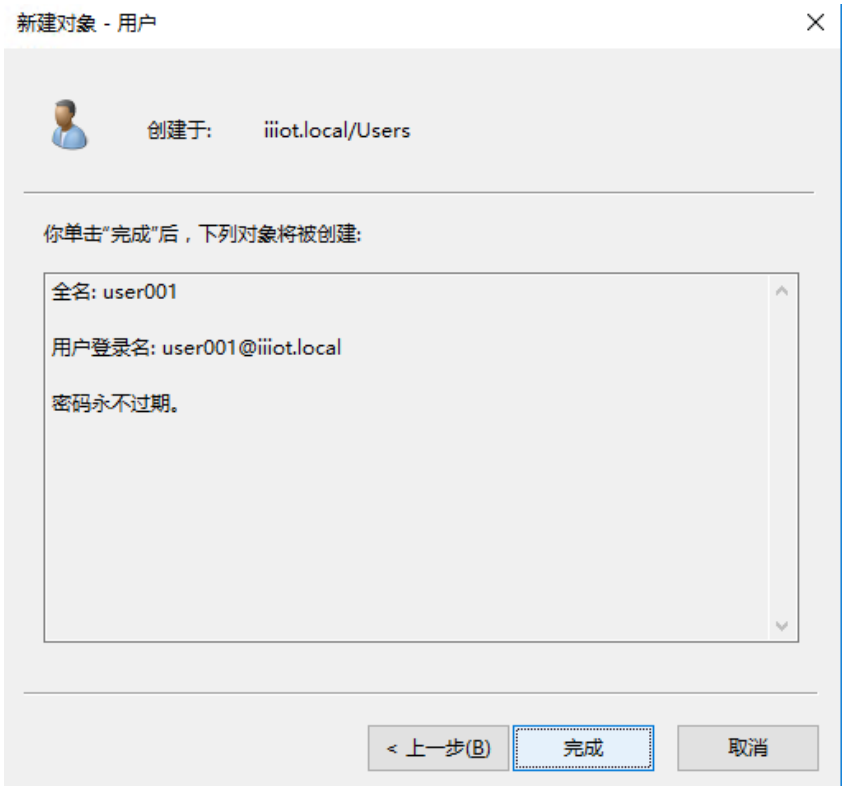


3) 选择密码策略为永不过期

设置用户密码，密码永不过期



点击<下一步>完成设置



4.9.2配置 SSID

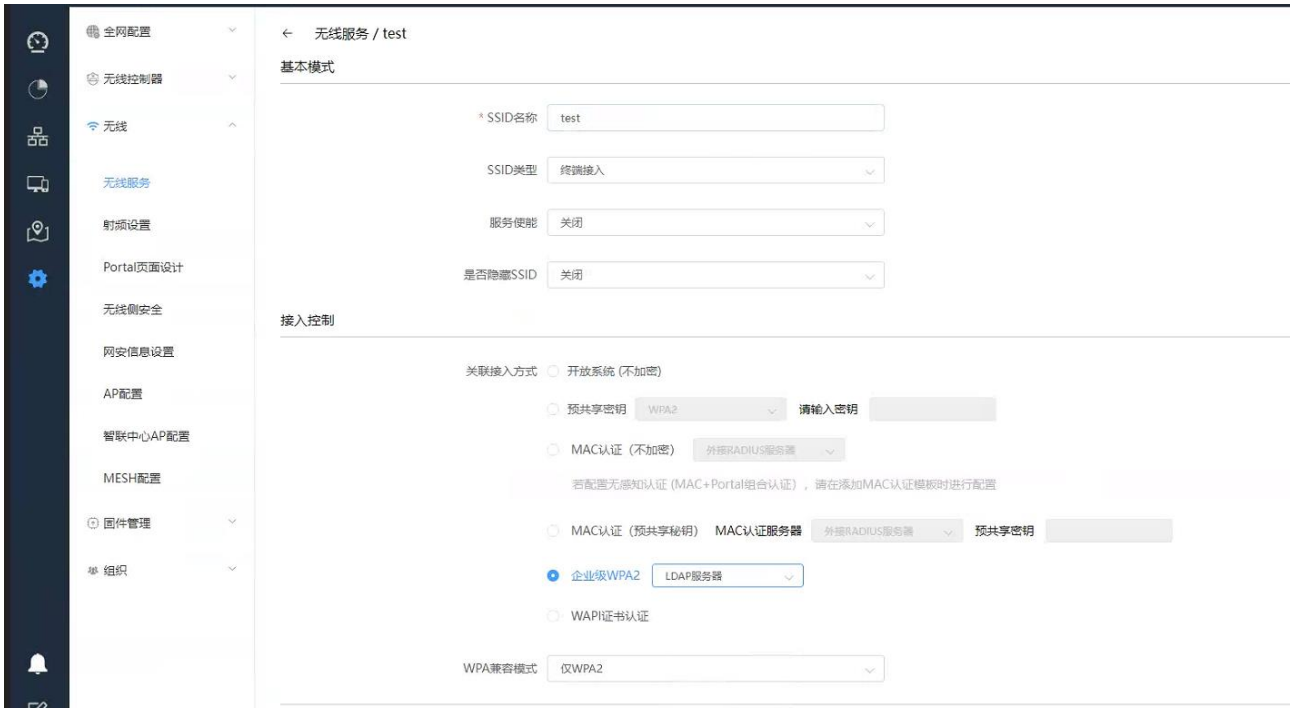
路径:【设置】>子菜单【无线】>子菜单【无线服务】，进入 WLAN 业务配置页面，选择模板配置 SSID

SSID 名称为：test

使能：开启

是否隐藏 SSID：广播 SSID

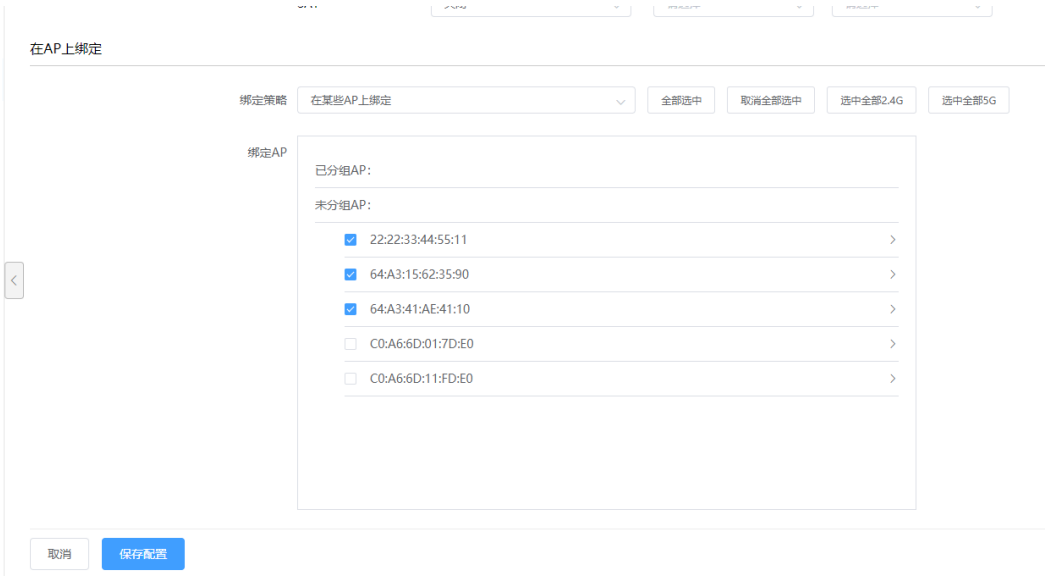
关联接入方式：MAC 认证（不加密）-LDAP 服务器



数据转发方式：二层桥接模式

VLAN 标记：使用预置 VLAN 标记-101

选择要绑定的 AP 并保存

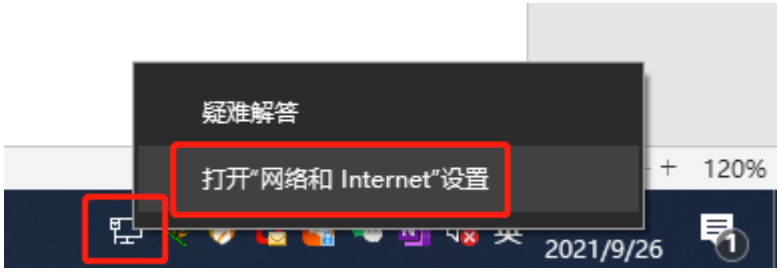


4.9.3 检查配置结果

完成配置后，用户可通过无线终端搜索到 SSID 为 test 的无线网络。

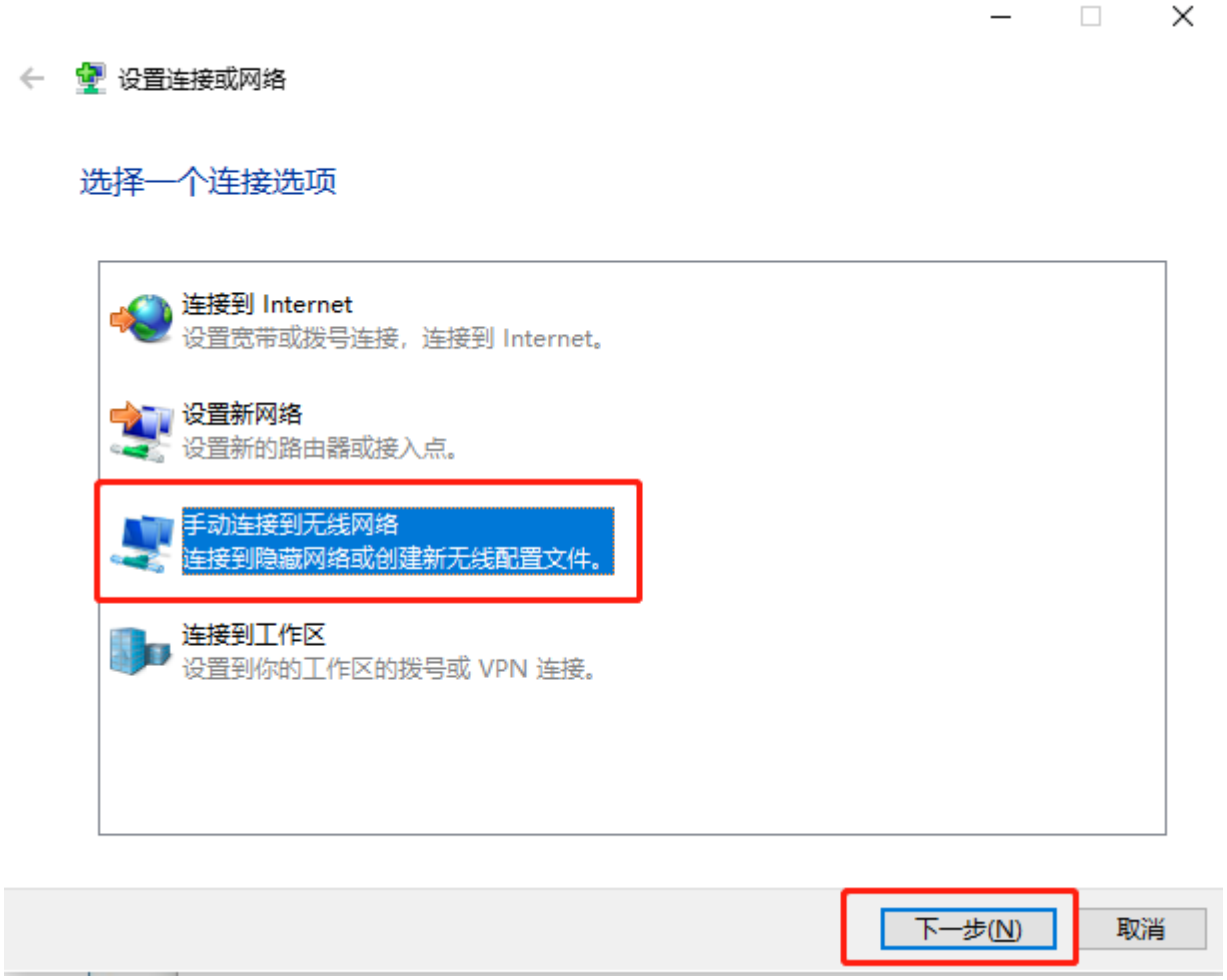
通过 LDAP 服务器上已添加账号和密码可关联到该无线网络。

4.9.4 附 1：Windows 客户端配置（EAP-TTLS）

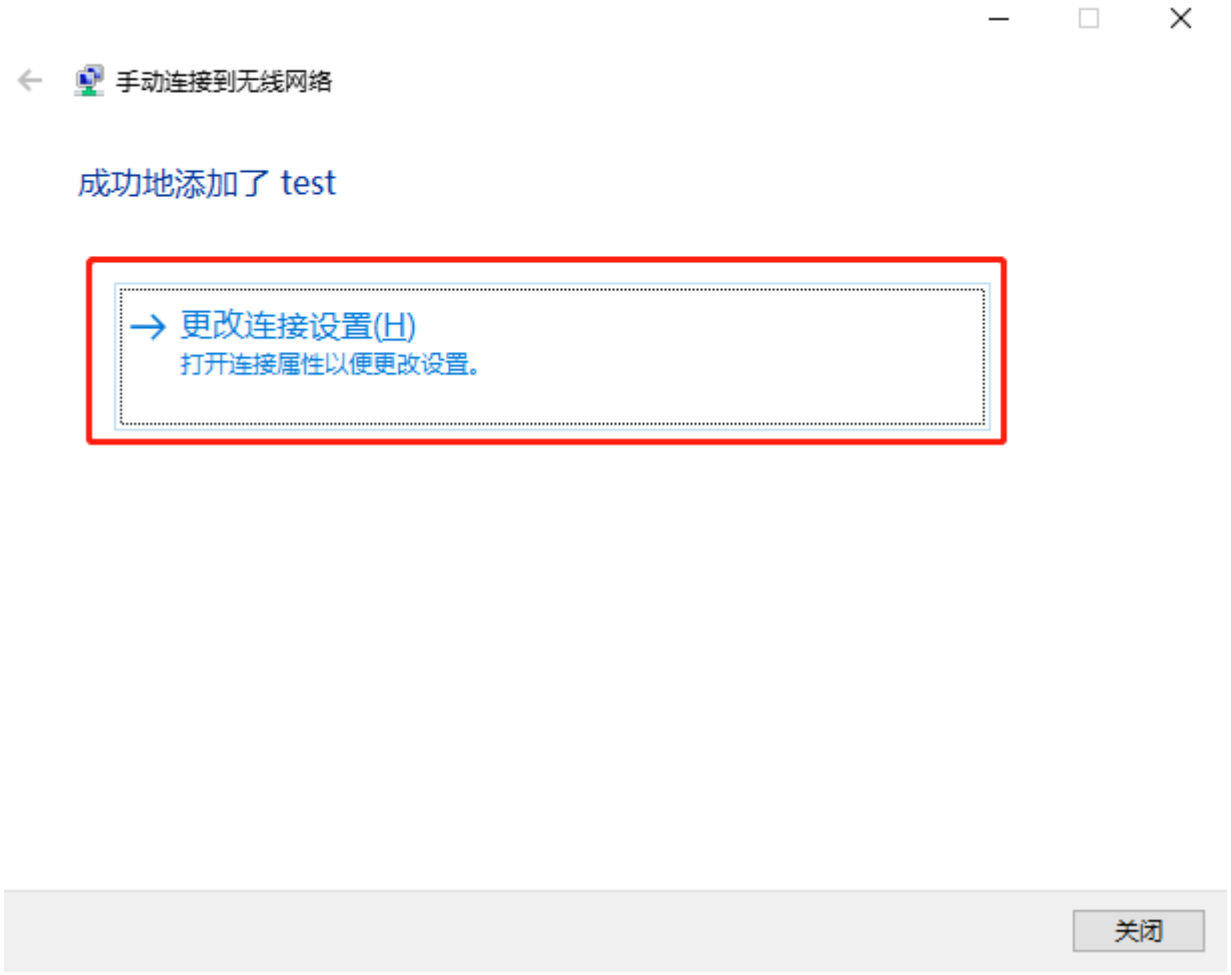


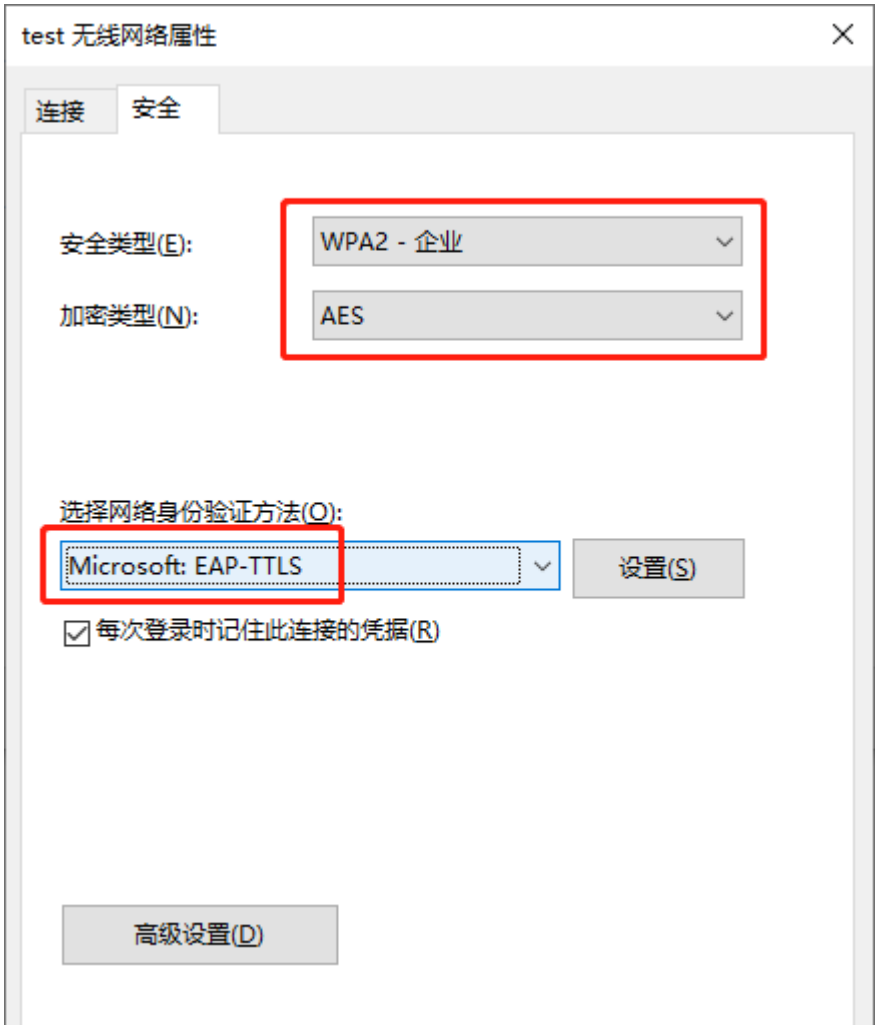

设置
主页
查找设置
网络和 Internet
状态
WLAN
以太网
拨号
VPN
飞行模式
移动热点
代理
状态
网络状态
以太网
专用网络
你已连接到 Internet
如果你的流量套餐有限制，则你可以将此网络设置为按流量计费的连接，或者更改其他属性。
以太网
最近 30 天内
28.66 GB
属性
数据使用量
显示可用网络
查看周围的连接选项。
高级网络设置
更改适配器选项
查看网络适配器并更改连接设置。
网络和共享中心
根据所连接到的网络，决定要共享的内容。
网络疑难解答
诊断并解决网络问题。
查看硬件和连接属性
Windows 防火墙
网络重置

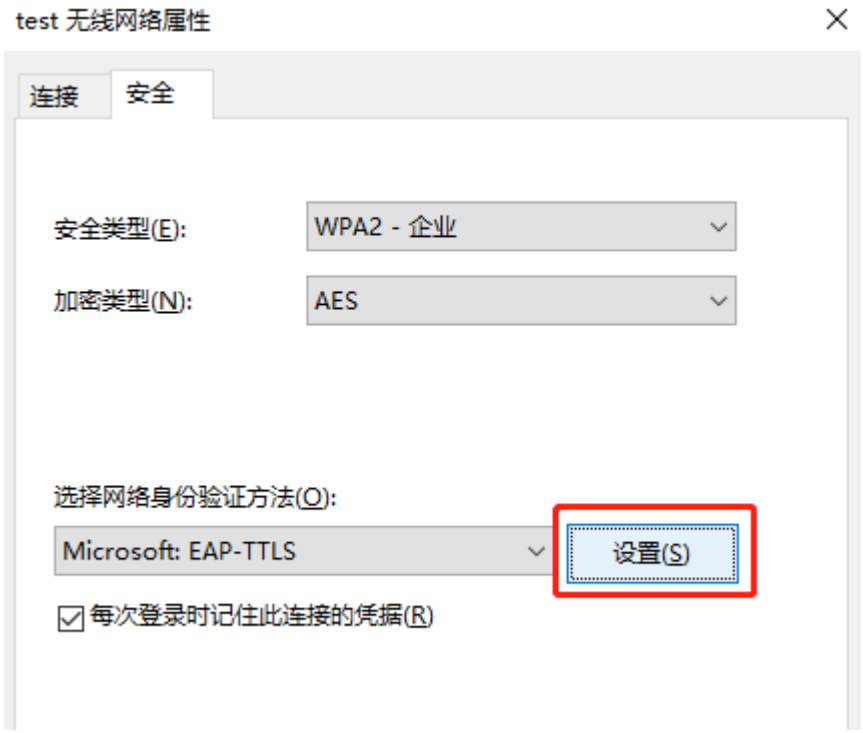

网络和共享中心
控制面板 › 所有控制面板项 › 网络和共享中心
控制面板主页
更改适配器设置
更改高级共享设置
媒体流式处理选项
查看基本网络信息并设置连接
查看活动网络
00psk_localdata
专用网络
访问类型: Internet
连接: 以太网
更改网络设置
设置新的连接或网络
设置宽带、拨号或 VPN 连接；或设置路由器或接入点。
问题疑难解答
诊断并修复网络问题，或者获得疑难解答信息。


设置连接或网络
选择一个连接选项
连接到 Internet
设置宽带或拨号连接，连接到 Internet。
设置新网络
设置新的路由器或接入点。
手动连接到无线网络
连接到隐藏网络或创建新无线配置文件。
连接到工作区
设置到你的工作区的拨号或 VPN 连接。
下一步(N)
取消

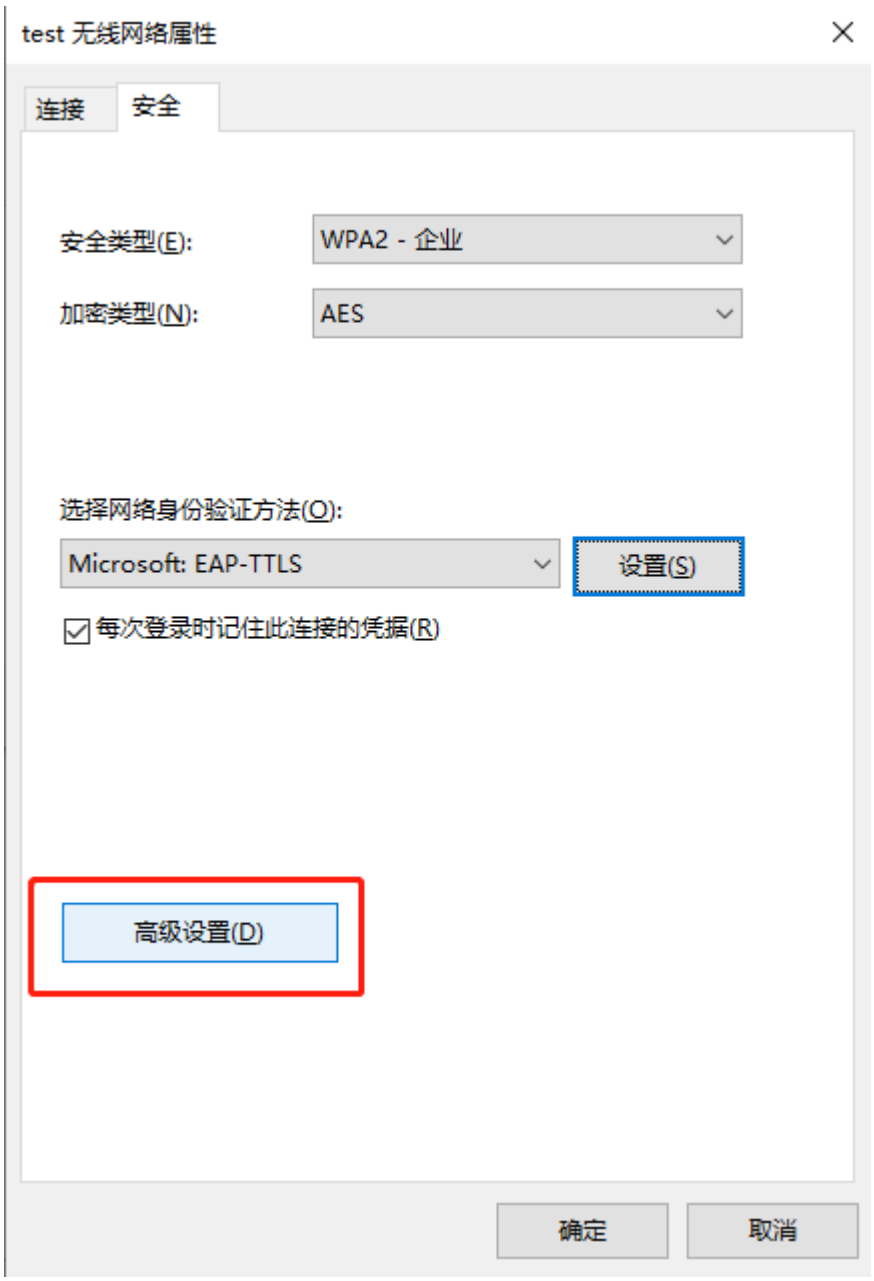

手动连接到无线网络
输入你要添加的无线网络的信息
网络名(E):
test
安全类型(S):
WPA2 - 企业
加密类型(R):
AES
安全密钥(C):
隐藏字符(H)
自动启动此连接(T)
即使网络未进行广播也连接(O)
警告: 如果选择此选项，则计算机的隐私信息可能存在风险。
下一步(N)
取消


手动连接到无线网络
成功地添加了 test
更改连接设置(H)
打开连接属性以便更改设置。
关闭


test 无线网络属性
连接
安全
安全类型(E):
WPA2 - 企业
加密类型(N):
AES
选择网络身份验证方法(O):
Microsoft: EAP-TTLS
设置(S)
每次登录时记住此连接的凭据(R)
高级设置(D)


test 无线网络属性
连接
安全
安全类型(E):
WPA2 - 企业
加密类型(N):
AES
选择网络身份验证方法(O):
Microsoft: EAP-TTLS
设置(S)
每次登录时记住此连接的凭据(R)


TTLS 属性
启用标识隐私(D)
服务器证书验证
连接到这些服务器(O):
受信任的根证书颁发机构(R):
AAA Certificate Services
AC Raíz Certicámara S.A.
AC RAIZ DNIE
AC RAIZ FNMT-RCM
ACCVRAIZ1
如果无法授权服务器，则不提示(P)
客户端身份验证
选择一个用于身份验证的非 EAP 方法(N)
未加密的密码(PAP)
自动使用 Windows 帐户名和密码(如果有域，也使用域)(W)
选择一个用于身份验证的 EAP 方法(E)
Microsoft: 智能卡或其他证书
配置(C)
确定
取消


test 无线网络属性
连接
安全
安全类型(E):
WPA2 - 企业
加密类型(N):
AES
选择网络身份验证方法(O):
Microsoft: EAP-TTLS
设置(S)
每次登录时记住此连接的凭据(R)
高级设置(D)
确定
取消


高级设置
802.1X 设置
802.11 设置
指定身份验证模式(P):
用户身份验证
保存凭据(C)
删除所有用户的凭据(D)
为此网络启用单一登录(S)
用户登录前立即执行(E)
用户登录后立即执行(F)
最大延迟(秒)(M):
10
允许单一登录期间显示其他对话框(L)
该网络为计算机和用户身份验证使用单独的虚拟 LAN(V)
确定
取消

4.9.5 附 2：手机端（安卓）EAP-TTLS 配置

手机端（IOS）配置（暂无）

MAC-OS 端配置（暂无）

4.10 本地 Portal 认证

4.10.1 Portal-配置注意事项

1) 业务 vlan 需要配置子网 ip；当使用智联中心 AP 时，需要在【无线】>【中心 AP 配置】中给对应的智联中心 AP 配置 VLAN 接口，再配置 portal 认证的 ssid。
2) 业务网段需要配置 dns,否则会导致 portal 认证页面无法弹出;(注:建议是所连接网络运营商的 dns)
3) 业务 vlan 外网不可达时,无法自动弹出 portal 页面,需手动进浏览器输入任意 ip 弹出 portal 页面;
4) 在业务网和管理网无法区分开时，AP 地址需加入 easy portal 的白名单，否则会导致 portal 认证异常;
5) 当前默认未开启 https 重新向，开启方法为:

   INOP(config)#apm profile 1

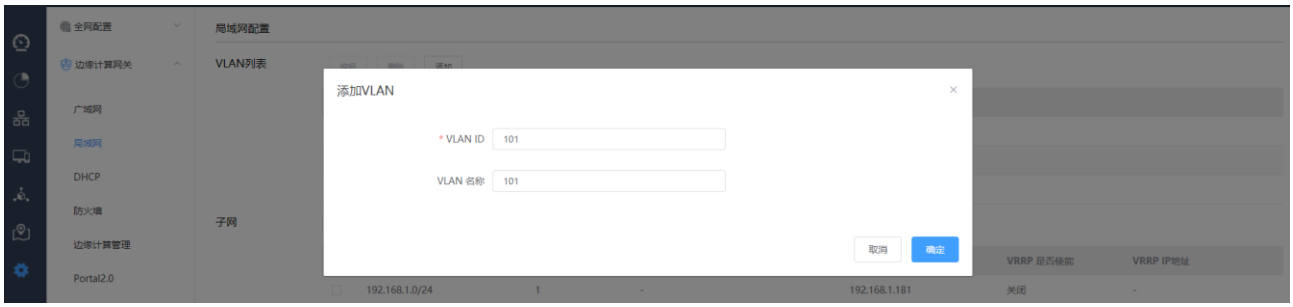
   INOP(apm-profile)#https-redirect enable
6) 配置顺序说明:
   a) 第一步：创建 portal 认证的业务 vlan 及配置相应 vlan 的接口地址;
   b) 第二步：配置 portal 认证的 SSID;

c） 第三步：根据选择的 portal 认证类型创建相应的认证用户；

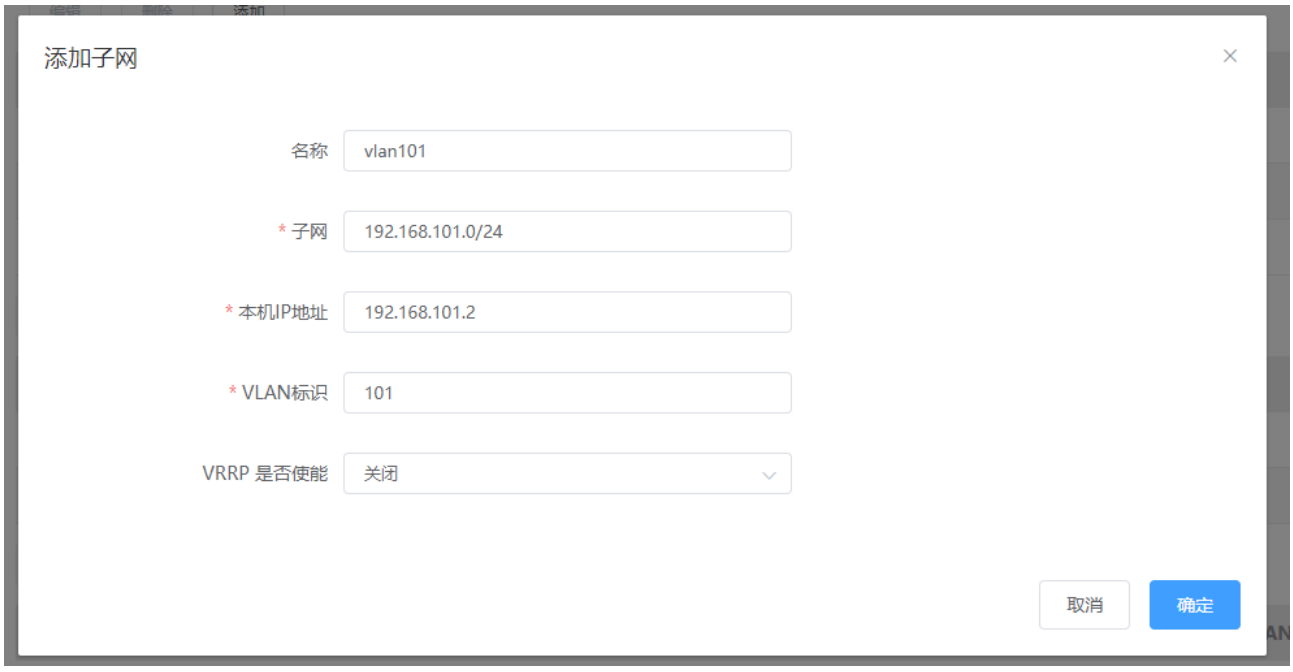
4.10.2 Portal-一键登录

4.10.2.1 配置子网 IP

路径：【设置】>子菜单【无线控制器】>子菜单【VLAN 列表】，添加业务 VLAN 101



路径：【设置】>子菜单【无线控制器】>子菜单【子网】，添加业务 VLAN 101 的子网，AC 配置子网 ip 为 192.168.101.2



4.10.2.2 配置 SSID

路径：【设置】>子菜单【无线】>子菜单【无线服务】，进入 WLAN 业务配置页面，选择模板配置 SSID

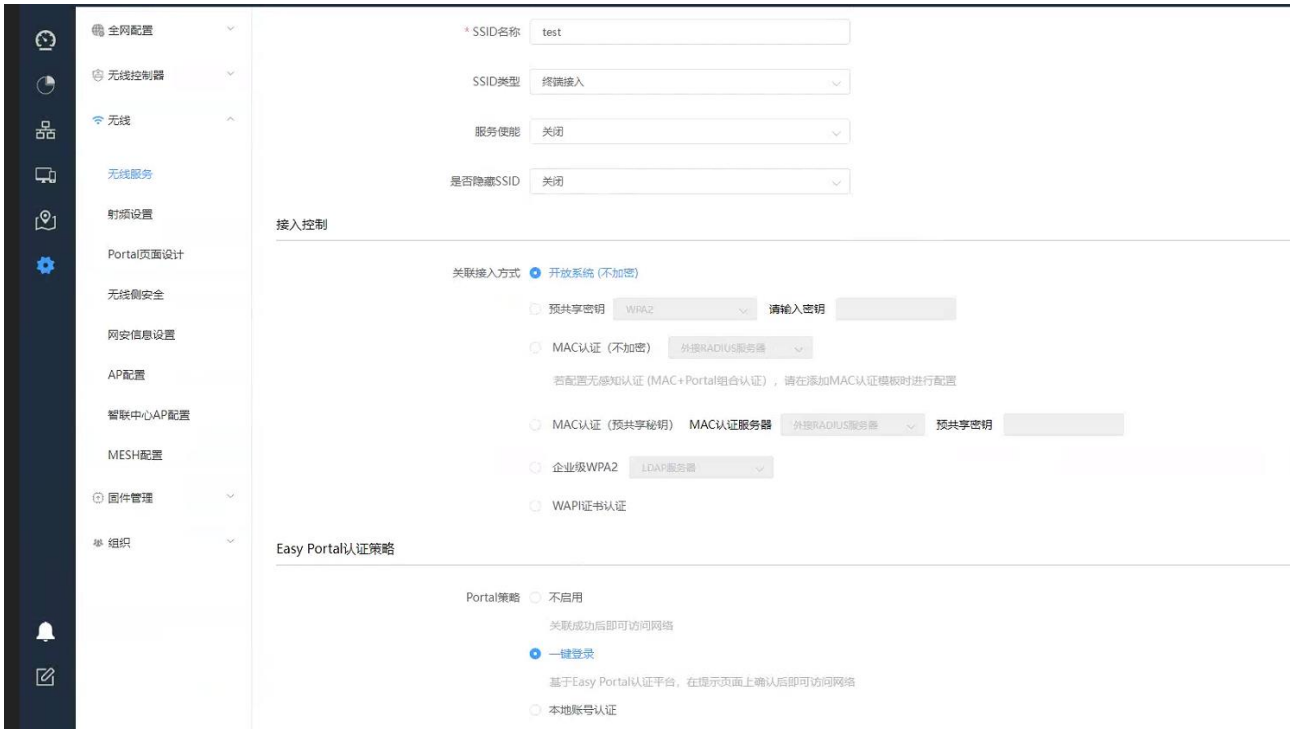
SSID 名称为：test

使能：开启

是否隐藏 SSID：广播 SSID

关联接入方式：开放系统（不加密）

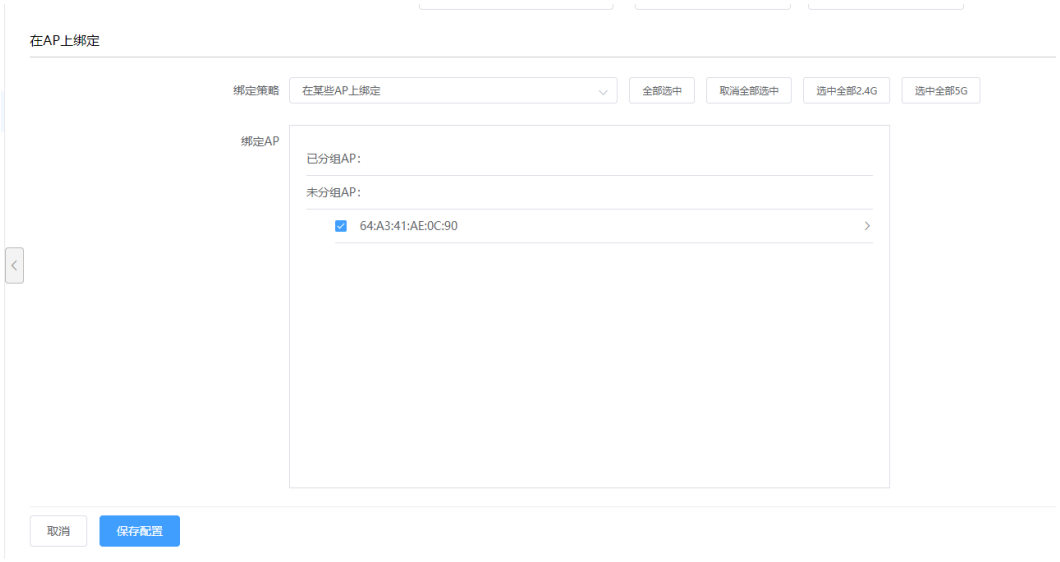
Easy Portal 认证策略：一键登录



数据转发方式：二层桥接模式

VLAN 标记：使用预置 VLAN 标记-101

选择要绑定的 AP 并保存



4.10.2.3 检查配置结果

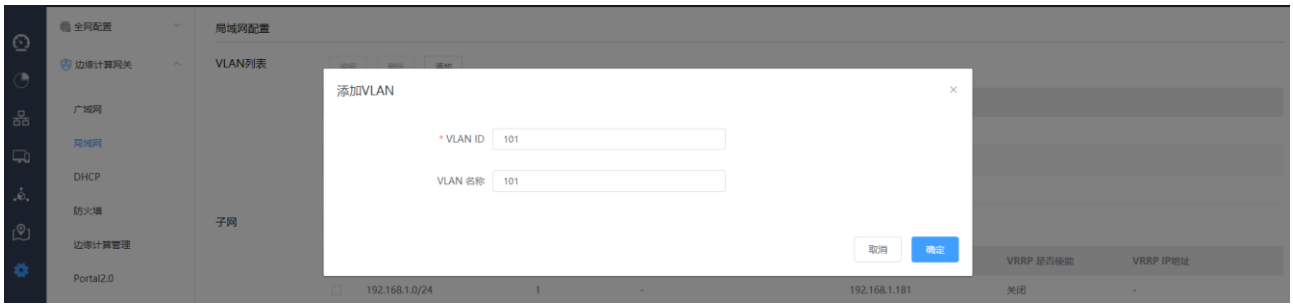
完成配置后，用户可通过无线终端搜索到 SSID 为 test 的无线网络。

终端连接上无线 SSID，在弹出的 web 认证界面上点击“一键登录”即可访问网络。

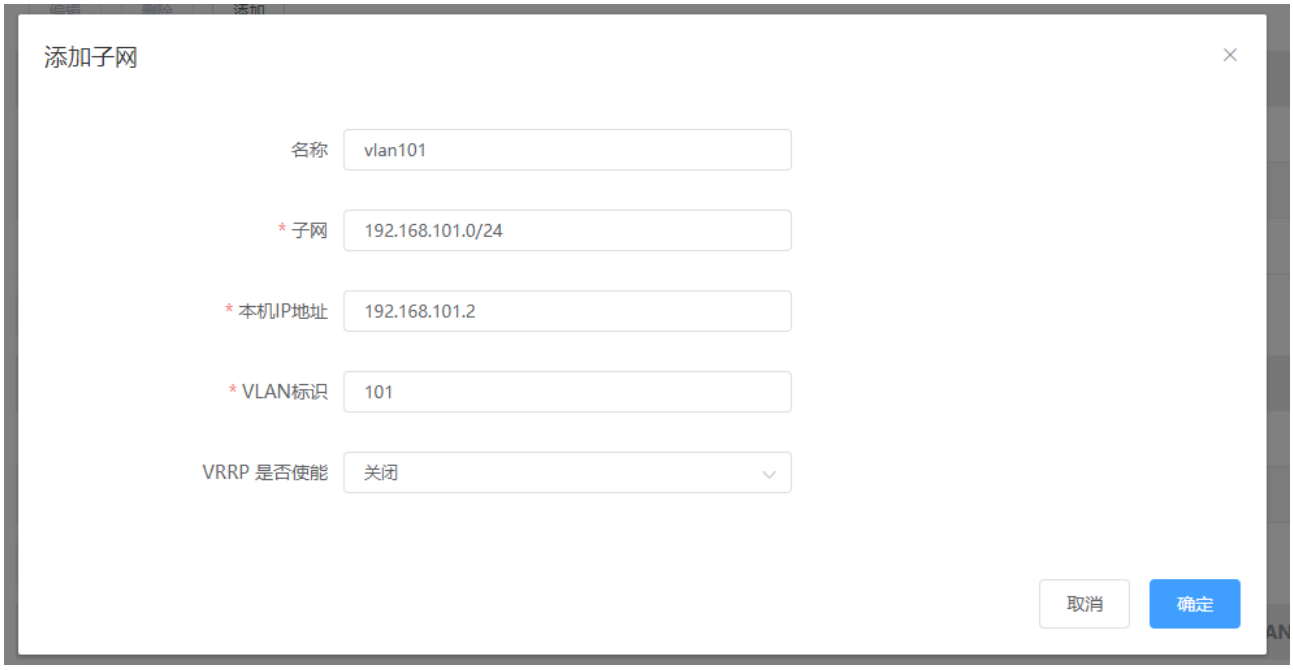
4.10.3 Portal-本地账号认证

4.10.3.1 配置子网 IP

路径:【设置】>子菜单【无线控制器】>子菜单【VLAN 列表】，添加业务 VLAN 101



路径:【设置】>子菜单【无线控制器】>子菜单【子网】，添加业务 VLAN 101 的子网，AC 配置子网 ip 为 192.168.101.2



4.10.3.2 配置 SSID

路径：【设置】>子菜单【无线】>子菜单【无线服务】，进入 WLAN 业务配置页面，选择模板配置 SSID

SSID 名称为：test

使能：开启

是否隐藏 SSID：广播 SSID

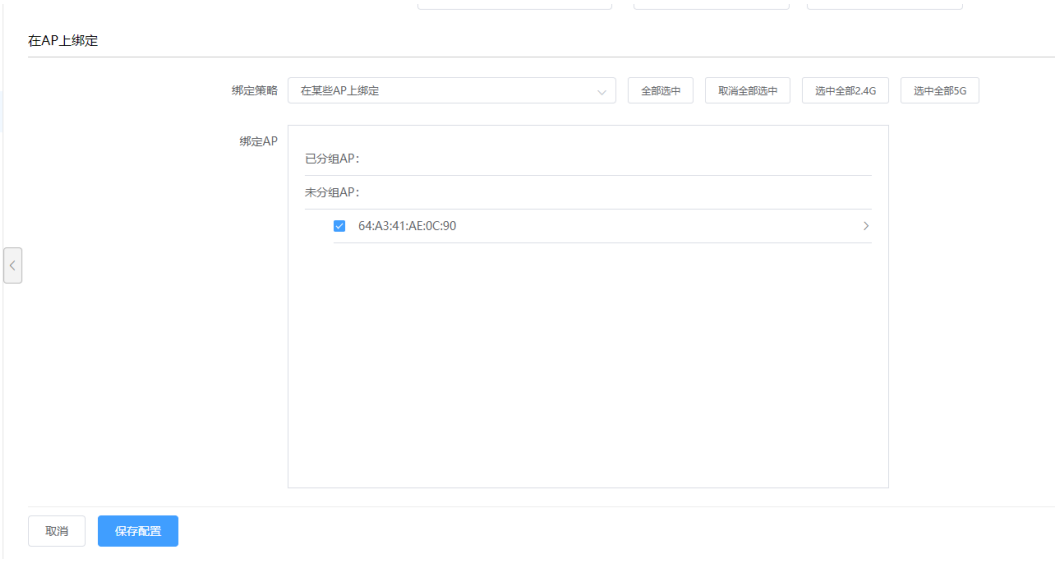
关联接入方式：开放系统（不加密）

Easy Portal 认证策略：本地账号认证

数据转发方式：二层桥接模式

VLAN 标记：使用预置 VLAN 标记-101

选择要绑定的 AP 并保存



4.10.3.3 portal 本地用户配置

✧ 配置认证策略模板：创建授权 portal 认证的模板，用户组/用户可绑定该模板。

路径:【设置】>子菜单【全网配置】>子菜单【用户管理】>子菜单【认证策略模板】><添加模板>

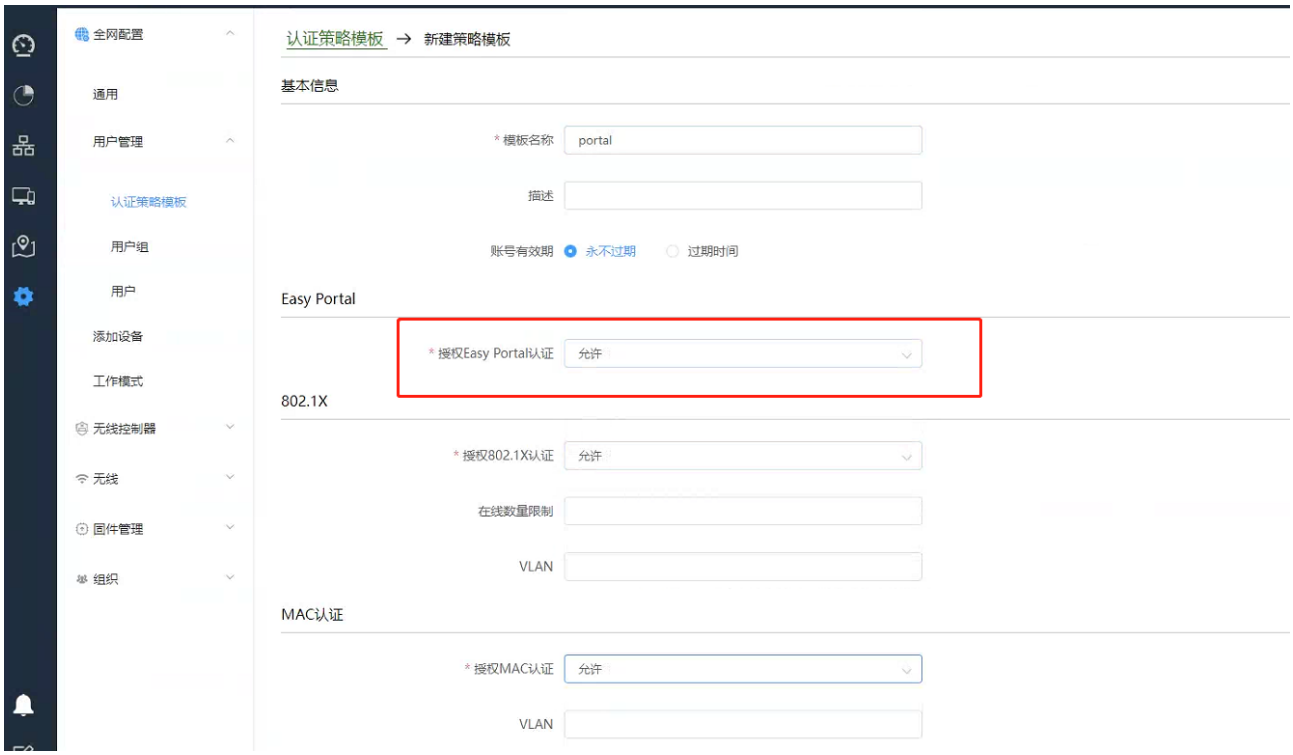
模板名称：可自定义

描述：可自定义

账号有效期：可选择永不过期或设置过期时间

Easy Portal：选择允许

802.1X 和 MAC 认证选择禁止授权



✧ 配置用户组：用户组上可绑定认证策略模板及 SSID

路径：【设置】>子菜单【全网配置】>子菜单【用户管理】>子菜单【用户组】><添加一级用户组>

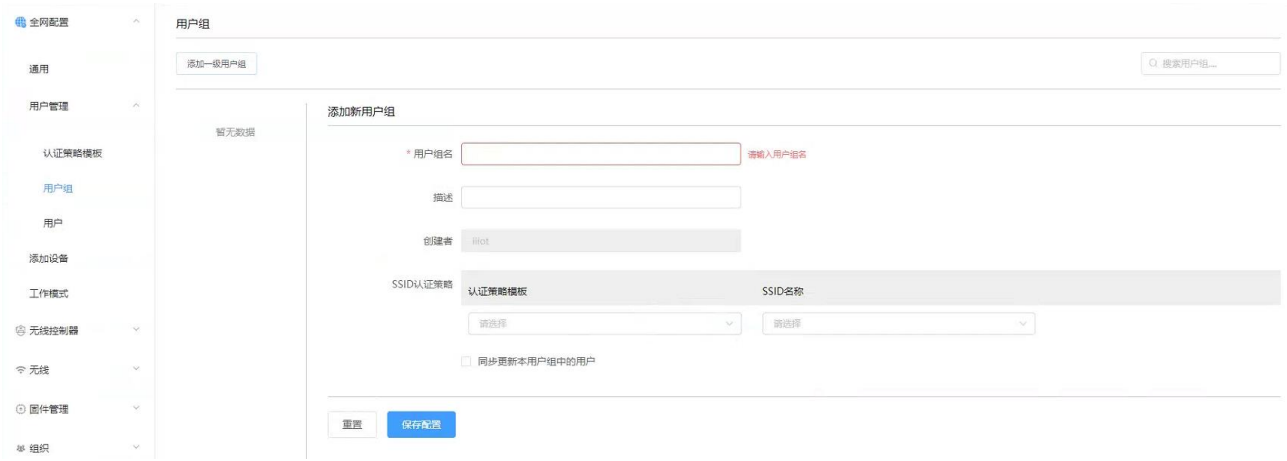
用户组名：可自定义

描述：可自定义

SSID 认证策略：选择上一步创建的认证策略模板（portal）及要绑定的 portal 认证的 SSID（test）

同步更新本用户组中的用户：选中后，会将本用户组中的认证策略模板和绑定的 SSID 同步到该用户组的所有用户。

点击<保存配置生效>

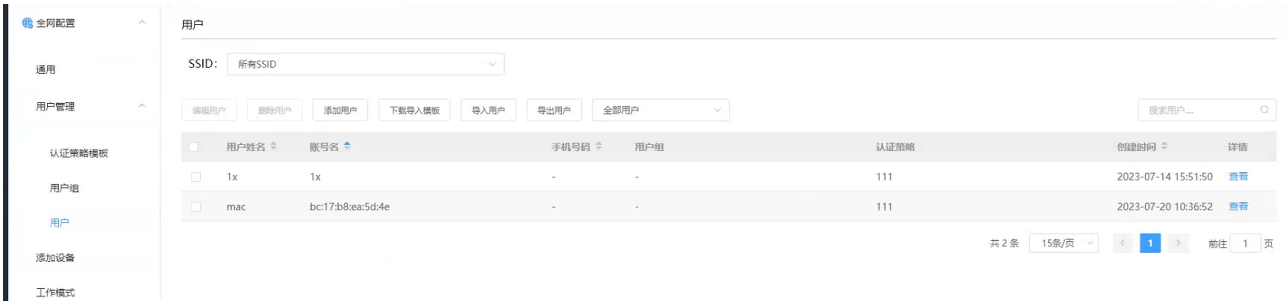


✧ 添加用户：添加 portal 认证用户

路径：【设置】>子菜单【全网配置】>子菜单【用户管理】>子菜单【用户】

SSID：在 SSID 下拉菜单选择 test 的 SSID

点击<添加用户>可添加单个用户；击<下载模板>，可通过模板批量导入用户

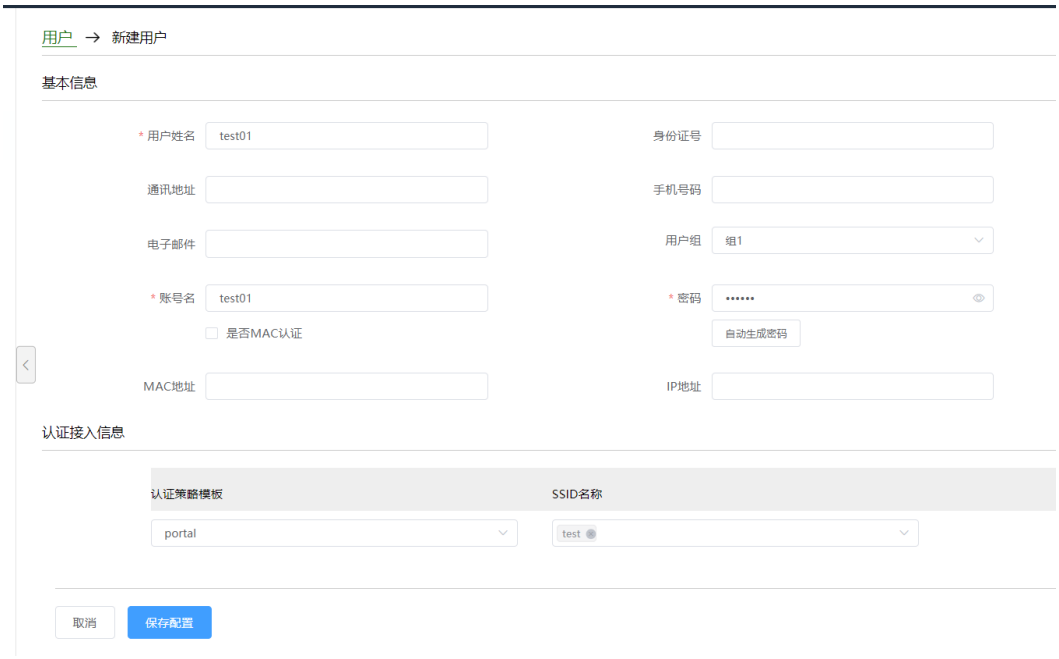


本例点击<添加用户>，弹出如下配置页面：

设置用户姓名、账号名和密码；

账号名栏填写账号名称；

选择用户分组-组 1，认证接入信息会自动变为组 1 中绑定的认证策略模板（portal）和 SSID（test），点击<保存配置>生效



4.10.3.4 检查配置结果

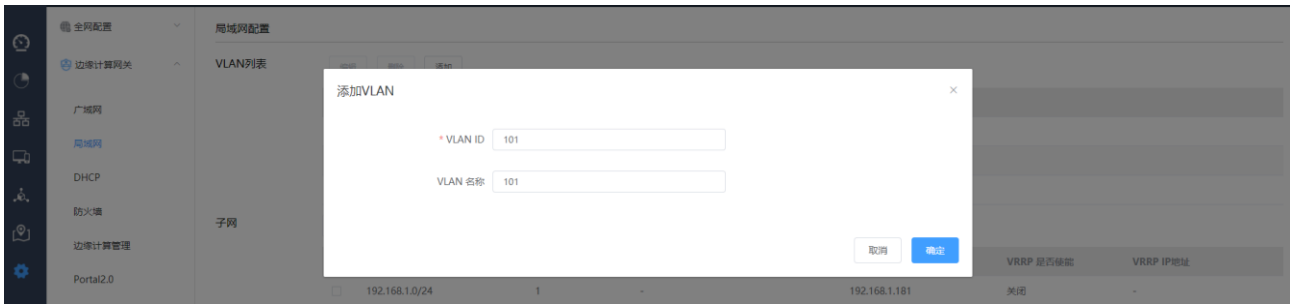
完成配置后，用户可通过无线终端搜索到 SSID 为 test 的无线网络。

终端连接上无线 SSID，在弹出的 web 认证界面上通过设置的 portal 账号密码可关联到该无线网络。

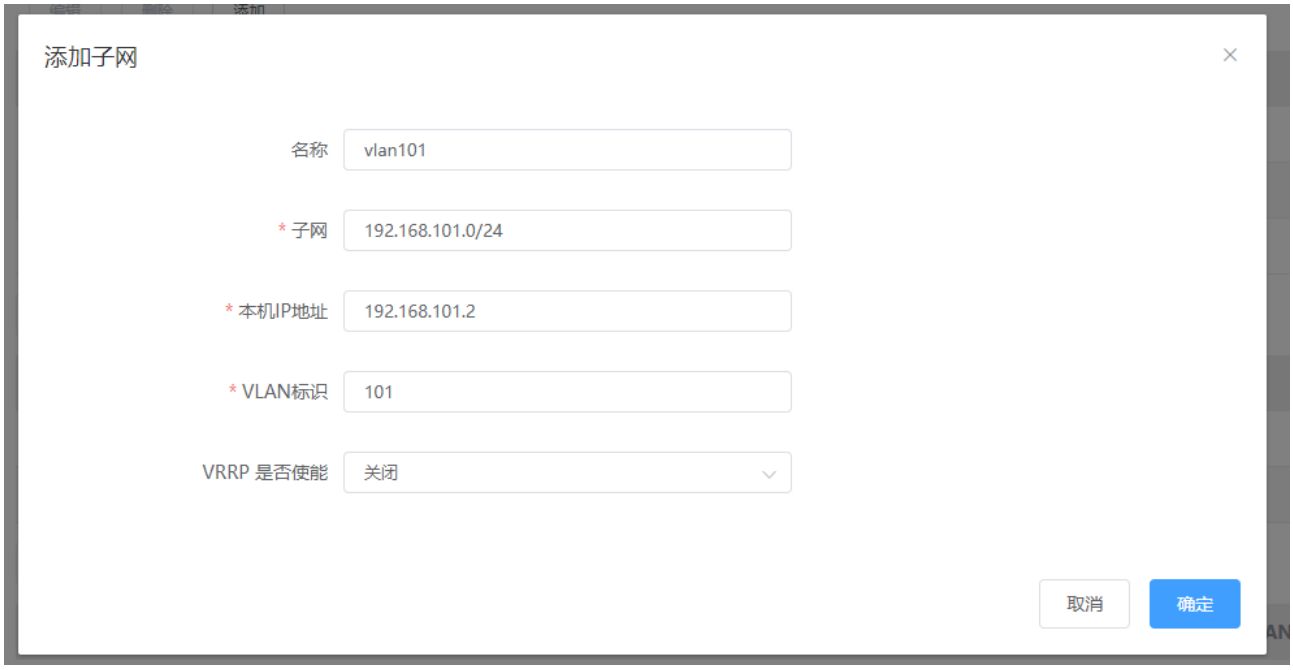
4.10.4 Portal-短信认证

4.10.4.1 配置子网 IP

路径:【设置】>子菜单【无线控制器】>子菜单【VLAN 列表】，添加业务 VLAN 101



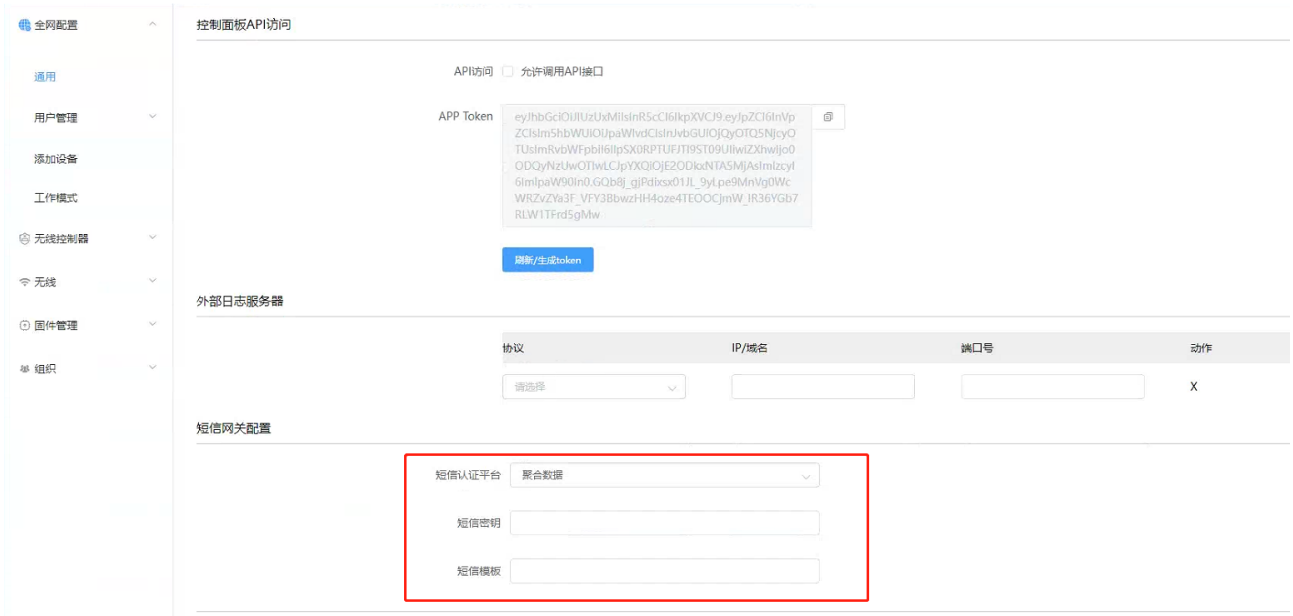
路径:【设置】>子菜单【无线控制器】>子菜单【局域网】，添加业务 VLAN 101 的子网，AC 配置子网 ip 为 192.168.101.2



4.10.4.2 配置短信网关

路径：【设置】>子菜单【全网配置】>子菜单【通用】，进入短信网关配置页面。

选择短信认证平台，填写短信密钥和短信模板信息并保存。



4.10.4.3 配置 SSID

路径：【设置】>子菜单【无线】>子菜单【无线服务】，进入 WLAN 业务配置页面，选择模板配置 SSID

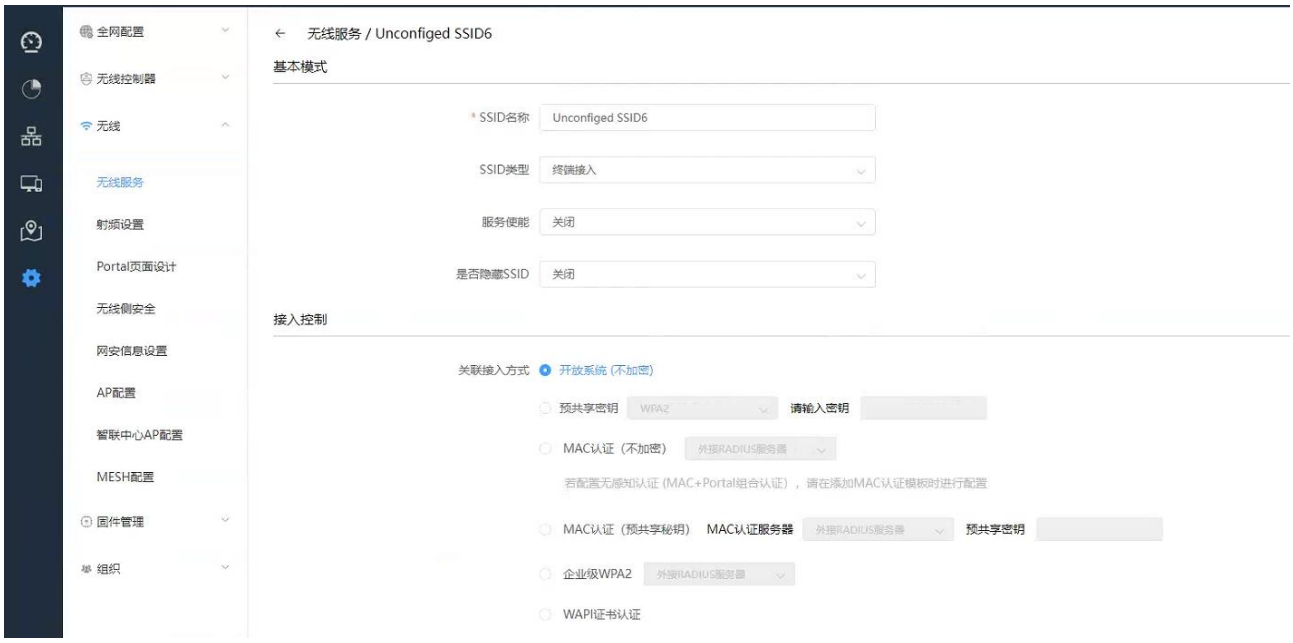
SSID 名称为：test

使能：开启

是否隐藏 SSID：广播 SSID

关联接入方式：开放系统（不加密）

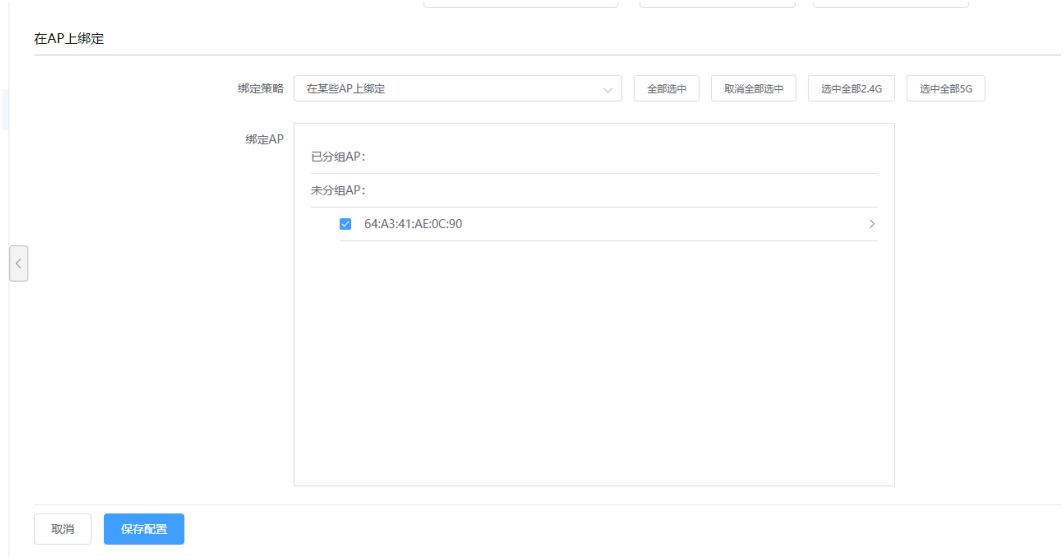
Easy Portal 认证策略：短信认证



数据转发方式：二层桥接模式

VLAN 标记：使用预置 VLAN 标记-101

选择要绑定的 AP 并保存



4.10.4.4 检查配置结果

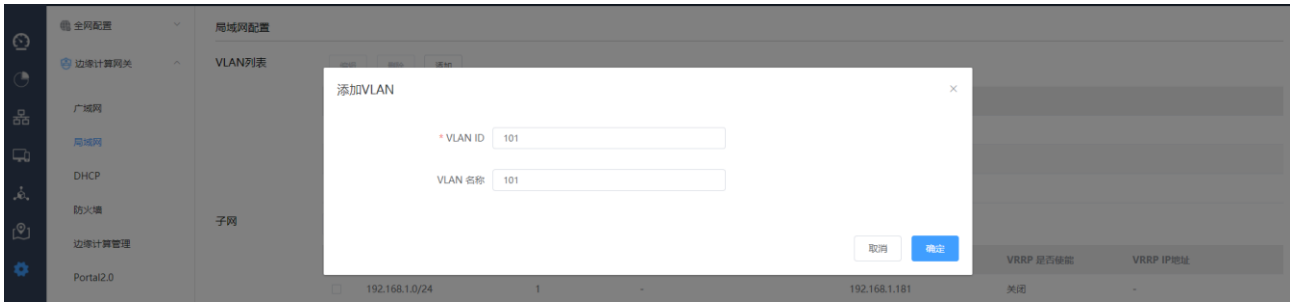
完成配置后，用户可通过无线终端搜索到 SSID 为 test 的无线网络。

终端连接上无线 SSID，在弹出的 portal 页面上输入手机号码获取短信验证码，填写验证码登录即可获取相应的上网权限。

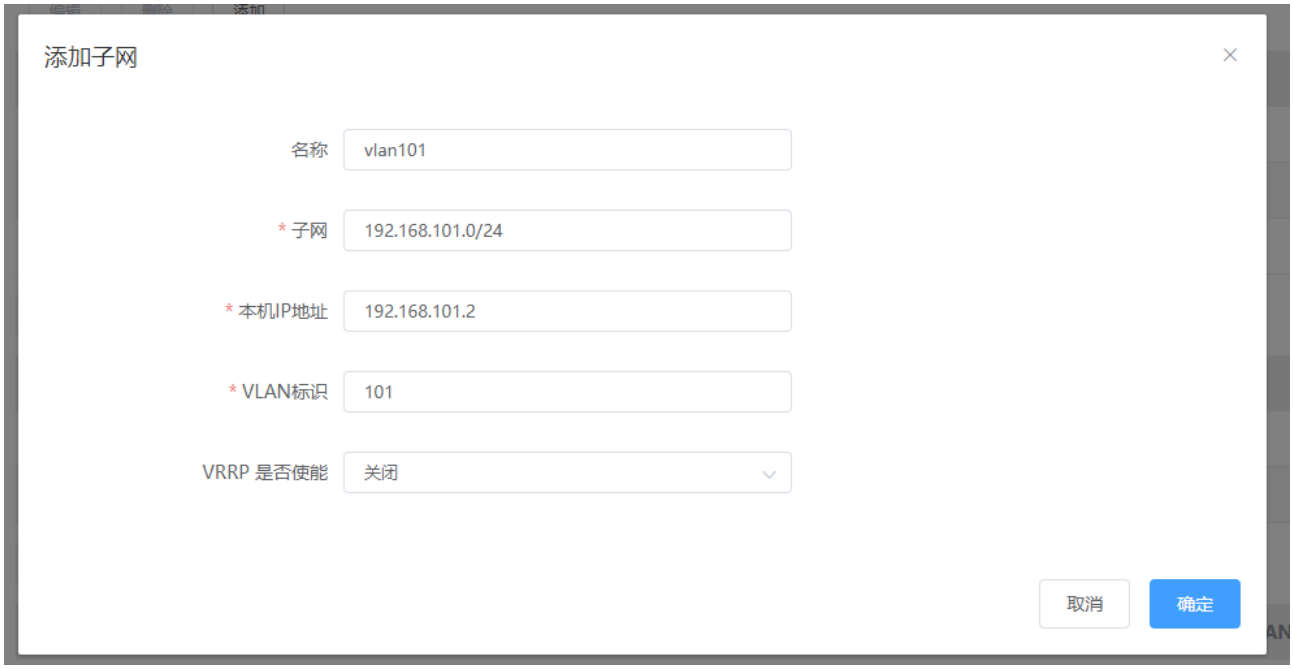
4.10.5 Portal-免认证，受限访问

4.10.5.1 配置子网 IP

路径：【设置】>子菜单【无线控制器】>子菜单【VLAN 列表】，添加业务 VLAN 101



路径：【设置】>子菜单【无线控制器】>子菜单【子网】，添加业务 VLAN 101 的子网，AC 配置子网 ip 为 192.168.101.2



4.10.5.2 配置 SSID

路径：【设置】>子菜单【无线】>子菜单【无线服务】，进入 WLAN 业务配置页面，选择模板配置 SSID

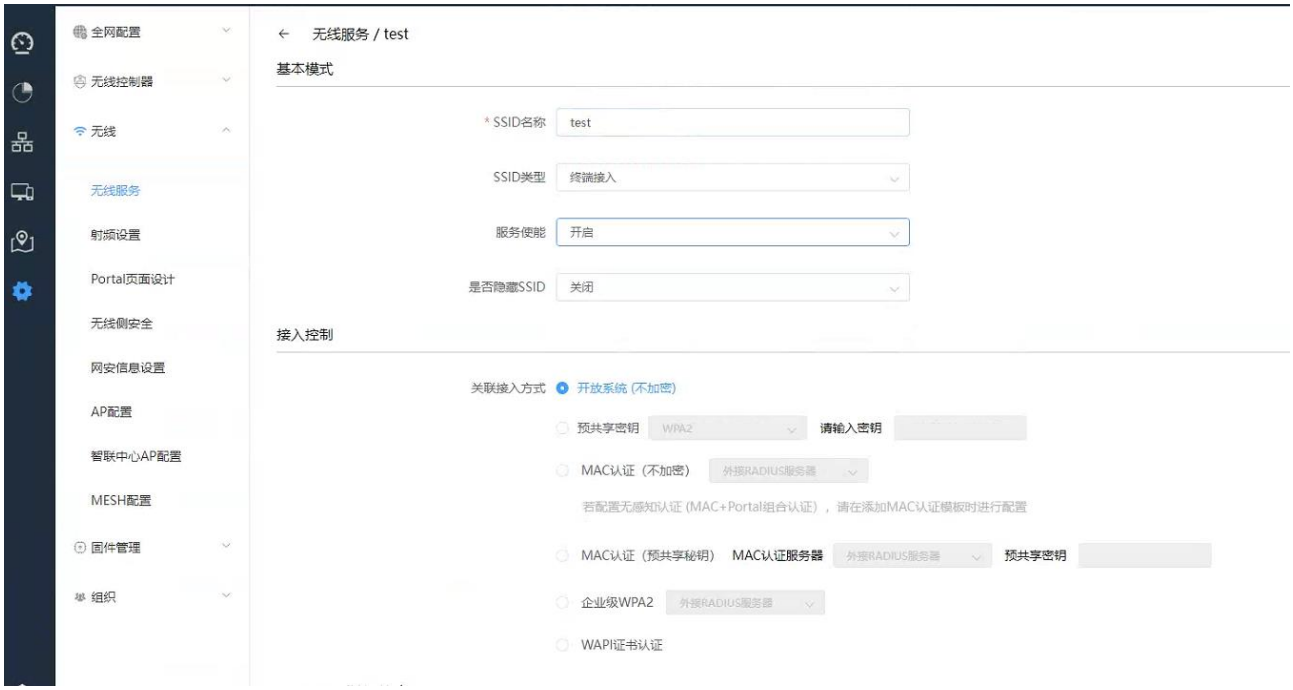
SSID 名称为：test

使能：开启

是否隐藏 SSID：广播 SSID

关联接入方式：开放系统（不加密）

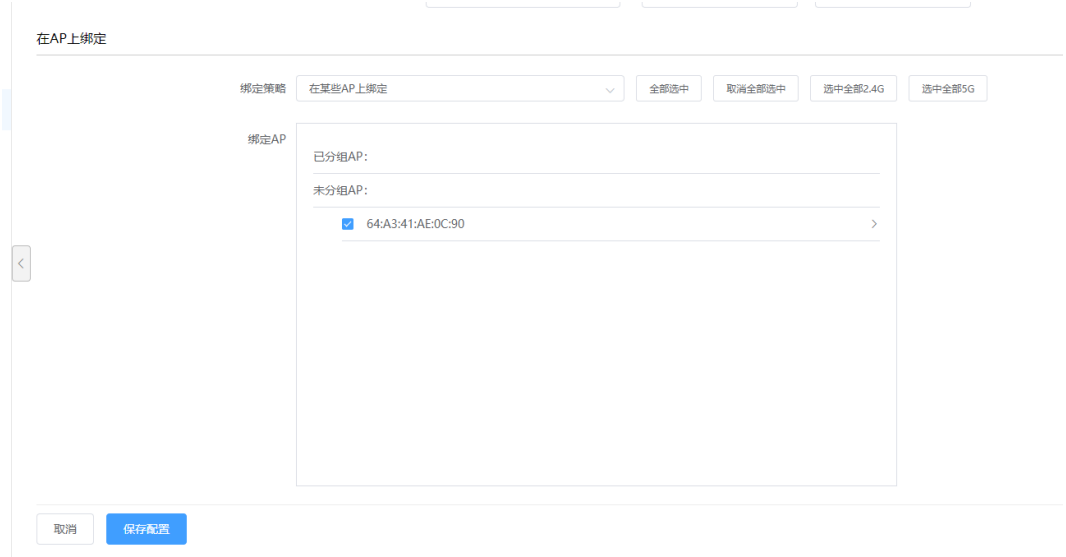
Easy Portal 认证策略：免认证，受限访问



数据转发方式：二层桥接模式

VLAN 标记：使用预置 VLAN 标记-101

选择要绑定的 AP 并保存

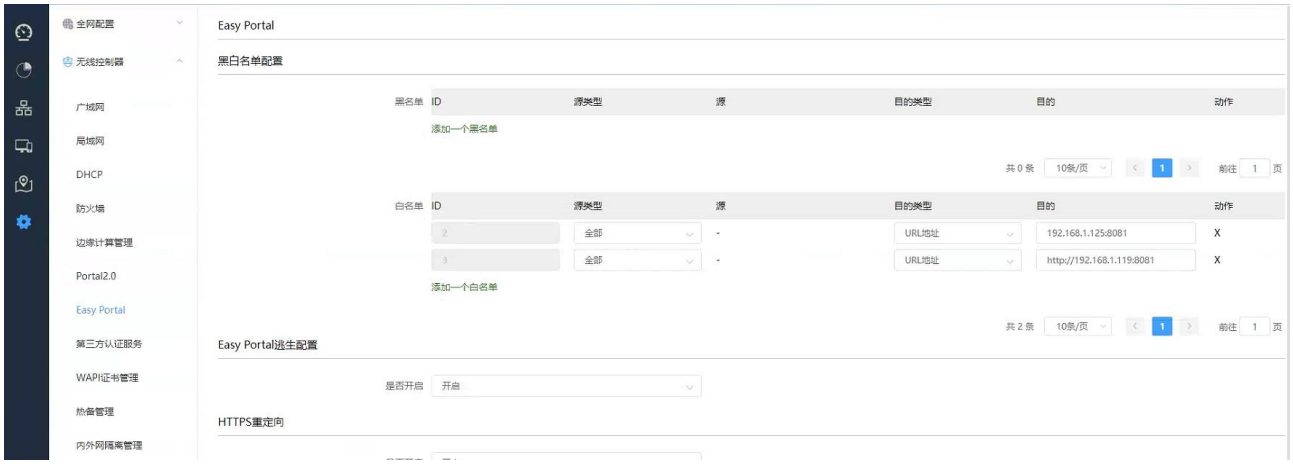


4.10.5.3 受限访问黑白名单设置

路径:【设置】>子菜单【无线控制器】>子菜单【Easy Portal】>【黑白名单配置】页面

点击<添加一个黑名单>或<添加一个白名单>配置限访问受限的网络资源

源类型可以为全部、IP 地址、Mac 地址、VLAN，目的类型可以为全部、IP 地址、URL 地址。详细如下图所示：



4.10.5.4 检查配置结果

完成配置后，用户可通过无线终端搜索到 SSID 为 test 的无线网络。

终端连接上无线 SSID，即可获取相应的上网权限。

4.10.6 Portal-LDAP

4.10.6.1 配置第三方认证服务

AC 上 LDAP 参数配置

路径:【设置】>子菜单【无线控制器】>子菜单【第三方认证服务】>【LDAP 认证服务器配置】

主/备服务器：可以是 IP 地址或域名，本例是 192.168.1.168

端口号：默认 389 主备必须相同（freeradius 限制）

通用服务器路径：用户搜索的基本路径，本例为：CN=Users,dc=inspur,dc=local

用户标识：openLDAP 使用 uid，windows server 使用 cn，本例为：cn

分组标识：openLDAP 使用 posixGroup(openldap)，windows server 使用 Group(windows ad)

用户名：管理用户，用户加域名后缀，本例为：dcao@inspur.local

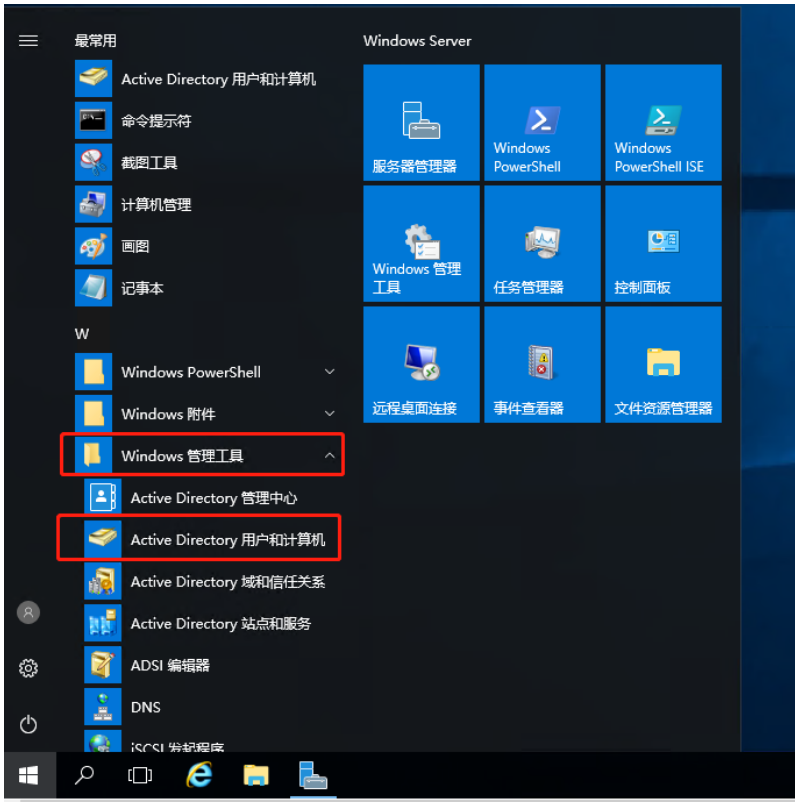
密码：管理用户的密码，本例为：12345678

Windows2000 前域名：可选择保留原有域名和不携带域名

2、LDAP 相关配置

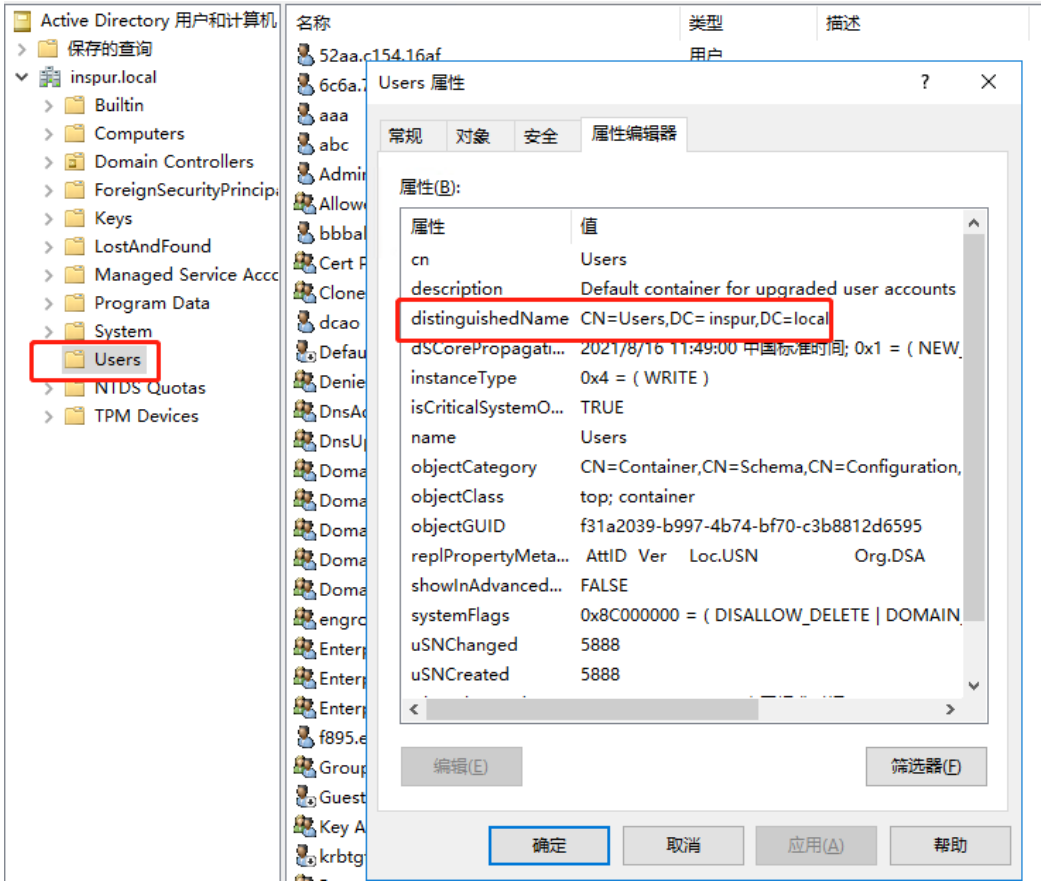
（1）通用服务器路径查看方法：

1） 通过菜单打开 AD 的用户管理



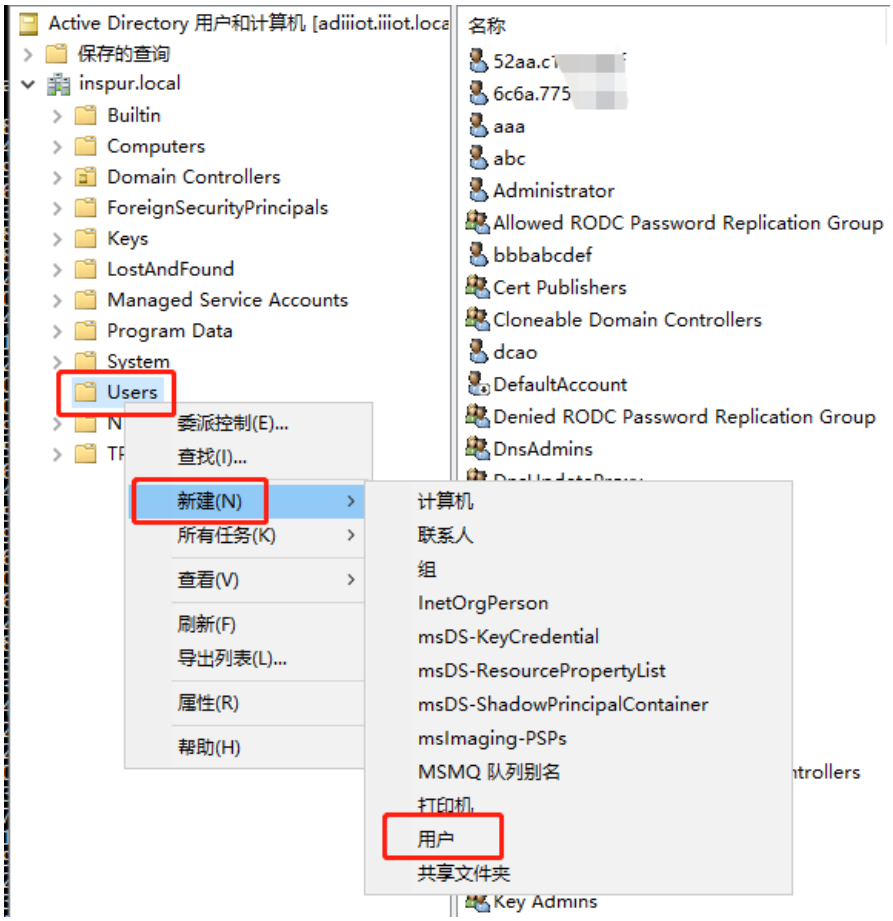
2） 在用户所属组上点击右键，选择属性出现以下对话框，可以看到通用搜索路径。为了提高效率在明确用户组的情况下可以从用户组开始，本例为：CN=Users,dc=inspur,dc=local。

如果不明确用户在哪个组，可以从下一级开始，例如，dc=inspur,dc=local



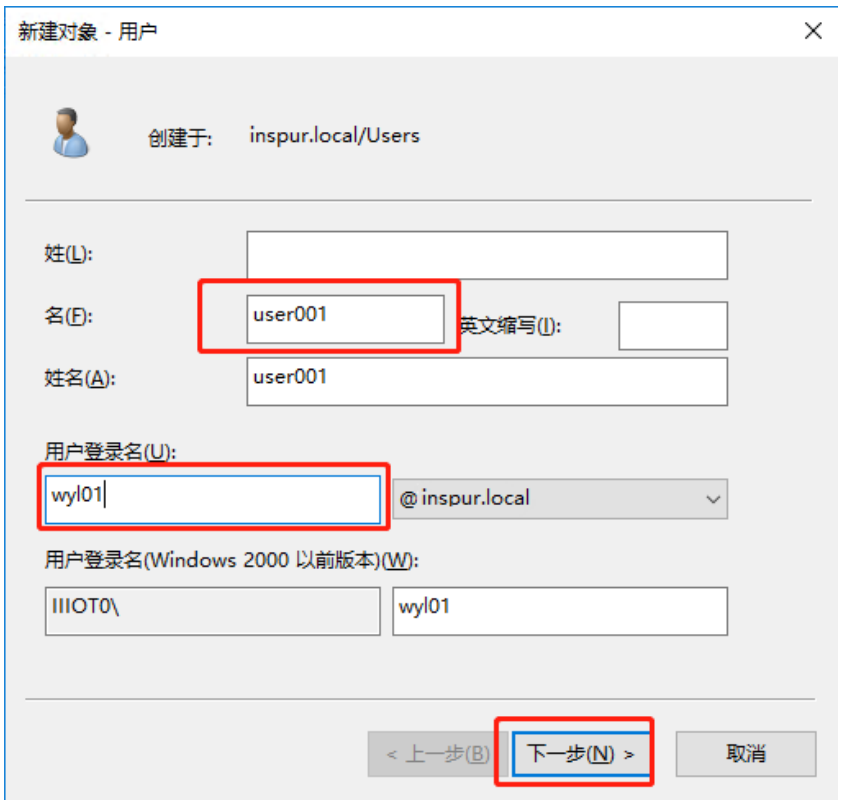
（2）认证用户的添加

1） 在 users 目录上点击右键，新建用户



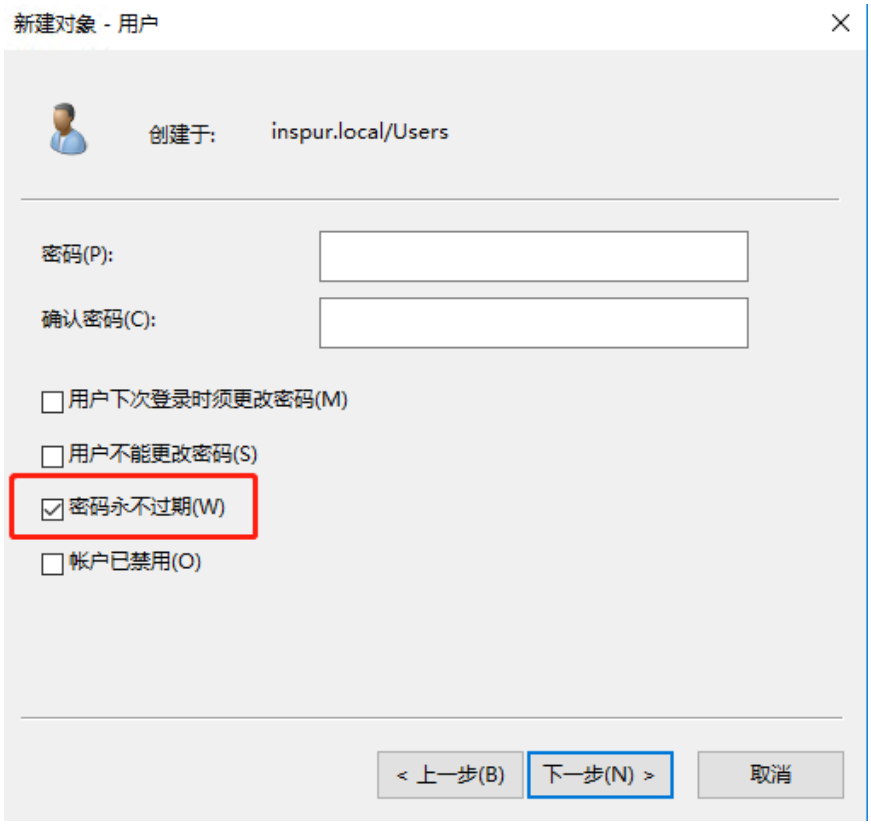
2) 填写用户信息

名（F）处填写 LDAP 认证的用户名



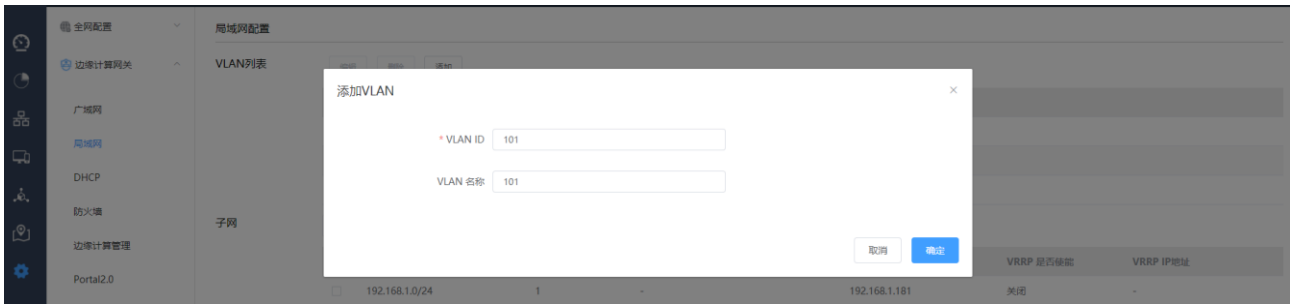
3) 选择密码策略为永不过期

设置用户密码，密码永不过期

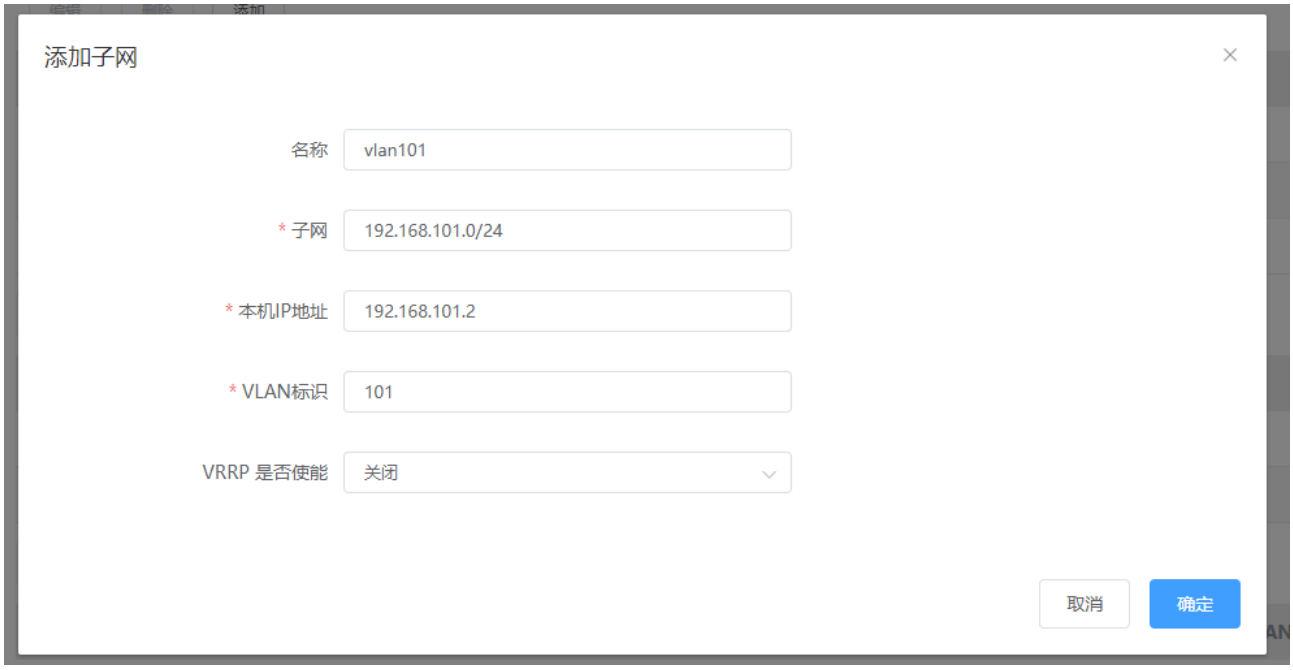


4.10.6.2 配置子网 IP

路径：【设置】>子菜单【无线控制器】>子菜单【VLAN 列表】，添加业务 VLAN 101



路径：【设置】>子菜单【无线控制器】>子菜单【子网】，添加业务 VLAN 101 的子网，AC 配置子网 ip 为 192.168.101.2



4.10.6.3 配置 SSID

路径：【设置】>子菜单【无线】>子菜单【无线服务】，进入 WLAN 业务配置页面，选择模板配置 SSID

SSID 名称为：test

使能：开启

是否隐藏 SSID：广播 SSID

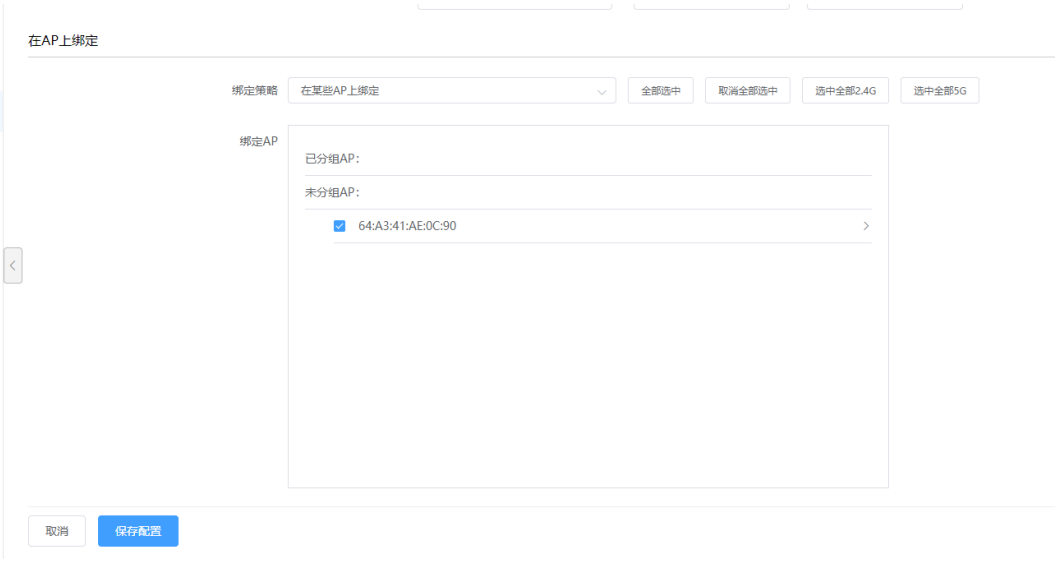
关联接入方式：开放系统（不加密）

Easy Portal 认证策略：LDAP

数据转发方式：二层桥接模式

VLAN 标记：使用预置 VLAN 标记-101

选择要绑定的 AP 并保存



4.10.6.4 检查配置结果

完成配置后，用户可通过无线终端搜索到 SSID 为 test 的无线网络。

终端连接上无线 SSID，在弹出的 portal 页面上输入 LDAP 服务器上已添加账号和密码登录即可获取相应的上网权限。

4.10.6.5 附：LDAP 组用户在线数量限制功能

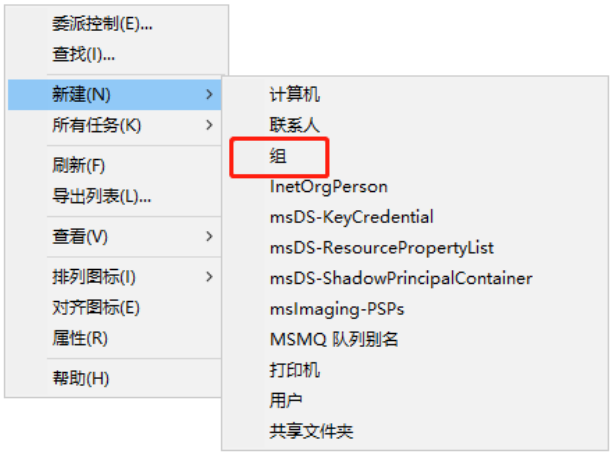
若要使用 LDAP 组用户在线数量限制功能，需要将 LDAP 用户加入到用户组，并在 AC 上创建同名用户组绑定认证策略。当并发在线设备数量超过配置的数量后，新用户无法认证通过。

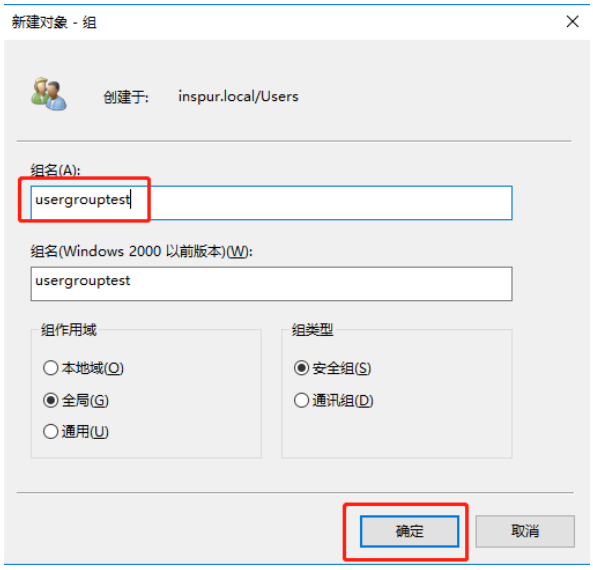
具体过程如下:

LDAP 服务器配置：

A.创建 LDAP 用户组

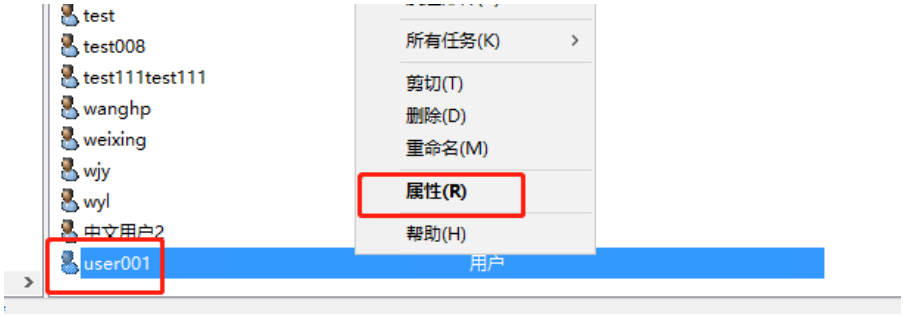
在 LDAP 服务器 users 目录上点击右键，新建组，输入要创建的组名，本例为 usergrouptest



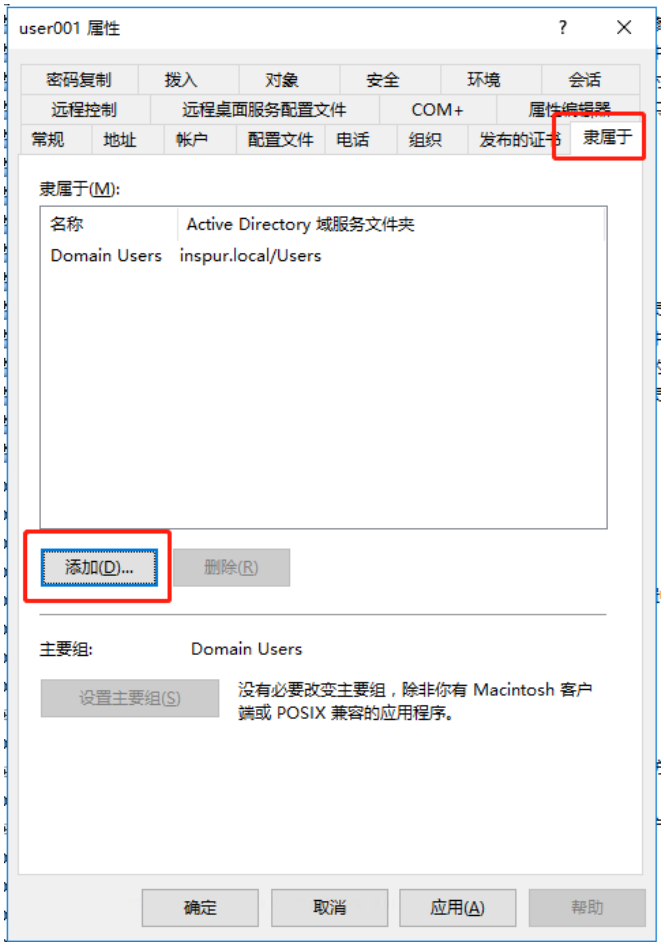


B. 将 LDAP 用户加入到用户组

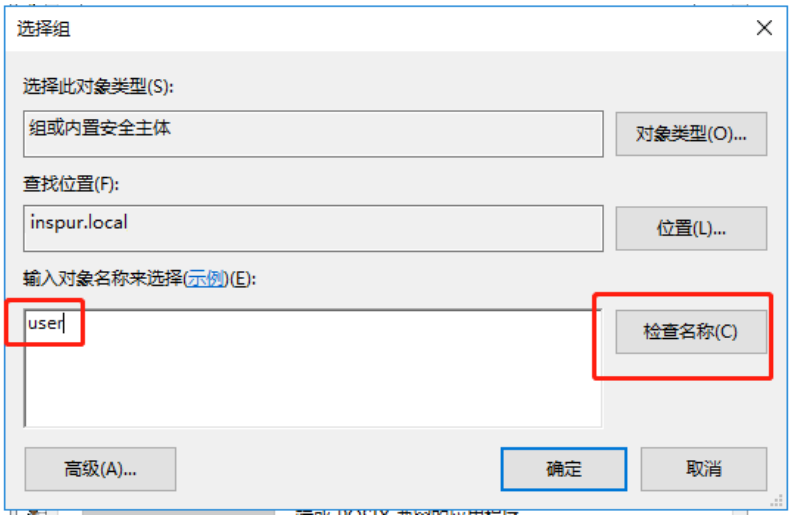
选择要设置的 LDAP 用户，点击右键，选择属性



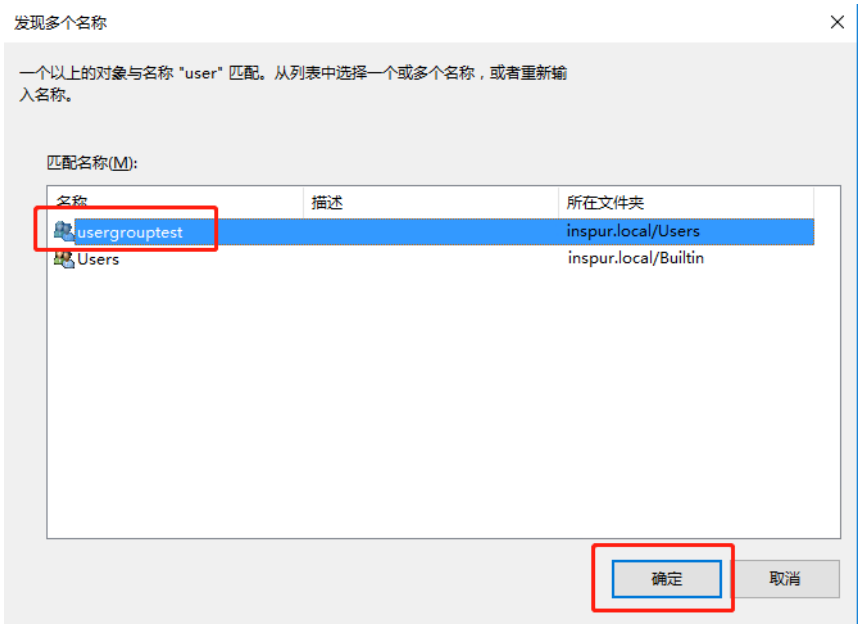
在“隶属于”标签页点击<添加>



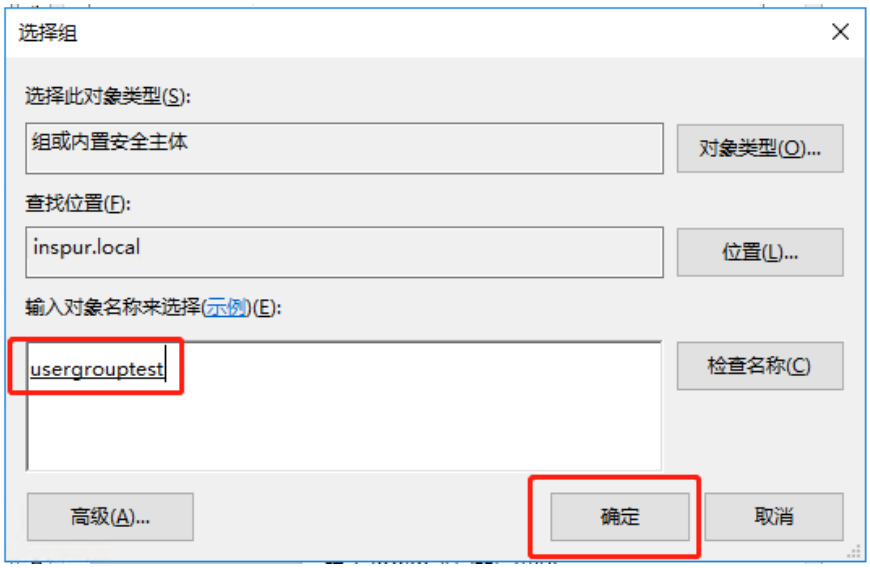
输入用户组关键字或全称，点击<检查名称>



选择用户组后点击<确定>



选择用户组后，用户组会带下划线，检查无误后，点击<确定>

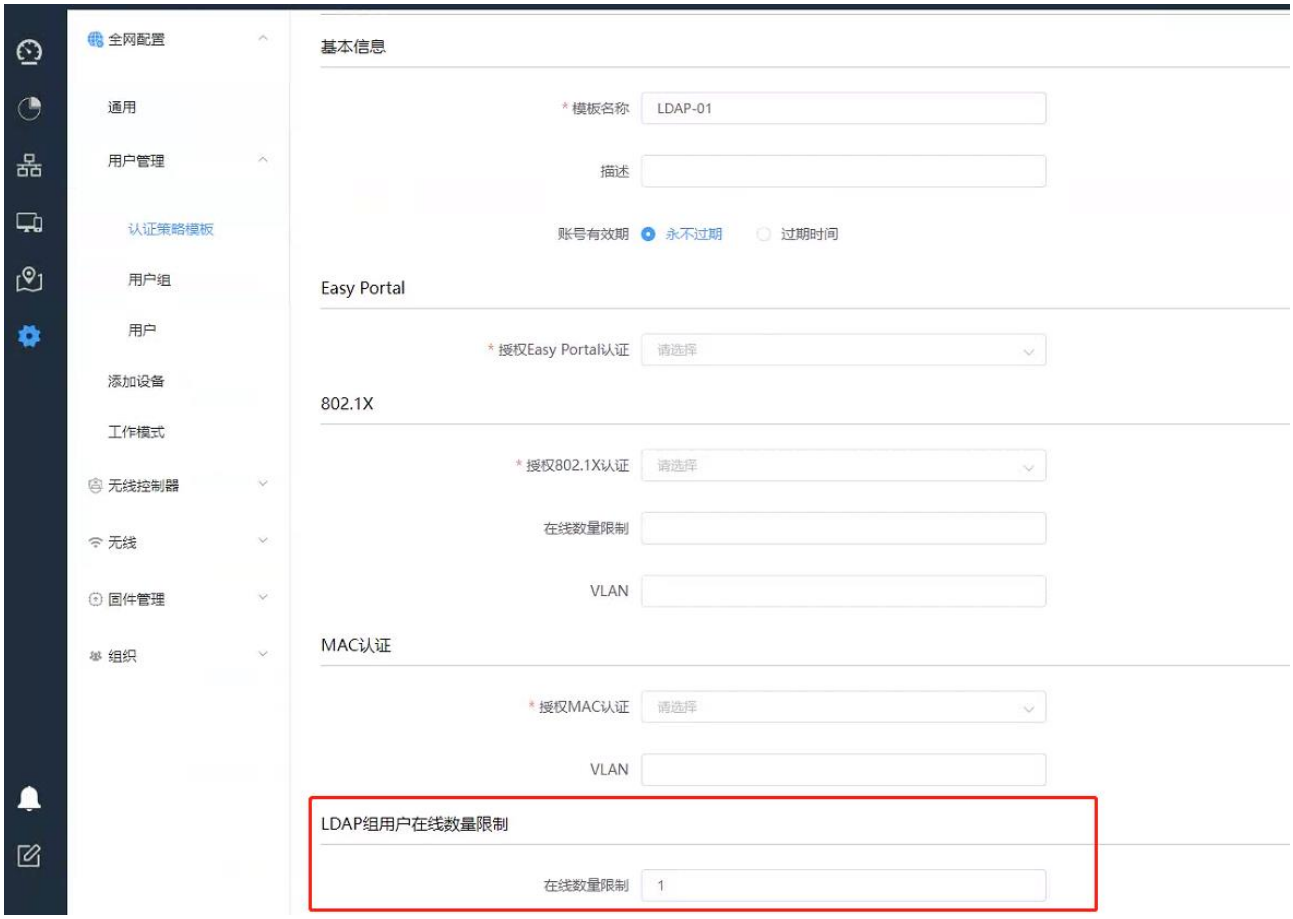


AC 配置：

A.创建认证策略模板

路径:【设置】>【全网配置】>【用户管理】>【认证策略模板】，点击<添加模板>

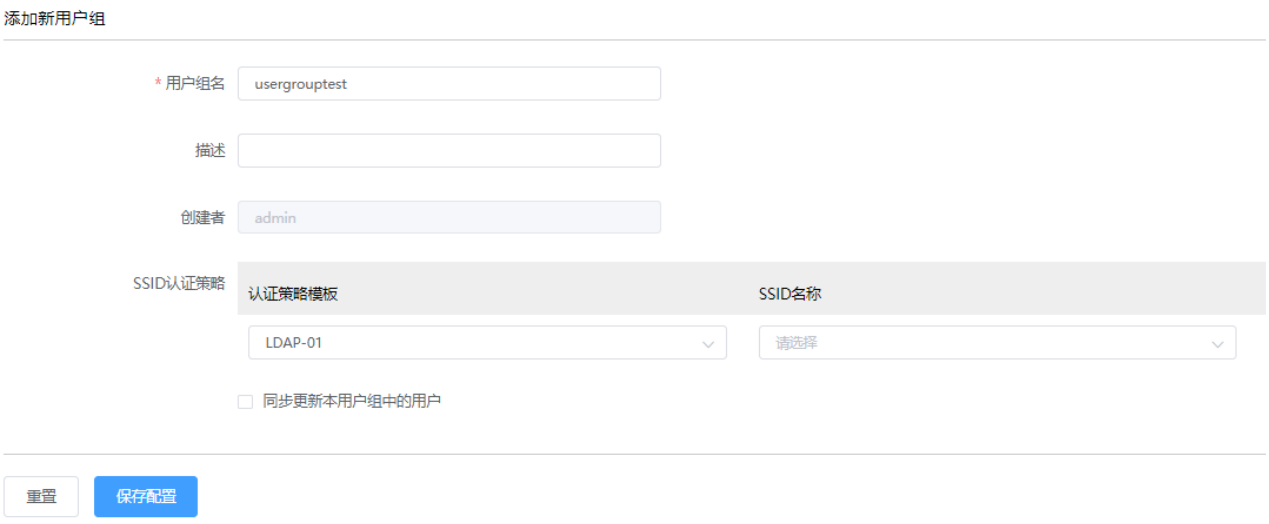
输入模板名称，在“LDAP 组用户在线数量限制”栏设置限制同时登录的终端数量，其余带星号的内容选择禁止，点击<保存配置>



B. 创建用户组

路径：【设置】>【全网配置】>【用户管理】>【用户组】，点击<添加一级用户组>

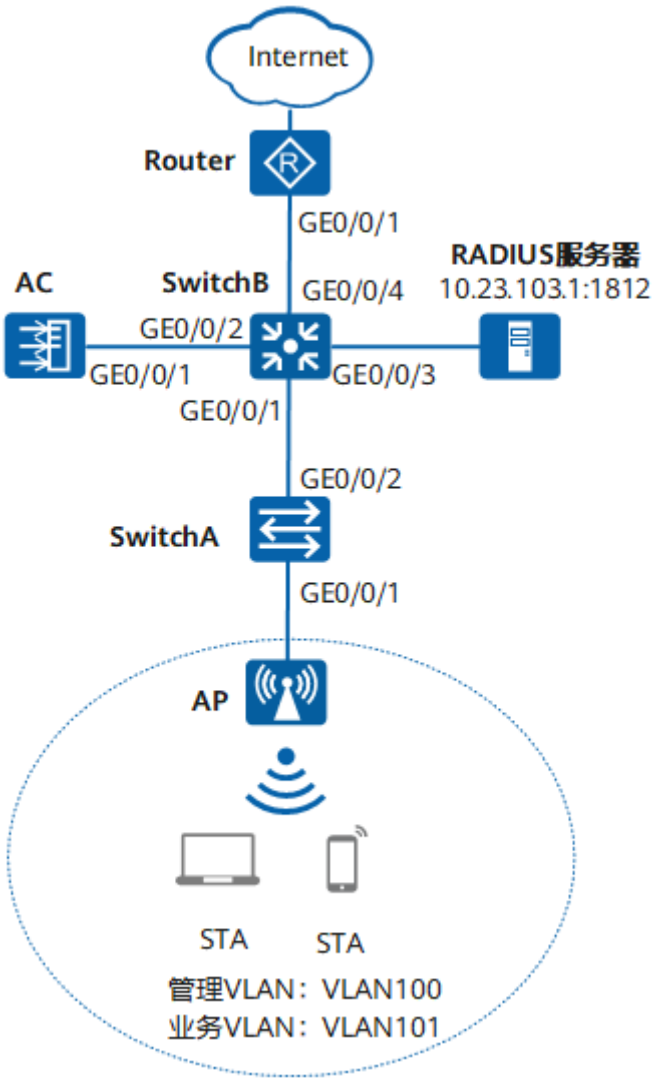
输入用户组名（必须与 LDAP 服务器上设置的用户组名相同），SSID 认证策略选择上一步创建的认证策略模板并保存配置。



5 典型配置

5.1 配置内部人员接入 WLAN 网络示例（802.1X 认证）

5.1.1 网络拓扑示意



5.1.2 业务需求

用户接入 WLAN 网络，使用 802.1X 客户端进行认证，输入正确的用户名和密码后可以无线上网。且在覆盖区域内移动发生漫游时，不影响用户的业务使用。

5.1.3组网需求

组网需求：

- AC 组网方式：旁挂二层组网。
- DHCP 部署方式：AC 作为 DHCP 服务器为 AP 分配 IP 地址，SwitchB 作为 DHCP 服务器为 STA 分配 IP 地址。
- 业务数据转发方式：本地转发。
- WLAN 认证方式：WPA-WPA2+802.1X。

5.1.4网络规划

配置项	规划数据
管理 VLAN	VLAN100
业务 VLAN	VLAN101
AC 的源接口	VLANIF100：10.23.100.254/24
DHCP 服务器	AC 作为 DHCP 服务器为 AP 分配 IP 地址，SwitchB 作为 DHCP 服务器为 STA 分配 IP 地址
AP 的 IP 地址池	10.23.100.1～10.23.100.200/24
STA 的 IP 地址池	10.23.101.1～10.23.101.200/24
RADIUS 认证 RADIUS 服务器参数	IP 地址：10.23.103.1 认证端口号：1812 共享密钥：inspur@123
802.1X 接入模板	认证方式：EAP
SSID 名称	SSID 名称：WLAN_test
安全策略	安全策略：WPA-WPA2+802.1X+AES
VAP 模板	转发模式：本地转发 业务 VLAN：VLAN101

5.1.5配置思路

- ✧ 配置 AP、AC 和周边网络设备之间实现网络互通。
- ✧ 配置 AC 局域网
- ✧ 配置 AP 在 AC 上线。
- ✧ 在 AC 上配置 WLAN 相关业务（SSID）。
- ✧ 配置第三方认证服务器。

5.1.6操作步骤

5.1.6.1 配置周边设备

配置接入交换机 SwitchA 的接口 GE0/0/1 和 GE0/0/2 加入 VLAN100 和 VLAN101。

```
inspur# enable
inspur# configure terminal
inspur(config)# hostname SwitchA
SwtchA(config)# vlan database
SwtchA(config-vlan)# vlan 100-101
SwtchA(config-vlan)# quit
SwtchA(config)# interface eth-0-1
SwtchA(config-if)# switchport mode trunk
SwtchA(config-if)# switchport trunk native vlan 100
SwtchA(config-if)# switchport trunk allowed vlan add 100-101
SwtchA(config-if)# quit
SwtchA(config)# interface eth-0-2
SwtchA(config-if)# switchport mode trunk
SwtchA(config-if)# switchport trunk allowed vlan add 100-101
SwtchA(config-if)# quit
```

配置汇聚交换机 SwitchB 的接口 GE0/0/1 加入 VLAN100 和 VLAN101，GE0/0/2 加入 VLAN100 和 VLAN102，GE0/0/3 加入 VLAN103，GE0/0/4 加入 VLAN104，创建 VLANIF102、VLANIF103 和 VLANIF104 接口，并配置下一跳为 Router 的缺省路由。

```
inspur# enable
inspur# configure terminal
inspur(config)# hostname SwitchB
SwtchB(config)# vlan database
SwtchB(config-vlan)# vlan 100-104
SwtchB(config-vlan)# quit
SwtchB(config)# interface eth-0-1
SwtchB(config-if)# switchport mode trunk
SwtchB(config-if)# switchport trunk allowed vlan add 100-101
SwtchB(config-if)# quit
SwtchB(config)# interface eth-0-2
SwtchB(config-if)# switchport mode trunk
SwtchB(config-if)# switchport trunk allowed vlan add 100
SwtchB(config-if)# switchport trunk allowed vlan add 102
SwtchB(config-if)# quit
SwtchB(config)# interface eth-0-3
SwtchB(config-if)# switchport mode trunk
SwtchB(config-if)# switchport trunk native vlan 103
SwtchB(config-if)# switchport trunk allowed vlan add 103
SwtchB(config-if)# quit
SwtchB(config)# interface eth-0-4
SwtchB(config-if)# switchport mode trunk
SwtchB(config-if)# switchport trunk native vlan 104
SwtchB(config-if)# switchport trunk allowed vlan add 104
SwtchB(config-if)# quit
SwtchB(config)# interface vlan 102
SwtchB(config-if)# ip address 10.23.102.1/24
SwtchB(config-if)# quit
SwtchB(config)# interface vlan 103
SwtchB(config-if)# ip address 10.23.103.2/24
SwtchB(config-if)# quit
```

```
SwtchB(config)# interface vlan 104
SwtchB(config-if)# ip address 10.23.104.1/24
SwtchB(config-if)# quit
SwtchB(config)# ip route 0.0.0.0 0.0.0.0 10.23.104.2
```

配置 Router 的接口 GE0/0/1 的 IP 地址，并配置指向 STA 网段的静态路由。

```
<Inspur> system-view
[Inspur] sysname Router
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] ip address 10.23.104.2 24
[Router-GigabitEthernet0/0/1] quit
[Router] ip route-static 10.23.101.0 24 10.23.104.1
```

5.1.6.2 配置 DHCP 服务器为 STA 分配 IP 地址

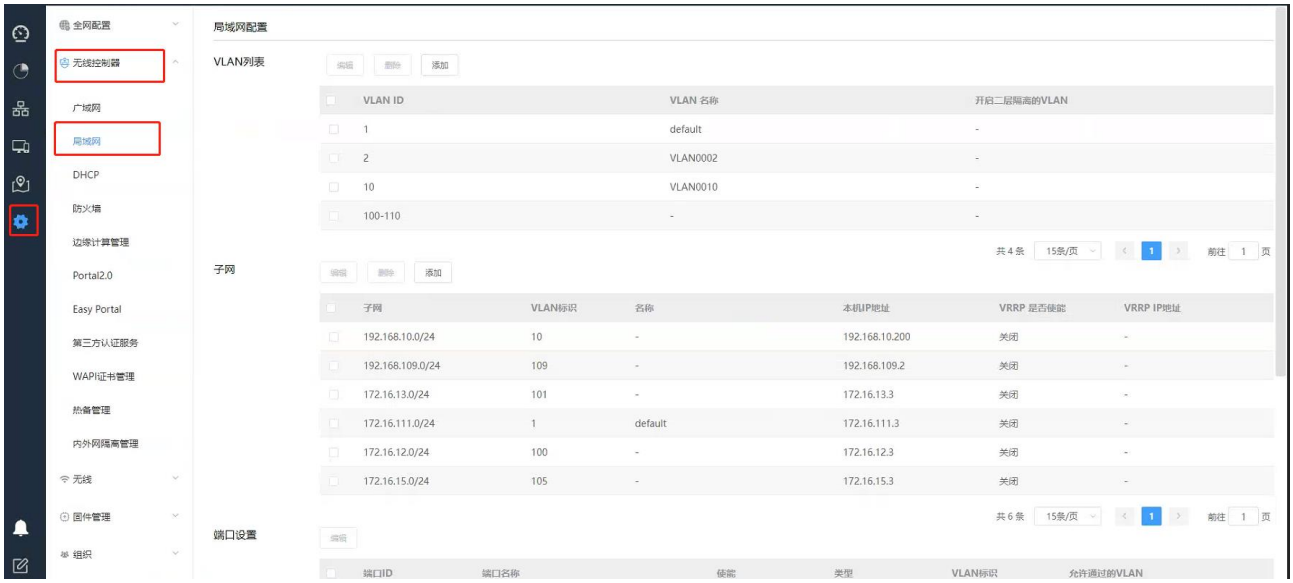
在 SwitchB 上配置 Interface Vlan 101 接口为 STA 提供 IP 地址。

```
SwtchB# enable
SwtchB# configure terminal
SwtchB(config)# dhcp server
SwtchB(config)# interface vlan 101
SwtchB(config)# ip address 10.23.101.254/24
SwtchB(config-if)# dhcp server enable
SwtchB(config-if)# dhcp excluded-address 10.23.101.251 10.23.101.254
SwtchB(config)# dhcp pool yewu_101
SwtchB(dhcp-config)# network 10.23.101.0/24
SwtchB(dhcp-config)# dns-server 114.114.114.114
SwtchB(dhcp-config)# gateway 10.23.101.254
SwtchB(dhcp-config)# lease 1 0 0
SwtchB(config-if)# quit
```

5.1.6.3 配置 AC 局域网

1. 进入 AC 局域网配置页面。

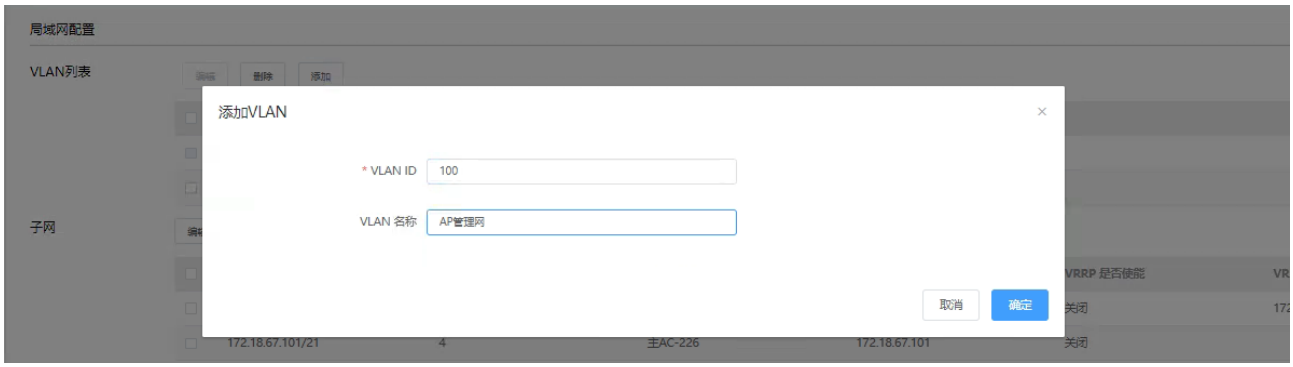
登录 AC Web 系统，单击菜单【设置】>子菜单【无线控制器】>子菜单【局域网】，进入“局域网”页面。



2. 配置网络互联。

a. 首先配置 AP 管理平面接口地址。

在“VLAN 列表”，单击选择<添加>按钮，添加 AP 管理平面的 VLAN 100 及业务 VLAN 101

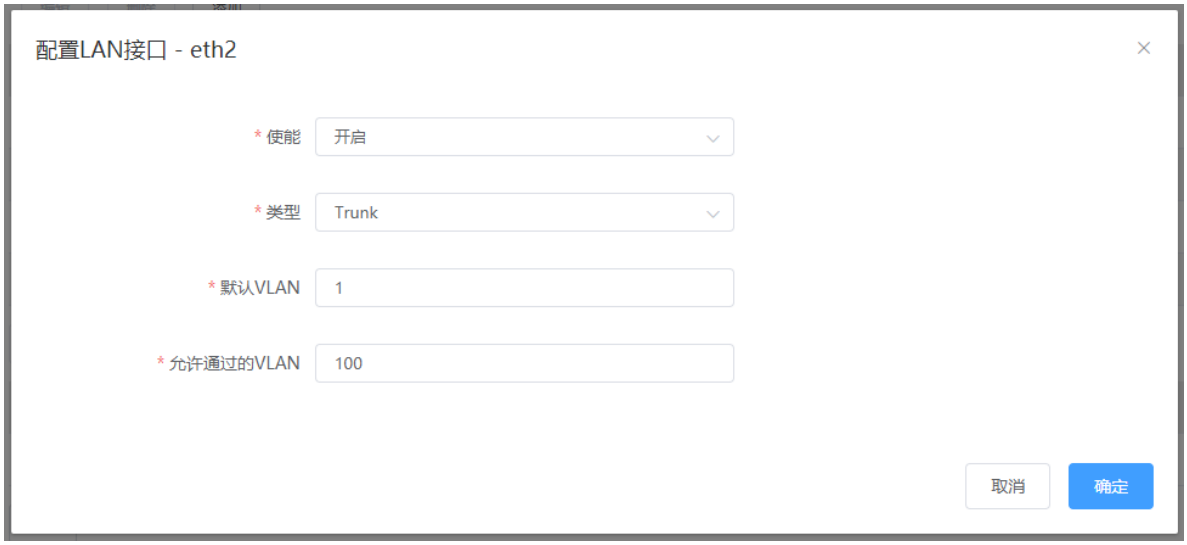


在“子网”中，单击选择<添加>按钮，创建 AP 管理平面的配置虚拟接口 Interface VLAN 100 接口地址 10.23.100.254。

单击<确定>按钮，AP 管理平面接口地址配置完成。

b. 配置 VLAN 及端口

选择旁挂核心交换机的连接端口“eth2”，单击<编辑>按钮，选择“接口类型”为“Trunk”，将“eth2”加入 VLAN100（管理 VLAN）。（如果 AC 直接连接 AP（AP 单独供电或 POE 模块供电时），需要在 AC 直连 AP 的接口上配置缺省 VLAN 为管理 VLAN100）

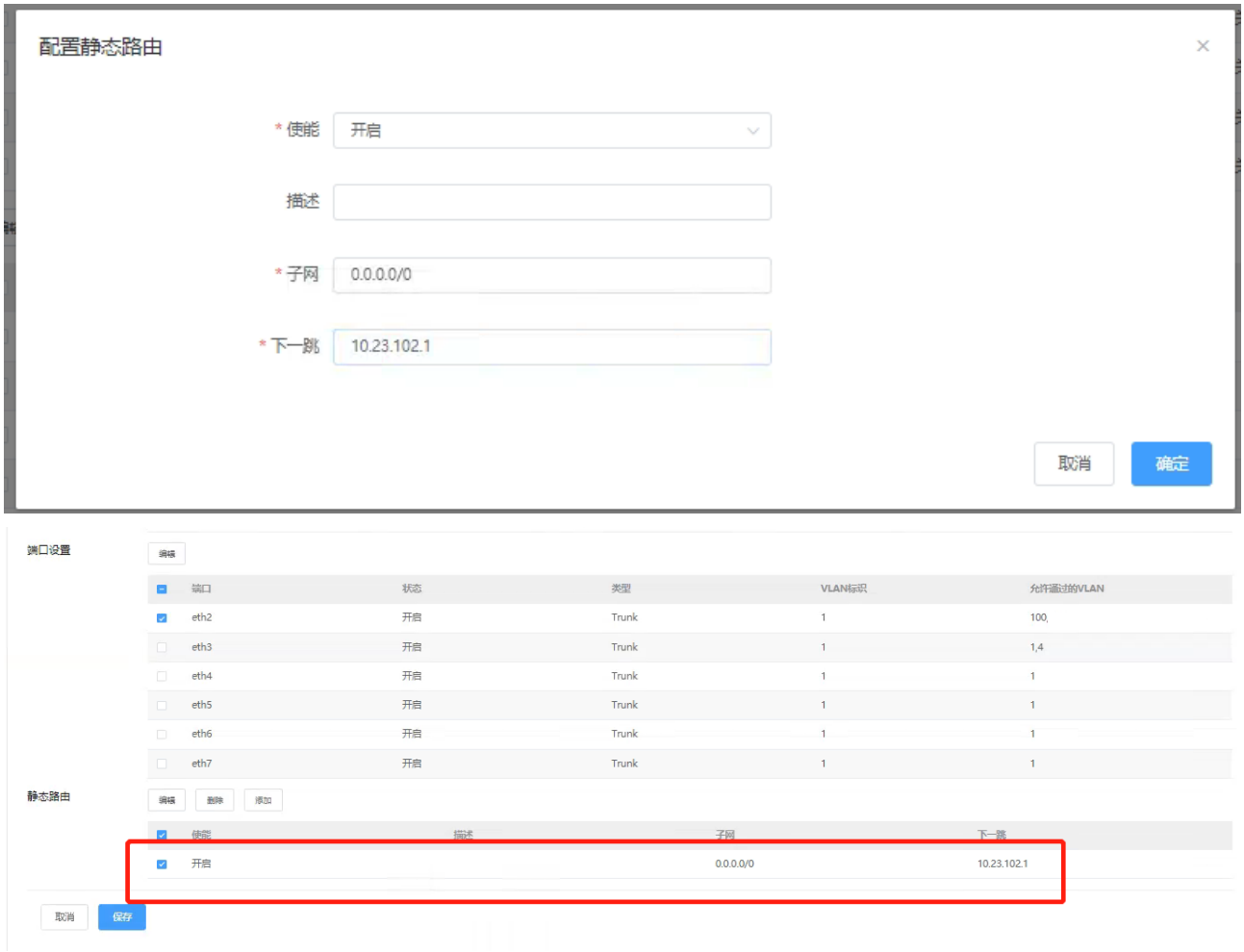


单击<确定>，完成配置。

c. 配置静态路由。

继续在【局域网】菜单下划鼠标，单击“静态路由”下的<添加>按钮，进入“添加静态路由表”页面。

配置“子网”为“10.0.0.0/0”，“下一跳”为“10.23.102.1”。



单击“确定”，完成静态路由表的配置。

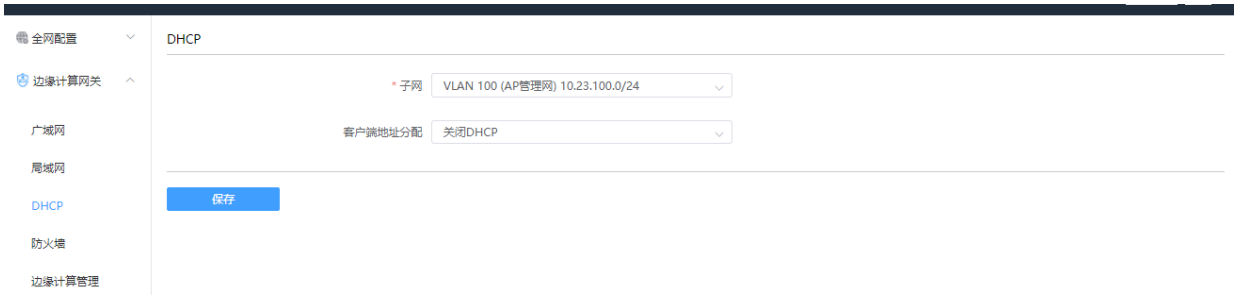
#【局域网】下的所有配置生效需单击页面最下方的<保存>按钮来完。（**重要提醒!!!**）

3. 配置 AP 在 AC 上线

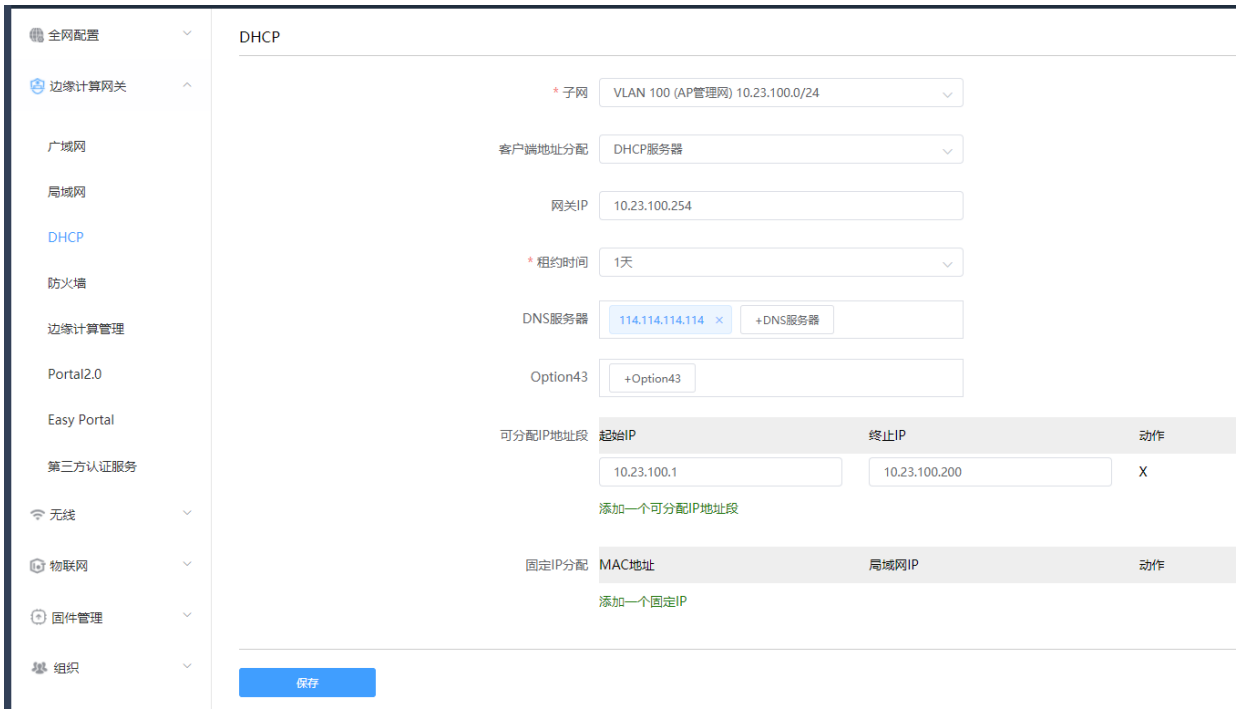
a.配置 AP 管理网 DHCP 服务：

单击菜单【设置】>子菜单【无线控制器】>子菜单【DHCP】，进入 DHCP 服务配置页面。

选择子网 VLAN 100（AP 管理网）10.23.100.0/24。



开启 DHCP 服务器，在“客户端地址分配”选项框选择“DHCP 服务器”。



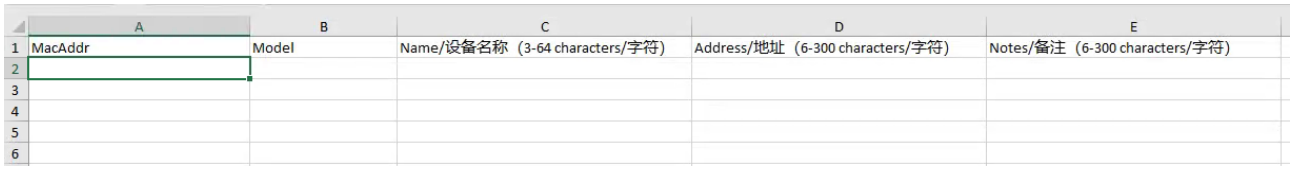
配置 DHCP 服务器各项参数，填写“网关 IP”“租约”、“DNS 服务器”“可分配 IP 地址段”等参数，点击<保存>按扭完成配置。

b. 手动添加 AP：

单击菜单【设置】>子菜单【全网配置】>子菜单【添加设备】，进入 AP 设备添加界面。

通过<添加设备>按钮、或<下载模板>按钮 + <批量导入设备至当前网络>按钮，可进行单个或批量添加 AP 到 AC。

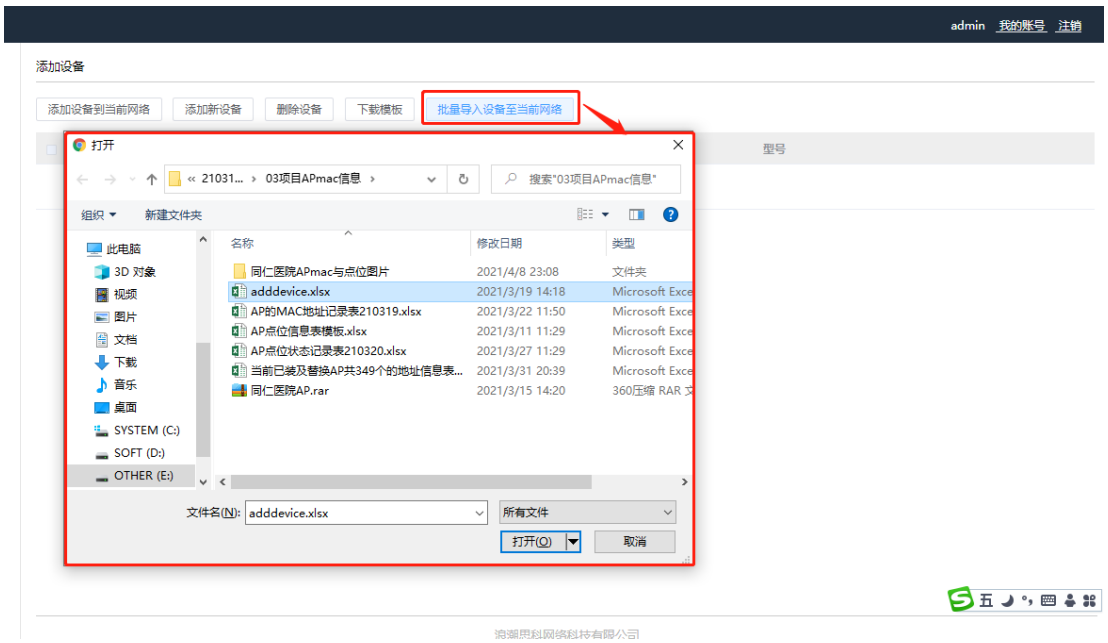
在 AP 模板文件中填写 AP 信息，示例如下“MACAddr：C0:A6:6D:02:5A:40”，“Model：5920i”，设备类型根据实际进行选择。



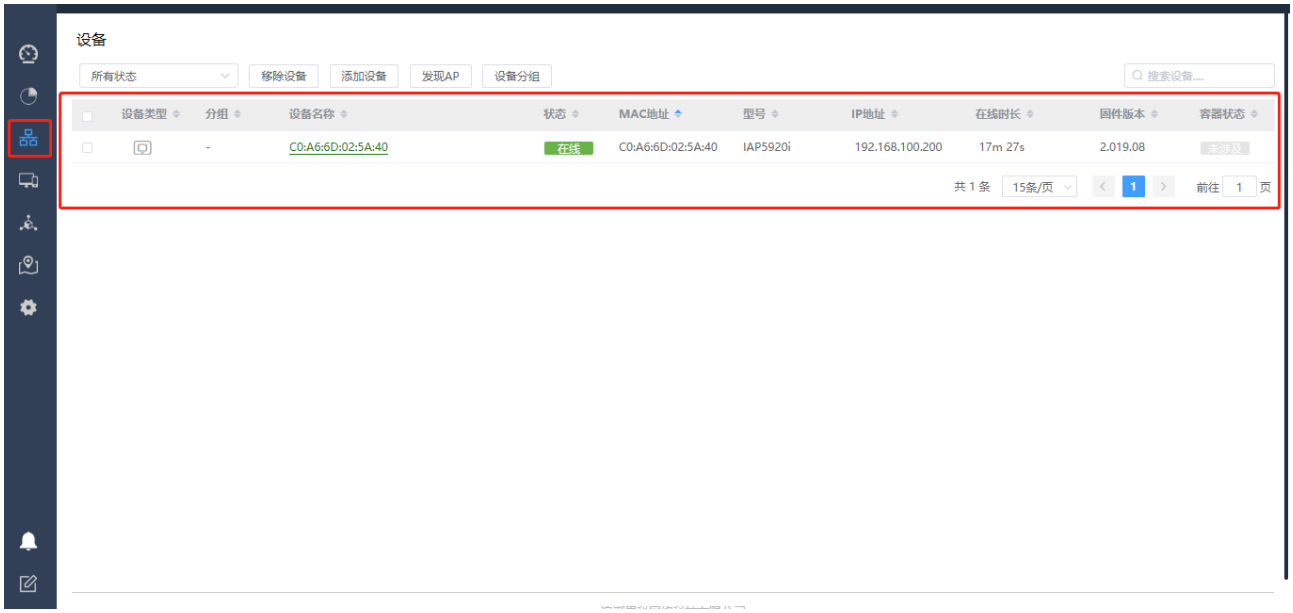
	A	B	C	D	E
1	MacAddr	Model	Name/设备名称（3-64 characters/字符）	Address/地址（6-300 characters/字符）	Notes/备注（6-300 characters/字符）
2					
3					
4					
5					
6					

如需添加多个 AP，可以参照以上表格及示例在 AP 模板文件中填写多条 AP 信息。

单击<批量导入设备至当前网络>按钮，选择填写后的模板文件，单击“打开”。



导入完成后，单击菜单【设备】，可查看添加的全部 AP 列表。

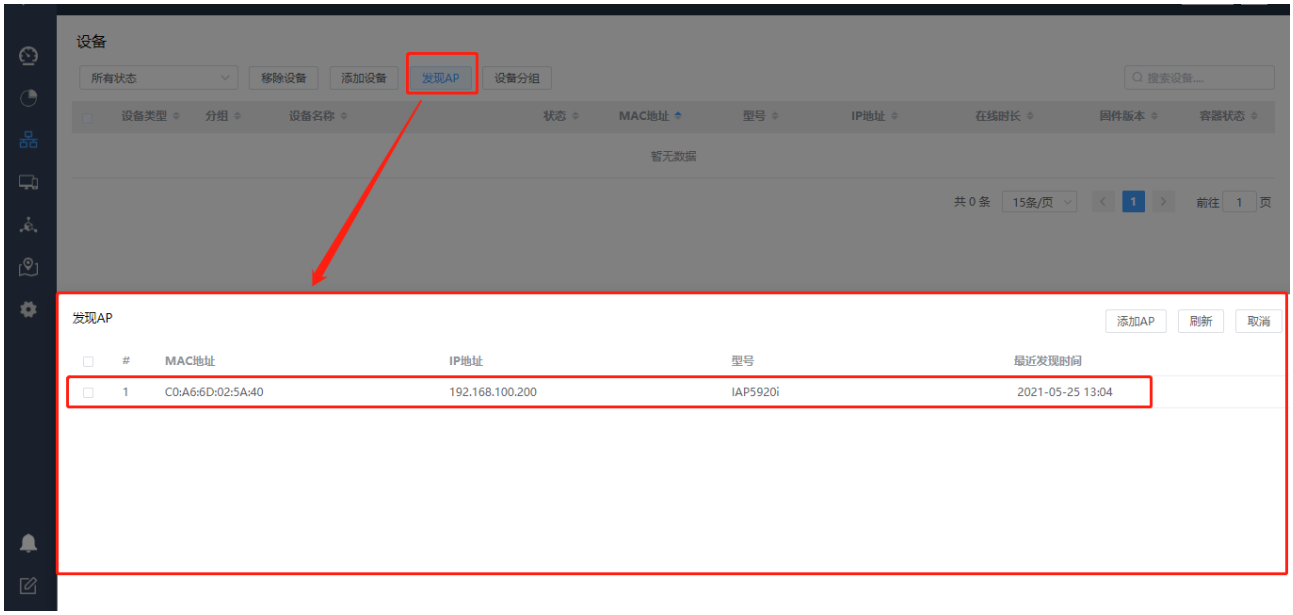


网络无异常情况下，几分钟后，AP 将依次上线。

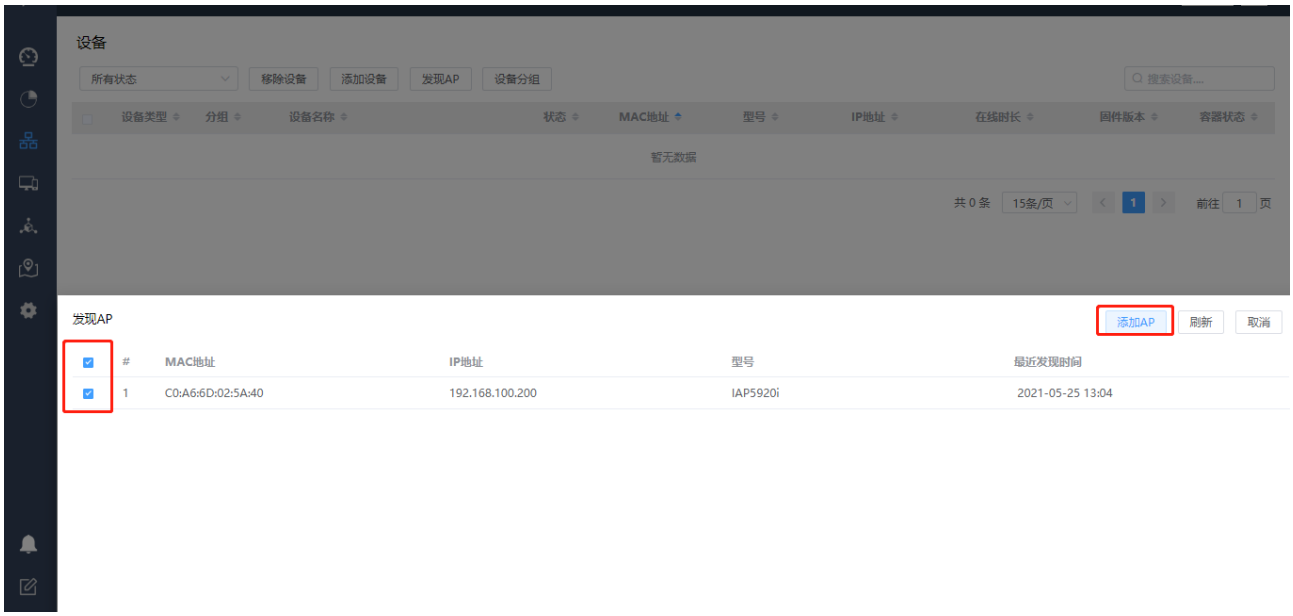
c. 自动添加 AP：

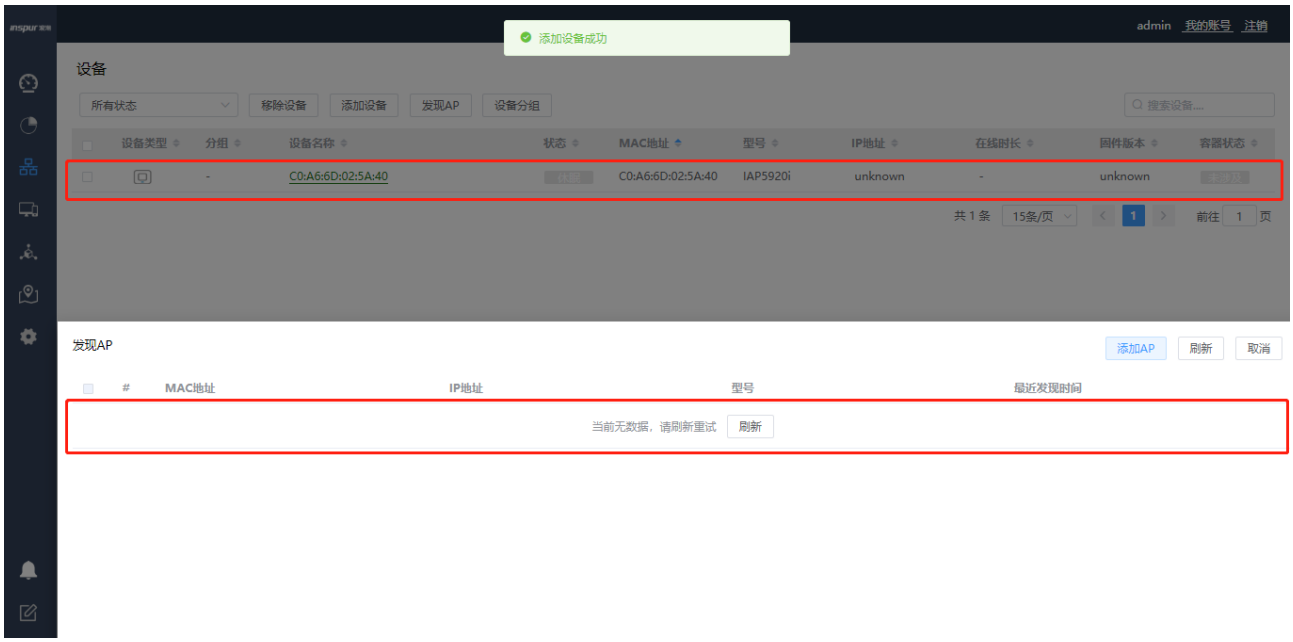
单击菜单【设备】，单击<发现 AP>按钮，可进入自动发现 AP 设备界面。

在 AP 与 AC 网络连通后，AP 自动获取到 AP 管理网 IP，单击<发现 AP>按钮，可立即发现在线的 AP 设备。



选定发现的 AP，单击<添加>按钮，将 AP 设备添加至 AP 设备列表，刷新 Web 页面，AP 状态变动为在线状态，自动添加 AP 成功。





5.1.6.4 配置 WLAN 业务

单击菜单【设置】>子菜单【无线】>子菜单【无线服务】，进入 WLAN 业务配置页面。

系统默认提供 15 个 SSID 模板，可任意选择一个进行修改，也可自行创建新模板；

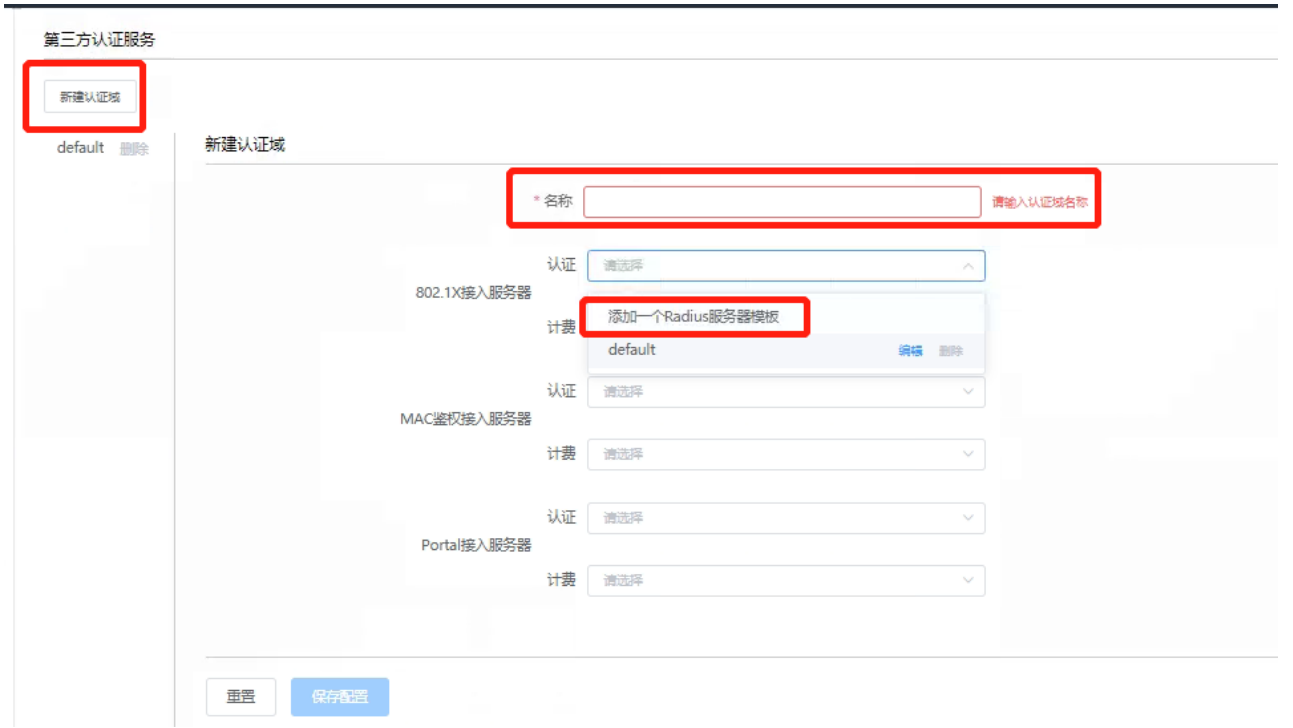
单击任意 SSID 可进入配置 SSID 名称、开关 SSID、是否隐藏、接入控制（开放、预共享密钥、MAC 认证、无感知认证、企业级 WPA2 等）、寻址和流量策略（转发模式、业务 VLAN ID、用户逃生）、防火墙策略、QoS、快速漫游、组播优化、定期关断、在 AP 上绑定等功能。

配置第三方认证服务器认证域

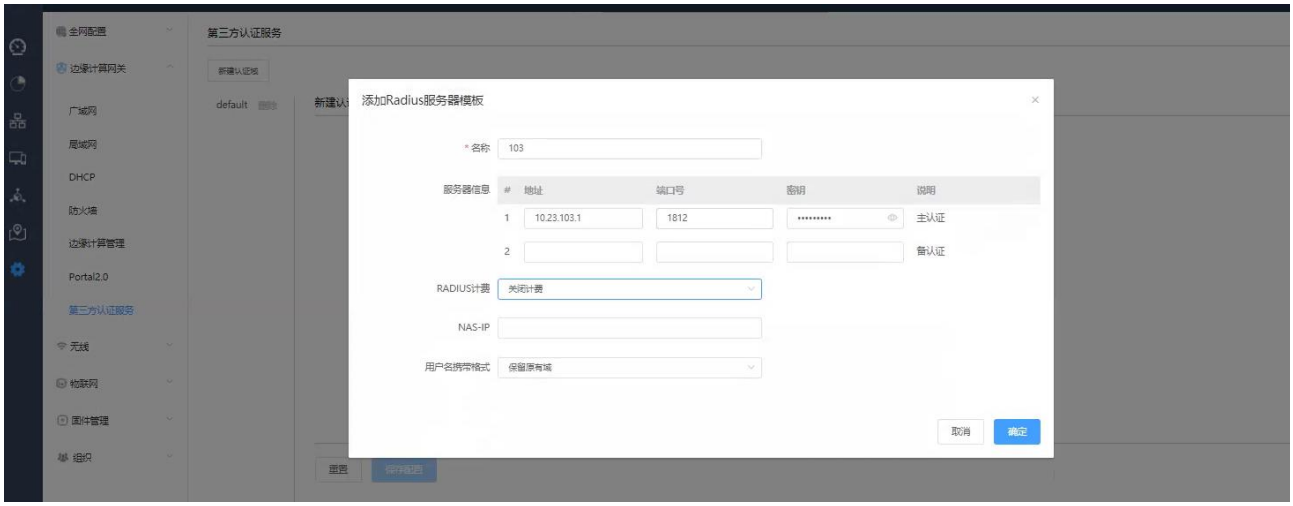
位置：【设置】>【无线控制器】>【第三方认证服务器】配置第三方认证服务器的认证域。

本例配置 1x 认证的认证域设置如下：

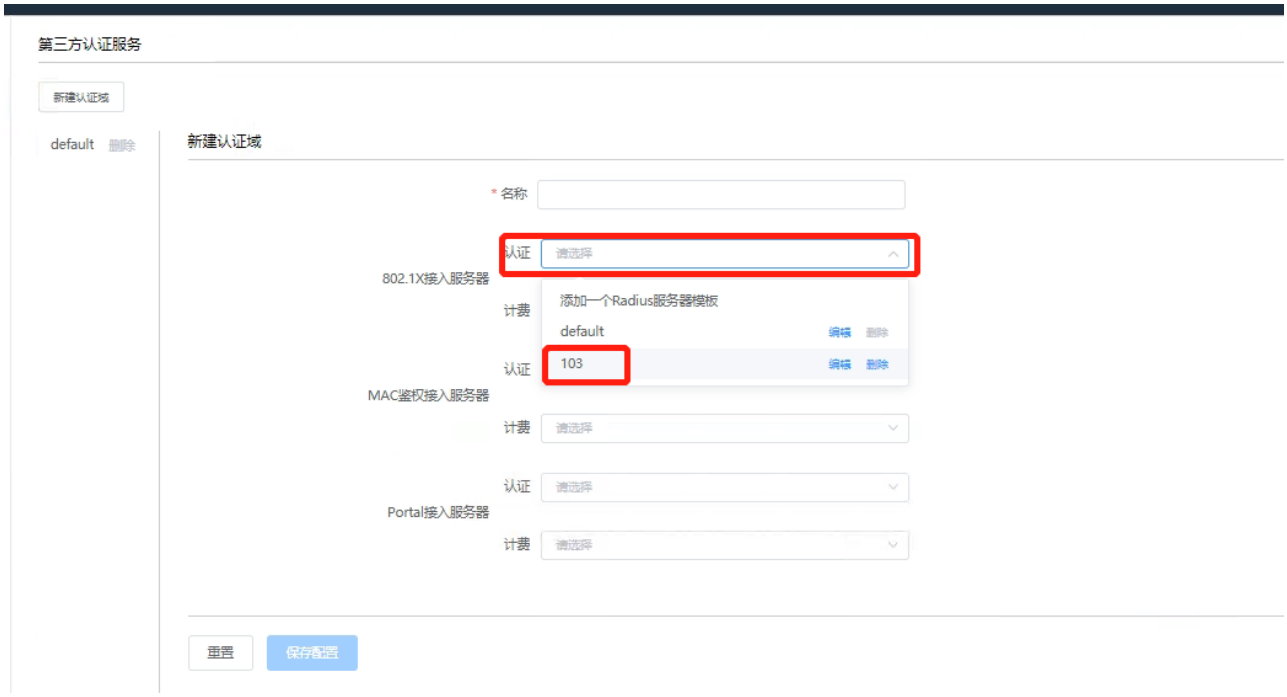
点击<新建认证域>，输入认证域“名称”，在 802.1X 接入服务器栏选择“添加一个 Radius 服务器模板”



输入认证服务器的地址、端口号和密钥，点击<确定>



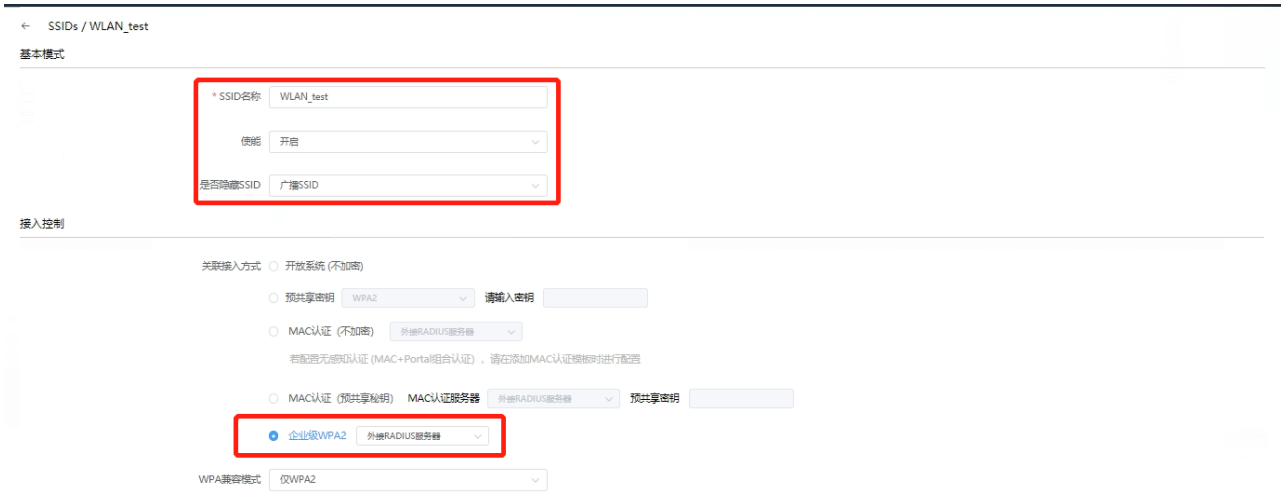
选择刚才创建的 Radius 服务器模版并保存配置，完成第三方服务器认证域配置。



创建 SSID

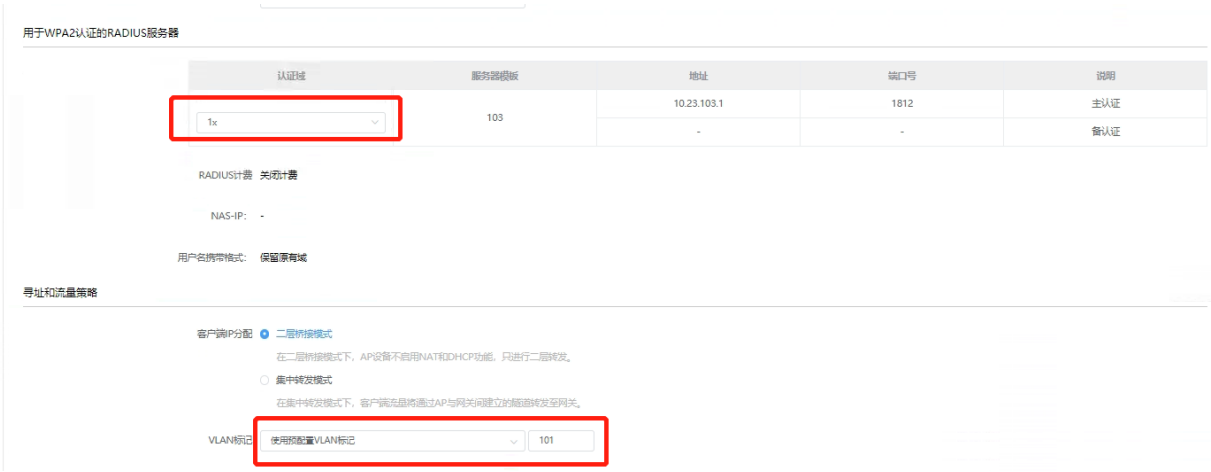
【设置】>【无线】>【无线服务】选择 SSID 模版进入编辑模式

输入 SSID 名称，开启使能，广播 SSID，关联接入方式选择 “企业级 WPA2（外置 RADIUS 服务器）”

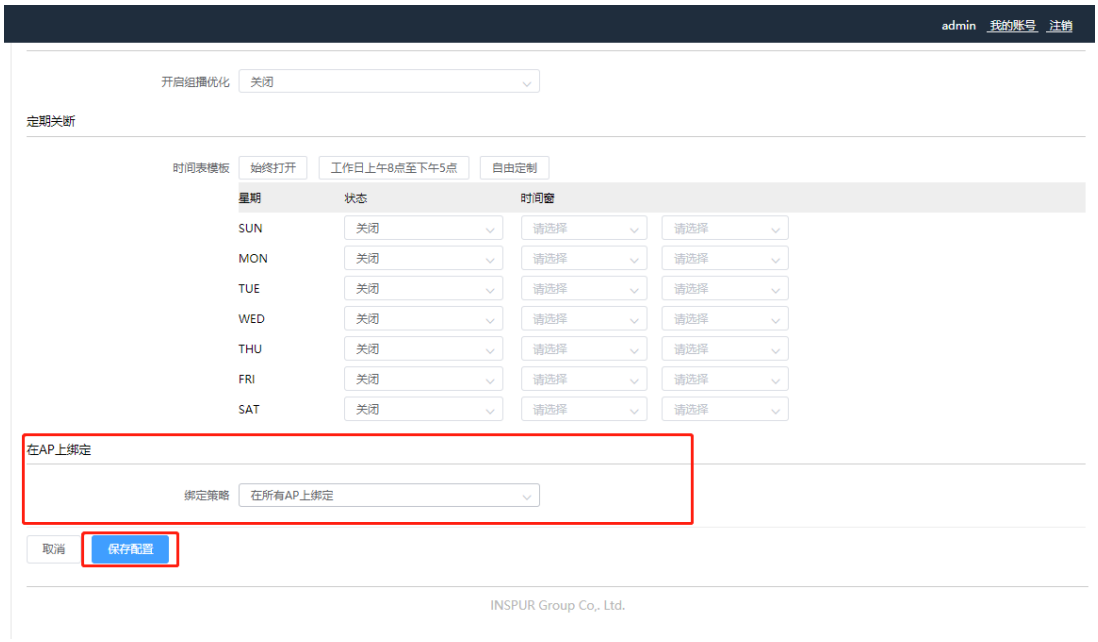


在“用于 WPA2 认证的 RADIUS 服务器”框选择刚才创建的认证域

#设置业务数据转发模式及业务网 VLAN，如下所示：



通过滑动鼠标配置好的策略应用至相应的 AP，如下所示：

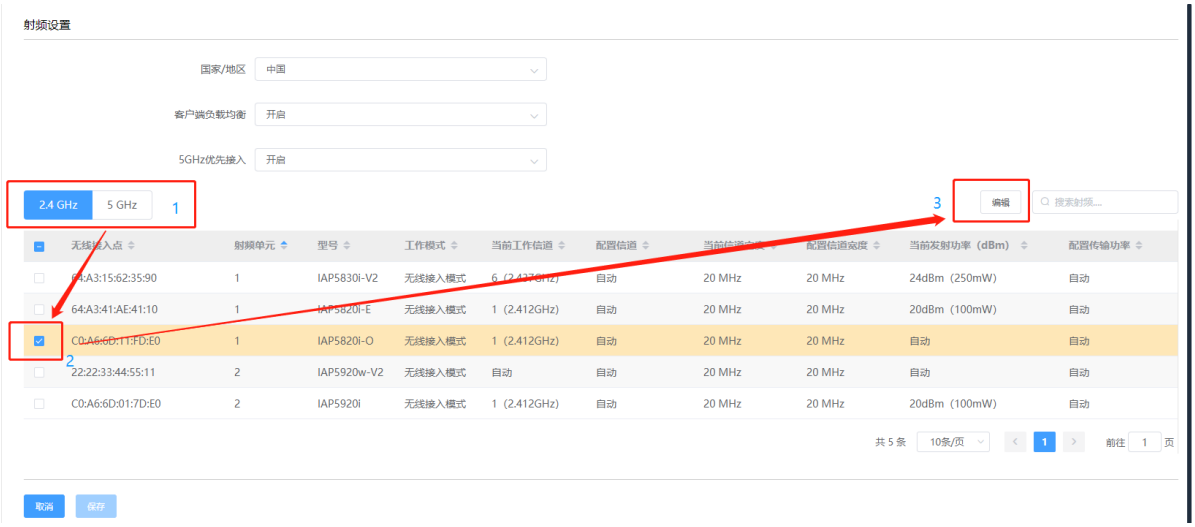


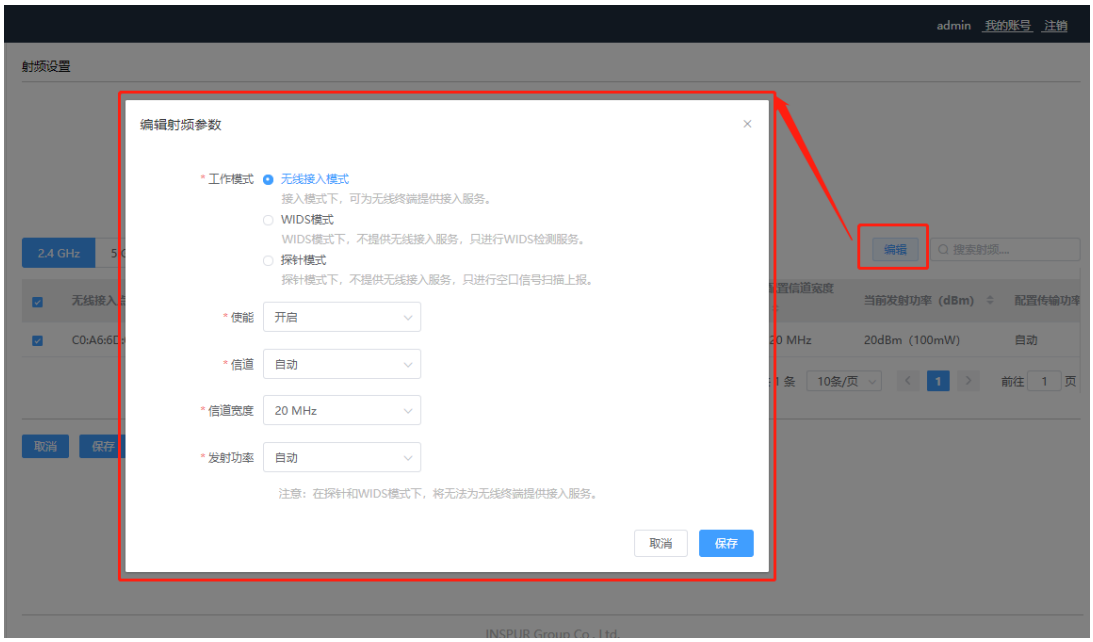
单击<保存配置>完成 WLAN 业务网络的配置。

配置 AP 的信道和功率

单击菜单【设置】>子菜单【无线】>子菜单【射频设置】，进入 AP 的信道和功率配置页面。

单击“射频设置”中<2.4G>或<5G>射频的选项按钮，选定需要进行编辑的 AP，点击右上方的<编辑>按钮，进入 AP 的信道、功率、频率宽度等参数的配置页面。





AP 信道的设定需根据整体周围信道情况进行统一考虑， 2.4G 中有 1、6、11 三个信道相互之间是不重叠的，5G 频段相邻信道之间不重叠；

配置第三方服务器

具体配置方法建议参考相应的产品手册。

检查配置结果

完成配置后，用户可通过无线终端搜索到 SSID 为 **WLAN_test** 的无线网络。

用户关联到无线网络上后，无线 PC 能够被分配相应的 IP 地址。

在 STA 上使用 802.1X 客户端进行认证，输入正确的用户名和密码后，STA 认证成功，正常访问 WLAN 网络。需要根据设置的认证方式 **PEAP** 对客户端进行相应的配置。

Windows xp 系统下的配置

a) 首先在无线网络属性中，添加 SSID 为 **WLAN_test**，并选择认证方式为 **WPA2**，加密使用的算法 **AES**。

b) 在“验证”选项卡中，选择 EAP 类型为 **PEAP**，单击“属性”，去掉验证服务器证书选项（此处不验证服务器证书），单击“配置”，去掉自动使用 Windows 登录名和密码选项，然后单击“确定”。

Windows 7 系统下的配置

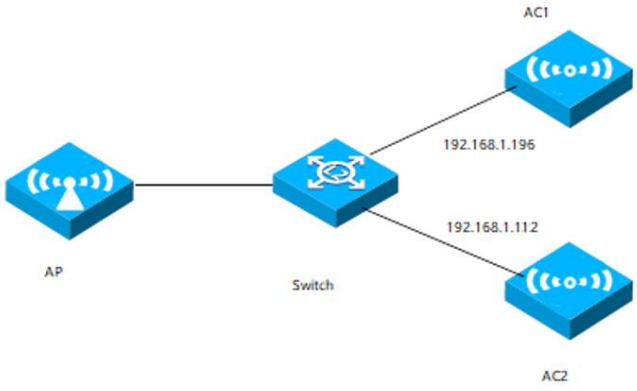
a) 进入管理无线网络页面，单击“添加”，选择手动创建网络配置文件，添加 SSID 为 **WLAN_test**，并选择认证方式为 **WPA2-企业**，加密使用的算法 **AES**，单击“下一步”。

b) 单击“更改连接设置”，进入“无线网络属性”界面，选择“安全”页签，单击“设置”，取消勾选“验证服务器证书”（此处不验证服务器证书），单击“配置”，取消勾选“自动使用 Windows 登录名和密码”，单击“确定”。

c) 单击“确定”，返回“无线网络属性”界面，单击“高级设置”，在“高级设置”界面，勾选“指定身份验证模式”，并选择身份验证模式为“用户身份验证”，单击“确定”。

5.2 AC 主备模式配置

5.2.1 网络拓扑示意



5.2.2 组网规划

配置项	规划数据
管理 VLAN	VLAN10
主 AC 管理 ip	192.168.1.196
备 AC 管理 ip	192.168.1.112
VRRP IP	192.168.1.100

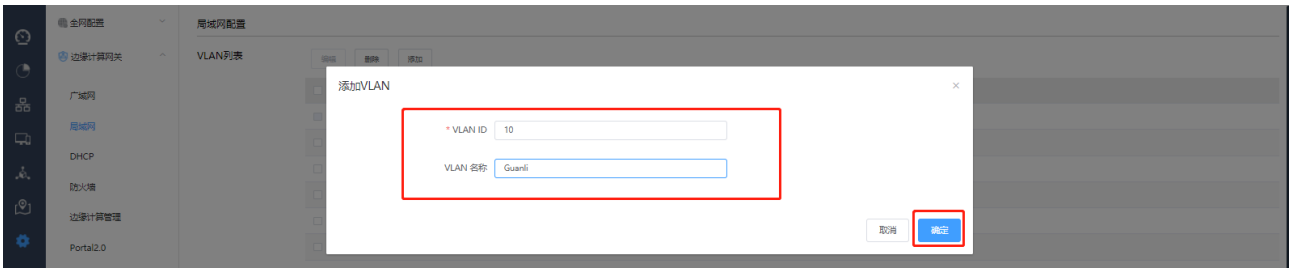
5.2.3 操作步骤

1) 如拓扑图所示，AC1 和 AC2 都在 vlan10 内， AC1 的 vlan10 的三层接口地址是 192.168.1.196，AC2 的三层接口地址是 192.168.1.112。

AC1 上的配置

【设置】>【无线控制器】>【局域网】，进入局域网配置页面。

在【VLAN 列表】点击<添加>，添加 VLAN10



在【子网】点击<添加>配置子网设置如下：

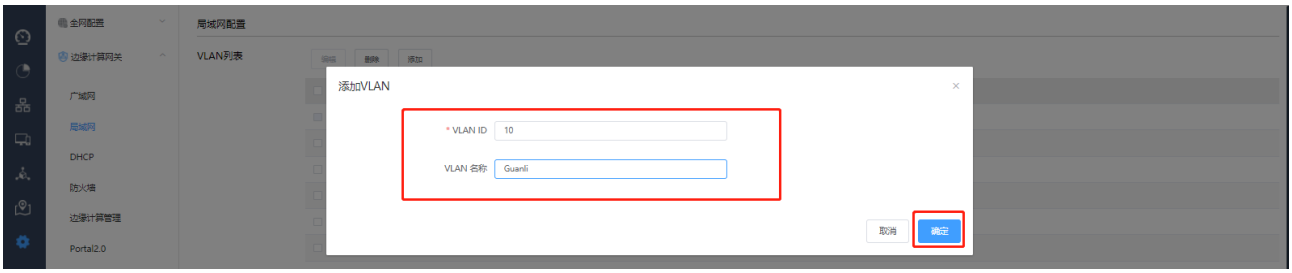
在【端口设置】将 VLAN10 加入端口

【设置】>【无线控制器】>【热备管理】，设置备份 AC 配置，备份 AC 的 IP 地址为 AC2 的 IP，设置 VRRP ID 并保存。

AC2 上的配置

【设置】>【无线控制器】>【局域网】，进入局域网配置页面。

在【VLAN 列表】点击<添加>，添加 VLAN10



在【子网】点击<添加>配置子网设置如下：

在【端口设置】将 VLAN10 加入端口

【设置】>【全局配置】>【通用】，设置备份 AC 配置，备份 AC 的 IP 地址为 AC1 的 IP，设置 VRRP ID 并保存。

#在 AC1 上通过 show vrrp 命令查看 vrrp 状态

```
XOS#show vrrp
IPv4 standby Information:
    Run Method    :  Real MAC
Total number of virtual routers : 1
Interface        VRID  state        Run    Adver    Auth    Virtual
                                    Pri    Timer    Type      IP
------------------------------------------------------------------------
vlan1.10         100   Master       100    1000 ms  --      192.168.1.100 (Not IP owner)
```

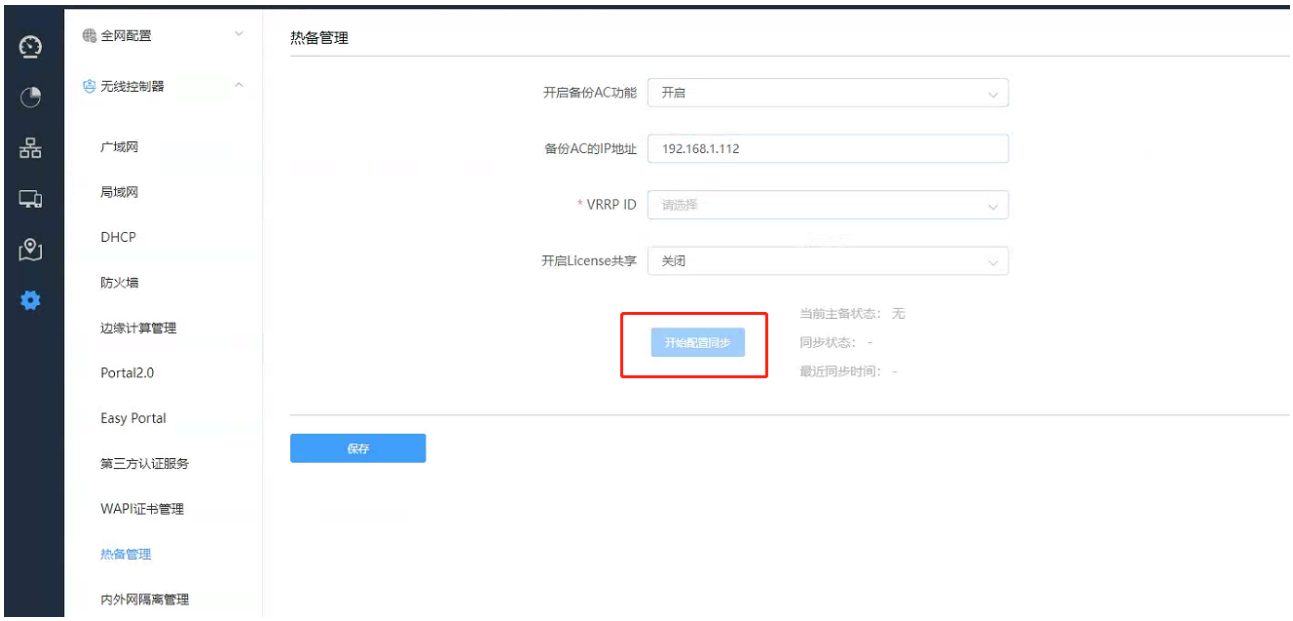
#在 AC2 上通过 show vrrp 命令查看 vrrp 状态

```
XOS#show vrrp
IPv4 standby Information:
    Run Method    :  Real MAC
Total number of virtual routers : 1
Interface        VRID  state        Run    Adver    Auth    Virtual
                                    Pri    Timer    Type      IP
------------------------------------------------------------------------
vlan1.10         100   Backup       100    1000 ms  --      192.168.1.100 (Not IP owner)
```

#可以看到 AC1 协商为 vrrp 的主设备，AC2 协商为 vrrp 的备设备（在优先级相同的情况下，IP 地址大的会协商为主设备）

主备配置同步

【设置】>【无线控制器】>【热备管理】>点击<开始配置同步>将主 AC 配置同步到备 AC 上，同步状态会显示为配置同步完成。AC 主备模式配置完成



验证结果

配置完成后，分别在主备 AC 上查看 vrrp 信息和 ap 信息，应该看到 vrrp 状态和 ap 的状态一致。

#在 AC1 命令行查看

```
XOS#show wlan ap all
NA:Never Assoc NI:No Ip I:Idle  J:Join  ID:Image Download  C:Config
DC:Data Check  R:Running  RS:Reset  M:Master  S:Slave
Running/Total APs                    :1/1
ID   Name                MAC         IP              Model     Time      State
------------------------------------------------------------------------------
1    C0A66D018200   c0a6.6d01.8200 192.168.1.118   iap5920i    0h8m21s     R/M
XOS#show vrrp detail
IPv4 standby Information:
    Run Method    :  Real MAC
Total number of virtual routers : 1
  Interface vlan1.10
    VRID          : 100               Adver Timer   :  1000 msec
    Admin Status  : UP                State         :  Master
    Config Pri    : 100               Running Pri   :  100
    Preempt Mode  : FALSE             Delay Time    :  0 msec
    Auth Type     : --                Key           :  --
    Virtual IP    : 192.168.1.100 (Not IP owner)
    Virtual MAC   : 0000-5e00-0164
    Master IP     : 192.168.1.196
    VRRP Track Information:
```

#在 AC2 命令行查看

```
XOS#show wlan ap all
NA:Never Assoc NI:No Ip I:Idle  J:Join  ID:Image Download  C:Config
DC:Data Check  R:Running  RS:Reset  M:Master  S:Slave
Running/Total APs                    :1/1
```

```
ID    Name                MAC          IP              Model     Time       State
-------------------------------------------------------------------------------
1     C0A66D018200    c0a6.6d01.8200 192.168.1.118   iap5920i     0h11m23s     R/S
XOS#show vrrp detail
IPv4 standby Information:
    Run Method    :  Real MAC
Total number of virtual routers : 1
  Interface vlan1.10
    VRID           : 100                Adver Timer  :  1000 msec
    Admin Status   : UP                 State        :  Backup
    Config Pri     : 100                Running Pri  :  100
    Preempt Mode   : FALSE              Delay Time   :  0 msec
    Auth Type      : --                 Key          :  --
    Virtual IP     : 192.168.1.100 (Not IP owner)
    Virtual MAC    : 0000-5e00-0164
    Master IP      : 192.168.1.112
    VRRP Track Information:
```

在 down 掉 AC1 的链路后，AC2 会成为主 AC，其上的 ap 状态也由 Slave 转变为 Master。

5.3 AC 双链路聚合配置

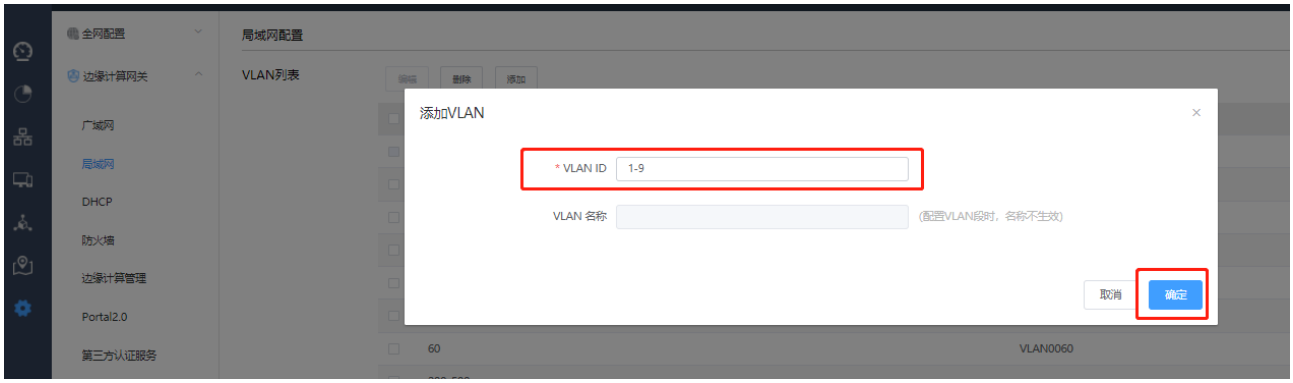
5.3.1 组网需求

将 AC 的 eth4 和 eth5 端口加入聚合组 1 ，配置 trunk vlan 1-9

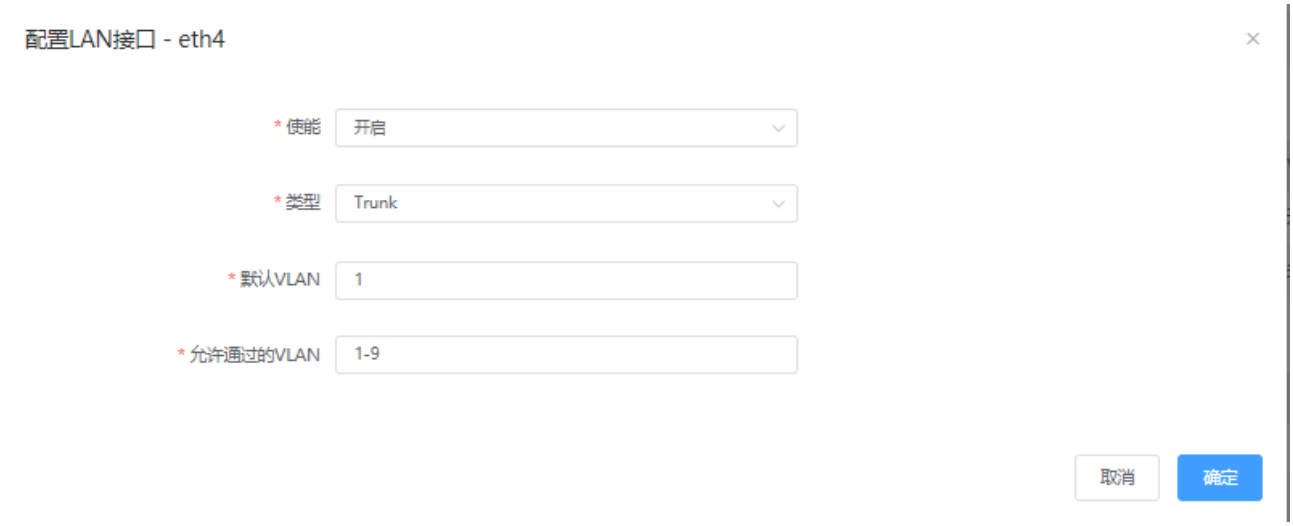
5.3.2 操作步骤

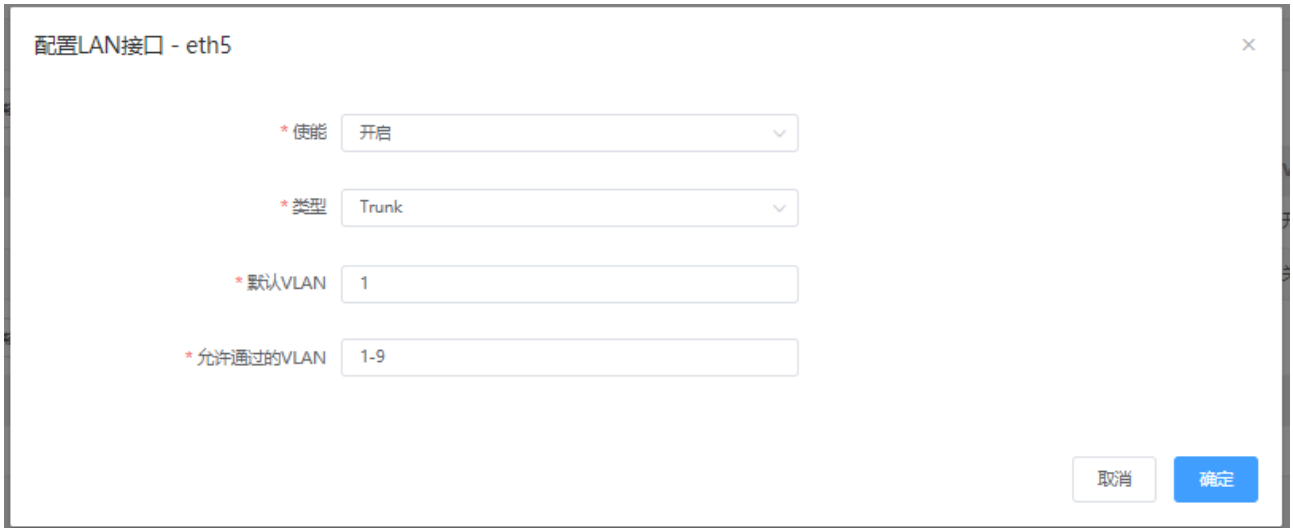
【设置】>【无线控制器】>【局域网】，进入局域网配置页面。

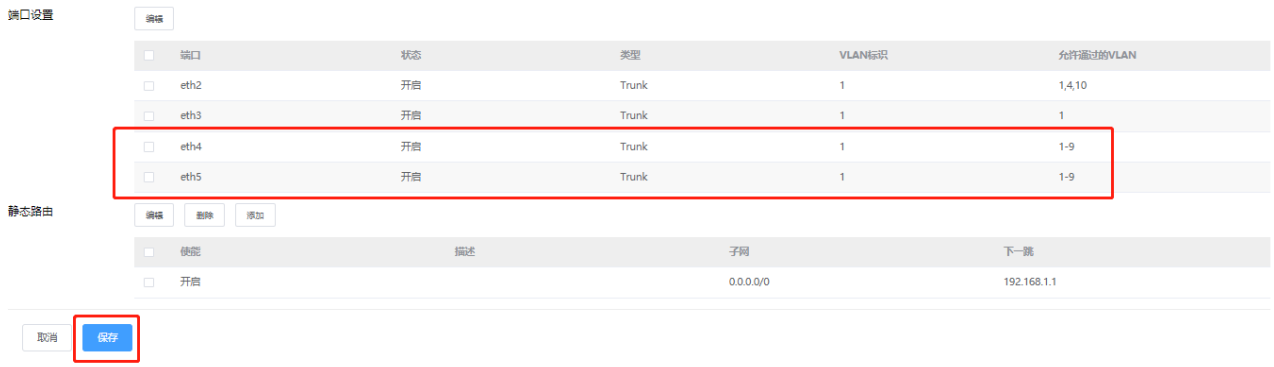
在【VLAN 列表】点击<添加>，添加 VLAN1-9，点击<确定>



在【端口设置】将 VLAN1-9 加入 eth4 和 eth5 端口并保存







登录 AC 命令行，将 eth4 和 eth5 加入到静态聚合组 1：

```
XOS(config)#interface eth4
XOS(config-if)#static-channel-group 1
XOS(config-if)#quit
XOS(config)#interface eth5
XOS(config-if)#static-channel-group 1
XOS(config-if)#quit
```

注意事项：配置前需保持加入聚合组的端口状态一致，否侧后配置的端口会提示无法加入。

show static-channel-group 可查看当前聚合组信息如下：

```
XOS(config)#show static-channel-group
```

```
% Static Aggregator: sa1
% Member:              Status:
   eth4                 INACTIVE
   eth5                 INACTIVE
```

配置聚合接口根据源 ip 和目的 ip 进行负载分担：

```
XOS(config)#interface sa1

XOS(config-if)#port-channel load-balance src-dst-ip  //缺省的负载分担模式是基于源 MAC 和目

的 MAC
```

检验结果

查看 AC 上聚合组的信息

```
XOS# show static-channel-group
% Static Aggregator: sa1
% Member:              Status:
   eth4                 ACTIVE
   eth5                 ACTIVE
```

查看接口状态

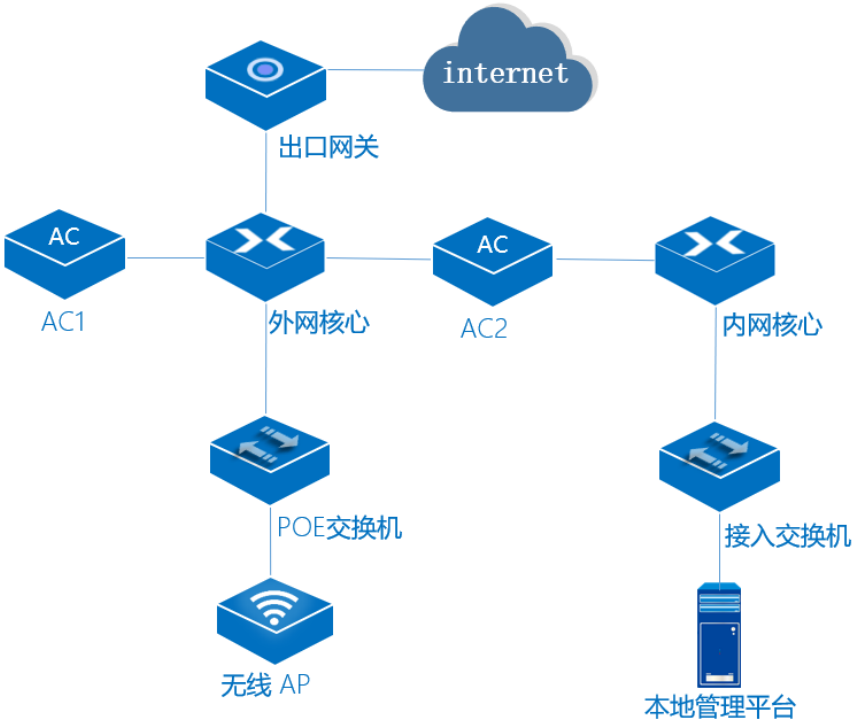
```
XOS#show interface brief
The brief information of interface(s) under bridge mode:
Status: ADM - administratively down
Duplex: A - auto;H - half;F - full
Type:A - access;T - trunk;H - hybrid
Interface             Status Speed  Duplex Type PVID Description
eth0                  DOWN   1g     F      A    4093
eth1                  DOWN   1g     F      A    4094
eth2                  DOWN   1g     F      T    1
eth3                  DOWN   1g     F      T    1
eth4                  UP       1g     F      T    1
eth5                  UP       1g     F      T    1
sa1                   UP       2g     F      T    1
```

查看负载分担模式

```
XOS# show etherchannel load-balance
% Lacp Aggregator: sa1
Source and Destination IP address
```

5.4 内外网隔离配置

5.4.1 网络拓扑示意



5.4.2 组网规划

配置项	规划数据
管理 VLAN	VLAN5
外网业务 VLAN	VLAN3
内网业务 VLAN	VLAN20
AC1 的管理地址	VLANIF5：10.110.55.181/24
AC2 的管理地址	VLANIF5：10.110.55.183/24
DHCP 服务器	外网核心作为 DHCP 服务器为 AP 和外网 STA 分配 IP 地址； AC2 作为 DHCP 服务器为内网 STA 分配 IP 地址。
AP 的 IP 地址池	10.110.55.100～10.110.55.200/24
外网 STA 的 IP 地址池	10.110.33.100～10.110.33.200/24
内网 STA 的 IP 地址池	192.168.20.100～192.168.20.200/24

SSID 名称	外网 SSID 名称：test01 内网 SSID 名称：test02
安全策略	安全策略：WPA-WPA2
VAP 模板	外网：转发模式-本地转发，业务 VLAN：VLAN3 内网：转发模式-集中转发，业务 VLAN：VLAN20

5.4.3配置思路

- ✧ 配置 AP、AC 和周边网络设备之间实现网络互通。
- ✧ 配置 AC 局域网
- ✧ 配置 AP 在 AC1 上线
- ✧ AC1 上开启受控 AC 功能
- ✧ AC2 上添加 AP，重启 AP 使 AP 在 AC2 上线
- ✧ 在 AC 上配置 WLAN 相关业务（SSID）

5.4.4操作步骤

5.4.4.1 配置周边设备

配置 POE 交换机

连 AP 的接口为 trunk 模式，透传 VLAN3 和 5，native vlan 5；

连外网核心的接口为 trunk 模式，透传 VLAN3 和 5。

配置接入交换机

接入交换机作为傻瓜交换机使用。

配置外网核心交换机

创建 VLAN5, VLANIF5：10.110.55.1/24，配置 VLANIF5 接口为 AP 提供 IP 地址；

创建 VLAN3，VLANIF3：10.110.33.1/24，配置 VLANIF3 接口为 STA 提供 IP 地址；

连 AC1、AC2 的接口为 trunk 模式，透传 VLAN 5；

连 POE 交换机的接口为 trunk 模式，透传 VLAN3 和 5；

配置下一跳为 Router 的缺省路由。

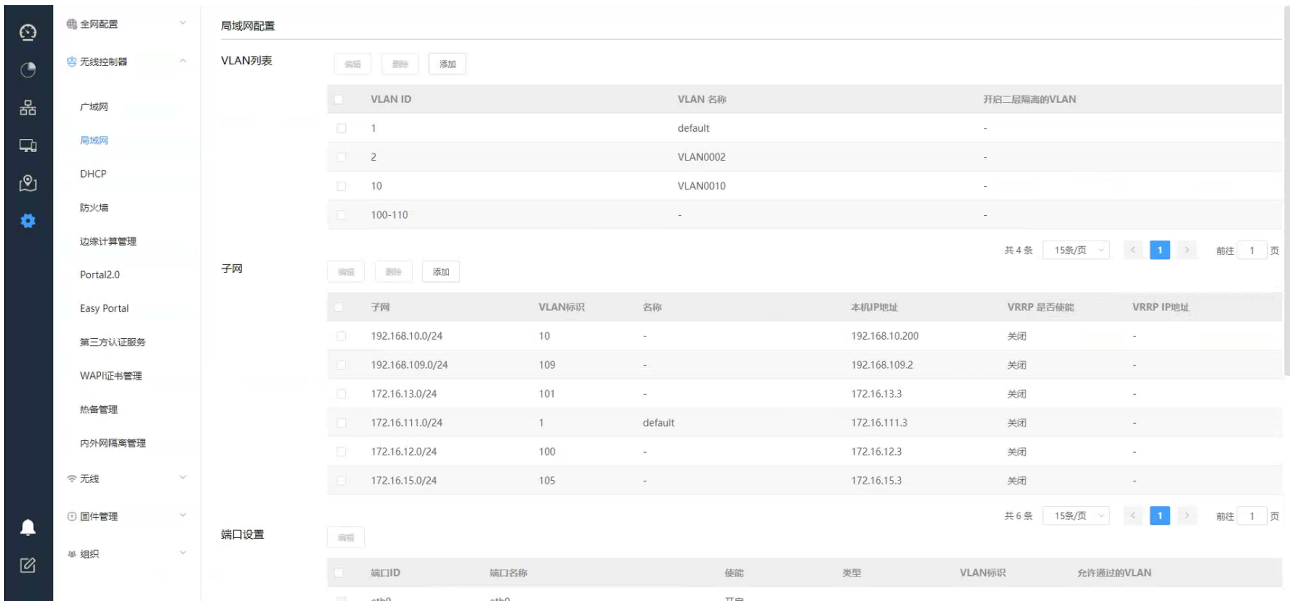
配置内网核心交换机

内网核心交换机作为傻瓜交换机使用。

5.4.4.2 配置 AC1

1. 配置 AC1 局域网

登录 AC1 Web 系统，单击菜单【设置】>子菜单【无线控制器】>子菜单【局域网】，进入“局域网配置”页面。

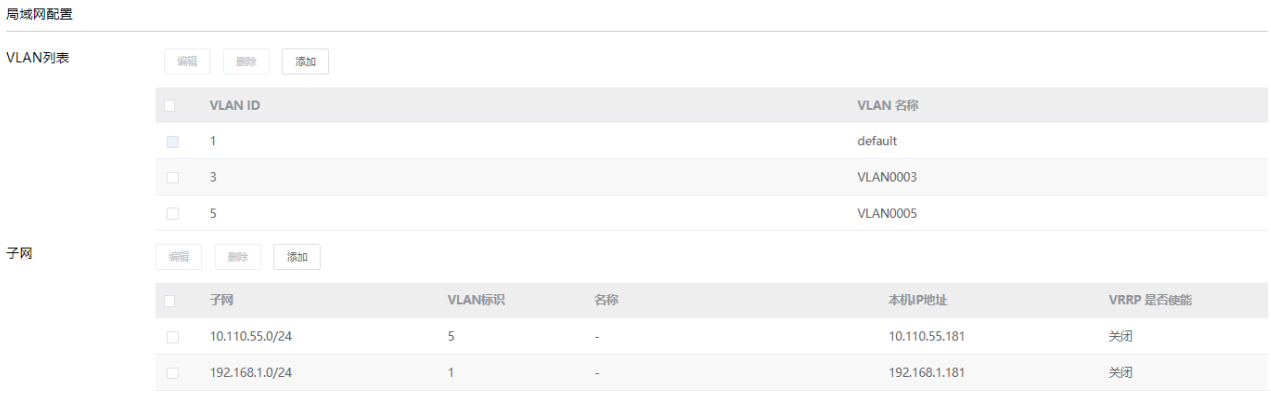


2. 配置网络互联

a. 配置 VLAN 和子网

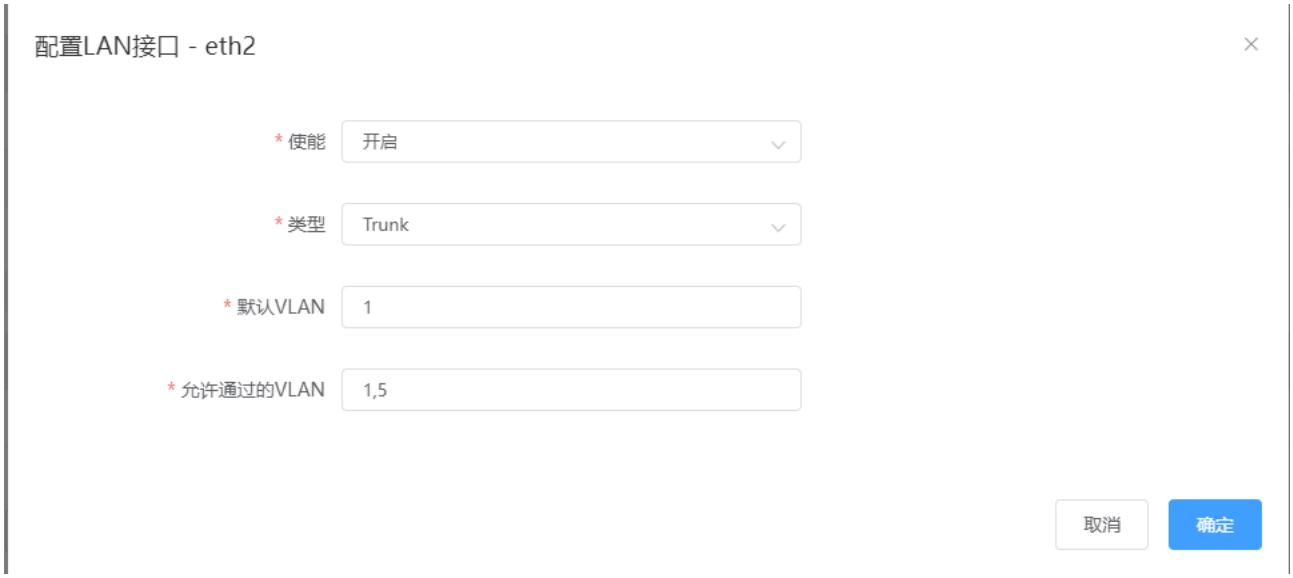
在“VLAN 列表”，单击选择<添加>按钮，添加管理平面的 VLAN 5 及业务 VLAN 3

在“子网”中，设置 vlan5 的子网为 10.110.55.0/24，本机地址为 10.110.55.181，单击<确定>并保存。



b. 配置端口

在“端口设置”中，选择旁挂核心交换机的连接端口“eth2”，单击<编辑>按钮，选择“接口类型”为“Trunk”，在“eth2”中加入管理 VLAN5，单击<确定>并保存，完成配置。



c. 配置静态路由

继续在【局域网】菜单下划鼠标，单击“静态路由”下的<添加>按钮，进入“添加静态路由表”页面。

配置“子网”为“0.0.0.0/0”，“下一跳”为“10.110.55.1”。

3. 添加并上线 AP

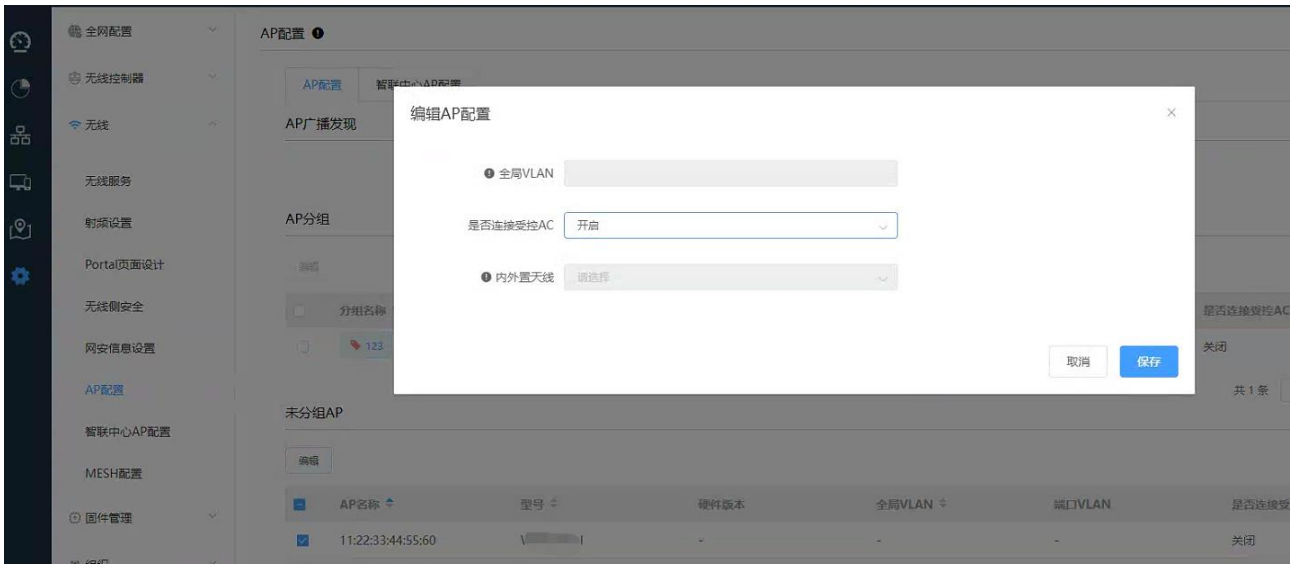
在 AC1 上通过“添加设备”或“模板导入”方式添加 AP 并上线

4. 开启受控 AC 配置

（1）单击菜单【设置】>子菜单【通用】，进入“受控 AC 配置”页面。

开启受控 AC 功能，配置受控 AC 的 IP 地址为 AC2 的地址 10.110.55.183 并保存。

（2）单击菜单【设置】>子菜单【无线】>子菜单【AP 配置】，进入“AP 配置”页面，选择 AP 点击<编辑>按钮，“是否连接受控 AC”选择“开启”，并保存配置。



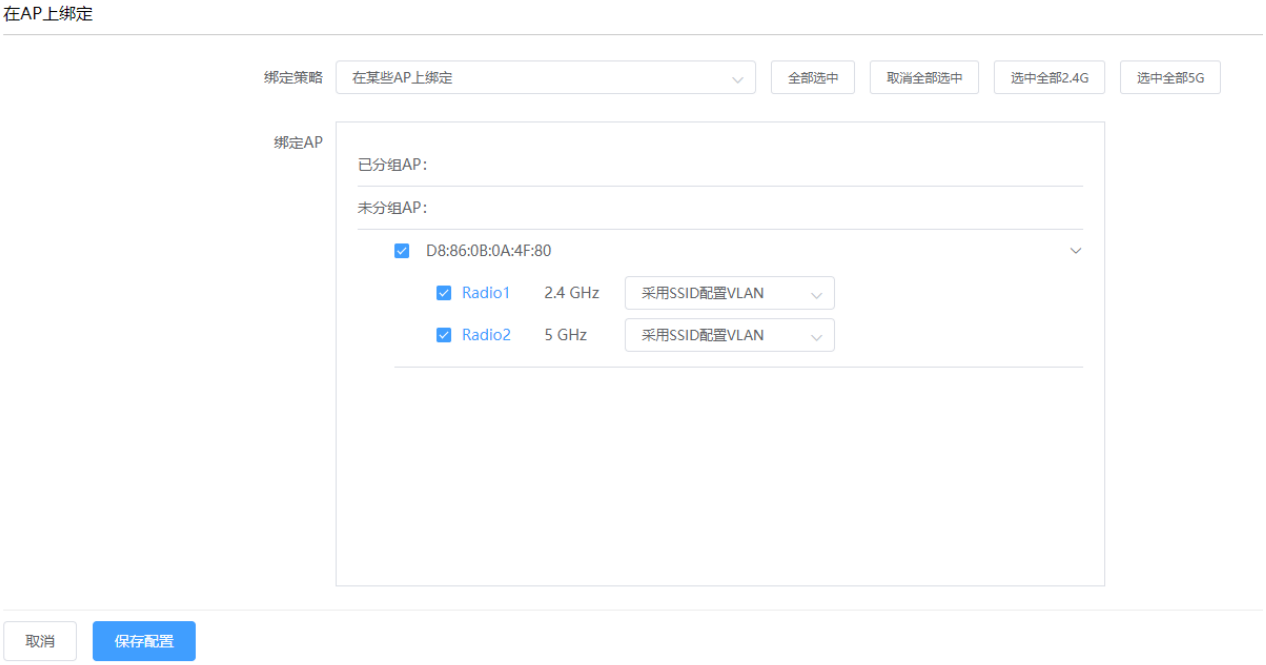
5. 配置 SSID

单击菜单【设置】>子菜单【无线】，进入“SSID”页面，编辑第一个 SSID 模板。

配置 SSID 名称、开启使能、选择预共享密钥方式

“数据转发方式”选择二层桥接模式，“VLAN 标记”选择使用预置 VLAN 标记，配置 VLAN 为 3，“DHCP 转发方式”选择本地转发模式

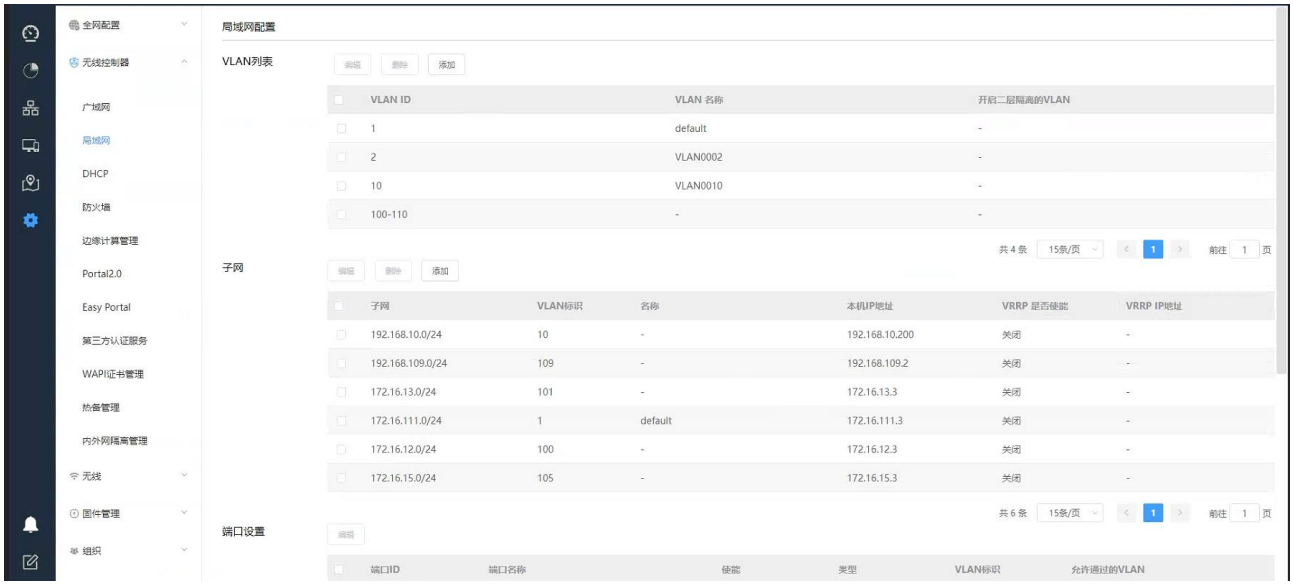
选择要绑定的 AP 点击“保存配置”



5.4.4.3 配置 AC2

1. 配置 AC2 局域网

登录 AC2 Web 系统，单击菜单【设置】>子菜单【无线控制器】>子菜单【局域网】，进入“局域网配置”页面。



2. 配置网络互联

a. 配置 VLAN 和子网。

在“VLAN 列表”，单击选择<添加>按钮，添加管理平面的 VLAN 5 及业务 VLAN 20

在“子网”中，设置 vlan5 的子网为 10.110.55.0/24，本机地址为 10.110.55.183，设置 vlan20 的子网为 192.168.20.0/24，本机地址为 192.168.20.1，单击<确定>并保存。

局域网配置

VLAN列表

编辑 删除 添加

VLAN ID	VLAN 名称
1	default
5	VLAN0005
20	VLAN0020

子网

编辑 删除 添加

子网	VLAN标识	名称	本机IP地址	VRRP 是否使能	VRRP IP地址
10.110.55.0/24	5	-	10.110.55.183	关闭	-
192.168.20.0/24	20	-	192.168.20.1	关闭	-
192.168.1.0/24	1	-	192.168.1.183	关闭	-

b. 配置端口

在“端口设置”中，选择连接外网核心交换机的端口“eth2”，单击<编辑>按钮，选择“接口类型”为“Trunk”，在“eth2”中加入管理 VLAN5；选择连接内网核心交换机的端口“eth3”，单击<编辑>按钮，选择“接口类型”为“Access”，在“eth3”中加入业务 VLAN20，单击<确定>并保存，完成配置。

端口设置

编辑

端口ID	端口名称	使能	类型	VLAN标识	允许通过的VLAN
eth0	eth0	开启	-	-	-
eth1	eth1	开启	-	-	-
eth2	eth2	开启	Trunk	1	1,5
eth3	eth3	开启	Access	20	-

c. 配置静态路由

在【局域网】页面，单击“静态路由”下的<添加>按钮，进入“添加静态路由表”页面。

配置“子网”为“0.0.0.0/0”，“下一跳”为“10.110.55.1”。

d. 配置 vlan20 的 DHCP

DHCP

* 子网 VLAN 20 (192.168.20.0/24) 192.168.20.0/24

客户端地址分配 DHCP服务器

网关IP 192.168.20.1

* 租约时间 4小时

DNS服务器 +DNS服务器

Option43 +Option43

可分配IP地址段

起始IP	终止IP	动作
192.168.20.100	192.168.20.200	X

添加一个可分配IP地址段

固定IP分配

MAC地址	局域网IP	动作

添加一个固定IP

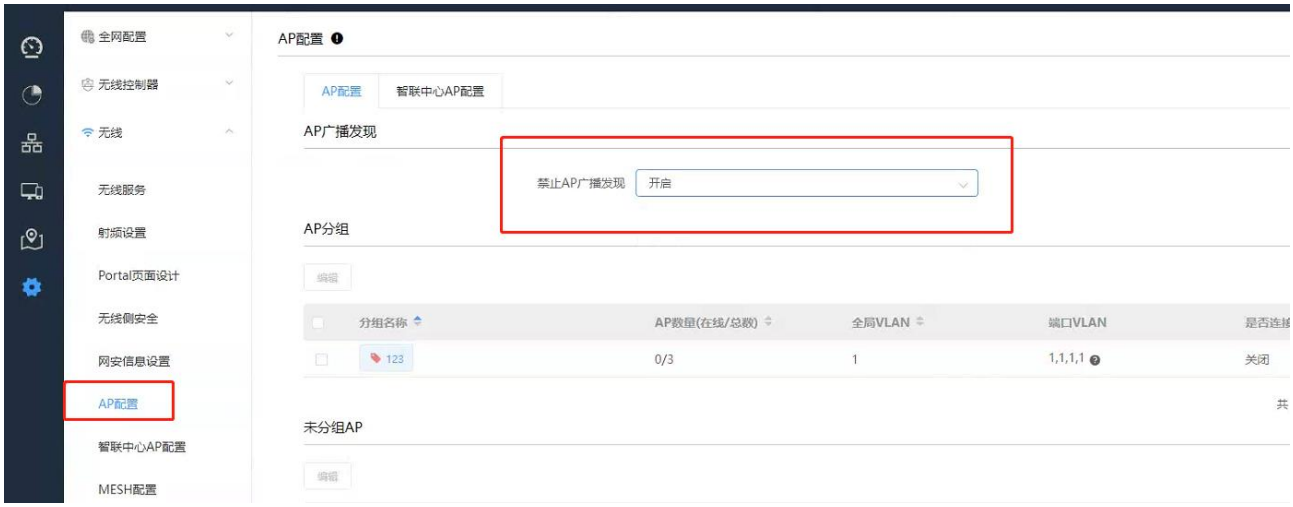
保存

3. 开启受控 AC 的禁止广播发现功能

因为受控 AC 和主控 AC 在一个二层网络内，为防止 AP 广播在受控 AC 上线，需要在受控 AC 上开启“禁止广播接入”

单击菜单【设置】>子菜单【无线】，进入“AP 配置”页面。

将 “禁止广播发现”功能开启并保存。



4. 添加并上线 AP

在 AC2 上通过“添加设备”或“模板导入”方式添加 AP

AP 上线后，在受控 AC 命令还查看 AP 状态为 R/M/V （V 代表 AP 在受控 AC 上线）

```
INOP#show wlan ap all
NA:Never Assoc NI:No Ip I:Idle  J:Join  ID:Image Download  C:Config
DC:Data Check  R:Running  RS:Reset  M:Master  S:Slave V:Virtual
Running/Total APs                    :1/1
ID  Name          MAC             IP             Model         Time       State Description
------------------------------------------------------------------------------------------
1   D8860B0A4F80  d886.0b0a.4f80  10.110.55.79   iap5821i      0h43m14s   R/M/V D8:86:0B:0A:4F:80
```

注意：

（1）如果 AC 和 AP 在同一个二层，需要在受控 AC 上开启禁止广播上线

```
INOP(config)#capwap discovery broadcast forbidden
```

（2）若开启受控 AC 功能之前，AP 已经在主控 AC 上线，则需要重启 AP 后才能在受控 AC 上线。

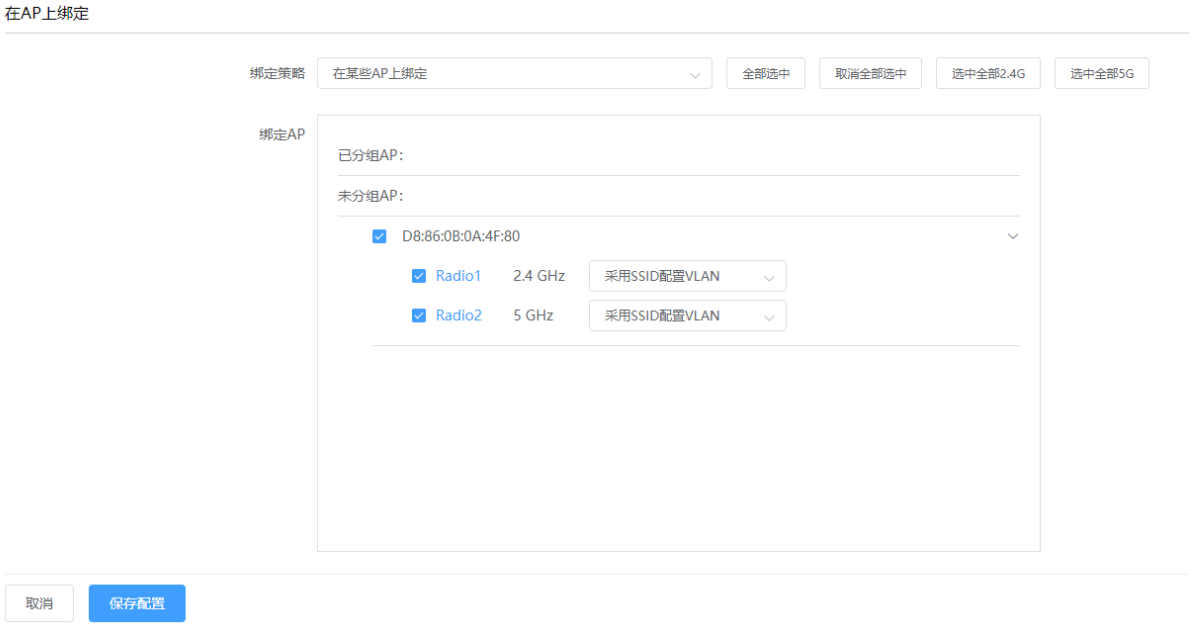
5. 配置 SSID

单击菜单【设置】>子菜单【无线】，进入“SSID”页面，编辑第一个 SSID 模板。

配置 SSID 名称、开启使能、选择预共享密钥方式

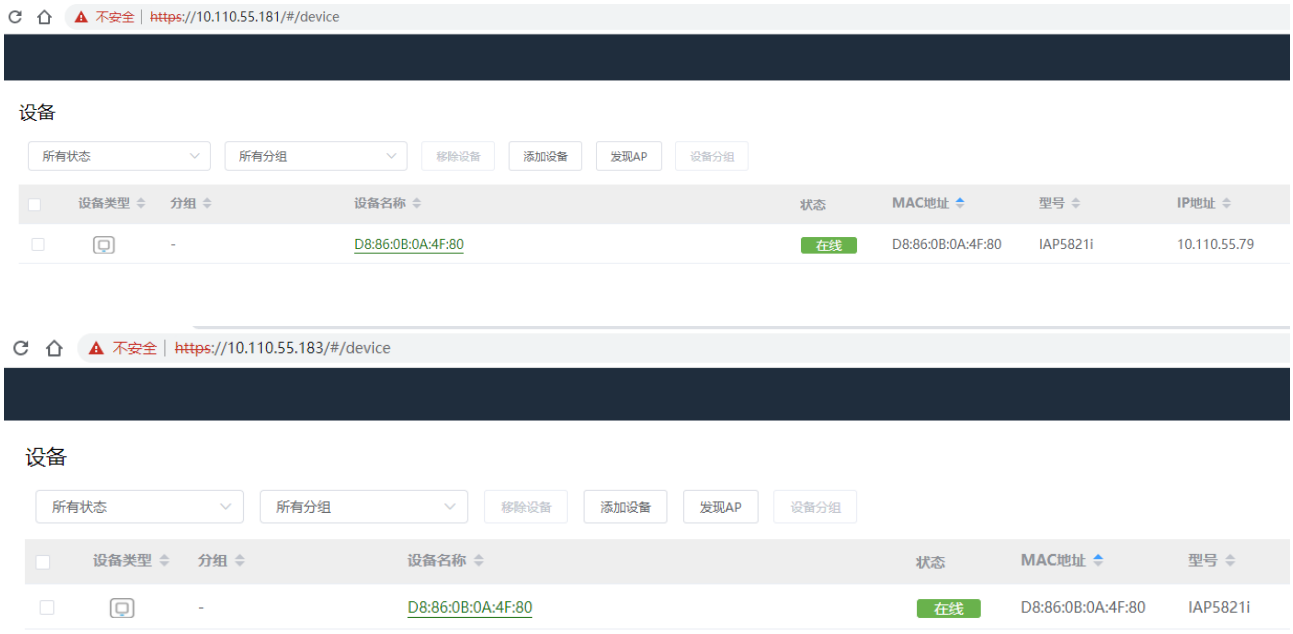
“数据转发方式”选择集中转发模式，“VLAN 标记”选择使用预置 VLAN 标记，配置 VLAN 为 20

选择要绑定的 AP 点击“保存配置”



5.4.4.4 检查配置结果

（1）AP 会同时在 AC1 和 AC2 上在线

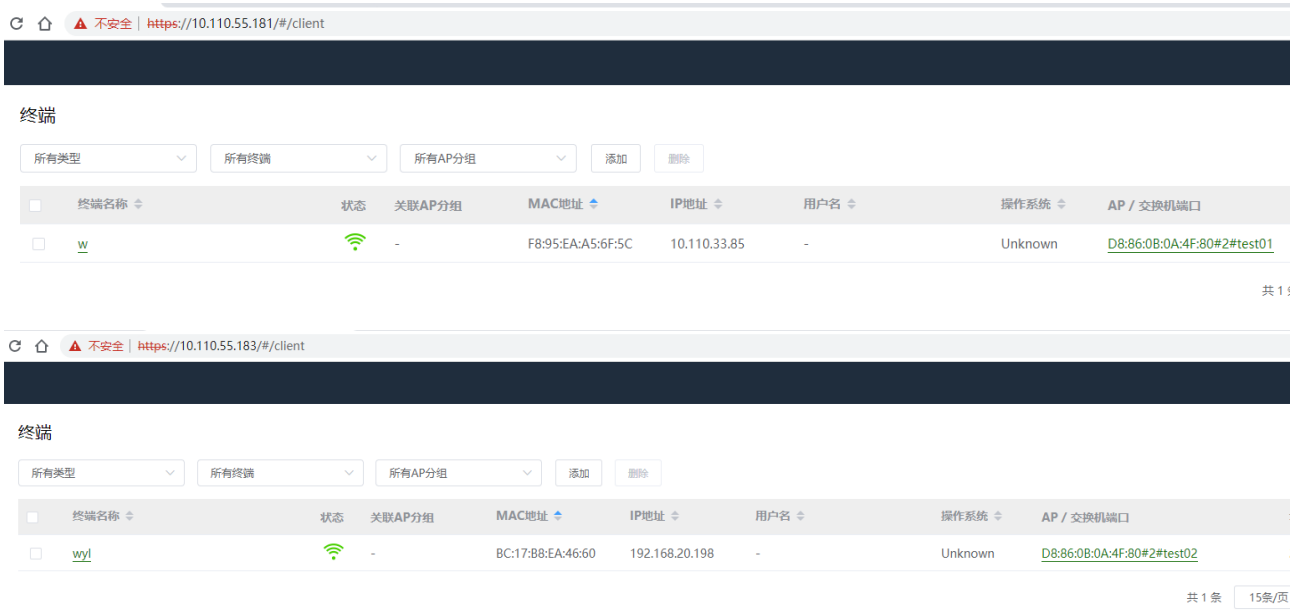


（2）终端关联验证

终端 1 关联 test01 可获取 vlan3 网段的 ip，可访问外网，无法访问内网的 192.168.20.0 网段的本地管理平台，在 AC1 上可看到该终端的关联信息，AC2 上无法看到该终端；

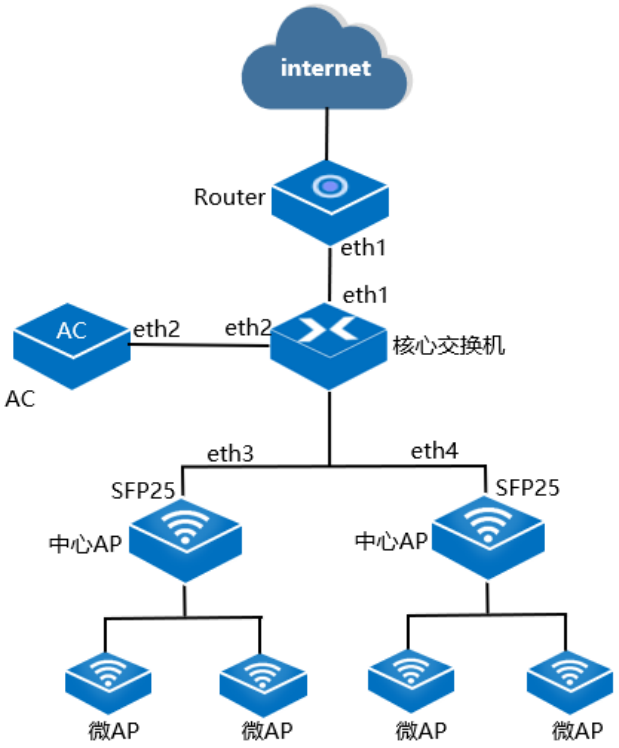
终端 2 关联 test02 可以获取 vlan20 网段的 ip，可访问内网的 192.168.20.0 网段的本地管理平台，无法访问外网，在 AC2 上可看到该终端的关联信息，AC1 上无法看到该终端；

终端 1 和终端 2 之间互相隔离。



5.5 智联中心 AP 组网示例

5.5.1 网络拓扑示意



5.5.2 业务需求

用户接入 WLAN 网络，使用 AC 内置的 Easy Portal 认证方式进行认证，输入正确的用户名和密码后可以无线上网。

5.5.3 组网需求

组网需求：

- AC 组网方式：旁挂二层组网。
- DHCP 部署方式：核心作为 DHCP 服务器为 AP 和 STA 分配 IP 地址。
- 业务数据转发方式：本地转发。
- WLAN 认证方式：Easy Portal。

5.5.4网络规划

配置项	规划数据
管理 VLAN	VLAN9
业务 VLAN	VLAN3
AC 的源接口	VLANIF9：10.110.99.185/24
DHCP 服务器	核心作为 DHCP 服务器为 AP 和 STA 分配 IP 地址
AP 的 IP 地址池	10.110.99.50～10.110.99.100/24
STA 的 IP 地址池	10.110.33.50～10.110.33.100/24
SSID 名称	SSID 名称：WLAN_test
安全策略	安全策略：开放系统（不加密）+Easy Porta 本地账号认证
VAP 模板	转发模式：本地转发 业务 VLAN：VLAN3

5.5.5配置思路

- ✧ 配置 AP、AC 和周边网络设备之间实现网络互通。
- ✧ 配置 AC 局域网
- ✧ 配置 AP 在 AC 上线。
- ✧ 在 AC 上配置 WLAN 相关业务（SSID）。
- ✧ 配置 Easy Portal 本地用户账号。

5.5.6操作步骤

5.5.6.1 配置周边设备

配置核心交换机

创建管理和业务 VLAN；

配置管理和业务地址池；

配置下一跳为 Router 的缺省路由。

```
vlan database
 vlan 1 to 4094 bridge 1
interface eth1
 switchport mode trunk
 switchport trunk allowed vlan add 100
 switchport trunk pvid 100
 description TO-Router
interface eth2
 switchport mode trunk
 switchport trunk allowed vlan add 1,9
 switchport trunk pvid 1
 description TO-AC
interface eth3
 switchport mode trunk
 switchport trunk allowed vlan add 3,9
 switchport trunk pvid 9
 description TO-AP
interface eth4
 switchport mode trunk
 switchport trunk allowed vlan add 3,9
 switchport trunk pvid 9
 description TO-AP
interface vlan1.3
 ip address 10.110.33.1/24
interface vlan1.9
 ip address 10.110.99.1/24
interface vlan1.200
 ip address 192.168.1.2/24
ip dhcp pool vlan3
 network 10.110.33.1/24
 range 10.110.33.50 10.110.33.100
```

```
 option43 ip 10.110.33.2
 lease-time 0 0 5 0
 default-router 10.110.33.1
 dns-server 202.106.46.151 202.106.195.68
ip dhcp pool vlan9
 network 10.110.99.1/24
 range 10.110.99.50 10.110.99.100
 default-router 10.110.99.1
 lease-time 0 0 30 0
 dns-server 202.106.46.151 202.106.195.68
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

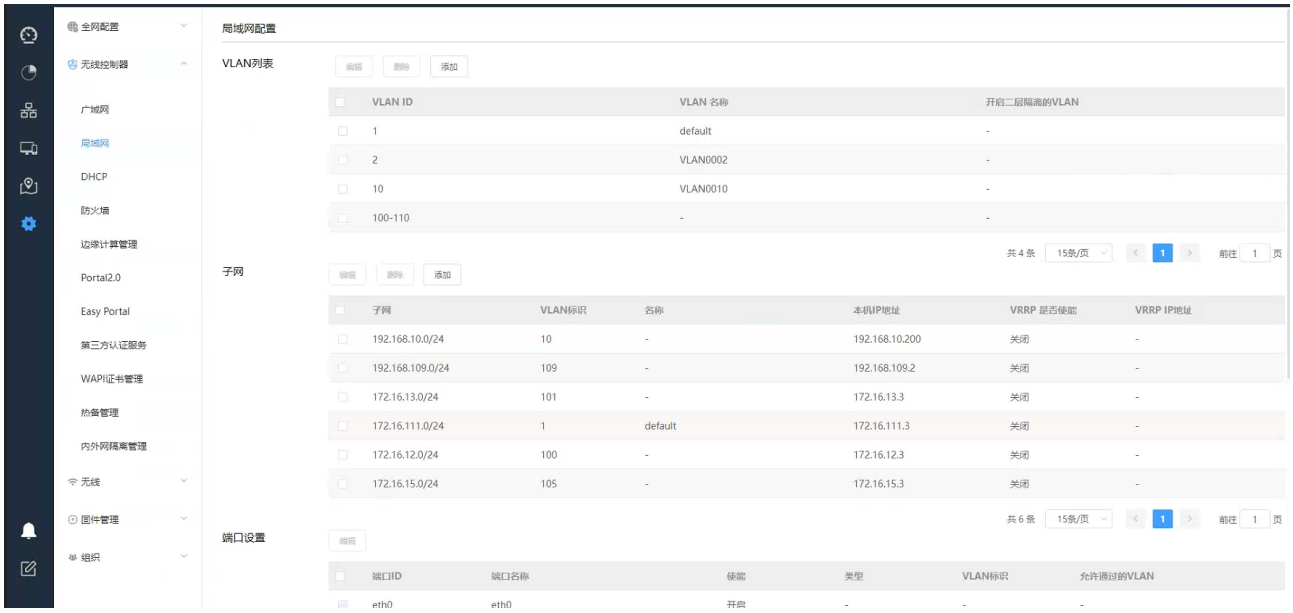
配置 Router 的接口 eth1 的 IP 地址，并配置指向 STA 网段的静态路由。

```
interface eth0
  ip address 192.168.1.1 24
ip route-static 10.110.33.0 255.255.255.0 192.168.1.2
```

5.5.6.2 配置 AC 局域网

1. 进入 AC 局域网配置页面。

登录 AC Web 系统，单击菜单【设置】>子菜单【无线控制器】>子菜单【局域网】，进入“局域网配置”页面。



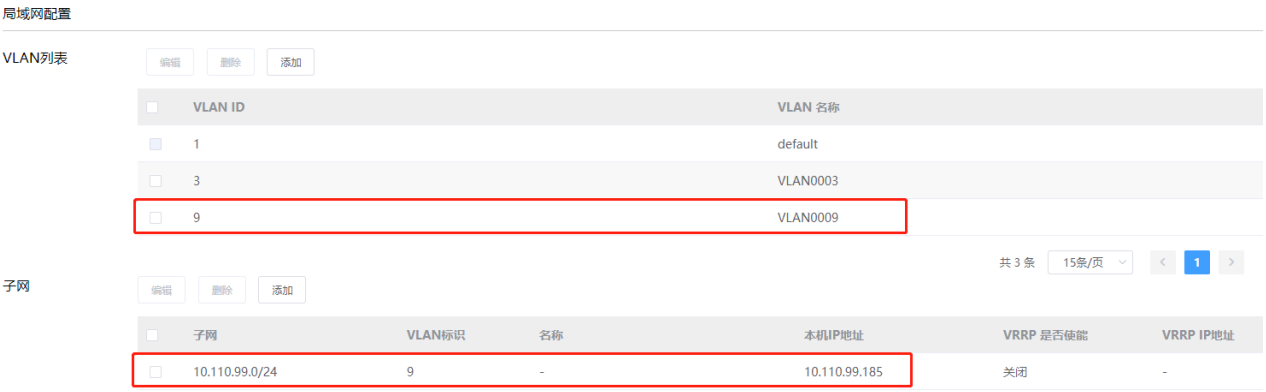
2. 配置网络互联。

a. 创建管理和业务 VLAN

在“VLAN 列表”，单击选择<添加>按钮，添加 AP 管理 VLAN 9 及业务 VLAN 3

在“子网”中，单击选择<添加>按钮，创建 AP 管理平面的配置虚拟接口 Interface VLAN 9 接口地址 10.110.99.185。

单击<确定>按钮，AP 管理平面接口地址配置完成。



b. 配置端口

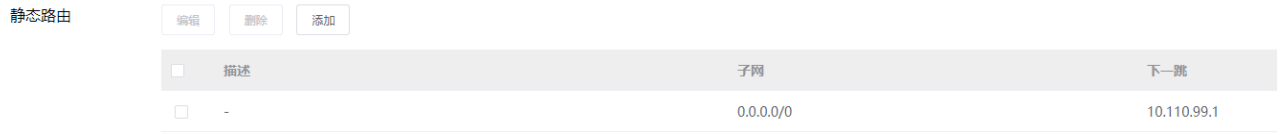
选择旁挂核心交换机的连接端口“eth2”，单击<编辑>按钮，选择“接口类型”为“Trunk”，将“eth2”加入 VLAN9（管理 VLAN）。

单击<确定>，完成配置。

c. 配置静态路由。

继续在【局域网】菜单下划鼠标，单击“静态路由”下的<添加>按钮，进入“添加静态路由表”页面。

配置“子网”为“0.0.0.0/0”，“下一跳”为“10.110.99.1”。

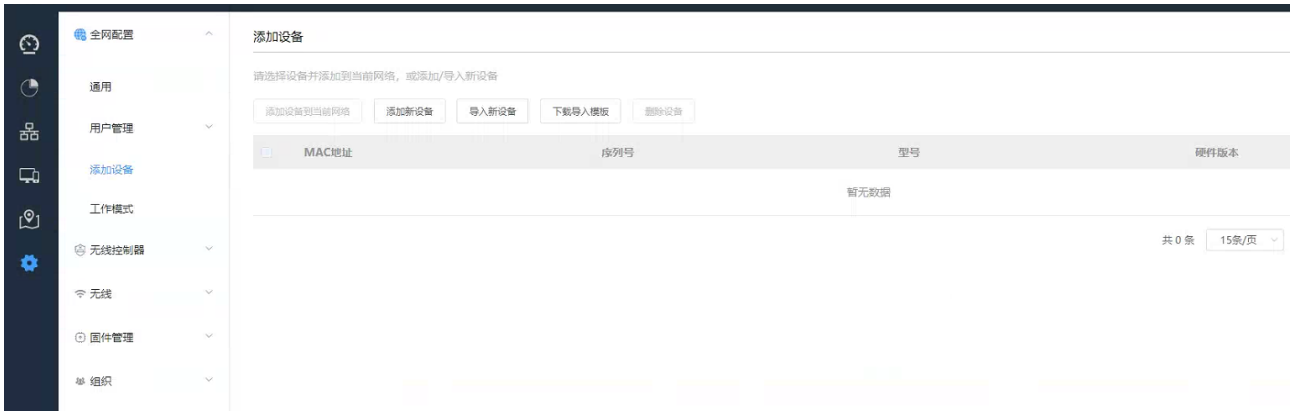


#【局域网】下的所有配置生效需单击页面最下方的<保存>按钮来完。（**重要提醒!!!**）

3. 配置中心 AP 在 AC 上线

手动添加 AP：

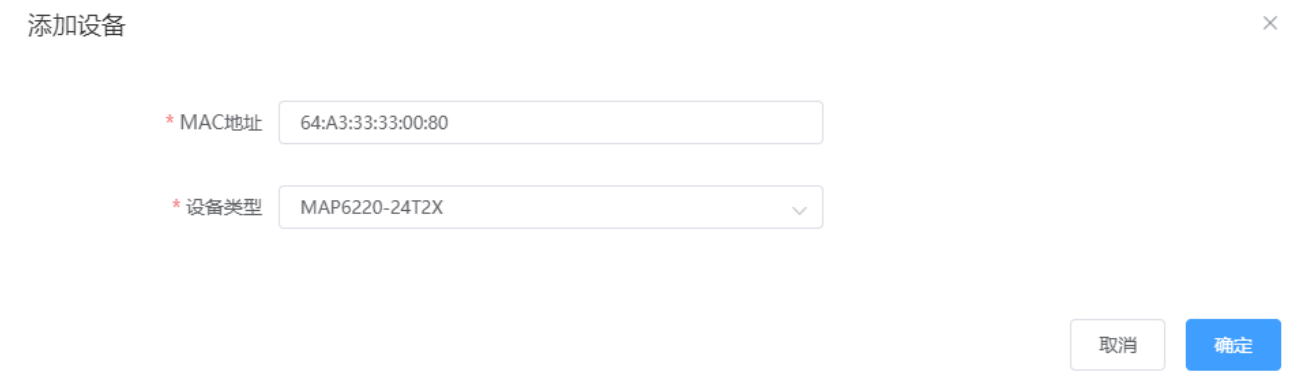
单击菜单【设置】>子菜单【全网配置】>子菜单【添加设备】，进入 AP 设备添加界面。



通过<添加设备>按钮、或<下载模板>按钮 + <批量导入设备至当前网络>按钮，可进行单个或批量添加 AP 到 AC。

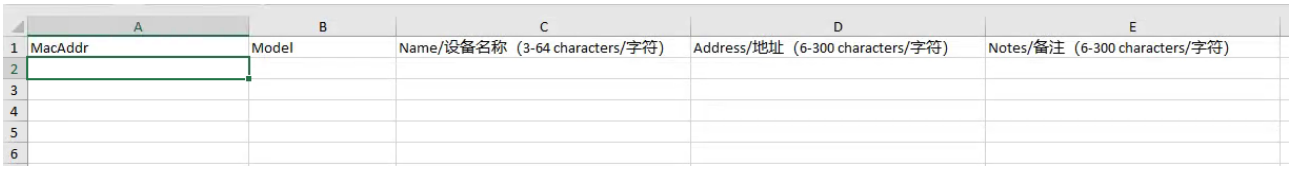
方法一：单独添加 AP：

点击<添加新设备>，填写 MAC 地址并选择设备类型



方法二：通过模板添加 AP

在下载的 AP 模板文件中填写 AP 信息，示例如下“MACAddr：64:A3:33:33:00:80”，“Model：MAP6220-24T2X”等信息，如需添加多个 AP，可以在 AP 模板文件中填写多条 AP 信息。



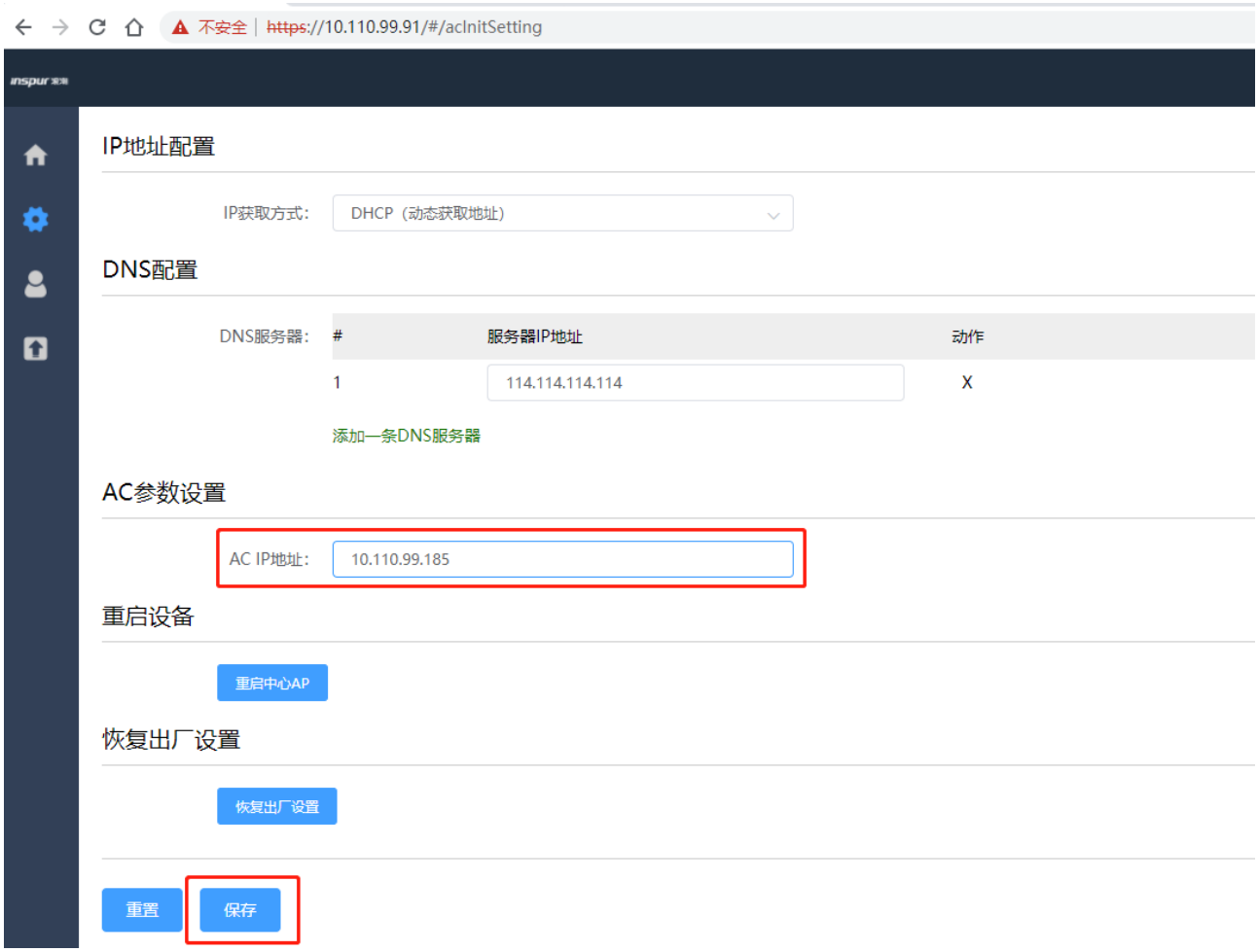
	A	B	C	D	E
1	MacAddr	Model	Name/设备名称（3-64 characters/字符）	Address/地址（6-300 characters/字符）	Notes/备注（6-300 characters/字符）
2					
3					
4					
5					
6					

单击<批量导入设备至当前网络>按钮，选择填写后的模板文件，单击“打开”。

导入完成后，单击菜单【设备】，可查看添加的全部 AP 列表。

若未配置 option 43，则需要登录中心 AP 的 WEB 管理页面配置 AC IP 地址。

中心 AP 手动配置 AC IP 地址方法：【设置】>【AC 参数设置】，配置 AC IP 地址并保存。

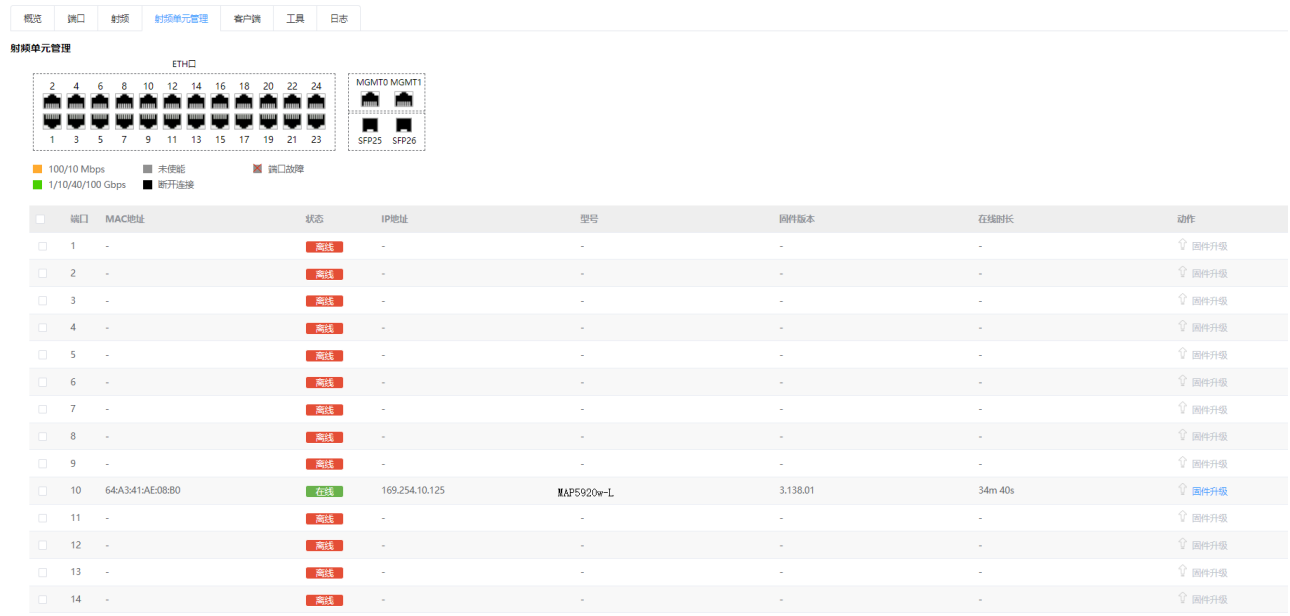


网络无异常情况下，几分钟后，AP 将依次上线。

网络无异常情况下，几分钟后，AP 将依次上线。

每台中心 AP 的 1-24 口一共可以连接 24 个智联远端单元射频模块（微 AP），微 AP 直接连接中心 AP 的 1-24 口即可，不需要单独配置微 AP。

从 AC WEB 的【设备】列表，进入中心 AP 的详情页面，在【概览】>【射频单元管理】可查看已连接的微 AP。



中心 AP 的 1-24 口分别对应微 AP1-微 AP24，每个微 AP 包含 1 个 2.4GHZ 射频和 1 个 5GHz 射频。

射频 ID1----微 AP1:2.4G

射频 ID2----微 AP1:5G

射频 ID3----微 AP2:2.4G

射频 ID4----微 AP2:5G

……

射频 ID47----微 AP24:2.4G

射频 ID48----微 AP24:5G

5.5.6.3 配置 WLAN 业务

配置中心 AP 的 VLAN 接口

使用 portal 认证时，需要为中心 AP 配置业务 VLAN 接口 IP

单击菜单【设置】>子菜单【无线】>子菜单【中心 AP 配置】，点击<添加>，选择需要配置的中心 AP，选择业务 VLAN，配置 IP 地址。

配置 SSID

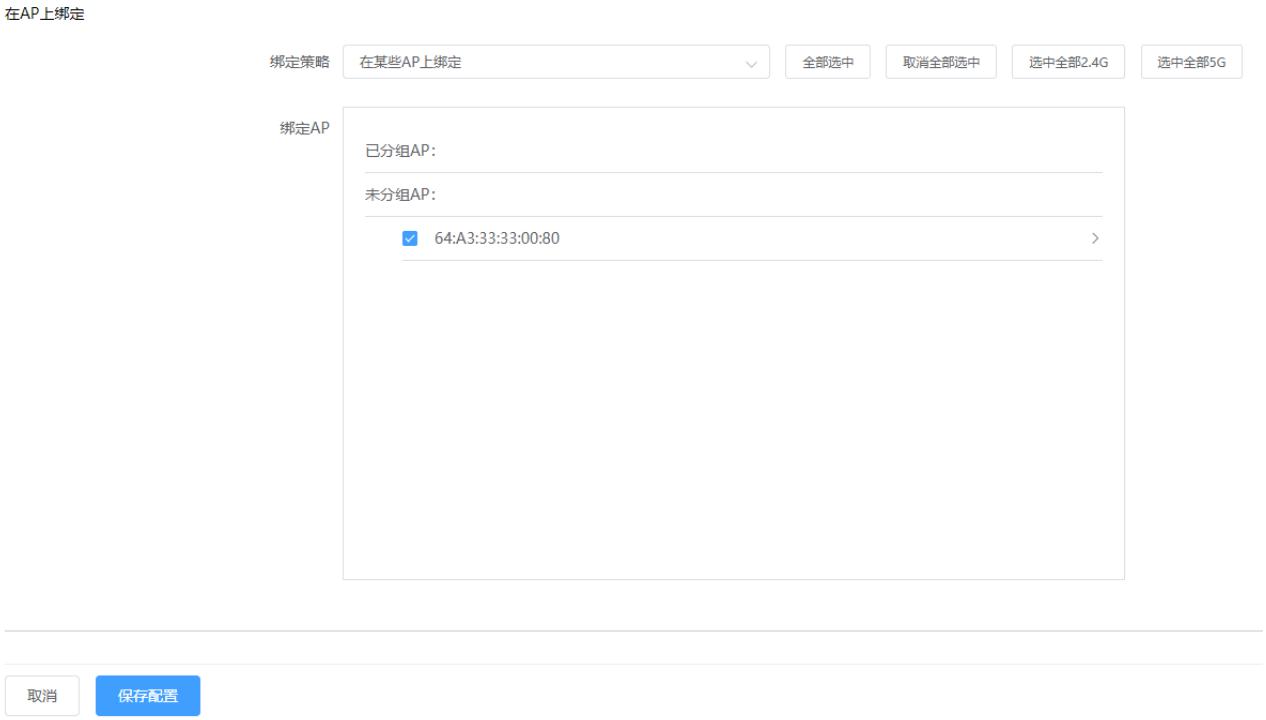
单击菜单【设置】>子菜单【无线】>子菜单【无线服务】，进入 WLAN 业务配置页面。

系统默认提供 15 个 SSID 模板，可任意选择一个进行修改；

单击任意 SSID 进入 SSID 编辑页面，配置 SSID 名称为 WLAN_test，开启使能，关联接入方式选择开放系统（不加密），Portal 策略选择本地账号认证。

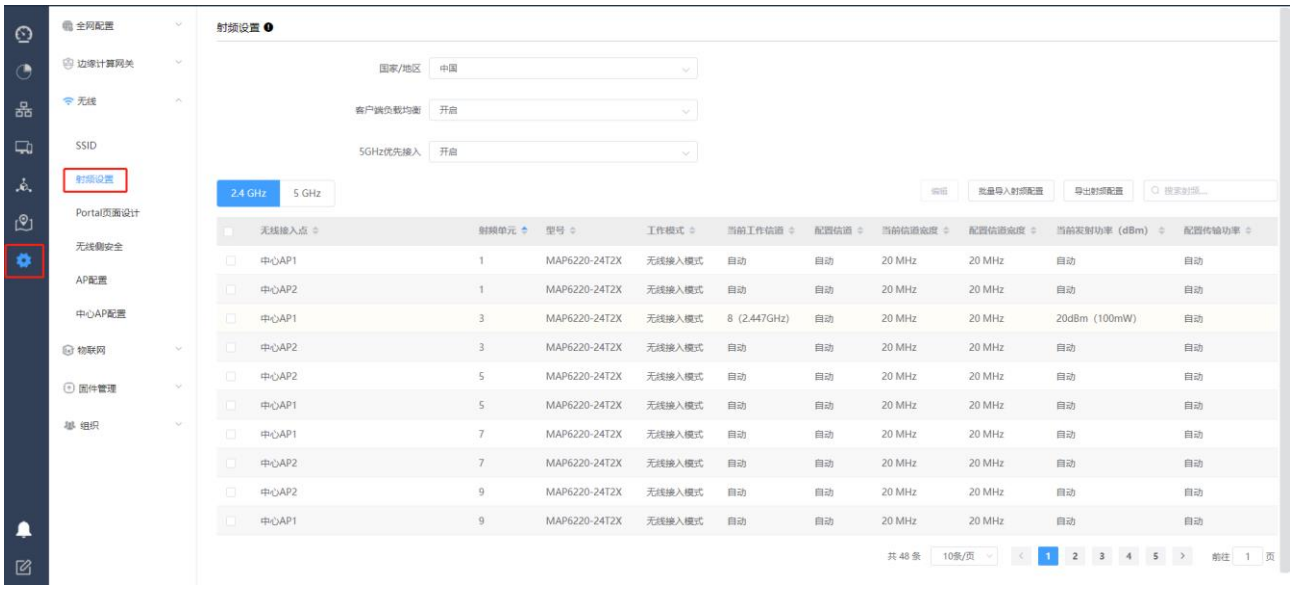
数据转发方式选择二层桥接模式，使用预配置 VLAN 标记 3，DHCP 转发方式选择本地转发模式。

绑定 AP 并保存配置。

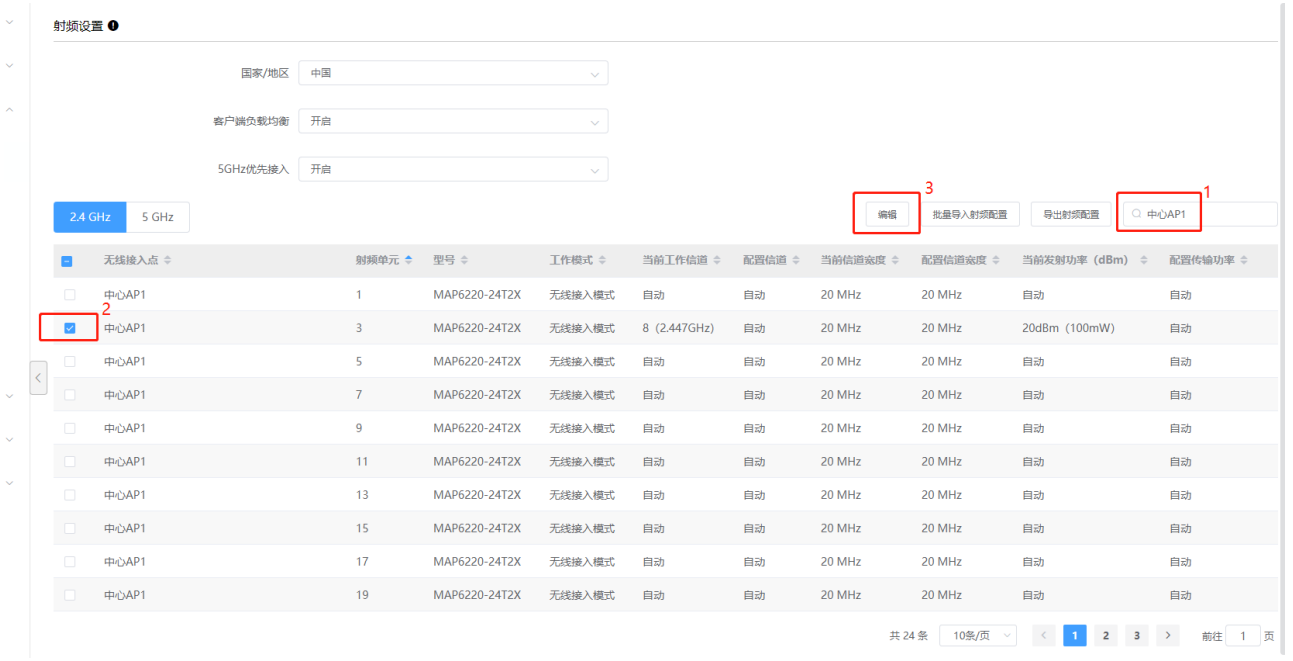


配置 AP 的信道和功率

单击菜单【设置】>子菜单【无线】>子菜单【射频设置】，进入 AP 的信道和功率配置页面。



单击“射频设置”中<2.4G>或<5G>射频的选项按钮，过滤框中可过滤要编辑的中心 AP，选定需要进行编辑的射频单元，点击右上方的<编辑>按钮，进入信道、信道宽度、发射功率等参数的配置页面。



Easy Portal 本地用户配置

配置认证策略模板：创建授权 portal 认证的模板，用户组/用户可绑定该模板。

路径：【设置】>子菜单【全网配置】>子菜单【用户管理】>子菜单【认证策略模板】><添加模板>

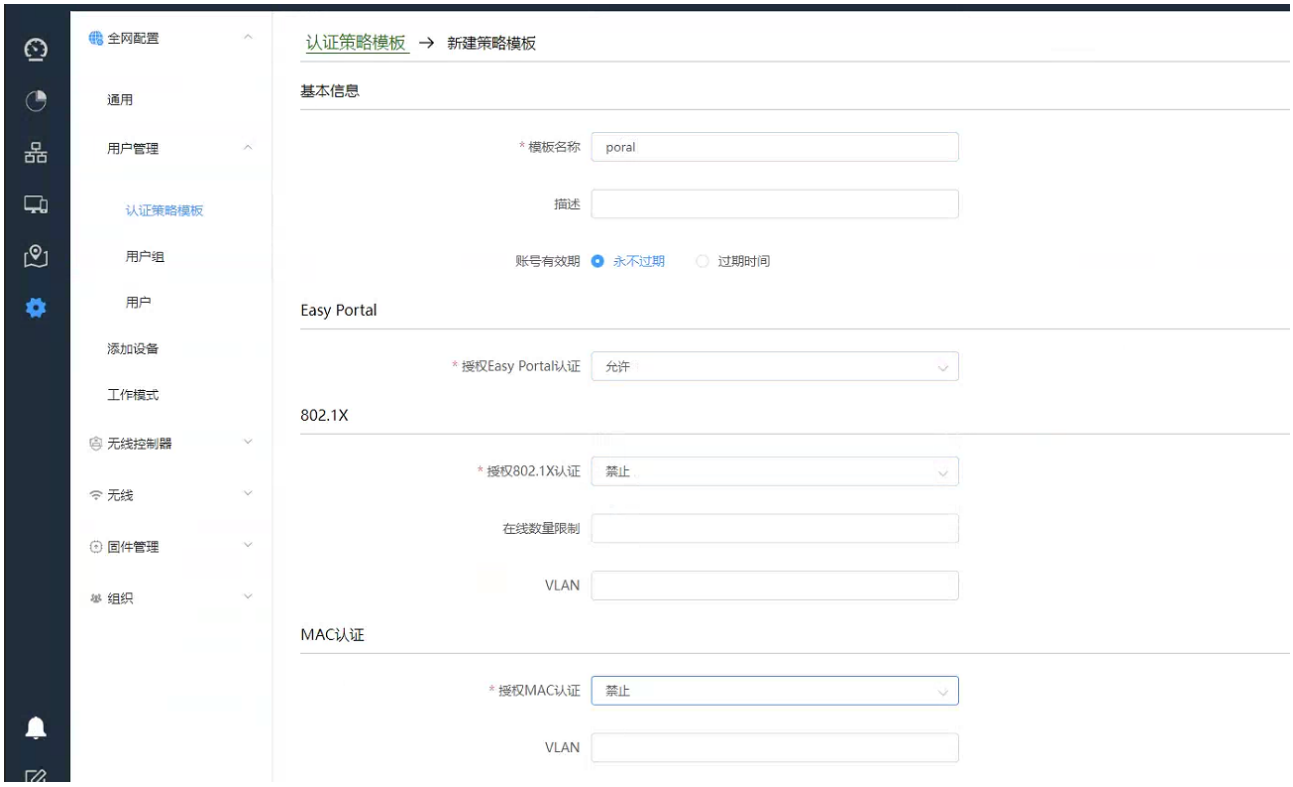
模板名称：可自定义

描述：可自定义

账号有效期：可选择永不过期或设置过期时间

Easy Portal：选择允许

802.1X 和 MAC 认证选择禁止授权



配置用户组：用户组上可绑定认证策略模板及 SSID

路径：【设置】>子菜单【全网配置】>子菜单【用户管理】>子菜单【用户组】><添加一级用户组>

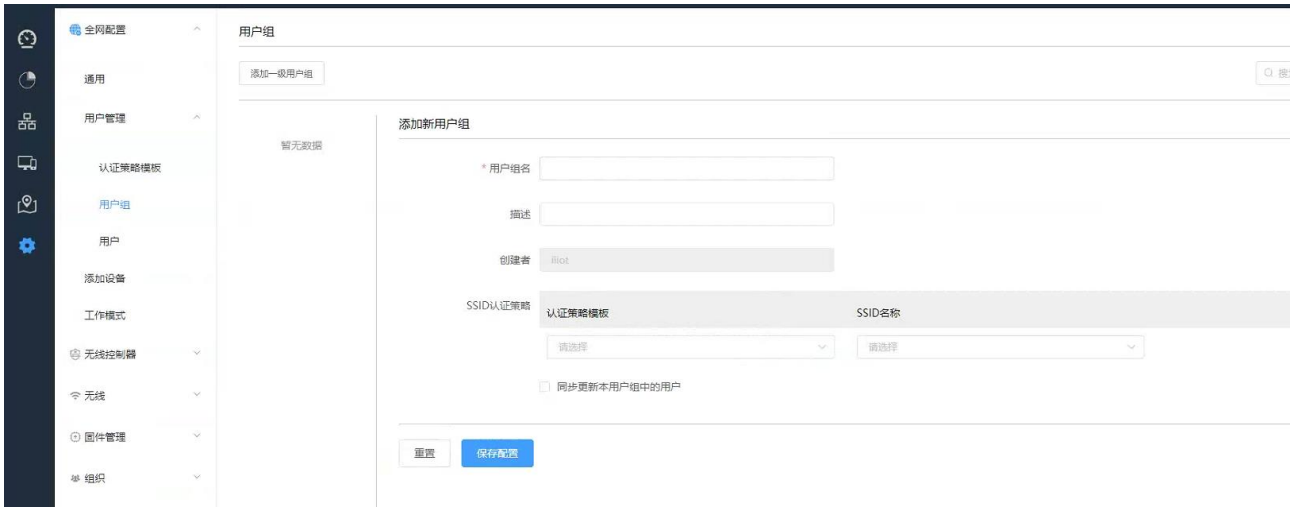
用户组名：可自定义

描述：可自定义

SSID 认证策略：选择上一步创建的认证策略模板（portal）及要绑定的 MAC 认证的 SSID（WLAN_test）

同步更新本用户组中的用户：选中后，会将本用户组中的认证策略模板和绑定的 SSID 同步到该用户组的所有用户。

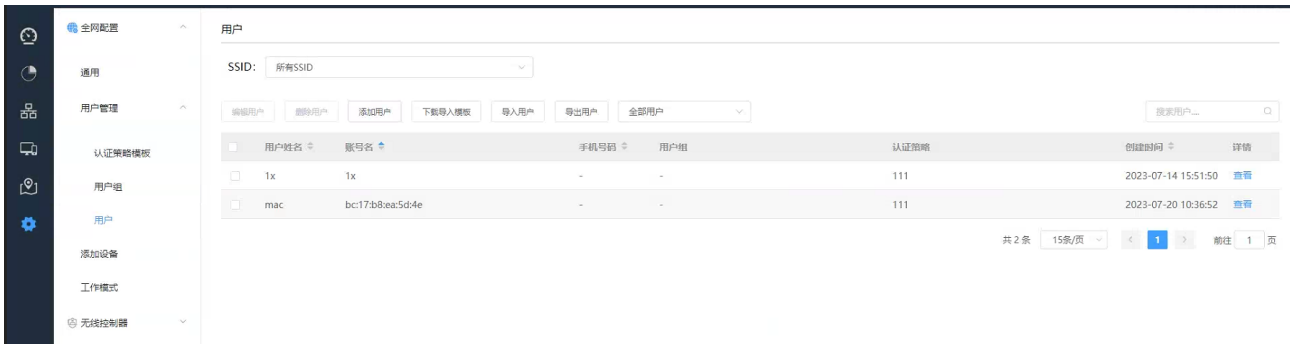
点击<保存配置生效>



添加用户：添加 portal 认证用户

路径：【设置】>子菜单【全网配置】>子菜单【用户管理】>子菜单【用户】

点击<添加用户>可添加单个用户；击<下载模板>，可通过模板批量导入用户



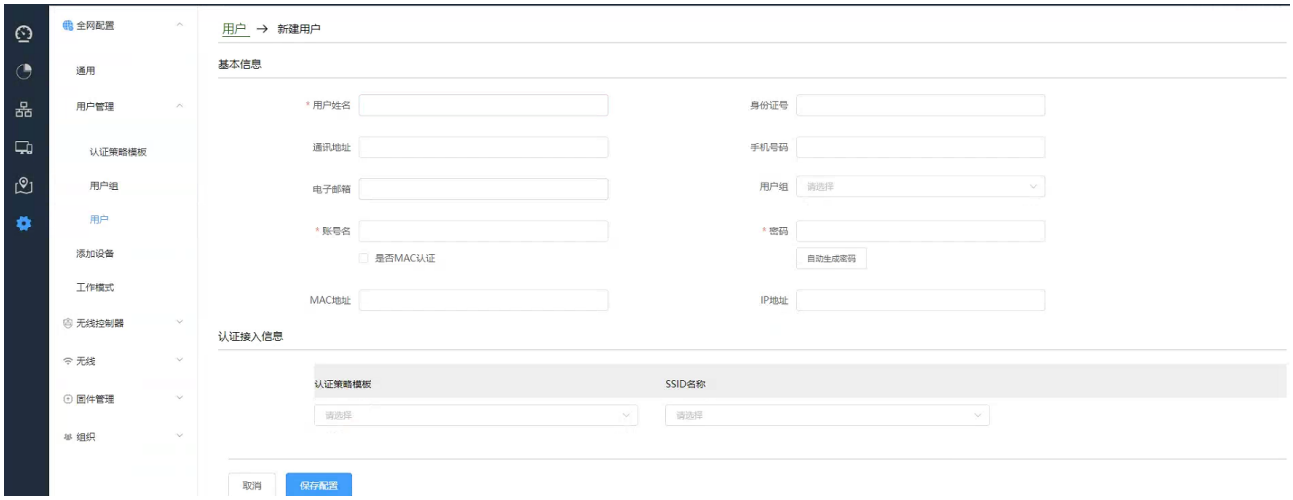
本例点击<添加用户>，弹出如下配置页面：

设置用户姓名、账号名和密码；

账号名栏填写账号名称；

选择用户分组-组 1，认证接入信息会自动变为组 1 中绑定的认证策略模板（portal）和 SSID（WLAN_test），

点击<保存配置>生效



5.5.6.4 检查配置结果

完成配置后，用户可通过无线终端搜索到 SSID 为 WLAN_test 的无线网络。

终端连接上无线 SSID，在弹出的 web 认证界面上通过设置的 portal 账号密码可关联到该无线网络。