SUNDRAY

WLAN 3.7.4.2 用户手册

SUNDRAY
信锐技术

目录

声明

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。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系信锐网科技术有限公司客户服务部。

前言

本手册各章节内容如下：

第 1 部分 SUNDRAY WLAN 产品安装指南。该部分主要介绍 WLAN 设备的外观特点及功能特性和性能参数，以及连接前的准备和注意事项。

第 2 部分 SUNDRAY WLAN NAC 控制台的使用，如何登陆控制台等。

第 3 部分 SUNDRAY WLAN NAP 介绍。

第 4 部分 SUNDRAY WLAN NAC 功能说明及使用。

第 5 部分 案例集。讲解各功能模块在常见环境下的配置案例。

本手册以 WLAN NAC-6200 为例进行配置。由于各型号产品硬件和软件规格存在一定差异，所有涉及产品规格的问题需要和信锐网科技术有限公司联系确认。

本书约定

图形界面格式约定

文字描述	代替符号	举例
按钮	边框+阴影+底纹	“确定”按钮可简化为确定
菜单项	『』or 【】	菜单项“系统设置”可简化为『系统设置』或【】
连续选择菜单项及子菜单项	→	选择【系统设置】→【接口配置】
下拉框、单选框、复选框选项	[ ]	复选框选项“启用用户”可简化为[启用用户]
窗口名	【】	如点击弹出【新增用户】窗口
提示信息	“”	提示框中显示“保存配置成功，配置已修改，需要重启 DLAN 服务才能生效，是否立即重启该服务?”

各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 **小心、注意：**提醒操作中应注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。

 **警告：**该标志后的注释需给予格外的关注，不当的操作可能会给人身造成伤害。

 **说明、提示、窍门：**对操作内容的描述进行必要的补充和说明。

技术支持

用户支持邮箱： support@sundray.com.cn

技术支持热线电话： 400-878-3389（手机、固话均可拨打）

公司网址： www.sundray.com.cn

致谢

感谢您使用我们的产品及用户手册，如果您对我们的产品或用户手册有什么意见和建议，您可以通过电话、论坛或电子邮件反馈给我们，我们将不胜感谢。

第1章 安装指南

本部分主要介绍了 SUNDRAY WLAN 系列产品的构成与硬件安装。硬件安装正确之后，您可以进行配置和调试。

1.1. 环境要求

SUNDRAY WLAN 设备可在如下的环境下使用。

- 输入电压：110V~230V
- 温度：0～45℃
- 湿度：5～90%

为保证系统能长期稳定的运行，应保证电源有良好的接地措施、防尘措施、保持使用环境的空气通畅和室温稳定。本产品符合关于环境保护方面的设计要求，产品的安放、使用和报废应遵照国家相关法律、法规要求进行。

1.2. 电源

SUNDRAY WLAN 系列产品使用交流 110V 到 230V 电源。在您接通电源之前，请保证您的电源有良好的接地措施。

1.3. 产品外观

图 1 SUNDRAY WLAN-NAC6200 外观图

图 2 SUNDRAY WLAN-NAC6200 前面板图

图 2：SUNDRAY WLAN-NAC6200 前面板（以 WLAN NAC-6200 为例）

1.CONSOLE(控制)口　　2.USB 口　　3.MANAGE(ETH0)　　4.ETH1

5.ETH2　　6.ETH3　　7.ETH4　　8.ETH5

告警灯在设备启动期间是红灯长亮的。一般一两分钟后红灯熄灭，说明正常启动。如红灯长时间不熄灭，请关闭设备等待 5 分钟后重新开机。如果还是长亮，请联系客服部门确认是否设备损坏。正常启动后，有时红灯会闪烁，这是正常现象，红灯闪烁表示设备正在写系统日志。

控制口仅供开发和测试调试使用。最终用户需通过控制台网口接入设备。

1.4. 配置与管理

在配置设备之前，您需要配备一台电脑，配置之前请确定该电脑的网页浏览器能正常使用（如 Internet Explorer），然后把电脑与 NAC 设备连接在同一个局域网内，通过网络对设备进行配置。

NAC 设备的管理口为 MANAGE(ETH0)口，管理口默认出厂 IP 为 10.252.252.252/24。初次登陆设备，请用网线连接 MANAGE(ETH0)口到局域网或直接连接电脑。

1.5. 设备接线方式

在背板上连接电源线，打开电源开关，此时前面板的 Power 灯（绿色，电源指示灯）和 Alarm 灯（红色，告警灯）会点亮。大约 1-2 分钟后 Alarm 灯熄灭，说明网关正常工作。

请用标准的 RJ-45 以太网线将 MANAGE(ETH0)口与内部局域网连接，对 WLAN-NAC 设备进行配置。

登录控制台后根据网络环境和部署要求配置『网络配置』和接线。（详情参见章节 3.2）

设备正常工作时 POWER 灯常亮，接线的数据接口 LINK 灯长亮，ACT 灯在有数据流量时会不停闪烁。ALARM 红色指示灯只在设备启动时因系统加载会长亮（约一分钟），正常工作时熄灭。如果在安装时此红灯长亮，请将设备断电重启，重启之后若红灯一直长亮不熄灭，请与我们联系。

网口直接连接 MODEM 和交换机应使用直连线、连接路由器和电脑网口应使用交叉线。当指示灯显示正常，但不能正常连接的时候，请检查连接线是否使用错误。直连网线与交叉网线的区别在于网线两端的线序不同，如下图：

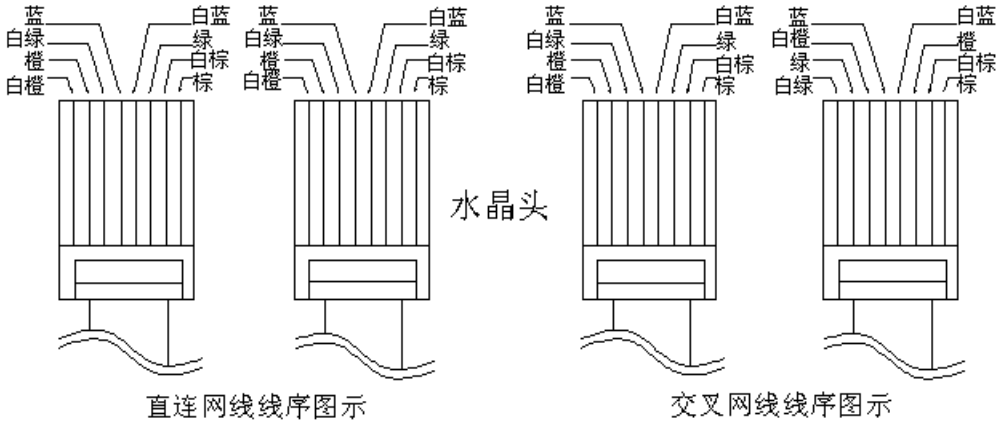


图 1　直连线、交叉线 线序

第2章 NAC 控制台的使用

2.1. 登录 WebUI 配置界面

WLAN-NAC 支持安全的 HTTPS 登录，使用的是 HTTPS 协议的标准端口登录。如果初始登录从管理口(MANAGE)登录，那么登录的 URL 为：https://10.252.252.252

HTTPS 登录 WEBUI 管理 NAC 可以防止配置过程在传输过程中被截获而产生的安全隐患。

如何登录 NAC 设备控制台页面？

按照前面所示方法接好线后，通过 WEB 界面来配置 SUNDRAY NAC 设备。方法如下：

首先为登陆控制台的电脑配置一个 10.252.252.X 网段的 IP（如配置 10.252.252.100），然后在 IE 浏览器中输入管理口的默认登陆 IP 及端口 https://10.252.252.252，出现一个如下图的安全提示：

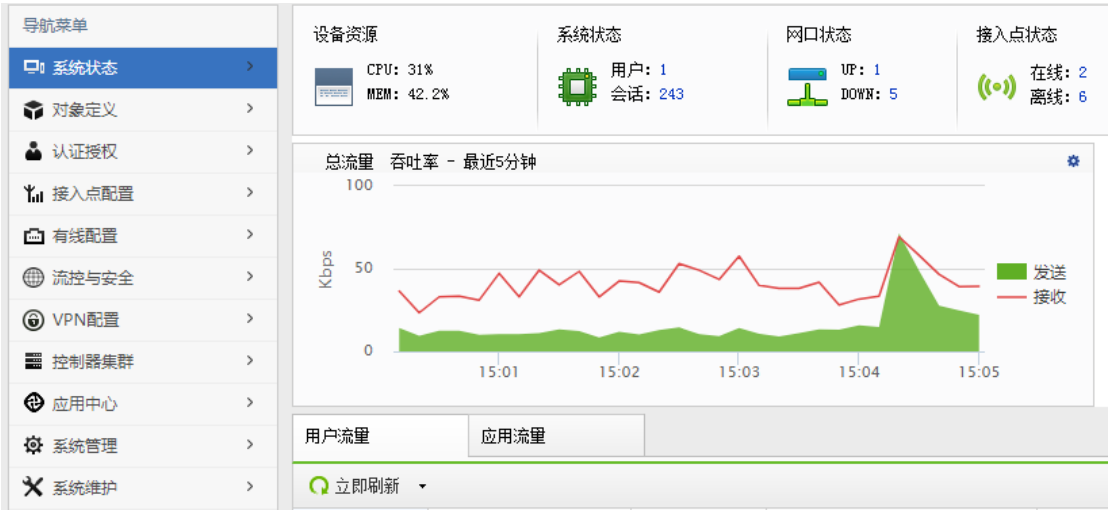
点击继续浏览此网站（不推荐）后出现以下的登录界面：

在登陆框输入『账号』和『密码』，点击登录按钮即可登录 WLAN 设备进行配置，出厂情况下的用户名和密码为 admin/admin。

如果需要查看当 NAC 设备的版本号，点击版本信息，即显示当前设备的版本信息。

2.2. 配置和使用

登录 WebUI 配置界面后，可以看到以下配置模块：包括『系统状态』、『对象定义』、『认证授权』、『接入点配置』、『有线配置』、『流控与安全』、『VPN 配置』、『控制器集群』、『应用中心』、『系统管理』、『系统维护』。



所有配置界面中的  图标，当鼠标放到此图标上时，可以显示当前配置项的简要帮助说明。后面的文档不再赘述。

第3章 WLAN-NAP 介绍

3.1. 型号与外观

NAP，全称 Network Access Point，简称 AP，信锐网络科技有限公司现多款无线 AP，每次新版本都会新增支持不同类型的 AP，当前版本支持型号如下介绍：

3.1.1. DIS-1220

信锐 DIS-1220 是信锐自主研发的 802.11n 无线接入点。DIS-1220 内置全向天线，支持 802.11b/g/n 协议，最大无线接入速率达 300Mbps，可供更快的无线上网和更大的无线覆盖范围。

信锐 DIS-1220 支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐控制器，为用户带来前所未有的快速体验和更安全的业务接入。

该系列产品基于室内放装型设计， 外观美观大方，安装方便， 适用于吸顶、壁挂以及桌面放装。

3.1.2. DIS-1320

信锐 DIS-1320 系列无线接入点是信锐自主研发的室内双频无线接入点。DIS-1320 系列无线接入点采用 2x2 MIMO 技术，支持 11a/n 和 11b/g/n 双频并发，整机最高可达 600Mbps，

可提供更快的无线上网和更大的无线覆盖范围。产品高达 600Mbps 的最大传输速率能够轻松满足各种无线业务的承载使用，如视频、语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。

设备采用千兆以太网口上行链路， 突破了百兆上行速率的限制，保证无线高速传输；支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐控制器，为用户带来前所未有的快速体验和更安全的业务接入。

信锐 DIS-1320 系列产品外观美观大方，安装方便，适用于吸顶、壁挂以及桌面放装。

3.1.3. **DIS-1520**

信锐 DIS-1520 无线接入点是信锐自主研发的新一代 802.11ac 高性能无线接入点。DIS-1520 支持 11ac/a/n 和 11b/g/n 双频并发，整机最高速率可达 1167Mbps，可提供更快的无线上网和更大的无线覆盖范围。产品高达 1.167Gbps 的最大传输速率能够轻松满足各种无线业务的承载使用，如视频、语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。

设备采用千兆以太网口上行链路，突破了百兆上行速率的限制，保证无线高速传输；支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐控制器，为用户带来前所未有的快速体验和更安全的业务接入。

信锐 DIS-1520 产品外观美观大方，安装方便， 适用于吸顶、壁挂以及桌面放装。

3.1.4. NAP-1500

信锐 NAP-1500 是信锐自主研发的 802.11n 无线接入点。NAP-1500 外置 5dBi 全向天线，支持 802.11b/g/n 协议，最大无线接入速率达 300Mbps，可提供更快的无线上网和更大的无线覆盖范围。

信锐 NAP-1500 提供 3 个有线以太网口，可以进行有线扩展，如接入台式机、打印机等。

信锐 NAP-1500 支持 DC 本地供电，配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

该系列产品采用放装型设计，外观美观大方，安装方便，适用于桌面放装。

3.1.5. NAP-1600

信锐 NAP-1600 无线接入点是信锐自主研发的新一代 802.11ac 高性能无线接入点。NAP-1600 内置天线，支持 11ac/a/n 和 11b/g/n 双频并发，整机最高速率可达 733Mbps，可提供更快的无线上网和更大的无线覆盖范围。产品高达 733Mbps 的最大传输速率能够轻松满足各种无线业务的承载使用，如视频、语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。

设备支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

信锐 NAP-1600 产品外观美观大方，安装方便，适用于吸顶、壁挂以及桌面放装。

3.1.6. NAP-1700

信锐 NAP-1700 无线接入点是信锐自主研发的新一代 802.11ac wave2 高性能无线接入点。NAP-1700 内置天线，支持 11ac/a/n 和 11b/g/n 双频并发，整机最高速率可达 1167Mbps，可提供更快的无线上网和更大的无线覆盖范围。产品高达 1167Mbps 的最大传输速率能够轻松满足各种无线业务的承载使用，如视频、语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。

设备支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信

锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

信锐 NAP-1700 产品外观美观大方，安装方便，适用于吸顶、壁挂以及桌面放装。

3.1.7. NAP-1720

信锐 NAP-1720-LTE 无线接入点是信锐自主研发的新一代 802.11ac wave2 多业务高性能无线接入点。NAP-1720-LTE 内置天线，支持 11ac/a/n 和 11b/g/n 双频并发，整机最高速率可达 1167Mbps，可提供更快的无线上网和更大的无线覆盖范围。同时支持 4 个有线接口拓展，可以接台式电脑机、有线监控等业务，满足信息化作业、视频、语音等多媒体业务，并提供 4G 全网通无线回传业务，在不方便部署有线出口的场景可以直接使用手机 SIM 作为数据回传，并且支持与有线带宽互为备份，让有线出口断开后，可以无缝切换到 4G 回传，不影响业务使用。

配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

信锐 NAP-1720-LTE 产品外观美观大方，安装方便，适用于壁挂以及桌面放装。

3.1.8. **NAP-2400**

信锐 NAP-2400 无线接入点是信锐自主研发的 802.11n 无线接入点。NAP-2400 内置 2x2 MIMO 高增益 天线，支持 802.11b/g/n 协议，最大无线接入速率达 300Mbps，可提供更快的无线上网和更大的无线覆盖范围。信锐 NAP-2400 能够轻松满足各种无线业务的承载使用，如视频、语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。 设备采用千兆以太网口上行链路，突破了百兆上行速率的限制，保证无线高速传输；支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐 NAC 系列控制器，为用户带来前所未有 的快速体验和更安全的业务接入。信锐 NAP-2400 产品外观美观大方，安装方便，适用于吸顶、壁挂以及桌面放装。

3.1.9. NAP-2400-P

面板式 NAP-2400-P 是信锐专门为酒店客房、宿舍、办公室和医院病房设计的的 802.11n 入墙式面板无线接入点。NAP-2400-P 的尺寸规格完全符合标准的 86 开关面板盒，可以在不破坏墙面装修的情况下安装在任意 86 面板盒上，极大的减少了部署成本。配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

NAP-2400-P 产品还集成了以太网口和 IP 电话接口，方便有线终端和电话接入，产品整体设计美观小巧，并且部署便捷，是酒店等环境无线网络建设的最佳选择。

3.1.10. NAP-2400-s

NAP-2400-s 是信锐自主研发的 802.11n 无线接入点。 支持 2.4G 频段组网、不带外置天线，便于安装和放置，更加美观。支持 802.11b/g/n 协议，最大无线接入速率达 300Mbps，可提供更快的无线上网和更大的无线覆盖范围。

信锐 NAP-2400-s 支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

该系列产品基于室内放装型设计，外观美观大方，安装方便，适用于吸顶、壁挂以及桌面放装。

3.1.11. NAP-2600

信锐 NAP-2600 系列无线接入点是信锐自主研发的室内双频无线接入点。NAP-2600 系列无线接入点采用 2x2 MIMO 技术，支持 11a/n 和 11b/g/n 双频并发，整机最高可达 600Mbps，可提供更快的无线上网和更大的无线覆盖范围。产品高达 600Mbps 的最大传输速率能够轻松满足各种无线业务的承载使用，如视频、语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。

设备采用千兆以太网口上行链路，突破了百兆上行速率的限制，保证无线高速传输；支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

信锐 NAP-2600 系列共分为内置天线、外置天线两款型号，产品外观美观大方，安装方便，适用于吸顶、壁挂以及桌面放装。

3.1.12. NAP-2800

信锐 NAP-2800 系列无线接入点是信锐自主研发的新一代室内智能双频无线接入点。NAP-2800 内置矩阵式智能天线，支持 11a/n 和 11b/g/n 双频并发，整机最高可达 600Mbps，可提供更快的无线上网和更大的无线覆盖范围。产品高达 600Mbps 的最大传输速率能够轻松满足各种无线业务的承载使用，如视频、语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。

设备采用千兆以太网口上行链路，突破了百兆上行速率的限制，保证无线高速传输；支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

信锐 NAP-2800 系列产品外观美观大方，安装方便，适用于吸顶、壁挂以及桌面放装.

3.1.13. NAP-2800-P

面板式 NAP-2800-P 是信锐专门为酒店客房、宿舍、办公室和医院病房设计的 802.11n 单频入墙式面板无线接入点，内置 2x2 MIMO 天线，支持 802.11b/g/n 协议，最大无线接入速率达 300Mbps。NAP-2800-P 的尺寸规格完全符合标准的 86 开关面板盒，可以在不破坏墙面装修的情况下安装在任意 86 面板盒上，极大的减少了部署成本。配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。NAP-2800-P 产品还集成了以太网口和 IP 电话接口，方便有线终端和电话接入，产品整体设计美观小巧，并且部署便捷，是酒店等环境无线网络建设的最佳选择。

3.1.14. NAP-3500-P

面板式 NAP-3500-P 是信锐专门为酒店客房、宿舍、办公室和医院病房设计的 802.11ac 高性能入墙式面板无线接入点，支持 11ac/a/n 和 11b/g/n 双频并发，最大无线接入速率达 733Mbps。NAP-3500-P 可以在不破坏墙面装修的情况下安装在任意 86 面板盒上，极大的减少了部署成本。配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

NAP-3500-P 产品整体设计美观小巧，并且部署便捷，是酒店等环境无线网络建设的最佳选择。

3.1.15. NAP-3560-P

面板式 NAP-3560-P 是信锐专门为酒店客房、宿舍、办公室和医院病房设计的的 802.11ac

wave 2 高性能入墙式面板无线接入点，内置 2x2 MIMO 天线，支持 802.11a/b/g/n/ac 协议，支持 11ac/a/n 和 11b/g/n 双频并发，最大无线接入速率达 1167Mbps。NAP-3560-P 可以在不破坏墙面装修的情况下安装在任意 86 面板盒上，极大的减少了部署成本。配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

NAP-3560-P 产品还集成了以太网口和 IP 电话接口，方便有线终端和电话接入，产品整体设计美观小巧，并且部署便捷，是酒店等环境无线网络建设的最佳选择。

3.1.16. NAP-3600

信锐 NAP-3600 无线接入点是信锐自主研发的新一代 802.11ac 高性能无线接入点。NAP-3600 内置矩阵 式智能天线，支持 11ac/a/n 和 11b/g/n 双频并发，整机最高速率可达 1166Mbps，可提供更快的无线上网和 更大的无线覆盖范围。产品高达 1Gbps 的最大传输速率能够轻松满足各种无线业务的承载使用，如视频、 语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。 设备采用千兆以太网口上行链路，突破了百兆上行速率的限制，保证无线高速传输；支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐 NAC 系列控制器，为用户带来前所未有 的快速体验和更安全的业务接入。 信锐 NAP-3600 产品外观美观大方，安装方便，适用于吸顶、壁挂以及桌面放装。

3.1.17. NAP-3600（MU）

信锐 NAP-3600(MU)无线接入点是信锐自主研发的新一代 802.11ac wave 2 高性能无线接入点。NAP-3600(MU)内置矩阵式智能天线，支持 11ac/a/n 和 11b/g/n 双频并发，整机最高速率可达 1167Mbps，可提供更快的无线上网和更大的无线覆盖范围。产品高达 1.167Gbps 的最大传输速率能够轻松满足各种无线业务的承载使用，如视频、语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。

设备采用千兆以太网口上行链路，突破了百兆上行速率的限制，保证无线高速传输；支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

信锐 NAP-3600(MU)产品外观美观大方，安装方便，适用于吸顶、壁挂以及桌面放装。

3.1.18. NAP-3600（SD）

信锐 NAP-3600（SD）是信锐自主研发的新一代 802.11ac 集成烟雾传感器应用的物联网 AP。高性能无线接入点 NAP-3600（SD）内置光电式烟雾传感器，NAP-3600（SD）内置矩阵式智能天线，支持 11ac/a/n 和 11b/g/n 双频并发，整机最高速率可达 1167Mbps，可提供更快的无线上网和更大的无线覆盖范围。产品高达 1.167Gbps 的最大传输速率能够轻松满足各种无线业务的承载使用，如视频、语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。

设备采用千兆以太网口上行链路，突破了百兆上行速率的限制，保证无线高速传输；支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

信锐 NAP-3600（SD）产品外观美观大方，安装方便，适用于吸顶、壁挂等。

3.1.19. NAP-3600-P

面板式 NAP-3600-P 是信锐自主研发的新一代 802.11ac 高性能无线接入点，是专门为酒店客房、宿舍、办公室和医院病房设计的 802.11ac 双频面板式无线接入点，内置 2x2 MIMO 天线，支持 802.11a/b/g/n/ac 协议，最大无线接入速率达 1167Mbps，配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。NAP-3600-P 产品还集成了以太网口和 IP 电话接口，方便有线终端和电话接入，产品整体设计美观，并且部署便捷，是酒店等环境无线网络建设的最佳选择。

3.1.20. NAP-3600-P（MU）

面板式 NAP-3600-P(MU)是信锐专门为酒店客房、宿舍、办公室和医院病房设计的的 802.11ac wave 2 高性能入墙式面板无线接入点，内置 2x2 MIMO 天线，支持 802.11a/b/g/n/ac 协议，支持 11ac/a/n 和 11b/g/n 双频并发，最大无线接入速率达 1167Mbps。NAP-3600-P(MU)可以在不破坏墙面装修的情况下安装在任意 86 面板盒上，极大的减少了部署成本。配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

NAP-3600-P(MU)产品还集成了以太网口和 IP 电话接口，方便有线终端和电话接入，产品整体设计美观小巧，并且部署便捷，是酒店等环境无线网络建设的最佳选择。

3.1.21. NAP-3620

信锐 NAP-3620 无线接入点是信锐自主研发的新一代 802.11ac 高性能无线接入点。NAP-3620 内置矩阵式智能天线，支持射频自定义切换，每路射频卡可独立自由切换成任意工作模式：2.4G+5G、2.4G+2.4G、5G+5G 三种模式，整机最高速率可达 1167Mbps，可提供更快的无线上网和更大的无线覆盖范围。产品高达 1.167Gbps 的最大传输速率能够轻松满足各种无线业务的承载使用，如视频、语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。

设备采用千兆以太网口上行链路，突破了百兆上行速率的限制，保证无线高速传输；支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

信锐 NAP-3620 产品外观美观大方，安装方便，适用于吸顶、壁挂以及桌面放装。

3.1.22. NAP-3620（R3）

信锐 NAP-3620(R3)无线接入点是信锐自主研发的新一代三频 802.11ac wave 2 高性能无线接入点。NAP-3620(R3)采用创新的三频设计，加了第三个四流 802.11ac wave2 射频，支持 2.4G、5G、5G 三频并发，整机最高速率可达 3Gbps，可提供更快的无线上网和更高的多用户并发。非常适用于会议室、报告厅、体育馆、会展中心、机场、食堂等高密环境。

设备采用双千兆以太网口，并且双电口同时支持 POE，实现了 POE 备份；支持 USB 接口，能够外接 U 盘以及物联网拓展；支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐 NAC 系列控制器，为用户带来前所未有的更安全、会营销、易管理、更兼容的无线网络。

信锐 NAP-3620(R3)产品外观美观大方，安装方便，适用于吸顶、壁挂以及桌面放装。

3.1.23. NAP-3680

信锐 NAP-3680 功分无线接入点是信锐自主研发的新一代 802.11ac 高性能无线接入点。NAP-3680 支持 8 个射频口，支持 11ac/a/n 和 11b/g/n 双频并发，整机最高速率可达 1167Mbps，可提供更快的无线上网和更大的无线覆盖范围。产品高达 1.167Gbps 的最大传输速率能够轻松满足各种无线业务的承载使用，如视频、语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。

设备采用千兆以太网口上行链路，突破了百兆上行速率的限制，保证无线高速传输；支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐 NAC 系列

控制器，为用户带来前所未有的快速体验和更安全的业务接入。

信锐 NAP-3680 产品外观美观大方，安装方便，适用于各种功分场景。

3.1.24. NAP-3700

信锐 NAP-3700 无线接入点是信锐自主研发的新一代 802.11ac wave 2 高性能无线接入点。NAP-3700 内置矩阵式智能天线，支持 11ac/a/n 和 11b/g/n 双频并发，整机最高速率可达 1267Mbps，可提供更快的无线上网和更大的无线覆盖范围。产品高达 1.267Gbps 的最大传输速率能够轻松满足各种无线业务的承载使用，如视频、语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。

设备采用千兆以太网口上行链路，突破了百兆上行速率的限制，保证无线高速传输；支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

信锐 NAP-3700 产品外观美观大方，安装方便，适用于吸顶、壁挂以及桌面放装。

3.1.25. NAP-3700（D）

信锐 NAP-3700（D）无线接入点是信锐自主研发的新一代 802.11ac wave 2 高性能无线接入点。NAP-3700（D）内置高增益智能定向天线，支持 11ac/a/n 和 11b/g/n 双频并发，整机最高速率可达 1267Mbps，可提供更快的无线上网和更大的无线覆盖范围。产品高达 1.267Gbps 的最大传输速率能够轻松满足各种无线业务的承载使用，如视频、语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。

设备采用千兆以太网口上行链路，突破了百兆上行速率的限制，保证无线高速传输；支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

信锐 NAP-3700（D）产品外观美观大方，安装方便，适用于吸顶、壁挂以及桌面放装。

3.1.26. NAP-4100V

信锐 NAP-4100V 无线接入点是信锐自主研发的新一代 802.11ac 工业级移动车载 AP。

NAP-4100V 移动车载 WiFi 覆盖设备，采用了最新 3G/4G 终端接入方案，支持 4G LTE 全网通（移动/联通/电信），以及采用最新 802.11ac 协议设计，支持 11ac/a/n 和 11b/g/n 双频

并发，整机最高速率可达 1167Mbps，适用车载移动环境下的 3G/4G 转 WiFi 的移动型 WLAN 的部署与构建。

移动车载 AP 高达 1.167Gbps 的最大传输速率能够轻松满足各种无线业务的承载使用，如视频、语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。信锐 NAP-4100V 采用防震、防松脱电源接口设计，支持 ACC 控制上下电，具有冲击防护、接口防松脱、防震等优势，安装方便，适用于抱杆或壁挂安装。

信锐 NAP-4100V 移动车载 WiFi 覆盖设备配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验、丰富的营销广告和更安全的业务接入。

3.1.27. NAP-4600

信锐 NAP-4600 无线接入点是信锐自主研发的新一代 802.11ac 高性能无线接入点。NAP-4600 内置 3x3 MIMO 高增益天线，支持 11ac/a/n 和 11b/g/n 双频并发，整机最高可达 1750Mbps，可提供更快的无线上网和更大的无线覆盖范围。产品高达 1750Mbps 的最大传输速率能够轻松满足各种无线业务的承载使用，如视频、语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。

设备采用千兆以太网口上行链路，突破了百兆上行速率的限制，保证无线高速传输；支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

信锐 NAP-4600 采用吸顶式设计，外观美观大方，安装方便，适用于吸顶部署。

3.1.28. NAP-4650

信锐 NAP-4650 无线接入点是信锐自主研发的新一代 802.11ac 高性能无线接入点。NAP-4650 内置 3x3 MIMO 高增益天线，内置物联网接口，支持 Bluetooth4.1（BLE），支持 iBeacon。支持 USB 接口，结合控制器可用于应用节流。支持 802.11ac/a/n 和 802.11b/g/n 双频并发，整机最高可达 1750Mbps，可提供更快的无线上网和更大的无线覆盖范围。产品高达 1750Mbps 的最大传输速率能够轻松满足各种无线业务的承载使用，如视频、语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。

设备拥有 2 个以太网口，千兆上行链路，突破了百兆上行速率的限制，保证无线高速传输；支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

信锐 NAP-4650 采用吸顶式设计，外观美观大方，安装方便，适用于吸顶部署。

3.1.29. **NAP-5600**

信锐 NAP-5600 无线接入点是信锐自主研发的新一代 802.11ac wave 2 智能无线接入点。NAP-5600 内置 智能天线，支持 11ac/a/n 和 11b/g/n 双频并发，整机最高可达 2.533Gbps，可提供更快的无线上网和更大的无线覆盖范围。产品高达 2.533Gbps 的最大传输速率能够轻松满足各种无线业务的承载使用，如视频、语音等多媒体业务，并提供智能射频、服务质量保证、无缝漫游等。

设备采用双千兆以太网口和一个千兆光口，并且双电口同时支持 POE，实现了 POE 备份；设备内置蓝牙功能，支持蓝牙 BLE；支持 USB 接口，能够外接 U 盘；支持本地供电与 PoE 远程供电，可根据客户现场供电环境进行灵活选择。配合信锐 NAC 系列控制器，为用户带来前所未有的更安全、会营销、易管理、更兼容的无线网络。

信锐 NAP-5600 采用吸顶式设计，外观美观大方，安装方便，适用于吸顶部署。

3.1.30. NAP-7600

信锐 NAP7600 室外无线接入点是信锐自主研发的支持 802.11a/b/g/n 双频并发的室外高速无线接入设备。采用 2x2 MIMO 技术，支持 11a/n 和 11b/g/n 双频并发，整机最高可达 600Mbps。设备采用千兆以太网口上行链路，保证无线高速传输；采用 PoE 远程供电，使网络部署更简单。

NAP-7600 采用了 IP 68 最高防护等级的外壳设计，支持全封闭防水、防潮、防尘以及防火、防晒等，在极端恶劣的室外环境中仍可正常使用，可有效避免室外恶劣天气和环境影响，不管是在潮湿的南方还是寒冷的北方都适用。NAP-7600 还支持点对点及点对多点中继网桥功能，提高了室外组网的方案可行性，配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

NAP-7600 室外无线接入点提供 4 个 N 型外置天线接口，可根据实际环境选择全向或定向外置天线，特别适合部署在风景区、校园、园区等室外环境中。

3.1.31. NAP-7800

信锐 NAP7800 室外无线接入点是信锐自主研发的支持 802.11ac 协议的双频室外高速无线接入设备。采用 2x2 MIMO 技术，支持 11a/n/ac 和 11b/g/n 双频并发，整机最高可达 1167Mbps。设备采用千兆以太网口上行链路，保证无线高速传输；采用 PoE 远程供电，使

网络部署更简单。

NAP-7800 采用了 IP 67 防护等级的外壳设计，支持全封闭防水、防潮、防尘以及防火、防晒等，在极端恶劣的室外环境中仍可正常使用，可有效避免室外恶劣天气和环境影响，不管是在潮湿的南方还是寒冷的北方都适用。NAP-7800 还支持点对点及点对多点中继网桥功能，提高了室外组网的方案可行性，配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

NAP-7800 室外无线接入点提供 4 个 N 型外置天线接口，可根据实际环境选择全向或定向外置天线，特别适合部署在风景区、校园、园区等室外环境中。

3.1.32. NAP-8000

信锐 NAP-8000 室外无线接入点是信锐自主研发的支持 802.11a/b/g/n/ac 的室外高速无线接入设备，采用 3x3 MIMO 技术，整机最高可达 1750Mbps。设备采用千兆电口/光口上行链路，保证无线高速传输；采用 PoE 远程供电，使网络部署更简单。

NAP-8000 采用了 IP 67 最高防护等级的外壳设计，支持全封闭防水、防潮、防尘以及防火、防晒等，在极端恶劣的室外环境中（-40℃-70℃）仍可正常使用，可有效避免室外恶劣天气和环境影响，不管是在潮湿的南方还是寒冷的北方都适用。NAP-8000 还支持点对点及点对多点中继网桥功能，提高了室外组网的方案可行性，配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

NAP-8000 室外无线接入点内置定向天线，同时提供 6 个 N 型外置天线接口，也能够选配外置天线，特别适合部署在风景区、校园、园区等室外环境中。

3.1.33. NAP-8000（L）

信锐 NAP-8000(L)室外无线接入点是信锐自主研发的支持 802.11a/b/g/n/ac 的室外高速无线接入设备，采用 2x2 MIMO 技术，整机最高可达 1167Mbps。设备采用千兆电口/光口上行链路，保证无线高速传输；采用 PoE 远程供电，使网络部署更简单。

NAP-8000(L)采用了 IP 67 最高防护等级的外壳设计，支持全封闭防水、防潮、防尘以及防火、防晒等，在极端恶劣的室外环境中（-40℃-70℃）仍可正常使用，可有效避免室外恶劣天气和环境影响，不管是在潮湿的南方还是寒冷的北方都适用。NAP-8000(L)还支持点对点及点对多点中继网桥功能，提高了室外组网的方案可行性，配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

NAP-8000(L)室外无线接入点内置定向天线，特别适合部署在风景区、校园、园区等室外环境中。

3.1.34. NAP-8100

信锐 NAP-8100 室外无线接入点是信锐自主研发的新一代三频 802.11ac wave 2 高性能室外无线接入点，采用三频八流技术，支持 2.4G、5G、5G 三频并发，支持 MU-MIMO 技术，整机最高可达 3000Mbps。设备采用千兆电口/光口上行链路，保证无线高速传输；采用 PoE 远程供电，蓝牙串口远程调试管理，使网络部署更简单。

NAP-8100 采用了 IP 68 最高防护等级的外壳设计，支持全封闭防水、防潮、防尘以及防火、防晒等，采用低温智能加热技术，在极端恶劣的室外环境中（-40℃-70℃）仍可正常使用，可有效避免室外恶劣天气和环境影响，不管是在潮湿的南方还是寒冷的北方都适用。NAP-8100 还支持点对点及点对多点中继网桥功能，提高了室外组网的方案可行性，配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

NAP-8100 室外无线接入点内置定向天线，无需额外部署外置天线，特别适合部署在风景区、校园、园区等室外环境中。

3.1.35. NAP-8100（L）

信锐 NAP-8100(L)室外无线接入点是信锐自主研发的支持 802.11 ac wave2 的室外高速无线接入设备，支持 MU-MIMO 技术，实现更高的传输效率，整机最高可达 1267Mbps。设备采用千兆电口/光口上行链路，保证无线高速传输；采用 PoE 远程供电，使网络部署更简单。

NAP-8100(L)采用了 IP 68 最高防护等级的外壳设计，支持全封闭防水、防潮、防尘以及防火、防晒等，采用低温智能加热技术，在极端恶劣的室外环境中（-40℃-70℃）仍可正常使用，可有效避免室外恶劣天气和环境影响，不管是在潮湿的南方还是寒冷的北方都适用。NAP-8100(L)还支持点对点及点对多点中继网桥功能，提高了室外组网的方案可行性，配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

NAP-8100(L)室外无线接入点提供 4 个 N 型外置天线接口，特别适合部署在风景区、校园、园区等室外环境中。

3.1.36. NAP-8100（L）-LTE

信锐 NAP-8100(L)-LTE 室外无线接入点是信锐自主研发的支持 802.11 ac wave2 的室外高速无线接入设备，NAP-8100(L)-LTE WiFi 覆盖设备，内置定向天线，采用了最新 3G/4G 终端接入方案，支持 4G LTE 全网通（移动/联通/电信），以及采用最新 802.11ac wave2 协议设计，支持 MU-MIMO 技术，实现更高的传输效率，支持 11ac wave2/a/n 和 11b/g/n 双频并发，整机最高可达 1267Mbps。设备采用千兆电口/光口上行链路，保证无线高速传输，适

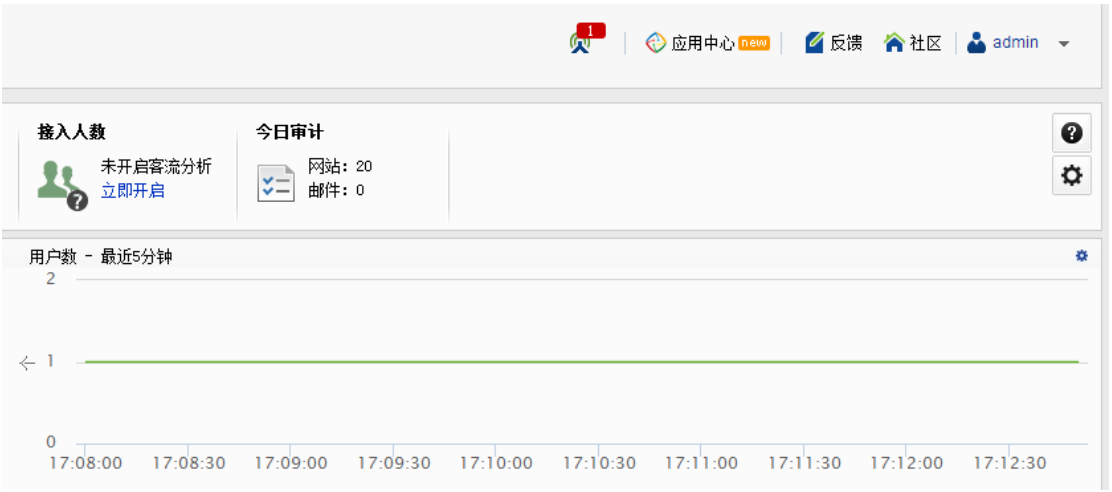
用室外环境或者室外不方便布线环境下的 3G/4G 转 WiFi 的 WLAN 的部署与构建。

NAP-8100(L)-LTE 采用了 IP 68 最高防护等级的外壳设计，支持全封闭防水、防潮、防尘以及防火、防晒等，采用低温智能加热技术，在极端恶劣的室外环境中（-40℃-70℃）仍可正常使用，可有效避免室外恶劣天气和环境影响，不管是在潮湿的南方还是寒冷的北方都适用。NAP-8100(L)-LTE 还支持点对点及点对多点中继网桥功能，提高了室外组网的方案可行性，配合信锐 NAC 系列控制器，为用户带来前所未有的快速体验和更安全的业务接入。

3.2. 部署

3.2.1. NAP 激活

NAP 部署在网络中，会自动发现 NAC，并从 NAC 上下载相应配置，首次使用 NAP，需要激活，激活页面是在 NAP 自动发现 NAC 后，在 NAC 的【接入点配置】→【无线接入点】→【发现新接入点】处进行激活，详细配置，请参考第 4 章第 4.5.4 小节。



提示：在 NAC 控制台的右上角，当有出现图标 

时，表示还有未激活的接入点，需要到【接入点配置】→【无线接入点】处激活

3.2.2. AP 发现 NAC 的原理

3.2.2.1. AP 配置静态 NAC 地址

1、AP 支持静态配置 NAC 的 IP 地址的，如果静态配置了 NAC 的 IP 地址，AP 就会向该 IP 的 NAC 单播发送发现请求报文，该 NAC 发现列表将会出现该 AP 信息。

2、激活 AP 时指定 NAC 的地址

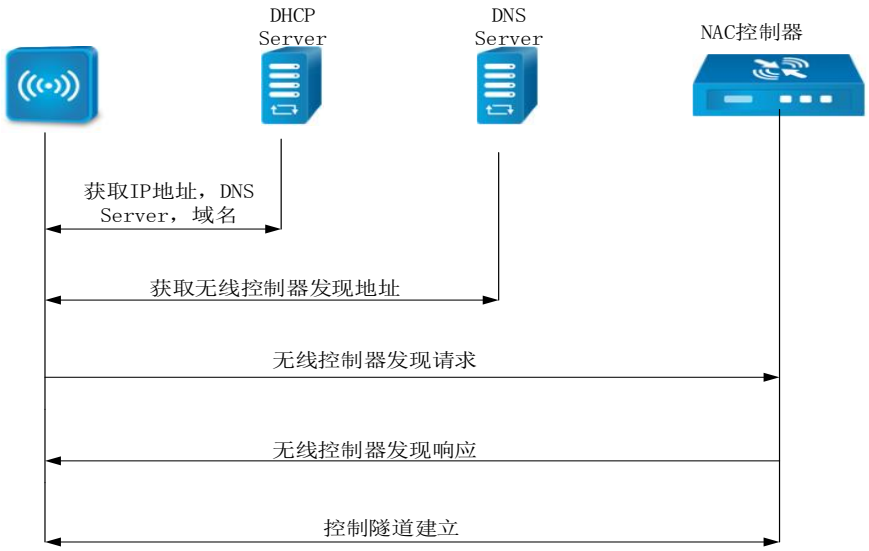
3、静态 IP 发现的应用场景，跨三层网络的状态下这种方式比较快速，因为是直接去发现 NAC。适用于 NAC 的 IP 不会改变的场景。

3.2.2.2. AP 通过 DNS 发现 NAC

1、AP 可通过 DHCP Server 获取 IP 地址，DNS Server 地址。

2、AP 向 DNS Server 发送 DNS 解析请求，DNS Server 在收到 AP 的解析请求后，回复 DNS 解析相应，将域名解析为 NAC 地址 。

3、AP 通过 DHCP 得到 DNS 地址，并通过 DNS 解析域名获取 NAC 地址后被 NAC 发现



4、使用 DNS 域名解析时 AP 的配置，可以手动指定 DNS 服务器，但这台服务器上必须能解析这个域名。

5、DNS 服务器的配置

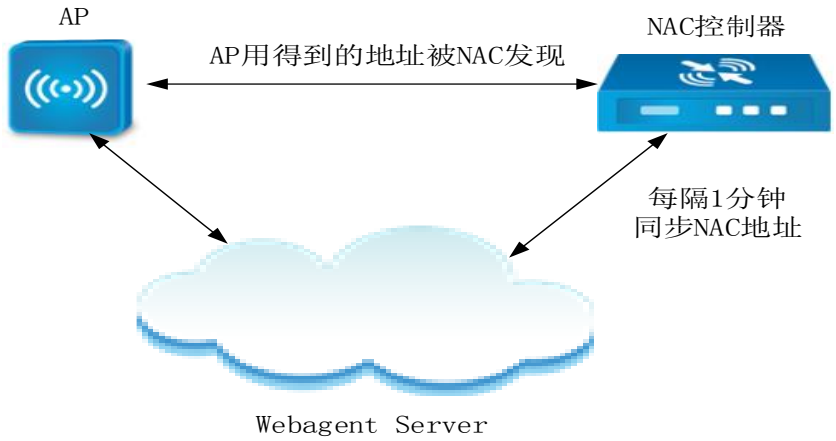
6、DNS 发现的应用场景，因为 DNS 域名容易记住，且这种方式也可以跨三层网络。适用于指导 NAC 域名的情况，不必关心 NAC 的 IP 是否变化。

3.2.2.3. AP 使用 webagent 的方式发现 NAC

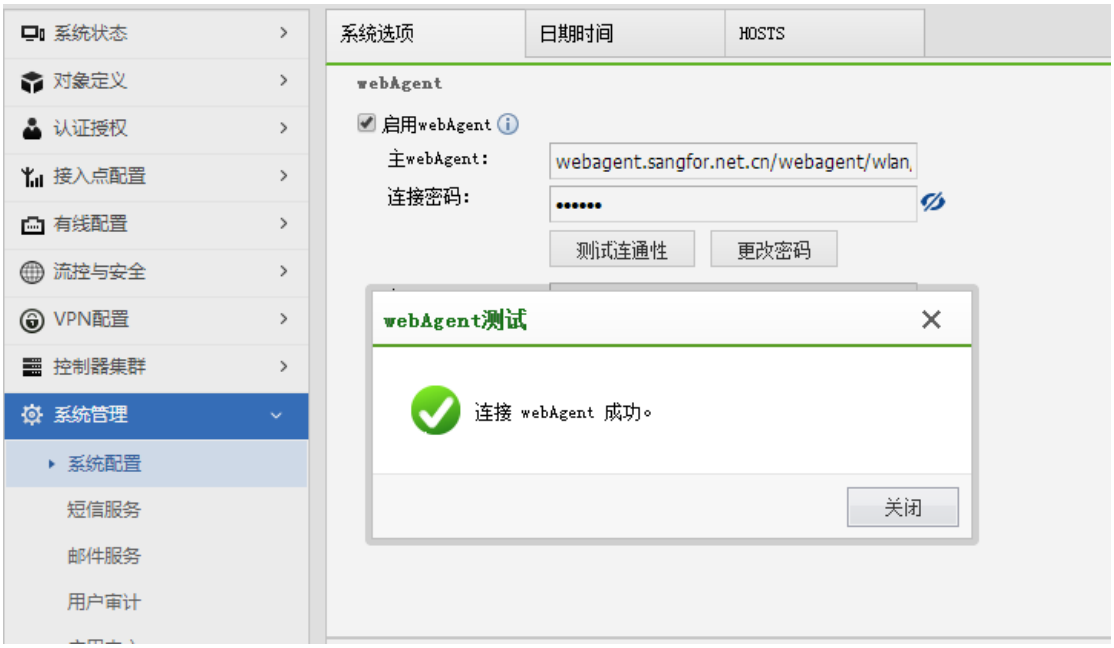
1、当 AP 和 NAC 都关联到同一个 webagent 服务器时，NAC 每隔 1 分钟向 webagent 发

送 get 请求更新 NAC 的出口地址到 webagent。即使 NAC 的地址发生变化，AP 还可以通过 webagent 服务器获取 NAC 的最新地址。本方式适用于 NAC 使用 pppoe 拨号上网时出口地址会发生变化，保证 AP 不会和 NAC 断开连接。

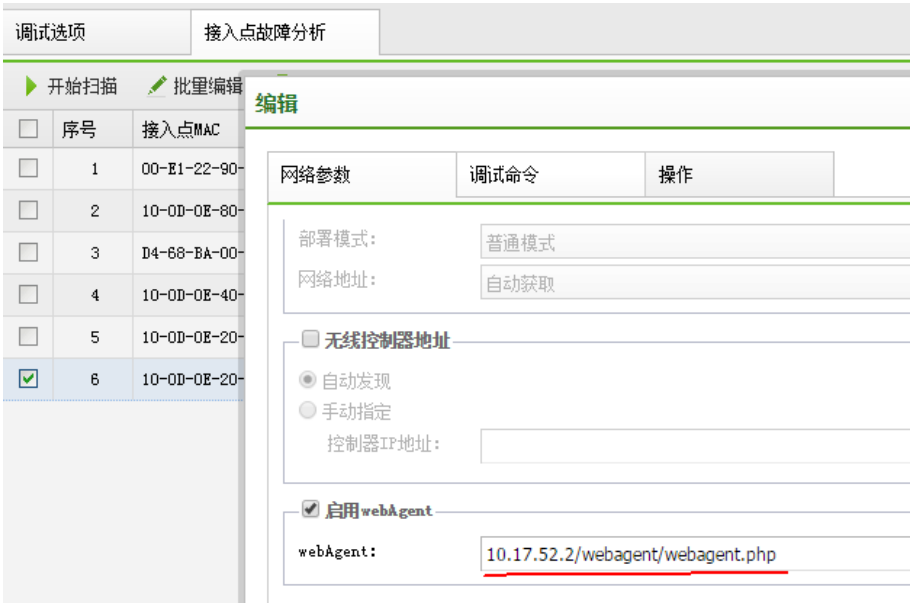
2、使用 webagent 方式发现 NAC 的图解



3、NAC 配置 webagent 界面



4、AP 在调试选项中填写 webagent 的地址 （这里只是提供 AP 发现 NAC 在 webagent 的场景的配置方法）



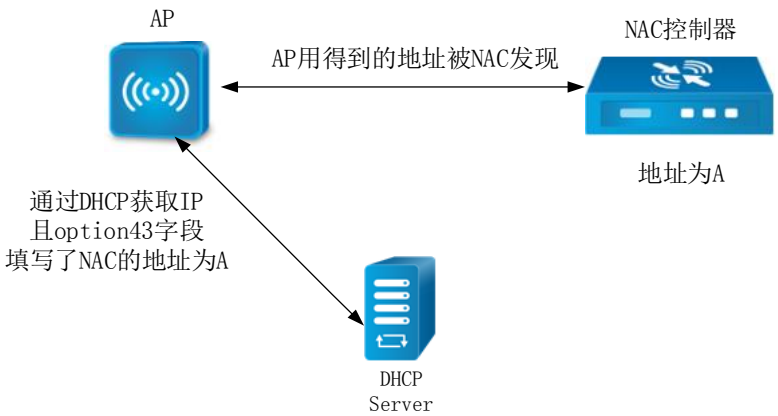
5、webagent 主要适用于 pppoe 拨号上网，因为这种方式下的 IP 会发生改变，有了这种机制就不必人工为 AP 修改 NAC 地址了。也是跨三层网络的。

3.2.2.4. AP 使用 DHCP option43 的方式发现 NAC

1、AP 通过 DHCP Server 获取 IP 地址，Option43 属性（携带 NAC 关联地址）

2、AP 从 Option43 属性中获取 NAC 控制器发现地址，向 NAC 发出单播发现请求

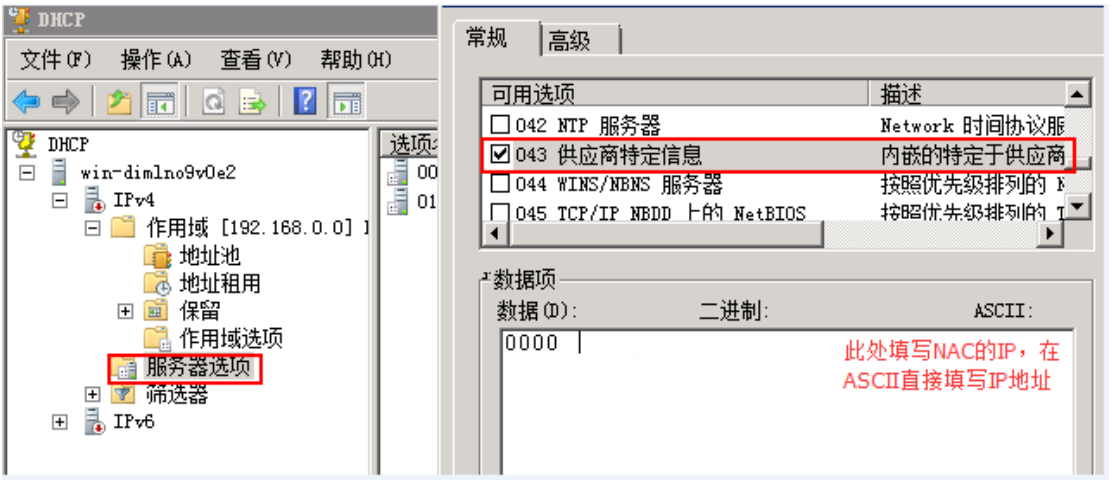
3、AP 通过 option43 字段发现 NAC 的图解



4、使用 NAC 的物理口或者 vlan 作为 dhcp 服务器。值得注意的是 option43 可以配置

NAC 的域名，此时要配置一个可以解析域名的 DNS 服务器地址或者 DHCP 分配的 DNS 上可以解析本域名

5、如果使用独立的 DHCP 服务器时可以如图方式配置



6、DHCP 服务器上 option43 字段的配置

7、生成 option43 字段的工具，下图是此工具的使用方法:

```
D:\zj_share\vs2015\cPlus\option43\Release>option43 192.168.22.1
生成的option43为：030C3139322E3136382E32322E31
```

8、这种方式下 AP 只需设置自动获取 IP 即可，很方便。适用于 AP 接入一个配置了

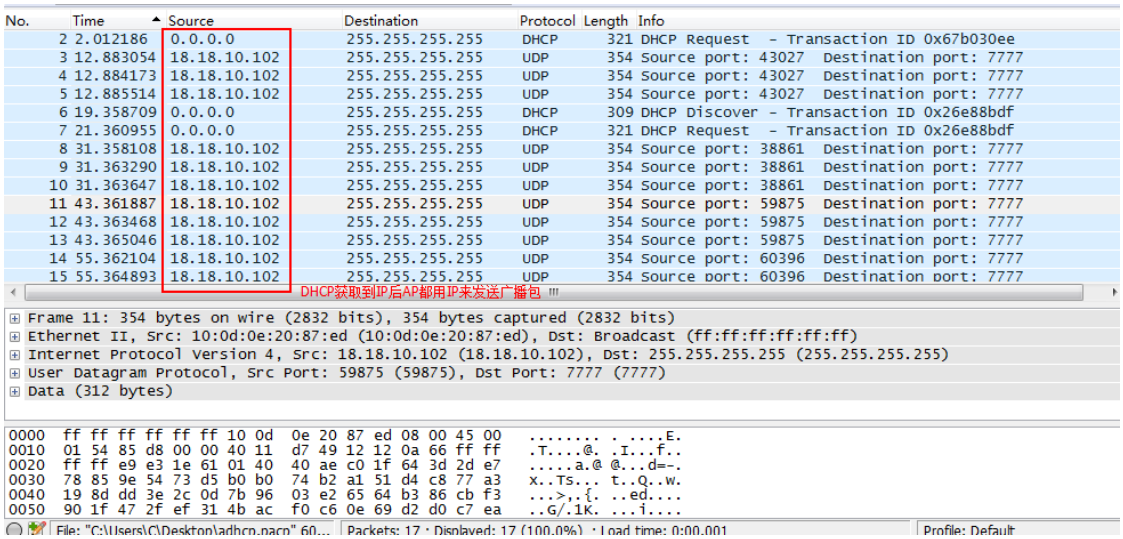
option43 字段的 DHCP 服务器的网络。适用于跨三层网络。

3.2.2.5. AP 通过发送广播发现 NAC

1、当 AP 通过 DHCP Server 获取到 IP 地址后，会通过广播的方式发起 NAC 的发现请求。因为此时 AP 已有 IP，则这个广播可以在三层网络间广播只是三层交换机不会转发这个广播包。理论上讲这也是一个二层网络上的发现方式，它和下面第六种有所区别。

2、广播发现 NAC 的网络拓扑图

3、此时在 NAC 上抓到的包都是有 IP 地址的 AP 发出的

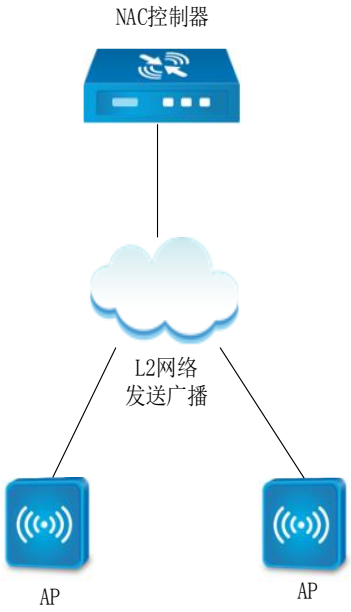


4、这种方式只能在局域网的二层环境下工作，因为此时 AP 有了 IP，所以发送的报文是有源 IP 的。同二层的 NAC 都能发现广播的 AP。

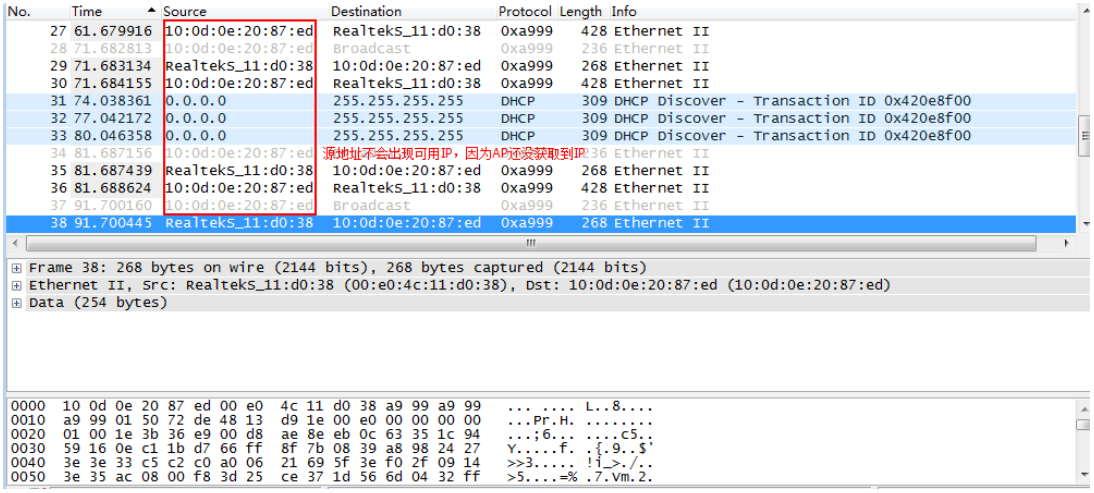
3.2.2.6. AP 通过二层广播发现 NAC

1、当 AP 处于无 IP 的状态，且所处的网络也没有 DHCP 服务器。那么此 AP 将一直没有 IP 地址，因此在二层网络上使用 MAC 地址进行广播。在此种方式下 AP 只能通过二层网络发送广播包去发现 NAC。

2、广播发现 NAC 的网络拓扑图和第五种一样的



3、此时在 NAC 上抓到的包都只显示 AP 的 MAC 地址



4、这种方式也只能在局域网的二层环境工作，因为 AP 还没有获取到 IP，则发送的报文源地址是 MAC。同二层的 NAC 都能发现广播的 AP。

3.2.2.7. 通过 AP 诊断工具发现 NAC

详细内容查看 4.12.5.3 章节。

提示：AP 发现 NAC 的优先级为 静态 IP ＞ DNS 发现 ＞ webagent ＞ DHCP option ＞ 广播 ＞ 二层广播

3.3. 恢复默认配置

在使用 AP 的过程中，AP 的恢复默认配置是很常用的一个步骤，默认的出厂 AP 会主动发起 DHCP 请求获取 IP 地址，并自动搜寻 NAC 接入，所以当遇到以下几种情况时，可以恢复出厂配置。

1、 当发现 AP 网络故障时

2、 给 AP 配置了固定 IP，忘记了 AP 的 IP，AP 连接不上 NAC 时

3、 当 AP 连接没有连接到正确的无线控制器上

4、 其他故障时

方法：AP 上有一个『Reset』按钮，长按 RESET 按钮 5-15 秒，除了 power 灯以外，wlan2g,wlan5g,status 灯都会灭一段时间，然后 AP 会自动热重启，并恢复默认出厂配置。

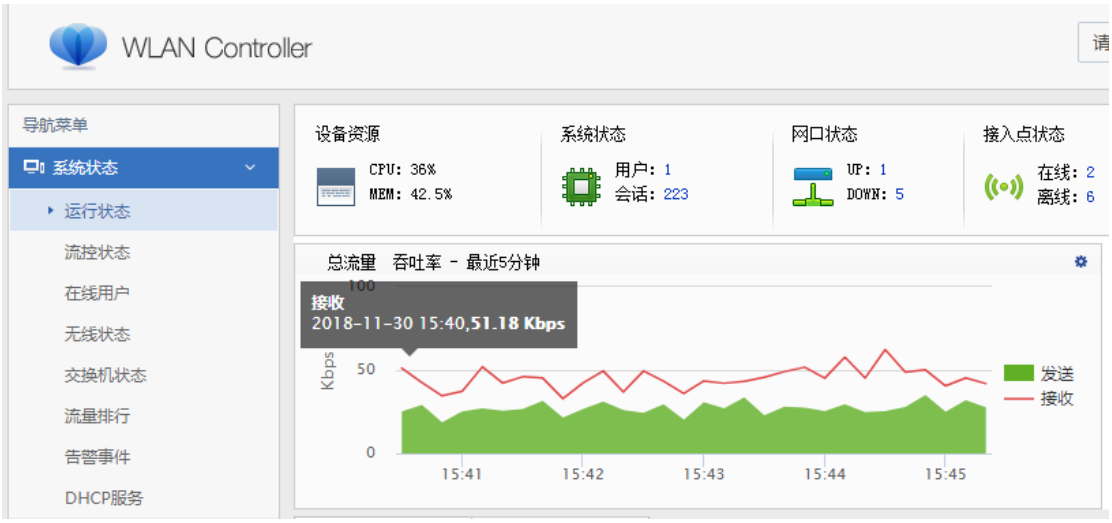
第4章 WLAN 控制器 NAC 功能说明

4.1. WLAN 帮助文档

对于 WLAN 控制器，每个菜单页面的配置页面右上角，设备页面都自带有帮助文档，该配置文档详细的介绍了无线 NAC 各种功能的使用方法以及原理介绍。

4.2. 系统状态

『系统状态』主要用于查看设备的基本状态信息，包括【运行状态】、【流控状态】、【在线用户】、【无线状态】、【交换机状态】、【流量排行】、【告警事件】、【DHCP 服务】。



4.2.1. 运行状态

『运行状态』可以查看设备运行的基本信息，包括 CPU/内存利用率、在线用户、当前会话数、接口信息、接入点状态、无线流量、接口吞吐率、应用流量、用户流量等信息。

4.2.1.1. CPU 和内存使用率

在【运行状态】界面上面可以直接看到 CPU 和内存的使用率以及接口的状态等信息。

在【运行状态】界面下面可以直接看到无线吞吐率的趋势图，以及在线用户的趋势图，还有当前的应用流量与用户流量。

4.2.1.2. 应用流量

在【运行状态】界面下方可以点击“展开”  ，详细的查看无线用户的详细应用流量和用户流量

应用流量 | 用户流量 | 收起

立即刷新

应用名称	应用类型	用户数	发送	接收	总流速	所占百分比
豆瓣网[浏览]	豆瓣网	1	81.57 Kbps	5.65 Mbps	5.73 Mbps	27.44 %
HTTP_GET	访问网站	23	242.80 Kbps	3.66 Mbps	3.90 Mbps	18.67 %
多线程下载	下载工具	3	43.75 Kbps	2.80 Mbps	2.84 Mbps	13.61 %
移动QQ音乐	音频视频	2	86.20 Kbps	2.66 Mbps	2.74 Mbps	13.11 %
360云盘[上传]	360云盘	1	1.09 Mbps	31.62 Kbps	1.12 Mbps	5.36 %
亚马逊	购物支付	4	1,016.34 Kbps	34.85 Kbps	1.03 Mbps	4.91 %
smtp发送邮件	邮件	1	879.48 Kbps	26.34 Kbps	905.81 Kbps	4.23 %
腾讯视频	Web流媒体	1	18.19 Kbps	671.09 Kbps	689.28 Kbps	3.22 %
其他网页论坛[网站浏览]	其他网页论坛	2	29.15 Kbps	528.48 Kbps	557.63 Kbps	2.61 %
SSL	网络协议	15	289.04 Kbps	80.81 Kbps	369.85 Kbps	1.73 %

点击应用流量下面的应用名称，还可以查看该应用流量的趋势图，可以选择 5 分钟，1 小时，最近 1 天，最近一周的该流量趋势图，便于掌握流量趋势情况，规划流控策略使用。选择方法如下图所示：

点击用户数，还可以看到当前应用流量的用户组成情况，如下图：

用户名	所属组	IP地址	发送	接收	总速率↓
74769	/sangforradius/	10.10.28.142	163.19 Kbps	16.44 Mbps	16.60 Mbps
69802	/sangforradius/	10.10.16.119	94.64 Kbps	4.90 Mbps	4.99 Mbps
91752	/sangforradius/	10.10.16.245	77.38 Kbps	633.10 Kbps	710.48 Kbps
87974	/sangforradius/	10.10.16.163	131.36 Kbps	141.98 Kbps	273.34 Kbps
81656	/sangforradius/	10.10.20.46	10.90 Kbps	260.35 Kbps	271.25 Kbps
B0-9F-BA-91-BC…	/PSK认证组/	10.10.26.213	38.50 Kbps	136.70 Kbps	175.20 Kbps
43204	/sangforradius/	10.10.16.160	11.06 Kbps	154.70 Kbps	165.77 Kbps
82348	/sangforradius/	10.10.22.134	5.58 Kbps	126.88 Kbps	132.45 Kbps
25055	/sangforradius/	10.10.16.151	6.06 Kbps	88.64 Kbps	94.70 Kbps
28063	/sangforradius/	10.10.28.61	4.93 Kbps	80.81 Kbps	85.74 Kbps

4.2.1.3. 用户流量

在【运行状态】页面底下还可以看到用户流量状况，当前哪些用户占用流量较多，默认依次按流量百分比从上到下进行排列，界面如下图：

应用流量 | 用户流量

立即刷新

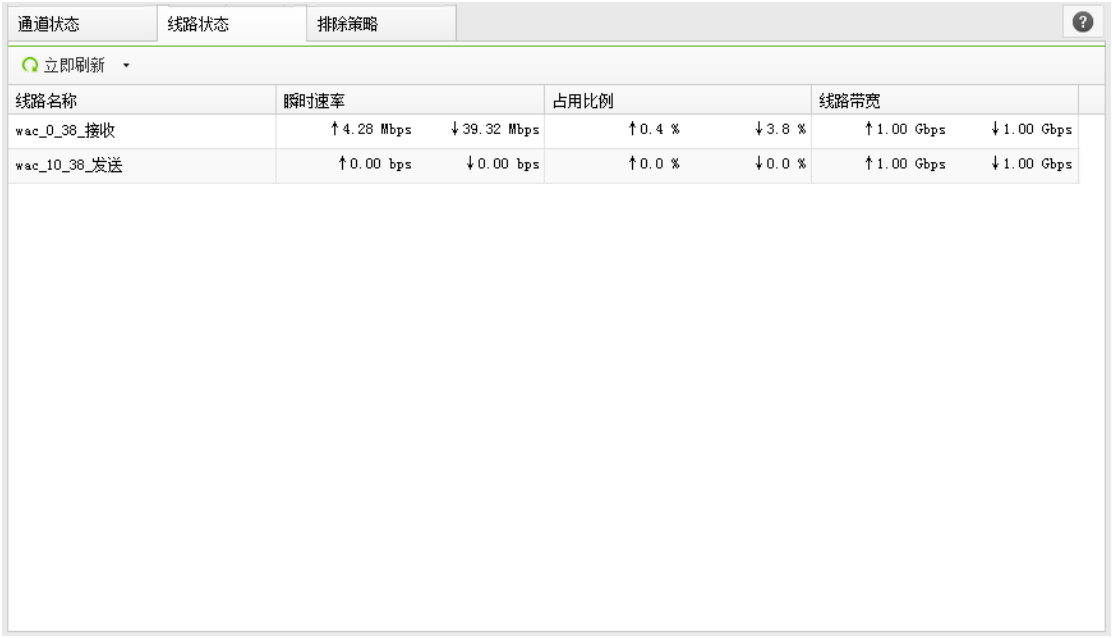
用户名	所属组	应用	IP地址	发送	接收	总流速	所占百分比
12519	/sangforradius/	QQ接收文件, HTTP_P…	10.10.16.143	590.91 Kbps	19.22 Mbps	19.80 Mbps	43.26 %
74769	/sangforradius/	HTTP_GET	10.10.28.142	78.48 Kbps	8.74 Mbps	8.81 Mbps	19.26 %
F8-A4-5F-…	/PSK认证组/	搜狐影音, HTTP_GET	10.10.17.201	388.40 Kbps	6.11 Mbps	6.49 Mbps	14.18 %
68634	/sangforradius/	天天动听, DNS协议	10.10.28.51	84.16 Kbps	1.45 Mbps	1.53 Mbps	3.35 %
48444	/sangforradius/	HTTP_GET, DNS协议, QQ	10.10.16.239	174.45 Kbps	1.04 Mbps	1.21 Mbps	2.65 %
44966	/sangforradius/	QQ传文件, QQ	10.10.26.7	1.08 Mbps	77.01 Kbps	1.16 Mbps	2.53 %
80402	/sangforradius/	QQ空间[浏览], DNS…	10.10.20.159	109.33 Kbps	988.08 Kbps	1.07 Mbps	2.34 %
28432	/sangforradius/	Lotus Notes, HTTP_…	10.10.16.155	73.54 Kbps	865.34 Kbps	938.88 Kbps	2.00 %
69802	/sangforradius/	HTTP_GET, 新浪微博…	10.10.16.119	39.88 Kbps	587.52 Kbps	627.41 Kbps	1.34 %
93013	/sangforradius/	腾讯视频, 移动QQ	10.10.18.196	5.02 Kbps	492.31 Kbps	497.34 Kbps	1.06 %

4.2.2. 流控状态

流控状态包含了【通道状态】、【线路状态】、【排除策略】，如下图显示，其中通道状态显示了流控通道配置后，每条通道的实时运行状态与当前配置。

通道名称	线路	瞬时速率	占用比例	用…	保证带宽	最大带宽	优…
1楼	wac_0_38…	↑403.96… ↓5.19 M…	↑0.0 % ↓0.5 %	18	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	中
2楼	wac_0_38…	↑119.79… ↓325.75…	↑0.0 % ↓0.0 %	10	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	中
3楼	wac_0_38…	↑755.43… ↓844.93…	↑0.1 % ↓0.1 %	11	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	中
4楼	wac_0_38…	↑330.87… ↓4.55 M…	↑0.0 % ↓0.4 %	13	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	中
5楼	wac_0_38…	↑61.77 … ↓50.94 …	↑0.0 % ↓0.0 %	8	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	高
6楼	wac_0_38…	↑31.93 … ↓26.23 …	↑0.0 % ↓0.0 %	3	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	中
7楼	wac_0_38…	↑2.26 M… ↓22.04 …	↑0.2 % ↓2.2 %	18	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	中
8楼	wac_0_38…	↑81.52 … ↓266.44…	↑0.0 % ↓0.0 %	9	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	中
楼顶	wac_0_38…	↑0.00 bps ↓0.00 bps	↑0.0 % ↓0.0 %	0	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	中
默认通道	wac_0_38…	↑62.00 … ↓493.13…	↑0.0 % ↓0.0 %	10	↑0.00 Kbps ↓0.00 Kbps	↑1.00 Gbps ↓1.00 Gbps	低
默认通道	wac_10_3…	↑0.00 bps ↓0.00 bps	↑0.0 % ↓0.0 %	0	↑0.00 Kbps ↓0.00 Kbps	↑1.00 Gbps ↓1.00 Gbps	低

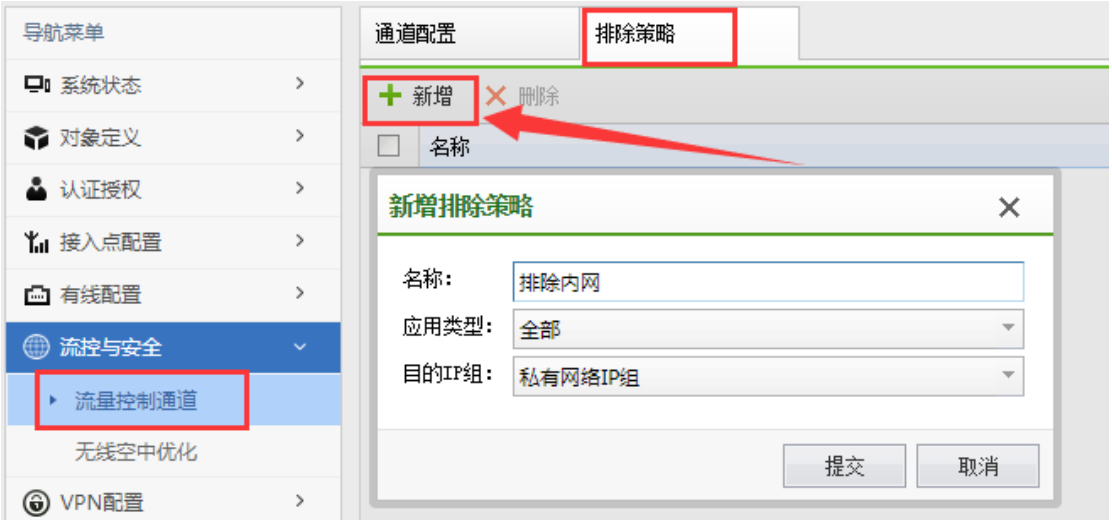
线路状态显示了每条线路的当前流量瞬时速率、线路占用比率，和线路带宽。线路状态是需要在【有线配置】-【线路带宽】根据实际线路情况提前配置并调用，才能在此处正常显示。



线路名称	瞬时速率		占用比例		线路带宽	
wac_0_38_接收	↑4.28 Mbps	↓39.32 Mbps	↑0.4 %	↓3.8 %	↑1.00 Gbps	↓1.00 Gbps
wac_10_38_发送	↑0.00 bps	↓0.00 bps	↑0.0 %	↓0.0 %	↑1.00 Gbps	↓1.00 Gbps

排除策略显示了在流控功能中，不受流控策略限制的流量状态，需要在【流控与安全】

-【流量控制通道】中添加排除策略，才可在此查看到。

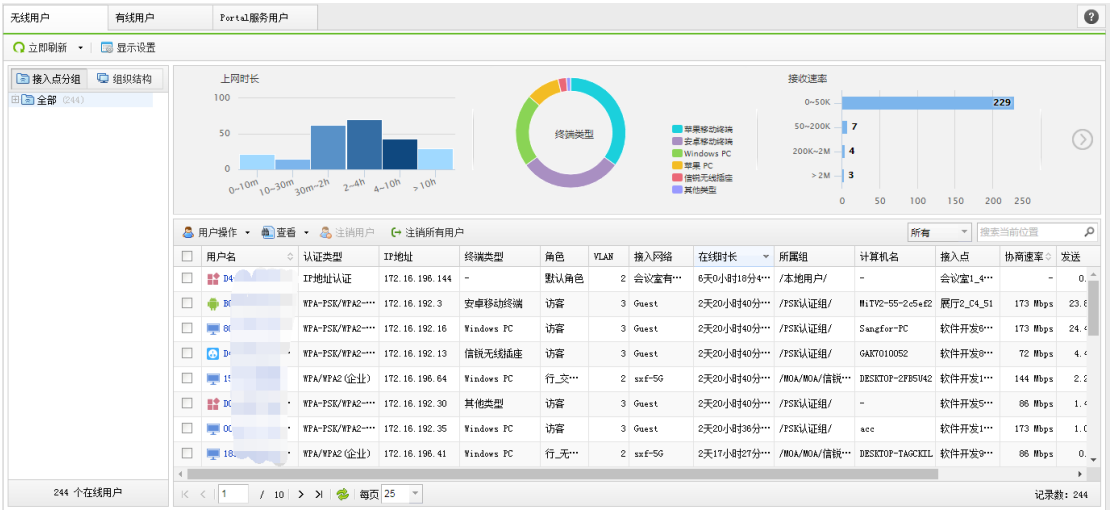


4.2.3. 在线用户

在线用户，可以看到当前接入网络的无线用户信息、有线用户信息以及 portal 服务用户信息。无线用户可以查看到用户名、所属组、认证方式、计算机名、IP 地址、角色、VLAN、接入网络、协商速率、发送、接收、在线时长、MAC 地址、无线协议、信道号、误码率、

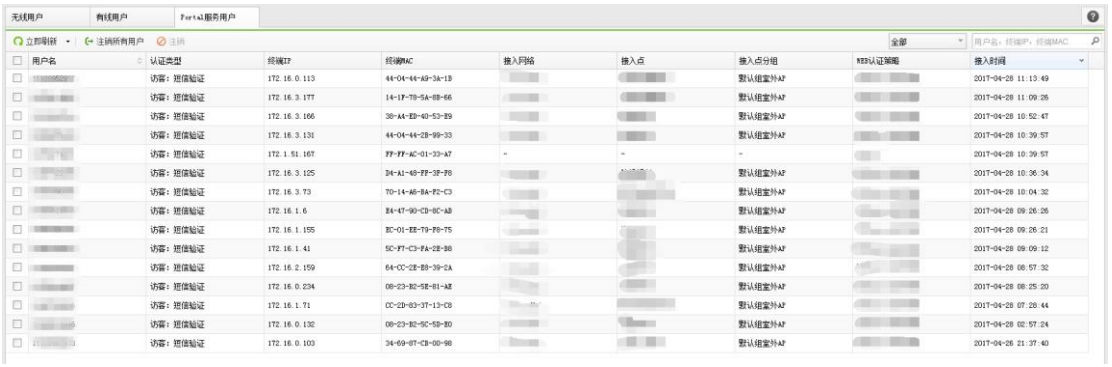
重传率、信号强度等各种详细信息。

无线用户除了以组织结构查看外，还支持以接入点分组的方式查看无线用户信息，如下图：



有线用户基本信息，可以查看到有线状态下的用户基本信息。包括用户名、IP 地址，收发流量，在线时长等信息。

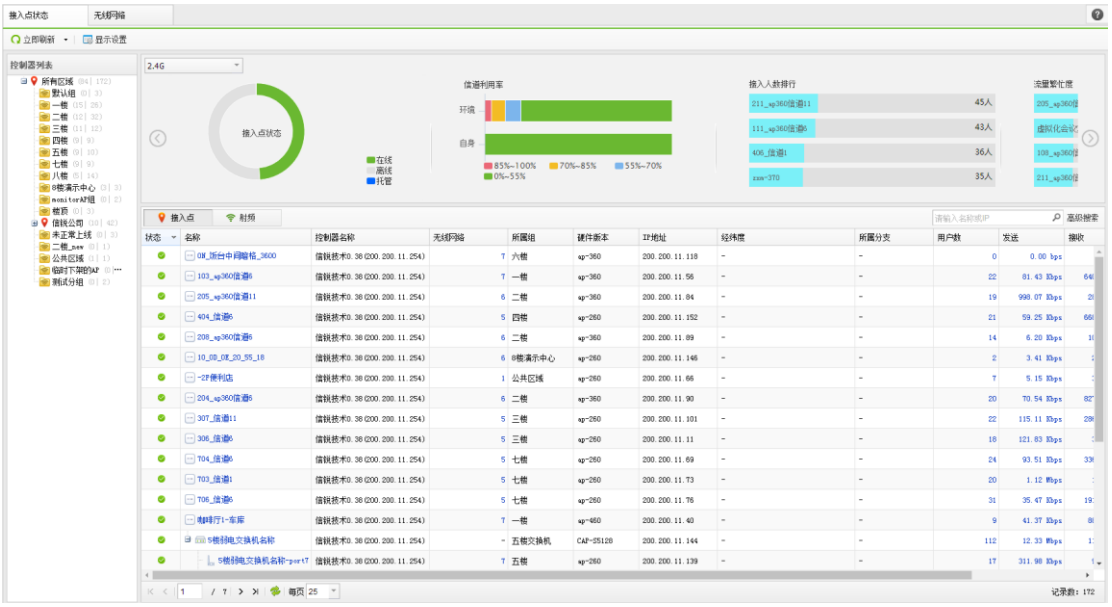
portal 服务用户信息，控制器做为 Portal 服务器，显示在 Portal 服务器上完成认证的用户。



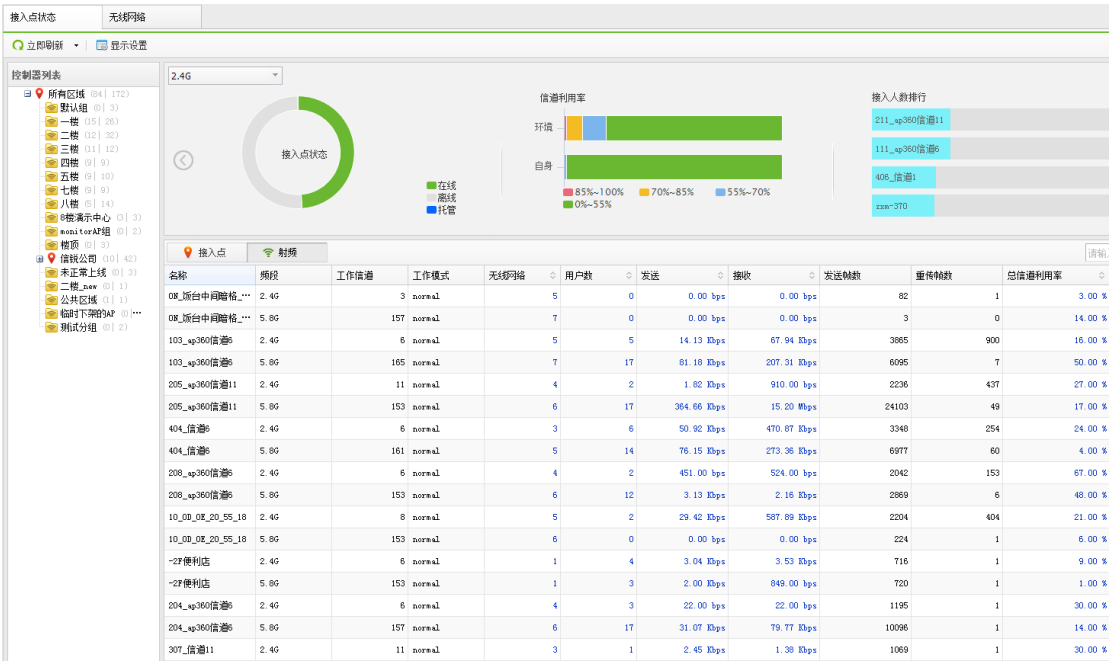
4.2.4. 无线状态

4.2.4.1. 接入点状态

在【接入点状态】中可以看到各个接入点的名称，在线状态，IP 地址，无线网络个数，用户数，流量接收、发送等基本信息



点击【射频】还可以看到每个 AP 的工作频段、工作信道、AP 承载的无线网络数量、信道利用率、噪声值、无线协议、重传率、误码率等信息。



点击【发送】或【接收】下面的数据，可以看到当前 AP 详细的上下行流量，还可以选择【最近 5 分钟】、【最近 1 小时】、【最近一天】、【最近一周】的流量图。

信道利用率：信道利用率数值代表信道的繁忙程度，信道利用率越低体验越稳定。

噪声值：指无线网络频率范围内的辐射电磁干扰。噪声问题容易引发无线数据帧的丢包及误码，如果一个接入点所处的位置噪声值比较高，严重影响数据传输，应考虑更换部署地点或清除干扰源。

无线协议：无线接入点的无线网络协议，例如无线网络协议，2.4G 支持 802.11b/g/n，5.8G 支持 802.11a/n/ac。

重传率：重传率越高，代表无线网络数据的丢包越严重。

误码率：误码率（BER：bit error ratio）是衡量数据在规定时间内数据传输精确性的指标。在无线数据通信中，如果发送的信号是"1"，而接收到的信号却是"0"，这就是"误码"，也就是发生了一个差错。在一定时间内收到的数字信号中发生差错的比特数与同一时间所收到的数字信号的总比特数之比,就叫做"误码率"。噪声、交流电或闪电造成的脉冲、传输设备

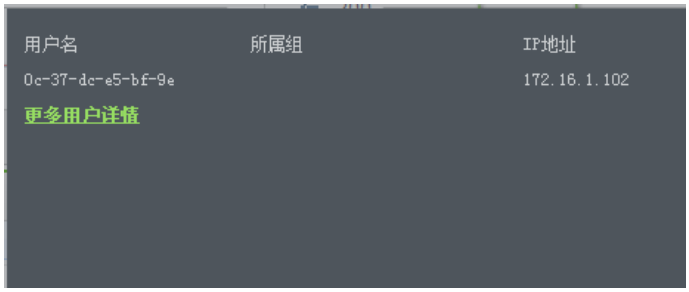
故障及其他因素都会导致误码。

4.2.4.2. 无线网络

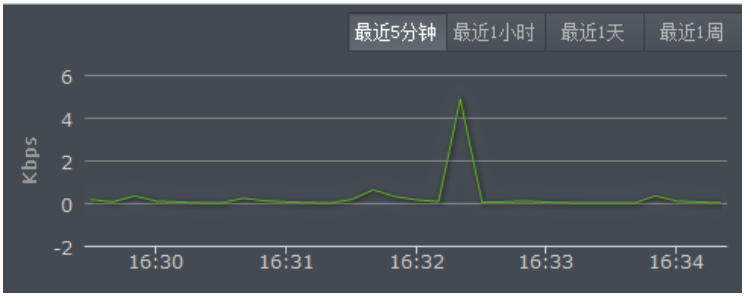
在【无线网络】中可以看到所有的无线网络情况，包括每个网络包含的接入点 AP 数量，当前网络的接入用户数，当前网络的发送和接收流量统计。

点击接入点，用户数，以及发送或接收可以看到相应的数据，比如点击接入点，就可以跳入到该网络所有接入点列表。

点击【用户数】时，就可以看到当前接入的用户的用户名，所属组，IP 地址信息。



点击【接收】或【发送】就可以看到当前网络【最近 5 分钟】、【最近 1 小时】、【最近 1 天】、【最近 1 周】的流量情况：



4.2.5. 交换机状态

显示交换机的运行状态，可查看交换机的在线状态、负载以及端口状态。可以通过交换机面板图看出来，交换机每个口的 Link/Act，PoE 供电状态。点击具体的某个口，可以看到端口的详情，包括 VLAN 和 PoE 的配置信息，以及流量趋势，端口收发包情况。

单独点击交换机名称可以查看交换机配置信息。

【普通模式】可以查看交换机的所属组、MAC 地址、管理 IP、描述、控制器、序列号、射频天线数、软件版本、硬件版本、管理 VLAN、交换机日志、整机吞吐。

4.2.6. 流量排行

【应用流量】排行可以查看所有用户的应用流量情况，依次按百分比从大到下排行，并显示该应用的用户数，与上下行流速，情况如下图，此功能的分析可以用于优化【流控与安全】中的流量控制策略。

序号	应用名称	应用类型	用户数	上行流速	下行流速	总流速	所占百分比
1	HTTP_GET	访问网站	20	358.70 Kbps	4.07 Mbps	4.42 Mbps	44.34 %
2	亚马逊	购物支付	2	1.31 Mbps	62.27 Kbps	1.37 Mbps	13.80 %
3	多线程下载	下载工具	4	23.27 Kbps	930.44 Kbps	953.71 Kbps	9.35 %
4	360云盘[上传]	360云盘	1	847.59 Kbps	22.90 Kbps	870.48 Kbps	8.53 %
5	腾讯视频	Web流媒体	1	16.42 Kbps	627.96 Kbps	644.38 Kbps	6.32 %
6	SSL	网络协议	16	399.30 Kbps	94.88 Kbps	494.18 Kbps	4.84 %
7	中国网络电视	P2P流媒体	1	336.30 Kbps	62.10 Kbps	398.40 Kbps	3.91 %
8	PPStream	P2P流媒体	1	239.32 Kbps	17.38 Kbps	256.70 Kbps	2.52 %
9	iCloud	网络存储	3	157.77 Kbps	56.21 Kbps	213.98 Kbps	2.10 %
10	HTTP_POST	HTTP_POST	10	53.82 Kbps	27.49 Kbps	81.31 Kbps	0.80 %
11	有道云笔记	网络存储	2	14.82 Kbps	33.63 Kbps	48.45 Kbps	0.47 %
12	DNS协议	DNS	44	18.82 Kbps	24.96 Kbps	43.78 Kbps	0.43 %
13	Microsoft ...	软件更新	1	1.82 Kbps	29.22 Kbps	31.04 Kbps	0.30 %
14	QQ	IM	17	6.57 Kbps	23.02 Kbps	29.59 Kbps	0.29 %

点击应用流量下面的应用名称，还可以查看该应用流量的趋势图，可以选择 5 分钟，1 小时，最近 1 天，最近一周的该流量趋势图，便于掌握流量趋势情况，规划流控策略使用。选择方法如下图所示：

【用户流量排行】可以看到用户流量状况，当前哪些用户占用流量较多，默认依次按流量百分比从上到下进行排列，界面如下图，此功能的分析可以用于优化【流控与安全】中的流量控制策略。

序号	用户名	IP地址	所属组	应用名称	上行流速	下行流速	总流速	所占百分比
1	31438	10.10.28.122	/sangforradius/	多线程下载, 豆瓣网[…	117.27 Kbps	2.13 Mbps	2.25 Mbps	22.74 %
2	18873	10.10.26.158	/sangforradius/	中国网络电视, QQ, HTT…	104.75 Kbps	1.38 Mbps	1.48 Mbps	14.97 %
3	35094	10.10.20.133	/sangforradius/	360云盘[上传], HTTP_…	953.73 Kbps	28.93 Kbps	982.66 Kbps	9.70 %
4	90957	10.10.17.67	/sangforradius/	多线程下载, HTTP_GET…	40.35 Kbps	717.11 Kbps	757.46 Kbps	7.48 %
5	45928	10.10.22.138	/sangforradius/	亚马逊	707.41 Kbps	18.69 Kbps	726.10 Kbps	7.17 %
6	C0-18-85-50-94…	10.10.16.24	/PSK认证组/	腾讯视频, HTTP_GET, QQ	19.70 Kbps	683.61 Kbps	703.30 Kbps	6.94 %
7	00-87-46-0F-61…	10.10.20.11	/PSK认证组/	HTTP_GET, HTTP_POST,…	43.17 Kbps	407.74 Kbps	450.91 Kbps	4.45 %
8	10207	10.10.30.203	/sangforradius/	HTTP_GET, 微信传文件…	38.37 Kbps	329.46 Kbps	367.83 Kbps	3.63 %
9	18-59-36-89-25…	10.10.30.15	/PSK认证组/	淘宝天猫, HTTP_GET, D…	29.29 Kbps	306.20 Kbps	335.49 Kbps	3.31 %
10	86840	10.10.18.13	/sangforradius/	移动QQ, Apple数据, SS…	50.91 Kbps	204.78 Kbps	255.69 Kbps	2.52 %
11	38584	10.10.20.33	/sangforradius/	iCloud, SSL, DNS协议	129.74 Kbps	102.09 Kbps	231.84 Kbps	2.29 %
12	B8-EE-65-20-31…	10.10.31.20	/PSK认证组/	PPStream	214.92 Kbps	15.45 Kbps	230.38 Kbps	2.27 %
13	D4-F4-6F-64-39…	10.10.18.188	/PSK认证组/	SSL	219.58 Kbps	8.33 Kbps	227.91 Kbps	2.25 %
14	B8-78-2E-BD-0E…	10.10.24.84	/PSK认证组/	亚马逊, 微信, DNS协议	178.66 Kbps	22.65 Kbps	201.30 Kbps	1.99 %

4.2.7. 告警事件

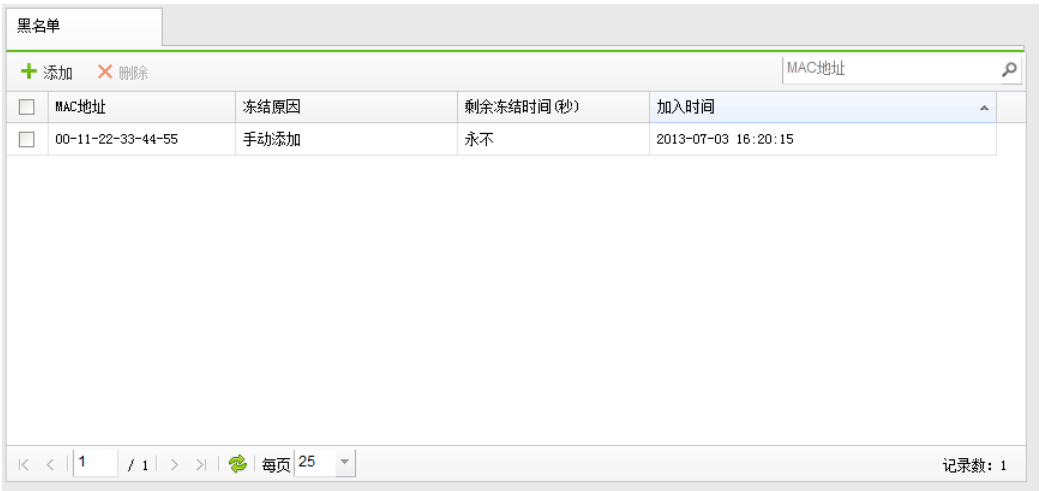
当设备运行时，会自动产生有告警事件、比如网口断开与连接情况，双机切换，AP 断开，钓鱼 AP 等告警信息会在这里显示，显示日志是为了让管理员知道最近设备运行状况，

是否有异常信息，可以到这里查询告警事件列表。

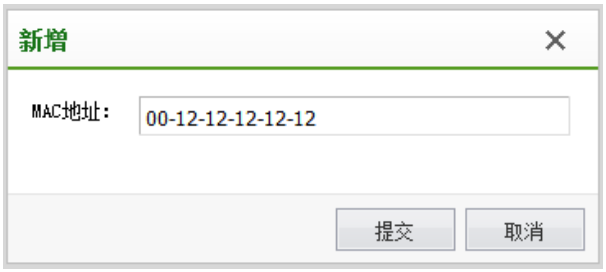
4.2.8. 黑名单

可以手动添加黑名单，以阻止指定的 MAC 地址终端连接有线和无线网络。

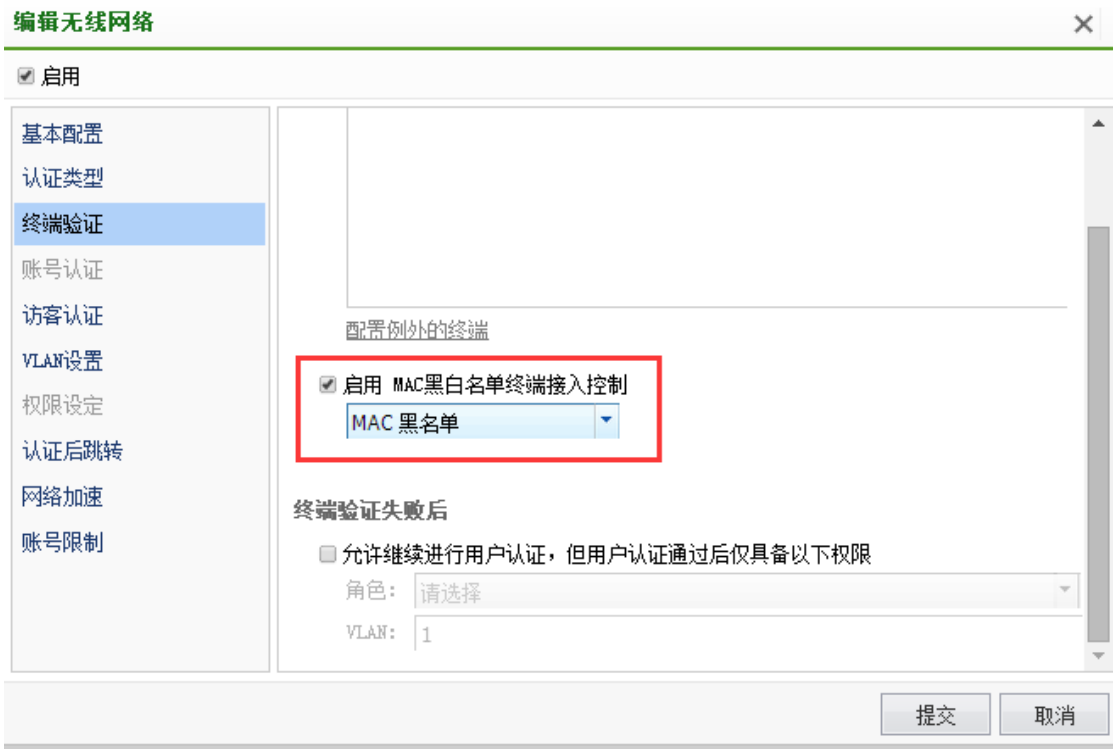
当终端进行暴破登录或者其它恶意攻击行为时，系统会将此终端的 MAC 地址加入黑名单，拒绝一段时间内该终端的连接请求。由终端类型绑定策略触发的非指定类型终端接入，系统也会将此终端 MAC 地址加入黑名单并拒绝该终端的连接请求，限制时间随策略而定。



点击【新增】菜单，添加 MAC 地址：



需要黑名单生效，需要在编辑无线网络中，终端验证下面，启用 MAC 黑名单功能，MAC 黑名单才能正常生效。



4.2.9. DHCP 服务

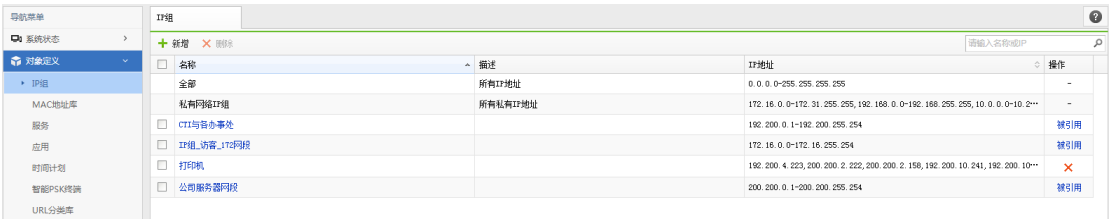
该页面可以观察到 NAC 作为 DHCP 服务器时，对外分配 IP 地址的分配情况：包括了 IP 地址、计算机名、MAC 地址、获取租约时间，租约过期时间：

4.3. 对象定义

『对象定义』用于配置【IP 组】、【MAC 地址库】、【服务】、【应用】、【时间计划】、【智能 PSK 终端】、【URL 分类库】、【终端类型库】。这里定义的对象，在后续的模块中会使用到，比如 IP 组和服务会应用到访问控制策略中，MAC 地址库将在使用 MAC 地址认证时黑白名单调用。

4.3.1. IP 组

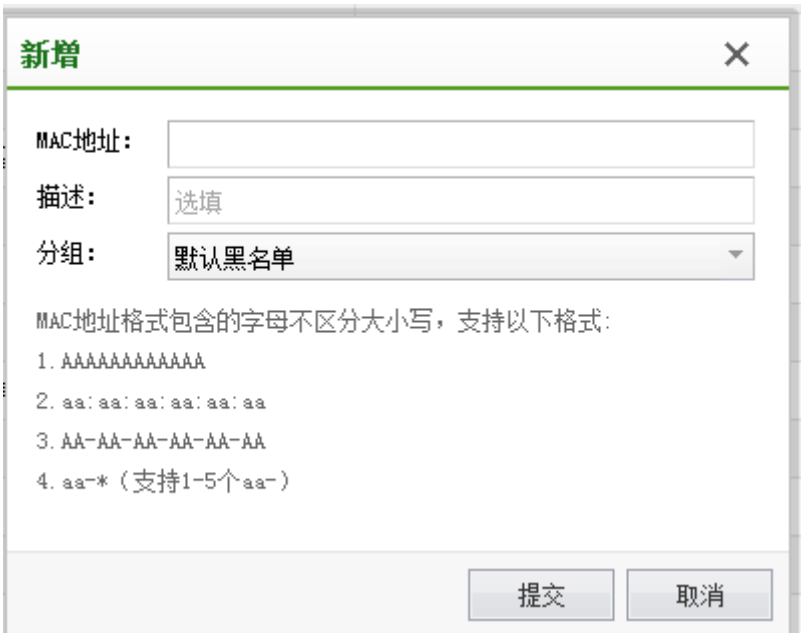
此页面可查看和新增 IP 组，IP 组用于后续【角色授权】中的【访问控制策略】，以及后续的【网络配置】中的【地址转换】。



4.3.2. MAC 地址库

将一个、多个 MAC 地址划分为一个 MAC 组，以便在系统的其它功能中调用，例如 web 免认证。

默认有默认黑名单和默认白名单两个分组，用户可以自定义分组。



4.3.3. 服务

『服务』分为【预定义服务】、【自定义服务】和【服务组】，服务组是【预定义服

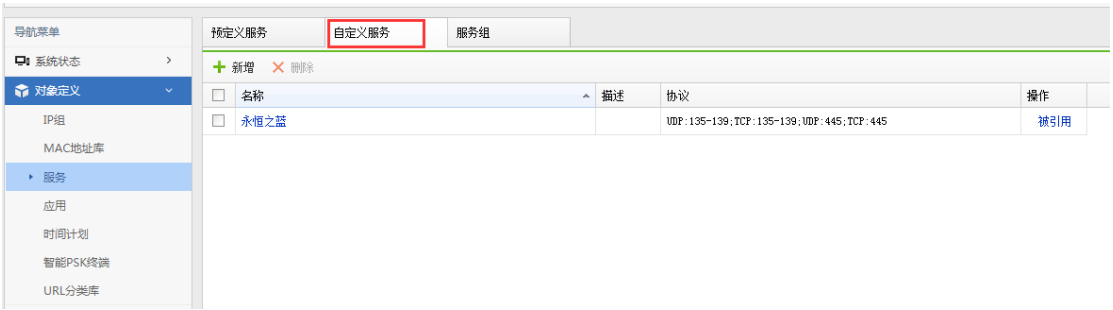
务】或【自定义服务】或 2 者的组合。用于后续【角色授权】中的【访问控制策略】。

4.3.3.1. 预定定义服务

【预定义服务】包括了 TCP，UDP 协议中各种常用端口号包含的应用协议，比如 BGP，DHCP、DNS、HTTP、FTP、SNMP、SSH 等。

4.3.3.2. 自定义服务

【自定义服务】可以让客户自定义所有需的不在预定义范围内的服务，比如客户自己的一些 C/S 架构的 OA 系统所使用的特殊端口号，都可以在这里自定义配置，配置界面如下：



4.3.3.3. 服务组

【服务组】就是【预定义服务】和【自定义服务】的组合，便于做复杂的控制策略时方便调用。而且可以节省原本需要多条控制策略的条数。

4.3.4. 应用

『应用』包括：【应用特征识别库】、【应用智能识别库】、【自定义应用】三类，网络应用流经无线控制器时，可通过特征，识别其应用类型，识别后，即可对连接进行基于应用策略控制、资源调度及流量审计。

4.3.4.1. 应用特征识别库

【应用特征识别库】中记录着应用的字节流特征，通过持续不断的收集及更新，保证应用识别的正确性，应用特征识别库升级需要序列号授权，过期后无法更新。

4.3.4.2. 应用智能识别库

某些类型的网络应用没有固定的字节流特征，需要通过智能的方式识别流量间

的关联性等来识别出其类型，应用智能识别库目前只支持 P2P 行为，支持灵敏度、排除端口的设置。

4.3.4.3. 自定义应用

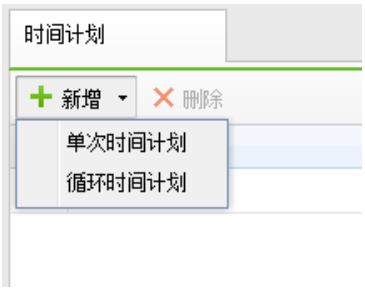
内网应用往往由于其私有性，应用特征识别库无法收集其网络流特征，可以将数据包方向、协议类型、IP 地址、端口号及域名作为应用的规则特征，自定义某种类型的应用，自定义应用同样适用于外网应用。

4.3.5. 时间计划

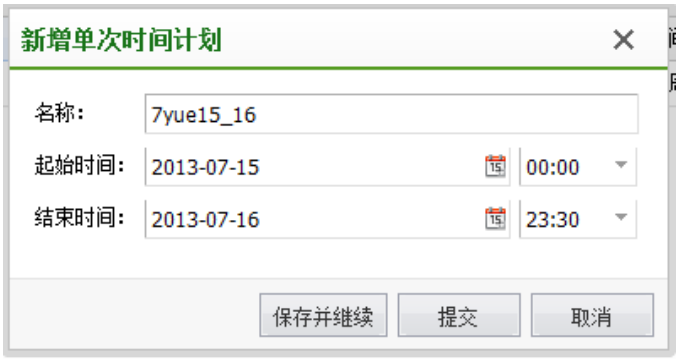
对于不同的无线或有线用户，我们需要在不同的时间段设置不同的访问控制策略以及流控策略，比如上班时间或下班时间，就需要配置时间计划，为了便于后续设置【认证授权】-【角色授权】-【访问控制策略】的生效时间，需要提前设置时间计划，『时间计划』分为

【单次时间计划】和【循环时间计划】。

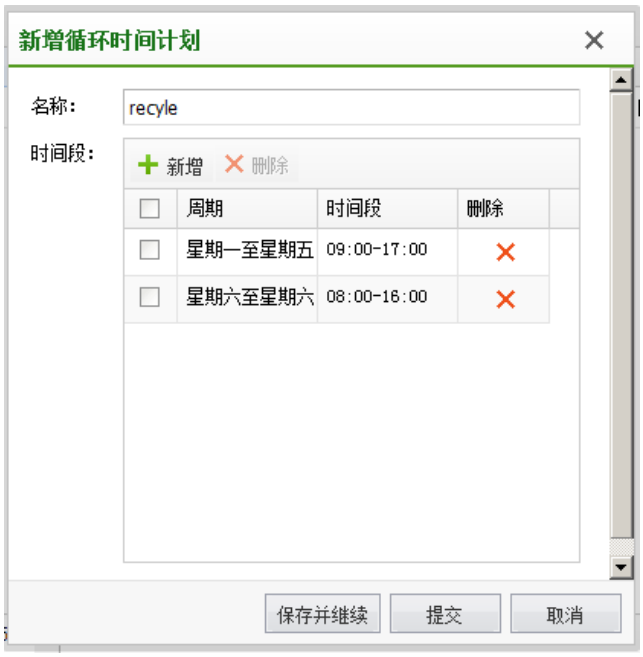
新增【单次时间计划】和【循环时间计划】:



设置循环时间时，大多数客户可以按照上班时间和下班时间，以及节假日方式设置循环时间，便与管理。



点击新增循环时间计划:



4.3.6. 智能 PSK 终端

4.3.6.1. 智能 PSK 终端

1、适用范围：

智能 PSK 终端页面配置的终端只针对智能 PSK 无线网络有效。

2、终端分类：

智能终端分为两类:信锐智能终端和普通智能终端;信锐智能终端需要输入该设备的 SN 码，普通智能终端需要输入指定的密钥。

3、问题排查：

信锐智能终端如果连接过其他 NAC，请删除该终端的记录，重新添加。

4.3.6.2. 平台对接

1、适用范围

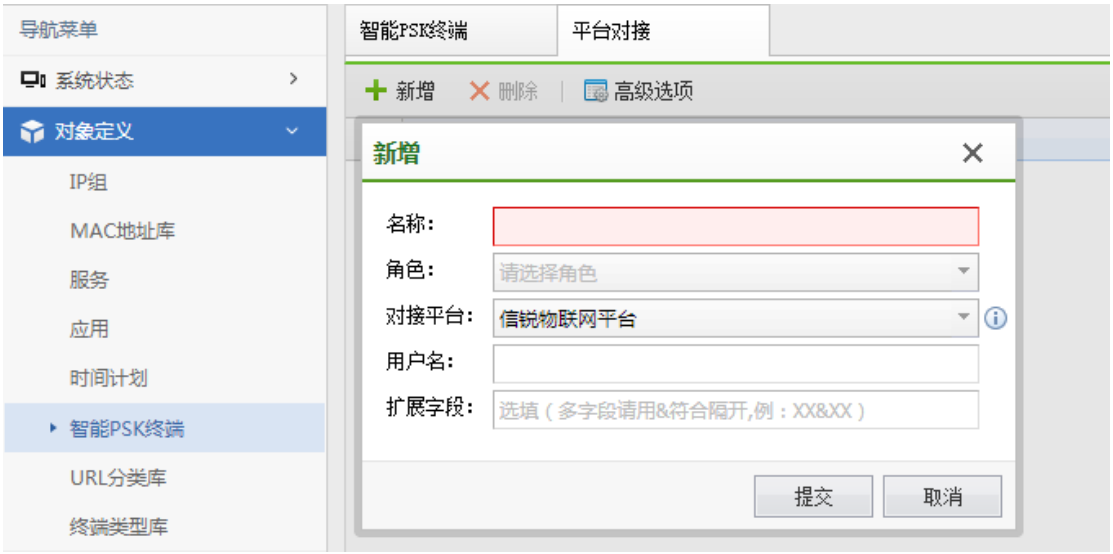
该页面仅适用于信锐智能终端。

2、对接平台配置

角色只能被一个对接平台配置引用；只有在 无线网络->权限设定 指定该角色才能为信锐智能设备下发对应的对接平台配置； 选择信锐物联网平台，用户需要指定自己注册在信锐物联网平台的用户名，扩展字段默认不填。

3、设备标识码

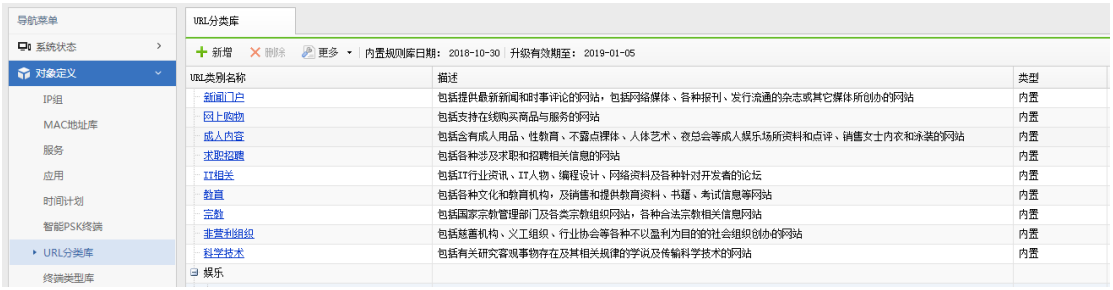
该字段用于标识不同的 NAC；如果信锐智能终端需要迁移到其他 NAC，为了保证正常接入无线网络，务必保证设备标识码一致。



4.3.7. URL 分类库

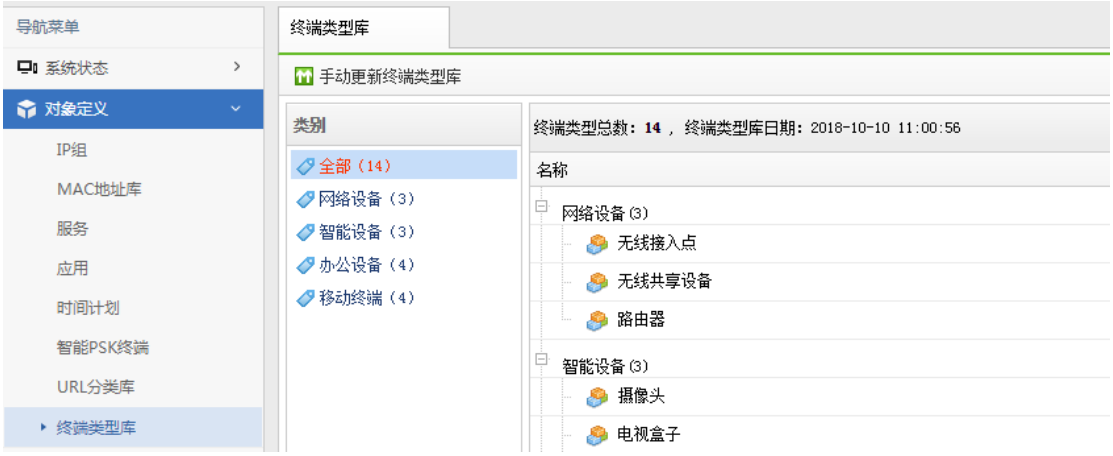
『URL 分类库』中是由信锐技术自主研发并收集的全国最大、最全、最专业的 URL 分类库。关于 URL 规则库的使用，需要在【认证授权】-【角色授权】-【访问控制策略】中新增规则，选择【应用】的方式来调用。另外对于少部分，客户内网自由的域名系统，如果无法识别到，用户还自定义 URL 类别，可将 URL 设置为内置的 URL 类别或自定义 URL 类别，也可以设置域名关键字，模糊匹配为某种类别。并设置自定义的 URL 类别优先级最高来优先调用。

URL 分类库的升级需要序列号授权，过期后无法更新。



4.3.8. 终端类型库

终端类型库中记录着终端的指纹特征，通过持续不断的收集及更新，保证终端类型识别的正确性，终端类型特征库支持手动和联网时自动更新。



4.4. 认证授权

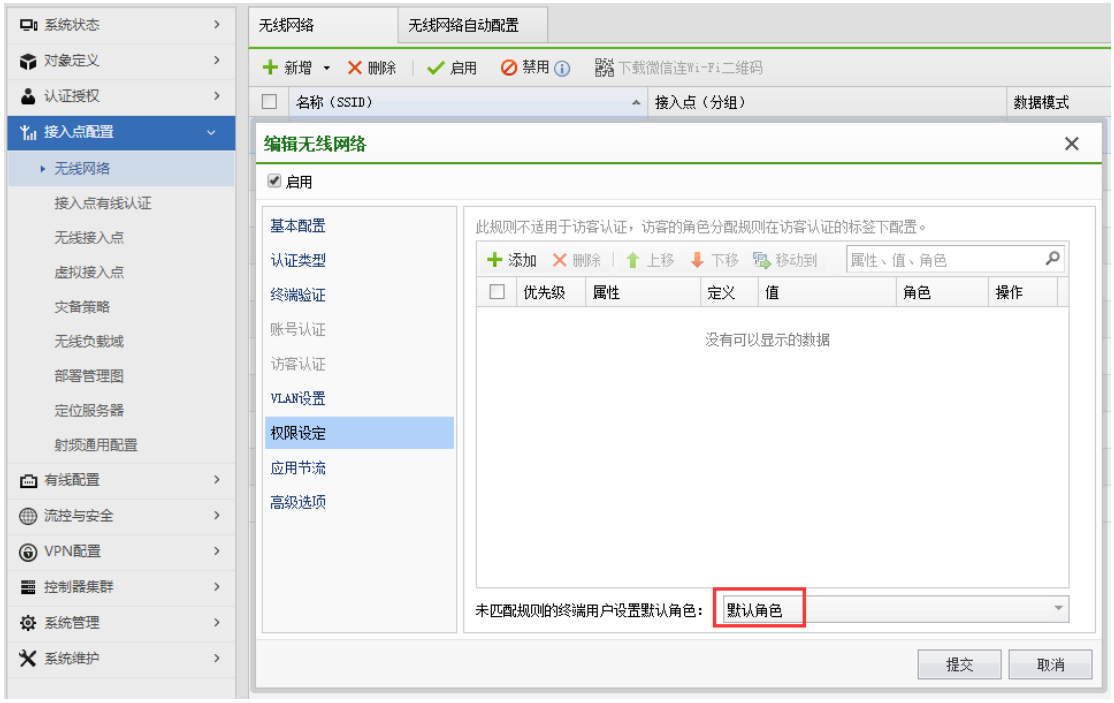
『认证授权』包含【角色授权】、【本地用户】、【访客帐号】、【证书管理】、【Web 认证】、【用户终端绑定】、【外部服务器】、【微信认证选项】、【单点登录】、【portal 服务】、【认证漫游域】、【Radius 服务】、【认证高级选项】。

4.4.1. 角色授权

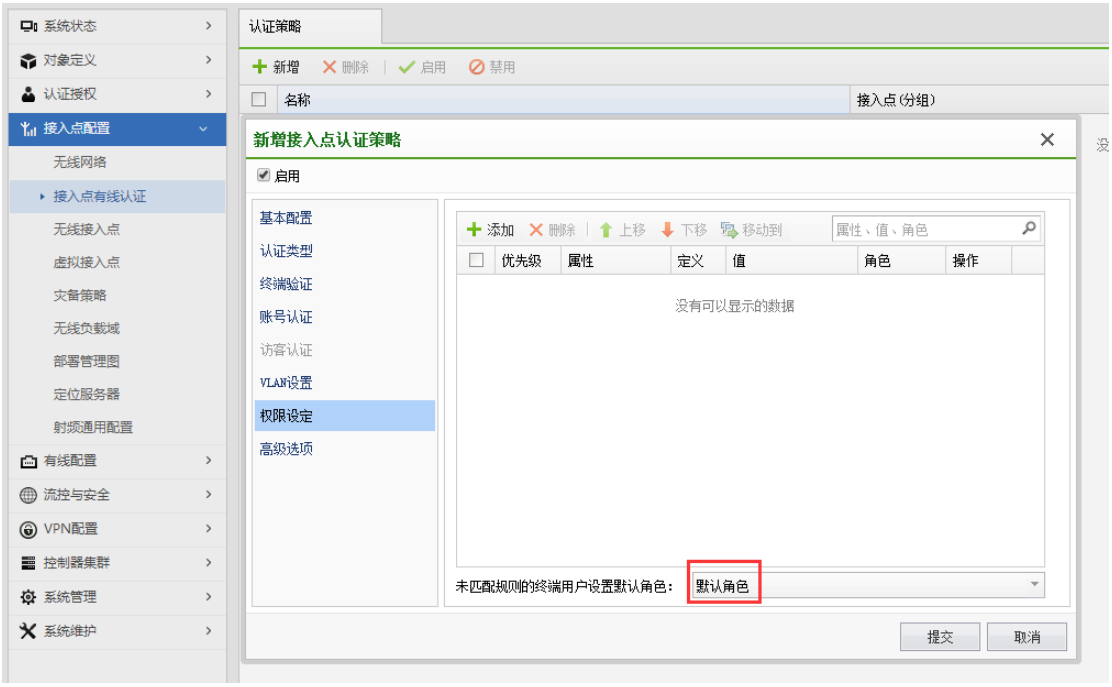
『角色授权』定义了用户可以访问网络的各种权限设定，包括【角色授权】、【访问控制策略】、【用户审计策略】、【流速限制策略】、【流量/时长配额策略】。

名称	访问控制策略	用户审计策略	流速限制策略	流量/时长配额策略	创建者	描述
DNS_yunxu	允许DNS				admin	
Only_dns	denayQQ,允许DNS				admin	
Only_local	只允许内网		sxf		admin	
getConfigTool	允许DNS				admin	
guest	no_access_local	check_all			admin	
vip_after_auth	vip_after_auth	check_all			admin	
vip_before_auth	vip_认证前策略	check_all			admin	
测试部	公司访客策略	check_all	公司访客策略	每天1GM	admin	
公司访客策略	公司访客策略	check_all			admin	

角色授权设置好后，并没有立刻被使用生效，需要在【接入点配置】-【无线网络】-【编辑无线网络】-【权限设定】中调用角色，匹配给无线用户。



另外【接入点配置】-【接入点有线认证】-【权限设定】可以定义了经过 AP 的有线用户的角色，如下图：



在【有线配置】-【有线认证】定义了直接经过 NAC 的有线用户的角色，如下图：

4.4.1.1. 角色授权

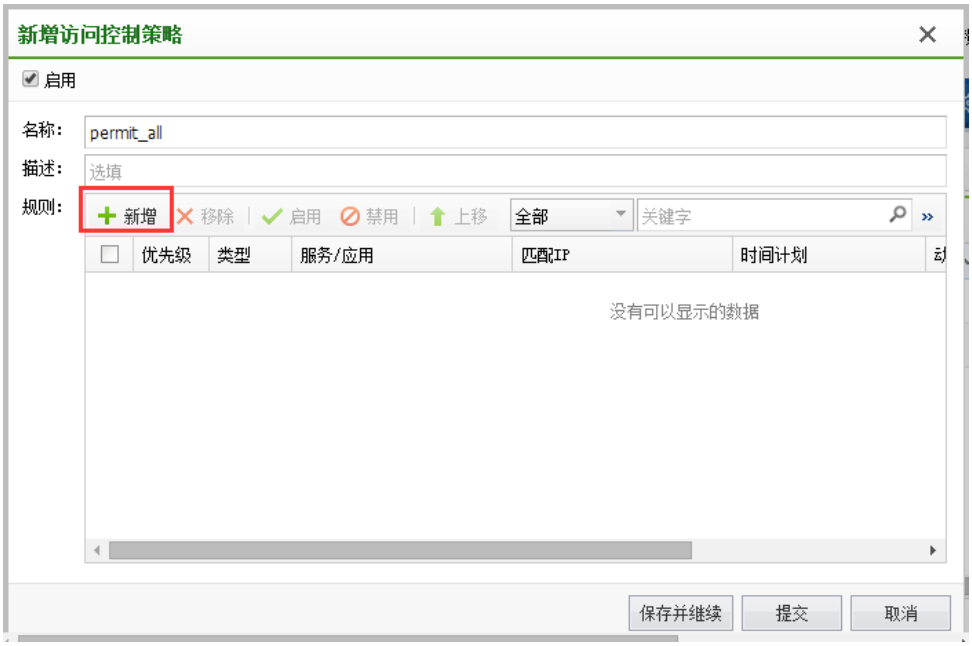
角色授权可以新增角色，然后调用左侧已经建立成功的访问控制策略、用户审计策略、和流速限制策略、以及流量/时长配额策略，也可以在角色授权中调用新增其他策略。

名称	访问控制策略	用户审计策略	流速控制策略
DNS_yunxu	允许DNS		
Only_dns	允许DNS		
Only_local	只允许内网		sxf
flow_contorl_tzm_test	permit_all		
fug	允许DNS		
getConfigTool	允许DNS		
guest	no_access_local	check_all	
vip_after_auth	vip_after_auth	check_all	
vip_before_auth	vip_认证前策略	check_all	
公司访客策略	公司访客策略	check_all	
公司人员策略	公司人员策略	check_all	
拒绝全部	拒绝全部		

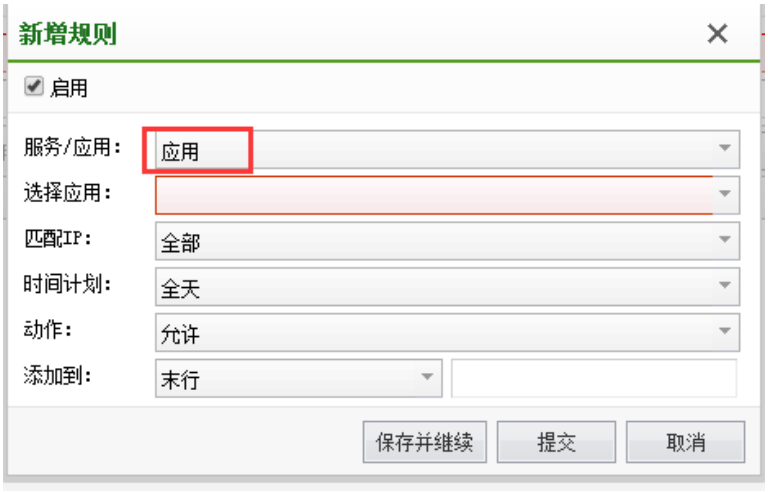
4.4.1.2. 访问控制策略

访问控制策略主要是用来限制无线终端用户可以访问的网络权限，一般网络设备设置网络权限会有 LAN 区域和 WAN 区域的划分，WLAN 不设置 LAN 区域和 WAN 区域的划分，只需要设置【用户发起】和【用户接收】2 个方向即可，配置策略还需要调用到对象定义中的【服务】、【应用】、【IP 组】以及【时间计划】。

[编辑访问控制策略]：可以新增多条访问控制策略，并且可以设置不同的优先级，策略会依次从上往下匹配。



新增规则

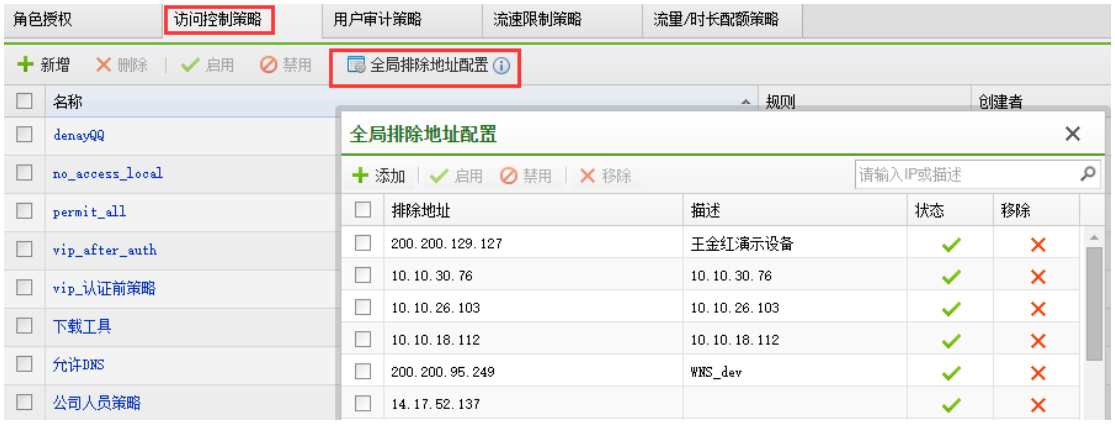


选择服务时，会调用【对象定义】中的服务，选择应用时，会调用【对象定义】中的应用。需要调用【应用】前，需要确保设备已经开启应用识别序列号，并且应用识别规则库与 URL 规则库需要处于最新状态。

URL 规则库如果未处于最新状态，会影响基于应用的访问控制策略的正常生效，需要点击立即更新更新到最新版本。

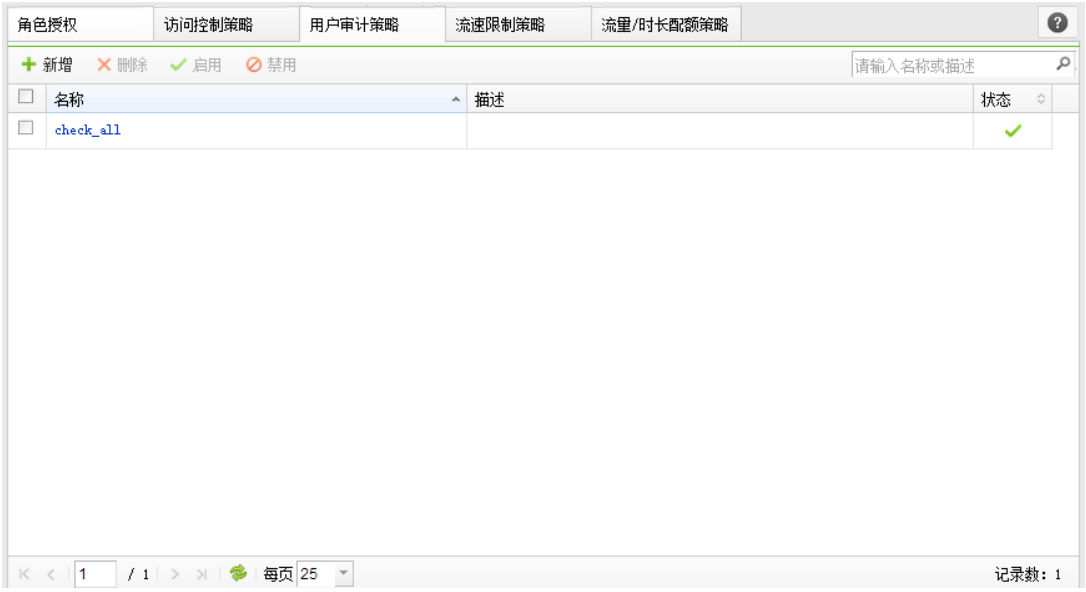
全局排除地址

添加到全局排查地址的 IP 或域名不受访客控制策略的限制



4.4.1.3. 用户审计策略

用户审计策略支持审计 HTTP 外发内容、访问网站/下载、邮件、FTP、telnet、网络应用、流量与上网时长。



HTTP 外发内容，包括 WebBBS 发帖、外发的 WebMail 邮件、通过网页上传的附件，通过网页上传的文本，微博等方式。HTTP 外发内容审计，不包括 HTTPS 方式的内容审计。

访问网站/下载，包括了 URL 规则库中所有类型的站点。邮件包括了标准的 SMTP/POP3 以及 IMAP 方式的邮件。FTP 包括 FTP 上传文件，也可以被审计，超过 50M 的文件，只会截取前 50M 文件大小。对于采用 SSL 加密的内容无法审计，比如 https 与 SMTPS/POP3S 等内容。

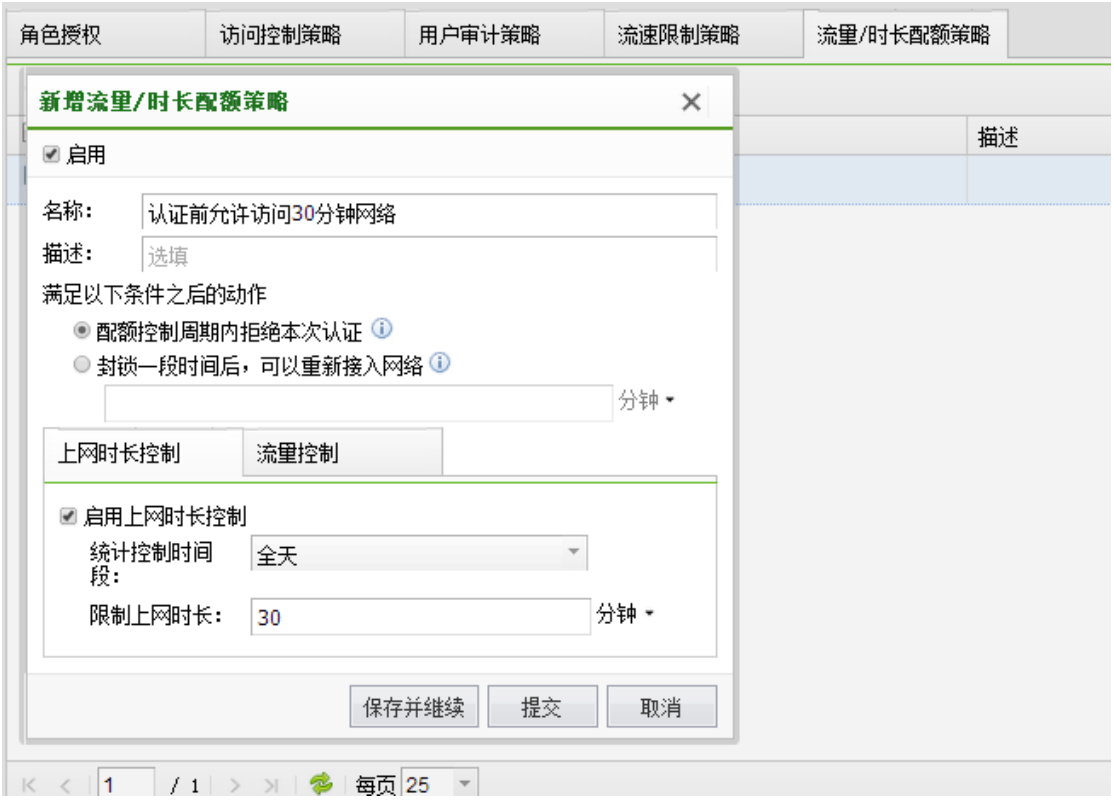
4.4.1.4. 流速限制策略

流速限制策略可以针对所有终端用户生效，包括有线与无线用户，但此功能只能限制用户的整体上行和下行的速率，无法根据应用进行流控，应用流控需要到【流控与安全】菜单下配置。该功能策略如下图：

流速限制策略可以对每一个终端进行流速限制，以避免部分终端的流速过大，影响整体无线用户体验。例如设定为发送最大限制为 512KB/s，则对使用此策略的每一个终端最大发送流速都将被限制为 512KB/s 秒。

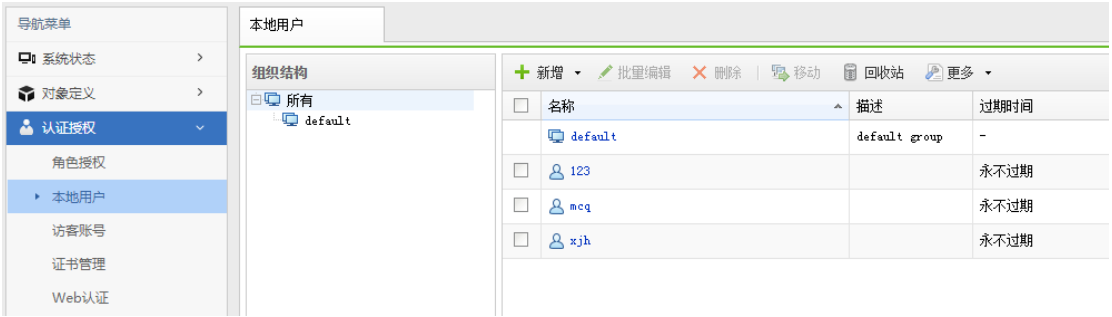
4.4.1.5. 流量/时长配额策略

流量/时长配额策略可以限制用户的上网时长和总流量大小，可以设置一个上网时长或者流量的阈值(上网的最大时长或者能使用的最大流量)，可以设置当用户上网达到这个阈值后在配额控制周期内不能再次进行认证或者只封锁一段时间后可以重新接入网络



4.4.2. 本地用户

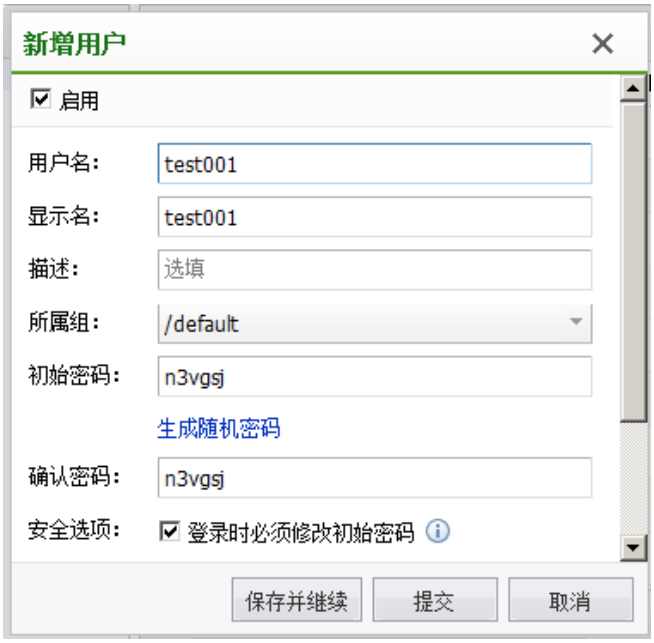
当企业没有外部认证服务器，或者不需要外部认证服务器时，可以在 NAC 上设置本地的用户，用于给无线终端的认证管理。



4.4.2.1. 新增用户

新增用户：新增一个用户，包括用户名，所属组，设置初始密码，并且可以设置登录时

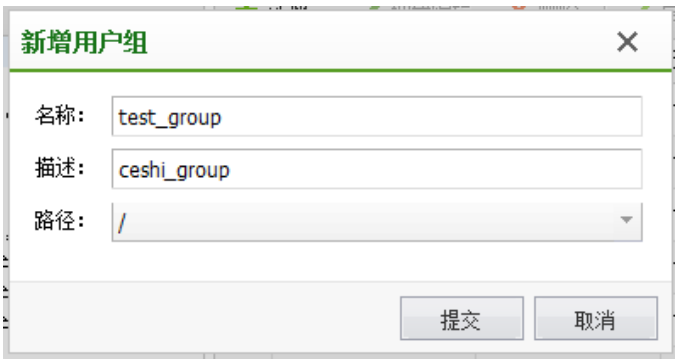
必须修改初始密码。



管理员可以为用户设置初次随机密码，然后勾选“登录时必须修改初始密码”，便于用户的认证管理。

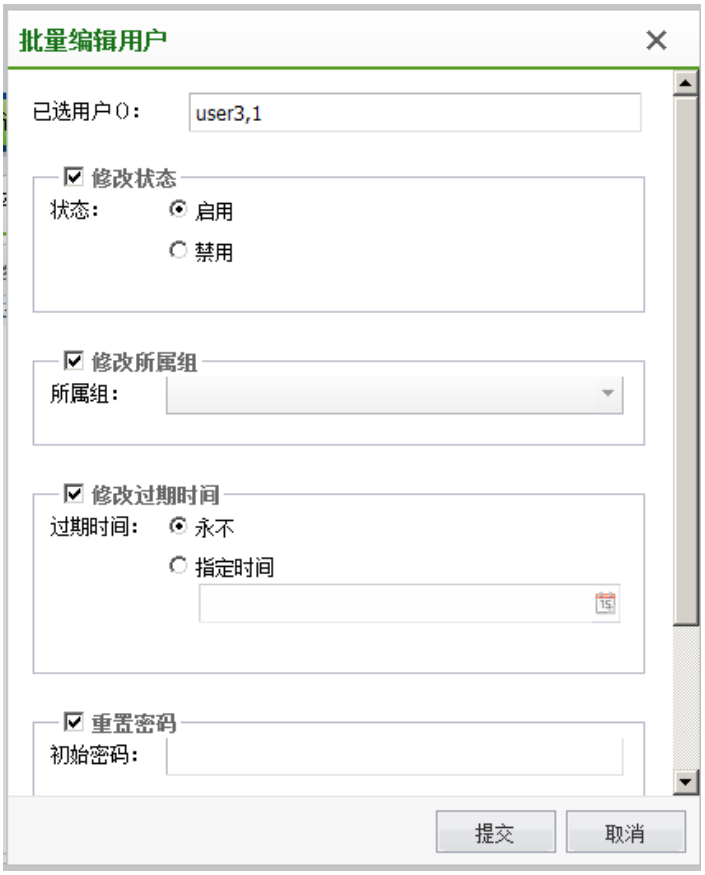
4.4.2.2. 新增用户组

新增用户组为了便于给无线用户分组管理，可以新增用户组，并选择路径，默认是跟组路径/。



4.4.2.3. 批量编辑用户

批量编辑用户：用于批量编辑用户的启用/禁用状态，所属组，有效期和密码修改，便于多用户管理和维护。



4.4.3. 访客帐号

【访客账号】存储所有的访客认证信息，包括短信验证的访客、二维码审核的访客、临时帐号访客、微信验证的访客等。

4.4.3.1. 短信认证

短信认证是指访问无线网络时，系统需要发送短信验证码到用户的手机上，用户输入验证码后，才能访问无线网络，此方式获取了访客用户的手机号码作为身份信息。

访客连接无线网络的过程如下：

1、连接到开放式的访客无线网络，例如无线网络名称为：Example-Guest。

2、打开浏览器，访问任意网站，系统将把用户的浏览器重定向到认证页面。

3、认证页面中，输入用户的手机号码，系统将把验证码发送到此手机。

4、认证页面中，输入短信中获取的验证码，通过认证。

短信认证方式的优点：

1、认证页面中，可以设置企业的广告等展示信息，提高企业形象。

2、可以获取访客的手机号码用于后续的短信营销。

3、简化了访客连接无线网络的体验。

4、短信认证的有效期为：永久生效。

短信认证服务

在部署短信认证的无线网络时，需要先启用短信认证服务，并正确配置短信发送参数。

系统支持的短信发送方式：

1、通过连接到无线控制器串口的短信猫发送

2、通过连接到外部服务器的短信猫发送

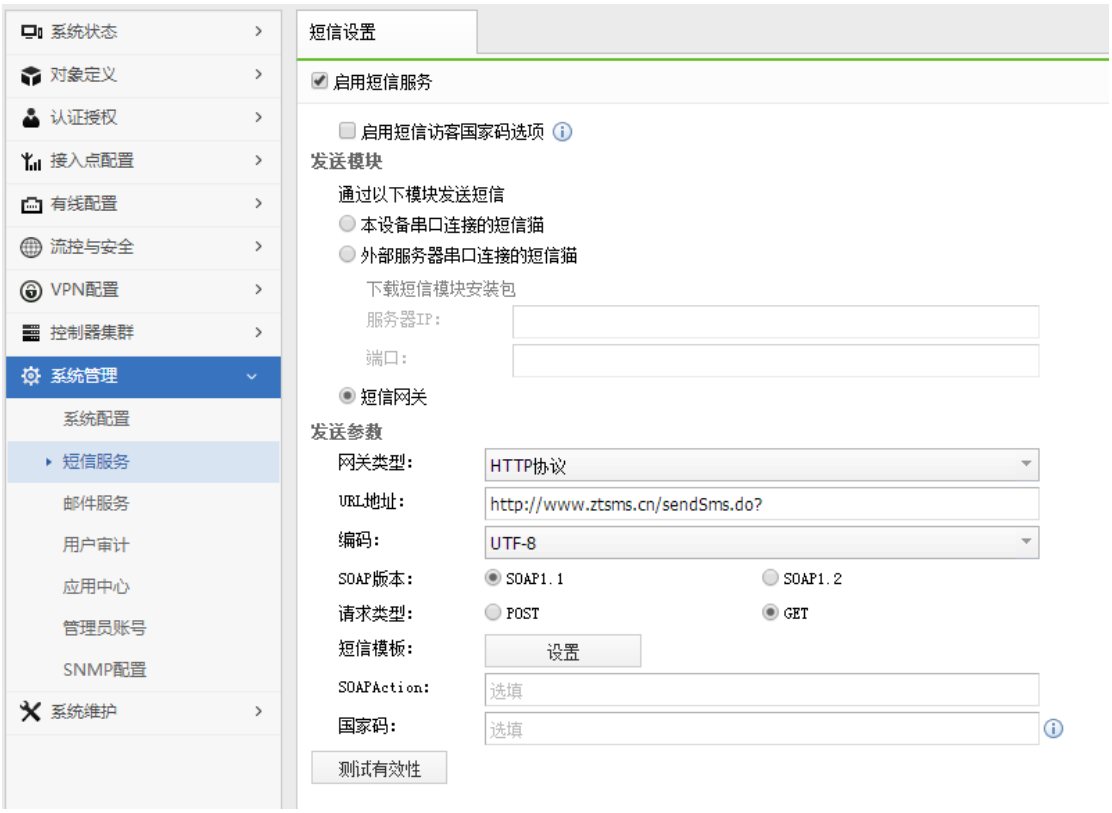
说明：如果无线控制器部署的机房中，手机网络信号差，导致无法发送短信。则可以选择把短信猫连接到一台服务器，并把服务器部署到此机房以外，且信号良好的环境中，由此服务器来代理发送短信。

部署步骤如下：

1、在短信认证选项界面中，下载“信锐短信发送服务程序”，并安装在运行 Windows XP，Windows 7，Windows Server 2003，Windows Server 2008，32 位系统的计算机中。

2、把短信猫连接到此计算机的串口/USB 口（取决于短信猫型号）。

3、确保无线控制器可以访问此计算机。并在无线控制器中，配置正确的短信发送参数。



还可以通过 WebServices 方式发送短信，通过 HTTP 方式的短信网关，此方法较为常用。

4.4.3.2. 二维码认证

此方式通常用于企业的访客无线网络认证，可以确保只有经过二维码审核的访客用户才具备无线网络访问权限。在 Web 认证中，可以指定审核人，在二维码审核时分配被审核人的角色和上网时长，并且记录访客信息。

1、访客连接无线网络的过程如下：

1）连接到开放式的访客无线网络，例如无线网络名称为：Example-Guest。

2）打开浏览器，访问任意网站，系统将把用户的浏览器重定向到认证页面。

3）认证页面中，显示企业配置的访客信息输入框（在二维码认证的认证附加信息中配置），访客输入对应信息后，点击下一步按钮，即可生成二维码。

4）访客的接待人员可以通过以下两种方式审核二维码:

- 使用手机连接到企业无线网络中，并具备审批权限。审批权限由 Web 认证方式指定，可以设置哪些角色作为审核人，哪些角色和上网时长可以由审核人分配给被审核人（在二维码认证的有效期中可以配置自定义的上网时长）。

- 接待人员，打开手机中的二维码应用，扫描访客的二维码，查看或者修改访客在认证页面中输入的访客信息，然后可以分配角色和上网时长给被审核人。需要说明的是，目前很多流行的互联网应用都提供了二维码扫描功能，例如腾讯微信(用此软件的时候需要审核人角色必须能正常访问互联网，因为此软件二维码扫描的时候要访问互联网才能正常使用)和我查查。

2、二维码审核的有效期

通过二维码审核后，访客可以在指定的期间访问无线网络。超过设置时间后，如果仍然需要访问无线网络，需要再次审核。

4.4.3.3. 临时帐号认证

此方式通常用于企业、酒店的访客无线网络认证，可以在访客登记后，接待人员创建一个临时账号，并设置账号的有效期。访客使用此账号完成无线网络认证。

以酒店的部署场景为例，顾客连接无线网络的过程如下：

顾客在酒店前台登记入住。

1、酒店的前台工作人员，在访客管理系统中，为此顾客添加一个临时账号，以手机号或者身份证号码作为账号的用户名，密码为手机号码或身份证号码的后 6 位。账号的有效时间设置为顾客的离店时间。

2、顾客连接到酒店部署的，开放式的无线网络，例如无线网络名称为：Example-Guest。

3、打开浏览器，访问任意网站，系统将把浏览器重定向到认证页面。

4、在认证页面中，输入此临时账号及密码，完成无线网络认证。

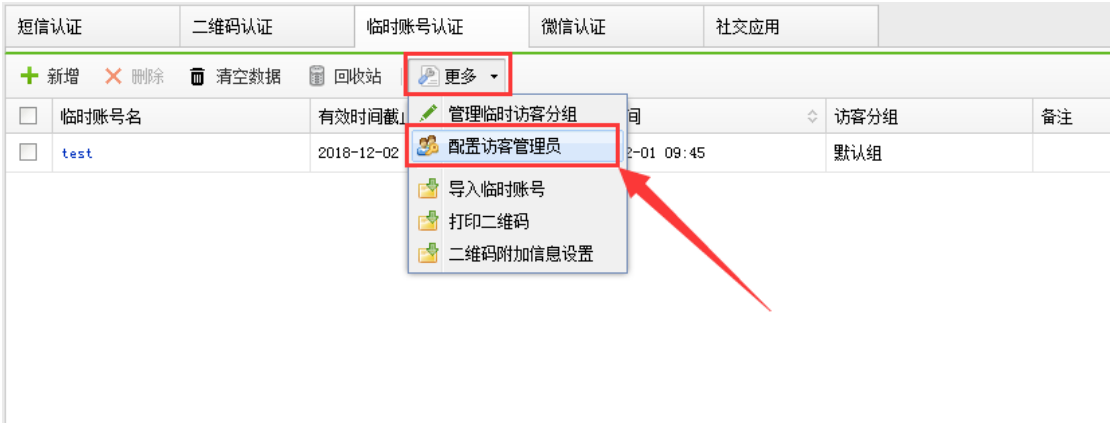
5、顾客离开酒店后，账号自动失效。

临时账号管理员

访客账号通常并非由网络管理员管理，而是由负责访客接待的人员管理。因此，系统提供了临时账号管理员，以区别于无线控制器的管理员。临时账号管理员只允管理访客账号，无法修改无线控制器的其它设置。

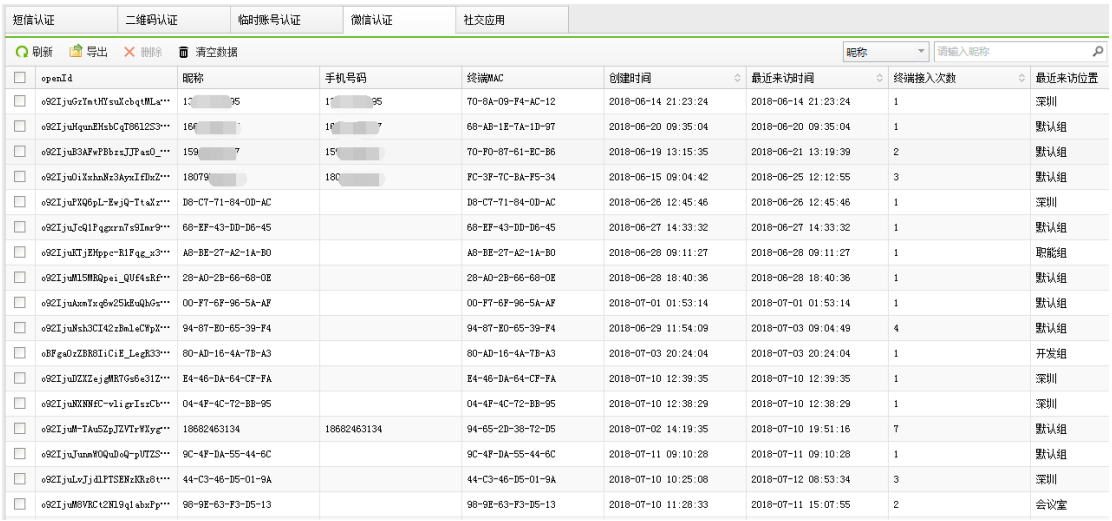
临时账号管理员的登录地址与无线控制器管理员不同，登录地址为：

https://设备地址/guest.php，例如：https://192.168.0.1/guest.php



4.4.3.4. 微信认证

此方式通常用于商场、超市的无线网络认证，可以确保只有关注过指定微信公众账号的访客用户才具备无线网络访问权限。认证选项中，可以设置关注微信后，每次申请上网的有效期。



openId	昵称	手机号码	终端MAC	创建时间	最近来访时间	终端接入次数	最近来访位置
o92IjuGzYmtHYsuXcbqtMLs···	1[redacted]95	1[redacted]95	70-8A-09-F4-AC-12	2018-06-14 21:23:24	2018-06-14 21:23:24	1	深圳
o92IjuHqunEHsbCqT861ZS3···	186[redacted]	18[redacted]7	68-A8-1E-7A-1D-97	2018-06-20 09:35:04	2018-06-20 09:35:04	1	默认组
o92IjuB3AFwPBbrsJJPasO_···	159[redacted]7	15[redacted]	70-F0-87-61-EC-B6	2018-06-19 13:15:35	2018-06-21 13:19:39	2	默认组
o92IjuDiXxhnNz3AyxIfDxZ···	18079[redacted]	18[redacted]	FC-3F-7C-BA-F5-34	2018-06-15 09:04:42	2018-06-25 12:12:55	3	默认组
o92IjuFXQ6pL-EwjQ-TtaXz···	D8-C7-71-84-0D-AC		D8-C7-71-84-0D-AC	2018-06-26 12:45:46	2018-06-26 12:45:46	1	深圳
o92IjuJcQ1PqgxrnTs9Imr9···	68-EF-43-DD-D6-45		68-EF-43-DD-D6-45	2018-06-27 14:33:32	2018-06-27 14:33:32	1	默认组
o92IjuKTjEMppc-R1Fqg_x3···	A8-BE-27-A2-1A-B0		A8-BE-27-A2-1A-B0	2018-06-28 09:11:27	2018-06-28 09:11:27	1	职能组
o92IjuM15MRQpei_QUf4sRf···	28-A0-2B-66-68-0E		28-A0-2B-66-68-0E	2018-06-28 18:40:36	2018-06-28 18:40:36	1	默认组
o92IjuAxmYxq6w25kEuQhGs···	00-F7-6F-96-5A-AF		00-F7-6F-96-5A-AF	2018-07-01 01:53:14	2018-07-01 01:53:14	1	默认组
o92IjuNsh3CI42zBmleCWpX···	94-87-E0-65-39-F4		94-87-E0-65-39-F4	2018-06-29 11:54:09	2018-07-03 09:04:49	4	默认组
oBFgaOrZBR8IiCiE_LegK33···	80-AD-16-4A-7B-A3		80-AD-16-4A-7B-A3	2018-07-03 20:24:04	2018-07-03 20:24:04	1	开发组
o92IjuDZXZejgMR7Gs6e31Z···	E4-46-DA-64-CF-FA		E4-46-DA-64-CF-FA	2018-07-10 12:39:35	2018-07-10 12:39:35	1	深圳
o92IjuHXNNfC-vliguIszCb···	04-4F-4C-72-BB-95		04-4F-4C-72-BB-95	2018-07-10 12:38:29	2018-07-10 12:38:29	1	深圳
o92IjuM-TAu5ZpJZVTrWXyg···	18682463134	18682463134	94-65-2D-38-72-D5	2018-07-02 14:19:35	2018-07-10 19:51:16	7	默认组
o92IjuJunwWOQuDoQ-pVTZS···	9C-4F-DA-55-44-6C		9C-4F-DA-55-44-6C	2018-07-11 09:10:28	2018-07-11 09:10:28	1	默认组
o92IjuLvJjdlPTSENzKRz8t···	44-C3-46-D5-01-9A		44-C3-46-D5-01-9A	2018-07-10 10:25:08	2018-07-12 08:53:34	3	深圳
o92IjuM8VRCt2N19qlabxFp···	98-9E-63-F3-D5-13		98-9E-63-F3-D5-13	2018-07-10 11:28:33	2018-07-11 15:07:55	2	会议室

访客连接无线网络的过程如下：

1、连接到开放式的访客无线网络，例如无线网络名称为：Example-WeChat。

2、打开浏览器，访问任意网站，系统将把用户的浏览器重定向到指定的认证页面。认证页面可以配置需要关注的微信公众账号名称。

3、认证页面中，提示用户关注微信公众账号。页面还有微信 APP 的下载链接。

4、用户这时有两种方式通过微信认证：

a)、 第一种是切换到微信应用，查找公众账号，然后关注该公众账号，关注之后可以在菜单栏中点击“我要上网”来申请上网，点击公众微信号发过来的信息中的超链接上网即可。

b)、 第二种适用于用户的无线终端无法安装微信应用的场景，用户点击认证页面下方的生成二维码链接，页面会生成一个二维码，适用已经通过微信认证的用户的无线终端，适用微信的“扫一扫”功能，扫描二维码即可上网。

注：配置无线网络 Example-WeChat 时，访客认证的认证方式选择微信认证时，所属无线网络的无线网络会默认放通微信流量。

4.4.3.5. 社交应用

此方式通常用于海外或港澳台等地区，终端用户可以使用 Facebook，Twitter，Line，Live，Instagram 账号进行授权，授权后关注商家账号即可通过认证。

通常，通过认证的用户，控制器可以获取到用户的用户 ID、用户名、终端 MAC 地址、邮箱地址、性别、年龄段等。但上述字段在用户没有配置的时候，是获取不到的。

配置社交应用认证时，认证前需要放通对应流量，推荐使用内置角色进行认证。

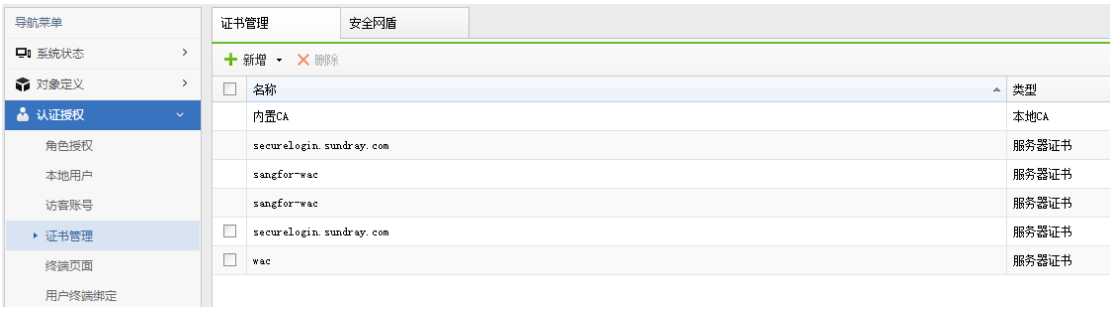
用户名	用户ID	终端MAC	邮箱	性别	年龄段	接入次数	最近接入位置	最近接入时间	创建时间
zhu[redacted]com	-	94-87-E0-09-52-CF	zhu[redacted]y.com	未识别	未识别	1	开发组	2018-09-22 09:10:31	2018-09-22 09:10:31
hsy[redacted]com	-	78-02-F8-32-F0-AF	hsy[redacted]com	未识别	未识别	1	开发组	2018-09-22 11:39:04	2018-09-22 11:39:04
wang[redacted]com	-	6C-B7-49-C1-5D-3B	war[redacted]qq***	未识别	未识别	1	开发组	2018-09-22 11:53:10	2018-09-22 11:53:10
25219[redacted]com	-	F4-F5-DB-CA-BC-31	25[redacted]com	未识别	未识别	1	开发组	2018-09-22 17:55:15	2018-09-22 17:55:15
25219[redacted]com	-	80-AD-16-4A-7B-9F	25[redacted]com	未识别	未识别	2	开发组	2018-09-25 11:55:42	2018-09-21 19:11:39
qi[redacted]om	-	DC-72-9B-DE-3C-BF	[redacted]com	未识别	未识别	1	开发组	2018-09-25 14:59:14	2018-09-25 14:59:14
yu[redacted]com	-	B8-C1-11-2C-43-9C	yu[redacted]com	未识别	未识别	1	开发组	2018-10-08 17:02:18	2018-10-08 17:02:18
51[redacted]com	-	9C-E3-3F-44-D8-F5	51[redacted].com	未识别	未识别	1	职能组	2018-10-17 14:29:32	2018-10-17 14:29:32

4.4.4. 证书管理

包含【证书管理】和【安全网盾】两个模块。

4.4.4.1. 证书管理

『证书管理』是用于管理【外部 CA】和管理【服务器证书】。配置证书管理后，可以在【接入点配置】-【无线网络】中选择认证方式属于“企业”方式认证的时候，启用证书方式认证。证书方式认证，大大加强了企业无线用户终端的安全接入。

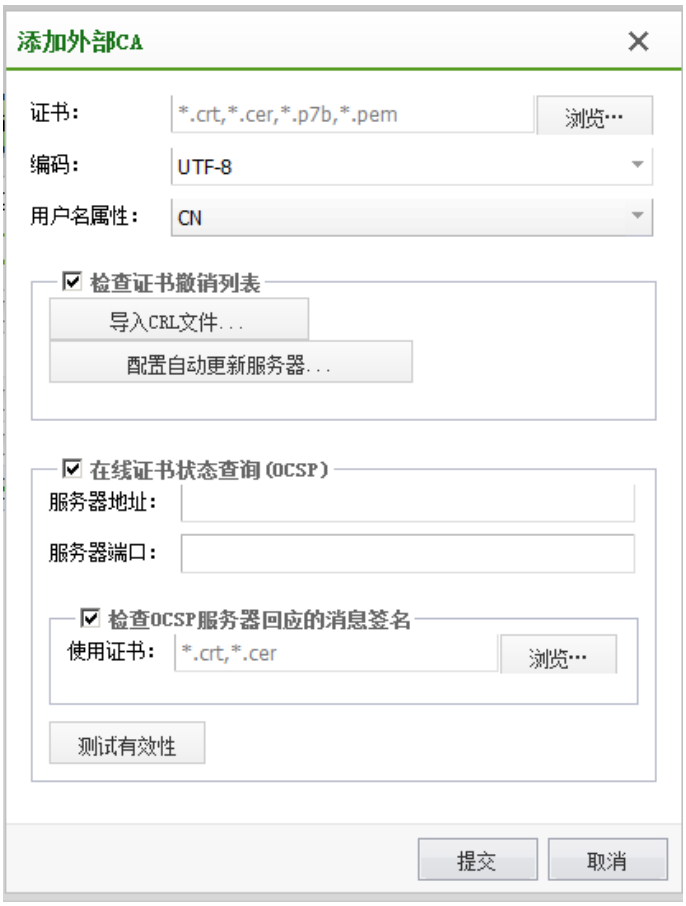


证书可以新增【外部 CA】、【服务器证书】、【WAPI-ASU 证书】和【WAPI-AE 证书】

4.4.4.1.1. 外部 CA 证书

【添加外部 CA】主要是通过在线方式去检测证书的有效性，不需要把用户认证证书导入到 NAC 设备上，当无线终端采用证书方式认证的，NAC 主动去与服务器进行交互认证。

验证证书用户的有效性。



【证书】:导入外部 CA 的根证书。

【编码】包括：UTF-8、UCS-2、GBK、GB2312、BIG5，指明该 CA 所颁发用户证书的编码格式，让 NAC 能正确提取用户证书的信息，如选择了 BIG5，但选择的证书是 UTF8，则会显示不正确。

【用户名属性】CN、Email 前缀、OID，用户认证成功后用指定的属性值显示为登录用户名。

【检查证书撤销列表】通过 CRL 文件或在线查询被吊销的证书。

【导入 CRL 文件】：CRL 文件可以简单的理解为一个记录了用户证书序列号的文

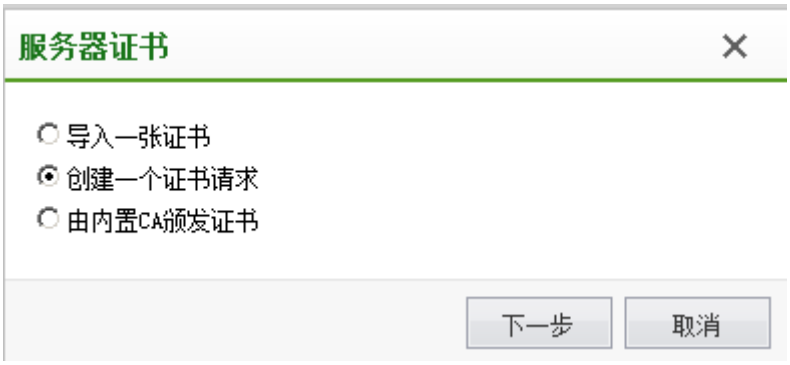
件，该文件由 CA 签发发布，记录了的证书序列号表示该证书已经失效。也就是 CRL 里面记录的证书序列号表示由这个 CA 签发的证书并且序列号在 CRL 文件里面的都已经是无效了的证书。

【在线证书状态查询】一般 CRL 文件并不是每天都发布，而是周期性的发布，而在这个周期内有可能其他证书被吊销了，所以可以配置在线证书状态实时去查询证书的有效性

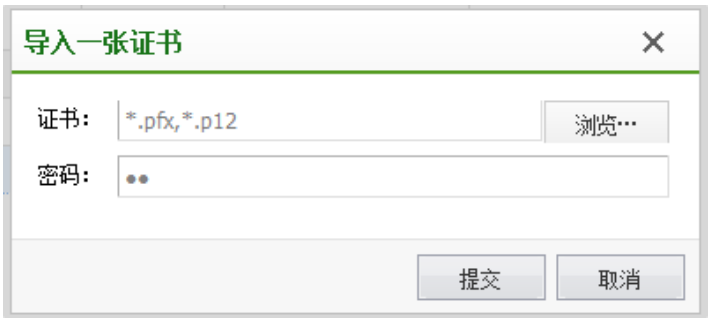
【检查 OCSP 服务器回应的消息签名】导入 OCSP 服务端签名证书的公钥，主要检测 OSCP 数据在传输过程中是否被篡改。

4.4.4.1.2. 服务器证书

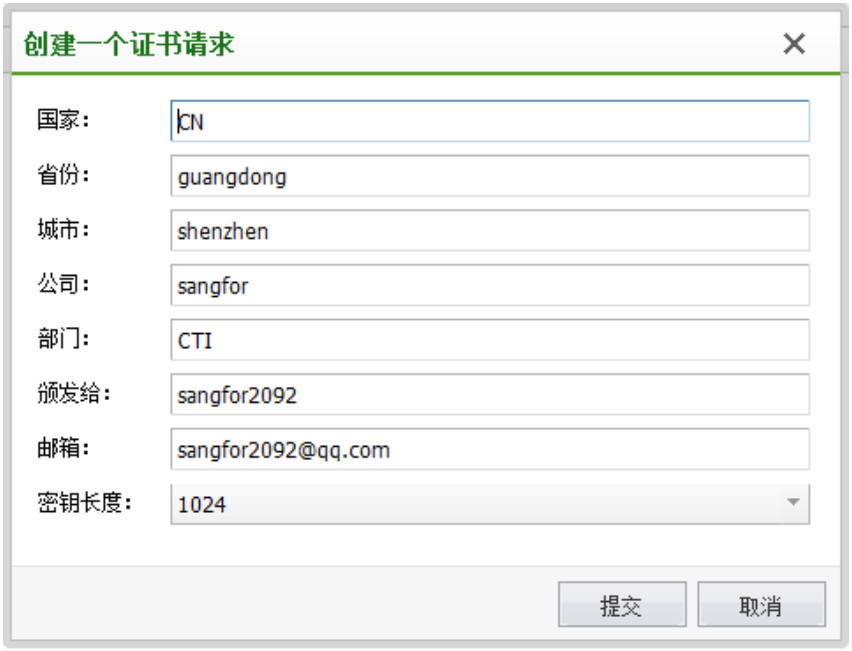
配置服务器证书，是为了让无线终端用户反向认证服务器是否合法，可以配置服务器证书，服务器证书可以通过 2 种方式生成。【导入一张证书】和【创建一个证书请求】，如下图：

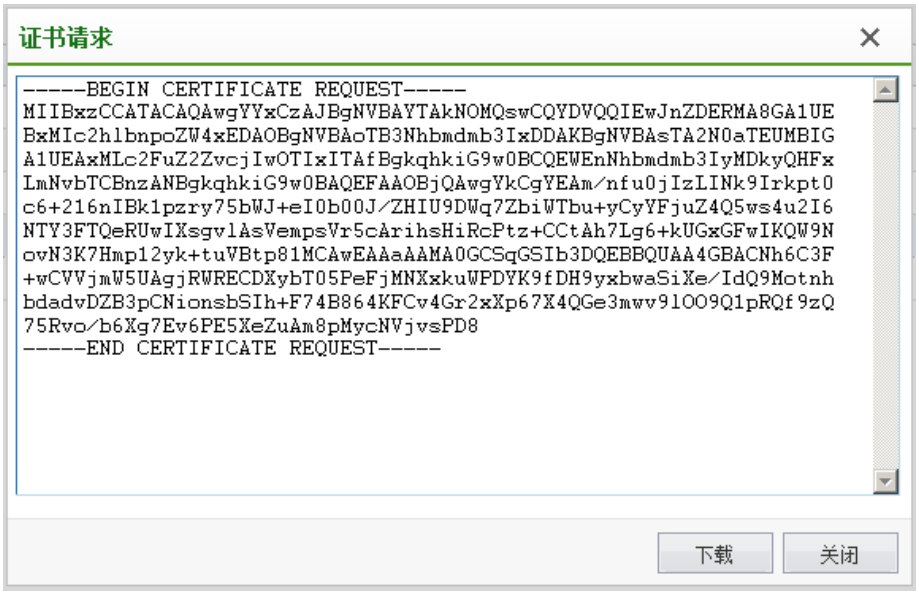


【导入一张证书】直接将已有的服务器证书的公钥私钥一起导入到设备里面。如果证书采用了密码，需要使用密码后，才可以正常导入。



【创建证书请求】：填写用户信息，包括国家、省份、城市、公司、部门、颁发给、邮箱、并设置密码长度，就可以创建一张证书请求文件：



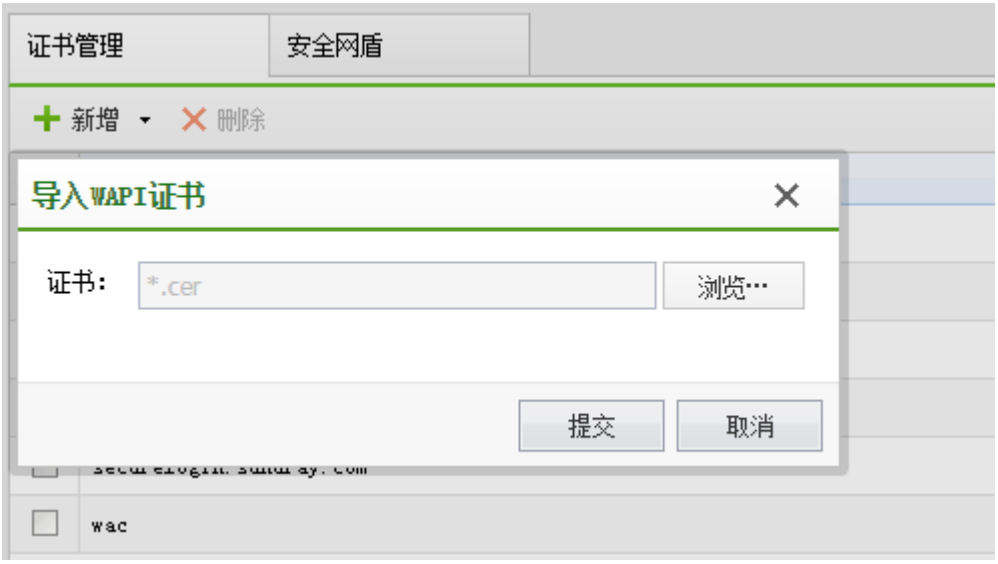


证书请求文件需要让 CA 签名，附上签名数据，有效期后，点击【处理未决的证书请求】再把证书导入到设备中，就可以在设备生成一张完整的服务器证书了。

内置 CA 颁发证书：由内置颁发证书，填写用户信息，包括国家、省份、城市、公司、部门、颁发给、邮箱，可以设置由 NAC 内置 CA 中心颁发的服务器证书。对于不同的 SSID 认证，可以设置不同的服务器证书。初次使用内置 CA 颁发证书前，需要对内置 CA 进行初始化。

4.4.4.1.3. 添加 WAPI-ASU 证书

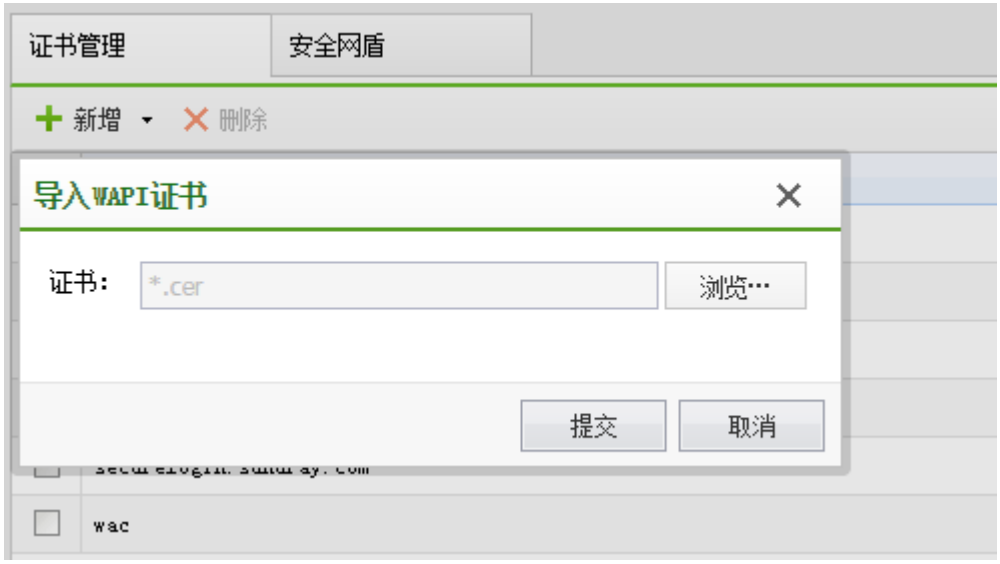
AS 服务器证书，安装到无线接入点（AP），用于 AP 在认证过程中进行证书签名验证。



4.4.4.1.4. 添加 WAPI-AE 证书

无线接入点（AP）的数字身份凭证。证书由 AS 服务器颁发、吊销等。支持以.cer 为后缀的证书文件（x509 标准 v3 版本）。

无线终端需要安装 WAPI-ASU 证书、用户证书，由 AS 服务器颁发之后，通过邮件或其他方式发送到无线终端。



4.4.4.2. 安全网盾

证书认证可避免由于密码泄漏，密码强度低等原因所导致的风险，是目前无线认证中最安全的认证方法。区别于传统的证书认证，信锐安全网盾可为用户自动配置无线网络，使无线连接更简单，更便捷。

下面针对一些名词做下解释：

1、组织结构：安全网盾的组织结构会同步 LDAP 服务器，本地用户的组织结构树，可按照企业实际组织结构显示分组。

2、用户名：安全网盾支持烧录本地用户证书，LDAP 服务器用户证书，用户名与本地用户，LDAP 服务器用户名保持一致。

3、安全网盾序列号：每一张安全网盾都有唯一的序列号，印刷在安全网盾的背面（Key S/N）。

4、证书有效期：证书有效期即安全网盾证书的过期时间，过期后将不能连接安全网盾无线网络，管理员也不能审批更新证书。

5、接入日志：接入日志中，记录了安全网盾最近 5 条的认证日志。

6、证书状态：记录安全网盾证书的状态。

7、有效：证书有效期大于 30 天。

8、即将过期：证书有效期小于 30 天。

9、待审批：控制器收到了更新安全网盾证书的请求。

10、已审批，未更新：管理员更新安全网盾证书。

11、证书已过期：证书已过有效期。

12、证书更新：当证书状态为即将过期或待审批时，管理员可以预先审批/审批安全网盾证书。

13、MAC 地址：安全网盾的 MAC 地址，初始值为‘-’，当网盾连接网络后更新。

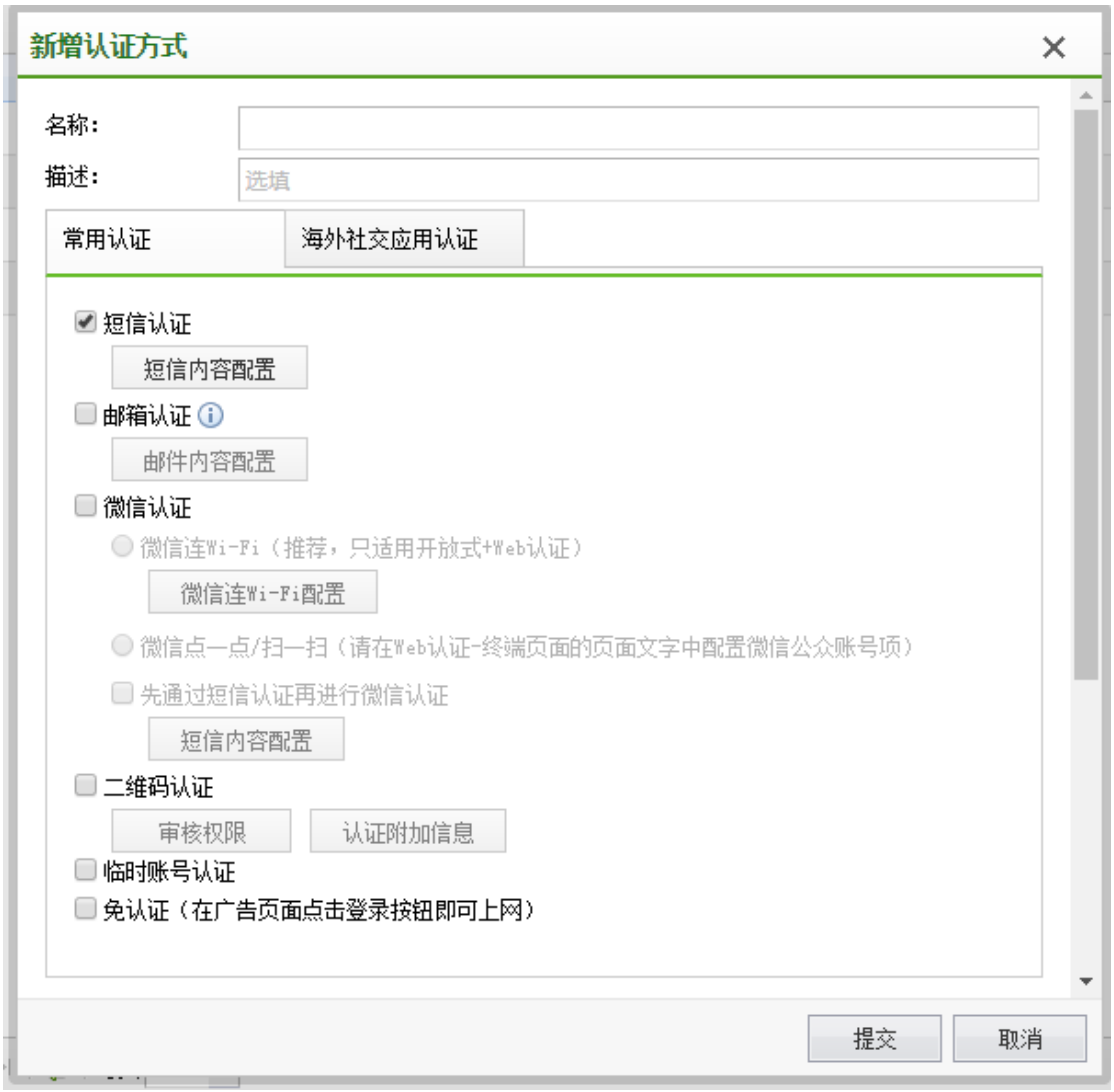
14、状态：安全网盾支持启禁用，禁用后无法接入安全网盾无线网络。

4.4.5. Web 认证

『Web 认证』包括【访客认证】、【终端页面】、【应用管理】、【消息栏模版】、【语言管理】五个模块

4.4.5.1. 访客认证

在部署用于访客使用的无线网络时，为了简化用户体验，通常设置为开放式的无线网络。但单纯的开放式的无线网络，存在无法验证访客身份的问题，因此通常需要设置认证方式。此方式主要部署在公众访问的无线网络中，例如部署在机场，交通枢纽，医院，酒店，商场，学校等地方。



4.4.5.1.1. 短信认证

启用短信认证时，需要到【系统管理】-【短信服务】页面配置短信设备，包括采用短信猫，外置短信服务器或外置短信网关。

短信认证是指访问无线网络时，系统需要发送短信验证码到用户的手机上，用户输入验证码后，才能访问无线网络，此方式获取了访客用户的手机号码作为身份信息。

访客连接无线网络的过程如下：

1、连接到开放式的访客无线网络，例如无线网络名称为：Example-Guest。

2、打开浏览器，访问任意网站，系统将把用户的浏览器重定向到认证页面。

3、认证页面中，输入用户的手机号码，系统将把验证码发送到此手机。

4、认证页面中，输入短信中获取的验证码，通过认证。

短信认证方式的优点：

1、认证页面中，可以设置企业的广告等展示信息，提高企业形象。

2、可以获取访客的手机号码用于后续的短信营销。

3、简化了访客连接无线网络的体验。

4.4.5.1.2. 邮箱认证

邮箱认证是指访问无线网络时，系统需要发送验证码及授权 url 发送到用户的邮箱上，用户输入验证码或者点击授权 url 后，才能访问无线网络，此方式获取了访客用户的邮箱地址作为身份信息。

访客连接无线网络的过程如下：

1、连接到开放式的访客无线网络，例如无线网络名称为：Example-Guest。

2、打开浏览器，访问任意网站，系统将把用户的浏览器重定向到认证页面。

3、认证页面中，输入用户的邮箱地址，系统将把验证码和授权 url 发送到此邮箱。

4、认证页面中，输入邮箱中获取的验证码或者点击授权 url，通过认证。

邮箱认证方式的优点：

1、迎合了国外使用邮箱较多的习惯，提升用户体验。

2、认证页面中，可以设置企业的广告等展示信息，提高企业形象。

3、可以获取访客的邮箱地址用于后续的邮件营销。

4、提供点击链接认证上网的方式，简化了访客连接无线网络的体验。

4.4.5.1.3. 微信认证

此方式通常用于商场、超市的无线网络认证，可以确保只有关注过指定微信公众账号的访客用户才具备无线网络访问权限。认证选项中，可以设置关注微信后，每次申请上网的有效期。

访客连接无线网络的过程如下：

连接到开放式的访客无线网络，例如无线网络名称为：Example-WeChat。

打开浏览器，访问任意网站，系统将把用户的浏览器重定向到指定的认证页面，点击认证页面上的微信连 WiFi 按钮跳转到微信完成微信认证。

PS：微信连 WiFi 相关参数需从微信公众平台后台获取后填入控制器。

4.4.5.1.4. 二维码认证

此方式通常用于企业的访客无线网络认证，可以确保只有经过二维码审核的访客用户才具备无线网络访问权限。认证选项中，可以设置审核通过后，访客可以访问无线网络的时长。

访客连接无线网络的过程如下：

1、连接到开放式的访客无线网络，例如无线网络名称为：Example-Guest。

2、打开浏览器，访问任意网站，系统将把用户的浏览器重定向到认证页面。

3、认证页面中，显示一个二维码。

4、访客的接待人员，也就是企业的内部员工，使用手机连接到企业无线网络中，并具备审批权限。审批权限由无线网络配置中指定，可以设置哪些角色的用户具备访客审批权限。

5、接待人员，打开手机中的二维码应用，扫描访客的二维码，访客即通过审核。需要说明的是，目前很多流行的互联网应用都提供了二维码扫描功能，例如腾讯微信(用此软件的时候需要审核人角色必须能正常访问互联网，因为此软件二维码扫描的时候要访问互联网才能正常使用)和我查查。

4.4.5.1.5. 临时访客认证

此方式通常用于企业、酒店的访客无线网络认证，可以在访客登记后，接待人员创建一个临时帐号，并设置帐号的有效期。访客使用此帐号完成无线网络认证。

以酒店的部署场景为例，顾客连接无线网络的过程如下：

1、顾客在酒店前台登记入住。

2、酒店的前台工作人员，在访客管理系统中，为此顾客添加一个临时帐号，以手机号或者身份证号码作为帐号的用户名，密码为手机号码或身份证号码的后 6 位。帐号的有效时间设置为顾客的离店时间。

3、顾客连接到酒店部署的，开放式的无线网络，例如无线网络名称为：Example-Guest。

4、打开浏览器，访问任意网站，系统将把浏览器重定向到认证页面。

5、在认证页面中，输入此临时帐号及密码，完成无线网络认证。

6、顾客离开酒店后，帐号自动失效。

访客帐号通常并非由网络管理员管理，而是由负责访客接待的人员管理。因此，系统提供了临时帐号管理员，以区别于无线控制器的管理员。临时帐号管理员只允管理访客帐号，无法修改无线控制器的其它设置。

临时帐号管理员的登录地址与无线控制器管理员不同，登录地址为： https://设备地址/guest.php，例如：https://192.168.0.1/guest.php

4.4.5.1.6. 免用户认证

免用户认证是指访问无线网络时，访客无需认证，在广告页面点击登录按钮即可上网。

访客连接无线网络的过程如下：

1、连接到访客无线网络，例如无线网络名称为：Example-Guest。

2、打开浏览器，访问任意网站，系统将把用户的浏览器重定向到认证页面。

3、认证页面中，用户点击登陆，直接上网。

免用户认证方式的优点：

1、认证页面中，可以设置企业的广告等展示信息，提高企业形象。

2、简化了访客连接无线网络的体验。

4.4.5.1.7. 社交应用认证

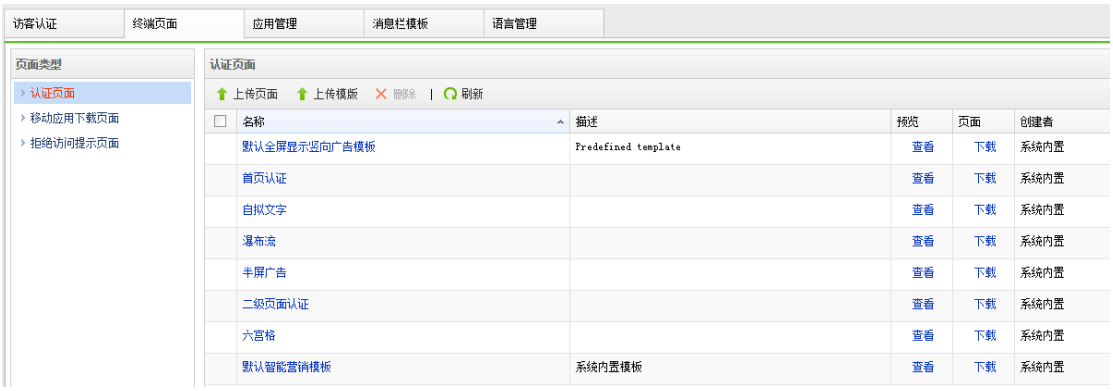
此方式通常用于海外或港澳台等地区，终端用户可以使用 Facebook，Twitter，Line，Live，Instagram 账号进行授权，授权后关注商家账号即可通过认证。

通常，通过认证的用户，控制器可以获取到用户的用户 ID、用户名、终端 MAC 地址、邮箱地址、性别、年龄段等。但上述字段在用户没有配置的时候，是获取不到的。

配置社交应用认证时，认证前需要放通对应流量，推荐使用内置角色进行认证。

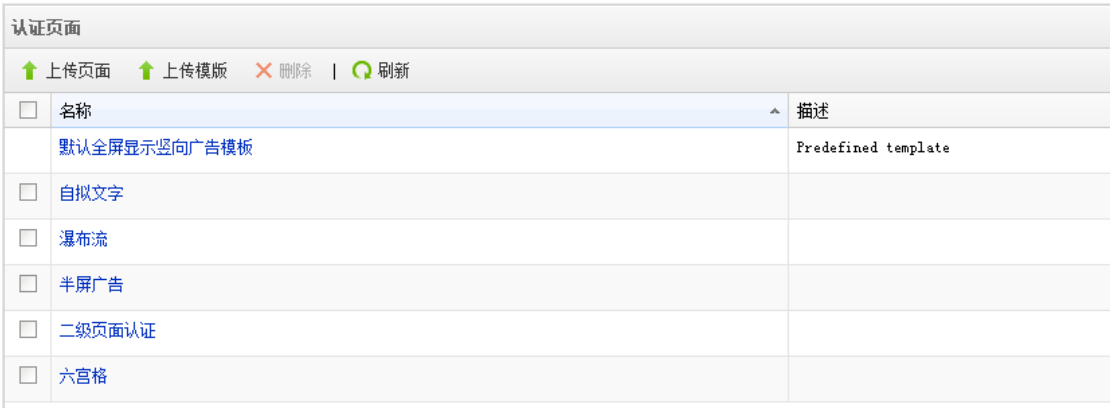
4.4.5.2. 终端页面

【终端页面】分为“认证页面”、“移动应用下载页面”、“拒绝访问提示页面”。



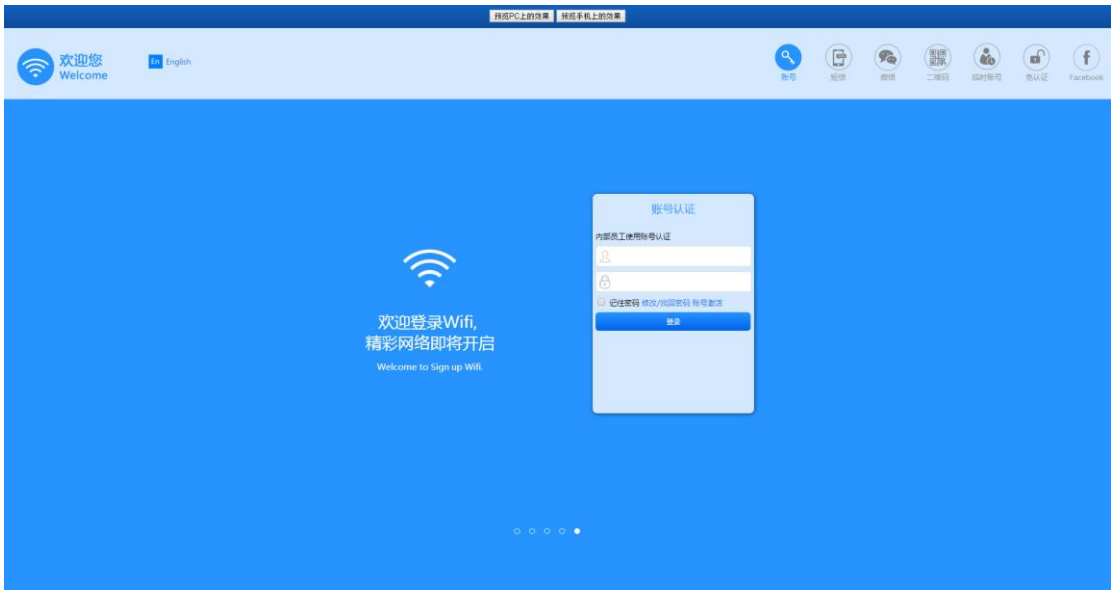
4.4.5.2.1. 认证页面

“认证页面”用于设置无线用户接入无线网络后，设置 WEB 认证跳转的页面，系统内置了 Web 认证页面的模板，系统允许您在默认模版的基础上，自定义认证页面的标题，背景，LOGO 等。如果您熟悉 Web 开发，可以上传自定义的页面。



1、默认全屏显示竖向广告模板

预览电脑认证效果图：



预览手机认证效果图：

2、自拟文字

预览电脑认证效果图：

预览手机认证效果图：

3、瀑布流

预览电脑认证效果图：

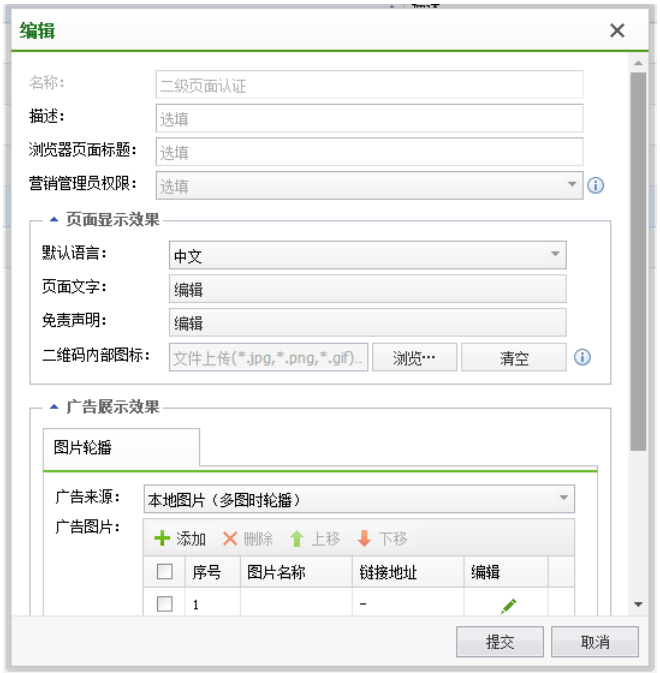
预览手机认证效果图：

4、半屏广告

预览电脑认证效果图：

预览手机认证效果图：

5、二级页面认证



预览电脑认证效果图：

预览手机认证效果图：

6、六宫格


编辑
二维码内部图标：
文件上传(*.jpg,*.png,*.gif)..
浏览…
清空
广告展示效果
图片轮播
六宫格
无线防钓鱼
营销推广
防终端拖滞
基于行为推广
终端类型识别
统一认证平台
提交
取消

预览电脑认证效果图：


客流分析
用户流动信息一手掌握
客流分析
无线防钓鱼
营销推广
防终端拖滞
基于行为推广
终端类型识别
统一认证平台
认证上网

预览手机认证效果图：

7、默认智能营销模版

智能营销模板支持更加丰富的区域显示规则，帮助营销人员结合天气环境情况，推送与顾客直观感受相吻合的广告内容，能让每个顾客看到与自己相关的"专属"信息，做到千人千面的展示效果。

支持一套模板多个门店使用，且不同门店展示不同广告内容。每个门店(单条显示规则）均支持引用接入点分组并配置多张广告图片，每张广告图片可以设定不同环境属性、用户属性、所在位置、推送时间进行智能展示。

支持每个显示规则引用不同的消息栏，以个性化的展示消息栏信息。消息栏信息可以在消息栏模板页面进行配置。

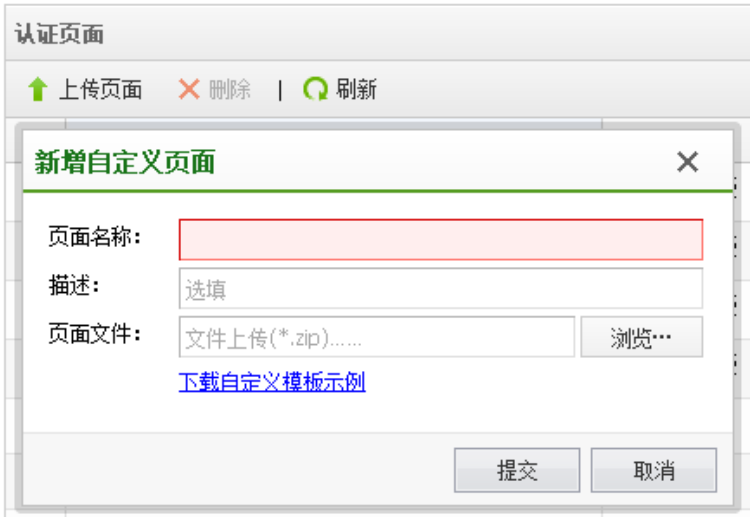
统一配置：在总部、多个门店场景下，可以启用统一配置，用于在指定生效时间内强制展示总部设定的广告内容，若部分门店不展示总部统一广告可以进行排除。

注：统一配置禁用或生效时间外，各门店恢复显示门店设定的独立广告内容。

页面效果图，参考“默认全屏显示竖向广告”。

4.4.5.2.2. 上传自定义页面

如果系统默认的认证页面还不能满足需求，还可以自定义页面，自定义页面需要下载“自定义模版示例”，按照示例标准进行上传页面



4.4.5.2.3. 访问拒绝页面

当用户被访问控制策略拒绝时，可以启用页面返回，提示用户访问被拒绝，也可以自定义编辑。

4.4.5.2.4. 移动应用下载页面

当您需要做手机应用推广时，需要先创建一个移动应用下载页面。在无线网络设置认证后跳转页面，勾选 APP 推广，再选择此处创建的页面。如果您使用了 APP 推广，别忘了在无线网络设置中开启应用缓存加速，这将大大节省您的网络带宽资源，提升终端下载体验。当前适配 IOS 和 Android 移动终端，移动终端访问时可直接下载，PC 端访问时将显示一个二维码图片，提示用户使用移动终端扫码下载。

4.4.5.3. 应用管理

应用管理用于配置各种社交软件做认证时所要对接的应用，以让不同社交软件的用户使用自己的社交账号接入 wifi。同时支持 like 功能，实现商超客户的品牌推广，目前支持 like 的社交软件有 Facebook，Twitter 和 Line。

4.4.5.4. 消息栏模版

消息栏的展示文字在终端页面的顶部，可以根据识别出的终端用户的系统语言，对应展示其相符合的语言文字。消息栏内容支持展示天气、室内外温度、湿度、PM2.5，使终端用户能直观在认证页面看到当前所处场所的环境信息。

通过修改内置消息栏模板文字，或者新增消息栏模板，可以由客户定义想要给终端用户展示的内容。

注意，此处的模板内容和语言管理中的语言模板内容相互独立，以便客户快速编辑。

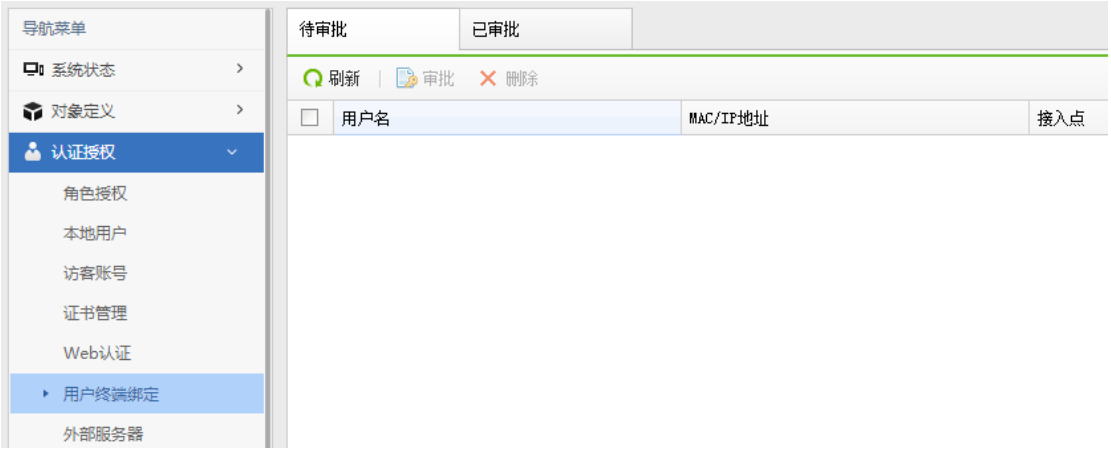
4.4.5.5. 语言模版

有中文（简体）和英文两个默认模板，客户可以根据应用场景，添加语言模板，使终端认证页面显示出更多的语言。

在添加其他国家或者区域的语言前，需要先下载英文模板，然后在英文模板的 json 中，将对应的英文内容修改为需要展示的语言内容。

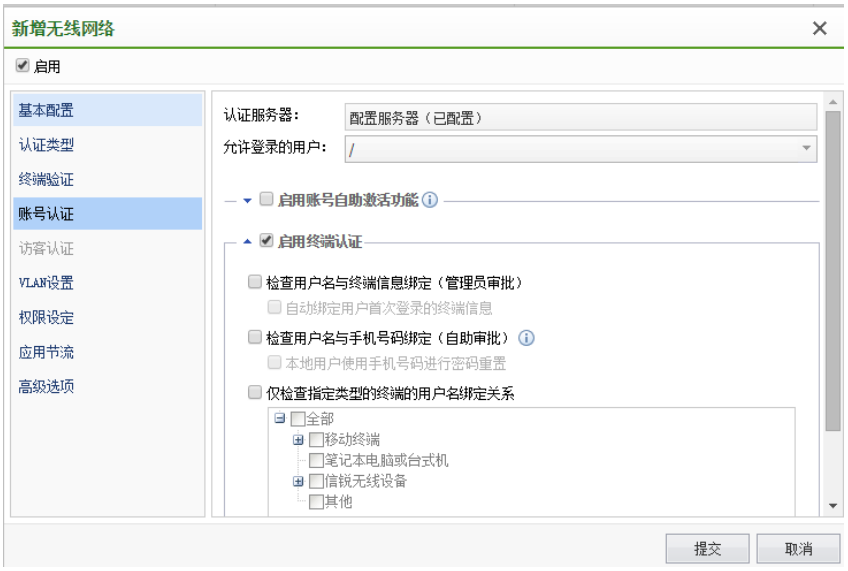
4.4.6. 用户终端绑定

设置用户与终端绑定信息，相关的验证设置请在认证选项/策略中开启。支持终端绑定功能的有无线网络认证、有线认证和 Portal 服务认证策略。支持“终端绑定”、“手机号码绑定”、“手机号码绑定、终端绑定”。



此页面中仅定义了用户终端的绑定关系，要启用绑定关系检查功能，还需要在【接入点配置】-【无线网络】-【编辑无线网络】-【账号认证】中勾选【启用终端认证】并且勾选【检查用户名与终端信息绑定】或【检查用户名与手机号码绑定】。

一个用户，最多支持绑定在 5 个 MAC 地址上，一个 MAC 可以绑定的用户名个数不受限制。用户名和 MAC 地址绑定都是双向绑定的关系。



用户终端绑定关系，可以通过以下几种方式创建：

1、手动添加：管理员通过手动添加或者 csv 表格文件导入方式，提供用户名与 终端信息的绑定关系。在有大量终端需要管理的环境中，这种方式的缺点是较大的管理工作量。

2、自动添加：无线网络中，可以设置为：用户第一次登录时，自动绑定登录的终端。此方式以牺牲少量的安全性作为代价，减少了管理工作量。

3、管理员审批：对于未授权终端上的登录请求，系统会拒绝此用户连接，并且把终端的信息加入到待审批列表中，网络管理员以人工审批的方式，来决定是否允许此未终端接入。

4.4.7. 外部服务器

『外部服务器』包括【认证服务器】、【虚拟服务器】

4.4.7.1. 认证服务器

如果企业已部署集中的用户数据库，或者认证服务器，无线网络可选择使用外部服务器来完成用户身份验证。

使用 WAPI 企业认证的无线网络，需要在 AS 服务器上面进行用户身份的验证。

802.1x 认证的企业无线网络，支持使用 RADIUS 中继的方式，把认证请求中继到外部的 RADIUS 服务器，完成用户验证。web 认证的无线网络，支持通过外部的 RADIUS 服务器或 LDAP 服务器，完成用户身份验证。第三方 PORTAL 认证的无线网络，对接外部的 PORTAL 服务器完成认证。

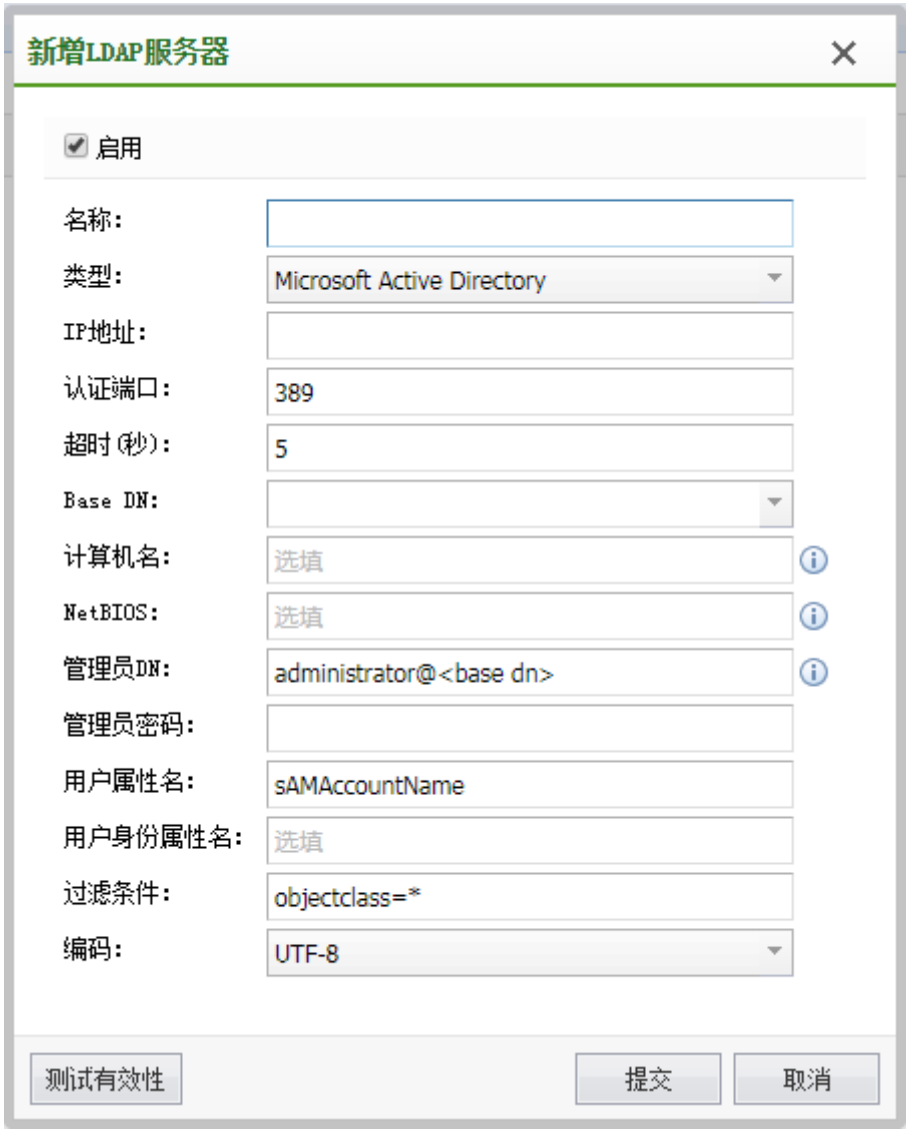
4.4.7.1.1. Radius 服务器

『新增 Radius 服务器』需要设置“名称”、“IP 地址”、“认证端口”、“计费端口”、“超时”、“共享密钥”、“采用协议”、“编码”，可选配置“NAS_ID”、“NAS_IP”、“用户身份属性 ID”，如下图：

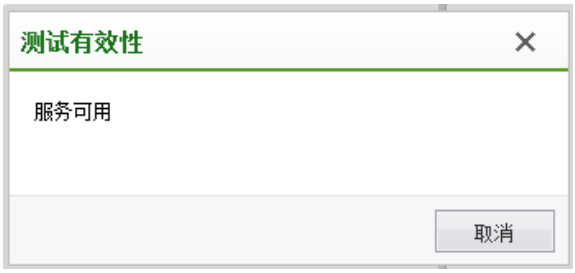
设置 Radius 服务器的时候可以另外设置获“取用户属性”，企业级认证时，NAC 会去用户数据库中去获取用户的组织结构，来作为无线终端的用户名和组织结构。这里可以选择与 radius 服务器对应的 LDAP 服务器。

4.4.7.1.2. LDAP 服务器

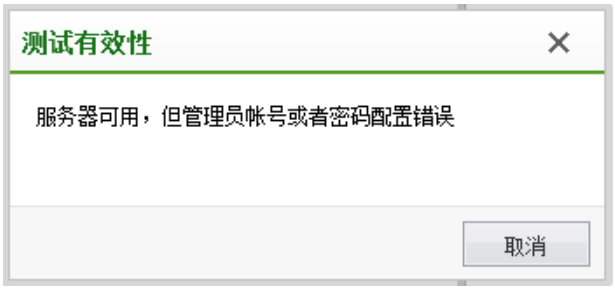
『新增 LDAP 服务器』：设置 LDAP 服务器需要设置“名称”、“类型”、“IP 地址”、“认证端口”、“超时（秒）”、“Base DN”、“管理员 DN”、“管理员密码”，可选填“计算机名”、“NetBIOS”，“用户属性名”、“用户身份属性名”、“过滤条件”和编码，如无特殊需求，保持默认即可。



配置完成后，可以点击测试有效性，测试 LDAP 服务器是否配置正确，如果服务器 IP 配置以及用户名和密码都配置正确，会提示服务器可用，如下图：

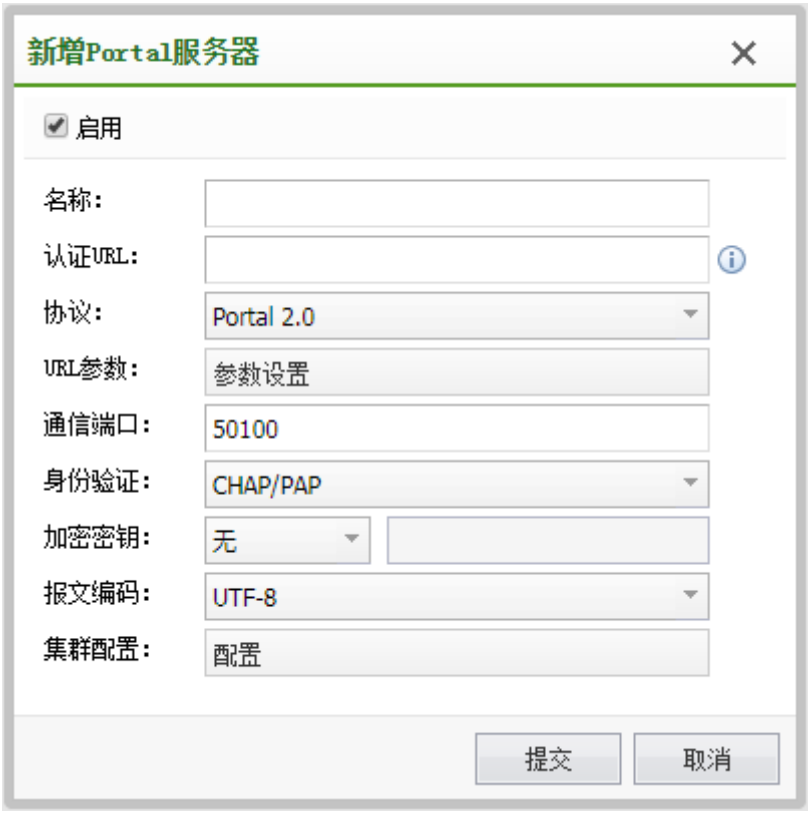


如果服务器 IP 配置都正确，用户名和密码配置格式不对或用户名和密码错误，会提示“服务器可用，但管理员账号或密码配置错误”。如下图：



4.4.7.1.3. Portal 服务器

添加外部 Portal 服务器，可以实现无线用户通过外部 Portal 服务认证上网。设置 Portal 服务器需要设置“名称”、“认证 URL”、“协议”、“URL 参数”、“通信端口”、“身份验证”、“加密密钥”、“报文编码”。



认证 URL：

PORTAL 服务器的 url 为终端接入无线网络时，被重定向到的地址。其中 urlid 可以使用占位符来扩展，占位符为：，占位符的值可以在认证服务器->Portal 服务器设置中配置。

认证 URL 支持配置为 IP 的形式和域名的形式。

认证 IP：

Portal 服务器的通信 IP，会自动从认证 URL 中提取

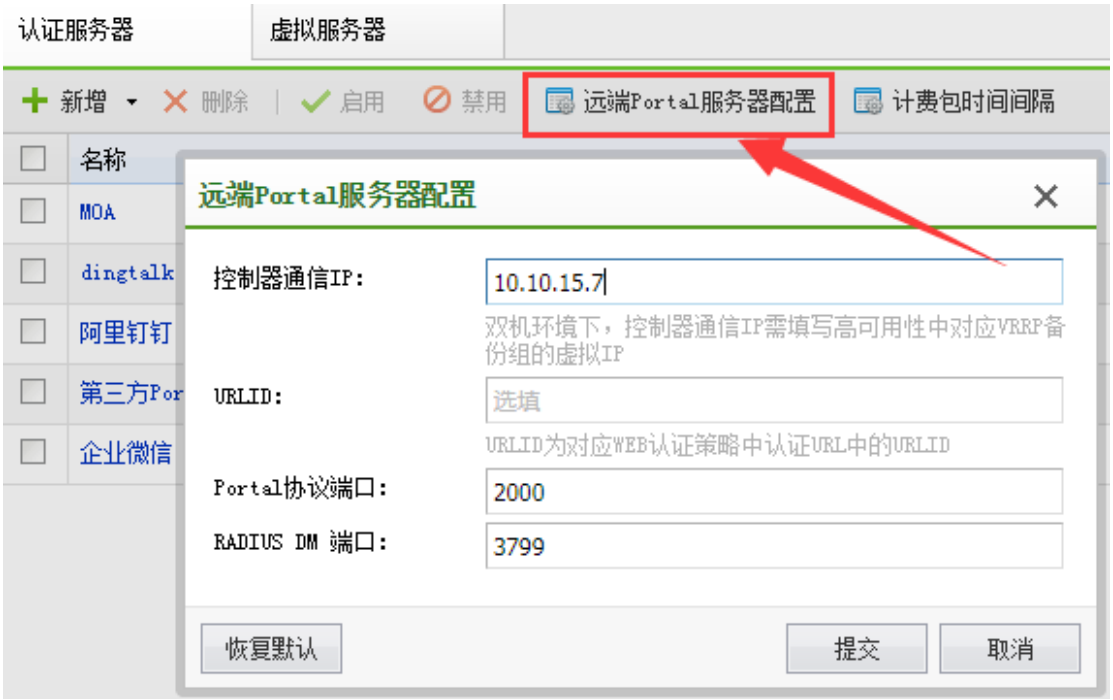
协议：

对接的 Portal 服务器类型，类型不在里面的，请选择 Portal 2.0 协议

URL 参数：

勾选某个参数类型，参数类型后面的输入框为自定义的参数名称。如勾选 SSID，自定义名称为 wlanssid，终端接入认证时，认证 URL 将会是：http://1.1.1.1:8080/portal/?wlanssid=xxx， ‘xxx”为终端接入的 SSID 名称。

远端 Portal 服务器配置:



控制器通信 IP：对接 Portal 服务器时，当前控制器作为 Portal 客户端，服务器会主动和当前控制器通信。通信 IP 是服务器主动访问客户端使用的 IP。

双机环境下，建议配置为高可用性中对应 VRRP 备份组的虚拟 IP。

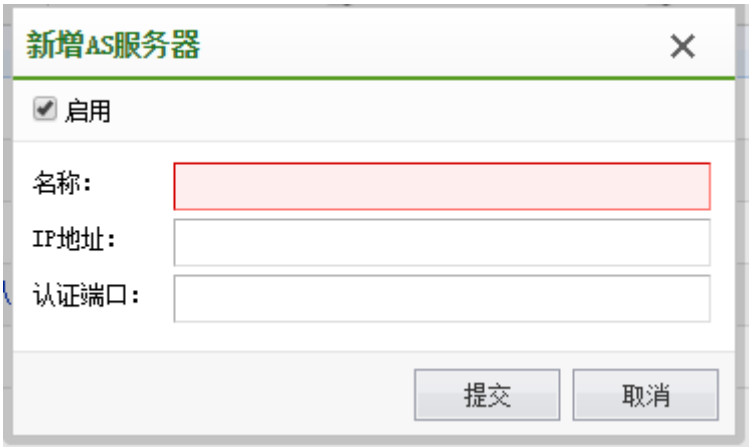
URLID：URLID 为对应 WEB 认证策略中认证 URL 中的 URLID。

Portal 协议端口：客户端监听的 Portal 服务端口。

RADIUS DM 端口：RADIUS 服务器主动下线一个用户时，使用的端口。

4.4.7.1.4. AS 服务器

AS 服务器适用于 WAPI 企业认证的无线网络中，作为外部认证服务器。



名称：AS 服务器的名称

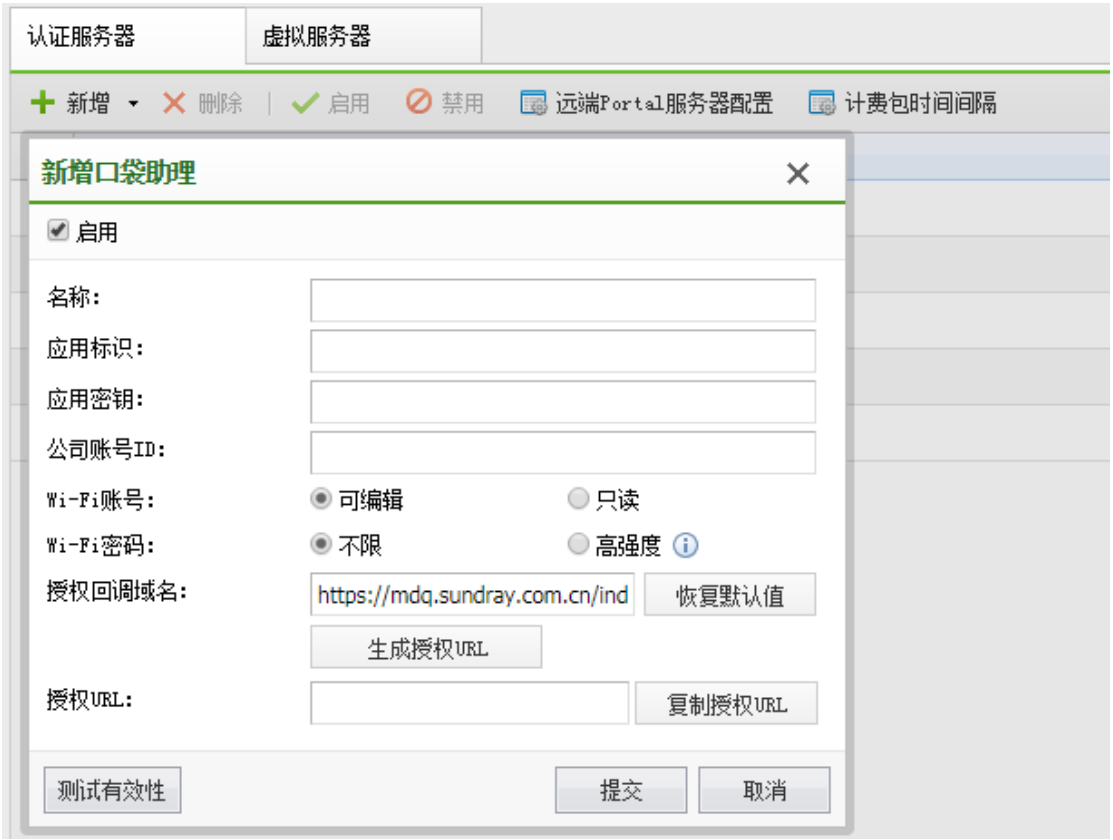
IP 地址：AS 服务器的 IP 地址

认证端口：服务器的认证端口，一般默认为 3810

4.4.7.1.5. 口袋助理

口袋助理认证是指将口袋助理移动办公平台作为认证服务器，用户通过使用口袋助理上创建的上网账号完成认证，实现无线上网账号与口袋助理的对接，便于用户对无线上网账号进行实时管理。

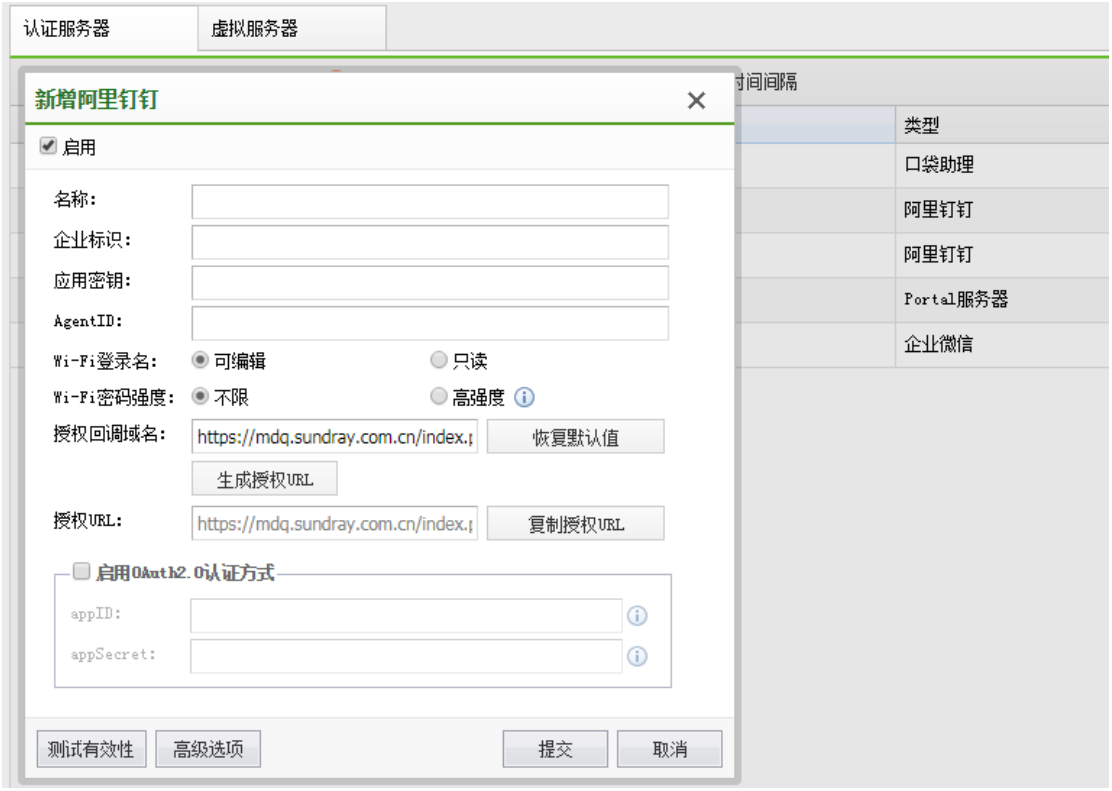
适用认证方式：1）WPA/WPA2 企业认证； 2）WEB 认证 - 账号认证



4.4.7.1.6. 阿里钉钉

阿里钉钉认证是指将阿里钉钉移动办公平台作为认证服务器，用户通过使用钉钉上创建的上网账号完成认证，实现无线上网账号与阿里钉钉的对接，便于用户对无线上网账号进行实时管理。

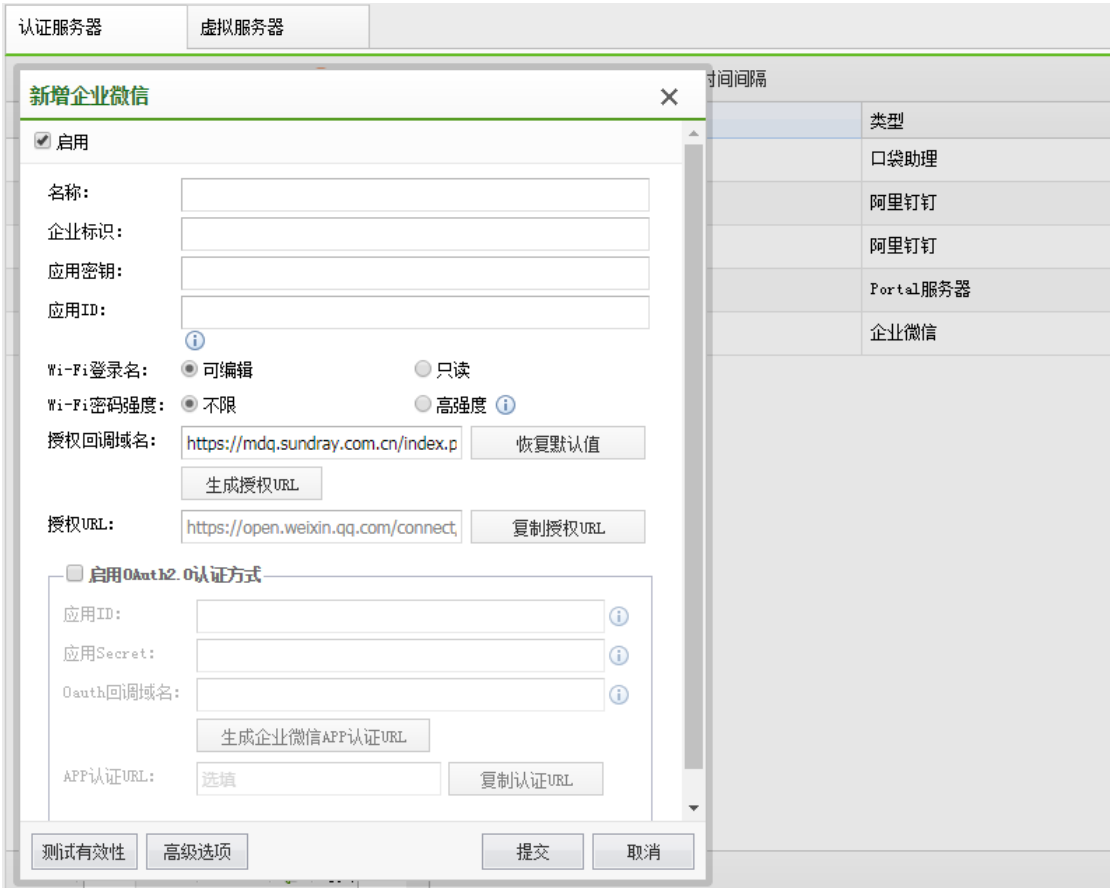
适用认证方式：1）WPA/WPA2 企业认证； 2）WEB 认证 - 账号认证



4.4.7.1.7. 微信企业号

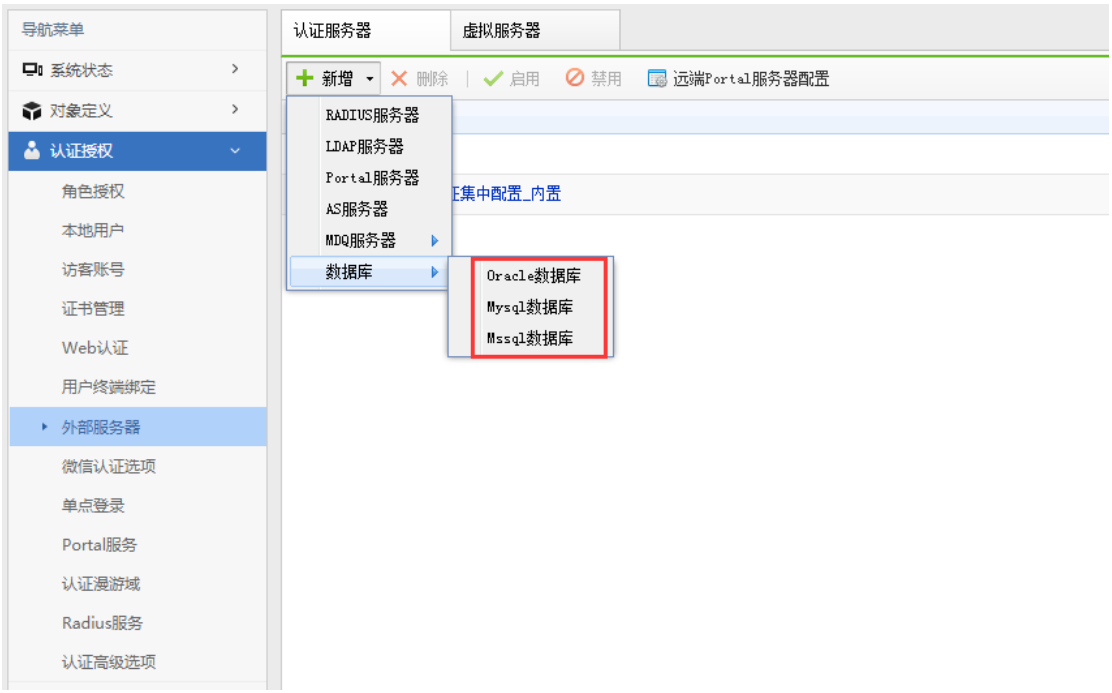
微信企业号认证是指将微信企业号移动办公平台作为认证服务器，用户通过使用微信企业号上创建的上网账号完成认证，实现无线上网账号与微信企业号的对接，便于使用微信企业号办公的用户对无线上网账号进行实时管理。

适用认证方式：1）WPA/WPA2 企业认证； 2）WEB 认证 - 账号认证



4.4.7.1.8. 数据库

目前无线控制器直接对接 Oracle 数据库、Mysql 数据库以及 Mssql 数据库，实现帐号认证和企业级认证



1、基本配置

基本配置是用于连接数据库的信息。

（1）名称：数据库认证服务器的名称。

（2）IP 地址：数据库的服务器地址。

（3）端口：数据库服务器使用（监听）的端口。

（4）超时（秒）：向数据库服务器查询用户信息时的查询超时时间。

（5）数据库名/SID：数据库中保存用户信息的数据库（数据库实例）的名称。

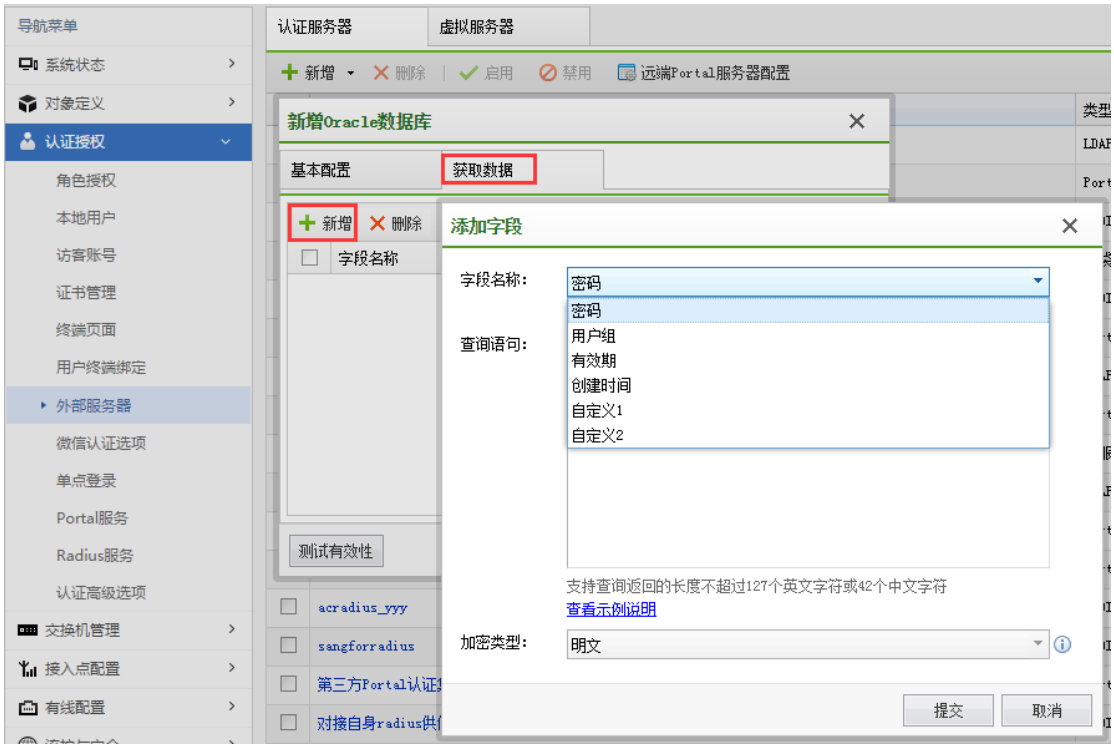
（6）管理员帐号：登录数据库的账号，该账号需要有查询“数据库名”指定的数据库的权限。

（7）管理员密码：登录数据库的账号对应的密码。

2、获取数据

用于配置获取数据库信息的 SQL 语句，支持 6 个字段信息的获取；

SQL 语句中使用$$USERNAME$$代表用户登录名。



（1）密码（必填）：用于查询用户的密码，作密码校验。portal 认证支持明文、MD4、MD5、SHA1、NT-Password 加密类型。企业认证支持明文、NT-Password。

（2）有效期和创建时间（可选）：用于校验用户是否有效。如果只配置有效期字段，具体使用方法见[外部数据库获取创建时间和有效期]。

（3）用户组（可选）：用于获取用户组做 vlan 匹配、权限匹配（无线网络配置）。支持中文编码，具体见[外部数据库对中文编码的支持]。

3、外部数据库对中文编码的支持

（1）用户名支持设置中文编码。

（2）用户组、自定义 1、自定义 2 这三个查询字段支持使用中文编码。

（3）支持的中文编码格式如下（UTF-8 是最为通用的格式；GBK 是常用的简体中文编码格式，BIG5 是常用的繁体中文编码格式）：

ORACLE:支持 UTF-8、GBK、BIG5

MYSQL:支持 UTF-8、GBK、BIG5、GB2312

SQLSERVER:支持 UTF-8、UCS-2、简体中文、繁体中文

4、外部数据库获取创建时间和有效期

WAC 支持%Y、%m、%d、%H、%M、%S 几个通配符，使用通配符在自定义格式中填写与数据库中内容同样的格式，WAC 就能够识别，其意义分别为：

%Y 年、%m 月、%d 日、%H 时、%M 分、%S 秒

根据数据库中的内容是字符串和内置格式，分别有不同的处理方式（根本目的都是转化

为字符串形式）

情况 1:字符串格式

数据库中的时间格式的类型是字符串，则使用匹配符按照本地的字符串的样式得到对应的格式；

例如数据库的时间内容是 2017-10-20 10:30:50，则自定义格式填%Y-%m-%d %H:%M:%S；

例如数据库的时间内容是 10:30:50,2017,10,20，则自定义格式填%H:%M:%S,%Y,%m,%d。

情况 2:内置时间格式

数据库中的时间类型是数据库内置的时间格式，则需要将内置时间格式转为指定的字符串格式。不同数据库有不同的转换处理函数；

a、对于 oracle，时间字段使用的是时间格式（包括 date、timestamp），使用 TO_CHAR 进行转换；

SELECT TO_CHAR(时间字段名, 'yyyy-mm-dd hh24:mi:ss') FROM EXTDB_USER_TB WHERE USERNAME = $$USERNAME$$；

格式中填写:%Y-%m-%d %H:%M:%S。

b、对于 mysql，时间字段使用的是时间格式（包括 date、datetime、timestamp），直接按照情况 1 处理即可 oracle 的 timestamp；

因为 mysql 查询到的内容直接就是 2019-10-20 10:30:50 或者 2019-10-20 形式的字符串。

c、对于 sqlserver，时间格式是 datetime，则使用 CONVERT 将 datetime 格式转为字符串（2017-01-01 12:00:00）的格式；

SQL 语句:SELECT CONVERT(nvarchar(24), 时间字段名, 20) FROM 表名 WHERE 用户名字段名 = $$USERNAME$$;

格式中填写:%Y-%m-%d %H:%M:%S。

d、对于 sqlserver，时间格式是 datetime 之外的格式，则使用 CAST 将其强制转换为 datetime，再使用 CONVERT 进行转换；

SQL 语句:SELECT CONVERT(nvarchar(24), CAST(时间字段名 AS DATETIME) FROM 表名 WHERE 用户名字段名 = $$USERNAME$$;

格式中填写:%Y-%m-%d %H:%M:%S。

5、外部数据库其它复杂 SQL 语句示例（SQLSERVER）

（1）联表查询

用户名和需要查询的内容（例如用户组）在不同的表中，需要使用外键进行关联查询

示例：

a、用户表 usertb 的内容如下，

id	username	grp_fk
1	test1	2

b、用户组表 grptb 的内容如下，

id	groupname
2	sundray

c、SQL 语句：

SELECT grptb.groupname FROM usertb,grptb WHERE usertb.username = $$USERNAME$$ and usertb.grp_fk = grptb.id;

（2）内容以键值对的形式保存（例如一些 radius 服务器），利用 max case 做“行转列”处理

示例：

a、用户表 usertb 的内容如下，我们需要提取其中的 attribute 列中，内容为"password"的行所对应的 value 作为密码

username	attribute	value
test1	password	pwd
test2	group	sundray

b、SQL 语句：

SELECT MAX(CASE WHEN attribute='password' THEN value ELSE ' ' END) AS MY_PASSWORD FROM usertb WHERE username = $$USERNAME$$

（3）截断用户名

因为 WAC 支持的用户名长度不能超过 95，如果数据库中的用户名长度超过 95，就需要将过长的用户名作截断。这种情况下可以使用 SUBSTRING 处理。

示例：

SELECT 密码字段名 FROM 表名 WHERE SUBSTRING(用户名字段名, 1, 95) = $$USERNAME$$

（4）去掉用户名前后缀

数据库中的用户名有一些前后缀，例如 XXX@sundray.com、sundray_XXX，我们想要用户使用 XXX 登陆。这种情况下可以使用 SUBSTRING 处理。

示例 1：

a、用户表 usertb 中的用户名都是 XXX@sundray.com 的形式，我们想要用户使用 XXX 登陆

b、SQL 语句 1：

SELECT 密码字段名 FROM 表名 WHERE

SUBSTRING(用户名字段名,

1,

(

CASE WHEN CHARINDEX('@sundray.com', USERNAME)=0 THEN

LEN(用户名字段名)

ELSE

CHARINDEX('@sundray.com', USERNAME)-1

END

)

) = $$USERNAME$$

示例 2：

用户表 usertb 中的用户名都是 XXX@sundray.com 的形式，我们想要用户使用 XXX 登陆

SQL 语句 1：

SELECT 密码字段名 FROM 表名 WHERE

SUBSTRING(用户名字段名,

(

CASE WHEN CHARINDEX(REVERSE('sundray_'), REVERSE(用户名字段名))=0 then

1

ELSE

2+len(用户名字段名)-CHARINDEX(REVERSE('sundray_'), REVERSE(用户名字段名))

END

),

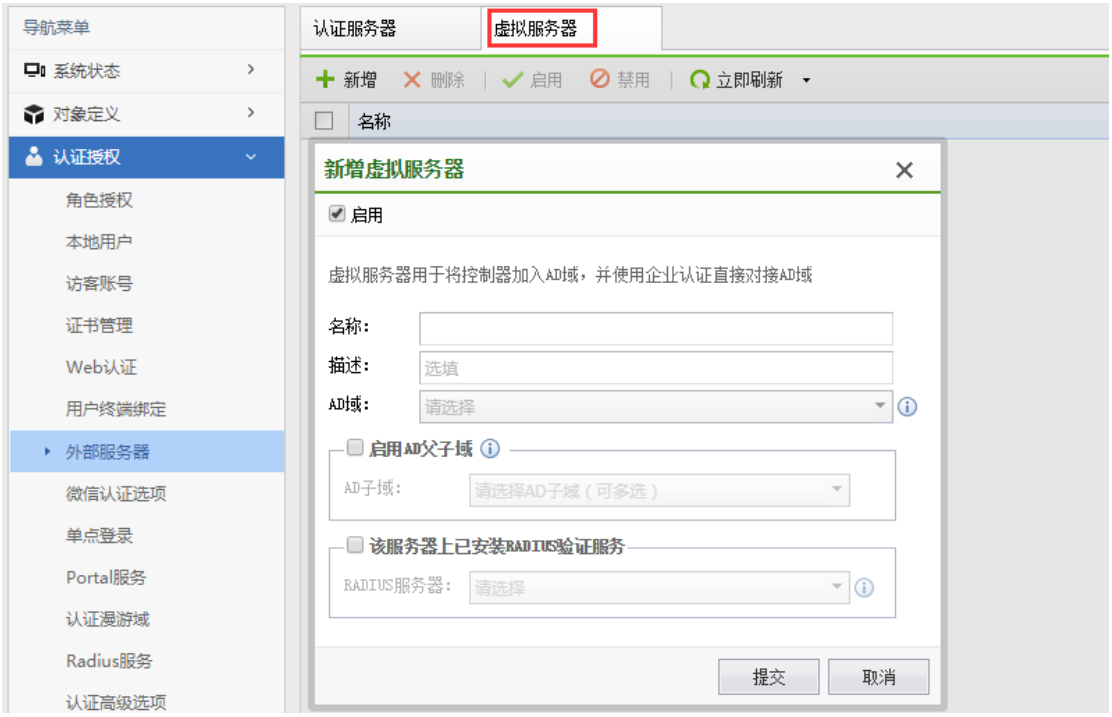
)LEN(用户名字段名)

) = $$USERNAME$$

4.4.7.2. 虚拟服务器

如果企业已部署多台微软 AD 域控制器且互相之间存在父子域关系，无线网络可选择使用虚拟服务器来完成用户身份验证。

虚拟服务器支持 TTLS-PAP 认证以及 EAP-MSCHAPv2 认证。



4.4.7.2.1. 未安装 RADIUS 验证服务虚拟服务器

适用于 WPA/WPA2 企业认证及 802.1X 无线网络的终结认证，需要用户启用 netbios 服务以支持对接 AD 域。

名称：虚拟服务器名称

AD 域：选择 AD 域服务器配置(可为父域或独立域)

AD 子域：选择与已添加 AD 域存在子域关系的 AD 域服务器配置

4.4.7.2.2. 已安装 RADIUS 验证服务的虚拟服务器

若用户不愿启用 netbios 服务且已安装 RADIUS 验证服务，用户可选择启用“该服务器上已安装 RADIUS 验证服务”对接 AD 域。

名称：虚拟服务器名称

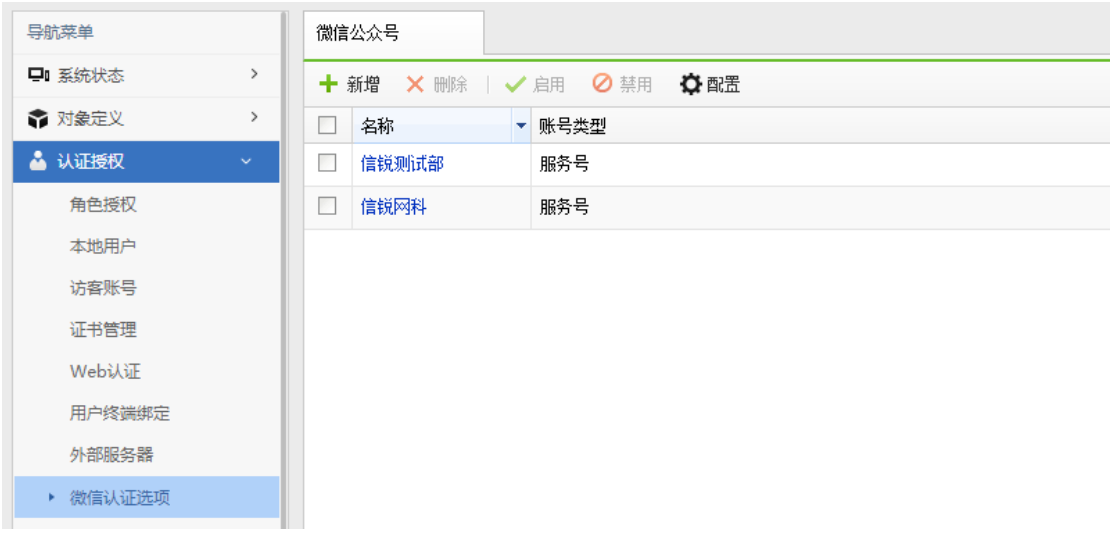
AD 域：选择 AD 域服务器配置(可为父域或独立域)

AD 子域：选择与已添加 AD 域存在子域关系的 AD 域服务器配置

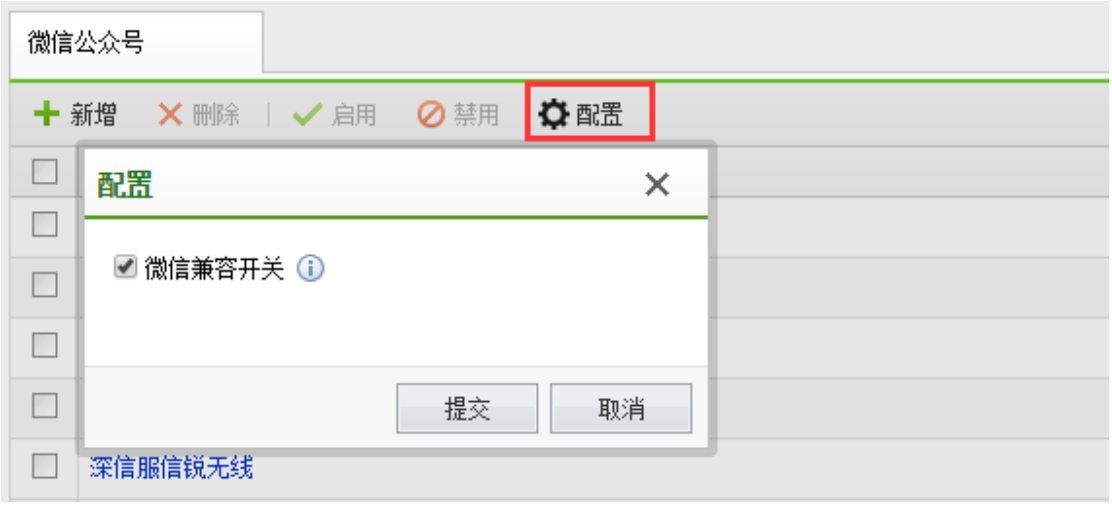
RADIUS 服务器：选择已在配置的 AD 域中注册 RADIUS 服务器

4.4.8. 微信认证选项

配置微信认证、微信推广功能，需要先配置好微信公众平台。



微信兼容性开关



第三方公众平台如果没有升级到 2.0 及其以上版本，需要开启此开关（默认为启用状态），否则微信认证方式将不能正常使用。

4.4.8.1. 微信推广功能

推广功能需要微信公众账号类型为服务号，且账号处于开发者模式。推广功能使用注意事项：

A、微信公众平台默认仅对保持关注且 48 小时内与公众平台有任何主动联系业务的用户才提供主动推广消息业务，超过这个限制用户将无法接收该消息；

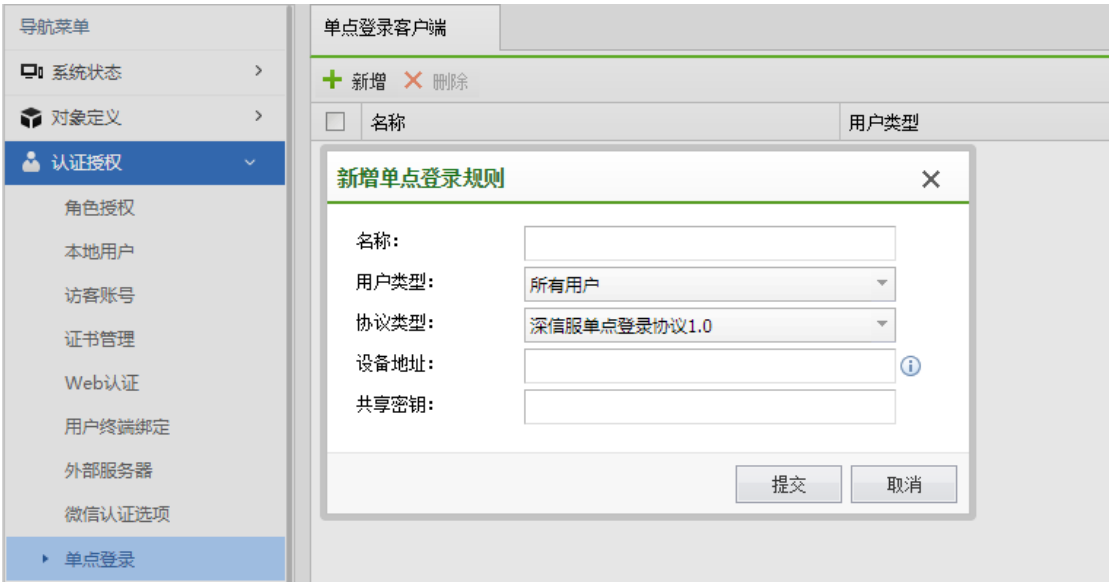
B、使用本功能请确认使用的第三方公众平台不会使用高级接口 access token,或者对应的第三方公众平台可以提供 access token 获取功能，否则将造成 access token 快速耗尽，导致本功能或者第三方公众平台异常（比如：微盟、微购等）。

4.4.9. 单点登录

单点登录，将用户的认证信息发送到深信服上网行为管理设备，避免终端通过控制器认证后，还需要再次认证。

1、本地转发，请在接入点（编辑->参数配置->其他配置）或者接入点分组（编辑->其他配置）中 ，配置认证信息转发。

2、集中转发和有线认证，由控制器转发认证信息，需要在该页进行配置。



4.4.9.1. 用户类型

无线用户：无线用户，包括本地转发和集中转发的用户

控制器有线用户：在控制器上完成有线认证的用户

接入点有线用户：完成接入有线认证的用户

所有用户：包括无线用户、控制器有线用户、接入点有线用户。

4.4.9.2. 协议类型

深信服单点登陆协议 0.1：深信服上网行为管理设备使用的单点登陆协议（AC11.0 之前版本支持），协议默认使用 1773 端口。

深信服单点登陆协议 1.0: 深信服上网行为管理设备使用的单点登陆协议（AC11.0 及后续版本支持），协议同时兼容 0.1 版本。协议默认使用 1775 端口。

深信服上网行为管理的配置菜单如下：

4.4.10. Portal 服务

控制器可作为 Portal 服务器为第三方设备提供 Portal 认证服务。

4.4.10.1. 服务器参数

无线控制器内置 Portal 服务器，Portal 服务器运行的必要参数。

协议端口：Portal 服务器监听的协议端口。

服务器通信 IP：当前控制器的通信 IP，双机部署时建议配置为 VRRP 中的虚拟 IP。

认证页面端口：默认是 80，配置为非 80 端口时，客户端配置 Portal 服务器的 URL 时需要带上端口号。

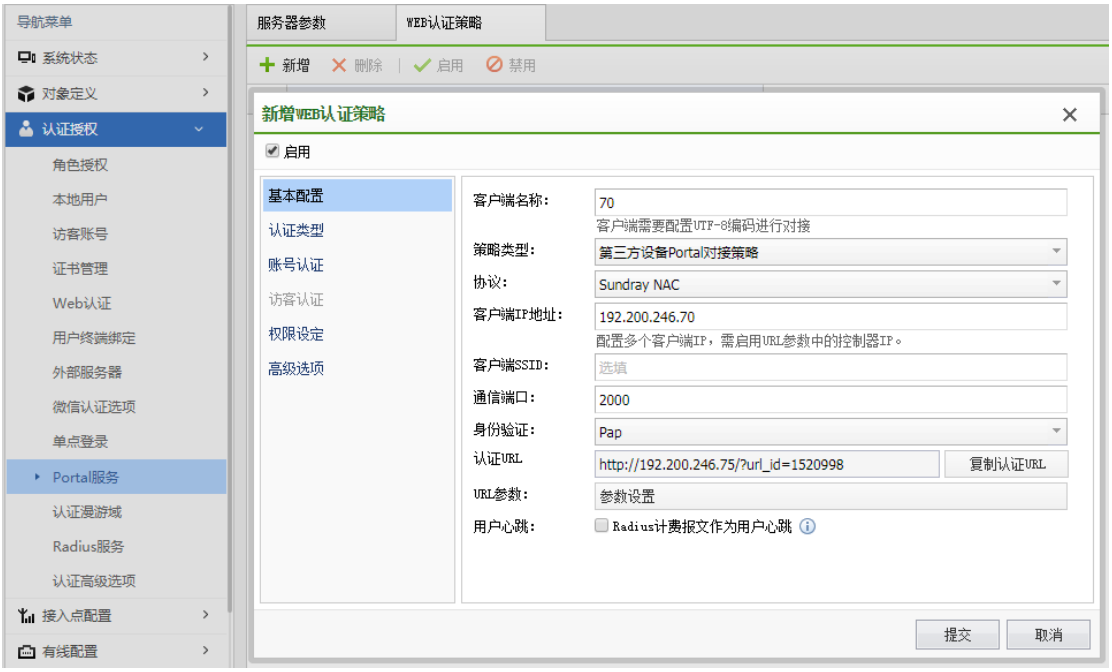
在线用户同步时间（分钟）：Portal 服务器主动向客户端同步用户的时间，针对 Aruba 和 Cisco 设备。

在线用户保留时间（小时）：超过保留时间，注销所有的在线用户。

Portal 页面超时重定向地址：Portal 页面超时（在 URL 参数中设置时间戳参数）后系统自动重定向的地址.

4.4.10.2. WEB 认证策略

WEB 认证策略给当前控制器的有线认证，第三方的 Portal 客户端（包括信锐控制器）对接时，配置认证页面、认证方式、权限设定方面的信息。



策略类型：分为第三方设备 Portal 对接策略和控制器有线认证策略。第三方设备 Portal 对接是指给当前设备的无线网络对接，第三方（包括信锐控制器）的 Portal 客户端对接。控制器有线认证策略是指给当前控制器的有线策略提供对接。

协议：当前 Portal 服务器支持对接的设备厂商类型和协议版本。不在列表里面的请选择 Portal2.0 标准协议。

身份验证：身份验证方法，包括 PAP 和 CHAP，这里的配置需要和客户端配置的 RADIUS 服务器的身份验证方法保持一致才能认证成功。

认证 URL：需要将这个 URL 拷贝到 Portal 客户端的认证 URL 里面去，客户端配置的和这里的不一致时，将会认证失败。

参数设置：Portal 客户端的认证 URL 里面携带的参数的名称。

开启本地认证（在控制器进行用户认证）：Portal2.0 协议里面，Portal 服务器和认证服务器可以分开配置。当 Portal 服务器启用了访客认证时，客户端的 RADIUS 服务器需要配置为当前控制器。

权限匹配：Portal 服务器对接有线认证时，权限匹配的结果就是有线认证的角色。提供给第三方设备 Portal 对接时，匹配到的角色将会通过 RADIUS 报文中的 Class 字段，以字符串的形式返回给 RADIUS 客户端。

4.4.11. 认证漫游域

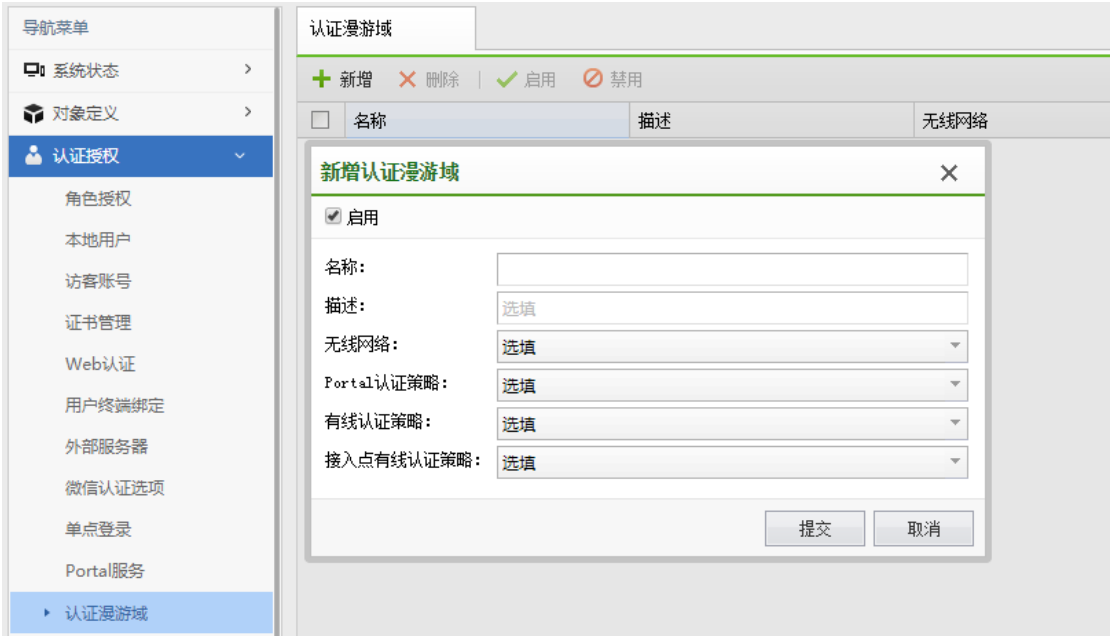
认证漫游域主要解决如下问题：

1、客户有多台不同厂商的 portal 客户端，终端在客户端 A 上认证成功后，漫游到控制器 B 后需要重新认证；

2、客户的第三方设备级联到控制器的接口做有线认证后，漫游到控制器的其他 ssid 上后需要重新认证。

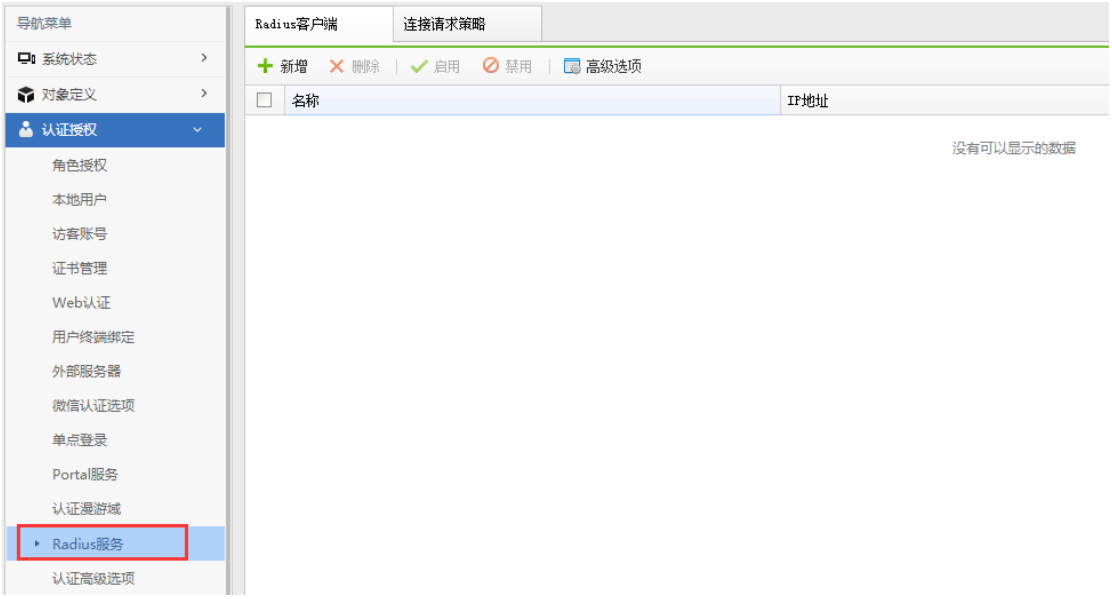
配置认证漫游域后，支持终端在不同类型的 portal 服务器上漫游；支持不同类型认证方式之间的漫游。

注意：只有相同的认证服务器的认证策略才能添加到一起，并且只支持账号认证，访客认证本身就支持漫游。



4.4.12. **Radius 服务**

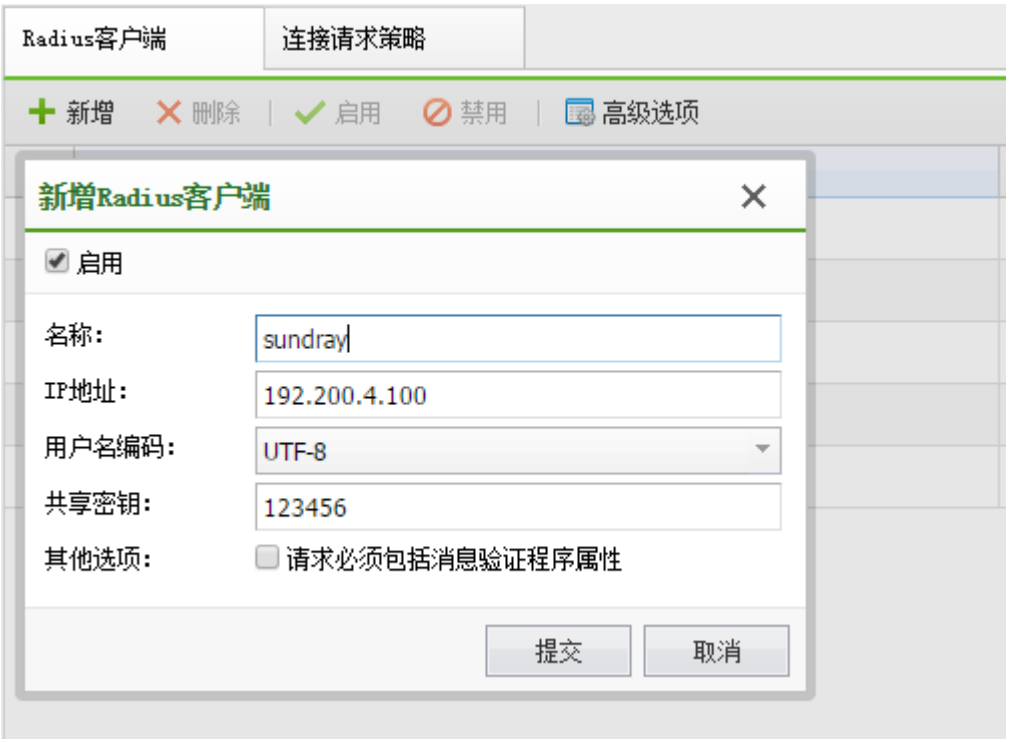
Radius 服务器负责接收客户端的连接请求、认证用户，然后返回客户端所有必要的配置和认证信息。



4.4.12.1. Radius 客户端

NAC 作为 Radius 服务对客户端进行认证和计费时，需要配置信任的客户端；

NAC 作为 Radius 客户端需要配置认证的服务器时请在外部服务器进行配置。



1、Radius 客户端—名称

Radius 客户端的名称，用于区分不同的 Radius 客户端。

2、Radius 客户端—IP 地址

客户端的 IP 地址，双机部署时建议配置为 VRRP 中的虚拟 IP。

3、Radius 客户端—用户名编码

服务器和客户端之前数据传输的编码类型，两端的编码一致才能保证验证的有效性。

4、Radius 客户端—共享秘钥

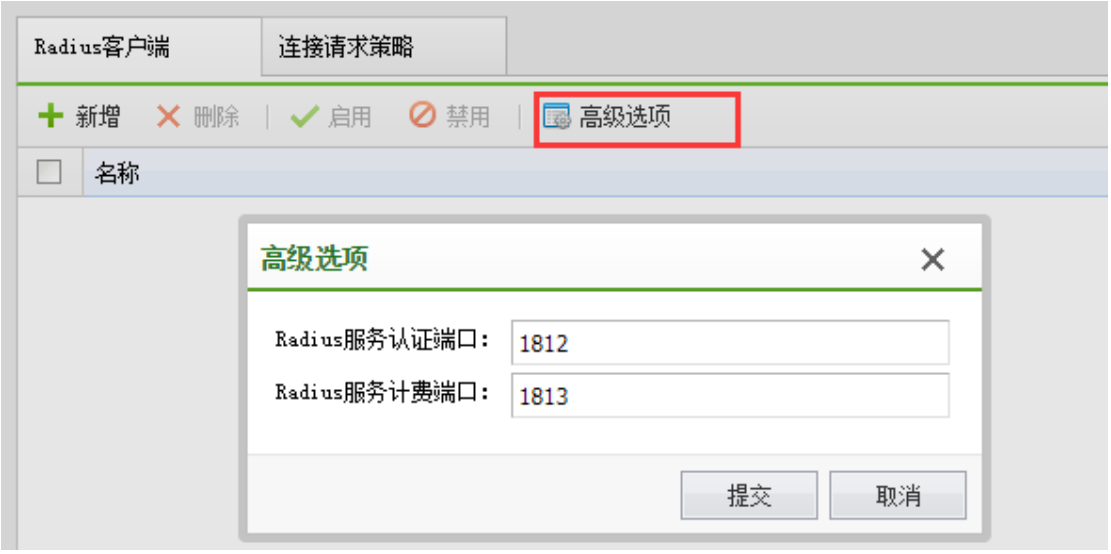
客户端和服务通过该共享密钥建立信任，两端密钥一致才可以建立信任。

5、Radius 客户端—其他选项

当勾选了“请求必须包括消息验证程序属性”表示请求的消息必须包含 Message-Authenticator 属性。

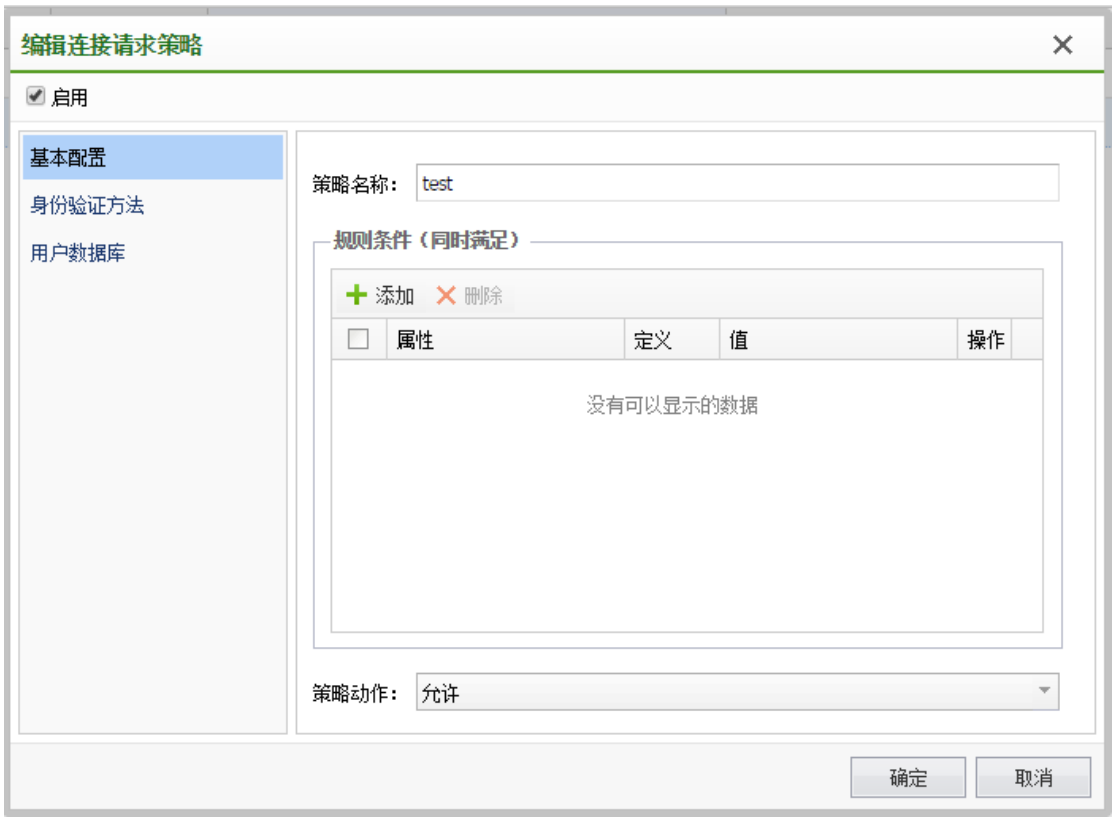
6、高级选项

配置 Radius 服务器的认证和计费端口，必须与客户端配置的端口一致。



4.4.12.2. 连接请求策略

认证的的策略配置，连接请求策略有优先级，当优先级高的策略为允许策略时，配置失败则不通过验证，当优先级高的策略为拒绝策略时，配置失败时则跳转至下一策略进行验证。

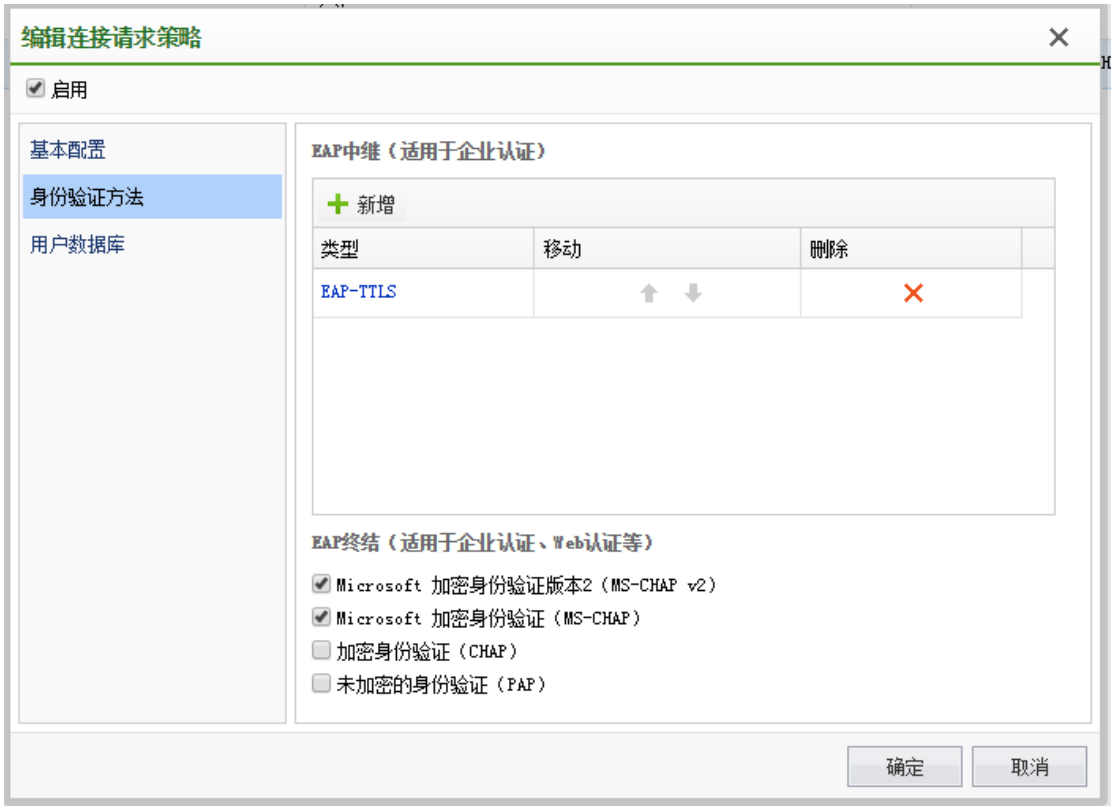


1、规则条件

通过传输 Radius 属性的值进行匹配。

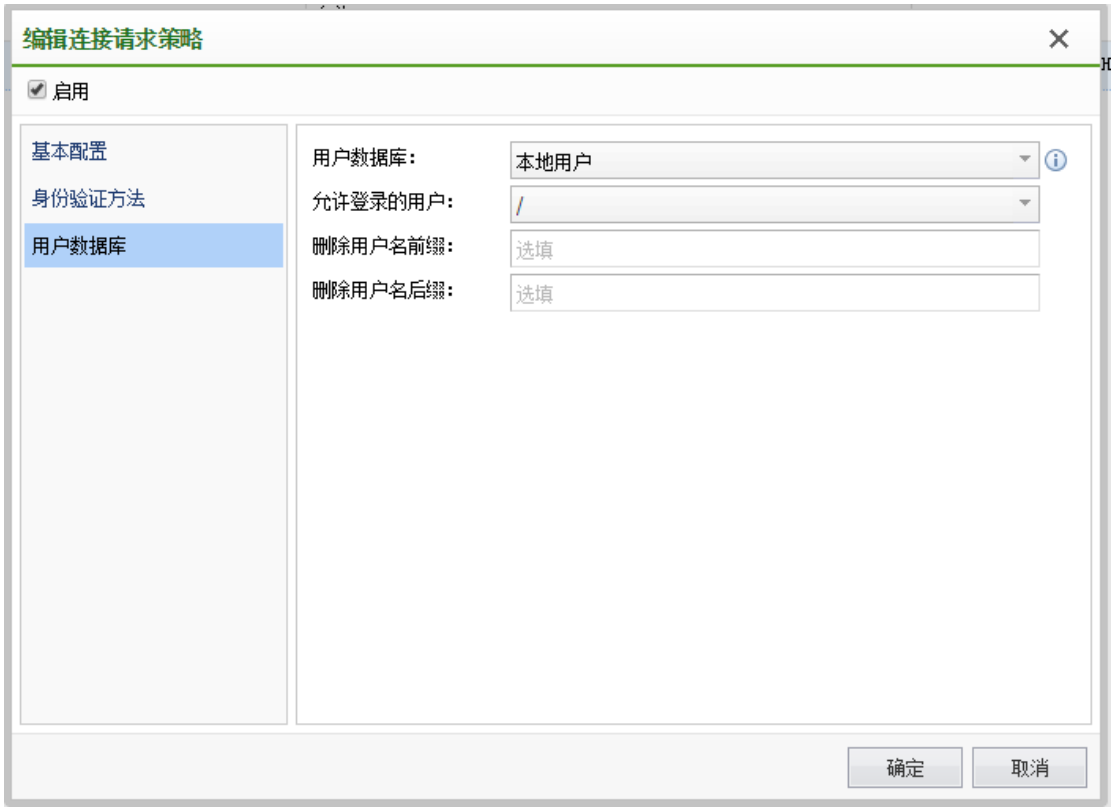
2、策略动作

允许或者拒绝匹配该策略的用户通过认证。



1、身份验证方法

认证的协议的选择，为了保证认证的有效性，请确保选择的身份验证方法包含了需要处理的认证协议类型。



1、用户数据库

选择认证数据的数据库（数据库需在在外部数据库进行配置）。

2、删除用户名前后缀

可以定义用户名的前、后缀，验证的用户名会删除定义的前、后缀再进行验证。

4.4.13. 认证高级选项

4.4.13.1. WEB 认证通用配置

1、认证域名：认证域名默认配置为：auth.wifi.com。Web 认证时，会跳转到该域名上来。

注：域名配置为公网上已经存在的域名时，Web 认证的用户访问该公网域名也会跳转到认证或注销页面。

2、认证域名解析的 IP：修改认证域名解析的 IP 地址之前，请确保要修改的 IP 地址不会冲突，否则将会出现终端进行 web 认证时无法打开认证页面。

3、访客认证免弹 Portal 页面有效期：弹出 Web 认证页面：短信认证、二维码认证、微信认证的用户，非首次接入无线网络，跳转到认证页面，不需要输入账号信息，只需要点击登录即可。

不弹出 Web 认证页面：短信认证、二维码认证、微信认证的用户，非首次接入无线网络，不跳转到认证页面，用户只需接入网络，无需认证即可上网。

该选项值仅对只配置了访客认证的无线网络生效。同时配置访客认证和账号认证，终端用户接入无线网络时，每次都会重定向至认证页面。

4、账号认证免弹 Portal 页面有效期：账号认证非首次认证，断开无线网络后，再次登录的时间间隔在阈值范围内时，不重定向至认证页面，超出阈值时间，终端用户将会重定向至认证页面。

5、手机号绑定验证：账号二次认证时，绑定手机号码之后，同一个终端在有效期之内无需再次绑定。

6、注销无流量用户：完成有线认证、接入点有线认证之后，终端在阈值内无流量产生，控制器会主动注销这个用户。

4.4.13.2. 访客认证选项

1、微信认证直通：微信认证唤起微信应用的时候，需要在认证过程中放通微信流量，以及和腾讯的微信服务器进行交互。唤起微信应用失败的时候，可以选择对终端进行免认证处理。

2、手机号登录有效期：手机号登录的认证有效期，通过短信认证之后可以访问无线网络的时长。超过该时间之后，需要重新获取验证认证上网。

3、微信登录有效期：微信认证有效期，通过微信认证之后可以访问无线网络的时长。超过该时间之后，需要重新在微信公众账号菜单中，申请上网。

4、二维码审核有效期：只通过二维码方式，二维码审核后，访客可以访问无线网络的时长。超过设置时间后，如果仍然需要访问无线网络，需要再次审核。

5、短信验证码有效期：短信认证获取到的验证码，使用的有效期。

5、海外社交应用认证有效期：通过海外社交应用之后可以访问无线网络的时长。有效期内终端无需再次输入登录信息等，只需在页面上点击“我要上网”即可。

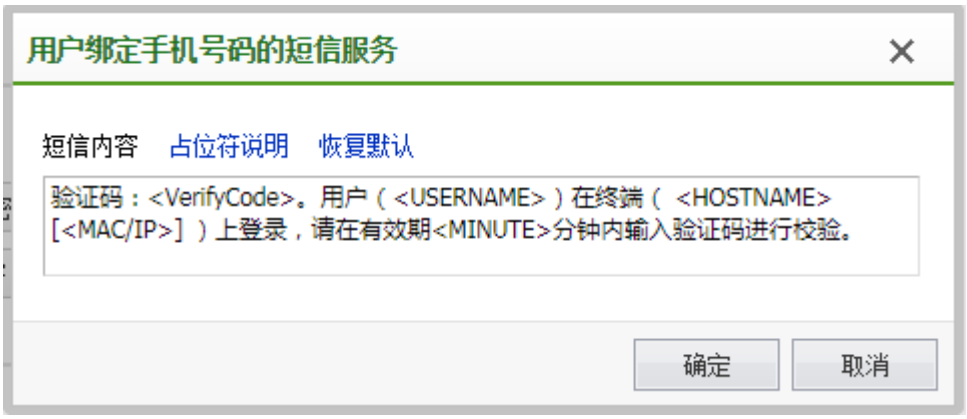
6、邮箱登录有效期：通过邮箱认证之后可以访问无线网络的时长。有效期内终端无需再次输入登录信息等，只需在页面上点击“我要上网”即可。

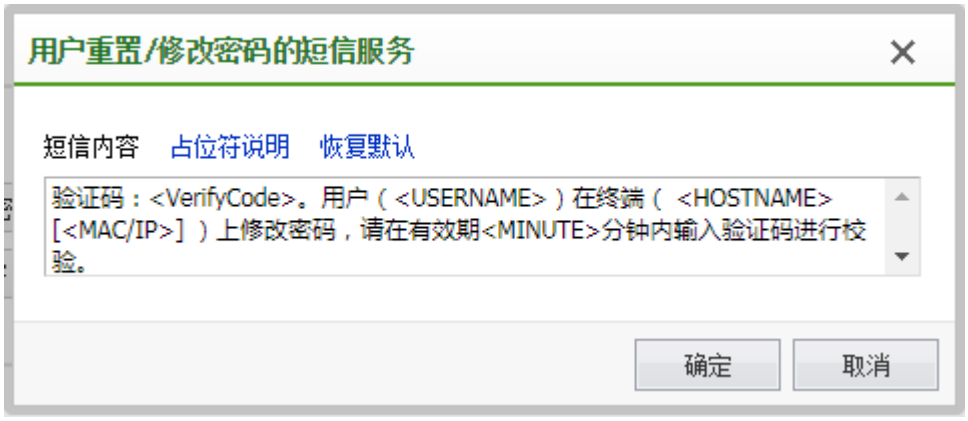
7、邮箱验证码有效期：邮箱认证获取到的验证码，使用的有效期。

8、自动登陆优先级：在同一个无线网络中配置多种认证方式的时候，如果一个终端使用过多种认证方式，再次认证时免登陆的优先级。

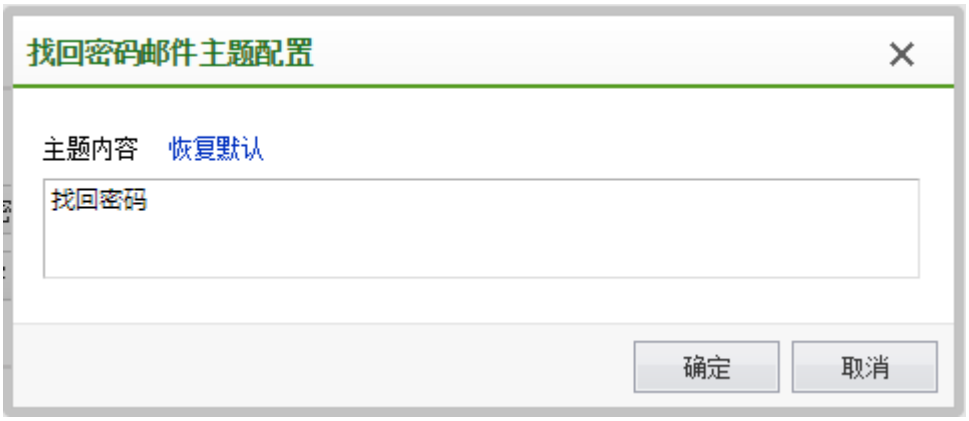
4.4.13.3. 模板内容配置

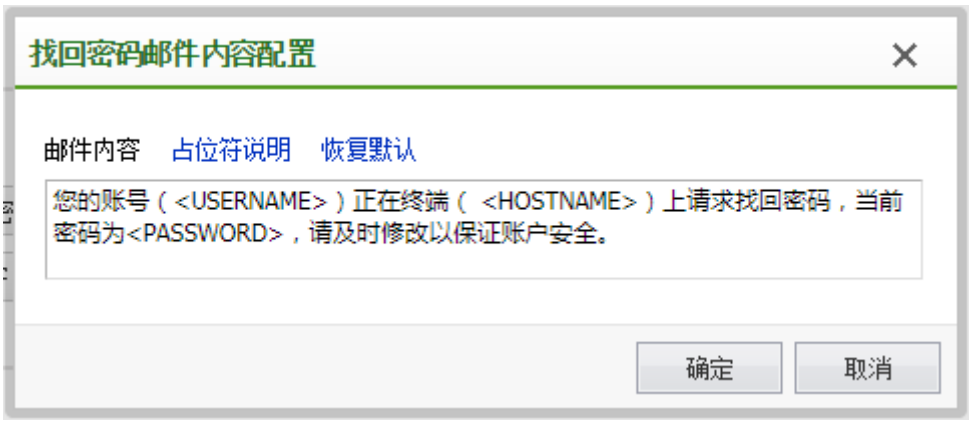
短信服务内容（二次认证)：二次认证时发送短信的模板。



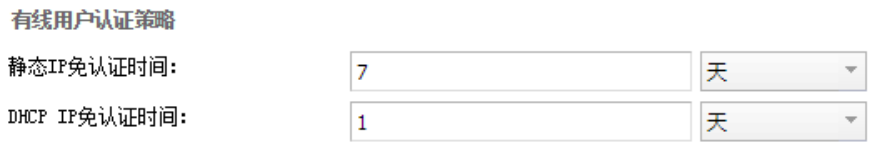


邮箱找回密码：本地用户使用邮箱找回密码时，邮件主题和邮件内容模板。





4.4.13.4. 有线用户认证策略



1、静态 IP 免认证有效期：有线认证，当网络环境为认证用户和认证接口跨三层网络，给终端配置使用静态 IP 部署时，终端用户 WEB 认证二次认证免认证的有效期。

2、DHCP IP 免认证时间：有线认证，当网络环境为认证用户和认证接口跨三层网络，给终端配置使用 DHCP 分配 IP 部署时，终端用户 WEB 认证二次认证免认证的有效期。

4.4.13.5. 其他配置

1、终端绑定管理员免审批有效期：启用此功能时，终端绑定管理员免审批为选定日期的 23:59。

2、第三方 portal 用户免认证：适用于 portal 对接场景，若第三方 portal 服务器不支持 MAC 免认证功能，启用此功能，终端用户认证通过后，在时长配额范围内不需要再次认证。

3、终端类型识别：开启精准终端类型识别，将会识别终端的操作系统。

4、剔除获取 IP 失败的终端：DHCP 获取失败，大部分无线终端 IP 地址会显示为 169.254.x.x。

（1）开关开启，超过超时时间，终端还未获取到 IP 地址，将会被踢下线让终端重新认证，重新获取 IP 地址。

（2）开关关闭，适用于内网使用 169.254.x.x 网段的客户，避免获取到这个网段的无线终端，被控制器误判为未获取到 IP 用户而踢掉。

4、云管家灾备选项：控制器与云服务器断开连接时，终端审批消息无法下发，认证用户不需要经过审批即可上网.

5、单点登录发送终端下线消息：控制器结合深信服 AC 做单点登录时，可选择是否将终端的下线报文单点登录发给深信服 AC。

6、用户名区分大小写：控制器默认会将账号认证的用户名转换成小写，勾选之后将不进行转换。

4.5. 接入点配置

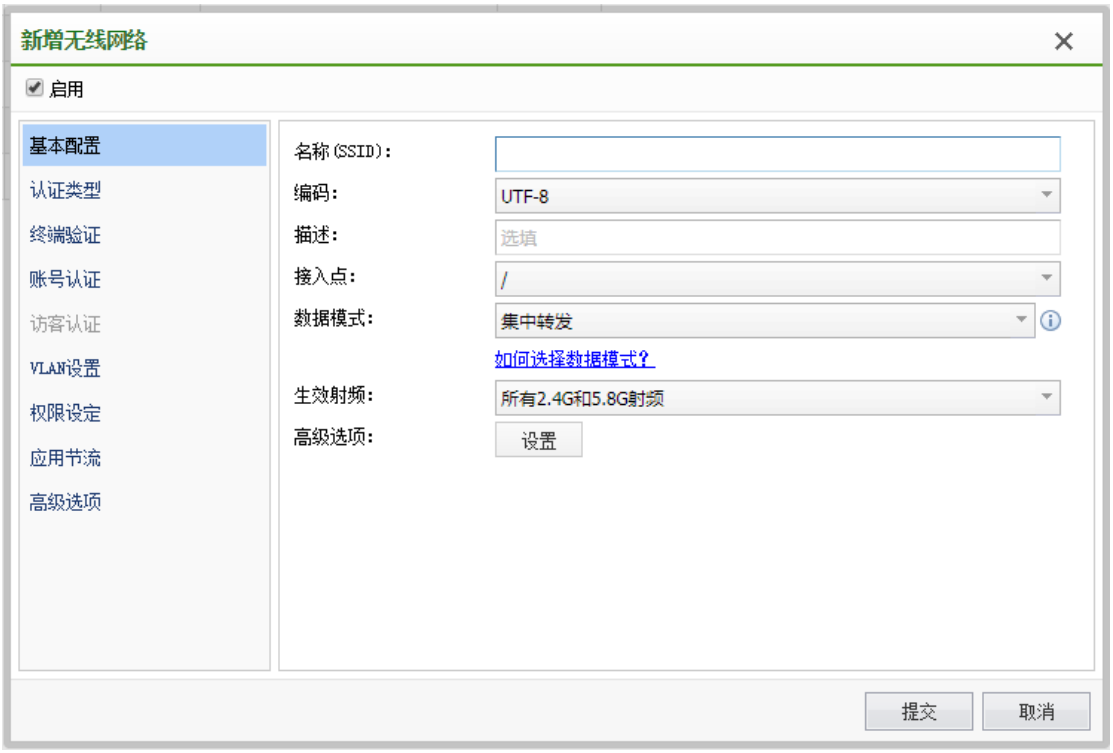
『接入点配置』包括【无线网络】、【本地转发应用控制】、【接入点有线认证】、【无线接入点】、【虚拟接入点】、【灾备策略】、【无线负载域】、【无线漫游域】、【部署管理图】、【定位服务器】、【射频通用配置】

4.5.1. 无线网络

『无线网络』：可以【新增】、【删除】、【启用】、【禁用】一个无线网络。新增无线网络需要设置无线终端接入的无线信号 SSID，认证方式，设置无线接入点范围，数据转发模式等，下面将一一详细讲解。下面的无线网络的配置截图：

无线网络号 SSID 可以设置为“汉语”，对汉语的支持比较好无线终端可以正常显示，多数 PC 无法正常显示，一般建议设置为英文类型的 SSID。

新增一个【无线网络】，包含【基本配置】、【认证类型】、【终端验证】、【帐号认证】、【访客认证】、【vlan 设置】、【权限设定】、【应用节流】、【高级选项】，如下图：



4.5.1.1. 基本配置

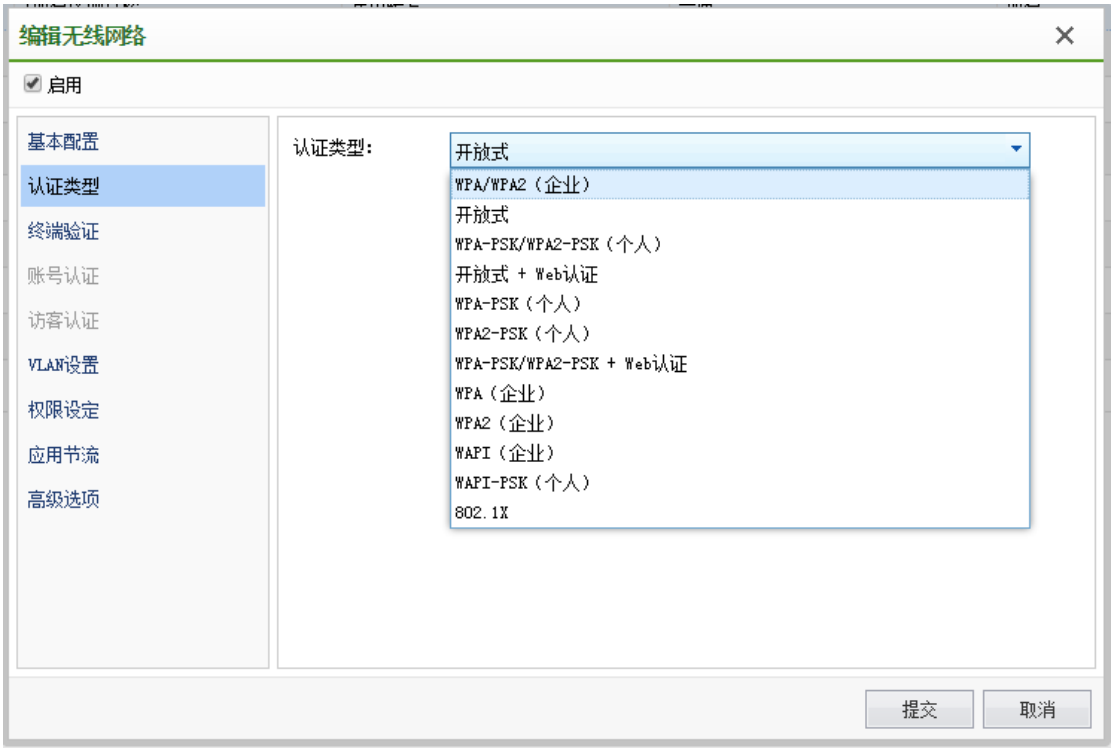
【基本配置】需要设置无线网络名称（SSID），并设置无线网络在哪些接入点 AP 上启用，以及该无线网络在 AP 上的数据转发模式，并设置工作频段。

数据转发模式分为集中转发，和本地转发模式，集中转发模式表示无线终端 STA 所有的上网业务数据到达 AP 后，由 AP 进行数据分装，由 AP 集中转发给 NAC，在由 NAC 集中转发出去上网。本地转发模式表示无线终端 STA 所有的上网业务数据到达 AP 后，由 AP 根据本地路由网关直接转发数据出去，不对数据包进行分装。

设置的频段分为 2.4G 和 5G 共 2 个频段，可以分别设置启用，也可以设置 2 个频段同时启用。其中高级选项中，可以针对该 SSID，每个 AP 接入人数做限制，隐藏 SSID 表示该

无线网络不主动广播其信号，无线终端不能自动发现该网络，必须在无线终端 STA 上手动填写 SSID，并设置才能接入该无线网络。营销广告推送设置，如果需要使用控制器营销推送功能，需要勾选以下 2 个设置。

4.5.1.2. 认证类型



认证类型有以下几种类型可以选择：

[WPA/WPA2(企业)]：选择 WPA 或 WPA2 加密方式的企业认证方式

[WPA（企业）]：仅选择 WPA 加密方式的企业认证方式

[WPA2（企业）]：仅选择 WPA2 加密方式的企业认证方式

[WPA-PSK（个人）]：选择 WPA 加密方式与预共享密钥的个人认证方式

[WPA2-PSK（个人）]：选择 WPA2 加密方式与预共享密钥的个人认证方式

[WPA/WPA2-PSK(个人)]：选择 WPA 或 WPA2 加密方式与预共享密钥的个人认证方式

[开放式]：选择开放式的无线接入方式认证

[开放式+WEB 认证]：选择开放式的无线接入方式与 WEB 方式认证组合

[WPA-PSK/WPA2-PSK+WEB 认证]：选择 WPA 或 WPA2 加密方式与预共享密钥认证方式接入无线网络，再结合 WEB 方式认证的组合。

下面我们对这些认证类型做一个简单的分类，以便进行功能区分，所以该分类依据是以功能性差别进行的划分，他们之间有重合的可能，比如开放式认证和 WEB 认证就可以结合一起使用，划分为如下四类：

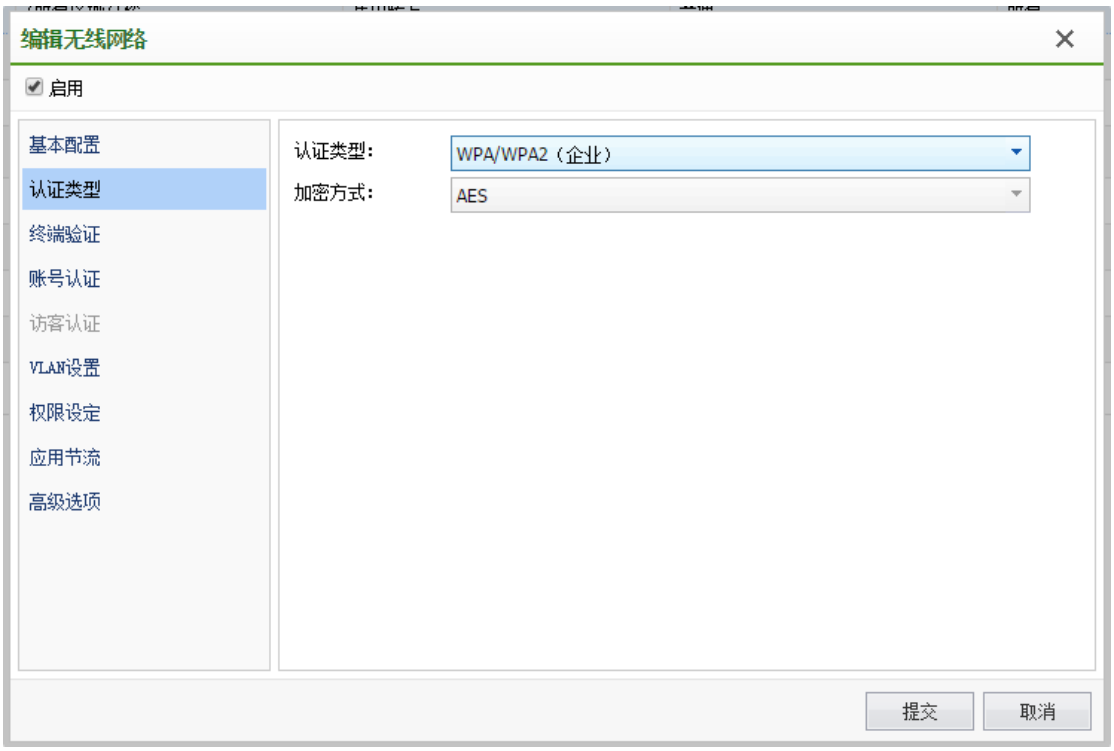
4.5.1.2.1. 企业方式认证

选择采用“企业”方式的认证还包括 WPA（企业）、WPA2(企业)、WAPI(企业)

加密方式：自动选择，包括 AES 和 TKIP，企业类型的认证，在终端验证和用户认证出现的界面与 WEB 方式认证是有所差别的，这些差别就决定了“企业方式认证”和“WEB 方式认证”与“个人方式认证”的差别。

企业方式认证是采用 802.1X 架构的认证方式，无线终端也需要采用配置 802.1X 方式认

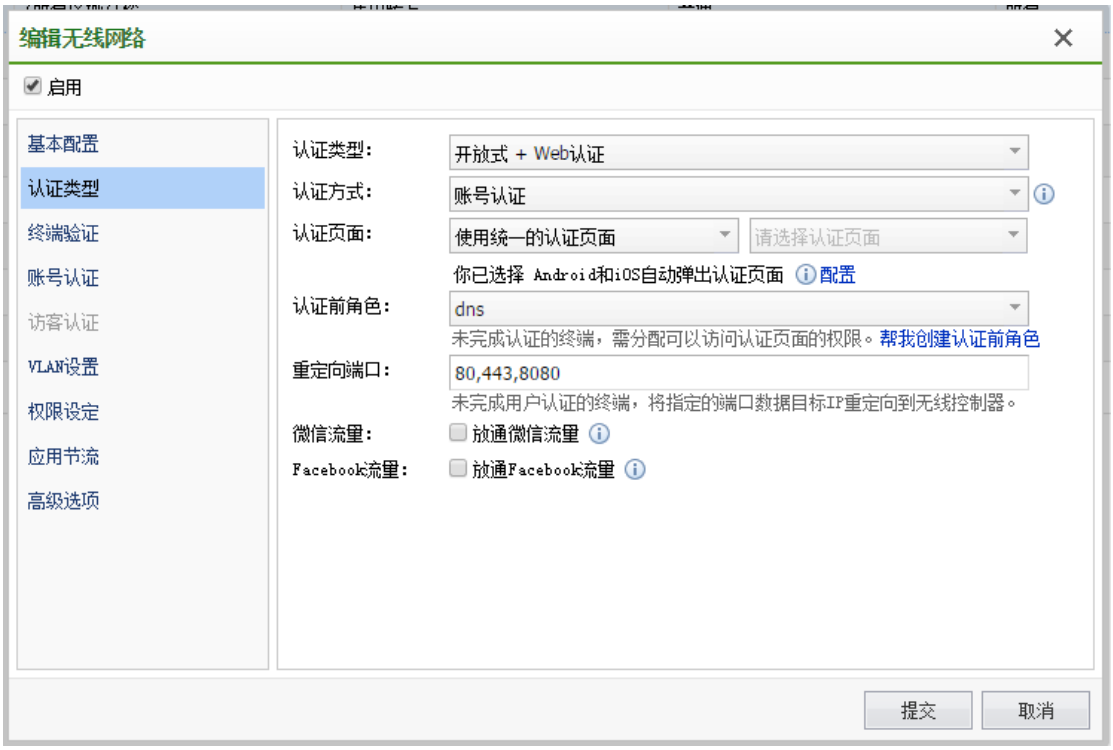
证。



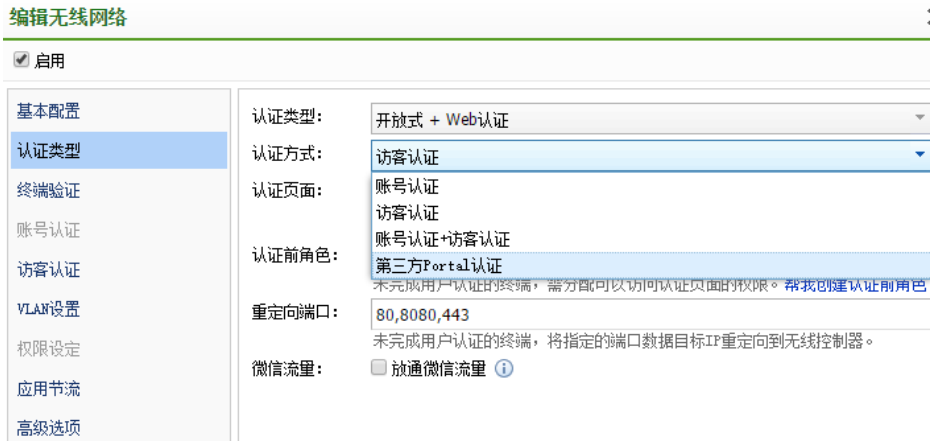
4.5.1.2.2. WEB 方式认证

web 认证是指无线终端接入无线网络后，浏览器访问任意网址，都会被重定向到登录页面，用户在网页上输入用户名、密码等方式通过认证后才能访问网络资源。

web 认证通常与开放式无线网络一起使用，也就是用户连接无线网络时，不需要任何认证。由于无线网络的流量未加密，因此 web 认证的无线网络，通常只用于非关键性的网络中，例如仅用于访客访问互联网，无法访问企业内部网络。



WEB 方式认证包括：WPA-PSK/WPA2-PSK+WEB 认证、开放式+WEB 认证；



认证方式：

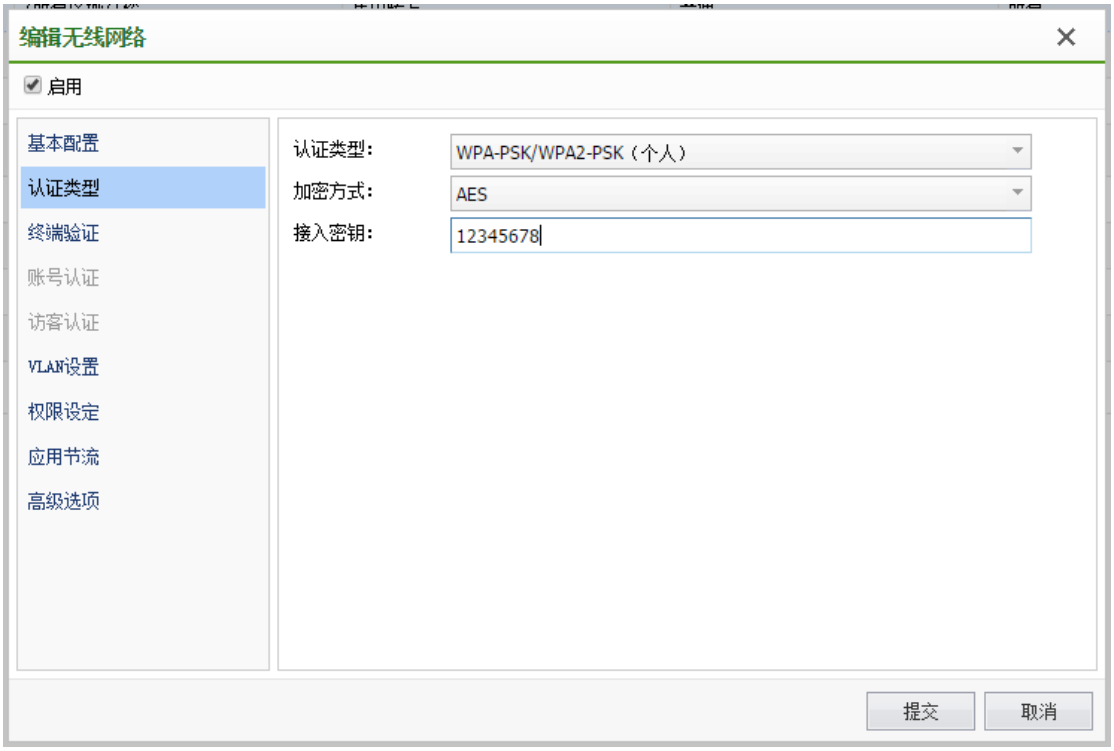
1、【帐号认证】、【访客认证】、【账号认证+访客认证】

2、【第三方 Portal 认证】可以对接外部 Portal 服务器实现外部 portal 认证。

认证页面是我们在【认证授权】-【认证页面】设置的自定义页面或者采用系统默认的页面。采用第三方 Portal 认证时，Portal 服务器选择【认证授权】-【认证服务器】中添加的 portal 服务器。认证前角色是指进行 WEB 认证成功前，默认可以使用的网络权限对应的角色，重定向端口是指无线终端 STA 有该端口的数据时，进行认证页面的重定向。

4.5.1.2.3. 个人方式认证

选择“个人”方式的认证

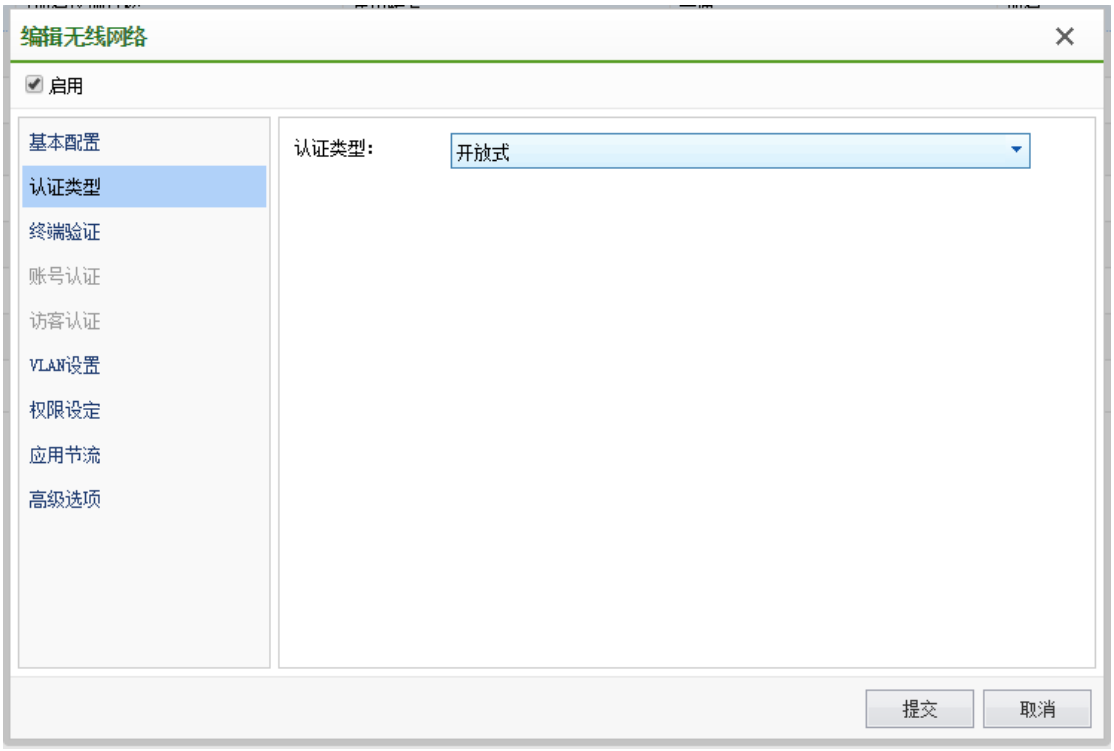


个人方式认证包括：WPA2-PSK（个人）、WPA-PSK（个人）、WPA/WPA2-PSK(个人)以及 WAPI-PSK（个人）。

加密方式：自动选择，包括 AES 和 TKIP 方式，接入密钥是只设置接入无线网络的预共享密钥。

4.5.1.2.4. 开放式认证

开放式认证是指无线终端用户接入无线网络时不需要进行验证即可正常接入无线。

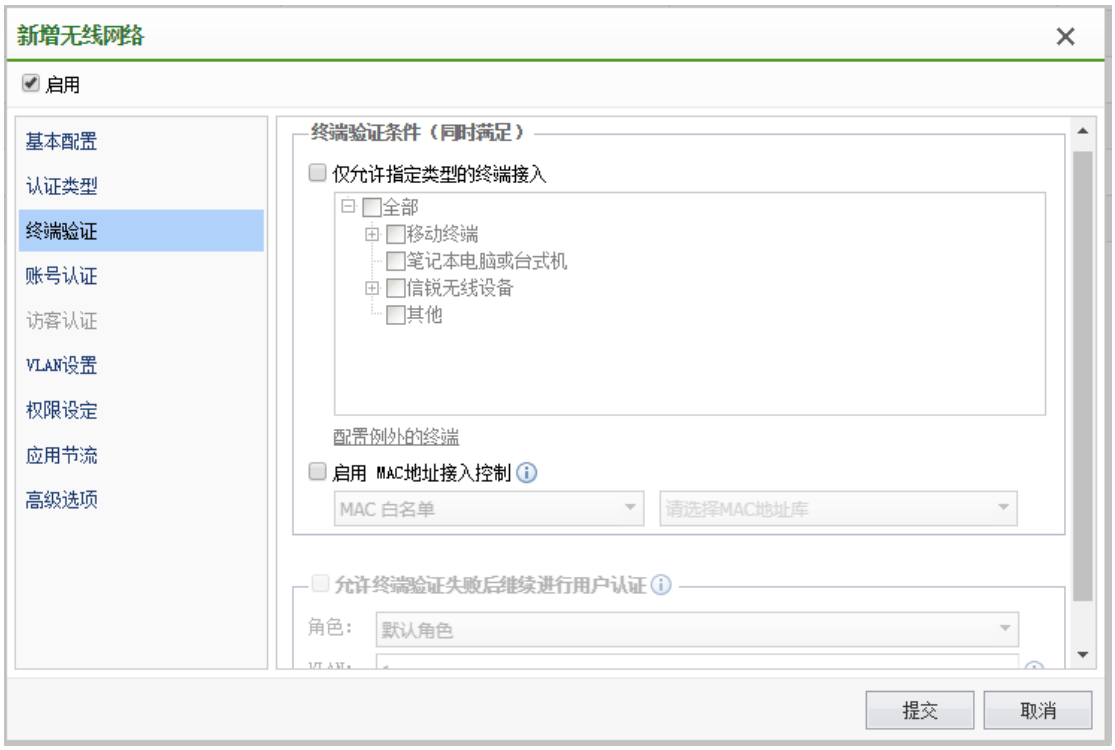


4.5.1.3. 终端验证

终端验证可以显示的内容是由已经选择的认证类型来决定的，选择不同的“认证方式”，会显示不同的页面，也就会有不同的功能性差异。

当选择了包含“开放式认证“和“个人认证”方式时，可以对无线终端的终端类型和 MAC 地址的合法性进行校验，其中 MAC 地址校验是通过启用“检测终端 MAC 黑白名单”来进行的。MAC 白名单是在【认证授权】-【MAC 白名单】预先设置好的合法 MAC 地址。

开放式+web 认证时，终端验证的配置如下：



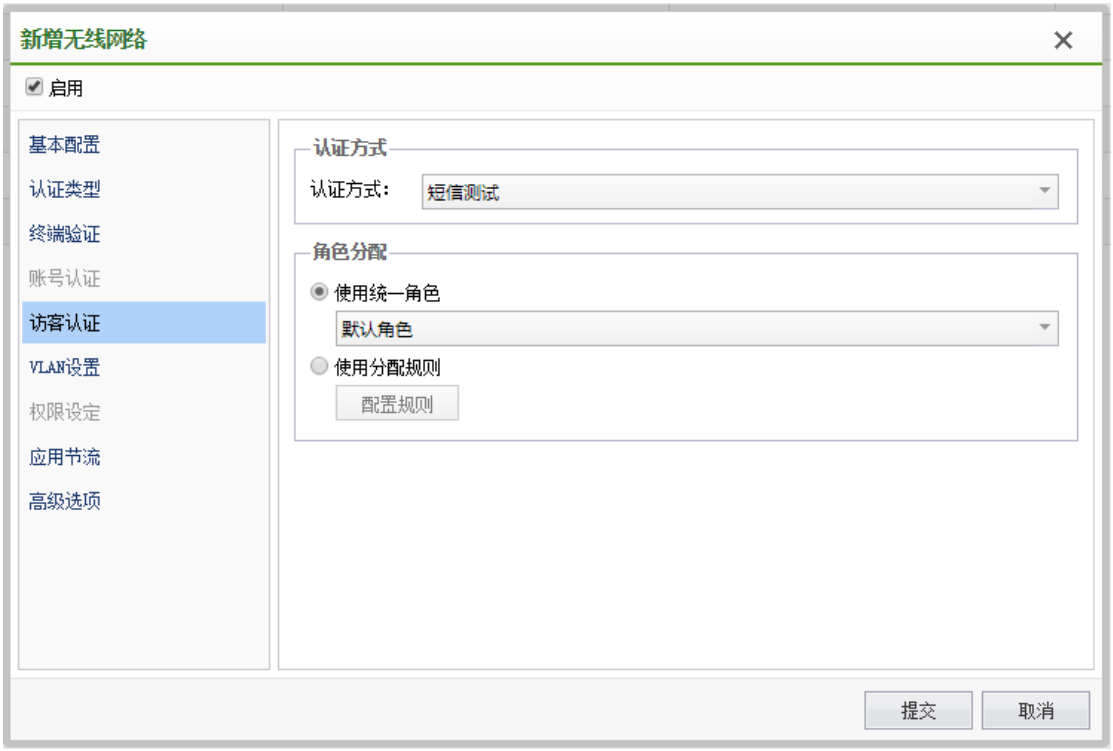
“终端验证失败后”表示即使 MAC 与终端类型验证失败后，也继续让该用户进行后续的 WEB 方式认证。如果不勾选该功能，只要无线终端的 MAC 验证不在【对象定义】中的【MAC 白名单】中，就完全拒绝该用户的进行进一步认证，直接拒绝其上网。

选择“企业”方式认证后，终端验证也可以启用检查终端 MAC 白名单。可以设置允许终端验证失败（或未加入域）时，继续进行用户认证，并设置认证通过后的角色。认证通过后的 vlan。为通过域计算机验证的客户端分配权限以登录到域，需要设置可以使用的角色让 PC 能正常登录到域，并设置对应的 vlan。

4.5.1.4. 访客认证

在部署用于访客使用的无线网络时，为了简化用户体验，通常设置为开放式的无线网络。但单纯的开放式的无线网络，存在无法验证访客身份的问题，因此通常需要设置认证方式。此方式主要部署在公众访问的无线网络中，例如部署在机场，交通枢纽，医院，酒店，商场，学校等地方。

访客认证方式参考 4.4.5.1 章节的“访客认证”。



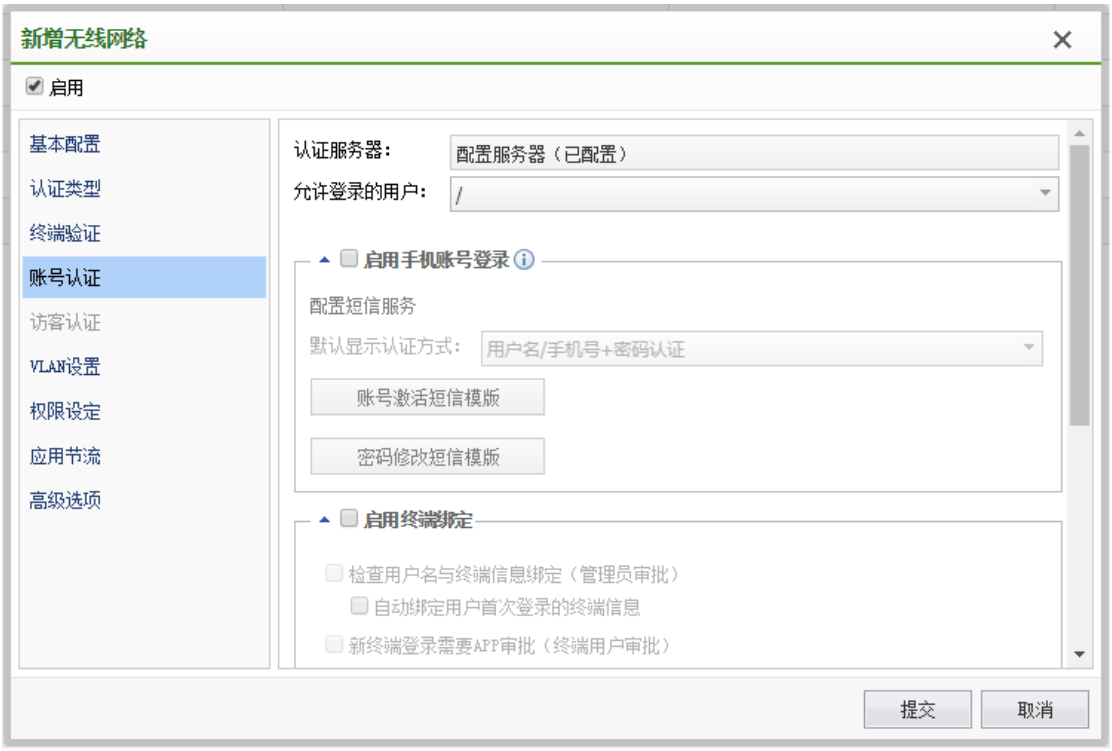
4.5.1.5. 帐号认证

4.5.1.5.1. Web 方式认证

当选择【开放式认证】和【个人认证】时不能选择配置【帐号认证】，只有选择【WEB 方式】或【企业】方式时才可以配置

如下是当选择企业或 WEB 方式认证时，可以配置的用户认证配置：

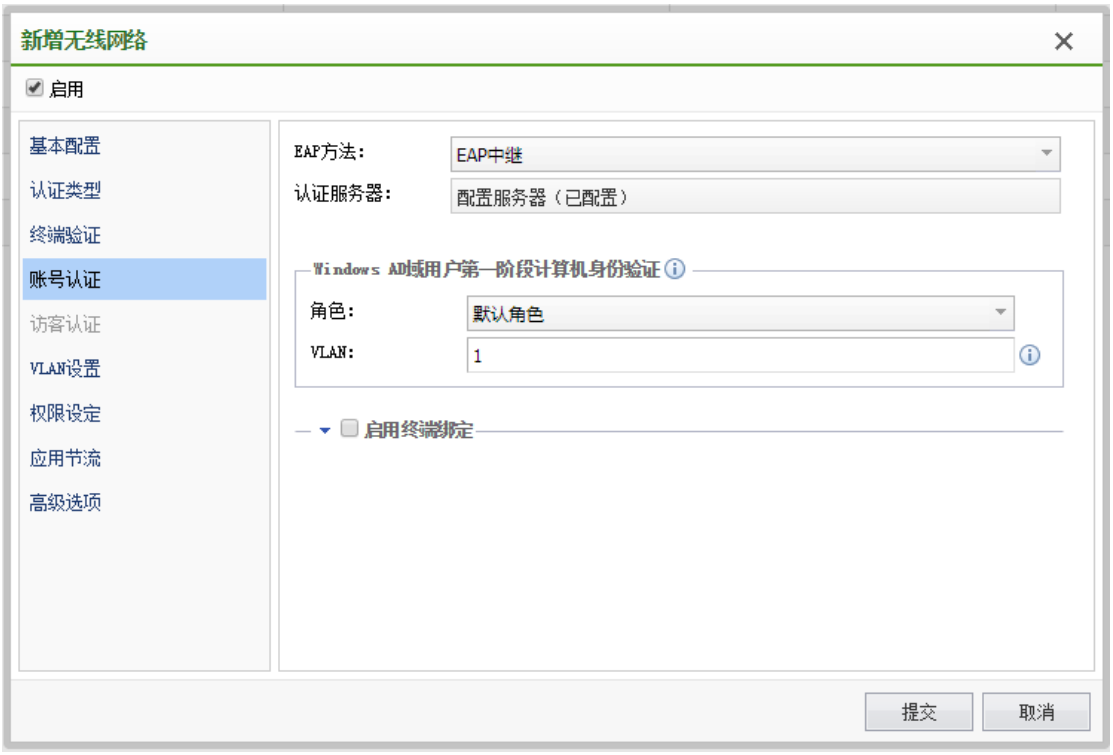
当选择 WEB 方式认证时，帐号配置页面如下



4.5.1.5.2. 企业方式

企业方式有以下下几种认证类型：EAP 终结与 EAP 中继 2 种方式。并可以设置服务器认证配置冗余，以及设置自动绑定最初认证用户名与 MAC 地址，并可以指定对某一类型的终端进行 MAC 地址绑定关系检查，比如 windows 终端。

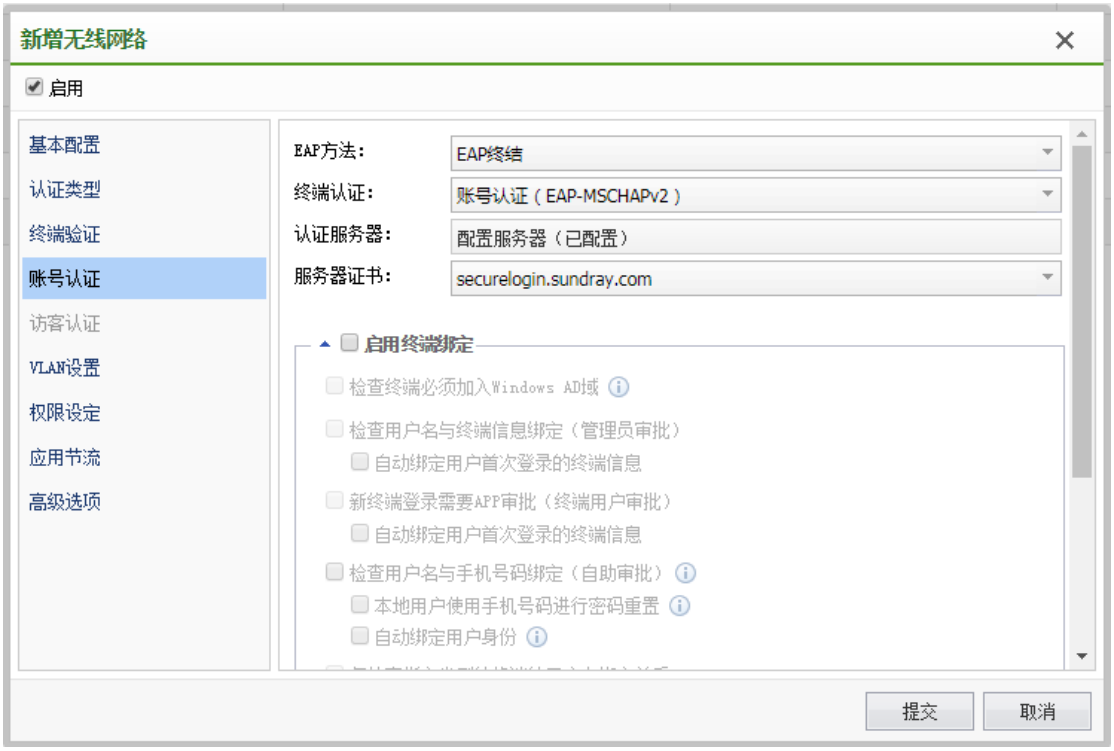
1、EAP 中继

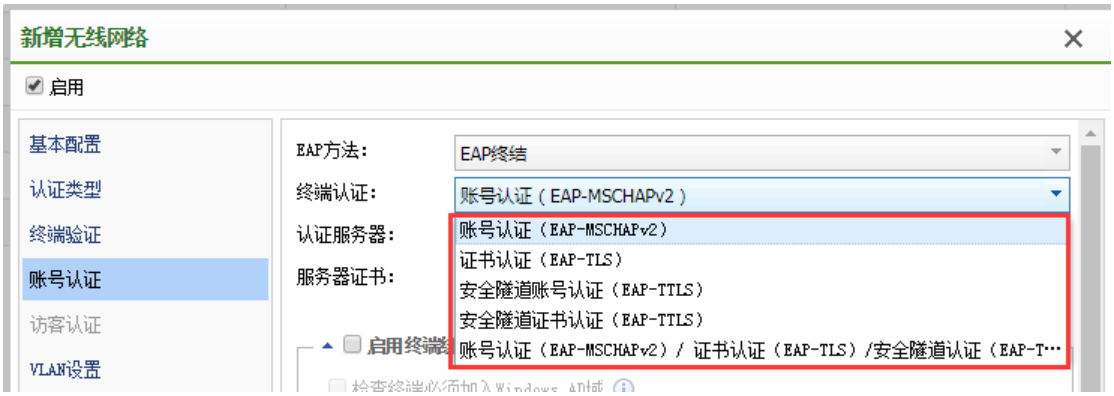


EAP 中继是指无线接入点把无线客户端的 EAP 报文直接转发到 RADIUS 服务器，由 RADIUS 服务器来完成认证过程。因此认证方法由 RADIUS 服务器中配置，与无线控制器无关。

在 WPA/WPA2-企业 无线网络中，通常使用的认证方式为 EAP-TLS 或者 PEAP-MSCHAPv2，因此需要确认 RADIUS 服务器支持所需的认证方式。常见的 RADIUS 认证服务器为微软 Windows Server 系列中提供的 IAS/NPS 服务。

2、EAP 终结





“EAP 终结：EAP-TLS” 是指由无线控制器来完成 EAP-TLS 认证过程。EAP-TLS 协议是在 EAP 协议框架上，使用 TLS 协议来完成身份认证，密钥交换功能。TLS 协议也是 HTTPS 协议的核心。因此 EAP-TLS 可以视为与 HTTPS 协议具备同等的安全性。

EAP-TLS 协议使用双向证书认证，要求服务器及客户端都使用证书，向对方证明身份。并使用非对称加密方式，在无线客户端及认证服务器间安全地协商数据加密密钥，保证无线数据传输的机密性及完整性。

由于使用了基于证书的身份验证方法，避免了基于密码认证方法所存在的由于密码泄漏，密码强度低等原因导致的密码被猜测或暴力破解的风险。因此 EAP-TLS 提供了目前无线认证中，最安全的认证方法。缺点是所有客户端都需要安装个人证书，部署比较复杂。

3、服务器证书（向无线用户证明身份）

在 EAP-TLS 身份验证过程中，服务器使用此证书创建 TLS 连接，并向客户端计算机证明身份。客户端可以选择验证此证书的颁发者及主题名称，来保证连接到正确的企业无线网络中，避免连接到由攻击者伪造的同名恶意网络导致的安全风险。

由于系统自带的服务器证书未被客户端信任，在 Windows 系统客户端中，如果无线网络配置选择了"验证服务器证书"，将导致客户端无法连接无线网络。因此需要了解关于服务器证书的要求，如果有必要，需要考虑向商业证书颁发机构购买证书。

4、CA 证书

用于检查客户端合法性的 CA 证书。客户端提交的证书将要求由此 CA 颁发，并通过此 CA 配置的有效性检查选项。

5、EAP 终结：PEAP-MSCHAPv2

“EAP 终结：PEAP-MSCHAPv2” 是指由无线控制器来完成 PEAP-MSCHAPv2 认证过程。

EAP-MSCHAPv2 是基于密码的认证方法，最初是由微软设计用于为拨号及 VPN 连接提供更安全的认证方法。虽然 EAP-MSCHAPv2 提供了更安全的认证方法，但存在的安全弱点是，如果攻击者能监听 EAP 报文，则可以通过离线的字典攻击，分析用户的密码。

把 EAP-MSCHAPv2 跟 PEAP 结合一起使用，得益于 PEAP 内部创建的 TLS 隧道所提供的健壮安全性，EAP-MSCHAPv2 的交互过程可以得到加密保护，从而防止了攻击者通过离线字典攻击方式来分析用户密码的安全弱点。

PEAP-MSCHAPv2 协议，由 2 个阶段组成：

阶段 1，PEAP。首先协商 PEAP 协议，创建一个只使用服务器证书的 TLS 隧道。在这个阶段中，客户端可以选择验证服务器证书，并检查服务器端证书的主题、颁发者等证书信息，完成对服务器证书的认证，避免连接到一个由攻击者创建的，名称相同的无线网络中导致的安全风险。

阶段 2，EAP-MSCHAPv2。在 PEAP 协议的 TLS 隧道内部，协商另外一个 EAP 方法，这里为：EAP-MSCHAPv2。在这一步中，客户端需要提供用户名及密码凭据，以完成对客户端的身份验证。验证完成后，RADIUS 服务器，会为每个客户端生成不同的会话密钥，以对接入点与无线客户端之间传输的无线数据包进行加密。

6、服务器证书（向无线用户证明身份）

在 PEAP-MSCHAPv2 协议阶段 1 中，服务器使用此证书创建 TLS 连接，并向客户端计算机证明身份。客户端可以选择验证此证书的颁发者及主题名称，来保证连接到正确的企业无线网络中，避免连接到由攻击者伪造的同名恶意网络导致的安全风险。

由于系统自带的服务器证书未被客户端信任，在 Windows 系统客户端中，如果无线网络配置选择了"验证服务器证书"，将导致客户端无法连接无线网络。因此需要了解关于服务器证书的要求，如果有必要，需要考虑向商业证书颁发机构购买证书。

7、允许登录用户

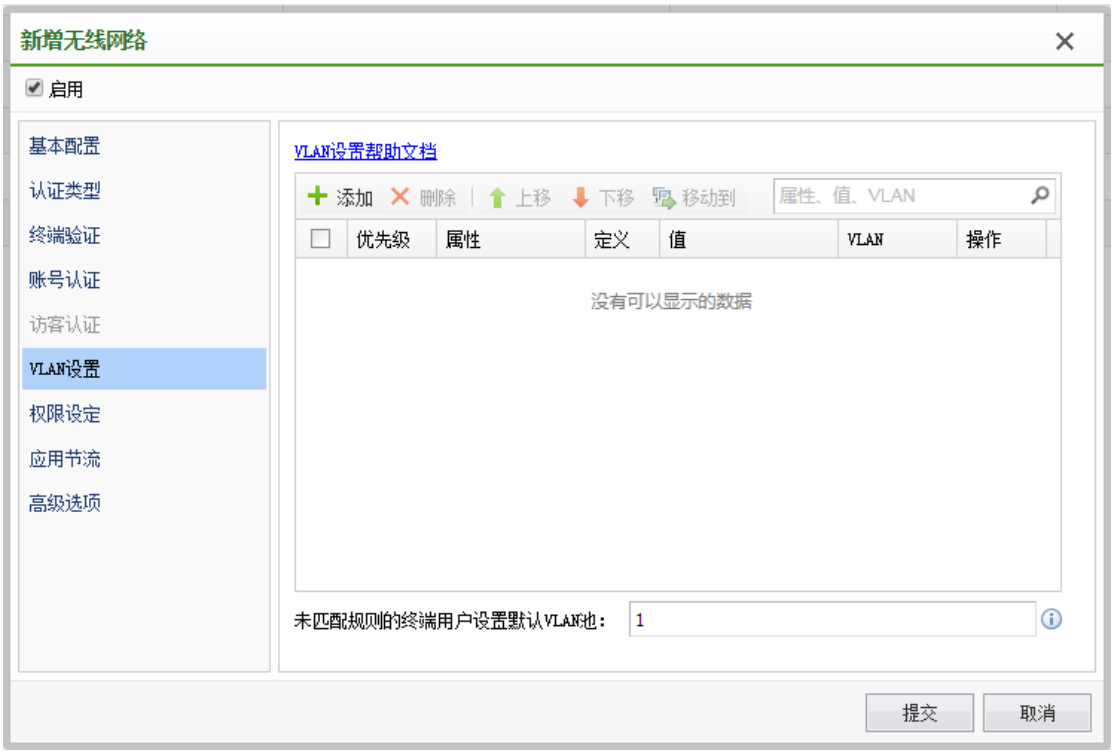
选择允许连接无线网络的组，默认选择根组，也就是所有本地用户都允许通过认证，并连接此无线网络。

8、RADIUS 服务器冗余

使用 RADIUS 中继模式下，允许配置多个 RADIUS 服务器，实现认证服务器的故障冗余备份。

4.5.1.6. VLAN 设置

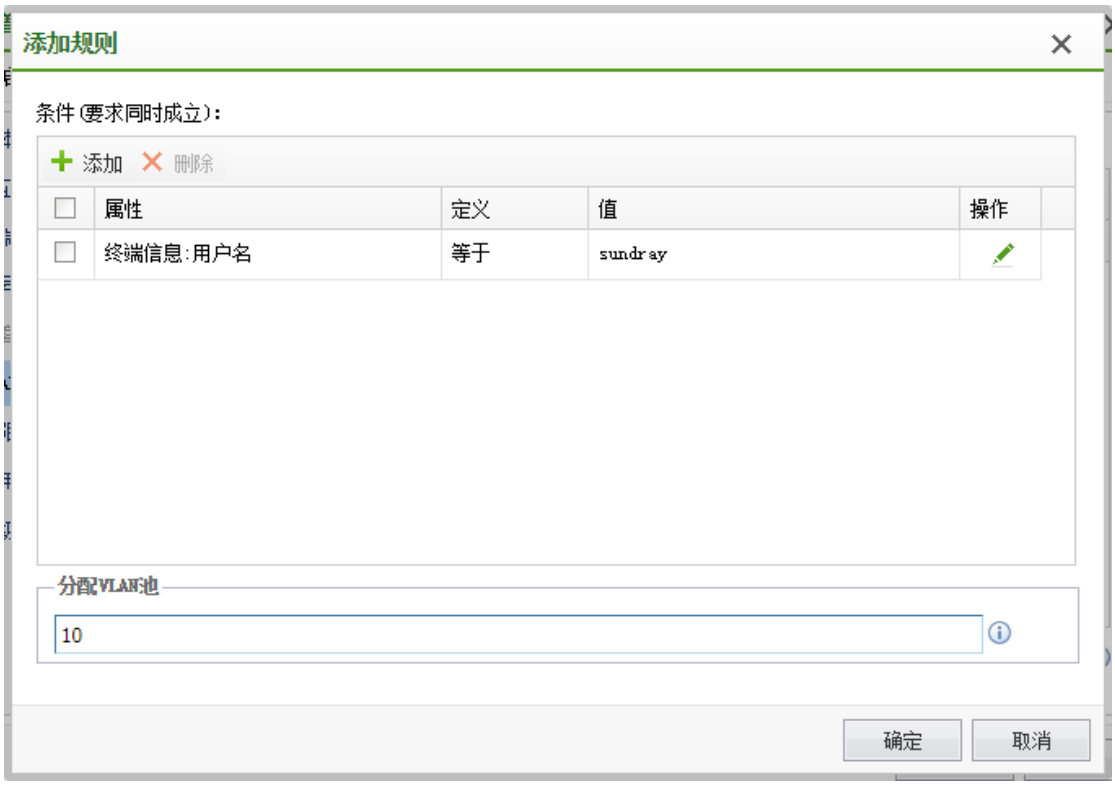
VLAN 配置是为了更好的实现无线终端的控制和管理，进行无线 VLAN 的划分；无线 VLAN 划分与有线网络 VLAN 的划分是有一些差别的，无线 VLAN 的划分以及 VLAN 之间的数据处理，是由 AP 和 NAC 针对无线网络用户进行管控和路由的，而 AP 和 NAC 之间是由隧道封装的。所以当采用集中转发时，无线 VLAN 的标签是在 AP 与 NAC 中间的隧道内。当本地转发数据时，配置 VLAN，无线数据标签由 AP 打上标签转发出去。



用户认证成功后，系统将提取出用户此次认证过程的所有属性，主要包括：用户名，所属组，接入的 AP，RADIUS 服务器返回的属性值，用户的 LDAP 属性值，证书中的属性值等。然后从上往下，按优先级方式查找角色以及 VLAN 分配规则表，如果用户的属性匹配上规则的条件，则根据规则中的设定值，为用户分配角色或 VLAN。

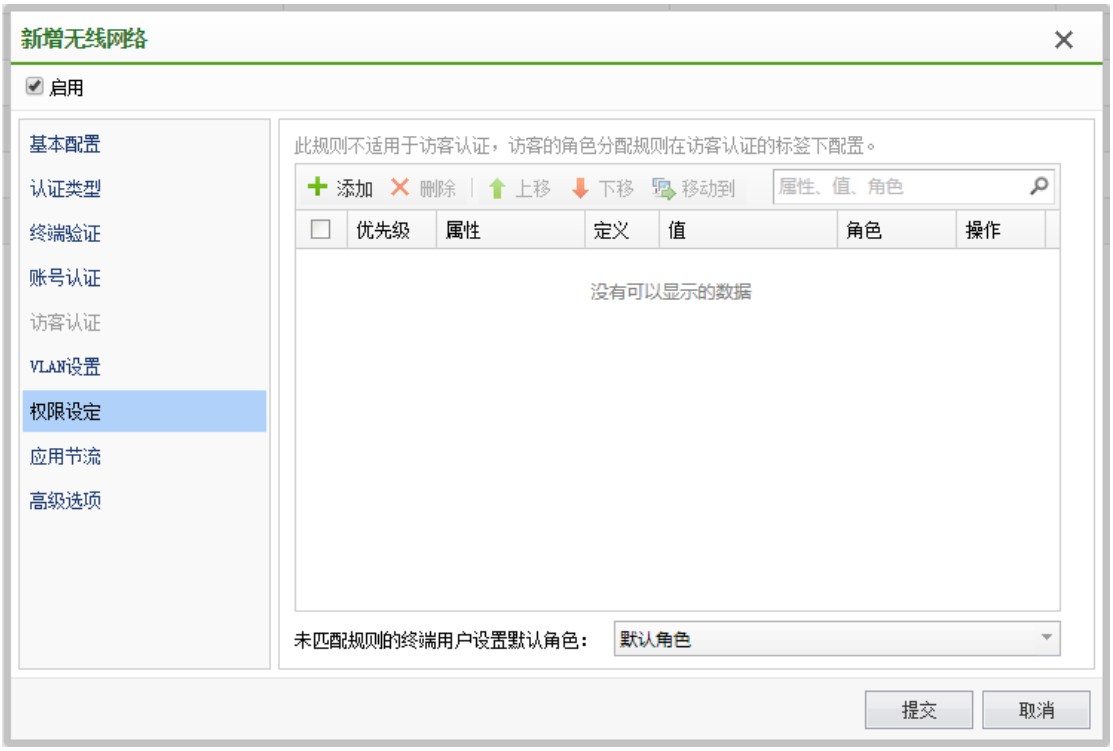
每一条规则中可以包含 1 个或多个条件，如果包含多个条件，则要求同时满足，才视为匹配此规则。如果用户未匹配规则表中的任何规则，则使用设定的 "默认角色" 和 "默认

VLAN"。



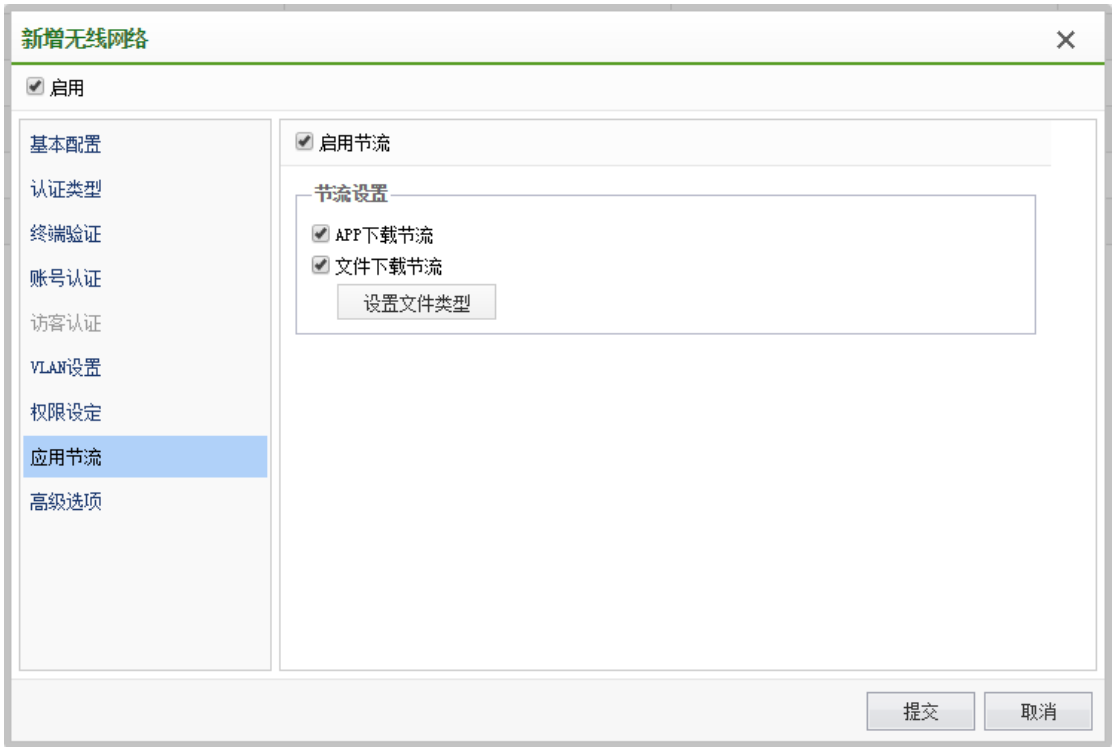
4.5.1.7. 权限设定

【权限设定】主要用于设定终端通过认证后，具有访问网络资源的权限，角色包括访问控制策略、审计策略、流速限制策略、流量与时长控制策略，可以根据 AP 组，无线终端用户组等信息详细的配置角色策略，可以根据 SSID 设置一个默认的角色，配置如下：



4.5.1.8. 应用节流

有利于节省您的网络带宽资源，提升终端浏览/下载体验。如果您使用了 APP 推广，推荐开启 APP 下载加速。

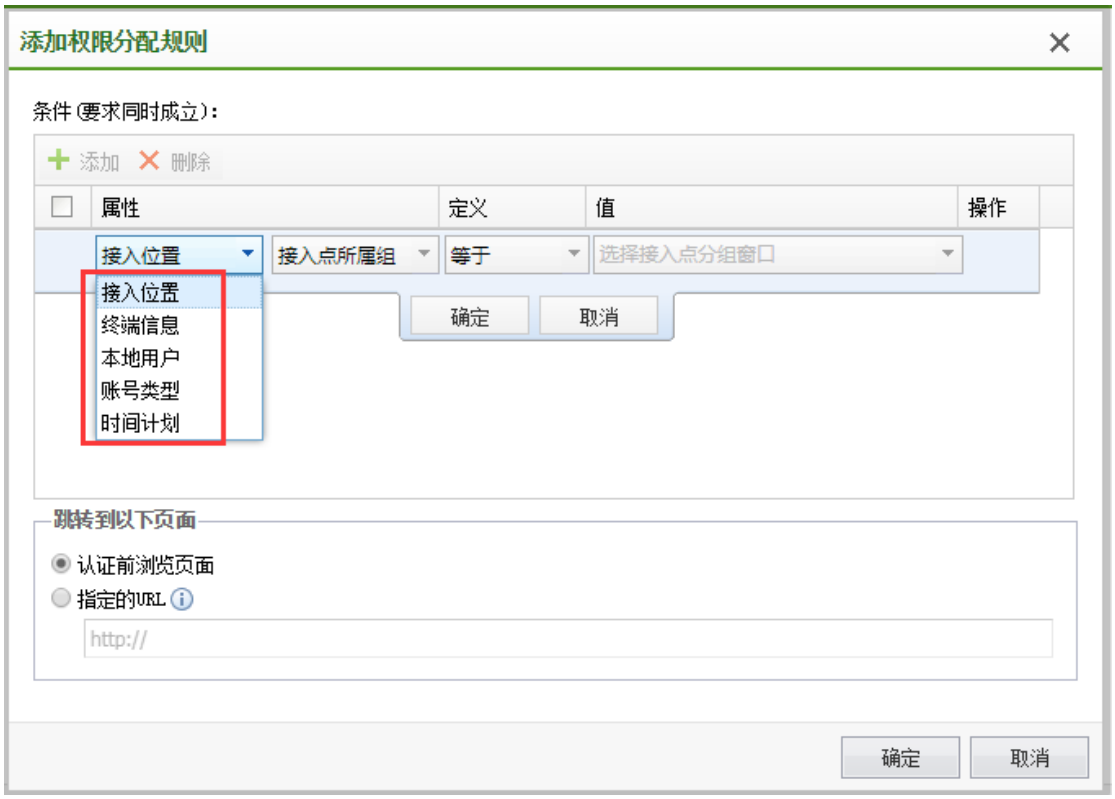


4.5.1.9. 高级选项

4.5.1.9.1. 认证后跳转

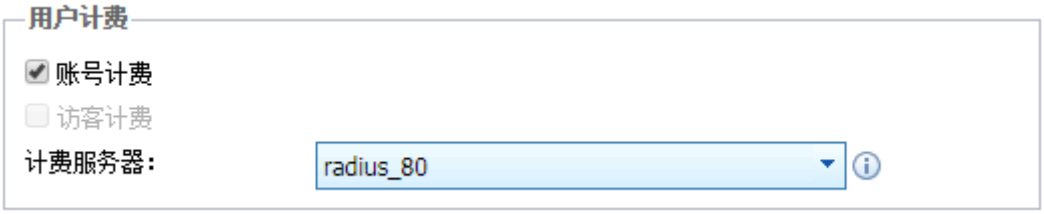
认证后跳转功能是指启用 WEB 认证后，帐号认证用户与访客认证用户通过认证后调整的页面，默认跳转到认证前浏览的页面，可以设置固定的 URL，配置如下：

还可以根据不同用户所在 AP 组的位置，以及用户组的方式指定认证跳转的页面，配置如下：



4.5.1.9.2. 用户计费

可针对 WEB 认证账号认证和访客认证的用户添加计费服务器进行计费。



4.5.1.9.3. 限制账号在多个终端同时登录

限制帐号同时登录的终端数，比如只允许帐号在一台终端上登录，不允许在多台终端上登录，就类似私有帐号与公有帐号的区别。

4.5.1.9.4. WEB 接入 MAC 免认证

Web 接入 MAC 免认证针对 WEB 认证的账号认证及访客认证有效，在该列表中排除的终端，连接无线后将不需要进行 WEB 认证直接分配对应角色。

4.5.1.10. 无线网络自动配置

无线网络自动配置，为了快速便捷的部署无线网络，便于管理员维护，可以在此配置无线网络自动配置，具体配置页面如下：

用户证书注册服务：“证书注册服务” 是无线网络自动配置方案的一部分。在部署基于证书认证，且使用内置 CA 颁发用户证书的无线网络时，需要启用 “证书注册服务”，使得“自动配置工具”能为用户自动申请并安装个人证书，才能完成无线网络的自动配置。

4.5.2. 本地转发应用控制

该功能可实现本地转发下基于应用的访问控制策略以及基于应用的流控，需确保有应用识别序列号。

4.5.2.1. 本地转发应用识别控制策略

控制策略模式：可选择基于服务控制或基于应用控制，选择基于应用控制，能识别具体应用进行相应的访问控制或是流量控制；

生效区域：选择需要进行本地转发应用控制的 接入点或是接入点分组；

排除目标 IP 地址：应用于本地内网环境中的服务器及终端这类需要额外直通访问的设备，访问这类设备的流量不会被识别和控制。

流量处理策略：关联需要生效的角色，流量处理方式选择应用控制，其他配置保持默认。此处需要注意的是，镜像报文的配置；镜像报文数量配置越大（配置范围为 2-15 个），应用识别效果会更好，识别率会更高。但是相应的，镜像报文过多时会降低终端访问网络时的响应速度，建议保持默认配置。

4.5.2.2. 本地转发流控策略

本地转发的流控策略类似于控制器流控功能，可以实现在总的流速限制条件下再对应用流控子通道进行带宽限制，只能做限制通道，不能做保障通道。

通道匹配的顺序取决于通道所处的位置，是从上往下逐个通道匹配的。

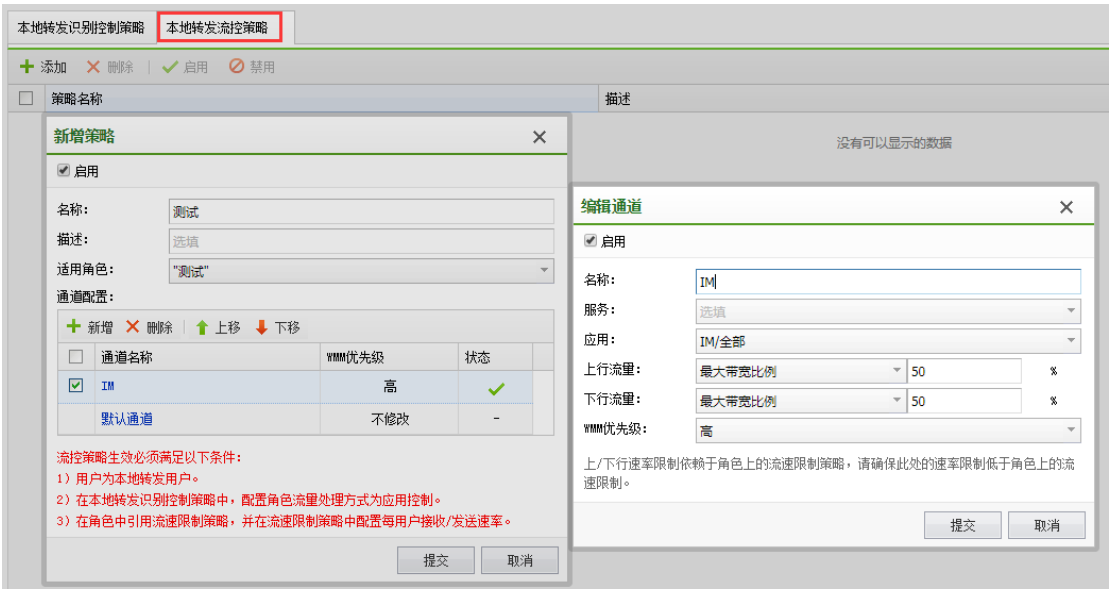
通道属性中的“优先级”，是指带宽分配以及数据包发送的优先级。

流控策略生效必须满足以下条件：

1）用户为本地转发用户。

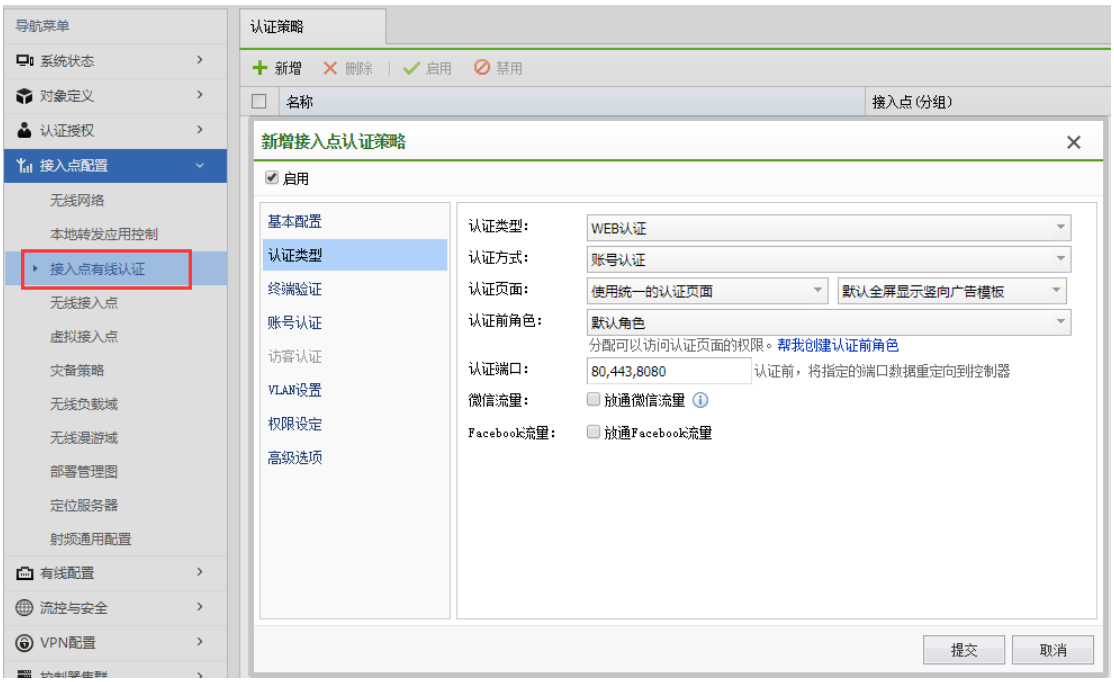
2）在本地转发识别控制策略中，配置角色流量处理方式为应用控制。

3）在角色中引用流速限制策略，并在流速限制策略中配置每用户接收/发送速率。



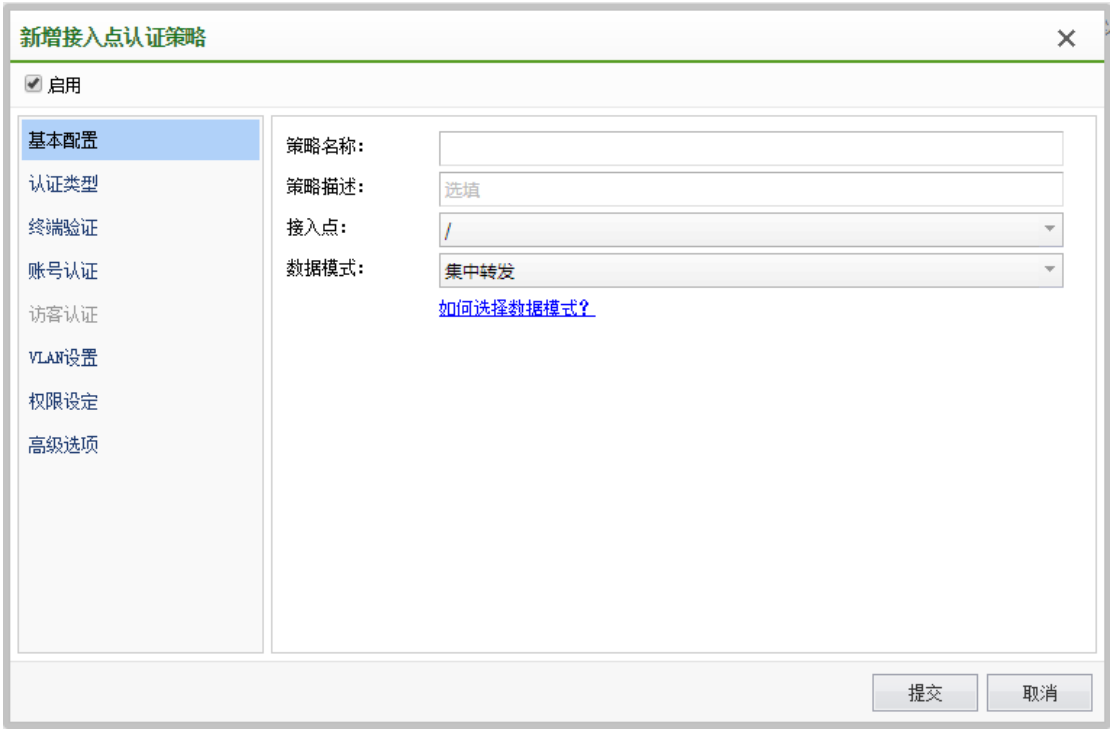
4.5.3. 接入点有线认证

接入点有线认证，主要指接在 AP 上的有线用户的认证方式，不包括在 NAC 上进行有线认证的用户。



4.5.3.1. 基本配置

基本配置，可以配置认证策略的名称，选择接入点（分组），只在选择的接入点（或分组）上提供网络接入服务。



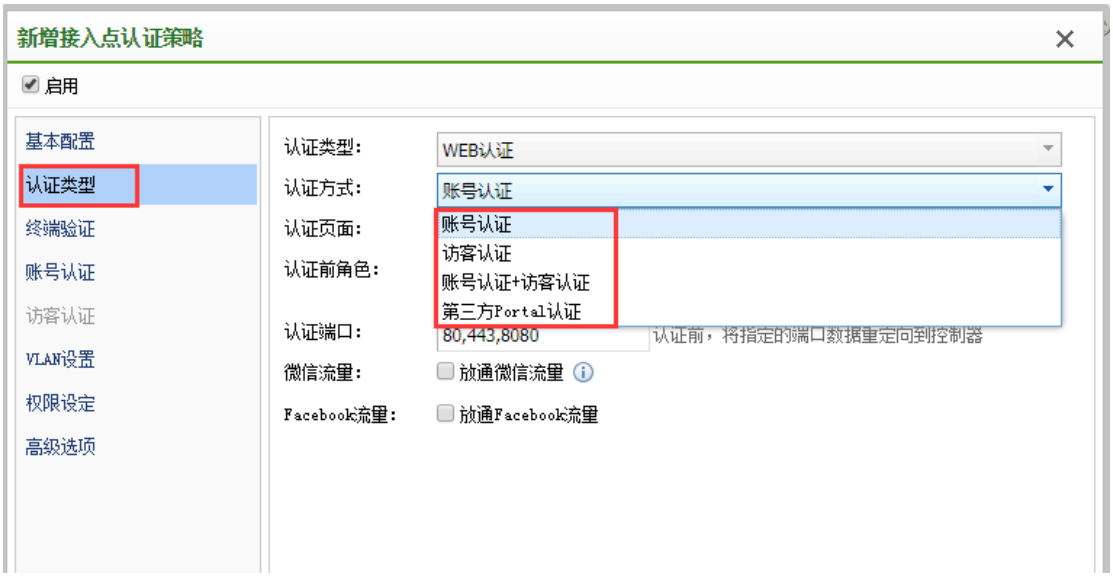
数据转发模式： 集中转发模式中，接入点（AP）与无线控制器之间建立 2 层的数据隧道，用户的所有网络流量，通过此隧道传输到无线控制器，无线控制器再把流量转发到有线网络中。最简单的方法，可以把此模式理解为：相当于用户直接连接到无线控制器。

本地转发是指用户的网络流量，由接入点（AP）直接转发到有线网络（不经过无线控制器）。最简单的方法，可以把此模式理解为：接入点的无线用户直接连接到了接入点（AP）上联网卡所连接的有线网络。

4.5.3.2. 认证类型

认证类型包括【IP 地址认证】和【web 认证】。IP 地址认证，无须认证即可连接到网

络。Web 认证，web 认证是指终端接入网络后，浏览器访问任意网址，都会被重定向到登录页面，用户在网页上输入用户名、密码等方式通过认证后才能访问网络资源。 有线认证配置类似于 4.5.1 节所提无线网络配置，可参考 4.5.1 节配置。



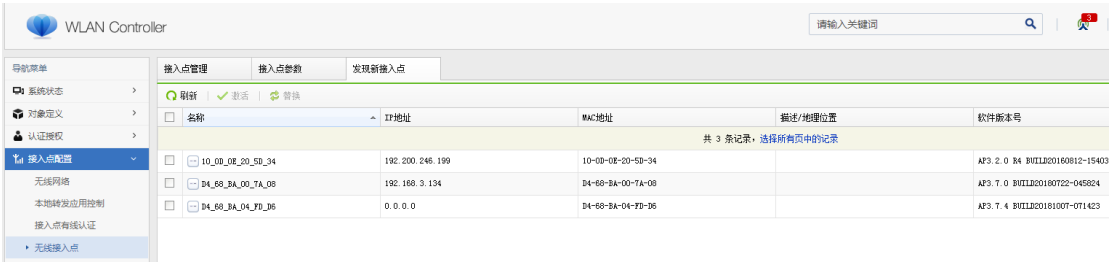
4.5.4. 无线接入点

无线接入点包括 AP 的发现与对 AP 的配置管理。

4.5.4.1. 发现新接入点

为防止未授权的接入点连接到无线控制器，并获取无线网络配置的风险。无线接入点（AP）连接到无线控制器后，并未进入工作状态，需要管理员在"发现新接入点"列表中，确认接入点的合法性，并手动执行激活操作，接入点才能正常工作。

当 AP 接入网络中，AP 会自动发现 NAC，当 AP 第一次发现 NAC 时，会在 NAC 上看到新的接入点，需要进行激活后，才能正常使用无线 AP，并下发配置。



提示：在 NAC 控制台的右上角，当有出现图标 

时，表示还有未激活的接入点，需要到该页面激活。

4.5.4.1.1. 激活 AP

当 NAC 上发现 AP 时，需要激活，激活按钮可用

点击激活后，配置界面如下：

可以编辑 AP 的名称，地理位置，便于后续 AP 的识别分组和管理，默认 AP 以其 MAC 地址为名称

所属组：配置 AP 所属于的管理组，便于对 AP 进行集中管理和配置。

发现控制器 IP：填写 AP 用于连接的 NAC 的 IP 地址，如果给 AP 填写了 NAC 的地

址，AP 下次重启后，会自动以该配置 IP 连接 NAC 并建立隧道

发现控制器域名：用于 AP 自动发现 NAC 用，当 AP 解析到该域名时，AP 会自动向 NAC 请求连接。NAC 发现该 AP 后，就可以对该 AP 进行策略下发配置了

网络地址：可以设置自动获取，也可以设置固定 IP 地址

4.5.4.1.2. 替换

接入点和交换机均支持设备替换功能，设备替换分为两种操作：

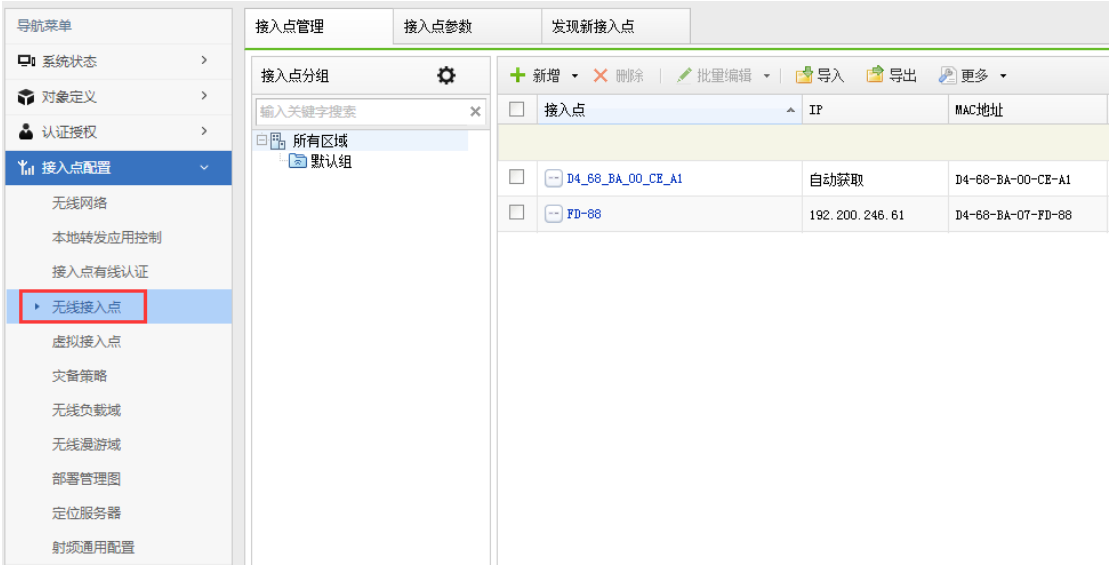
交换机激活的时候，设备类型分为两种：

发现新设备时，可以将要激活的设备替换为已经激活过的设备。替换时，可以选择将旧设备删除或是重新激活。

接入点管理或交换机管理页面，可以选择将两个设备的配置互相替换。

4.5.4.2. 接入点管理

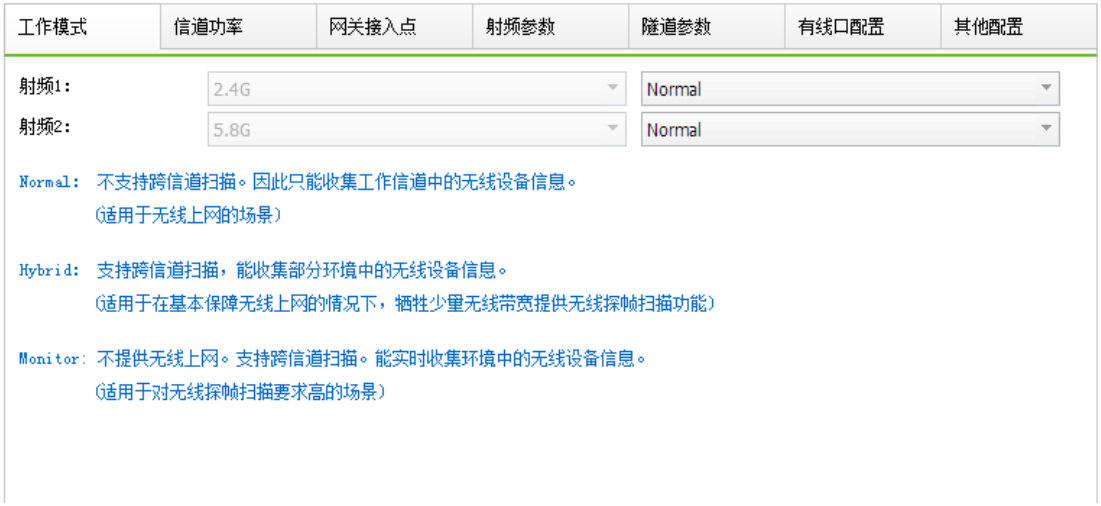
对所有无线接入点进行全部集中分组和管理，包括配置无线信号，工作模式，射频工作范围，隧道参数等。



如果有大批量的 AP 需要集中配置，也可以下载采用下面接入点管理文件的示列文件进行批量的编辑和导入。

4.5.4.2.1. 工作模式

可以分为三种，分别是：Normal，Hybrid 和 Monitor 模式，如下图：



Normal 模式：表示是正常工作模式，AP 在该模式下，AP 可以固定工作信道，如果选择为 auto，射频和信道参数只会在 AP 每次加电时自动调整一次，后续都会稳定在该频率

范围和信道上工作，不会变化，除非手动去【射频管理】菜单下手动点击调整。

Hybrid 模式：混合模式，默认选择该模式，AP 在该模式下，射频和信道参数会默认每个 10 分钟检测一次，如果发现当前信道通讯质量没有其他信道通讯质量好，会自动切换到质量更好的信道进行通讯。Hybrid 模式 AP 也可以用于钓鱼 AP 反制，但是反制效果不及 Monitor 模式 AP 效果好。

Monitor 模式：监控模式，在该模式下，无线网络不能正常使用，主要用于钓鱼 AP 反制。

4.5.4.2.2. 信道功率

可以在此对每个 AP 的功率和信道进行手动调整，在网络优化时，才需要手动配置此项功能。不同类型 AP 支持最大功率不一样，需要正确选择 AP 可工作的功率范围，配置界面如下：

4.5.4.2.3. 网关接入点

在 AP 为网关模式本地转发时，在这里配置用于给 AP 下的终端分配地址的地址池。

4.5.4.2.4. 射频参数

射频参数主要用于选择 AP 是工作在 2.4G 频段还是 5.8G 频段，以及选择网络协议 b/g/n 和 a/g/n 的选择，是否启用功分方案、调整信道、功率、等射频相关的功能。

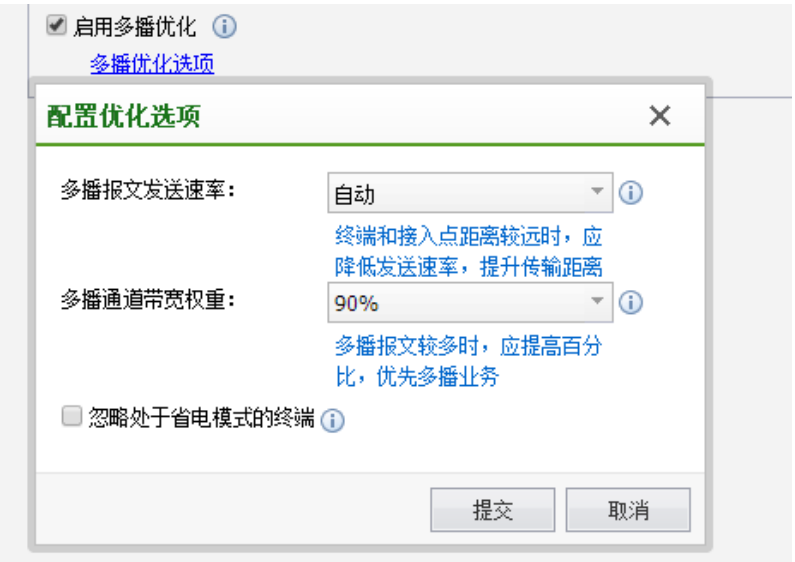
1、5G 接入探测帧引导

在无线网络环境中，无论终端是否接入到无线网络，都会定期在每一个信道发送广播

probe request（探测帧请求）。当在无线用户比较多的网络环境中时，会产生大量以低速率发送的 probe reponse（探测帧响应）报文，影响接入点整体的吞吐量。启用高密优化选项后，接入点将不会响应终端广播的 probe request（探测请求），降低了由于低速率发送 probe response（探测帧响应）消耗的性能空间，提升高密度场景用户的无线上网体验。

2、多播优化

一般当单接入点覆盖范围内超过 40 个终端时，建议开启此功能。



无线接入点默认以 1Mbps 速率来发送多播报文，在多播报文较多的情况下会严重降低无线网络的总体吞吐率。目前可通过如下方式来提高无线网络的整体总体吞吐率。

（1）多播报文发送速率：

自动: 系统将持续评估当前的无线网络环境，自动选择一个更优，且不显著影响广播报文可靠性的速率来发送广播报文，提高了无线网络的总体吞吐率。

固定速率: 无线接入点若以固定速率发送多播报文，可防止低速终端拉低多播报文整体吞吐率。适用于终端与无线热点距离在 10 米以内非干扰的多播应用场景。

（2）多播通道带宽权重：

在开启用户间平均分配带宽或者流量通道间动态分配带宽时，默认多播通道占用权重比例为 90%。若当前环境处于多播应用场景，可根据实际情况调整多播通道占用的权重比例。比如电子书包场景，建议将多播通道占用权重设置为 90%。

（3）忽略省电模式的终端：

按照 802.11 协议规定，如果接入点上有一个无线终端处于省电模式，则系统需要将所有的多播进行缓存，等到 beacon 帧发送后才能进行发送。这样在实时的多播应用场景下，如果存在睡眠的无线终端，将会导致多播报文无法快速及时发送，影响用户体验。

启用该功能后，接入点发送多播报文时将会忽略处于省电模式的无线终端，直接将报文发送出去。由于该功能实际上打破了 802.11 协议的定义，会造成处于省电模式的无线客户端无法接收到多播报文，所以仅对特殊场景应用（例如电子书包）可以考虑启用。

3、终端速率限制

该功能是信锐技术产品自研的优势功能，对于距离远的低速终端，拒绝其接入，可以提高其他正常信号范围内用户的上网体验。

通常情况下，离无线接入点越远的地方，终端接入进来的速率会越低。通过限制终端接入的速率，可以限制边缘区域的低速终端接入，这样可以提高无线接入点的吞吐效率，也能防止非目标用户的接入。限制的速率越大，有效的接入范围越小；限制的速率越小，有效的接入范围越大；不限制时，有效接入范围为最大。如果部署无线接入点的密度较大时，接入点的信号覆盖范围会较小，边缘接入的终端速率也相对较大些，如果想限制边缘终端用户接入，可以将限制的速率调大。如果部署无线接入点的密度较小时，接入点的信号覆盖范围会较大，边缘接入的终端速率也相对较小些，如果想限制边缘终端用户接入，可以将限制的速率调小。

4、数据传输速率下限

通常情况下，离无线接入点越远的地方，数据传输速率会越低。通过限制数据传输速率，可以限制边缘区域的低速终端接入，这样可以提高无线接入点的吞吐效率，也能防止非目标用户的接入。

5、限制 beacon 帧发送速率

Beacon 帧发送速率低时，对应睡眠周期拉长，节能省电，但是新连进来的设备就要很久才能显示出来这个 wifi 热点；Beacon 帧发送速率高时，发送 beacon 较为频繁，适合漫游之类的环境，可以高速切换到功率高，性能好的 AP 身上，但是会占用信道传输正常数据。

6、天线 MIMO

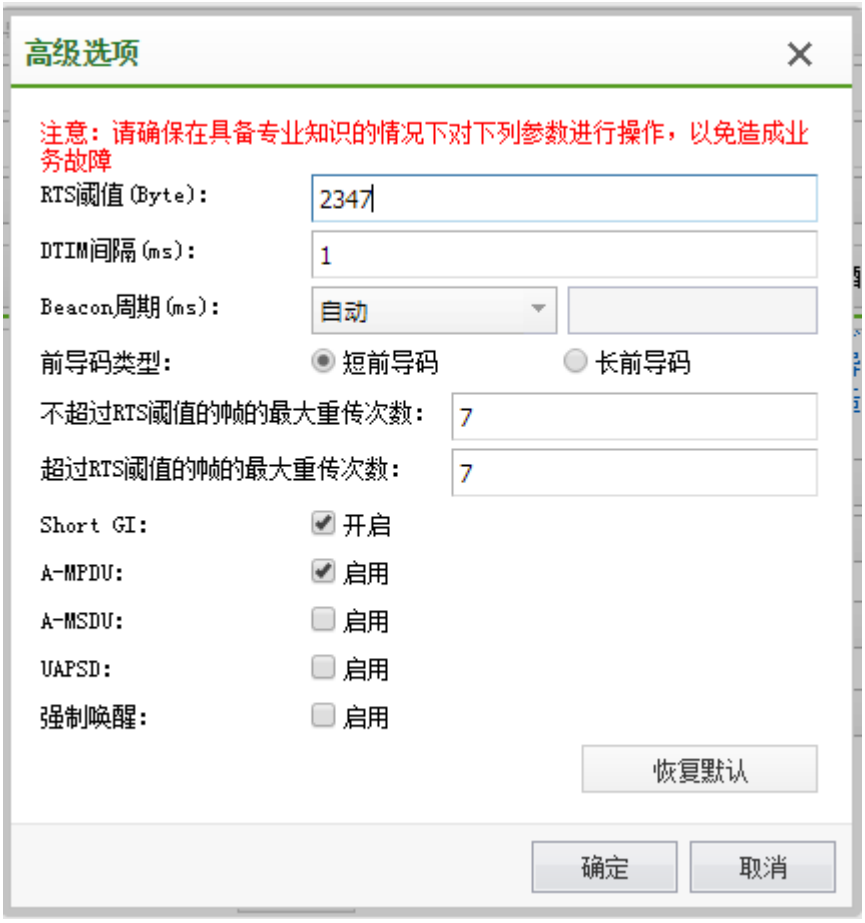
在做室外网桥/中继，或者部署一个狭长区域的时候，往往需要使用抛物面定向天线，但目前很多定向天线，只有 1 个天线接头，很少有支持 2X2 的，即使支持，很多体积和价格都过高，因此为了节约用户成本，需要将接入点上不用的天线关闭掉。

7、高密优化

在无线网络环境中，无论终端是否接入到无线网络，都会定期在每一个信道发送广播 probe request（探测帧请求）。当在无线用户比较多的网络环境中时，会产生大量以低速率发送的 probe reponse（探测帧响应）报文，影响接入点整体的吞吐量。启用高密优化选项后，接入点将不会响应终端广播的 probe request（探测请求），降低了由于低速率发送 probe response（探测帧响应）消耗的性能空间，提升高密度场景用户的无线上网体验。

8、高级选项

涉及到无线数据的传输效率问题，默认不建议也不推荐修改。



4.5.4.2.5. 隧道参数

隧道参数：可以设置 AP 到 NAC 之间的数据隧道是否启用加密。用于设置 AP 与 NAC

之间的控制隧道保活时间，在较差的网络环境中，放大隧道保活时间，可避免因网络抖动造成的 AP 频繁断线，如非必要，一般不建议修改。

4.5.4.2.6. 有线口配置

有线口配置是指 AP 上的物理二层口，可以配置成 Trunk 口和 Access 口。当 VLAN 属性为 Trunk 时，允许 VLAN 是可以放通 vlan 范围，Native VLAN 是判断是否添加或剥离 vlan 头。

4.5.4.2.7. 中继网桥

单个 AP 的参数配置里，还包含“中继网桥”的配置。中继网桥即无线中继与无线网桥，也就是 WDS（Wiresless Distribution System,无线分布系统），通过桥接方式，无线连接不同的局域网以及扩展无线局域网的覆盖范围。

一般用于有线部署不方便或者虽然有有线网络，但是网络拓扑配置不方便的场景。

传统的 wds 实现方式存在如下问题：

（1）client ap 仅仅充当无线天线的功能，所有业务都集中在 root ap 上处理，从无线覆盖的角度来看，root ap 和 client ap 的业务负载是对等的，导致 root ap 和 client ap 上的数据处理负载不均衡，即 client ap 过于空闲，root ap 过于繁忙。另外 root ap 可能会连接多个 client ap，更加重了这种不平衡，使得 root ap 成为了系统局部的一个业务瓶颈。

（2）AP 一旦作为 client ap 的角色，都是不支持企业级认证的，仅仅支持到 wep 和 wpa psk。

（3）配置 client ap 时，必须手动配置指定 root ap，一旦网络拓扑发生变化，需要让 client ap 连接到别的 root ap 时，需要通过无线连接告知 root ap，在操作上比较复杂

而本功能完美地解决了上述存在的不足和缺陷，即：

（1）通过对 client ap 上的业务数据使用不同于传统 wds 机制的处理和转发方式，client ap 可以支持现有 7 种认证方式，即 WPA/WAP2（企业）、开放式、WPA-PSK/WPA2-PSK（个人）、WPA、WPA2、WPA-PSK/WPA2-PSK（个人）+ Web 认证、开放式+Web 认证。

（2）在本功能的实现中，root ap 仅仅只充当交换机的角色，即 root ap 仅负责转发数据，client ap 上的业务有 client ap 自己处理。

（3）client ap 通过自动发现机制发现和连接 root ap，实现了 root ap 的动态主备冗余，当一台 root ap 出现故障的时候，client ap 会自动连接到其他的 root ap 上，避免了 root ap 的单点故障。client AP 动态选路连接 root ap 存在限制条件：client ap 和 root ap 必须属于同一个 AP 分组。

（4）client ap 无法支持控制器灾备。

（5）root ap 上提供给 client ap 建立 WDS 连接的 SSID 和接入密钥以及连接频段可配置。client ap 上支持配置要连接的 root ap 的连接 SSID 以及接入密钥。

注：1)组建 WDS 网络之间的接入点所选择的无线频段必须是相同的。
2）Root 网关模式和 client 普通模式：client 的 wan 口 IP 不可以配成与 Root 的 wan 口 IP 相同网段；client 的 wan 口 IP 要从 Root 的子网上获取， Root 为网关模式时，桥接口为 trunk，native vlan 是子网的默认 vlan。因为 client 的桥接口是 trunk native1， wan 口 vlan 需要默认与 eth0 相同是 vlan1；client 上的用户如果是本地转发, 那么策略 vlan 只能配成 Root 上的子网的 vlan， 在 Root 上的子网内转发。因为 Root 是网关模式， eth0 口是 access1，client 通过桥接发上来的本地转发的带 vlan 的用户报文不能从 Root 的 eth0 转发出去；client 上的用户如果是集中转发, 那么策略 vlan 可以随意配。
3）Root 普通模式和 client 普通模式：client 的 wan 口 IP 应该与 Root 的 wan 口 IP 相同网段；client 上的用户本地转发/集中转发都可以

4）慢速移动桥接：慢速移动桥接主要解决传统无线网卡单链路漫游效果差的问题，提供双链路（client）保证慢速移动过程中的网络连通性，仅支持 NAP3620/AP362 和 NAP3620（R3）/AP 533(R3)。

4.5.4.2.8. 其他配置

1、认证信息转发

将本地转发的用户转发到其他设备，避免再次认证。

2、认证页面缓存

适用于远程部署的接入点，可以节省接入点和控制器之间的流量。该功能将认证页面缓存到内存中，不需要接入点的 USB 支持。

3、无线信息采集

配置接入点上是否上报终端发现信息、邻居接入点的信息到控制器。

4、USB 接口工作模式

对于有 USB 接口的接入点，USB 口的工作模式。需要将应用加速功能缓存到接入点时，请将模式配置为 USB 缓存功能。

5、上联口链路检查

此功能用于当接入点上联口出现异常时通过重启接入点的方法进行自动恢复。 上联口链路检查默认开启，默认 600s。此功能触发需要满足以下四个条件：接入点和控制器断开隧道； 接入点 ping 不通网关和控制器；接入点上联口 up；接入点上联口 rx tx 都不变。

6、蓝牙工作模式

此模式仅支持蓝牙的 AP（NAP4650）可配置，可结合微信摇一摇.周边使用，其中参数由微信摇一摇周边提供。

7、烟感配置

烟感 AP 可以检测是否发生火灾，在部署烟感 AP 的地方如果有火灾出现迹象，烟感 AP 会立即告警，并将检测到的告警信息同步到控制器

蜂鸣方式：长鸣或者短鸣；长鸣是指：蜂鸣器鸣叫期间不会暂停；短鸣是指：蜂鸣器鸣叫期间蜂鸣器暂停和鸣叫交替进行。

启用烟雾消失后停止蜂鸣：如果烟感检测到无烟雾时会停止蜂鸣器鸣叫，未启用则蜂鸣器会一直鸣叫，烟雾消失时，鸣叫也不会停止

手动停止蜂鸣器鸣叫，需要在无线状态对应 AP 中设置烟感探测暂停选项

目前只支持 AP-360-SD/NAP-3600-SD。

8、2/3/4G 线路

此功能通过 4G 模块解决公交车等不能部署有线场景上网的问题。有线和 4G 模块都可以做为 AP 的出口，优先使用哪个页面可配，优先链路网络恢复后，可切换到优先链路。

9、延迟下电

开启此功能后，当车用 ACC 电源关闭时，AP 会延迟指定的时间再关闭系统，用于防止车辆中途短时间熄火导致 AP 系统不稳定。

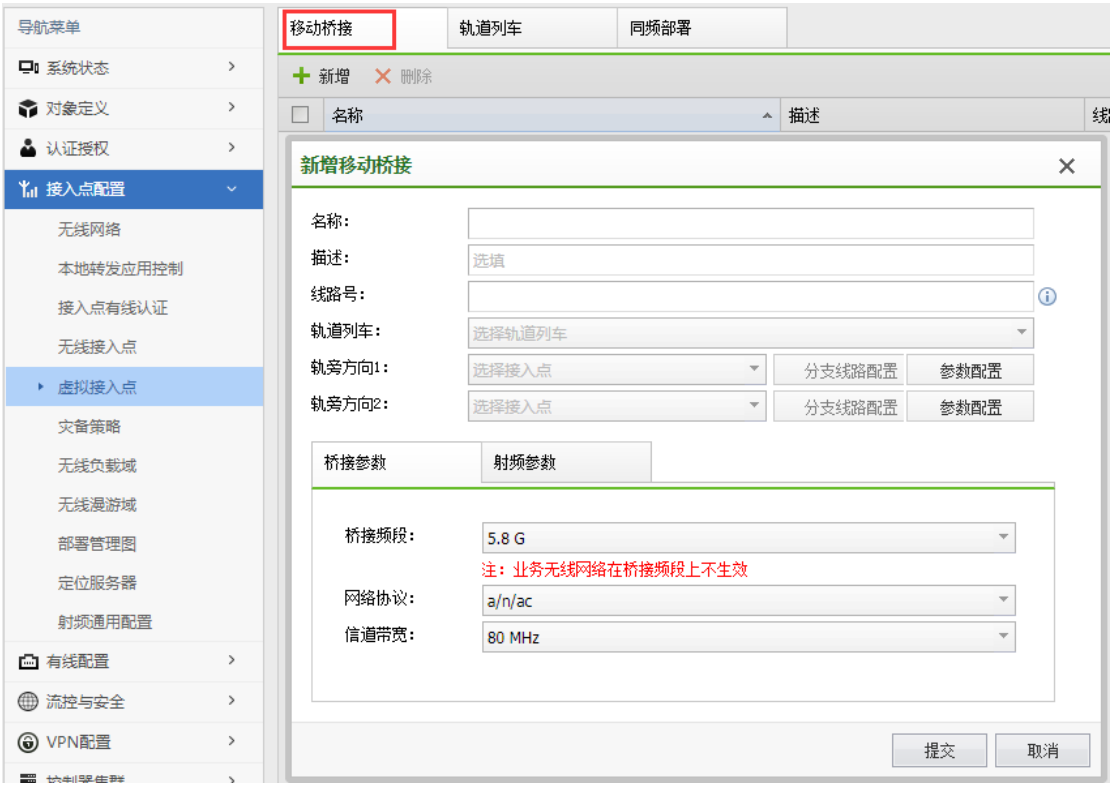
4.5.5. 虚拟接入点

虚拟接入点包含【移动桥接】、【轨道列车】、【同频部署】这几个功能。

4.5.5.1. 移动桥接

移动桥接配置轨道 WIFI 功能，该功能是专门针对轨道交通行业用户使用场景设计的，可以满足乘客从进入站台、站台候车、列车运行、到站下车、离开站台，整个过程中都能正常使用免费 WIFI，可以有效解决运营商的网络在轨道交通行业在一些位置和列车运行过程中网络不稳定和无信号覆盖，从而导致乘客上网体验差的问题，同时结合信锐完善的用户画

像、定位和商业推广功能，增加了轨道交通运营商的广告与营收的机会。



1、车头接入点

车头接入点是指列车头、列车尾用于和轨旁进行数据转发的 AP，此 AP 不能配置业务 wlan，车内乘客也无法接入该 AP 的 wlan 上网，车头接入点可以配置 Trunk vlan 的 Native VLAN 和允许 VLAN，不能配置信道(自动匹配轨旁路线 AP 的信道)。

2、轨旁路线

轨旁路线是指列车运行过程中，轨道旁边的所有 AP 组成的网络，列车运行过程中车头接入点要实时与轨旁路线里面对应的 AP 建立车地链接，把列车内上网需求通过无线的方式转接到轨旁路线 AP，轨旁路线 AP 再接入有线轨道交通系统，保证网络连通性，根据轨道部署实际方案，可以在不同的方向建立不同的轨旁线路，来满足列车在不同的行驶方向分别建立车地通信，轨旁路线中的 AP 不支持配置业务 wlan，轨旁路线可以配置 Trunk vlan 的 Native VLAN 和允许 VLAN，能配置桥接信道。

3、桥接参数

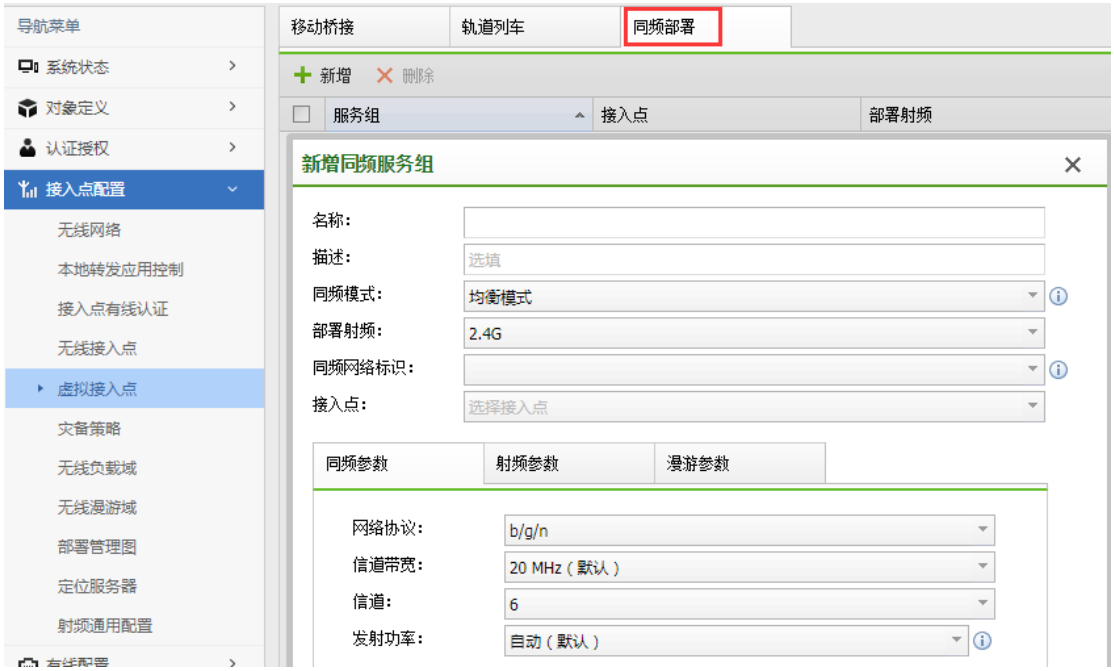
SSID 和接入秘钥是车头接入点与轨旁路线建立车地通信关键参数，车地通信的桥接频段限定为 5.8G(该频段可以更好的保证车地通信的效果)，网络协议和信道带宽根据实际需要配置，业务无线网络在桥接频段上不生效。

4、射频参数

只能配置 5.8G 频段，发射功率是给车头接入点、轨旁路线的 AP 统一配置发射功率大小，高级选项请确保在具备专业知识的情况下对下列参数进行操作，以免造成业务故障。

4.5.5.2. 同频部署

同频部署是针对医疗查房及工厂车间等对无线连接的稳定性有较高要求的应用场景提供的无线漫游解决方案，为生产终端提供零漫游的无线网络覆盖。终端在零漫游的无线网络中自由移动时，保障业务流量不中断。此功能致力于解决终端在传统蜂窝部署的无线网络中因位置移动产生漫游而导致的业务中断问题，提高行业用户的生产效率。



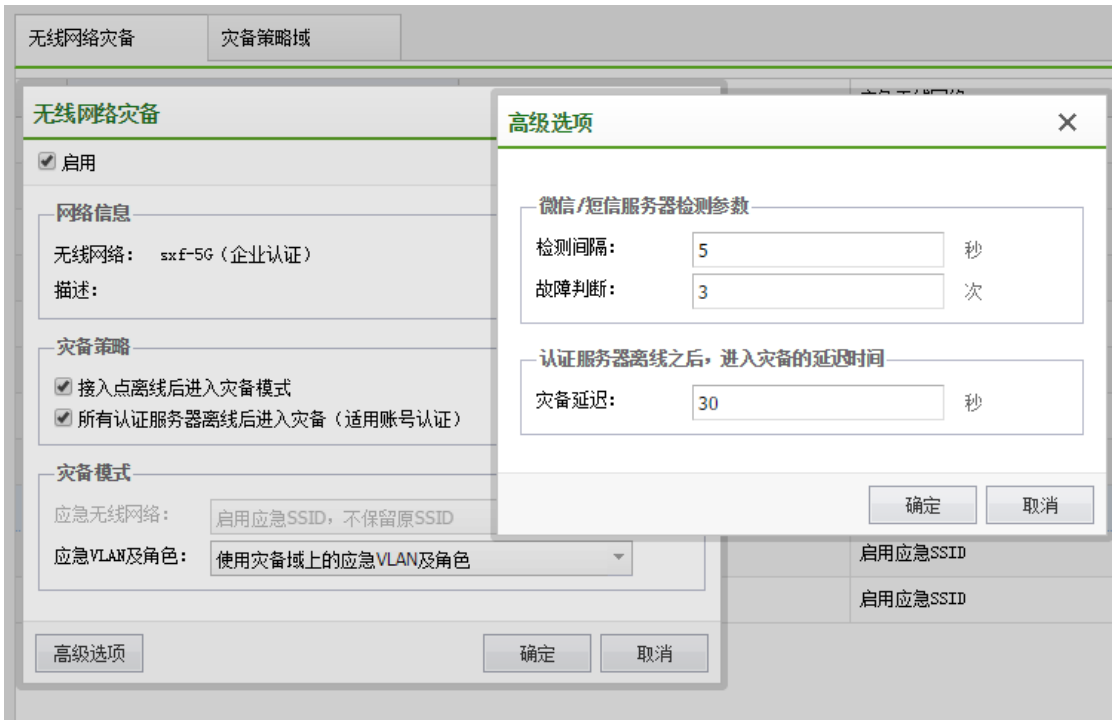
同频服务组是配置零漫游无线网络(同频无线网络)的基本组。新增同频服务组时，需要指定同频频段、选择同频接入点。零漫游无线网络配置时选择相应同频服务组配置即可。

零漫游无线网络(同频无线网络)可以在 2.4G 和 5.8G 两个频段建立零漫游的无线网络，分别同时支持 WPA/WPA2(企业)、WPA-PSK/WPA2-PSK(个人)等多种认证方式，满足客户不同生产场景下的设备接入要求。

4.5.6. 灾备策略

4.5.6.1. 无线网络灾备

用于配置无线网络在接入点在无法连接无线控制器、用户认证服务器、短信服务器或微信服务器进入灾备模式的时候，这个无线网络使用哪个应急无线网络、应急 VLAN 和角色。



高级选项

灾备延迟：是指认证服务器与控制器断开连接后，延迟多长时间生效灾备。

检测间隔：检测微信\短信服务器的间隔时间。

故障判断：检测到服务器连续故障多少次，才认为需要生效灾备。

4.5.6.2. 灾备策略域

用于将无线接入点划分为不同的区域，配置这个区域下接入点进入灾备的条件和进入灾备后使用的应急 VLAN 和应急角色。

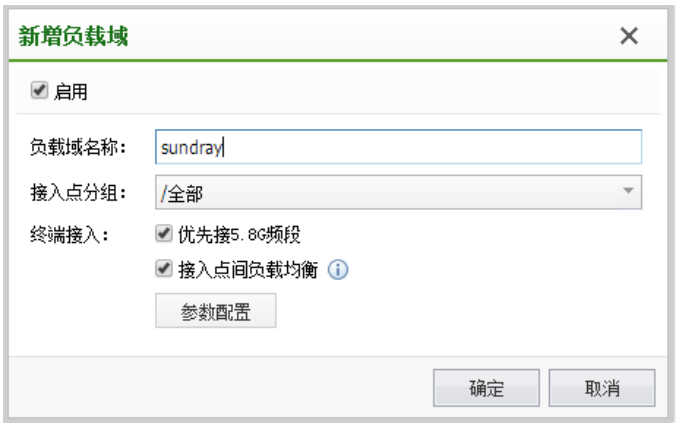
注意：

应急 VLAN 环境下必须存在 DHCP 服务器，否则终端无法获取到 IP 地址。

无线网络根据不同用户信息匹配不同用户 vlan，灾备模式下都会使用同一个灾备 VLAN。

4.5.7. 无线负载域

按接入点分组划分出一个区域，控制该区域的终端接入时是否优先接入 5.8g 频段、是否开启接入点间负载均衡和动态负载引导，也可以控制该区域的射频是否需要射频信号覆盖补偿。



4.5.7.1. 优先接入 5.8G 频段

用来引导双频无线客户端优先接入无线环境中的 5.8G 网络，勾选后，可以提高 5.8G 网络的利用率。

4.5.7.2. 接入点间负载均衡

客户端连接无线网络时，如果同时探测到多个接入点的信号，通常会选择连接信号强度最高的接入点。这可能会导致相邻的几个接入点间，负载不平衡，例如某个接入点服务了大量的用户，但临近的另外一个接入点仍然比较空闲。

启用接入点间负载均衡功能后，在用户接入网络时，如果已连接用户数超过指定值时，将会执行负载均衡(当无线客户端连接到某个繁忙的接入点后， 此接入点将拒绝该客户端接入， 迫使无线客户端漫游到一个附近较空闲的接入点。 如果拒绝失败，则会使用漫游引导报文， 引导无线客户端漫游到人数较少， 信道利用率较低的接入点)，以平衡接入点的负载。 负载均衡操作只会在物理上邻近，且处于相同分组的接入点间进行。

符合较空闲的接入点必须满足两个条件：

检测到无线客户端信号强度大于等于页面上配置的信号强度阈值；

邻居接入点上的接入人数减去该接入点上接入人数的差值大于页面上配置的接入人数差值。比如： 邻居接入点上的接入人数为 10，页面上配置的接入人数差值为 3，则此时该接入点上的接入人数应该小于等于 10-3=7。

4.5.7.3. 动态负载引导(防终端粘滞)

动态负载引导功能是指终端距离接入点较远时，接入点主动使终端发生漫游，提高终端上网体验。即接入点检测到的终端的信号强度小于信号强度阈值，并且该终端的无线流量小于阈值流量时，接入点会使终端发生漫游。 仅使用 1 台 AP 时不建议启用该功能。

1、负载参数：只有负载参数同时满足时，优先接入 5.8G 频段和接入点间负载均衡才会被触发。

2、人数阈值：接入点上达到的在线用户数，建议取值为 10。

3、人数差值：用来决策可接入的邻居接入点，建议取值范围[1,5]。AP 部署密度较大时，

取值越大体验越好；AP 部署密度较小时，取值越小体验越好。

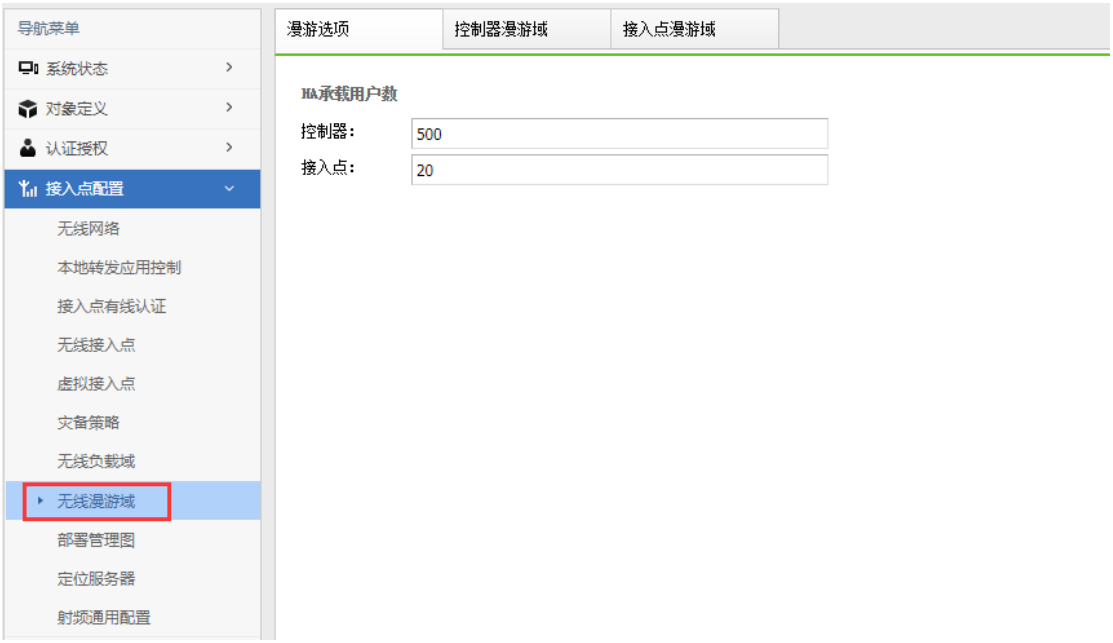
4、信号强度阈值：用来决策参与负载均衡的邻居接入点， 建议取值范围[-90, -70]。AP 部署密度较大时，取较大值效果较好；AP 部署密度较小时，取较小值效果较好。

5、总信道利用率：用来决策参与负载均衡的接入点，建议取值范围为[60,90]，其中：总信道利用率=环境中的信道利用率+自身信道利用率。

6、弱终端参数：只有弱终端参数同时满足时，动态负载引导才会被触发。

7、智能射频：射频信号覆盖补偿，接入点异常/离线时，由邻居接入点自动放大功率进行信号覆盖

4.5.8. 无线漫游域



4.5.8.1. 功能概述

1、主要解决的客户问题

（1）终端跨 VLAN 漫游时，偶尔会出现终端没有重新获取 IP 地址的情况，导致无法上网；

（2）终端跨设备跨 VLAN 漫游时，偶尔会出现终端没有重新获取 IP 地址的情况，导致无法上网。

2、给客户带来的价值

终端在跨 VLAN 漫游和跨设备漫游时，可以继续上网。

4.5.8.2. 配置方法

控制器漫游域对集中转发生效。漫游域针对组网需要跨 VLAN 漫游的情况，如组网不涉及跨 VLAN 漫游，则无需使用控制器漫游域。

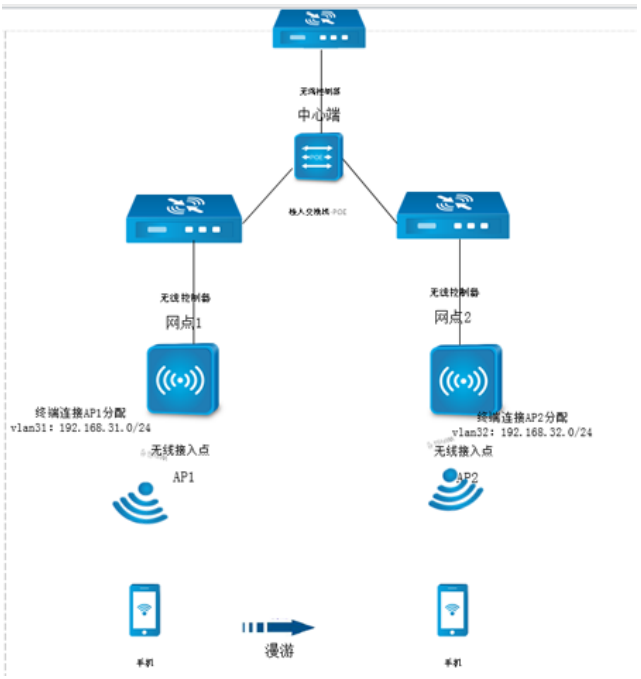
1、同控制器漫游：终端在同一台控制器上漫游

（1）存在如下集中转发的组网，为解决终端从接入点 1 漫游到接入点 2 能继续上网，漫游域配置如下。

（2）控制器漫游域的 HA 网络是给终端分配的 VLAN 和 IP，将需要漫游的 IP 和 VLAN 写到一个漫游域中，终端连接无线网络 VLAN31 对应的地址段 192.168.31.0，VLAN32 对应的地址段为 192.168.32.0，归属则选择本控制器。

2、跨控制器漫游

（1）存在集中认证且网点集中转发如图的组网，为解决终端跨控制器漫游可以正常上网，漫游域配置如下：



（2）添加漫游控制器的通信地址。

、

（3）根据设备分配的 VLAN 配置控制器漫游域，将需要漫游的 VLAN 和 IP 地址写到一个漫游域中，终端连接网点 1 控制器上的接入点分配 VLAN31 的地址段 192.168.31.0/24，终端连接网点 2 控制器上的接入点分配 VLAN32 的地址 192.168.32.0/24。

3、控制器 HA 承载用户数

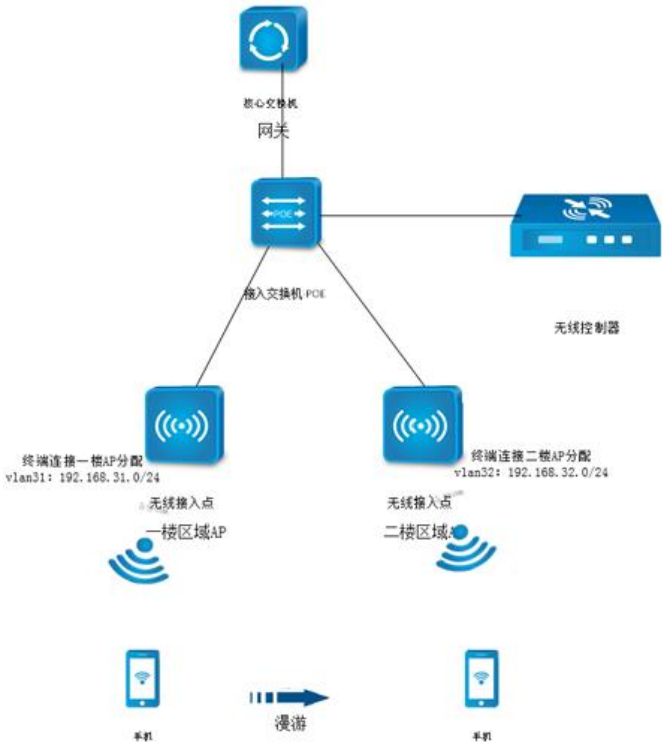
跨控制器漫游的时候，允许漫游回家乡控制器的最大用户数，如果漫游的用户数超过该阈值，则踢除用户让其重新连接，减轻家乡控制器压力。

四、接入点漫游域配置方法。

接入点漫游域对本地转发生效。漫游域针对组网需要跨 VLAN 漫游的情况，如组网不涉及跨 VLAN 漫游，则无需使用漫游域。

（1）同控制器漫游

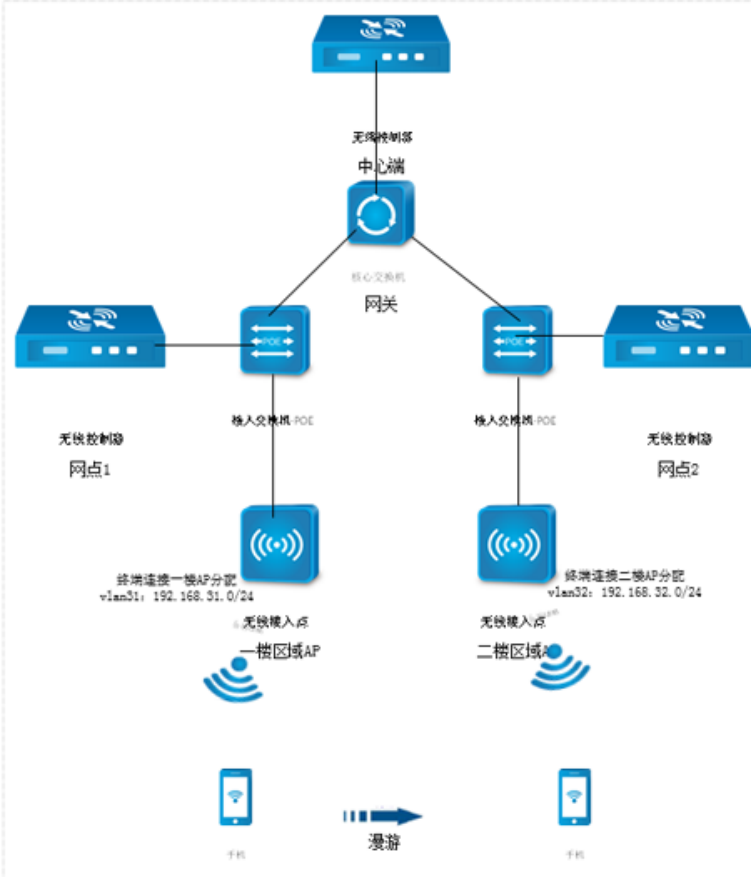
1.存在如下本地转发的组网，为解决终端从接入点 1 漫游到接入点 2 能继续上网，漫游域配置如下：



2.根据 VLAN 分配的地址配置接入点漫游域，将需要漫游的 IP 和 VLAN 配置在同一个漫游域中。终端连接一楼区域接入点分配 VLAN31 的地址段 192.168.31.0/24，终端连接二楼接入点分配 VLAN32 的地址 192.168.32.0/24。

（2）跨控制器漫游。

1.存在集中认证且网点本地转发如图的组网，为解决终端跨控制器漫游可以正常上网，漫游域配置如下：



2.添加漫游控制器的通信地址。

3.根据设备分配的 VLAN 配置控制器漫游域，将需要漫游的 IP 和 VLAN 配置在同一个

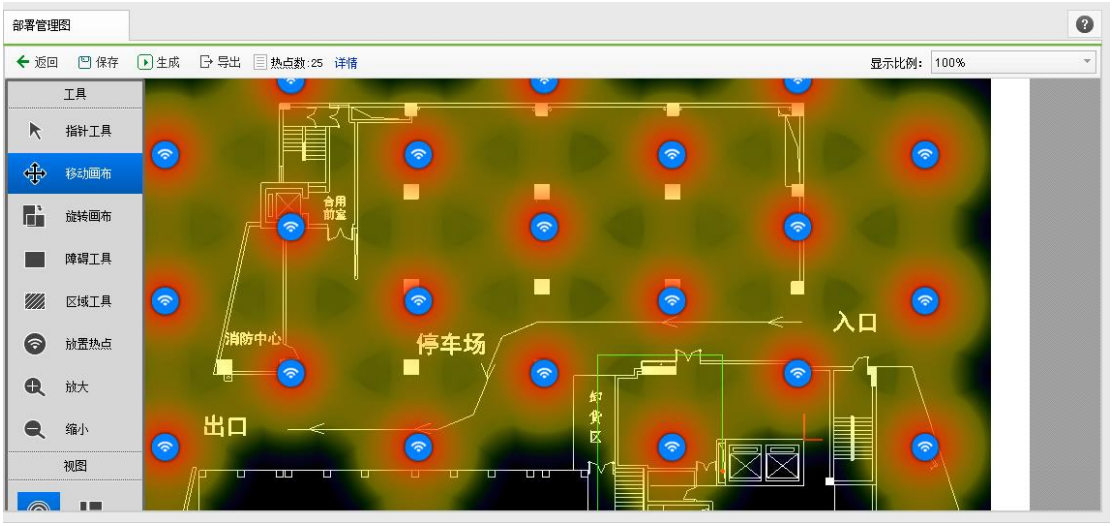
漫游域中，终端连接网点 1 控制器上的接入点分配 VLAN31 的地址段 192.168.31.0/24，终端连接网点 2 控制器上的接入点分配 VLAN32 的地址 192.168.32.0/24。

（3）接入点 HA 承载用户数。

本地转发漫游的时候，允许漫游回家乡接入点的最大用户数，如果漫游的用户数超过该阈值，则踢除用户让其重新连接，减轻家乡接入点的压力。

4.5.9. 部署管理图

部署管理图可以用于建模工勘，评估 AP 使用个数，以及展示信号覆盖情况。

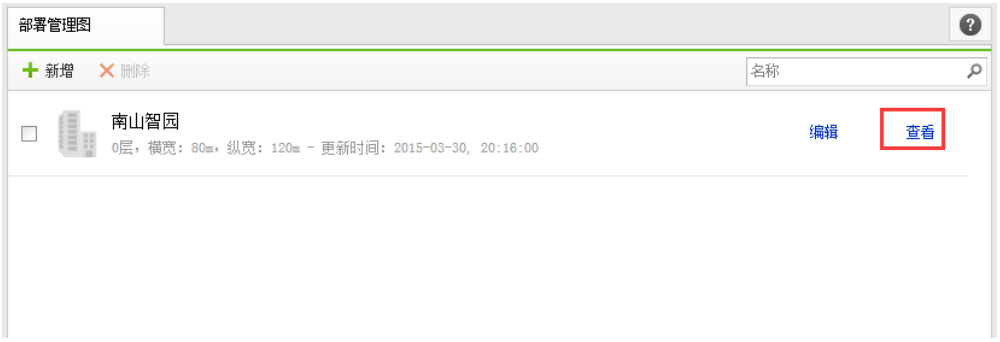


4.5.9.1. 建筑物列表页面

用于管理建筑物。基于建筑物创建的楼层会继承建筑物的尺寸数据、单位及接入点型号。

4.5.9.2. 楼层列表页面

固定接入点个数。 要求用户指定 AP 的个数。该选项用于用户知道 AP 数量但不知道如何部署的场景，系统可以给出参考性的部署建议。



帮我确定接入点个数。要求用户输入编辑楼层大概有多少数量的用户接入到无线网络。该选项用于用户不知道 AP 的数量，也不知道如何部署的场景。系统可以给出参考性的 AP 数量和部署建议。

4.5.9.3. 部署页面

障碍物。所有对无线射频信号产生衰减作用的物体的统称。比如砖墙，混凝土墙，木门，玻璃窗等等。

不需要覆盖 WLAN 的区域。在该区域标识的范围内，系统不会部署任何 AP。

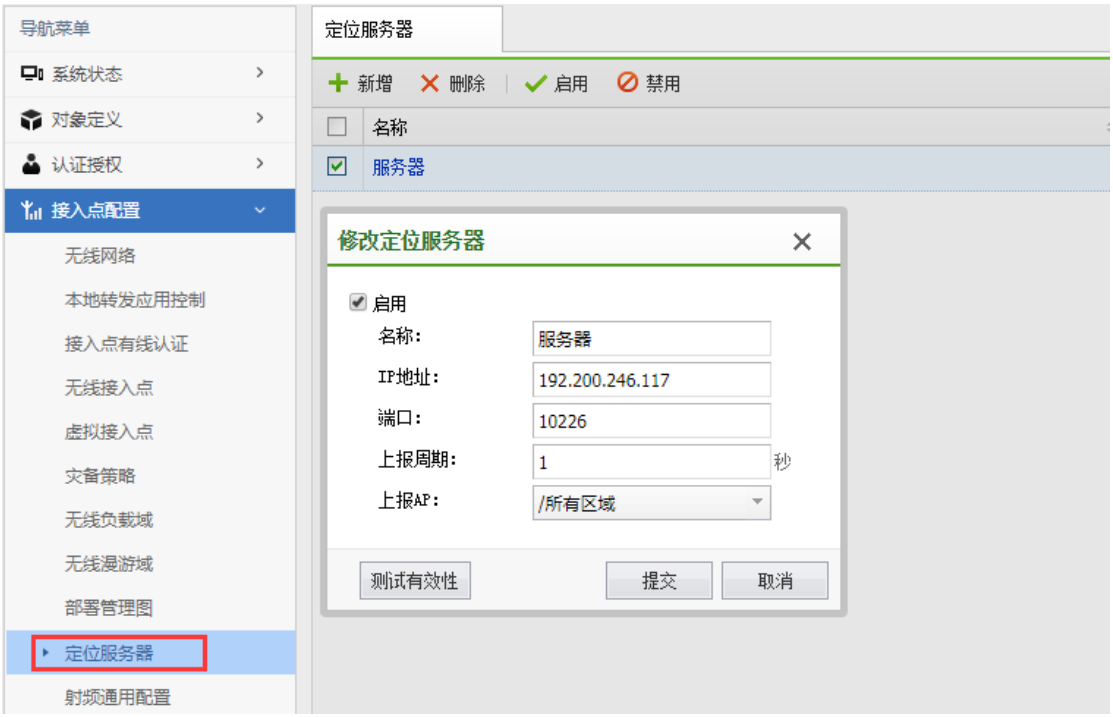
WLAN 覆盖区域。该区域可以用于因接入人数不同而有特殊要求的场景，例如食堂等大部分时间没有人的地方可能不需要部署太多的 AP，但又要求有信号覆盖的时候，可以用该区域；或者在会议室这种接入人数比较密集的地方也可以使用该区域。

信号视图。该视图将显示 AP 的信号覆盖状态。

布局视图。该视图将隐藏 AP 的信号覆盖状态，用户只能看到 AP 的布放位置。

4.5.10. 定位服务器

开放接口包括定位服务器，目前无线控制器做定位需要结合第三方定位厂商一起做定位，我们的无线仅提供底层信息数据支持。

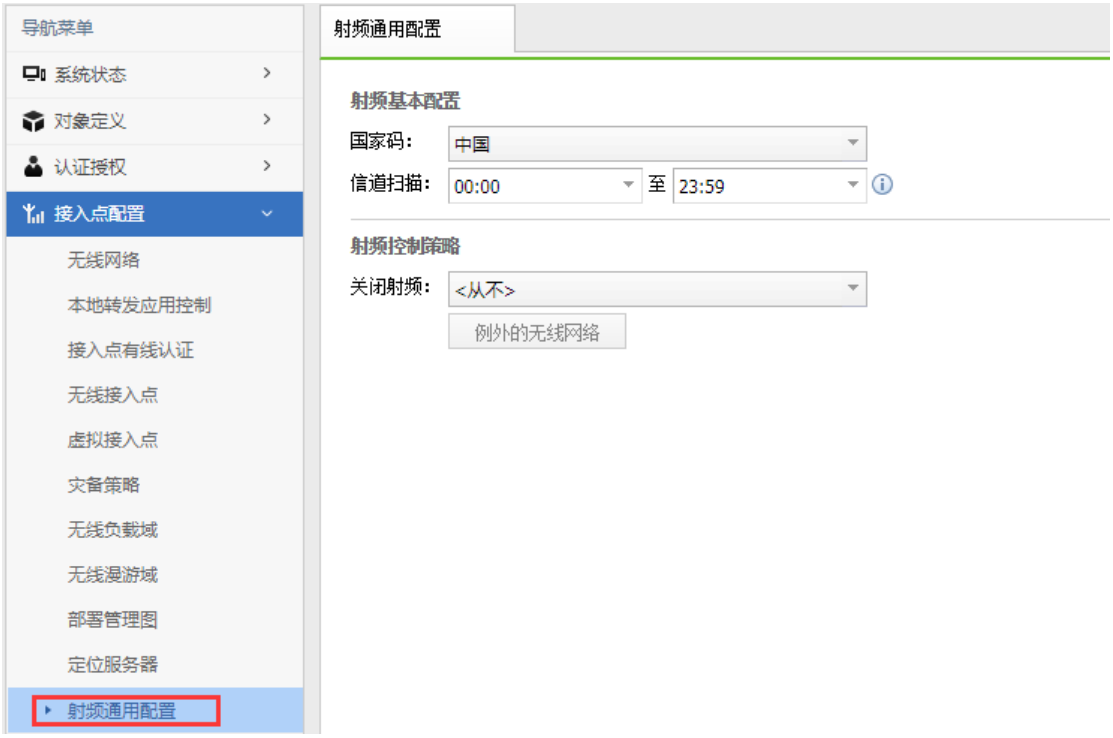


针对自己拥有定位算法的客户，我们提供了定位所需的数据。

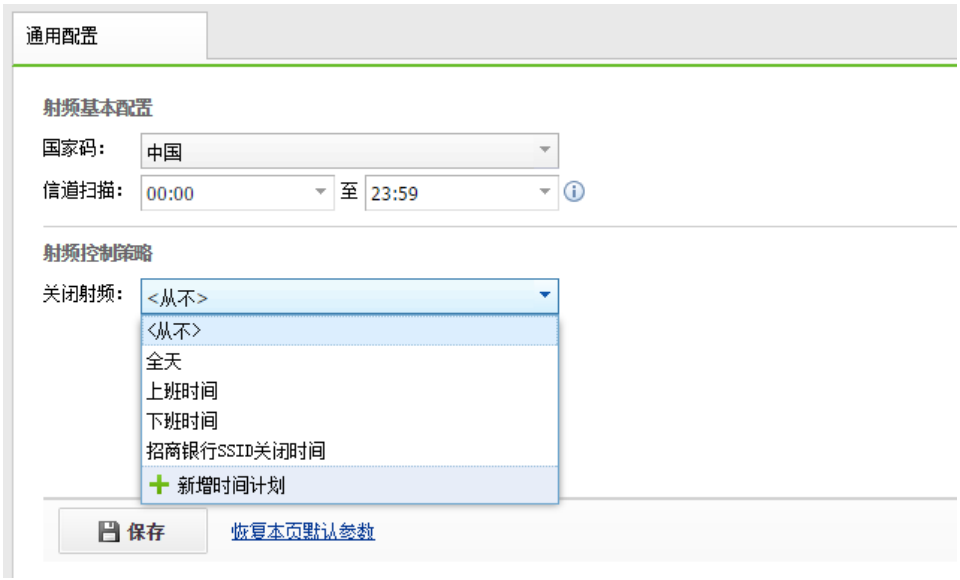
配置定位服务器，可以获取的信息：AP 的 MAC 地址、STA 的 MAC 地址、射频类型、无线信道、终端类型、是否关联上 AP、关联 AP 的 MAC 地址、信号强度 RSSI、底噪 noise floor 等。开启此功能需要开启定位服务器序列号。

4.5.11. 射频通用配置

当选择不同的国家码时，AP 可以工作的频率范围是不一样的，可以根据当地法律选择不同的国家码。



射频控制策略，可以选择 AP 信号发射信号时间，比如下班时间自动关闭 WIFI 射频信号，一定程度上可以提升安全性以及省电。



4.6. 有线配置

4.6.1. 接口管理

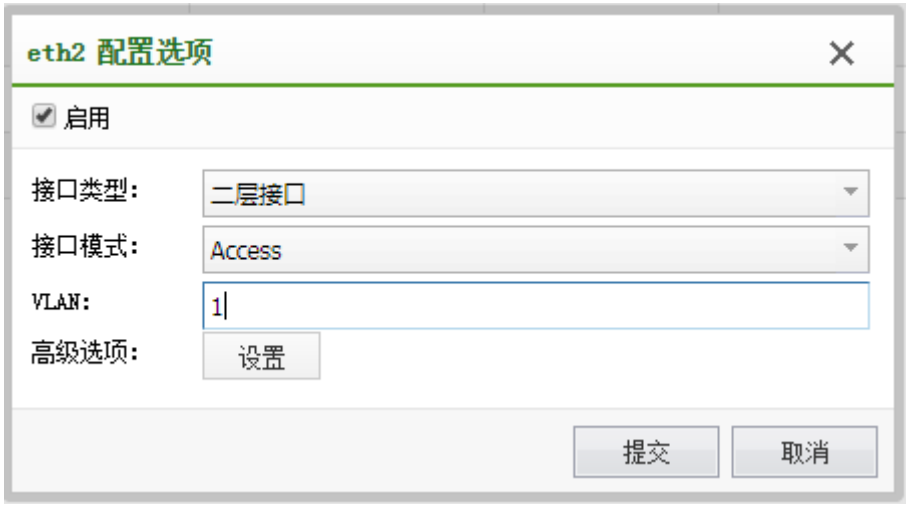
接口管理主要用于设置接口的 IP 地址以及工作模式，接口的工作模式是由部署需求决定的，需要根据网络环境设置合理的接口地址与工作模式，NAC 才能正常工作。

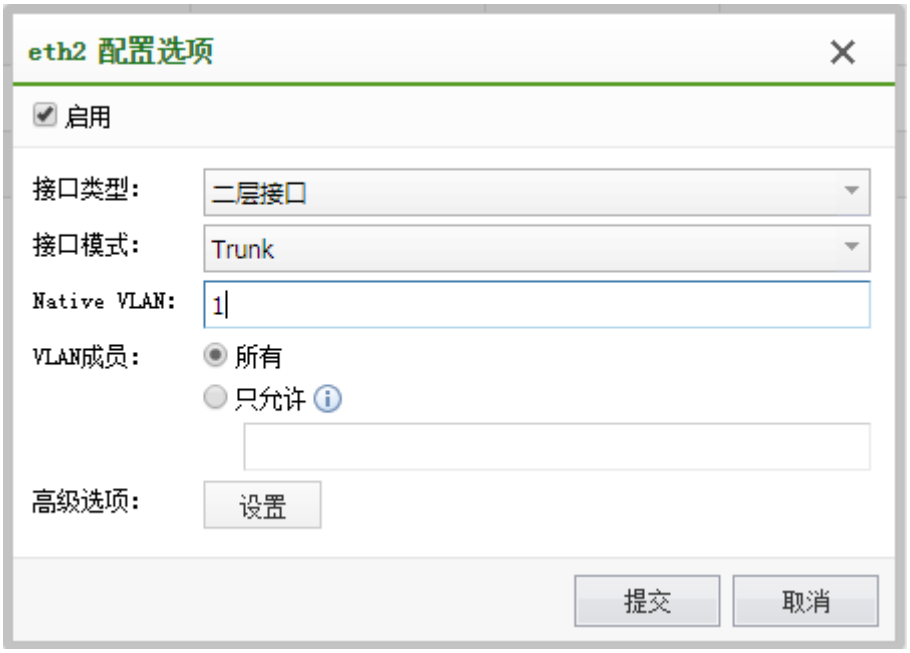
4.6.1.1. 物理接口

物理接口中，eth0 默认是管理口，属性是 3 层路由口，默认 IP 地址是 10.252.252.252，掩码：255.255.255.0。

4.7.1.1.1 二层接口

接口可以设置为 2 层接口，2 层接口包括 access 模式和 trunk 模式两种，截图如下：



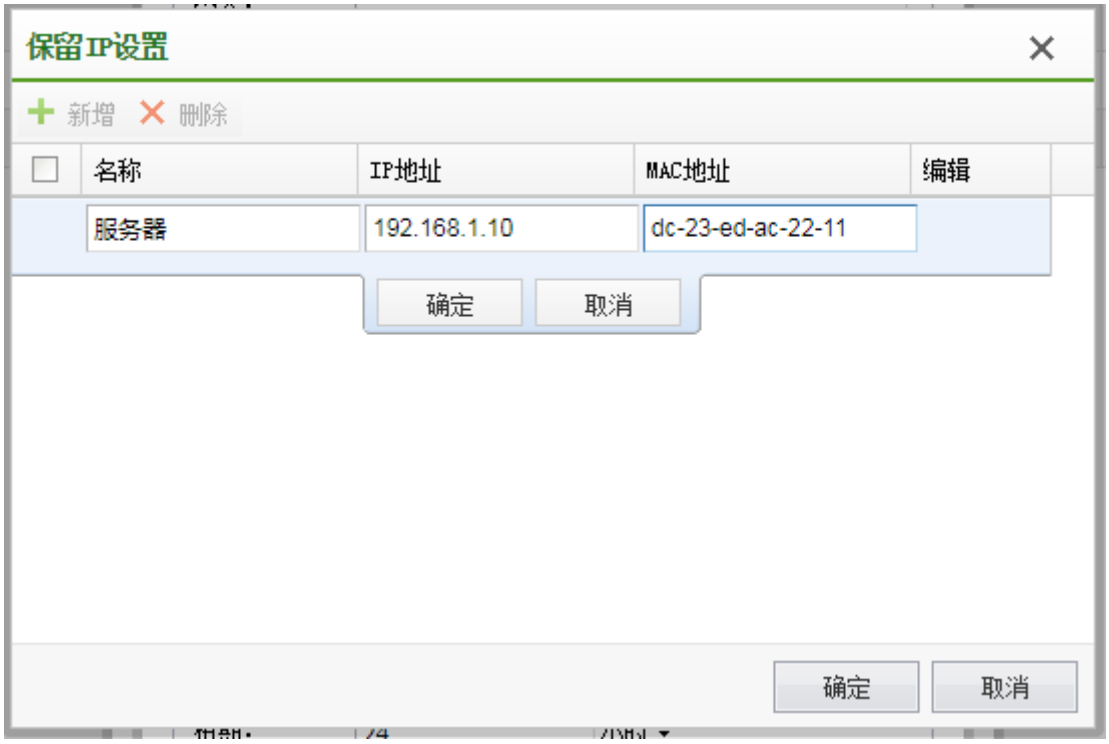


4.7.1.1.2 三层接口

三层接口支持自动获取 IP，配置固定 IP、PPPOE 拨号，当配置固定 IP 时，可以启用配置 DHCP 服务器，配置 DHCP 方法与地址池如下：

NAC 的 DHCP 配置比常规的 DHCP 服务器多了一个 option43 的选项，该选项的 IP 一般建议填写 NAC 的 IP，主要用户 AP 自动获取 IP 时，如果 DHCP 服务器是 NAC，获取 option43 字段的 IP 地址时，会自动向该 IP 发起自动发现协议的数据报文，让 AP 可以自动发现 NAC，并加入 NAC 的管控。

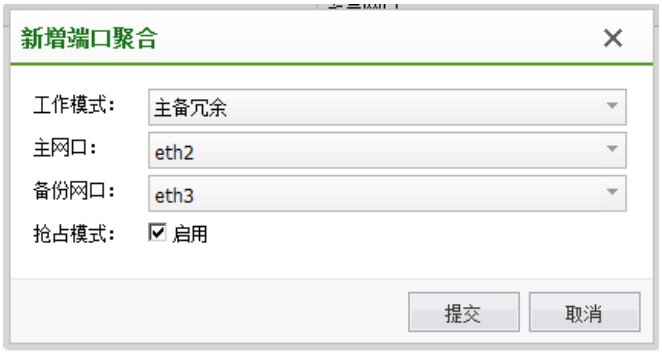
保留 IP 地址可以将保留下来的地址分配给某个固定的终端。



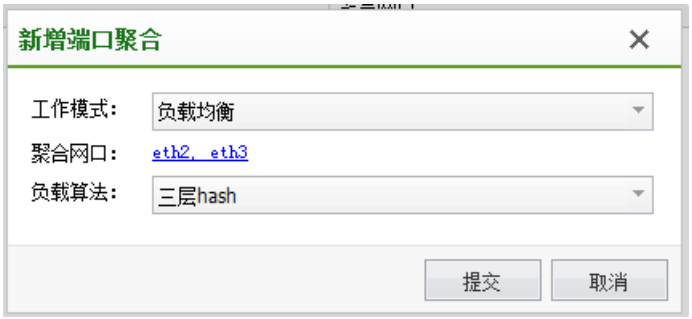
4.6.1.2. 端口聚合

当有需要使用多个网口聚合的环境时，可以配置端口聚合功能，控制器使用的聚合协议为 lacp 如下图：

聚合接口包括主备模式的，主接口先跑流量，当主接口故障时，备份网口启用，如果启用抢占模式，当主接口从故障中恢复过来时，会抢占优先跑数据。

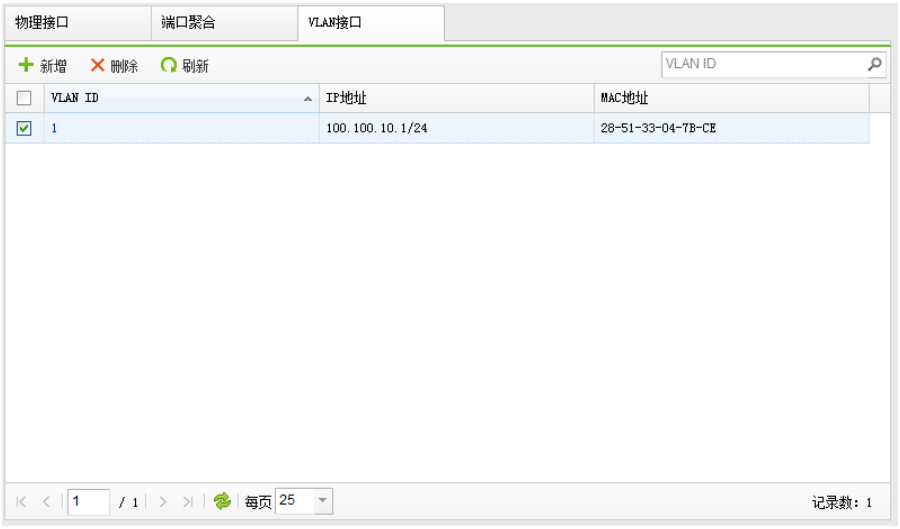


聚合接口还可以有负载均衡的方式，负载均衡时，可以选择多个网口，以 3 层 Hash 方式或 2 层 Hash 方式进行负载，如下图：



4.6.1.3. VLAN 接口

VLAN 接口在需要配置 3 层虚拟接口的时候可以配置，配置界面如下：



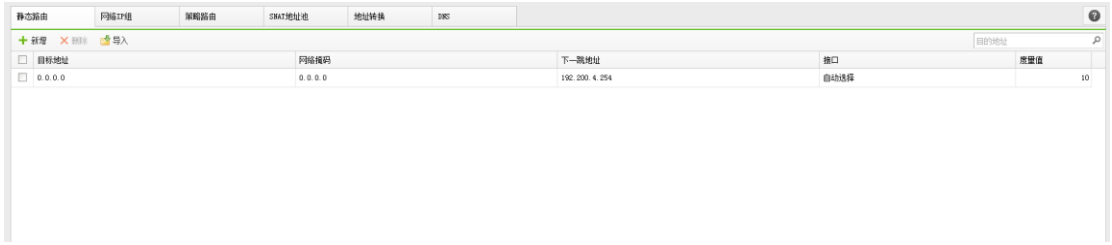
编辑 VLAN 接口界面如下，也可以启用 DHCP 服务，方法与界面同物理接口的 3 层口配置：

4.6.2. 网络配置

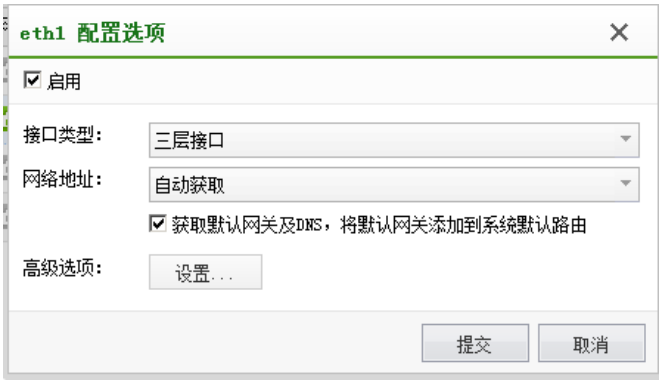
网络配置主要包括以下模块：【静态路由】、【网络 IP 组】、【策略路由】、【SNAT 地址池】、【地址转换】、【DNS】六个部分。

4.6.2.1. 静态路由

静态路由：静态路由，填写目的地址，网络掩码，下一跳，并选择自动选择接口，并设置度量值即可。一般为了保障 NAC 能正常上网，需要配置 8 个 0 的默认静态路由，尤其是在【接口管理】处，配置的 3 层接口都是手动配置时。



当 3 层接口配置了 DHCP 时，可以勾选设置默认网关自动添加系统路由，也会后台自动添加 8 个 0 的默认静态路由，保障 NAC 可以正常上网，如下图：



4.6.2.2. 网络 IP 组

4.6.2.3. 策略路由

策略路由可以根据不同的源 IP 和目的 IP，以及协议，自动选择下一跳进行数据包发送选路，更好的适应的复杂网络环境的适应能力，如下图：

4.6.2.4. SNAT 地址池

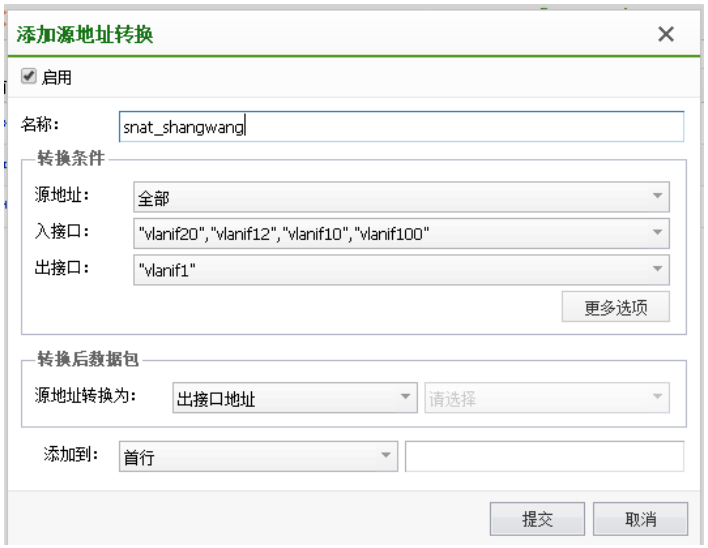
4.6.2.5. 地址转换

地址转换包括【源地址转换】、【目的地址转换】、【双向地址转换】三种类型，下面

将一一介绍

4.6.2.5.1. 源地址转换

源地址转换也称为 SNAT，主要用与给无线终端设置代理上网规则的，当无线终端采用集中转发模式，并给无线终端分配了私有 IP 地址时，一般都需要在 NAC 上配置源地址转换的代理上网规则。



4.6.2.5.2. 目的地址转换

目的地址转换也叫做 DNAT，常用于内网有服务器需要发布，NAC 以网关模式部署时，对内网进行端口映射，配置方法如上图。该功能针对无线终端用户用得很少。

4.6.2.6. DNS

配置 NAC 设备的自身上网的 DNS 服务器，用于 NAC 自身的上网，NTP 服务同步，系统更新以及针对内网启用 DNS 代理功能。

当启用 DNS 代理功能时，内网的 PC 和无线终端，可以设置设备的接口作为 DNS 服务器解析服务器来配置，可以保证这些用户能正常解析域名上网。

4.6.3. 线路带宽

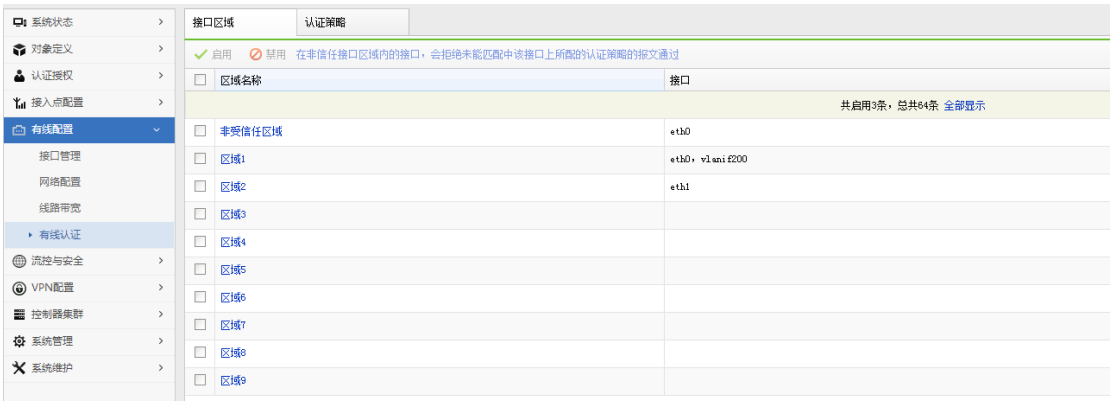
线路带宽配置是为了，在流控与安全中，调用时使用。线路带宽基于接口配置，且 NAC 没有明显区分外网口与内网口，从某个接口进，则这条流对于这个接口属于下行，从某个接口出，则这条流对这个接口属于上行。有需要时，可以针对内网和外网设置不同接口对应线路来进行流控。

设备在正常转发数据的时候，数据会从一个接口进，从另外一个接口出，在这个接口上配置了线路，经过这个线路的数据才能被流控，最多支持 16 条线路(设备型号不同支持最大线路数不同)。 在配置线路的时候，接口类型可以有多种选择：物理口、三层 vlanif 口、二层聚合口，可以根据不同的组网需要选择不同类型的接口。在选择接口的实时候需要遵循以下几个原则：

第一：如果已经配置了一条 vlanif 口，同时某个二层口在这个 vlan 内（access 的 vlanid 为该 vlanifid，或者 trunk vlan 列表中有该 vlan），那么这个二层口就不允许再配置成一条新的线路。 第二：如果一个二层口和一个 vlanif 接口都配置成线路，修改这个二层接口的 vlan 属性时，不能修改为线路中 vlanif 接口的 vlan 值。 第三：配置线路时，不能选择聚合口下面的物理接口。

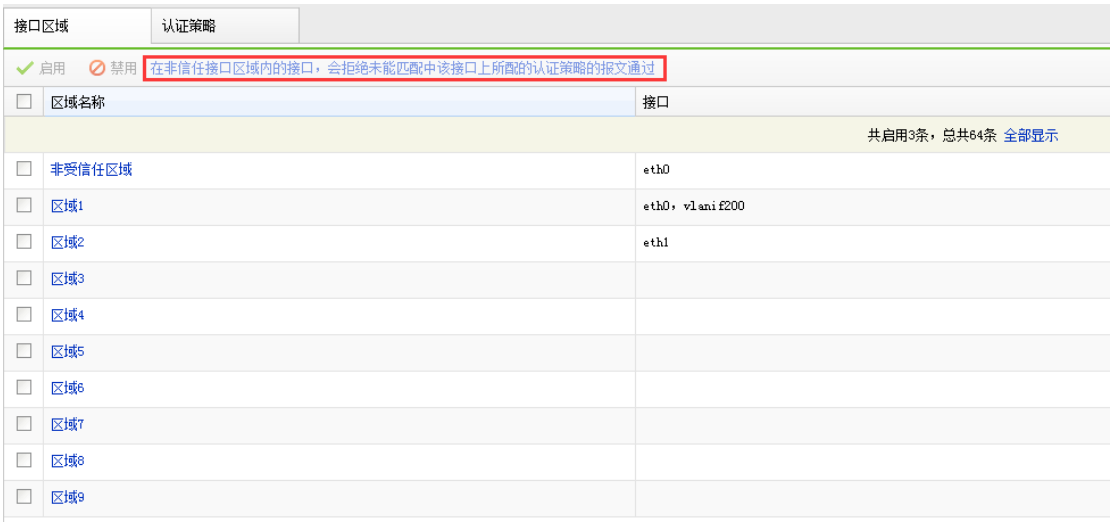
4.6.4. 有线认证

经过 NAC 控制器的有线用户，可以选择对有线用户进行认证，认证策略在【有线配置】-【有线认证】下配置策略。



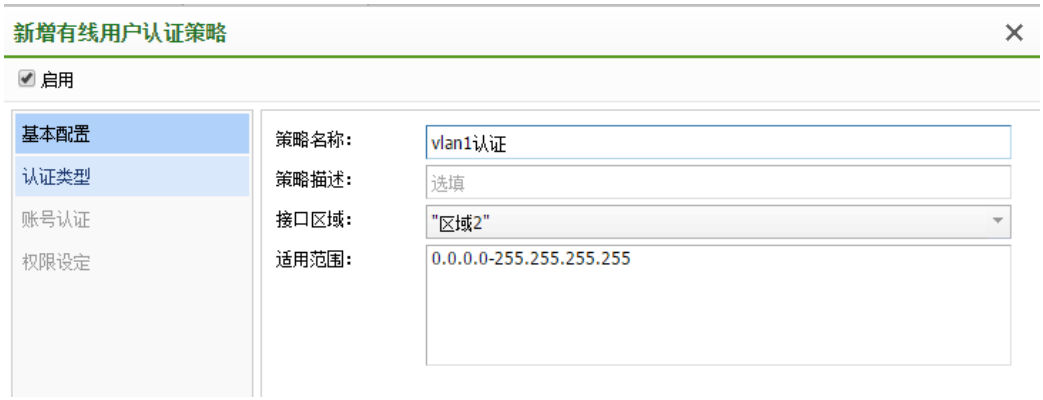
4.6.4.1. 接口区域

控制器认证配置，可以对认证做出一些特殊配置，比如通过定义非信任接口直接拒绝掉某个接口的所有流量，不再采取认证。



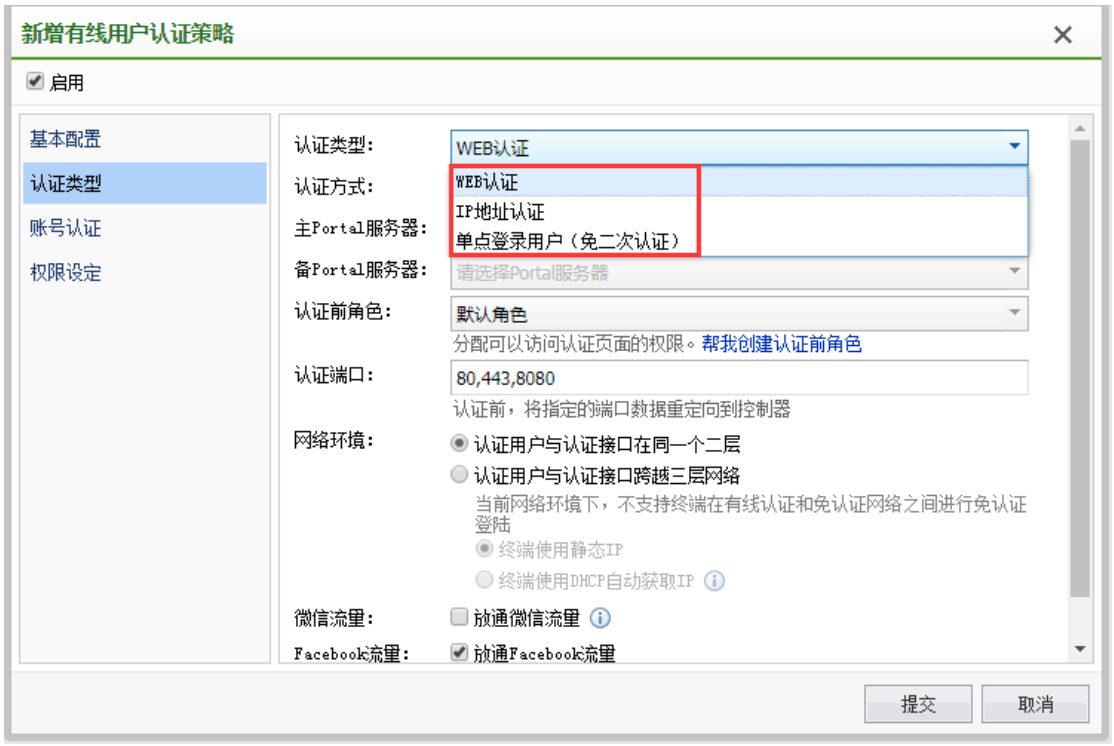
4.6.4.2. 认证策略

认证策略的名称，只在选择数据通过时需要认证的接口。支持物理接口、聚合接口和 VLAN 接口，选择 TRUNK 模式的接口时可指定需要认证的 VLAN。只在选择需要认证的用户范围，支持 IP 地址及 MAC 地址



4.6.4.3. 认证类型

IP 地址认证，web 认证。IP 地址认证，无须认证即可连接到网络。web 认证：web 认证是指终端接入网络后，浏览器访问任意网址，都会被重定向到登录页面，用户在网页上输入用户名、密码等方式通过认证后才能访问网络资源。



Web 认证支持在本控制器上进行 Portal 认证，此时选择【认证授权】-【portal 服务】-【web 认证策略】中添加的认证策略。也支持对接外部 portal 服务器进行 portal 认证。

4.7. 流控与安全

流量管理系统可以对不同用户及应用的网络流量进行管理，划分。提供了带宽保证和带宽限制功能，通过带宽保证功能可以保证重要应用的带宽，带宽限制功能可以做到根据本地用户、服务器认证用户、用户接入方式、用户角色、源 IP、位置、终端类型限制上下行总带宽、各种应用的带宽等。

流量管理系统同时提供流量子通道的功能，可以根据需求建立流量子通道，对通道流量做更为细化的分配。

一级通道是指处在最顶层的一级带宽通道。子通道是指在某个通道下面再创建的带宽通道。子通道用于满足多层次划分带宽的需求。子通道的通道条件从属于上一级通道。

例如：高校，线路带宽 100Mbps，需要把 50Mbps 划分 A 校区，50Mbps 划分给 B 校区，各校区再把带宽划分到各学院。这时候，就需要单独为校区 A，校区 B 创建一个一级带宽通道。然后在校区 A/B 通道下面再创建子通道。

4.7.1. 流量控制通道

流量通道：在网络没有进行流量管理前，线路中所传输的网络流量不分优先级，自由竞争线路的带宽。而流量通道是指在一条线路内，可以人为再细分成多个虚拟的带宽通道，流量管理系统正是基于通道的方式对线路的带宽进行管理。

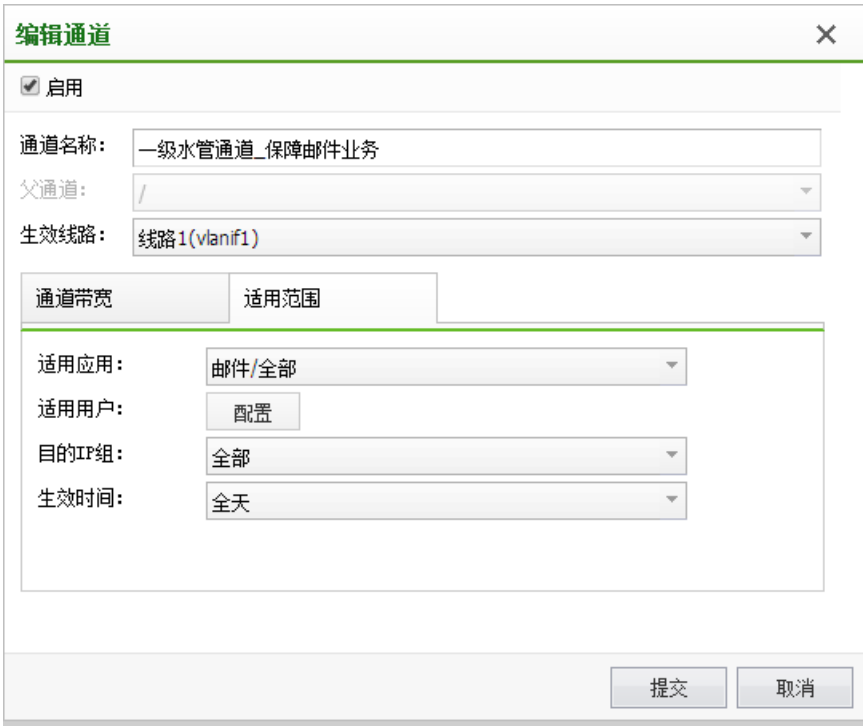
通道可以设定最小保证带宽，最大限制带宽，每 IP 带宽上限，带宽优先级。

通道属性中的优先级，是指带宽分配的优先级，并不是通道匹配的优先级。通道匹配的顺序取决于通道所处的位置，是从上往下逐个通道匹配的。

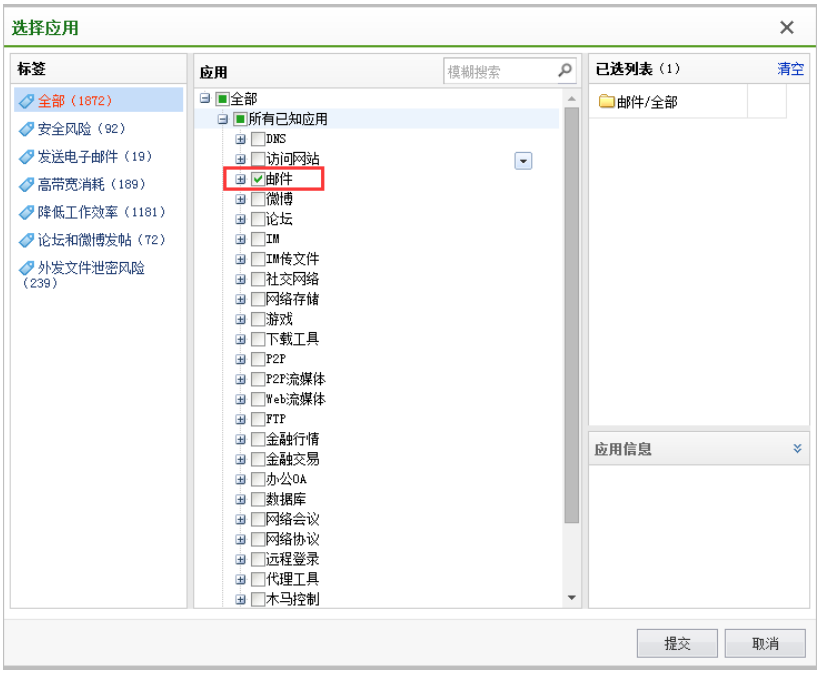
通过流量管理，可以实现的主要功能有：1、动态保证重要网络应用的带宽 2、通道内，不同 IP 间，带宽平均分配 3、限制网络应用的带宽 4、控制每 IP 的最大带宽

4.7.1.1. 通道条件

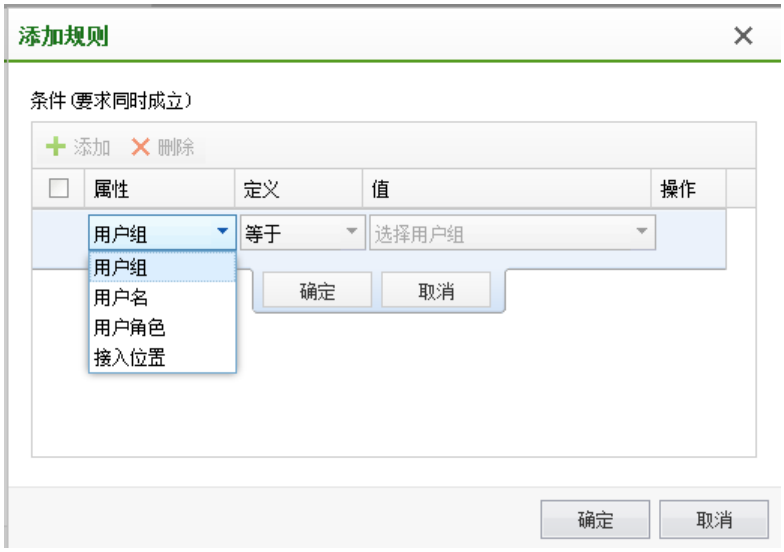
可以依据用户，源 IP/IP 范围，应用，时间，目的地址来设定带宽通道的条件，设备接收到数据包时，会依次从上往下匹配带宽通道，找到第一个匹配的通道，从而为这个数据包找到正确的带宽通道。



选择应用



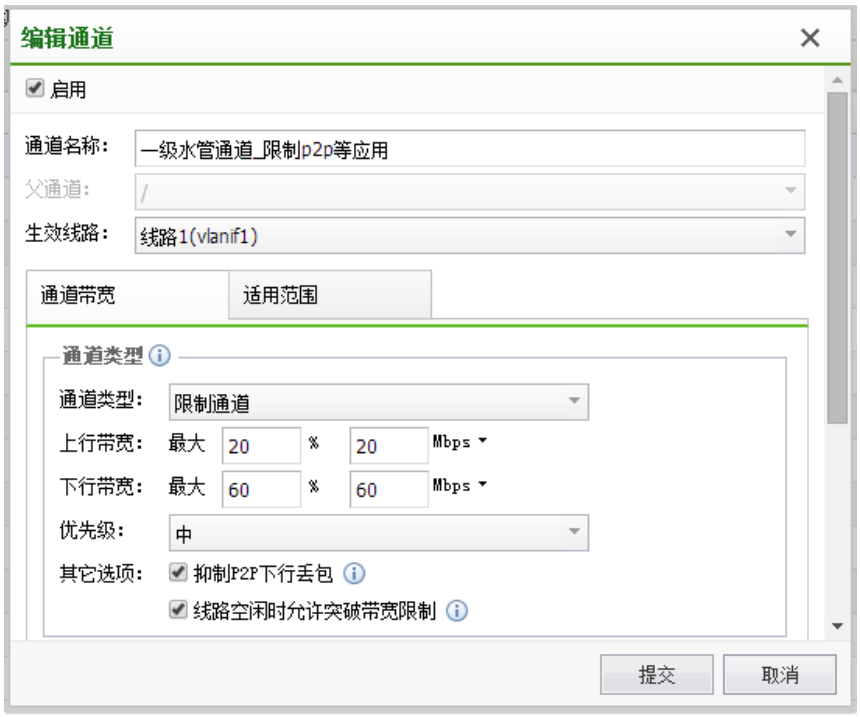
选择通道适用范围，包括用户组、用户、用户角色、接入位置等条件



4.7.1.2. 限制通道

限制通道设定通道的最大带宽，该类型的通道不能设定最小保证带宽（或者说保证带宽数值为 0）。抑制 P2P 下行丢包：有效的增强 p2p 应用的流控，增加流控通道的有效性。限

制通道可以设置，线路空闲时允许突破带宽限制。

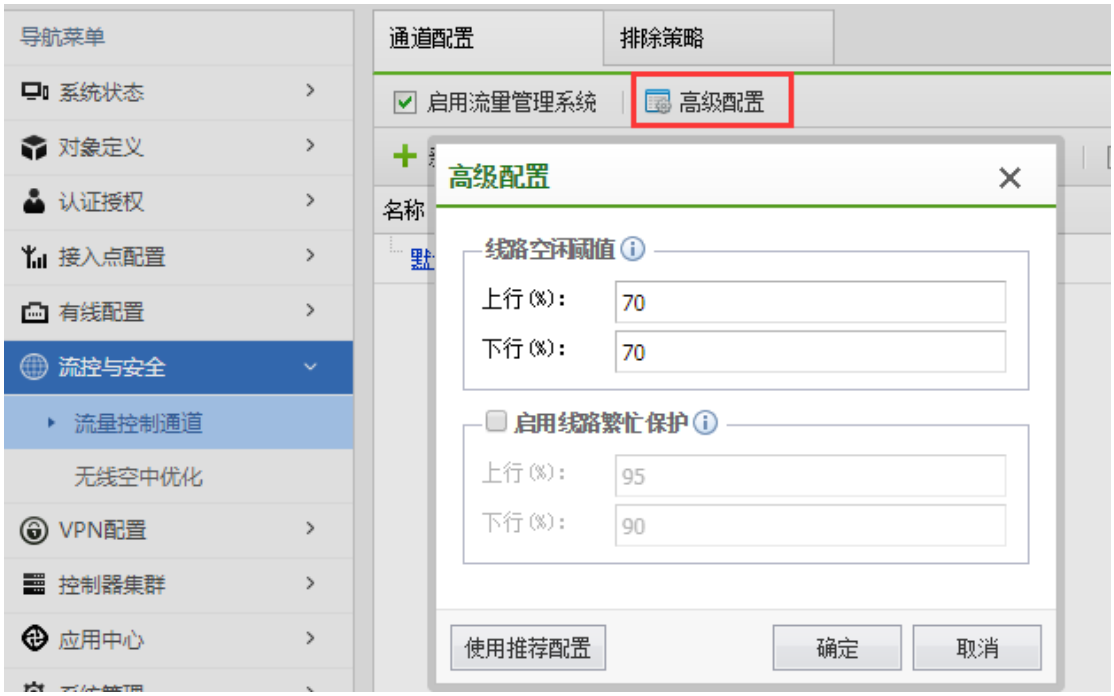


4.7.1.3. 保障通道

保障通道是指可以设定最小保证带宽的通道，用于保证重要的网络应用的带宽。如果某个时刻所生效的通道中，所配置的保证带宽总和已经超过线路的带宽，则会按比例压缩，使得保证带宽总和不会超过线路设定带宽。保证通道也可以设定最大限制带宽。通过“系统状态->流控状态”页面可以查看到当前生效的通道的实际保证带宽，以及通道的实时速率等信息。

4.7.1.4. 高级配置

线路空闲阀值：带宽值低于此值，视为线路空闲，此时限制通道才支持突破带宽限制。线路繁忙保护：不让带宽值跑满，否则一些对带宽敏感的应用很容易丢包，比如视频流量



4.7.1.5. 复制通道到所有线路

由于流控策略是基于线路出口的，如果有多条线路出口，必要时可以在所有线路按照相同流控策略复制到所有线路。

4.7.2. 无线空中优化

4.7.2.1. 射频提速

射频提速功能可以减少无用的广播包转发至无线终端，增加无线的传输的稳定性，并有效的提高无线终端的数据传输效率。包含广播优化，电子书包优化功能。

启用用户间平均分配带宽：同一无线接入点上同一频段的所有无线终端用户之间带宽分配权重相同，当无线接入点传输带宽不足时，每个终端占用的无线时间保持基本一致；带宽足够时，用户带宽将不受此限制。

ARP 转单播：从有线测到无线终端的 ARP 广播包，在 NAC 和 AP 有记录的 ARP 对应表会转为单播，而不再采用广播数据，提高数据的传送效率

禁止 DHCP 请求发往无线终端：对于无线测的终端，默认是以上网类的 PC、平板、智能手机等终端，默认不包括 DHCP 服务器的，所以启用该功能可以有效抑制 DHCP 请求包发往无线终端测，提高传输效率。

禁止 ipv6 报文发往无线终端：目前绝大多数情况不使用 ipv6 协议，开启此开关可以减少空中的 ipv6 报文，优化无线网络环境。

禁止 mdns 发往无线终端：mdns 报文用于在没有传统 dns 服务器的情况下广播发现局域网内的主机。目前苹果系统的产品支持较多，如果要使用类似 Bonjour 这样的软件，请在

使用的 vlan 不开启禁止功能。

禁止 nbns 发往无线终端：windows 系统的名称解析协议的数据包，在局域网内一般会大量存在，严重时会影响用户的上网数据传输。

电子书包多播优化功能：对于默认的 802.11 协议中，对于广播数据是有一定速率限制的，为了适应新环境下的网络需求，有效且合理的提升了广播包的发送速率，增加了无线终端发送速率。

4.8. VPN 配置

NAC 集成了 SangforVPN，标准 IpsecVPN，接入点 VPN 三种 VPN。

『VPN 配置』包含了【DLAN 运行状态】、【基本配置】、【用户管理】、【连接管理】、【第三方对接】、【接入点 VPN】、【高级设置】。

4.8.1. DLAN 运行状态

此页面可以查看当前的 VPN 连接和网络流量信息。页面如下

点击开启可开启 VPN 服务。

点击停止可暂时停止 VPN 服务。

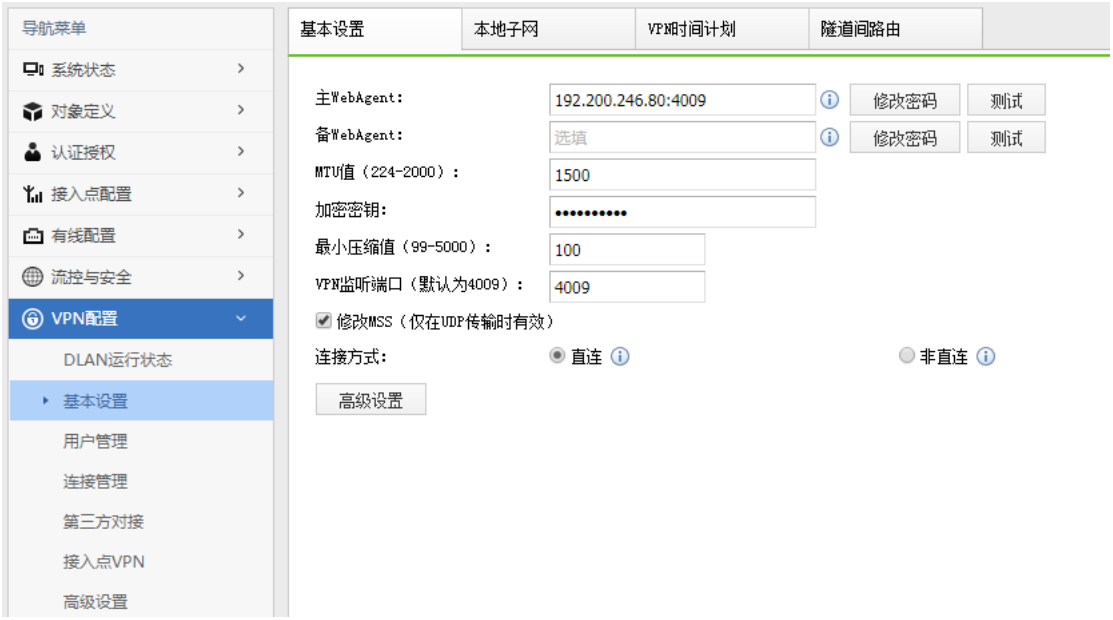
点击刷新，则显示实时的 vpn 连接信息以及流量信息。

在【输入用户名】输入框中输入用户名，可以快速找到当前用户的连接情况。可以进行模糊搜索。

注意：需要开启 VPN 服务，VPN 配置才会生效。

4.8.2. 基本设置

【基本设置】用于配置 Sangfor VPN 的服务端。页面如下



主、备 WebAgent：指动态 IP 寻址文件在 WEB 服务器中的地址，包括主 WebAgent 和备份 WebAgent 地址。

如果是“动态寻址（总部非固定 IP）”请填写“WebAgnet 网页地址”（一般为.php 结尾的网页地址），填写完 Webagent 后可以点击测试按钮查看是否能够连通，如果总部是“固定 IP”，请按照“IP 地址:端口”的格式填写，如 202.96.134.133:4009。点击修改密码可以设置 Webagent 密码，以防止非法用户盗用 Webagent 更新虚假 IP 地址，只对网页地址有效。点击加密密钥可以设置共享密钥，防止非法设备接入。

注意：如果设置了『WebAgent 密码』，一旦遗失该密码则无法恢复，只能联系深信服科技客户服务中心重新生成一个不包含 Webagent 密码的文件并替换原有文件。如果设置了『共享密钥』，则所有 VPN 网点都必须设置相同的『共享密钥』才能相互连接通信。如果是多线路且都是固定 IP 的情况下，可以采用“IP1#IP2:port”的方式来填写 Webagent。

『MTU 值』：用于设置 VPN 数据的最大 MTU 值，默认为 1500。

『最小压缩值』：用于设置对 VPN 数据启用压缩的最小数据包大小，默认为 99。

『VPN 监听端口』：用于设置 VPN 服务的监听端口，缺省为 4009，可根据需要设置。

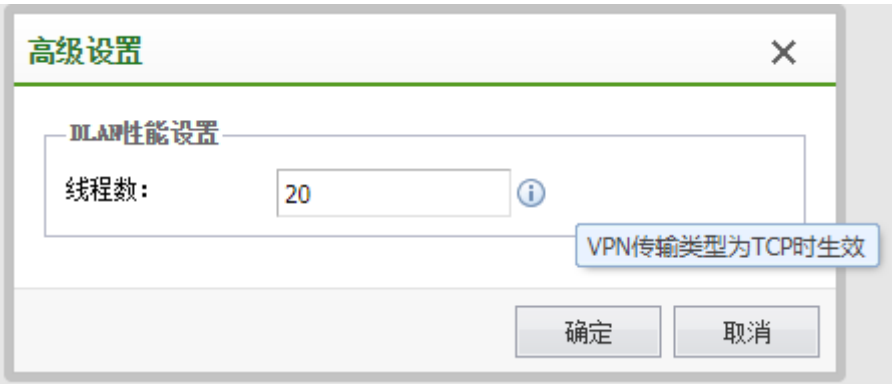
『修改 MSS』：用于设置 UDP 传输模式下 VPN 数据的最大分片。

注：『MTU 值』、『最小压缩值』、『修改 MSS』一般情况下请保留默认值，如需设置，请在深信服技术支持工程师的指导下修改。

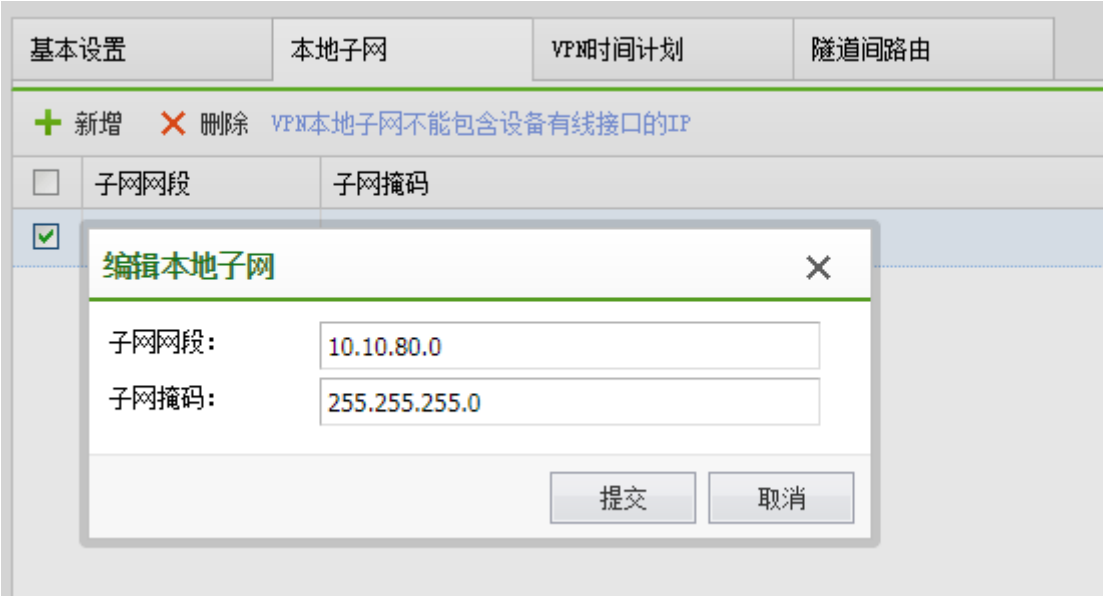
『直连』、『非直连』：用于设置网关与 Internet 的连接方式，如果能直接获得 Internet

IP 或者能通过端口映射等方式让 Internet 用户可以访问到网关设备的 VPN 端口，则可设置为“直连”，不能获得 Internet IP 的连接方式则需设置为“非直连”。

点击高级设置可以进行 VPN 性能设置，线程数设置，如下图所示：



本地子网：配置走 Sangfor VPN 的网段，此网段会同步给其他建立 sangfor VPN 连接的设备。



VPN 时间计划：配置 VPN 独立的时间计划。

隧道建路由：通过配置源网络号和源子网掩码，以及目的网络号和目的子网掩码以及建立 VPN 连接的目的路由用户，实现隧道间路由的目的。

为实现隧道间路由，需完成以下两个步骤：

1、在 VPN 客户端的基本设置->本地子网处，创建本地子网的相关配置（子网网段与子网掩码）；

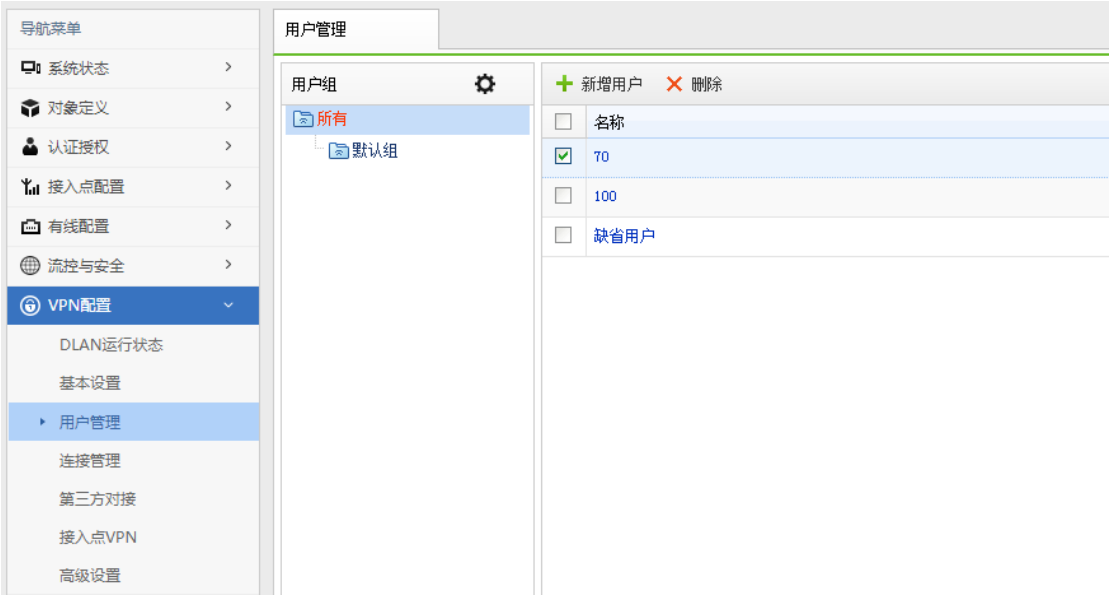
2、在 VPN 客户端的基本设置->隧道间路由处，新增隧道间路由配置。源网络号与子网掩码与本地子网配置一致。目的网络号和目的子网掩码的配置则随着用户的需要有所不同：

（1）设置成 VPN 服务端的本地子网配置，则允许访问 VPN 服务端内网资源；

（2）勾选“启用”通过目的路由用户上网，则目的网络号和目的子网掩码都自动填充为 0.0.0.0 和 0.0.0.0 代表所有流量均通过隧道间路由进行访问。

4.8.3. 用户管理

『用户管理』用于管理 VPN 接入账号信息，设置允许接入 VPN 的用户名、初始密码，设置账号使用的加密算法、账号有效时间。页面如下：



『新增用户』：可依次设置接入账号的『用户名』、『初始密码』、『确认密码』、『算法』、『描述』、等信息，如下图：

『使用组属性』：用于对用户进行分组，如勾选[使用组属性]，则可激活选择『用户组』设置，选择将该用户加入到某一个用户组并应用这个组的公共属性。

设置『使用组属性』前请先新增用户组。用户加入用户组后，该用户的『加密算法』、『权限设置』、『高级』将无法再单独设置。

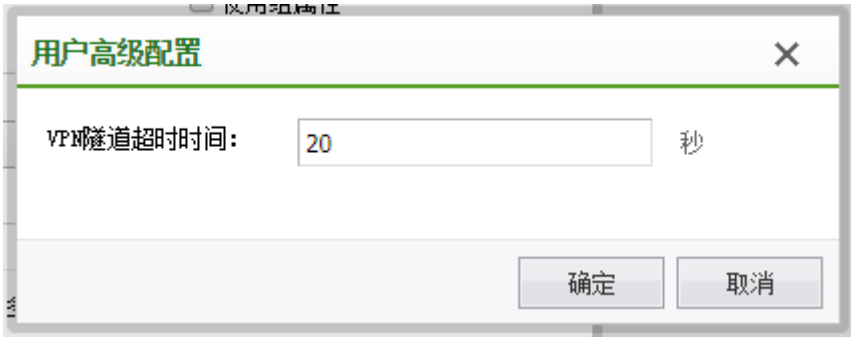
『有效时间』和『启用过期时间』：用于设置“接入账号”的有效时间及过期时间。

『启用压缩』：用于设置对网关设备与该用户之间传输的数据使用压缩算法进行压缩。

该设置是 SANGFOR VPN 的独特技术，在低带宽的环境下能有效利用有限带宽，加速数据传输，但并不适用于所有网络环境，实际应用中可根据情况进行设置。

『启用多用户登录』：用于设置是否允许多个用户同时共用该账号登录 VPN。

点击高级页面，可以设置【VPN 隧道超市时间】，页面如下



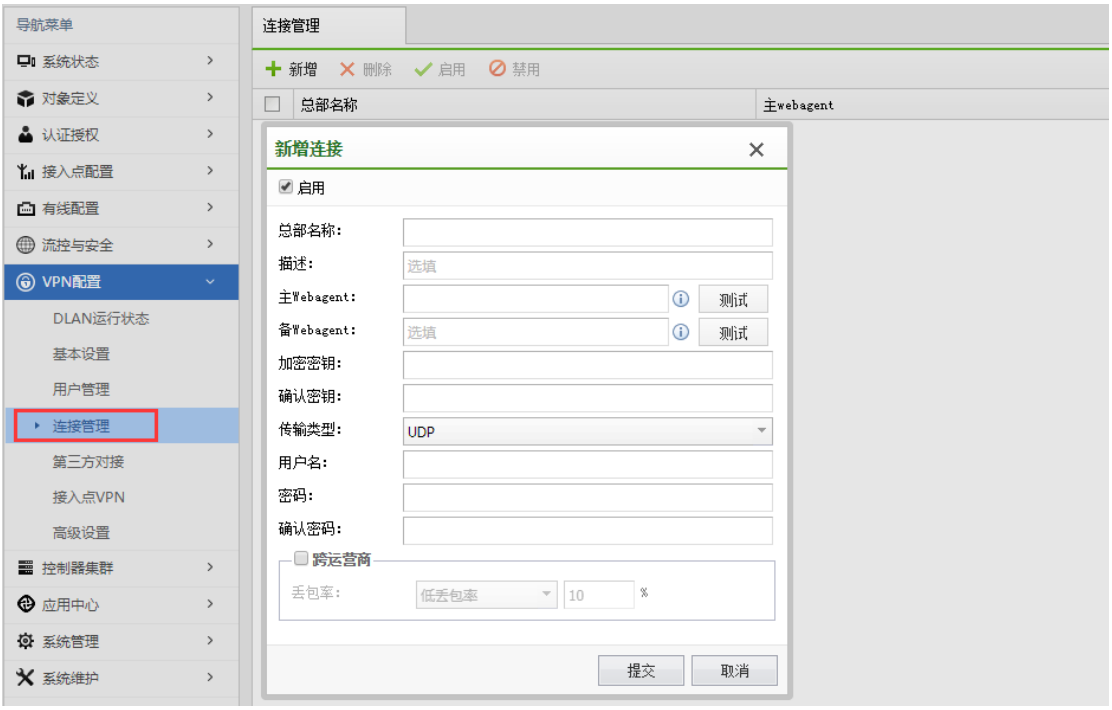
点击删除 确认删除可对勾选的用户进行删除操作。页面如下

4.8.4. 连接管理

为了实现多个网络节点的互联（组成“网状”网络），VPN 硬件网关提供了对网络节点互联的自主管理和设置功能。可在『连接管理』中进行相关的设置。页面如下：

注意：连接管理只有此设备当分支使用需要连接其他 Sangfor VPN 设备时才需要启用，否则本端是 VPN 总部设备的不需要启用连接管理。

『新增』：可以添加到一个到其他 VPN 总部的连接。页面如下：



总部名称：用于标记连接名称，可以任意填写。

描述：可自行定义描述信息。

主/备份 Webagent：用于填写需要连接的总部的对应 Webagent，点测试按钮可以测试 Webagent 是否工作正常。

传输类型：可选“TCP”或“UDP”，用于决定传输 VPN 数据包的类型，默认为 UDP 模式。

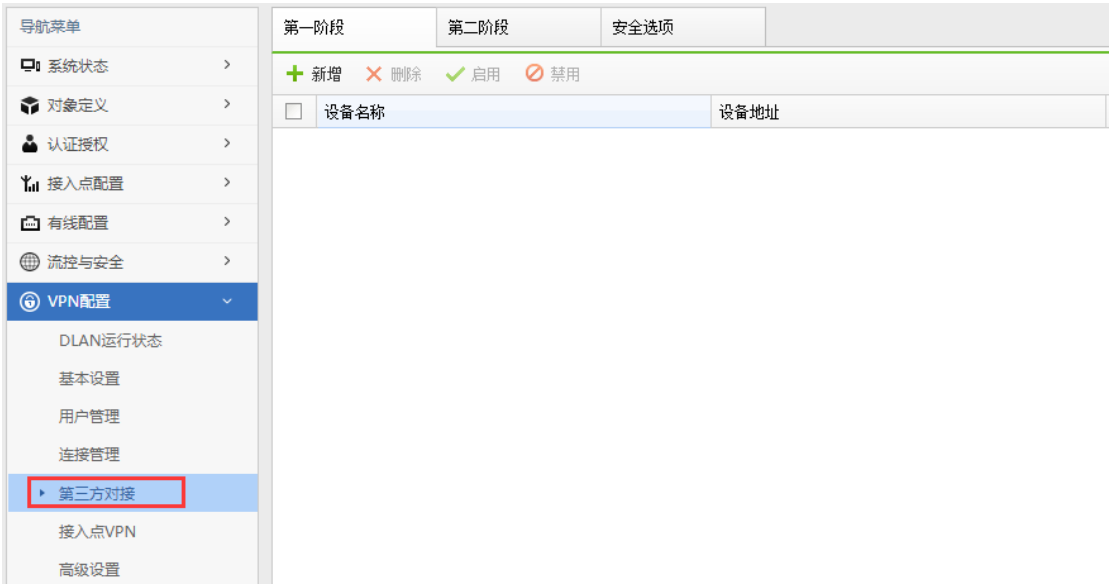
用户名和密码：请根据总部提供的接入账号信息来填写。

跨运营商：适用于总部分支采用了不同运营商线路互联且经常丢包的情况下。可以选择“低丢包率”、“高丢包率”和“手动设置”。

注意：跨运营商功能需要额外激活，否则该功能无效。只要总部激活跨运营商功能，则所有连接到该总部的移动用户均可启用跨运营商功能。如果是设备和设备之间互连，则需要双方都开启跨运营商序列号，否则该功能无效。

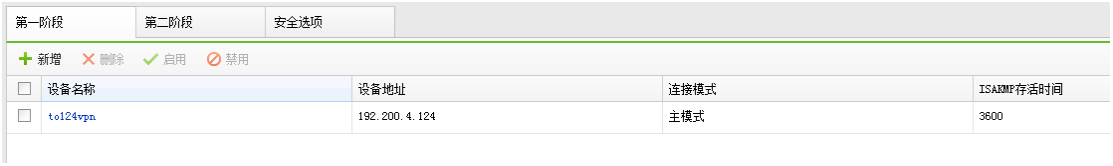
4.8.5. 第三方对接

SUNDRAY IPSEC VPN 系列硬件设备提供了与第三方 IPSEC VPN 设备互联的功能，能与第三方的 IPSEC VPN 设备建立标准 IPSec VPN 连接。

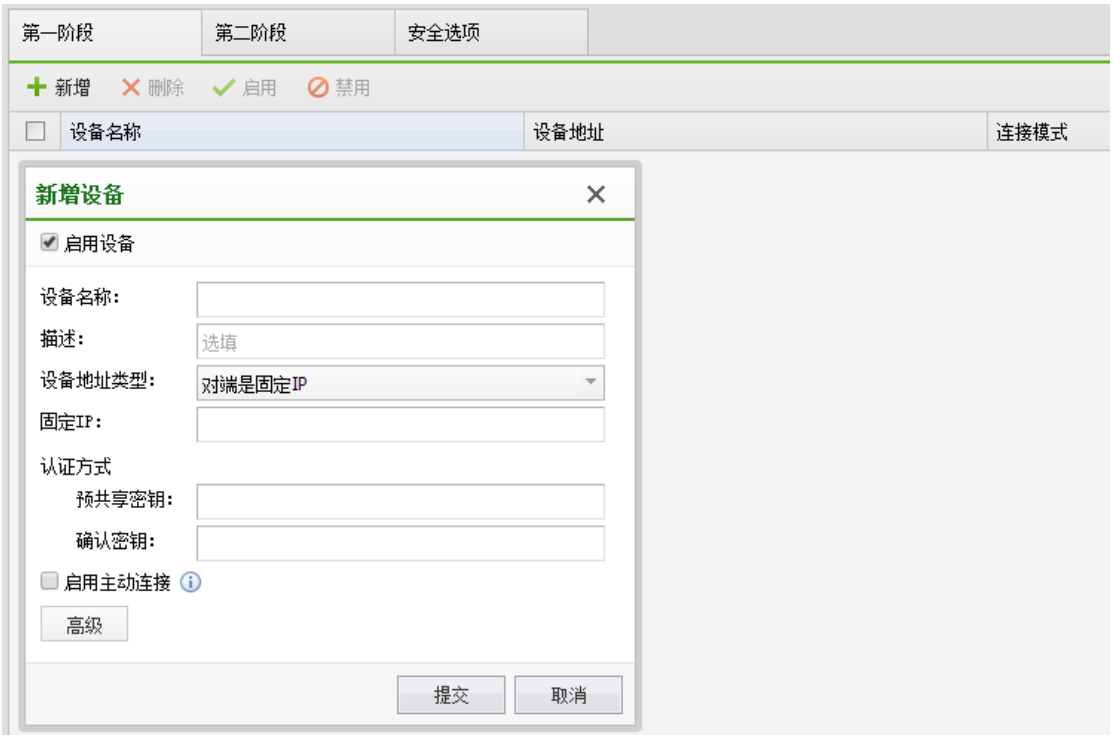


『第一阶段』用于设置需要与 SUNDRAY IPSEC VPN 硬件网关建立标准 IPSec 连

接的对端 IPSEC VPN 设备的相关信息，也就是标准 IPSec 协议协商的第一阶段。页面如下：



点击新增，页面如下：



设备名称：可自行定义。

描述：可自行定义。

设备地址类型：包括对端是固定 IP、对端是动态 IP、对端是固定域名三种。请根据实际情况选择。选择固定 IP，就填写上对端的 IP 地址；选择动态域名，就填写上对端外网绑定的域名。

注意：标准 IPSEC 不允许连接的双方都是动态 IP，只能允许其中一方为动态 IP。

预共享密钥及确认密钥：填入正确的预共享密钥，并确保连接双方采用的都是相同的预共享密钥。

点击高级，显示【高级选项】对话框，可进行其它高级设置，如下图：

ISAKMP 存活时间：标准 IPSEC 协商的第一阶段存活时间，只支持按秒计时方式。

重试次数：当 VPN 故障断开后，重试连接的次数，超过次数还未能连上，则不再主动发起连接，除非有 VPN 流量触发才能再次主动发起连接。

协商模式：包括主模式和野蛮模式两种类型。主模式适用于双方均为固定 IP 或者一方固定 IP 一方动态域名方式，并且不支持 NAT 穿透；野蛮模式适用于其中一方为拨号的情况，并且支持 NAT 穿透。

DH 群：设置 Diffie-Hellman 密钥交换的群类型，包括 1、2、5 三种，请与对端设备配置保持一致。

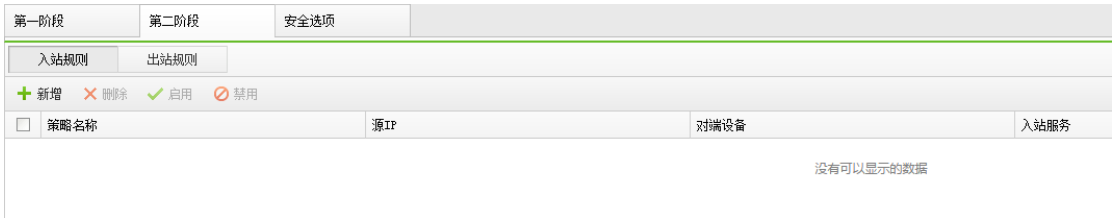
认证算法：选择数据认证的 Hash 算法，包括 MD5。

加密算法：选择数据加密的算法，包括 DES、3DES、AES。

野蛮模式的身份 ID 有 3 种表达方式，一种为 IP 地址；一种为域名字符串（FQDN）格式，可以为任意的网址或者一串字符串；另一种为用户字符串（USER_FQDN），需要是“xxx@xxx.xxx”这种格式。

第二阶段：

『入站策略』用于设置由对端发到本端的数据包规则，策略较多时自动分页显示。可以在右上角搜索策略名称、源 IP、对端设备名称等；其中对于源 IP 是“子网+掩码”的策略，仅搜索的是子网，不搜索掩码。



策略名称及描述：可自行定义。

源 IP 类型：包括单个 IP、子网+掩码两种类型。分别指定对端 VPN 数据的源 IP 是单个 IP 还是整个网段，并正确填入对端 VPN 数据的源地址。

对端设备：该出站策略跟对端哪个设备相关联。

入站服务：定义对端哪些类型的服务允许进入 VPN 隧道传输至本端内网。

有效时间及过期时间：在什么时间范围内，该入站策略有效。其中『有效时间』可选『生效时间内允许』，『生效时间内拒绝』。

出站策略：用于设置从本端发往对端的数据包规则，点击新增，显示【策略设置】对话框，页面如下：

策略名称及描述：可自行定义。

源 IP 类型：包括单个 IP、子网+掩码两种类型。分别指定 VPN 数据的源 IP 是单个 IP 还是整个网段，并正确填入 VPN 数据的源地址。

对端设备：该出站策略跟对端哪个设备相关联。

安全选项：该出站策略跟哪个安全选项相关联。

SA 生存时间：标准 IPSEC 第二阶段协商的存活时间，同样只支持按秒计时。

出站服务：定义哪些类型的服务允许进入 VPN 隧道传输至对端内网。

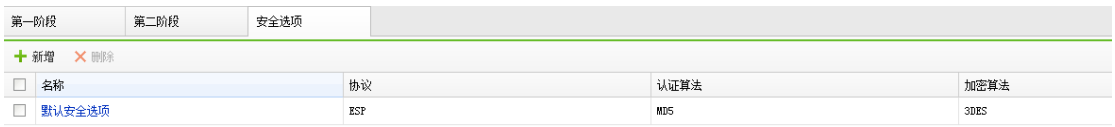
有效时间及过期时间：在什么时间范围内，该出站策略有效。其中『有效时间』可选『生效时间内允许』，『生效时间内拒绝』。

注意：『有效时间』模块，只在连接双方都是 SUNDRAY 设备情况下生效，与其他厂商设备互联时无效。

启用密钥完美向前保护：根据对端设备情况而定，如果对端启用了 PFS，则本端也需要勾上此选项，否则不用勾选。

注意：『出站规则』和『入站规则』中的『出站服务』、『入站服务』和『有效时间』均为 SUNDRAY 扩展的规则，此类规则仅在本端设备生效，在与第三方设备建立 VPN 连接的过程中不会协商此类规则。『出站策略』和『入站策略』中策略所对应的源 IP 地址是指『源 IP 类型』和『本/对端服务』中所设置的源 IP 的交集。

『安全选项』用于与对端建立标准 IPSec 连接时所使用的参数，页面如下：



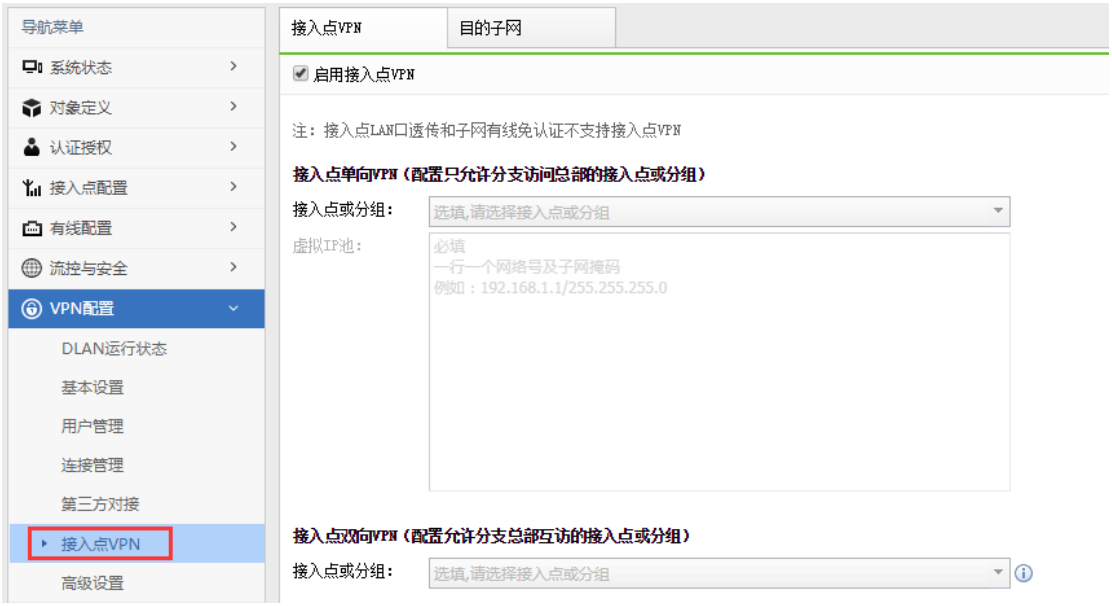
在建立与第三方设备的 IPSec 连接前，请先确定对端设备采用何种连接策略，包括：使用的『协议』（AH 或 ESP）、『认证算法』（MD5 或 SHA-1）、『加密算法』（DES、3DES、AES）。点击新增，添加新的选项，页面如下：

SUNSRAY IPSEC VPN 系列硬件设备会使用设置好的连接策略与对端协商建立 IPSec 连接。

『安全选项』中的『加密算法』用于设置标准 IPSec 连接的第二阶段所使用的数据加密算法，如果要与多个采用不同连接策略的设备互联，需要分别将各个设备使用的连接策略添加到『安全选项』中。

4.8.6. 接入点 VPN

接入点 VPN 主要用于远程部署场景，分部要通过分部的 VPN 访问总部资源、或者总部分部互访。由 AP 和控制器之间建立 VPN 隧道，传输总分部之间的流量。

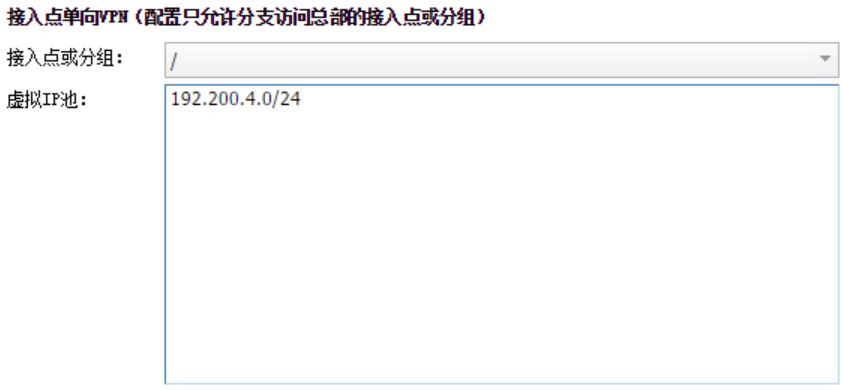


虚拟 IP 池：由接入点 VPN 系列硬件设备指定设备内网中空闲的一段 IP 作为移动用户接入时的虚拟 IP。当移动用户接入后，分配一个虚拟 IP 给移动用户，移动用户对总部的任何操作都是以分配的 IP 作为源 IP、就完全和在总部局域网内一样。例如使用虚拟 IP 的移动接入后，无论总部局域网的计算机是否把网关指向总部接入点 VPN 系列硬件设备，移动用户均可以访问，还可以为接入的移动用户指定 DNS 等网络属性。

创建移动虚拟 IP 池。虚拟 IP 池中的 IP 相当于是直连在总部控制器网关设备的网

段。

在【虚拟 IP 池】对话框，设置“IP 池”的起止 IP 即可。页面如下：



分支网络部分走本地转发，部分走集中转发。

满足分支远程 AP 本地转发下的用户即想访问公网，又想访问总部资源的需求。

分两种场景：

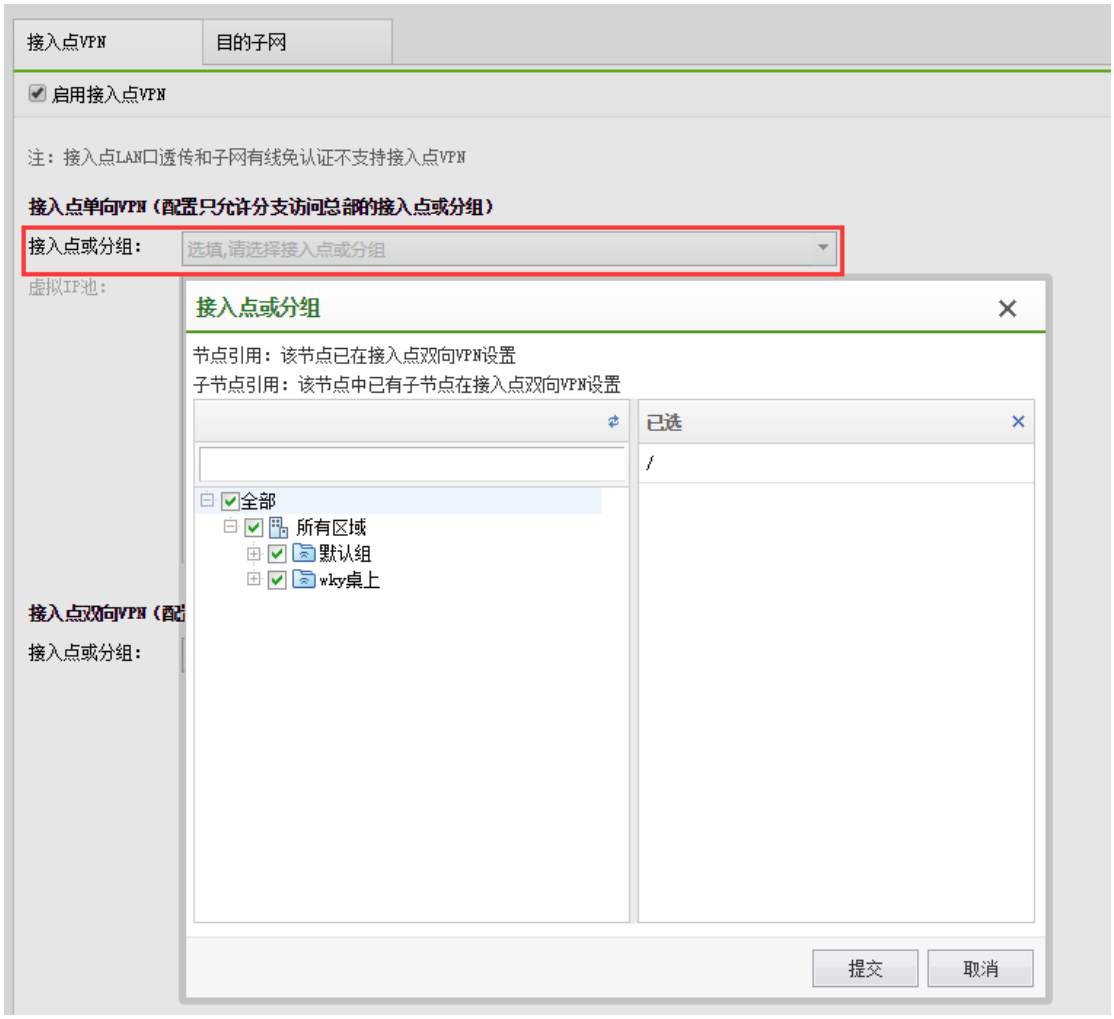
场景 1：只允许分支访问总部。

配置方法：在虚拟 IP 池中设置足够多的虚拟 IP。将总部资源的 IP 填写到目的子网中，即可。

场景 2：允许分支总部互访。

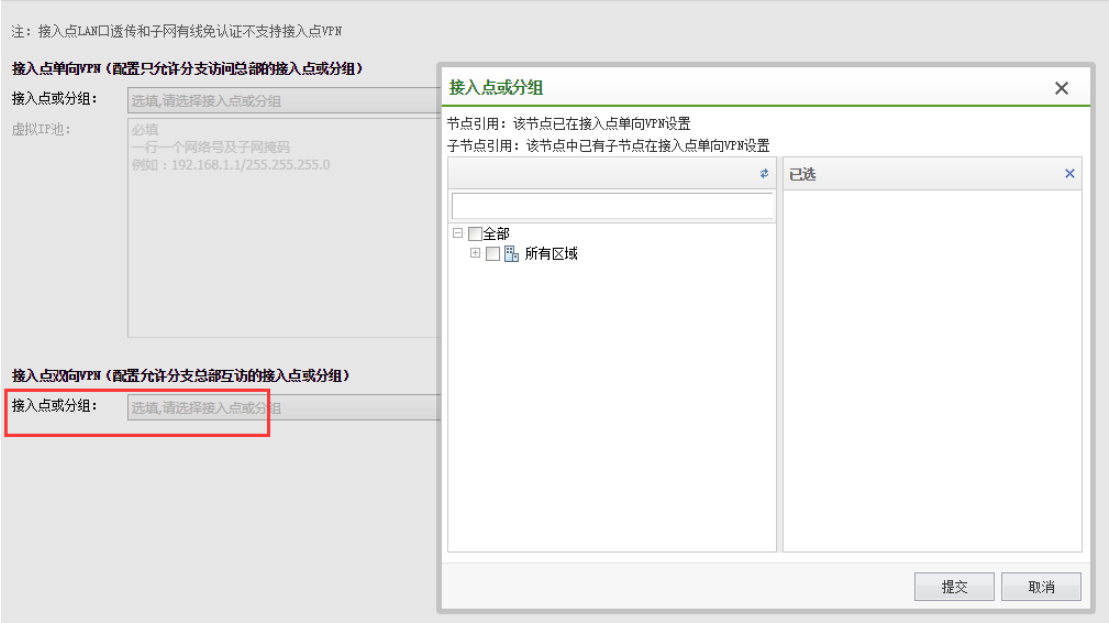
配置方法：需要划分每个 AP 的子网网段，保证子网网段不冲突。将总部资源的 IP 填写到目的子网中。

接入点单向 VPN，只允许分支访问总部：

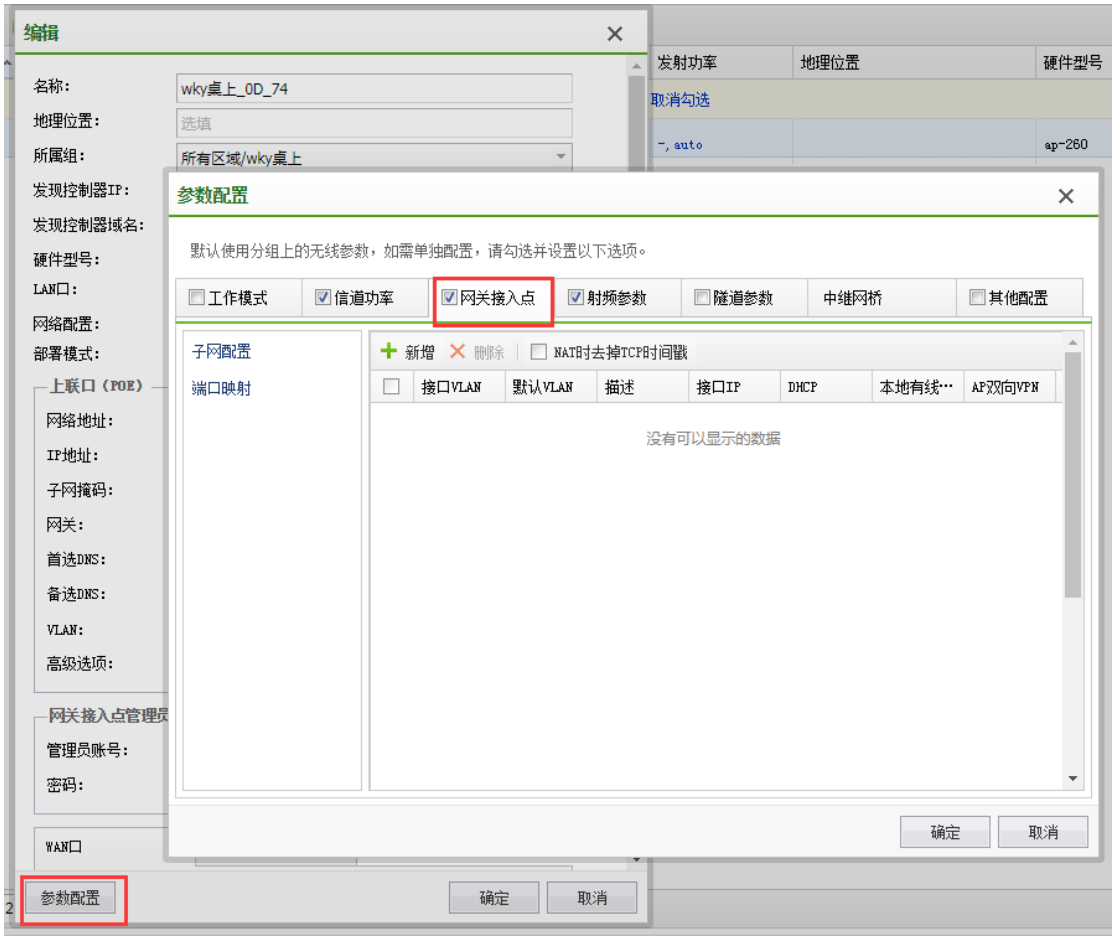


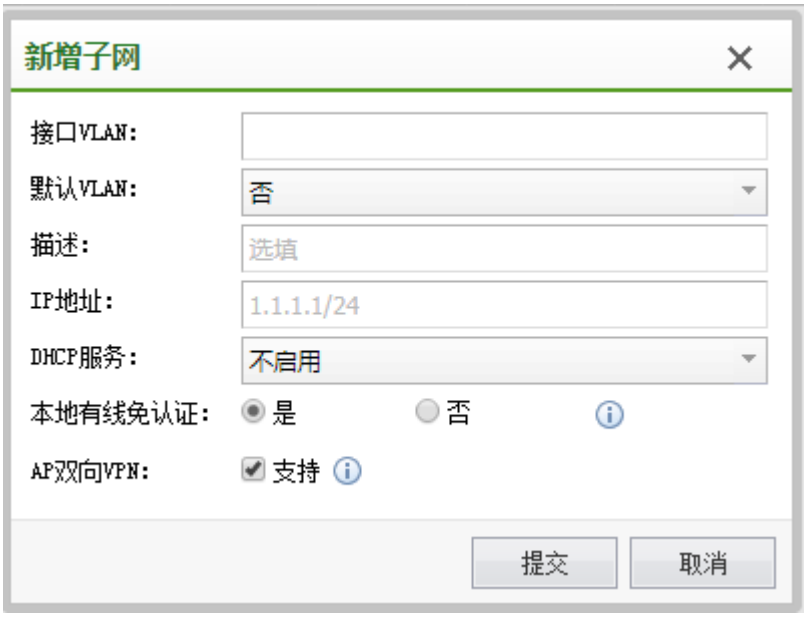
接入点双向 VPN：允许总分部互访。

在接入点双向 VPN（配置允许分支总部互访的接入点或分组）选项下，接入点或分组里选择需要双向互访的 AP 或者 AP 组。



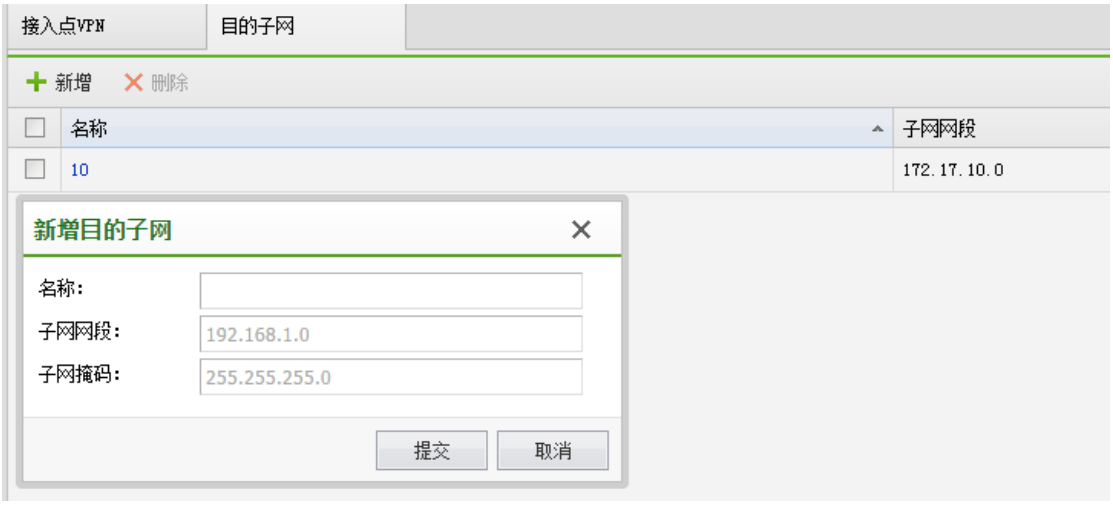
在 AP 端，需要开启【AP 双向 VPN】的支持，具体在【接入点配置】【无线接入点】，点开对应的接入点，AP 选择网关模式，点参数配置，选中【网关接入点】，点添加，勾选【双向 VPN 支持】。



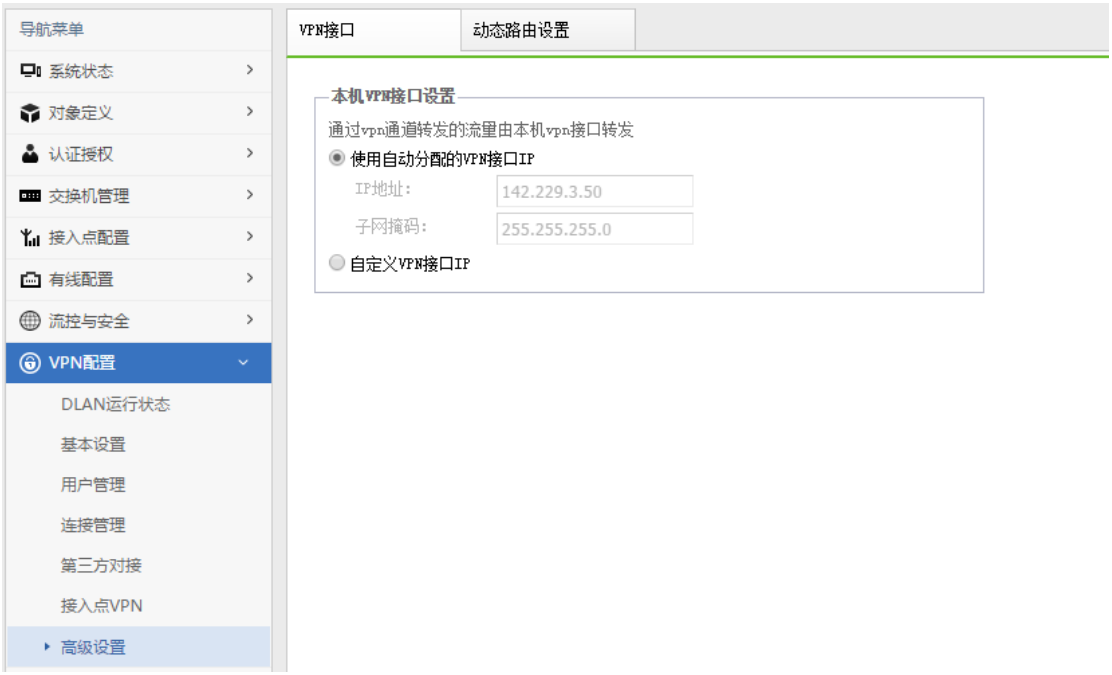


【目的子网】配置分支走集中转发的网段。配置远程 AP 下的用户访问哪些 IP 时走集

中转发。



4.8.7. 高级设置



VPN 接口：

支持自动分配和手动配置，可在此接口上做地址转换。

动态路由设置：

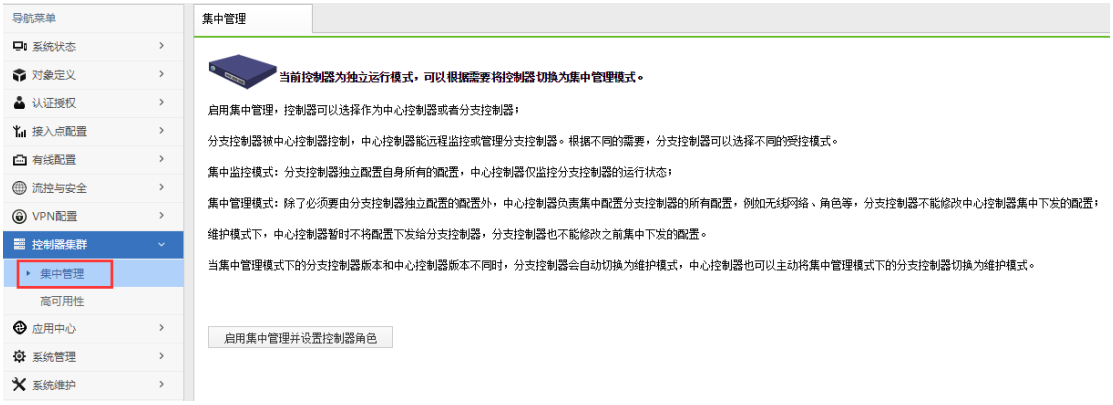
动态将 VPN 的路由表通告给接在控制器内网的路由器。

允许通告接入点 VPN 的 IP 地址：将 AP VPN 目的子网路由下发给内网路由器。

4.9. 控制器集群

4.9.1. 集中管理

集中管理用于多控制器情况下，选一台主控制器，管理别的控制器。集中管理中 NAC 控制器分三种角色：独立控制器，网点控制器，中心端控制器。以下逐一说明。

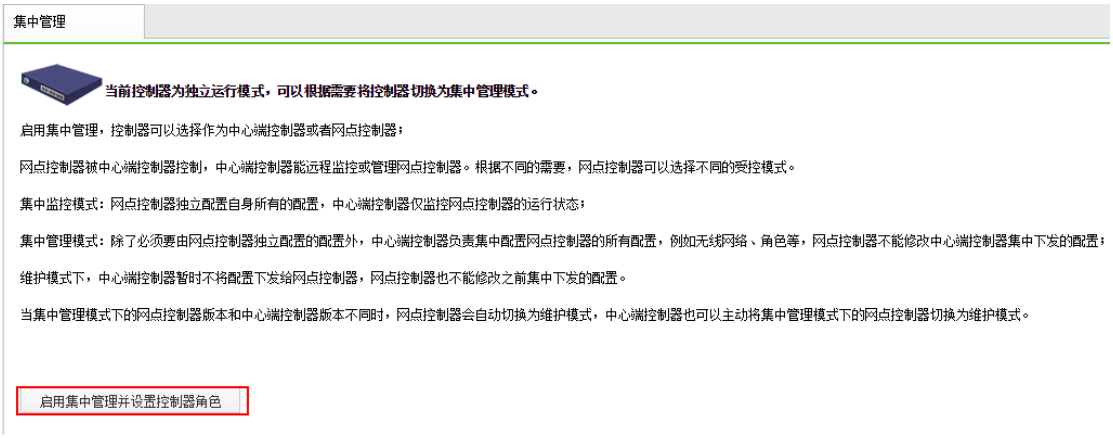


独立控制器：未开启集中管理功能。

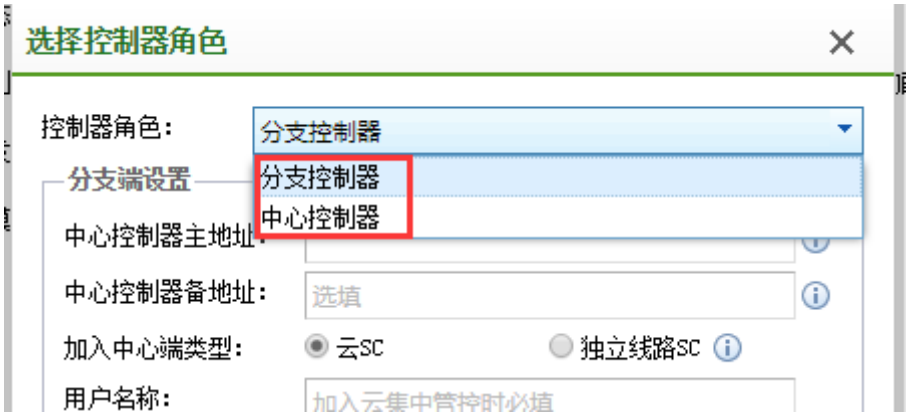
分支控制器：分支分三种状态（管理，监控，维护）。管理状态：需要中心端和网点版本一致，由中心端集中配置下发无线网络等集中管理的配置；监控状态：网点自己管理配置；维护状态：当中心端和网点版本不一致时自动切换，或由中心端管理员主动切换，维护状态下暂时不下发配置，网点也不可以修改集中管理的配置。

中心控制器：增加、删除、编辑网点账号。批量切换网点的状态（管理，监控，维护）。导入导出网点账号。生成网点的解控密码。远程登陆到网点的控制器。

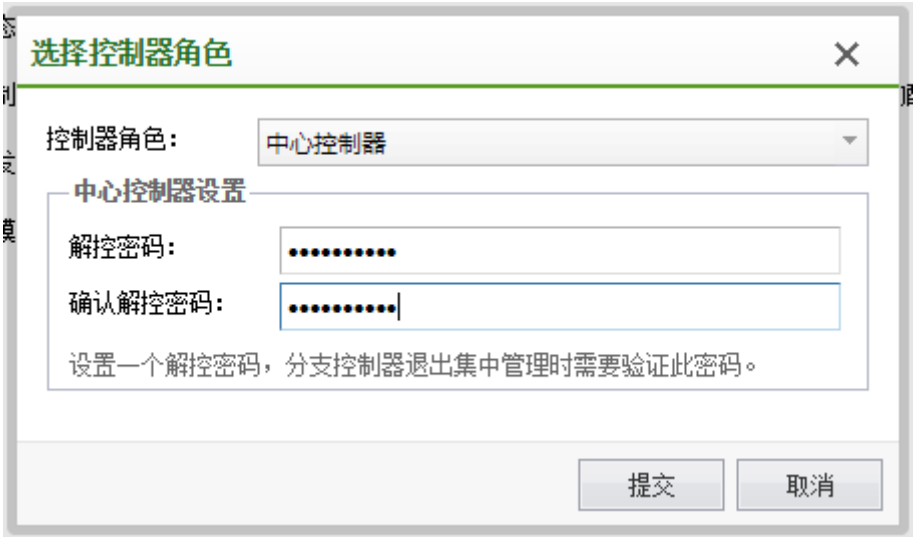
点击启用集中管理并设置控制器角色



可以选择该控制器的角色，如果是主控端，就选择中心控制器，如果是受控端，就选择分支控制器。

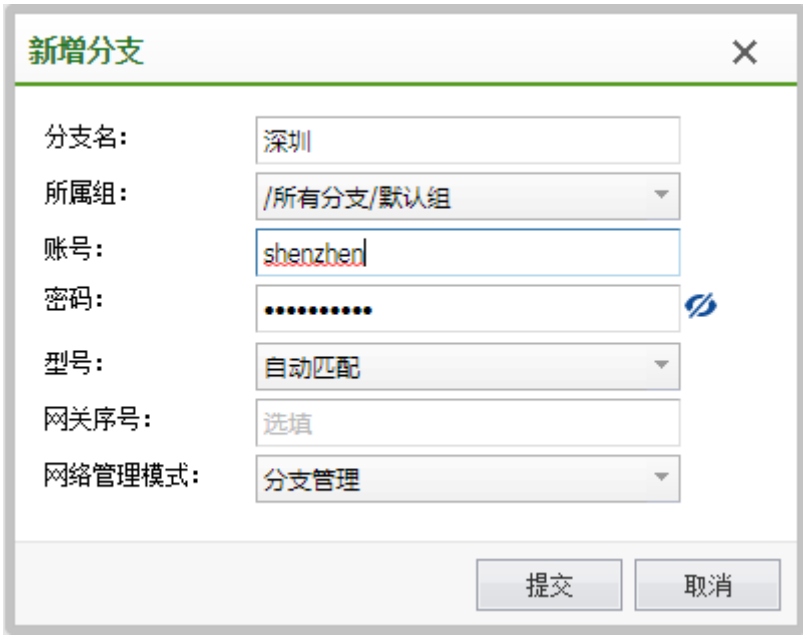


假如是中心端控制器角色，填写解控密码。解控密码用于加入到该中心端的网点控制来退出集中管理。



点确定点提交后，该控制器就配置成了中心控制器角色。

新增分支控制器，分支名标识分支用，可以自定义；所属组可将分支放到某个分组目录里面；帐号密码是用于分支控制器加入中心控制器的时候定义的帐号密码。网络管理模式可以选择分支管理或中心端管理，分支管理下分支可自行管理自己的【接口管理】和【网络配置】，中心端管理下由中心端统一管理分支的【接口管理】和【网络配置】。



在网点控制器，点击启用集中管理并设置控制器角色，开启集中管理功能。控制器角色选择分支控制器。分支端设置：输入中心端主地址和在中心控制器定义好的帐号密码。

管理模式可选监控模式和管理模式。最后点提交即可加入管理。

如果选择管理模式，部分配置将被中心端覆盖，且会删除营销中心的数据请先备份当前配置，请先备份相应数据。

在中心控制器端根据状态，如果是在线，就表示网点控制器已经加入成功。该界面包含了网点、操作、IP 地址、版本号、状态、接口点、在线用户、安全事件、工作模式、主备机、最近更新时间、日志。其中操作可以切换该网点控制器的控制模式。接入点显示了网点控制器上的 AP 状态，分别有未激活，激活，离线三个状态，点击未激活的那项可以激活网点 AP。日志可以看到中心端对网点控制器的操作是否下发等日志。

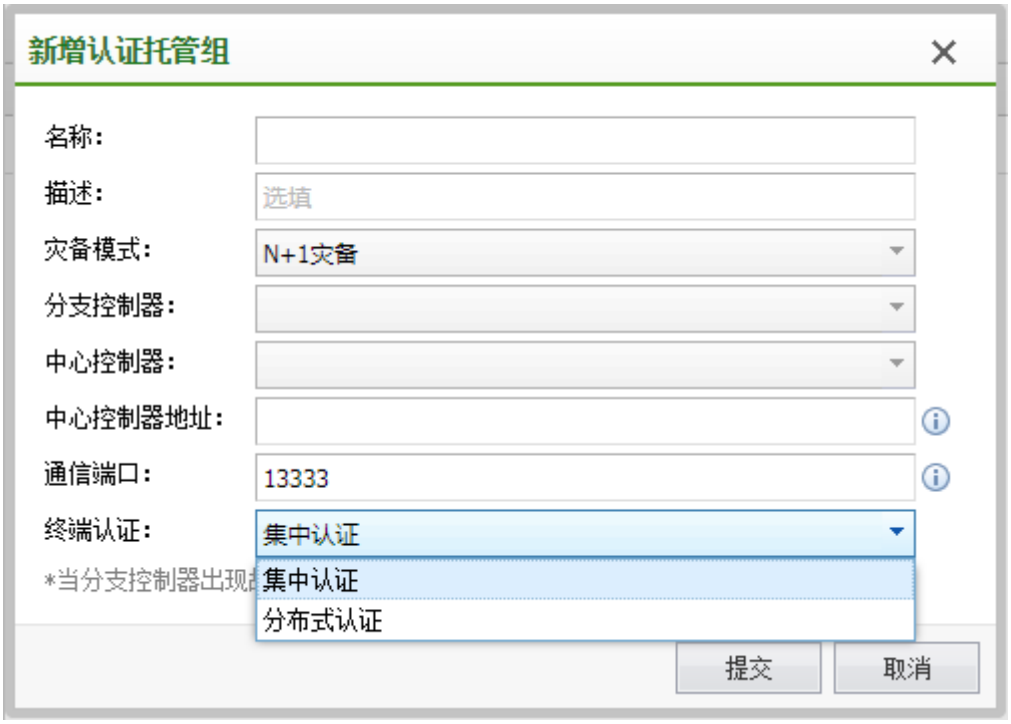
认证托管组分为“1+1 灾备”和“N+1 灾备”。

“1+1 灾备”下两台分支控制器互为灾备，当任意一台控制器宕机后，由另一台控制器接管 AP。类似于异地双机，两台控制器会同步配置，会将控制器 1 的配置覆盖到控制器 2。在此模式下，两台控制器会同步配置及认证信息。故当 AP 被另一台控制器接管后，终端用户无需重新认证。信息同步使用 TCP13333 端口，需要保证两台控制器通信 IP 可以互相通信。

“N+1 灾备”下指定 1 为中心控制器，N 为分支端，即当分支设备宕机后，由中心端接管 AP（即类似之前版本的集中管理）可以手动指定一台网点控制器为集中认证的中心控制器，N 为分支控制器。分为集中认证与分布式认证。

集中认证：所有用户在指定的中心控制器上统一认证。

分布式认证：用户在各自接入的分支控制器认证，不能实现跨 NAC 免认证漫游。



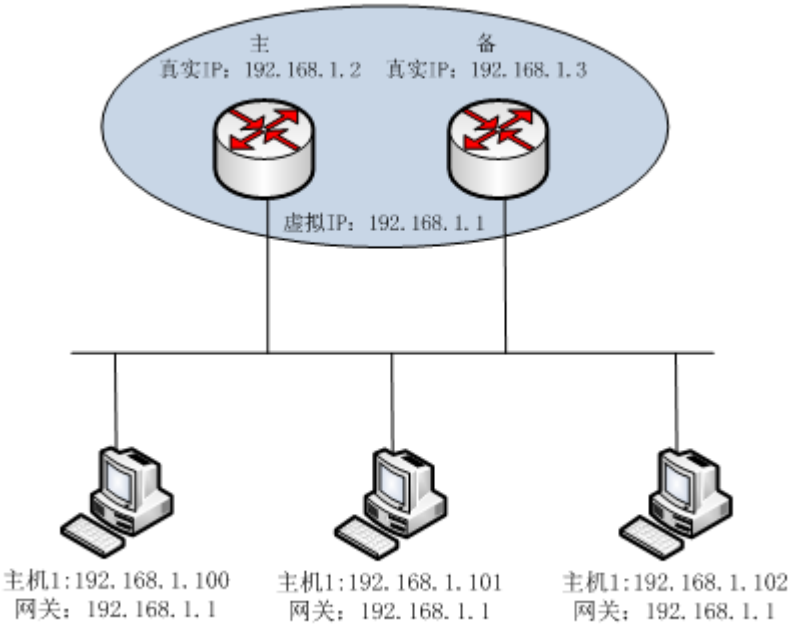
4.9.2. 高可用性

无线网络部署为集中转发模式时，所有无线用户的流量都将经过控制器集中转发，因此存在单点故障导致网络中断的风险。通过部署 2 台控制器，可以实现无线控制器间的负载均衡，以及网络的高可用性，避免单台无线控制器故障时导致无线网络不可用的风险。

4.9.2.1. VRRP 组

VRRP（Virtual Router Redundancy Protocol）协议，提供了虚拟 IP 的机制来解决网关 IP 在多个路由器间迁移的问题。在 3 层部署的环境中，无线客户端的默认网关指向无线控制器的 VLAN 接口地址，因此在双机部署中，当某台设备故障时，VLAN 接口的 IP 地址需要使用 VRRP 协议迁移到备份设备上，从而保证无线用户仍然能够正常访问网络。

VRRP 的虚拟 IP 迁移通过备份组机制实现，基本原理如下：

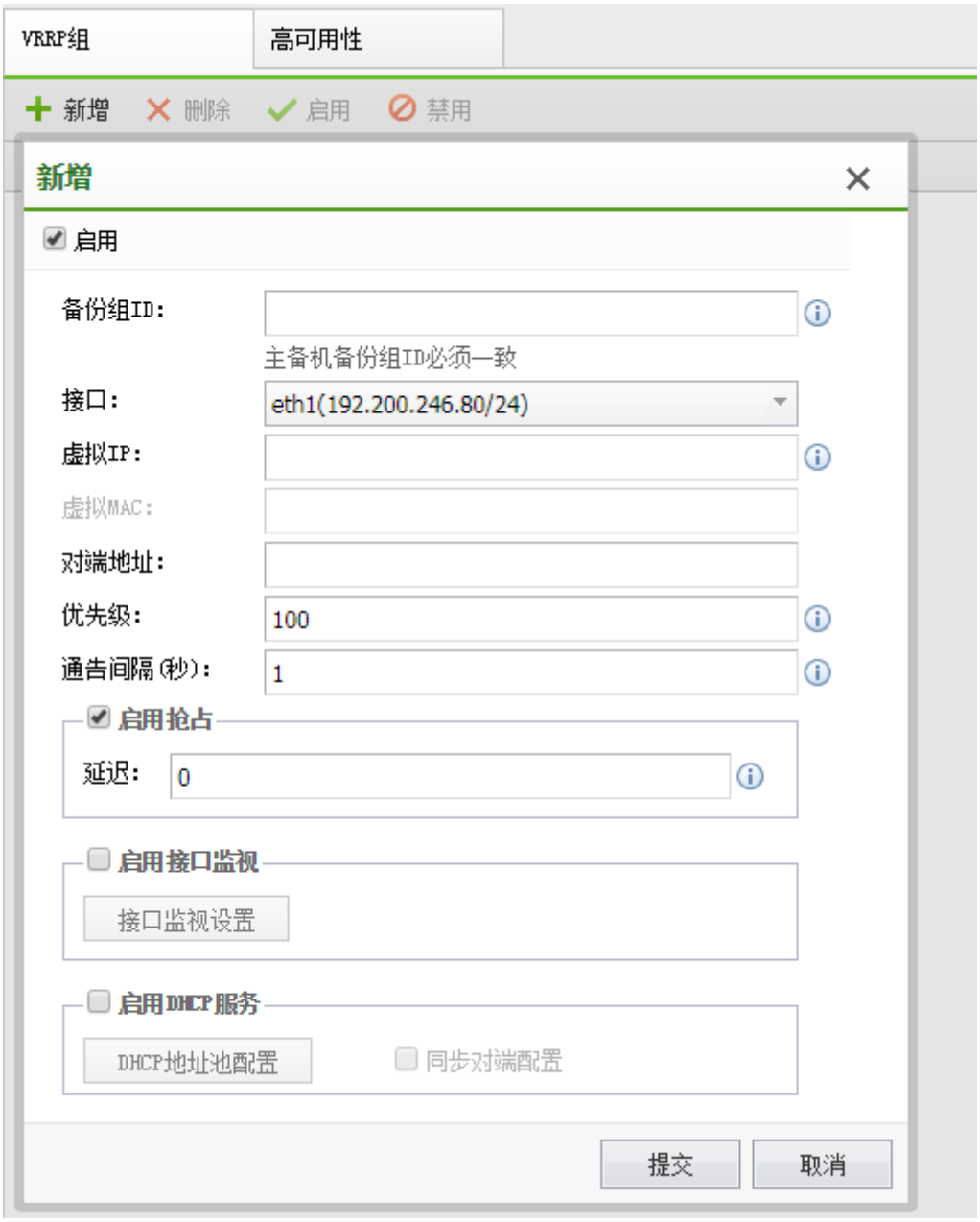


把两个路由器划分为一个 VRRP 备份组，备份组设置一个虚拟 IP。

备份组内的路由器，使用基于优先级的选举机制，优先级较高的为 Master 路由器，其余为 Backup 路由器。

只有 Master 路由器，才真正持有备份组的虚拟 IP，也就是对于其它主机询问此虚拟 IP 的 ARP 请求，PING 请求等，只有 Master 路由器会回应。

Master 路由器定期发送 VRRP 通告报文，通知备份组内的其他路由器自己工作正常。Backup 路由器则监听通告报文的到来，如果在一定时间内没有收到 Master 路由器的通告报文，则优先级最高的 Backup 路由器将转化为 Master 路由器。


VRRP组
高可用性
新增
删除
启用
禁用
新增
启用
备份组ID:
主备机备份组ID必须一致
接口:
eth1(192.200.246.80/24)
虚拟IP:
虚拟MAC:
对端地址:
优先级:
100
通告间隔(秒):
1
启用抢占
延迟:
0
启用接口监视
接口监视设置
启用DHCP服务
DHCP地址池配置
同步对端配置
提交
取消

4.9.2.2. 高可用性

1、通信网口

双机热备情况下，两台无线控制器之间，需要同步内部状态信息，例如心跳信号，在线用户信息，漫游信息，无线射频调整决策信息等。因此在控制器上，通常需要分别使用一个专用的网口来完成双机状态同步。此选项选择用于状态同步的物理接口。

2、对端地址

对端控制器的 IP 地址，系统使用所选择的物理接口及对端地址来完成双机状态同步。因此对端地址是指双机心跳线所连接的对端接口 IP 地址。

3、管理 VRRP

选择一个 VRRP 备份组作为管理 VRRP 组，在此备份组中，Master 状态的设备将作为“主管理设备”。只有登录到“主管理设备”，才允许修改系统配置。

4、主备配置

主机选择允许编辑配置，备机选择同步对端配置，双机热备才会搭建成功。

4.10. 应用中心

『应用中心』包含【序列号】、【服务配置】、【信锐云】三个功能模块。

4.10.1. 序列号

使用无线控制器前，必须向设备供应商购买有效的产品或功能序列号。NAC 的版本序列号包括设备序列号和软件升级序列号，设备序列号决定了一个 NAC 最多可以管理 AP 的个数。软件升级序列有效，NAC 才可以正常升级软件版本，配置界面如下：

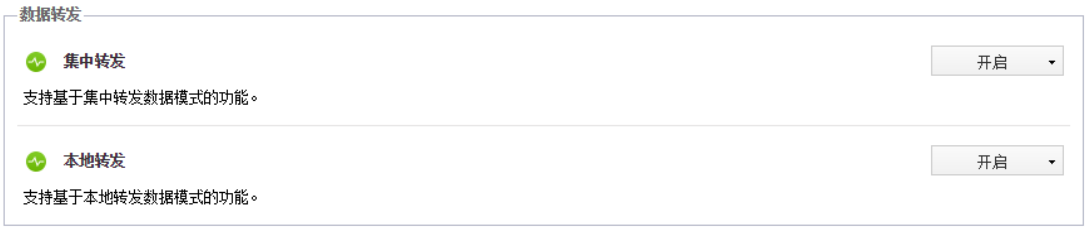
4.10.2. 服务配置

本页面可以配置控制器需要开启、关闭哪些功能，在不需要使用某类功能时可以选择禁用服务，以便最大化的节省系统资源消耗，使系统能够将更多的资源分配给已开启的功能，使其更加流畅的运行。

4.10.2.1. 数据转发

集中转发：适用于所有接入点都使用集中转发模式。禁用服务可以释放大量资源，需要重启设备。该服务禁用状态时“集中转发应用识别”服务和集中转发无线网络也将被禁用。

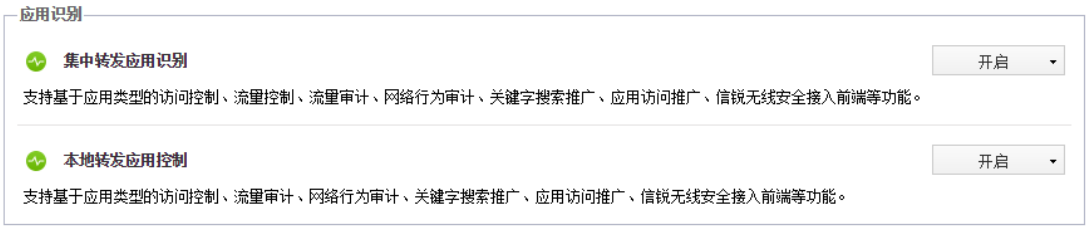
本地转发：适用于所有接入点都使用本地转发模式。禁用服务可以释放大量资源，需要重启设备。该服务禁用状态时“本地转发应用识别”服务和本地转发无线网络也将被禁用。



4.10.2.2. 应用识别

集中转发应用识别：功能开启之后，将会识别集中转发用户的应用。关闭后可以释放部分资源，无需重启设备。禁用服务可以释放大量资源，需要重启设备。

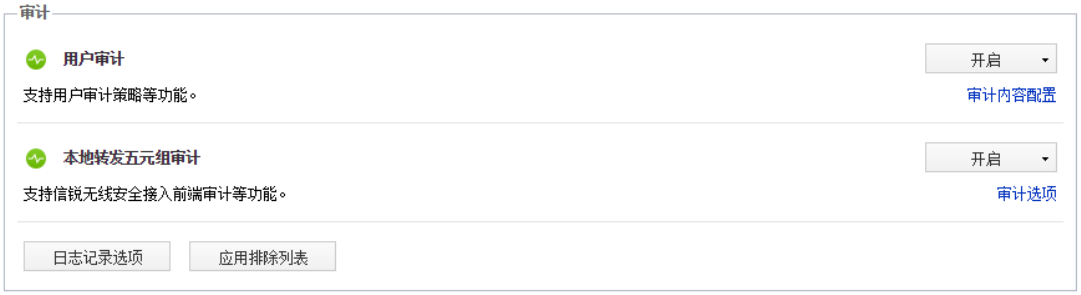
开启本地转发应用识别：功能开启之后，将会识别本地转发用户的应用。启用功能之后，需要在本地转发应用识别选项中选择，需要开启识别的本地转发的无线网络或是接入点有线认证策略，默认不勾选。功能开启之后，将会消耗接入点 2%-5%的上行带宽。



4.10.2.3. 审计

用户审计：开启功能，需要启用内置日志中心或是配置一个外置的日志中心。

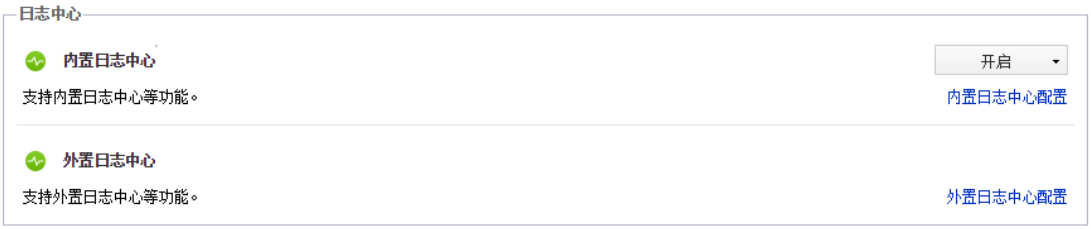
本地转发五元组审计：开启功能，可以审计本地转发用户的五元组信息。



4.10.2.4. 日志中心

内置日志中心：开启和关闭内置日志中心，配置磁盘预警和自动删除数据选项。

外置日志中心：开启和关闭内置日志中心，管理外置日志中心的同步账号。



4.10.2.5. 特色服务

信锐无线安全接入前端：开启、关闭信锐无线安全接入前端服务。服务开启时将采集的终端信息、上网行为信息等上报给第三方设备。

物联网服务：开启、关闭物联网功能。服务开启时才能进行物联网设备的部署和管理

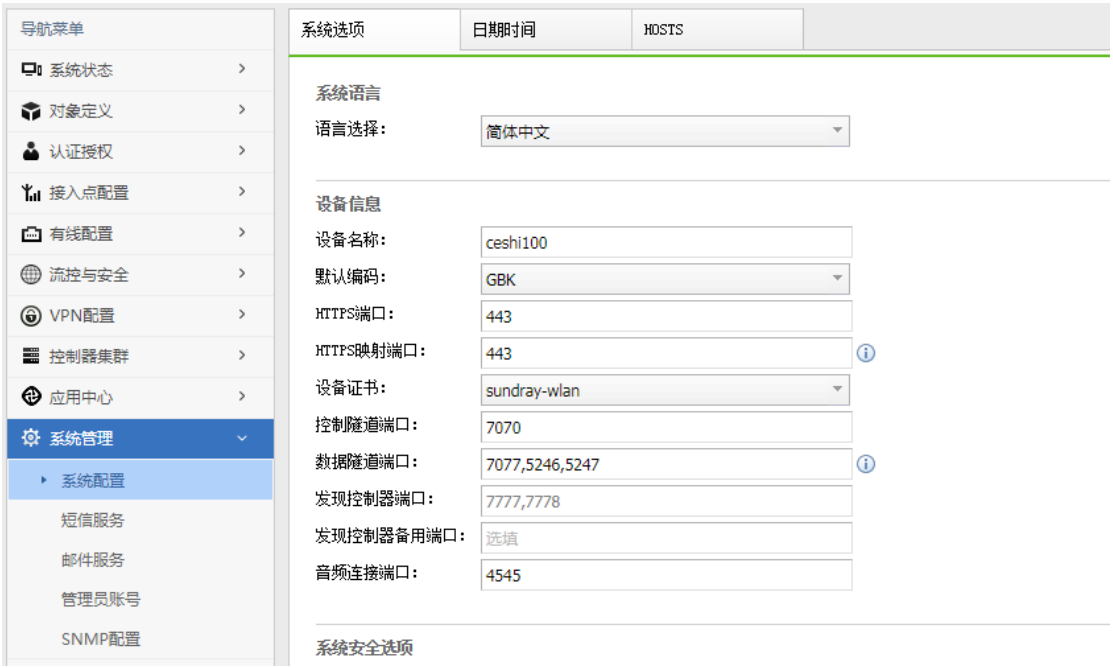
VPN 服务：开启、关闭 VPN 服务。服务开启时才能在 VPN 配置页面进行配置。

数据分析平台：开启、关闭数据分析平台服务。服务开启时才允许进行数据分析平台配置项配置。

4.11. 系统管理

『系统管理』包括以下几个模块【系统配置】、【短信服务】、【邮件服务】、【管理

员账号】、【SNMP 配置】，下面我们将一一介绍上述功能



4.11.1. 系统配置

4.11.1.1. 系统选项

系统选项可以配置关于设备的基本信息，包括设备的中英版本切换，可以在此选择切换。

1、设备信息

设备名称：填写设备的名称

默认编码：选择你所在国家/地区的本地编码，例如简体中文选择 GBK，繁体中文选择 BIG5。设备的部分功能需要依赖于正确地选择此编码。例如在 Windows 无线客户端中，PEAP-MSCHAPv2 认证过程中发送的用户名使用本地编码格式，而本地用户数据库中用户名为 utf-8 编码。如果需要支持中文用户名，则系统在认证过程中需要知道原始编码，并转换为 utf-8 编码。

HTTPS 端口：控制台登录界面端口

设备证书：给 NAC 设备设置证书，用于安全登录 NAC 设备。

控制隧道端口：默认控制隧道端口号 7070，手动指定端口号范围：1024-65535。

数据隧道端口：默认数据隧道端口号 7077，手动指定端口号范围：1024-65535。

发现控制器端口：发现控制器端口号默认 7777。

发现控制器备用端口：手动指定备用端口号范围：1024-65535。修改备用端口号后，默认的端口 7777 还可以发现控制器。

集中管理端口：默认集中管理端口号 5000，手动指定端口号范围：1024-65535。

2、系统安全选项

控制台超时：管理员登录控制台后，如果在设定的超时时间内，未进行任何操作，则系统会注销此次登录。

3、webAgent

webAgent 功能用于解决接入点跨广域网/公网远程部署时，由于控制器没有固定 IP 地址，导致接入点无法与控制器无法进行通信的问题。使用该功能时，请联系客服或技术支持获取 webAgent 服务。

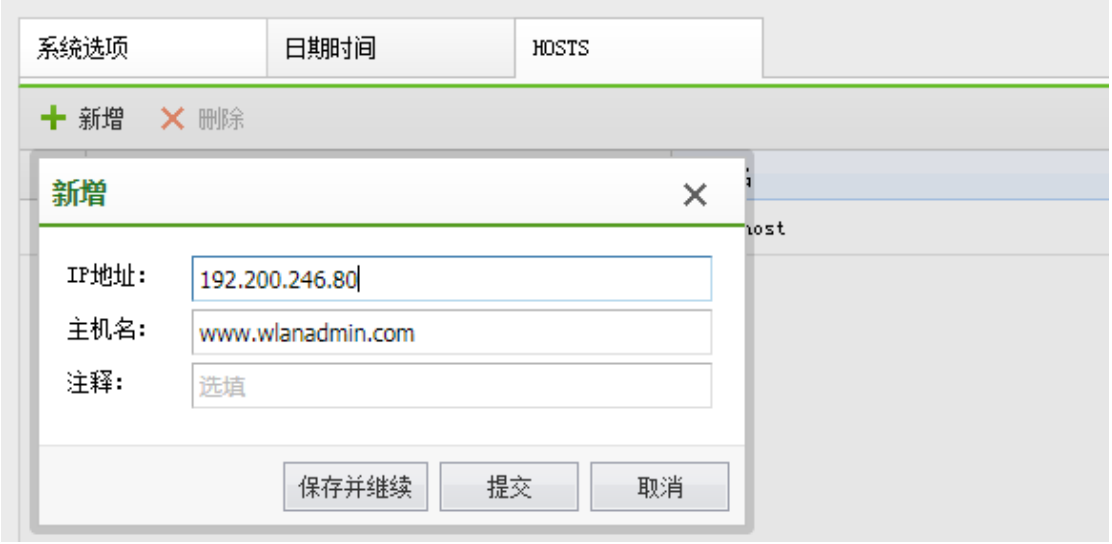
注：开启 webagent 功能时，需要开放 7777（udp 协议）、7070（tcp 协议）、7077（udp 协议）、800（tcp 协议）端口号。

4.11.1.2. 日期时间

设置系统时间，可以通过获取本地 PC 或通过同步 NTP 服务器的方式同步时间，如下图，并可以设置设备工作所在的时区。

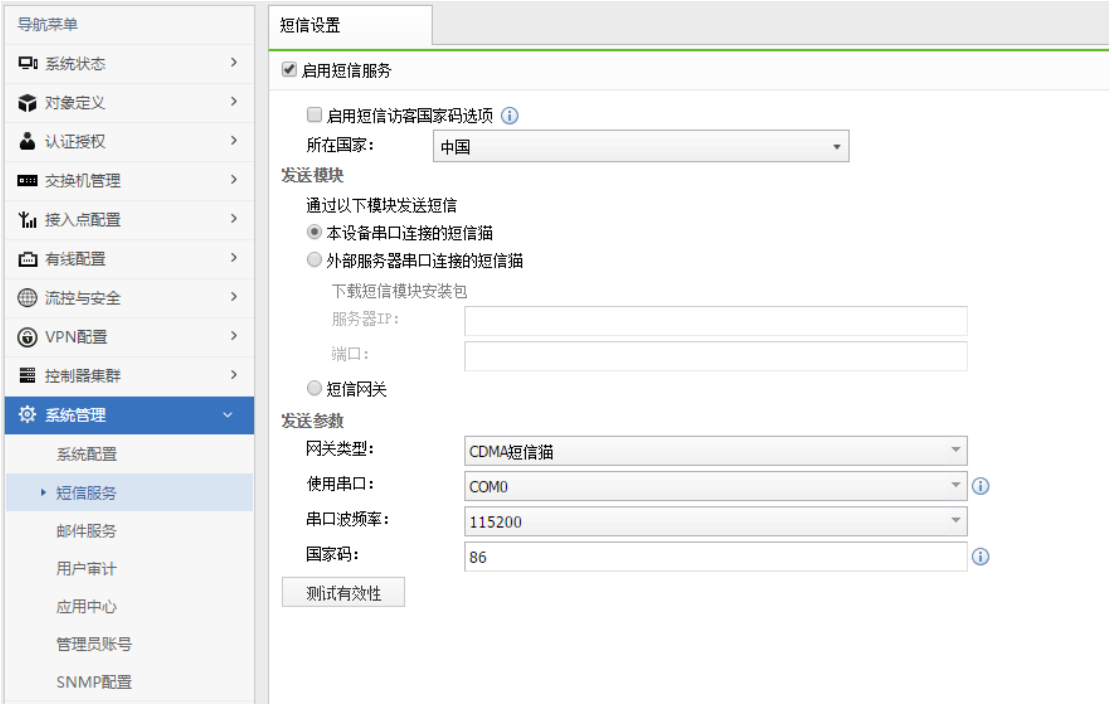
4.11.1.3. HOSTS

当指定我们设备作为域名解析服务器时，可以通过设置 HOSTS 对外解析域名已经设置好的域名，而且后续还可以设置 DNS 代理，真正实现以我们设备的 IP 地址作为服务器解析所有的域名。当网络中设置以 NAC 的 IP 为 DNS 服务器时，并设置了 HOSTS 中对于域名 wwww.adminwlan.com 的 IP 时，AP 会以该域名对应的 IP 去自动发现 NAC，实现 NAC 对 AP 的管控。



4.11.2. 短信服务

在部署短信认证的无线网络时，需要先启用短信认证服务，并正确配置短信发送参数。

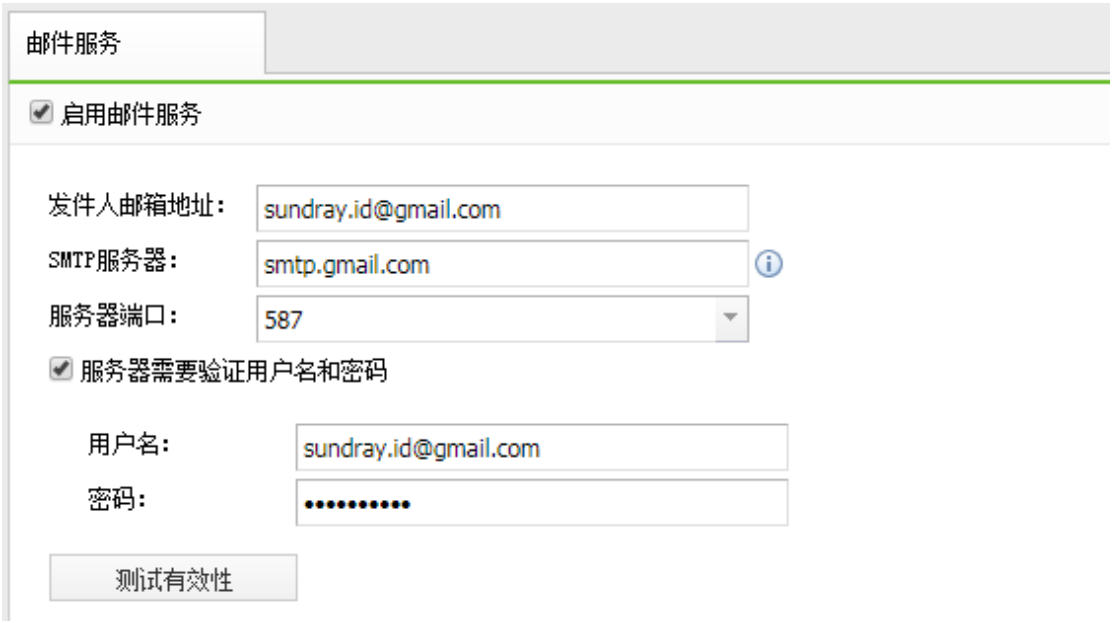


系统支持的短信发送方式：通过连接到无线控制器串口的短信猫发送、通过连接到外部服务器的短信猫发送、通过短信网关发送。

说明：如果无线控制器部署的机房中，手机网络信号差，导致无法发送短信。则可以选择把短信猫连接到一台服务器，并把服务器部署到此机房以外，且信号良好的环境中，由此服务器来代理发送短信。

4.11.3. 邮件服务

本地用户数据库中邮箱绑定类型的账号绑定邮箱后，可以通过邮件找回密码，管理员也可以将用户名密码发送到用户绑定的邮箱中。使用之前需要启用并正确配置邮件服务。



发件人邮箱地址：邮件发件人账号，需要在 smtp 服务器上注册。

SMTP 服务器器：邮件发送服务器，可以填写域名或者服务器 ip 地址，默认端口 25。

用户名：邮件服务器校验使用的用户名，建议与发件人邮箱地址保存一致。

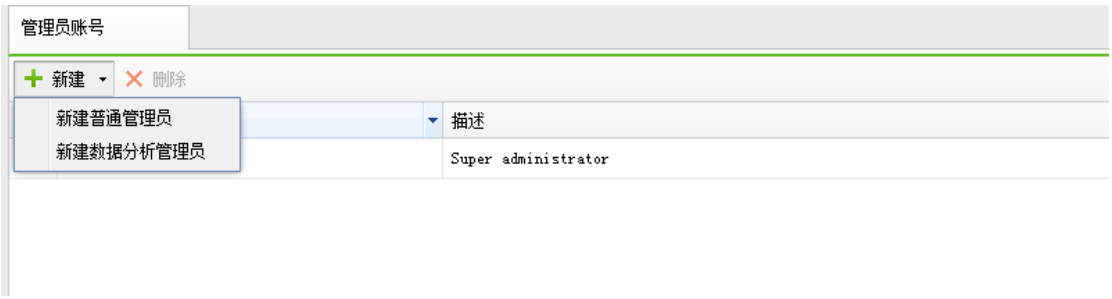
密码：邮件服务器校验密码，即用户名对应的密码。

4.11.4. 管理员账号

默认系统内置了 admin 超级管理员，用于登录设备。

超级管理员账号：默认 admin/admin 是 webui 的超级管理员，只能修改自身密码，可以新增和删除和修改其他用户的用户名和密码。

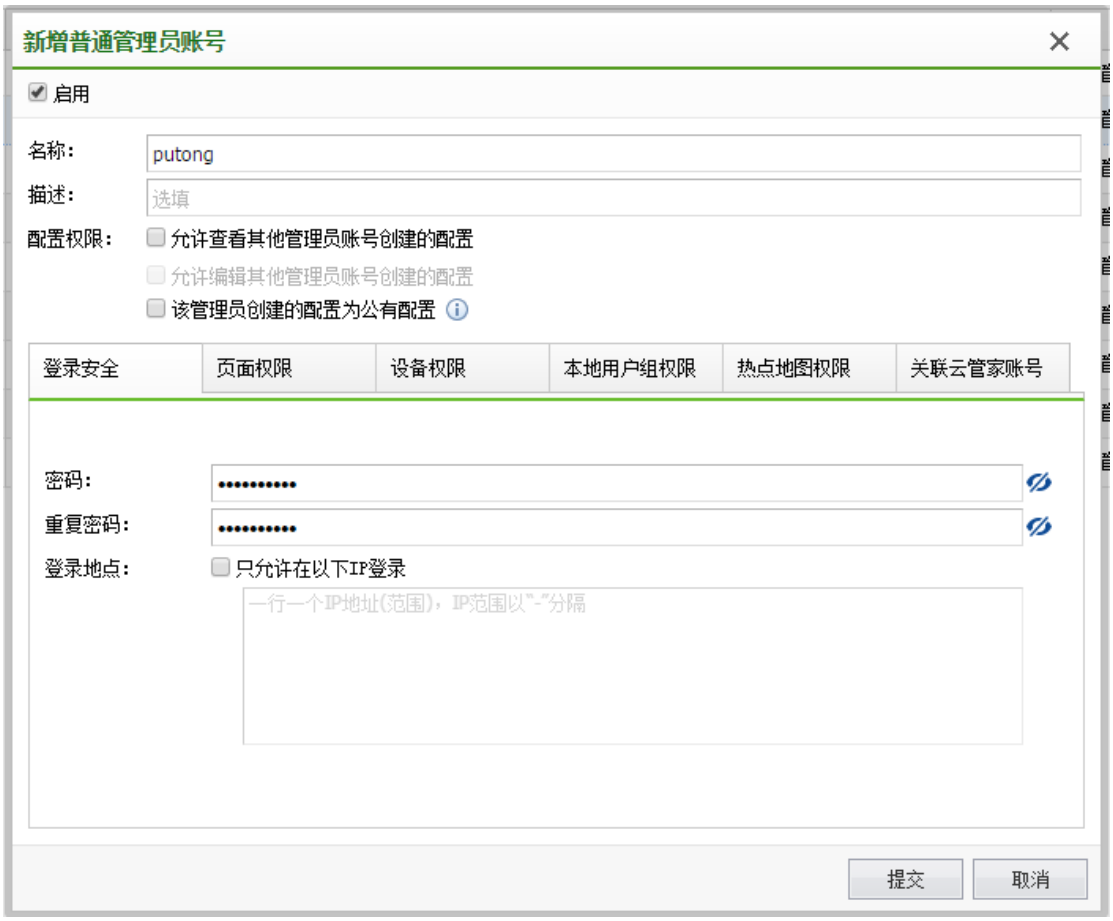
新建分为新建普通管理员和新建数据分析管理员。



4.11.4.1. 普通管理员

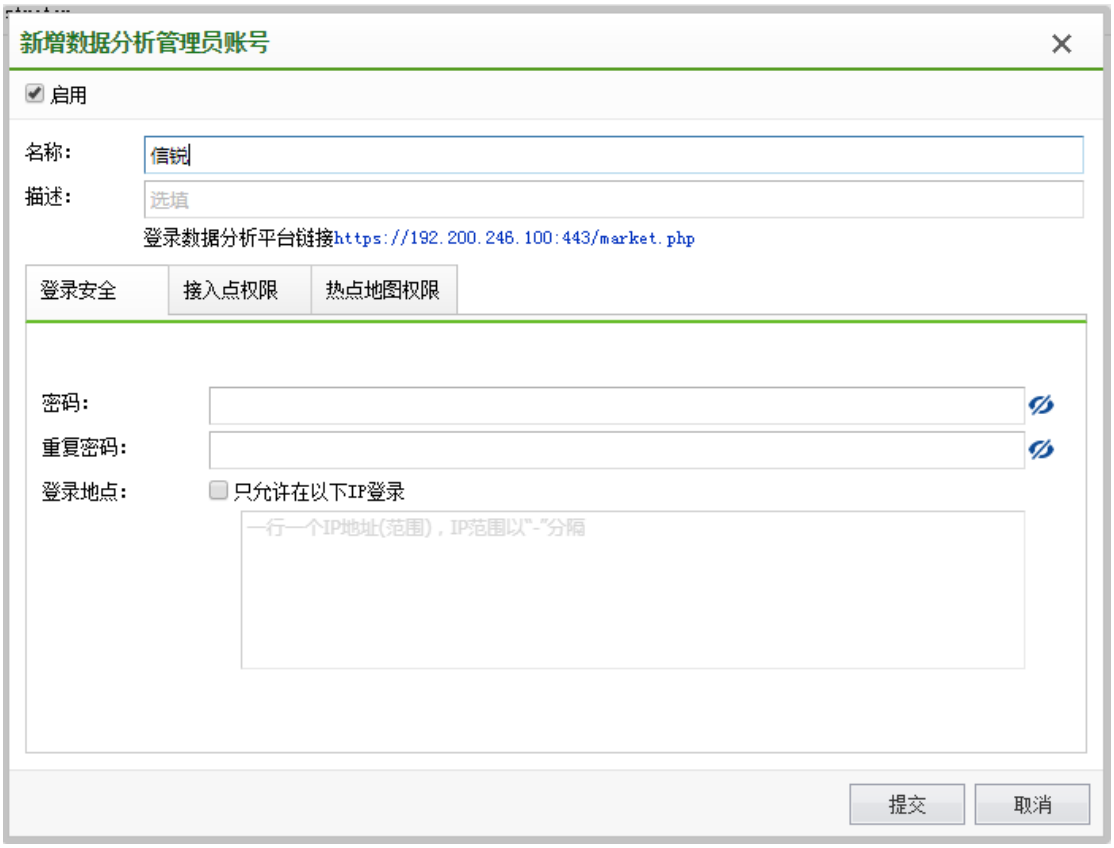
可以查看控制台页面和营销中心页面，支持按页面配置权限，按分支或接入点分组配置权限，按本地用户组织结构配置权限，热点地图权限，并且可以关联云管家账号。

支持创建公有配置，查看或修改其他管理员的配置。



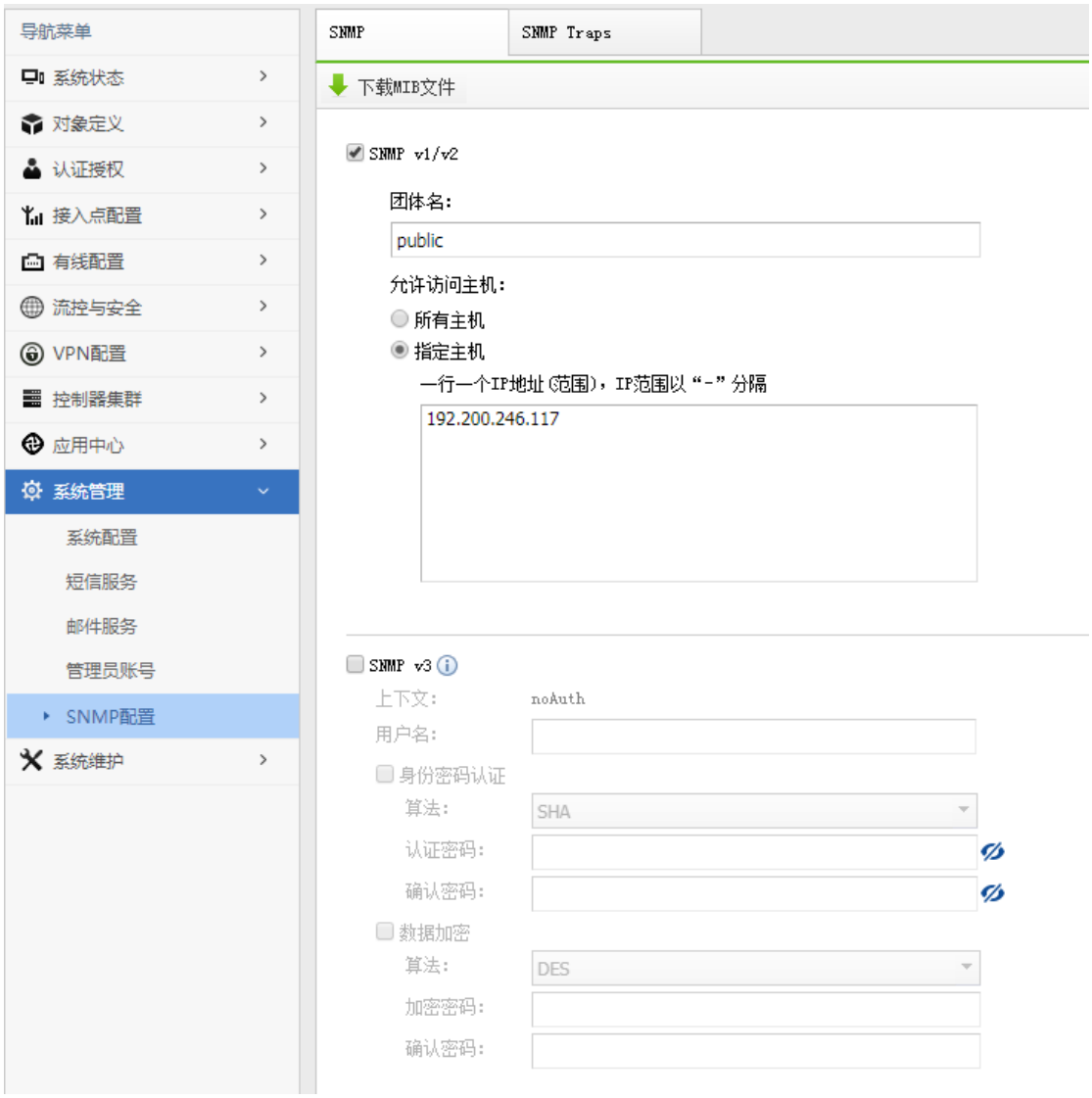
4.11.4.2. 营销管理员

只允许登陆营销中心页面，支持针对接入点和热点地图分权。



4.11.5. SNMP 配置

SNMP(Simple Network Management Protocol,简单网络管理协议)，用于管理网络中上众多的软硬件平台。开启后可以通过 snmp 协议查询本设备系统信息，如设备型号，内存使用，硬盘使用率，cpu 消耗等。



4.11.5.1. SNMP V1/V2

SNMP 的第一版本和第二版本。它们都是基于团体名进行报文认证。

4.11.5.2. SNMP V3

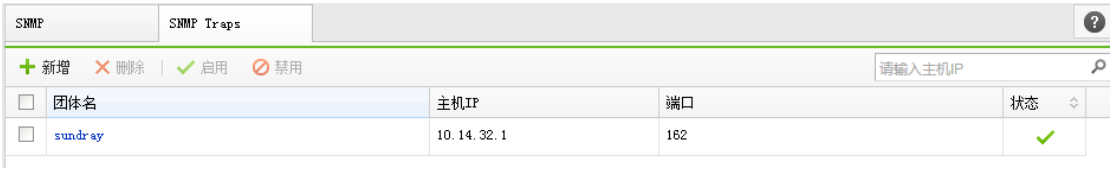
SNMP 的第三版本此版本提供重要的安全性功能，其中就包括了认证和加密两项。认证需要提供认证方式（MD5，SHA）和认证密码。加密需要提供加密方式（DES）和加密密钥。

4.11.5.3. MIB

MIB（Management Information Base，管理信息库），是由网络管理协议访问的管理对象数据库，也可理解为是所有可管理对象的集合。下载本设备 MIB 后，再导入到相应的管理端后，可以管理或查询的本设备的一些基本信息，如设备信号，内存使用，硬盘使用，CPU 消耗等。

4.11.5.4. SNMP Traps

SNMP trap 又称 SNMP 陷阱，启用后可以让本设备主动发送信息到管理端，而不需要等到的管理端轮询后再发送。需要配置管理端的 IP 地址和端口，以及团体名。支持向多个管理端发送信息。



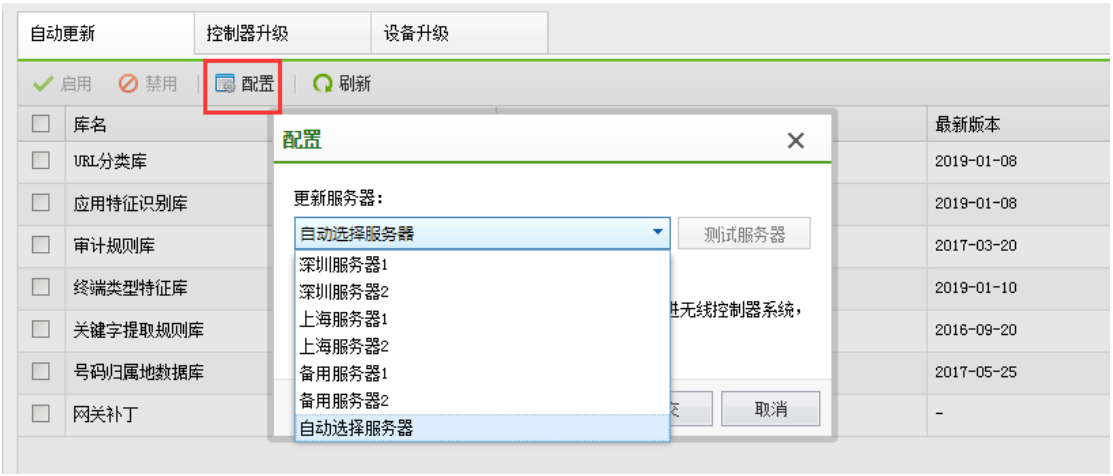
4.12. 系统维护

『系统维护』包括如下几个功能模块【系统更新】、【日志查看】、【备份恢复】、【故障排除】、【调试选项】、【重启及格式化】、【命令行控制台】、【导出系统记录】、【设备授权更新】；下面将一一讲解

4.12.1. 系统更新

4.12.1.1. 自动更新

启用自动更新：NAC 可以自动更新系统补丁，实现 NAC 功能的优化。更新服务器可以选择“自动更新服务器”，也可以手动选择“深圳服务器”、“上海服务器”或“备用”服务器。



当勾选“加入用户体验改善计划”时，表示允许发送系统质量报告给信锐技术，帮助我们改进无线控制器系统，该报告不会涉及您组织的任何信息。

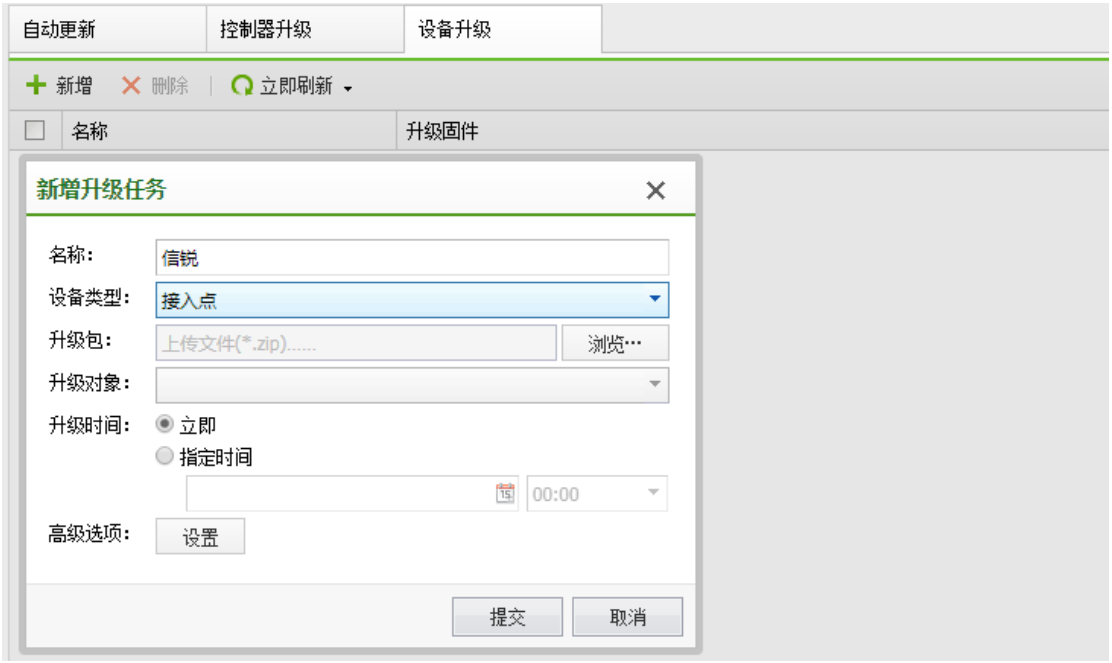
4.12.1.2. 设备升级

设备升级包括正式包升级与补丁包升级，设备升级功能可以替代原有信锐系列升级客户端给设备升级的方法，并且可以支持升级补丁包与补丁包回滚操作。

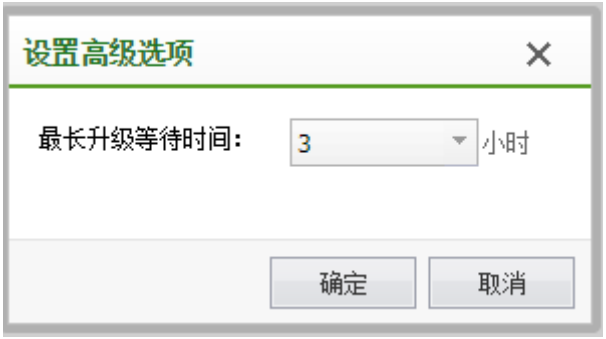
提示：为了保障升级顺畅、稳定，建议正式包升级时，采用专业的客户端升级，详细方法参考第六章。

4.12.1.3. 设备升级

接入点/交换机为零配置设备，通常并不需要关心设备的软件版本。接入点或交换机连接到无线控制器后，会自动从无线控制器中下载并安装系统。如果要升级到最新版本，只需要升级无线控制器，不需要单独升级无线接入点或交换机。该页面的升级功能，主要提供给设备供应商的技术支持人员使用。



新增升级任务还可以设置高级选项：设置最长升级等待时间，当 AP 并没有立刻接入 NAC 时，可以设置比较长的升级等待时间，当 AP 接入 NAC 时，NAC 就会自动给 AP 升级，设置界面如下图：

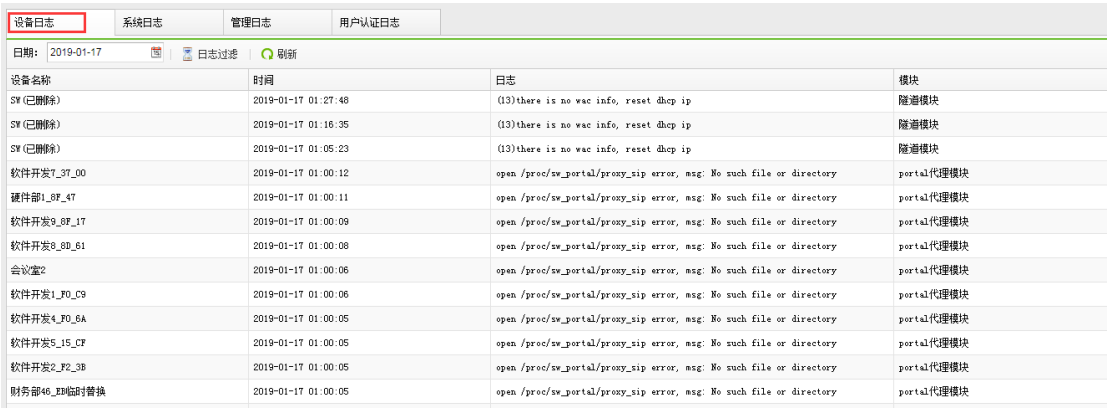


提示：当 AP 接入 NAC 控制器时，AP 版本与 NAC 版本不匹配，AP 会自动升降到与 NAC 相同版本，只有当 AP 不能顺利升级到 NAC 版本时，或者 AP 版本是比 NAC 版本低但兼容的 β 版本时，才需要在控制台上主动加载包给 AP 升级。

4.12.2. 日志查看

4.12.2.1. 接入点日志

查看接入点日志产生的日志，协助发现及排除故障。

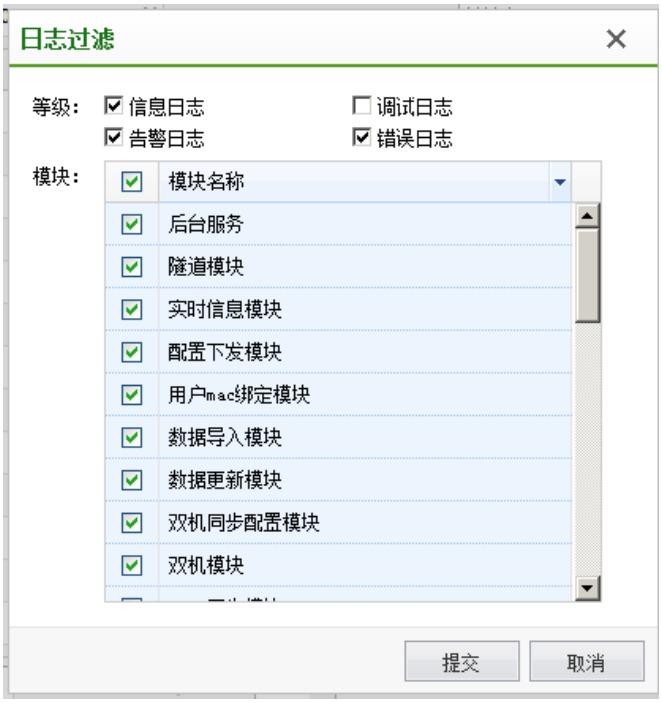


4.12.2.2. 系统日志

系统日志主要用于分析设备是否工作异常，系统日志有【信息日志】，【告警日志】、【调试日志】、和【错误日志】四种类型，并且可以根据需要选择某一个功能模块，专门查

看该功能模块的日志，便于分析 NAC 是否有故障和异常，日志过滤选项界面如下

日志过滤选项界面如下：



4.12.2.3. 管理日志

管理日志主要用于记录管理员登陆系统，注销系统，和修改系统配置的记录，便于进管理员操作的记录和审计。且日志可以通过记录“成功”和“失败”的方式进行记录和过滤，

还可以进行操作对象的过滤，配置界面如下图

时间	日志	操作对象
2019-01-17 11:11:00	登录系统	系统管理
2019-01-17 10:51:27	登录系统	系统管理
2019-01-17 10:12:28	编辑VLAN 2	有线配置
2019-01-17 10:11:23	编辑VLAN 2	有线配置
2019-01-17 10:10:20	编辑VLAN 2	有线配置
2019-01-17 09:58:52	编辑VLAN 2	有线配置
2019-01-17 09:52:43	账号 cpxx 第3次尝试登录	系统管理
2019-01-17 09:52:13	登录系统	系统管理
2019-01-17 09:52:07	账号 admin 第1次尝试登录	系统管理
2019-01-17 09:52:05	账号 cpxx 第2次尝试登录	系统管理
2019-01-17 09:51:59	账号 cpxx 第1次尝试登录	系统管理

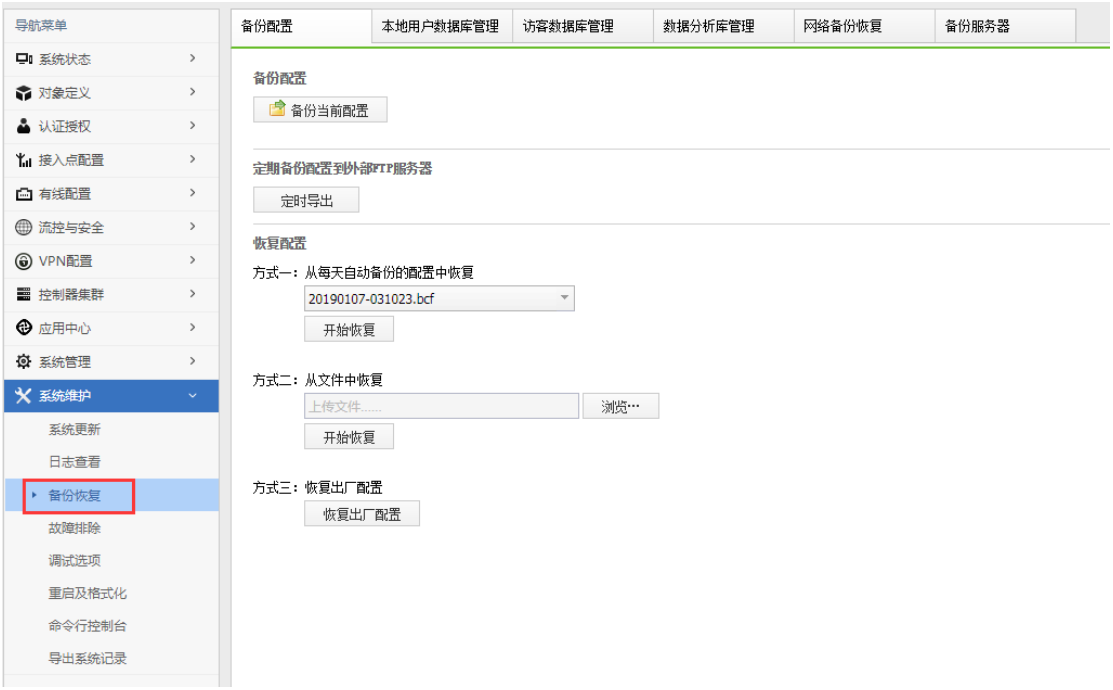
日志过滤配置界面如下图：

4.12.2.4. 用户认证日志

用户认证日志主要用于记录用户接入无线和退出无线的认证日志，用户分析用户认证情况，可以在设置的时间范围内，根据在 IP 地址，和用户名查询：

时间	事件	用户名	用户组	用户类型	认证方式	IP地址	终端MAC	接入点	接入点分组
2019-01-17 11:23:15	接入	68-EF-43-29-7…	/PSK认证组/	本地用户	WPA-PSK/WPA2-…	-	68-EF-43-29-7…	软件开发4_FO_6A	开发组
2019-01-17 11:23:11	退出	E8-B2-AC-42-4…	/PSK认证组/	本地用户	WPA-PSK/WPA2-…	-	E8-B2-AC-42-4…	会议室4_46_4E	会议室
2019-01-17 11:23:10	接入	99243	/MOA/MOA/信锐…	外部用户	WPA/WPA2(企业)	172.16.196.62	D4-68-BA-21-1…	软件开发3_ED_99	开发组
2019-01-17 11:23:08	退出	99243	/MOA/MOA/信锐…	外部用户	WPA/WPA2(企业)	172.16.196.62	D4-68-BA-21-1…	软件开发3_ED_99	开发组
2019-01-17 11:23:08	接入	E8-B2-AC-42-4…	/PSK认证组/	本地用户	WPA-PSK/WPA2-…	-	E8-B2-AC-42-4…	会议室4_46_4E	会议室
2019-01-17 11:22:50	退出	E8-B2-AC-42-4…	/PSK认证组/	本地用户	WPA-PSK/WPA2-…	-	E8-B2-AC-42-4…	会议室4_46_4E	会议室
2019-01-17 11:22:47	接入	E8-B2-AC-42-4…	/PSK认证组/	本地用户	WPA-PSK/WPA2-…	-	E8-B2-AC-42-4…	会议室4_46_4E	会议室
2019-01-17 11:22:33	IP改变	69719	/MOA/MOA/信锐…	外部用户	WPA/WPA2(企业)	172.16.196.148	78-62-56-E8-0…	硬件部1_8F_47	职能组
2019-01-17 11:22:33	接入	69719	/MOA/MOA/信锐…	外部用户	WPA/WPA2(企业)	-	78-62-56-E8-0…	硬件部1_8F_47	职能组
2019-01-17 11:22:33	退出	69719	/MOA/MOA/信锐…	外部用户	WPA/WPA2(企业)	172.16.196.148	78-62-56-E8-0…	会议室2	会议室
2019-01-17 11:22:31	退出	78130	/MOA/MOA/信锐…	外部用户	WPA/WPA2(企业)	172.16.196.29	64-76-BA-8F-5…	HR2_5D_F3	职能组
2019-01-17 11:22:17	接入	14421	/MOA/MOA/信锐…	外部用户	WPA/WPA2(企业)	172.16.196.235	F8-C3-9E-0F-2…	软件开发4_FO_6A	开发组

4.12.3. 备份恢复



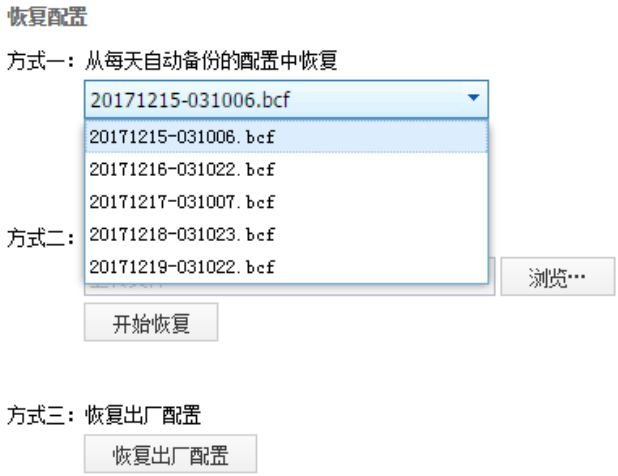
4.12.3.1. 备份配置

点击备份配置时，可以从 NAC 上下载当前系统配置，并可以保存到在 PC 上，用户可以自行保存。也可以采用方式二：从文件中恢复的方法还原下载的配置，点击备份配置时，可以下载的配置文件如下，是 bcf 格式的文件。

还可以采用备份自动备份到 FTP 服务器的方法备份

恢复配置

方式一：从每天自动备份的配置中恢复，默认系统会自动备份最近一周的配置



方式二：从之前备份的配置进行恢复

方式三：直接点击“恢复出厂配置”。

4.12.3.2. 本地数据库管理

系统中保存了大量用户账号信息，因此定期对设备本地用户数据执行备份操作是一个良好的管理习惯。

在以下情况下，可以考虑从最近备份的数据中恢复系统，以尽快恢复您的数据，并减少损失：

（1）设备损坏或丢失，需要更换全新的硬件设备

（2）设备误配置，例如误删除了大量的用户账号信息

本地用户数据库备份，有以下几种形式：

自动备份：系统每天会自动执行一次本地用户数据库备份操作，并保存在设备内置磁盘中，只保留 3 天的备份文件。

手动备份：管理员从控制台本地用户数据库管理页面中，下载当前的本地用户数据库备份文件，并保存在管理员的本地计算机中。手动备份的本地用户数据库备份文件由于保存在设备之外，将具备更高的可靠性，即使设备损坏或丢失，购买新的设备后，仍然可以从备份文件中恢复，因此建议定期执行手动备份操作。

定期备份本地用户数据库到外部 FTP 服务器：系统每天凌晨 03:10 开始，会自动将设备

的本地用户数据库上传到外部 ftp 服务器。可以避免因本设备故障而导致本地用户数据丢失的问题。

4.12.3.3. 访客数据库管理

数据管理包括清空数据、生成客流分析原始数据、数据备份与恢复

提供三种方式恢复数据库

1、使用立即备份导出的数据库进行数据库恢复。

2、使用每日 2 点-3 点自动备份的数据库进行数据库恢复。

3、将数据库恢复至被全量同步覆盖之前的还原点，只用于搭建过双机的设备。

4.12.3.4. 数据分析管理

清空数据：点击该选系，就会清空客流分析和热点地图的客流数据，还会清空推广统计的数据。注：清空后无法恢复。

生成客流原始数据：可以生成前一天的客流分析用户数据，也可以生成所有的客流分析的用户数据。

自动导出：如果配置了 FTP 服务器，可以每天自动将前一天的客流分析的用户数据导出到 FTP 服务器上。

数据备份与恢复：手工备份客流分析和推广统计数据。

手动备份:手动备份客流与推广数据，导出备份数据文件。注：可能需要较长时间，请耐心等待。

从手动备份恢复：使用手动备份的数据进行数据恢复。

4.12.3.5. 网络备份恢复

系统中保存了大量网络配置信息，因此定期对设备网络配置执行备份操作是一个良好的管理习惯。

在以下情况下，可以考虑从最近备份的数据中恢复网络配置，以尽快恢复您的网络，并减少损失：

1、设备损坏或丢失，需要更换全新的硬件设备

2、设备误配置，例如误删除了大量的网络配置

3、分支设备性能不够，需要升级新设备

网络备份恢复，只有一种形式：手动备份

管理员从控制台网络备份恢复页面中，下载当前的网络配置备份文件，并保存在管理员的本地计算机中。手动备份的网络配置备份文件由于保存在设备之外，将具备更高的可靠性，即使设备损坏或丢失，分支替换新设备，购买新的设备后，仍然可以从备份文件中恢复，因此建议定期执行手动备份操作。

4.12.3.6. 备份服务器

配置还可以采用备份自动备份到 FTP 服务器的方法备份。备份服务器用于备份系统配置和人流量分析的数据。

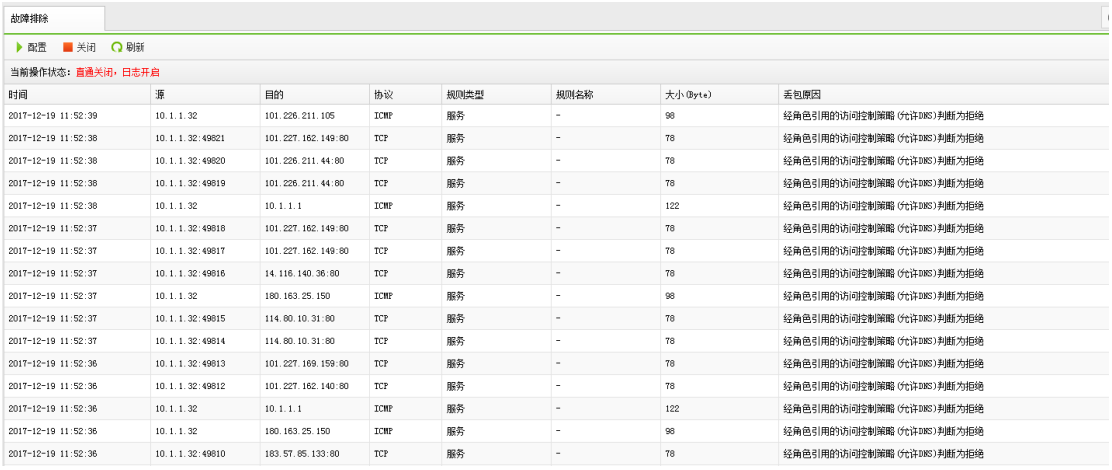
4.12.4. 故障排除

故障排除，主要用于网络故障时，用于排查问题原因，当无线终端可能由于配置问题导致用户无法正常上网时，进行故障排除和数据直通，使用方法与深信服 AC 设备类似，先是

开启故障日志，也可以同时开启数据直通。提供了以下功能：

显示被系统拦截的数据包日志，以及拦截原因。当用户无法访问网络时，可以开启数据包拦截日志，并输入 IP 地址过滤，以查看数据包被拦截的原因。

开启直通，数据包将完全不受策略的控制，直接转发。此功能在遇到策略配置错误所导致的网络访问故障时，能快速地恢复网络。直通开启后，为了方便定位原因，系统将仍然输出数据包拦截日志，但实际上并未拦截数据包。

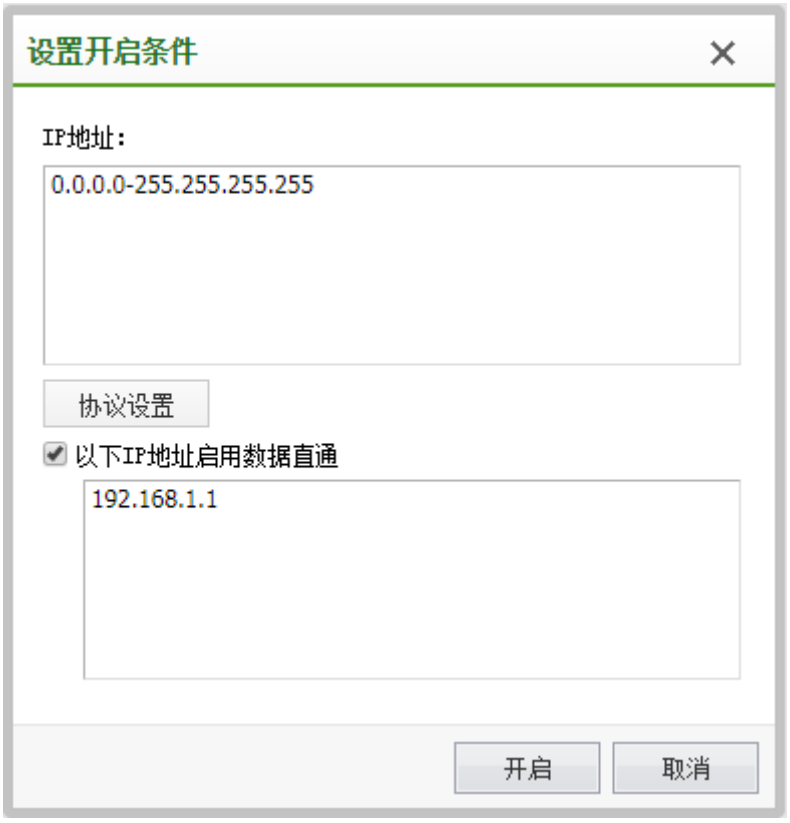

故障排除

配置 关闭 刷新

当前操作状态：直通关闭，日志开启

时间	源	目的	协议	规则类型	规则名称	大小(Byte)	丢包原因
2017-12-19 11:52:39	10.1.1.32	101.226.211.105	ICMP	服务	-	98	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:38	10.1.1.32:49821	101.227.162.149:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:38	10.1.1.32:49820	101.226.211.44:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:38	10.1.1.32:49819	101.226.211.44:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:38	10.1.1.32	10.1.1.1	ICMP	服务	-	122	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:37	10.1.1.32:49818	101.227.162.149:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:37	10.1.1.32:49817	101.227.162.149:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:37	10.1.1.32:49816	14.116.140.36:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:37	10.1.1.32	180.163.25.150	ICMP	服务	-	98	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:37	10.1.1.32:49815	114.80.10.31:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:37	10.1.1.32:49814	114.80.10.31:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:36	10.1.1.32:49813	101.227.169.159:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:36	10.1.1.32:49812	101.227.162.140:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:36	10.1.1.32	10.1.1.1	ICMP	服务	-	122	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:36	10.1.1.32	180.163.25.150	ICMP	服务	-	98	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:36	10.1.1.32:49810	183.57.85.133:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝

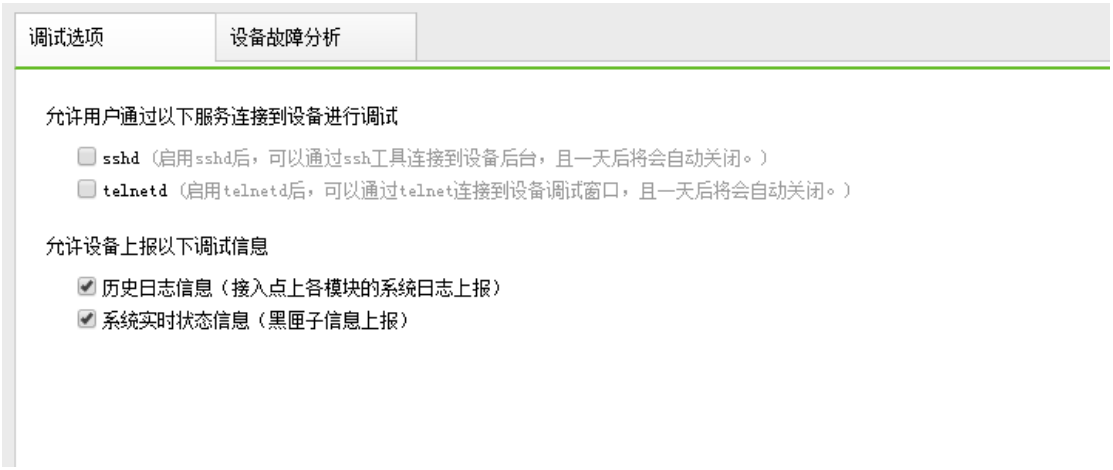
设置开启条件界面如下图：



4.12.5. 调试选项

4.12.5.1. 调试选项

允许用户通过 sshd，telentd 方式连接到本设备上进行调试。允许用户通过开启历史日志信息和系统实时状态信息开关，采集设备的相关日志信息（不包含任何用户配置信息）。



4.12.5.2. 设备故障分析

当设备工作不正常时，可以使用该功能修改查看设备状态，定位故障原因，使设备正常工作。工作不正常是指设备已经连入网络，但是无法连接上 wac 甚至无法发现，这时可以用该故障分析功能进行调试。主要功能为修改网络配置，查询 CLI 命令，恢复默认配置。如果设备工作正常，无需使用此功能。注意，如果操作不当可能适得其反。

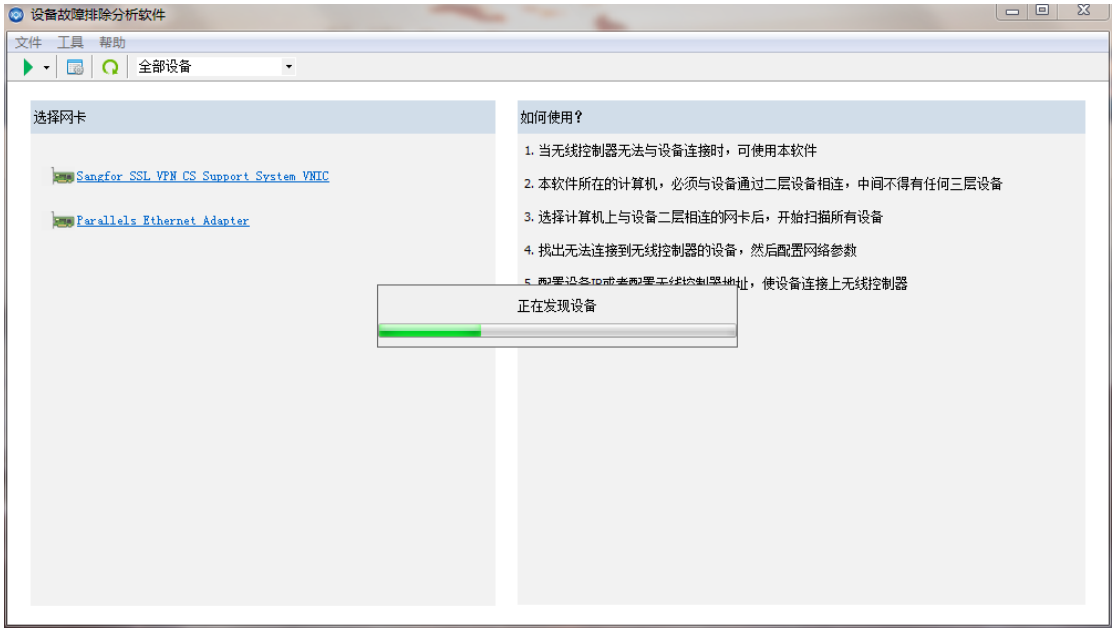
网页版工具只能扫描到与 NAC 二层相连的 AP；如果 AP 与 NAC 三层连接，则需要在 AP 的二层网络中接入一台 PC，下载 AP 诊断工具，在这台 PC 上运行工具调试 AP。网页版工具默认使用 NAC 的登陆密码去操作 AP，如果密码输入不正确会提示用户重新输入密码。

如果 AP 网络配置有误，例如 IP、网关、掩码不正确 导致不能和 NAC 通讯，点击开始配置通过设置正确的数据即可解决。

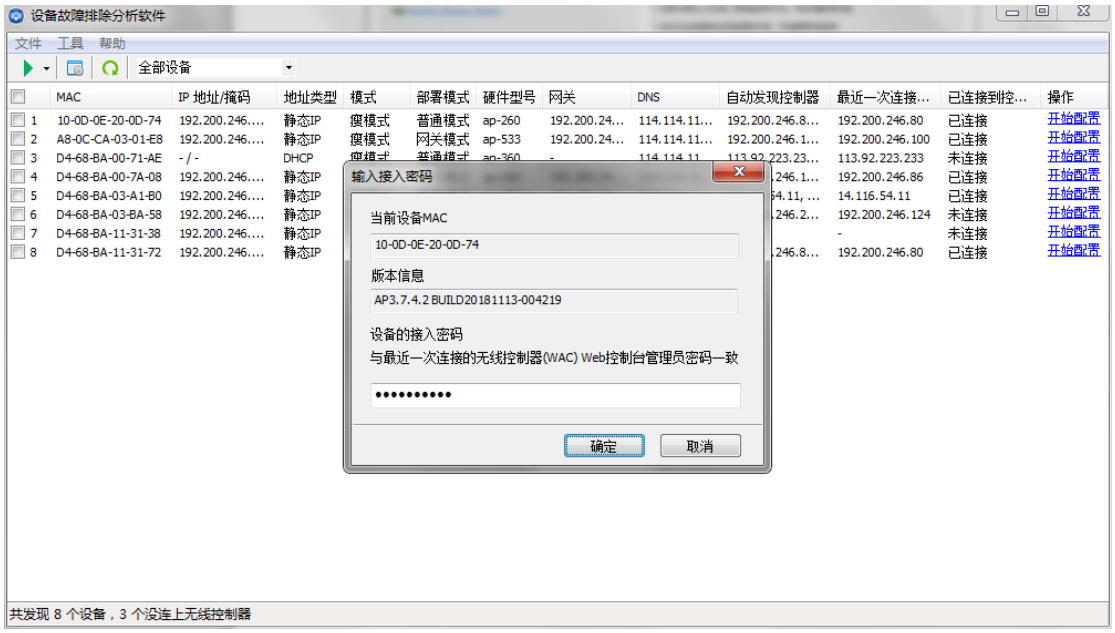
4.12.5.3. AP 诊断工具

AP 诊断工具客户端版本可以下载到 Windows 系统上运行，并且需要在 PC 上安装 winpcap 后才能可以使用。常用于 AP 无法自动发现 NAC 的场景，比如无 DHCP 环境，远程 AP 配置，AP 掉线故障排查，拨号 AP 配置 Webagent 等环境。目前该工具配置功能只能临时保存在 AP 上，如果 AP 重启会失效，需要 AP 在 NAC 上线后，从 NAC 上下发配置保存到 AP 上，AP 重启配置才不会失效。

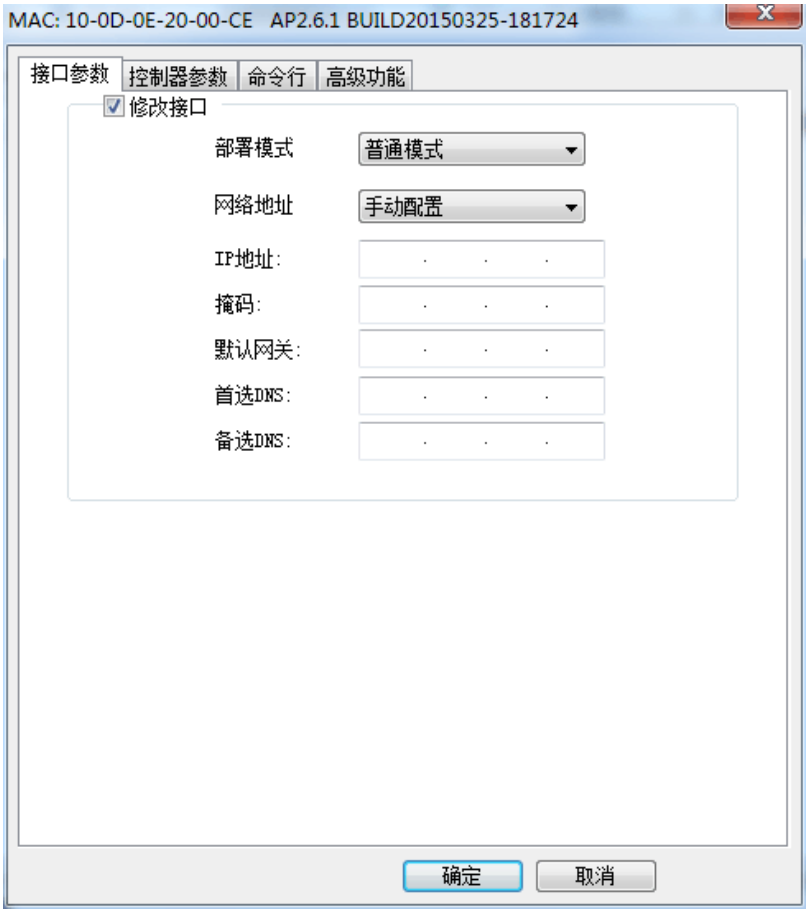
选择本地网卡后扫描 AP，页面如下：



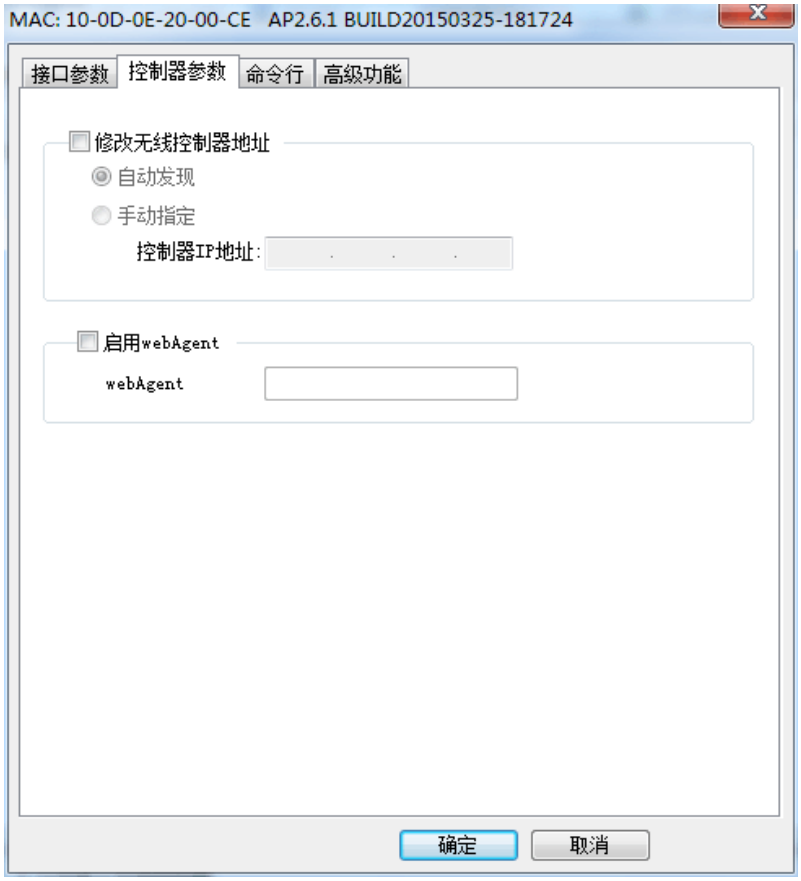
登录 AP。



配置 AP 接口参数：修改 AP 的部署模式，IP 地址 ，网关信息等。

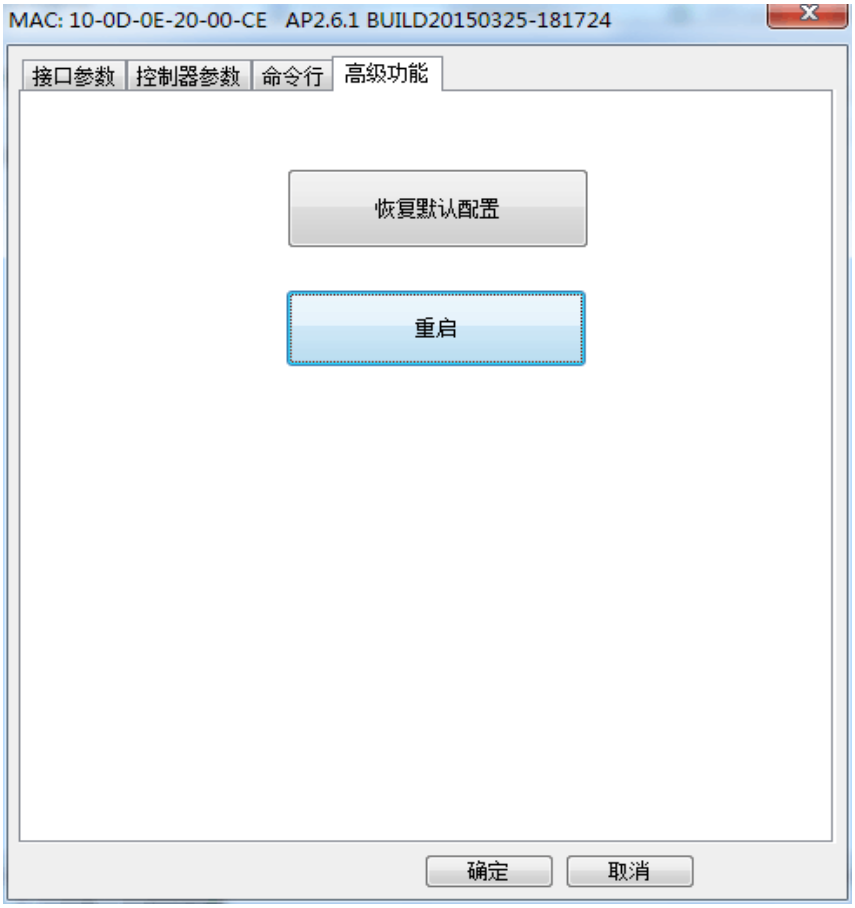


控制器参数：修改无线控制器 IP 地址，webagent 地址。



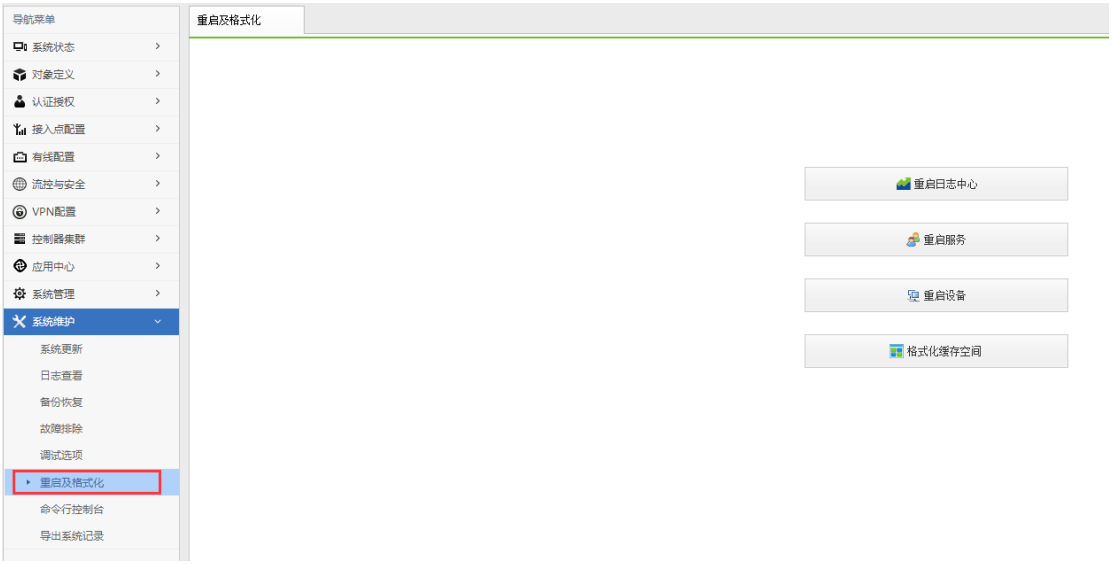
命令行：在命令行下可以执行一些简单的调试命令

高级配置：恢复 AP 的默认配置，重启 AP



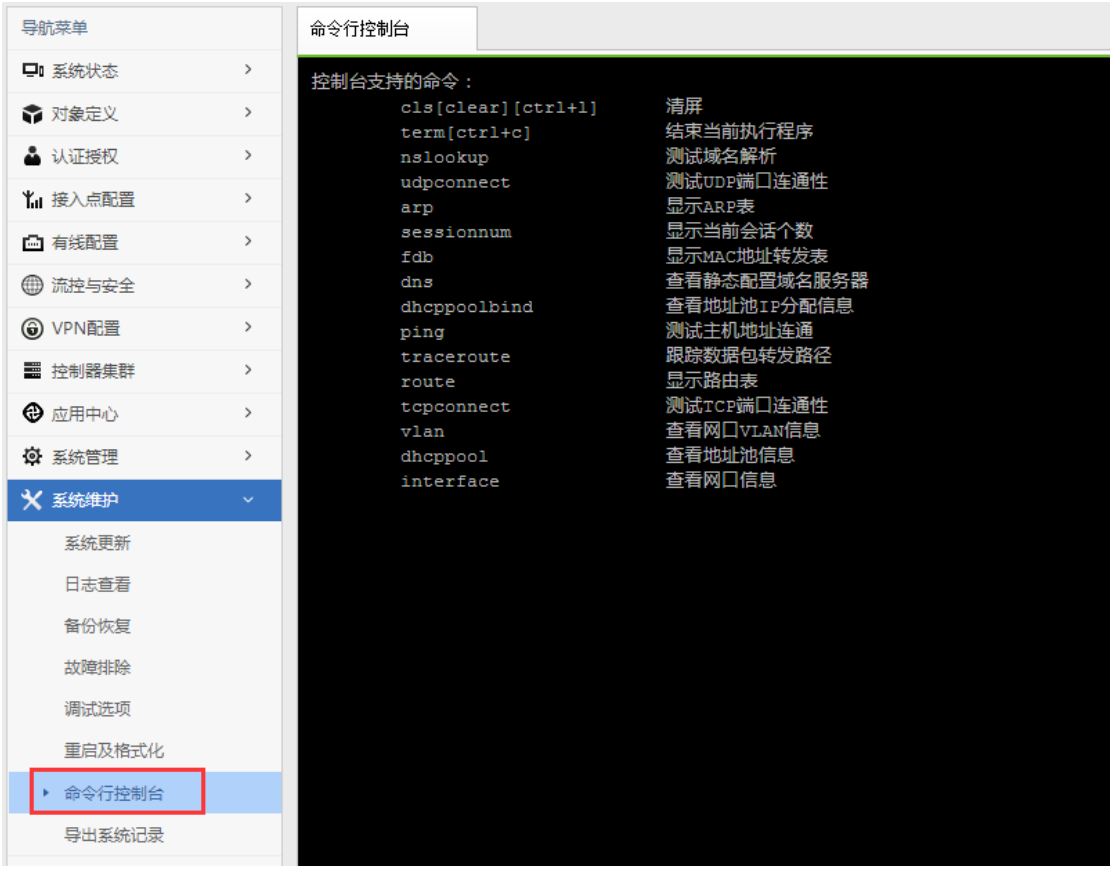
4.12.6. 重启及格式化

在 WEB 页面上重启数据中心、重启服务、重启设备、格式化缓存空间



4.12.7. 命令行控制台

提供可直接操作 nac 设备的调试命令，用于排除问题。

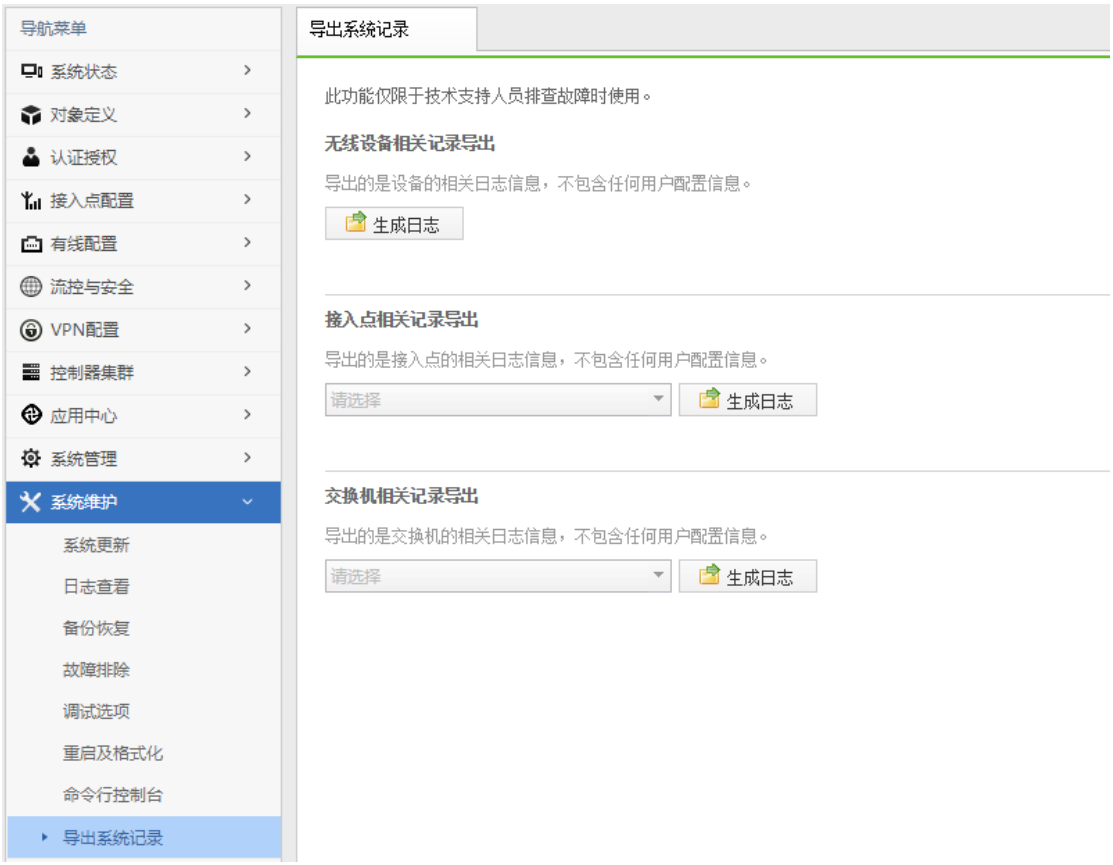


支持命令：

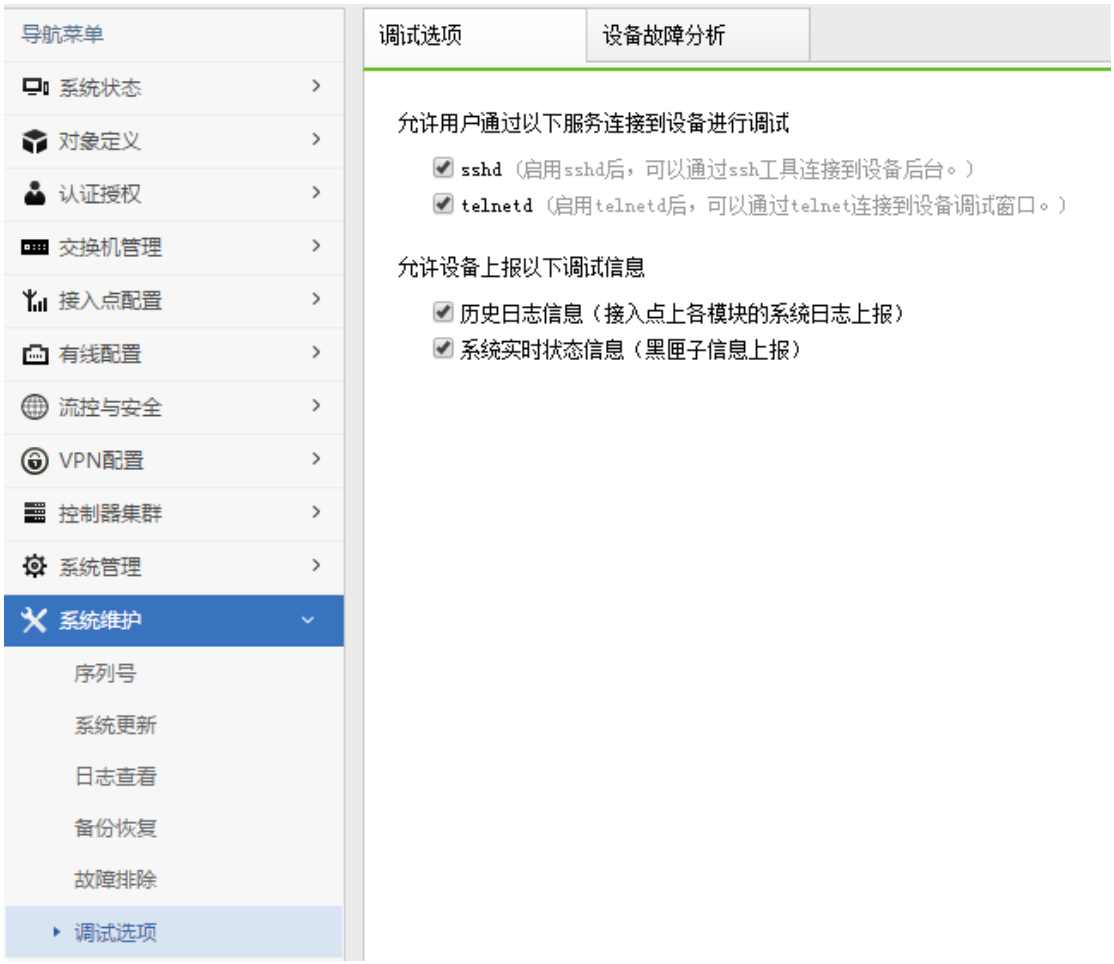
cls[clear][ctrl+l]	清屏
term[ctrl+c]	结束当前执行程序
vrrp	显示 VRRP 表
udpconnect	测试 UDP 端口连通性
arp	显示 ARP 表
sessionnum	显示当前会话个数
fdb	显示 MAC 地址转发表
dns	查看域名服务器
dhcppoolbind	查看地址池 IP 分配信息
ping	测试主机地址连通
traceroute	跟踪数据包转发路径
route	显示路由表
tcpconnect	测试 TCP 端口连通性
vlan	查看网口 VLAN 信息
dhcppool	查看地址池信息
interface	查看网口信息

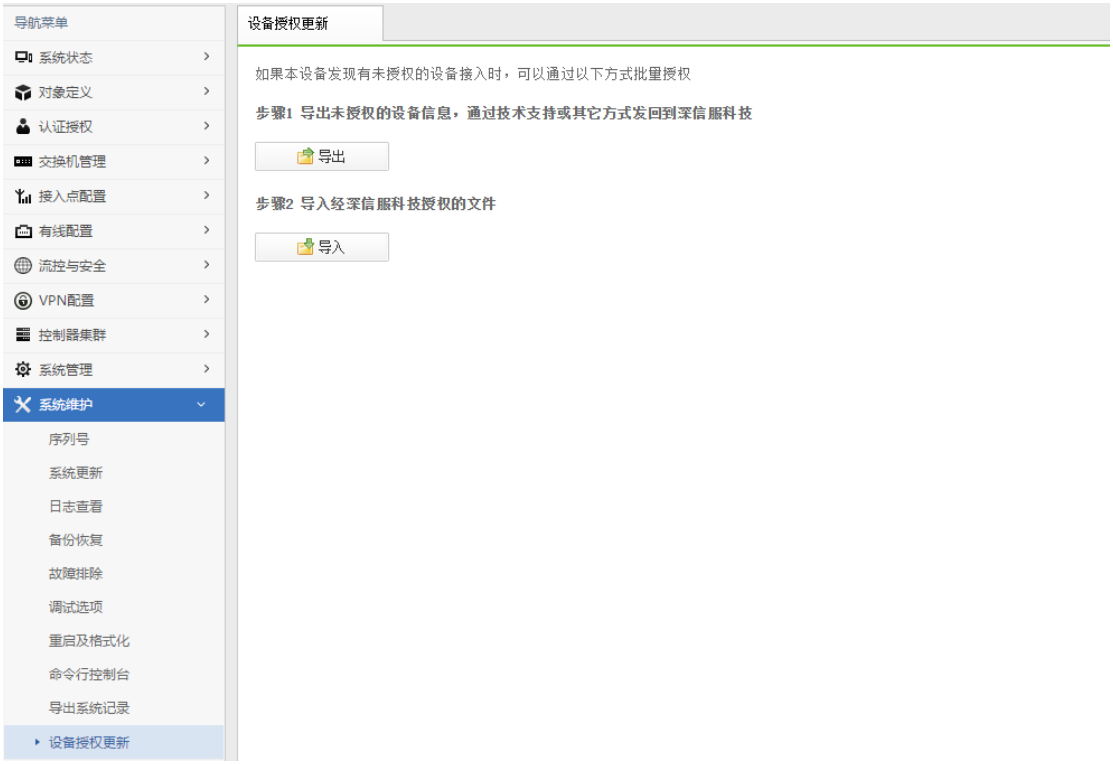
4.12.8. 导出系统记录

导出系统记录，用于研发技术支持人员排查故障时使用。其中导出无线设备相关记录包含系统日志、服务日志、bugreport、blackbox、core（mininac 不导出）、APpinit 启动日志。接入点相关记录包含接入点日志、bugreport、blackbox。



要导出关于 AP 的系统记录日志，需要在调试选项菜单下，开启允许 AP 上报调试信息，如下图：


导航菜单
系统状态
对象定义
认证授权
交换机管理
接入点配置
有线配置
流控与安全
VPN配置
控制器集群
系统管理
系统维护
序列号
系统更新
日志查看
备份恢复
故障排除
调试选项
调试选项
设备故障分析
允许用户通过以下服务连接到设备进行调试
sshd（启用sshd后，可以通过ssh工具连接到设备后台。）
telnetd（启用telnetd后，可以通过telnet连接到设备调试窗口。）
允许设备上报以下调试信息
历史日志信息（接入点上各模块的系统日志上报）
系统实时状态信息（黑匣子信息上报）



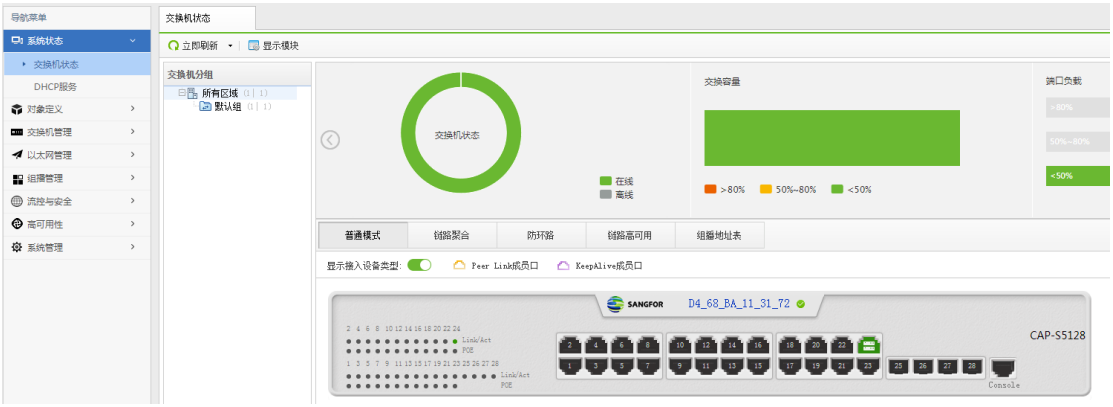
4.13. 交换机管理中心

『交换机管理中心』包括【系统状态】、【对象定义】、【交换机管理】、【以太网管理】、【组播管理】、【流控与安全】、【高可用性】、【系统管理】这 8 个菜单选项。

4.13.1. 系统状态

4.13.1.1. 交换机状态

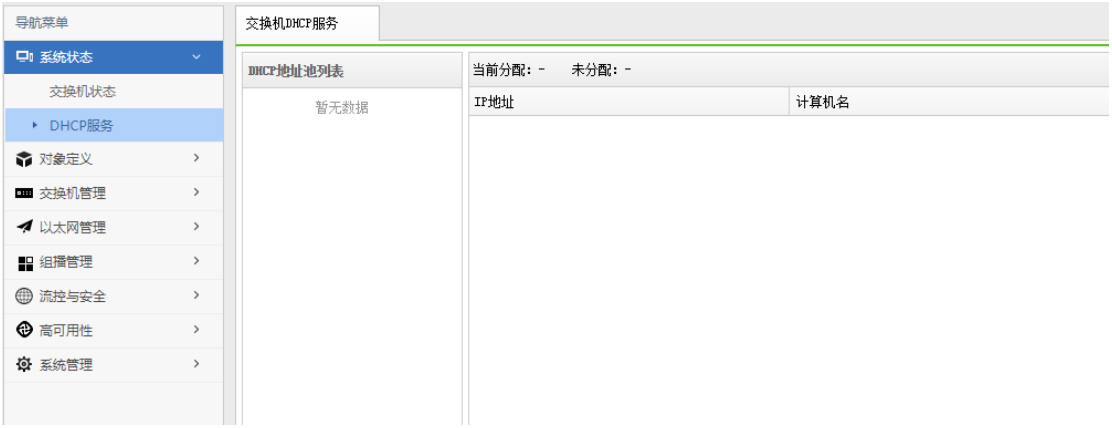
显示交换机的运行状态，可查看交换机的在线状态、负载以及端口状态。可以通过交换机面板图看出来，交换机每个口的 Link/Act，PoE 供电状态。点击具体的某个口，可以看到端口的详情，包括 VLAN 和 PoE 的配置信息，以及流量趋势，端口收发包情况。



4.13.1.2. DHCP 服务

显示控制器上的交换机中所有已启用 DHCP 服务的接口，并可以查看接口的 IP 地址分配情况。

交换机 DHCP 服务能够实现用户地址和配置信息的动态分配和集中管理，可以快速、动态地为用户分配和管理 IP 地址，保证 IP 地址的合理分配，提高 IP 地址使用效率。

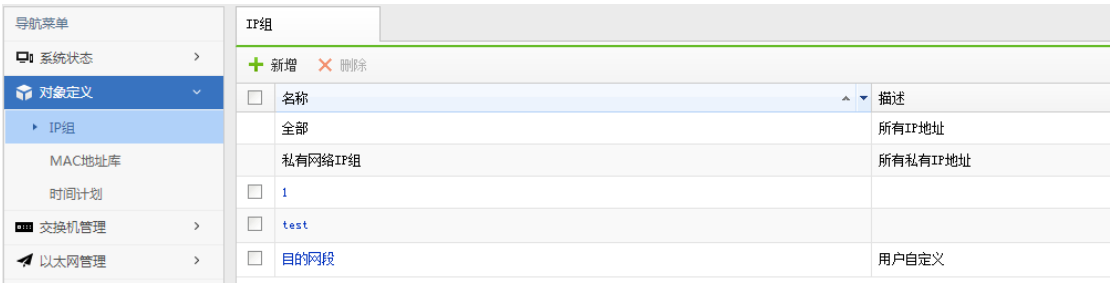


4.13.2. 对象定义

『对象定义』用于配置【IP 组】、【MAC 地址库】、【服务】、【应用】、【时间计划】、【智能 PSK 终端】、【URL 分类库】、【终端类型库】。这里定义的对象，在后续的模块中会使用到，比如 IP 组和服务会应用到访问控制策略中，MAC 地址库将在使用 MAC 地址认证时黑白名单调用。

4.13.2.1. IP 组

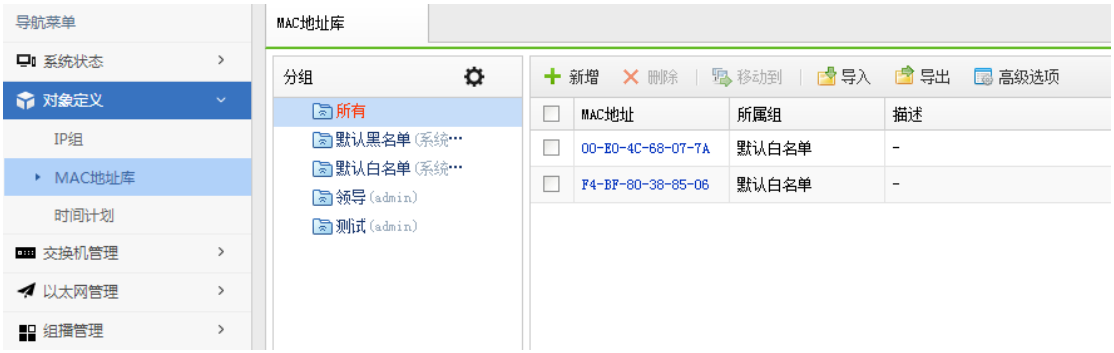
此页面可查看和新增 IP 组，IP 组用于后续【角色授权】中的【访问控制策略】，以及后续的【网络配置】中的【地址转换】。



4.13.2.2. MAC 地址库

将一个、多个 MAC 地址划分为一个 MAC 组，以便在系统的其它功能中调用，例如

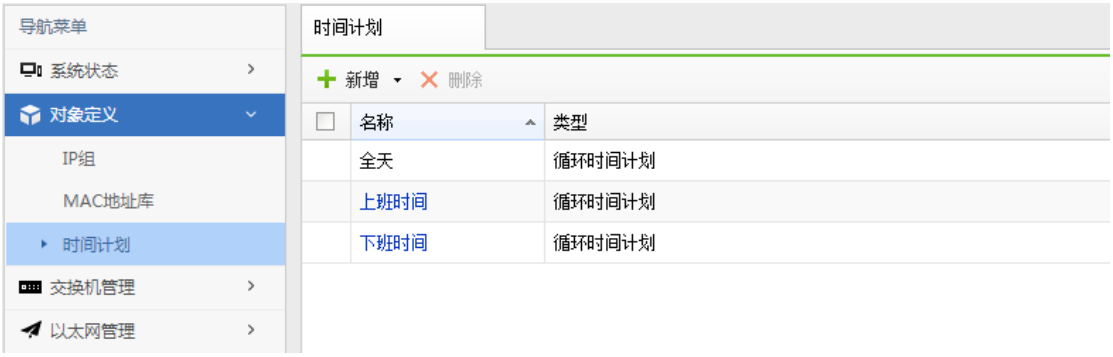
web 免认证。



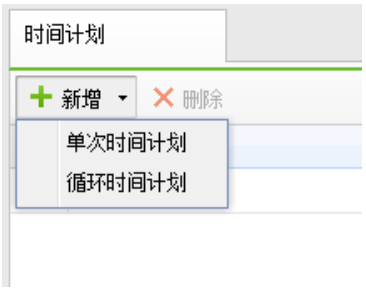
默认有默认黑名单和默认白名单两个分组，用户可以自定义分组。

4.13.2.3. 时间计划

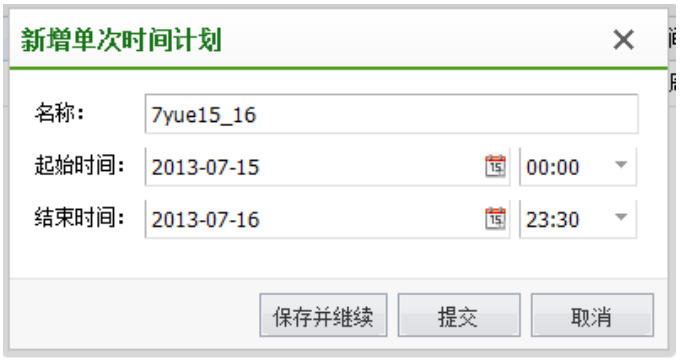
对于不同的无线或有线用户，我们需要在不同的时间段设置不同的访问控制策略以及流控策略，比如上班时间或下班时间，就需要配置时间计划，为了便于后续设置【认证授权】-【角色授权】-【访问控制策略】的生效时间，需要提前设置时间计划，『时间计划』分为【单次时间计划】和【循环时间计划】。



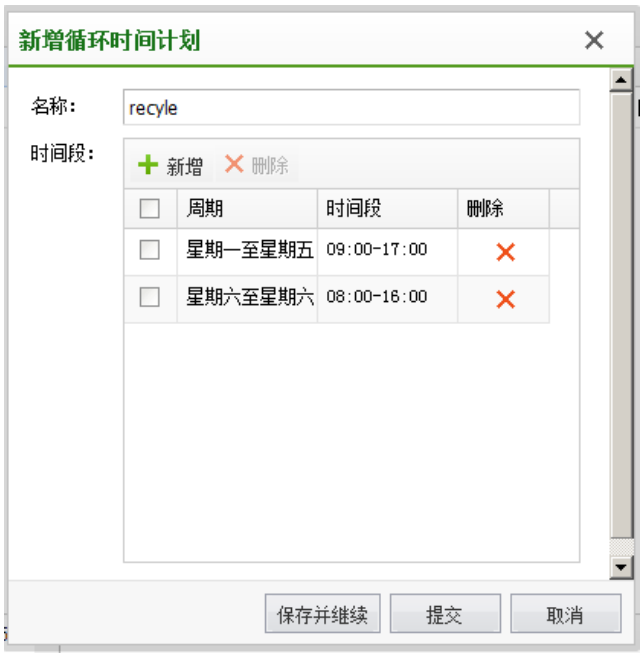
新增【单次时间计划】和【循环时间计划】:



设置循环时间时，大多数客户可以按照上班时间和下班时间，以及节假日方式设置循环时间，便与管理。



点击新增循环时间计划:



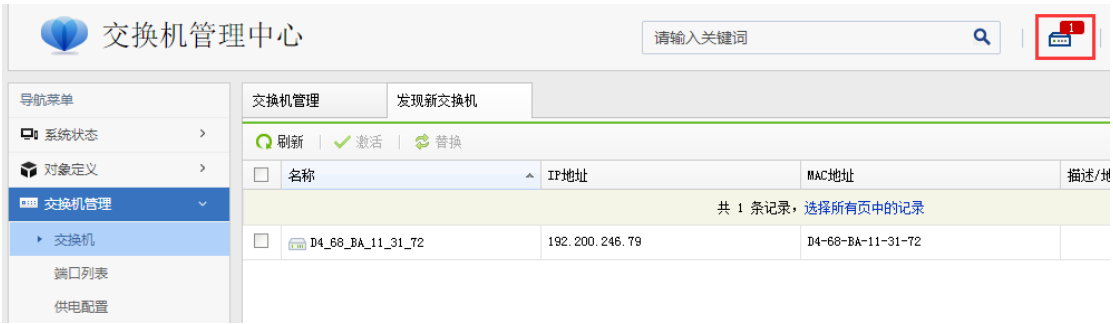
4.13.3. 交换机管理

『交换机管理』包含【交换机】、【端口列表】、【供电配置】三个功能模块。

4.13.3.1. 交换机

4.13.3.1.1. 发现新交换机

交换机的发现和激活和无线接入点方式类似，具体方法参照 4.5.4.1 章节。



为了让控制器统一管理交换机，当交换机接入内网时，并未进入工作状态，需要管理员在"发现新交换机"列表中，手动执行激活操作，交换机才能正常工作。

当交换机接入网络中，交换机会自动发现 NAC，当交换机第一次发现 NAC 时，会在 NAC 上看到新的交换机，需要进行激活后，才能正常使用交换机，并下发配置。

在 NAC 控制台的右上角，当有出现图标  时，表示还有未激活的交换机，需要到该页面激活。

当 NAC 上发现交换机时，需要激活，激活按钮可用。

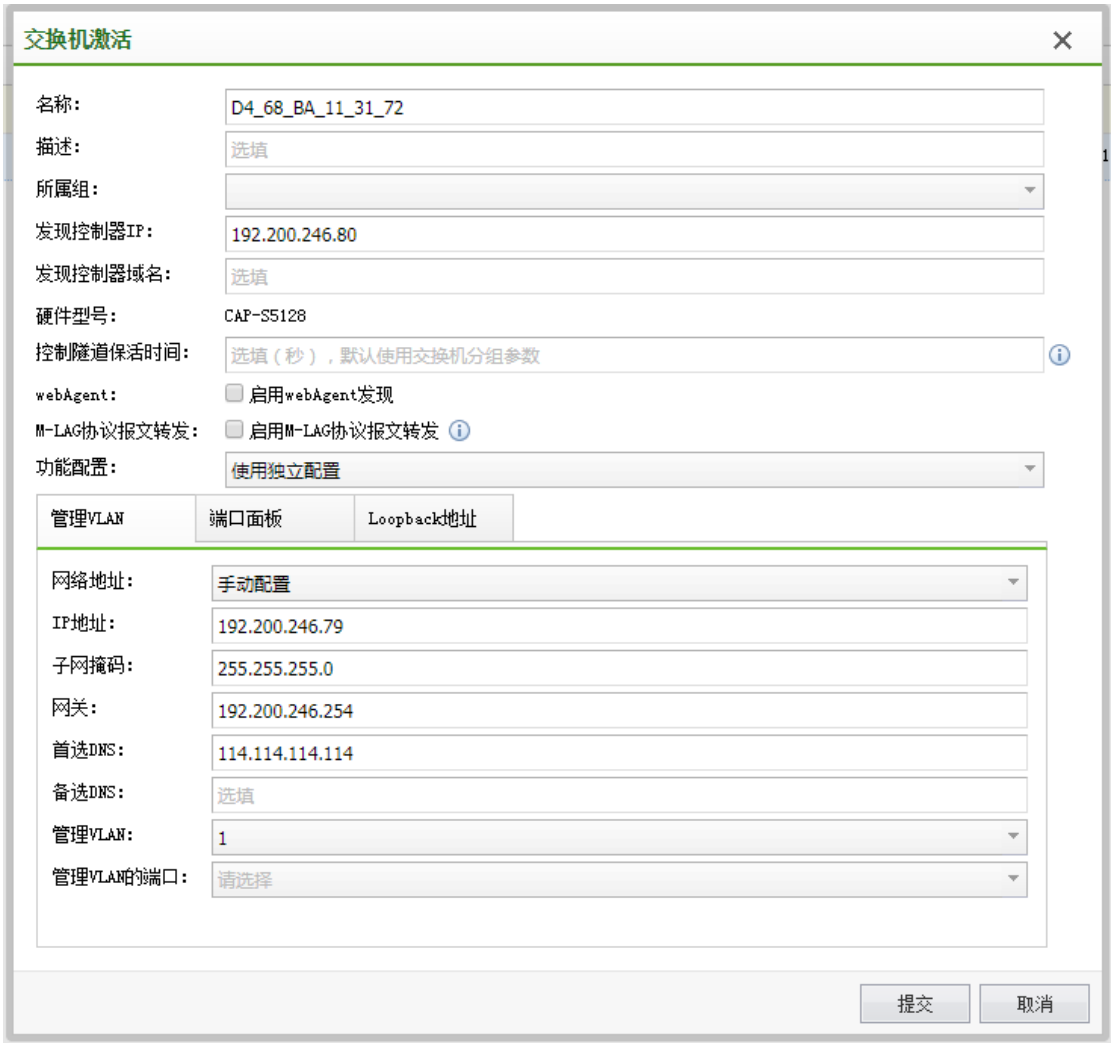
激活的时候，交换机只支持配置为普通模式，不支持网关模式。

交换机激活的时候，设备类型分为两种：

射频交换机：激活的时候，交换机端口会默认添加射频 AP，射频 AP 插到交换机端口上时，可以即插即用。

普通交换机（除射频交换机外）：激活的时候，序列号字段为选填，但只有填写了序列号，才能在无线接入点页面添加射频交换机配置，这样射频 AP 才能正常工作。

点击激活后，配置界面如下：



可以编辑交换机的名称，地理位置，便于后续交换机的识别分组和管理，默认交换机以其 MAC 地址为名称。

名称：编辑交换机名称，便于识别交换机。

描述：对交换机进行描述便于是被交换机。

所属组：配置交换机所属于的管理组，便于对交换机进行集中管理和配置。

发现控制器 IP：填写交换机用于连接的 NAC 的 IP 地址，如果给交换机填写了 NAC 的地址，交换机下次重启后，会自动以该配置 IP 连接 NAC 并建立隧道

发现控制器域名：用于交换机自动发现 NAC 用，当交换机解析到该域名时，交换机会自动向 NAC 请求连接。NAC 发现该交换机后，就可以对该交换机进行策略下发配置了。

硬件型号:交换机的型号

射频序列号：交换机序列号分为普通交换机序列号和射频交换机序列号。普通交换机序列号要添加射频交换机，需要给指定交换机开启序列号；射频交换机序列号给射频交换机专用，激活射频交换机没有超过序列号时，都会为射频交换机自动添加射频交换机，以达到即插即用的目的。

控制隧道保活时间：填写控制隧道保活时间，默认 12 秒，如果网络环境较差，可修改控制器隧道时间，降低交换机频繁上下线次数。

Webagent：发现控制器的一种方式，webagent 地址可联系 400 进行申请开通。

网络地址：可以设置自动获取，也可以设置固定 IP 地址。如果设置的固定 IP 地址，与当前交换机获取到的 IP 地址不一致，配置生效下发后，有可能会导致交换机不能在当前网络上网，并使交换机与 NAC 失去联系，所以一般设置交换机的 IP 地址为自动获取。

管理 VLAN 和管理端口:配置交换机的上联口以及管理 VLAN。管理 VLAN 是指要通过 SSH、TELNET 访问交换机，需要将使用的交换机端口添加到管理 VLAN。

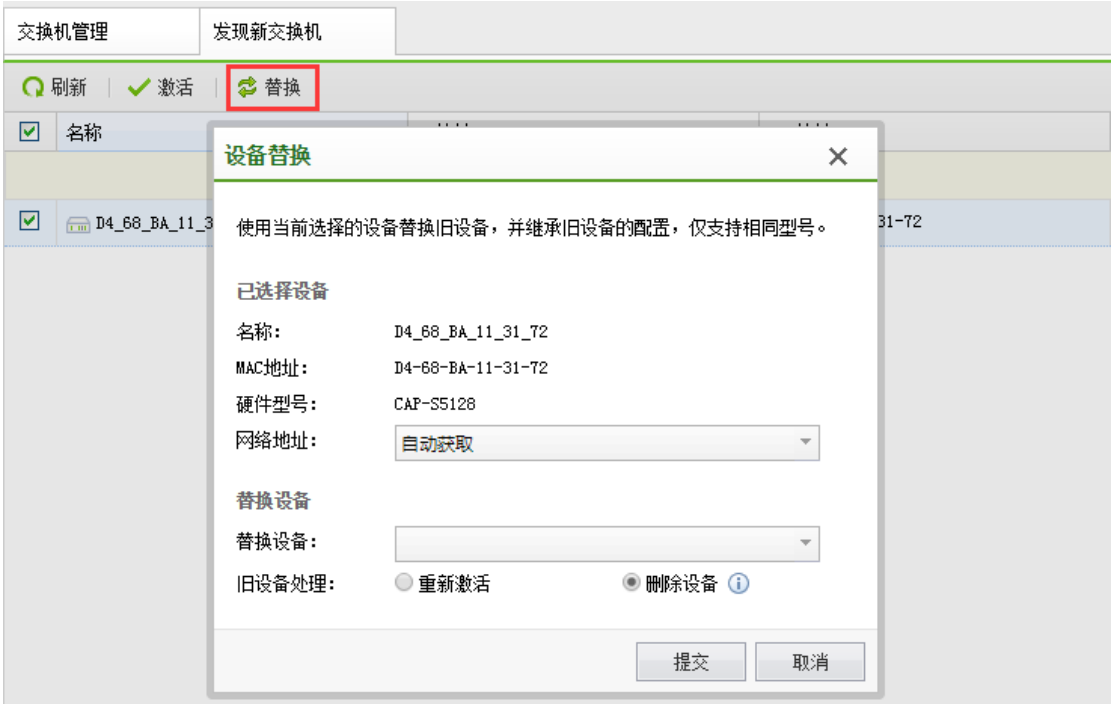
4.13.3.1.2. 设备替换

接入点和交换机均支持设备替换功能，设备替换分为两种操作：

交换机激活的时候，设备类型分为两种：

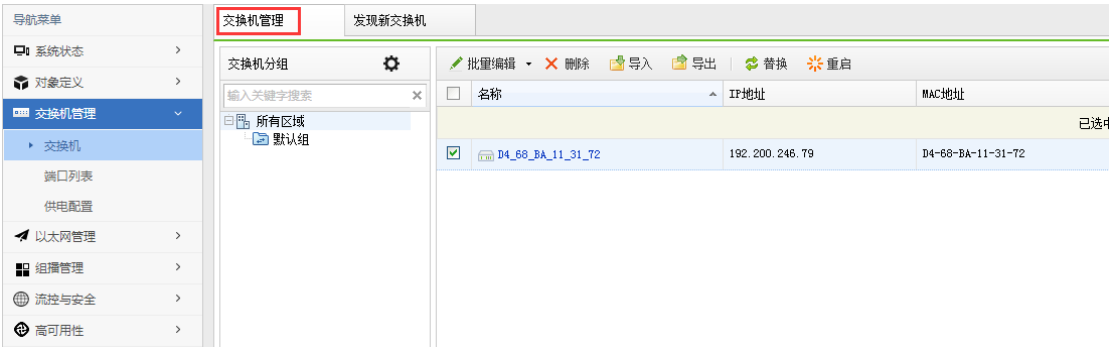
1. 发现新设备时，可以将要激活的设备替换为已经激活过的设备。替换时，可以选择将旧设备删除或是重新激活。

2．接入点管理或交换机管理页面，可以选择将两个设备的配置互相替换。



4.13.3.1.3. 交换机管理

对所有交换机进行全部集中分组和管理，包括配置管理 vlan、DNS 地址、静态路由等。



1、DNS 地址

如果启用了 DNS 代理，客户端的 DNS 服务器可以指向交换机。交换机接收到 DNS 请

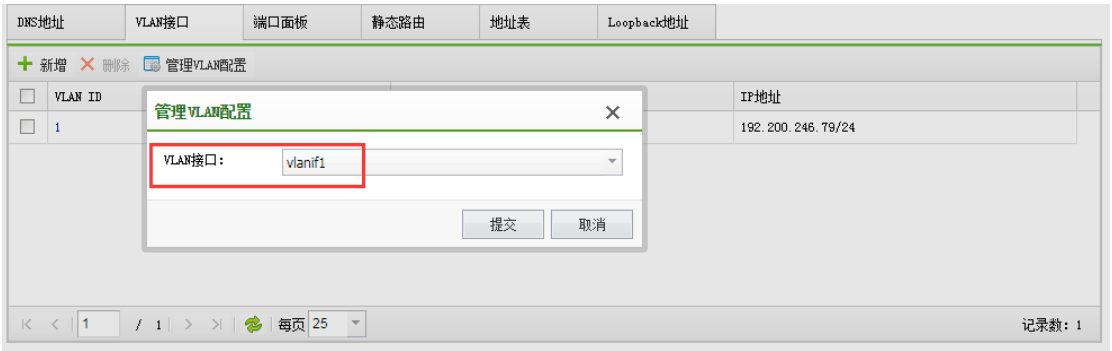
求后，会转发到这里设置的外部 DNS 服务器解析。

2、VLAN 接口

VLAN（Virtual Local Area Network）即虚拟局域网，是将一个物理的 LAN 在逻辑上划分成多个广播域的通信技术。VLAN 内的主机间可以直接通信，而 VLAN 间不能直接互通，从而将广播报文限制在一个 VLAN 内。

通过配置 VLANIF 接口、子接口方式可以实现 VLAN 间的通信。

管理 VLAN：配置交换机的上联口以及管理 VLAN 是指要通过 SSH、TELNET 访问交换机，需要将使用的交换机端口添加到管理 VLAN。



3、端口面板

可以单个或批量修改接口的 VLAN 属性、PoE 属性、流量控制、风暴抑制等配置；

4、静态路由

静态路由是一种需要管理员手工配置的特殊路由。当网络结构比较简单时，只需配置静态路由就可以使网络正常工作；在复杂网络环境中，配置静态路由可以改进网络的性能，并可为重要的应用保证带宽。

5、地址表

（1）配置静态 MAC 地址

设备通过源 MAC 地址学习自动建立 MAC 地址表时，无法区分合法用户和非法用户的报文，带来了安全隐患。为了提高安全性，网络管理员可手工在 MAC 地址表中加入特定 MAC 地址表项，将用户设备与接口绑定，从而防止非法用户骗取数据。

为了避免 MAC 地址表项爆炸式增长，可以手工配置动态 MAC 表项的老化时间。老化时间越短，路由器对周边的网络变化越敏感，适合在网络拓扑变化比较频繁的环境；老化时间越长，路由器对周边的网络变化越不敏感，适合在网络拓扑比较稳定的环境。

当需要配置的静态 MAC 表项较多，并且静态 MAC 表项中 MAC 地址与端口在同一二层环境时，可以采用自动扫描与绑定方式批量配置。

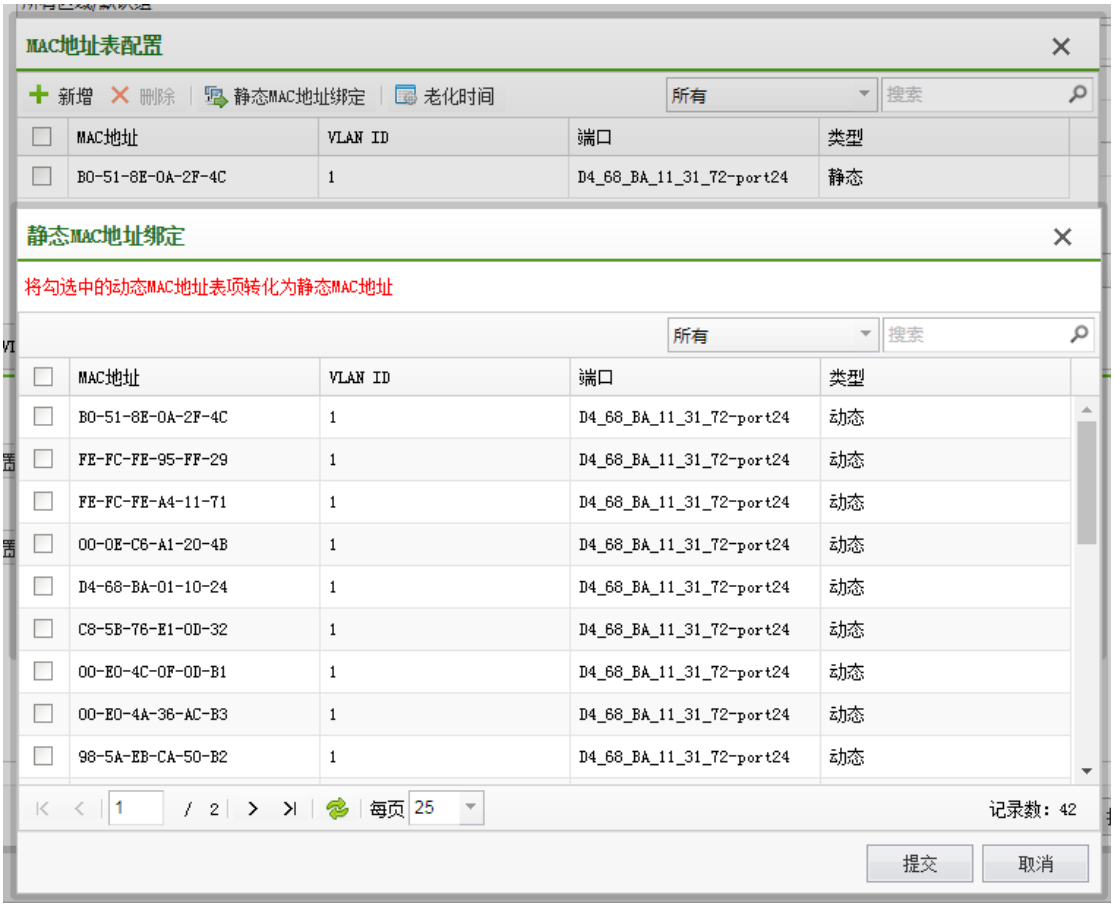
（2）配置静态 ARP 地址

静态 ARP 表项不会被老化，不会被动态 ARP 表项覆盖，因此配置静态 ARP 表项可以增加通信的安全性。

当老化时间超时后，设备会清除动态 ARP 表项。此时如果设备转发 IP 报文匹配不到对应的 ARP 表项，则会重新生成动态 ARP 表项，如此循环重复。

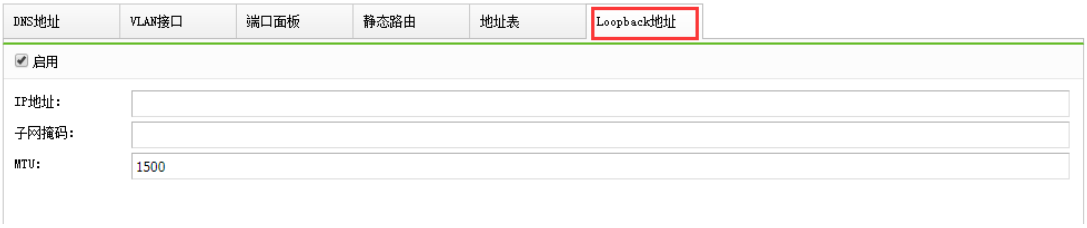
用户可以通过手工方式或者自动扫描与绑定的方式配置静态 ARP 表项：当需要配置的静态 ARP 表项较少时，可以采用手工方式新增或删除；当需要配置的静态 ARP 表项较多，并且静态 ARP 表项中 IP 地址与 VLANIF 接口的 IP 地址在同一网段时，可以采用自动扫描与绑定方式批量配置。


DNS地址
VLAN接口
端口面板
静态路由
地址表
Loopback地址
MAC地址表
MAC地址表配置
ARP地址表
ARP地址表配置


MAC地址表配置
新增
删除
静态MAC地址绑定
老化时间
所有
搜索
MAC地址
VLAN ID
端口
类型
B0-51-8E-0A-2F-4C
1
D4_68_BA_11_31_72-port24
静态
静态MAC地址绑定
将勾选中的动态MAC地址表项转化为静态MAC地址
FE-FC-FE-95-FF-29
FE-FC-FE-A4-11-71
00-0E-C6-A1-20-4B
D4-68-BA-01-10-24
C8-5B-76-E1-0D-32
00-E0-4C-0F-0D-B1
00-E0-4A-36-AC-B3
98-5A-EB-CA-50-B2
动态
每页
25
记录数：42
提交
取消

6、Loopback 地址

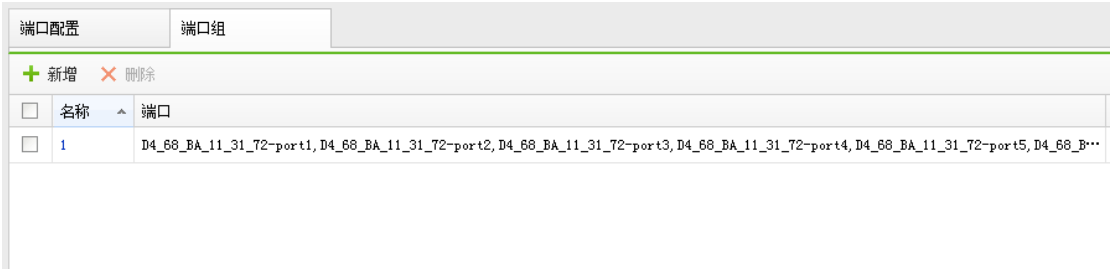
Loopback 接口创建后除非手工关闭该接口，否则 Loopback 接口物理层状态和链路层协议永远处于 UP 状态，用户可通过配置 Loopback 接口达到提高网络可靠性的目的。



4.13.3.2. 端口列表

激活在当前控制器（包括集中管理的分支）的交换机的所有端口列表，在此页面可以批量编辑所选端口的基本信息、PoE 属性、VLAN 属性，以达到方便管理操作的目的。

端口组实现为多个接口批量配置命令的功能，减少单独配置的输入错误，同时节省人力。

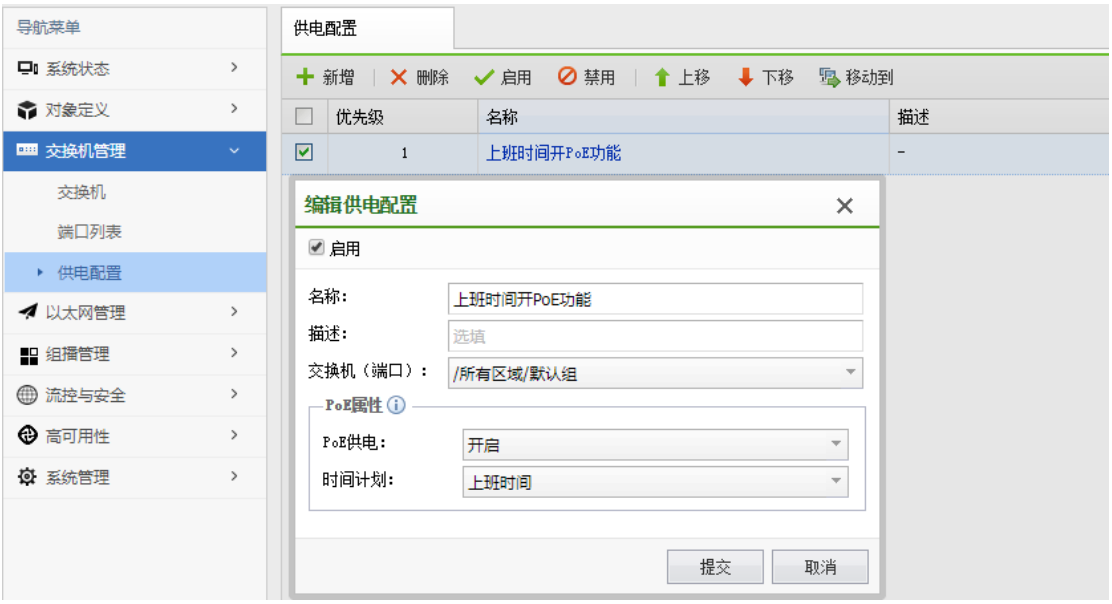


4.13.3.3. 供电配置

供电配置管理功能可以配置 PoE 交换机的供电属性，也可以配置时间计划给交换机的端口，以实现统一管理、科学省电的需求。

交换机和控制器断开一定时间之后（5 分钟），所有端口会保持供电状态。

未激活的 PoE 交换机，所有端口会保持供电状态。



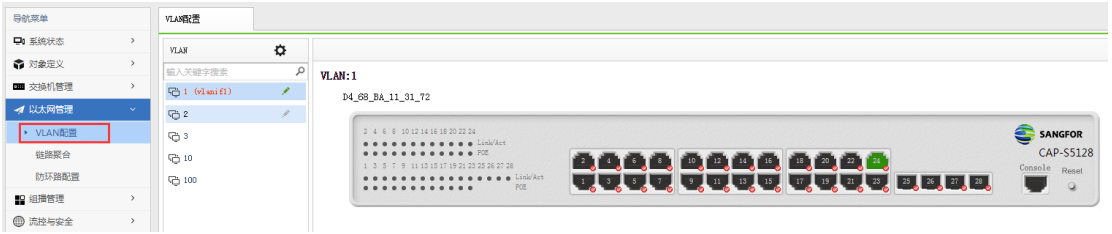
4.13.4. 以太网管理

『以太网管理』包含【VLAN 配置】、【链路聚合】、【防环路配置】三个功能模块。

4.13.4.1. VLAN 配置

以全局、统一的视图来管理交换机和控制器的 VLAN 配置。每个 VLAN 的视图中包括当前控制器以及分支的 VLAN-设备-端口三者的关系。功能适用于网络开局部署，统一规划 VLAN 配置，也适用于网络维护时，需要批量修改多台设备之间的 VLAN。

初始情况下，设备会默认添加 VLAN 1，交换机激活时，所有端口默认为 Access VLAN 1。

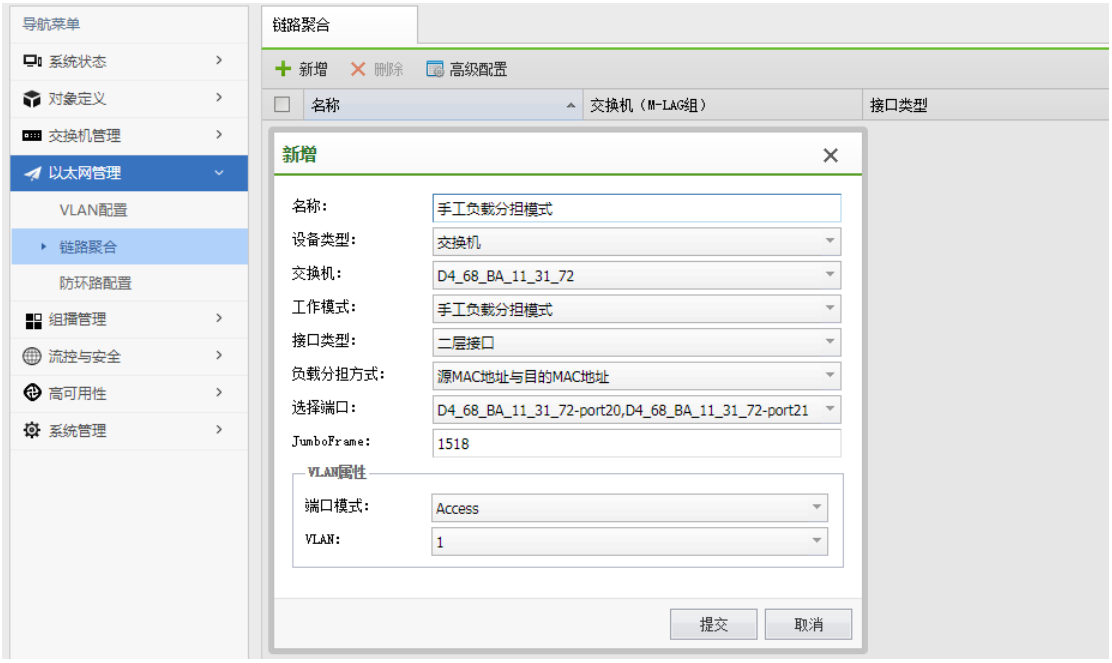


4.13.4.2. 链路聚合

链路聚合（Link Aggregation）是将多条物理链路捆绑在一起成为一条逻辑链路，从而实现增加带宽、提高可靠性、负载分担的目的。根据是否启用链路聚合控制协议 LACP，链路聚合分为手工负载分担模式和 LACP 模式。

手工负载分担模式链路聚合

手工负载分担模式下，Eth-Trunk 的建立、成员端口的加入由手工配置，没有链路聚合控制协议的参与。该模式下所有活动链路都参与数据的转发，平均分担流量，因此称为负载分担模式。



名称：编辑链路聚合策略名称。

工作模式：配置链路聚合的工作模式，链路聚合模式支持手工负载分担/LACP 静态模式。

接口类型：默认为二层接口，链路聚合支持二层接口聚合和三层接口聚合。

负载分担方式：选择负载分担方式。支持源 MAC 地址与目的 MAC 地址、源 MAC 地址、目的 MAC 地址。默认为源 MAC 地址与目的 MAC 地址。

选择端口：选择要做链路聚合的端口。

JumboFrame：默认为 1518，支持 1518~9192。

VLAN 属性：配置聚合口的 Access 模式或 Trunk 模式。

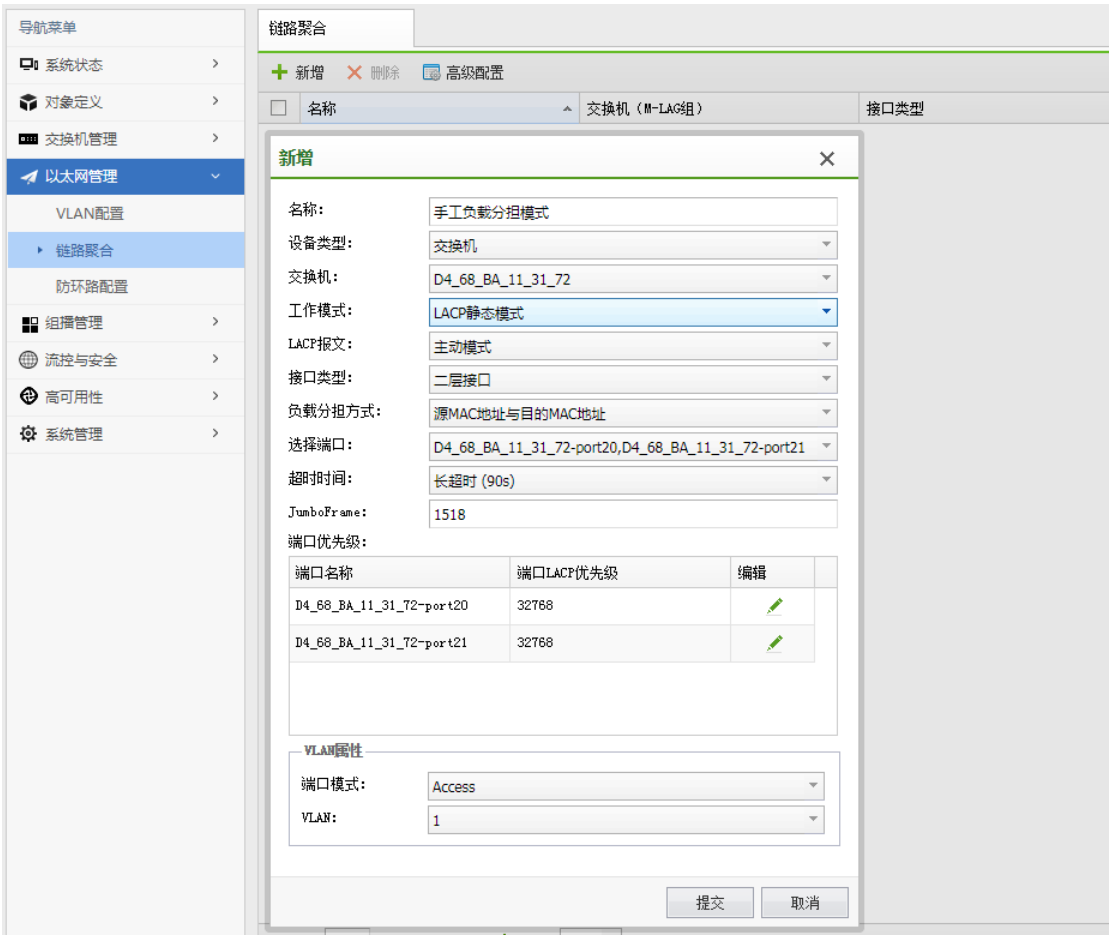

三层聚合口也可以配置 DHCP 服务，配置方法与三层物理口和 VLAN 接口配置方法一样，均需要将接口配置成静态 IP 地址才可以开启 DHCP 服务或配置 DHCP 中继。

LACP 模式链路聚合

作为链路聚合技术，手工负载分担模式 Eth-Trunk 可以完成多个物理端口聚合成一个 Eth-Trunk 口来提高带宽，同时能够检测到同一聚合组内的成员链路有断路等有限故障，但是无法检测到链路层故障、链路错连等故障。

为了提高 Eth-Trunk 的容错性，并且能提供备份功能，保证成员链路的高可靠性，出现了链路聚合控制协议 LACP（Link Aggregation Control Protocol），LACP 模式就是采用 LACP 的一种链路聚合模式。

LACP 为交换数据的设备提供一种标准的协商方式，以供设备根据自身配置自动形成聚合链路并启动聚合链路收发数据。聚合链路形成以后，LACP 负责维护链路状态，在聚合条件发生变化时，自动调整或解散链路聚合。



名称：编辑链路聚合策略名称。

工作模式：配置链路聚合的工作模式，链路聚合模式支持手工负载分担/LACP 静态模式。

LACP 报文：选择 LACP 报文支持的工作模式为：主动协商、被动协商。默认为主动协商。

接口类型：默认为二层接口，链路聚合支持二层接口聚合和三层接口聚合

负载分担方式：选择负载分担方式。支持源 MAC 地址与目的 MAC 地址、源 MAC 地址、目的 MAC 地址。默认为源 MAC 地址与目的 MAC 地址。

选择端口：选择要做链路聚合的端口。

超时时间：超过超时时间，没有收到 LACP 协议报文，聚合组就无法建立，默认 90 秒。

JumboFrame：默认为 1518，支持 1518~9192。

端口优先级：设置端口 LACP 优先级，默认为 32768。

VLAN 属性：配置聚合口的 Access 模式或 Trunk 模式。

三层聚合口也可以配置 DHCP 服务，配置方法与三层物理口和 VLAN 接口配置方法一样，均需要将接口配置成静态 IP 地址才可以开启 DHCP 服务或配置 DHCP 中继。

4.13.4.3. 防环路配置

以太网交换网络中为了进行链路备份，提高网络可靠性，通常会使用冗余链路。但是使用冗余链路会在交换网络上产生环路，引发广播风暴以及 MAC 地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为解决交换网络中的环路问题，提出了生成树协议 STP（Spanning Tree Protocol）。

与众多协议的发展过程一样，生成树协议也是随着网络的发展而不断更新的，从最初的 IEEE 802.1D 中定义的 STP 到 IEEE 802.1W 中定义的快速生成树协议 RSTP（Rapid Spanning Tree Protocol），再到最新的 IEEE 802.1S 中定义的多生成树协议 MSTP（Multiple Spanning Tree Protocol）。

在生成树协议中，MSTP 兼容 RSTP、STP，RSTP 兼容 STP。

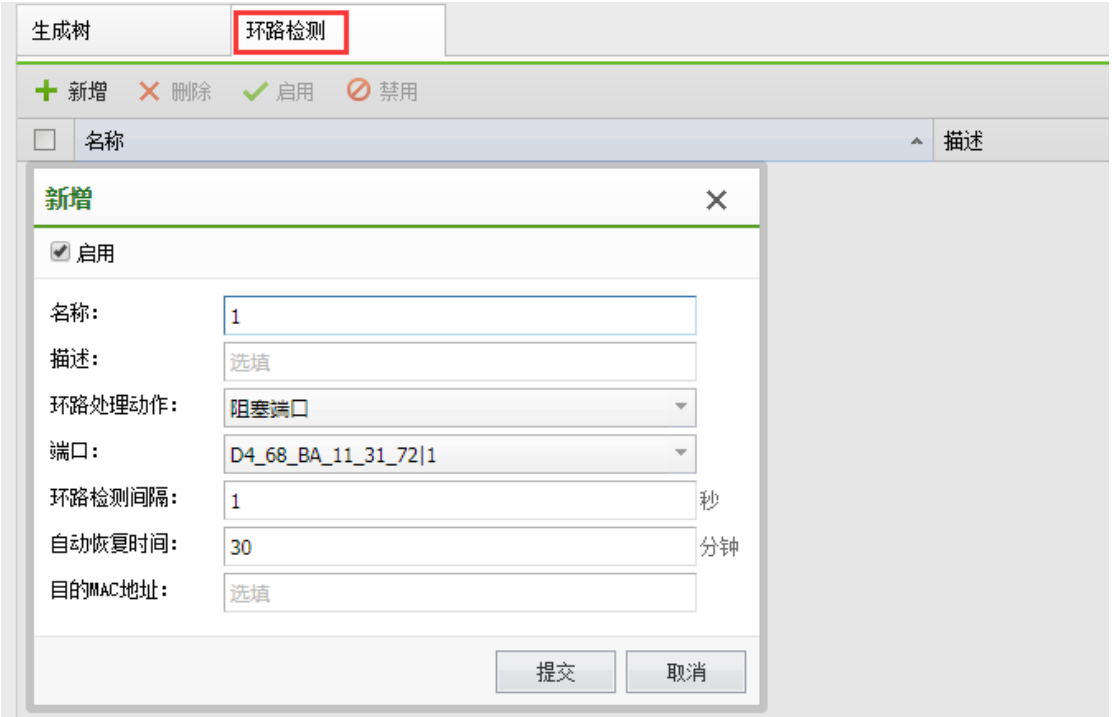
4.13.4.3.1. 生成树

简单模式下，支持一键启用所有交换机的防环路功能，如有部分设备不需要开启防环路，可在排除列表中设置。

高级模式下，可以在策略列表中添加需要开启防环路功能的交换机，更多防环路参数请在策略中配置。

4.13.4.3.2. 环路检测

环路检测机制可发现某个端口下的环路，并通知用户检查网络连接和配置情况，以避免对整个网络造成严重影响。



环路处理动作：环路处理动作是指发现二层网络中的环路以后所采取的处理方式，常用方式包括阻塞端口、关闭端口、退出环路 vlan。

环路检测间隔：环路检测间隔是环路检测报文的发送时间间隔，通过环路检测报文来确定各端口是否出现环路、以及存在环路的端口上是否已消除环路等。

自动恢复时间：当设备检测到某端口出现环路后，若在一定环路检测时间间隔内仍未收到环路检测报文，就认为该端口上的环路已消除，自动将该端口恢复为正常转发状态。

目的 MAC 地址：环路检测报文的目的 MAC 地址默认为广播地址，用户可根据实际需要进行配置。

4.13.5. 组播管理

IGMP Snooping 即组播侦听功能，可以实现组播数据在数据链路层的转发和控制。当主机和上游三层设备之间传递的 IGMP 协议报文通过二层组播设备时，IGMP Snooping 分析报

文携带的信息，根据这些信息建立和维护二层组播转发表，从而指导组播数据在数据链路层按需转发，减少二层网络中的广播报文，节约网络带宽，增强组播信息的安全性。

版本号

IGMPv1 主要基于查询和响应机制来完成对组播组成员的管理。与 IGMPv1 相比，IGMPv2 增加了查询器选举机制和离开组机制。IGMPv3 在兼容和继承 IGMPv1 和 IGMPv2 的基础上，进一步增强了主机的控制能力，并增强了查询和报告报文的功能。

查询间隔

查询间隔是指查询者发送普遍组查询报文之间的时间间隔。普遍组查询报文用于向与其连接的所有子网进行轮询来发现是否有组员存在。

健壮系数

查询器的健壮系数是为了弥补可能发生的网络丢包而设置的报文重传次数。

源 IP 地址

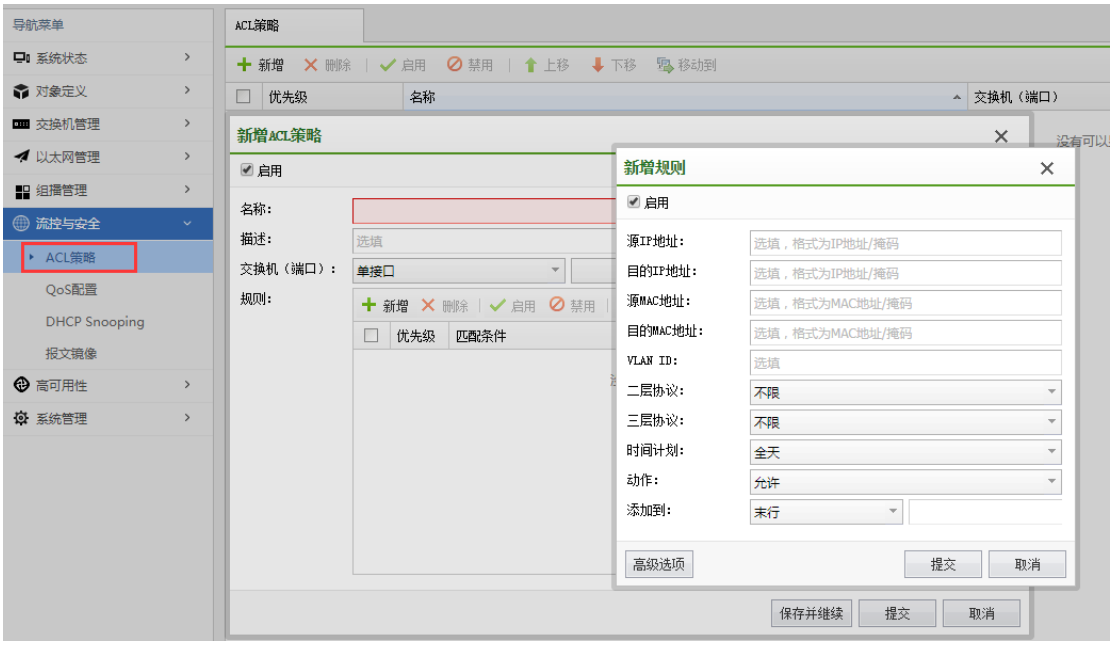
用户可根据实际需要配置查询器的源 IP 地址，从而建立数据链路层组播转发表项，进行组播数据转发。

4.13.6. 流控与安全

『流控与安全』包含【ACL 策略】、【QoS 配置】、【DHCP Snooping】、【报文镜像】四个功能模块。

4.13.6.1. ACL 策略

ACL（Access Control List）即访问控制列表，是一个有序的规则的集合，通过匹配报文中信息与规则中参数来对数据包进行分类，并执行规则对应的动作。



源/目的 IP 地址

支持使用以太网帧的源 IP 地址（地址段）或目的 IP 地址（地址段）来定义 ACL 规则。

源/目的 MAC 地址

支持使用以太网帧的源 MAC 地址或目的 MAC 地址来定义 ACL 规则。

VLAN ID

支持使用以太网帧的 VLAN ID 来定义 ACL 规则。

二层/三层协议

支持使用二层/三层网络协议来定义 ACL 规则，包括 ARP、RARP、ICMP、TCP、UDP、IGMP、IP、OSPF 等协议。

时间计划

时间计划是指 ACL 规则生效的时间段，表示仅在指定时间段内按该规则过滤。

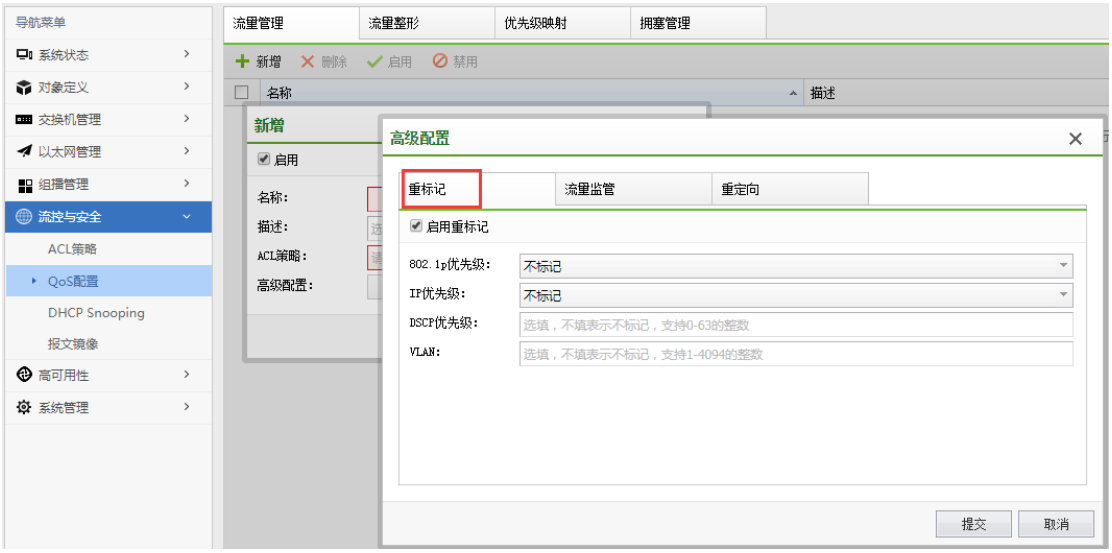
4.13.6.2. QoS 配置

QoS（Quality of Service）即服务质量，是指网络通信过程中，允许用户业务在丢包率、延迟、抖动和带宽等方面获得可预期的服务水平。

4.13.6.2.1. 流量管理

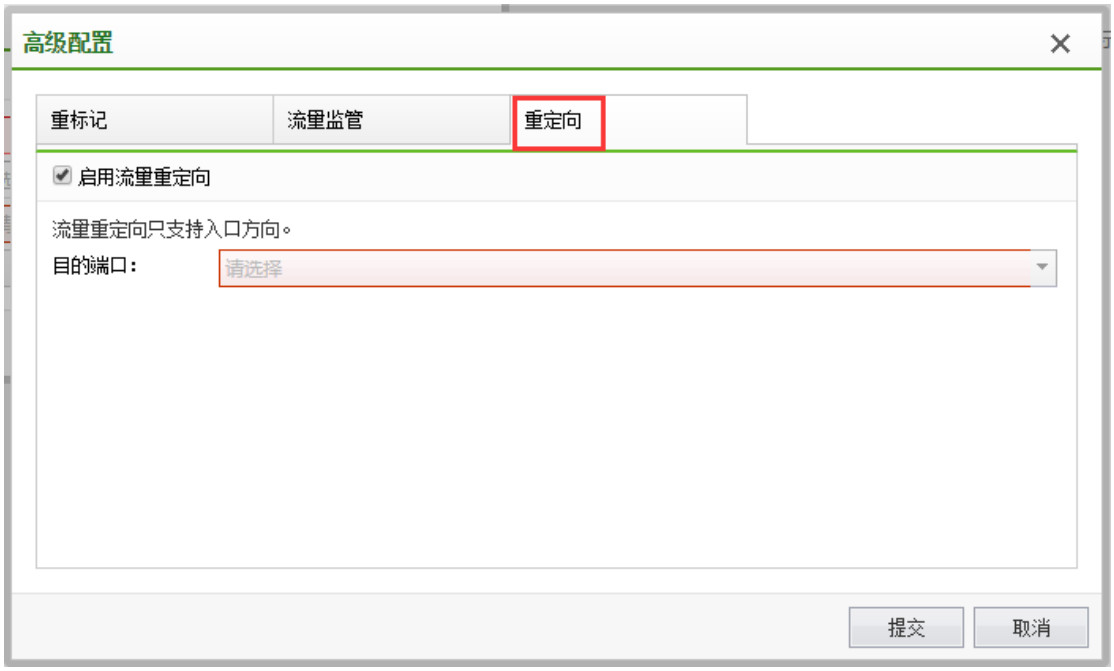
流量管理功能包括重标记、流量监管、重定向等。

重标记：通过设置报文的优先级或标志位，重新定义报文的优先级。



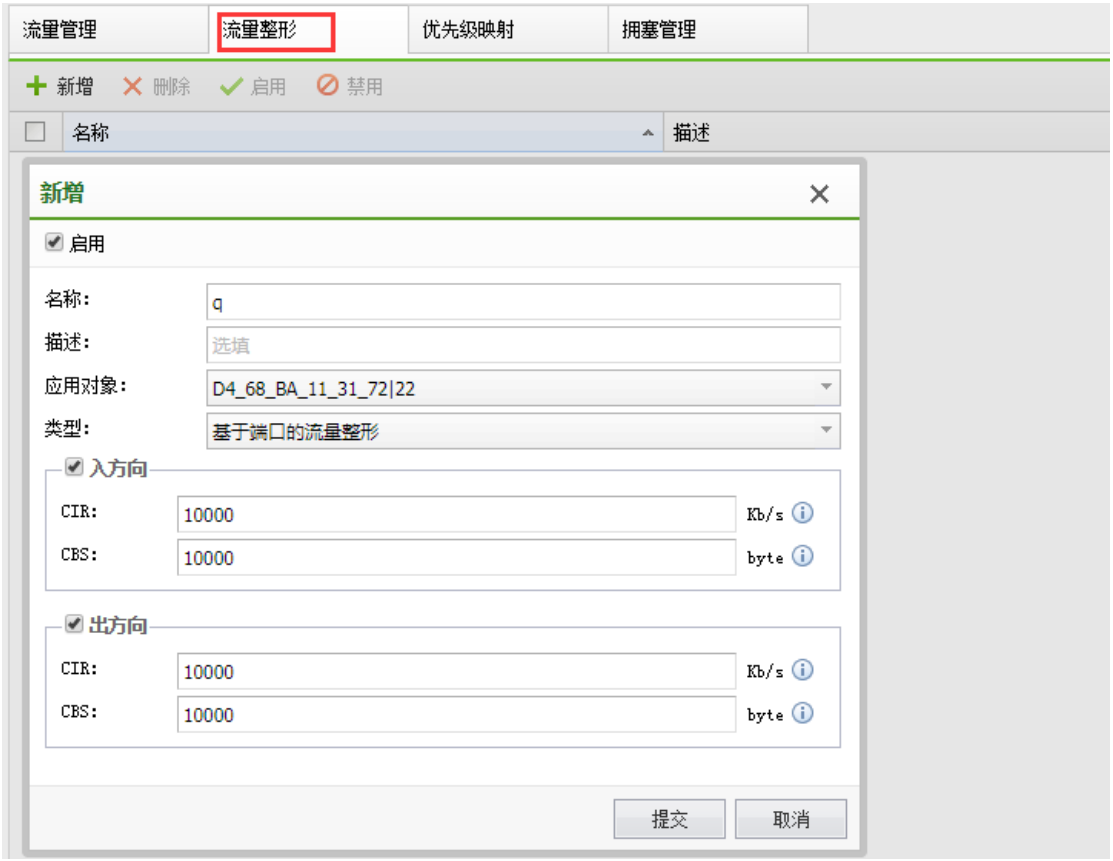
流量监管：通过监控进入网络的流量速率，将输入流量限制在一个合理范围内。

重定向：将符合流分类的报文流重定向到其他端口进行处理。



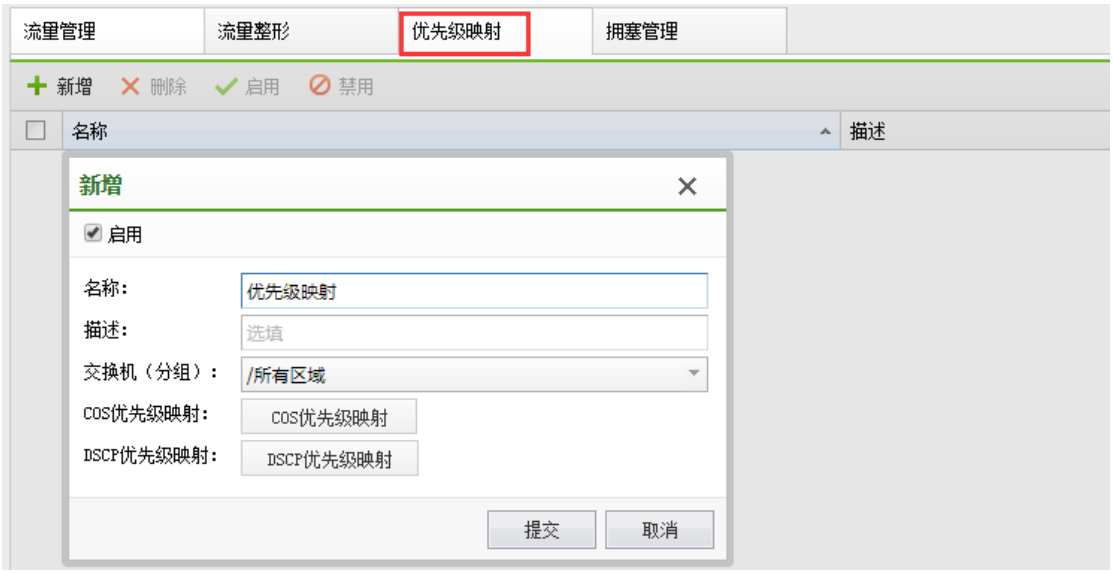
4.13.6.2.2. 流量整形

流量整形是一种主动调整流量输出速率的措施，对上游输入的不规整流量进行缓冲，使流量输出趋于平稳，从而解决下游设备的拥塞问题。



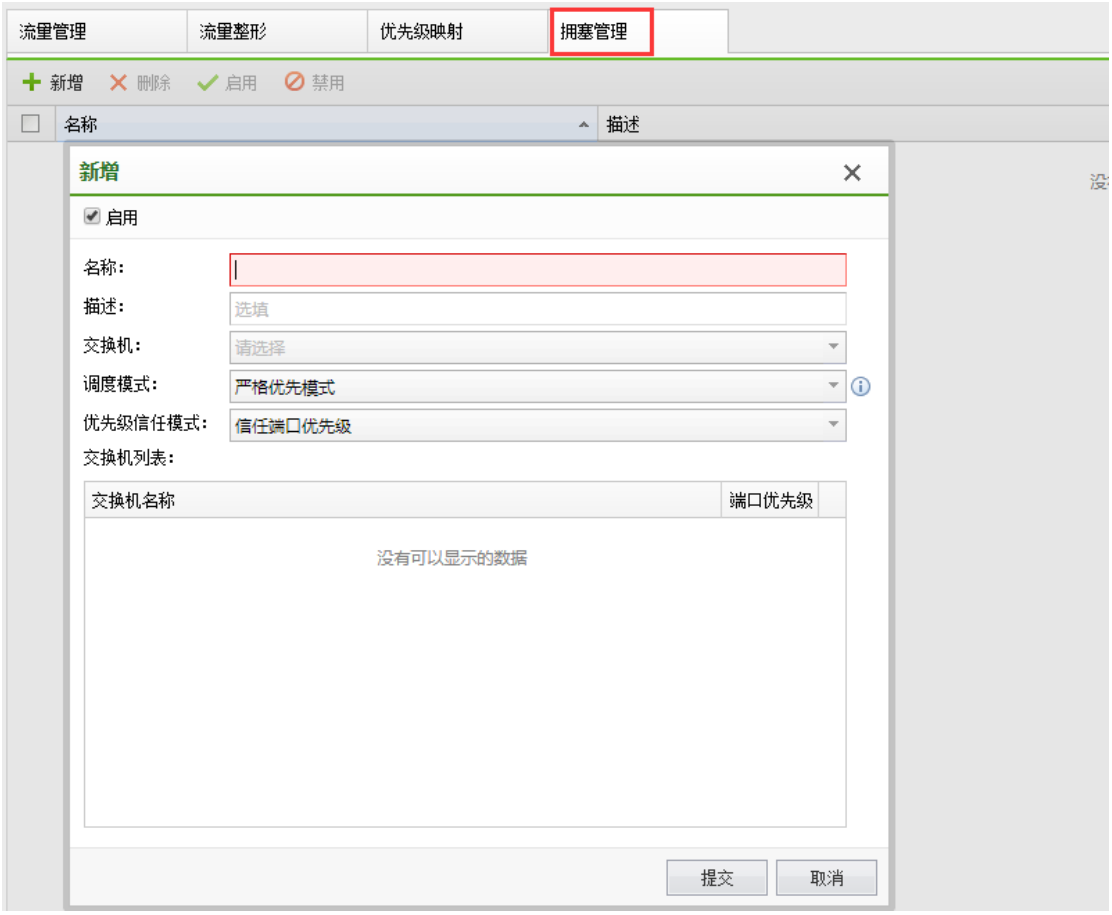
4.13.6.2.3. 优先级映射

优先级映射实现从 COS 优先级到 DSCP 优先级之间的映射，设备可根据优先级提供有差别的 QoS 服务。



4.13.6.2.4. 拥塞管理

当时延敏感业务要求得到比非时延敏感业务更高质量的 QoS 服务，且网络中间歇性的出现拥塞，此时需要进行拥塞管理。拥塞管理一般采用排队技术，使用不同的调度算法来发送队列中的报文流。常用调度模式包括严格优先模式、轮询模式、加权轮询模式、严格优先+加权轮询模式和差分加权轮询模式。



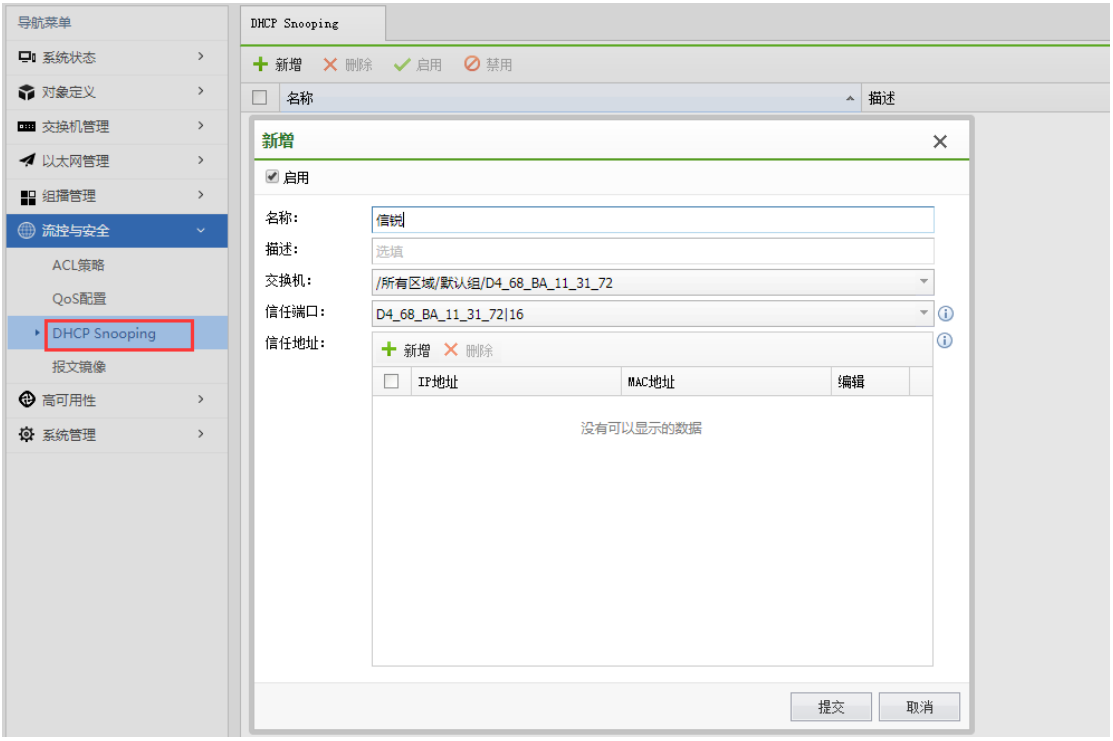
常用优先级信任模式包括信任报文优先级和信任端口优先级。信任报文优先级是指直接根据报文携带的报文优先级来转发数据，信任端口优先级分两种情况：

1.当入口报文不带 802.1p 优先级，设备将使用端口优先级，根据此优先级查找 802.1p 优先级到内部优先级映射表，然后为报文标记内部优先级。

2.当入口报文携带 802.1p 优先级，此时按报文携带的 802.1p 优先级，查找 802.1p 优先级到内部优先级映射表，然后为报文标记内部优先级。

4.13.6.3. DHCP Snooping

DHCP Snooping 是 DHCP 的一种安全特性，用于保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址，防止网络上针对 DHCP 攻击。



信任端口

信任端口正常转发接收到的 DHCP 应答报文，非信任端口在接收到 DHCP 服务器响应的 DHCP Ack、DHCP Nak、DHCP Offer 和 DHCP Decline 报文后，丢弃该报文。

信任地址

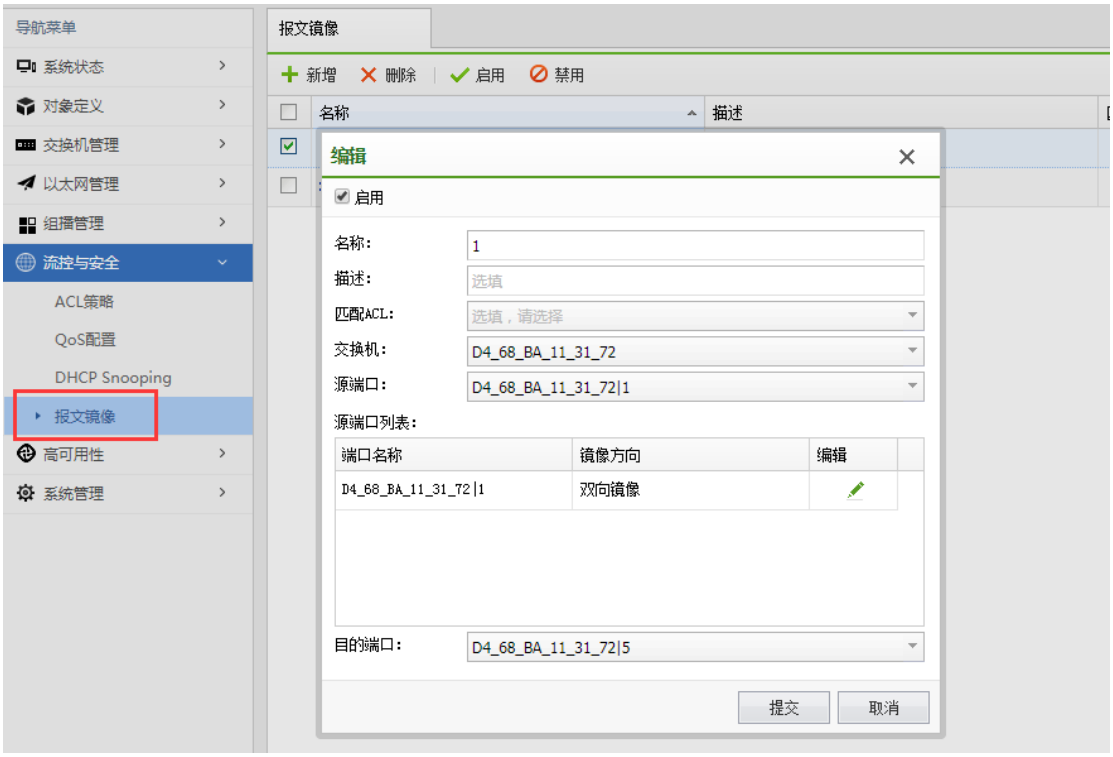
信任 IP 地址是指当 DHCP 响应报文的源 IP 地址与配置项相匹配时，允许报文通过。

信任 MAC 地址是指当 DHCP 响应报文的源 MAC 地址与配置项相匹配时，允许报文通过

信任 IP+MAC 地址是指当 DHCP 响应报文的源 MAC 地址和源 IP 地址与配置项完全匹配时，允许报文通过。

4.13.6.4. DHCP Snooping

网络运行过程中，经常需要对网络设备的端口状况进行监控和分析。如果直接对转发端口进行监控和分析，可能会影响端口的转发效率。用户可以通过配置镜像功能，将网络中某个接口（镜像端口）接收或发送的报文，复制一份到指定接口（观测端口），然后发送到和观测端口直连的报文分析设备上。用户通过分析镜像报文，可进行网络监控和故障排查。



端口镜像

指将镜像端口接收或发送的报文完整地复制输出到指定的观测端口。

匹配 ACL 的流镜像

匹配 ACL 的流镜像：指将镜像与匹配 ACL 相结合，只复制满足特定条件的报文，过滤报文分析设备不关心的报文，为报文分析提供更精细的控制，提高报文分析设备的工作效率。

源端口

源端口是镜像端口，即报文流经的端口。

目的端口

目的端口是观察端口，即报文重新发送至的指定端口。

4.13.7. 高可用性

『高可用性』包含【链路高可用性】、【M-LAG 组】二个功能模块。

4.13.7.1. 链路高可用性

4.13.7.1.1. 备份链路

备份链路，又叫做灵活链路。一个备份链路由两个端口组成，其中一个端口作为另一个的备份。备份链路常用于双上行组网，提供可靠高效的备份和快速的切换机制。

主用链路和备用链路

备份链路组中处于转发状态的链路称为主用链路，处于阻塞状态的链路称为备用链路。

主端口和从端口

备份链路组的主用和备用链路在特定的设备上体现为端口或者聚合组端口，此处统称为端口。为了区分备份链路组中的两个端口，将两个端口分别命名为主端口和从端口。备份链路组中的从接口在备份链路组启动后会被阻塞。

FLUSH 报文

端口切换之后，备份链路通过发送 FLUSH 报文通知其他设备进行地址刷新，且相关设备必须使能 Flush 报文接收功能。但是，由于该技术为私有技术，目前只限于我司的交换机、华为、华三的设备能够识别该报文。对于不识别 FLUSH 报文的设备，只能通过流量触发 MAC 地址的更新。

抢占配置

抢占配置方式选择立即抢占，即备份链路组中主链路出现故障并倒换到从链路后，当原主链路故障恢复后，立刻进行备份链路倒换。抢占配置选择延时抢占，即等待延时时间到达后，根据备份链路组的接口最后获得的 Up/Down 状态处理备份链路组的状态。抢占配置方式选择不抢占，即为了保持流量稳定，原有的主用链路将维持在阻塞状态，不进行抢占。

4.13.7.1.2. 上行链路监控

上行链路监控是一种端口联动方案，它能通过监控设备的上行端口，根据其 UP/DOWN 状态的变化来触发下行端口 UP/DOWN 状态的变化，从而触发下游设备上的拓扑协议进行链路的切换。

上行接口

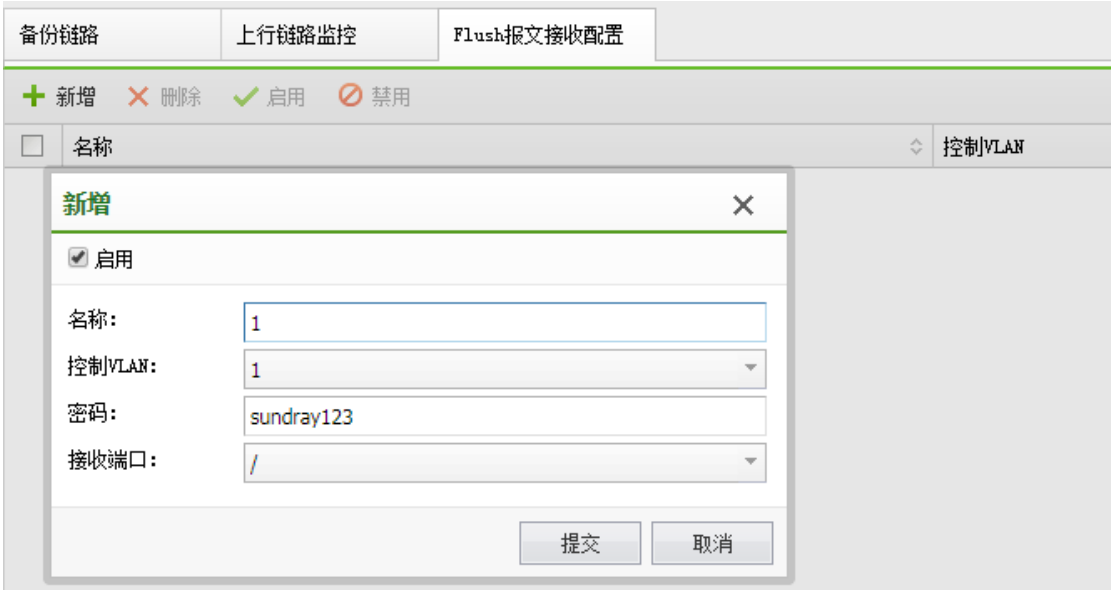
上行接口是上行链路监控组中的被监控的端口，上行链路监控组的上行接口可以是以太网端口（电口或光口）、聚合口或备份链路组。

下行接口

下行接口是上行链路监控组中的监控端口，上行链路监控组的下行接口可以是以太网端口（电口或光口）或聚合口。

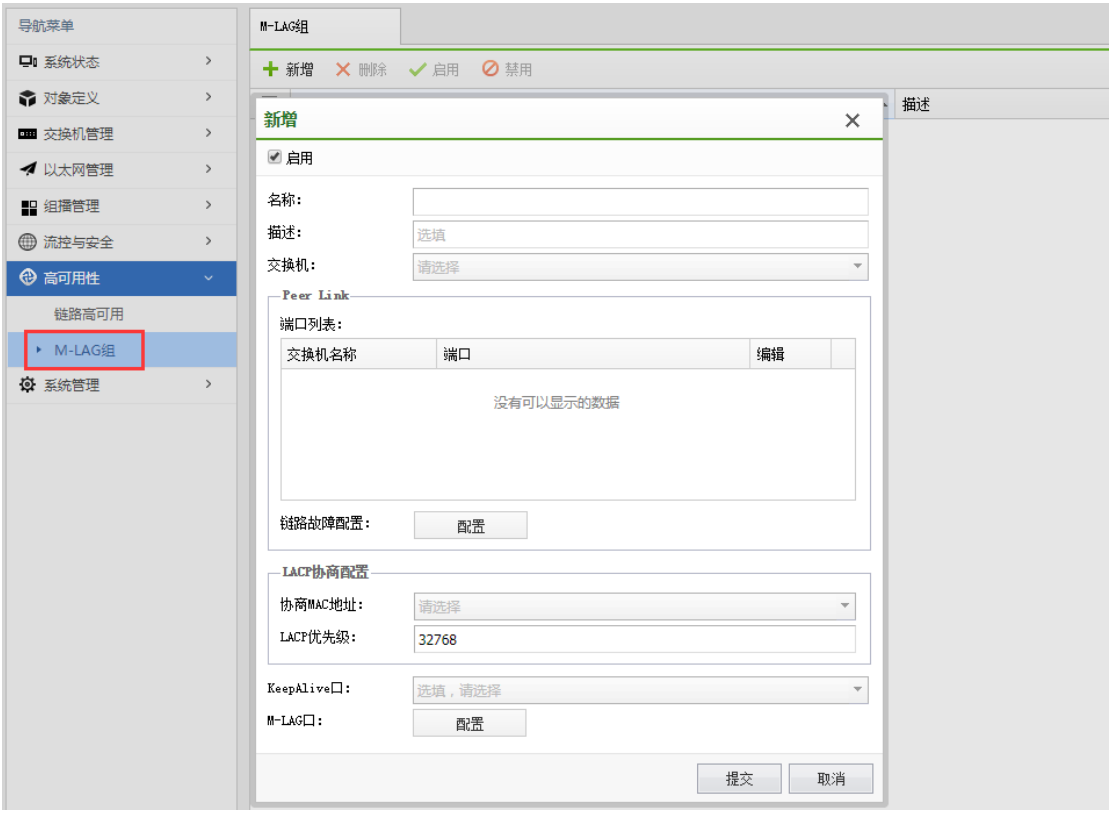
4.13.7.1.3. Flush 报文接收配置

支持独立配置 Flush 报文接收功能，并配置接口接收 Flush 报文的加密方式、接收控制 VLAN ID 和密码。当上游设备收到 Flush 报文时，判断该 Flush 报文的发送控制 VLAN 是否在收到报文的接口配置的接收控制 VLAN 列表中。如果不在接收控制 VLAN 列表中，设备对该 Flush 报文不做处理，直接转发；如果在接收控制 VLAN 列表中，设备会处理收到 Flush 报文，进而执行 MAC 地址转发表项和 ARP 表项的刷新操作。



4.13.7.2. M-LAG 组

M-LAG（Multichassis Link Aggregation Group）即跨设备链路聚合组，是一种实现跨设备链路聚合的机制，将一台设备与另外两台设备进行跨设备链路聚合，从而把链路可靠性从单板级提高到了设备级，组成双活系统。



Peer Link 口

Peer Link 链路两端直连的接口均为 Peer Link 接口，支持配置光口，电口，聚合口。

链路故障配置

Peer Link 链路是一条直连链路，用于交换协商报文及传输部分流量，保证 M-LAG 的正常工作。Peer Link 故障但心跳状态正常会导致备设备上除管理网口、peer-link 接口以及自定义的排除端口以外的物理接口处于 DOWN 状态，此时双归场景变为单归场景。一旦配置 Peer Link 链路故障恢复，处于 DOWN 状态的物理接口默认将在 120 秒时间自动恢复为 Up 状态。

LACP 协商配置

部署 M-LAG 的两台设备与用户侧设备之间的链路已经分别配置为聚合链路。为了提高

可靠性，建议将链路聚合模式配置为 LACP 模式。用户需确定协商 MAC 地址和 LACP 优先级以方便进行 LACP 协商配置，用来适用于 LACP 模式的 Eth-Trunk 组成的 M-LAG。

KeepAlive 口

KeepAlive 链路是一条三层互通链路，用于 M-LAG 主备设备间发送双主检测报文。

正常情况下，双主检测链路不会参与 M-LAG 的任何转发行为，只在故障场景下，用于检查是否出现双主的情况。用于检测对端的选举状态是否正常。

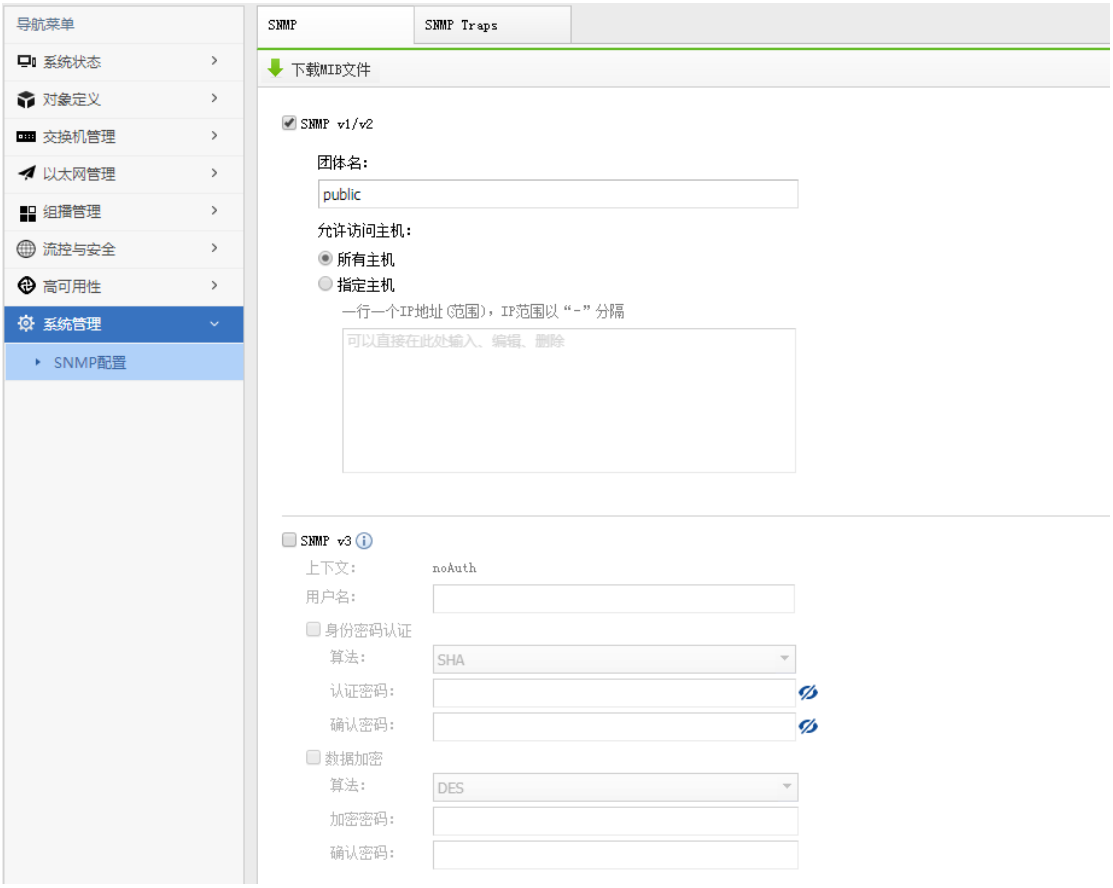
M-LAG 口

M-LAG 口是 M-LAG 主备设备上连接上下行设备的 Eth-Trunk 接口。加入同一 M-LAG 口的接口，对外表现为同一个聚合接口。

4.13.8. 系统管理

4.13.8.1. SNMP 配置

SNMP(Simple Network Management Protocol,简单网络管理协议)，用于管理网络中上众多的软硬件平台。开启后可以通过 snmp 协议查询本设备系统信息，如设备型号，内存使用，硬盘使用率，cpu 消耗等。



SNMP v1/v2

SNMP 的第一版本和第二版本。它们都是基于团体名进行报文认证。

SNMP v3

SNMP 的第三版本。此版本提供重要的安全性功能，其中就包括了认证和加密两项。认证需要提供认证方式（MD5，SHA）和认证密码。加密需要提供加密方式（DES）和加密密钥。

MIB

MIB（Management Information Base，管理信息库），是由网络管理协议访问的管理对象数据库，也可理解为是所有可管理对象的集合。下载本设备 MIB 后，再导入到相应的管理

端后，可以管理或查询的本设备的一些基本信息，如设备信号，内存使用，硬盘使用，CPU 消耗等。

SNMP Traps

SNMP Trap 又称 SNMP 陷阱，启用后可以让本设备主动发送信息到管理端，而不需要等到的管理端轮询后再发送。需要配置管理端的 IP 地址和端口，以及团体名。支持向多个管理端发送信息。

4.14. 数据分析平台

『数据分析平台』即以前的“营销中心”功能，包含了【数据分析】、【数据分析管理】、【终端监视】三个大的功能菜单，其中【数据分析】包含了【行业画像】、【热点地图】、【全屏列表】、【人流量统计】、【搜索分析】、【推广统计】、【对比分析】、【天气画像】、【访客画像】、【访客信息】、【广播状态】共 11 个子菜单；【数据分析管理】 包含了【区域管理】、【身份管理】、【认证页面】、【推广任务】、【推广模板】、【推广规则】、【无线广播】、【标签与关键字】、【工作日历】、【天气信息配置】共 10 个子菜单；【终端监视】包含了【监视策略】、【终端数据库】、【自动签到】共三个子菜单。

4.14.1. 数据分析

4.14.1.1. 行业画像

4.14.1.1.1. 行业画像

行业画像是对账号认证的用户所产生的上网数据进行分析与展示，并可以导出数据分析的结果报表，点击图表可以查看详细的图表数据。根区域及子区域在 数据分析管理->区域管理->分支区域 配置。

支持导出子区域的数据分析报表。

名词解释：

- 接入用户数：接入的用户总数
- 互访交流：子区域之间，人员的流动情况
- 考勤数据：到岗率、准点率、在岗时长
- 气候环境：按照天气统计考勤数据->到岗率、准点率、在岗时长
- 热点区域：各个子区域的用户接入次数
- 应用使用时长：应用的使用时长累计情况
- 位置驻留时长：在某位置，各子区域人员的累计驻留情况
- 环比：当前所选时间范围与上一期对应时间范围的数据变化对比的趋势(上升/下降)。如果上一期没有数据或者数据为 0，且本期数据对比上一期的数据有所上升，环比值显示为“-”

子区域

点击子区域可以查看子区域的上网数据分析情况，支持导出子区域的数据分析报表。点击考勤日历中的某一天，可以查看当天人员的到岗情况。

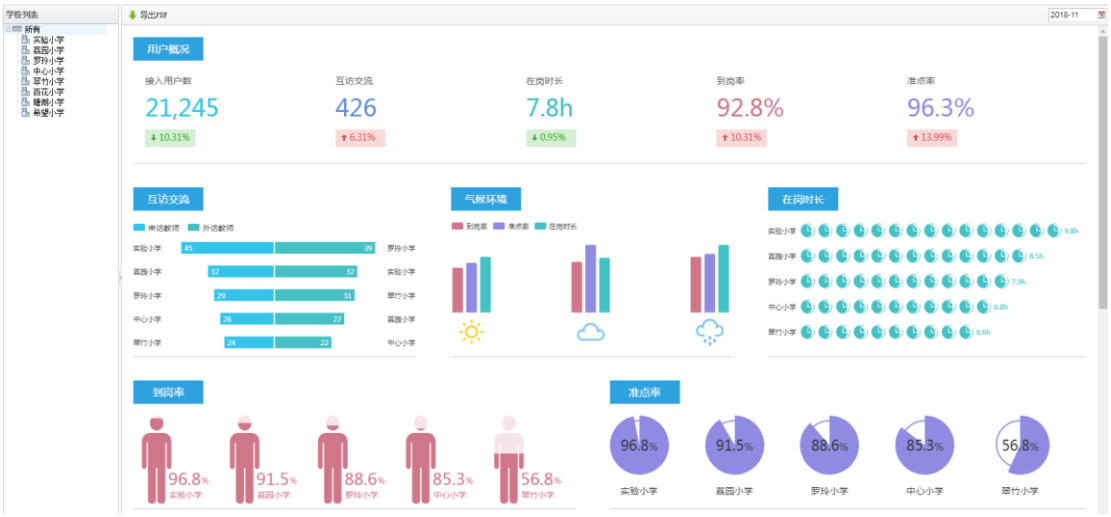


图 1

场景说明：

领导想要知道员工到岗在岗，工作时的投入程度，方便对员工评优升职；并且希望可以知道各分支，各部门的在职数据（如图 1）。

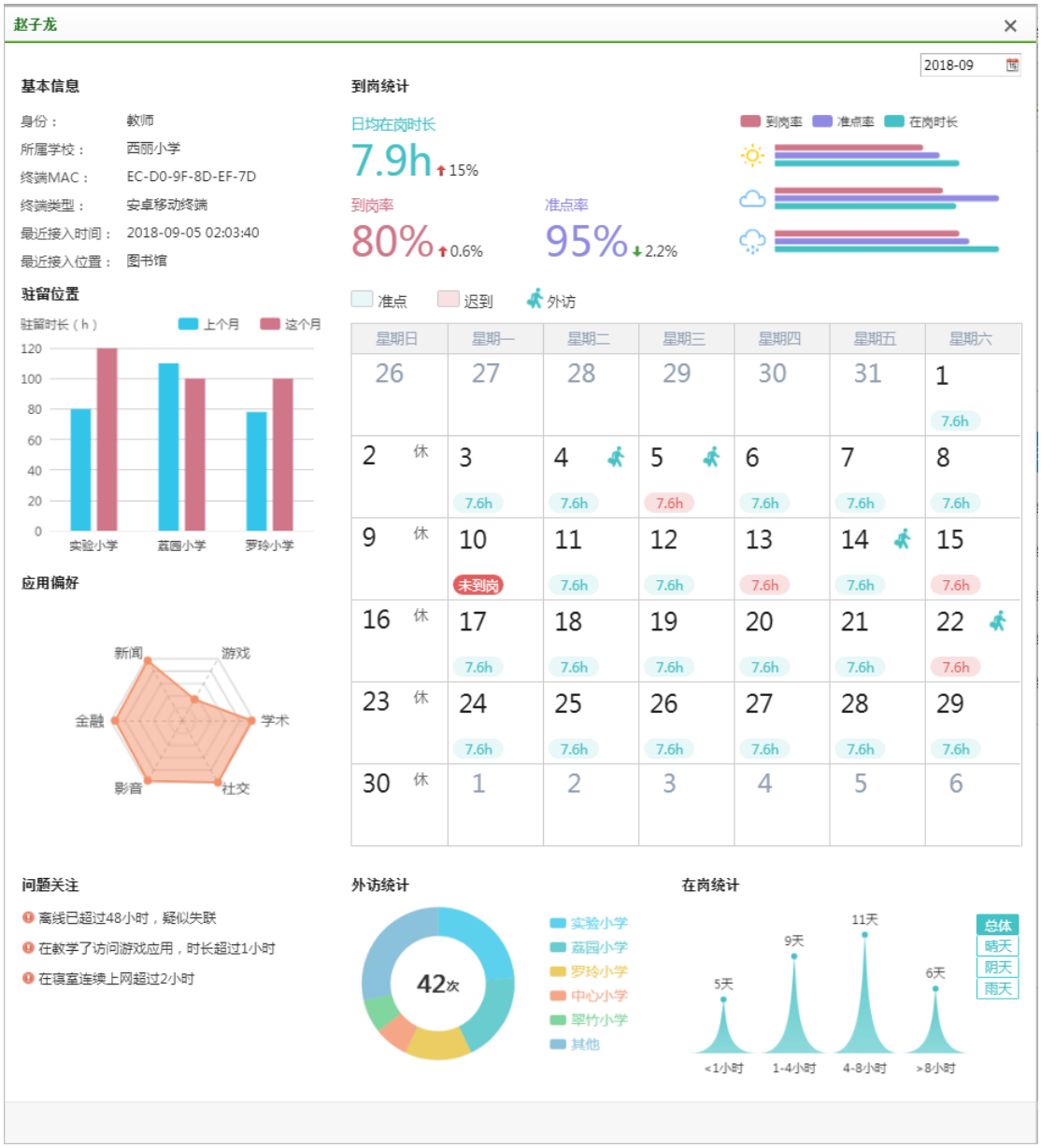

赵子龙
2018-09
基本信息
身份： 教师
所属学校： 西丽小学
终端MAC： EC-D0-9F-8D-EF-7D
终端类型： 安卓移动终端
最近接入时间： 2018-09-05 02:03:40
最近接入位置： 图书馆
驻留位置
驻留时长（h）
上个月
这个月
实验小学
荔园小学
罗玲小学
应用偏好
新闻
游戏
金融
学术
影音
社交
到岗统计
日均在岗时长
7.9h 15%
到岗率
80% 0.6%
准点率
95% 2.2%
到岗率
准点率
在岗时长
准点
迟到
外访
星期日
星期一
星期二
星期三
星期四
星期五
星期六
问题关注
离线已超过48小时，疑似失联
在教学了访问游戏应用，时长超过1小时
在寝室连续上网超过2小时
外访统计
42次
实验小学
荔园小学
罗玲小学
中心小学
翠竹小学
其他
在岗统计
总体
晴天
阴天
雨天
5天
9天
11天
6天
<1小时
1-4小时
4-8小时
>8小时

图 2

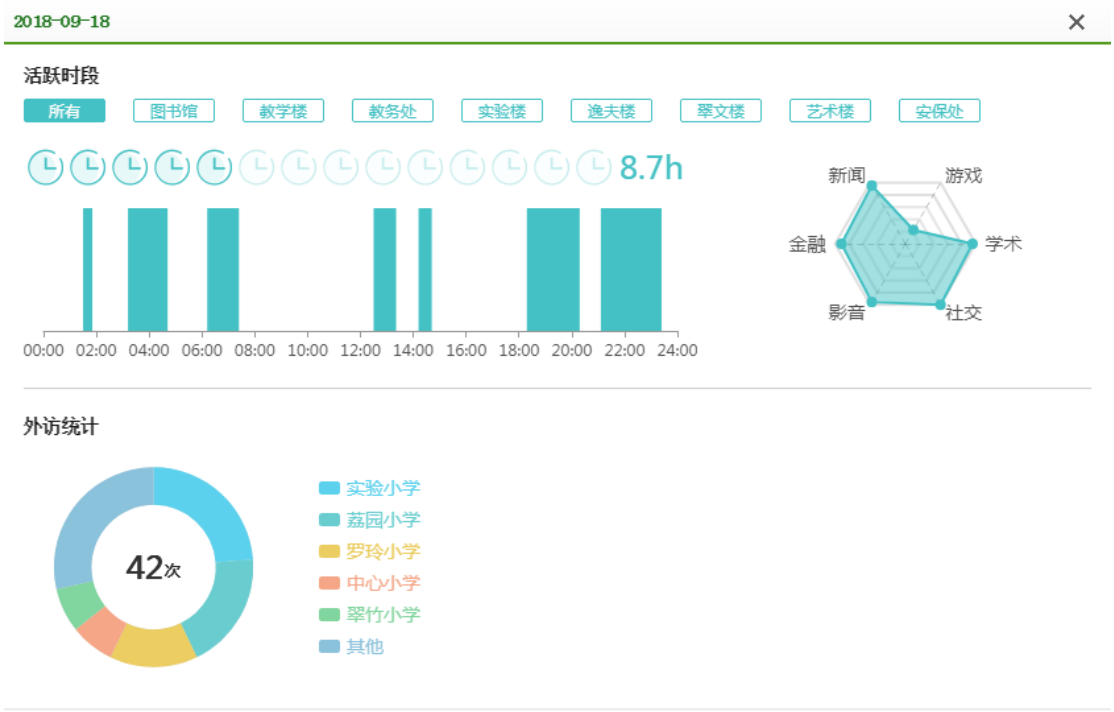


图 3

配置步骤：

1. 进入 数据分析管理->区域管理->分支区域，按分支位置，在背景图上部署分支（或建筑/分组），在各个分支（建筑/分组）上部署不同位置（如办公室，教学楼等）。

2. 进入 数据分析管理->区域管理->位置标签，系统已内置标签，内置标签不可删除，且新增位置标签必须部署在内置标签下（如内置了标签学校，此时新增标签办公室，分支区域页面父目录应打上学校标签，子目录则打上办公室），给分支区域打上标签后，即可在行业画像页面按标签对数据进行统计汇总。

3. 进入 数据分析管理->身份管理->用户身份，系统已根据行业内置了用户身份，内置身份需要关联认证后角色（只有账号认证才可以统计用户画像），只有匹配上用户身份，行业画像页面才会统计该用户数据。

4. 此外，控制器还支持查看个人画像（如图 2），个人画像包括基本信息，到岗统计，驻留位置，应用偏好，问题关注，外访统计，在岗统计；支持按月过滤用户数据，考勤日数据支持点击查看详情（如图 3）。

展会模式：

具体部署效果可进入展会模式查看

1. 在 数 据 分 析 平 台 的 URL 后 添 加 ?showdemo ， 如 ： https://192.168.1.1/WLAN/market.php?showdemo

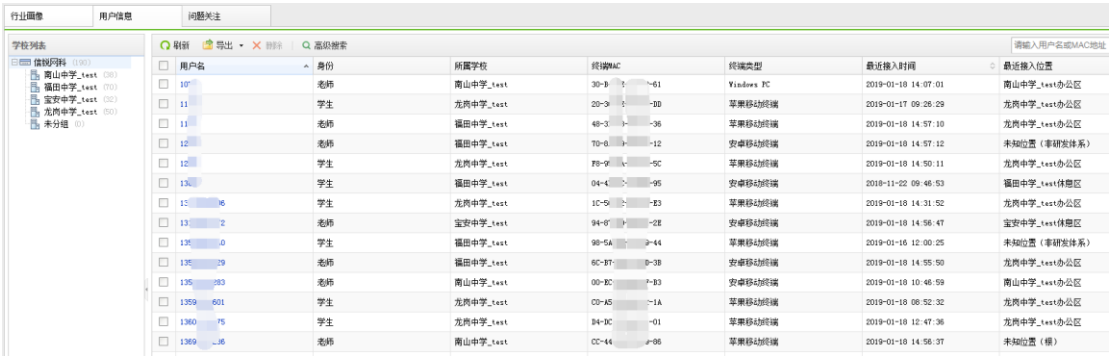
2. 进入 数据分析->行业画像，可查看数据展示效果。

4.14.1.1.2. 用户信息

展示用户信息列表，点击用户名，可以查看该用户的个人画像信息。如该用户是考勤身份，则个人画像中有考勤日历，点击考勤日历可查看该用户当天的上网情况。

考勤身份在 数据分析管理->工作日历 配置。

支持导出用户信息，以及导出用户信息的考勤数据。



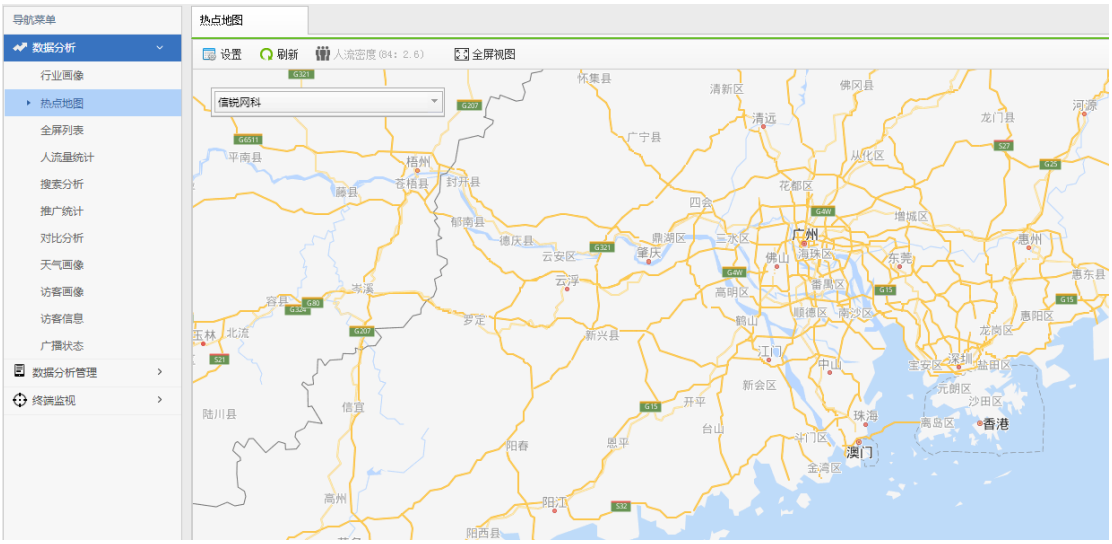
4.14.1.1.3. 问题关注

展示用户触发的行为信息列表，并支持列表导出。

用户行为在 数据分析管理->区域管理->用户行为 配置。

4.14.1.2. 热点地图

热点地图功能是为了解决接入点多或者是部署后分支结构过多而带来的设备管理复杂的问题。该功能以地图式的展现方式，分层管理设备，以掌握设备的实时运行状态。



人流密度序列号不开，热点地图位置会显示在系统状态中。

热点地图支持四种对象实体

区域、建筑物、接入点、楼层，区域或楼层能够增加接入点，集中管理可以绑定分支

当前流速

当前地图（当前所在楼层或是区域、建筑视图）里的所有接入点的实时流速，包括上传、下载流量。点击数字可以查看趋势。

在线用户

当前地图所有接入点的在线用户数。点击数字可以查看趋势。

接入点状态

当前地图内的接入点数量以及状态。点击数字可以查看在线、离线的接入点详情。

无线流量

当前地图（当前所在楼层或是区域、建筑视图）里的所有接入点的累计流量，包括上、下行流量之和。点击数字可以查看趋势。

搜索

该操作支持搜索用户和接入点。用户名支持用户名、IP 地址、MAC 地址的模糊搜索。接入点支持名称、MAC 地址的模糊搜索。

设置

禁止告警选项，图标上面不会显示安全告警的标记。

选择摘要信息中所要显示的内容，该配置为实体图标旁悬浮显示的摘要信息的内容。

锁定

锁定操作防止误操作而挪动实体图标的位置，该配置项只对当前浏览器登陆的用户生效。

小地图

大地图的缩略图，可以预览整个地图。以及支持拖动来快速切换。小地图上面的下拉框显示的是当前位置，点击可以弹出“快速定位”窗口。

4.14.1.2.1. 人流密度

人流密度功能需要开启序列号，并手动开启该功能，设置合适的比列尺，信号强度检测值与驻留时间，才能正常查看。新版本支持动态播放，便于查看人流的动态变化情况。动态播放时间维度：24 小时、7 天、自定义。

人流密度功能需要开启序列号。

要使用人流密度功能，需要配置 WLAN，且接入点启用 2.4G 的射频。

人流密度功能显示的是当前地图（当前区域、楼层）在指定时间内的人群分布情况。在

单位面积(单位面积根据蓝图的像素和比例尺决定)内，同一终端同一天仅计算一次。要查看人流密度，当前地图需要满足以下几个条件：

部署背景蓝图

编辑区域、楼层实体，蓝图选择从本地导入一张。楼层实体还可以复用之前楼层配置好的蓝图。

比例尺配置

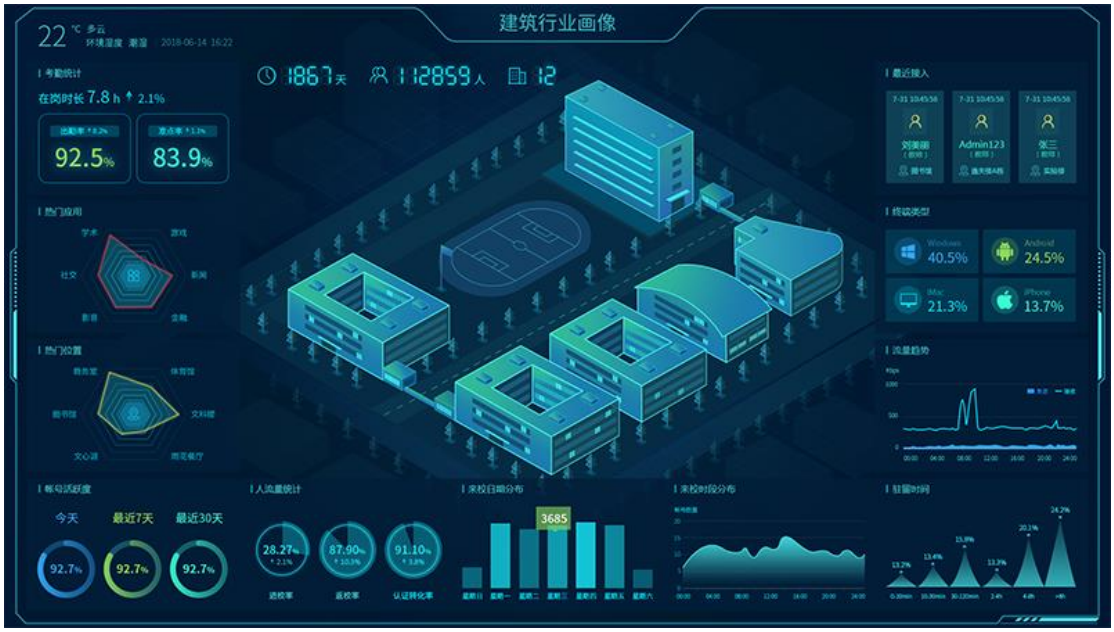
打开“人流密度分析功能配置”窗口，在配置好蓝图的前提下，编辑对应区域、楼层的比例尺，输入蓝图上 100 个像素对应的物理距离，或者是点击“测距”，选取两个像素点，然后输入两个像素点对应的物理距离。

对该楼层或区域启用人流密度分析功能。该功能默认不启用

打开“人流密度分析功能配置”窗口，在配置好蓝图、比例尺的前提下，启用对应区域、楼层的的人流密度分析功能。

4.14.1.3. 大屏展示

负责人需要将系统部署成果展示给上级或来访宾客，丰富的图表可直观展示出系统关键数据，便于进行数据分析并针对分析结果作出决策。为满足上述需求，现支持对系统关键信息进行投屏，且投屏数据可配，帮助客户定制独一无二的大屏展示。



配置步骤：

1、大屏展示支持四种模式，建筑图，区域图，全国地图，百度地图，用户可根据所在组织的行业及规模大小，选择合适的模式进行投屏。

2、用户可按需对投屏数据进行选择组合，投屏数据来源于客流统计，推广统计，访客画像，账号安全画像，行业画像，运维数据（共 25 幅统计图）。

3、用户可设置大屏标题，修改天气，上传背景图（全国地图无需上传，使用百度地图需要在控制器->应用中心配置）,数据绑定（绑定区域管理后，可显示对应区域数据）。

展会模式：

具体部署效果可进入展会模式查看

在数据分析平台的 URL 后添加 ?showdemo，如：https://192.168.1.1/WLAN/market.php?showdemo

进入 数据分析->全屏列表，打开任意大屏查看投屏效果。

4.14.1.4. 人流量统计

统计到访的用户，从首次到店用户、新登记用户，接入用户，非首次到店用户等角度对用户进行精细化的分类统计，然后进行累积到店，返店率，平均驻留时间和驻留时间分布等多维度的统计和分析，统计和分析数据还支持导出，以便根据客户需求进行更多更深入的分析处理。

环比：当前所选时间范围与上一期对应时间范围的数据变化对比的趋势(上升/下降)，若上一期无数据时则显示为“-”。

1、集中管理可以查看分支的客流分析

2、.查询客流分析数据只能通过 AP 组和区域，不能通过热点地图的区域建筑

统计和分析的数据主要作用有：

可以从多个维度具体、直观地了解店铺、超市或商场的到访客户信息；

可以通过不同区域数据、不同 AP 组数据的横向对比，了解访客的整体分布情况；

可以通过数据随日期变化的趋势，了解到访客户的变化，同时还能反映出同期经营活动的效果；

可以反映本期人流量较上一期的变化趋势及速度，调整营销战略；

可以提取一段时间内人流量数据的共性，了解客户的来访偏好，便于做针对性营销。

人流量分析功能在使用时除了要开启本模块的开关，还依赖于客流分析序列号和无线接入点（或接入点分组）射频参数中的功能开关。可以设置根据 AP 分组或者区域建筑进行数据统计，还可以根据到店客户驻留时间阈值和信号强度阈值来设置到店客户和驻留时间的记录灵敏度，统计数据可以按时间进行对比。

4.14.1.5. 搜索分析

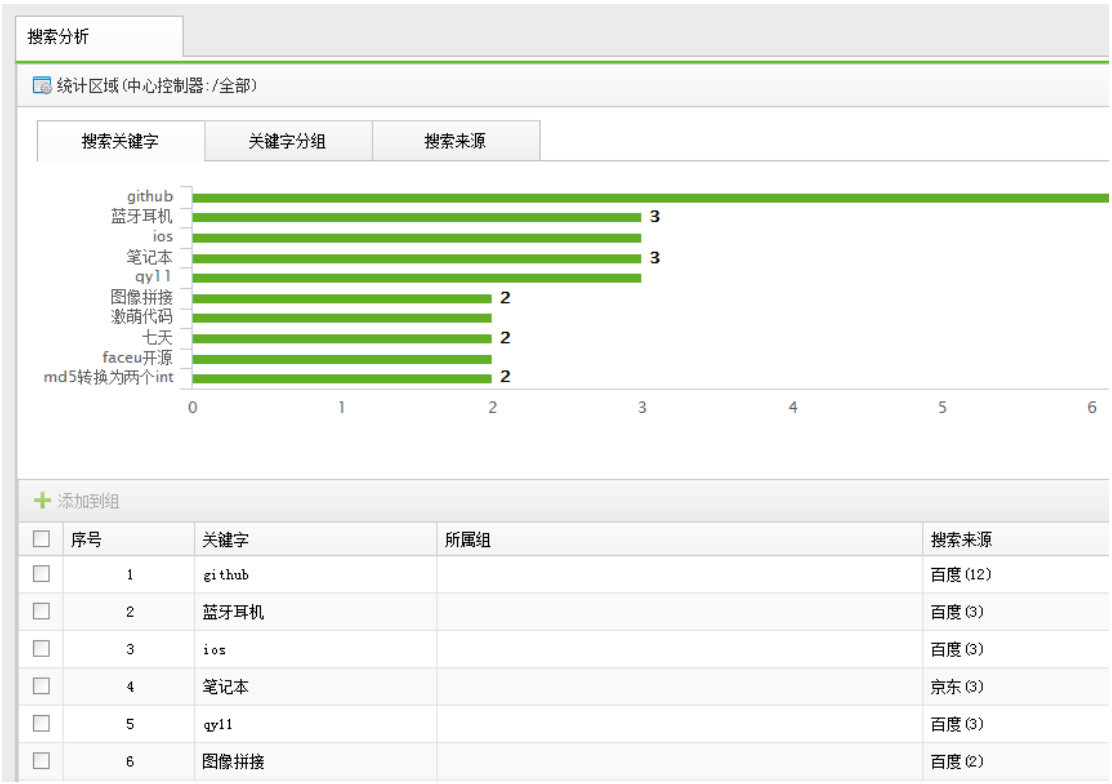
点击【搜索分析】页面如下图所示，如果开启此功能，会统计到用户通过各大搜索引擎搜索的关键字。

统计区域：可以选择 AP，了解用户通过具体 AP 点位搜索的关键字。

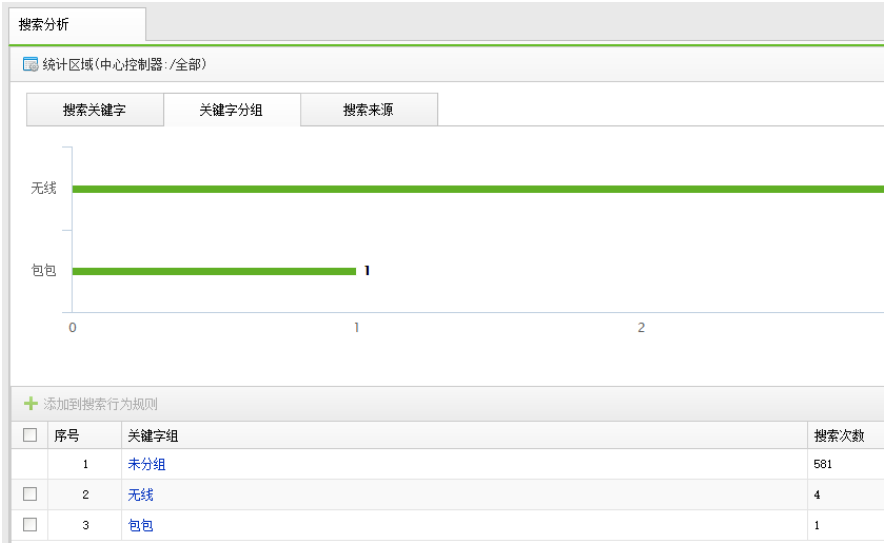
统计时间段：可以通过选择时间范围，来查看不同时间范围的关键字统计情况。默认有【最近 7 天】和【最近 30 天】两个按钮。

【搜索分析】界面列出了搜索关键字、关键字分组、搜索来源。

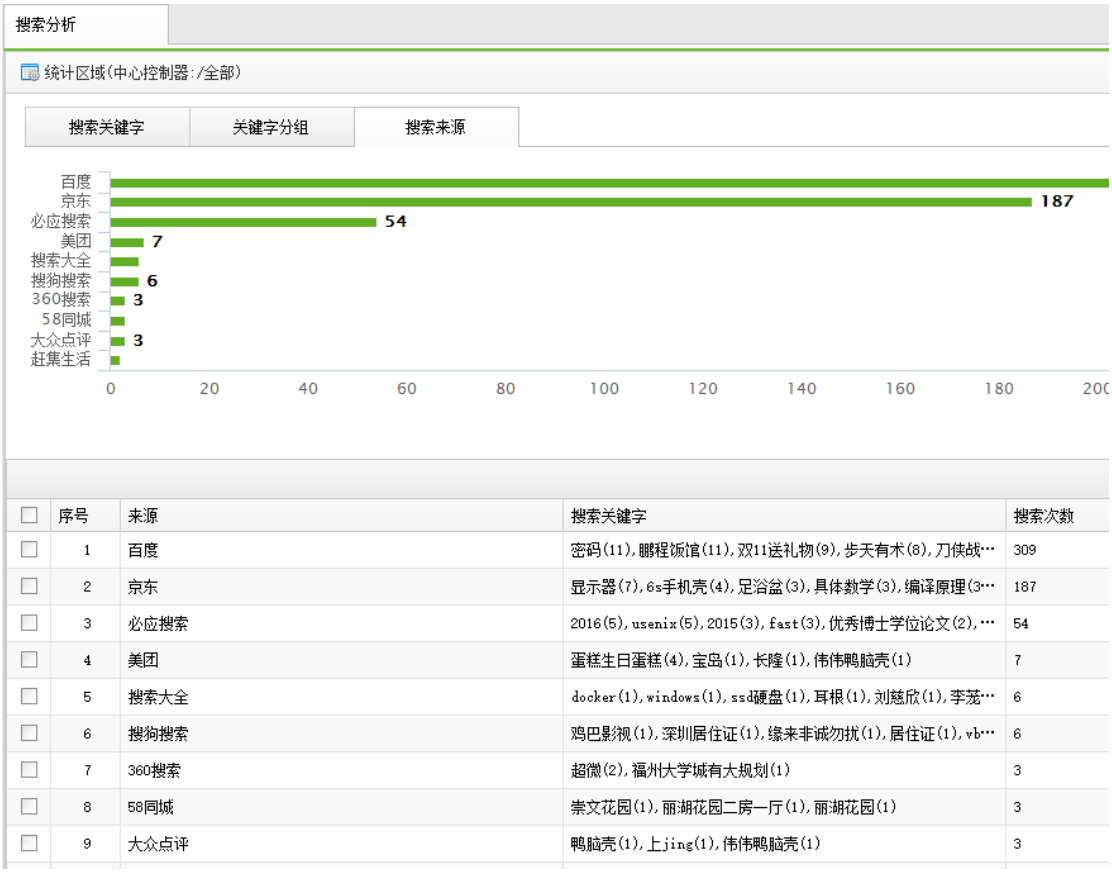
搜索关键字显示了用户通过搜索引擎搜索到的关键字及搜索次数。



关键字分组，对用户搜索的关键字做了归类。界面可以看到不同类别的关键字搜索次数。



搜索来源，显示了用户使用的搜索引擎的种类及使用这些引擎搜索的次数。

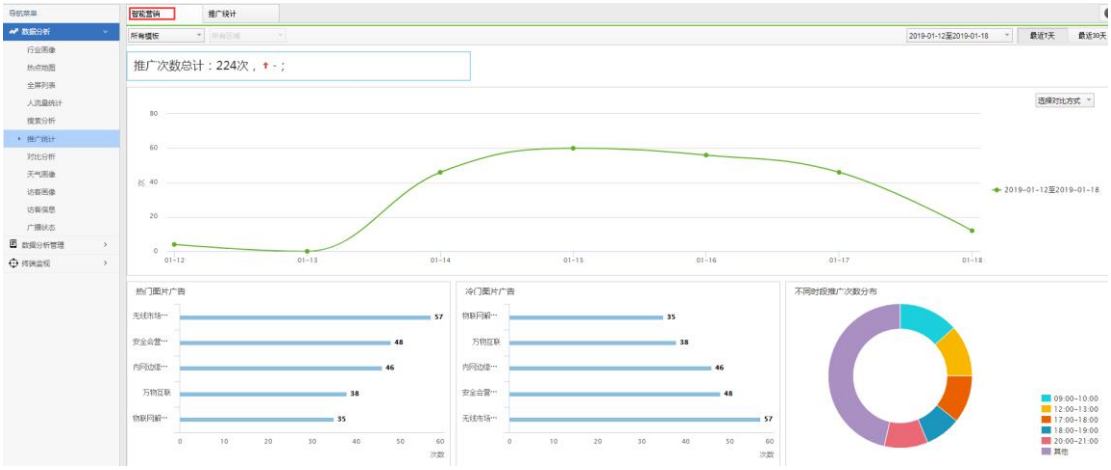


序号	来源	搜索关键字	搜索次数
1	百度	密码(11),鹏程饭馆(11),双11送礼物(9),步天有术(8),刀侠战…	309
2	京东	显示器(7),6s手机壳(4),足浴盆(3),具体数学(3),编译原理(3…	187
3	必应搜索	2016(5),usenix(5),2015(3),fast(3),优秀博士学位论文(2),…	54
4	美团	蛋糕生日蛋糕(4),宝岛(1),长隆(1),伟伟鸭脑壳(1)	7
5	搜索大全	docker(1),windows(1),ssd硬盘(1),耳根(1),刘慈欣(1),李菟…	6
6	搜狗搜索	鸡巴影视(1),深圳居住证(1),缘来非诚勿扰(1),居住证(1),vb…	6
7	360搜索	超微(2),福州大学城有大规划(1)	3
8	58同城	崇文花园(1),丽湖花园二房一厅(1),丽湖花园(1)	3
9	大众点评	鸭脑壳(1),上jing(1),伟伟鸭脑壳(1)	3

4.14.1.6. 推广统计

4.14.1.6.1. 智能营销

智能营销模板支持更加丰富的区域显示规则，帮助营销人员结合天气环境情况，推送与顾客直观感受相吻合的广告内容，能让每个顾客看到与自己相关的"专属"信息，做到千人千面的展示效果。



支持一套模板多个门店使用，且不同门店展示不同广告内容。每个门店(单条显示规则）均支持引用接入点分组并配置多张广告图片，每张广告图片可以设定不同环境属性、用户属性、所在位置、推送时间进行智能展示。

支持每个显示规则引用不同的消息栏，以个性化的展示消息栏信息。消息栏信息可以在消息栏模板页面进行配置。

统一配置：在总部、多个门店场景下，可以启用统一配置，用于在指定生效时间内强制展示总部设定的广告内容，若部分门店不展示总部统一广告可以进行排除。

注：统一配置禁用或生效时间外，各门店恢复显示门店设定的独立广告内容。

4.14.1.6.2. 推广统计

统计不同的推广类型、推广方式所推广出去的信息数量，可以根据推广类型、微信公众平台和推广时间等条件进行统计。

统计数据的主要作用是分析推广力度，同时也可以结合推广的具体内容进一步分析不同推广内容的推广效果。

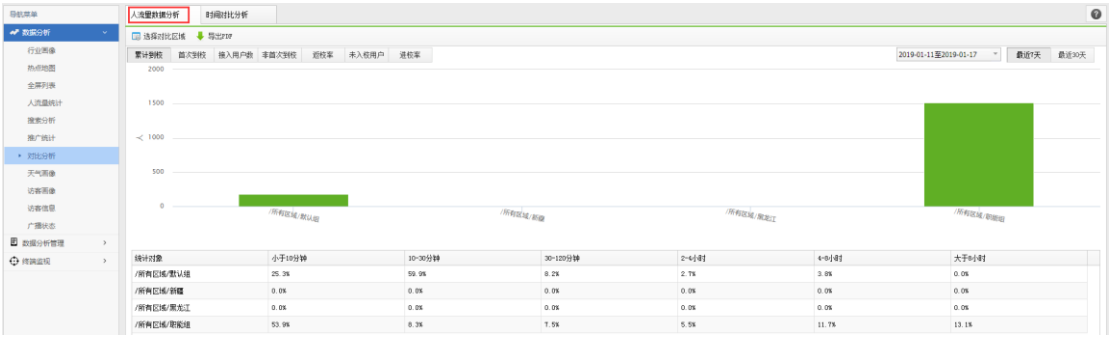
推广任务可以创建和管理微信或者短信群发消息的任务，并查看各推广任务的详细完成

情况。

4.14.1.7. 对比分析

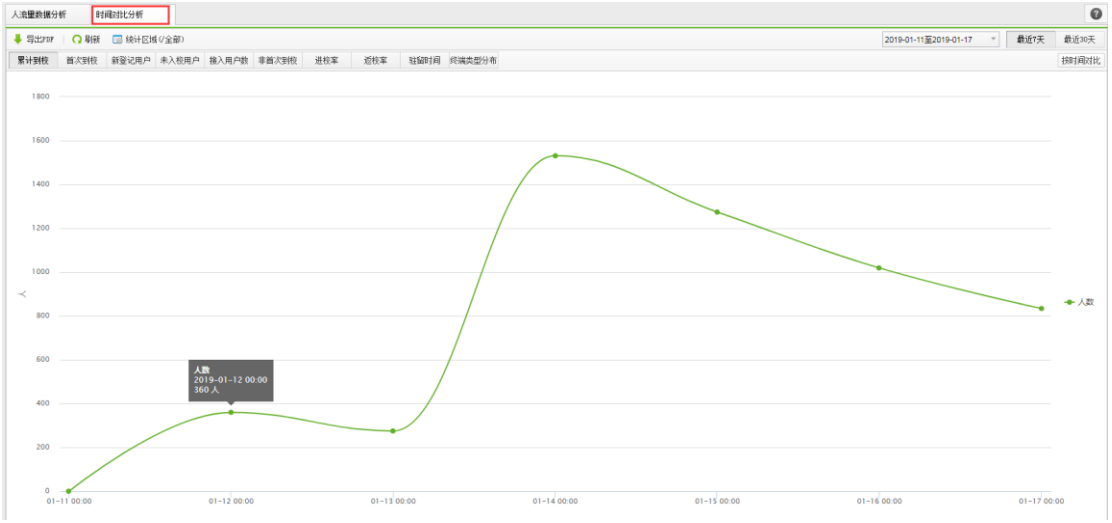
4.14.1.7.1. 人流量数据分析

选择分支或者 AP 组等条件进行人流量分析，对比人流量数据。



4.14.1.7.2. 时间对比分析

选择分支或者 AP 组等条件进行时间对比分析。



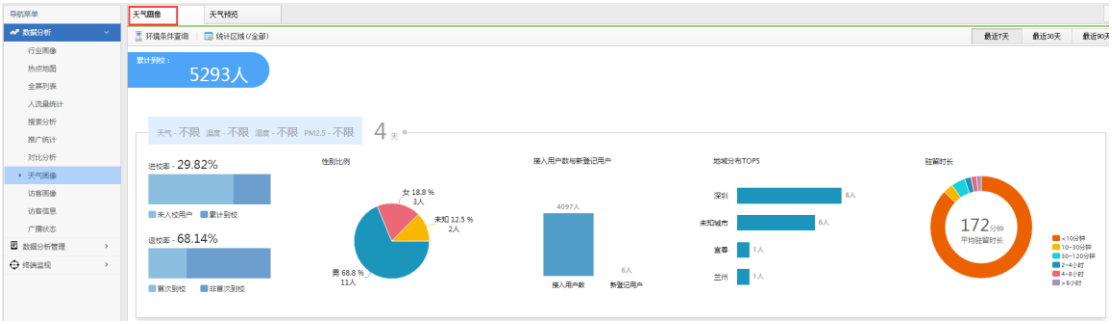
4.14.1.8. 天气画像

商超、景区等具备经营性质的场所的决策人员需要天气、温度、湿度等环境数据，利用这些数据关联天气对访客的数量、偏好的影响，做针对性的分析。

关联环境数据对访客的数量、偏好的影响进行统计，让运营人员可以结合天气情况直观的查看不同区域访客数量、未到店人数、首次入店人数、老用户人数、地域等数据可视化的展现。

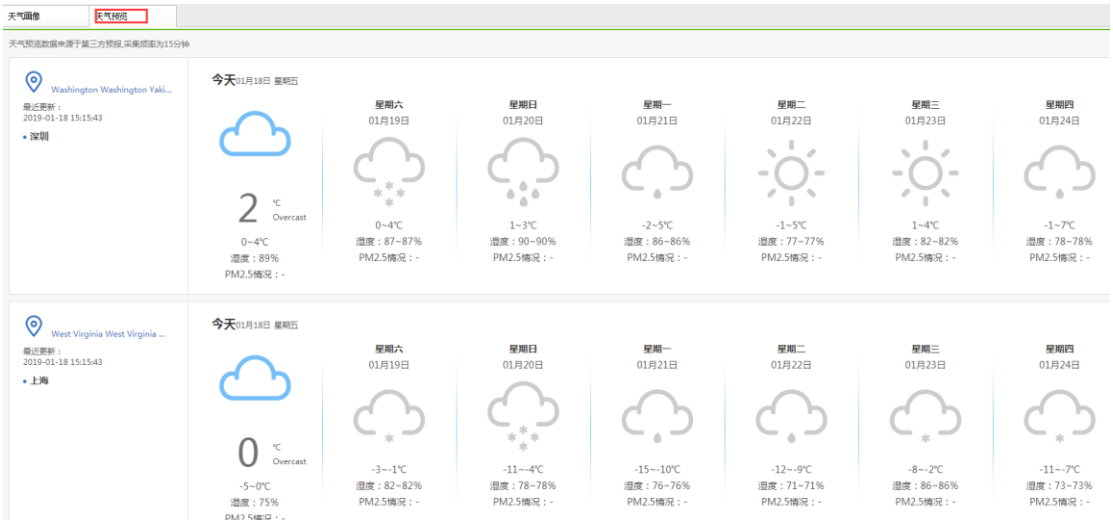
4.14.1.8.1. 天气画像

环境条件查询：可以设置天气条件组合，在对应的天气条件下，可以查询最近 7 天/30 天/90 天的不同维度的人流量统计数据。对于环境组合条件，可以设置显示/隐藏，以及上下移动。 统计区域：默认显示全部，过滤统计区域后，在对应的环境条件查询下，可以看到不同的 AP 组下面的人流量数据。



4.14.1.8.2. 天气预览

根据[区域环境参数]页面配置的采样地点展示当天及未来一周的天气信息。 注：天气预览数据来源于第三方预报。采集频率为：[数据分析管理->区域信息配置->区域环境参数->采样频率设置]中设定的值。



4.14.1.9. 访客画像

访客画像功能是对所有接入的短信/微信用户进行用户画像，分析大量用户的 WIFI 使用情况所形成的画像内容，具体画像内容包括：

时间画像：分析用户的来访时间偏好，包括用户偏好于在星期几来访，每天来访的高峰时间段，每天的 WIFI 使用时长分布。

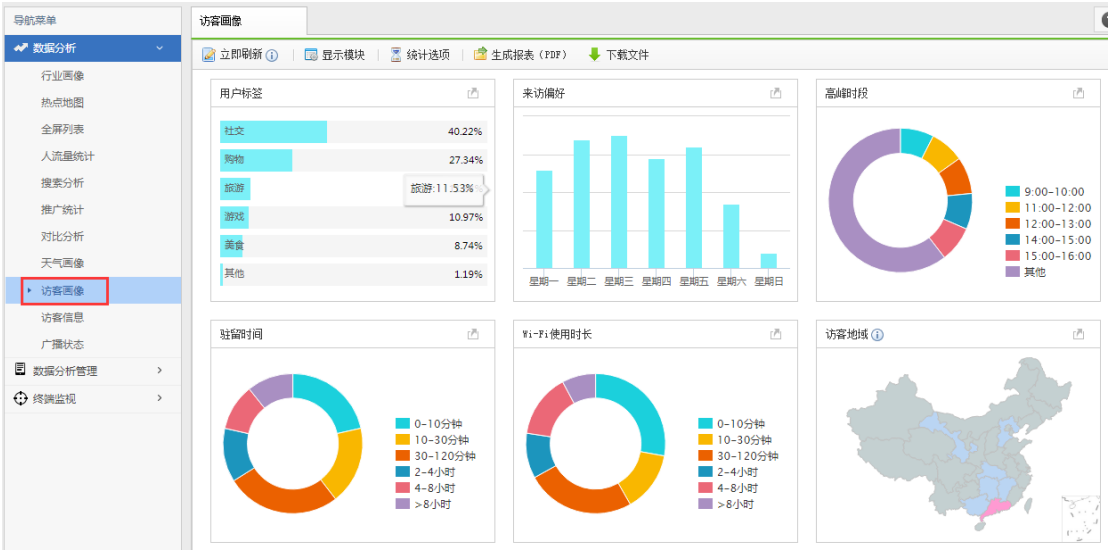
人物画像：可以分析用户的性别、地域分布，访客的性别（通过微信获取），地域（通过手机号码归属地或者是微信获取），终端类型分布。

应用画像：分析用户的应用使用偏好，即用户是购物达人、影视达人、理财达人等应用分析。

自定义画像：控制器会收集的访客信息里面，可以通过筛选条件过滤出一批访客用户，再给这批选定的用户手动打上一个自定义的标签，如：VIP 用户、白金用户等标记。

使用访客画像功能需要开启功能序列号的访客画像序列号，并且，需要在开启客流分析功能。请在系统管理->营销中心配置->功能设置->启用客流分析功能。

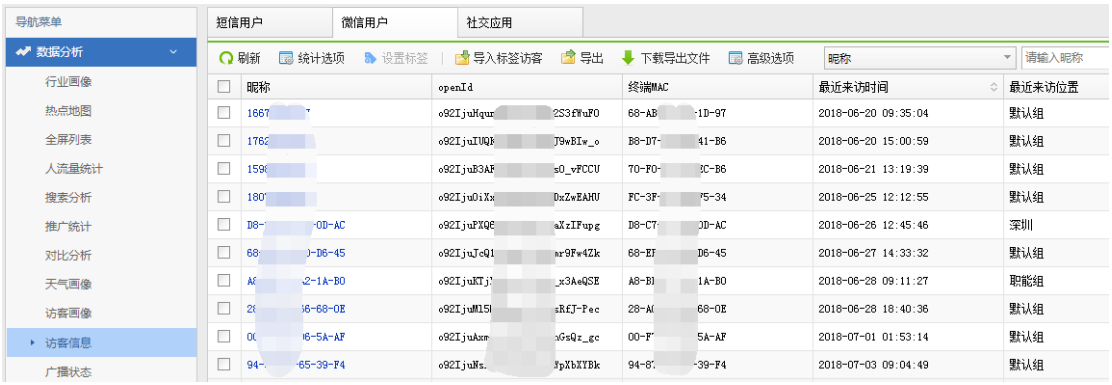
立即归档：用户画像每天凌晨将一天统计的信息，进行分析归档，生成各类画像数据。立即归档是立即对当天的数据进行归档，在数据流较大的情况下，立即归档可能会需要 2-3 分钟时间。



4.14.1.10. 访客信息

可以记录下短信认证和微信认证的用户的行为轨迹，包括活跃度、来访偏好、Wi-Fi 使

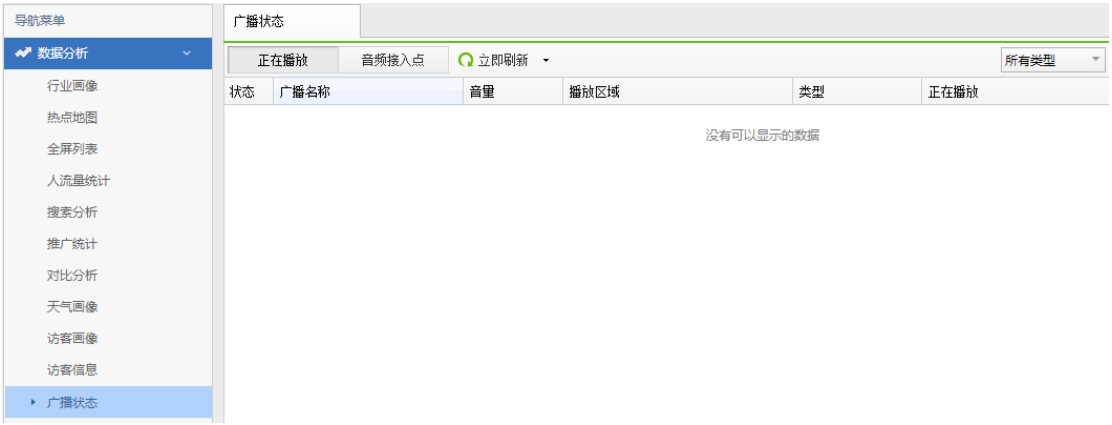
用时长、出现时段等，并可以给根据访客的行为给访客添加不同的标签，更好地来实现后期的营销推广。



4.14.1.11. 广播状态

显示正在播放的音频任务，包含广播计划、音频广播、营销推广、APP 音频。

显示正在播放音频任务的音频接入点以及接入点的基本信息。



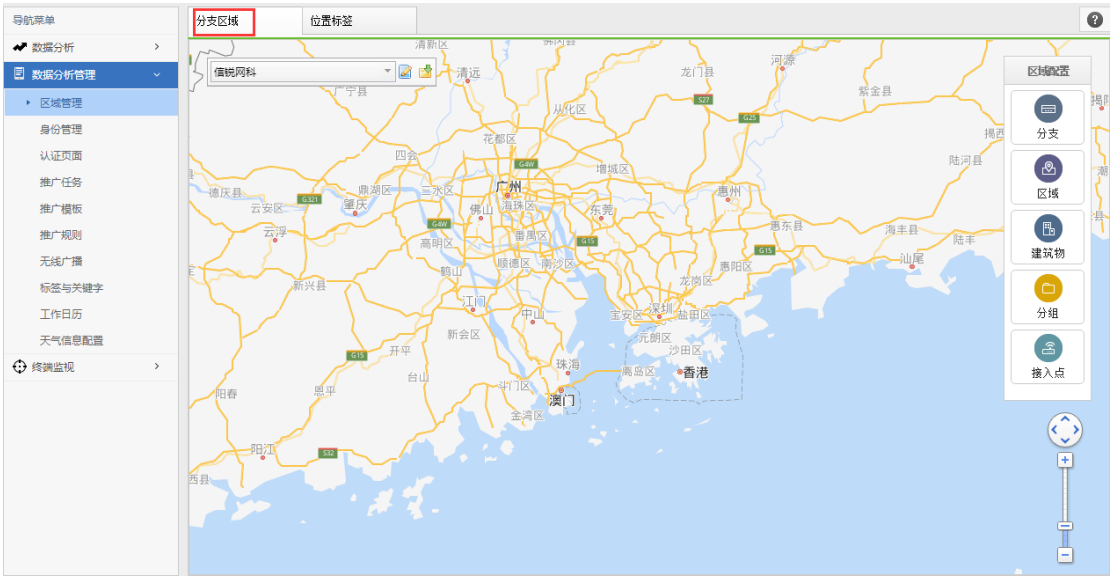
4.14.2. 数据分析管理

4.14.2.1. 区域管理

4.14.2.1.1. 分支区域

支持四种实体，分支、区域、建筑物、分组，四种实体都可以增加接入点，集中管理可以绑定分支。

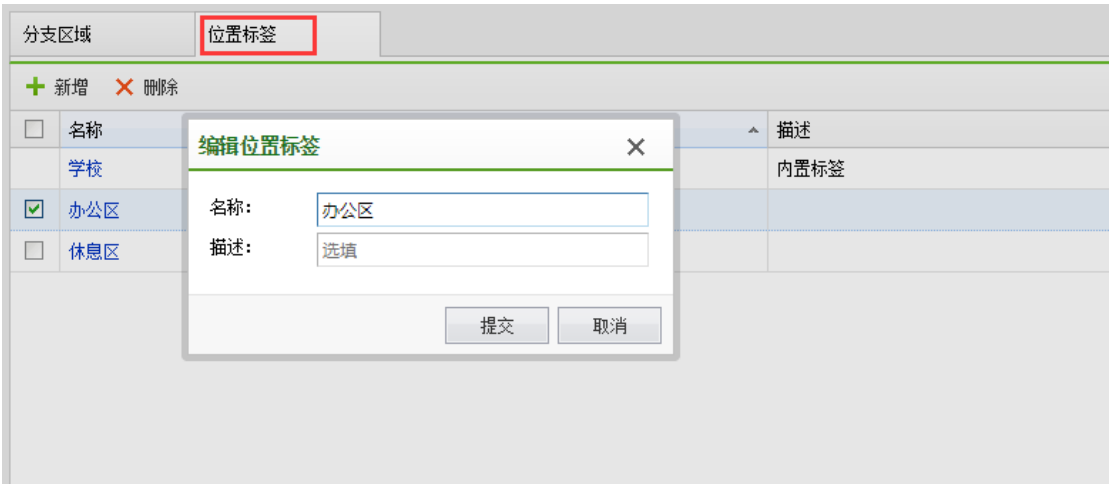
可以为实体配置标签，有内置标签的实体为行业画像的子区域。



4.14.2.1.2. 位置标签

有一个内置标签，绑定了内置标签的实体为行业画像的子区域。

可根据实际需要配置其他的位置标签。



4.14.2.2. 身份管理

4.14.2.2.1. 用户身份

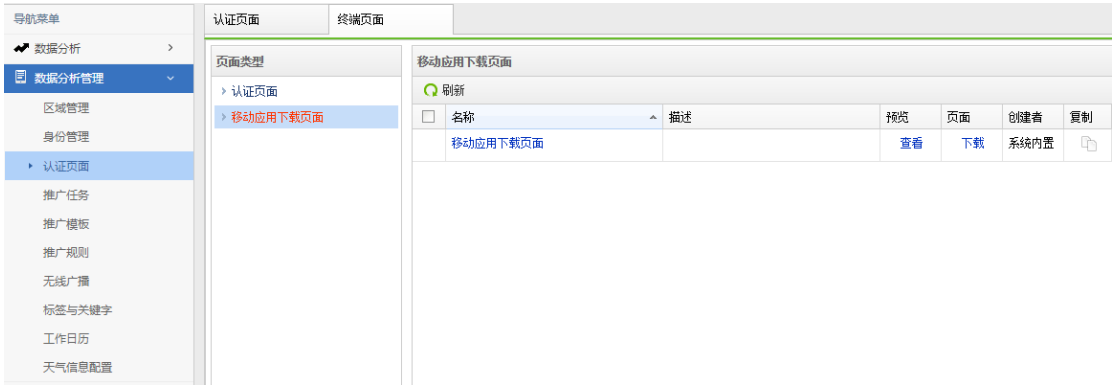
根据行业切换，有不同的内置身份，可以为用户身份配置身份归属地。归属地要绑定为有内置标签的实体，并为该实体的用户配置相应的角色。

4.14.2.2.2. 用户行为

为用户配置离线规则或应用规则，并设置触发规则后的短信告知人。离线规则触发后 10 分钟内推送短信，应用规则触发后第二天 7 点推送短信。

4.14.2.3. 认证页面

与【认证授权】→【终端页面】内容相同。



4.14.2.4. 推广任务

推广任务可以创建和管理微信或者短信群发消息的任务，并查看各推广任务的详细完成情况。

4.14.2.5. 推广模版

4.14.2.5.1. 微信推广模版

创建或删除微信推广模板，支持文本和图文两种类型，并可以预览模板实现的效果。

文本模板内容简洁，配置简单。

图文模板内容丰富，直观生动。“标题+描述+图片”的预览界面更直观的呈现推广内容，从而能更好的吸引用户关注。

4.14.2.5.2. 短信推广模版

创建或删除短信推广模板，仅支持文本，并可以预览模板实现的效果。

4.14.2.5.3. 全屏网页模版

创建或删除网页推广模板，支持本地模板和外部 URL 两种类型，支持本地模板的可以预览模板实现的效果。

如果您计划把广告内容制作成图片，则推荐使用本地模板方式推送图片广告。

如果您已经拥有公司主页，可以使用外部 URL 的方式推送公司主页。

4.14.2.5.4. 内嵌网页模板

创建或删除内嵌网页推广模板，您可以配置网页内嵌方式显示的图片，以及点击图片后跳转的 URL。

图片支持本地上传和外部 URL 两种类型，其中本地上传支持预览模板实现的效果。

不论本地上传还是外部 URL 链接图片，尺寸建议为 400*60 像素，大小不宜超过 100K，否则可能会影响展示效果。

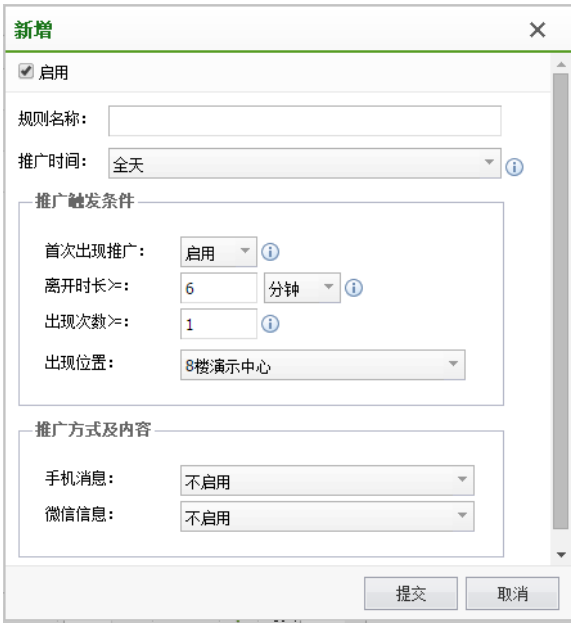
4.14.2.6. 推广规则

推广规则包括终端出现、首次接入、在线时长、搜索分析和应用访问五种方式的推送规则。

4.14.2.6.1. 终端出现

创建或删除终端出现推广规则，根据此规则针对已经认证过短信或微信的用户进行相应的推广。

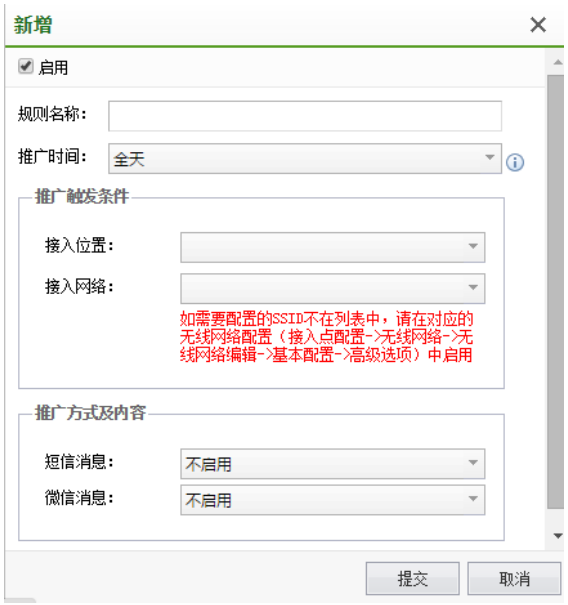
规则支持启用禁用和优先级调整，由高到低匹配规则列表，只有匹配中的第一条规则生效。



4.14.2.6.2. 首次接入

创建或删除首次接入推广规则，根据此规则针对首次认证短信或微信的用户进行相应的推广。

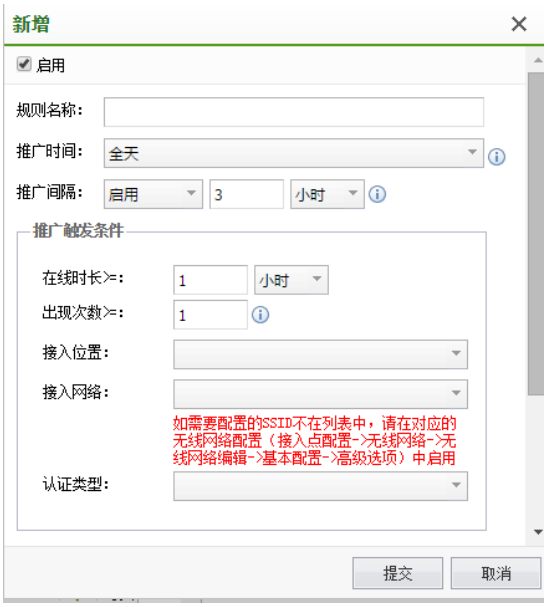
规则支持启用禁用和优先级调整，由高到低匹配规则列表，只有匹配中的第一条规则生效。



4.14.2.6.3. 在线时长

创建或删除在线时长推广规则，根据此规则针对当前在线用户进行短信、微信或网页推广。

规则支持启用禁用和优先级调整，由高到低匹配规则列表，只有匹配中的第一条规则生效。



4.14.2.6.4. 搜索行为

创建或删除搜索行为推广规则，根据此规则针对当前在线用户进行短信、微信或网页内嵌广告推广。

规则支持启用禁用和优先级调整，由高到低匹配规则列表，只有匹配中的第一条规则生效。

4.14.2.6.5. 应用访问

创建或删除应用访问推广规则，根据此规则针对用户使用应用或访问网站进行广告推送。

短信和微信推送仅支持访客用户。

规则支持启用禁用和优先级调整，由高到低匹配规则列表，只有匹配中的第一条规则生效。

应用访问推送的短信和微信广告模板支持占位符。

4.14.2.7. 无线广播

4.14.2.7.1. 广播计划

管理定时广播任务。

功能介绍：

1、管理广播计划

支持添加、删除、启用、禁用广播计划。

2、搜索

通过右上角的搜索框可以按名称搜索指定广播计划。 支持模糊搜索。

3、创建广播计划

支持选择在指定 AP 上播放，选择要播放的播单、播放方式、播放时间、是否使用 AP

上的音量、任务触发的优先级。

4、高级选项

优先级：不同类型的音频广播在同一时段发生时，将优先保证高优先级的播放；相同优先级的广播，相互之间无法中断。

中断后操作：可以选择取消任务，也支持断点续播。

4.14.2.7.2. 播单列表

音频文件的集合，方便音频广播计划的引用。

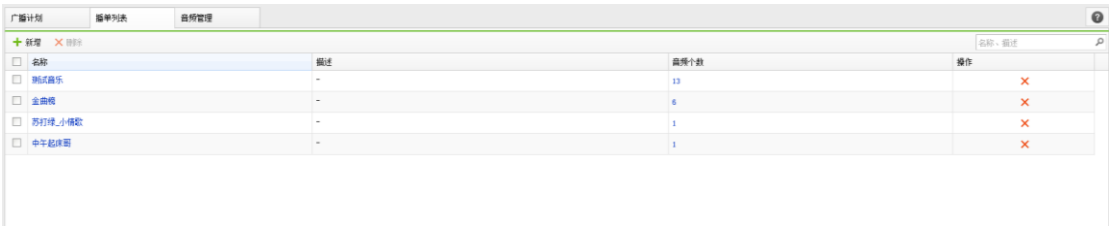
功能介绍：

1、创建播单

支持添加、删除播单内的音频文件，及调整音频顺序。

2、搜索

通过右上角的搜索框可以按名称和描述搜索指定播单。 支持模糊搜索。



4.14.2.7.3. 音频管理

管理控制器上的音频文件。

功能介绍：

1、音频上传

可以上传本地音频文件到控制器，支持高低音质的选择。建议使用低音质，对带宽资源消耗小。

2、搜索和过滤

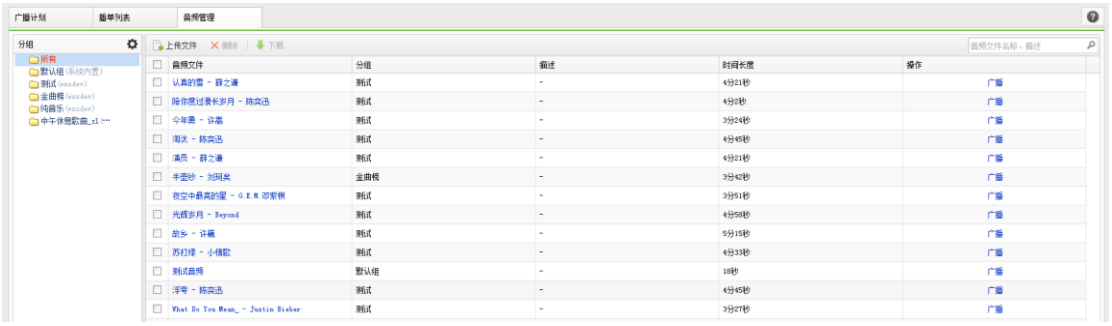
通过右上角的搜索框可以按名称和描述搜索指定音频。支持模糊搜索。

3、音频分组

添加、删除音频分组。

4、立即播放指定音频

选择某个音频，点击广播操作，可以选择在指定 AP 上播放，并支持使用此任务的音量或使用 AP 的音量。



4.14.2.8. 标签与关键字

4.14.2.8.1. 应用标签

应用标签内建了常用的安全风险、发送电子邮件、高带宽消耗、降低工作效率、论坛与微博发帖、外发文件泄密风险，也可以自定义标签，将关心的应用的放到标签内，方便系统其他模块引用，提供给应用访问推广规则使用。

4.14.2.8.2. 关键字组

关键字组可以管理关键字，将关键字分类存放。

4.14.3. 终端监视

4.14.3.1. 主要解决的客户问题

1.无法实时对贵重物品、易燃易爆等物品定位监管；

2.贵重资产容易出现丢失的情况，想用的时候又很难找到。

4.14.3.2. 给客户带来的价值

1.对没有无线模块的重要物品进行监控、跟踪；

2.快速查找物资的位置，减少人工成本，提高效率；

3.设置监控策略，可以防止设备被盗窃。

4.14.3.3. 配置方法

1、蓝牙终端监控接入点配置

（1）NAC 上激活支持 USB 接口的接入点，将蓝牙适配器接在接入点的 USB 接口。

（2）接入点分组-》编辑-》其他配置-》USB 接口工作模式，选择 USB 蓝牙，监控接入点蓝牙覆盖范围内的蓝牙标签。

2、无线终端监控接入点配置

（1）NAC 上激活任意型号的接入点。

（2）NAC 上配置无线网络，接入点配置-》无线网络页面，新增无线网络，接入点选择能覆盖这个区域的所有接入点，以达到监控范围内无线终端的目的。

说明：

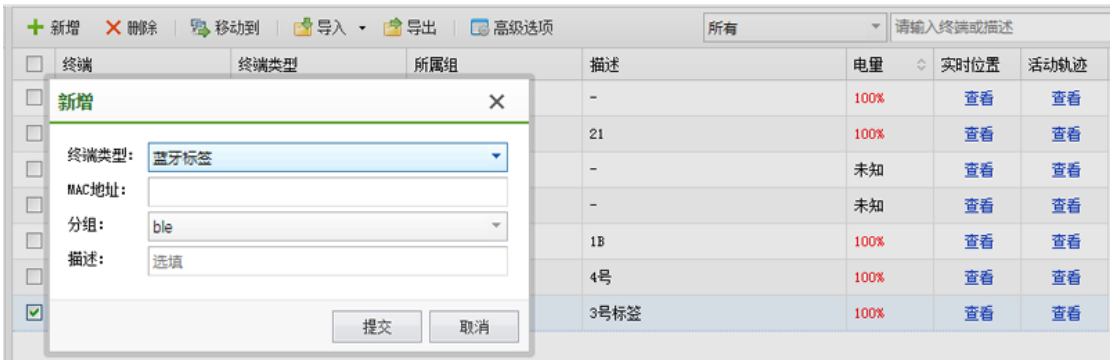
（1）蓝牙监控功能需要开启蓝牙序列号。

（2）蓝牙终端监控和无线终端监控可以共用同一个接入点。

3、添加监控终端

【营销中心】-【终端监视】-【终端数据库】页面，新增终端，终端类型选择【蓝牙标签】，MAC 地址填写标签上的 MAC 地址，将标签贴到需要监控的资产上，如果是无线终

端，新增监控终端时，终端类型就选择无线终端。



（1）终端类型：分蓝牙标签和无线终端，无线终端又分为 MAC 地址和用户名类型。

（2）分组：将不同类别的 MAC 地址或用户名保存在多个分组中，以便系统其它功能调用，如:终端监视。

（3）移动：终端数据记录可以通过“移动到”功能，调整到不同的分组中。

（4）导入导出：通过导入导出功能，可以快速的获取和添加终端数据，通过下载并按照示例模板填写，以保证导入模板的正确性。

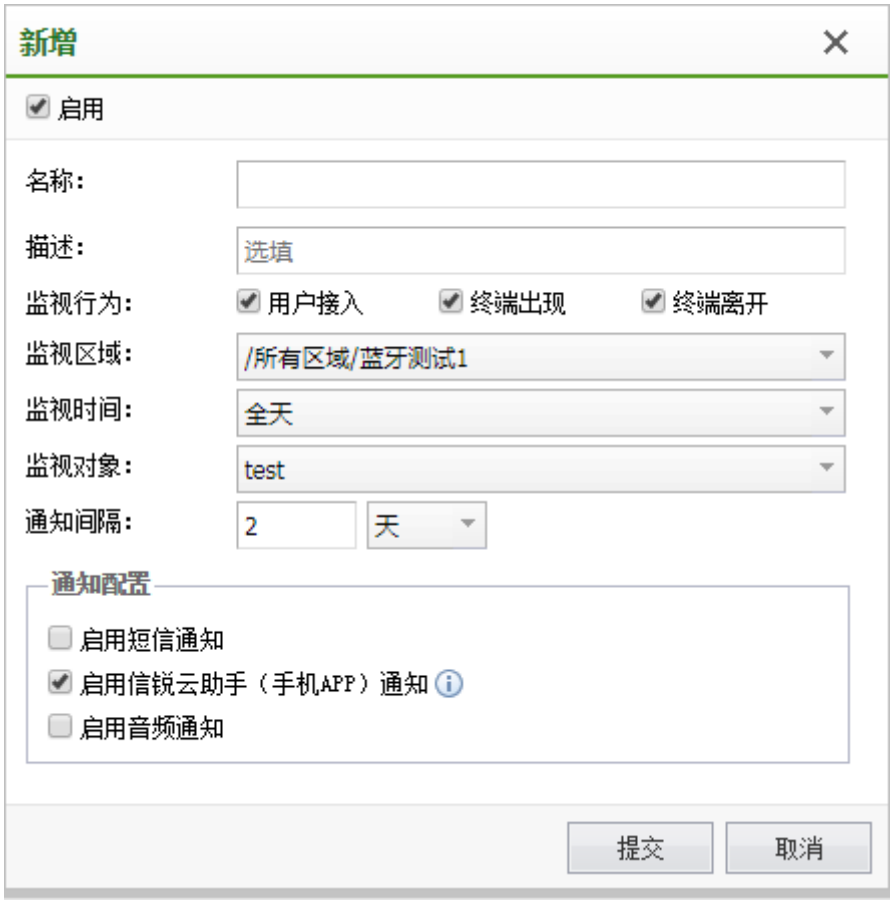
（5）高级选项

1）蓝牙标签电量告警阈值：设置蓝牙标签最低电量告警阈值，当蓝牙标签电量达到配置的阈值，就会在指定的告警时间定时推送低电量告警消息给管理员。

2）电量告警推送时间：默认时间为上午 10:00，可以根据实际需求修改推送时间。

4 、配置终端监控策略。

【营销中心】-【终端监视】-【监视策略】页面，新增监控策略，通知配置有以下三种，短信通知，信锐云助手（手机 APP）通知和音频通知。



该策略用于配置在不同时间、不同区域，监视多种终端行为。目前支持的监控行为分为三种。

1）用户接入：

当终端数据库分组中的无线终端（MAC 地址或用户名）接入无线网络时，NAC 会通过 APP 或音频消息告知管理员监视终端接入。当需要监控特定的设备是否接入监视区域内的 Wi-Fi 时，可在策略中勾选这一监控行为。

2）终端出现：

当终端数据库分组中的终端（MAC 地址）出现在监视区域时，NAC 会通过 APP 或音频消息告知管理员监视终端出现。当需要在 Wi-Fi 覆盖区域内监控指定设备时，可在策略中勾选这一监控行为。

3）终端离开：

当终端数据库分组中的终端（MAC 地址）离开监视区域时，NAC 会通过 APP 或音频消息告知管理员监视终端离开。

此外，系统对蓝牙标签有两种默认监控行为：

1）蓝牙标签拆除告警：

此告警不需要在页面配置，当 NAC 加入云管家，蓝牙标签被拆除感光后，就会触发拆除告警，系统将发送告警信息到管理员的信锐云助手 APP。

2）蓝牙标签低电量告警：

此告警不需要在页面配置，当 NAC 加入云管家，蓝牙标签的电量到达设置的低电量阈值时，就会触发低电量告警，系统将发送告警信息到管理员的信锐云助手 APP。

通知配置

1）短信通知：

启用短信通知，需要在 NAC【系统配置】-【短信服务】页面配置可用的短信服务器，监控策略里面配置上需要通知的管理员手机号。

2）云助手 APP 通知：

在【系统管理】-【应用中心】-【信锐云】页面，有终端监视的总开关，是终端监控消息能推送到 APP 的必要条件，此开关默认开启，若禁用则所有关于终端监控的消息均不会推送到 APP。而每一条监控策略中，有启用信锐云助手通知这一必要条件，默认开启，用于选择具体的监控行为是否推送到 APP 上。

3）音频通知：

启用音频通知方式，可以选择 NAC 上支持音频的接入点，匹配上监控策略接入点播放对应的告警通知。

注意事项

部分被监控的无线终端进入休眠模式，可能会被判定为终端离开。

5、部署热点地图

【营销中心】-【数据分析】-【热点地图】页面，添加区域、建筑及楼层，楼层里面添加接入点，配置好人流密度比例尺，并启用人流密度功能。

6、查看监控终端的实时位置和活动轨迹

【营销中心】-【终端监视】-【终端数据库】页面，点击被监控终端的实时位置或活动轨迹。

（1）实时位置

点击实时位置列的“查看”按钮，则能关联到热点地图，显示终端当前在地图中定位到的位置。此功能需开启【系统管理】-【应用中心】-【营销中心】页面的“启用客流分析”，即可以开启热点地图的定位功能。

（2）活动轨迹

点击活动轨迹列的“查看”按钮，可看到终端在监控范围内的活动轨迹记录。点击坐标值，则可跳转到热点地图，查看接入点在地图中的历史位置。此功能也需要开启【系统管理】-【应用中心】-【营销中心】页面的“启用客流分析”。

（3）注意事项

终端数据库支持从模板中导入，以及从微信访客和短信访客中导入这三种方式，可快速的将已使用微信和短信认证过的终端记录加入到终端数据库中。

4.15. 边缘安全

『边缘安全』包含了【边缘可视】、【无线安全】、【交换机安全】、【控制器安全】、【边缘监控】、【安全日志】六个大的功能菜单，其中【边缘可视】包含了【账号状态】、【安全状态】、【终端状态】、【黑名单】、【热点分析】共 5 个子菜单；【无线安全】 包含了【无线射频防护】、【接入点网络安全】、【无线攻击防御】共 3 个子菜单；【交换机安全】包含了【有线终端审批】、【有线终端安全】共 2 个子菜单；【控制器安全】包含了

【控制器网络安全】1 个子菜单；【边缘监控】包含了【安全联动】1 个子菜单；【安全日志】包含了【安全日志】1 个子菜单。

4.15.1. 边缘可视

4.15.1.1. 账号状态

安全事件

显示无线欺骗攻击，ARP 欺骗，DHCP 泛洪攻击，ARP 扫描攻击，IP 扫描攻击，端口扫描攻击，DDOS 攻击，无线泛洪攻击；10 分钟检测 1 次。

账号活跃度

显示闲置账号和活跃账号的分布，超过 5 天未登录的是闲置账号，5 天以内登录的是活跃账号。

账号日期分布

显示周一到周日，登录的账号数量。同 1 个账号，在同一天重复上下线，只统计 1 次。

账号时段分布

显示 1 天之内，不同时间段登录的账号数量。同一个账号，在 15 分钟之内，重复上线下线，只统计 1 次。

账号对接行为

显示账号的接入行为。

终端类型信息

显示不同的账号，使用什么样的终端登录。

终端数量信息

显示同一个账号，在多少个终端登录过。

4.15.1.2. 安全状态

显示当前无线网络环境下，无线控制器、接入点的安全状态。

安全状态检测的事件类型包括：钓鱼 AP，有干扰的邻居 AP，非法 AD-Hoc，无线泛洪攻击，DDOS 攻击，爆破攻击，BSSID 冲突检测，私设 ip，无线欺骗攻击，ip 冲突，ARP 欺骗，DHCP 泛洪攻击，ARP 扫描攻击，ip 扫描攻击，端口扫描攻击。

安全状态可以查看时间段分别为今天、某一天、最近 7 天和最近 30 天发生的各种安全事件的简要信息。

趋势图 ：攻击者个数的趋势信息。

饼图 ：各种安全事件的比例。

详情 ：此攻击者出现的时间段。

4.15.1.3. 终端状态

显示终端状态，可查看终端数量（在线和离线终端）、终端类型分布、闲置终端、终端离线分布、终端离线趋势及终端迁移和安全事件的行为、次数。可以通过类型分布的饼状图，查看不同类型具体的占比，同时可以通过趋势图，查看一段时间内终端的变化情况，包括离线趋势、迁移情况等。另外，还可点击相应的表项查看相对应的模块具体的数据信息，如：点击“闲置终端”中离线时间大于 10 天的设备，可看到该设备的 mac 地址、主机名和最近登陆时间。

4.15.1.4. 黑名单

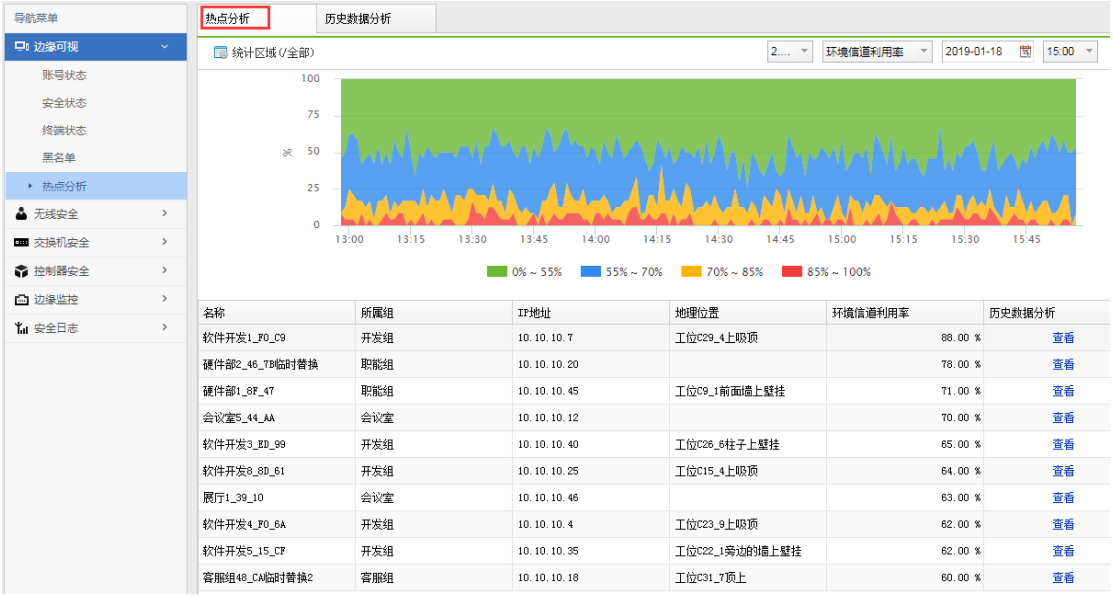
管理员可以手动添加黑名单，以阻止指定的 MAC 地址终端连接有线和无线网络。

当终端进行暴破登录或者其它恶意攻击行为时，系统会将此终端的 MAC 地址加入黑名单，拒绝一段时间内该终端的连接请求。由终端类型绑定策略触发的非指定类型终端接入，系统也会将此终端 MAC 地址加入黑名单并拒绝该终端的连接请求，限制时间随策略而定。

4.15.1.5. 热点分析

4.15.1.5.1. 热点分析

热点分析中，根据环境信道利用率、自身信道利用率、重传率、误码率、噪声值、同频干扰等参数划定的区间，将无线接入点划入指定的区间。管理员通过分析接入点在各个区间的分布情况，排查接入点的问题，并通过增加接入点、调整接入点位置等方式，提高无线网络的整体服务质量。



名称	所属组	IP地址	地理位置	环境信道利用率	历史数据分析
软件开发1_F0_C9	开发组	10.10.10.7	工位C29_4上吸顶	88.00 %	查看
硬件部2_46_TB临时替换	职能组	10.10.10.20		78.00 %	查看
硬件部1_8F_47	职能组	10.10.10.45	工位C9_1前面墙上壁挂	71.00 %	查看
会议室5_44_AA	会议室	10.10.10.12		70.00 %	查看
软件开发3_ED_99	开发组	10.10.10.40	工位C26_6柱子上壁挂	65.00 %	查看
软件开发8_8D_61	开发组	10.10.10.25	工位C15_4上吸顶	64.00 %	查看
展厅1_39_10	会议室	10.10.10.46		63.00 %	查看
软件开发4_F0_6A	开发组	10.10.10.4	工位C23_9上吸顶	62.00 %	查看
软件开发5_15_CF	开发组	10.10.10.35	工位C22_1旁边的墙上壁挂	62.00 %	查看
客服组48_CA临时替换2	客服组	10.10.10.18	工位C31_7顶上	60.00 %	查看

环境信道利用率

环境信道利用率代表接入点所观测到的当前信道的繁忙程度，是接入点自身收发包所占用的信道比例和其它无线节点收发包所占用的信道比例之和。

自身信道利用率

自身信道利用率代表接入点自身由于收发包所占用的信道比例。

重传率

重传率越高，代表无线网络数据的丢包越严重。

误码率

在一定时间内收到的数字信号中发生差错的比特数与同一时间所收到的数字信号的总比特数之比。

同频干扰

当前无线接入点周围，与该接入点同信道的无线接入点的个数。

繁忙度

统计接入点当前的用户数、会话数、流量等信息，生成的 TOP N 排行信息。

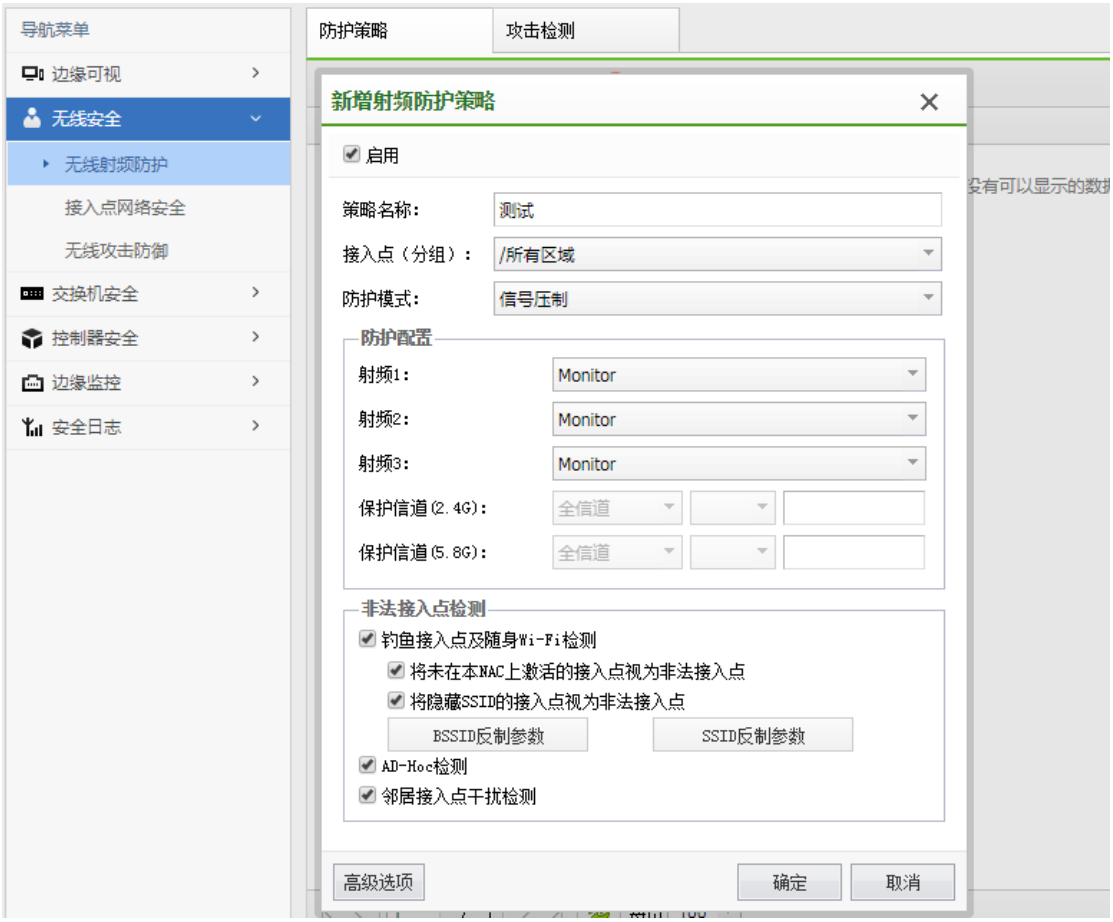
4.15.1.5.2. 历史数据分析

可以查询单个接入点的流量、用户、会话数、信道利用率、噪声值等历史数据信息，单个终端的传输速率、信号强度、通信质量等历史数据信息。

4.15.2. 无线安全

4.15.2.1. 无线射频防护

4.15.2.1.1. 防护策略



1、钓鱼接入点检测

可以按一个或多个接入点分组划分出一个区域保护这个区域内的射频信号不被其他 ap 的射频信号干扰。

2、钓鱼接入点检测

网络中未经授权或者有恶意的 AP，它可以是私自接入到网络中的 AP、未配置的

AP、攻击者操作的 AP。这些 AP 上面部署了和无线控制上面有相同或是相似 SSID 的无线网络，终端用户接入这些 SSID 的无线网络之后，账号等一些隐私信息可能会被窃取。

配置参数可以配置需要检测的 SSID、BSSID，其中 SSID 是进行相似或者相同的检测，BSSID 是进行完全匹配检测。

配置例外是指将 SSID 或 BSSID 加入白名单，不进行加入黑名单、反制的操作。

3、非法 AD-Hoc

把无线客户端的工作模式设置为 Ad-hoc 模式，Ad-hoc 终端可以不需要任何设备支持而直接进行通讯。

4、邻居接入点干扰检测

和钓鱼 AP 类似。区别在于这一类 AP 通常不是恶意的，只是检测到的信号强度超过一定阈值

4.15.2.1.2. 攻击检测

1、泛洪攻击（Flooding 攻击）

无线控制器在短时间内接收大量同种类型的报文，将导致系统资源被大量占用，可能无法处理无线用户的数据报文。启用泛洪攻击检测可以识别此类攻击，并自动将发起攻击的终端 MAC 地址添加到黑名单，一段时间内禁止接入无线网络。

2、欺骗攻击

欺骗攻击是指攻击者假冒其他设备/终端的名义发送报文。例如：假冒无线接入点的身份，向无线客户端发送解除认证的报文，导致无线终端断开无线连接。启用欺骗攻击检测可以识别此类攻击，将发起攻击的终端 MAC 地址添加到黑名单，一段时间内禁止接入无线网络。

3、BSSID 冲突检测

BSSID 冲突检测是指检测到环境中 BSSID 地址冲突，可能会造成无线终端接入到有冲突的 BSSID 的 AP，会造成网络掉线，丢包等不可预知的情况。

4.15.2.2. 接入点网络安全

接入点网络安全是针对 AP 端做的防护措施。该界面分为 DHCP 防御和二层防御，以下分别说明。

4.15.2.2.1. DHCP 防御

启用接入点收信人的 DHCP 服务器功能，AP 只转发受信任的 DHCP 响应，屏蔽不合法的 DHCP 服务器，适用于本地转发。每个接入点最多只支持 10 条受信任 DHCP 服务器。

4.15.2.2.2. 二层防御

支持网关 ARP 防御功能，以及无线用户隔离，确保网络安全。

网关智能识别：智能识别网关，如果所有终端都是静态 IP，此功能不生效。

开启 ARP 欺骗防御：开启此功能后，手动配置和智能识别的网关会被默认保护起来。开启无线用户隔离：禁止无线终端之前互相通信。

4.15.2.3. 无线攻击防御

该界面分为私设 IP 防御、DDOS 防御、扫描防御三项。以下分别说明。

4.15.2.3.1. 私设 IP 防御

禁止客户端使用静态 IP 地址

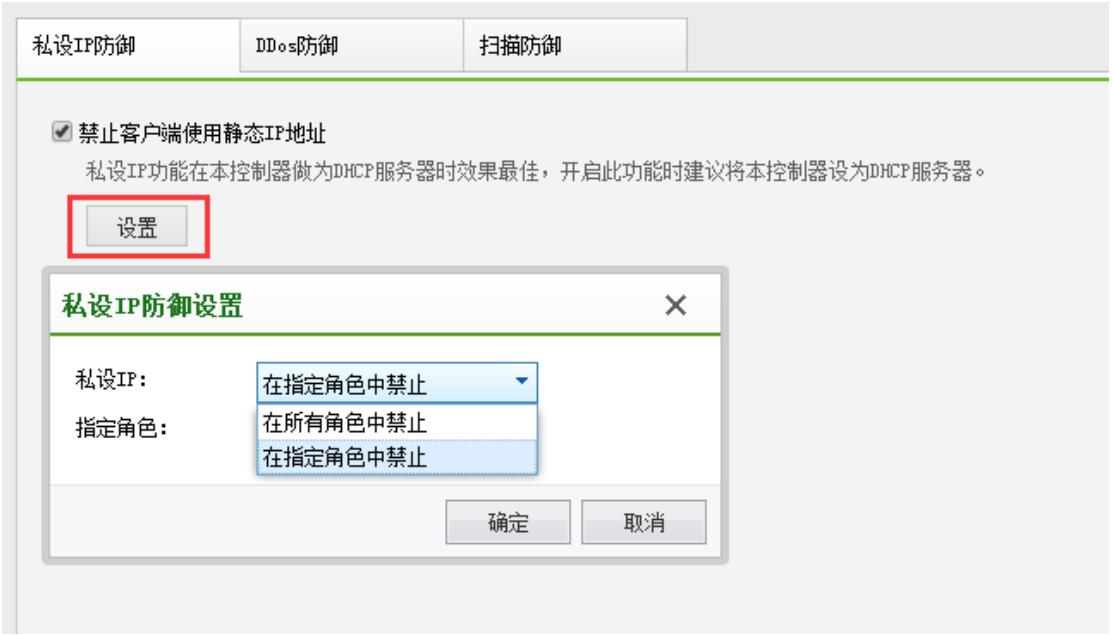
在绝大部分的无线网络部署中，无线客户端都使用 DHCP 方式获取 IP 地址、网关、DNS 等。因此，为了避免手动配置 IP 地址可能带来的 IP 冲突问题，系统提供了禁止配置静态 IP 地址的功能。启用此选项的额外好处是，可以阻止无线客户端进行 ARP 欺骗攻击。此选项仅支持集中转发的无线用户。

此功能的实现过程如下：

系统将持续监听无线客户端的 DHCP 分配过程数据包，并从 DHCP 报文中，获取无线客户端的 MAC 地址以及分配的 IP 地址，据依据此信息构建有效的 IP，MAC 对应关系数据库。

检测无线客户端发出的 ARP 数据包，检查 IP 与 MAC 地址对应关系的合法性，丢弃不合法的 ARP 包。

可以针对不同的角色选择性的配置该功能。



4.15.2.3.2. DDos 防御

DDoS 攻击在众多网络攻击技术中，是一种简单有效并且具有很大危害性的攻击方法。它通过各种手段消耗网络带宽和系统资源，使网络陷于瘫痪状态。在无线网络中，大部

分 DDoS 攻击行为并不是由用户故意发起的，而是由于计算机感染了病毒或恶意软件造成的。

DDoS 攻击防御模块通过统计无线客户端的数据包速率，连接数等信息，有效识别并阻挡无线客户端发起的 DDoS 攻击行为，降低对无线网络的影响。

4.15.2.3.3. 扫描防御

该功能可以防御网络中 ARP、IP、端口扫描攻击。

防御选项：防御 ARP 扫描，IP 扫描，端口扫描攻击，超过设置阈值的用户行为将被识别为扫描攻击。

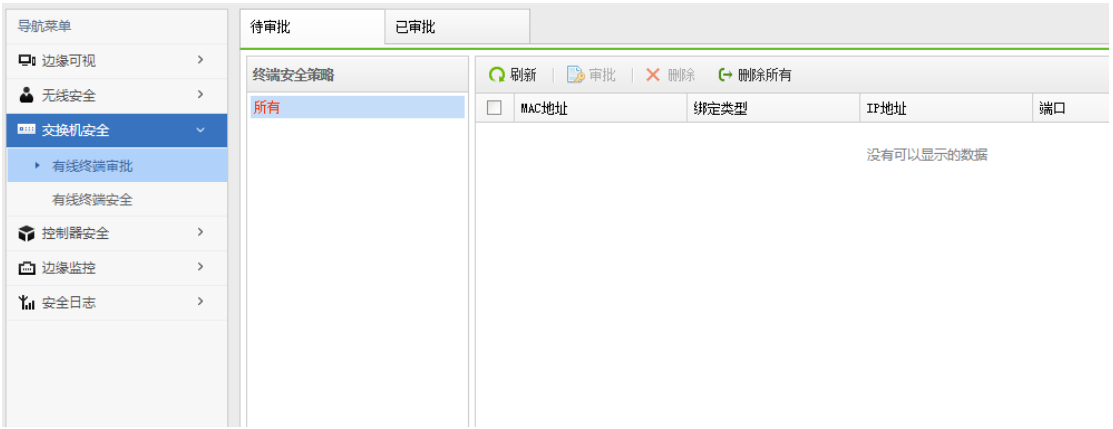
防御动作：可以将攻击者加入黑名单，并支持设置冻结的时间。

4.15.3. 交换机安全

4.15.3.1. 有线终端审批

4.15.3.1.1. 待审批

终端策略中的终端地址绑定功能与终端位置绑定功能可触发终端进入待审批列表，并阻塞流量；管理员可手动进行审批操作，以放通流量。

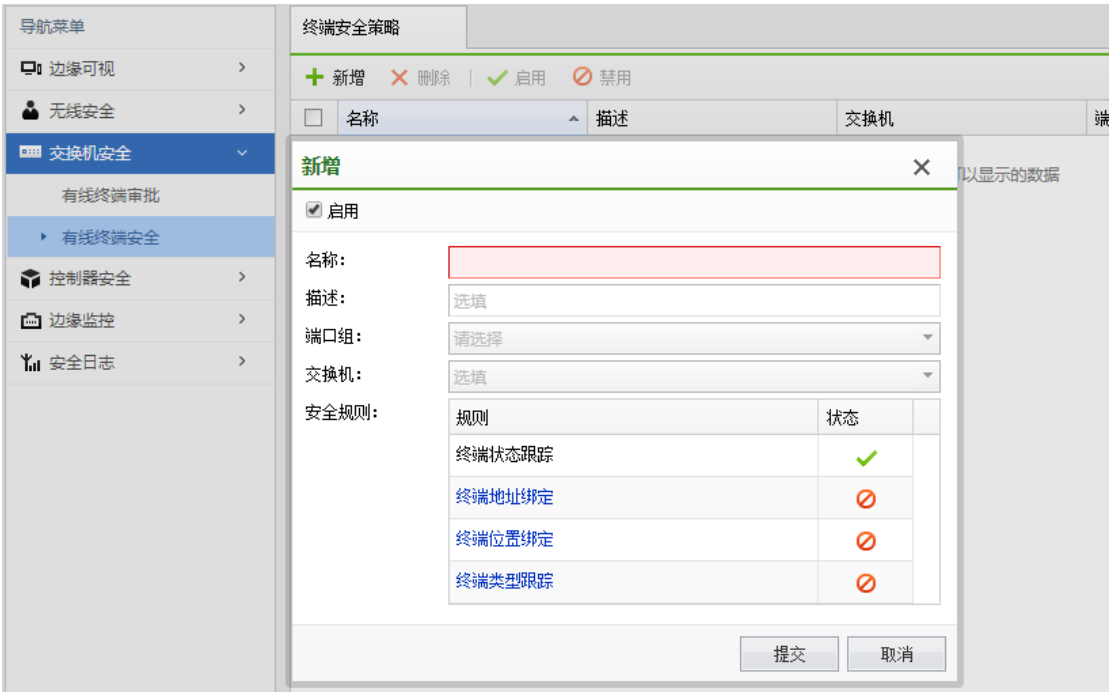


4.15.3.1.2. 已审批

已审批的终端对应关系进入已审批列表，并放通流量。默认老化时间为永不老化，支持配置自定义老化时间。

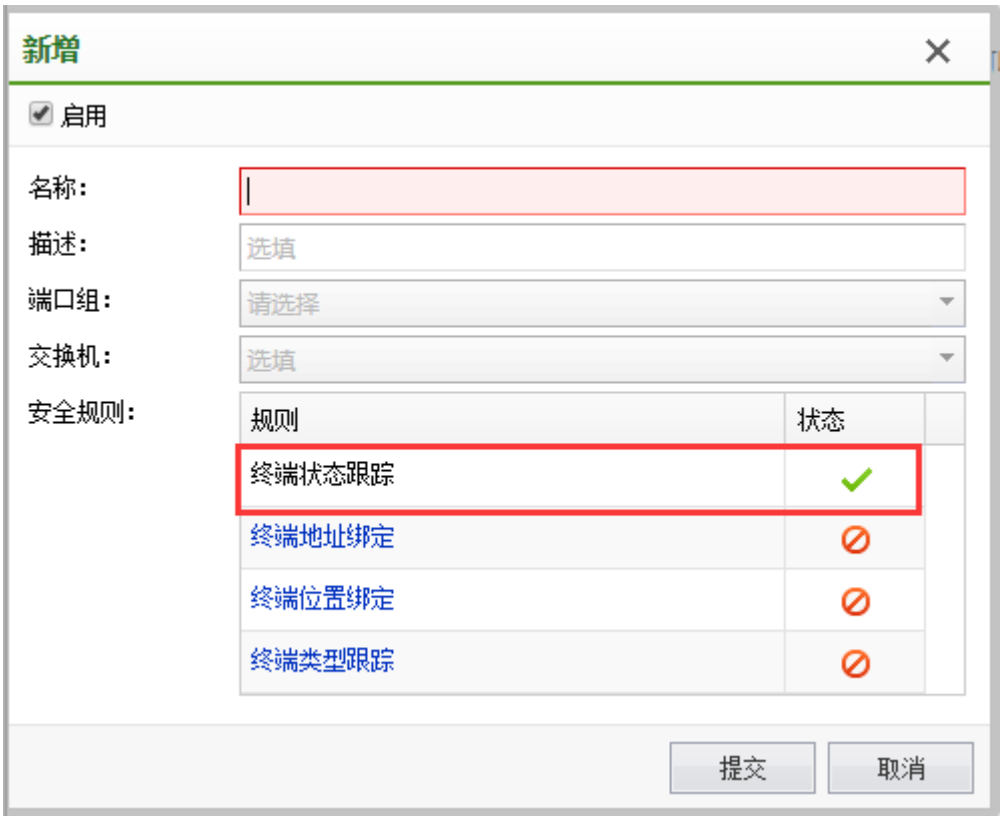
4.15.3.2. 有线终端安全

终端安全策略，是帮助用户管理、识别和跟踪其网络环境下的终端而建立的人性化功能，解决用户对网络安全的需求并为其提供了快捷有效的实现方法。



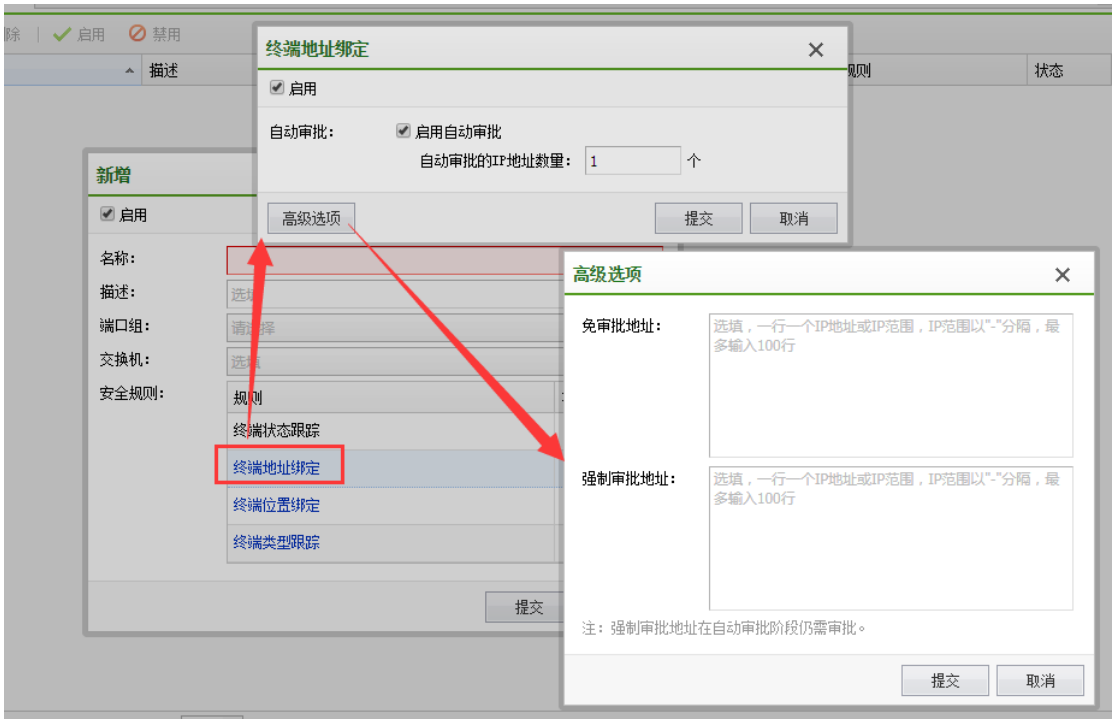
4.15.3.2.1. 终端状态跟踪

用于跟踪连接交换机端口的终端状态，包括在线、离线、类型等具体的信息并显示在状态页面。



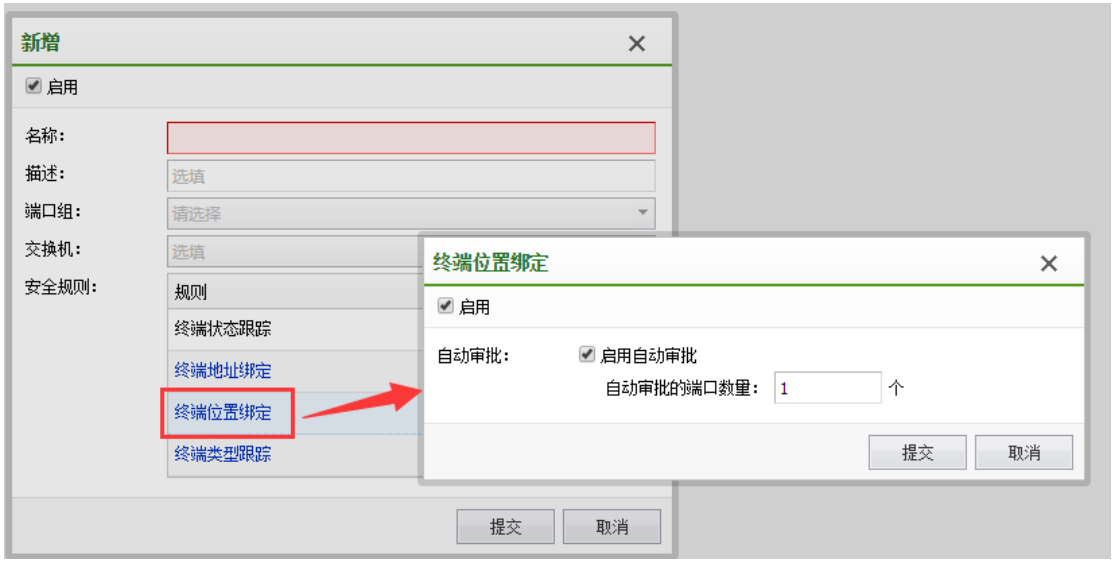
4.15.3.2.2. 终端地址绑定

用于绑定终端和 ip 地址，实现 IT 管理员对其网络环境下的 ip 地址的监管；可启用自动审批并设置审批数量来实现批量操作的自动化，也可手动审批；其中，自动审批的个数是包含已审批列表的终端对应关系个数。另有免审批和强制审批功能，免审批地址在更换 IP 地址时无需审批，强制审批地址在自动审批阶段仍需审批。



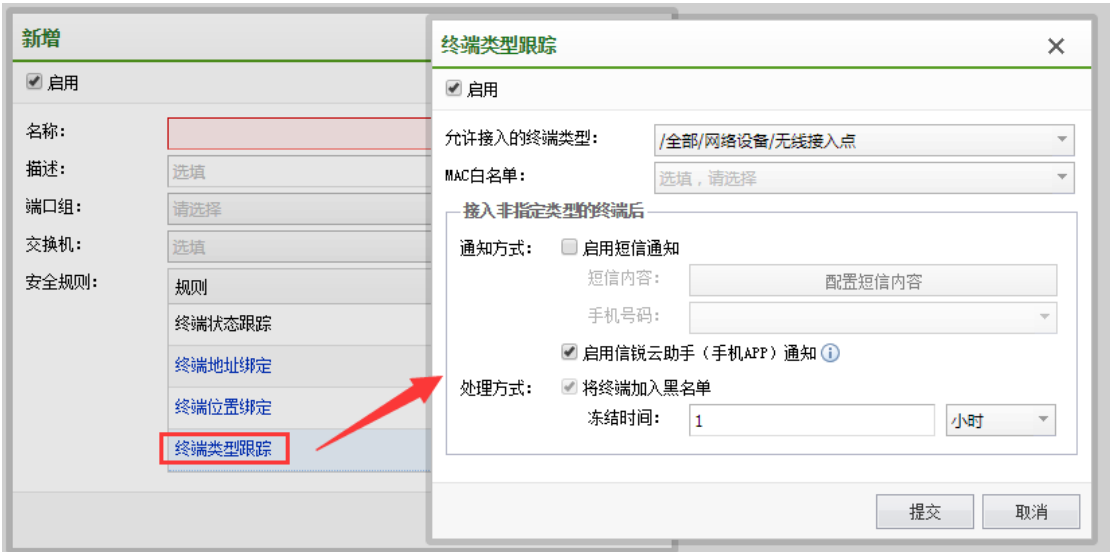
4.15.3.2.3. 终端位置绑定

用于绑定终端和端口，实现监管端口下联设备的功能；可启用自动审批并设置审批数量来实现批量操作的自动化，也可手动审批。



4.15.3.2.4. 终端类型绑定

用于跟踪下联终端的类型状态，帮助用户实时获取下联终端的各种信息；可限制接入的设备类型并通知用户。



4.15.4. 控制器安全

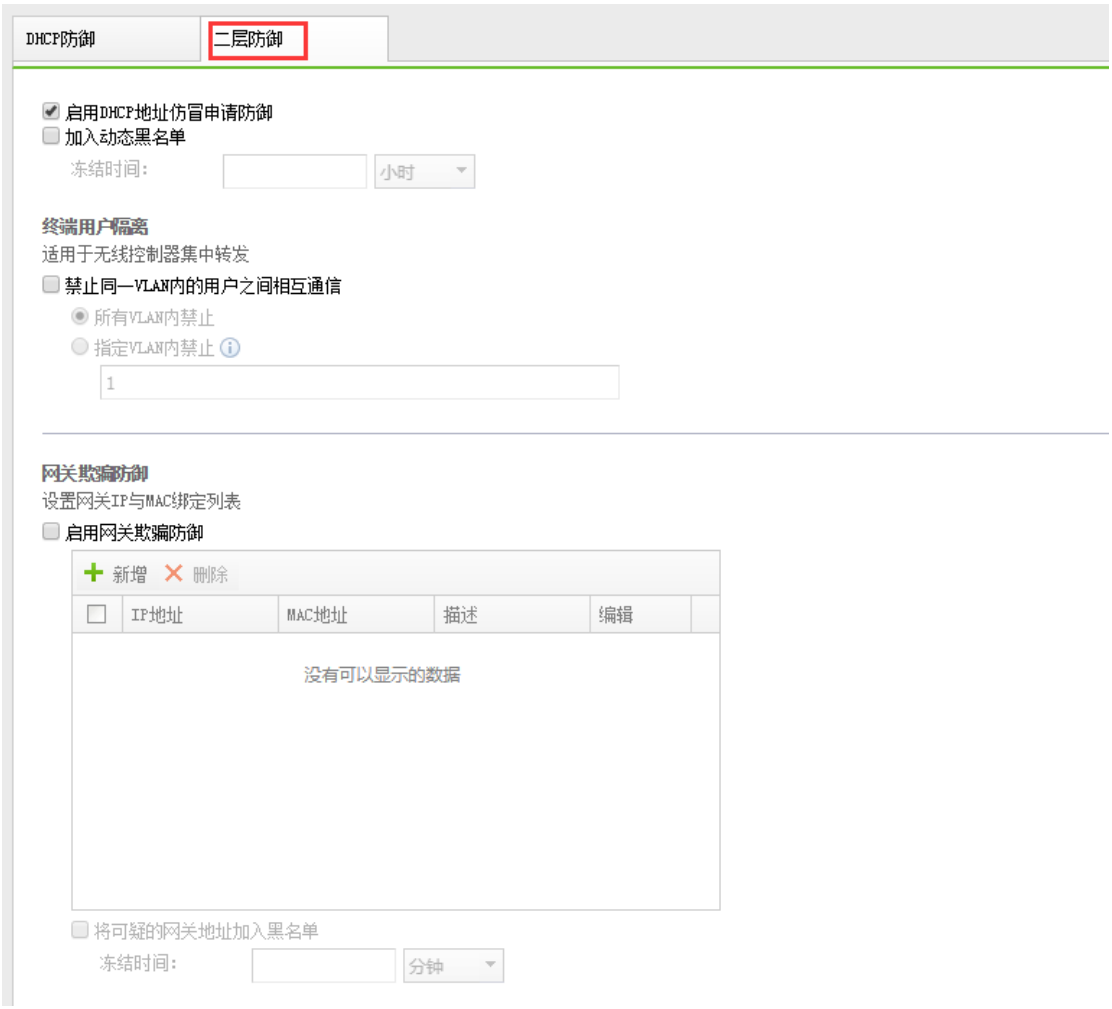
4.15.4.1. 控制器网络安全

4.15.4.1.1. DHCP 防御

启用控制器受信任的 DHCP 服务器功能，可以让 AP 下面的无线终端用户，只能收到受信任的 DHCP 服务器的 IP 分配请求，这样可以防止网络中存在伪造的 DHCP 服务器给无线终端分配 IP 地址，造成上不了网的情况。该功能在无线 2.2 版本前仅在集中转发是生效，从 2.2 版本后，集中转发与本地转发都生效。


导航菜单
边缘可视
无线安全
交换机安全
控制器安全
控制器网络安全
边缘监控
安全日志
DHCP防御
二层防御
启用控制器受信任的DHCP服务器
只转发受信任的DHCP响应，屏蔽不合法的DHCP服务器，适用于集中转发（本机的DHCP服务器已默认添加到受信任列表中）
新增
删除
启用
禁用
VLAN
IP地址
MAC地址
状态
编辑
没有可以显示的数据

4.15.4.1.2. 二层防御



1、DHCP 请求泛洪攻击防御

默认开启，防御 DHCP 泛洪攻击行为，防止 DHCP 地址池被耗尽。

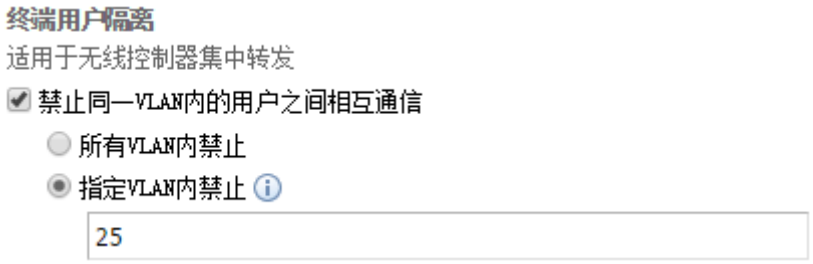
2、终端用户隔离

通常情况下，同一 VLAN 的用户间是可以相互通信的，但在无线接入的环境下，移动终端间相互通信，存在较大安全隐患。例如部署用于公众上网的无线网络中，多个无线用户之间没有直接通信的需求，在此环境下，启用此选项可以减少无线终端间的报文，提高了无线网络性能，同时提高了安全性。还有避免某些感染了病毒的终端传播病毒的风险。

禁止同一 VLAN 内的用户之间相互通信后， 只要是通过同一无线接入点接入的，所有

VLAN 相同的无线用户间将不能相互通信。这样不仅可以降低了安全风险，还可以减少移动终端间的广播报文。

不同 VLAN 间是否能相互通信，由第三方路由设备控制，本设备暂不支持。通常不同 VLAN 间默认是不能通信的。



3、网关欺骗

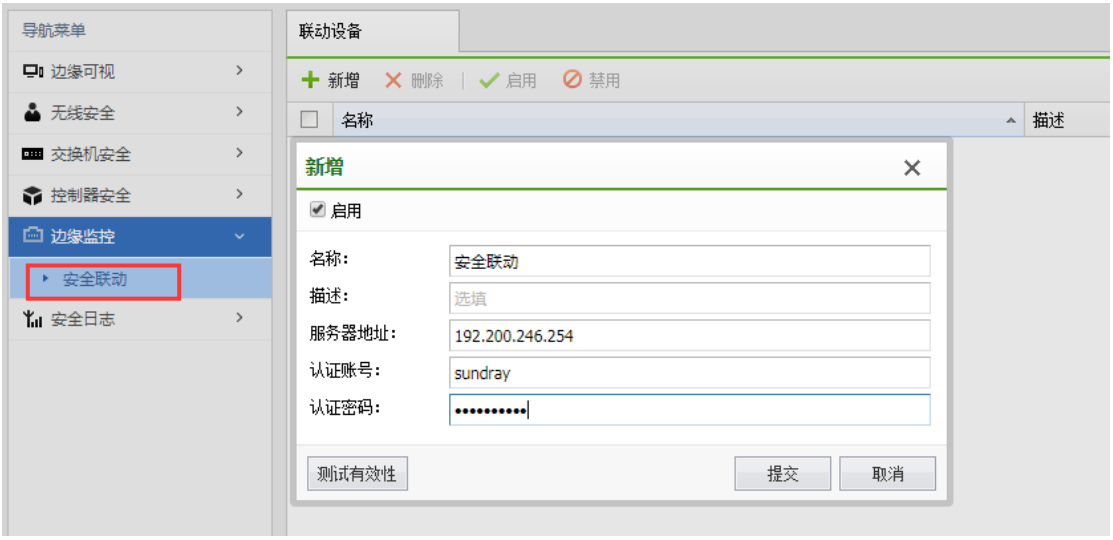
攻击者通过伪造 ARP 报文，截获原本发向网关的报文，对网络安全构成威胁。网关防御欺骗防御支持将配置网关 mac 和 ip 的绑定关系，可以有效遏制这种攻击。适用于集中转发环境。

注意：IP、MAC 中其中一个出现在配置中，并不满足对应关系，将被识别为网关欺骗攻击。

4.15.5. 边缘监控

4.15.5.1. 安全联动

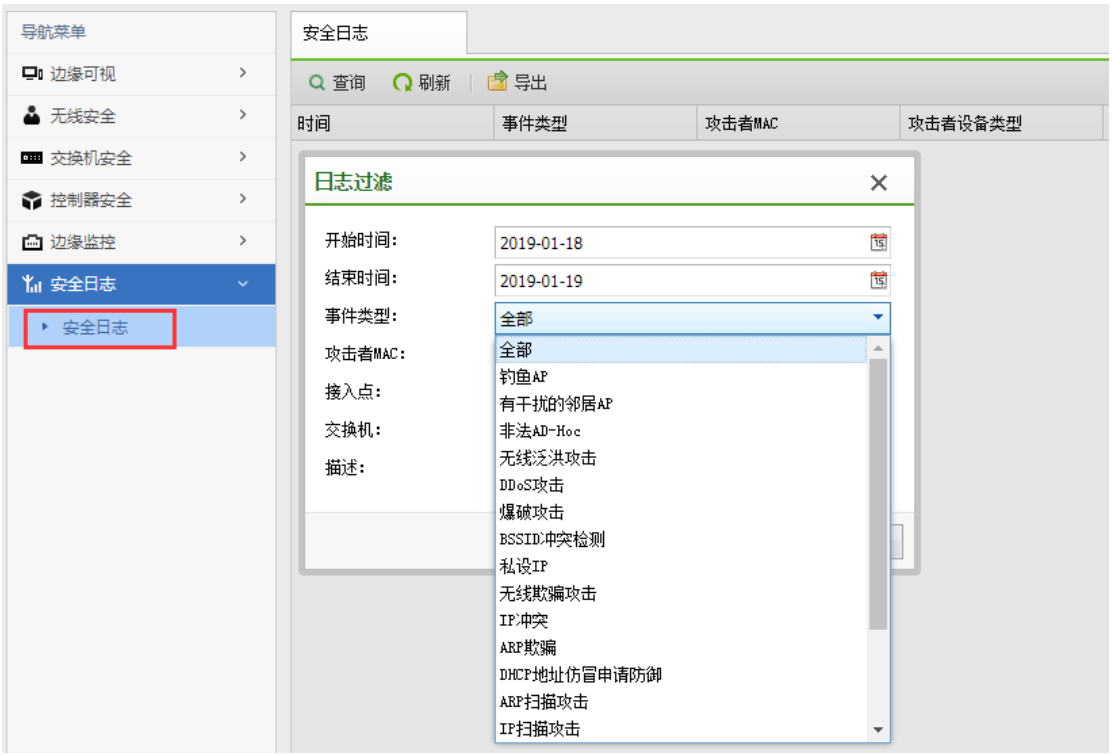
支持联动深信服安全设备进行用户安全可视化和内网边缘安全管理。



4.15.6. 安全日志

4.15.6.1. 安全日志

记录所有的检测到的无线网络安全事件，并记录检测到的结果。



安全日志

查询 刷新 导出

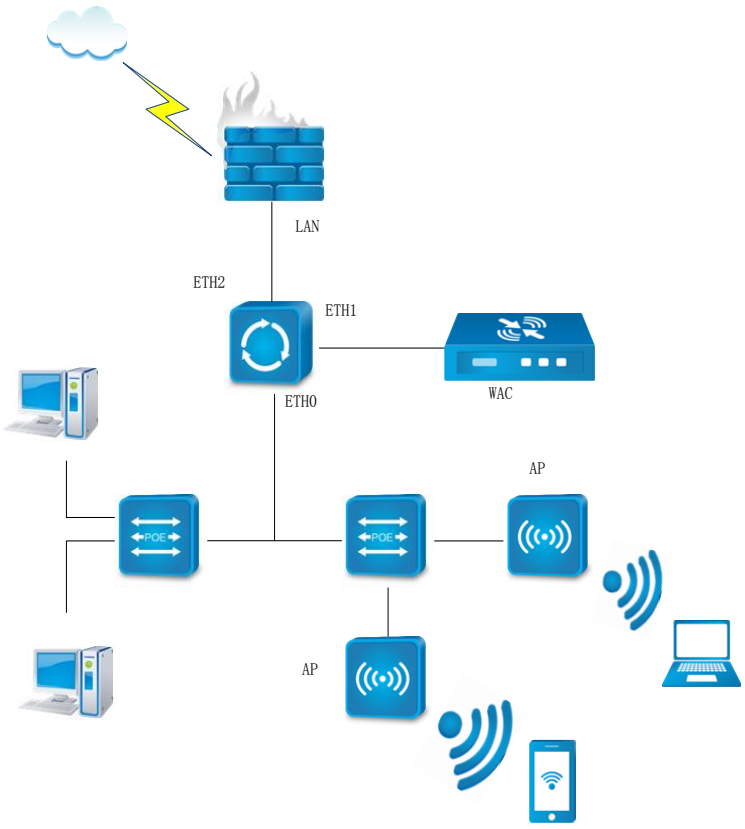
时间	事件类型	攻击者MAC	攻击者设备类型	发现后动作	描述	设备
2019-01-14 20:22:30	钓鱼AP	D4-68-BA-88-D3-D7	接入点	告警并反制	检测出钓鱼AP: zz_2003_localaccount(D4-···	
2019-01-14 20:22:28	钓鱼AP	D4-68-BA-08-D3-D7	接入点	告警并反制	检测出钓鱼AP: zz_2003_localaccount(D4-···	
2019-01-14 20:22:28	钓鱼AP	D4-68-BA-2B-BA-58	接入点	告警并反制	检测出钓鱼AP: zz_2003_ercode(D4-68-BA-···	
2019-01-10 17:15:55	有干扰的邻居AP	D4-68-BA-8E-8D-61	接入点	告警并反制	检测出高强度邻居AP: Guest(D4-68-BA-8E-···	
2019-01-10 17:15:48	有干扰的邻居AP	D8-55-A3-DA-BB-CC	接入点	告警并反制	检测出高强度邻居AP: ES_8889(D8-55-A3-D···	
2019-01-10 17:15:48	有干扰的邻居AP	A8-0C-CA-6A-6B-F4	接入点	告警并反制	检测出高强度邻居AP: 00_3.7.9.2_lz14(A8···	
2019-01-10 17:15:24	有干扰的邻居AP	A8-0C-CA-B2-6B-F4	接入点	告警并反制	检测出高强度邻居AP: 00_3.7.9.2_lz7(A8-···	
2019-01-10 17:15:24	有干扰的邻居AP	10-0F-0E-20-11-05	接入点	告警并反制	检测出高强度邻居AP: 1ttttt(10-0F-0E-20···	
2019-01-10 17:15:18	有干扰的邻居AP	D4-68-BA-01-01-01	接入点	告警并反制	检测出高强度邻居AP: test01_IPv6_psk(D4···	
2019-01-10 17:15:18	有干扰的邻居AP	70-3A-73-0F-36-01	接入点	告警并反制	检测出高强度邻居AP: zt_test_465(70-3A-···	
2019-01-10 17:15:18	有干扰的邻居AP	D4-68-BA-0C-01-CC	接入点	告警并反制	检测出高强度邻居AP: test01_IPv6_open(D···	
2019-01-10 17:15:18	有干扰的邻居AP	A8-0C-CA-5A-6B-F4	接入点	告警并反制	检测出高强度邻居AP: 00_3.7.9.2_lz12(A8···	

第5章 案例集

5.1. 设备部署配置案例

5.1.1. 部署案例

用户网络是复杂跨三层的网络环境，购买 WLAN-NAC 设备以单臂部署在 3 层交换机上，实现对内网的所有无线 AP 进行集中管控和认证，通常部署 WLAN 时，部署的 AP 个数会非常多，下面部署案例中，都只以 2-3 个 AP 作为范例表示。图中，NAC 以单臂模式部署在客户网络 3 层交换机上，3 层交换机是内网 PC 的网关，如下图所示：

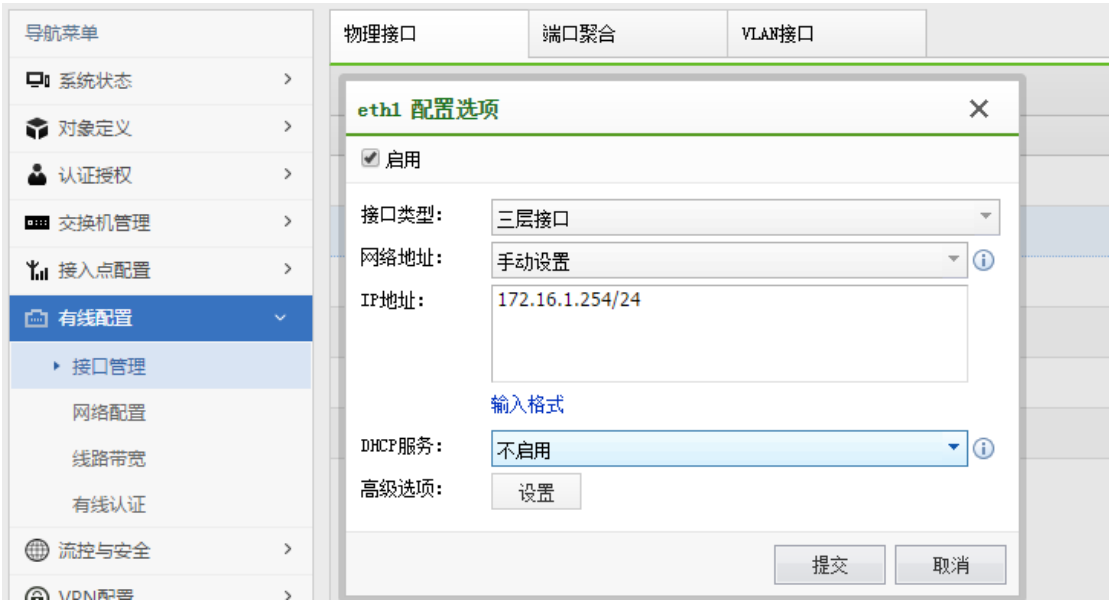


网络环境：三层交换机 eth0 口：192.168.1.1/24,eth1 口：172.16.1.1/24，eth2:10.0.0.1/24，FW：lan 口 10.0.0.2/24，NAC：172.16.1.254/24

第一步：通过管理口(ETH0)的默认 IP 登录设备。管理口的默认 IP 是 10.252.252.252/24，

在电脑上配置一个相同网段的 IP 地址，通过 https://10.252.252.252 登录设备。

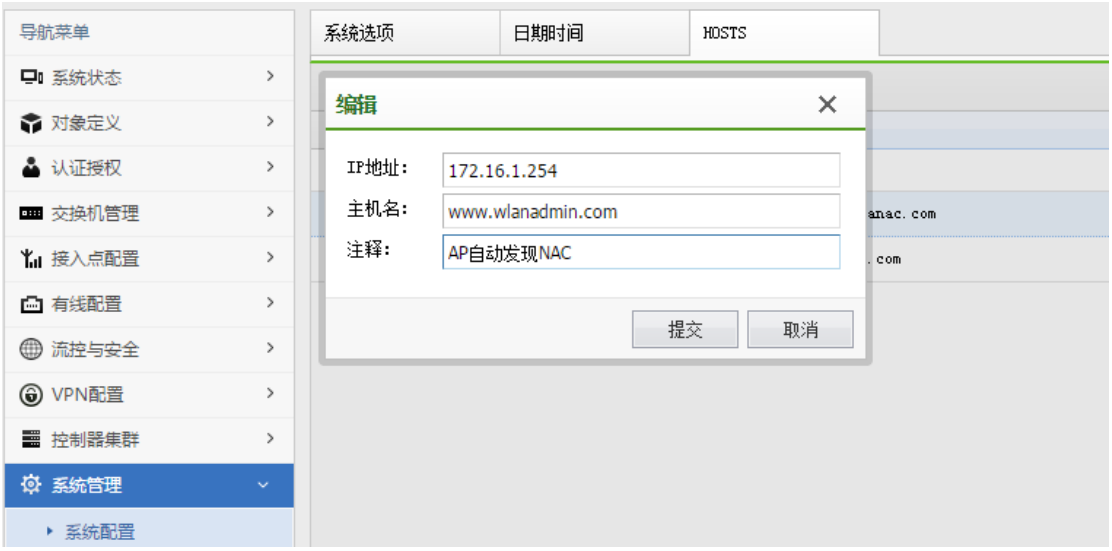
第二步：配置 NAC 可以上网，通过『有线配置』→『接口管理』，点击需要设置成外网接口的接口，如 eth1，出现以下页面：



配置 eth1 接口 IP 地址为：172.16.1.254/24

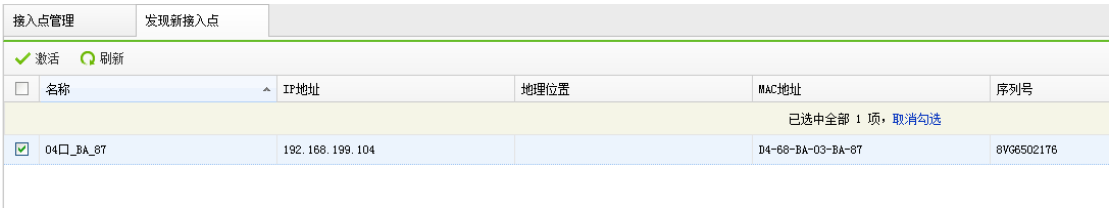
第三步：配置 NAC，让 NAC 可以正常上网，到【有线配置】-【网络配置】处添加 8 个 0 的静态路由

第四步：在 NAC 上配置 HOSTS，并启用 DNS 代理，当 AP 获取解析到的默认域名 www.wlanadmin.com 为 NAC 的 IP 地址时，AP 会自动发现 NAC。在【系统管理】-【系统配置】-【HOSTS】这里配置 NAC 的 IP 地址 172.16.1.254 的主机名为：www.wlanadmin.com。并在【有线配置】-【网络配置】-【DNS】配置 DNS 地址，并且启用 DNS 代理。



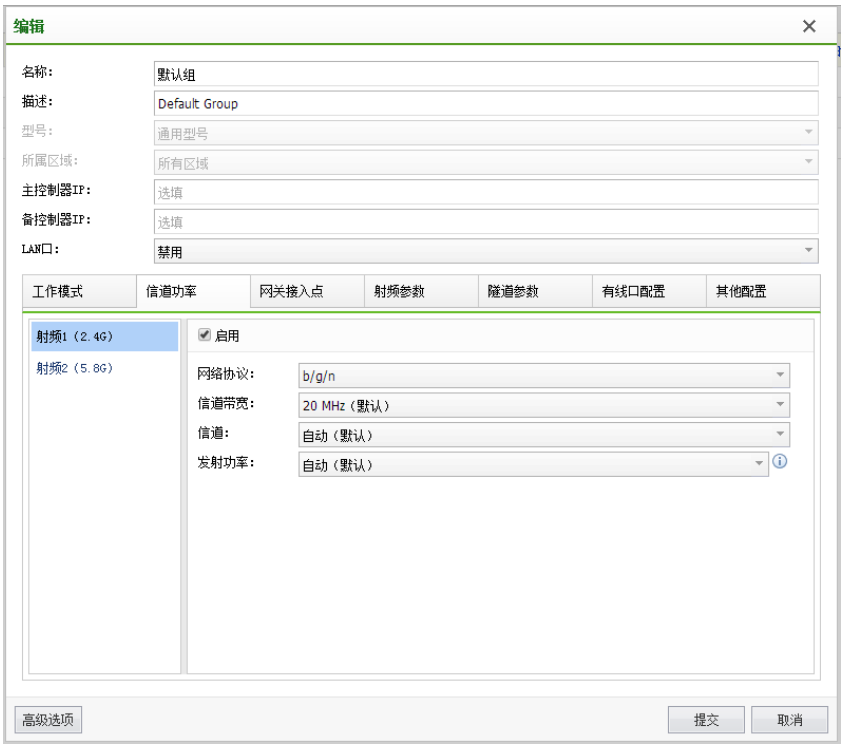
需要在 3 层交换机启用 DHCP，并且对配置分发的 DNS 服务器为 NAC 的 LAN 口 IP 地址：172.16.1.254。

第五步：激活 AP，当 AP 第一次部署在网络中时，默认会通过 DHCP 请求获取 IP 地址，会生成默认网关，并且获取到 DNS。这是 AP 会默认请求域名 www.wlanadmin.com，会向解析到的 IP 发起连接协议，这里 NAC 上就可以在【接入点配置】-【无线接入点】-【发现新接入点】处激活 AP。（因环境原因，截图中的 IP 地址应该为 192.168.199.104/24 网段的 IP 地址）



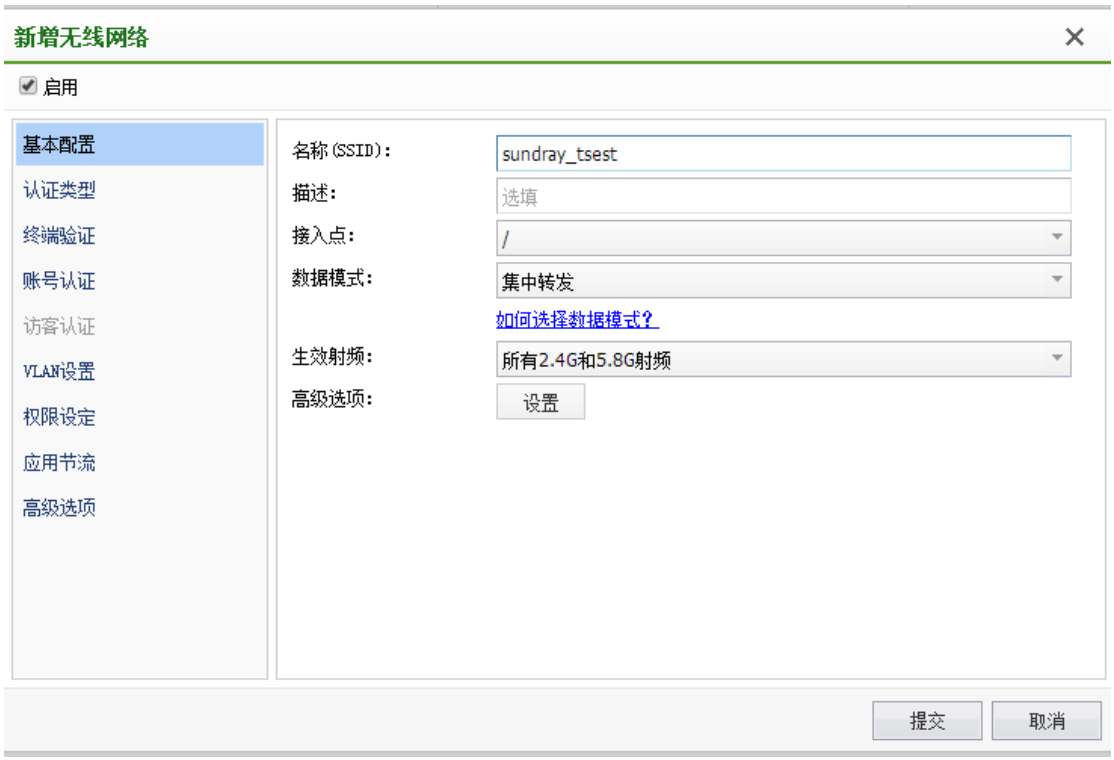
激活 AP 时，选择 AP 的所属于组为“默认组”，网络地址配置为：自动获取，控制器 IP 和控制器域名都不需要填写。

第六步：编辑默认组，在【接入点管理】-【无线接入点】，点击【默认组】，编辑默认组的工作模式和信道功率，工作模式选择为 normal,信道功率同时启用 2.4G 频段和 5.8G 频段，其余为默认。

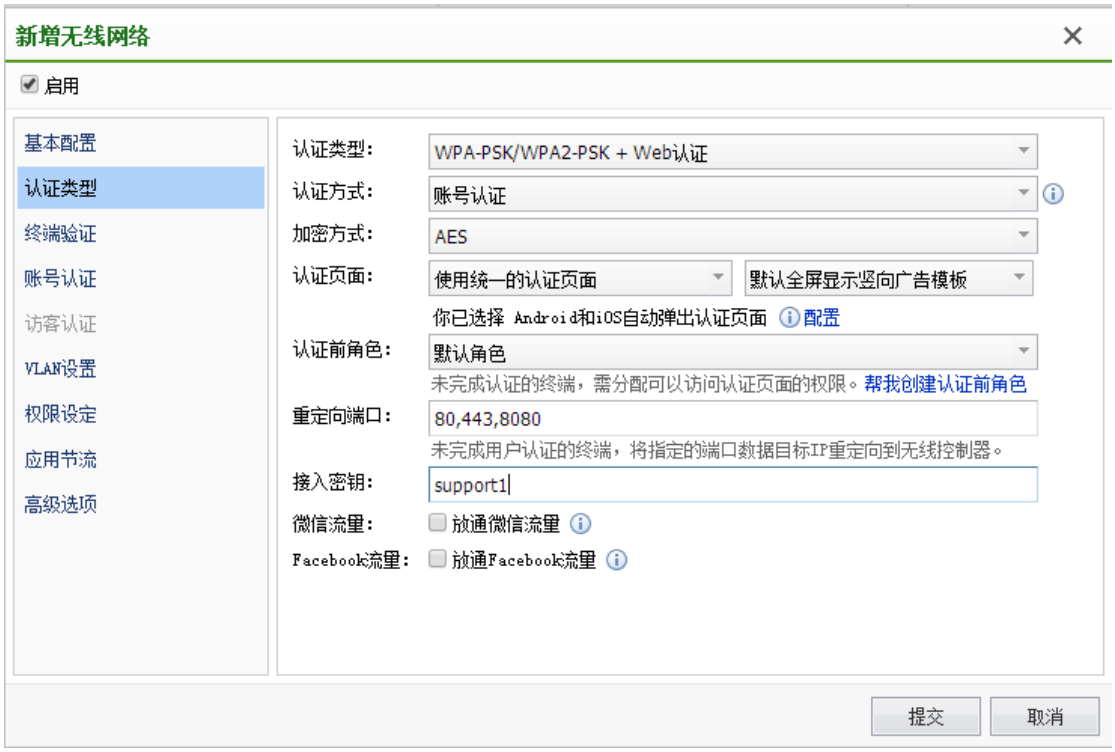


第七步：新增无线网络“sundray_test”并选择该网络匹配的 AP 组为默认组，以及设置该无线网络的认证方式。数据转发模式选择为“本地转发模式”。设置频段选择“所

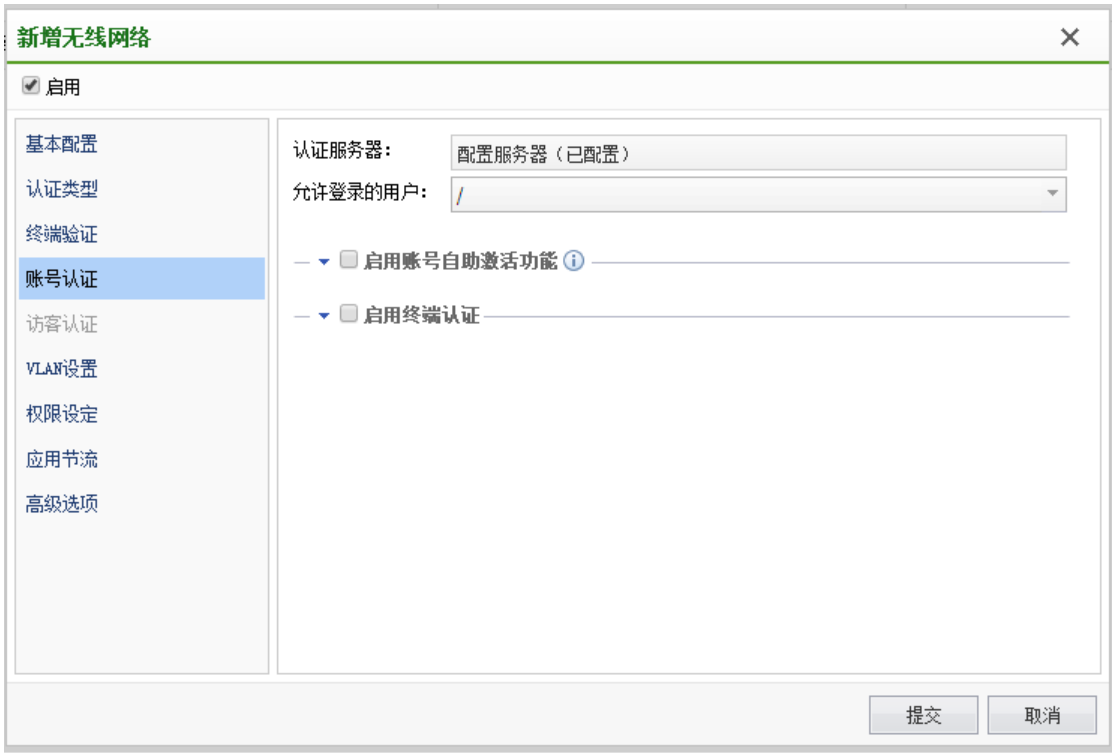
有”。



认证类型选择为：“WPA-PSK/WPA2-PSK+ Web 认证”，并设置接入密钥为“support1”。

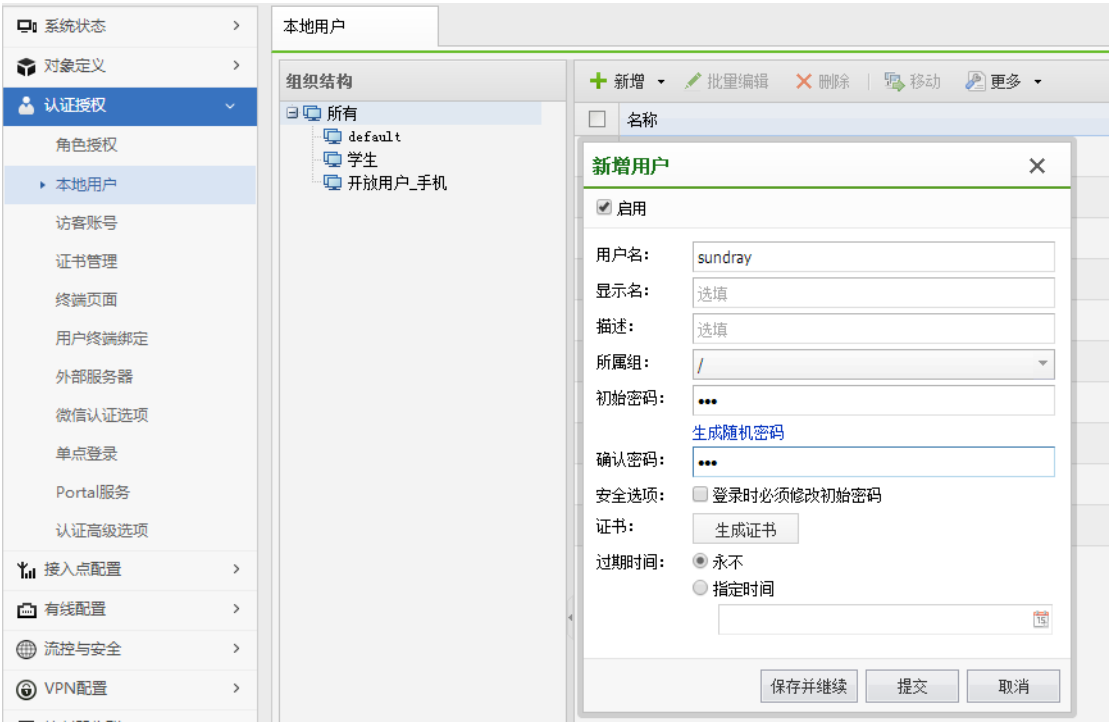


终端验证不启用，设置用户认证为“本地用户”方式，允许登录的用户组为所有。



VLAN 配置和角色分配这个案例默认就可以了，暂时不需要配置。

第八步：新增本地用户，当无线终端接入 WEB 认证时，需要输入本地用户名和密码才可以正常上网。



第6章 附录

6.1. SUNDRAY 设备升级系统的使用

SUNDRAY 设备升级系统可用于对设备进行内核版本升级和备份恢复设备配置。在设备出现致命错误时，也可通过 SUNDRAY 设备升级系统把设备恢复到出厂状态。同时，SUNDRAY 设备升级系统还可以启动技术支持工具来检查系统网口工作状态，路由等配置信息以及更改网口工作模式等。

SUNDRAY 设备升级系统为绿色版软件，解压后即可使用，解压文件里包含一个文件夹和一个主程序，界面如下：

双击打开主程序的主界面，界面如下：

『设备 IP 地址』：连接的 SUNDRAY 设备的 IP 地址，格式为 IP：端口，也可以直接输入 IP 地址进行访问，则默认连接的是该 IP 地址的 51111 端口。

『管理员密码』：WLAN 设备的默认密码为 dlanrecover 或者是与 WLAN 设备的控制台密码保持一致，与所连接的 WLAN 设备的版本有关。

『查找设备』：通过点击查找设备来搜索局域网内部的 SUNDRAY 设备。

输入 SUNDRAY 设备的 IP 地址以及管理员密码后，点击连接即可连接到设备进行系统升级、恢复默认配置等操作，界面如下：

『当前设备信息』：用于显示连接的 SUNDRAY 设备的版本信息以及连接的 IP 地址。

『设备升级』：对当前连接的 SUNDRAY 设备进行升级操作，包括在线升级和从本地加载升级包进行升级。

在线升级：

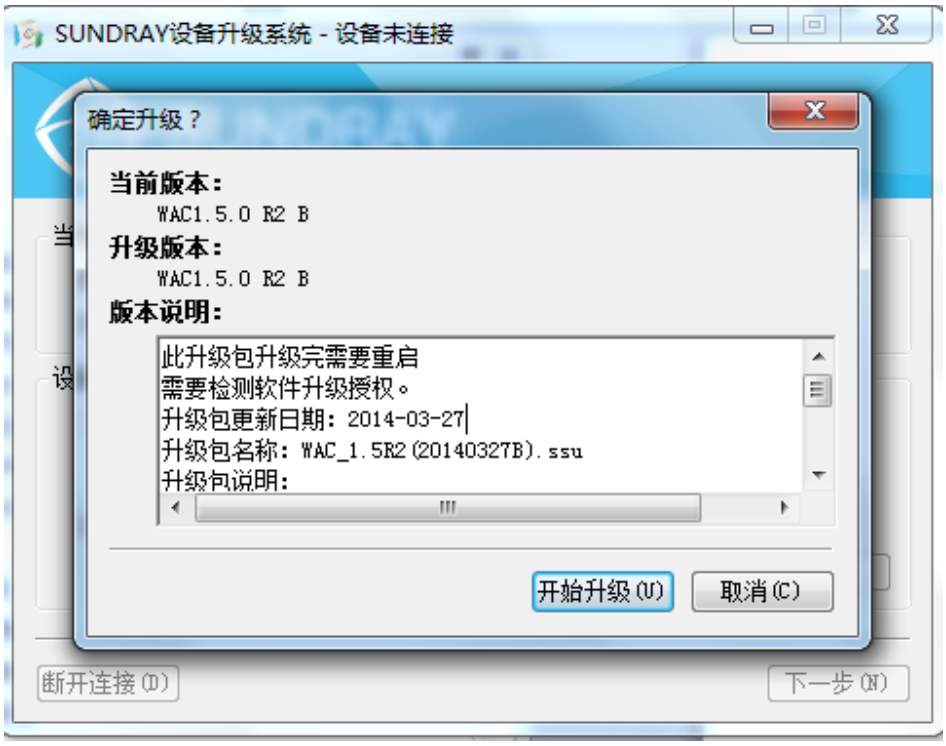
选择在线升级，点击选择版本，SUNDRAY 设备升级系统会自动判定设备当前版本支持升级到哪个版本，并自动列出可以支持升级的版本信息，选择期望升级到的版本，点击确定后，系统会自动从服务器上下载升级包进行升级操作。

1.使用 SUNDRAY 设备升级系统进行在线升级时，要求所连接的 SUNDRAY 设备能够正常上网，否则将不能进行在线升级。

2.SUNDRAY 设备的某些版本不支持在线升级功能，具体请联系信锐技术客户服务中心确认。

从本地加载升级包：

选择从本地加载升级包，点击浏览，选择下载到本地的相应升级包，然后点击下一步，显示当前升级包的基本信息，确认无误后，点击开始升级进行升级操作，界面如下：

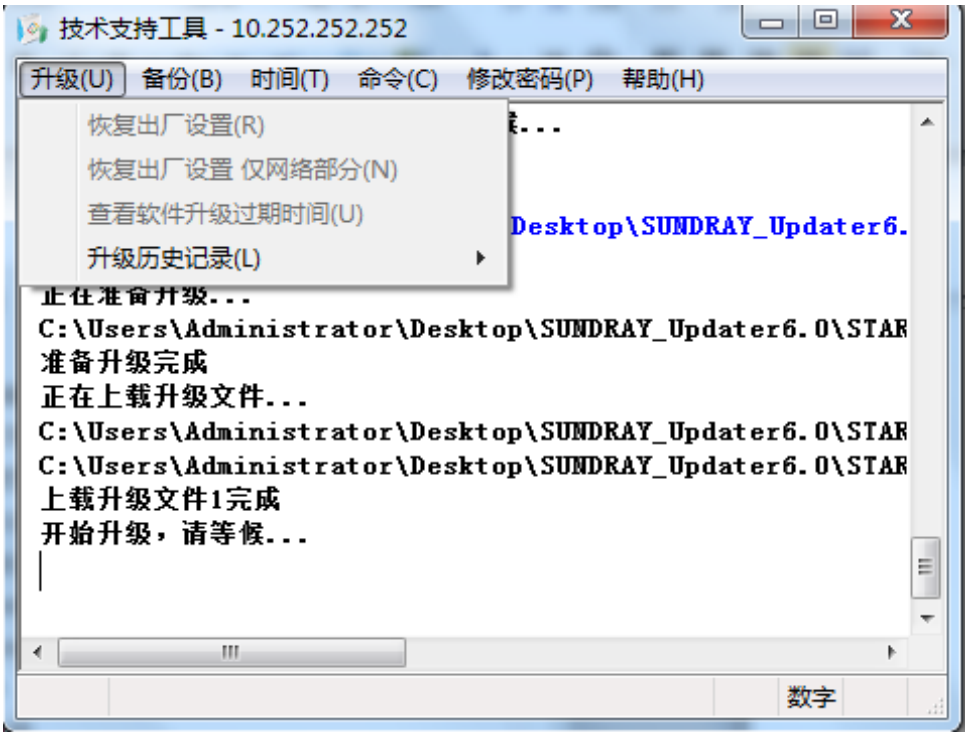


升级完成后，设备升级状态里会显示“升级成功”，界面如下：

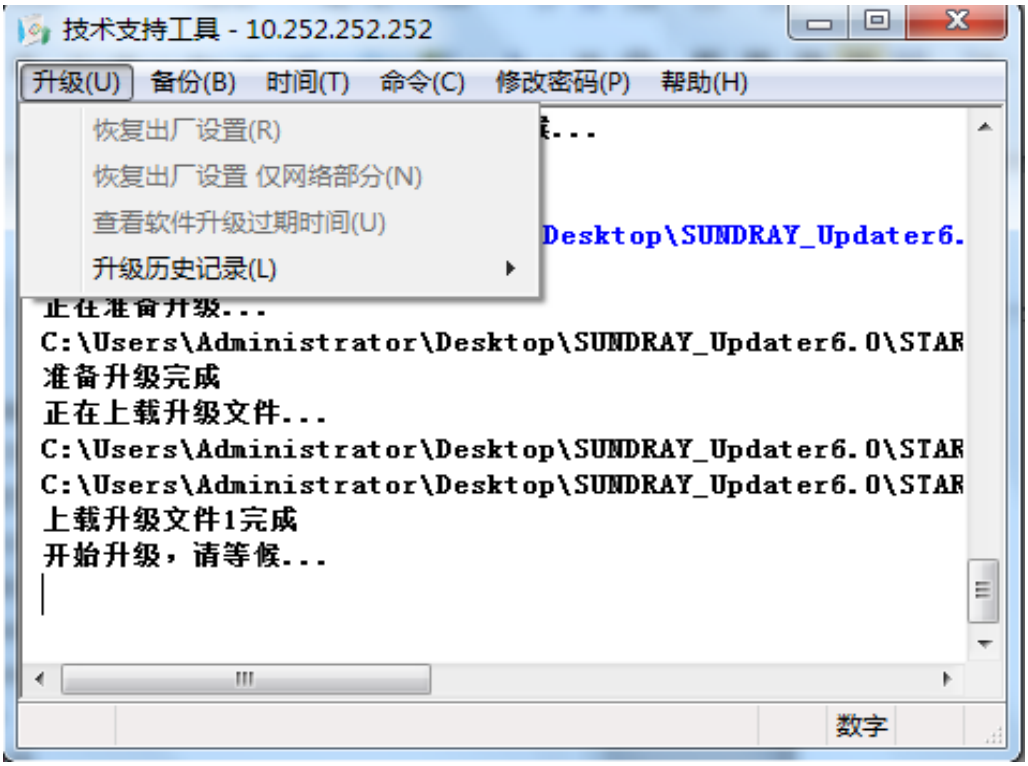
1．升级具有一定的风险，如升级不当会导致设备损坏。请勿自行升级。如需升级请联系信锐技术客户服务部。

启动技术支持工具：

SUNDRAY 设备升级系统连接到 SUNDRAY 设备后，可以按 F10 或 Ctrl+Shift+F10 启动技术支持工具。技术支持工具有『升级』、『备份』、『时间』、『命令』、『修改密码』和『帮助』几个菜单，下面分别介绍它们的功能。



『升级』：包括恢复出厂设置，恢复出厂设置仅网络部分，查看软件升级过期时间和升级历史记录。如下图：



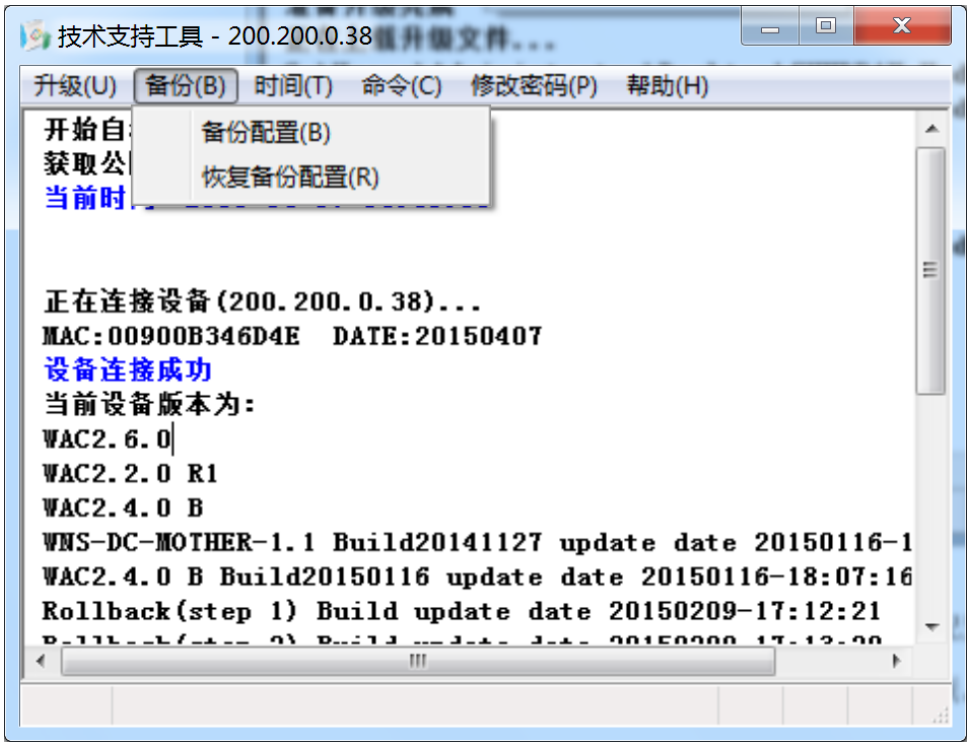
[恢复出厂设置]：用于将 SUNDRAY 硬件设备恢复到默认配置，需要通过加载升级包将设备恢复出厂设置。

[恢复出厂设置仅网络部分]：只能在没有连接到设备时才能使用。会将设备的网络配置恢复到默认出厂配置，此操作是通过广播包发送命令进行操作的，会对局域网内的所有 SUNDRAY 硬件网关生效，有一定危险性，请勿擅自点击操作。

[查看软件升级过期时间]：检测当前网关是否处于升级服务有效期内。若不在升级服务有效期内，则不能升级，需要购买相应授权才能升级。

[升级历史记录]：用于查看当前设备的以往升级历史，或者查看或清除本地的历史升级记录。

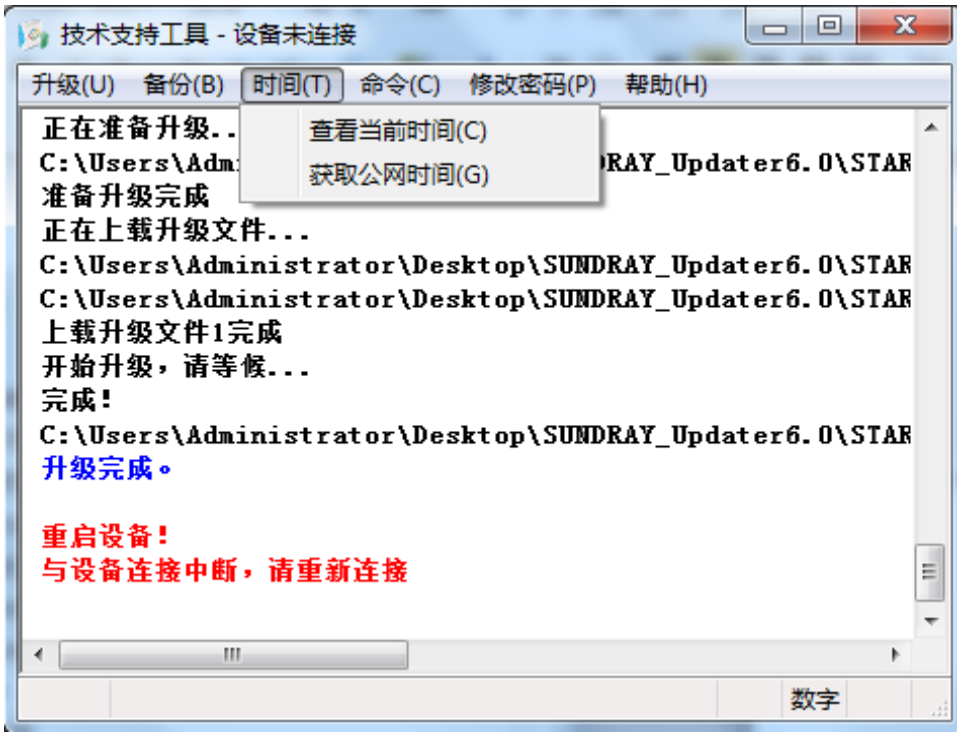
『备份』：包括备份配置、恢复备份配置选项，如下图：



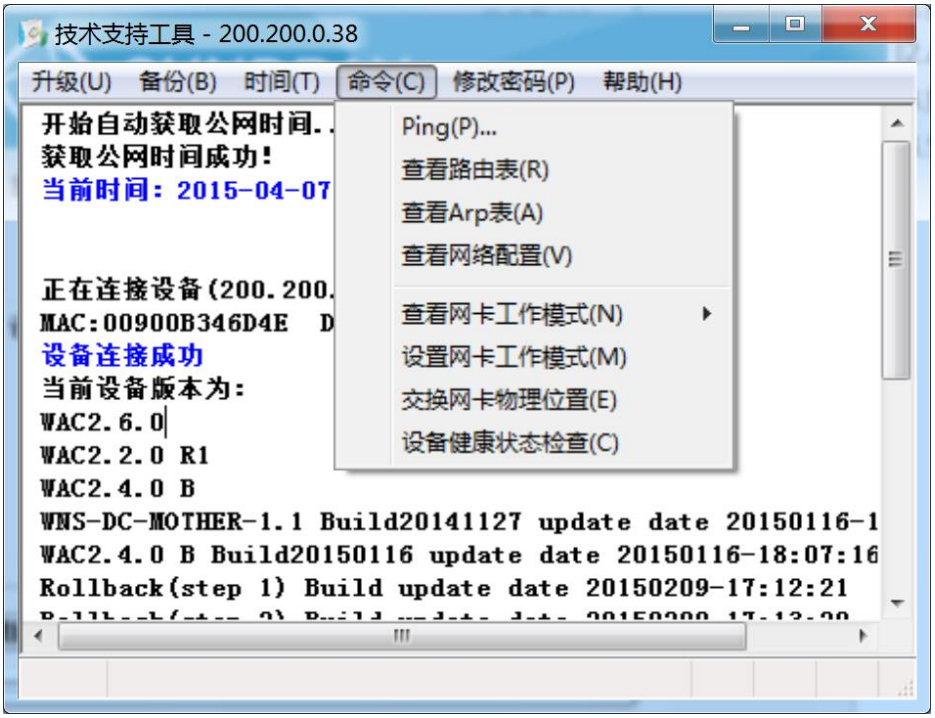
[备份配置]：将设备现有的配置信息进行备份。

[恢复备份配置]：将以前备份过的配置信息恢复到设备中。

『时间』用来查看当前时间和同步公网时间，来效验设备升级授权是否过期。如下图：



『命令』：包括 Ping、查看路由表、查看 Arp 表、查看网络配置、查看网卡工作模式、设置网卡工作模式、交换网卡物理位置以及设备健康状态检查选项。如下图：



[Ping]：登录设备后，从设备往外网 ping，以验证设备是否和外网连通。

[查看路由表]：查看设备本机的路由表。

[查看 ARP 表]：查看设备本机的 ARP 表，因为 NAC 属于特殊无线网络设备，通过升级客户端方式查看的 ARP 不代表其内部真实的 ARP 表，所以该返回值不具备参考性。

[查看网络配置]：查看设备本机的网络配置，包括接口 IP 配置等。

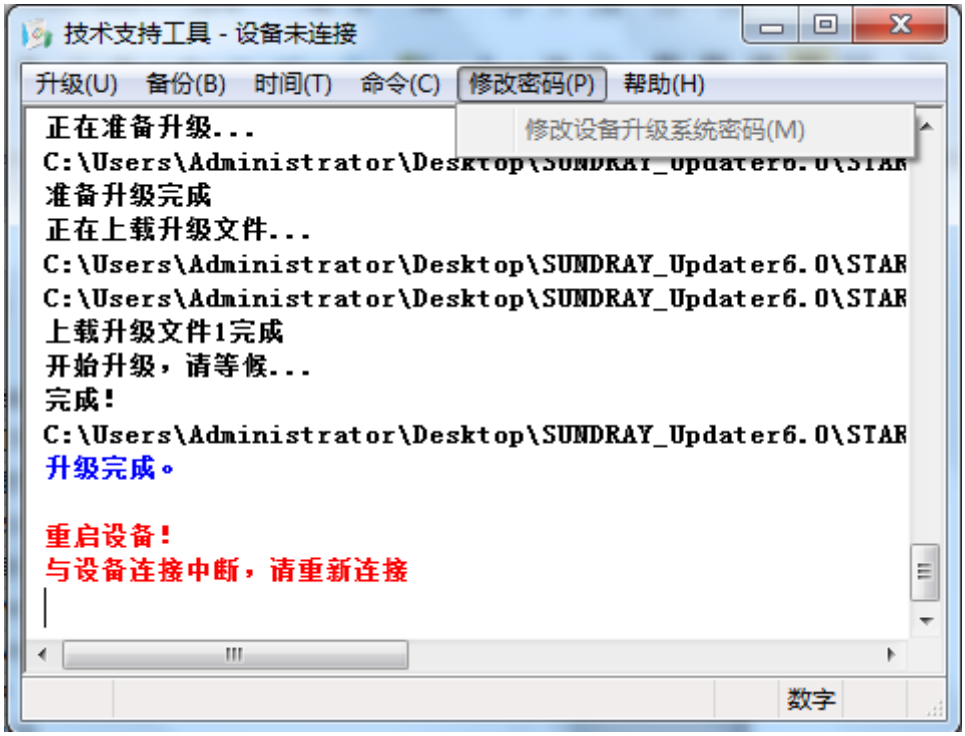
[查看网卡工作模式]：查看设备各网卡的工作模式。

[设置网卡工作模式]：NAC 产品线该功能不可用。

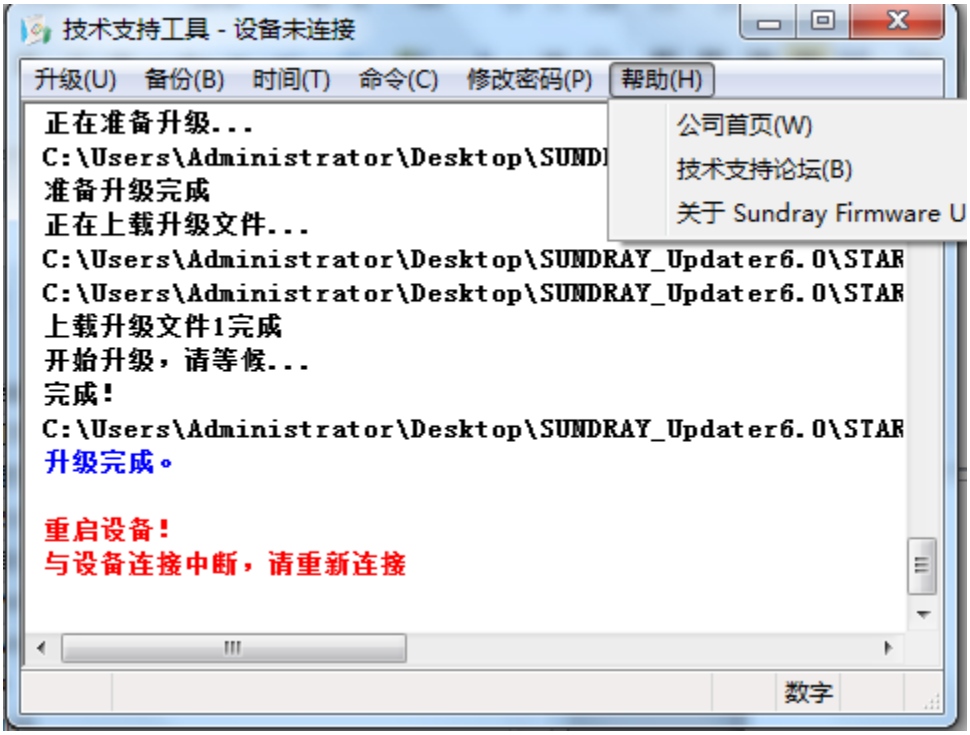
[交换网卡物理位置]：NAC 产品线，该功能不可用。

[设备健康状态检查]：通过在线检测或者是上传脚本来检测设备的硬件状态。

『修改密码』：用于修改 SUNDRAY 设备升级系统密码，如下图：



『帮助』包括公网首页的链接，技术支持论坛的链接和查看当前 Updater 的版本信息。



6.2. 安全网卡使用指导

6.2.1. 基本配置

6.2.1.1. 公共环境

6.2.1.1.1. 操作系统

Windows xp ， Windows 7， Windows 8 ， Windows 8.1 ， Windows10

6.2.1.1.2. AD 域环境

（1）Windows server 2008 版本 AD 域 10.15.30.108（父域），域名 test.com，远程和 AD 域密码都为 Sundray123；

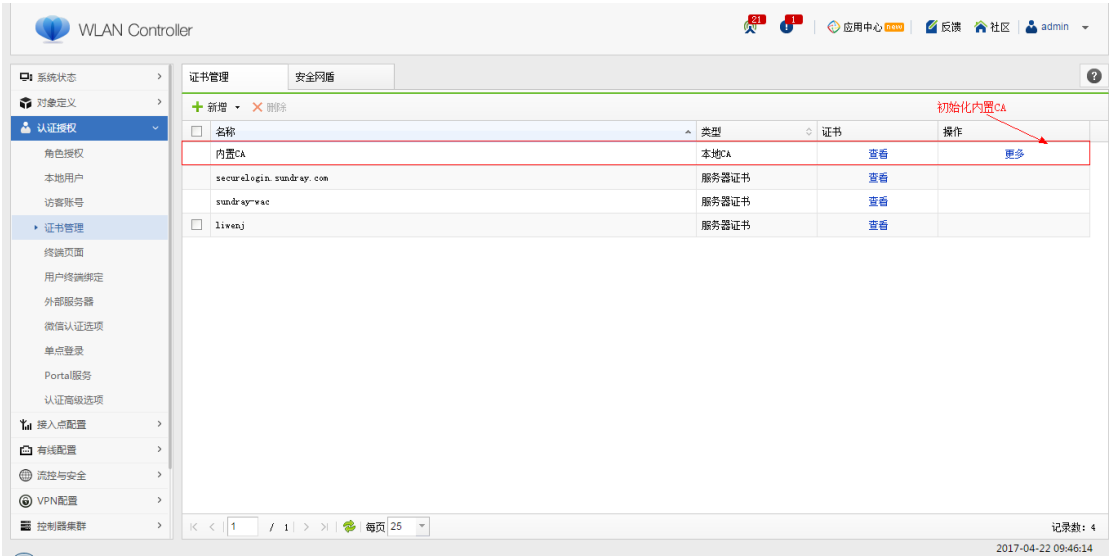
（2）Windows server 2008 版本 AD 域 10.15.30.109（子域），域名 testsun.test.com，远

程和 AD 域密码都为 Sangfor123。

6.2.1.2. 配置无线控制器

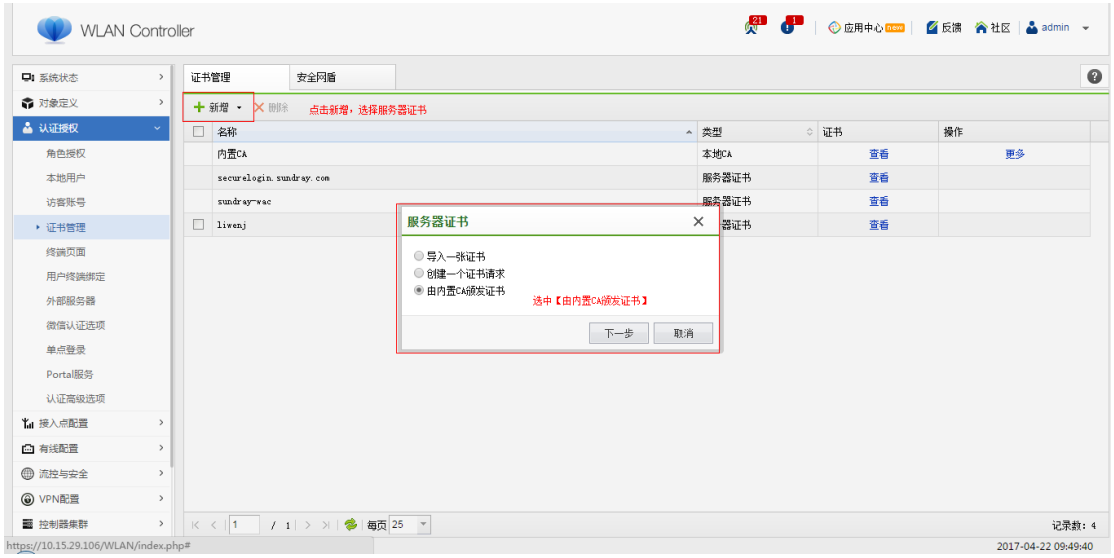
6.2.1.2.1. 初始化内置 CA 证书

登录无线控制器，【认证授权】->【证书管理】->【证书管理】，选择查看内置 CA，点击“初始化”。



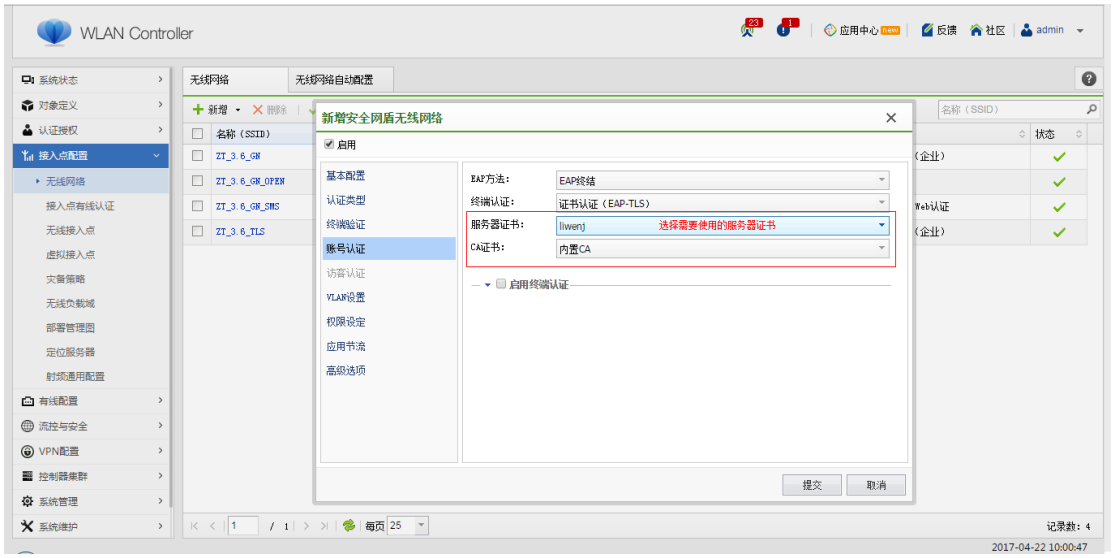
6.2.1.2.2. 创建服务器证书

初始化内置 CA 后，点击【新增】->【服务器证书】->【由内置 CA 颁发证书】，创建一个由内置 CA 颁发的服务器证书。



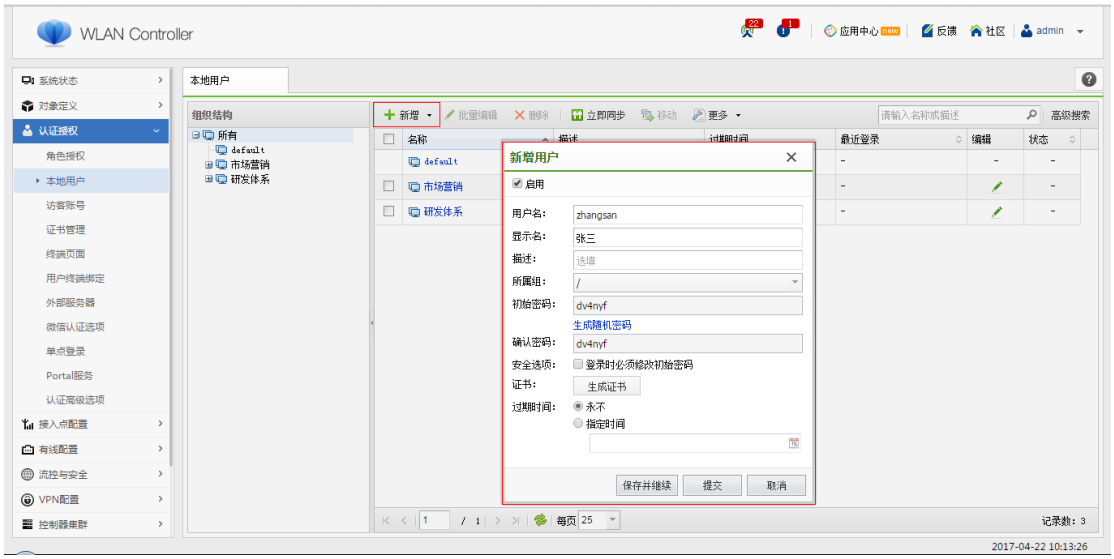
6.2.1.2.3. 配置安全网盾无线网络

【接入点配置】->【无线网络】->【新增】->【新增安全网盾无线网络】，名称（SSID）：zd_3.6_GN_tls_dev，认证类型默认为【WPA/WPA2（企业）】、加密方式默认为【AES】、EAP 方法默认为【EAP 终结】、终端认证默认为【证书认证（EAP-TLS）】，服务器证书可为任一由内置 CA 颁发的服务器证书，CA 证书选择【内置 CA】。



6.2.1.2.4. 配置本地用户

【认证授权】->【本地用户】->【新增】，新建本地用户账号。

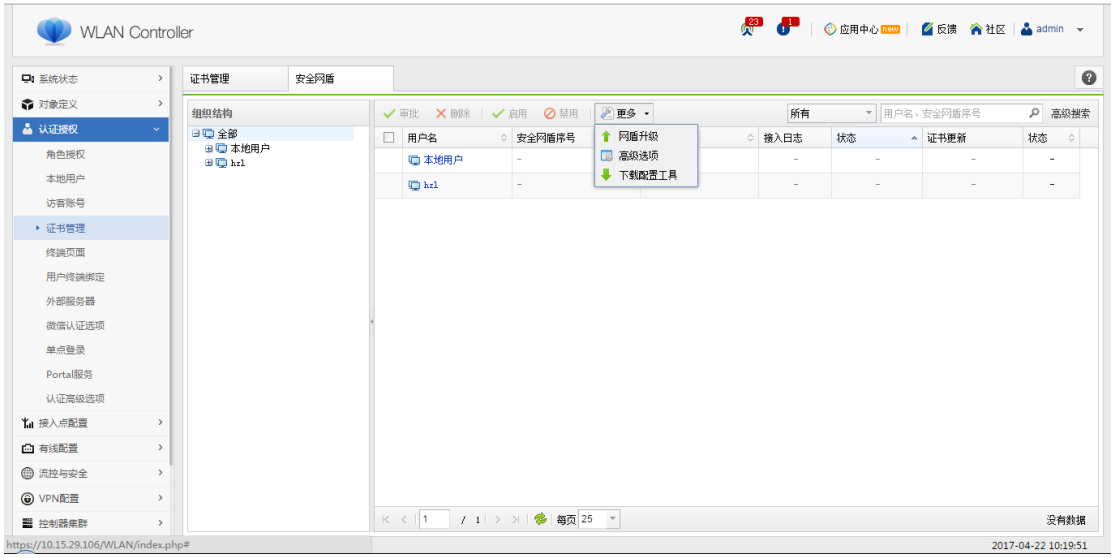


6.2.1.3. 配置工具烧录网卡

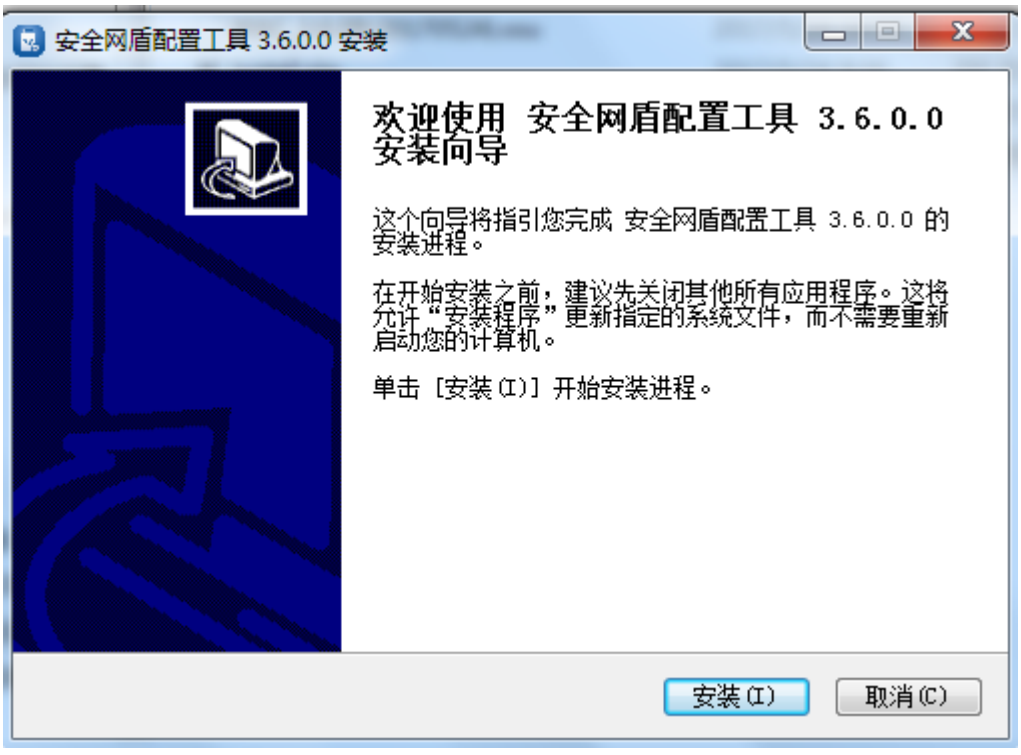
6.2.1.3.1. 配置工具安装

只有安装了配置工具，管理员才可以烧录安全网盾。请按照如下步骤进行网卡的软件安装。Windows XP、Windows Vista、Windows 7、Windows 8 和 Windows 10 系统下的安装步骤相似，以下以 Windows 7 的安装界面为例进行说明。

1）登录无线控制器，【认证授权】->【证书管理】->【安全网盾】，进入到安全网盾页面后，【更多】->【下载配置工具】，下载配置工具安装包。



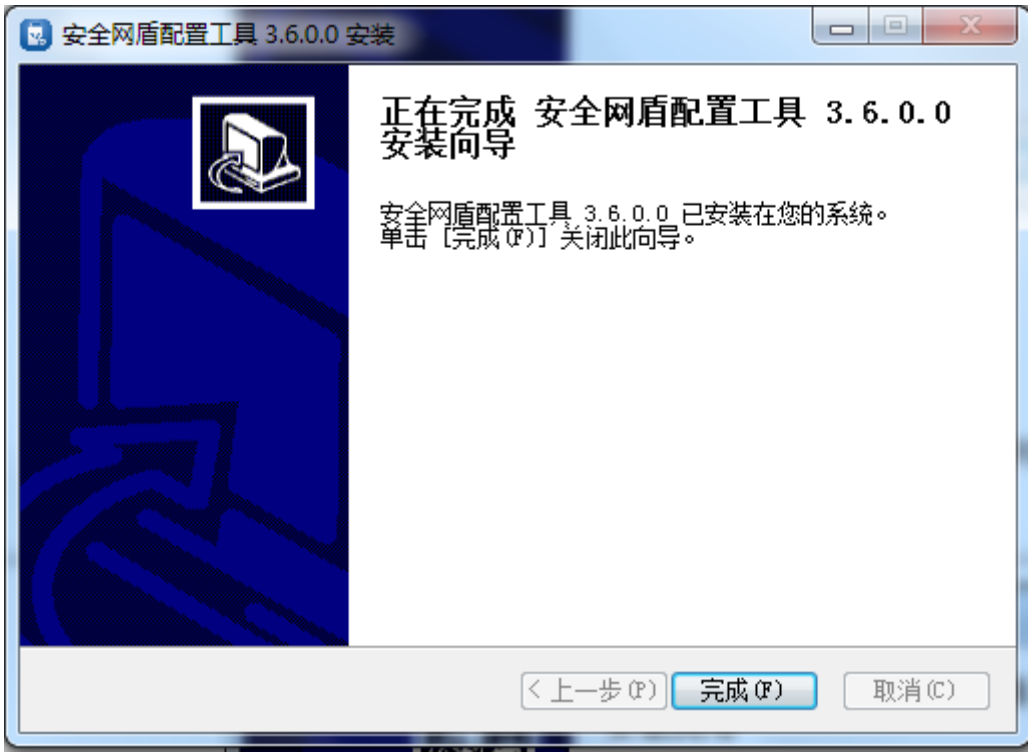
2） 鼠标双击配置工具安装文件，点击“安装”，开始安装程序。



3）接下来的安装过程大约需要几分钟的时间，请稍作等待。

4）当出现以下界面时，表示已完成安装，同时桌面会生成配置工具快捷键  ，

点击“完成”退出安装向导。



6.2.1.3.2. 配置工具使用

1）运行配置工具

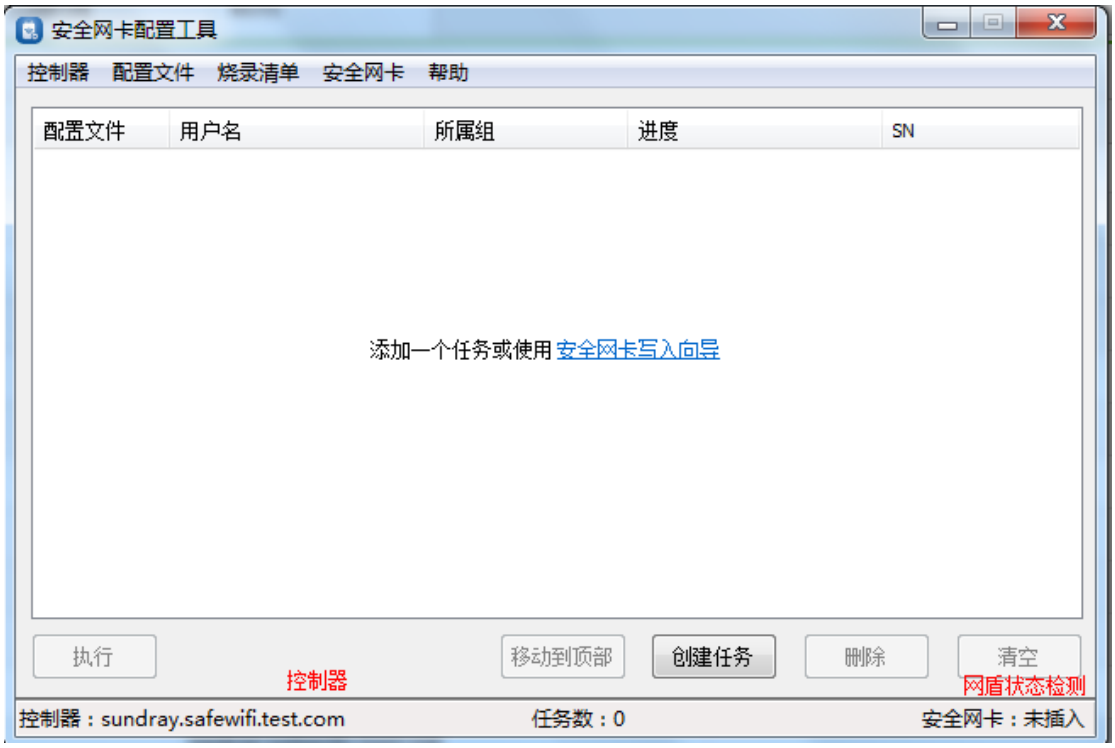
双击桌面上配置工具的快捷键 

，打开配置工具。

2）配置工具连接控制器

进入配置工具登录页面，输入无线控制器的地址或域名、端口号（默认为 443，需要与控制器保持一致），管理员账号密码后点击“连接”。

控制器连接成功会进入配置工具主页面，页面左下角显示控制器地址/域名，右下角实时监测网卡插入状态。



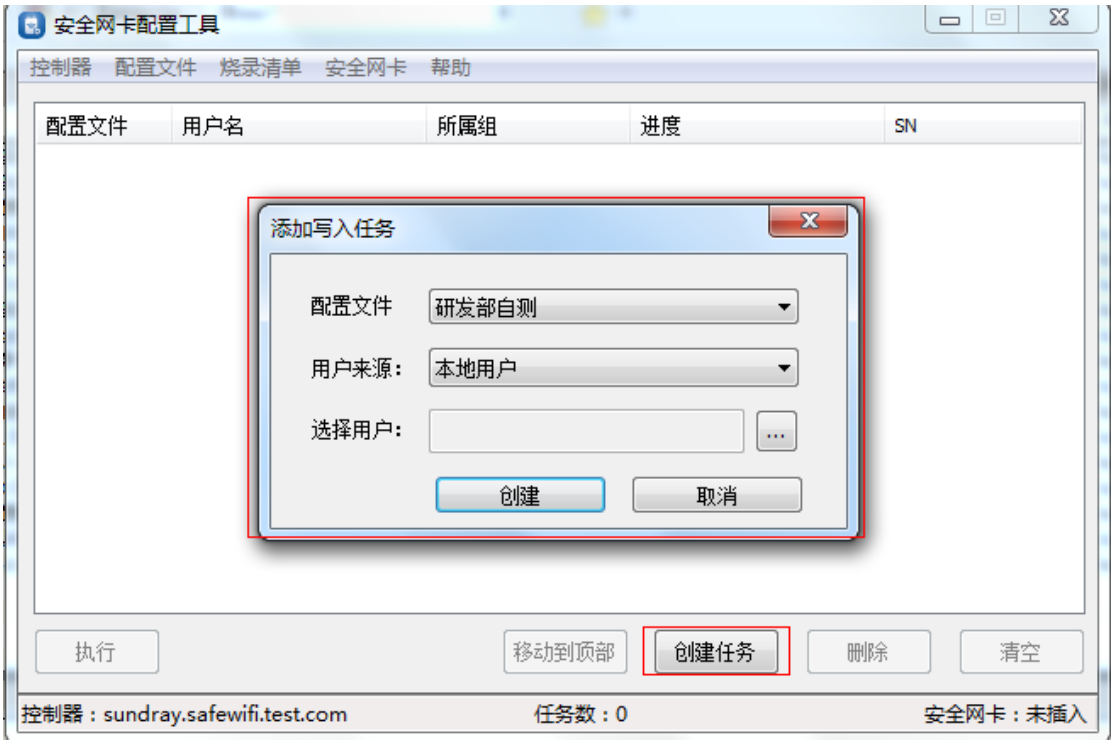
3）配置工具添加配置文件

【配置工具主页面】->【配置文件】->【添加】，新增一个配置文件，文件名称为【研

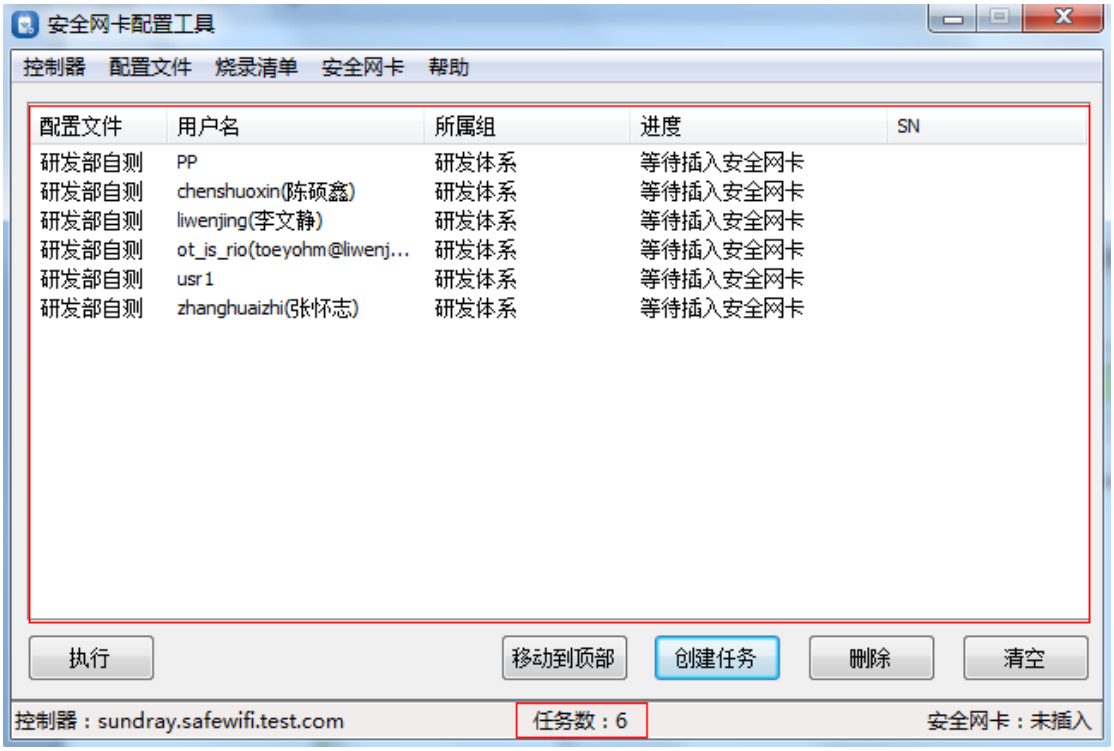
发部自测】，写入网卡的无线网络只能是安全网盾无线网络（见左图），设置完成后点击下一步，设置证书有效期及初始 PIN 等属性信息（见右图），点击完成。

4） 配置工具添加写入任务

点击配置工具主页面的快捷键【创建任务】，添加网卡写入任务，用户来源选择本地用户，用户选择 WAC 上配置的本地用户组【研发体系】，点击创建。

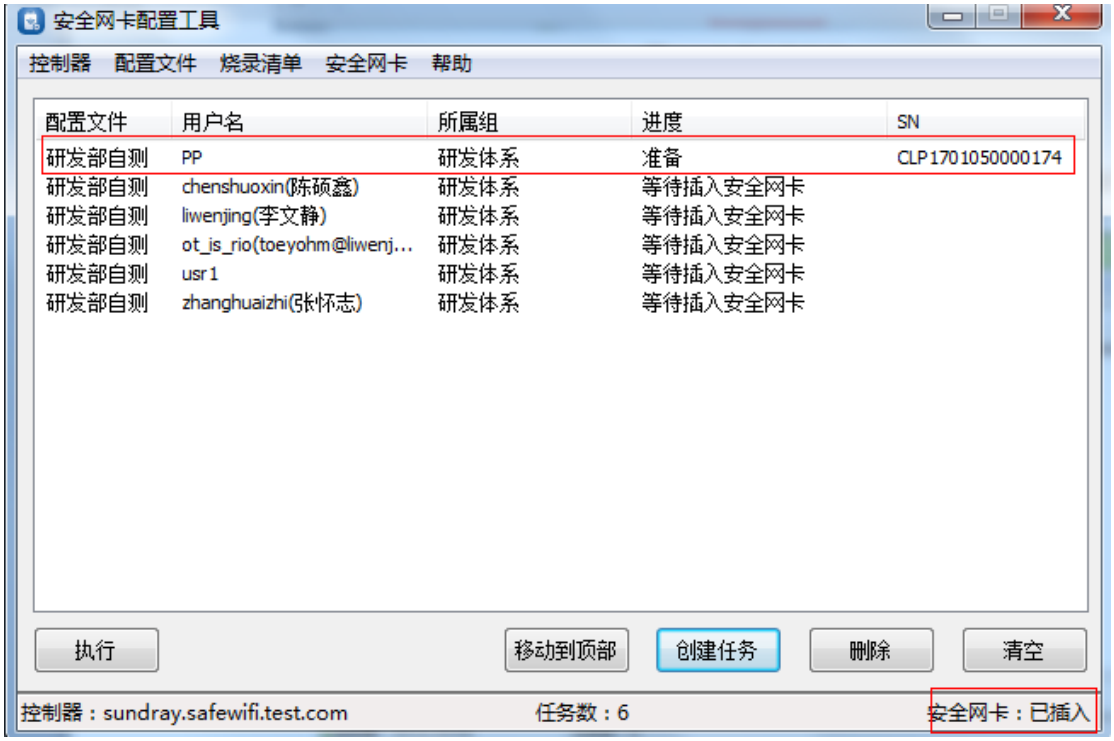


点击【创建】按钮后，配置工具主页面会自动生成任务列表。

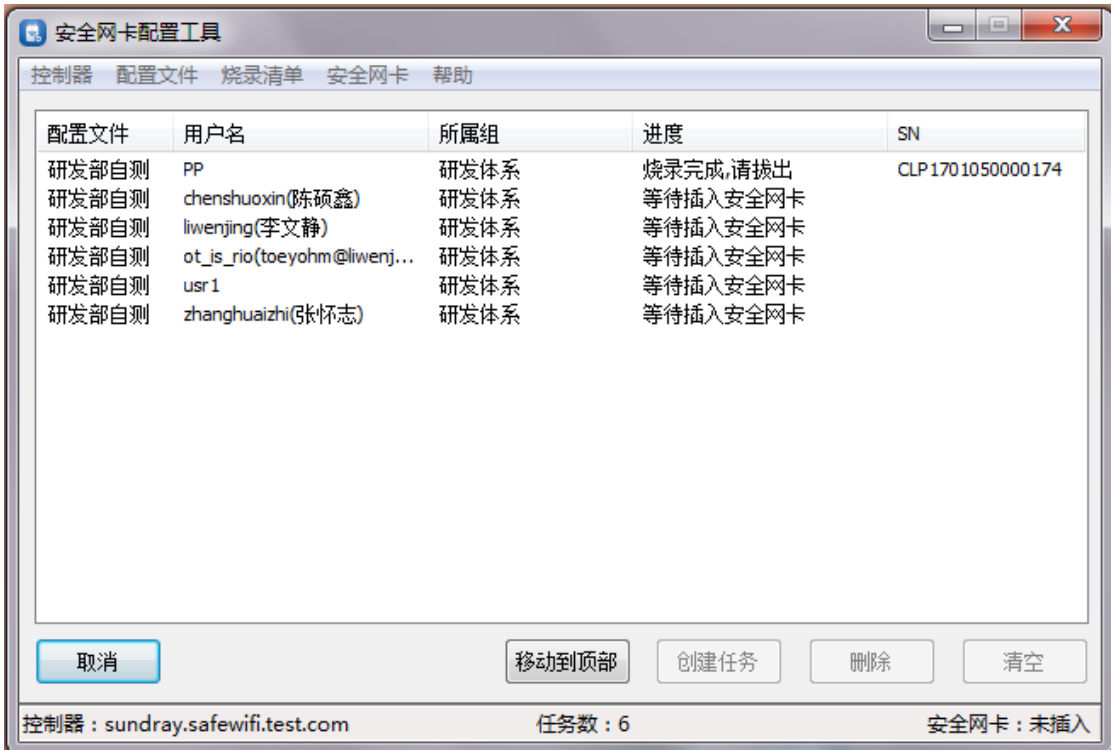


5）配置工具写入网卡配置

网卡插到管理员 PC 上，右下角状态更新为已插入，进度为“准备”状态，点击配置工具主页面执行按钮，即可开始烧录任务。

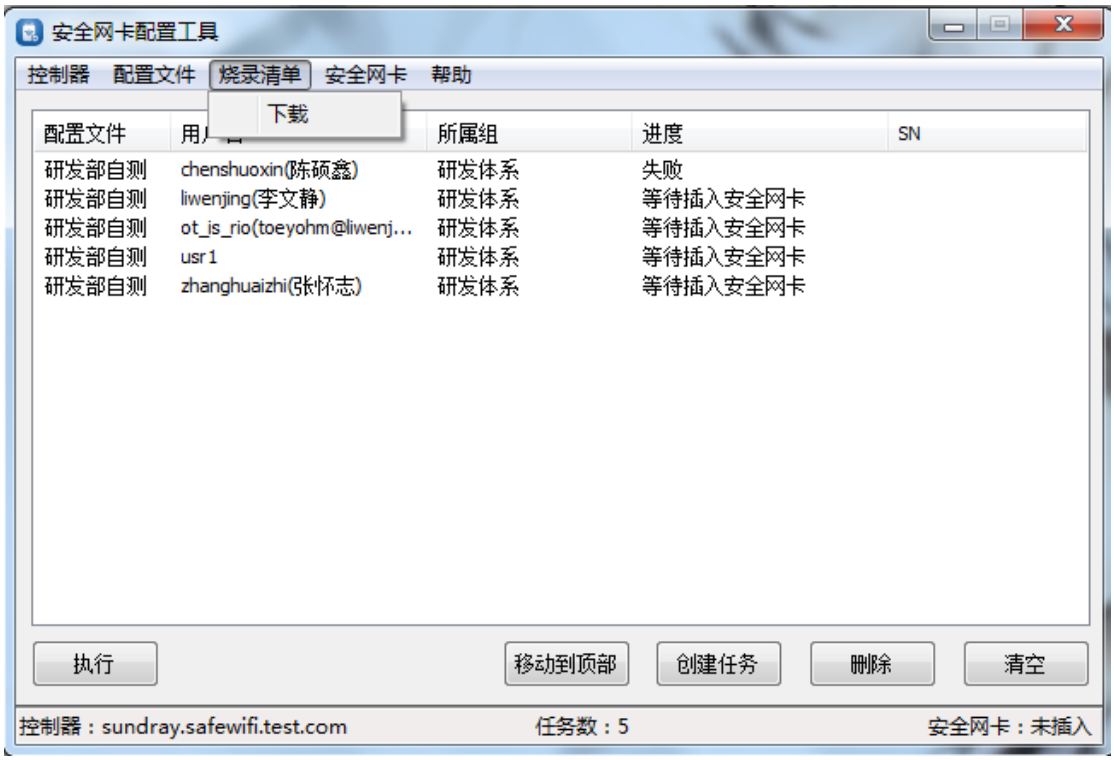


进度为“烧录完成，请拔出”，此时可以拔掉该网卡，管理员再插上第二个网卡，开始写第二个账号。



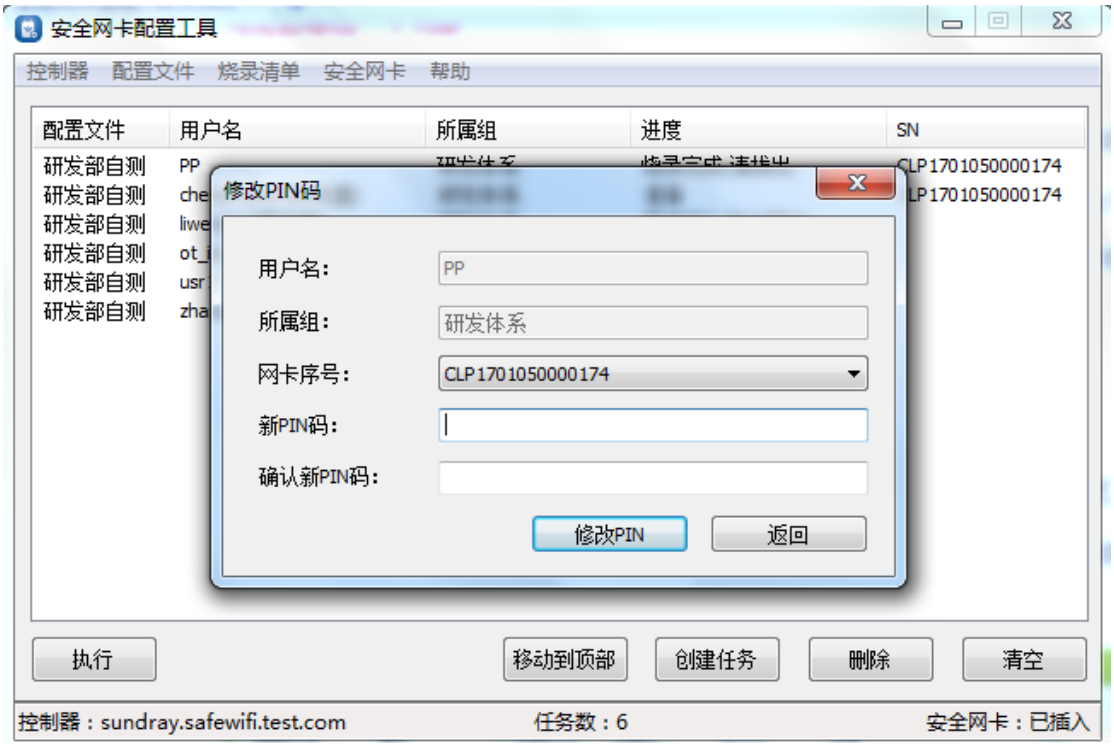
6）下载烧录清单

烧录网卡结束后，点击【烧录清单】—>【下载】，可以下载烧录成功的任务记录，烧录清单中包含用户的组织结构，用户名及安全网盾的 SN 码。



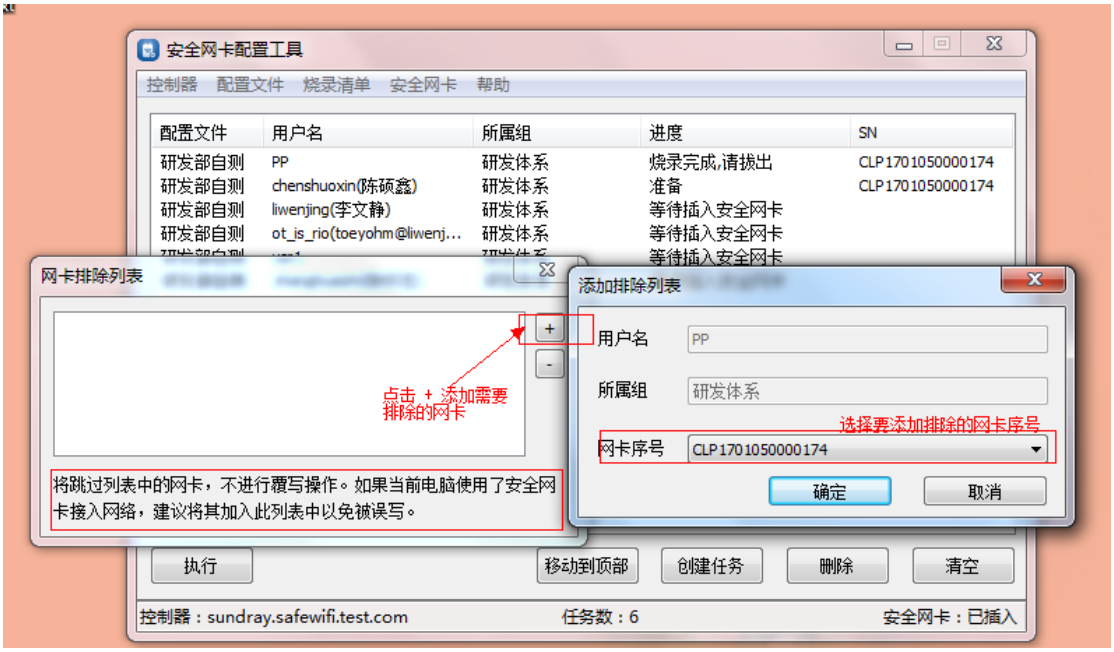
7）配置工具修改网卡 PIN 码

用户使用网卡时如果忘记了网卡的 PIN 码或安全网盾被锁，无法连接无线网络，可以找管理员修改。网卡插到管理员 PC 上，打开配置工具连接控制器成功后，【安全网盾】->【修改用户 PIN 码】，选择插入的网卡 SN 码，输入新 PIN 码和确认 PIN 码，点击“修改 PIN”按钮，修改成功。



8） 配置工具添加网卡排除列表

如果管理员已经在使用智能网卡办公，给其他人烧录网卡时，需要在配置工具上先把自己的网卡添加到排除列表。配置工具页->安全网盾->网卡排除列表->添加，选择管理员的网卡加入到排除列表。



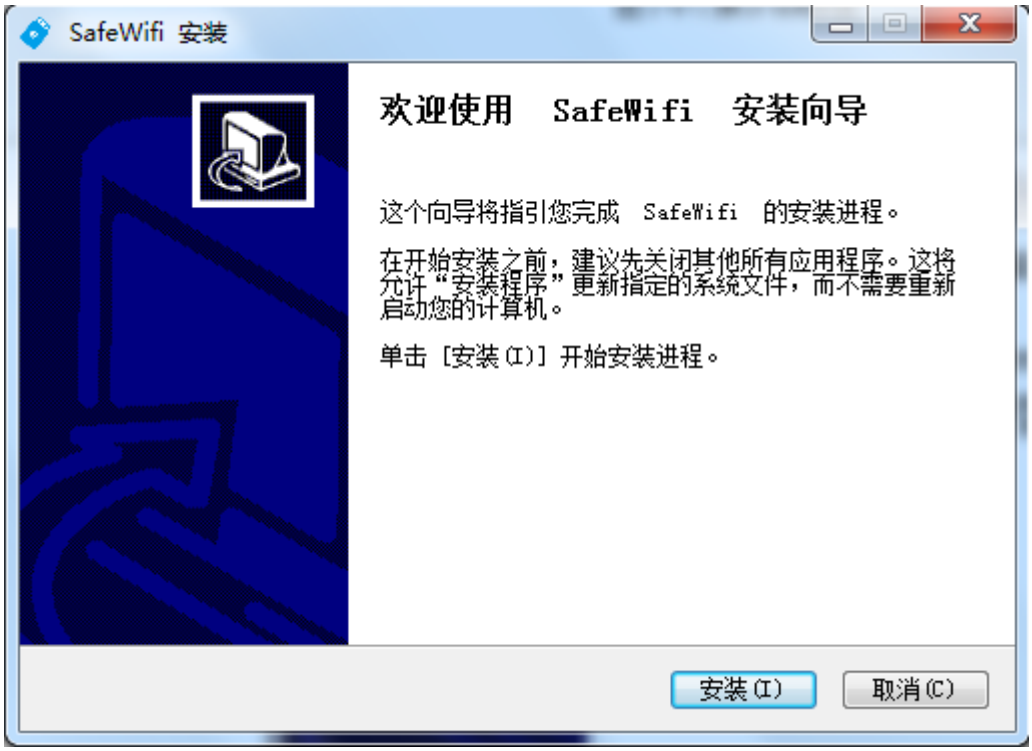
6.2.1.4. 终端使用安全网盾

6.2.1.4.1. 网卡驱动和服务程序安装

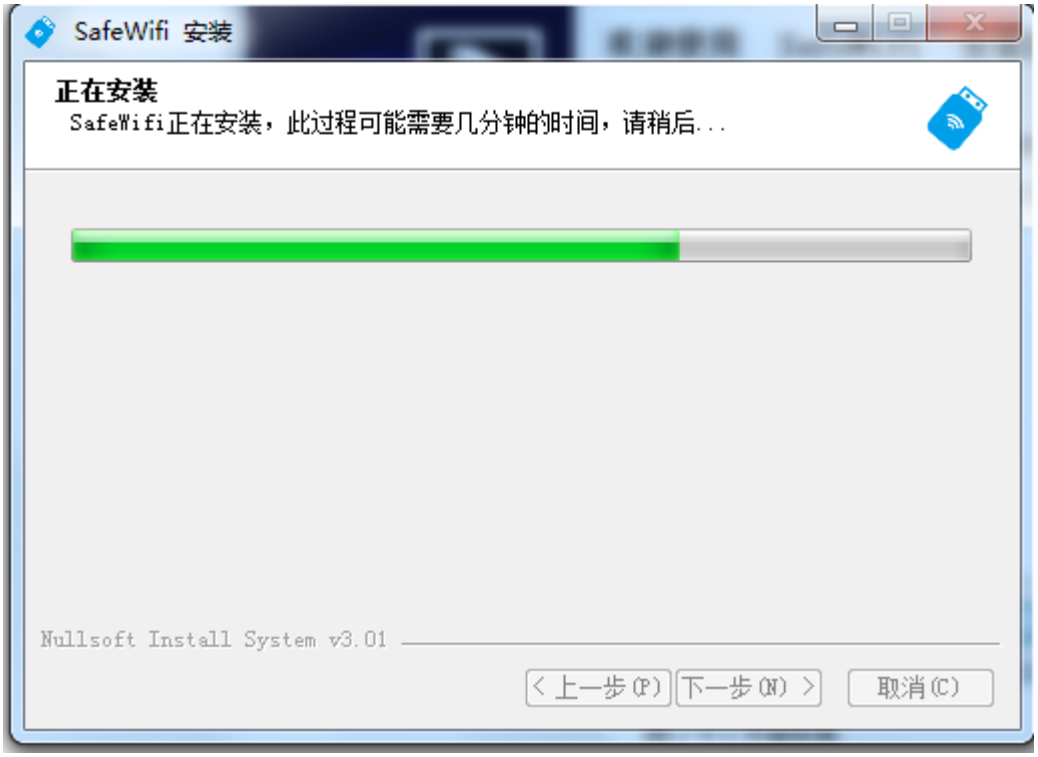
只有安装网卡驱动和安全服务，安全网盾才可以正常使用。请按照如下步骤进行网卡的软件安装。Windows XP、Windows Vista、Windows 7、Windows 8 和 Windows 10 系统下的安装步骤相似，以下以 Windows 7 的安装界面为例进行说明。

1） 打开包装取出网卡，将网卡插到 PC 的 USB 接口，PC 上弹出 CD-ROM 自动播放窗口；

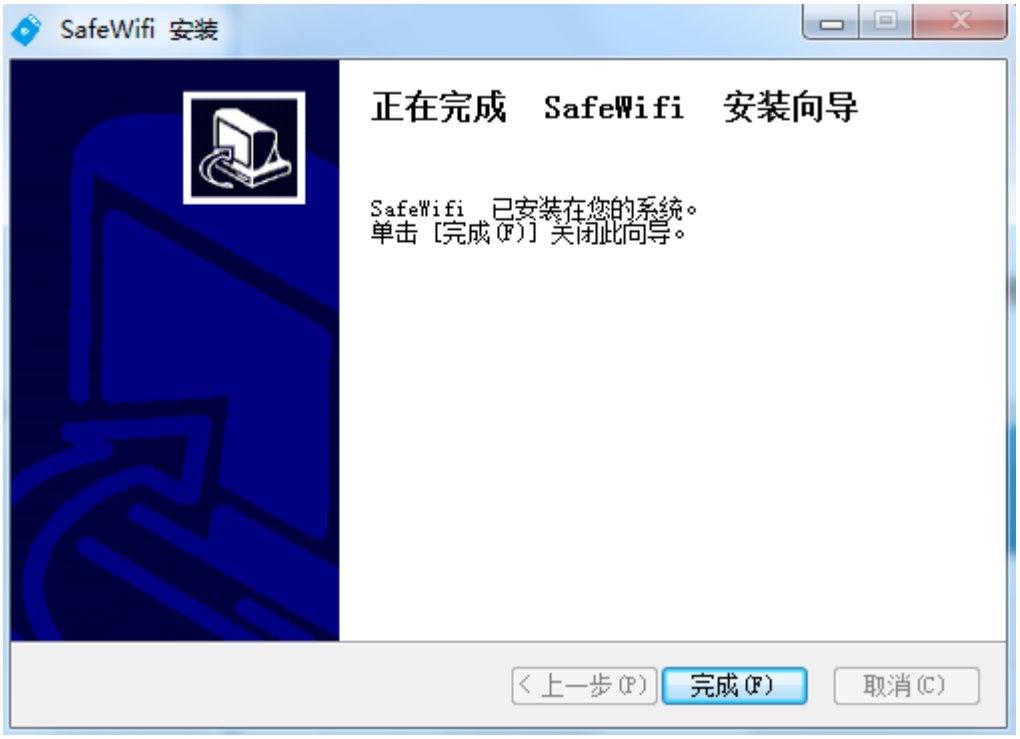
2） 点击“运行 Setup.exe”，开始安装驱动和服务程序



3） 接下来的安装过程大约需要几分钟的时间，请稍作等待。



4）安装完成，点击“完成”退出安装向导



6.2.1.4.2. 终端连接无线网络

终端安装好安全服务后，不会创建桌面快捷方式，仅当服务检测到安全网盾插入后才会显示托盘进程。

1）输入 PIN 码

终端使用未初始化过的安全网盾时，会自动弹出修改 PIN 码的弹框，修改 PIN 码后才能使用网卡。

若安全网盾已经修改过 PIN 码，则会请弹出输入 PIN 码的弹框，输入后才可以使用网卡。

PIN 码输入说明：

1.终端首次使用安全网盾时，会弹出输入 PIN 码的弹框（若安全网盾未初始化则弹出修改 PIN 码弹框），此后该终端再使用该网卡时，只要 PIN 码没有改变，就不用再输入 PIN 码；

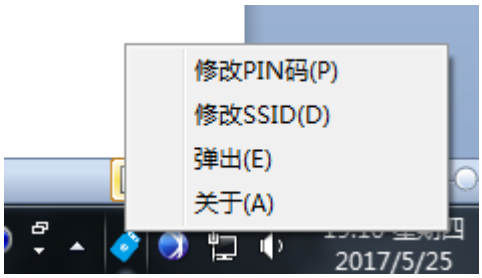
2.若安全网盾的 PIN 码发生改变，则要求重新输入 PIN 码。

2）连接网络

插入智能网卡后会自动连接到预置的无线网络。不需要用户手动打开无线列表连网。打开终端的无线网络列表，可以看到已成功连接上预置的无线网络，终端可正常上网。

3）终端修改 PIN 码

点击托盘上的无线网卡安全服务图标，选择“修改 PIN 码”，弹出修改框，输入当前 PIN 码、新 PIN 码和确认 PIN 码，点击“确定”后修改成功。

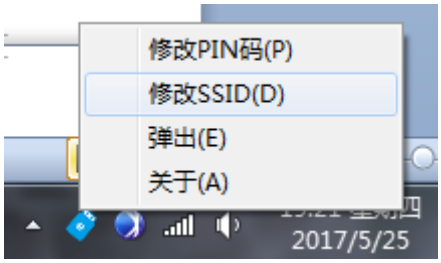


4）修改 SSID

管理员为规范无线网络名称，可能会修改安全网盾无线网络的 SSID（修改前 SSID：

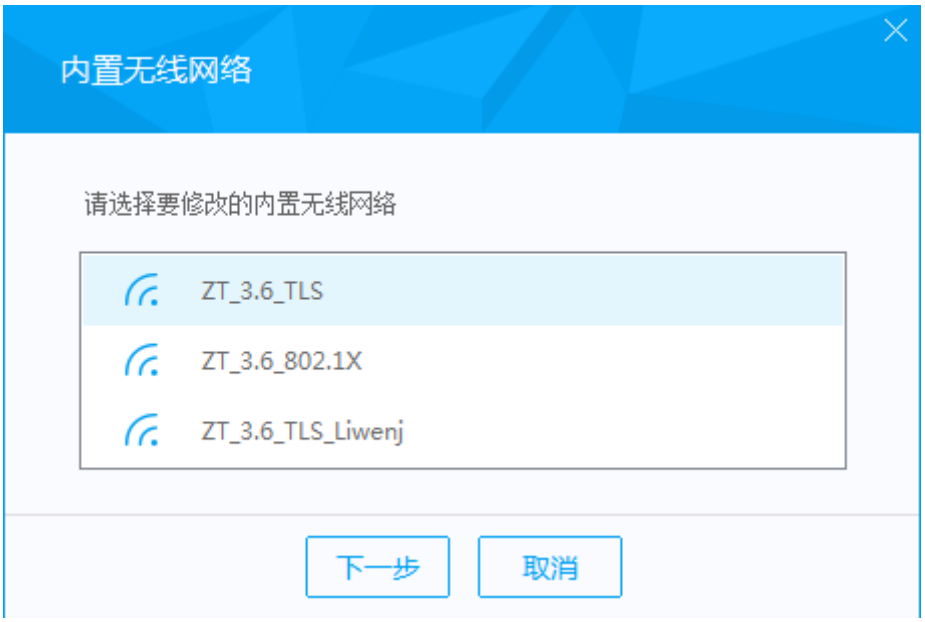
1111，修改后 SSID：1_Layer_Office），为保证安全网盾可以接入新的无线网络，用户可以选择托盘菜单中的修改 SSID，来更新安全网盾内置无线配置。具体操作如下：

第一步：点击托盘图标，在弹出菜单中选择修改 SSID。



第二步：修改 SSID 前需要确认您的身份，请输入正确 PIN 码。

第三步：选中需要修改的 SSID 后点击确认。



第四步：选择修改后的 SSID，更新安全网盾的无线网络配置。

5）版本号

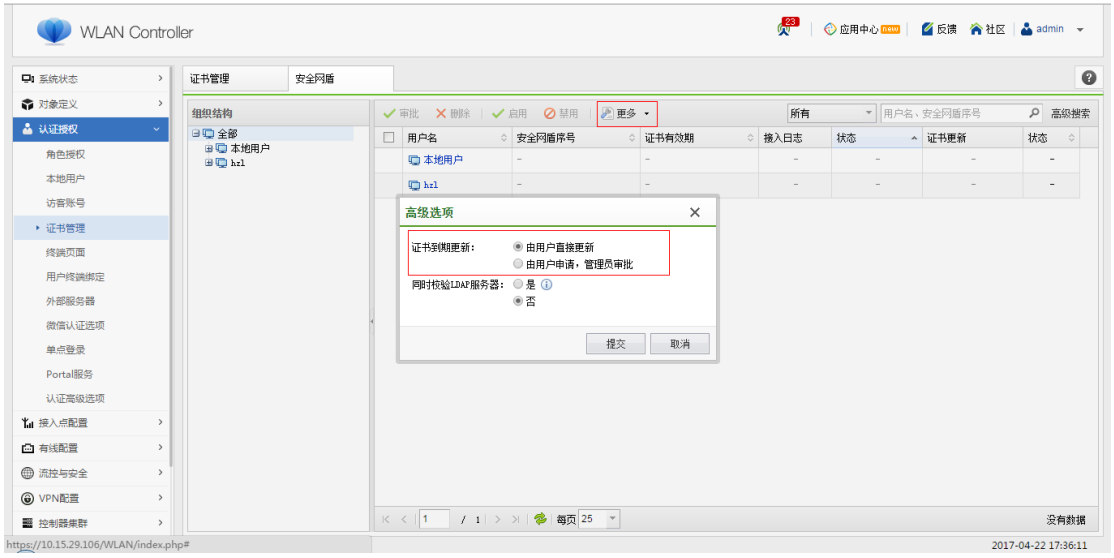
终端查看安全服务版本号，点击托盘图标，弹出菜单中点击【关于】选项。

6）弹出智能网卡

点击托盘图标，选择【弹出】选项，托盘图标弹出提示“请移除安全网盾”后，拔掉网卡后托盘图标弹出提示“安全网盾已移除”。

6.2.1.4.3. 证书更新

证书更新分为两种方式，由管理员审批或用户自动更新，以管理员账号登录控制器，【认证授权】->【证书管理】->【安全网盾】->【更多】->【高级选项】（见图），设置证书更新方式。

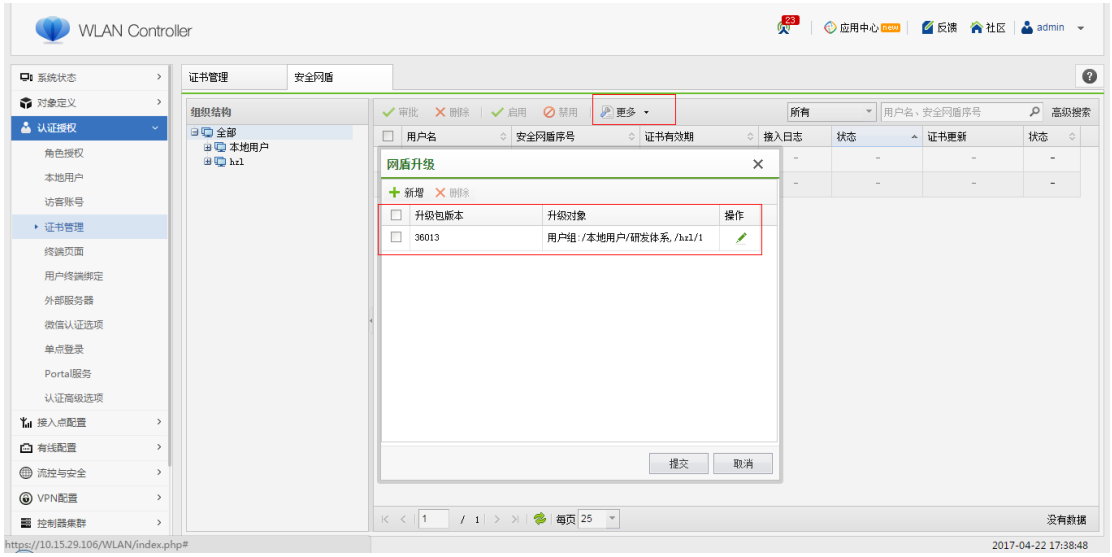


由管理员审批：若安全网盾证书有效期小于 30 天，控制器上证书状态为即将过期，管理员可预先审批，或等收到审批请求时审批（快过期网卡接入无线网络后会向控制器发送审批请求，管理员可看到证书状态为待审批），过期的安全网盾不能接入网络。

由用户直接更新：若安全网盾有效期小于 30 天，网卡接入无线网络后会自动从控制器上下载新证书。

6.2.1.4.4. 网盾升级

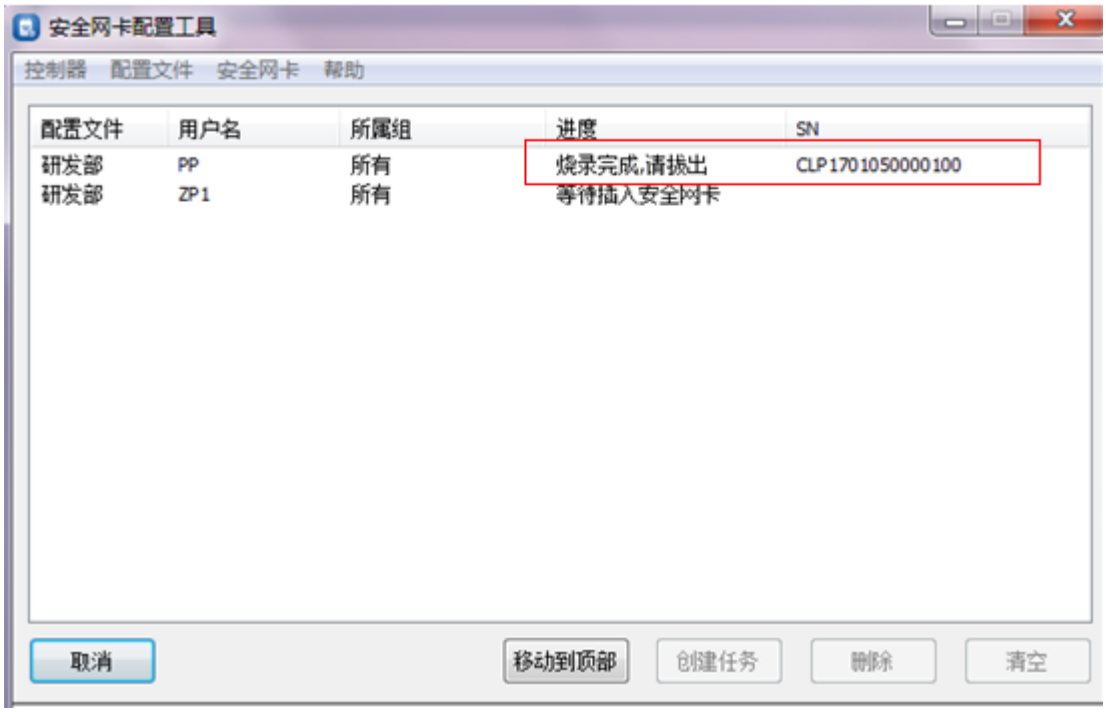
若网盾推出新功能，管理员可以在【认证授权】->【证书管理】->【安全网盾】->【更多】->【网盾升级】页面中设置想要升级的网盾（见图），升级对象支持配置单个组，多个组，单个网卡，多个网卡。



6.2.2. 问题检查方法

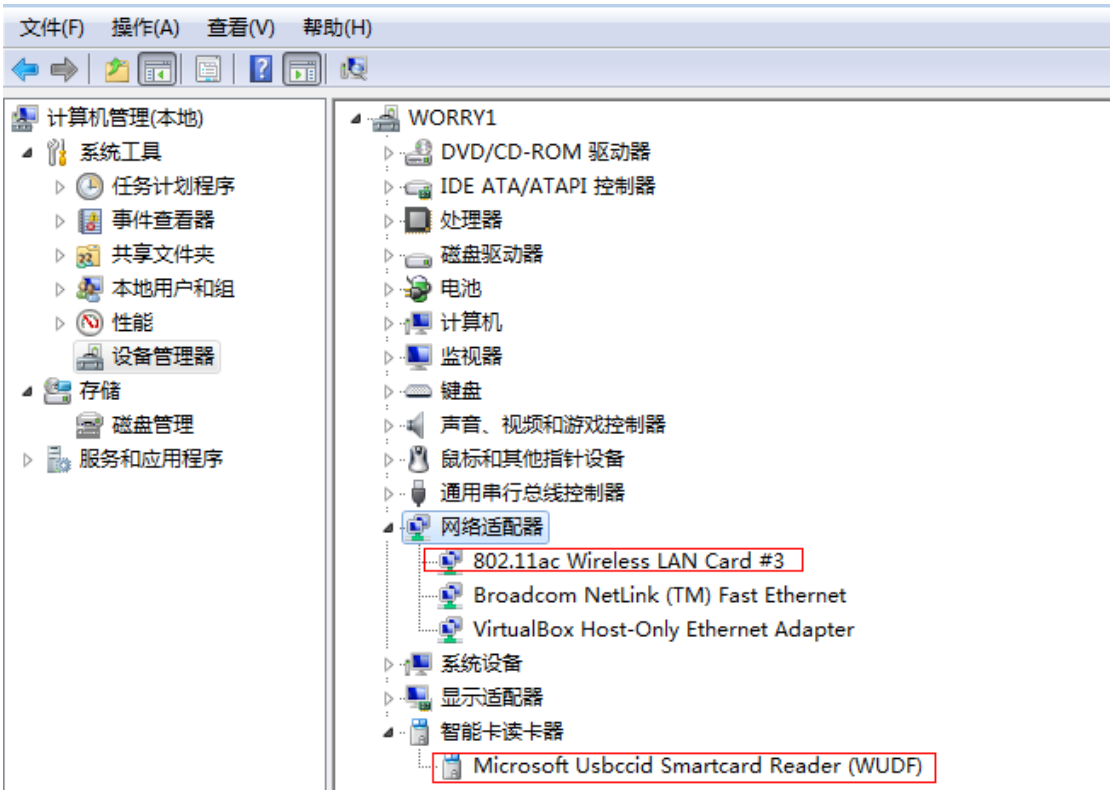
6.2.2.1. 网卡配置写入成功的标准

网卡配置工具显示框对应的 SN 码任务状态为“烧录完成，请拔出”。



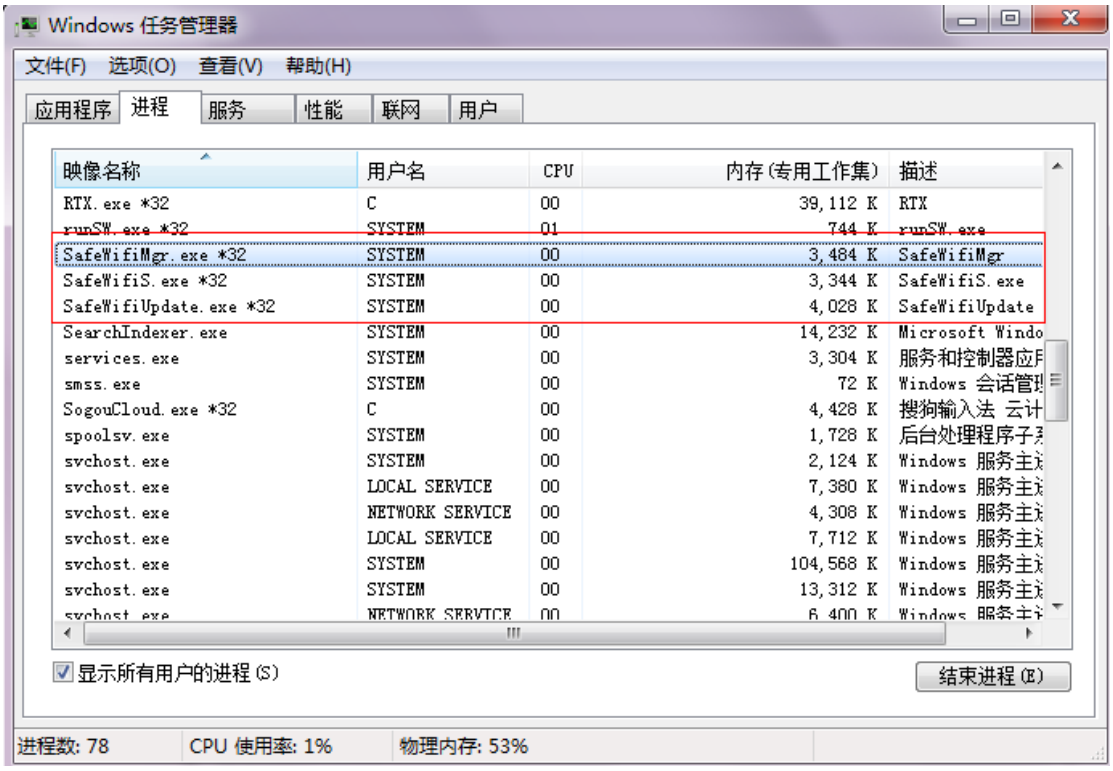
6.2.2.2. 驱动安装成功的标准

驱动安装成功标志网卡和 key 驱动安装成功标志，PC 的计算机设备管理器网络适配器中可以看到无线网卡的驱动，设备管理器中新增一个智能卡读卡器的驱动，同时可以看到网卡的状态灯有闪烁。



6.2.2.3. 安全服务程序安装成功的标准

检查 PC 安全服务进程、托盘图标进程和服务升级进程运行正常，插入安全网盾后会显示托盘图标，并弹出提示“安全网盾已插入”，启动任务管理器，可以看到 SafeWifis.exe，SafeWifUpdate.exe，SafeWifisMgr.exe 进程正常运行。



6.2.2.4. 内置 CA 证书认证成功的标准

1）终端可以接入无线网络，且使用浏览器访问百度，可以访问成功；

2）WAC 的在线用户可以查看到该用户的信息，认证类型为证书认证，用户名为对应网卡写入的账号，且该用户显示的组织结构与实际用户服务一致。

6.2.2.5. 基本的调试方法

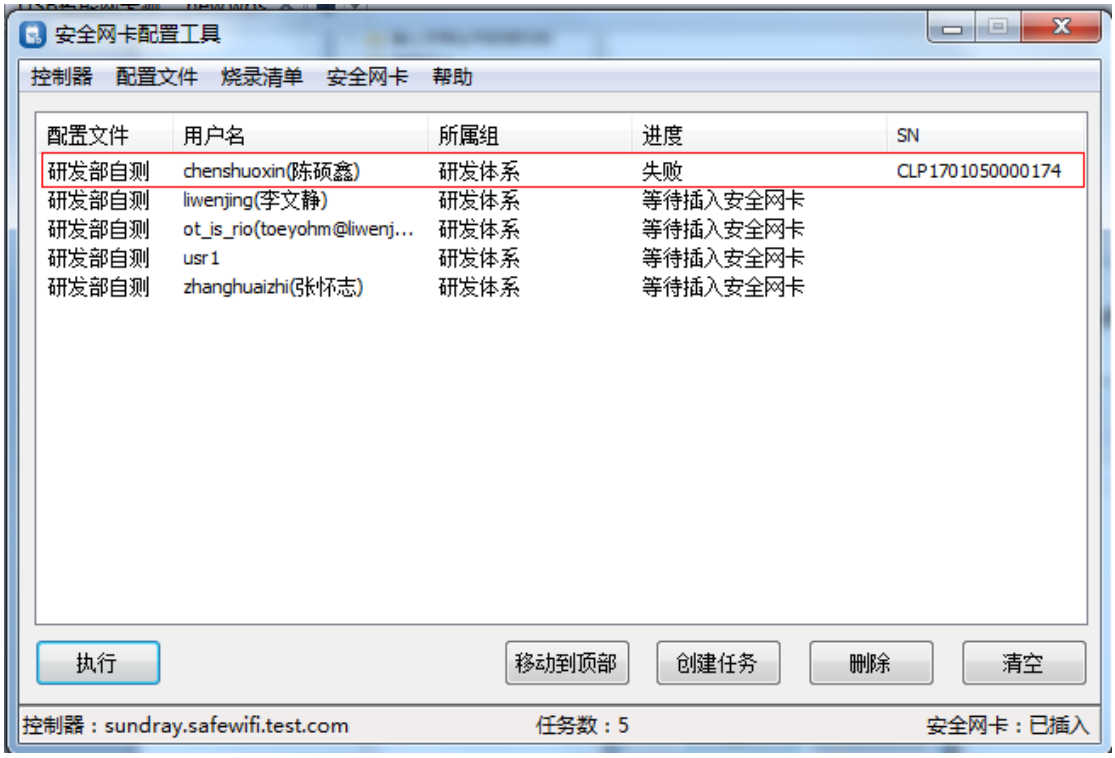
6.2.2.5.1. 终端服务升级调试方法

安全服务安装目录 C:\Program Files (x86)\SafeWiFiSetup\SafeWifiS 下会有 setup.exe，update.ini 文件生成，升级结束后注册表及关于对话框均会更新版本号。

6.2.3. 失败场景的 FAQ

6.2.3.1. 网卡配置写入失败

1）检查网卡在写入任务过程中是否被拔出，烧录任务的进度是不是失败；

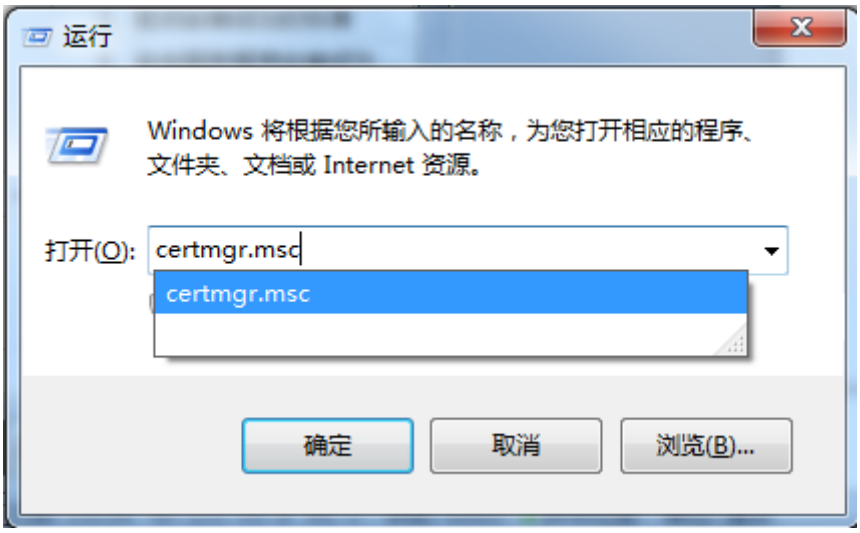


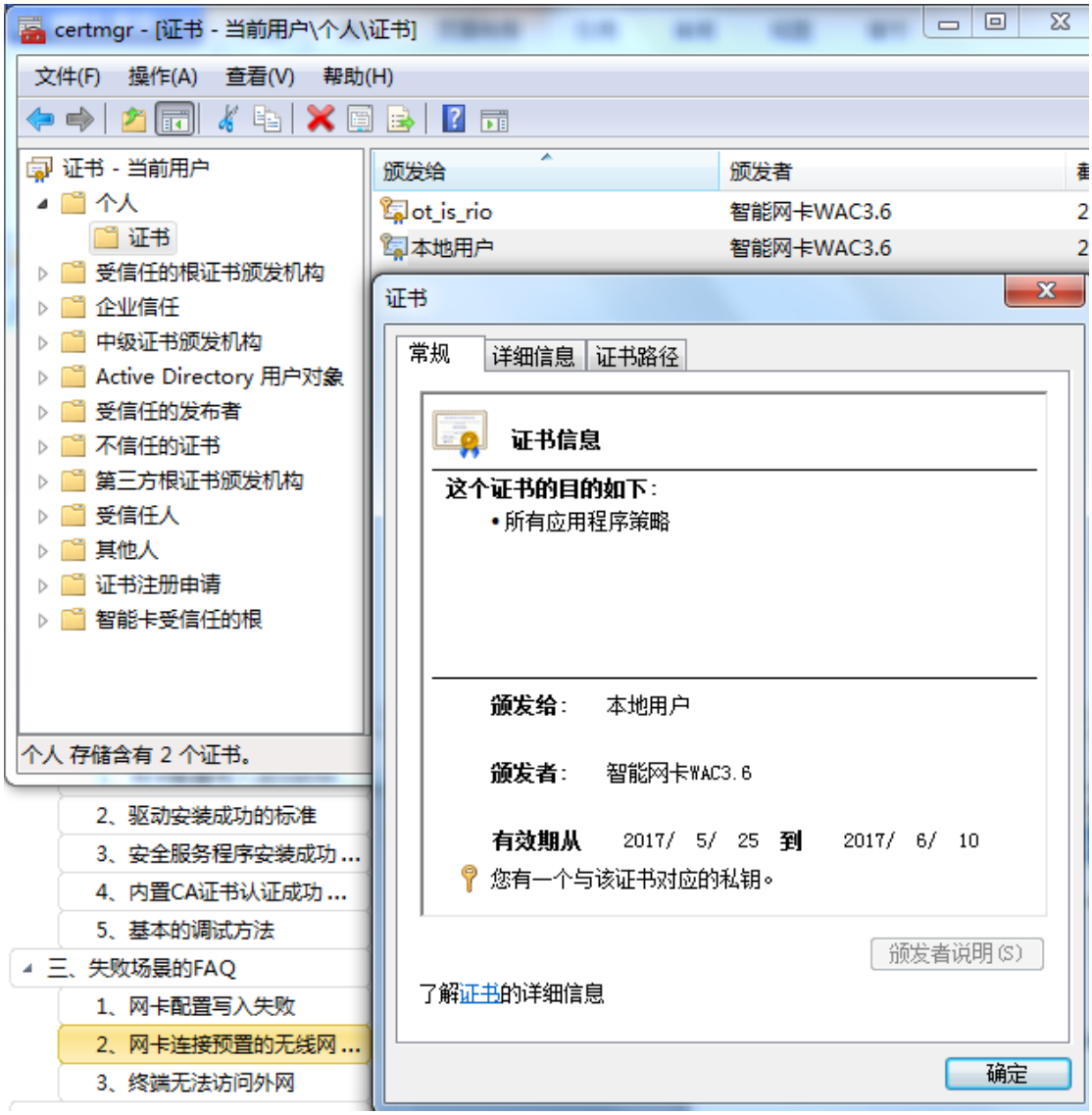
6.2.3.2. 网卡连接预置的无线网络失败

1）按照二（2）中的标准检查智能网卡驱动是否安装好，如果没有安装好重新安装驱动；

2）如果驱动都安装好了，再按照二（3）中的标准检查安全服务程序是否安装好，如果没有安装好重新安装服务程序；

3）如果安全服务安装好了，检查 PC 中的证书是否正确，检查有效期，方法如下：


运行
Windows 将根据您所输入的名称，为您打开相应的程序、
文件夹、文档或 Internet 资源。
打开(O):
certmgr.msc
certmgr.msc
确定
取消
浏览(B)...



4）如果证书正确，先登录控制器查看该安全网盾有没有被禁用，如果没有，若账号是 AD 域上的账号，检查 LDAP 服务器和 WAC 的网络是否可以互通，用网卡中写入的账号和密码测试一下 LDAP 服务器的有效性，是否能通过，如果账号是本地用户，检查下账号名有没有修改，如果没有被修改检查下用户有没有过期或者被禁用；

5）如果步骤 4 没有问题，则把无线网络频段指定 5.8G，排除无线网络干扰的问题；终端重新接入无线网络，检查是否接入成功；如果接入成功，则是无线网络干扰导致的；

6）如果接入失败，则配置一个 open 的无线网络，转发模式和分配的 vlan 和企业认证

相同，使用无线终端接入 open 的无线网络，检查是否可以接入成功；如果 open 的接入成功，则说明企业认证可能存在问题，请联系我们确认；

6.2.3.3. 终端无法访问外网

检查 WAC 的网络是否可以访问外网。检查 WAC 的网线是否接好，如果确认接好，如果 ping 不通，则排查网络问题：

1）检查 wac 是否可以 ping 通网关地址，如果 ping 不通则检查 wac 配置的 ip 地址是否正确，每个机架都有自己对应的 vlan，需要配置对应 vlan 的地址（机架的纸条上有写对应的 vlan 及地址段）；子网掩码需要是 16 位，wac 网线是否有接在机架出口的交换机上；

2）同一个机架的其他设备是否可以 ping 通出口网关；如果其他设备可以 ping 通，则换个已确认可以使用的网线尝试下；

3）检查 WAC 地址是否可以 ping 200.200.0.20，如果可以 ping 通 200.200.0.20，检查 WAC 的 DNS 服务器是否配置正确，如果 DNS 服务器没有问题，则找 hdd/xjh 确认出口网关上是否放通 WAC 的上网权限；

4）如果无法 ping 通 200.200.0.20，检查 WAC 是否有配置静态路由，如果没有配置则配置对应 vlan 的静态路由；如果配置了，则检查静态路由配置的网关地址是否正确，每个 vlan 需要配置对应的网关地址。