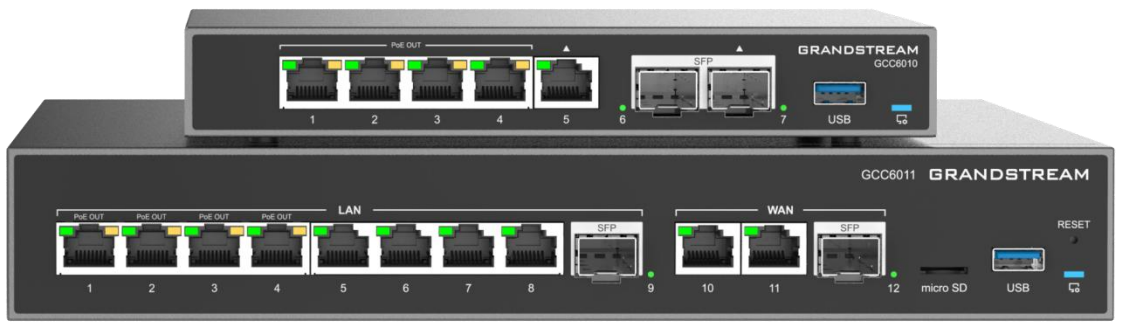
深圳市潮流网络技术有限公司

GCC6010|GCC6011|GCC601W

企业级超融合有线/无线网关

网络设备-用户手册



技术支持

深圳市潮流网络技术有限公司为客户提供全方位的技术支持。您可以与本地代理商或服务提供商联系，也可以与公司总部直接联系。

地址：深圳市南山区科技园北区酷派大厦C座14楼

邮编：518057

网址：http://www.grandstream.cn

客服电话：0755-26014600

客服传真：0755-26014601

技术支持热线：4008755751

技术支持论坛：http://forums.grandstream.com/forums

网上问题提交系统：http://www.grandstream.com/support/submit-a-ticket

商标注明

和其他潮流网络商标均为潮流网络技术有限公司的商标。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

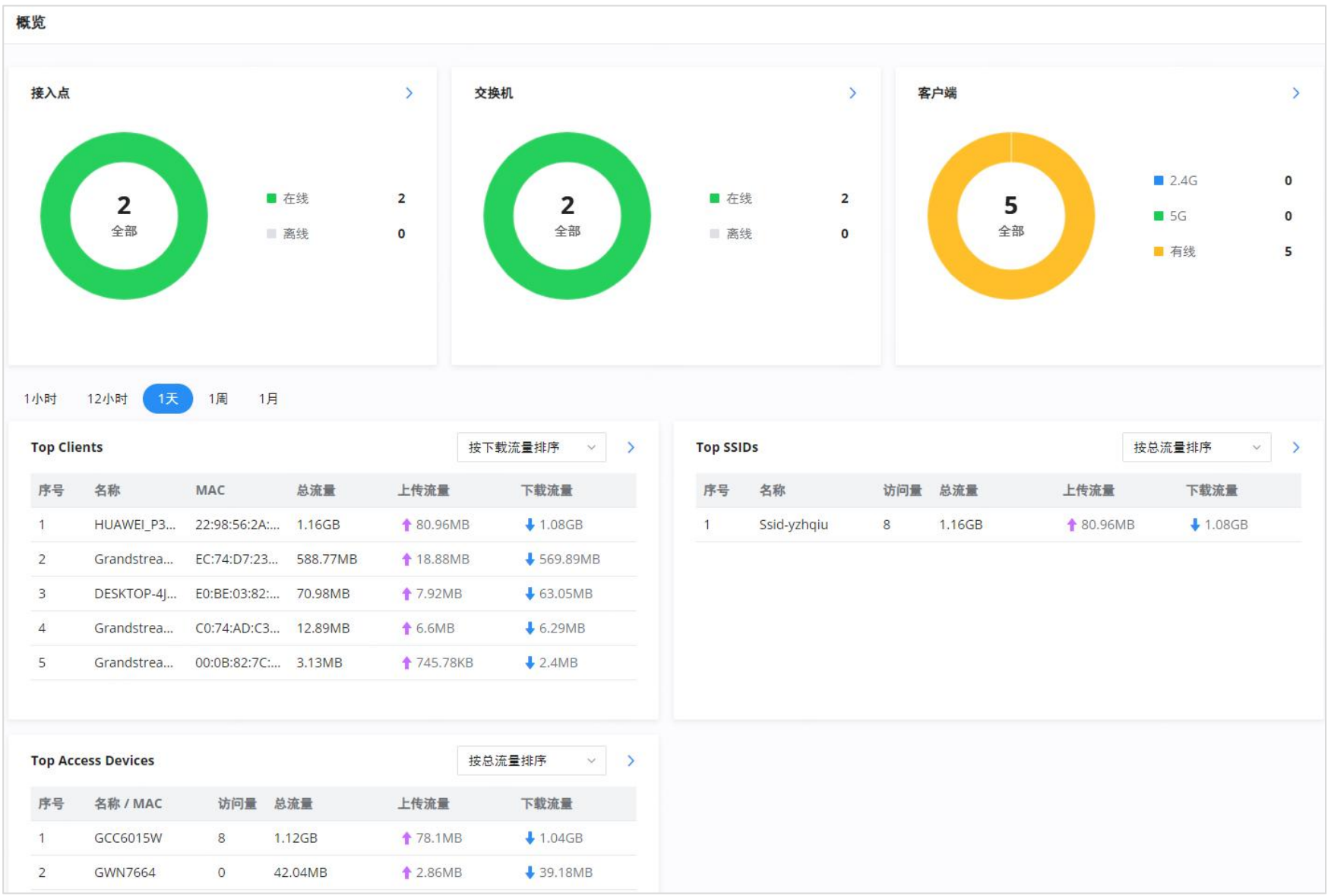
在本指南中，我们将介绍GCC601X(W)网络设备模块的配置参数。

概览

在网络管理的上下文中，网络节点是指形成被监控的互连基础设施的单个设备或组件，如交换机和接入点。这些节点为分析提供数据点，帮助监控平台评估整个网络的运行状况、性能和安全性。

成功登录GCC601X(W)的网络设备Web界面后，概览网页将以仪表板样式提供GCC601X(W)信息的总体视图，以便于监控。

请参阅下图：



概览

接入点	显示在线和在线的访问设备总数。
交换机	显示与GCC601X配对的交换机列表，并显示在线和离线状态设备。
客户	显示无线（2.4 G和5G）和有线连接的客户端总数。
Top客户	显示Top客户端列表，用户可以通过上传或下载对客户端列表进行分类。用户可以点击进入客户端页面查看更多选项。 您可以通过以下方式对连接的客户端进行排序： ● 上传：显示设备使用的总下载速率 ● 下载：显示设备使用的总上传速率 用户还可以指定显示数据的时间跨度，可以是1小时、12小时、1天、1周或1个月

Top SSID	显示Top SSID列表，用户可以根据连接到每个SSID的客户端数量或结合上传和下载的数据使用情况对列表进行分类。用户可以点击进入SSID页面以获得更多选项。 您可以按以下方式对连接的客户端进行排序：连接的设备总数，或访问次数
Top接入点	显示Top接入点列表，根据连接到每个接入点的客户端数量或结合上传和下载的数据使用情况对列表进行分类。单击箭头访问基本和高级配置选项页面。

概览页

AP管理

用户可以添加接入点，该接入点可以使用GCC601X(W)设备中的嵌入式控制器进行控制。

用户可以配对或接管接入点，以便能够对其进行配置。

在GCC601X(W)AP嵌入式控制器上执行的配置将被推送到接入点，提供了对GWN接入点的集中管理。

添加新的访问点

要向GCC601X(W)添加GWN接入点，请导航到Web UI→AP管理

GCC601X(W)无线型号将有一个嵌入式默认AP，带有设备本身的名称，而有线型号（GCC601X）没有任何嵌入式AP。

GWN76XX AP固件版本1.0.25.30及更高版本支持GCC设备的官方在线更新和管理。

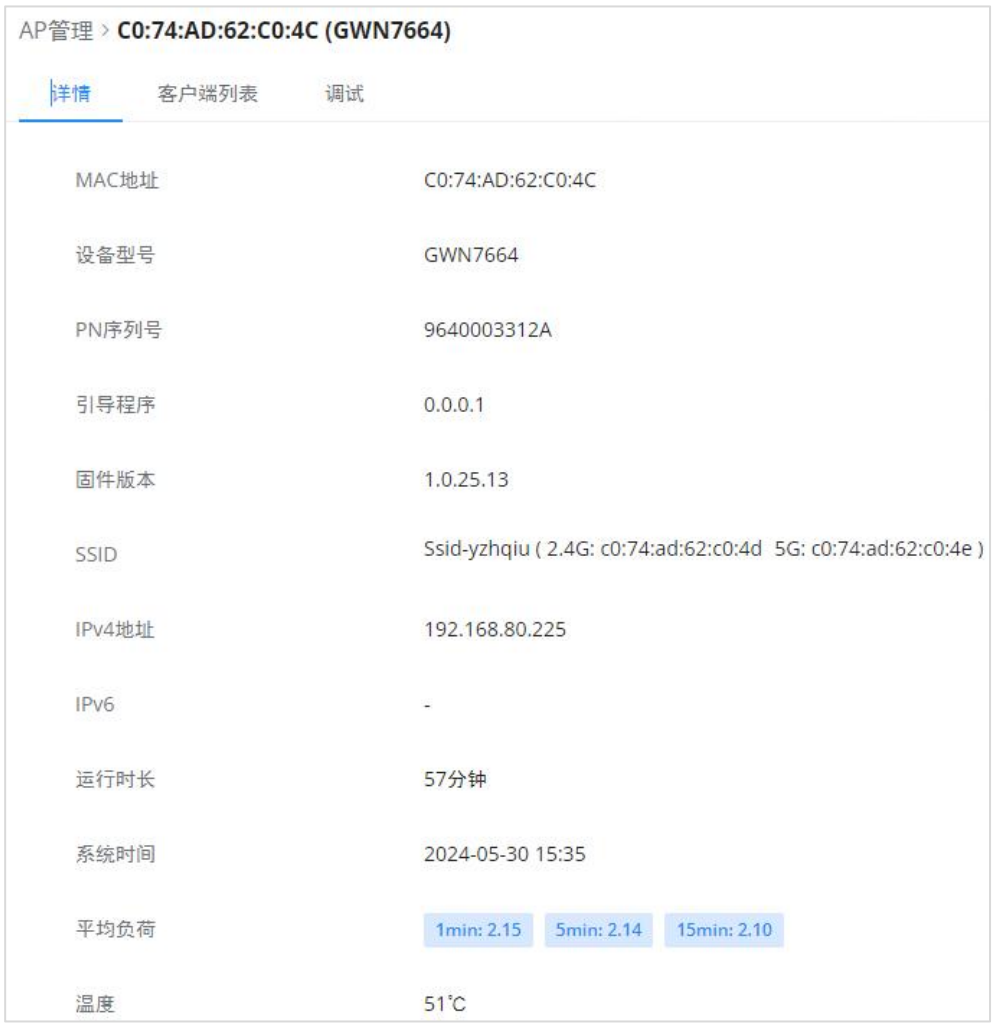
接入点列表

配对AP：配对未设置为主AP时使用此按钮。

接管AP：使用此按钮接管以前被设置为不同主设备的从设备的接入点。要成功配对设备，网络管理员必须输入主设备的密码。

单击配对的GWN AP以查看详细信息、客户端列表和调试工具。

详细信息部分包含配对AP的详细信息，如固件版本、SSID、IP地址、温度等。请参阅下图：



配对APs-详细信息

客户端列表部分列出了通过该AP连接的所有客户端，包括许多信息，如MAC地址、设备名称、IP地址、带宽等。

配对APs-客户端列表

添加接入点后，用户可以选择该接入点并执行以下操作之一：

- 配置AP
- 升级AP
- 删除AP
- 重启AP
- 转移AP
- 分配SSIDs到AP
- 定位AP

配置页面允许管理员升级、重新启动、添加到SSIDs、配置、转移网络组、传输AP、发现AP、故障转移。

GCC601X(W)配置页

升级AP

选择要升级的从属 升级 AP，然后按按钮。

重新启动从属AP

要重新启动从属AP，请选择它，然后单击 重启 按钮。将显示以下确认消息：

重新启动接入点

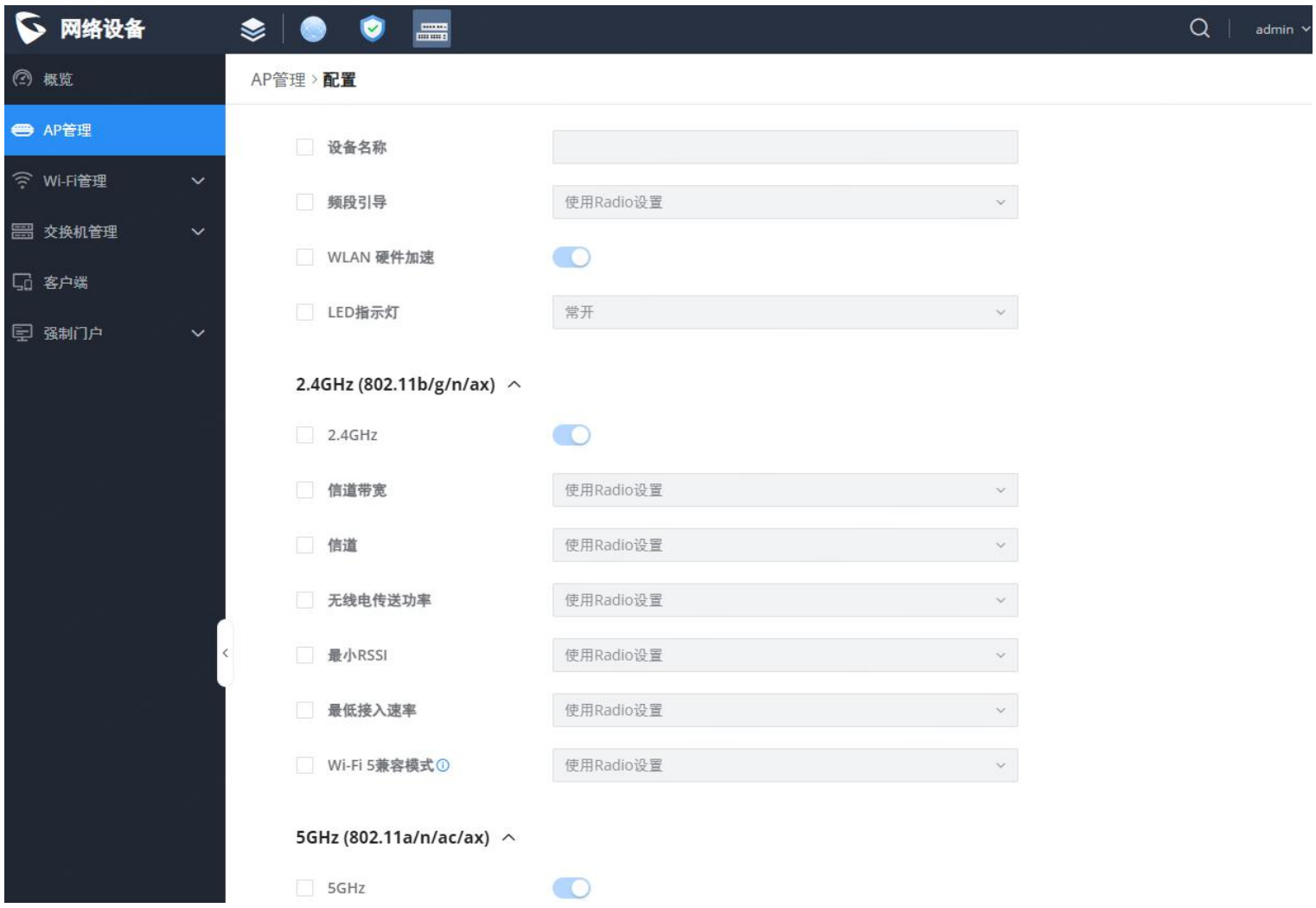
删除访问点

要删除接入点，请选择它，然后单击删除按钮，将显示以下确认消息：

删除接入点

配置接入点

要配置接入点，请选择并单击 配置 按钮。将弹出一个新的配置页面：



设备名称	设置GWN76xx的名称及其MAC地址来标识它。
频段引导	频段控制将帮助客户重定向到2.4 G或5G无线频段（视设备支持的内容而定），以提高效率并从最大吞吐量中获益。允许四种选择： ● 禁用频段控制：这将禁用频段控制功能，接入点将接受客户端选择的频段。 ● 2G优先：2G频段优先于5G频段。 ● 5G优先：5G频段优先于2G频段 ● 平衡：频段控制将在连接到2G和5G的客户端之间进行平衡。 ● 使用Radio设置：将使用Radio页面下确定的值。
LED指示灯	确认LED：四个选项可用：使用系统设置，始终打开，始终关闭，或 时间表。
2.4 g/5G(802.11 b/g/n/ax)	
禁用2.4 GHz/5GHz	此功能允许用户在AP上禁用/启用其2.4 GHz/5GHz频段。
信道带宽	选择信道带宽，注意宽信道将提供更好的速率/吞吐量，窄信道将具有更少的干扰。建议在非常高的密度下使用20Mhz环境。 默认为“使用Radio设置”，AP将使用Radio下确定的值。
信道	选择使用Radio设置或指定频道，默认为自动。请注意，建议的频道取决于系统设置→维护下的国家设置。 默认为“使用Radio设置”，AP将使用Radio页面下确定的值。
Radio功率	根据需要广播的小区大小设置Radio功率 可用：“低”、“中”、“高”、“自定义”和“使用Radio设置”。 默认为“使用Radio设置”，AP将使用Radio下确定的值。
启用最小RSSI	确定是否启用/禁用最小RSSI功能。此选项可以禁用或启用，并手动设置或设置为使用Radio设置。
最低接入速率	指定是否限制客户端的最低访问速率。该功能可以保证客户端与接入点之间的连接质量。此选项可以禁用或启用，并手动设置或设置为使用Radio设置。
Wi-Fi 5兼容模式	某些旧设备对Wi-Fi6支持不好，可能扫描不到信号或者连接不上等。开启后，将会切换到Wi-Fi5模式，解决兼容问题，同时会关闭Wi-Fi6的相关功能。

将SSIDs分配给AP

单击图标，将创建的SSIDs分配给所选AP。

注意

一旦达到SSID的最大数量，不能将设备添加到任何其他SSID中。

定位AP

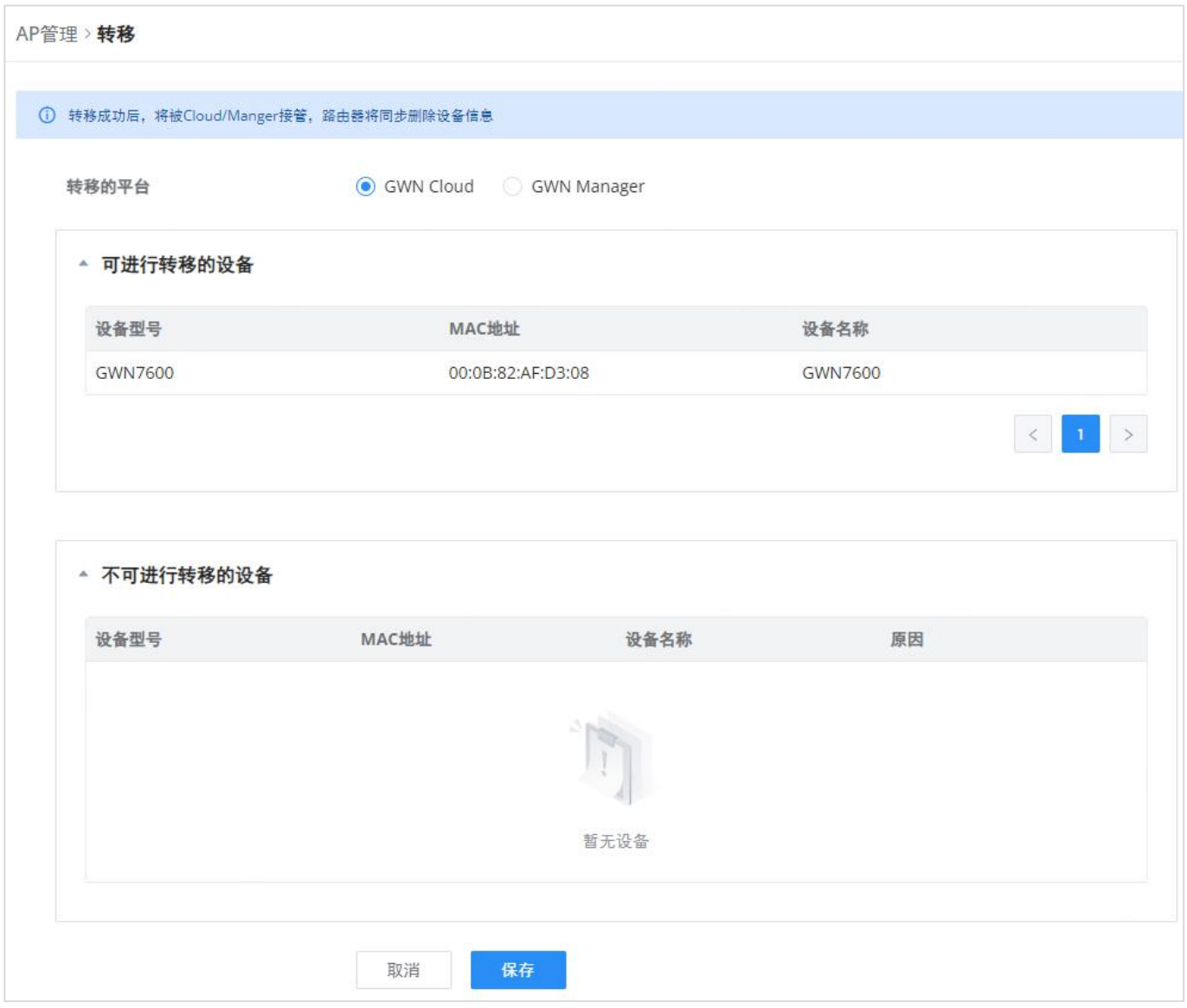
通过单击图标 ，允许GCC610X(W)向连接的AP发送LED通知以定位它。

将接入点转移到GDMS

设备能够将其配对的GWN接入点传输到GDMS。

在AP管理→接入点页面上，选择一个或多个AP，然后点击“转移”按钮，如下所示：

在下一页，选择GDMS（云或本地），然后单击“保存”按钮。用户将被自动转发到GDMS（云或本地）登录。



将AP转移到GDMS

注：

转移成功后，将由云/管理器接管，GCC601X(W)将同步删除设备信息。

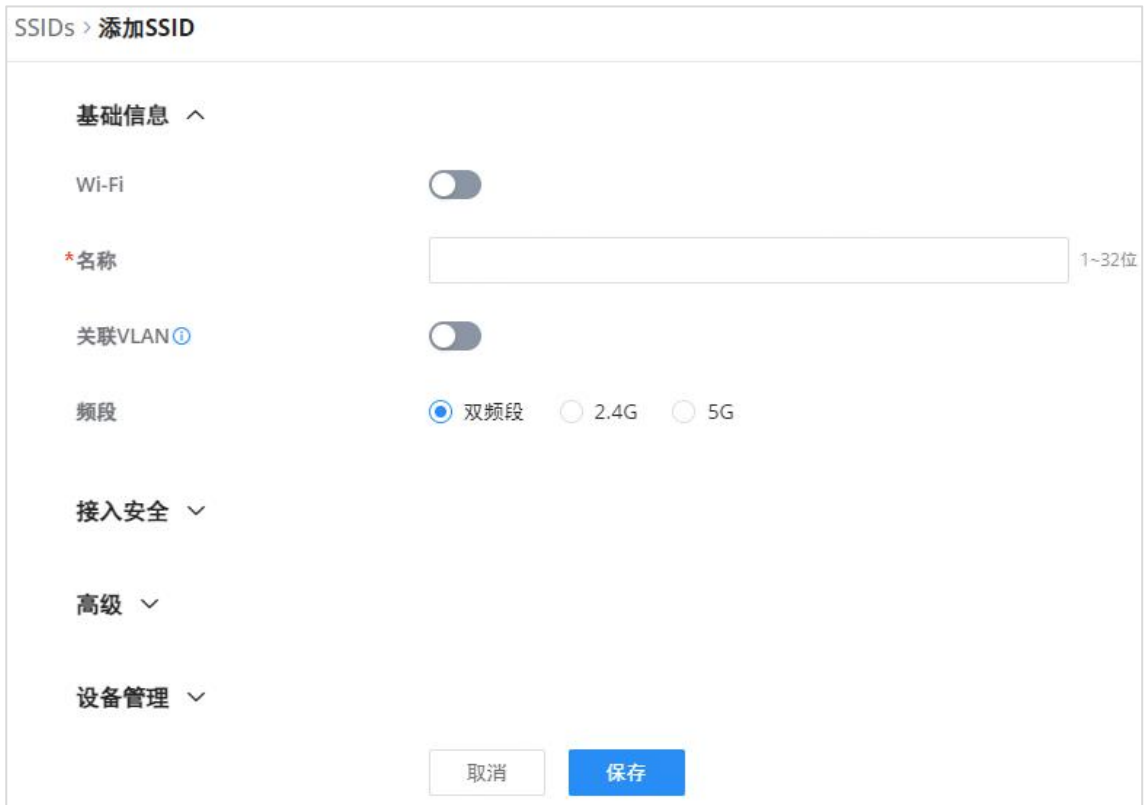
Wi-Fi管理

SSIDs

在此页面上，用户可以配置SSID设置。Wi-Fi SSID将由配对的接入点广播。这提供了对所创建的SSIDs的集中控制，从而使管理许多GWN接入点变得更加容易和方便。

SSID页

要添加SSID，用户应单击“添加”按钮，然后将出现以下页面：



添加SSID

基本资料	
Wi-Fi	打开/关闭Wi-Fi SSID。
名称	输入SSID的名称。
关联VLAN	切换“开”以启用VLAN，然后从列**表中**指定VLAN或单击“添加VLAN”以添加一个。
SSID频段	选择Wi-Fi SSID频段。 ● 双频段：两个频段都将启用。 ● 2.4 G：仅启用2.4 G频段。 ● 5G：仅启用5G频段。
访问安全性	
安全模式	选择Wi-Fi SSID的安全模式。 ● Open ● WPA/WPA2 ● WPA2 ● WPA2/WPA3 ● WPA3 ● WPA3-192
WPA密钥模式	根据所选的安全模式，WPA密钥模式会有所不同，以下选项可用于每个相应的安全模式。 ● Open：它不会有任何WPA键模式 ● WPA/WPA2：它将有PSK和802.1 X WPA密钥模式

	● WPA2：它将有PSK，802.1 x，没有半径的PPSK和有半径的PPSK ● WPA2/WPA3：它将有SAE-PSK和802.1 x ● 支持WPA3：SAE和802.1 x ● 支持WPA3-192：802.1 x
WPA加密类型	选择加密类型： ● AES ● AES/TKIP
WPA共享密钥	输入共享关键短语。连接到Wi-Fi SSID时，需要输入此关键短语。
启用强制网络门户	打开/关闭强制网络门户。 ● 强制网络门户策略：选择创建的强制网络门户策略。
黑名单过滤	选择Wi-Fi SSID的黑名单， 请参阅[黑名单]声明
客户端隔离	● 关闭：允许无线客户端之间的访问。 ● Radio：所有无线客户端将相互隔离。 ● 互联网：访问任何私人IP地址将被阻止。 ● 网关MAC：除了认证网关之外的私有IP地址将被阻止。
高级	
SSID隐藏	启用后，无线设备将无法扫描此Wi-Fi，只能通过手动添加网络进行连接。
DTIM周期	确定Beacon中的传递轨迹指示消息（DTIM）周期。客户端将在每个确定的DTIM周期检查设备中的缓冲数据。出于节能考虑，您可以设置一个较高的值。 请输入1到10之间的整数。
无线客户端限制	确认无线客户端的限制，有效范围为1到256。如果每个Radio都有一个独立的SSID，则每个SSID会有相同的限制。因此，将限制设置为256会将每个SSID独立限制为256个客户端。
客户端活动超时（秒）	如果客户端持续在所设时间内未产生任何流量，设备将会踢除它的接入 。客户端活动超时的默认时长为300秒。
组播广播抑制	● 禁用：所有广播和多播包都将被转发到无线接口。 ● 启用：除DHCP/ARP/IGMP/ND外，所有广播和多播包都将被丢弃。 ● 启用ARP代理：同时启用ARP代理来启用优化。
将IP多播转换为单播	● 禁用：不会将IP多播数据包转换为单播数据包。 ● 被动：设备不会主动发送IGMP查询，IGMP监听条目可能会在300秒后老化，无法作为多播数据转发。 ● 主动：设备将主动发送IGMP查询，并保持IGMP窥探条目更新。
预约	启用，然后从下拉列表中选择，或者创建可以使用此SSID的时间表。

802.11 r	支持Wi-Fi网络中移动设备的快速漫游，通过启用预身份认证和密钥缓存，减少接入点之间转换期间的连接丢失。
802.11 k	通过提供有关附近接入点的信息，使设备能够优化其Wi-Fi连接， 协助无缝漫游和网络效率的提高。
802.11v	通过启用无线资源测量和辅助漫游等功能来增强网络管理，从而改善Wi-Fi环境中的整体网络性能和客户端体验。
ARP代理	一旦启用，设备将避免将ARP消息传输到工作站，同时主动应答局域网中的ARP请求。
U-APSD	确定是否启用U-APSD（计划外自动节能交付）。
带宽限制	打开/关闭带宽限制 ***注：****如果启用了硬件加速，带宽限制不会生效。请转到网络设置/网络加速以禁用*
最大上载带宽	限制此SSID使用的上传带宽。范围是1~1024，如果为空，没有限制。这些值可以设置为Kbps或Mbps。
最大下载带宽	限制此SSID使用的下载带宽。范围是1~1024，如果为空，没有限制，值可以设置为Kbps或Mbps。
带宽限制	打开/关闭带宽计划；如果打开，则**从下拉**列表中选择一个时间表或单击“创建时间表”。
设备管理	
在此部分，用户可以添加和删除可以广播Wi-Fi SSID的GWN接入点。还可以选择通过MAC地址或名称搜索设备。	

添加SSID

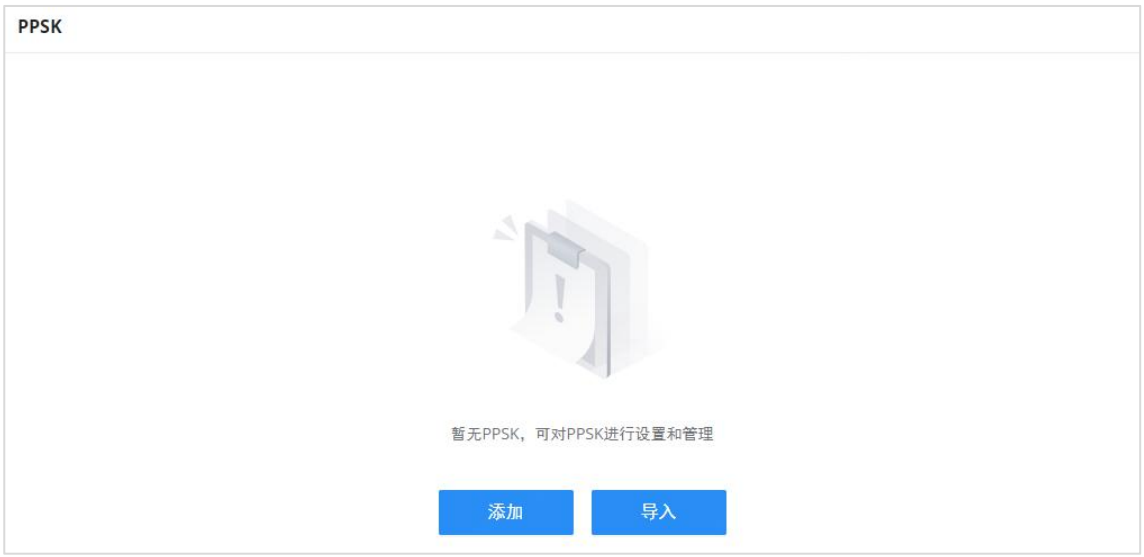
> **注意**
>
> 只有GCC6010W和GCC6015W具有嵌入式AP的默认SSID

私有预共享密钥(PPSK)

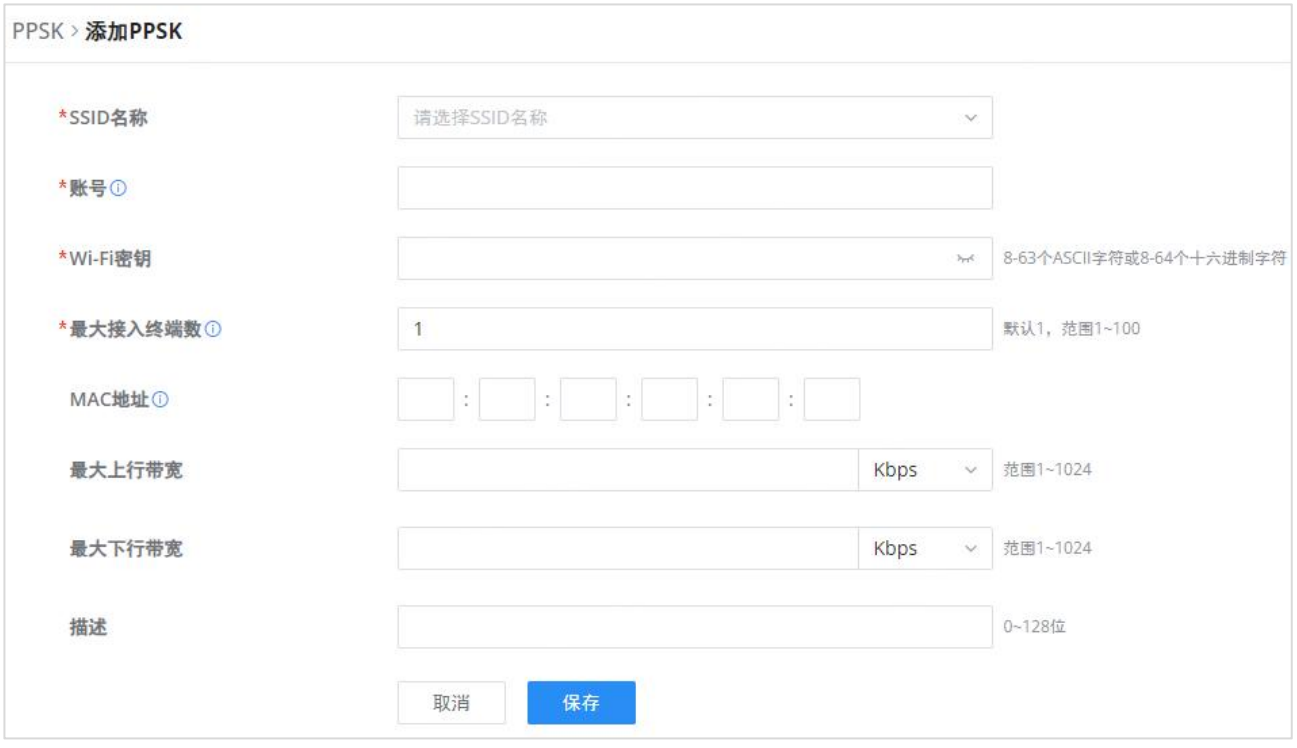
PPSK（私有预共享密钥）是一种为每组客户端创建Wi-Fi密码的方法，而不是为所有客户端使用一个密码。配置PPSK时，用户可以指定Wi-Fi密码、最大访问客户端数量以及最大上传和下载带宽。

要开始使用PPSK，请遵循以下步骤：

1. 首先，创建一个SSID，将WPA密钥模式设置为不带RADIUS的PPSK或带RADIUS的PPSK。
2. 导航到Web UI→AP管理→PPSK页面，然后单击“添加”按钮，然后填写如下字段：



PPSK页面



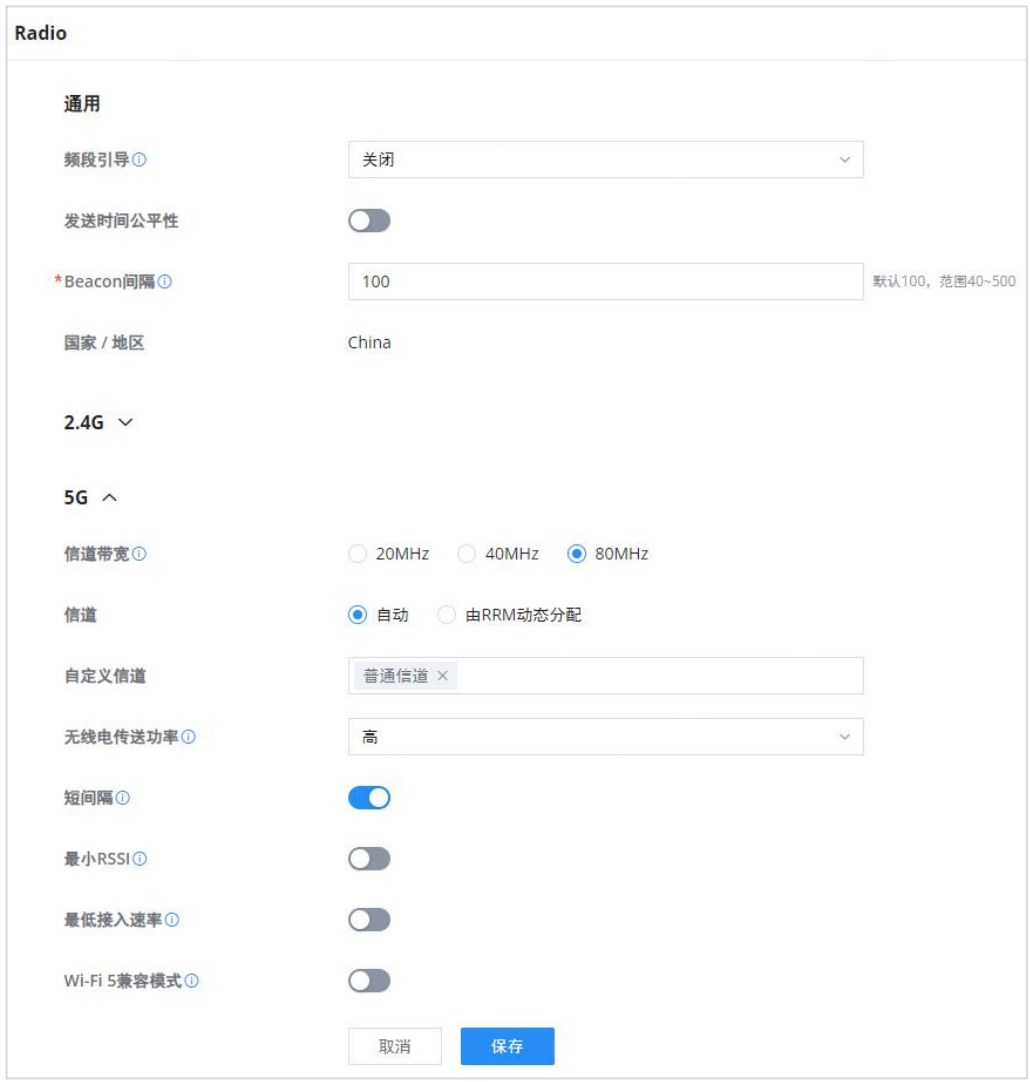
添加PPSK

SSID名称	从下拉列表中选择以前确认的SSID WPA键模式设置为不带半径的PPSK或带半径的PPSK。
账号	如果所选SSID中的WPA密钥模式是“带RADIUS的PPSK”，则该帐户是RADIUS服务器的用户帐户。
Wi-Fi密钥	指定Wi-Fi密码
最大接入终端数	配置同一PPSK帐户允许联机的最大设备数量。
MAC地址	输入MAC地址 ***注意：****只有当访问客户端的最大数量设置为1时，此字段才可用。*
最大上载带宽	以Mbps或Kbps为单位指定最大上传带宽。
最大下载带宽	以Mbps或Kbps为单位指定最大下载带宽。
描述	指定PPSK的说明

添加PPSK

Radio

在Wi-Fi管理→Radio下，用户将能够为GCC创建的所有Wi-Fi SSIDs设置常规无线设置。这些设置将在与GCC配对的接入点级别上生效。



Radio

通用	
频段引导	频段导向功能分为四项：1）2.4 G优先，引导双客户端到2.4 G频段；2）5G优先，将双客户端尽可能引向频谱资源更丰富的5G频段；3）平衡，根据2.4 G和5G的频谱利用率访问这两个频段之间的平衡。为了更好地使用该功能，建议通过SSIDs→高级→启用语音企业启用语音企业。
发送时间公平性	启用通话时间公平性将使接入点和客户端之间的传输更加有效。这是通过向连接到接入点的所有设备提供相等的通话时间来实现的。
Beacon间隔	确定Beacon周期，Beacon周期决定802.11Beacon管理帧GCC发送的频率。请输入一个40到500.1之间的整数。当GCC启用多个间隔值不同的SSIDs时，最大值将生效；2。当GCC启用少于3个SSIDs时，间隔值在40到500之间有效；3。当GCC启用多于2个但少于9个SSIDs时，间隔值将在100到500之间有效；4.当GCC启用8个以上SSIDs时，间隔值在200到500之间有效。注意：网格功能在启用时将占用一部分。
国家/地区	此选项显示已选择的国家/地区。要编辑该区域，请导航至系统设置→基本设置。
2.4G和5G	
信道带宽	选择信道带宽。 ● 2.4 G：20Mhz、20&40Mhz、40Mhz ● 5G：20Mhz、40Mhz、80Mhz
信道	选择接入点如何选择特定信道。 ● 自动： ● 由RRM动态分配

自定义信道	从下拉列表中选择一个自定义频道，有两个类别： • 普通信道 • DFS信道
Radio功率	请根据实际情况选择Radio功率，过高的Radio功率会增加设备之间的干扰。 • 低 • 中 • 高 • 自定义 • 由RRM动态分配 • 自动
短间隔	如果在非多路径环境下启用，这可以提高无线连接速率。
最小RSSI	当信号强度低于最小RSSI时，客户端将被断开连接（除非是Apple设备）。
最低接入速率	指定是否限制客户端的最低访问速率。该功能可以保证连接质量。
Wi-Fi 5兼容模式	一些旧设备不太支持Wi-Fi6，可能无法扫描信号或连接不良。启用后会切换到Wi-Fi5模式，解决兼容性问题。同时会关闭Wi-Fi6相关功能。

Radio

Mesh

通过嵌入在GCC601X(W)设备中的控制器，用户可使用GWN接入点配置Wi-Fi Mesh。配置集中，用户可以查看Mesh的拓扑结构。

- **配置**

要在Mesh网络中成功配置GWN接入点，用户必须首先将接入点与GCC配对，然后在接入点上配置相同的SSID。完成后，用户应导航到AP管理→网格→配置，然后启用网格并配置相关信息，如下图所示。

网格结构

有关需要配置的参数的更多信息，请参考下表。

Mesh	启用网格。启用后，AP在同一个VLAN中最多只能支持5个双频SSIDs和10个单频SSIDs。
扫描间隔（分钟）	确定AP扫描网格的时间间隔。有效范围是1-5。默认值为5。
无线级联	定义无线级联号。有效范围是1-3。默认值为3。
接口	显示哪个界面将用于网格。

网格结构

- **拓扑**

在此页面上，用户将能够看到GWN接入点在Mesh网络中配置时的拓扑结构。该页面将显示与AP相关的信息，如MAC地址、RSSI、信道、IP地址和客户端。它还会显示网格中的级联。

Mesh拓扑

黑名单

黑名单是GCC601X(W)中的一项功能，使用户能够阻止可用的无线客户端或手动添加MAC地址。

要创建新的黑名单，请导航到“Web UI→访问控制→黑名单”下。

- **从列表中添加设备**

输入黑名单的名称，然后从列表中添加设备。

黑名单页

- **手动添加设备**

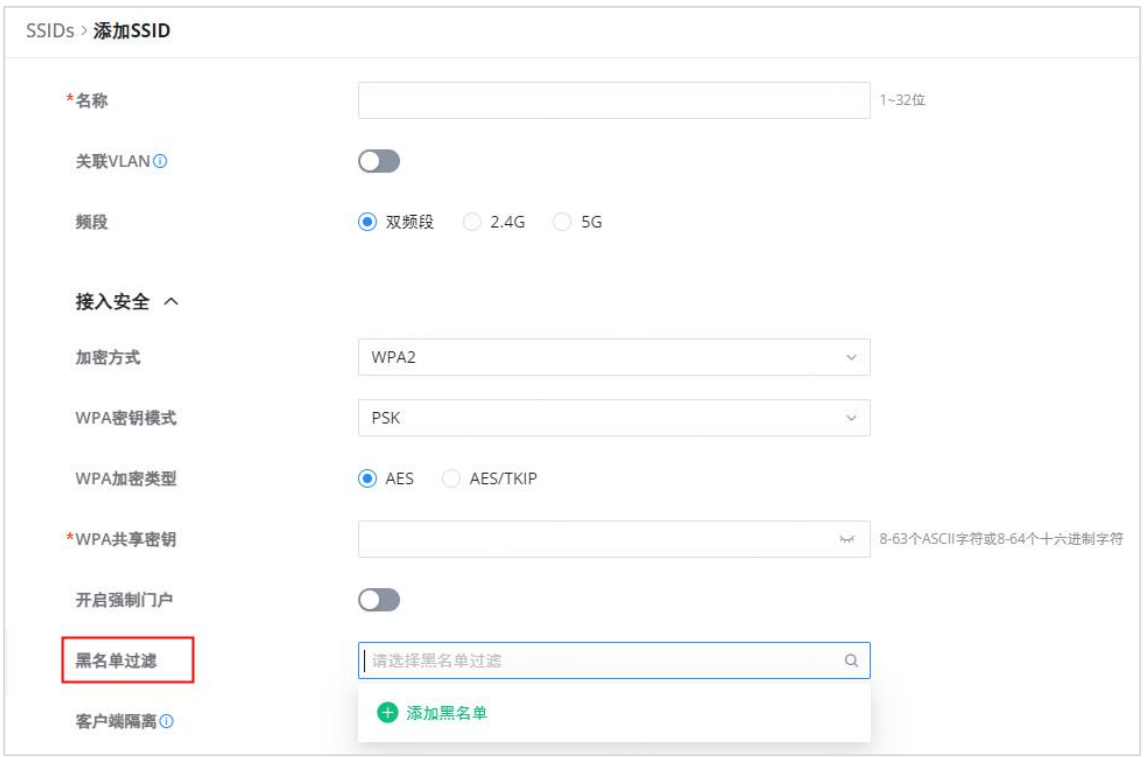
输入黑名单的名称，然后添加设备的MAC地址。

添加黑名单

创建黑名单后，要使其生效，用户需要将其应用于所需的SSID。

导航到“Web UI→Wi-Fi管理→SSID”，单击“添加”按钮创建新的SSID，或单击“编辑”图标编辑以前创建的SSID，向下滚动到“访问安全”部分，然后查找“黑名单过滤”选项，最后从列表中选择以前创建的黑名单，用户可以选择一个或多个，或单击列表底部的“创建黑名单”创建新的黑名单。

请参阅下图：



交换机管理

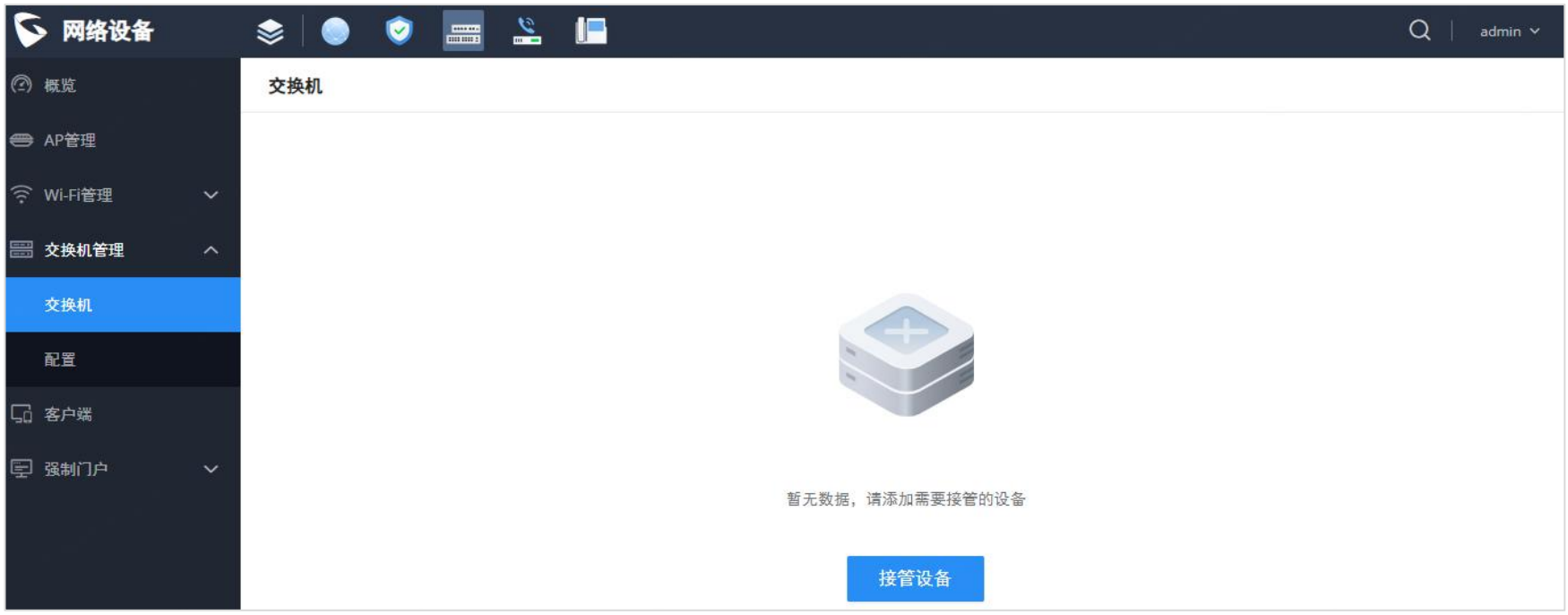
交换机管理包括通过GCC601X监督和控制网络交换机。这包括配置、监控和优化交换机，以实现高效的资源分配和网络故障排除。GCC601X(W)简化了交换机管理，允许组织动态调整其网络基础设施，而无需重大的物理硬件变化，增强了灵活性，并实现了按需服务交付。

以下GWN78xx交换机可由GCC设备管理：

- GWN7801(P)/7802(P)/7803(P)　　1.0.5.34+
- GWN7811(P)/7812(P)/7813(P)/7830/7831　　1.0.7.50+

交换机

用户可以接管GCC601X网络节点的GWN交换机，其工作方式是使用ARP扫描协议发现附近的设备，输入交换机的初始登录密码来接管这些交换机的配置。



接管交换机

接管设备

在发现的GWN78xx交换机中，您可以选择要接管或配置的设备，以完成此操作：

1. 转到交换机管理→交换机。

2. 单击图标 接管设备 显示接管设备设置。

3. 从显示的GWN78xx交换机列表中，选择您想要接管的GWN78xx。

4. 输入其初始登录密码。（在设备的标签上寻找）

5. 单击保存以访问GWN交换机的设置参数。

接管交换机

重新启动设备

要重新启动GWN78xx，请选择GWN交换机，然后单击 “重启”图标。

升级设备

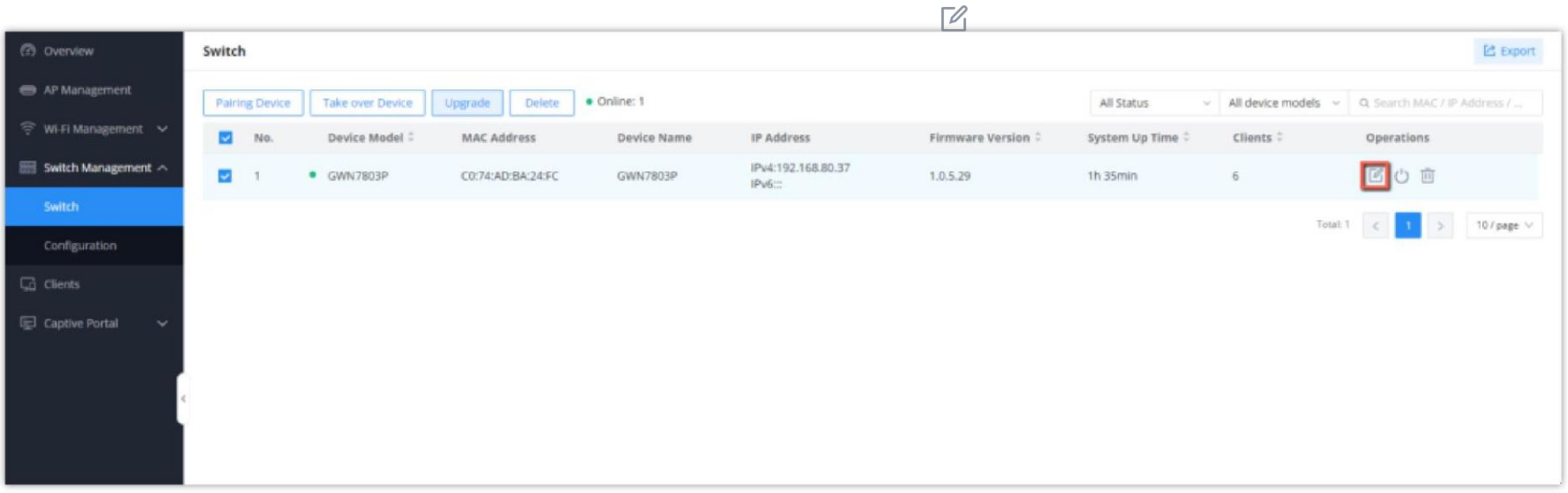
要升级GWN交换机，请选择设备，然后单击“升级”图标。

配置

此部分将包含单个和全局交换机配置以及端口配置文件设置，每个部分都有自己的配置参数。

单个交换机配置

单个交换机配置指的是可以在每个交换机上单独定义的不同设置和参数，要进行配置，请选择所需的交换机，然后单击图标



将出现以下参数：

设备名称	确认设备显示名称

设备备注	包含有关设备的附加信息
设备密码	设置设备SSH远程登录密码和设备web登录密码。
RADIUS身份认证	选择将用于身份认证的RADIUS服务器
添加VLAN接口	
VLAN	选择交换机将使用的VLAN ID，每个VLAN ID只能创建一个VLAN接口，因此不能再选择已使用的VLAN ID。
IPv4地址类型	选择交换机的IP是静态学习还是通过DHCP动态学习
IPv4地址/前置长度	定义VLAN IPv4地址及其子网掩码
IPv6	启用/禁用IPv6
链路本地地址	确认IPv6地址是否自动分配给VLAN，或人工确认
IPv6地址/预加密长度	定义VLAN IPv6地址及其子网掩码
全球单播地址	**有状态DH**CPv6：通过DHCPv6服务器获取IPv6**地址和预认证**。无状态DHCPv6：提供前置、DNS等。根据GCC广告；DHCPv6只提供其他确认信息，不分配地址，需要使用RA数据包的prefinex进行地址分配。 **无状态自动配置：使用**EUI-64格式形成，仅DHCPv6 生成地址的前64位，前6位长度为64。 **SLAAC（无状态地址**自动识别）：允许设备自动 根据从GCC广告接收到的网络预确认他们的IPv6地址，简化VLAN内的网络设置和管理，而无需手动分配地址或DHCP服务器。

全局交换机配置

全局交换机配置将应用于添加的多个GWN交换机的参数。

RADIUS身份认证	
RADIUS身份认证	选择RADIUS服务器或单击添加新RADIUS创建新服务器
添加RADIUS身份认证	
名称	定义RADIUS服务器的名称
认证服务器	RADIUS中的“认证服务器”设置在网络访问尝试期间负责认证用户凭据的服务器。身份认证服务器将按显示的顺序（从上到下）使用，RADIUS服务器将在这些身份认证服务器之后使用。您可以在 认证服务器，您最多可以定义两个认证服务器。
RADIUS计费服务器	RADIUS计费服务器指定负责记录和跟踪用户网络使用数据的服务器。最多可以定义两个RADIUS计费服务器

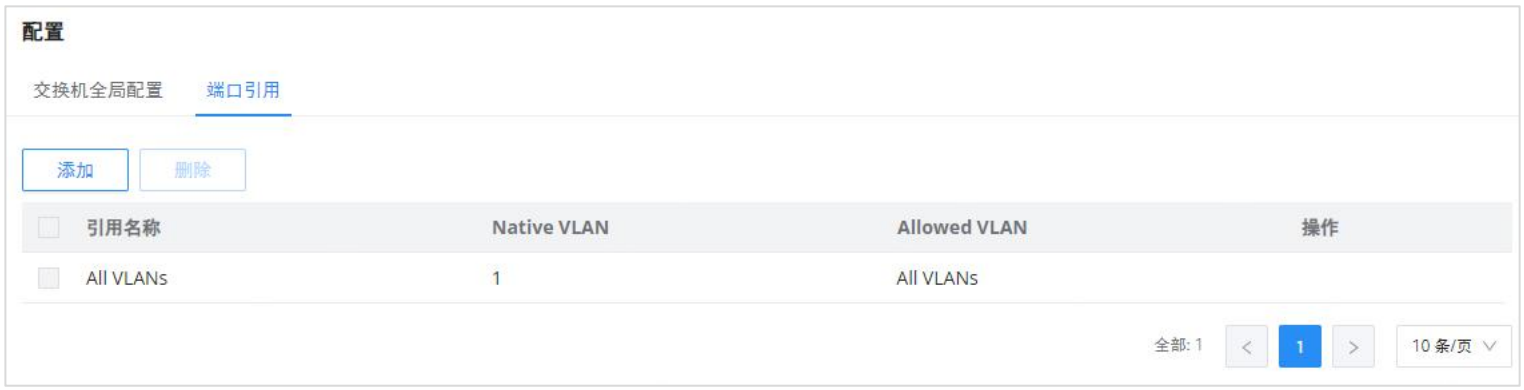
RADIUS NAS ID	确认最多包含48个字符的RADIUS NAS ID。支持字母数字字符， 特殊字符“~！@#$%&*()-+=_”和空格
最大重传次数	设置向RADIUS服务器发送数据包的最大尝试次数
最大重传次数	设置在重新发送RADIUS数据包之前等待RADIUS服务器响应的最长时间
计费更新时长（秒）	设置向RADIUS服务器发送计费更新的频率，单位为秒。输入数字30 ~ 604800。如果外部启动页面也配置了这个，那么外部值将具有优先级。
语音VLAN	
语音VLAN	打开/关闭语音VLAN。
组播	
IGMP侦听VLAN	选择IGMP窥探VLAN。
MLD侦听VLAN	选择MLD监听VLAN。
未知多播数据包	确定交换机（IGMP侦听/MLD侦听）如何处理来自未知组的数据包，可用的选项是丢弃数据包或通过数据包影响网络，建议将其设置为“丢弃”
DHCP侦听设置	
DHCP侦听	打开/关闭DHCP侦听，如果启用，请选择将应用DHCP侦听的VLAN
802.1 x	
VLAN	确定是否为全局端口启用访客LAN功能。
其他	
巨型帧	输入巨型帧的大小。范围：1518-10000

端口引用

端口配置文件是一种配置，可用于一次将许多设置应用于交换机端口，以便快速批量更改设置。

默认情况下，您可以找到一个名为“All VLANs”的不可编辑端口配置文件，此设置是默认设置，应用于任何添加的交换机上的所有连接端口。

要创建新的自定义端口配置文件，请单击图标 添加 。



端口配置文件配置

添加端口配置文件——常规

添加端口配置文件——安全性

通用	
引用名称	指定引用文件的名称。
本地VLAN	从下拉列表中选择本机VLAN（默认局域网）。
允许的VLAN	从下拉列表中检查允许的VLAN（一个或多个VLAN）。
语音VLAN	打开或关闭语音VLAN。 ***注意：****请首先在全局局域网设置中启用语音VLAN。*
速率	从下拉列表中指定速率（端口速率）。
双工模式	选择双工模式： ● 自动协商：接口的双工状态由本地端口和对等端口之间的自动协商决定。 ● 全双工：强制全双工，接口允许同时发送和接收数据包。 ● 半双工：强制半双工，接口一次只发送或接收数据包。
流量控制	启用后，如果本地设备发生拥塞，设备将向对等设备发送消息，通知其暂时停止发送数据包。接收到消息后，对等设备停止向本地设备发送数据包。 ***注意：****当双工模式为“半双工”时，交通控制不生效。*
入方向限速	打开或关闭进入速率限制。
CIR(Kbps)	确认承诺信息率，即交易通过的平均比率 穿过。

出方向限速	打开或关闭出站速率限制。
CIR(Kbps)	确认承诺信息率，即交易通过的平均比率 穿过。
LLDP-MED	打开或关闭LLDP医疗。
网络策略TLV	打开或关闭网络策略TLV。
安全	
风暴控制	打开或关闭风暴控制。
端口隔离	打开或关闭端口隔离。
端口安全	打开或关闭端口安全性。 ***注**：启用后，开始MAC地址学习，包括动态和静态MAC地址。*
最大MAC数	指定允许的最大MAC地址数。 ***注**意：达到最大数量后，如果收到源MAC地址不存在的数据包，无论目的MAC地址是否存在，交换机都会认为有来自非法用户的攻击，并根据端口保护规定保护接口。*
Sticky MAC	打开或关闭Sticky MAC。 ***注**意：启用后，接口会将学习到的安全动态MAC地址转换为粘性MAC。如果达到了MAC地址的最大数量，则接口所获取的非粘性MAC条目中的MAC地址将被丢弃，并且根据端口保护定义来确定是否报告陷阱警报。*
802.1 x认证	打开或关闭802.1 x身份认证。
用户认证模式	从下拉列表中选择用户身份认证模式 ● **基于Mac**：允许多个用户在不影响彼此的情况下进行身份认证； ● **基于端口**：允许对多个用户进行身份认证。只要一个用户通过了身份认证，其他用户就可以免于身份认证。
方法	从下拉列表中选择方法。
访客VLAN	打开或关闭访客VLAN。 ***注**意：首先在全局局域网设置中启用访客VLAN。*
端口控制	从下拉列表中选择端口控制： ● 禁用 ● 强制认证 ● 强制非认证 ● 自动
重认证	确定是否为连接到端口的设备启用重新身份认证。

添加端口配置文件

添加端口配置文件后，用户可以将其应用于GWN设备/设备组端口（例如：GWN交换机）。

在“交换机设备”页面下，选择相关设备，在“端口”选项卡下，选择端口，然后在这些端口上应用端口配置文件。

客户端

“客户端”页面保存了当前或以前连接到不同LAN子网的所有设备和用户的列表，包括MAC地址、IP地址、持续时间、上传和下载信息等详细信息。

可以从GCC601X的Web GUI→网络设置→客户端访问客户端列表，为有线和无线客户端执行不同的操作。

- 单击“清除离线客户端”从列表中删除未连接的客户端。
- 单击“导出”按钮，以EXCEL格式将客户端列表导出到本地设备。

请参阅下图：

客户端页面

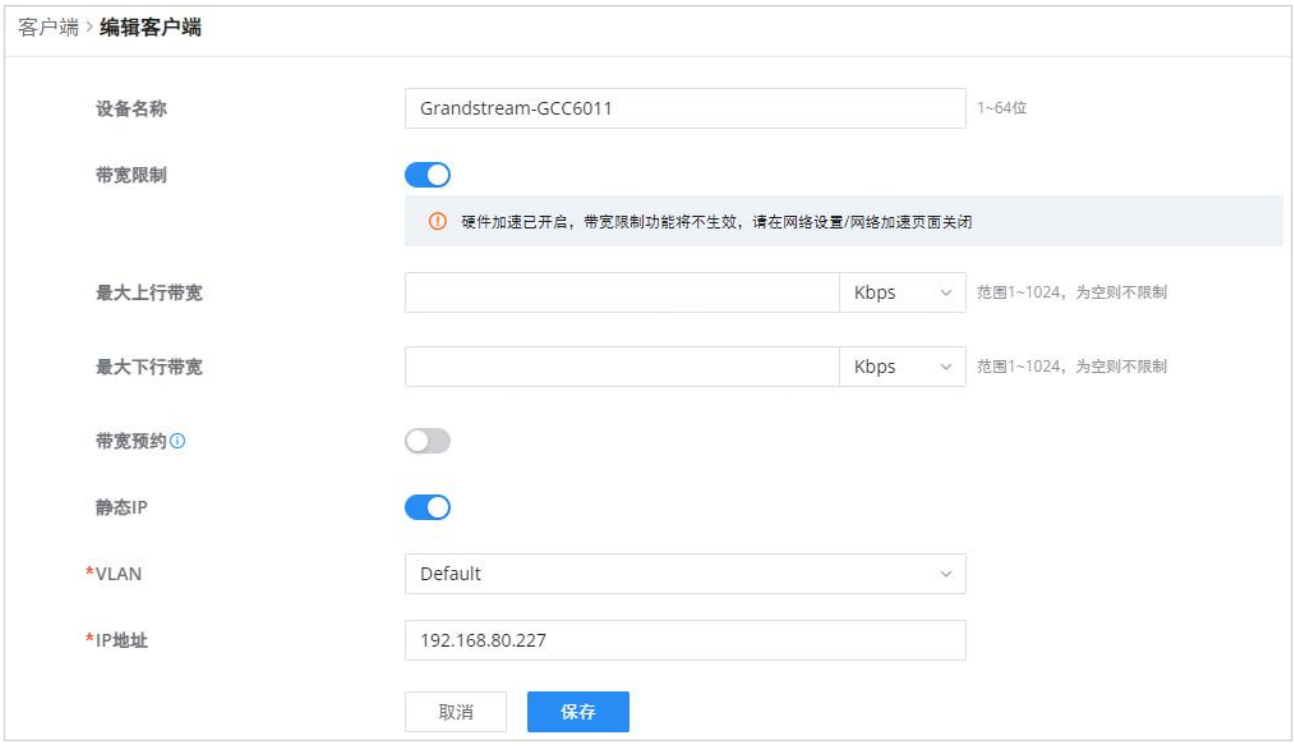
MAC地址	本节显示连接到GCC的所有设备的MAC地址。
设备名称	本节显示连接到GCC的所有设备的名称。
VLAN	显示客户端连接的VLAN。
IP地址	本节显示连接到GCC的所有设备的IP地址。
连接类型	本节显示设备正在使用的连接类型。有两种类型可用于连接： ● 无线：使用GCC的接入点。 ● 有线：使用有线以太网，或者直接连接到GCC的局域网端口，或者通过交换机。
信道	如果设备通过接入点连接，GCC将检索设备连接到哪个信道的信息。
SSID名称	如果设备通过接入点连接，GCC将检索设备连接到哪个SSID的信息。
关联设备	在接入点或GCC接入点的情况下，此部分将显示所用设备的MAC地址。
连接时长	这表示设备连接到GCC的时间。
RSSI	RSSI代表接收信号强度指示器。它指示连接到与GCC配对的AP的设备的无线信号强度。
工作站模式	此栏表示接入点的站模式。
总流量	设备和GCC之间交换的总数据。
上传流量	设备上传的数据总数。
下载流量	设备下载的数据总数。

实时速率	设备使用的实时WAN带宽。
链路速率	此栏表示链路可以传输的总速率。
制造商	此栏表示该设备的制造商。
操作系统	此栏表示设备上安装的操作系统。

客户端页面

- **编辑设备**

在“操作”列下，单击“编辑”图标设置设备名称，并为设备分配VLAN ID和静态地址。还可以限制该设备的带宽，从预约列表中分配一个时间表。请参阅下图：



编辑设备

- **删除设备**

要删除设备，请转到操作列并单击按钮 然后点击“删除”。请注意，您只能删除离线设备，不能删除在线设备。

强制门户

GCC601X上的强制网络门户功能有助于定义登录页面（网页），当尝试访问互联网时，该页面将显示在Wi-Fi客户端的浏览器上。一旦连接，Wi-Fi客户端将被迫查看该登录页面并与之交互，然后才能获得互联网接入许可。

强制网络门户功能可以从GCC601X网络设备的“强制网络门户”进行配置。

策略

用户可以在此页面上自定义门户策略。单击“添加”按钮添加新策略，或单击“编辑”编辑以前添加的策略。

策略页

策略配置页面允许添加多个强制网络门户策略，这些策略将应用于SSIDs，并包含不同身份认证类型的选项。

策略名称	输入策略名称。
启动页	• 内部 • 外部
客户端有效期	指定客户端网络连接的过期时间。超时后，客户端应重新认证以供进一步网络使用。
客户端闲置超时（分）	指定访客网络连接的空闲超时值。超时后，访客应重新认证以供进一步网络使用。
每日限额	启用时，客户端每天只允许访问一次。

启动页定制	选择自定义启动页面。
登录页面	通过页面设置门户身份认证，以自动跳转到目标页面。
HTTPS重定向	如果启用，从工作站发送的HTTP和HTTPS请求都将使用HTTPS协议进行重定向。并且工作站在认证前进行HTTPS浏览时可能会收到无效认证错误。如果禁用，将只重定向http请求。
安全门户	如果启用，STA和GCC之间的通信将使用HTTPS协议。否则，将使用HTTP协议。
预身份认证规则	设置预身份认证规则，允许客户端在成功身份认证之前访问一些URL。
认证后规则	设置post身份认证以限制用户在身份认证成功后访问以下地址。

策略页

启动页

启动页面允许用户通过易于配置的菜单生成定制的启动页面，该页面将在用户尝试连接到Wi-Fi时显示给用户。

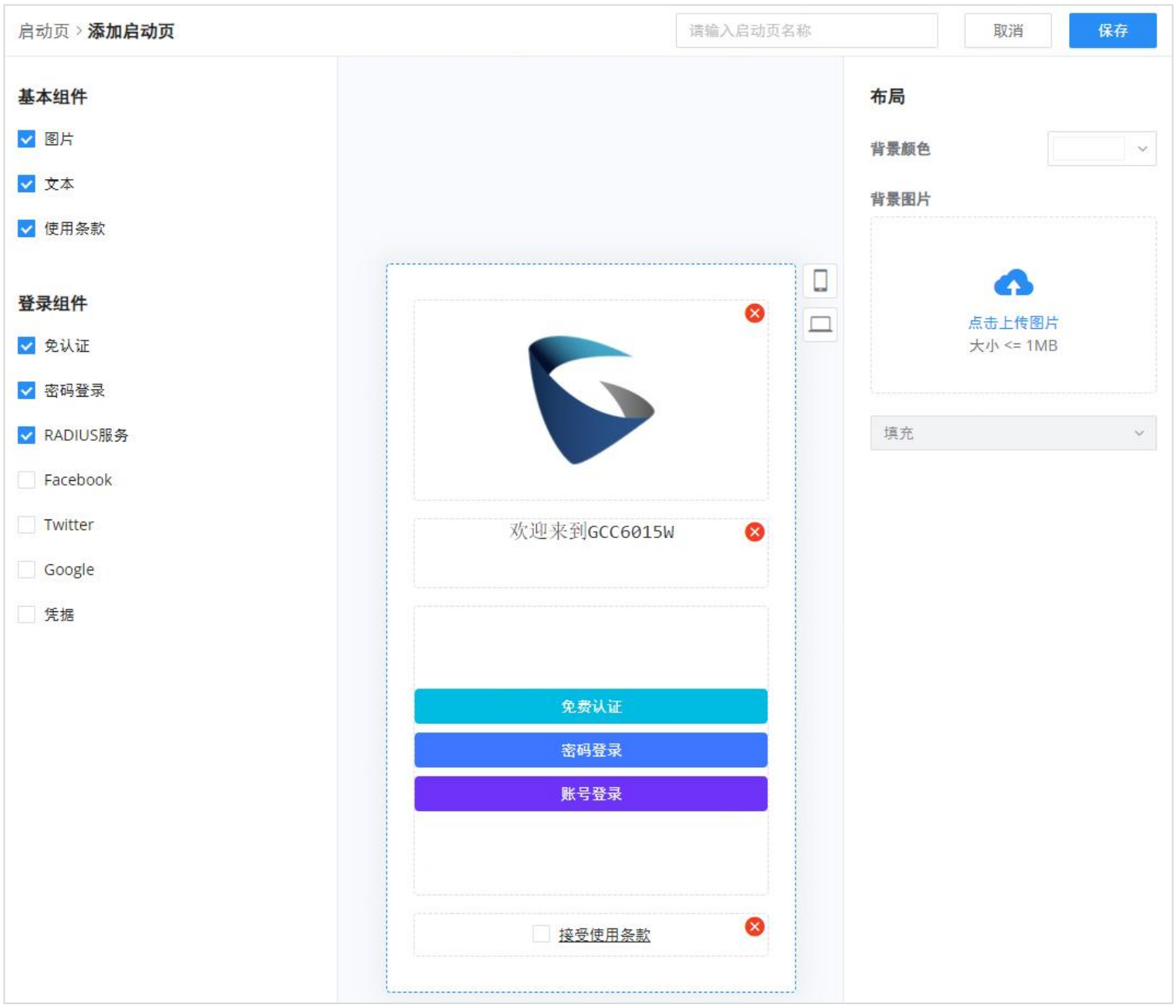
在此菜单上，用户可以创建多个启动页面，并将每个页面分配给单独的强制网络门户策略，以实施选择身份认证类型。

生成工具提供了一种直观的“所见即所得”方法，通过非常丰富的操作工具定制强制网络门户。

要添加启动页面，请单击“添加”按钮或单击“编辑”图标来编辑以前添加的页面。

用户可以设置以下内容：

- 身份认证类型：从支持的身份认证方法中添加一种或多种方式（简单密码、RADIUS服务器、免费、脸书、Twitter、Google和凭据）。
- 设置要在启动页面上显示的图片（公司徽标）。
- 自定义页面布局和背景颜色。
- 自定义使用条款文本。
- 可视化移动设备和笔记本电脑的预览。



添加/编辑启动页面

访客

此页面显示通过强制网络门户连接的客户端的信息，包括MAC地址、主机名、身份认证类型等。

要导出所有访客的列表，请点击“导出访客列表”按钮，然后将下载一个EXCEL文件。

访客页面

凭据

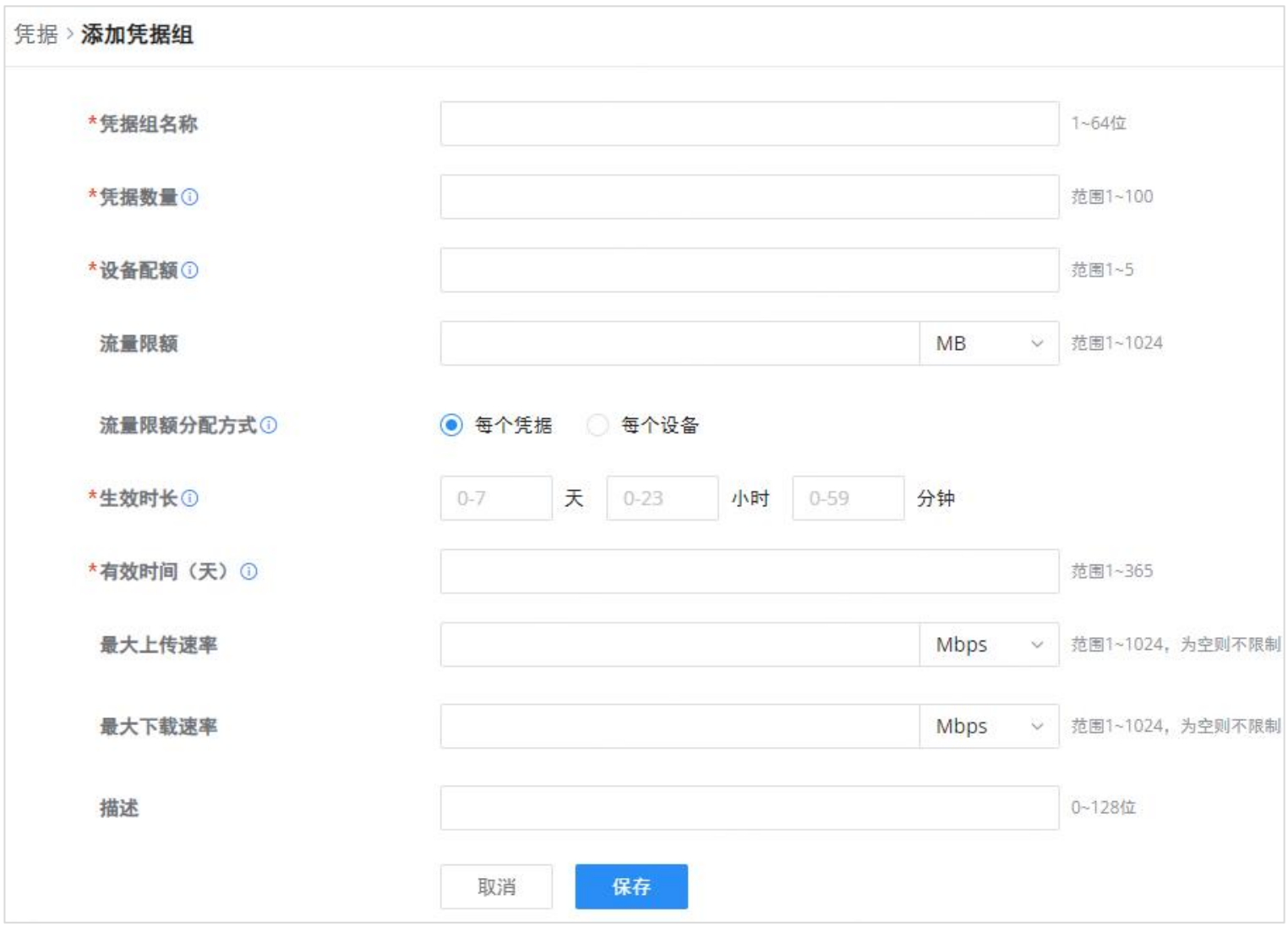
凭据功能将允许客户使用平台控制器随机生成的代码在有限的时间内访问互联网。

例如，一家咖啡店可以使用凭据代码通过Wi-Fi向客户提供互联网接入，凭据代码可以在每个命令中交付。一旦凭据过期，客户就不能再连接到互联网。

请注意，多个用户可以使用单个凭据进行连接，凭据的过期持续时间在允许的用户之一首次成功连接后开始计算。

同时，管理员可以根据当前网络负载，用户配置文件(VIP客户获得比普通客户更快的速度等)和可用的互联网连接(光纤，DSL或电缆等.)设置每个创建凭据的数据带宽限制，以避免连接拥塞和服务缓慢。

单击“添加”按钮创建凭据组。填写字段时，请参考下图。



添加/编辑凭据

> **注：**
>
> 通过强制网络门户连接的客户端（包括凭据）将列在强制网络门户→访客下的访客页面上。

添加凭据组

凭据组名称	定义凭据组名称
凭据数量	确定要创建的凭据数量，有效范围为1-100个凭据
设备配额	设置已创建凭据允许的最大设备数量（基于MAC），有效范围为1-5
流量限额	定义一个用户可以传输的最大数据量（以字节为单位） 访问受限或过期，这可以用MB或GB定义，范围是1-1024
流量限额分配方式	定义分配方法 ● 每个凭据：字节限制将分配给凭据内的所有设备 ● 每个设备：每个设备的总使用量是字节限制
生效时长	定义凭据有效的时限，并可用于访问网络。
有效时间（天）	确定凭据的有效期。过期后，凭据无效。

最大上载速率	定义访问使用凭据的网络。
最大下载速率	定义访问的用户可以下载数据的最大速率使用凭据的网络。
描述	为创建的凭据提供详细说明