配置9800 WLC和Aruba ClearPass — 访客接入和FlexConnect

目录

相关信息

简介

本文档介绍Catalyst 9800无线LAN控制器(WLC)与Aruba ClearPass的集成，以提供访客无线服务集标识符(SSID)，该SSID利用集中式Web身份验证(CWA)在接入点(AP)部署的Flexconnect模式下向无线客户端进行身份验证。

访客无线身份验证由访客门户支持，带有匿名可接受用户策略(AUP)页面，托管在Aruba Clearpass的安全隔离区(DMZ)网段中。

先决条件

本指南假设已配置并验证以下组件：

- 所有相关组件均同步到网络时间协议(NTP)，并验证其时间是否正确（证书验证需要）
- 运行DNS服务器(访客流量流需要，证书撤销列表(CRL)验证)
- 可操作的DHCP服务器
- 可选的证书颁发机构(CA)（签署CPPM托管访客门户时需要）
- Catalyst 9800 WLC
- Aruba ClearPass服务器（需要平台许可证、访问许可证、板载许可证）
- Vmware ESXi

要求

Cisco 建议您了解以下主题：

- C9800部署和新配置模型
- C9800上的Flexconnect交换
- 9800 CWA身份验证(请参阅:https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213920-central-web-authentication-cwa-on-cata.html)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行17.3.4c的Cisco Catalyst C9800-L-C
- 思科Catalyst C9130AX
- Aruba ClearPass，6-8-0-109592和6.8-3补丁
- MS Windows服务器 Active Directory（GP配置为向受管终端自动发布基于计算机的证书）带选项43和选项60的DHCP服务器DNS 服务器NTP服务器对所有组件进行时间同步CA

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

该图显示了访客WiFi接入交换的详细信息，然后允许访客用户访问网络：

1.访客用户与远程办公室中的访客Wifi关联。

2.初始RADIUS访问请求由C9800代理到RADIUS服务器。

3.服务器在本地MAC终端数据库中查找提供的访客MAC地址。
如果未找到MAC地址，则服务器会使用MAC身份验证绕行(MAB)配置文件进行响应。此RADIUS响应包括：

- URL重定向访问控制列表(ACL)
- URL重定向

4.客户端通过IP Learn过程为其分配IP地址。

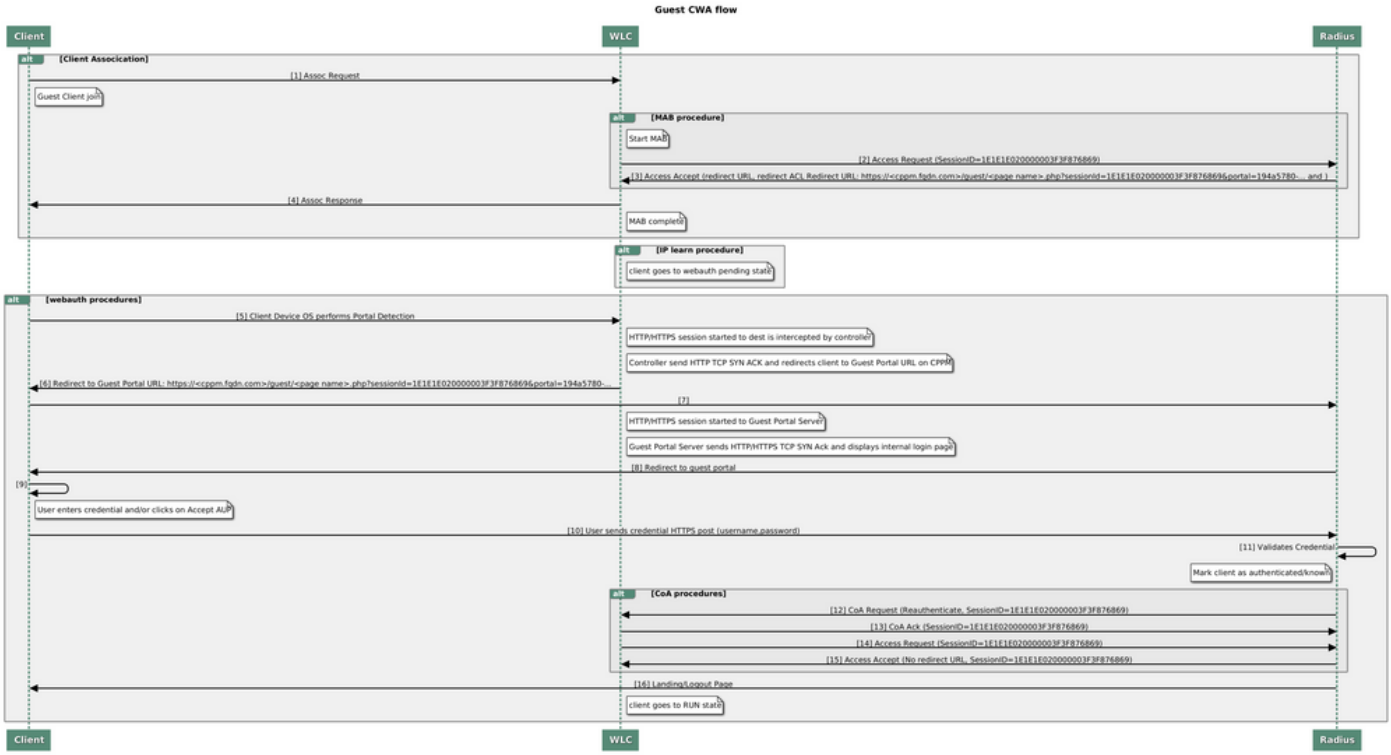
5. C9800将访客客户端（由其MAC地址标识）转换为“Web Auth Pending”状态。

6.大多数与访客WLAN关联的现代设备操作系统都执行某种强制网络门户检测。
确切的检测机制取决于具体的操作系统实施。客户端操作系统会打开一个弹出窗口（伪浏览器）对话框，其中页面由C9800重定向到访客门户URL，由RADIUS服务器托管，作为RADIUS访问接受响应的一部分提供。

7.访客用户接受显示的弹出窗口ClearPass上的条款和条件，在其终端数据库(DB)中为客户端MAC地址设置一个标志，以指示客户端已完成身份验证，并通过根据路由表选择接口（如果ClearPass上存在多个接口）来启动RADIUS授权更改(CoA)。

8. WLC将访客客户端转换为“运行”状态，用户无需进一步重定向即可访问Internet。

> **注意**：有关Cisco 9800外部、锚点无线控制器与RADIUS和外部托管访客门户的状态流程图，请参阅本文的附录部分。



访客中心Web身份验证(CWA)状态图

CWA访客企业部署的流量

在具有多个分支机构的典型企业部署中，每个分支机构都设置为在访客接受EULA后通过访客门户提供对访客的安全分段访问。

在此配置示例中，9800 CWA用于访客接入，通过集成到单独的ClearPass实例，该实例专门为网络安全DMZ中的访客用户部署。

访客必须接受DMZ ClearPass服务器提供的Web同意弹出门户中列出的条款和条件。此配置示例重点介绍匿名访客访问方法（即，无需访客用户名/密码即可对访客门户进行身份验证）。

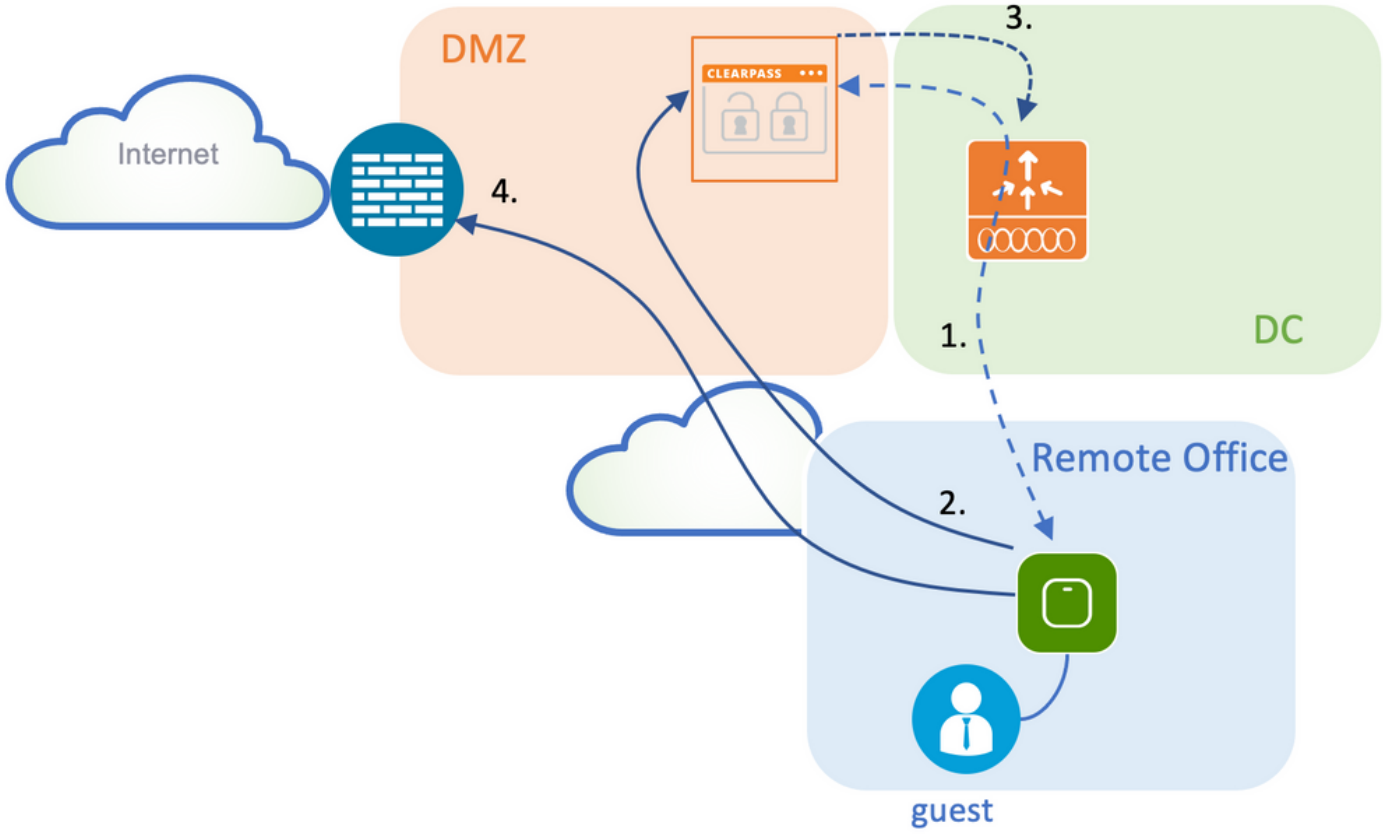
与此部署对应的流量如图所示：

1. RADIUS - MAB阶段

2.访客客户端URL重定向到访客门户

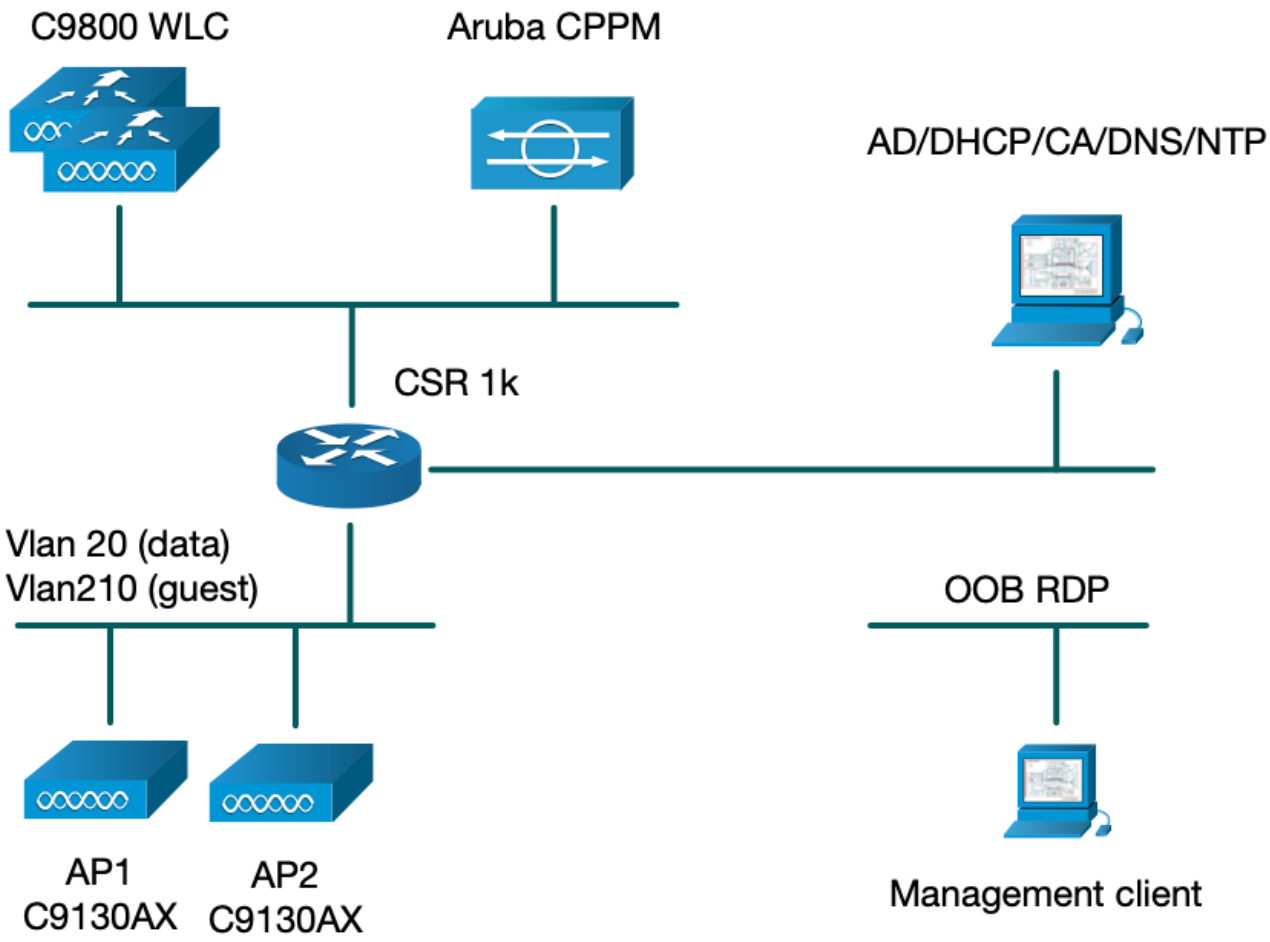
3.访客在访客门户上接受EULA后，RADIUS CoA Reauthenticate从CPPM颁发到9800 WLC

4.允许访客访问互联网



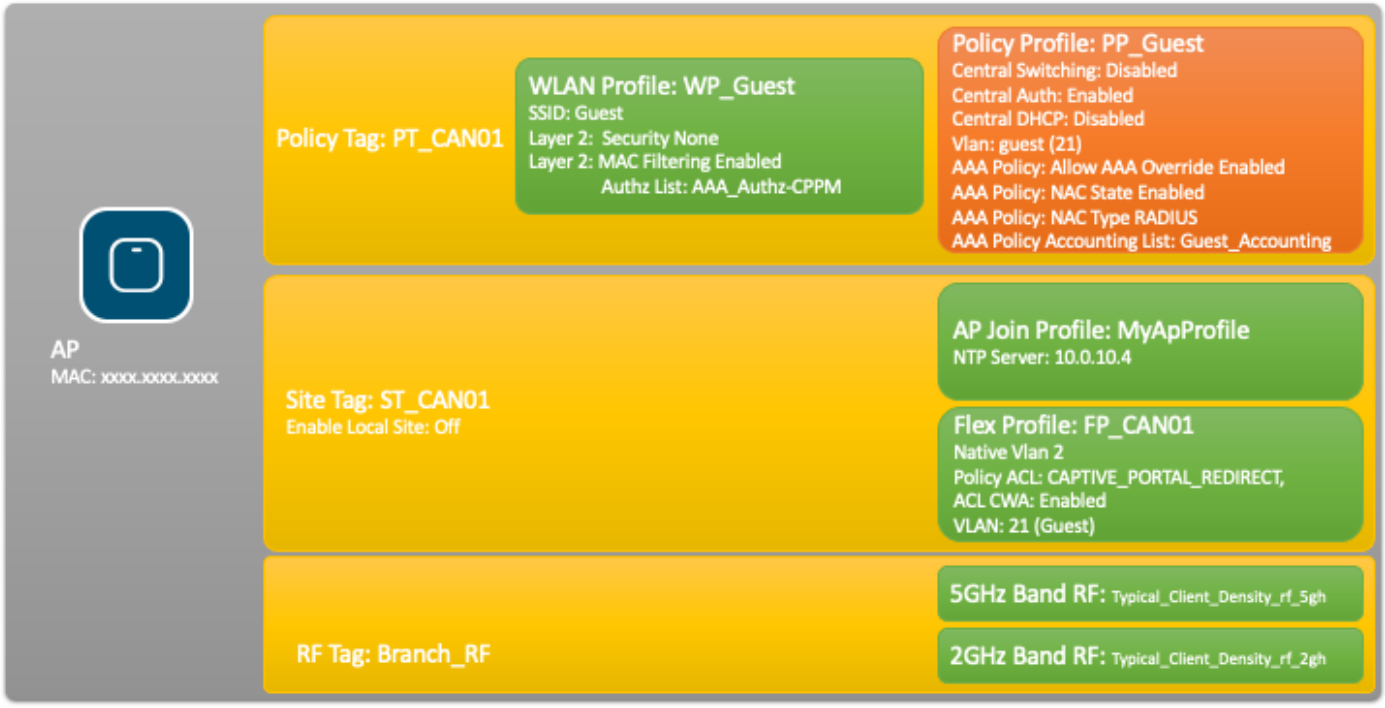
网络图

注意：出于实验室演示目的，单个/组合的Aruba CPPPM服务器实例用于同时提供访客和公司SSID网络访问服务器(NAS)功能。最佳实践实施建议独立NAS实例。



配置

在此配置示例中，利用C9800上的新配置模式创建必要的配置文件和标记，为企业分支机构提供dot1x企业访问和CWA访客访问。下图总结了生成的配置：

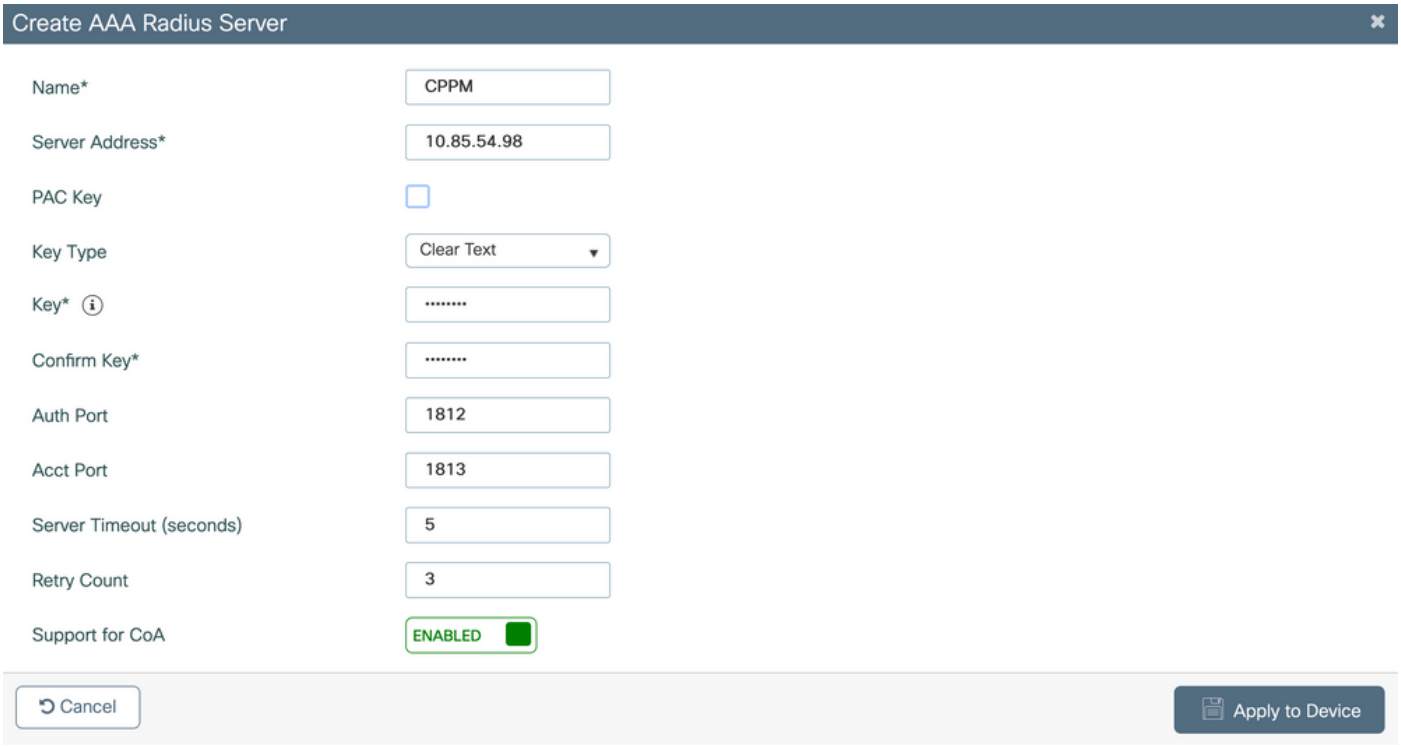


配置访客无线接入C9800参数

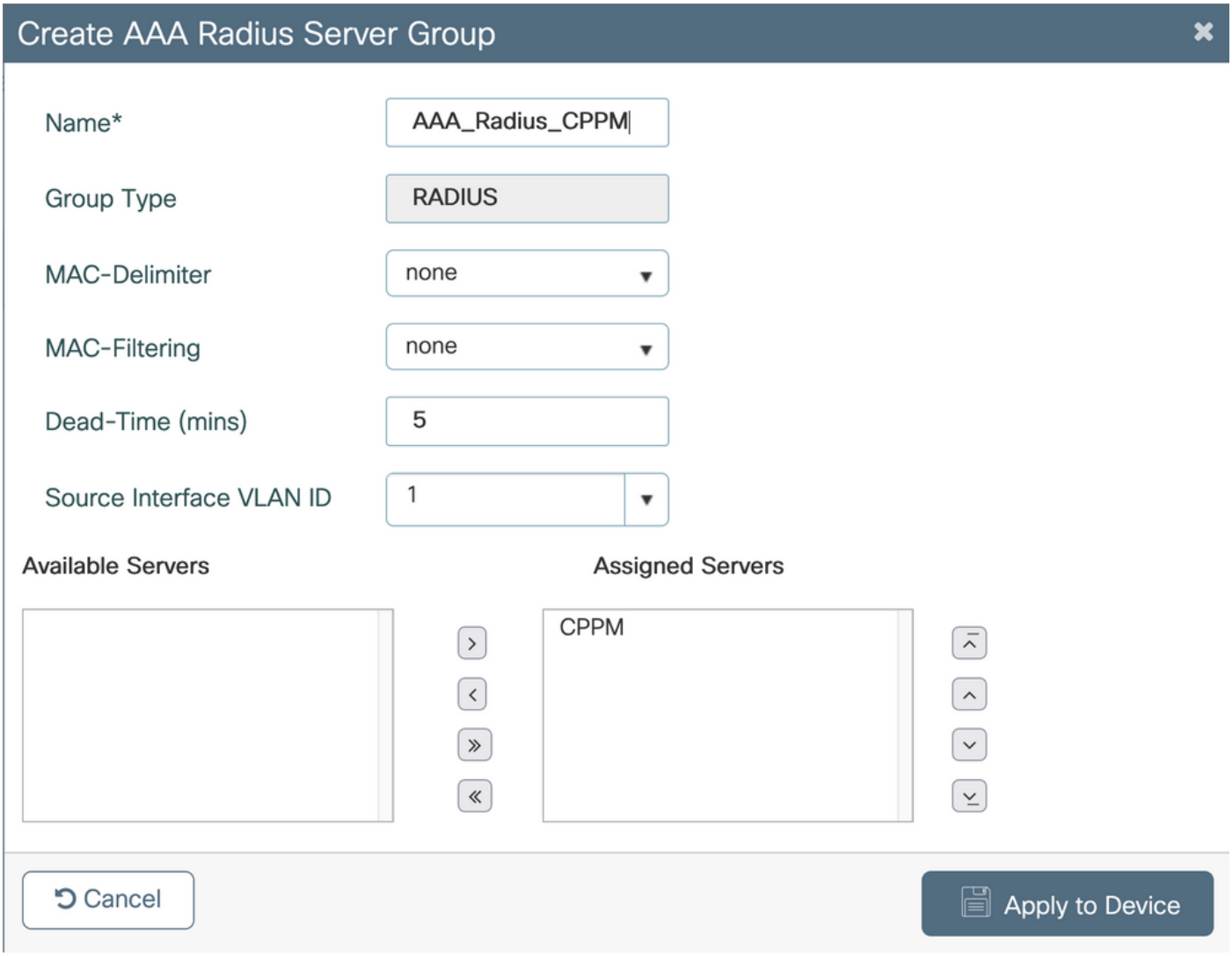
C9800 — 访客的AAA配置

> **注意**：关于Cisco Bug ID CSCvh03827，请确保定义的身份验证、授权和记帐(AAA)服务器未进行负载均衡，因为机制依赖WLC中的SessionID持续性进行ClearPass RADIUS交换。

步骤1.将Aruba ClearPass DMZ服务器添加到9800 WLC配置并创建身份验证方法列表。导航到 **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > +Add**并输入RADIUS服务器信息。

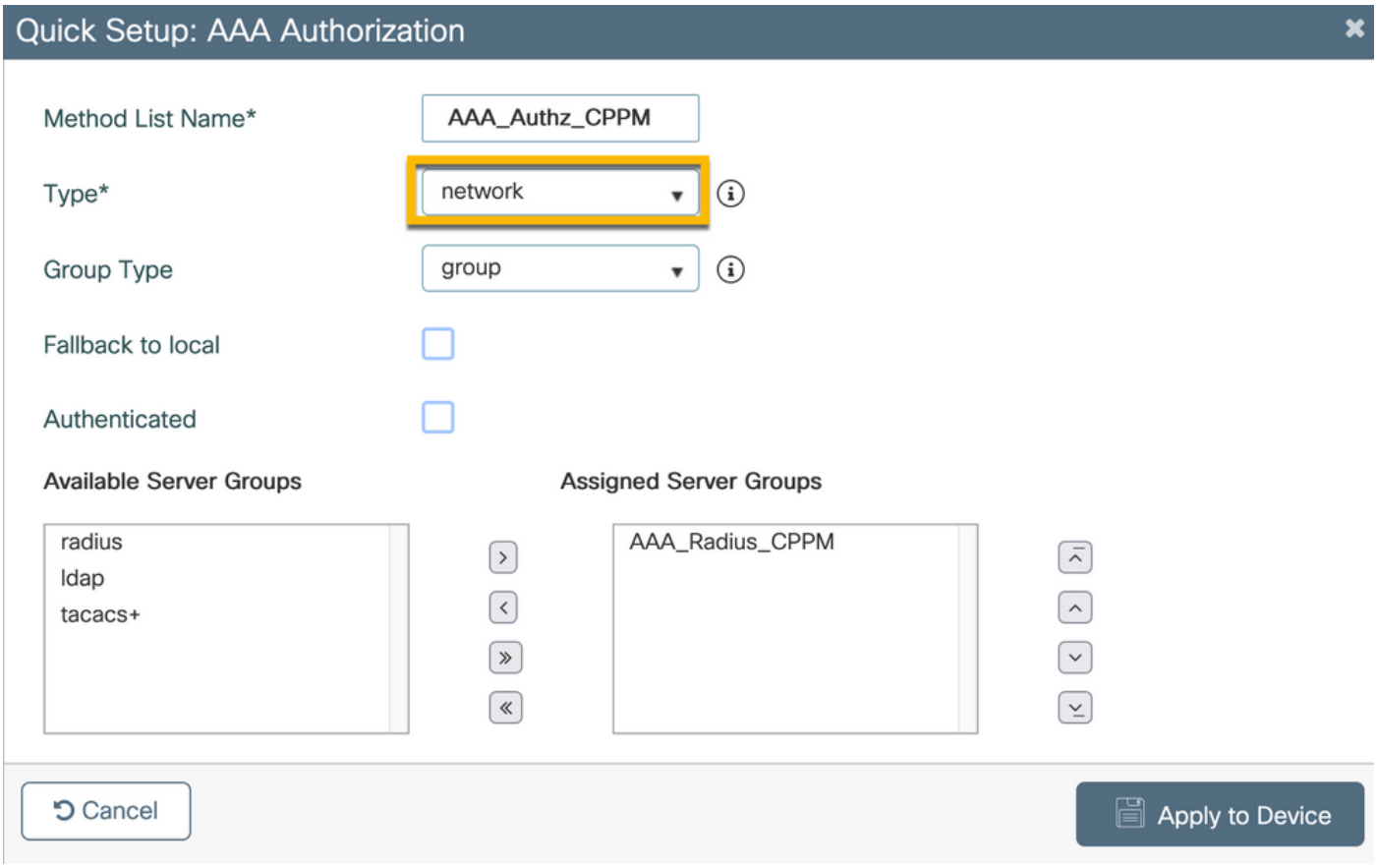


步骤2.定义访客的AAA服务器组，并将步骤1中配置的服务器分配给此服务器组。导航到**Configuration > Security > AAA > Servers/Groups > RADIUS > Groups > +Add。**

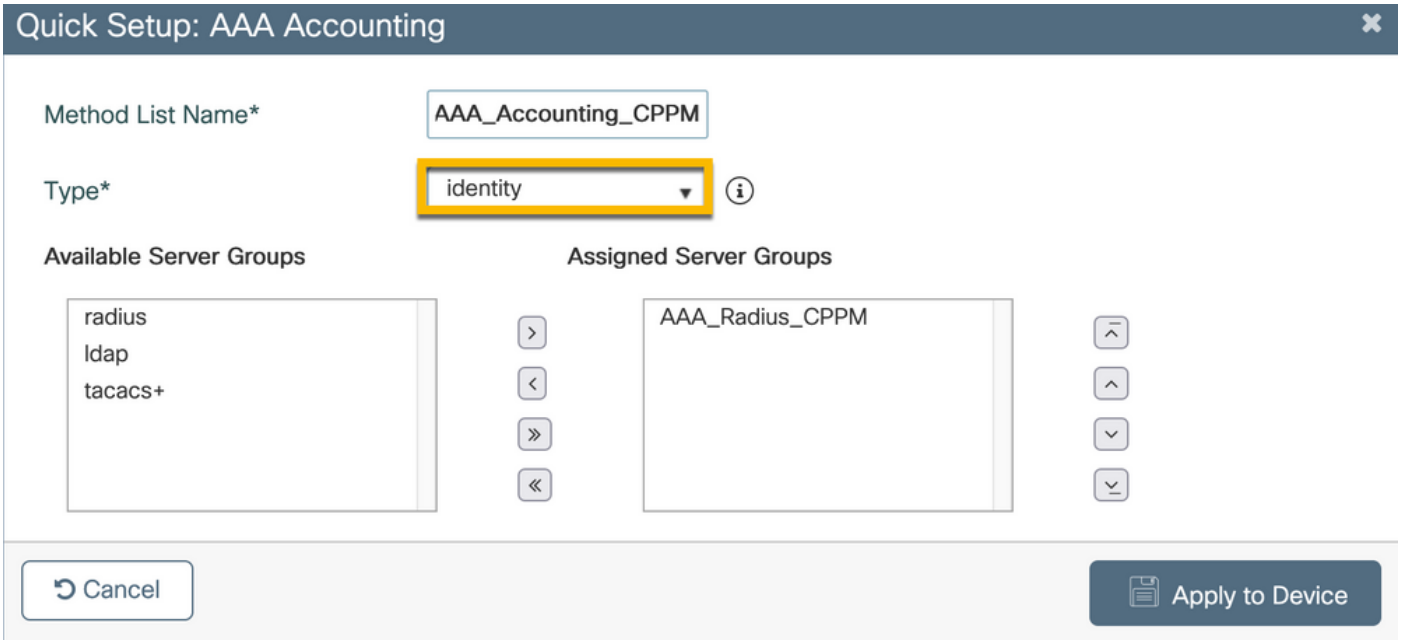


步骤3.定义访客访问的授权方法列表并映射在步骤2中创建的服务器组。导航到**配置>安全> AAA >**

AAA方法列表>授权> +添加。选择**Type Network**，然后选择**步骤2中配置的AAA Server Group。**



第4步：为访客访问创建记账方法列表并映射在步骤2中创建的服务器组。导航到**配置>安全> AAA > AAA方法列表>记账> +添加。**从下拉菜单中选择**Type Identity**，然后选择**步骤2中配置的AAA Server Group。**



C9800 — 配置重定向ACL

重定向ACL定义必须重定向到访客门户的流量与允许无重定向通过的流量。在这里，ACL拒绝意味着绕过重定向或通过，而允许意味着重定向到门户。对于每个流量类，在创建访问控制条目

(ACE)并创建与入口和出口流量均匹配的ACE时，您需要考虑流量的方向。

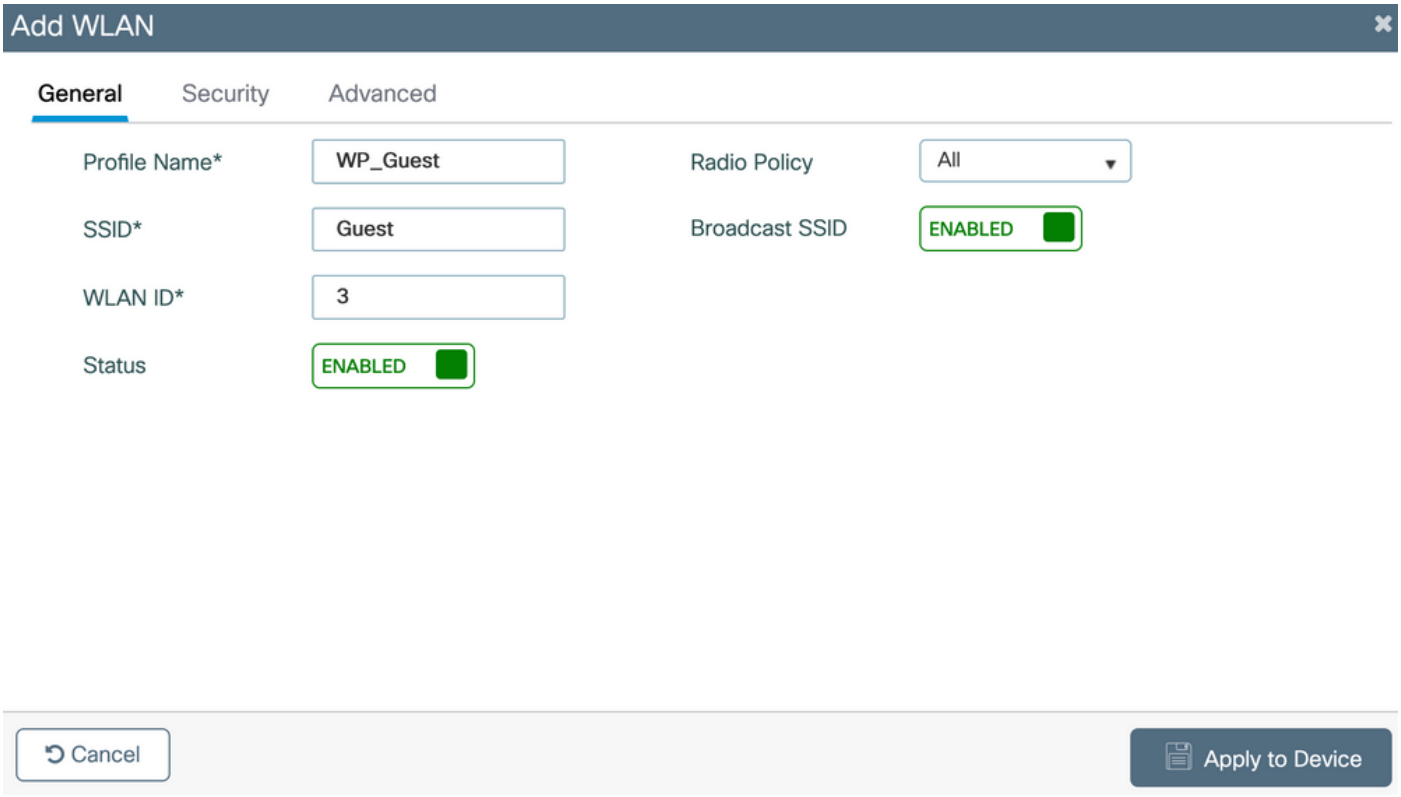
导航到**Configuration > Security > ACL**，然后定义名为**CAPTIVE_PORTAL_REDIRECT**的新ACL。使用以下ACE配置ACL:

- ACE1:允许双向互联网控制消息协议(ICMP)流量绕过重定向，主要用于验证可达性。
- ACE10、ACE30:允许双向的DNS流量流向DNS服务器10.0.10.4，并且不会重定向到门户。触发访客流需要DNS查找和响应拦截。
- ACE70、ACE80、ACE110、ACE120:允许用户通过门户对访客强制网络门户进行HTTP和HTTPS访问。
- ACE150:所有HTTP流量（UDP端口80）都会被重定向。

Sequence ▲	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port
1	deny	any		any		icmp		
10	deny	any		10.0.10.4		udp		eq domain
30	deny	10.0.10.4		any		udp	eq domain	
70	deny	any		10.85.54.98		tcp		eq 443
80	deny	10.85.54.98		any		tcp	eq 443	
110	deny	any		10.85.54.98		tcp		eq www
120	deny	10.85.54.98		any		tcp	eq www	
150	permit	any		any		tcp		eq www

C9800 — 访客WLAN配置文件配置

步骤1.导航到**配置>标记和配置文件>无线> +添加**。创建新的SSID配置文件WP_Guest，并广播访客客户端与之关联的SSID 'Guest'。

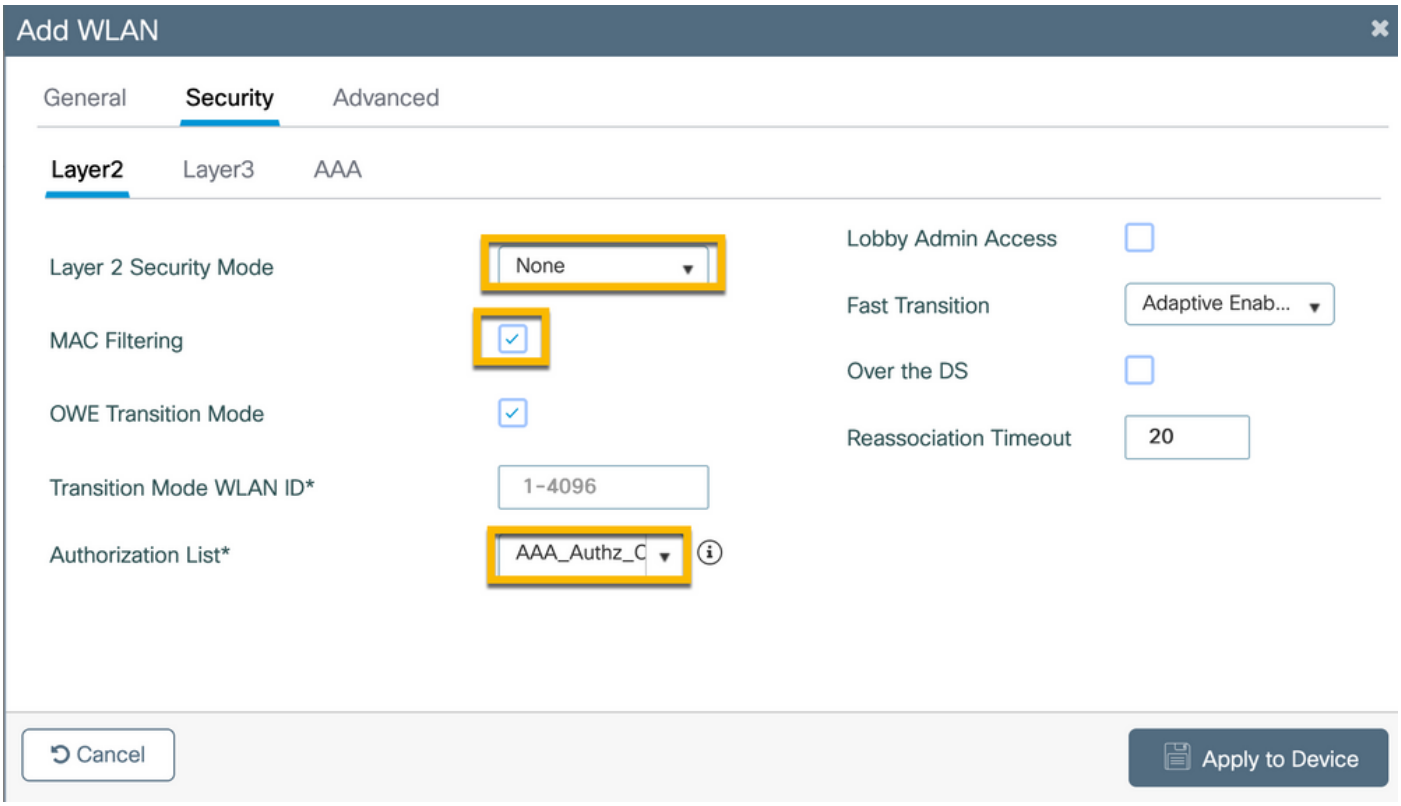


在同一**Add WLAN**对话框下，导航到**Security > Layer 2**选项卡。

— 第2层安全模式：无

-MAC 过滤:启用

— 授权列表：AAA_Authz_CPPPM（在步骤3下配置，作为AAA配置的一部分）



C9800 — 访客策略配置文件定义

在C9800 WLC GUI上，导航到**配置>标记和配置文件>策略> +添加**。

名称：PP_Guest

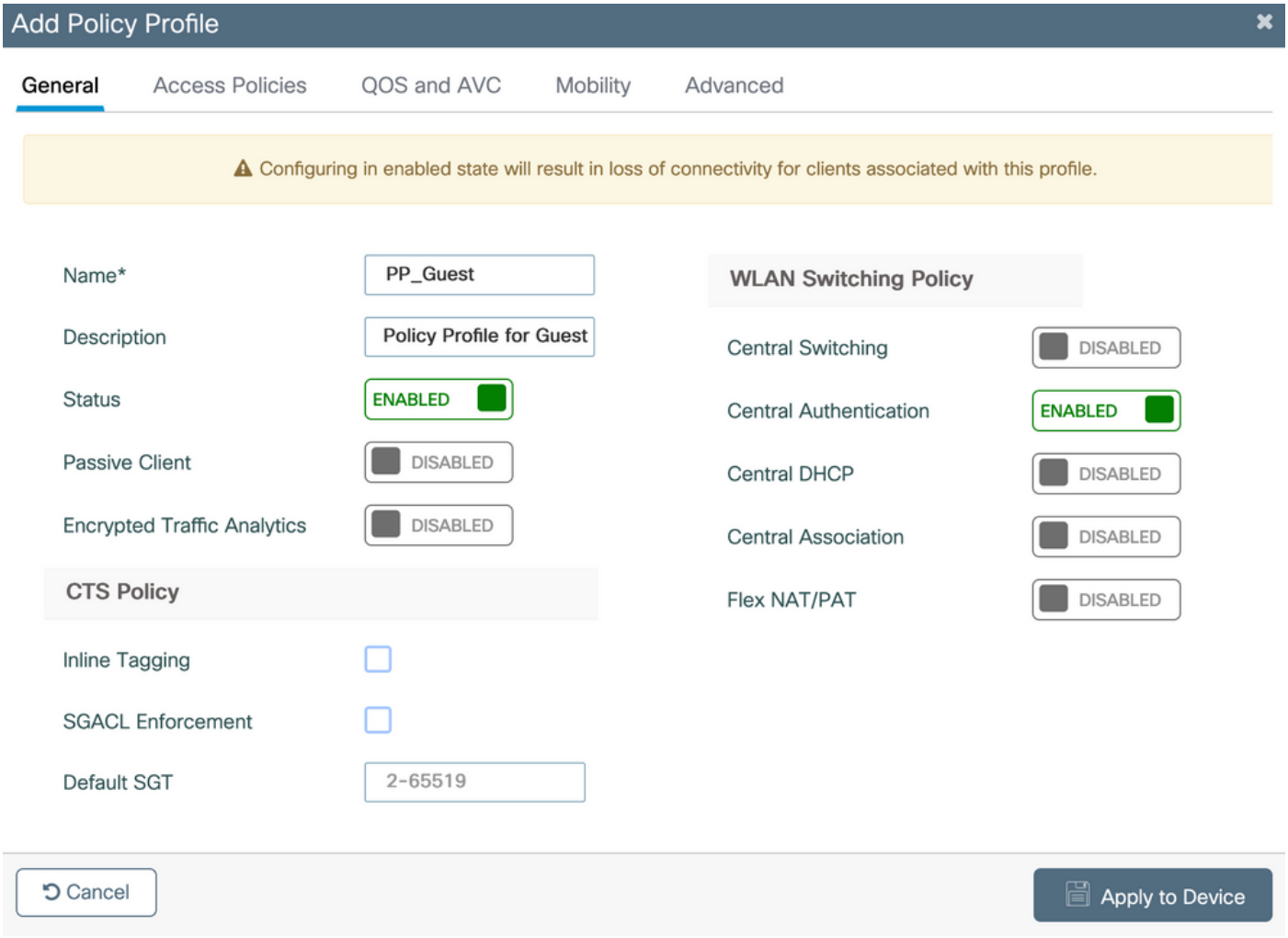
状态:启用

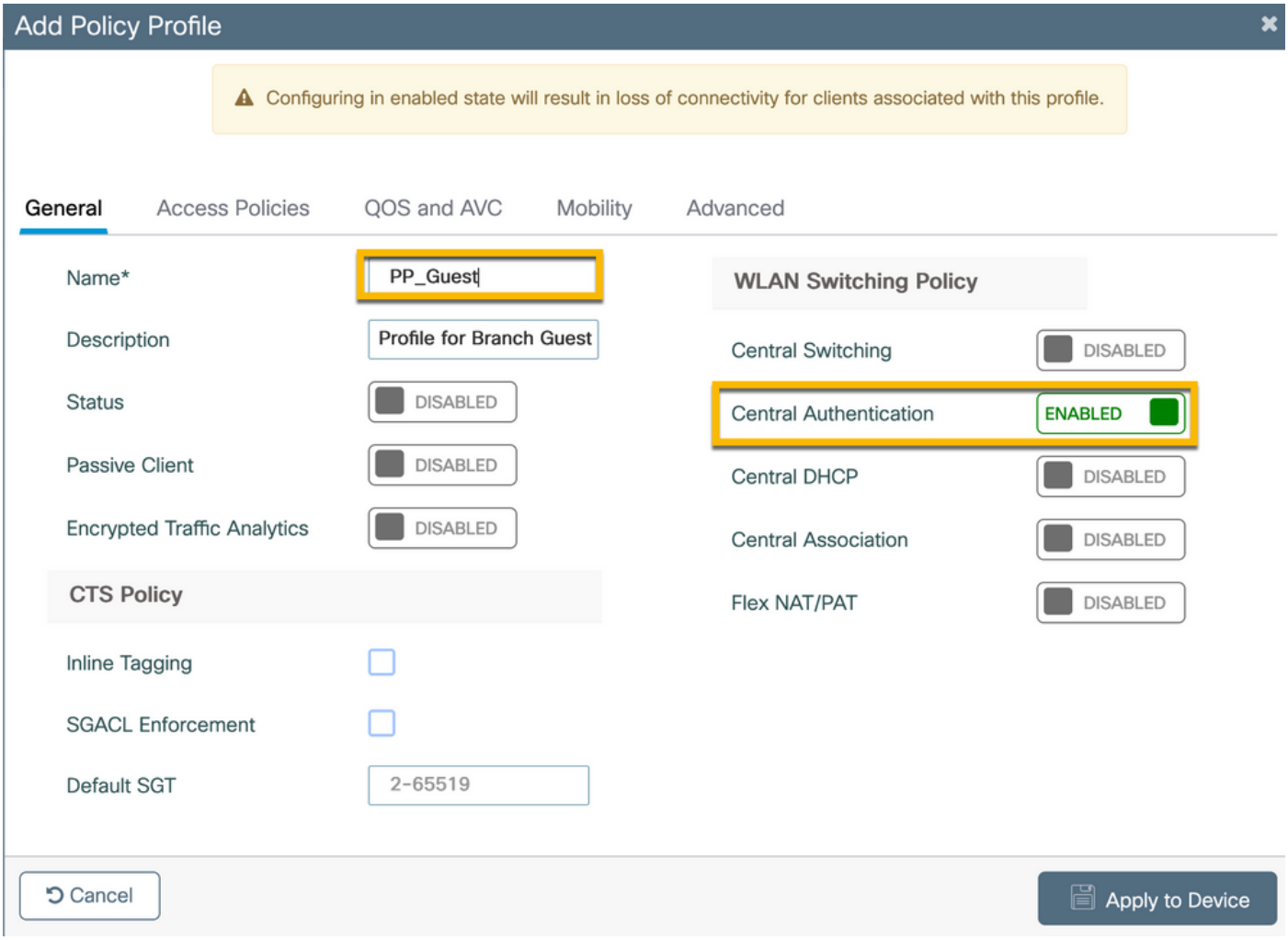
集中交换：禁用

集中身份验证：启用

中央DHCP:禁用

中央协会：禁用


Add Policy Profile
General
Access Policies
QOS and AVC
Mobility
Advanced
Configuring in enabled state will result in loss of connectivity for clients associated with this profile.
Name*
PP_Guest
Description
Policy Profile for Guest
Status
ENABLED
Passive Client
DISABLED
Encrypted Traffic Analytics
DISABLED
CTS Policy
Inline Tagging
SGACL Enforcement
Default SGT
2-65519
WLAN Switching Policy
Central Switching
DISABLED
Central Authentication
ENABLED
Central DHCP
DISABLED
Central Association
DISABLED
Flex NAT/PAT
DISABLED
Cancel
Apply to Device



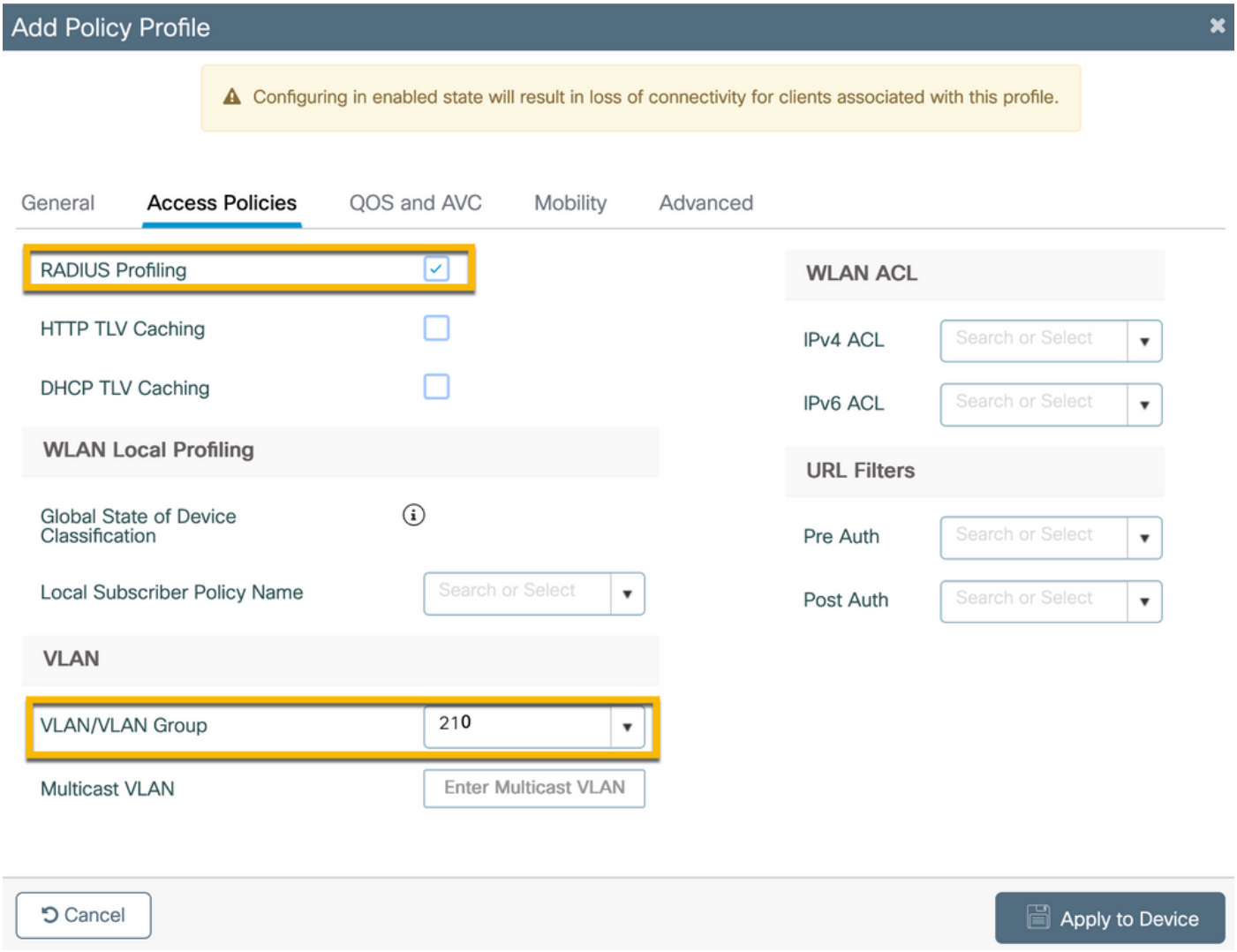
导航到同一**Add Policy Profile**对话框中的**Access Policies**选项卡。

- RADIUS分析：启用

- VLAN/VLAN组：210（即，VLAN 210是每个分支机构位置的访客本地VLAN）

> **注意**：在9800 WLC上的VLAN下，必须在VLAN/VLAN组类型VLAN编号中定义Flex的访客VLAN。

已知缺陷：如果在WLC下和Flex配置文件中定义了相同的Flex访客VLAN，则Cisco bug ID CSCvn48234会导致不广播SSID。



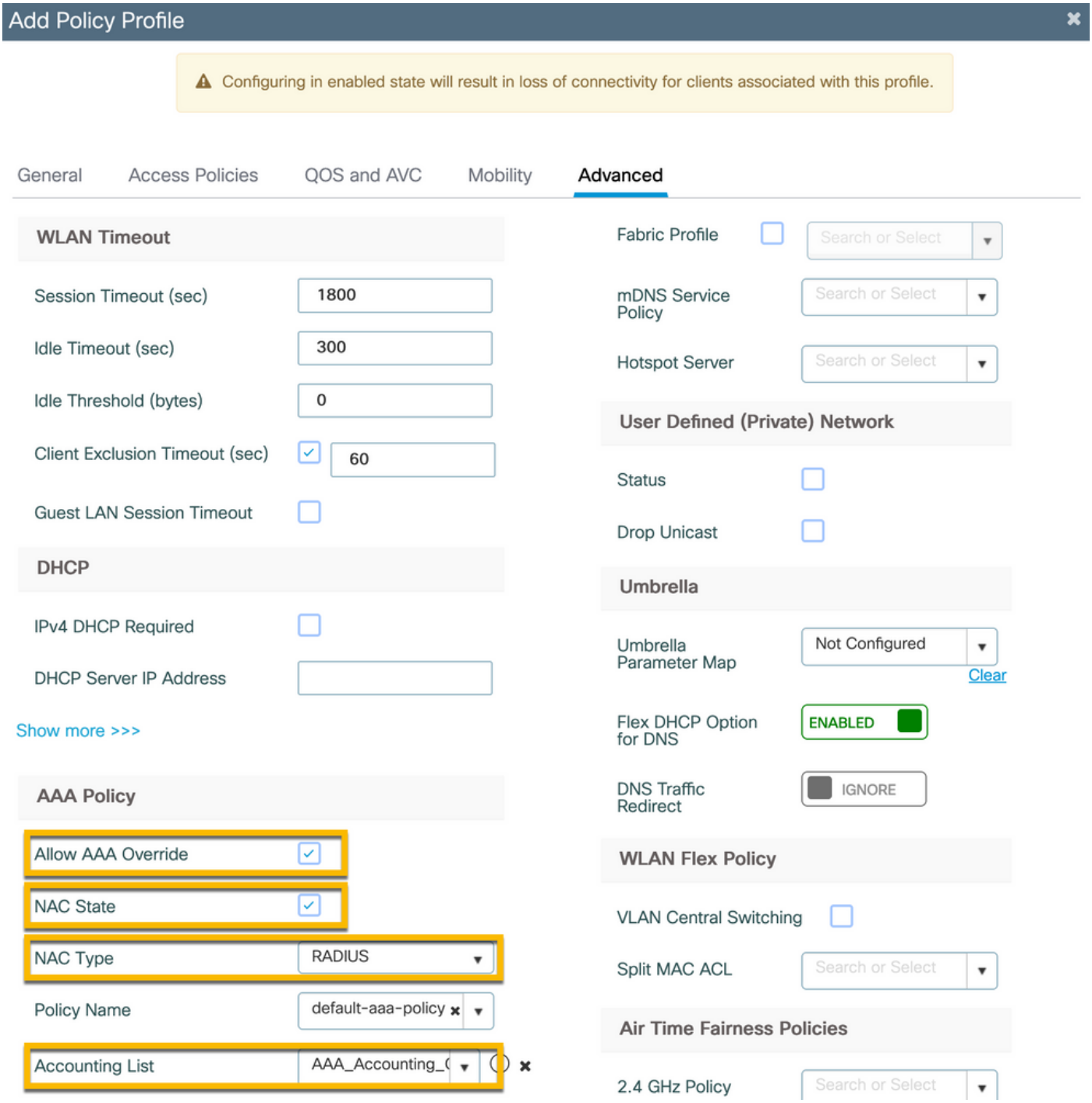
在同一**Add Policy Profile对话**框中，导航到**Advanced**选项卡。

— 允许AAA覆盖：启用

- NAC状态：启用

- NAC类型：RADIUS

— 记帐列表：AAA_Accounting_CPPPM（在步骤4中定义。作为AAA配置的一部分）



注意：要启用C9800 WLC以接受RADIUS CoA消息，需要"网络准入控制(NAC)状态 — 启用"。

C9800 — 策略标记

在C9800 GUI上，导航到**配置>标记和配置文件>标记>策略> +添加。**

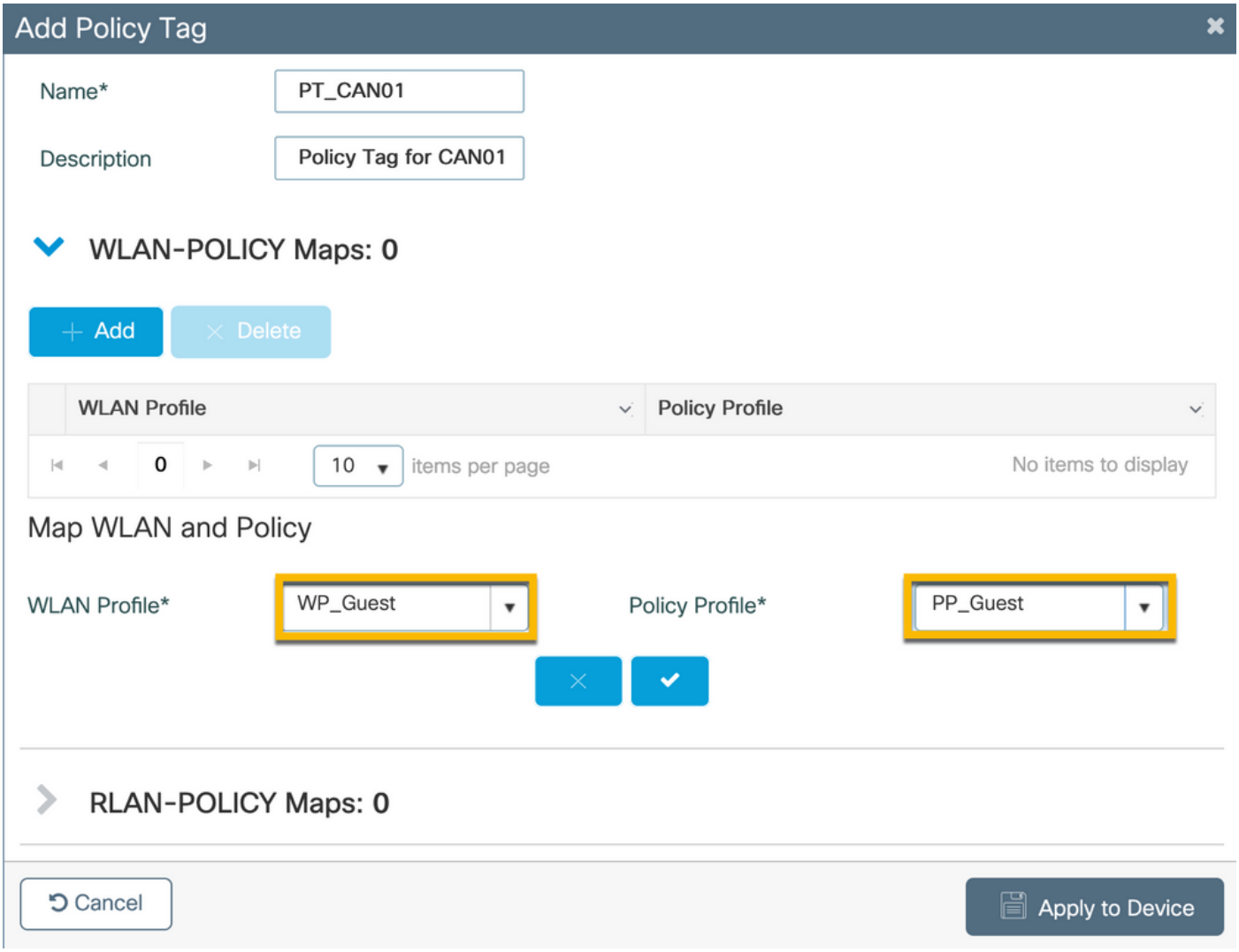
-姓名 :PT_CAN01

-描述:CAN01分支站点的策略标签

在同一个对话框**Add Policy Tag**中，在**WLAN-POLICY MAPS**下，单击**+Add**，并将之前创建的WLAN配置文件映射到策略配置文件：

- WLAN配置文件：WP_Guest

— 策略配置文件：PP_Guest

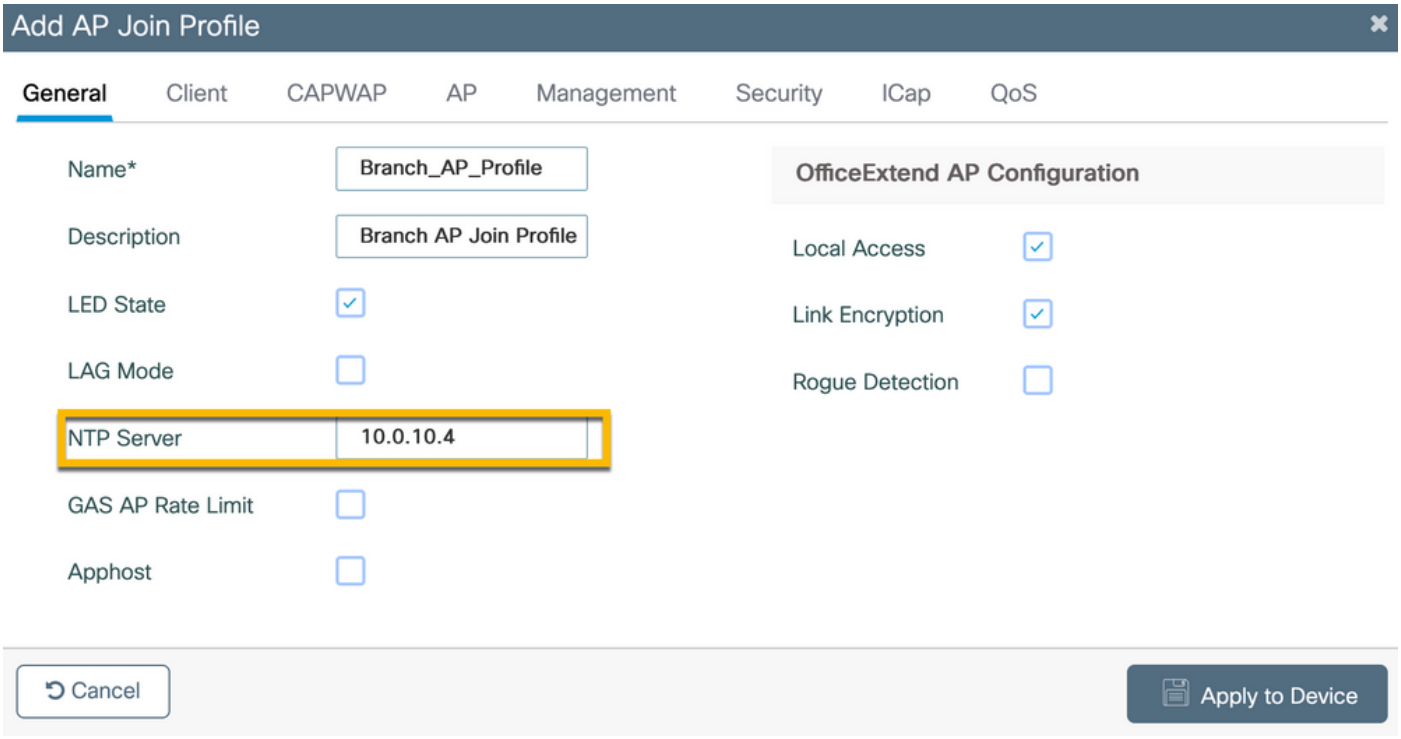


C9800 - AP加入配置文件

在C9800 WLC GUI上，导航到**配置>标记和配置文件> AP加入> +添加。**

-姓名 :Branch_AP_Profile

-NTP 服务器:10.0.10.4（请参阅实验拓扑图）。 这是Branch中的AP用于同步的NTP服务器。



C9800 - Flex配置文件

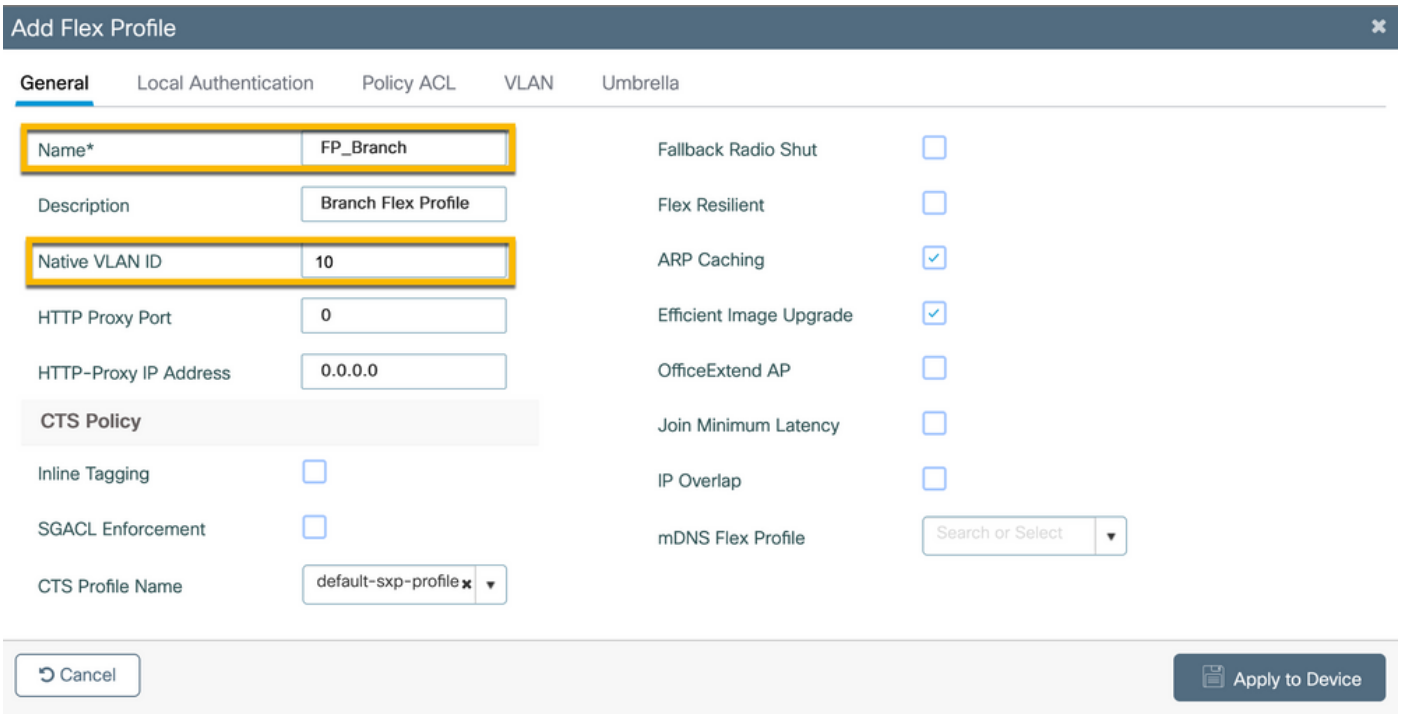
配置文件和标签是模块化的，可以重复用于多个站点。

对于FlexConnect部署，如果所有分支机构站点使用相同的VLAN ID，您可以重复使用相同的Flex配置文件。

步骤1.在C9800 WLC GUI上，导航到**配置>标记和配置文件> Flex > +Add**。

-姓名 :FP_Branch

— 本征VLAN ID:10（仅在您有一个非默认本地VLAN且要有AP管理接口时需要）

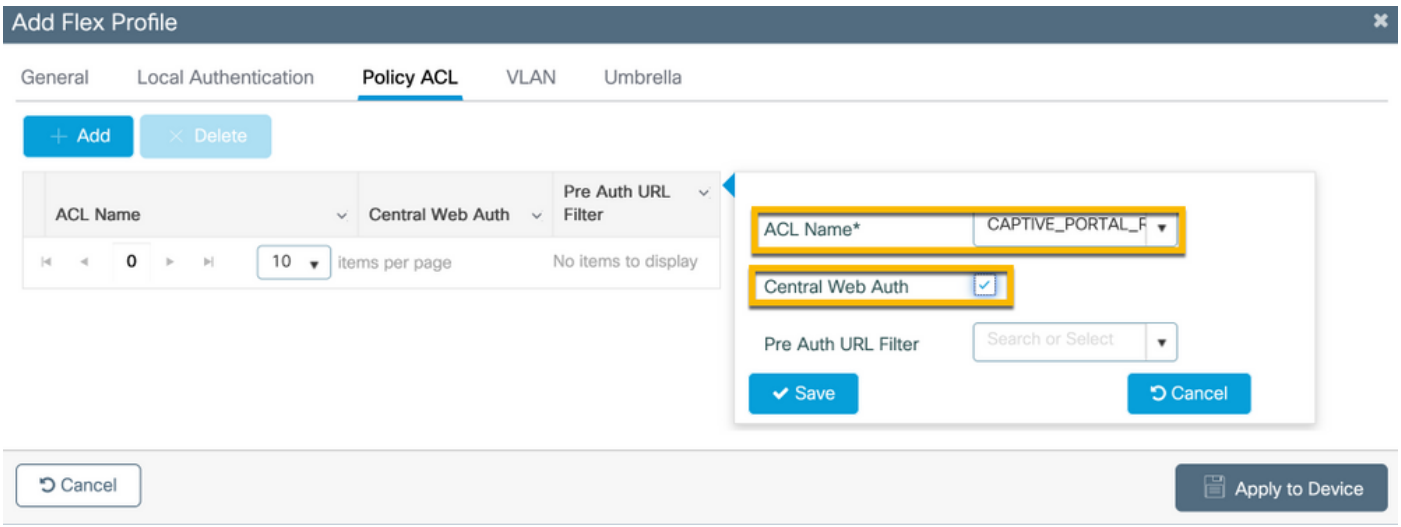


在同一添加**Flex Profile**对话框中，导航到**策略ACL**选项卡，然后单击**+添加**。

-ACL 名称:CAPTIVE_PORTAL_REDIRECT

— 集中Web身份验证：启用

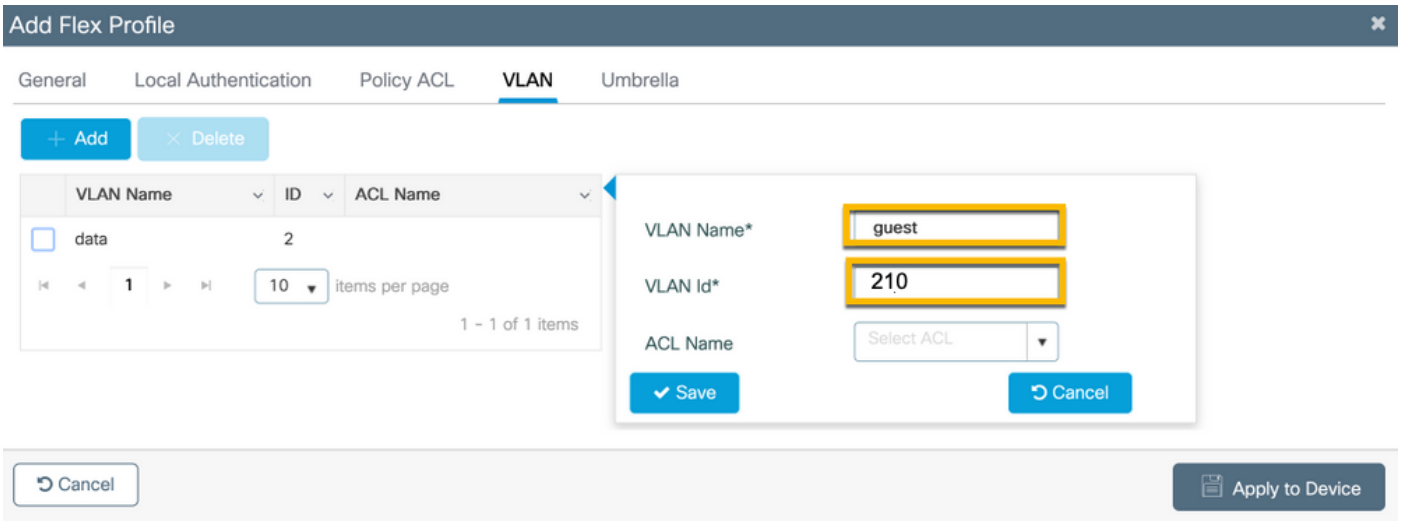
在Flexconnect部署中，当重定向发生在AP而不是C9800上时，预期每个托管AP都将在本地下载重定向ACL。



在**Add Flex Profile**对话框中，导航到**VLAN**选项卡，然后单击**+Add**（请参见实验拓扑图）。

-VLAN 名称:访客

-VLAN ID:210



C9800 — 站点标记

在9800 WLC GUI上，导航到**配置>标签和配置文件>标签>站点>添加**。

注意：为每个需要支持两个无线SSID的远程站点创建唯一的站点标记（如所述）。

地理位置、站点标签和Flex Profile配置之间有1-1映射。

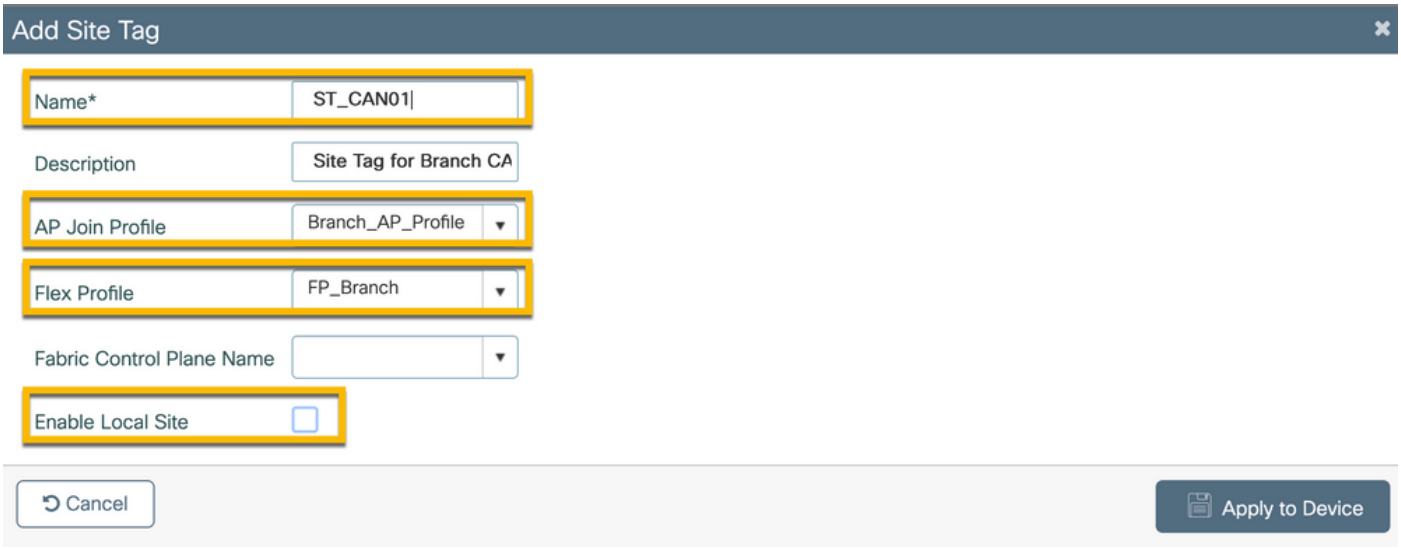
FlexConnect站点必须具有与其关联的FlexConnect配置文件。每个flex connect站点最多可以有100个接入点。

-姓名 :ST_CAN01

- AP加入配置文件：Branch_AP_Profile

- Flex配置文件：FP_Branch

— 启用本地站点：禁用



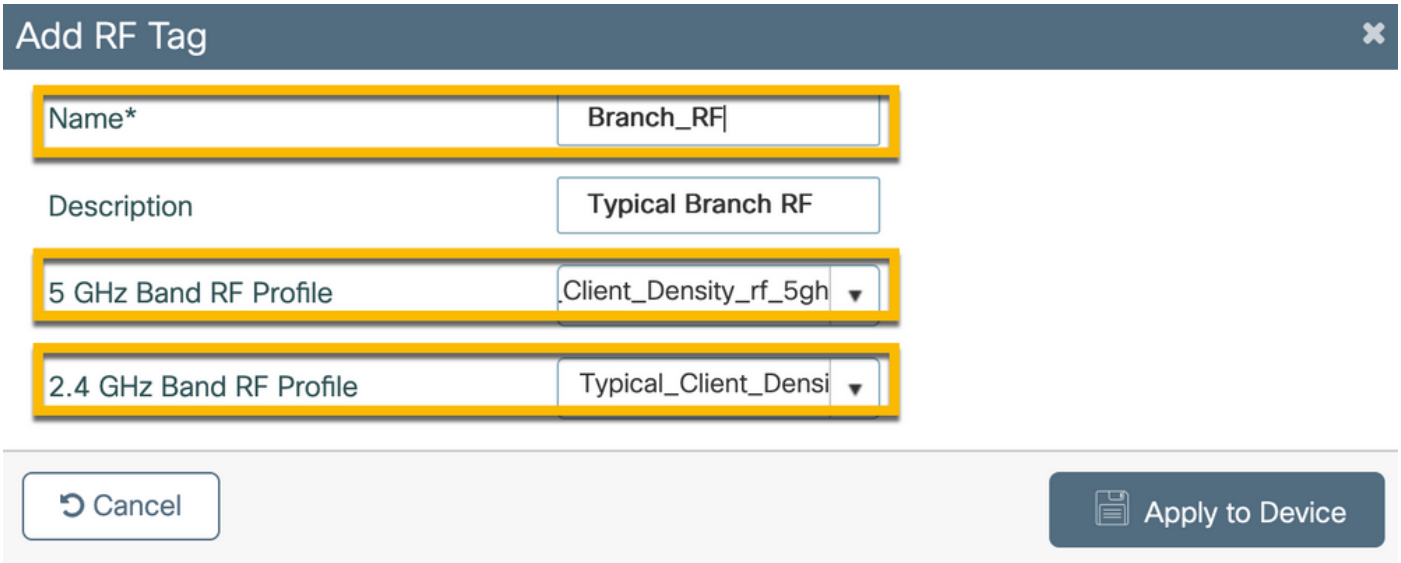
C9800 - RF配置文件

在9800 WLC GUI上，导航到**Configuration > Tags & Profiles > Tags > RF > Add**。

-姓名 :Branch_RF

- 5 GHz频段射频(RF)配置文件：Typical_Client_Density_5gh（系统定义的选项）

- 2.4 GHz频段RF配置文件：Typical_Client_Density_2gh（系统定义的选项）



C9800 — 为AP分配标记

有两个选项可用于将定义的标记分配到部署中的单个AP:

— 基于AP名称的分配，利用regex规则匹配AP名称字段中的模式(**Configure > Tags & Profiles > Tags > AP > Filter**)

— 基于AP以太网MAC地址的分配(**配置>标记和配置文件>标记> AP >静态**)

在使用DNA Center的生产部署中，强烈建议使用DNAC和AP PNP工作流程，或使用9800中提供的静态批量逗号分隔值(CSV)上传方法，以避免手动分配每个AP。导航到**Configure > Tags & Profiles > Tags > AP > Static > Add**(注意**Upload File**选项)。

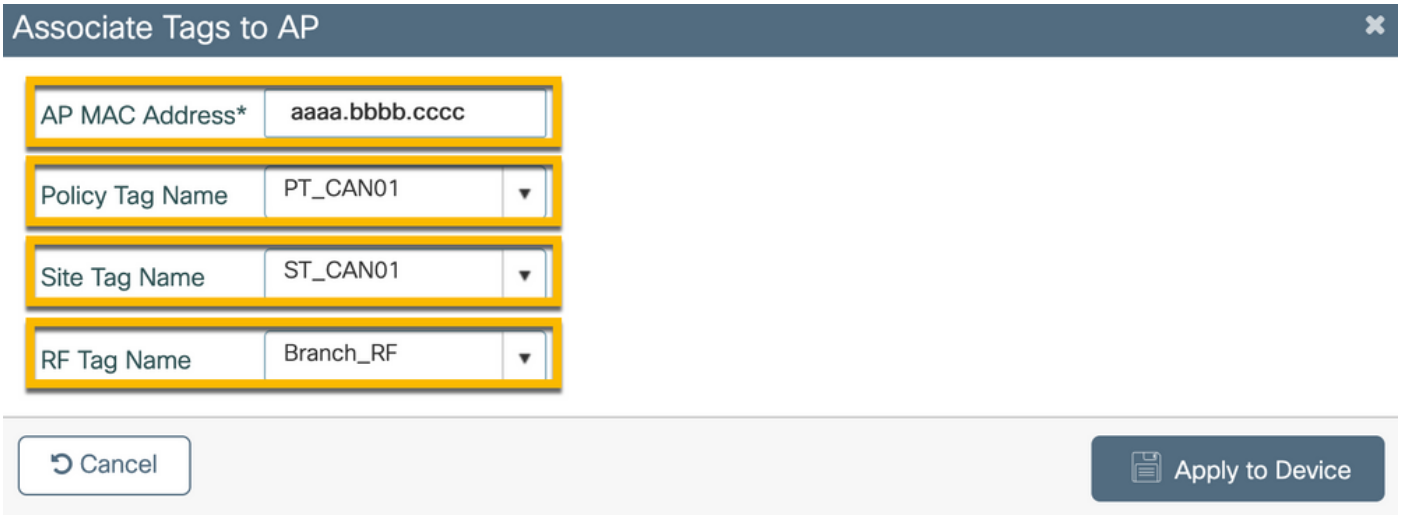
- AP MAC地址：<AP_ETHERNET_MAC>

— 策略标记名称：PT_CAN01

— 站点标记名称：ST_CAN01

- RF标记名称：Branch_RF

> **注意**：从Cisco IOS®-XE 17.3.4c开始，每个控制器最多有1,000个正则表达式规则限制。如果部署中的站点数量超过此数量，则必须使用静态的每MAC分配。



> **注意**：或者，要利用基于AP名称正则表达式的标签分配方法，请导航到**配置>标签和配置文件>标签> AP >过滤器>添加**。

-姓名 :BR_CAN01

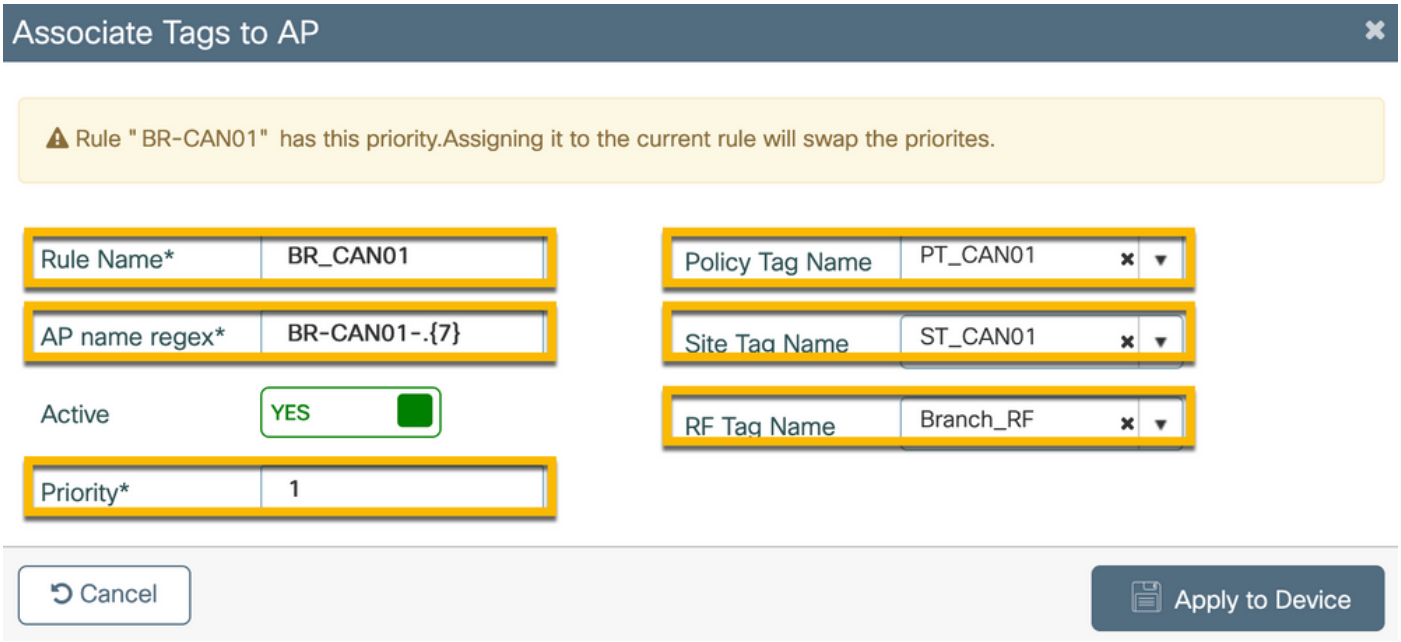
- AP名称正则表达式：BR-CAN01-.(7)(此规则与组织中采用的AP名称约定匹配。在本示例中，标签被分配给具有“AP名称”字段的AP，该字段包含“BR_CAN01 — ”，后跟任意七个字符。)

-优先级：1

— 策略标记名称：PT_CAN01（如定义）

— 站点标记名称：ST_CAN01

- RF标记名称：Branch_RF



配置Aruba CPPM实例

有关基于生产/最佳实践的Aruba CPPM配置，请联系您当地的HPE Aruba SE资源。

Aruba ClearPass服务器初始配置

Aruba ClearPass使用开放式虚拟化格式(OVF)模板部署在ESXi <>服务器上，该服务器分配以下资源：

- 两个保留的虚拟CPU
- 6 GB RAM
- 80 GB磁盘（必须在初始虚拟机部署后手动添加，然后才能启动计算机）

申请许可证

通过以下方式应用平台许可证：**管理(Administration)>服务器管理器(Server Manager)>许可(Licensing)**。添加**平台**、**访问**和板载**许可证**。

服务器主机名

导航到**管理>服务器管理器>服务器配置**，然后选择新调配的CPPM服务器。

-主机名:cppm

- FQDN:cppm.example.com

— 验证管理端口IP编址和DNS

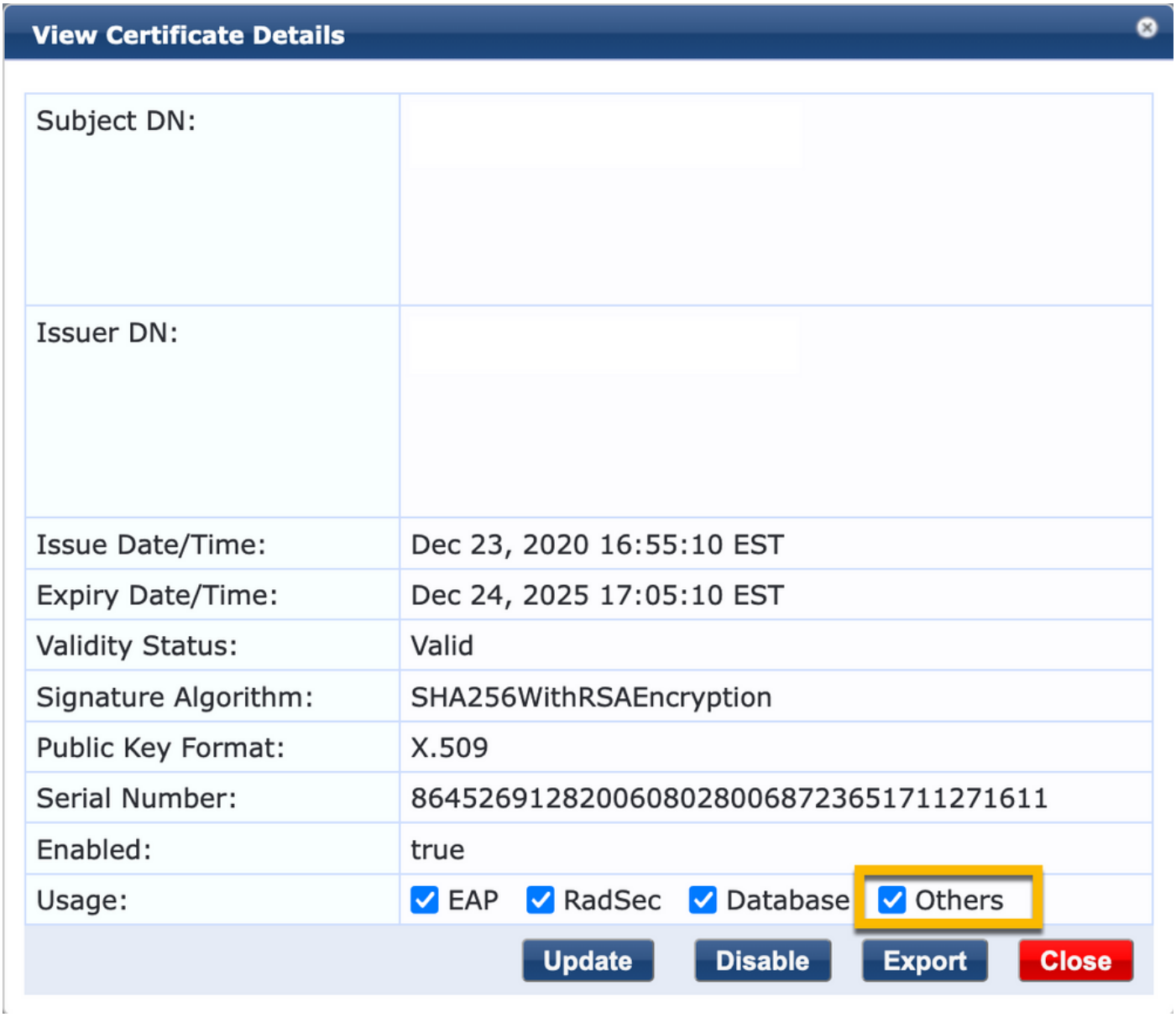
生成CPPPM Web服务器证书(HTTPS)

当ClearPass Guest Portal页面通过HTTPS呈现给连接到分支中的访客Wifi的访客客户端时，使用此证书。

步骤1.上传CA发布链证书。

导航到**管理>证书>信任列表>添加**。

-使用率:启用其他



步骤2.创建证书签名请求。

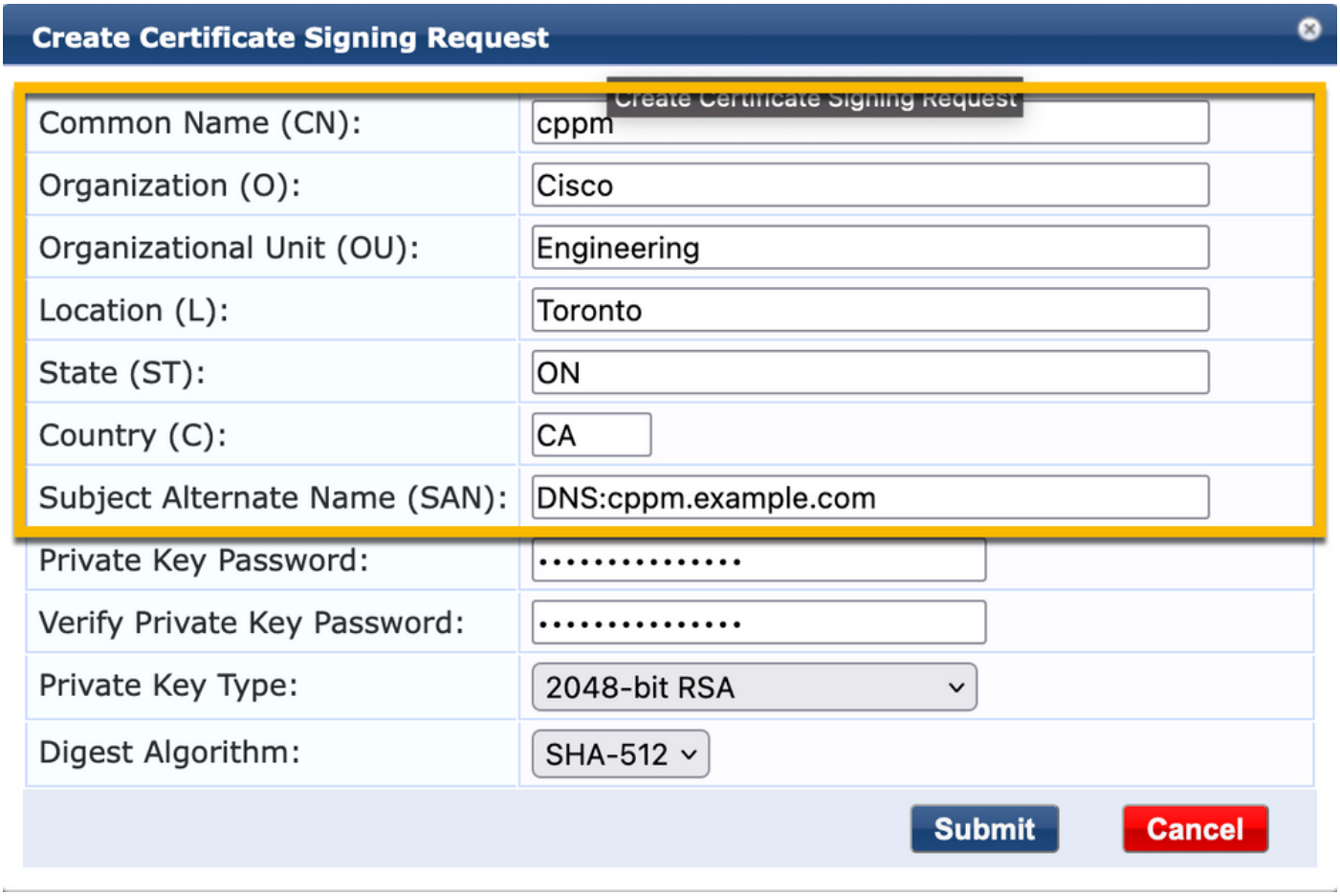
导航到**管理>证书>证书存储>服务器证书>用法：HTTPS服务器证书。**

— 单击**Create Certificate Signing Request**

— 公用名：CPPM

— 组织：**cppm.example.com**

确保填充SAN字段（SAN中必须存在通用名称，IP和其他FQDN必须根据需要存在）。 格式为DNS:**<fqdn1>、DNS:<fqdn2>、IP<ip1>。**



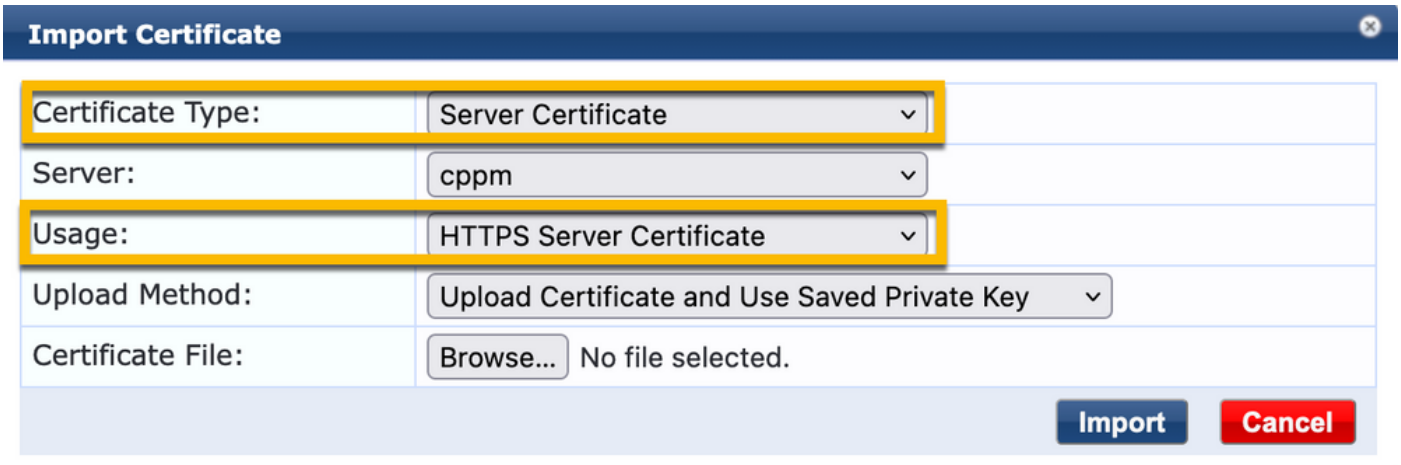
第3步：在所选的CA中，签署新生成的CPPM HTTPS服务CSR。

步骤4.导航到**证书模板> Web服务器>导入证书。**

— 证书类型：服务器证书

-使用率:HTTP服务器证书

-证书文件:浏览并选择CA签名的CPPM HTTPS服务证书



将C9800 WLC定义为网络设备

导航到**Configuration > Network > Devices > Add。**

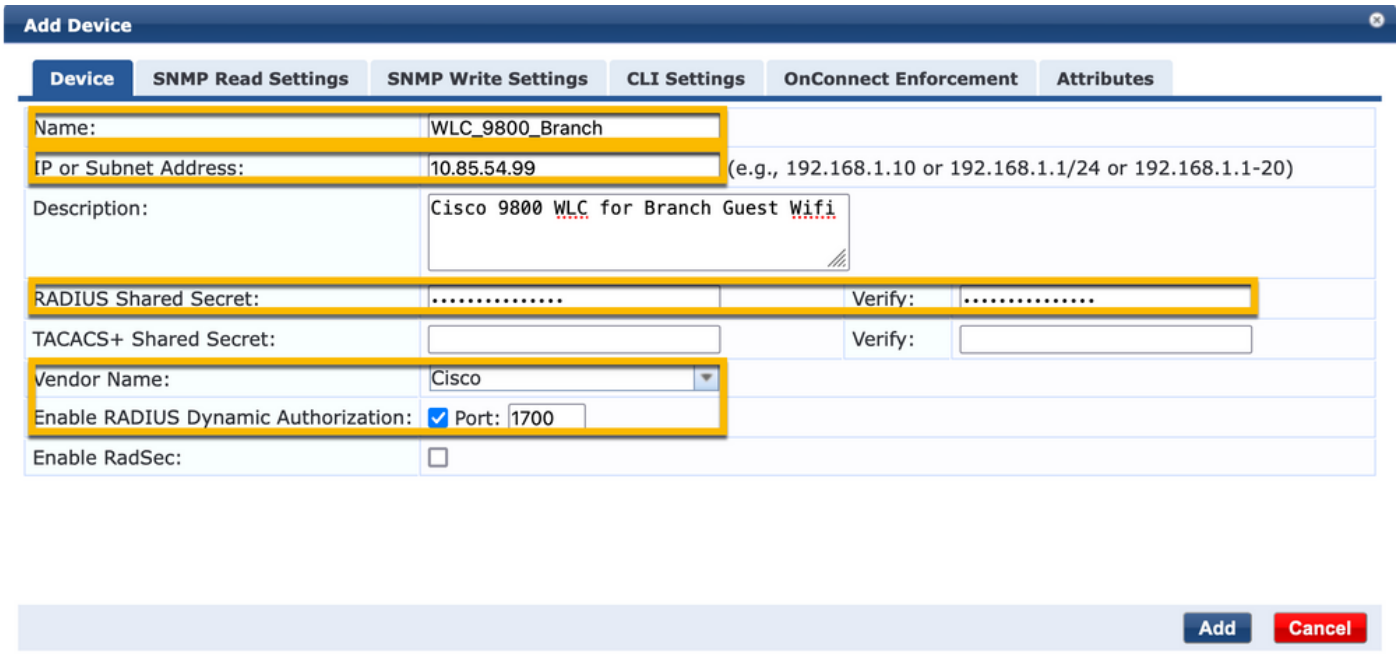
-姓名 :WLC_9800_Branch

- IP或子网地址：10.85.54.99（请参阅实验拓扑图）

- RADIUS共享思科：<WLC RADIUS密码>

-供应商名称: 思科

— 启用RADIUS动态授权：1700

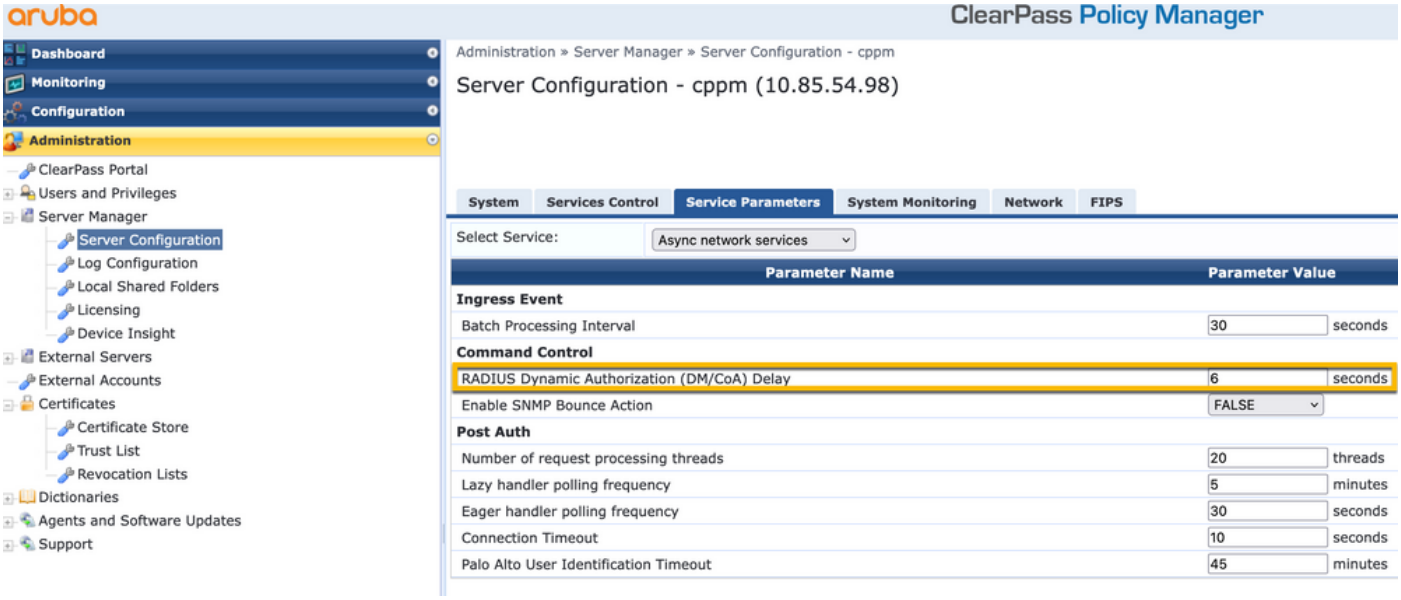


访客门户页面和CoA计时器

在整个配置中设置正确的计时器值非常重要。如果未调整计时器，您可能会遇到客户端未处于“运行状态”的循环Web门户重定向。
要注意的计时器：

- 门户Web登录计时器：此计时器将延迟重定向页面，然后才允许访问访客门户页面通知CPPPM服务状态转换、注册终端自定义属性“Allow-Guest-Internet”值，并触发从CPPPM到WLC的CoA进程。导航到**Guest > Configuration > Pages > Web Logins**。
  — 选择访客门户名称：实验室匿名访客注册（此访客门户页面配置如图所示）
  — 单击**Edit**
  — 登录延迟：6 秒

- ClearPass CoA延迟计时器：这会延迟CoA消息从ClearPass发送到WLC。在CoA确认(ACK)从WLC返回之前，CPPM在内部成功转换客户端终端状态时需要此步骤。实验室测试显示来自WLC的亚毫秒响应时间，如果CPPM尚未完成终端属性的更新，则来自WLC的新RADIUS会话将与未经身份验证的MAB服务实施策略相匹配，并且客户端将再次获得重定向页面。导航到**CPPM > Administration > Server Manager > Server Configuration**，然后选择**CPPM Server > Service Parameters**。
  - RADIUS动态授权(DM/CoA)延迟 — 设置为6秒



ClearPass — 访客CWA配置

ClearPass-side CWA配置包括(3)服务点/阶段：

ClearPass组件	服务类型	目的
1.策略管理器	服务：MAC 验证	如果自定义属性**Allow-Guest-In** = TRUE，则允许它进入网络。 ，触发**Redirect**和**COA:重新验证**
2.访客	Web登录	显示匿名登录AUP页面。 Post-auth set custom attribute **Allow-Guest-Internet** = TRUE。
3.策略管理器	服务：基于Web的身份验证	将终端更新为**已知** 设置自定义**属性Allow-Guest-In** = TRUE **COA:重新验证**

ClearPass端点元数据属性：允许 — 访客 — 互联网

创建类型为Boolean的元数据属性，以在客户端在“Webauth Pending”和“Run”状态之间转换时跟踪访客终端状态：

— 连接到wifi的新访客将默认元数据属性设置为Allow-Guest-Internet=false。基于此属性，客户端身份验证通过MAB服务

— 当您点击AUP Accept按钮时，访客客户端的元数据属性更新为Allow-Guest-Internet=true。随后基于此属性设置为True的MAB允许对互联网进行非重定向访问

导航到ClearPass > Configuration > Endpoints，从列表中选择任何终端，点击**Attributes**选项卡，使用值**false**添加**Allow-Guest-Internet**并**Save**。

> **注意**：您也可以编辑同一端点，并在之后删除此属性 — 此步骤仅创建可在策略中使用的端点元数据数据库中的字段。

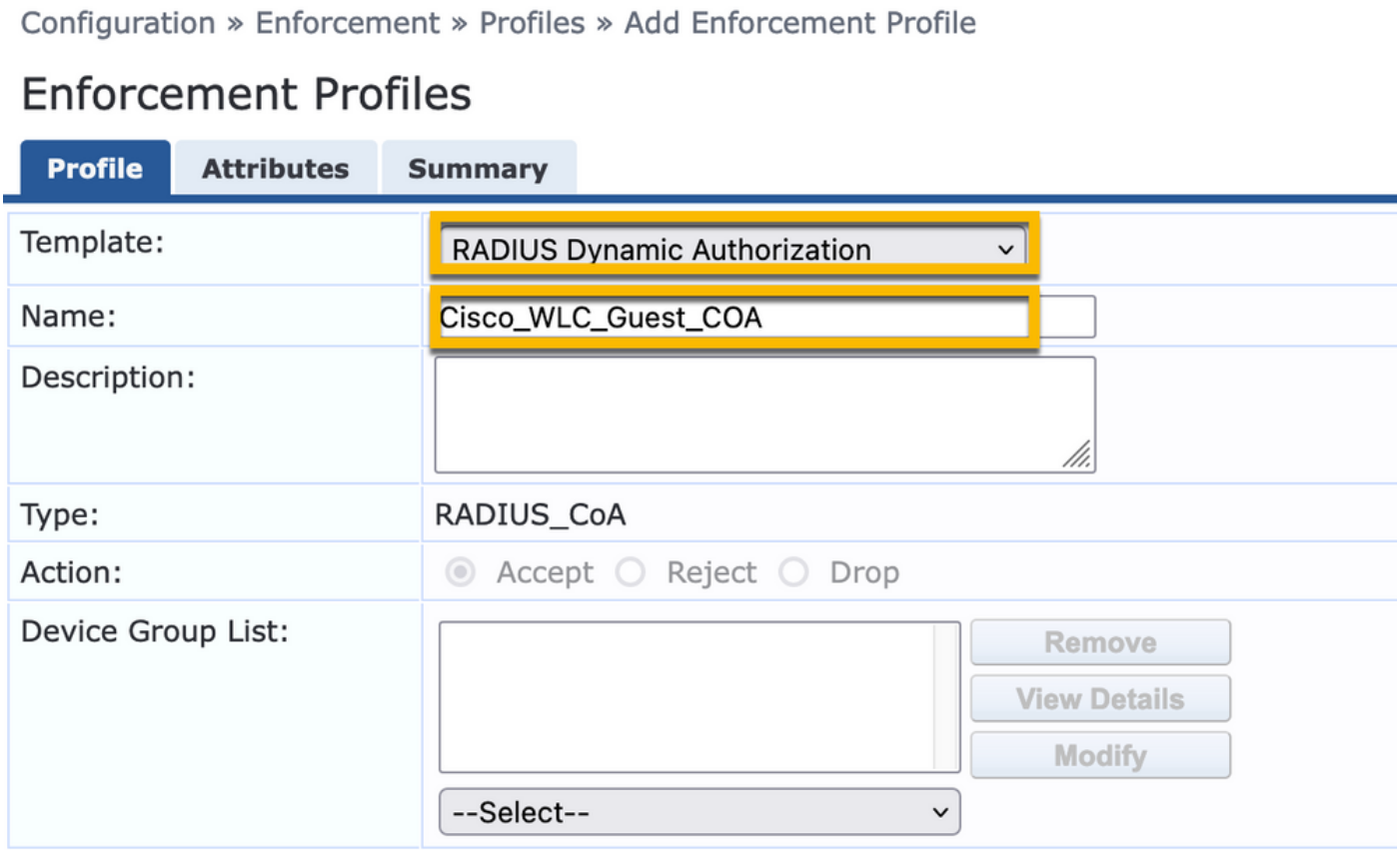
ClearPass重新验证实施策略配置

创建在客户端接受Guest Portal页面上的AUP后立即分配给访客客户端的强制配置文件。

导航到**ClearPass > Configuration > Profiles > Add**。

— 模板：RADIUS动态授权

-姓名 :Cisco_WLC_Guest_COA



Radius:IETF	Calling-Station-Id	%{Radius:IETF:Calling-Station
Radius：思科	Cisco-AVPair	subscriber:command=reauther e
Radius：思科	Cisco-AVPair	%{Radius:Cisco:Cisco-AVPair:subscriber:audit-sessio
Radius：思科	Cisco-AVPair	subscriber:reauthenticate-type type=last

ClearPass访客门户重定向实施配置文件配置

在CPPM终端数据库中找不到MAC地址且“Allow-Guest-Internet”设置为“**true**”时，创建在初始MAB阶段应用于访客的强制配置文件。

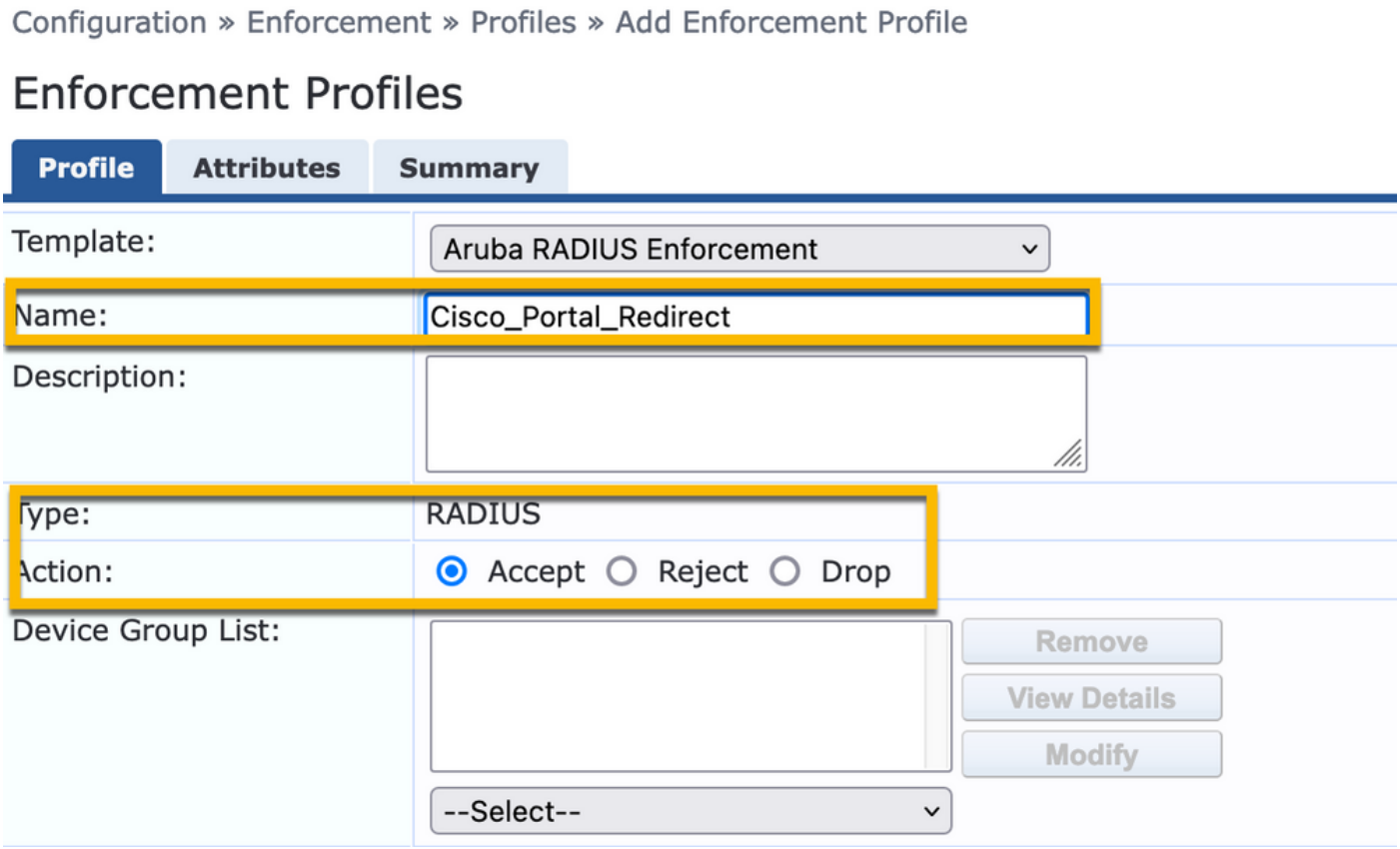
这会导致9800 WLC将访客客户端重定向到CPPM访客门户进行外部身份验证。

导航到**ClearPass > Enforcement > Profiles > Add**。

-姓名 :Cisco_Portal_Redirect

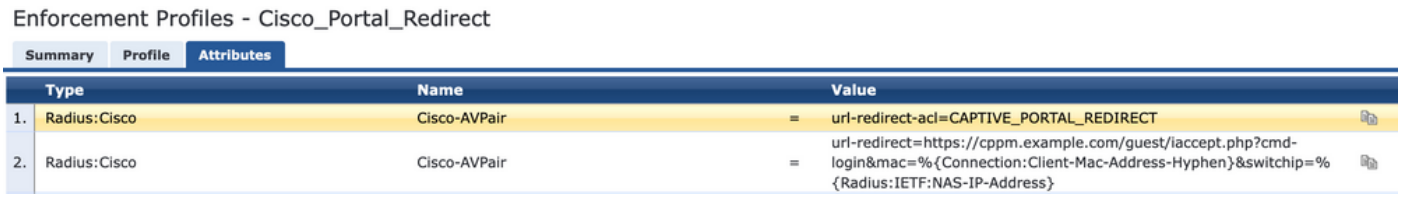
-类型 :RADIUS

-动作:Accept（接受）



ClearPass重定向实施配置文件

在同一对话框的**属性**选项卡下，根据此映像配置两个属性：



ClearPass重定向配置文件属性

url-redirect-acl属性设置为**CAPTIVE-PORTAL-REDIRECT**，这是在C9800上创建的ACL的名称。

> **注意**：RADIUS消息中只传递对ACL的引用，而不传递ACL内容。在9800 WLC上创建的ACL的名称必须与此RADIUS属性的值完全匹配，这一点很重要。

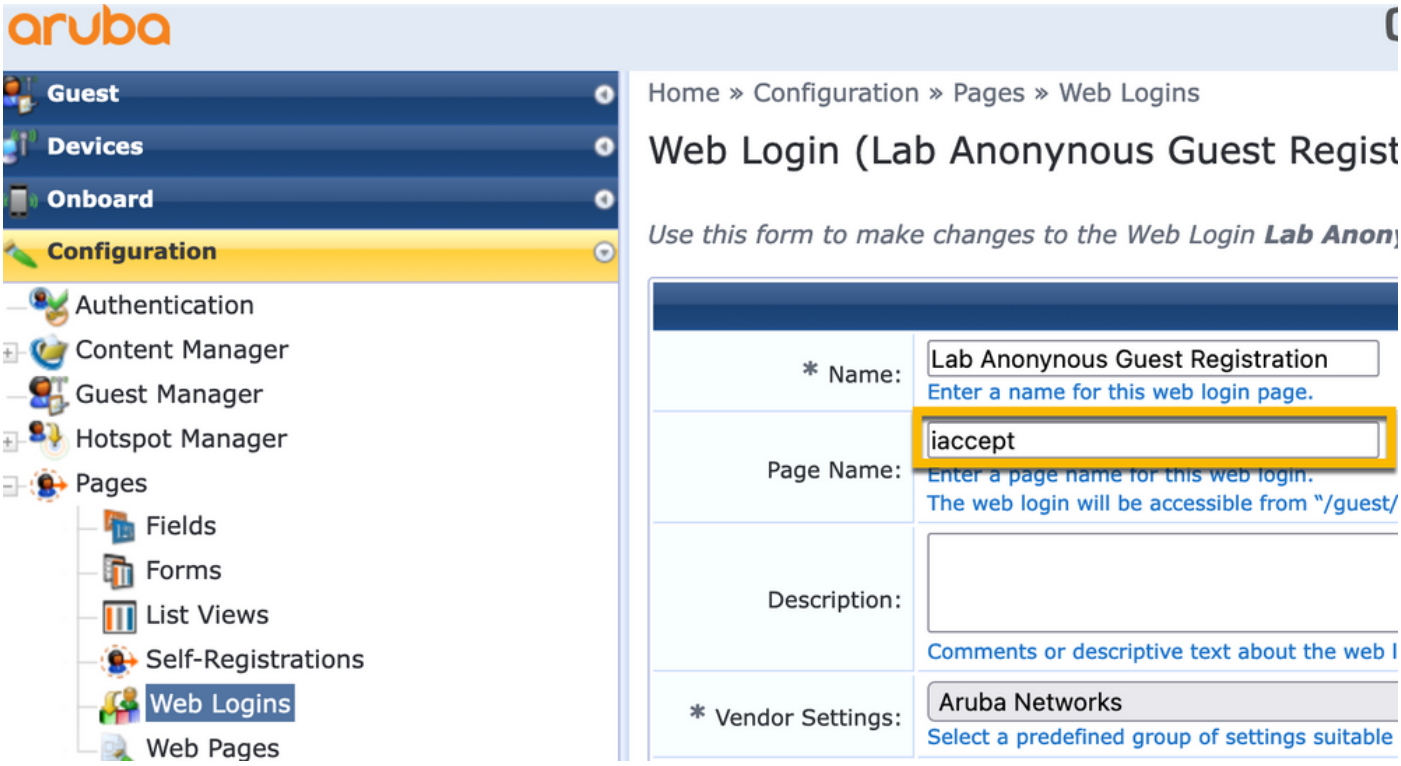
url-redirect属性由多个参数组成：

- **托管访客**门户的目标URL，https://cppm.example.com/guest/iaccept.php
- **访客客户**端MAC，宏%{Connection:Client-Mac-Address-Hyphen}
- **身份验证**器IP（9800 WLC触发重定向），宏%{Radius:IETF:NAS-IP-Address}
- **cmd-login操**作

导航到**CPPM > Guest > Configuration > Pages > Web Logins > Edit**时，会看到ClearPass Guest Web Login Page的URL。

在本例中，CPPM中的访客门户页面名称定义为**iaccept**。

注意：访客门户页面的配置步骤如中所述。



注意：对于思科设备，通常使用**audit_session_id**，但其他供应商不支持该功能。

ClearPass元数据实施配置文件配置

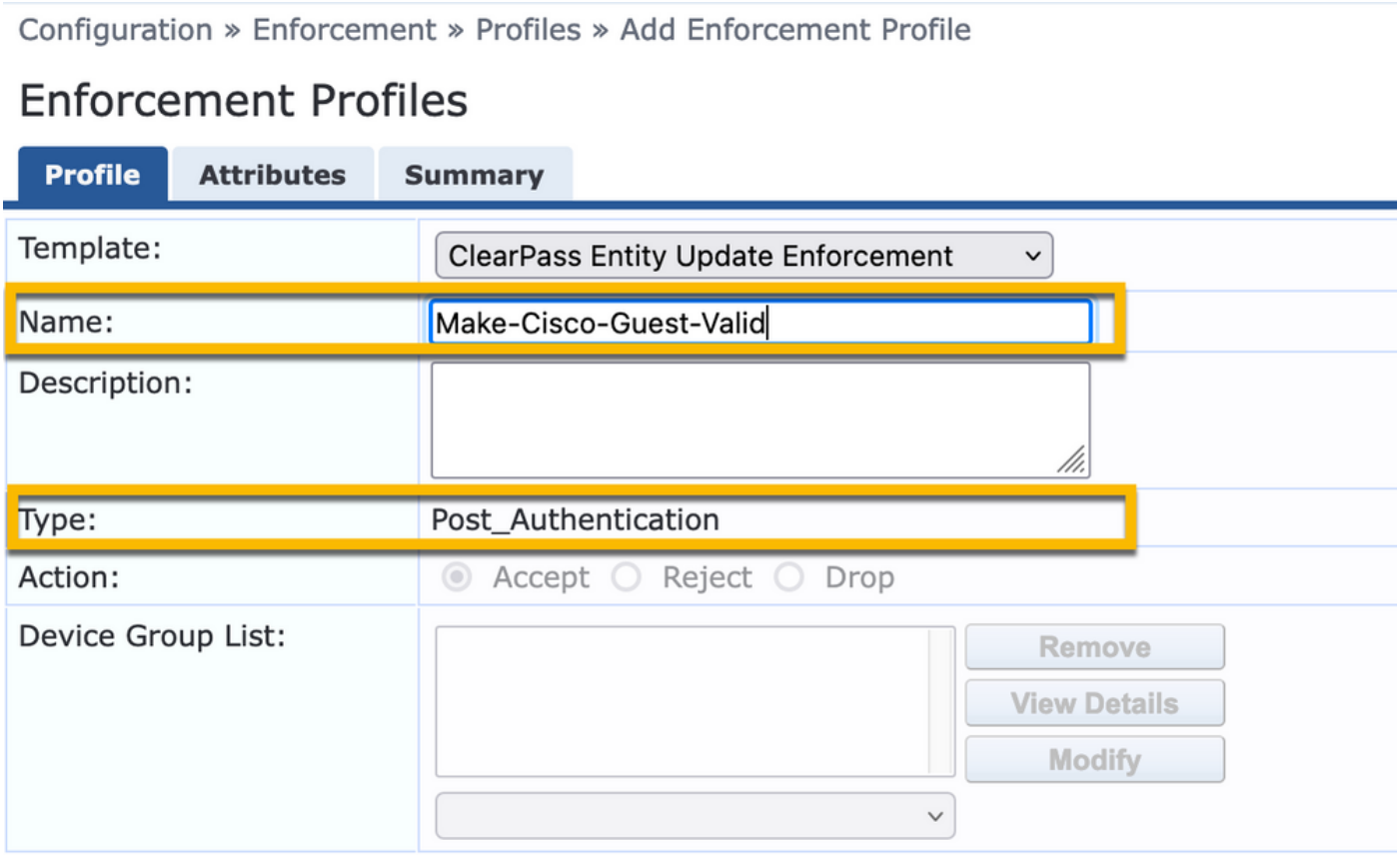
配置实施配置文件，以更新用于CPPM跟踪状态转换的终端元数据属性。

此配置文件应用于终端数据库中的访客客户端MAC地址条目，并将“**Allow-Guest-Internet**”参数设置为“**true**”。

导航到**ClearPass > Enforcement > Profiles > Add**。

— 模板：ClearPass实体更新实施

-类型 :Post_Authentication



在同一对话框中，选择**Attributes**选项卡。

-类型 :终端

-姓名 :允许 — 访客 — 互联网

> **注意**：要将此名称显示在下拉菜单中，您必须手动为至少一个终端定义此字段，如步骤中所述。

-价值:true

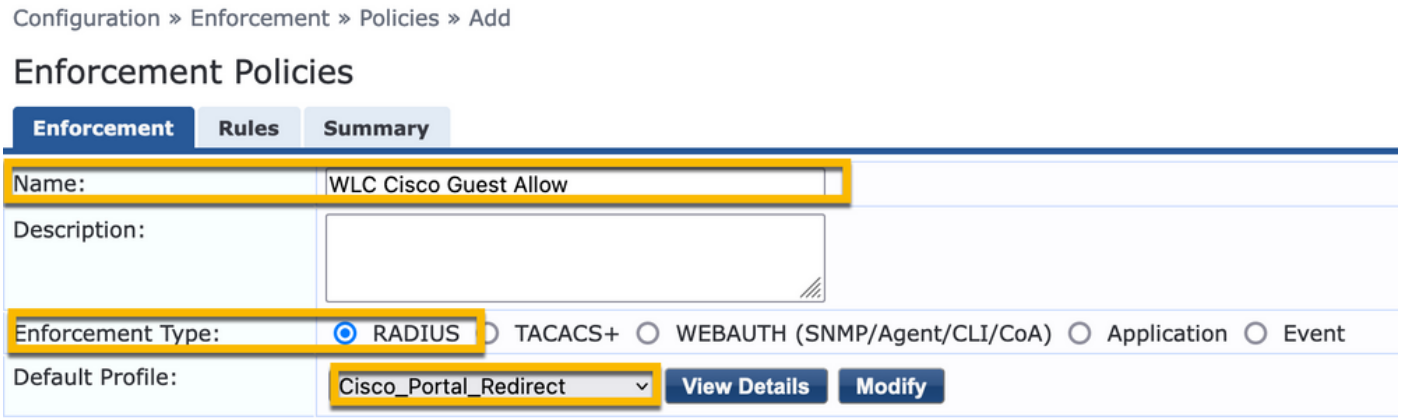
ClearPass访客互联网访问实施策略配置

导航到**ClearPass > Enforcement > Policies > Add。**

-姓名 :WLC思科访客允许

— 实施类型：RADIUS

-缺省配置文件:Cisco_Portal_Redirect



在同一对话框中，导航到**Rules**选项卡，然后单击**Add Rule**。

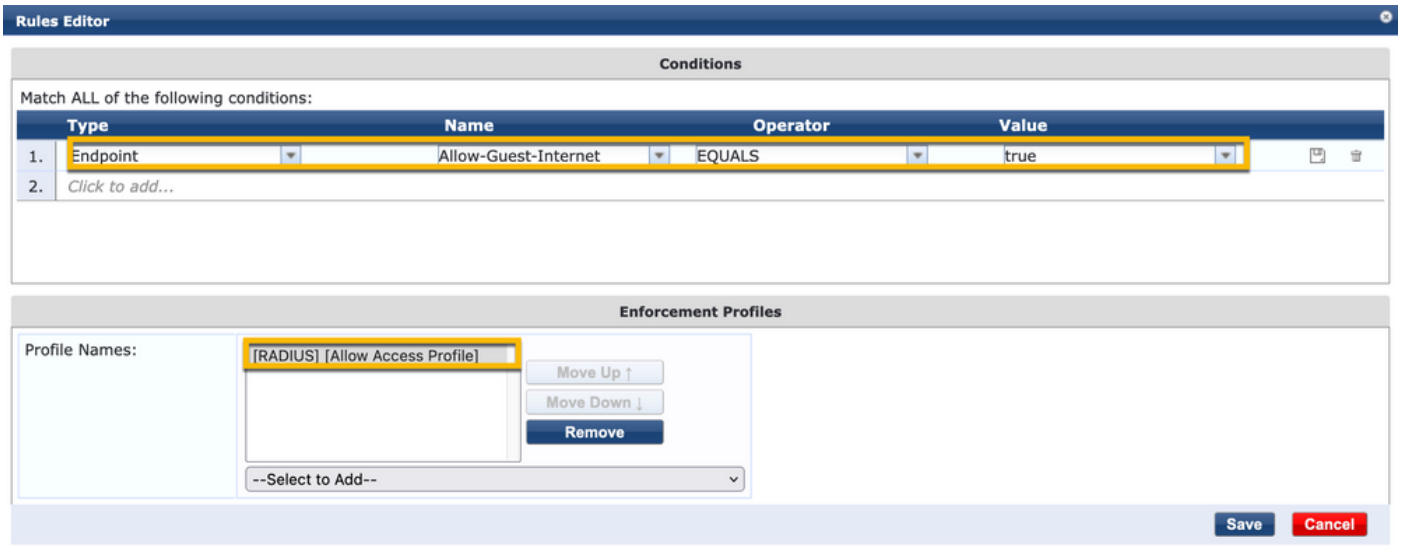
-类型 :终端

-姓名 :允许 — 访客 — 互联网

— 操作员 ：等于

— 值为True

— 配置文件名称/选择添加：[RADIUS] [允许访问配置文件]



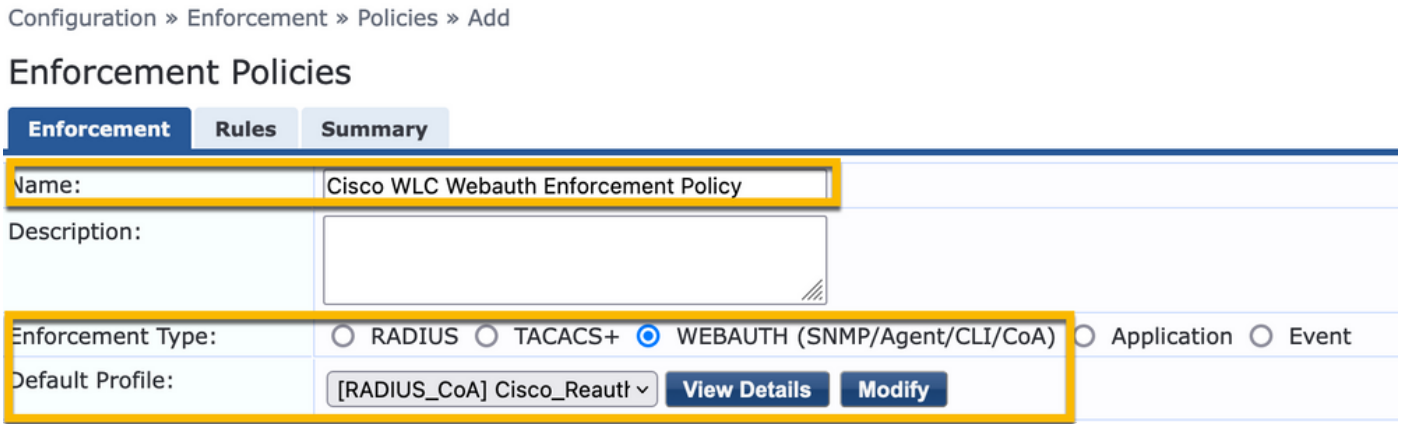
ClearPass访客在AUP后实施策略配置

导航到**ClearPass > Enforcement > Policies > Add**。

-姓名 :Cisco WLC Webauth实施策略

— 实施类型：WEBAUTH(SNMP/Agent/CLI/CoA)

-缺省配置文件:[RADIUS_CoA] Cisco_Reauthenticate_Session



在同一对话框中，导航到**规则>添加**。

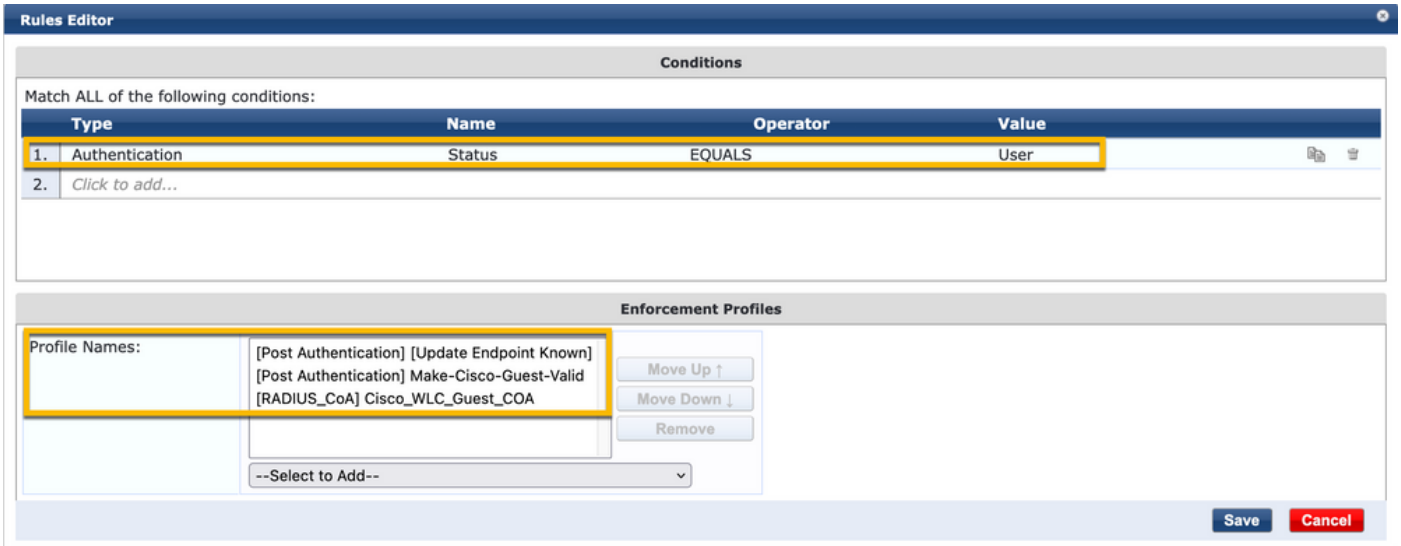
-条件:身份验证

-姓名 :状态

— 操作员：等于

-价值:用户

— 配置文件名称：<add each>:
- [身份验证后] [更新终端已知]
- [Post Authentication] [Make-Cisco-Guest-Valid]
- [RADIUS_CoA] [Cisco_WLC_Guest_COA]



> **注意**：如果您遇到具有连续访客门户重定向伪浏览器弹出窗口的方案，则表明CPPM计时器需要调整或RADIUS CoA消息在CPPM和9800 WLC之间无法正确交换。检验这些站点。

— 导航到**CPPPM > Monitoring > Live Monitoring > Access Tracker**，并确保RADIUS日志条目包含RADIUS CoA详细信息。

— 在**9800 WLC**上，导航到**故障排除>数据包捕获**，在预期接收RADIUS CoA数据包的接口上启用pcap，并验证是否从CPPM收到RADIUS CoA消息。

ClearPass MAB身份验证服务配置

服务在属性值(AV)对Radius: 思科 | CiscoAVPair | cisco-wlan-ssid

导航到**ClearPass > Configuration > Services > Add**。

“服务”选项卡：

-姓名 :访客门户 — Mac身份验证

-类型 :MAC 验证

-更多选项:选择授权，配置文件终端

添加匹配规则：

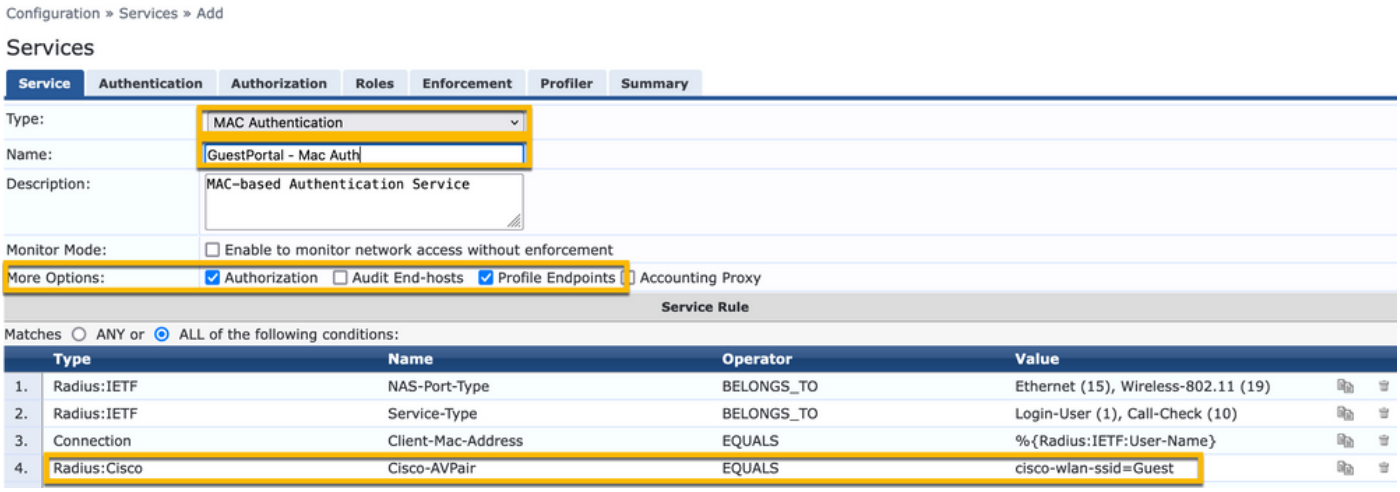
-类型 :RADIUS: 思科

-姓名 :Cisco-AVPair

— 操作员：等于

-价值:cisco-wlan-ssid=Guest（匹配配置的访客SSID名称）

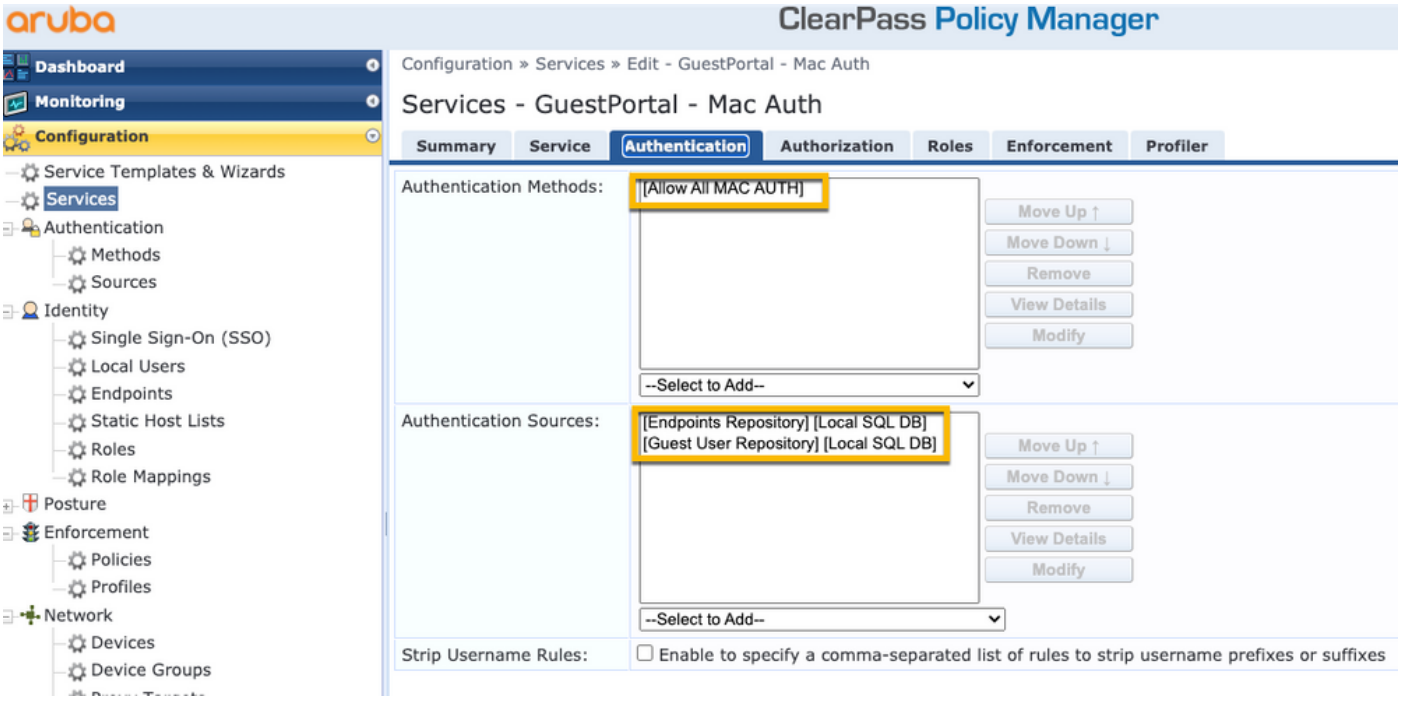
注意：“Guest”是通过9800 WLC广播的访客SSID的名称。



在同一对话框中，选择**Authentication**选项卡。

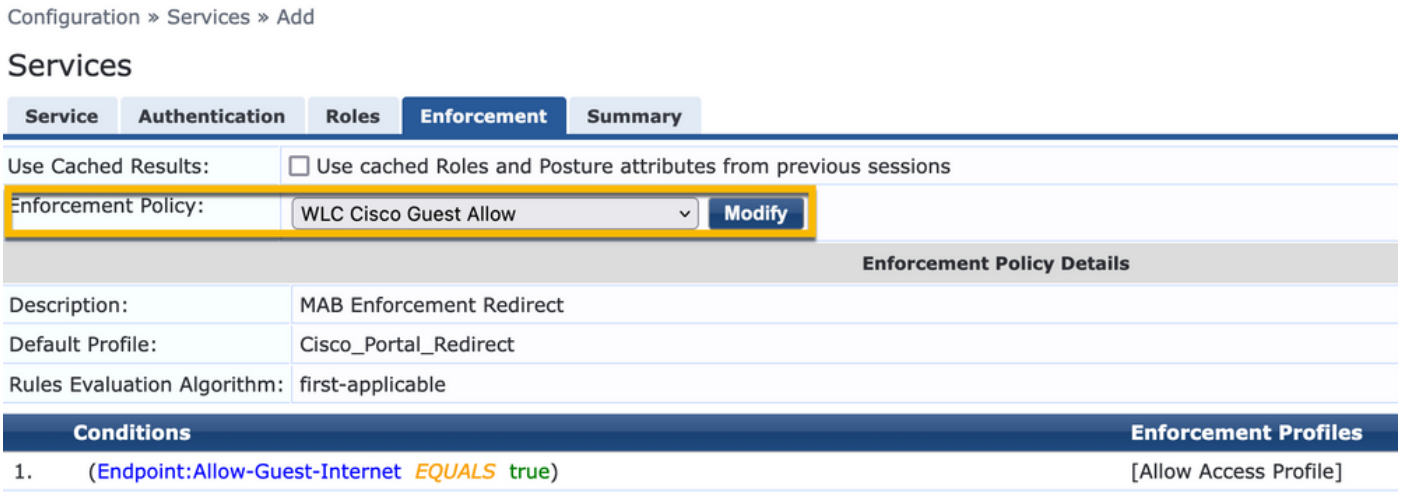
— 身份验证方法：删除[MAC AUTH]，添加[允许所有MAC AUTH]

— 身份验证源：[终端存储库][本地SQL数据库],[访客用户存储库][本地SQL数据库]

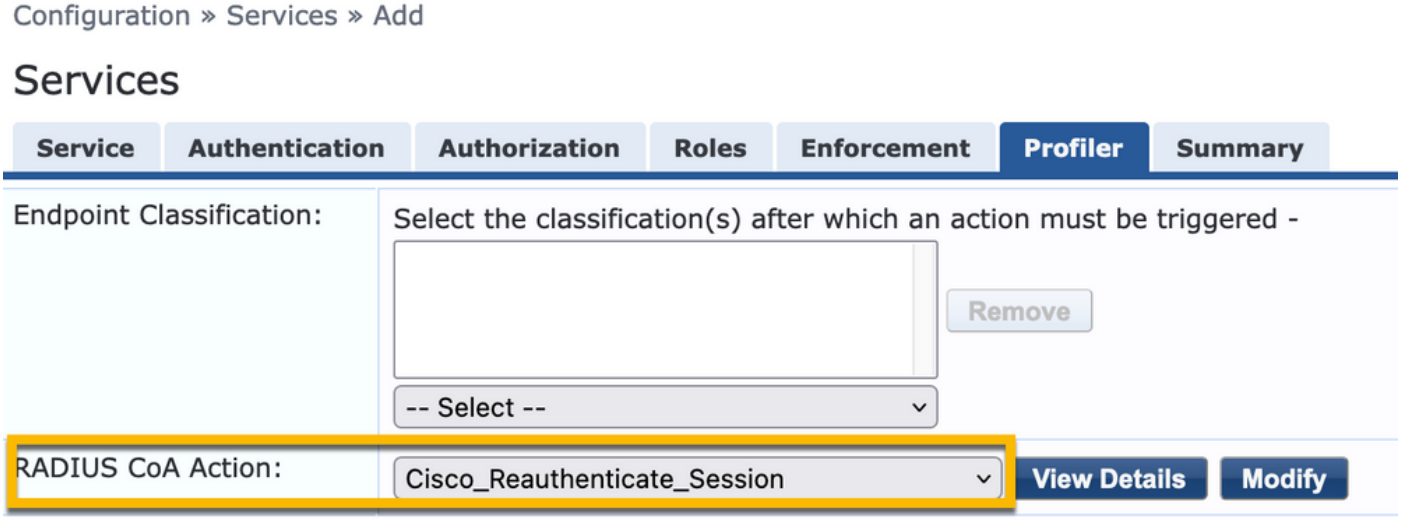


在同一对话框中，选择**Enforcement**选项卡。

— 实施策略：WLC思科访客允许



在同一对话框中，选择**Enforcement**选项卡。

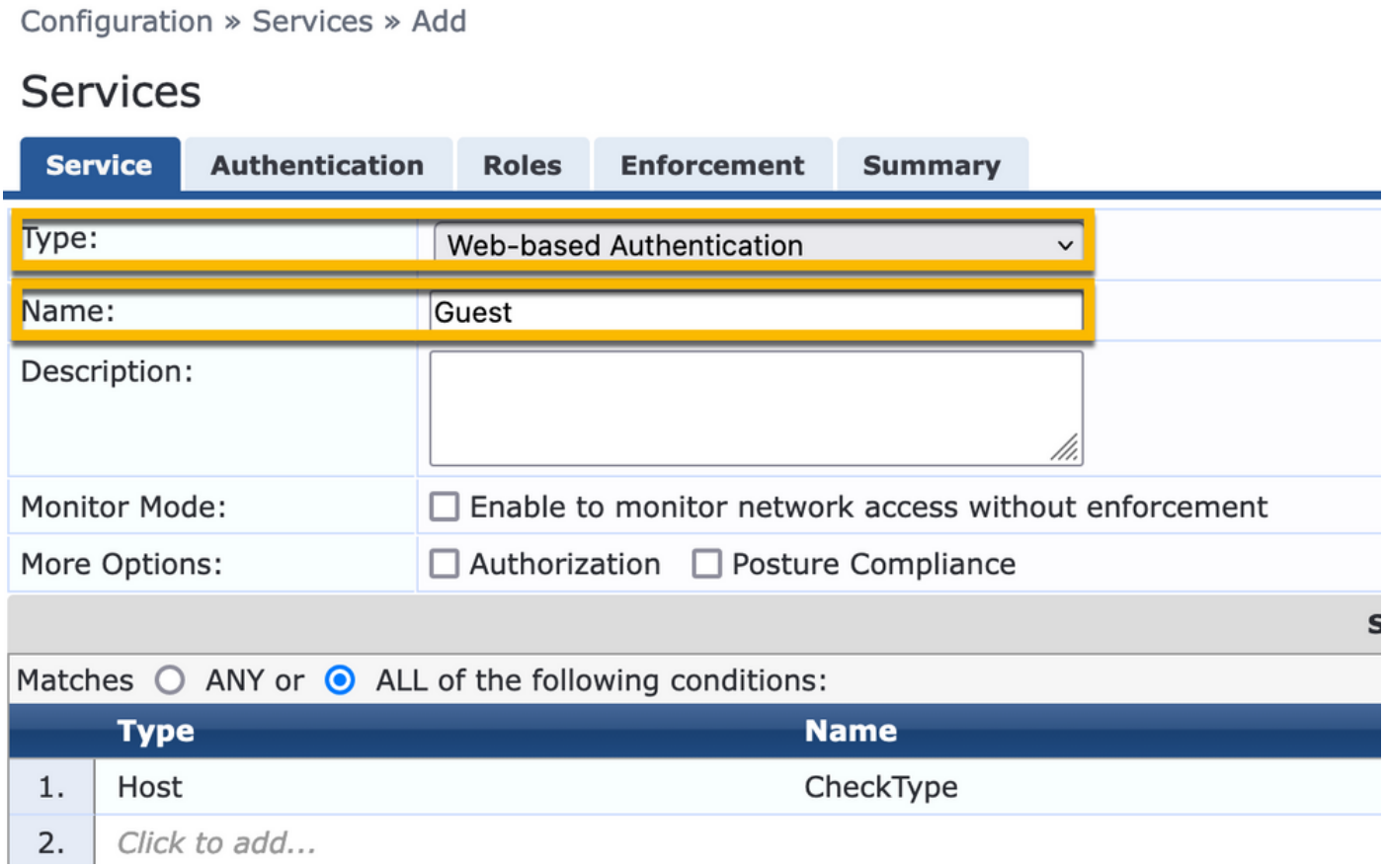


ClearPass Webauth服务配置

导航到**ClearPass > Enforcement > Policies > Add**。

-姓名 :Guest_Portal_Webauth

-类型 :基于Web的身份验证



在同一对话框中，在**Enforcement**选项卡下，Enforcement Policy:Cisco WLC Webauth实施策略。

ClearPass - Web登录

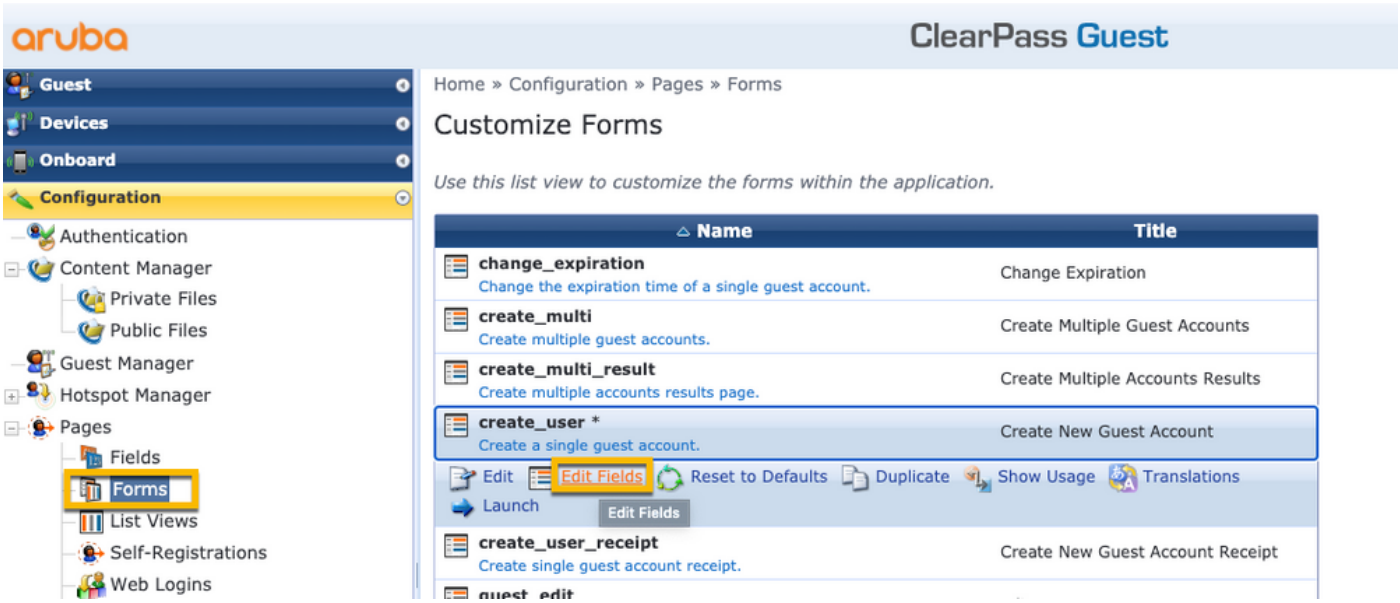
对于Anonymous AUP Guest Portal页面，请使用没有密码字段的单个用户名。

使用的用户名必须定义/设置以下字段：

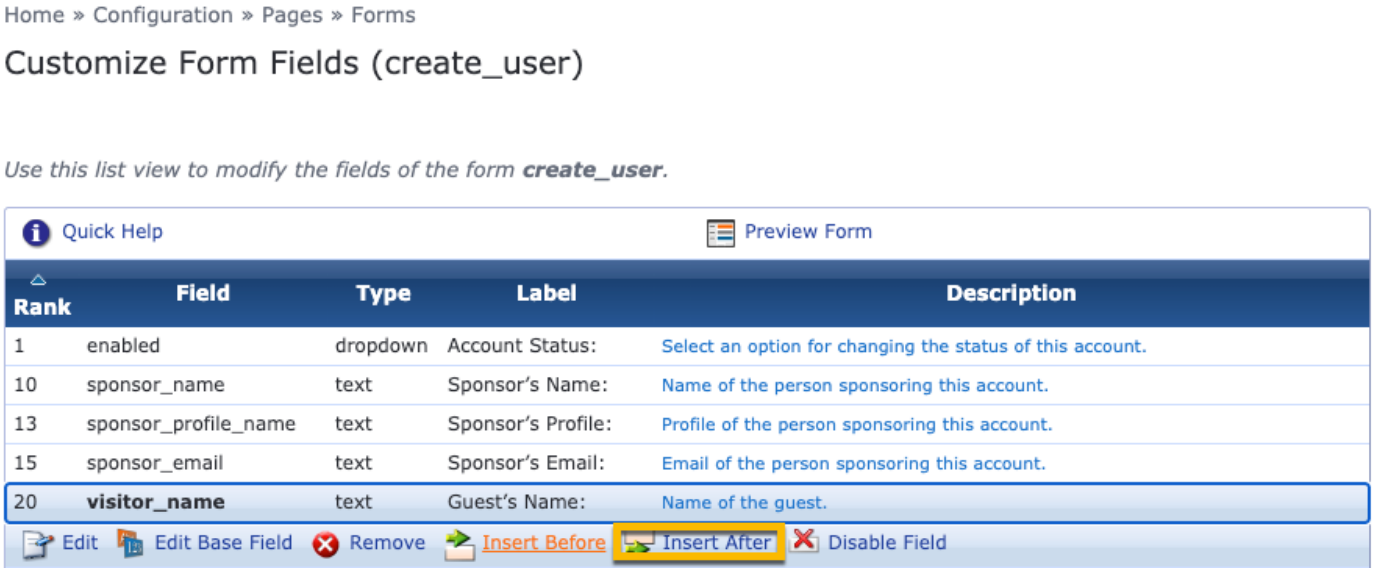
username_auth |用户名身份验证： | 1

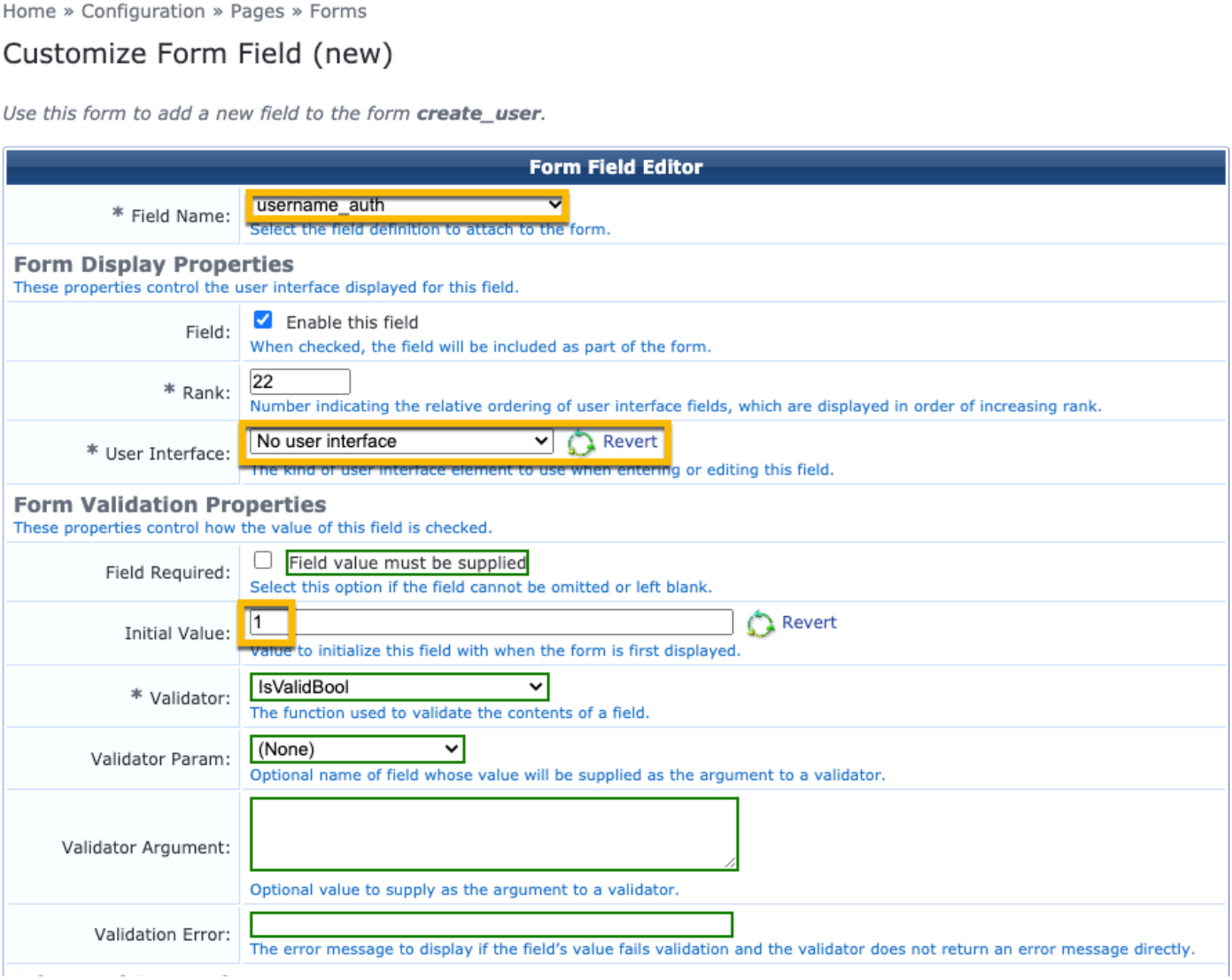
要设置用户的“username_auth”字段，必须首先在“edit user”表单中显示该字段。导航到**ClearPass >**

Guest > Configuration > Pages > Forms，然后选择create_user表单。



选择visitor_name（第20行），然后单击Insert After。





现在创建要在AUP访客门户页面后面使用的用户名。

导航到**CPPPM > Guest > Guest > Manage Accounts > Create**。

-来宾姓名:访客WiFi

-公司名称: 思科

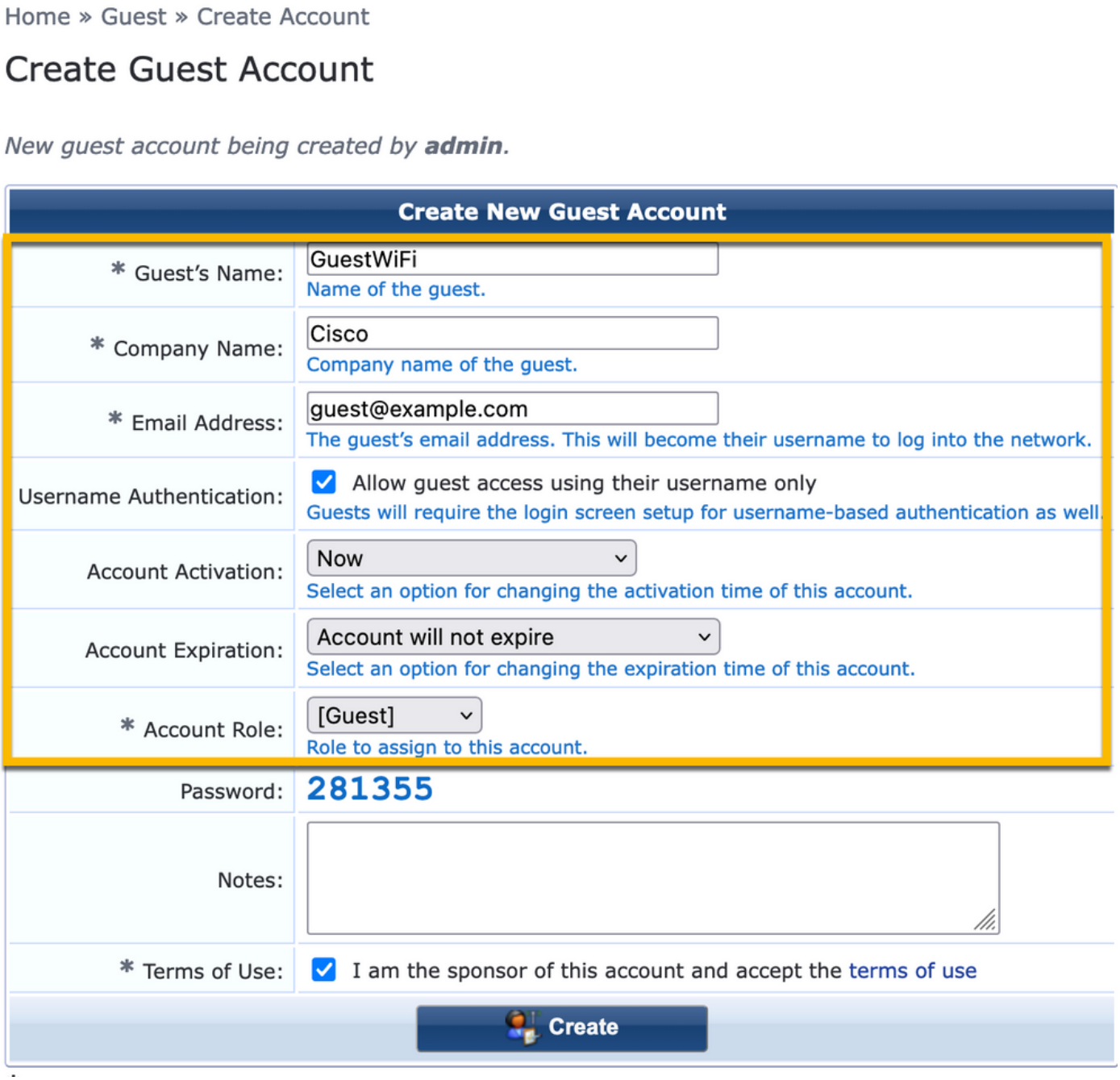
- 电子邮件地址:guest@example.com

— 用户名身份验证：仅允许访客使用其用户名访问：启用

-账户激活:现在

-帐户有效期限:帐户未过期

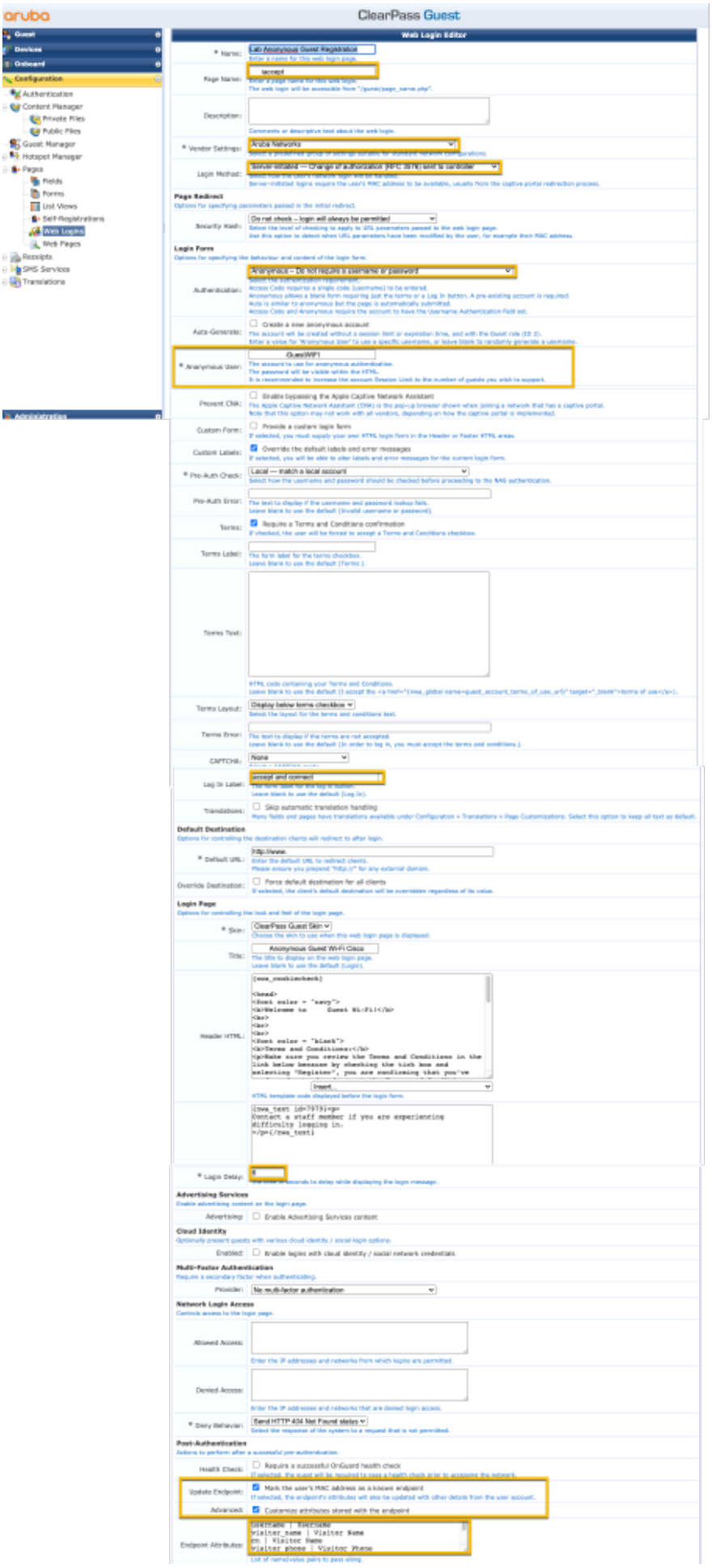
— 使用条款：我是发起人：启用



创建Web登录表单。导航到**CPPM > Guest > Configuration > Web Logins**。

身份验证后部分中的终端属性：

用户名 |用户名
visitor_name |访问者姓名
cn |访问者姓名
visitor_phone |访客电话
邮件 |电子邮件
邮件 |电子邮件
sponsor_name |保证人姓名
sponsor_email |发起人电子邮件
允许 — 访客 — 互联网 | true

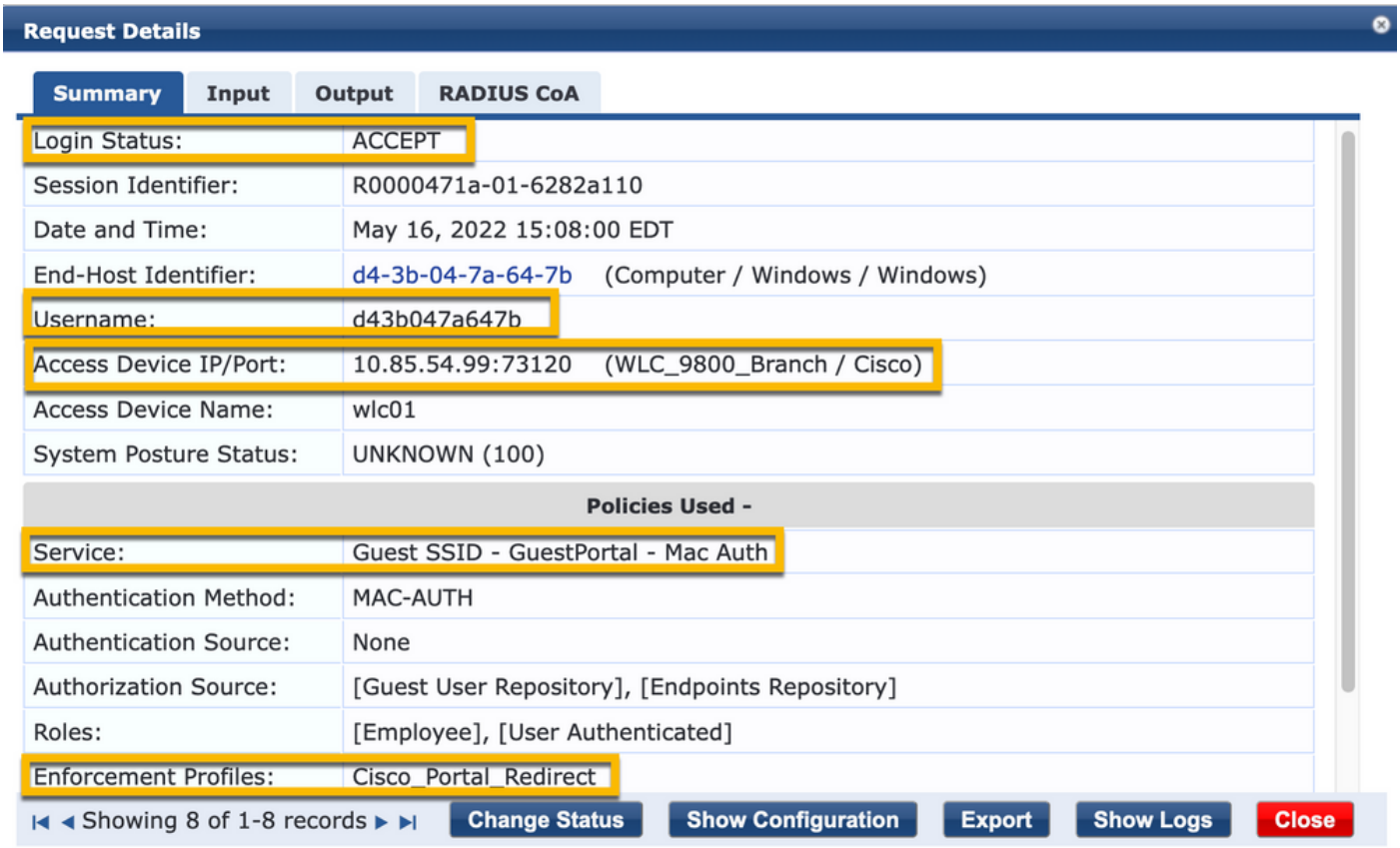

aruba
ClearPass Guest
Web Login Editor
Guest
Devices
Onboard
Configuration
Authentication
Content Manager
Private Files
Public Files
Guest Manager
Hotspot Manager
Pages
Fields
Forms
List Views
Self-Registrations
Web Logins
Web Pages
Receipts
SMS Services
Translations
Administration
* Name:
Page Name:
Description:
* Vendor Settings:
Aruba Networks
Login Method:
Page Redirect
Security Hash:
Login Form
Authentication:
Auto-Generate:
* Anonymous User:
GuestWiFi
Prevent CNA:
Custom Form:
Custom Labels:
* Pre-Auth Check:
Local — match a local account
Pre-Auth Error:
Terms:
Require a Terms and Conditions confirmation
Terms Label:
Terms Text:
Terms Layout:
Display below terms checkbox
Terms Error:
CAPTCHA:
None
Log In Label:
accept and connect
Translations:
Skip automatic translation handling
Default Destination
* Default URL:
http://www.
Override Destination:
Force default destination for all clients
Login Page
* Skin:
ClearPass Guest Skin
Title:
Anonymous Guest Wi-Fi Cisco
Header HTML:
Insert...
* Login Delay:
Advertising Services
Advertising:
Enable Advertising Services content
Cloud Identity
Enabled:
Enable login with cloud identity / social network credentials
Multi-Factor Authentication
Provider:
No multi-factor authentication
Network Login Access
Allowed Access:
Denied Access:
* Deny Behavior:
Send HTTP 404 Not Found status
Post-Authentication
Health Check:
Require a successful OnGuard health check
Update Endpoint:
Mark the user's MAC address as a known endpoint
Advanced:
Customize attributes stored with the endpoint
Endpoint Attributes:
Username | Username
Visitor Name | Visitor Name
cn | Visitor Name
Visitor Phone | Visitor Phone

验证 — 访客CWA授权

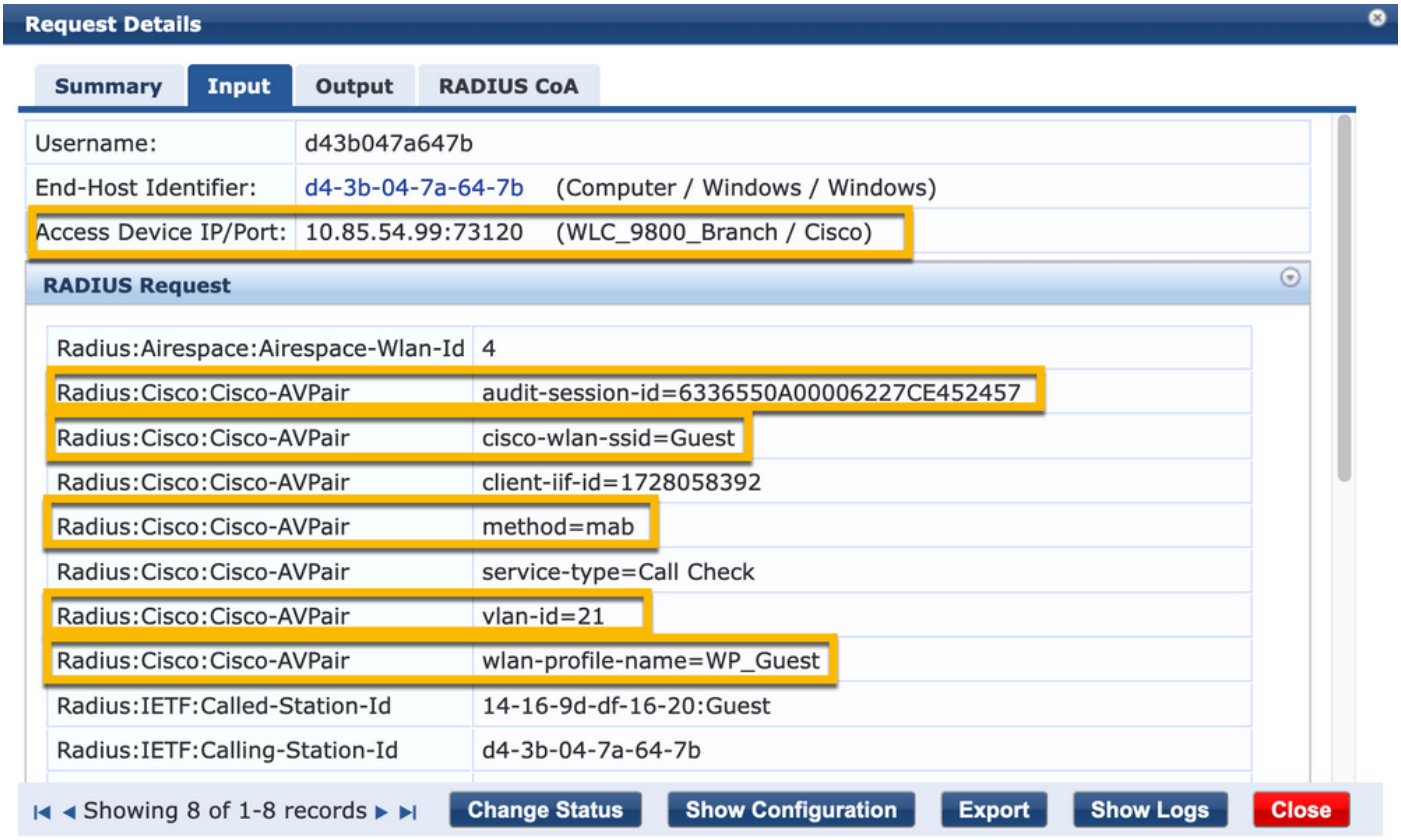
在CPPPM中，导航到**Live Monitoring > Access Tracker**。

连接并触发MAB服务的新访客用户。

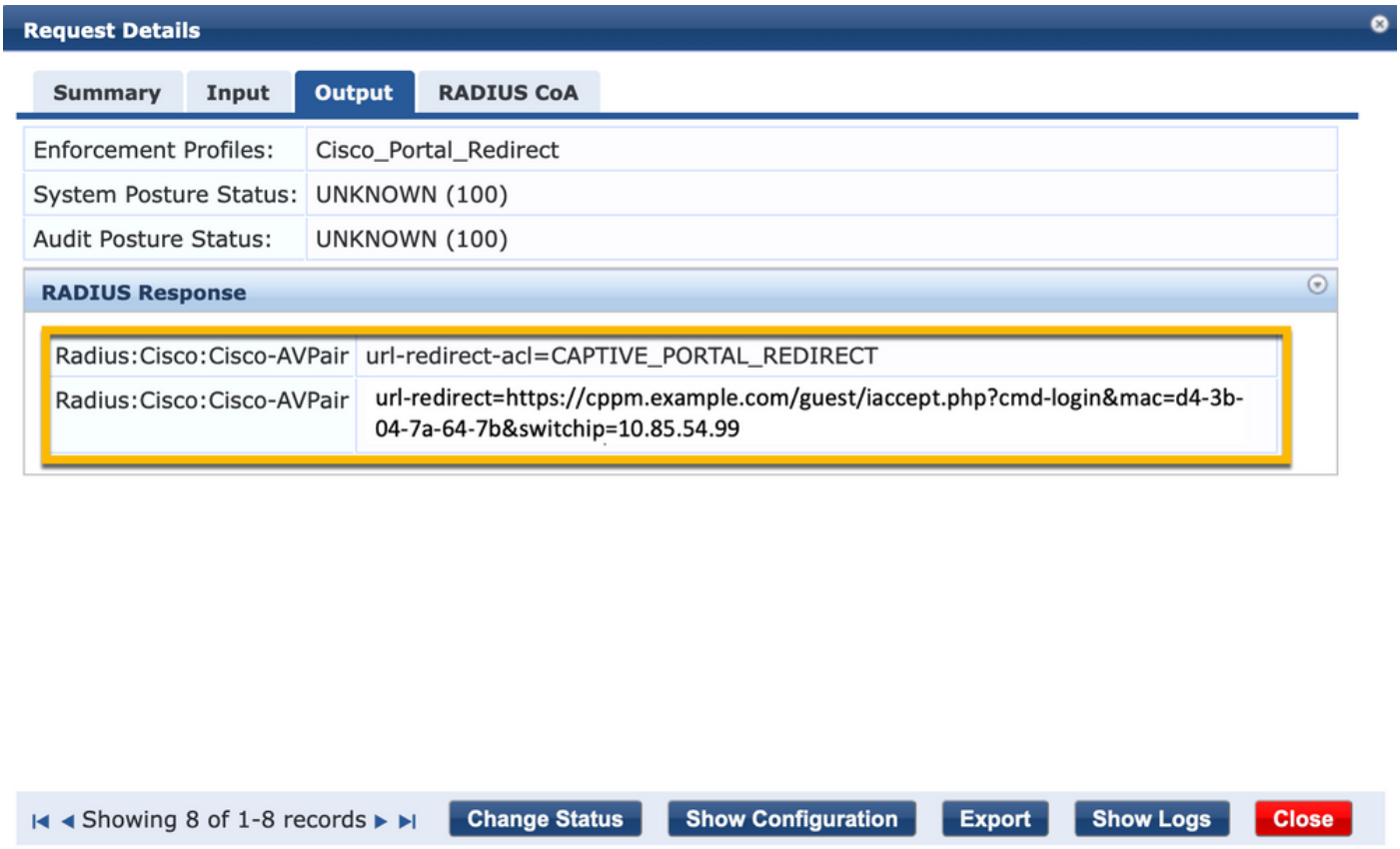
摘要选项卡：



在同一对话框中，导航到**Input(输入)选**项卡。



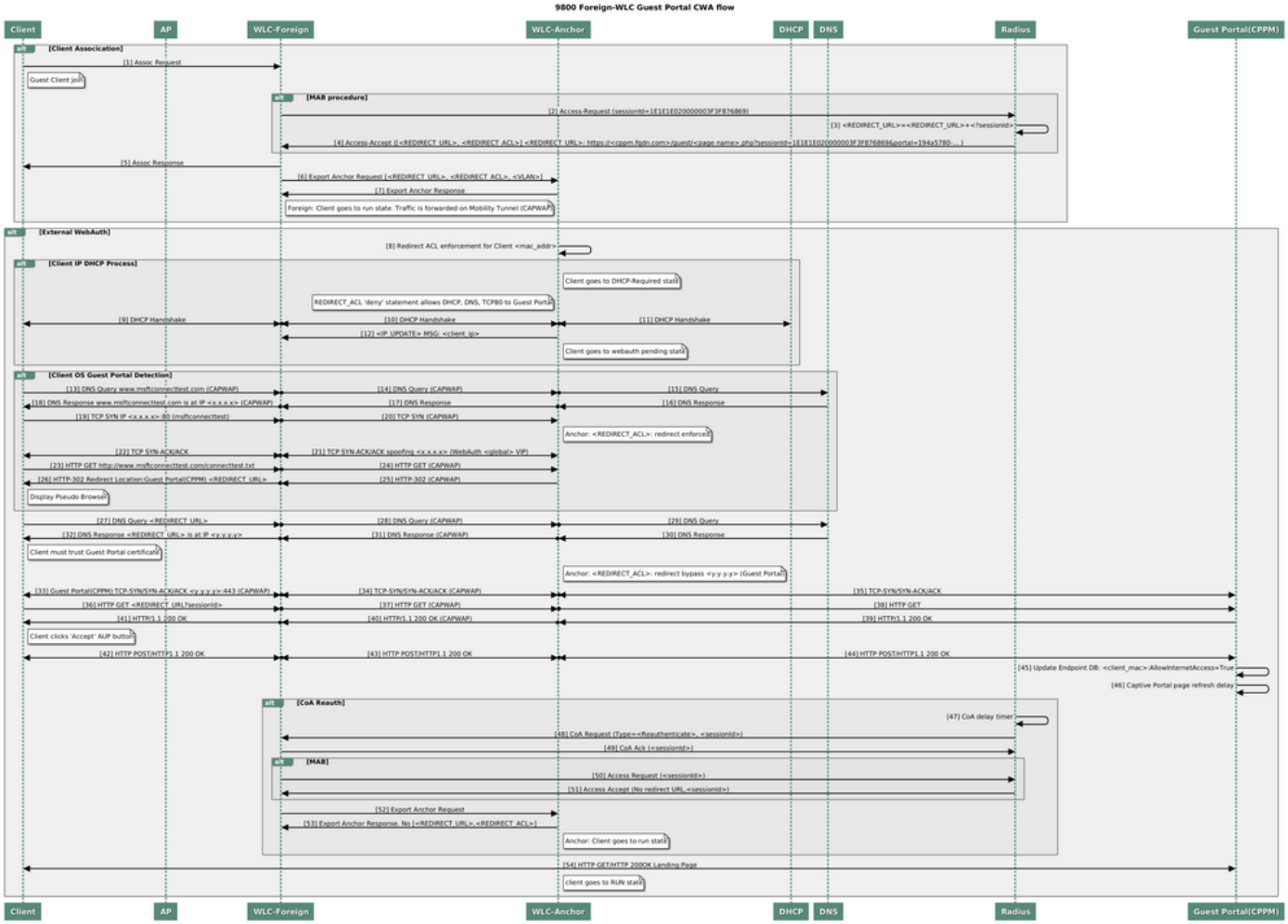
在同一对话框中，导航到**输出**选项卡。



Appendix

为便于参考，此处提供了思科9800外部锚点控制器与RADIUS服务器和外部托管访客门户交互的状

态流程图。



具有锚点WLC的访客中心Web身份验证状态图

相关信息

- [Cisco 9800部署最佳实践指南]
- [了解Catalyst 9800无线控制器配置模型]
- [了解Catalyst 9800无线控制器上的FlexConnect]

- [技术支持和文档 - Cisco Systems]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。