配置9800 WLC与Aruba ClearPass - Dot1x &用于分支机构部署的FlexConnect

目录

简介

本文档介绍Catalyst 9800无线控制器与Aruba ClearPass策略管理器(CPPM)和Microsoft Active Directory(AD)的集成，以在Flexconnect部署中为无线客户端提供dot1x身份验证。

先决条件

要求

Cisco建议您了解这些主题并且已经过配置和验证：

- Catalyst 9800无线控制器
- Aruba ClearPass服务器（需要平台许可证、访问许可证、板载许可证）
- 可运行的Windows AD
- 可选证书颁发机构(CA)
- 可操作的DHCP服务器
- 可操作的DNS服务器（证书CRL验证所需）
- ESXi
- 所有相关组件均同步到NTP并验证其时间是否正确（证书验证需要）
- 主题知识： C9800部署和新配置模型C9800上的FlexConnect操作 Dot1x身份验证

使用的组件

本文档中的信息基于下列硬件和软件版本：

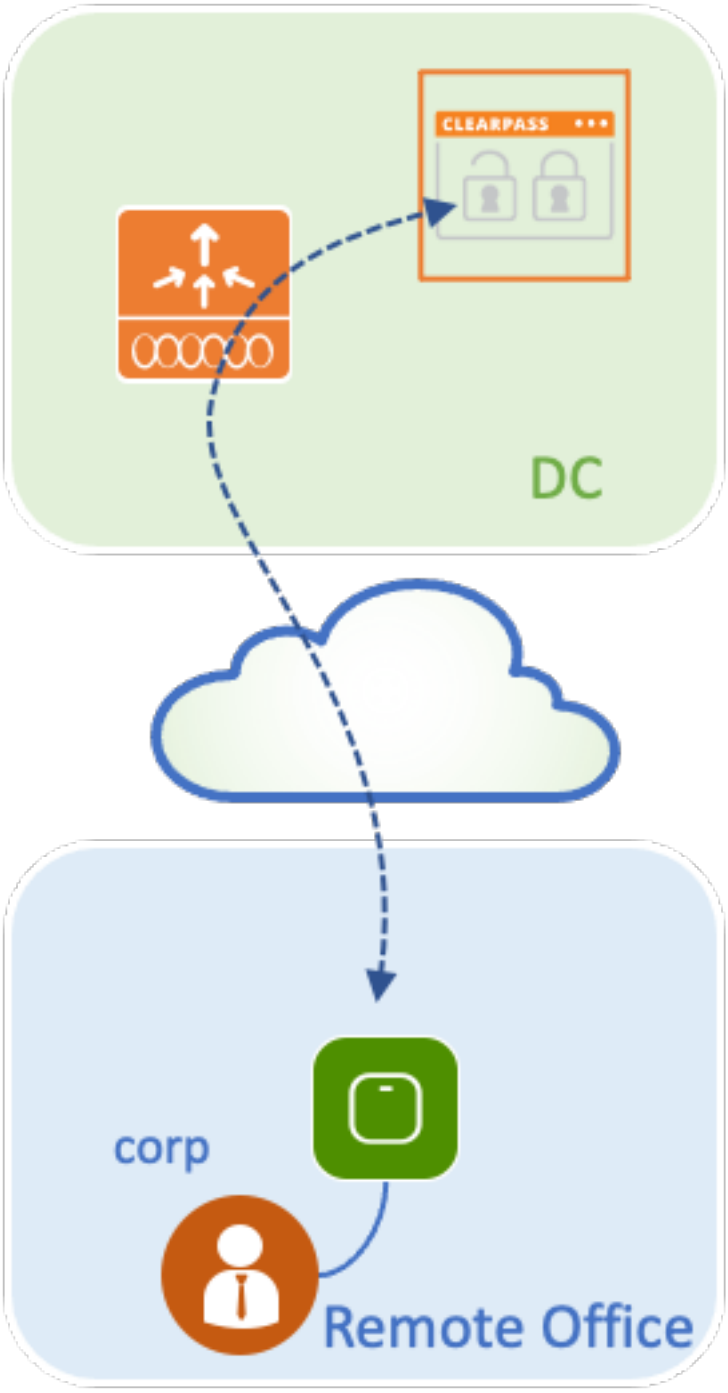
- C9800-L-C Cisco IOS-XE 17.3.3
- C9130AX、4800 AP
- Aruba ClearPass，6-8-0-109592和6.8-3补丁
- MS Windows服务器 Active Directory（GP配置为向托管终端自动发布基于计算机的证书）带选项43和选项60的DHCP服务器DNS 服务器NTP服务器对所有组件进行时间同步CA

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。

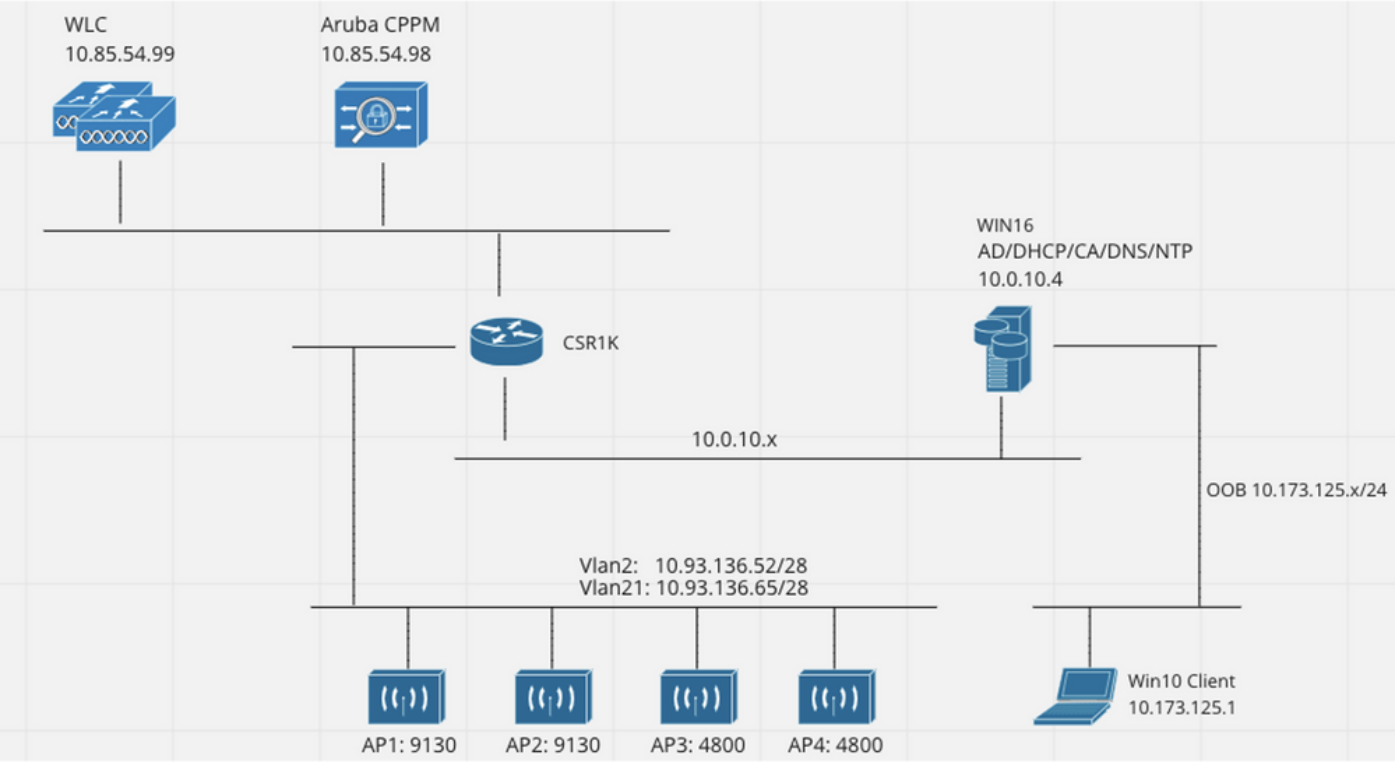
背景信息

流量传输

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向企业员工提供dot1x访问权限。在此配置示例中，PEAP用于通过部署在中央数据中心(DC)中的ClearPass实例为企业用户提供dot1x访问。 计算机证书与针对Microsoft AD服务器的员工凭证验证结合使用。

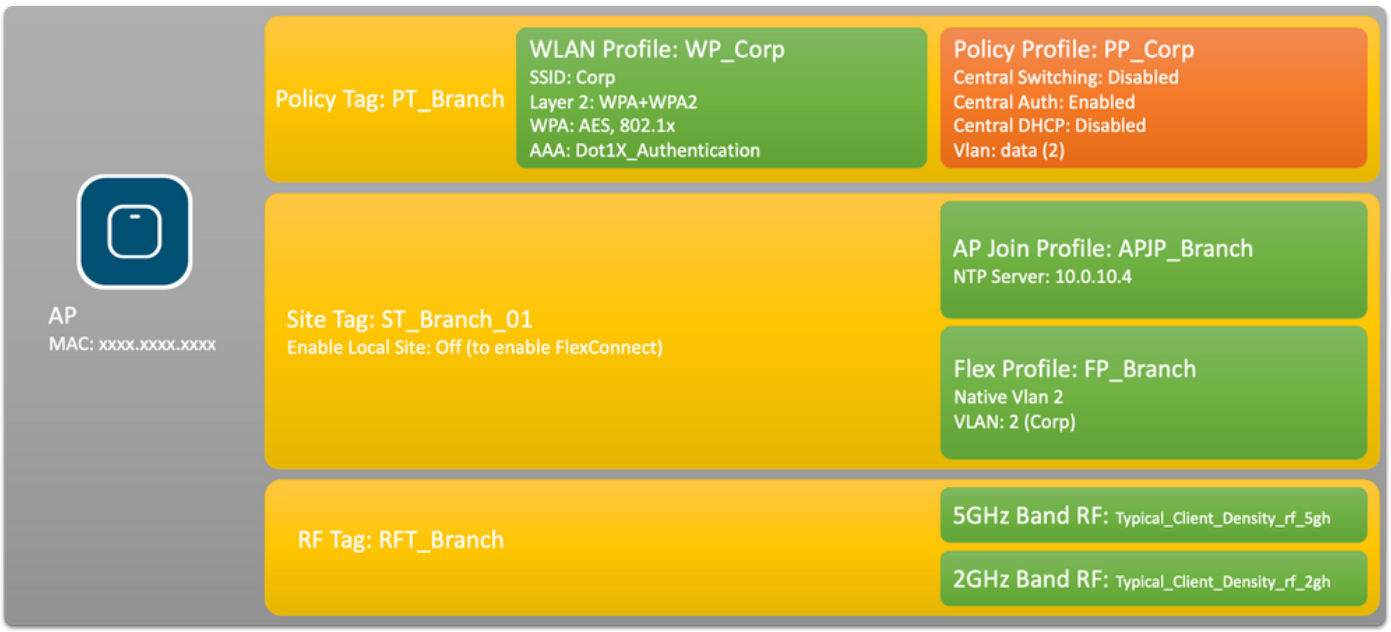


网络图



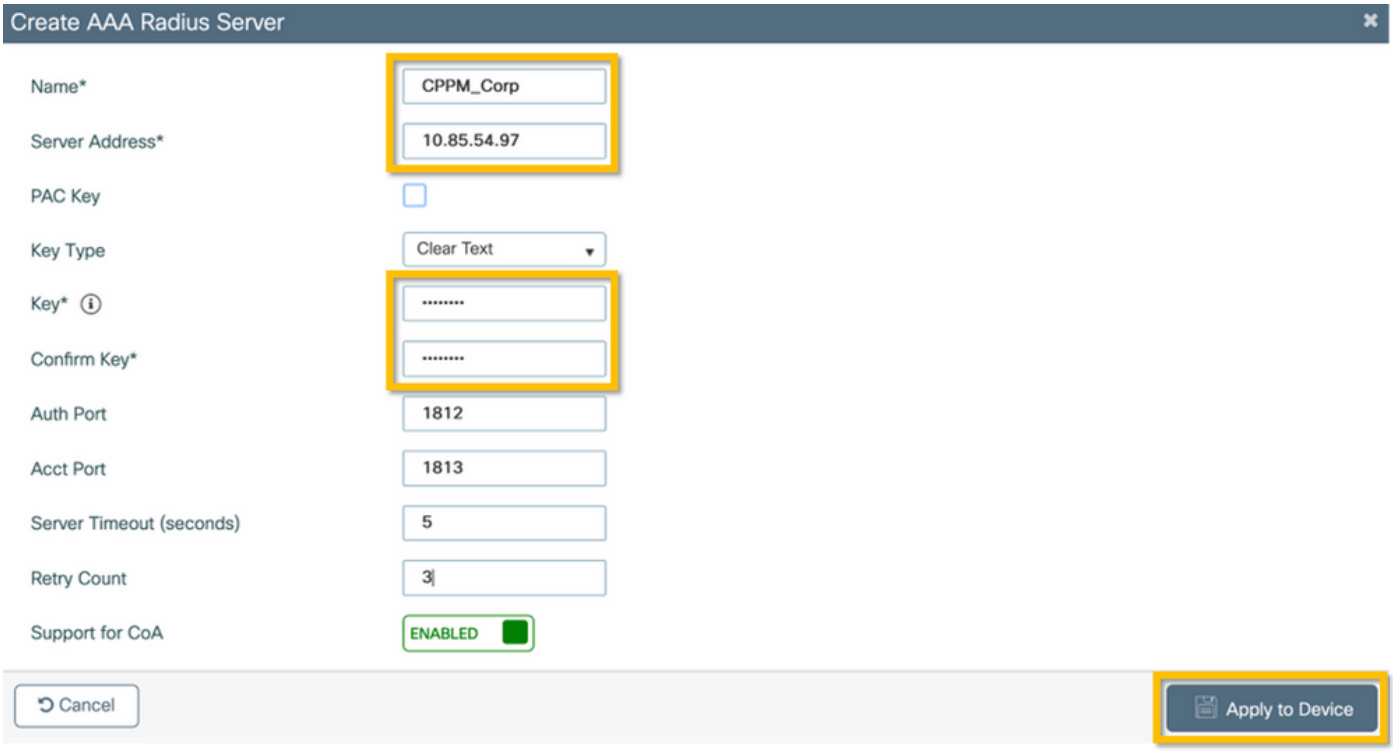
配置Catalyst 9800无线控制器

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。结果配置在图中总结。

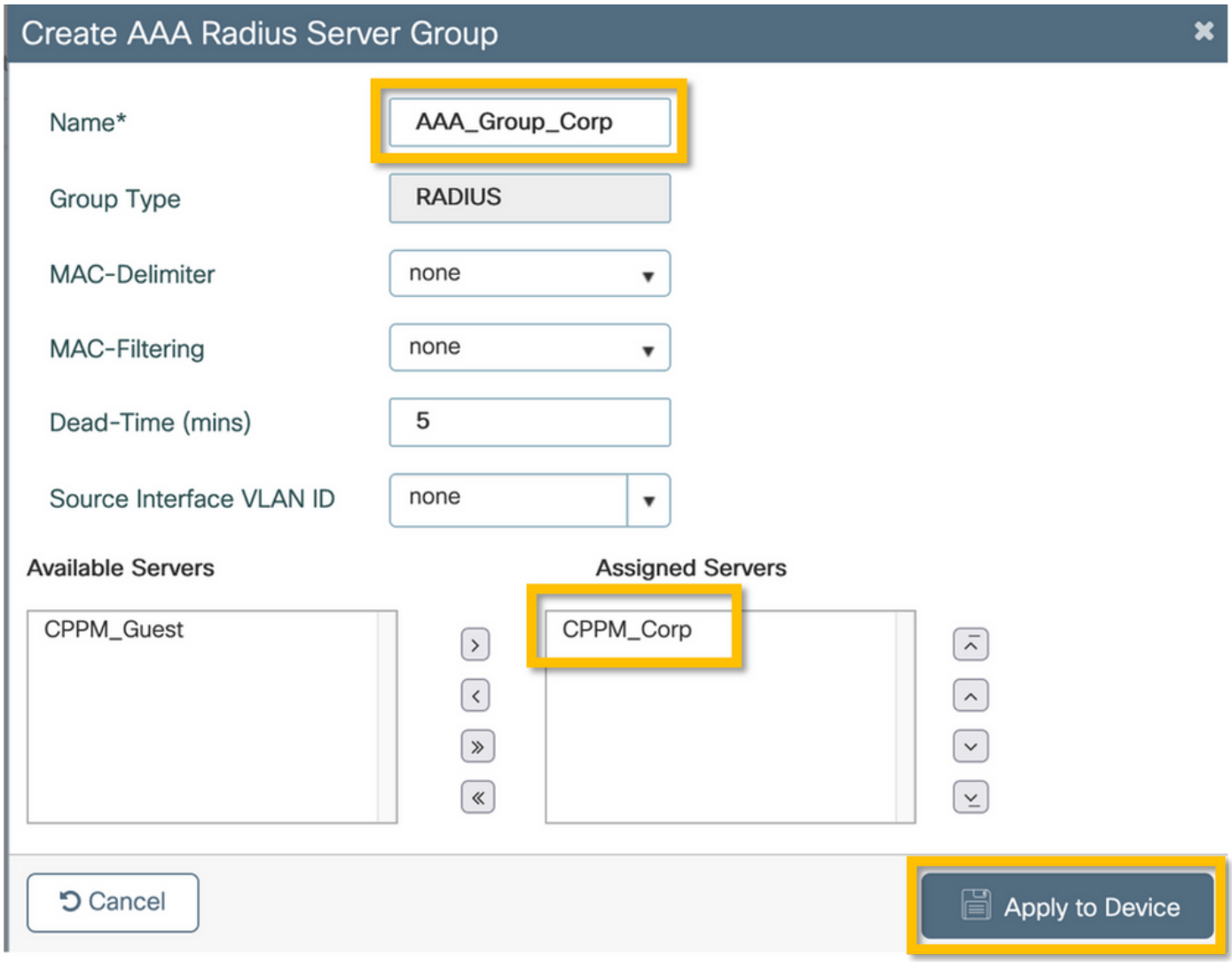


C9800 — 配置dot1x的AAA参数

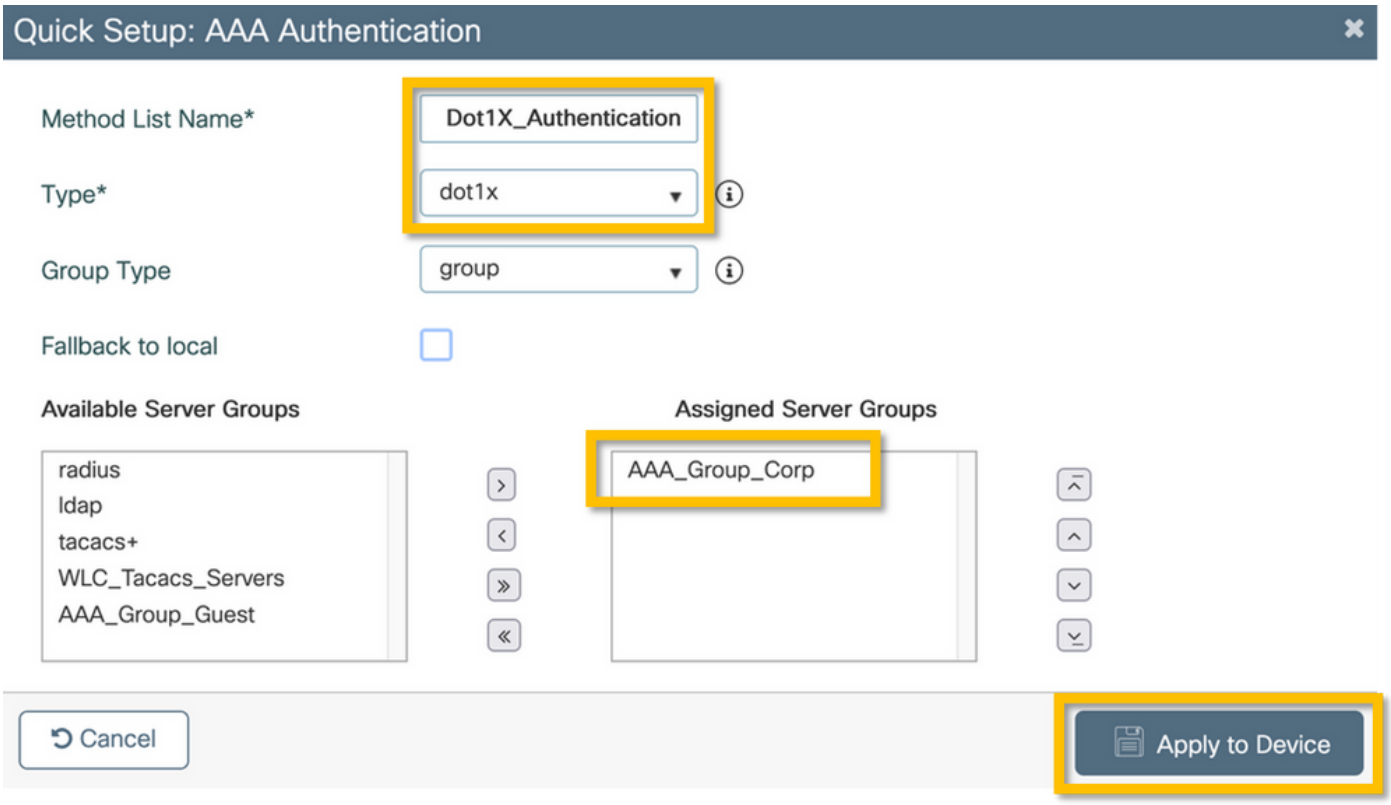
步骤1.将Aruba ClearPass策略管理器“公司”服务器添加到9800 WLC配置。导航到**配置>安全> AAA >服务器/组> RADIUS >服务器。单击+Add**并输入RADIUS服务器信息。单击**Apply to Device**按钮，如下图所示。



步骤2.为企业用户定义AAA服务器组。导航到**配置>安全> AAA >服务器/组> RADIUS >组**，然后单击**+Add**，**输**入RADIUS服务器组名并分配RADIUS服务器信息。单击**Apply to Device**按钮，如下图所示。

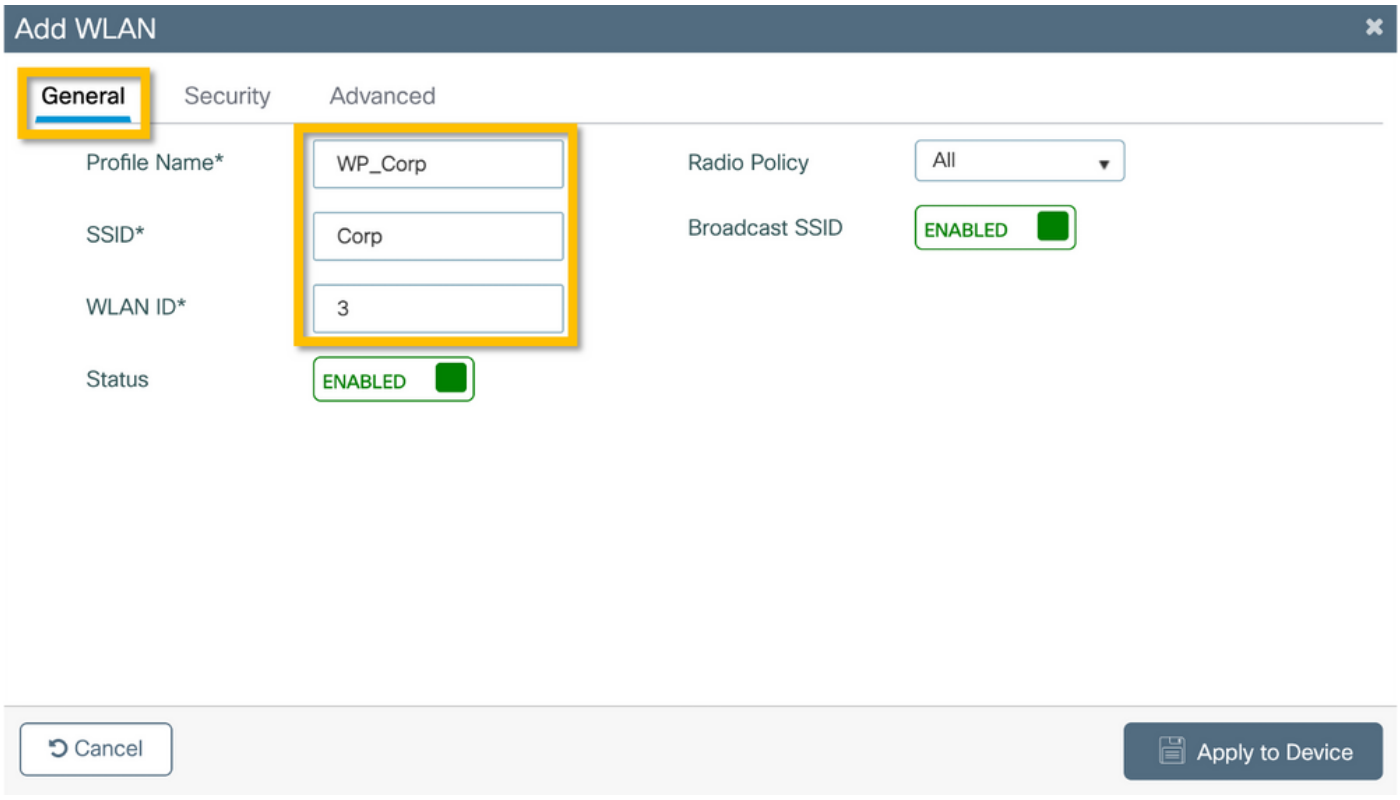


步骤3.为企业用户定义dot1x身份验证方法列表。导航到**Configuration > Security > AAA > AAA Method List > Authentication**，然后单击**+Add**。从下拉菜单中选择**类型dot1x**。单击**应用到设备**按钮，如下图所示。

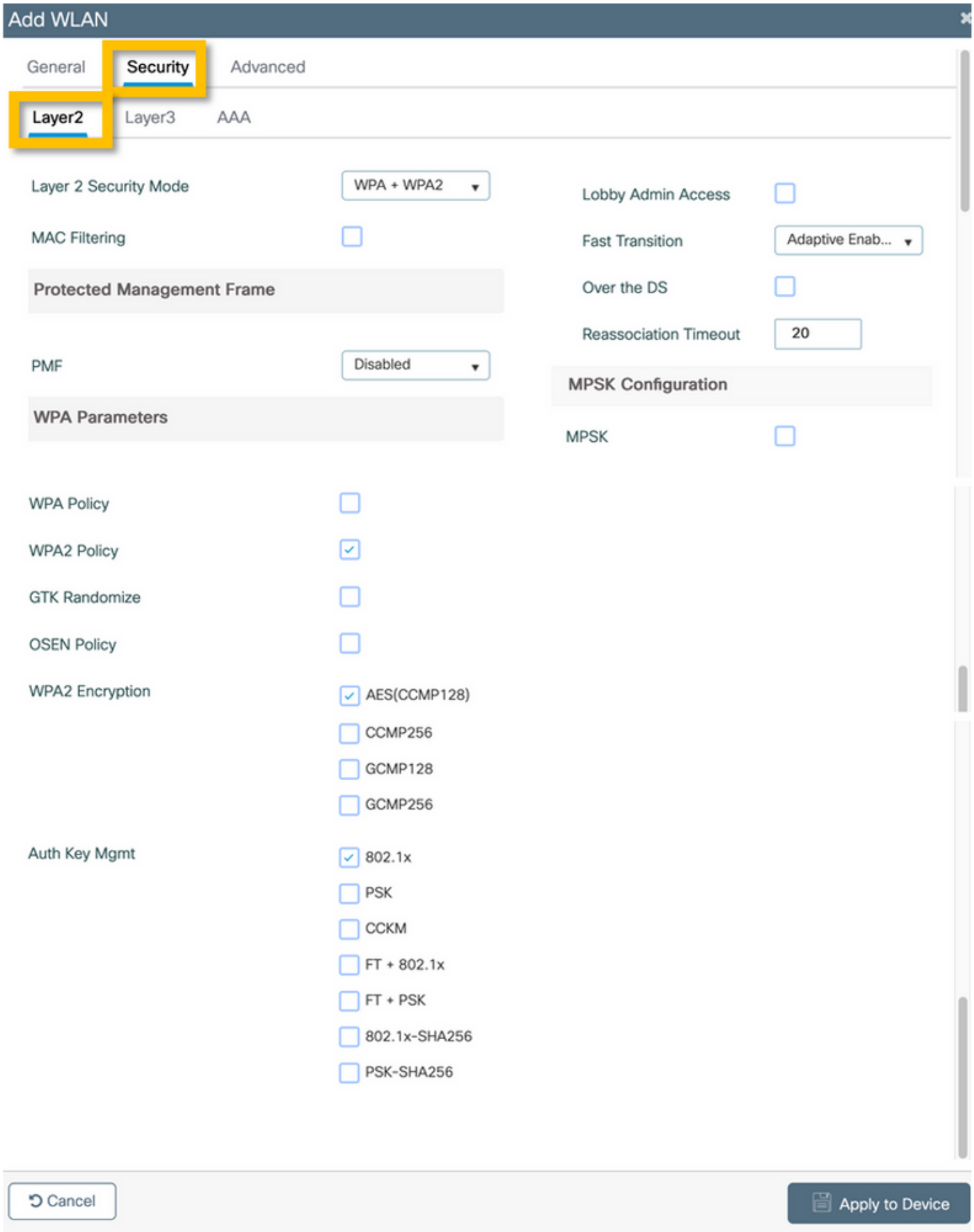


C9800 — 配置"公司"WLAN配置文件

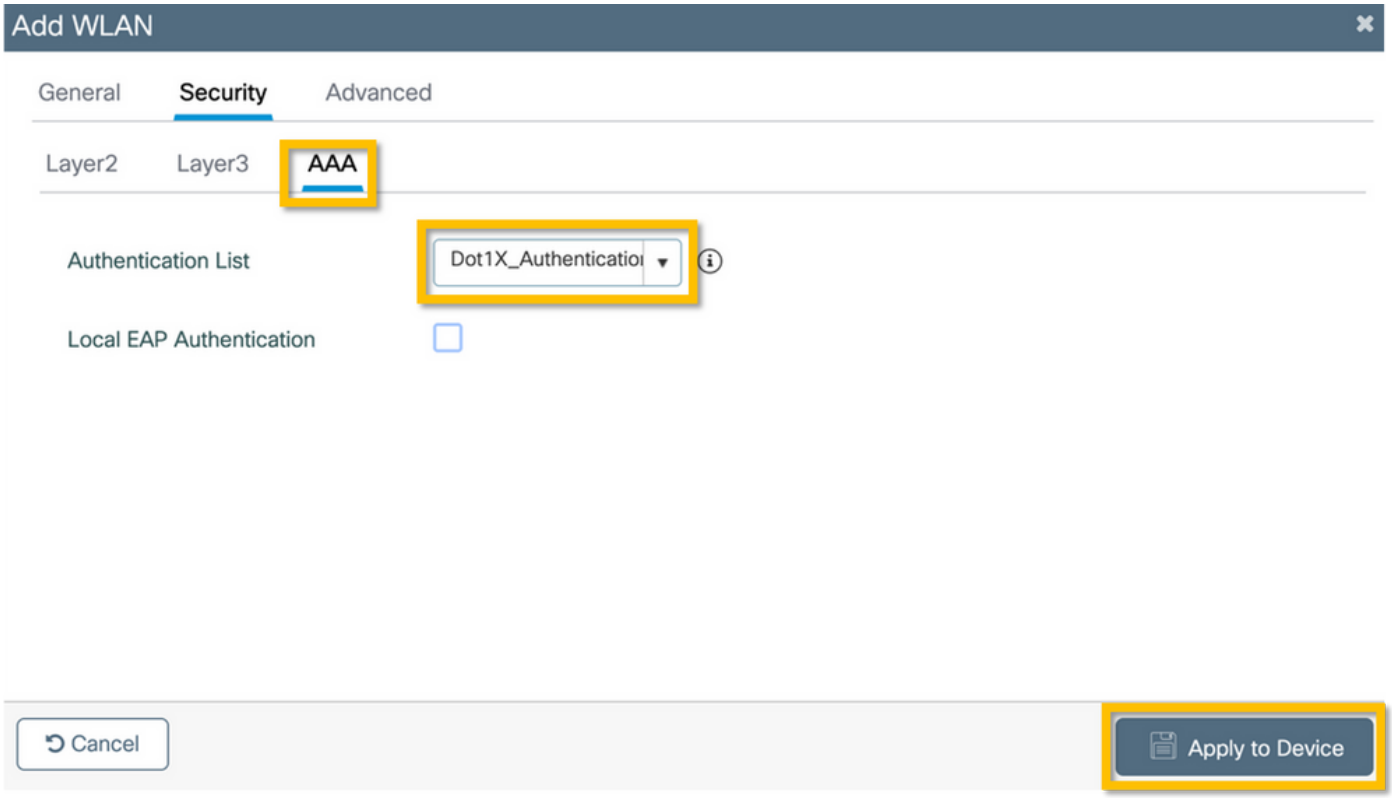
步骤1.导航到**配置>标签和配置文件>无线**，然后点击**+添加**。输入配置文件名称、SSID"Corp"和尚未使用的WLAN ID。



步骤2.导航到Security选项卡和Layer2子选项卡。无需更改此配置示例的任何默认参数。

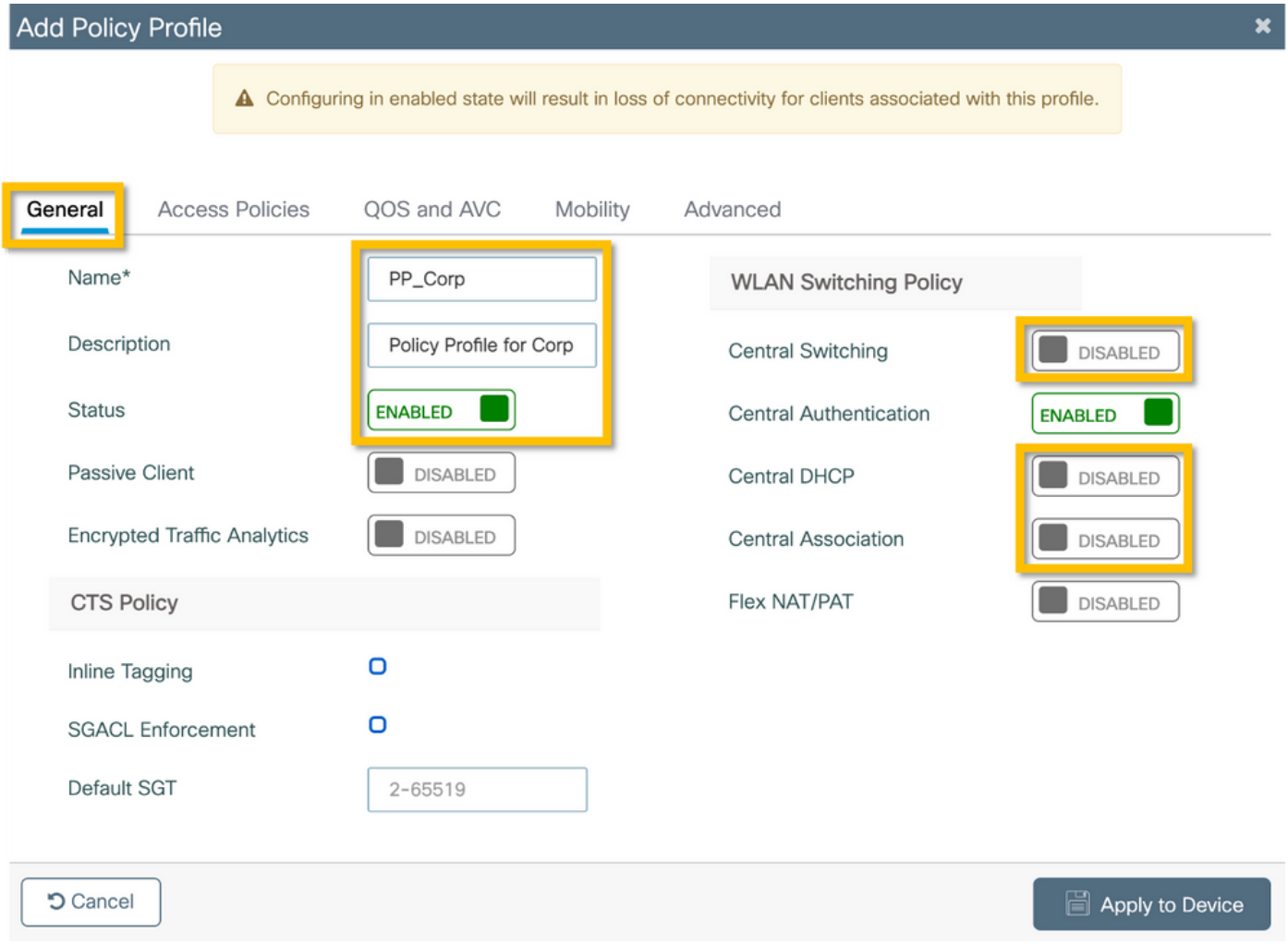


步骤3.导航到AAA子选项卡，然后选择之前配置的身份验证方法列表。单击Apply to Device按钮，如下图所示。

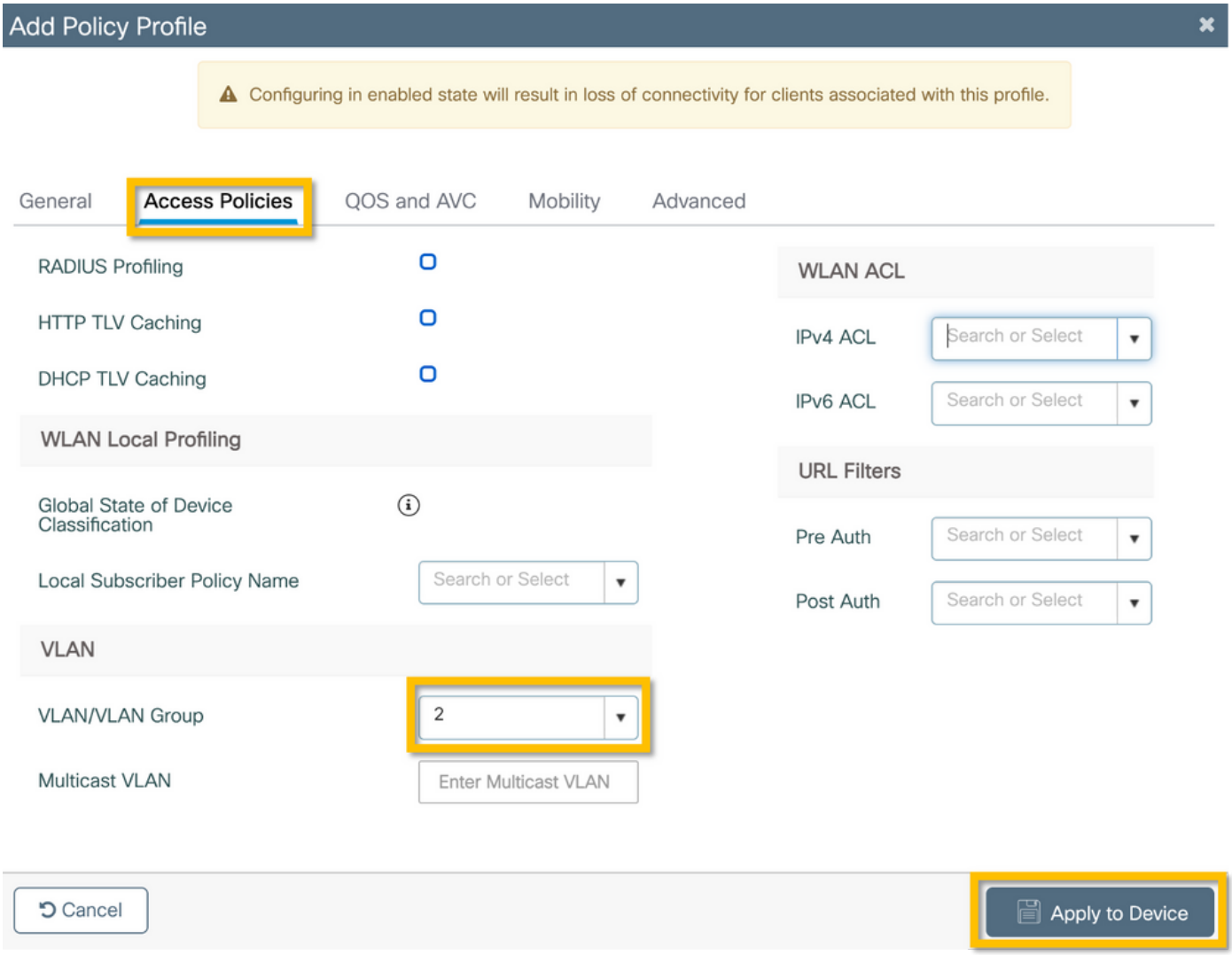


C9800 — 配置策略配置文件

步骤1.导航到**配置>标记和配置文件>策略**，然后单击**+添加**，然后输入策略配置文件名称和说明。启用策略，并禁用集中交换、DHCP和关联，因为企业用户流量在AP进行本地交换，如图所示。



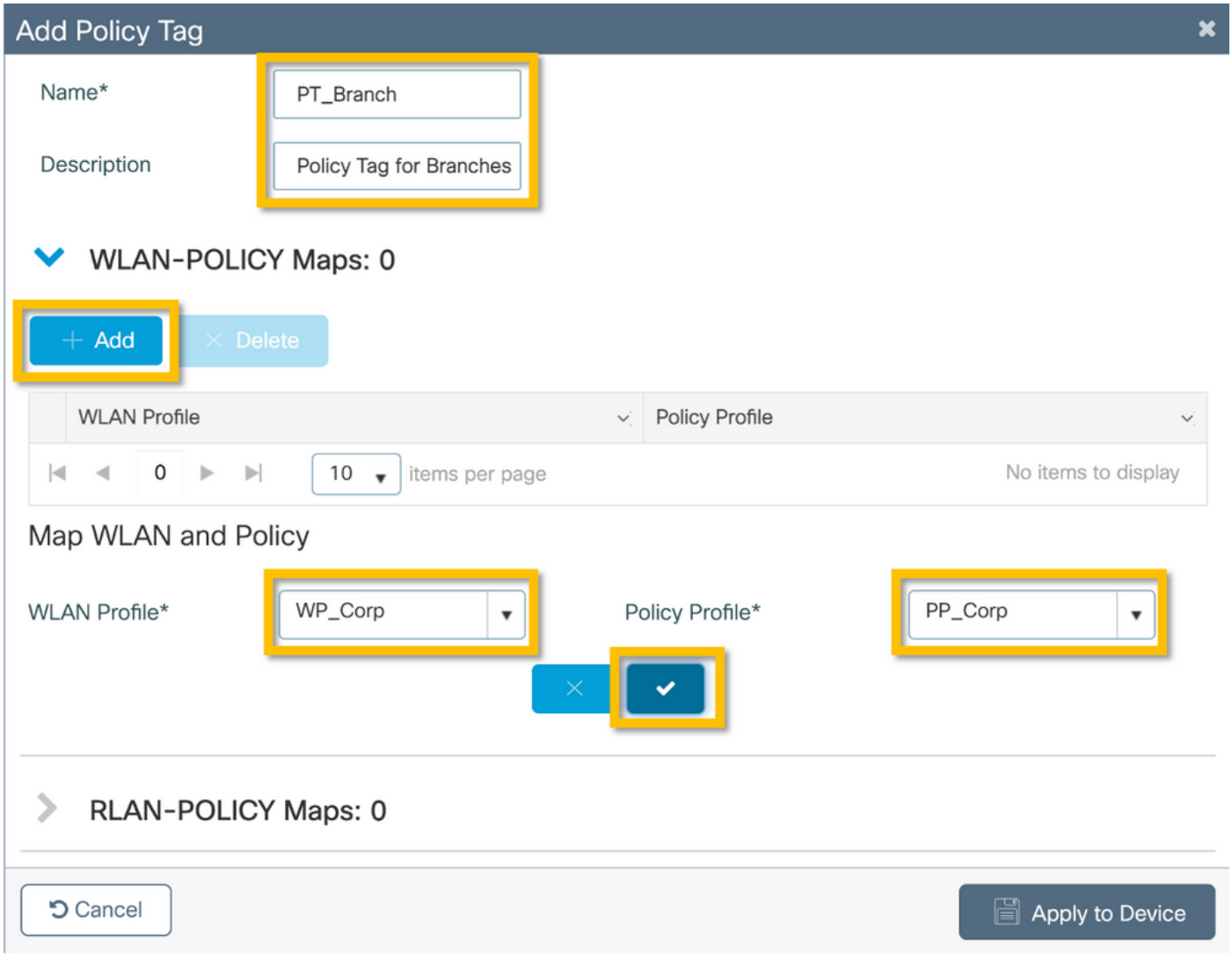
步骤2.导航到**访问策略**选项卡，并手动输入要在分支机构用于企业用户流量的VLAN的ID。无需在C9800本身上配置此VLAN。必须在Flex配置文件中对其进行配置，详细信息将进一步说明。请勿从下拉列表中选择VLAN名称(请参阅Cisco Bug ID CSCvn48234 了解更多信息)。 单击**Apply to Device**按钮，如下图所示。



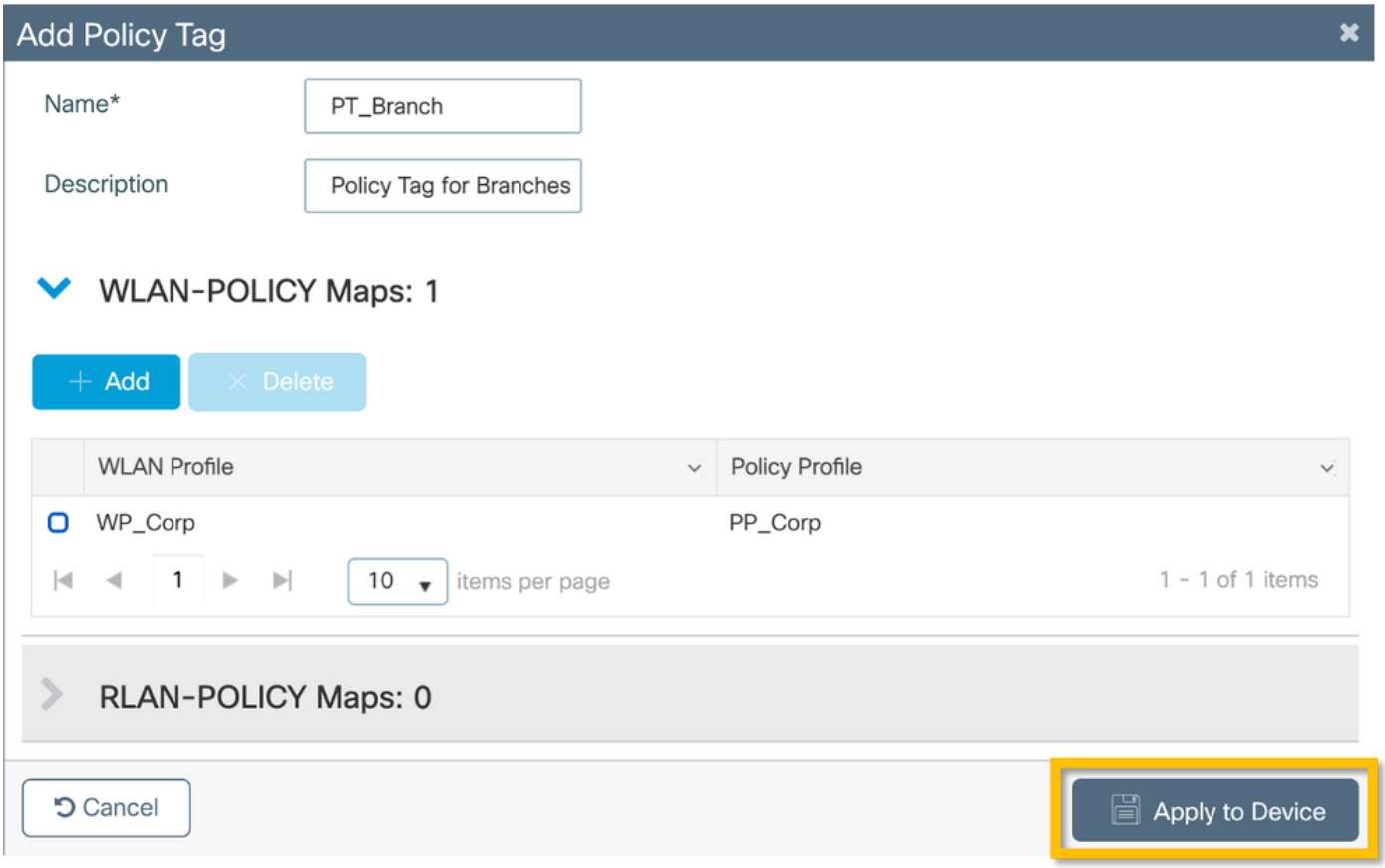
C9800 — 配置策略标记

创建WLAN配置文件(WP_Corp)和策略配置文件(PP_Corp)后，必须相应地创建策略标记以将这些WLAN和策略配置文件绑定在一起。此策略标记应用于接入点。将此策略标记分配给接入点，以触发这些接入点的配置，从而在其上启用所选SSID。

步骤1.导航到**配置>标记和配置文件>标记**，选择**策略**选项卡，然后单击**+添加**。输入策略标记名称和说明。点击**WLAN-POLICY Maps**下的**+Add**。选择之前创建的WLAN配置文件和策略配置文件，然后单击复选标记按钮，如图所示。



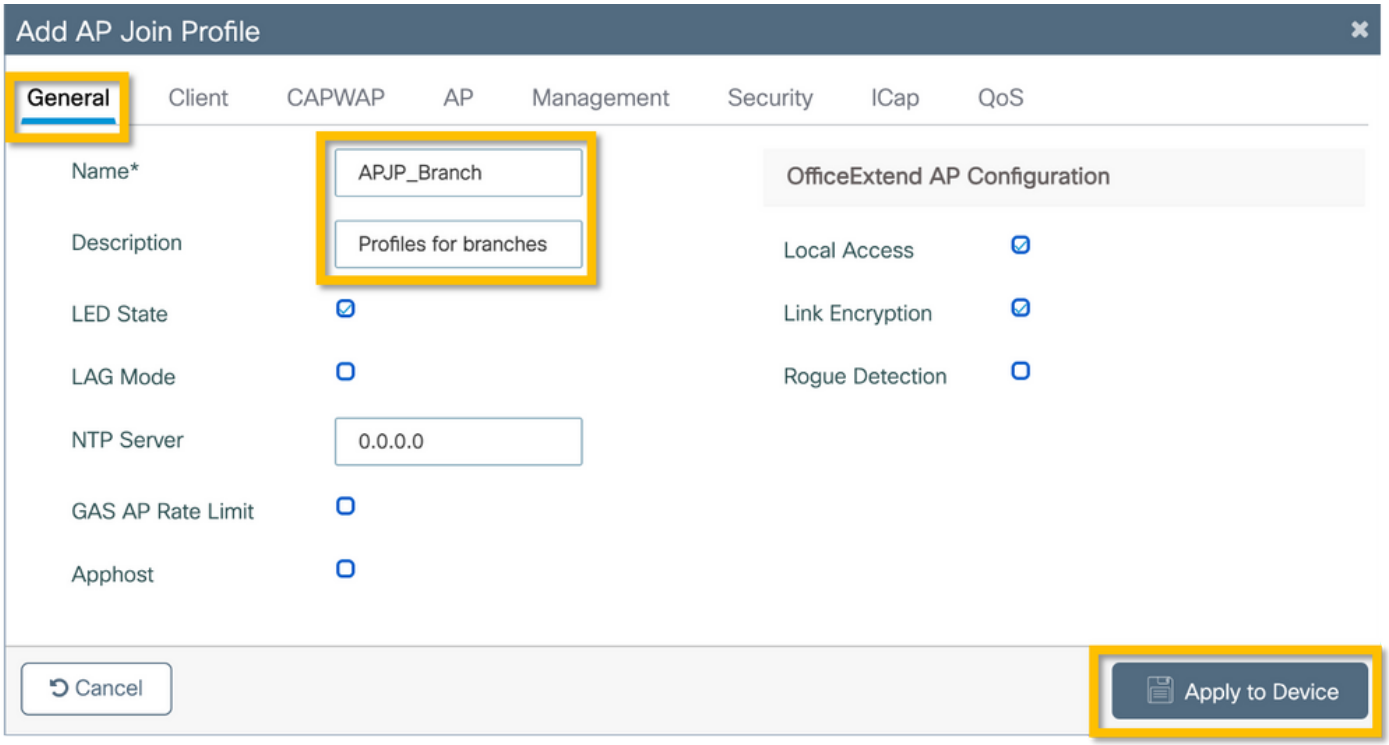
步骤2.如图所示，验证并点击Apply to Device按钮。



C9800 - AP加入配置文件

AP加入配置文件和Flex配置文件需要配置并分配到具有站点标记的接入点。每个分支必须使用不同的站点标记，才能支持一个分支内的802.11r快速过渡(FT)，同时限制客户端PMK在该分支的AP之间的分配。在多个分支之间不要重复使用同一站点标记。配置AP加入配置文件。如果所有分支都类似，您可以使用单个AP加入配置文件；如果某些配置的参数必须不同，则可以创建多个配置文件。

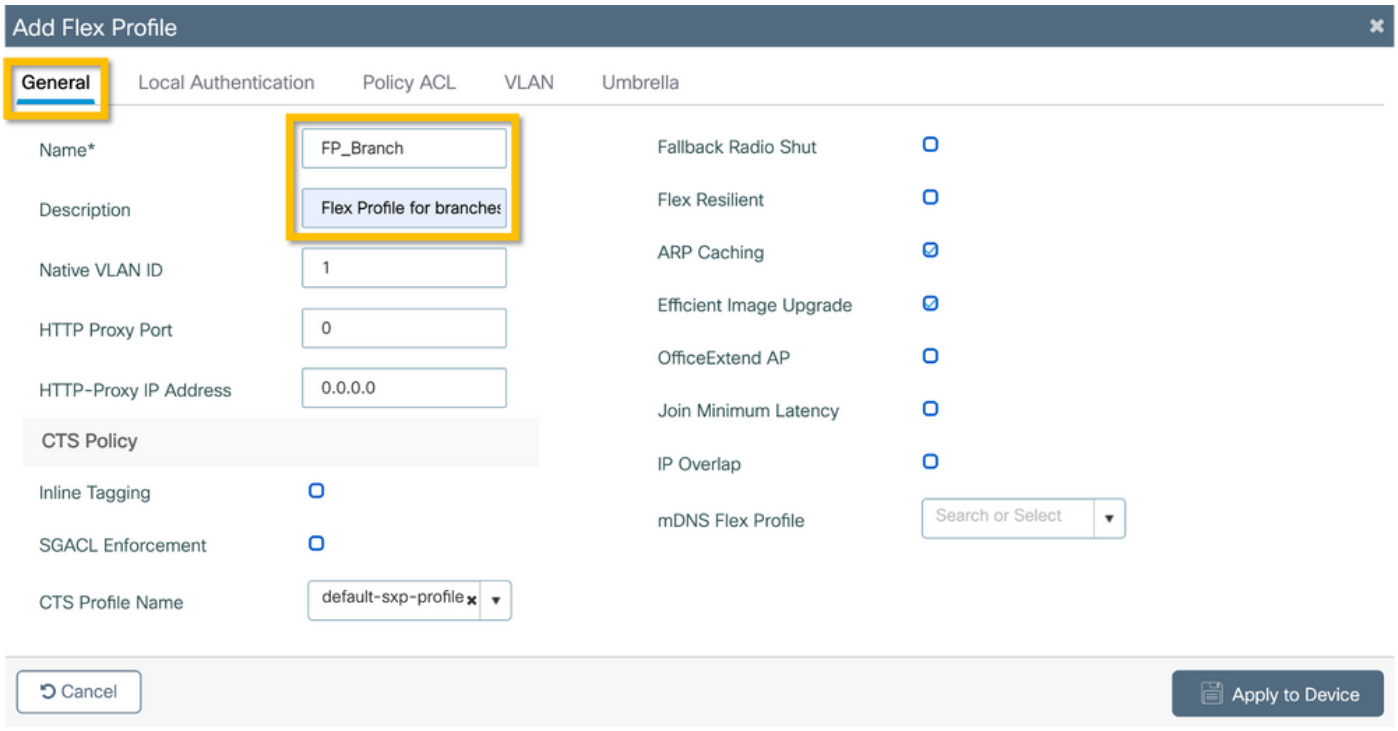
步骤1.导航到**配置>标记和配置文件> AP加入**，然后单击**+添加**。输入AP加入配置文件的名称和说明。单击**Apply to Device**按钮，如下图所示。



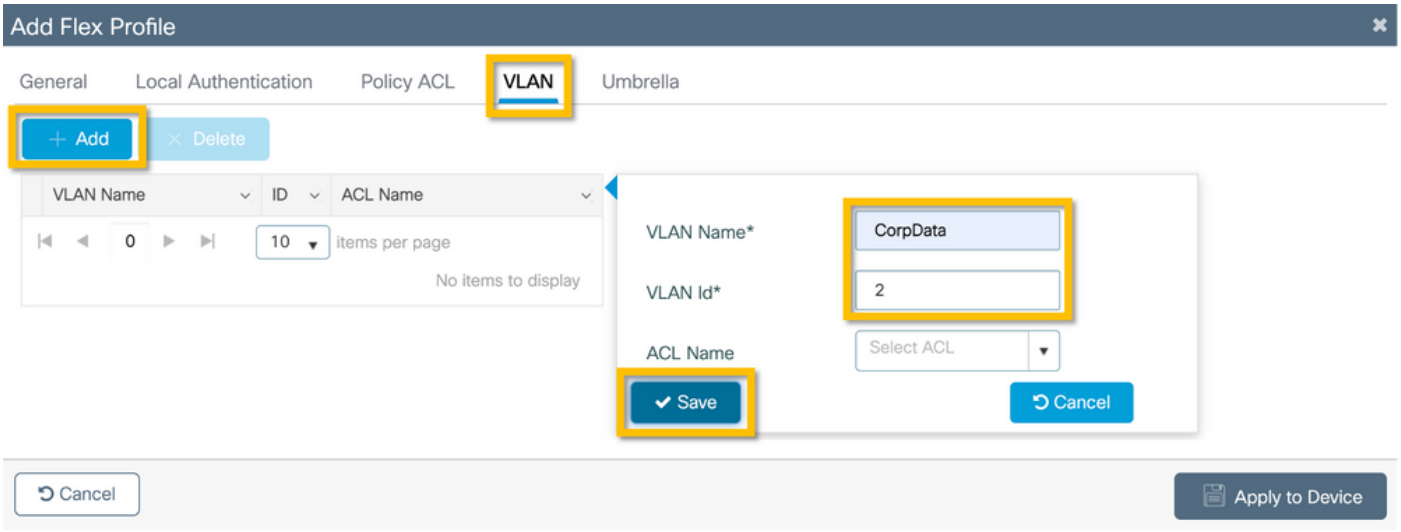
C9800 - Flex配置文件

现在配置Flex配置文件。同样，如果所有分支类似，并且具有相同的VLAN/SSID映射，则可以使用单个配置文件。或者，如果某些配置的参数（如VLAN分配）不同，您可以创建多个配置文件。

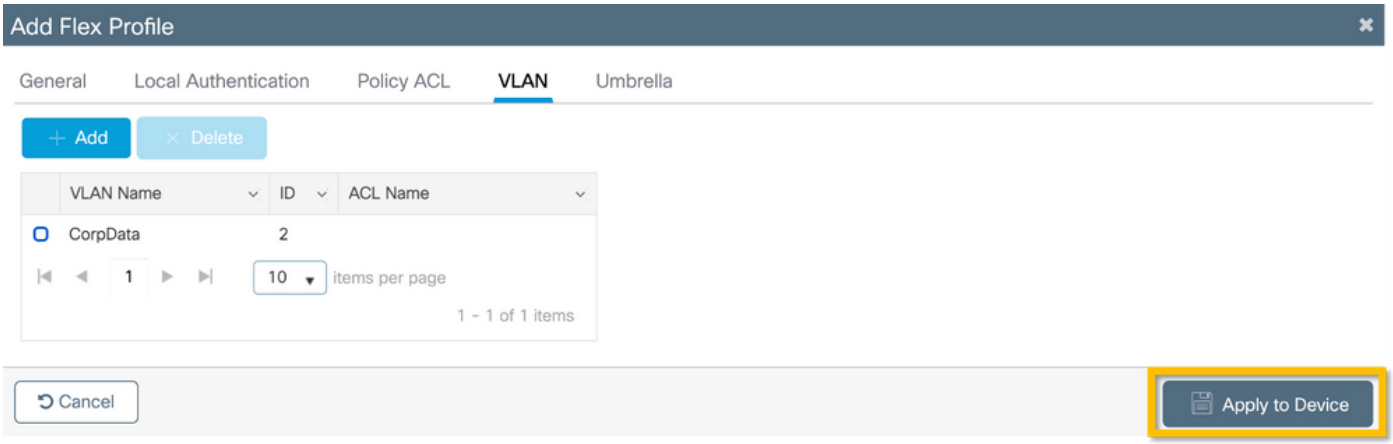
步骤1.导航到**配置>标签和配置文件> Flex**，然后点击**+添加**。输入Flex配置文件的名称和说明。



步骤2.导航到**VLAN**选项卡，然后单击**+Add**。输入分支机构本地VLAN的VLAN名称和ID，AP必须使用这些VLAN在本地交换企业用户流量。单击**Save**按钮，如下图所示。



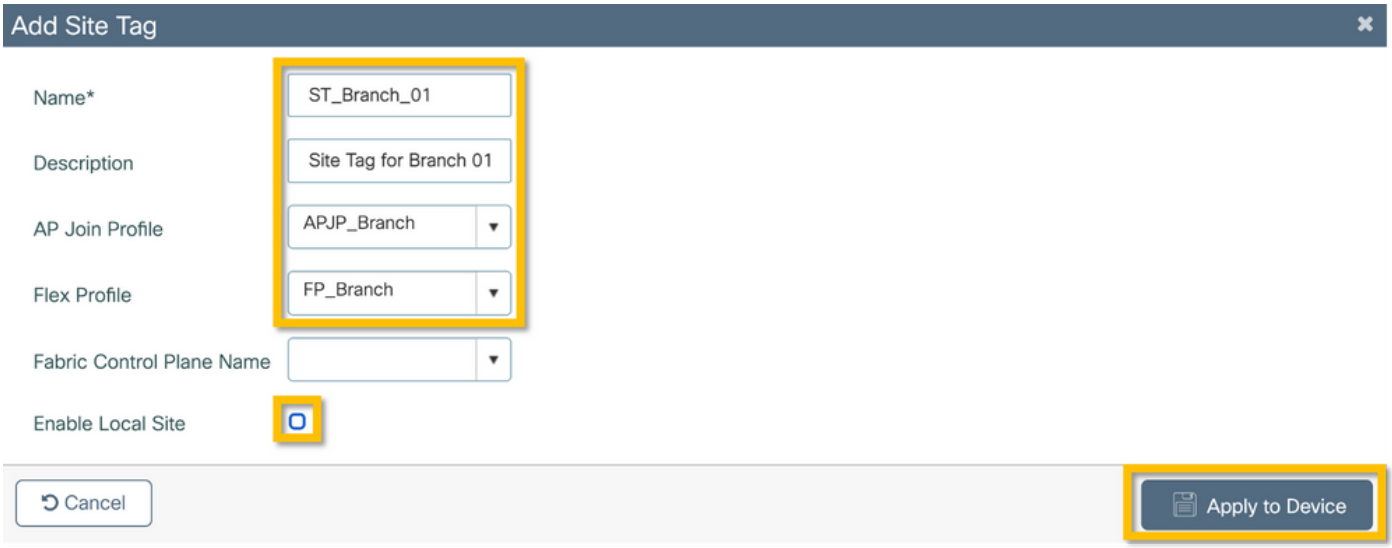
步骤3.如图所示，验证并点击**Apply to Device**按钮。



C9800 — 站点标记

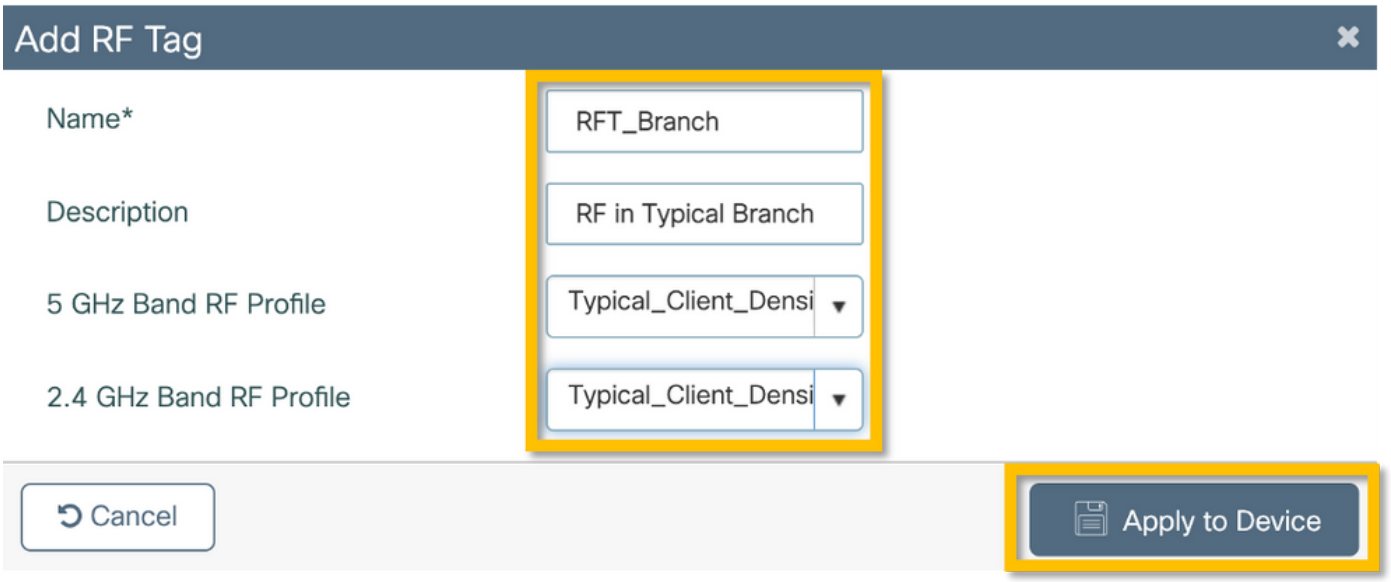
站点标记用于将加入配置文件和Flex配置文件分配到接入点。如前所述，每个分支必须使用不同的站点标记以支持分支内的802.11r快速过渡(FT)，但仅限制客户端PMK在该分支的AP之间的分配。在多个分支之间不要重复使用同一站点标记。

步骤1.导航到**配置>标记和配置文件>标记**，选择**站点**选项卡，然后单击**+添加**。输入站点标签名称和说明，选择创建的AP加入配置文件，取消选中**启用本地站点**框，最后选择之前创建的Flex配置文件。取消选中**Enable Local Site**框以将接入点从**Local Mode**更改为**FlexConnect**。最后，单击**Apply to Device**按钮，如下图所示。



C9800 - RF标记

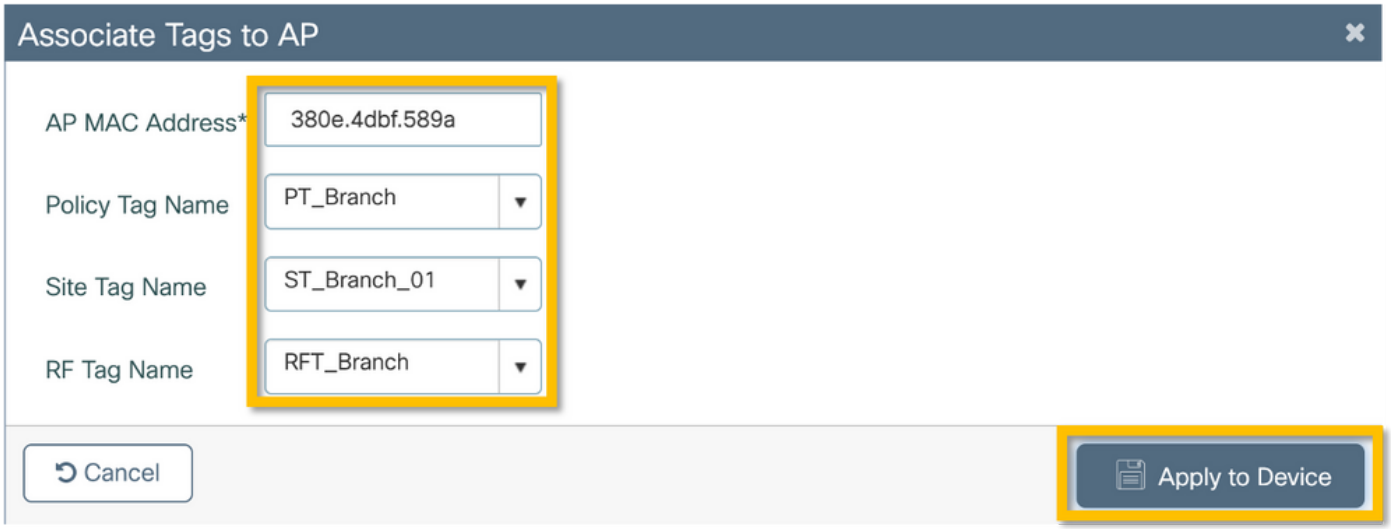
步骤1.导航到**配置>标记和配置文件> 标记**，选择**RF**选项卡，然后单击**+添加。输入RF标记的名称和说明。从下拉菜单中选择系统定义的**RF配置文件。单击**Apply to Device**按钮，如下图所示。



C9800 — 为AP分配标记

现在创建包含配置接入点所需的各种策略和配置文件的标记，我们必须将它们分配给接入点。本节介绍如何根据接入点的以太网MAC地址手动执行分配给该接入点的静态标记。对于产品生产环境，建议使用Cisco DNA Center AP PNP工作流程，或使用9800中提供的静态批量CSV上传方法。

步骤1.导航到**配置>标记和配置文件>标记**，选择**AP**选项卡，然后选择**静态**选项卡。单击**+Add**并输入AP MAC地址，然后选择以前定义的策略标记、站点标记和RF标记。单击**Apply to Device**按钮，如本图所示。



配置Aruba CPPM

Aruba ClearPass策略管理器服务器初始配置

Aruba clearpass通过OVF模板在ESXi服务器上部署，具有以下资源：

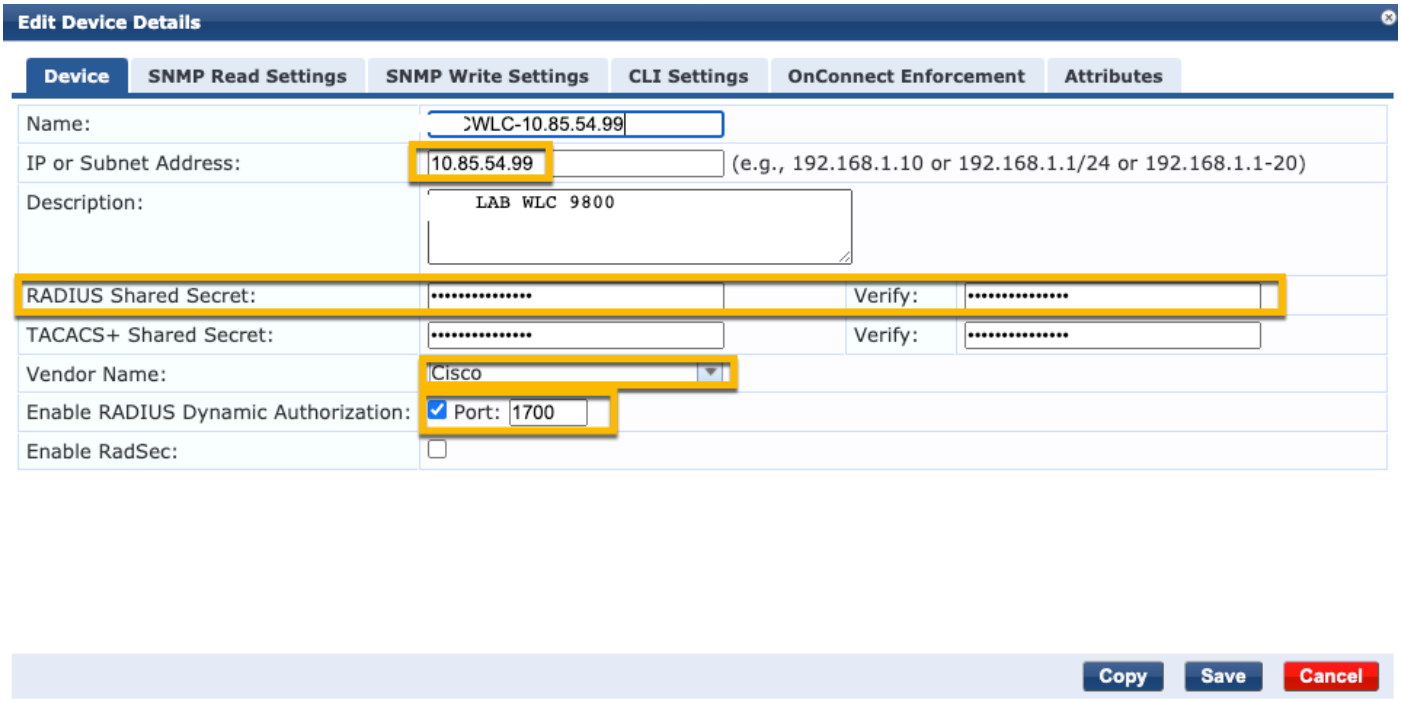
- 2个保留的虚拟CPU
- 6 GB RAM
- 80 GB磁盘（必须在初始虚拟机部署后手动添加，然后才能启动计算机）

应用许可证

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**接入和入网**

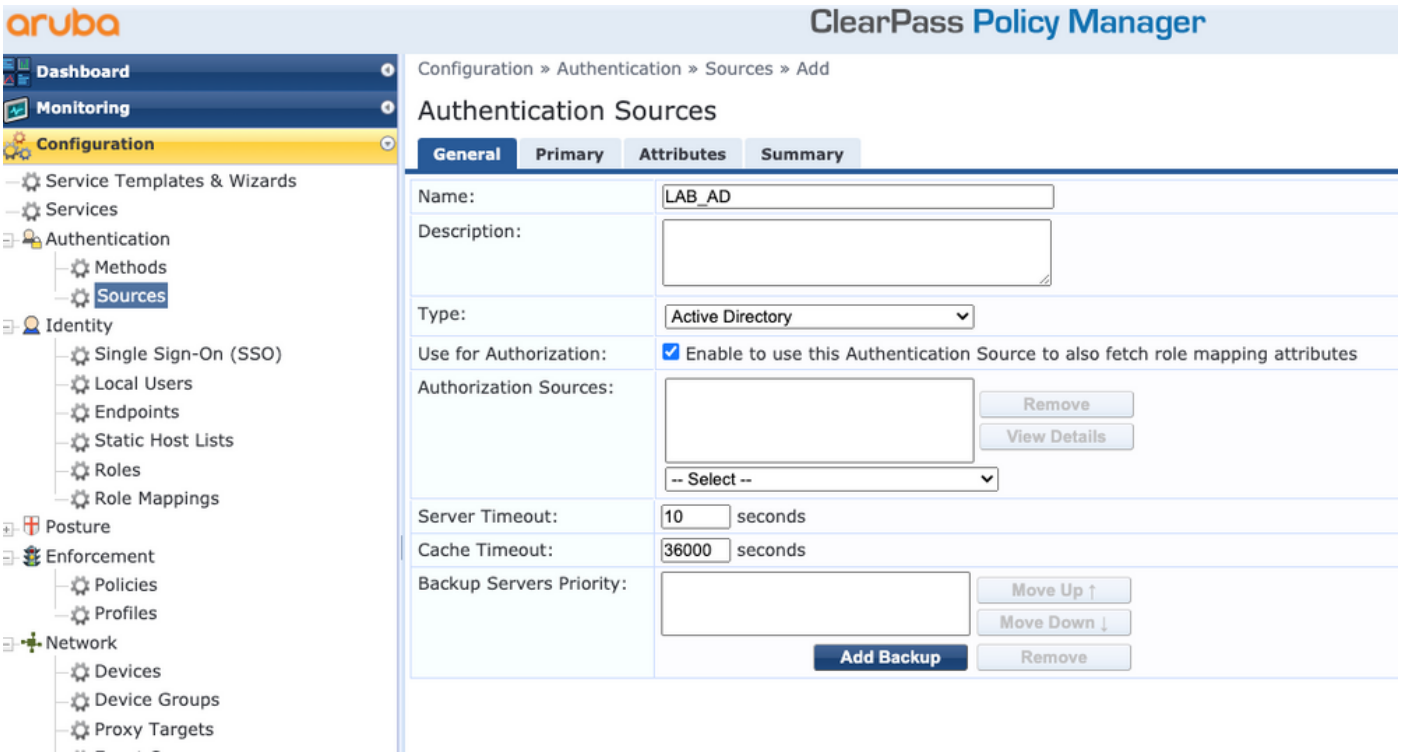
添加C9800无线控制器作为网络设备

导航到**配置>网络>设备>添加**，如下图所示。



配置CPPM以使用Windows AD作为身份验证源

导航到Configuration > Authentication > Sources > Add。选择类型:Active Directory从下拉菜单中，如此图所示。



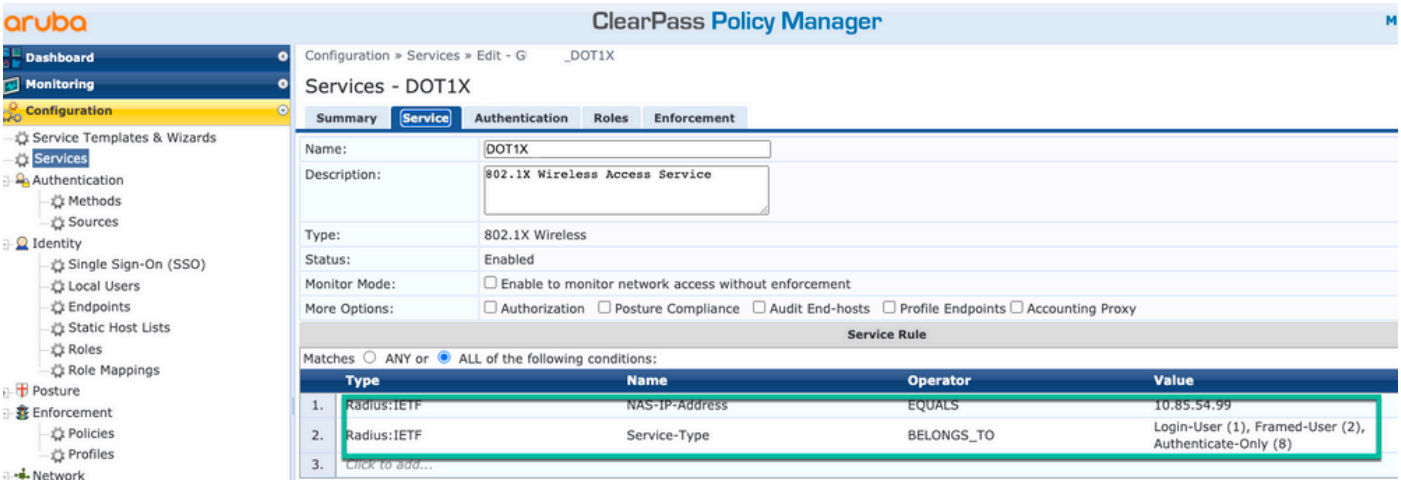
配置CPPM Dot1X身份验证服务

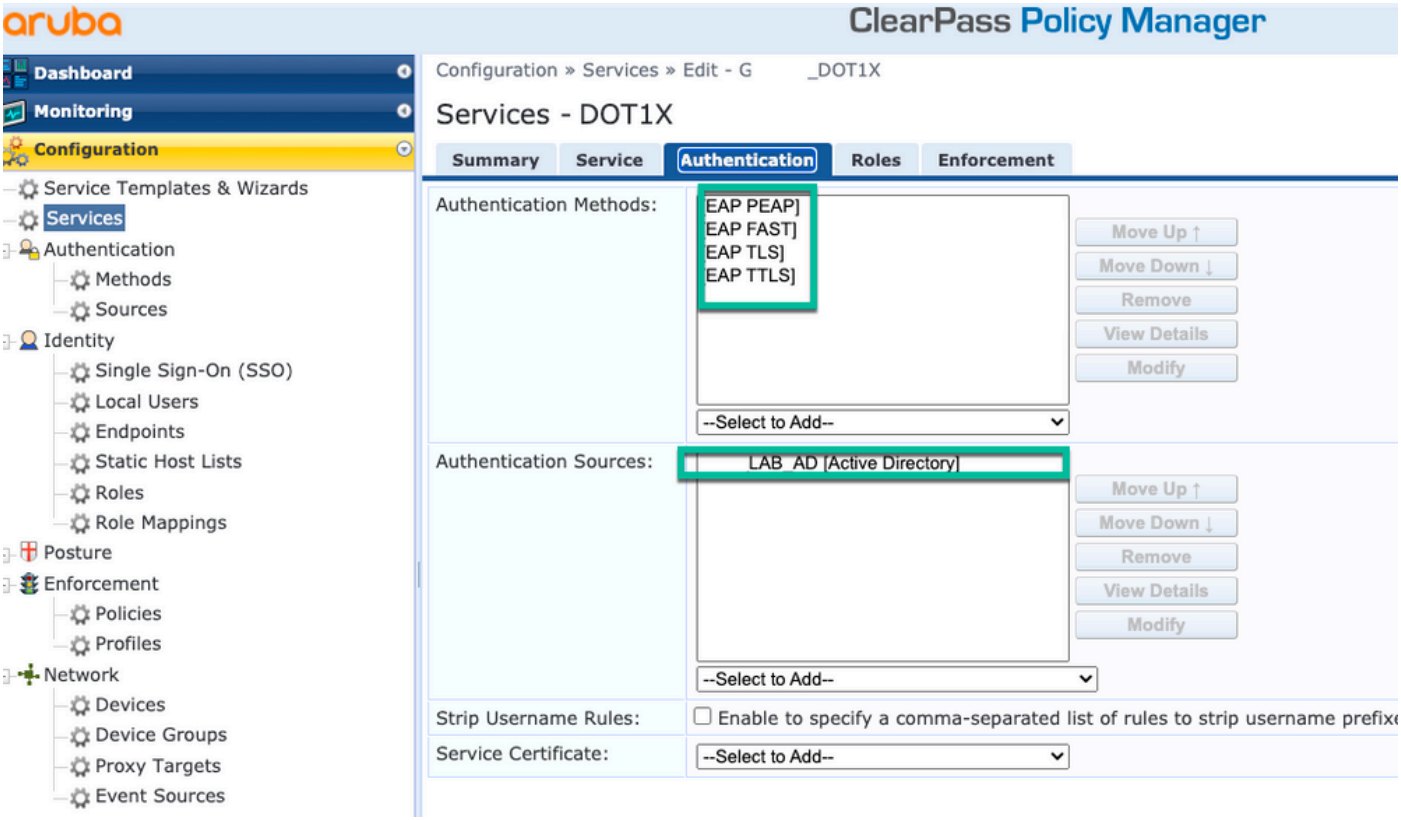
步骤1.创建匹配多个RADIUS属性的“服务”：

- Radius:IETF |名称：NAS-IP-Address |等于 | <IP ADDR>
- Radius:IETF |名称：服务类型 |等于 |1,2,8

步骤2.对于生产环境，建议匹配SSID名称而不是“NAS-IP-Address”，以便多WLC部署满足一个条件

。 Radius:Cisco:Cisco-AVPair | cisco-wlan-ssid | Dot1XSSID





验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

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）。