在思科企业无线接入点中配置RADIUS

目标

本文档旨在向您展示如何在思科业务无线(CBW)接入点(AP)中配置RADIUS。

适用设备 |固件版本

- 140AC(产品手册) | 10.4.1.0（下载最新）
- 145AC(产品手册) | 10.4.1.0（下载最新）
- 240AC(产品手册) | 10.4.1.0(下载最新版本)

简介

如果您希望在CBW AP中配置RADIUS，您已到达正确的位置！CBW AP支持最新的802.11ac Wave 2标准，以实现更高的性能、更高的接入和更高密度网络。它们提供行业领先的性能和高度安全可靠的无线连接，提供强大的移动最终用户体验。

远程身份验证拨入用户服务(RADIUS)是设备连接和使用网络服务的身份验证机制。它用于集中身份验证、授权和记帐目的。RADIUS服务器通过输入的登录凭证验证用户的身份来规范对网络的访问。例如，大学校园中安装了公共Wi-Fi网络。只有拥有密码的学生才能访问这些网络。RADIUS服务器检查用户输入的密码，并根据需要授予或拒绝对无线局域网(WLAN)的访问权。

如果您已准备好在CBW AP上配置RADIUS，我们开始吧！

目录

在CBW AP上配置RADIUS

此切换部分突出显示初学者的提示。

登录

登录主AP的Web用户界面(UI)。为此，请打开Web浏览器并输入https://ciscobusiness.cisco。在继续之前，您可能会收到警告。输入您的凭证。您也可以通过在Web浏览器中输入https://[ipaddress]（主AP）来访问主AP。

工具提示

如果您对用户界面中的字段有疑问，请检查以下工具提示：

查找“展开主菜单”图标时遇到问题？

导航至屏幕左侧的菜单，如果未看到菜单按钮，请单击此图标打开侧栏菜单。 

思科业务应用

这些设备具有与Web用户界面共享某些管理功能的配套应用。并非Web用户界面中的所有功能都可在应用中使用。

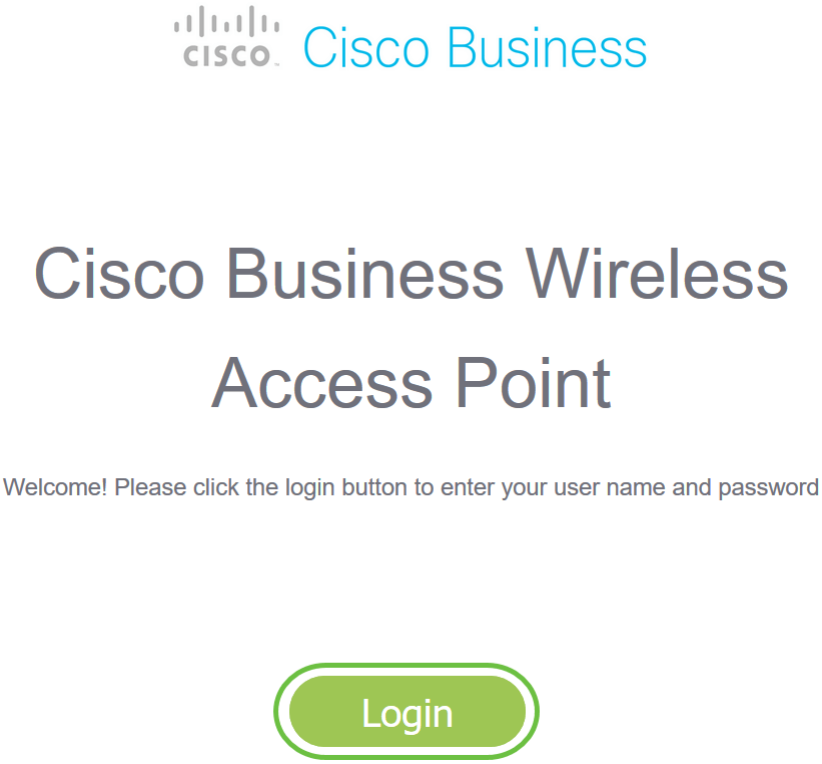
下载iOS应用 下载Android应用

常见问题

如果您仍有未回答的问题，您可以查看我们的常见问题文档。 常见问题

第 1 步

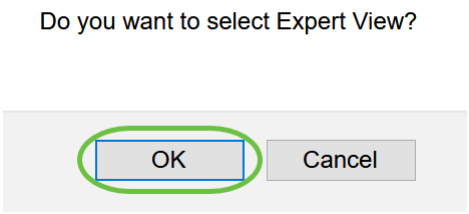
使用有效的用户名和密码登录CBW AP。



步骤 2

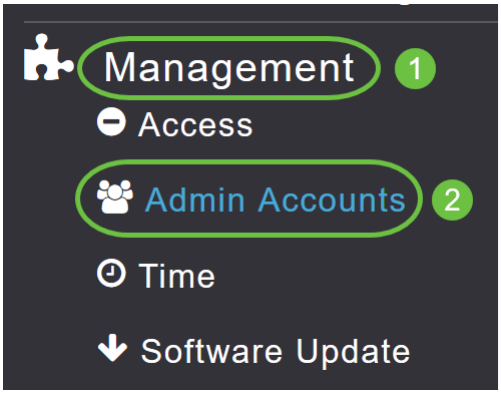
单击Web用**户界**面(UI)顶部的双向箭头符号以切换到*专家视图*。

您将看到以下弹出屏幕。单击**确定**继续。



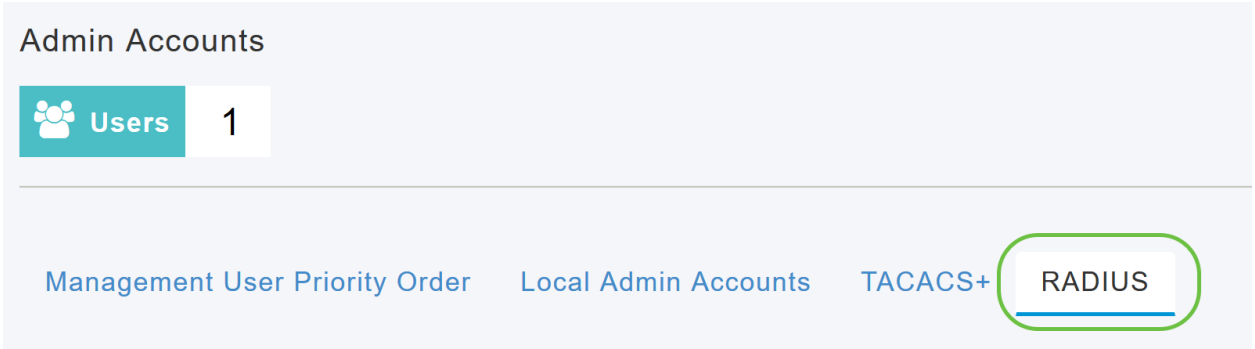
步骤 3

导航至**Management > Admin Accounts**。



步骤 4

要添加RADIUS服务器，请单击RADIUS**选项**卡。

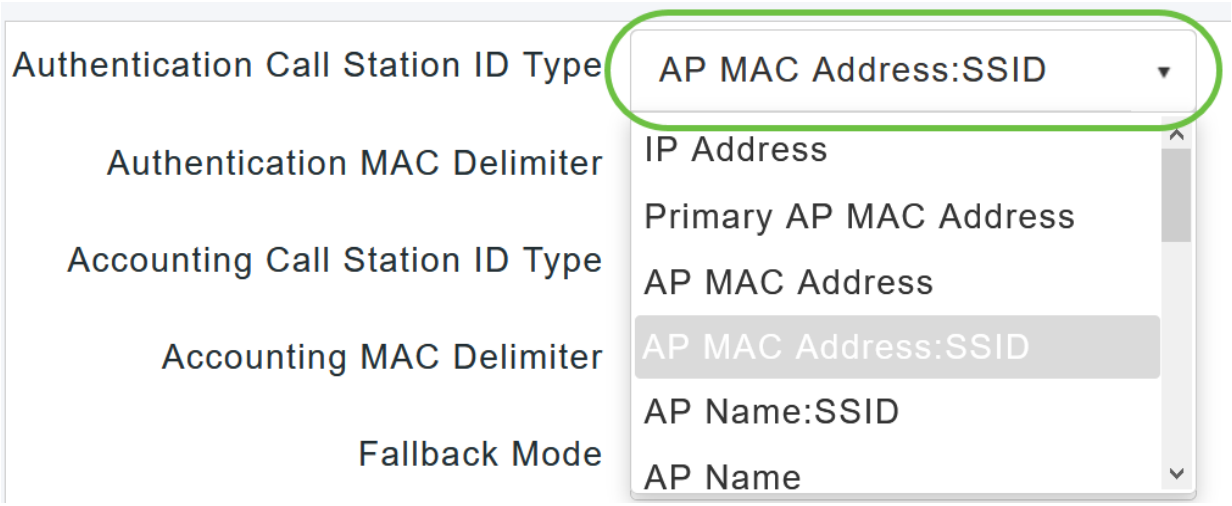


步骤 5

从*Authentication Call Station ID Type*下拉列表中，在Access-Request消息中选择发送到RADIUS服务器的选项。可以使用以下选项：

- *IP Address*
- *主AP MAC地址*
- *AP MAC地址*
- *AP MAC地址：SSID*
- *AP名称：SSID*
- *AP 名称*
- *AP组*
- *弹性组*
- *AP位置*
- *VLAN ID*

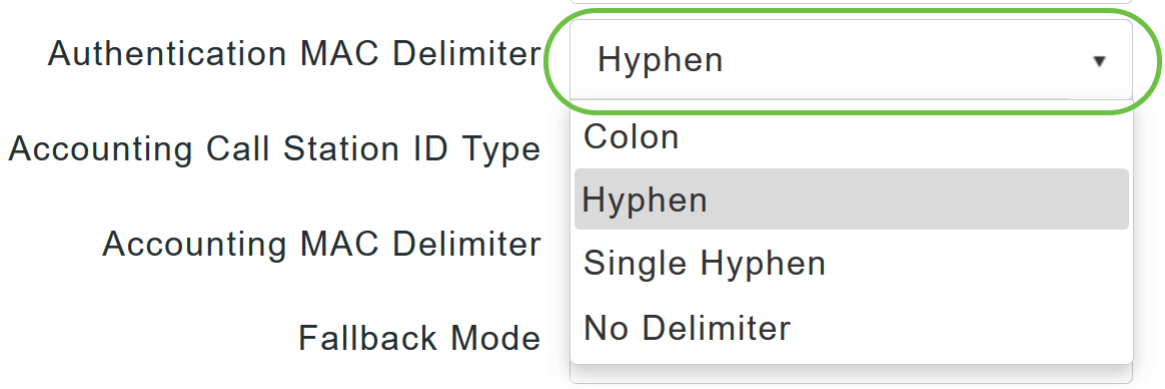
- *AP以太网MAC地址*
- *AP以太网MAC地址：SSID*
- *AP标签地址*
- *AP标签地址：SSID*
- *AP MAC:SSID AP组*
- *AP以太网MAC:SSID AP组*



步骤 6

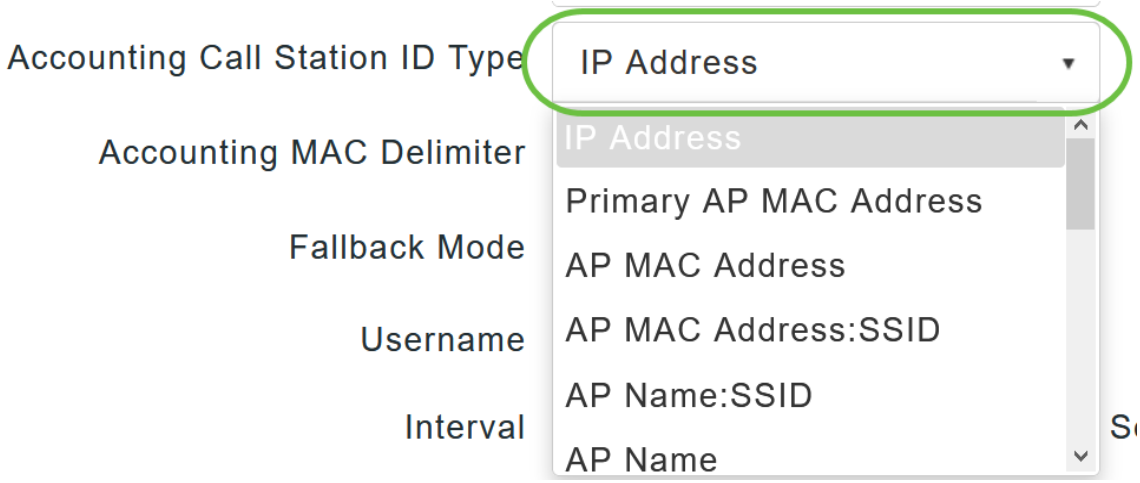
从下拉列*表中选择*Authentication MAC Delimiter。选项有：

- *冒号*
- *连字符*
- *单连字符*
- *无分隔符*



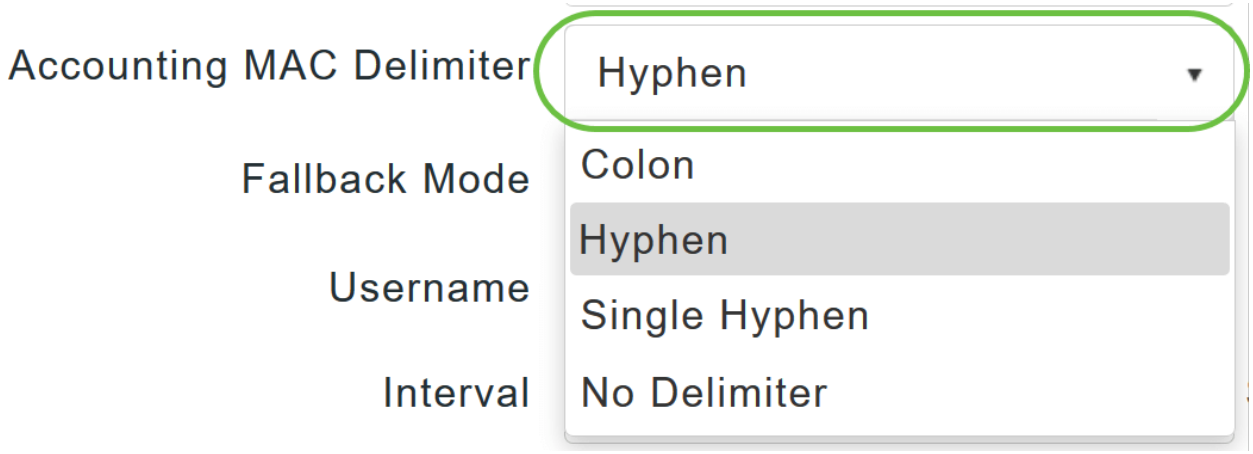
步骤 7

从下拉*列表中选择Accounting Call Station ID Type*。



步骤 8

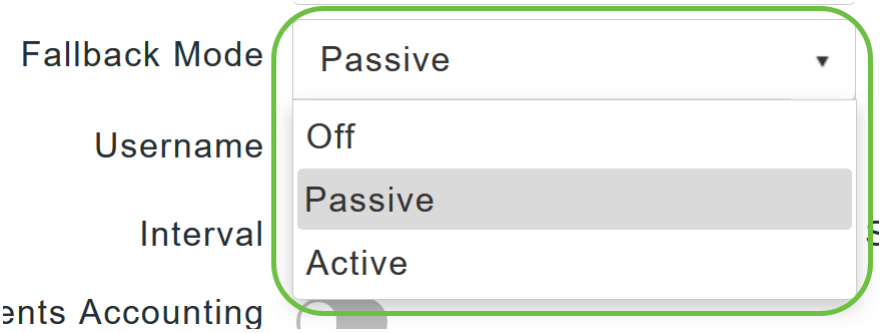
从下拉列*表中选择Accounting MAC Delimiter*。



步骤 9

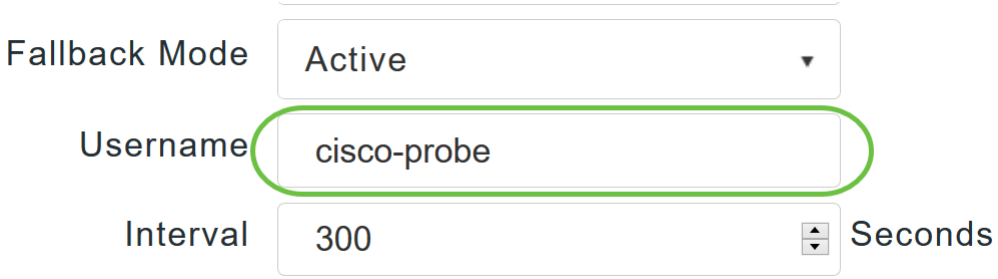
从下拉列表*中指*定RADIUS服务器回退模式。它可以是以下其中一项：

- *关闭* — 禁用RADIUS服务器回退。这是默认值。
- *被动* — 使主AP从可用备份服务器恢复到优先级较低的服务器，而不使用无关的探测消息。主AP会在一段时间内忽略所有非活动服务器，并在需要发送RADIUS消息时稍后重试。
- *活动* — 通过使用RADIUS探测消息主动确定标记为非活动的服务器是否重新联机，使主AP从可用备份服务器恢复到优先级较低的服务器。主AP会忽略所有活动RADIUS请求的所有非活动服务器。一旦主服务器收到来自恢复的ACS服务器的响应，活动回退RADIUS服务器将不再向请求活动探测身份验证的服务器发送探测消息。



步骤 10

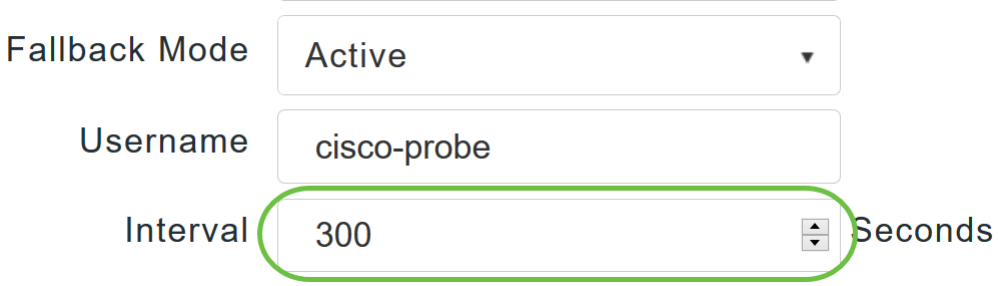
如果启用了*Active Fallback模式*，请在Username字段中输入要在非活动服务器探测中发送的*名称*。



最多可输入16个字母数字字符。默认值为**cisco-probe**。

步骤 11

如果启用了*活动回退模式*，请在“间隔”字段中输入探测间隔值(以秒为单位)。该间隔在被动模式下用作非活动时间，在主动模式下用作探测间隔。

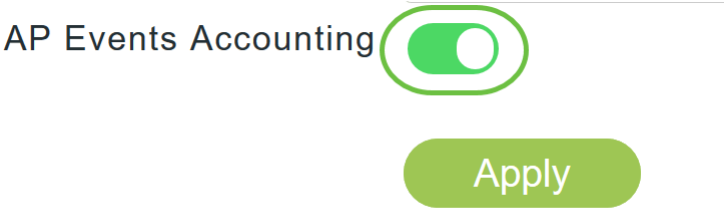


有效范围为180至3600秒，默认值为**300**秒。

步骤 12

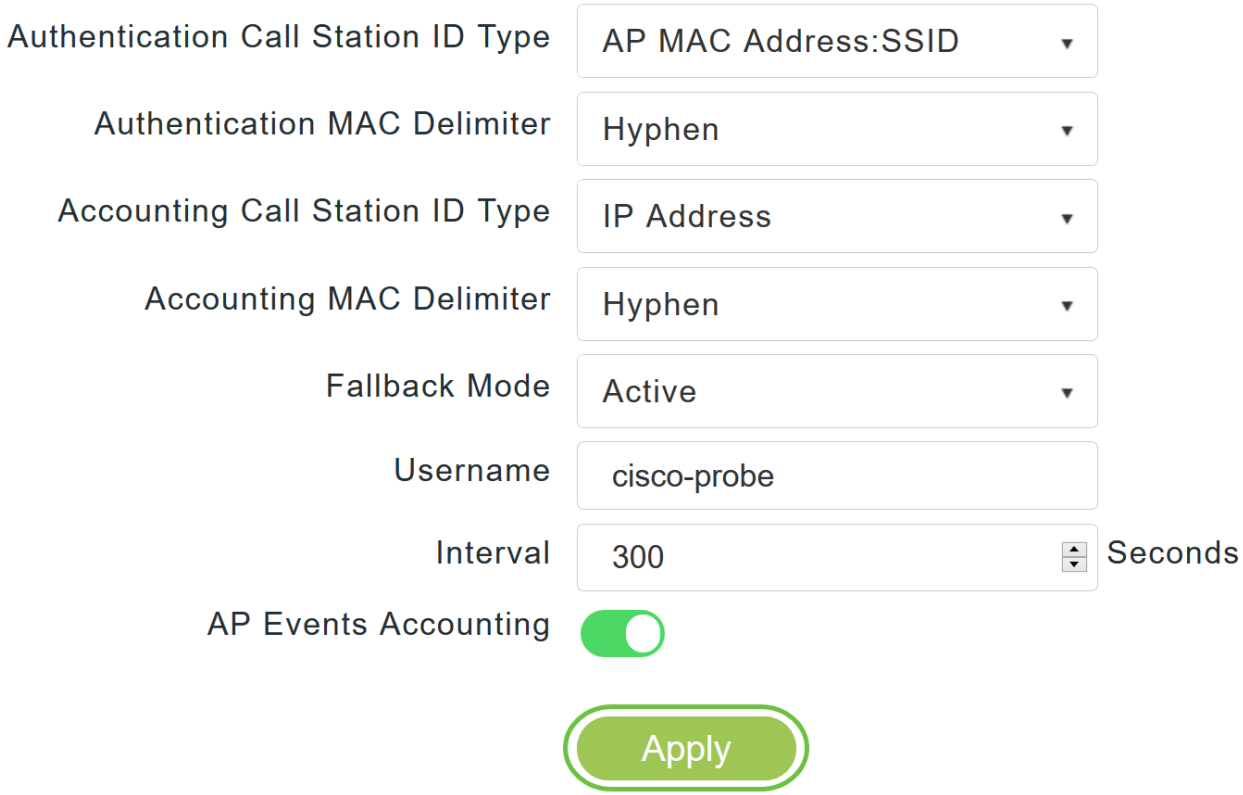
启用AP *Events Accounting滑块*按钮以激活向RADIUS服务器发送记帐请求。

在网络问题期间，AP会加入/取消主AP。启用此选项可确保监控这些事件并将记帐请求发送到RADIUS服务器以帮助您检测网络问题。



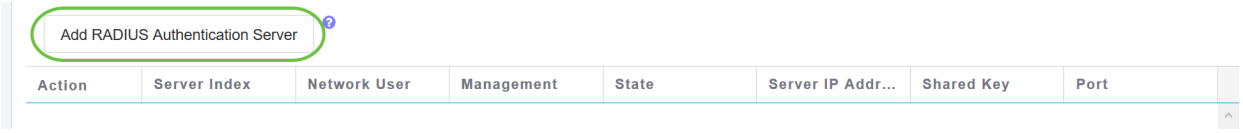
步骤 13

单击 **Apply**。



步骤 14

要配置RADIUS身份验证服务器，请点击**添加RADIUS身份验证服务器**。

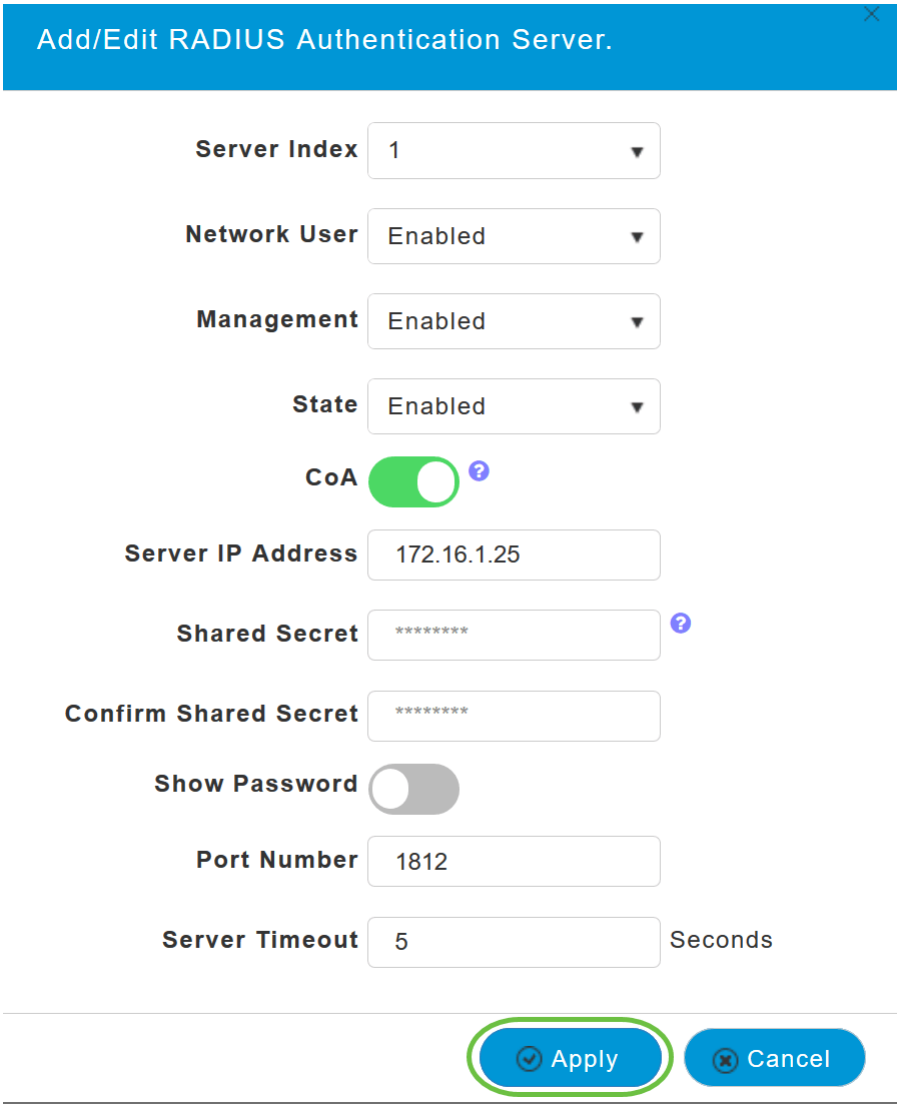


步骤 15

在“*添加/编辑RADIUS身份*验证”弹出窗口中，配置以下内容：

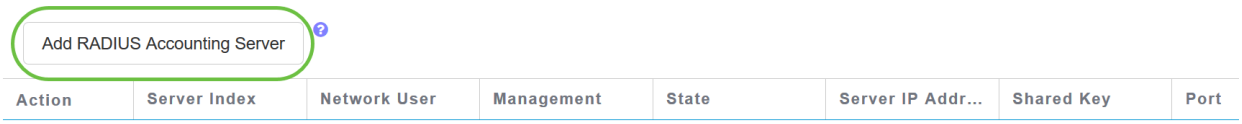
- *服务器索*引 — 选择1到6
- *网络用户* — 启用状态。默认情况下，此选项为Enabled
- *管理* — 启用状态。默认情况下，此选项为Enabled
- *状态* — 启用状态。默认情况下，此选项为Enabled
- *CoA* — 通过移动滑块按钮可以选择启用此选项
- *服务器IP地址* — 输入RADIUS服务器的IPv4地址
- *共享密*钥 — 输入共享密钥
- *Port Number* — 输入用于与RADIUS服务器通信的端口号。
- *服务器超时* — 输入服务器超时

单击 **Apply**。



步骤 16

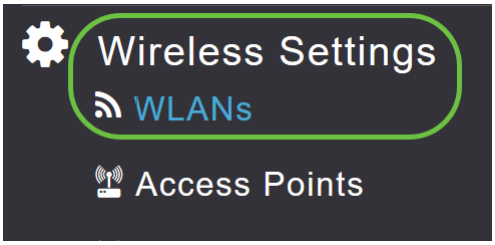
要添加*RADIUS记帐服务器*，您将按照步骤15中的步骤执行，因为页面包含类似的字段。



配置WLAN

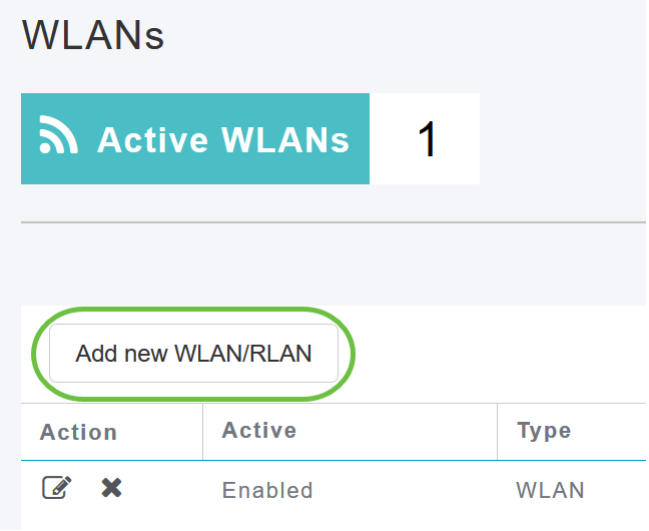
第 1 步

要配置要使用RADIUS处理WPA2身份验证的WLAN，请导航至“无线设置”>“WLAN”。



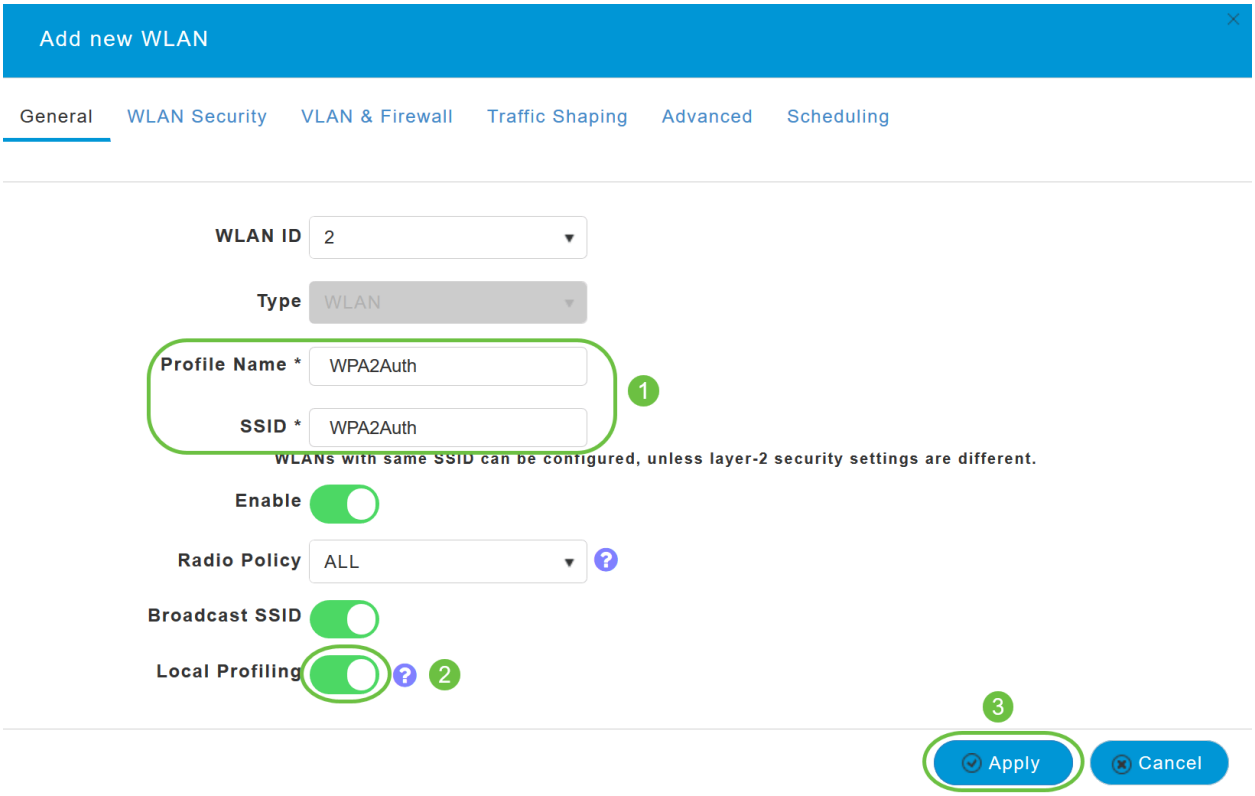
步骤 2

单击“**Add New WLAN/RLAN**”。



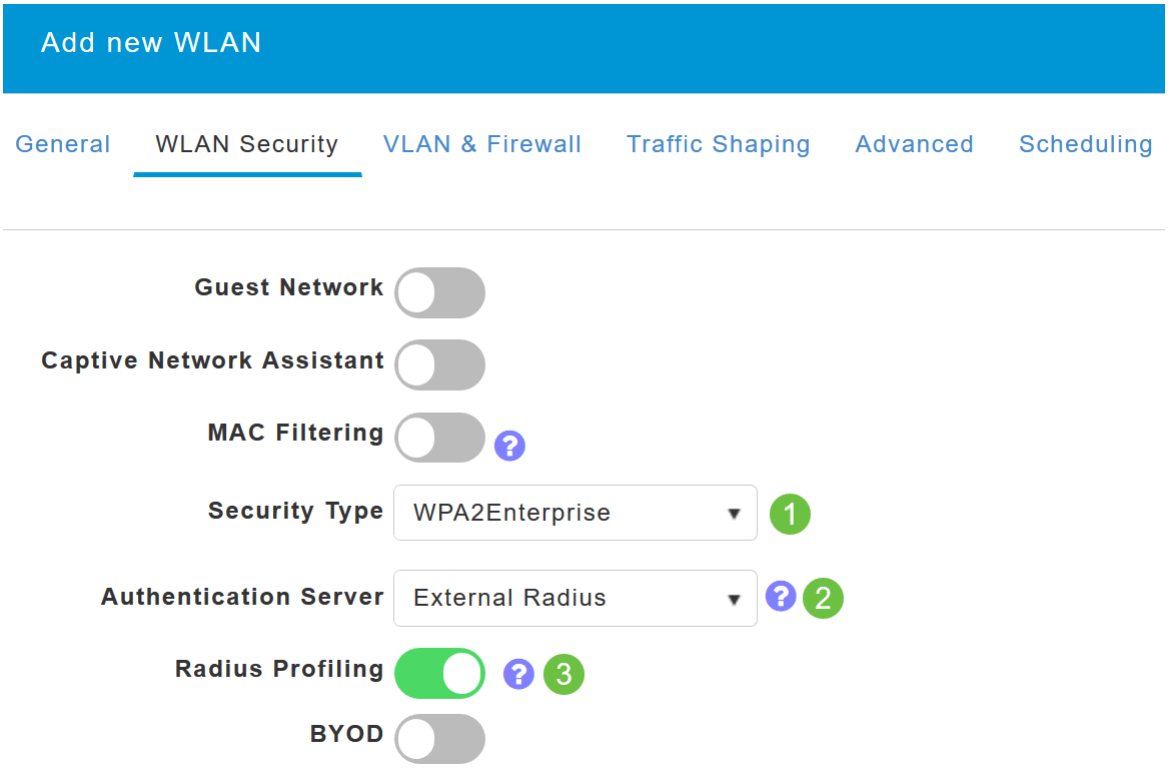
步骤 3

在“常规”选项卡中，输入“*配置文件名称*”。*SSID*字段将自动填充。您可以选择启用本*地分析*。单击**Apply**。



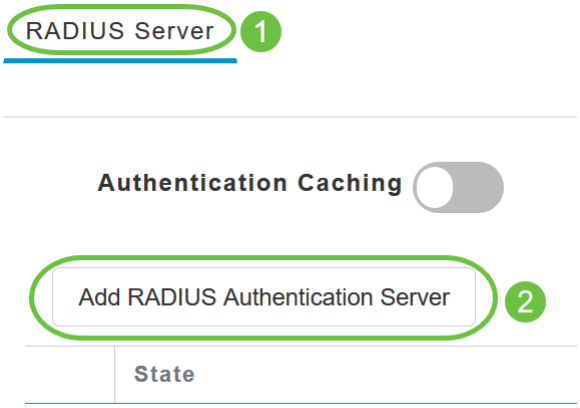
步骤 4

导航至WLAN*安全选*项卡。从“*安全类型*”下拉菜单中，选**择WPA2Enterprise**。选择**External Radius**作为*身份验证服务器*。您可以选择启用*Radius分析*。



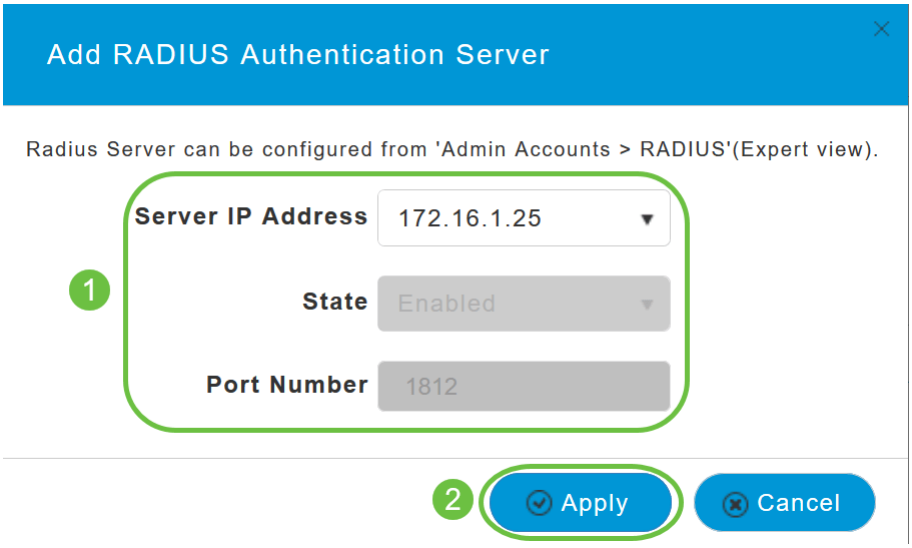
步骤 5

导航至*RADIUS服务器*部分。单击添**加RADIUS身份验证服务器。**



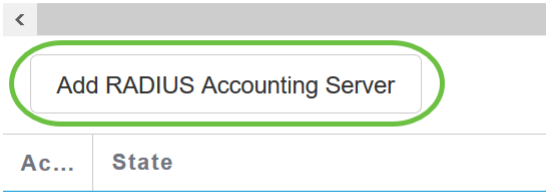
步骤 6

验证已配置的RADIUS身份验证服务器的详细信息，然后单击**Apply**。



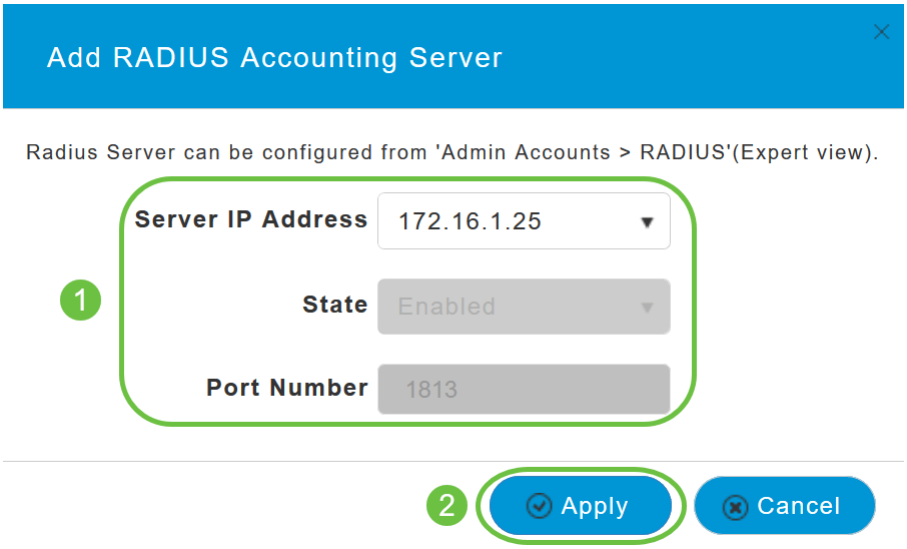
步骤 7

单击添加**RADIUS记帐服务器**。



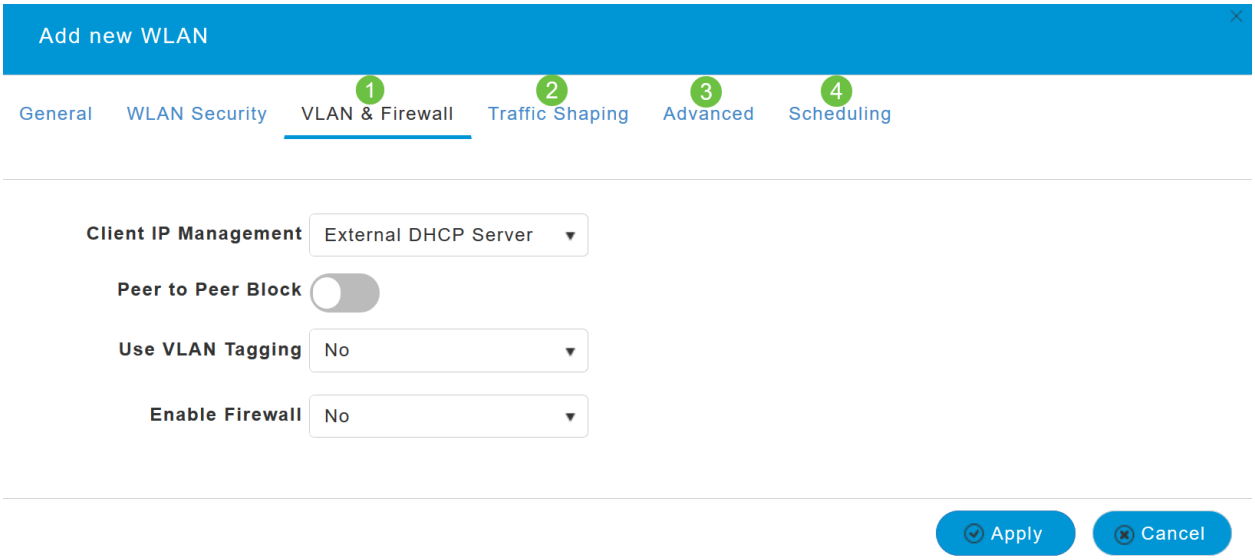
步骤 8

验证您配置的RADIUS记帐服务器的详细信息，然后单击**Apply**。



步骤 9

导航至*VLAN & Firewall*、*流量整形*、*高级*和*调度*选项卡，以根据您的网络首选项配置设置。单击**Apply**。

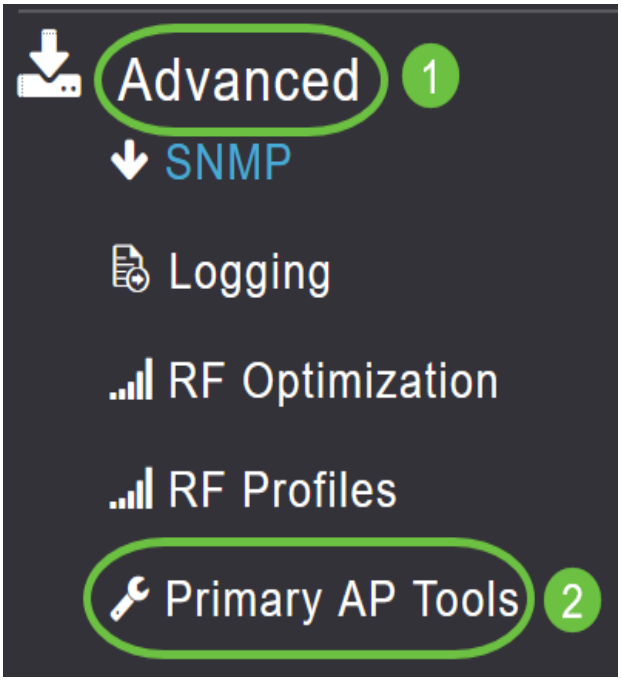


确认

要测试RADIUS身份验证，请执行以下操作：

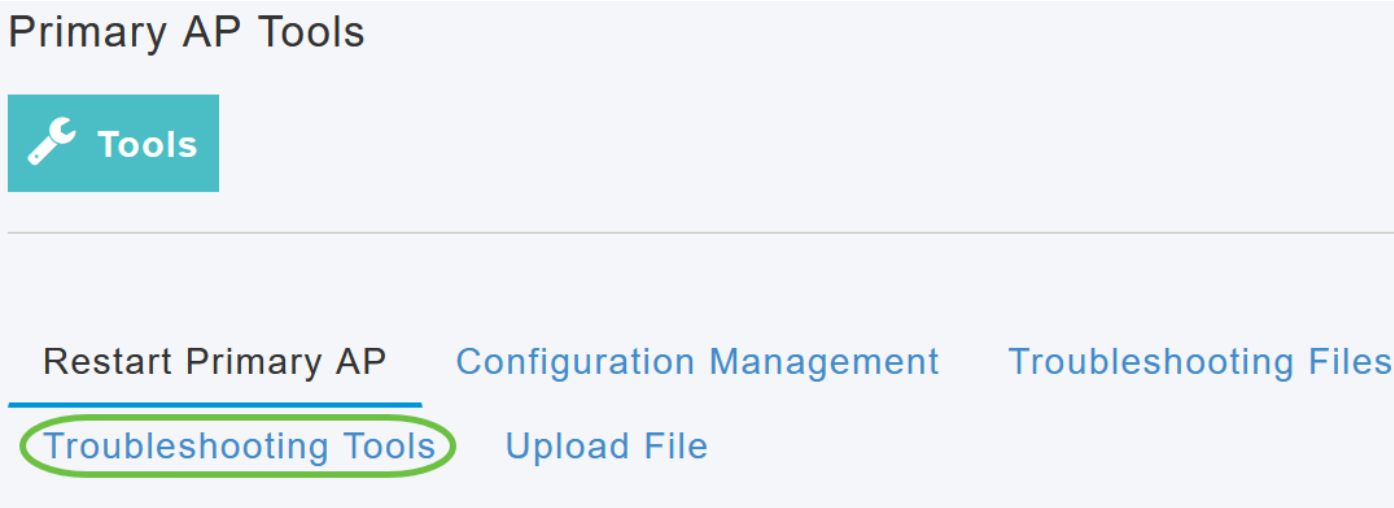
第 1 步

导航至**Advanced > Primary AP Tools**。



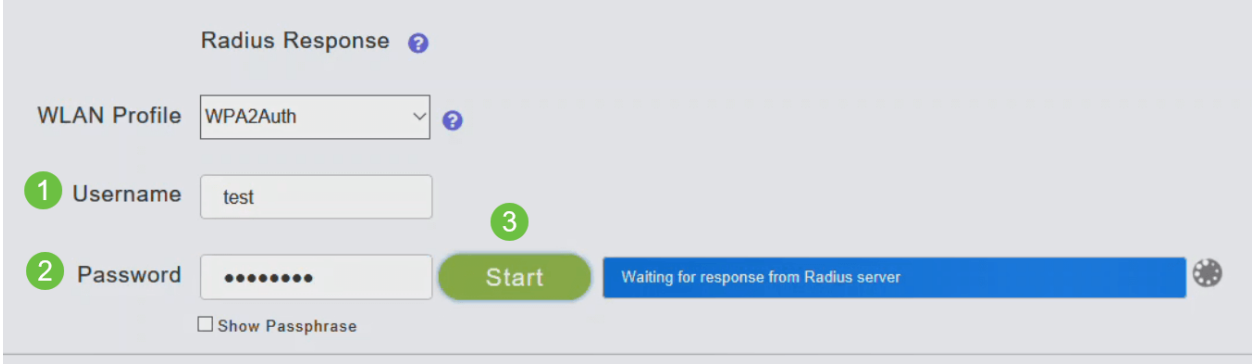
步骤 2

单击“Troubleshooting Tools(**故障排除工具**)”。



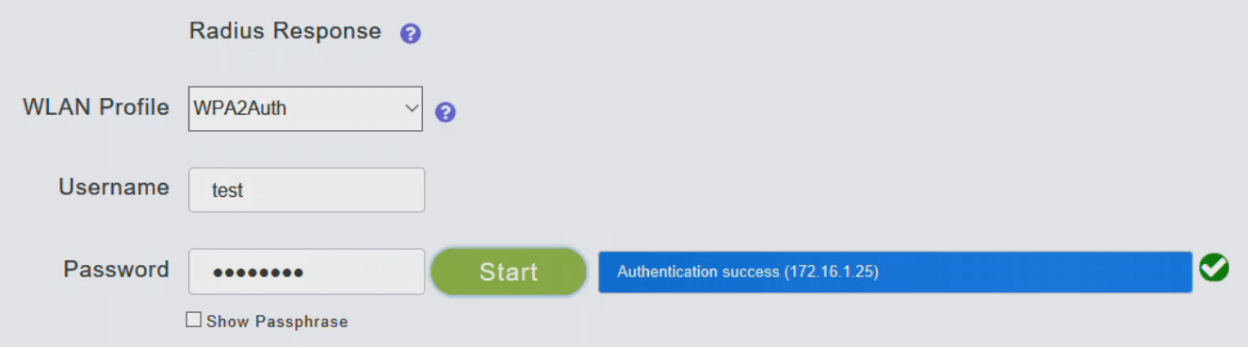
步骤 3

在*Radius Response*部分，输入您之前配置的WLAN配置文件的*Username*和*Password*，然后单击*Start*。



步骤 4

验证成功完成后，您将在屏幕上看到以下通知。



结论

给你！您现在已学习在CBW AP上配置RADIUS的步骤。有关更高级的配置，请参阅《思科*业务无线接入点管理指南*》。

常见问题 固件升级 RLAN 应用分析 客户端分析 主要AP工具 Umbrella WLAN用户 日志记录 流量整形 罗格 干扰源 配置管理 端口配置网状模式