在WAP125接入点上配置访客接入实例表

目标

WAP125接入点的访客接入功能提供与设备范围内的临时无线客户端的无线连接。它的工作方式是让接入点广播两个不同的服务集标识符(SSID):一个用于主网络，另一个用于访客网络。然后，访客将重定向到强制网络门户，在该门户中，访客需要输入其凭证。实际上，这将确保主网络的安全，同时仍允许访客访问Internet。

强制网络门户的设置(如会话超时和重定向统一资源定位器(URL))在WAP125基于Web的实用程序的访客访问实例表中配置。访客访问功能在酒店和办公室大堂、餐厅和商场中特别有用。

本文旨在向您展示如何配置WAP125接入点的访客接入实例表。它假设已配置Web门户区域设置表和访客组表的设置。有关配置这两种设置的说明，请单击此处。

适用设备

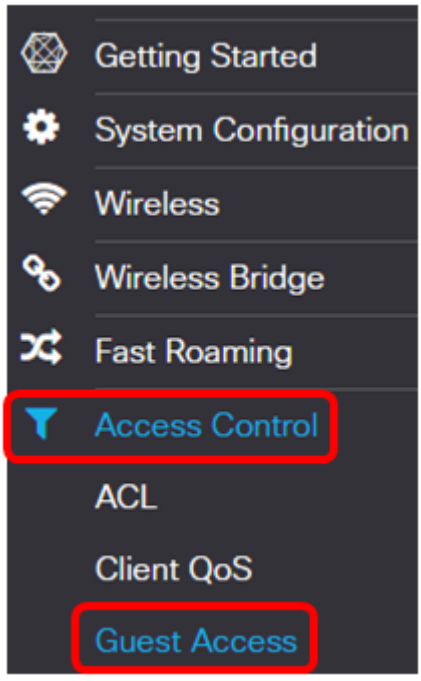
- WAP125

软件版本

- 1.0.0.4 - WAP581
- 1.0.0.5 - WAP125

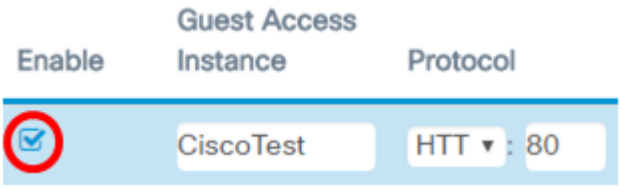
配置访客访问实例表

步骤1.登录WAP125的基于Web的实用程序，然后选择**Access Control > Guest Access**。

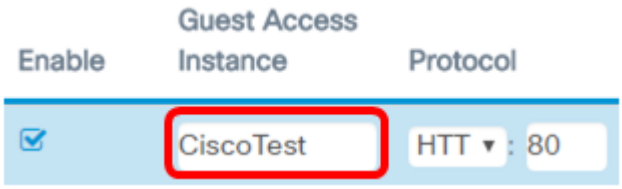


注意：本文中的图像取自WAP125。菜单选项可能因设备型号而异。

步骤2.验证Guest Access Instance Enable复选框**是否**已选中，以确保Guest Access处于活动状态。



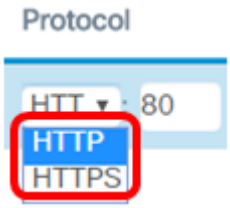
步骤3.在Guest Access Instance字段中输入实*例的名*称。最多可包含32个字母数字字符。



注意：在本例中，输入CiscoTest。

步骤4.为访客访问实例选择协议。选项有：

- HTTP — 此选项也称为超文本传输协议(HTTP)。 在验证所请求的网页时，它不提供加密。
- HTTPS — 此选项也称为超文本传输协议安全(HTTPS)。 这意味着计算机与其联系的网站之间的所有通信都已加密。



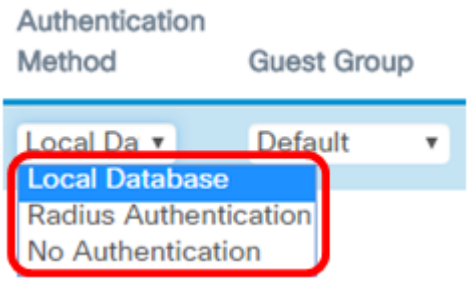
注意：在本例中，选择HTTP。

步骤5.在Protocol字段旁输入端口号。端口号有助于在协议到达服务器时识别协议。

注意：在本例中，输入80。

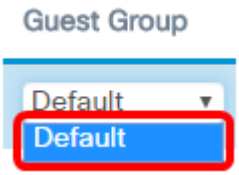
步骤6.从Authentication Method下拉列表中选择身份验证方法。当客户端通过强制网络门户进行身份验证时，接入点将使用此功能。选项有：

- 本地数据库 — 此选项允许WAP设备从本地存储的文件验证用户的凭证。如果选择此选项，请完成步骤7到步骤10，然后继续配置访客组表。
- RADIUS身份验证 — 此选项允许接入点通过远程身份验证拨入用户服务(RADIUS)服务器验证用户。如果选择此选项，请完成步骤7到步骤10，然后继续配置RADIUS Authentication。
- No Authentication — 此选项禁用身份验证并允许无线客户端在不输入其凭证的情况下连接到访客网络。如果选择此选项，请跳至步骤11。



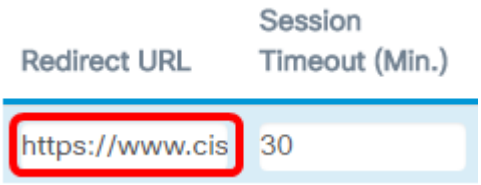
注意：在本例中，选择了本地数据库。

步骤7.从Guest Group下拉列表中选择一个组。



注意：在本例中，自动选择Default。

步骤8.在“重定向URL”字段中输入凭证后，输入要重*定向的*地址。

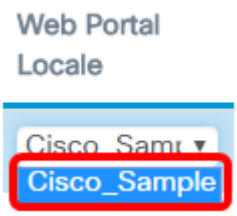


注意：地址应以HTTP或HTTPS开头。在本例中，输入https://www.cisco.com。

步骤9.在Session Timeout(Min.)字段中输入会话超*时前的分钟*数。

注意：在本例中，输入30。

步骤10.从Web门户区域设置下拉列表中选择Web门户配置文件。



注意：在本例中，会自动选择Cisco_Sample。有关如何配置Web门户区域设置的说明，请单击此处。

现在应配置访客接入实例表。

配置访客组表

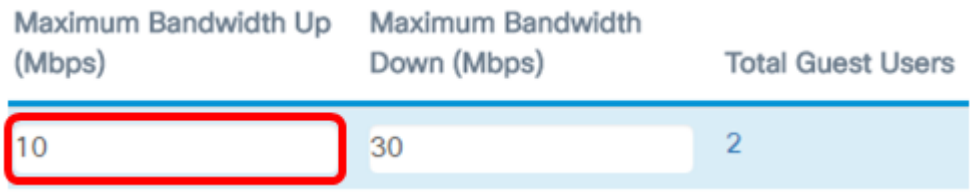
步骤7.在Guest Group Name字段中输入访客*组的名*称。访客组名称最长可包含32个字符。

注意：在本例中，输入CiscoGuests。

步骤8.在Idle Timeout(Min.)字段中输入提示超*时前的分钟*数。

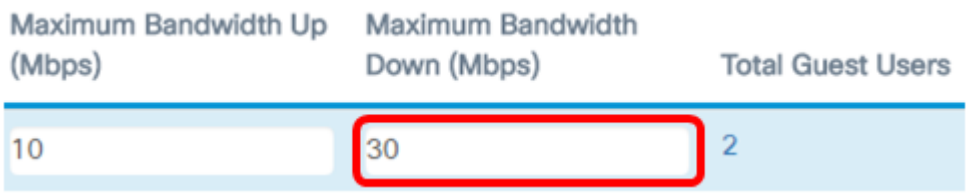
注意：在本例中，输入5。

步骤9.在Maximum Bandwidth Up(Mbps)字*段中输入最大上传*速度。这是无线客户端使用强制网络门户时可以发送的最大带宽（以Mbps为单位）。最大带宽可以是0到300，其中0是默认值。



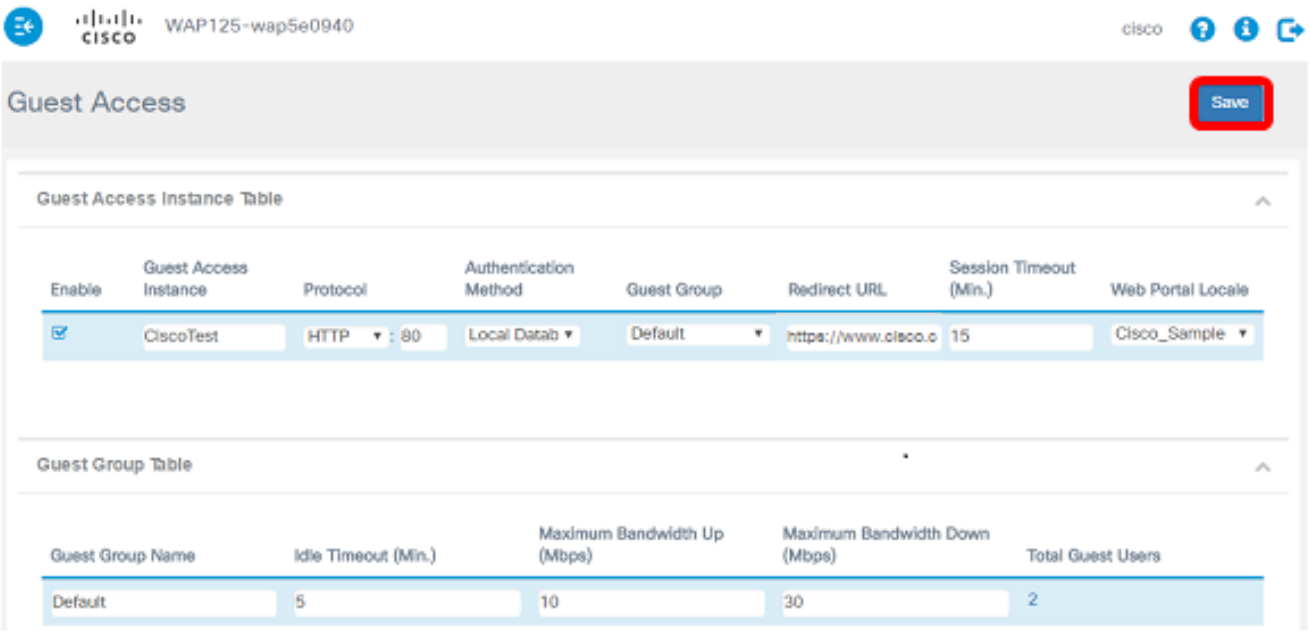
注意：在本例中，输入10。

步骤10.在Maximum Bandwidth Down(Mbps)字*段中输入最大下载*速度。这将是无线客户端使用强制网络门户时可接收的最大带宽（以Mbps为单位）。最大带宽可以是0到300，其中0是默认值。



注意：在本例中，输入30。

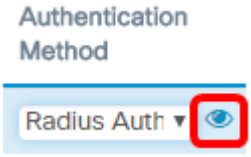
步骤11.单击保**存**。



现在应使用本地数据库身份验证配置访客访问实例表。

RADIUS 身份验证

步骤1.点击View按钮。

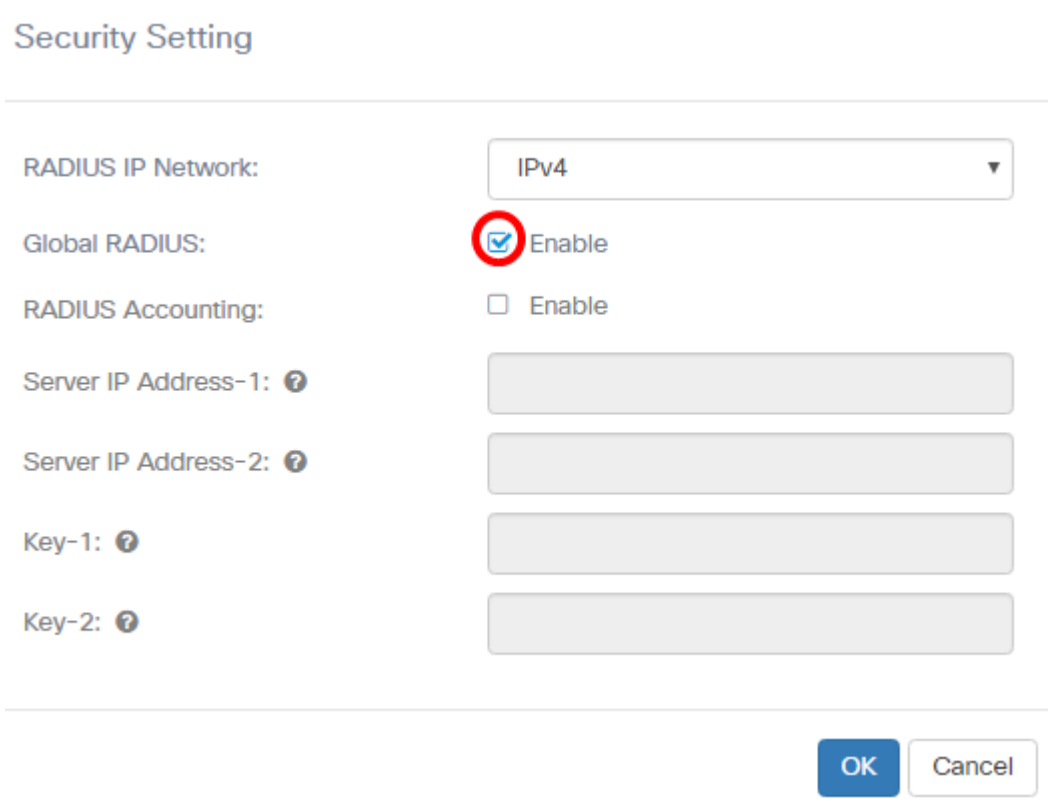


步骤2.在Security Setting弹出窗口中，从RADIUS IP Network下拉列表中选择RADIUS IP网络。选项有：

- IPv4 — 此选项是网络中最常用的IP编址形式。它使用32位格式来标识网络中的主机。
- IPv6 — 此选项是用于替换IPv4格式的下一代IP地址标准。IPv6使用128位编址系统而不是IPv4中使用的32位编址系统，从而解决了地址稀缺问题。

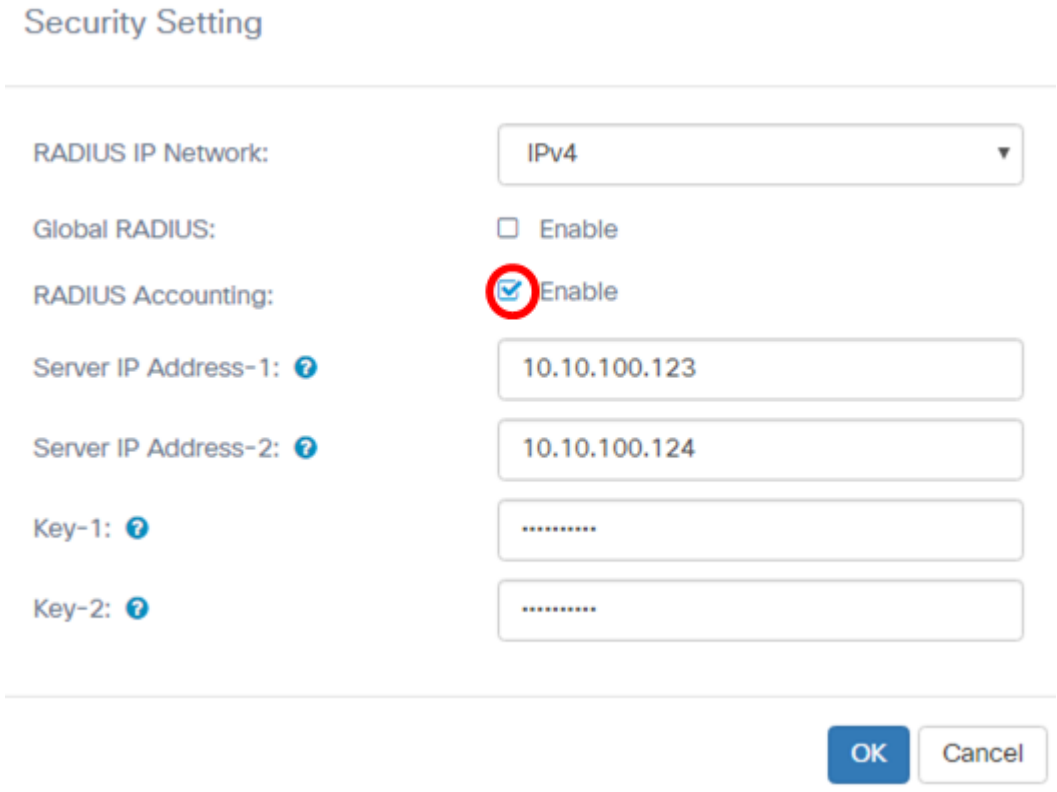
注意：在本例中，选择IPv4。

步骤3.（可选）选中Global RADIUS **Enable**复选框，使强制网络门户使用不同的RADIUS服务器集。

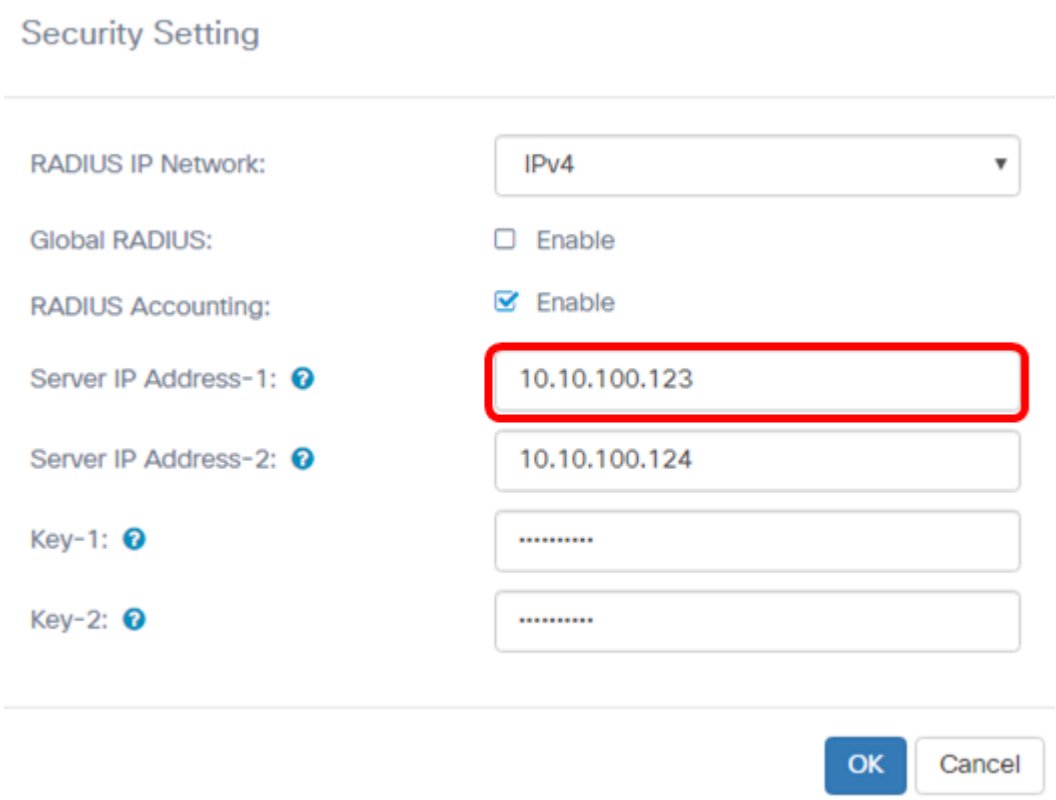


注意：启用后，无需为“安全设置”区域配置其他配置。继续执行步骤9。在本例中，全局RADIUS已启用。

步骤4.（可选）选中RADIUS Accounting **Enable** 复选框，使接入点跟踪并测量特定用户消耗的资源，如系统时间和发送和接收的数据量。

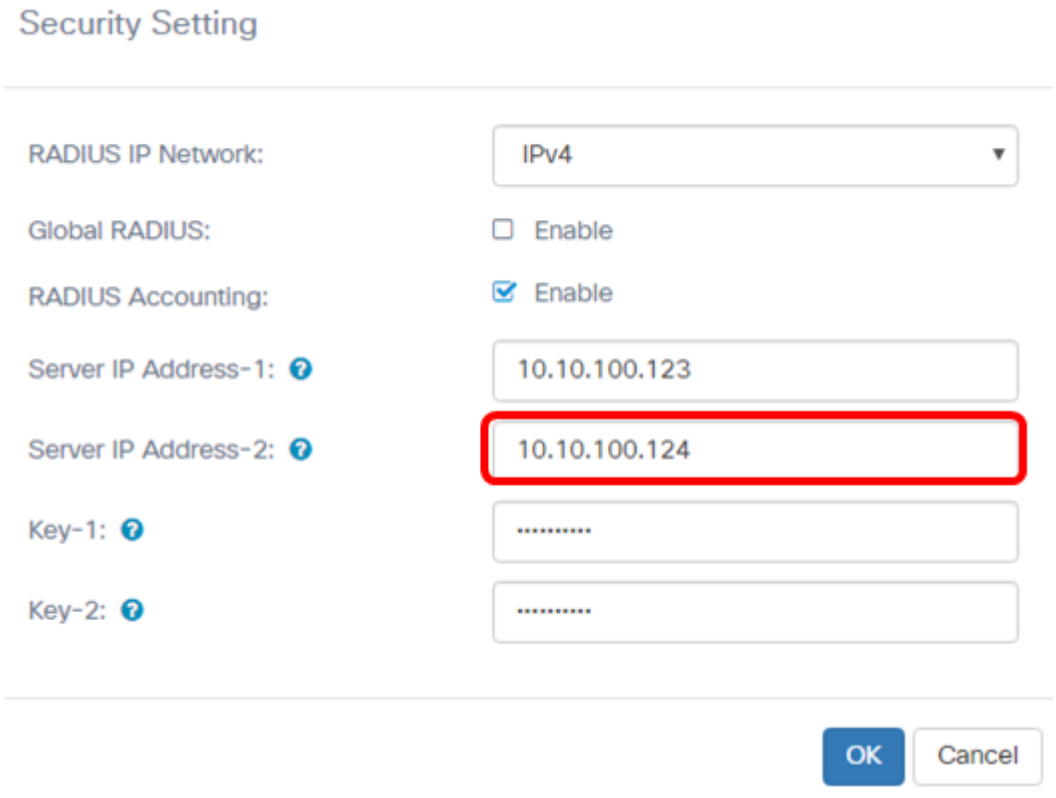


步骤5.（可选）在Server IP Address-1字段中输入主RADIUS服务器的IPv4*或IPv6地*址。



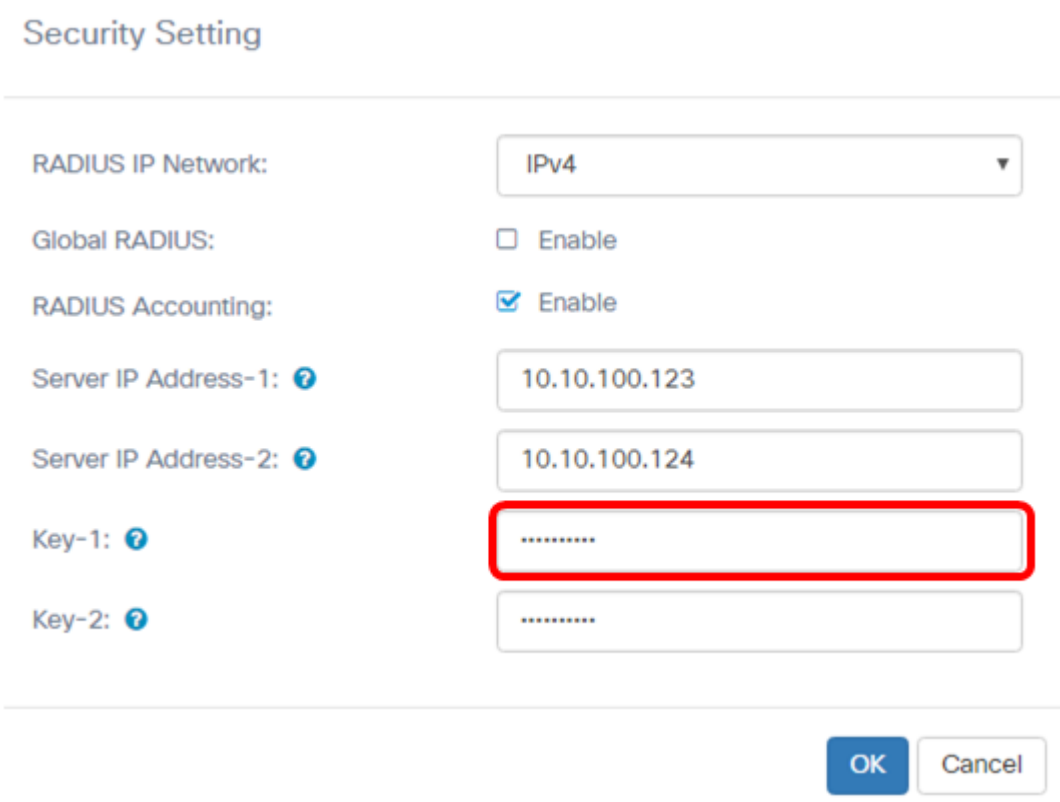
注意：在本例中，输入10.10.100.123。

步骤6.（可选）在Server IP Address-2字段中输入备用RADIUS服务器的IPv4*或IPv6地*址。

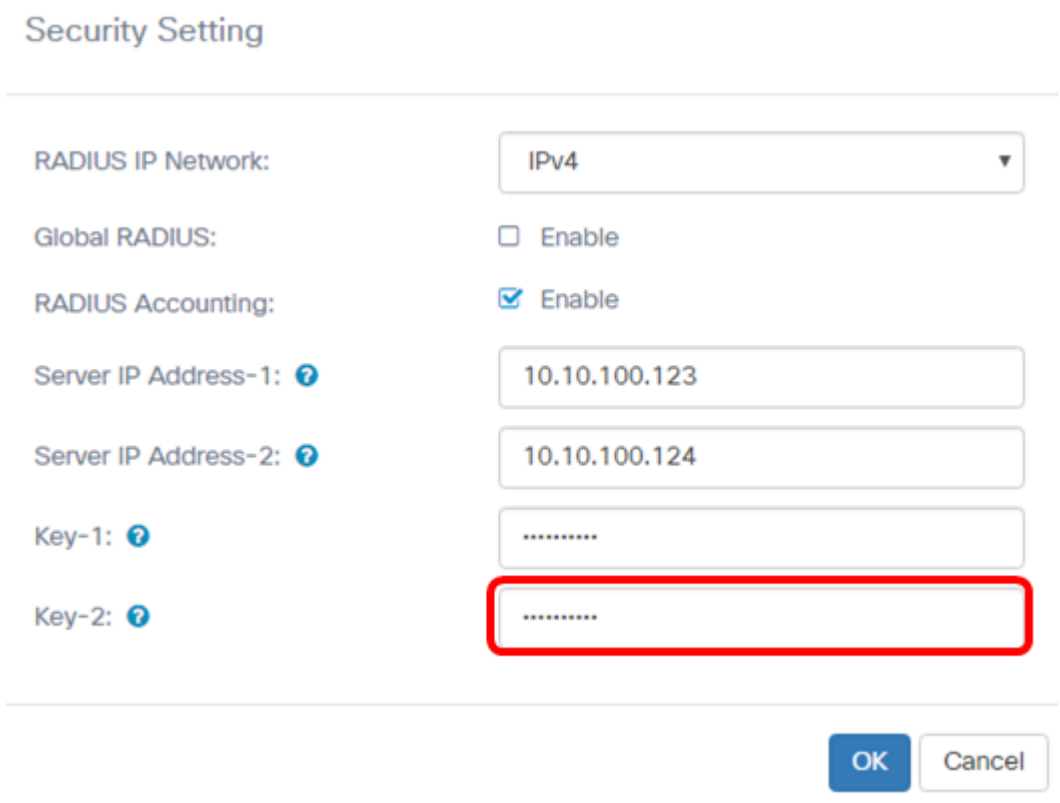


注意：在本例中，输入10.10.100.124。

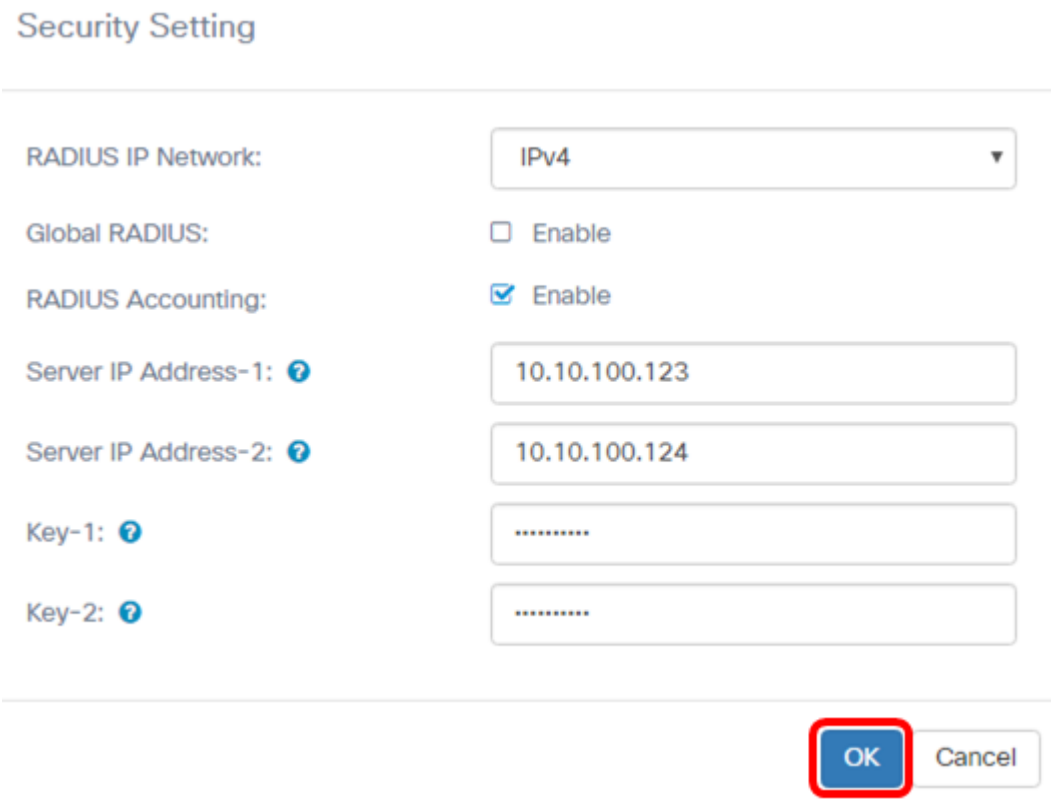
步骤7.（可选）在Key-1字段中输入接入点用于验证主RADIUS服务器*的密码*。此字段中的条目区分大小写，并且必须与主RADIUS服务器上配置的条目匹配。密钥最多可包含63个字母数字字符。



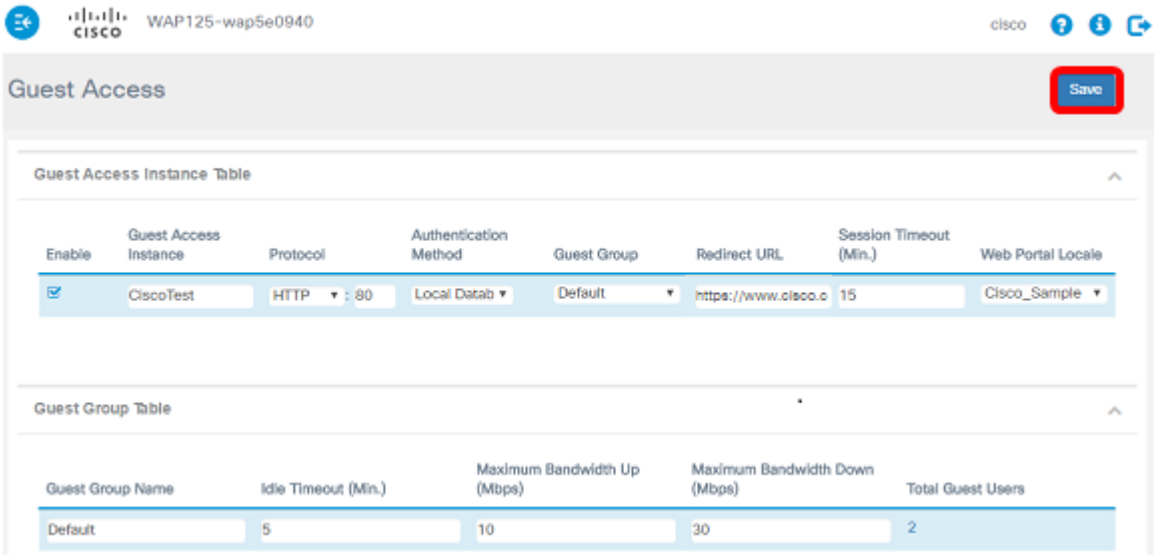
步骤8.（可选）在Key-2字段中输入接入点用于验证辅助RADIUS服务器*的密码*。此字段中的条目区分大小写，并且必须与主RADIUS服务器上配置的条目匹配。密钥最多可包含63个字母数字字符。



步骤9.单击**OK**。



步骤10.单击“保存”。



现在应使用RADIUS身份验证方法配置访客接入实例表。