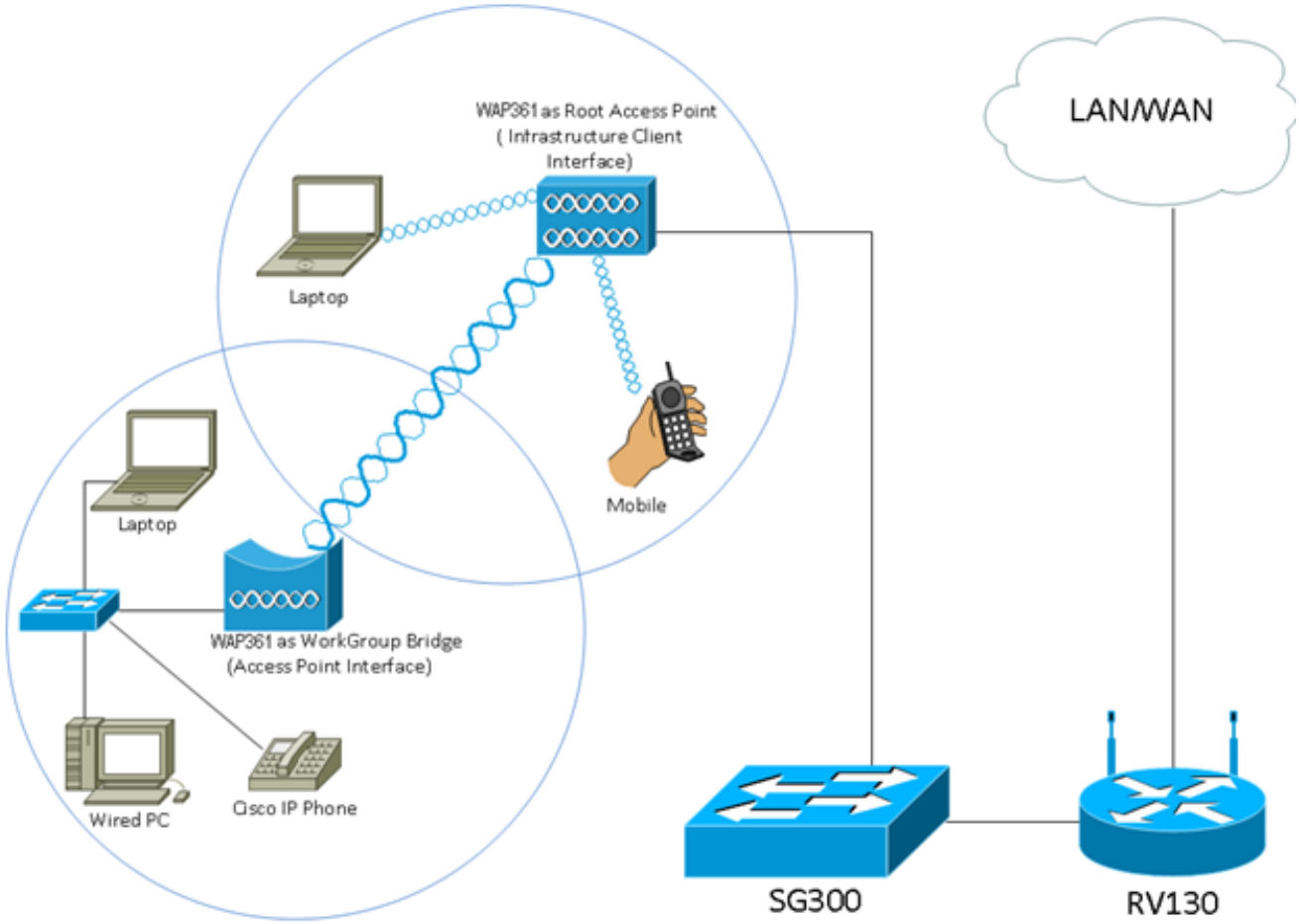
# 在无线接入点(WAP)上配置工作组网桥

## 目标

工作组桥接功能使无线接入点(WAP)能够桥接远程客户端与无线局域网(LAN)之间的流量，后者通过工作组桥接模式连接。与远程接口相关联的WAP设备称为接入点接口，而与无线LAN相关联的WAP设备称为基础设施接口。工作组桥可让仅具有有线连接的设备连接到无线网络。当无线分发系统(WDS)功能不可用时，建议使用工作组桥接模式作为替代模式。




注意：上面的拓扑显示了工作组网桥模型示例。有线设备连接到交换机，交换机连接到WAP的LAN接口。WAP充当接入点接口，连接到基础设施接口。

本文旨在向您展示如何在两个WAP之间配置工作组网桥。

## 适用设备

- WAP100系列
- WAP300系列
- WAP500系列

## 软件版本

- 1.0.0.17 —WAP571、WAP571E
- 1.0.1.7 — WAP150、WAP361
- 1.0.2.5 — WAP131、WAP351
- 1.0.6.5 — WAP121、WAP321
- 1.2.1.3 — WAP551、WAP561
- 1.3.0.3 — WAP371

## 配置工作组网桥

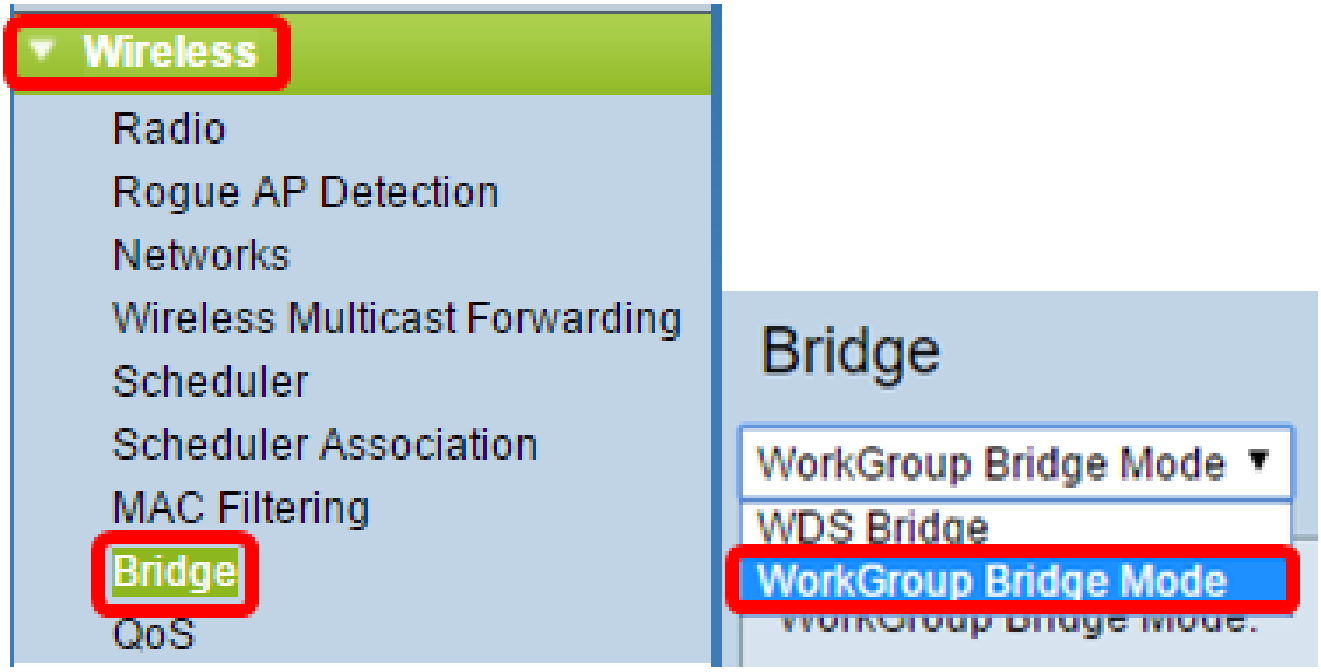
### 基础设施客户端接口

步骤1:登录WAP的基于Web的实用程序，并选择Wireless > WorkGroup Bridge。

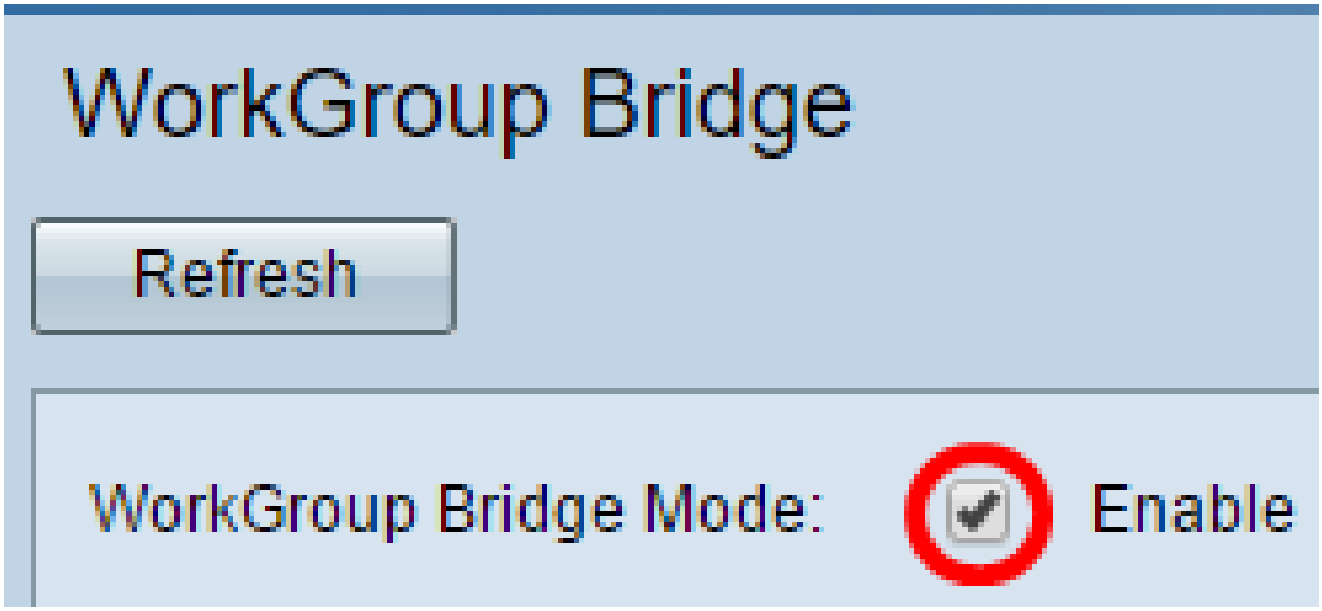
注意：菜单选项可能会因您使用的设备型号而异。除非另有说明，否则下面的图像取自WAP361。



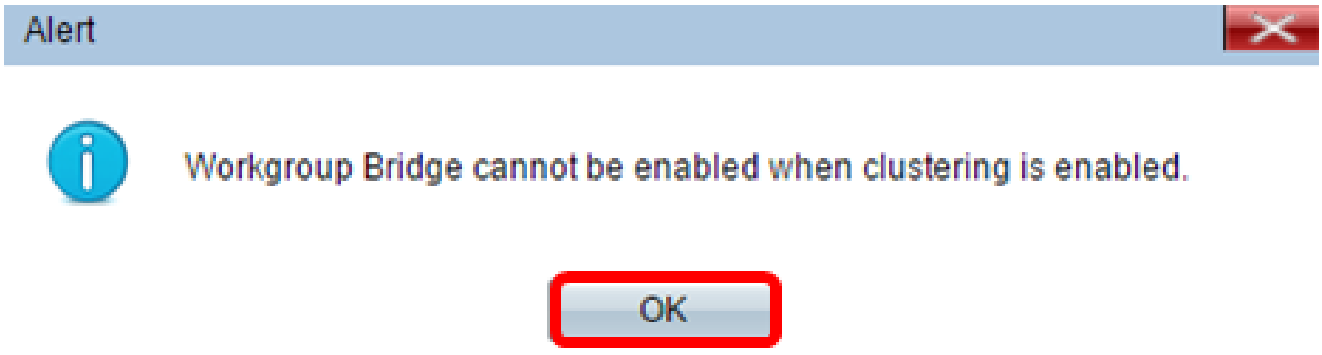

对于WAP571和WAP571E，请选择Wireless > Bridge > WorkGroup Bridge Mode。




第二步：选中Enable WorkGroup Bridge Mode复选框。

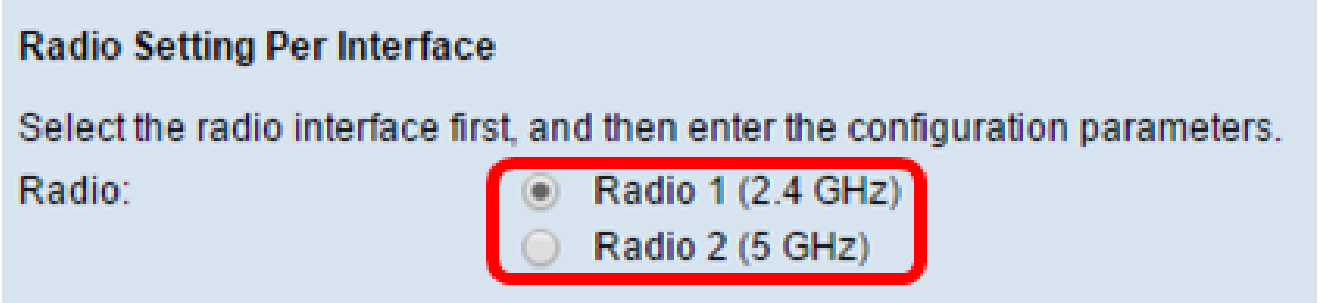



注意：如果在WAP上启用集群，弹出窗口将通知您禁用集群，以便工作组网桥正常工作。单击 OK 继续。要禁用集群，请从导航窗格中选择Single Point Setup，然后选择Access Points > Disable Single Point Setup。



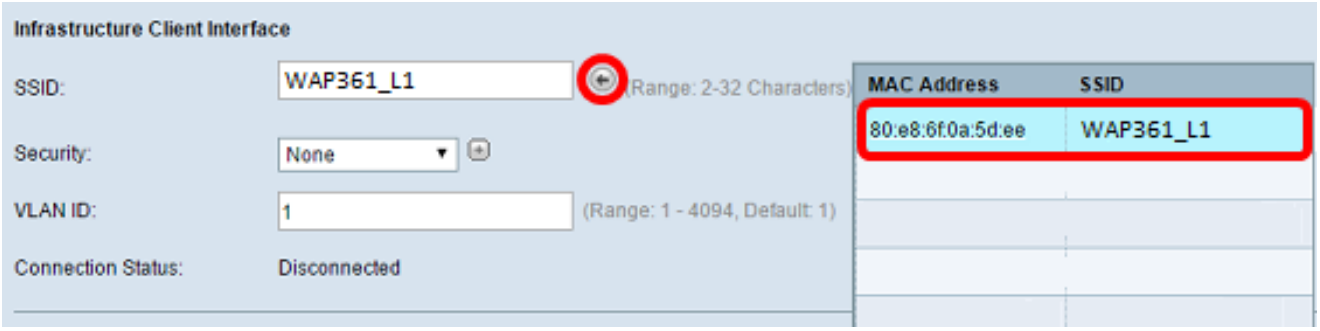
第三步：单击“工作组网桥”的无线电接口。将一个无线电配置为工作组桥接时，另一个无线电保持运行。无线电接口对应于WAP的无线电频带。WAP配备用于在两个不同的无线电接口上广播。配置一个无线电接口的设置不会影响另一个无线电接口。无线电接口选项可能因WAP型号而异。某些WAP显示Radio 1 as 2.4 GHz，而某些WAP显示Radio 2 as 2.4 GHz。

注意：此步骤仅适用于带双频段的以下WAP：WAP131、WAP150、WAP351、WAP361、WAP371、WAP561、WAP571、WAP571E。在本示例中，选择Radio 1。



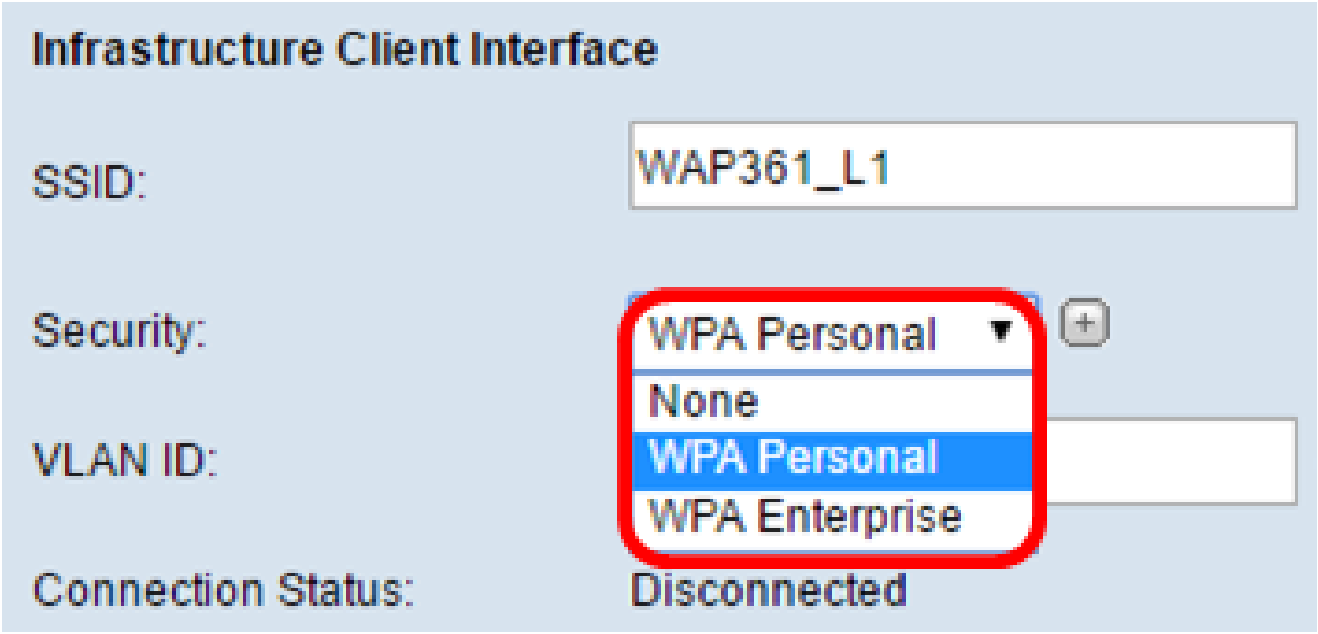

第四步：在SSID字段中输入服务集标识符(SSID)名称，或者单击字段旁边的箭头按钮扫描邻居。这用作设备和远程客户端之间的连接。您可以为基础设施客户端SSID输入2到32个字符。

注意：启用非法AP检测非常重要。若要了解有关如何启用上述功能的详细信息，请单击此处。在本例中，点击箭头按钮选择WAP361_L1作为基础设施客户端接口的SSID。




第五步：在Infrastructure Client Interface区域中，从Security下拉列表中选择要作为上游WAP设备上的客户端工作站进行身份验证的安全类型。选项有：

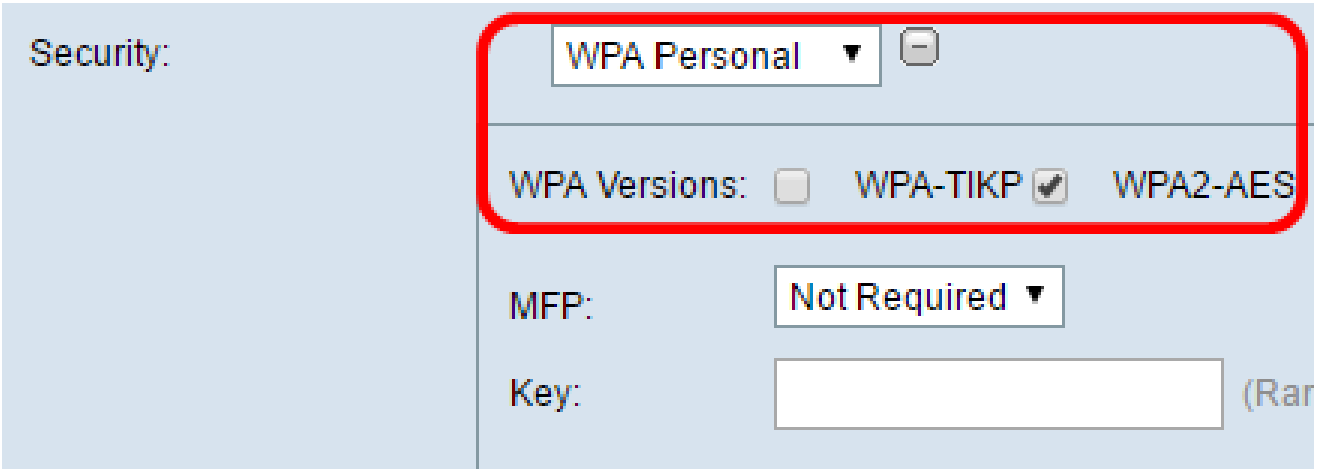
- 无-打开或不打开安全性。这是默认设置。如果选择此项，请跳到步骤18。
- WPA个人- WPA个人可支持长度为8-63个字符的密钥。建议使用WPA2，因为它采用更强大的加密标准。跳至步骤6进行配置。
- WPA企业版— WPA企业版比WPA个人版更高级，是推荐的身份验证安全方案。它使用受保护的可扩展身份验证协议(PEAP)和传输层安全(TLS)。请跳到步骤9进行配置。这种安全类型通常用于办公环境，需要配置远程身份验证拨入用户服务(RADIUS)服务器。单击此处可了解有关RADIUS服务器的详细信息。




注意：在本例中，选择了“WPA个人”。

第六步：单击+并选中WPA-TKIP或WPA2-AES复选框，以确定基础设施客户端接口将使用哪种WPA加密。

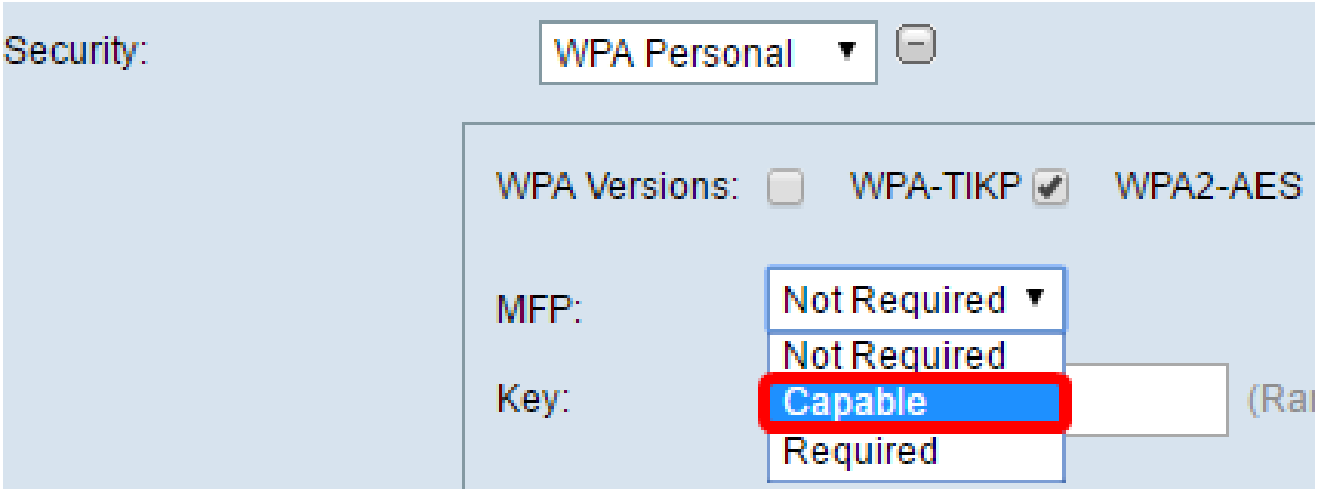
注意：如果所有无线设备都支持WPA2，请将基础设施客户端安全设置为WPA2-AES。对于WPA，加密方法是RC4；对于WPA2，加密方法是AES。建议使用WPA2，因为它采用更强大的加密标准。本例使用WPA2-AES。



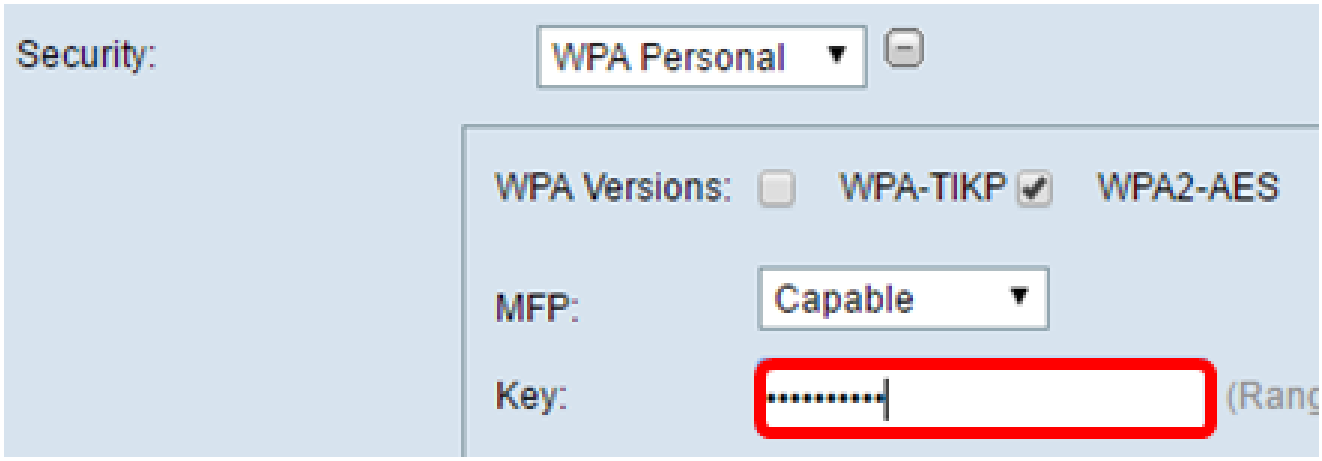

第7步（可选）如果在步骤6中选中了WPA2-AES，请从“管理帧保护(MFP)”下拉列表中选择一个选项，以决定是否希望WAP具有受保护的帧。要了解有关MFP的详细信息，请单击此处。选项有：

- Not Required -禁用MFP的客户端支持。
- Capable —允许支持MFP的客户端和不支持MFP的客户端加入网络。这是WAP上的默认MFP设置。
- 必需-仅当协商MFP时，才允许客户端进行关联。如果设备不支持MFP，则不允许它们加入网络。

注意：在本示例中，选择Capable。



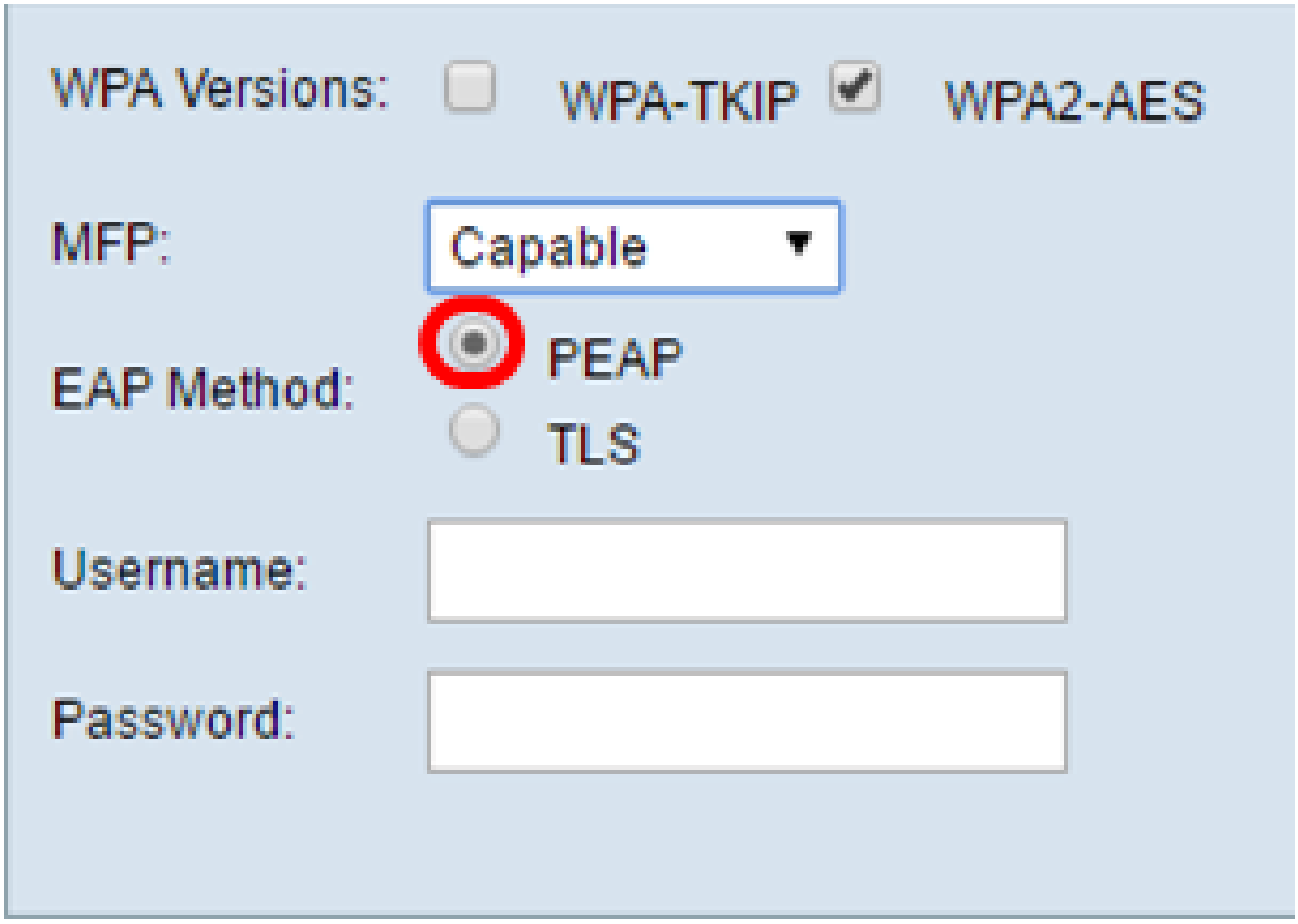

步骤 8在Key字段中输入WPA加密密钥。密钥的长度必须为8-63个字符。这是字母、数字和特殊字符的组合。它是首次连接到无线网络时使用的密码。然后，跳至步骤18。




步骤 9如果在步骤5中选择了WPA企业，请点击EAP方法的单选按钮。

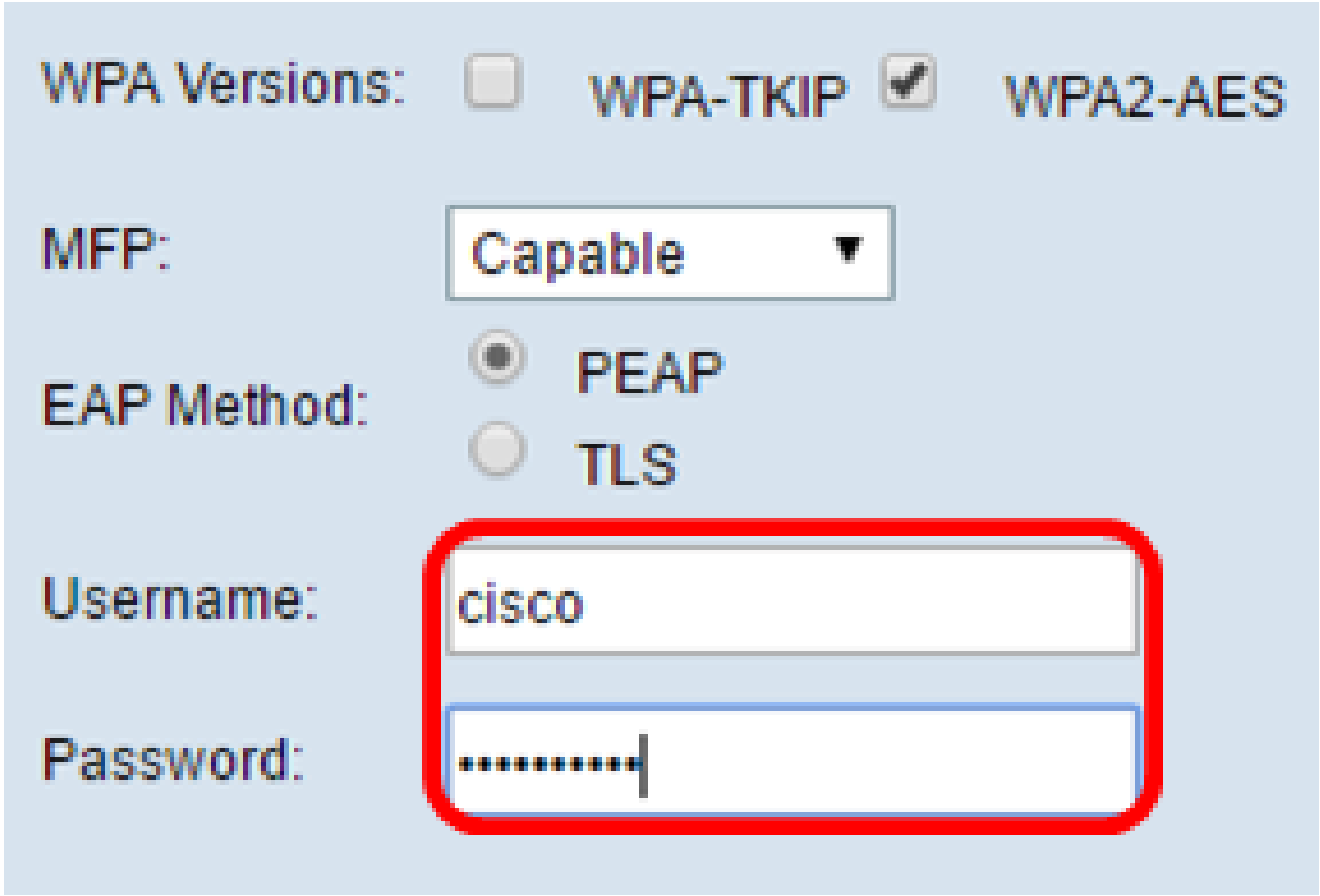
可用选项定义如下：

- PEAP —此协议为WAP下的每个无线用户提供支持AES加密标准的个人用户名和密码。由于PEAP是基于密码的安全方法，因此您的Wi-Fi安全基于客户端的设备凭证。如果您具有弱密码或不安全的客户端，PEAP可能会带来潜在严重的安全风险。它依赖于TLS，但避免在每个客户端上安装数字证书。相反，它通过用户名和密码提供身份验证。
- TLS - TLS要求每个用户都有一个额外的证书来获得访问权限。如果您有额外的服务器和必要的基础设施，来验证网络中的用户，则TLS会更安全。

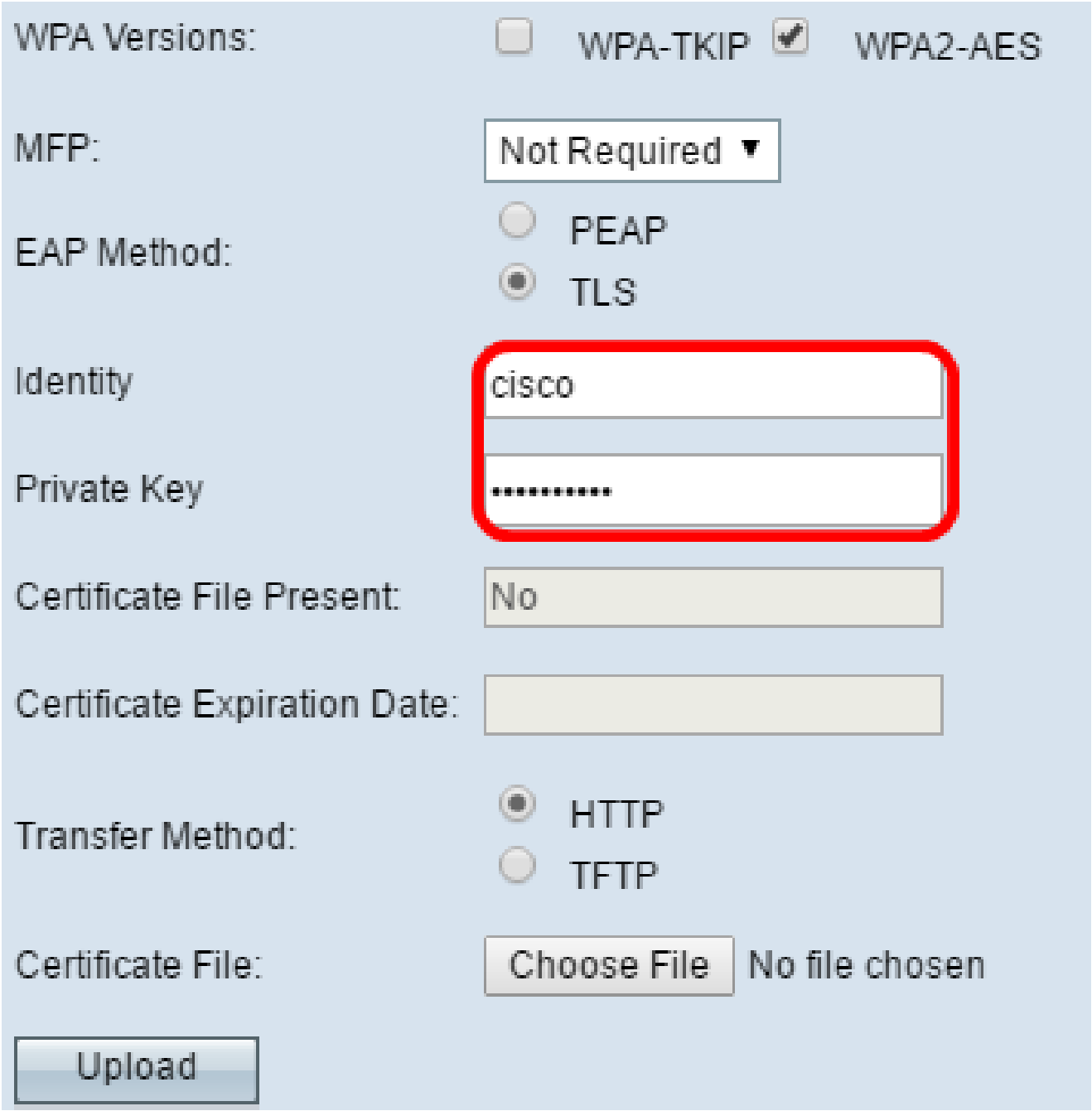



注意：在本示例中，选择PEAP。

步骤 10在Username和Password字段中输入基础设施客户端的用户名和口令。这是用于连接到基础设施客户端接口的登录信息；请参阅您的基础设施客户端接口以查找此信息。然后，跳至步骤18。

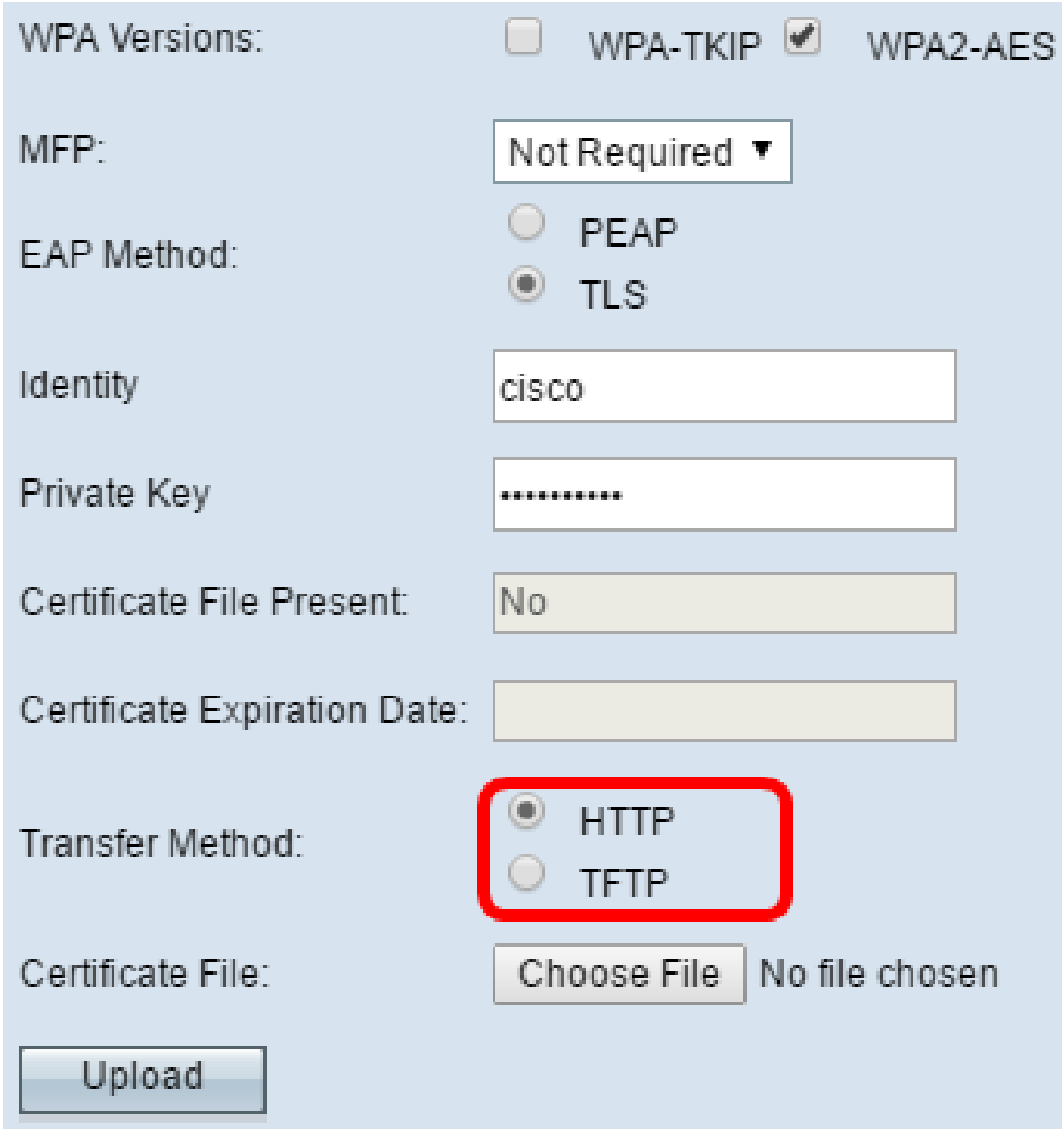



步骤 11如果在步骤9中单击TLS，请在身份和私钥字段中输入基础设施客户端的标识和私钥。




步骤 12在transfer method区域中，点击以下选项的单选按钮：

- TFTP -简单文件传输协议(TFTP)是文件传输协议(FTP)的简化非安全版本。它主要用于在公司网络之间分发软件或验证设备。如果单击TFTP，请跳到步骤15。
- HTTP -超文本传输协议(HTTP)提供客户端可用于提供身份验证框架的简单质询-响应身份验证框架。




注意：如果WAP上已存在证书文件，则Certificate File Present和Certificate Expiration Date字段将填充相关信息。否则，它们将为空白。

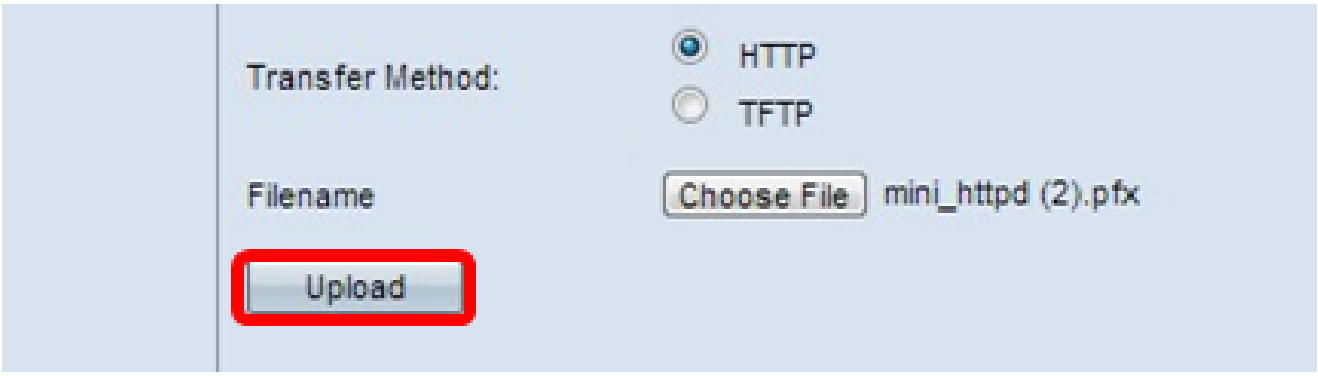
HTTP

步骤 13单击Choose File按钮以查找并选择证书文件。文件必须具有正确的证书文件扩展名（例如.pem或.pfx），否则，将不会接受该文件。

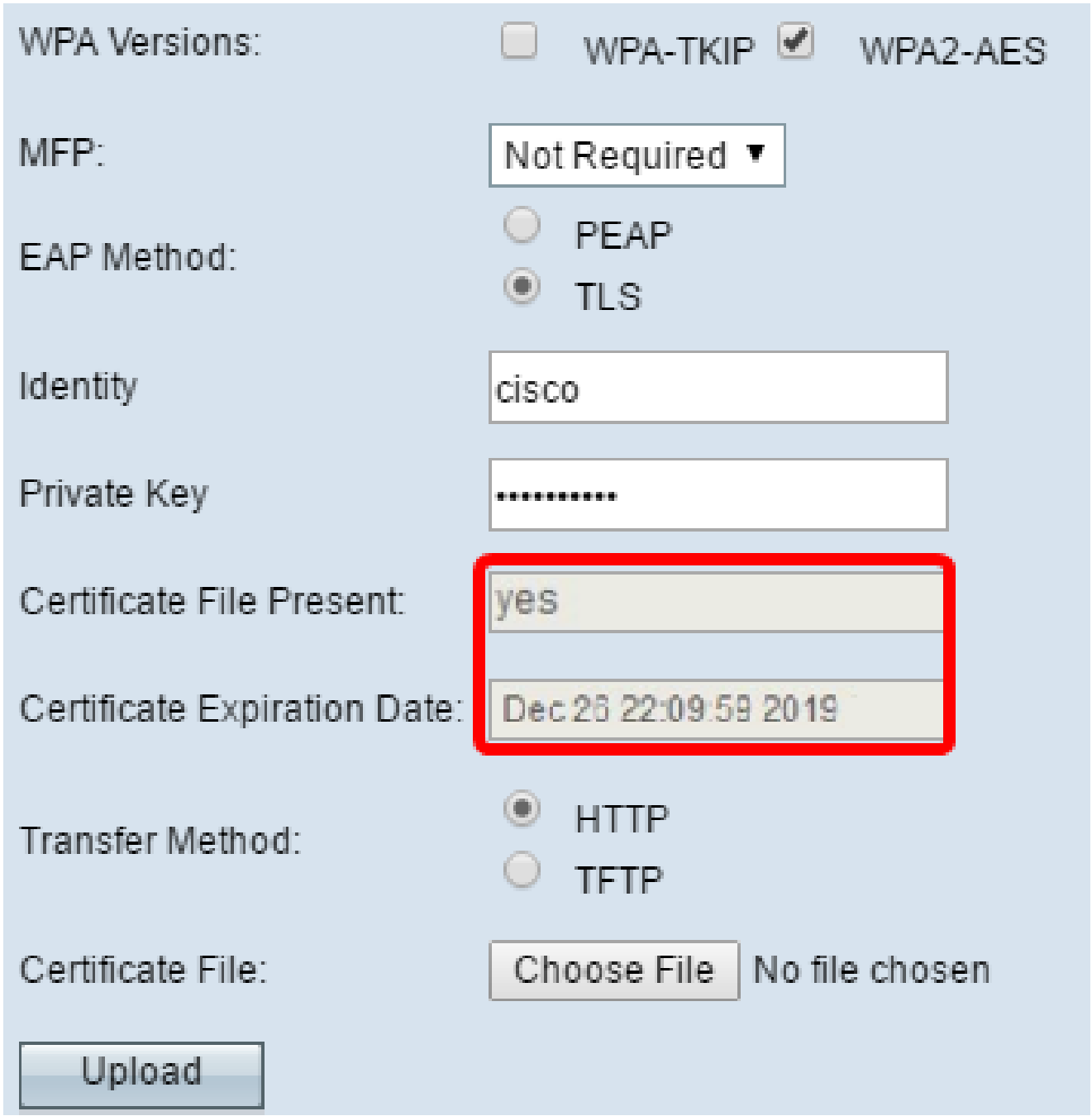
注意：在本示例中，选择mini_httpd(2)。pfx。




步骤 14点击上传以上传选定的证书文件。跳至步骤18。




Certificate File Present 和Certificate Expiration Date 字段将自动更新。




TFTP

步骤 15 如果您在步骤12中单击了TFTP，请在文件名字段中输入证书文件的文件名。

注意：在本示例中，使用mini_httpd.pem。




步骤 16在TFTP Server IPv4 Address字段中输入TFTP服务器地址。

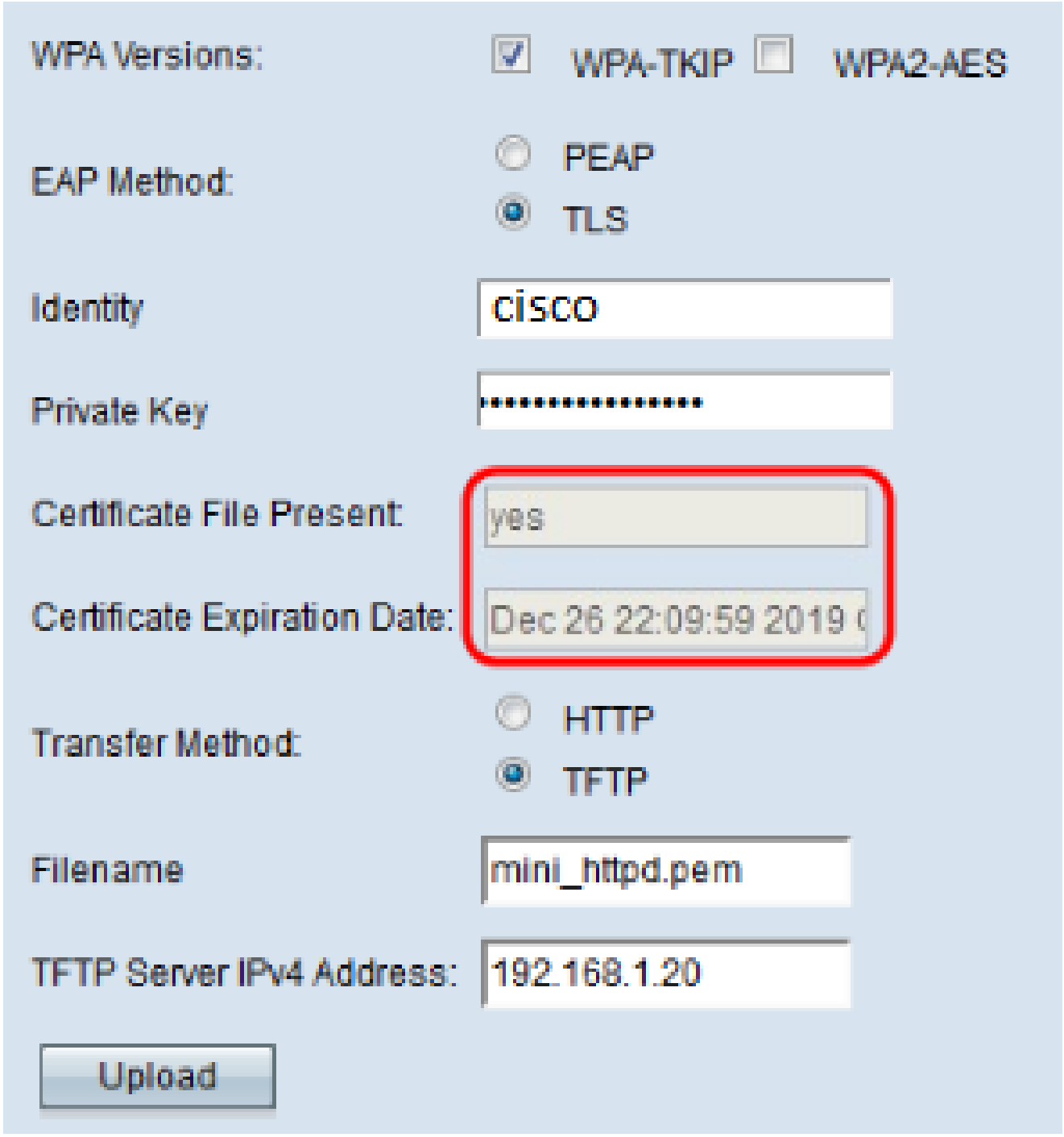
注意：在本例中。TFTP服务器地址使用192.168.1.20。




步骤 17单击Upload按钮以上传指定的证书文件。

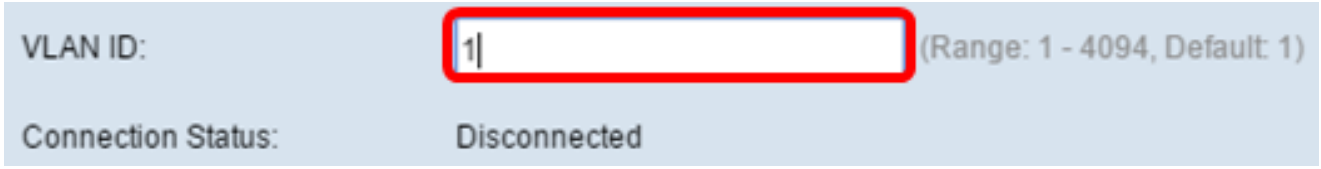



Certificate File Present 和Certificate Expiration Date 字段将自动更新。



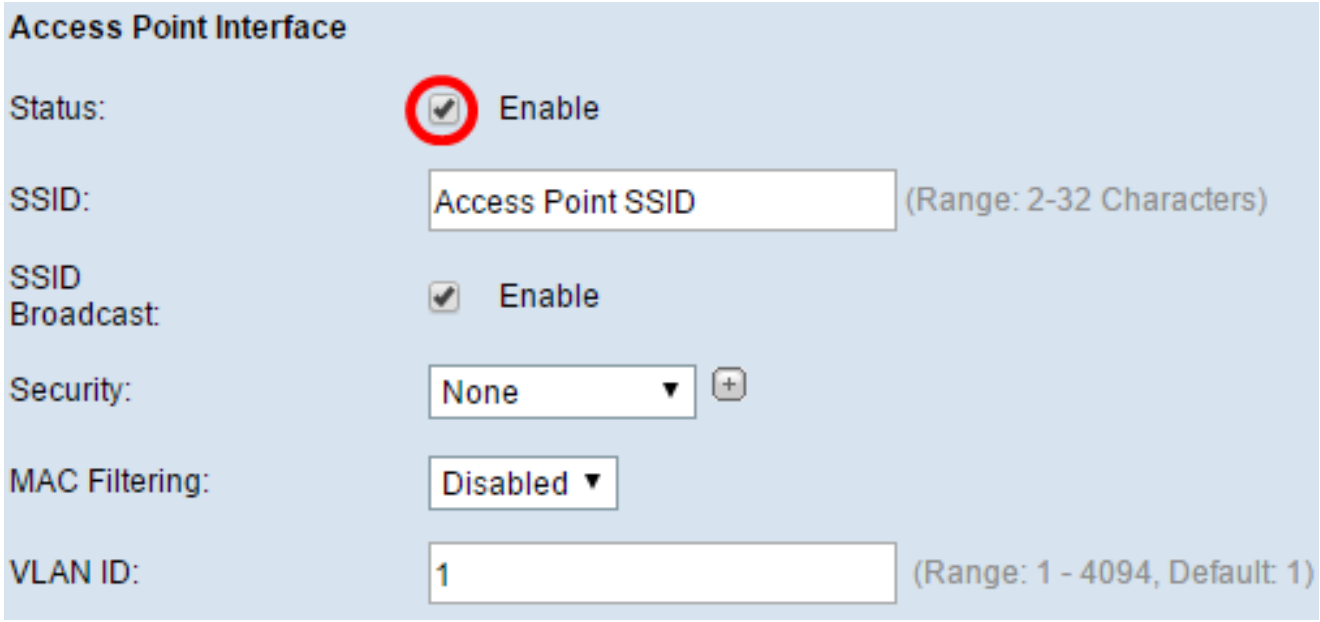

步骤 18. 输入基础设施客户端接口的VLAN ID。默认值是 1。

注意：在本示例中，使用默认VLAN ID。




## 接入点接口

步骤1:选中Enable Status复选框以在接入点接口上启用桥接。

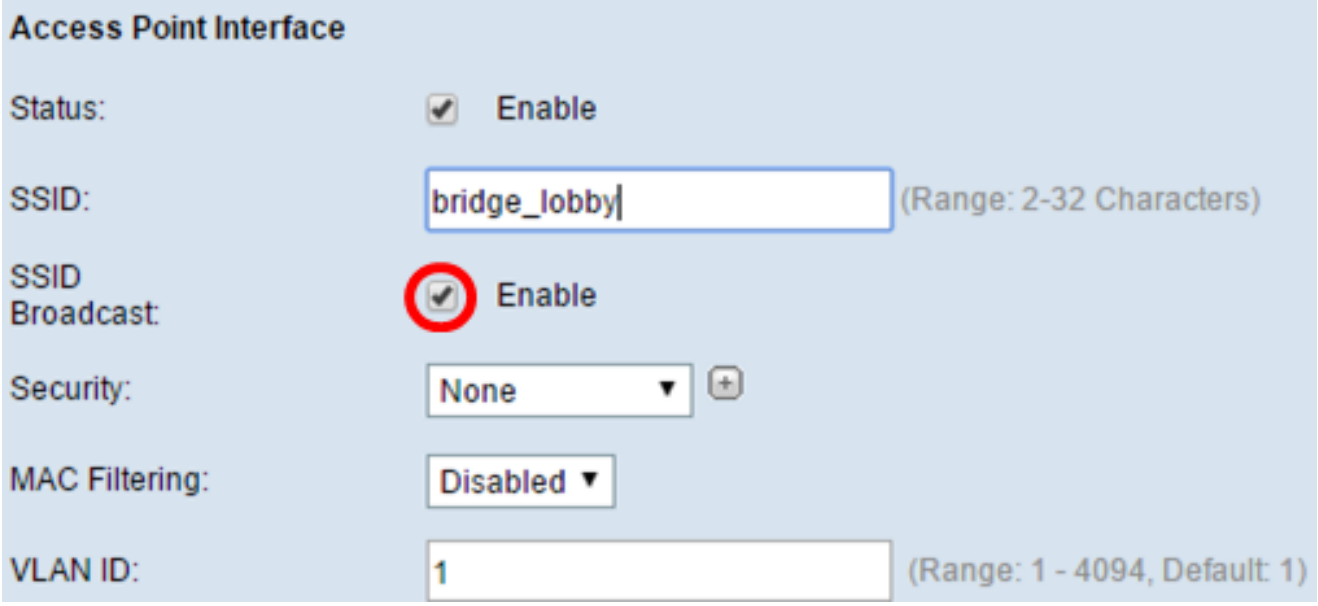



第二步：在SSID字段中输入接入点的SSID。SSID长度必须介于2到32个字符之间。默认设置为接入点SSID。

注意：在本示例中，使用的SSID是bridge_lobby。



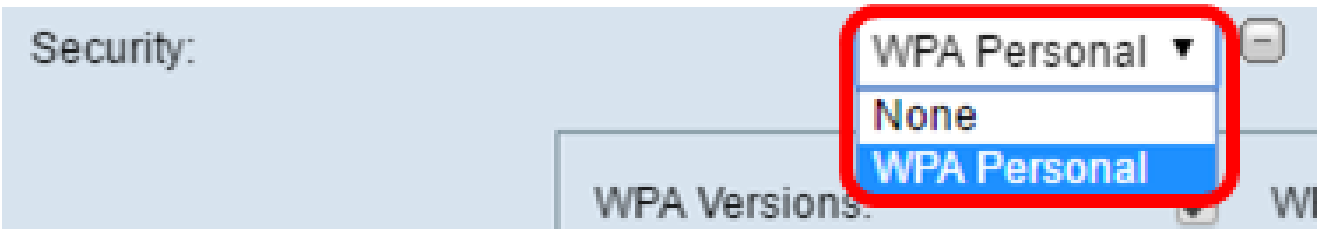

第3步：（可选）如果不想广播SSID，请取消选中Enable SSID Broadcast复选框。这样做将使搜索无线接入点的用户看不到接入点；只有知道SSID的用户才能连接到该接入点。默认情况下启用SSID广播。




第四步：从Security下拉列表中选择向WAP验证下游客户端工作站的安全类型。

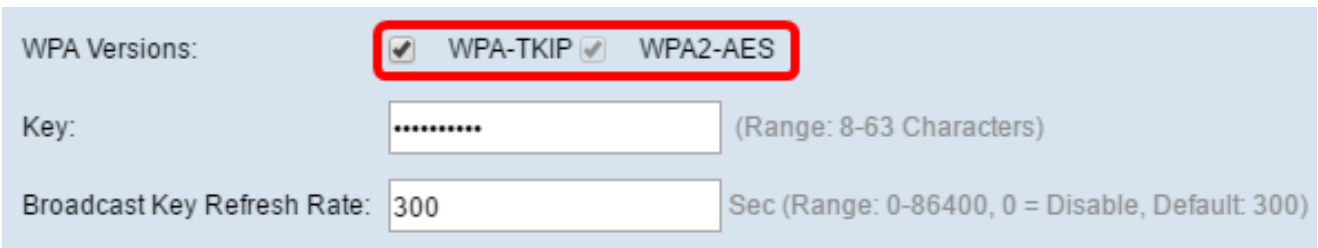
可用选项定义如下：

- 无-打开或无安全性。这是默认值。如果选择此项，请跳到步骤10。
- WPA个人- Wi-Fi保护访问(WPA) Personal可支持长度为8到63个字符的密钥。加密方法为TKIP或带分组链消息认证码协议(CCMP)的计数器密码模式。建议使用带有CCMP的WPA2，因为它与仅使用64位RC4标准的临时密钥完整性协议(TKIP)相比，具有更强大的加密标准-高级加密标准(AES)。

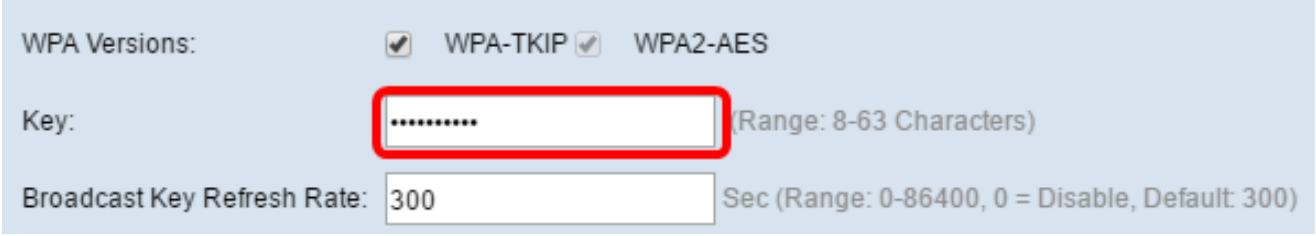



第五步： 选中WPA-TKIP或WPA2-AES复选框以确定接入点接口将使用哪种WPA加密。默认情况下，这些选项处于启用状态。

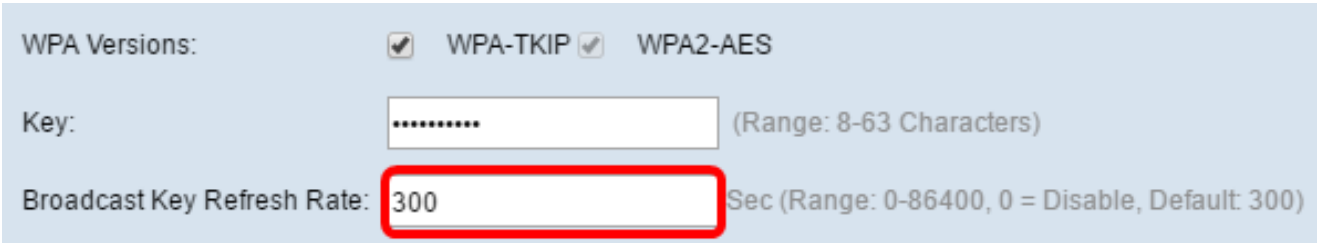
注意：如果所有无线设备都支持WPA2，则将基础设施客户端安全设置为WPA2-AES。对于WPA，加密方法是RC4；对于WPA2，加密方法是AES。建议使用WPA2，因为它采用更强大的加密标准。本例使用WPA2-AES。




第六步：在Key字段中输入共享WPA密钥。密钥的长度必须为8-63个字符，可以包含字母数字字符、大写和小写字符以及特殊字符。



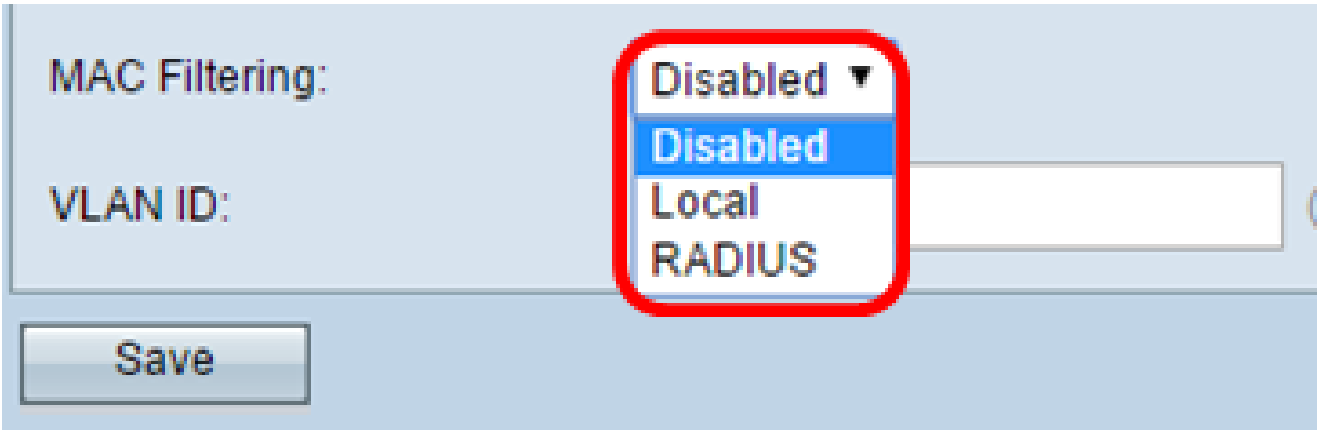

步骤 7.在Broadcast Key Refresh Rate字段中输入速率。广播密钥刷新率指定安全密钥刷新与此接入点关联的客户端的时间间隔。速率必须介于0到86400之间，并且值为0表示禁用该功能。默认值为 300。




步骤 8从MAC Filtering下拉列表中选择要为接入点接口配置的MAC过滤类型。启用后，系统会根据用户使用的客户端的MAC地址授予或拒绝用户对WAP的访问。

可用选项定义如下：

- 已禁用-所有客户端均可访问上游网络。这是默认值。
- 本地—可以访问上游网络的一组客户端被限制为本地定义的MAC地址列表中指定的客户端。
- RADIUS -可访问上游网络的一组客户端被限制在RADIUS服务器的MAC地址列表中指定的客户端。



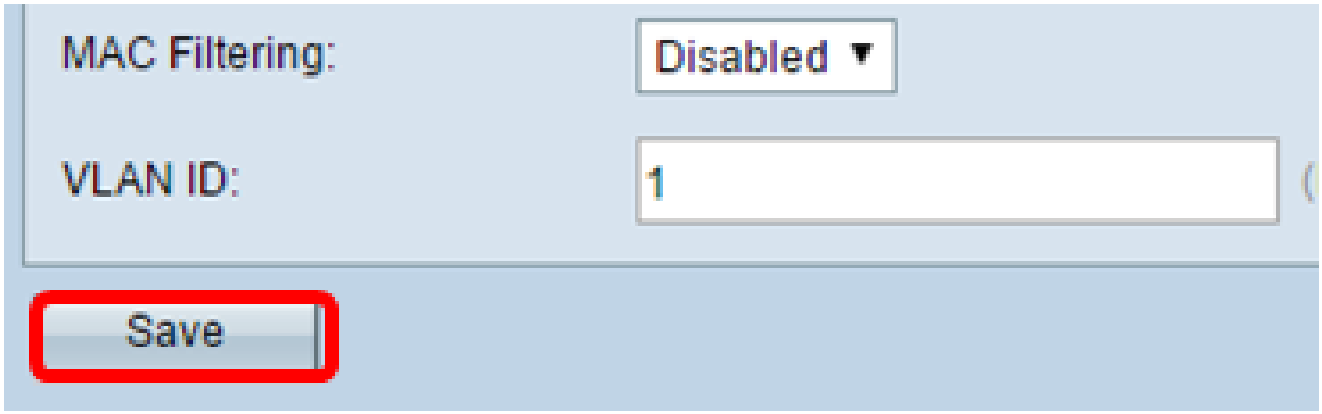

注意：在本示例中，选择Disabled。

步骤 9在VLAN ID字段中输入接入点接口的VLAN ID。

注意：为了允许桥接数据包，接入点接口和有线接口的VLAN配置应与基础设施客户端接口的VLAN配置相匹配。




步骤 10单击 Save（保存）保存所进行的更改。




现在，您应该已经成功地在无线接入点上配置了工作组网桥。

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）。

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）。

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）。

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）。

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）。