在WAP351、WAP131和WAP371上配置VAP

目标

虚拟接入点(VAP)将无线LAN划分为多个广播域，这些广播域与以太网VLAN无线等效。VAP在一个物理WAP设备中模拟多个接入点。Cisco WAP131支持多达四个VAP，Cisco WAP351和WAP371支持多达八个VAP。

本文档的目标是向您展示如何在WAP351、WAP131和WAP371接入点上配置VAP。

适用设备

·WAP351

·WAP131

·WAP371

软件版本

·V1.0.0.39(WAP351)

·V1.0.0.39(WAP131)

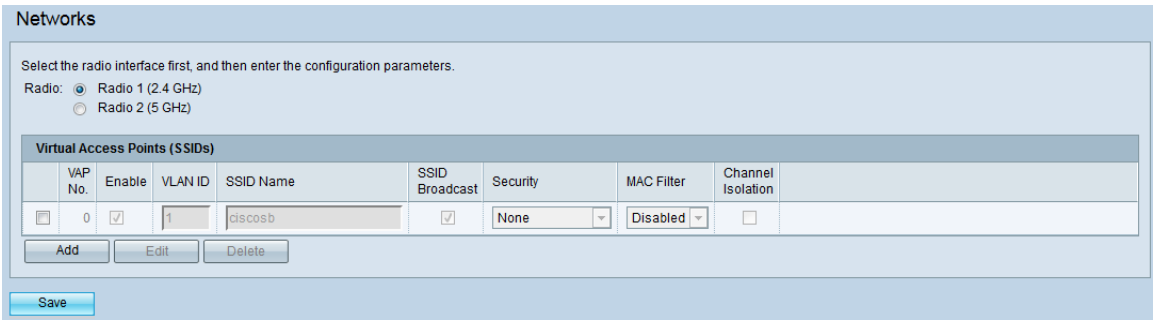
·V1.2.0.2(WAP371)

添加和配置VAP

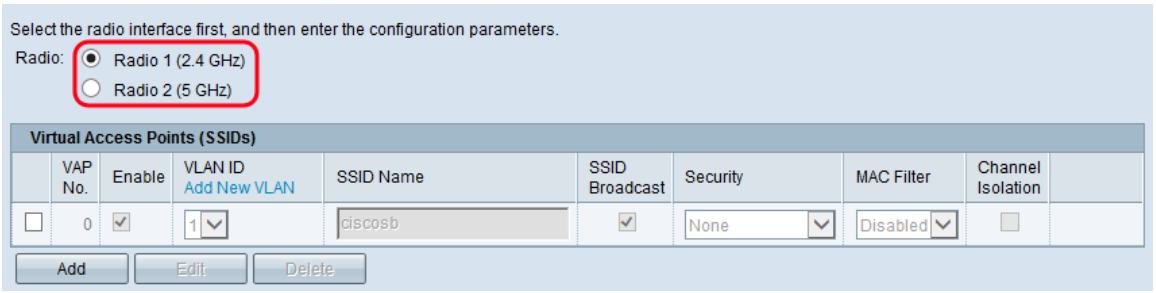
注意：每个VAP由用户配置的服务集标识符(SSID)标识。 多个VAP不能具有相同的SSID名称。

注意：要使无线网络正常运行，必须启用并正确配置已配置的VAP关联的无线电。有关详细信息，请参阅*在WAP131和WAP351上配置基本无线电设置*或*在WAP371上配置基本无线电设置*

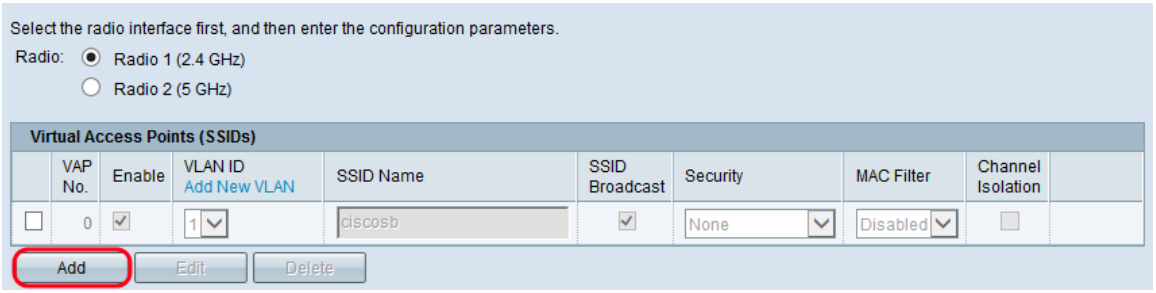
步骤1.登录Web配置实用程序并导航至**Wireless > Networks**。系统将显示*Networks*页面：



步骤2.在*Radio*字段中，为要在其上配置VAP的无线电选择单选按钮。

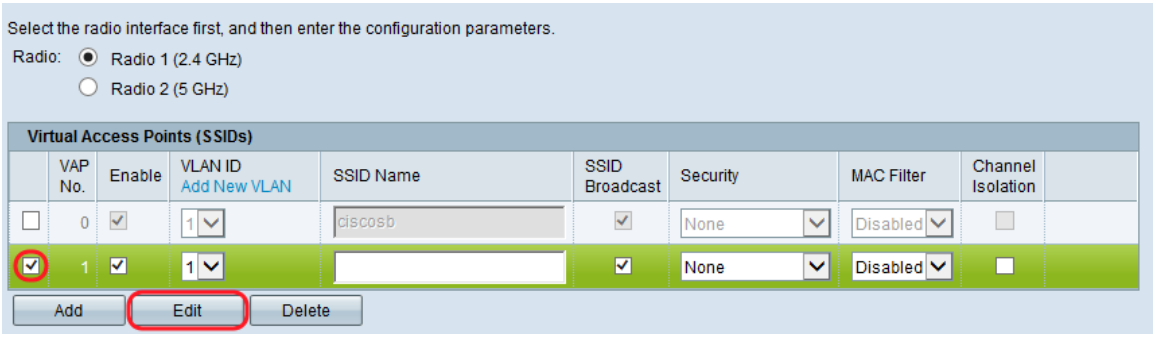


步骤3.要添加新VAP，请单击**Add**。表中将显示一个新VAP。

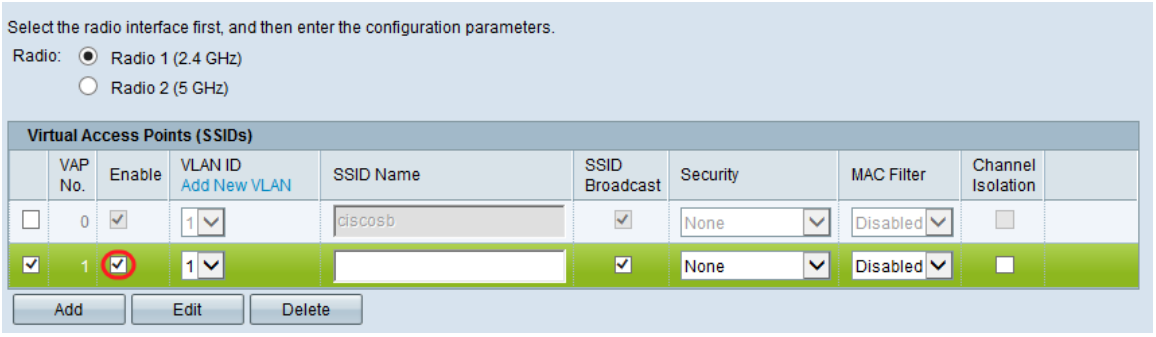


注意：WAP131支持最多4个VAP，而WAP371和WAP351支持最多8个VAP。

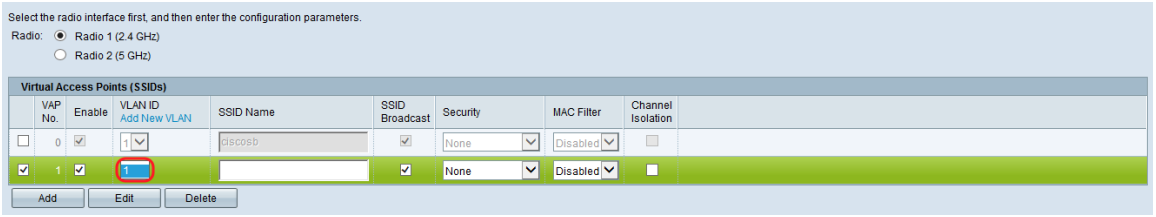
步骤4.要开始编辑VAP，请单击表条目最左侧的复选框，然后单击“编辑”。这将允许您修改所选VAP的灰显字段。



步骤5.要启用VAP的使用，请确保选中*Enable*复选框。

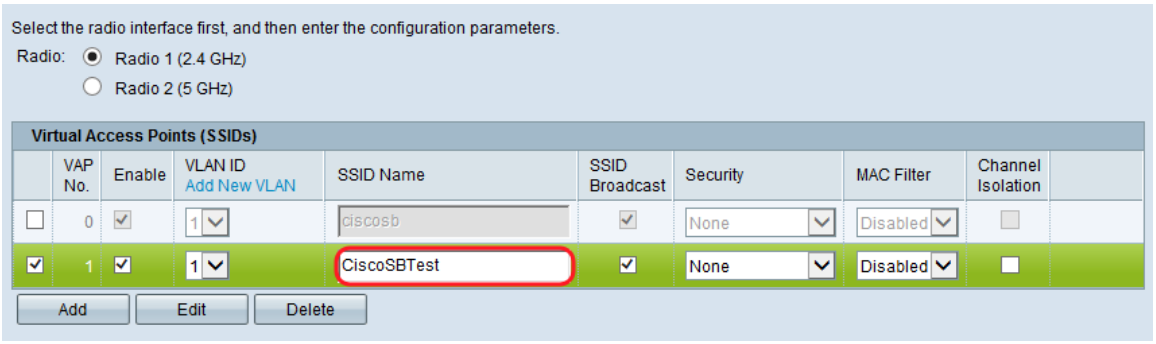


步骤6.在*VLAN ID*字段中，指定要与VAP关联的VLAN ID。如果使用WAP131或WAP371，请输入VLAN ID。您可以输入的最大值为4094。

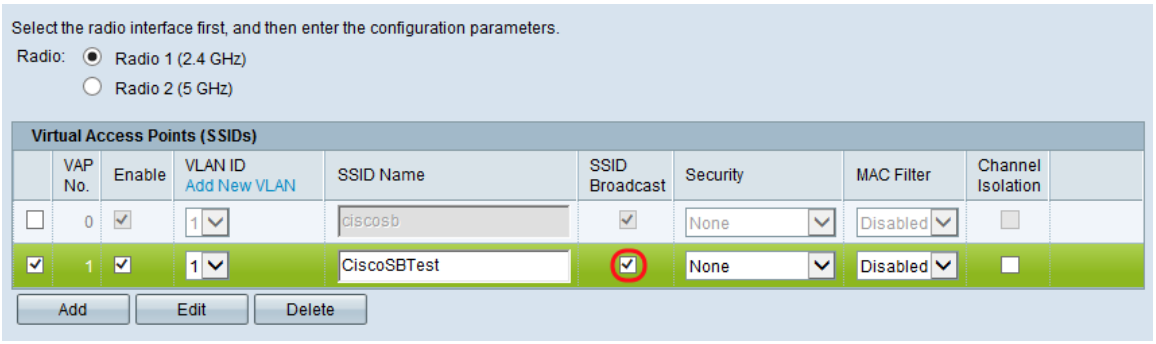


注意：输入的VLAN ID必须存在于您的网络中，并且必须正确配置。有关详细信息，*请参阅WAP351接入点上的VLAN配置*、*管理WAP131上的标记和无标记VLAN ID*或*管理WAP371上的标记和无标记VLAN ID*。

步骤7.在SSID Name字段中输入无线网络的名称。每个VAP必须具有唯一的SSID名称。

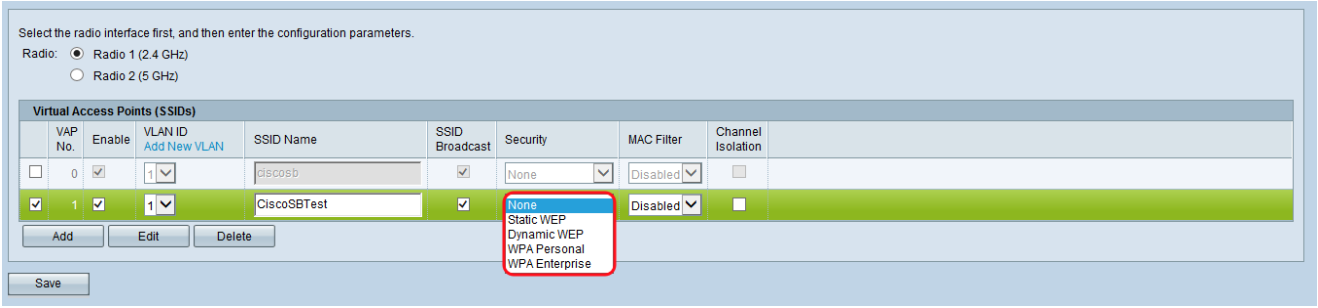


步骤8.如果要向客户端广播SSID名称，请选中*SSID Broadcast*复选框。这将向客户端显示其可用网络列表中的SSID名称。



配置安全设置

步骤1.从*Security*下拉列表中选择连接VAP所需的身份验证方法。如果选择了除“无”之**外的任**何选项，将显示其他字段。



可用选项如下：

- 无
- 静态 WEP
- 动态 WEP
- WPA个人
- WPA企业

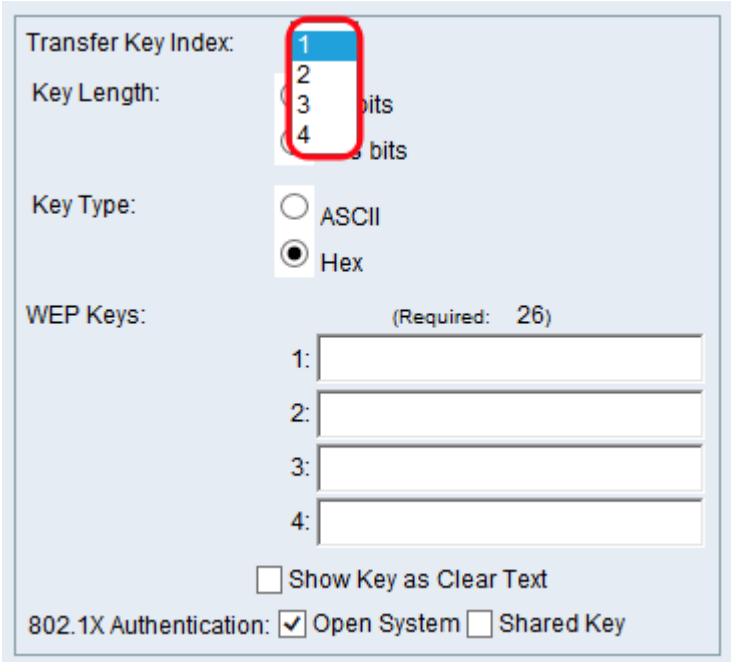
注意：WPA个人和WPA企业是最高安全性的首选身份验证类型。静态WEP和动态WEP应仅用于传统设备，并要求无线电设置为802.11a或802.11b/g模式。有关详细信息，请参阅*在WAP131和WAP351上配置基本无线电设置*或*在WAP371上配置基本无线电设置*。

静态 WEP

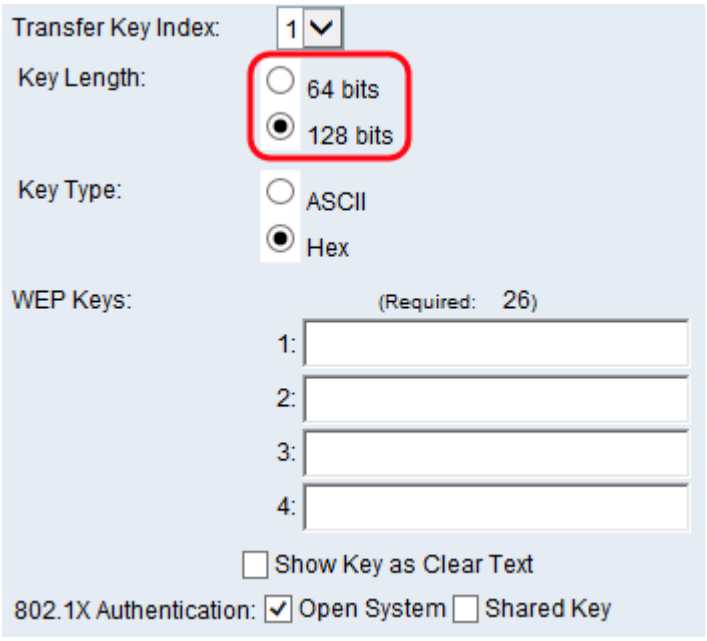
静态WEP是最不安全的身份验证方法。它根据静态密钥加密无线网络中的数据。非法获取此静态密钥已变得简单，因此WEP身份验证应仅在必要时用于传统设备。

注意：选择"*静态WEP"作*为您的安全方法时，系统会显示提示，提示您您的安全方法选择非常不安全。

步骤1.在*传输密钥索引*下拉列表中，从设备用于加密数据的密钥列表中选择WEP密钥的索引。

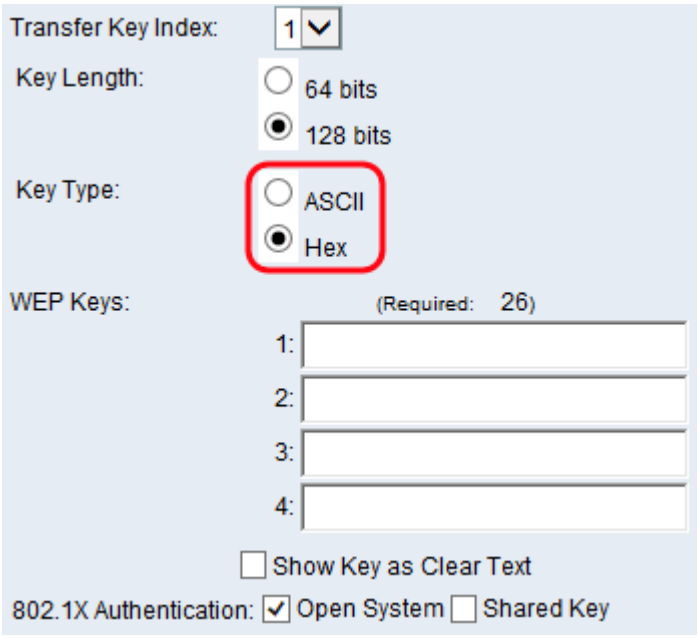


步骤2.从Key Length字段中选择单选*按钮*，以指定密钥的长度是64位还是128位。

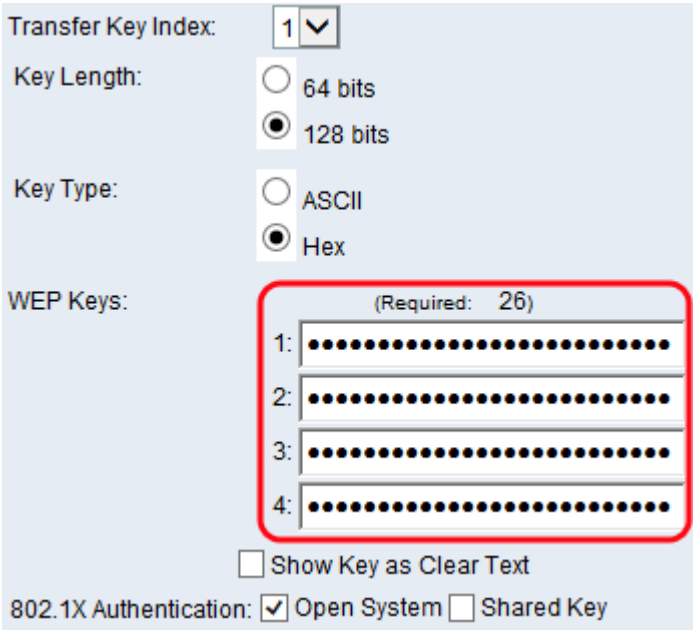


步骤3.在Key Type(*密钥类型*)字段中，选择要输入ASCII或十六进制格式的密钥。ASCII包含键

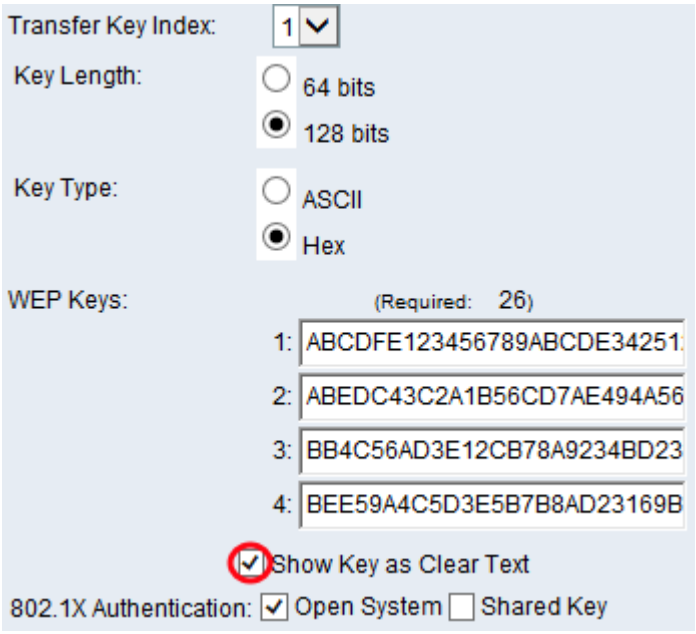
盘上的所有字母、数字和符号，而十六进制只能使用数字或字母A-F。



步骤4.在“WEP*密钥*”字段中，为设备输入最多4个不同的WEP密钥。每个要连接到此网络的客户端必须在设备指定的同一插槽中具有相同的WEP密钥之一。

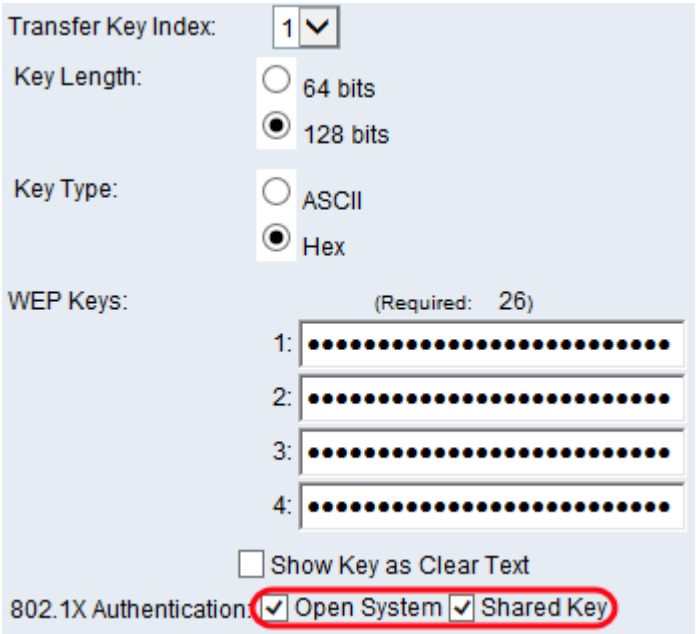


步骤5.（可选）如果显示键的字符串，请*单击Show Key as Clear Text*字段中的复选框。



注意：当在WAP351、WAP131或WAP371上使用不同的固件时，*Show Key as Clear Text*字段可能丢失。

步骤6.在*802.1X Authentication*字段中，通过选择“开放系统”和/或“共享密钥”选项，*指定要使用的身份验*证算法。当静态WEP是安全模式时，身份验证算法定义了用于确定客户端站点是否允许与WAP设备关联的方法。



可用选项定义如下：

·开放系统 — 无论客户端站点是否具有正确的WEP密钥，身份验证都允许任何客户端站点与WAP设备关联。此算法用于纯文本、IEEE 802.1X和WPA模式。当身份验证算法设置为*Open System*时，任何客户端都可以与WAP设备关联。

·共享密钥 — 身份验证要求客户端站点拥有正确的WEP密钥，以便与WAP设备关联。当身份验证算法设置为*共享密*钥时，WEP密钥不正确的站点无法与WAP设备关联。

·Open System and Shared Key — 当您选择了这两种身份验证算法时，配置为在共享密钥模式下使用WEP的客户端站必须具有有效的WEP密钥才能与WAP设备关联。此外，配置为使用WEP作为开放系统（未启用共享密钥模式）的客户端站点可以与WAP设备关联，即使它

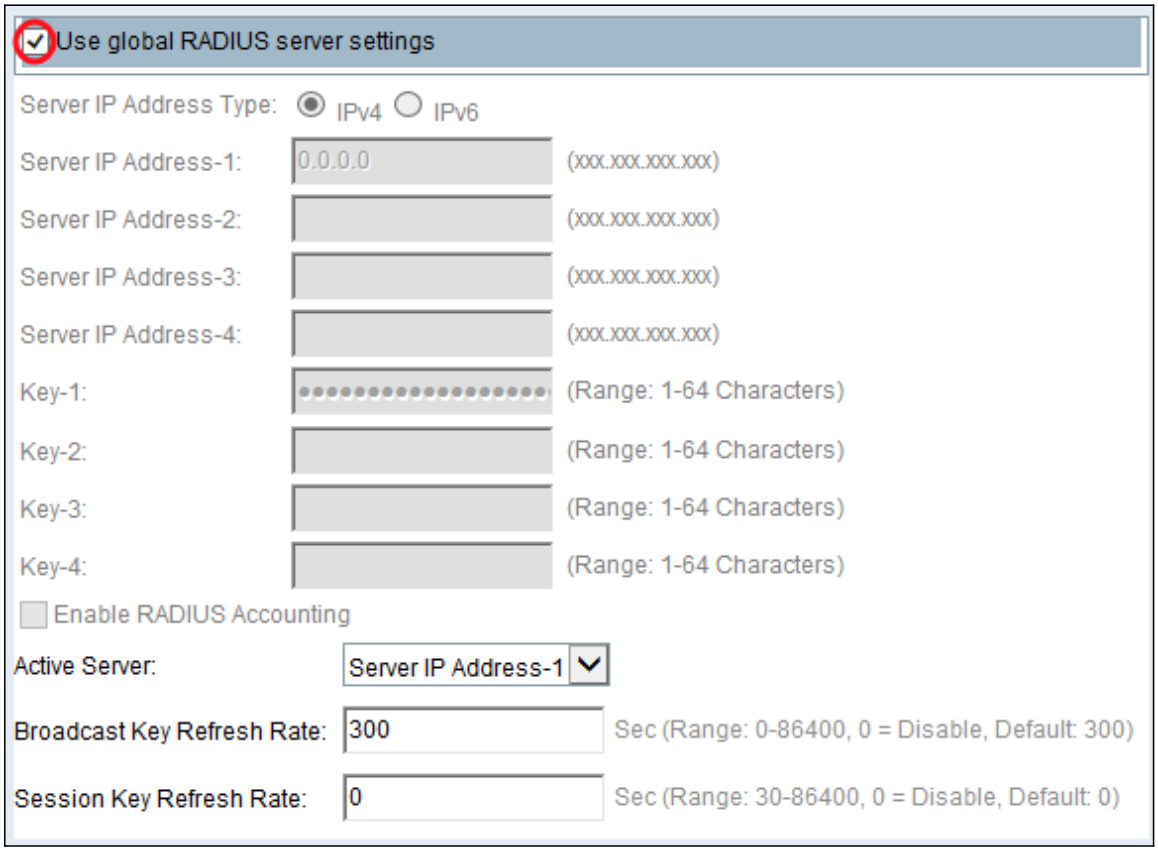
们没有正确的WEP密钥。

步骤7.单击“**保存**”。

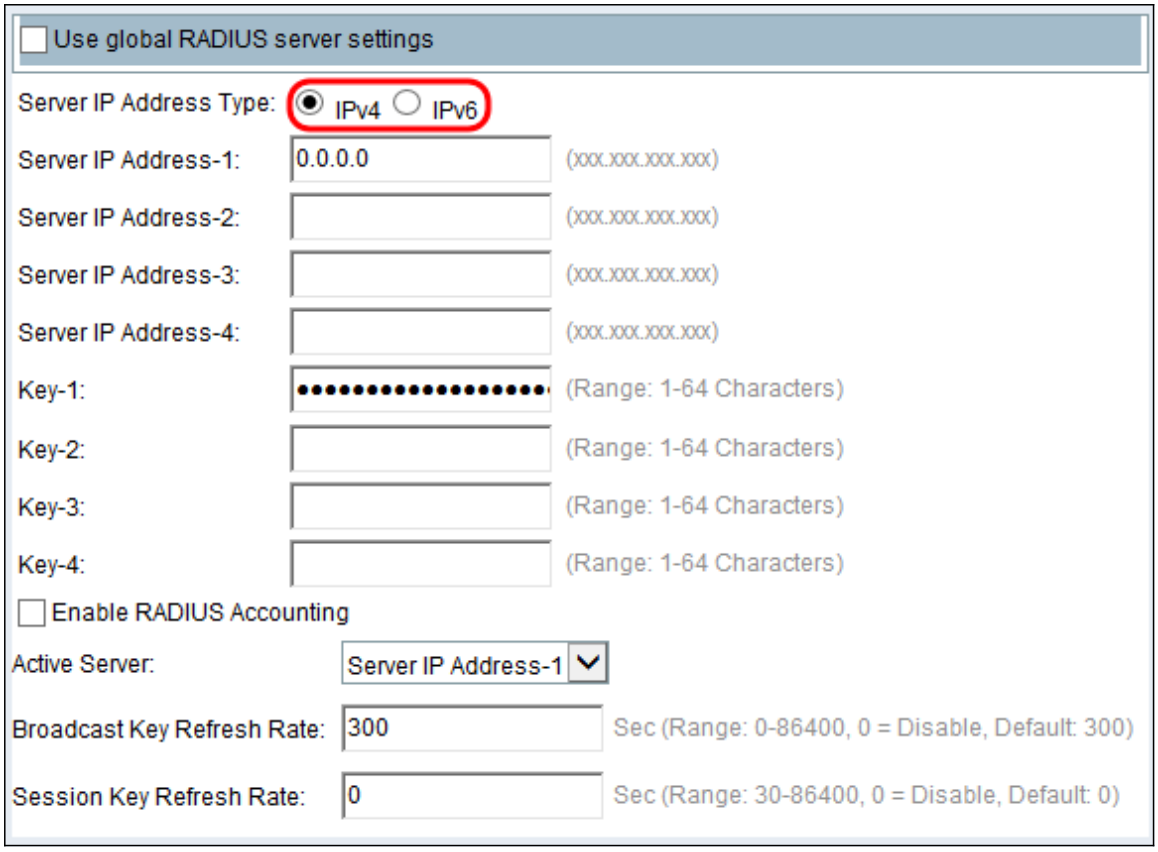
动态 WEP

动态WEP是指802.1x技术和可扩展身份验证协议(EAP)的组合。 此模式需要使用外部RADIUS服务器对用户进行身份验证。WAP设备需要支持EAP的RADIUS服务器，例如Microsoft Internet Authentication Server。要与Microsoft Windows客户端配合使用，身份验证服务器必须支持受保护的EAP(PEAP)和MSCHAP v2。您可以使用IEEE 802.1X模式支持的各种身份验证方法，包括证书、Kerberos和公钥身份验证，但必须配置客户端站点使用与WAP设备相同的身份验证方法。

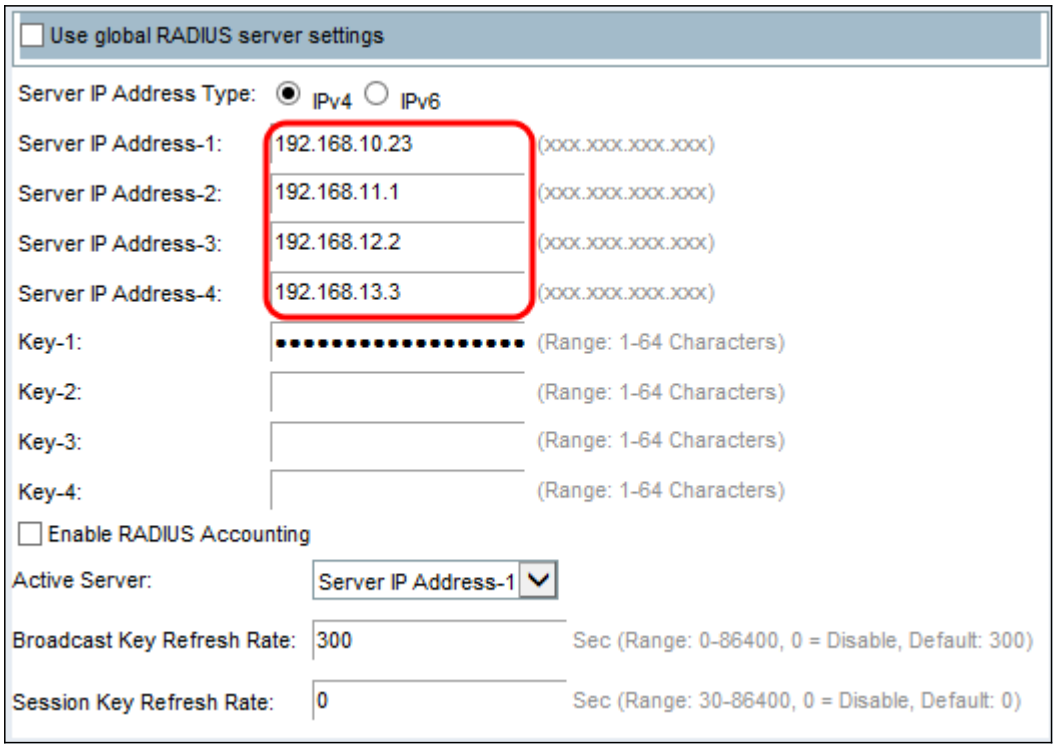
步骤1.默认情况下，选中*Use global RADIUS服务器*设置。如果要将VAP配置为使用不同的RADIUS服务器集，请取消选中此复选框。否则，请跳至步骤8。



步骤2.在Server IP Address Type字*段中，选*择WAP设备使用的服务器IP地址类型。选项是*IPv4*或*IPv6*。IPv4使用点分十进制记法表示的32位二进制数。IPv6使用十六进制数和冒号来表示128位二进制数。WAP设备仅联系RADIUS服务器或服务器，了解您在此字段中选择的地址类型。如果选择IPv6，则跳至步骤4。

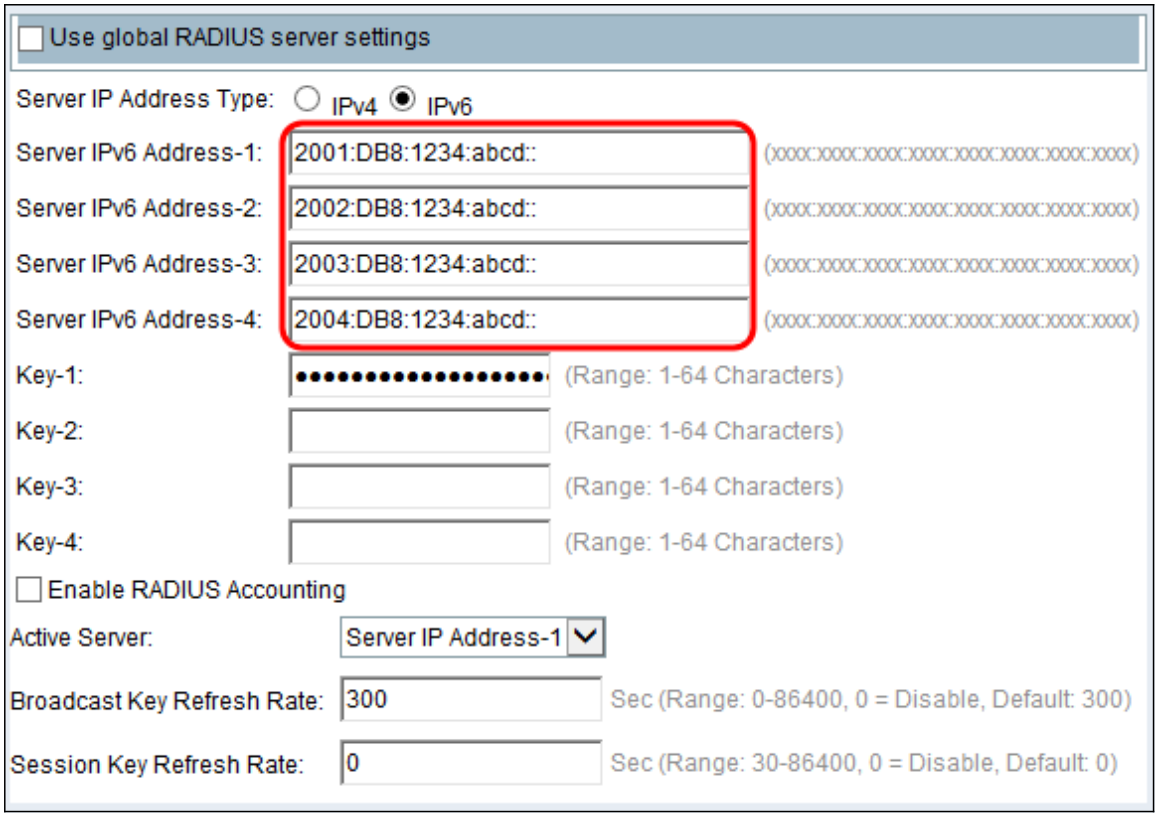


步骤3.如果在步骤2**中选**择了IPv4，请输入默认所有VAP使用的RADIUS服务器的IP地址。然后跳至步骤5。



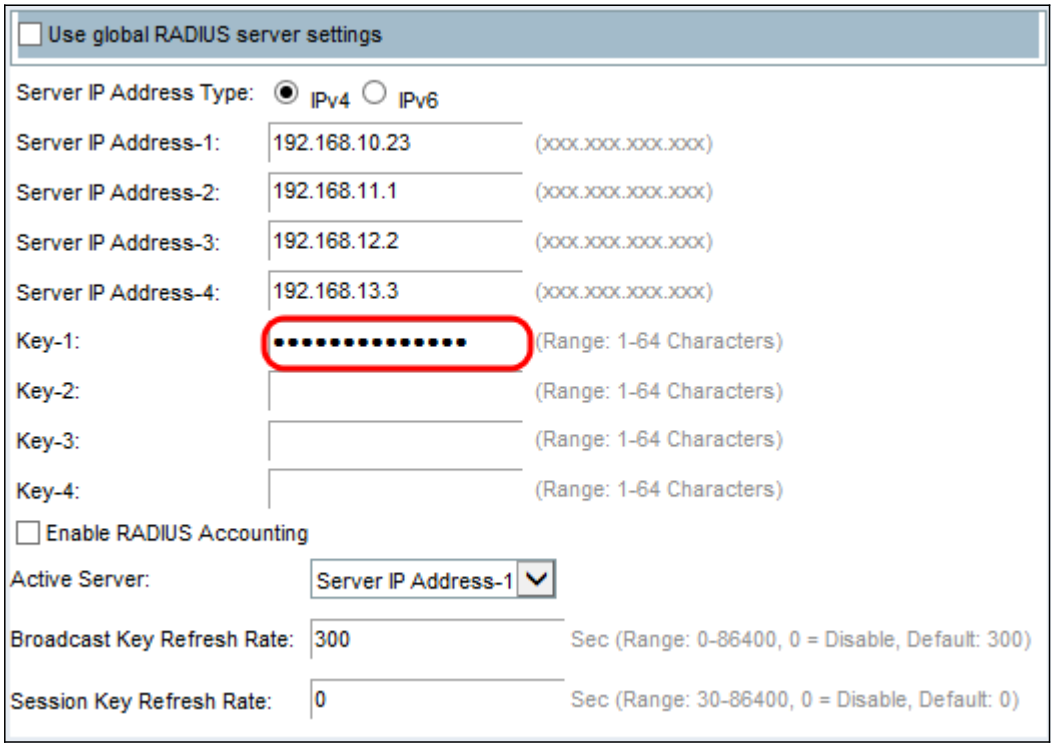
注意：您最多可以有三个IPv4备份RADIUS服务器地址。如果主服务器的身份验证失败，则会按顺序尝试每个已配置的备份服务器。

步骤4.如果已在步**骤2中**选择了IPv6，请输入主全局RADIUS服务器的IPv6地址。

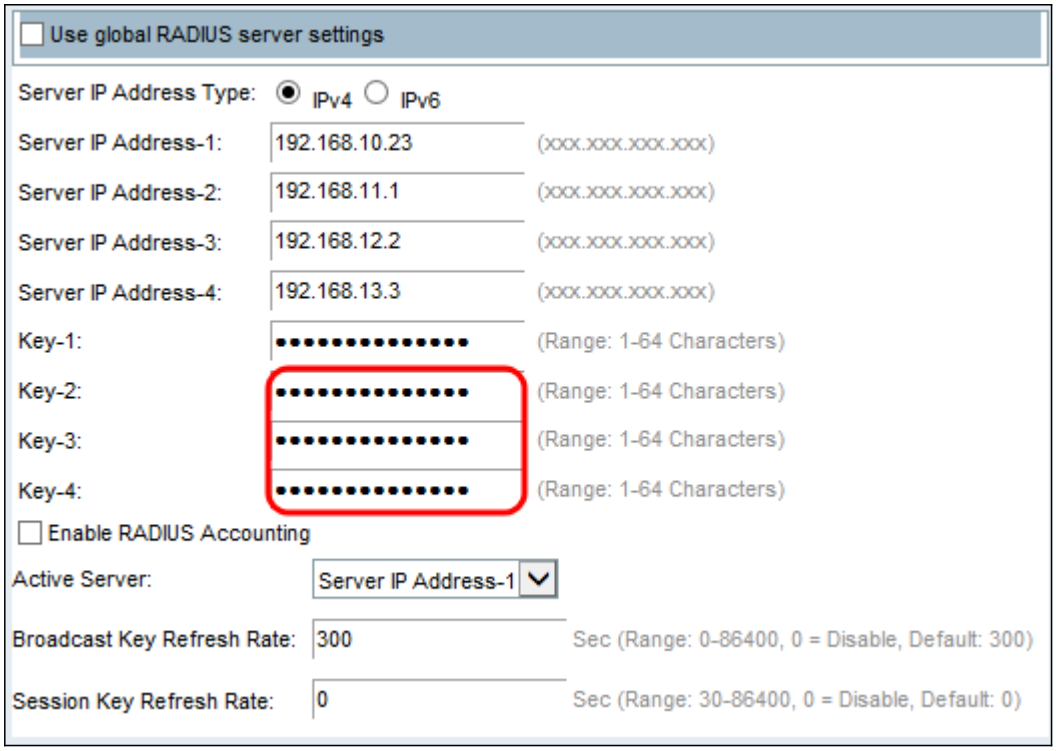


注意：您最多可以有三个IPv6备份RADIUS服务器地址。如果主服务器的身份验证失败，则会按顺序尝试每个已配置的备份服务器。

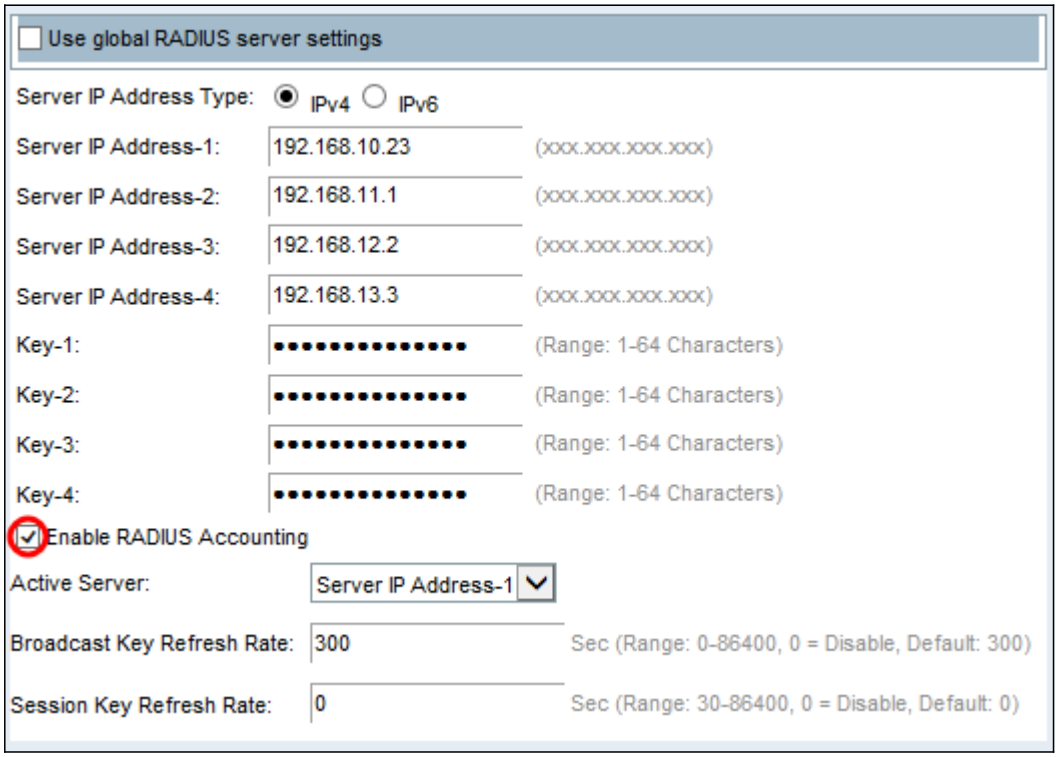
步骤5.在*Key-1*字段中，输入WAP设备用于向主RADIUS服务器进行身份验证的共享密钥。



步骤6.在*Key-2* 到*Key-4* 字段中，输入与已配置的备份RADIUS服务器关联的RADIUS密钥。服务器IP地址2使*用Key-2*，服务器IP地址3使*用Key-*3，服务器IP地址4使*用Key-4*。

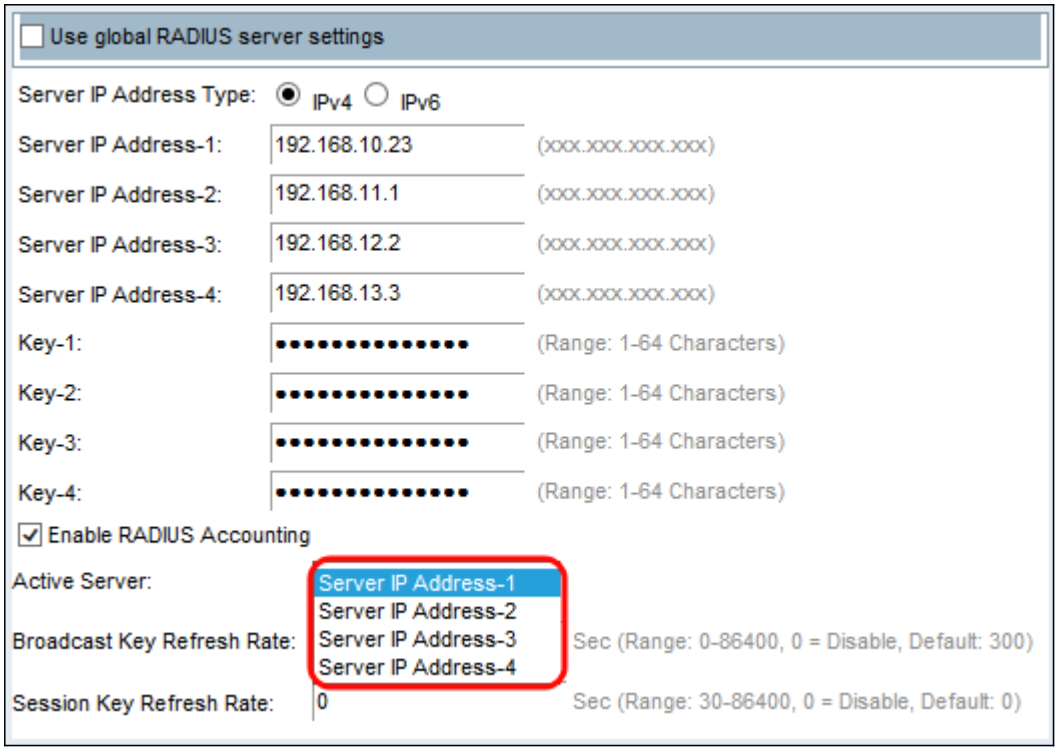


第7步。（可选）在*启用RADIUS记帐*字段中，如果要启用跟踪和测量特定用户消耗的资源，请选中此复选框。启用RADIUS记帐将跟踪系统时间以及发送和接收的数据量。信息将存储在Radius服务器中。这将为主RADIUS服务器和所有备份服务器启用。

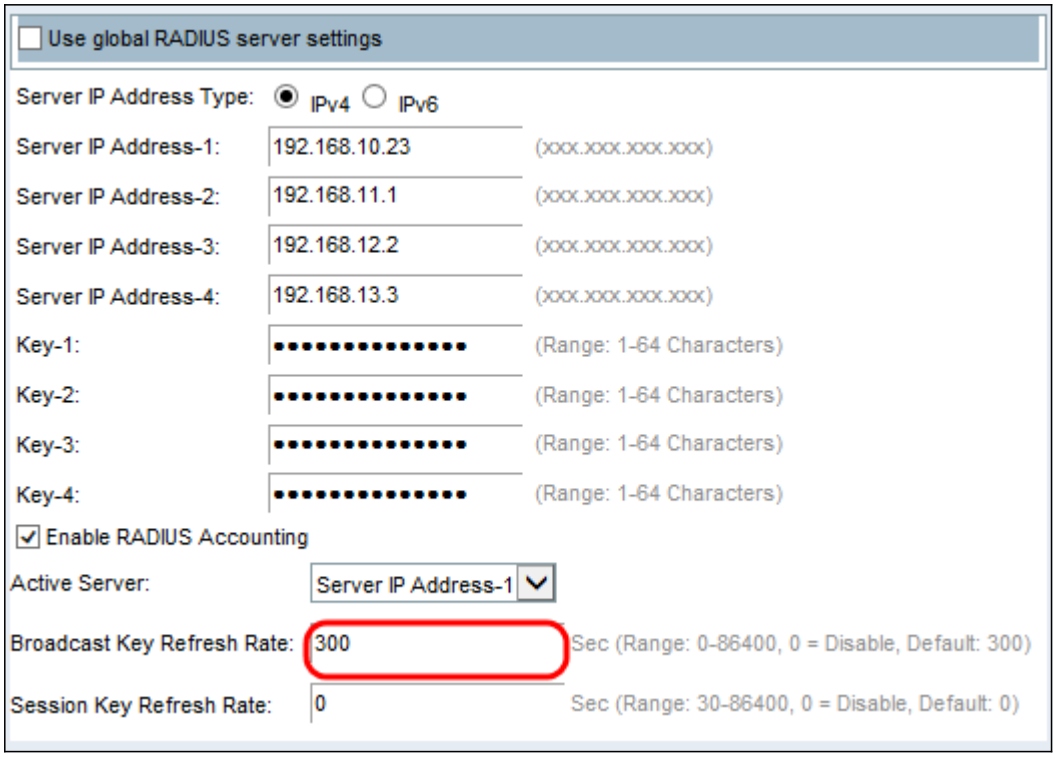


注意：如果启用了RADIUS记帐，则会为主RADIUS服务器和所有备份服务器启用

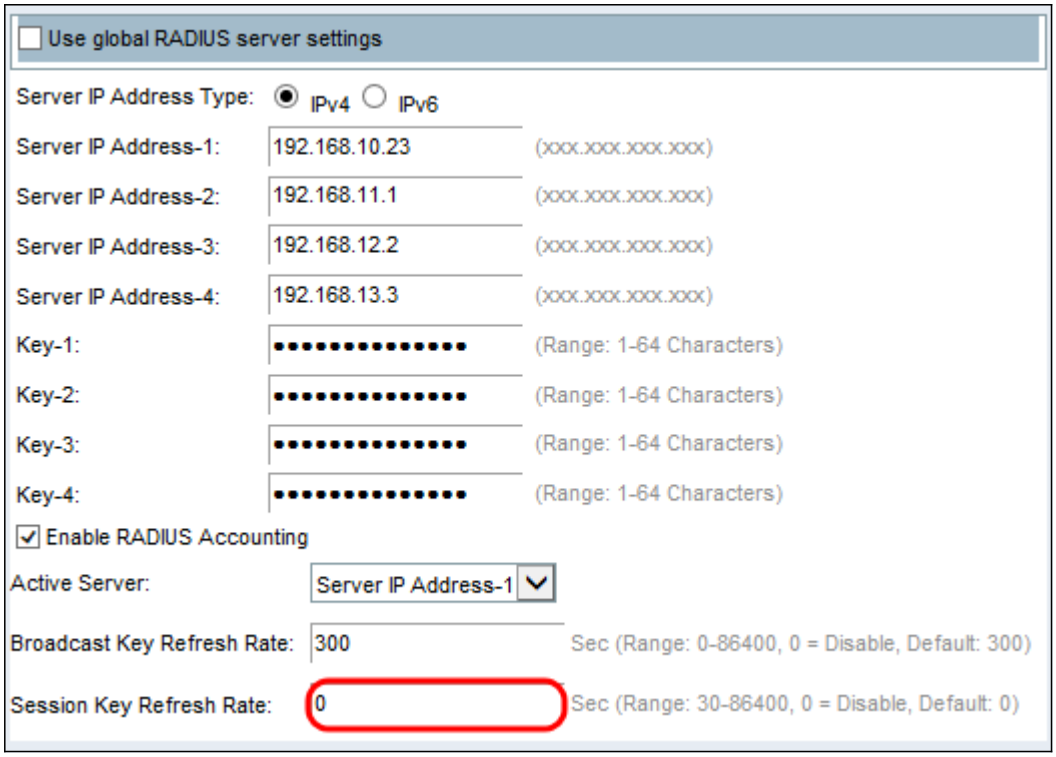
步骤8.在Active Server字段中选择第一个处于活动状态*的服*务器。这允许手动选择活动RADIUS服务器，而不是让WAP设备尝试按顺序联系每个已配置的服务器并选择第一个处于活动状态的服务器。



步骤9.在Broadcast Key Refresh Rate字*段中，输入与此VAP关联的客户端的广播（组）密钥刷新间隔。*默认时间为 300 秒钟。



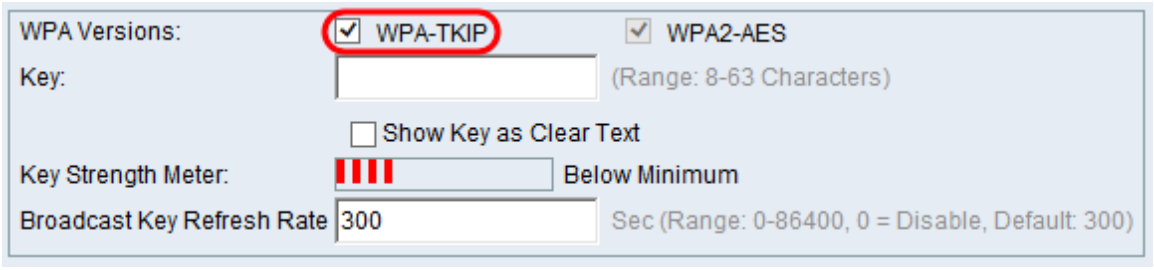
步骤10.在Session Key Refresh Rate字*段中，输入WAP设备刷新与VAP关联的每个客户端的会话（单播）密钥的间隔。*默认值为 0。



WPA个人

WPA个人是Wi-Fi联盟IEEE 802.11i标准，包括AES-CCMP和TKIP加密。WPA使用预共享密钥(PSK)，而不是使用IEEE 802.1X和EAP（在企业WPA安全模式中使用）。PSK仅用于凭证的初始检查。WPA也称为WPA-PSK。此安全模式对于支持原始WPA的无线客户端向后兼容。

步骤1.如果要启*用WPA-TKIP*，请在WPA Versions字*段中选中WPA-TKIP*复选框。您可以同时启用WPA-TKIP和WPA2-AES。WAP始终支持WPA2-AES，因此您无法配置它。



可用选项定义如下：

·WPA-TKIP — 网络中有一些客户端站点仅支持原始WPA和TKIP安全协议。根据最新的WiFi联盟要求，不建议仅选择WPA-TKIP。

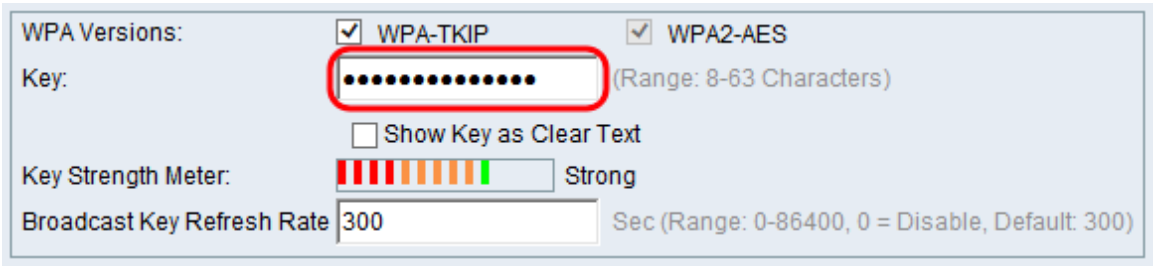
·WPA2-AES — 网络上的所有客户端站点都支持WPA2和AES-CCMP密码/安全协议。此WPA版本根据IEEE 802.11i标准提供最佳安全性。根据最新的WiFi联盟要求，AP必须始终支持此模式。

·WPA-TKIP和WPA2-AES — 如果网络有客户端的混合，其中一些支持WPA2，而其他仅支持原始WPA，请选中这两个复选框。此设置允许WPA和WPA2客户端站点关联和验证，但对支持它的客户端使用更强健的WPA2。此WPA配置允许更多的互操作性，而不是某些安全性。

注意：WPA客户端必须具有其中一个密钥（有效TKIP密钥或有效AES-CCMP密钥）才能与

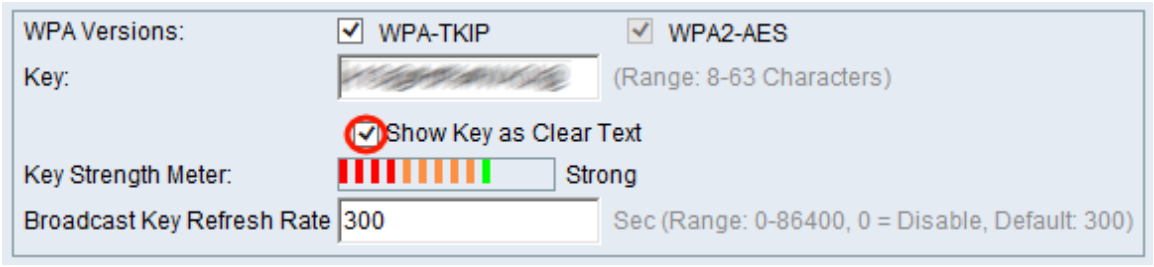
WAP设备关联。

步骤2.在“密钥”字段中，输入用于WPA个人安全的共享密钥。输入至少8个字符，最多63个字符。



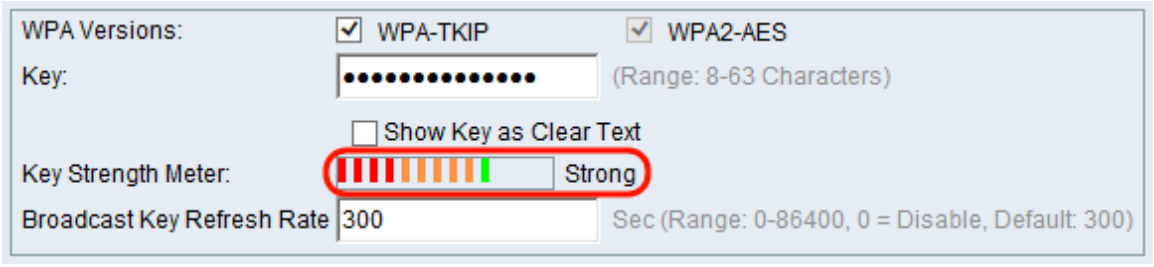
注意：可接受的字符包括大写和小写字母、数字和特殊符号(?!/\@#$%^&*)。

步骤3.（可选）如果希望键入的文*本可见，请选*中Show Key as Clear Text复选框。默认情况下，该复选框处于未选中状态。

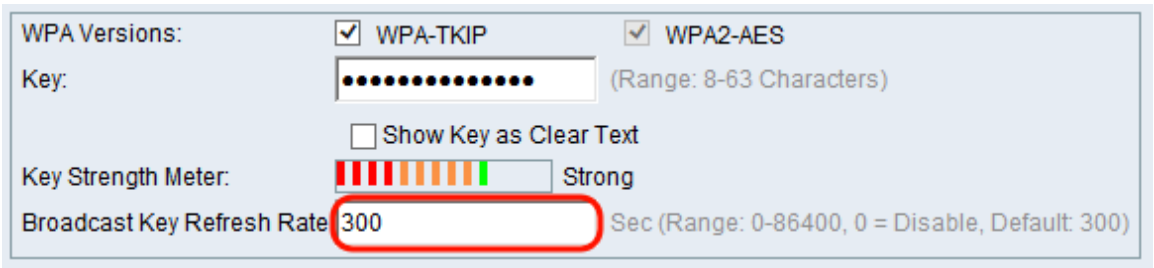


注意：当在WAP351、WAP131或WAP371上使用不同的固件时，*Show Key as Clear Text*字段可能丢失。

注意：Key *Strength Meter字段*是WAP设备根据复杂性标准检查密钥的位置，这些复杂性标准包括使用多少种不同类型的字符以及密钥的长度。如果启用WPA-PSK复杂性检查功能，则除非密钥满足最低条件，否则不接受该密钥。有关WPA-PSK复杂性的详细信息，*请参阅*为WAP131、WAP351和WAP371配置密码复杂性。



步骤4.在Broadcast Key Refresh Rate字*段中，输入与此VAP关联的客户端的广播（组）密钥刷新间隔*。默认时间为 300 秒钟。

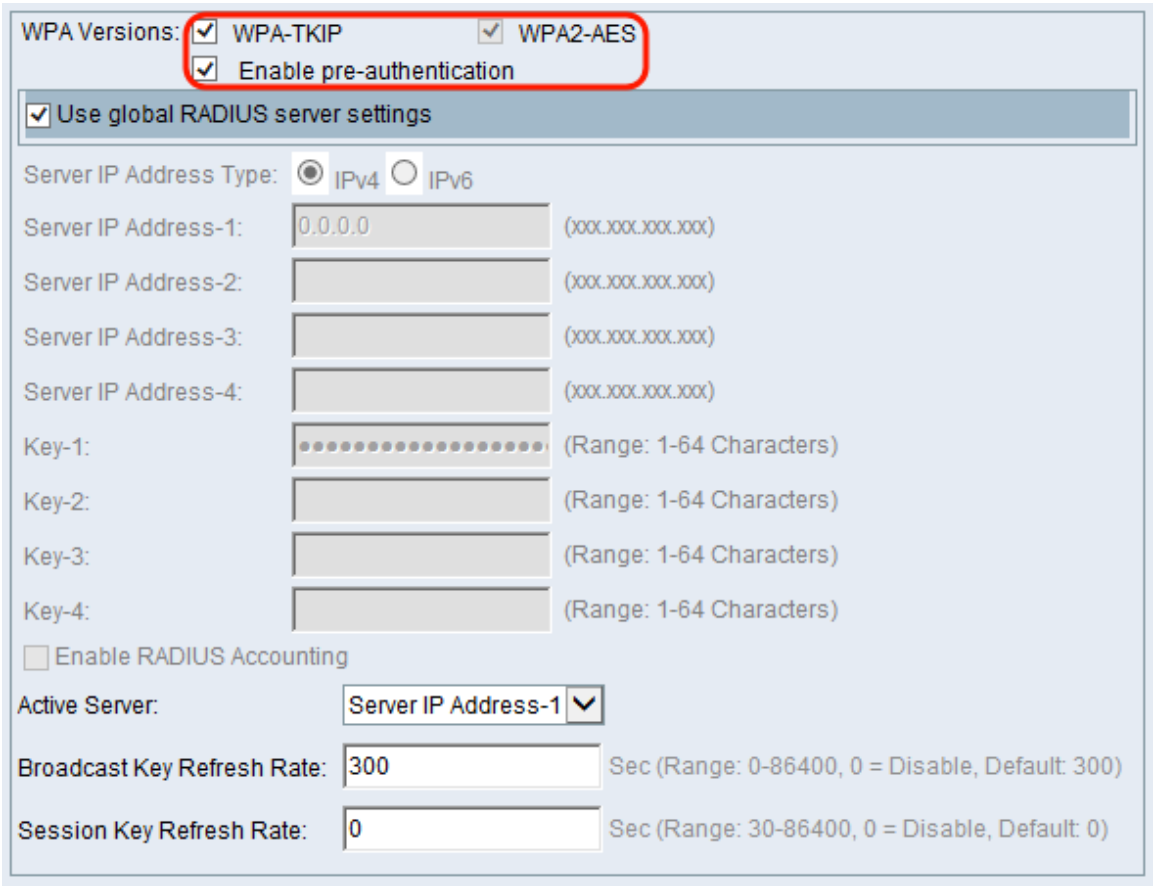


WPA企业

WPA企业版RADIUS是Wi-Fi联盟IEEE 802.11i标准的实施，包括CCMP(AES)和TKIP加密。企业模式需要使用RADIUS服务器对用户进行身份验证。安全模式向后兼容支持原始WPA的无线客户端。

注意：默认情况下，动态VLAN模式处于启用状态，这允许RADIUS身份验证服务器决定站点使用哪个VLAN。

步骤1.在“WPA版本”字段中，选中要支持的客户端工作站类型的复选框。默认情况下，它们都处于启用状态。AP必须始终支持WPA2-AES，因此您无法配置它。



可用选项定义如下：

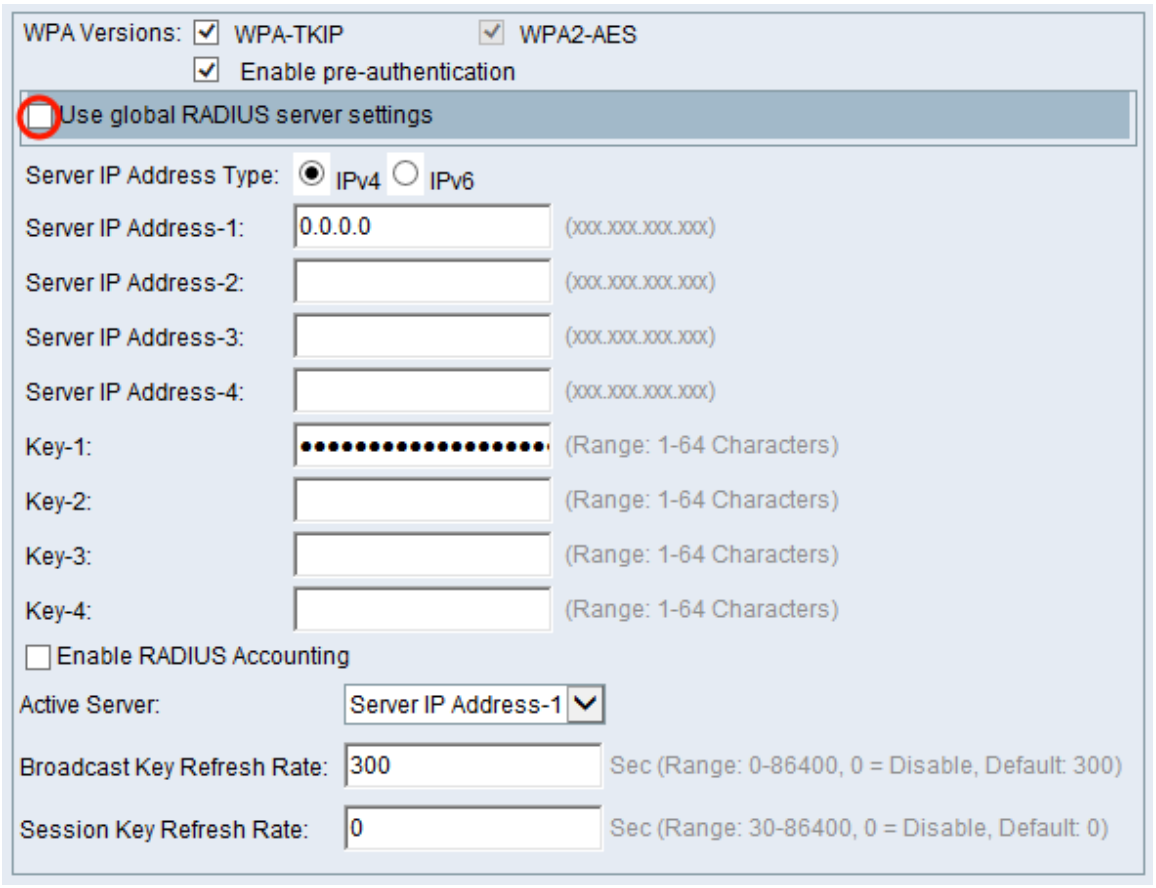
·WPA-TKIP — 网络中有一些客户端站点仅支持原始WPA和TKIP安全协议。请注意，根据最新的WiFi联盟要求，不允许为接入点仅选择WPA-TKIP。

·WPA2-AES — 网络上的所有客户端站点都支持WPA2版本和AES-CCMP密码/安全协议。此WPA版本提供符合IEEE 802.11i标准的最佳安全性。根据最新的Wi-Fi联盟要求，WAP必须始终支持此模式。

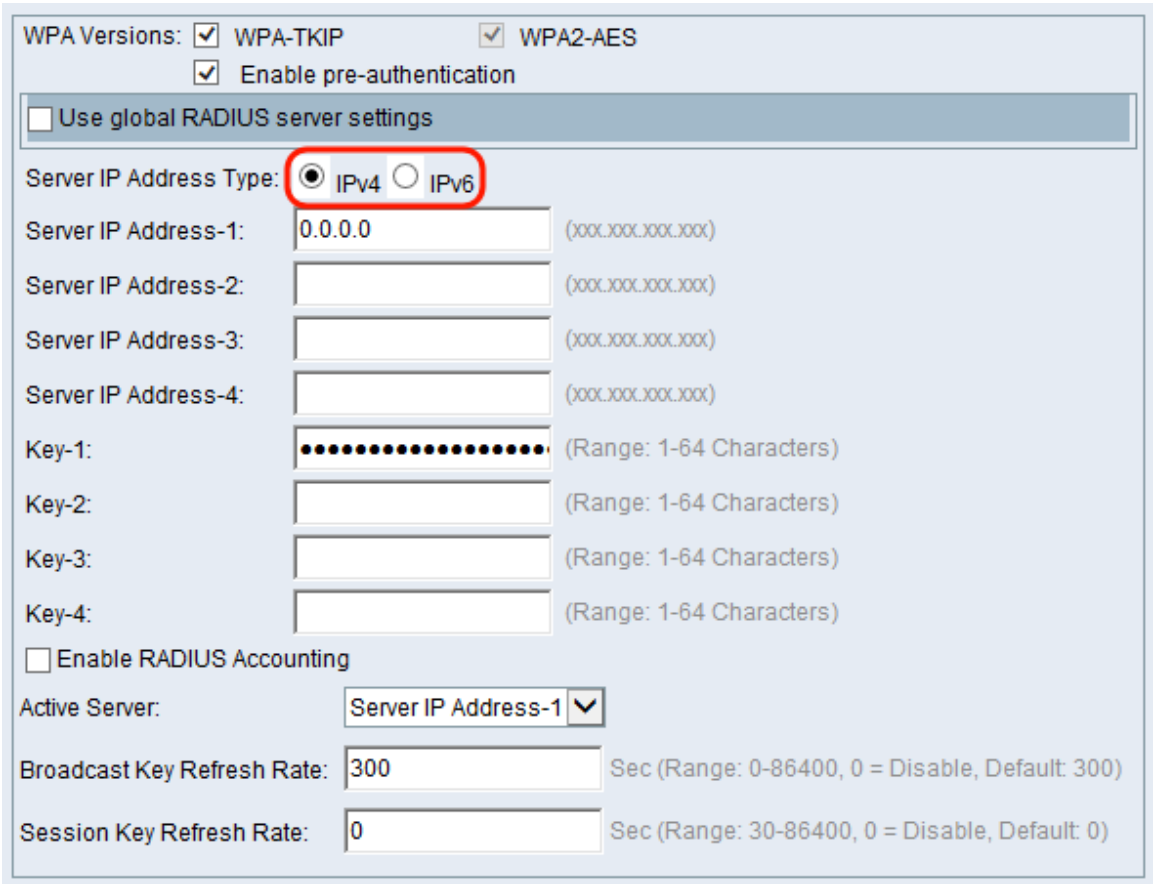
·启用预身份验证 — 如果只选择WPA2或WPA和WPA2作为WPA版本，则可以为WPA2客户端启用预身份验证。如果希望WPA2无线客户端发送预身份验证数据包，请选中此选项。预身份验证信息从客户端当前使用的WAP设备中继到目标WAP设备。启用此功能有助于加快连接到多个WAP的漫游客户端的身份验证。如果您为WPA版本选择了WPA，则此选项不适用，因为原始WPA不支持此功能。

注意：配置为使用WPA和RADIUS的客户端工作站必须具有以下地址和密钥之一：有效的TKIP RADIUS或有效的CCMP(AES)IP地址和RADIUS密钥。

步骤2.默认情况下，选中*Use global RADIUS服务器*设置。如果要将VAP配置为使用不同的RADIUS服务器集，请取消选中此复选框。否则，请跳至步骤9。

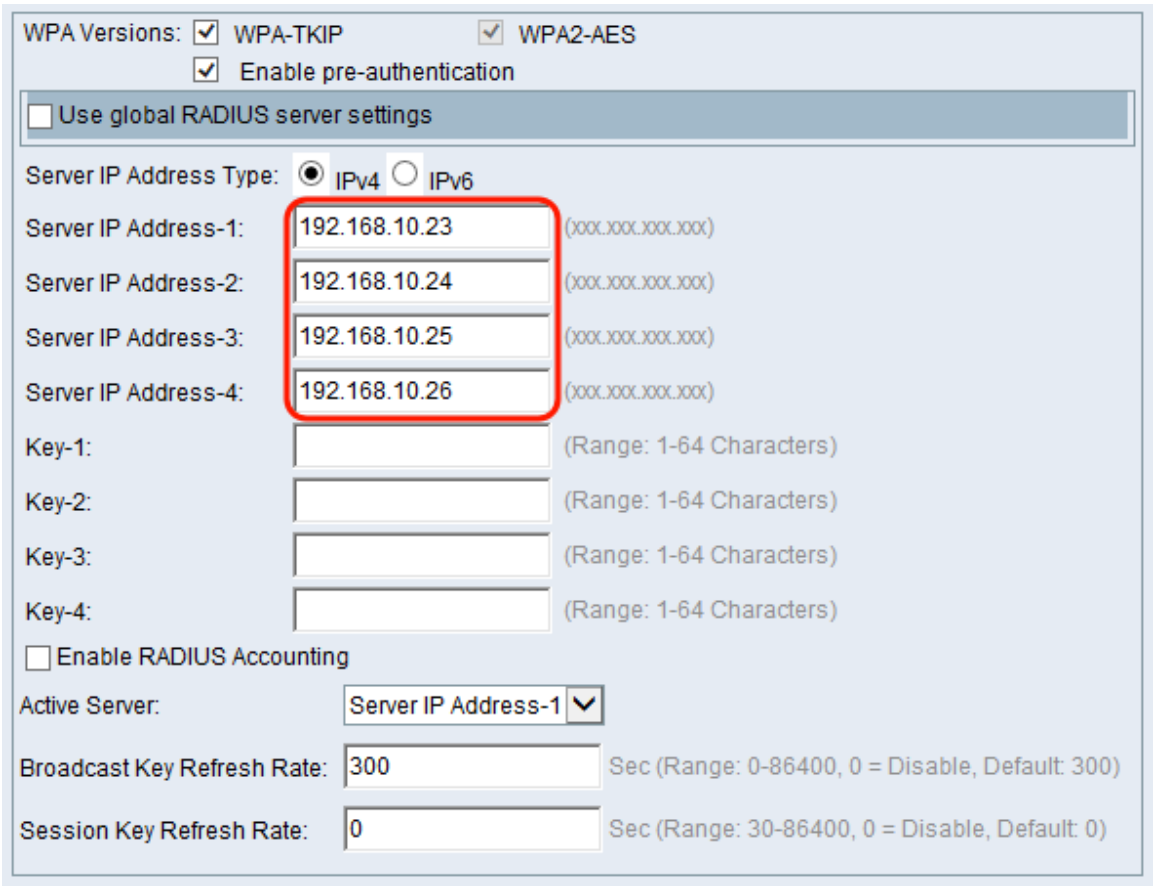


步骤3.在Server IP Address Type字*段中，选*择WAP设备使用的服务器IP地址类型。选项是*IPv4*或*IPv6*。IPv4使用点分十进制记法表示的32位二进制数。IPv6使用十六进制数和冒号来表示128位二进制数。WAP设备仅联系RADIUS服务器或服务器，了解您在此字段中选择的地址类型。



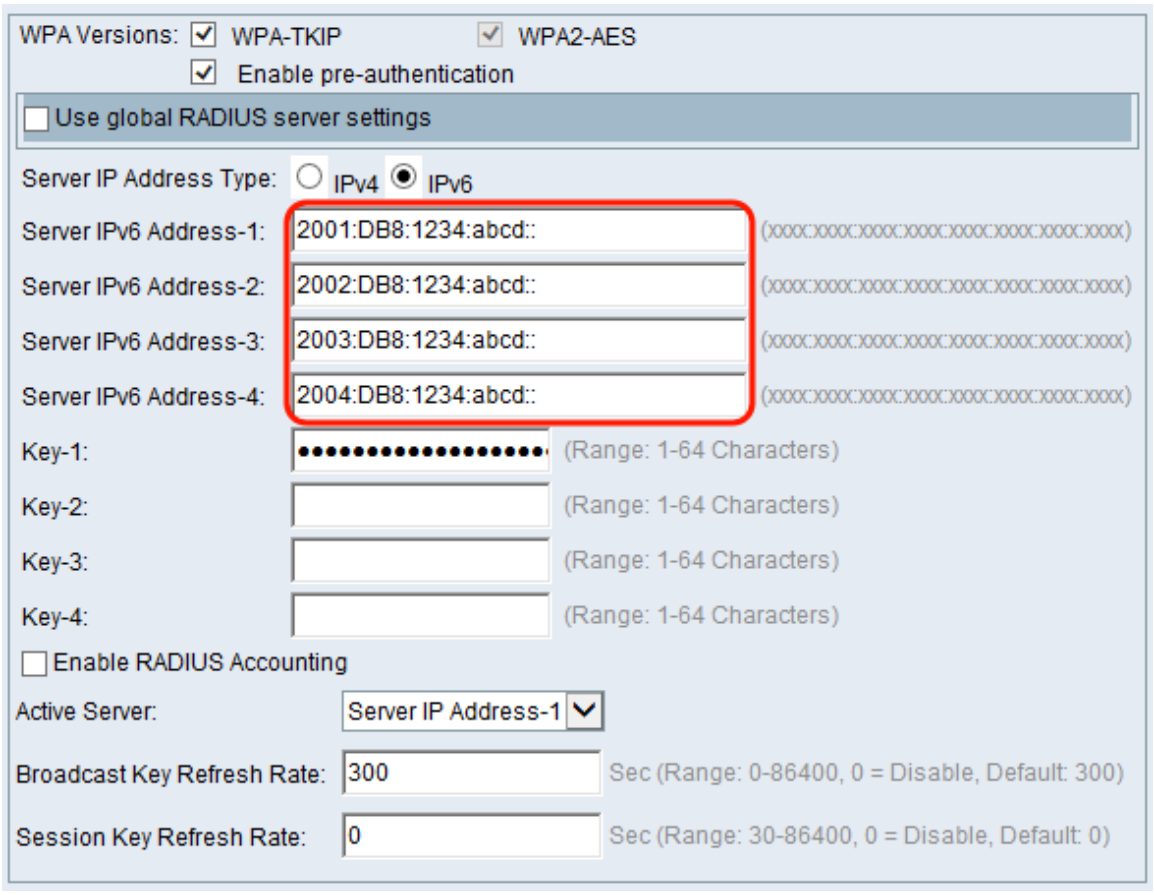
步骤4.如果在步骤2**中选**择了IPv4，请输入默认所有VAP使用的RADIUS服务器的IP地址。然

后跳至步骤6。



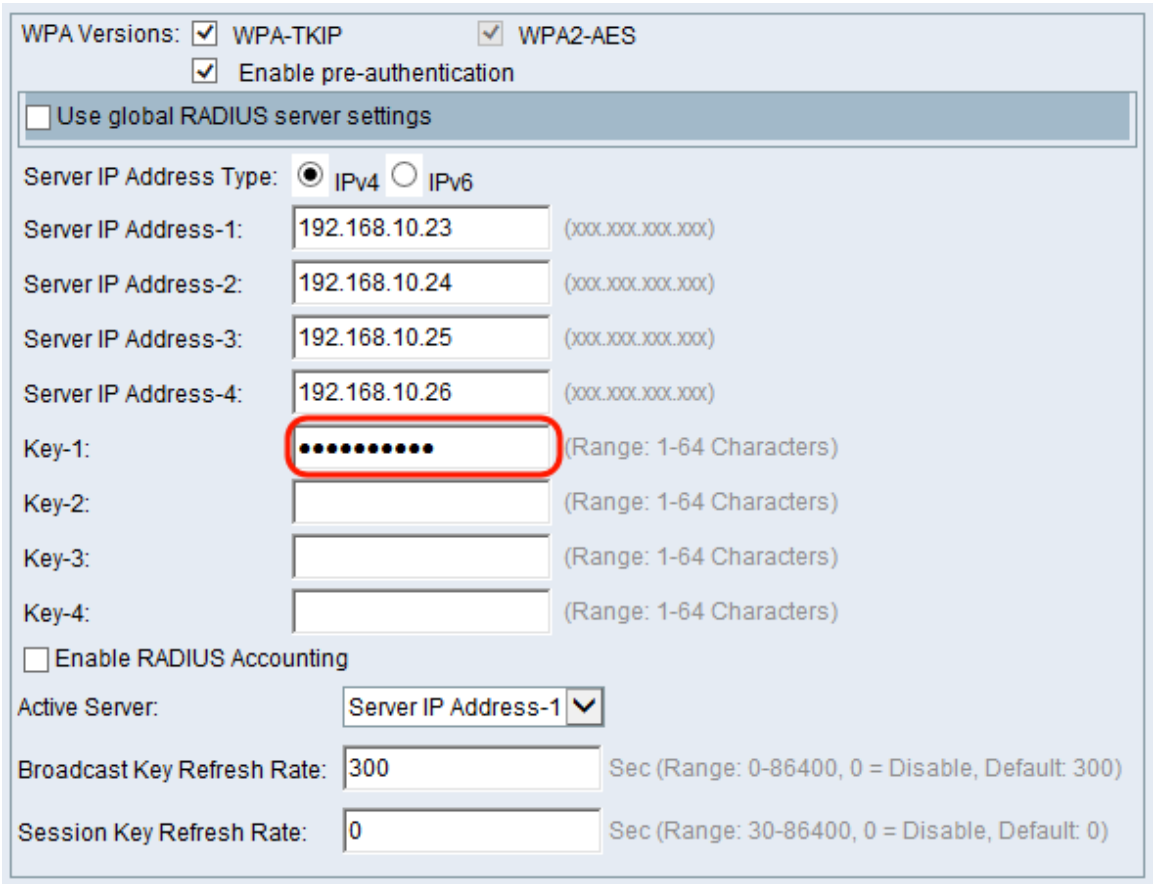
注意：您最多可以有三个IPv4备份RADIUS服务器地址。如果主服务器的身份验证失败，则会按顺序尝试每个已配置的备份服务器。

步骤5.如果在步骤**2中选**择了IPv6，请输入主全局RADIUS服务器的IPv6地址。



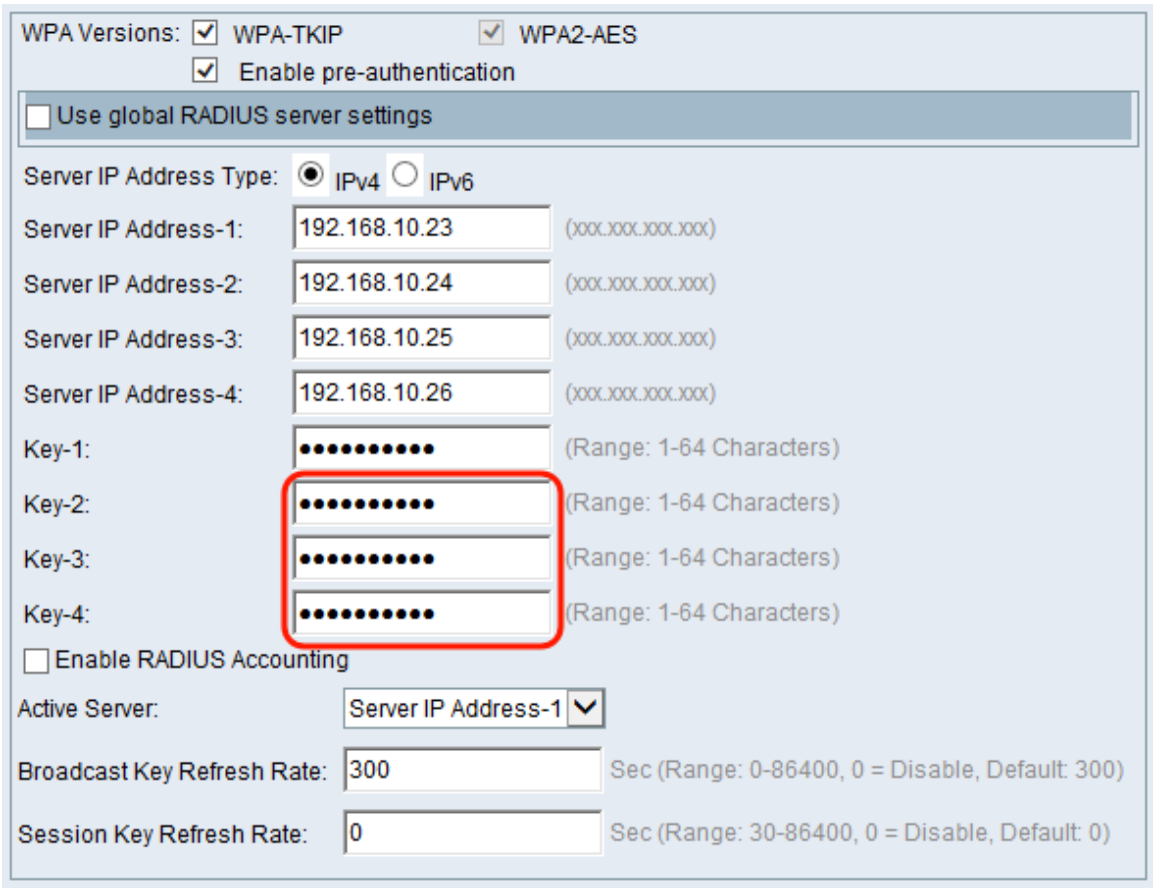
注意：您最多可以有三个IPv6备份RADIUS服务器地址。如果主服务器的身份验证失败，则会按顺序尝试每个已配置的备份服务器。

步骤6.在*Key-1*字段中，输入WAP设备用于向主RADIUS服务器进行身份验证的共享密钥。

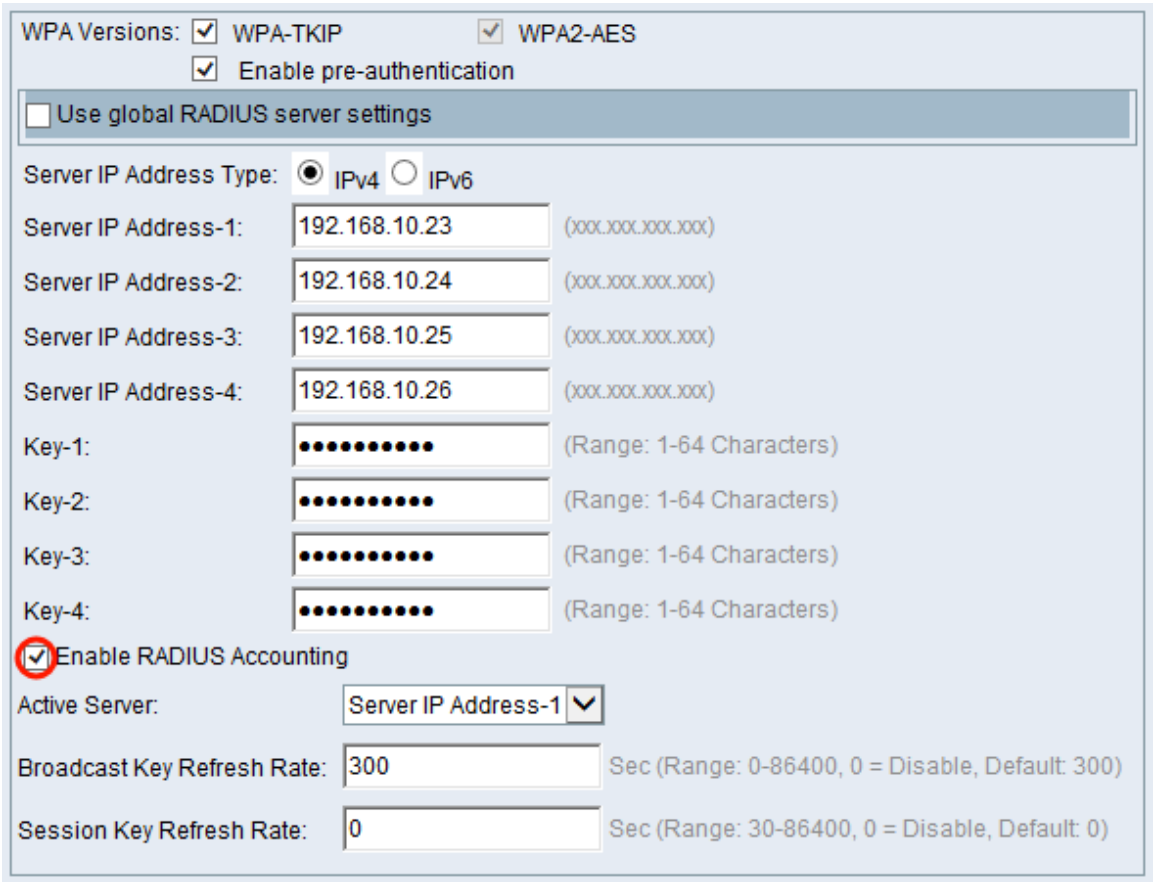


步骤7.在Key-*2到Key-*4字*段中*，输入与已配置的备份RADIUS服务器关联的RADIUS密钥。服

务器IP地址2使*用Key-2*，服务器IP地址3使*用Key-*3，服务器IP地址4使用*Key-4*。

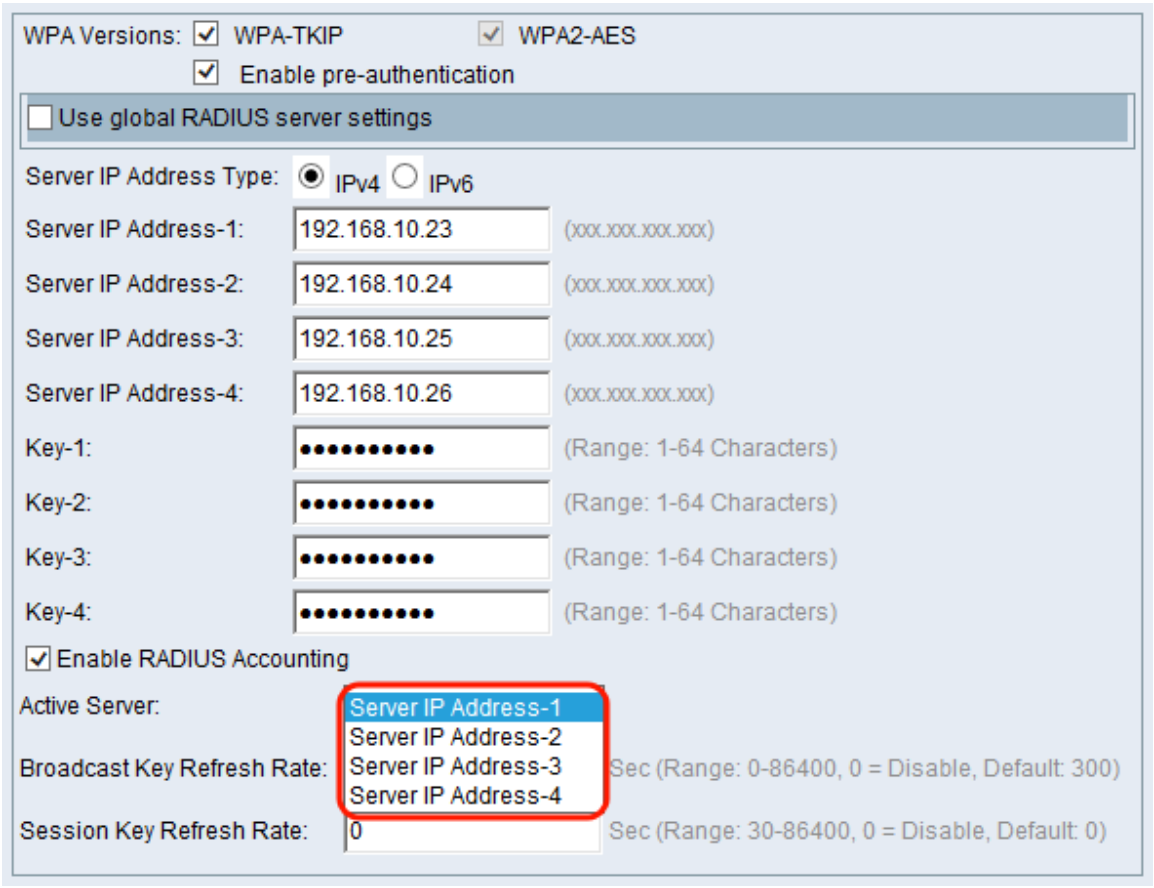


第8步。（可选）在*启用RADIUS记帐*字段中，如果要启用跟踪和测量特定用户消耗的资源，请选中此复选框。启用RADIUS记帐功能将允许您跟踪特定用户的系统时间以及发送和接收的数据量。

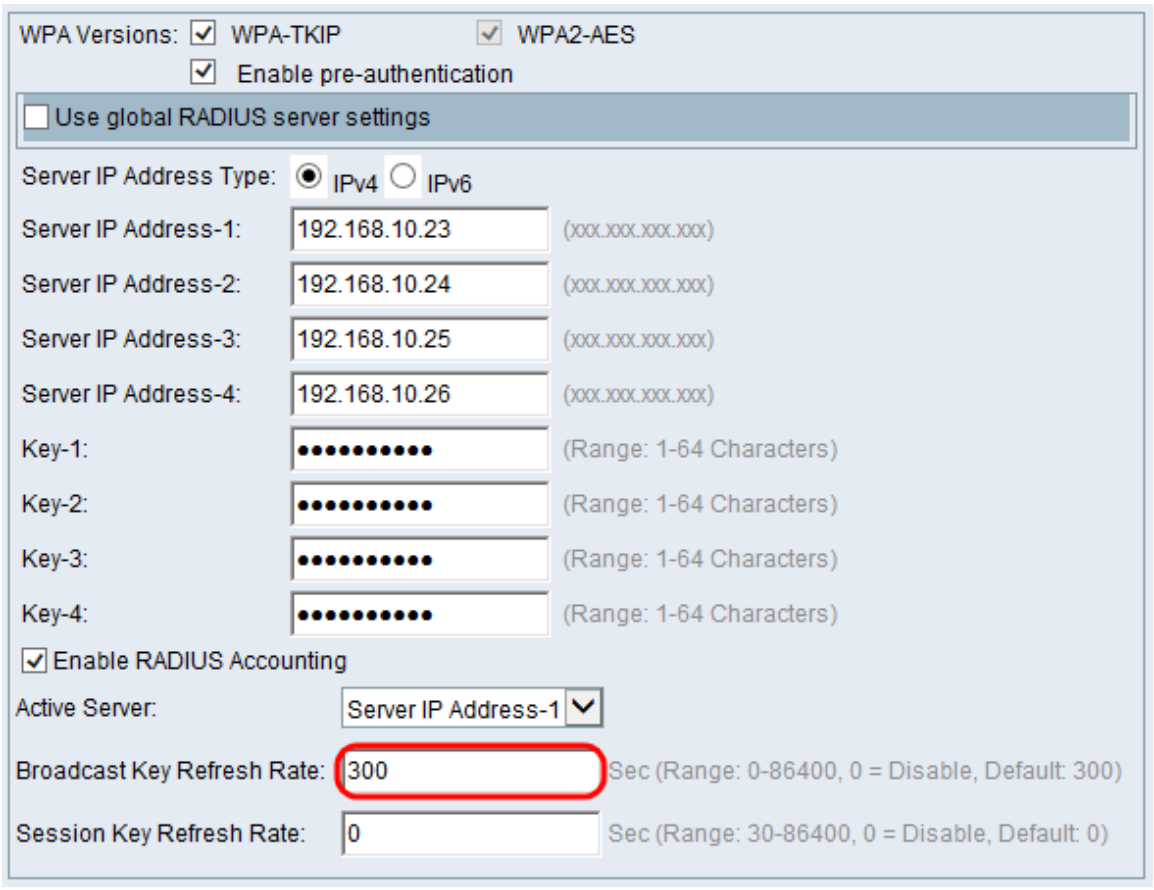


注意：如果启用RADIUS记帐，则会为主RADIUS服务器和所有备份服务器启用它。

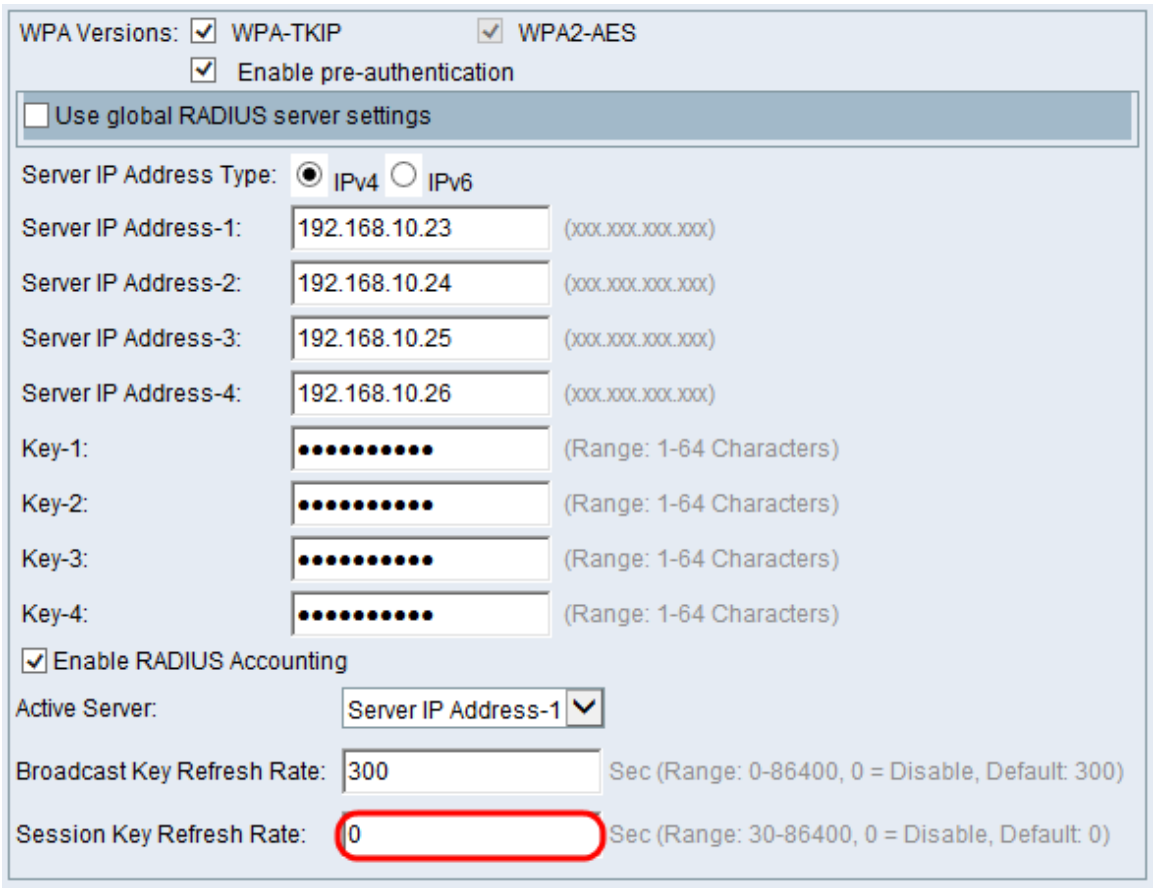
步骤9.在Active Server字段中选择第一个处于活动状态*的服*务器。这允许手动选择活动RADIUS服务器，而不是让WAP设备尝试按顺序联系每个已配置的服务器。



步骤10.在Broadcast Key Refresh Rate字*段中，输入与此VAP关联的客户端的广播（组）密钥刷新间隔*。默认时间为 300 秒钟。



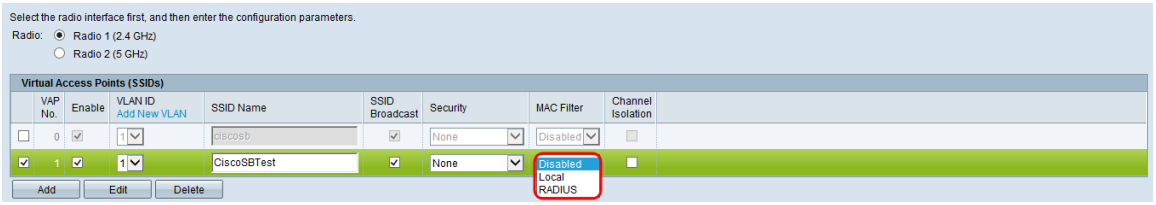
步骤11.在Session Key Refresh Rate字*段中，输入WAP设备刷新与VAP关联的每个客户端的会话（单播）密钥的间隔*。默认值为 0。



MAC过滤器

MAC过滤器指定可访问此VAP的站点是否限于已配置的MAC地址全局列表。

步骤1.在MAC Filter下*拉列*表中，选择所需的MAC过滤类型。



可用选项定义如下：

·禁用 — 不使用MAC过滤。

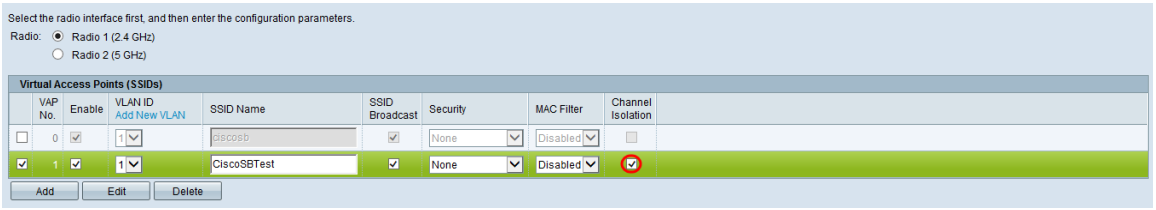
·本地 — 使用您在MAC过滤部分配置的MAC身份验证列表，了解有关MAC过滤的详细信息，请参阅*如何在WAP351和WAP131上配置MAC过滤*。

·RADIUS — 在外部RADIUS服务器上使用MAC身份验证列表。

信道隔离

禁用信道隔离后，无线客户端可以通过WAP设备发送流量，以正常方式相互通信。启用后，WAP设备会阻止同一VAP上无线客户端之间的通信。WAP设备仍允许其无线客户端与网络上的有线设备之间、通过WDS链路以及与不同VAP关联的其他无线客户端之间的数据流量，但不允许在无线客户端之间。

步骤1.如果要启*用信道隔*离，请在Channel Isolation字段中选中复选框。



步骤2.单击“保**存”**。

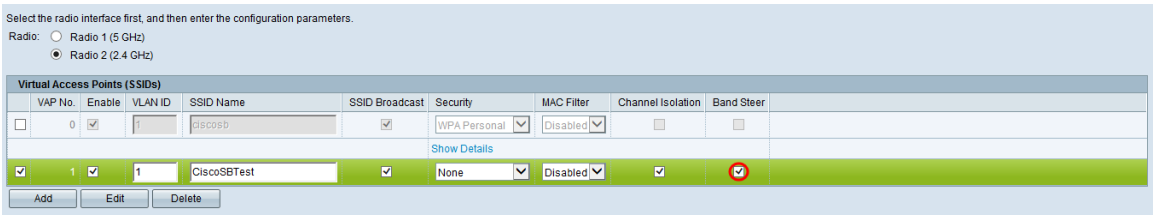
注意：保存新设置后，相应的进程可能会停止并重新启动。发生这种情况时，WAP设备可能会失去连接。我们建议您在连接中断对无线客户端影响最小时更改WAP设备设置。

频带转向

Band Steer仅在WAP371上可用。Band Steer通过将双频受支持的客户端从2.4 GHz频段转向5 GHz频段，有效利用5 GHz频段。这可释放2.4GHz频段，供没有双无线电支持的传统设备使用。

注意：需要启用5 GHz和2.4 GHz无线电才能使用频带转向。有关启用无线电的详细信息，请*参阅如何在WAP371上配置基本无线电设置*。

步骤1.频段转向是按VAP配置的，需要在两个无线电上启用。如果要启用频带转向，请选中“频带转向”(Band Steer)字段中的复选框。

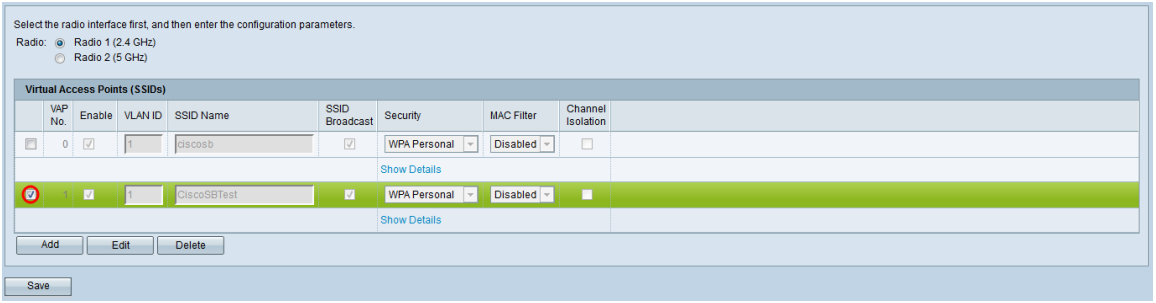


注意：在具有时间敏感语音或视频流量的VAP上，不鼓励频段转向。即使5 GHz无线电恰巧使用的带宽较少，它也会尝试引导客户端使用该无线电。

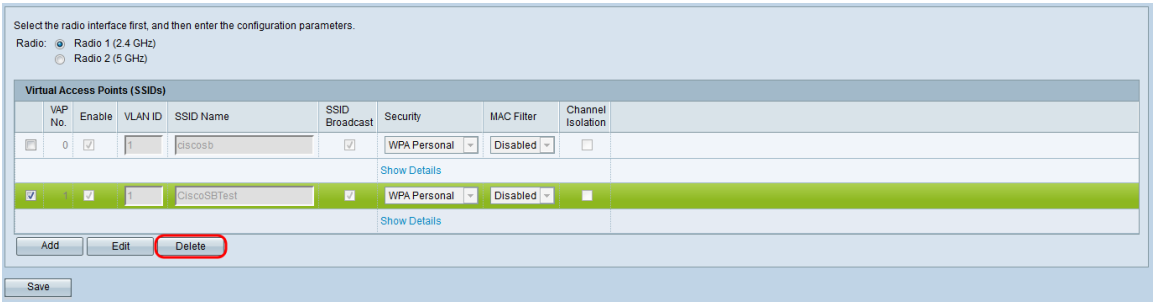
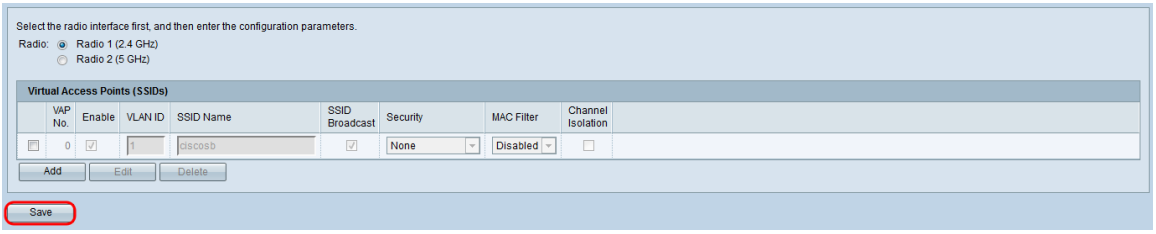
步骤2.单击“保存”。

删除VAP

步骤1.选中要删除的VAP复选框。



步骤2.单击**Delete**删除VAP。



步骤3.单击“保存”永久保存删除。