

配置在WAP351、WAP131和WAP371的VAP

客观

虚拟访问访问接入点(VAPs)分段无线局域网到以太网VLAN无线等同的多广播域。VAPs模拟在一个物理WAP设备的多接入点。Cisco WAP131支持四VAPs，并且Cisco WAP351和WAP371支持八VAPs。

本文目标将显示您如何配置在WAP351、WAP131和WAP371接入点的VAP。

可适用的设备

- WAP351
- WAP131
- WAP371

软件版本

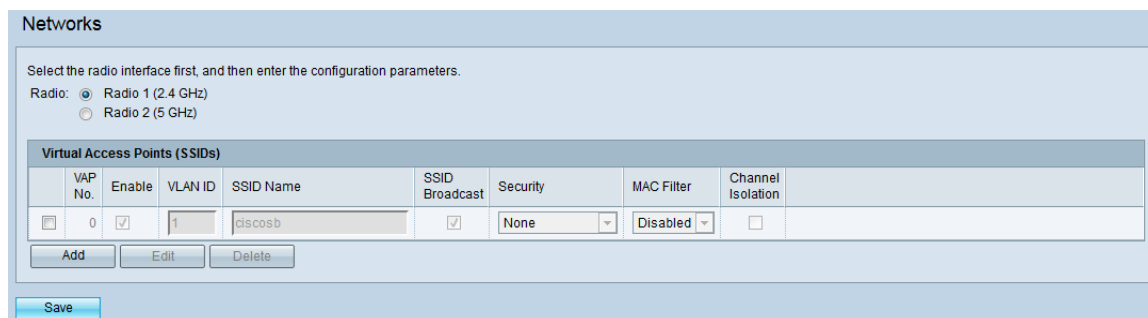
- V1.0.0.39 (WAP351)
- V1.0.0.39 (WAP131)
- V1.2.0.2 (WAP371)

添加并且配置VAP

Note:每个VAP是由一用户配置的服务集标识(SSID)确定的。多个VAPs不能有同样SSID名称。

Note:为了您的无线网络能作用，无线电您的被配置的VAP与一定是产生关联启用的和适当配置。欲知更多信息，请参阅[配置在WAP131和WAP351的基本的无线电设置](#)或者[配置在WAP371的基本的无线电设置](#)

步骤1.登陆到Web配置工具并且连接对**无线>网络**。网络页出版：



The screenshot shows the 'Networks' configuration page. It includes a radio selection for 'Radio 1 (2.4 GHz)' and 'Radio 2 (5 GHz)'. Below is a table for 'Virtual Access Points (SSIDs)' with columns for VAP No., Enable, VLAN ID, SSID Name, SSID Broadcast, Security, MAC Filter, and Channel Isolation. A single VAP is listed with VAP No. 0, Enable checked, VLAN ID 1, SSID Name 'ciscosb', SSID Broadcast checked, Security 'None', MAC Filter 'Disabled', and Channel Isolation unchecked. Buttons for 'Add', 'Edit', 'Delete', and 'Save' are visible.

VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>

Step 2.在辐射场，为您希望配置VAPs的无线信号发射请选择单选按钮。

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (2.4 GHz)
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

第3步。要添加新的VAP，请点击添加。新的VAP在表里将出现。

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (2.4 GHz)
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	1		<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

Note:而WAP371和WAP351支持8 VAPs，WAP131支持4 VAPs。

第4步。要开始编辑VAP，请点击在最左端的复选框条目然后点击编辑。这将允许您修改您选择了VAP的变灰字段。

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (2.4 GHz)
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1		<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

第5步。对VAP的enable (event)使用方法，请保证Enable复选框被检查。

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (2.4 GHz)
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1		<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

第6步。在VLAN ID字段，请指定您希望与VAP产生关联的VLAN ID。如果使用WAP131或WAP371，请进入在VLAN ID。您能输入的最大值是4094。

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (2.4 GHz)
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1		<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

Note:被输入的VLAN ID在您的网络必须存在和适当配置。欲知更多信息，请参阅在[WAP351接入点](#)，[管理被标记的和未标记的VLAN ID的VLAN配置在WAP131](#)或者[管理被标记的和在WAP371的未标记的VLAN ID](#)。

步骤7.输入无线网络的名字在SSID名称字段。每个VAP必须有唯一的SSID名字。

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (2.4 GHz)
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
	VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

第8.步。如果类似SSID名称会是广播给客户端请检查SSID广播复选框。这将显示SSID名称可用的网络他们的列表的客户端。

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (2.4 GHz)
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
	VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

配置安全设置

步骤1.选择要求连接到从安全下拉列表的VAP的认证方法。如果除无之外的任何选项选择，另外的字段将出现。

可用的选项如下：

- 无
- 静态 WEP
- 动态WEP
- 私有的WPA
- WPA企业

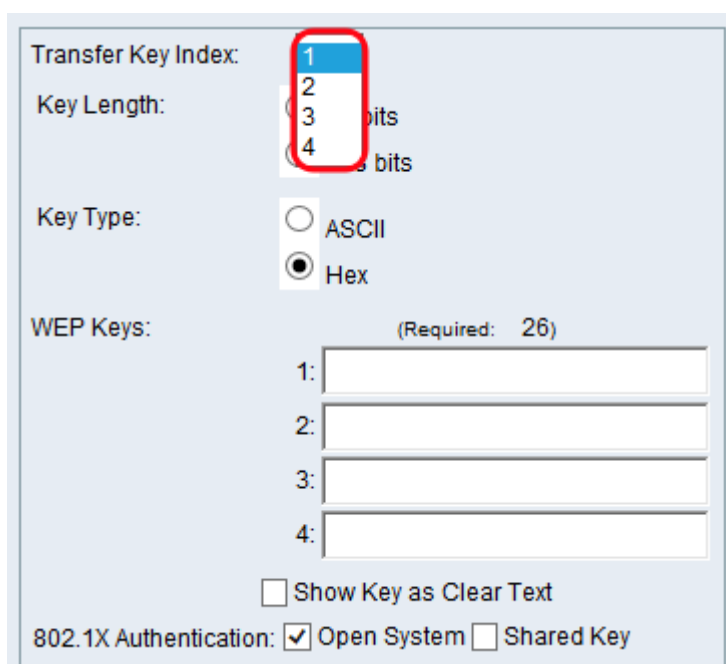
Note:私有的WPA和WPA企业是最大安全性的首选认证类型。静态WEP和动态WEP应该只与传统设备一起使用并且要求无线电设置为802.11a或802.11b/g将使用的模式。欲知更多信息，请参阅[配置在WAP131和WAP351的基本的无线电设置](#)或者[配置在WAP371的基本的无线电设置](#)。

静态 WEP

静态WEP是最少安全的认证方法。它加密在根据一个静态键的无线网络的数据。变得简单非法地得到此静态键，因此WEP身份验证应该当必要时只与传统设备一起使用。

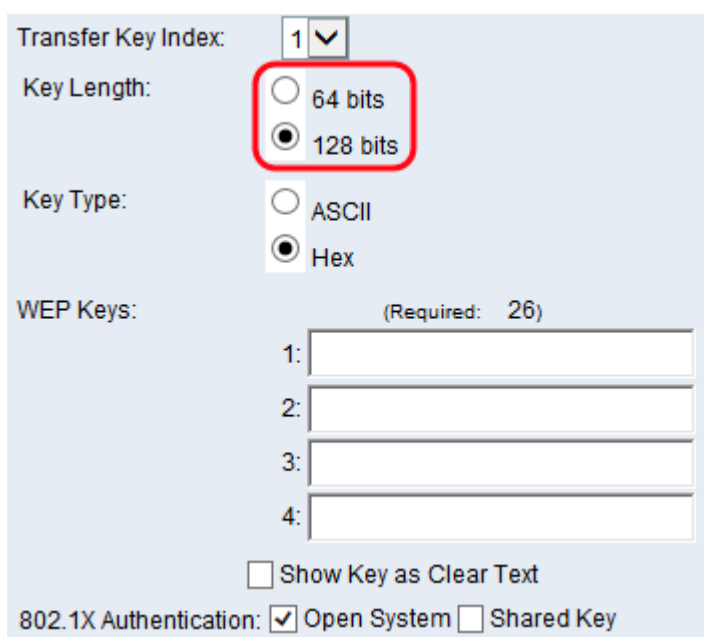
Note:当选择静态WEP作为您的安全方法时，提示将看来并且告诉您您的安全方法选择是非常不安全的。

Step 1.在Transfer键索引下拉列表中，请选择WEP密钥的索引从键列表在设备将使用加密数据的那之下。



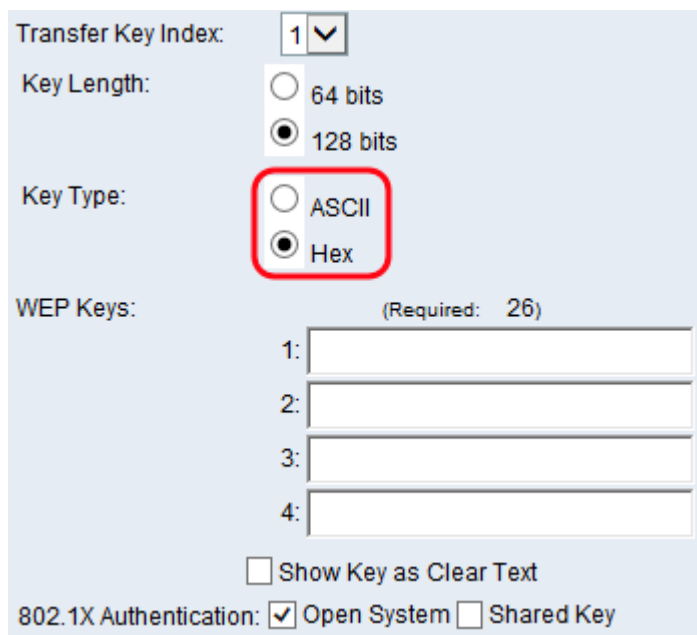
The screenshot shows the WEP configuration interface. The 'Transfer Key Index' dropdown menu is open, showing options 1, 2, 3, and 4. Option 1 is selected and highlighted with a red box. Below the dropdown, the 'Key Length' field is visible, with options for 64 bits and 128 bits. The 'Key Type' field has radio buttons for ASCII and Hex, with Hex selected. The 'WEP Keys' section has four input fields labeled 1, 2, 3, and 4, with a '(Required: 26)' label above them. There is a checkbox for 'Show Key as Clear Text' which is unchecked. At the bottom, the '802.1X Authentication' section has radio buttons for 'Open System' (checked) and 'Shared Key' (unchecked).

步骤2.从密钥长度字段选择一个单选按钮指定键是否是64位或128字节长。



The screenshot shows the WEP configuration interface. The 'Transfer Key Index' dropdown menu is closed, showing '1'. The 'Key Length' field has radio buttons for '64 bits' and '128 bits', with '128 bits' selected and highlighted with a red box. The 'Key Type' field has radio buttons for ASCII and Hex, with Hex selected. The 'WEP Keys' section has four input fields labeled 1, 2, 3, and 4, with a '(Required: 26)' label above them. There is a checkbox for 'Show Key as Clear Text' which is unchecked. At the bottom, the '802.1X Authentication' section has radio buttons for 'Open System' (checked) and 'Shared Key' (unchecked).

第3步。在**关键类型**字段，请选择您是否在ASCII或十六进制格式希望输入键。ASCII包括所有字母、编号和符号在**关键董事会**，当十六进制必须使用仅编号时或在A-F上写字。



Transfer Key Index: 1

Key Length: 64 bits 128 bits

Key Type: ASCII Hex

WEP Keys: (Required: 26)

1:

2:

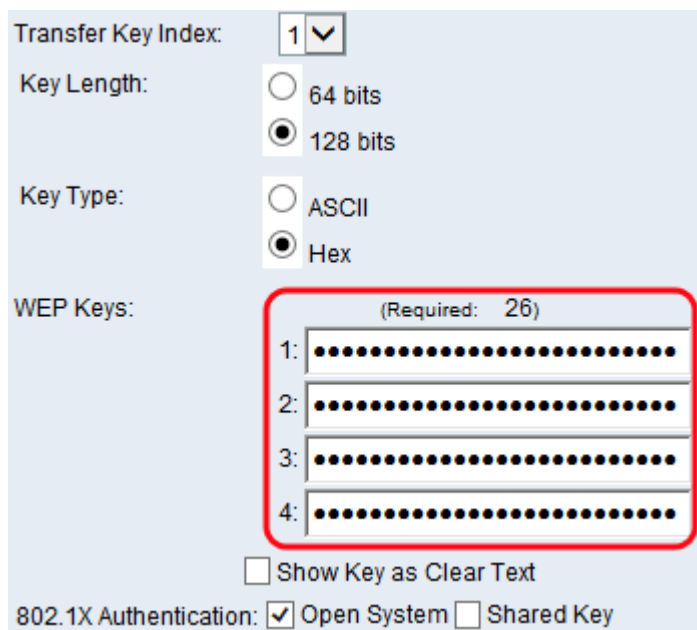
3:

4:

Show Key as Clear Text

802.1X Authentication: Open System Shared Key

第4步。在**WEP密钥**关键字域，请输入您的设备的4把不同的WEP密钥。将连接到此网络的每个客户端必须有设备在同一slot的同样WEP密钥指定的之一。



Transfer Key Index: 1

Key Length: 64 bits 128 bits

Key Type: ASCII Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

Show Key as Clear Text

802.1X Authentication: Open System Shared Key

第5步(可选)点击在**显示键**的复选框作为明文领域，如果显示键的字符串。

Transfer Key Index: 1

Key Length: 64 bits
 128 bits

Key Type: ASCII
 Hex

WEP Keys: (Required: 26)

1: ABCDFE123456789ABCDE34251.
2: ABEDC43C2A1B56CD7AE494A56
3: BB4C56AD3E12CB78A9234BD23
4: BEE59A4C5D3E5B7B8AD23169B

Show Key as Clear Text

802.1X Authentication: Open System Shared Key

Note: 当使用在WAP351时的一个不同的固件，WAP131或者WAP371，显示键作为明文领域可能失踪。

第6步。在802.1X认证字段，请指定您要通过选择选项使用开放式系统和共享密钥的认证算法。认证算法定义了使用确定的方法客户端工作站是否允许与WAP设备产生关联，当静态WEP是安全模式时。

Transfer Key Index: 1

Key Length: 64 bits
 128 bits

Key Type: ASCII
 Hex

WEP Keys: (Required: 26)

1:
2:
3:
4:

Show Key as Clear Text

802.1X Authentication: Open System Shared Key

可用的选项被定义如下：

- 开放式系统—认证允许所有客户端工作站与WAP设备产生关联是否该客户端工作站有正确的WEP密钥。此算法用于纯文本，IEEE 802.1X和WPA模式。当认证算法设置为开放式系统时，所有客户端能与WAP设备产生关联。
- 共享密钥—认证要求客户端工作站有正确的WEP密钥为了与WAP设备产生关联。当认证算法设置为共享密钥时，与不正确的WEP密钥的一个位置不能与WAP设备产生关联。
- 开放式系统和共享密钥—当您选择了这两种认证算法时，被配置的客户端工作站使用WEP在共享密钥模式必须有一把有效WEP密钥为了与WAP设备产生关联。并且，被配置的客户端工作站使用WEP作为一个开放式系统(没启动的共享密钥模式)能与WAP设备产生关联

，即使他们没有正确的WEP密钥。

步骤7.点击“Save”。

动态WEP

动态WEP是指802.1x技术和可扩展的认证协议(EAP)的组合。此模式要求使用一个外部RADIUS服务器验证用户。WAP设备要求支持EAP的一个RADIUS服务器，例如Microsoft互联网认证服务器。要工作与微软视窗客户端，认证服务器必须支持Protected EAP (PEAP)和MSCHAP v2。您能使用IEEE 802.1X模式支持，包括证书，Kerberos各种各样的认证方法和公共密钥认证中的任一个，但是您必须配置客户端工作站使用WAP设备使用的同一个认证方法。

步骤1.默认情况下使用全局RADIUS服务器设置被检查。如果要配置VAP使用一组不同的RADIUS服务器，请非选定复选框。否则请跳到第8.步。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Step 2.在服务器IP地址类型字段，请选择服务器IP地址类型您的WAP设备用途。选项是IPv4或IPv6。在点分十进制表示方法表示的IPv4用途32位二进制数。IPv6使用十六进制数字和冒号表示128-bit二进制数。WAP设备联系仅RADIUS服务器或服务器的您在此字段选择的地址类型。如果选择IPv6，则请跳到第4.步。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▾

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

第3步。如果选择了在第2步的IPv4，请输入默认情况下所有VAPs使用RADIUS服务器的IP地址。然后请跳到第5步。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▾

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Note:您能有三个IPv4备份的RADIUS服务器地址。如果认证用主要服务器失效，每个被配置的备份服务器依顺序被尝试。

第4步。如果选择了在第2步的IPv6，请输入主要的全局RADIUS服务器的IPv6地址。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IPv6 Address-1: (xxxxCxxxxCxxxxCxxxxCxxxxCxxxxCxxxxCxxxxCxxxx)

Server IPv6 Address-2: (xxxxCxxxxCxxxxCxxxxCxxxxCxxxxCxxxxCxxxxCxxxx)

Server IPv6 Address-3: (xxxxCxxxxCxxxxCxxxxCxxxxCxxxxCxxxxCxxxxCxxxx)

Server IPv6 Address-4: (xxxxCxxxxCxxxxCxxxxCxxxxCxxxxCxxxxCxxxxCxxxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Note:您能有三个IPv6备份的RADIUS服务器地址。如果认证用主要服务器失效，每个被配置的备份服务器依顺序被尝试。

第5步。在Key-1字段，请进入在WAP设备使用验证到主要的RADIUS服务器的被共享的密钥。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

第6步。在对Key-4字段的Key-2中，请进入在RADIUS关键关联与被配置的备份的RADIUS服务器。服务器IP Address-2使用Key-2，服务器IP地址3使用Key-3，并且服务器IP地址4使用Key-4。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

在 *Enable (event) RADIUS* 认为的字段第7步(可选)，检查复选框，如果想要对 enable (event) 跟踪，并且测量资源一个特定用户消耗了。启用 RADIUS 认为将跟踪系统时间和传输和接收的相当数量数据。信息在 RADIUS 服务器将被存储。这为主要的 RADIUS 服务器和所有备份服务器将是启用的。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

Note: 如果有认为 enable (event) 的 RADIUS，为主要的 RADIUS 服务器和所有备份服务器是启用的

步骤8. 选择是活跃的在激活服务器领域的第一个服务器。活动 RADIUS 服务器的此 enable (event) 手工的选择，而不是有 WAP 设备尝试依顺序联系每个配置的服务器和选择是活跃的第一个服务器。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1
Server IP Address-2
Server IP Address-3
Server IP Address-4

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

第9步。在广播键刷新率字段，请进入在广播的间隔(组)键为与此VAP产生关联的客户端被刷新。默认值是300秒。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

第10步。在会议密钥刷新率字段，请输入WAP设备刷新与VAP产生关联的每个客户端的会话的间隔(单播)键。默认值是0。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

私有的WPA

私有的WPA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和用于企业WPA安全模式。PSK使用最初检查仅证书。WPA也指WPA-PSK。此安全模式为支持原始WPA的无线客户端是向后兼容。

Step 1.在WPA版本字段，如果希望对enable (event) WPA-TKIP，请检查WPA-TKIP复选框。您能安排WPA-TKIP和WPA2-AES同时被启用。WAP总是支持WPA2-AES，因此您不能配置它。

WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter: Below Minimum

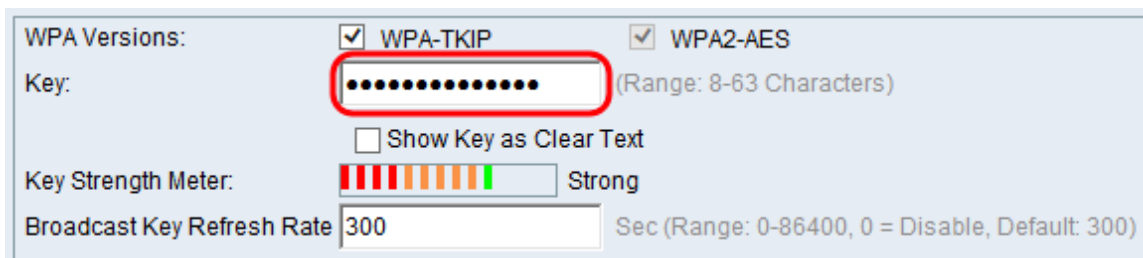
Broadcast Key Refresh Rate Sec (Range: 0-86400, 0 = Disable, Default: 300)


可用的选项被定义如下：

- WPA-TKIP —网络有只支持原始WPA和TKIP安全协议的一些客户端工作站。根据最新的WiFi联盟需求，选择仅WPA-TKIP不是推荐的。
- WPA2-AES —网络的所有客户端工作站支持WPA2和AES-CCMP密码/安全协议。此WPA版本提供最佳的安全每个IEEE 802.11i标准。根据最新的WiFi联盟需求，AP必须一直支持此模式。
- WPA-TKIP和WPA2-AES —如果网络有客户端的混合，一些支持WPA2和其他支持仅原始WPA，请检查两个复选框。此设置让WPA和WPA2客户端工作站联合和验证，但是使用更加稳健的WPA2支持它的客户端。此WPA配置在若干安全位置准许更多互通性。

Note:WPA客户端必须有这些的键(一个有效TKIP键或一个有效AES-CCMP键)之一能与WAP设备产生关联。

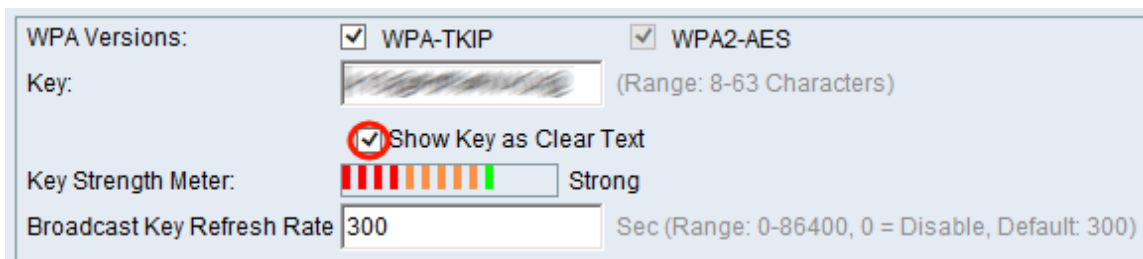
Step 2.在关键字段，请进入在WPA私有安全的被共享的密钥。输入8个字符和至少最多63个字符。




WPA Versions: WPA-TKIP WPA2-AES
Key: (Range: 8-63 Characters)
 Show Key as Clear Text
Key Strength Meter:  Strong
Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Note:可接受的字符包括大写和小写字母的字母、数字位和特殊符号(?!@#%&*)。

第3步(可选的)检查显示键作为明文复选框，如果想要文本您键入是可视的。默认情况下复选框被不选定。



WPA Versions: WPA-TKIP WPA2-AES
Key: (Range: 8-63 Characters)
 Show Key as Clear Text
Key Strength Meter:  Strong
Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

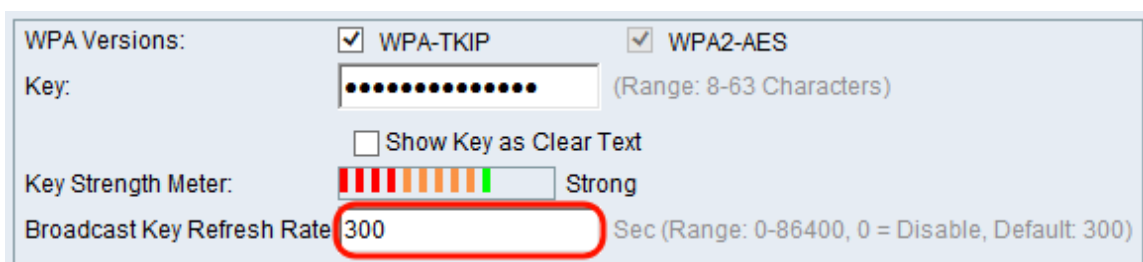
Note: 当使用在WAP351时的一个不同的固件，WAP131或者WAP371，显示键作为明文领域可能失踪。


Note: 密钥强度公尺领域是WAP设备根据复杂性标准检查键例如的地方多少不同类型的字符使用，并且键多久是。如果WPA-PSK复杂性检查功能是启用的，键没有被接受，除非满足最低的标准。关于WPA-PSK复杂性的更多信息，请参见[配置WAP131、WAP351和WAP371的密码复杂性](#)。



WPA Versions: WPA-TKIP WPA2-AES
Key: (Range: 8-63 Characters)
 Show Key as Clear Text
Key Strength Meter:  Strong
Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

第4步。在广播键刷新率字段，请进入在广播的间隔(组)键为与此VAP产生关联的客户端被刷新。默认值是300秒。



WPA Versions: WPA-TKIP WPA2-AES
Key: (Range: 8-63 Characters)
 Show Key as Clear Text
Key Strength Meter:  Strong
Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

WPA企业

与RADIUS的WPA企业是Wi-Fi联盟IEEE 802.11i标准，包括CCMP (AES)和TKIP加密的实施。企业模式要求使用RADIUS服务器验证用户。安全模式与支持原始WPA的无线客户端是向后

兼容。

Note:默认情况下动态VLAN模式启动，允许RADIUS验证服务器决定哪个VLAN使用位置。

Step 1.在WPA版本字段，请检查复选框将支持的客户端工作站的种类。默认情况下他们全部被启用。AP必须一直支持WPA2-AES，因此您不能配置它。

The screenshot shows a configuration window for WPA settings. At the top, under 'WPA Versions:', there are three checked checkboxes: 'WPA-TKIP', 'WPA2-AES', and 'Enable pre-authentication'. Below this is a section for 'Use global RADIUS server settings' which is also checked. The 'Server IP Address Type' is set to 'IPv4'. There are four input fields for 'Server IP Address-1' through 'Server IP Address-4', with the first one containing '0.0.0.0'. Below these are four input fields for 'Key-1' through 'Key-4', each with a range of 1-64 characters. At the bottom, there is an unchecked checkbox for 'Enable RADIUS Accounting', a dropdown for 'Active Server' set to 'Server IP Address-1', and two input fields for 'Broadcast Key Refresh Rate' (set to 300) and 'Session Key Refresh Rate' (set to 0).

可用的选项被定义如下：

- WPA-TKIP —网络有只支持原始WPA和TKIP安全协议的一些客户端工作站。注意选择仅WPA-TKIP接入点的不根据最新的WiFi联盟需求允许。
- WPA2-AES —网络的所有客户端工作站支持WPA2版本和AES-CCMP密码安全协议。此WPA版本提供最佳的安全每个IEEE 802.11i标准。根据最新的Wi-Fi联盟需求，WAP必须一直支持此模式。
- Enable (event)预验证—如果选择仅WPA2或WPA和WPA2作为WPA版本，您能WPA2客户端的enable (event)预验证。如果希望WPA2无线客户端发送预验证信息包，请检查此选项。预验证信息从WAP设备被传递客户端当前使用对目标WAP设备。启用此功能可帮助加速连接到多个WAPs的漫游的客户端的认证。此选项不适用，如果为WPA版本选择了WPA，因为原始WPA不支持此功能。

Note:被配置的客户端工作站以RADIUS使用WPA必须有这些地址和键之一：一个有效TKIP RADIUS或有效CCMP (AES) IP地址和RADIUS键。

步骤2.默认情况下使用全局RADIUS服务器设置被检查。如果要配置VAP使用一组不同的RADIUS服务器，请非选定复选框。否则请跳到第9步。

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
 Key-2: (Range: 1-64 Characters)
 Key-3: (Range: 1-64 Characters)
 Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

第3步。在服务器IP地址类型字段，请选择服务器IP地址类型您的WAP设备用途。选项是IPv4或IPv6。在点分十进制表示方法表示的IPv4用途32位二进制数。IPv6使用十六进制数字和冒号表示128-bit二进制数。WAP设备联系仅RADIUS服务器或服务器的您在此字段选择的地址类型。

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
 Key-2: (Range: 1-64 Characters)
 Key-3: (Range: 1-64 Characters)
 Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

第4步。如果选择了在第2步的IPv4，请输入默认情况下所有VAPs使用RADIUS服务器的IP地

址。然后请跳到第6步。

WPA Versions: <input checked="" type="checkbox"/> WPA-TKIP <input checked="" type="checkbox"/> WPA2-AES	
<input checked="" type="checkbox"/> Enable pre-authentication	
<input type="checkbox"/> Use global RADIUS server settings	
Server IP Address Type:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Server IP Address-1:	<input type="text" value="192.168.10.23"/> (xxx.xxx.xxx.xxx)
Server IP Address-2:	<input type="text" value="192.168.10.24"/> (xxx.xxx.xxx.xxx)
Server IP Address-3:	<input type="text" value="192.168.10.25"/> (xxx.xxx.xxx.xxx)
Server IP Address-4:	<input type="text" value="192.168.10.26"/> (xxx.xxx.xxx.xxx)
Key-1:	<input type="text"/> (Range: 1-64 Characters)
Key-2:	<input type="text"/> (Range: 1-64 Characters)
Key-3:	<input type="text"/> (Range: 1-64 Characters)
Key-4:	<input type="text"/> (Range: 1-64 Characters)
<input type="checkbox"/> Enable RADIUS Accounting	
Active Server:	<input type="text" value="Server IP Address-1"/> ▼
Broadcast Key Refresh Rate:	<input type="text" value="300"/> Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate:	<input type="text" value="0"/> Sec (Range: 30-86400, 0 = Disable, Default: 0)

Note:您能有三个IPv4备份的RADIUS服务器地址。如果认证用主要服务器失效，每个被配置的备份服务器依顺序被尝试。

第5步。如果选择了在第2步的IPv6，请输入主要的全局RADIUS服务器的IPv6地址。

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IPv6 Address-1: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Server IPv6 Address-2: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Server IPv6 Address-3: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Server IPv6 Address-4: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Note:您能有三个IPv6备份的RADIUS服务器地址。如果认证用主要服务器失效，每个被配置的备份服务器依顺序被尝试。

第6步。在Key-1字段，请进入在WAP设备使用验证到主要的RADIUS服务器的被共享的密钥。

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

第7步。在对Key-4字段的Key-2中，请进入在RADIUS关键关联与被配置的备份的RADIUS服务器。服务器IP Address-2使用Key-2，服务器IP地址3使用Key-3，并且服务器IP地址4使用Key-4。

The screenshot shows a configuration window for RADIUS settings. At the top, there are checkboxes for WPA Versions: WPA-TKIP (checked), WPA2-AES (checked), and Enable pre-authentication (checked). Below this is a section titled 'Use global RADIUS server settings' with an unchecked checkbox. The 'Server IP Address Type' is set to IPv4 (selected). There are four fields for 'Server IP Address-1' through 'Server IP Address-4', each containing an IP address (192.168.10.23 to 192.168.10.26) and a placeholder '(xxx.xxx.xxx.xxx)'. Below these are four fields for 'Key-1' through 'Key-4', each containing a masked key (represented by dots) and a placeholder '(Range: 1-64 Characters)'. The 'Key-2' field is highlighted with a red rectangle. At the bottom, there is an unchecked checkbox for 'Enable RADIUS Accounting', a dropdown for 'Active Server' set to 'Server IP Address-1', and two fields for refresh rates: 'Broadcast Key Refresh Rate' (300 Sec) and 'Session Key Refresh Rate' (0 Sec).

在Enable (event) RADIUS认为的字段第8步(可选)，检查复选框，如果想要对enable (event)跟踪，并且测量资源一个特定用户消耗了。启用RADIUS认为将允许您跟踪一个传输和接收的特定用户的系统时间和相当数量数据。

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
 Key-2: (Range: 1-64 Characters)
 Key-3: (Range: 1-64 Characters)
 Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Note:如果认为启用的RADIUS，它为主要的RADIUS服务器和所有备份服务器是启用的。

步骤9.选择是活跃的在激活服务器领域的第一个服务器。活动RADIUS服务器的此enable (event)手工的选择，而不是有WAP设备尝试依顺序联系每个配置的服务器。

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
 Key-2: (Range: 1-64 Characters)
 Key-3: (Range: 1-64 Characters)
 Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

第10.步。在广播键刷新率字段，请进入在广播的间隔(组)键为与此VAP产生关联的客户端被刷

新。默认值是300秒。

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
Server IP Address-2: (xxx.xxx.xxx.xxx)
Server IP Address-3: (xxx.xxx.xxx.xxx)
Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
Key-2: (Range: 1-64 Characters)
Key-3: (Range: 1-64 Characters)
Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

第11步。在会议密钥刷新率字段，请输入WAP设备刷新与VAP产生关联的每个客户端的会话的间隔(单播)键。默认值是0。

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
Server IP Address-2: (xxx.xxx.xxx.xxx)
Server IP Address-3: (xxx.xxx.xxx.xxx)
Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
Key-2: (Range: 1-64 Characters)
Key-3: (Range: 1-64 Characters)
Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

MAC过滤器

MAC过滤器指定能访问此VAP的位置是否限于MAC地址一张被配置的全局列表。

Step 1.在MAC过滤器下拉列表中，请选择MAC过滤的期望类型。

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (2.4 GHz)
 Radio 2 (5 GHz)

VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	iscoob	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled Local RADIUS	<input type="checkbox"/>

Add Edit Delete

可用的选项被定义如下：

- 失效—不使用MAC过滤。
- 本地—使用您在过滤部分的MAC配置的MAC验证列表，得知更多过滤的MAC，是指[如何配置过滤在WAP351和WAP131的MAC](#)。
- RADIUS —使用在一个外部RADIUS服务器的MAC验证列表。

信道隔离

当信道隔离是失效的时，无线客户端能通过发送数据流通常互相沟通通过WAP设备。当启用，WAP设备阻拦无线客户端之间的通信同样VAP的。WAP设备仍然允许其无线客户端和有线设备之间的数据流量在网络，在WDS链路间和有其他无线客户端的与不同的VAP相关联，但是不在无线客户端中。

Step 1.在信道隔离字段，如果希望对enable (event)信道隔离，请检查复选框。

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (2.4 GHz)
 Radio 2 (5 GHz)

VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	iscoob	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input checked="" type="checkbox"/>

Add Edit Delete

步骤2.点击“Save”。

Note:在新的设置被保存后，对应的进程可能被终止和被重新启动。当此情况发生时，WAP设备可能丢失连接。我们建议您更改WAP设备设置，当连接损耗最少影响您的无线客户端时。

波段操舵

波段操舵只是可用的在WAP371。波段操舵是通过操纵从2.4千兆赫波段的双波段支持的客户端有效使用5千兆赫波段到5千兆赫波段。这释放2.4GHz波段供没有双重无线电技术支持的传统设备使用。

Note:5个千兆赫和2.4千兆赫无线电需要被启用使用波段操舵。关于启用无线电的更多信息请参见[如何配置在WAP371的基本的无线电设置](#)。

步骤1.波段操舵在每VAP基本类型的a在两无线电被配置并且需要被启用。如果希望对enable (event)波段操舵，请检查在波段操舵字段的复选框。

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Add Edit Delete

Note:波段操舵在与时间敏感的语音或视频流量的VAPs没有鼓励。即使5千兆赫无线电偶然使用较少带宽，设法操纵客户端到该无线电。

步骤2.点击“Save”。

删除VAP

Step 1.检查您要删除VAP的复选框。

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (2.4 GHz)
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	

Add Edit Delete

Save

步骤2.点击删除删除VAP。

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (2.4 GHz)
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	

Add Edit Delete

Save

步骤3.点击“Save”永久保存您的删除。

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (2.4 GHz)
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	

Add Edit Delete

Save