RV215W的基本无线设置配置

目标

无线网络是不通过电缆连接的计算机网络。无线局域网(WLAN)是一种无线网络，它通过使用无线电通信在短距离内连接多个设备。

本文解释如何在RV215W上配置基本无线设置，包括网络安全配置。

索引

•常规设置
·编辑无线表
·禁用安全
·配置WEP安全
·配置WPA个人安全
·配置WPA-Enterprise安全
·配置WPA2 — 个人/WPA2 — 个人混合安全
·配置WPA2-Enterprise/WPA2-Enterprise混合安全
·编辑MAC过滤
·访问时间
·编辑访客网络
·配置WPS方法1
·配置WPS方法2
·配置WPS方法3

适用设备

• RV215W

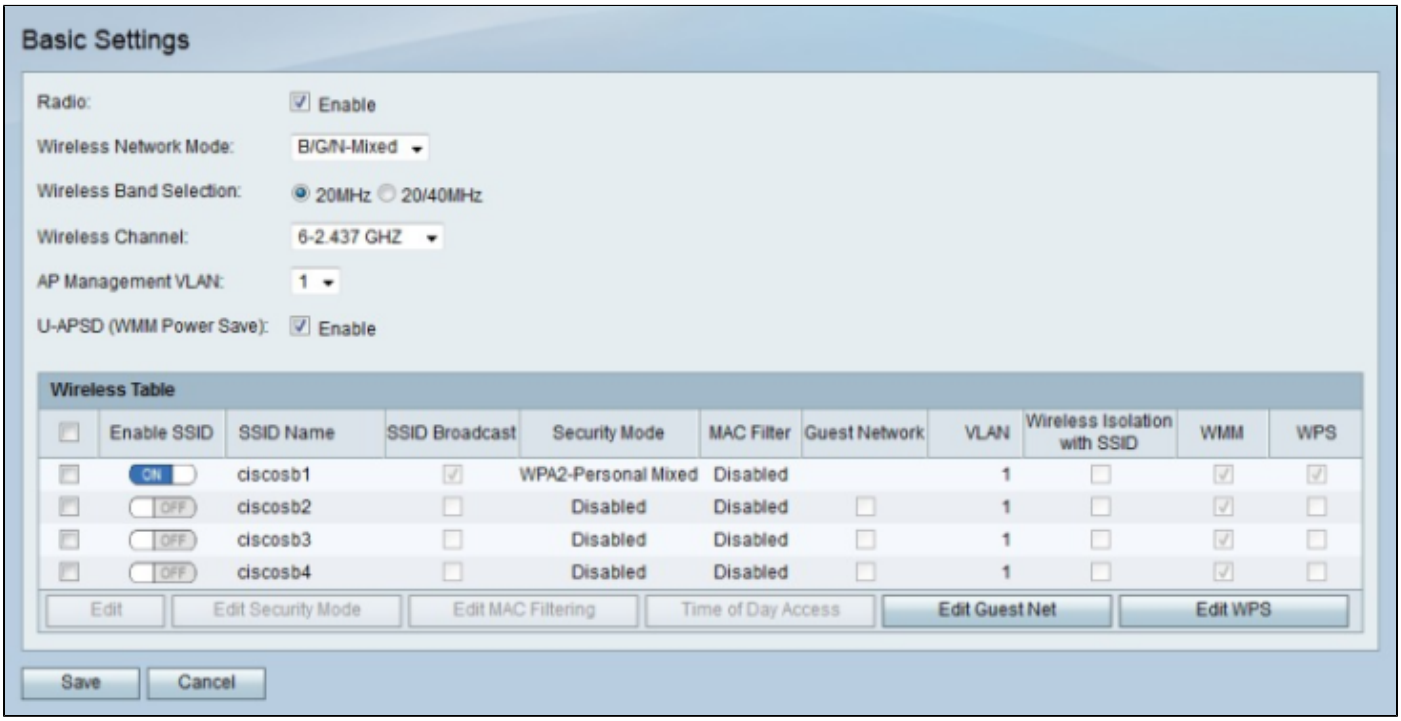
软件版本

•1.1.0.5

基本设置配置

常规设置

步骤1.登录到Web配置实用程序并选择Wireless > Basic Settings。将打开基本设置页面：



步骤2.选中Radio字段中的Enable以启用无线电。

步骤3.从Wireless Network Mode下拉列表中选择无线模式。

· B/G/N-Mixed — 网络包含wireless-B、wireless-G和wireless-N设备的混合。

·仅B — 网络仅包含wireless-B设备。

· G-Only — 网络仅包含wireless-G设备。

·仅N — 网络仅包含wireless-N设备。

· B/G-Mixed — 网络包含wireless-B和wireless-G设备的混合。

· G/N Mixed — 网络包含wireless-G和wireless-N设备的混合。

步骤4.如果网络模式包含wireless-N设备，则在Wireless Band Selection字段中点击与无线信号的所需带宽对应的单选按钮。带宽越高，信号可以承载的数据量就越大。

· 20 MHz — 无线信号的标准频率。

· 20/40 MHz — 自动使用20 MHz和40 MHz信号。40 MHz信号可提供更多带宽，但容易出现更多干扰。此选项仅在连接的无线设备与40 MHz频率兼容时使用。

步骤5.从Wireless Channel下拉列表中选择无线电的无线信道。选择当前未由邻居网络使用的通道。

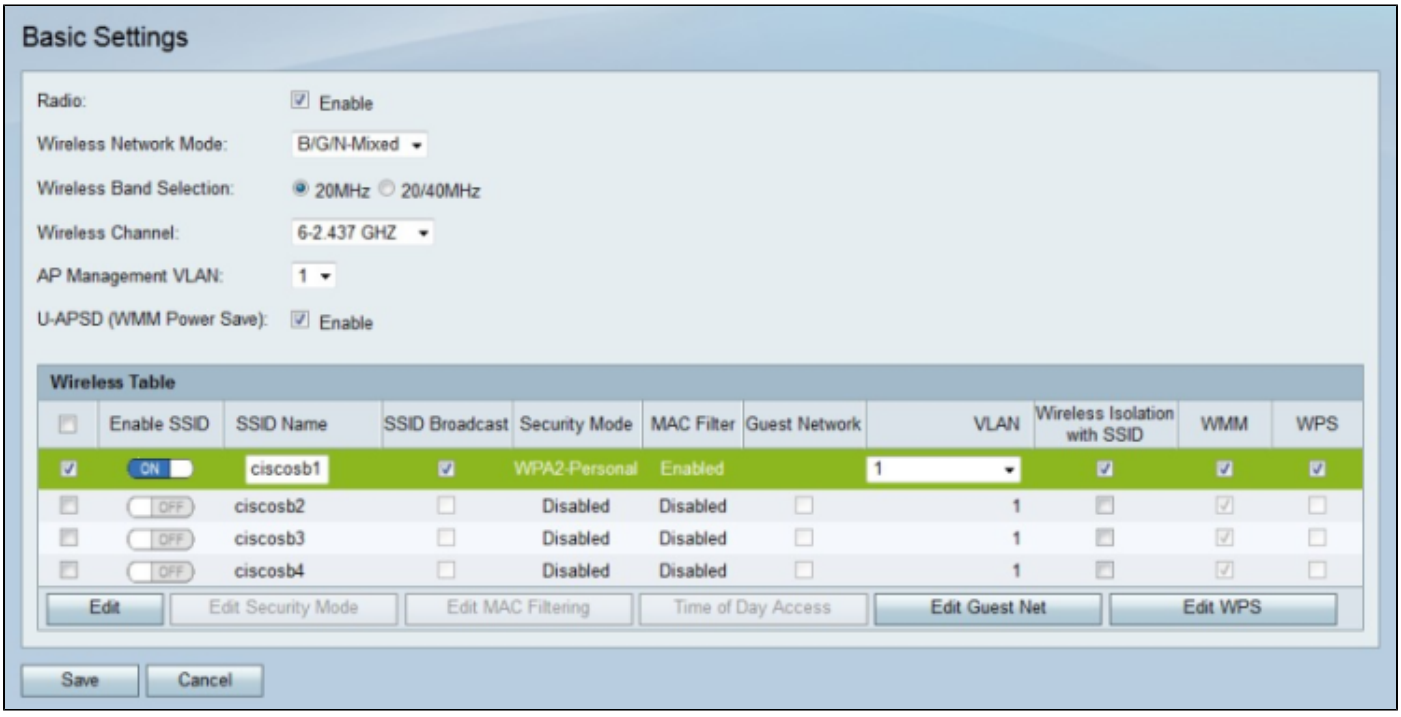
步骤6.从AP管理VLAN下拉列表中选择要成为管理VLAN的VLAN。

第7步。（可选）在U-APSD字段中选中Enable，以启用未计划的自动节能传输(U-APSD)。U-APSD是允许无线电节省功率的功能。但是，U-APSD可能会降低无线电吞吐性能。

步骤8.单击Save。

编辑无线表

步骤1.登录到Web配置实用程序并选择Wireless > Basic Settings。将打开基本设置页面：



步骤2.选中要在无线表中编辑的网络的复选框。

步骤3.单击Edit编辑指定的网络。

步骤4.单击Enable SSID按钮启用网络。服务集标识符(SSID)是无线网络的名称。

步骤5.在SSID Name字段中输入网络名称。网络上的所有设备必须使用此SSID相互通信。

步骤6.选中SSID Broadcast以启用无线广播。启用SSID广播时，RV215W会向附近的无线设备通告其可用性。

步骤7.选中Guest Network以使配置的网络成为访客网络。访客网络是专为临时用户设计的网络的一小部分。这用于允许访客使用网络，而无需暴露私有Wi-Fi密钥。

注意：无法在AP管理VLAN上配置访客网络。

步骤8.从VLAN下拉列表中选择与网络关联的VLAN。

步骤9.选中Wireless Isolation with SSID以禁止指定网络上的设备相互通信。

步骤10.选中WMM以在网络上启用Wi-Fi多媒体(WMM)。WMM用于增强无线设备上的多媒体流。WMM为通过无线连接发送的多媒体流量提供更高的优先级。

步骤11.（可选）选中WPS，将指定的网络分配为Wi-Fi Protected Setup(WPS)网络。WPS是一种可实现轻松且安全网络配置的功能。此功能使设备能够轻松连接到网络。

步骤12.单击Save。

禁用安全

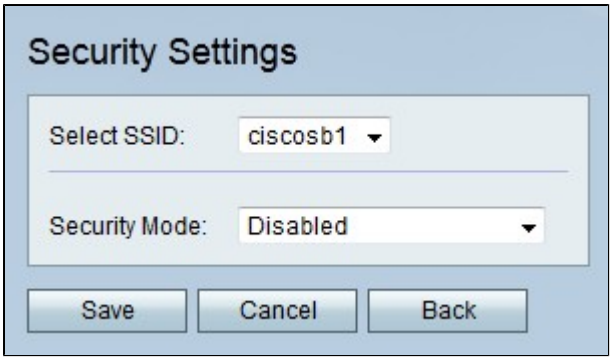
设置测试网络时，为了便于使用，可能会禁用RV215W上的无线安全，但不建议禁用安全。

步骤1.登录到Web配置实用程序并选择Wireless > Basic Settings。将打开基本设置页面。

步骤2.选中要编辑的网络框。

步骤3.单击Edit Security Mode编辑指定网络的安全性。Security Settings页面打开：

步骤4.（可选）从Select SSID下拉列表中选择要为其配置安全性的SSID。



步骤5.从Security Mode下拉列表中选择Disabled。已禁用无线网络的安全性。

步骤6.单击Save。

配置WEP安全

有线等效保密(WEP)是一种保护无线网络的算法。WEP提供的基本加密方法比WPA的安全性低。当连接的网络设备不支持WPA时，使用WEP。

步骤1.登录到Web配置实用程序并选择Wireless > Basic Settings。将打开基本设置页面。

步骤2.选中要编辑的网络框。

步骤3.单击Edit Security Mode编辑指定网络的安全性。Security Settings页面打开：



步骤4.（可选）从Select SSID下拉列表中选择要为其配置安全性的SSID。

步骤5.从Security Mode（安全模式）下拉列表中选择WEP。

步骤6.从Authentication Type下拉列表中选择无线网络的身份验证类型。

·开放系统 — 任何人都可以关联接入点，但需要WEP密钥才能通过网络的接入点传递流量。

·共享密钥 — 需要一个WEP密钥来与接入点关联并通过网络接入点的流量。

步骤7.从Encryption下拉列表中选择WEP密钥的加密方法。

· 10/64位（10个十六进制数字） — 提供40位密钥。

· 26/128位（26个十六进制数字） — 提供104位密钥。这是更安全的加密。

步骤8.在Passphrase字段中输入大于八个字符的口令。

第9步：点击生成(Generate)，在密钥1、密钥2、密钥3和密钥4字段中创建密钥。

注意：您也可以在Key 1、Key 2、Key 3和Key 4字段中手动输入密钥。

步骤10.从TX Key下拉列表中选择用户访问无线网络时必须输入的密钥。

步骤11.（可选）选中Unmask Password以显示密钥的字符串。

步骤12.单击Save。

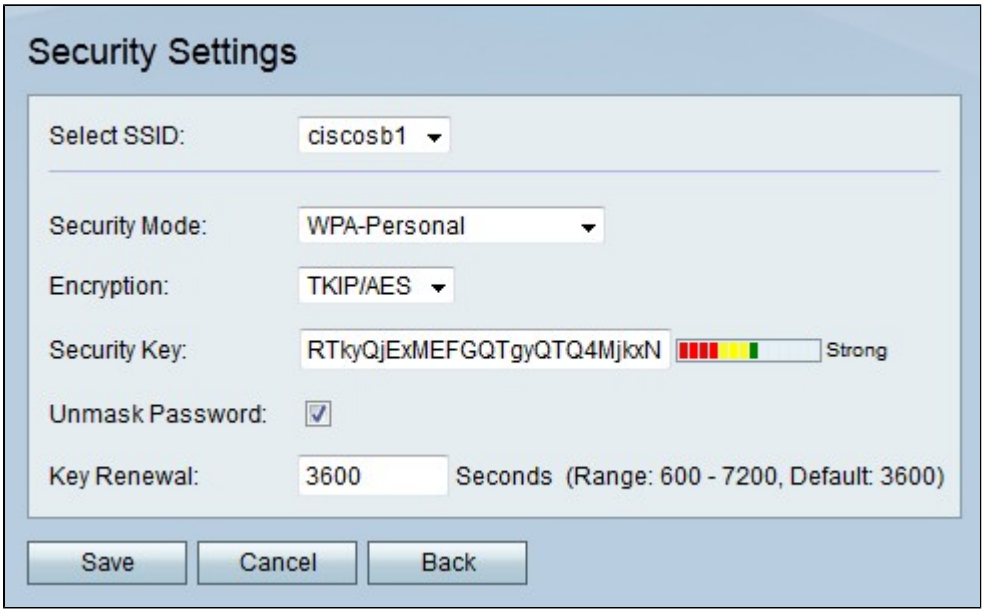
配置WPA个人安全

Wi-Fi保护访问(WPA)是无线网络的安全标准。由于WEP中存在安全缺陷，因此创建了WPA来替换WEP。WPA-Personal是WPA的一个版本，用于只有少数用户的网络。WPA-Personal提供每个用户用于访问无线网络的共享密钥。WPA引入了密钥加密方法：临时密钥完整性协议(TKIP)和高级加密标准(AES)。 更多的网络设备支持TKIP，但AES是更强大的加密方法。

步骤1.登录到Web配置实用程序并选择Wireless > Basic Settings。将打开基本设置页面。

步骤2.选中要编辑的网络框。

步骤3.单击Edit Security Mode编辑指定网络的安全性。Security Settings页面打开：



步骤4.（可选）从Select SSID下拉列表中选择要为其配置安全性的SSID。

步骤5.从Security Mode（安全模式）下拉列表中选择WPA-Personal。

步骤6.从Encryption下拉列表中选择WPA密钥的加密方法。

· TKIP/AES — 当并非所有连接到无线网络的设备都支持AES时，选择此选项。

· AES — 如果连接到无线设备的所有设备都支持AES，则首选此选项。

步骤7.在Security Key字段中输入安全密钥。

步骤8.（可选）选中Unmask Password以显示密钥的字符串。

步骤9.在“密钥续订”字段中输入时间。这是RV215W在生成新密钥之前使用密钥的时间。

步骤10.单击Save。

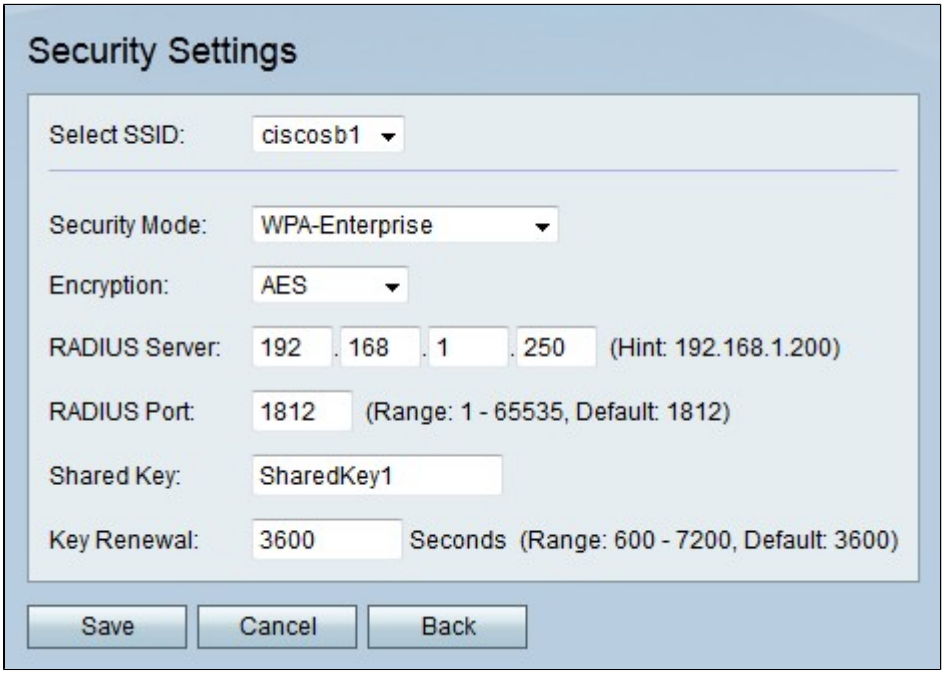
配置WPA-Enterprise安全

Wi-Fi保护访问(WPA)是无线网络的安全标准。由于WEP中存在安全缺陷，因此创建了WPA来替换WEP。WPA-Enterprise是WPA的一个版本，建议用于具有许多用户（如企业）的网络。用于获取访问的身份验证由RADIUS服务器控制。这意味着每个连接的用户都将获得访问无线网络的唯一密钥。WPA引入了密钥加密方法：临时密钥完整性协议(TKIP)和高级加密标准(AES)。 更多的网络设备支持TKIP，但AES是更强大的加密方法。

步骤1.登录到Web配置实用程序并选择Wireless > Basic Settings。将打开基本设置页面。

步骤2.选中要编辑的网络框。

步骤3.单击Edit Security Mode编辑指定网络的安全性。Security Settings页面打开：



步骤4.（可选）从Select SSID下拉列表中选择要为其配置安全性的SSID。

步骤5.从Security Mode下拉列表中选择WPA-Enterprise。

步骤6.从Encryption下拉列表中选择WPA密钥的加密方法。

· TKIP/AES — 当并非所有连接到无线网络的设备都支持AES时，选择此选项。

· AES — 如果连接到无线设备的所有设备都支持AES，则首选此选项。

步骤7.在RADIUS Server字段中输入RADIUS服务器的IP地址。

步骤8.在RADIUS Port字段中输入用于访问RADIUS服务器的端口号。

步骤9.在Shared Key字段中输入无线用户的预共享密钥。预共享密钥是供所有用户使用的密钥。预共享密钥功能是与RADIUS身份验证一起添加的安全功能。

步骤10.在“密钥续订”字段中输入时间。这是RV215W在生成新密钥之前使用密钥的时间。

步骤11.单击Save。

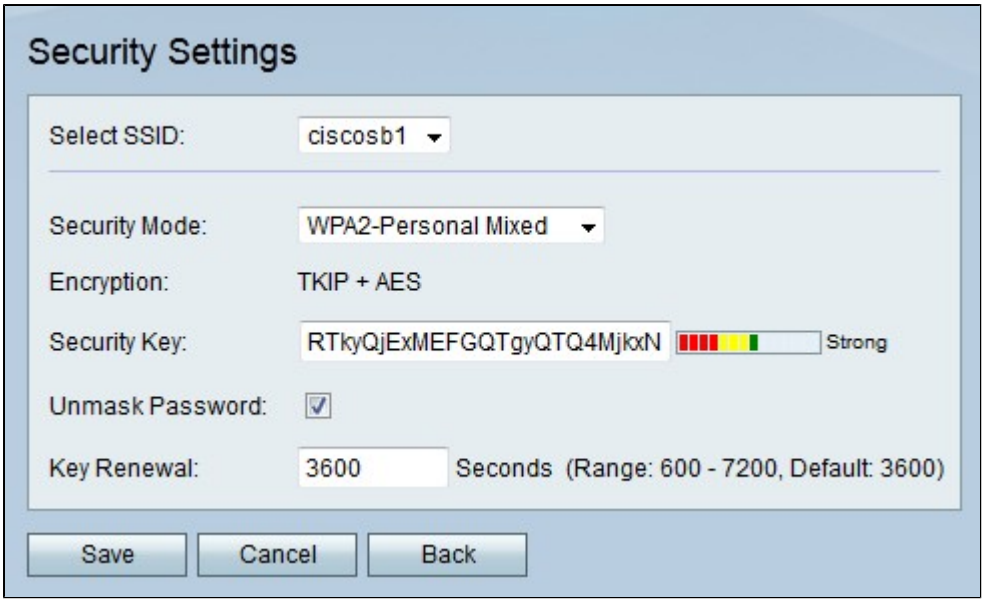
配置WPA2 — 个人/WPA2 — 个人混合安全

Wi-Fi保护访问2(WPA2)是无线网络的安全标准。WPA2是WPA的增强版。WPA2提供比WPA更高的安全性，但WPA2需要更高的处理能力。WPA2-Personal/WPA2-Personal Mixed是WPA2的版本，用于用户较少的网络中。WPA2-Personal Mixed旨在向后兼容无法使用WPA2的较旧设备。如果可能，请勿使用WPA2-Personal Mixed，因为它提供的连接安全性较低。WPA2-Personal提供每个用户用于访问无线网络的共享密钥。WPA2使用临时密钥完整性协议(TKIP)和高级加密标准(AES)加密方法。 更多的网络设备支持TKIP，但AES是更强大的加密方法。

步骤1.登录到Web配置实用程序并选择Wireless > Basic Settings。将打开基本设置页面。

步骤2.选中要编辑的网络框。

步骤3.单击Edit Security Mode编辑指定网络的安全性。Security Settings页面打开：



步骤4.（可选）从Select SSID下拉列表中选择要为其配置安全性的SSID。

步骤5.从Security Mode下拉列表中选择WPA2-Personal或WPA2-Personal Mixed。当无线网络上的所有设备都支持AES时，使用WPA2-Personal。当并非所有设备都支持AES时，使用WPA2-Personal Mixed。

注意：安全方法使用的加密类型显示在Encryption字段中。

步骤6.在Security Key字段中输入安全密钥。

步骤7.（可选）选中Unmask Password以显示密钥的字符串。

步骤8.在Key Renewal字段中输入时间。这是RV215W在生成新密钥之前使用密钥的时间。

步骤9.单击Save。

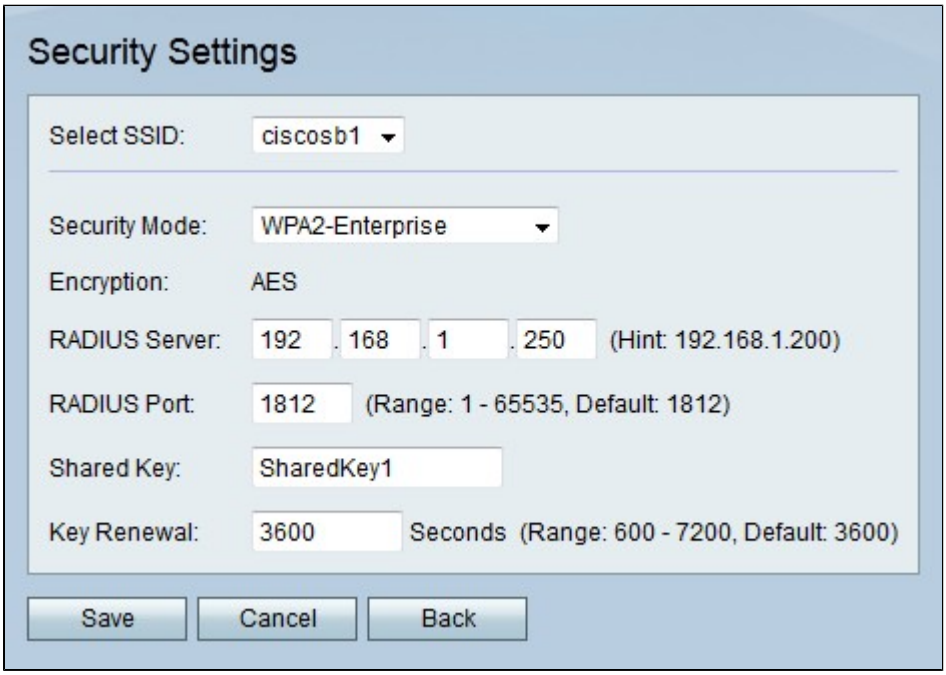
配置WPA2-Enterprise/WPA2-Enterprise混合安全

Wi-Fi保护访问2(WPA2)是无线网络的安全标准。WPA2是WPA的增强版。WPA2提供比WPA更高的安全性，但WPA2需要更高的处理能力。WPA2-Enterprise/WPA2-Enterprise Mixed是WPA2的版本，用于具有许多用户（如企业）的网络。WPA2-Enterprise Mixed设计用于向后兼容不能使用WPA2的较旧设备。如果可能，请勿使用WPA2-Enterprise Mixed，因为它提供的连接安全性较低。确定用户是否获得访问权限的身份验证由RADIUS服务器控制。这意味着每个连接的用户都将获得访问无线网络的唯一密钥。WPA2使用临时密钥完整性协议(TKIP)和高级加密标准(AES)加密方法。更多的网络设备支持TKIP，但AES是更强大的加密方法。

步骤1.登录到Web配置实用程序并选择Wireless > Basic Settings。将打开基本设置页面。

步骤2.选中要编辑的网络框。

步骤3.单击Edit Security Mode编辑指定网络的安全性。Security Settings页面打开：



步骤4.（可选）从Select SSID下拉列表中选择要为其配置安全性的SSID。

步骤5.从Security Mode下拉列表中选择WPA2-Enterprise或WPA2-Enterprise Mixed。当无线网络上的所有设备都支持AES时，使用WPA2-Enterprise。当并非所有设备都支持AES时，使用WPA2-Enterprise Mixed。

注意：安全方法使用的加密类型显示在Encryption字段中。

步骤6.在RADIUS Server字段中输入RADIUS服务器的IP地址。

步骤7.在RADIUS Port字段中输入用于访问RADIUS服务器的端口。

步骤8.在Shared Key字段中输入无线用户的预共享密钥。预共享密钥是供所有用户使用的密钥。预共享密钥功能是与RADIUS身份验证一起添加的安全功能。

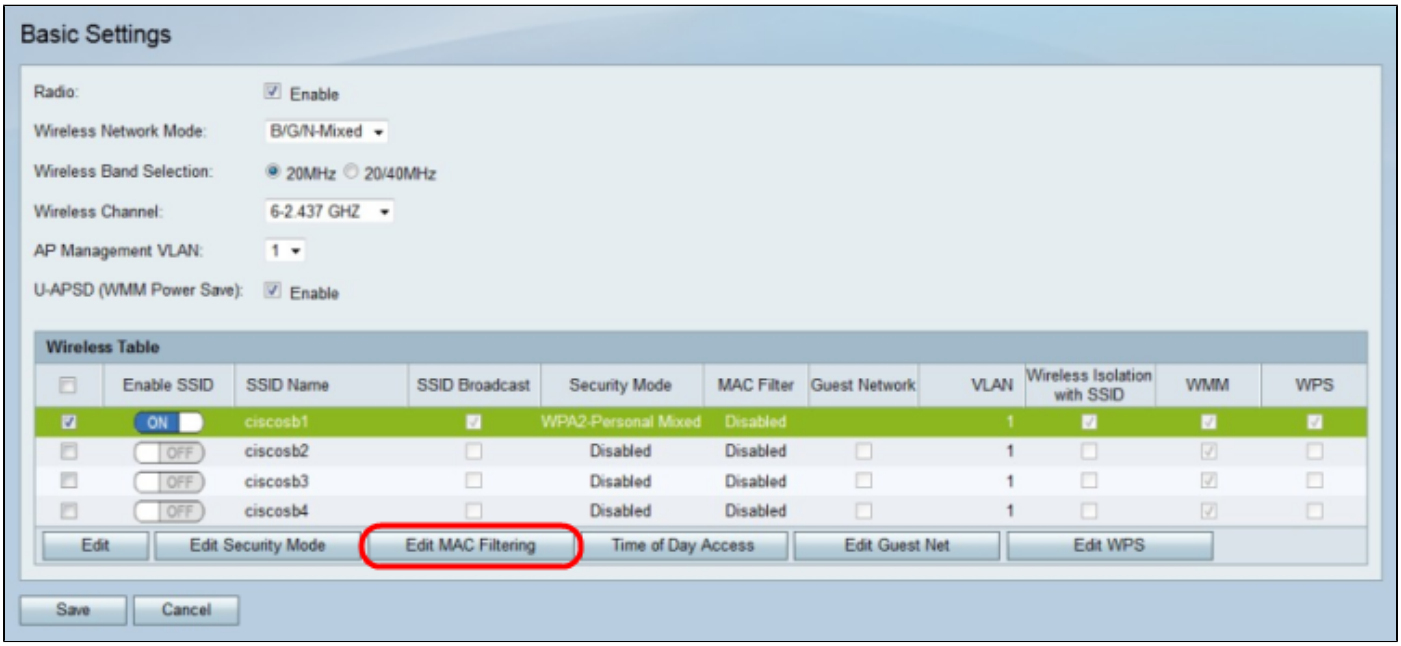
步骤9.在“密钥续订”字段中输入时间。这是RV215W在生成新密钥之前使用密钥的时间。

步骤10.单击Save。

编辑MAC过滤

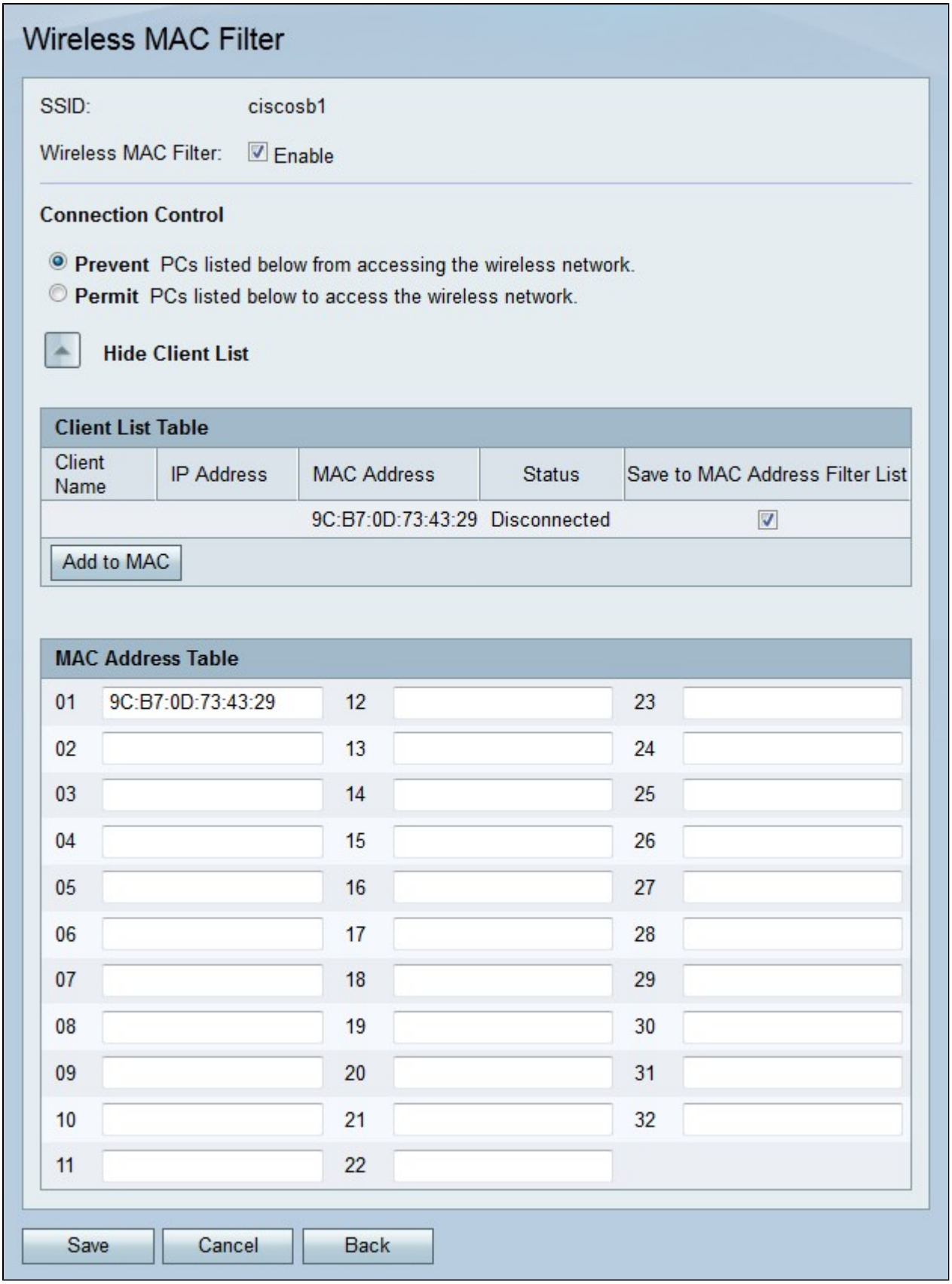
MAC过滤用于根据连接设备的MAC地址允许或拒绝对无线网络的访问。

步骤1.登录到Web配置实用程序并选择Wireless > Basic Settings。将打开基本设置页面：



步骤2.选中要编辑的网络框。

步骤3.单击Edit MAC Filtering为指定的网络创建MAC访问控制列表。Wireless MAC Filter页面打开：



步骤4.选中Enable以启用网络上的MAC过滤。

步骤5.点击与Connection Control字段中的所需列表类型对应的单选按钮。

·阻止PC — 阻止具有所列的MAC地址的PC进入网络。

· Permit PCs — 允许具有列出的MAC地址的PC进入网络。

步骤6.在MAC地址表中输入所需的MAC地址。

第 7 步： 点击保存。

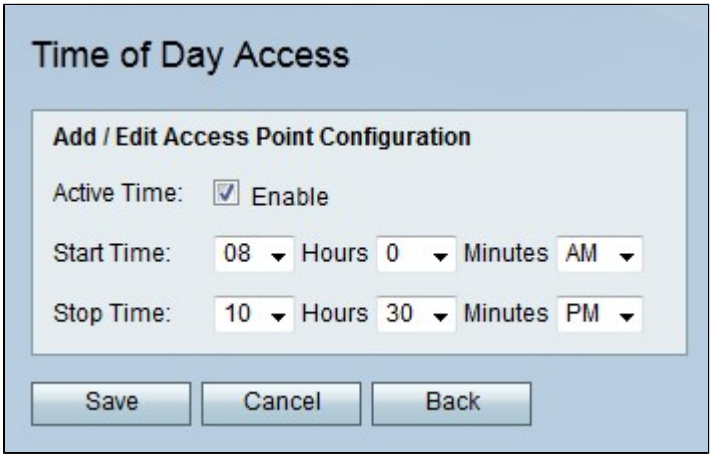
访问时间

“访问时间”功能仅允许根据已配置的计划访问用户。

步骤1.登录到Web配置实用程序并选择Wireless > Basic Settings。将打开基本设置页面：

步骤2.选中要编辑的网络框。

步骤3.单击Time of Day Access配置用户何时可以访问指定的网络。Time of Day Access页面打开：



步骤4.选中Active Time字段中的Enable，启用对网络的当日访问时间。

步骤5.在“开始时间”字段中输入开始访问网络的时间。

步骤6.在Stop Time字段中输入网络访问结束的时间。

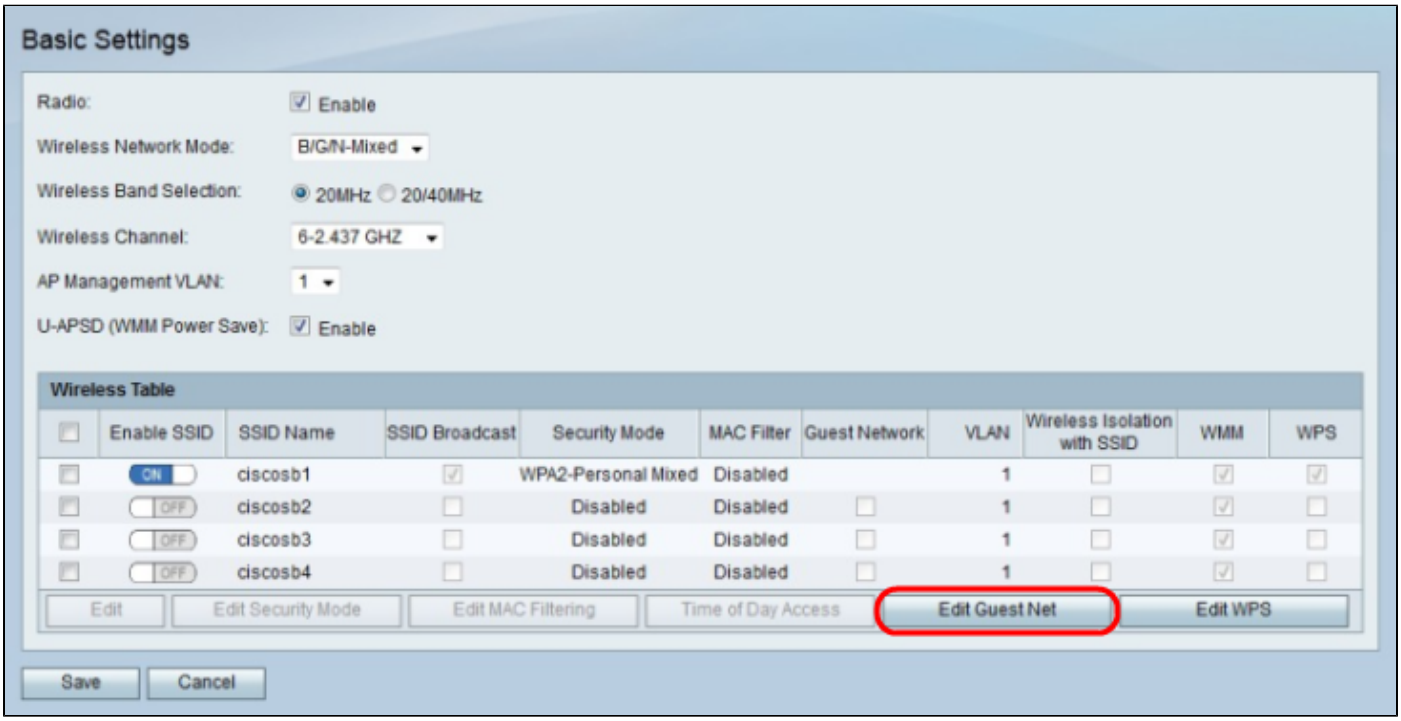
第 7 步： 点击保存。

编辑访客网络

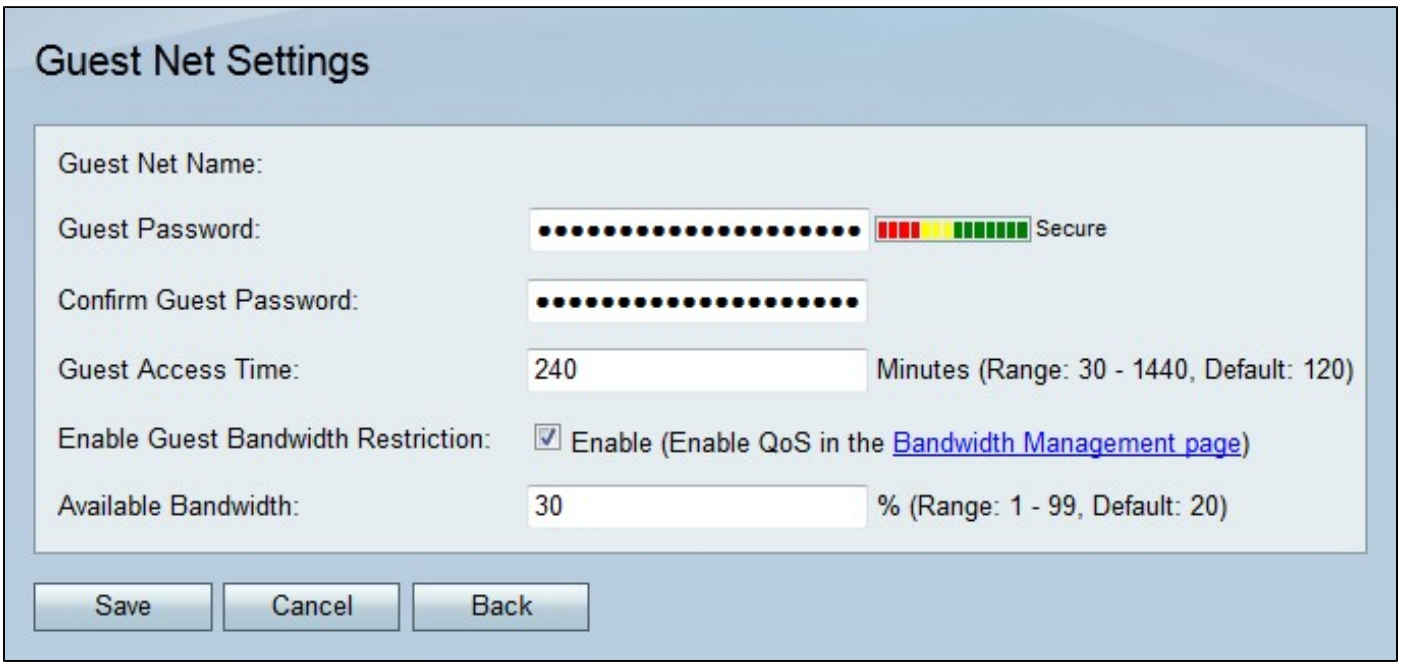
访客网络是专为临时用户设计的网络的一小部分。这用于允许访客使用网络，而无需暴露私有Wi-

Fi密钥。访客网络可以配置为限制用户的访问时间和带宽使用。

步骤1.登录到Web配置实用程序并选择Wireless > Basic Settings。将打开基本设置页面：



步骤2.单击Edit Guest Network配置访客网络。将打开访客网络设置页面：



步骤3.在Guest Password字段中输入用户用于输入访客网络的密码。

步骤4.在Confirm Guest Password字段中重新输入用户将用于输入访客网络的密码。

步骤5.在Guest Access Time中输入允许用户与访客网络保持连接的时间。

步骤6.选中Enable Guest Bandwidth Restriction以限制访客网络接收的带宽量。

注意：必须在Bandwidth Management页面上启用Bandwidth Management。

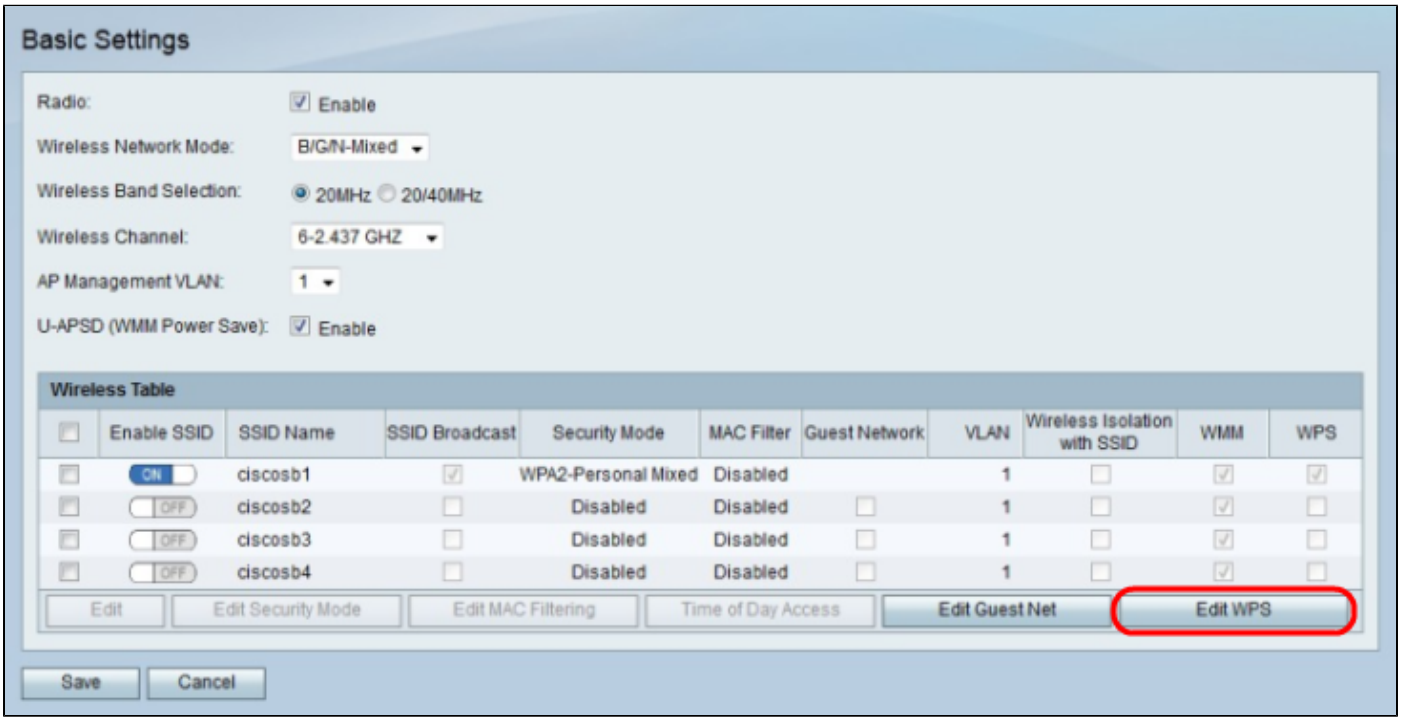
步骤7.在Available Bandwidth字段中输入访客网络可用的带宽百分比。

步骤8.单击Save。

配置WPS方法1

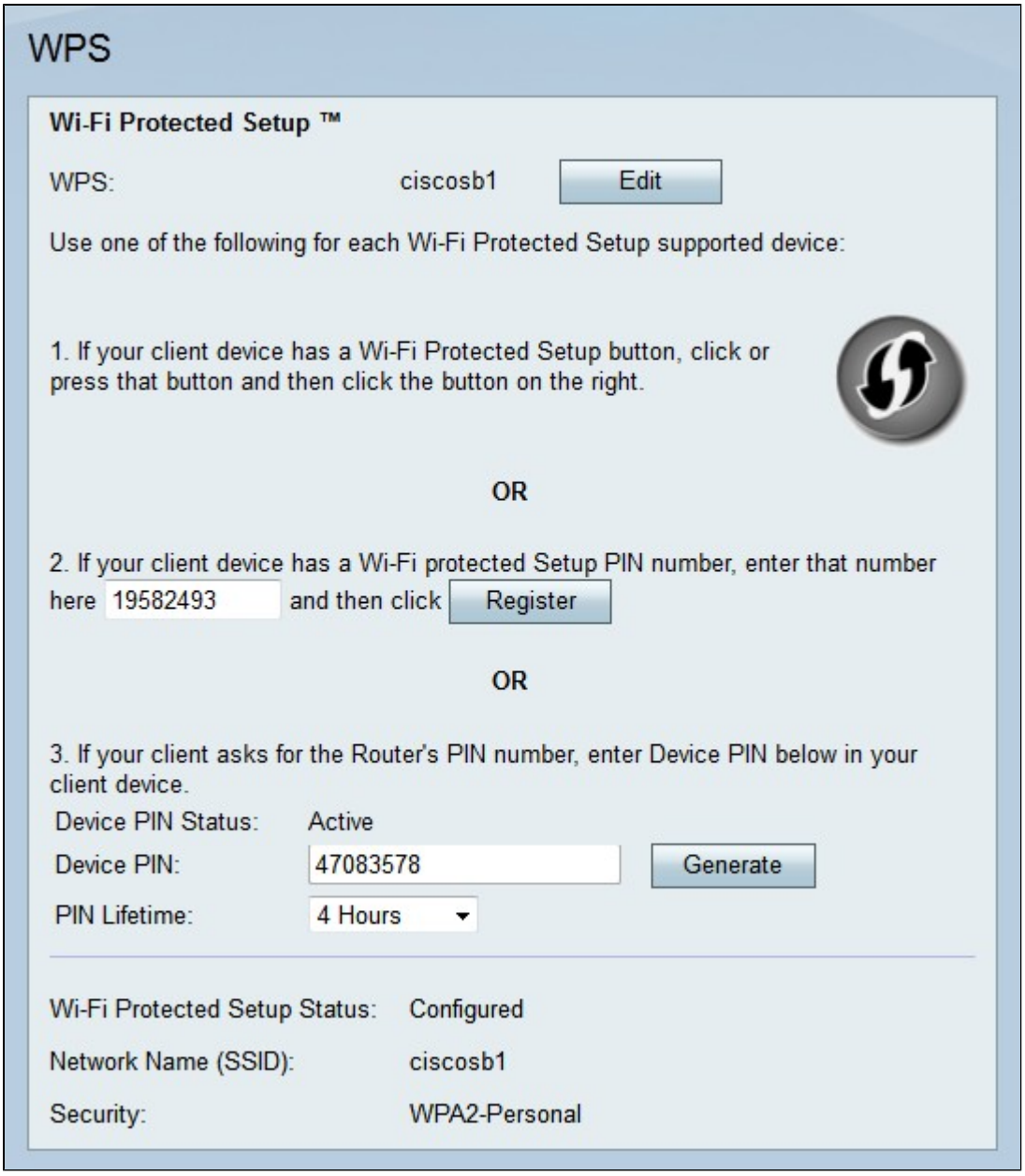
Wi-Fi Protected Setup(WPS)是一项提供简单且安全的无线网络设置的功能。要连接到WPS，连接设备必须支持WPS且必须与WPA安全兼容。第一种配置方法是要求按下RV215W WPS按钮和客户端设备按钮的简单方法。按下这两个按钮后，客户端设备即连接到WPS网络。

步骤1.登录到Web配置实用程序并选择Wireless > Basic Settings。将打开基本设置页面：



步骤2.单击Edit WPS以配置WPS。将打开WPS页面：

注意：WPS页面也可以通过无线> WPS访问。



步骤3.单击Edit选择要启用WPS的无线网络。



步骤4.点击WPS页面上的WPS按钮。

步骤5.点击客户端设备或客户端设备的实用程序屏幕上的WPS按钮，将客户端设备连接到WPS网络。

以下字段显示WPS配置的信息。

· Wi-Fi Protected Setup Status - WPS配置的状态。

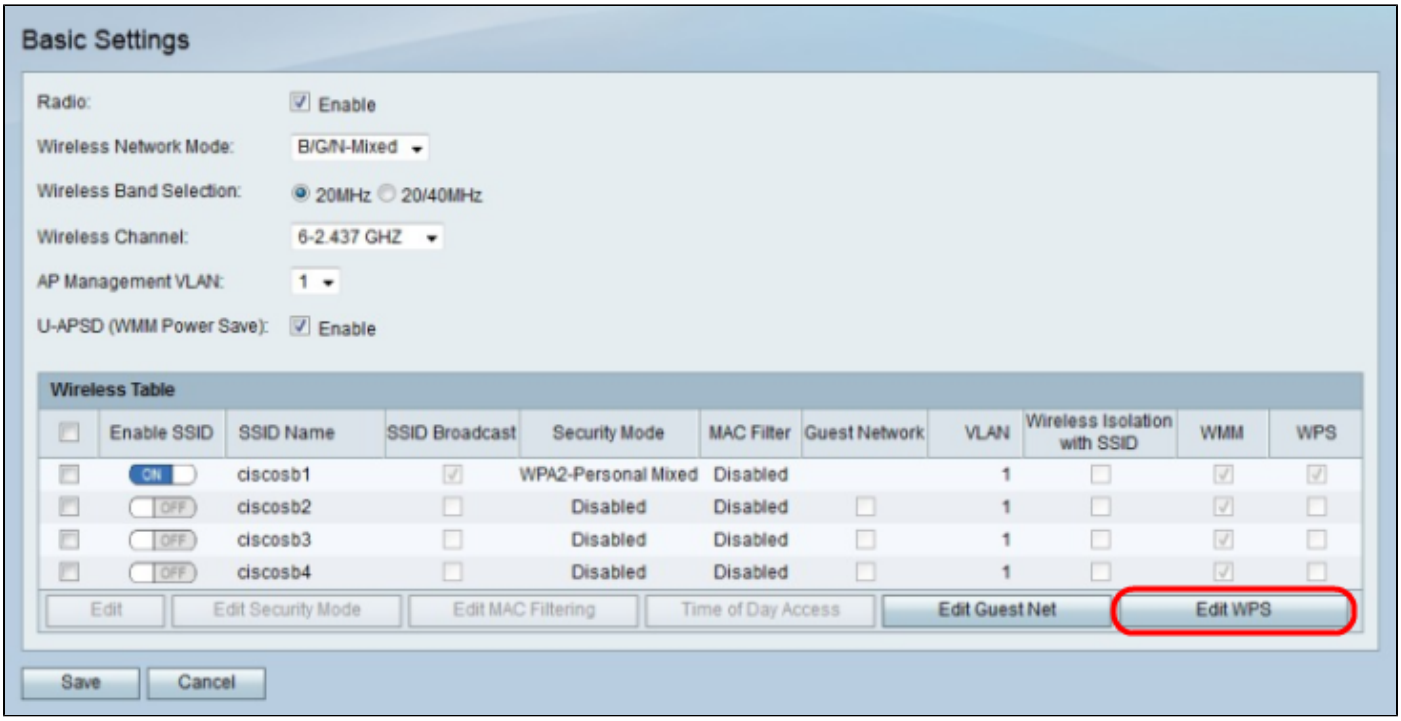
·网络名称(SSID) — 由RV215W分配给WPS配置的网络名称。

· WPA2-Personal - WPS配置使用的安全类型。

配置WPS方法2

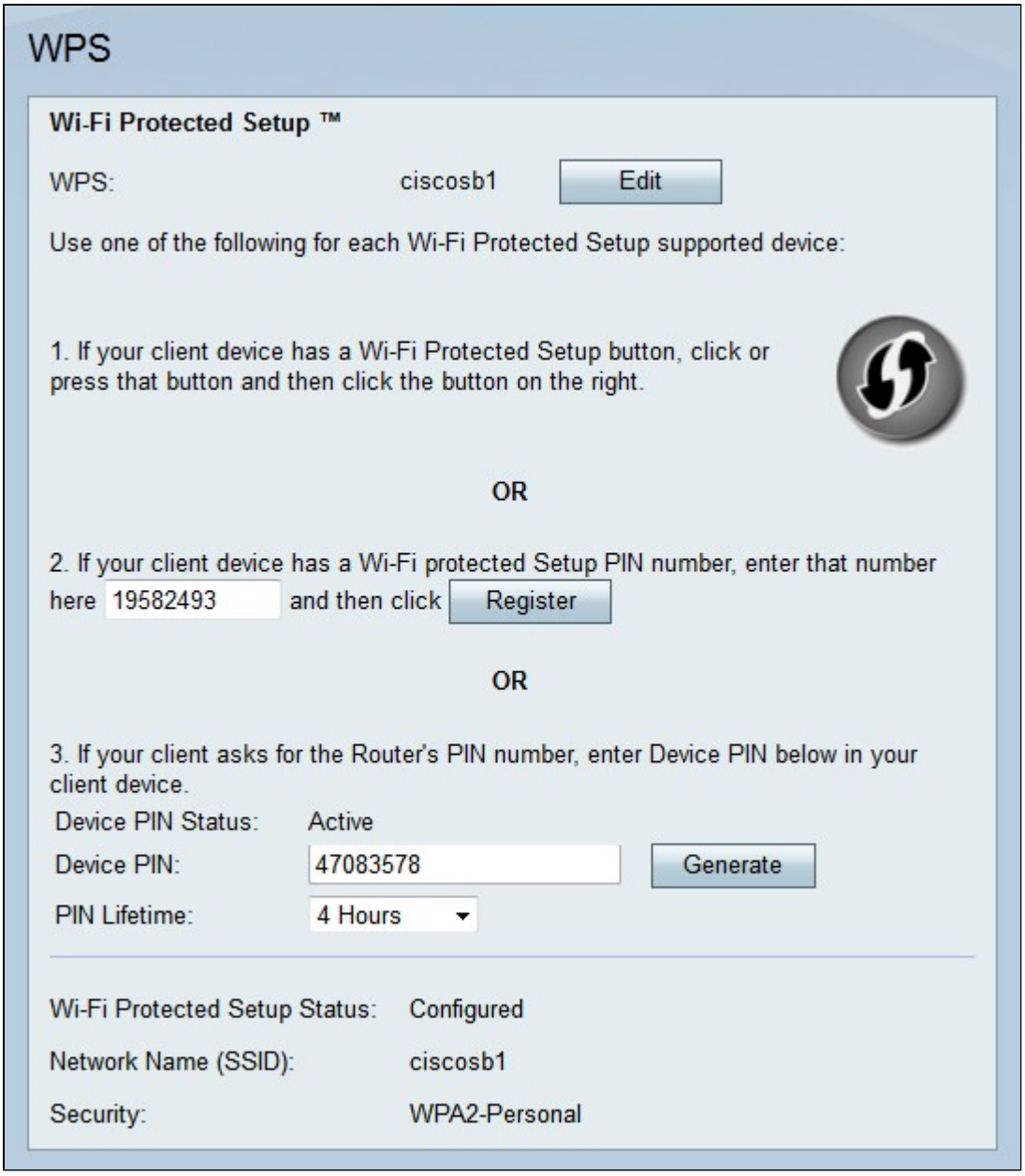
Wi-Fi Protected Setup(WPS)是一项提供简单且安全的无线网络设置的功能。要连接到WPS，连接设备必须支持WPS且必须与WPA安全兼容。第二种方法需要客户端设备的PIN号。在WPS页面上输入PIN编号后，客户端设备将连接到WPS网络。

步骤1.登录到Web配置实用程序并选择Wireless > Basic Settings。将打开基本设置页面：



步骤2.单击Edit WPS以配置WPS。将打开WPS页面：

注意：WPS页面也可以通过无线> WPS访问。



步骤3.单击Edit选择要启用WPS的无线网络。

步骤4.输入客户端设备的PIN码。

步骤5.单击Register创建WPS网络。

以下字段显示WPS配置的信息。

· Wi-Fi Protected Setup Status - WPS配置的状态。

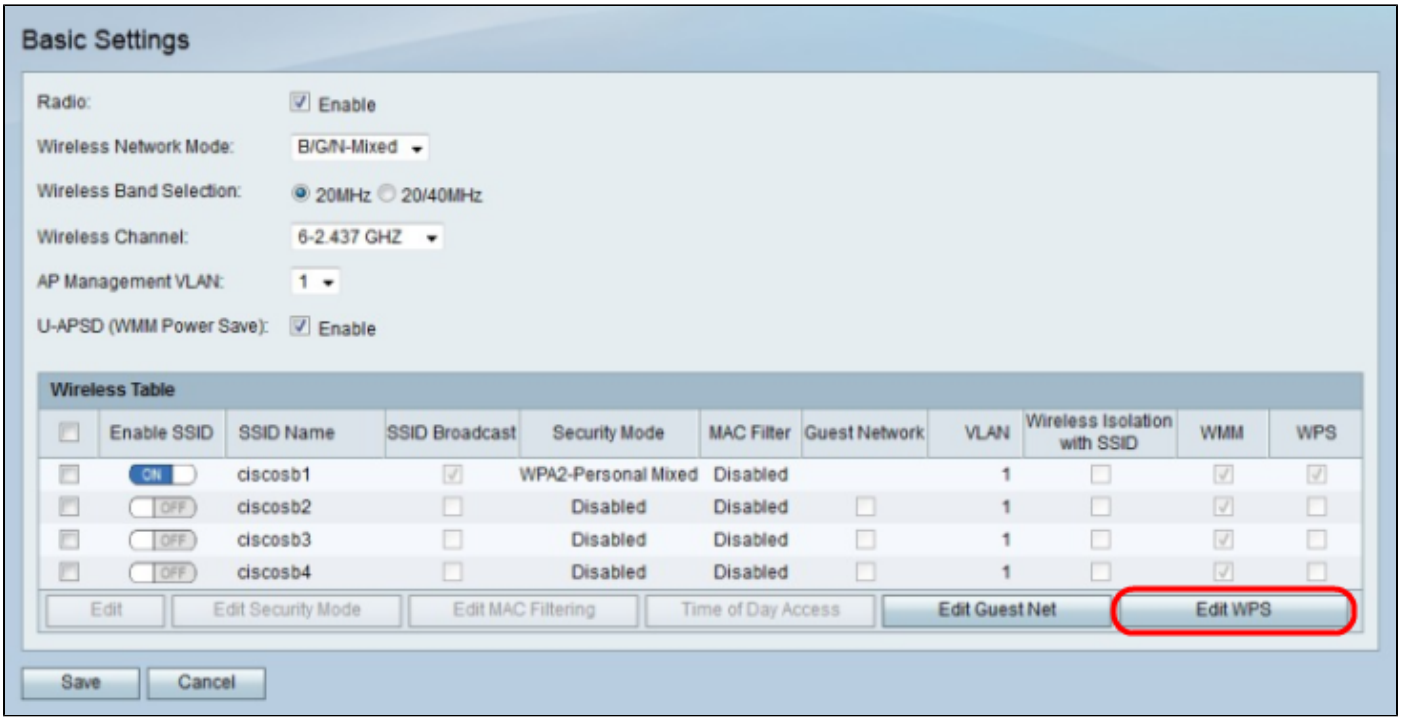
·网络名称(SSID) — 由RV215W分配给WPS配置的网络名称。

· WPA2-Personal - WPS配置使用的安全类型。

配置WPS方法3

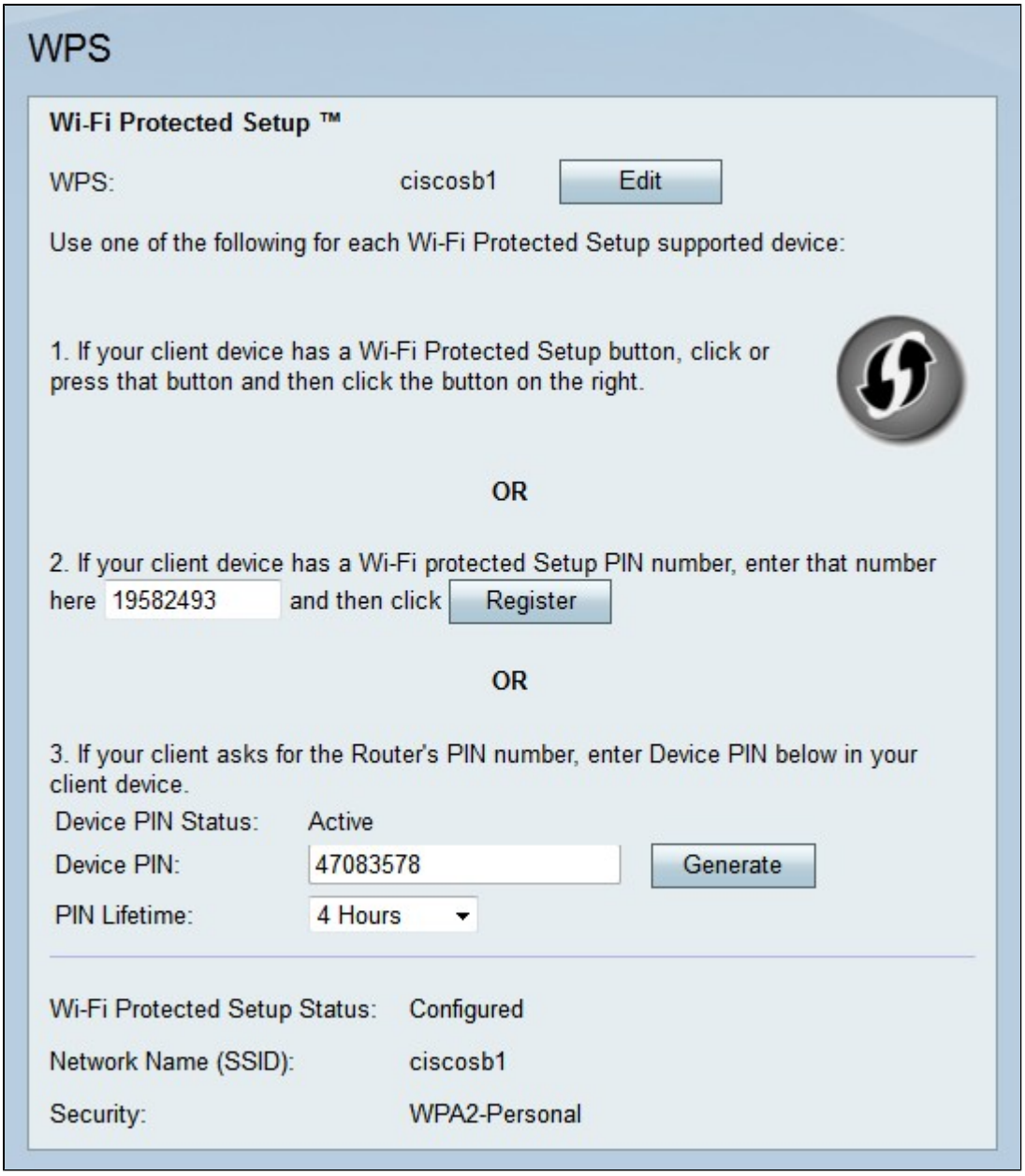
Wi-Fi Protected Setup(WPS)是一项提供简单且安全的无线网络设置的功能。要连接到WPS，连接设备必须支持WPS且必须与WPA安全兼容。第三种方法要求用户在客户端设备的WPS配置页面上输入RV215W的PIN号码。

步骤1.登录到Web配置实用程序并选择Wireless > Basic Settings。将打开基本设置页面：



步骤2.单击Edit WPS以配置WPS。将打开WPS页面：

注意：WPS页面也可以通过无线> WPS访问。



步骤3.单击Edit选择要启用WPS的无线网络。

步骤4.单击Generate生成RV215W的PIN号。

步骤5.从PIN Lifetime下拉列表中选择生成新PIN之前经过的时间。

步骤6.在客户端设备配置中输入给定的RV215W PIN编号。客户端设备连接到WPS网络。

以下字段显示WPS配置的信息。

· Wi-Fi Protected Setup Status - WPS配置的状态。

·网络名称(SSID) — 由RV215W分配给WPS配置的网络名称。

· WPA2-Personal - WPS配置使用的安全类型。

如果您想查看RV215W路由器的所有其他文档，请单击此处。

观看与本文相关的视频...

点击此处查看思科的其他技术讲座

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）。