

# RV110W上的SSID安全设置

## 目标

安全模式为无线网络提供保护。不同的服务集ID(SSID)可以有不同的安全模式。SSID可能对网络执行不同的功能；因此，SSID可能需要不同的安全措施。本文说明如何在RV110W上配置SSID的安全设置。

## 适用设备

- RV110W

## 步骤

步骤1.使用Web配置实用程序选择Wireless > Basic Settings。

Basic Settings

Radio:  Enable

Wireless Network Mode: B/G/N-Mixed

Wireless Band Selection:  20MHz  20/40MHz

Wireless Channel: 6-2.437 GHZ

AP Management VLAN: 1

U-APSD (WMM Power Save):  Enable

<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	VLAN	Wireless Isolation with SSID	WMM	WPS Hardware Button
<input checked="" type="checkbox"/>	ON	ciscosb1	<input checked="" type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/>	OFF	ciscosb2	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/>	OFF	ciscosb3	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/>	OFF	ciscosb4	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>

Edit Edit Security Mode Edit MAC Filtering Time of Day Access

Save Cancel

<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	VLAN	Wireless Isolation with SSID	WMM	WPS Hardware Button
<input checked="" type="checkbox"/>	ON	ciscosb1	<input checked="" type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/>	OFF	ciscosb2	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/>	OFF	ciscosb3	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/>	OFF	ciscosb4	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>

Edit Edit Security Mode Edit MAC Filtering Time of Day Access

步骤2.在Wireless Table (无线表)中，勾选要为其编辑安全设置的SSID的复选框。

步骤3.单击“编辑安全模式”。这将打开“安全设置”页。

The screenshot shows a 'Security Settings' window. At the top, it says 'Security Settings'. Below that, there is a 'Select SSID:' dropdown menu with 'ciscosb1' selected. Underneath is a 'Security Mode:' dropdown menu with 'Disabled' selected. At the bottom, there are three buttons: 'Save', 'Cancel', and 'Back'.

步骤4.从Select SSID下拉菜单中，选择要编辑其安全设置的SSID。

## 禁用安全模式

此过程显示如何禁用SSID的安全模式，该模式无需安全信息即可使用SSID。

步骤1.从Security Mode下拉菜单中，选择**Disabled**。

步骤2.单击**Save**以保存更改，**Cancel**以放弃更改，或单击**Back**返回上一页。

## WEP安全模式

此过程显示如何将有线等效保密(WEP)设置为SSID的安全模式。WEP不是最安全的安全模式，但是，如果某些网络设备不支持WPA，则它可能是唯一的选项。

步骤1.从Security Mode下拉菜单中，选择**WEP**。

The screenshot shows a 'Security Settings' window. At the top, it says 'Security Settings'. Below that, there is a 'Select SSID:' dropdown menu with 'ciscosb1' selected. Underneath is a 'Security Mode:' dropdown menu with 'WEP' selected. Below that is an 'Authentication Type:' dropdown menu with 'Open System' selected and '(Default: Open System)' in parentheses. Below that is an 'Encryption:' dropdown menu with '10/64-bit(10 hex digits)' selected. Below that is a 'Passphrase:' field with a 'Generate' button to its right. Below that are four 'Key' fields (Key 1, Key 2, Key 3, Key 4) and a 'TX Key:' dropdown menu with '1' selected. Below that is an 'Unmask Password:' checkbox which is unchecked. At the bottom, there are three buttons: 'Save', 'Cancel', and 'Back'.

步骤2.从Authentication Type下拉菜单中，选择一个选项。

- 开放系统 — 此选项比共享密钥身份验证更直接、更安全。
- 共享密钥 — 此选项比开放系统安全。

步骤3.从Encryption下拉菜单中，选择10/64位（10个十六进制数字）（使用40位密钥）或26/128位（26个十六进制数字）（使用104位密钥）。

步骤4.在Passphrase字段中，输入长度至少为8个字符的字母和数字的密码。

步骤5.单击**Generate**在Key字段中创建四个WEP密钥，或在Key字段中手动输入WEP密钥。

步骤6.从TX Key下拉菜单中，选择要用作共享密钥的WEP密钥的Key字段编号。

步骤7.如果要显示**密码字符**，请选中Unmask Password复选框。

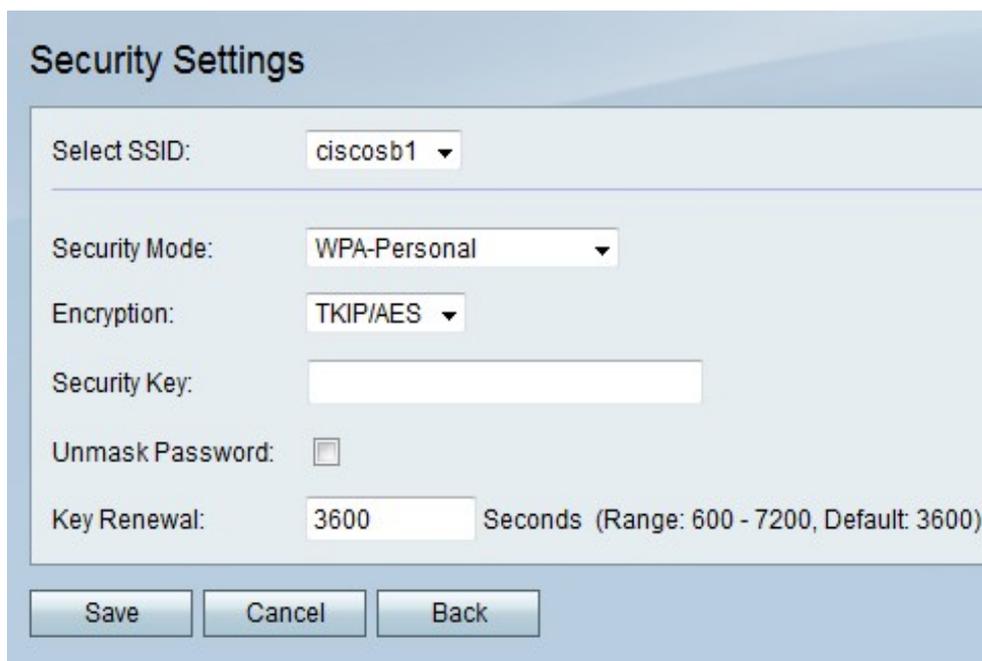
步骤8.单击**Save**以保存更改，**Cancel**以放弃更改，或单击Back返回上一页。

## WPA — 个人、WPA2 — 个人和WPA2 — 个人混合安全模式

Wi-Fi保护访问(WPA)是比WEP更强的安全模式。WPA-Personal可以使用临时密钥完整性协议(TKIP)或高级加密标准(AES)进行加密。WPA2-Personal仅使用AES进行加密，使用预共享密钥(PSK)进行身份验证。WPA2-Personal Mixed可同时支持WPA和WPA2客户端，并使用AES和PSK。此过程显示如何将WPA-Personal、WPA2-Personal或WPA2-Personal Mixed设置为SSID的安全模式。

步骤1.从Security Mode下拉菜单中选择一个选项。

- WPA-Personal — 此选项支持AES和TKIP。
- WPA2-Personal — 此选项支持AES和PSK。
- WPA2 — 个人混合 — 此选项同时支持WPA和WPA2客户端。



步骤2.如果选择WPA-Personal，请从Encryption下拉菜单中选择加密类型。

- TKIP/AES — 此选项与不支持AES的旧设备兼容。
- AES — 此选项比TKIP/AES更安全。

步骤3.在Security Key字段中，输入限制对网络访问的字母和数字短语。

步骤4.如果要显示**密码字符**，请选中取消掩码密码复选框。

步骤5.在Key Renewal字段中，输入网络重新发送密钥的频率（以秒为单位）。

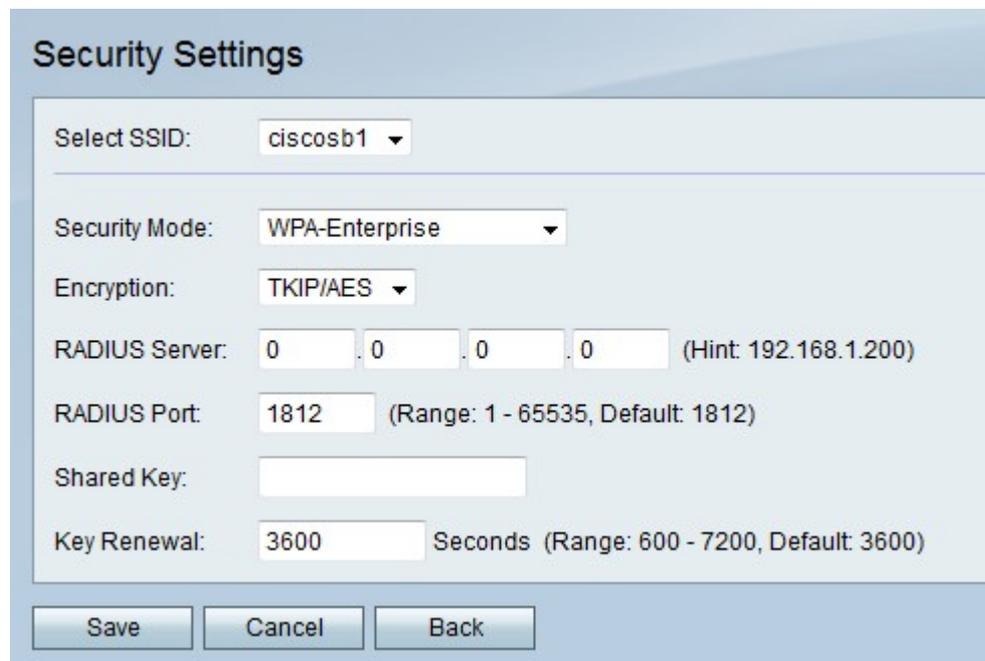
步骤6.单击**Save**以保存更改，**Cancel**以放弃更改，或单击Back返回上一页。

## WPA-Enterprise、WPA2-Enterprise和WPA2-Enterprise混合安全模式

企业安全模式使用远程身份验证拨入用户服务(RADIUS)服务器身份验证。RADIUS是使用独立服务器的网络协议，进出网络的流量必须通过RADIUS服务器。此过程显示如何将WPA-Enterprise、WPA2-Enterprise或WPA2-Enterprise Mixed设置为SSID的安全模式。

步骤1.从Security Mode下拉菜单中选择一个选项。

- WPA-Enterprise — 此选项使用RADIUS、AES和TKIP。
- WPA2-Enterprise — 此选项使用RADIUS、AES和PSK。
- WPA2 — 企业混合 — 此选项使用RADIUS并同时支持WPA和WPA2客户端。



步骤2.如果选择WPA-Enterprise，请从Encryption下拉菜单中选择加密类型。

- TKIP/AES — 此选项与不支持AES的旧设备兼容。
- AES — 此选项比TKIP/AES更安全。

步骤3.在RADIUS Server字段中，输入RADIUS服务器的IP地址。

步骤4.在RADIUS Port字段中，输入网络访问RADIUS服务器的端口号。

步骤5.在Shared Key字段中，输入限制对网络访问的字母和数字短语。

步骤6.在Key Renewal字段中，输入网络更新密钥的频率（以秒为单位）。

步骤7.单击**Save**保存更改，**Cancel**放弃更改，或单击**Back**返回上一页。