

在RV110W的SSID安全设置

客观

安全模式无线网络的提供保护。不同的服务集ID (Ssid)能有不同的安全模式。Ssid可能执行网络的不同的功能;因此， Ssid可能要求不同的安全措施。此条款说明如何配置一SSID的安全设置在RV110W。

可适用的设备

- RV110W

步骤程序

第 1 步：请使用Web配置工具选择无线>基本设置。

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

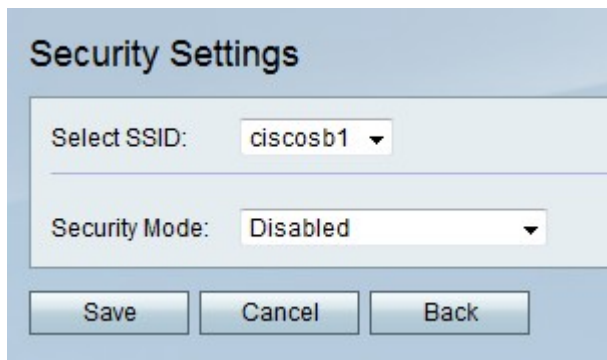
Save Cancel

<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

Step 2.在无线表里，请检查您要编辑安全设置SSID的复选框。

步骤3.点击编辑安全模式。这打开安全设置页。



Security Settings

Select SSID: ciscosb1

Security Mode: Disabled

Save Cancel Back

第 4 步：从挑选SSID下拉菜单，请选择您要编辑安全设置的SSID。

禁用安全模式

此程序显示如何禁用SSID的安全模式哪些不会要求安全信息使用SSID。

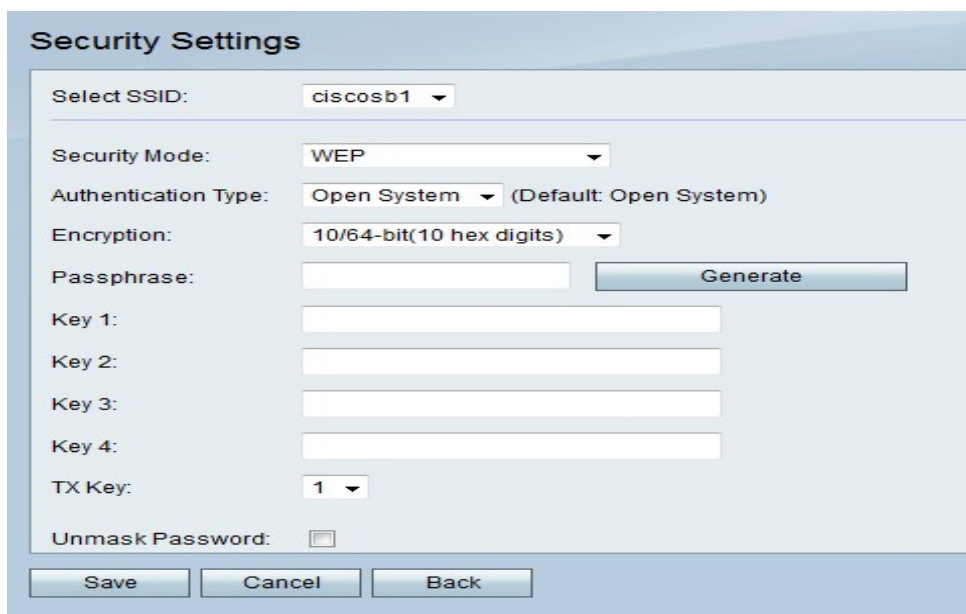
第 1 步：从安全模式下拉菜单，请选择失效。

步骤2.点击“Save”保存更改，取消丢弃他们，或者回到回归到上一页。

WEP安全模式

此程序显示如何设置有线等效保密(WEP)作为SSID的安全模式。WEP不是最安全的安全模式，但是它可能是唯一选择，如果一些网络设备不支持WPA。

第 1 步：从安全模式下拉菜单，请选择WEP。



Security Settings

Select SSID: ciscosb1

Security Mode: WEP

Authentication Type: Open System (Default: Open System)

Encryption: 10/64-bit(10 hex digits)

Passphrase:

Key 1:

Key 2:

Key 3:

Key 4:

TX Key: 1

Unmask Password:

Save Cancel Back

Step 2.从认证类型下拉菜单，请选择选项。

- 开放式系统—此选项比共享密钥认证是更多直接和安全。
- 共享密钥—此选项比开放式系统较不安全。

第 3 步：从加密下拉菜单，请选择10/64-bit(10六角形的位)，使用40位键，或者26/128-bit(26六角形的位)，使用一个104-bit键。

第 4 步：在长期是至少8个字符的密码短语字段，请进入与字母和编号的一密码短语。

步骤5.点击**生成**创建在关键字段的四把WEP密钥或者手工输入WEP密钥在关键字段。

第6.步。从TX关键下拉菜单，请选择您要使用作为共享密钥WEP密钥的关键字段编号。

第7步：如果要显示密码字符，请检查**撕下假面具密码**复选框。

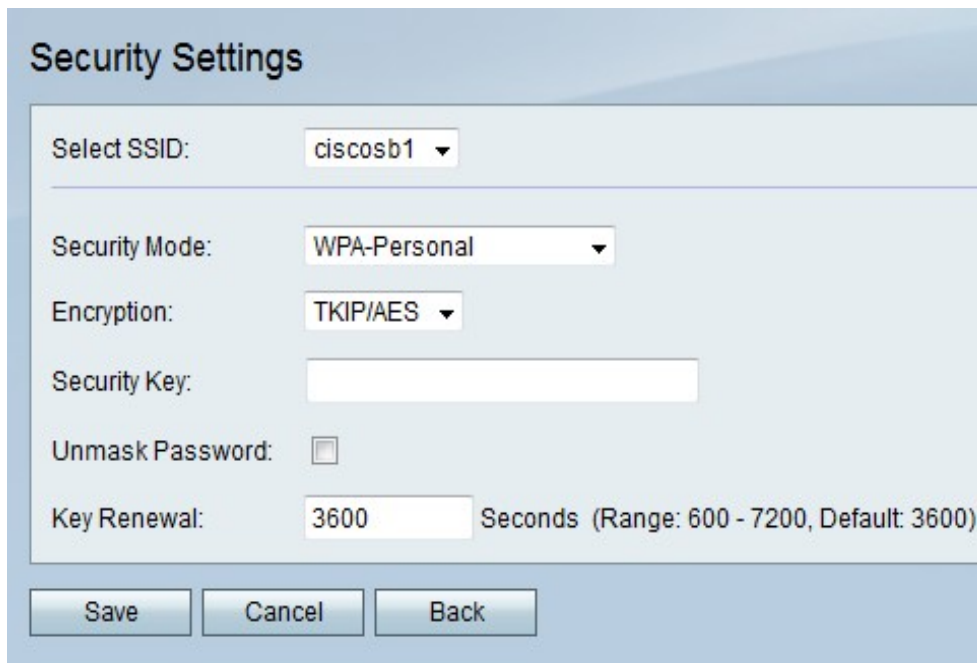
步骤8.点击**“Save”**保存更改，**取消**丢弃他们，或者**回到**回归到上一页。

WPA私有，WPA2-Personal和WPA2-Personal混合安全模式

Wi-Fi保护访问(WPA)是比WEP严格的安全模式。WPA私有能为加密使用临时密钥完整性协议(TKIP)或高级加密标准(AES)。WPA2-Personal使用仅AES加密和一个预共用的键(PSK)认证的。被混合的WPA2-Personal能支持WPA和WPA2客户端并且使用AES和PSK。此程序显示如何设置WPA私有，作为SSID的安全模式被混合的WPA2-Personal或者WPA2-Personal。

第1步：从安全模式下拉菜单，请选择选项。

- WPA私有—此选项支持AES和TKIP。
- WPA2-Personal —此选项支持AES和PSK。
- 被混合的WPA2-Personal —此选项支持WPA和WPA2客户端。



Step 2.如果选择WPA私有，从加密下拉菜单请选择加密类型。

- TKIP/AES —此选项是与不支持AES的更旧的设备兼容。
- AES —此选项比TKIP/AES安全。

第3步：在安全密钥关键字域，请输入限制对网络的访问字母和编号的说明。

第4步：如果要显示密码字符，请检查**撕下假面具密码**复选框。

第5步：在关键续订字段，请输入以秒钟网络多频繁更新键。

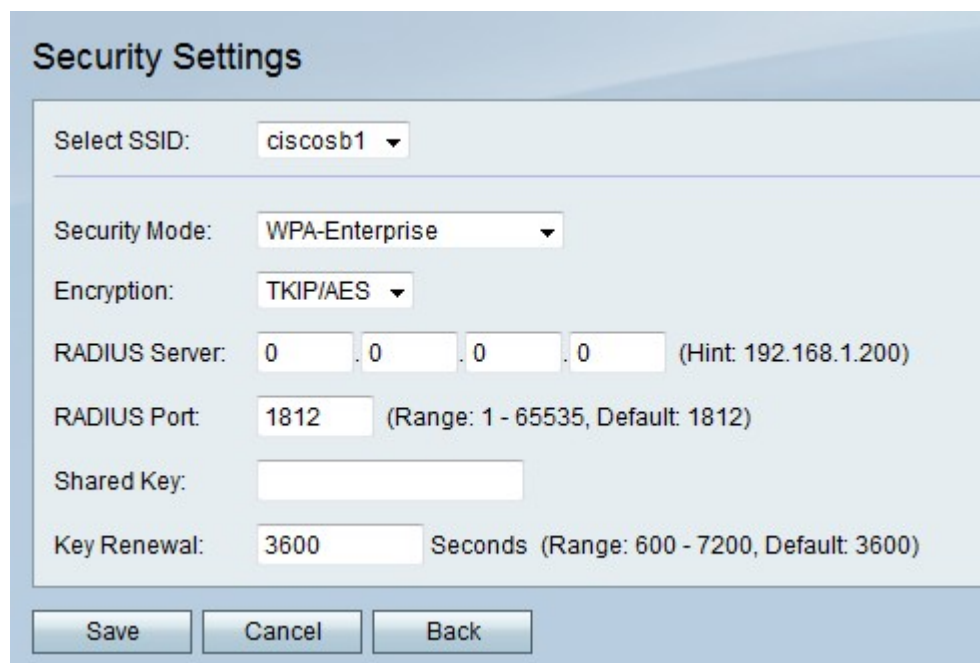
步骤6.点击**“Save”**保存更改，**取消**丢弃他们，或者**回到**回归到上一页。

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

企业安全模式使用远程认证拨入用户服务(RADIUS)服务器验证。RADIUS是使用一个独立服务器的网络协议，并且到/从网络的数据流必须穿过RADIUS服务器。此程序显示如何设置WPA企业、作为SSID的安全模式被混合的WPA2-Enterprise或者WPA2-Enterprise。

第 1 步：从安全模式下拉菜单，请选择选项。

- WPA企业—此选项使用RADIUS、AES和TKIP。
- WPA2-Enterprise —此选项使用RADIUS、AES和PSK。
- WPA2-Enterprise混合了—此选项使用RADIUS并且支持WPA和WPA2客户端。



Step 2.如果选择WPA企业，从加密下拉菜单请选择加密类型。

- TKIP/AES —此选项是与不支持AES的更旧的设备兼容。
- AES —此选项比TKIP/AES安全。

第 3 步：在RADIUS服务器领域，请输入RADIUS服务器的IP地址。

第 4 步：在RADIUS端口字段，请输入网络访问RADIUS服务器的端口号。

第 5 步：在共享密钥关键字域，请输入限制对网络的访问字母和编号的说明。

第6步。在关键续订字段，请输入以秒钟网络多频繁更新键。

步骤7.点击“**Save**”保存更改，**取消**丢弃他们，或者**回到**回归到上一页。