SSID Security Settings on the RV110W

Objective

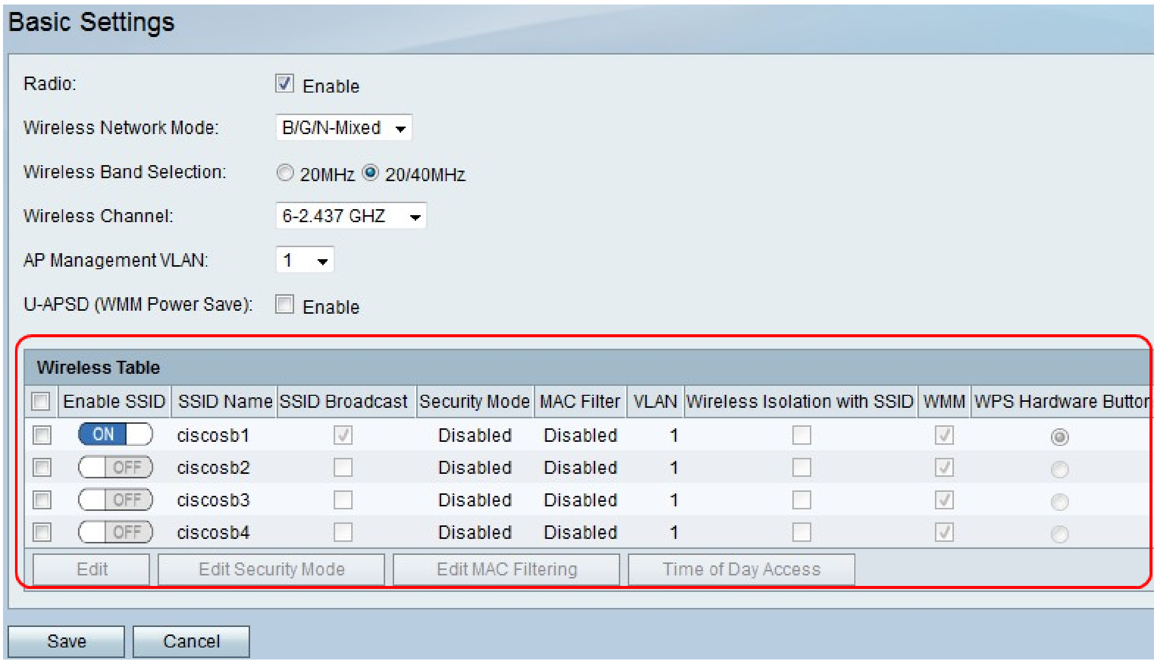
Security Modes offer protection for a wireless network. Different Service Set IDs (SSIDs) can have different security modes. SSIDs may perform different functions for the network; therefore, SSIDs may require different security measures. This article explains how to configure the security settings for an SSID on the RV110W.

Applicable Devices

- RV110W

Steps of Procedure

Step 1. Use the web configuration utility to choose **Wireless > Basic Settings**.



Basic Settings

Radio: ☑ Enable

Wireless Network Mode: B/G/N-Mixed

Wireless Band Selection: ○ 20MHz ● 20/40MHz

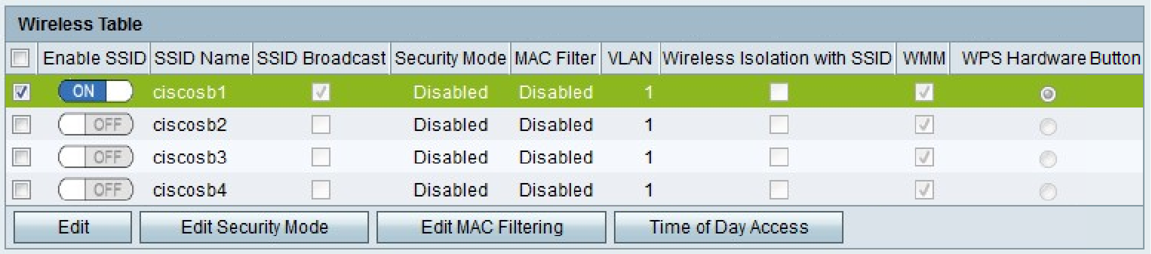
Wireless Channel: 6-2.437 GHZ

AP Management VLAN: 1

U-APSD (WMM Power Save): ☐ Enable

Wireless Table

☐	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	VLAN	Wireless Isolation with SSID	WMM	WPS Hardware Buttor
☐	ON	ciscosb1	☑	Disabled	Disabled	1	☐	☑	●
☐	OFF	ciscosb2	☐	Disabled	Disabled	1	☐	☑	○
☐	OFF	ciscosb3	☐	Disabled	Disabled	1	☐	☑	○
☐	OFF	ciscosb4	☐	Disabled	Disabled	1	☐	☑	○

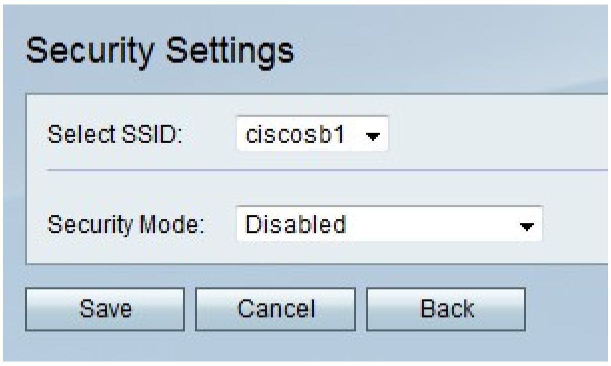


Wireless Table

☐	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	VLAN	Wireless Isolation with SSID	WMM	WPS Hardware Button
☑	ON	ciscosb1	☑	Disabled	Disabled	1	☐	☑	●
☐	OFF	ciscosb2	☐	Disabled	Disabled	1	☐	☑	○
☐	OFF	ciscosb3	☐	Disabled	Disabled	1	☐	☑	○
☐	OFF	ciscosb4	☐	Disabled	Disabled	1	☐	☑	○

Step 2. In the Wireless Table, check the checkbox of an SSID for which you want to edit the security settings.

Step 3. Click **Edit Security Mode**. This opens the *Security Settings* page.



Security Settings

Select SSID: ciscosb1

Security Mode: Disabled

Step 4. From the Select SSID drop-down menu, choose an SSID for which you want to edit security settings.

Disable Security Mode

This procedure shows how to disable the security mode of an SSID which will require no security information to use the SSID.

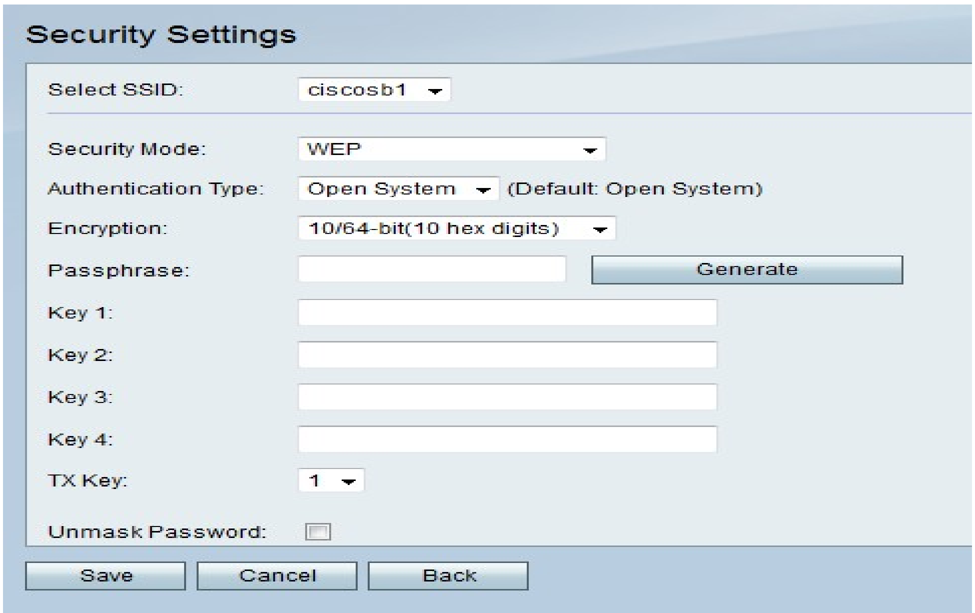
Step 1. From the Security Mode drop-down menu, choose **Disabled**.

Step 2. Click **Save** to save changes, **Cancel** to discard them, or **Back** to return to the previous page.

WEP Security Mode

This procedure shows how to set Wired Equivalent Privacy (WEP) as the security mode of an SSID. WEP is not the most secure security mode, but it may be the only option if some network devices do not support WPA.

Step 1. From the Security Mode drop-down menu, choose **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: □

Step 2. From the Authentication Type drop-down menu, choose an option.

- Open System — This option is more direct and more secure than Shared Key Authentication.
- Shared Key — This option is less secure than Open System.

Step 3. From the Encryption drop-down menu, choose 10/64-bit(10 hex digits), which uses a

40-bit key, or 26/128-bit(26 hex digits), which uses a 104-bit key.

Step 4. In the Passphrase field, enter a passphrase with letters and numbers that is at least 8 characters long.

Step 5. Click **Generate** to create four WEP keys in the Key fields, or manually enter the WEP keys in the Key fields.

Step 6. From the TX Key drop-down menu, choose the Key field number of the WEP key that you want to use as the shared key.

Step 7. Check the **Unmask Password** checkbox if you want to reveal password characters.

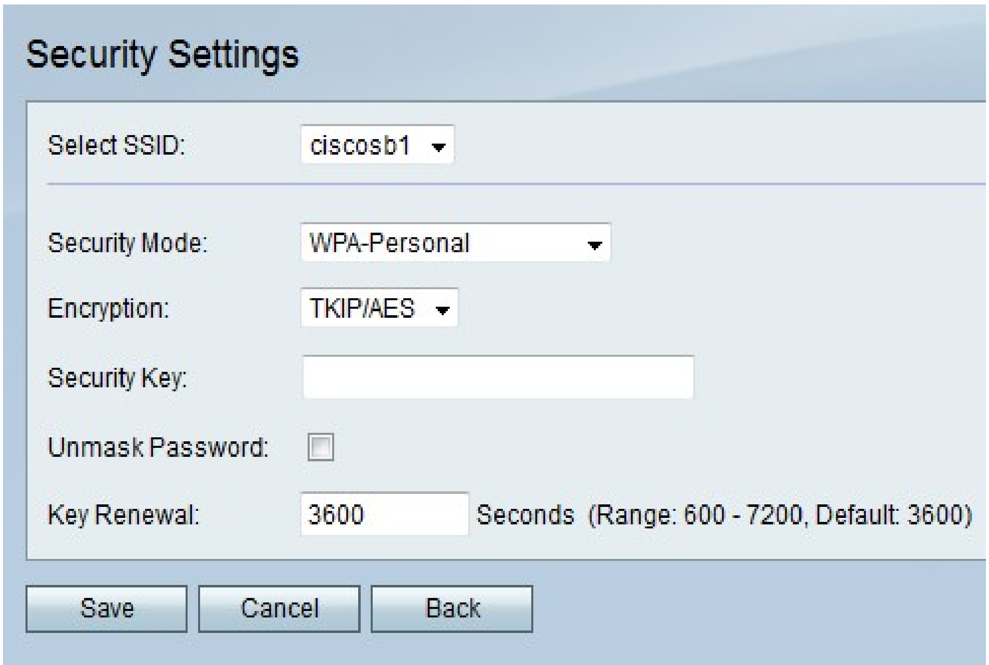
Step 8. Click **Save** to save changes, **Cancel** to discard them, or **Back** to return to the previous page.

WPA-Personal, WPA2-Personal, and WPA2-Personal Mixed Security Mode

Wi-Fi Protected Access (WPA) is a security mode that is stronger than WEP. WPA-Personal can utilize either Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES) for encryption. WPA2-Personal uses only AES for encryption and a Preshared Key (PSK) for authentication. WPA2-Personal Mixed is able to support both WPA and WPA2 clients and uses AES and PSK. This procedure shows how to set up WPA-Personal, WPA2-Personal, or WPA2-Personal Mixed as the security mode for an SSID.

Step 1. From the Security Mode drop-down menu, choose an option.

- WPA-Personal — This option supports AES and TKIP.
- WPA2-Personal — This options supports AES and PSK.
- WPA2-Personal Mixed — This option supports both WPA and WPA2 clients.



Security Settings

Select SSID: ciscosb1

Security Mode: WPA-Personal

Encryption: TKIP/AES

Security Key:

Unmask Password: □

Key Renewal: 3600 Seconds (Range: 600 - 7200, Default: 3600)

Step 2. If you choose WPA-Personal, choose an encryption type from the Encryption drop-down menu.

- TKIP/AES — This option is compatible with older devices that do not support AES.

- AES — This option is more secure than TKIP/AES.

Step 3. In the Security Key field, enter a phrase of letters and numbers that restricts access to the network.

Step 4. Check the **Unmask Password** checkbox if you want to reveal password characters.

Step 5. In the Key Renewal field, enter how often in seconds the network renews the key.

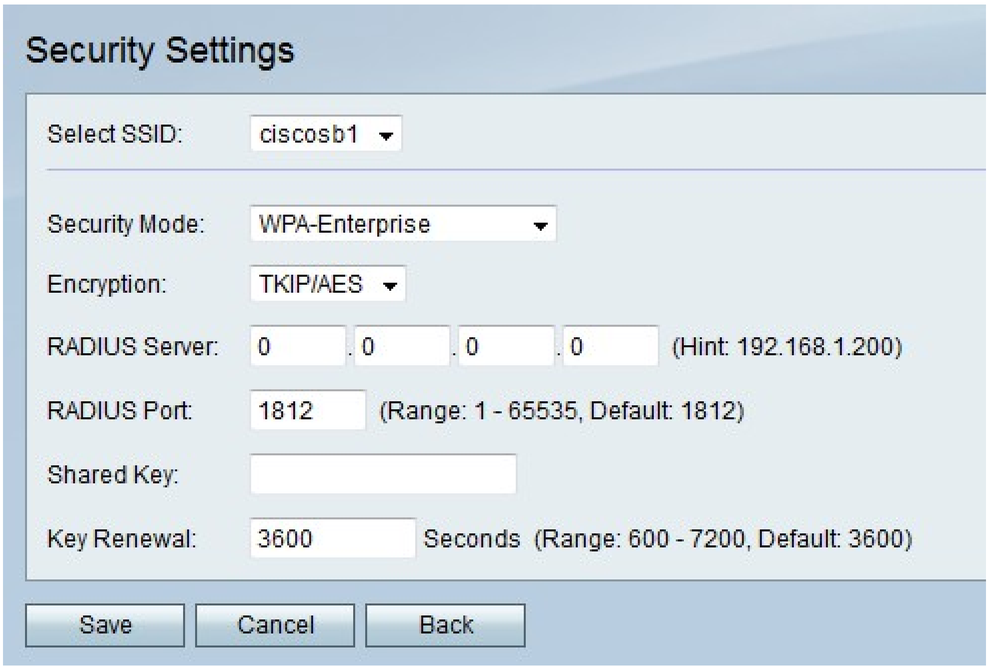
Step 6. Click **Save** to save changes, **Cancel** to discard them, or **Back** to return to the previous page.

WPA-Enterprise, WPA2-Enterprise, and WPA2-Enterprise Mixed Security Mode

The Enterprise Security Modes use Remote Authentication Dial In User Service (RADIUS) server authentication. RADIUS is a network protocol which utilizes a separate server, and traffic to and from the network must pass through the RADIUS server. This procedure shows how to set up WPA-Enterprise, WPA2-Enterprise, or WPA2-Enterprise Mixed as the security mode for an SSID.

Step 1. From the Security Mode drop-down menu, choose an option.

- WPA-Enterprise — This option uses RADIUS, AES, and TKIP.
- WPA2-Enterprise — This option uses RADIUS, AES, and PSK.
- WPA2-Enterprise Mixed — This option uses RADIUS and supports both WPA and WPA2 clients.



Security Settings

Select SSID: ciscosb1

Security Mode: WPA-Enterprise

Encryption: TKIP/AES

RADIUS Server: 0 . 0 . 0 . 0 (Hint: 192.168.1.200)

RADIUS Port: 1812 (Range: 1 - 65535, Default: 1812)

Shared Key:

Key Renewal: 3600 Seconds (Range: 600 - 7200, Default: 3600)

Step 2. If you choose WPA-Enterprise, choose an encryption type from the Encryption drop-down menu.

- TKIP/AES — This option is compatible with older devices that do not support AES.
- AES — This option is more secure than TKIP/AES.

Step 3. In the RADIUS Server field, enter the IP address of the RADIUS server.

Step 4. In the RADIUS Port field, enter the port number on which the network accesses the RADIUS server.

Step 5. In the Shared Key field, enter a phrase of letters and numbers that restricts access to the network.

Step 6. In the Key Renewal field, enter how often in seconds the network renews the key.

Step 7. Click **Save** to save changes, **Cancel** to discard them, or **Back** to return to the previous page.