

Configuración de seguridad SSID en el RV110W

Objetivo

Los modos de seguridad ofrecen protección para una red inalámbrica. Los diferentes ID de conjunto de servicios (SSID) pueden tener modos de seguridad diferentes. Los SSID pueden realizar diferentes funciones para la red; por lo tanto, los SSID pueden requerir diferentes medidas de seguridad. En este artículo se explica cómo configurar los parámetros de seguridad para un SSID en el RV110W.

Dispositivos aplicables

- RV110W

Pasos del procedimiento

Paso 1. Utilice la utilidad de configuración web para elegir **Wireless > Basic Settings**.

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

<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"/>	<input checked="" type="checkbox"/>	ciscosb1	<input checked="" type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/>	<input type="checkbox"/>	ciscosb2	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/>	<input type="checkbox"/>	ciscosb3	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/>	<input type="checkbox"/>	ciscosb4	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>

Paso 2. En la tabla inalámbrica, active la casilla de verificación de un SSID para el que desea editar los parámetros de seguridad.

Paso 3. Haga clic en **Editar modo de seguridad**. Se abre la página *Configuración de seguridad*.

Security Settings

Select SSID:

Security Mode:

Paso 4. En el menú desplegable Seleccionar SSID, elija un SSID para el que desee editar los parámetros de seguridad.

Desactivar modo de seguridad

Este procedimiento muestra cómo inhabilitar el modo de seguridad de un SSID que no requerirá información de seguridad para utilizar el SSID.

Paso 1. En el menú desplegable Modo de seguridad, elija **Desactivado**.

Paso 2. Haga clic en **Guardar** para guardar los cambios, **Cancelar** para descartarlos o **Atrás** para volver a la página anterior.

Modo de seguridad WEP

Este procedimiento muestra cómo establecer la privacidad equivalente a conexión con cables (WEP) como el modo de seguridad de un SSID. WEP no es el modo de seguridad más seguro, pero puede ser la única opción si algunos dispositivos de red no admiten WPA.

Paso 1. En el menú desplegable Security Mode (Modo de seguridad), elija **WEP**.

Security Settings

Select SSID:

Security Mode:

Authentication Type: (Default: Open System)

Encryption:

Passphrase:

Key 1:

Key 2:

Key 3:

Key 4:

TX Key:

Unmask Password:

Paso 2. En el menú desplegable Authentication Type (Tipo de autenticación), elija una opción.

- Sistema abierto: esta opción es más directa y segura que la autenticación de clave compartida.
- Shared Key (Clave compartida): esta opción es menos segura que Open System (Sistema abierto).

Paso 3. En el menú desplegable Encryption (Encriptación), elija 10/64-bit (10 dígitos hexadecimales), que utiliza una clave de 40 bits, o 26/128 bits (26 dígitos hexadecimales), que utiliza una clave de 104 bits.

Paso 4. En el campo Passphrase (Frase de paso), introduzca una frase de paso con letras y números de al menos 8 caracteres.

Paso 5. Haga clic en **Generar** para crear cuatro claves WEP en los campos Clave o introduzca manualmente las claves WEP en los campos Clave.

Paso 6. En el menú desplegable TX Key (Clave de transmisión), elija el número de campo Key (Clave) de la clave WEP que desea utilizar como clave compartida.

Paso 7. Marque la casilla de verificación **Desenmascarar contraseña** si desea mostrar los caracteres de contraseña.

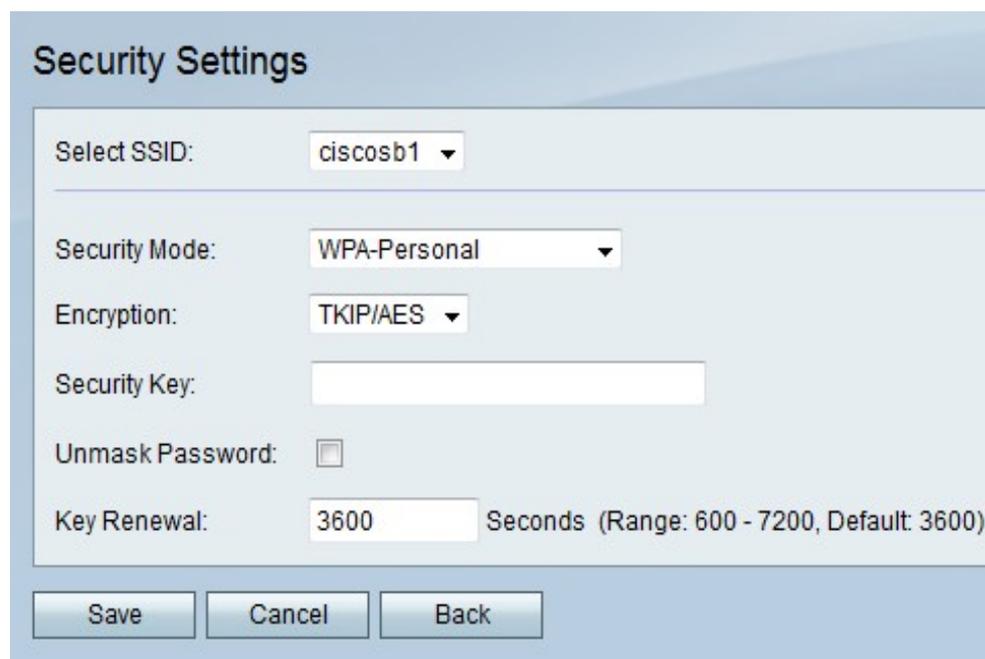
Paso 8. Haga clic en **Guardar** para guardar los cambios, **Cancelar** para descartarlos o **Atrás** para volver a la página anterior.

Modo de seguridad mixta WPA-Personal, WPA2-Personal y WPA2-Personal

El acceso Wi-Fi protegido (WPA) es un modo de seguridad más fiable que WEP. WPA-Personal puede utilizar el protocolo de integridad de clave temporal (TKIP) o el estándar de cifrado avanzado (AES) para el cifrado. WPA2-Personal utiliza solo AES para el cifrado y una clave precompartida (PSK) para la autenticación. WPA2-Personal Mixed es compatible con clientes WPA y WPA2 y utiliza AES y PSK. Este procedimiento muestra cómo configurar WPA-Personal, WPA2-Personal o WPA2-Personal Mixed como modo de seguridad para un SSID.

Paso 1. En el menú desplegable Security Mode (Modo de seguridad), elija una opción.

- WPA-Personal: esta opción admite AES y TKIP.
- WPA2-Personal: esta opción admite AES y PSK.
- WPA2-Personal Mixed: esta opción admite clientes WPA y WPA2.



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)

Save Cancel Back

Paso 2. Si selecciona WPA-Personal, elija un tipo de encriptación en el menú desplegable

Encryption (Encriptación).

- TKIP/AES: esta opción es compatible con dispositivos antiguos que no admiten AES.
- AES: esta opción es más segura que TKIP/AES.

Paso 3. En el campo Clave de seguridad, introduzca una frase de letras y números que restrinja el acceso a la red.

Paso 4. Marque la casilla de verificación **Desenmascarar contraseña** si desea mostrar los caracteres de contraseña.

Paso 5. En el campo Key Renewal (Renovación de claves), introduzca la frecuencia en segundos con la que la red renueva la clave.

Paso 6. Haga clic en **Guardar** para guardar los cambios, **Cancelar** para descartarlos o **Atrás** para volver a la página anterior.

Modo de seguridad mixta WPA-Enterprise, WPA2-Enterprise y WPA2-Enterprise

Los Modos de Seguridad Empresarial utilizan la autenticación de servidor RADIUS (Servicio de usuario de acceso telefónico de autenticación remota). RADIUS es un protocolo de red que utiliza un servidor separado, y el tráfico hacia y desde la red debe pasar a través del servidor RADIUS. Este procedimiento muestra cómo configurar WPA-Enterprise, WPA2-Enterprise o WPA2-Enterprise Mixed como modo de seguridad para un SSID.

Paso 1. En el menú desplegable Security Mode (Modo de seguridad), elija una opción.

- WPA-Enterprise: esta opción utiliza RADIUS, AES y TKIP.
- WPA2-Enterprise: esta opción utiliza RADIUS, AES y PSK.
- WPA2-Enterprise Mixed: esta opción utiliza RADIUS y admite clientes WPA y WPA2.

The screenshot shows the 'Security Settings' configuration interface. The 'Select SSID' dropdown is set to 'ciscosb1'. The 'Security Mode' dropdown is set to 'WPA-Enterprise'. The 'Encryption' dropdown is set to 'TKIP/AES'. The 'RADIUS Server' field consists of four input boxes, each containing '0', with a hint '(Hint: 192.168.1.200)'. The 'RADIUS Port' field has an input box with '1812' and a range '(Range: 1 - 65535, Default: 1812)'. The 'Shared Key' field is an empty input box. The 'Key Renewal' field has an input box with '3600' and the text 'Seconds (Range: 600 - 7200, Default: 3600)'. At the bottom, there are three buttons: 'Save', 'Cancel', and 'Back'.

Paso 2. Si elige WPA-Enterprise, elija un tipo de encriptación en el menú desplegable Encryption (Encriptación).

- TKIP/AES: esta opción es compatible con dispositivos antiguos que no admiten AES.
- AES: esta opción es más segura que TKIP/AES.

Paso 3. En el campo Servidor RADIUS, introduzca la dirección IP del servidor RADIUS.

Paso 4. En el campo RADIUS Port (Puerto RADIUS), introduzca el número de puerto en el que la red accede al servidor RADIUS.

Paso 5. En el campo Shared Key (Clave compartida), introduzca una frase de letras y números que restrinja el acceso a la red.

Paso 6. En el campo Key Renewal (Renovación de claves), introduzca la frecuencia en segundos con la que la red renueva la clave.

Paso 7. Haga clic en **Guardar** para guardar los cambios, **Cancelar** para descartarlos o **Atrás** para volver a la página anterior.