Ajustes de seguridad SSID en el RV110W

Objetivo

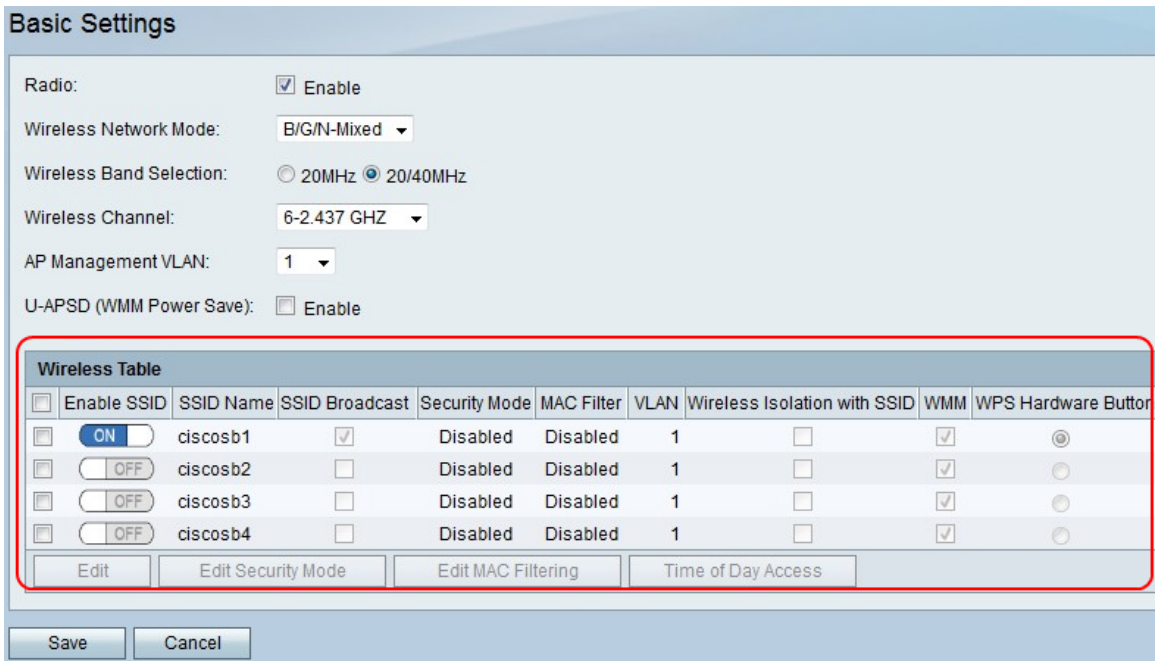
Protección de la oferta de los modos seguros para una red inalámbrica. Diverso conjunto de servicio ID (SSID) puede tener diversos modos seguros. Los SSID pueden realizar diversas funciones para la red; por lo tanto, los SSID pueden requerir diversas medidas de seguridad. Este artículo explica cómo configurar los ajustes de seguridad para un SSID en el RV110W.

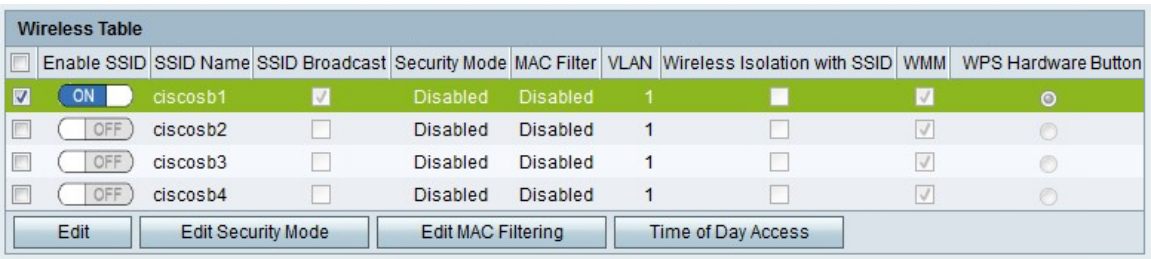
Dispositivos aplicables

- RV110W

Pasos del procedimiento

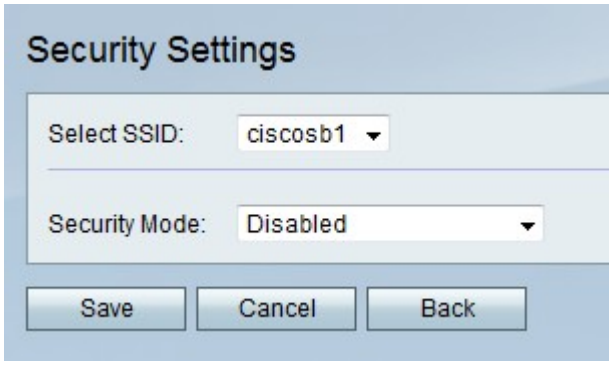
Paso 1. Utilice la utilidad de configuración de la red para elegir la **Tecnología inalámbrica > las configuraciones básicas**.





Paso 2. En la tabla inalámbrica, marque el checkbox de un SSID para el cual usted quiera editar los ajustes de seguridad.

Paso 3. El tecleo **edita al modo seguro**. Esto abre la página de los *ajustes de seguridad*.



Paso 4. Del menú desplegable selecto SSID, elija un SSID para el cual usted quiera editar los ajustes de seguridad.

Inhabilite al modo seguro

Este procedimiento muestra cómo inhabilitar al modo seguro de un SSID cuál no requerirá ninguna información sobre seguridad utilizar el SSID.

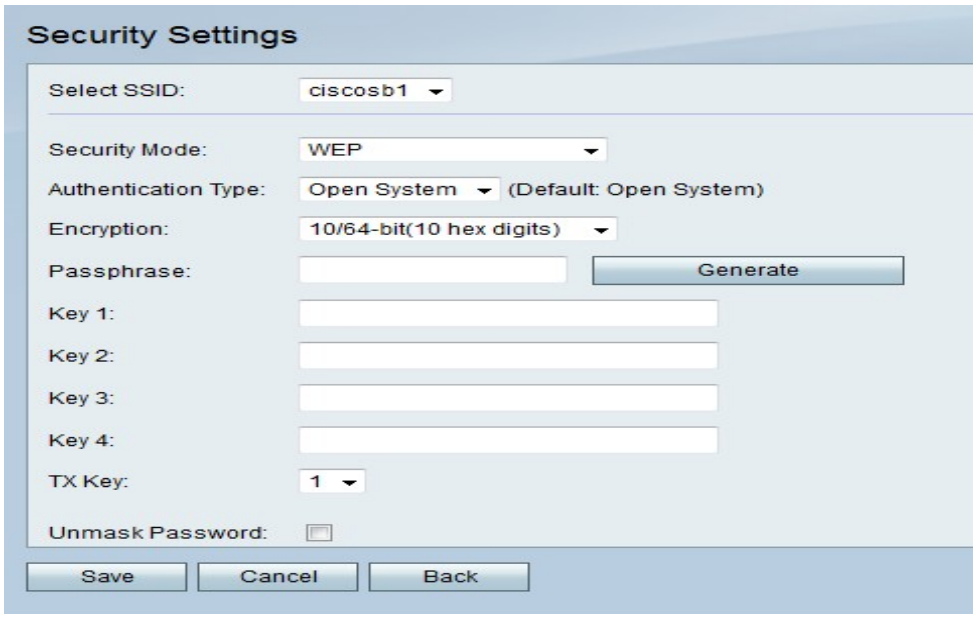
Paso 1. Del menú desplegable del modo seguro, elija **discapacitado**.

Paso 2. **Salvaguardia del** tecleo para salvar los cambios, **cancelación** para desecharlos, o **de nuevo a la** vuelta a la página previa.

Modo seguro WEP

Este procedimiento muestra cómo fijar el Wired Equivalent Privacy (WEP) como el modo seguro de un SSID. El WEP no es el modo seguro más seguro, sino que puede ser la única opción si algunos dispositivos de red no soportan el WPA.

Paso 1. Del menú desplegable del modo seguro, elija el **WEP**.



Paso 2. Del menú desplegable del tipo de autenticación, elija una opción.

- Sistema operativo — Esta opción es más directo y más seguro que la clave de autenticación compartida.
- Clave compartida — Esta opción es menos segura que el sistema operativo.

Paso 3. Del menú desplegable del cifrado, elija los dígitos hexadecimales 10/64-bit(10), que utiliza una clave 40-bit, o los dígitos hexadecimales 26/128-bit(26), que utiliza una clave del 104-bit.

Paso 4. En el campo del passphrase, ingrese un passphrase con las cartas y los números que es por lo menos 8 caracteres de largo.

Paso 5. Haga clic **generan** para crear cuatro claves WEP en los campos claves, o ingresan manualmente las claves WEP en los campos claves.

Paso 6. Del menú desplegable de la clave TX, elija el número de campo clave de la clave WEP que usted quiere utilizar como la clave compartida.

Paso 7. Marque la **casilla de verificación Password (Contraseña) del desenmascarar** si usted quiere revelar los caracteres de la contraseña.

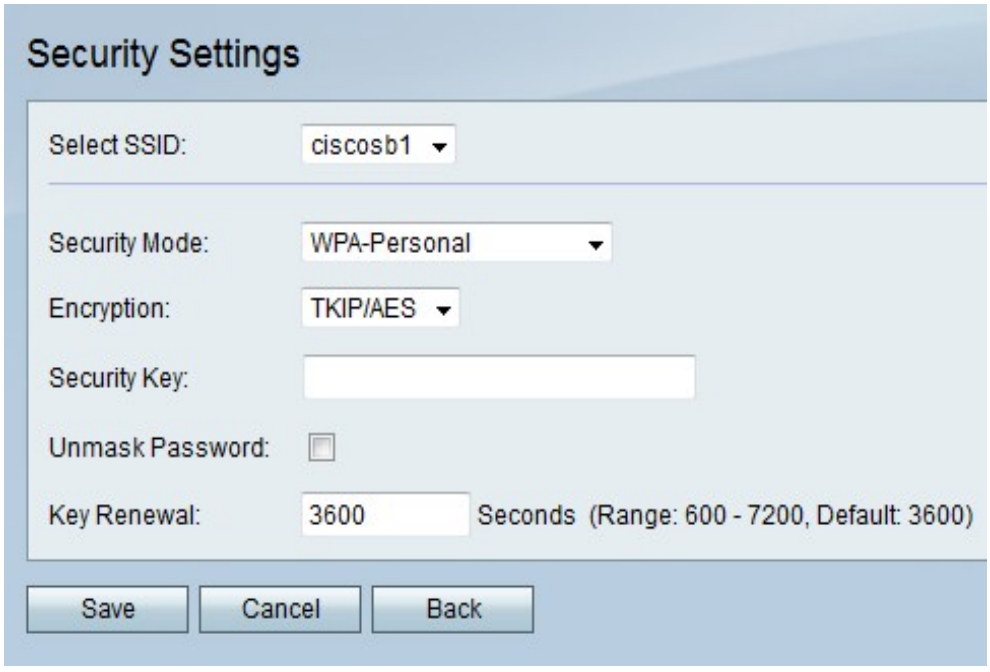
Paso 8. **Salvaguardia del** tecleo para salvar los cambios, **cancelación** para desecharlos, o **de nuevo a la** vuelta a la página previa.

WPA-personal, WPA2-Personal, y modo seguro mezclado WPA2-Personal

El Acceso protegido de Wi-Fi (WPA) es un modo seguro que es más fuerte que el WEP. WPA-personal puede utilizar el Temporal Key Integrity Protocol (TKIP) o el Advanced Encryption Standard (AES) para el cifrado. WPA2-Personal utiliza solamente el AES para el cifrado y una clave del preshared (PSK) para la autenticación. WPA2-Personal mezclado puede soportar los clientes WPA y WPA2 y utiliza el AES y el PSK. Este procedimiento muestra cómo configurar WPA-personal, WPA2-Personal, o WPA2-Personal mezclado como el modo seguro para un SSID.

Paso 1. Del menú desplegable del modo seguro, elija una opción.

- WPA-personal — Esta opción soporta el AES y el TKIP.
- WPA2-Personal — Este las opciones soportan el AES y el PSK.
- WPA2-Personal se mezcló — Esta opción soporta los clientes WPA y WPA2.



Paso 2. Si usted elige WPA-personal, elija un tipo de encripción del menú desplegable del

cifrado.

- TKIP/AES — Esta opción es compatible con más viejos dispositivos que no soporten el AES.
- AES — Esta opción es más segura que TKIP/AES.

Paso 3. En el campo de clave de seguridad, ingrese una frase de las cartas y de los números que restrinja el acceso a la red.

Paso 4. Marque la **casilla de verificación Password (Contraseña) del desenmascarar** si usted quiere revelar los caracteres de la contraseña.

Paso 5. En el campo dominante de la renovación, ingrese cuantas veces en los segundos la red renueva la clave.

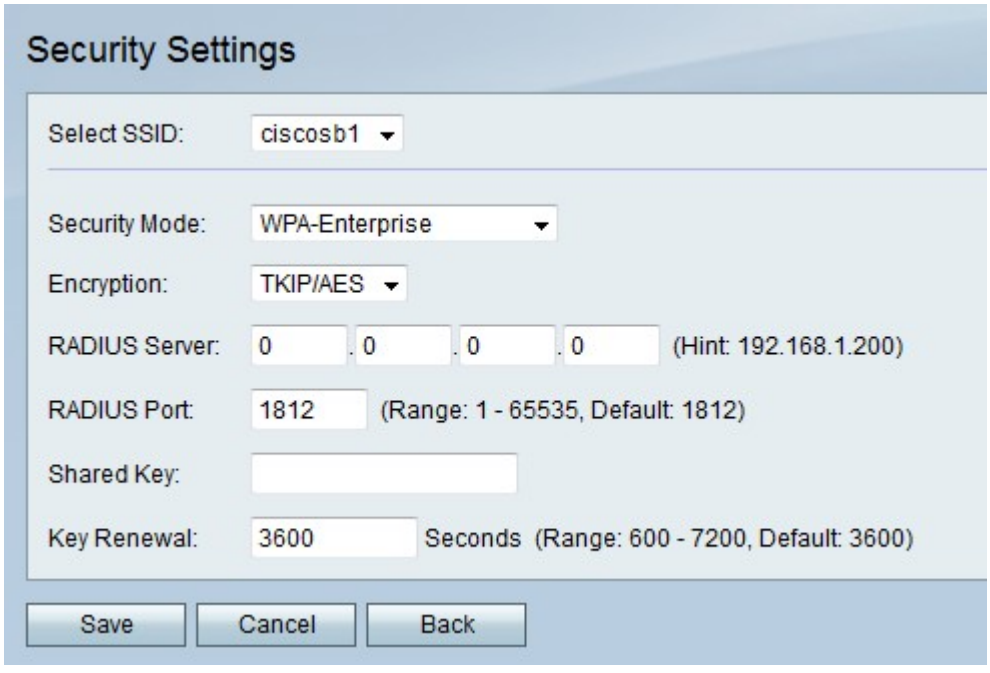
Paso 6. **Salvaguardia del** tecleo para salvar los cambios, **cancelación** para desecharlos, o **de nuevo a la** vuelta a la página previa.

WPA-empresa, WPA2-Enterprise, y modo seguro mezclado WPA2-Enterprise

La autenticación de servidor del Remote Authentication Dial In User Service del uso de los modos seguros de la empresa (RADIUS). El RADIUS es un Network Protocol que utiliza a un servidor separado, y el tráfico a y desde la red debe pasar a través del servidor de RADIUS. Este procedimiento muestra cómo configurar la WPA-empresa, WPA2-Enterprise, o WPA2-Enterprise mezclado como el modo seguro para un SSID.

Paso 1. Del menú desplegable del modo seguro, elija una opción.

- WPA-empresa — Esta opción utiliza el RADIUS, el AES, y el TKIP.
- WPA2-Enterprise — Esta opción utiliza el RADIUS, el AES, y el PSK.
- WPA2-Enterprise se mezcló — Esta opción utiliza el RADIUS y soporta los clientes WPA y WPA2.



Paso 2. Si usted elige la WPA-empresa, elija un tipo de encripción del menú desplegable del cifrado.

- TKIP/AES — Esta opción es compatible con más viejos dispositivos que no soporten el AES.
- AES — Esta opción es más segura que TKIP/AES.

Paso 3. En el campo del servidor de RADIUS, ingrese el IP Address del servidor de RADIUS.

Paso 4. En el campo de puerto RADIUS, ingrese el número del puerto en el cual los accesos a la red el servidor de RADIUS.

Paso 5. En el campo de clave compartida, ingrese una frase de las cartas y de los números que restrinja el acceso a la red.

Paso 6. En el campo dominante de la renovación, ingrese cuantas veces en los segundos la red renueva la clave.

Paso 7. Salvaguardia del tecleo para salvar los cambios, cancelación para desecharlos, o de nuevo a la vuelta a la página previa.