Configurações de segurança do SSID no RV110W

Objetivo

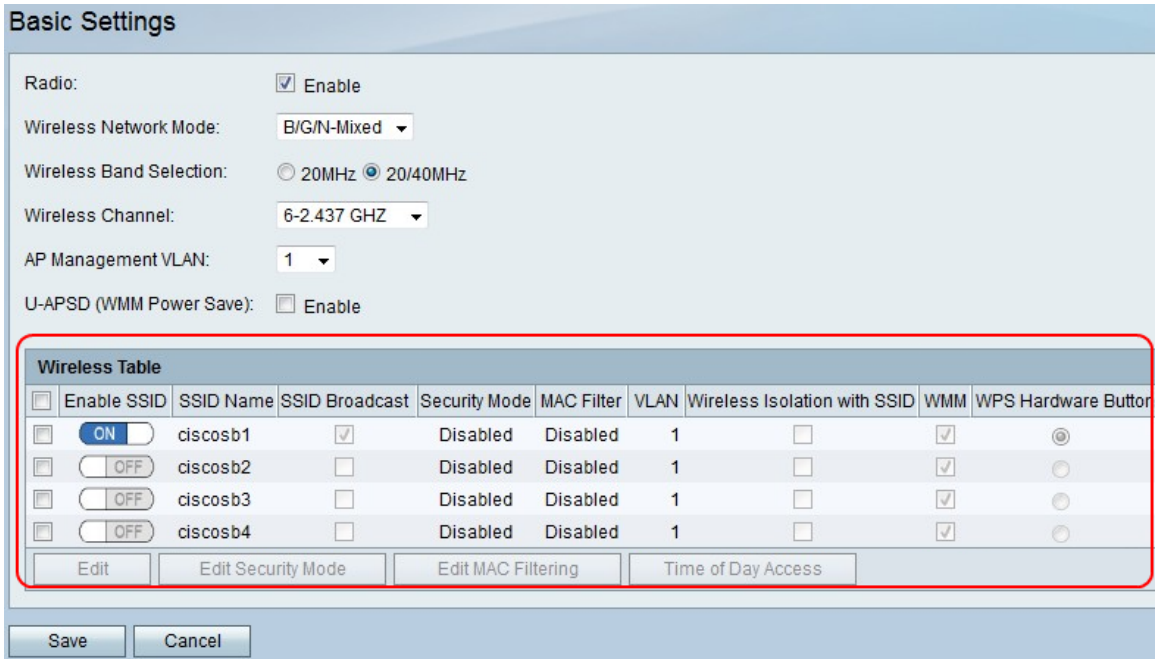
Os modos de segurança oferecem proteção para uma rede sem fio. Diferentes IDs do conjunto de serviços (SSIDs) podem ter diferentes modos de segurança. Os SSID podem desempenhar funções diferentes para a rede; portanto, os SSIDs podem exigir medidas de segurança diferentes. Este artigo explica como definir as configurações de segurança de um SSID no RV110W.

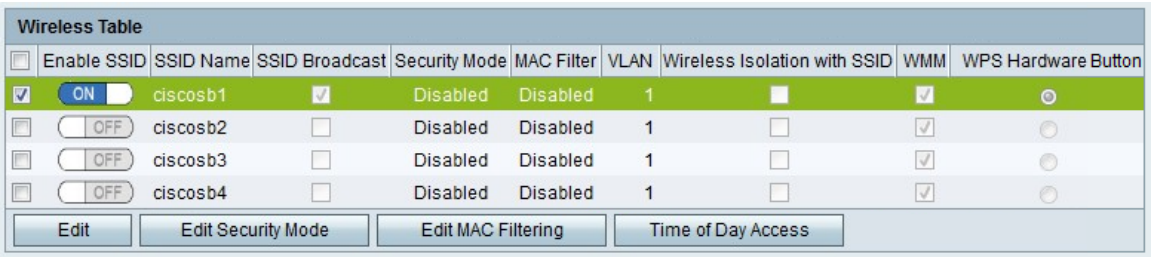
Dispositivos aplicáveis

- RV110W

Etapas do procedimento

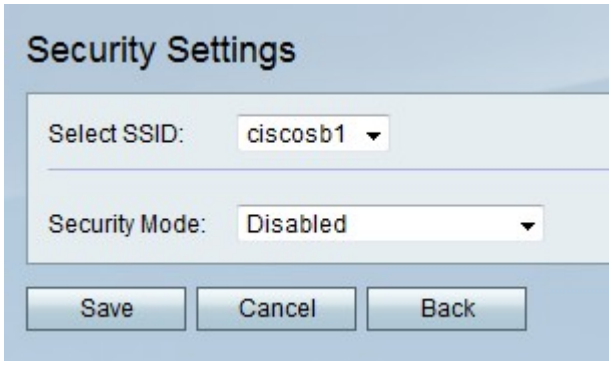
Etapa 1. Use o utilitário de configuração da Web para escolher **Wireless > Basic Settings**.





Etapa 2. Na Tabela de conexões sem fio, marque a caixa de seleção de um SSID para o qual deseja editar as configurações de segurança.

Etapa 3. Clique em **Editar modo de segurança**. Isso abre a página *Configurações de segurança*.



Etapa 4. No menu suspenso Select SSID (Selecionar SSID), escolha um SSID para o qual deseja editar as configurações de segurança.

Desativar Modo de Segurança

Este procedimento mostra como desativar o modo de segurança de um SSID que não exigirá informações de segurança para usar o SSID.

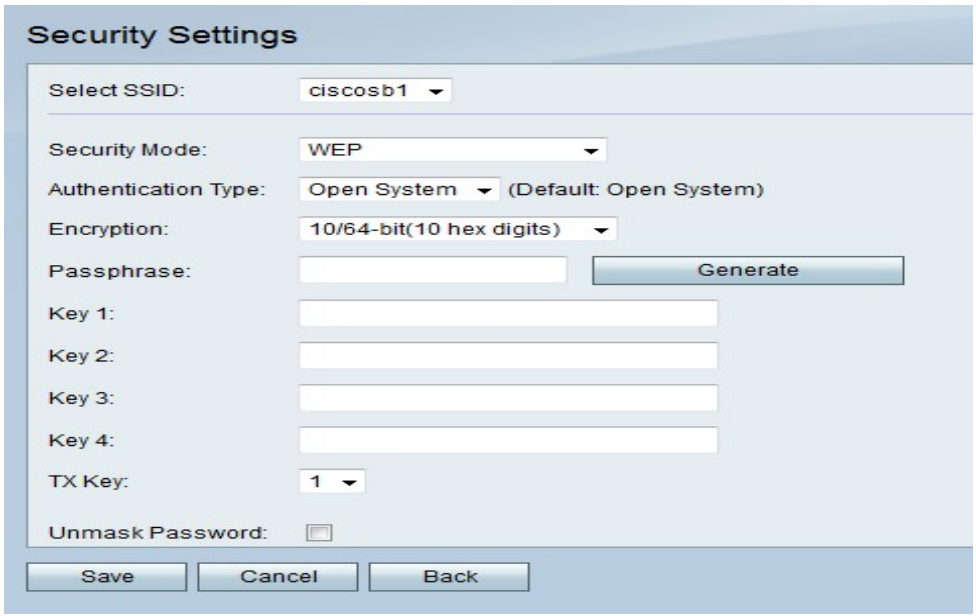
Etapa 1. No menu suspenso Security Mode (Modo de segurança), escolha **Disabled (Desabilitado)**.

Etapa 2. Clique em **Salvar** para salvar as alterações, **Cancelar** para descartá-las ou **Voltar** para retornar à página anterior.

Modo de segurança WEP

Este procedimento mostra como definir WEP (Wired Equivalent Privacy) como o modo de segurança de um SSID. A WEP não é o modo de segurança mais seguro, mas pode ser a única opção se alguns dispositivos de rede não suportam a WPA.

Etapa 1. No menu suspenso Security Mode (Modo de segurança), escolha **WEP**.



Etapa 2. No menu suspenso Authentication Type (Tipo de autenticação), escolha uma opção.

- Open System (Sistema aberto) — Essa opção é mais direta e mais segura que a Shared Key Authentication (Autenticação de chave compartilhada).

- Shared Key (Chave compartilhada) — Essa opção é menos segura que o Open System (Sistema aberto).

Etapa 3. No menu suspenso Encryption (Criptografia), escolha 10/64 bits (10 dígitos hexadecimais), que usa uma chave de 40 bits, ou 26/128 bits (26 dígitos hexadecimais), que usa uma chave de 104 bits.

Etapa 4. No campo Passphrase (Senha), insira uma senha com letras e números de pelo menos 8 caracteres.

Etapa 5. Clique em **Gerar** para criar quatro chaves WEP nos campos Chave ou insira manualmente as chaves WEP nos campos Chave.

Etapa 6. No menu suspenso TX Key (Chave TX), escolha o número do campo Key (Chave) da chave WEP que você deseja usar como a chave compartilhada.

Passo 7. Marque a caixa de seleção **Desmascarar senha** se quiser revelar caracteres de senha.

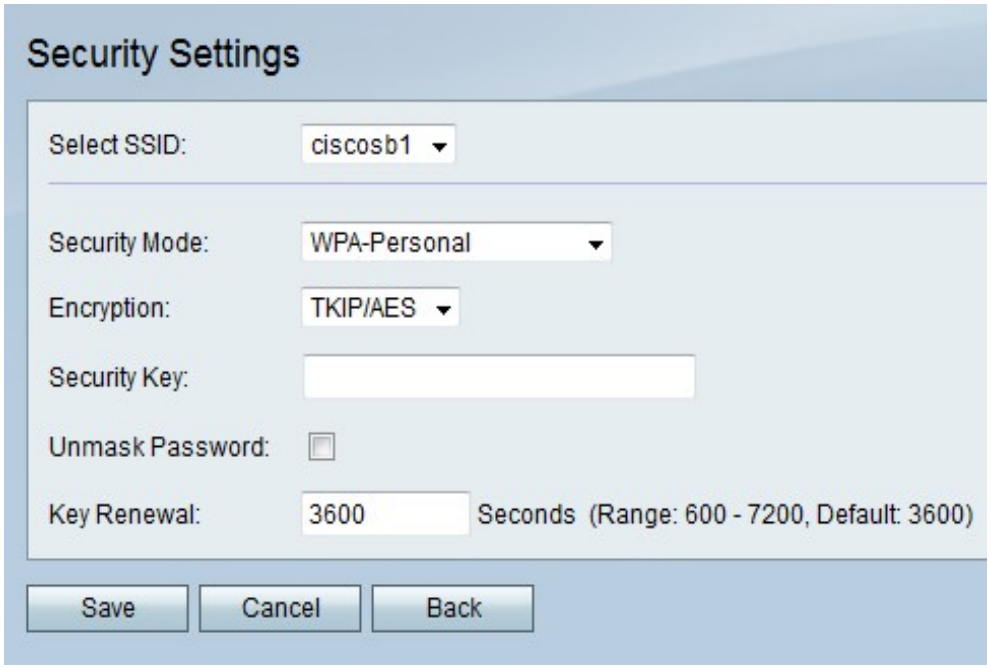
Etapa 8. Clique em **Salvar** para salvar as alterações, **Cancelar** para descartá-las ou **Voltar** para retornar à página anterior.

Modo de segurança mista WPA-Personal, WPA2-Personal e WPA2-Personal

O WPA (Wi-Fi Protected Access) é um modo de segurança mais forte que o WEP. A WPA-Personal pode utilizar o Temporal Key Integrity Protocol (TKIP) ou o Advanced Encryption Standard (AES) para criptografia. A WPA2-Personal usa apenas AES para criptografia e uma chave pré-compartilhada (PSK) para autenticação. A WPA2-Personal Mixed é capaz de suportar clientes WPA e WPA2 e usa AES e PSK. Este procedimento mostra como configurar WPA-Personal, WPA2-Personal ou WPA2-Personal Mixed como o modo de segurança de um SSID.

Etapa 1. No menu suspenso Security Mode (Modo de segurança), escolha uma opção.

- WPA-Personal — Esta opção suporta AES e TKIP.
- WPA2-Personal — Essa opção suporta AES e PSK.
- WPA2-Personal Mixed — Esta opção suporta clientes WPA e WPA2.



Etapa 2. Se você escolher WPA-Personal, escolha um tipo de criptografia no menu suspenso Encryption (Criptografia).

- TKIP/AES — Essa opção é compatível com dispositivos mais antigos que não suportam AES.
- AES — Essa opção é mais segura que TKIP/AES.

Etapa 3. No campo Chave de segurança, insira uma frase de letras e números que restrinja o acesso à rede.

Etapa 4. Marque a caixa de seleção **Desmascarar senha** se quiser revelar caracteres de senha.

Etapa 5. No campo Key Renewal (Renovação de chave), insira a frequência com que a rede renova a chave em segundos.

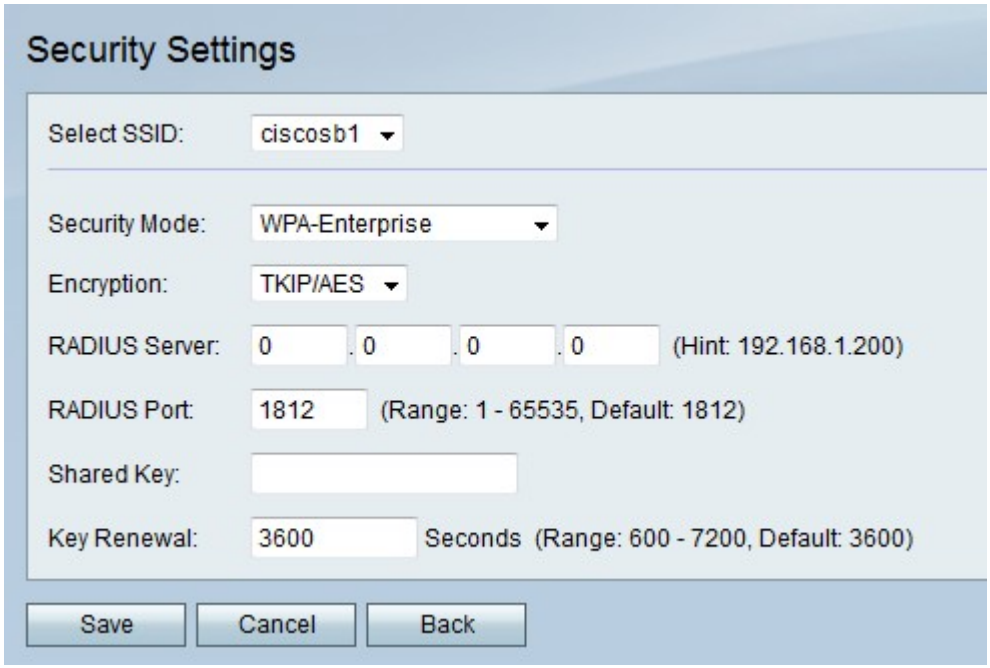
Etapa 6. Clique em **Salvar** para salvar as alterações, **Cancelar** para descartá-las ou **Voltar** para retornar à página anterior.

Modo de segurança mista WPA-Empresa, WPA2-Empresa e WPA2-Empresa

Os Modos de Segurança Empresarial usam autenticação de servidor RADIUS (Remote Authentication Dial In User Service). RADIUS é um protocolo de rede que utiliza um servidor separado e o tráfego de e para a rede deve passar pelo servidor RADIUS. Este procedimento mostra como configurar WPA-Empresa, WPA2-Empresa ou WPA2-Empresa Misto como o modo de segurança para um SSID.

Etapa 1. No menu suspenso Security Mode (Modo de segurança), escolha uma opção.

- WPA-Enterprise — Essa opção usa RADIUS, AES e TKIP.
- WPA2-Enterprise — Essa opção usa RADIUS, AES e PSK.
- WPA2-Enterprise Mixed — Esta opção usa RADIUS e suporta clientes WPA e WPA2.



Etapa 2. Se você escolher WPA-Enterprise, escolha um tipo de criptografia no menu suspenso Encryption (Criptografia).

- TKIP/AES — Essa opção é compatível com dispositivos mais antigos que não suportam AES.
- AES — Essa opção é mais segura que TKIP/AES.

Etapa 3. No campo Servidor RADIUS, insira o endereço IP do servidor RADIUS.

Etapa 4. No campo Porta RADIUS, insira o número da porta na qual a rede acessa o servidor RADIUS.

Etapa 5. No campo Chave compartilhada, insira uma frase de letras e números que restrinja o acesso à rede.

Etapa 6. No campo Key Renewal (Renovação de chave), insira a frequência com que a rede renova a chave em segundos.

Passo 7. Clique em **Salvar** para salvar as alterações, **Cancelar** para descartá-las ou **Voltar** para retornar à página anterior.