Impostazioni di sicurezza SSID su RV110W

Obiettivo

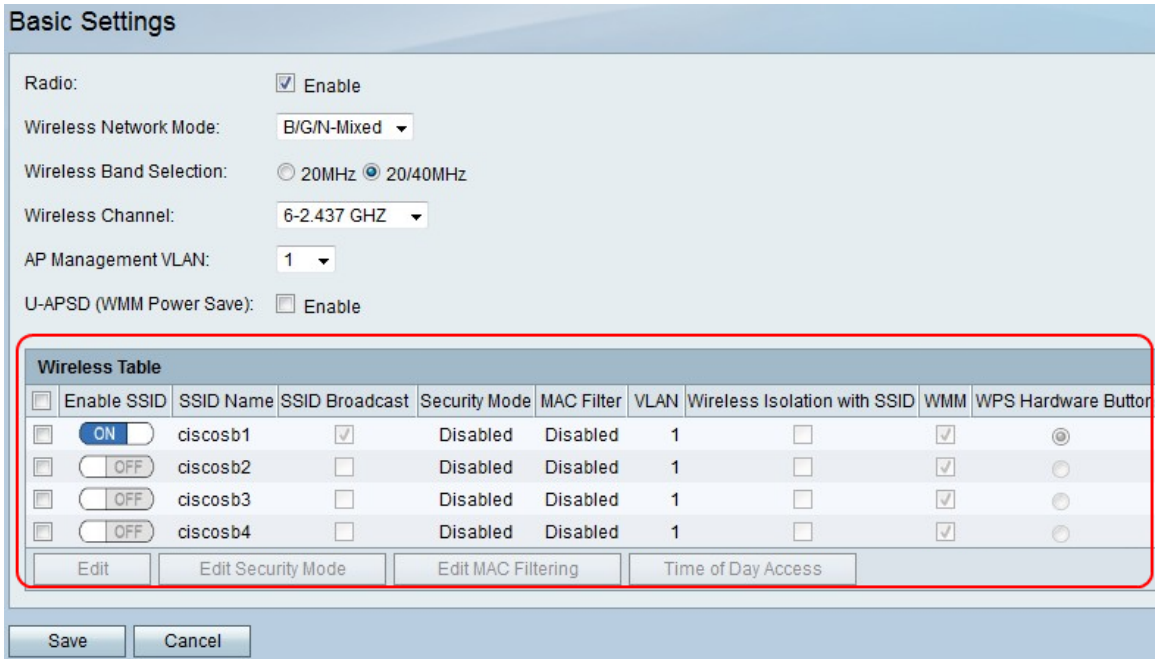
Le modalità di sicurezza offrono protezione per una rete wireless. Diversi SSID (Service Set ID) possono avere modalità di protezione diverse. Gli SSID possono svolgere diverse funzioni per la rete; pertanto, gli SSID possono richiedere misure di sicurezza diverse. Questo articolo spiega come configurare le impostazioni di sicurezza per un SSID sull'RV110W.

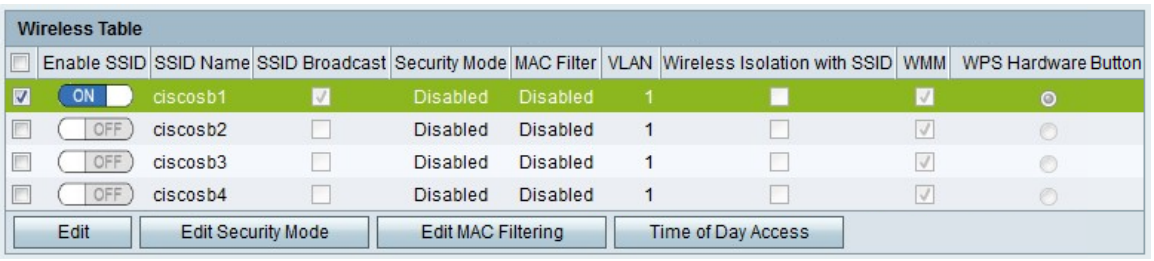
Dispositivi interessati

- RV110W

Fasi della procedura

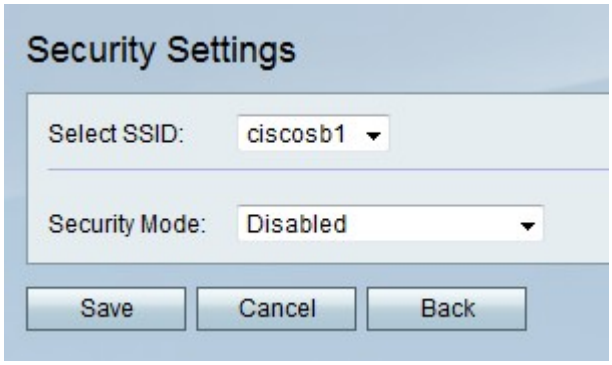
Passaggio 1. Usare l'utility di configurazione Web per scegliere **Wireless > Impostazioni di base**.





Passaggio 2. Nella tabella Wireless, selezionare la casella di controllo di un SSID di cui si desidera modificare le impostazioni di protezione.

Passaggio 3. Fare clic su **Modifica modalità di protezione**. Verrà visualizzata la pagina *Impostazioni protezione*.



Passaggio 4. Dal menu a discesa Seleziona SSID, scegliere un SSID per il quale si desidera modificare le impostazioni di sicurezza.

Disabilita modalità di protezione

In questa procedura viene illustrato come disattivare la modalità di protezione di un SSID che non richiederà informazioni di protezione per l'utilizzo del SSID.

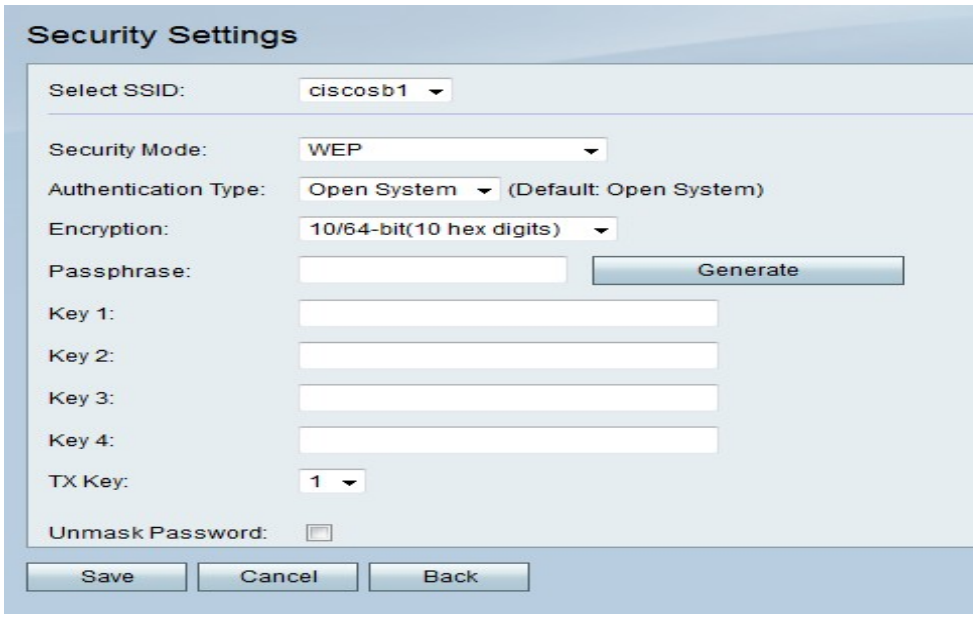
Passaggio 1. Dal menu a discesa Modalità di sicurezza, scegliere **Disabilitato**.

Passaggio 2. Fare clic su **Salva** per salvare le modifiche, su **Annulla** per eliminarle o su **Indietro** per tornare alla pagina precedente.

Modalità di protezione WEP

In questa procedura viene illustrato come impostare la modalità di protezione WEP (Wired Equivalent Privacy) di un SSID. WEP non è la modalità di protezione più sicura, ma può essere l'unica opzione se alcuni dispositivi di rete non supportano WPA.

Passaggio 1. Dal menu a discesa Modalità di protezione, scegliere **WEP**.



Passaggio 2. Dal menu a discesa Tipo di autenticazione, scegliere un'opzione.

- Sistema aperto: questa opzione è più diretta e sicura dell'autenticazione con chiave condivisa.
- Chiave condivisa: questa opzione è meno sicura di Apri sistema.

Passaggio 3. Dal menu a discesa Encryption, scegliere 10/64-bit (10 cifre esadecimali), che

usa una chiave a 40 bit, o 26/128-bit (26 cifre esadecimali), che usa una chiave a 104 bit.

Passaggio 4. Nel campo Passphrase, inserire una passphrase con lettere e numeri lunga almeno 8 caratteri.

Passaggio 5. Fare clic su **Genera** per creare quattro chiavi WEP nei campi Chiave oppure immettere manualmente le chiavi WEP nei campi Chiave.

Passaggio 6. Dal menu a discesa Chiave TX, scegliere il numero del campo Chiave della chiave WEP che si desidera utilizzare come chiave condivisa.

Passaggio 7. Selezionare la casella di controllo **Unmask password** se si desidera visualizzare i caratteri della password.

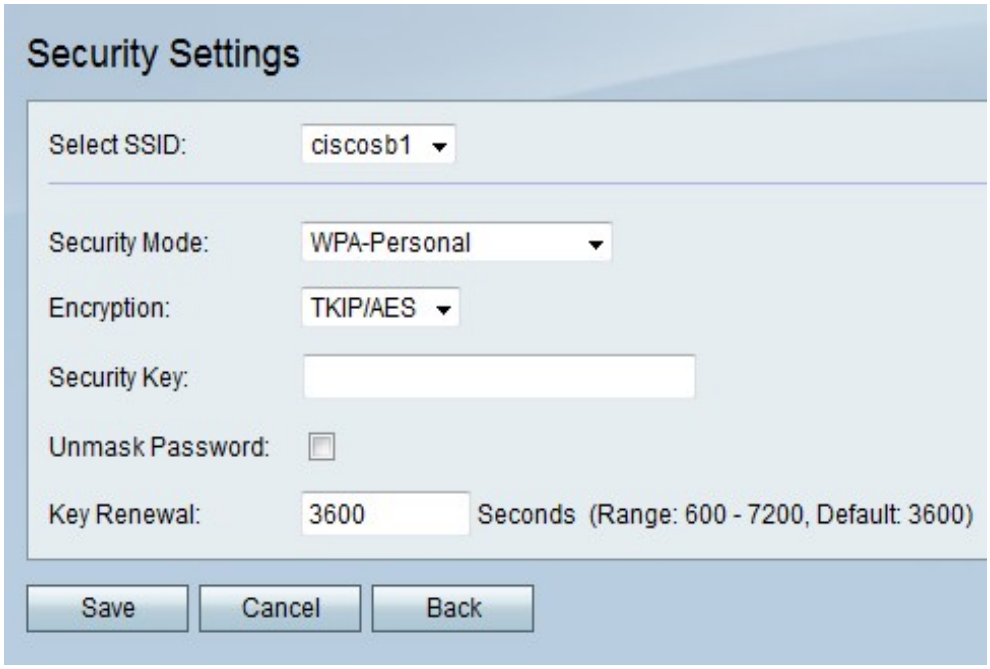
Passaggio 8. Fare clic su **Salva** per salvare le modifiche, **Annulla** per eliminarle o **Indietro** per tornare alla pagina precedente.

Modalità di protezione mista WPA-Personale, WPA2-Personale e WPA2-Personale

WPA (Wi-Fi Protected Access) è una modalità di protezione più avanzata di WEP. WPA-Personale può utilizzare il protocollo TKIP (Temporal Key Integrity Protocol) o AES (Advanced Encryption Standard) per la crittografia. WPA2-Personale utilizza solo AES per la crittografia e una chiave già condivisa (PSK) per l'autenticazione. WPA2-Personal Mixed è in grado di supportare entrambi i client WPA e WPA2 e utilizza AES e PSK. In questa procedura viene illustrato come impostare WPA-Personale, WPA2-Personale o WPA2-Personale misto come modalità di protezione per un SSID.

Passaggio 1. Dal menu a discesa Modalità di protezione, scegliere un'opzione.

- WPA-Personale - Questa opzione supporta AES e TKIP.
- WPA2-Personale — questa opzione supporta AES e PSK.
- WPA2-Personale misto: questa opzione supporta client WPA e WPA2.



Passaggio 2. Se si sceglie WPA-Personale, scegliere un tipo di cifratura dal menu a discesa Cifratura.

- TKIP/AES: questa opzione è compatibile con i dispositivi meno recenti che non supportano AES.
- AES: questa opzione è più sicura di TKIP/AES.

Passaggio 3. Nel campo Chiave di accesso, inserire una frase di lettere e numeri che limiti l'accesso alla rete.

Passaggio 4. Selezionare la casella di controllo **Unmask password** se si desidera visualizzare i caratteri della password.

Passaggio 5. Nel campo Rinnovo chiave, immettere la frequenza in secondi con cui la rete rinnova la chiave.

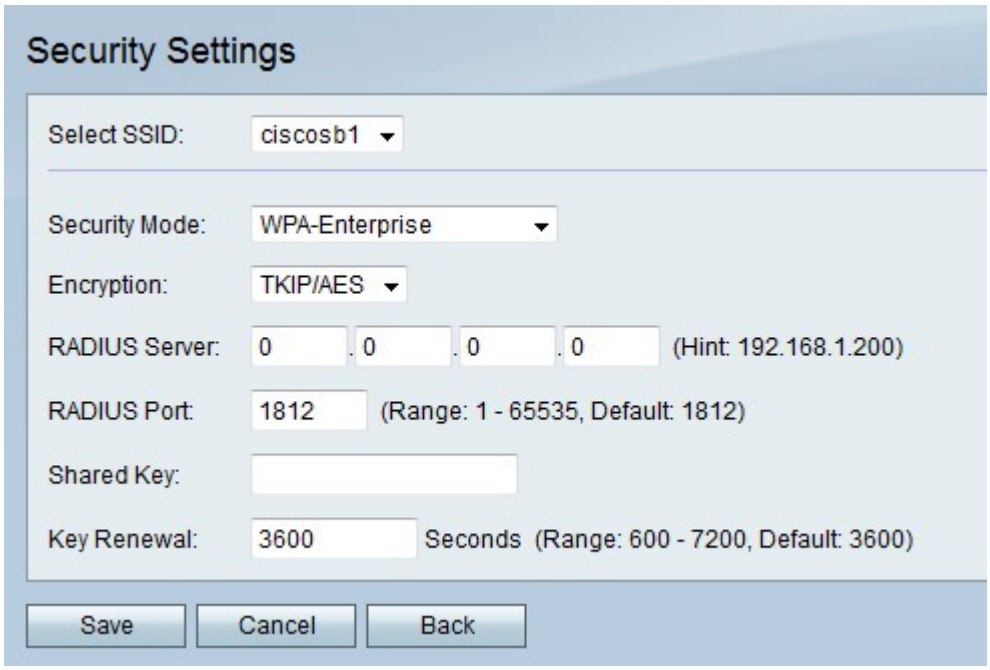
Passaggio 6. Fare clic su **Salva** per salvare le modifiche, **Annulla** per eliminarle o **Indietro** per tornare alla pagina precedente.

Modalità di sicurezza mista WPA-Enterprise, WPA2-Enterprise e WPA2-Enterprise

Le modalità di protezione Enterprise utilizzano l'autenticazione server RADIUS (Remote Authentication Dial In User Service). RADIUS è un protocollo di rete che utilizza un server separato e il traffico da e verso la rete deve passare attraverso il server RADIUS. In questa procedura viene illustrato come impostare WPA-Enterprise, WPA2-Enterprise o WPA2-Enterprise Mixed come modalità di protezione per un SSID.

Passaggio 1. Dal menu a discesa Modalità di protezione, scegliere un'opzione.

- WPA-Enterprise: questa opzione utilizza RADIUS, AES e TKIP.
- WPA2-Enterprise: questa opzione utilizza RADIUS, AES e PSK.
- WPA2-Enterprise Mixed: questa opzione utilizza RADIUS e supporta client WPA e WPA2.



Passaggio 2. Se si sceglie WPA-Enterprise, scegliere un tipo di cifratura dal menu a discesa Cifratura.

- TKIP/AES: questa opzione è compatibile con i dispositivi meno recenti che non supportano

AES.

- AES: questa opzione è più sicura di TKIP/AES.

Passaggio 3. Nel campo Server RADIUS, immettere l'indirizzo IP del server RADIUS.

Passaggio 4. Nel campo Porta RADIUS, immettere il numero della porta sulla quale la rete accede al server RADIUS.

Passaggio 5. Nel campo Chiave condivisa, inserire una frase di lettere e numeri che limiti l'accesso alla rete.

Passaggio 6. Nel campo Rinnovo chiave, immettere la frequenza in secondi con cui la rete rinnova la chiave.

Passaggio 7. Fare clic su **Salva** per salvare le modifiche, **Annulla** per eliminarle o **Indietro** per tornare alla pagina precedente.