

Configurazione delle impostazioni wireless di base su RV215W

Obiettivo

Le reti wireless sono reti di computer non connesse tramite cavi. Una rete WLAN (Wireless Local Area Network) è un tipo di rete wireless che collega più dispositivi su una breve distanza tramite l'utilizzo di una comunicazione radio.

Questo articolo spiega come configurare le impostazioni wireless di base sull'RV215W, inclusa la configurazione della sicurezza di rete.

Indice

- [Impostazioni generali](#)
- [Modifica tabella wireless](#)
- [Disabilitare la sicurezza](#)
- [Configurazione della protezione WEP](#)
- [Configurazione della protezione WPA-Personale](#)
- [Configurazione della protezione WPA-Enterprise](#)
- [Configurazione della protezione mista WPA2-Personal/WPA2-Personal](#)
- [Configurazione della protezione mista WPA2-Enterprise/WPA2-Enterprise](#)
- [Modifica del filtro MAC](#)
- [Accesso all'ora](#)
- [Modifica rete guest](#)
- [Configurazione metodo 1 WPS](#)
- [Configurazione metodo 2 WPS](#)
- [Configurazione del metodo WPS 3](#)

Dispositivi interessati

- RV215W

Versione del software

- 1.1.0.5

Configurazione delle impostazioni di base

Impostazioni generali

Passaggio 1. Accedere all'utility di configurazione Web e scegliere Wireless > Impostazioni di base. Viene visualizzata la pagina Impostazioni di base:

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

	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	Guest Network	VLAN	Wireless Isolation with SSID	WMM	WPS
☐	☒ ON	ciscosb1	☒	WPA2-Personal Mixed	Disabled	☐	1	☐	☒	☒
☐	☐ OFF	ciscosb2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb4	☐	Disabled	Disabled	☐	1	☐	☒	☐

Edit Edit Security Mode Edit MAC Filtering Time of Day Access Edit Guest Net Edit WPS

Save Cancel

Passaggio 2. Selezionare Attiva nel campo Radio per attivare la radio wireless.

Passaggio 3. Dall'elenco a discesa Modalità di rete wireless, scegliere la modalità wireless.

- B/G/N-Mixed: la rete contiene una combinazione di dispositivi wireless-B, wireless-G e wireless-N.
- Solo B: la rete contiene solo periferiche B wireless.
- G-Only: la rete contiene solo periferiche wireless-G.
- Solo N: la rete contiene solo periferiche Wireless-N.
- B/G-Mixed: la rete contiene una combinazione di dispositivi wireless-B e wireless-G.
- G/N Misto: la rete contiene una combinazione di dispositivi wireless-G e wireless-N.

Passaggio 4. Se la modalità di rete contiene periferiche Wireless-N, fare clic sul pulsante di opzione corrispondente alla larghezza di banda desiderata nel campo Selezione banda wireless. Maggiore è la larghezza di banda, maggiore è la quantità di dati che il segnale può trasportare.

- 20 MHz: la frequenza standard per un segnale wireless.
- 20/40 MHz: utilizza automaticamente un segnale da 20 MHz e 40 MHz. Un segnale a 40 MHz fornisce maggiore larghezza di banda ma è soggetto a maggiori interferenze. Questa opzione viene utilizzata solo se le periferiche wireless collegate sono compatibili con la frequenza di 40 MHz.

Passaggio 5. Dall'elenco a discesa Canale wireless, scegliere un canale wireless per la radio. Scegliere un canale attualmente non utilizzato dalle reti adiacenti.

Passaggio 6. Dall'elenco a discesa VLAN di gestione dell'access point scegliere una VLAN che deve diventare la VLAN di gestione.

Passaggio 7. (Facoltativo) Selezionare Abilita nel campo U-APSD per abilitare la funzione di risparmio energetico automatico non programmata (U-APSD). U-APSD è una funzione che permette alla radio di risparmiare energia. Tuttavia, U-APSD può ridurre le prestazioni di throughput della radio.

Passaggio 8. Fare clic su Save (Salva).

Modifica tabella wireless

Passaggio 1. Accedere all'utility di configurazione Web e scegliere Wireless > Impostazioni di base. Viene visualizzata la pagina Impostazioni di base:

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

☐	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	Guest Network	VLAN	Wireless Isolation with SSID	WMM	WPS
☒	☒ ON	ciscosb1	☒	WPA2-Personal	Enabled	☐	1	☒	☒	☒
☐	☐ OFF	ciscosb2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb4	☐	Disabled	Disabled	☐	1	☐	☒	☐

Passaggio 2. Selezionare la casella di controllo della rete che si desidera modificare nella tabella Wireless.

Passaggio 3. Fare clic su Modifica per modificare la rete specificata.

Passaggio 4. Fare clic sul pulsante Abilita SSID per abilitare la rete. SSID (Service Set Identifier) è il nome della rete wireless.

Passaggio 5. Inserire il nome della rete nel campo Nome SSID. Tutti i dispositivi della rete devono utilizzare questo SSID per comunicare tra loro.

Passaggio 6. Selezionare SSID Broadcast per abilitare la trasmissione wireless. RV215W annuncia la propria disponibilità ai dispositivi wireless nelle vicinanze quando è abilitata la trasmissione SSID.

Passaggio 7. Selezionare Rete guest per rendere la rete configurata una rete guest. Una rete guest è una piccola sezione di una rete progettata per utenti temporanei. Questa opzione consente agli utenti guest di utilizzare la rete senza dover esporre chiavi Wi-Fi private.

Nota: Impossibile configurare la rete guest sulla VLAN di gestione AP.

Passaggio 8. Dall'elenco a discesa VLAN, selezionare la VLAN associata alla rete.

Passaggio 9. Verificare l'isolamento wireless con SSID per impedire che le periferiche della rete specificata possano comunicare tra loro.

Passaggio 10. Selezionare WMM per abilitare Wi-Fi Multimedia (WMM) sulla rete. WMM viene utilizzato per migliorare lo streaming di contenuti multimediali su dispositivi wireless. WMM assegna una priorità più alta al traffico multimediale inviato tramite una connessione wireless.

Passaggio 11. (Facoltativo) Selezionare WPS per assegnare la rete specificata come rete WPS (Wi-Fi Protected Setup). WPS è una funzionalità che consente una configurazione di rete semplice e sicura. Questa funzione consente ai dispositivi di connettersi facilmente alla rete.

Passaggio 12. Fare clic su Save (Salva).

Disabilita protezione

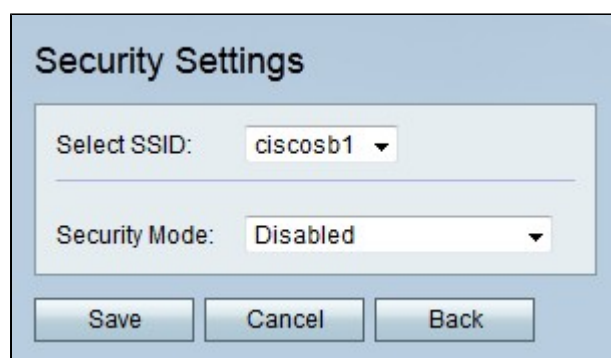
La protezione wireless può essere disattivata sulla RV215W per una maggiore facilità d'uso durante la configurazione delle reti di prova, ma non è consigliabile disattivare la protezione.

Passaggio 1. Accedere all'utility di configurazione Web e scegliere Wireless > Impostazioni di base. Viene visualizzata la pagina Impostazioni di base.

Passaggio 2. Selezionare la casella della rete che si desidera modificare.

Passaggio 3. Fare clic su Modifica modalità di protezione per modificare la protezione della rete specificata. Viene visualizzata la pagina Impostazioni protezione:

Passaggio 4. (Facoltativo) Dall'elenco a discesa Seleziona SSID scegliere l'SSID per cui si desidera configurare la sicurezza.



The screenshot shows a web interface titled "Security Settings". It contains two dropdown menus. The first is labeled "Select SSID:" and has "ciscosb1" selected. The second is labeled "Security Mode:" and has "Disabled" selected. Below these are three buttons: "Save", "Cancel", and "Back".

Passaggio 5. Dall'elenco a discesa Modalità di sicurezza scegliere Disabilitato. La protezione è disattivata per la rete wireless.

Passaggio 6. Fare clic su Save (Salva).

Configurare la protezione WEP

WEP (Wired Equivalent Privacy) è un algoritmo che protegge una rete wireless. WEP fornisce un metodo di crittografia di base meno sicuro di WPA. WEP viene utilizzato quando i dispositivi di rete collegati non supportano WPA.

Passaggio 1. Accedere all'utilità di configurazione Web e scegliere Wireless > Impostazioni di base. Viene visualizzata la pagina Impostazioni di base.

Passaggio 2. Selezionare la casella della rete che si desidera modificare.

Passaggio 3. Fare clic su Modifica modalità di protezione per modificare la protezione della rete specificata. Viene visualizzata la pagina Impostazioni protezione:



The screenshot shows a web interface titled "Security Settings". It contains several configuration options:

- Select SSID:** A dropdown menu with "ciscosb1" selected.
- Security Mode:** A dropdown menu with "WEP" selected.
- Authentication Type:** A dropdown menu with "Open System" selected, with "(Default: Open System)" in parentheses.
- Encryption:** A dropdown menu with "26/128-bit(26 hex digits)" selected.
- Passphrase:** A text input field containing "passphrase1" and a "Generate" button.
- Key 1:** A text input field filled with dots.
- Key 2:** A text input field filled with dots.
- Key 3:** A text input field filled with dots.
- Key 4:** A text input field filled with dots.
- TX Key:** A dropdown menu with "1" selected.
- Unmask Password:** An unchecked checkbox.

At the bottom of the form are three buttons: "Save", "Cancel", and "Back".

Passaggio 4. (Facoltativo) Dall'elenco a discesa Seleziona SSID scegliere l'SSID per cui si desidera configurare la sicurezza.

Passaggio 5. Dall'elenco a discesa Modalità di protezione scegliere WEP.

Passaggio 6. Dall'elenco a discesa Tipo di autenticazione scegliere un tipo di autenticazione per la rete wireless.

- Sistema aperto: chiunque può associarsi al punto di accesso, ma la chiave WEP è necessaria per far passare il traffico attraverso il punto di accesso della rete.
- Chiave condivisa: è necessaria una chiave WEP per l'associazione al punto di accesso e per il passaggio del traffico attraverso il punto di accesso della rete.

Passaggio 7. Dall'elenco a discesa Crittografia scegliere un metodo di crittografia per la chiave WEP.

- 10/64 bit (10 cifre esadecimali) - Fornisce una chiave a 40 bit.
- 26/128 bit (26 cifre esadecimali) - Fornisce una chiave a 104 bit. Questa è la crittografia più sicura.

Passaggio 8. Inserire una passphrase con più di otto caratteri nel campo Passphrase.

Passaggio 9. Fare clic su Genera per creare le chiavi nei campi Chiave 1, Chiave 2, Chiave 3 e Chiave 4.

Nota: È inoltre possibile immettere manualmente le chiavi nei campi Chiave 1, Chiave 2, Chiave 3 e Chiave 4.

Passaggio 10. Dall'elenco a discesa TX Key (Chiave TX), selezionare la Chiave che gli utenti devono immettere per accedere alla rete wireless.

Passaggio 11. (Facoltativo) Selezionare Unmask Password per visualizzare le stringhe di caratteri dei tasti.

Passaggio 12. Fare clic su Save (Salva).

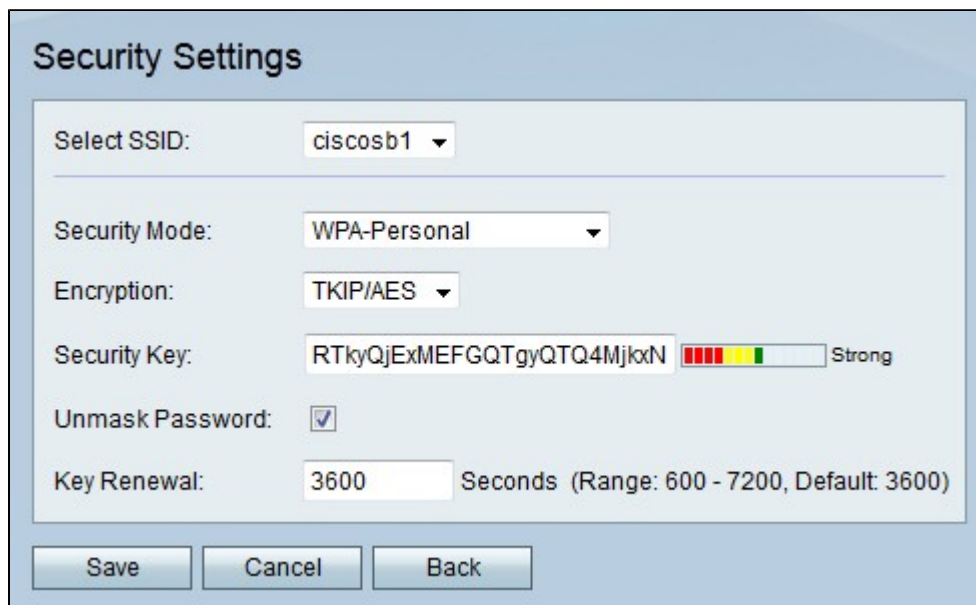
Configura protezione WPA-Personale

WPA (Wi-Fi Protected Access) è uno standard di sicurezza per le reti wireless. WPA è stato creato per sostituire WEP a causa dei difetti di sicurezza di WEP. WPA-Personale è una versione di WPA utilizzata per reti con pochi utenti. WPA-Personale fornisce una chiave condivisa che ogni utente utilizzerà per accedere alla rete wireless. WPA è stato introdotto con i metodi di crittografia delle chiavi TKIP (Temporal Key Integrity Protocol) e AES (Advanced Encryption Standard). Più dispositivi di rete supportano TKIP, tuttavia AES è il metodo di crittografia più avanzato.

Passaggio 1. Accedere all'utility di configurazione Web e scegliere Wireless > Impostazioni di base. Viene visualizzata la pagina Impostazioni di base.

Passaggio 2. Selezionare la casella della rete che si desidera modificare.

Passaggio 3. Fare clic su Modifica modalità di protezione per modificare la protezione della rete specificata. Viene visualizzata la pagina Impostazioni protezione:



The screenshot shows a web interface titled "Security Settings". It contains several configuration fields:

- Select SSID:** A dropdown menu with "ciscosb1" selected.
- Security Mode:** A dropdown menu with "WPA-Personal" selected.
- Encryption:** A dropdown menu with "TKIP/AES" selected.
- Security Key:** A text input field containing "RTkyQjExMEFGQTgyQTQ4MjIxN". To the right of the input is a strength indicator with four colored bars (red, red, yellow, green) and the word "Strong".
- Unmask Password:** A checkbox that is checked.
- Key Renewal:** A text input field containing "3600", followed by the text "Seconds (Range: 600 - 7200, Default: 3600)".

At the bottom of the form are three buttons: "Save", "Cancel", and "Back".

Passaggio 4. (Facoltativo) Dall'elenco a discesa Seleziona SSID scegliere l'SSID per cui si desidera configurare la sicurezza.

Passaggio 5. Dall'elenco a discesa Modalità di protezione scegliere WPA-Personale.

Passaggio 6. Dall'elenco a discesa Crittografia scegliere un metodo di crittografia per la chiave WPA.

- TKIP/AES: questa opzione è selezionata quando non tutti i dispositivi collegati alla rete wireless supportano AES.
- AES: questa opzione è preferibile se tutti i dispositivi collegati ai dispositivi wireless supportano AES.

Passaggio 7. Immettere una chiave di sicurezza nel campo Chiave di sicurezza.

Passaggio 8. (Facoltativo) Selezionare Unmask Password per visualizzare la stringa di caratteri della chiave.

Passaggio 9. Inserire un'ora nel campo Rinnovo chiave. Questa è la quantità di tempo che la RV215W utilizzerà per generare una nuova chiave.

Passaggio 10. Fare clic su Save (Salva).

Configura protezione WPA-Enterprise

WPA (Wi-Fi Protected Access) è uno standard di sicurezza per le reti wireless. WPA è stato creato per sostituire WEP a causa dei difetti di sicurezza di WEP. WPA-Enterprise è una versione di WPA consigliata per una rete con molti utenti, ad esempio un'azienda. L'autenticazione utilizzata per ottenere l'accesso è controllata da un server RADIUS. Ciò significa che a ogni utente connesso verrà assegnata una chiave univoca per accedere alla rete wireless. WPA è stato introdotto con i metodi di crittografia delle chiavi TKIP (Temporal Key Integrity Protocol) e AES (Advanced Encryption Standard). Più dispositivi di rete supportano TKIP, tuttavia AES è il metodo di crittografia più avanzato.

Passaggio 1. Accedere all'utility di configurazione Web e scegliere Wireless > Impostazioni di base. Viene visualizzata la pagina Impostazioni di base.

Passaggio 2. Selezionare la casella della rete che si desidera modificare.

Passaggio 3. Fare clic su Modifica modalità di protezione per modificare la protezione della rete specificata. Viene visualizzata la pagina Impostazioni protezione:

The screenshot shows a web-based configuration interface titled "Security Settings". It contains several fields for configuring wireless security:

- Select SSID:** A dropdown menu with "ciscosb1" selected.
- Security Mode:** A dropdown menu with "WPA-Enterprise" selected.
- Encryption:** A dropdown menu with "AES" selected.
- RADIUS Server:** Four input fields containing "192", "168", "1", and "250", followed by the text "(Hint: 192.168.1.200)".
- RADIUS Port:** An input field containing "1812", followed by the text "(Range: 1 - 65535, Default: 1812)".
- Shared Key:** An input field containing "SharedKey1".
- Key Renewal:** An input field containing "3600", followed by the text "Seconds (Range: 600 - 7200, Default: 3600)".

At the bottom of the form are three buttons: "Save", "Cancel", and "Back".

Passaggio 4. (Facoltativo) Dall'elenco a discesa Seleziona SSID scegliere l'SSID per cui si desidera configurare la sicurezza.

Passaggio 5. Dall'elenco a discesa Modalità di protezione scegliere WPA-Enterprise.

Passaggio 6. Dall'elenco a discesa Crittografia scegliere un metodo di crittografia per la chiave WPA.

- TKIP/AES: questa opzione è selezionata quando non tutti i dispositivi collegati alla rete wireless supportano AES.
- AES: questa opzione è preferibile se tutti i dispositivi collegati ai dispositivi wireless supportano AES.

Passaggio 7. Immettere l'indirizzo IP del server RADIUS nel campo Server RADIUS.

Passaggio 8. Immettere il numero di porta utilizzato per accedere al server RADIUS nel campo Porta RADIUS.

Passaggio 9. Immettere la chiave già condivisa per gli utenti wireless nel campo Chiave condivisa. Una chiave già condivisa è una chiave utilizzata per tutti gli utenti. La funzionalità di chiave già condivisa è una funzionalità di protezione aggiuntiva insieme all'autenticazione RADIUS.

Passaggio 10. Inserire un'ora nel campo Rinnovo chiave. Questa è la quantità di tempo che la RV215W utilizzerà per generare una nuova chiave.

Passaggio 11. Fare clic su Save (Salva).

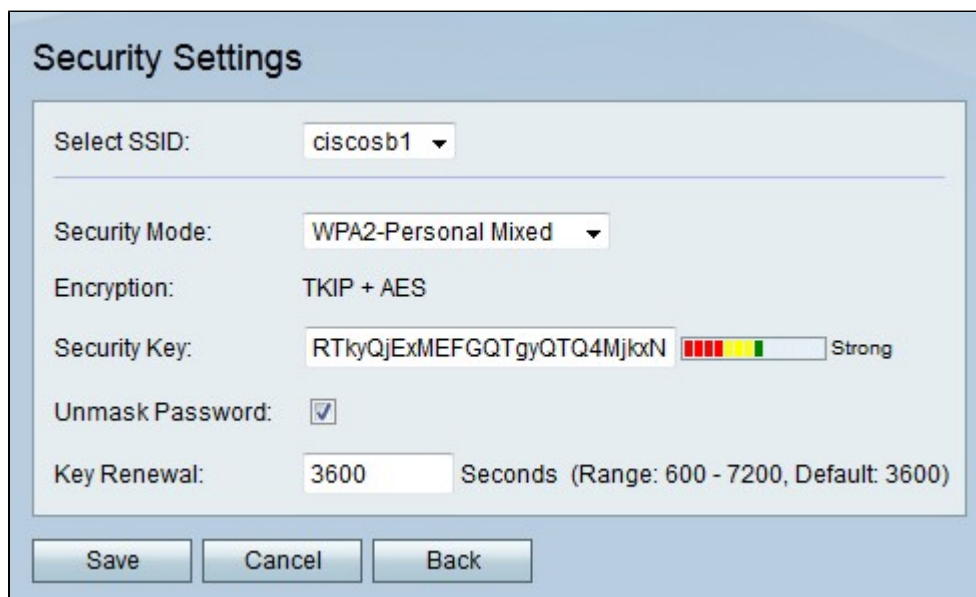
Configurazione della protezione mista WPA2-Personale/WPA2-Personale

Wi-Fi Protected Access 2 (WPA2) è uno standard di sicurezza per le reti wireless. WPA2 è un miglioramento di WPA. WPA2 offre una maggiore protezione rispetto a WPA, tuttavia richiede una maggiore potenza di elaborazione. WPA2-Personale/WPA2-Personale misto sono versioni di WPA2 utilizzate per reti con pochi utenti. WPA2-Personal Mixed è progettato per la compatibilità con le versioni precedenti dei dispositivi che non sono in grado di utilizzare WPA2. Se possibile, non utilizzare WPA2-Personal Mixed in quanto offre una connessione meno sicura. WPA2-Personale fornisce una chiave condivisa che ogni utente utilizzerà per accedere alla rete wireless. WPA2 utilizza i metodi di crittografia TKIP (Temporal Key Integrity Protocol) e AES (Advanced Encryption Standard). Più dispositivi di rete supportano TKIP, tuttavia AES è il metodo di crittografia più avanzato.

Passaggio 1. Accedere all'utility di configurazione Web e scegliere Wireless > Impostazioni di base. Viene visualizzata la pagina Impostazioni di base.

Passaggio 2. Selezionare la casella della rete che si desidera modificare.

Passaggio 3. Fare clic su Modifica modalità di protezione per modificare la protezione della rete specificata. Viene visualizzata la pagina Impostazioni protezione:



Security Settings

Select SSID: ciscosb1

Security Mode: WPA2-Personal Mixed

Encryption: TKIP + AES

Security Key: RTkyQjExMEFGQTgyQTQ4MjlkxN Strong

Unmask Password: ☒

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

Save Cancel Back

Passaggio 4. (Facoltativo) Dall'elenco a discesa Seleziona SSID scegliere l'SSID per cui si desidera configurare la sicurezza.

Passaggio 5. Dall'elenco a discesa Modalità di protezione scegliere WPA2-Personale o WPA2-Personale misto. WPA2-Personale viene utilizzato quando tutti i dispositivi della rete wireless supportano AES. WPA2-Personal Mixed viene utilizzato quando non tutti i dispositivi supportano AES.

Nota: Il tipo di crittografia utilizzato dal metodo di protezione viene visualizzato nel campo Crittografia.

Passaggio 6. Immettere una chiave di sicurezza nel campo Chiave di sicurezza.

Passaggio 7. (Facoltativo) Selezionare Unmask Password per visualizzare le stringhe di caratteri del tasto.

Passaggio 8. Inserire un'ora nel campo Rinnovo chiave. Questa è la quantità di tempo che la RV215W utilizzerà per generare una nuova chiave.

Passaggio 9. Fare clic su Save (Salva).

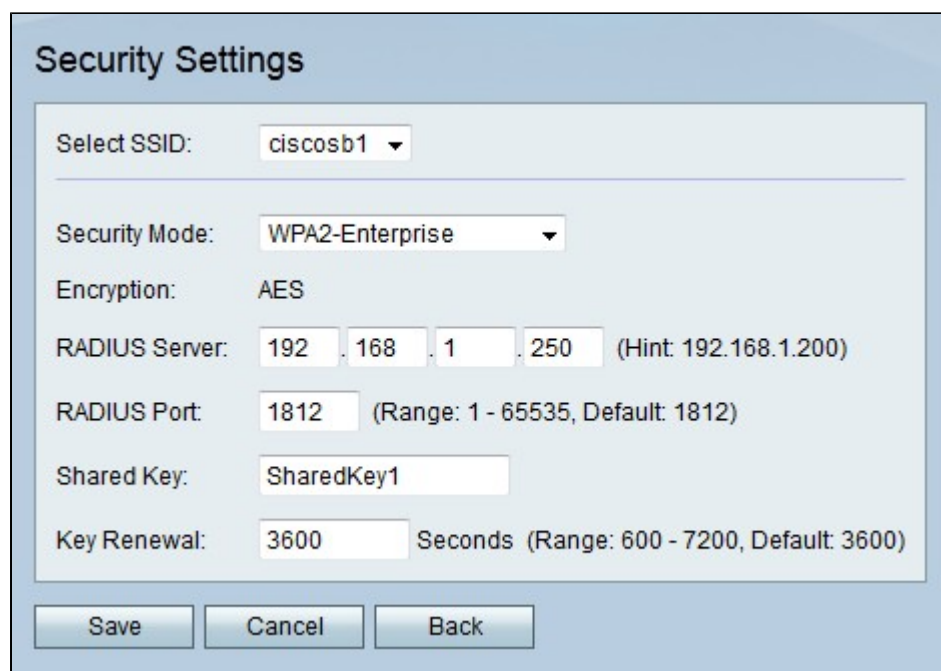
Configurazione della protezione mista WPA2-Enterprise/WPA2-Enterprise

Wi-Fi Protected Access 2 (WPA2) è uno standard di sicurezza per le reti wireless. WPA2 è un miglioramento di WPA. WPA2 offre una maggiore protezione rispetto a WPA, tuttavia richiede una maggiore potenza di elaborazione. WPA2-Enterprise/WPA2-Enterprise Mixed sono versioni di WPA2 utilizzate per reti con molti utenti, ad esempio un'azienda. WPA2-Enterprise Mixed è progettato per la compatibilità con le versioni precedenti dei dispositivi che non sono in grado di utilizzare WPA2. Se possibile, non utilizzare WPA2-Enterprise Mixed in quanto fornisce una connessione meno sicura. L'autenticazione per determinare se un utente ottiene l'accesso è controllata da un server RADIUS. Ciò significa che a ogni utente connesso verrà assegnata una chiave univoca per accedere alla rete wireless. WPA2 utilizza i metodi di crittografia TKIP (Temporal Key Integrity Protocol) e AES (Advanced Encryption Standard). Più dispositivi di rete supportano TKIP, tuttavia AES è il metodo di crittografia più avanzato.

Passaggio 1. Accedere all'utility di configurazione Web e scegliere Wireless > Impostazioni di base. Viene visualizzata la pagina Impostazioni di base.

Passaggio 2. Selezionare la casella della rete che si desidera modificare.

Passaggio 3. Fare clic su Modifica modalità di protezione per modificare la protezione della rete specificata. Viene visualizzata la pagina Impostazioni protezione:



The screenshot shows a web interface titled "Security Settings". It contains several configuration fields for a wireless network. At the top, there is a "Select SSID:" dropdown menu with "ciscosb1" selected. Below this is a "Security Mode:" dropdown menu with "WPA2-Enterprise" selected. The "Encryption:" field is set to "AES". The "RADIUS Server:" field consists of four input boxes containing "192", "168", "1", and "250", with a hint "(Hint: 192.168.1.200)". The "RADIUS Port:" field has an input box with "1812" and a range note "(Range: 1 - 65535, Default: 1812)". The "Shared Key:" field has an input box with "SharedKey1". The "Key Renewal:" field has an input box with "3600" and a range note "(Range: 600 - 7200, Default: 3600)". At the bottom, there are three buttons: "Save", "Cancel", and "Back".

Passaggio 4. (Facoltativo) Dall'elenco a discesa Seleziona SSID scegliere l'SSID per cui si desidera configurare la sicurezza.

Passaggio 5. Dall'elenco a discesa Modalità di protezione scegliere WPA2-Enterprise o WPA2-Enterprise Mixed. WPA2-Enterprise viene utilizzato quando tutti i dispositivi della rete wireless supportano AES. WPA2-Enterprise Mixed viene utilizzato quando non tutti i dispositivi supportano AES.

Nota: Il tipo di crittografia utilizzato dal metodo di protezione viene visualizzato nel campo Crittografia.

Passaggio 6. Immettere l'indirizzo IP del server RADIUS nel campo Server RADIUS.

Passaggio 7. Immettere la porta utilizzata per accedere al server RADIUS nel campo Porta RADIUS.

Passaggio 8. Immettere la chiave già condivisa per gli utenti wireless nel campo Chiave condivisa. Una chiave già condivisa è una chiave utilizzata per tutti gli utenti. La funzionalità di chiave già condivisa è una funzionalità di protezione aggiuntiva insieme all'autenticazione RADIUS.

Passaggio 9. Inserire un'ora nel campo Rinnovo chiave. Questa è la quantità di tempo che la RV215W utilizzerà per generare una nuova chiave.

Passaggio 10. Fare clic su Save (Salva).

Modifica filtro MAC

Il filtro MAC viene usato per autorizzare o negare l'accesso alla rete wireless in base all'indirizzo MAC del dispositivo di connessione.

Passaggio 1. Accedere all'utilità di configurazione Web e scegliere Wireless > Impostazioni di base. Viene visualizzata la pagina Impostazioni di base:

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

	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	Guest Network	VLAN	Wireless Isolation with SSID	WMM	WPS
☒	ON	ciscosb1	☒	WPA2-Personal Mixed	Disabled	☐	1	☒	☒	☒
☐	OFF	ciscosb2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	OFF	ciscosb3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	OFF	ciscosb4	☐	Disabled	Disabled	☐	1	☐	☒	☐

Edit Edit Security Mode Edit MAC Filtering Time of Day Access Edit Guest Net Edit WPS

Save Cancel

Passaggio 2. Selezionare la casella della rete che si desidera modificare.

Passaggio 3. Fare clic su Modifica filtro MAC per creare un elenco di controllo di accesso MAC per la rete specificata. Viene visualizzata la pagina Wireless MAC Filter:

Wireless MAC Filter

SSID: ciscosb1

Wireless MAC Filter: ☒ Enable

Connection Control

☒ **Prevent** PCs listed below from accessing the wireless network.

☐ **Permit** PCs listed below to access the wireless network.

Hide Client List

Client List Table

Client Name	IP Address	MAC Address	Status	Save to MAC Address Filter List
		9C:B7:0D:73:43:29	Disconnected	☒

Add to MAC

MAC Address Table

01	9C:B7:0D:73:43:29	12		23	
02		13		24	
03		14		25	
04		15		26	
05		16		27	
06		17		28	
07		18		29	
08		19		30	
09		20		31	
10		21		32	
11		22			

Save

Cancel

Back

Passaggio 4. Selezionare Enable per abilitare il filtro MAC sulla rete.

Passaggio 5. Fare clic sul pulsante di opzione corrispondente al tipo di elenco desiderato nel campo Controllo connessione.

- Impedisci l'accesso alla rete da parte dei PC con gli indirizzi MAC elencati.
- Autorizza PC: consente ai PC con gli indirizzi MAC elencati di accedere alla rete.

Passaggio 6. Inserire gli indirizzi MAC desiderati nella tabella degli indirizzi MAC.

Passaggio 7. Fare clic su Save (Salva).

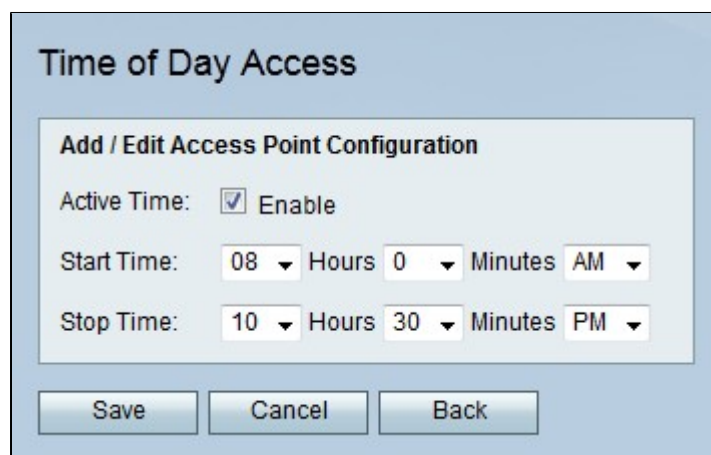
Accesso all'ora

La funzionalità di accesso ora del giorno viene utilizzata per consentire l'accesso agli utenti solo in base a una pianificazione configurata.

Passaggio 1. Accedere all'utility di configurazione Web e scegliere Wireless > Impostazioni di base. Viene visualizzata la pagina Impostazioni di base:

Passaggio 2. Selezionare la casella della rete che si desidera modificare.

Passaggio 3. Fare clic su Accesso ora del giorno per configurare quando gli utenti possono accedere alla rete specificata. Viene visualizzata la pagina Accesso ora del giorno:



Time of Day Access

Add / Edit Access Point Configuration

Active Time: ☒ Enable

Start Time: 08 Hours 0 Minutes AM

Stop Time: 10 Hours 30 Minutes PM

Save Cancel Back

Passaggio 4. Selezionare Abilita nel campo Orario attivo per abilitare l'accesso all'ora del giorno per la rete.

Passaggio 5. Inserire l'ora in cui ha inizio l'accesso alla rete nel campo Ora di inizio.

Passaggio 6. Inserire l'ora in cui termina l'accesso alla rete nel campo Ora di arresto.

Passaggio 7. Fare clic su Save (Salva).

Modifica rete guest

Una rete guest è una piccola sezione di una rete progettata per utenti temporanei. Questa funzione consente agli utenti guest di utilizzare la rete senza dover esporre chiavi Wi-Fi private. È possibile configurare una rete guest per limitare il tempo di accesso e l'utilizzo della larghezza di banda di un utente.

Passaggio 1. Accedere all'utility di configurazione Web e scegliere Wireless > Impostazioni di base. Viene visualizzata la pagina Impostazioni di base:

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	Guest Network	VLAN	Wireless Isolation with SSID	WMM	WPS
☐	☒ ON	ciscosb1	☒	WPA2-Personal Mixed	Disabled	☐	1	☐	☒	☒
☐	☐ OFF	ciscosb2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb4	☐	Disabled	Disabled	☐	1	☐	☒	☐

Edit Edit Security Mode Edit MAC Filtering Time of Day Access **Edit Guest Net** Edit WPS

Save Cancel

Passaggio 2. Fare clic su Modifica rete guest per configurare la rete guest. Viene visualizzata la pagina Impostazioni rete guest:

Guest Net Settings

Guest Net Name:

Guest Password:  Secure

Confirm Guest Password:

Guest Access Time: Minutes (Range: 30 - 1440, Default: 120)

Enable Guest Bandwidth Restriction: ☒ Enable (Enable QoS in the [Bandwidth Management page](#))

Available Bandwidth: % (Range: 1 - 99, Default: 20)

Passaggio 3. Immettere una password che gli utenti utilizzeranno per accedere alla rete guest nel campo Password guest.

Passaggio 4. Immettere nuovamente la password che gli utenti utilizzeranno per accedere alla rete guest nel campo Conferma password guest.

Passaggio 5. Immettere l'ora in cui gli utenti possono rimanere connessi alla rete guest nel campo Ora di accesso guest.

Passaggio 6. Selezionare Abilita limitazione larghezza di banda guest per limitare la quantità di larghezza di banda che la rete guest riceve.

Nota: La gestione della larghezza di banda deve essere abilitata nella pagina Gestione larghezza di banda.

Passaggio 7. Immettere la percentuale della larghezza di banda disponibile per la rete guest nel campo Larghezza di banda disponibile.

Passaggio 8. Fare clic su Save (Salva).

Configura metodo WPS 1

Wi-Fi Protected Setup (WPS) è una funzione che consente di configurare una rete wireless in modo semplice e sicuro. Per connettersi a WPS, il dispositivo di connessione deve supportare WPS e deve essere compatibile con la protezione WPA. Il primo metodo di configurazione è un metodo semplice che richiede la pressione del pulsante RV215W WPS e del pulsante del

dispositivo client. Una volta premuti entrambi i pulsanti, il dispositivo client è collegato alla rete WPS.

Passaggio 1. Accedere all'utility di configurazione Web e scegliere Wireless > Impostazioni di base. Viene visualizzata la pagina Impostazioni di base:

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	Guest Network	VLAN	Wireless Isolation with SSID	WMM	WPS
☐	☒ ON	ciscosb1	☒	WPA2-Personal Mixed	Disabled	☐	1	☐	☒	☒
☐	☐ OFF	ciscosb2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb4	☐	Disabled	Disabled	☐	1	☐	☒	☐

Edit Edit Security Mode Edit MAC Filtering Time of Day Access Edit Guest Net **Edit WPS**

Save Cancel

Passaggio 2. Fare clic su Modifica WPS per configurare WPS. Viene visualizzata la pagina WPS:

Nota: È possibile accedere alla pagina WPS anche tramite Wireless > WPS.

WPS

Wi-Fi Protected Setup™

WPS: ciscosb1

Use one of the following for each Wi-Fi Protected Setup supported device:

1. If your client device has a Wi-Fi Protected Setup button, click or press that button and then click the button on the right.



OR

2. If your client device has a Wi-Fi protected Setup PIN number, enter that number here and then click

OR

3. If your client asks for the Router's PIN number, enter Device PIN below in your client device.

Device PIN Status: Active

Device PIN:

PIN Lifetime:

Wi-Fi Protected Setup Status: Configured

Network Name (SSID): ciscosb1

Security: WPA2-Personal

Passaggio 3. Fare clic su Modifica per scegliere la rete wireless in cui abilitare WPS.

WPS

Wi-Fi Protected Setup™

WPS: ciscosb1

Use one of the following for each Wi-Fi Protected Setup supported device:

1. If your client device has a Wi-Fi Protected Setup button, click or press that button and then click the button on the right.



OR

2. If your client device has a Wi-Fi protected Setup PIN number, enter that number here 19582493 and then click

OR

3. If your client asks for the Router's PIN number, enter Device PIN below in your client device.

Device PIN Status: Active

Device PIN: 47083578

PIN Lifetime: 4 Hours ▼

Wi-Fi Protected Setup Status: Configured

Network Name (SSID): ciscosb1

Security: WPA2-Personal

Passaggio 4. Fare clic sul pulsante WPS nella pagina WPS.

Passaggio 5. Per connettere il dispositivo client alla rete WPS, fare clic sul pulsante WPS nel dispositivo client o in una schermata di utilità del dispositivo client.

Nei campi seguenti vengono visualizzate le informazioni relative alla configurazione di WPS.

- Stato Wi-Fi Protected Setup - Stato della configurazione WPS.
- Nome di rete (SSID) - Nome di rete assegnato alla configurazione WPS dalla RV215W.
- WPA2-Personale — il tipo di protezione utilizzato dalla configurazione WPS.

Configura metodo 2 WPS

Wi-Fi Protected Setup (WPS) è una funzione che consente di configurare una rete wireless in modo semplice e sicuro. Per connettersi a WPS, il dispositivo di connessione deve supportare WPS e deve essere compatibile con la protezione WPA. Il secondo metodo richiede il numero PIN del dispositivo client. Una volta immesso il PIN nella pagina WPS, il dispositivo client si connette alla rete WPS.

Passaggio 1. Accedere all'utility di configurazione Web e scegliere Wireless > Impostazioni di base. Viene visualizzata la pagina Impostazioni di base:

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	Guest Network	VLAN	Wireless Isolation with SSID	WMM	WPS
☐	☒ ON	ciscosb1	☒	WPA2-Personal Mixed	Disabled	☐	1	☐	☒	☒
☐	☐ OFF	ciscosb2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb4	☐	Disabled	Disabled	☐	1	☐	☒	☐

Edit Edit Security Mode Edit MAC Filtering Time of Day Access Edit Guest Net **Edit WPS**

Save Cancel

Passaggio 2. Fare clic su Modifica WPS per configurare WPS. Viene visualizzata la pagina WPS:

Nota: È possibile accedere alla pagina WPS anche tramite Wireless > WPS.

WPS

Wi-Fi Protected Setup™

WPS: ciscosb1

Use one of the following for each Wi-Fi Protected Setup supported device:

1. If your client device has a Wi-Fi Protected Setup button, click or press that button and then click the button on the right.



OR

2. If your client device has a Wi-Fi protected Setup PIN number, enter that number here and then click

OR

3. If your client asks for the Router's PIN number, enter Device PIN below in your client device.

Device PIN Status: Active

Device PIN:

PIN Lifetime:

Wi-Fi Protected Setup Status: Configured

Network Name (SSID): ciscosb1

Security: WPA2-Personal

Passaggio 3. Fare clic su Modifica per scegliere la rete wireless in cui attivare WPS.

Passaggio 4. Immettere il numero PIN del dispositivo client.

Passaggio 5. Fare clic su Registra per creare la rete WPS.

Nei campi seguenti vengono visualizzate le informazioni relative alla configurazione di WPS.

- Stato Wi-Fi Protected Setup - Stato della configurazione WPS.
- Nome di rete (SSID) - Nome di rete assegnato alla configurazione WPS dalla RV215W.
- WPA2-Personale — il tipo di protezione utilizzato dalla configurazione WPS.

Configura metodo WPS 3

Wi-Fi Protected Setup (WPS) è una funzione che consente di configurare una rete wireless in modo semplice e sicuro. Per connettersi a WPS, il dispositivo di connessione deve supportare WPS e deve essere compatibile con la protezione WPA. Il terzo metodo richiede all'utente di immettere il numero PIN della RV215W nella pagina di configurazione WPS del dispositivo client.

Passaggio 1. Accedere all'utilità di configurazione Web e scegliere Wireless > Impostazioni di base. Viene visualizzata la pagina Impostazioni di base:

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

	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	Guest Network	VLAN	Wireless Isolation with SSID	WMM	WPS
☐	☒ ON	ciscosb1	☒	WPA2-Personal Mixed	Disabled	☐	1	☐	☒	☒
☐	☐ OFF	ciscosb2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb4	☐	Disabled	Disabled	☐	1	☐	☒	☐

Edit Edit Security Mode Edit MAC Filtering Time of Day Access Edit Guest Net **Edit WPS**

Save Cancel

Passaggio 2. Fare clic su Modifica WPS per configurare WPS. Viene visualizzata la pagina WPS:

Nota: È possibile accedere alla pagina WPS anche tramite Wireless > WPS.

WPS

Wi-Fi Protected Setup™

WPS: ciscosb1

Use one of the following for each Wi-Fi Protected Setup supported device:

1. If your client device has a Wi-Fi Protected Setup button, click or press that button and then click the button on the right.



OR

2. If your client device has a Wi-Fi protected Setup PIN number, enter that number here 19582493 and then click

OR

3. If your client asks for the Router's PIN number, enter Device PIN below in your client device.

Device PIN Status: Active

Device PIN: 47083578

PIN Lifetime: 4 Hours ▼

Wi-Fi Protected Setup Status: Configured

Network Name (SSID): ciscosb1

Security: WPA2-Personal

Passaggio 3. Fare clic su Modifica per scegliere la rete wireless in cui attivare WPS.

Passaggio 4. Fare clic su Genera per generare un numero PIN per RV215W.

Passaggio 5. Dall'elenco a discesa Durata PIN scegliere il periodo di tempo che deve trascorrere prima che venga generato un nuovo PIN.

Passaggio 6. Immettere il numero PIN RV215W specificato nella configurazione del dispositivo client. Il dispositivo client si connette alla rete WPS.

Nei campi seguenti vengono visualizzate le informazioni relative alla configurazione di WPS.

- Stato Wi-Fi Protected Setup - Stato della configurazione WPS.

- Nome di rete (SSID) - Nome di rete assegnato alla configurazione WPS dalla RV215W.
- WPA2-Personale — il tipo di protezione utilizzato dalla configurazione WPS.

Per tutta la documentazione sul router RV215W, fare clic [qui](#).

Qui è disponibile un video relativo a questo articolo...

[Fare clic qui per visualizzare altre Tech Talks di Cisco](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).