

# Impostazioni wireless di base sul router VPN CVR100W

## Obiettivo

Una rete WLAN (Wireless Local Area Network) utilizza la comunicazione radio per connettere le periferiche wireless a una rete LAN. Un esempio è un hotspot Wi-Fi in un bar. Le reti wireless sono utili in quanto riducono i costi di cablaggio ed è facile da configurare.

Questo articolo spiega come configurare le impostazioni wireless di base sul router VPN CVR100W, compresa la configurazione della sicurezza di rete. Per le impostazioni wireless avanzate, fare riferimento all'articolo [Configurazione wireless avanzata sul router VPN CVR100W](#).

## Dispositivo applicabile

·CVR100W VPN Router

## Versione del software

•1.0.1.19

## Configurazione 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

Wi-Fi Power: 100%

Wireless Network Mode: B/G/N-Mixed

Wireless Band Selection:  20MHz  20/40MHz

Wireless Channel: Auto

AP Management VLAN: 1

U-APSD (WMM Power Save):  Enable

<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID2	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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

Save Cancel

Passaggio 2. Selezionare la casella di controllo **Attiva** nel campo Radio per attivare la radio wireless.

Passaggio 3. Dall'elenco a discesa Wi-Fi Power (Alimentazione Wi-Fi), scegliere

l'alimentazione Wi-Fi. Questa alimentazione wi-fi controlla la potenza del trasmettitore della radio wi-fi. Questa funzione è utile per ridurre o aumentare la gamma del segnale. Questa funzione consente di risparmiare energia.

- 100%: questa opzione consente di attivare la potenza 100% dei trasmettitori radio.

- 50%: questa opzione consente il 50% della potenza del trasmettitore radio.

Passaggio 4. Dall'elenco a discesa Modalità di rete wireless, scegliere la modalità wireless. Questa opzione è basata sulle funzionalità wireless dei dispositivi nella rete.

- B/G/N-Mixed: la rete è costituita da una combinazione di dispositivi wireless-B, wireless-G e wireless-N.

- Solo B: la rete è costituita solo da dispositivi wireless-B.

- G-Only: la rete è costituita esclusivamente da dispositivi wireless-G.

- Solo N: la rete è costituita esclusivamente da dispositivi wireless-N.

- B/G-Mixed: la rete è costituita da una combinazione di dispositivi wireless-B e wireless-G.

- G/N Misto: la rete è costituita da una combinazione di dispositivi wireless-G e wireless-N.

Passaggio 5. Se la modalità di rete è costituita da periferiche Wireless-N, fare clic sul pulsante di opzione corrispondente alla larghezza di banda desiderata del segnale wireless nel campo Selezione banda wireless. Maggiore è la larghezza di banda, maggiore è la quantità di dati che il segnale può trasportare.

- 20 MHz: 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 una maggiore larghezza di banda ma è suscettibile a maggiori interferenze. Questa opzione viene utilizzata solo se le periferiche wireless collegate sono compatibili con la frequenza di 40 MHz.

Passaggio 6. Dall'elenco a discesa Canale wireless, scegliere un canale wireless per la radio. Scegliere un canale attualmente non utilizzato dalle reti adiacenti. Se più radio utilizzano lo stesso canale, è possibile che si verifichino interferenze.

Passaggio 7. Dall'elenco a discesa VLAN di gestione dell'access point, scegliere la VLAN di gestione. La VLAN di gestione è la VLAN utilizzata per la gestione dei dispositivi da una postazione remota.

Passaggio 8. (Facoltativo) Per abilitare il risparmio di energia automatico non pianificato (U-APSD), selezionare **Abilita** nel campo 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 9. Fare clic su **Salva**.

## Modifica tabella wireless

Passaggio 1. Selezionare la casella di controllo della rete che si desidera modificare nella tabella Wireless.

Wireless Table											
<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID2	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Passaggio 2. Fare clic su **Modifica** per modificare la rete specificata.

Passaggio 3. Selezionare la casella di controllo **Abilita SSID** per abilitare la rete. SSID (Service Set Identifier) è il nome della rete wireless.

Passaggio 4. Nel campo Nome SSID, immettere il nome della rete. Tutti i dispositivi della rete utilizzano questo SSID per comunicare tra loro.

Passaggio 5. Selezionare la casella di controllo **Trasmissione SSID** per abilitare la trasmissione wireless. Quando la trasmissione SSID è abilitata, la disponibilità del router VPN CVR100W viene annunciata ai dispositivi wireless nelle vicinanze.

Passaggio 6. (Facoltativo) Per modificare la modalità di protezione, fare riferimento a [Modifica modalità di protezione](#).

Passaggio 7. (Facoltativo) Per modificare il filtro MAC, consultare il documento sulla [modifica del filtro MAC](#).

Passaggio 8. (Facoltativo) Per abilitare Cisco Simple Connect (CSC), selezionare la casella di controllo **CSC**. CSC consente di configurare in modo semplice una rete wireless e di connettere facilmente le periferiche wireless alla rete. Il dispositivo wireless utilizza CSC per ottenere l'SSID e la password della rete, che consentono la connessione automatica alla rete. Per modificare CSC, fare riferimento a [Modifica CSC](#).

**Nota:** La VLAN di Cisco Simple Connect non può essere la stessa della VLAN corrente o di un altro SSID.

Passaggio 9. Dall'elenco a discesa VLAN, selezionare la VLAN associata alla rete.

Passaggio 10. Selezionare la casella di controllo **Isolamento SSID** per impedire la comunicazione tra le periferiche della rete specificata.

Passaggio 11. Selezionare **WMM** per abilitare Wi-Fi Multimedia (WMM) sulla rete. WMM viene utilizzato per migliorare lo streaming di contenuti multimediali su dispositivi wireless. Il traffico multimediale inviato tramite una connessione wireless quando WMM è attivato ha una priorità più alta.

Passaggio 12. 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.

**Nota:** Per configurare WPS sul router VPN CVR100W, fare riferimento all'articolo [WiFi Protected Setup \(WPS\) sul router VPN CVR100W](#).

Passaggio 13. Fare clic su **Salva**.

## Modifica modalità di protezione

Passaggio 1. Selezionare la casella di controllo della rete che si desidera modificare nella tabella Wireless.

Wireless Table										
<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID2	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Buttons: Edit, **Edit Security Mode**, Edit MAC Filtering, Time of Day Access, Edit Guest Net, Edit CSC, Edit WPS

Passaggio 2. Fare clic su **Modifica modalità di protezione** per modificare la protezione della rete specificata. Verrà visualizzata la pagina *Impostazioni protezione*.

### Security Settings

Select SSID: Cisco-4D61

Security Mode: **WPA2-Personal** (dropdown menu open showing: Disabled, **WEP**, WPA-Personal, WPA-Enterprise, WPA2-Personal, WPA2-Personal Mixed, WPA2-Enterprise, WPA2-Enterprise Mixed)

Encryption: [Color indicator] Very Strong

Security Key: [Input field]

Show Password: [Input field]

Key Renewal: [Input field] (Range: 600 - 7200, Default: 3600)

Buttons: Save, Cancel, Back

Passaggio 3. (Facoltativo) Per modificare il SSID per cui si desidera configurare la sicurezza, scegliere il SSID desiderato dall'elenco a discesa Seleziona SSID.

Passaggio 4. Dall'elenco a discesa Modalità di protezione scegliere la modalità di protezione da configurare.

·[Disabilita sicurezza](#) - Questa opzione disabilita la sicurezza sul router VPN CVR100W.

·[WEP Security](#) — Wired Equivalent Privacy (WEP) è un algoritmo utilizzato per proteggere una rete wireless. WEP viene utilizzato per fornire un metodo di crittografia di base meno sicuro di WPA. WEP viene utilizzato quando i dispositivi di rete collegati non supportano WPA.

·[WPA-Personal Security](#) — Wi-Fi Protected Access (WPA) è uno standard di sicurezza per le reti wireless. WPA-Personale è una versione di WPA utilizzata per reti costituite da pochi utenti. WPA-Personale fornisce una chiave condivisa che ogni utente utilizza 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).

·[WPA-Enterprise Security](#) — WPA-Enterprise è una versione di WPA consigliata per una rete composta da numerosi utenti. L'autenticazione per accedere alla rete è controllata da un server RADIUS. A ogni utente connesso viene 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).

·[WPA2-Personal Security](#): WPA2 è un miglioramento di WPA e offre una maggiore protezione rispetto a WPA. WPA2-Personale è una versione di WPA2 utilizzata per reti con pochi utenti. WPA2-Personale è più sicuro di WPA2-Personale misto. WPA2-Personale fornisce una chiave condivisa che ogni utente utilizza per accedere alla rete wireless.

·[WPA2-Personal Mixed Security](#) — WPA2-Personal Mixed è una versione di WPA2 utilizzata per reti con pochi utenti. WPA2-Personal Mixed supporta la compatibilità con le versioni precedenti per i dispositivi meno recenti che non possono utilizzare WPA2. WPA2-Personal Mixed è una connessione meno sicura.

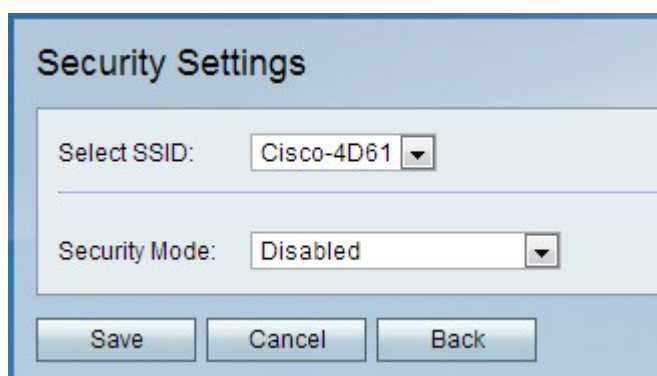
·[WPA2-Enterprise Security](#) — WPA2-Enterprise è una versione di WPA2 utilizzata per reti con numerosi utenti. WPA2-Enterprise è più sicuro di WPA2-Enterprise Mixed. L'autenticazione utilizzata per ottenere l'accesso è controllata da un server RADIUS. Ciò significa che a ogni utente connesso verrà assegnata una chiave univoca per accedere alla rete wireless.

·[WPA2-Enterprise Mixed Security](#) — WPA2-Enterprise Mixed è una versione di WPA2 utilizzata per reti con numerosi utenti. WPA2-Enterprise Mixed supporta la compatibilità con le versioni precedenti per i dispositivi meno recenti che non possono utilizzare WPA2. WPA2-Enterprise Mixed offre una connessione meno sicura rispetto a WPA2-Enterprise. 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.

## Disabilita protezione

La protezione wireless può essere disabilitata sul router VPN CVR100W per una maggiore facilità d'uso durante la configurazione delle reti di prova.

**Nota:** La disattivazione della protezione non è consigliata.



The screenshot shows a 'Security Settings' window. It has a title bar and a light blue background. Inside, there are two dropdown menus. The first is labeled 'Select SSID:' and has 'Cisco-4D61' selected. The second is labeled 'Security Mode:' and has 'Disabled' selected. At the bottom, there are three buttons: 'Save', 'Cancel', and 'Back'.

Passaggio 1. Dall'elenco a discesa Modalità di sicurezza scegliere **Disabilitato**. La protezione è disattivata per la rete wireless.

Passaggio 2. Fare clic su **Salva**.

## Configurare la protezione WEP

Passaggio 1. Dall'elenco a discesa Modalità di protezione scegliere **WEP**.

Passaggio 2. Dall'elenco a discesa Tipo di autenticazione scegliere un tipo di autenticazione per la rete wireless.

- Sistema aperto: qualsiasi dispositivo di rete può essere associato al punto di accesso, ma la chiave WEP è necessaria per far passare il traffico attraverso il punto di accesso.

- Chiave condivisa: è necessaria una chiave WEP per l'associazione al punto di accesso. Viene anche usato per far passare il traffico attraverso il punto di accesso.

Passaggio 3. 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 opzione è più sicura.

Passaggio 4. Nel campo Passphrase, immettere una passphrase più lunga di otto caratteri. La passphrase è utile per ricordare con maggiore facilità le impostazioni di protezione di rete.

Passaggio 5. 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,

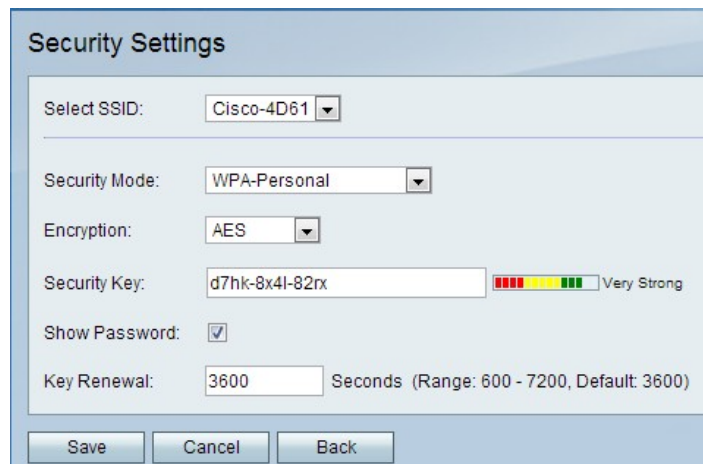
Chiave 3 e Chiave 4.

Passaggio 6. Dall'elenco a discesa TX Key (Chiave TX), selezionare la Chiave che gli utenti devono immettere per accedere alla rete wireless.

Passaggio 7. (Facoltativo) Selezionare la casella di controllo **Show Password** per visualizzare le stringhe di caratteri dei tasti.

Passaggio 8. Fare clic su **Salva**.

## Configura protezione WPA-Personale



The screenshot shows a 'Security Settings' window with the following fields and options:

- Select SSID: Cisco-4D61
- Security Mode: WPA-Personal
- Encryption: AES
- Security Key: d7hk-8x4l-82rx (with a strength indicator showing 'Very Strong')
- Show Password:
- Key Renewal: 3600 Seconds (Range: 600 - 7200, Default: 3600)

Buttons at the bottom: Save, Cancel, Back.

Passaggio 1. Dall'elenco a discesa Modalità di protezione scegliere **WPA-Personale**.

Passaggio 2. Dall'elenco a discesa Crittografia scegliere un metodo di crittografia per la chiave WPA.

·TKIP/AES: questa opzione viene scelta quando i dispositivi connessi alla rete wireless non supportano tutti AES.

·AES: questa opzione è preferibile se tutti i dispositivi collegati alla rete wireless supportano AES.

Passaggio 3. Immettere una chiave di sicurezza nel campo Chiave di sicurezza. La chiave di protezione è una passphrase costituita da lettere e cifre. I dispositivi utilizzano la chiave di protezione per connettersi alla rete.

Passaggio 4. (Facoltativo) Per visualizzare la stringa di caratteri del tasto, selezionare la casella di controllo **Mostra password**.

Passaggio 5. Nel campo Rinnovo chiave, immettere il tempo in secondi impiegato dal router VPN CVR100W per generare una nuova chiave.

Passaggio 6. Fare clic su **Salva**.

## Configura protezione WPA-Enterprise

Passaggio 1. Dall'elenco a discesa Modalità di protezione scegliere **WPA-Enterprise**.

Passaggio 2. Dall'elenco a discesa Crittografia scegliere un metodo di crittografia per la chiave WPA.

·TKIP/AES: questa opzione viene scelta quando i dispositivi connessi alla rete wireless non supportano tutti AES.

·AES: questa opzione è preferibile se tutti i dispositivi collegati alla rete wireless supportano AES.

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

Passaggio 4. Nel campo Porta RADIUS, immettere il numero di porta utilizzato per accedere al server RADIUS.

Passaggio 5. Nel campo Chiave condivisa, immettere la chiave già condivisa per gli utenti wireless. Una chiave già condivisa è una chiave utilizzata da tutti gli utenti. La funzionalità della chiave già condivisa è una funzionalità di protezione aggiuntiva.

Passaggio 6. Nel campo Rinnovo chiave, immettere il tempo in secondi impiegato dal router VPN CVR100W per generare una nuova chiave.

Passaggio 7. Fare clic su **Salva**.

## Configurazione della protezione mista WPA2-Personale/WPA2-Personale



Security Settings

Select SSID: Cisco-4D61

Security Mode: WPA2-Personal Mixed

Encryption: TKIP + AES

Security Key: d7hk-8x4l-82rx ■■■■ ■■ Very Strong

Show Password:

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

Save Cancel Back

Passaggio 1. Dall'elenco a discesa Modalità di protezione scegliere **WPA2-Personale** o **WPA2-Personale misto**.

**Nota:** WPA2-Personal viene utilizzato quando tutti i dispositivi della rete wireless supportano AES. WPA2-Personal Mixed viene utilizzato quando i dispositivi della rete non supportano tutti l'AES. Il tipo di crittografia utilizzato dal metodo di protezione viene visualizzato nel campo Crittografia.

Passaggio 2. Nel campo Chiave di sicurezza, immettere una chiave di sicurezza. La chiave di protezione è una passphrase costituita da lettere e cifre. I dispositivi utilizzano la chiave di protezione per connettersi alla rete.

Passaggio 3. (Facoltativo) Per visualizzare le stringhe di caratteri della chiave, selezionare la casella di controllo **Mostra password**.

Passaggio 4. Nel campo Rinnovo chiave, immettere il tempo in secondi corrispondente al tempo in cui il router VPN CVR100W utilizza la chiave prima di generarne una nuova.

Passaggio 5. Fare clic su **Salva**.

## Configurazione della protezione mista WPA2-Enterprise/WPA2-Enterprise

**Security Settings**

Select SSID: Cisco-4D61

Security Mode: WPA2-Enterprise Mixed

Encryption: TKIP + AES

RADIUS Server: 192 . 168 . 1 . 220 (Hint: 192.168.1.200)

RADIUS Port: 1812 (Range: 1 - 65535, Default: 1812)

Shared Key: Sharedkey1

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

Save Cancel Back

Passaggio 1. Dall'elenco a discesa Modalità di protezione scegliere **WPA2-Enterprise** o **WPA2-Enterprise Mixed**.

**Nota:** WPA2-Enterprise viene utilizzato quando tutti i dispositivi della rete wireless supportano AES. WPA2-Enterprise Mixed viene utilizzato quando i dispositivi della rete non supportano tutti AES. Il tipo di crittografia utilizzato dal metodo di protezione viene visualizzato nel campo Crittografia.

Passaggio 2. Nel campo Server RADIUS, immettere l'indirizzo IP del server RADIUS.

Passaggio 3. Nel campo Porta RADIUS, immettere il numero di porta utilizzato per accedere al server RADIUS.

Passaggio 4. Nel campo Chiave condivisa, immettere la chiave già condivisa per gli utenti wireless. Una chiave già condivisa è una chiave utilizzata da tutti gli utenti. La funzionalità della chiave già condivisa è una funzionalità di protezione aggiuntiva.

Passaggio 5. Nel campo Rinnovo chiave, immettere il tempo in secondi impiegato dal router VPN CVR100W per generare una nuova chiave.

Passaggio 6. Fare clic su **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.

**Basic Settings**

Radio:  Enable

Wi-Fi Power: 100%

Wireless Network Mode: B/G/N-Mixed

Wireless Band Selection:  20MHz  20/40MHz

Wireless Channel: Auto

AP Management VLAN: 1

U-APSD (WMM Power Save):  Enable

<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID2	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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

Save Cancel

Passaggio 1. Selezionare la casella di controllo della rete che si desidera modificare.

Passaggio 2. 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 Filtering**

SSID Name: Cisco-4D61

Wireless MAC Filtering:  Enable

**Connection Control**

Prevent PCs listed below from accessing the wireless network.

Permit PCs listed below to access the wireless network.

Show Client List

MAC Address Table					
01	1A:2B:3C:4D:5E:6F	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 3. Selezionare **Enable** per abilitare il filtro MAC sulla rete.

Passaggio 4. Fare clic sul pulsante di opzione corrispondente al tipo di elenco desiderato nel campo Controllo connessione.

- Impedisci l'accesso alla rete ai PC con gli indirizzi MAC elencati.
- Permit PC — Consente ai PC con gli indirizzi MAC elencati di accedere alla rete.

Passaggio 5. Nella tabella degli indirizzi MAC, immettere gli indirizzi MAC desiderati.

Passaggio 6. Fare clic su **Salva**.

## Accesso ora

La funzionalità di accesso ora del giorno viene utilizzata per consentire l'accesso agli utenti

in base a una pianificazione configurata.

Wireless Table										
<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID2	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Buttons: Edit, Edit Security Mode, Edit MAC Filtering, **Time of Day Access**, Edit Guest Net, Edit CSC, Edit WPS

Passaggio 1. Selezionare la casella di controllo della rete che si desidera modificare.

Passaggio 2. 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: 03 Hours 0 Minutes AM

Stop Time: 12 Hours 0 Minutes AM

Buttons: Save, Cancel, Back

Passaggio 3. Selezionare **Abilita** nel campo Orario attivo per abilitare l'accesso all'ora del giorno per la rete.

Passaggio 4. Nel campo Ora di inizio, inserire l'ora in cui ha inizio l'accesso alla rete.

Passaggio 5. Nel campo Ora di arresto, immettere l'ora in cui termina l'accesso alla rete.

Passaggio 6. Fare clic su **Salva**.

## Modifica rete guest

Una rete guest è una sezione di una rete progettata per utenti temporanei. Questa funzione consente agli utenti guest di accedere alla 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.

**Basic Settings**

Radio:  Enable

Wi-Fi Power: 100%

Wireless Network Mode: B/G/N-Mixed

Wireless Band Selection:  20MHz  20/40MHz

Wireless Channel: Auto

AP Management VLAN: 1

U-APSD (WMM Power Save):  Enable

<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID2	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Passaggio 1. 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

Guest Password:

Hide Password:

Lease Time: 120 Minutes

Total Guest Allowed: 5

Passaggio 2. Nel campo Password guest, immettere una password che gli utenti utilizzeranno per accedere alla rete guest.

Passaggio 3. (Facoltativo) Per nascondere la password nella pagina, selezionare la casella di controllo nel campo Nascondi password.

Passaggio 4. Nel campo Durata lease, immettere il tempo in minuti durante il quale gli utenti possono rimanere connessi alla rete guest.

Passaggio 5. Dall'elenco a discesa Totale ospiti consentiti, scegliere il numero totale di ospiti consentiti.

Passaggio 6. Fare clic su **Salva**.

## Modifica CSC

CSC consente di configurare in modo semplice una rete wireless e di connettere facilmente le periferiche wireless alla rete. Il dispositivo wireless utilizza CSC per ottenere l'SSID e la

password della rete, che consentono la connessione automatica alla rete.

Wireless Table										
<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-1	<input checked="" type="checkbox"/>	Disabled	Disabled	<input checked="" type="checkbox"/>	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Buttons: Edit, Edit Security Mode, Edit MAC Filtering, Time of Day Access, Edit Guest Net, **Edit CSC**, Edit WPS

Passaggio 1. Selezionare la casella di controllo della rete che si desidera modificare.

Passaggio 2. Fare clic su **Edit CSC** per modificare Cisco Simple Connect.

Passaggio 3. Selezionare la casella di controllo CSC.

Passaggio 4. Dall'elenco a discesa VLAN, selezionare la VLAN da usare per CSC.

**Nota:** La VLAN Cisco Simple Connect non può essere la stessa della VLAN SSID corrente o di un'altra VLAN SSID. Per creare una nuova VLAN, fare riferimento all'articolo [Appartenenza della VLAN sul router CVR100W](#).

**Nota:** CSC può avere effetto solo su WDS (Wireless Distribution System) su SSID1. Fare riferimento all'articolo [WDS \(Wireless Distribution System\) sul router CVR100W](#).

Passaggio 5. Fare clic su **Salva**.