

Grundlegende Wireless-Einstellungen des CVR100W VPN-Routers

Ziel

Ein Wireless Local Area Network (WLAN) verwendet Funkverbindungen, um Wireless-Geräte mit einem LAN zu verbinden. Ein Beispiel ist ein Wi-Fi-Hotspot in einem Café. Wireless-Netzwerke sind nützlich, da sie die Verkabelungskosten senken und leicht einzurichten sind.

In diesem Artikel wird erläutert, wie Sie die grundlegenden Wireless-Einstellungen auf dem CVR100W VPN-Router konfigurieren. Dazu gehört auch die Konfiguration der Netzwerksicherheit. Erweiterte Wireless-Einstellungen finden Sie im Artikel [Erweiterte Wireless-Konfiguration auf dem CVR100W VPN-Router](#).

Anwendbares Gerät

·CVR100W VPN-Router

Softwareversion

·1.0.1.19

Grundlegende Konfigurationskonfiguration

Allgemeine Einstellungen

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Wireless > Basic Settings (Wireless > Grundeinstellungen)**. Die Seite *Grundeinstellungen* wird geöffnet:

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

	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
☒	☒	Cisco-4D61	☒	WPA2-Personal	Disabled	☐	1	☐	☒	☒
☐	☐	cisco-SSID2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐	cisco-SSID3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐	cisco-guest	☒	Disabled	Disabled	☐	3	☒	☒	☐

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

Save Cancel

Schritt 2: Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld Radio (Funkübertragung), um die Wireless-Funkübertragung zu aktivieren.

Schritt 3: Wählen Sie aus der Dropdown-Liste Wi-Fi Power (Wi-Fi-Stromversorgung) die Wi-Fi-Stromversorgung aus. Diese Wi-Fi-Stromversorgung steuert die Transmitterleistung des Wi-Fi-Radios. Diese Funktion ist nützlich, um den Signalbereich zu reduzieren oder zu vergrößern. Diese Funktion dient der Energieeinsparung.

- 100 % - Diese Option ermöglicht 100 % Radio Transmitter-Leistung.
- 50 % - Diese Option ermöglicht die Stromversorgung von 50 % Funksendern.

Schritt 4: Wählen Sie aus der Dropdown-Liste Wireless Network Mode (Wireless-Netzwerkmodus) den Wireless-Modus aus. Diese Option basiert auf den Wireless-Funktionen der Geräte im Netzwerk.

- B/G/N-Mixed (Gemischt B/G/N): Das Netzwerk besteht aus einer Kombination aus Wireless-B-, Wireless-G- und Wireless-N-Geräten.
- B-Only (Nur B): Das Netzwerk besteht nur aus Wireless-B-Geräten.
- G-Only (Nur G): Das Netzwerk besteht nur aus Wireless-G-Geräten.
- N-Only (Nur N): Das Netzwerk besteht nur aus Wireless-N-Geräten.
- B/G-Mixed - Das Netzwerk besteht aus einer Kombination aus Wireless-B- und Wireless-G-Geräten.
- G/N Mixed (Gemischt): Das Netzwerk besteht aus einer Kombination aus Wireless-G- und Wireless-N-Geräten.

Schritt 5: Wenn der Netzwerkmodus aus Wireless-N-Geräten besteht, klicken Sie im Feld Wireless Band Selection (Wireless-Frequenzauswahl) auf das Optionsfeld, das der gewünschten Bandbreite des Wireless-Signals entspricht. Die höhere Bandbreite weist auf die größere Datenmenge hin, die das Signal übertragen kann.

- 20 MHz - Die Standardfrequenz für ein Wireless-Signal.
- 20/40 MHz — Verwendet automatisch ein 20-MHz- und 40-MHz-Signal. Ein 40-MHz-Signal bietet mehr Bandbreite, ist aber anfällig für weitere Interferenzen. Diese Option wird nur verwendet, wenn die angeschlossenen Wireless-Geräte mit einer 40-MHz-Frequenz kompatibel sind.

Schritt 6: Wählen Sie aus der Dropdown-Liste Wireless Channel (Wireless-Kanal) einen Wireless-Kanal für die Funkübertragung aus. Wählen Sie einen Kanal aus, der derzeit nicht von Nachbarnetzwerken verwendet wird. Wenn mehrere Funkmodule denselben Kanal verwenden, kann es zu Störungen kommen.

Schritt 7: Wählen Sie aus der Dropdown-Liste AP Management VLAN (AP-Management-VLAN) das Management-VLAN aus. Das Management-VLAN ist das VLAN für die Verwaltung von Geräten von einem Remote-Standort aus.

Schritt 8: (Optional) Aktivieren Sie im Feld U-APSD die Option **Enable** (Aktivieren), um die ungeplante automatische Stromspeicherung (U-APSD) zu aktivieren. U-APSD ist eine Funktion, mit der die Funkeinheit Strom sparen kann. U-APSD kann jedoch die Durchsatzleistung der Funkeinheit verringern.

Schritt 9: Klicken Sie auf **Speichern**.

Wireless-Tabelle bearbeiten

Schritt 1: Aktivieren Sie in der Wireless-Tabelle das Kontrollkästchen des Netzwerks, das Sie bearbeiten möchten.

Wireless Table											
☐	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS	
☒	☒	Cisco-4D61	☒	WPA2-Personal	Disabled	☐	1	☐	☒	☒	
☐	☐	cisco-SSID2	☐	Disabled	Disabled	☐	1	☐	☒	☐	
☐	☐	cisco-SSID3	☐	Disabled	Disabled	☐	1	☐	☒	☐	
☐	☐	cisco-guest	☒	Disabled	Disabled	☐	3	☒	☒	☐	
<input checked="" type="button" value="Edit"/> Edit Security Mode Edit MAC Filtering Time of Day Access Edit Guest Net Edit CSC Edit WPS											

Schritt 2: Klicken Sie auf **Bearbeiten**, um das angegebene Netzwerk zu bearbeiten.

Schritt 3: Aktivieren Sie das Kontrollkästchen **SSID aktivieren**, um das Netzwerk zu aktivieren. Service Set Identifier (SSID) ist der Name des Wireless-Netzwerks.

Schritt 4: Geben Sie im Feld SSID Name (SSID-Name) den Namen des Netzwerks ein. Alle Geräte im Netzwerk verwenden diese SSID, um miteinander zu kommunizieren.

Schritt 5: Aktivieren Sie das Kontrollkästchen **SSID Broadcast**, um Wireless Broadcast zu aktivieren. Wenn SSID-Broadcast aktiviert ist, wird die Verfügbarkeit des CVR100W VPN-Routers an Wireless-Geräte in der Nähe angekündigt.

Schritt 6: (Optional) Informationen zum Bearbeiten des Sicherheitsmodus finden Sie unter [Sicherheitsmodus bearbeiten](#).

Schritt 7: (Optional) Informationen zum Bearbeiten des MAC-Filters finden Sie unter [MAC-Filterung bearbeiten](#).

Schritt 8: (Optional) Um Cisco Simple Connect (CSC) zu aktivieren, aktivieren Sie das Kontrollkästchen **CSC**. CSC ermöglicht die einfache Einrichtung eines Wireless-Netzwerks und die einfache Verbindung von Wireless-Geräten mit dem Netzwerk. Das Wireless-Gerät verwendet CSC, um die SSID und das Kennwort des Netzwerks abzurufen, wodurch eine automatische Verbindung zum Netzwerk möglich wird. Informationen zum Bearbeiten des CSC finden Sie unter [CSC bearbeiten](#).

Hinweis: Das VLAN von Cisco Simple Connect kann nicht mit dem aktuellen oder anderen VLANs der SSID identisch sein.

Schritt 9: Wählen Sie aus der VLAN-Dropdown-Liste das VLAN aus, das dem Netzwerk zugeordnet ist.

Schritt 10: Aktivieren Sie das Kontrollkästchen **SSID-Isolierung**, um zu verhindern, dass Geräte im angegebenen Netzwerk miteinander kommunizieren.

Schritt 11: Aktivieren Sie **WMM**, um Wi-Fi Multimedia (WMM) im Netzwerk zu aktivieren. WMM wird verwendet, um das Streaming von Multimedia-Inhalten über Wireless-Geräte zu verbessern. Multimedia-Datenverkehr, der über eine Wireless-Verbindung gesendet wird, wenn WMM aktiviert ist, erhält eine höhere Priorität.

Schritt 12: Aktivieren Sie **WPS**, um das angegebene Netzwerk als WPS-Netzwerk (Wi-Fi Protected Setup) zuzuweisen. WPS ist eine Funktion, die eine einfache und sichere Netzwerkkonfiguration ermöglicht. Mit dieser Funktion können Geräte problemlos eine Verbindung zum Netzwerk herstellen.

Hinweis: Informationen zur Konfiguration von WPS auf dem CVR100W VPN-Router finden Sie im Artikel [WiFi Protected Setup \(WPS\) auf dem CVR100W VPN-Router](#).

Schritt 13: Klicken Sie auf **Speichern**.

Sicherheitsmodus bearbeiten

Schritt 1: Aktivieren Sie in der Wireless-Tabelle das Kontrollkästchen des Netzwerks, das Sie bearbeiten möchten.

Wireless Table										
☐	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
☒	☒	Cisco-4D61	☒	WPA2-Personal	Disabled	☐	1	☐	☒	☒
☐	☐	cisco-SSID2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐	cisco-SSID3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐	cisco-guest	☒	Disabled	Disabled	☐	3	☒	☒	☐
Edit Edit Security Mode Edit MAC Filtering Time of Day Access Edit Guest Net Edit CSC Edit WPS										

Schritt 2: Klicken Sie auf **Sicherheitsmodus bearbeiten**, um die Sicherheit des angegebenen Netzwerks zu bearbeiten. Die Seite *Sicherheitseinstellungen* wird geöffnet.

Security Settings

Select SSID: Cisco-4D61

Security Mode: WPA2-Personal

Disabled

WEP

WPA-Personal

WPA-Enterprise

WPA2-Personal

WPA2-Personal Mixed

WPA2-Enterprise

WPA2-Enterprise Mixed

Encryption:

Very Strong

Security Key:

Show Password: ☐

Key Renewal:

range: 600 - 7200, Default: 3600

Save Cancel Back

Schritt 3: (Optional) Um die SSID zu ändern, für die Sie die Sicherheit konfigurieren möchten, wählen Sie die gewünschte SSID aus der Dropdown-Liste SSID auswählen.

Schritt 4: Wählen Sie aus der Dropdown-Liste Security Mode (Sicherheitsmodus) den zu konfigurierenden Sicherheitsmodus aus.

·[Deaktivieren der Sicherheit](#) - Diese Option deaktiviert die Sicherheit des CVR100W VPN-Routers.

·[WEP-Sicherheit](#) - Wired Equivalent Privacy (WEP) ist ein Algorithmus zur Sicherung eines Wireless-Netzwerks. WEP wird verwendet, um eine grundlegende Verschlüsselungsmethode bereitzustellen, die weniger sicher ist als WPA. WEP wird verwendet, wenn verbundene Netzwerkgeräte WPA nicht unterstützen.

·[WPA-Personal Security](#) - Wi-Fi Protected Access (WPA) ist ein Sicherheitsstandard für Wireless-Netzwerke. WPA-Personal ist eine Version von WPA, die für Netzwerke mit wenigen Benutzern verwendet wird. WPA-Personal stellt einen gemeinsamen Schlüssel bereit, den jeder Benutzer für den Zugriff auf das Wireless-Netzwerk verwendet. WPA wurde mit den Schlüsselverschlüsselungsmethoden Temporal Key Integrity Protocol (TKIP) und Advanced Encryption Standard (AES) eingeführt.

·[WPA-Enterprise Security](#) - WPA-Enterprise ist eine Version von WPA, die für ein Netzwerk mit mehreren Benutzern empfohlen wird. Die Authentifizierung zum Zugriff auf das Netzwerk wird von einem RADIUS-Server gesteuert. Jeder verbundene Benutzer erhält einen eindeutigen Schlüssel für den Zugriff auf das Wireless-Netzwerk. WPA wurde mit den Schlüsselverschlüsselungsmethoden Temporal Key Integrity Protocol (TKIP) und Advanced Encryption Standard (AES) eingeführt.

·[WPA2-Personal Security](#): WPA2 ist eine Erweiterung von WPA und bietet mehr Sicherheit als WPA. WPA2-Personal ist eine Version von WPA2, die für Netzwerke mit wenigen Benutzern verwendet wird. WPA2-Personal ist sicherer als WPA2-Personal Mixed (Gemischt). WPA2-Personal stellt einen gemeinsamen Schlüssel bereit, den jeder Benutzer für den Zugriff auf das Wireless-Netzwerk verwendet.

·[WPA2-Personal Mixed Security](#) (WPA2-Personal-Gemischt) ist eine Version von WPA2, die für Netzwerke mit wenigen Benutzern verwendet wird. WPA2-Personal Mixed unterstützt Abwärtskompatibilität für ältere Geräte, die WPA2 nicht verwenden können. WPA2-Personal Mixed (WPA2-Personal-Gemischt) ist eine weniger sichere Verbindung.

·[WPA2-Enterprise Security](#) - WPA2-Enterprise ist eine Version von WPA2, die für Netzwerke mit zahlreichen Benutzern verwendet wird. WPA2-Enterprise ist sicherer als WPA2-Enterprise-Gemischt. Die zum Zugriff verwendete Authentifizierung wird von einem RADIUS-Server gesteuert. Das bedeutet, dass jedem angeschlossenen Benutzer ein eindeutiger Schlüssel für den Zugriff auf das Wireless-Netzwerk zugewiesen wird.

·[WPA2-Enterprise Mixed Security](#) (WPA2-Enterprise Gemischt) ist eine Version von WPA2, die für Netzwerke mit zahlreichen Benutzern verwendet wird. WPA2-Enterprise Mixed unterstützt Abwärtskompatibilität für ältere Geräte, die WPA2 nicht verwenden können. WPA2-Enterprise Mixed bietet eine weniger sichere Verbindung als WPA2-Enterprise. Die zum Zugriff verwendete Authentifizierung wird von einem RADIUS-Server gesteuert. Das bedeutet, dass jedem angeschlossenen Benutzer ein eindeutiger Schlüssel für den Zugriff auf das Wireless-Netzwerk zugewiesen wird.

Deaktivieren der Sicherheit

Die Wireless-Sicherheit kann auf dem CVR100W VPN-Router deaktiviert werden, um die Verwendung bei der Einrichtung von Testnetzwerken zu vereinfachen.

Hinweis: Die Deaktivierung der Sicherheit wird nicht empfohlen.

Security Settings

Select SSID: Cisco-4D61 ▼

Security Mode: Disabled ▼

Save Cancel Back

Schritt 1: Wählen Sie aus der Dropdown-Liste Security Mode (Sicherheitsmodus) die Option **Disabled (Deaktiviert)** aus. Die Sicherheit für das Wireless-Netzwerk ist deaktiviert.

Schritt 2: Klicken Sie auf **Speichern**.

WEP-Sicherheit konfigurieren

Security Settings

Select SSID: Cisco-4D61 ▼

Security Mode: WEP ▼

Authentication Type: Open System ▼ (Default: Open System)

Encryption: 10/64-bit(10 hex digits) ▼

Passphrase: Passphrase1 Generate

Key 1:

Key 2:

Key 3:

Key 4:

TX Key: 1 ▼

Show Password: ☐

Save Cancel Back

Schritt 1: Wählen Sie aus der Dropdown-Liste Security Mode (Sicherheitsmodus) die Option **WEP** aus.

Schritt 2: Wählen Sie aus der Dropdown-Liste Authentication Type (Authentifizierungstyp) einen Authentifizierungstyp für das Wireless-Netzwerk aus.

- Offenes System - Jedes Netzwerkgerät kann eine Verbindung zum Access Point herstellen. Der WEP-Schlüssel ist jedoch erforderlich, um Datenverkehr durch den Access

Point zu leiten.

·Shared Key (Gemeinsamer Schlüssel): Für die Verbindung mit dem Access Point ist ein WEP-Schlüssel erforderlich. Er wird auch verwendet, um Datenverkehr durch den Access Point zu leiten.

Schritt 3: Wählen Sie aus der Dropdown-Liste Verschlüsselung eine Verschlüsselungsmethode für den WEP-Schlüssel aus.

·10/64-Bit(10 Hexadezimalziffern) - Stellt eine 40-Bit-Taste bereit.

·26/128-Bit(26 Hexadezimalziffern) - Stellt eine 104-Bit-Taste bereit. Diese Option ist sicherer.

Schritt 4: Geben Sie im Feld Passphrase eine Passphrase mit mehr als acht Zeichen ein. Eine Passphrase ist hilfreich, um die Einstellungen für die Netzwerksicherheit einfacher zu merken.

Schritt 5: Klicken Sie in den Feldern Schlüssel 1, Schlüssel 2, Schlüssel 3 und Schlüssel 4 auf **Generieren**, um Schlüssel zu erstellen.

Hinweis: Sie können die Tasten auch manuell in die Felder Schlüssel 1, 2, 3 und 4 eingeben.

Schritt 6: Wählen Sie in der Dropdown-Liste TX Key (TX-Schlüssel) den Schlüssel aus, den Benutzer eingeben müssen, um auf das Wireless-Netzwerk zuzugreifen.

Schritt 7: (Optional) Aktivieren Sie das Kontrollkästchen **Kennwort anzeigen**, um die Zeichenfolgen der Schlüssel anzuzeigen.

Schritt 8: Klicken Sie auf **Speichern**.

WPA-Personal-Sicherheit konfigurieren

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)

At the bottom are buttons for 'Save', 'Cancel', and 'Back'.

Schritt 1: Wählen Sie aus der Dropdown-Liste Security Mode (Sicherheitsmodus) die Option **WPA-Personal** aus.

Schritt 2: Wählen Sie aus der Dropdown-Liste Verschlüsselung eine Verschlüsselungsmethode für den WPA-Schlüssel aus.

·TKIP/AES: Diese Option wird gewählt, wenn Geräte, die mit dem Wireless-Netzwerk verbunden sind, nicht alle AES unterstützen.

·AES: Diese Option ist vorzuziehen, wenn alle mit dem Wireless-Netzwerk verbundenen Geräte AES unterstützen.

Schritt 3: Geben Sie im Feld Sicherheitsschlüssel einen Sicherheitsschlüssel ein. Der Sicherheitsschlüssel ist eine Passphrase, die aus Buchstaben und Ziffern besteht. Geräte verwenden den Sicherheitsschlüssel, um eine Verbindung zum Netzwerk herzustellen.

Schritt 4: (Optional) Um die Zeichenfolge des Schlüssels anzuzeigen, aktivieren Sie das Kontrollkästchen **Kennwort anzeigen**.

Schritt 5: Geben Sie im Feld Key Renewal (Schlüsselverlängerung) die Zeit in Sekunden ein, die der CVR100W VPN-Router den Schlüssel verwendet, bevor ein neuer generiert wird.

Schritt 6: Klicken Sie auf **Speichern**.

WPA-Enterprise-Sicherheit konfigurieren

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

- Select SSID:** A dropdown menu with "Cisco-4D61" 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 "220", with a hint "(Hint: 192.168.1.200)".
- RADIUS Port:** An input field containing "1812", with a range note "(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".

Schritt 1: Wählen Sie aus der Dropdown-Liste Security Mode (Sicherheitsmodus) die Option **WPA-Enterprise** aus.

Schritt 2: Wählen Sie aus der Dropdown-Liste Verschlüsselung eine Verschlüsselungsmethode für den WPA-Schlüssel aus.

·TKIP/AES: Diese Option wird gewählt, wenn Geräte, die mit dem Wireless-Netzwerk verbunden sind, nicht alle AES unterstützen.

·AES: Diese Option ist vorzuziehen, wenn alle mit dem Wireless-Netzwerk verbundenen Geräte AES unterstützen.

Schritt 3: Geben Sie im Feld RADIUS Server (RADIUS-Server) die IP-Adresse des RADIUS-Servers ein.

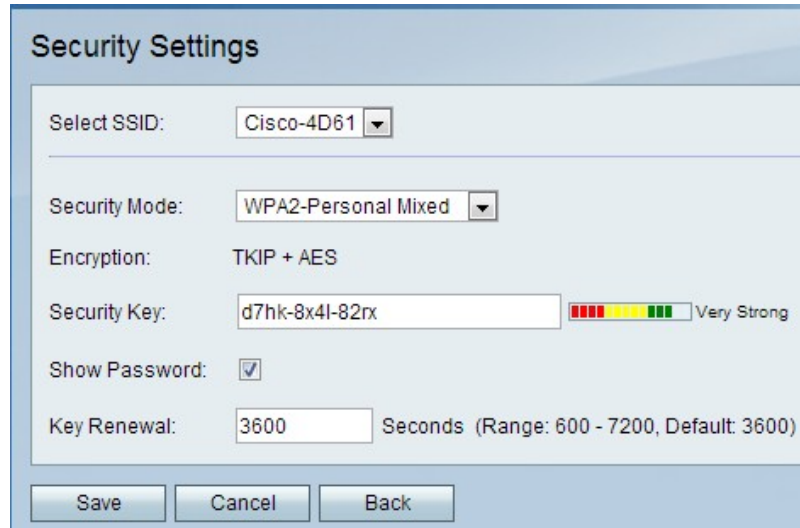
Schritt 4: Geben Sie im Feld RADIUS Port (RADIUS-Port) die Portnummer ein, die für den Zugriff auf den RADIUS-Server verwendet wird.

Schritt 5: Geben Sie im Feld "Freigegebener Schlüssel" den vorinstallierten Schlüssel für die Wireless-Benutzer ein. Ein vorinstallierter Schlüssel ist ein Schlüssel, der von allen Benutzern verwendet wird. Die Funktion eines vorinstallierten Schlüssels ist eine zusätzliche Sicherheitsfunktion.

Schritt 6: Geben Sie im Feld Key Renewal (Schlüsselverlängerung) die Zeit in Sekunden ein, die der CVR100W VPN-Router den Schlüssel verwendet, bevor ein neuer generiert wird.

Schritt 7: Klicken Sie auf **Speichern**.

WPA2-Personal-/WPA2-Personal-Gemischte Sicherheit konfigurieren



The screenshot shows a 'Security Settings' window. At the top, 'Select SSID:' is set to 'Cisco-4D61'. Below, 'Security Mode:' is set to 'WPA2-Personal Mixed'. 'Encryption:' is set to 'TKIP + AES'. 'Security Key:' is 'd7hk-8x4l-82rx', with a strength indicator showing four red bars and two green bars, labeled 'Very Strong'. 'Show Password:' is checked. 'Key Renewal:' is set to '3600' seconds, with a range of '600 - 7200, Default: 3600'. At the bottom are 'Save', 'Cancel', and 'Back' buttons.

Schritt 1: Wählen Sie aus der Dropdown-Liste Security Mode (Sicherheitsmodus) die Option **WPA2-Personal** oder **WPA2-Personal Mixed** (**WPA2-Personal** oder **WPA2-Personal Gemischt**).

Hinweis: WPA2-Personal wird verwendet, wenn alle Geräte im Wireless-Netzwerk AES unterstützen. WPA2-Personal Mixed wird verwendet, wenn Geräte im Netzwerk nicht alle AES unterstützen. Der von der Sicherheitsmethode verwendete Verschlüsselungstyp wird im Feld Verschlüsselung angezeigt.

Schritt 2: Geben Sie im Feld Sicherheitsschlüssel einen Sicherheitsschlüssel ein. Der Sicherheitsschlüssel ist eine Passphrase, die aus Buchstaben und Ziffern besteht. Geräte verwenden den Sicherheitsschlüssel, um eine Verbindung zum Netzwerk herzustellen.

Schritt 3: (Optional) Um die Zeichenfolgen des Schlüssels anzuzeigen, aktivieren Sie das Kontrollkästchen **Kennwort anzeigen**.

Schritt 4: Geben Sie im Feld Key Renewal (Schlüsselverlängerung) die Zeit in Sekunden für die Zeit ein, in der der CVR100W VPN-Router den Schlüssel verwendet, bevor ein neuer generiert wird.

Schritt 5: Klicken Sie auf **Speichern**.

WPA2-Enterprise/WPA2-Enterprise Mixed Security konfigurieren

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

Schritt 1: Wählen Sie aus der Dropdown-Liste Security Mode (Sicherheitsmodus) die Option **WPA2-Enterprise** oder **WPA2-Enterprise Mixed (WPA2-Enterprise Gemischt)**.

Hinweis: WPA2-Enterprise wird verwendet, wenn alle Geräte im Wireless-Netzwerk AES unterstützen. WPA2-Enterprise Mixed wird verwendet, wenn Geräte im Netzwerk nicht alle AES unterstützen. Der von der Sicherheitsmethode verwendete Verschlüsselungstyp wird im Feld Verschlüsselung angezeigt.

Schritt 2: Geben Sie im Feld RADIUS Server (RADIUS-Server) die IP-Adresse des RADIUS-Servers ein.

Schritt 3: Geben Sie im Feld RADIUS Port (RADIUS-Port) die Portnummer ein, die für den Zugriff auf den RADIUS-Server verwendet wird.

Schritt 4: Geben Sie im Feld "Freigegebener Schlüssel" den vorinstallierten Schlüssel für die Wireless-Benutzer ein. Ein vorinstallierter Schlüssel ist ein Schlüssel, der von allen Benutzern verwendet wird. Die Funktion eines vorinstallierten Schlüssels ist eine zusätzliche Sicherheitsfunktion.

Schritt 5: Geben Sie im Feld Key Renewal (Schlüsselverlängerung) die Zeit in Sekunden ein, die der CVR100W VPN-Router den Schlüssel verwendet, bevor ein neuer generiert wird.

Schritt 6: Klicken Sie auf **Speichern**.

MAC-Filterung bearbeiten

Mithilfe der MAC-Filterung wird der Zugriff auf das Wireless-Netzwerk basierend auf der MAC-Adresse des angeschlossenen Geräts zugelassen oder verweigert.

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

	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
☒	☒	Cisco-4D61	☒	WPA2-Personal	Disabled	☐	1	☐	☒	☒
☐	☐	cisco-SSID2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐	cisco-SSID3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐	cisco-guest	☒	Disabled	Disabled	☐	3	☒	☒	☐

Schritt 1: Aktivieren Sie das Kontrollkästchen des Netzwerks, das Sie bearbeiten möchten.

Schritt 2: Klicken Sie auf **MAC-Filterung bearbeiten**, um eine MAC-Zugriffskontrollliste für das angegebene Netzwerk zu erstellen. Die Seite *Wireless MAC Filter* wird geöffnet:

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	
02		13	
03		14	
04		15	
05		16	
06		17	
07		18	
08		19	
09		20	
10		21	
11		22	
		23	
		24	
		25	
		26	
		27	
		28	
		29	
		30	
		31	
		32	

Schritt 3: Aktivieren Sie **Aktivieren**, um die MAC-Filterung im Netzwerk zu aktivieren.

Schritt 4: Klicken Sie im Feld Verbindungssteuerung auf das Optionsfeld für den gewünschten Listentyp.

- Verhindert, dass PCs mit den aufgeführten MAC-Adressen in das Netzwerk eindringen.
- Zulassen von PCs - Ermöglicht PCs mit den aufgeführten MAC-Adressen, in das Netzwerk einzudringen.

Schritt 5: Geben Sie in der MAC-Adresstabelle die gewünschten MAC-Adressen ein.

Schritt 6: Klicken Sie auf **Speichern**.

Tageszeit

Die Funktion "Tageszeitzugriff" wird verwendet, um Benutzern den Zugriff auf Basis eines konfigurierten Zeitplans zu ermöglichen.

Wireless Table										
☐	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
☒	☒	Cisco-4D61	☒	WPA2-Personal	Disabled	☒	1	☒	☒	☒
☐	☐	cisco-SSID2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐	cisco-SSID3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐	cisco-guest	☒	Disabled	Disabled	☐	3	☒	☒	☐
EditEdit Security ModeEdit MAC FilteringTime of Day AccessEdit Guest NetEdit CSCEdit WPS										

Schritt 1: Aktivieren Sie das Kontrollkästchen des Netzwerks, das Sie bearbeiten möchten.

Schritt 2: Klicken Sie auf **Time of Day Access**, um zu konfigurieren, wann Benutzer auf das angegebene Netzwerk zugreifen können. Die Seite *Time of Day Access* (Tageszeitzugriff) wird geöffnet:

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

SaveCancelBack

Schritt 3: Aktivieren Sie **Aktivieren** im Feld "Active Time" (Aktive Zeit), um den Tageszeitzugriff für das Netzwerk zu aktivieren.

Schritt 4: Geben Sie im Feld Startzeit den Zeitpunkt ein, zu dem der Netzwerkzugriff beginnt.

Schritt 5: Geben Sie im Feld Stopp Time (Stopp-Zeit) die Zeit ein, zu der der Netzwerkzugriff beendet wird.

Schritt 6: Klicken Sie auf **Speichern**.

Gastnetzwerk bearbeiten

Ein Gastnetzwerk ist ein Teil eines Netzwerks, das für temporäre Benutzer entwickelt wurde. So können Gäste auf das Netzwerk zugreifen, ohne dass private Wi-Fi-Schlüssel verfügbar sein müssen. Ein Gastnetzwerk kann so konfiguriert werden, dass die Zugriffszeit und die Bandbreitennutzung eines Benutzers beschränkt werden.

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

	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
☐	☒	Cisco-4D61	☒	WPA2-Personal	Disabled	☐	1	☐	☒	☒
☐	☐	disco-SSID2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐	disco-SSID3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☒	☐	disco-guest	☒	Disabled	Disabled	☐	3	☒	☒	☐

Schritt 1: Klicken Sie auf **Edit Guest Network**, um das Gastnetzwerk zu konfigurieren. Die Seite *Gastnetzeinstellungen* wird geöffnet:

Guest Net Settings

Guest Net Name: guest

Guest Password:

Hide Password: ☒

Lease Time: 120 Minutes

Total Guest Allowed: 5

Schritt 2: Geben Sie im Feld Guest Password (Gastkennwort) ein Kennwort ein, das die Benutzer verwenden werden, um das Gastnetzwerk einzugeben.

Schritt 3: (Optional) Um das Kennwort auf der Seite auszublenden, aktivieren Sie das Kontrollkästchen im Feld Kennwort ausblenden.

Schritt 4: Geben Sie im Feld Lease Time (Leasingzeit) die Zeit in Minuten ein, zu der die Benutzer mit dem Gastnetzwerk verbunden bleiben dürfen.

Schritt 5: Wählen Sie aus der Dropdown-Liste "Zulässige Gesamtgäste" die Gesamtzahl der zulässigen Gäste aus.

Schritt 6: Klicken Sie auf **Speichern**.

CSC bearbeiten

CSC ermöglicht die einfache Einrichtung eines Wireless-Netzwerks und die einfache Verbindung von Wireless-Geräten mit dem Netzwerk. Das Wireless-Gerät verwendet CSC,

um die SSID und das Kennwort des Netzwerks abzurufen, wodurch eine automatische Verbindung zum Netzwerk möglich wird.

Wireless Table										
☐	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
☐	☒	Cisco-4D61	☒	WPA2-Personal	Disabled	☐	1	☐	☒	☒
☒	☒	Cisco-1	☒	Disabled	Disabled	☒	5	☒	☒	☐
☐	☐	cisco-SSID3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐	cisco-guest	☒	Disabled	Disabled	☐	3	☒	☒	☐
EditEdit Security ModeEdit MAC FilteringTime of Day AccessEdit Guest NetEdit CSCEdit WPS										

Schritt 1: Aktivieren Sie das Kontrollkästchen des Netzwerks, das Sie bearbeiten möchten.

Schritt 2: Klicken Sie auf **Edit CSC**, um Cisco Simple Connect zu bearbeiten.

Schritt 3: Aktivieren Sie das Kontrollkästchen CSC.

Schritt 4: Wählen Sie aus der VLAN-Dropdown-Liste das VLAN aus, das für CSC verwendet wird.

Hinweis: Das Cisco Simple Connect VLAN darf nicht mit dem aktuellen oder anderen SSID-VLAN identisch sein. Weitere Informationen zum Erstellen eines neuen VLAN finden Sie im Artikel [VLAN Membership \(VLAN-Mitgliedschaft\) auf dem CVR100W Router](#).

Hinweis: CSC kann nur das Wireless Distribution System (WDS) auf SSID1 aktivieren. Weitere Informationen finden Sie im Artikel [Wireless Distribution System \(WDS\) auf dem CVR100W Router](#).

Schritt 5: Klicken Sie auf **Speichern**.