SSID-Sicherheitseinstellungen auf der RV110W

Ziel

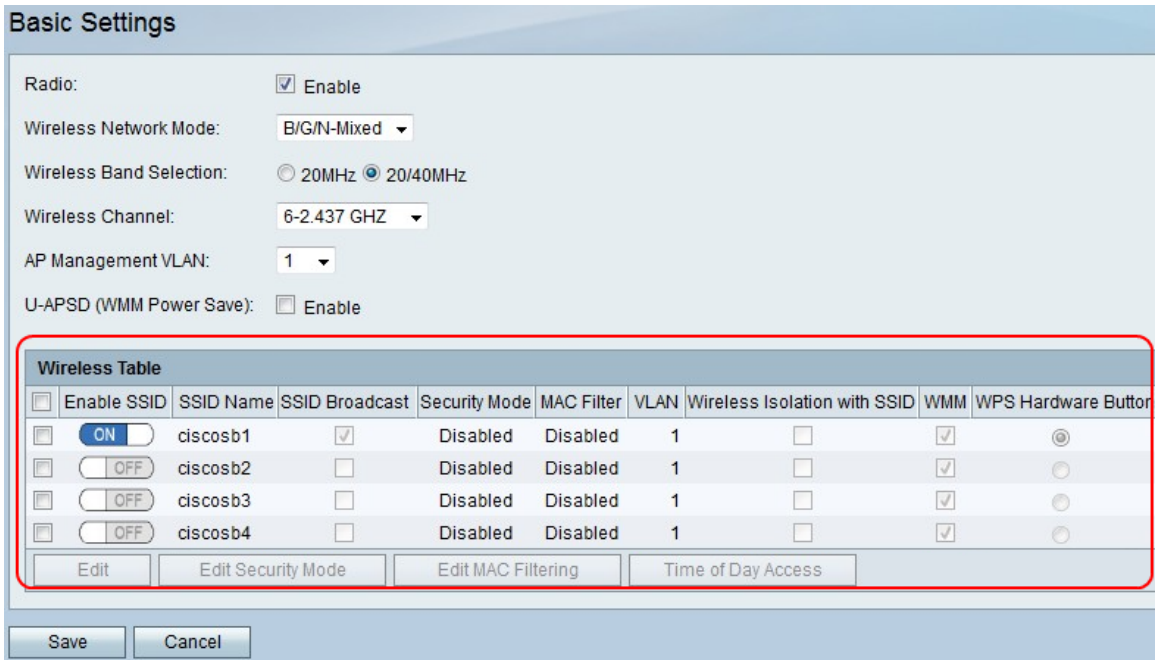
Sicherheitsmodi bieten Schutz für ein Wireless-Netzwerk. Verschiedene Service Set IDs (SSIDs) können unterschiedliche Sicherheitsmodi aufweisen. SSIDs können verschiedene Funktionen für das Netzwerk ausführen. SSIDs können daher unterschiedliche Sicherheitsmaßnahmen erfordern. In diesem Artikel wird erläutert, wie die Sicherheitseinstellungen für eine SSID auf der RV110W konfiguriert werden.

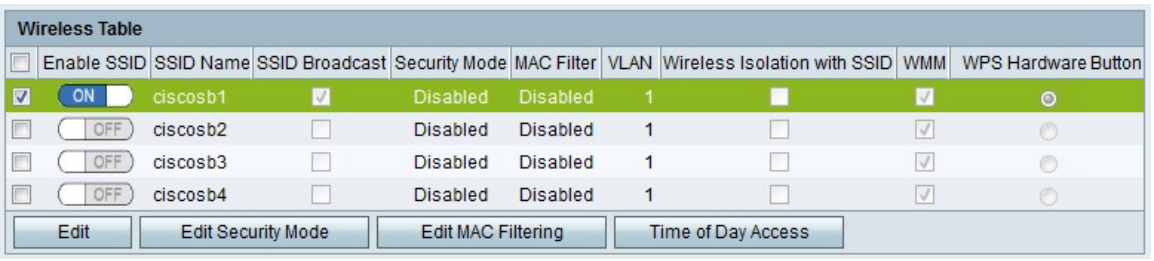
Anwendbare Geräte

- RV110 W

Verfahrensschritte

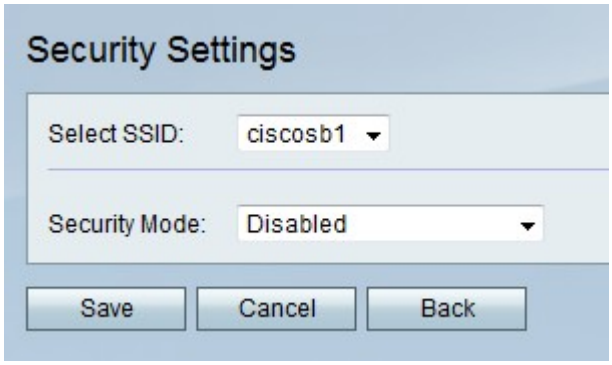
Schritt 1: Wählen Sie mit dem Webkonfigurationsprogramm **Wireless > Basic Settings (Wireless > Grundeinstellungen)**.





Schritt 2: Aktivieren Sie in der Wireless-Tabelle das Kontrollkästchen einer SSID, für die Sie die Sicherheitseinstellungen bearbeiten möchten.

Schritt 3: Klicken Sie auf **Sicherheitsmodus bearbeiten**. Daraufhin wird die Seite *Sicherheitseinstellungen* geöffnet.



Schritt 4: Wählen Sie im Dropdown-Menü SSID auswählen eine SSID aus, für die Sie die Sicherheitseinstellungen bearbeiten möchten.

Deaktivieren des Sicherheitsmodus

Dieses Verfahren zeigt, wie der Sicherheitsmodus einer SSID deaktiviert wird, der keine Sicherheitsinformationen für die Verwendung der SSID erfordert.

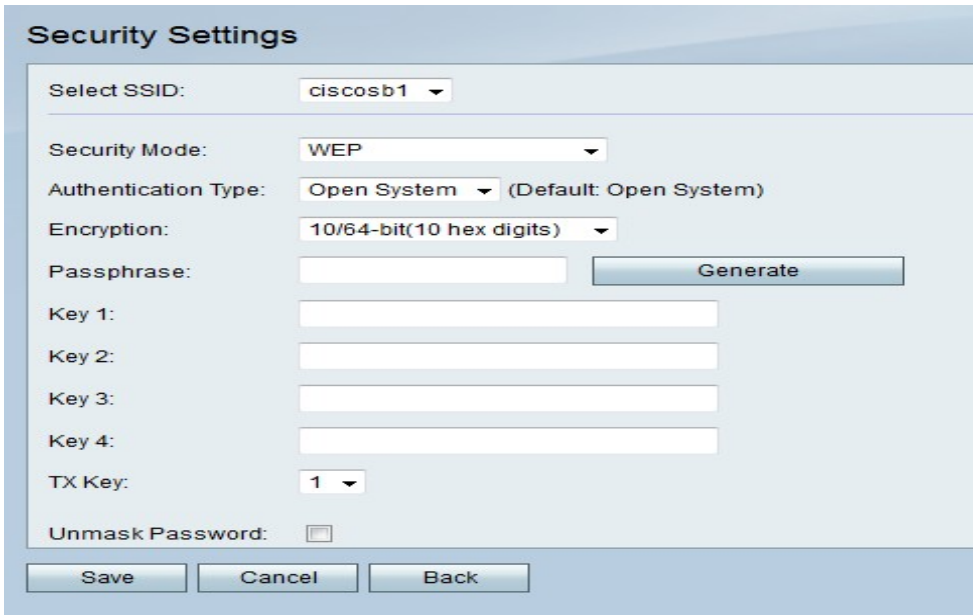
Schritt 1: Wählen Sie im Dropdown-Menü Security Mode (Sicherheitsmodus) die Option **Disabled (Deaktiviert)** aus.

Schritt 2: Klicken Sie auf **Speichern**, um die Änderungen zu speichern, **Abbrechen**, um sie zu verwerfen, oder **Zurück,** um zur vorherigen Seite zurückzukehren.

WEP-Sicherheitsmodus

Dieses Verfahren zeigt, wie Wired Equivalent Privacy (WEP) als Sicherheitsmodus einer SSID festgelegt wird. WEP ist nicht der sicherste Sicherheitsmodus, kann jedoch die einzige Option sein, wenn einige Netzwerkgeräte WPA nicht unterstützen.

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



Schritt 2: Wählen Sie im Dropdown-Menü Authentifizierungstyp eine Option aus.

- Open System (System öffnen): Diese Option ist direkter und sicherer als die Authentifizierung mit gemeinsam genutztem Schlüssel.

- Shared Key (Freigegebener Schlüssel): Diese Option ist weniger sicher als Open System (System öffnen).

Schritt 3: Wählen Sie im Dropdown-Menü Verschlüsselung die Option 10/64-Bit (10 Hexadezimalziffern) aus, bei der ein 40-Bit-Schlüssel verwendet wird, oder die Option 26/128-Bit (26 Hexadezimalziffern), bei der ein 104-Bit-Schlüssel verwendet wird.

Schritt 4: Geben Sie im Feld Passphrase eine Passphrase mit Buchstaben und Zahlen ein, die mindestens 8 Zeichen lang ist.

Schritt 5: Klicken Sie auf **Generate** (Generieren), um vier WEP-Schlüssel in den Schlüsselfeldern zu erstellen, oder geben Sie die WEP-Schlüssel manuell in die Schlüsselfelder ein.

Schritt 6: Wählen Sie im Dropdown-Menü TX Key (TX-Schlüssel) die Nummer des Schlüsselfelds für den WEP-Schlüssel aus, den Sie als gemeinsamen Schlüssel verwenden möchten.

Schritt 7: Aktivieren Sie das Kontrollkästchen **Unmask Password** (Kennwort für die Unmaske), wenn Sie Kennwortzeichen preisgeben möchten.

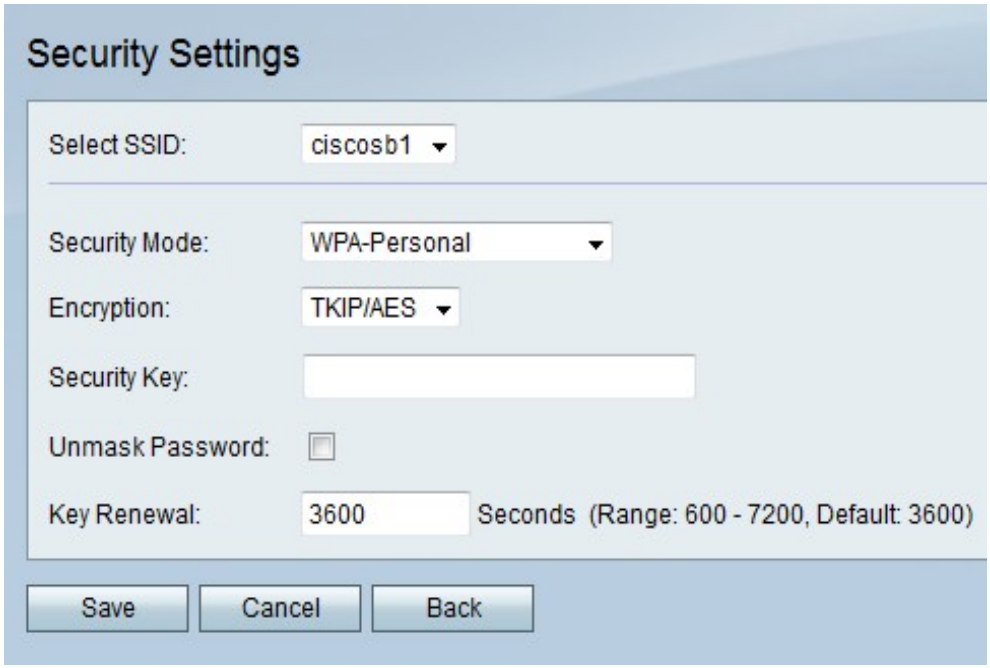
Schritt 8: Klicken Sie auf **Speichern**, um die Änderungen zu speichern, **Abbrechen**, um sie zu verwerfen, oder **Zurück,** um zur vorherigen Seite zurückzukehren.

Gemischten Sicherheitsmodus WPA-Personal, WPA2-Personal und WPA2-Personal

Wi-Fi Protected Access (WPA) ist ein Sicherheitsmodus, der stärker ist als WEP. WPA-Personal kann entweder Temporal Key Integrity Protocol (TKIP) oder Advanced Encryption Standard (AES) für die Verschlüsselung verwenden. WPA2-Personal verwendet nur AES für die Verschlüsselung und einen PSK für die Authentifizierung. WPA2-Personal Mixed kann WPA- und WPA2-Clients unterstützen und verwendet AES und PSK. Dieses Verfahren zeigt, wie WPA-Personal, WPA2-Personal oder WPA2-Personal Mixed als Sicherheitsmodus für eine SSID eingerichtet wird.

Schritt 1: Wählen Sie im Dropdown-Menü Security Mode (Sicherheitsmodus) eine Option aus.

- WPA-Personal: Diese Option unterstützt AES und TKIP.
- WPA2-Personal: Diese Option unterstützt AES und PSK.
- WPA2-Personal Mixed (WPA2-Personal-Gemischt): Diese Option unterstützt WPA- und WPA2-Clients.



Schritt 2: Wenn Sie WPA-Personal auswählen, wählen Sie im Dropdown-Menü Verschlüsselung einen Verschlüsselungstyp aus.

- TKIP/AES: Diese Option ist mit älteren Geräten kompatibel, die AES nicht unterstützen.
- AES: Diese Option ist sicherer als TKIP/AES.

Schritt 3: Geben Sie im Feld Sicherheitsschlüssel eine Zeichenfolge und eine Zeichenfolge ein, die den Zugriff auf das Netzwerk einschränkt.

Schritt 4: Aktivieren Sie das Kontrollkästchen **Unmask Password** (Kennwort für die Unmaske), wenn Sie Kennwortzeichen preisgeben möchten.

Schritt 5: Geben Sie im Feld Key Renewal (Schlüsselverlängerung) ein, wie oft das Netzwerk den Schlüssel in Sekunden verlängert.

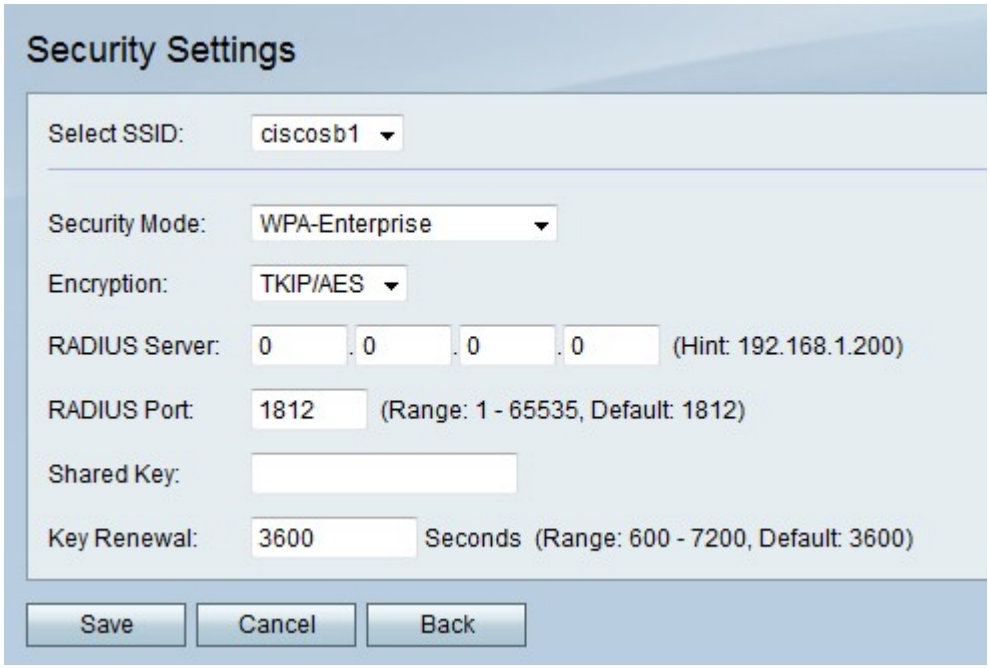
Schritt 6: Klicken Sie auf **Speichern**, um die Änderungen zu speichern, **Abbrechen**, um sie zu verwerfen, oder **Zurück,** um zur vorherigen Seite zurückzukehren.

WPA-Enterprise, WPA2-Enterprise und WPA2-Enterprise Mixed Security Mode

Die Enterprise-Sicherheitsmodi verwenden die RADIUS-Serverauthentifizierung (Remote Authentication Dial In User Service). RADIUS ist ein Netzwerkprotokoll, das einen separaten Server verwendet. Der Datenverkehr zum und vom Netzwerk muss über den RADIUS-Server geleitet werden. Dieses Verfahren zeigt, wie WPA-Enterprise, WPA2-Enterprise oder WPA2-Enterprise Mixed als Sicherheitsmodus für eine SSID eingerichtet wird.

Schritt 1: Wählen Sie im Dropdown-Menü Security Mode (Sicherheitsmodus) eine Option aus.

- WPA-Enterprise (WPA-Enterprise): Diese Option verwendet RADIUS, AES und TKIP.
- WPA2-Enterprise (WPA2-Enterprise): Diese Option verwendet RADIUS, AES und PSK.
- WPA2-Enterprise Mixed (WPA2-Enterprise-Gemischt): Diese Option verwendet RADIUS und unterstützt WPA- und WPA2-Clients.



Schritt 2: Wenn Sie WPA-Enterprise auswählen, wählen Sie im Dropdown-Menü Verschlüsselung einen Verschlüsselungstyp aus.

- TKIP/AES: Diese Option ist mit älteren Geräten kompatibel, die AES nicht unterstützen.
- AES: Diese Option ist sicherer als TKIP/AES.

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, auf der das Netzwerk auf den RADIUS-Server zugreift.

Schritt 5: Geben Sie im Feld "Freigegebener Schlüssel" einen Satz von Buchstaben und Zahlen ein, die den Zugriff auf das Netzwerk einschränken.

Schritt 6: Geben Sie im Feld Key Renewal (Schlüsselverlängerung) ein, wie oft das Netzwerk den Schlüssel in Sekunden verlängert.

Schritt 7: Klicken Sie auf **Speichern**, um die Änderungen zu speichern, **Abbrechen**, um sie zu verwerfen, oder **Zurück,** um zur vorherigen Seite zurückzukehren.