

# SSID security instellingen op de RV110W

## Doel

Security modi bieden bescherming voor een draadloos netwerk. Verschillende Service Set-ID's (SSID's) kunnen verschillende beveiligingsmodi hebben. SSID's kunnen verschillende functies voor het netwerk vervullen; SSID's kunnen daarom verschillende beveiligingsmaatregelen vereisen. Dit artikel legt uit hoe u de beveiligingsinstellingen voor een SSID op de RV110W kunt configureren.

## Toepasselijke apparaten

- RV110 W

## Stappen van orde

Stap 1. Gebruik het web configuratie hulpprogramma om **draadloos > basisinstellingen** te kiezen.

Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	VLAN	Wireless Isolation with SSID	WMM	WPS Hardware Button
<input checked="" type="checkbox"/>	ciscosb1	<input checked="" type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/>	ciscosb2	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/>	ciscosb3	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/>	ciscosb4	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>

Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	VLAN	Wireless Isolation with SSID	WMM	WPS Hardware Button
<input checked="" type="checkbox"/>	ciscosb1	<input checked="" type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/>	ciscosb2	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/>	ciscosb3	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/>	ciscosb4	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>

Stap 2. Controleer in de draadloze tabel het selectieteken van een SSID waarvoor u de beveiligingsinstellingen wilt bewerken.

Stap 3. Klik op **Beveiliging**. Dit opent de pagina *Beveiligingsinstellingen*.

The screenshot shows a 'Security Settings' window. At the top, the title 'Security Settings' is displayed. Below it, there are two dropdown menus: 'Select SSID:' with 'ciscosb1' selected, and 'Security Mode:' with 'Disabled' selected. At the bottom of the window, there are three buttons: 'Save', 'Cancel', and 'Back'.

Stap 4. Kies in het vervolgkeuzemenu SSID selecteren een SSID waarvoor u beveiligingsinstellingen wilt bewerken.

## Beveiligingsmodus uitschakelen

Deze procedure toont hoe de veiligheidsmodus van een SSID wordt uitgeschakeld. Deze optie vereist geen veiligheidsinformatie om de SSID te gebruiken.

Stap 1. Kies in het vervolgkeuzemenu Security Mode de optie **Uitgeschakeld**.

Stap 2. Klik op **Opslaan** om wijzigingen op te slaan, **Annuleren** om ze weg te gooien of **Terug** naar de vorige pagina.

## Wi-beveiligingsmodus

Deze procedure toont hoe u Wired Equivalent Privacy (EFN) als veiligheidsmodus van een SSID kunt instellen. De beveiligingsmodus is niet het meest beveiligd, maar het kan de enige optie zijn als sommige netwerkkapparaten geen WAP ondersteunen.

Stap 1. Kies in het vervolgkeuzemenu Security Mode **en** kies **EFN**.

The screenshot shows a 'Security Settings' window. The 'Select SSID:' dropdown is set to 'ciscosb1'. The 'Security Mode:' dropdown is set to 'WEP'. The 'Authentication Type:' dropdown is set to 'Open System' with '(Default: Open System)' in parentheses. The 'Encryption:' dropdown is set to '10/64-bit(10 hex digits)'. There is a 'Passphrase:' input field with a 'Generate' button to its right. Below that are four 'Key' input fields labeled 'Key 1:', 'Key 2:', 'Key 3:', and 'Key 4:'. The 'TX Key:' dropdown is set to '1'. At the bottom left, there is an 'Unmask Password:' checkbox. At the bottom of the window, there are three buttons: 'Save', 'Cancel', and 'Back'.

Stap 2. Kies een optie in het vervolgkeuzemenu Verificatietype.

- Open System — Deze optie is directer en veiliger dan Shared Key Verificatie.
- Shared Key — Deze optie is minder veilig dan Open System.

Stap 3. Kies in het vervolgkeuzemenu Encryptie een 10/64-bits (10 hex cijfers), die een 40-

bits toets of 26/128-bits (26 hex cijfers) gebruikt, die een 104-bits toets gebruikt.

Stap 4. Voer in het veld Wachtwoord in met een wachtwoord dat uit ten minste 8 tekens bestaat.

Stap 5. Klik op **Generate** om vier de sleutels van EVN in de Kernvelden te maken, of handmatig de sleutels van EVN in de Kernvelden in te voeren.

Stap 6. Kies in het vervolgkeuzemenu TX-toets het toetstitel-veldnummer van de EFN-toets die u als gedeelde toets wilt gebruiken.

Stap 7. Controleer het selectieteken **Wachtwoord** voor **onmasker** als u wachtwoordtekens wilt vrijgeven.

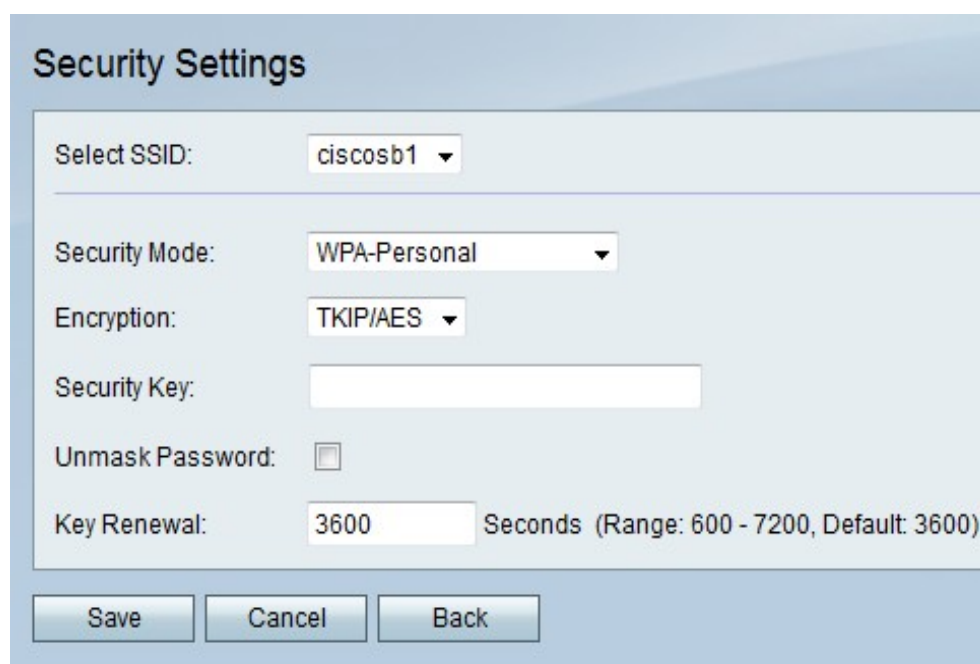
Stap 7. Klik op **Opslaan** om wijzigingen op te slaan, **Annuleren** om ze weg te gooien of **Terug** naar de vorige pagina.

## WAP-Persoonlijke, WAP2-Persoonlijke en WAP2-persoonlijke beveiligingsmodus

Wi-Fi Protected Access (WAP) is een beveiligingsmodus die sterker is dan EFG. WAP-Mobile kan ofwel Temporal Key Integrity Protocol (TKIP) of Advanced Encryption Standard (AES) gebruiken voor encryptie. WAP2-Mobile gebruikt alleen AES voor encryptie en een PreShared Key (PSK) voor verificatie. WAP2-persoonlijk Gemengde is in staat om zowel de cliënten van WAP als WAP2 te steunen en gebruikt AES en PSK. Deze procedure toont hoe u WAP-persoonlijk, WAP2-Persoonlijk of Gemengde WAP2-Persoonlijk als veiligheidsmodus voor een SSID kunt instellen.

Stap 1. Kies een optie in het vervolgkeuzemenu Security Mode.

- WAP-Persoonlijk - Deze optie ondersteunt AES en TKIP.
- WAP2-Persoonlijk — Deze opties ondersteunen AES en PSK.
- Gemengde WAP2 - deze optie ondersteunt zowel de WAP- als de WAP2-clients.



Security Settings

Select SSID: ciscosb1

Security Mode: WPA-Personal

Encryption: TKIP/AES

Security Key:

Unmask Password:

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

Save Cancel Back

Stap 2. Als u WAP-Mobile kiest, kiest u een coderingstype in het vervolgkeuzemenu Encryptie.

- TKIP/AES — Deze optie is compatibel met oudere apparaten die AES niet ondersteunen.
- AES — Deze optie is veiliger dan TKIP/AES.

Stap 3. Voer in het veld Security Key een zinsnede van letters en getallen in die de toegang tot het netwerk beperkt.

Stap 4. Controleer het selectieteken **Wachtwoord** voor **onmasker** als u wachtwoordtekens wilt vrijgeven.

Stap 5. Voer in het veld Belangrijkste vernieuwing in hoe vaak in seconden het netwerk de toets vernieuwt.

Stap 6. Klik op **Opslaan** om wijzigingen op te slaan, **Annuleren** om ze weg te gooien of **Terug** naar de vorige pagina.

## Mix-security modus voor WAP-ondernemingen, WAP2-ondernemingen en WAP2-ondernemingen

De Enterprise Security Mode maakt gebruik van een afstandsbediening voor verificatie van de RADIUS-server (Dial In User Service). RADIUS is een netwerkprotocol dat een aparte server gebruikt en het verkeer naar en van het netwerk moet via de RADIUS-server worden doorgegeven. Deze procedure toont hoe u WAP-Enterprise, WAP2-Enterprise of Gemengde WAP2-Enterprise als veiligheidsmodus voor een SSID kunt instellen.

Stap 1. Kies een optie in het vervolgkeuzemenu Security Mode.

- WAP-Enterprise — Deze optie gebruikt RADIUS, AES en TKIP.
- WAP2-Enterprise — Deze optie gebruikt RADIUS, AES en PSK.
- Gemengde WAP2-Enterprise — Deze optie gebruikt RADIUS en ondersteunt zowel WAP- als WAP2-clients.

Stap 2. Als u WAP-Enterprise kiest, kiest u een coderingstype in het vervolgkeuzemenu Encryptie.

- TKIP/AES — Deze optie is compatibel met oudere apparaten die AES niet ondersteunen.
- AES — Deze optie is veiliger dan TKIP/AES.

Stap 3. Voer in het veld RADIUS-server het IP-adres van de RADIUS-server in.

Stap 4. Voer in het veld RADIUS-poort het poortnummer in waarop het netwerk toegang heeft tot de RADIUS-server.

Stap 5. Voer in het veld Shared Key een zinsnede van letters en getallen in die de toegang tot het netwerk beperkt.

Stap 6. Voer in het veld Verlengen sleutel in hoe vaak in seconden het netwerk de toets vernieuwt.

Stap 7. Klik op **Opslaan** om wijzigingen op te slaan, **Annuleren** om ze weg te gooien of **Terug** naar de vorige pagina.