

Basisconfiguratie voor draadloze instellingen op RV215W

Doel

Draadloze netwerken zijn computernetwerken die niet met kabels zijn verbonden. Een Wireless Local Area Network (WLAN) is een draadloos netwerk dat meerdere apparaten op korte afstand verbindt door middel van radiocommunicatie.

In dit artikel wordt uitgelegd hoe u de basisinstellingen voor draadloze communicatie op de RV215W kunt configureren, inclusief de configuratie van netwerkbeveiliging.

indexeren

- [Algemene instellingen](#)
- [Draadloze tabel bewerken](#)
- [Beveiliging uitschakelen](#)
- [WEP-beveiliging configureren](#)
- [WPA-Personal Security configureren](#)
- [WPA-Enterprise Security configureren](#)
- [WPA2-Personal/WPA2-Personal Mixed Security configureren](#)
- [WPA2-Enterprise/WPA2-Enterprise Mixed Security configureren](#)
- [MAC-filtering bewerken](#)
- [Tijdstip van dagtoegang](#)
- [Gastnetwerk bewerken](#)
- [WPS-methode 1 configureren](#)
- [WPS-methode 2 configureren](#)
- [WPS-methode 3 configureren](#)

Toepasselijke apparaten

- RV215W

Softwareversie

- 1.1.0.5

Basisconfiguratie-instellingen

Algemene instellingen

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies Draadloos > Basisinstellingen. De pagina Basisinstellingen wordt geopend:

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

Stap 2. Schakel het selectievakje Inschakelen in het veld Radio in om de draadloze radio in te schakelen.

Stap 3. Kies in de vervolgkeuzelijst Draadloze netwerkmodus de draadloze modus.

- B/G/N-Mixed - Het netwerk bevat een mix van draadloze B-, draadloze G- en draadloze N-apparaten.
- B-Only — Het netwerk bevat alleen draadloze B-apparaten.
- G-Only — Het netwerk bevat alleen draadloze G-apparaten.
- N-Only — Het netwerk bevat alleen draadloze N-apparaten.
- B/G-Mixed - Het netwerk bevat een mix van draadloze B- en draadloze G-apparaten.

- G/N Mixed - Het netwerk bevat een mix van draadloze G- en draadloze N-apparaten.

Stap 4. Als de netwerkmodus draadloze N-apparaten bevat, klikt u op de keuzerondje die overeenkomt met de gewenste bandbreedte van het draadloze signaal in het veld Selectie draadloze band. Hoe hoger de bandbreedte, hoe groter de hoeveelheid gegevens die het signaal kan dragen.

- 20 MHz - De standaardfrequentie voor een draadloos signaal.
- 20/40 MHz — gebruikt automatisch een signaal van 20 MHz en 40 MHz. Een 40 MHz-sig-naal biedt meer bandbreedte, maar is vatbaar voor meer interferentie. Deze optie wordt alleen gebruikt als de aangesloten draadloze apparaten compatibel zijn met een frequentie van 40 MHz.

Stap 5. Kies in de vervolgkeuzelijst Wireless Channel een draadloos kanaal voor de radio. Kies een kanaal dat momenteel niet wordt gebruikt door naburige netwerken.

Stap 6. Kies in de vervolgkeuzelijst AP Management VLAN een VLAN dat het beheer-VLAN wordt.

Stap 7. (Optioneel) Schakel Inschakelen in het U-APSD-veld in om Ongeplande automatische energiebesparingslevering (U-APSD) in te schakelen. U-APSD is een functie waarmee de radio energie kan besparen. U-APSD kan echter de doorvoerprestaties van de radio verlagen.

Stap 8. Klik op Save (Opslaan).

Draadloze tabel bewerken

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies Draadloos > Basisinstellingen. De pagina Basisinstellingen wordt geopend:

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	☐	☒	☐

Stap 2. Schakel het selectievakje in van het netwerk dat u wilt bewerken in de Draadloze tabel.

Stap 3. Klik op Bewerken om het opgegeven netwerk te bewerken.

Stap 4. Klik op de knop SSID inschakelen om het netwerk in te schakelen. Service Set Identifier (SSID) is de naam van het draadloze netwerk.

Stap 5. Voer de naam van het netwerk in het veld SSID-naam in. Alle apparaten in het netwerk moeten deze SSID gebruiken om met elkaar te communiceren.

Stap 6. Controleer SSID-broadcast om draadloze broadcast in te schakelen. De RV215W maakt reclame voor de beschikbaarheid ervan voor draadloze apparaten in de buurt wanneer SSID-uitzending is ingeschakeld.

Stap 7. Controleer het gastnetwerk om van het geconfigureerde netwerk een gastnetwerk te maken. Een gastnetwerk is een klein deel van een netwerk dat is ontworpen voor tijdelijke gebruikers. Dit wordt gebruikt om gasten in staat te stellen het netwerk te gebruiken zonder de noodzaak om privé Wi-Fi-sleutels bloot te leggen.

Opmerking: Het gastnetwerk kan niet worden geconfigureerd op het VLAN voor AP-beheer.

Stap 8. Kies in de vervolgkeuzelijst VLAN de VLAN die aan het netwerk is gekoppeld.

Stap 9. Controleer de draadloze isolatie met SSID om te voorkomen dat apparaten in het opgegeven netwerk met elkaar communiceren.

Stap 10. Controleer WMM om Wi-Fi Multimedia (WMM) in het netwerk in te schakelen. WMM wordt gebruikt om het streamen van multimedia via draadloze apparaten te verbeteren. WMM geeft multimedieverkeer dat via een draadloze verbinding wordt verzonden, een hogere prioriteit.

Stap 11. (Optioneel) Controleer WPS om het opgegeven netwerk toe te wijzen als een Wi-Fi Protected Setup (WPS)-netwerk. WPS is een functie die een eenvoudige en veilige netwerkconfiguratie mogelijk maakt. Met deze functie kunnen apparaten eenvoudig verbinding maken met het netwerk.

Stap 12. Klik op Save (Opslaan).

Beveiliging uitschakelen

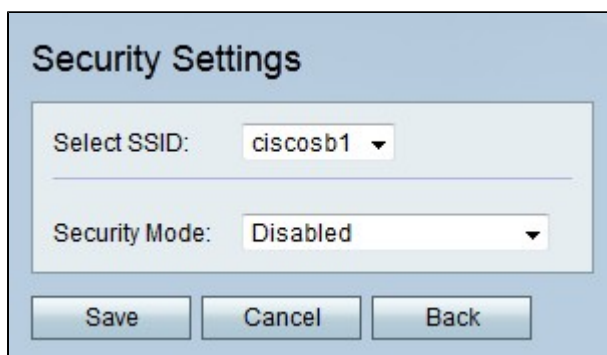
Draadloze beveiliging kan op de RV215W worden uitgeschakeld voor gebruiksgemak bij het instellen van testnetwerken, maar het uitschakelen van de beveiliging wordt niet aanbevolen.

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies Draadloos > Basisinstellingen. De pagina Basisinstellingen wordt geopend.

Stap 2. Schakel het selectievakje in van het netwerk dat u wilt bewerken.

Stap 3. Klik op Beveiligingsmodus bewerken om de beveiliging van het opgegeven netwerk te bewerken. De pagina Beveiligingsinstellingen wordt geopend:

Stap 4. (Optioneel) Kies in de vervolgkeuzelijst Selecteer de SSID waarvoor u de beveiliging wilt configureren.



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".

Stap 5. Kies Uitgeschakeld in de vervolgkeuzelijst Beveiligingsmodus. De beveiliging is uitgeschakeld voor het draadloze netwerk.

Stap 6. Klik op Save (Opslaan).

WEP-beveiliging configureren

Wired Equivalent Privacy (WEP) is een algoritme dat een draadloos netwerk beveiligt. WEP biedt een eenvoudige coderingsmethode die minder veilig is dan WPA. WEP wordt gebruikt wanneer aangesloten netwerkapparaten WPA niet ondersteunen.

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies Draadloos > Basisinstellingen. De pagina Basisinstellingen wordt geopend.

Stap 2. Schakel het selectievakje in van het netwerk dat u wilt bewerken.

Stap 3. Klik op Beveiligingsmodus bewerken om de beveiliging van het opgegeven netwerk te bewerken. De pagina Beveiligingsinstellingen wordt geopend:



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".

Stap 4. (Optioneel) Kies in de vervolgkeuzelijst Selecteer de SSID waarvoor u de beveiliging wilt configureren.

Stap 5. Kies in de vervolgkeuzelijst Beveiligingsmodus WEP.

Stap 6. Kies in de vervolgkeuzelijst Type verificatie een verificatietype voor het draadloze netwerk.

- Open systeem: iedereen kan een verbinding maken met het toegangspunt, maar de WEP-sleutel is nodig om verkeer door het toegangspunt van het netwerk te leiden.
- Gedeelde sleutel - Een WEP-sleutel is nodig om verbinding te maken met het toegangspunt en om verkeer door het toegangspunt van het netwerk te leiden.

Stap 7. Kies in de vervolgkeuzelijst Codering een coderingsmethode voor de WEP-sleutel.

- 10/64-bits (10 hexadecimale cijfers) — Biedt een 40-bits sleutel.
- 26/128-bits (26 hexadecimale cijfers) — Biedt een 104-bits sleutel. Dit is de veiligere encryptie.

Stap 8. Voer in het veld Wachtwoordgroep een wachtwoordzin in die groter is dan acht tekens.

Stap 9. Klik op Genereren om sleutels te maken in de velden Sleutel 1, Sleutel 2, Sleutel 3 en Sleutel 4.

Opmerking: U kunt ook handmatig sleutels invoeren in de velden Sleutel 1, Sleutel 2, Sleutel 3 en Sleutel 4.

Stap 10. Kies in de vervolgkeuzelijst TX-sleutel de sleutel die gebruikers moeten invoeren om toegang te krijgen tot het draadloze netwerk.

Stap 11. (Optioneel) Controleer Wachtwoord ontmaskeren om de tekenreeksen van de toetsen te onthullen.

Stap 12. Klik op Save (Opslaan).

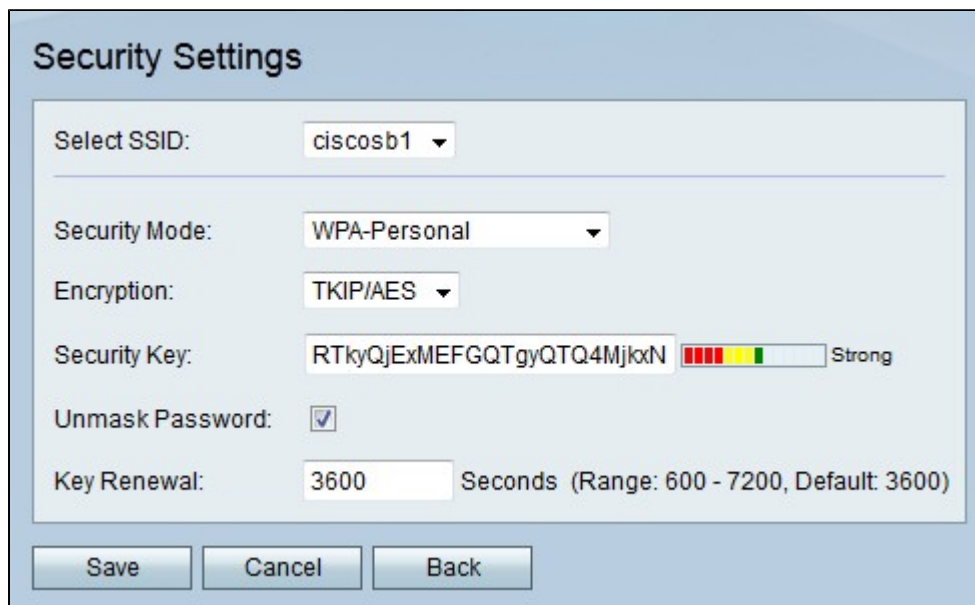
WPA-Personal Security configureren

Wi-Fi Protected Access (WPA) is een beveiligingsstandaard voor draadloze netwerken. WPA is gemaakt om WEP te vervangen vanwege de beveiligingsfouten in WEP. WPA-Personal is een versie van WPA die wordt gebruikt voor netwerken met slechts een paar gebruikers. WPA-Personal biedt een gedeelde sleutel die elke gebruiker zal gebruiken om toegang te krijgen tot het draadloze netwerk. WPA werd geïntroduceerd met de belangrijkste encryptiemethoden Temporal Key Integrity Protocol (TKIP) en Advanced Encryption Standard (AES). Meer netwerkapparaten ondersteunen TKIP, maar AES is de sterkere coderingsmethode.

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies Draadloos > Basisinstellingen. De pagina Basisinstellingen wordt geopend.

Stap 2. Schakel het selectievakje in van het netwerk dat u wilt bewerken.

Stap 3. Klik op Beveiligingsmodus bewerken om de beveiliging van het opgegeven netwerk te bewerken. De pagina Beveiligingsinstellingen wordt geopend:



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

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

At the bottom of the window are three buttons: 'Save', 'Cancel', and 'Back'.

Stap 4. (Optioneel) Kies in de vervolgkeuzelijst Selecteer de SSID waarvoor u de beveiliging wilt configureren.

Stap 5. Kies in de vervolgkeuzelijst Beveiligingsmodus WPA-Personal.

Stap 6. Kies in de vervolgkeuzelijst Codering een coderingsmethode voor de WPA-sleutel.

- TKIP/AES — Deze optie wordt gekozen wanneer niet alle apparaten die zijn aangesloten op het draadloze netwerk AES ondersteunen.
- AES — Deze optie heeft de voorkeur als alle apparaten die zijn aangesloten op de draadloze apparaten AES ondersteunen.

Stap 7. Voer een beveiligingssleutel in het veld Beveiligingssleutel in.

Stap 8. (Optioneel) Controleer Wachtwoord ontmaskeren om de tekenreeks van de sleutel te onthullen.

Stap 9. Voer een tijd in het veld Vernieuwing sleutel in. Dit is de hoeveelheid tijd die de RV215W

de sleutel zal gebruiken voordat deze een nieuwe genereert.

Stap 10. Klik op Save (Opslaan).

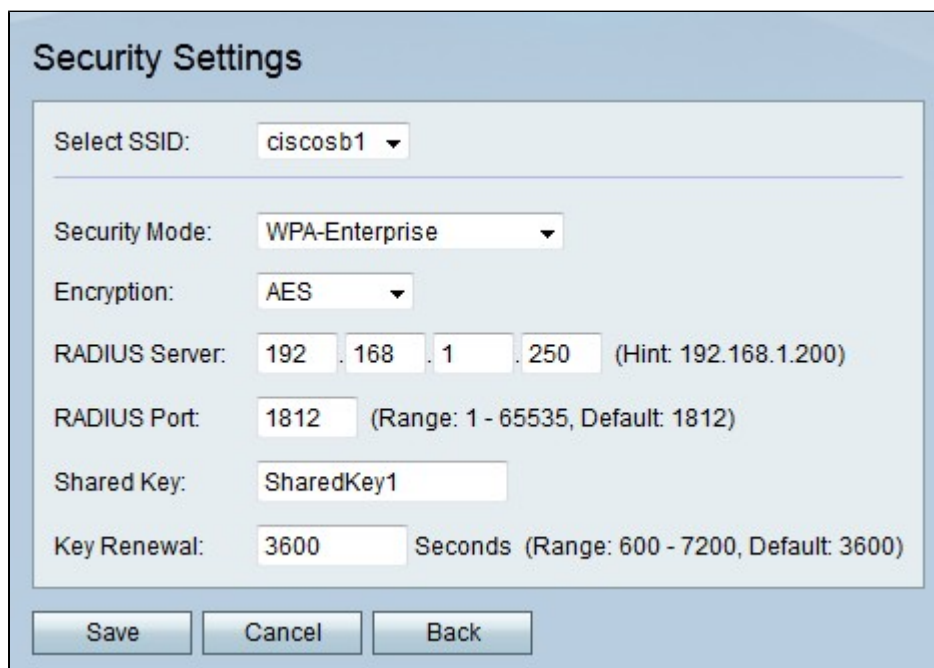
WPA-Enterprise Security configureren

Wi-Fi Protected Access (WPA) is een beveiligingsstandaard voor draadloze netwerken. WPA is gemaakt om WEP te vervangen vanwege de beveiligingsfouten in WEP. WPA-Enterprise is een versie van WPA die wordt aanbevolen voor een netwerk met veel gebruikers, zoals een bedrijf. De verificatie die wordt gebruikt om toegang te krijgen, wordt beheerd door een RADIUS-server. Dit betekent dat elke aangesloten gebruiker een unieke sleutel krijgt om toegang te krijgen tot het draadloze netwerk. WPA werd geïntroduceerd met de belangrijkste encryptiemethoden Temporal Key Integrity Protocol (TKIP) en Advanced Encryption Standard (AES). Meer netwerkapparaten ondersteunen TKIP, maar AES is de sterkere coderingsmethode.

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies Draadloos > Basisinstellingen. De pagina Basisinstellingen wordt geopend.

Stap 2. Schakel het selectievakje in van het netwerk dat u wilt bewerken.

Stap 3. Klik op Beveiligingsmodus bewerken om de beveiliging van het opgegeven netwerk te bewerken. De pagina Beveiligingsinstellingen wordt geopend:



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 "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 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 "Seconds" and a range note "(Range: 600 - 7200, Default: 3600)".

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

Stap 4. (Optioneel) Kies in de vervolgkeuzelijst Selecteer de SSID waarvoor u de beveiliging wilt configureren.

Stap 5. Kies in de vervolgkeuzelijst Beveiligingsmodus WPA-Enterprise.

Stap 6. Kies in de vervolgkeuzelijst Codering een coderingsmethode voor de WPA-sleutel.

- TKIP/AES — Deze optie wordt gekozen wanneer niet alle apparaten die zijn aangesloten op het draadloze netwerk AES ondersteunen.
- AES — Deze optie heeft de voorkeur als alle apparaten die zijn aangesloten op de draadloze apparaten AES ondersteunen.

Stap 7. Voer het IP-adres van de RADIUS-server in het veld RADIUS-server in.

Stap 8. Voer het poortnummer in dat wordt gebruikt om toegang te krijgen tot de RADIUS-server in het veld RADIUS-poort.

Stap 9. Voer de vooraf gedeelde sleutel in voor de draadloze gebruikers in het veld Gedeelde sleutel. Een vooraf gedeelde sleutel is een sleutel die voor alle gebruikers wordt gebruikt. De vooraf gedeelde sleutelfunctie is een extra beveiligingsfunctie naast de RADIUS-verificatie.

Stap 10. Voer een tijd in het veld Vernieuwing sleutel in. Dit is de hoeveelheid tijd die de RV215W de sleutel zal gebruiken voordat deze een nieuwe genereert.

Stap 11. Klik op Save (Opslaan).

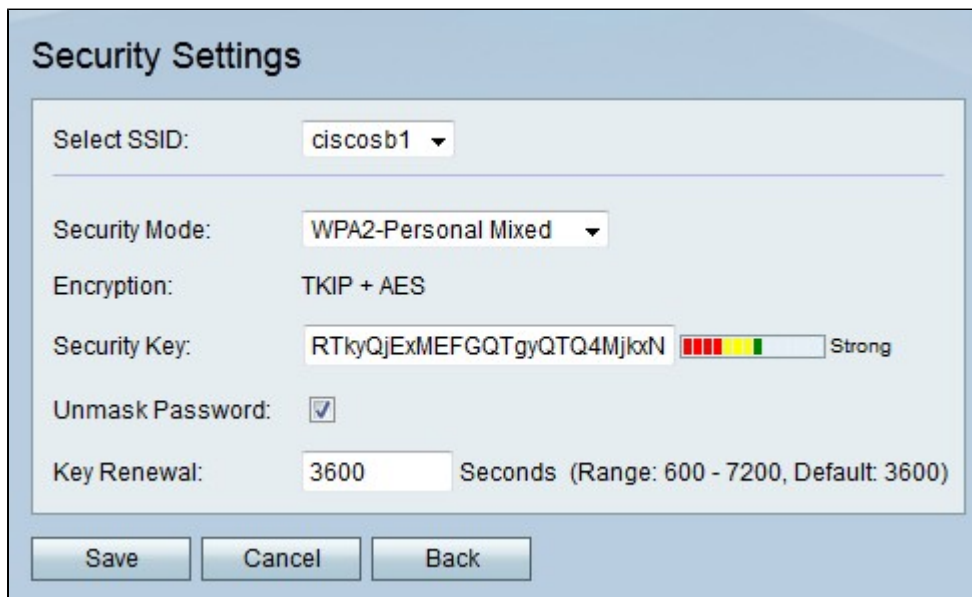
WPA2-Personal/WPA2-Personal Mixed Security configureren

Wi-Fi Protected Access 2 (WPA2) is een beveiligingsstandaard voor draadloze netwerken. WPA2 is een uitbreiding van WPA. WPA2 biedt meer beveiliging dan WPA, maar WPA2 vereist meer verwerkingskracht. WPA2-Personal/WPA2-Personal Mixed zijn versies van WPA2 die worden gebruikt voor netwerken met weinig gebruikers. WPA2-Personal Mixed is ontworpen voor achterwaartse compatibiliteit voor oudere apparaten die geen WPA2 kunnen gebruiken. Gebruik indien mogelijk WPA2-Personal Mixed niet, omdat het een minder veilige verbinding biedt. WPA2-Personal biedt een gedeelde sleutel die elke gebruiker zal gebruiken om toegang te krijgen tot het draadloze netwerk. WPA2 gebruikt de encryptiemethoden Temporal Key Integrity Protocol (TKIP) en Advanced Encryption Standard (AES). Meer netwerkapparaten ondersteunen TKIP, maar AES is de sterkere coderingsmethode.

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies Draadloos > Basisinstellingen. De pagina Basisinstellingen wordt geopend.

Stap 2. Schakel het selectievakje in van het netwerk dat u wilt bewerken.

Stap 3. Klik op Beveiligingsmodus bewerken om de beveiliging van het opgegeven netwerk te bewerken. De pagina Beveiligingsinstellingen wordt geopend:



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

- Select SSID:** A dropdown menu showing 'ciscosb1'.
- Security Mode:** A dropdown menu showing 'WPA2-Personal Mixed'.
- Encryption:** A text field showing 'TKIP + AES'.
- Security Key:** A text field showing 'RTkyQjExMEFGQTgyQTQ4MjlxN' with a strength indicator (four red bars, one yellow, one green) and the label 'Strong'.
- Unmask Password:** A checkbox that is checked.
- Key Renewal:** A text field showing '3600' with the label 'Seconds (Range: 600 - 7200, Default: 3600)'.

At the bottom of the dialog box are three buttons: 'Save', 'Cancel', and 'Back'.

Stap 4. (Optioneel) Kies in de vervolgkeuzelijst Selecteer de SSID waarvoor u de beveiliging wilt configureren.

Stap 5. Kies in de vervolgkeuzelijst Beveiligingsmodus WPA2-Personal of WPA2-Personal Mixed. WPA2-Personal wordt gebruikt wanneer alle apparaten op het draadloze netwerk AES ondersteunen. WPA2-Personal Mixed wordt gebruikt wanneer niet alle apparaten AES ondersteunen.

Opmerking: Het type codering dat door de beveiligingsmethode wordt gebruikt, wordt weergegeven in het veld Codering.

Stap 6. Voer een beveiligingssleutel in het veld Beveiligingssleutel in.

Stap 7. (Optioneel) Controleer Wachtwoord ontmaskeren om de tekenreeksen van de sleutel te onthullen.

Stap 8. Voer een tijd in het veld Vernieuwing sleutel in. Dit is de hoeveelheid tijd die de RV215W de sleutel zal gebruiken voordat deze een nieuwe genereert.

Stap 9. Klik op Save (Opslaan).

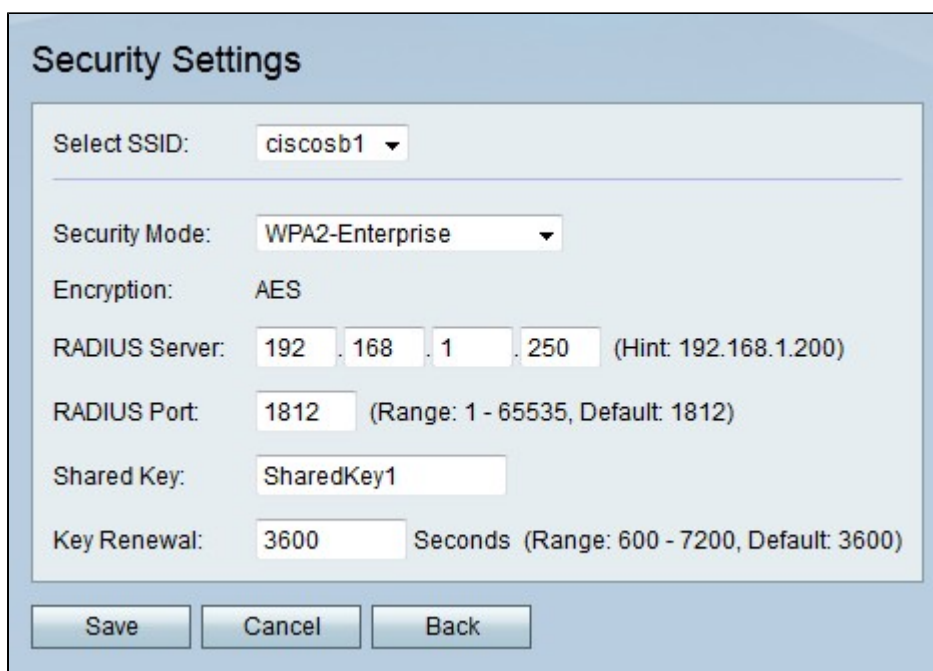
Gemengde beveiliging WPA2-Enterprise/WPA2-Enterprise configureren

Wi-Fi Protected Access 2 (WPA2) is een beveiligingsstandaard voor draadloze netwerken. WPA2 is een uitbreiding van WPA. WPA2 biedt meer beveiliging dan WPA, maar WPA2 vereist meer verwerkingskracht. WPA2-Enterprise / WPA2-Enterprise Mixed zijn versies van WPA2 die worden gebruikt voor netwerken met veel gebruikers, zoals een bedrijf. WPA2-Enterprise Mixed is ontworpen voor achterwaartse compatibiliteit voor oudere apparaten die geen WPA2 kunnen gebruiken. Gebruik indien mogelijk WPA2-Enterprise Mixed niet, omdat dit een minder veilige verbinding biedt. De verificatie om te bepalen of een gebruiker toegang krijgt, wordt beheerd door een RADIUS-server. Dit betekent dat elke aangesloten gebruiker een unieke sleutel krijgt om toegang te krijgen tot het draadloze netwerk. WPA2 gebruikt de encryptiemethoden Temporal Key Integrity Protocol (TKIP) en Advanced Encryption Standard (AES). Meer netwerkapparaten ondersteunen TKIP, maar AES is de sterkere coderingsmethode.

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies Draadloos > Basisinstellingen. De pagina Basisinstellingen wordt geopend.

Stap 2. Schakel het selectievakje in van het netwerk dat u wilt bewerken.

Stap 3. Klik op Beveiligingsmodus bewerken om de beveiliging van het opgegeven netwerk te bewerken. De pagina Beveiligingsinstellingen wordt geopend:



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 "WPA2-Enterprise" selected.
- Encryption:** A text field with "AES" entered.
- RADIUS Server:** Four input fields containing "192", "168", "1", and "250", followed by a hint "(Hint: 192.168.1.200)".
- RADIUS Port:** An input field with "1812" and a range note "(Range: 1 - 65535, Default: 1812)".
- Shared Key:** An input field with "SharedKey1" entered.
- Key Renewal:** An input field with "3600" and a range note "(Range: 600 - 7200, Default: 3600)".

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

Stap 4. (Optioneel) Kies in de vervolgkeuzelijst Selecteer de SSID waarvoor u de beveiliging wilt configureren.

Stap 5. Kies in de vervolgkeuzelijst Beveiligingsmodus WPA2-Enterprise of WPA2-Enterprise Mixed. WPA2-Enterprise wordt gebruikt wanneer alle apparaten op het draadloze netwerk AES ondersteunen. WPA2-Enterprise Mixed wordt gebruikt wanneer niet alle apparaten AES ondersteunen.

Opmerking: Het type codering dat door de beveiligingsmethode wordt gebruikt, wordt weergegeven in het veld Codering.

Stap 6. Voer het IP-adres van de RADIUS-server in het veld RADIUS-server in.

Stap 7. Voer de poort in die wordt gebruikt om toegang te krijgen tot de RADIUS-server in het veld RADIUS-poort.

Stap 8. Voer de vooraf gedeelde sleutel in voor de draadloze gebruikers in het veld Gedeelde sleutel. Een vooraf gedeelde sleutel is een sleutel die voor alle gebruikers wordt gebruikt. De vooraf gedeelde sleutelfunctie is een extra beveiligingsfunctie naast de RADIUS-verificatie.

Stap 9. Voer een tijd in het veld Vernieuwing sleutel in. Dit is de hoeveelheid tijd die de RV215W de sleutel zal gebruiken voordat deze een nieuwe genereert.

Stap 10. Klik op Save (Opslaan).

MAC-filtering bewerken

MAC-filtering wordt gebruikt om toegang tot het draadloze netwerk toe te staan of te weigeren op basis van het MAC-adres van het verbindingsapparaat.

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies Draadloos > Basisinstellingen. De pagina Basisinstellingen wordt geopend:

The screenshot shows the 'Basic Settings' page of a web configuration utility. The 'Radio' section is expanded, showing settings for 'Enable', 'Wireless Network Mode', 'Wireless Band Selection', 'Wireless Channel', 'AP Management VLAN', and 'U-APSD (WMM Power Save)'. Below this is a 'Wireless Table' with columns for 'Enable SSID', 'SSID Name', 'SSID Broadcast', 'Security Mode', 'MAC Filter', 'Guest Network', 'VLAN', 'Wireless Isolation with SSID', 'WMM', and 'WPS'. The table contains four rows of wireless networks. The first row is highlighted in green. Below the table are buttons for 'Edit', 'Edit Security Mode', 'Edit MAC Filtering' (highlighted with a red circle), 'Time of Day Access', 'Edit Guest Net', and 'Edit WPS'. At the bottom are 'Save' and 'Cancel' buttons.

	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	☐	☒	☐

Stap 2. Schakel het selectievakje in van het netwerk dat u wilt bewerken.

Stap 3. Klik op MAC-filtering bewerken om de MAC-toegangscontrolelijst voor het opgegeven netwerk te maken. De pagina Draadloos MAC-filter wordt geopend:

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

Stap 4. Schakel Inschakelen in om MAC-filtering in het netwerk in te schakelen.

Stap 5. Klik op het keuzerondje dat overeenkomt met het gewenste lijsttype in het veld Verbindingsbeheer.

- Voorkomen dat pc's met de vermelde MAC-adressen het netwerk binnenkomen.
- Sta pc's toe - Hiermee kunnen pc's met de vermelde MAC-adressen het netwerk betreden.

Stap 6. Voer de gewenste MAC-adressen in de MAC-adrestabel in.

Stap 7. Klik op Save (Opslaan).

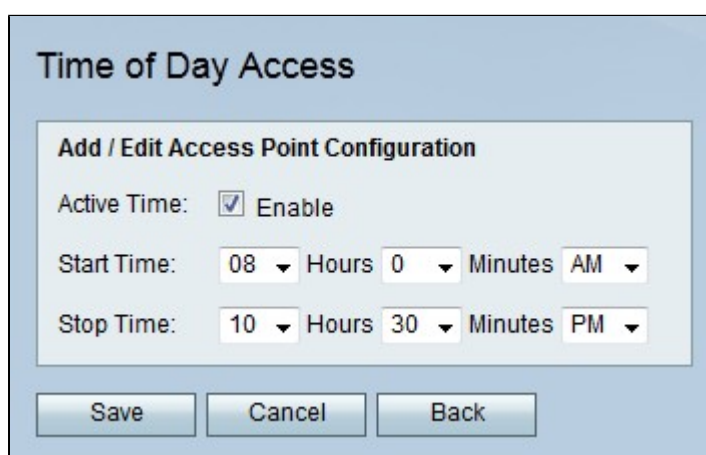
Tijdstip van de dag Toegang

De Time of Day Access-functie wordt gebruikt om alleen toegang toe te staan aan gebruikers op basis van een geconfigureerd schema.

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies Draadloos > Basisinstellingen. De pagina Basisinstellingen wordt geopend:

Stap 2. Schakel het selectievakje in van het netwerk dat u wilt bewerken.

Stap 3. Klik op Time of Day Access om te configureren wanneer gebruikers toegang hebben tot het opgegeven netwerk. De pagina Time of Day Access wordt geopend:



The screenshot shows a web-based configuration window titled "Time of Day Access". Inside the window, there is a section titled "Add / Edit Access Point Configuration". Below this title, there is a checkbox labeled "Active Time:" which is checked and followed by the word "Enable". Below the checkbox, there are two rows of time selection controls. The first row is for "Start Time:" and shows "08" for Hours, "0" for Minutes, and "AM" for the period. The second row is for "Stop Time:" and shows "10" for Hours, "30" for Minutes, and "PM" for the period. At the bottom of the window, there are three buttons: "Save", "Cancel", and "Back".

Stap 4. Schakel het selectievakje Inschakelen in het veld Actieve tijd in om de tijd van de dag voor toegang tot het netwerk in te schakelen.

Stap 5. Voer in het veld Begintijd het tijdstip in waarop de toegang tot het netwerk begint.

Stap 6. Voer het tijdstip in waarop de toegang tot het netwerk eindigt in het veld Stoptijd.

Stap 7. Klik op Save (Opslaan).

Gastnetwerk bewerken

Een gastnetwerk is een klein deel van een netwerk dat is ontworpen voor tijdelijke gebruikers. Dit wordt gebruikt om gasten in staat te stellen het netwerk te gebruiken zonder de noodzaak om privé Wi-Fi-sleutels bloot te leggen. Een gastnetwerk kan worden geconfigureerd om de toegangstijd en het bandbreedtegebruik van een gebruiker te beperken.

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies Draadloos > Basisinstellingen. De pagina Basisinstellingen wordt geopend:

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

Stap 2. Klik op Gastnetwerk bewerken om het gastnetwerk te configureren. De pagina Gastnetwerk-instellingen wordt geopend:

Guest Net Settings

Guest Net Name:

Guest Password: Secure

Confirm Guest Password:

Guest Access Time: 240 Minutes (Range: 30 - 1440, Default: 120)

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

Available Bandwidth: 30 % (Range: 1 - 99, Default: 20)

Stap 3. Voer een wachtwoord in dat de gebruikers zullen gebruiken om het gastnetwerk in te voeren in het veld Gastwachtwoord.

Stap 4. Voer het wachtwoord opnieuw in dat de gebruikers zullen gebruiken om het gastnetwerk in te voeren in het veld Gastwachtwoord bevestigen.

Stap 5. Geef de tijd op waarop de gebruikers verbinding mogen houden met het gastnetwerk in de tijd voor gasttoegang.

Stap 6. Schakel Gastbandbreedtebeperking inschakelen in om de hoeveelheid bandbreedte die het gastnetwerk ontvangt te beperken.

Opmerking: Bandbreedtebeheer moet zijn ingeschakeld op de pagina Bandbreedtebeheer.

Stap 7. Voer het percentage van de bandbreedte in dat beschikbaar moet zijn voor het gastnetwerk in het veld Beschikbare bandbreedte.

Stap 8. Klik op Save (Opslaan).

WPS-methode 1 configureren

Wi-Fi Protected Setup (WPS) is een functie die een eenvoudige en veilige draadloze netwerkinstallatie biedt. Om verbinding te maken met WPS, moet het verbindingsapparaat WPS ondersteunen en compatibel zijn met WPA-beveiliging. De eerste configuratiemethode is een eenvoudige methode waarbij de RV215W WPS-knop en de knop voor het clientapparaat moeten worden ingedrukt. Zodra beide knoppen zijn ingedrukt, wordt het clientapparaat verbonden met

het WPS-netwerk.

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies Draadloos > Basisinstellingen. De pagina Basisinstellingen wordt geopend:

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

Stap 2. Klik op WPS bewerken om WPS te configureren. De pagina WPS wordt geopend:

Opmerking: De WPS-pagina is ook toegankelijk via Draadloos > 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

Stap 3. Klik op Bewerken om het draadloze netwerk te kiezen waarop u WPS wilt inschakelen.

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

Stap 4. Klik op de WPS-knop op de WPS-pagina.

Stap 5. Klik op de WPS-knop op het clientapparaat of op een hulpscherm van het clientapparaat om het clientapparaat te verbinden met het WPS-netwerk.

De volgende velden geven informatie weer over de WPS-configuratie.

- Wi-Fi Protected Setup Status — De status van de WPS-configuratie.
- Netwerknaam (SSID) — De netwerknaam die door de RV215W aan de WPS-configuratie is toegewezen.
- WPA2-Personal — Het type beveiliging dat de WPS-configuratie gebruikt.

WPS-methode 2 configureren

Wi-Fi Protected Setup (WPS) is een functie die een eenvoudige en veilige draadloze netwerkinstallatie biedt. Om verbinding te maken met WPS, moet het verbindingsapparaat WPS ondersteunen en compatibel zijn met WPA-beveiliging. De tweede methode vereist het pincode-nummer van het clientapparaat. Zodra de pincode is ingevoerd op de WPS-pagina, maakt het clientapparaat verbinding met het WPS-netwerk.

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies Draadloos > Basisinstellingen. De pagina Basisinstellingen wordt geopend:

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

Stap 2. Klik op WPS bewerken om WPS te configureren. De pagina WPS wordt geopend:

Opmerking: De WPS-pagina is ook toegankelijk via Draadloos > 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

Stap 3. Klik op Bewerken om te kiezen op welk draadloos netwerk u WPS wilt inschakelen.

Stap 4. Voer de pincode van het clientapparaat in.

Stap 5. Klik op Registreren om het WPS-netwerk te maken.

De volgende velden geven informatie weer over de WPS-configuratie.

- Wi-Fi Protected Setup Status — De status van de WPS-configuratie.
- Netwerknaam (SSID) — De netwerknaam die door de RV215W aan de WPS-configuratie is toegewezen.
- WPA2-Personal — Het type beveiliging dat de WPS-configuratie gebruikt.

WPS-methode 3 configureren

Wi-Fi Protected Setup (WPS) is een functie die een eenvoudige en veilige draadloze netwerkinstallatie biedt. Om verbinding te maken met WPS, moet het verbindingssapparaat WPS ondersteunen en compatibel zijn met WPA-beveiliging. De derde methode vereist dat de gebruiker het pincode van de RV215W invoert op de WPS-configuratiepagina van het clientapparaat.

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies Draadloos > Basisinstellingen. De pagina Basisinstellingen wordt geopend:

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

Stap 2. Klik op WPS bewerken om WPS te configureren. De pagina WPS wordt geopend:

Opmerking: De WPS-pagina is ook toegankelijk via Draadloos > 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

Stap 3. Klik op Bewerken om te kiezen op welk draadloos netwerk u WPS wilt inschakelen.

Stap 4. Klik op Genereren om een pincode te genereren voor de RV215W.

Stap 5. Kies in de vervolgkeuzelijst PIN Lifetime de tijd die verstrijkt voordat een nieuwe PIN wordt gegenereerd.

Stap 6. Voer het opgegeven RV215W-pincode in de configuratie van het clientapparaat in. Het clientapparaat maakt verbinding met het WPS-netwerk.

De volgende velden geven informatie weer over de WPS-configuratie.

- Wi-Fi Protected Setup Status — De status van de WPS-configuratie.

- Netwerknnaam (SSID) — De netwerknnaam die door de RV215W aan de WPS-configuratie is toegewezen.
- WPA2-Personal — Het type beveiliging dat de WPS-configuratie gebruikt.

Als u alle andere documentatie over de RV215W-router wilt zien, klikt u [hier](#).

Bekijk een video gerelateerd aan dit artikel ...

[Klik hier om nog meer Tech Talks van Cisco te bekijken](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.