

RV215W的基本無線設定配置

目標

無線網路是不通過電纜連線的電腦網路。無線區域網路(WLAN)是一種無線網路，它通過使用無線電通訊在短距離內連結多個裝置。

本文說明如何在RV215W上配置基本無線設定，包括網路安全配置。

索引

- [General Settings](#)
- [編輯無線表](#)
- [禁用安全](#)
- [配置WEP安全](#)
- [配置WPA個人安全性](#)
- [配置WPA — 企業安全](#)
- [配置WPA2 — 個人/WPA2 — 個人混合安全](#)
- [配置WPA2 — 企業/WPA2 — 企業混合安全](#)
- [編輯MAC過濾](#)
- [訪問當天時間](#)
- [編輯訪客網路](#)
- [設定WPS方法1](#)
- [設定WPS方法2](#)
- [設定WPS方法3](#)

適用裝置

- RV215W

軟體版本

- 1.1.0.5

基本設定配置

常規設定

步驟1.登入到Web配置實用程式並選擇無線>基本設定。將開啟Basic Settings頁面：

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

步驟2.選中Radio欄位中的Enable以啟用無線電。

步驟3.從Wireless Network Mode下拉選單選擇無線模式。

- B/G/N-Mixed — 網路包含wireless-B、wireless-G和wireless-N裝置的混合。
- 僅B — 網路僅包含無線 — B裝置。
- G-Only — 網路僅包含wireless-G裝置。
- 僅N — 網路僅包含無線 — N裝置。
- B/G-Mixed — 網路包含wireless-B和wireless-G裝置的混合。
- G/N Mixed — 網路包含wireless-G和wireless-N裝置的混合。

步驟4.如果網路模式包含wireless-N裝置，則在Wireless Band Selection欄位中按一下與無線訊號的所需頻寬對應的單選按鈕。頻寬越高，訊號可傳輸的資料量就越多。

- 20 MHz — 無線訊號的標準頻率。
- 20/40 MHz — 自動使用20 MHz和40 MHz訊號。40 MHz訊號可提供更多頻寬，但容易產生更多干擾。僅當連線的無線裝置與40 MHz頻率相容時，才使用此選項。

步驟5.從Wireless Channel下拉選單中選擇無線電的無線通道。選擇當前未由鄰居網路使用的通道。

步驟6.從AP管理VLAN下拉選單中選擇要成為管理VLAN的VLAN。

步驟7. (可選) 在U-APSD欄位中選中Enable，以啟用未計畫的自動節能交付(U-APSD)。U-APSD是一種允許無線電節省功率的功能。但是，U-APSD可能會降低無線電的吞吐量效能。

步驟8.按一下「Save」。

編輯無線表

步驟1.登入到Web配置實用程式並選擇無線>基本設定。將開啟Basic Settings頁面：

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	☐	☒	☐

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

Buttons: Save, Cancel

步驟2.在Wireless Table中選中要編輯的網路覈取方塊。

步驟3.按一下Edit以編輯指定的網路。

步驟4.按一下Enable SSID按鈕啟用網路。服務組識別碼(SSID)是無線網路的名稱。

步驟5.在SSID名稱欄位中輸入網路名稱。網路中的所有裝置必須使用此SSID相互通訊。

步驟6.檢查SSID Broadcast以啟用無線廣播。啟用SSID廣播時，RV215W會將其可用性通告給附近的無線裝置。

步驟7.檢查訪客網路，將已配置的網路設定為訪客網路。訪客網路是專為臨時使用者設計的網路的一小部分。這用於允許訪客使用網路，而無需暴露私有Wi-Fi金鑰。

附註：無法在AP管理VLAN上配置訪客網路。

步驟8.從VLAN下拉式清單中選擇與網路關聯的VLAN。

步驟9.選中Wireless Isolation with SSID，不允許指定網路上的裝置相互通訊。

步驟10.選中WMM以在網路上啟用Wi-Fi多媒體(WMM)。WMM用於增強無線裝置上的多媒體流。WMM為通過無線連線傳送的多媒體流量提供更高的優先順序。

步驟11. (可選) 檢查WPS，將指定的網路分配為Wi-Fi Protected Setup(WPS)網路。WPS是一種支援簡單而安全的網路配置的功能。此功能使裝置能夠輕鬆連線到網路。

步驟12.按一下「Save」。

禁用安全

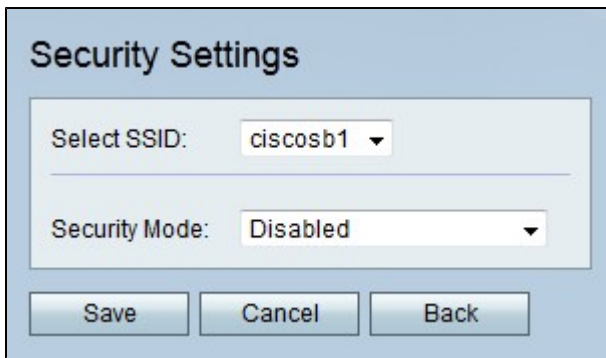
在設定測試網路時，為了便於使用，可能會禁用RV215W上的無線安全功能，但不建議禁用安全功能。

步驟1.登入到Web配置實用程式並選擇無線>基本設定。將開啟Basic Settings頁面。

步驟2.選中要編輯的網路框。

步驟3.按一下Edit Security Mode以編輯指定網路的安全。將開啟Security Settings頁面：

步驟4. (可選) 從Select SSID下拉選單中選擇要為其配置安全性的SSID。

A screenshot of a 'Security Settings' dialog box. It has a light blue header with the title 'Security Settings'. Below the header is a white content area. Inside this area, there is a 'Select SSID:' label followed by a dropdown menu showing 'ciscosb1'. Below that is a 'Security Mode:' label followed by a dropdown menu showing 'Disabled'. At the bottom of the dialog box, there are three buttons: 'Save', 'Cancel', and 'Back'.

步驟5.從「Security Mode」下拉式清單中選擇Disabled。已禁用無線網路的安全性。

步驟6.按一下「Save」。

配置WEP安全

有線等效保密(WEP)是一種保護無線網路的演算法。WEP提供了一種安全性低於WPA的基本加密方法。當連線的網路裝置不支援WPA時，使用WEP。

步驟1.登入到Web配置實用程式並選擇無線>基本設定。將開啟Basic Settings頁面。

步驟2.選中要編輯的網路框。

步驟3.按一下Edit Security Mode以編輯指定網路的安全。將開啟Security Settings頁面：

The image shows a 'Security Settings' dialog box with a light blue header and a white body. At the top, 'Select SSID:' is followed by a dropdown menu showing 'ciscosb1'. Below this is a horizontal line. The 'Security Mode:' dropdown is set to 'WEP'. 'Authentication Type:' is set to 'Open System' with '(Default: Open System)' in parentheses. 'Encryption:' is set to '26/128-bit(26 hex digits)'. The 'Passphrase:' field contains 'passphrase1' and there is a 'Generate' button to its right. Below the passphrase field are four 'Key' fields (Key 1, Key 2, Key 3, Key 4), each with a dotted text input area. The 'TX Key:' dropdown is set to '1'. At the bottom left is an 'Unmask Password:' checkbox, which is unchecked. At the bottom are three buttons: 'Save', 'Cancel', and 'Back'.

步驟4. (可選) 從Select SSID下拉選單中選擇要為其配置安全性的SSID。

步驟5.從「Security Mode」下拉式清單中選擇WEP。

步驟6.從Authentication Type下拉選單中選擇無線網路的身份驗證型別。

- 開放系統 — 任何人都可以與接入點關聯，但需要WEP金鑰才能使流量通過網路的接入點。
- 共用金鑰 — 需要一個WEP金鑰才能與接入點關聯並通過網路接入點的流量。

步驟7.從Encryption下拉選單中，為WEP金鑰選擇加密方法。

- 10/64位 (10個十六進位制數字) — 提供40位金鑰。
- 26/128位 (26個十六進位制數字) — 提供104位金鑰。這是更安全的加密。

步驟8.在「密碼」欄位中輸入大於八個字元的密碼。

步驟9.按一下Generate在Key 1、Key 2、Key 3和Key 4欄位中建立金鑰。

附註：您也可以在Key 1、Key 2、Key 3和Key 4欄位中手動輸入金鑰。

步驟10.從TX Key下拉選單中選擇使用者訪問無線網路時必須輸入的金鑰。

步驟11. (可選) 選中Unmask Password以顯示金鑰的字串。

步驟12.按一下「Save」。

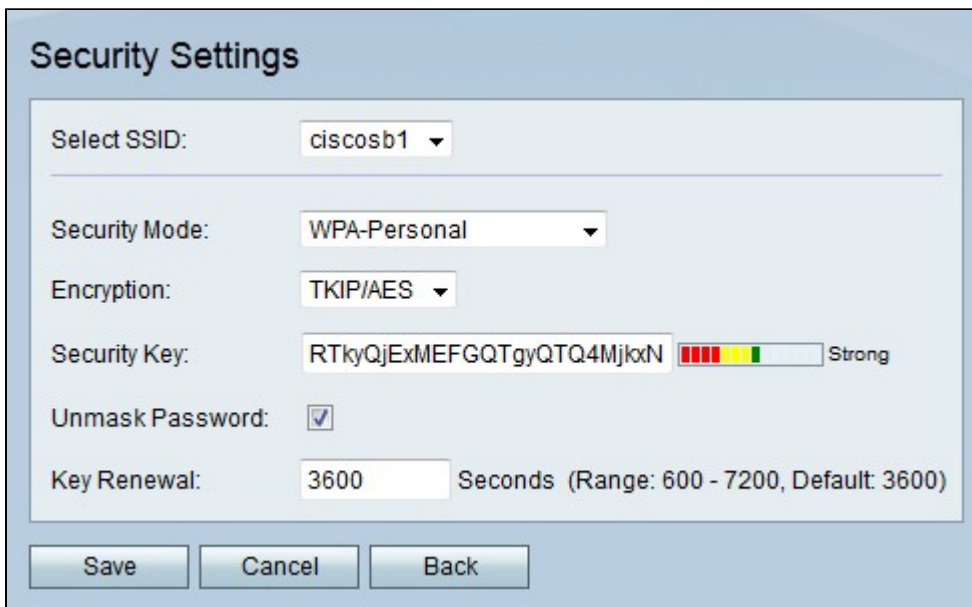
配置WPA個人安全

Wi-Fi保護訪問(WPA)是無線網路的安全標準。由於WEP存在安全缺陷，因此建立了WPA來取代WEP。WPA-Personal是WPA的一個版本，用於只有少數使用者的網路。WPA-Personal提供共用金鑰，每個使用者將使用該金鑰訪問無線網路。WPA引入了金鑰加密方法：臨時金鑰完整性協定(TKIP)和高級加密標準(AES)。更多網路裝置支援TKIP，但AES是更強大的加密方法。

步驟1.登入到Web配置實用程式並選擇無線>基本設定。將開啟Basic Settings頁面。

步驟2.選中要編輯的網路框。

步驟3.按一下Edit Security Mode以編輯指定網路的安全。將開啟Security Settings頁面：



步驟4. (可選) 從Select SSID下拉選單中選擇要為其配置安全性的SSID。

步驟5.從「Security Mode」下拉選單中選擇WPA-Personal。

步驟6.從Encryption下拉選單中，為WPA金鑰選擇加密方法。

- TKIP/AES — 當並非所有連線到無線網路的裝置都支援AES時，會選擇此選項。
- AES — 如果連線到無線裝置的所有裝置都支援AES，則首選此選項。

步驟7.在「安全金鑰」欄位中輸入安全金鑰。

步驟8. (可選) 選中Unmask Password以顯示金鑰的字串。

步驟9.在Key Renewal欄位中輸入時間。這是RV215W在生成新金鑰之前使用金鑰的時間。

步驟10.按一下「Save」。

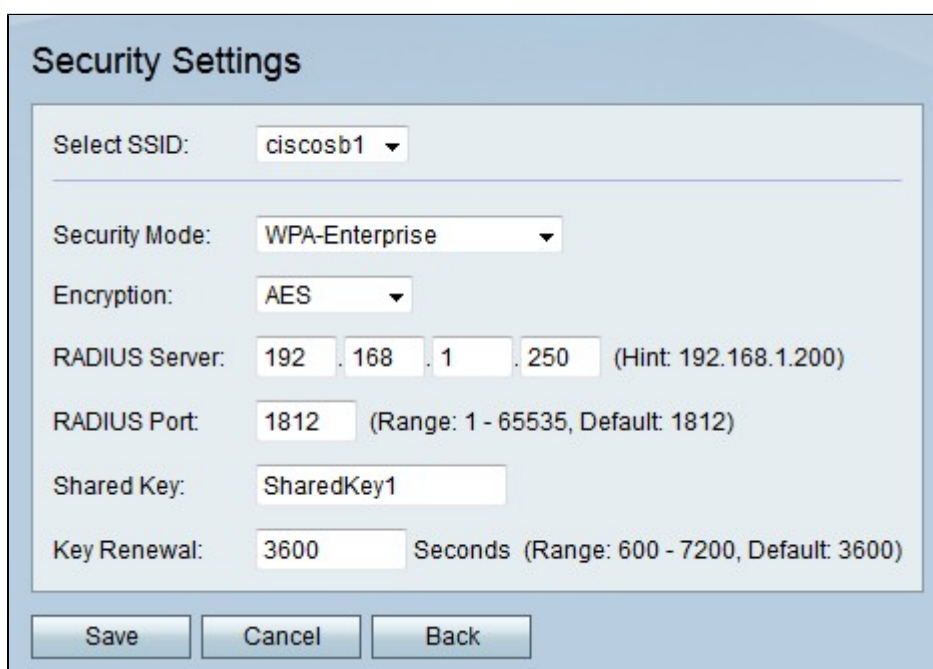
配置WPA — 企業安全

Wi-Fi保護訪問(WPA)是無線網路的安全標準。由於WEP存在安全缺陷，因此建立了WPA來取代WEP。WPA-Enterprise是WPA的一個版本，建議用於具有許多使用者 (如企業) 的網路。用於獲取訪問許可權的身份驗證由RADIUS伺服器控制。這意味著每個連線的使用者都將獲得訪問無線網路的唯一金鑰。WPA引入了金鑰加密方法：臨時金鑰完整性協定(TKIP)和高級加密標準(AES)。更多網路裝置支援TKIP，但AES是更強大的加密方法。

步驟1.登入到Web配置實用程式並選擇無線>基本設定。將開啟Basic Settings頁面。

步驟2.選中要編輯的網路框。

步驟3.按一下Edit Security Mode以編輯指定網路的安全。將開啟Security Settings頁面：



The screenshot shows the 'Security Settings' window. It contains the following fields and controls:

- 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 the text '(Hint: 192.168.1.200)'.
- RADIUS Port:** An input field containing '1812', followed by the text '(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)'.
- Buttons:** At the bottom, there are three buttons: 'Save', 'Cancel', and 'Back'.

步驟4. (可選) 從Select SSID下拉選單中選擇要為其配置安全性的SSID。

步驟5.從「Security Mode」下拉選單中選擇WPA-Enterprise。

步驟6.從Encryption下拉選單中，為WPA金鑰選擇加密方法。

- TKIP/AES — 當並非所有連線到無線網路的裝置都支援AES時，會選擇此選項。
- AES — 如果連線到無線裝置的所有裝置都支援AES，則首選此選項。

步驟7.在「RADIUS伺服器」欄位中輸入RADIUS伺服器的IP地址。

步驟8.在「RADIUS埠」欄位中輸入用於訪問RADIUS伺服器的埠號。

步驟9.在「共用金鑰」欄位中輸入無線使用者的預共用金鑰。預共用金鑰是供所有使用者使用的金鑰。預共用金鑰功能是與RADIUS驗證一起新增的安全功能。

步驟10.在Key Renewal欄位中輸入時間。這是RV215W在生成新金鑰之前使用金鑰的時間。

步驟11.按一下「Save」。

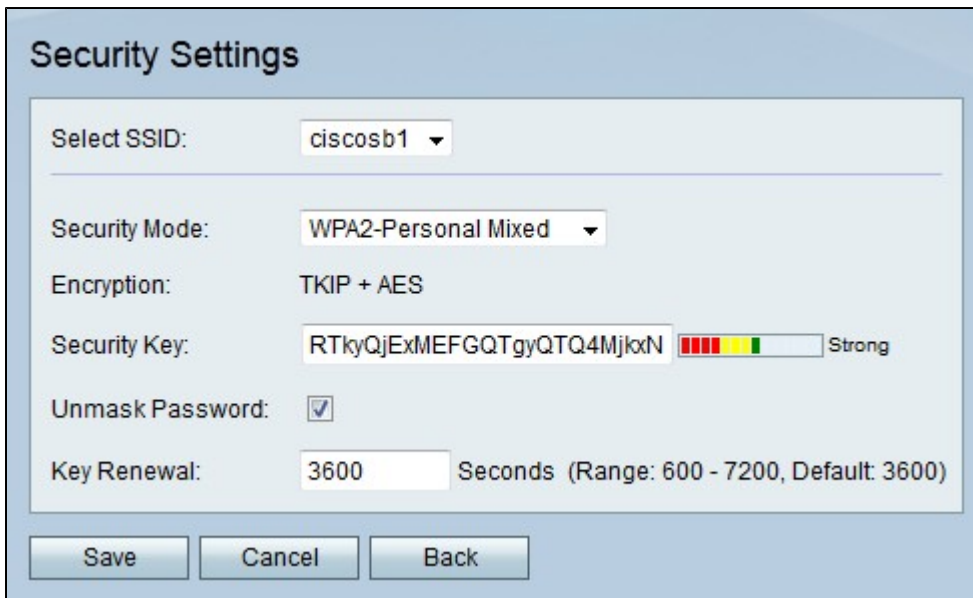
配置WPA2 — 個人/WPA2 — 個人混合安全

Wi-Fi保護訪問2(WPA2)是無線網路的安全標準。WPA2是WPA的增強功能。WPA2比WPA更安全，但WPA2需要更多的處理能力。WPA2 — 個人/WPA2 — 個人Mixed是WPA2的版本，用於使用者數很少的網路。WPA2-Personal Mixed旨在為不能使用WPA2的舊裝置提供向後相容性。如果可能，請勿使用WPA2-Personal Mixed，因為它提供的連線安全性較低。WPA2-Personal提供共用金鑰，每個使用者將使用該金鑰訪問無線網路。WPA2使用臨時金鑰完整性協定(TKIP)和高級加密標準(AES)加密方法。更多網路裝置支援TKIP，但AES是更強大的加密方法。

步驟1.登入到Web配置實用程式並選擇無線>基本設定。將開啟Basic Settings頁面。

步驟2.選中要編輯的網路框。

步驟3.按一下Edit Security Mode以編輯指定網路的安全。將開啟Security Settings頁面：



步驟4. (可選) 從Select SSID下拉選單中選擇要為其配置安全性的SSID。

步驟5.從「安全模式」下拉選單中選擇WPA2-Personal或WPA2-Personal Mixed。當無線網路上的所有裝置都支援AES時，使用WPA2-Personal。當並非所有裝置都支援AES時，使用WPA2-Personal Mixed。

附註：安全方法使用的加密型別將顯示在「加密」欄位中。

步驟6.在Security Key欄位中輸入安全金鑰。

步驟7. (可選) 勾選Unmask Password以顯示金鑰的字串。

步驟8.在Key Renewal欄位中輸入時間。這是RV215W在生成新金鑰之前使用金鑰的時間。

步驟9.按一下「Save」。

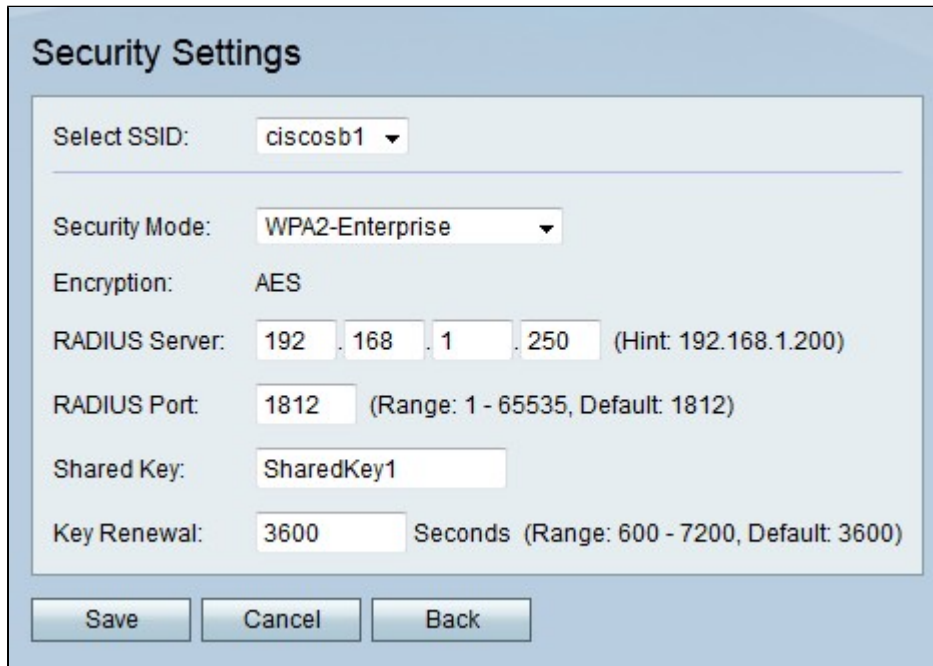
配置WPA2 — 企業/WPA2 — 企業混合安全

Wi-Fi保護訪問2(WPA2)是無線網路的安全標準。WPA2是WPA的增強功能。WPA2比WPA更安全，但WPA2需要更多的處理能力。WPA2 — 企業/WPA2 — 企業混合是WPA2的版本，用於具有許多使用者 (如企業) 的網路。WPA2 — 企業混合是為不能使用WPA2的較舊裝置提供向後相容而設計的。如果可能，不要使用WPA2 — 企業混合，因為它提供的連線安全性較低。確定使用者是否獲得訪問許可權的身份驗證由RADIUS伺服器控制。這意味著每個連線的使用者都將獲得訪問無線網路的唯一金鑰。WPA2使用臨時金鑰完整性協定(TKIP)和高級加密標準(AES)加密方法。更多網路裝置支援TKIP，但AES是更強大的加密方法。

步驟1.登入到Web配置實用程式並選擇無線>基本設定。將開啟Basic Settings頁面。

步驟2.選中要編輯的網路框。

步驟3.按一下Edit Security Mode以編輯指定網路的安全。將開啟Security Settings頁面：

The image shows a 'Security Settings' dialog box with a light blue header and a white body. Inside the body, there are several configuration fields: 'Select SSID:' with a dropdown menu showing 'ciscosb1'; 'Security Mode:' with a dropdown menu showing 'WPA2-Enterprise'; 'Encryption:' with a text field showing 'AES'; 'RADIUS Server:' with four text fields containing '192', '168', '1', and '250', followed by a hint '(Hint: 192.168.1.200)'; 'RADIUS Port:' with a text field containing '1812' and a range note '(Range: 1 - 65535, Default: 1812)'; 'Shared Key:' with a text field containing 'SharedKey1'; and 'Key Renewal:' with a text field containing '3600' and a range note '(Range: 600 - 7200, Default: 3600)'. At the bottom of the dialog, there are three buttons: 'Save', 'Cancel', and 'Back'.

步驟4. (可選) 從Select SSID下拉選單中選擇要為其配置安全性的SSID。

步驟5.從「安全模式」下拉選單中選擇WPA2-Enterprise或WPA2-Enterprise Mixed。當無線網路上的所有裝置都支援AES時，使用WPA2-Enterprise。當並非所有裝置都支援AES時，使用WPA2 — 企業混合。

附註：安全方法使用的加密型別將顯示在「加密」欄位中。

步驟6.在「RADIUS伺服器」欄位中輸入RADIUS伺服器的IP地址。

步驟7.在「RADIUS埠」欄位中輸入用於訪問RADIUS伺服器的埠。

步驟8.在「共用金鑰」欄位中輸入無線使用者的預共用金鑰。預共用金鑰是供所有使用者使用的金鑰。預共用金鑰功能是與RADIUS驗證一起新增的安全功能。

步驟9.在Key Renewal欄位中輸入時間。這是RV215W在生成新金鑰之前使用金鑰的時間。

步驟10.按一下「Save」。

編輯MAC過濾

MAC過濾用於根據連線裝置的MAC地址允許或拒絕對無線網路的訪問。

步驟1.登入到Web配置實用程式並選擇無線>基本設定。將開啟Basic Settings頁面：

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

步驟2.選中要編輯的網路框。

步驟3.按一下編輯MAC過濾以建立指定網路的MAC訪問控制清單。Wireless MAC Filter頁面開啟：

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			

步驟4.選中Enable以在網路上啟用MAC過濾。

步驟5.點選與Connection Control欄位中的所需清單型別對應的單選按鈕。

·阻止PC — 阻止具有所列的MAC地址的PC進入網路。

- Permit PCs — 允許具有列出的MAC地址的PC進入網路。

步驟6.在MAC地址表中輸入所需的MAC地址。

步驟7.按一下「Save」。

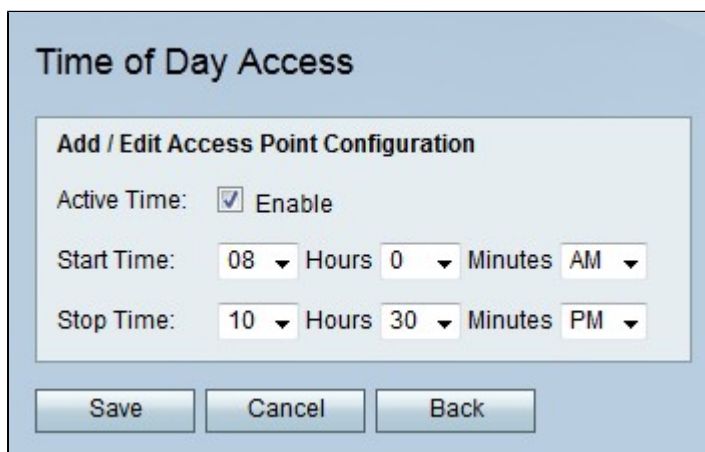
訪問當天時間

「訪問時間」功能僅允許根據已配置的計畫訪問使用者。

步驟1.登入到Web配置實用程式並選擇無線>基本設定。將開啟Basic Settings頁面：

步驟2.選中要編輯的網路框。

步驟3.按一下Time of Day Access配置使用者何時可以訪問指定的網路。此時將開啟時間訪問頁面：



The image shows a 'Time of Day Access' configuration window. It has a title bar 'Time of Day Access' and a subtitle 'Add / Edit Access Point Configuration'. Inside, there is a section 'Active Time:' with a checked checkbox and the word 'Enable'. Below this, there are two rows of time selection controls. The first row is for 'Start Time:' with dropdowns for '08' (Hours), '0' (Minutes), and 'AM'. The second row is for 'Stop Time:' with dropdowns for '10' (Hours), '30' (Minutes), and 'PM'. At the bottom, there are three buttons: 'Save', 'Cancel', and 'Back'.

步驟4.選中Active Time欄位中的Enable以啟用對網路的當日時間訪問。

步驟5.在Start Time欄位中輸入網路接入開始的時間。

步驟6.在「停止時間」欄位中輸入網路訪問結束的時間。

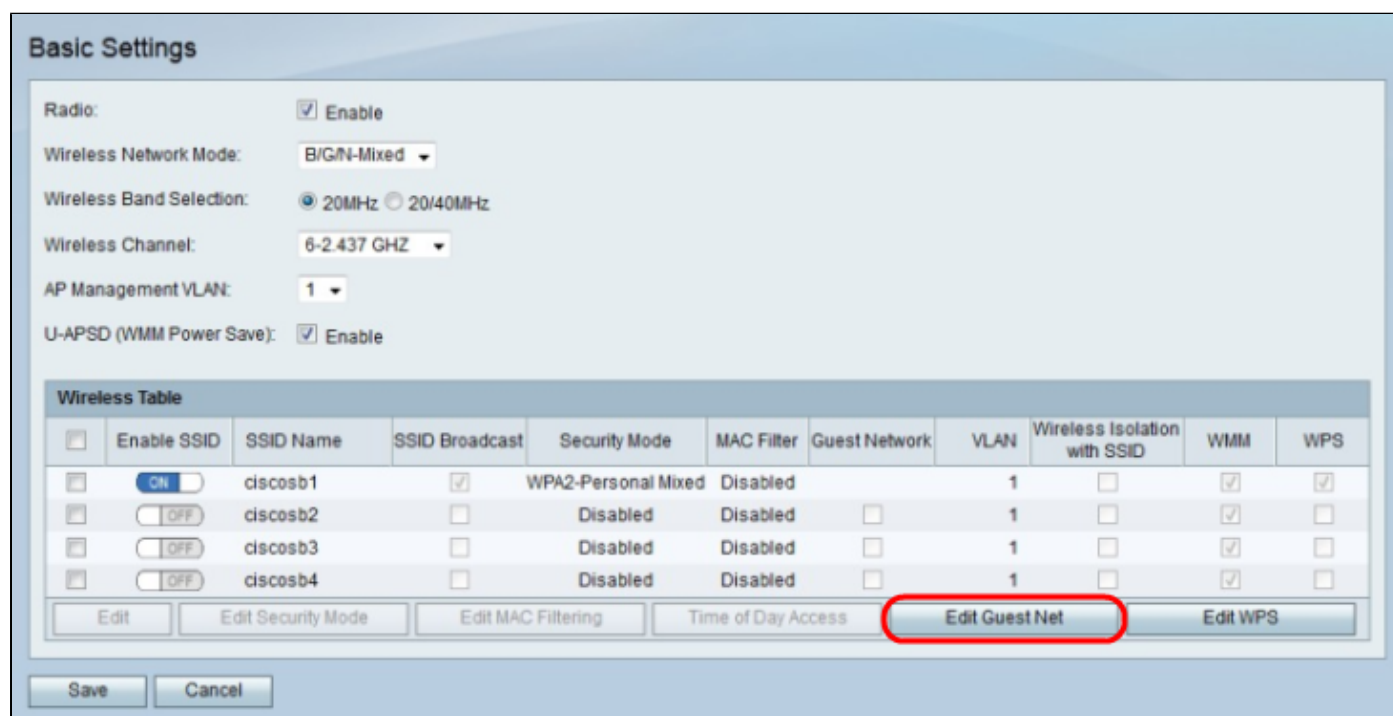
步驟7.按一下「Save」。

編輯訪客網路

訪客網路是專為臨時使用者設計的網路的一小部分。這用於允許訪客使用網路，而無需暴露私有Wi-

Fi金鑰。可以將訪客網路配置為限制使用者的訪問時間和頻寬使用。

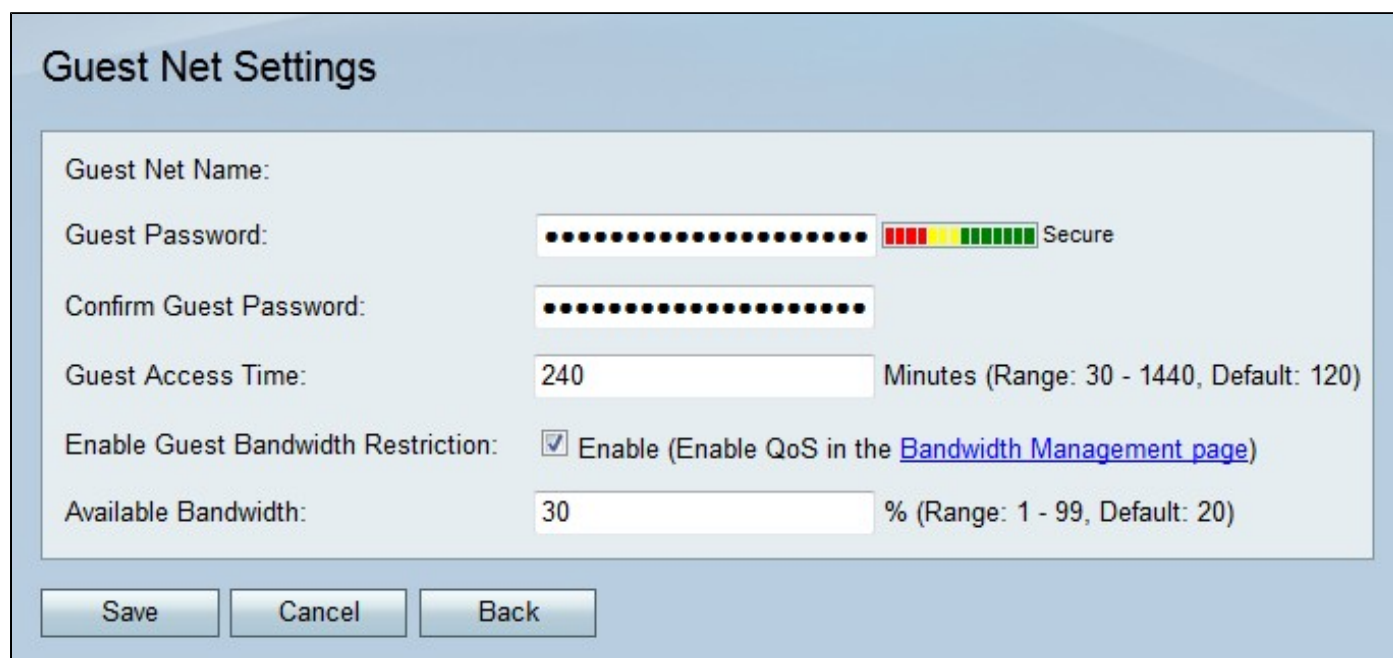
步驟1.登入到Web配置實用程式並選擇無線>基本設定。將開啟Basic Settings頁面：



The image shows the 'Basic Settings' page of a network configuration utility. It includes fields for Radio (checked), Wireless Network Mode (B/G/N-Mixed), Wireless Band Selection (20MHz), Wireless Channel (6-2.437 GHz), AP Management VLAN (1), and U-APSD (checked). Below these 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 lists four SSIDs: ciscosb1, ciscosb2, ciscosb3, and ciscosb4. The 'Edit Guest Net' button is highlighted with a red circle.

	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	Guest Network	VLAN	Wireless Isolation with SSID	WMM	WPS
☐	☒	ciscosb1	☒	WPA2-Personal Mixed	Disabled	☐	1	☐	☒	☒
☐	☐	ciscosb2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐	ciscosb3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐	ciscosb4	☐	Disabled	Disabled	☐	1	☐	☒	☐

步驟2.按一下Edit Guest Network以設定訪客網路。Guest Net Settings頁面隨即開啟：



The image shows the 'Guest Net Settings' page. It includes fields for Guest Net Name, Guest Password (with a strength indicator), Confirm Guest Password, Guest Access Time (240 minutes), Enable Guest Bandwidth Restriction (checked), and Available Bandwidth (30%). The 'Save' button is highlighted.

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)

步驟3.在Guest Password欄位中輸入使用者用於輸入訪客網路的密碼。

步驟4.在Confirm Guest Password欄位中重新輸入使用者用於輸入訪客網路的密碼。

步驟5.在「訪客接入時間」中輸入允許使用者保持與訪客網路連線的時間。

步驟6.選中Enable Guest Bandwidth Restriction以限制訪客網路接收的頻寬量。

附註：必須在Bandwidth Management頁面上啟用Bandwidth Management。

步驟7.在Available Bandwidth欄位中輸入可供訪客網路使用的頻寬百分比。

步驟8.按一下「Save」。

配置WPS方法1

Wi-Fi Protected Setup(WPS)是一種提供簡單且安全的無線網路設定的功能。為了連線到WPS，連線裝置必須支援WPS並且必須與WPA安全相容。第一種配置方法是要求按下RV215W WPS按鈕和客戶端裝置按鈕的簡單方法。按下這兩個按鈕後，客戶端裝置即連線到WPS網路。

步驟1.登入到Web配置實用程式並選擇無線>基本設定。將開啟Basic Settings頁面：

The screenshot shows the 'Basic Settings' page of a web configuration utility. The 'Radio' section is expanded, showing options like '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 'Edit WPS' button is highlighted with a red circle.

	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	Guest Network	VLAN	Wireless Isolation with SSID	WMM	WPS
☐	☒	ciscosb1	☒	WPA2-Personal Mixed	Disabled	☐	1	☐	☒	☒
☐	☐	ciscosb2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐	ciscosb3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐	ciscosb4	☐	Disabled	Disabled	☐	1	☐	☒	☐

Buttons: Edit, Edit Security Mode, Edit MAC Filtering, Time of Day Access, Edit Guest Net, Edit WPS, Save, Cancel.

步驟2.按一下Edit WPS配置WPS。WPS頁面隨即開啟：

附註：也可通過Wireless > WPS訪問WPS頁面。

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

步驟3.按一下Edit以選擇要啟用WPS的無線網路。

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

步驟4.按一下WPS頁面上的WPS按鈕。

步驟5.按一下客戶端裝置或客戶端裝置的實用程式螢幕上的WPS按鈕，將客戶端裝置連線到WPS網路。

以下欄位顯示WPS配置的資訊。

- Wi-Fi Protected Setup Status - WPS配置的狀態。
- 網路名稱(SSID) — 由RV215W分配給WPS配置的網路名稱。
- WPA2 — 個人 — WPS配置使用的安全型別。

配置WPS方法2

Wi-Fi Protected Setup(WPS)是一種提供簡單且安全的無線網路設定的功能。為了連線到WPS，連線裝置必須支援WPS並且必須與WPA安全相容。第二種方法需要客戶端裝置的PIN號。在WPS頁面上輸入PIN編號後，客戶端裝置將連線到WPS網路。

步驟1.登入到Web配置實用程式並選擇無線>基本設定。將開啟Basic Settings頁面：

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

步驟2.按一下Edit WPS配置WPS。WPS頁面隨即開啟：

附註：也可通過Wireless > WPS訪問WPS頁面。

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

步驟3.按一下Edit以選擇要啟用WPS的無線網路。

步驟4.輸入客戶端裝置的PIN碼。

步驟5.按一下註冊以建立WPS網路。

以下欄位顯示WPS配置的資訊。

- Wi-Fi Protected Setup Status - WPS配置的狀態。
- 網路名稱(SSID) — 由RV215W分配給WPS配置的網路名稱。
- WPA2 — 個人 — WPS配置使用的安全型別。

配置WPS方法3

Wi-Fi Protected Setup(WPS)是一種提供簡單且安全的無線網路設定的功能。為了連線到WPS，連線裝置必須支援WPS並且必須與WPA安全相容。第三種方法要求使用者在客戶端裝置的WPS配置頁面上輸入RV215W的PIN號。

步驟1.登入到Web配置實用程式並選擇無線>基本設定。將開啟Basic Settings頁面：

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

步驟2.按一下Edit WPS配置WPS。WPS頁面隨即開啟：

附註：也可通過Wireless > WPS訪問WPS頁面。

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

步驟3.按一下Edit以選擇要啟用WPS的無線網路。

步驟4.按一下Generate以生成RV215W的PIN碼。

步驟5.從PIN Lifetime下拉選單中，選擇生成新PIN之前經過的時間。

步驟6.在客戶端裝置配置中輸入給定的RV215W PIN編號。客戶端裝置連線到WPS網路。

以下欄位顯示WPS配置的資訊。

· Wi-Fi Protected Setup Status - WPS配置的狀態。

· 網路名稱(SSID) — 由RV215W分配給WPS配置的網路名稱。

- WPA2 — 個人 — WPS配置使用的安全型別。

如果您想檢視RV215W路由器的所有其他文檔，請按一下[此處](#)。

觀看與本文相關的影片...

[按一下此處以觀看思科的技術演講](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。