

# CVR100W VPN路由器上的基本無線設定

## 目標

無線區域網路(WLAN)利用無線電通訊將無線裝置連線到LAN。例如，咖啡館的Wi-Fi熱點。無線網路非常有用，因為它降低了佈線成本且易於設定。

本文說明如何在CVR100W VPN路由器上配置基本無線設定，其中包括網路安全配置。有關高級無線設定，請參閱[CVR100W VPN路由器上的高級無線配置](#)文章。

## 適用的裝置

- CVR100W VPN路由器

## 軟體版本

- 1.0.1.19

## 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Wireless > Basic Settings。將開啟基本設定頁面：

<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID2	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

步驟2.選中Radio欄位中的Enable覈取方塊以啟用無線通訊。

步驟3.從Wi-Fi電源下拉選單中選擇wi-fi電源。此wi-fi電源控制wi-fi無線電的發射器功率。該功能有助於減小或增大訊號的範圍。此功能用於節省電力。

- 100% — 此選項啟用100%無線電發射器功率。

- 50% — 此選項啟用50%的無線電發射器功率。

步驟4.從Wireless Network Mode下拉選單選擇無線模式。此選項基於網路中裝置的無線功能

。

- B/G/N-Mixed — 網路混合使用wireless-B、 wireless-G和wireless-N裝置。
- 僅B — 網路僅包含無線 — B裝置。
- G-Only — 網路僅包含無線 — G裝置。
- 僅N — 網路僅包含無線 — N裝置。
- B/G-Mixed — 網路由wireless-B和wireless-G裝置混合組成。
- G/N Mixed — 網路由wireless-G和wireless-N裝置混合組成。

步驟5.如果網路模式由wireless-N裝置組成，則在Wireless Band Selection欄位中點選與無線訊號的所需頻寬對應的單選按鈕。更高的頻寬表示訊號可傳輸的資料量更大。

- 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，但容易受到更多干擾。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6.從Wireless Channel下拉選單中選擇無線電的無線通道。選擇鄰居網路當前未使用的通道。如果多個無線電使用同一通道，則可能會發生干擾。

步驟7.從AP管理VLAN下拉選單中，選擇管理VLAN。管理VLAN是用於管理遠端位置裝置的VLAN。

步驟8. ( 可選 ) 要啟用未計畫的自動節能傳輸(U-APSD)，請在U-APSD欄位中選中**Enable**。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9.按一下「**Save**」。

## 編輯無線表

步驟1.選中要在無線表中編輯的網路覈取方塊。

Wireless Table										
<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID2	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

步驟2.按一下**Edit**以編輯指定的網路。

步驟3.選中**Enable SSID**覈取方塊以啟用網路。服務組識別碼(SSID)是無線網路的名稱。

步驟4.在SSID Name欄位中輸入網路名稱。網路上的所有裝置都使用此SSID相互通訊。

步驟5.選中**SSID Broadcast** 覈取方塊以啟用無線廣播。啟用SSID廣播後，CVR100W VPN路由器的可用性會通告給附近的無線裝置。

步驟6. ( 可選 ) 若要編輯安全模式，請參閱[編輯安全模式](#)。

步驟7. ( 可選 ) 要編輯MAC過濾器，請參閱[編輯MAC過濾](#)。

步驟8. ( 可選 ) 若要啟用思科簡易連線(CSC)，請勾選**CSC**覈取方塊。CSC可以輕鬆設定無線網路，並允許無線裝置輕鬆連線到網路。無線裝置使用CSC獲取網路的SSID和密碼，從而自動連線到網路。要編輯CSC，請參閱[編輯CSC](#)。

**附註：**思科簡單連線的VLAN不能與當前或其他SSID的VLAN相同。

步驟9.從VLAN下拉式清單中選擇與網路關聯的VLAN。

步驟10.選中**SSID Isolation**覈取方塊以阻止指定網路上的裝置相互通訊。

步驟11.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。啟用WMM時，通過無線連線傳送的多媒體流量會獲得更高的優先順序。

步驟12.檢查**WPS**，將指定的網路分配為Wi-Fi Protected Setup(WPS)網路。WPS是一種支援簡單和安全網路配置的功能。此功能使裝置能夠輕鬆連線到網路。

**附註：**要在CVR100W VPN路由器上配置WPS，請參閱[CVR100W VPN路由器上的WiFi Protected Setup\(WPS\)](#)文章。

步驟13.按一下「**Save**」。

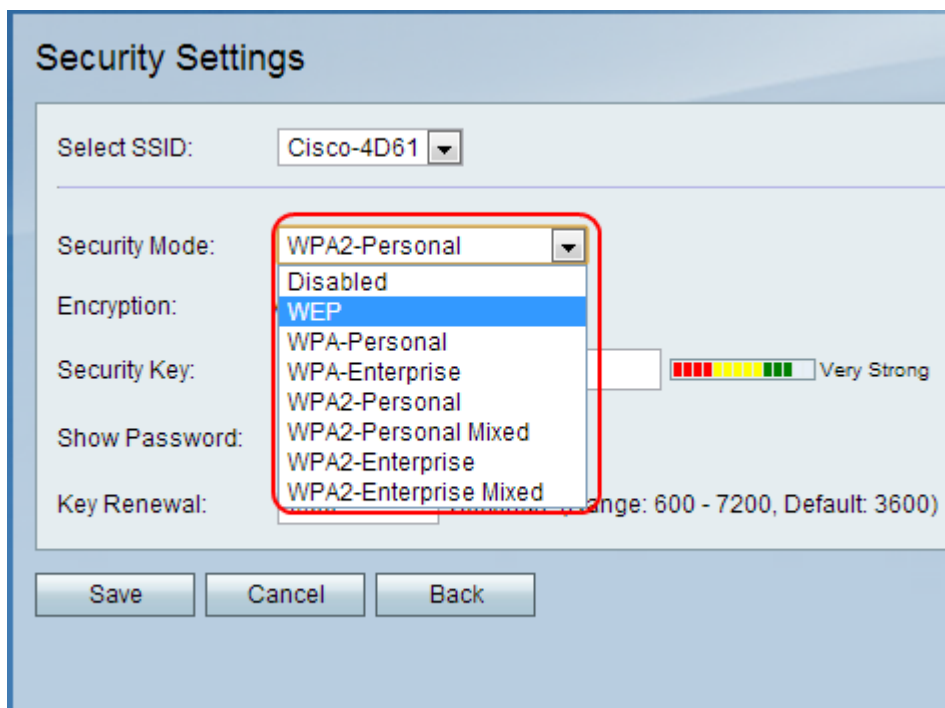
## 編輯安全模式

步驟1.選中要在無線表中編輯的網路覈取方塊。



<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID2	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

步驟2.按一下**Edit Security Mode**以編輯指定網路的安全。將開啟**Security Settings**頁面。



Security Settings

Select SSID: Cisco-4D61

Security Mode: WPA2-Personal

Encryption: WEP

Security Key: [ ] Very Strong

Show Password: [ ]

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

Save Cancel Back

步驟3. ( 可選 ) 要更改要為其配置安全性的SSID，請從Select SSID下拉選單中選擇所需的

SSID。

步驟4.從Security Mode下拉選單中選擇要配置的安全模式。

·[Disable Security](#) — 此選項禁用CVR100W VPN路由器上的安全。

·[WEP安全](#) — 有線等效保密(WEP)是用於保護無線網路的演算法。WEP用於提供比WPA更安全的基本加密方法。當連線的網路裝置不支援WPA時，使用WEP。

·[WPA — 個人安全](#) - Wi-Fi保護訪問(WPA)是無線網路的安全標準。WPA-Personal是WPA的一個版本，用於包含幾個使用者的網路。WPA-Personal提供每個使用者用於訪問無線網路的共用金鑰。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)。

·[WPA-Enterprise Security](#) — WPA-Enterprise是WPA的一個版本，推薦用於包含大量使用者的網路。訪問網路的身份驗證由RADIUS伺服器控制。每個連線的使用者都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)。

·[WPA2 — 個人安全](#) — WPA2是WPA的增強功能，比WPA更安全。WPA2-Personal是WPA2的一個版本，用於使用者數量很少的網路。WPA2 — 個人比WPA2 — 個人「混合」更安全。WPA2-Personal提供共用金鑰，每個使用者使用該金鑰訪問無線網路。

·[WPA2 — 個人混合安全](#) — WPA2 — 個人混合是WPA2的一個版本，用於使用者數很少的網路。WPA2-Personal Mixed支援對不能使用WPA2的舊裝置的向後相容性。WPA2-Personal Mixed是一種安全性較低的連線。

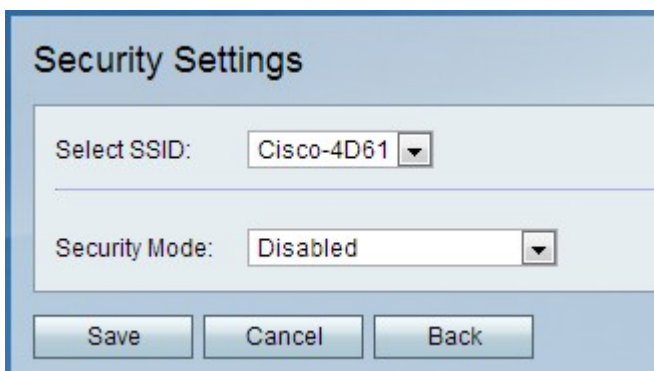
·[WPA2 — 企業安全](#) — WPA2 — 企業版是用於包含大量使用者的網路的WPA2版本。WPA2 — 企業比WPA2 — 企業混合更安全。用於獲取訪問的身份驗證由RADIUS伺服器控制。這意味著每個連線的使用者都將獲得訪問無線網路的唯一金鑰。

·[WPA2 — 企業混合安全](#) — WPA2 — 企業混合是WPA2的版本，用於具有大量使用者的網路。WPA2-Enterprise Mixed支援不能使用WPA2的舊裝置的向後相容性。與WPA2-Enterprise相比，WPA2-Enterprise Mixed提供的連線安全性較低。用於獲取訪問的身份驗證由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。

## 禁用安全

設定測試網路時，為了便於使用，CVR100W VPN路由器上可能會禁用無線安全。

附註：不建議禁用安全性。



The image shows a screenshot of the 'Security Settings' configuration window. At the top, the title 'Security Settings' is displayed. Below the title, there are two dropdown menus. The first is labeled 'Select SSID:' and is currently set to 'Cisco-4D61'. The second is labeled 'Security Mode:' and is currently set to 'Disabled'. At the bottom of the window, there are three buttons: 'Save', 'Cancel', and 'Back'.

步驟1. 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2.按一下「Save」。

## 配置WEP安全

The screenshot shows the 'Security Settings' configuration window. At the top, 'Select SSID' is set to 'Cisco-4D61'. Below that, 'Security Mode' is set to 'WEP', 'Authentication Type' is 'Open System', and 'Encryption' is '10/64-bit(10 hex digits)'. The 'Passphrase' field contains 'Passphrase1' and has a 'Generate' button next to it. There are four 'Key' fields (Key 1 through Key 4), each containing a series of dots. The 'TX Key' dropdown is set to '1'. At the bottom, there is a 'Show Password' checkbox which is unchecked. At the very bottom of the window are three buttons: 'Save', 'Cancel', and 'Back'.

步驟1.從Security Mode下拉選單中選擇WEP。

步驟2.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 — 任何網路裝置都可以與接入點關聯，但需要WEP金鑰才能通過接入點的流量。
- 共用金鑰 — 需要一個WEP金鑰才能與接入點關聯。它還用於通過接入點的流量。

步驟3.從Encryption下拉選單中選擇WEP金鑰的加密方法。

- 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。此選項更安全。

步驟4.在「密碼短語」欄位中輸入大於八個字元的密碼短語。密碼對於使網路安全設定更易於記憶非常有用。

步驟5.按一下**Generate**，在Key 1、Key 2、Key 3和Key 4欄位中建立金鑰。

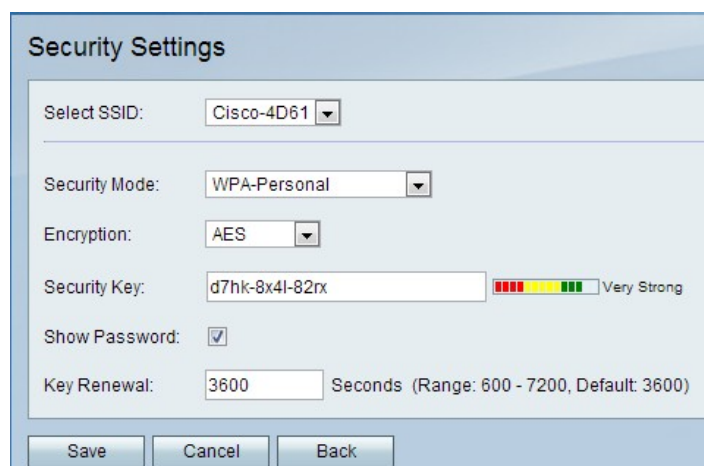
**附註：**您也可以在Key 1、Key 2、Key 3和Key 4欄位中手動輸入金鑰。

步驟6.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7. ( 可選 ) 勾選**Show Password** 覈取方塊以顯示關鍵字的字串。

步驟8.按一下「**Save**」。

## 配置WPA個人安全



步驟1.從「Security Mode」下拉選單中選擇**WPA-Personal**。

步驟2.從Encryption下拉選單中，為WPA金鑰選擇加密方法。

- TKIP/AES — 當連線到無線網路的裝置不全部支援AES時，會選擇此選項。
- AES — 如果連線到無線網路的所有裝置都支援AES，則首選此選項。

步驟3.在「安全金鑰」欄位中輸入安全金鑰。安全金鑰是由字母和數字組成的密碼短語。裝置使用安全金鑰連線到網路。

步驟4. ( 可選 ) 要顯示金鑰的字串，請選中**Show Password**覈取方塊。

步驟5.在Key Renewal欄位中，輸入CVR100W VPN路由器在生成新金鑰之前使用該金鑰的時間 ( 以秒為單位 )。

步驟6.按一下「**Save**」。

## 配置WPA — 企業安全



The screenshot shows the 'Security Settings' dialog box. At the top, 'Select SSID:' is set to 'Cisco-4D61'. Below that, 'Security Mode:' is set to 'WPA-Enterprise'. 'Encryption:' is set to 'AES'. The 'RADIUS Server:' field is split into four boxes containing '192', '168', '1', and '220', with a hint '(Hint: 192.168.1.200)'. 'RADIUS Port:' is '1812' with a range of '1 - 65535, Default: 1812'. 'Shared Key:' is 'SharedKey1'. 'Key Renewal:' is '3600' seconds with a range of '600 - 7200, Default: 3600'. At the bottom are 'Save', 'Cancel', and 'Back' buttons.

步驟1.從「Security Mode」下拉選單中選擇WPA-Enterprise。

步驟2.從Encryption下拉選單中，為WPA金鑰選擇加密方法。

·TKIP/AES — 當連線到無線網路的裝置不全部支援AES時，會選擇此選項。

·AES — 如果連線到無線網路的所有裝置都支援AES，則首選此選項。

步驟3.在「RADIUS伺服器」欄位中，輸入RADIUS伺服器的IP地址。

步驟4.在「RADIUS連線埠」欄位中，輸入用於存取RADIUS伺服器的連線埠號碼。

步驟5.在「共用金鑰」欄位中，輸入無線使用者的預共用金鑰。預共用金鑰是所有使用者使用的金鑰。預共用金鑰功能是附加的安全功能。

步驟6.在Key Renewal欄位中，輸入CVR100W VPN路由器在生成新金鑰之前使用該金鑰的時間（以秒為單位）。

步驟7.按一下「Save」。

## 配置WPA2 — 個人/WPA2 — 個人混合安全

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

步驟1.從「安全模式」下拉選單中選擇WPA2-Personal或WPA2-Personal Mixed。

**附註：**當無線網路上的所有裝置都支援AES時，使用WPA2-Personal。當網路上的裝置都不支援AES時，使用WPA2-Personal Mixed。安全方法使用的加密型別顯示在「加密」欄位中。

步驟2.在「安全金鑰」欄位中輸入安全金鑰。安全金鑰是由字母和數字組成的密碼短語。裝置使用安全金鑰連線到網路。

步驟3. ( 可選 ) 要檢視金鑰的字串，請選中**Show Password**覈取方塊。

步驟4.在Key Renewal欄位中，輸入CVR100W VPN路由器在生成新金鑰之前使用該金鑰的時間 ( 以秒為單位 )。

步驟5.按一下**Save**。

## 配置WPA2 — 企業/WPA2 — 企業混合安全



The screenshot shows the 'Security Settings' configuration page. The 'Select SSID' dropdown is set to 'Cisco-4D61'. The 'Security Mode' dropdown is set to 'WPA2-Enterprise Mixed'. The 'Encryption' is set to 'TKIP + AES'. The 'RADIUS Server' is configured with IP address 192.168.1.220 (with a hint '192.168.1.200'). The 'RADIUS Port' is set to 1812 (with a range of 1-65535 and a default of 1812). The 'Shared Key' is set to 'Sharedkey1'. The 'Key Renewal' is set to 3600 seconds (with a range of 600-7200 and a default of 3600). At the bottom, there are three buttons: 'Save', 'Cancel', and 'Back'.

步驟1. 從「安全模式」下拉選單中選擇**WPA2-Enterprise**或**WPA2-Enterprise Mixed**。

**附註：**當無線網路上的所有裝置都支援AES時，使用WPA2-Enterprise。當網路上的裝置都不支援AES時，使用WPA2 — 企業混合。安全方法使用的加密型別顯示在「加密」欄位中。

步驟2.在「RADIUS伺服器」欄位中，輸入RADIUS伺服器的IP地址。

步驟3.在「RADIUS連線埠」欄位中，輸入用於存取RADIUS伺服器的連線埠號碼。

步驟4.在「共用金鑰」欄位中，輸入無線使用者的預共用金鑰。預共用金鑰是所有使用者使用的金鑰。預共用金鑰功能是附加的安全功能。

步驟5.在Key Renewal欄位中，輸入CVR100W VPN路由器在生成新金鑰之前使用該金鑰的時間 ( 以秒為單位 )。

步驟6.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。

The screenshot shows the 'Basic Settings' page for a wireless network. The 'Radio' section is checked 'Enable'. 'Wi-Fi Power' is set to 100%. 'Wireless Network Mode' is 'B/G/N-Mixed'. 'Wireless Band Selection' is '20MHz'. 'Wireless Channel' is 'Auto'. 'AP Management VLAN' is '1'. 'U-APSD (WMM Power Save)' is unchecked. Below this is a 'Wireless Table' with columns: Enable SSID, SSID Name, SSID Broadcast, Security Mode, MAC Filter, CSC, VLAN, SSID Isolation, WMM, and WPS. The first row, 'Cisco-4D61', is highlighted in green and has 'WPA2-Personal' security mode and 'Disabled' MAC filter. The 'Edit Security Mode' button for this row is circled in red. Other rows include 'cisco-SSID2', 'cisco-SSID3', and 'cisco-guest'. At the bottom are 'Save' and 'Cancel' buttons.

步驟1.選中要編輯的網路覈取方塊。

步驟2.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：

The screenshot shows the 'Wireless MAC Filtering' page. The 'SSID Name' is 'Cisco-4D61'. 'Wireless MAC Filtering' is checked 'Enable'. Under 'Connection Control', 'Permit' is selected. There is a 'Show Client List' button. Below is a 'MAC Address Table' with 11 rows. The first row has the MAC address '1A:2B:3C:4D:5E:6F' in the first column and '12' in the second column. The rest of the table is empty. At the bottom are 'Save', 'Cancel', and 'Back' buttons.

步驟3.選中**Enable**以在網路上啟用MAC過濾。

步驟4.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5.在MAC地址表中，輸入所需的MAC地址。

步驟6.按一下「**Save**」。

## 訪問當天時間

「訪問時間」功能用於根據配置的計畫允許訪問使用者。

<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID2	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

步驟1.選中要編輯的網路覈取方塊。

步驟2.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：

### Time of Day Access

**Add / Edit Access Point Configuration**

Active Time:  Enable

Start Time:  Hours  Minutes

Stop Time:  Hours  Minutes

步驟3.選中Active Time欄位中的**Enable**以啟用對網路的當日時間訪問。

步驟4.在Start Time欄位中，輸入開始訪問網路的時間。

步驟5.在Stop Time欄位中輸入網路訪問結束的時間。

步驟6.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部分。這用於允許訪客訪問網路，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。

### Basic Settings

Radio:  Enable

Wi-Fi Power:

Wireless Network Mode:

Wireless Band Selection:  20MHz  20/40MHz

Wireless Channel:

AP Management VLAN:

U-APSD (WMM Power Save):  Enable

<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID2	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

步驟1. 按一下**Edit Guest Network**以設定訪客網路。**Guest Net Settings**頁面開啟：

### Guest Net Settings

Guest Net Name: guest

Guest Password:

Hide Password:

Lease Time:  Minutes

Total Guest Allowed:

步驟2.在「訪客密碼」欄位中，輸入使用者用於輸入訪客網路的密碼。

步驟3. ( 可選 ) 要在頁面上隱藏密碼，請選中Hide Password欄位中的覈取方塊。

步驟4.在「租用時間」欄位中，輸入允許使用者保持連線到訪客網路的時間 ( 以分鐘為單位 )。

步驟5.從Total Guest Allowed下拉選單中，選擇允許的訪客總數。

步驟6.按一下「Save」。

## 編輯CSC

CSC可以輕鬆設定無線網路，並允許無線裝置輕鬆連線到網路。無線裝置使用CSC獲取網路的SSID和密碼，從而自動連線到網路。

Wireless Table										
<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-1	<input checked="" type="checkbox"/>	Disabled	Disabled	<input checked="" type="checkbox"/>	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

步驟1.選中要編輯的網路覈取方塊。

步驟2.按一下Edit CSC以編輯Cisco Simple Connect。

步驟3.選中CSC覈取方塊。

步驟4.從VLAN下拉式清單中選擇用於CSC的VLAN。

附註：Cisco簡單連線VLAN不能與當前或其他SSID VLAN相同。要建立新的VLAN，請參閱[CVR100W路由器上的VLAN成員資格](#)一文。

附註：CSC只能在SSID1上啟用無線分佈系統(WDS)。請參閱[CVR100W路由器上的無線分佈系統\(WDS\)](#)文章。

步驟5.按一下Save。