

# 在WAP121和WAP321接入點上進行欺詐接入點(AP)檢測

## 目標

無管理系統接入點(AP)是指未經系統管理員明確授權而安裝在網路上的接入點。欺詐接入點會帶來安全威脅，因為任何能夠訪問該區域的人都可以故意或不知情地安裝無線接入點，以允許未經授權的使用者訪問網路。*Rogue AP Detection* 頁面顯示有關這些接入點的資訊。您可以將任何授權接入點新增到受信任接入點清單。本文說明如何在WAP121和WAP321接入點上檢測欺詐接入點(AP)

## 適用裝置

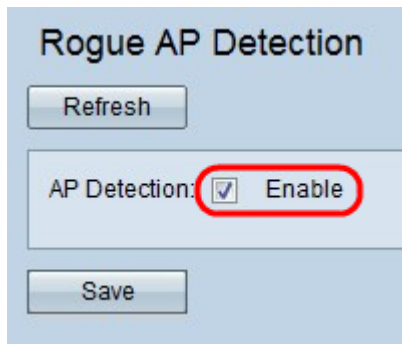
- WAP121
- WAP321

## 軟體版本

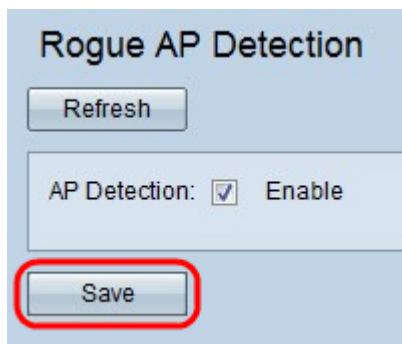
- 1.0.3.4

## 欺詐AP檢測配置

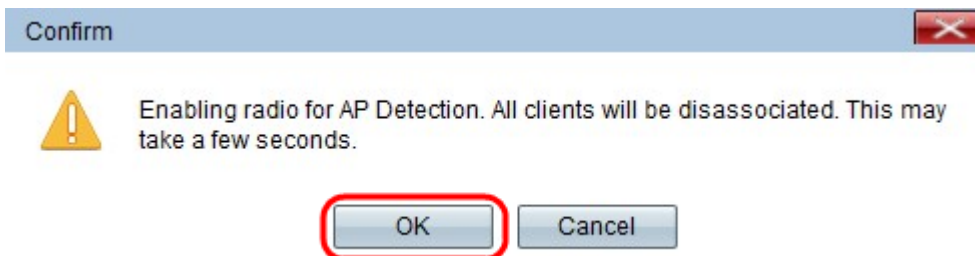
步驟1.登入到Access Point Configuration Utility，然後選擇**Wireless > Rogue AP Detection**。*Rogue AP Detection*頁面開啟：



步驟2.選中**Enable**以啟用AP檢測。



步驟3.啟用AP檢測後，按一下**Save**以顯示檢測到的欺詐接入點的清單。將出現警告螢幕。

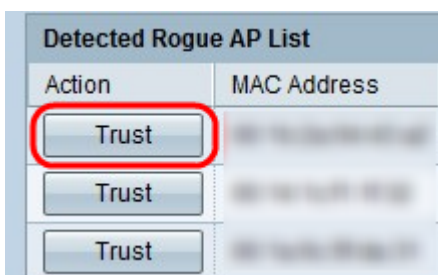


步驟4. 按一下OK以繼續。「檢測到的無管理AP」清單如下所示。

Detected Rogue AP List													
Action	MAC Address	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates
Trust	08:00:27:00:00:00	102	AP	WiFi-Router	Off	Off	2.4	1	1	■	5	Fri Dec 31 12:00:04 1999	1,2,5,5,6,9,11
Trust	08:00:27:00:00:00	102	AP	WiFi-Router	Off	Off	2.4	1	1	■	3	Fri Dec 31 12:00:04 1999	1,2,5,5,6,9,11
Trust	08:00:27:00:00:00	100	AP	(Non Broadcasting)	On	Off	2.4	1	1	■	5	Fri Dec 31 12:00:04 1999	1,2,5,5,6,9,11
Trust	08:00:27:00:00:00	100	AP	(Non Broadcasting)	On	Off	2.4	1	1	■	3	Fri Dec 31 12:00:02 1999	1,2,5,5,6,9,11
Trust	08:00:27:00:00:00	102	AP	WiFi-Router	On	On	2.4	1	1	■	6	Fri Dec 31 12:00:04 1999	1,2,5,5,6,9,11
Trust	08:00:27:00:00:00	102	AP	WiFi-Router	Off	Off	2.4	1	1	■	5	Fri Dec 31 12:00:04 1999	1,2,5,5,6,9,11
Trust	08:00:27:00:00:00	102	AP	WiFi-Router	Off	Off	2.4	1	1	■	4	Fri Dec 31 12:00:04 1999	1,2,5,5,6,9,11

顯示檢測到的接入點的以下資訊：

- MAC地址 — 檢測到的AP的MAC地址。
- 信標間隔（毫秒） — 檢測到的無線接入點使用的信標間隔。信標幀由AP按固定間隔傳輸，以通告無線網路的存在。傳送信標幀的預設時間是每100毫秒一次。
- 型別 — 檢測到的裝置的型別。可以是AP或Ad hoc。
- SSID — 檢測到的AP的SSID。
- 隱私 — 指示相鄰AP是否有任何安全性。
- WPA — 指示檢測到的無線接入點的WPA安全是關閉還是開啟。
- 頻段 — 表示在檢測到的AP上使用的IEEE 802.11模式。可以是2.4或5。
- 通道 — 檢測到的AP當前廣播的通道。
- 速率 — 檢測到的AP當前廣播的速率。
- 訊號 — 從檢測到的AP發射的無線電訊號的強度。
- 信標 — 自首次檢測到無線接入點以來從無線接入點接收的信標總數。
- 最後一個信標 — 從檢測到的AP接收的最後一個信標的日期和時間。
- 速率 — 檢測到的無線接入點所支援的速率集和基本速率集（兆位/秒）。



步驟5. 按一下條目旁邊的Trust，將其新增到Trusted AP List表中。您可以通過下載獲取信任清

單，並將當前清單儲存到您的PC，要下載/備份，請轉至[下載/備份信任的AP清單](#)。

Trusted AP List							
Action	MAC Address	Type	SSID	Privacy	Band	Channel	
<b>Untrust</b>	00:00:00:00:00:00	AP	XXXXXXXXXXXX	Off	2.4	4	

步驟6。（可選）如果要刪除Trusted AP清單，請按一下**Untrust**。

## 下載/備份受信任的AP清單

### Download/Backup Trusted AP List

Save Action:  Download (PC to AP)  
 Backup (AP to PC)

Source File Name:  No file selected.

File Management Destination:  Replace  
 Merge

步驟1.選擇是要從PC下載當前受信任的AP清單，還是要從「儲存操作」將當前清單儲存到PC。

- 下載 ( PC到AP ) — 如果要從檔案匯入清單並替換已知AP清單的內容，請轉至[下載 \( PC到AP \)](#)。
- 備份 ( AP到PC ) — 如果要將當前清單儲存到PC，請轉至[備份 \( AP到PC \)](#)。

### 下載 ( PC到AP )

### Download/Backup Trusted AP List

Save Action:  Download (PC to AP)  
 Backup (AP to PC)

Source File Name:  Example\_test.txt

File Management Destination:  Replace  
 Merge

步驟1.按一下**Download(PC to AP)**單選按鈕從PC下載清單。

步驟2.按一下**Browse**在PC上查詢該檔案。匯入檔案應為副檔名為.txt或.cfg的純文字檔案檔案。匯入檔案中的條目是十六進位制格式的MAC地址，每個八位組用冒號分隔。條目必須用單個空格分開。檔案必須僅包含MAC地址，然後AP接受該檔案。

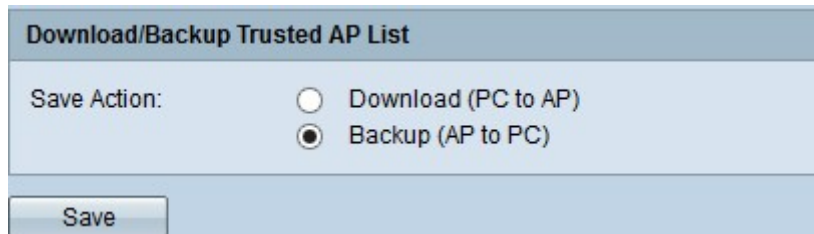
步驟3.選擇File Management Destination替換或新增內容到Trusted AP List。

- 替換 — 匯入清單並替換受信任AP清單的內容
- 合併 — 匯入已匯入檔案的AP並將其新增到「可信的AP」清單中。

**附註：**匯入完成後，螢幕將刷新，匯入檔案中的AP的MAC地址將顯示在已知的AP清單中。

步驟4.按一下**Save**以儲存所做的所有變更。

### 備份 ( AP到PC )



Download/Backup Trusted AP List

Save Action:  Download (PC to AP)  
 Backup (AP to PC)

Save

步驟1.按一下**Backup(AP to PC)**單選按鈕將清單儲存到PC。

步驟2.按一下**儲存**以儲存所做的更改，然後出現一個通知視窗，如下所示，提供了檔案的資訊。

