WAP561和WAP551上的欺詐接入點(AP)檢測

目標

欺詐接入點(AP)是在未經網路管理員同意的情況下安裝在安全網路上的接入點。惡意AP可能會帶來安全威脅，因為任何在您的網路範圍內安裝無線路由器的人都有可能訪問您的網路。*Rogue AP Detection* 頁面提供有關您的範圍內的無線網路的資訊。本文說明如何檢測惡意AP並建立受信任AP清單。

附註：*Rogue AP Detection*頁面沒有安全功能。AP信任清單供您自己使用，並不比不受信任的AP更安全。

適用裝置

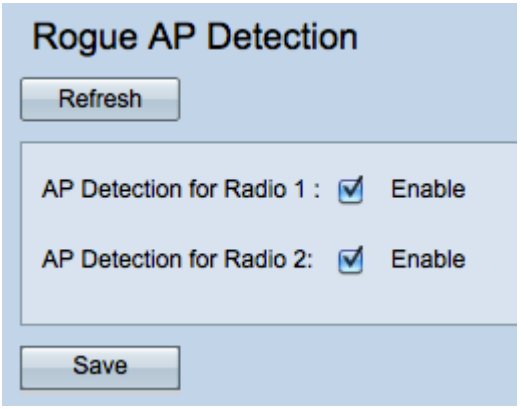
·WAP551
· WAP561

軟體版本

•1.0.4.2

欺詐AP檢測配置

步驟1.登入到Web配置實用程式並選擇**Wireless > Rogue AP Detection**。*Rogue AP Detection* 頁面開啟：

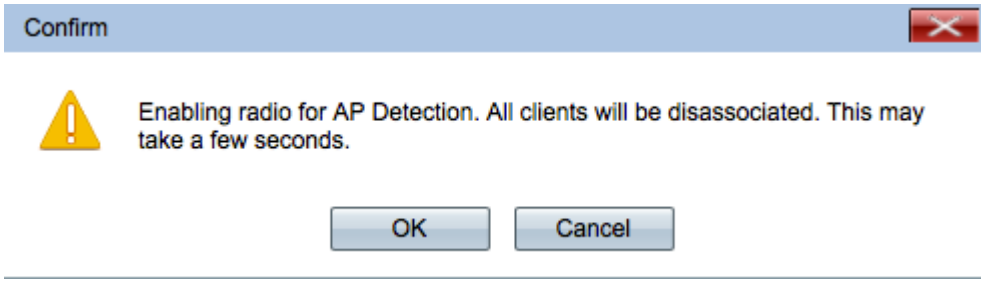


檢視欺詐AP統計資訊

步驟1.選中**Enable**以啟用所需無線電的AP檢測，以顯示欺詐AP統計資訊。

注意：WAP561有兩個可以啟用的無線電，而WAP551隻有一個要啟用的無線電。

步驟2.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。將顯示確認視窗。



步驟3.按一下**OK**以繼續。

附註：您網路上的無線客戶端將暫時失去連線。

Detected Rogue AP List

Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA
Trust	[redacted]	wlan0	102	AP	[redacted]	On	On
Trust	[redacted]	wlan0	102	AP	[redacted]	Off	Off
Trust	[redacted]	wlan0	100	AP	[redacted]	On	Off
Trust	[redacted]	wlan0	102	AP	[redacted]	On	On

顯示檢測到的接入點的以下資訊：

·MAC地址 — 惡意AP的MAC地址。

·無線電 — 可以加入的惡意AP上的物理無線電。

·信標間隔 — 非法AP使用的信標間隔。每個AP定期傳送信標幀，以通告其無線網路的存在。

·型別 — 檢測到的裝置的型別。可以是AP或Ad hoc。

·SSID — 惡意AP的服務集識別符號(SSID)，也稱為網路名稱。

·隱私 — 指示是否在欺詐AP上啟用安全。Off表示欺詐AP未啟用安全措施，而On表示欺詐AP未啟用安全措施。

·WPA — 指示是否為惡意AP啟用WPA安全。

Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates
2.4	1	1		5	Fri Dec 31 12:00:04 1999	**1**,**2**,**5.5**,6,9,**11**,12,18,24,36,48,54
2.4	1	1		4	Fri Dec 31 12:00:04 1999	**1**,**2**,**5.5**,6,9,**11**,12,18,24,36,48,54
2.4	1	1		1	Wed Dec 31 16:00:23 1969	**1**,**2**,**5.5**,6,9,**11**,12,18,24,36,48,54
2.4	1	1		4	Fri Dec 31 12:00:04 1999	**1**,**2**,**5.5**,6,9,**11**,12,18,24,36,48,54

·頻段 — 惡意AP上使用的IEEE 802.11模式。

- 2.4 — 正在使用IEEE 802.11b、802.11g或802.11n模式（或組合）。

- 5 — 正在使用IEEE 802.11a或802.11n模式（或同時使用兩者）。

·通道 — 非法AP廣播的通道（屬於無線電頻譜）。

·速率 — 非法AP當前傳輸的速率（以百萬位元組為單位）。

·訊號 — 惡意AP發出的無線電訊號的強度。若要檢視以分貝表示的訊號強度，請將滑鼠懸停在條形圖上。

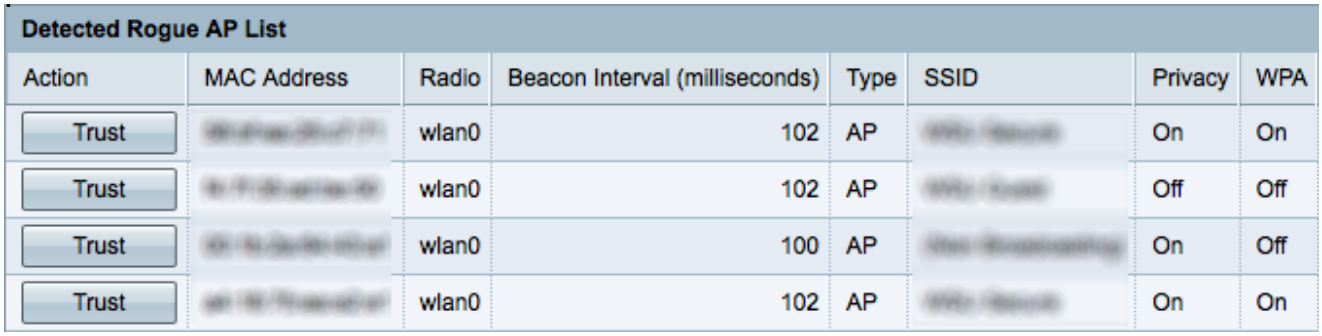
·信標 — 自第一次檢測到欺詐AP以來從它接收的信標總數。

·最後一個信標 — 從惡意AP接收最後一個信標的日期和時間。

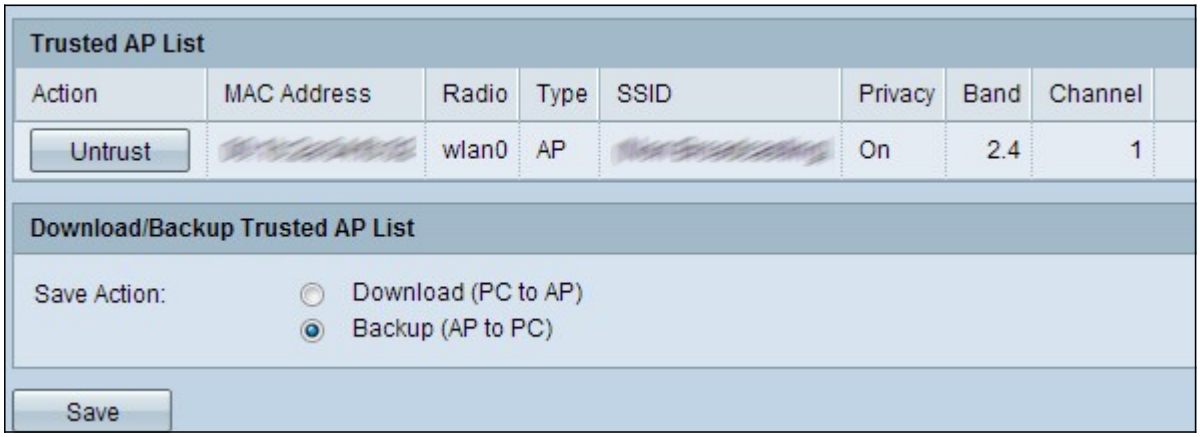
·速率 — 檢測到的無線接入點所支援的速率集和基本速率集（兆位/秒）。

建立受信任的AP清單

附註：需要啟用欺詐接入點檢測，以建立受信任的AP清單。如果尚未檢視*欺詐AP統計資訊*，請完成此部分。



步驟1.點選AP條目旁邊的**Trust**，將其新增到Trusted AP List（受信任的AP清單）。



步驟2.（可選）要從受信任的AP清單中刪除AP條目，請按一下**Untrust**。

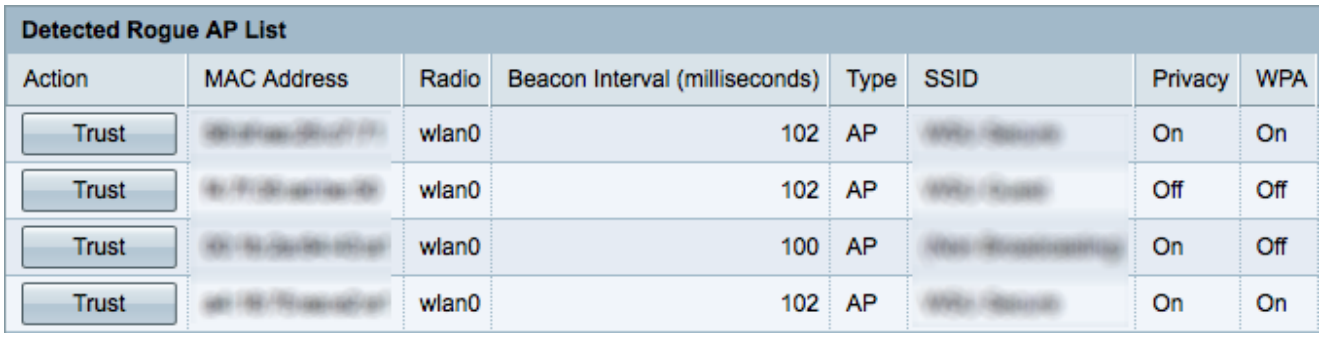
步驟3.點選Save Action欄位中的**Backup(AP to PC)**單選按鈕，將Trusted AP List儲存到檔案。

步驟4.按一下**Save**儲存受信任的AP清單。WAP建立一個.cfg檔案，該檔案包含受信任AP清單中所有MAC地址的清單。

匯入受信任的AP清單

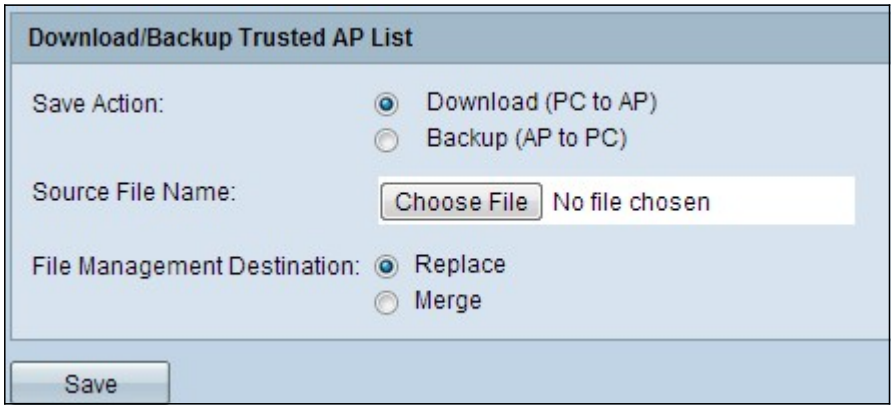
附註：需要啟用欺詐接入點檢測，以建立受信任的AP清單。如果尚未檢視*欺詐AP統計資訊*，請完成此部分。

步驟1.登入到Web配置實用程式並選擇**Wireless > Rogue AP Detection**。*Rogue AP Detection*頁面開啟：



Detected Rogue AP List

Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA
Trust	[redacted]	wlan0	102	AP	[redacted]	On	On
Trust	[redacted]	wlan0	102	AP	[redacted]	Off	Off
Trust	[redacted]	wlan0	100	AP	[redacted]	On	Off
Trust	[redacted]	wlan0	102	AP	[redacted]	On	On



步驟2.向下滾動到Download/Backup Trusted AP List區域，然後點選**Download(PC to AP)**單選按鈕，從儲存的清單中匯入已知AP清單。

步驟3.在「Source File Name」欄位中按一下**Browse**，然後選擇您的檔案。匯入的檔案必須具有.txt或.cfg副檔名。檔案應為十六進位制格式的MAC地址清單。

步驟4.在File Management Destination欄位中，按一下**Replace**以覆蓋受信任AP清單，或按一下**Merge**以新增到受信任AP清單。

步驟5.按一下**Save**以匯入檔案。

注意：在上傳檔案中定義的AP會從「檢測到的AP清單」移動到「受信任的AP清單」。