

WAP351和WAP371接入點上的欺詐AP檢測

目標

無管理接入點(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。非法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安裝無線接入點，以允許未經授權的使用者訪問網路。無管理AP檢測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。

本文檔的目的是解釋如何在WAP351和WAP371接入點上檢測欺詐接入點(AP)。

適用裝置

- WAP351
- WAP371

軟體版本

- 1.0.0.39(WAP351)
- 1.2.0.2(WAP371)

欺詐AP檢測配置

附註：要為無線電配置非法AP檢測，必須先在無線>無線部分啟用該無線電。如需詳細資訊，請參閱[在WAP131和WAP351上設定基本無線電設定](#)和[WAP371上設定基本無線電設定](#)的文章。

步驟1.登入到Web配置實用程式並選擇Wireless > Rogue AP Detection。出現Rogue AP Detection視窗：

Rogue AP Detection

Refresh

AP Detection for Radio 1 (2.4 GHz): Enable

AP Detection for Radio 2 (5 GHz): Enable

Save

Detected Rogue AP List

Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates
--------	-------------	-------	--------------------------------	------	------	---------	-----	------	---------	------	--------	---------	-------------	-------

Trusted AP List

Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel
--------	-------------	-------	------	------	---------	------	---------

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

Save

步驟2.選中AP Detection for Radio 1或AP Detection for Radio 2覈取方塊，選擇要啟用非法AP檢測的無線電介面。在WAP351上，Radio 1隻能檢測2.4 GHz範圍的AP，而Radio 2隻能檢測5 GHz範圍的AP。在WAP371上，Radio 1隻能檢測5 GHz範圍的AP，而Radio 2隻能檢

測2.4 GHz範圍的AP。

Rogue AP Detection

Refresh

AP Detection for Radio 1 (2.4 GHz): Enable

AP Detection for Radio 2 (5 GHz): Enable

Save

Detected Rogue AP List

Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates
--------	-------------	-------	--------------------------------	------	------	---------	-----	------	---------	------	--------	---------	-------------	-------

Trusted AP List

Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel
--------	-------------	-------	------	------	---------	------	---------

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

Save

步驟3. 按一下Save按鈕為所選單選介面啟用非法AP檢測。

Rogue AP Detection

Refresh

AP Detection for Radio 1 (2.4 GHz): Enable

AP Detection for Radio 2 (5 GHz): Enable

Save

Detected Rogue AP List

Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates
--------	-------------	-------	--------------------------------	------	------	---------	-----	------	---------	------	--------	---------	-------------	-------

Trusted AP List

Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel
--------	-------------	-------	------	------	---------	------	---------

Download/Backup Trusted AP List

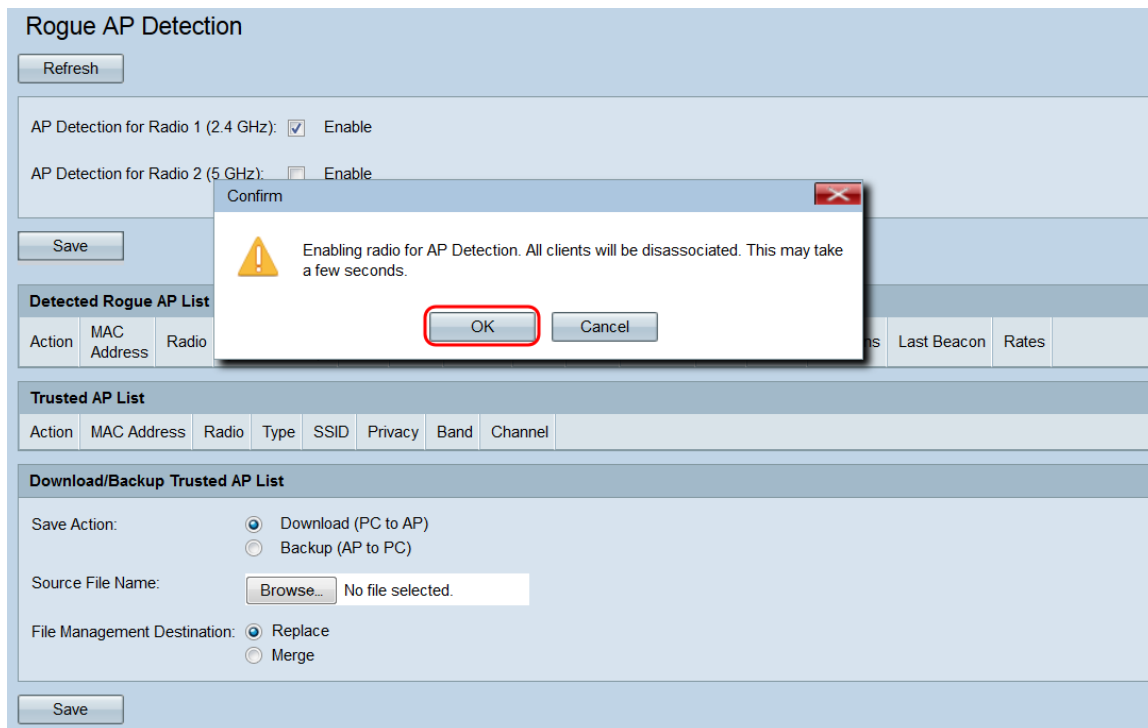
Save Action: Download (PC to AP)
 Backup (AP to PC)

Source File Name: No file selected.

File Management Destination: Replace
 Merge

Save

步驟4. 如果啟用欺詐接入點檢測，將出現一個彈出視窗，提示當前連線的所有客戶端都將斷開連線。按一下OK繼續。



啟用欺詐接入點檢測後，檢測到的每個接入點都會顯示在檢測到的欺詐接入點清單中。

Detected Rogue AP List														
Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates
Trust	██████████	Radio 1:VAP0	102	AP	██████████	On	On	2.4	1	6	█	567	Wed Feb 11 11:27:14 2015	6,9,12,18,24,36,48,54
Trust	██████████	Radio 1:VAP0	102	AP	██████████	Off	Off	2.4	1	6	█	567	Wed Feb 11 11:27:14 2015	6,9,12,18,24,36,48,54
Trust	██████████	Radio 1:VAP0	102	AP	██████████	On	On	2.4	1	6	█	570	Wed Feb 11 11:27:14 2015	6,9,12,18,24,36,48,54
Trust	██████████	Radio 1:VAP0	102	AP	██████████	On	On	2.4	6	6	█	2	Fri Dec 31 18:12:51 1999	6,9,12,18,24,36,48,54
Trust	██████████	Radio 1:VAP0	102	AP	██████████	Off	Off	2.4	6	6	█	4	Fri Dec 31 18:12:55 1999	6,9,12,18,24,36,48,54
Trust	██████████	Radio 1:VAP0	102	AP	██████████	On	On	2.4	6	6	█	6	Fri Dec 31 18:12:55 1999	6,9,12,18,24,36,48,54

顯示檢測到的接入點的以下資訊：

- 操作 — 按一下此欄位中的信任按鈕會將相應的AP新增到受信任AP清單，並將其從檢測到的無管理AP清單中刪除。
- MAC地址 — 顯示檢測到的AP的MAC地址。
- 無線電 — 表示檢測到接入點的WAP無線電。
- 信標間隔 — 顯示檢測到的無線接入點使用的信標間隔（以毫秒為單位）。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 — 顯示檢測到的裝置的型別。它可以是AP或Ad hoc。Ad hoc裝置使用不涉及無線接入點的本地無線連線。
- SSID — 顯示檢測到的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 — 顯示檢測到的AP當前廣播的通道。
- 速率 — 顯示檢測到的AP當前廣播的速率(Mbps)。

·訊號 — 顯示來自AP的無線電訊號的強度。

·信標 — 顯示自首次檢測到AP以來從AP接收的信標總數。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。

·最後一個信標 — 顯示從AP接收的最後一個信標的日期和時間。

·速率 — 列出檢測到的無線接入點支援的速率和基本速率（兆位/秒）。

步驟5.如果您信任或識別到檢測到的AP，請按一下清單中其條目旁邊的Trust按鈕。這會將對應的AP新增到受信任AP清單，並將其從檢測到的無管理AP清單中刪除。信任AP只會將其新增到清單中，對WAP的操作沒有影響。這些清單是可用於採取進一步行動的組織工具。

Detected Rogue AP List														
Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates
Trust	██████████	Radio 1:VAP0	102	AP	██████████	On	On	2.4	1	6	█	567	Wed Feb 11 11:27:14 2015	6,9,12,18,24,36,48,54
Trust	██████████	Radio 1:VAP0	102	AP	██████████	Off	Off	2.4	1	6	█	567	Wed Feb 11 11:27:14 2015	6,9,12,18,24,36,48,54
Trust	██████████	Radio 1:VAP0	102	AP	██████████	On	On	2.4	1	6	█	570	Wed Feb 11 11:27:14 2015	6,9,12,18,24,36,48,54
Trust	██████████	Radio 1:VAP0	102	AP	██████████	On	On	2.4	6	6	█	2	Fri Dec 31 18:12:51 1999	6,9,12,18,24,36,48,54
Trust	██████████	Radio 1:VAP0	102	AP	██████████	Off	Off	2.4	6	6	█	4	Fri Dec 31 18:12:55 1999	6,9,12,18,24,36,48,54
Trust	██████████	Radio 1:VAP0	102	AP	██████████	On	On	2.4	6	6	█	6	Fri Dec 31 18:12:55 1999	6,9,12,18,24,36,48,54

步驟6.要管理受信任的AP，請向下滾動至受信任的AP清單。當您按一下其各自的Trust按鈕時，檢測到的非法AP位於此處。

Trusted AP List							
Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel
Untrust	██████████	Radio 1:VAP0	AP	██████████	On	2.4	1
Untrust	██████████	Radio 1:VAP0	AP	██████████	Off	2.4	1

步驟7.如果不再信任受信任的AP，請按一下其對應的Untrust按鈕。這將將其移回檢測到的欺詐AP清單。

Trusted AP List							
Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel
Untrust	██████████	Radio 1:VAP0	AP	██████████	On	2.4	1
Untrust	██████████	Radio 1:VAP0	AP	██████████	Off	2.4	1

備份/下載受信任AP清單

步驟1. 如果要下載或備份受信任AP清單，請向下滾動到下載/備份受信任AP清單部分。

Download/Backup Trusted AP List

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

Source File Name:

File Management Destination: Replace
 Merge

步驟2.在 *Save Action*欄位中，選擇其中一個單選按鈕：

- 下載 (PC到AP) — 如果要將現有受信任AP清單從PC下載到WAP，請選擇此選項。
- 備份 (AP到PC) — 如果要將受信任的AP清單備份到PC，請選擇此選項。如果選擇此選項，請跳至[步驟5](#)。

Download/Backup Trusted AP List

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

Source File Name:

File Management Destination: Replace
 Merge

步驟3.如果在上一步中選擇了Download(PC to AP)，請按一下Source File Name欄位中的Browse...按鈕，選擇您的PC上的受信任AP清單檔案。

Download/Backup Trusted AP List

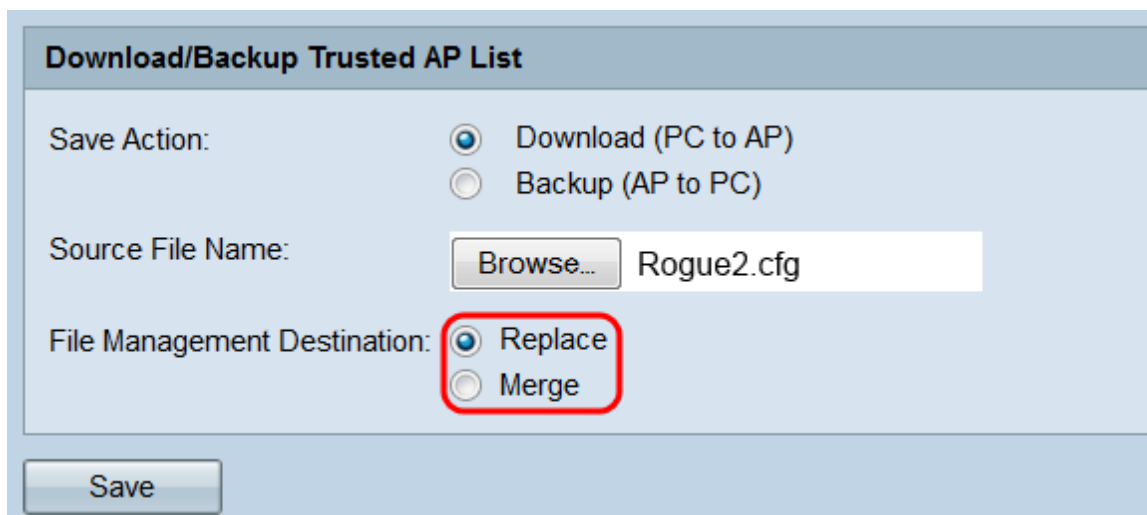
Save Action: Download (PC to AP)
 Backup (AP to PC)

Source File Name:

File Management Destination: Replace
 Merge

附註：檔案必須以.cfg結尾。

步驟4. 在 *File Management Destination* 欄位中，選擇 **Replace** 或 **Merge** 單選按鈕。替換將導致下載的檔案完全覆蓋WAP上的現有受信任AP清單，而Merge僅將檔案中的新AP新增到受信任AP清單中。



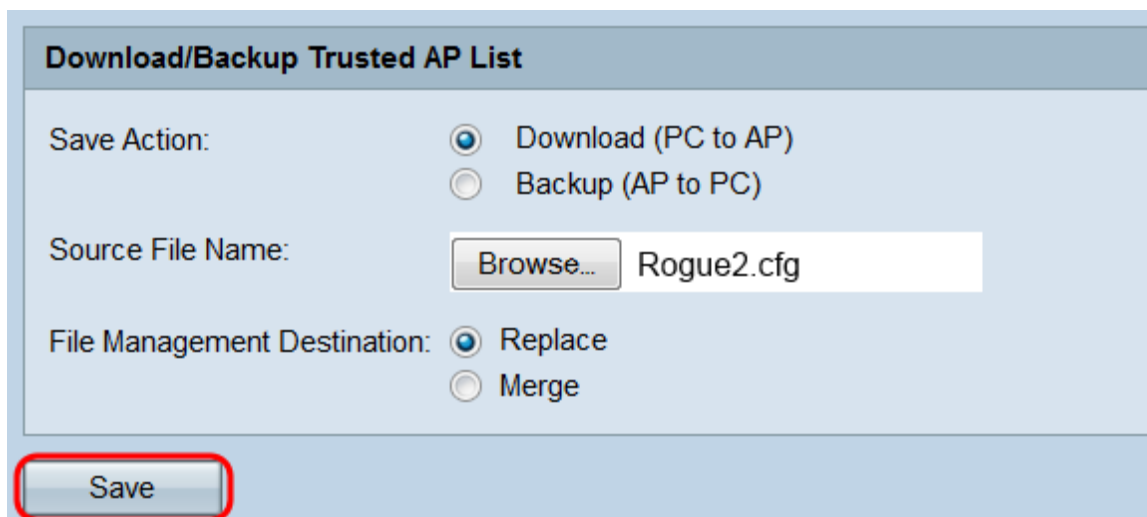
Download/Backup Trusted AP List

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

Source File Name:

File Management Destination: **Replace**
 Merge

步驟5. 按一下「**Save**」。根據您在 *Save Action* 欄位中所做的選擇，WAP會將受信任AP清單備份到PC或將指定的受信任AP清單下載到WAP。



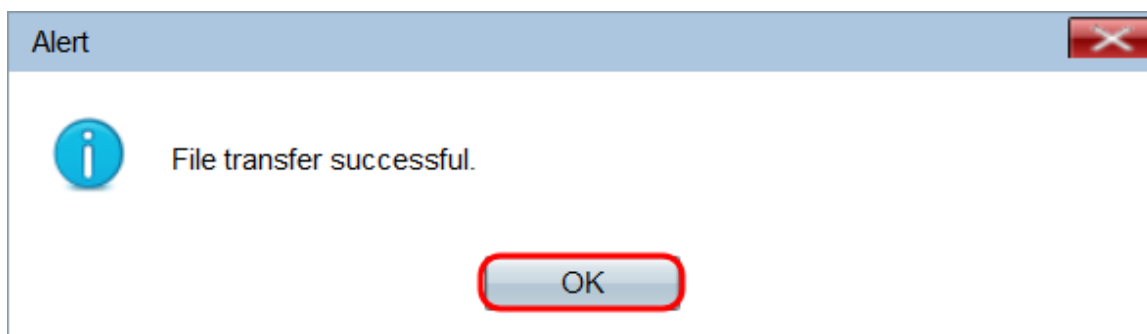
Download/Backup Trusted AP List

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

Source File Name:

File Management Destination: Replace
 Merge

步驟6. 如果您正在執行備份，將出現一個對話方塊視窗，要求將受信任的AP清單儲存到您的電腦。如果您正在下載檔案，將顯示一個彈出視窗，說明傳輸成功。按一下「**OK**」（確定）。



Alert

File transfer successful.