

# 識別思科企業無線網路中的惡意客戶端

## 目標

本文的目標是向您展示如何在Cisco Business Wireless(CBW)傳統或網狀網路中識別欺詐接入點(AP)和欺詐無線客戶端。

## 適用裝置 | 韌體版本

- 140AC([產品手冊](#)) | 10.0.1.0([下載最新版本](#))
- 141ACM([產品手冊](#)) | 10.0.1.0 ([下載最新版本](#)) — 擴展器僅用於網狀網路
- 142ACM([產品手冊](#)) | 10.0.1.0 ([下載最新版本](#)) — 擴展器僅用於網狀網路
- 143ACM([產品手冊](#)) | 10.0.1.0 ([下載最新版本](#)) — 擴展器僅用於網狀網路
- 145AC([產品手冊](#)) | 10.0.1.0([下載最新版本](#))
- 240AC([產品手冊](#)) | 10.0.1.0([下載最新版本](#))
- 150AX([產品介紹](#)) | 10.3.2.0([下載最新版本](#))
- 151AXM([產品手冊](#)) | 10.3.2.0([下載最新版本](#))

CBW 15x系列裝置與CBW 14x/240系列裝置不相容，不支援在同一個LAN上共存。

## 簡介

CBW接入點(AP)基於802.11 a/b/g/n/ac (第2波)，帶有內建天線。它們可以用作傳統的獨立裝置或網狀網路的一部分。

在完美的世界中，每個人都在使用無線網路時都會尊重他人且誠實。不幸的是，我們並不生活在一個完美的世界中。作為管理員，您的任務是瞭解任何潛在問題。

非法AP是指未經您允許而安裝在網路上的AP。惡意客戶端是任何其它檢測到的裝置，不屬於您的公司。

這些連線可能是完全無辜的，但是這些無賴總有嘗試攻擊您的網路或竊取敏感資訊的風險。要掌握這一點，您可以檢視欺詐AP和欺詐客戶端。檢測到這些惡意程式後，無法通過AP將其阻止，但會提供資訊供進一步調查。

CBW AP將僅檢測您當前使用的通道或重疊的通道上的欺詐行為。

## 檢視欺詐AP

此切換部分突出顯示初學者提示。

## 登入

登入到主AP的Web使用者介面(UI)。要執行此操作，請開啟Web瀏覽器並輸入 <https://ciscobusiness.cisco>。在繼續操作之前，您可能會收到警告。輸入您的憑據。您也可以通過將 [https://\[ipaddress\]](https://[ipaddress]) (主AP的) 輸入Web瀏覽器來訪問主AP。

## 工具提示

如果您對使用者介面中的欄位有疑問，請檢查是否提供如下所示的工具提示：



## 查詢「Expand Main Menu ( 展開主選單 )」圖示時遇到問題？

導航到螢幕左側的選單，如果未看到選單按鈕，請按一下此圖示開啟側欄選單。



## 思科企業應用程式

這些裝置具有配套應用，這些應用與Web使用者介面共用一些管理功能。Web使用者介面中的所有功能在應用中並非都可用。

[下載iOS應用](#) [下載Android應用](#)

## 常見問題

如果您還有未回答的問題，可以查閱我們的常見問題文檔。 [常見問題](#)

### 步驟1

登入到主AP的Web使用者介面(UI)。若要執行此操作，請開啟Web瀏覽器並輸入 <https://ciscobusiness.cisco>。在繼續操作之前，您可能會收到警告。輸入您的憑據。

您也可以直接在Web瀏覽器中輸入 <https://<ipaddress>> ( 主AP ) 來訪問主AP。

如果您不熟悉所使用的術語，請檢視 [思科業務：新術語辭彙表](#)。

### 步驟2

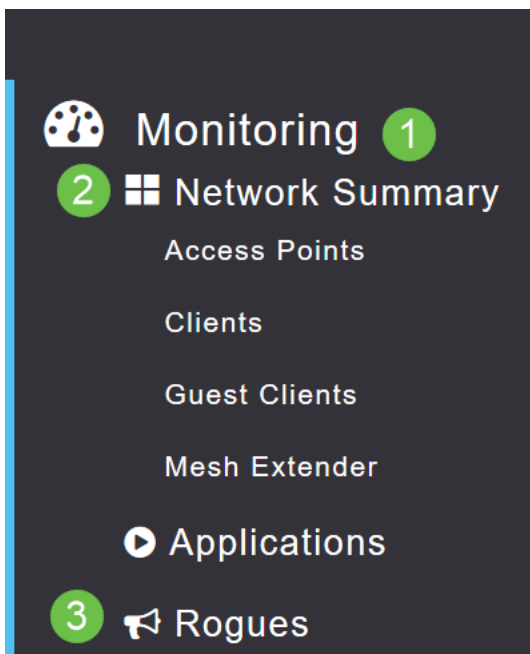
要進行這些配置，您需要處於 *Expert View*(專家檢視)。按一下Web UI 右上選單上的箭頭圖示可切換到「*Expert View*(專家檢視)」。



Switch to Expert View

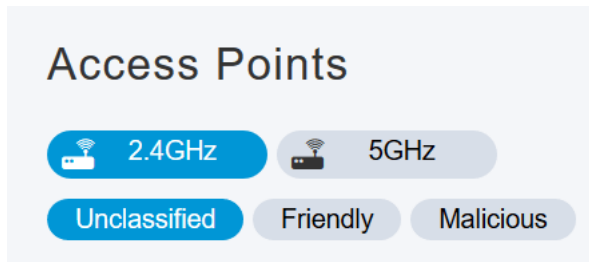
### 步驟3

導航到 **Monitoring > Network Summary > Rogues > Access Points**。



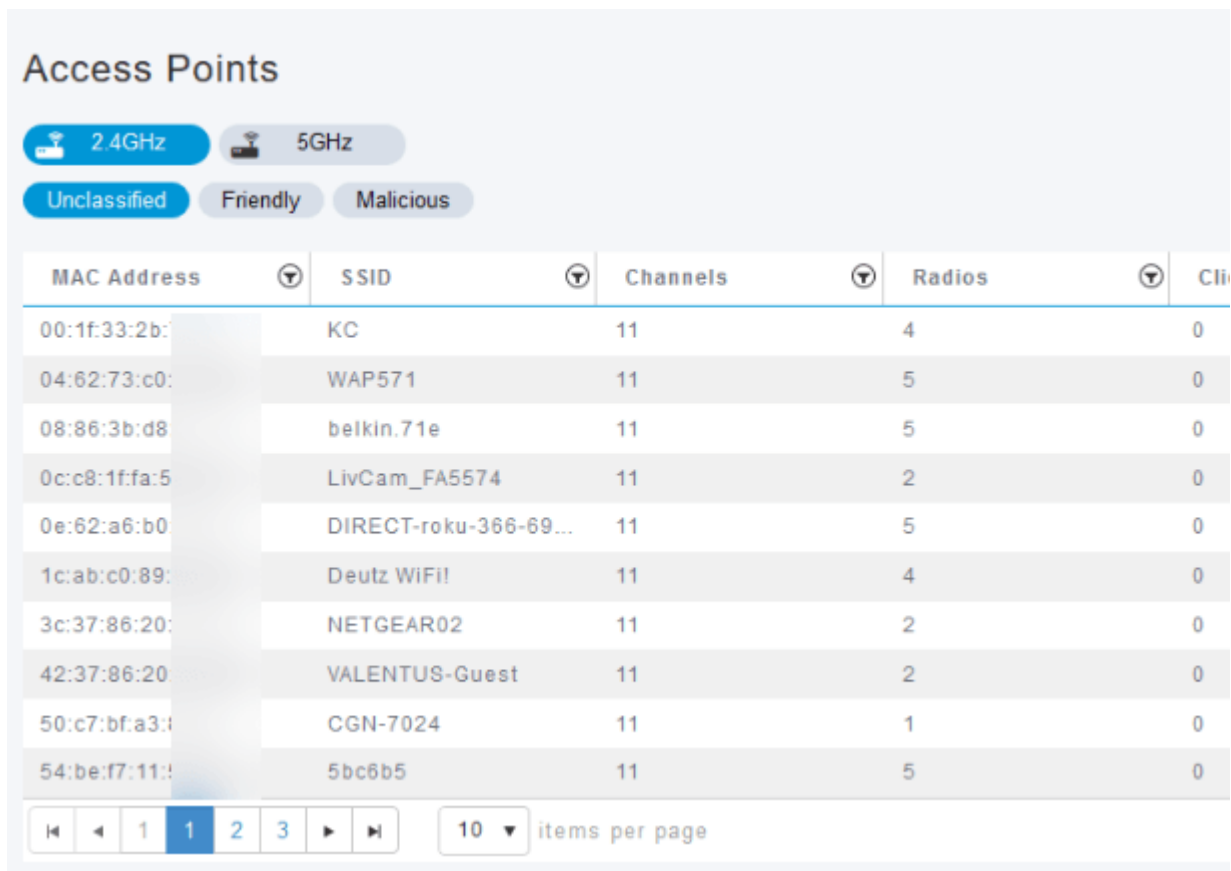
## 步驟4

開啟此頁面後，您可以通過按一下頁籤選擇檢視2.4 GHz或5 GHz。預設情況下，所有惡意AP都標籤為「未分類」。AP不會更改惡意AP的標籤，這是您可以手動執行的操作。



## 步驟5

列出惡意AP，您可以按一下其中的任意一個，進行進一步調查。



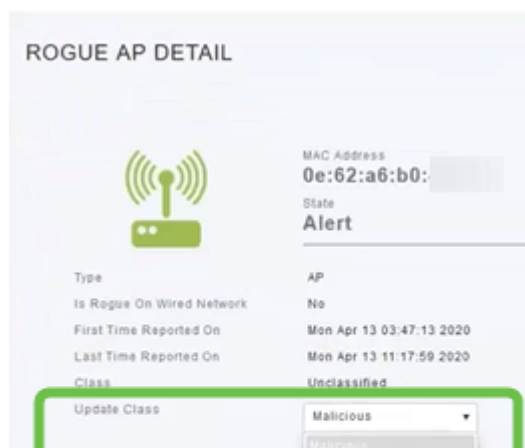
The screenshot shows the 'Access Points' table with the following data:

MAC Address	SSID	Channels	Radios	Cli
00:1f:33:2b:...	KC	11	4	0
04:62:73:c0:...	WAP571	11	5	0
08:86:3b:d8:...	belkin.71e	11	5	0
0c:c8:1f:fa:5...	LivCam_FA5574	11	2	0
0e:62:a6:b0:...	DIRECT-roku-366-69...	11	5	0
1c:ab:c0:89:...	Deutz WiFi!	11	4	0
3c:37:86:20:...	NETGEAR02	11	2	0
42:37:86:20:...	VALENTUS-Guest	11	2	0
50:c7:bf:a3:...	CGN-7024	11	1	0
54:be:f7:11:...	5bc6b5	11	5	0

At the bottom of the table, there is a pagination control showing '10 items per page' and a list of page numbers (1, 2, 3).

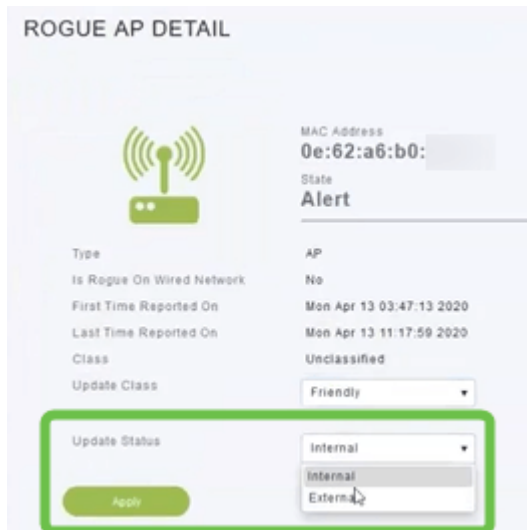
## 第6步 (可選)

如果要將任何AP分類為 *Friendly* 或 *Malicious*，可以從 *Update Class* 下的下拉選單中選擇任一選項。您可能希望這樣做，以便您在未來檢視未分類接入點時，不必對整個清單進行排序。完成後請務必按一下 **Apply**。



## 第7步 ( 可選 )

如果要將AP標籤為 *Internal* ( 在網路中 ) 或 *External* ( 可能是相鄰公司 ) ，可以在 *Update Status* 部分執行此操作。完成後按一下 **Apply**。



## 檢視欺詐客戶端

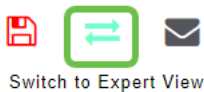
### 步驟1

登入到主AP的Web UI。若要執行此操作，請開啟Web瀏覽器並輸入 <https://ciscobusiness.cisco>。在繼續操作之前，您可能會收到警告。輸入您的憑據。

您也可以直接在Web瀏覽器中輸入 <https://<ipaddress>> ( 主AP ) 來訪問主AP。對於某些操作，您可以訪問思科企業移動應用。

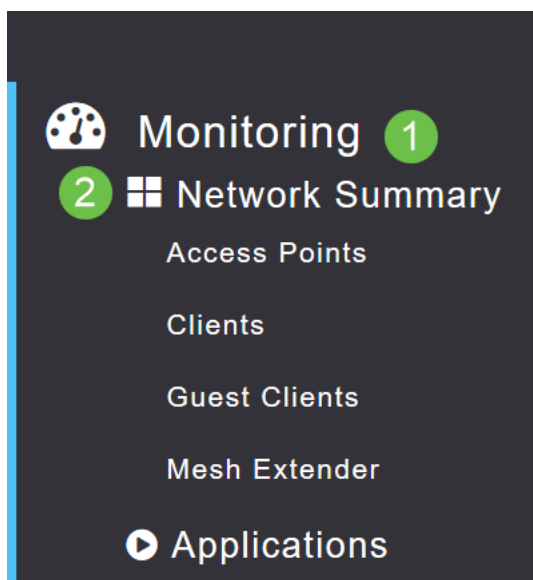
### 步驟2

要進行這些配置，您需要處於 *Expert View* (專家檢視)。按一下Web UI右上選單上的箭頭圖示可切換到「*Expert View* (專家檢視)」。有關設定RADIUS伺服器的詳細資訊，請檢出 [Radius](#)



### 步驟3

導航到 **Monitoring > Network Summary > Rogues > Clients**。



## 步驟4

如果存在任何惡意客戶端，則會列出這些客戶端。在此示例中，未檢測到任何惡意客戶端。

MAC Address	AP Mac	SSID	Radios	Last Seen	State	Wired
No items to display						

## 結論

現在，您能夠看到網路中的惡意程式。如果您正在使用的頻道上看到許多無管理系統，則可以更改頻道。請牢記一些注意事項，請檢視更改RF通道文章（連結，如果可用）。

[常見問題](#) [Radius 韌體升級](#) [RLAN 應用程式分析](#) [客戶端分析](#) [主要AP工具](#) [Umbrella WLAN使用者](#) [日誌記錄](#) [流量調節](#) [羅格](#) [干擾源](#) [組態管理](#) [埠配置網狀模式](#) [歡迎使用CBW網狀網路](#) [使用電子郵件驗證和RADIUS記帳的訪客網路](#) [疑難排解](#) [使用帶CBW的Draytek路由器](#)

## 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）。