

# 识别思科企业无线网络中的恶意客户端

## 目标

本文的目的是向您展示如何在思科企业无线(CBW)传统或网状网络中识别欺诈接入点(AP)和欺诈无线客户端。

## 适用设备 | 固件版本

- 140AC([产品手册](#)) | 10.0.1.0(下载[最新版本](#))
- 141ACM([产品手册](#)) | 10.0.1.0 ([下载最新](#)) — 扩展器仅用于网状网络
- 142ACM([产品手册](#)) | 10.0.1.0 ([下载最新](#)) — 扩展器仅用于网状网络
- 143ACM([产品手册](#)) | 10.0.1.0 ([下载最新](#)) — 扩展器仅用于网状网络
- 145AC([产品手册](#)) | 10.0.1.0(下载[最新版本](#))
- 240AC([产品手册](#)) | 10.0.1.0(下载[最新版本](#))
- 150AX([产品手册](#)) | 10.3.2.0(下载[最新版本](#))
- 151AXM([产品手册](#)) | 10.3.2.0(下载[最新版本](#))

CBW 15x系列设备与CBW 14x/240系列设备不兼容，不支持在同一LAN上共存。

## 简介

CBW接入点(AP)基于802.11 a/b/g/n/ac(Wave 2)，带有内置天线。它们可以用作传统的独立设备或网状网络的一部分。

在完美的世界中，使用无线网络时，每个人都要尊重他人且诚实。不幸的是，我们生活的世界并不完美。作为管理员，您的工作是了解任何潜在的问题。

非法AP是指未经您允许而安装在网络上的AP。非法客户端是任何其它检测到的设备，不属于您的公司。

这些连接可能是完全无辜的，但是这些恶意程序始终存在攻击您的网络或窃取敏感信息的风险。要掌握这一点，您可以查看欺诈AP和欺诈客户端。一旦检测到这些恶意程序，便无法通过AP进行阻止，但是它确实会为您提供信息以供进一步调查。

CBW AP将仅检测您当前使用的信道或重叠信道上的欺诈。

## 查看欺诈AP

此切换部分突出显示初学者提示。

## 登录

登录主AP的Web用户界面(UI)。为此，请打开Web浏览器并输入<https://ciscobusiness.cisco>。在继续操作之前，您可能会收到警告。输入您的凭据。您也可以通过在Web浏览器中输入[https://\[ipaddress\]](https://[ipaddress]) (主AP的) 来访问主AP。

## 工具提示

如果您对用户界面中的字段有疑问，请检查如下所示的工具提示：



## 查找“Expand Main Menu ( 展开主菜单 )”图标时出错？

导航到屏幕左侧的菜单，如果未看到菜单按钮，请单击此图标打开侧栏菜单。



## 思科业务应用

这些设备具有配套应用，这些应用与Web用户界面共享一些管理功能。Web用户界面中的所有功能在应用中并非都可用。

[下载iOS应用](#) [下载Android应用](#)

## 常见问题

如果您仍有未回答的问题，可以查阅我们的常见问题解答文档。 [常见问题](#)

### 第 1 步

登录主AP的Web用户界面(UI)。为此，请打开Web浏览器并输入 <https://ciscobusiness.cisco>。在继续操作之前，您可能会收到警告。输入您的凭证。

您也可以通过在Web浏览器中输入 <https://<ipaddress>> ( 主AP ) 来访问主AP。

如果您对使用的术语不熟悉，请查看 [思科业务：新术语词汇表](#)。

### 步骤 2

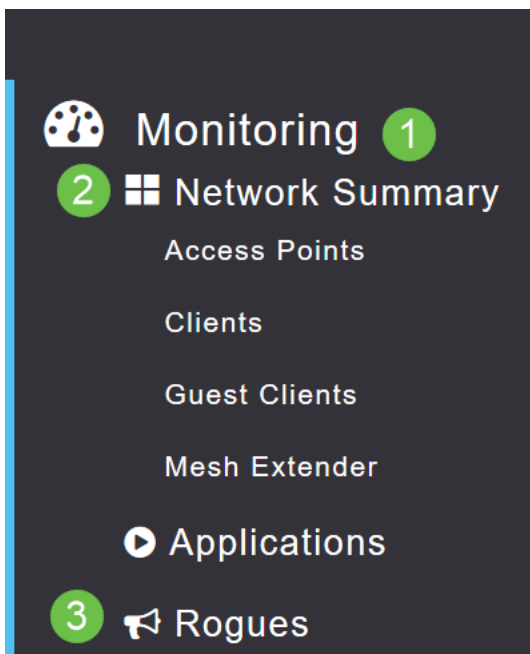
要进行这些配置，您需要处于 *Expert View* 中。点击Web UI右上菜单上的箭头图标可切换到 *Expert View*。



Switch to Expert View

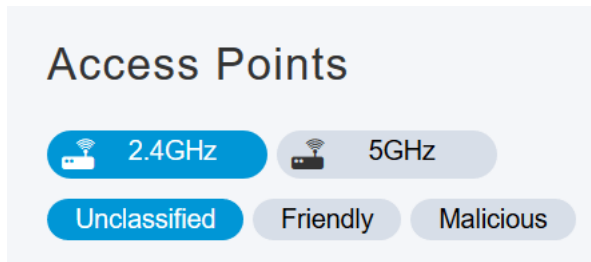
### 步骤 3

导航到 [监控](#) > [网络摘要](#) > [欺诈](#) > [接入点](#)。



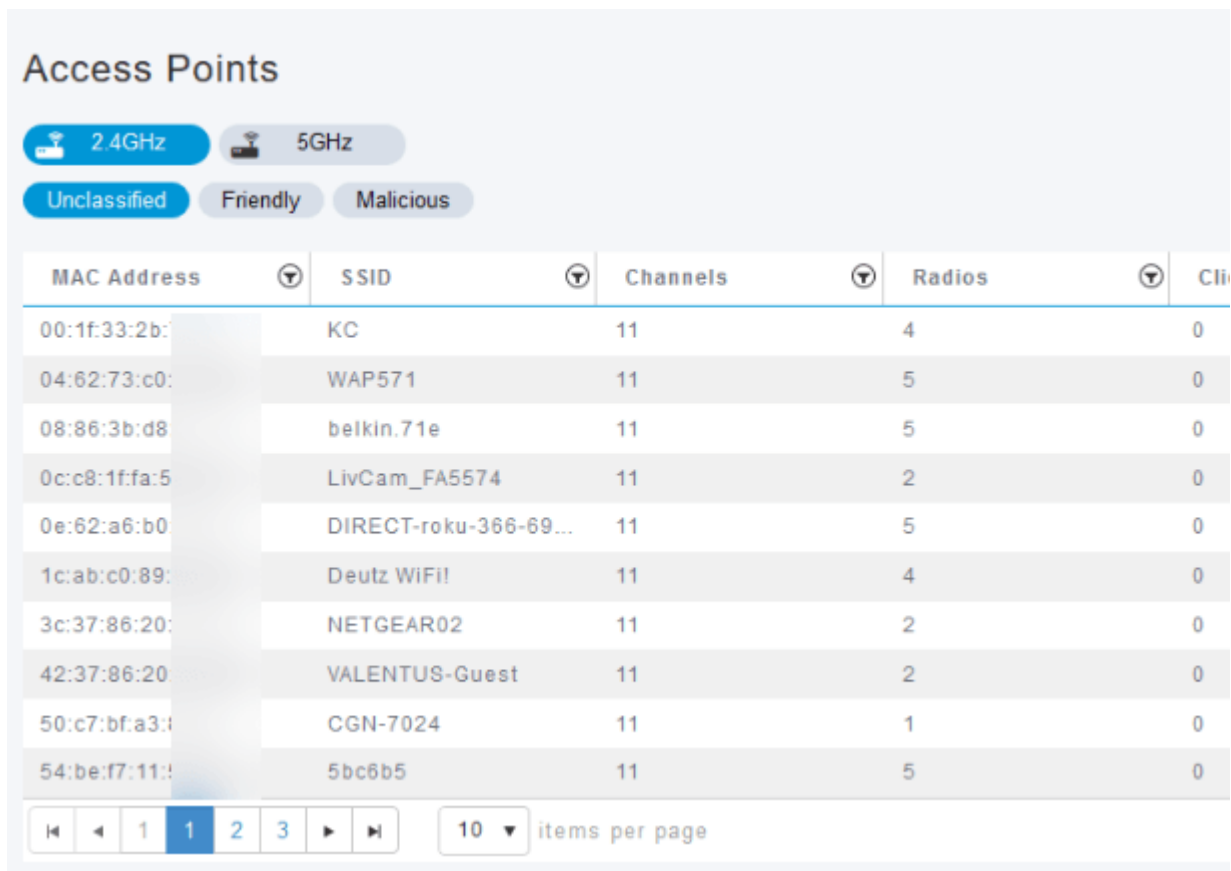
## 步骤 4

打开此页面后，您可以通过单击选项卡选择查看2.4 GHz或5 GHz。默认情况下，所有欺诈AP都标记为“未分类”。AP不会更改欺诈AP的标签，这是您可以手动执行的操作。



## 步骤 5

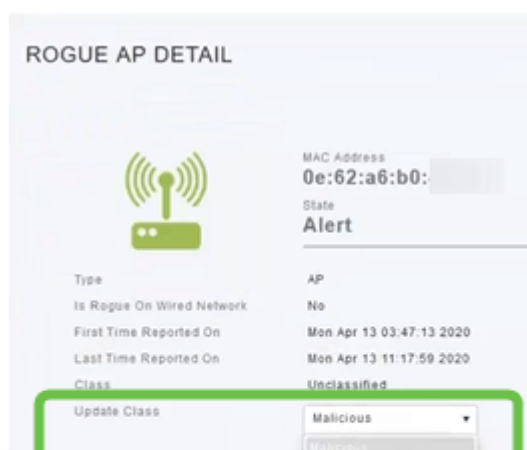
列出欺诈AP，您可以点击其中任何一个进行进一步调查。



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

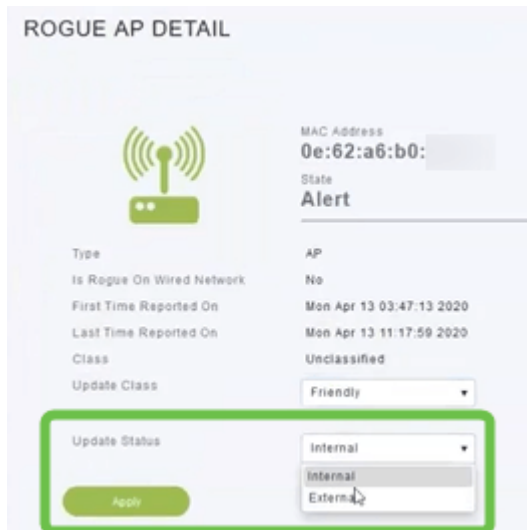
## 步骤 6 ( 可选 )

如果要任何AP分类为 *Friendly* 或 *Malicious*，可以从 *Update Class* 下的下拉菜单中选择任一选项。您可能希望这样做，以便您在未来查看未分类接入点时，不必对整个列表进行排序。完成后请务必单击 **Apply**。



## 步骤 7 ( 可选 )

如果要将AP标记为 *Internal* ( 在网络中 ) 或 *External* ( 可能是相邻公司 ) ，可以在 *Update Status* 部分中执行此操作。完成后单击 **Apply**。



## 查看欺诈客户端

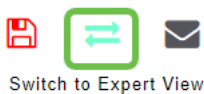
### 第 1 步

登录到主AP的Web UI。为此，请打开Web浏览器并输入 <https://ciscobusiness.cisco>。在继续操作之前，您可能会收到警告。输入您的凭证。

您也可以通过在Web浏览器中输入 <https://<ipaddress>> ( 主AP ) 来访问主AP。对于某些操作，您可以访问思科企业移动应用。

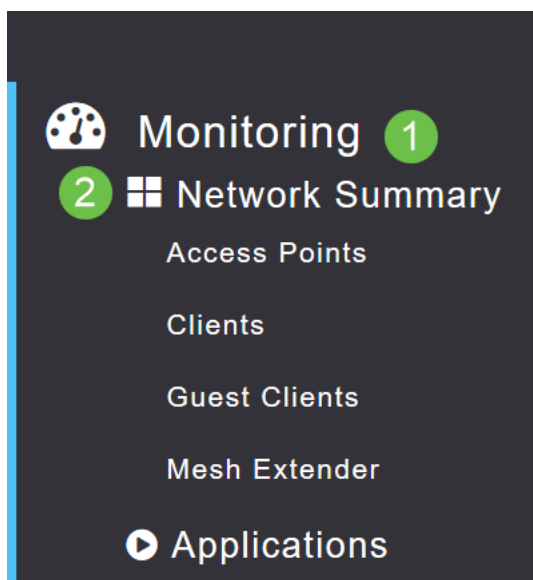
### 步骤 2

要进行这些配置，您需要处于 *Expert View* 中。点击Web UI右上菜单上的箭头图标可切换到 *Expert View*。有关设置RADIUS服务器的详细信息，请查看 [Radius](#)



### 步骤 3

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



## 步骤 4

如果存在任何恶意客户端，它们将被列出。在本示例中，未检测到欺诈客户端。

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

## 结论

现在，您可以看到网络中的恶意程序。如果您在正在使用的信道上看到许多欺诈，则可以更改该信道。需要记住一些注意事项，因此请查看更改RF信道文章（链接，如果可用）。

[常见问题](#) [RADIUS 固件升级](#) [RLAN 应用分析](#) [客户端分析](#) [主要AP工具](#) [Umbrella](#) [WLAN用户](#) [日志记录](#) [流量整形](#) [流氓无赖](#) [干扰源](#) [配置管理](#) [端口配置](#) [网状模式](#) [欢迎使用CBW网状网络](#) [使用邮件身份验证和RADIUS记账的访客网络](#) [故障排除](#) [使用带CBW的Draytek路由器](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。