

解決統一無線網路中的欺詐檢測和緩解

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[惡意軟體概述](#)

[欺詐檢測](#)

[非通道掃描](#)

[監控模式掃描](#)

[本地模式和監控模式比較](#)

[欺詐識別](#)

[惡意記錄](#)

[欺詐詳細資訊](#)

[匯出欺詐事件](#)

[欺詐記錄超時](#)

[惡意檢測器AP](#)

[可擴充性注意事項](#)

[RLDP](#)

[RLDP注意事項](#)

[交換器連線埠追蹤](#)

[惡意軟體分類](#)

[欺詐分類規則](#)

[HA事實](#)

[Flex-Connect事實](#)

[欺詐緩解](#)

[惡意遏制](#)

[惡意遏制詳細資訊](#)

[自動遏制](#)

[惡意遏制警告](#)

[交換器連線埠關閉](#)

[設定](#)

[配置欺詐檢測](#)

[配置用於欺詐檢測的通道掃描](#)

[配置無管理系統分類](#)

[配置欺詐緩解](#)

[配置手動遏制](#)

[自動遏制](#)

[使用Prime Infrastructure](#)

[驗證](#)

[疑難排解](#)

[如果未檢測到欺詐裝置](#)

[有用的調試](#)

[預期的陷阱日誌](#)

[行動](#)

[如果流氓未被分類](#)

[有用的調試](#)

[行動](#)

[RLDP找不到惡意程式](#)

[有用的調試](#)

[行動](#)

[惡意檢測器AP](#)

[AP控制檯中的有用調試命令](#)

[惡意遏制](#)

[預期調試](#)

[建議](#)

[結論](#)

[相關資訊](#)

簡介

本檔案介紹思科無線網路上的惡意軟體偵測和緩解。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco無線Lan控制器。
- Cisco Prime Infrastructure。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行8.8.120.0版的Cisco整合無線Lan控制器 (5520、8540和3504系列)。
- Wave 2 AP 1832、1852、2802和3802系列。
- Wave 1 AP 3700、2700和1700系列。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

惡意軟體概述

無線網路擴展了有線網路，提高了員工的工作效率和資訊訪問能力。但是，未經授權的無線網路帶來了額外的安全隱患。對有線網路的埠安全考慮較少，無線網路很容易擴展到有線網路。因此，如果員工將自己的接入點 (思科或非思科) 帶入安全可靠的無線或有線基礎設施，並允許未經授權的使用者訪問此安全網路，則很容易危及安全網路。

欺詐檢測允許網路管理員監控並消除這種安全問題。思科統一網路架構提供流氓檢測方法，可實現完整的流氓識別和遏制解決方案，而無需昂貴且難以證明的重疊網路和工具。

共用您的頻譜且未由您管理的任何裝置都可能被視為惡意裝置。流氓會在以下情況下變得危險：

- 設定使用與您的網路（蜜罐）相同的服務集識別符號(SSID)時
- 在有線網路上檢測到它時
- 臨時流氓
- 由外部人員設定時，多數情況下帶有惡意意圖

最佳實踐是使用惡意檢測來最大程度降低安全風險，例如在企業環境中。

但是，在某些情況下不需要進行欺詐檢測，例如Office Extend Access Point(OEAP)部署、全市範圍以及戶外。

使用室外網狀AP來檢測惡意代碼幾乎沒有什麼價值，但使用資源來進行分析。

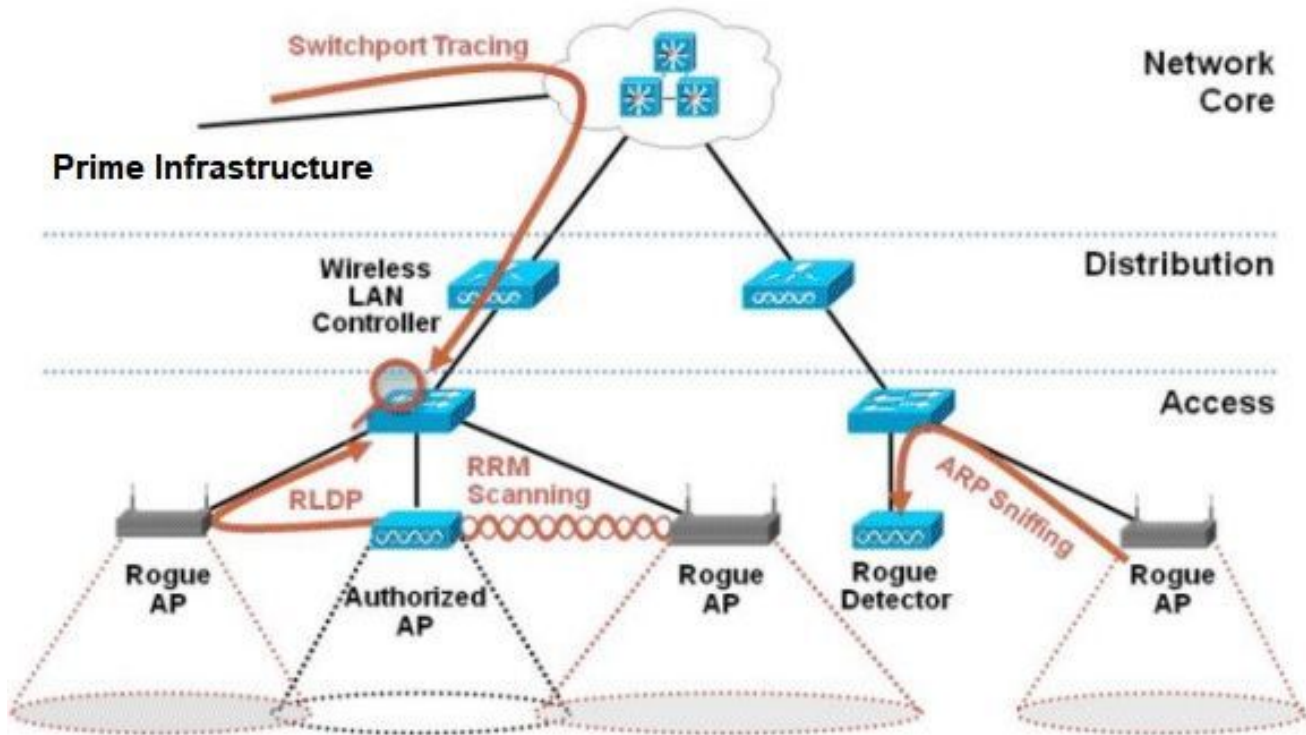
最後，評估（或完全避免）流氓自動遏制至關重要，因為如果任其自動運行，將會出現潛在的法律問題和責任。

思科統一無線網路(UWN)解決方案中的欺詐裝置管理分為三個主要階段：

- 檢測 — 無線電資源管理(RRM)掃描用於檢測欺詐裝置的存在。
- 分類 — 欺詐位置發現協定(RLDP)、欺詐檢測器（僅限第1波AP）和交換機埠跟蹤用於識別欺詐裝置是否連線到有線網路。流氓分類規則也有助於根據流氓特徵將其過濾到特定類別中。
- 緩解 — 交換機埠關閉、欺詐位置和欺詐遏制用於跟蹤其物理位置並消除欺詐裝置的威脅。

Cisco Rogue Management Diagram

Multiple Methods

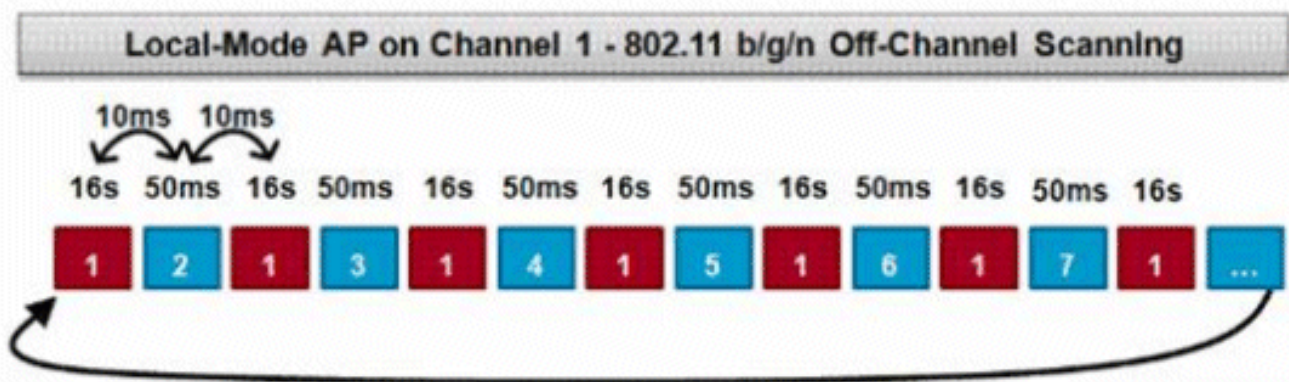


欺詐檢測

惡意軟體本質上是共用您的頻譜、但不受您控制的任何裝置。這包括欺詐接入點、無線路由器、欺詐客戶端和欺詐ad-hoc網路。Cisco UWN使用多種方法檢測基於Wi-Fi的惡意裝置，例如非通道掃描和專用監控模式功能。Cisco Spectrum Expert還可用於識別不基於802.11協定的欺詐裝置，例如藍芽網橋。

非通道掃描

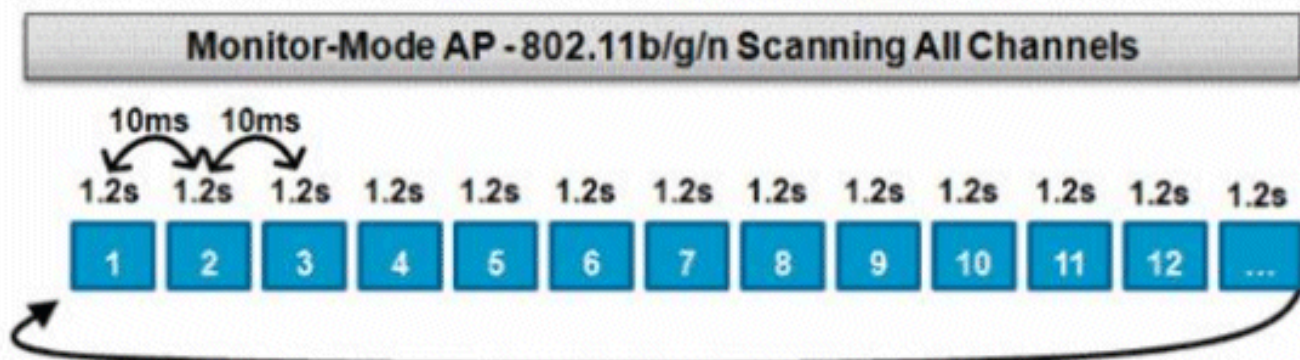
此操作由本地和Flex-Connect（在連線模式下）模式AP執行，並採用時間分段技術，該技術允許使用相同的無線電進行客戶端服務和通道掃描。由於每16秒轉換到通道外50ms的時間，預設情況下，AP僅將一小部分時間用於不為客戶端提供服務。另請注意，會出現10ms的通道更改間隔。在預設掃描間隔180秒內，每個2.4Ghz FCC通道(1-11)至少掃描一次。對於其他管制域（如ETSI），AP處於非通道狀態的時間百分比稍高。通道清單和掃描間隔都可以在RRM配置中調整。這會將效能影響限制為最大1.5%，且演算法中內建有智慧以在需要傳送高優先順序QoS訊框（例如語音）時暫停掃描。



本圖描述了2.4GHz頻段中本地模式AP的通道外掃描演算法。如果AP有一個無線電，則在5GHz無線電上並行執行類似的操作。每個紅色方塊表示在AP主通道上花費的時間，而每個藍色方塊表示在相鄰通道上用於掃描的時間。

監控模式掃描

此操作由監控模式和自適應wIPS監控模式AP執行，它們利用100%的無線電時間掃描各個頻帶中的所有通道。這樣可以加快檢測速度，並且每個通道可以花費更多時間。監控模式AP在檢測欺詐客戶端方面也非常出色，因為它們可以更全面地檢視每個通道中發生的活動。



本圖描述了2.4GHz頻帶中監控模式AP的通道外掃描演算法。如果AP有一個無線電，則在5GHz無線電上並行執行類似的操作。

本地模式和監控模式比較

本地模式AP在WLAN客戶端服務和掃描通道以發現威脅之間分割循環。因此，本地模式AP在遍歷所有通道時花費的時間更長，而且它花在收集任何特定通道上的資料上的時間也更少，因此客戶端操作不會中斷。因此，與監控模式AP相比，欺詐和攻擊檢測時間更長（3至60分鐘），可以檢測到的空中攻擊範圍更小。

此外，對突發流量（如惡意客戶端）的檢測確定性要低得多，因為AP必須在傳輸或接收流量的同時位於流量的通道上。這變成了一種概率的練習。監控模式AP將所有週期用於掃描通道，以查詢欺詐和空中攻擊。監控模式AP可同時用於自適應wIPS、位置（情景感知）服務和其他監控模式服務。

部署監控模式AP時，其優點是檢測時間更短。當監控模式AP額外配置了自適應wIPS時，可以檢測到更廣泛的空中威脅和攻擊。

本地模式AP	監控模式AP
為客戶端提供分時非通道掃描	專用掃描
偵聽每個通道上的50毫秒	偵聽每個通道上的1.2秒
可配置為掃描： <ul style="list-style-type: none"> • 所有頻道 • 國家/地區管道 (預設) • DCA通道 	掃描所有通道

欺詐識別

如果本地、flex-connect或監控模式AP偵聽來自欺詐裝置的探測響應或信標，則此資訊將通過CAPWAP傳送到進程的無線LAN控制器(WLC)。為了防止誤報，使用了多種方法來確保其他基於Cisco的受管AP不被識別為欺詐裝置。這些方法包括移動組更新、RF鄰居資料包和允許通過Prime Infrastructure(PI)列出友好AP。

惡意記錄

雖然控制器的無管理系統裝置資料庫僅包含當前檢測到的無管理系統組，但PI還包括一個事件歷史記錄，並記錄不再顯示的無管理系統組。

欺詐詳細資訊

CAPWAP AP在通道外傳輸50毫秒，以偵聽惡意客戶端、監控噪音和通道干擾。檢測到的任何欺詐客戶端或AP都會傳送到控制器，控制器會收集以下資訊：

- 非法AP MAC地址
- 檢測到欺詐的AP的名稱
- 惡意連線的客戶端MAC地址
- 安全策略
- 序言
- 訊雜比(SNR)
- 接收器訊號強度指示器(RSSI)
- 欺詐檢測通道
- 檢測到欺詐的無線電

- 惡意SSID (如果廣播惡意SSID)
- 非法IP地址
- 第一次和最後一次報告流氓行為
- 通道寬度

匯出欺詐事件

為了將欺詐事件匯出到第三方網路管理系統(NMS)進行存檔，WLC允許新增額外的SNMP陷阱接收器。當控制器檢測到欺詐或清除欺詐時，包含此資訊的陷阱會傳送給所有SNMP陷阱接收器。通過SNMP匯出事件的一個警告是，如果多個控制器檢測到相同的欺詐行為，NMS會看到重複的事件，因為關聯只在PI完成。

欺詐記錄超時

欺詐AP一旦新增到WLC記錄中，它就會一直保留在那裡，直到不再出現。在使用者可配置超時 (預設值為1200秒) 之後，_unclassified_category中的欺詐已過期。

其他狀態(如_Contained_and_Friendly_)中的惡作劇將持續存在，以便重新出現時對其應用適當的分類。

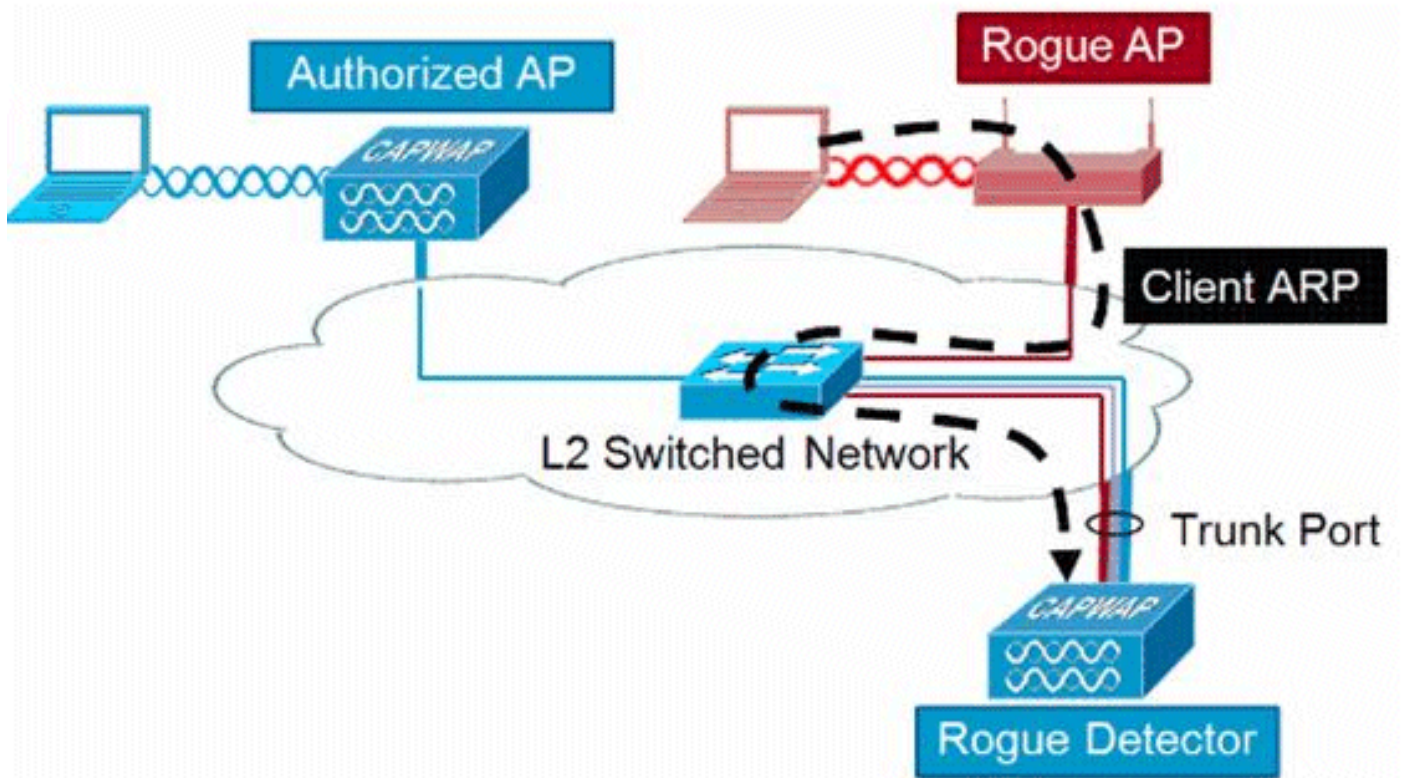
惡意記錄具有最大資料庫大小，該資料庫大小在控制器平台之間可變：

- 3504 — 檢測和遏制多達600個欺詐AP和1500個欺詐客戶端
- 5520 — 檢測和遏制最多24000惡意AP和32000 Rogue Clients
- 8540 — 檢測和遏制最多24000惡意AP和32000 Rogue Clients

惡意檢測器AP

欺詐檢測器AP旨在將空中偵聽的欺詐資訊與從有線網路獲取的ARP資訊相關聯。如果在無線中聽到作為欺詐AP或客戶端的MAC地址，並且也在有線網路上聽到MAC地址，則確定該欺詐位於有線網路上。如果檢測到欺詐無線接入點位於有線網路上，則該欺詐無線接入點的警報嚴重性將提高到_critical_。欺詐檢測器AP無法成功識別使用NAT的裝置背後的欺詐客戶端。

當欺詐AP具有某種形式的身份驗證 (WEP或WPA) 時，使用此方法。在欺詐AP上配置身份驗證形式時，輕量AP無法關聯，因為它不知道在欺詐AP上配置的身份驗證方法和憑據。



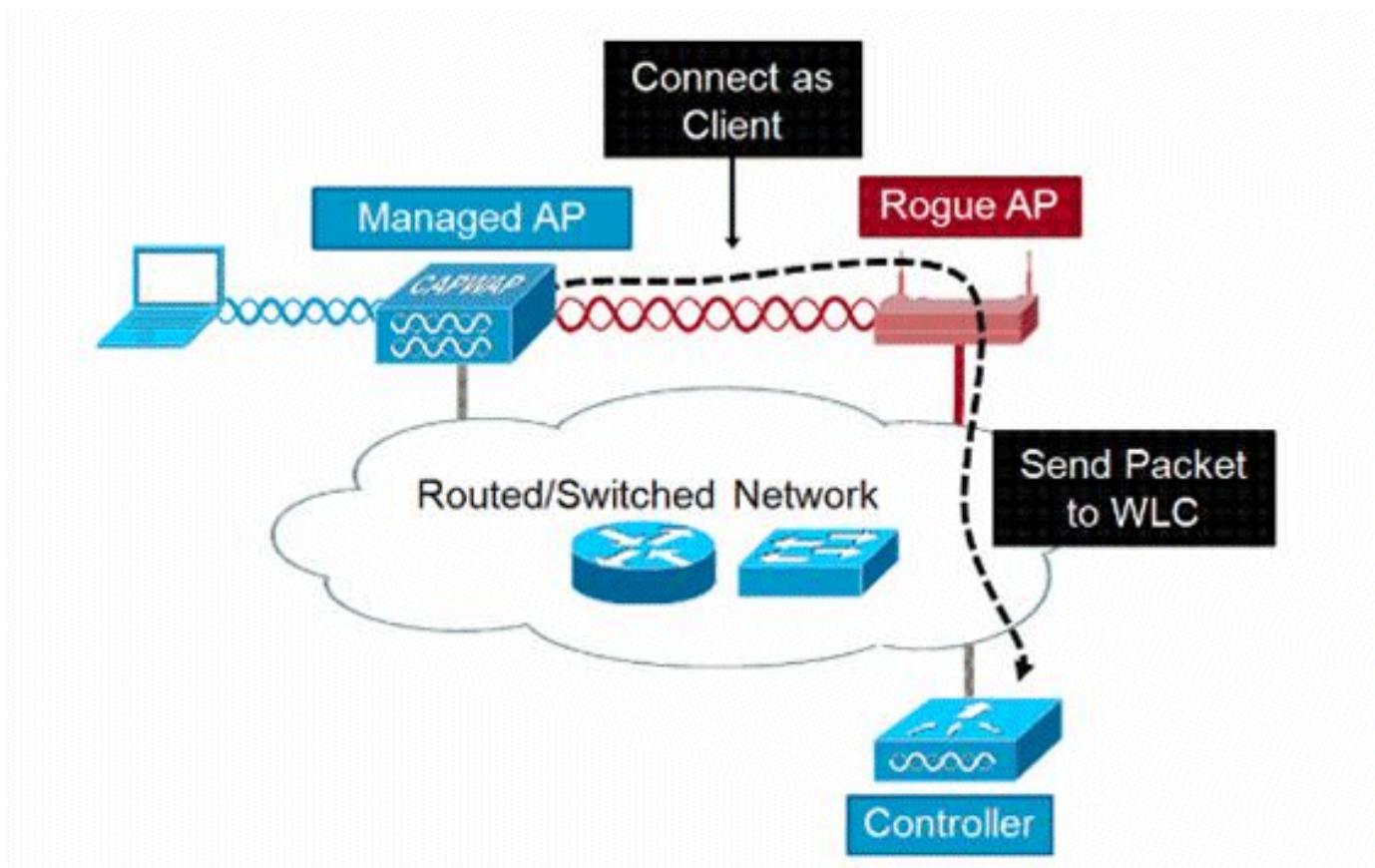
 注意：只有第1波AP可以配置為欺詐檢測器。

可擴充性注意事項

欺詐檢測器AP最多可以檢測到500個惡意客戶端和500個惡意客戶端。如果欺詐檢測器放置在含有太多欺詐裝置的中繼上，則會超出這些限制，從而導致問題。為了防止發生這種情況，請將惡意檢測器AP保留在網路的分佈層或接入層。

RLDP

RLDP的目標是識別特定欺詐AP是否連線到有線基礎設施。此功能實質上使用距離最近的AP作為無線客戶端連線到欺詐裝置。作為使用者端建立連線後，會傳送一個封包，其中包含WLC的目的地址，用來評估AP是否已連線到有線網路。如果檢測到欺詐無線接入點位於有線網路上，則該欺詐無線接入點的警報嚴重性會提高到嚴重。



這裡列出了RLDP演算法：

1. 通過使用訊號強度值確定距離欺詐最近的統一AP。
2. 然後，AP作為WLAN客戶端連線到欺詐路由器，在它超時之前嘗試三次關聯。
3. 如果關聯成功，則AP使用DHCP獲取IP地址。
4. 如果取得了IP位址，則AP（充當WLAN使用者端）會將UDP封包傳送到每個控制器IP位址。
5. 如果控制器從客戶端接收到甚至一個RLDP資料包，則該惡意軟體被標籤為線上狀態，嚴重性為「嚴重」。

 註：如果在控制器網路和惡意裝置所在網路之間設定了過濾規則，則RLDP資料包無法到達控制器。

RLDP注意事項

- RLDP只能與廣播其SSID（禁用身份驗證和加密）的開放無管理AP配合使用。
- RLDP要求充當客戶端的受管AP能夠通過DHCP在欺詐網路上獲取IP地址
- 手動RLDP可用於多次嘗試和跟蹤欺詐上的RLDP。

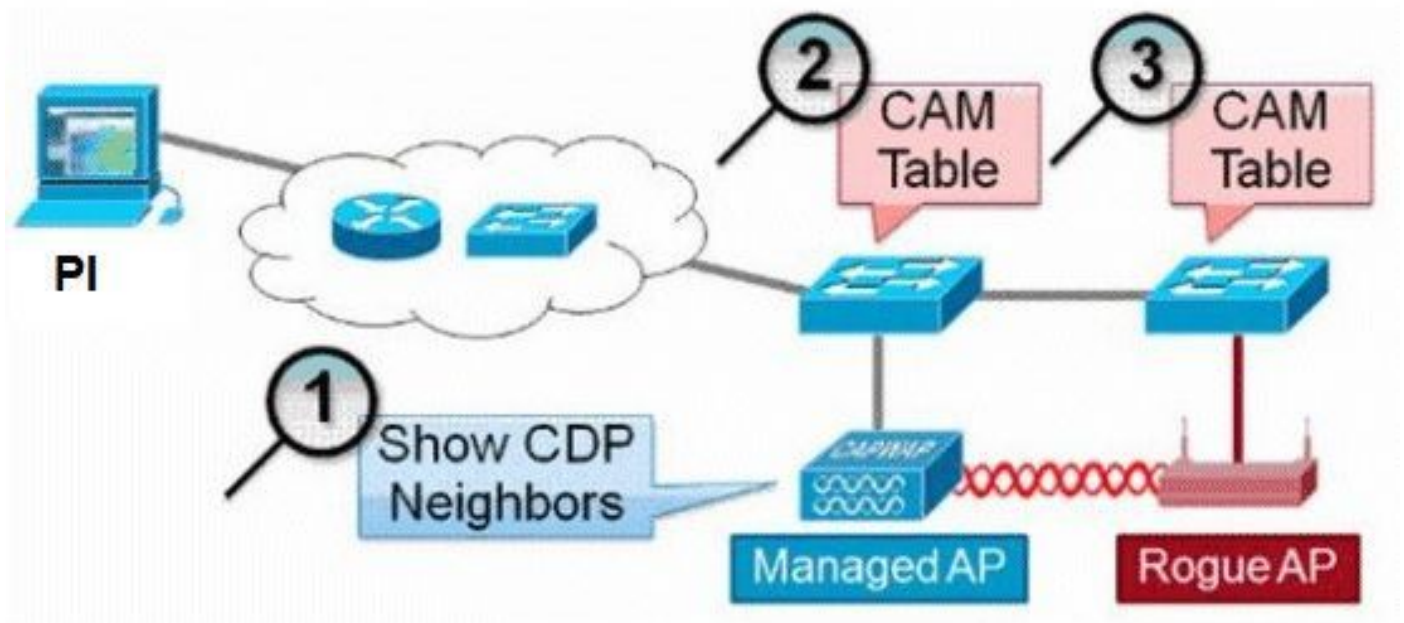
- 在RLDP進程上，AP無法為客戶端提供服務。這會對本地模式AP的效能和連線性產生負面影響。
- RLDP不會嘗試連線到在5GHz DFS通道中運行的欺詐AP。

交換器連線埠追蹤

交換機埠跟蹤是一種惡意AP緩解技術。雖然交換機埠跟蹤是在PI上啟動的，但它同時利用CDP和SNMP資訊來跟蹤到網路中特定埠的欺詐行為。

為了運行交換機埠跟蹤，必須將網路中的所有交換機使用SNMP憑證新增到PI。雖然只讀憑證可以識別欺詐裝置所在的埠，但讀寫憑證允許PI也關閉埠，因此它包含威脅。

目前，此功能僅適用於運行啟用CDP的Cisco IOS®的Cisco交換機，並且必須在託管AP上啟用CDP。



交換器連線埠追蹤的演演算法如下：

1. PI找到最接近的AP，它檢測空中欺詐AP，並檢索其CDP鄰居。
2. 然後，PI使用SNMP檢查鄰居交換機中的CAM表，查詢正匹配以識別欺詐位置。
3. 正匹配基於準確的惡意MAC地址、+1/-1惡意MAC地址、任何惡意客戶端MAC地址或基於MAC地址中固有的供應商資訊的OUI匹配。
4. 如果在最近的交換器上找不到正相符專案，則PI會在最多兩跳遠的相鄰交換器上繼續搜尋（預設情況下）。

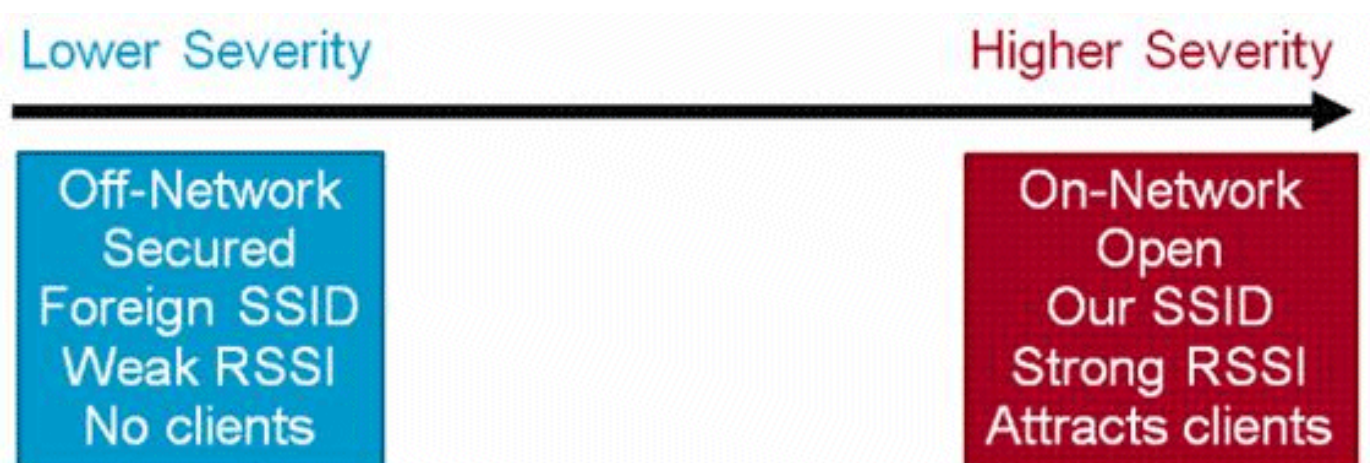
Wired-Side Tracing Techniques

Comparison

	How it Works	What It Detects	Accuracy
Switchport Tracing	<ol style="list-style-type: none"> 1. AP hears rogue over air 2. Detecting AP advises of nearby switches 3. Trace starts on nearby switches 4. Results reported in order of probability 5. Administrator may disable port 	<ul style="list-style-type: none"> • Open APs • Secured APs • NAT APs 	<ul style="list-style-type: none"> • Moderate
RLDP	<ol style="list-style-type: none"> 1. AP hears rogue over air 2. Detecting AP connects as client to rogue AP 3. Detecting AP sends RLDP packet 4. If RLDP packet seen at WLC, then on wire 	<ul style="list-style-type: none"> • Open APs • NAT APs 	<ul style="list-style-type: none"> • 100%
Rogue Detector	<ol style="list-style-type: none"> 1. Place detector AP on trunk 2. Detector receives all rogue MACs from WLC 3. Detector AP matches rogue MACs from wired-side ARPs 	<ul style="list-style-type: none"> • Open APs • Secured APs • NAT APs 	<ul style="list-style-type: none"> • High

惡意軟體分類

預設情況下，Cisco UWN檢測到的所有惡意程式均被視為未分類。如本圖所示，可以根據包括RSSI、SSID、安全型別、開啟/關閉網路以及客戶端數量在內的許多標準對惡意軟體進行分類：



欺詐分類規則

流氓分類規則，允許您定義一組條件，將流氓標籤為惡意或友好。這些規則是在PI或WLC上設定的，但會在發現新的惡意程式時，在控制器上執行。

請參閱[檔案無線LAN控制器\(WLC\)和Prime基礎架構\(PI\)中的基於規則的欺詐分類](#)，以取得更多有關WLC中欺詐規則的資訊。

HA事實

如果手動將任何無管理系統裝置移到包含狀態（任何類）或友好狀態，則這些資訊儲存在備用Cisco WLC快閃記憶體中；但是資料庫不會更新。發生HA切換時，載入之前備用Cisco WLC快閃記憶體中的欺詐清單。

在「高可用性」場景中，如果將欺詐檢測安全級別設定為「高」或「嚴重」，則備用控制器上的欺詐計時器僅在欺詐檢測掛起穩定時間（即300秒）後啟動。因此，備用控制器上的作用中組態只會在300秒後反射。

Flex-Connect事實

處於連線模式的FlexConnect AP（已啟用欺詐檢測）會從控制器獲取包含清單。如果在控制器中設定了自動包含SSID和自動包含adhoc，則這些配置將設定為處於連線模式的所有FlexConnect AP，並且AP將其「儲存」在其記憶體中。

當FlexConnect AP移動到獨立模式時，將執行以下任務：

- 由控制器設定的包含繼續。
- 如果FlexConnect AP檢測到任何欺詐AP的SSID與基礎SSID（在FlexConnect AP所連線的控制器中配置的SSID）的SSID相同，則在進入獨立模式之前，如果從控制器啟用了「自動包含SSID」，則系統開始遏制操作。
- 如果FlexConnect AP檢測到任何臨時欺詐，則當控制器處於連線模式時，如果從控制器啟用自動包含臨時設定，則限制會啟動。

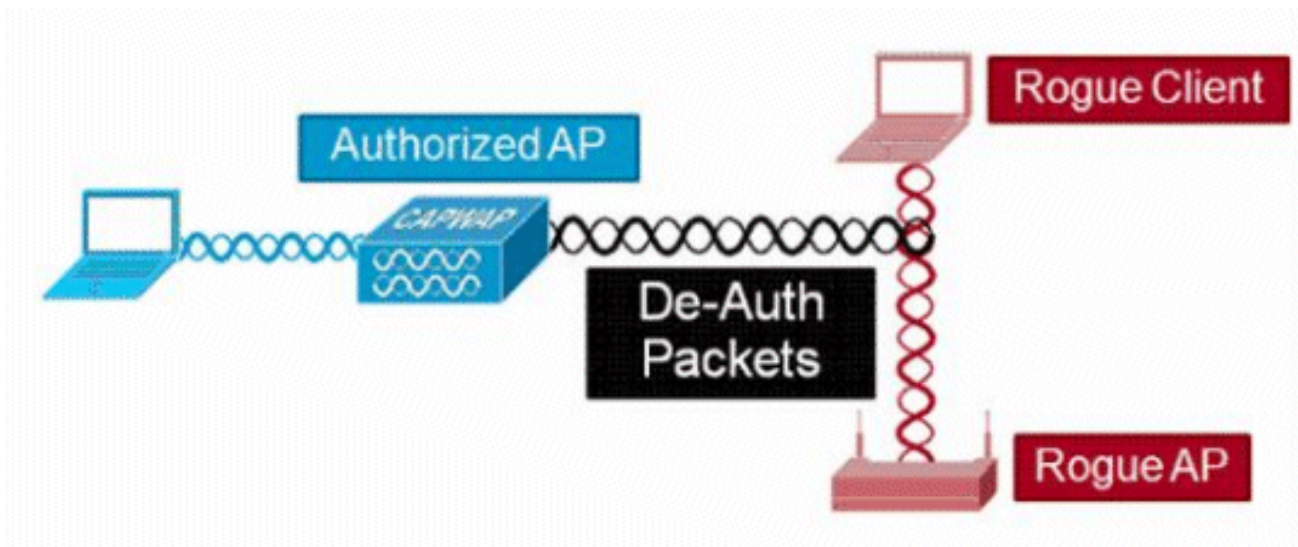
當獨立FlexConnect AP返回連線模式時，將執行以下任務：

- 所有遏制都將被清除。
- 從控制器發起的包含會接管操作。

欺詐緩解

惡意遏制

遏制是一種方法，它使用無線資料包臨時中斷欺詐裝置上的服務，直到可以物理方式移除該服務。遏制使用惡意AP的欺騙源地址來欺騙解除身份驗證資料包，以便啟動任何關聯的客戶端。



惡意遏制詳細資訊

在無客戶端的欺詐AP上啟動的遏制僅使用傳送到廣播地址的反身份驗證幀：

Source	Destination	Data Rate	Size	Protocol
Rogue AP	Ethernet Broadcast	6.0	144	802.11 Beacon
Rogue AP	Ethernet Broadcast	6.0	56	802.11 Deauth
Rogue AP	Ethernet Broadcast	6.0	30	802.11 Deauth

Broadcast Deauth frames only

在帶有客戶端的欺詐AP上啟動的包含使用傳送到廣播地址和客戶端地址的去身份驗證幀：

Source	Destination	Data Rate	Size	Protocol
Rogue AP	Ethernet Broadcast	6.0	144	802.11 Beacon
Rogue AP	Ethernet Broadcast	6.0	56	802.11 Deauth
Rogue AP	Ethernet Broadcast	6.0	30	802.11 Deauth
Rogue AP	Rogue Client	6.0	30	802.11 Deauth
Rogue AP	Rogue Client	6.0	30	802.11 Deauth
Rogue AP	Rogue Client	6.0	30	802.11 Deauth

Broadcast and Unicast Deauth frames

在受管AP的電源級別和最低啟用資料速率下傳送包含資料包。

遏制每100毫秒至少傳送2個資料包：

Source	Destination	De...	Size	Relative Time	Protocol
W Rogue AP	Ethernet Broadcast	6.0	56	0.000000	802.11 Deauth
W Rogue AP	Ethernet Broadcast	6.0	30	0.000004	802.11 Deauth
W Rogue AP	Ethernet Broadcast	6.0	144	0.000007	802.11 Beacon
W Rogue AP	Ethernet Broadcast	6.0	56	0.102414	802.11 Deauth
W Rogue AP	Ethernet Broadcast	6.0	30	0.102419	802.11 Deauth

~100ms

註：非監控模式AP執行的包含以500ms的間隔傳送，而不是以監控模式AP使用的100ms間隔傳送。

- 單個欺詐裝置可以由1到4個受管AP控制，它們協同工作以暫時緩解威脅。
- 可通過使用本地模式、監控模式和flex-connect (連線) 模式AP來執行包含。對於flex-connect AP的本地模式，每個無線電最多可以包含三個非法裝置。對於監控模式AP，每個無線電最多可以包含六個欺詐裝置。

自動遏制

除了通過PI或WLC GUI手動啟動非法裝置上的遏制功能外，在某些情況下還可以自動啟動遏制。此組態位於PI或控制器介面的Rogue Policies一節的Generalin下。預設情況下會禁用這些功能，啟用這些功能只是為了消除造成最大損害的威脅。

- Rogue on Wire — 如果識別出非法裝置要連線到有線網路，則會自動將其置於控制之下。
- 使用我們的SSID — 如果欺詐裝置使用的SSID與控制器上配置的SSID相同，則自動包含該SSID。此功能旨在解決蜜罐攻擊所造成的損害。
- 欺詐AP上的有效客戶端 — 如果發現Radius/AAA伺服器中列出的客戶端與欺詐裝置關聯，則僅針對該客戶端啟動包含功能，可防止該客戶端與任何非託管AP關聯。
- AdHoc Rogue AP — 如果發現ad-hoc網路，則會自動包含它。

惡意遏制警告

- 由於密封使用部分受管AP無線電時間傳送取消身份驗證幀，因此資料和語音客戶端的效能受到多達20%的負面影響。對於資料客戶端，影響是吞吐量降低。對於語音客戶端，控制可能導致對話中斷並降低語音品質。
- 對鄰居網路發起遏制可能會產生法律影響。在啟動遏制之前，請確保流氓裝置位於您的網路內並構成安全風險。

交換器連線埠關閉

使用SPT跟蹤交換機埠後，在PI中有一個選項可以禁用該埠。管理員必須手動執行本練習。如果從網路物理上刪除了欺詐裝置，則有一個選項可用於通過PI啟用交換機埠。

設定

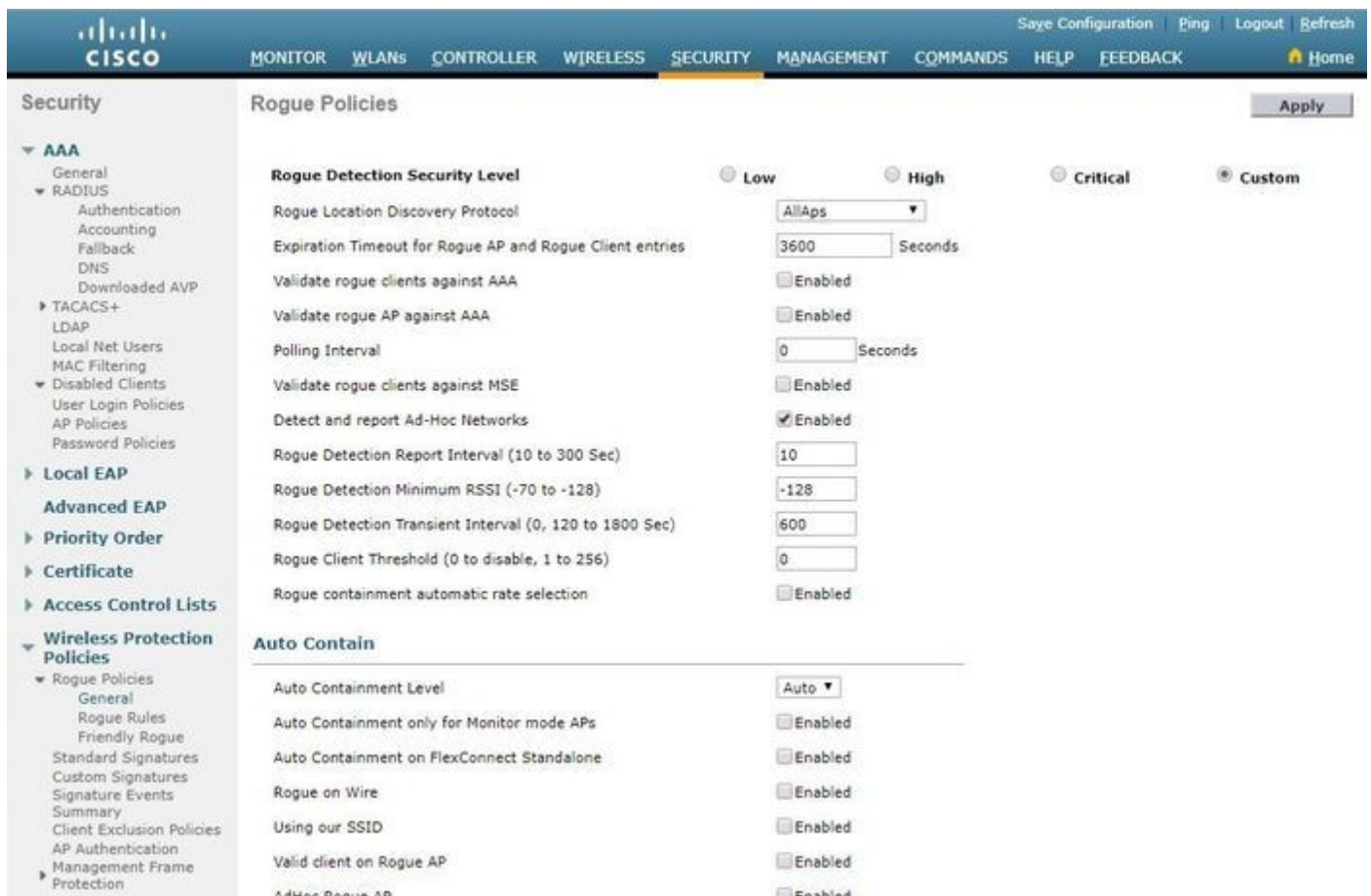
配置欺詐檢測

預設情況下，控制器中會啟用欺詐偵測。

要配置各種選項，請導航至安全>無線保護策略>欺詐策略>常規。例如：

步驟 1.更改非法AP超時。

步驟 2.啟用對ad-hoc欺詐網路的檢測。



The screenshot displays the Cisco WLC configuration interface for Rogue Policies. The left sidebar shows the navigation menu with 'Wireless Protection Policies' expanded to 'Rogue Policies'. The main content area is divided into two sections: 'Rogue Detection Security Level' and 'Auto Contain'.

Rogue Detection Security Level:

- Level: Custom (selected)
- Rogue Location Discovery Protocol: All Aps
- Expiration Timeout for Rogue AP and Rogue Client entries: 3600 Seconds
- Validate rogue clients against AAA: Disabled
- Validate rogue AP against AAA: Disabled
- Polling Interval: 0 Seconds
- Validate rogue clients against MSE: Disabled
- Detect and report Ad-Hoc Networks: Enabled (checked)
- Rogue Detection Report Interval (10 to 300 Sec): 10
- Rogue Detection Minimum RSSI (-70 to -128): -128
- Rogue Detection Transient Interval (0, 120 to 1800 Sec): 600
- Rogue Client Threshold (0 to disable, 1 to 256): 0
- Rogue containment automatic rate selection: Disabled

Auto Contain:

- Auto Containment Level: Auto
- Auto Containment only for Monitor mode APs: Disabled
- Auto Containment on FlexConnect Standalone: Disabled
- Rogue on Wire: Enabled
- Using our SSID: Enabled
- Valid client on Rogue AP: Enabled
- AdHoc Rogue AP: Enabled

在CLI上：

```
<#root>
```

```
(Cisco Controller) >
```

```
config rogue ap timeout ?
```

```
<seconds> The number of seconds<240 - 3600> before rogue entries are flushed
```

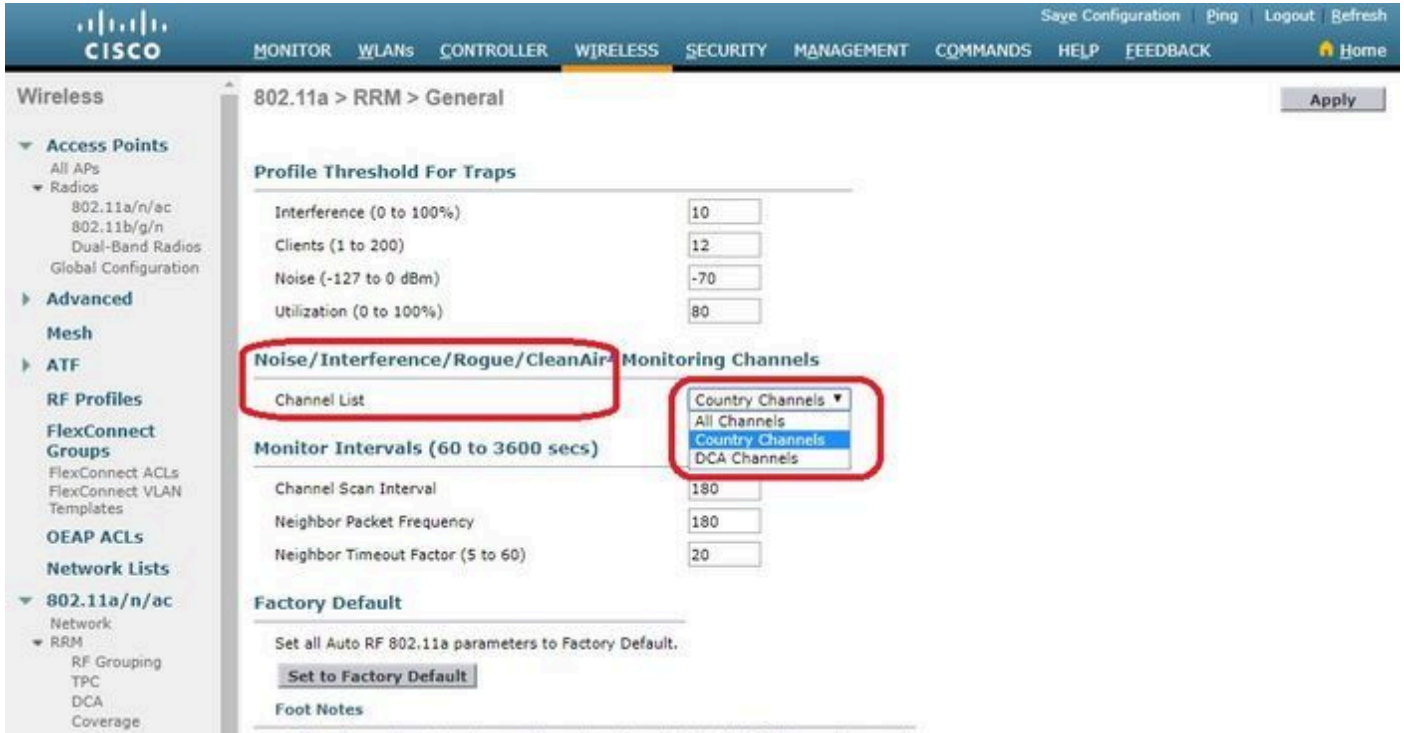
```
(Cisco Controller) >
```

```
config rogue adhoc enable/disable
```

為欺詐檢測配置通道掃描

對於本地/Flex-Connect/Monitor模式AP，在RRM配置下有一個選項，允許使用者選擇掃描哪些通道以查詢欺詐裝置。取決於配置，AP會掃描所有通道/國家/地區通道/DCA通道以查詢無管理系統。

若要在GUI中設定此設定，請導覽至Wireless > 802.11a/802.11b > RRM > General，如下圖所示。



在CLI上：

```
<#root>
```

```
(Cisco Controller) >
```

```
config advanced 802.11a monitor channel-list ?
```

```
all           Monitor all channels
country       Monitor channels used in configured country code
dca           Monitor channels used by automatic channel assignment
```

配置無管理系統分類

手動對欺詐AP分類

要將惡意AP分類為友好、惡意或未分類，請導航到Monitor > Rogue > Unclassified AP，然後點選特定的惡意AP名稱。從下拉式清單中選擇選項，如下圖所示。

Monitor

Rogue AP Detail

Summary

- Access Points
- Cisco CleanAir
- Statistics
- CDP
- Rogues
 - Friendly APs
 - Malicious APs
 - Custom APs
 - Unclassified APs
 - Rogue Clients
 - Adhoc Rogues
 - Friendly Adhoc
 - Malicious Adhoc
 - Custom Adhoc
 - Unclassified Adhoc
 - Rogue AP ignore-list
- Clients
- Sleeping Clients
- Multicast
- Applications
- Lync
- Local Profiling

MAC Address: 00:06:91:43:6d:e2

Type: AP

Is Rogue On Wired Network?: No

First Time Reported On: Thu May 30 16:21:30 2019

Last Time Reported On: Fri May 31 13:07:11 2019

Class Type: Malicious

State: No

Manually Contained: No

Update Status: -- Choose New Status --

APs that detected this Rogue

Base Radio MAC	AP Name	SSID	Channel	Channel Width (Mhz)	Radio Type	Security Policy	Pre-A
b4:de:31:c6:30:c0	AP2800-1	Cisco-17D90F4C	6	20	802.11n2.4G	Open	Long

[Clients associated to this Rogue AP](#)

在CLI上:

```
<#root>
```

```
(Cisco Controller) >
```

```
config rogue ap ?
```

```
classify      Configures rogue access points classification.
friendly      Configures friendly AP devices.
rldp          Configures Rogue Location Discovery Protocol.
ssid          Configures policy for rogue APs advertsing our SSID.
timeout       Configures the expiration time for rogue entries, in seconds.
valid-client  Configures policy for valid clients which use rogue APs.
```

若要手動從欺詐清單中移除欺詐條目，請導覽至Monitor > Rogue > Unclassified AP，然後按一下 Remove，如下圖所示。

Monitor

Unclassified Rogue APs

Entries 1 - 50 of 140

Current Filter: None [Change Filter] [Clear Filter]

Remove
Contain
Move to Alert

MAC Address	SSID	Channel	# Detecting Radios	Number of Clients	Status
00:06:91:43:6d:e2	Cisco-17D90F4C	6	1	0	Alert
00:1a:2b:58:6b:13	NUMERICABLE-29F3	6	1	0	Alert
00:22:ce:ff:38:aa	S7afb7	11	1	0	Alert
00:22:ce:ff:47:5a	d9b9a9	Unknown	0	0	Alert
00:23:be:30:59:18	368a98	11	1	0	Alert
00:23:be:51:85:01	eb4fb0	11	1	0	Alert

要將惡意AP配置為友好AP，請導航至安全>無線保護策略>惡意策略>友好路由，然後新增惡意MAC地址。

新增的友好無管理系統專案可以從Monitor > Rogues > Friendly Roguepage進行驗證，如下圖所示

Security

Friendly Rogue > Create

Apply

MAC Address: 11:22:33:44:55:66

Type: Friendly

配置欺詐檢測器AP

要通過GUI將AP配置為欺詐檢測器，請導航至Wireless > All APs。選擇AP名稱並更改AP模式，如下圖所示。

在CLI上:

```
<#root>
```

```
(Cisco Controller) >
```

```
config ap mode rogue AP_Managed
```

Changing the AP's mode cause the AP to reboot.
Are you sure you want to continue? (y/n) y

為欺詐檢測器AP配置交換機埠

```
interface GigabitEthernet1/0/5
description Rogue Detector
switchport trunk native vlan 100
switchport mode trunk
```



註：此配置中的本地VLAN是具有IP連線至WLC的VLAN。

配置RLDP

要在控制器GUI中配置RLDP，請導航至安全>無線保護策略>欺詐策略>常規。

The screenshot shows the Cisco Security configuration interface for Rogue Policies. The 'Rogue Location Discovery Protocol' is highlighted with a red box. The 'Rogue Detection Security Level' is set to 'Custom', and the 'Rogue Location Discovery Protocol' dropdown is set to 'MonitorModeAps'. The 'Auto Contain' section is also visible.

監控模式AP — 僅允許處於監控模式的AP參與RLDP。

所有AP — 本地/Flex-Connect/監控模式AP均參與RLDP進程。

Disabled — 不會自動觸發RLDP。但是，使用者可以通過CLI為特定MAC地址手動觸發RLDP。

 **注意：** 如果監控模式AP和本地/Flex-Connect AP都檢測到特定欺詐超過-85dbm RSSI，則監控模式AP將優先於本地/Flex-Connect AP以執行RLDP。

在CLI上:

```
<#root>
```

```
(Cisco Controller) >
```

```
config rogue ap rldp enable
```

```
?
```

```
alarm-only      Enables RLDP and alarm if rogue is detected
auto-contain    Enables RLDP, alarm and auto-contain if rogue is detected.
```

```
(Cisco Controller) >config rogue ap rldp enable alarm-only ?
```

```
monitor-ap-only Perform RLDP only on monitor AP
```

只能通過命令提示符配置RLDP時間表和手動觸發器。手動啟動RLDP:

<#root>

(Cisco Controller) >

config rogue ap rldp initiate

?

<MAC addr> Enter the MAC address of the rogue AP (e.g. 01:01:01:01:01:01).

有關RLDP的時間表：

<#root>

(Cisco Controller) >

config rogue ap rldp schedule ?

add	Enter the days when RLDP scheduling to be done.
delete	Enter the days when RLDP scheduling needs to be deleted.
enable	Configure to enable RLDP scheduling.
disable	Configure to disable RLDP scheduling.

(Cisco Controller) >

config rogue ap rldp schedule add ?

fri	Configure Friday for RLDP scheduling.
sat	Configure Saturday for RLDP scheduling.
sun	Configure Sunday for RLDP scheduling.
mon	Configure Monday for RLDP scheduling.
tue	Configure Tuesday for RLDP scheduling.
wed	Configure Wednesday for RLDP scheduling.
thu	Configure Thursday for RLDP scheduling.

可以使用以下命令配置RLDP重試次數：

<#root>

(Cisco Controller) >

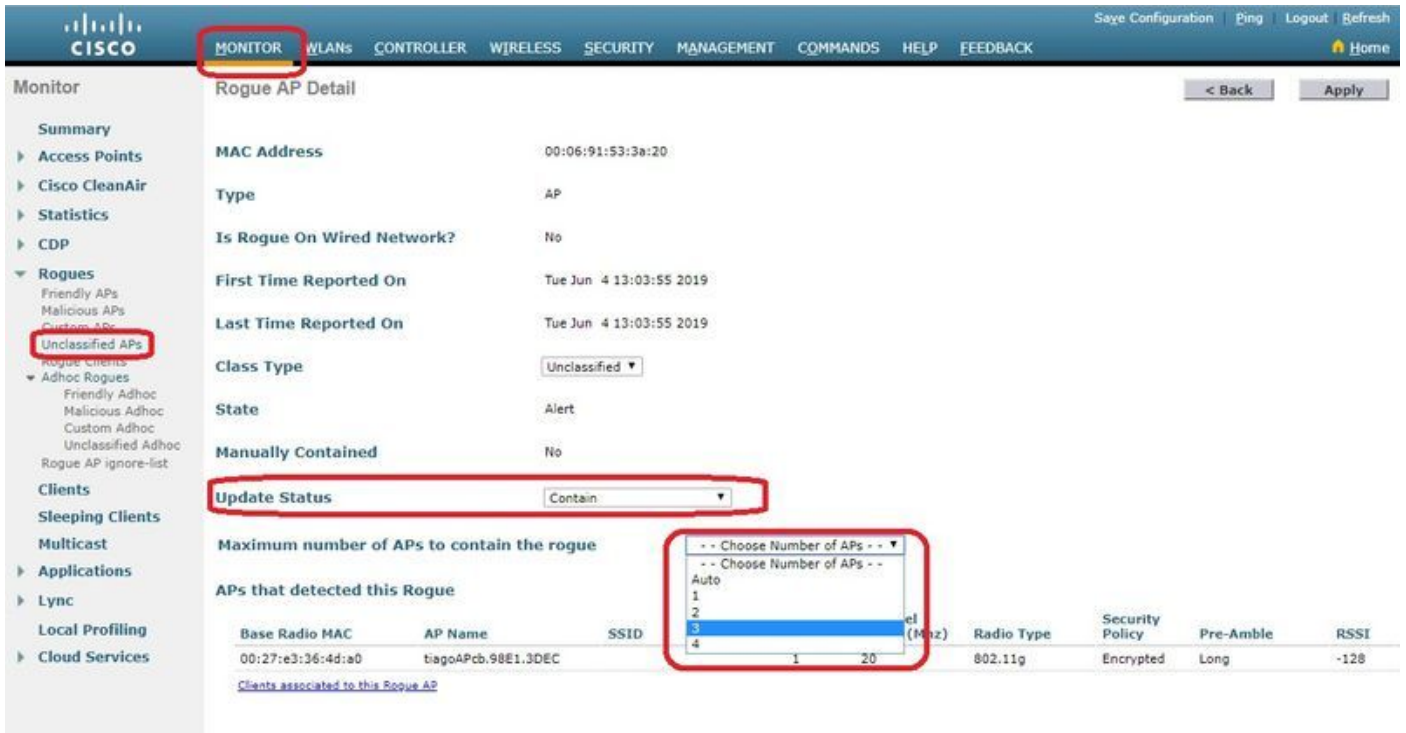
config rogue ap rldp retries ?

<count> Enter the no.of times(1 - 5) RLDP to be tried per Rogue AP.

配置欺詐緩解

配置手動遏制

若要手動控制非法AP，請導覽至Monitor > Rogues > Unclassified，如下圖所示。



在CLI上:

```
<#root>
```

```
(Cisco Controller) >
```

```
config rogue client
```

```
?
```

```
aaa
```

Configures to validate if a rogue client is a valid client which uses AAA/local databases.

```
alert
```

Configure the rogue client to the alarm state.

```
contain
```

Start to contain a rogue client.

```
delete
```

Delete rogue Client

```
mse
```


Configures to validate if a rogue client is a valid client which uses MSE.

```
(Cisco Controller) >
```

```
config rogue client contain 11:22:33:44:55:66
```

```
?
```


```
<num of APs> Enter the maximum number of Cisco APs to actively contain the rogue client [1-4].
```

 註：特定欺詐可以包含1-4個AP。預設情況下，控制器使用一個AP來包含客戶端。如果兩個AP能夠檢測到特定的欺詐，則無論該AP模式如何，具有最高RSSI的AP都將包含客戶端。

自動遏制

要配置自動遏制，請轉到安全>無線保護策略>無管理系統策略>常規，然後為網路啟用所有適用的選項。

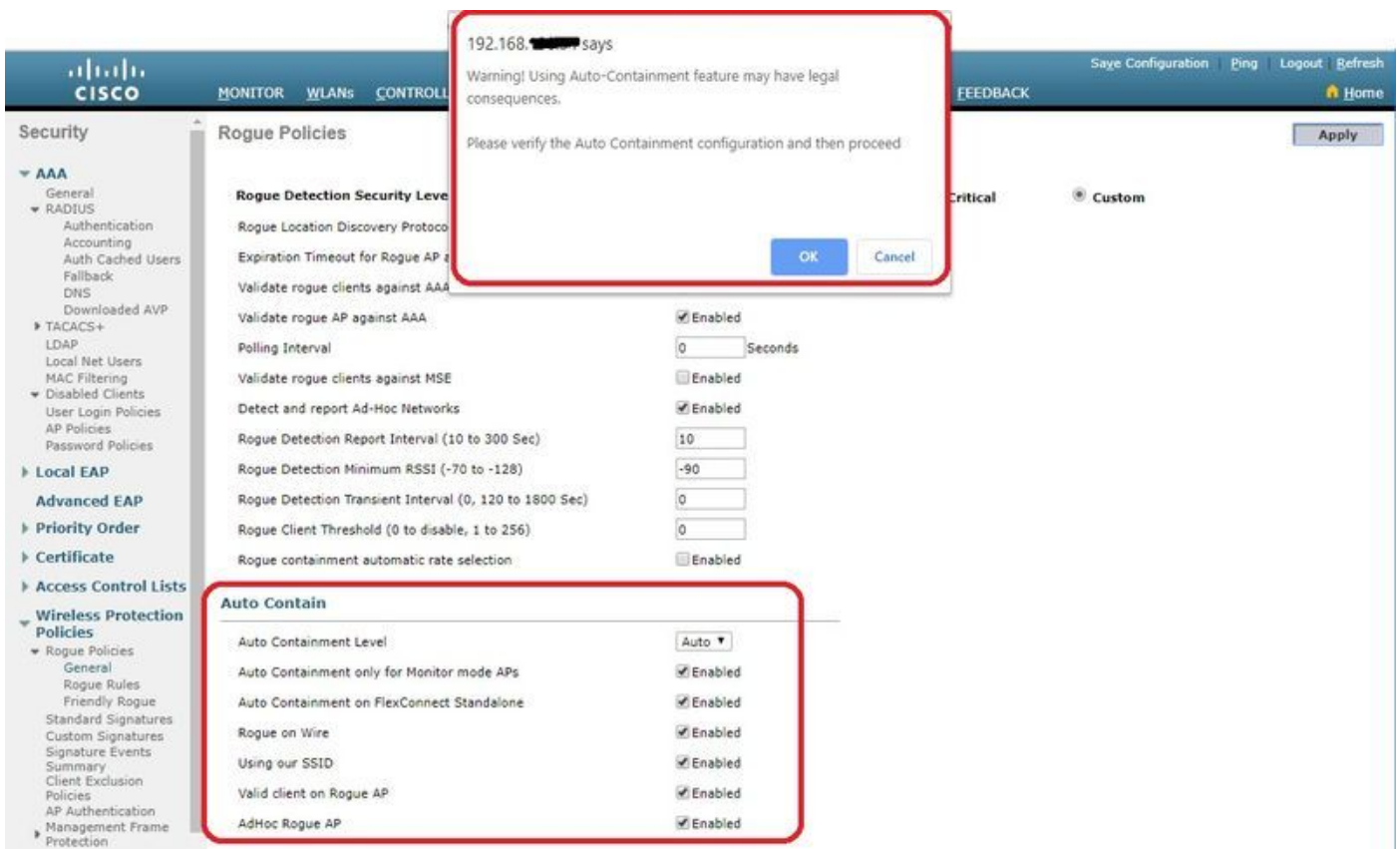
如果您希望Cisco WLC自動包含某些欺詐裝置，請選中這些框。否則，將覈取方塊保持未選中狀態，即預設值。

 **警告：**啟用這些引數中的任何一個時，系統會顯示以下消息：「使用此功能會產生法律後果。是否要繼續？」工業、科學和醫療(ISM)頻段中的2.4和5 GHz頻率對公眾開放，無需許可證即可使用。因此，控制另一方網路上的裝置可能會產生法律後果。

以下是自動包含引數：

參數	說明
自動包含級別	<p>下拉選單，您可以在其中從1到4中選擇欺詐自動遏制級別。</p> <p>當通過任何自動遏制策略將欺詐裝置移動到被包含狀態時，您最多可以選擇四個用於自動遏制的AP。</p> <p>您也可以選擇Auto（自動）以自動選擇用於自動包含的AP數量。Cisco WLC根據RSSI選擇所需的AP數量以有效遏制。</p> <p>與每個包含級別關聯的RSSI值如下：</p> <ul style="list-style-type: none">• 1 — 0到-55 dBm• 2 — -75至-55 dBm• 3 — -85至-75 dBm• 4 — 小於-85 dBm
僅對監控模式AP自動包含	選中此覈取方塊可啟用監控模式AP以進行自動包含。預設設定為禁用狀態。
FlexConnect獨立版上的自動包含	選中此覈取方塊可在獨立模式下啟用FlexConnect AP上的自動包含功能。預設設定為禁用狀態。當FlexConnect AP處於獨立模式時，您只能啟用使用我們的SSID或AdHoc欺詐AP自動遏制策略。獨立AP連線回Cisco WLC後，包含停止。
有線欺詐	選中該覈取方塊，可自動包含有線網路上檢測到的惡意程式。預設設定為禁用狀態。
使用我們的SSID	選中該覈取方塊，可自動包含通告網路SSID的那些無管理系統。如果未選擇

參數	說明
	此引數，Cisco WLC僅在檢測到此類欺詐時生成警報。預設設定為禁用狀態。
欺詐AP上的有效客戶端	選中此覈取方塊，可自動包含與受信任客戶端相關聯的欺詐接入點。如果未選擇此引數，Cisco WLC僅在檢測到此類欺詐時生成警報。預設設定為禁用狀態。
AdHoc欺詐AP	覈取方塊可自動包含由Cisco WLC檢測到的ad-hoc網路。如果未選擇此引數，Cisco WLC僅在檢測到此類網路時生成警報。預設設定為禁用狀態。



按一下Apply以將資料傳送到Cisco WLC，但不會在電源循環中保留資料；這些引數會暫時儲存在易失性RAM中。

在CLI上:

```
<#root>
```

```
(Cisco Controller) >
```

```
config rogue adhoc ?
```

```
alert Stop Auto-Containment, generate a trap upon detection of the adhoc rogue.
```


auto-contain	Automatically contain adhoc rogue.
contain	Start to contain adhoc rogue.
disable	Disable detection and reporting of Ad-Hoc rogues.
enable	Enable detection and reporting of Ad-Hoc rogues.
external	Acknowledge presence of a adhoc rogue.

(Cisco Controller) >

```
config rogue adhoc auto-contain ?
```

(Cisco Controller) >

```
config rogue adhoc auto-contain
```

```
Warning! Use of this feature has legal consequences  
Do you want to continue(y/n) :y
```

使用Prime Infrastructure

Cisco Prime Infrastructure 可用於設定和監控一個或多個控制器以及關聯的AP。Cisco PI擁有便於進行大型系統監視和控制的工具。在思科無線解決方案中使用Cisco PI時，控制器會定期確定客戶端、非法接入點、非法接入點客戶端、射頻ID(RFID)標籤位置，並將這些位置儲存在Cisco PI資料庫中。

Cisco Prime Infrastructure 支援基於規則的分類，並使用在控制器上設定的分類規則。發生以下事件後，控制器會將陷阱傳送到Cisco Prime Infrastructure:

- 如果未知接入點首次進入「友好」狀態，則僅當無管理系統狀態為「警報」時，控制器才會向Cisco Prime基礎設施傳送陷阱。如果陷阱狀態為Internal或External，則它不會傳送陷阱。
- 如果在逾時時間到期後移除arogueentry，控制器會向Cisco Prime Infrastructure Forrogue存取點傳送陷阱，這些存取點會分類為惡意（警示、威脅）或未分類（警示）。控制器不會刪除具有以下狀態的條目：Contained、Contained Pending、Internal和External。

驗證


若要在圖形介面的控制器中尋找欺詐詳細資訊，請導覽至Monitor > Rogues，如下圖所示。

The screenshot shows the Cisco WLC Monitor interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar has a 'Monitor' section with sub-items: Summary, Access Points, Cisco CleanAir, Statistics, CDP, Rogues (expanded), Clients, Sleeping Clients, and Multicast. The 'Rogues' section is further expanded to show 'Adhoc Rogues'. The main content area is titled 'Unclassified Rogue APs' and shows a table of detected APs. The table has columns for MAC Address, SSID, Channel, # Detecting Radios, Number of Clients, and Status. The table contains 10 entries, all with a status of 'Alert'.

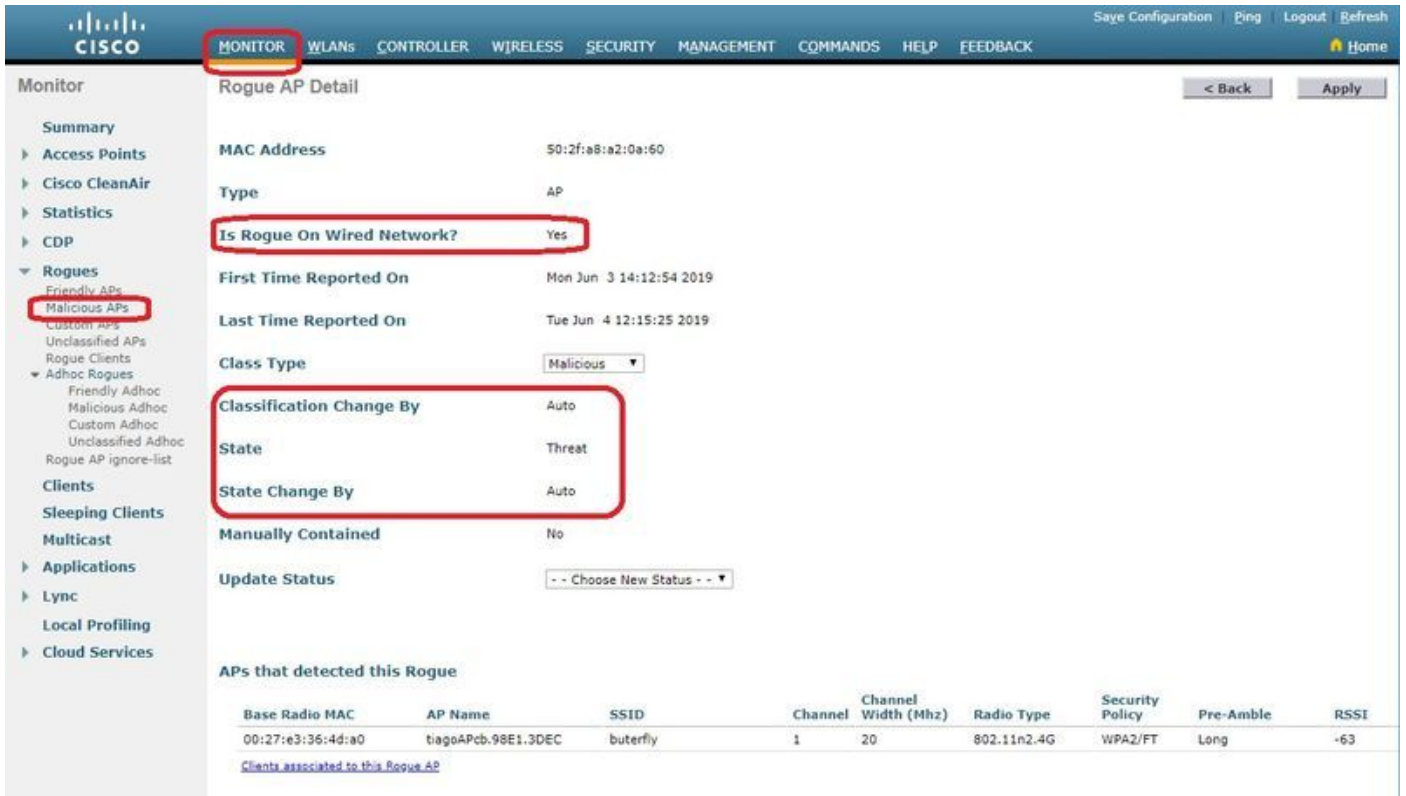
MAC Address	SSID	Channel	# Detecting Radios	Number of Clients	Status
00:a3:8e:db:01:a0	blizzard	13	1	0	Alert
00:a3:8e:db:01:a1	Unknown	13	1	0	Alert
00:a3:8e:db:01:a2	Unknown	13	1	0	Alert
00:a3:8e:db:01:b1	Unknown	40	2	0	Alert
00:a3:8e:db:01:b2	Unknown	40	2	0	Alert
50:2f:a8:a2:0d:40	buterfly	11	1	0	Alert
2c:97:26:61:d2:79	MEO-61D279	Unknown	0	0	Alert
8e:97:26:61:d2:7a	MEO-WiFi	6	1	0	Alert
ac:22:05:ea:21:26	NOWO-A2121	1	1	0	Alert
c4:e9:84:c1:c8:90	MEO-50E3EC	6	1	0	Alert

在此頁面中，可針對流氓進行不同的分類：

- 友好AP — 管理員標籤為友好的AP。
- 惡意AP — 通過RLDP或欺詐檢測器AP識別為惡意的AP。
- 自定義AP — 被欺詐規則歸類為自定義的AP。
- 未分類的AP — 預設情況下，惡意AP在控制器中顯示為未分類清單。
- Rogue Clients — 連線到Rogue AP的客戶端。
- Adhoc Rogues — 即席欺詐客戶端。
- 惡意AP忽略清單 — 通過PI列出。

 注意：如果WLC和自治AP由同一PI管理，則WLC會在「無管理AP忽略」清單中自動列出此自治AP。WLC中無需其他組態即可啟用此功能。

按一下特定欺詐條目以獲取該欺詐的詳細資訊。以下是有線網路中偵測到欺詐的範例：



在CLI上:

<#root>

(Cisco Controller) >

show rogue ap summary

```
Rogue Detection Security Level..... custom
Rogue Pending Time..... 180 secs
Rogue on wire Auto-Contain..... Disabled
Rogue uses our SSID Auto-Contain..... Disabled
Valid client on rogue AP Auto-Contain..... Disabled
Rogue AP timeout..... 1200
Rogue Detection Report Interval..... 10
Rogue Detection Min Rssi..... -90
Rogue Detection Transient Interval..... 0
Rogue Detection Client Num Threshold..... 0
Validate rogue AP against AAA..... Enabled
Rogue AP AAA validation interval..... 0 secs
Total Rogues(AP+Ad-hoc) supported..... 600
Total Rogues classified..... 12
```

MAC Address	Class	State	#Det Aps	#Rogue Clients	#Highest det-AP	RSSI	#RSSI	#Channel
00:a3:8e:db:01:a0	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-16	13	
00:a3:8e:db:01:a1	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-16	13	
00:a3:8e:db:01:a2	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-16	13	
00:a3:8e:db:01:b0	Malicious	Threat	2	1	00:27:e3:36:4d:a0	-27	40	
00:a3:8e:db:01:b1	Unclassified	Alert	2	0	00:27:e3:36:4d:a0	-28	40	
00:a3:8e:db:01:b2	Unclassified	Alert	2	0	00:27:e3:36:4d:a0	-28	40	
50:2f:a8:a2:0a:60	Malicious	Threat	1	2	00:27:e3:36:4d:a0	-66	1	

50:2f:a8:a2:0d:40 Unclassified Alert	1	0	00:27:e3:36:4d:a0 -65	11
9c:97:26:61:d2:79 Unclassified Alert	1	0	00:27:e3:36:4d:a0 -89	6
ac:22:05:ea:21:26 Unclassified Alert	1	0	00:27:e3:36:4d:a0 -89	(1,5)
c4:e9:84:c1:c8:90 Unclassified Alert	1	0	00:27:e3:36:4d:a0 -89	(6,2)
d4:28:d5:da:e0:d4 Unclassified Alert	1	0	00:27:e3:36:4d:a0 -85	13

(Cisco Controller) >

show rogue ap detailed 50:2f:a8:a2:0a:60

```

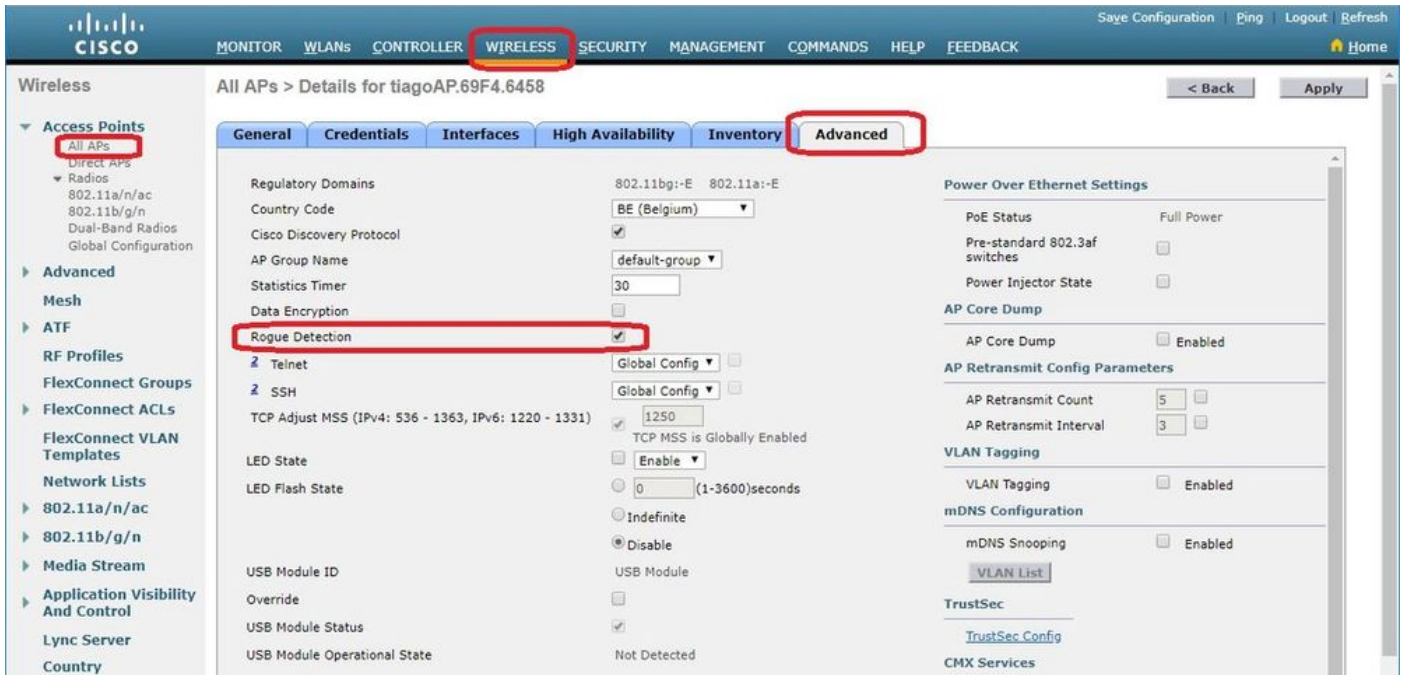
Rogue BSSID..... 50:2f:a8:a2:0a:60
Is Rogue on Wired Network..... Yes
Classification..... Malicious
Classification change by..... Auto
Manual Contained..... No
State..... Threat
State change by..... Auto
First Time Rogue was Reported..... Tue Jun  4 13:06:55 2019
Last Time Rogue was Reported..... Wed Jun  5 08:25:57 2019
Reported By
  AP 1
    MAC Address..... 00:27:e3:36:4d:a0
    Name..... tiagoAPcb.98E1.3DEC
    Radio Type..... 802.11n2.4G
    SSID..... buterfly
    Channel..... 1
    RSSI..... -64 dBm
    SNR..... 29 dB
    Security Policy..... WPA2/FT
    ShortPreamble..... Disabled
    Last reported by this AP..... Wed Jun  5 08:25:57 2019

```

疑難排解

如果未檢測到欺詐裝置

驗證AP上是否已啟用欺詐檢測。在GUI上：



在CLI中：

```
<#root>
```

```
(Cisco Controller) >show ap config general tiagoAPcb.98E1.3DEC
```

```
Cisco AP Identifier..... 13
Cisco AP Name..... tiagoAPcb.98E1.3DEC
[...]
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Local
Public Safety ..... Disabled
AP SubMode ..... Not Configured

Rogue Detection ..... Enabled

Remote AP Debug ..... Disabled
Logging trap severity level ..... informational
KPI not configured .....
Logging syslog facility ..... kern
S/W Version ..... 8.8.120.0
Boot Version ..... 1.1.2.4
[...]
Power Type/Mode..... PoE/Full Power
Number Of Slots..... 3
AP Model..... AIR-AP3802I-I-K9
AP Image..... AP3G3-K9W8-M
Cisco IOS Version..... 8.8.120.0
Reset Button..... Enabled
AP Serial Number..... FGL2114A4SU
[...]
```

使用以下命令可以在AP上啟用惡意檢測：

```
<#root>
```

```
(Cisco Controller) >
```

```
config rogue detection enable ?
```

```
all          Applies the configuration to all connected APs.
```

```
<Cisco AP>  Enter the name of the Cisco AP.
```

本地模式AP僅掃描國家/地區通道/DCA通道並取決於配置。如果欺詐裝置位於任何其他通道中，如果網路中沒有監控模式AP，控制器將無法識別該欺詐裝置。發出此命令，以驗證：

```
<#root>
```

```
(Cisco Controller) >
```

```
show advanced 802.11a monitor
```

```
Default 802.11a AP monitoring
```

```
802.11a Monitor Mode..... enable
```

```
802.11a Monitor Mode for Mesh AP Backhaul..... disable
```

```
802.11a Monitor Channels..... Country channels
```

```
802.11a RRM Neighbor Discover Type..... Transparent
```

```
802.11a RRM Neighbor RSSI Normalization..... Enabled
```

```
802.11a AP Coverage Interval..... 90 seconds
```

```
802.11a AP Load Interval..... 60 seconds
```

```
802.11a AP Monitor Measurement Interval..... 180 seconds
```

```
802.11a AP Neighbor Timeout Factor..... 20
```

```
802.11a AP Report Measurement Interval..... 180 seconds
```

- 欺詐AP不會廣播到SSID。
- 確保未將惡意AP MAC地址新增到友好無管理系統清單中或通過PI允許該地址。
- 無法到達從惡意AP發往檢測到惡作劇的AP的信標。這可以通過使用接近AP檢測器欺詐的監聽器捕獲資料包來驗證。
- 本地模式AP最多可能需要9分鐘來檢測惡意 (3個循環180x3)。
- 思科AP無法在公共安全通道(4.9 Ghz)等頻率上檢測欺詐行為。
- 思科AP無法檢測在FHSS (跳頻擴頻) 上工作的欺詐裝置。

有用的調試

```
<#root>
```

```
(Cisco Controller) >
```


*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Found Rogue AP: 00:a3:8e:db:01:a1 on slot 0

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue SSID timestmap expired. last update at 0

*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check: knownApCount=0, totalNumOfRogueE

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 New RSSI report from AP 00:27:e3:36:4d:a0 rssi

*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check: avgNumOfRogues[0]/10=4, rogueAla

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 SYNC for Channel (new/old : 40/0) or channel w

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue SSID timestmap expired. last update at 0

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 rg changed rssi prev -28, new -28

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 SYNC for Channel (new/old : 13/0) or channel w

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Updated AP report 00:27:e3:36:4d:a0 rssi -28,

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Updated AP report 00:27:e3:36:4d:a0 rssi -16,

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 RadioType: 3 lradInfo->containSlotId = 1 Receiv

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue before Rule Classification : Class unclas

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Created rogue client table for Rogue AP at 0xff

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue is Rule candidate for : Class Change by

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Added Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Applying Rogue rule to this MAC

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Looking for Rogue b0:72:bf:93:e0:d7 in known AP

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue AP b0:72:bf:93:e0:d7 is not found either

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue After Rule Classification : Class unclass

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Manual Contained Flag = 0, trustlevel = 2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Scheduled pending Time 184 and expiry time 1200

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 ssidLen = 0 min = 0 00:a3:8e:db:01:b2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Change state from 0 to 1 for rogue AP b0:72:bf:

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 This rogue does not use my ssid. Rogue ssid=

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg change state Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue AP: 00:a3:8e:db:01:b2 autocontain = 2 Mo

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue detected by AP: 00:27:e3:36:4d:a0

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Checking Impersonation source 00:a3:8e:db:01:b2

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 RadioType: 3 lradInfo->containSlotId = 2 Receiv

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 New RSSI report from AP 00:27:e3:36:4d:a0 rssi

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue is Rule candidate for : Class Change by

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Send Rogue Info Notificaiton for AP report 00:

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Applying Rogue rule to this MAC

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue SSID timestmap set to 1559723997. Detecti

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg send new rssi -59

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue After Rule Classification : Class unclass

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Updated AP report 00:27:e3:36:4d:a0 rssi -59,

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Manual Contained Flag = 0, trustlevel = 2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue detected by AP: 00:27:e3:36:4d:a0

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 ssidLen = 0 min = 0 00:a3:8e:db:01:a1

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 RadioType: 3 lradInfo->containSlotId = 2 Receiv

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 This rogue does not use my ssid. Rogue ssid=

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue before Rule Classification : Class unconf

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue AP: 00:a3:8e:db:01:a1 autocontain = 2 Mo

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue state is pending or lrad, cannot apply ro

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue doesnt qualify for rule classification :

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Checking Impersonation source 00:a3:8e:db:01:a1

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Manual Contained Flag = 0, trustlevel = 1

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Known AP 0 mfp global 0 AP Auth Global 0 mfp Im

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Checking Impersonation source b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Known AP 0 mfp global 0 AP Auth Global 0 mfp Im

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Found Rogue AP: 00:a3:8e:db:01:b0 on slot 0

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg new Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 New RSSI report from AP 00:27:e3:36:4d:a0 rssi

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue SSID timestmap set to 1559723997. Detecti

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 New RSSI report from AP 00:27:e3:36:4d:a0 rssi

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 SYNC for Channel (new/old : 40/0) or channel w

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559723997. Detecti

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 rg changed rssi prev -28, new -26

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 SYNC for Channel (new/old : 1/0) or channel wi

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Updated AP report 00:27:e3:36:4d:a0 rssi -26,

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 rg changed rssi prev -65, new -63

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue detected by AP: 00:27:e3:36:4d:a0

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Updated AP report 00:27:e3:36:4d:a0 rssi -63,

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 RadioType: 3 lradInfo->containSlotId = 1 Receiv

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue detected by AP: 00:27:e3:36:4d:a0

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 RadioType: 3 lradInfo->containSlotId = 2 Receiv

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Manual Contained Flag = 0, trustlevel = 7

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue before Rule Classification : Class malici

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 ssidLen = 8 min = 8 00:a3:8e:db:01:b0

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Manual Contained Flag = 0, trustlevel = 7

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 This rogue does not use my ssid. Rogue ssid=bl

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 ssidLen = 8 min = 8 50:2f:a8:a2:0a:60

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue AP: 00:a3:8e:db:01:b0 autocontain = 2 Mo

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 This rogue does not use my ssid. Rogue ssid=but

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue AP: 50:2f:a8:a2:0a:60 autocontain = 2 Mo

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Known AP 0 mfp global 0 AP Auth Global 0 mfp Im

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Checking Impersonation source 50:2f:a8:a2:0a:60

```

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Known AP 0 mfp global 0 AP Auth Global 0 mfp Im
*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 APF processing Rogue Client: on slot 0
*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 Rogue Client IPv6 addr: Not known
*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 APF processing Rogue Client: on slot 0
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue Client ssid: blizzard
*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 Rogue Client IPv6 addr: Not known
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue Client ssid: butterfly
*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 New AP report 00:27:e3:36:4d:a0 rssi -37, snr
*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 rgc change from -38 RSSI -37
*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 rgc change from -39 RSSI -39
*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 Updated AP report 00:27:e3:36:4d:a0 rssi -37, s
*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 Updated AP report 00:27:e3:36:4d:a0 rssi -39, s
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 APF processing Rogue Client: on slot 0

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue Client IPv6 addr: Not known

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue Client ssid: butterfly

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 New AP report 00:27:e3:36:4d:a0 rssi -62, snr
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rgc change from -61 RSSI -62
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Updated AP report 00:27:e3:36:4d:a0 rssi -62, s
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Looking for Rogue b0:72:bf:93:e0:d7 in known AP
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue AP b0:72:bf:93:e0:d7 is not found either
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Change state from 1 to 2 for rogue AP b0:72:bf:
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg change state Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 rg change state Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 Deleting Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 Freed rogue client table for Rogue AP at 0xffff0

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 rg delete for Rogue AP: b0:72:bf:93:e0:d7

```

預期的陷阱日誌

一旦檢測到欺詐行為/將其從欺詐清單中刪除：

0	2019年6月5日 週三09:01:57	欺詐客戶端：b4:c0:f5:2b:4f:90被1 AP檢測到欺詐客戶端 Bssid:a6:b1:e9:f0:e8:41，狀態：警報，上次檢測AP :00:27:e3:36:4d:a0欺詐客戶 端網關mac 00:00:00:02:02:02。
1	2019年6月5日 週三09:00:39	無管理AP:9c:97:26:61:d2:79 從基本無線電MAC中移除：00:27:e3:36:4d:a0介面 編號：0(802.11n(2.4 GHz))
2	2019年6月5日 週三08:53:39	無管理AP:7c:b7:33:c0:51:14 從基本無線電MAC中移除：00:27:e3:36:4d:a0介面 編號：0(802.11n(2.4 GHz))
3	2019年6月5日 週三08:52:27	欺詐客戶端：fc:3f:7c:5f:b1:1b被1個AP檢測到欺詐客戶端 Bssid:50:2f:a8:a2:0a:60，狀態：警報，上次檢測AP:00:27:e3:36:4d:a0欺詐客戶

	端網關mac 00:26:44:73:c5:1d。
4	2019年6月5日 週三08:52:17
	無管理AP:d4:28:d5:da:e0:d4 從基本無線電MAC中移除：00:27:e3:36:4d:a0介面 編號：0(802.11n(2.4 GHz))

行動

1. 如果懷疑網路中可能存在欺詐行為，請將通道掃描配置為所有通道。
2. 非法檢測器AP的數量和位置可能因每層樓一到每棟樓而有所不同，具體取決於有線網路的佈局。建議建築物每層至少有一個欺詐檢測器AP。由於欺詐檢測器AP需要中繼到要監控的所有第2層網路廣播域，因此位置取決於網路的邏輯佈局。

如果流氓未被分類

驗證是否正確配置了欺詐規則。

有用的調試

```
<#root>
```

```
(Cisco Controller) >
```

```
debug dot11 rogue rule enable
```

```
(Cisco Controller) >*emWeb: Jun 05 09:12:27.095:
```

```
Debugging session started on Jun 05 09:12:27.095 for WLC AIR-CT3504-K9 Version :8.8.120.0 SN :FCW2245M0
```

```
(Cisco Controller) >
```

```
*apfRogueTask_1: Jun 05 09:12:57.135: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16, maxRssiLr
```

```
*apfRogueTask_3: Jun 05 09:12:57.135: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLr
```

```
*apfRogueTask_1: Jun 05 09:12:57.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89, maxRssiLr
```

```
*apfRogueTask_1: Jun 05 09:13:27.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89, maxRssiLr
```

```
*apfRogueTask_3: Jun 05 09:13:27.135: 50:2f:a8:a2:0d:40 Rogue Rule Classify Params: rssi=-62, maxRssiLr
```

```
*apfRogueTask_3: Jun 05 09:13:27.135: 50:2f:a8:a2:0d:40
```

```
Rogue Classification:malicious, RuleName:TestRule, Rogue State:Containment Pending
```

```
*apfRogueTask_3: Jun 05 09:13:27.136: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLr
```

```
*apfRogueTask_1: Jun 05 09:13:57.136: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16, maxRssiLr
```

```
*apfRogueTask_3: Jun 05 09:13:57.136: 50:2f:a8:a2:0d:40 Rogue Classification:malicious, RuleName:TestRu
```

```
*apfRogueTask_3: Jun 05 09:13:57.136: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLr
```

行動

如果您有已知的惡意條目，請將其新增到友好清單中，或使用AAA啟用驗證，並確保身份驗證、授

權和記帳(AAA)資料庫中存在已知的客戶端條目。

RLDP找不到惡意程式

- 如果欺詐在DFS通道中，則RLDP不起作用。
- RLDP僅在惡意WLAN處於開啟狀態且DHCP可用時起作用。
- 如果本地模式AP為DFS通道中的客戶端提供服務，則它不參與RLDP進程。
- AP型號1800i、1810 OEAP、1810W、1815、1830、1850、2800和3800系列AP不支援RLDP。

有用的調試

```
<#root>
```

```
(Cisco Controller) >
```

```
debug dot11 rldp enable
```

```
!--- RLDp not available when AP used to contain only has invalid channel for the AP country code
```

```
*apfRLDP: Jun 05 12:24:41.291: 50:2f:a8:a2:0a:61 Received request to detect Rogue
```

```
*apfRLDP: Jun 05 12:24:41.291: 50:2f:a8:a2:0a:61 Entering apfFindClosestLrad
```

```
*apfRLDP: Jun 05 12:24:41.292: Rogue detected slot :0 Rogue contains SlotId :2
```

```
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61
```

```
Invalid channel 1 for the country IL for AP 00:27:e3:36:4d:a0
```

```
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61 Cannot find any AP to perform RLDp operation
```

```
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61 Exiting apfFindClosestLrad
```

```
*apfRLDP: Jun 05 12:24:41.292: Waiting for ARLDP request
```

```
!--- ROGUE detected on DFS channel
```

```
*apfRLDP: Jun 05 12:43:16.659: 50:2f:a8:a2:0d:4e Received request to detect Rogue
```

```
*apfRLDP: Jun 05 12:43:16.659: 50:2f:a8:a2:0d:4e Entering apfFindClosestLrad
```

```
*apfRLDP: Jun 05 12:43:16.660: Rogue detected slot :1 Rogue contains SlotId :1
```

```
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e
```

```
Our AP 00:27:e3:36:4d:a0 detected this rogue on a DFS Channel 100
```

```
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e Cannot find any AP to perform RLDp operation
```

```
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e Exiting apfFindClosestLrad
```

```
*apfRLDP: Jun 05 12:43:16.660: Waiting for ARLDP request
```

```
!--- RLDp is not supported on AP model 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series
```

```
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Received request to detect Rogue
```

```
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Entering apfFindClosestLrad
```

```
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a
```

```
Skipping RLDp on AP 94:d4:69:f5:f7:e0 AP Model: AIR-AP1852I-E-K9
```

```
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Cannot find any AP to perform RLDp operation
```

```
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Exiting apfFindClosestLrad
```

*apfRLDP: Jun 05 12:52:41.980: Waiting for ARLDP request

!--- Association TO ROGUE AP

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Received request to detect Rogue

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Entering apfFindClosestLrad

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Skipping RLDP on AP 94:d4:69:f5:f7:e0 AP Model: AIR-AP

*apfRLDP: Jun 05 15:02:49.602: Rogue detected slot :0 Rogue contains SlotId :0

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61

Monitor Mode AP found b4:de:31:a4:e0:30 with RSSI -61

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 found closest monitor AP b4:de:31:a4:e0:30 slot = 0, c

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Exiting apfFindClosestLrad

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Found RAD: 0xffd682b5b8, slotId = 0, Type=1

*apfRLDP: Jun 05 15:02:50.102: 50:2f:a8:a2:0a:61 AP b4:de:31:a4:e0:30 Client b4:de:31:a4:e0:31 Slot = 0

*apfRLDP: Jun 05 15:02:50.102: 50:2f:a8:a2:0a:61 WARNING!!!! mscb already exists!

*apfRLDP: Jun 05 15:02:50.102: b4:de:31:a4:e0:31 In rldpSendAddMobile:724 setting Central switched to T

*apfRLDP: Jun 05 15:02:50.302: 50:2f:a8:a2:0a:61

rldp started association, attempt 1

*apfRLDP: Jun 05 15:02:55.346: 50:2f:a8:a2:0a:61 RLDP could not finish the association in time. RLDP St

*apfRLDP: Jun 05 15:02:55.346: 50:2f:a8:a2:0a:61 rldp started association, attempt 2

*apfRLDP: Jun 05 15:03:00.390: 50:2f:a8:a2:0a:61 RLDP could not finish the association in time. RLDP St

*apfRLDP: Jun 05 15:03:00.390: 50:2f:a8:a2:0a:61 rldp started association, attempt 3

*apfOpenDtlSocket: Jun 05 15:03:00.608: apfRoguePreamble = 0 mobile b4:de:31:a4:e0:31.

*apfOpenDtlSocket: Jun 05 15:03:00.808:

50:2f:a8:a2:0a:61 RLDP state RLDP_ASSOC_DONE

(3).

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61

Successfully associated with rogue: 50:2F:A8:A2:0A:61

!--- Attempt to get ip from ROGUE

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61

Starting dhcp

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61

Initializing RLDP DHCP for rogue 50:2f:a8:a2:0a:61

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 htype: Ethernet

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 hlen: 6

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 hops: 1

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 xid: 0x3da1f13

```
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31      secs: 0
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31      flags: 0x0
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31      hw_addr: B4:DE:31:A4:E0:31
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31      client IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31      my IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31      server IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31      gateway IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31      options:
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31      DHCP message: 1 DISCOVER
*apfRLDP: Jun 05 15:03:00.870: DHCP option: 39/57.2: (2)
*apfRLDP: Jun 05 15:03:00.870:      [0000] 02 40
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31      host name: RLDP
*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 RLDP DHCP SELECTING for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.877: 50:2f:a8:a2:0a:61 Initializing RLDP DHCP for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.877: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      htype: Ethernet
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      hlen: 6
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      hops: 1
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      xid: 0x3da1f13
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      secs: 0
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      flags: 0x0
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      hw_addr: B4:DE:31:A4:E0:31
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      client IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      my IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31      server IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31      gateway IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31      options:
*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31      DHCP message: 1 DISCOVER
*apfRLDP: Jun 05 15:03:10.878: DHCP option: 39/57.2: (2)
*apfRLDP: Jun 05 15:03:10.878:      [0000] 02 40
*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31      host name: RLDP
```

```

*apfRLDP: Jun 05 15:03:10.878: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.878: 50:2f:a8:a2:0a:61 RLDP DHCP SELECTING for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 Initializing RLDP DHCP for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          htype: Ethernet
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          hlen: 6
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          hops: 1
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          xid: 0x3da1f13
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          secs: 0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          flags: 0x0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          hw_addr: B4:DE:31:A4:E0:31
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          client IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          my IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          server IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          gateway IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          options:
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          DHCP message: 1 DISCOVER
*apfRLDP: Jun 05 15:03:20.885: DHCP option: 39/57.2: (2)
*apfRLDP: Jun 05 15:03:20.885:          [0000] 02 40
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          host name: RLDP
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP 50:2f:a8:a2:0a:61

!--- RLDP DHCP fails as there is no DHCP server providing IP address

*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 RLDP DHCP FAILED state for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 DHCP failed
*apfRLDP: Jun 05 15:03:20.885: Waiting for ARLDP request

```

行動

1. 對可疑的欺詐條目手動啟動RLDP。
2. 定期安排RLDP。
3. RLDP可以部署在本地或監控模式AP上。對於大多數可擴展的部署，為了消除對客戶端服務的任何影響，應儘可能在監控模式AP上部署RLDP。但是，此建議要求以典型比率部署監控模式AP，即每5個本地模式AP部署1個監控模式AP。自適應wIPS監控模式下的AP也可以用於此任務。

惡意檢測器AP

在AP控制檯中使用此命令可看到欺詐檢測器中的欺詐條目。對於有線欺詐，標誌將移動以設定狀態。

```
<#root>
```

```
tiagoAP.6d09.eff0#
```

```
show capwap rm rogue detecto
```

```
r
```

```
LWAPP Rogue Detector Mode
```

```
Current Rogue Table:
```

```
Rogue hindex = 0: MAC 502f.a8a2.0a61,
```

```
flag = 0
```

```
, unusedCount = 1
```

```
Rogue hindex = 0: MAC 502f.a8a2.0a60,
```

```
flag = 0
```

```
, unusedCount = 1
```

```
Rogue hindex = 7: MAC 502f.a8a2.0d41,
```

```
flag = 0
```

```
, unusedCount = 1
```

```
Rogue hindex = 7: MAC 502f.a8a2.0d40,
```

```
flag = 0
```

```
, unusedCount = 1
```

```
!--- once rogue is detected on wire, the flag is set to 1
```

AP控制檯中的有用調試命令

```
<#root>
```

```
Rogue_Detector#
```

```
debug capwap rm rogue detector
```

```
*Jun 05 08:37:59.747: ROGUE_DET: Received a rogue table update of length 170
```

```
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac4
```

```
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac5
```

```
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1aca
```

```
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acb
```

```
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acc
```

```
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acd
```

```
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acf
```

```
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0024.1431.e9ef
```

```
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0024.148a.ca2b
```

```
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2d
```

```
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2f
```



```
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3570
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3574
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357b
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357c
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357d
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357f
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3dcd
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff0
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff2
*Jun 05 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4aec
*Jun 05 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4b77
*Jun 05 08:37:59.774: ROGUE_DET: Flushing rogue entry 0040.96b9.4794
*Jun 05 08:37:59.774: ROGUE_DET: Flushing rogue entry 0022.0c97.af80
*Jun 05 08:37:59.775: ROGUE_DET: Flushing rogue entry 0024.9789.5710
*Jun 05 08:38:19.325: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 05 08:38:19.325: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
*Jun 05 08:39:19.323: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 05 08:39:19.324: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
```

惡意遏制

預期調試

<#root>

```
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Updated AP report b4:de:31:a4:e0:30 rssi -33, s
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Looking for Rogue 00:a3:8e:db:01:b0 in known AP
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue AP 00:a3:8e:db:01:b0 is not found either
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue in same state as before : 6 ContainmentLev

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue detected by AP: b4:de:31:a4:e0:30
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RadioType: 2 lradInfo->containSlotId = 1 Receiv

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue before Rule Classification :

Class malicious, Change by Auto State Contained Change by Auto

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue doesnt qualify for rule classification :
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Manual Contained Flag = 0, trustlevel = 6
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0

Rogue AP: 00:a3:8e:db:01:b0 autocontain = 1 Mode = 6

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 apfRogueMode : 6 apfRogueContainmentLevel : 4 1

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Trying Containment on 1 band for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Skipping xor radio for 1 band and cont slotid 1
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Found 0 channels to try containment for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Trying Containment on 2 band for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue detected on detected slot 0 contains slot
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Found 1 channels to try containment for rogue
```

```
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC 00:27:e3:36:4d:a0 RSSI = -28 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC 00:27:e3:36:4d:a0 RSSI = -31 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC b4:de:31:a4:e0:30 RSSI = -33 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC 00:27:e3:36:4d:a0 RSSI = -28 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC 00:27:e3:36:4d:a0 RSSI = -31 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC b4:de:31:a4:e0:30 RSSI = -33 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP b4:de:31:a4:e0:30
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0
```

Contains rogue with 3 container AP(s).Requested containment level : 4

```
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Checking Impersonation source 00:a3:8e:db:01:b0
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Known AP 0 mfp global 0 AP Auth Global 0 mfp Im
```

建議

1. 本地/Flex-Connect模式AP每次可包含3台裝置，而監控模式AP每次可包含6台裝置。因此，請確保AP未包含允許的最大裝置數。在此案例中，使用者端處於包含掛起狀態。
2. 驗證自動包含規則。

結論

思科集中式控制器解決方案中的欺詐檢測和遏制是業內最有效、干擾最小的方法。為網路管理員提供的靈活性使網路管理員能夠適應任何網路需求，從而更加定製。

相關資訊

- [思科無線控制器組態設定指南8.8版 — 欺詐管理](#)
- [思科無線LAN控制器\(WLC\)組態最佳實踐](#)
- [WLC 3504 8.5版部署指南](#)
- [Cisco 5520無線LAN控制器部署指南](#)
- [思科無線控制器和輕量接入點版本說明，思科無線版本8.8.120.0](#)

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）。