

# Unified Wireless Networkにおける不正検出と緩和の解決

## 内容

---

### [はじめに](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [不正の概要](#)

#### [不正検出](#)

##### [オフチャネルスキャン](#)

##### [モニタモードのスキャン](#)

##### [ローカルモードとモニタモードの比較](#)

##### [不正の特定](#)

##### [不正レコード](#)

##### [不正の詳細](#)

##### [不正イベントをエクスポートするには](#)

##### [不正レコードのタイムアウト](#)

##### [Rogue Detector AP](#)

##### [スケーラビリティに関する考慮事項](#)

#### [RLDP](#)

##### [RLDPの注意事項](#)

##### [スイッチポートトレース](#)

#### [不正分類](#)

##### [不正分類ルール](#)

#### [HAファクト](#)

#### [Flex-Connectの概要](#)

### [不正緩和](#)

#### [不正抑止](#)

##### [不正抑止の詳細](#)

##### [自動抑止](#)

##### [不正抑止の注意事項](#)

#### [スイッチポートのシャットダウン](#)

### [設定](#)

#### [不正検出の設定](#)

##### [不正検出のためのチャネルスキャンの設定](#)

#### [不正分類の設定](#)

#### [不正緩和の設定](#)

##### [手動抑止の設定](#)

##### [自動抑止](#)

### [Prime Infrastructureを使用](#)

### [確認](#)

### [トラブルシューティング](#)

#### [不正が検出されない場合](#)

---

[有益なデバッグ](#)

[一般的なトラップ ログ](#)

[推奨事項](#)

[不正が分類されない場合](#)

[有益なデバッグ](#)

[推奨事項](#)

[RLDPが不正を検出しない](#)

[有益なデバッグ](#)

[推奨事項](#)

[Rogue Detector AP](#)

[AP コンソール内の便利なデバッグ コマンド](#)

[不正抑止](#)

[予想されるデバッグ](#)

[推奨事項](#)

[結論](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、Ciscoワイヤレスネットワークでの不正の検出と緩和について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco ワイヤレス LAN コントローラ。
- Cisco Prime Infrastructure.

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- バージョン8.8.120.0が稼働するCisco Unified Wireless Lan Controller ( 5520、8540、および3504シリーズ )
- Wave 2 AP 1832、1852、2802、および3802シリーズ。
- Wave 1 AP 3700、2700、1700シリーズ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 不正の概要

ワイヤレス ネットワークを導入すると有線ネットワークが拡張され、作業者の生産性が向上し、情報へのアクセスが拡大します。ただし、認証されていないワイヤレス ネットワークを追加すると、セキュリティの懸念が高まります。有線ネットワークではポートのセキュリティにあまり注意が向けられていませんが、ワイヤレス ネットワークもその延長上で考えられがちです。そのため、セキュリティでしっかりと保護されているワイヤレスまたは有線のインフラストラクチャに、従業員が各自のアクセス ポイント ( シスコまたはシスコ以外 ) を持ち込むと、せっかくセキュリティで保護されているネットワークに対して不正なユーザ アクセスが許可されてしまうため、セキュアなネットワークが簡単に危険にさらされてしまいます。

ネットワーク管理者は不正検出を行うことで、このセキュリティの問題を監視して、解消することができます。Cisco Unified Network アーキテクチャには、不正の特定と抑止を高度に実行するソリューションを提供する不正検出の方法が用意されています。高価で有効性を検証しにくい追加のネットワークとツールは必要ありません。

スペクトルを共有し、管理者によって管理されていないデバイスは不正と見なされます。不正が危険と見なされるのは、次のような状況です。

- ネットワーク ( ハニーポット ) と同じ Service Set Identifier (SSID) を使用するようにセットアップする場合
- 有線ネットワークで検出されたとき
- アドホック不正
- 部外者が設定した場合、ほとんどの場合、悪意のある意図で

ベストプラクティスは、不正検出を使用して、たとえば企業環境などのセキュリティリスクを最小限に抑えることです。

ただし、Office Extend Access Point (OEAP) の導入、市全域、屋外など、不正検出が不要なシナリオもあります。

屋外のメッシュ AP を使用して不正を検出しても、分析にリソースを使用する一方で、ほとんど価値がありません。

最後に、不正の自動封じ込めを評価する ( または完全に回避する ) ことが重要です。これは、自動運用のままにしておくと、法的な問題や法的責任が発生する可能性があるためです。

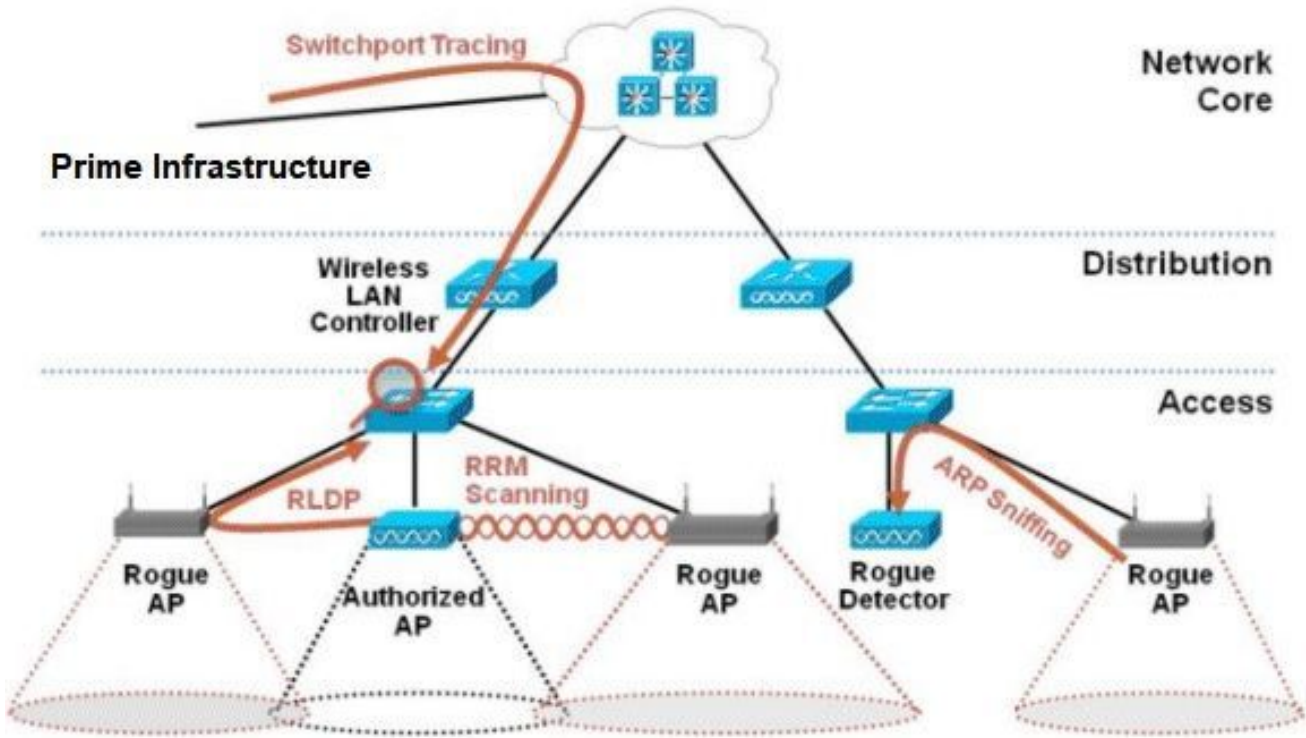
Cisco Unified Wireless Network ( UWN ) ソリューションの不正デバイス管理には、3 つの主な段階があります。

- 検出 : Radio Resource Management (RRM) スキャンは、不正デバイスの存在を検出するために使用されます。
- 分類 : Rogue Location Discovery Protocol (RLDP)、Rogue Detector ( Wave 1 AP のみ )、およびスイッチポートトレースを使用して、不正デバイスが有線ネットワークに接続されているかどうかを識別します。不正分類ルールは、不正をその特性に基づいて特定のカテゴリに

フィルタリングする際にも役立ちます。

- 緩和：スイッチポートの閉鎖、不正の場所、および不正の抑止を使用して、不正の物理的な場所を突き止め、不正デバイスの脅威を無効にします。

## Cisco Rogue Management Diagram Multiple Methods



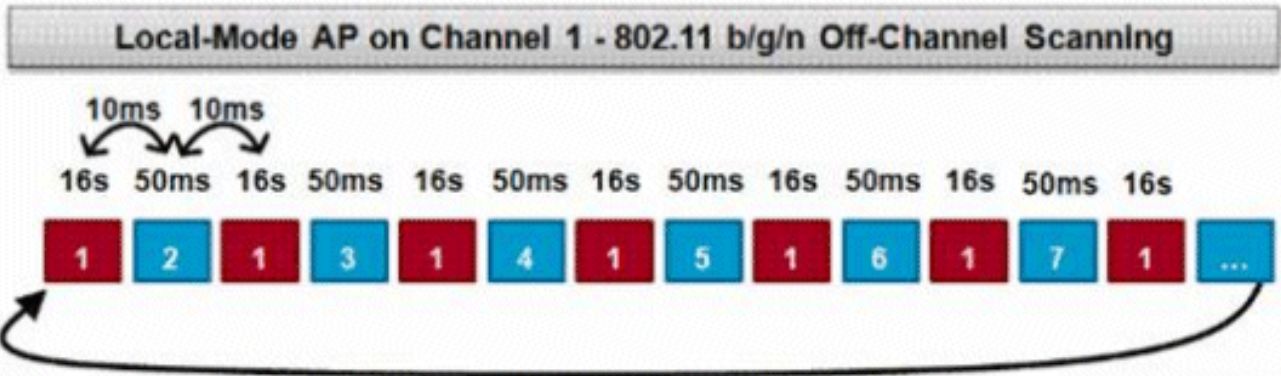
### 不正検出

不正とは、本質的に、スペクトルを共有するが制御できないデバイスのことです。これには、不正なアクセスポイント、ワイヤレスルータ、不正なクライアント、および不正なアドホックネットワークが含まれます。Cisco UWNは、オフチャネルスキャンや専用モニタモード機能など、Wi-Fiベースの不正デバイスを検出するためのさまざまな方法を使用します。また、Cisco Spectrum Expert を使用して、Bluetooth ブリッジなどの 802.11 プロトコルに基づかない不正デバイスを特定できます。

### オフチャネルスキャン

この操作は、ローカルおよびFlex-Connect ( 接続モード ) モードのAPによって実行され、同じ無線を使用したクライアントサービスとチャンネルスキャンを可能にするタイムスライシング技術を利用します。オフチャネルへの移行が16秒ごとに50ミリ秒の期間にわたって行われると、APはデフォルトで、クライアントにサービスを提供しないためにその時間のごく一部しか費やしません。また、10ミリ秒のチャンネル変更間隔が発生していることにも注意してください。デフォルトの180秒のスキャン間隔では、それぞれの2.4Ghz FCC チャンネル ( 1-11 ) が少なくとも一度はスキャンされます。ETSIなどのその他の規制区域では、APはオフチャネル状態になり、その割合がわ

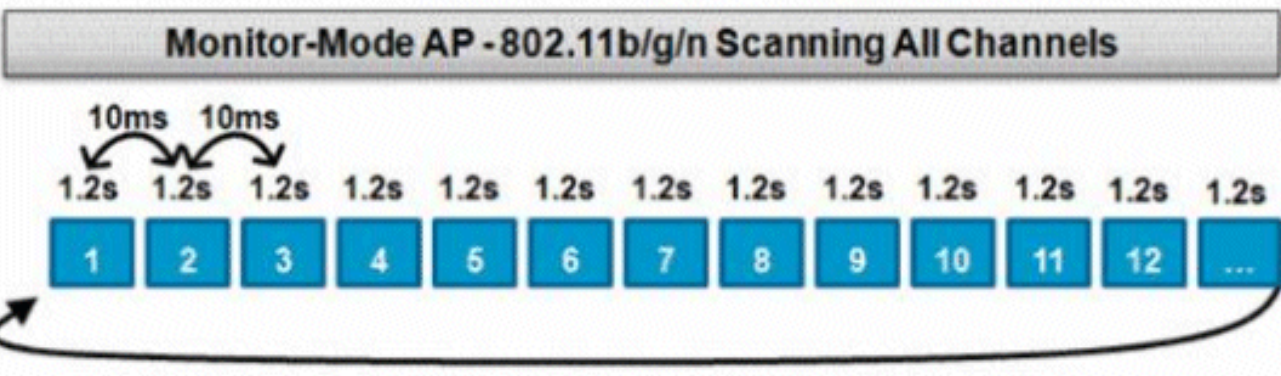
ずかに高くなります。RRM 設定では、チャンネルのリストとスキャン間隔の両方を調整できます。これにより、パフォーマンスへの影響が最大1.5 %に制限され、音声などの優先度の高いQoSフレームを配信する必要があるときにスキャンを一時停止するインテリジェンスがアルゴリズムに組み込まれます。



この図は、2.4GHz周波数帯のローカルモードAPのオフチャンネルスキャンアルゴリズムを示しています。APに5GHz無線がある場合は、同様の操作が並行して実行されます。赤い四角はAPのホームチャンネルで費やされた時間を表し、青い四角はスキャン目的で隣接チャンネルで費やされた時間を表します。

#### モニタモードのスキャン

この操作は、モニタモードAPと適応型wIPSモニタモードAPで実行されます。これらのモニタモードAPは、無線時間の100 %を利用して、それぞれの周波数帯域のすべてのチャンネルをスキャンします。これにより、検出の速度が大幅に向上し、より多くの時間をそれぞれのチャンネルに費やすことができます。モニタモードAPは、各チャンネルで発生するアクティビティをより包括的に把握できるため、不正クライアントの検出にも優れています。



この図は、2.4 GHzの周波数帯域におけるモニタモードAPのオフチャンネルスキャンアルゴリズムを示しています。APに5GHz無線がある場合は、同様の操作が並行して実行されます。

#### ローカルモードとモニタモードの比較

ローカルモードAPは、WLANクライアントのサービスと脅威のチャンネルスキャンの間でサイクルを分割します。その結果、ローカルモードAPがすべてのチャンネルを巡回するのに時間がかかり、

クライアントの動作が中断されないように、特定のチャンネルの収集データに費やす時間が短縮されます。そのため、不正と攻撃の検出時間がより長くなり（3分～60分）、検出できる地上波攻撃がモニタモードAPよりも狭い範囲に限られます。

さらに、不正クライアントなどのバーストトラフィックの検出は、トラフィックの送受信と同時にAPをトラフィックのチャンネル上に配置する必要があるため、はるかに確定的ではありません。これにより、確率に課題が生じます。モニタモードAPは、不正や地上波攻撃を検出するために、チャンネルのスキャンにすべてのサイクルを費やします。モニタモードAPはAdaptive wIPS、場所（状況認識）サービス、およびその他のモニタモードサービスで同時に使用できます。

モニタモードAPを導入する利点は、検出にかかる時間が短いことです。モニタモードAPがAdaptive wIPSとともに追加で設定されている場合、より幅広い地上波の脅威と攻撃を検出できます。

ローカルモードAP	モニタモードAP
クライアントにタイムスライシングのオフチャンネルスキャンを提供	専用スキャン
各チャンネルで50ミリ秒間リスンする	各チャンネルで1.2sをリスン
スキャンを設定可能： <ul style="list-style-type: none"> <li>すべてのチャンネル</li> <li>国チャンネル（デフォルト）</li> <li>DCAチャンネル</li> </ul>	すべてのチャンネルをスキャン

### 不正の特定

不正デバイスからのプローブ応答またはビーコンがローカルモード、フレックスコネクモード、またはモニタモードのAPで受信された場合、この情報はCAPWAP経由でプロセスのワイヤレスLANコントローラ(WLC)に通信されます。誤検知を防ぐために、さまざまな方法を使用して、他のシスコベースの管理対象APが不正デバイスとして識別されないようにします。これらの方法には、モビリティグループのアップデート、RFネイバーパケット、Prime Infrastructure(PI)を介した許可リスト対応APなどがあります。

### 不正レコード

不正デバイスのコントローラのデータベースには、検出された不正の現在のセットのみが含まれていますが、PIには、見えなくなった不正のイベント履歴とログも含まれています。

### 不正の詳細

CAPWAP AP は、不正クライアント、ノイズ、チャンネル干渉を監視するために、50 ミリ秒間オフチャンネルになります。検出された不正クライアントや不正 AP はコントローラに送信され、次の情報が収集されます。

- 不正 AP の MAC アドレス
- 不正が検出された AP の名前
- 不正な接続クライアントの MAC アドレス
- セキュリティ ポリシー
- プリアンプル
- 信号対雑音比 ( SNR )
- Receiver Signal Strength Indicator ( RSSI )
- 不正検出のチャンネル
- 不正が検出された無線
- 不正 SSID ( 不正 SSID がブロードキャストされている場合 )
- 不正 IP アドレス
- 不正がレポートされた最初と最後の時間
- チャンネル幅

不正イベントをエクスポートするには

不正イベントをサードパーティのネットワーク管理システム ( NMS ) にエクスポートしてアーカイブするために、WLC には追加の SNMP トラップ レシーバを追加できます。コントローラによって不正が検出またはクリアされると、この情報を含むトラップがすべての SNMP トラップ レシーバに送信されます。SNMP によるイベントのエクスポートに関する注意点は、複数のコントローラが同じ不正を検出した場合、関連付けは PI でのみ行われるため、NMS によって重複するイベントが表示されることです。

不正レコードのタイムアウト

不正 AP が WLC レコードに追加されると、その不正 AP は認識されなくなるまで WLC に残ります。ユーザが設定可能なタイムアウト ( デフォルトは 1200 秒 ) を過ぎると、\_unclassified\_category 内の不正はエージングアウトします。

\_Contained\_and\_Friendly\_などの他の状態にある不正は保持され、それらが再び現れると適切な分類が適用されます。

不正レコードのデータベースの最大サイズは、コントローラ プラットフォームによって異なります。

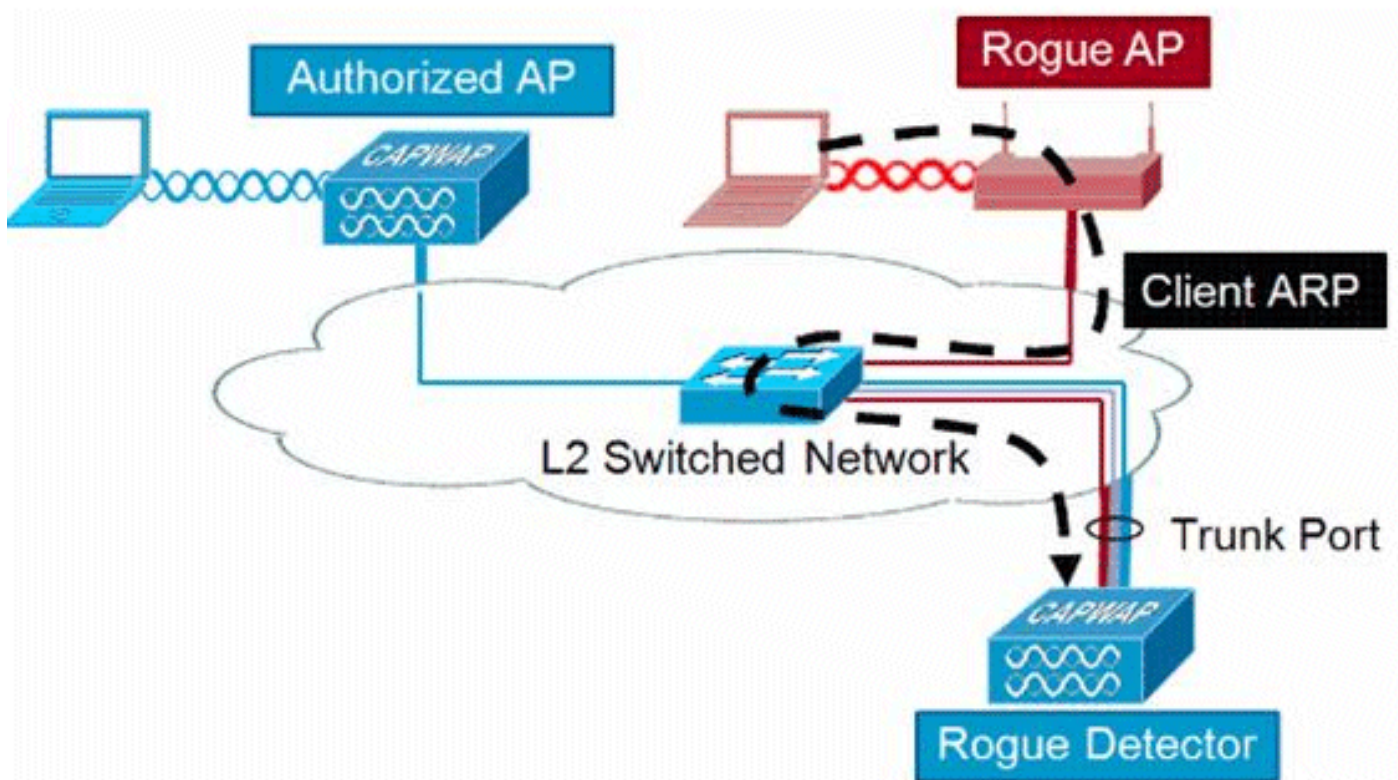



- 3504 – 最大600の不正APと1500の不正クライアントの検出と抑制
- 5520 : 最大24000の不正APと32000の不正クライアントの検出と抑制
- 8540 : 最大24000台の不正APと32000台の不正クライアントの検出と抑制

## Rogue Detector AP

Rogue Detector AP は地上波で受信された不正情報を有線ネットワークから取得した ARP 情報と関連付けることを目的とします。MAC アドレスが不正 AP または不正クライアントとして地上波で受信され、有線ネットワークでも受信されると、有線ネットワーク上に不正が存在することが決定します。不正が有線ネットワーク上にあることが検出されると、その不正APのアラーム重大度は `_critical_` に上がります。Rogue Detector APは、NATを使用するデバイスの背後にある不正クライアントを特定できません。

これは、不正 AP に何らかの認証 ( WEP または WPA ) が設定されている場合に使用される手法です。認証の形式が不正APで設定されている場合、Lightweight APは不正APで設定されている認証方式とクレデンシャルを知らないため、関連付けできません。



 注:Rogue Detectorとして設定できるのはWave 1 APだけです。

## スケーラビリティに関する考慮事項

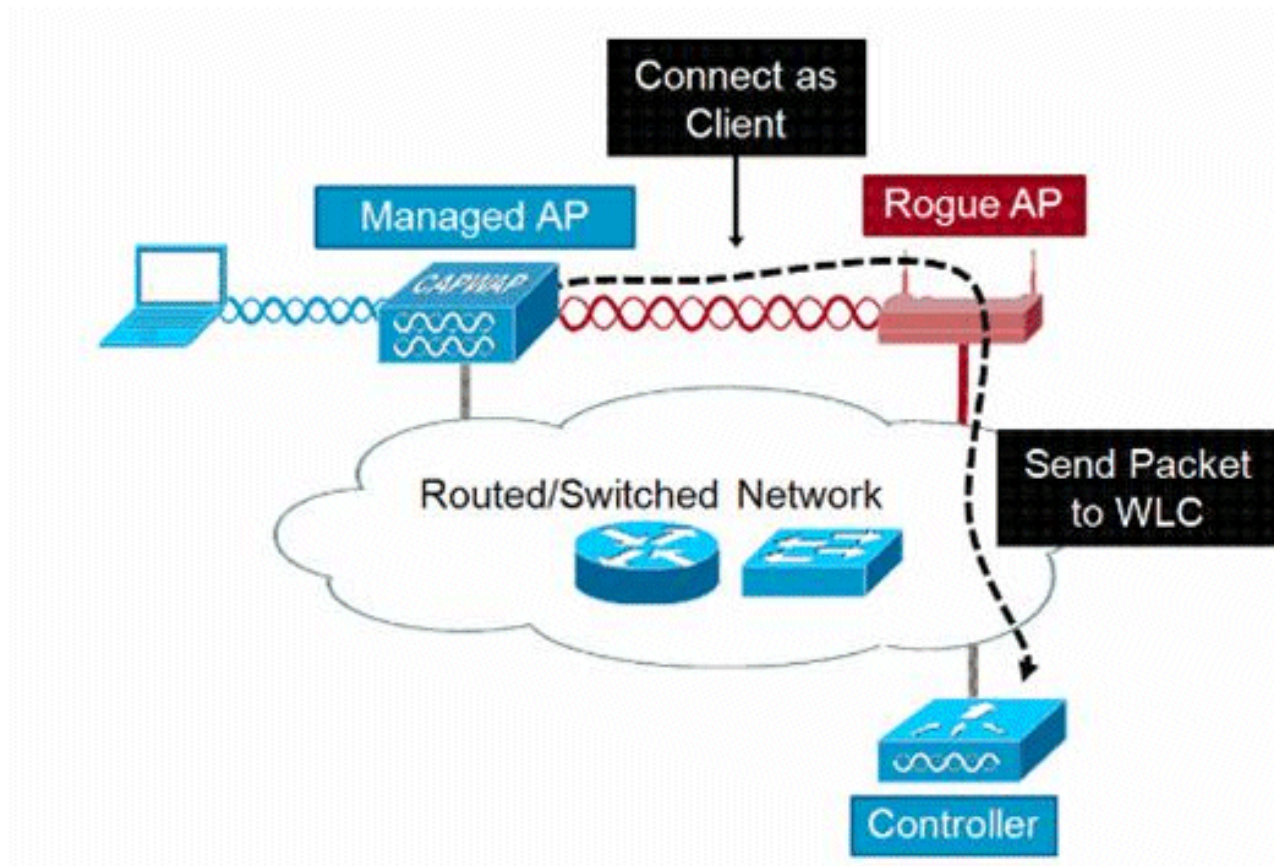
Rogue Detector AP は最大 500 個の不正と 500 個の不正クライアントを検出できます。Rogue Detectorがトランク上に配置されている不正デバイスの数が多すぎると、これらの制限を超えるため問題が発生します。これが発生しないようにするには、Rogue Detector APをネットワーク



のディストリビューションレイヤまたはアクセスレイヤに配置します。

## RLDP


RLDP の目的は、特定の不正 AP が有線インフラストラクチャに接続されているかどうかを特定することです。この機能は基本的に、最も近いAPを使用して、ワイヤレスクライアントとして不正デバイスに接続します。クライアントとしての接続後、APが有線ネットワークに接続されているかどうかを評価するために、WLCの宛先アドレスを含むパケットが送信されます。不正が有線ネットワーク上にあることが検出された場合、その不正 AP のアラーム重大度は重大に引き上げられます。



次に、RLDP のアルゴリズムを示します。

1. 信号強度値を使用して、不正に最も近いUnified APを特定します。
2. 次に、APはWLANクライアントとして不正に接続し、タイムアウトする前に3つのアソシエーションを試行します。
3. アソシエーションが成功すると、APはDHCPを使用してIPアドレスを取得します。
4. IPアドレスが取得されると、AP (WLANクライアントとして機能)は各コントローラIPアドレスにUDPパケットを送信します。
5. コントローラがクライアントからRLDPパケットを1つでも受信すると、その不正は接続済みとマーキングされ、重大度は重大になります。

---

 注：コントローラネットワークと不正デバイスがあるネットワークの間にフィルタルールが設定されている場合、RLDPパケットはコントローラに到達できません。

---

## RLDP の注意事項

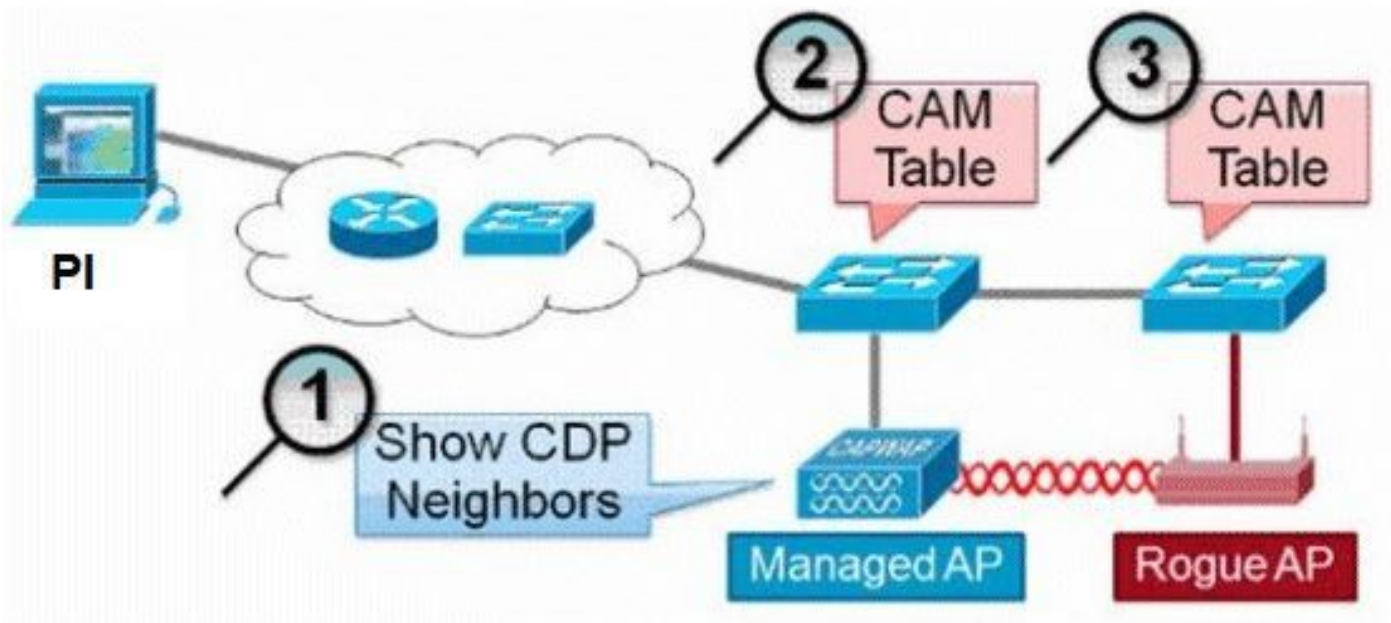
- RLDPは、認証と暗号化が無効になっているSSIDをブロードキャストするオープンな不正APでのみ動作します。
- RLDPでは、クライアントとして機能する管理対象APが不正ネットワーク上のDHCP経由でIPアドレスを取得できる必要があります
- 手動 RLDP を使用して、不正に対して RLDP トレースを何度も試行できます。
- RLDPプロセスでは、APはクライアントにサービスを提供できません。これは、ローカルモードAPのパフォーマンスと接続に悪影響を及ぼします。
- RLDPは、5GHz DFSチャンネルで動作する不正APへの接続を試行しません。

## スイッチポートトレース

スイッチポートトレースは、不正なAPを軽減する手法です。スイッチポートトレースはPIで開始されますが、CDPとSNMPの両方の情報を使用して、ネットワーク内の特定のポートまで不正を追跡します。

スイッチポートトレースを実行するには、ネットワーク内のすべてのスイッチをSNMPクレデンシャルでPIに追加する必要があります。読み取り専用クレデンシャルは不正が存在するポートを特定するために機能しますが、読み取り/書き込みクレデンシャルを使用すると、PIはポートをシャットダウンすることもできるため、脅威を封じ込めることができます。

現時点では、この機能はCDPが有効なCisco IOS®が稼働するCiscoスイッチでのみ動作します。また、管理対象APでもCDPを有効にする必要があります。



スイッチポートトレースのアルゴリズムを次に示します。

1. PIは最も近いAPを見つけ、無線で不正なAPを検出し、そのCDPネイバーを取得します。
2. 次にPIはSNMPを使用してネイバースイッチ内のCAMテーブルを調べ、正の一致を探して不正な場所を特定します。
3. 正一致は、完全に一致する不正 MAC アドレス、不正 MAC アドレスの +1/-1、任意の不正クライアント MAC アドレス、または MAC アドレスに継承されたベンダー情報に基づく OUI の一致に基づきます。
4. 最も近いスイッチで正の一致が見つからない場合、PIは最大2ホップ離れたネイバースイッチで検索を続行します ( デフォルト )。

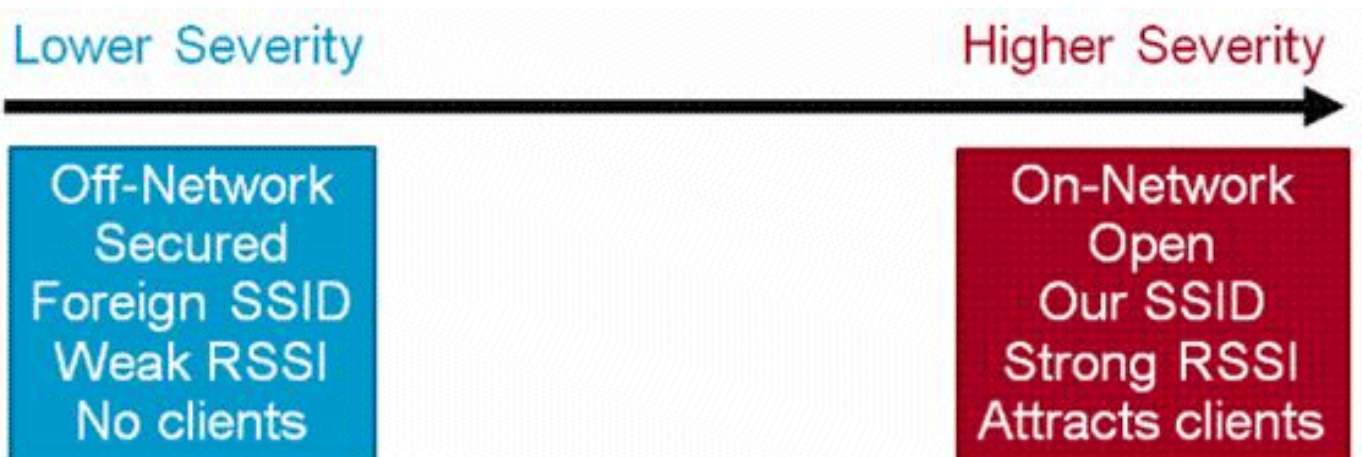
# Wired-Side Tracing Techniques

## Comparison

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

## 不正分類

デフォルトでは、Cisco UWN で検出されたすべての不正は未分類と見なされます。次の図に示すように、不正は、RSSI、SSID、セキュリティタイプ、オン/オフネットワーク、クライアント数など、さまざまな基準で分類できます。





## 不正分類ルール

不正分類ルールを使用すると、不正を悪意のある不正または友好的な不正としてマークする一連の条件を定義できます。これらのルールはPIまたはWLCで設定されますが、新しい不正が検出されるたびにコントローラで実行されます。

WLCでの不正ルールの詳細については、『[ワイヤレスLANコントローラ\(WLC\)およびPrime Infrastructure\(PI\)でのルールベースの不正分類](#)』を参照してください。

## HAファクト

任意の不正デバイスをcontained状態（任意のクラス）またはfriendly状態に手動で移動すると、この情報はスタンバイ側のCisco WLCフラッシュメモリに保存されますが、データベースは更新されません。HAスイッチオーバーが発生すると、以前スタンバイ状態のCisco WLCフラッシュメモリから不正リストがロードされます。

ハイアベイラビリティのシナリオでは、不正検出のセキュリティレベルが高または重大に設定されている場合、スタンバイコントローラの不正タイマーは不正検出が安定するまでの時間（300秒）の後にのみ開始されます。したがって、スタンバイコントローラのアクティブな設定は、300秒後にのみ反映されます。

## Flex-Connectの概要

接続モードの（不正検出が有効な）FlexConnect APは、コントローラから抑止リストを取得します。コントローラでauto-contain SSIDとauto contain adhocが設定されている場合、これらの設定は接続モードのすべてのFlexConnect APに設定され、APはその設定をメモリに保存します。

FlexConnect APがスタンドアロンモードに移行すると、次のタスクが実行されます。

- コントローラによって設定された抑止は続行されます。
- FlexConnect APが、インフラストラクチャSSID（FlexConnect APが接続されているコントローラで設定されたSSID）と同じSSIDを持つ不正APを検出した場合、スタンドアロンモードに移行する前にコントローラでSSIDの自動包含が有効になっていれば、抑止が開始されます。
- FlexConnect APがアドホックな不正を検出した場合、接続モードのときにコントローラからauto-containing adhocが有効になっていれば、抑止が開始されます。

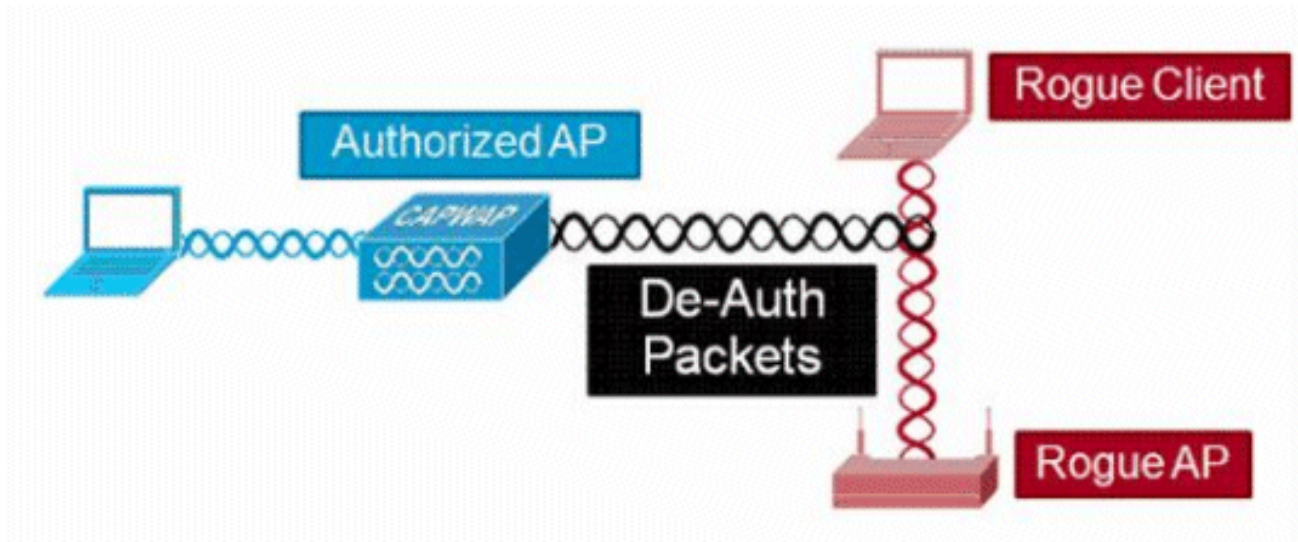
スタンドアロンFlexConnect APが接続モードに戻ると、次のタスクが実行されます。

- すべてのコンテインメントがクリアされます。
- コントローラから開始された抑止が引き継ぎます。

## 不正緩和

## 不正抑止

抑止とは、地上波パケットを使用して、不正デバイスが物理的に削除されるまで、不正デバイスのサービスを一時的に中断する方法です。抑止は、不正APのスプーフィングされた送信元アドレスを持つ認証解除パケットのスプーフィングと連携して動作するため、関連付けられているすべてのクライアントが起動されます。



## 不正抑止の詳細

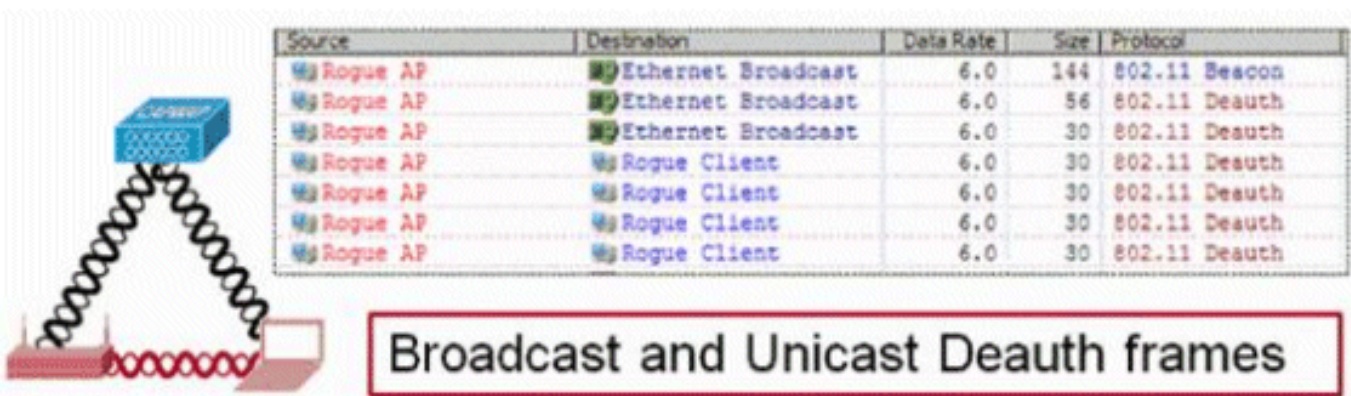
クライアントがない不正APで開始された抑止は、ブロードキャストアドレスに送信された認証解除フレームのみを使用します。

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**

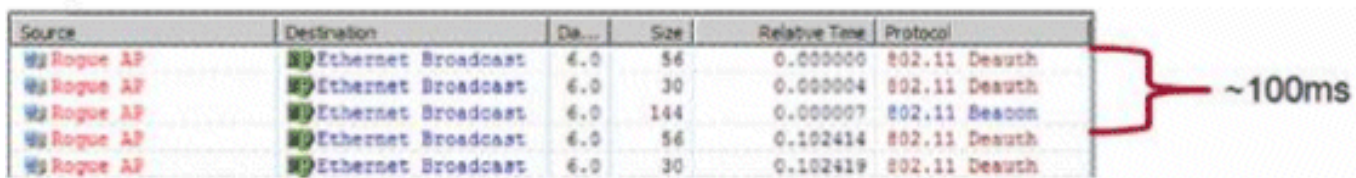
クライアントを含む不正APで開始された抑止は、ブロードキャストアドレスとクライアントアドレスに送信された認証解除フレームを使用します。





抑止パケットは、管理対象 AP の出力レベルと、イネーブルになっている最小のデータ レートで送信されます。

抑止は 100 ミリ秒ごとに少なくとも 2 つのパケット送信します。



**注：** モニタモード AP 以外の AP で実行される抑止は、モニタモード AP で使用される 100 ミリ秒間隔ではなく、500 ミリ秒間隔で送信されます。

- 個別の不正デバイスは、1 つから 4 つの管理対象 AP によって抑止されます。管理対象 AP は連係して脅威を一時的に緩和します。
- 抑止は、ローカルモード、モニタモード、およびフレックス接続 ( 接続 ) モードの AP を使用して実行できます。Flex-Connect AP のローカルモードでは、無線ごとに最大 3 つの不正デバイスを抑止できます。モニタモード AP の場合、無線あたり最大 6 つの不正デバイスを抑止できます。

### 自動抑止

PI または WLC GUI を使用して不正デバイスの抑止を手動で開始する機能に加えて、特定のシナリオで抑止を自動的に起動する機能もあります。この設定は、PI またはコントローラインターフェイスの Rogue ポリシーの General in にあります。これらの各機能はデフォルトで無効になっており、最も被害の大きい脅威を無効にするためにのみ有効にされます。

- Rogue on Wire : 不正デバイスが有線ネットワークに接続されていることが特定されると、自動的に抑止状態になります。
- SSID の使用 : 不正デバイスがコントローラで設定されているものと同じ SSID を使用する場合、そのデバイスは自動的に抑止されます。この機能は、障害を引き起こす前にハニーポット攻撃に対応するための機能です。

- Valid client on Rogue AP:Radius/AAAサーバにリストされているクライアントが不正デバイスに関連付けられていることが検出されると、そのクライアントに対してのみ抑止が起動され、管理対象ではないAPへの関連付けが阻止されます。
- AdHoc Rogue AP : アドホックネットワークが検出されると、自動的に抑止されます。

## 不正抑止の注意事項

- 抑止では管理対象AP無線時間の一部を使用して認証解除フレームが送信されるため、データクライアントと音声クライアントの両方のパフォーマンスが最大20%の悪影響を受けます。データクライアントの場合、この影響によりスループットが低下します。音声クライアントの場合、抑止によって、会話が中断されたり、音声品質が低下したりすることがあります。
- ネイバーネットワークに対して封じ込めを行うと、法的な影響が生じる可能性があります。抑止を起動する前に、不正デバイスがネットワーク内にあり、セキュリティ リスクを引き起こすことを確認してください。

## スイッチポートのシャットダウン

SPTを使用してスイッチポートをトレースすると、PIでそのポートを無効にするオプションがあります。管理者はこの操作を手動で行う必要があります。不正がネットワークから物理的に削除されている場合に、PIを介してスイッチポートを有効にするオプションがあります。

# 設定

## 不正検出の設定

デフォルトでは、コントローラでの不正検出はイネーブルです。

さまざまなオプションを設定するには、Security > Wireless Protection Policies > Rogue Policies > Generalの順に移動します。例：

ステップ 1：不正 AP のタイムアウトを変更します。

ステップ 2：アドホック不正ネットワークの検出をイネーブルにします。

CLI から、

```
<#root>
```

```
(Cisco Controller) >
```

```
config rogue ap timeout ?
```

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

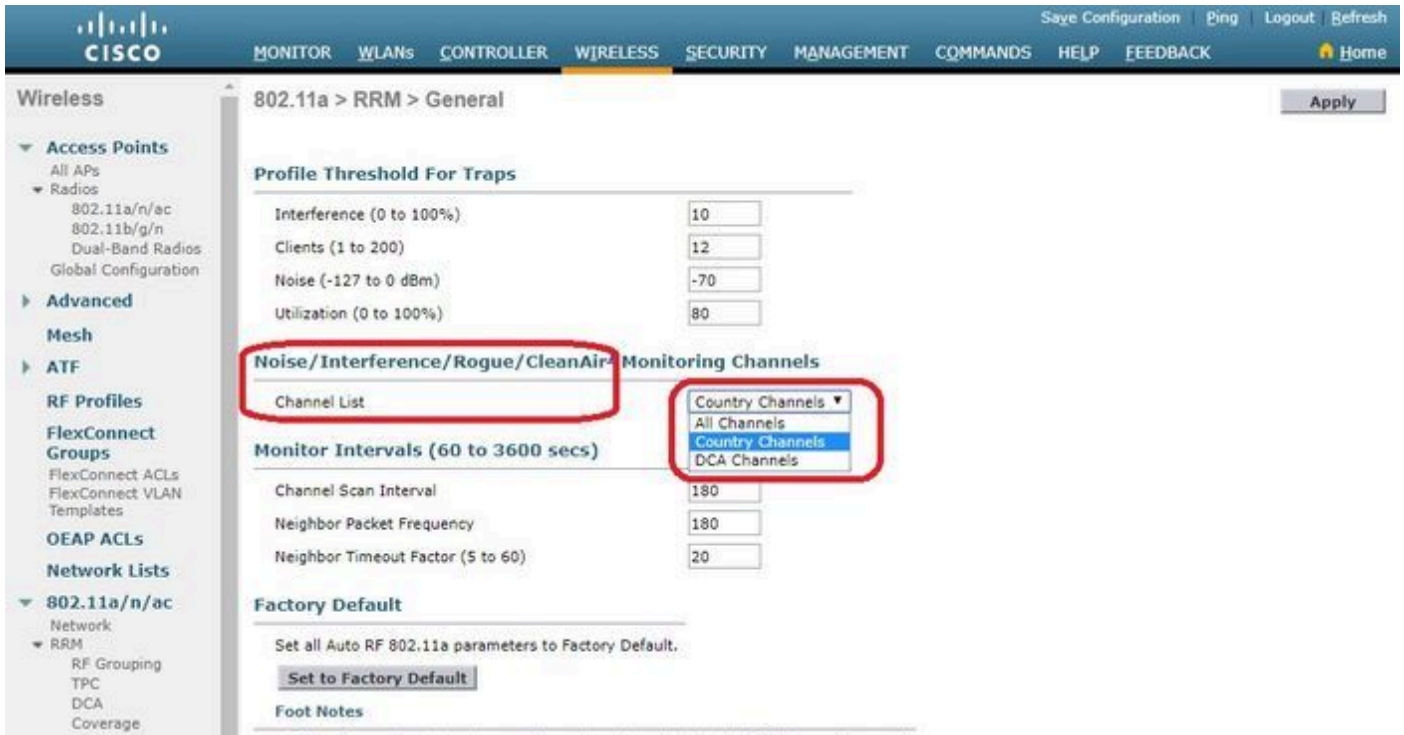
```
(Cisco Controller) >
```

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

## 不正検出のためのチャンネルスキャンの設定

ローカル/Flex-Connect/モニタモードのAPの場合、不正をスキャンするチャンネルをユーザが選択できるオプションがRRM設定の下にあります。設定に応じて、APはすべてのチャンネル/コントリブーチャンネル/DCAチャンネルで不正をスキャンします。

これをGUIから設定するには、図に示すように、Wireless > 802.11a/802.11b > RRM > Generalの順に移動します。



CLI から、

```
<#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
```

## 不正分類の設定

### 不正 AP の手動分類

不正APをFriendly、Malicious、またはUnclassifiedとして分類するには、Monitor > Rogue > Unclassified APsの順に移動し、特定の不正APの名前をクリックします。図に示すように、ドロップダウンリストからオプションを選択します。

The screenshot shows the Cisco Meraki Monitor interface. The top navigation bar includes links for Save Configuration, Ping, Logout, Refresh, and Home. The main menu on the left is expanded to 'Rogues', with sub-items for Friendly APs, Malicious APs, Custom APs, Unclassified APs, Rogue Clients, and Adhoc Rogues. The 'Rogue AP Detail' page shows the following information:

- 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: Unclassified (dropdown menu is open showing options: Unclassified, Friendly, Malicious, Unclassified, Custom)
- State: No
- Manually Contained: No
- Update Status: -- Choose New Status -- (dropdown menu)

Below the details is a table titled '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

There is a link below the table: [Clients associated to this Rogue AP](#)

CLI から、

<#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.

```

不正エントリを不正リストから手動で削除するには、図に示すように、Monitor > Rogue > Unclassified APsの順に移動し、Removeをクリックします。



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	57afb7	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

不正APを友好的なAPとして設定するには、Security > Wireless Protection Policies > Rogue Policies > Friendly Rogues and add the rogue MAC addressの順に移動します。

追加された友好的な不正エントリは、図に示すように、Monitor > Rogues > Friendly Roguepageから確認できます。

Security

Friendly Rogue > Create

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

Type: Friendly

Apply

## Rogue Detector AP の設定

GUIを使用してAPをRogue Detectorとして設定するには、Wireless > All APsの順に移動します。AP名を選択し、図に示すようにAPモードを変更します。



The screenshot shows the Cisco Wireless Controller GUI. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WIRELESS' tab is active. The left sidebar shows a tree view with 'All APs' selected. The main area displays the configuration for APb4de.318b.fee0. The 'General' tab is active, and the 'AP Mode' dropdown menu is open, with 'Rogue Detector' selected. Other fields include AP Name, Location, AP MAC Address, Base Radio MAC, Admin Status, and various version and IP configuration details.

CLI から、

```
<#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

## Rogue Detector AP のスイッチ ポートの設定

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



注：この設定のネイティブVLANは、WLCにIP接続できるVLANです。


## RLDP の設定

コントローラのGUIでRLDPを設定するには、Security > Wireless Protection Policies > Rogue Policies > Generalの順に移動します。

Monitor Mode APs : モニタ モードの AP にのみ RLDP への参加を許可します。

All APs : ローカル/Flex-Connect/モニタモードのAPがRLDPプロセスに参加します。

Disabled : RLDP は自動的にトリガーされません。ただし、ユーザは CLI から特定の MAC アドレスに対して RLDP を手動でトリガーできます。

 注 : モニタモードAPは、ローカル/Flex-Connect APの両方が-85dbm RSSIを超える特定の不正を検出した場合、RLDPを実行するためにローカル/Flex-Connect APよりも優先されます。

CLI から、

<#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

RLDPスケジュールおよび手動トリガーは、コマンドプロンプトからのみ設定できます。RLDPを手動で開始するには、次の手順に従います。

```
<#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).
```

RLDPのスケジュールの場合：

```
<#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.
```

RLDPの再試行は、次のコマンドで設定できます。

```
<#root>
```

```
(Cisco Controller) >
```

```
config rogue ap rldp retries ?
```

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

## 不正緩和の設定

### 手動抑止の設定

不正APを手動で抑止するには、図に示すように、Monitor > Rogues > Unclassifiedの順に移動します。

The screenshot shows the Cisco Controller GUI. The top navigation bar has 'MONITOR' highlighted. The left sidebar shows 'Rogues' expanded, with 'Unclassified APs' selected. The main content area displays 'Rogue AP Detail' for a specific AP. The 'Update Status' dropdown is set to 'Contain'. A 'Maximum number of APs to contain the rogue' dropdown is also visible, with a value of 3 selected. Below this, a table lists APs that detected the rogue client.

Base Radio MAC	AP Name	SSID	Radio Type	Security Policy	Pre-Ambble	RSSI
00:27:e3:36:4d:a0	tiagoAPcb.98E1.3DEC		802.11g	Encrypted	Long	-128

CLI から、

```
<#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].

 注：特定の不正は1～4個のAPで抑止できます。デフォルトでは、コントローラはクライアントを含めるために1つのAPを使用します。2つのAPで特定の不正が検出される場合、APのモードにかかわらず、最も高いRSSIを持つAPがクライアントを抑止します。

## 自動抑止

自動抑止を設定するには、Security>Wireless Protection Policies>Rogue Policies>Generalの順に進み、ネットワークに適用可能なすべてのオプションを有効にします。

Cisco WLCに特定の不正デバイスを自動的に含める場合は、これらのボックスをオンにします。それ以外の場合は、デフォルト値のチェックボックスをオフのままにします。

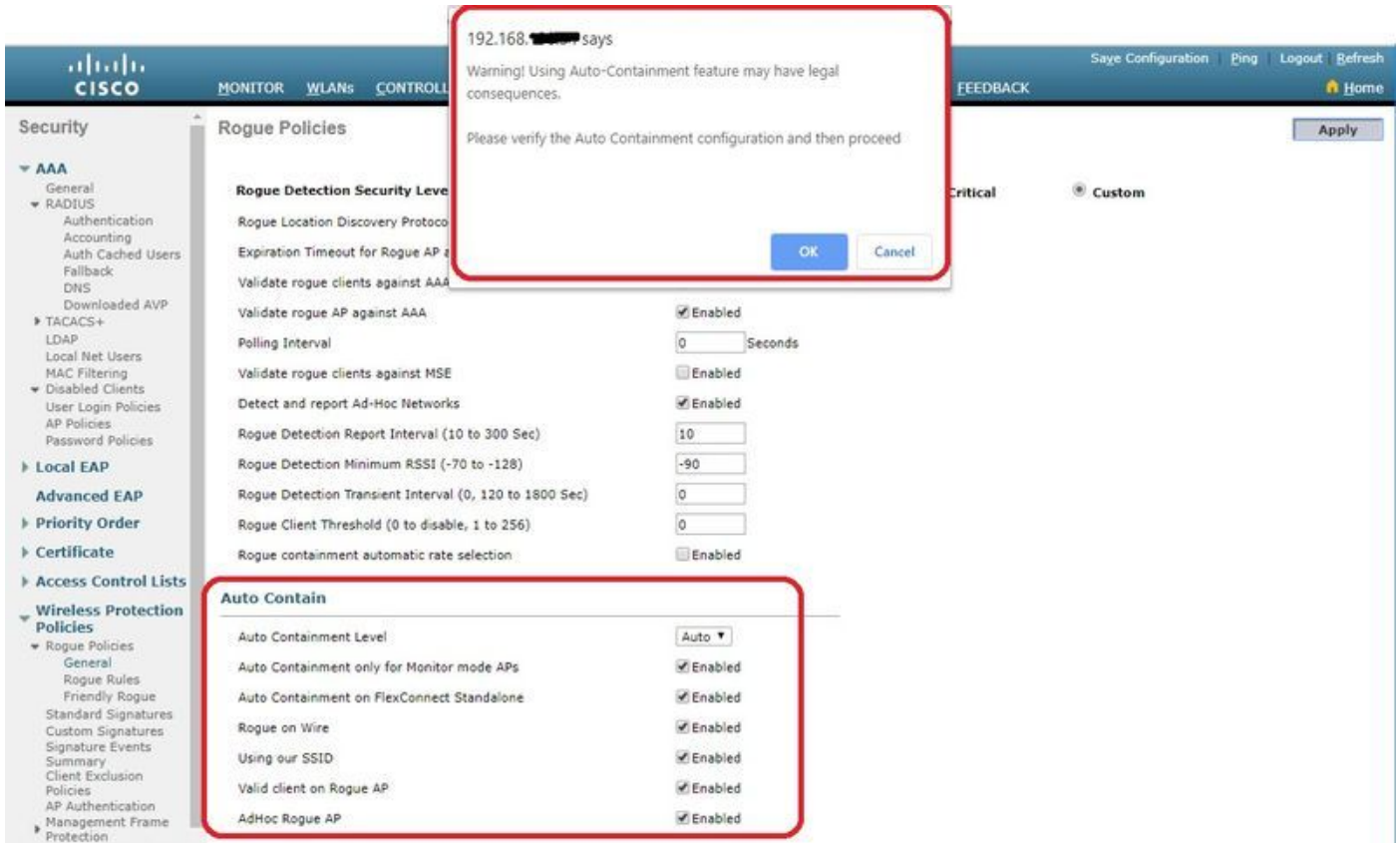
 警告：これらのパラメータのいずれかを有効にすると、「この機能の使用は法的な影響を及ぼします。続行しますか？」 Industrial, Scientific, and Medical (ISM)帯域の2.4 GHzおよび5 GHzの周波数は一般に公開されており、ライセンスなしで使用できます。そのため、他のパーティのネットワークにデバイスを封じ込めると、法的な影響が生じる可能性があります。

Auto Containパラメータは次のとおりです。

パラメータ	説明
自動封じ込めレベル	<p>ドロップダウンリストから、不正の自動抑止レベルを1～4から選択できます。</p> <p>任意の自動抑止ポリシーを使用して不正が封じ込められた状態に移行した場合、最大4つのAPを自動抑止に選択できます。</p> <p>自動抑止に使用するAPの数を自動的に選択するには、Autoを選択することもできます。Cisco WLCは、効果的な封じ込めに必要なAPの数をRSSIに基づいて選択します。</p> <p>各コンテインメントレベルに関連付けられるRSSI値は次のとおりです。</p> <ul style="list-style-type: none"><li>• 1 — 0 ~ -55 dBm</li><li>• 2 — -75 ~ -55 dBm</li><li>• 3 — -85 ~ -75 dBm</li><li>• 4 — -85 dBm未満</li></ul>
自動コンテインメントはモニタモードAPに対してのみ実行	自動抑止のモニタモードAPを有効にするチェックボックスをオンにします。デフォルトは無効ステートです。

パラメータ	説明
FlexConnectスタンドアロンでの自動抑止	<p>スタンドアロンモードのFlexConnect APで自動抑止を有効にするチェックボックスをオンにします。デフォルトは無効ステートです。</p> <p>FlexConnect APがスタンドアロンモードの場合、有効にできるのはUse our SSIDまたはAdHoc Rogue AP auto containmentポリシーだけです。スタンドアロンAPがCisco WLCに接続し直すと、抑止は停止します。</p>
有線での不正	<p>を有効にして、有線ネットワークで検出された不正を自動的に抑止します。デフォルトは無効ステートです。</p>
SSIDを使用する	<p>ネットワークのSSIDをアドバタイズする不正を自動的に含めることができるようにするには、このチェックボックスをオンにします。このパラメータを選択しない場合、Cisco WLCはこのような不正が検出されたときのみアラームを生成します。デフォルトは無効ステートです。</p>
不正AP上の有効なクライアント	<p>を有効にして、信頼できるクライアントが関連付けられている不正なアクセスポイントを自動的に抑止します。このパラメータを選択しない場合、Cisco WLCはこのような不正が検出されたときのみアラームを生成します。デフォルトは無効ステートです。</p>
アドホック不正AP	<p>Cisco WLCによって検出されたアドホックネットワークを自動的に含めることができるようにするためのチェックボックス。このパラメータを選択しない場合、Cisco WLCはそのようなネットワークが検出されたときのみアラームを生成します。デフォルトは無効ステートです。</p>





ApplyをクリックしてCisco WLCにデータを送信しますが、データは電源を再投入しても保持されません。これらのパラメータは揮発性RAMに一時的に保存されます。

CLI から、

```
<#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
```

# Prime Infrastructureを使用

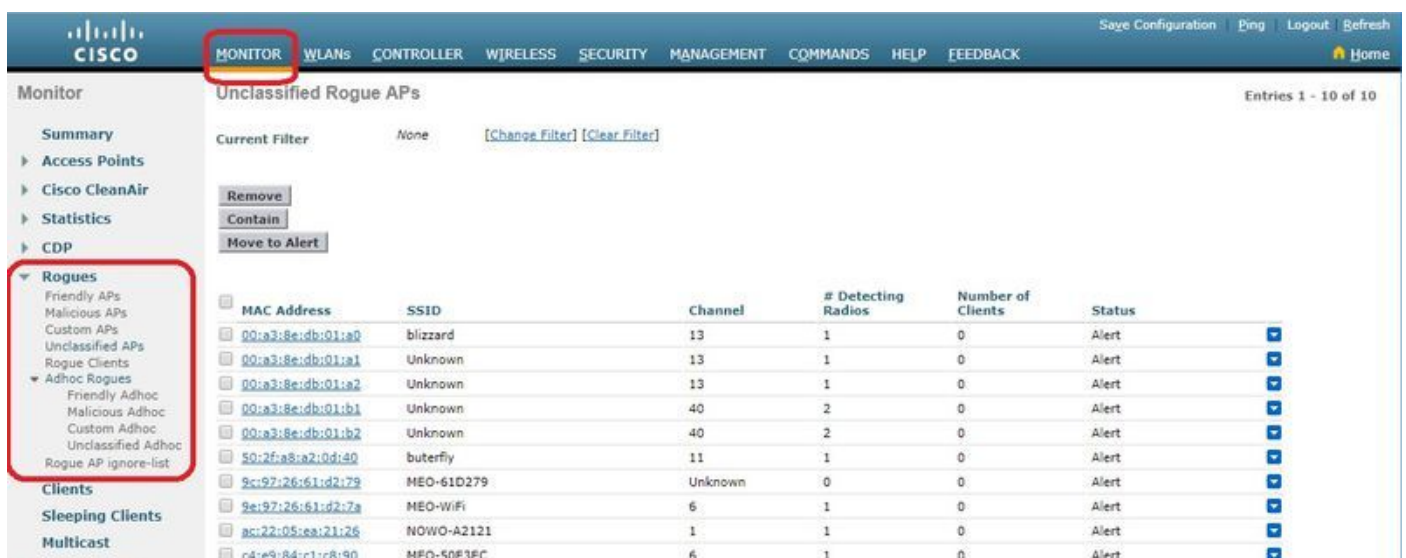
Cisco Prime Infrastructureを使用すると、1つ以上のコントローラおよび関連するAPを設定および監視できます。Cisco PIには、大規模なシステムの監視と制御を容易にするツールがあります。シスコのワイヤレスソリューションでCisco PIを使用すると、コントローラはクライアント、不正なアクセスポイント、不正なアクセスポイントクライアント、無線周波数ID(RFID)タグの場所を定期的に判別し、その場所をCisco PIデータベースに保存します。

Cisco Prime Infrastructureは、ルールベースの分類をサポートし、コントローラで設定された分類ルールを使用します。コントローラは、次のイベントの後にトラップをCisco Prime Infrastructureに送信します。

- 不明なアクセスポイントが初めてFriendly状態に移行すると、コントローラは不正の状態がAlertの場合にのみトラップをCisco Prime Infrastructureに送信します。theroguestateがInternalまたはExternalの場合、トラップは送信されません。
- タイムアウトの期限が切れた後にarogueentryが削除された場合、コントローラはMalicious (アラート、脅威) またはUnclassified (アラート) に分類されたCisco Prime Infrastructureforrogueaccess point(APAP)にトラップを送信します。コントローラは、Contained、Contained Pending、Internal、およびExternalの各プロパティを持つエントリを削除しません。

## 確認

グラフィカルインターフェイスでコントローラ内の不正の詳細を検索するには、図に示すように、Monitor > Roguesの順に移動します。




The screenshot shows the Cisco Prime Infrastructure web interface. The 'MONITOR' tab is selected in the top navigation bar. The left sidebar shows the 'Rogues' section expanded, with a red box highlighting it. The main content area displays 'Unclassified Rogue APs' with a table of detected rogue access points.

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	butterfly	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

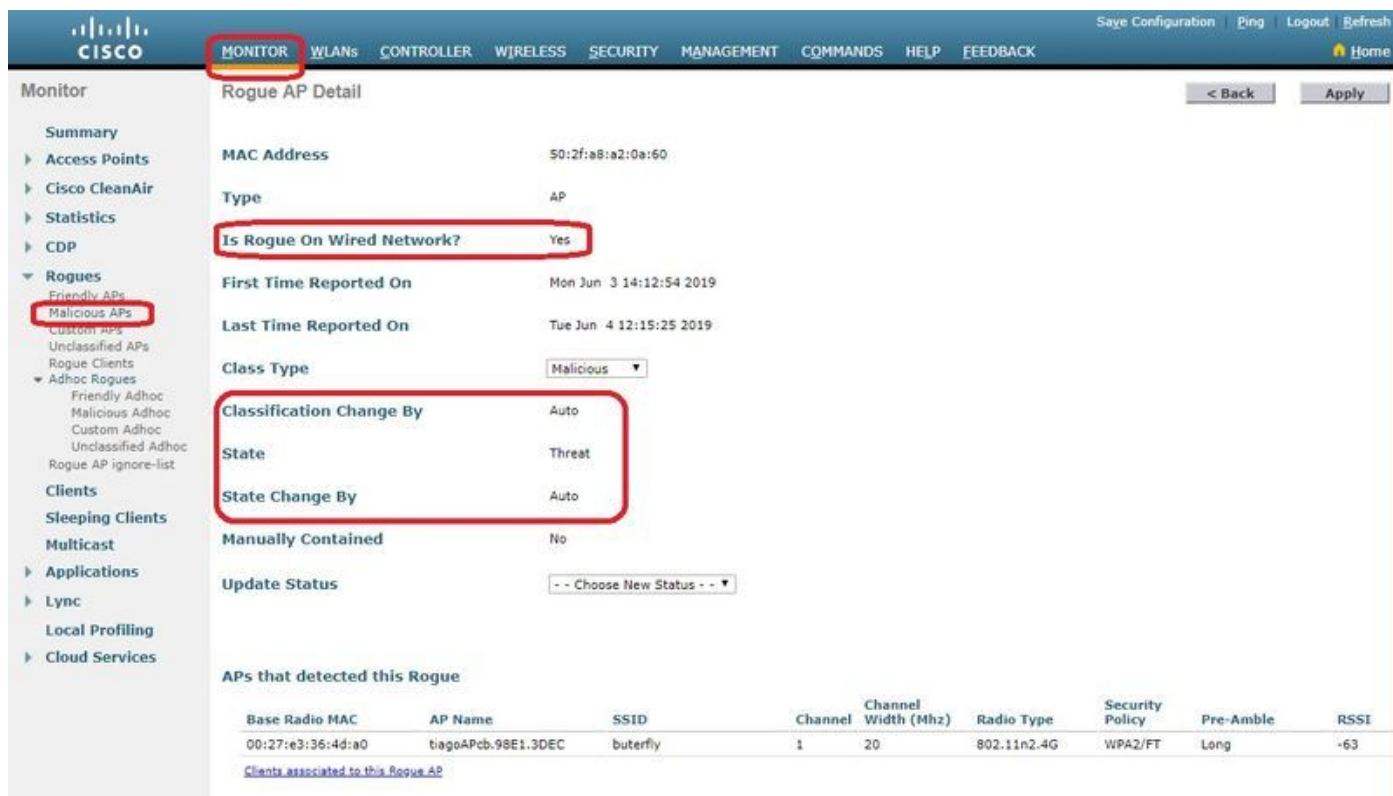
このページでは、不正のさまざまな分類を利用できます。

- Friendly APs : 管理者によって友好的とマーキングされている AP です。
- Malicious APs:RLDPまたはRogue Detector APを介して悪意のあるAPとして識別された AP。

- Custom APs:Rogue RulesによってCustomに分類されたAPです。
- Unclassified APs : デフォルトでは、不正APは未分類リストとしてコントローラに表示されます。
- Rogue Clients : 不正 AP に接続されているクライアントです。
- Adhoc Rogues : アドホックの不正クライアントです。
- Rogue AP ignore list:PIを通じてリストされます。

 注:WLCとAutonomous APが同じPIによって管理されている場合、WLCは自動的にこのAutonomous APをRogue AP ignore listにリストします。この機能をイネーブルにするために、WLCでの追加の設定は必要ありません。

特定の不正エントリをクリックして、その不正の詳細を取得します。有線ネットワークで検出された不正の例を次に示します。



The screenshot shows the Cisco WLC Monitor interface. The 'MONITOR' tab is selected. The left sidebar shows the navigation menu with 'Rogues' expanded to 'Malicious APs'. The main content area displays 'Rogue AP Detail' for a specific AP. Key fields are highlighted with red boxes: 'Is Rogue On Wired Network?' (Yes), 'Classification Change By' (Auto), and 'State' (Threat). Below the details is a table titled 'APs that detected this Rogue'.

Base Radio MAC	AP Name	SSID	Channel	Channel Width (Mhz)	Radio Type	Security Policy	Pre-Ambble	RSSI
00:27:e3:36:4d:a0	tiagoAPcb.98E1.3DEC	butterfly	1	20	802.11n.2.4G	WPA2/FT	Long	-63

CLI から、

```
<#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 RSSI det-Ap	#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
```

```

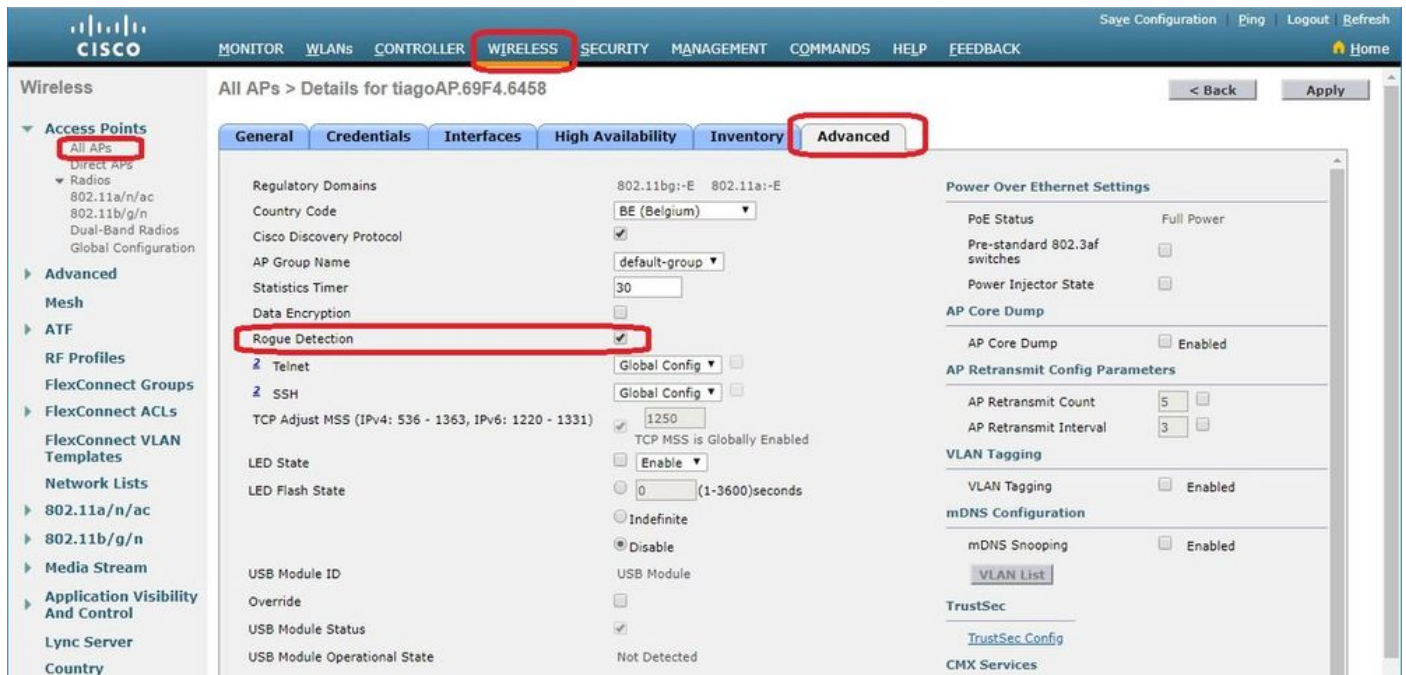
Rogue BSSID..... 50:2f:a8:a2:0a:60
Is Rogue on Wired Network..... Yes
Classification..... Malicious
Classification change by..... Auto
Manual Contained..... No
State..... Threat
State change by..... Auto
First Time Rogue was Reported..... Tue Jun 4 13:06:55 2019
Last Time Rogue was Reported..... Wed 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

```

トラブルシューティング

## 不正が検出されない場合

APで不正検出が有効になっていることを確認します。GUIの場合：



CLIで次のコマンドを実行します。

```
<#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
[...]
```

次のコマンドを使用して、APで不正検出をイネーブルにできます。

```
<#root>
```

```
(Cisco Controller) >
```

```
config rogue detection enable ?
```

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

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

ローカルモードAPはカントリーチャンネル/DCAチャンネルのみをスキャンし、設定によって異なります。不正が他のチャンネルにある場合、ネットワークにモニターモードAPがなければ、コントローラではその不正を特定できません。確認するため、次のコマンドを発行します。

```
<#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
```

- 不正APはSSIDをブロードキャストしません。
- 不正APのMACアドレスが友好的な不正リストに追加されていないか、またはPIを通じてリストで許可されていないことを確認します。
- 不正APからのビーコンは、不正を検出したAPに到達できません。これは、APディテクタの不正に近いスニファを使用してパケットをキャプチャすることで確認できます。
- ローカルモードのAPが不正を検出するまでに最大9分かかることがあります ( 3サイクル 180x3 ) 。
- Cisco AP では、パブリック セーフティ チャンネル ( 4.9 Ghz ) のような周波数上にある不正を検出できません。



- Cisco APは、FHSS ( 周波数ホッピングスペクトラム拡散 ) で動作する不正を検出できません。

## 有益なデバッグ

```
<#root>
```

```
(Cisco Controller) >
```

```
debug client
```

```
(If rogue mac is known)
```

```
(Cisco Controller) >
```

```
debug client 50:2f:a8:a2:0a:60
```

```
(Cisco Controller) >*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Found Rogue AP: 50:2f:a8:a2:0a:60
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 New RSSI report from AP 00:27:e3:36:4d:a0 rssi -55
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559724417. Detected
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 SYNC for Channel (new/old : 1/0) or channel width
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 rg changed rssi prev -64, new -55
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Updated AP report 00:27:e3:36:4d:a0 rssi -55,
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue detected by AP: 00:27:e3:36:4d:a0
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 RadioType: 3 lradInfo->containSlotId = 2 Received
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue before Rule Classification : Class malicious
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue doesnt qualify for rule classification : Class
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Manual Contained Flag = 0, trustlevel = 7
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 ssidLen = 8 min = 8 50:2f:a8:a2:0a:60
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 This rogue does not use my ssid. Rogue ssid=but
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue AP: 50:2f:a8:a2:0a:60 autocontain = 2 Mo
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Checking Impersonation source 50:2f:a8:a2:0a:60
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Known AP 0 mfp global 0 AP Auth Global 0 mfp Im
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue Client ssid: butterfly
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue Client ssid: butterfly
```

```
<#root>
```

```
(Cisco Controller) >
```

```
debug dot11 rogue enable
```

```
(Cisco Controller) >*emWeb: Jun 05 08:39:46.828:
Debugging session started on Jun 05 08:39:46.828 for WLC AIR-CT3504-K9 Version :8.8.120.0 SN :FCW22
*iappSocketTask: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 Posting Rogue AP Iapp Report from AP for proces

*apfRogueTask_2: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 fakeAp check: slot=0, entryIndex=0, (Radio_upTi
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid b0:72:bf:93:e0:d7 src l
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 50:2f:a8:a2:0a:60 src
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:a1 src
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:b0 src
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 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 entries 5 slotId 0 bssid 00:a3:8e:db:01:b2 src
*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

```

## 一般的なトラップ ログ

不正が検出されるか、不正リストから削除されると、次のようになります。

0	2019年6月5日	不正クライアント : b4:c0:f5:2b:4f:90は1つのAPによって検出されます不正ク
---	-----------	---

	(水) 09:01:57	クライアントBSSID:a6:b1:e9:f0:e8:41、状態：アラート、最終検出AP:00:27:e3:36:4d:a0不正クライアントゲートウェイmac 00:00:00:02:02:02。
1	2019年6月5日 (水) 09:00:39	不正AP:9c:97:26:61:d2:79をベース無線MACから削除:00:27:e3:36:4d:a0インターフェイス番号：0(802.11n(2.4 GHz))
2	2019年6月5日 (水) 08:53:39	不正AP:7c:b7:33:c0:51:14、ベースRadio MACから削除:00:27:e3:36:4d:a0インターフェイス番号：0(802.11n(2.4 GHz))
3	2019年6月5日 (水) 08:52:27	不正クライアント：fc:3f:7c:5f:b1:1b is detected by 1 APs Rogue Client Bssid: 50:2f:a8:a2:0a:60, State: Alert, Last detecting AP :00:27:e3:36:4d:a0 Rogue Client gateway mac 00:26:44:73:c5:1d.
4	2019年6月5日 (水) 08:52:17	不正AP(AP):d4:28:d5:da:e0:d4、ベースRadio MACから削除:00:27:e3:36:4d:a0インターフェイス番号：0(802.11n(2.4 GHz))

## 推奨事項

1. ネットワークに不正があると疑われる場合は、すべてのチャンネルに対してチャンネルスキャンを設定します。
2. Rogue Detector APの数と場所は、フロアごとに1つから建物ごとに1つまでさまざまであり、有線ネットワークのレイアウトによって異なります。フロアまたは建物ごとに少なくとも1つのRogue Detector APを配備することをお勧めします。Rogue Detector APでは、モニタ対象のすべてのレイヤ2ネットワークブロードキャストドメインへのトランクが必要であるため、配置はネットワークの論理レイアウトに依存します。

## 不正が分類されない場合

不正ルールが適切に設定されているかどうか確認します。

## 有益なデバッグ

<#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
```

## 推奨事項

既知の不正エントリがある場合は、友好的なリストに追加するか、AAAによる検証を有効にして、既知のクライアントエントリが認証、認可、およびアカウントリング(AAA)データベースにあることを確認します。

## RLDPが不正を検出しない

- 不正が DFS チャンネルにある場合、RLDP は動作しません。
- RLDPは、不正WLANが開いていて、DHCPが使用可能な場合にのみ機能します。
- ローカルモードAPがDFSチャンネルでクライアントにサービスを提供する場合、RLDPプロセスには参加しません。
- RLDPは、APモデル1800i、1810 OEAP、1810W、1815、1830、1850、2800、および3800シリーズのAPではサポートされていません。

## 有益なデバッグ

```
<#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  
\*apfOpenDtIsocket: Jun 05 15:03:00.608: apfRoguePreamble = 0 mobile b4:de:31:a4:e0:31.  
\*apfOpenDtIsocket: 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
```

## 推奨事項

1. 疑わしい不正エントリ上で RLDP を手動で起動してください。
2. RLDP が定期的に行われるようにスケジュールを設定してください。
3. RLDP はローカル AP またはモニタ モード AP に配備できます。ほとんどのスケーラブルな展開では、クライアントサービスへの影響を排除するために、可能な場合はモニタモード AP に RLDP を展開します。ただし、この推奨事項では、5 つのローカル モード AP ごとに 1 つのモニタ モード AP という一般的な比率で、モニタ モード AP のオーバーレイを配備する必要があります。この作業には、Adaptive WIPS モニタ モードの AP を活用することもできます。

## Rogue Detector AP

Rogue Detector の不正エントリは、AP コンソールで次のコマンドを使用して確認できます。有線の不正の場合、フラグは set ステータスに移動します。

```
<#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 コンソール内の便利なデバッグ コマンド

<#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
```

不正抑止

予想されるデバッグ

<#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 ContainmentLe

*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
*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
*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
*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
*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

```

## 推奨事項

1. ローカル/Flex-ConnectモードのAPには、無線ごとに3台のデバイスを一度に含めることができ、モニタモードのAPには無線ごとに6台のデバイスを含めることができます。その結果、APに許可されている最大デバイス数が含まれていないことを確認します。最大数のデバイスが抑止されていると、クライアントは抑止の保留状態にあります。
2. 自動抑止ルールを検証してください。

## 結論

シスコの中央集中型コントローラ ソリューションの不正検出と抑止は、業界でも最も効果的で影響の少ない不正検出/抑止手法です。ネットワーク管理者はさらに柔軟にソリューションをカスタマイズして、ネットワークの要件に対応できます。

## 関連情報

- [Cisco Wireless Controllerコンフィギュレーションガイド、リリース8.8 – 不正管理](#)

- [Cisco Wireless LAN Controller\(WLC\)の設定のベストプラクティス](#)
- [WLC 3504リリース8.5導入ガイド](#)
- [Cisco 5520ワイヤレスLANコントローラ導入ガイド](#)
- [Cisco Wireless ControllerとLightweightアクセスポイントのリリースノート、Cisco Wirelessリリース8.8.120.0](#)



## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。