

# Résolution des problèmes de détection et de réduction des intrusions dans un réseau sans fil unifié

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Présentation des indésirables](#)

[Détection de systèmes indésirables](#)

[Analyse hors canal](#)

[Analyse en mode surveillance](#)

[Comparaison des modes local et moniteur](#)

[Identification des indésirables](#)

[Enregistrements indésirables](#)

[Détails des indésirables](#)

[Pour exporter des événements indésirables](#)

[Délai d'enregistrement non autorisé](#)

[Point d'accès Rogue Detector](#)

[Considérations d'évolutivité](#)

[RLDP](#)

[Avertissements du protocole RLDP](#)

[Suivi des ports de commutateur](#)

[Classification des indésirables](#)

[Règles de classification non fiables](#)

[Faits HA](#)

[Faits sur FlexConnect](#)

[Atténuation des indésirables](#)

[Confinement des systèmes non fiables](#)

[Détails du confinement des indésirables](#)

[Confinement Automatique](#)

[Mises en garde contre les systèmes non fiables](#)

[Port du commutateur fermé](#)

[Configuration](#)

[Configurer la détection des systèmes non fiables](#)

[Configurer l'analyse des canaux pour la détection des indésirables](#)

[Configurer la classification non fiable](#)

[Configuration de la réduction des indésirables](#)

[Configurer le confinement manuel](#)

[Confinement Automatique](#)

[Avec Prime Infrastructure](#)

[Vérification](#)

[Dépannage](#)

[Si Le Rogue N'Est Pas Détecté](#)

[Débogages utiles](#)

[Journaux des interruptions attendus](#)

[Recommandations](#)

[Si le non autorisé n'est pas classé](#)

[Débogages utiles](#)

[Recommandations](#)

[Le protocole RLDP ne localise pas les indésirables](#)

[Débogages utiles](#)

[Recommandations](#)

[Point d'accès Rogue Detector](#)

[Commandes Debug utiles dans une console AP](#)

[Confinement des systèmes non fiables](#)

[Débogages attendus](#)

[Recommandations](#)

[Conclusion](#)

[Informations connexes](#)

## Introduction

Ce document décrit la détection et la réduction des intrusions sur les réseaux sans fil Cisco.

Les réseaux sans fil étendent les réseaux filaires et augmentent la productivité des travailleurs et l'accès aux informations. Cependant, un réseau sans fil non autorisé présente un souci de couche de sécurité supplémentaire. La sécurité du port sur les réseaux filaires est moins mise de l'avant, et les réseaux sans fil sont une extension facile aux réseaux filaires. Par conséquent, un employé qui introduit son propre point d'accès (Cisco ou non Cisco) dans une infrastructure filaire ou sans fil bien sécurisée et qui autorise l'accès d'utilisateurs non autorisés à ce réseau par ailleurs sécurisé, peut facilement compromettre un réseau sécurisé.

La détection des systèmes non fiables permet à l'administrateur réseau de surveiller et d'éliminer ce problème de sécurité. L'architecture de réseau unifié Cisco fournit des méthodes de détection des systèmes non fiables qui permettent une solution complète d'identification et de confinement des systèmes non fiables, sans nécessiter de réseaux et d'outils superposés coûteux et difficiles à justifier.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleurs Lan Sans Fil Cisco.
- Infrastructure Cisco Prime.

## Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleurs LAN sans fil Cisco Unified (gammes 5520, 8540 et 3504) qui exécutent la version 8.8.120.0.
- Séries de points d'accès 1832, 1852, 2802 et 3802 de phase 2.
- Gammes AP 3700, 2700 et 1700 phase 1.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Présentation des indésirables

Tout périphérique qui partage votre spectre et n'est pas géré par vous peut être considéré comme un pirate. Un pirate devient dangereux dans les scénarios suivants :

- Lorsque vous utilisez le même SSID (Service Set Identifier) que votre réseau (honeypot).
- Lorsqu'il est détecté sur le réseau câblé.
- Des criminels ad hoc.
- Configuration par un tiers, la plupart du temps, avec une intention malveillante.

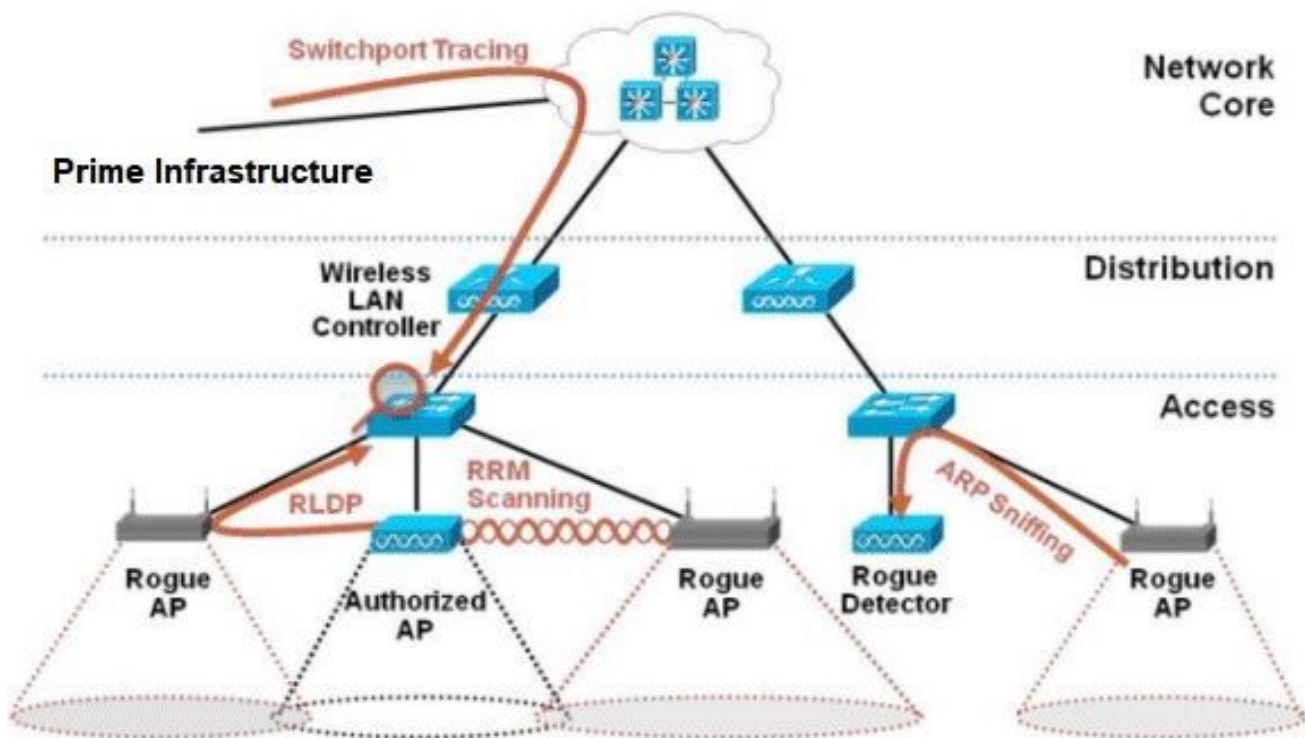
La meilleure pratique consiste à utiliser la détection des systèmes non fiables pour minimiser les risques de sécurité, par exemple dans un environnement d'entreprise. Cependant, dans certains cas, la détection des systèmes non fiables n'est pas nécessaire, par exemple dans le déploiement d'un point d'accès Office Extend (OEAP), dans toute la ville et en extérieur. Avec l'utilisation de points d'accès maillés extérieurs pour détecter les indésirables fournirait peu de valeur alors qu'il utiliserait des ressources pour analyser. Enfin, il est essentiel d'évaluer (ou d'éviter complètement) le confinement automatique non autorisé, car il existe des problèmes et des responsabilités juridiques potentiels si le confinement est laissé à fonctionner automatiquement.

La solution Cisco Unified Wireless Network (UWN) comporte trois phases principales de gestion des périphériques indésirables :

- Détection : une analyse de gestion des ressources radio (RRM) est utilisée pour détecter la présence de périphériques indésirables.
- Classification : le protocole RLDP (Rogue Location Discovery Protocol), les détecteurs de périphériques non autorisés (points d'accès de phase 1 uniquement) et les traces de port du commutateur sont utilisés pour identifier si le périphérique non autorisé est connecté au réseau câblé. Les règles de classification des produits malveillants permettent également de classer les produits malveillants dans des catégories spécifiques en fonction de leurs caractéristiques.
- Atténuation : l'arrêt du port du commutateur, l'emplacement non autorisé et le confinement des périphériques non autorisés sont utilisés dans pour localiser leur emplacement physique et pour neutraliser la menace du périphérique non autorisé.

# Cisco Rogue Management Diagram

## Multiple Methods

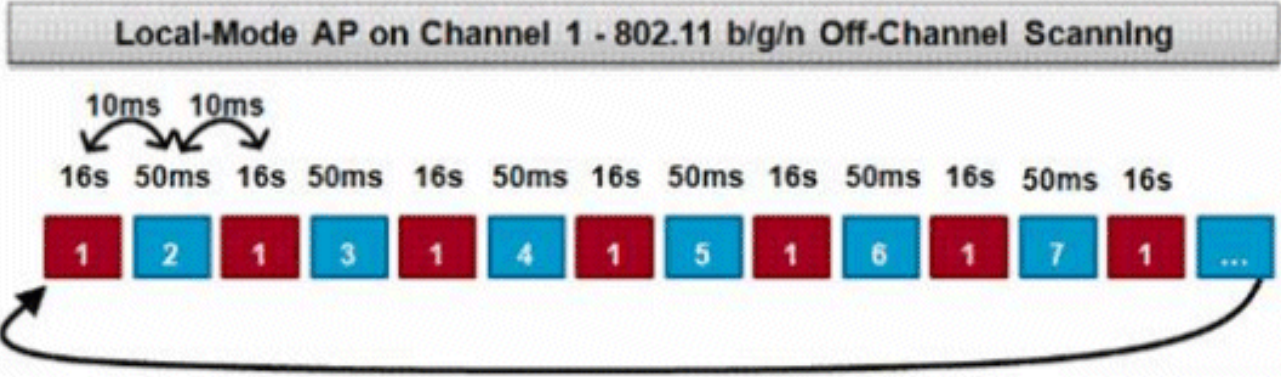


## Détection de systèmes indésirables

Un pirate est essentiellement un périphérique qui partage votre spectre, mais qui n'est pas sous votre contrôle. Cela inclut les points d'accès non autorisés, les routeurs sans fil, les clients non autorisés et les réseaux ad hoc non autorisés. Cisco UWN utilise un certain nombre de méthodes pour détecter les périphériques indésirables basés sur le Wi-Fi, tels qu'une analyse hors canal et des fonctionnalités de mode de surveillance dédiées. Cisco Spectrum Expert peut également être utilisé pour identifier les périphériques non conformes au protocole 802.11, tels que les ponts Bluetooth.

### Analyse hors canal

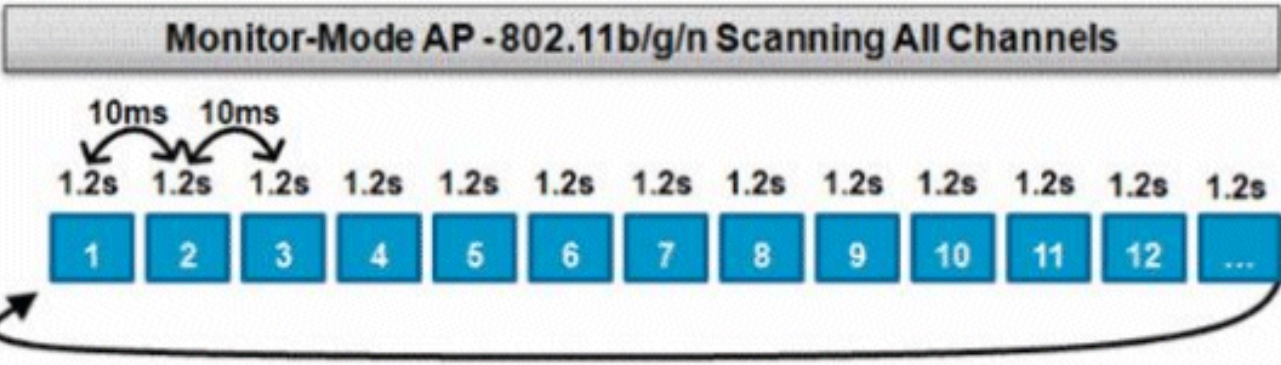
Cette opération est effectuée par les points d'accès en mode local et Flex-Connect (en mode connecté) et utilise une technique de découpage de temps qui permet le service client et l'analyse de canal avec l'utilisation de la même radio. Avec le passage à off channel pendant une période de 50 ms toutes les 16 secondes, le point d'accès, par défaut, ne passe qu'un petit pourcentage de son temps à ne pas servir les clients. Notez également qu'un intervalle de changement de canal de 10 ms se produit. Dans l'intervalle d'analyse par défaut de 180 secondes, chaque canal FCC 2,4 GHz (1-11) est analysé au moins une fois. Pour d'autres domaines réglementaires, tels que l'ETSI, le point d'accès est hors canal pendant un pourcentage de temps légèrement supérieur. La liste des canaux et l'intervalle d'analyse peuvent être ajustés dans la configuration RRM. Cela limite l'impact sur les performances à un maximum de 1,5 % et l'intelligence est intégrée à l'algorithme pour suspendre l'analyse lorsque des trames QoS de priorité élevée, telles que la voix, doivent être fournies.



Ce graphique est une représentation de l'algorithme de balayage hors canal pour un point d'accès en mode local dans la bande de fréquences de 2,4 GHz. Une opération similaire est effectuée en parallèle sur la radio 5 GHz si le point d'accès en possède une. Chaque carré rouge représente le temps passé sur le canal d'accueil des points d'accès, tandis que chaque carré bleu représente le temps passé sur les canaux adjacents à des fins d'analyse.

**Analyse en mode surveillance**

Cette opération est effectuée par les points d'accès en mode de surveillance Monitor Mode et Adaptive wIPS qui utilisent 100 % du temps radio pour balayer tous les canaux dans chaque bande de fréquence respective. Cela permet une plus grande vitesse de détection et permet de passer plus de temps sur chaque canal individuel. Les points d'accès en mode surveillance sont également bien meilleurs pour détecter les clients indésirables, car ils disposent d'une vue plus complète de l'activité qui se produit dans chaque canal.



Ce graphique est une représentation de l'algorithme de balayage hors canal pour un point d'accès en mode moniteur dans la bande de fréquences de 2,4 GHz. Une opération similaire est effectuée en parallèle sur la radio 5 GHz si le point d'accès en possède une.

**Comparaison des modes local et moniteur**

Un point d'accès en mode local répartit ses cycles entre le service des clients WLAN et l'analyse des canaux à la recherche de menaces. Par conséquent, il faut plus de temps à un point d'accès en mode local pour parcourir tous les canaux, et il passe moins de temps à collecter des données sur un canal particulier afin que les opérations du client ne soient pas interrompues. Par conséquent, les temps de détection des attaques et des attaques indésirables sont plus longs (3 à 60 minutes) et une plus petite plage d'attaques en direct peut être détectée qu'avec un point d'accès en mode surveillance.

En outre, la détection du trafic par salves, tel que les clients indésirables, est beaucoup moins déterministe, car le point d'accès doit se trouver sur le canal du trafic au moment où le trafic est transmis ou reçu. Cela devient un exercice de probabilités. Un point d'accès en mode surveillance passe tous ses cycles à l'analyse des canaux pour rechercher les attaques indésirables et en direct. Un point d'accès en mode surveillance peut être utilisé simultanément pour Adaptive WIPS, les services de localisation (sensibles au contexte) et d'autres services en mode surveillance.

Lorsque des points d'accès en mode surveillance sont déployés, les avantages sont des délais de détection réduits. Lorsque les points d'accès en mode surveillance sont également configurés avec Adaptive WIPS, une gamme plus large de menaces et d'attaques en direct peut être détectée.

### **Points d'accès en mode local**

Sert les clients avec une analyse hors canal par tranches de temps

Écoute pendant 50 ms sur chaque canal

Configurable pour l'analyse :

- Tous les canaux
- Canaux par pays (par défaut)
- canaux DCA

### **AP en mode surveillance**

Analyse dédiée

Écoute 1,2 s sur chaque canal

Analyse tous les canaux

## **Identification des indésirables**

Si la réponse de sonde ou les balises d'un périphérique non autorisé sont entendues par des points d'accès locaux, en mode connexion flexible ou en mode surveillance, alors ces informations sont communiquées via CAPWAP au contrôleur LAN sans fil (WLC) pour le processus. Afin d'empêcher les faux positifs, un certain nombre de méthodes sont utilisées pour s'assurer que d'autres AP gérés basés sur Cisco ne sont pas identifiés comme un périphérique non autorisé. Ces méthodes incluent les mises à jour de groupes de mobilité, les paquets de voisinage RF et les points d'accès autorisés par liste via Prime Infrastructure (PI).

## **Enregistrements indésirables**

Bien que la base de données des périphériques non autorisés du contrôleur ne contienne que l'ensemble actuel des périphériques non autorisés détectés, l'interface IP inclut également un historique des événements et consigne les périphériques non autorisés qui ne sont plus détectés.

## **Détails des indésirables**

Un point d'accès CAPWAP sort du canal pendant 50 ms afin d'écouter les clients indésirables, de surveiller le bruit et les interférences de canal. Tous les clients ou points d'accès indésirables détectés sont envoyés au contrôleur, qui collecte ces informations :

- Adresse MAC du point d'accès non autorisé
- Nom de l'AP détecté comme indésirable
- Adresse MAC du ou des clients connectés non autorisés
- Stratégie de sécurité
- Le préambule
- Le rapport signal/bruit (SNR)
- L'indicateur RSSI (Receiver Signal Strength Indicator)

- Canal de détection des systèmes non fiables
- Radio dans laquelle un ordinateur non autorisé est détecté
- SSID non autorisé (si le SSID non autorisé est diffusé)
- Adresse IP non autorisée
- La première et la dernière fois que le voyous est signalé
- Largeur du canal

## Pour exporter des événements indésirables

Afin d'exporter des événements indésirables vers un système de gestion de réseau (NMS) tiers pour l'archivage, le WLC autorise l'ajout de récepteurs d'interruptions SNMP supplémentaires. Lorsqu'un pirate est détecté ou effacé par le contrôleur, un déroutement contenant ces informations est communiqué à tous les récepteurs de déroutement SNMP. Une mise en garde avec l'exportation d'événements via SNMP est que si plusieurs contrôleurs détectent le même non autorisé, des événements en double sont vus par le NMS comme la corrélation est seulement effectuée à PI.

## Délai d'enregistrement non autorisé

Une fois qu'un AP non autorisé a été ajouté aux enregistrements du WLC, il reste là jusqu'à ce qu'il ne soit plus vu. Après un délai d'attente configurable par l'utilisateur (valeur par défaut de 1 200 secondes), un utilisateur indésirable de la catégorie **\_unclassified\_category** expire.

Les programmes indésirables dans d'autres états tels que **\_Container\_and\_Friendly\_** persistent de sorte que la classification appropriée leur soit appliquée s'ils réapparaissent.

La taille maximale de la base de données pour les enregistrements non autorisés est variable sur les plates-formes de contrôleur :

- 3504 - Détection et confinement de jusqu'à 600 points d'accès indésirables et 1 500 clients indésirables
- 5520 - Détection et confinement de 24000 points d'accès indésirables et 32000 clients indésirables
- 8540 - Détection et confinement de 24000 points d'accès indésirables et 32000 clients indésirables

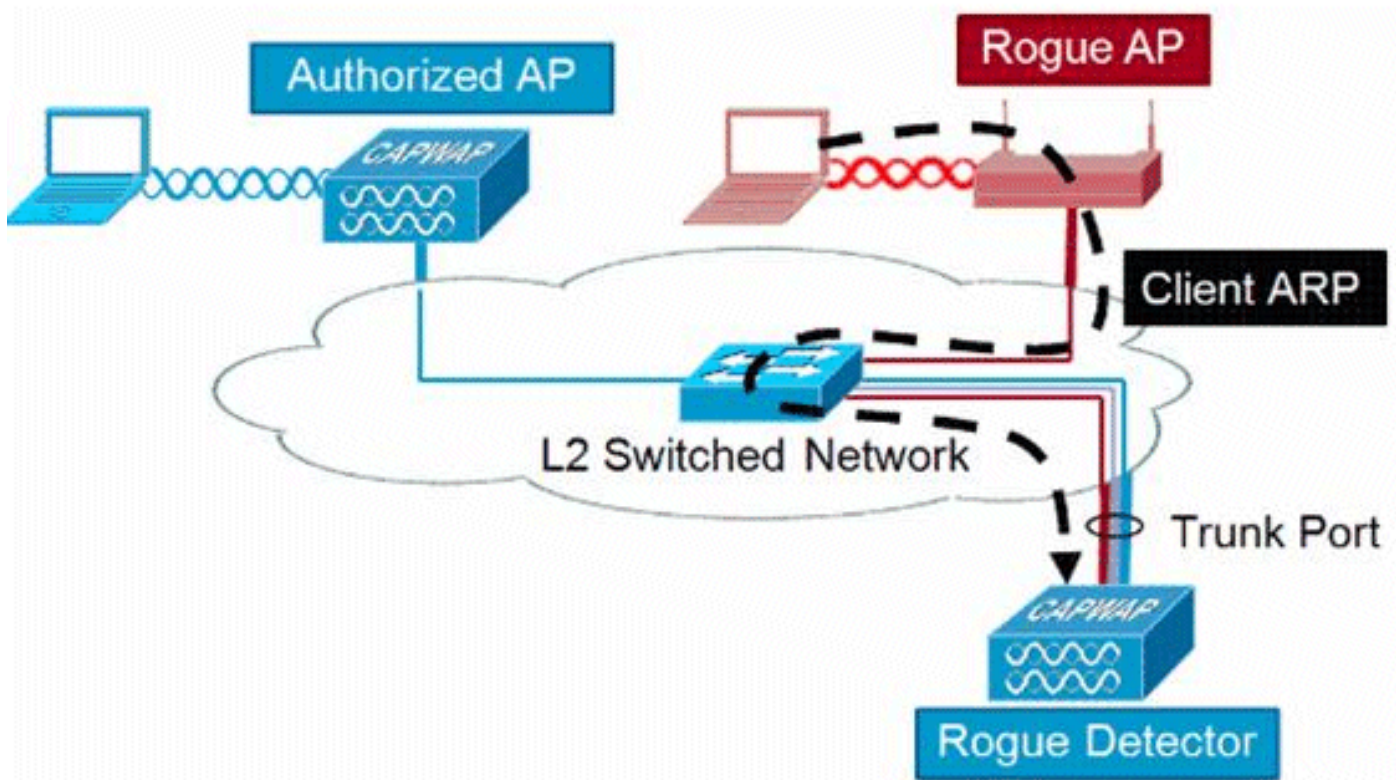
## Point d'accès Rogue Detector

Un point d'accès détecteur de voyous vise à mettre en corrélation les informations indésirables entendues dans l'air avec les informations ARP obtenues à partir du réseau câblé. Si une adresse MAC est entendue par radio en tant que point d'accès ou client non autorisé et qu'elle est également entendue sur le réseau câblé, il est déterminé que l'adresse non autorisée se trouve sur le réseau câblé. Si le point d'accès non autorisé est détecté comme étant sur le réseau câblé, la gravité de l'alarme pour ce point d'accès non autorisé est élevée à **\_critical\_**. Un point d'accès de détection de systèmes non autorisés ne parvient pas à identifier les clients non autorisés derrière un périphérique qui utilise la fonction NAT.

Cette approche est utilisée lorsque le point d'accès non autorisé possède une forme d'authentification, WEP ou WPA. Lorsqu'une forme d'authentification est configurée sur un point d'accès non autorisé, le point d'accès léger ne peut pas s'associer car il ne connaît pas la



méthode d'authentification et les informations d'identification configurées sur le point d'accès non autorisé.



**Note:** Seuls les points d'accès de phase 1 peuvent être configurés comme détecteurs de systèmes non fiables.

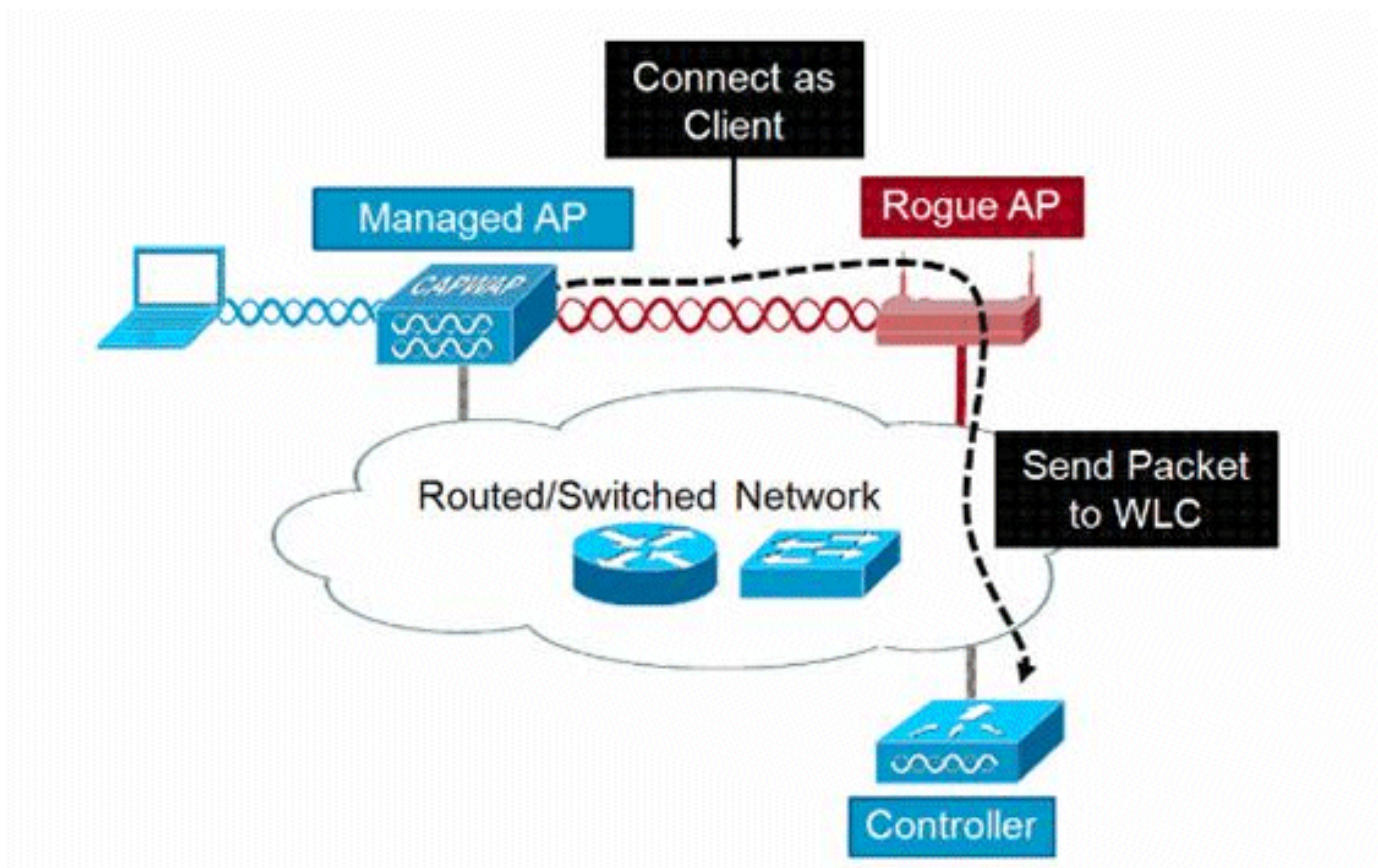
### Considérations d'évolutivité

Un point d'accès détecteur de systèmes non autorisés peut détecter jusqu'à 500 systèmes non autorisés et 500 clients non autorisés. Si le détecteur de périphériques non autorisés est placé sur une agrégation comportant trop de périphériques non autorisés, ces limites sont dépassées, ce qui entraîne des problèmes. Afin d'éviter que cela se produise, gardez les points d'accès détecteurs indésirables au niveau de la couche de distribution ou d'accès de votre réseau.

### RLDP

Le but du protocole RLDP est d'identifier si un point d'accès non autorisé spécifique est connecté à l'infrastructure filaire. Cette fonctionnalité utilise essentiellement le point d'accès le plus proche pour se connecter au périphérique indésirable en tant que client sans fil. Après la connexion en tant que client, un paquet est envoyé avec l'adresse de destination du WLC pour évaluer si le point d'accès est connecté au réseau câblé. Si le point d'accès non autorisé est détecté comme étant sur le réseau câblé, la gravité de l'alarme pour ce point d'accès non autorisé est élevée à critique.





L'algorithme du protocole RLDP est répertorié ici :

1. Identifiez le point d'accès unifié le plus proche de l'unité non autorisée en utilisant les valeurs de puissance du signal.
2. Le point d'accès se connecte ensuite au client non autorisé en tant que client WLAN, tente trois associations avant d'expirer.
3. Si l'association réussit, l'AP utilise alors DHCP pour obtenir une adresse IP.
4. Si une adresse IP a été obtenue, l'AP (qui agit comme un client WLAN) envoie un paquet UDP à chacune des adresses IP du contrôleur.
5. Si le contrôleur reçoit ne serait-ce qu'un seul des paquets RLDP du client, ce voyous est marqué comme étant connecté avec un niveau de gravité critique.

**Note:** Les paquets RLDP ne peuvent pas atteindre le contrôleur si les règles de filtrage sont en place entre le réseau du contrôleur et le réseau où se trouve le périphérique non autorisé.

### Avertissements du protocole RLDP

- Le protocole RLDP fonctionne uniquement avec des points d'accès non autorisés ouverts qui diffusent leur SSID avec authentification et chiffrement désactivés.
- Le protocole RLDP exige que le point d'accès géré qui agit en tant que client puisse obtenir une adresse IP via DHCP sur le réseau non autorisé
- Le protocole RLDP manuel peut être utilisé pour effectuer plusieurs tentatives et tracer le protocole RLDP sur un ordinateur non autorisé.
- Sur le processus RLDP, le point d'accès ne peut pas servir les clients. Cela a un impact négatif sur les performances et la connectivité des AP en mode local.

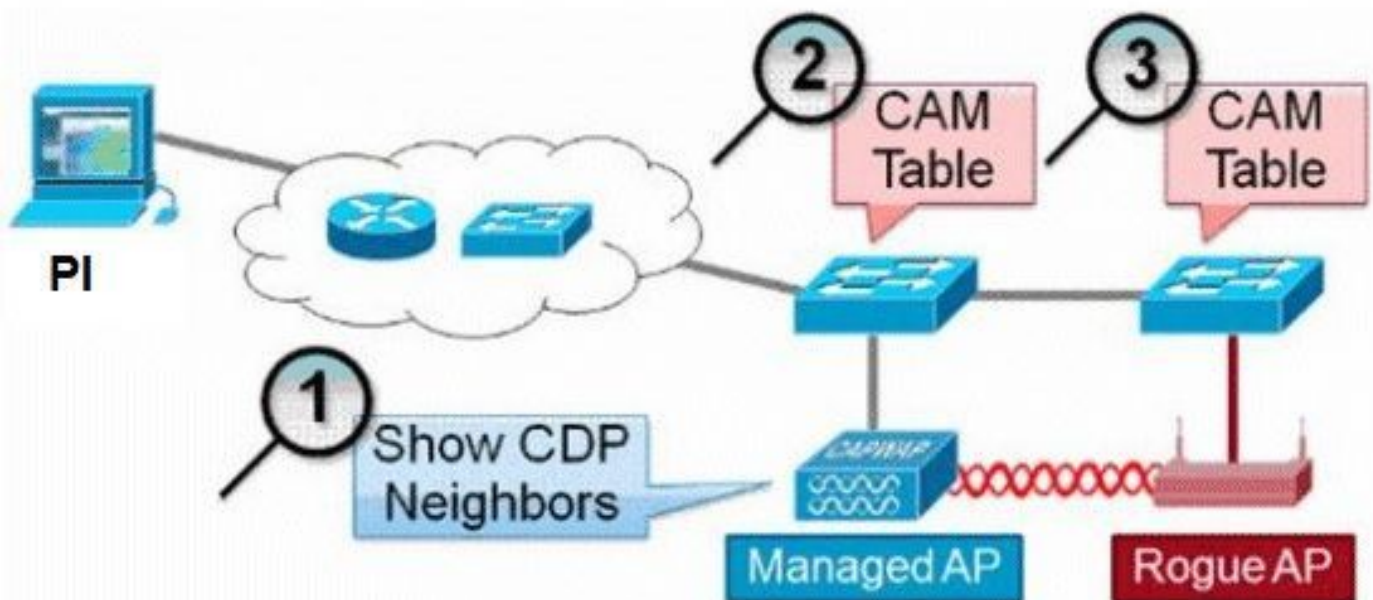
- Le protocole RLDP ne tente pas de se connecter à un point d'accès non autorisé fonctionnant sur un canal DFS 5 GHz.

## Suivi des ports de commutateur

Le suivi des ports de commutateur est une technique de réduction des AP indésirables. Bien que le suivi du port de commutateur soit initié au niveau de l'interface de protocole, il utilise les informations CDP et SNMP pour suivre un pirate jusqu'à un port spécifique du réseau.

Pour que le suivi du port du commutateur s'exécute, tous les commutateurs du réseau doivent être ajoutés à l'interface de protocole avec des informations d'identification SNMP. Bien que les informations d'identification en lecture seule permettent d'identifier le port sur lequel se trouve le voyant, les informations d'identification en lecture-écriture permettent à l'interpréteur de protocole d'arrêter également le port, ce qui permet de contenir la menace.

À l'heure actuelle, cette fonctionnalité fonctionne uniquement avec les commutateurs Cisco qui exécutent Cisco IOS® avec CDP activé, et CDP doit également être activé sur les points d'accès gérés.



L'algorithme de suivi du port de commutateur est répertorié ici :

1. L'IP recherche le point d'accès le plus proche, qui détecte le point d'accès non autorisé par liaison radio et récupère ses voisins CDP.
2. L'interpréteur de protocole utilise ensuite le protocole SNMP pour examiner la table CAM dans le commutateur voisin. Il recherche une correspondance positive pour identifier l'emplacement non autorisé.
3. Une correspondance positive est basée sur l'adresse MAC non autorisée exacte, +1/-1 sur l'adresse MAC non autorisée, toute adresse MAC de client non autorisé ou une correspondance OUI basée sur les informations du fournisseur inhérentes à une adresse MAC.
4. Si aucune correspondance positive n'est trouvée sur le commutateur le plus proche, l'interpréteur de protocole poursuit la recherche dans les commutateurs voisins jusqu'à deux

sauts (par défaut).

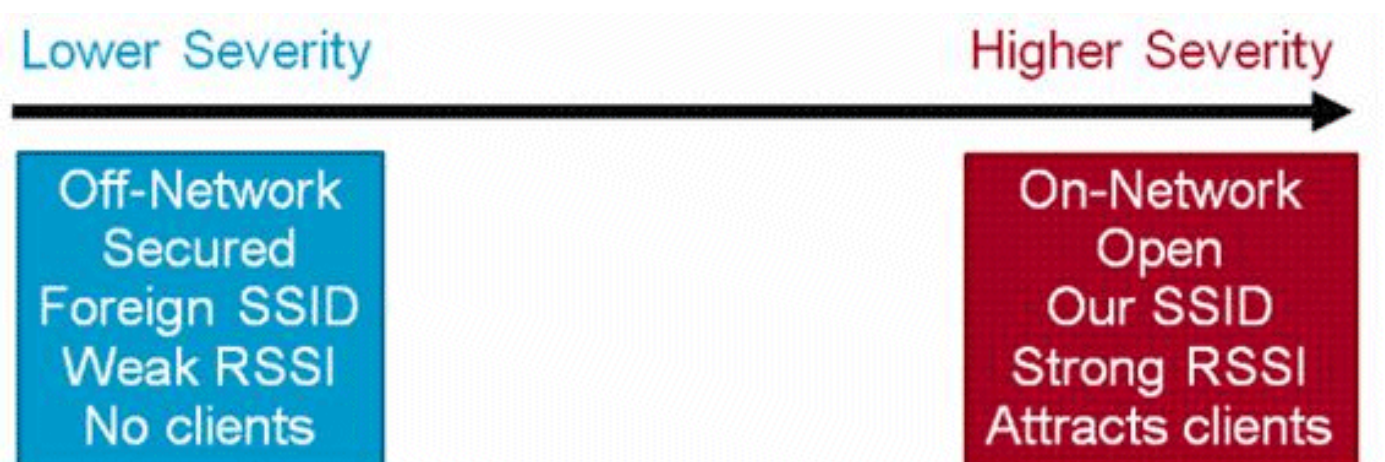
# Wired-Side Tracing Techniques

## 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>

## Classification des indésirables

Par défaut, tous les programmes indésirables détectés par le Cisco UWN sont considérés comme non classifiés. Comme l'illustre ce schéma, les routeurs peuvent être classés selon plusieurs critères, notamment RSSI, SSID, type de sécurité, réseau actif/inactif et nombre de clients :



Règles de classification non fiables



Les règles de classification des systèmes non fiables vous permettent de définir un ensemble de conditions marquant un système non fiable comme étant malveillant ou convivial. Ces règles sont configurées au niveau du PI ou du WLC, mais elles sont toujours exécutées sur le contrôleur à mesure que de nouveaux routeurs sont découverts.

Lisez le [document Classification des systèmes non fiables basée sur des règles dans les contrôleurs de réseau local sans fil \(WLC\) et l'infrastructure principale \(PI\)](#) pour plus d'informations sur les règles non fiables dans les WLC.

## Faits HA

Si vous déplacez manuellement un périphérique non autorisé vers l'état contenu (toute classe) ou convivial, ces informations sont stockées dans la mémoire flash Cisco WLC de secours ; cependant, la base de données n'est pas mise à jour. Lorsque la commutation haute disponibilité se produit, la liste non fiable de la mémoire flash Cisco WLC en veille est chargée.

Dans un scénario de haute disponibilité, si le niveau de sécurité de détection des systèmes non fiables est défini sur Élevé ou Critique, le compteur des systèmes non fiables sur le contrôleur de secours démarre uniquement après le temps de stabilisation de la détection des systèmes non fiables, qui est de 300 secondes. Par conséquent, les configurations actives sur le contrôleur de secours sont reflétées seulement après 300 secondes.

## Faits sur FlexConnect

Un point d'accès FlexConnect (avec la détection des indésirables activée) en mode connecté prend la liste de confinement du contrôleur. Si le contrôleur définit les paramètres auto-container SSID et auto-container adhoc, ces configurations sont définies sur tous les points d'accès FlexConnect en mode connecté et le point d'accès les stocke dans sa mémoire.

Lorsque le point d'accès FlexConnect passe en mode autonome, les tâches suivantes sont effectuées :

- Le confinement défini par le contrôleur se poursuit.
- Si le point d'accès FlexConnect détecte un point d'accès non autorisé qui a le même SSID que celui de l'infra-SSID (SSID configuré dans le contrôleur auquel le point d'accès FlexConnect est connecté), alors le confinement démarre si le SSID contenant automatiquement a été activé à partir du contrôleur avant de passer au mode autonome.
- Si le point d'accès FlexConnect détecte une anomalie adhoc, la contenance démarre si la contenance automatique adhoc a été activée à partir du contrôleur lorsqu'il était en mode connecté.

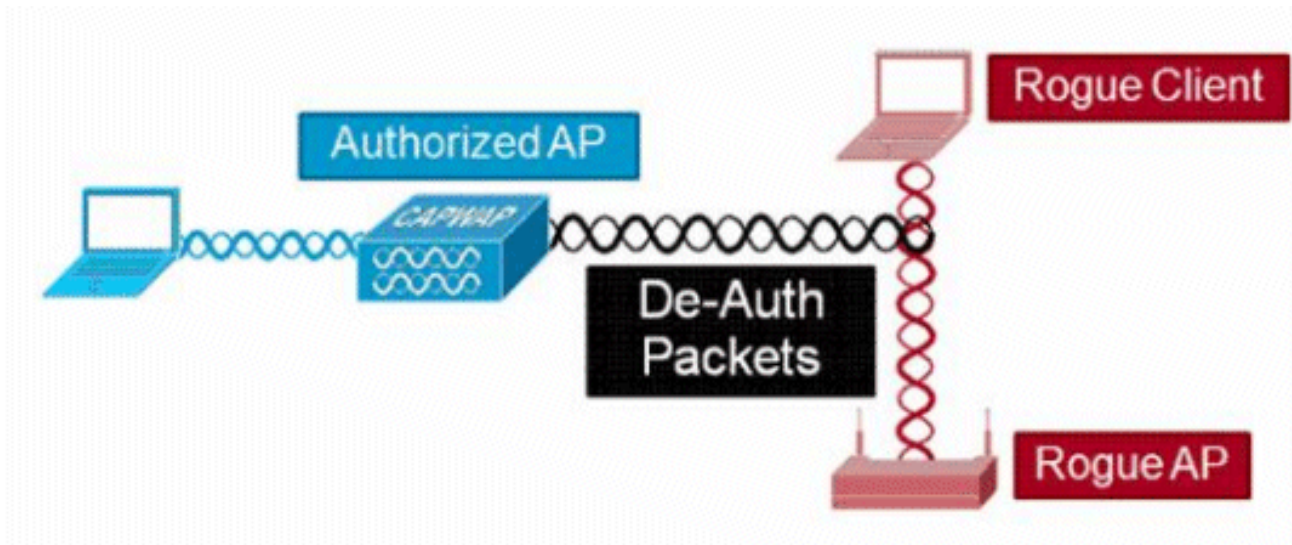
Lorsque le point d'accès autonome FlexConnect revient au mode connecté, les tâches suivantes sont effectuées :

- Tout le confinement est effacé.
- Le confinement initié par le contrôleur prend le relais.

## Atténuation des indésirables

### Confinement des systèmes non fiables

Le confinement est une méthode qui utilise des paquets en direct pour interrompre temporairement le service sur un périphérique non autorisé jusqu'à ce qu'il puisse être physiquement supprimé. Le confinement fonctionne avec l'usurpation de paquets de désauthentification avec l'adresse source usurpée du point d'accès non autorisé, de sorte que tous les clients associés sont rejetés.



### Détails du confinement des indésirables

Une contention initiée sur un AP non autorisé avec aucun client utilise uniquement des trames de désauthentification envoyées à l'adresse de diffusion :

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**

Un confinement initié sur un point d'accès non autorisé avec des clients utilise des trames de désauthentification envoyées à l'adresse de diffusion et à l'adresse du ou des clients :


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
Rogue AP	Rogue Client	6.0	30	802.11 Deauth

**Broadcast and Unicast Deauth frames**

Les paquets de confinement sont envoyés au niveau de puissance du point d'accès géré et au débit de données activé le plus faible.

Le confinement envoie au moins 2 paquets toutes les 100 ms :

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



**Note:** Un confinement effectué par des points d'accès en mode non surveillance est envoyé à un intervalle de 500 ms au lieu de l'intervalle de 100 ms utilisé par les points d'accès en mode surveillance.

- Un périphérique non autorisé individuel peut être contenu par 1 à 4 points d'accès gérés qui fonctionnent conjointement pour atténuer temporairement la menace.
- Le confinement peut être effectué par l'utilisation du mode local, du mode moniteur et du mode Flex-Connect (connecté) des points d'accès. Pour le mode local des points d'accès à connexion flexible, un maximum de trois périphériques indésirables par radio peut être contenu. Pour les points d'accès en mode surveillance, un maximum de six périphériques indésirables par radio peut être contenu.

## Confinement Automatique

En plus du lancement manuel du confinement sur un périphérique non autorisé via IP ou l'interface utilisateur graphique du WLC, il est également possible de lancer automatiquement le confinement dans certains scénarios. Cette configuration se trouve sous Général dans la section Stratégies non fiables de l'interface IP ou de contrôleur. Chacune de ces fonctions est désactivée par défaut et ne doit être activée que pour éliminer les menaces qui causent le plus de dommages.

- Non fiable sur câble : si un périphérique non fiable est identifié comme étant connecté au réseau câblé, il est automatiquement placé sous confinement.
- Utilisation de notre SSID : si un périphérique non autorisé utilise un SSID identique à celui configuré sur le contrôleur, il est automatiquement contenu. Cette fonctionnalité vise à traiter une attaque de pot de miel avant qu'elle ne cause des dommages.
- Client valide sur le point d'accès non autorisé : si un client répertorié dans le serveur Radius/AAA est associé à un périphérique non autorisé, la contention est lancée sur ce client uniquement, elle l'empêche de s'associer à un point d'accès non géré.
- Point d'accès non autorisé ad hoc : si un réseau ad hoc est détecté, il est automatiquement contenu.

## Mises en garde contre les systèmes non fiables

- Comme le confinement utilise une partie du temps radio du point d'accès géré pour envoyer les trames de désauthentification, les performances des clients de données et voix sont affectées négativement jusqu'à 20 %. Pour les clients de données, l'impact est une réduction



du débit. Pour les clients vocaux, le confinement peut entraîner des interruptions de conversations et une qualité vocale réduite.

- Le confinement peut avoir des implications juridiques lorsqu'il est lancé contre des réseaux voisins. Assurez-vous que le périphérique non autorisé se trouve sur votre réseau et qu'il présente un risque de sécurité avant de lancer le confinement.

## Port du commutateur fermé

Une fois qu'un port de commutateur est suivi par l'utilisation de SPT, il y a une option pour désactiver ce port dans PI. L'administrateur doit effectuer cet exercice manuellement. Une option est disponible pour activer le port de commutateur via IP si le voyant est physiquement supprimé du réseau.

## Configuration

### Configurer la détection des systèmes non fiables

La détection des systèmes non fiables est activée par défaut dans le contrôleur.

Afin de configurer diverses options, accédez à **Security > Wireless Protection Policies > Rogue Policies > General**. Par exemple :

Étape 1 : modification du délai d'attente pour les points d'accès non autorisés

Étape 2 : activation de la détection des réseaux indésirables ad hoc

The screenshot shows the Cisco WLC configuration page for 'Rogue Policies' under the 'Security' tab. The interface includes a navigation menu on the left and a main configuration area on the right. The 'Rogue Policies' section is expanded to show the 'General' configuration. The 'Rogue Detection Security Level' is set to 'Custom'. The 'Rogue Location Discovery Protocol' is set to 'All Aps'. The 'Expiration Timeout for Rogue AP and Rogue Client entries' is set to 3600 seconds. The 'Validate rogue clients against AAA' and 'Validate rogue AP against AAA' options are disabled. The 'Polling Interval' is set to 0 seconds. The 'Validate rogue clients against MSE' option is disabled. The 'Detect and report Ad-Hoc Networks' option is checked and enabled. The 'Rogue Detection Report Interval (10 to 300 Sec)' is set to 10. The 'Rogue Detection Minimum RSSI (-70 to -128)' is set to -128. The 'Rogue Detection Transient Interval (0, 120 to 1800 Sec)' is set to 600. The 'Rogue Client Threshold (0 to disable, 1 to 256)' is set to 0. The 'Rogue containment automatic rate selection' option is disabled. The 'Auto Contain' section is also visible, with 'Auto Containment Level' set to 'Auto' and several other options like 'Auto Containment only for Monitor mode APs', 'Auto Containment on FlexConnect Standalone', 'Rogue on Wire', 'Using our SSID', 'Valid client on Rogue AP', and 'AdHoc Rogue AP' all being disabled.

## À partir de la CLI :

```
(Cisco Controller) >config rogue ap timeout ?
```

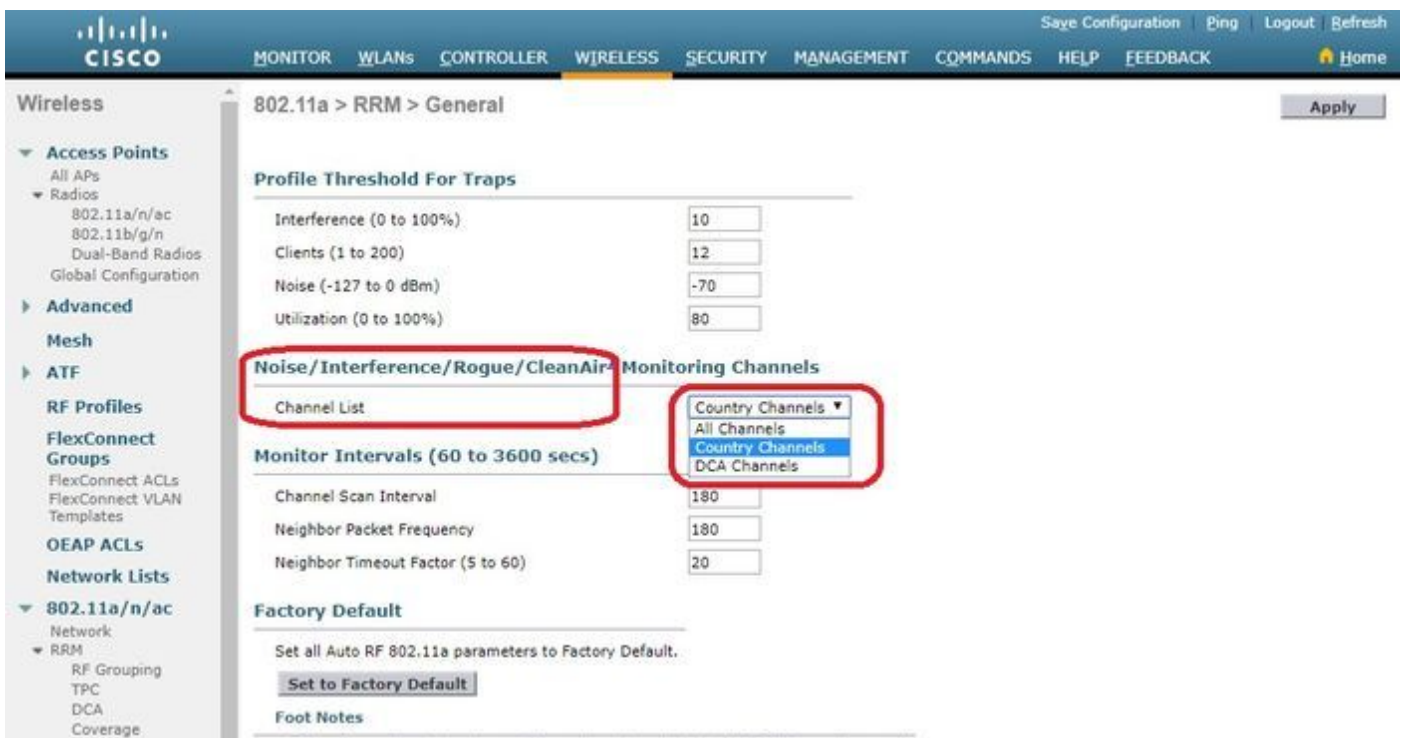
```
<seconds>      The number of seconds<240 - 3600> before rogue entries are flushed
```

```
(Cisco Controller) >config rogue adhoc enable/disable
```

## Configurer l'analyse des canaux pour la détection des indésirables

Pour un point d'accès en mode local/Flex-Connect/Monitor, il existe une option sous la configuration RRM qui permet à l'utilisateur de choisir quels canaux sont analysés pour détecter les routeurs. Cela dépend de la configuration, le point d'accès analyse tous les canaux/canaux de pays/canaux DCA à la recherche d'éléments indésirables.

Afin de configurer ceci à partir de l'interface graphique, naviguez à **Wireless > 802.11a/802.11b > RRM > General**, comme indiqué dans l'image.



## À partir de la CLI :

```
(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
```

## Configurer la classification non fiable

### Classification manuelle d'un point d'accès non autorisé

Afin de classer un AP indésirable comme sympathique, malveillant ou non classifié, naviguez

à **Monitor > Rogue > Unclassified APs**, et cliquez sur le nom de l'AP indésirable particulier. Sélectionnez l'option dans la liste déroulante, comme illustré dans l'image.

**Rogue AP Detail**

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** (selected from dropdown)  
 State: Malicious  
 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](#)

À partir de la CLI :

(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.

Afin de supprimer manuellement une entrée indésirable de la liste des indésirables, naviguez vers **Monitor > Rogue > Unclassified APs**, et cliquez sur **Remove**, comme indiqué dans l'image.

**Unclassified Rogue APs**

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

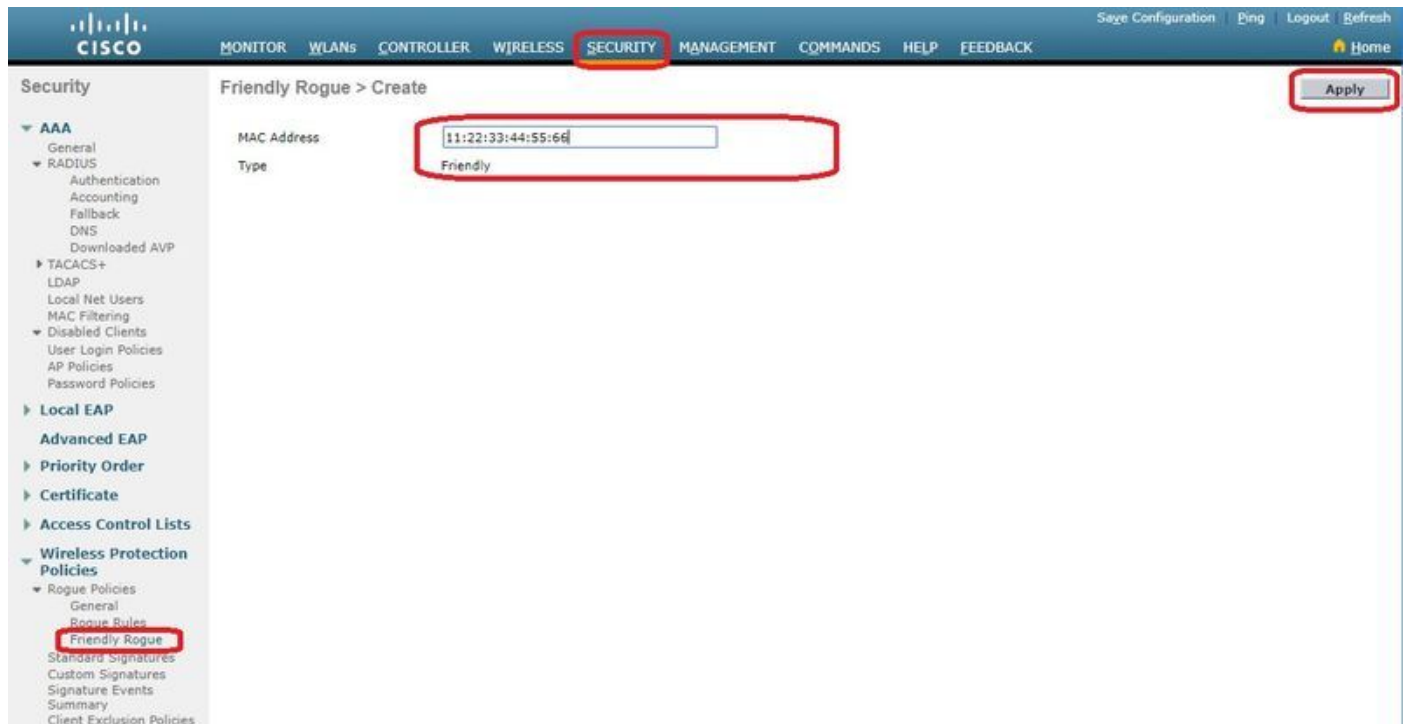
Remove  
Contain  
Move to Alert

MAC Address	SSID	Channel	# Detecting Radios	Number of Clients	Status
00:06:91:43:6d:e2	Cisco-17D90F4C	6	1	0	Alert
00:1a:7b:58:db:13	NUMERICABLE-29F3	6	1	0	Alert
00:22:ce:ff:38:a9	57afb7	11	1	0	Alert
00:22:ce:ff:47:5a	d9b9e9	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

Afin de configurer un point d'accès non autorisé comme point d'accès convivial, accédez à

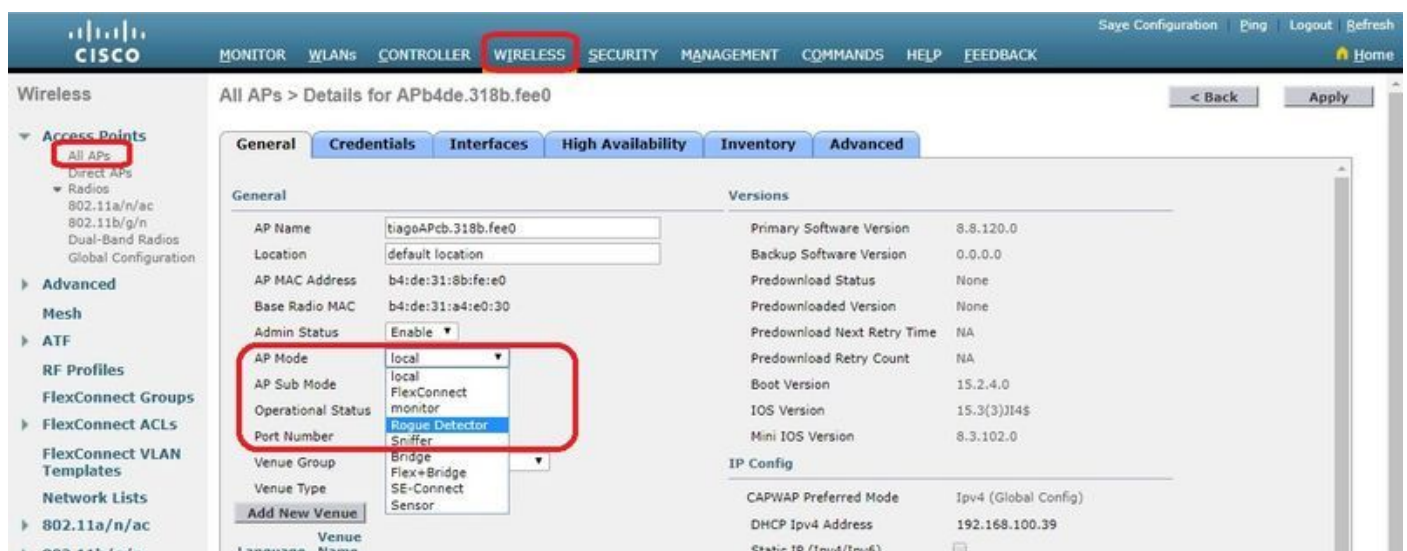
Security > Wireless Protection Policies > Rogue Policies > Friendly Rogues et ajoutez l'adresse MAC non autorisée.

Les entrées indésirables conviviales ajoutées peuvent être vérifiées à partir de Monitor > Rogues > Friendly Roguepage, comme illustré dans l'image.



## Configuration d'un point d'accès Rogue Detector

Afin de configurer le point d'accès en tant que détecteur de voyous via l'interface graphique utilisateur, naviguez vers Wireless > All APs. Choisissez le nom de l'AP et changez le mode AP comme indiqué dans l'image.



À partir de la CLI :

```
(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



## Configurer le port de commutation pour un point d'accès de détection des indésirables

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

**Note:** Le VLAN natif dans cette configuration est un VLAN qui a une connectivité IP au WLC.

## Configurer le protocole RLDP

Afin de configurer le RLDP dans l'interface graphique du contrôleur, naviguez vers **Security > Wireless Protection Policies > Rogue Policies > General**.

The screenshot shows the Cisco WLC configuration page for 'Rogue Policies' under the 'Security' tab. The 'Rogue Detection Security Level' is set to 'High'. The 'Rogue Location Discovery Protocol' is set to 'MonitorModeAps'. The 'Auto Contain' section is also visible, with 'Auto Containment Level' set to '1'.

Parameter	Value
Rogue Detection Security Level	High
Rogue Location Discovery Protocol	MonitorModeAps
Expiration Timeout for Rogue AP and Rogue Client entries	0
Validate rogue clients against AAA	Enabled
Validate rogue AP against AAA	Enabled
Polling Interval	0
Validate rogue clients against MSE	Enabled
Detect and report Ad-Hoc Networks	Enabled
Rogue Detection Report Interval (10 to 300 Sec)	10
Rogue Detection Minimum RSSI (-70 to -128)	-90
Rogue Detection Transient Interval (0, 120 to 1800 Sec)	0
Rogue Client Threshold (0 to disable, 1 to 256)	0
Rogue containment automatic rate selection	Enabled
Auto Containment Level	1
Auto Containment only for Monitor mode APs	Enabled
Auto Containment on FlexConnect Standalone	Enabled
Rogue on Wire	Enabled
Using our SSID	Enabled
Valid client on Rogue AP	Enabled
AdHoc Rogue AP	Enabled

**Points d'accès en mode surveillance** - Autorise uniquement les points d'accès en mode surveillance à participer au protocole RLDP.

**Tous les AP** - en mode Local/Flex-Connect/Monitor participent au processus RLDP.

**Disabled** : le protocole RLDP n'est pas déclenché automatiquement. Cependant, l'utilisateur peut déclencher manuellement le protocole RLDP pour une adresse MAC particulière via l'interface de ligne de commande.

**Note:** Le point d'accès en mode surveillance obtient la préférence sur le point d'accès local/Flex-Connect pour exécuter le protocole RLDP si les deux détectent un élément indésirable particulier au-delà de -85dbm RSSI.

À partir de la CLI :

(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

La planification RLDP et le déclenchement manuel ne peuvent être configurés qu'à partir d'une invite de commandes. Pour lancer manuellement le protocole RLDP :

(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).

Pour le calendrier du protocole RLDP :

(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.

Les tentatives RLDP peuvent être configurées avec la commande :

(Cisco Controller) >**config rogue ap rldp retries ?**

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

## Configuration de la réduction des indésirables

### Configurer le confinement manuel

Afin de contenir manuellement un AP non autorisé, naviguez vers **Monitor > Rogues > Unclassified**, comme indiqué dans l'image.



The screenshot displays the Cisco WLC Monitor interface. The 'MONITOR' tab is active. The main content area shows 'Rogue AP Detail' for a specific AP. Key details include:
 

- MAC Address: 00:06:91:53:3a:20
- Type: AP
- Is Rogue On Wired Network?: No
- First Time Reported On: Tue Jun 4 13:03:55 2019
- Last Time Reported On: Tue Jun 4 13:03:55 2019
- Class Type: Unclassified
- State: Alert
- Manually Contained: No

 The 'Update Status' dropdown is set to 'Contain'. Below this, there is a table titled 'APs that detected this Rogue' with columns: Base Radio MAC, AP Name, SSID, and RSSI. A dropdown menu for 'Choose Number of APs' is open, showing options from 1 to 4. The table shows one entry for AP 'tiagoAPcb.90E1.3DEC' with an RSSI of -128.

## À partir de la CLI :

(Cisco Controller) >**config rogue client** ?

aaa Configures to validate if a rogue client is a valid client which uses AAA/local database.  
 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].

**Note:** Un pirate particulier peut être contenu avec 1-4 AP. Par défaut, le contrôleur utilise un point d'accès pour contenir un client. Si deux AP sont capables de détecter un rogue particulier, l'AP avec le RSSI le plus élevé contient le client quel que soit le mode AP.

## Confinement Automatique

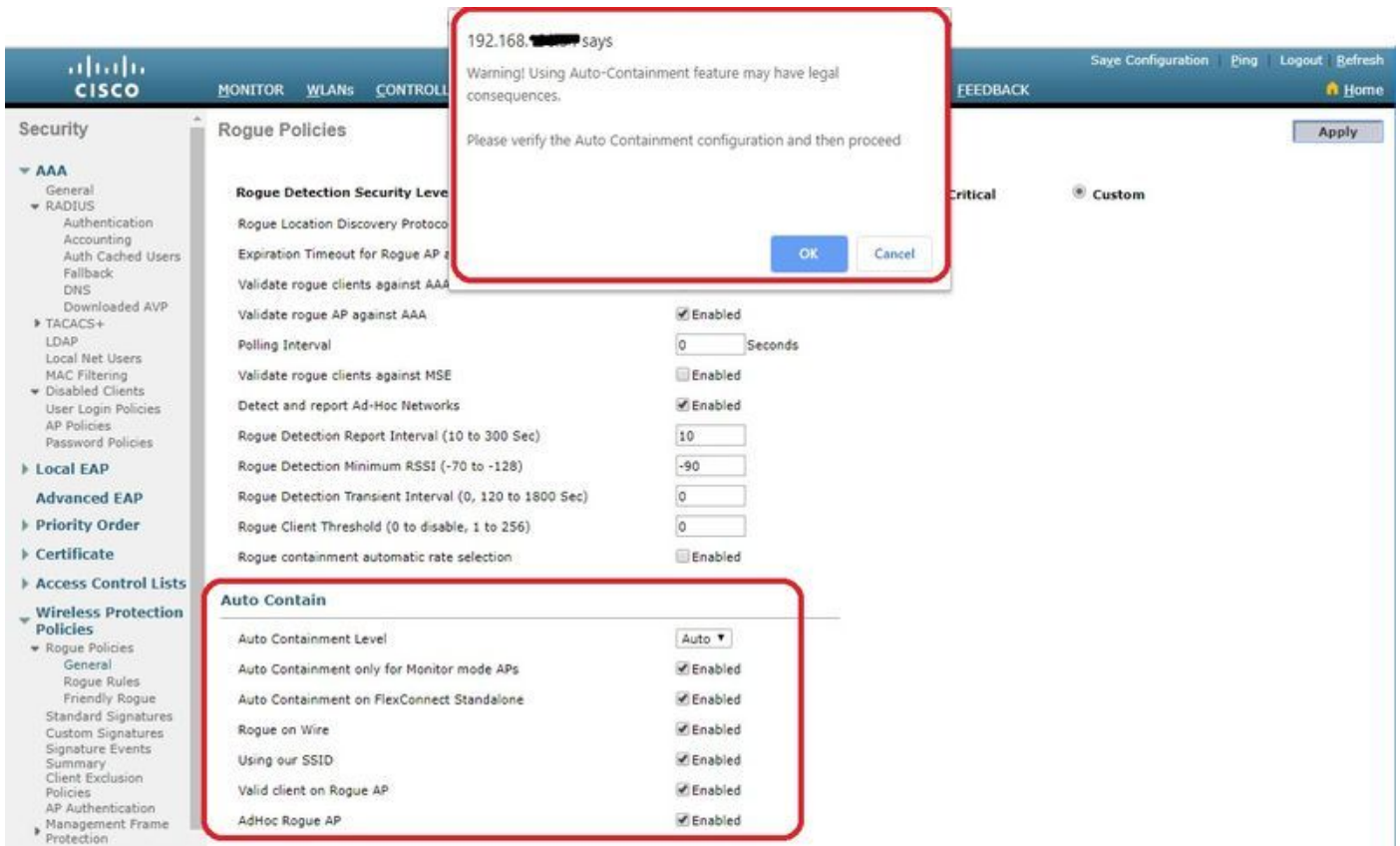
Pour configurer le confinement automatique, accédez à **Sécurité>Stratégies de protection sans fil>Stratégies non fiables>Général**, puis activez toutes les options applicables à votre réseau.

Si vous souhaitez que le WLC Cisco contienne automatiquement certains périphériques non autorisés, cochez ces cases. Sinon, ne cochez pas les cases, qui sont la valeur par défaut.

**Avertissement :** Lorsque vous activez l'un de ces paramètres, le message suivant s'affiche :  
 « L'utilisation de cette fonction a des conséquences juridiques. Voulez-vous continuer ? »  
 Les fréquences 2,4 et 5 GHz de la bande ISM (Industrial, Scientific, and Medical) sont ouvertes au public et peuvent être utilisées sans licence. Ainsi, le confinement des périphériques sur le réseau d'une autre partie peut avoir des conséquences juridiques.

Voici les paramètres de contenance automatique :

Paramètre	Description
Niveau de confinement automatique	Liste déroulante dans laquelle vous pouvez choisir le niveau de confinement automatique non autorisé de 1 à 4. Vous pouvez choisir jusqu'à quatre points d'accès pour le confinement automatique lorsqu'un non autorisé passe à l'état contenu via l'une des stratégies de confinement automatique. Vous pouvez également sélectionner Auto pour sélectionner automatiquement le nombre de points d'accès utilisés pour le confinement automatique. Le WLC Cisco choisit le nombre requis de points d'accès en fonction du RSSI pour un confinement efficace. La valeur RSSI associée à chaque niveau de confinement est la suivante : <ul style="list-style-type: none"><li>• 1 - 0 à -55 dBm</li><li>• 2 - -75 à -55 dBm</li><li>• 3 - -85 à -75 dBm</li><li>• 4 — Inférieur à -85 dBm</li></ul>
Confinement automatique uniquement pour les points d'accès en mode Surveillance	Cochez cette case pour activer les points d'accès en mode surveillance pour le confinement automatique. L'état par défaut est désactivé.
Confinement automatique sur FlexConnect autonome	Cochez cette case pour activer la contenance automatique sur les points d'accès FlexConnect en mode autonome. L'état par défaut est désactivé. Lorsque les points d'accès FlexConnect sont en mode autonome, vous pouvez uniquement activer les politiques de confinement automatique Utiliser notre SSID ou Point d'accès non autorisé ad hoc. Le confinement s'arrête après la reconnexion du point d'accès autonome au WLC Cisco.
Défaut sur fil	Cochez cette case pour que contienne automatiquement les éléments indésirables détectés sur le réseau câblé. L'état par défaut est désactivé.
Utiliser notre SSID	Cochez cette case pour que contienne automatiquement les éléments indésirables qui annoncent le SSID de votre réseau. Si vous ne sélectionnez pas ce paramètre, le WLC Cisco ne génère une alarme que lorsqu'un tel non autorisé est détecté. L'état par défaut est désactivé.
Client valide sur le point d'accès non autorisé	Cochez la case que vous activez pour contenir automatiquement un point d'accès non autorisé auquel des clients approuvés sont associés. Si vous ne sélectionnez pas ce paramètre, le WLC Cisco ne génère une alarme que lorsqu'un tel non autorisé est détecté. L'état par défaut est désactivé.
Point d'accès indésirable ad hoc	Cochez la case que vous activez pour contenir automatiquement les réseaux ad hoc qui sont détectés par le WLC Cisco. Si vous ne sélectionnez pas ce paramètre, le WLC Cisco génère une alarme uniquement lorsqu'un tel réseau est détecté. L'état par défaut est désactivé.



Cliquez sur Apply pour envoyer des données au WLC Cisco, mais les données ne sont pas conservées tout au long d'un cycle d'alimentation ; ces paramètres sont stockés temporairement dans la mémoire vive volatile.

À partir de la CLI :

```
(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
```

## Avec Prime Infrastructure

L'infrastructure Cisco Prime peut être utilisée pour configurer et surveiller un ou plusieurs contrôleurs et points d'accès associés. Cisco PI dispose d'outils pour faciliter la surveillance et le contrôle des systèmes de grande taille. Lorsque vous utilisez Cisco PI dans votre solution sans fil Cisco, les contrôleurs déterminent périodiquement l'emplacement du client, du point d'accès non autorisé, du client du point d'accès non autorisé, de l'étiquette d'identification par radiofréquence (RFID) et stockent les emplacements dans la base de données Cisco PI.

L'infrastructure Cisco Prime prend en charge la classification basée sur des règles et utilise les règles de classification configurées sur le contrôleur. Le contrôleur envoie des dérouterments à l'infrastructure Cisco Prime après ces événements :

- Si un point d'accès inconnu passe à l'état Convivial pour la première fois, le contrôleur envoie une interruption à l'infrastructure Cisco Prime uniquement si l'état non autorisé est Alerte. Il n'envoie pas de dérouterment si le domaine est **interne** ou **externe**.
- Si aroqueentry est supprimé après l'expiration du délai d'attente, le contrôleur envoie un dérouterment à Cisco Prime Infrastructure pour les points d'accès non autorisés classés comme **malveillants** (alerte, menace) ou **non classés** (alerte). Le contrôleur ne supprime pas les entrées avec ces états d'invité : **Contenu**, **Contenu en attente**, **interne** et **externe**.

## Vérification

Afin de trouver des détails indésirables dans un contrôleur dans l'interface graphique, naviguez à **Monitor > Rogues**, comme montré dans l'image.

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
9e: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

Dans cette page, différentes classifications sont disponibles pour les indésirables :

- Points d'accès conviviaux : points d'accès marqués comme étant conviviaux par l'administrateur.
- Points d'accès malveillants : points d'accès identifiés comme malveillants via le protocole RLDP ou le point d'accès de détection des indésirables.
- Points d'accès personnalisés : points d'accès classés comme personnalisés par des règles non fiables.
- Points d'accès non classés : par défaut, les points d'accès non classés sont affichés comme liste non classée dans le contrôleur.
- Clients non autorisés : clients connectés à des points d'accès non autorisés.
- Ordinateurs non autorisés - Ordinateurs non autorisés.
- Rogue AP ignore list - Comme indiqué par PI.

**Note:** Si le WLC et le point d'accès autonome sont gérés par le même PI, le WLC répertorie automatiquement ce point d'accès autonome dans la liste Ignorer les points d'accès indésirables. Aucune configuration supplémentaire n'est requise dans le WLC pour activer cette fonctionnalité.

Cliquez sur une entrée non autorisée particulière afin d'obtenir les détails de cette non autorisée. Voici un exemple d'un Rogue détecté sur un réseau câblé :

**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
- Cloud Services

**Rogue AP Detail**

MAC Address: 50:2f:a8:a2:0a:60

Type: AP

**Is Rogue On Wired Network?: Yes**

First Time Reported On: Mon Jun 3 14:12:54 2019

Last Time Reported On: Tue Jun 4 12:15:25 2019

Class Type: Malicious

**Classification Change By: Auto**

State: Threat

State Change By: Auto

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-Ambble	RSSI
00:27:e3:36:4d:a0	tiagoAPcb.98E1.3DEC	butterfly	1	20	802.11n2.4G	WPA2/FT	Long	-63

[Clients associated to this Rogue AP](#)

À partir de la CLI :

(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	#Rogue	#Highest	RSSI	#RSSI
#Channel	#Second Highest	#RSSI	#Channel	Aps	Clients	det-Ap	
RSSI	Det-Ap						
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
00:27:e3:36:4d:a0			-37	40			
00:a3:8e:db:01:b1	Unclassified	Alert	2	0	00:27:e3:36:4d:a0	-28	40
00:27:e3:36:4d:a0			-36	40			
00:a3:8e:db:01:b2	Unclassified	Alert	2	0	00:27:e3:36:4d:a0	-28	40

```

00:27:e3:36:4d:a0 -37      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

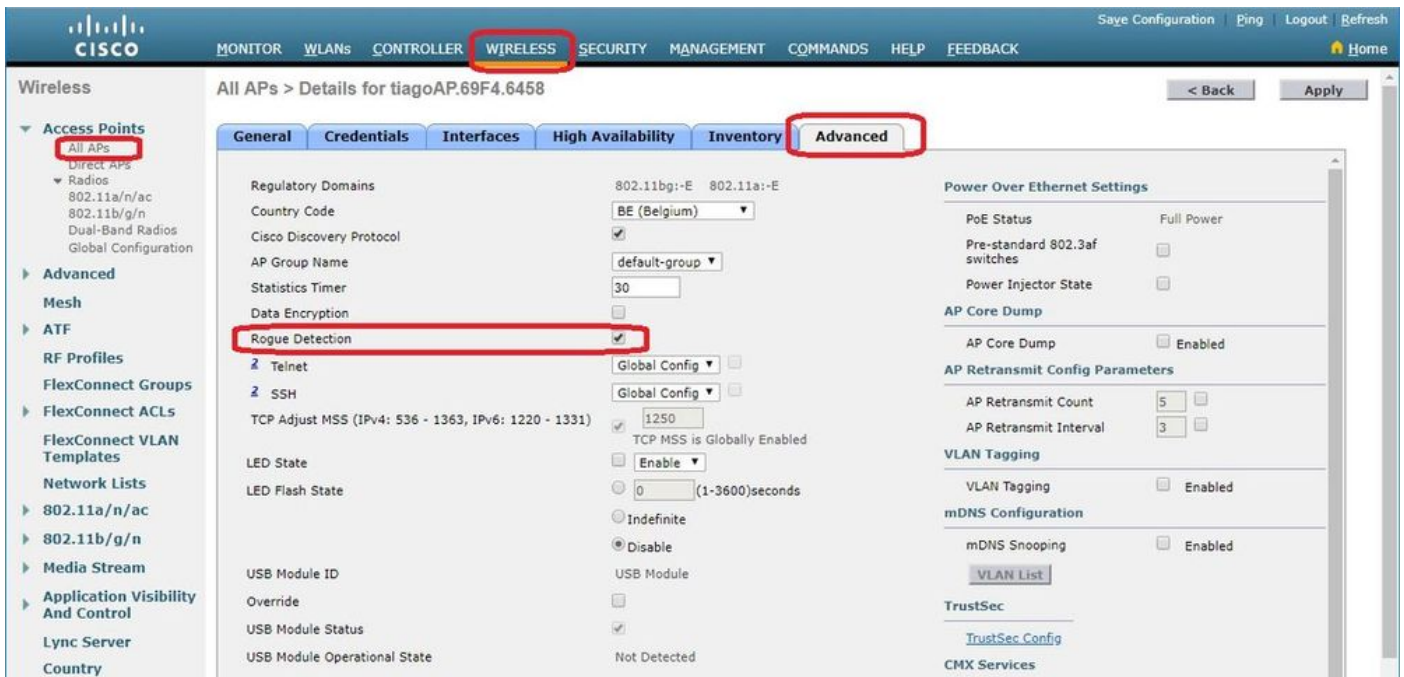
```

## Dépannage

### Si Le Rogue N'Est Pas Détecté

Vérifiez que la détection des systèmes non fiables est activée sur le point d'accès. Sur l'interface utilisateur graphique :





Dans la CLI :

```
(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
[...]
```

La détection des indésirables peut être activée sur un AP avec cette commande :

```
(Cisco Controller) >config rogue detection enable ?
all Applies the configuration to all connected APs.
<Cisco AP> Enter the name of the Cisco AP.
```

Un point d'accès en mode local analyse uniquement les canaux de pays/canaux DCA et dépend de la configuration. Si le voyant est dans un autre canal, le contrôleur ne peut pas identifier le

voyant si vous n'avez pas de points d'accès en mode surveillance dans le réseau. Pour vérifier, émettez la commande suivante :

```
(Cisco Controlller) >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
```

- Le point d'accès non autorisé ne diffuse pas le SSID.
- Assurez-vous que l'adresse MAC du point d'accès non autorisé n'est pas ajoutée à la liste des points d'accès non autorisés ou autorisée via IP.
- Les balises du point d'accès non autorisé ne sont pas accessibles au point d'accès qui a détecté des routeurs. Ceci peut être vérifié par la capture des paquets avec un analyseur proche du voyant de détection AP.
- Un point d'accès en mode local peut prendre jusqu'à 9 minutes pour détecter un élément indésirable (3 cycles 180x3).
- Les points d'accès Cisco ne sont pas en mesure de détecter les périphériques indésirables sur des fréquences telles que le canal de sécurité publique (4,9 GHz).
- Les points d'accès Cisco ne sont pas en mesure de détecter les routeurs qui fonctionnent sur FHSS (Frequency Hopping Spread Spectrum).

## Débogages utiles

```
(Cisco Controlller) >debug client
```

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

```
(Cisco Controlller) >debug client 50:2f:a8:a2:0a:60
```

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

```
*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, snr 39 wepMode 81 wpaMode 86, detectinglratypes :20
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559724417.
Detecting lrads: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 SYNC for Channel (new/old : 1/0) or
channel width (new/old :0/0) change detected on Detecting lrads: 00:27:e3:36:4d:a0
*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, snr 39
*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 lradsInfo->containSlotId = 2
ReceiveSlotId = 0 ReceiveBandId = 0
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue before Rule Classification : Class
malicious, Change by Auto State Threat Change by Auto

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue doesnt qualify for rule
classification : Class malicious, Change by Auto State Threat Change by Auto

*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=buterfly

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue AP: 50:2f:a8:a2:0a:60 autocontain
= 2 Mode = 7

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Checking Impersonation source
50:2f:a8:a2:0a:60 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 7, apAuthEnabled on mac 0,
ptype 318505456 mfp_supported 1
*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 Impersonation 0 ids flags 2

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

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

```
(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
:FCW2245M09Y Hostname tiagoWLCcb
*iappSocketTask: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 Posting Rogue AP Iapp Report from AP for
processing Payload version:cl, slot:0 , Total Entries:5, num entries this packet:5 Entry index
:0, pakLen:285

*apfRogueTask_2: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 fakeAp check: slot=0, entryIndex=0,
(Radio_upTime-now)=152838
*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 b0:72:bf:93:e0:d7 channel 1 rssi -59 ssid SMA1930072865
*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 50:2f:a8:a2:0a:60 channel 1 rssi -63 ssid buterfly
*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 00:a3:8e:db:01:a1 channel 13 rssi -16 ssid
*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 a4:c3:f0:cf:db:18 channel 40 rssi -26 ssid blizzard
*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 -28, snr 61 wepMode 81 wpaMode 82, detectinglratypes :30
*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 00:a3:8e:db:01:b2 channel 40 rssi -28 ssid
*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 Detecting lrads: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check: knownApCount=0,
totalNumOfRogueEntries=5, #entriesThisPkt=5, #totalEntries=5
*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 -16, snr 76 wepMode 81 wpaMode 82, detectinglratypes :28
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check: avgNumOfRogues[0]/10=4,
rogueAlarmInitiated[0]=0
```

\*apfRogueTask\_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 SYNC for Channel (new/old : 40/0) or channel width (new/old :0/0) change detected on Detecting lrad: 00:27:e3:36:4d:a0

\*apfRogueTask\_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue SSID timestmap expired. last update at 0 Detecting lrad: 00:27:e3:36:4d:a0

\*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 width (new/old :0/0) change detected on Detecting lrad: 00:27:e3:36:4d:a0

\*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, snr 61

\*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, snr 76

\*apfRogueTask\_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 RadioType: 3 lradInfo->containSlotId = 1 ReceiveSlotId = 0 ReceiveBandId = 1

\*apfRogueTask\_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue before Rule Classification : Class unclassified, Change by Default State Alert Change by Default

\*apfRogueTask\_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Created rogue client table for Rogue AP at 0xffff0617238

\*apfRogueTask\_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue is Rule candidate for : Class Change by Default State Change by Default

\*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 table

\*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 in AP list or neighbor, known or Mobility group AP lists

\*apfRogueTask\_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue After Rule Classification : Class unclassified, Change by Default State Alert Change by Default

\*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 for rogue AP b0:72:bf:93:e0:d7

\*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:93:e0:d7

\*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 Mode = 2

\*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 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 2, apAuthEnabled on mac 0, ptype -155740480 mfp\_supported 1

\*apfRogueTask\_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 RadioType: 3 lradInfo->containSlotId = 2 ReceiveSlotId = 0 ReceiveBandId = 0

\*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 -59, snr 36 wepMode 81 wpaMode 83, detectinglradtypes :20

\*apfRogueTask\_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue is Rule candidate for : Class Change by Default State Change by Default

\*apfRogueTask\_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Send Rogue Info Notificaiton for AP report 00:27:e3:36:4d:a0 Rogue ssid change from to SMA1930072865

\*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. Detecting lrad: 00:27:e3:36:4d:a0

\*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 unclassified, Change by Default State Alert Change by Default

\*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, snr 36

\*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 ReceiveSlotId = 0 ReceiveBandId = 0

\*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 unconfigured, Change by Default State Pending Change by Default

\*apfRogueTask\_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue AP: 00:a3:8e:db:01:a1 autocontain = 2 Mode = 2

\*apfRogueTask\_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue state is pending or lrad, cannot apply rogue rule

\*apfRogueTask\_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue doesnt qualify for rule classification : Class unconfigured, Change by Default State Pending Change by Default

\*apfRogueTask\_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Checking Impersonation source 00:a3:8e:db:01:a1 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 2, apAuthEnabled on mac 0, ptype -155740480 mfp\_supported 1

\*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 Impersonation 0 ids flags 6

\*apfRogueTask\_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Checking Impersonation source b0:72:bf:93:e0:d7 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 1, apAuthEnabled on mac 0, ptype 318505456 mfp\_supported 1

\*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 Impersonation 0 ids flags 2

\*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 -26, snr 61 wepMode 81 wpaMode 82, detectinglradtypes :32

\*apfRogueTask\_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue SSID timestmap set to 1559723997. Detecting lrad: 00:27:e3:36:4d:a0

\*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 -63, snr 5 wepMode 81 wpaMode 86, detectinglradtypes :20

\*apfRogueTask\_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 SYNC for Channel (new/old : 40/0) or

channel width (new/old :0/0) change detected on Detecting lrad: 00:27:e3:36:4d:a0  
\*apfRogueTask\_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559723997.  
Detecting lrad: 00:27:e3:36:4d:a0  
\*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 width (new/old :0/0) change detected on Detecting lrad: 00:27:e3:36:4d:a0  
\*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, snr 61  
\*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, snr 5  
\*apfRogueTask\_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 RadioType: 3 lradInfo->containSlotId = 1  
ReceiveSlotId = 0 ReceiveBandId = 1  
  
\*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  
ReceiveSlotId = 0 ReceiveBandId = 0  
  
\*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  
malicious, Change by Auto State Threat Change by Auto  
  
\*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=blizzard  
  
\*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 Mode = 7  
  
\*apfRogueTask\_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 This rogue does not use my ssid. Rogue  
ssid=buterfly  
  
\*apfRogueTask\_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue AP: 50:2f:a8:a2:0a:60 autocontain  
= 2 Mode = 7  
  
\*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 Impersonation 0 ids flags 2  
  
\*apfRogueTask\_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Checking Impersonation source  
50:2f:a8:a2:0a:60 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 7, apAuthEnabled on mac 0,  
ptype 318505456 mfp\_supported 1  
\*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 Impersonation 0 ids flags 2  
  
\*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: buterfly



```

*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 50
*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, snr 50
*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, snr 43
*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 32
*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, snr 32
*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 table
*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 in AP list or neighbor, known or Mobility group AP lists
*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:93:e0:d7
*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
0xffff0617238
*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

```

## Journaux des interruptions attendus

Une fois qu'un programme non autorisé est détecté/supprimé de la liste :

```

mer juin 5 Client non autorisé : b4:c0:f5:2b:4f:90 est détecté par 1 APs Rogue Client Bssid:
0 09:01:57 a6:b1:e9:f0:e8:41, État : Alerte, dernière détection AP :00:27:e3:36:4d:a0 Rogue Client gate
2019 mac 00:00:00:02:02:02.
mer juin 5 Point d'accès non autorisé : 9c:97:26:61:d2:79 supprimé du MAC radio de base :
1 09:00:39 00:27:e3:36:4d:a0 Numéro d'interface : 0(802.11n(2,4 GHz))
2019
mer juin 5 Point d'accès non autorisé : 7c:b7:33:c0:51:14 supprimé du MAC radio de base :
2 08:53:39 00:27:e3:36:4d:a0 Numéro d'interface : 0(802.11n(2,4 GHz))
2019
mer juin 5 Client non autorisé : fc:3f:7c:5f:b1:1b est détecté par 1 point d'accès Rogue Client Bssid:
3 08:52:27 50:2f:a8:a2:0a:60, État : Alerte, dernière détection AP :00:27:e3:36:4d:a0 Rogue Client gate
2019 mac 00:26:44:73:c5:1d.
mer juin 5 Point d'accès non autorisé : d4:28:d5:da:e0:d4 supprimé du MAC radio de base :
4 08:52:17 00:27:e3:36:4d:a0 Numéro d'interface : 0(802.11n(2,4 GHz))

```

## Recommandations

1. Configurez l'analyse des canaux sur tous les canaux si vous suspectez des problèmes potentiels sur votre réseau.
2. Le nombre et l'emplacement des points d'accès détecteurs de systèmes non fiables peuvent varier d'un par étage à un par bâtiment et dépendent de la disposition du réseau câblé. Il est conseillé d'avoir au moins un détecteur de voyous AP dans chaque étage d'un bâtiment. Comme un point d'accès détecteur de systèmes non autorisés nécessite une agrégation vers tous les domaines de diffusion réseau de couche 2 à surveiller, le positionnement dépend de la disposition logique du réseau.

## Si le non autorisé n'est pas classé

Vérifiez que les règles non autorisées sont correctement configurées.

## Débugages utiles

```
(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
:FCW2245M09Y Hostname tiagoWLCcb
```

```
(Cisco Controller) >
```

```
*apfRogueTask_1: Jun 05 09:12:57.135: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154623, wep=1, ssid=blizzard slotId = 0
channel = 13 snr = 76 dot11physupport =
```

```
*apfRogueTask_3: Jun 05 09:12:57.135: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154683, wep=1, ssid= slotId = 0 channel = 13
snr = 77 dot11physupport = 3
```

```
*apfRogueTask_1: Jun 05 09:12:57.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=5790, wep=1, ssid=NOWO-A2121 slotId = 0
channel = 1 snr = 4 dot11physupport = 3
```

```
*apfRogueTask_1: Jun 05 09:13:27.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=5820, wep=1, ssid=NOWO-A2121 slotId = 0
channel = 1 snr = 4 dot11physupport = 3
```

```
*apfRogueTask_3: Jun 05 09:13:27.135: 50:2f:a8:a2:0d:40 Rogue Rule Classify Params: rssi=-62,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154353, wep=1, ssid=buterfly slotId = 0
channel = 11 snr = 30 dot11physupport =
```

```
*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,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154713, wep=1, ssid= slotId = 0 channel = 13
snr = 77 dot11physupport = 3
```

```
*apfRogueTask_1: Jun 05 09:13:57.136: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154683, wep=1, ssid=blizzard slotId = 0
channel = 13 snr = 76 dot11physupport =
```

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

```
*apfRogueTask_3: Jun 05 09:13:57.136: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154743, wep=1, ssid= slotId = 0 channel = 13
snr = 77 dot11physupport = 3
```

## Recommandations

Si vous avez des entrées non autorisées connues, ajoutez-les dans la liste conviviale ou activez la validation avec AAA et assurez-vous que les entrées de client connues sont présentes dans la base de données AAA (Authentication, Authorization and Accounting).

## Le protocole RLDP ne localise pas les indésirables

- Si le voyant est dans le canal DFS, le protocole RLDP ne fonctionne pas.
- Le protocole RLDP fonctionne uniquement si le réseau local sans fil non autorisé est ouvert et que le protocole DHCP est disponible.
- Si le point d'accès en mode local sert le client dans le canal DFS, il ne participe pas au processus RLDP.
- Le protocole RLDP n'est pas pris en charge sur les AP des modèles 1800i, 1810, OEAP, 1810W, 1815, 1830, 1850, 2800 et 3800.

## Débogages utiles

```
(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 APs
```

```
*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-AP1852I-E-K9 *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, channel = 1

*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 TRUE
*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 State(2)

*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 State(2)

*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

```

## Recommandations

1. Lancez manuellement le protocole RLDP sur les entrées non autorisées suspectes.
2. Planifiez régulièrement le protocole RLDP.
3. Le protocole RLDP peut être déployé sur des points d'accès locaux ou en mode surveillance. Pour la plupart des déploiements évolutifs et pour éliminer tout impact sur le service client, le protocole RLDP doit être déployé sur les points d'accès en mode surveillance lorsque cela est possible. Cependant, cette recommandation exige qu'une superposition de point d'accès en mode surveillance soit déployée avec un rapport typique de 1 point d'accès en mode surveillance pour 5 points d'accès en mode local. Les points d'accès en mode de surveillance WIPS adaptatif peuvent également être utilisés pour cette tâche.

## Point d'accès Rogue Detector

L'entrée de voyous dans un détecteur de voyous peut être vue avec cette commande dans la console AP. Pour les systèmes filaires non autorisés, l'indicateur se déplace pour définir l'état.

```

tiagoAP.6d09.eff0#show capwap rm rogue detector
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

## Commandes Debug utiles dans une console AP

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.alcc.0e9e
*Jun 05 08:38:19.325: ROGUE_DET: Got wired mac 001d.alcc.0e9e
*Jun 05 08:39:19.323: ROGUE_DET: Got ARP src 001d.alcc.0e9e
*Jun 05 08:39:19.324: ROGUE_DET: Got wired mac 001d.alcc.0e9e
```

## Confinement des systèmes non fiables

### Débugages attendus

```
*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, snr 59
*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 table
*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 in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue in same state as before : 6
ContainmentLevel : 4 level 4

*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
ReceiveSlotId = 1 ReceiveBandId = 1

*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 : Class malicious, Change by Auto State Contained Change by Auto
```

\*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 lineNumber : 8225 apfRogueManualContained : 0 function :  
apfUpdateRogueContainmentState

\*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 1 for detecting lrad 00:27:e3:36:4d:a0.

\*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 totClientsDetected = 2

\*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 totClientsDetected = 2

\*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 totClientsDetected = 1

\*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. Containment mode 1

\*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. Containment mode 1

\*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. Containment mode 1

\*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 detected by b4:de:31:a4:e0:30, FailCnt 0, mode 6, apAuthEnabled on mac 0, ptype 318505456 mfp\_supported 1

\*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 Impersonation 0 ids flags 3

## Recommandations

1. Le point d'accès en mode local/Flex-Connect peut contenir 3 périphériques à la fois par radio et le point d'accès en mode surveillance peut contenir 6 périphériques par radio. Par conséquent, assurez-vous que le point d'accès ne contient pas déjà le nombre maximal de périphériques autorisés. Dans ce scénario, le client est dans un état de confinement en attente.
2. Vérifier les règles de confinement automatique.

## Conclusion

La détection et le confinement des systèmes non fiables au sein de la solution de contrôleur centralisé Cisco constituent la méthode la plus efficace et la moins intrusive du secteur. La

flexibilité offerte à l'administrateur réseau permet un ajustement plus personnalisé qui peut s'adapter à toutes les exigences du réseau.

## Informations connexes

- [Guide de configuration du contrôleur sans fil Cisco, version 8.8 - Gestion des systèmes non fiables](#)
- [Meilleures pratiques de configuration du contrôleur LAN sans fil \(WLC\) Cisco](#)
- [Guide de déploiement du WLC 3504 version 8.5](#)
- [Guide de déploiement du contrôleur LAN sans fil Cisco 5520](#)
- [Notes de version pour les contrôleurs sans fil et les points d'accès légers Cisco, Cisco Wireless version 8.8.120.0](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.