Erkennung und Unterbindung von nicht autorisierten Access Points in einem einheitlichen Wireless-Netzwerk

Inhalt

Einleitung

Dieses Dokument beschreibt die Erkennung und Eindämmung von nicht autorisierten Access Points in Cisco Wireless-Netzwerken.

Drahtlose Netzwerke erweitern kabelgebundene Netzwerke und steigern die Mitarbeiterproduktivität und den Zugriff auf Informationen. Ein nicht autorisiertes Wireless-Netzwerk stellt jedoch eine weitere Sicherheitsbedrohung dar. Die Port-Sicherheit in kabelgebundenen Netzwerken wird nicht ausreichend berücksichtigt, und Wireless-Netzwerke sind eine einfache Erweiterung von kabelgebundenen Netzwerken. Aus diesem Grund kann ein Mitarbeiter, der seinen eigenen Access Point (von Cisco oder einem Drittanbieter) in eine gut gesicherte Wireless- oder kabelgebundene Infrastruktur einbringt und nicht autorisierten Benutzern Zugriff auf dieses ansonsten gesicherte Netzwerk gewährt, leicht ein sicheres Netzwerk gefährden.

Die Erkennung nicht autorisierter APs ermöglicht dem Netzwerkadministrator die Überwachung und Beseitigung dieser Sicherheitsbedenken. Die Cisco Unified Network-Architektur bietet Verfahren zur Erkennung von nicht autorisierten Access Points und ermöglicht so eine umfassende Lösung zur Identifizierung und Eindämmung von nicht autorisierten Access Points, ohne dass kostspielige und schwer zu rechtfertigende Overlay-Netzwerke und -Tools erforderlich sind.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Wireless LAN Controller
- Cisco Prime-Infrastruktur.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Unified Wireless LAN Controller (Serien 5520, 8540 und 3504) mit Version 8.8.120.0
- Wave 2 APs der Serien 1832, 1852, 2802 und 3802
- Serie Wave 1 APs 3700, 2700 und 1700.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Übersicht über nicht autorisierte APs

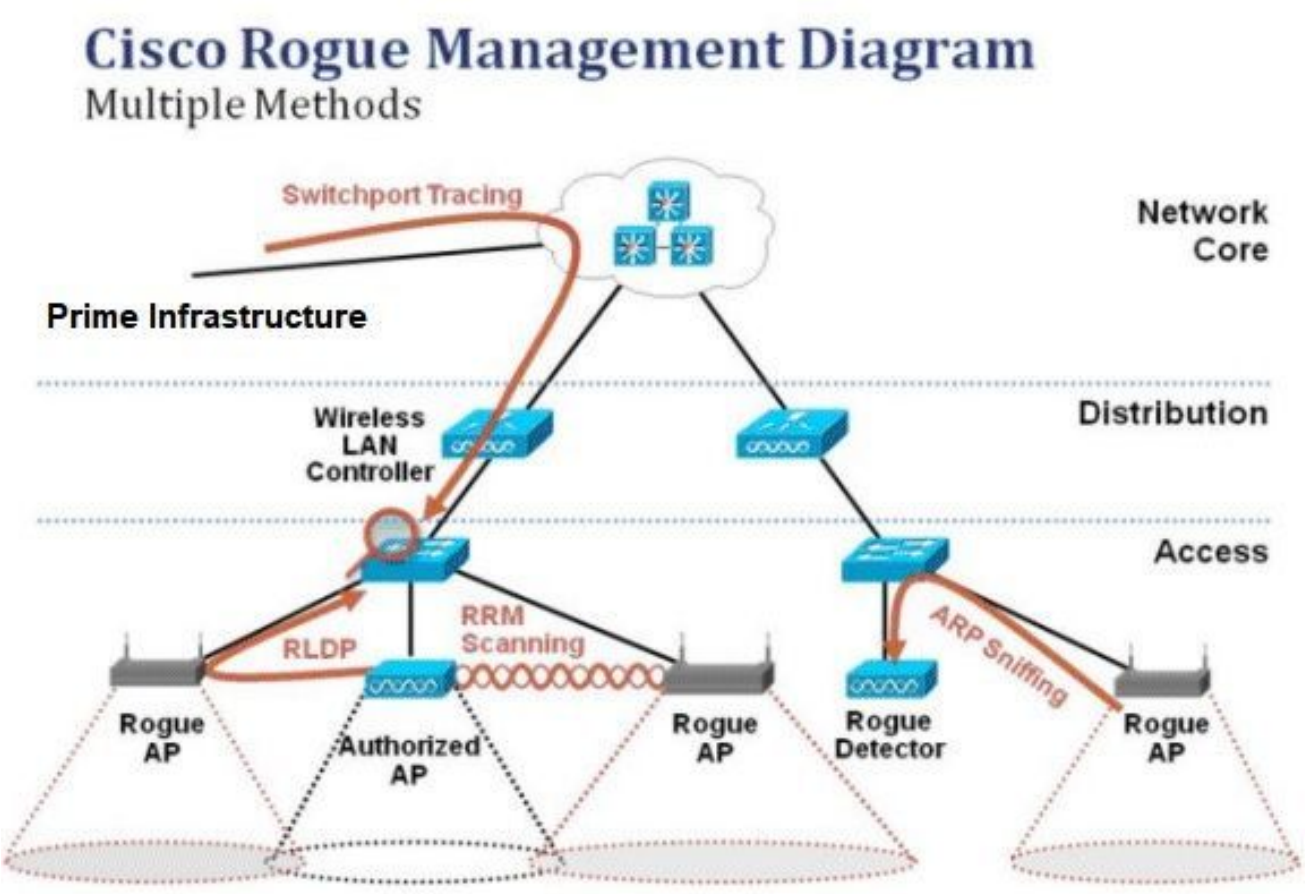
Jedes Gerät, das Ihr Spektrum teilt und nicht von Ihnen verwaltet wird, kann als unberechtigtes Gerät angesehen werden. Ein unberechtigtes Gerät wird in folgenden Szenarien gefährlich:

- Bei der Konfiguration zur Verwendung desselben Service Set Identifier (SSID) wie Ihr Netzwerk (Honeypot).
- Wenn sie im kabelgebundenen Netzwerk erkannt wird.
- Ad-hoc-Schurken.
- Einrichtung durch einen Außenstehenden, meistens mit böswilliger Absicht.

Die Best Practice besteht darin, nicht autorisierte Erkennungsmechanismen zu verwenden, um Sicherheitsrisiken zu minimieren, beispielsweise in einer Unternehmensumgebung. Es gibt jedoch bestimmte Szenarien, in denen eine Erkennung von unberechtigten Geräten nicht erforderlich ist, z. B. bei der Bereitstellung von Office Extend Access Points (OEAP) im gesamten Stadtgebiet und im Außenbereich. Mit der Verwendung von Outdoor-Mesh-APs zur Erkennung von unberechtigten Geräten wäre wenig Wert, während es Ressourcen für die Analyse nutzen würde. Und schließlich ist es entscheidend, eine unkontrollierte Autoeindämmung zu evaluieren (oder gänzlich zu vermeiden), da es potenzielle rechtliche Probleme und Verbindlichkeiten gibt, wenn diese automatisch funktionieren.

Die Cisco Unified Wireless Network (UWN)-Lösung besteht im Wesentlichen aus drei Phasen für das Management nicht autorisierter Geräte:

- Erkennung - Ein RRM-Scan (Radio Resource Management) erkennt nicht autorisierte Geräte.
- Klassifizierung - Mithilfe von RLDP (Rogue Location Discovery Protocol), RLDP (Rogue Detectors) (nur Wave 1-APs) und Switch-Port-Traces wird ermittelt, ob das unautorisierte Gerät mit dem kabelgebundenen Netzwerk verbunden ist. Regeln für die nicht autorisierte Klassifizierung helfen auch dabei, unberechtigte Benutzer anhand ihrer Merkmale in bestimmte Kategorien einzuteilen.
- Eindämmung: Die Abschaltung von Switch-Ports, nicht autorisierte Standorte und die Blockierung von nicht autorisierten Geräten werden eingesetzt, um die physische Position des Geräts zu ermitteln und die Bedrohung durch nicht autorisierte Geräte zu neutralisieren.

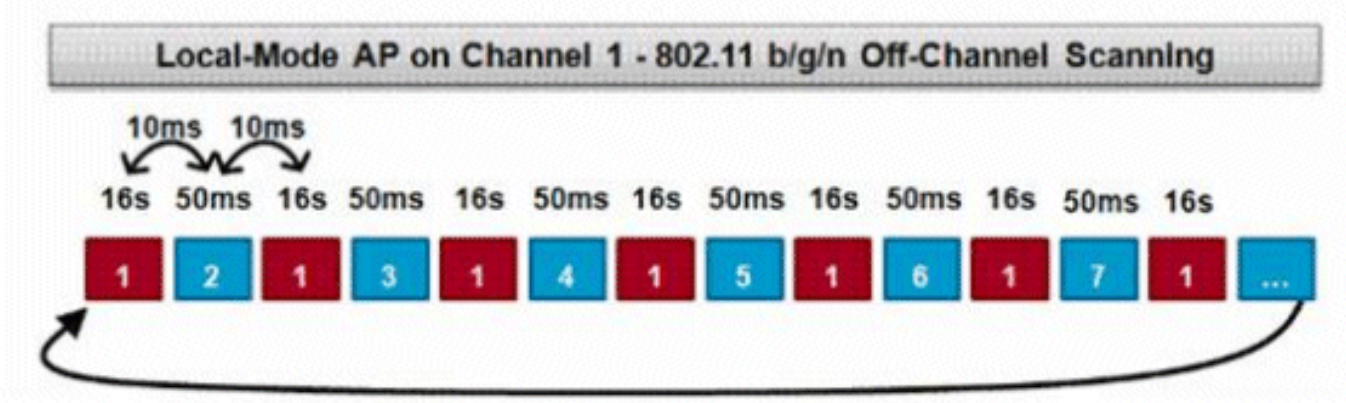


Erkennung nicht autorisierter APs

Ein unberechtigtes Gerät ist praktisch jedes Gerät, das Ihr Spektrum teilt, aber nicht unter Ihrer Kontrolle ist. Dazu gehören nicht autorisierte Access Points, Wireless-Router, nicht autorisierte Clients und nicht autorisierte Ad-hoc-Netzwerke. Das Cisco UWN verwendet eine Reihe von Methoden zur Erkennung von Wi-Fi-basierten nicht autorisierten Geräten, z. B. einen Off-Channel-Scan und Funktionen für einen dedizierten Überwachungsmodus. Cisco Spectrum Expert kann auch verwendet werden, um nicht autorisierte Geräte zu identifizieren, die nicht auf dem 802.11-Protokoll basieren, z. B. Bluetooth-Bridges.

Scan außerhalb des Kanals

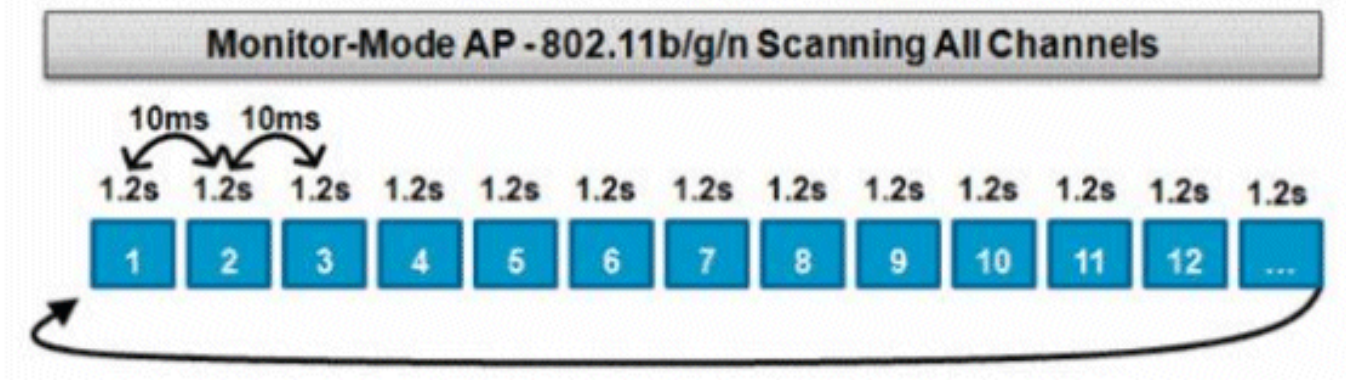
Dieser Vorgang wird von Zugangspunkten im lokalen und Flex-Connect-Modus (im verbundenen Modus) durchgeführt. Dabei wird eine Zeitschlitztechnik verwendet, die unter Verwendung derselben Funkeinheit einen Client-Dienst- und Kanalscan ermöglicht. Wenn der Kanal für einen Zeitraum von 50 ms alle 16 Sekunden ausgeschaltet wird, verbringt der Access Point standardmäßig nur einen kleinen Prozentsatz seiner Zeit damit, keine Clients zu bedienen. Beachten Sie, dass ein Kanalwechselintervall von 10 ms auftritt. Im Standard-Abtastintervall von 180 Sekunden wird jeder 2,4-GHz-FCC-Kanal (1−11) mindestens einmal abgetastet. Bei anderen Zulassungsdomänen wie ETSI ist der Access Point für einen etwas höheren Prozentsatz der Zeit deaktiviert. Sowohl die Kanalliste als auch das Abtastintervall können in der RRM-Konfiguration angepasst werden. Dadurch sind die Auswirkungen auf die Leistung auf maximal 1,5 % begrenzt, und der Algorithmus verfügt über intelligente Funktionen, um den Scan auszusetzen, wenn QoS-Frames mit hoher Priorität, z. B. Sprache, bereitgestellt werden müssen.



Diese Grafik zeigt den Off-Channel-Scan-Algorithmus für einen lokalen Modus AP im 2,4 GHz Frequenzband. Ein ähnlicher Vorgang wird parallel auf dem 5-GHz-Funkmodul durchgeführt, wenn ein AP vorhanden ist. Jedes rote Quadrat stellt die Zeit dar, die für den Hauptkanal der Access Points aufgewendet wurde, während jedes blaue Quadrat die Zeit darstellt, die für Scanzwecke auf benachbarten Kanälen aufgewendet wurde.

Scan des Überwachungsmodus

Diese Operation wird von Monitor Mode und Adaptive wIPS Monitor Mode APs durchgeführt, die 100% der Funkzeit nutzen, um alle Kanäle in jedem jeweiligen Frequenzband zu scannen. Dies ermöglicht eine schnellere Erkennung und mehr Zeit für jeden einzelnen Kanal. APs im Überwachungsmodus sind auch bei der Erkennung von unberechtigten Clients deutlich überlegen, da sie eine umfassendere Übersicht über die Aktivitäten in den einzelnen Kanälen haben.



Diese Grafik zeigt den Off-Channel-Scan-Algorithmus für einen Überwachungsmodus AP im 2,4 GHz Frequenzband. Ein ähnlicher Vorgang wird parallel auf dem 5-GHz-Funkmodul durchgeführt, wenn ein AP vorhanden ist.

Vergleich des lokalen und des Überwachungsmodus

Ein Zugangspunkt im lokalen Modus teilt seine Zyklen zwischen dem Dienst von WLAN-Clients und dem Abtasten der Kanäle nach Bedrohungen auf. Dadurch benötigt ein Zugangspunkt im lokalen Modus mehr Zeit, um alle Kanäle zu durchlaufen, und er verbringt weniger Zeit in der Sammlung von Daten auf einem bestimmten Kanal, sodass der Client-Betrieb nicht unterbrochen wird. Infolgedessen sind die Erkennungszeiten für nicht autorisierte Zugriffe und Angriffe länger (3 bis 60 Minuten) und es kann ein kleinerer Bereich von Over-the-air-Angriffen erkannt werden als bei einem AP im Überwachungsmodus.

Darüber hinaus ist die Erkennung von Burst-Datenverkehr, z. B. nicht autorisierter Clients,

wesentlich weniger deterministisch, da sich der Access Point auf dem Datenverkehrskanal befinden muss, während der Datenverkehr übertragen oder empfangen wird. Dies wird eine Übung in Wahrscheinlichkeiten. Ein AP im Überwachungsmodus verbringt alle seine Zyklen mit dem Abtasten von Kanälen, um nach unberechtigten und Over-the-Air-Angriffen zu suchen. Ein AP im Überwachungsmodus kann gleichzeitig für adaptives wIPS, standortbasierte (kontextsensitive) Services und andere Überwachungsmodusservices verwendet werden.

Wenn APs im Überwachungsmodus bereitgestellt werden, können die Vorteile durch eine kürzere Erkennungszeit erzielt werden. Wenn die APs im Überwachungsmodus zusätzlich mit Adaptive wIPS konfiguriert werden, kann ein breiteres Spektrum von drahtlosen Bedrohungen und Angriffen erkannt werden.

APs im lokalen Modus	Überwachungsmodus-APs
Ermöglicht Clients die zeitgesteuerte Suche außerhalb des Kanals	Dedizierter Scan
Hört 50 ms auf jedem Kanal zu	Abhören von 1,2 s auf jedem Kanal
Konfigurierbar für die Suche: • Alle Kanäle • Länderkanäle (Standard) • DCA-Kanäle	Scannt alle Kanäle

Nicht autorisierte Identifizierung

Wenn die Antwort auf eine Anfrage oder Beacons von einem nicht autorisierten Gerät entweder von lokalen APs im Flex-Connect- oder im Überwachungsmodus gehört werden, werden diese Informationen über CAPWAP an den Wireless LAN Controller (WLC) für den Prozess übermittelt. Um Fehlalarme zu verhindern, werden eine Reihe von Methoden verwendet, um sicherzustellen, dass andere verwaltete Access Points von Cisco nicht als nicht autorisiertes Gerät identifiziert werden. Zu diesen Methoden gehören Updates von Mobilitätsgruppen, RF-Nachbarpakete und zugelassene listenfreundliche APs über die Prime-Infrastruktur (PI).

Schurkenaufzeichnungen

Während die Controller-Datenbank mit nicht autorisierten Geräten nur den aktuellen Satz erkannter nicht autorisierter Geräte enthält, enthält die PI auch einen Ereignisverlauf und protokolliert nicht mehr erkannte nicht autorisierte Geräte.

Details zu nicht autorisierten Angriffen

Ein CAPWAP-Access Point schaltet 50 ms lang den Kanal aus, um auf unautorisierte Clients zu hören, Störungen und Kanalinterferenzen zu überwachen. Alle erkannten nicht autorisierten Clients oder APs werden an den Controller gesendet, der die folgenden Informationen erfasst:

- Die MAC-Adresse des nicht autorisierten AP
- Name des erkannten unberechtigten APs
- Die MAC-Adresse des/der nicht autorisierten verbundenen Clients
- Sicherheitsrichtlinie
- Die Präambel
- Signal-Rausch-Verhältnis
- Der Receiver Signal Strength Indicator (RSSI)

- Kanal der Entdeckung nicht autorisierter APs
- Funkmodul, in dem unberechtigte Geräte erkannt werden
- Nicht autorisierte SSID (wenn die nicht autorisierte SSID übertragen wird)
- Nicht autorisierte IP-Adresse
- Das erste und letzte Mal, wenn ein unberechtigtes Gerät gemeldet wird
- Kanalbreite

So exportieren Sie nicht autorisierte Ereignisse

Um nicht autorisierte Ereignisse zur Archivierung in ein Netzwerkmanagementsystem (NMS) eines Drittanbieters zu exportieren, ermöglicht der WLC das Hinzufügen zusätzlicher SNMP-Trap-Empfänger. Wenn ein unberechtigtes Gerät vom Controller erkannt oder entfernt wird, wird ein Trap, der diese Informationen enthält, an alle SNMP-Trap-Empfänger übermittelt. Ein Problem beim Exportieren von Ereignissen über SNMP besteht darin, dass doppelte Ereignisse vom NMS erkannt werden, wenn mehrere Controller dasselbe unberechtigte Gerät erkennen, da die Korrelation nur bei PI erfolgt.

Timeout für nicht autorisierte Datensätze

Wenn ein nicht autorisierter AP den WLC-Datensätzen hinzugefügt wurde, bleibt er dort, bis er nicht mehr angezeigt wird. Nach einer vom Benutzer konfigurierbaren Zeitüberschreitung (Standardwert: 1200 Sekunden) ist ein unberechtigtes Gerät in der Kategorie_unclassited_out veraltet.

Schurken in anderen Zuständen wie_Contained_and_Friendly_ bleiben erhalten, sodass die entsprechende Klassifizierung auf sie angewendet wird, wenn sie wieder auftreten.

Es gibt eine maximale Datenbankgröße für nicht autorisierte Datensätze, die für alle Controller-Plattformen unterschiedlich ist:

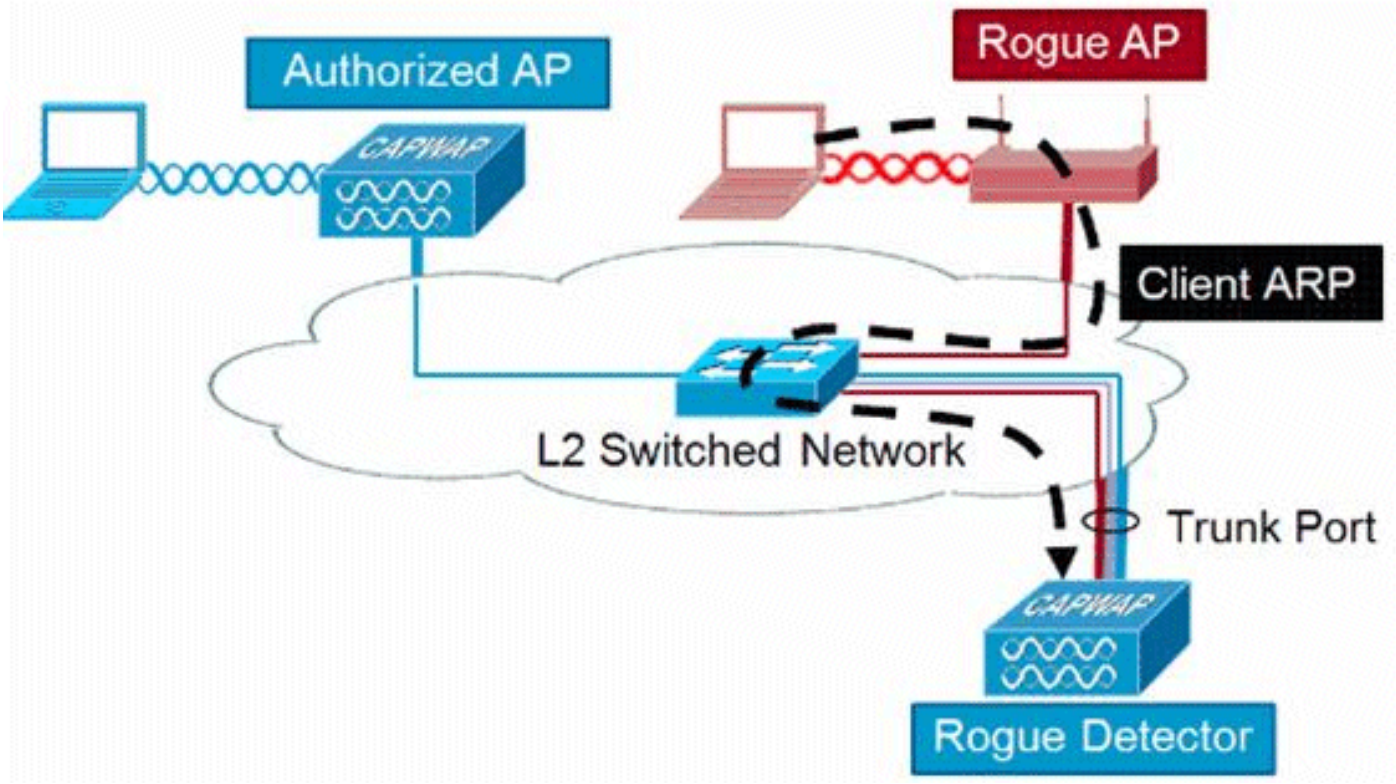
- 3504 - Erkennung und Eindämmung von bis zu 600 nicht autorisierten APs und 1.500 nicht autorisierten Clients
- 5520 - Erkennung und Eindämmung von bis zu 24000 nicht autorisierten APs und 32000 nicht autorisierten Clients
- 8540 - Erkennung und Eindämmung von bis zu 24000 nicht autorisierten APs und 32000 nicht autorisierten Clients

AP zur Erkennung nicht autorisierter APs

Ein nicht autorisierter Detektor AP zielt darauf ab, nicht autorisierte Informationen, die über Funk gehört werden, mit ARP-Informationen zu korrelieren, die aus dem kabelgebundenen Netzwerk abgerufen werden. Wenn eine MAC-Adresse drahtlos als unberechtigter Access Point oder Client abgehört wird und auch im kabelgebundenen Netzwerk zu hören ist, wird der unberechtigte Benutzer als Teil des kabelgebundenen Netzwerks erkannt. Wenn das unberechtigte Gerät im kabelgebundenen Netzwerk erkannt wird, wird der Schweregrad des Alarms für diesen unberechtigten Access Point auf_critical_gesetzt. Ein nicht autorisierter Access Point ist bei der Identifizierung von nicht autorisierten Clients hinter einem Gerät, das NAT verwendet, nicht erfolgreich.

Dieser Ansatz wird verwendet, wenn nicht autorisierte APs eine Form der Authentifizierung

aufweisen, entweder WEP oder WPA. Wenn eine Form der Authentifizierung auf einem nicht autorisierten Access Point konfiguriert ist, kann der Lightweight Access Point keine Verbindung herstellen, da er die Authentifizierungsmethode und die auf dem nicht autorisierten Access Point konfigurierten Anmeldeinformationen nicht kennt.



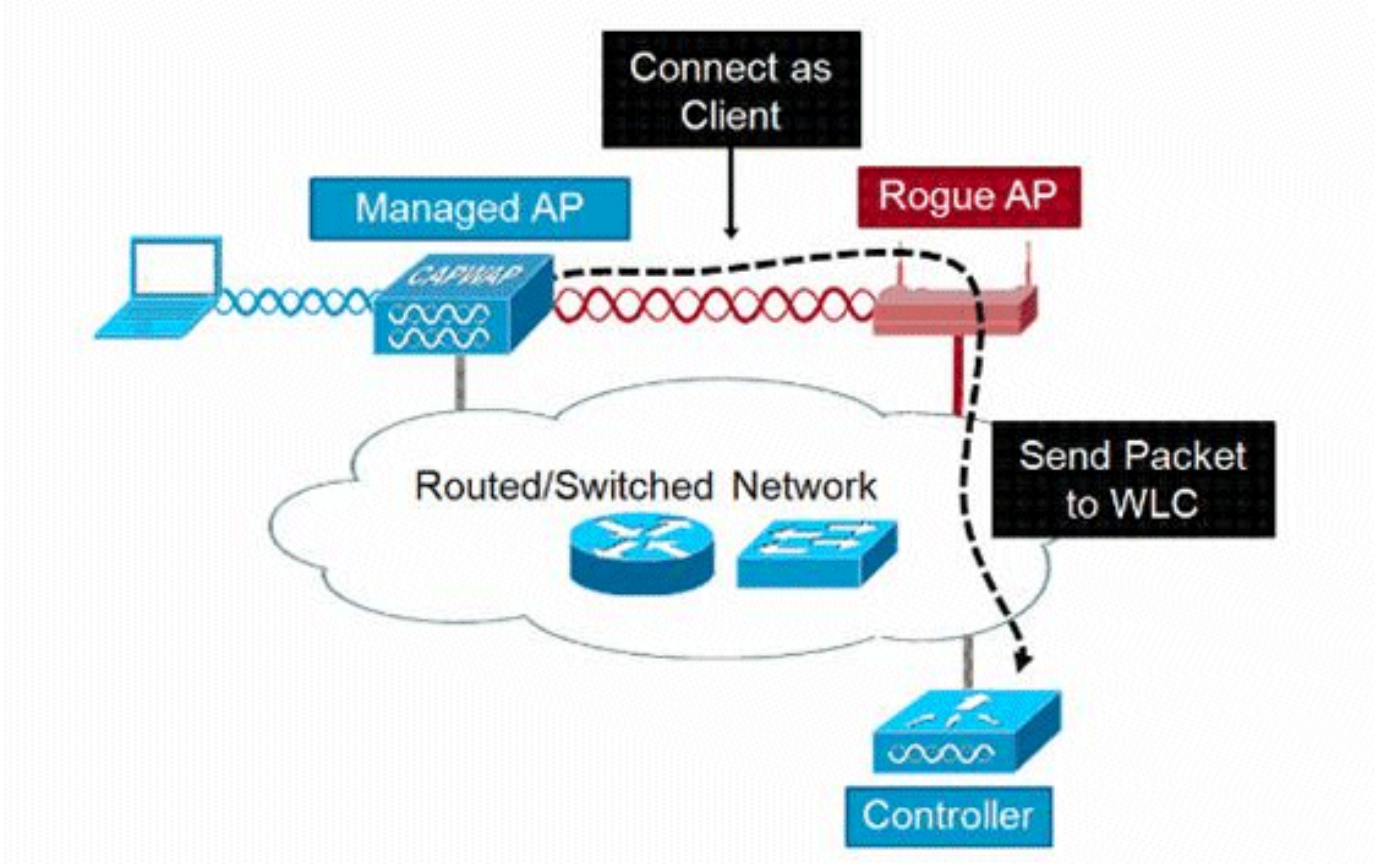
Anmerkung: Nur APs der Phase 1 können als Entdecker für nicht autorisierte APs konfiguriert werden.

Überlegungen zur Skalierbarkeit

Ein nicht autorisierter AP kann bis zu 500 nicht autorisierte Benutzer und 500 nicht autorisierte Clients erkennen. Wenn der Rogue-Detektor auf einem Trunk mit zu vielen Rogue-Geräten platziert wird, werden diese Grenzwerte überschritten, was Probleme verursacht. Um dies zu verhindern, sollten Sie nicht autorisierte Access Points auf der Distribution- oder Zugriffsebene Ihres Netzwerks belassen.

RLDP

Ziel des RLDP ist es, zu ermitteln, ob ein bestimmter nicht autorisierter AP mit der kabelgebundenen Infrastruktur verbunden ist. Bei dieser Funktion wird im Wesentlichen der AP verwendet, der dem unautorisierten Gerät als Wireless-Client am nächsten liegt. Nach der Verbindung als Client wird ein Paket mit der Zieladresse des WLC gesendet, um zu prüfen, ob der AP mit dem kabelgebundenen Netzwerk verbunden ist. Wenn festgestellt wird, dass sich das unberechtigte Gerät im kabelgebundenen Netzwerk befindet, wird der Schweregrad des Alarms für diesen unberechtigten Access Point auf "Kritisch" gesetzt.



Der Algorithmus von RLDP ist hier aufgeführt:

1. Identifizieren Sie den Unified AP, der dem unautorisierten Access Point am nächsten ist, durch Verwendung von Signalstärkenwerten.
2. Der Access Point stellt dann eine Verbindung mit dem unberechtigten Gerät als WLAN-Client her und versucht, drei Zuordnungen herzustellen, bevor eine Zeitüberschreitung auftritt.
3. Wenn die Zuordnung erfolgreich ist, verwendet der WAP DHCP, um eine IP-Adresse abzurufen.
4. Wenn eine IP-Adresse abgerufen wurde, sendet der WAP (der als WLAN-Client fungiert) ein UDP-Paket an jede der Controller-IP-Adressen.
5. Wenn der Controller auch nur eines der RLDP-Pakete vom Client empfängt, wird dieses unberechtigte Gerät als On-Wire-Paket mit einem kritischen Schweregrad markiert.

Anmerkung: Die RLDP-Pakete können den Controller nicht erreichen, wenn die Filterregeln zwischen dem Controller-Netzwerk und dem Netzwerk vorhanden sind, in dem sich das unautorisierte Gerät befindet.

Vorbehalte gegen RLDP

- RLDP funktioniert nur mit offenen, nicht autorisierten Access Points, die ihre SSID mit deaktivierter Authentifizierung und Verschlüsselung übertragen.
- RLDP erfordert, dass der verwaltete WAP, der als Client fungiert, eine IP-Adresse über DHCP im nicht autorisierten Netzwerk abrufen kann
- Mit dem manuellen RLDP kann mehrfach versucht werden, ein unautorisiertes Gerät zu verfolgen.

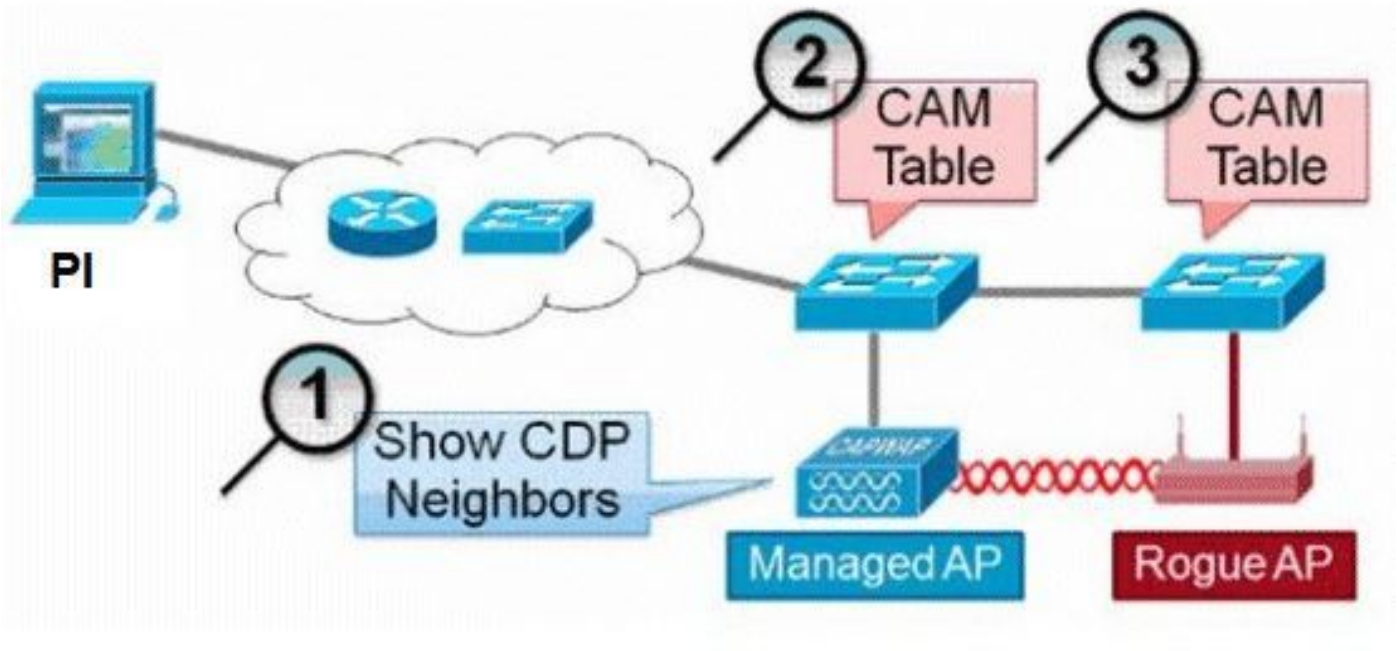
- Beim RLDP-Prozess kann der Access Point keine Clients bedienen. Dies wirkt sich negativ auf die Leistung und die Konnektivität der APs im lokalen Modus aus.
- RLDP versucht nicht, eine Verbindung zu einem nicht autorisierten Access Point herzustellen, der in einem 5-GHz-DFS-Kanal betrieben wird.

Switch-Port-Spuren

Die Switch-Port-Verfolgung ist eine Technik zur Verhinderung nicht autorisierter APs. Obwohl die Switch-Port-Verfolgung am PI initiiert wird, verwendet sie sowohl CDP- als auch SNMP-Informationen, um ein unautorisiertes Gerät bis zu einem bestimmten Port im Netzwerk zu verfolgen.

Damit die Switch-Port-Nachverfolgung ausgeführt werden kann, müssen alle Switches im Netzwerk der IP-Adresse mit SNMP-Anmeldeinformationen hinzugefügt werden. Obwohl schreibgeschützte Anmeldedaten den Port identifizieren, an dem sich das unautorisierte Gerät befindet, ermöglichen Schreibzugriff-Anmeldedaten es der PI, den Port ebenfalls herunterzufahren, wodurch die Bedrohung eingedämmt wird.

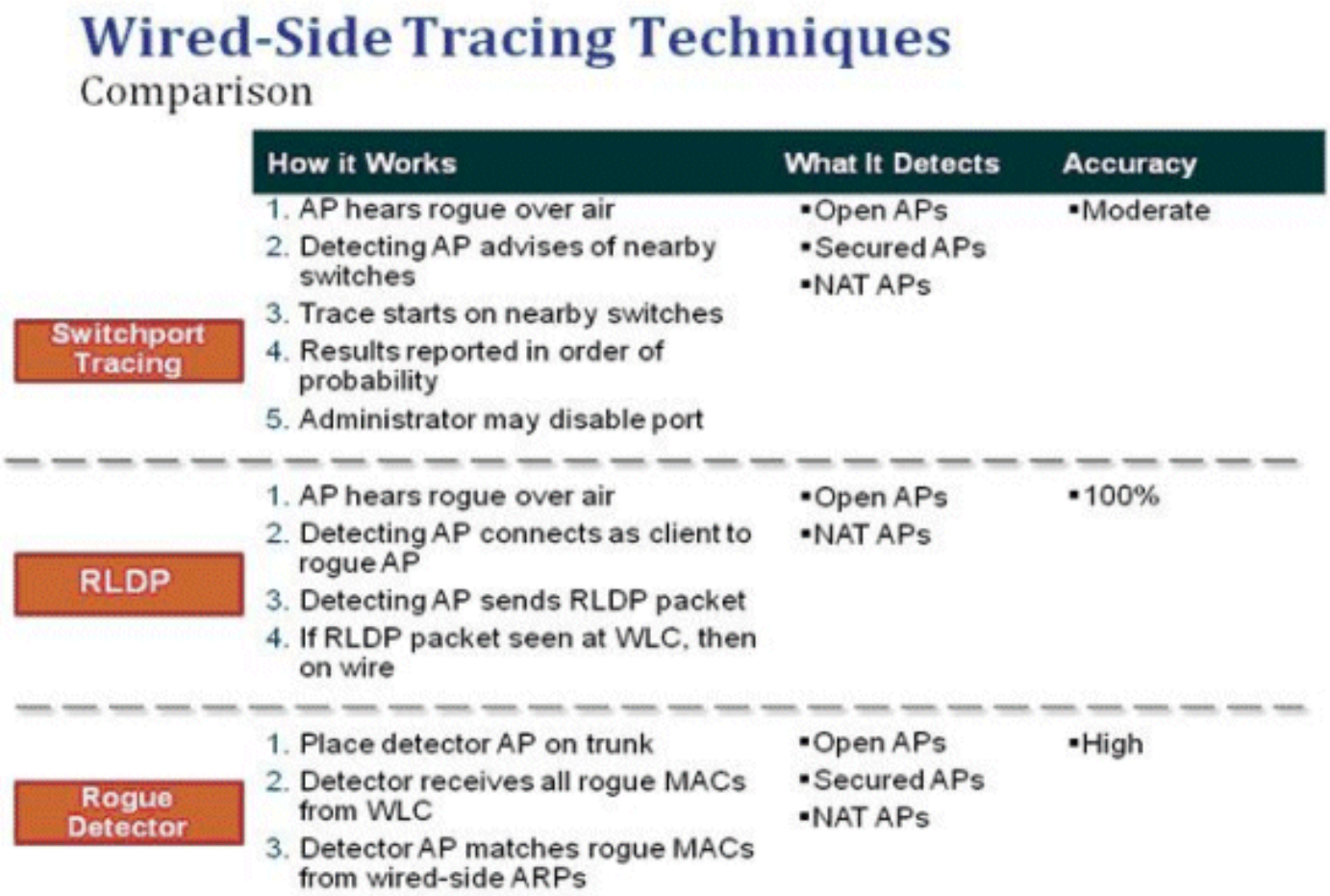
Derzeit funktioniert diese Funktion nur mit Cisco Switches, auf denen Cisco IOS® mit aktiviertem CDP ausgeführt wird. CDP muss auch auf den verwalteten APs aktiviert sein.



Der Algorithmus für die Switch-Port-Nachverfolgung ist hier aufgeführt:

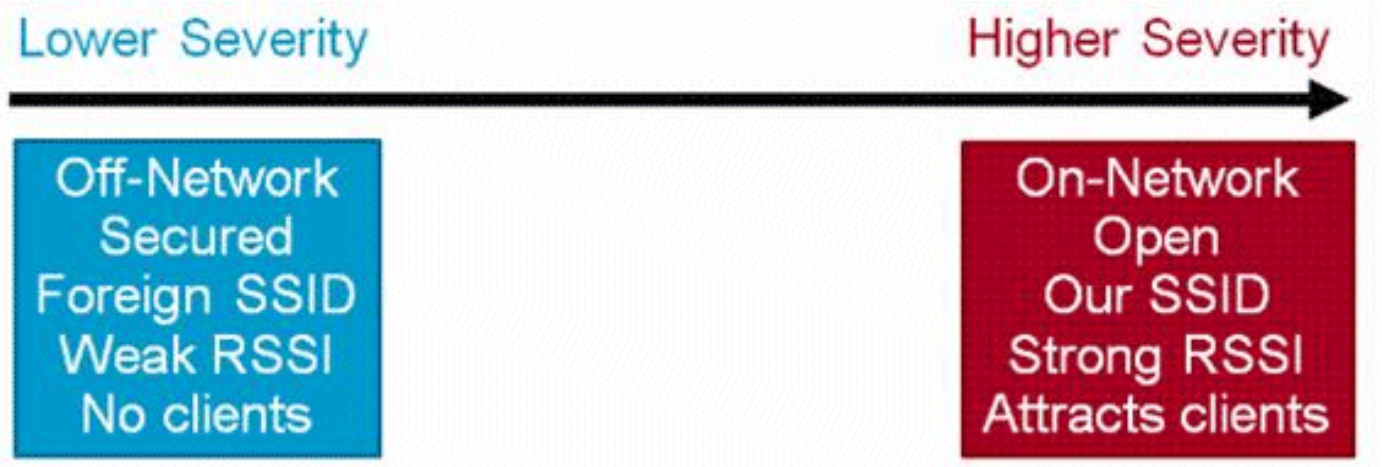
1. Der PI findet den AP, der den unberechtigten Access Point drahtlos erkennt, und ruft dessen CDP-Nachbarn ab.
2. Die PI verwendet SNMP, um die CAM-Tabelle im benachbarten Switch zu überprüfen. Die unautorisierte Stelle wird durch eine positive Übereinstimmung identifiziert.
3. Eine positive Übereinstimmung basiert auf der exakten unautorisierten MAC-Adresse, +1/−1 der unautorisierten MAC-Adresse, auf beliebigen unautorisierten Client-MAC-Adressen oder auf einer OUI-Übereinstimmung basierend auf den einer MAC-Adresse inhärenten Herstellerinformationen.
4. Wenn auf dem nächstgelegenen Switch keine positive Übereinstimmung gefunden wird,

setzt die PI die Suche in benachbarten Switches bis zu zwei Hops entfernt fort (standardmäßig).



Klassifizierung nicht autorisierter APs

Standardmäßig werden alle vom Cisco UWN erkannten unberechtigten Geräte als nicht klassifiziert betrachtet. Wie in dieser Grafik gezeigt, können nicht autorisierte APs anhand verschiedener Kriterien klassifiziert werden, darunter RSSI, SSID, Sicherheitstyp, Ein-/Aus-Netzwerk und Anzahl der Clients:



Regeln für die nicht autorisierte Klassifizierung

Regeln für die Klassifizierung nicht autorisierter APs ermöglichen Ihnen die Definition einer Reihe von Bedingungen, die ein unberechtigtes Programm entweder als schädlich oder als vertrauenswürdig markieren. Diese Regeln werden in der PI oder im WLC konfiguriert, sie werden jedoch immer auf dem Controller ausgeführt, wenn neue unberechtigte Benutzer erkannt werden.

Weitere Informationen zu nicht autorisierten Regeln in den WLCs finden Sie im DokumentRule Based Rogue Classification in Wireless LAN Controllers (WLC) and Prime Infrastructure (PI).

HA-Fakten

Wenn Sie ein nicht autorisiertes Gerät manuell in den geschlossenen Zustand (jede Klasse) oder den benutzerfreundlichen Zustand versetzen, werden diese Informationen im Cisco WLC-Standby-Flash-Speicher gespeichert. Die Datenbank wird jedoch nicht aktualisiert. Bei einem HA-Switchover wird die Liste der nicht autorisierten Access Points aus dem Cisco WLC-Flash-Speicher geladen, der zuvor im Standby-Modus war.

Wenn in einem Hochverfügbarkeitsszenario die Sicherheitsstufe für die Erkennung nicht autorisierter Geräte entweder auf "Hoch" oder "Kritisch" festgelegt ist, startet der unautorisierte Timer auf dem Standby-Controller erst nach der Stabilisierungszeit für die Erkennung nicht autorisierter Geräte, die 300 Sekunden beträgt. Die aktiven Konfigurationen des Standby-Controllers werden daher erst nach 300 Sekunden wiedergegeben.

Fakten zu FlexConnect

Ein FlexConnect-AP (mit aktivierter Erkennung unberechtigter APs) im verbundenen Modus übernimmt die Eindämmungsliste vom Controller. Wenn im Controller automatisch enthaltene SSID und automatisch enthaltene Adhoc-Werte festgelegt wurden, werden diese Konfigurationen auf alle FlexConnect-APs im verbundenen Modus festgelegt, und der Access Point speichert sie im Speicher.

Wenn der FlexConnect AP in den Standalone-Modus wechselt, werden die folgenden Aufgaben ausgeführt:

- Das vom Controller eingestellte Containment wird fortgesetzt.
- Wenn der FlexConnect-WAP einen nicht autorisierten WAP erkennt, der die gleiche SSID wie die Infrarot-SSID hat (SSID ist im Controller konfiguriert, mit dem der FlexConnect-WAP verbunden ist), wird die Eindämmung gestartet, wenn die automatische SSID-Speicherung vom Controller aktiviert wurde, bevor er in den Standalone-Modus wechselt.
- Wenn der FlexConnect-WAP einen unberechtigten Adhoc-Zugriff erkennt, wird die Eindämmung gestartet, wenn der automatische Eindämmung-Adhoc vom Controller im verbundenen Modus aktiviert wurde.

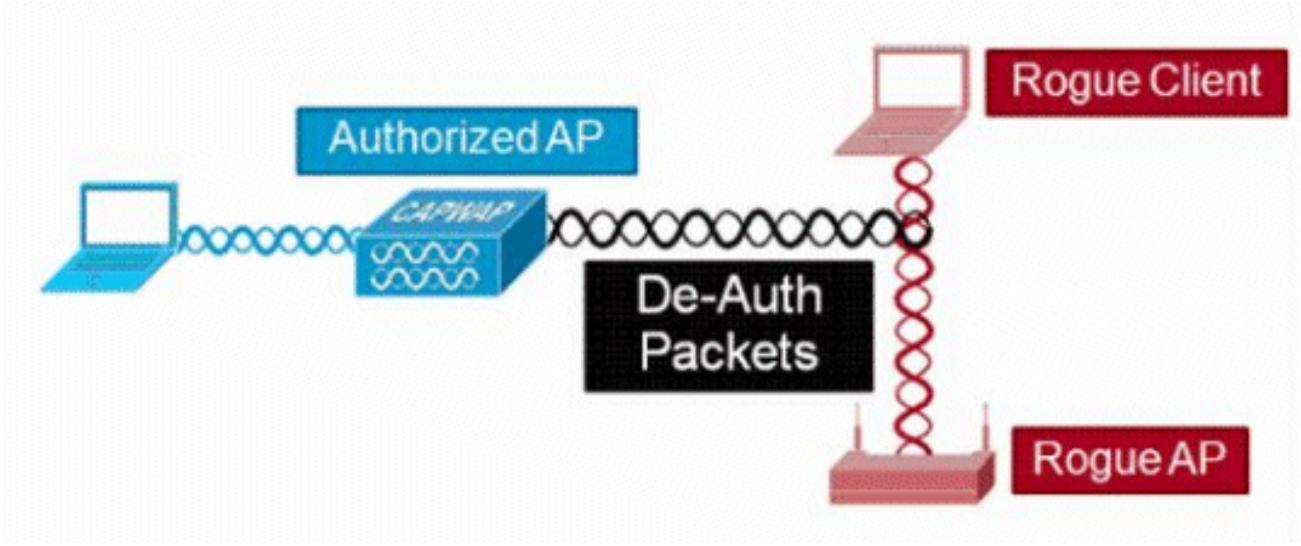
Wenn der eigenständige FlexConnect AP wieder in den verbundenen Modus wechselt, werden folgende Aufgaben ausgeführt:

- Alle Containments werden gelöscht.
- Vom Controller initiierte Eindämmung übernimmt.

Verhinderung von nicht autorisierten Zugriffen

Blockierung nicht autorisierter APs

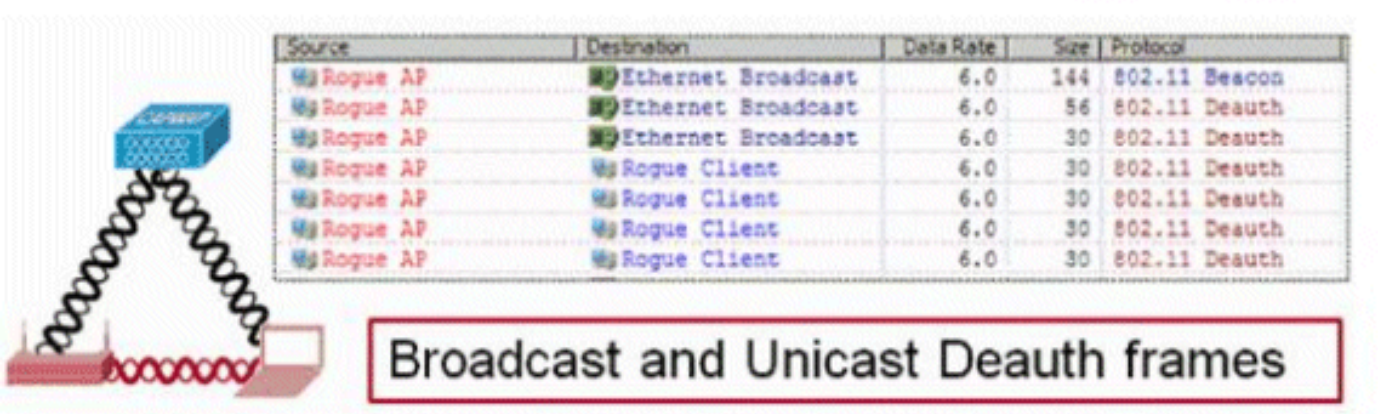
Eindämmung: Bei dieser Methode werden Over-the-Air-Pakete verwendet, um den Dienst auf einem nicht autorisierten Gerät vorübergehend zu unterbrechen, bis es physisch entfernt werden kann. Die Eindämmung funktioniert mit dem Spoof von Deauthentifizierungspaketen mit der gefälschten Quelladresse des nicht autorisierten Access Points, sodass alle verbundenen Clients gestartet werden.



Details zu nicht autorisierter Eindämmung

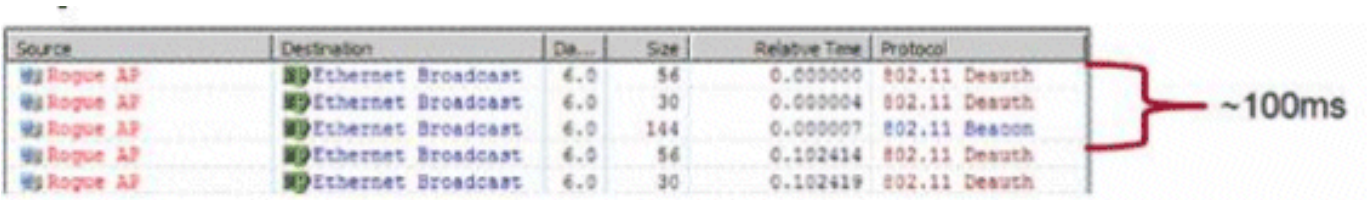
Eine Eindämmung, die auf einem nicht autorisierten Access Point ohne Clients initiiert wird, verwendet nur an die Broadcast-Adresse gesendete De-Authentifizierungs-Frames:

Ein Containment, das auf einem nicht autorisierten Access Point mit einem oder mehreren Clients initiiert wird, verwendet De-Authentifizierungs-Frames, die an die Broadcast-Adresse und die Client(s)-Adresse gesendet werden:



Eindämmungspakete werden mit der Leistung des verwalteten AP und der niedrigsten aktivierten Datenrate gesendet.

Containment sendet mindestens 2 Pakete alle 100 ms:



> **Anmerkung:** Eine von APs im Nicht-Überwachungsmodus ausgeführte Eindämmung wird in einem Intervall von 500 ms anstatt des von APs im Überwachungsmodus verwendeten Intervalls von 100 ms gesendet.

- Ein einzelnes nicht autorisiertes Gerät kann von 1 bis 4 verwalteten APs eingeschlossen werden, die gemeinsam die Bedrohung vorübergehend reduzieren.
- Die Eindämmung kann mithilfe von APs im lokalen Modus, im Überwachungsmodus und im Flex-Connect-Modus (verbunden) erfolgen. Für den lokalen Modus von Flex-Connect-APs können maximal drei nicht autorisierte Geräte pro Funk enthalten sein. Bei APs im Überwachungsmodus können maximal sechs nicht autorisierte Geräte pro Funk enthalten sein.

Automatische Eindämmung

Neben der manuellen Initiierung der Eindämmung auf einem nicht autorisierten Gerät über PI oder die WLC-GUI besteht die Möglichkeit, die Eindämmung unter bestimmten Szenarien automatisch zu starten. Diese Konfiguration befindet sich unter **Allgemim AbschnittRichtlinien für nicht autorisierte** Zugriffe der PI- oder Controller-Schnittstelle. Jede dieser Funktionen ist standardmäßig deaktiviert und sollte nur aktiviert werden, um die Bedrohungen zu neutralisieren, die den größten Schaden verursachen.

- Nicht autorisierte drahtgebundene Geräte - Wenn ein nicht autorisiertes Gerät als mit dem kabelgebundenen Netzwerk verbunden identifiziert wird, wird es automatisch in die Schranke verwiesen.
- Verwendung unserer SSID: Wenn ein nicht autorisiertes Gerät eine SSID verwendet, die mit der auf dem Controller konfigurierten identisch ist, wird diese automatisch enthalten. Diese Funktion soll einen Angriff auf einen Honigtopf abwehren, bevor er Schaden anrichtet.

- Gültiger Client auf nicht autorisiertem AP: Wenn festgestellt wird, dass ein im Radius-/AAA-Server aufgeführter Client mit einem nicht autorisierten Gerät verknüpft ist, wird die Eindämmung nur gegen diesen Client gestartet, sodass dieser nicht mit einem nicht verwalteten AP verknüpft werden kann.
- Ad-Hoc Rogue AP - Wenn ein Ad-hoc-Netzwerk entdeckt wird, wird es automatisch eingeschlossen.

Hinweise zur Schurkeneindämmung

- Da die Eindämmung einen Teil der Funkzeit des verwalteten Access Points für das Senden der Frames zur Deauthentifizierung verwendet, wird die Leistung für Daten- und Sprach-Clients um bis zu 20 % beeinträchtigt. Bei Daten-Clients wird der Durchsatz reduziert. Bei Sprach-Clients kann die Eindämmung zu Gesprächsunterbrechungen und einer reduzierten Sprachqualität führen.
- Eindämmung kann rechtliche Folgen haben, wenn sie gegen Nachbarnetzwerke eingeleitet wird. Stellen Sie sicher, dass sich das nicht autorisierte Gerät in Ihrem Netzwerk befindet und ein Sicherheitsrisiko darstellt, bevor Sie mit der Eindämmung beginnen.

Schließen des Switch-Ports

Sobald ein Switch-Port durch die Verwendung von SPT verfolgt wird, gibt es eine Option zum Deaktivieren dieses Ports in PI. Administrator muss diese Übung manuell durchführen. Es steht eine Option zur Verfügung, um den Switch-Port über PI zu aktivieren, wenn unberechtigte Geräte physisch aus dem Netzwerk entfernt werden.

Konfigurieren

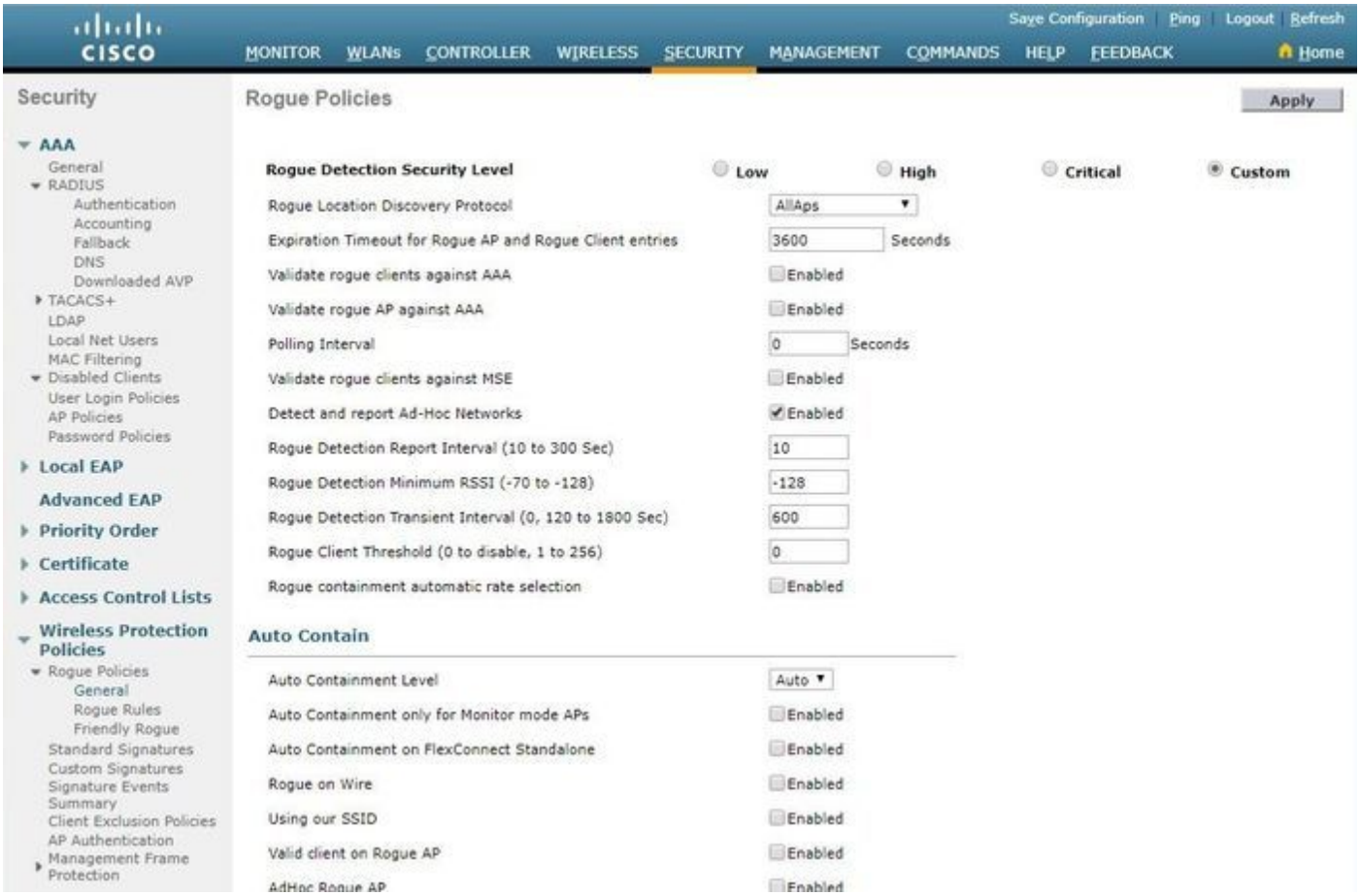
Konfigurieren der Erkennung nicht autorisierter APs

Die Erkennung nicht autorisierter APs ist auf dem Controller standardmäßig aktiviert.

Um verschiedene Optionen zu konfigurieren, navigieren Sie **zuSicherheit > Drahtlosschutzrichtlinien > Richtlinien für nicht autorisierte Zugriffe > Allgemein**. Als Beispiel:

Schritt 1: Ändern Sie die Zeitüberschreitung für nicht autorisierte Access Points.

Schritt 2: Aktivieren Sie die Erkennung von unautorisierten Ad-hoc-Netzwerken.



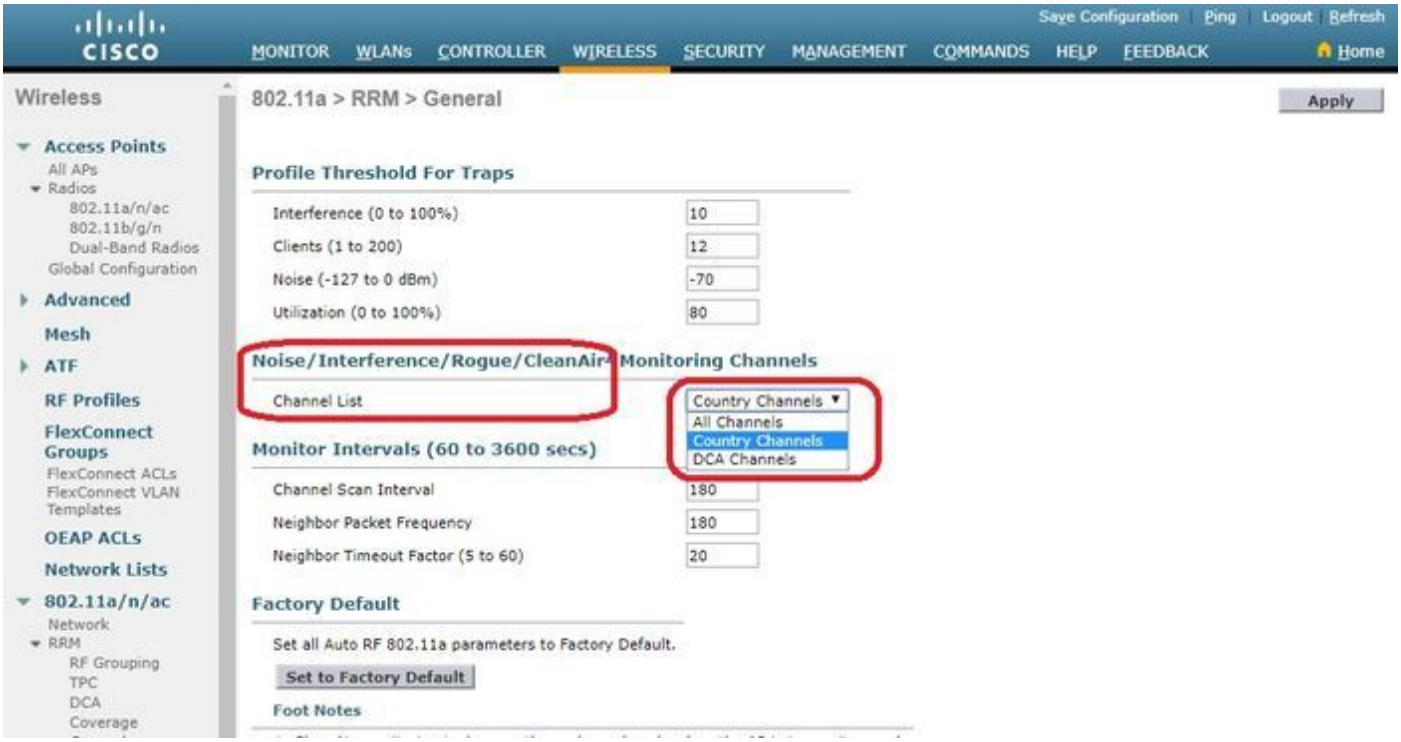
Über die CLI:

```
(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
```

Kanalsuche für Erkennung nicht autorisierter APs konfigurieren

Für einen AP im lokalen/Flex-Connect/Überwachungsmodus steht eine Option unter der RRM-Konfiguration zur Verfügung, mit der der Benutzer auswählen kann, welche Kanäle auf unberechtigte APs gescannt werden. Abhängig von der Konfiguration durchsucht der WAP alle Channel-/Country-Channel-/DCA-Channels nach unberechtigten Geräten.

Um dies über die GUI zu konfigurieren, navigieren Sie **zu Wireless > 802.11a/802.11b > RRM > General (Wireless > 802.11a/802.11b > RRM > Allgemein)**, wie im Bild gezeigt.



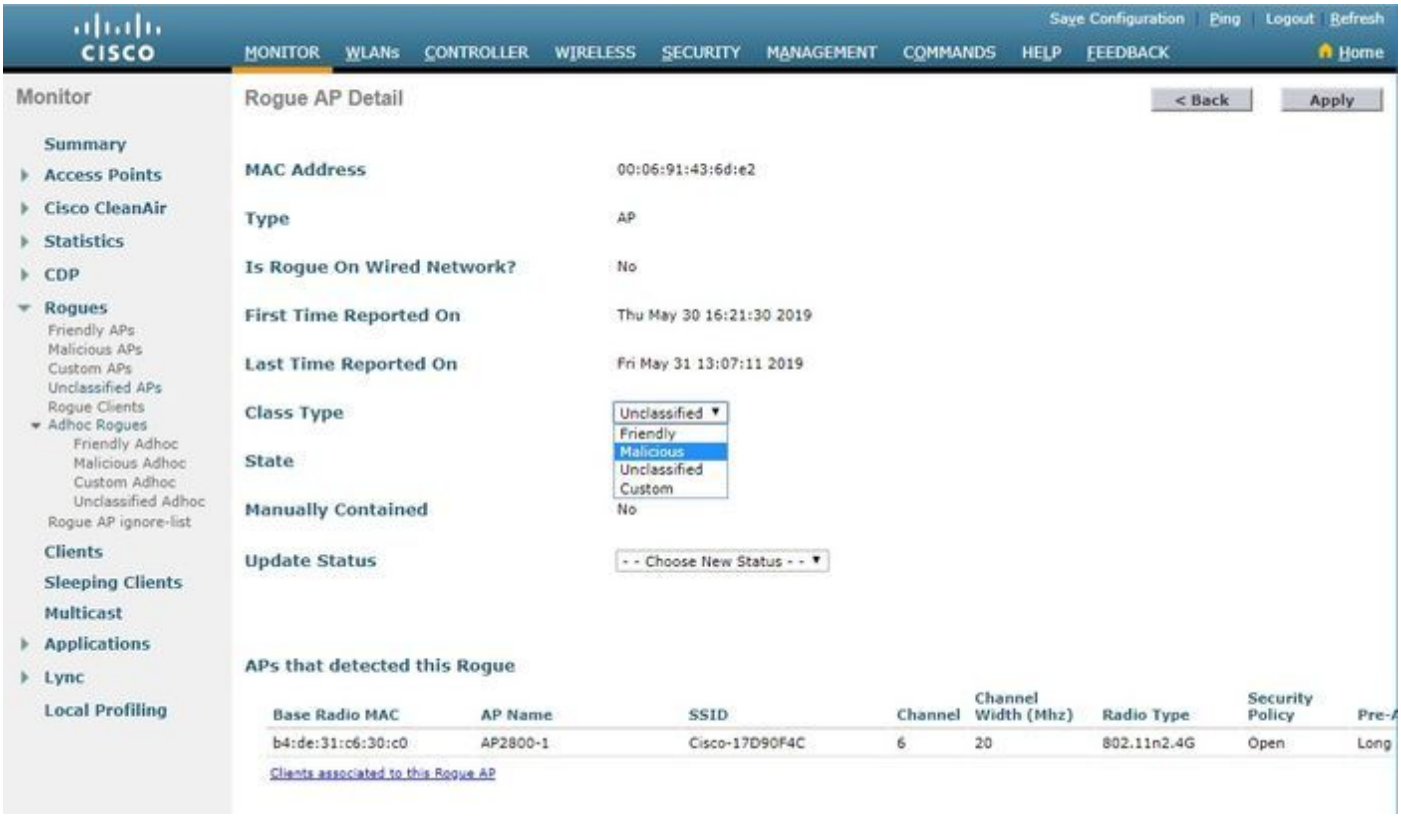
Über die CLI:

```
(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
```

Konfigurieren der Rogue-Klassifizierung

Manuelles Klassifizieren von nicht autorisierten APs

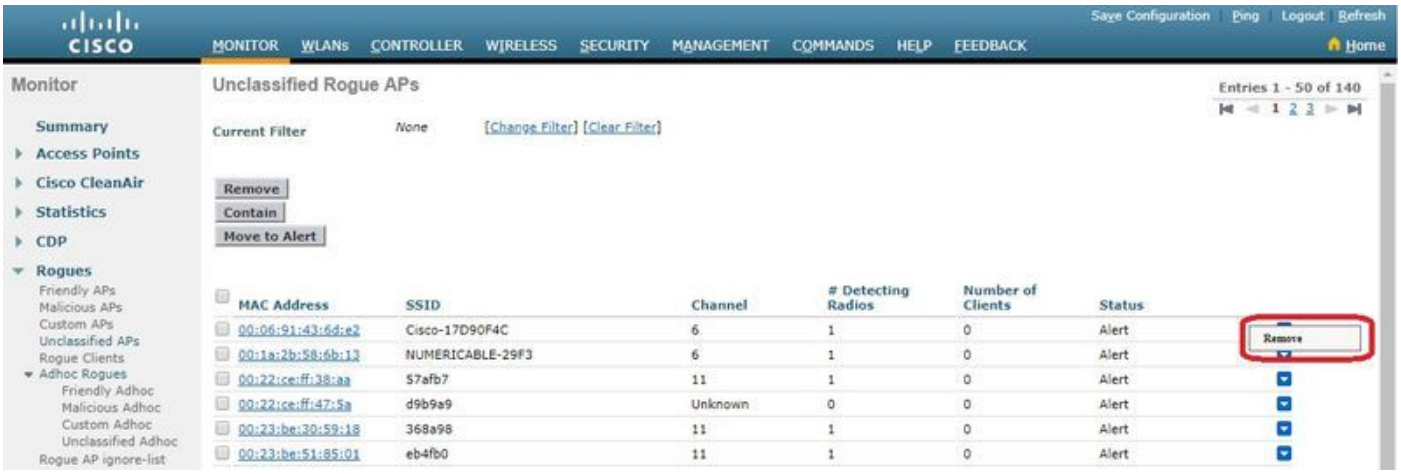
Um einen nicht autorisierten Access Point als benutzerfreundlich, schädlich oder nicht klassifiziert zu klassifizieren, navigieren Sie **zu Monitor > Rogue > Unclassized** APs, und klicken Sie auf den jeweiligen Namen des nicht autorisierten Access Points. Wählen Sie die Option aus der Dropdown-Liste aus, wie im Bild dargestellt.



Über die CLI:

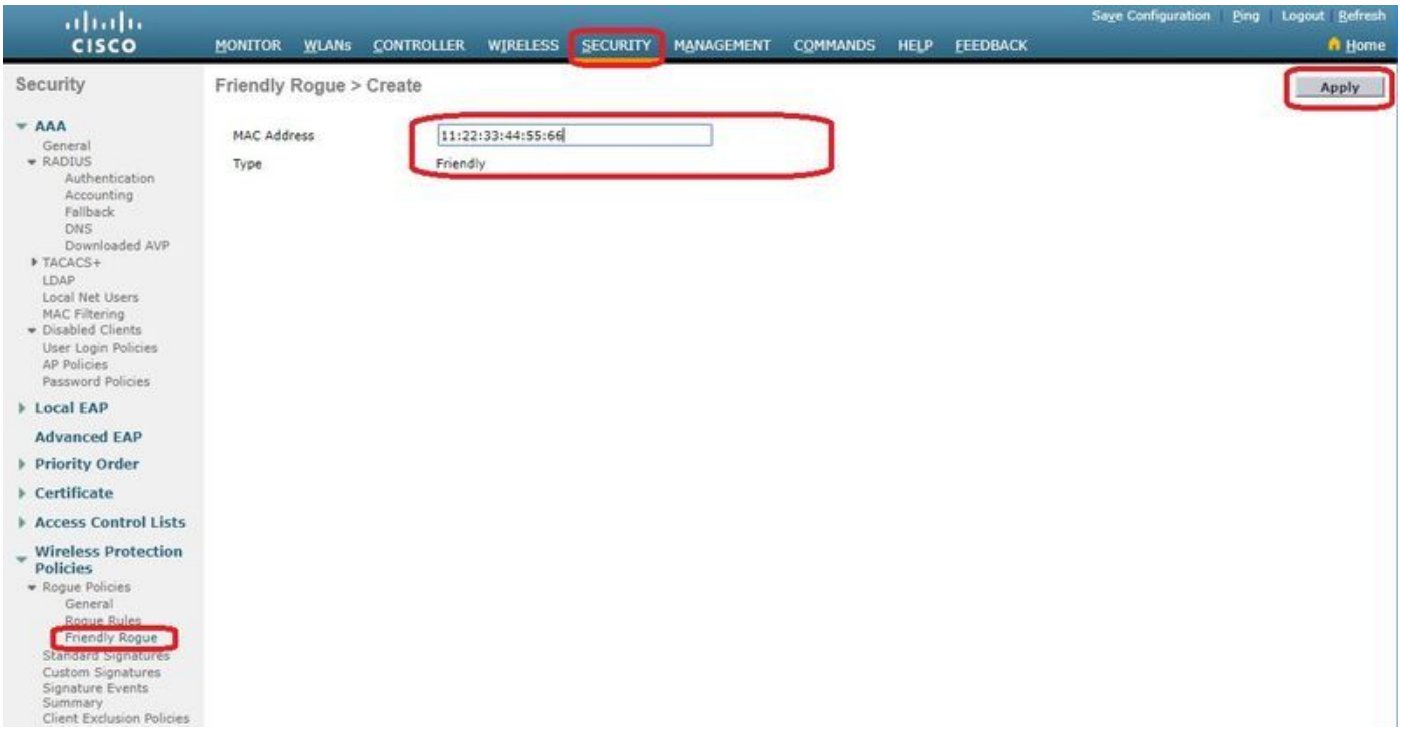
```
(Cisco Controller) >config rogue ap ?

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.
```

Um einen nicht autorisierten Eintrag manuell aus der Liste der nicht autorisierten Access Points zu entfernen, navigieren Sie **zu Monitor > Rogue > Unclassited** APs, und **klicken Sie auf Remove (Entfernen)**, wie im Bild gezeigt.



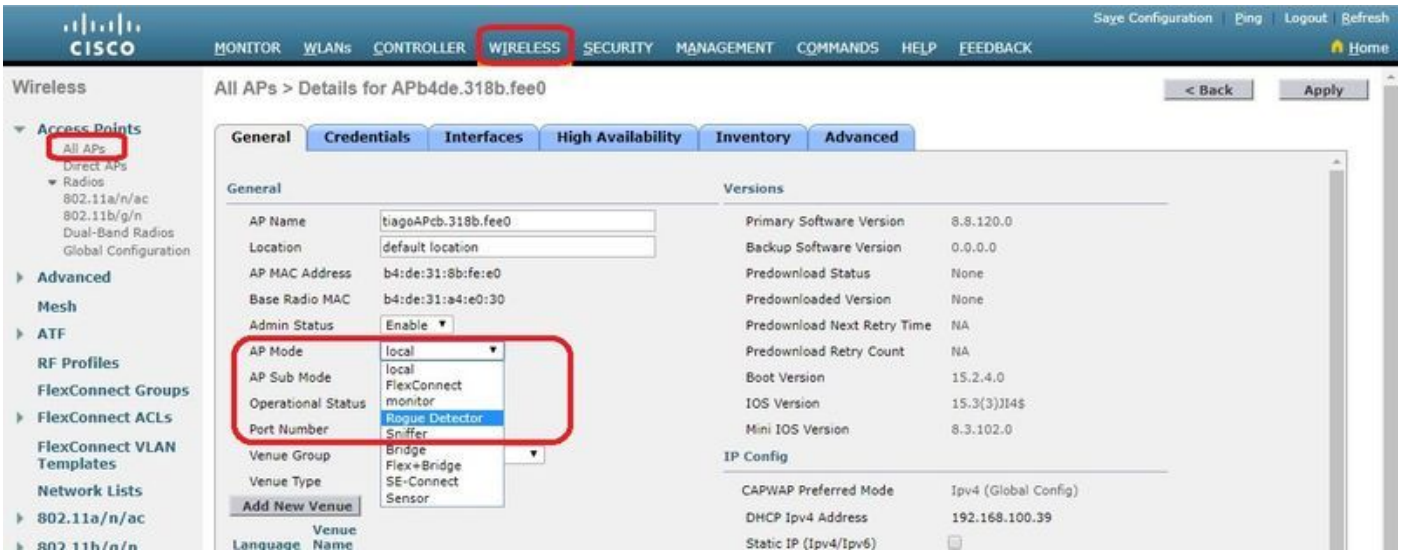
Um einen nicht autorisierten Access Point als benutzerfreundlichen Access Point zu konfigurieren, navigieren Sie **zu Security > Wireless Protection Policies > Rogue Policies > Friendly** Roguesund fügen Sie die nicht autorisierte MAC-Adresse hinzu.

Die hinzugefügten unberechtigten Einträge können **vonMonitor > Rogues > Friendly** Roguepage überprüft werden, wie im Bild gezeigt.



Konfigurieren eines AP zur Erkennung nicht autorisierter APs

Um den Access Point über die Benutzeroberfläche als nicht autorisierten Detektor zu konfigurieren, navigieren Sie zu Wireless > All APs (Wireless > Alle Access Points). Wählen Sie den AP-Namen aus, und ändern Sie den AP-Modus wie im Bild dargestellt.



Über die 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
```

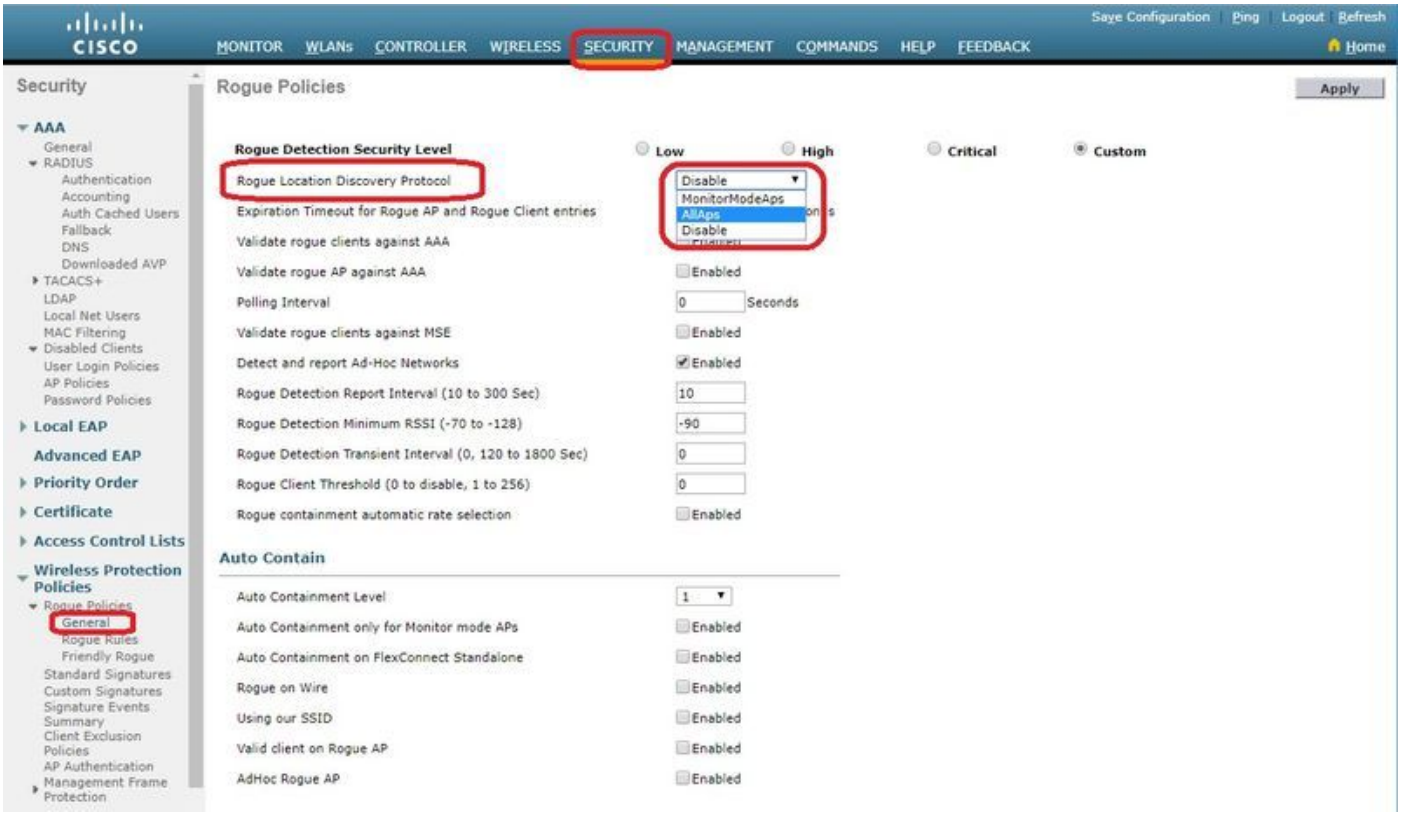
Switch-Port für einen Access Point zur Erkennung nicht autorisierter APs konfigurieren

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

> **Anmerkung:** Das native VLAN in dieser Konfiguration verfügt über eine IP-Verbindung mit dem WLC.

RLDP konfigurieren

Um RLDP in der Controller-GUI zu konfigurieren, navigieren Sie **zu Security > Wireless Protection Policies > Rogue Policies > General**.



Überwachungsmodus-APs - Ermöglicht nur APs im Überwachungsmodus, am RLDP teilzunehmen.

Alle APs - lokale/Flex-Connect/Überwachungsmodus-APs sind am RLDP-Prozess beteiligt.

Disabled (Deaktiviert): RLDP wird nicht automatisch ausgelöst. Der Benutzer kann jedoch über die CLI RLDP manuell für eine bestimmte MAC-Adresse auslösen.

> **Anmerkung:** Der AP im Überwachungsmodus bevorzugt den lokalen/Flex-Connect-AP bei der Ausführung von RLDP, wenn beide APs einen bestimmten unberechtigten Angriff mit mehr als -85 dBm RSSI erkennen.

Über die 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
```

Der RLDP-Zeitplan und der manuelle Trigger können nur über die Eingabeaufforderung konfiguriert werden. So starten Sie RLDP manuell:

```
(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).
```

Zeitplan für 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.
```

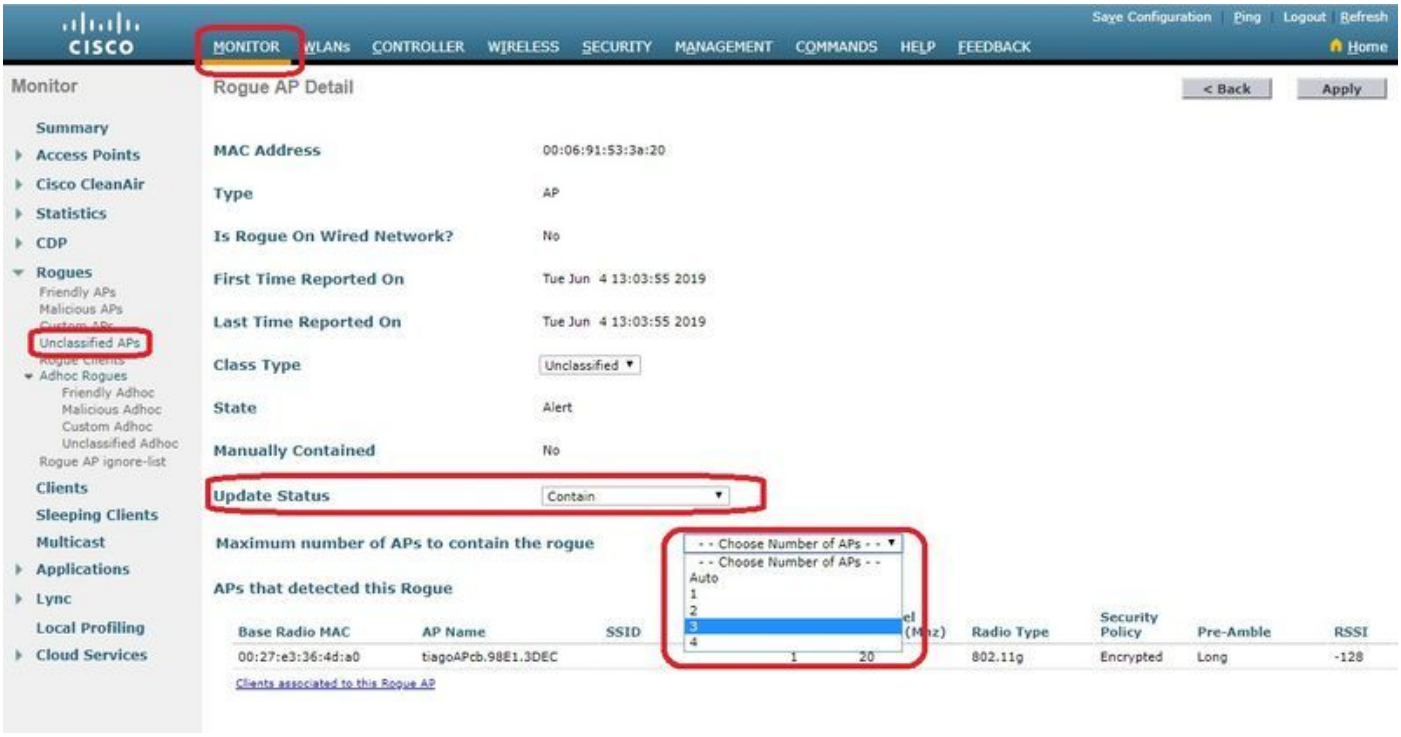
RLDP-Wiederholungsversuche können mit dem folgenden Befehl konfiguriert werden:

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

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

Konfigurieren der Verhinderung nicht autorisierter APs

Manuelle Eindämmung konfigurieren

Um einen nicht autorisierten Access Point manuell einzuschließen, navigieren Sie **zuMonitor > Rogues > Unclassited** (Überwachen > nicht klassifiziert), wie im Bild dargestellt.



Über die 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].
```

> **Anmerkung:** Ein bestimmtes unberechtigtes Gerät kann mit 1-4 APs geschützt werden. Standardmäßig verwendet der Controller einen Access Point für einen Client. Wenn zwei APs ein bestimmtes unberechtigtes Gerät erkennen können, enthält der Access Point mit dem höchsten RSSI den Client unabhängig vom AP-Modus.

Automatische Eindämmung

Um die automatische Eindämmung **zu** konfigurieren, gehen Sie **zu**Sicherheit**>Wireless-Schutzrichtlinien>Nicht autorisierte Richtlinien>Allgemein**, und aktivieren Sie alle zutreffenden Optionen für Ihr Netzwerk.

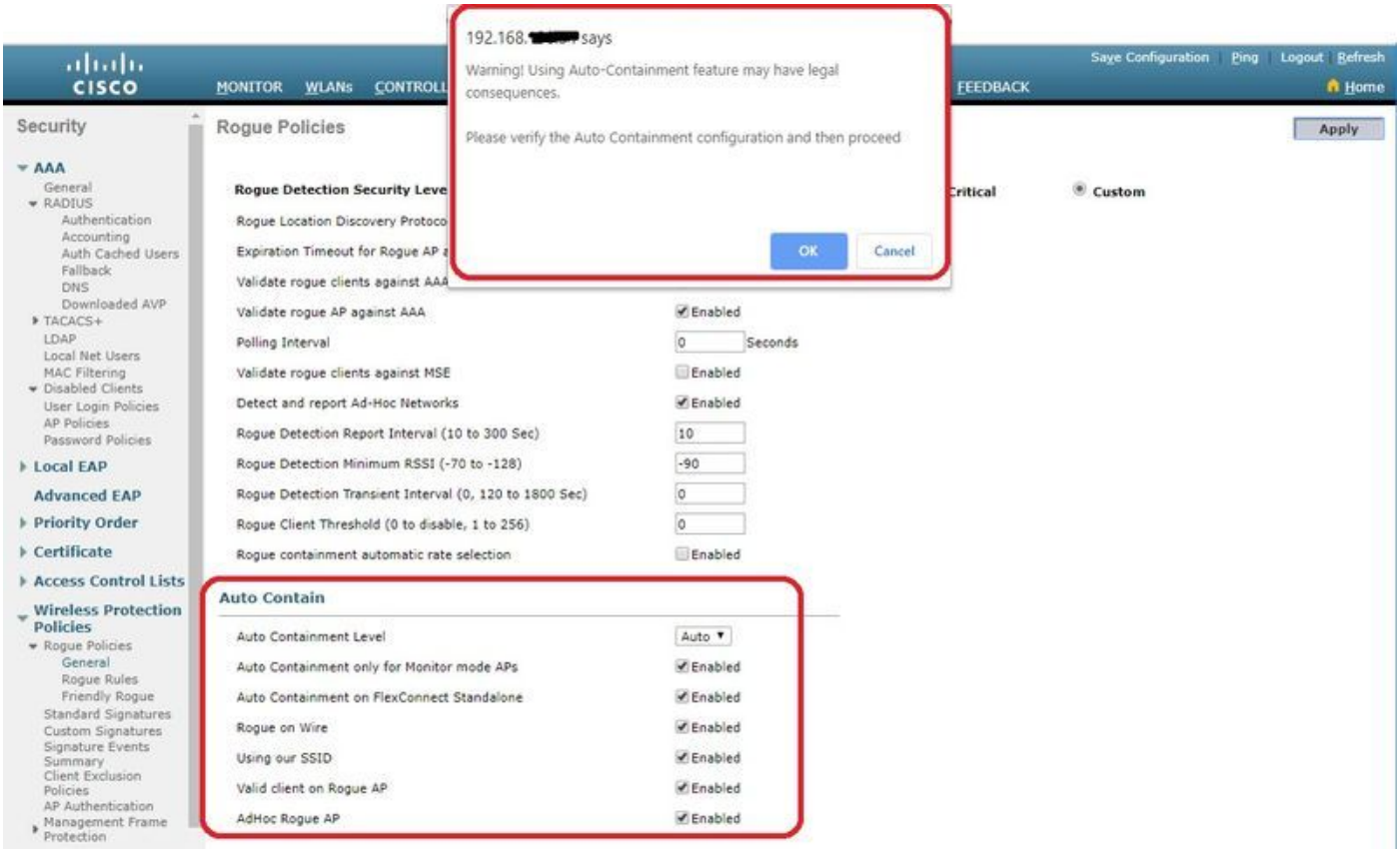
Wenn der Cisco WLC bestimmte nicht autorisierte Geräte automatisch enthalten soll, aktivieren Sie diese Kontrollkästchen. Lassen Sie andernfalls die Kontrollkästchen deaktiviert. Dies ist der Standardwert.

> **Warnung:** Wenn Sie einen dieser Parameter aktivieren, wird die Meldung angezeigt: "Die Verwendung dieser Funktion hat rechtliche Folgen. Möchten Sie fortfahren?" Die 2,4- und 5-GHz-Frequenzen im ISM-Band (Industrial, Scientific, and Medical) sind öffentlich zugänglich und können ohne Lizenz genutzt werden. Daher kann die Eindämmung der Geräte im

Netzwerk anderer Anbieter rechtliche Folgen haben.

Dies sind die Parameter zum automatischen Einschließen:

Parameter	Beschreibung
Auto-Containment-Ebene	Dropdown-Liste, aus der Sie die Stufe für die automatische Blockierung von unberechtigten Geräten zwischen 1 und 4 auswählen können. Sie können bis zu vier APs für die automatische Eindämmung auswählen, wenn ein unberechtigtes Gerät über eine der Richtlinien für die automatische Eindämmung in einen geschlossenen Zustand versetzt wird. Sie können auch Auto (Automatisch) auswählen, um die Anzahl der APs für die automatische Eindämmung auszuwählen. Der Cisco WLC wählt die erforderliche Anzahl an APs basierend auf dem RSSI aus, um eine effektive Eindämmung zu gewährleisten. Der RSSI-Wert, der jeder Eindämmungsebene zugeordnet ist, lautet wie folgt: • 1 - 0 bis -55 dBm • 2 - -75 bis -55 dBm • 3 - -85 bis -75 dBm • 4 - weniger als -85 dBm
Automatische Eindämmung nur für APs im Überwachungsmodus	Kontrollkästchen, das Sie auswählen können, um die Überwachungsmodus-APs für die automatische Eindämmung zu aktivieren. Standardmäßig ist diese Option deaktiviert.
Automatische Eindämmung bei eigenständiger FlexConnect-Lösung	Aktivieren Sie das Kontrollkästchen, um die automatische Eindämmung auf FlexConnect-APs im Standalone-Modus zu aktivieren. Standardmäßig ist diese Option deaktiviert. Wenn sich die FlexConnect-APs im Standalone-Modus befinden, können Sie nur die Auto-Containment-Richtlinien SSID oder AdHoc für nicht autorisierte APs verwenden aktivieren. Das Containment wird beendet, nachdem der eigenständige AP wieder mit dem Cisco WLC verbunden ist.
Nicht autorisiert an Draht	Aktivieren Sie dieses Kontrollkästchen, um die im kabelgebundenen Netzwerk erkannten unberechtigten Geräte automatisch einzuschließen. Standardmäßig ist diese Option deaktiviert.
SSID verwenden	Aktivieren Sie dieses Kontrollkästchen, um die unberechtigten Geräte automatisch einzuschließen, die die SSID Ihres Netzwerks melden. Wenn Sie diesen Parameter nicht auswählen, generiert der Cisco WLC nur dann einen Alarm, wenn ein solches unberechtigtes Gerät erkannt wird. Standardmäßig ist diese Option deaktiviert.
Gültiger Client auf nicht autorisiertem AP	Aktivieren Sie das Kontrollkästchen, um automatisch einen nicht autorisierten Access Point einzuschließen, dem vertrauenswürdige Clients zugeordnet sind. Wenn Sie diesen Parameter nicht auswählen, generiert der Cisco WLC nur dann einen Alarm, wenn ein solches unberechtigtes Gerät erkannt wird. Standardmäßig ist diese Option deaktiviert.
Nicht autorisierter AdHoc-AP	Aktivieren Sie dieses Kontrollkästchen, um automatisch Ad-hoc-Netzwerke einzuschließen, die vom Cisco WLC erkannt werden. Wenn Sie diesen Parameter nicht auswählen, generiert der Cisco WLC nur dann einen Alarm, wenn ein solches Netzwerk erkannt wird. Standardmäßig ist diese Option deaktiviert.



Klicken Sie auf Apply (Anwenden), um Daten an den Cisco WLC zu senden, die Daten bleiben jedoch während des Ein- und Ausschaltzyklus nicht erhalten. Diese Parameter werden vorübergehend im flüchtigen RAM gespeichert.

Über die 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
```

Mit Prime-Infrastruktur

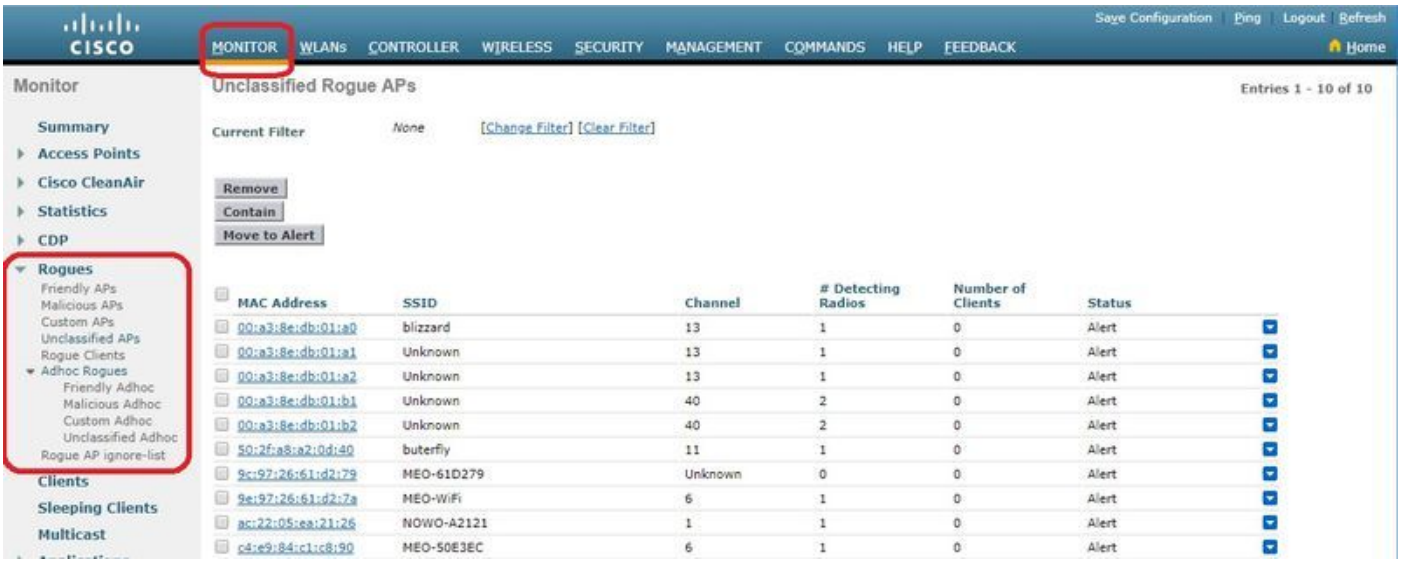
Die Cisco Prime-Infrastruktur kann zur Konfiguration und Überwachung eines oder mehrerer Controller und zugehöriger APs verwendet werden. Cisco PI verfügt über Tools zur Überwachung und Steuerung großer Systeme. Wenn Sie Cisco PI in Ihrer Cisco Wireless-Lösung verwenden, bestimmen Controller regelmäßig den Client, den nicht autorisierten Access Point, den nicht autorisierten Access Point-Client und den Standort der RFID-Tags und speichern die Standorte in der Cisco PI-Datenbank.

Die Cisco Prime-Infrastruktur unterstützt die regelbasierte Klassifizierung und nutzt die auf dem Controller konfigurierten Klassifizierungsregeln. Der Controller sendet Traps an die Cisco Prime-Infrastruktur, nachdem folgende Ereignisse aufgetreten sind:

- Wenn ein unbekannter Access Point zum ersten Mal in den Status "Freundlich" wechselt, sendet der Controller nur dann eine Trap an die Cisco Prime-Infrastruktur, wenn der Status "Unbefugter" "Alarm" lautet. Es sendet keine Falle, wenn der Zustand **intern** oder **extern** ist.
- Wenn nach Ablauf der Zeitüberschreitung ein Eintrag entfernt wird, sendet der Controller eine Trap an Cisco Prime-Infrastruktur für unautorisierte Access Points, die als **bösartig (**Warnung, Bedrohung) oder **unklassifiziert (**Warnung) kategorisiert sind. Der Controller entfernt keineLogeinträge mit den folgenden Gastegaten: **Enthalten, Ausstehend, Intern** und **Extern.**

Überprüfung

Um unberechtigte Details in einem Controller in der grafischen Benutzeroberfläche zu finden, navigieren Sie **zu Monitor > Unberechtigte**, wie im Bild dargestellt.

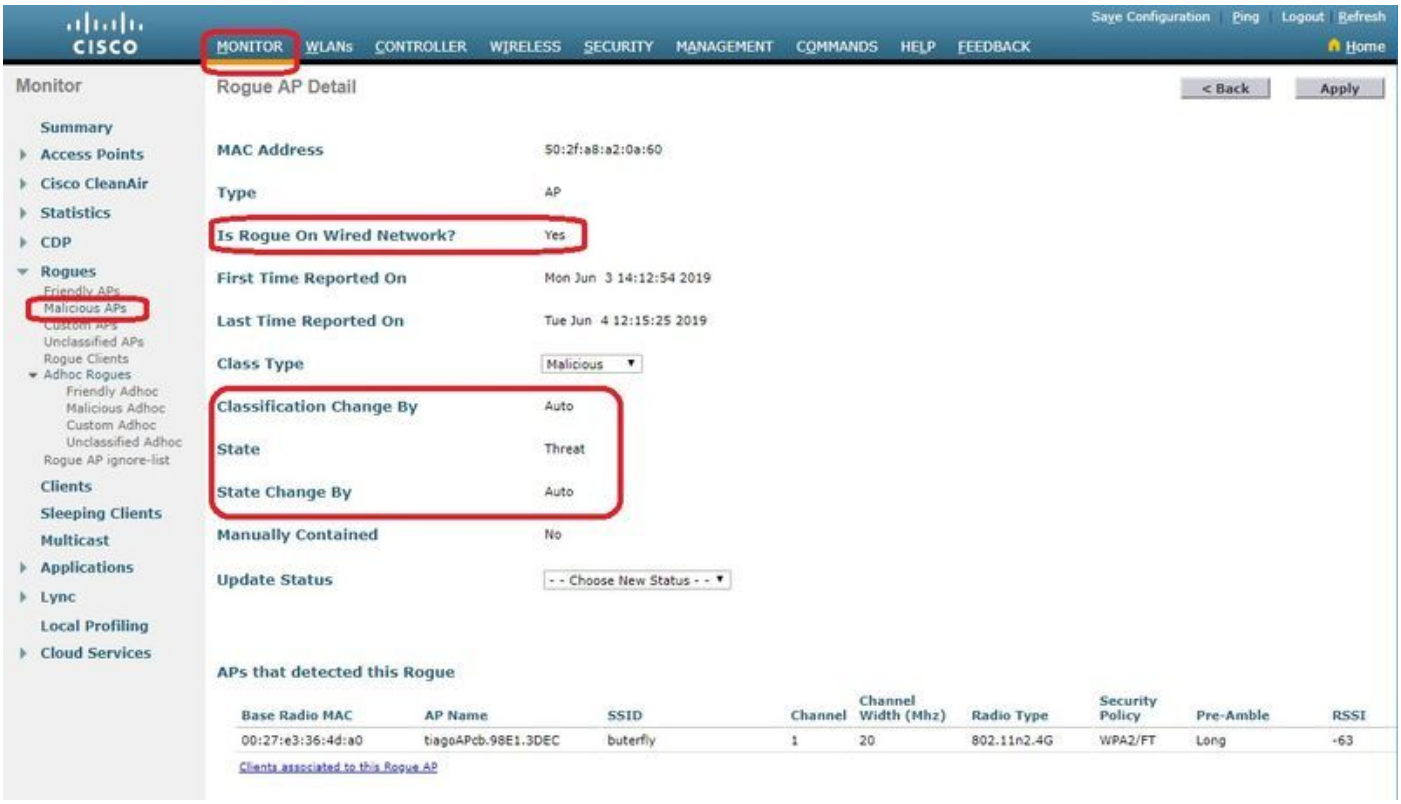


Auf dieser Seite finden Sie verschiedene Klassifizierungen für unberechtigte Benutzer:

- Benutzerfreundliche APs - APs, die vom Administrator als benutzerfreundlich markiert wurden.
- Schädliche APs - APs, die über RLDP oder Rogue Detection AP als schädlich identifiziert werden.
- Benutzerdefinierte APs - APs, die von nicht autorisierten Regeln als benutzerdefiniert klassifiziert werden.
- Nicht klassifizierte APs - Nicht autorisierte APs werden im Controller standardmäßig als nicht klassifizierte Liste angezeigt.
- Nicht autorisierte Clients - Mit nicht autorisierten APs verbundene Clients
- Adhoc-Schurken - Unberechtigte Adhoc-Clients.
- Ignorierliste für nicht autorisierte APs - Wie durch PI aufgeführt.

Anmerkung: Wenn der WLC und der autonome Zugangspunkt von derselben PI verwaltet werden, listet der WLC diesen autonome Zugangspunkt automatisch in der Ignorierliste für nicht autorisierte Zugangspunkte auf. Für diese Funktion ist keine zusätzliche Konfiguration in WLC erforderlich.

Klicken Sie auf einen bestimmten Rogue-Eintrag, um die Details dieses Rogue zu erhalten. Das folgende Beispiel zeigt eine Entdeckung nicht autorisierter APs in einem kabelgebundenen Netzwerk:



Über die 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
```

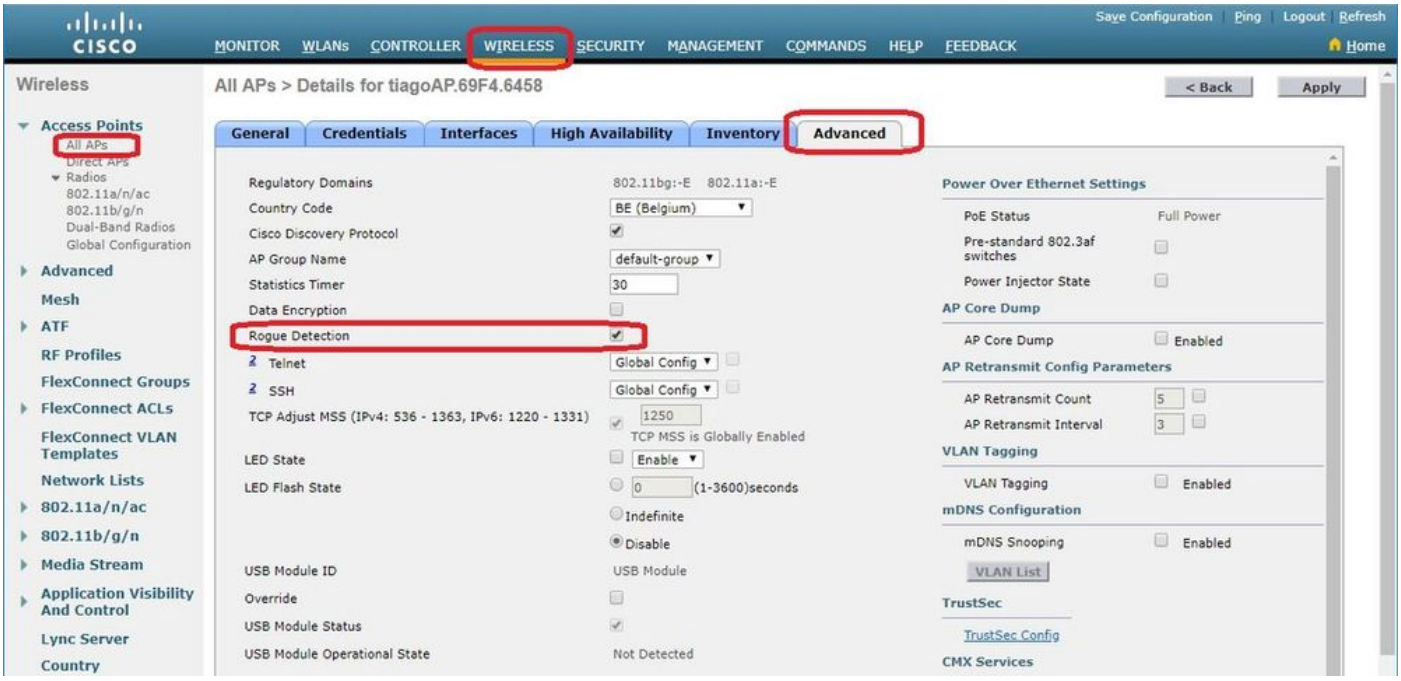
```
00:27:e3:36:4d:a0 -36    40
00:a3:8e:db:01:b2 Unclassified Alert               2    0       00:27:e3:36:4d:a0 -28    40
00:27:e3:36:4d:a0 -37    40
50:2f:a8:a2:0a:60 Malicious    Threat              1    2       00:27:e3:36:4d:a0 -66    1
50:2f:a8:a2:0d:40 Unclassified Alert               1    0       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
```

Fehlerbehebung

Wenn die nicht autorisierte Person nicht erkannt wird

Überprüfen Sie, ob die Erkennung von unberechtigten Geräten auf dem Access Point aktiviert ist.
Benutzeroberfläche:



In der 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
[...]
```

Die Erkennung nicht autorisierter APs kann mithilfe des folgenden Befehls aktiviert werden:

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

Ein AP im lokalen Modus scannt nur Länderkanäle/DCA-Kanäle und hängt von der Konfiguration ab. Befindet sich das unberechtigte Gerät in einem anderen Kanal, kann der Controller das

unberechtigte Gerät nicht identifizieren, wenn im Netzwerk keine APs im Überwachungsmodus vorhanden sind. Geben Sie diesen Befehl aus, um Folgendes zu überprüfen:

```
(Cisco Controller) >show advanced 802.11a monitor

Default 802.11a AP monitoring
  802.11a Monitor Mode.......................... enable
  802.11a Monitor Mode for Mesh AP Backhaul..... disable
  802.11a Monitor Channels..................... Country channels
  802.11a RRM Neighbor Discover Type............ Transparent
  802.11a RRM Neighbor RSSI Normalization....... Enabled
  802.11a AP Coverage Interval.................. 90 seconds
  802.11a AP Load Interval...................... 60 seconds
  802.11a AP Monitor Measurement Interval....... 180 seconds
  802.11a AP Neighbor Timeout Factor............ 20
  802.11a AP Report Measurement Interval........ 180 seconds
```

- Nicht autorisierter AP wird von der SSID nicht übertragen.
- Stellen Sie sicher, dass die MAC-Adresse des nicht autorisierten Access Points nicht in der benutzerfreundlichen Liste der nicht autorisierten Access Points hinzugefügt wurde oder über PI aufgelistet werden darf.
- Beacons des nicht autorisierten Access Points sind für den Access Point, der unautorisierte Access Points erkannt hat, nicht erreichbar. Dies kann durch die Erfassung der Pakete mit einem Sniffer in der Nähe des AP-Detektor Rogue überprüft werden.
- Ein AP im lokalen Modus kann bis zu 9 Minuten benötigen, um ein unberechtigtes Gerät zu erkennen (3 Zyklen, 180 x 3).
- Cisco APs sind nicht in der Lage, unberechtigte Funkfrequenzen wie den Kanal für öffentliche Sicherheit (4,9 GHz) zu erkennen.
- Cisco APs können keine unberechtigten Geräte erkennen, die mit FHSS (Frequency Hopping Spread Spectrum) arbeiten.

Nützliche Debugs

```
(Cisco Controller) >debug client
```

```
         (If rogue mac is known)
(Cisco Controller) >debug client 50:2f:a8:a2:0a:60

(Cisco Controller) >*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Found Rogue AP:
50:2f:a8:a2:0a:60 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, detectinglradtypes :20
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559724417.
Detecting lrad: 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 lrad: 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 lradInfo->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:c1, 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, detectinglradtypes :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 lrad: 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, detectinglradtypes :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 0xfff0617238

*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: buterfly

*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
0xfff0617238

*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
```

Erwartete Trap-Protokolle

Sobald ein unberechtigtes Gerät erkannt/aus der Liste entfernt wurde:

0	Mi 05 Jun 09:01:57 2019	Nicht autorisierter Client: b4:c0:f5:2b:4f:90 wird von 1 APs Rogue Client Bssid **erkannt**: a6:b1:e9:f0:e8:41, Status: Alert, Letzte Erkennung AP :00:27:e3:36:4d:a0 Rogue Client gate mac 00:00:00:02:02:02.
1	Mi 05 Jun 09:00:39 2019	Nicht autorisierter AP: 9c:97:26:61:d2:79 **entfernt** von Base Radio MAC: 00:27:e3:36:4d:a0 Schnittstellennummer:0(802.11n(2,4 GHz))
2	Mi 05.06.2019 08:53:39	Nicht autorisierter AP: 7c:b7:33:c0:51:14 **entfernt** von Base Radio MAC: 00:27:e3:36:4d:a0 Schnittstellennummer:0(802.11n(2,4 GHz))
3	Mi 05.06.2019 08:52:27	Nicht autorisierter Client: fc:3f:7c:5f:b1:1b wird von 1 APs Rogue Client Bssid **erkannt**: 50:2f:a8:a2:0a:60, Zustand: Alert, Letzte Erkennung AP :00:27:e3:36:4d:a0 Rogue Client gateway mac 00:26:44:73:c5:1d.
4	Mi	Nicht autorisierter AP: d4:28:d5:da:e0:d4 **entfernt** von Base Radio MAC: 00:27:e3:36:4d:a0

05.06.2019 08:52:17 Schnittstellennummer:0(802.11n(2,4 GHz))

Empfehlungen

1. Konfigurieren Sie den Kanalscan für alle Kanäle, wenn Sie potenzielle Unbefugte in Ihrem Netzwerk vermuten.
2. Die Anzahl und der Standort der Access Points von nicht autorisierten Access Points variieren von einem Standort pro Etage bis zu einem Access Point pro Gebäude und hängen vom Layout des kabelgebundenen Netzwerks ab. Es empfiehlt sich, in jedem Stockwerk eines Gebäudes mindestens einen Schurkendetektor AP zu haben. Da ein nicht autorisierter Access Point einen Trunk zu allen zu überwachenden Layer-2-Netzwerk-Broadcast-Domänen benötigt, hängt die Platzierung vom logischen Layout des Netzwerks ab.

Wenn die nicht autorisierte Person nicht klassifiziert ist

Überprüfen Sie, ob die nicht autorisierten Regeln richtig konfiguriert sind.

Nützliche Debugs

```
(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
```

Empfehlungen

Wenn Sie bekannte unautorisierte Einträge haben, fügen Sie diese in der angezeigten Liste hinzu, oder aktivieren Sie die Validierung mit AAA, und stellen Sie sicher, dass bekannte Clienteinträge in der AAA-Datenbank (Authentication, Authorization and Accounting) vorhanden sind.

RLDP findet keine unberechtigten Benutzer

- Befindet sich das unberechtigte Gerät im DFS-Kanal, funktioniert RLDP nicht.
- RLDP funktioniert nur, wenn das unautorisierte WLAN geöffnet ist und DHCP verfügbar ist.
- Wenn der Access Point im lokalen Modus den Client im DFS-Kanal bedient, ist er nicht am RLDP-Prozess beteiligt.
- RLDP wird von AP-Zugangspunkten der Serien 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800 und 3800 nicht unterstützt.

Nützliche Debugs

```
(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
```

Empfehlungen

1. Initiieren Sie RLDP manuell bei verdächtigen unbefugten Einträgen.
2. Planen Sie RLDP regelmäßig.
3. RLDP kann auf APs im lokalen oder Überwachungsmodus bereitgestellt werden. Bei den meisten skalierbaren Bereitstellungen und zur Vermeidung von Beeinträchtigungen des Client-Service muss RLDP nach Möglichkeit auf APs im Überwachungsmodus bereitgestellt werden. Für diese Empfehlung ist es jedoch erforderlich, dass ein Überwachungsmodus-AP-Overlay mit einem typischen Verhältnis von einem Überwachungsmodus-AP für jeweils fünf lokale Modus-APs bereitgestellt wird. APs im adaptiven wIPS-Überwachungsmodus können für diese Aufgabe ebenfalls verwendet werden.

AP zur Erkennung nicht autorisierter APs

Mit diesem Befehl in der AP-Konsole können Sie nicht autorisierte Zugriffe auf einen nicht autorisierten Detektor erkennen. Bei nicht autorisierten kabelgebundenen Geräten wird das Flag in den Status gesetzt.

```
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
```

Nützliche Debug-Befehle in einer AP-Konsole

```
Rogue_Detector#debug capwap rm rogue detector

*Jun 05 08:37:59.747: ROGUE_DET: Received a rogue table update of length 170
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac4
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac5
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1aca
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acb
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acc
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acd
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acf
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0024.1431.e9ef
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0024.148a.ca2b
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2d
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2f
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3570
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3574
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357b
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357c
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357d
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357f
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3dcd
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff0
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff2
*Jun 05 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4aec
*Jun 05 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4b77
*Jun 05 08:37:59.774: ROGUE_DET: Flushing rogue entry 0040.96b9.4794
*Jun 05 08:37:59.774: ROGUE_DET: Flushing rogue entry 0022.0c97.af80
*Jun 05 08:37:59.775: ROGUE_DET: Flushing rogue entry 0024.9789.5710
*Jun 05 08:38:19.325: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 05 08:38:19.325: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
*Jun 05 08:39:19.323: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 05 08:39:19.324: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
```

Blockierung nicht autorisierter APs

Erwartete Debugs

```
*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
```

Empfehlungen

1. Der Access Point im lokalen/Flex-Connect-Modus kann jeweils drei Geräte pro Funkeinheit enthalten, der Access Point im Überwachungsmodus kann jeweils sechs Geräte pro Funkeinheit enthalten. Stellen Sie deshalb sicher, dass der Access Point nicht bereits die maximal zulässige Anzahl an Geräten enthält. In diesem Szenario befindet sich der Client in einem ausstehenden Containment-Zustand.
2. Überprüfen der Regeln für die automatische Eindämmung

Schlussfolgerung

Die Erkennung und Eindämmung von nicht autorisierten APs in der zentralisierten Controller-

Lösung von Cisco ist die effektivste und unaufdringlichste Methode der Branche. Dank der Flexibilität, die der Netzwerkadministrator erhält, können alle Netzwerkanforderungen individuell angepasst werden.

Zugehörige Informationen

- Konfigurationsleitfaden für Cisco Wireless Controller, Version 8.8 - Verwaltung nicht autorisierter APs
- Cisco Wireless LAN Controller (WLC) - Best Practices für die Konfiguration
- WLC 3504 Version 8.5 - Bereitstellungsleitfaden
- Bereitstellungsleitfaden für Cisco 5520 Wireless LAN Controller
- Versionshinweise für Cisco Wireless Controller und Lightweight Access Points, Cisco Wireless Release 8.8.120.0

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.