حل مشكلات اكتشاف الأخطاء والتخفيف منها في شبكة السلكية موحدة

المحتويات

- المقدمة
- المتطلبات الأساسية
  - المتطلبات
  - المكونات المستخدمة
- نظرة عامة على المخادعين
  - اكتشاف المخادع
    - فحص خارج القناة
    - فحص وضع المراقبة
    - مقارنة بين الوضع المحلي ووضع الشاشة
    - التعرف على المخادع
    - تسجيلات مرام
    - التفاصيل المخادعة
    - تصدير الأحداث المراقبة
    - التمام مسجل الدخول
    - نقطة الوصول الكاشف المخادع
    - اعتبارات قابلية التوسع
  - RLDP
    - تحفظات RLDP
    - مسارات منفذ الهوك
  - تصنيف المراقبين
    - قواعد تصنيف المراقبين
  - HA قناة
  - قناة الاتصال المرن
- تخفيف مخاطر المخادعة
  - احتواء المخادعين
    - التفاصيل الاحتواء المخادعة
    - احتواء تلقائي
    - احتواء مرام
  - تشغيل منفذ الهوك القافية
- التكوين
  - تكوين الكشف عن الأخطاء
    - تكوين الماسح الضوئي للقناة الاكتشاف المخادع
  - تكوين تصنيف المخادع
  - تكوين تخفيف الأخطاء
    - تكوين الاحتواء اليدوي
    - احتواء تلقائي
- مع البنية الأساسية ل Prime
- التحقق من الصحة
- استكشاف الأخطاء وإصلاحها
  - إذا لم يتم اكتشاف الهوك

- تصحيح الأخطاء المفيدة
- سجلات الأحداث المتوقعة
- توصيات

إذا كان الوغد غير مصنف

- تصحيح الأخطاء المفيدة
- توصيات

برنامج RLDP يقوم بحجب الوغد الأول

- تصحيح الأخطاء المفيدة
- توصيات

عملاء المخادعين الذين يحاولون الوصول إلى نقطة الوصول (AP)

- تصحيح الأخطاء المفيدة في وحدة تحكم نقطة الوصول
- توصيات

محاولات المخادعين

- تصحيح الأخطاء المتوقعة
- توصيات

المرفقات

معلومات ذات صلة

المقدمة

يصف هذا وثيقة كشف الأخطاء والتخفيف من آثارها على شبكات Cisco اللاسلكية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- وحدات التحكم في شبكة LAN اللاسلكية من Cisco.
- البنية الأساسية ل Cisco Prime.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- وحدات التحكم في الشبكة المحلية (LAN) اللاسلكية الموحدة من Cisco (السلسل 3504 و 8540 و 5520) التي تشغل الإصدار 8.8.120.0.
- نقاط الوصول من السلسلة 1832 و 1852 و 2802 و 3802.
- نقاط الوصول من السلسلة 1700 و 2700 و 3700 من الموجة 1.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

نظرة عامة على المخادعين

توسع الشبكات اللاسلكية الشبكات السلكية وتزيد من إنتاجية العاملين والوصول

إلى المعلومات. ومع ذلك، تمثل الشبكة اللاسلكية غير المصرح بها طبقة إضافية من المخاطر الأمنية. مع تقليل التفكير في أمان المنفذ على الشبكات السلكية، تعد الشبكات اللاسلكية امتدادا سهلا للشبكات السلكية. وبالتالي، فإن الموظف الذي يحضر نقطة الوصول الخاصة به (Cisco أو غير Cisco) إلى بنية أساسية السلكية أو سلكية مؤمنة بشكل جيد ويسمح للمستخدمين غير المصرح لهم بالوصول إلى هذه الشبكة التي كانت مؤمنة بشكل آخر، يمكنه بسهولة أختراق شبكة آمنة.

يتيح الكشف المخادع لمسؤول الشبكة إمكانية مراقبة مشكلة الأمان هذه والقضاء عليها. توفر بنية الشبكة الموحدة من Cisco طرقا للكشف المخادع التي تتيح الحماية الكاملة للتعرية والاحتواء المخادعين دون الحاجة إلى شبكات وأدوات تغشية مكلفة يصعب تبريرها.

يمكن إعتبار أي جهاز يشارك طيفك والتي تمت إدارته من قبلك على أنه مخادع. ويصبح الوغد خطيرا في مثل هذه السيناريوهات:

- عند الإعداد استخدام نفس معرف مجموعة الخدمة (SSID) مثل شبكتك (قاعدة عسل)
- عند اكتشافه على الشبكة السلكية
- عرائس مخصصة
- عند إعداده من قبل شخص من الخارج، في معظم الأحيان، بنية خبيثة

وأفضل الممارسات هي إستخدام الكشف عن المرقين للتقليل إلى أدنى حد من المخاطر الأمنية، مثل، في بيئة الشركات.

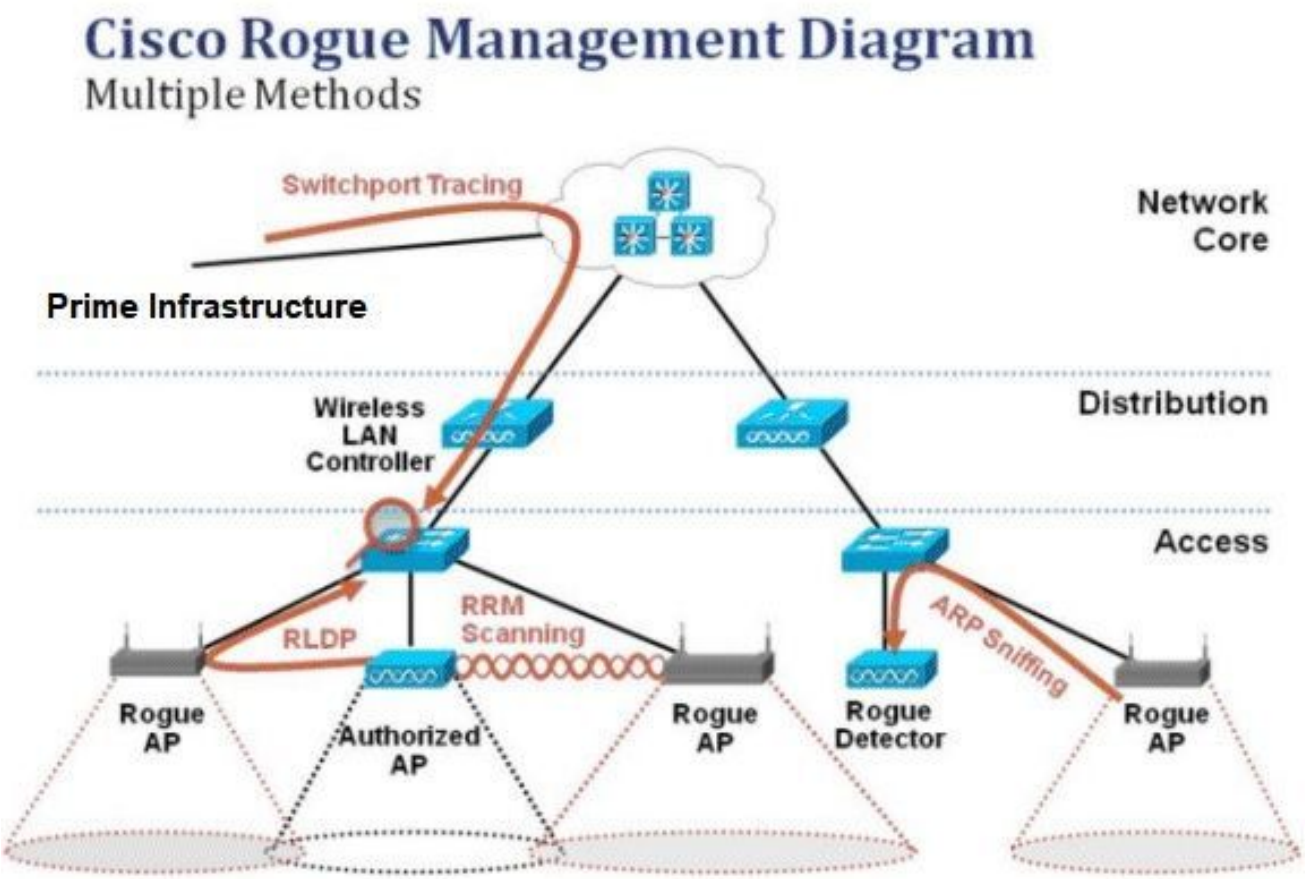
ومع ذلك، هناك سيناريوهات معينة ال تحتاج فيها إلى الكشف عن المخادع، على سبيل المثال، في نشر Office Extend Access Point (OEAP) وفي جميع أنحاء المدينة وفي الأماكن الخارجية.

إن إستخدام نقاط وصول الشبكة العنكبوتية الخارجية للكشف عن المخادعين لن يقدم قيمة كبيرة في حين أنه سوف يستخدم الموارد للتحليل.

وأخيرا، من الأهمية بمكان تقييم (أو تجنب الاحتواء التلقائي المحتشم بالكامل)، لأن هناك قضايا قانونية ومسؤوليات قانونية محتملة إذا تركت للعمل بشكل تلقائي.

هناك ثالث مراحل رئيسية لإدارة الأجهزة المخادعة في حل الشبكة اللاسلكية الموحدة (UWN) من Cisco:

- الكشف - يتم إستخدام فحص إدارة الموارد اللاسلكية (RRM) لاكتشاف وجود أجهزة مخادعة.
- التصنيف - يتم إستخدام بروتوكول اكتشاف الموقع الدوار (RLDP)، أو اكتشاف الدجل (نقاط الوصول (AP) من الموجة 1 فقط) وتوابع منافذ المحول لتحديد ما إذا كان الجهاز الدخيل متصال بالشبكة السلكية. كما تساعد قواعد تصنيف المرقين في ترشيح المرقين إلى فئات محددة استنادا إلى خصائصهم.
- التخفيف - يتم إستخدام إغالق منافذ المحول والموقع الدوار والاحتواء الدوار لتعقب موقعها الفعلي وإبطال تهديد الجهاز الدجال.

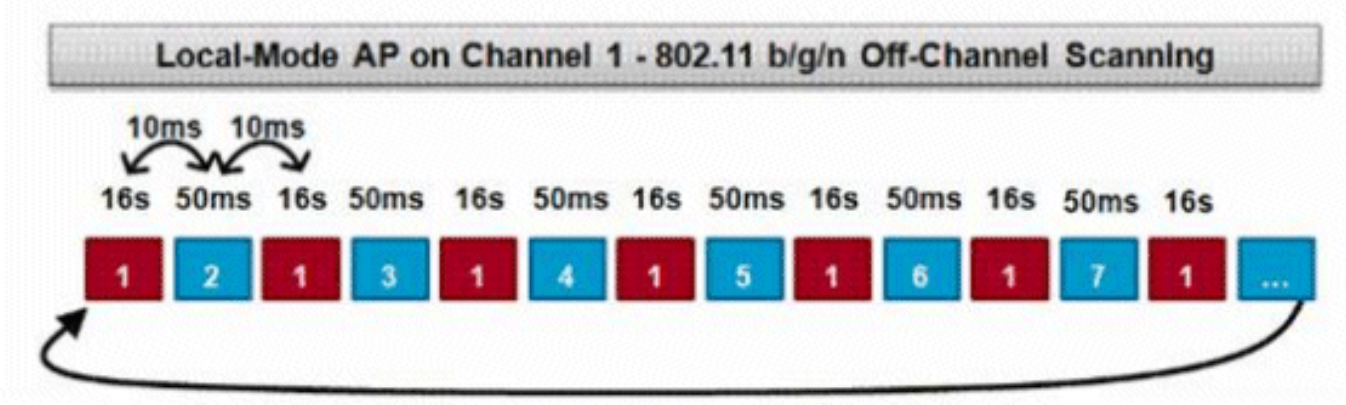


اكتشاف المخادع

المخادع أساسا وه أي جهاز يشارك طيفك، لكنه ليس تحت سيطرتك. ويتضمن ذلك نقاط الوصول الدخيلة والموجهات اللاسلكية والعملاء المخادعين وشبكات ألأقران المخادعة. يستخدم UWN من Cisco عددا من الطرق لاكتشاف ألأجهزة المخادعة المستندة إلى شبكة Wi-Fi مثل المسح الضوئي خارج القناة وإمكانات وضع الشاشة المخصصة. كما يمكن إستخدام Cisco Spectrum Expert لتحديد ألأجهزة المخادعة التي لا تستند إلى بروتوكول 802.11، مثل جسور Bluetooth.

فحص خارج القناة

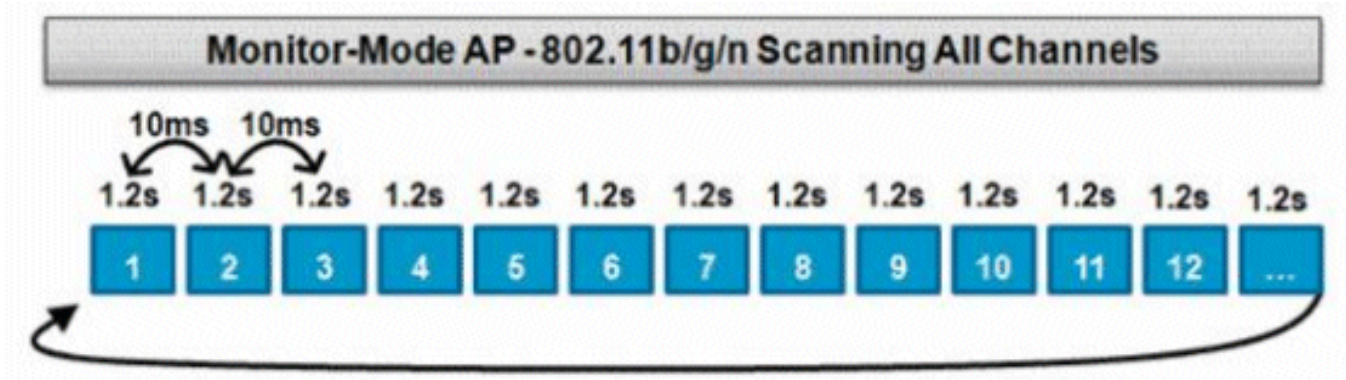
يتم تنفيذ هذه العملية بواسطة نقاط الوصول في الوضع المحلي و Flex-Connect (في الوضع المتصل) وتستخدم تقنية تقسيم الوقت التي تتيح خدمة العميل وفحص القناة، باستخدام نفس الراديو. مع القناة لمدة 50 ملي ثانية كل 16 ثانية، يقضي نقطة الوصول تنفق بشكل افتراضي نسبة صغيرة فقط من وقتها لعدم خدمة العملاء. لاحظ أيضا أن هناك فترة تغيير قناة 10 ملي ثانية تحدث. في الفاصل الافتراضي للمسح الضوئي من 180 ثانية، يتم مسح كل قناة 2.4 جيجاهيرتز FCC (1–11) ضوئيا مرة واحدة على ألأقل. بالنسبة للمجالات التنظيمية ألأخرى، مثل ETSI، تكون نقطة الوصول خارج القناة لنسبة مئوية أعلى قليلا من الوقت. يمكن ضبط كل من قائمة القنوات وفترة المسح الضوئي في تكوين RRM. وهذا يؤدي إلى تحديد تأثير ألأداء بحد أقصى 1.5٪، كما يتم تضمين ميزة الذكاء في الخوارزمية لإيقاف الفحص مؤقتا عندما تكون هناك حاجة لتسليم إطارات جودة الخدمة ذات ألأولوية العالية، مثل الصوت.



هذا الرسم هو وصف لخوارزمية المسح الضوئي خارج القناة لنقطة الوصول في الوضع المحلي في مدى الموجات 2.4 جيجاهيرتز. وتتم عملية مماثلة بالتوازي على جهاز الراديو بتردد 5 جيجاهيرتز إذا كان لدى نقطة الوصول حضور واحد. كل مربع أحمر يمثل الوقت المصروف على قناة APs الرئيسية، بينما كل مربع أزرق يمثل الوقت المصروف على القنوات المجاورة لأغراض المسح.

فحص وضع المراقبة

يتم تنفيذ هذه العملية بواسطة نقاط الوصول في وضع الشاشة Monitor Mode و Adaptive WIPS Monitor Mode APs التي تستخدم 100٪ من وقت الراديو لمسح جميع القنوات في كل نطاق ترددي خاص. وهذا يتيح سرعة اكتشاف أكبر ويتيح قضاء وقت أكبر على كل قناة. تكون نقاط الوصول في وضع المراقبة أيضا متفوقة على اكتشاف العملاء المخادعين حيث إن لديهم طريقة عرض أكثر شمولا للنشاط الذي يحدث في كل قناة.



هذا الرسم هو وصف لخوارزمية المسح الضوئي خارج القناة لنقطة الوصول في وضع جهاز العرض في مدى الموجات 2.4 جيجاهيرتز. وتتم عملية مماثلة بالتوازي على جهاز الراديو بتردد 5 جيجاهيرتز إذا كان لدى نقطة الوصول حضور واحد.

مقارنة بين الوضع المحلي ووضع الشاشة

تقسم نقطة الوصول للوضع المحلي دوراتها بين خدمة عملاء WLAN ومسح القنوات بحثا عن التهديدات. نتيجة لذلك، تستغرق نقطة الوصول في الوضع المحلي وقتا أطول للدوران عبر جميع القنوات، كما تنفق وقتا أقل في بيانات التجميع على أي قناة معينة حتى لا تتم تعطيل عملاء العميل. ونتيجة لذلك، تكون أوقات رصد الهجمات والشجارات أطول (من 3 إلى 60 دقيقة) ويمكن اكتشاف نطاق أصغر من الهجمات التي تتم عبر الهواء مقارنة مع

نقطة الوصول في وضع الشاشة.

علاوة على ذلك، فإن الكشف عن حركة المرور المتقطعة، مثل العملاء المخادعين، أقل تحديدا لأن نقطة الوصول (AP) يجب أن تكون على قناة حركة المرور في نفس الوقت الذي يتم فيه إرسال حركة المرور أو استقبالها. يصبح هذا تمرينا على الاحتمالات. تقضي نقطة الوصول الخاصة بوضع الشاشة جميع دوراتها على مسح القنوات للبحث عن المخادعين والهجمات التي تتم عبر الهواء. يمكن إستخدام نقطة الوصول الخاصة بوضع جهاز العرض في نفس الوقت لخدمات وضع جهاز العرض القابل للتكيف والموقع (مع مراعاة السياق) وخدمات وضع جهاز العرض الأخرى.

عندما يتم نشر نقاط الوصول في وضع المراقبة، تكون الفوائد أقل وقت للكشف. عندما يتم تكوين نقاط الوصول في وضع المراقبة بشكل إضافي باستخدام نظام منع الاختراقات (WIPS) القابل للتكيف، يمكن اكتشاف نطاق أوسع من التهديدات والهجمات عبر الهواء.

نقاط الوصول إلى الوضع المحلي	نقاط الوصول إلى وضع جهاز العرض
يخدم العملاء من خلال ميزة تقسيم الوقت بالمسح الضوئي خارج القناة	مسح ضوئي مخصص
يتم الآن الاستماع إلى 50 مللي ثانية على كل قناة	يستمع لـ 1.2s على كل قناة
قابل للتهيئة للمسح: • كافة القنوات • قنوات البلد (الافتراضي) • قنوات DCA	مسح كل القنوات

التعرف على المخادع

إذا تم الاستماع إلى إستجابة المسبار أو أجهزة الإرشاد من جهاز مخادع من قبل نقاط وصول (APs) محلية أو ذات اتصال مرن وأن في وضع المراقبة، حينئذ يتم توصيل هذه المعلومات عبر CAPWAP إلى وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) للعميل. لمنع الإيجابيات الخاطئة، يتم إستخدام عدد من الطرق لضمان عدم تعريف نقاط الوصول الأخرى المدارة المستندة إلى Cisco على أنها جهاز مخادع. وتتضمن هذه الطرق تحديثات مجموعة التنقل وحزم RF المجاورة ونقاط الوصول (AP) المألوفة للقائمة المسموح بها عبر البنية الأساسية الأساسية الأساسية لـ Prime (PI).

تسجيلات مارقة

في حين أن قاعدة بيانات الجهاز الداوار الخاصة بوحدة التحكم تحتوي فقط على المجموعة الحالية من المخادع التي تم اكتشافها، فإن pi تتضمن أيضا سجل حدث ومراوغات سجل لم

تعد مرئية.

التفاصيل المخادعة

تقوم نقطة الوصول CAPWAP بالانتقال خارج القناة لمدة 50 مللي ثانية للاستماع إلى العملاء المخادعين والمراقبة بحثا عن الوضوء وتادخل القنوات. يتم إرسال أي عملاء مخادعين تم اكتشافهم إلى وحدة التحكم، والتي تجمع المعلومات التالية:

- عنوان MAC لنقطة الوصول المخادعة
- اسم نقطة الوصول التي تم الكشف عنها كشخص مارق
- عنوان MAC الخاص بالعميل (العملاء) المتصل المخادع
- سياسة أمنية
- الديباجة
- نسبة الإشارة إلى الضوضاء (SNR)
- مؤشر قوة إشارة المستقبل (RSSI)
- قناة كشف الدجل
- الراديو الذي يتم فيه الكشف عن وجود مارق
- SSID المخادع (في حالة بث SSID المخادع)
- عنوان IP المخادع
- أول آخر مرة يتم الإبلاغ عن الوغد
- عرض القناة

لتصدير الأحداث المارقة

من أجل تصدير الأحداث المخادعة إلى نظام إدارة شبكة جهة خارجية (NMS) للأشفة، تسمح وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) بإضافة مستقبلات مصيدة SNMP. عندما يتم اكتشاف وأ مسح أحد المخادع بواسطة وحدة التحكم، يتم توصيل المعلومات التي تحتوي على هذه المعلومات إلى جميع مستقبلات مصيدة SNMP. واحد تذكير مع تصدير الأحداث عبر SNMP وهو أنه إذا كشفت وحدات التحكم المتعددة عن نفس المخادع، فإن الأحداث المكررة يتم رؤيتها بواسطة NMS حيث يتم عمل الارتباط فقط عند PI.

انتهاء مهلة السجل الدخيلة

بمجرد إضافة نقطة وصول مخادعة إلى سجلات عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، تبقى هناك حتى ال تعود مرئية. بعد مهلة قابلة للتكوين من قبل المستخدم (1200 ثانية بشكل افتراضي)، انتهت صالحية مارق في الفئة_unclassified_.

تستمر الأوغاد في الدول الأخرى مثل_CONTAINED_و_FRIENDLY_ حتى يتم تطبيق

التصنيف المناسب عليهم في حالة إعادة ظهورهم.

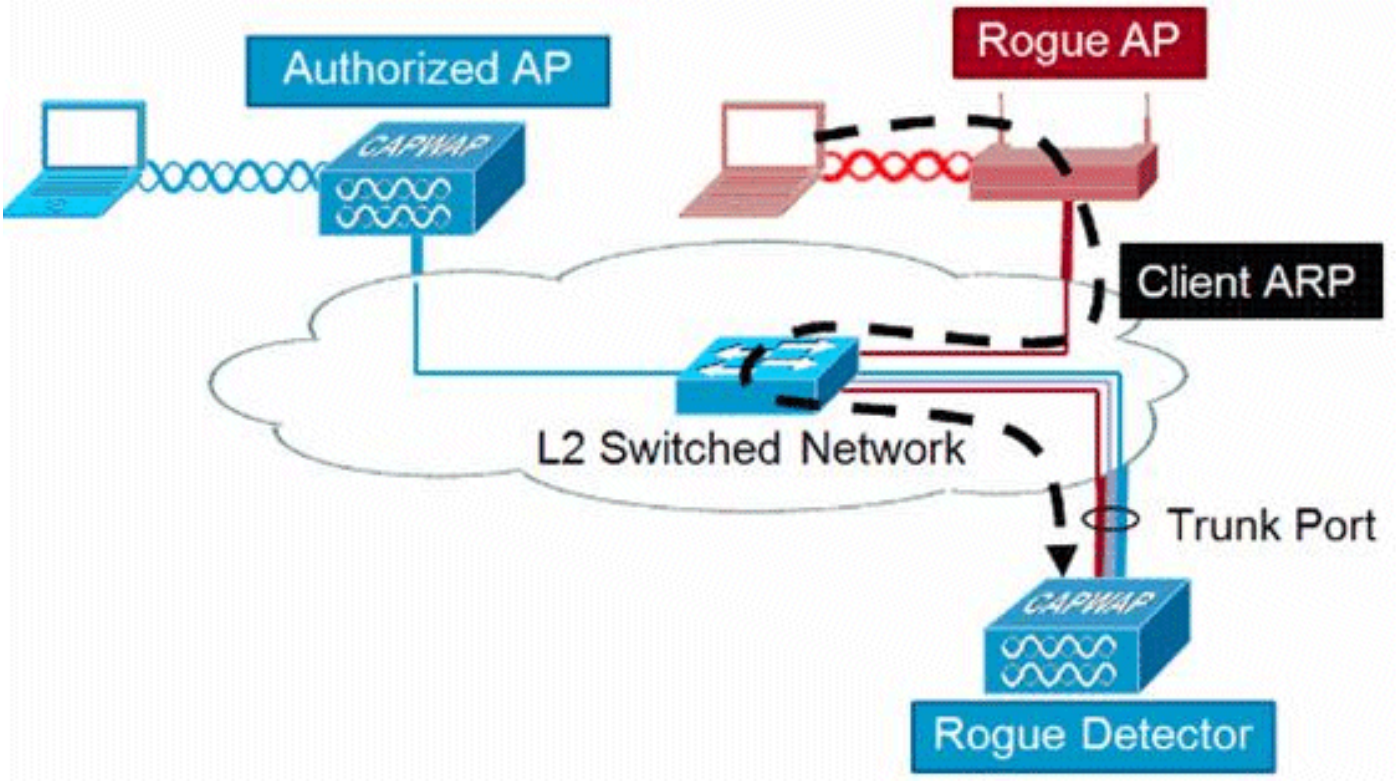
هناك الحد الأقصى لحجم قاعدة البيانات للسجلات المخادعة التي تتغير عبر الأنظمة الأساسية لوحدة التحكم:

- 3504 - اكتشاف واحتواء ما يصل إلى 600 نقطة وصول دخيلة و 1500 عميل مخادع
- 5520 - اكتشاف ما يصل إلى 24000 نقطة وصول دخيلة و 32000 عميل مارق واحتوائهم
- 8540 - اكتشاف ما يصل إلى 24000 نقطة وصول دخيلة و 32000 عميل مارق واحتوائهم

نقطة الوصول الكاشف المخادع

تهدف نقطة وصول (AP) لمقارنة المعلومات المخادعة التي يتم الحصول عليها عبر الهواء بمعلومات بروتوكول تحليل العناوين (ARP) التي يتم الحصول عليها من الشبكة السلكية. إذا تم سماع عنوان MAC عبر الهواء على أنه نقطة وصول أو عميل مخادع وتم سماعه أيضا على الشبكة السلكية، فإن المخادع سيتم تحديدها لتكون على الشبكة السلكية. إذا تم اكتشاف وجود المخادع على الشبكة السلكية، فسيتم رفع مستوى خطورة التنبيه الخاص بنقطة الوصول المخادعة إلى_critical_. نقطة الوصول الخاصة بمكتشف المخادع غير ناجحة في التعرف على العملاء المخادعين خلف جهاز يستخدم NAT.

يستخدم هذا الأسلوب عندما يكون لنقطة الوصول المخادعة شكل من أشكال المصادقة، إما WEP أو WPA. عندما يتم تكوين نموذج مصادقة على نقطة وصول (AP) مخادعة، لا يمكن لنقطة الوصول في الوضع Lightweight القارنة لأنها لا تعرف أسلوب المصادقة وبيانات الاعتماد التي تم تكوينها على نقطة الوصول (AP) المخادعة.



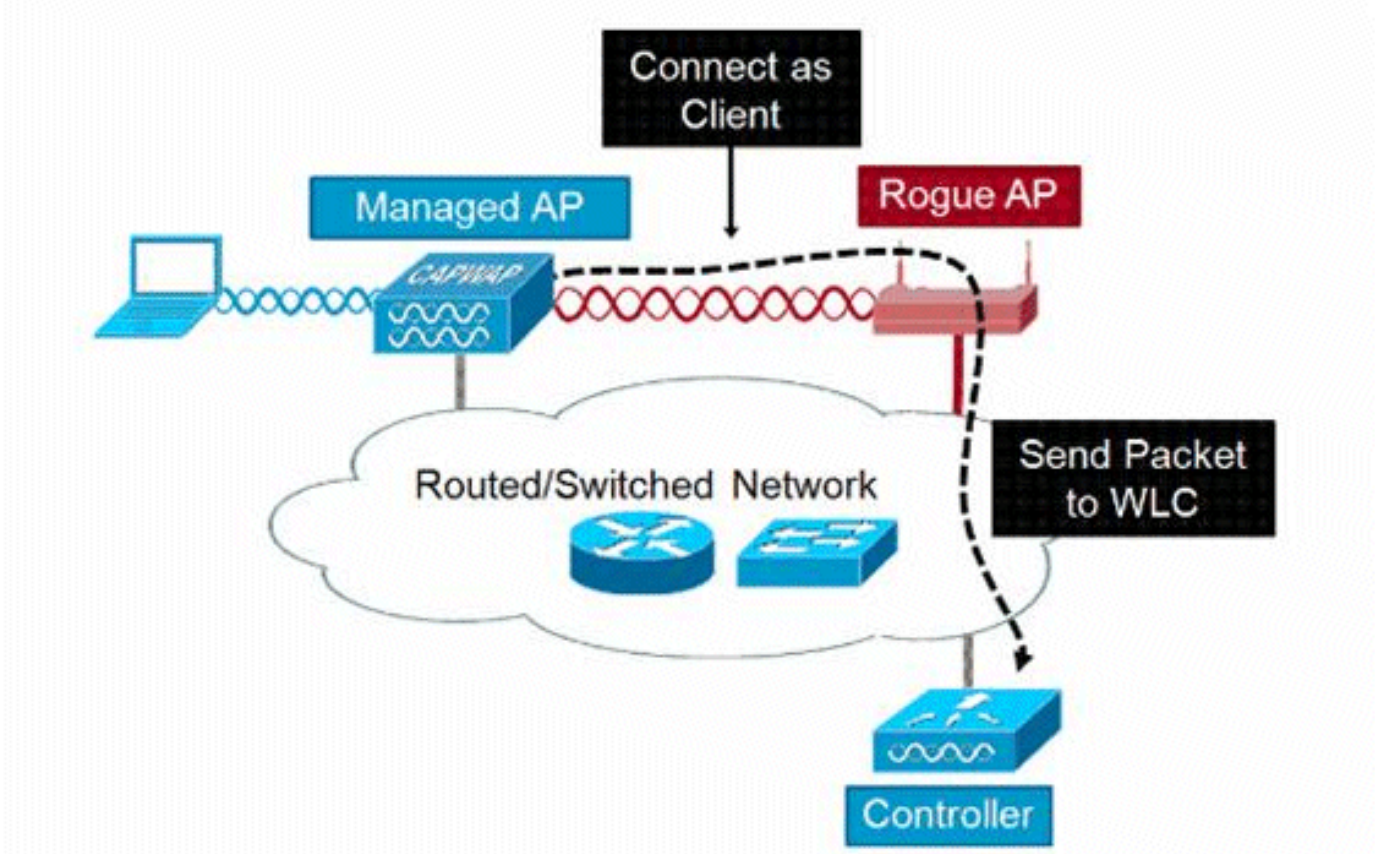
ملاحظة: يمكن تكوين نقاط الوصول من الموجة 1 فقط كأجهزة كشف مخادعة.

اعتبارات قابلية التوسعة

يمكن لنقطة الوصول المخادعة اكتشاف ما يصل إلى 500 مخادع و 500 عميل مخادع. إذا تم وضع جهاز الكشف المخادع على خط اتصال يحتوي على العديد من الأجهزة المخادعة، فإنه يتم تجاوز هذه الحدود، مما يتسبب في حدوث مشاكل. لمنع حدوث هذا، احتفظ بنقاط الوصول للمكتشف الدوار في طبقة التوزيع أو الوصول في شبكتك.

RLDP

يهدف بروتوكول RLDP إلى تحديد ما إذا كانت نقطة وصول (AP) مخادعة معينة متصلة بالبنية الأساسية السلكية. تستخدم هذه الميزة بشكل أساسي أقرب نقطة وصول (AP) للاتصال بالجهاز الدوار كعميل السلكي. بعد الاتصال كعميل، يتم إرسال حزمة مع عنوان الوجهة الخاص بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) لتقييم ما إذا كانت نقطة الوصول متصلة بالشبكة السلكية. في حالة اكتشاف وجود المخادع على الشبكة السلكية، يتم رفع مستوى خطورة التنبيه لنقطة الوصول المخادعة هذه إلى مستوى خطير.



يتم سرد خوارزمية RLDP هنا:

1. التعرف على أقرب نقطة وصول موحدة إلى المخادع باستخدام قيم قوة الإشارة.

2. بعد ذلك تتصل نقطة الوصول بالمخالف كعميل لشبكة WLAN، وتدخل ثالث جمعيات قبل أن ينتهي الوقت.

3. إذا نجح الاقتران، فإن ap يستعمل DHCP أن ينال عنوان.

4. إذا تم الحصول على عنوان IP، فإن نقطة الوصول (التي تعمل كعميل WLAN) ترسل حزمة UDP إلى كل عنوان IP لوحدة التحكم.

5. إذا تلقت وحدة التحكم حزمة واحدة من حزم RLDP من العميل، فيتم وضع علامة على هذا الشخص المخادع كجهاز متصل بالأسلاك مع خطورة بالغة.

ملاحظة: يتعذر على حزم RLDP الوصول إلى وحدة التحكم في حالة وجود قواعد التصفية بين شبكة وحدة التحكم والشبكة التي يوجد بها الجهاز الدوار.

تحفظات RLDP

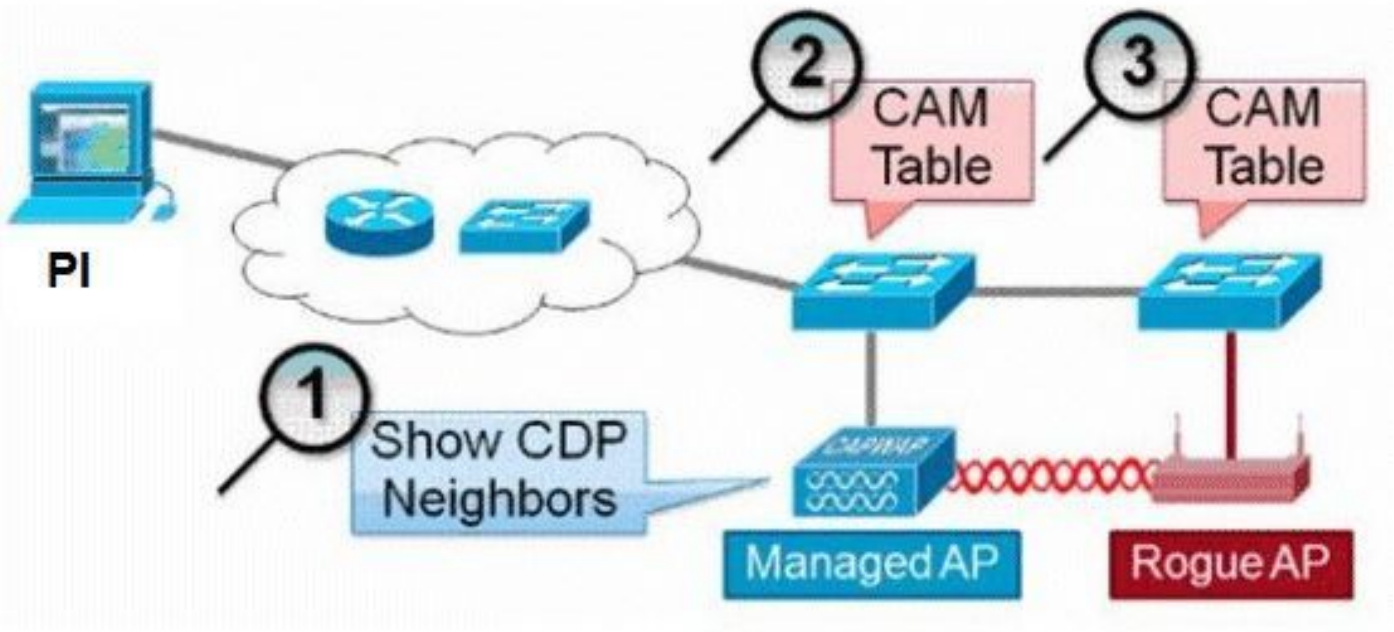
- يعمل بروتوكول RLDP فقط مع نقاط الوصول المخادعة المفتوحة التي تبث SSID الخاصة بها مع تعطيل المصادقة والتشفير.
- يتطلب RLDP أن تكون نقطة الوصول المدارة التي تعمل كعميل قادرة على الحصول على عنوان IP عبر DHCP على الشبكة المخادعة
- يمكن إستخدام RLDP اليدوي لمحاولة تتبع RLDP على مارق عدة مرات.
- في عملية RLDP، يتعذر على نقطة الوصول (AP) خدمة العملاء. يؤثر هذا سلبا على الأداء والاتصال لنقاط الوصول في الوضع المحلي.
- لا يحاول بروتوكول RLDP الاتصال بنقطة وصول مخادعة تعمل في قناة DFS بسرعة 5 جيجاهرتز.

مسارات منفذ المحول

تتبع منفذ المحول هو تقنية تخفيف نقطة الوصول المخادعة. وعلى الرغم من أنه يتم بدء تتبع منفذ المحول في PI، إلا أنه يستخدم معلومات بروتوكول CDP وبروتوكول SNMP على حد سواء لتعقب مرور البيانات نزولا إلى منفذ معين في الشبكة.

لكي يتم تشغيل تتبع منفذ المحول، يجب إضافة جميع المحولات في الشبكة إلى PI باستخدام بيانات اعتماد SNMP. على الرغم من أن بيانات الاعتماد للقراءة فقط تعمل لتعريف المنفذ الذي يتم تشغيله في الشاشة المارقة، إلا أن بيانات الاعتماد للقراءة والكتابة تسمح لشركة PI بإيقاف تشغيل المنفذ أيضا، وبالتالي فهي تحتوي على التهديد.

في هذا الوقت، تعمل هذه الميزة فقط مع محولات Cisco التي تشغل برنامج Cisco IOS® مع تمكين CDP، كما يجب تمكين CDP على نقاط الوصول (APs) المدارة.



يتم سرد خوارزمية تتبع منفذ المحول هنا:

1. ويجد بروتوكول الإنترنت (PI) أقرب نقطة وصول، والتي تكتشف نقطة الوصول المخادعة عبر الهواء، وتسترجع جاراتها في بروتوكول CDP.

2. وبعد ذلك يستخدم PI بروتوكول SNMP لفحص جدول CAM داخل المحول المجاور، فيبحث عن تطابق إيجابي لتحديد موقع المخادع.

3. – تعتمد التطابق الإيجابي على عنوان MAC المخادع تمامًا، +1/1 عنوان MAC المخادع، أي عناوين MAC للعملاء المخادعين، أو تطابق WI استنادًا إلى معلومات المورد المتأصلة في عنوان MAC.

4. إن لم يعثر على تطابق إيجابي على أقرب مفتاح، لـ PI يواصل البحث في مجاور مفتاح إلى إثنان حركة بعيدًا (افتراضيًا).

Wired-Side Tracing Techniques
Comparison

	How it Works	What It Detects	Accuracy
Switchport Tracing	1. AP hears rogue over air 2. Detecting AP advises of nearby switches 3. Trace starts on nearby switches 4. Results reported in order of probability 5. Administrator may disable port	•Open APs •Secured APs •NAT APs	•Moderate
RLDP	1. AP hears rogue over air 2. Detecting AP connects as client to rogue AP 3. Detecting AP sends RLDP packet 4. If RLDP packet seen at WLC, then on wire	•Open APs •NAT APs	•100%
Rogue Detector	1. Place detector AP on trunk 2. Detector receives all rogue MACs from WLC 3. Detector AP matches rogue MACs from wired-side ARPs	•Open APs •Secured APs •NAT APs	•High

تصنيف المارقين

بشكل افتراضي، يتم إعتبار جميع الأخطاء التي تم الكشف عنها بواسطة UWN من Cisco غير مصنفة. كما هو موضح في هذا الرسم، يمكن تصنيف الأخطاء بناء على عدد من المعايير التي تتضمن RSSI و SSID ونوع الأمان وتشغيل/إيقاف الشبكة وعدد من العملاء:

قواعد تصنيف المرافق

قواعد التصنيف المخادعة، تسمح لك بتعريف مجموعة من الشروط التي تميز المخادع على أنه راض أو ودي. يتم تكوين هذه القواعد في PI أو WLC، ولكنها يتم تنفيذها دائما على وحدة التحكم عند اكتشاف مخادع جديدة.

أقرأ [تصنيف المراوغة المستند إلى قاعدة المستندات في وحدات التحكم في الشبكة المحلية اللاسلكية (WLC) والبنية الأساسية الأساسية (PI)](#) للحصول على مزيد من المعلومات حول القواعد المخادعة في وحدات التحكم في الشبكة المحلية اللاسلكية (WLC).

حقائق HA

إذا قمت بنقل أي جهاز مخادع يدويا إلى حالة محتواة (أي فئة) أو حالة سهلة، يتم تخزين هذه المعلومات في ذاكرة Cisco WLC flash الاحتياطية، ومع ذلك، ال يتم تحديث قاعدة البيانات. عندما يحدث تبديل HA، يتم تحميل القائمة المخادعة من ذاكرة Flash الخاصة بالموحل (WLC) الاحتياطي السابق من Cisco WLC.

في سيناريو "التوفر العالي"، إذا تم تعيين مستوى أمان "الكشف عن المخادع" إلى "عالي" أو "هام"، يبدأ عداد الوقت المخادع الموجود على وحدة التحكم الاحتياطية فقط بعد وقت تثبيت تثبيت محوالت الكشف عن المخادع، والذي يبلغ 300 ثانية. وبالتالي، ال تنعكس التكوينات النشطة على وحدة التحكم الاحتياطية إال بعد 300 ثانية.

حقائق الاتصال المرن

تأخذ نقطة الوصول FlexConnect (مع تمكين الكشف المخادع) في الوضع المتصل قائمة الاحتواء من وحدة التحكم. في حالة تعيين كل من SSID التي تحتوي تلقائيا على SSID وميزة "إحتواء تلقائي" في وحدة التحكم، فعندئذ يتم تعيين هذه التكوينات على جميع نقاط الوصول FlexConnect في الوضع المتصل وتقوم نقطة الوصول بتخزين هذه التكوينات في ذاكرتها.

عندما تنتقل نقطة الوصول (AP) من FlexConnect إلى الوضع المستقل، يتم تنفيذ المهام التالية:

- ال تزال عملية الاحتواء التي وضعها المراقب مستمرة.
- إذا اكتشفت نقطة الوصول FlexConnect أي نقطة وصول مخادعة تحتوي على نفس SSID (تم تكوين SSID في وحدة التحكم التي يتم توصيل معرف SSID الموجود ضمن SSID بها)، فسيتم بدء الاحتواء إذا تم تمكين SSID الاحتواء التلقائي من وحدة التحكم قبل تحريكها إلى الوضع المستقل.
- إذا اكتشفت نقطة الوصول FlexConnect أي دوار أقران، يبدأ الاحتواء إذا تم تمكين ميزة "الاحتواء التلقائي" من وحدة التحكم عندما كانت في الوضع المتصل.

عندما تنتقل نقطة الوصول المستقلة FlexConnect AP مرة أخرى إلى الوضع المتصل، يتم تنفيذ هذه المهام:

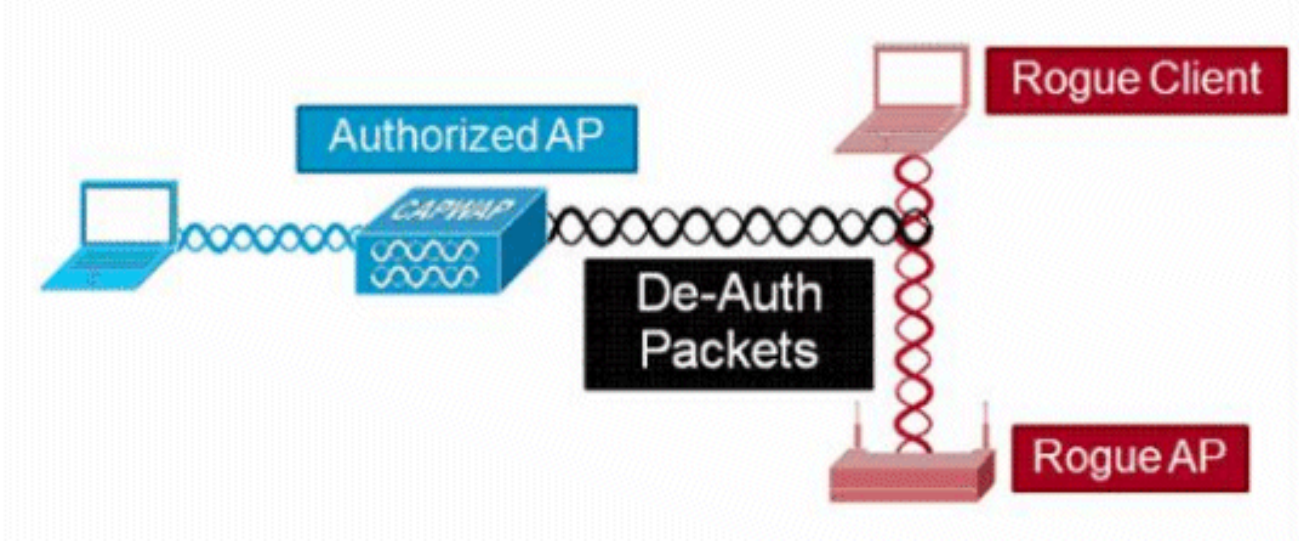
- يتم مسح جميع الاحتواء.

- عملية الاحتواء التي بدأت من قبل وحدة التحكم.

تخفيف المخاطر المخادعة

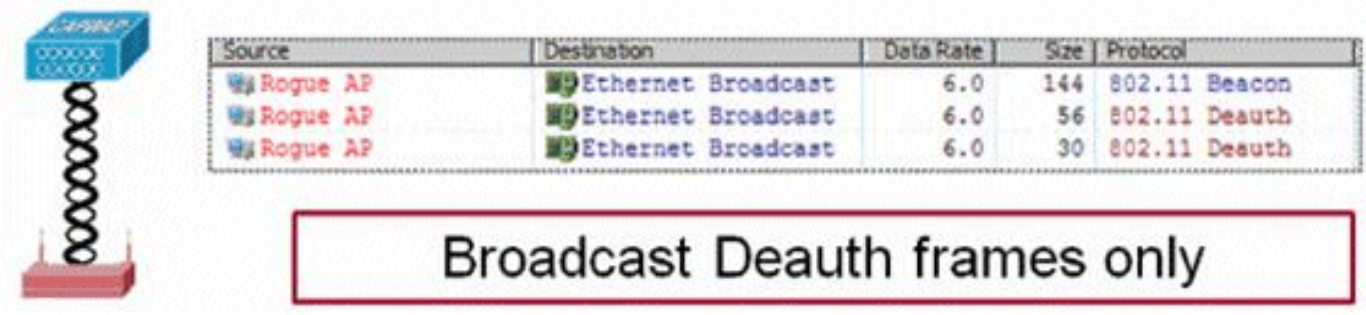
إحتواء المخادعين

الاحتواء هي طريقة تستخدم الحزم المنقولة عبر الهواء لمقاطعة الخدمة مؤقتا على جهاز مخادع حتى يمكن إزالته ماديا. يعمل الاحتواء مع انتحال حزم إلغاء المصادقة مع عنوان المصدر المنتحلة لنقطة الوصول المخادعة بحيث يتم إيقاف تشغيل أي عملاء مرتبطين.

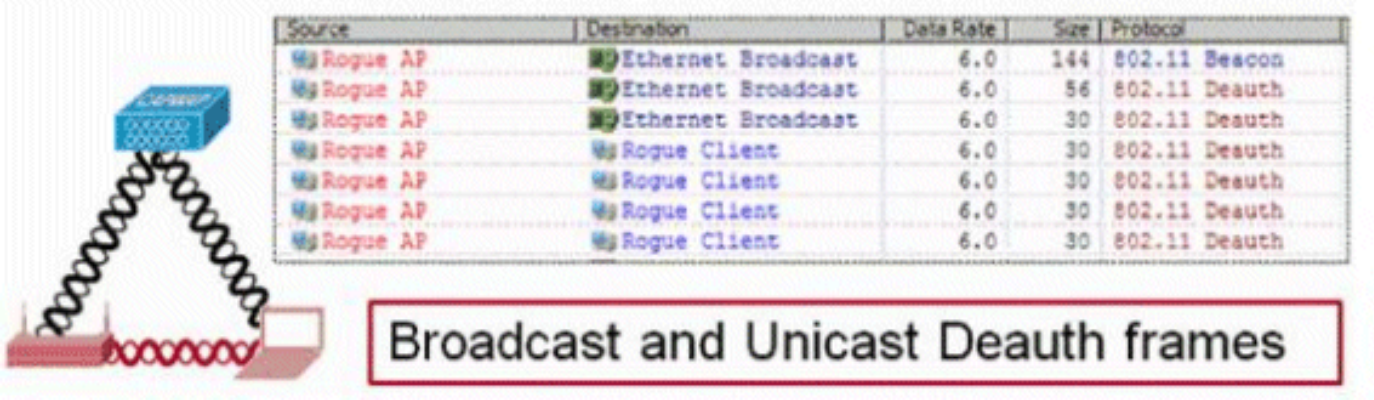


تفاصيل الاحتواء المخادعة

ال تستخدم عملية الاحتواء التي يتم بدء تشغيلها على نقطة وصول (AP) مخادعة بدون عملاء إلا إطارات إلغاء المصادقة التي يتم إرسالها إلى عنوان البث:

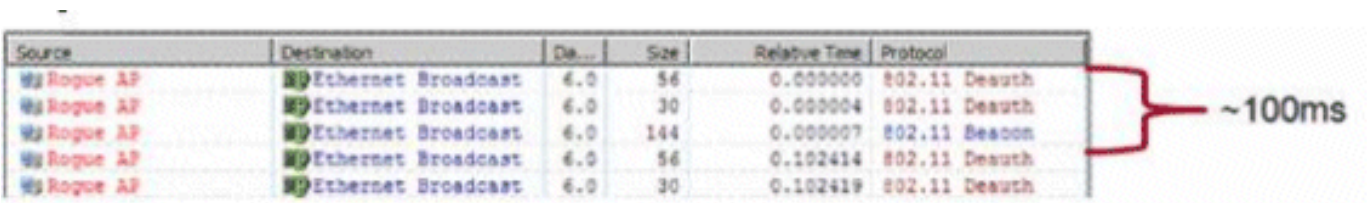


يتم بدء الاحتواء على نقطة وصول (نقاط) مخادعة مع إستخدام إطارات إلغاء المصادقة المرسلة إلى عنوان البث وإلى عنوان (عناوين) العميل:



يتم إرسال حزم الاحتواء على مستوى طاقة نقطة الوصول المدارة وأقل معدل ممكن للبيانات.

ترسل الاحتواء وحدتين على الأقل كل 100 ملي ثانية:



ملاحظة: يتم إرسال إحتواء يتم إجراؤه من قبل نقاط الوصول في الوضع غير المرافق في فترة زمنية قدرها 500 ملي ثانية بدلا من الفاصل الزمني الذي يبلغ 100 ملي ثانية المستخدم من قبل نقاط الوصول في وضع المراقبة.

- يمكن إحتواء أي جهاز مخادع فردي من خلال ما بين 1 إلى 4 نقاط وصول مدارة تعمل بالإقتران لتخفيف التهديد بشكل مؤقت.
- يمكن تنفيذ الاحتواء باستخدام نقاط الوصول في الوضع المحلي ووضع المراقبة ووضع الاتصال المرن (المتصل). بالنسبة للوضع المحلي لنقاط الوصول ذات الاتصال المرن، يمكن إحتواء ثلاثة أجهزة مخادعة كحد أقصى لكل جهاز لاسلكي. بالنسبة لنقاط الوصول في وضع الشاشة، يمكن إحتواء ستة أجهزة مخادعة كحد أقصى لكل جهاز لاسلكي.

إحتواء تلقائي

بالإضافة إلى بدء الاحتواء يدويا على جهاز مخادع عبر PI أو واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، هناك أيضا القدرة على بدء الاحتواء تلقائيا في ظل سيناريوهات معينة. تم العثور على هذا التكوين ضمن قسم السياسات المخادعة لواجهة PI أو واجهة وحدة التحكم. يتم تعطيل كل من هذه المميزات بشكل افتراضي ويجب تمكينها فقط لإبطال التهديدات التي تسبب أكبر ضرر.

- المخادعة عبر السلك - في حالة التعرف على جهاز مخادع بأنه متصل بالشبكة السلكية، يتم وضعه تلقائيا تحت الاحتواء.

- إستخدام SSID الخاص بنا - إذا كان الجهاز الدوار يستخدم SSID مماثل للمعرف المكون على وحدة التحكم، فإنه يتم إحتوائه تلقائيا. وتهدف هذه الميزة إلى معالجة هجوم بزيت العسل قبل أن تتسبب في حدوث الضرر.

- عميل صالح على نقطة الوصول الدخيلة - إذا وجد أن عميل مدرج في خادم RADIUS/AAA مرتبط بجهاز مخادع، يتم تشغيل الاحتواء ضد ذلك العميل فقط، ويمنعه من الاقتران إلى أي نقطة وصول (AP) غير مدارة.

- نقطة الوصول المخادعة المخصصة - في حالة اكتشاف شبكة أقران، يتم احتواؤها تلقائيا.

إحتواء مارق

- ولأن الاحتواء يستخدم جزء من وقت راديو نقطة الوصول المدارة لإرسال إطارات إلغاء المصادقة، فإن الأداء لكل من عملاء البيانات والصوت يتأثر بشكل سلبي بنسبة تصل إلى 20٪. بالنسبة لعملاء البيانات، يكون التأثير أقل في الخرج. بالنسبة لعملاء الصوت، قد يتسبب الاحتواء في حدوث مقاطعات في المحادثات وتقليل جودة الصوت.

- قد يكون للاحتواء تداعيات قانونية عندما يتم إطلاقه ضد الشبكات المجاورة. تأكد من أن الجهاز المخادع موجود داخل شبكتك ويشكل مخاطر أمنية قبل بدء عملية الاحتواء.

إيقاف تشغيل منفذ المحول

إذا كنت تتبع مفتاح ميناء بالإستعامل من SPT، هناك خيار أن يعجز أن ميناء في PI. يجب على المسؤول إجراء هذا التدريب يدويا. يتوفر خيار لتمكين منفذ المحول من خلال PI إذا تمت إزالة الواقي فعليا من الشبكة.

التكوين

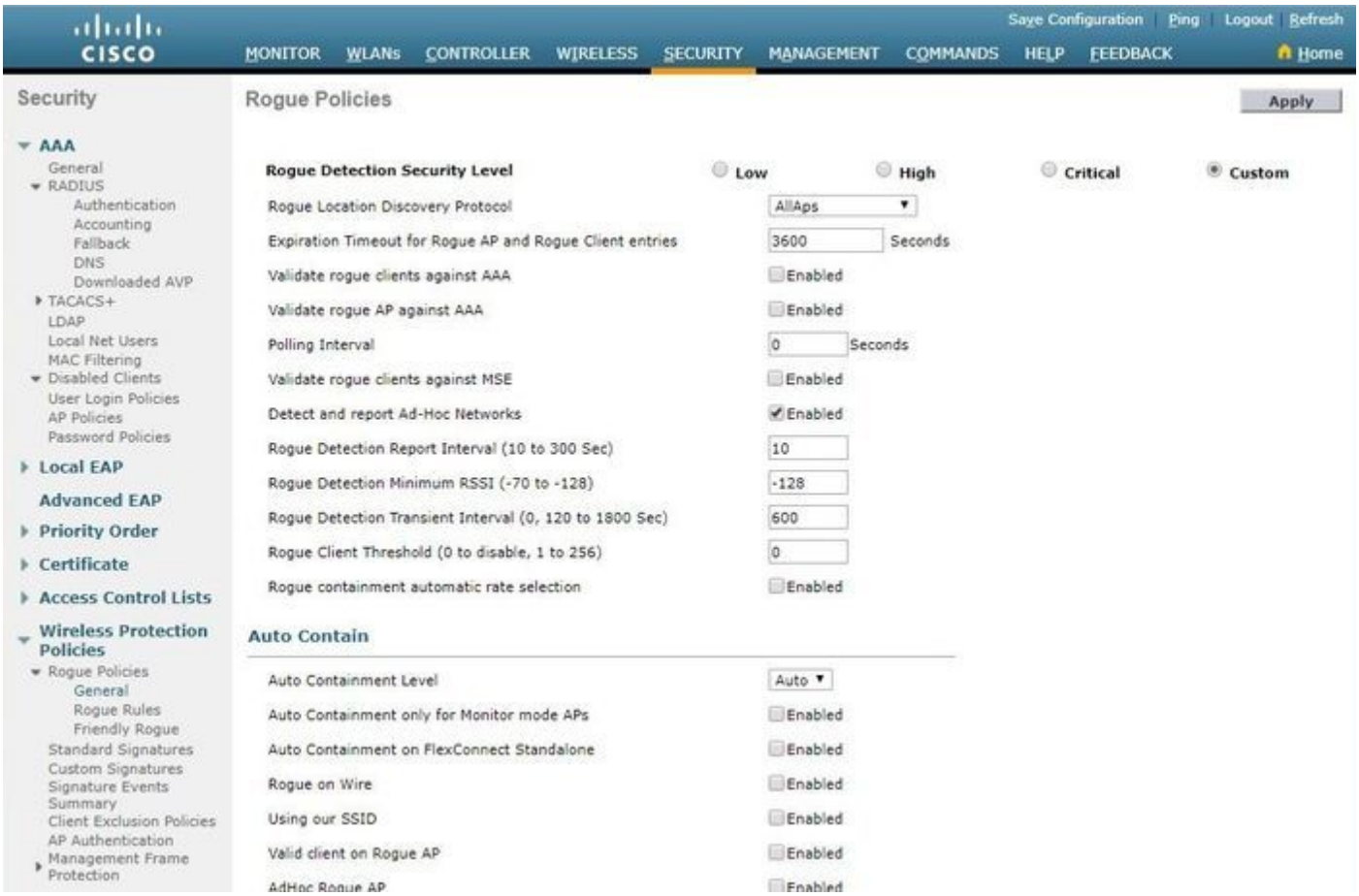
تكوين الكشف عن الأخطاء

يتم تمكين الكشف المخادع في وحدة التحكم بشكل افتراضي.

من أجل تكوين خيارات مختلفة، انتقل إلى التأمين > سياسات الحماية اللاسلكية > السياسات المخادعة > عامة. على سبيل المثال:

الخطوة 1. تغيير المهلة لنقاط الوصول المخادعة.

الخطوة 2. تمكين اكتشاف شبكات المخادعة المؤقتة.



من واجهة سطر الأوامر:

<#root>

```
(Cisco Controller) >
```

config rogue ap timeout ?

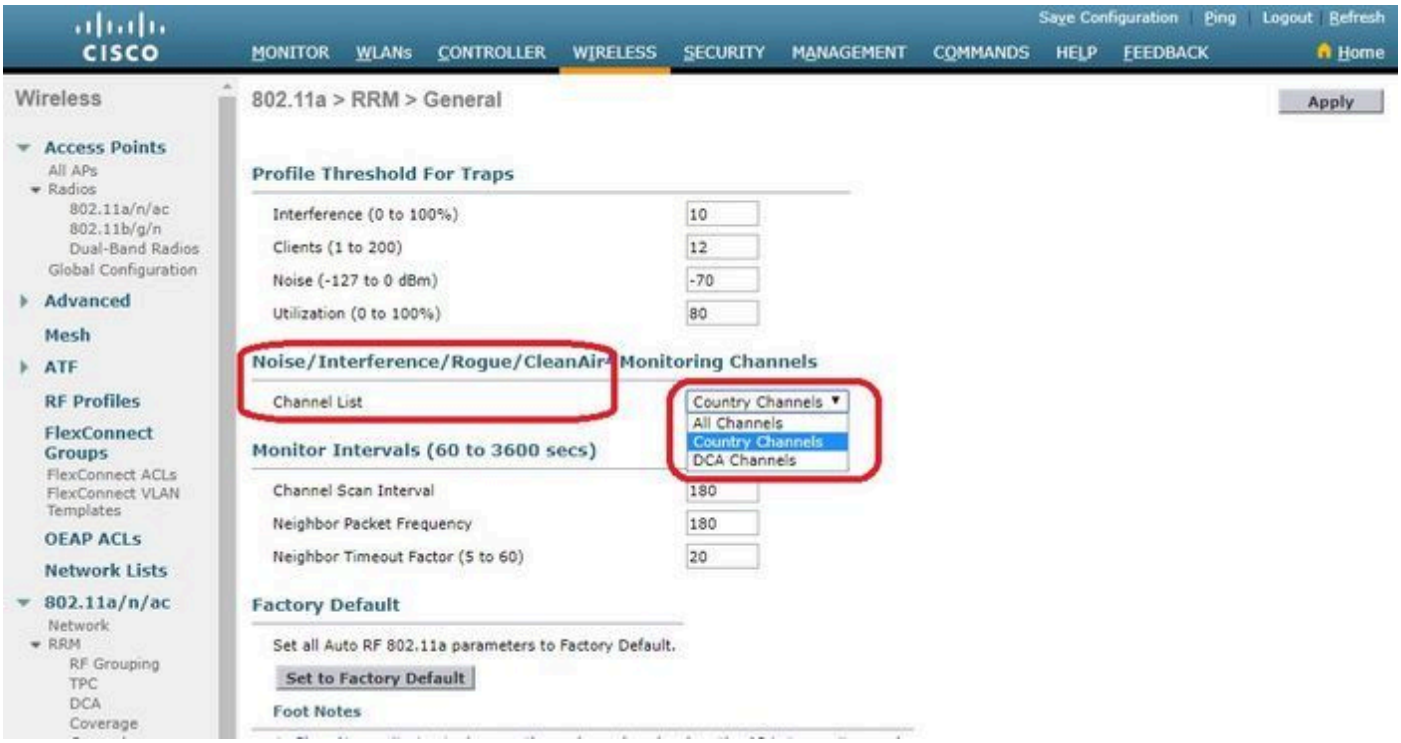
```
<seconds>      The number of seconds<240 - 3600> before rogue entries are flushed

(Cisco Controller) >
```

config rogue adhoc enable/disable

تكوين فحص القناة للكشف عن المخادع

بالنسبة لنقطة الوصول من الوضع المحلي/Flex-Connect/Monitor، هناك خيار ضمن تكوين RRM يسمح للمستخدم باختيار القنوات التي يتم مسحها ضوئيا للظلال. يعتمد على التكوين، وتمسح نقطة الوصول كل القناة/البلد/قناة DCA بحثا عن المخادعين.

دخلت in order to شكلت هذا من ال gui، السلكي>802.11a/802.11b>RRM>عام، كما هو موضح في الصورة.



من واجهة سطر الأوامر:

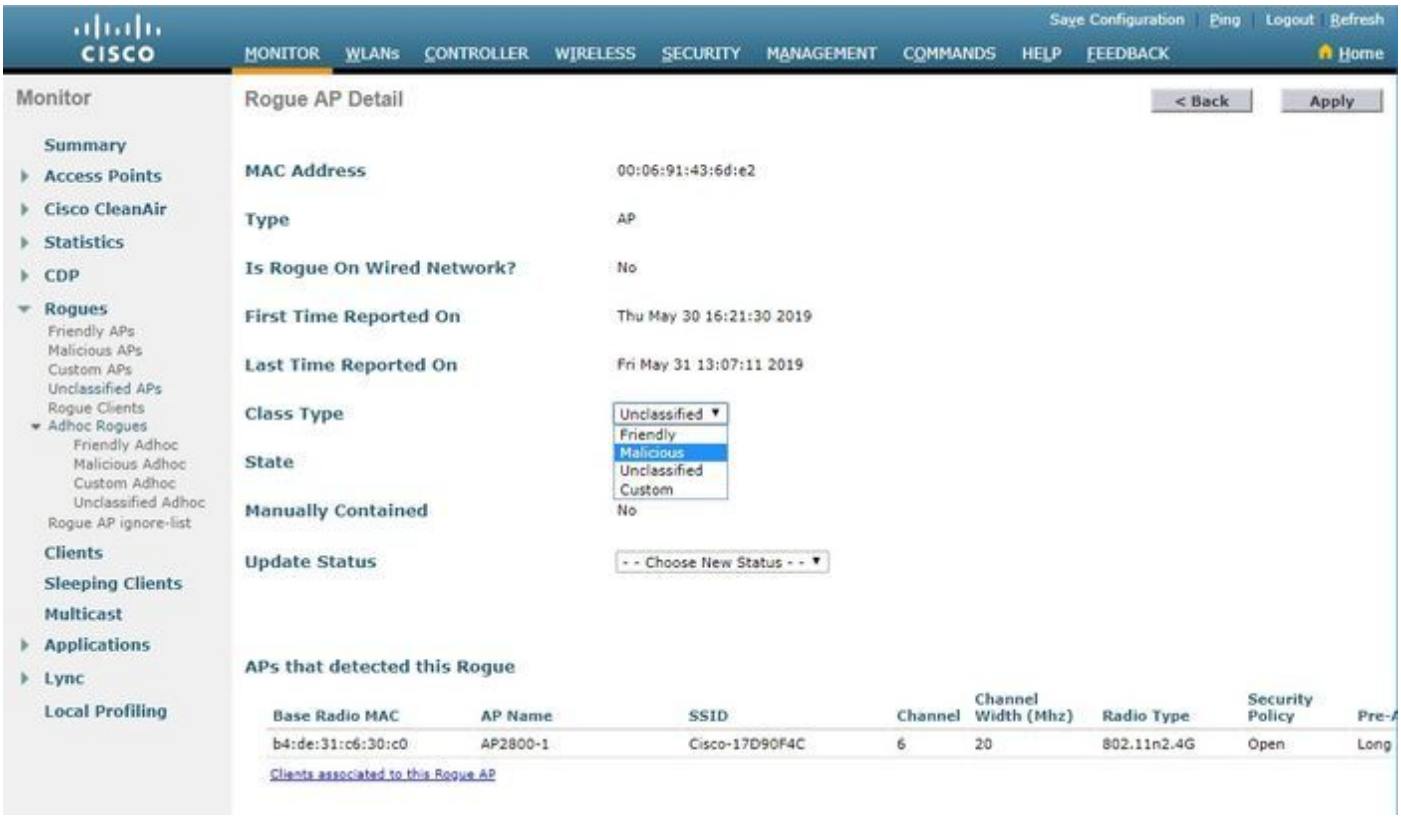
<#root>

```
(Cisco Controller) >

config advanced 802.11a monitor channel-list ?


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

تكوين تصنيف المخادع

تصنيف نقطة وصول مخادعة يدويا

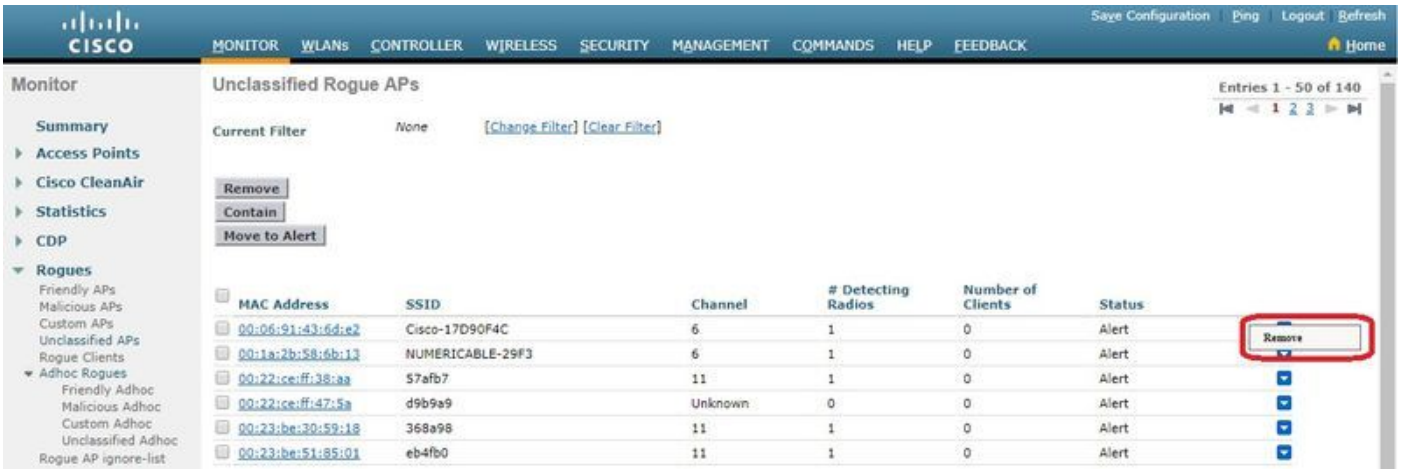
من أجل تصنيف نقطة وصول (AP) مخادعة أو ضارة أو غير مصنفة، انتقل إلى Monitor > مخادع > نقاط وصول (AP) غير مصنفة، وانقر فوق اسم نقطة الوصول المخادعة المعين. أختر الخيار من القائمة المنسدلة، كما هو موضح في الصورة.



من واجهة سطر الأوامر:

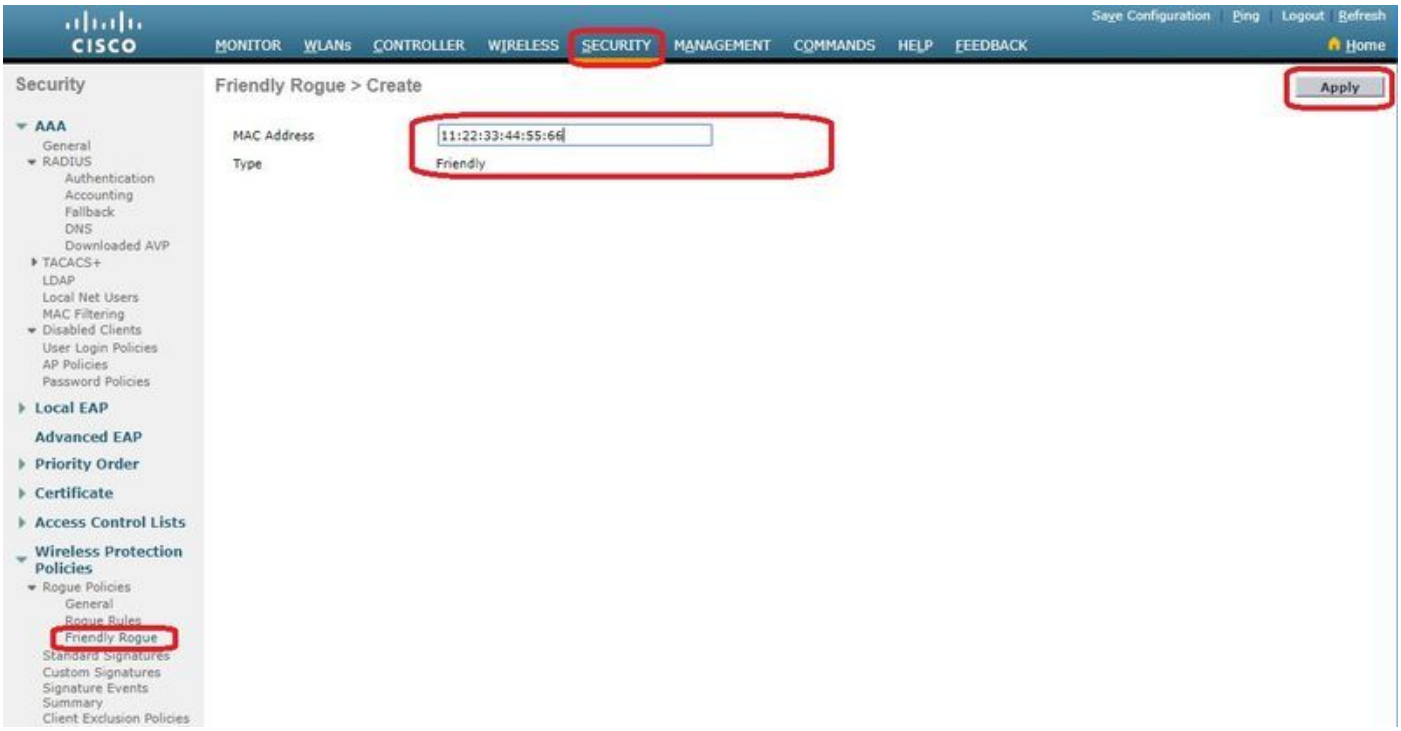
```
<#root>

(Cisco Controller) >

config rogue ap ?


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

لإزالة إدخال مخادع يدويا من القائمة المخادعة، انتقل إلىMonitor > مخادع > نقاط وصول (AP) غير مصنفة، وانقر فوق إزالة، كما هو موضح في الصورة.



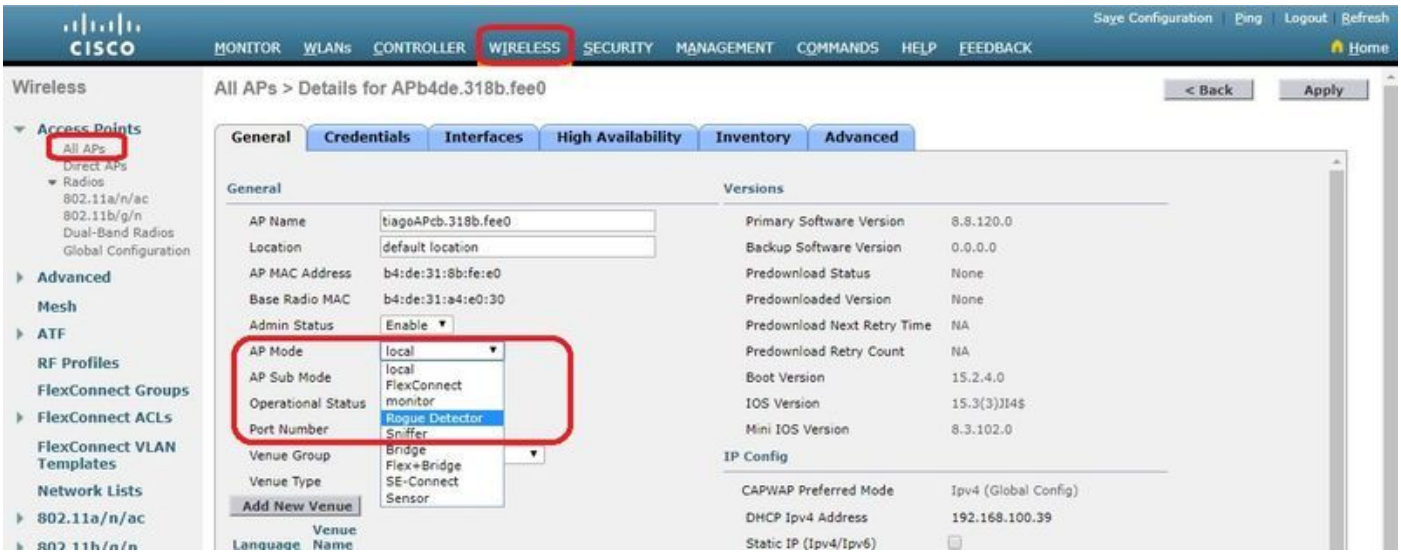
من أجل تكوين نقطة وصول (AP) مخادعة كنقطة وصول (AP) سهلة، انتقل إلىSecurity (الأمان) > سياسات الحماية اللاسلكية > السياسات المخادعة > الأجهزة الصديقة وأضف عنوان MAC المخادع.

يمكن التحقق من الإدخالات المخادعة المأمولة المضافة من الشاشة > المخادع > الصفحة المأمولة، كما هو موضح في الصورة.



تكوين نقطة وصول لمكتشف المخادع

من أجل تكوين نقطة الوصول كمكتشف مخادع من خلال واجهة المستخدم الرسومية، انتقل إلى لاسلكي > جميع نقاط الوصول. أختر اسم نقطة الوصول وقم بتغيير وضع نقطة الوصول كما هو موضح في الصورة.



من واجهة سطر الأوامر:

```
<#root>

(Cisco Controller) >

config ap mode rogue AP_Managed


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

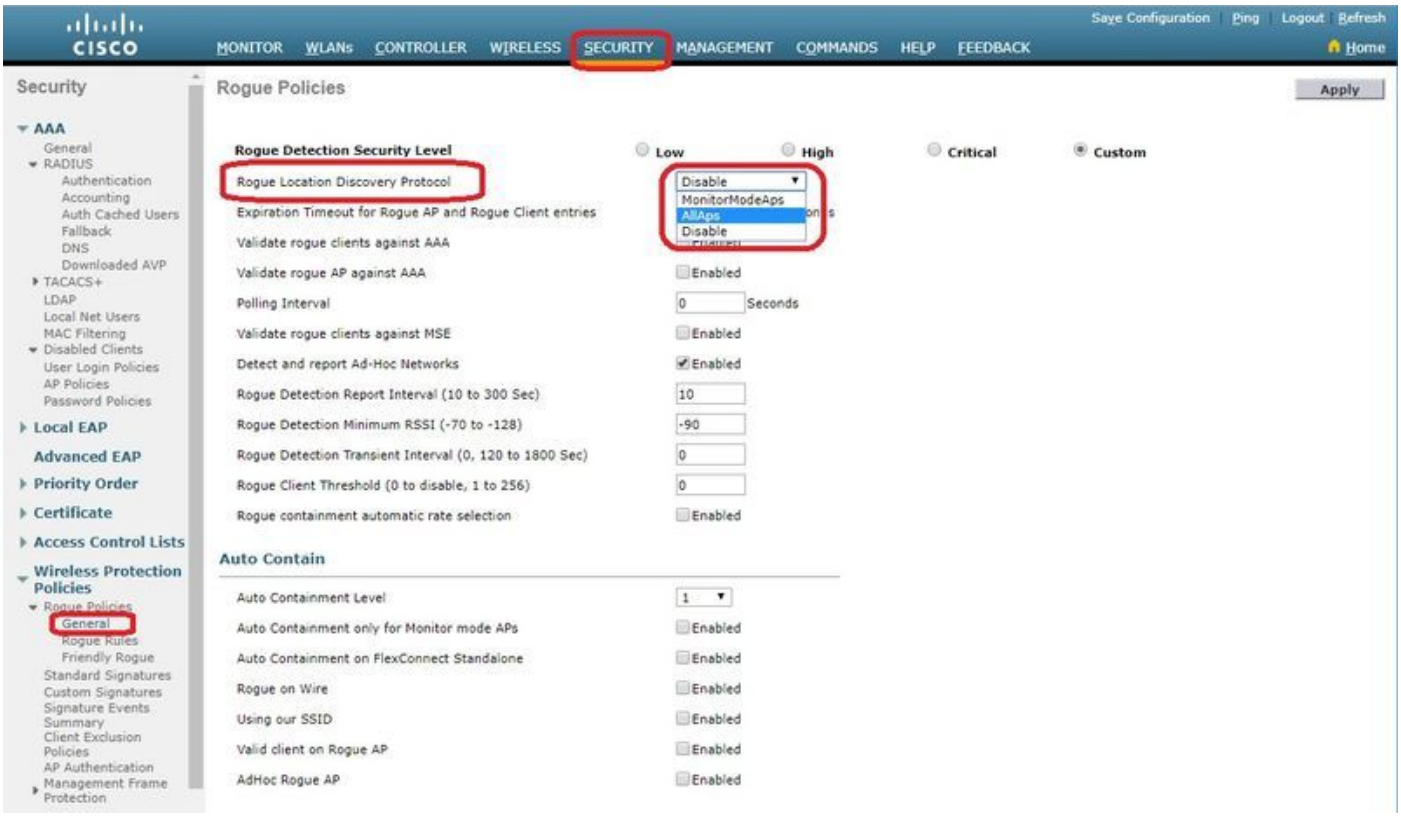
تكوين SwitchPort لنقطة الوصول الخاصة بمكتشف المخادع

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

ملاحظة: ال VLAN أهلي طبيعي في هذا تشكيل أن يتلقى اتصال IP إلى ال WLC.

تكوين RLDP

من أجل تكوين RLDP في واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم، انتقل إلىالأمان > سياسات الحماية اللاسلكية > السياسات المخادعة > عامة.



نقاط الوصول إلى وضع المراقبة- يسمح فقط لنقاط الوصول في وضع المراقبة بالمشاركة في RLDP.

جميع نقاط الوصول (APs)- مشاركة نقاط الوصول (APs) إلى الوضع "محلي/مرن-connect/monitor" في عملية RLDP.

معطل- الا يتم تشغيل RLDP تلقائيا. ومع ذلك، يمكن للمستخدم تشغيل RLDP يدويا لعنوان MAC معين من خلال CLI (واجهة سطر الأوامر).

ملاحظة: تحصل نقطة الوصول في وضع المراقبة على الأفضلية على نقطة الوصول المحلية/Flex-Connect AP لتنفيذ RLDP إذا اكتشف كل منهما حالة مرور معينة تتجاوز RSSI بديسيبل -85.

من واجهة سطر الأوامر:

<#root>

```
(Cisco Controller) >

config rogue ap rldp enable

 ?

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

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

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

لا يمكن تكوين جدول RLDP والمشغل اليدوي إلا من خلال موجه الأوامر. لبدء RLDP يدويا:

```
<#root>

(Cisco Controller) >

config rogue ap rldp initiate

 ?

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

بالنسبة لجدول RLDP:

```
<#root>

(Cisco Controller) >

config rogue ap rldp schedule ?


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


(Cisco Controller) >

config rogue ap rldp schedule add ?


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

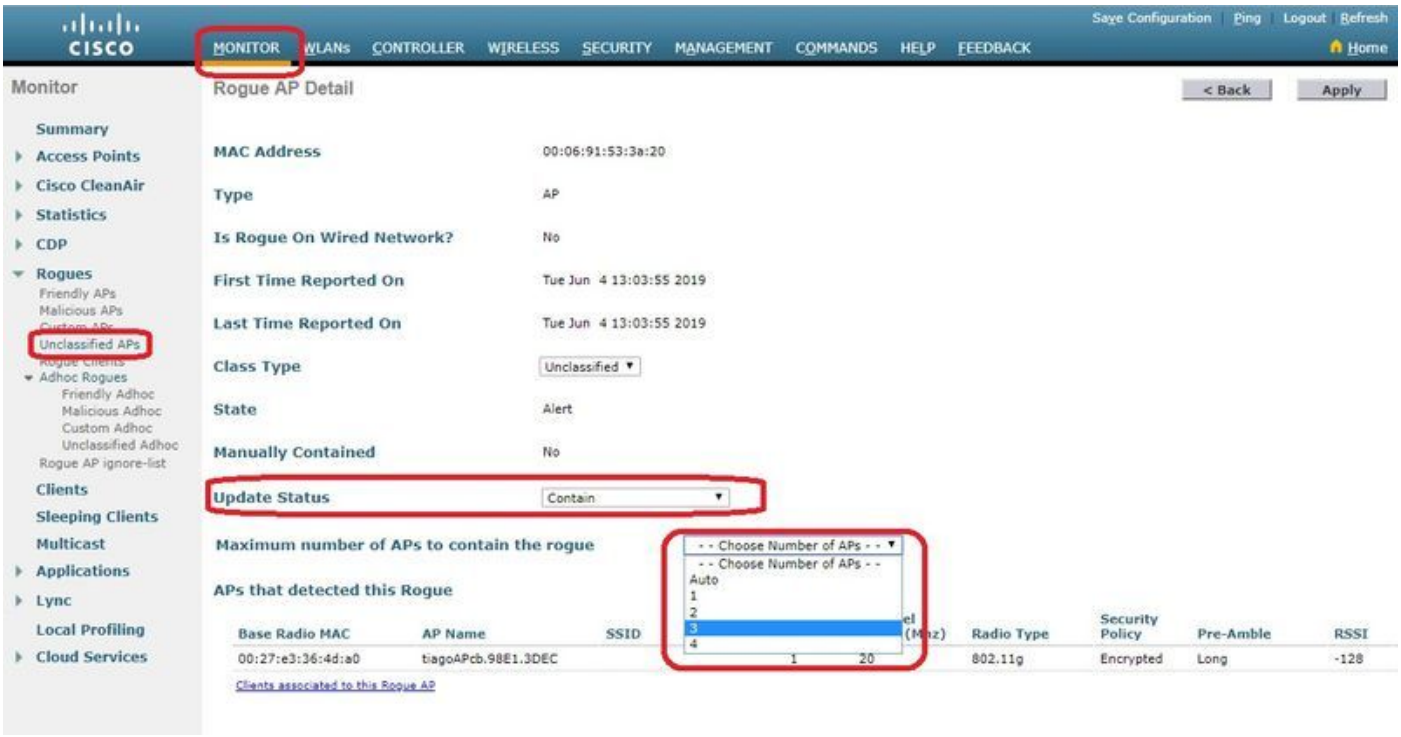
يمكن تكوين عمليات إعادة محاولة RLDP باستخدام الأمر:

```
<#root>

(Cisco Controller) >

config rogue ap rldp retries ?


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

تكوين تخفيف الأخطاء

تكوين الاحتواء اليدوي

من أجل إحتواء نقطة وصول مخادعة يدويا، انتقل إلىMonitor > مخادع > غير مصنفة، كما هو موضح في الصورة.



من واجهة سطر الأوامر:

<#root>

```
(Cisco Controller) >
```

config rogue client

```
 ?

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

ملاحظة: يمكن إحتواء مارق معين ب 1-4 نقاط وصول. وبشكل افتراضي، تستخدم وحدة التحكم نقطة وصول واحدة لاحتواء عميل. إذا تمكن إثنان من نقاط الوصول من اكتشاف دخيل معين، تحتوي نقطة الوصول (AP) التي تحتوي على أعلى RSSI على العميل بغض النظر عن وضع AP.

إحتواء تلقائي

لتكوين الاحتواء التلقائي، انتقل إلىSecurity>سياسات الحماية اللاسلكية>السياسات المخادعة>General، وقم بتمكين جميع الخيارات القابلة للتطبيق على شبكتك.

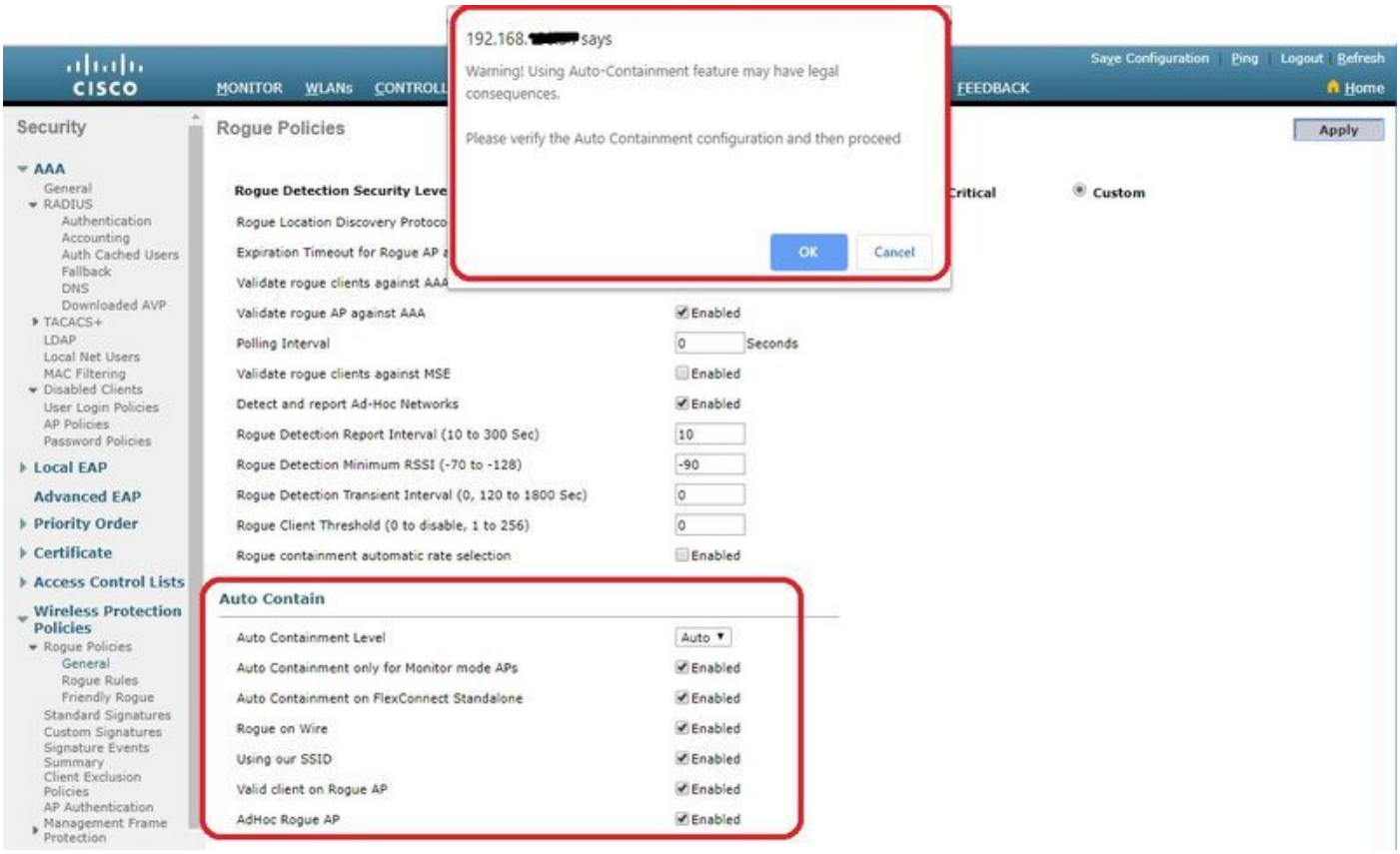
إذا كنت تريد أن يحتوي عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من Cisco تلقائيا على أجهزة دخيلة معينة، فحدد هذه المربعات. وإلا، أترك خانات الاختيار غير محددة، والتي هي القيمة الافتراضية.

تحذير: عند تمكين أي من هذه المعلمات، تظهر الرسالة: يؤدي إستخدام هذه الميزة إلى 2. 4 و 5 - غيغاهرتز ضمن حزمة ISM تكون الترددات التي تريد المتابعة؟ لها عواقب قانونية. عادة ما تكون هذه الترددات مخصصة للاستخدام الصناعي والعلمي والطبي ويمكن إستخدامها بدون ترخيص. على هذا النحو، قد يؤدي إحتواء الأجهزة على شبكة طرف آخر إلى عواقب قانونية.

هذه هي المعلمات التي تحتوي تلقائيا على:

باراميتر	الوصف
مستوى الاحتواء التلقائي	قائمة منسدلة يمكنك منها إختيار مستوى الاحتواء التلقائي المخادع من 1 إلى 4. يمكنك إختيار ما يصل إلى أربع نقاط وصول للاحتواء التلقائي عند نقل مارق إلى حالة إحتواء من خلال أي من نهج الاحتواء التلقائي. يمكنك أيضا إختيار تلقائي للتحديد التلقائي لعدد نقاط الوصول المستخدمة للاحتواء التلقائي. تختار Cisco WLC العدد المطلوب من نقاط الوصول المستندة إلى RSSI من أجل الاحتواء الفعال. قيمة RSSI المقترنة بكل مستوى إحتواء هي كما يلي: • من 0 إلى -55 ديسيبل لكل ميلليواط • 2 — من -55 إلى -75 ديسيبل لكل ميلليواط • 3 — من -75 إلى -85 ديسيبل لكل ميلليواط • 4 — أقل من -85 ديسيبل لكل ميلليواط
الاحتواء التلقائي فقط لنقاط	خانة الاختيار التي يمكنك تحديدها لتمكين نقاط الوصول إلى وضع الشاشة للاحتواء التلقائي. التقصير دولة معأق.

باراماتر	الوصف
الوصول في وضع جهاز العرض	
إحتواء تلقائي على تقنية FlexConnect المستقلة	خانة الاختيار التي يمكنك تحديدها لتمكين الاحتواء التلقائي على نقاط الوصول من FlexConnect في الوضع المستقل. التقصير دولة مأعق. عندما تكون نقاط الوصول FlexConnect في الوضع المستقل، يمكنك تمكين إستخدام سياسات الاحتواء التلقائي لنقاط الوصول (AP) المخادعة أو SSID. يتوقف الاحتواء بعد اتصال نقطة الوصول المستقلة مرة أخرى بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) من Cisco.
سلك مخادع	خانة الاختيار التي يمكنك تمكينها لاحتواء المراوغات التي تم الكشف عنها على الشبكة السلكية تلقائيا. التقصير دولة مأعق.
إستخدام SSID	خانة الاختيار التي يمكنك تمكينها لاحتواء الأوغاد التي تعلن عن SSID الخاص بشبكتك تلقائيا. إن يترك أنت هذا معلم غير محدد، ال cisco WLC فقط في دلإ إذا كان هذا معلم مدعوما. التقصير دولة مأعق.
عميل صالح على نقطة الوصول الدخيلة	خانة الاختيار التي يمكنك تمكينها بحيث تحتوي تلقائيا على نقطة وصول دخيلة مقترنة بها معلومات موثوق بها. إن يترك أنت هذا معلم غير محدد، ال cisco WLC فقط في دلإ إذا كان هذا معلم مدعوما. التقصير دولة مأعق.
نقطة الوصول المخادعة المخصصة	خانة الاختيار التي يمكنك تمكينها لاحتواء شبكات الأقران تلقائيا التي تم الكشف عنها بواسطة Cisco WLC. إن يترك أنت هذا معلم غير محدد، ال cisco WLC فقط في دلإ إذا كان هذا معلم مدعوما. التقصير دولة مأعق.



انقر فوق تطبيق لإرسال البيانات إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من Cisco، ولكن لا يتم الاحتفاظ بالبيانات عبر دورة طاقة؛ ويتم تخزين هذه المعلمات مؤقتا في ذاكرة الوصول العشوائي المتطايرة.

من واجهة سطر الأوامر:

<#root>

```
(Cisco Controller) >

config rogue adhoc ?


alert           Stop Auto-Containment, generate a trap upon detection of the
                    adhoc rogue.
auto-contain    Automatically contain adhoc rogue.
contain         Start to contain adhoc rogue.
disable         Disable detection and reporting of Ad-Hoc rogues.
enable          Enable detection and reporting of Ad-Hoc rogues.
external        Acknowledge presence of a adhoc rogue.

(Cisco Controller) >

config rogue adhoc auto-contain ?

(Cisco Controller) >

config rogue adhoc auto-contain

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

مع البنية الأساسية ل Prime

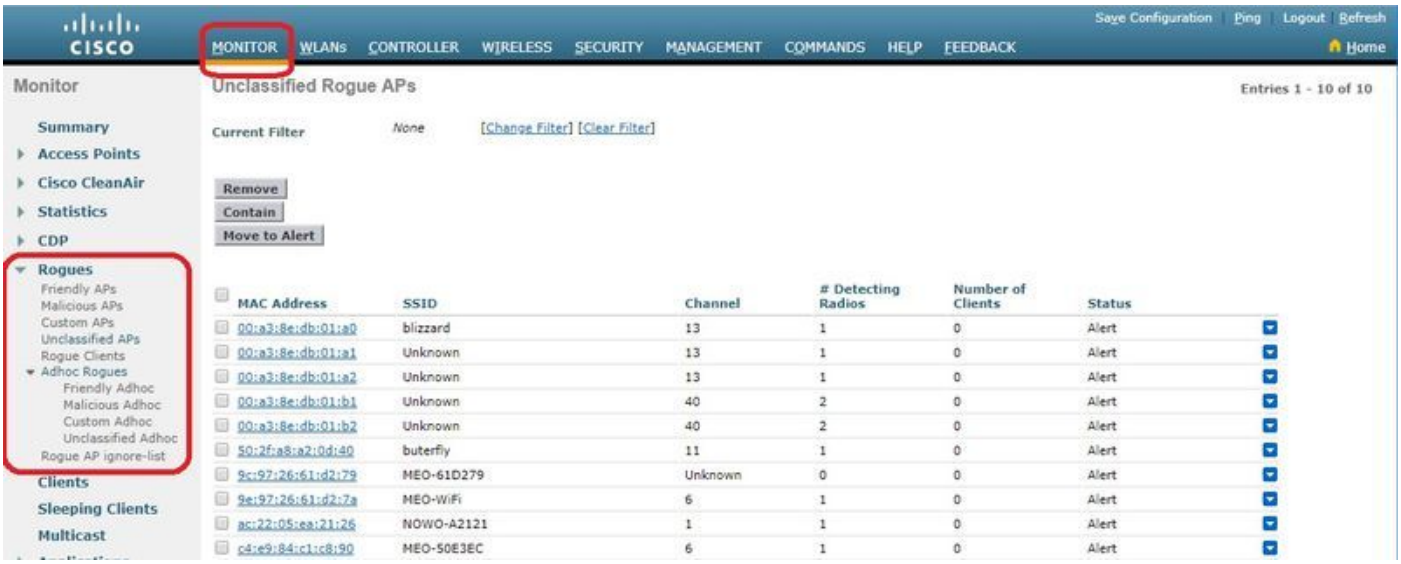
يمكن إستخدام البنية الأساسية ل Cisco Prime لتكوين وحدة تحكم واحدة أو أكثر ونقاط الوصول (AP) المرتبطة ومراقبتها. تحتوي تقنية معلومات الأداء (PI) من Cisco على أدوات لتسهيل مراقبة النظام الكبير والتحكم فيه. عندما تستخدم Cisco PI في حل Cisco اللاسلكي، تحدد وحدات التحكم بشكل دوري العميل ونقطة الوصول الدخيلة وزبون نقطة الوصول الدخيلة وموقع عالمة معرف التردد اللاسلكي (RFID) وتخزن المواقع في قاعدة بيانات Cisco PI.

تدعم البنية الأساسية ل Cisco Prime التصنيف المستند إلى قواعد وتستخدم قواعد التصنيف التي تم تكوينها على وحدة التحكم. ترسل وحدة التحكم المعلومات إلى Cisco Prime Infrastructure بعد هذه الأحداث:

- إذا انتقلت نقطة وصول غير معروفة إلى الدولة الصديقة لأول مرة، يرسل جهاز التحكم مصيدة إلى Cisco Prime Infrastructure فقط إذا كانت الحالة المخادعة في حالة تنبيه. والا يرسل فخ إذا كانت الحوزة الحرارية داخلية أو خارجية.
- إذا تمت إزالة arogueentry بعد انتهاء المهلة، يرسل جهاز التحكم مصيدة إلى نقاط الوصول إلى البنية الأساسية ل Cisco Prime INFRASTRUCTUREREFrogueaccess التي يتم تصنيفها على أنها ضارة (تنبيه، تهديد) أو غير مصنفة (تنبيه). ال تقوم وحدة التحكم بإعادة توجيه الإدخالات باستخدام وحدات التخزين المؤقتة: المضمنة والمعلقة والداخلية والخارجية.

التحقق من الصحة

للعثور على التفاصيل المخادعة في وحدة تحكم في الواجهة الرسومية، انتقل إلىMonitor > المخادع، كما هو موضح في الصورة.



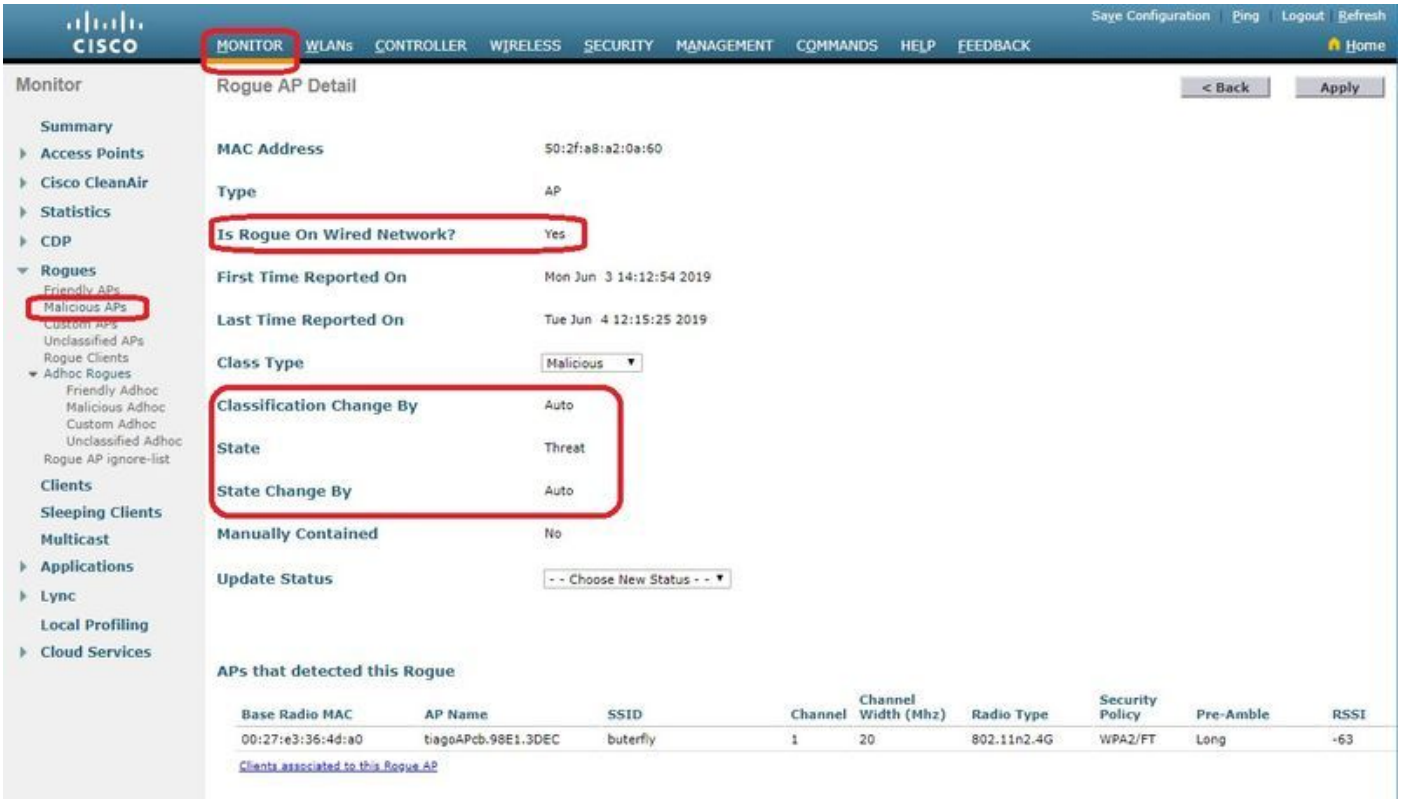
في هذه الصفحة، يتوفر تصنيف مختلف للوسطاء:

- نقاط الوصول المألوفة - نقاط الوصول التي تم وضع عالمة عليها كصديقة من قبل المسؤول.

- نقاط الوصول (AP) الضارة - التي يتم تعريفها على أنها ضارة عبر RLDP أو نقاط الوصول (AP) للمكتشف المخادع.
- نقاط الوصول المخصصة - نقاط الوصول التي يتم تصنيفها كقواعد مخصصة بواسطة قواعد مخادعة.
- نقاط الوصول غير المصنفة - يتم عرض نقاط الوصول المخادعة بشكل افتراضي كقائمة غير مصنفة في وحدة التحكم.
- العملاء المخادعون - العملاء متصلون بنقاط الوصول المخادعة.
- الأوغاد - العملاء المزيفون الأقران.
- قائمة تجاهل نقاط الوصول (AP) المخادعة - كما هو مدرج من خلال PI.

ملاحظة: إذا تم إدارة WLC ونقطة الوصول المستقلة بواسطة PI نفسها، فإن WLC يسرد تلقائيا نقطة الوصول المستقلة هذه في قائمة تجاهل نقاط الوصول المخادعة. لا يوجد تكوين إضافي مطلوب في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لتمكين هذه الميزة.

انقر فوق إدخال مارق معين للحصول على تفاصيل حول هذا المارقة. فيما يلي مثال على مخادع تم اكتشافه على الشبكة السلكية:



من واجهة سطر الأوامر:

```
<#root>

(Cisco Controller) >
```

show rogue ap summary

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

MAC Address       Class        State                #Det #Rogue  #Highest RSSI     #RSSI  #Channel
                                                    Aps  Clients  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:a3:8e:db:01:b1 Unclassified Alert                2    0       00:27:e3:36:4d:a0 -28    40
00:a3:8e:db:01:b2 Unclassified Alert                2    0       00:27:e3:36:4d:a0 -28    40
50:2f:a8:a2:0a:60 Malicious    Threat               1    2       00:27:e3:36:4d:a0 -66    1
50:2f:a8:a2:0d:40 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -65    11
9c:97:26:61:d2:79 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -89    6
ac:22:05:ea:21:26 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -89    (1,5)
c4:e9:84:c1:c8:90 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -89    (6,2)
d4:28:d5:da:e0:d4 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -85    13

(Cisco Controller) >
```

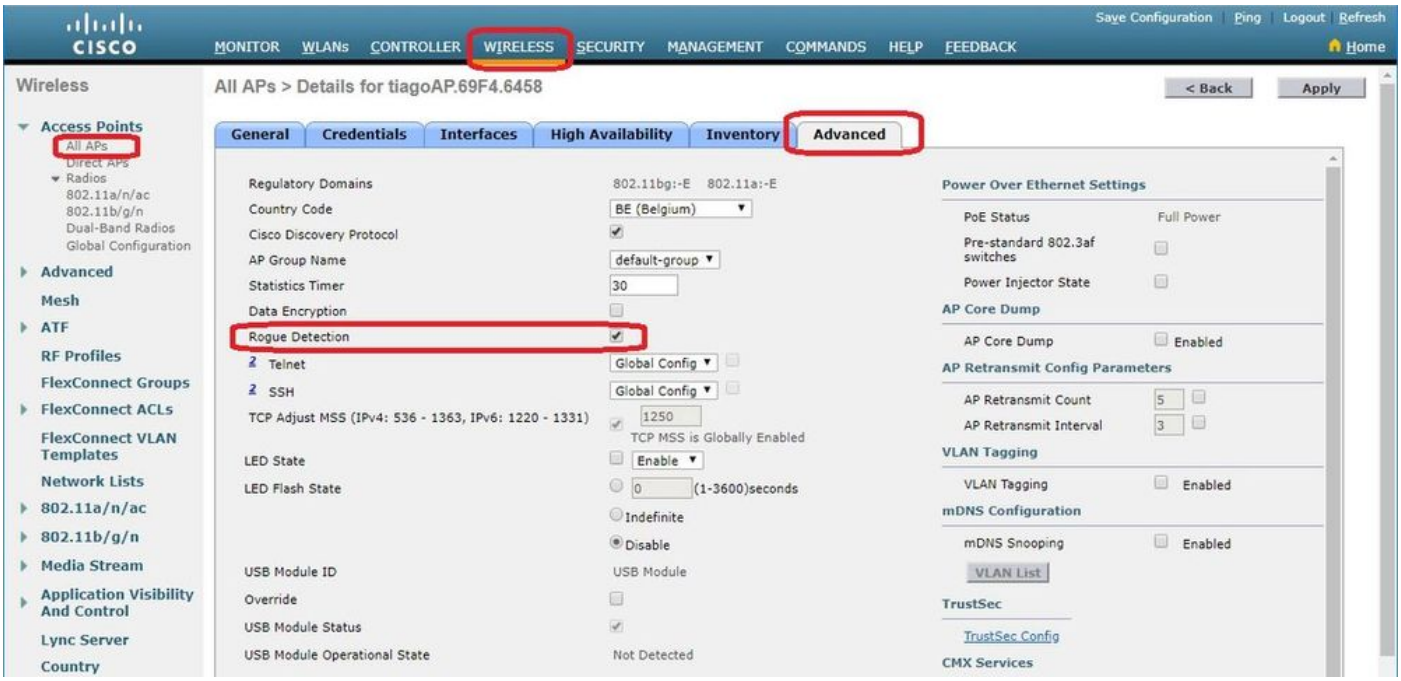
show rogue ap detailed 50:2f:a8:a2:0a:60

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

استكشاف الأخطاء وإصلاحها

إذا لم يتم اكتشاف الوغد

تحقق من تمكين الكشف المخادع على نقطة الوصول. على واجهة المستخدم الرسومية:



في واجهة سطر الأوامر:

```
<#root>

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

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

Rogue Detection ................................. Enabled

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

```
Reset Button..................................... Enabled
AP Serial Number................................. FGL2114A4SU
[...]
```

يمكن تمكين الكشف المخادع على نقطة وصول باستخدام هذا الأمر:

<#root>

```
(Cisco Controller) >
```

config rogue detection enable ?

```
all             Applies the configuration to all connected APs.
<Cisco AP>      Enter the name of the Cisco AP.
```

تقوم نقطة الوصول من الوضع المحلي بمسح قنوات البلد/DCA فقط وتعتمد على التكوين. إذا كان المخادع في أي قناة أخرى، فإن وحدة التحكم لا تستطيع تعريف المخادع إذا لم يكن لديك نقاط وصول في وضع المراقبة في الشبكة. أصدر هذا الأمر للتحقق من:

<#root>

```
(Cisco Controller) >
```

show advanced 802.11a monitor

```
Default 802.11a AP monitoring
  802.11a Monitor Mode........................... enable
  802.11a Monitor Mode for Mesh AP Backhaul...... disable

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

  802.11a RRM Neighbor Discover Type............. Transparent
  802.11a RRM Neighbor RSSI Normalization........ Enabled
  802.11a AP Coverage Interval................... 90 seconds
  802.11a AP Load Interval....................... 60 seconds
  802.11a AP Monitor Measurement Interval........ 180 seconds
  802.11a AP Neighbor Timeout Factor............. 20
  802.11a AP Report Measurement Interval......... 180 seconds
```

- تم تثبيت نقطة الوصول المخادعة SSID.
- تأكد من عدم إضافة عنوان MAC لنقطة الوصول المخادعة في قائمة المخادع المأمولة أو أنه مسموح بإدراجه من خلال PI.
- يمكن الوصول إلى أجهزة الإرشاد من نقطة الوصول المخادعة إلى نقطة الوصول (AP) التي كشفت عن وجود مخادع. يمكن التحقق من هذا الإجراء من خلال التقاط الحزم التي تحتوي على sniffer قريبة من معالج مكتشف AP.
- يمكن لنقطة الوصول في الوضع المحلي أن تستغرق ما يصل إلى 9 دقائق لاكتشاف

المخادع (3 دورات 180x3).

- لا يمكن لنقاط الوصول من Cisco اكتشاف العثرات على ترددات مثل قناة السلامة العامة (4.9 جيجاهرتز).
- لا يمكن لنقاط الوصول من Cisco اكتشاف الأوغاد التي تعمل على FHSS (طيف انتشار تخطي الترددات).

تصحيح الأخطاء المفيدة

<#root>

(Cisco Controller) >

debug client

(If rogue mac is known)
(Cisco Controller) >

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

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

*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
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559724417. Detecti
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60  SYNC for Channel (new/old : 1/0) or channel wi
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 rg changed rssi prev -64, new -55
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Updated AP report 00:27:e3:36:4d:a0  rssi -55,
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 RadioType: 3 lradInfo->containSlotId = 2 Receiv

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

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

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

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

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

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

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

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

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

<#root>

(Cisco Controller) >

debug dot11 rogue enable

```
(Cisco Controller) >*emWeb: Jun 05 08:39:46.828:
Debugging session started on Jun 05 08:39:46.828  for WLC AIR-CT3504-K9   Version :8.8.120.0  SN :FCW224
*iappSocketTask: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 Posting Rogue AP Iapp Report from AP for proces

*apfRogueTask_2: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 fakeAp check: slot=0, entryIndex=0, (Radio_upTi
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid b0:72:bf:93:e0:d7 src
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 50:2f:a8:a2:0a:60 src
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:a1 src
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:b0 src
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 New RSSI report from AP 00:27:e3:36:4d:a0  rssi
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:b2 src
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Found Rogue AP: 00:a3:8e:db:01:a1 on slot 0

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue SSID timestmap expired. last update at 0
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check:  knownApCount=0, totalNumOfRogueE
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 New RSSI report from AP 00:27:e3:36:4d:a0  rssi
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check:  avgNumOfRogues[0]/10=4, rogueAla
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2  SYNC for Channel (new/old : 40/0) or channel w
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue SSID timestmap expired. last update at 0
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 rg changed rssi prev -28, new -28
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1  SYNC for Channel (new/old : 13/0) or channel w
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Updated AP report 00:27:e3:36:4d:a0  rssi -28,
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Updated AP report 00:27:e3:36:4d:a0  rssi -16,
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 RadioType: 3 lradInfo->containSlotId = 1 Receiv

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

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

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

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

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

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Looking for Rogue b0:72:bf:93:e0:d7 in known AP
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue AP b0:72:bf:93:e0:d7 is not found either
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue After Rule Classification : Class unclass

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

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Scheduled pending Time 184 and expiry time 1200
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 ssidLen = 0 min = 0 00:a3:8e:db:01:b2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Change state from 0 to 1 for rogue AP b0:72:bf:
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 This rogue does not use my ssid. Rogue ssid=

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

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

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Checking Impersonation source 00:a3:8e:db:01:b2
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 RadioType: 3 lradInfo->containSlotId = 2 Receiv

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 New RSSI report from AP 00:27:e3:36:4d:a0  rssi
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue is Rule candidate for  : Class Change by
```

```
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7  Send Rogue Info Notificaiton for AP report 00:
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Applying Rogue rule to this MAC

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue SSID timestmap set to 1559723997. Detecti
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg send new rssi -59
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue After Rule Classification : Class unclass

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Updated AP report 00:27:e3:36:4d:a0  rssi -59,
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Manual Contained Flag = 0, trustlevel = 2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 ssidLen = 0 min = 0 00:a3:8e:db:01:a1

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

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



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

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

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

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

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Checking Impersonation source 00:a3:8e:db:01:a1
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Manual Contained Flag = 0, trustlevel = 1

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

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

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

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

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 New RSSI report from AP 00:27:e3:36:4d:a0  rssi
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue SSID timestmap set to 1559723997. Detecti
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 New RSSI report from AP 00:27:e3:36:4d:a0  rssi
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0  SYNC for Channel (new/old : 40/0) or channel w
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559723997. Detecti
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 rg changed rssi prev -28, new -26
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60  SYNC for Channel (new/old : 1/0) or channel wi
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Updated AP report 00:27:e3:36:4d:a0  rssi -26,
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 rg changed rssi prev -65, new -63
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Updated AP report 00:27:e3:36:4d:a0  rssi -63,
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 RadioType: 3 lradInfo->containSlotId = 1 Receiv

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 RadioType: 3 lradInfo->containSlotId = 2 Receiv

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

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

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

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

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

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

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

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

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

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

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Checking Impersonation source 50:2f:a8:a2:0a:60
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Known AP 0 mfp global 0 AP Auth Global 0 mfp Im

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 APF processing Rogue Client: on slot 0

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 Rogue Client IPv6 addr: Not known

*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 APF processing Rogue Client: on slot 0

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue Client ssid: blizzard

*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 Rogue Client IPv6 addr: Not known

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue Client ssid: 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
*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 rgc change from -38 RSSI -37
*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 rgc change from -39 RSSI -39
*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 Updated AP report 00:27:e3:36:4d:a0 rssi -37, s
*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 Updated AP report 00:27:e3:36:4d:a0 rssi -39, s
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 APF processing Rogue Client: on slot 0

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

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue Client ssid: 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
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rgc change from -61 RSSI -62
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Updated AP report 00:27:e3:36:4d:a0 rssi -62, s
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Looking for Rogue b0:72:bf:93:e0:d7 in known AP
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue AP b0:72:bf:93:e0:d7 is not found either
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Change state from 1 to 2 for rogue AP b0:72:bf:
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg change state Rogue AP: b0:72:bf:93:e0:d7

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

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

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 Freed rogue client table for Rogue AP at 0xfff0

*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
```

سجلات المدائمة المتوقعة

بمجرد اكتشاف/إزالة أحد المخادعين من القائمة المخادعة:

0	المتزوج 5 يونيو، 09:01:57:2019	العميل المخادع: يتم اكتشاف b4:c0:f5:2b:4f:90 بواسطة 1 نقطة وصول نقطة الوصول المخادعة BSSID: a6:b1:e9:f0:e8:41، الحالة: تنبيه، آخر كشف (APs) عميل مخادع mac بوابة عميل مخادع 00:27:e3:36:4d:a0 :لنقطة الوصول 00:00:00:02:02:02.
1	المتزوج في 5 يونيو: 09:00:39 2019	نقطة الوصول المخادعة: 9c:97:26:61:d2:79 التي تمت إزالتها من جهاز طلب (MAC) عبر الراديو الأساسي: التحكم في الوصول للوسائط no:0(802.11n(2.4 جيجاهرتز) الواجهة 00:27:e3:36:4d:a0
2	متزوج 5 يونيو، 5:53:39 م 2019 م	نقطة الوصول الدخيلة: 7c:b7:33:c0:51:14 التي تمت إزالتها من جهاز طلب (MAC) عبر الراديو الأساسي: التحكم في الوصول للوسائط no:0(802.11n(2.4 جيجاهرتز) الواجهة 00:27:e3:36:4d:a0
3	متزوج 5 يونيو، 5:52:27:2019 م	العميل المخادع: يتم اكتشاف FC:3f:7c:5f:b1:1b بواسطة 1 نقطة وصول BSSID: 50:2f:a8:a2:0a:60، الحالة: تنبيه، آخر اكتشاف (APs) عميل مخادع mac بوابة عميل مخادعة 00:27:e3:36:4d:a0 :لنقطة الوصول 00:26:44:73:c5:1d.
4	متزوج 5 يونيو، 5:52:17:2019 م	نقطة الوصول الدخيلة D4:28:d5:da:e0:d4 التي تمت إزالتها من جهاز طلب التحكم في الوصول للوسائط اللاسلكية الأساسية:00:27:e3:36:4d:a0 الواجهة no:0(802.11n(2.4 جيجاهرتز)

توصيات

1. قم بتكوين فحص القناة إلى جميع القنوات إذا كنت تشك في وجود مخادع محتمل في شبكتك.
2. يمكن أن يختلف عدد نقاط الوصول الخاصة بأجهزة كشف المخادع وموقعها من واحد لكل طابق إلى واحد لكل مبنى، ويتوقف ذلك على طبوغرافية الشبكة اللاسلكية. من المستحسن أن يكون هناك نقطة وصول مخادعة واحدة على الأقل في كل طابق من المباني. لأن نقطة الوصول المخادعة تتطلب خطا اتصال لجميع مجالات بث شبكة الطبقة 2 التي يجب مراقبتها، فإن الوضع يعتمد على التخطيط المنطقي للشبكة.

إذا كان الوغد غير مصنف

تحقق من تكوين القواعد المخادعة بشكل صحيح.

تصحيح الأخطاء المفيدة

```
<#root>

(Cisco Controller) >

debug dot11 rogue rule enable


(Cisco Controller) >*emWeb: Jun 05 09:12:27.095:
Debugging session started on Jun 05 09:12:27.095 for WLC AIR-CT3504-K9 Version :8.8.120.0 SN :FCW2245M0
```

```
(Cisco Controller) >
*apfRogueTask_1: Jun 05 09:12:57.135: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16, maxRssiLra
*apfRogueTask_3: Jun 05 09:12:57.135: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLra

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

*apfRogueTask_1: Jun 05 09:13:27.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89, maxRssiLra
*apfRogueTask_3: Jun 05 09:13:27.135: 50:2f:a8:a2:0d:40 Rogue Rule Classify Params: rssi=-62, maxRssiLra
*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, maxRssiLra

*apfRogueTask_1: Jun 05 09:13:57.136: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16, maxRssiLra
*apfRogueTask_3: Jun 05 09:13:57.136: 50:2f:a8:a2:0d:40 Rogue Classification:malicious, RuleName:TestRu

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

توصيات

إذا كانت لديك إدخالات مخادعة معروفة، أضفها في القائمة المسموح بها أو قم بتكوين سياسة المصادقة والتفويض والمحاسبة (AAA) للتحقق من الصحة باستخدام المصادقة والتفويض والمحاسبة (AAA) للعميل المعروفة في قاعدة بيانات المصادقة والتفويض والمحاسبة (AAA).

إن برنامج RLDP الخاص بك يعمل على الأغلب

- إذا كان الوغد في قناة DFS، فإن RLDP لا يعمل.
- لا يعمل RLDP إذا كانت الشبكة المحلية اللاسلكية (WLAN) المخادعة مفتوحة وكان DHCP غير متوفر.
- إذا كانت نقطة الوصول من الوضع المحلي تخدم العميل في قناة DFS، فإنها لا تشارك في عملية RLDP.
- لا يدعم برنامج RLDP في نقاط الوصول من السلسلة 1800i و 1810 OEAP و 1810W و 1815 و 1830 و 1850 و 2800 و 3800 Series AP.

تصحيح الأخطاء المفيدة

```
<#root>

(Cisco Controller) >

debug dot11 rldp enable
```

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

*apfRLDP: Jun 05 12:24:41.291: 50:2f:a8:a2:0a:61 Received request to detect Rogue
*apfRLDP: Jun 05 12:24:41.291: 50:2f:a8:a2:0a:61 Entering apfFindClosestLrad
*apfRLDP: Jun 05 12:24:41.292: Rogue detected slot :0 Rogue contains SlotId :2
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61
```

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

```
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61 Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61 Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:24:41.292: Waiting for ARLDP request

!--- ROGUE detected on DFS channel

*apfRLDP: Jun 05 12:43:16.659: 50:2f:a8:a2:0d:4e Received request to detect Rogue
*apfRLDP: Jun 05 12:43:16.659: 50:2f:a8:a2:0d:4e Entering apfFindClosestLrad
*apfRLDP: Jun 05 12:43:16.660: Rogue detected slot :1 Rogue contains SlotId :1
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e
```

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

```
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:43:16.660: Waiting for ARLDP request

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

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

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

```
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:52:41.980: Waiting for ARLDP request

!--- Association TO ROGUE AP

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Received request to detect Rogue
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Entering apfFindClosestLrad
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Skipping RLDP on AP 94:d4:69:f5:f7:e0 AP Model: AIR-AP
*apfRLDP: Jun 05 15:02:49.602: Rogue detected slot :0 Rogue contains SlotId :0
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61
```

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

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

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

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

*apfRLDP: Jun 05 15:02:50.102: b4:de:31:a4:e0:31 In rldpSendAddMobile:724 setting Central switched to T
*apfRLDP: Jun 05 15:02:50.302: 50:2f:a8:a2:0a:61
```

rldp started association, attempt 1

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

*apfRLDP: Jun 05 15:02:55.346: 50:2f:a8:a2:0a:61 rldp started association, attempt 2
*apfRLDP: Jun 05 15:03:00.390: 50:2f:a8:a2:0a:61 RLDP could not finish the association in time. RLDP St

*apfRLDP: Jun 05 15:03:00.390: 50:2f:a8:a2:0a:61 rldp started association, attempt 3
*apfOpenDtlSocket: Jun 05 15:03:00.608: apfRoguePreamble = 0 mobile b4:de:31:a4:e0:31.
*apfOpenDtlSocket: Jun 05 15:03:00.808:
```

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

(3).

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

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

!--- Attempt to get ip from ROGUE

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

Starting dhcp

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

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

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST

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

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

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

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

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

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 flags: 0x0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 hw_addr: B4:DE:31:A4:E0:31

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 client IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 my IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 server IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 gateway IP: 0.0.0.0

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

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 DHCP message: 1 DISCOVER

*apfRLDP: Jun 05 15:03:00.870: DHCP option: 39/57.2: (2)

*apfRLDP: Jun 05 15:03:00.870: [0000] 02 40

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 host name: RLDP

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 RLDP DHCP SELECTING for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.877: 50:2f:a8:a2:0a:61 Initializing RLDP DHCP for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.877: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 htype: Ethernet

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 hlen: 6

```
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31         hops: 1

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31          xid: 0x3da1f13

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31         secs: 0

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31        flags: 0x0

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31        hw_addr: B4:DE:31:A4:E0:31

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31      client IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31          my IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31      server IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31     gateway IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31   options:

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31         DHCP message: 1 DISCOVER

*apfRLDP: Jun 05 15:03:10.878: DHCP option: 39/57.2: (2)

*apfRLDP: Jun 05 15:03:10.878:      [0000] 02 40

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31           host name: RLDP

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

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31        htype: Ethernet

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31         hlen: 6

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31         hops: 1

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          xid: 0x3da1f13

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31         secs: 0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31        flags: 0x0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31        hw_addr: B4:DE:31:A4:E0:31

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      client IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          my IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      server IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31     gateway IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31   options:

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31         DHCP message: 1 DISCOVER

*apfRLDP: Jun 05 15:03:20.885: DHCP option: 39/57.2: (2)
```

```
*apfRLDP: Jun 05 15:03:20.885:      [0000] 02 40

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          host name: RLDP

*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP 50:2f:a8:a2:0a:61

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

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

توصيات

1. ابدأ تطبيق RLDP يدويا على الإدخالات المخادعة المشبوهة.
2. جدولة RLDP بشكل دوري.
3. يمكن نشر RLDP على نقاط الوصول (APs) المحلية أو وضع المراقبة. بالنسبة لعمليات النشر الأكثر قابلية للتوسع، وللقضاء على أي تأثير على خدمة العملاء، يتم نشر تقنية RLDP على نقاط الوصول في وضع المراقبة عند الإمكان. ومع ذلك، تتطلب هذه التوصية أن يتم نشر تغشية نقطة وصول (AP) لوضع المراقبة بنسبة نموذجية مثل نقطة وصول واحدة لوضع جهاز العرض لكل 5 نقاط وصول في الوضع المحلي. كما يمكن الاستفادة من نقاط الوصول (APs) في وضع جهاز العرض طراز wIPS القابل للتكيف لهذه المهمة.

نقطة الوصول لكاشف المخادع

يمكن رؤية الإدخال المخادع في جهاز كشف المخادع باستخدام هذا الأمر في وحدة تحكم AP. بالنسبة للمخادعين السلكيين، تنتقل العملة إلى تعيين الحالة.

```
<#root>

tiagoAP.6d09.eff0#

show capwap rm rogue detecto

r
 LWAPP Rogue Detector Mode
  Current Rogue Table:
  Rogue hindex = 0: MAC 502f.a8a2.0a61,

flag = 0

, unusedCount = 1
  Rogue hindex = 0: MAC 502f.a8a2.0a60,

flag = 0

, unusedCount = 1
  Rogue hindex = 7: MAC 502f.a8a2.0d41,

flag = 0
```

```
, unusedCount = 1
  Rogue hindex = 7: MAC 502f.a8a2.0d40,
```

flag = 0

```
, unusedCount = 1

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

أوامر تصحيح الأخطاء المفيدة في وحدة تحكم نقطة الوصول (AP)

<#root>

```
Rogue_Detector#
```

debug capwap rm rogue detector

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

إحتواء المخادعين

تصحيح الأخطاء المتوقع

<#root>

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

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

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

Class malicious, Change by Auto State Contained Change by Auto



*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue doesnt qualify for rule classification :

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Manual Contained Flag = 0, trustlevel = 6

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0

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



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

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Trying Containment on 1 band for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Skipping xor radio for 1 band and cont slotid 1
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Found 0 channels to try containment for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Trying Containment on 2 band for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue detected on detected slot 0 contains slot
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Found 1 channels to try containment for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC 00:27:e3:36:4d:a0 RSSI = -28
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC 00:27:e3:36:4d:a0 RSSI = -31
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC b4:de:31:a4:e0:30 RSSI = -33
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC 00:27:e3:36:4d:a0 RSSI = -28 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC 00:27:e3:36:4d:a0 RSSI = -31 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC b4:de:31:a4:e0:30 RSSI = -33 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP b4:de:31:a4:e0:30
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0

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


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

توصيات

1. يمكن أن تحتوي نقطة الوصول من الوضع المحلي/Flex-Connect على 3 أجهزة في كل مرة لكل جهاز السلكي، ويمكن أن تحتوي نقطة الوصول من وضع الشاشة على 6 أجهزة لكل جهاز السلكي. وبنتيجة لذلك، تأكد من أن نقطة الوصول ال تحتوي بالفعل على الحد الأقصى لعدد الأجهزة المسموح بها. في هذه السيناريو، يكون العميل في حالة تعليق الاحتواء.

2. التحقق من قواعد الاحتواء التلقائي.

القرار

يعد اكتشاف الأجهزة المخادعة واحتوائها داخل حدود التحكم المركزية من Cisco الطريقة الأكثر فعالية والأقل تدخلا في هذه الصناعة. تتيح المرونة المتوفرة لمسؤول الشبكة إمكانية توفير مرائمة أكثر تخصيصا يمكنها إستيعاب أي متطلبات للشبكة.

معلومات ذات صلة

- دليل تكوين وحدة التحكم اللاسلكية من Cisco، الإصدار 8.8 - الإدارة الدخيلة
- أفضل ممارسات تكوين Cisco Wireless LAN Controller (WLC)
- دليل نشر WLC 3504 الإصدار 8.5
- دليل نشر وحدة تحكم الشبكة المحلية (LAN) اللاسلكية Cisco 5520
- ملاحظات الإصدار الخاصة بوحدات التحكم اللاسلكية من Cisco ونقاط الوصول في وضع Lightweight، Cisco Wireless، الإصدار 8.8.120.0

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).