통합 무선 네트워크에서 비인가 탐지 및 완화 해결

목차

소개

이 문서에서는 Cisco 무선 네트워크의 비인가 탐지 및 차단에 대해 설명합니다.

무선 네트워크는 유선 네트워크를 확장하고 작업자 생산성과 정보 액세스를 향상시킵니다. 그러나 무단 무선 네트워크는 추가적인 보안 문제를 야기합니다. 유선 네트워크의 포트 보안에는 거의 관심이 없으며, 무선 네트워크는 유선 네트워크로 쉽게 확장됩니다. 따라서 자신의 액세스 포인트(Cisco 또는 Cisco 이외)를 보안이 잘 된 무선 또는 유선 인프라에 연결하고 무단 사용자가 이 보안 네트워크에 액세스하도록 허용하는 직원은 보안 네트워크를 쉽게 손상시킬 수 있습니다.

비인가 탐지는 네트워크 관리자가 이러한 보안 문제를 모니터링하고 제거할 수 있게 해줍니다. Cisco Unified Network Architecture는 비인가 탐지를 위한 방법을 제공하므로 비용이 많이 들고 타당성을 검증하기 어려운 오버레이 네트워크 및 툴을 사용할 필요 없이 완전한 비인가 식별 및 억제 솔루션을 구현할 수 있습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Wireless Lan Controller.
- Cisco Prime Infrastructure입니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 8.8.120.0을 실행하는 Cisco Unified Wireless Lan Controller(5520, 8540 및 3504 Series).
- Wave 2 AP 1832, 1852, 2802 및 3802 시리즈
- 1차 AP 3700, 2700 및 1700 시리즈

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

비인가 개요

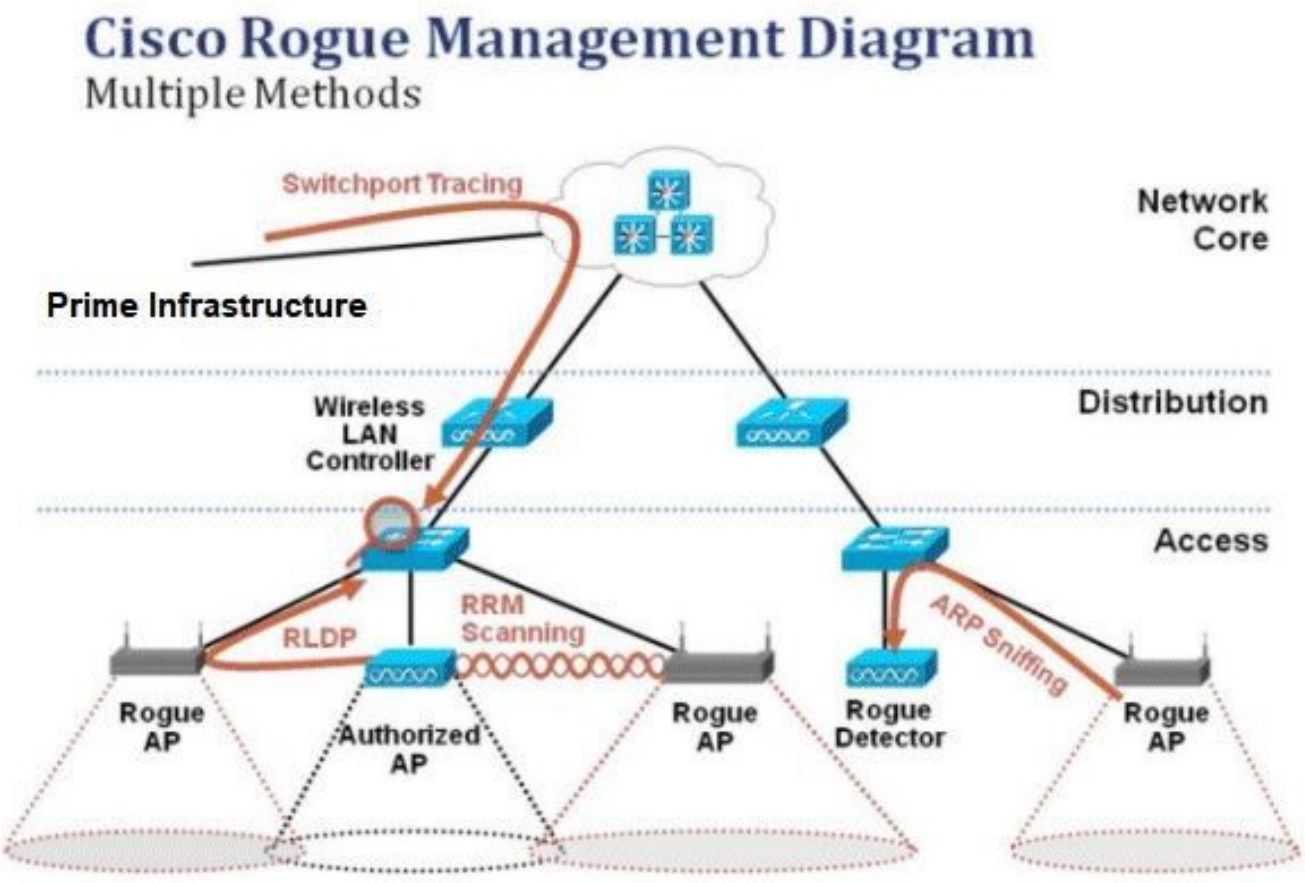
스펙트럼을 공유하고 사용자가 관리하지 않는 디바이스는 비인가 디바이스로 간주될 수 있습니다. 비인가 다음 시나리오에서 위험해집니다.

- 네트워크(허니팟)와 동일한 SSID(Service Set Identifier)를 사용하도록 설정하는 경우.
- 유선 네트워크에서 탐지되는 경우
- 임시 비인가
- 대개 외부 사용자가 악의적인 의도를 가지고 설정합니다.

모범 사례는 로그 탐지를 사용하여 기업 환경 등에서 보안 위험을 최소화하는 것입니다. 그러나 OEAP(Office Extend Access Point) 구축, 도시 전체 및 옥외에서 비인가 탐지가 필요하지 않은 특정 시나리오가 있습니다. 비인가 탐지를 위해 실외 메시 AP를 사용할 경우 분석 리소스에는 거의 도움이 되지 않습니다. 마지막으로, 자동으로 작동되도록 방치할 경우 법적 문제 및 책임의 가능성이 있으므로 비인가 자동 차단을 평가(또는 아예 회피)하는 것이 중요합니다.

Cisco Unified Wireless Network(UWN) 솔루션에는 3가지 주요 비인가 디바이스 관리 단계가 있습니다.

- 탐지 - RRM(Radio Resource Management) 검사는 비인가 디바이스의 존재를 탐지하는 데 사용됩니다.
- 분류 - RLDP(Rogue Location Discovery Protocol), 비인가 탐지기(Wave 1 AP에만 해당) 및 스위치 포트 추적은 비인가 디바이스가 유선 네트워크에 연결되었는지 확인하는 데 사용됩니다. 비인가 분류 규칙은 또한 그 특성에 기초하여 비인가를 특정 카테고리로 여과하는 것을 돕는다.
- 완화 - 스위치 포트 종료, 비인가 위치 및 비인가 차단을 사용하여 물리적 위치를 추적하고 비인가 디바이스의 위협을 무력화합니다.

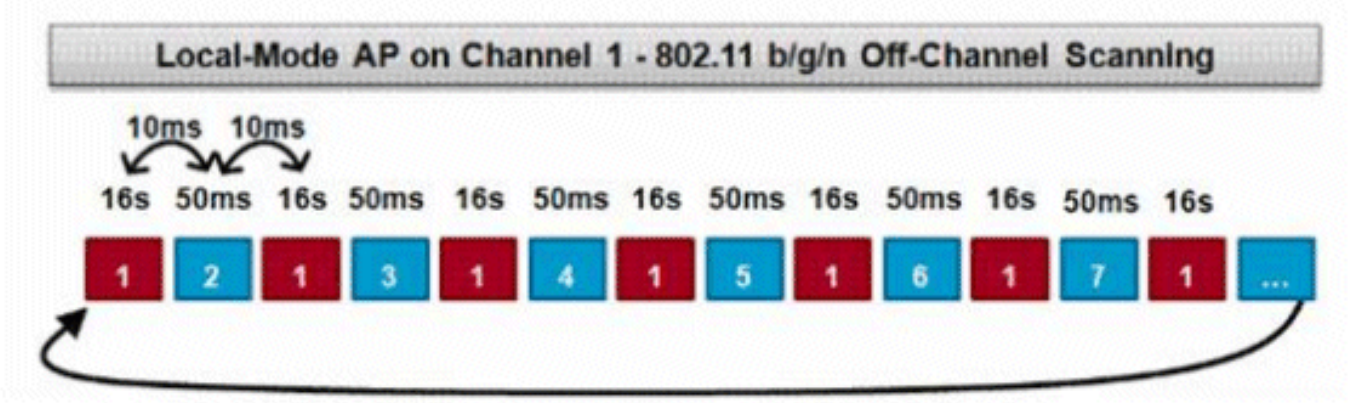


비인가 탐지

비인가 디바이스는 기본적으로 스펙트럼을 공유하지만 제어하지 않는 모든 디바이스입니다. 여기에는 비인가 액세스 포인트, 무선 라우터, 비인가 클라이언트, 비인가 애드혹 네트워크가 포함됩니다. Cisco UWN은 다양한 방법을 사용하여 Wi-Fi 기반 비인가 디바이스(예: 오프 채널 스캔 및 전용 모니터 모드 기능)를 탐지합니다. Cisco Spectrum Expert를 사용하여 Bluetooth 브리지와 같은 802.11 프로토콜을 기반으로 하지 않는 비인가 디바이스를 식별할 수도 있습니다.

오프 채널 스캔

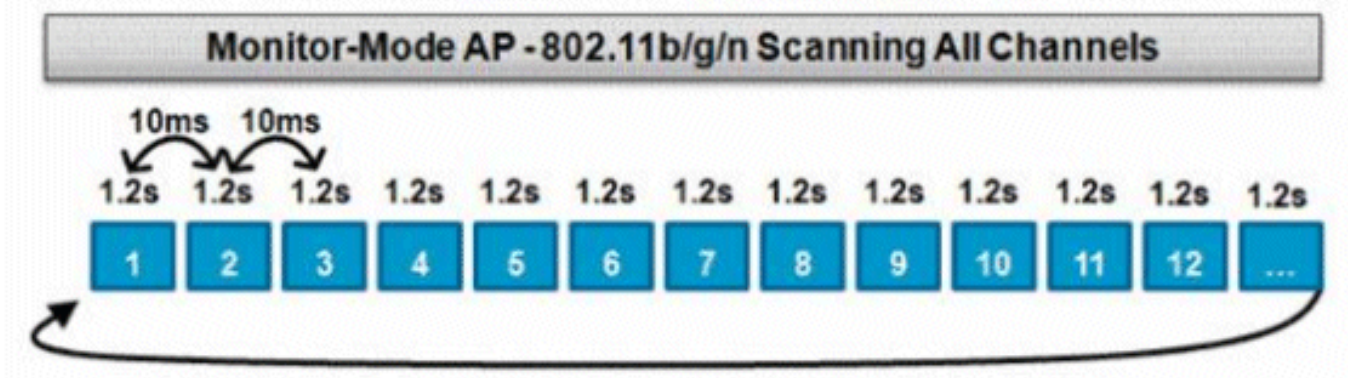
이 작업은 로컬 및 Flex-Connect(연결 모드) 모드 AP에서 수행되며, 동일한 무선 장치를 사용하여 클라이언트 서비스 및 채널 검사를 허용하는 시간 분할 기술을 사용합니다. 16초마다 50ms씩 오프 채널로 이동하므로 AP는 기본적으로 클라이언트에 서비스를 제공하지 않는 데 약간의 시간만 사용합니다. 또한 10ms 채널 변경 간격이 발생합니다. 기본 스캔 간격 180초에서는 각 2.4Ghz FCC 채널(1-11)이 한 번 이상 스캔됩니다. ETSI와 같은 기타 규정 도메인의 경우 AP가 약간 더 높은 시간 백분율로 채널 외부에 있습니다. RRM 컨피그레이션에서 채널 목록 및 스캔 간격을 모두 조정할 수 있습니다. 이는 성능 영향을 최대 1.5%로 제한하며, 음성과 같은 우선 순위가 높은 QoS 프레임을 전달해야 할 때 스캔을 일시 중단하도록 인텔리전스가 알고리즘에 내장되어 있습니다.



이 그래픽은 2.4GHz 주파수 대역의 로컬 모드 AP에 대한 오프 채널 스캔 알고리즘을 나타낸 것이다. AP에 AP가 하나 있는 경우 5GHz 라디오에서 유사한 작업이 병렬로 수행됩니다. 각 빨간색 정사각형은 AP 홈 채널에서 소요된 시간을 나타내며, 각 파란색 정사각형은 스캔을 위해 인접한 채널에서 소요된 시간을 나타냅니다.

모니터 모드 스캔

이 작업은 각 주파수 대역의 모든 채널을 스캔하기 위해 무선 시간을 100% 활용하는 모니터 모드 및 적응형 wIPS 모니터 모드 AP에 의해 수행됩니다. 이를 통해 탐지 속도를 높이고 각 개별 채널에 더 많은 시간을 투자할 수 있습니다. 모니터 모드 AP는 각 채널에서 발생하는 활동을 보다 포괄적으로 볼 수 있으므로 비인가 클라이언트를 훨씬 더 효과적으로 탐지할 수 있습니다.



이 그래픽은 2.4GHz 주파수 대역의 모니터 모드 AP에 대한 오프 채널 스캔 알고리즘을 나타낸 것이다. AP에 AP가 하나 있는 경우 5GHz 라디오에서 유사한 작업이 병렬로 수행됩니다.

로컬 모드 및 모니터 모드 비교

로컬 모드 AP는 WLAN 클라이언트의 서비스와 위협 채널 스캔 간에 주기를 분할합니다. 그 결과, 로컬 모드 AP가 모든 채널을 순환하는 데 시간이 더 오래 걸리고, 클라이언트 작업이 중단되지 않도록 특정 채널에서 데이터를 수집하는 데 걸리는 시간이 줄어듭니다. 따라서 비인가 및 공격 탐지 시간이 더 길며(3~60분), 모니터 모드 AP보다 더 작은 범위의 OTA(over-the-air) 공격을 탐지할 수 있습니다.

또한 비인가 클라이언트와 같은 버스트 트래픽에 대한 탐지는 트래픽이 전송 또는 수신됨과 동시에 AP가 트래픽의 채널에 있어야 하므로 훨씬 덜 확실합니다. 이것은 확률의 연습이 됩니다. 모니터 모드 AP는 모든 주기를 채널 검사에 할애하여 비인가 및 무선 공격을 검색합니다. 모니터 모드 AP는 적응형 wIPS, 위치(상황 인식) 서비스 및 기타 모니터 모드 서비스에 동시에 사용할 수 있습니다.

모니터 모드 AP가 구축되면 탐지 시간이 단축됩니다. Adaptive wIPS를 사용하여 모니터 모드 AP를

추가로 구성하면 더 광범위한 무선 위협 및 공격을 탐지할 수 있습니다.

로컬 모드 AP	모니터 모드 AP
시간 분할 오프 채널 스캔으로 클라이언트 서비스 각 채널에서 50ms 수신 대기 스캔 구성 가능: • 모든 채널 • 국가 채널(기본값) • DCA 채널	전용 스캔 각 채널에서 1.2s 수신 모든 채널 검사

비인가 식별

로컬, Flex-Connect 또는 모니터 모드 AP에서 비인가 디바이스의 프로브 응답 또는 비콘을 수신하는 경우, 이 정보는 CAPWAP를 통해 WLC(Wireless LAN Controller)에 전달됩니다. 오탐을 방지하기 위해 다양한 방법을 사용하여 기타 관리되는 Cisco 기반 AP가 비인가 디바이스로 식별되지 않도록 합니다. 이러한 방법에는 모빌리티 그룹 업데이트, RF 네이버 패킷, PI(Prime Infrastructure)를 통한 허용 목록 친화적 AP 등이 있습니다.

비인가 레코드

컨트롤러의 비인가 디바이스 데이터베이스에는 탐지된 현재 비인가 세트만 포함되어 있지만, PI에는 더 이상 표시되지 않는 이벤트 기록 및 로그 비인가도 포함됩니다.

비인가 세부 정보

CAPWAP AP는 비인가 클라이언트를 수신 대기하고, 노이즈 및 채널 간섭을 모니터링하기 위해 50ms 동안 오프 채널로 전환됩니다. 탐지된 비인가 클라이언트 또는 AP는 컨트롤러로 전송되며, 컨트롤러에서 다음 정보를 수집합니다.

- 비인가 AP MAC 주소
- 비인가 탐지된 AP의 이름
- 비인가 연결된 클라이언트 MAC 주소
- 보안 정책
- 서문
- 신호 대 잡음 비율(SNR)
- 수신기 RSSI(Signal Strength Indicator)
- 비인가 탐지 채널
- 비인가 탐지된 라디오
- 비인가 SSID(비인가 SSID가 브로드캐스트되는 경우)
- 비인가 IP 주소
- 비인가 처음 및 마지막 보고
- 채널 폭

비인가 이벤트를 내보내려면

로그 이벤트를 보관을 위해 서드파티 NMS(Network Management System)로 내보내려면 WLC에서 추가 SNMP 트랩 수신기를 추가할 수 있습니다. 컨트롤러에서 비인가를 감지하거나 제거하면 이 정보가 포함된 트랩이 모든 SNMP 트랩 수신자에게 전달됩니다. SNMP를 통한 이벤트 내보내기의 한 가지 주의 사항은 여러 컨트롤러가 동일한 비인가를 탐지하는 경우, 상관관계가 PI에서만 수행되므

로 NMS에서 중복 이벤트가 확인된다는 것입니다.

비인가 레코드 시간 초과

비인가 AP가 WLC 기록에 추가되면 더 이상 표시되지 않을 때까지 그대로 유지됩니다. 사용자 구성 가능한 시간 초과(기본값 1200초) 후_unclassified_category의 **비인가**가 시간 초과됩니다.

다른 상태(예: **_Contained_**and**_Friendly_**)의 비인가는 다시 나타나는 경우 적절한 분류가 적용되도록 유지됩니다.

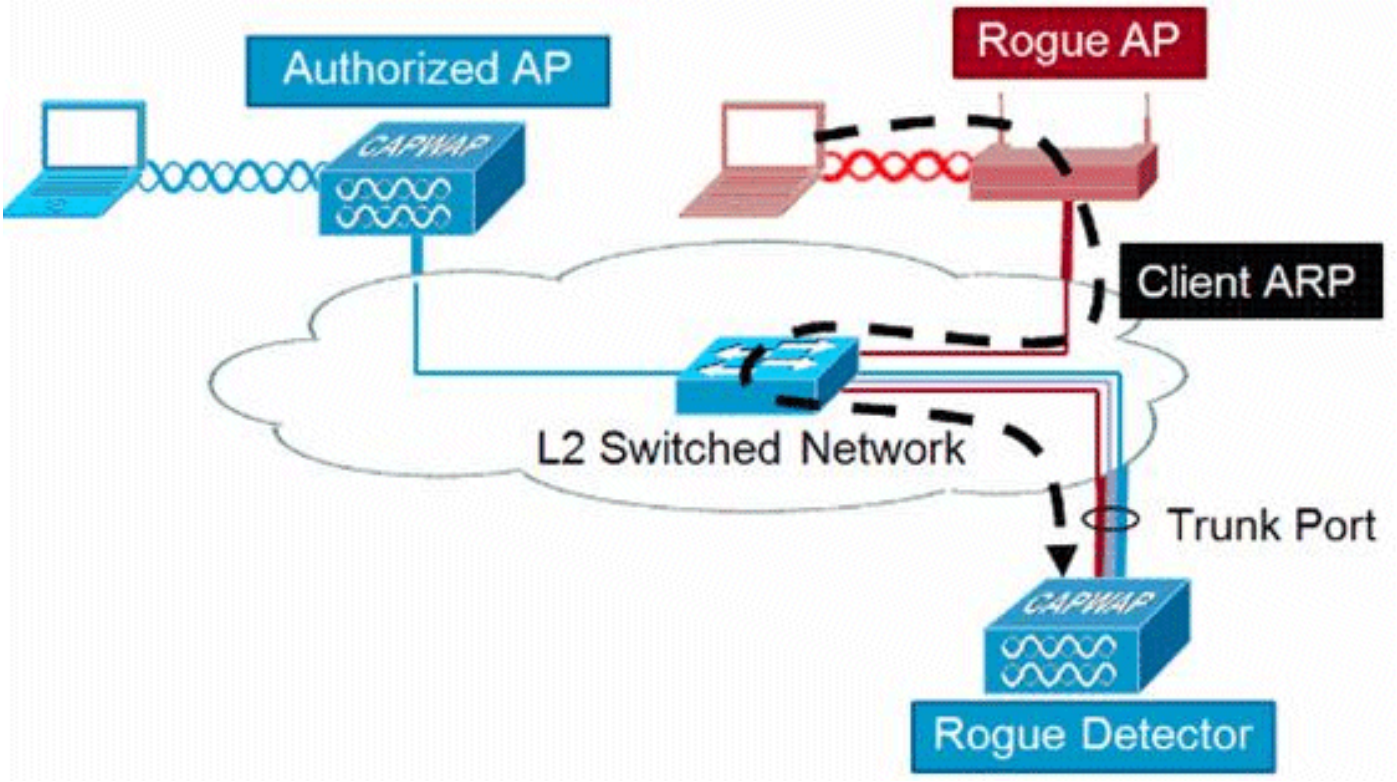
컨트롤러 플랫폼 간에 가변적인 비인가 레코드에 대한 최대 데이터베이스 크기가 있습니다.

- 3504 - 최대 600개의 비인가 AP 및 1500개의 비인가 클라이언트 탐지 및 억제
- 5520 - 최대 24000개의 비인가 AP 및 32000 비인가 클라이언트 탐지 및 억제
- 8540 - 최대 24000개의 비인가 AP 및 32000 비인가 클라이언트 탐지 및 억제

비인가 탐지기 AP

비인가 탐지기 AP는 무선으로 수신되는 비인가 정보와 유선 네트워크에서 얻은 ARP 정보의 상관성을 분석합니다. MAC 주소가 비인가 AP 또는 클라이언트로서 무선으로 수신되고 유선 네트워크에서도 들리면 비인가 AP 주소가 유선 네트워크에 있는 것으로 확인됩니다. 비인가 AP가 유선 네트워크에 있는 것으로 탐지되면 해당 비인가 AP에 대한 경보 심각도가**_critical_로** 높아집니다. 비인가 탐지기 AP는 NAT를 사용하는 디바이스 뒤의 비인가 클라이언트를 식별하지 못합니다.

비인가 AP에 WEP 또는 WPA와 같은 일종의 인증이 있는 경우 이 접근 방식이 사용됩니다. 비인가 AP에 인증 형식이 구성된 경우 비인가 AP에 구성된 인증 방법 및 자격 증명을 모르기 때문에 경량형 AP가 연결할 수 없습니다.



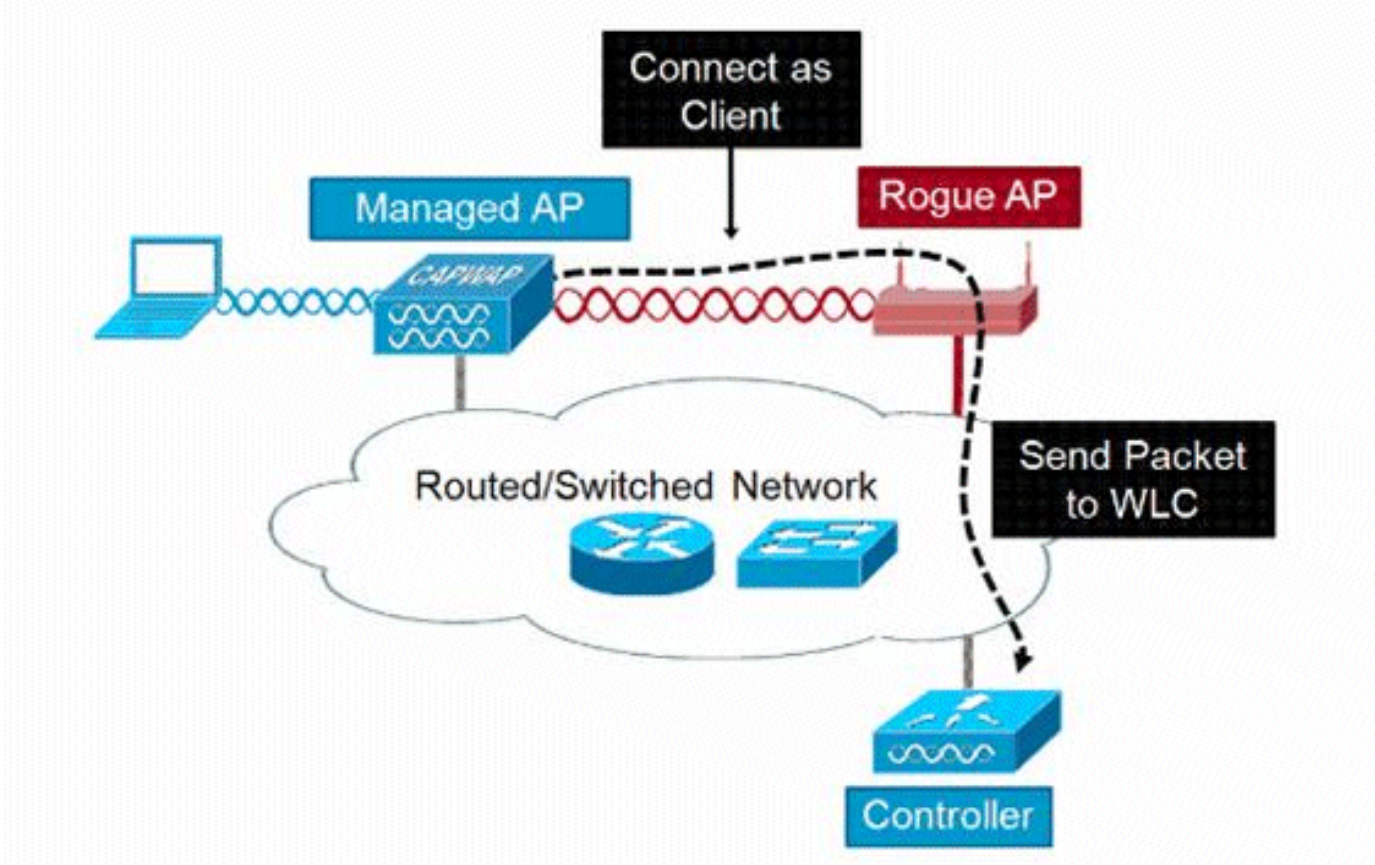
참고: Wave 1 AP만 비인가 탐지기로 구성할 수 있습니다.

확장성 고려 사항

비인가 탐지기 AP는 최대 500개의 비인가 및 500개의 비인가 클라이언트를 탐지할 수 있습니다. 비인가 탐지기가 너무 많은 비인가 디바이스가 있는 트렁크에 배치되면 이러한 제한이 초과되어 문제가 발생합니다. 이 문제가 발생하지 않도록 하려면 비인가 탐지기 AP를 네트워크의 디스트리뷰션 또는 액세스 레이어에 유지하십시오.

RLDP

RLDP의 목적은 특정 비인가 AP가 유선 인프라에 연결되었는지 확인하는 것입니다. 이 기능은 기본적으로 가장 가까운 AP를 사용하여 비인가 디바이스에 무선 클라이언트로 연결합니다. 클라이언트로 연결한 후 AP가 유선 네트워크에 연결되어 있는지 확인하기 위해 WLC의 대상 주소와 함께 패킷이 전송됩니다. 비인가 AP가 유선 네트워크에 있는 것으로 탐지되면 해당 비인가 AP에 대한 경보 심각도가 심각도로 높아집니다.



RLDP의 알고리즘은 다음과 같습니다.

1. 신호 강도 값을 사용하여 비거에 가장 가까운 Unified AP를 식별합니다.
2. 그런 다음 AP가 비인가 클라이언트에 WLAN 클라이언트로 연결하여 시간 초과되기 전에 세 가지 연결을 시도합니다.
3. 연결에 성공하면 AP는 DHCP를 사용하여 IP 주소를 가져옵니다.
4. IP 주소를 얻은 경우 AP(WLAN 클라이언트 역할을 함)는 각 컨트롤러 IP 주소로 UDP 패킷을 전송합니다.

5. 컨트롤러에서 클라이언트로부터 RLDP 패킷 중 하나라도 수신하는 경우, 해당 비인가 패킷은 심각도가 critical인 온 와이어로 표시됩니다.

참고: 필터 규칙이 컨트롤러 네트워크와 비인가 디바이스가 있는 네트워크 사이에 있는 경우 RLDP 패킷이 컨트롤러에 도달할 수 없습니다.

RLDP의 주의

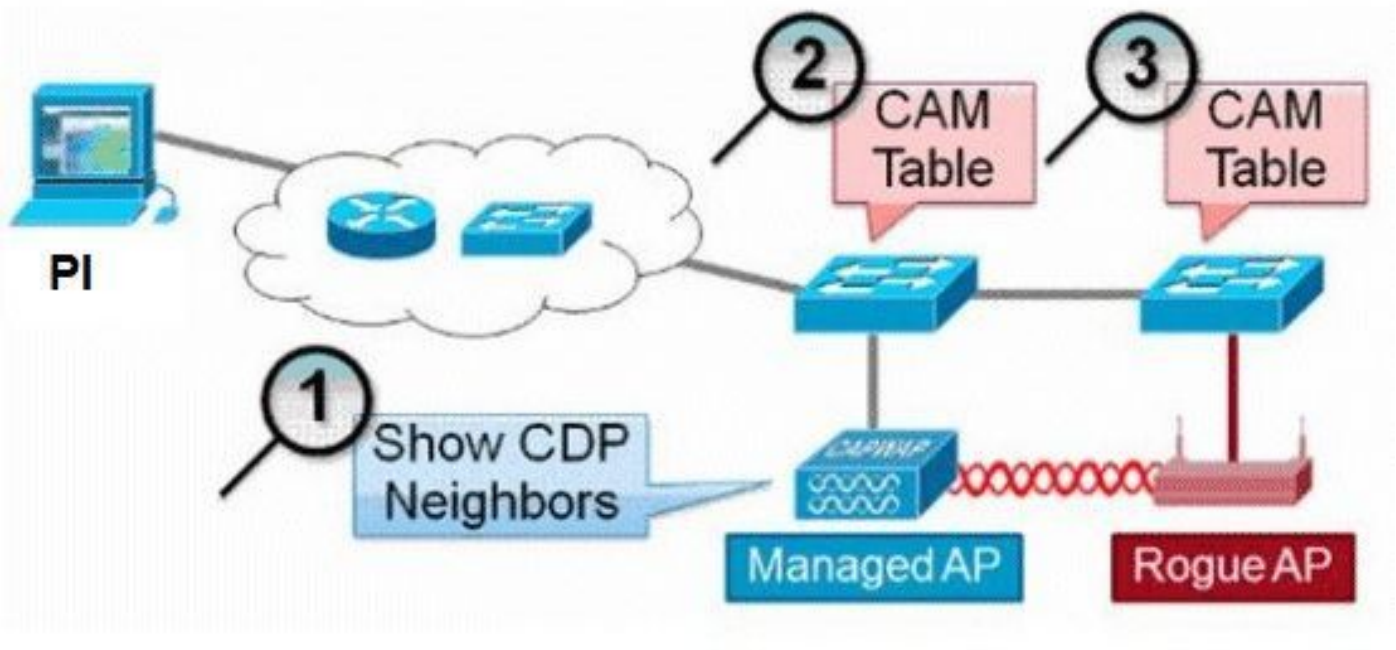
- RLDP는 인증 및 암호화가 비활성화된 상태에서 SSID를 브로드캐스트하는 개방형 비인가 AP에서만 작동합니다.
- RLDP에서는 클라이언트 역할을 하는 관리 대상 AP가 비인가 네트워크에서 DHCP를 통해 IP 주소를 가져올 수 있어야 합니다
- 수동 RLDP를 사용하여 비인가 상태에서 RLDP 추적을 여러 번 시도할 수 있습니다.
- RLDP 프로세스에서 AP가 클라이언트를 지원할 수 없습니다. 이는 로컬 모드 AP의 성능 및 연결에 부정적인 영향을 미칩니다.
- RLDP는 5GHz DFS 채널에서 작동하는 비인가 AP에 연결을 시도하지 않습니다.

스위치 포트 추적

스위치 포트 추적은 비인가 AP 차단 기술입니다. 스위치 포트 추적은 PI에서 시작되지만 CDP 및 SNMP 정보를 모두 활용하여 네트워크의 특정 포트로 비인가를 추적합니다.

스위치 포트 추적이 실행되려면 네트워크의 모든 스위치를 SNMP 자격 증명으로 PI에 추가해야 합니다. 읽기 전용 자격 증명은 비인가 포트가 켜져 있는 포트를 식별하는 데 사용되지만, 읽기-쓰기 자격 증명은 PI가 포트를 종료하도록 허용하므로 위협도 포함합니다.

현재 이 기능은 CDP가 활성화된 Cisco IOS®를 실행하는 Cisco 스위치에서만 작동하며, CDP도 매니지드 AP에서 활성화해야 합니다.



스위치 포트 추적을 위한 알고리즘은 다음과 같습니다.

1. PI는 가장 가까운 AP를 찾아 비인가 AP를 무선으로 탐지하고 CDP 네이버를 검색합니다.

2. 그런 다음 PI는 SNMP를 사용하여 네이버 스위치 내의 CAM 테이블을 검사하고, 비인가 위치를 식별하기 위해 양의 일치를 찾습니다.
3. 양의 매칭은 정확한 비인가 MAC 주소, 비인가 MAC 주소 +1/−1, 비인가 클라이언트 MAC 주소 또는 MAC 주소에 고유한 벤더 정보에 기반한 OUI 매칭을 기반으로 합니다.
4. 가장 가까운 스위치에서 일치하는 양수가 발견되지 않으면 PI는 최대 2홉 떨어진 네이버 스위치에서 검색을 계속합니다(기본값).

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

비인가 분류

기본적으로 Cisco UWN에서 탐지되는 모든 로그는 미분류 로귀로 간주됩니다. 이 그림에서 볼 수 있듯이 비인가는 RSSI, SSID, 보안 유형, 네트워크 온/오프, 클라이언트 수 등 여러 기준에 따라 분류될 수 있습니다.

비인가 분류 규칙

비인가 분류 규칙을 사용하면 비인가를 악의적이거나 친숙한 것으로 표시하는 조건 집합을 정의할 수 있습니다. 이러한 규칙은 PI 또는 WLC에서 구성되지만, 새 로그가 검색되면 컨트롤러에서 항상 수행됩니다.

WLC(Wireless LAN Controller) 및 PI(Prime Infrastructure)의 Rule Based Rogue Classification을 읽고 WLC의 Rogue 규칙에 대한 자세한 내용을 확인하십시오.

HA 팩트

비인가 디바이스를 포함된 상태(모든 클래스) 또는 친절한 상태로 수동으로 이동하면 이 정보는 대기 Cisco WLC 플래시 메모리에 저장됩니다. 그러나 데이터베이스는 업데이트되지 않습니다. HA 전환이 발생하면 이전에 대기 중인 Cisco WLC 플래시 메모리의 로그 목록이 로드됩니다.

고가용성 시나리오에서 비인가 탐지 보안 수준이 High(높음) 또는 Critical(위험)로 설정된 경우 대기 컨트롤러의 비인가 타이머는 비인가 탐지 보류 안정화 시간(300초) 이후에만 시작됩니다. 따라서 스탠바이 컨트롤러의 액티브 컨피그레이션은 300초 후에만 반영됩니다.

Flex-Connect 사실

연결 모드의 FlexConnect AP(비인가 탐지가 활성화된 상태)는 컨트롤러에서 억제 목록을 가져옵니다. 컨트롤러에 자동 포함 SSID 및 자동 포함 애드혹이 설정된 경우 이러한 컨피그레이션은 연결 모드의 모든 FlexConnect AP로 설정되고 AP는 이를 메모리에 저장합니다.

FlexConnect AP가 독립형 모드로 이동하면 다음 작업이 수행됩니다.

- 컨트롤러에서 설정한 컨테인먼트가 계속됩니다.
- FlexConnect AP가 인프라 SSID(FlexConnect AP가 연결된 컨트롤러에 구성된 SSID)와 동일한 SSID를 가진 비인가 AP를 탐지하는 경우, 독립형 모드로 이동하기 전에 컨트롤러에서 자동 SSID 포함이 활성화된 경우 억제가 시작됩니다.
- FlexConnect AP가 애드혹 비인가를 탐지하면 연결 모드에 있을 때 컨트롤러에서 자동 억제 애드혹이 활성화된 경우 억제가 시작됩니다.

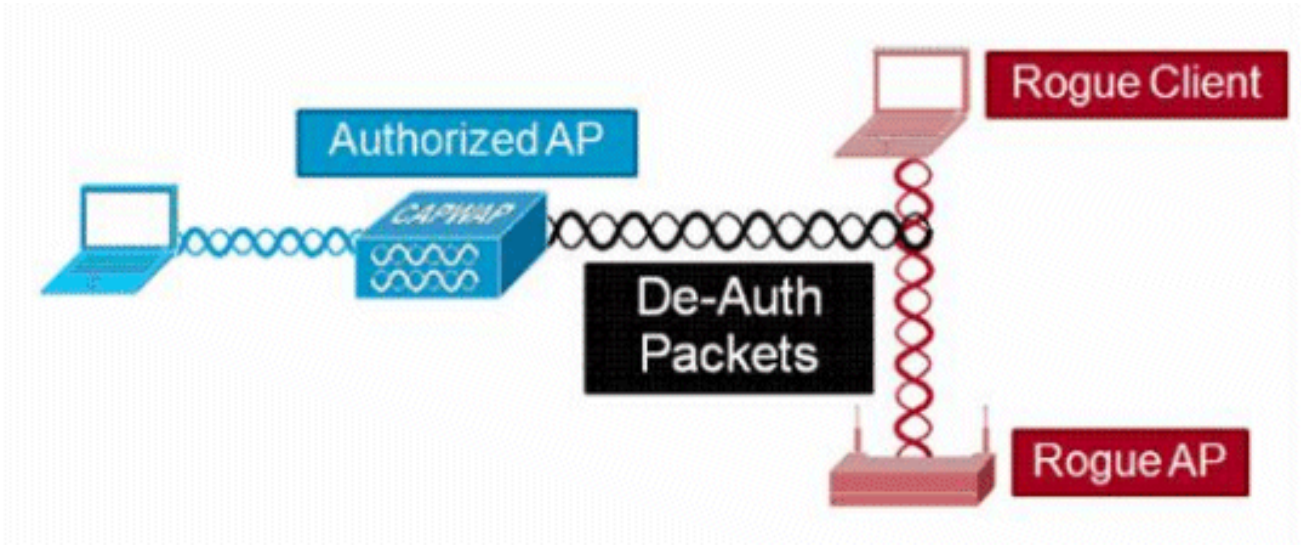
독립형 FlexConnect AP가 연결 모드로 다시 이동하면 다음 작업이 수행됩니다.

- 모든 억제가 해제됩니다.
- 컨트롤러에서 시작된 억제가 적용됩니다.

비인가 완화

비인가 억제

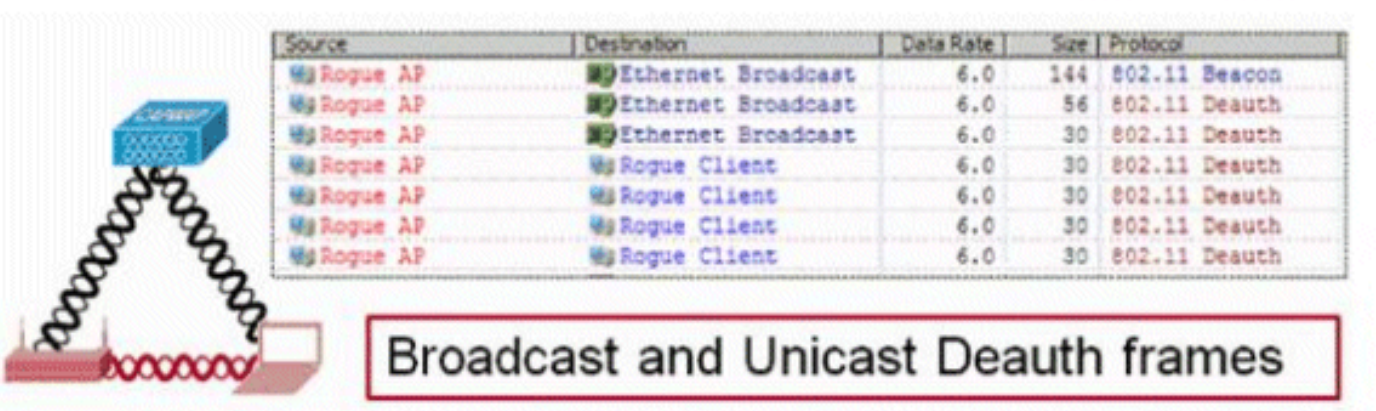
억제는 OTA(over-the-air) 패킷을 사용하여 비인가 디바이스에서 물리적으로 제거될 때까지 서비스를 일시적으로 중단하는 방법입니다. 억제는 비인가 AP의 스푸핑된 소스 주소와 함께 인증 해제 패킷의 스푸핑과 함께 작동하므로 연결된 모든 클라이언트가 해제됩니다.



비인가 억제 세부사항

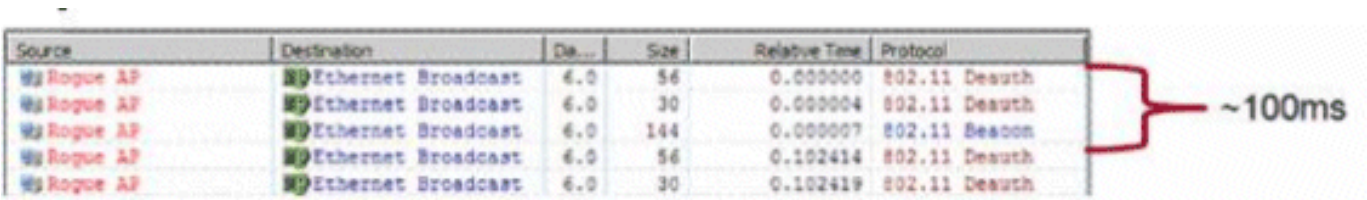
클라이언트가 없는 비인가 AP에서 시작된 억제는 브로드캐스트 주소로 전송된 인증 취소 프레임만 사용합니다.

클라이언트가 있는 비인가 AP에서 시작된 격리는 브로드캐스트 주소 및 클라이언트 주소로 전송된 인증 취소 프레임을 사용합니다.



억제 패킷은 관리되는 AP의 전력 레벨 및 가장 낮은 활성화된 데이터 속도로 전송됩니다.

억제 기능은 100ms마다 최소 2개의 패킷을 전송합니다.



> **참고:** 비모니터 모드 AP에 의해 수행되는 격리는 모니터 모드 AP에서 사용되는 100ms 간격이 아니라 500ms 간격으로 전송됩니다.

- 개별 비인가 디바이스는 위협을 일시적으로 완화하기 위해 함께 작동하는 1~4개의 관리 AP에 포함될 수 있습니다.
- 로컬 모드, 모니터 모드 및 Flex-Connect(Connected) 모드 AP를 사용하여 억제를 수행할 수 있습니다. Flex-connect AP의 로컬 모드에서는 라디오당 최대 3개의 비인가 디바이스를 포함할 수 있습니다. 모니터 모드 AP의 경우 라디오당 최대 6개의 비인가 디바이스를 포함할 수 있습니다.

자동 억제

PI 또는 WLC GUI를 통해 비인가 디바이스에서 억제를 수동으로 시작하는 것 외에도 특정 시나리오에서 억제를 자동으로 시작하는 기능도 있습니다. 이 컨피그레이션은 PI 또는 컨트롤러 **인터페이스**의 Rogue Policies 섹션에서 Generalin에 있습니다. 이러한 각 기능은 기본적으로 비활성화되어 있으며 가장 큰 피해를 일으키는 위협을 무효화하는 데만 활성화됩니다.

- 비인가 온 와이어(Rogue on Wire) - 비인가 디바이스가 유선 네트워크에 연결된 것으로 확인되면 자동으로 격리됩니다.
- SSID 사용 - 비인가 디바이스가 컨트롤러에 구성된 것과 동일한 SSID를 사용하는 경우 자동으로 포함됩니다. 이 기능은 허니팟 공격이 피해를 일으키기 전에 해결하는 것을 목표로 합니다.
- 비인가 AP의 유효한 클라이언트 - Radius/AAA 서버에 나열된 클라이언트가 비인가 디바이스와 연결된 것으로 확인되면 해당 클라이언트에 대해서만 억제가 실행되어 관리되지 않는 AP와의 연결이 차단됩니다.
- AdHoc 비인가 AP - Ad-hoc 네트워크가 검색되면 자동으로 포함됩니다.

비인가 억제 주의 사항

- 격리는 관리 대상 AP의 무선 시간 중 일부를 사용하여 인증 해제 프레임을 전송하기 때문에 데이터 및 음성 클라이언트 모두에 대한 성능은 최대 20%의 부정적인 영향을 받습니다. 데이터 클라이언트의 경우 처리량이 감소합니다. 음성 클라이언트의 경우 억제를 통해 대화가 중단되고 음성 품질이 저하될 수 있습니다.
- 인접 네트워크에 대한 억제를 시작할 경우 법적 문제가 발생할 수 있습니다. 억제를 시작하기 전에 비인가 디바이스가 네트워크 내에 있고 보안 위험이 있는지 확인하십시오.

스위치 포트 종료

스위치 포트가 SPT의 사용으로 추적되면 PI에서 해당 포트를 비활성화하는 옵션이 있습니다. 관리자는 이 작업을 수동으로 수행해야 합니다. 비인가(rogue)가 네트워크에서 물리적으로 제거된 경우 PI를 통해 스위치 포트를 활성화하는 옵션을 사용할 수 있습니다.

구성

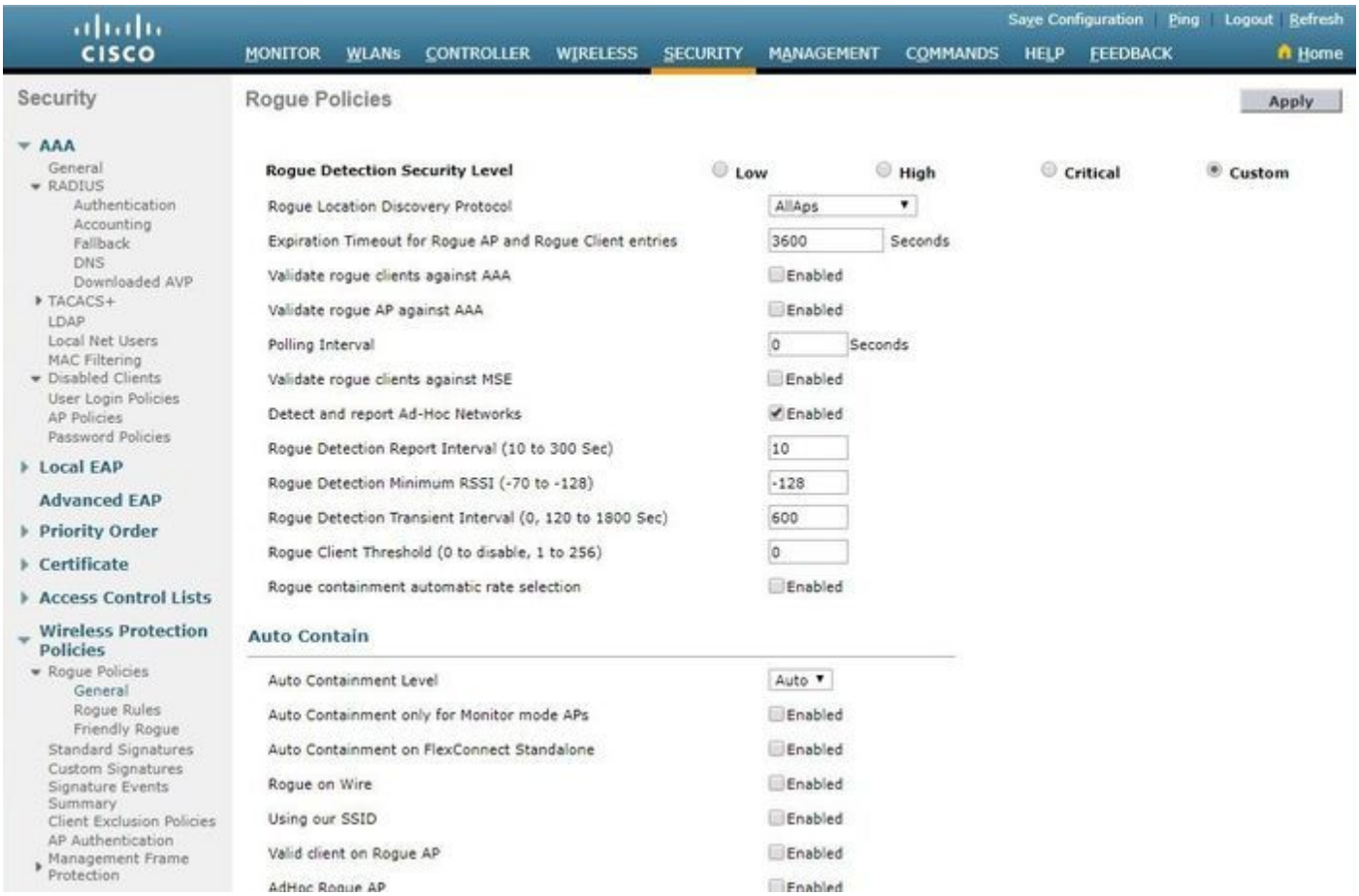
비인가 탐지 구성

비인가 탐지는 기본적으로 컨트롤러에서 활성화됩니다.

다양한 옵션을 구성하려면 Security(보안) > Wireless **Protection Policies(무선 보호 정책) > Rogue Policies(비인가 정책) > General(일반)으로 이동합니다**. 예:

1단계. 비인가 AP에 대한 시간 제한을 변경합니다.

2단계. Ad-hoc 비인가 네트워크 탐지를 활성화합니다.



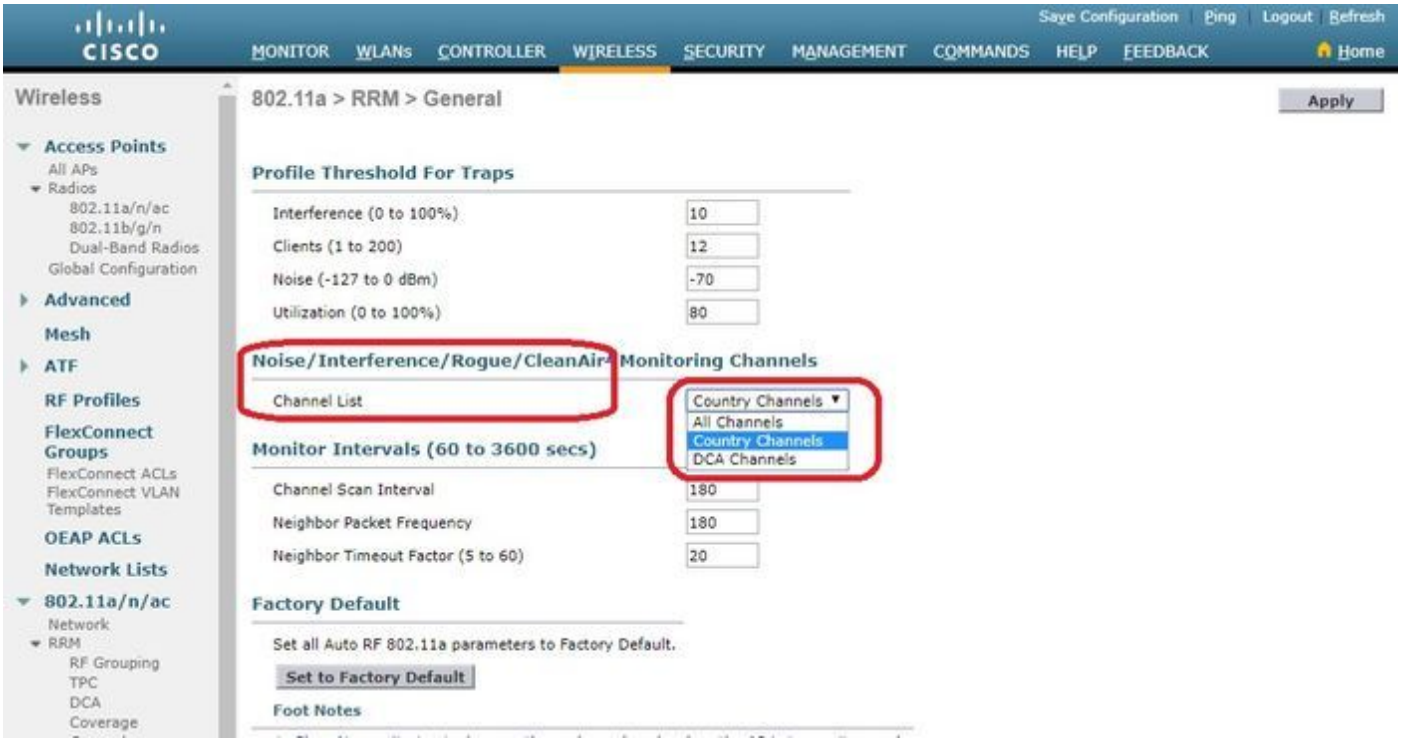
CLI에서:

```
(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
```

비인가 탐지에 대한 채널 스캔 구성

로컬/Flex-Connect/모니터 모드 AP의 경우 RRM 컨피그레이션 아래에 어떤 채널에서 비인가를 검사할지 선택할 수 있는 옵션이 있습니다. 구성에 따라 AP가 모든 채널/국가 채널/DCA 채널에서 비인가를 검사합니다.

GUI에서 이를 구성하려면 이미지에 표시된 대로 **Wireless(무선) > 802.11a/802.11b > RRM > General(일반)**으로 이동합니다.



CLI에서:

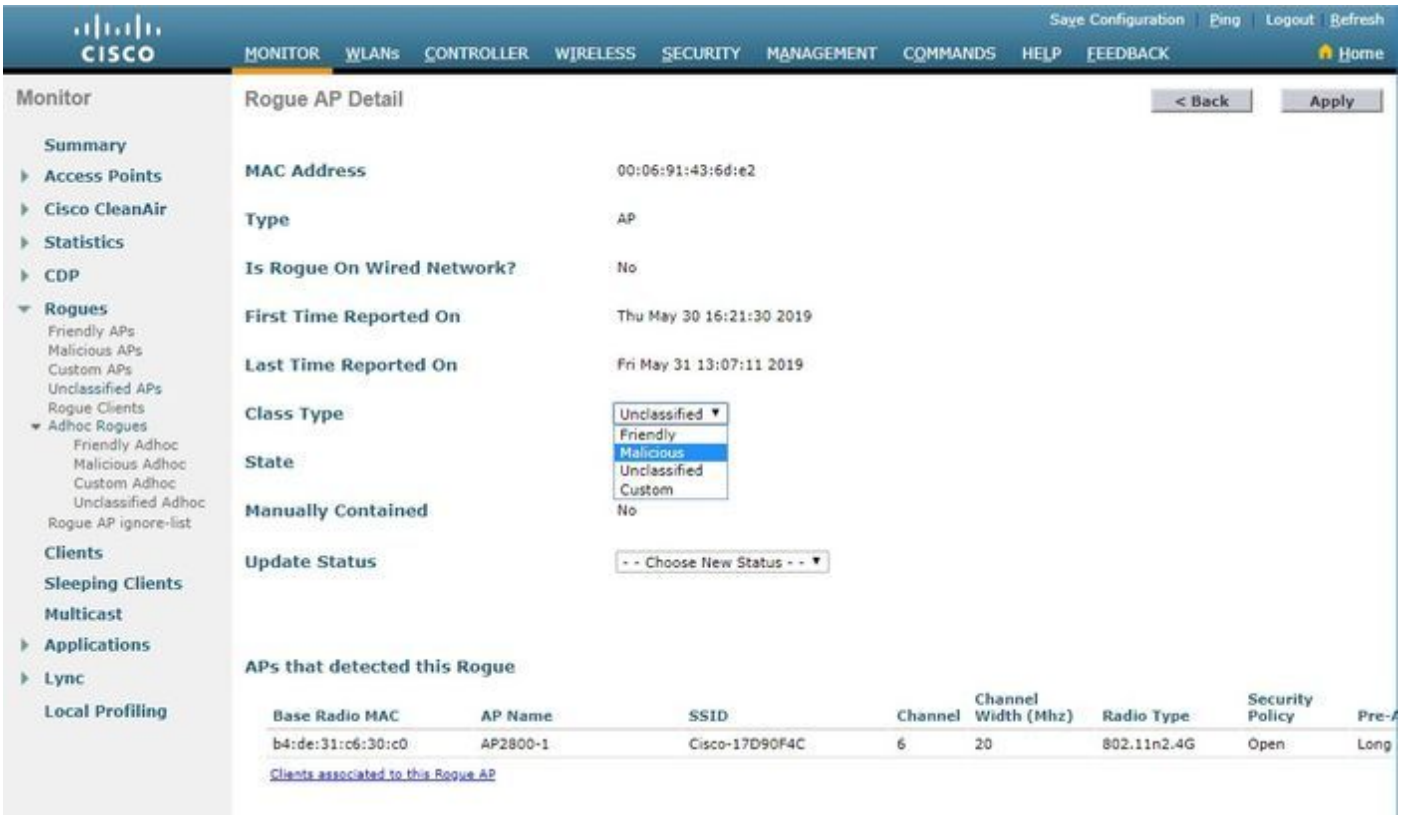
```
(Cisco Controller) >config advanced 802.11a monitor channel-list ?

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

비인가 분류 구성

비인가 AP 수동 분류

비인가 AP를 친절, 악의적 또는 미분류 AP로 분류하려면 **Monitor(모니터링) > Rogue(비인가) > Unclassified** APs(미분류 AP)로 이동하여 특정 비인가 AP 이름을 클릭합니다. 이미지에 표시된 대

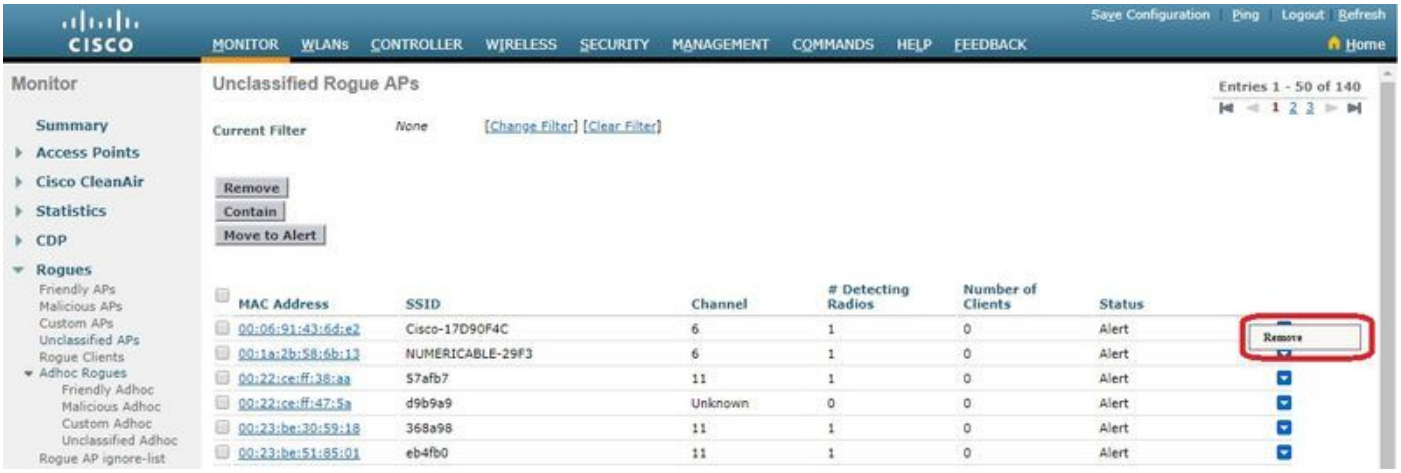
로 드롭다운 목록에서 옵션을 선택합니다.



CLI에서:

```
(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.
```

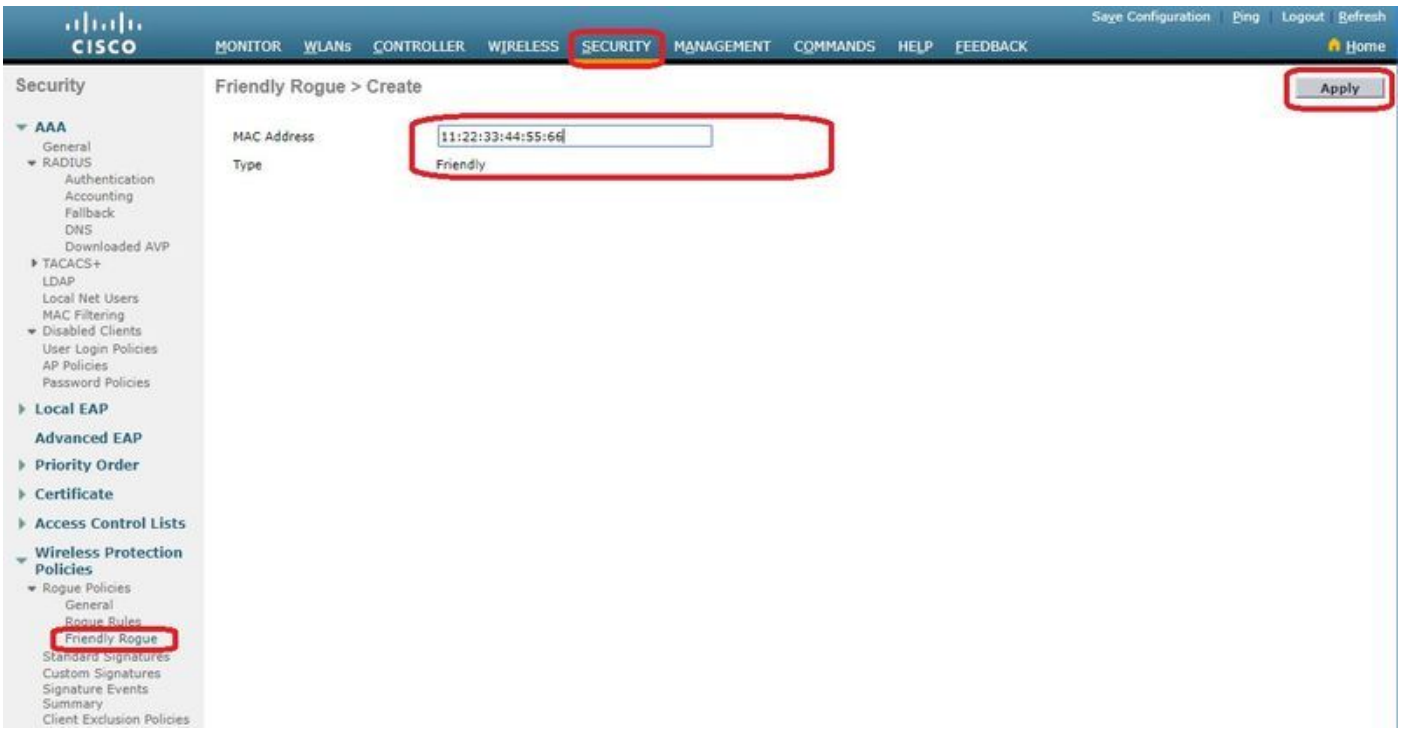
비인가 목록에서 비인가 항목을 수동으로 제거하려면 이미지에 표시된 대로 **Monitor(모니터링) > Rogue(비인가) > Unclassified** APs(분류되지 않은 AP)로 **이동하고 Remove(제거)**를 클릭합니다.



비인가 AP를 친화적 AP로 구성하려면 **Security(보안) > Wireless Protection Policies(무선 보호 정책) > Rogue Policies(비인가 정책) > Friendly Roges(친숙한** 로그)로 이동하고 비인가 MAC 주소를

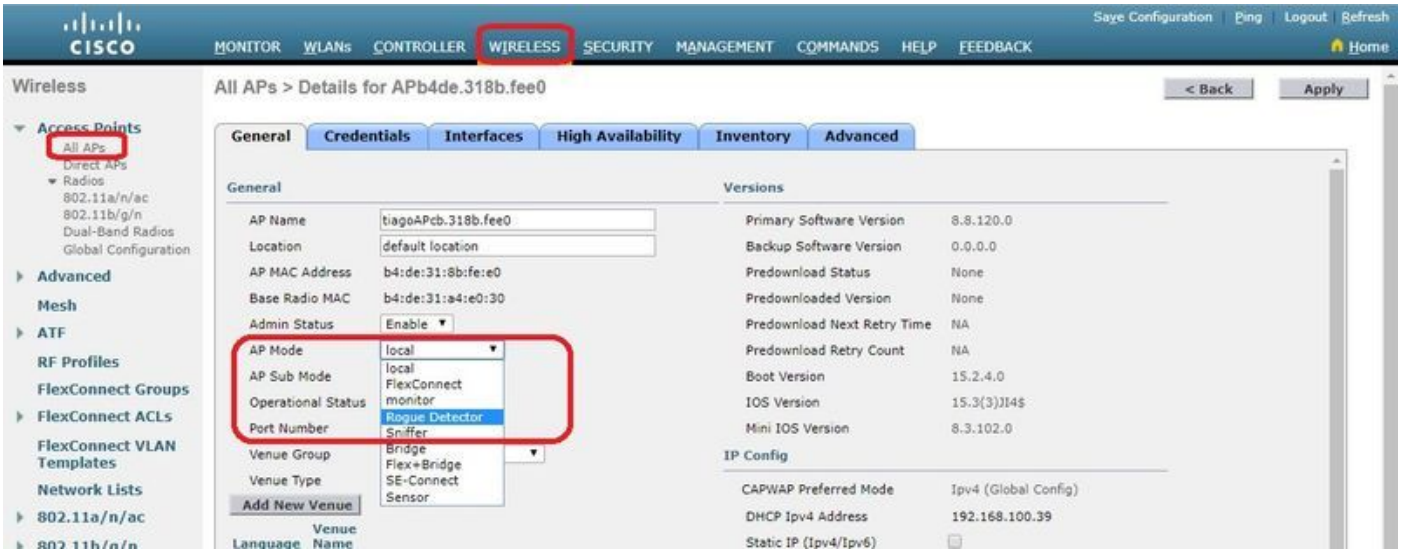
추가합니다.

추가된 Friendly Rogue 항목은 이미지에 표시된 대로 **Monitor(모니터) > Rogues(비인가) > Friendly** Roguepage(친숙한 비인가)에서 확인할 수 있습니다.



비인가 탐지기 AP 구성

GUI를 통해 AP를 비인가 탐지기로 구성하려면 Wireless(무선) > All APs(모든 AP)로 이동합니다. 이미지에 표시된 대로 AP 이름을 선택하고 AP 모드를 변경합니다.



CLI에서:

```
(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
```

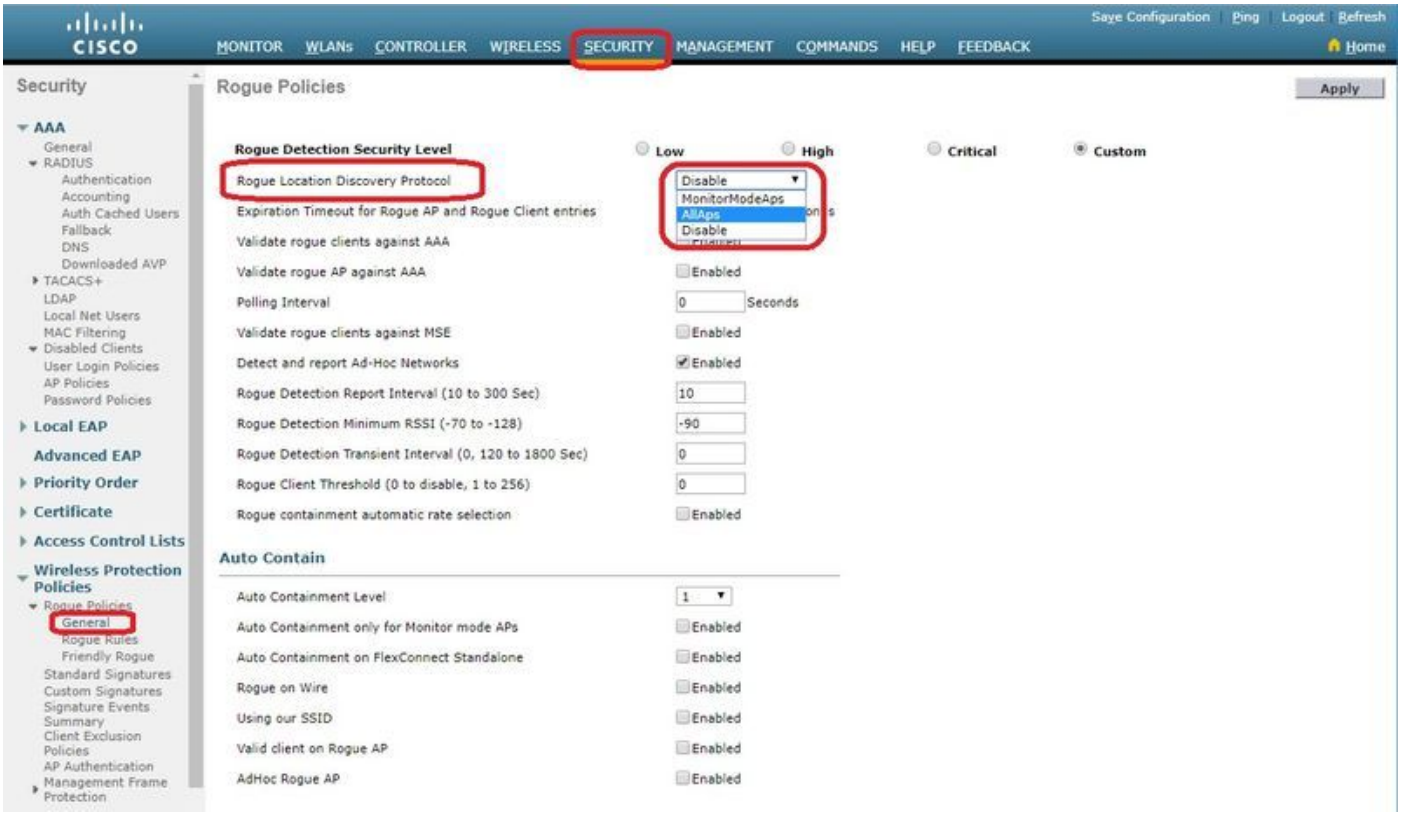
비인가 탐지기 AP에 대한 Switchport 구성

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

참고: 이 컨피그레이션의 네이티브 VLAN은 WLC에 대한 IP 연결이 있는 VLAN입니다.

RLDP 구성

컨트롤러 GUI에서 RLDP를 구성하려면 **Security(보안) > Wireless Protection Policies(무선 보호 정책) > Rogue Policies(비인가 정책) > General(일반)으로 이동합니다**.



Monitor Mode APs(모니터 모드 AP) - 모니터 모드의 AP만 RLDP에 참여할 수 있습니다.

모든 AP- Local/Flex-Connect/Monitor 모드 AP가 RLDP 프로세스에 참여합니다.

Disabled(비활성화됨) - RLDP가 자동으로 트리거되지 않습니다. 그러나 사용자는 CLI를 통해 특정 MAC 주소에 대해 RLDP를 수동으로 트리거할 수 있습니다.

참고: 모니터 모드 AP는 로컬/Flex-Connect AP보다 선호도가 높으므로 둘 다 -85dbm RSSI를 초과하는 특정 비인가를 탐지할 경우 RLDP를 수행합니다.

CLI에서:

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

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

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

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

RLDP 일정 및 수동 트리거는 명령 프롬프트를 통해서만 구성할 수 있습니다. RLDP를 수동으로 시작하려면

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

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

RLDP 일정:

```
(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.
```

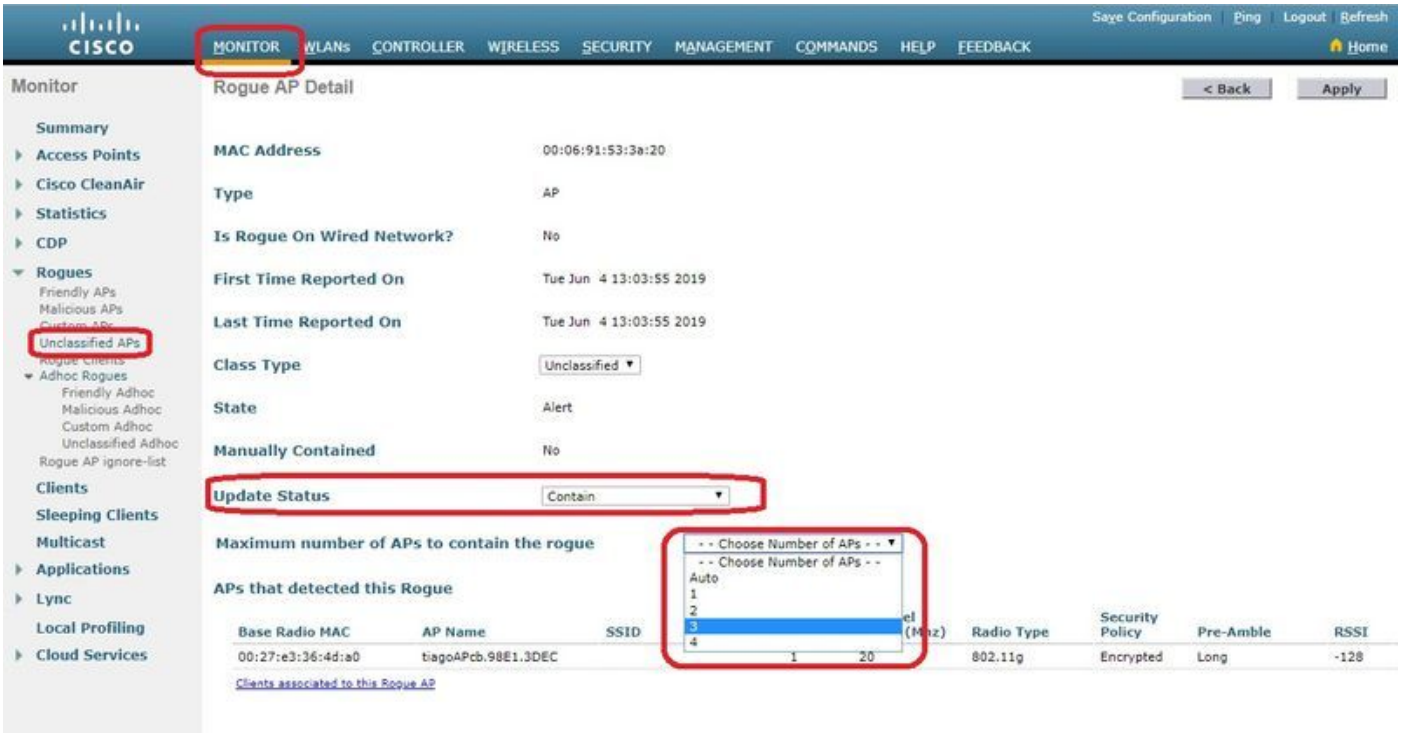
RLDP 재시도는 다음 명령으로 구성할 수 있습니다.

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

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

비인가 완화 구성

수동 억제 구성

비인가 AP를 수동으로 포함하려면 이미지에 표시된 대로 **Monitor(모니터링) > Rogues(비분류**) > Unclassified(미분류)로 이동합니다.



CLI에서:

```
(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].
```

> **참고:** 특정 비인가 AP는 1~4개까지 포함할 수 있습니다. 기본적으로 컨트롤러는 하나의 AP를 사용하여 클라이언트를 포함합니다. 두 AP가 특정 비인가를 탐지할 수 있는 경우, AP 모드에 관계없이 RSSI가 가장 높은 AP에 클라이언트가 포함됩니다.

자동 억제

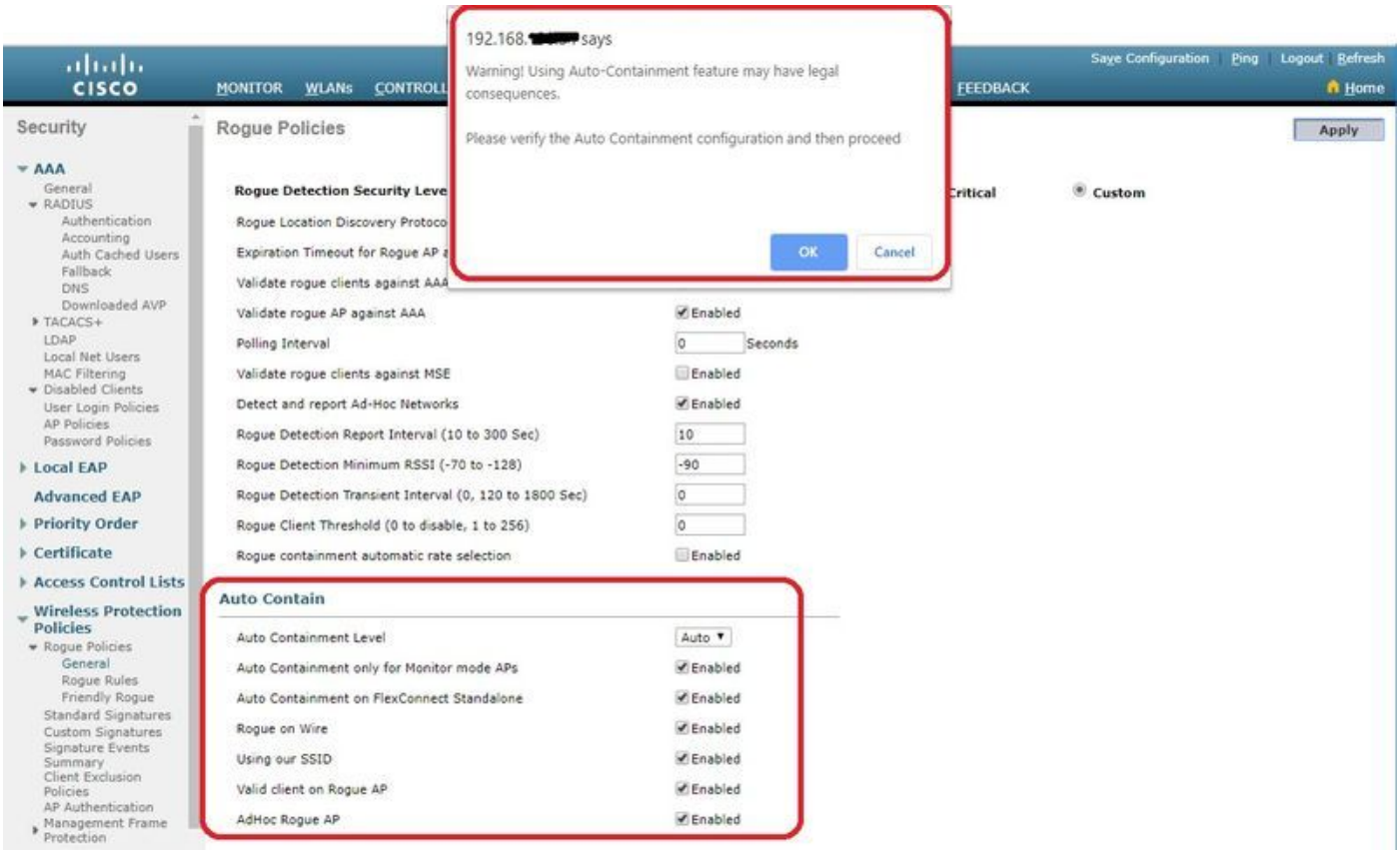
자동 억제를 구성하려면 **Security>Wireless Protection Policies>Rogue Policies>General**로 이동하여 **네트워크에** 적용할 수 있는 모든 옵션을 활성화합니다.

Cisco WLC에 특정 비인가 디바이스를 자동으로 포함하도록 하려면 해당 확인란을 선택합니다. 그렇지 않으면 확인란을 선택하지 않은 상태로 둡니다(기본값).

> **경고:** 이러한 매개변수 중 하나를 활성화하면 "이 기능의 사용은 법적 결과를 초래합니다. 계속하시겠습니까?" ISM(Industrial, Scientific, and Medical) 대역의 2.4GHz 및 5GHz 주파수는 일반인에게 공개되며 라이선스 없이 사용할 수 있다. 따라서 다른 당사자의 네트워크에 있는 디바이스를 억제한다면 법적 결과를 초래할 수 있습니다.

다음은 자동 포함 매개변수입니다.

매개변수	설명
자동 억제 레벨	비인가 자동 억제 레벨을 1에서 4까지 선택할 수 있는 드롭다운 목록입니다. 비인가 AP가 자동 억제 정책을 통해 포함된 상태로 이동될 경우 자동 억제를 위해 최대 4개의 AP를 선택할 수 있습니다. 자동 억제에 사용되는 AP 수를 자동으로 선택하려면 Auto(자동)를 선택할 수도 있습니다. Cisco WLC는 효과적인 억제를 위해 RSSI에 따라 필요한 AP 수를 선택합니다. 각 포함 레벨과 연결된 RSSI 값은 다음과 같습니다. • 1 - 0 ~ -55dBm • 2 - -75 ~ -55dBm • 3 - -85 ~ -75dBm • 4 - -85dBm 미만
모니터 모드 AP에 대해서만 자동 억제	자동 억제를 위해 모니터 모드 AP를 활성화하기 위해 선택할 수 있는 확인란을 선택합니다. 기본값은 disabled 상태입니다.
FlexConnect 독립형 자동 억제	독립형 모드의 FlexConnect AP에서 자동 억제를 활성화하도록 선택할 수 있는 확인란을 선택합니다. 기본값은 disabled 상태입니다. FlexConnect AP가 독립형 모드인 경우 Use our SSID or AdHoc Rogue AP auto containment policies(SSID 또는 AdHoc 비인가 AP 자동 억제 정책 사용)만 활성화할 수 있습니다. 독립형 AP가 Cisco WLC에 다시 연결되면 격리가 중지됩니다.
비인가 온라인	유선 네트워크에서 탐지된 비인가를 자동으로 포함하려면 이 확인란을 선택합니다. 기본값은 disabled 상태입니다.
SSID 사용	네트워크의 SSID를 광고하는 해당 비인가를 자동으로 포함하도록 활성화하는 확인란을 선택합니다. 이 매개변수를 선택하지 않은 상태로 두면 Cisco WLC는 비인가 메시지가 탐지될 때만 경보를 생성합니다. 기본값은 disabled 상태입니다.
비인가 AP의 유효한 클라이언트	신뢰할 수 있는 클라이언트가 연결된 비인가 액세스 포인트를 자동으로 포함하려면 이 확인란을 선택합니다. 이 매개변수를 선택하지 않은 상태로 두면 Cisco WLC는 비인가 메시지가 탐지될 때만 경보를 생성합니다. 기본값은 disabled 상태입니다.
애드혹 비인가 AP	Cisco WLC에서 탐지된 Ad-hoc 네트워크를 자동으로 포함하도록 설정하는 확인란을 선택합니다. 이 매개변수를 선택하지 않은 상태로 두면 Cisco WLC는 해당 네트워크가 탐지될 때만 경보를 생성합니다. 기본값은 disabled 상태입니다.



Apply(적용)를 클릭하여 Cisco WLC로 데이터를 보내지만 데이터가 전력 사이클 전반에 보존되지 않습니다. 이러한 매개변수는 휘발성 RAM에 임시로 저장됩니다.

CLI에서:

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

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

(Cisco Controller) >config rogue adhoc auto-contain ?
(Cisco Controller) >config rogue adhoc auto-contain
 Warning! Use of this feature has legal consequences
         Do you want to continue(y/n) :y
```

Prime Infrastructure와

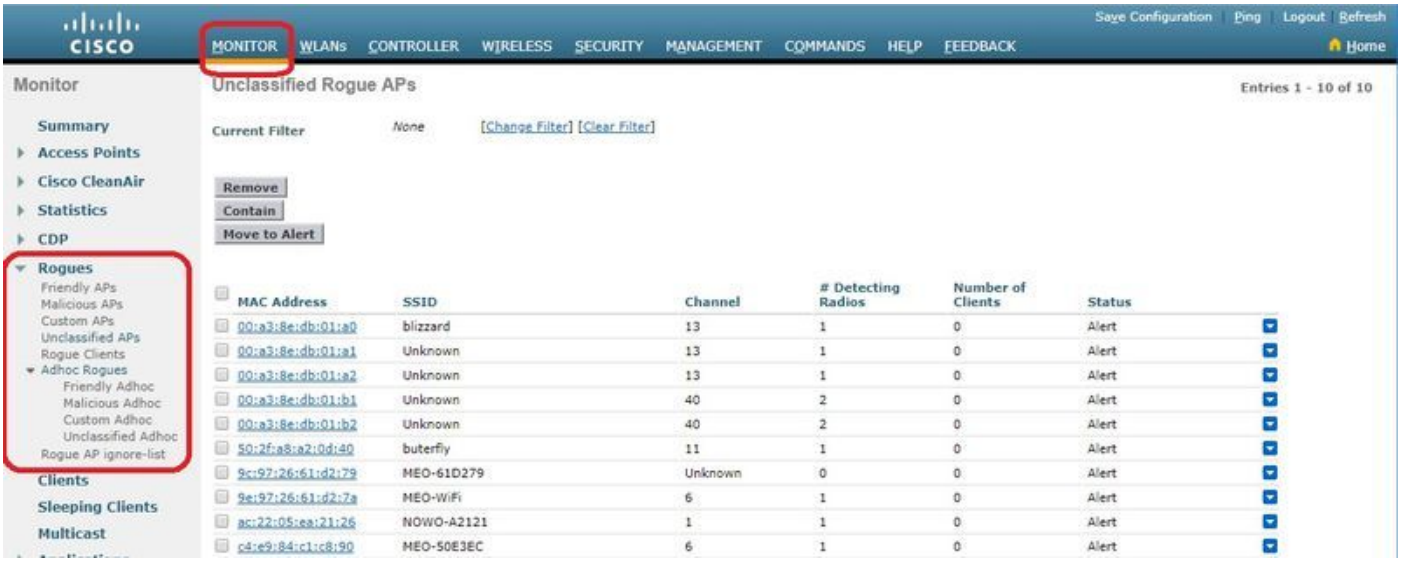
Cisco Prime Infrastructure를 사용하여 하나 이상의 컨트롤러 및 관련 AP를 구성하고 모니터링할 수 있습니다. Cisco PI에는 대용량 시스템의 모니터링 및 제어를 지원하는 툴이 있습니다. Cisco 무선 솔루션에서 Cisco PI를 사용하는 경우 컨트롤러는 정기적으로 클라이언트, 비인가 액세스 포인트, 비인가 액세스 포인트 클라이언트, RFID(무선 주파수 ID) 태그 위치를 확인하고 Cisco PI 데이터베이스에 위치를 저장합니다.

Cisco Prime Infrastructure는 규칙 기반 분류를 지원하고 컨트롤러에 구성된 분류 규칙을 사용합니다. 컨트롤러는 다음 이벤트 후에 Cisco Prime Infrastructure에 트랩을 전송합니다.

- 알 수 없는 액세스 포인트가 처음으로 Friendly(친숙한) 상태로 전환되는 경우 컨트롤러는 비인가 상태가 Alert(알림)인 경우에만 Cisco Prime Infrastructure에 트랩을 전송합니다. 내부 또는 외부인 경우 트랩**을** 전송하지 **않습니다.**
- 시간이 만료된 후 arogueentry가 제거되면 컨트롤러는 **Malicious**(Alert, Threat) 또는 Unclassified(Alert)로 분류된 Cisco Prime Infrastructureforrogueaccess 포인트에 트랩을 보냅니다. 컨트롤러는 다음과 같은 게스트가 있는 항목을 제거하지 않습니다. **포함, 포함 보류**, **내부** 및 **외부**

다음을 확인합니다.

그래픽 인터페이스의 컨트롤러에서 비인가 세부사항을 찾으려면 이미지에 표시된 대로 **Monitor(모니터링) >** Rogues(비인가)로 이동합니다.

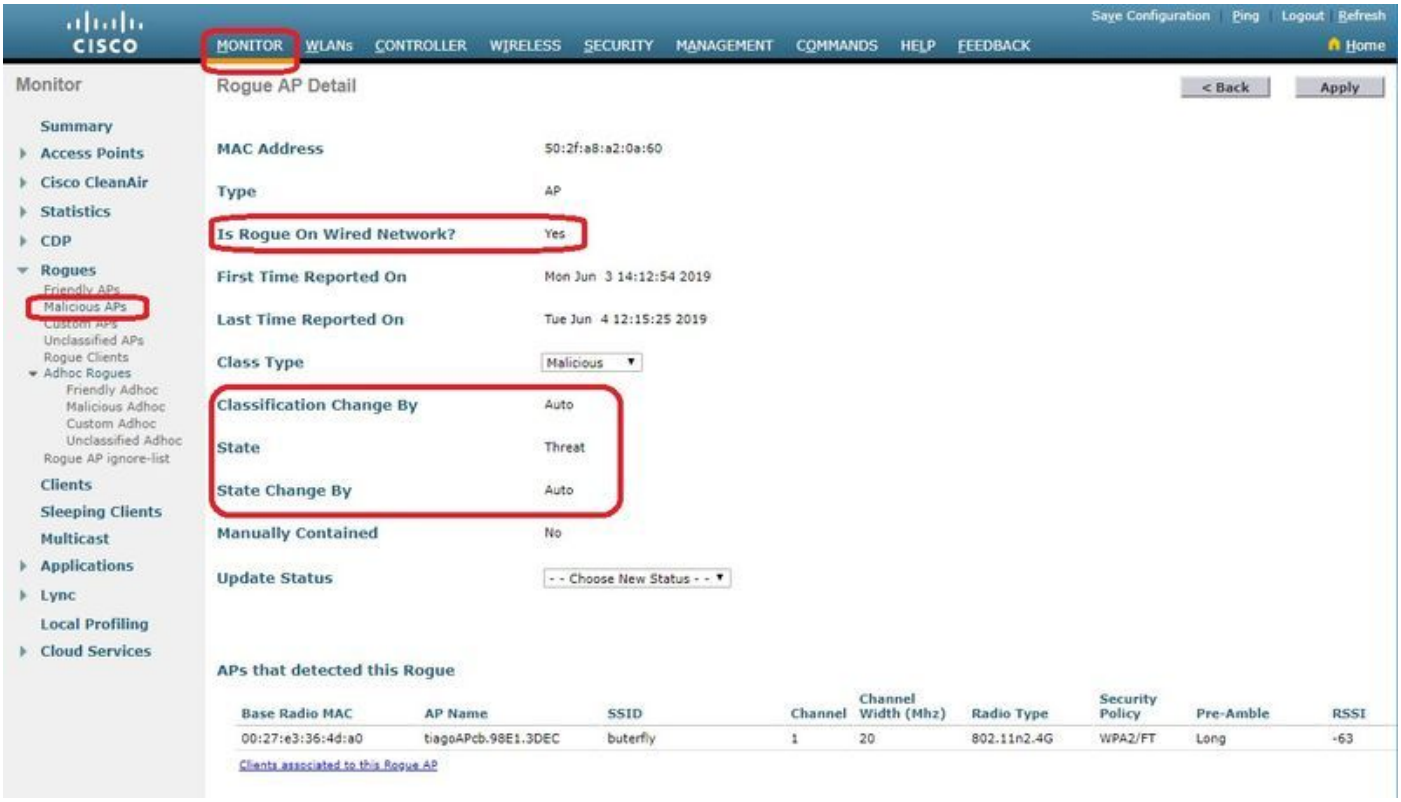


이 페이지에서는 여러 가지 비인가 분류를 사용할 수 있습니다.

- 친숙한 AP - 관리자가 친숙한 것으로 표시한 AP.
- 악성 AP - RLDP 또는 비인가 탐지기 AP를 통해 악성으로 확인된 AP.
- 사용자 지정 AP - 비인가 규칙에 의해 사용자 지정으로 분류된 AP.
- 미분류 AP - 기본적으로 비인가 AP는 컨트롤러에서 미분류 목록으로 표시됩니다.
- 비인가 클라이언트 - 비인가 AP에 연결된 클라이언트.
- Adhoc 비인가 - Adhoc 비인가 클라이언트.
- 비인가 AP 무시 목록 - PI를 통해 나열됨

참고: WLC 및 자동 AP가 동일한 PI에 의해 관리되는 경우 WLC는 Rogue AP 무시 목록에 이 자동 AP를 자동으로 나열합니다. 이 기능을 활성화하기 위해 WLC에 추가 컨피그레이션이 필요하지 않습니다.

특정 비인가 항목을 클릭하면 해당 비인가의 세부 정보를 확인할 수 있습니다. 다음은 유선 네트워크에서 탐지된 비인가 사례입니다.



CLI에서:

```
(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
```

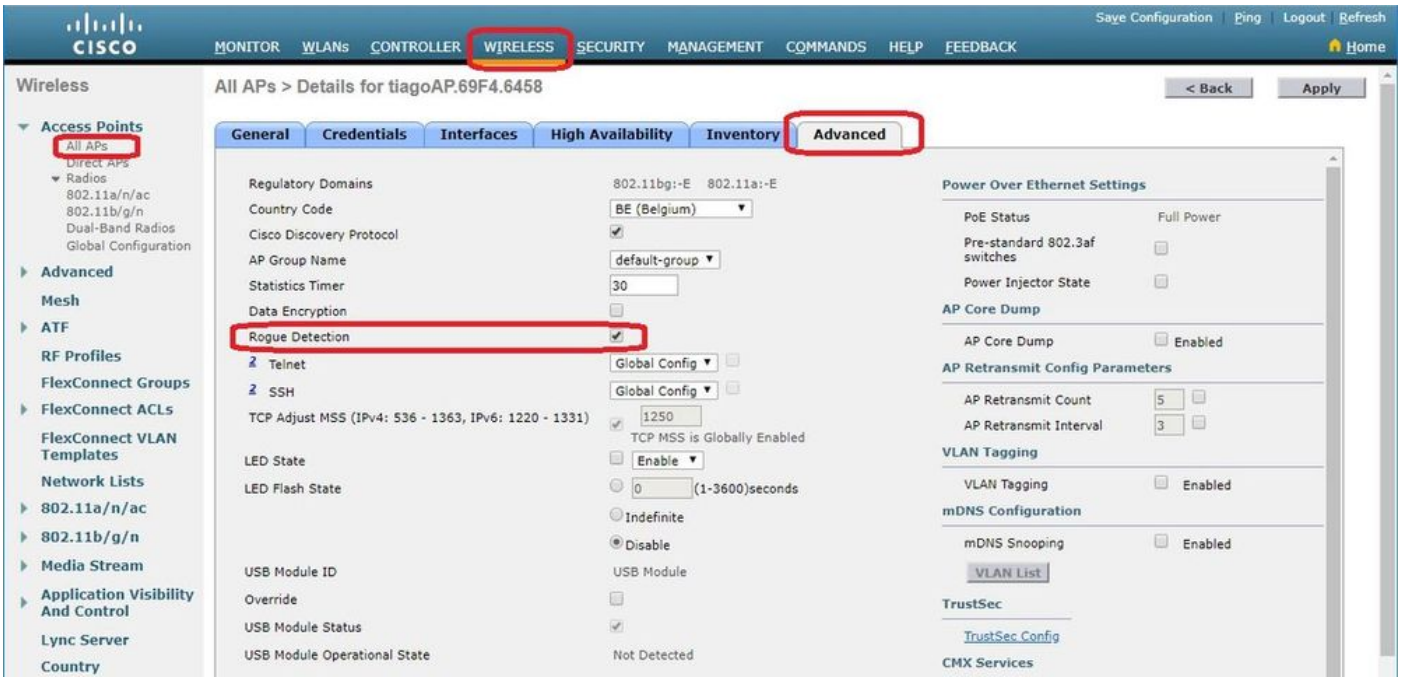
```
9c:97:26:61:d2:79 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -89    6
ac:22:05:ea:21:26 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -89    (1,5)
c4:e9:84:c1:c8:90 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -89    (6,2)
d4:28:d5:da:e0:d4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

문제 해결

비인가 탐지되지 않은 경우

AP에서 비인가 탐지가 활성화되었는지 확인합니다. GUI에서:



CLI에서:

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

비인가 탐지는 다음 명령을 사용하여 AP에서 활성화할 수 있습니다.

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

로컬 모드 AP는 국가 채널/DCA 채널만 스캔하며 컨피그레이션에 따라 다릅니다. 비인가 채널이 다른 채널에 있는 경우 네트워크에 모니터 모드 AP가 없는 경우 컨트롤러가 비인가를 식별할 수 없습니다. 다음을 확인하려면 이 명령을 실행합니다.

```
(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
```

- 비인가 AP는 SSID를 브로드캐스트하지 않습니다.
- 비인가 AP의 MAC 주소가 친숙한 비인가 목록에 추가되거나 PI를 통해 나열되지 않는지 확인합니다.
- 비인가 AP의 비콘은 비인가를 탐지한 AP에 연결할 수 없습니다. 이는 AP 탐지기 로그와 가까운 스니퍼로 패킷을 캡처하여 확인할 수 있습니다.

- 로컬 모드 AP는 비인가(3 cycle 180x3)를 탐지하는 데 최대 9분이 걸릴 수 있습니다.
- Cisco AP는 공용 안전 채널(4.9Ghz)과 같은 주파수에서 비인가를 감지할 수 없습니다.
- Cisco AP는 FHSS(Frequency Hopping Spread Spectrum)에서 작동하는 비인가를 감지할 수 없습니다.

유용한 디버그

```
(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
```

예상 트랩 로그

비인가 목록이 탐지/제거되면

0	2019년 6월 5일 수요일 09:01:57	비인가 클라이언트: b4:c0:f5:2b:4f:90이 1 AP의 비인가 클라이언트 Bssid에 의해 **탐지됨**: a6:b1:e9:f0:e8:41, 상태: 알림, 마지막으로 탐지한 AP:00:27:e3:36:4d:a0 비인가 클라이언 이트웨이 mac 00:00:00:02:02:02입니다.
1	6월 5일 수요일 09:00:39 2019	비인가 AP: 9c:97:26:61:d2:79 기본 무선 MAC에서 **제거되었습니다.** 00:27:e3:36:4d:a0 인 이스 번호:0(802.11n(2.4GHz))
2	2019년 6월 5일 수요일 08:53:39	비인가 AP: 7c:b7:33:c0:51:14 기본 무선 MAC에서 **제거되었습니다**. 00:27:e3:36:4d:a0 인 이스 번호:0(802.11n(2.4GHz))
3	2019년 6월 5일 수요일 08:52:27	비인가 클라이언트: fc:3f:7c:5f:b1:1b는 1 AP의 비인가 클라이언트 Bssid에 의해 **탐지됩니** 50:2f:a8:a2:0a:60, 상태: 알림, 마지막 탐지 AP:00:27:e3:36:4d:a0 비인가 클라이언트 게이 이 mac 00:26:44:73:c5:1d.
4	2019년 6월 5일 수요일 08:52:17	비인가 AP: d4:28:d5:da:e0:d4**가** 기본 무선 MAC에서 제거되었습니다. 00:27:e3:36:4d:a0 페이스 번호:0(802.11n(2.4GHz))

권장 사항

1. 네트워크에서 잠재적 비인가 의심될 경우 모든 채널에 대한 채널 검사를 구성합니다.
2. 비인가 탐지기 AP의 수와 위치는 층당 1개에서 건물당 1개로 다양할 수 있으며 유선 네트워크의 레이아웃에 따라 달라집니다. 건물의 각 층에는 비인가 탐지기 AP가 하나 이상 있는 것이 좋습니다. 비인가 탐지기 AP는 모니터링할 모든 레이어 2 네트워크 브로드캐스트 도메인에 대한 트렁크를 필요로 하므로, 위치는 네트워크의 논리적 레이아웃에 따라 달라집니다.

Rogue가 분류되지 않은 경우

비인가 규칙이 올바르게 구성되었는지 확인합니다.

유용한 디버그

```
(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
```

권장 사항

알려진 비인가 항목이 있는 경우 목록을 추가하거나 AAA와의 검증을 활성화하고 알려진 클라이언트 항목이 AAA(Authentication, Authorization and Accounting) 데이터베이스에 있는지 확인합니다.

RLDP에서 비인가 검색 안 함

- 비거가 DFS 채널에 있으면 RLDP가 작동하지 않습니다.
- RLDP는 비인가 WLAN이 열려 있고 DHCP를 사용할 수 있는 경우에만 작동합니다.
- 로컬 모드 AP가 DFS 채널에서 클라이언트를 서비스하는 경우 RLDP 프로세스에 참여하지 않습니다.
- RLDP는 AP 모델 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800 및 3800 Series AP에서 지원되지 않습니다.

유용한 디버그

```
(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
```

권장 사항

1. 의심스러운 비인가 항목에서 수동으로 RLDP를 시작합니다.
2. 정기적으로 RLDP를 예약합니다.
3. RLDP는 로컬 또는 모니터 모드 AP에 구축할 수 있습니다. 대부분의 확장 가능한 구축에서 클라이언트 서비스에 대한 영향을 없애기 위해 가능한 경우 RLDP를 모니터 모드 AP에 구축해야 합니다. 그러나 이 권장 사항에서는 5개의 로컬 모드 AP마다 모니터 모드 AP 오버레이를 1개의 모니터 모드 AP로 일반적인 비율로 구축해야 합니다. 적응형 wIPS 모니터 모드의 AP도 이 작업에 활용할 수 있습니다.

비인가 탐지기 AP

비인가 탐지기의 비인가 항목은 AP 콘솔에서 이 명령을 통해 확인할 수 있습니다. 유선 비인가의 경우 플래그가 설정 상태로 이동합니다.

```
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
```

AP 콘솔의 유용한 디버그 명령

```
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
```

비인가 억제

예상 디버그

```
*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
```

권장 사항

1. 로컬/Flex-Connect 모드 AP는 라디오당 한 번에 3개의 디바이스를 포함할 수 있으며, 모니터 모드 AP는 라디오당 6개의 디바이스를 포함할 수 있습니다. 따라서 AP에 허용된 최대 디바이스 수가 포함되어 있지 않은지 확인합니다. 이 시나리오에서 클라이언트는 포함 보류 상태입니다.
2. 자동 억제 규칙을 확인합니다.

결론

Cisco 중앙 집중식 컨트롤러 솔루션 내에서 비인가 탐지 및 억제는 업계에서 가장 효과적이고 덜 간섭하는 방법입니다. 네트워크 관리자에게 제공되는 유연성을 통해 모든 네트워크 요구 사항을 충족할 수 있는 보다 맞춤화된 환경을 구축할 수 있습니다.

관련 정보

- Cisco Wireless Controller 컨피그레이션 가이드, 릴리스 8.8 - 비인가 관리
- Cisco WLC(Wireless LAN Controller) 컨피그레이션 모범 사례
- WLC 3504 릴리스 8.5 배포 가이드
- Cisco 5520 Wireless LAN Controller 구축 설명서
- Cisco Wireless Controllers 및 Lightweight Access Points, Cisco Wireless Release 8.8.120.0 릴리스 정보

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.