적응형 wIPS ELM 구성 및 구축 설명서

목차

소개

Cisco wIPS(Adaptive Wireless Intrusion Prevention System) 솔루션은 ELM(Enhanced Local Mode) 기능을 추가하여 관리자가 별도의 오버레이 네트워크 없이 구축된 액세스 포인트(AP)를 사용하여 포괄적인 보호를 제공할 수 있도록 합니다(그림 1). ELM과 기존의 적응형 wIPS 구축 환경에서는 PCI 규정 준수 요구 사항을 제공하거나 무단 보안 액세스, 침투 및 공격으로부터 보호하기 위해 전용 모니터 모드(MM) AP가 필요합니다(그림 2). ELM은 CapEx 및 OpEx 비용을 절감하면서 무선 보안 구현을 용이하게 하는 비교 가능한 솔루션을 효과적으로 제공합니다. 이 문서에서는 ELM에만 중점을 두며 MM AP를 통해 기존 wIPS 구축 이점을 수정하지 않습니다.

그림 1 - 향상된 로컬 모드 AP 구축

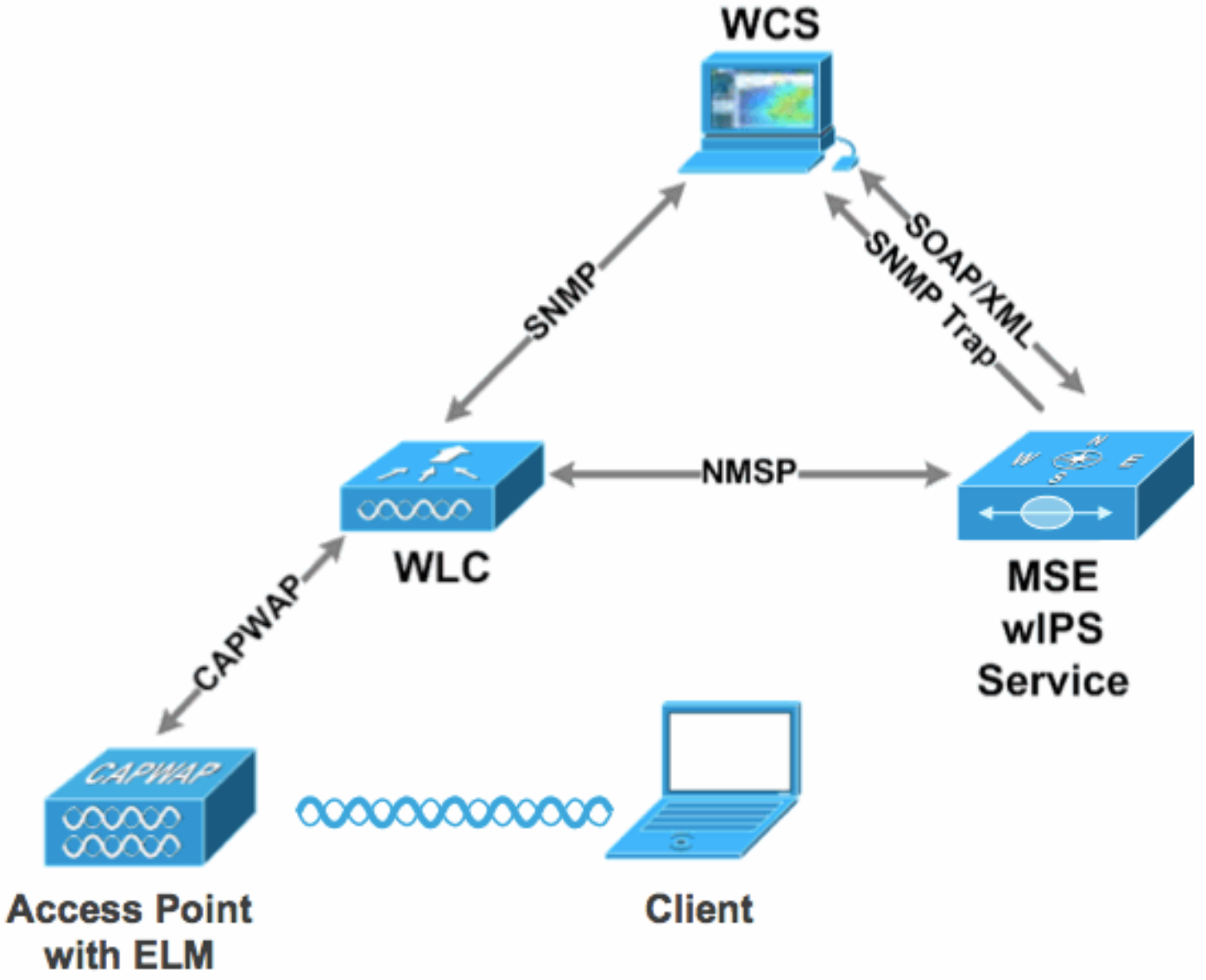
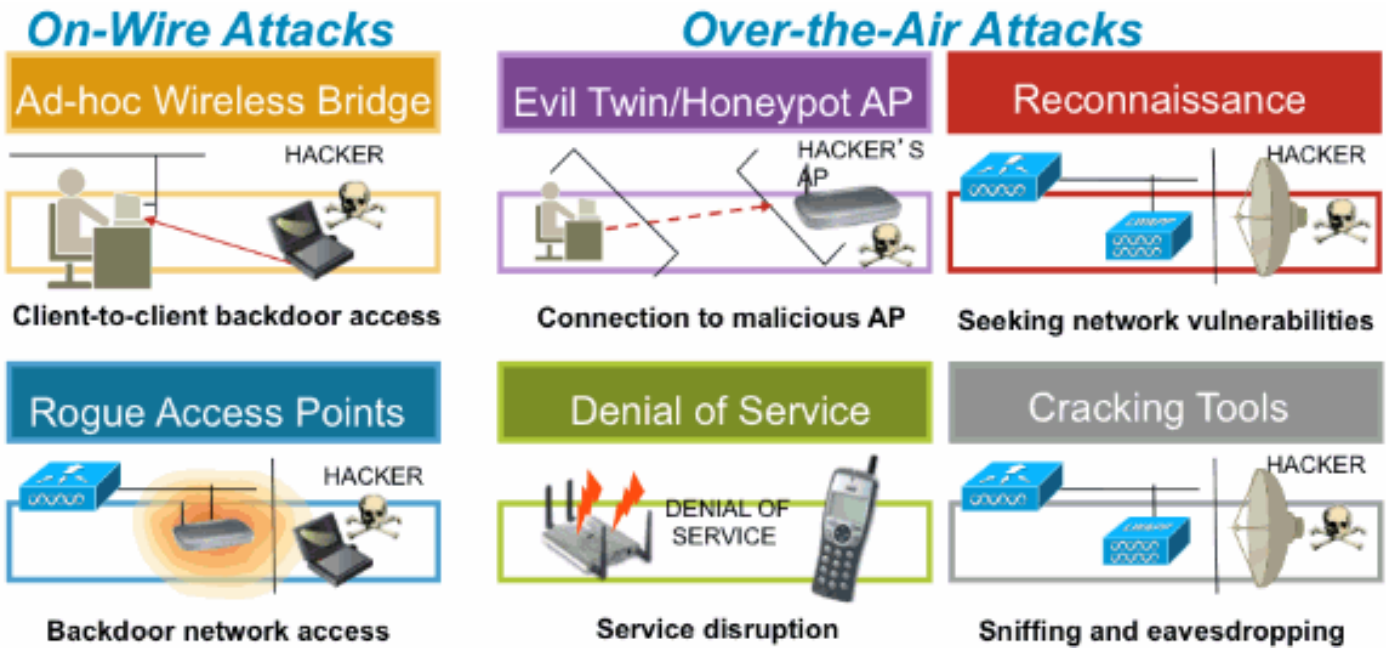


그림 2 - 주요 무선 보안 위협



사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

ELM 필수 구성 요소 및 최소 코드 버전

- WLC(Wireless LAN Controller) - 버전 7.0.116.xx 이상
- AP - 버전 7.0.116.xx 이상
- WCS(Wireless Control System) - 버전 7.0.172.xx 이상
- Mobility Services Engine - 버전 7.0.201.xx 이상

WLC 플랫폼 지원

ELM은 WLC5508, WLC4400, WLC 2106, WLC2504, WiSM-1 및 WiSM-2WLC 플랫폼에서 지원됩니다.

지원 AP

ELM은 3500, 1250, 1260, 1040 및 1140을 포함하는 11n AP에서 지원됩니다.

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

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

ELM wIPS 경보 흐름

공격은 신뢰할 수 있는 인프라 AP에서 발생한 경우에만 관련이 있습니다. ELM AP는 컨트롤러를 탐지하고 컨트롤러와 통신하며 WCS 관리와의 보고를 위해 MSE와의 상관관계를 분석합니다. 그림 3은 관리자의 관점에서 경보 흐름을 보여줍니다.

1. 인프라 디바이스("신뢰할 수 있는" AP)에 대해 시작된 공격
2. CAPWAP를 통해 WLC로 통신되는 ELM AP에서 탐지됨
3. NMSP를 통해 MSE에 투명하게 전달됨
4. SNMP 트랩을 통해 WCS로 전송된 MSE에서 wIPS 데이터베이스에 로그인됨

5. WCS에 표시됨

그림 3 - 위협 감지 및 경보 흐름

ELM의 구축 고려 사항

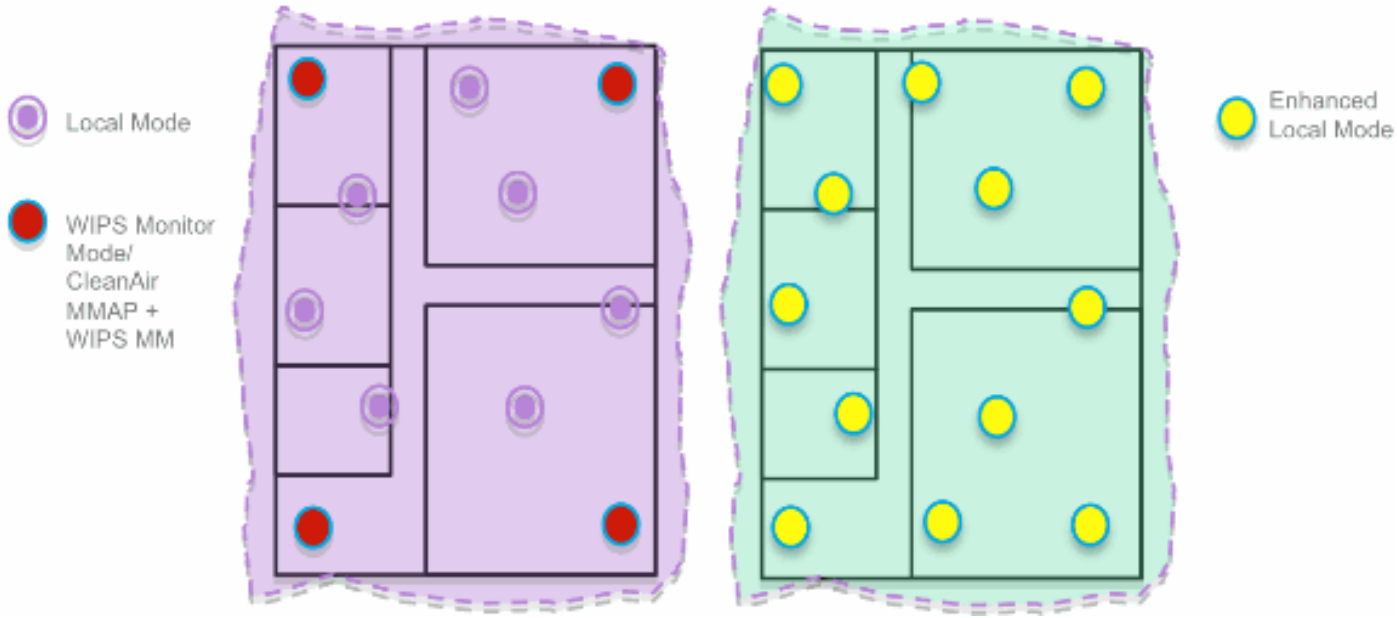
Cisco에서는 네트워크 오버레이 및/또는 비용을 고려할 때 네트워크의 모든 AP에서 ELM을 활성화하여 대부분의 고객 보안 요구 사항을 충족할 것을 권장합니다. ELM의 기본 기능은 데이터, 음성 및 비디오 클라이언트, 서비스의 성능을 저하시키지 않으면서 온채널 공격에 효과적으로 대응합니다.

ELM vs 전용 MM

그림 4는 wIPS MM AP와 ELM의 표준 구축 간의 일반적인 차이점을 보여줍니다. 검토에서 두 모드의 일반적인 적용 범위 범위는 다음을 제안합니다.

- 전용 wIPS MM AP는 일반적으로 15,000~35,000평방피트에 해당
- 클라이언트 서비스 AP는 일반적으로 3,000~5,000제곱피트에 해당됩니다.

그림 4 - MM AP와 모든 ELM AP 오버레이



기존의 적응형 wIPS 구축에서는 5개의 로컬 모드 AP마다 1MM AP의 비율을 사용하는 것이 좋습니다. 이는 최상의 커버리지를 위해 네트워크 설계 및 전문가의 안내에 따라 달라질 수 있습니다. 관리자는 ELM을 고려하여 기존 모든 AP에 대해 ELM 소프트웨어 기능을 활성화하기만 하면 성능을 유지하면서 로컬 데이터 서비스 모드 AP에 MM wIPS 작업을 효과적으로 추가할 수 있습니다.

온채널 및 오프채널 성능

MM AP는 WLAN 클라이언트에 서비스를 제공하지 않으므로 모든 채널을 스캔하는 데 라디오 시간의 100%를 사용합니다. ELM의 주요 기능은 데이터, 음성 및 비디오 클라이언트 및 서비스의 성능을 저하시키지 않으면서 온채널 공격에 효과적으로 대응합니다. 가장 큰 차이점은 로컬 모드에서 오프 채널 스캐닝을 달리한다는 것입니다. 오프 채널 스캐닝은 활동에 따라 공격을 분류하고 결정할 수 있는 충분한 정보를 수집하는 데 필요한 최소한의 체류 시간을 제공합니다. 예를 들어, 연결된 음성 클라이언트와 AP의 RRM 검사가 지연되어 음성 클라이언트가 연결되어 서비스가 영향을 받지 않도록 할 수 있습니다. 이러한 점을 고려할 때, 오프 채널 동안의 ELM 탐지는 최선의 노력으로 간주된다. 모든, 국가 또는 DCA 채널에서 작동하는 인접 ELM AP는 효과가 향상되므로 모든 로컬 모드 AP에서 ELM을 활성화하여 보호 범위를 극대화하는 것이 좋습니다. 모든 채널에서 전시간 전용 검사를 수행해야 하는 경우 MM AP를 구축하는 것이 좋습니다.

다음 사항에서는 로컬 모드 및 MM AP의 차이점을 검토합니다.

- Local Mode AP(로컬 모드 AP) - WLAN 클라이언트에 시간 슬라이싱 오프 채널 검사를 제공하고, 각 채널에서 50ms를 수신 대기하며, 모든/국가/DCA 채널에 대해 구성 가능한 검사를 지원합니다.
- Monitor Mode AP(모니터 모드 AP) - WLAN 클라이언트를 지원하지 않으며 검사 전용이며 각 채널에서 1.2를 수신 대기하고 모든 채널을 검사합니다.

WAN 링크를 통한 ELM

Cisco는 저대역폭 WAN 링크에 ELM AP를 구축하는 등 까다로운 시나리오에서 기능을 최적화하기 위해 많은 노력을 기울였습니다. ELM 기능은 AP에서 공격 시그니처를 확인하는 전처리 과정을 포함하며 느린 링크에서 작동하도록 최적화되었습니다. 모범 사례로서, WAN을 통한 ELM으로 성능을 검증하기 위해 기준을 테스트하고 측정하는 것이 좋습니다.

CleanAir 통합

ELM 기능은 다음과 같은 기존 CleanAir 스펙트럼 인식 이점을 통해 MM AP 구축과 유사한 성능 및 이점으로 CleanAir 운영을 크게 보완합니다.

- 전용 실리콘 레벨 RF 인텔리전스
- 스펙트럼 인식, 자동 복구, 자동 최적화
- 비표준 채널 위협 및 간섭 탐지 및 완화
- Bluetooth, 전자 레인지, 무선 전화기 등과 같은 비 Wi-Fi 감지 기능

- RF 방해 장치와 같은 RF 레이어 DOS 공격 탐지 및 위치 파악

ELM의 기능 및 이점

- 로컬 및 H-REAP AP를 서비스하는 데이터에서 적응형 wIPS 스캐닝
- 별도의 오버레이 네트워크 없이도 보호
- 기존 wIPS 고객에게 무료 SW 다운로드로 제공
- 무선 LAN에 대한 PCI 규정 준수 지원
- 전체 802.11 및 비 802.11 공격 탐지
- 포렌식 및 보고 기능 추가
- 기존 CUWM 및 WLAN 관리와 통합
- 통합 또는 전용 MM AP를 설정할 수 있는 유연성
- AP에서의 전처리는 데이터 백홀을 최소화합니다(즉, 매우 낮은 대역폭 링크에서 작동).
- 서비스 데이터에 대한 영향 감소

ELM 라이센싱

ELM wIPS는 주문에 새로운 라이센스를 추가합니다.

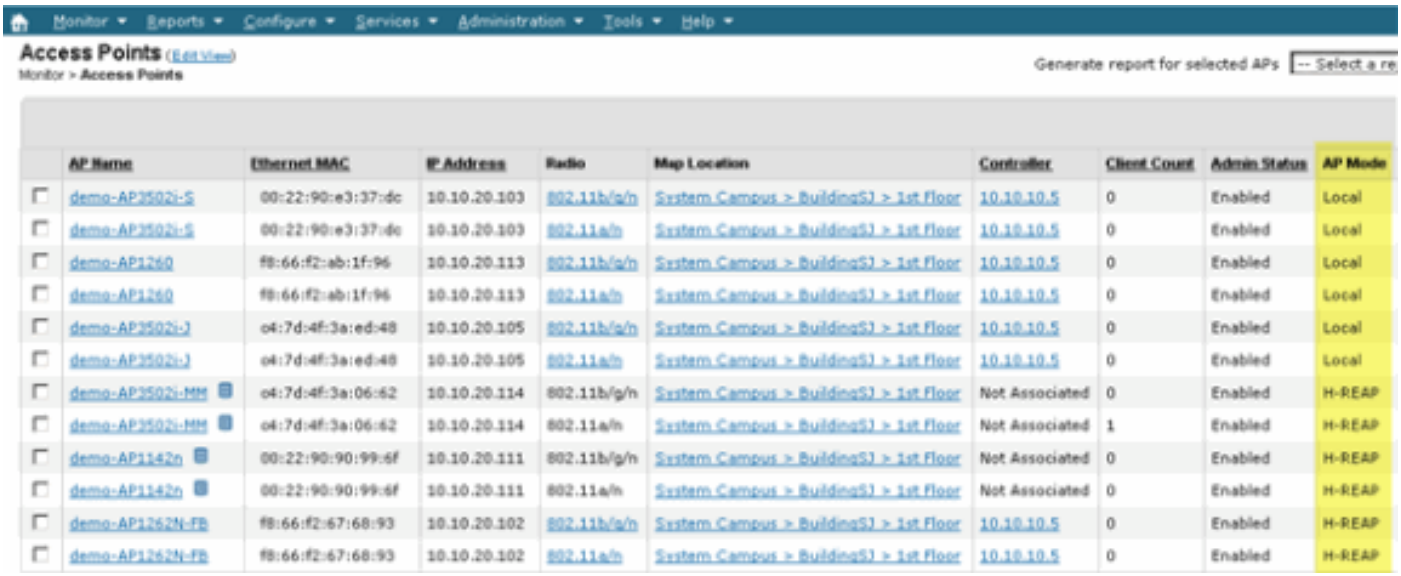
- AIR-LM-WIPS-xx - Cisco ELM wIPS 라이센스
- AIR-WIPS-AP-xx - Cisco Wireless wIPS 라이센스

추가 ELM 라이센스 참고 사항:

- wIPS MM AP 라이센스 SKU가 이미 설치되어 있는 경우, 해당 라이센스를 ELM AP에도 사용할 수 있습니다.
- wIPS 라이센스 및 ELM 라이센스는 모두 wIPS 엔진의 플랫폼 라이센스 한도에 포함됩니다(각각 3310의 경우 2000개 AP, 335x의 경우 3000개 AP).
- 평가판 라이센스에는 최대 60일 동안 wIPS용 AP 10개, ELM용 AP 10개가 포함됩니다. ELM 이전에는 평가판 라이센스로 최대 20wIPS MM AP를 사용할 수 있었습니다. ELM을 지원하는 소프트웨어 버전의 최소 요구 사항을 충족해야 합니다.

WCS로 ELM 구성

그림 5 - WCS를 사용하여 ELM 구성

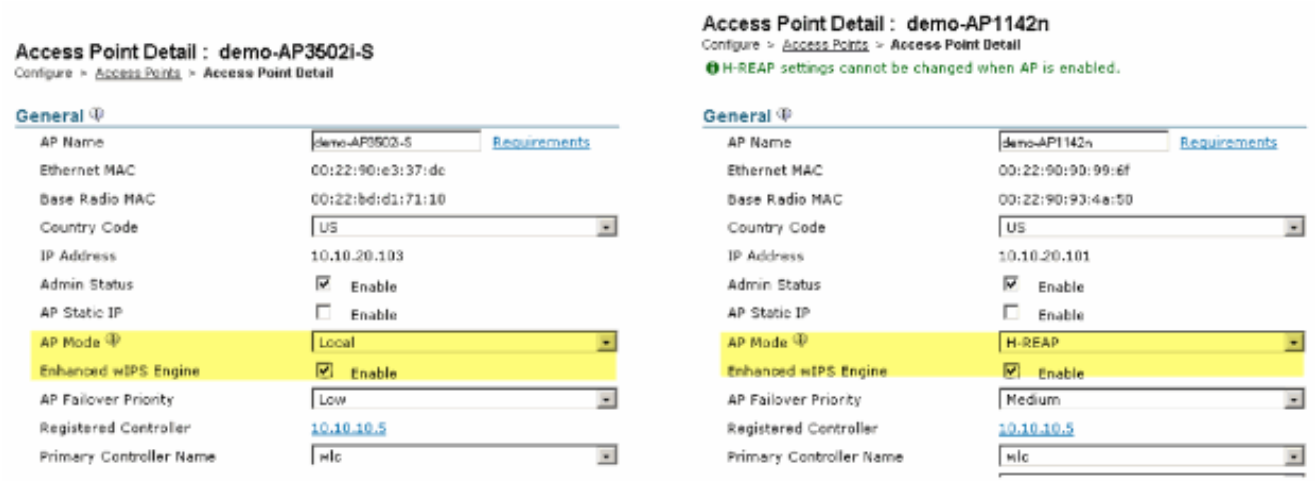


1. "Enhanced wIPS Engine"을 활성화하기 전에 WCS에서 AP의 802.11b/g 및 802.11a 무선 장치를 모두 비활성화합니다.

   참고: 연결된 모든 클라이언트는 연결이 끊기고, 무선 장치가 활성화될 때까지 가입하지 않습니다.

2. 하나의 AP를 구성하거나 여러 경량 AP에 대해 WCS 컨피그레이션 템플릿을 사용합니다. 그림 6을 참조하십시오.

   그림 6 - ELM(Enhanced wIPS Engine) 하위 모드 활성화



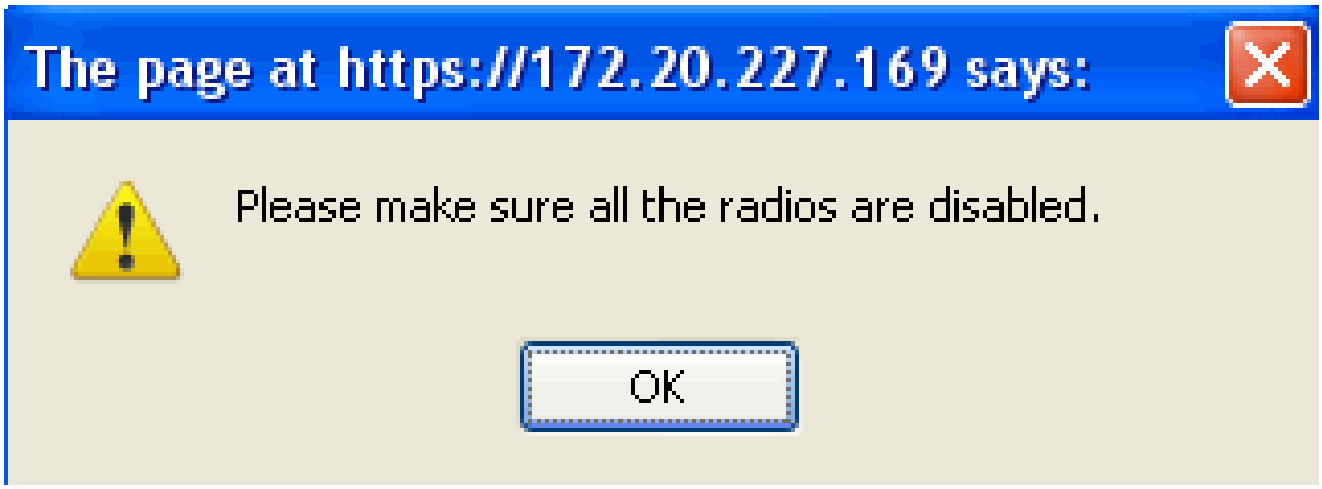
3. Enhanced wIPS Engine(고급 wIPS 엔진)을 선택하고 Save(저장)를 클릭합니다.

   a. 향상된 wIPS 엔진을 활성화해도 AP가 재부팅되지 않습니다.

   b. H-REAP가 지원됩니다. 로컬 모드 AP와 동일한 방식으로 활성화합니다.

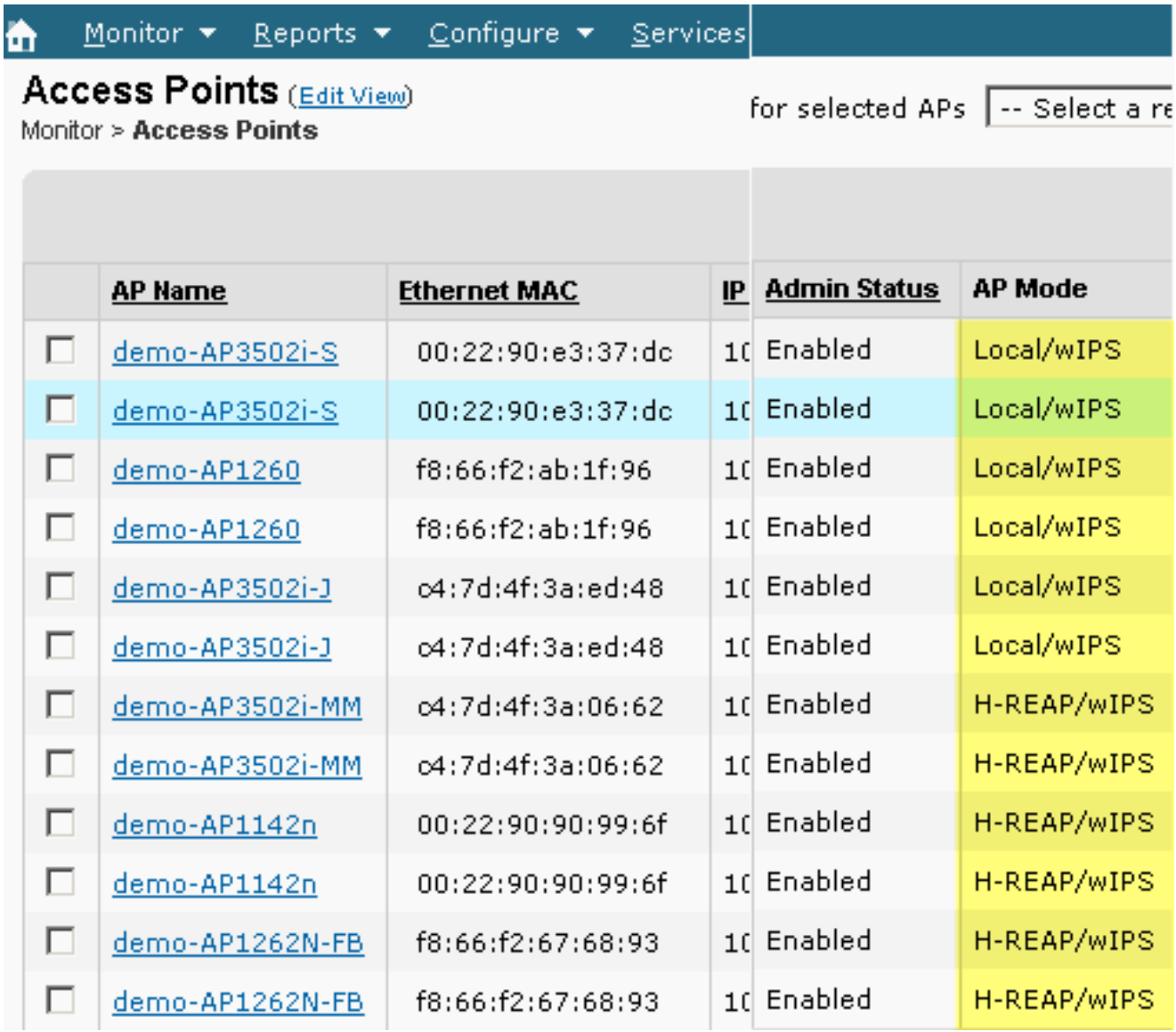
   참고: 이 AP의 무선 장치 중 하나가 활성화된 경우 WCS는 컨피그레이션을 무시하고 그림 7의 오류를 발생시킵니다.

   그림 7 - ELM을 활성화하기 전에 AP 무선 비활성화 WCS 알림



4. AP 모드가 "Local or H-REAP"에서 Local/wIPS 또는 H-REAP/wIPS로 변경되었는지 확인하여 컨피그레이션 성공을 확인할 수 있습니다. 그림 8을 참조하십시오.

그림 8 - 로컬 및/또는 H-REAP에 wIPS를 포함하도록 AP 모드를 표시하는 WCS



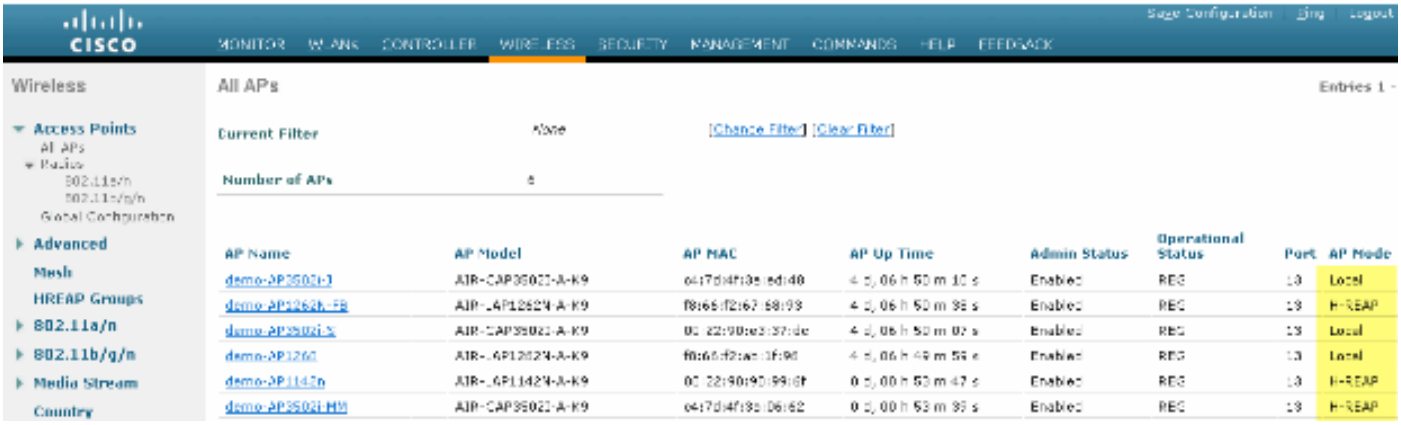
5. 1단계에서 비활성화된 무선 장치를 활성화합니다.

6. wIPS 프로파일을 생성한 다음 컨트롤러에 푸시하여 컨피그레이션을 완료합니다.

   참고: wIPS에 대한 전체 구성 정보는 Cisco Adaptive wIPS Deployment Guide를 참조하십시오.

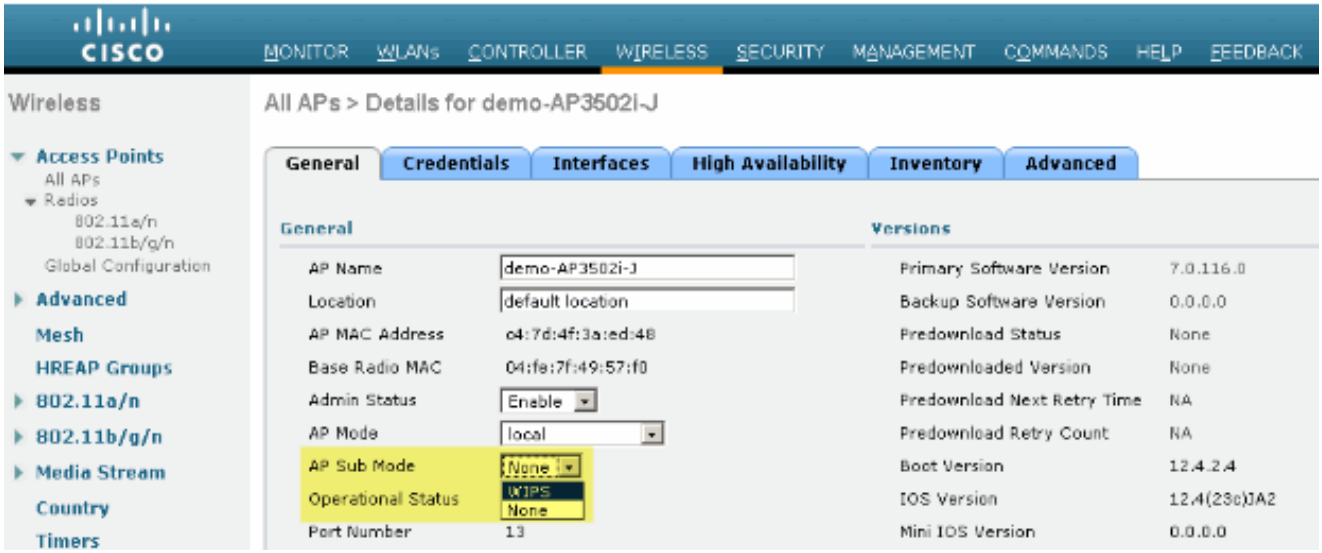
WLC에서 컨피그레이션

그림 9 - WLC로 ELM 구성



1. Wireless(무선) 탭에서 AP를 선택합니다.

   그림 10 - WLC에서 wIPS ELM을 포함하도록 AP 하위 모드 변경



2. AP Sub Mode(AP 하위 모드) 드롭다운 메뉴에서 wIPS(wIPS)를 선택합니다(그림 10).

3. 구성을 적용한 다음 저장합니다.

참고: ELM 기능이 작동하려면 wIPS 라이센싱과 함께 MSE 및 WCS가 필요합니다. WLC에서만 AP 하위 모드를 변경하면 ELM이 활성화되지 않습니다.

ELM에서 탐지된 공격

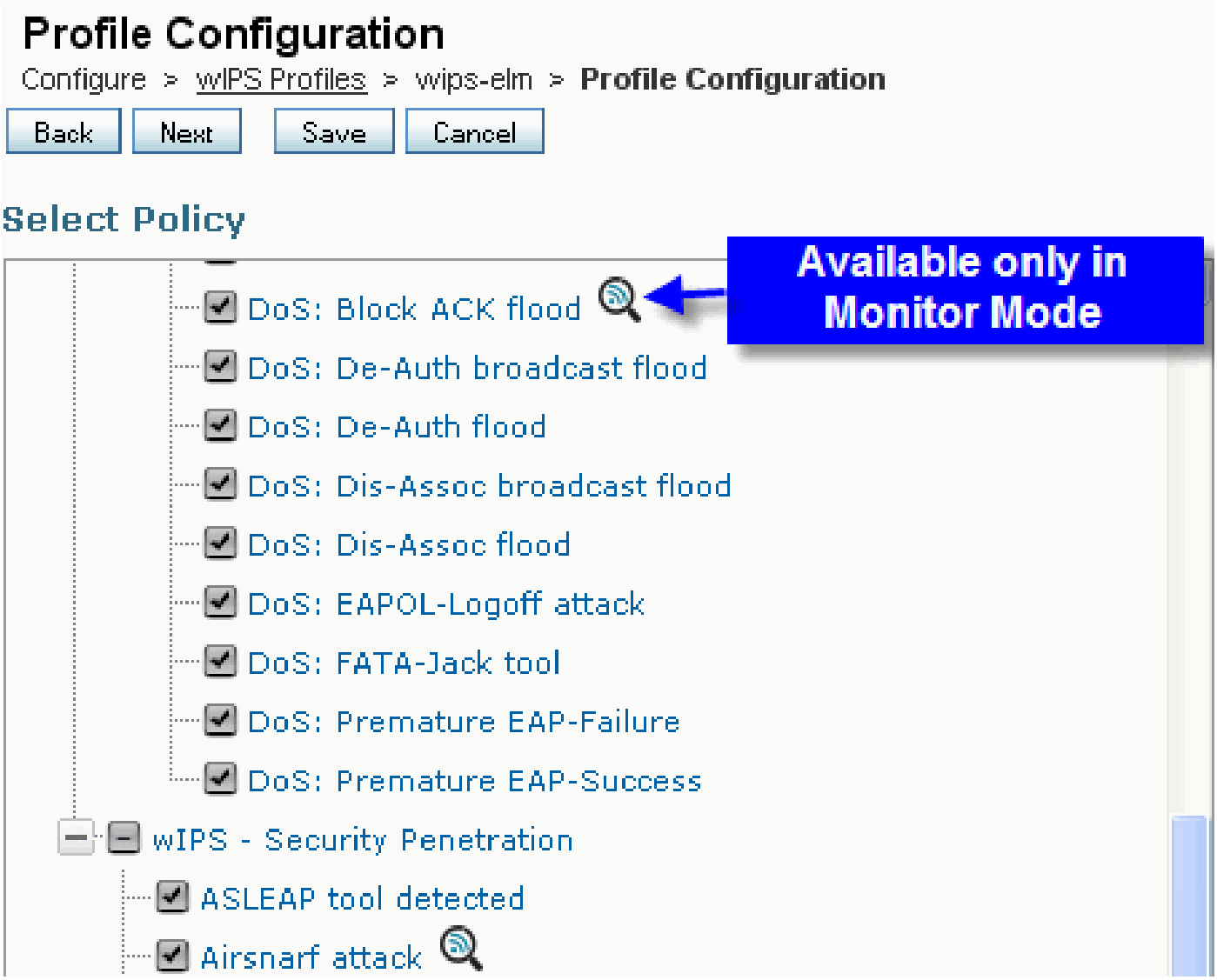
표 1 - wIPS 시그니처 지원 매트릭스

탐지된 공격	느릅나무	MM
AP에 대한 DoS 공격		
연결 플러드	Y	Y
연결 테이블 오버플로	Y	Y
인증 플러드	Y	Y
EAPOL-Start 공격	Y	Y
PS-Poll 플러드	Y	Y
프로브 요청 플러드	네트워킹	Y
인증되지 않은 연결	Y	Y
인프라에 대한 DoS 공격		
CTS 플러드	네트워킹	Y
퀸즐랜드 공과대학교 익스플로잇	네트워킹	Y
RF 재밍	Y	Y
RTS 플러드	네트워킹	Y
가상 캐리어 공격	네트워킹	Y
스테이션에 대한 DoS 공격		
인증 실패 공격	Y	Y
ACK 플러드 차단	네트워킹	Y
De-Auth 브로드캐스트 플러드	Y	Y
De-Auth 플러드	Y	Y
Disassoc 브로드캐스트 플러드	Y	Y
디스아스크 플러드	Y	Y
EAPOL-로그오프 공격	Y	Y
FATA-Jack 툴	Y	Y
조기 EAP 실패	Y	Y
조기 EAP-성공	Y	Y

보안 침투 공격		
ASLEAP 툴이 탐지됨	Y	Y
에어스나프 공격	네트워킹	Y
ChopChop 공격	Y	Y
WLAN 보안 이상 징후에 의한 제로 데이 공격	네트워킹	Y
디바이스 보안 이상 징후에 의한 Day-Zero 공격	네트워킹	Y
AP에 대한 디바이스 탐색	Y	Y
EAP 방법에 대한 사전 공격	Y	Y
802.1x 인증에 대한 EAP 공격	Y	Y
위조 AP 탐지	Y	Y
위조 DHCP 서버가 탐지됨	네트워킹	Y
빠른 WEP 크랙 도구가 검색되었습니다.	Y	Y
조각화 공격	Y	Y
허니팟 AP 탐지됨	Y	Y
핫스팟터 도구가 검색되었습니다.	네트워킹	Y
부적절한 브로드캐스트 프레임	네트워킹	Y
형식이 잘못된 802.11 패킷 탐지	Y	Y
중간자 공격	Y	Y
Netstumbler가 탐지됨	Y	Y
Netstumbler 피해자 발견	Y	Y
PSPF 위반이 탐지됨	Y	Y
소프트 AP 또는 호스트 AP가 탐지됨	Y	Y
스푸핑된 MAC 주소가 탐지됨	Y	Y
의심스러운 업무 시간 외 트래픽 탐지	Y	Y
벤더 목록별 무단 연결	네트워킹	Y
무단 연결이 감지되었습니다.	Y	Y
Wellenriter가 탐지됨	Y	Y

참고: CleanAir를 추가하면 비 802.11 공격도 탐지할 수 있습니다.

그림 11 - WCS wIPS 프로필 보기



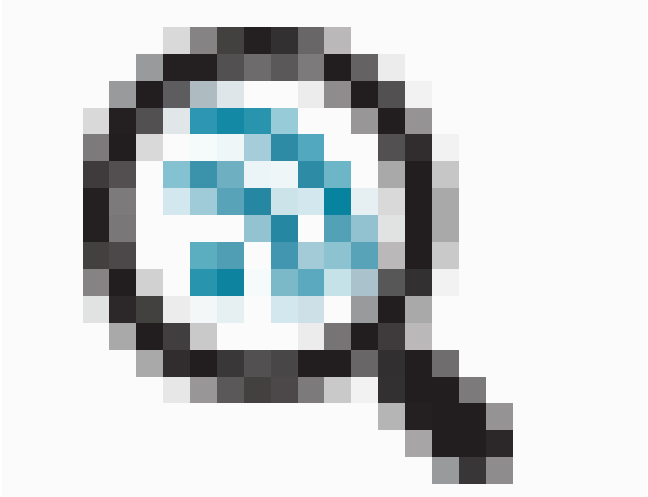


그림 11에서는 WCS에서 wIPS 프로파일을 구성하면 아이콘은 AP가 MM 단위인 경우에만 공격이 탐지됨을 나타내고 ELM인 경우에만 최선의 노력을 나타냅니다.

ELM 문제 해결

다음 항목을 확인합니다:

- NTP가 구성되었는지 확인합니다.
- MSE 시간 설정이 UTC인지 확인합니다.
- 디바이스 그룹이 작동하지 않을 경우 오버레이 프로파일 SSID를 Any와 함께 사용합니다. AP를 재부팅합니다.
- 라이센스가 구성되어 있는지 확인합니다(현재 ELM AP에서 KAM 라이센스를 사용 중).
- wIPS 프로필이 너무 자주 변경되면 MSE 컨트롤러를 다시 동기화합니다. WLC에서 프로파일이 활성화되어 있는지 확인합니다.
- WLC가 MSE CLI를 사용하는 MSE의 일부인지 확인합니다.

    1. MSE에 대한 SSH 또는 텔넷
    2. Execute /opt/mse/wips/bin/wips_cli - 이 콘솔을 사용하여 다음 명령에 액세스하여 적응형 wIPS 시스템의 상태에 대한 정보를 수집할 수 있습니다.
    3. show wlc all - wIPS 콘솔 내에서 문제가 발생합니다. 이 명령은 MSE의 wIPS 서비스와 능동적으로 통신하는 컨트롤러를 확인하는 데 사용됩니다. 그림 12를 참조하십시오.

    그림 12 - MSE wIPS 서비스를 통한 WLC 활성 확인 MSE CLI

```
<#root>

wIPS>

show wlc all


WLC MAC               Profile             Profile
Status                   IP
Onx Status Status
-----------------------------------------------
-----------------------------------------------
----
00:21:55:06:F2:80    WCS-Default         Policy
active on controller     172.20.226.197
Active
```

- MSE CLI를 사용하는 MSE에서 경보가 감지되는지 확인합니다.
    - show alarm list - wIPS 콘솔 내에서 문제가 발생합니다. 이 명령은 wIPS 서비스 데이터베이스에 현재 포함된 경보를 나열하는 데 사용됩니다. key 필드는 특정 알람에 할당된 고유한 해시 키입니다. Type 필드는 경보의 유형입니다. 그림 13의 이 차트는 경보 ID 및

설명 목록을 보여줍니다.

그림 13 - MSE CLI show alarm list 명령

<#root>

```
wIPS>

show alarm list

Key         Type  Src MAC
LastTime              Active          First Time
-----------------------------------------------
-----------------------------------------
89          89    00:00:00:00:00:00     2008/09/04
18:19:26  2008/09/07 02:16:58   1
65631       95    00:00:00:00:00:00     2008/09/04
17:18:31  2008/09/04 17:18:31   0
1989183     99    00:1A:1E:80:5C:40     2008/09/04
18:19:44  2008/09/04 18:19:44   0
```

First Time 및 Last Time 필드는 알람이 탐지된 타임스탬프를 나타내며 UTC 시간으로 저장됩니다. Active(활성) 필드는 경보가 현재 감지되는지 여부를 강조 표시합니다.

- MSE 데이터베이스 지우기
  - MSE 데이터베이스가 손상되었거나 다른 문제 해결 방법이 작동하지 않는 경우 데이터베이스를 지우고 다시 시작하는 것이 가장 좋습니다.

    그림 14 - MSE 서비스 명령

```
1. /etc/init.d/msed stop
2. Remove the database using the command 'rm
/opt/mse/locserver/db/linux/server-eng.db'
3. /etc/init.d/msed start
```

관련 정보

- Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 7.0.116.0
- Cisco Wireless Control System 컨피그레이션 가이드, 릴리스 7.0.172.0
- 기술 지원 및 문서 – Cisco Systems

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.