

# CMX 성능 최적화

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[오버로드된 CMX 노드의 신호](#)

[CMX 로드 재배포](#)

[로컬로 관리되는 MAC 주소 필터링](#)

[프로빙 클라이언트 추적](#)

[탐지 알고리즘 조정](#)

[VM 리소스 증가](#)

[CMX 그룹화\(이전의 AP 그룹화\)](#)

[추가 노드 구축](#)

[DNA 공간 - 클라우드로 작업 오프로드](#)

[관련 버그](#)

## 소개

이 문서에서는 추적 중인 많은 장치를 수용하기 위해 단일 CMX(Connected Mobile Experience) 노드의 로드를 인식하고 재배포하는 방법에 대해 설명합니다. 이와 같은 문제는 프로브 클라이언트 추적이 활성화된 공개 영역 또는 설정의 대규모 구축에서 자주 발생합니다.

## 사전 요구 사항

### 요구 사항

이 문서에서는 CMX의 기본 설정 및 컨피그레이션에 대한 지식을 보유하고 있으며 대규모 구축에서 성능을 최적화하기 위한 팁과 방법에만 초점을 두고 있습니다.

### 사용되는 구성 요소

이 문서에 표시된 모든 명령과 예는 3375 어플라이언스에서 실행되는 8.8.125 코드와 CMX 10.6.1을 실행하는 3504 WLC에서 수행되었습니다.

## 오버로드된 CMX 노드의 신호

CMX 노드의 오버로드로 인해 여러 가지 문제가 발생할 수 있습니다.

- 서비스를 시작할 수 없음
- 서비스가 갑자기 중단/중단됨
- 0개의 활성 클라이언트를 보여주는 분석 서비스

- 분석 또는 위치 서비스가 심각한 상태임을 알리는 경보 및 이메일 알림
- 기본 CMX 노드와 보조 CMX 노드 간에 HA 설정 불가

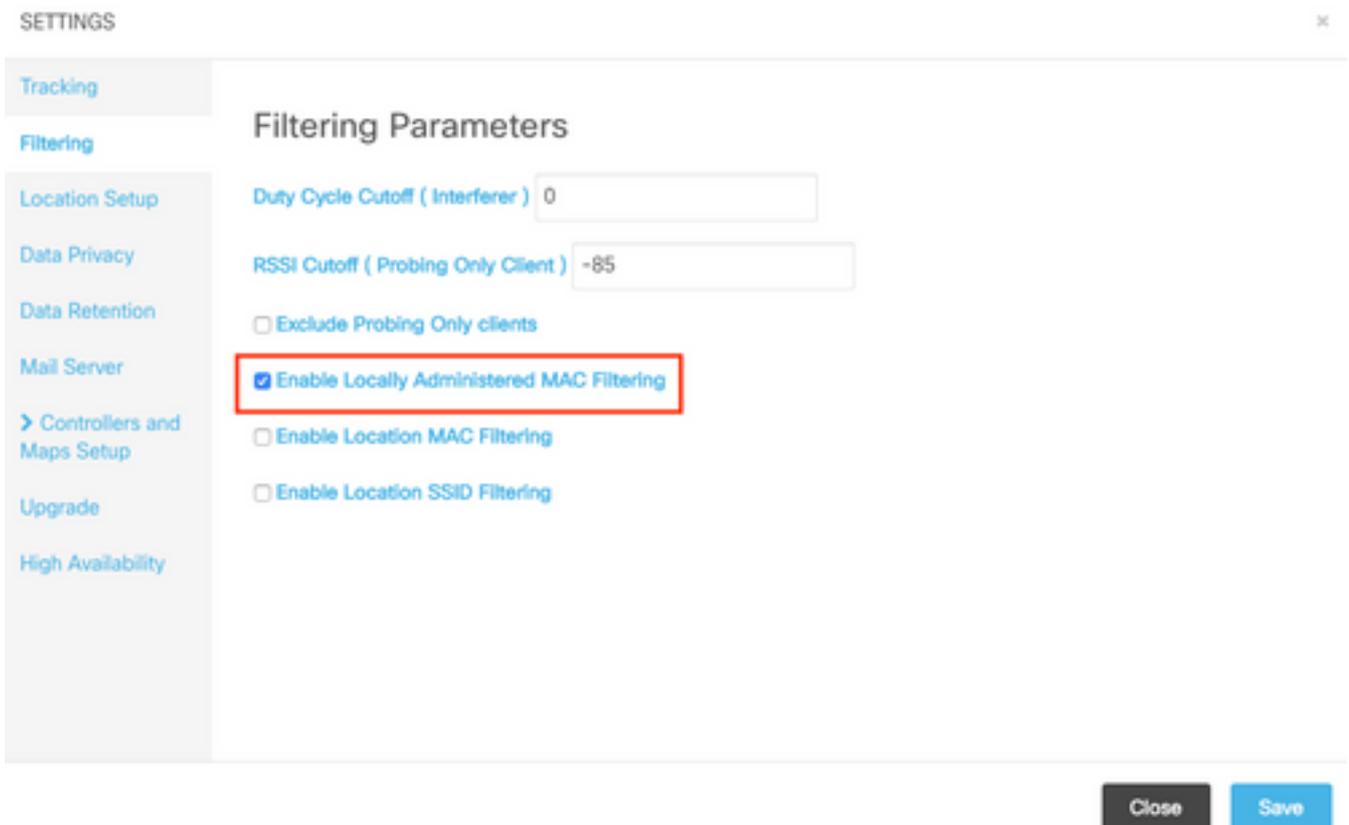
## CMX 로드 재배포

### 로컬로 관리되는 MAC 주소 필터링

2014년 IOS 8 릴리스부터 증가하는 개인정보 문제로 인해 스마트폰 제조업체는 프로브 요청을 전송할 때마다 디바이스에서 무작위로 생성된 새 MAC 주소를 사용하는 MAC 임의 설정이라는 기능을 구현하기 시작했습니다. 임의의 MAC 주소를 생성할 때 제조업체는 주소가 무작위임을 나타내는 특수 비트가 있는 "로컬에서 관리" MAC 주소를 사용하거나 실제 주소와 구별되지 않는 완전히 무작위 주소를 생성하도록 결정할 수 있습니다. 프로브 시 실제 MAC 주소를 사용하는 클라이언트의 수가 매우 적습니다.

CMX는 이러한 위조 랜덤 MAC 주소를 필터링할 수 있는 방법을 가지고 있습니다. System(시스템)->Settings(설정)->Filtering(필터링)에서 항상 "Enable Locally Administered MAC filtering(로컬로 관리되는 MAC 필터링 활성화)"이 선택되어 있는지 확인합니다.

**참고:** 이 필드는 CMX 10.6.0의 웹 인터페이스에서 제거되었으며 기본적으로 항상 활성화되어 있습니다.



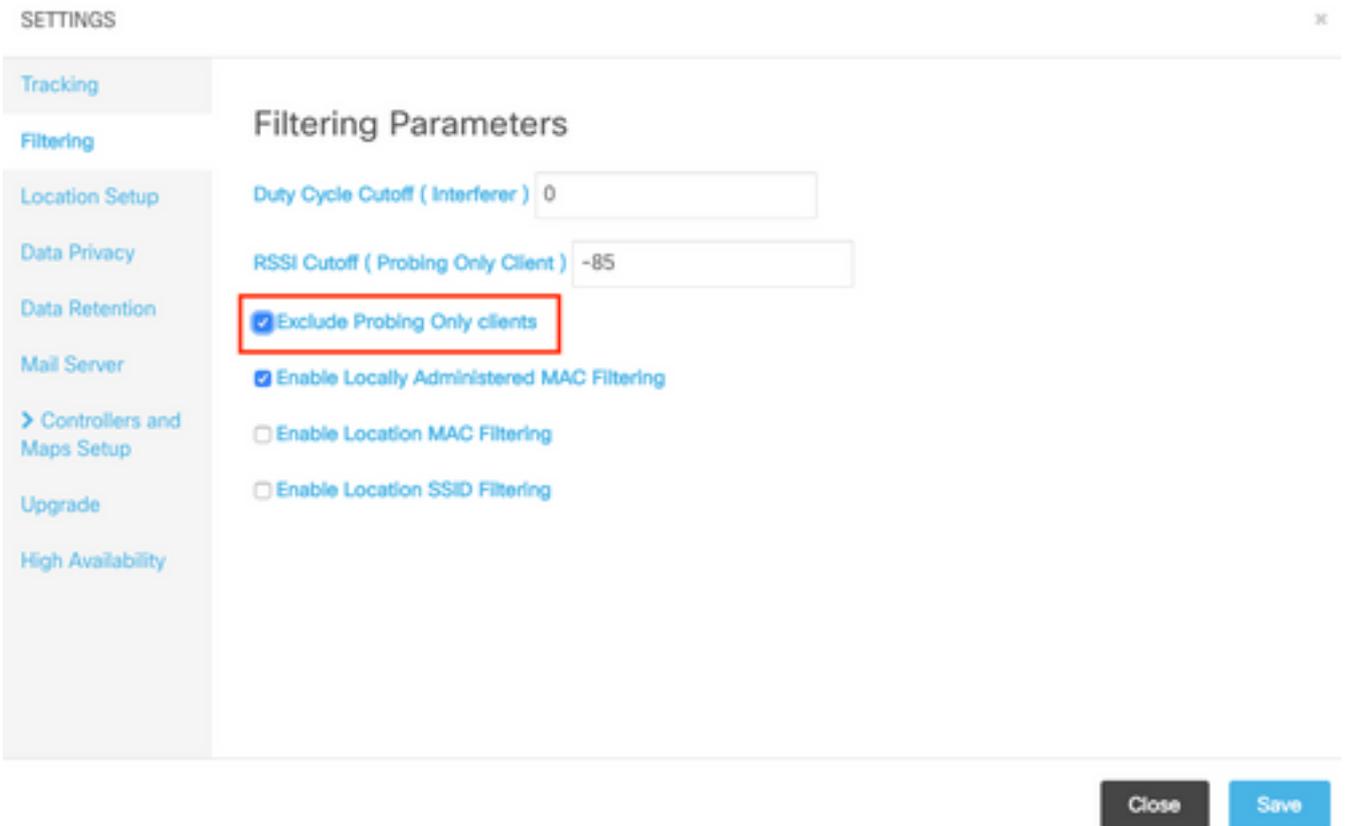
### 프로빙 클라이언트 추적

Cisco TAC에서 처리하는 CMX 오버로드의 가장 일반적인 근본 원인은 프로브 전용 클라이언트를 추적하는 것입니다. 이 기능을 활성화하면 연결되지 않은 클라이언트의 위치 추적이 가능합니다. 쇼핑몰이나 기차역 같은 공공장소에는 방문자가 매우 많으며 하이엔드 CMX 노드에서도 그 한계를 매우 능가하는 경우가 많습니다.

프로빙 클라이언트를 추적하는 설정에서 무작위로 생성된 MAC 주소도 클라이언트 수에 매우 큰 영향을 미칩니다.

Apple과 같은 일부 제조업체는 프로브 시 표준을 따르고 로컬에서 관리되는 임의의 MAC 주소를 사용하고 있습니다. 즉, iPhone 장치는 CMX에서 프로브 및 연결 해제 시 탐지되지 않습니다. 표준을 따르지 않고 로컬에서 관리되지 않는 임의의 MAC 주소를 사용하는 디바이스는 프로브 요청을 보낼 때마다 CMX에서 새 클라이언트로 기록됩니다(몇 초마다 발생할 수 있음). 그 결과 프로빙 클라이언트 수는 네트워크에 있는 실제 디바이스 수보다 훨씬 높거나 낮을 수 있습니다.

System(시스템)->Settings(설정)->Filtering(필터링) 아래의 CMX 웹 인터페이스에서 "Exclude Probing Only Clients(프로브만 클라이언트 제외)" 옵션을 선택하여 프로빙 클라이언트 추적을 비활성화할 수 있습니다.



위에서 언급한 모든 변동으로 인해 프로빙 클라이언트 수를 풋폴 카운터로 사용할 수 없으며 Cisco TAC에서는 프로빙 클라이언트 추적에 대해 강력히 권장합니다.

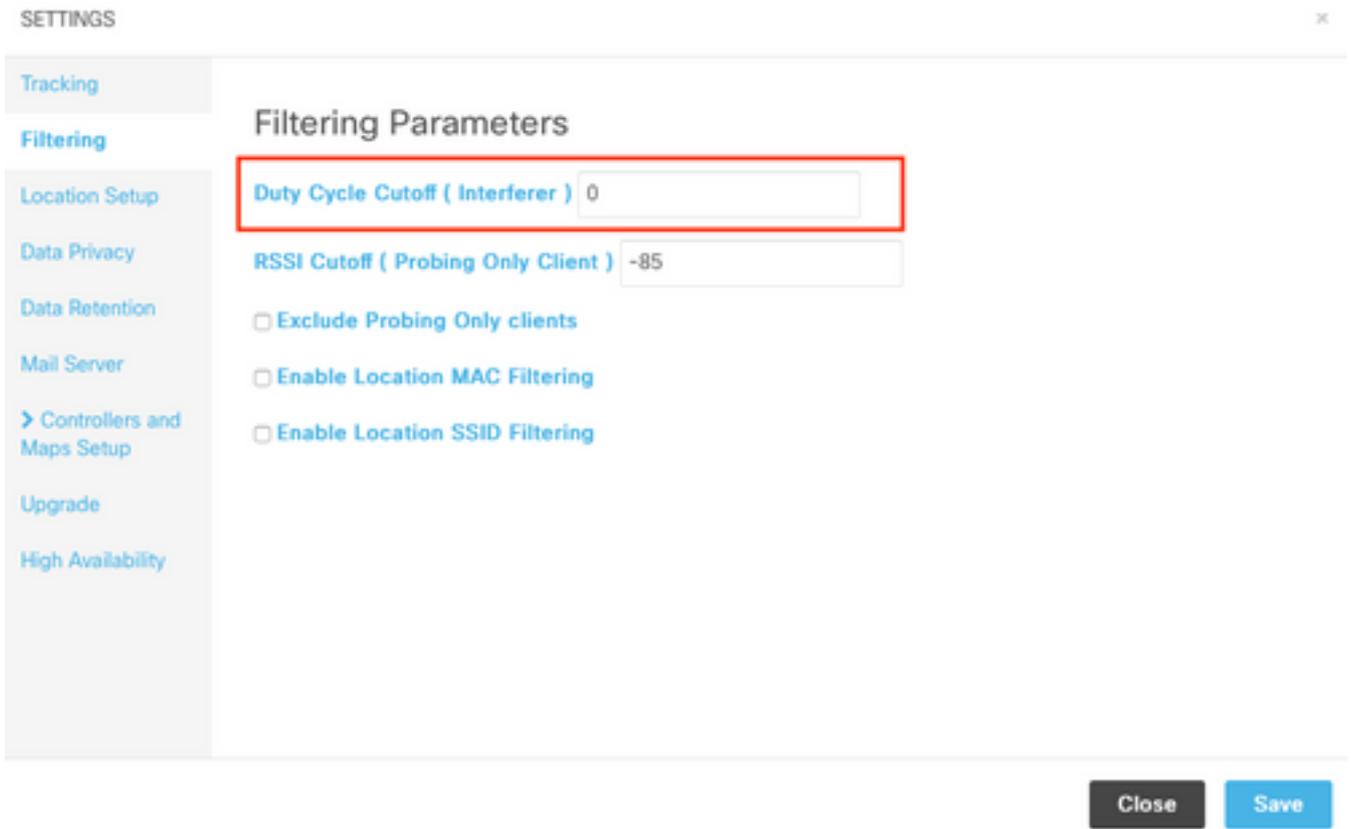
## 탐지 알고리즘 조정

CMX에서 필터링 옵션을 조정하면 녹화하는 프로빙 클라이언트 수가 크게 제한됩니다. 클라이언트 탐지에 크게 영향을 미치는 두 가지 주요 옵션(특히 프로브만 해당)이 있습니다.

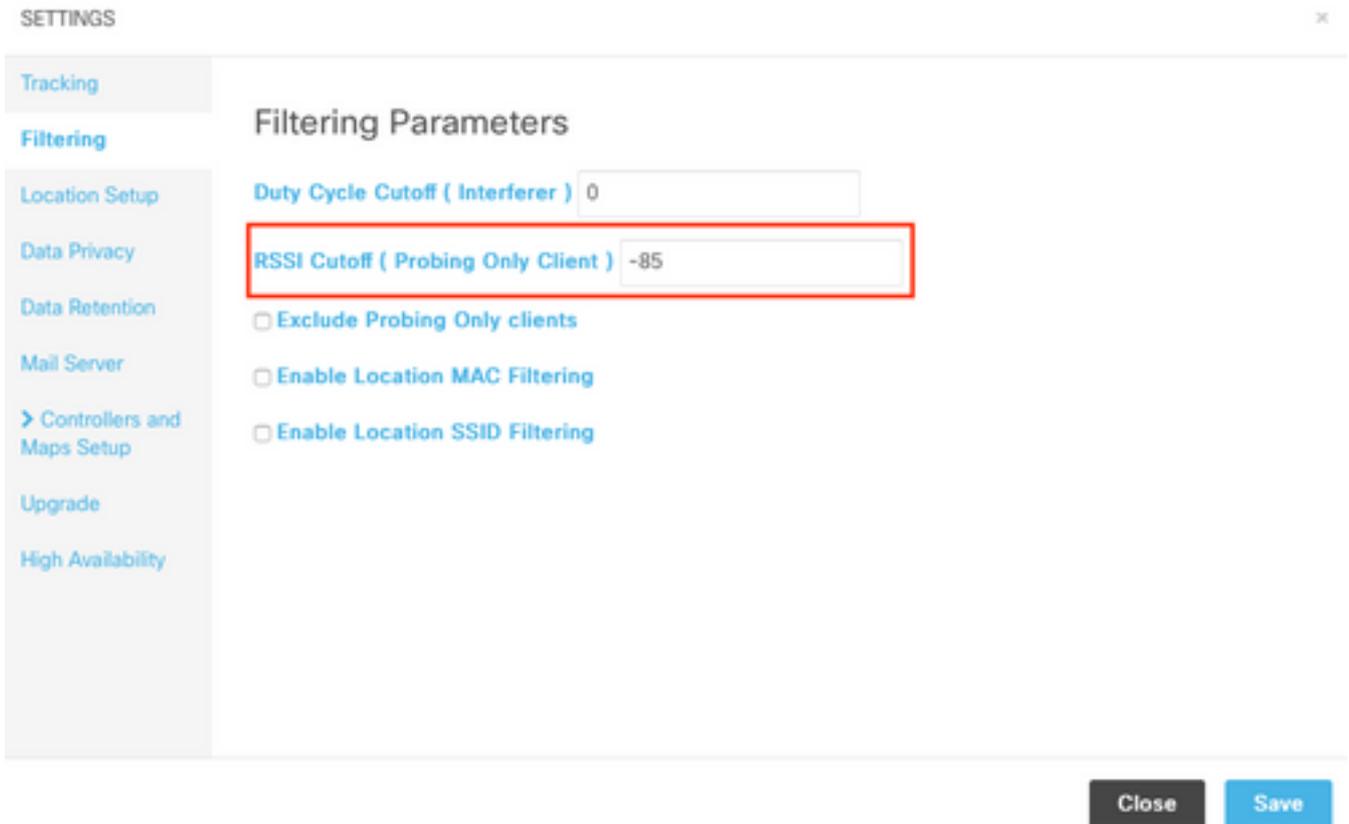
1. 듀티 사이클 컷오프(간섭 요인)
2. RSSI 컷오프
3. 클라이언트를 들어야 하는 최소 AP의 양이 기록되므로

밀도가 높고 인구 밀도가 높은 지역에서는 간섭원이 많을 것으로 예상됩니다. 블루투스 시계 같은 장치는 네트워크에 큰 영향을 미치지 않을 것입니다. 간섭 요인 듀티 사이클의 가치를 50에 가깝게 높임으로써 공기 시간의 50%를 차지하고 있는 강력한 간섭 요인만 CMX에 기록됩니다. 이 값은 System(시스템)->Settings(설정)->Filtering(필터링):

**참고:**막대한 양의 간섭 데이터를 기록하지 않기 위해 CMX는 일정 시간 동안 존재하는 간섭 요인만 기록합니다.



**RSSI 컷오프** 기능은 실제로 입력되지 않고 프레미스를 통과하는 클라이언트를 기록하지 않도록 하는 데 사용됩니다. 이는 클라이언트 추적만 활성화되고 버스 정류장 또는 인근 거리에 대한 탐지를 활성화하여 구축에 큰 영향을 미칠 수 있습니다. 기본적으로 이 값은 -85dBm으로 설정됩니다. 이 값을 변경하기 전에 구내외 클라이언트의 RSSI를 측정해야 합니다. 이 값은 System(시스템)->Settings(설정)->Filtering(필터링):



CMX 10.6부터 CMX에서 기록하기 위해 클라이언트를 듣기 위해 필요한 최소 AP의 양을 변경하는 것은 API 호출을 통해서만 가능합니다. 먼저 GET 요청을 사용하여 현재 컨피그레이션을 볼 수 있습니다.

```
[cmxadmin@mse3375 ~]$ curl -X get http://localhost/api/config/v1/filteringParams/1
{"name":null,"allowedMacs":[],"disallowedMacs":[],"blockedList":[],"noLocationSsids":[],"noAnalyticsSsids":[],"disallowprobingclienttracking":false,"macfilter":false,"ssidfilter":false,"probin
grssicutoff":-
85,"minapwithvalidrssi":1,"filterLocallyAdministered":true,"objectId":0,"dutyCycleCutoff":0}
```

이 설정에서 minapwithvalidrssi 값은 기본값인 1로 설정됩니다. POST 요청을 사용하여 이 값을 3으로 변경할 수 있습니다. 이러한 설정이 적용되면 RSSI의 세 번째 AP에서 수신한 클라이언트가 지정된 최소 AP와 같거나 더 높은 CMX에 의해 기록됩니다.

```
[cmxadmin@mse3375 ~]$ curl -X POST -H "Content-Type: application/json" -d
'{"minapwithvalidrssi":3}' http://localhost/api/config/v1/filteringParams/1
값을 변경한 후 GET 요청을 수행하여 설정이 성공적으로 적용되었는지 확인합니다.
```

## VM 리소스 증가

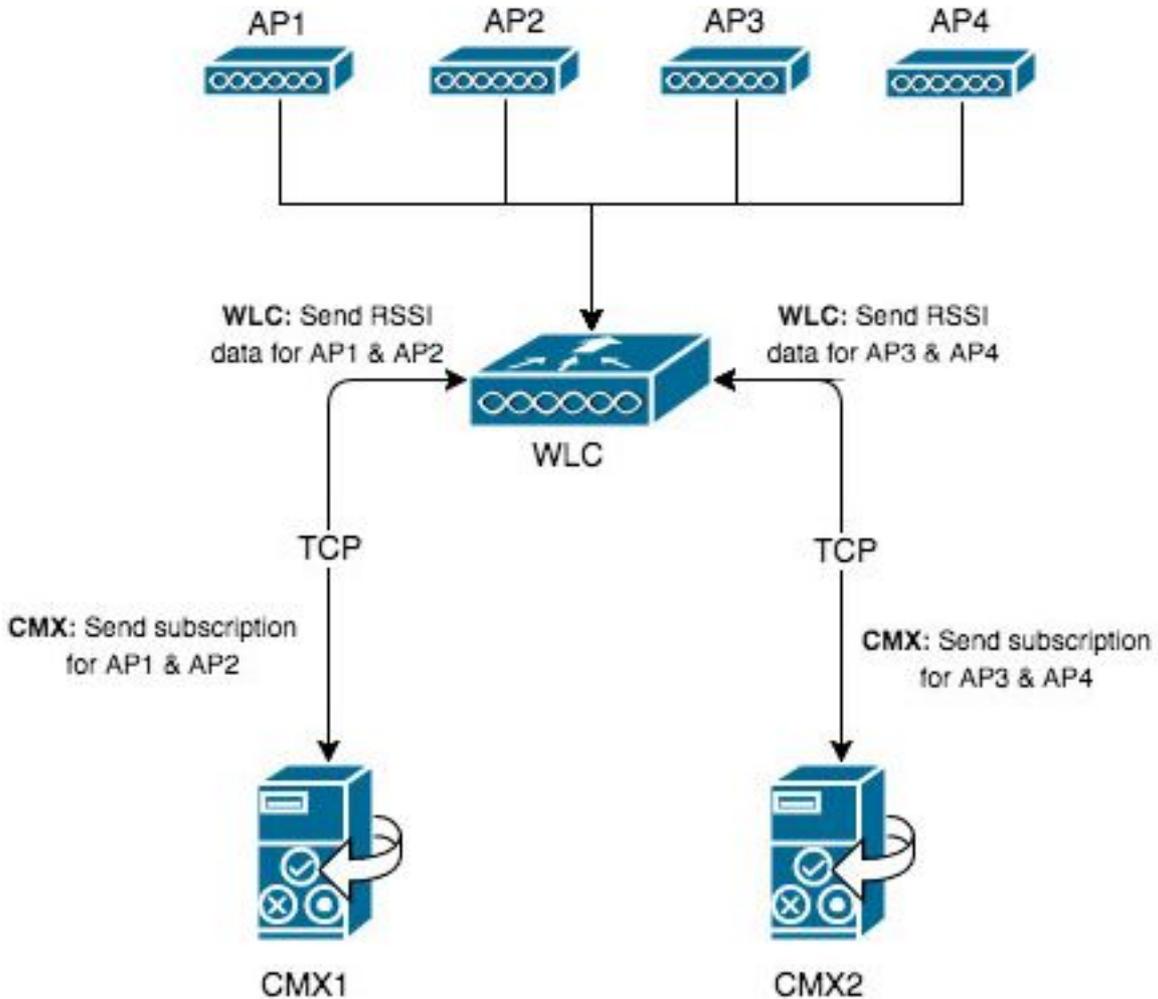
현재 CMX 노드가 VM에서 실행 중이고 해당 크기가 모든 클라이언트를 수용할 만큼 충분하지 않을 경우 VM 리소스와 처리 능력을 높일 수 있습니다. 더 많은 CPU 코어, 메모리 및 디스크 공간을 할당하기만 하면 됩니다. CMX Low-end, Standard 및 High-End 노드에 대한 정확한 요구 사항은 [여기](#)에서 확인할 수 있습니다.

현재 CMX 설정이 이미 하이 엔드 노드인 경우 이 문서에 언급된 다른 옵션을 고려하십시오.

**참고:** VM에서 스냅샷을 활성화하면 성능이 저하될 수 있으며 프로덕션 환경에서는 권장되지 않습니다.

## CMX 그룹화(이전의 AP 그룹화라고도 함)

CMX Grouping(CMX 그룹화)은 CMX 10.5 이상 및 AireOS WLC에서 8.7 이상 릴리스를 실행할 수 있는 기능입니다. 8.7 릴리스 열차는 향후 업데이트를 받지 않으므로 8.8 이상 릴리스를 사용하는 것이 좋습니다. 이 기능을 사용하면 단일 컨트롤러가 AP 그룹을 선택하고 특정 CMX 노드에 그룹을 지정하여 여러 CMX 노드에 로드를 분산할 수 있습니다. 이러한 AP 그룹은 WLC의 AP 그룹 기능과 관련이 없습니다.



CMX1의 맵에는 AP1 및 AP2만 배치됩니다. CMX1은 맵에 있는 2개의 AP에 대해 WLC와 통신합니다. CMX 그룹화 기능이 활성화되면 AP1 및 AP2에서 기록한 모든 정보(관련 및 프로브 전용 클라이언트, 간섭 요인, BLE 비콘, RFID 태그 포함)는 CMX1에만 전송됩니다.

단일 컨트롤러는 최대 4개의 NMSP 연결을 설정할 수 있습니다. 즉, CMX 노드를 4개까지 추가할 수 있습니다. 4개의 하이엔드 노드를 사용할 경우 이론적으로 매일 최대 360,000(4x90,000) 고유 클라이언트 MAC 주소를 기록할 수 있습니다.

WLC가 다음 test 명령으로 연결할 수 있는 CMX 서버의 양을 늘릴 수 있습니다

```
(Cisco Controller) >test cloud-server cmx max-tls-connections
test cloud-server cmx max-tls-connections <2-6>
```

**중요:** CMX 그룹화 기능을 사용하지 않고 8.7 이하 또는 8.7 이상의 코드를 실행하는 컨트롤러를 여러 WLC에 추가할 수 없습니다. 이로 인해 특히 HyperLocation 설정에서 부정확한 데이터가 기록될 수 있습니다.

이 컨트롤러가 추가될 모든 CMX 노드에서 기능을 활성화하고 서비스를 재시작하는 데 필요합니다.

1. 다음 명령을 사용하여 기능을 활성화합니다.

```
cmxctl config featureflags nmsplb.cmxgrouping true
```

true를 false로 바꾸면 기능이 비활성화됩니다.

2. CMX 에이전트 다시 시작:

```
cmxctl restart agent
```

3. NMSP 로드 밸런서를 다시 시작합니다.

```
cmxctl nmsplb stop
cmxctl nmsplb start
```

4. 기능이 성공적으로 활성화되었는지 확인하려면 다음을 실행합니다.

```
[cmxadmin@cmx3375 ~]$ cmxctl config featureflags
```

location.compactlocationhistory	false
configuration.oi.host	true
configuration.apimport	false
location.ssidfilterpersistblockedmacs	false
location.rogueapclienthistory	false
<b>nmsplb.cmxgrouping</b>	<b>true</b>
monit	true
container.influxdbreporter	true
nmsplb.autolearnssids	true
configuration.highendbypass	false
apiserver.enabled	true
location.computelocthroughassociatedap	false
analytics.queuetime	false

Monitor(모니터링) > Cloud Services(클라우드 서비스) > CMX에서 활성화된 CMX 노드가 표시되어야 합니다."없음"은 그룹화 기능이 비활성화된 반면, "그룹 보기"는 활성화되었음을 나타냅니다.

CISCO **MONITOR** WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Monitor

- Summary
- Access Points
- Cisco CleanAir
- Statistics
- CDP
- Rogues
- Clients
- Sleeping Clients
- Multicast
- Applications
- Lync
- Local Profiling
- Cloud Services
  - CMX**
  - Telemetry
    - Network Assurance
    - Webhook

**CMX Server**

CMX Server IP	Services	Sub-Services	AP Monitor Service Configuration	Group Subscriptions
10.48.71.41	RSSI	Mobile Station Tags Rogues		<a href="#">see Groups</a>
10.48.39.25	Info	Mobile Station Rogues		<a href="#">None</a>
	RSSI	Mobile Station Tags		
	Info	Mobile Station		
	Statistics	Mobile Station		

"See Group(그룹 보기)" 페이지를 열면 이 CMX 노드가 가입된 AP 목록에 액세스할 수 있습니다.

**CMX Server Ip :** 10.48.71.41

Group Name	Services	Sub-Services	AP Monitor Service Configuration	AP Subscriptions
	RSSI	Mobile Station		
CMX_10.48.71.41	Info	Mobile Station		<a href="#">list of Aps</a>
	Statistics	Mobile Station		

**CMX Server IP :** 10.48.71.41

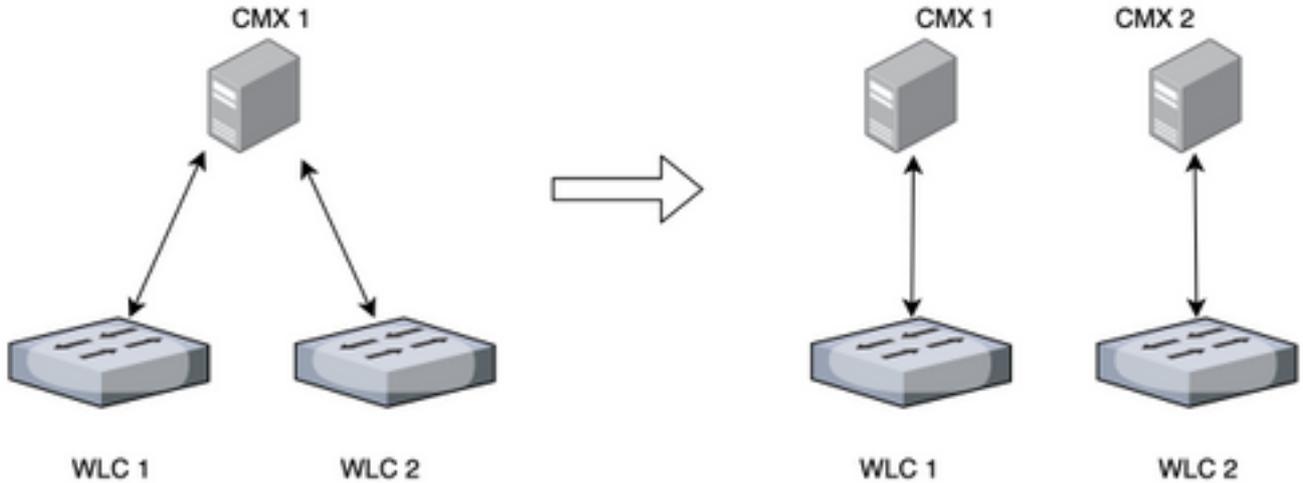
**CMX Group Name :** CMX\_10.48.71.41

No of AP	Base Radio Mac
1	00:2c:c8:de:2a:20
2	f4:cf:e2:40:a5:c0
3	f4:db:e6:80:9b:a0

이 컨트롤러에 연결된 총 4개의 AP 중 3개만 CMX 맵에 배치됩니다. WLC는 CMX에서 이 정보를 학습하고 10.48.71.41에 있는 CMX 노드로 탐지된 정보만 전송합니다.

## 추가 노드 구축

네트워크가 여러 무선 컨트롤러로 구성된 경우 추가 CMX 노드를 구축하고 여러 WLC와 CMX 간에 1-1 매핑을 생성할 수 있습니다. WLC 버전에는 특별한 요구 사항이 없습니다. 단일 WLC를 동시에 여러 CMX 노드에 추가하지 않도록 하십시오.



## DNA 공간 - 클라우드로 작업 오프로드

Cisco의 새로운 클라우드 플랫폼 DNA Spaces는 클라이언트 추적을 클라우드로 이동하는 것을 목표로 합니다. 리소스는 현재 로드와 따라 자동으로 할당됩니다. 다음과 같은 여러 가지 방법으로 무선 네트워크를 클라우드로 연결할 수 있습니다.

1. WLC를 클라우드로 직접 연결
2. DNA Spaces Connector(프록시 역할을 하는 소규모 VM인 컨트롤러는 클라우드로 노출되지 않음)
3. CMX를 클라우드의 게이트웨이로 사용(이 옵션은 HyperLocation 구축에 필요함)

## 관련 버그

- [CSCVq25953](#) - Location SSID Filtering(위치 SSID 필터링)을 활성화하면 로컬에서 관리되는 MAC의 제외가 비활성화되고 그 반대의 경우도 마찬가지입니다.