Optimize CMX Performance

Contents

Introduction

This article will explain how to recognize and then redistribute the load of a single CMX (Connected Mobile eXperience) node in order to accommodate large amount of devices being tracked. Problems like this are often observed in extremely large deployments in public areas or setups where probing client tracking is enabled.

Prerequisites

Requirements

This article assumes you have knowledge of the basic setup and configuration of a CMX and focuses only on tips and tricks to optimze performance in large deployments.

Components Used

All the commands and examples shown in this article were performed on 3504 WLC running 8.8.125 code and CMX 10.6.1 running on 3375 appliance.

Signs of an Overloaded CMX Node

Overload of a CMX node can result is several different problems:

- Services not being able to start
- Services abruptly stopping/crashing
- Analytics service showing 0 active clients

- Alarms and email alerts saying analytics or location service is in critical health
- Inability to establish HA between primary and secondary CMX node

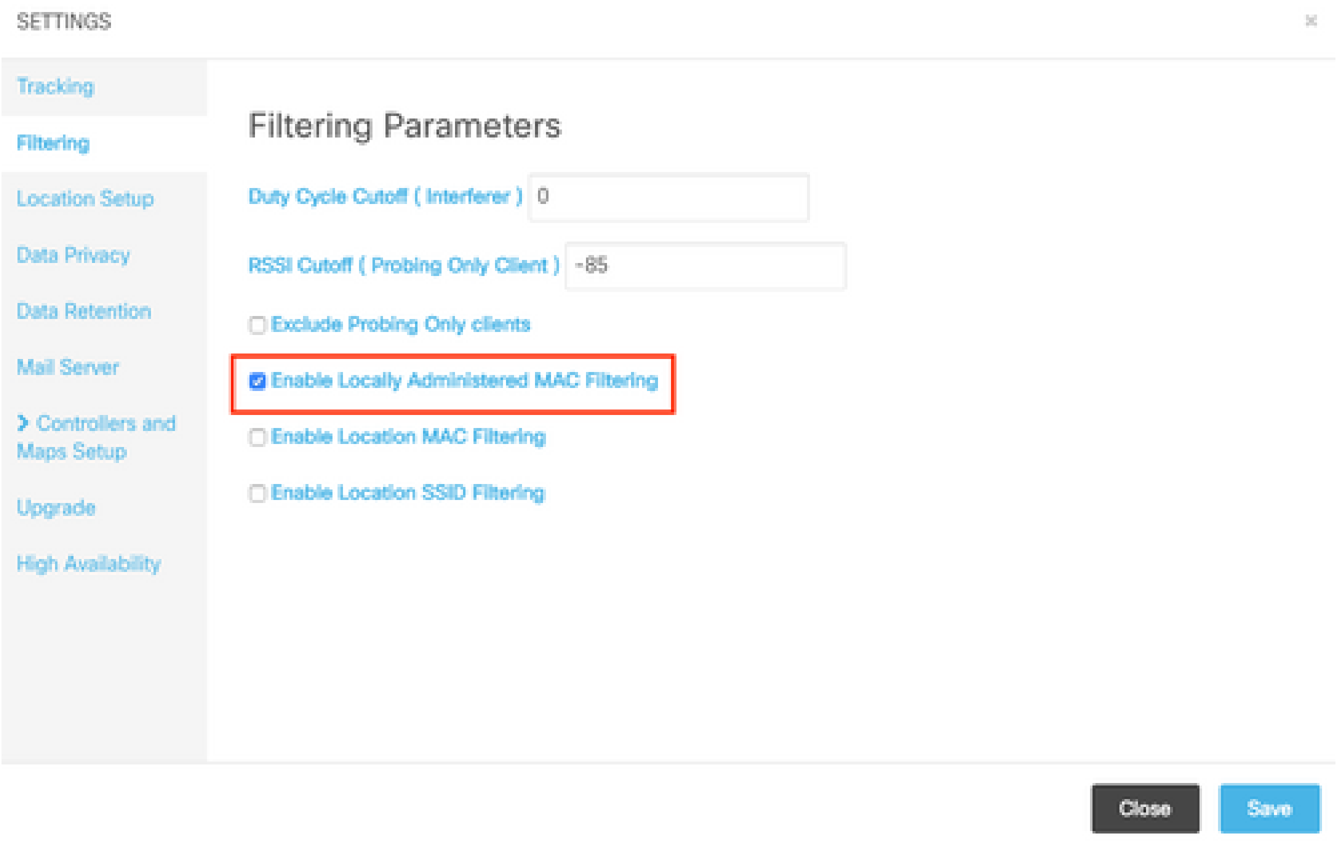
Redistribute CMX Load

Filtering Locally Administered MAC Addresses

Due to growing privacy concerns, starting with IOS 8 release in 2014, smartphone manufacturers have started to implement a feature called MAC randomization where devices would use new randomly generated MAC address every time they send a probe request. When generating a random MAC address, manufacturers can decide to either use "locally administered" MAC address which has a special bit that indicates that the address is random or simply generate a completely random address not distinguishable from a real one. Very small number of clients actually uses their real MAC address when probing.

CMX has a way to filter these fake random MAC addresses. Under System->Settings->Filtering, always make sure that "Enable Locally Administered MAC filtering" is checked.

> **Note**: This field has been removed from web interface in CMX 10.6.0 and is always enabled by default



SETTINGS

Filtering Parameters

Duty Cycle Cutoff (Interferer) 0

RSSI Cutoff (Probing Only Client) -85

☐ Exclude Probing Only clients

☑ Enable Locally Administered MAC Filtering

☐ Enable Location MAC Filtering

☐ Enable Location SSID Filtering

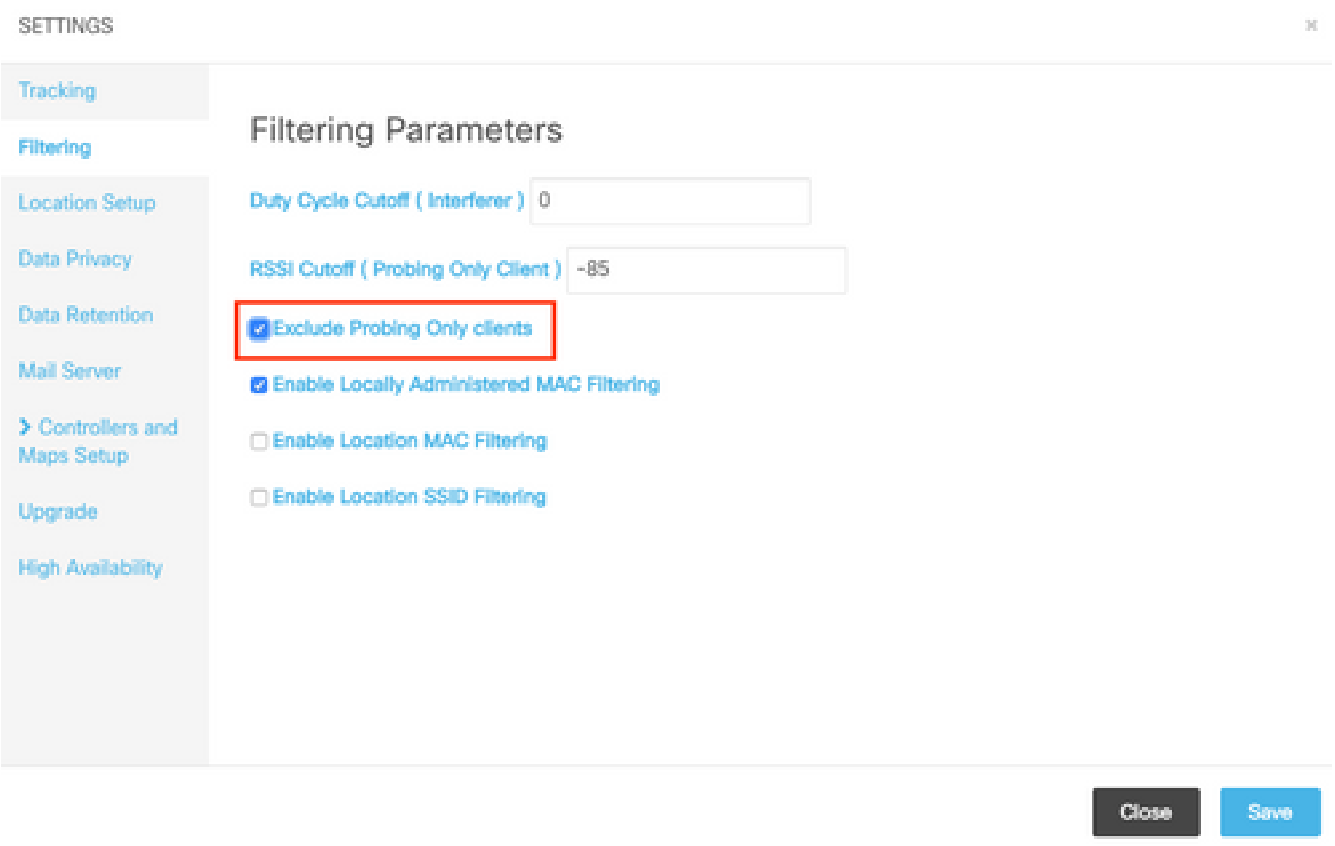
Tracking of Probing Clients

Most common root cause of a CMX overload that Cisco TAC deals with is tracking of probing only clients. Enabling this feature allows location tracking of unassociated clients. Open public areas like shopping malls and train station with huge number of visitors will very often exceed the limitations even of a High-end CMX node.

In setups that are tracking probing clients, randomly generated MAC addresses also have a very big impact on client count.

Some manufacturers like Apple are following a standard and using locally administered random MAC addresses when probing, which means that **iPhone devices will never be detected by CMX** when probing and unassociated. Devices that are not following the standard and using random MAC addresses that are not locally administered will be **recorded by CMX as a new client every time they send out the probe request** (which can happen every couple of seconds). As a result, the probing client count can be significantly higher/lower that the actual number of devices in the network.

Tracking of probing clients can be disabled from CMX web interfaces under System->Settings->Filtering by checking the option "Exclude Probing Only clients":



Filtering Parameters

Duty Cycle Cutoff (Interferer) 0

RSSI Cutoff (Probing Only Client) -85

☑ Exclude Probing Only clients

☑ Enable Locally Administered MAC Filtering

☐ Enable Location MAC Filtering

☐ Enable Location SSID Filtering

Due to all of the above-mentioned variations, probing client count should not be used as a footfall counter and Cisco TAC highly recommends against tracking of probing clients.

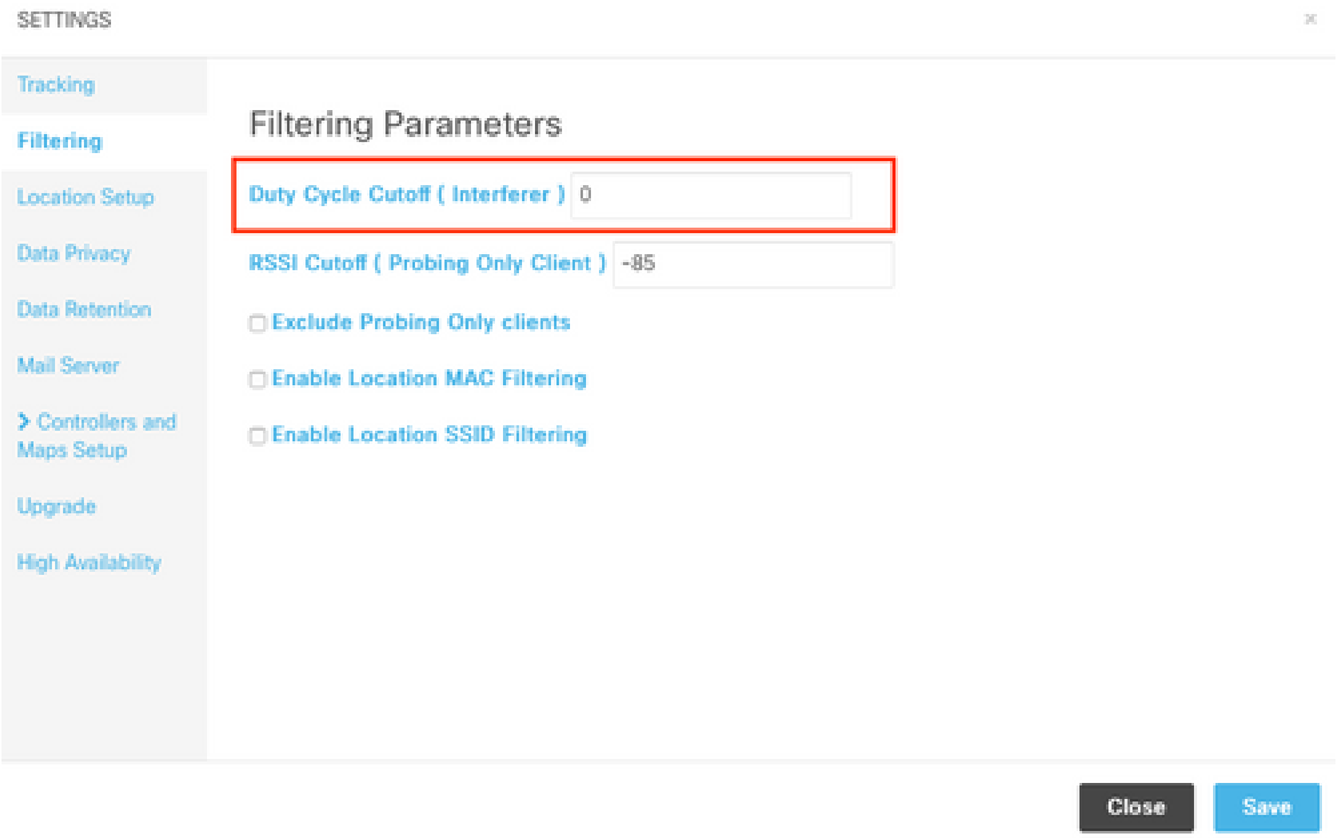
Detection Algorithm Tweaking

By tweaking the filtering options on CMX, the number of probing clients getting recorded can be severely limited. There are 2 main options that have significant impact on (especially probing only) client detection:

1. Duty Cycle Cutoff (Interferer)
2. RSSI Cutoff
3. Minimum amount of APs that need to hear the client, so it gets recorded

In a dense and highly populated areas, it is expected to have large number of interferers. Devices like Bluetooth watches will not have a huge impact on the network. By increasing the value of interferer duty cycle closer to, for example, 50, only strong interferers that are taking over 50% of the air-time will be recorded by CMX. This value can be configured from the CMX web interface, under System->Settings->Filtering:

> **Note**: To avoid recording huge amount of interferer data, CMX is only recording the interferers that are present for certain amount of time.



SETTINGS

Filtering Parameters

Duty Cycle Cutoff (Interferer) 0

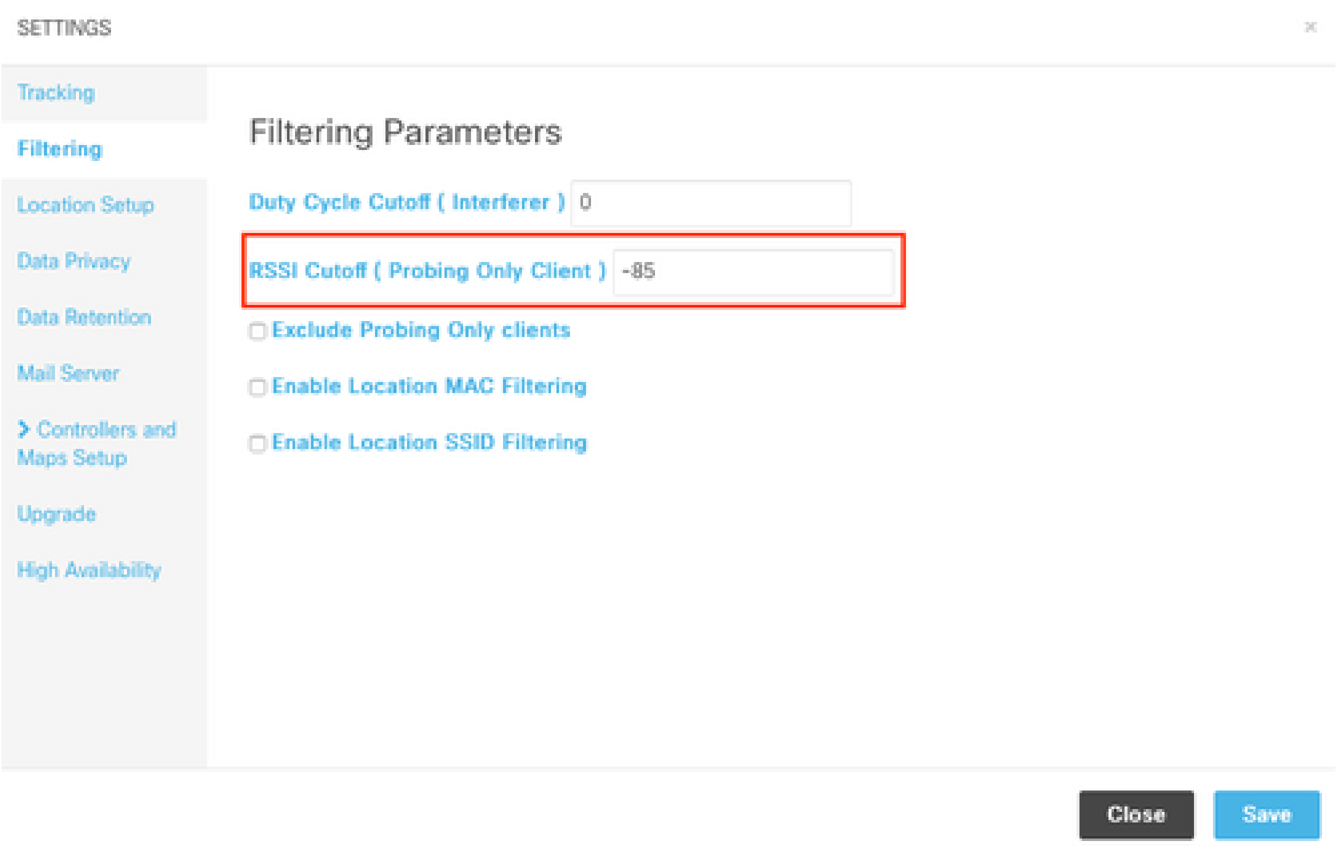
RSSI Cutoff (Probing Only Client) -85

□ Exclude Probing Only clients

□ Enable Location MAC Filtering

□ Enable Location SSID Filtering

RSSI cutoff feature is used to avoid recording clients that are just passing by the premises and not actually entering. This can have a huge impact on deployments with probing only client tracking enabled and a bus station or a street nearby. By default, this value is set to -85 dBm. Before changing this value, RSSI of a client outside of premises should be measured. This value can be configured from the CMX web interface, under System->Settings->Filtering:



Filtering Parameters

Duty Cycle Cutoff (Interferer) 0

RSSI Cutoff (Probing Only Client) -85

□ Exclude Probing Only clients

□ Enable Location MAC Filtering

□ Enable Location SSID Filtering

As of CMX 10.6, changing the **minimum amount of AP required to hear a client** for it to be recorded by CMX can only be done through an API call. First, a GET request can be used to see the current configuration:

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

In this setup, the value minapwithvalidrssi is set to 1, which is the default value. Changing this value to 3 can be done using a POST request. Once these settings are applied, client will be recorded by CMX once it is heard by the third AP at RSSI equal or better than the minimum specified one:

```
[cmxadmin@mse3375 ~]$ curl -X POST -H "Content-Type: application/json" -d
'{"minapwithvalidrssi":3}' http://localhost/api/config/v1/filteringParams/1
```

After changing any of the values, make sure to perform a GET request to confirm the settings have been successfully applied.

Increasing the VM resources

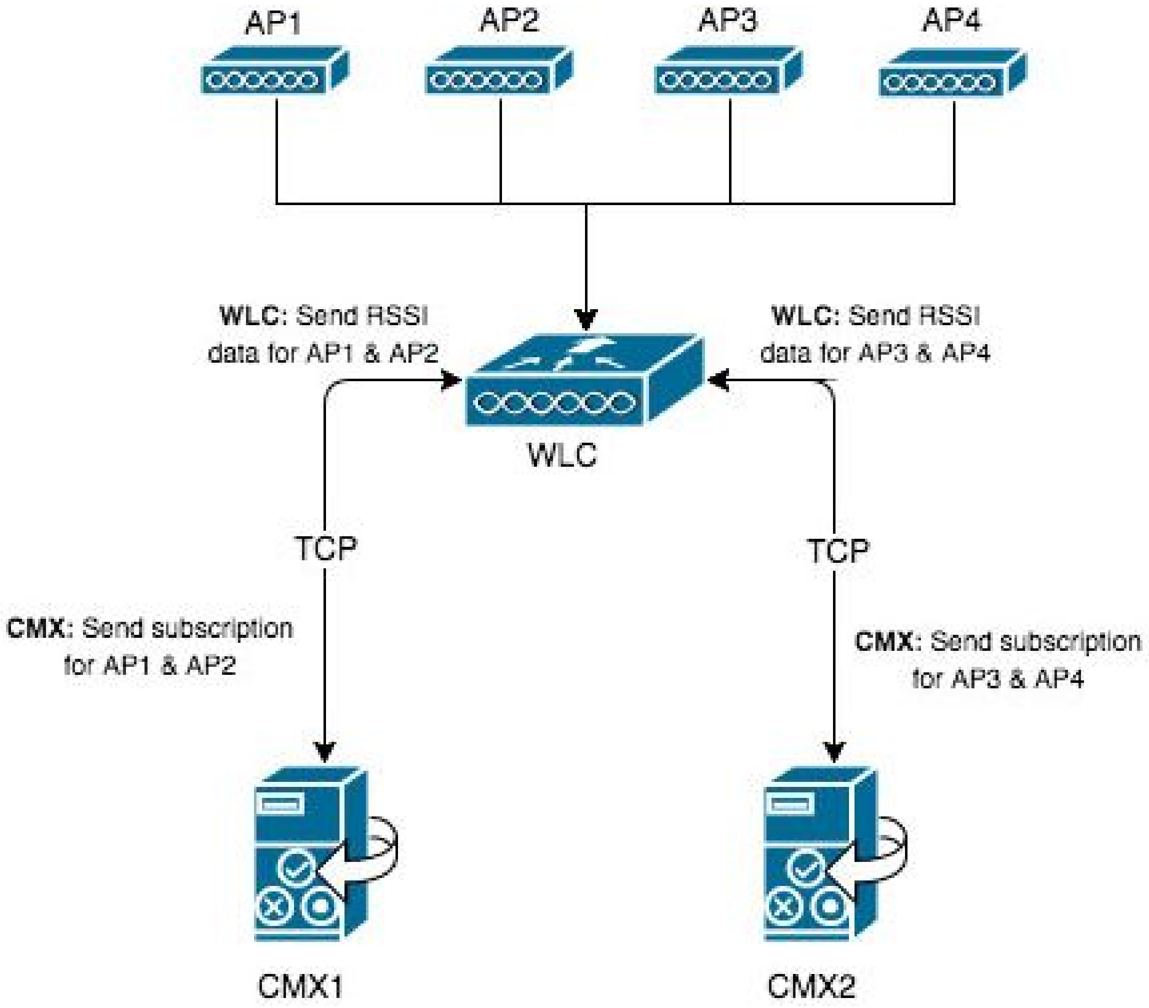
If a current CMX node is running in a VM and its size is not enough to accommodate all the clients, it is possible to increase the VM resources and therefore its processing power. Simply allocate more CPU cores, memory and disk space. Exact requirements for CMX Low-end, Standard and High-end node can be found HERE.

If current CMX setup is already a High-end node, consider other options mentioned in this article.

> **Note**: Having a snapshot active on a VM can have negative performance impact and is not recommended for production environments.

CMX Grouping (formerly known as AP Grouping)

CMX Grouping is a feature available on CMX 10.5 or later and AireOS WLCs running releases 8.7 or later. Since 8.7 release train will not receive updates in the future, it is recommended to use 8.8 or later release. This feature allows a single controller to distribute the load to multiple CMX nodes by selecting groups of APs and assigning a group to specific CMX node. These groups of APs are not related to the AP Group feature on the WLC.


AP1
AP2
AP3
AP4
WLC: Send RSSI data for AP1 & AP2
WLC: Send RSSI data for AP3 & AP4
WLC
TCP
TCP
CMX: Send subscription for AP1 & AP2
CMX: Send subscription for AP3 & AP4
CMX1
CMX2

Maps on CMX1 only have AP1 and AP2 placed. CMX1 will communicate with WLC about those 2 APs that are found on the map. Once CMX grouping feature is enabled, all the information recorded by the AP1 and AP2 (including associated and probing only clients, interferers, BLE beacons, RFID tags..) will be sent only to the CMX1.

A single controller can have up to 4 NMSP connections established at the time, meaning up to 4 CMX nodes can be added to it. With 4 High-end nodes, this would theoretically allow up to 360,000 (4x90,000) unique client mac addresses to be recorded per day.

It is possible to boost the amount of CMX servers a WLC can connect to with the following test command

```
[cmxadmin@mse3375 ~]$ curl -X POST -H "Content-Type: application/json" -d
```

```
'{"minapwithvalidrssi":3}' http://localhost/api/config/v1/filteringParams/1
```

> **Important**: Controller running a code lower than 8.7 or higher than 8.7 without CMX Grouping feature enabled should never be added to multiple WLCs. This can cause inaccurate data to be recorded, especially in HyperLocation setups.

On every CMX node that this controller will be added to, its required to enable the feature and restart the services:

1. Enable the feature using the command:

   ```
   [cmxadmin@mse3375 ~]$ curl -X POST -H "Content-Type: application/json" -d
   '{"minapwithvalidrssi":3}' http://localhost/api/config/v1/filteringParams/1
   ```

   Replacing the word `true` with `false` disables the feature.
2. Restart CMX agent:

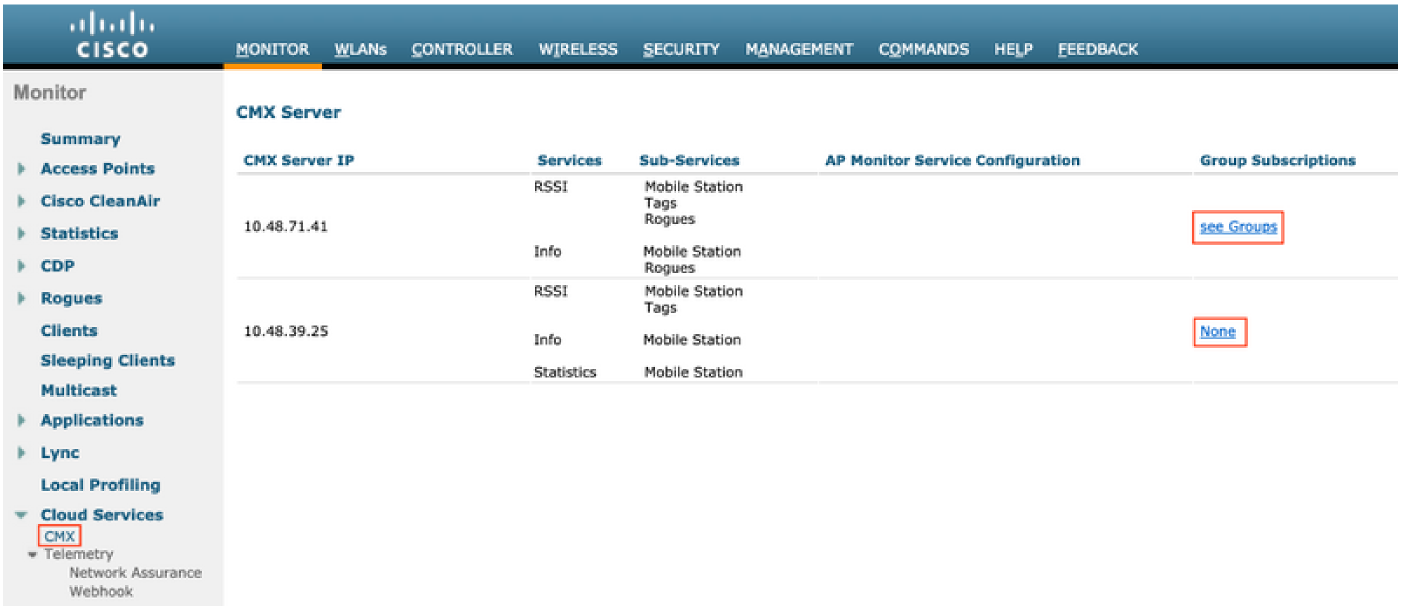
   ```
   [cmxadmin@mse3375 ~]$ curl -X POST -H "Content-Type: application/json" -d
   '{"minapwithvalidrssi":3}' http://localhost/api/config/v1/filteringParams/1
   ```

3. Restart the NMSP Load Balancer:

   ```
   [cmxadmin@mse3375 ~]$ curl -X POST -H "Content-Type: application/json" -d
   '{"minapwithvalidrssi":3}' http://localhost/api/config/v1/filteringParams/1
   ```
4. To check if the feature has been successfully enabled, run:

   ```
   [cmxadmin@cmx3375 ~]$ cmxctl config featureflags
   +----------------------------------------+-------+
   | location.compactlocationhistory        | false |
   +----------------------------------------+-------+
   | configuration.oi.host                  | true  |
   +----------------------------------------+-------+
   | configuration.apimport                 | false |
   +----------------------------------------+-------+
   | location.ssidfilterpersistblockedmacs  | false |
   +----------------------------------------+-------+
   | location.rogueapclienthistory          | false |
   +----------------------------------------+-------+
   | nmsplb.cmxgrouping                     | true  |
   +----------------------------------------+-------+
   | monit                                  | true  |
   +----------------------------------------+-------+
   | container.influxdbreporter             | true  |
   +----------------------------------------+-------+
   | nmsplb.autolearnssids                  | true  |
   +----------------------------------------+-------+
   | configuration.highendbypass            | false |
   +----------------------------------------+-------+
   | apiserver.enabled                      | true  |
   +----------------------------------------+-------+
   | location.computelocthroughassociatedap | false |
   +----------------------------------------+-------+
   | analytics.queuetime                    | false |
   +----------------------------------------+-------+
   ```

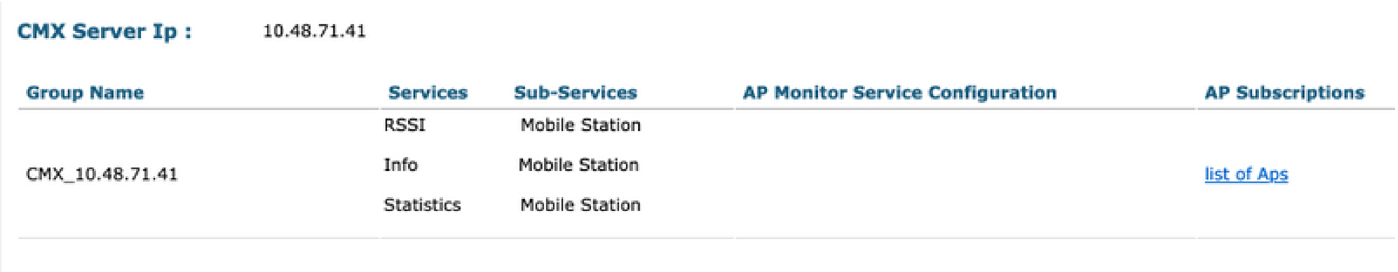
Under Monitor > Cloud Services > CMX it should be visible which CMX node has grouping feature enabled. "None" indicates grouping feature is disabled, while "see Groups" that it is enabled.



CMX Server

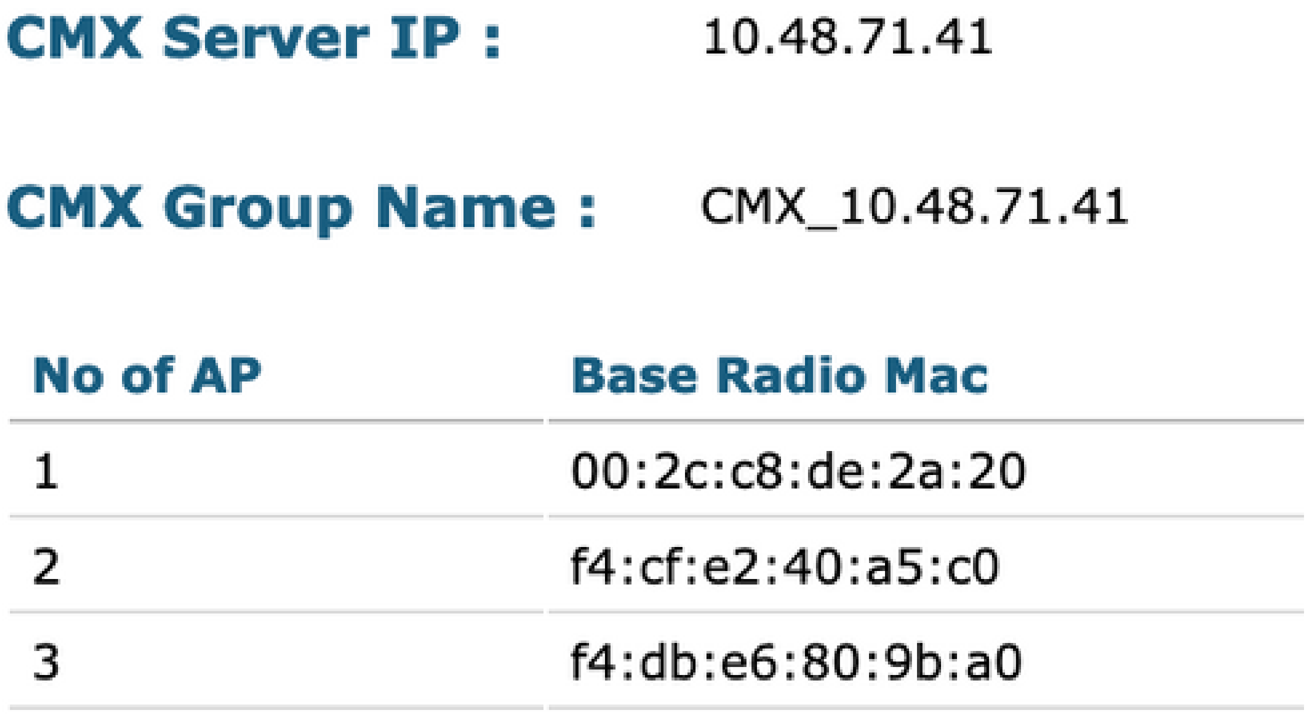
CMX Server IP	Services	Sub-Services	AP Monitor Service Configuration	Group Subscriptions
10.48.71.41	RSSI	Mobile Station Tags Rogues		see Groups
	Info	Mobile Station Rogues		
10.48.39.25	RSSI	Mobile Station Tags		None
	Info	Mobile Station		
	Statistics	Mobile Station		

Opening the "see Group" page, it is possible to access the list of APs this CMX node is subscribed to.



CMX Server Ip : 10.48.71.41

Group Name	Services	Sub-Services	AP Monitor Service Configuration	AP Subscriptions
CMX_10.48.71.41	RSSI	Mobile Station		list of Aps
	Info	Mobile Station		
	Statistics	Mobile Station		



CMX Server IP : 10.48.71.41

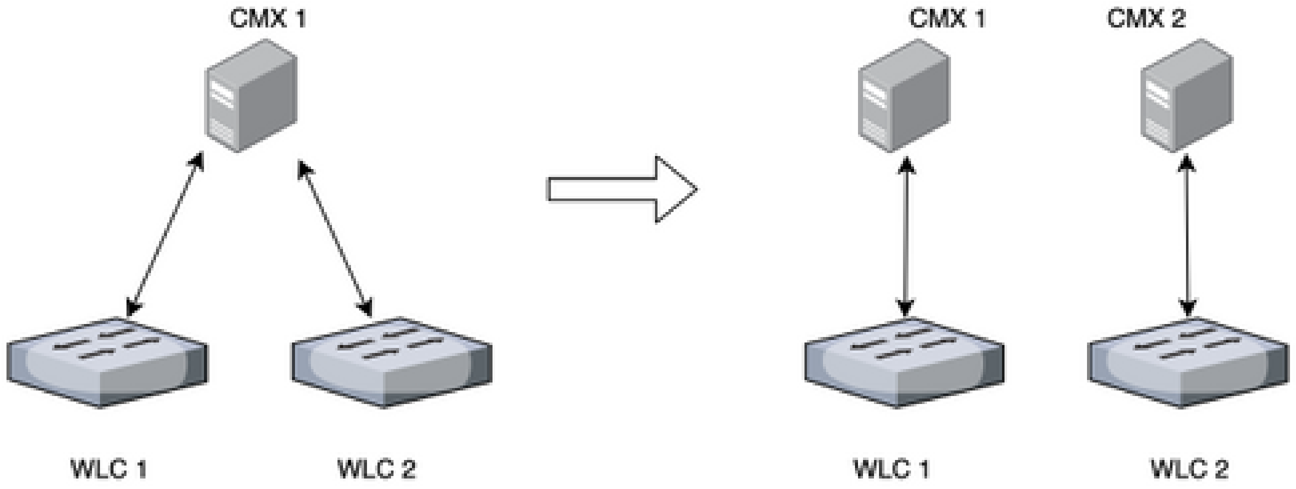
CMX Group Name : CMX_10.48.71.41

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

Out of the total 4 APs associated to this controller, only 3 are placed on the CMX map. WLC learns this from CMX and only sends information detected by them to the CMX node located on 10.48.71.41.

Additional Node Deployments

If the network consists of multiple wireless controllers, it's possible to deploy additional CMX nodes and create a 1-1 mapping between multiple WLCs and CMXs. There are no special requirements when it comes WLC version. Make sure not to have a single WLC added to multiple CMX nodes at the same time.



DNA Spaces - Offloading the Work to the Cloud

Cisco's new cloud platform DNA Spaces aims to move the client tracking to the cloud. The resources are automatically allocated based on the current load. It is possible to connect your wireless network to the cloud in several ways:

1. Directly connecting WLC to the cloud
2. DNA Spaces Connector (a small VM that acts as a proxy, controllers are not exposed to the cloud)
3. Using CMX as a gateway for cloud (this option is necessary for HyperLocation deployments)

Relevant bugs

- CSCvq25953 - Enabling Location SSID Filtering disables the exclusion of locally administered MACs and vice versa