

# Configuration et dépannage de l'hyperlocalisation dans CMX

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Acronymes utilisés](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

## Introduction

Ce document décrit comment configurer et dépanner l'hyperlocalisation dans Connected Mobile Experiences (CMX).

## Conditions préalables

### Conditions requises

Cisco vous recommande de connaître le guide de déploiement d'Hyperlocation.

### Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CMX 10.2.3-34
- WLC 2504 / 8.2.130.0
- AIR-CAP3702I-E-K9

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Ce document aide à dépanner Fast Locate et Hyperlocation lorsqu'ils ne fonctionnent pas comme prévu.

L'hyperlocalisation est une fonctionnalité de Cisco qui améliore la précision de l'emplacement. Vous pouvez en savoir plus sur cette fonctionnalité dans le [Guide de déploiement d'hyperlocalisation](#).

L'hyperlocalisation utilise les données relatives au niveau RSSI (client) et à l'angle d'arrivée (AoA) fournies par le point d'accès (AP).

Pour utiliser l'hyperemplacement, vous devez disposer d'un module d'hyperlocalisation (Wireless Security and Monitor/WSM) avec une antenne Halo. L'antenne Halo possède 32 antennes à l'intérieur et peut détecter d'où provient la sonde/le paquet, à l'exception des informations RSSI (Received Signal Strength Indication), ce qui rend l'emplacement plus précis. Plus d'informations peuvent être trouvées [ici](#).

En outre, Hyperlocation est une fonctionnalité qui ne peut être activée que lorsque CMX est installé sur l'appareil physique MSE (Mobility Services Engine) 3365 ou sur les applications virtuelles haut de gamme.

Reportez-vous au tableau 3. de la [feuille de données CMX](#) pour vérifier les directives matérielles.

Si vous n'êtes pas sûr des spécifications en cours d'exécution sur l'appliance virtuelle, vous pouvez émettre l'une des commandes suivantes :

```
cmxos inventory  
cmxos verify
```

## Acronymes utilisés

WLC - Contrôleur LAN sans fil

AoA - Angle d'arrivée

CMX - Connected Mobile Experience

Point d'accès - Point d'accès

NMSP - Network Mobility Service Protocol

SNMP - Simple Network Management Protocol

Interface utilisateur graphique - Interface utilisateur graphique

CLI - Interface de ligne de commande

ICMP - Internet Control Message Protocol

HTTP - Hyper Text Transfer Protocol

RSSI : indication de puissance du signal reçue

NTP - Network Time Protocol

MAC - Contrôle d'accès au support

WSM - Module de sécurité et de surveillance sans fil

## Configuration

Étape 1. Activer l'hyperemplacement sur le WLC.

Afin d'activer l'hyperemplacement sur le WLC, utilisez cette ligne de commande :

```
(Cisco Controller) >config advanced hyperlocation enable
```

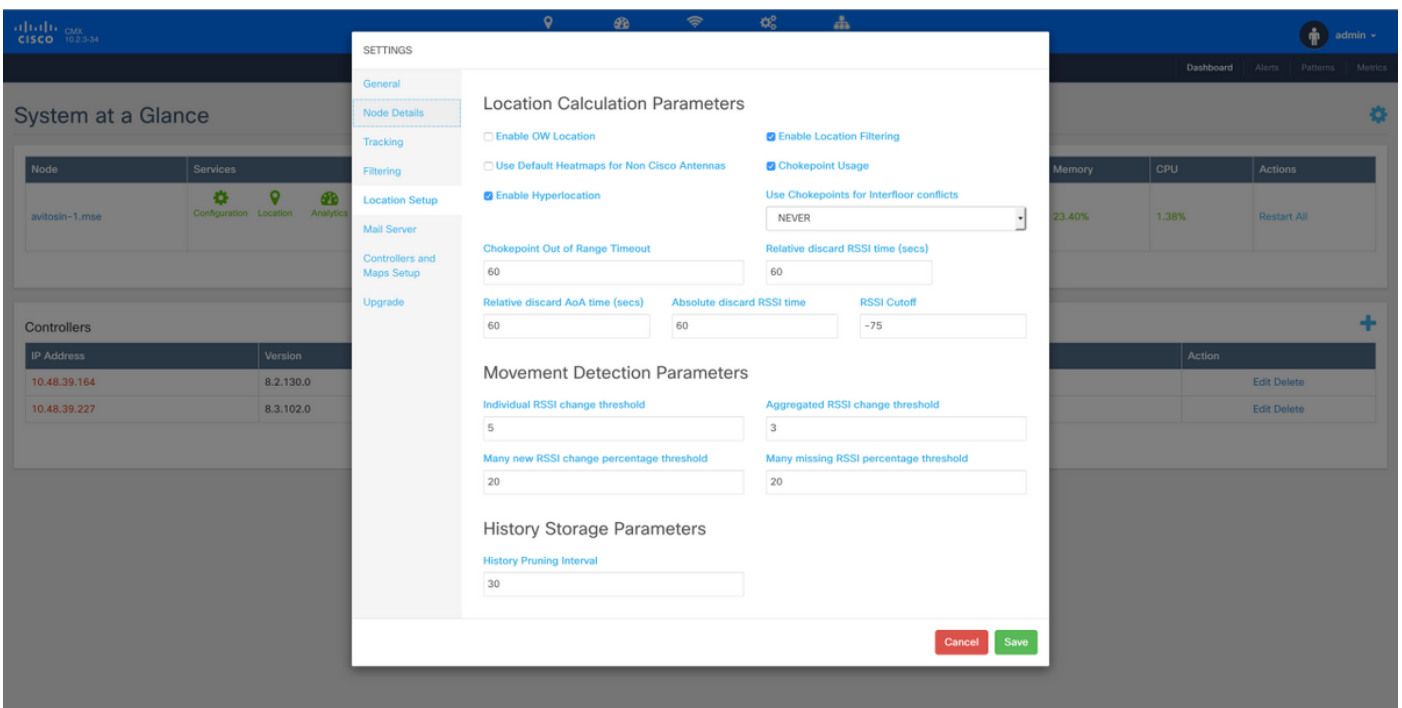
Il est également possible d'activer l'hyperemplacement dans l'interface graphique du WLC :

Accédez à **Wireless > Access Points > Global configuration > Enable Hyperlocation (case à cocher)**.

Étape 2. Activez Hyperlocation sur CMX.

Afin d'activer l'hyperemplacement dans le CMX, connectez-vous à l'interface utilisateur graphique et exécutez cette étape :

Naviguez jusqu'à **System > (Gear Icon) > Location Setup > Enable Hyperlocation (Case à cocher)** comme indiqué dans cette image.



Cela active également la fonction de localisation rapide (c'est-à-dire l'emplacement basé sur les trames de données), de sorte qu'elle doit être activée tant que vous avez des points d'accès ou des radios en mode de surveillance (non hyperlocation) ou avec le module d'hyperlocalisation. Il existe différents paramètres liés au service de localisation, que vous pouvez modifier. Vous trouverez plus d'informations ici ; [lien](#).

Étape 3. Vérifiez l'hyperemplacement sur le WLC.

Afin de vérifier si l'hyperemplacement est activé sur le WLC :

```
(Cisco Controller) >show advanced hyperlocation summary
Hyperlocation..... UP
Hyperlocation NTP Server..... 10.48.39.33
Hyperlocation pak-rssi Threshold..... -70
Hyperlocation pak-rssi Trigger-Threshold..... 10
Hyperlocation pak-rssi Reset-Threshold..... 8
Hyperlocation pak-rssi Timeout..... 3

AP Name          Ethernet MAC      Slots  Hyperlocation
-----
AP78ba.f99f.3c24  78:ba:f9:9d:a6:e0  3      UP
```

#### Étape 4. Vérifiez si le module Hyperlocation est détecté sur le point d'accès.

```
(Cisco Controller) >show ap inventory ?
```

```
<Cisco AP>      Enter the name of the Cisco AP.

all             Displays inventory for all Cisco APs
```

```
(Cisco Controller) >show ap inventory all
```

```
Inventory for AP78ba.f99f.3c24

NAME: "AP3700"      , DESCR: "Cisco Aironet 3700 Series (IEEE 802.11ac) Access Point"

PID: AIR-CAP3702I-E-K9,  VID: V03,  SN: FCW1915N9YJ

NAME: "Dot11Radio2"  , DESCR: "802.11N XOR Radio"

PID: AIR-RM3010L-E-K9 ,  VID: V01,  SN: FOC19330ASB

MODULE NAME: "Hyperlocation Module w/Antenna" ,DESCR: "Advanced Security Module (.11acW1)
w/Ant"

PID: AIR-RM3010L-E-K9 ,VID: V01 ,SN: FOC19330ASB ,MaxPower: 2000mW
```

```
(Cisco Controller) >show ap module summary all
```

```
AP Name          External Module Type
-----
AP78ba.f99f.3c24  Hyperlocation Module w/Antenna
```

**Note:** Il n'est pas possible de détecter si l'antenne halo est connectée au module d'hyperlocalisation. Vous devez le vérifier physiquement.

#### Étape 5. Vérifiez l'hyperemplacement sur le point d'accès.

```
ap#show capwap client rcb
```

```
-----OUTPUT OMITTED-----
```

```
Nexthop MAC Address      : 0014.f15f.f7ca
HYPERLOCATION ADMIN STATE : 1
WLC GATEWAY MAC          : 00:14:F1:5F:F7:CA
WLC HYPERLOCATION SRC PORT : 9999
BLE Module State         : ENABLED
MSE IP[0]                : 10.48.71.21
MSE PORT[0]              : 2003
```

```
-----OUTPUT OMITTED-----
```

Le point d'accès est celui qui envoie les messages AoA au CMX qui est transféré via le WLC. Assurez-vous que l'adresse IP MSE mentionnée est celle que vous voulez utiliser car une seule adresse IP MSE est prise en charge sur les points d'accès.

Assurez-vous que **WLC GATEWAY MAC** est l'adresse MAC de la passerelle du WLC, si CMX et le WLC ne sont pas dans le même sous-réseau.

Sinon, **WLC GATEWAY MAC** est l'adresse MAC CMX.

Étape 6. Vérifiez l'hyperemplacement sur CMX.

La première étape consiste à vérifier si tous les services sont exécutés sur CMX. Les mises en surbrillance sont utilisées par la fonction Hyperlocation.

```
[cmxadmin@avitosin-1 ~]$ cmxctl status
```

```
Done
```

```
The nodeagent service is currently running with PID: 19316
```

```
+-----+-----+-----+-----+
| Host      | Service      | Status  | Uptime (HH:mm) |
+-----+-----+-----+-----+
| avitosin-1.mse | Analytics | Running | 1 days, 02:14 |
+-----+-----+-----+-----+
| avitosin-1.mse | Cache_6378 | Running | 1 days, 02:15 |
+-----+-----+-----+-----+
| avitosin-1.mse | Cache_6379 | Running | 1 days, 02:14 |
+-----+-----+-----+-----+
| avitosin-1.mse | Cache_6380 | Running | 1 days, 02:14 |
+-----+-----+-----+-----+
| avitosin-1.mse | Cache_6381 | Running | 1 days, 02:14 |
+-----+-----+-----+-----+
| avitosin-1.mse | Cache_6382 | Running | 1 days, 02:14 |
+-----+-----+-----+-----+
| avitosin-1.mse | Cache_6383 | Running | 1 days, 02:14 |
+-----+-----+-----+-----+
| avitosin-1.mse | Cache_6385 | Running | 1 days, 02:14 |
+-----+-----+-----+-----+
```

avitosin-1.mse	Cassandra	Running	1 days, 02:15	
+-----+				
avitosin-1.mse	Confd	Running	1 days, 02:14	
+-----+				
avitosin-1.mse	Configuration	Running	1 days, 02:13	
+-----+				
avitosin-1.mse	Connect	Running	1 days, 02:13	
+-----+				
avitosin-1.mse	Consul	Running	1 days, 02:15	
+-----+				
avitosin-1.mse	Database	Running	1 days, 02:15	
+-----+				
avitosin-1.mse	Haproxy	Running	1 days, 02:14	
+-----+				
avitosin-1.mse	Hyperlocation	Running	1 days, 02:12	
+-----+				
avitosin-1.mse	Influxdb	Running	1 days, 02:14	
+-----+				
avitosin-1.mse	Iodocs	Running	1 days, 02:14	
+-----+				
avitosin-1.mse	Location	Running	1 days, 02:13	
+-----+				
avitosin-1.mse	Matlabengine	Running	1 days, 02:12	
+-----+				
avitosin-1.mse	Metrics	Running	1 days, 02:14	
+-----+				
avitosin-1.mse	Nmsplb	Running	0 days, 01:47	
+-----+				
avitosin-1.mse	Qlesspyworker	Running	1 days, 02:14	
+-----+				

Étape 7. Vérifiez si le CMX reçoit les informations AoA du WLC.

```
tcpdump -i eth0 dst port 2003 -w aoa3.pcap
```

La capture Wireshark prouve que le CMX reçoit les informations AoA comme l'illustre l'image.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
2	0.003747	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
3	1.087479	10.48.39.214	10.48.71.21	UDP	130	9999 → 2003 Len=88
4	2.733577	10.48.39.214	10.48.71.21	UDP	130	9999 → 2003 Len=88
5	2.999859	10.48.39.251	10.48.71.21	UDP	178	9999 → 2003 Len=136
6	3.001227	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
7	4.355249	10.48.39.214	10.48.71.21	UDP	146	9999 → 2003 Len=104
8	5.999538	10.48.39.251	10.48.71.21	UDP	178	9999 → 2003 Len=136
9	6.000959	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
10	8.999418	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
11	9.000791	10.48.39.251	10.48.71.21	UDP	178	9999 → 2003 Len=136
12	9.262904	10.48.39.214	10.48.71.21	UDP	146	9999 → 2003 Len=104
13	10.894785	10.48.39.214	10.48.71.21	UDP	130	9999 → 2003 Len=88
14	11.995126	10.48.39.251	10.48.71.21	UDP	194	9999 → 2003 Len=152
15	11.999193	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
16	14.994902	10.48.39.251	10.48.71.21	UDP	178	9999 → 2003 Len=136
17	14.996368	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
18	17.994857	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
19	17.996231	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
20	18.102843	10.48.39.251	10.48.71.21	UDP	130	9999 → 2003 Len=88
21	21.098408	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
22	21.099952	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
23	24.098574	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
24	24.099804	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
25	27.098099	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
26	27.099839	10.48.39.251	10.48.71.21	UDP	130	9999 → 2003 Len=88
27	28.880307	10.48.39.164	10.48.71.21	UDP	146	9999 → 2003 Len=104
28	28.881569	10.48.39.214	10.48.71.21	CAPP	146	CAPP MD5 Encrypted
29	30.094237	10.48.39.251	10.48.71.21	UDP	178	9999 → 2003 Len=136
30	30.097812	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
31	30.513451	10.48.39.214	10.48.71.21	UDP	130	9999 → 2003 Len=88
32	30.515926	10.48.39.164	10.48.71.21	UDP	130	9999 → 2003 Len=88

▶ Frame 1: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)  
 ▶ Ethernet II, Src: CiscoInc\_2a:c4:a3 (00:06:f6:2a:c4:a3), Dst: Vmware\_99:4e:19 (00:50:56:99:4e:19)  
 ▶ Internet Protocol Version 4, Src: 10.48.39.251, Dst: 10.48.71.21  
 ▶ User Datagram Protocol, Src Port: 9999 (9999), Dst Port: 2003 (2003)  
 ▼ Data (120 bytes)  
 Data: ae 2f 44 f0 00 00 b4 5f ef 06 fd cb b7 6c 03 c7 ...  
 [Length: 120]

Étape 8. Vérifier le déploiement de la carte/du point d'accès physique.

Il est très important de s'assurer que la flèche sur l'AP est configurée pour pointer dans la direction réelle sur la carte, sinon la précision de l'emplacement peut être désactivée. Techniquement, il n'est pas nécessaire que tous les points d'accès d'un étage aient leurs flèches dans la même direction, mais fortement recommandé d'éviter toute erreur dans la carte (par exemple en cas de remplacement de point d'accès, il est très facile d'oublier de reconfigurer l'orientation de l'antenne).

Il est important de comprendre que la précision ne peut être que comme prévu lorsque le client est détecté simultanément par 4 points d'accès avec un RSSI supérieur à -75 dbm. Si, pour une raison physique quelconque, certaines zones ne satisfont pas à ces exigences, la précision doit être inférieure à ce qui était prévu.

## Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

La procédure de vérification est déjà traitée dans la section Configurer, le cas échéant.

## Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dans cette section, nous aborderons des scénarios spécifiques à CMX. S'il existe des pare-feu entre le WLC et le CMX, vous devez ouvrir ces ports :

- 16113 Network Mobility Services Protocol (NMSP)
- AoA 2003 (l'AP encapsule le paquet AoA dans Capwap vers le WLC, par conséquent le port 2003 doit être ouvert entre le WLC et le CMX)
- 80 HTTP
- 443 HTTPS
- Internet Control Message Protocol (ICMP)
- 161, 162 SNMP (Simple Network Management Protocol)

Scénario 1. L'hyperemplacement est activé sur le CMX et n'est pas activé sur le WLC.

Dans ce cas, aucun message AoA n'est envoyé du WLC à CMX. Activez l'hyperemplacement dans sur WLC et vérifiez si CMX reçoit les messages AoA sur le port 2003 du WLC.

Scénario 2. Le WLC ne se synchronise pas avec CMX, mais il est accessible.

Dans ce cas, vérifiez les configurations NTP (Network Time Protocol) à la fois sur le CMX et le WLC (vérifiez la date)

Exécutez la commande **# show capwap client rcb** sur l'AP pour afficher ceci :

```
NextHop MAC Address           : 0014.f15f.f7ca
HYPERLOCATION ADMIN STATE      : 1
WLC GATEWAY MAC               : 00:14:F1:5F:F7:CA
WLC HYPERLOCATION SRC PORT     : 9999
BLE Module State              : ENABLED
Remote Machine's IP          : 0.0.0.0
```

## Informations connexes

- Consultez la liste de contrôle de dépannage de l'hyperlocalisation de CMX - . Si toutes ces étapes ne pointent pas vers le problème, consultez les [forums d'assistance](#) de cisco pour obtenir de l'aide (les résultats présentés dans ce document et la liste de contrôle vous aident certainement à résoudre votre problème sur les forums) ou ouvrez une demande d'assistance du TAC.
- [Support et documentation techniques - Cisco Systems](#)