

# Konfiguration und Fehlerbehebung für Hyperlocation in CMX

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Verwendete Abkürzungen](#)

[Konfigurieren](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einführung

Dieses Dokument beschreibt die Konfiguration und Fehlerbehebung von Hyperlocation in Connected Mobile Experiences (CMX).

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, den Hyperlocation-Bereitstellungsleitfaden kennen zu lernen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

Dieses Dokument unterstützt Sie bei der Behebung von Problemen mit der schnellen Suche und Hyperlocation, wenn diese nicht wie erwartet funktionieren.

Hyperlocation ist eine Funktion von Cisco, die die Standortgenauigkeit erhöht. Weitere Informationen zu diesem Feature finden Sie im [Hyperlocation Deployment Guide](#).

Hyperlocation verwendet die vom Access Point (AP) bereitgestellten Daten über den Client (RSSI-Level) und den Angle of Arrival (AoA).

Um den Hyperlocation verwenden zu können, benötigen Sie ein Hyperlocation-Modul (Wireless Security und Monitor/WSM) mit Halo-Antenne. Die Halo-Antenne verfügt über 32 Antennen im Inneren und kann erkennen, wo die Sonde/das Paket eingetroffen ist, abgesehen von den Informationen zur Signalstärke (Received Signal Strength Indication, RSSI), wodurch der Standort präziser wird. Weitere Informationen finden Sie [hier](#).

Hyperlocation ist außerdem eine Funktion, die nur aktiviert werden kann, wenn CMX auf der physischen Appliance der 3365 Mobility Services Engine (MSE) oder der High-End Virtual Applications installiert ist.

Siehe Tabelle 3. des [CMX-Datenblatts](#) zur Überprüfung der Hardware-Richtlinien.

Wenn Sie sich nicht sicher sind, welche Spezifikationen auf der virtuellen Appliance ausgeführt werden, können Sie einen der folgenden Befehle ausführen:

```
cmxos inventory  
cmxos verify
```

## Verwendete Abkürzungen

WLC = Wireless LAN Controller

AoA - Ankunfts Winkel

CMX - Connected Mobile Experience

AP = Access Point

NMSP = Network Mobility Service Protocol

SNMP = Simple Network Management Protocol

GUI - Grafische Benutzeroberfläche

CLI = Command Line Interface

ICMP = Internet Control Message Protocol

HTTP: Hyper Text Transfer Protocol

RSSI = Received Signal Strength Indication

NTP = Network Time Protocol

MAC = Media Access Control

WSM = Wireless Security and Monitoring Module

## Konfigurieren

### Schritt 1: Aktivieren von Hyperlocation auf WLC

Um Hyperlocation auf WLC zu aktivieren, verwenden Sie die folgende Befehlszeile:

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

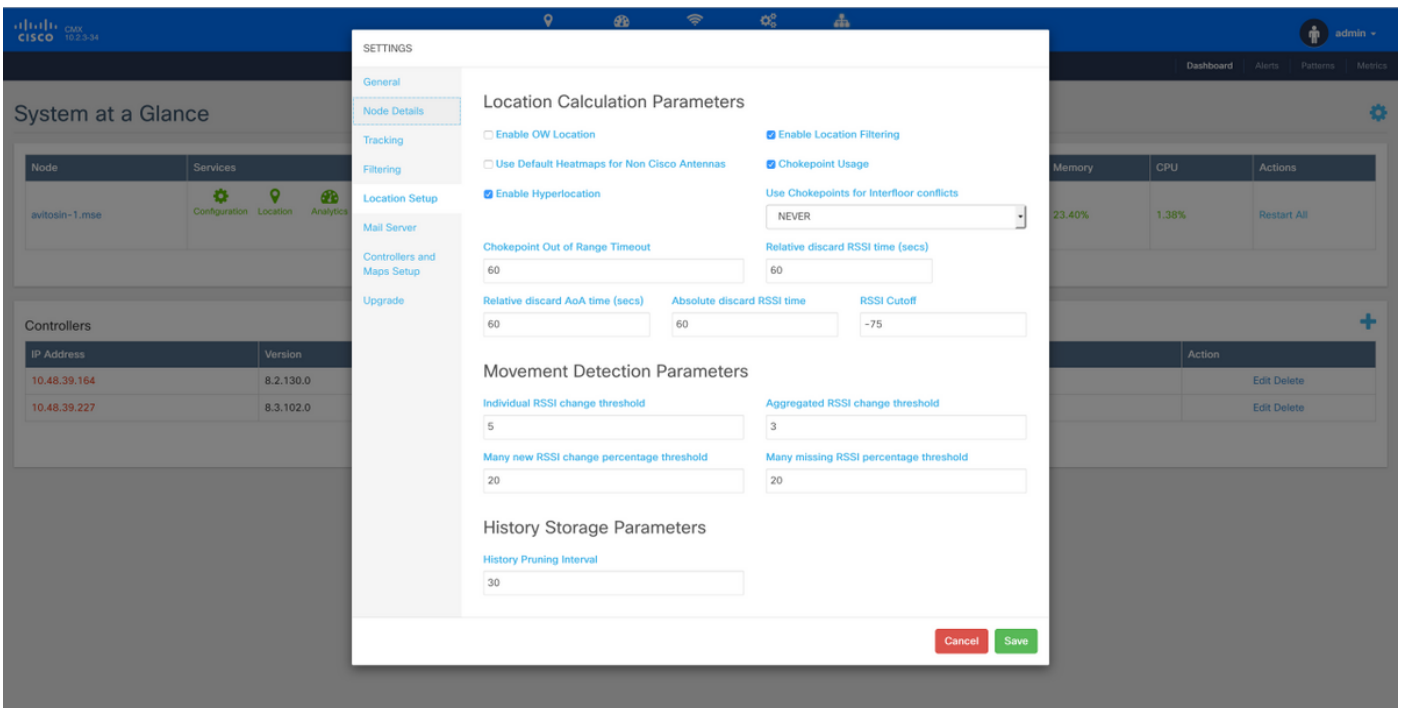
Die Hyperlocation kann auch in der WLC-GUI aktiviert werden:

Navigieren Sie zu **Wireless > Access Points > Global Configuration > Enable Hyperlocation (Kontrollkästchen)**.

### Schritt 2: Aktivieren Sie Hyperlocation auf dem CMX.

Um Hyperlocation in CMX zu aktivieren, melden Sie sich bei der GUI an, und führen Sie den folgenden Schritt aus:

Navigieren Sie zu **System > (Zahnrad-Symbol) > Location Setup > Enable Hyperlocation (Kontrollkästchen)**, wie in diesem Bild gezeigt.



Dies aktiviert auch Fast Locate (d. h. standortbasiert auf Daten-Frames), sodass es aktiviert wird, solange Sie über (nicht Hyperlocation-)Überwachungsmodus-APs oder -Funkmodule oder über das Hyperlocation-Modul verfügen. Es gibt verschiedene Parameter im Zusammenhang mit dem Standortdienst, die Sie anpassen können. Weitere Informationen finden Sie hier; [Link](#).

### Schritt 3: Überprüfen der Hyperlocation auf WLC

So prüfen Sie, ob die Hyperlocation auf dem WLC aktiviert ist:

(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
```

#### Schritt 4: Überprüfen Sie, ob das Hyperlocation-Modul am Access Point erkannt wird.

(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
```

**Hinweis:** Es ist nicht möglich festzustellen, ob die Halo-Antenne mit dem Hyperlocation-Modul verbunden ist. Sie müssen das physisch überprüfen.

#### Schritt 5: Überprüfen der Hyperlocation auf dem Access Point

```
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-----
```

Der Access Point sendet die AoA-Nachrichten an den CMX, der über den WLC weitergeleitet wird. Stellen Sie sicher, dass die angegebene MSE-IP die IP ist, die Sie verwenden möchten, da auf den APs nur eine MSE-IP unterstützt wird.

Stellen Sie sicher, dass die **WLC-GATEWAY-MAC** die MAC-Gateway-Adresse des WLC ist, wenn CMX und der WLC sich nicht im gleichen Subnetz befinden.

Andernfalls ist die **WLC-GATEWAY-MAC**-Adresse die CMX-MAC-Adresse.

Schritt 6: Überprüfen Sie die Hyperlocation in CMX.

Der erste Schritt besteht darin, zu überprüfen, ob alle Dienste auf CMX ausgeführt werden. Die hervorgehobenen Elemente werden vom Hyperlocation-Feature verwendet.

```
[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

Schritt 7: Überprüfen Sie, ob der CMX die AoA-Informationen vom WLC erhält.

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

Die Wireshark-Erfassung belegt, dass das CMX die im Bild gezeigten AoA-Informationen erhält.

Apply a display filter ... <%%/>

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]

Schritt 8: Überprüfen Sie die Map/Physical AP Deployment.

Es ist sehr wichtig, sicherzustellen, dass der Pfeil des Access Points so konfiguriert ist, dass er in die tatsächliche Richtung auf der Karte zeigt. Andernfalls kann die Standortgenauigkeit abgeschaltet werden. Es ist technisch nicht erforderlich, dass alle APs eines Stockwerks ihre Pfeile in die gleiche Richtung weisen, aber es wird dringend empfohlen, Fehler in der Karte zu vermeiden (z. B. bei einem Austausch des Access Points, ist es sehr leicht zu vergessen, die Antennenausrichtung neu zu konfigurieren).

Es ist wichtig zu verstehen, dass die Genauigkeit nur dann wie erwartet erreicht werden kann, wenn der Client gleichzeitig von 4 APs mit einem RSSI besser als -75 dBm erkannt wird. Erfüllen einige Bereiche aus irgendeinem physischen Grund diese Anforderungen nicht, so muss die Genauigkeit geringer sein als erwartet.

## Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Überprüfungsverfahren wird ggf. bereits im Abschnitt Konfigurieren erläutert.

## Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

In diesem Abschnitt werden CMX-spezifische Szenarien erläutert. Wenn zwischen dem WLC und CMX Firewalls vorhanden sind, müssen Sie diese Ports öffnen:

- 16113 Network Mobility Services Protocol (NMSP)
- 2003 AoA (Der AP kapselt das AoA-Paket in Capwap in Richtung WLC ein, daher muss Port 2003 zwischen WLC und CMX offen sein)
- 80 HTTP
- 443 HTTPS
- Internet Control Message Protocol (ICMP)
- 161, 162 Simple Network Management Protocol (SNMP)

Szenario 1. Der Hyperlocation ist auf dem CMX aktiviert und auf dem WLC nicht aktiviert.

In diesem Fall werden keine AoA-Nachrichten vom WLC an CMX gesendet. Aktivieren Sie die Hyperlocation in WLC, und überprüfen Sie, ob CMX die AoA-Meldungen an Port 2003 vom WLC empfängt.

Szenario 2. Der WLC lässt sich nicht mit CMX synchronisieren, ist aber erreichbar.

In diesem Fall überprüfen Sie die NTP-Konfigurationen (Network Time Protocol) auf dem CMX und dem WLC (überprüfen Sie das Datum).

Führen Sie den Befehl **# show capwap client rcb** auf dem Access Point aus, um Folgendes anzuzeigen:

```
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
```

## Zugehörige Informationen

- Überprüfen Sie die CMX Hyperlocation Troubleshooting-Checkliste - . Wenn alle diese Schritte nicht auf das Problem hinweisen, besuchen Sie die Cisco [Support-Foren](#), um Hilfe zu erhalten (die in diesem Dokument und in der Checkliste präsentierten Ausgaben helfen Ihnen definitiv, Ihr Problem in den Foren einzugrenzen), oder öffnen Sie eine TAC-Support-Anfrage.
- [Technischer Support und Dokumentation - Cisco Systems](#)