The Cisco CMX Detect and Locate Service

Overview of the Detect and Locate Service

The Cisco Connected Mobile Experiences (Cisco CMX) **DETECT & LOCATE** service enables you to view and track devices in your deployment.

Using the **DETECT & LOCATE** service, you can either view all the access points (APs) deployed in all the buildings of a campus or view the APs deployed on the individual floors of each building. You can also locate Wi-Fi tags, Wi-Fi interferers, and Bluetooth low energy (BLE) Tags.

Initial Configurations

In order to use the **DETECT & LOCATE** service, the following initial configurations have to be performed:

• Import maps—For information about this, see Importing Maps and Cisco Wireless Controllers.

• Add controllers—For information about concept, see Adding Cisco WLCs.

Viewing or Tracking Devices

Procedure

Step 1   Log in to Cisco Connected Mobile Experiences (Cisco CMX).

Step 2   Click **DETECT & LOCATE**.

Step 3   Using the left pane of the **Activity Map** window, navigate to the desired building and floor.

The **Activity Map** window displays a list of icons to the right.

Figure 1: Activity Map Window
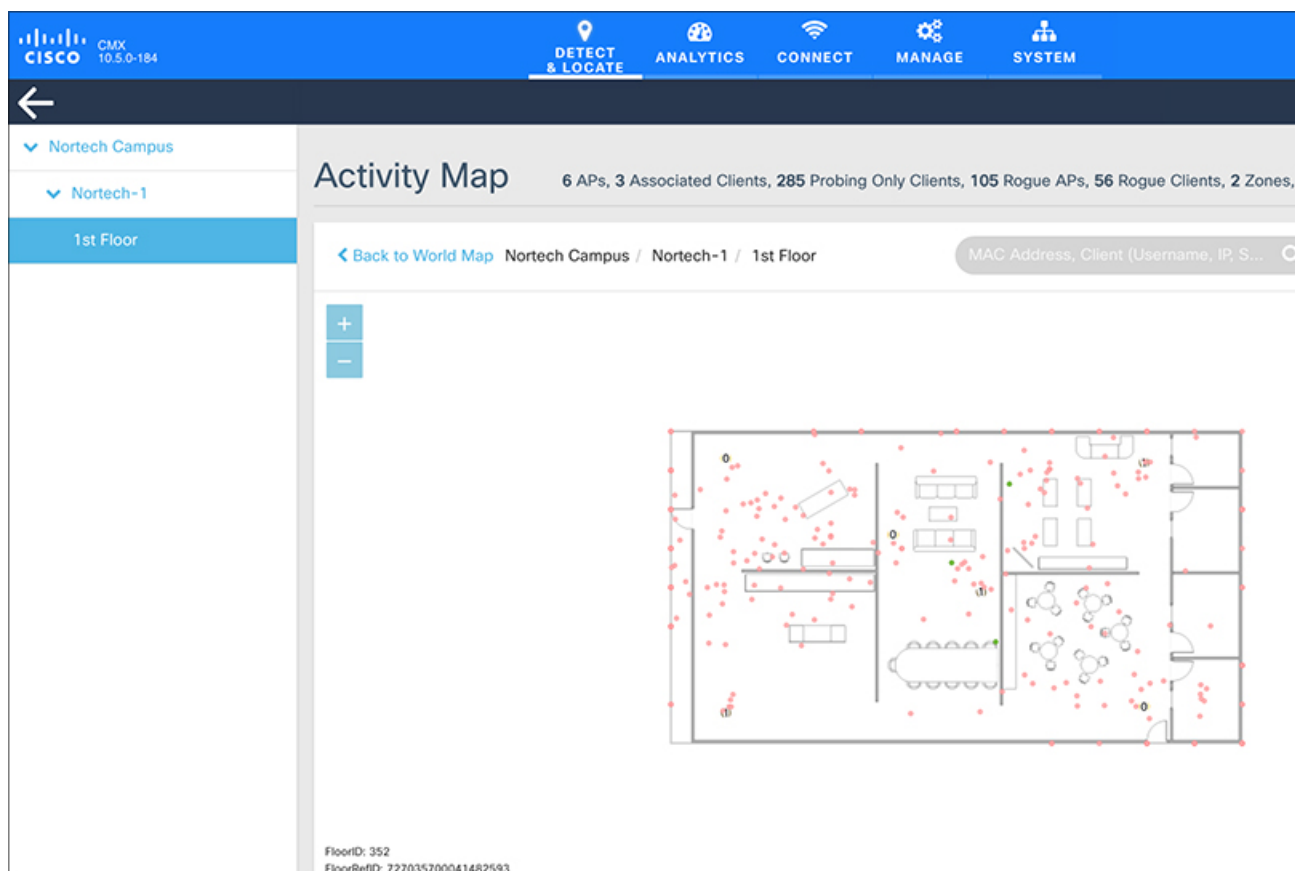
Step 4   Choose any combination of the following icons to customize your view of the devices:

- **Clients**—Click the **Clients** icon to show or hide all the client devices (connected and detected) that are being tracked by your Cisco CMX. Client devices are displayed either as red dots (probing clients) or green dots (connected clients). Clicking on connected clients show the AP that the client is associated with (blue lines) and the APs that are participating in the location calculation (red lines), and while clicking on a probing of unassociated client displays the APs that are being used to detect the clients (red lines).

Note   The maximum number of clients (connected and detected) that can be displayed at a given time is 2000. If this limit is exceeded, only connected clients are displayed, again up to a maximum of 2000 (see the figure below). However, if the number of total connected clients also exceeds 2000, no clients are displayed. In such a scenario, we recommend that you use the Analytics service to view the client information.

- **Heatmap**—Click the **Heatmap** ⚲ icon to show or hide areas with varying concentrations of client devices. Areas with a high concentration of client devices are marked bright red, as shown in this figure.
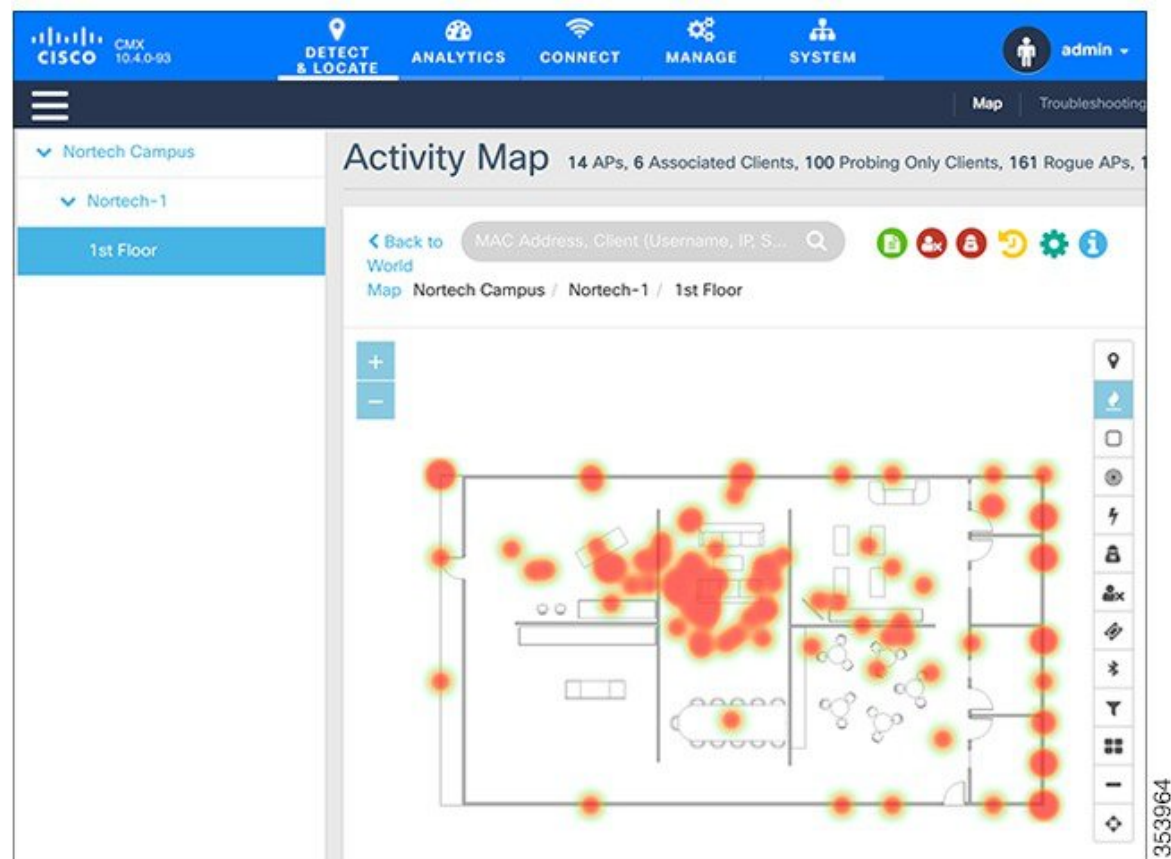
- **Zones**—Click the **Zones** ☐ icon to show or hide the zones on a specific floor.

- **Access Points**—Click the **Access Points** ◉ icon to show or hide all the APs that have been deployed on a specific floor. APs are displayed as circular objects, with a number in the center. This number indicates the number of clients connected to that specific AP. Inactive access points (red circle with a hyphen) are also detected.

Cisco CMX shares Access Points grouping information to Cisco WLC every time when a NMSP connection is established. To get a list of APs connected to the Cisco WLC, Cisco CMX performs a SNMP get action on the Cisco WLC. Based on the list of APs recived from the Cisco WLC and the APs on the map, identify the subset of APs and prepare a grouping request to send to the controller. You can store the AP grouping information on the datastore.

Note
- In Cisco CMX Release 10.2.1, when you select an access point icon from a floor map displayed on the **Activity Map** window, the Access Point information area includes Angles information.

- Clicking an AP shows the clients connected to it (blue lines), the probing clients that are detected by the AP (red lines), and additional information such as height, orientation, and X,Y location of the AP.

- If you have a Cisco Hyperlocation module that is attached to the back of your Cisco Aironet 3700 and 3600 Series APs, you can track the location of customers, visitors, or assets to about one meter in an ideal environment. Currently, the Hyperlocation solution works for the associated clients only.

- **Interferers**—Click the **Interferers** ⚡ icon to show or hide all the RF interferers that have been detected by the wireless network, and their zone of impact.

Note In Cisco CMX release 10.4, the BLE Beacons management page is no longer available on the Cisco CMX user interface. Beacon notifications are no longer provided. BLE beacons detected by Cisco CleanAir are displayed on Cisco CMX as interferers. BLE-related information is no longer available on the apidocs file.

- **Rogue APs**—Click the **Rogue APs** icon to show or hide the rogue access points. Rogue access points are those access points that are not part of the Cisco CMX infrastructure access points and not managed by Cisco CMX. They are classified as Unclassified, Malicious, Friendly, and Custom and indicated by different colors on the Activity Map.

- **Rogue Clients**—Click the **Rogue Clients** icon to show or hide rogue clients. Rogue clients are clients connected to rogue access points.

Note To track rogue access points and clients, enable the tracking parameters **Rogue Access Points** and **Rogue Clients** in the **Network Location Service** window under the **System** tab. For more information, see Setting Device-Tracking Parameters.

- **BLE Tags**—Click the **BLE Tags** ❋ icon to show or hide BLE-transmitting devices that have been detected by the wireless network.

Note	A beacon is detected as an interferer. A common problem faced in the context of beacons is tracking not being enabled. In such a scenario, you can modify the tracking configurations using the System service. For more information, see the Viewing or Tracking Devices, on page 2.

Click **Beacons** to view the beacon attributes related to the selected beacon profile.

- If the beacon is chirping with iBeacon profile, Cisco CMX displays the properties such as UUID, Major and Minor number.

- If the beacon is chirping with Eddystone-UID profile, Cisco CMX displays the properties such as Namespace and Instance-Id.

- If the beacon is chirping with Eddystone-URL profile, Cisco CMX displays the HTTP resource URL being broadcasted by that beacon.

- **Tags**—Click the **Tags** ✎ icon to show or hide Wi-Fi tags. The vendor specific information related to the tags are displayed in raw format.

- **Filters**—Click the **Filters** ▽ icon to filter the display of devices based on parameters such as Connection Status, Manufacturer, and Service Set Identifier (SSID).

- **Inclusion & Exclusion Regions**—Click the **Inclusion & Exclusion Regions** ▦ icon to view the inclusion and exclusion regions on a floor. The inclusion and exclusion regions are created in Cisco Prime Infrastructure. In Cisco CMX, you can view these regions, but you cannot modify them. The inclusion regions are shown in green, and the exclusion regions are shown in gray.

- **Thick Walls**—Click the **Thick Walls** icon to view any thick walls that have been created on prime infrastructure and included on the floor. Thick wall improves location by modeling areas of high RF signal attenuation with more accuracy.

- **GPS Markers**—Click the **GPS Markers** to view any GPS markers that are placed on the floor. When at least three GPS markers are placed on a floor, the system can use these to provide GPS co-ordinates, in additional to X, and Y co-ordinates in client location API requests.

Viewing Device Details

Procedure

Step 1	Log in to Cisco Connected Mobile Experiences (Cisco CMX).
Step 2	Click **DETECT & LOCATE**.
Step 3	Using the left pane of the **Activity Map** window, navigate to the desired building and floor.
	The **Activity Map** window displays a list of icons to the right.
Step 4	Click the corresponding icon to show the desired devices, for example, client devices, APs, beacons, and so on.

Step 5   Click the corresponding device on the map.

A pane displaying details of the device, such as MAC address, IP address, status, and so on is displayed.

Customizing Client Refresh Rates

The DETECT & LOCATE service enables you to configure the refresh rate for clients' position on a floor map. The refresh interval can be used to configure how frequently a client's positions will be polled to determine their positions. The default refresh rate is five seconds. The refresh rate gets automatically reset when you navigate to another tab or log in again. The client refresh rates are temporary and is not stored in the CMX.

Procedure

Step 1   Log in to Cisco Connected Mobile Experiences (Cisco CMX) either as an admin user or a user with Location role.

Step 2   Click **DETECT & LOCATE**.

Step 3   Using the left pane of the **Activity Map** window, navigate to the desired building and floor.

The **Activity Map** window displays a list of icons to the right.

Step 4   Click the **Gear** icon to configure the client refresh rate.
A pane indicating the client refresh intervals is displayed.

Step 5   Use the + or - icon to increase or decrease the client refresh rates. The refresh rates are in seconds. The range is one to 30 seconds.

Step 6   Click **OK**.

The client, represented by dots on the map, will be refreshed with the new configured rate.

Customizing Device Views Using Filters

Procedure

Step 1   Log in to Cisco Connected Mobile Experiences (Cisco CMX) either as an admin user or a user with Location role.

Step 2   Click **DETECT & LOCATE**.

Step 3   Using the left pane of the **Activity Map** window, navigate to the desired building and floor.

The **Activity Map** window displays a list of icons to the right.

Step 4   Click the corresponding icon to show the desired devices, for example, client devices, APs, beacons, and so on. The more icons you click, the more filtering options are enabled.

Adding and Deleting Filters

Procedure

Step 1   Log in to Cisco Connected Mobile Experiences (Cisco CMX).

Step 2   Click **DETECT & LOCATE**.

Step 3   Using the left pane of the **Activity Map** window, navigate to the desired building and floor.

The **Activity Map** window displays a list of icons to the right.

Step 4   Click the corresponding icon to show the desired devices, for example, client devices, APs, beacons, and so on. The more icons you click, the more filtering options are enabled.

Step 5   Click the **Filter** ▼ icon.

Step 6   In the **Filters** dialog box that is displayed, you can add or remove client filters based on the following parameters:

- **Connection Status**—Unassociated or Connected

- **Device Manufacturer Type**—Name of the device manufacturer, for example, Apple, Samsung, and so on

- **SSID**—Device's SSID

Searching for a Device

Procedure

Step 1   Log in to Cisco Connected Mobile Experiences (Cisco CMX).

Step 2   Click **DETECT & LOCATE**.

Step 3   Using the left pane of the **Activity Map** window, navigate to the desired building and floor.

Step 4   In the **Search** field of the **Activity Map** window, enter any of the following parameters to search for or filter a desired device:

- **MAC Address**—Enter the corresponding client's MAC address in lowercase, colon delimited, for example, 00:a0:22:bc:e2:00.

- **Device IP Address**—Enter the client's IPv4 or IPv6 address in dotted format, for example, 10.22.12.212.

- **SSID**—Enter the client's SSID in free-form text.

- **Device Manufacturer**—Enter specific manufacturer names, for example, Apple, Samsung, and so on in free-form text.

- **Username**—Enter the client's username in free-form text.

> **Note**   When performing a device search based on MAC address, if a device is not located on the specific floor that you are on, a dialog box is displayed that shows the floor in which the specific device is currently on. In addition, you can search based on MAC address for a specific date.

Client Playback

The Client Playback feature enables you to locate and track the movement of clients in a venue. You can track the activity of one client at a time.

Procedure

Step 1   Log in to Cisco Connected Mobile Experiences (Cisco CMX).

Step 2   Click **DETECT & LOCATE**.

Step 3   Using the left pane of the **Activity Map** window, navigate to the desired building and floor.

Step 4   Search the client you want to track using the its MAC ID.

For more information about how to search client devices, see Searching for a Device, on page 7.

Step 5   Click the **Client Movement History Playback** icon ↺ .

The Client Playback (see the image below) pane is displayed .

Step 6   Click the **Play** icon to start client playback.
You can also change the date in order to view the playback on a specific date, by clicking the **Calendar** icon. You can increase the speed of the playback by clicking the **2x** button.

Data Privacy

In Europe, a new law, General Data Protection Regulation (GDPR) is in force effective May 25, 2018. GDPR intends to strengthen and unify data protection for individuals.

Cisco CMX 10.5 introduces the Data Privacy feature to be compliant with the GDPR requirements. This feature allows Cisco CMX to ensure data protection by not disclosing clients details such as MAC address, username, and IP address.

> **Note**   By default, the Data Privacy feature is disabled.

The Data Privacy feature works with the Mac Hashing **On/Off** options. This feature is applicable only for wireless clients. Other connected devices such as interferers, rogue clients, and RFID and BLE tags are not

affected. If the Data Privacy feature is enabled, Cisco CMX will not process client information such as username, IP address, and manufacturer details.

- **Mac Hashing On**—Cisco CMX hashes MAC address of all the clients. As a customer you need not explicitly opt to record the consent for this action. Active client count on the Cisco CMX Detect and Locate dashboard and Systems Service Dashboard will appear as double the actual number for the initial 5 to 10 minutes when clients already exist. After this duration, the active client count resumes to the correct count.

  If MAC Hashing is on, the MAC addresses of all the clients are hashed on the nmsplb service, and the location computed with the hashed MAC addresses.

- **Mac Hashing Off**—You must enter the MAC address of all the devices that have a location calculated manually to Cisco CMX. Alternatively, Cisco CMX can fetch the details from a CMX Connect interaction where a customer explicitly accepts the **Terms and Conditions** that allow customers' MAC address to have a calculated location associated with them. All Analytics and Connect data is based on the data from MAC addresses in which specific tracking has been enabled. If a customer does not explicitly approve, or a MAC address is not manually entered, Cisco CMX does not record the location of that MAC address.

After enabling Data Privacy, you can choose to perform these tasks:

- Not retain the connect data, and delete all the connect clients data by using the **cmxctl config connect deleteClientsAll** command.

- Delete all the history data by using the **cmxctl config data deleteAll** command. You may have to restart Cisco CMX if you delete history data.

The Data Privacy feature has 4 components:

- **Mac Hashing**—If Mac Hashing is turned on, you must input the SALT value (alphanumeric text used to safeguard passwords in storage) that is being used to anonymize the real MAC addresses. This is referred as current SALT. Cisco CMX uses the SHA1 one-way cryptographic function for MAC hashing. This helps to protect the user identity and the real MAC addresses are not stored in Cisco CMX. The Opt In client list is not checked in this mode and all client devices are tracked.

  You can specify a future date as SALT. Cisco CMX runs a job that checks for the SALT to be applied for that particular day. If a new SALT is available, this is used for MAC hashing. Cisco CMX requires the current SALT if MAC hashing is turned on.

- **Opt In**—This is used to collect user consent. As a Cisco CMX admin, you can decide the way you want to collect the consent. Cisco CMX stores the Location and Analytics consent separately. Also, because the Location service is the single source for Analytics data, devices that have not given consent for Location tracking will not be tracked for Analytics too.

  ✎

  Note   Consent is stored in the database, and unless explicitly removed, will always be available in the system.

- **Data Retention**—This offers a configurable way to retain or purge long-live data such as location history and analytics raw data. When the Data Privacy feature is turned on for the first time, the database contains the real MAC addresses. As an administrator, you can decide to either back up the data and then purge it or directly purge it. Run the **cmxctl config data delete** command to purge this data. Restart the Cisco CMX after purging the data.

• **Disk Encryption**—Cisco CMX 10.5 supports CentOS7. You cannot upgrade to Cisco CMX 10.5.x from releases earlier than Cisco CMX Release 10.5. You must install and depoly the Cisco CMX 10.5.x OVA or ISO file on your system. For more information, see the *Cisco Mobility Services Engine Virtual Appliance Installation Guide for Cisco CMX Release 10.5* at:

https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-installation-guides-list.html

CMX Grouping

The CMX Grouping feature (formerly known as AP Grouping) allows Cisco CMX to form an Access Point (AP) group consisting of all the APs learned from maps.

Note	By default this feature is disabled.

The CMX Grouping feature helps to improve Cisco CMX performance in the following scenarios:

• Cisco CMX learns about the APs from the maps to compute the APs' location. However, in some instances, Cisco CMX will not have all the APs from the controller. In such a scenario, Cisco CMX will have to discard the RSSI probes received from the APs that are not available on maps.

• For Hyperlocation, Cisco CMX supports 1000 APs. Only 1 Cisco CMX with Hyperlocation enabled can be added to the controller. However, a large controller such as a Cisco 8500 Series Wireless Controller, managing 15,000 APs, has a lot to offer.

• Cisco CMX supports the exclusion of probing clients filter. This indicates that Cisco CMX discards the RSSI probes that is used for probing clients. However this filtering adds significant load on Cisco CMX when the probing clients are too many.

In Cisco WLC 8.7 or later, Cisco CMX communicates about the AP group to the controller, and the controller sends NMSP and UDP data for APs participating in the group. In Cisco WLC 8.7 or later, support is added to send only the required NMSP data to Cisco CMX. Note that Cisco CMX can subscribe to NMSP data of specific APs or AP groups based on the active services in Cisco WLC.

The performance of Cisco CMX can be optimized in the following ways:

• Cisco CMX will not receive the NMSP and UDP data for the APs that are not available on maps.

• This helps Cisco CMX to form AP groups uniquely (no AP should be duplicated across AP groups) to receive the Hyperlocation data, which in turn helps leverage Cisco WLC's capacity to full extent.

• When exclude probing client filter is enabled, Cisco WLC 8.7 and later perform filtering and will do not send the NMSP data to Cisco CMX.

For more information on how Cisco WLC supports NMSP by AP Groups, see the "NMSP by AP Groups with Subscription List from CMX" section in the *Cisco Wireless Controller Configuration Guide*.

This figure shows a sample architecture of a Cisco CMX Grouping:

Figure 2: Cisco CMX Grouping
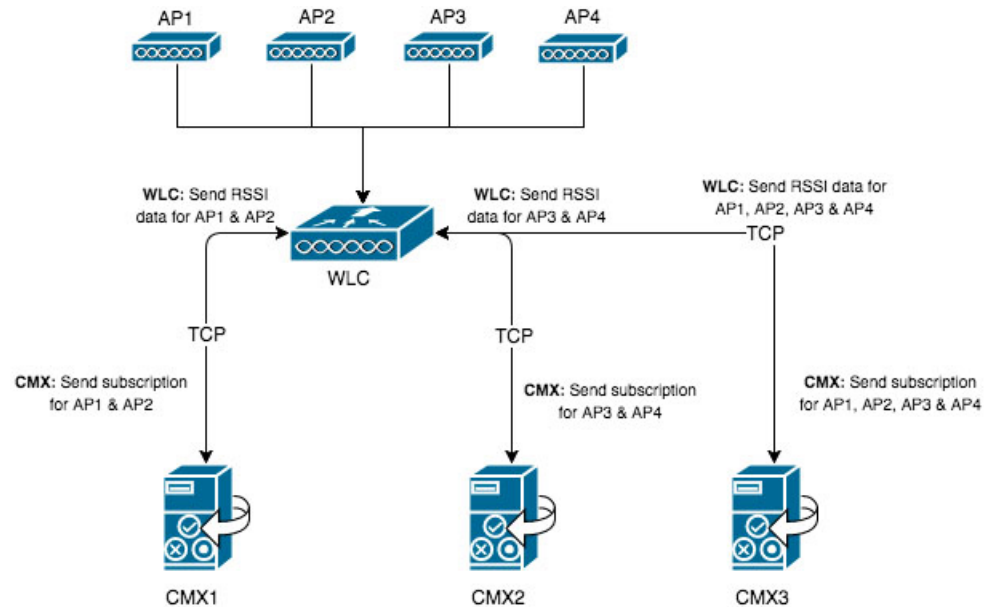
Tip One important requirement for Cisco CMX grouping to work is that AP groups must always contain unique APs. This means that no AP should be repeated across the AP groups. If you have same APs in multiple AP groups, you must correct this error manually.

Note Caveats CSCvj54236 and CSCvi63871 provide information about Cisco WLC 8.7 and 8.7 special have limitations identified with respect to Cisco CMX. Cisco CMX Grouping does not work with hyperlocation deployments because of these limitations.

The CMX Grouping feature only supports wireless clients. Rogue clients are not supported.

Procedure

Step 1 Enable the Cisco CMX Grouping feature by entering this command: **cmxctl config feature flags nmsplb.cmxgrouping true**

Note To disable the feature, run the **cmxctl config feature flags nmsplb.cmxgrouping false** command.

Step 2 Restart Cisco CMX by entering this command: **cmxctl restart agent**

Step 3 Stop the Load Balancer service, used for NMSP messages to Location services by entering this command: **cmxctl nmsplb stop**

Step 4 Restart the Load Balancer service used for NMSP messages by running this command:**cmxctl nmsplb start**

To verfiy if the CMX Grouping feature is enabled, run the **cmxctl config featureflags** command and verify the value for *nmsplb.cmxgrouping*.

In WLC 8.7 and later, run the **show nmsp subscription group detail services** *<ip address> CMX_<ip address>* command to verify the subscription. In the command, replace *<ip address>* with your Cisco CMX IP address.

Enabling Hyperlocation and FastLocate in Cisco CMX

The Cisco Hyperlocation solution is a suite of technologies that enables advanced location capabilities through a mix of software and hardware innovations. Cisco CMX Release 10.2.1 supports the Angle of Arrival (AoA) technology available on Cisco Aironet 3600 and 3700 access points with a Hyperlocation module and a Hyperlocation antenna. Cisco CMX uses advanced location algorithms to extract phase differences to accurately locate associated wireless clients up to one meter accuracy in an optimal deployment.

The Cisco Hyperlocation module with advanced security also integrates Bluetooth Low Energy (BLE) beacons with the module. Customers can take advantage of BLE beacon deployment powered over Ethernet and centrally managed from the convenience of a data center. This eliminates the need for local IT engineers to perform an inspection walk of BLE beacon health, using an app on their Smart devices. Cisco Hyperlocation brings virtual BLE beacon technology so that a single Hyperlocation module appears as five different BLE beacons to consumer applications.

Cisco CMX FastLocate technology enables quick location refresh for connected Wi-Fi clients. RSSI from data packets and probe frames, when available, are used for calculating a location. This technology is available with both centrally switched WLANs and FlexConnect (locally switched WLANs). Cisco Aironet 700, 1700, 2600, 2700, 3600, and 3700 APs support Cisco CMX FastLocate when used with Cisco WLC Release 8.1.123.0 or later.

Accuracy results for the Cisco FastLocate feature are reflected in the Cisco CMX Accuracy Tool under the **50% and 75% Error Distance** columns. Accuracy is considered good if the distance displayed under those columns is 10 meters or less, meaning the client will be detected less than 10 meters from its actual position. For information about configuring Cisco FastLocate, see "FastLocate for Cisco Wave 2 Access Points" section in the *Cisco Wireless Controller Configuration Guide, Release 8.6* at:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-6/config-guide/b_cg86/location_services.html#ID2048

Note
- The above result is only valid for smart devices.

- We recommend that you have all the APs in the same group on a particular floor. If you cannot have APs in the same group, then plan to include nearby APs in the same group. All AP groups available on the same floor must be synchronized to the same NTP server.

- Ensure that you disable the global **Hyperlocation** option and enable **Hyperlocation** option speific for AP group. We recommend that you do not set the XOR radio to monitor mode manually. When you enable Hyperlocation in the AP group, the XOR radio settings are taken care by default.

The following are the recommended AP modes:

- Enhanced Local Mode—APs scan opportunistically on-current channel and off-channel with up to ~15 percent performance impact to data-serving radios.

- Monitor Mode—APs scan on 2.4 and 5 GHz bands.

- Modular Mode—Cisco 3600 and 3700 APs with Hyperlocation Module or Wireless Security Module (WSM) scan on 2.4 and 5 GHz bands with no impact to data-serving radios.

Note

- The FastLocate and Hyperlocation features are supported in Cisco CMX 10.2.1 and later.

- In Cisco CMX Release 10.4, FastLocate feature is supported on Cisco Aironet 2800/3800 access points running Cisco Release 8.6 or later.

- In Cisco CMX Release 10.3.1, the Hyperlocation feature supports 10,000 tracked devices—1000 Cisco access points (APs) with up to 10 connected clients per AP—on Cisco 3365 Mobility Services Engine (MSE) and Cisco high-end MSE Virtual Appliances (v MSE) running Cisco CMX Release 10.3.1 and later.

- The Hyperlocation and FastLocate features are supported in Cisco WLC 8.1.123.0 and later.

- Currently, a Hyperlocation-enabled Cisco WLC can support only one Hyperlocation-enabled Cisco CMX.

- The Hyperlocation feature is not supported on a virtual Cisco WLC.

Procedure

Step 1   Log in to Cisco Connected Mobile Experiences (Cisco CMX).

Step 2   Choose **SYSTEM** > **Dashboard**.

Step 3   Click the **Gear** icon at the top-right corner of the window.
The **SETTINGS** window is displayed.

Step 4   Click the **Location Setup** tab.

Step 5   In the **Location Calculation Parameters** window, check the **Enable Hyperlocation / FastLocate/ BLE Management** check box.

Step 6   Add Cisco WLC to Cisco CMX.

Note   If hyperlocation is enabled and one controller is in active status, and no data is received for almost 15 minutes an alert is generated with the following description "Hyperlocation is enabled on CMX, however no AOA data is received". The alert service type is Hyperlocation and alert type is Service_Status.

As a work around, maintain a one to one mapping between controller and Cisco CMX. Only one controller can serve one Cisco CMX box with hyperlocation enabled. If two hyperlocation enabled Cisco CMX boxes are using the same controller, disable hyperlocation service in one of the Cisco CMX box.

Hyperlocation Mixed Mode Support

Cisco CMX Release 10.4 now supports a mixed deployment of Cisco Hyperlocation access points (AP) and non-Hyperlocation AP on the same floor map. If the client is associted to a regular access point but has a hyperlocation enabled access point near by, AoA computation is performed to provide an an acceptable accuracy. All Cisco Hyperlocation APs must be within a contiguous area. Increased accuracy on the floor is only within the convex hull of the Hyperlocation contiguous are

Hyperlocation groups are formed consisting both hyperlocation and regular access points. The floor mode is decided when generating the hyperlocation group. There following are the three supported modes:

• RSSI mode-All access points on the floor are regular APs.

• Mixed mode: Few APs on the floor are Halo APs.

> **Note** Use the **cmxctl config hyperlocation mixmode***Floor ID* command to enable hyperlocation mixed mode.
>
> We recommend that you use this command in a deployment senario where there are both Hyperlocation enabled APs and non Hyperlocation APs on the same floor map. The improved location accuracy that comes from the use of Hyperlocation AP will occur within the convex hull of the Hyperlocation APs. Outside of this convex standard location accuracy results will occur. At the edges of the convex hull there may also be lower accuracy then when clients are at least 10M inside of the convex hull. This command does not support the interspersion of Hyperlocation AP with non Hyperlocation AP. If this is type of deployment is used, then there will be no improvement in location over standard probe RSSI based location.
>
> An example of an supported deployment is as follows:
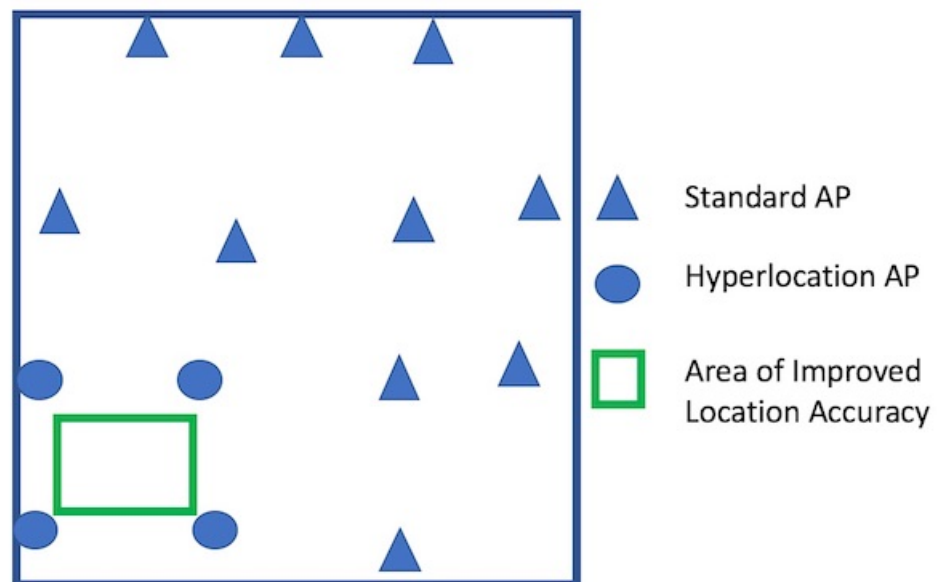
• Halo mode: All APs on the floor are Halo APs.

Running Hyperlocation Diagnostics

Hyperlocation Diagnostics is a tool that can find common issues in a Hyperlocation deployment.

Hyperlocation Diagnostics executes a set of tests to verify any common issues with Hyperlocation. These tests are executed against an existing Hyperlocation setup on a floor. The floor should have clients associated to Hyperlocation access points to validate complete functionality.

Procedure

Step 1   Log in to Cisco Connected Mobile Experiences (Cisco CMX) either as an admin user or a user with Location role.

Step 2   Choose **DETECT & LOCATE** > **Troubleshooting**.

The **Hyperlocation Diagnostics** window is displayed. As this is a floor-level test, select a building and floor. Note that only floors with hyperlocation access points are populated here.

Step 3   (Optional) Add the details and credentials of a controller and an access point for a more detailed report.

Step 4 Click **Run Diagnostics** and wait for a few minutes.

a) Click the **Troubleshooting guide** for a detailed description of each test.

TROUBLESHOOTING GLOSSARY

Close window ×

1) Check Hyperlocation calculation is enabled on CMX ▾

2) Check Hyperlocation enabled on wireless LAN controller ▾

3) Check wireless LAN controller AP radios are installed properly ▾

4) Check wireless LAN controller AP radios are operating properly ▾

5) Check wireless LAN controller added to CMX ▾

6) Check NMSP connection on wireless LAN controller ▾

7) Check NTP configuration on CMX ▾

8) Check NTP configuration on wireless LAN controller ▾

9) Check AP has correct time configuration ▾

10) Check CMX and wireless LAN controller time difference ▾

11) Check map has Hyperlocation APs ▾

12) Check for missing Hyperlocation APs ▾

Step 5   Observe a sample test result. The Test Type indicates which deployment component is being tested, and it can be CMX, WLC, or AP.

Test No	Test Type	Test Name	Results	Actions
1)	CMX	Check Hyperlocation calculation is enabled on CMX	Passed ▾	
2)	WLC	Check Hyperlocation enabled on wireless LAN controller	Passed ▾	
3)	WLC	Check wireless LAN controller AP radios are installed properly	Failed ▾	Fix Issue
4)	WLC	Check wireless LAN controller AP radios are operating properly	Passed ▾	
5)	CMX	Check wireless LAN controller added to CMX	Passed ▾	
6)	WLC	Check NMSP connection on wireless LAN controller	Passed ▾	
7)	CMX	Check NTP configuration on CMX	Failed ▾	Fix Issue
8)	WLC	Check NTP configuration on wireless LAN controller	Passed ▾	
9)	AP	Check AP has correct time configuration	Passed ▾	
10)	WLC	Check CMX and wireless LAN controller time difference	Passed ▾	

Step 6   If a test has failed, click **Fix Issue** for instructions on how to resolve the issue.

> Close window ▾
>
> **Test:** Check wireless LAN controller AP radios are installed properly
>
> **Test Description:**
> Check wireless LAN controller AP radios are installed properly
>
> **How to fix this issue:**
>
> 1. Restart the access point
>
> 2. Restart the NMSPLB service

Step 7   Expand a passed test result to see further details of the test.

| 1) | CMX | Check Hyperlocation calculation is enabled on CMX | Passed ▾ |
| 2) | WLC | Check Hyperlocation enabled on wireless LAN controller | Passed ▾ |

Hyperlocation is enabled on the wireless LAN controller

```
show advanced hyperlocation summary
Hyperlocation.................................. UP
Hyperlocation NTP Server......................... 10.22.243.24
Hyperlocation pak-rssi Threshold................. -90
Hyperlocation pak-rssi Trigger-Threshold......... 3
Hyperlocation pak-rssi Reset-Threshold........... 1
Hyperlocation pak-rssi Timeout................... 3
AP Name Ethernet MAC Slots Hyperlocation
---------------- -------------------- ------- ------------
CMX-AP02-6509.8990 3c:08:f6:d9:08:a0 3 UP
CMX-AP06-6193.96e4 b8:38:61:a8:ba:a0 3 UP
CMX-AP01-6193.9720 b8:38:61:a8:bc:60 3 UP
CMX-AP04-61a6.84ac b8:38:61:b1:c8:d0 3 UP
CMX-AP05-61af.42c4 b8:38:61:b4:53:60 3 UP
CMX-AP03-61af.42cc b8:38:61:b4:53:70 3 UP
```

| 3) | WLC | Check wireless LAN controller AP radios are installed properly | Failed ▾ | Fix Issue |

Step 8   If the **Check AoA messages increasing for access points** test has failed, expand the test.

This may happen if there aren't clients to communicate with the access point, and hence the message count does not increase.

1)	CMX	Check Hyperlocation calculation is enabled on CMX	Passed ▾

2)	WLC	Check Hyperlocation enabled on wireless LAN controller	Passed ▾

Hyperlocation is enabled on the wireless LAN controller

```
show advanced hyperlocation summary
Hyperlocation..................................... UP
Hyperlocation NTP Server......................... 10.22.243.24
Hyperlocation pak-rssi Threshold................. -90
Hyperlocation pak-rssi Trigger-Threshold......... 3
Hyperlocation pak-rssi Reset-Threshold........... 1
Hyperlocation pak-rssi Timeout................... 3
AP Name Ethernet MAC Slots Hyperlocation
---------------- -------------------- ------- ------------
CMX-AP02-6509.8990 3c:08:f6:d9:08:a0 3 UP
CMX-AP06-6193.96e4 b8:38:61:a8:ba:a0 3 UP
CMX-AP01-6193.9720 b8:38:61:a8:bc:60 3 UP
CMX-AP04-61a6.84ac b8:38:61:b1:c8:d0 3 UP
CMX-AP05-61af.42c4 b8:38:61:b4:53:60 3 UP
CMX-AP03-61af.42cc b8:38:61:b4:53:70 3 UP
```

3)	WLC	Check wireless LAN controller AP radios are installed properly	Failed ▾	Fix Issue

a) Expand the test for a further look, and ensure that there is a significant difference for the first and second reading for access points that are connected to clients.

18)	CMX	Check AoA messages are increasing for access points	Passed ▾

All access points have increasing AoA messages

AP Name	AP MAC	AP IP	Result
CMX-AP01-6193.9720	b8:38:61:a8:bc:60	10.22.243.128	Message count is increasing
CMX-AP02-6509.8990	3c:08:f6:d9:08:a0	10.22.243.164	Message count is increasing
CMX-AP03-61af.42cc	b8:38:61:b4:53:70	10.22.243.113	Message count is increasing
CMX-AP04-61a6.84ac	b8:38:61:b1:c8:d0	10.22.243.123	Message count is increasing
CMX-AP05-61af.42c4	b8:38:61:b4:53:60	10.22.243.141	Message count is increasing
CMX-AP06-6193.96e4	b8:38:61:a8:ba:a0	10.22.243.126	Message count is increasing

Message count for AP-CMX-AP01-6193.9720

Message count for first reading 1700336

Message count after 10 second interval 1700348

Message count for AP-CMX-AP02-6509.8990

Message count for first reading 1706098

Message count after 10 second interval 1706110

Message count for AP-CMX-AP03-61af.42cc

| 3) | WLC | Check wireless LAN controller AP radios are installed properly | Indeterminate ▾ | Fix Issue |

Wireless LAN controller credentials were not provided. The test can be run manually.

1. On the wireless controller run the command 'show ap module summary all'
2. Check each Hyperlocation access point for the module 'Hyperlocation Module w/Antenna'

If you haven't provided the optional controller and access point details, the corresponding tests will not be executed, and the result is marked INDETERMINATE for your reference.

Configure Hyperlocation Groupings

The Hyperlocation deployment calculates location in the following manner. During the time period of a slot, the respective master emits bar packets. Bar responses are sent by client devices in the vicinity. The slaves access point listen to these response packets. The master and slaves then use the collected information to calculate the location of a client, as a collective activity. This process is repeated, with the master and slaves of the next slot. If a floor is too large, there maybe more than one masters. The master and slaves form groups, and a floor may have more than one such group.

Procedure

Step 1   Open the CMX Dashboard, **Detect and Locate>Troubleshooting**. As this is a floor-level test, select a building and floor. Note that only floors with hyperlocation access points are populated here.

Step 2   Click **View Hyperlocation Groupings** to configure a different master for a slot.

Note   You can observe that each slot has an allocated time which is listed below the slot. There are also two frequency bands, 2.4 and 5 GHz, each with scan times. Scan time is the total time allocated to scan every slot of a band at least once. Since there are two such bands, 2.4 and 5 GHz, the total Refresh time is the sum of these two, and is the time taken to scan all slots of all bands.

Location (Please select building & floor)

Nortech-1[6] ⬍   1st Floor [6 APs] ⬍

Please Provide Controller Credentials:

Credentials are optional. Tests requiring credentials will be skipped if not provided.
Controller IP: **10.22.243.56**
(Credentials are not saved and only used during diagnostics)

username   password   SSH ⬍   Verify Credentials

Please Provide Access Point Credentials:

(These credentials will be applicable for all APs of the floor)

username   password   SSH ⬍   Verify Credentials

Run Diagnostics   View Hyperlocation Groupings

Step 3 Click a frequency band, and select a slot. You can observe the master access point for the site marked by M, and the slaves marked by S. You can also change the master to a more appropriate one in this page.

Step 4 Observe details of the master access point of a slot, like bandwidth, channel and client count.

Step 5 Observe the distance of a slave AP from the respective master.

Step 6   Observe that each slot has an allocated time which is listed below the slot. There are also two frequency bands, 2.4 and 5 GHz, each with scan times. Scan time is the total time allocated to scan every slot of a band at least once. Since there are two such bands, 2.4 and 5 GHz, the total Refresh time is the sum of these two, and is the time taken to scan all slots of all bands.

Controlling the Probing Client Expiry Time

Probing clients count is usually more visible on CMX than compared to Wireless LAN Controller (WLC). WLC tracks the clients until the client no longer probes for more than five minutes, whereas CMX maintains the probing client for 10 minutes.

Connected Clients do not have this behavior because, WLC notifies CMX when the clients are disconnected from the network. You can perform additional configuration changes on CMX, if you want to minimize the probing client count on CMX.

⚠️

Caution   We do not recommend to set the value less than five minutes because some clients may not sent probe and in that case CMX will lose such clients. This configuration change could also increase the Analytics service processing time.

Procedure

Step 1	Log in to Cisco Connected Mobile Experiences (Cisco CMX).
Step 2	Click **DETECT & LOCATE**.
Step 3	Choose **SYSTEM > Settings > Filtering**.
Step 4	Specify the **RSSI Cutoff** value as -75.

> **Note**   Setting the RSSI cutoff to -75 affects the probing clients only. This allows Cisco CMX to filter out weak probing clients in the initial stage.

Step 5	Navigate to **/opt/cmx/etc/** and open the **node.conf** file.
Step 6	To set the expiry time, at the end of the Location Services section, add **user_options=-Dredis_ttl=5**.

> **Note**   Cisco CMX maintains the default age out for clients as 10 minutes and when the client leaves the network, CMX usually takes 10 to 15 minutes to clean up the stale client details. If you set the age out to five minutes, Cisco CMX will perform the clean up in five to 10 minutes. Together, the RSSI cutoff and age-out settings, help Cisco CMX to narrow down the probing client count with respect to the WLC count.

Step 7	To restart the CMX agent, run the command **cmxctl agent restart**.
Step 8	To restart the Location Services, run the command **cmxctl location restart**.

Supported Access Points for Cisco CMX 10.5 Location Features with Cisco WLC 8.7

The following table lists the Cisco CMX 10.5 Location features and the APs that support these features:

Table 1: Supported Access Points

Location Feature	Supported Marvel-Based Cheetah Access Points	Supported Cisco IOS Access Points (2700, 3700, 3600)
FastLocate	2800, 3800	2700, 3700, 3600
Hyperlocation	4800	3602E and 3702E with HALO radio module 3010 (RM3010L)
Hyperlocation Mix mode	HALO (3602E and 3702E with HALO radio module 3010 - RM 3010L) and non-HALO (all Cisco IOS)	
Tuna antenna support	Not supported	3602E, 3702E

Location Feature	Supported Marvel-Based Cheetah Access Points	Supported Cisco IOS Access Points (2700, 3700, 3600)
BLE	Integrated BLE: 1800, 1810, 1815, AP1542 (Outdoor) 5 dynamic beacons for AP 4800. Floor beacons are available as beta version only.	Not supported

Measuring Client Location Accuracy Using the Location Accuracy Test

From Cisco CMX 10.2, you can perform a location accuracy test for a single device with multiple location points. You can use the Location Accuracy Test tool to validate the placement and number of access points to ensure that the CMX deployment is giving the best location accuracy experience. The Location Accuracy tool provides an administrator the ability to quantify the location accuracy for a specific location by using a Wi-FI device to measure the difference between the actual and calculated location of a device

To run a location accuracy test, perform the following task:

Procedure

Step 1   Log in to Cisco Connected Mobile Experiences (Cisco CMX).

Step 2   Click **DETECT & LOCATE**.

Step 3   Using the left pane of the **Activity Map** window, navigate to the desired building and floor.

Step 4   Use the search option on the **Activity Map** window to search for a device, for example, Client, RFID Tag, or BLE Tag. In this task, we will choose a client.

Step 5   Click the corresponding connected client, indicated by a green dot.

The **Client** dialog box is displayed.

Step 6   Click the **LOCATION ACCURACY TEST** ⚲ icon to start the location accuracy test.

Step 7   In the **Enter a test name** text box, type a name for the location accuracy test, and then press the **Enter**.

A dialog box, asking you to place the ⚲ marker at the client device's actual position on the map, is displayed.

Step 8   Drag the marker to the correct position.
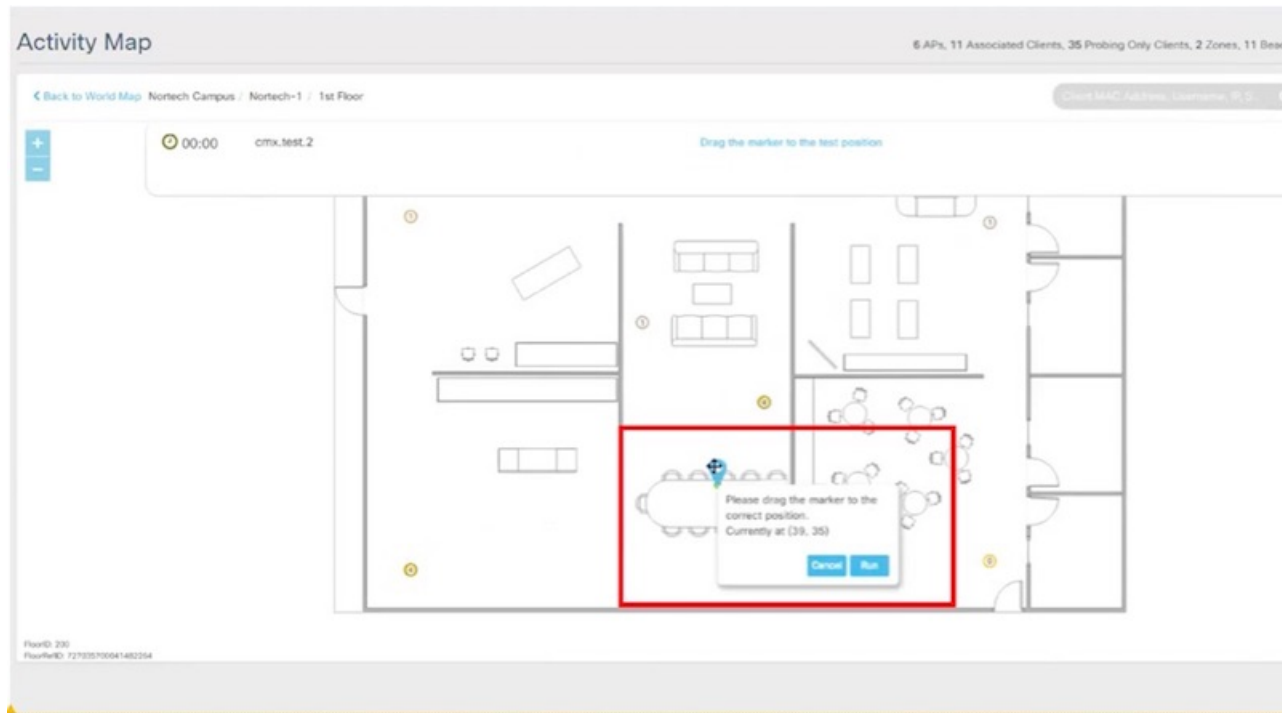
Step 9 Click **Run**.

Observe the increasing samples. This indicates the number of times the client is detected at the pin-pointed location. You can run the test for any required amount of time. The elapsed time of the test is displayed.

Step 10 Refresh your client frequently so that it exchanges information with the access points around it.

Step 11 Click **Pause** when you finish testing of the current location.

You can move your device to another location and continue testing (repeat Step 8 through Step 10). Wait for 30 seconds before resuming the test at a new spot, to eliminate any movement related discrepancies in the test result. Try to collect at least twenty samples at each spot, running the test at a spot for around five minutes.

Step 12 After you complete testing all the location points, click **Finished? View Result** to fetch the test results.

A dialog box, showing 10 m accuracy and Average Error Distance is displayed.
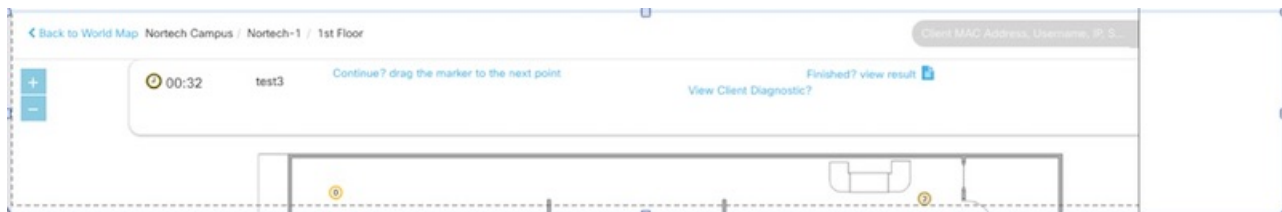
Step 13   Click **View accuracy test report** ⬛ icon on the top-right corner of the window to view the list of accuracy tests that you performed. This report enables you to restart a test, download the latest log or all logs, or email the test results.

The Location Accuracy Test window is displayed with the test details such as test name, status, MAC address, floor, start time, location computation frequency, measurements on correct floor (in percentage), accuracy and error distance. Click **Export All** to export the test results as CSV files.

Note	Even when the test is in progress, you can click **View accuracy test report** to monitor all the tests. You can pause a running test by clicking **Pause**. You can continue a paused test by clicking **Relaunch**. To finish the test and get the results, click the **Report** icon.
	To remove a report from the test report table, click **Delete**.

The Location Accuracy Test window is displayed. You can view all the previous test results in this window, not restricted to the selected floor, but includes all test runs. You also can download the log files, email the test results, and delete the tests.

Step 14   Analyze the test results.

What to do next

You can also perform the Location Accuracy Test using the Cisco CMX mobile application. The Cisco CMX mobile application complements the Cisco CMX product by providing a set of monitoring and testing tools for CMX deployments. The application enables users to monitor the status of CMX, monitor the number of

devices being tracked, receive alerts, test the location accuracy of the deployment, and test the latency of location updates. For more information, see https://blogs.cisco.com/wireless/introducing-the-cisco-cmx-mobile-app-for-deployment-administrators.

Analyzing Location Accuracy Results

Observe the test results in the figure below.

The test results displayed indicate that for 100% of the time, Cisco CMX locates the client within this many meters from where the client is actually located.

It also indicates that for 50% of the time, Cisco CMX locates the client within this many meters from where the client is actually located. A good location accuracy test result for an RSSI deployment is 10 meters, and 4 to 5 meters for FastLocate.

Observe the complete location-accuracy test below:

Ensure that **Measurements on Correct Floor** should be at 100%. This is an indicator of whether the client has been detected by the access points on the same floor, and not on a different floor. You can delete the test and the corresponding log files using the cross buttons here.

Understanding Client Diagnostics

Client diagnostics is a way to understand whether the tested client is sending messages to Cisco CMX for location-accuracy calculations.You can view Client Diagnostics during the location accuracy test.

Below is a sample test report.

It is best to ensure that all the tests here are in Passed status.

You can also email a summary of the messages to your Technical Support department for troubleshooting. Given below are some of the outputs of individual tests.

Figure 3: Sample Output: Check Client History

Figure 4: Sample Output: Check Heatmaps are generated

Figure 5: Sample Output: Reasons for location failure

Analyzing Location Accuracy Log Files

This task analyzes the Location Accuracy log files stored in `/opt/cmx/srv/location/accuracy`.

Procedure

Step 1   Telnet into the CMX box and navigate to the `/opt/cmx/srv/location/accuracy` directory where location accuracy results are stored by default.

Step 2   Navigate to the folder named after your test.

Step 3   Navigate into the logs folder, where the log files are stored.

Step 4   Use the grep command to find entries with COMPUTE in this log file.

```
cat <filename>.log.temp | grep COMPUTE
```

The following is a sample output that is displayed. You can see new entries added to the log file, while the location-accuracy test is performed. Activate your device to see the addition of fresh entries.

Location Accuracy for Hyperlocation Deployments

You can also run Location accuracy tests to test the efficiency of your hyperlocation deployment. Run the test from the **Map Tab** of **Detect and Locate**. Here are some points that will help improve the test results.

• As samples are collected every 3-5 seconds, set the refresh rate of the dashboard to five minutes before running the test.

- A good location accuracy result for a hyperlocation deployment has an Average Error Distance of around one meter.

- Convex hull is the perimeter formed by drawing lines connecting 3 or more APs in a AP group. Ensure that a test client is within the convex hull of an AP group.

- Do not choose a client that is in a spot between AP groups, our outside the convex hull of AP groups.

- You can use the Location Accuracy test to calculate latency in a Hyperlocation deployment. This is especially useful if you would like to know when clients visit your store in order to send personnel to greet them. You can find the latency by moving a test client, and observing how many seconds it takes for your Cisco CMX location accuracy dashboard to update itself with the new client location. Usually, it takes around 2-3 seconds to update its location. Ideally, latency should not be more than 5 seconds for a hyperlocation deployment.