Context-Aware Planning and Verification

This chapter describes a number of tools and configurations that can be used to enhance the location accuracy of elements (clients, tags, rogue clients, and rogue access points) within an indoor or outdoor area.

Context-Aware Service (CAS) installed on a mobility services engine retrieves location information as well as other contextual information such as temperature and asset availability about a client or tag (Cisco CX version 1 or later) from access points.

Note
Non-Cisco CX tags are not tracked or mapped by Cisco WCS.

Note
Context-Aware Service was previously referred to as Cisco location-based services.

This chapter contains the following sections:

- Planning for Data, Voice, and Location Deployment, page 7-2
- Creating and Applying Calibration Models, page 7-4
- Inspecting Location Readiness and Quality, page 7-9
- Verifying Location Accuracy, page 7-10
- Using Chokepoints to Enhance Tag Location Reporting, page 7-13
- Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting, page 7-19
- Using Tracking Optimized Monitor Mode to Enhance Tag Location Reporting, page 7-22
- Defining Inclusion and Exclusion Regions on a Floor, page 7-23
- Defining a Rail Line on a Floor, page 7-29
- Modifying Context-Aware Service Parameters, page 7-33
- Configuring a Location Template, page 7-49
- Enabling Location Services on Wired Switches and Wired Clients, page 7-52
- Verifying an NMSP Connection to a Mobility Services Engine, page 7-57
Planning for Data, Voice, and Location Deployment

You can calculate the recommended number and location of access points based on the services (data, voice, location, or a combination) that are active.

To calculate the recommended number and placement of access points on a floor, follow these steps:

**Step 1** In Cisco WCS, choose Monitor > Maps.

**Step 2** Click the appropriate map name link in the summary list that appears.

If you selected a building map, select a floor map from the Building View page.

A map appears showing placement of all installed elements (access points, clients, tags) and their received signal strength indicator (RSSI). RSSI is indicated by the colored rings that surround the element. To identify the exact RSSI for that element, refer to the RSSI legend (color bar) at the top of the page.

**Note** Access points, clients, and tags must be selected (check boxes selected) in the Floor Settings pane of the Monitor > Maps page to appear on the map (see Figure 7-1).
Step 3 From the Select a command drop-down list, choose the Planning Mode. Click Go.
A map appears with planning mode options at the top of the page (see Figure 7-2).

Figure 7-2 Planning Mode page

Step 4 Click Add APs.
In the page that appears, drag the dashed rectangle over the map location for which you want to calculate the recommended access points.

Note Adjust the size or placement of the rectangle by selecting the edge of the rectangle and holding down the Shift key. Move the mouse as necessary to outline the targeted location.

Step 5 Select the check box next to the service that will be used on the floor. Options are Data/Coverage (default), Voice, Location, and Location with Monitor Mode APs. Click Calculate.
The recommended number of access points appears.

Note Each service option includes all services that are listed above it. For example, if you select the Location check box, the calculation will consider data/coverage, voice, and location in determining the number of access points required.

Note Recommended calculations assume the need for consistently strong signals. In some cases, fewer access points may be required than recommended.

Step 6 Click Apply to generate a map based on the recommended number of access points and their proposed placement in the selected area.
Creating and Applying Calibration Models

If the provided RF models do not sufficiently characterize your floor layout, you can create and apply a calibration model to your floor that better represents its attenuation characteristics. In environments in which many floors share common attenuation characteristics (such as in a library), you can create one calibration model and apply it to floors with the same physical layout and same deployment.

You can collect data for a calibration using one of two methods:

- Data point collection—Selects calibration points and calculates their coverage area one location at a time.
- Linear point collection—Selects a series of linear paths and then calculates the coverage area as you traverse the path. This approach is generally faster than data point collection. You can also employ data point collection to augment location data missed by the linear paths.

Calibration models can only be applied to clients, rogue clients, and rogue access points. Calibration for tags is done using the Aeroscout System Manager. For more information on tag calibration, see the documentation available at the following URL: http://support.aeroscout.com

A client device that supports both 802.11a/n and 802.11b/g/n radios is recommended in order to expedite the calibration process for both spectrums.

Use a laptop or other wireless device to open a browser to WCS and perform the calibration process.

To create and apply data point and linear calibration models, follow these steps:

Step 1 Choose Monitor > Maps
Step 2 From the Select a command drop-down list, choose RF Calibration Models. Click Go.
Step 3 From the Select a command drop-down list, choose Create New Model. Click Go.
Step 4 Assign a name to the model. Click OK.

The new model appears along with the other RF calibration models, but its status is listed as Not Yet Calibrated.
**Step 5** To start the calibration process, click the **model name** link. A new page appears which showing the details of the new model (see Figure 7-3).

*Figure 7-3  New Calibration Model Details page*

![New Calibration Model Details page](image)

*Note* In this page, you can rename and delete the calibration model by choosing the proper option from the Select a command list. When renaming the model, enter the new name before selecting Rename Model.

**Step 6** From the Select a command drop-down list, choose **Add Data Points** and click **Go**.

**Step 7** If you are performing this process from a mobile device connected to WCS through the Cisco Centralized architecture, the MAC address text box is automatically populated with the address of the device. Otherwise, you can manually enter the MAC address of the device you are using to perform the calibration. MAC addresses that are manually entered must be delimited with colons (such as FF:FF:FF:FF:FF:FF).

*Note* Use only associated clients to collect calibration data.

**Step 8** Choose the appropriate campus, building, and floor where the calibration is to be performed (see Figure 7-4). Click **Next**.
Step 9  When the chosen floor map and access point locations appear, a grid of plus marks (+) indicates the locations where data is collected for calibration.

Using these locations as guidelines, you can perform either a point or linear data collection by appropriate placement of either the Calibration Point pop-up (point) or the Start and Finish pop-ups (linear) that appear on the map when the respective options appear. Figure 7-5 shows the starting page for a point calibration.

Figure 7-5  Positioning Calibration Points

a. To perform a point collection, follow these steps:
   1. From the Collection Method drop-down list, choose **Point** and select the **Show Data Points** check box if not already selected. A calibration point pop-up appears on the map.
   2. Position the tip of the calibration point pop-up at a data point (+) and click **Go**. A panel appears showing the progress of the data collection.
3. When the data collection is complete for a selected data point and the coverage area is plotted on the map, move the calibration point pop-up to another data point and click Go.

Note: The coverage area plotted on the map is color coded and corresponds with the specific wireless LAN standard used to collect that data (see the left pane). Additionally, the progress of the calibration process is indicated by two status bars above the legend, one for 802.11a/n and one for 802.11b/g/n.

Note: To delete data points, click Delete and move the black square that appears over the appropriate data points. Resize the square as necessary by pressing Ctrl and moving the mouse.

4. Repeat steps a1 to a3 until the calibrations status bar of the relevant spectrums (802.11a/n, 802.11b/g/n) display as done.

Note: The calibration status bar indicates data collection for the calibration as done, after at least 50 distinct locations and 150 measurements have been gathered. For every location point saved in the calibration process, more than one data point is gathered. The progress of the calibration process is indicated by two status bars above the legend, one for 802.11b/g/n and one for 802.11a/n.

b. To do a linear collection, follow these steps:

1. From the Collection Method drop-down list, choose Linear and select the Show Data points check box if not already selected. A line appears on the map with both Start and Finish pop-ups (see Figure 7-6).

2. Position the tip of the Start pop-up at the starting data point.

3. Position the Finish pop-up at the ending data point.

4. Position yourself with your laptop at the starting data point and click Go. Walk steadily towards the end point along the defined path. The left pane appears indicating data collection is in progress.

Note: Do not stop data collection until you reach the end point even if the data collection bar indicates completion.

5. Press the space bar (or Done on the data collection panel) when you reach the end point. The collection panel displays the number of samples taken before it closes to reveal the map. The map displays all the coverage areas where data was collected. (see Figure 7-6).

Note: To delete data points selected in error, click Delete and move the black square that appears over the appropriate data points. Resize the square as necessary by pressing Ctrl and moving the mouse.
Creating and Applying Calibration Models

### Step 10
To calibrate the data points, click the name of the calibration model at the top of the page. The main page for that model appears.

### Step 11
From the Select a command drop-down list, choose **Calibrate** and click **Go**.

### Step 12
Click **Inspect Location Quality** when calibration completes. A map appears showing RSSI readings.

### Step 13
To use the newly created calibration model, you must apply the model to the floor on which it was created (and on any other floors with similar attenuation characteristics). Navigate to **Monitor > Maps** and find the floor. At the floor map interface, choose **Edit Floor Area** from the drop-down list and click **Go**.

### Step 14
From the **Floor Type (RF Model)** drop-down list, choose the newly created calibration model. Click **OK** to apply the model to the floor.

---

**Note**
This process can be repeated for as many models and floors as needed. After a model is applied to a floor, all locations are determined using the specific collected attenuation data from the calibration model.

---

**Figure 7-6 Linear Data Collection**

The coverage area is color-coded and corresponds with the specific wireless LAN standard (802.11a/n, 802.11b/g/n, or 802.11a/b/g/n) used to collect that data (See legend in the left pane).

6. Repeat Steps b2 to b5 until the status bar for the respective spectrum is complete.

**Note**
You can augment linear collection with data point collection to address missed coverage areas. Refer to **Step 9 a.**
Note
It is generally observed that the point calibration gives more accurate calibration than line calibration.

Inspecting Location Readiness and Quality

You can configure WCS to verify the ability of an existing access point deployment to estimate the true location of a client, rogue client, rogue access point, or tag within 7 meters at least 90% of the time. Location readiness calculation is determined by the number and placement of access points.

Using data points gathered during a physical inspection and calibration you can verify that a location meets the location specification (7 meters, 90%).

This section consists of the following topics:
- Inspecting Location Readiness Using Access Point Data, page 7-9
- Inspecting Location Quality Using Calibration Data, page 7-10

Inspecting Location Readiness Using Access Point Data

To inspect location readiness using access point data, follow these steps:

**Step 1** In Cisco WCS, choose Monitor > Maps.

**Step 2** Click the appropriate floor location link from the list.
A map appears showing placement of all installed access points, clients, and tags and their relative signal strength.

**Note** If RSSI is not displayed, you can enable AP Heatmaps in the Floor Settings pane.

**Note** If clients, 802.11 tags, access points, and interferers are not displayed, verify that their respective check boxes are selected in the Floor Settings panel. Additionally, licenses for both clients and tags must be purchased for each of them to be tracked. For more information, see the Cisco 3300 Series Mobility Services Engine Licensing and Ordering Guide at the following URL: http://www.cisco.com/en/US/products/ps9742/products_data_sheets_list.html

**Note** Refer to Chapter 2, “Adding and Deleting Mobility Services Engines and Licenses,” for details on installing client and tag licenses.

**Step 3** From the Select a command drop-down list, choose Inspect Location Readiness and click Go.
A color-coded map appears showing those areas that do (Yes) and do not (No) meet the 10 meter, 90% location specification.
Inspecting Location Quality Using Calibration Data

After completing a calibration model based on data points generated during a physical tour of the area, you can inspect the location quality of the access points. To inspect location quality based on calibration, follow these steps:

---

**Step 1**
In Cisco WCS, choose **Monitor > Maps**.

**Step 2**
From the Select a command drop-down list, choose **RF Calibration Model** Click **Go**.

A list of defined calibration models appears.

**Step 3**
Click the appropriate calibration model. Details on the calibration including date of last calibration, number of data points by signal type (802.11a, 802.11 b/g) used in the calibration, location, and coverage are displayed.

**Step 4**
In the same page, click the **Inspect Location Quality** link found under the Calibration Floors heading. A color-coded map noting percentage of location errors appears.

---

**Note**
You can modify the distance selected to see the effect on the location errors.

---

Verifying Location Accuracy

By verifying for location accuracy, you are ensuring that the existing access point deployment can estimate the location accuracy of the deployment.

You can analyze the location accuracy of non-rogue and rogue clients, asset tags, and interferers by using the Accuracy Tool. The Accuracy Tool enables you to run either a scheduled or on-demand location accuracy test. Both tests are configured and executed through a single window.

Using the Location Accuracy Tool to Test Location Accuracy

There are two ways to test location accuracy:

- **Scheduled Accuracy Testing**–Employed when clients and tags are already deployed and associated to the wireless LAN infrastructure. Scheduled tests can be configured and saved when clients and tags are already pre-positioned so that the test can be run on a regularly scheduled basis.

- **On-Demand Accuracy Testing**–Employed when elements are associated but not pre-positioned. On demand testing allows you to test the location accuracy of clients, tags, and interferers at a number of different locations. It is generally used to test the location accuracy for a small number of clients, tags and interferers.

Both are configured and executed through a single window.

This section consists of the following topics:

- **Using Scheduled Accuracy Testing to Verify Accuracy of Current Location**, page 7-11
- **Using On-Demand Location Accuracy Testing**, page 7-12
Verifying Location Accuracy

Using Scheduled Accuracy Testing to Verify Accuracy of Current Location

To configure a scheduled accuracy test, follow these steps:

**Step 1** Choose Tools > Location Accuracy Tool.

**Step 2** From the Select a command drop-down list, choose New Scheduled Accuracy Test.

**Step 3** Enter a test name.

**Step 4** Select an area type from the drop-down list.

**Step 5** Campus is configured as system campus by default. There is no need to change this setting.

**Step 6** Select the building from the drop-down list.

**Step 7** Select the floor from the drop-down list.

**Step 8** Select the begin and end time of the test by entering the days, hours, and minutes. Hours are represented using a 24-hour clock.

**Note** When entering the test start time, be sure to allow enough time to position testpoints on the map prior to the test start.

**Step 9** Select the destination point for the test results. You can have the report emailed to you or you can download the test results from the Accuracy Tests > Results page. Reports are in PDF format.

**Note** If you select the email option, a SMTP Mail Server must first be defined for the target email address. Choose Administrator > Settings > Mail Server Configuration to enter the appropriate information.

**Step 10** Click Position Testpoints. The floor map appears with a list of all clients and tags on that floor with their MAC addresses.

**Step 11** Select the check box next to each client and tag for which you want to check the location accuracy.

When you select the MAC address check box for a client or tag, two overlapping icons appear on the map for that element.

One icon represents the actual location and the other the reported location.

**Note** To enter a MAC address for a client or tag that is not listed, select the Add New MAC check box and enter the MAC address and click Go. An icon for the element appears on the map. If the newly added element is on the mobility services engine but on a different floor, the icon appears in the left corner (0,0) position.

**Step 12** If the actual location for an element is not the same as the reported location, drag the actual location icon for that element to the correct position on the map.

**Note** Only the actual location icon can be dragged.

**Step 13** Click Save when all elements are positioned. A panel appears confirming successful accuracy testing.

**Step 14** Click OK to close the confirmation panel. You are returned to the Accuracy Tests summary page.
Verifying Location Accuracy

Note
The accuracy test status appears as Scheduled when the test is about to execute. A status of In Progress appears when the test is running and Idle when the test is complete. A Failure status appears when the test is not successful.

Step 15
To view the results of the location accuracy test, click Test name and then click Download on the page that appears.

The Scheduled Location Accuracy Report includes the following information:
- A summary location accuracy report that details the percentage of elements that fell within various error ranges
- An error distance histogram
- A cumulative error distribution graph
- An error distance over time graph
- A summary by each MAC address whose location accuracy was tested noting its actual location, error distance and a map showing its spatial accuracy (actual vs. calculated location) and error distance over time for each MAC.

Using On-Demand Location Accuracy Testing

An on-demand accuracy test is run when elements are associated but not pre-positioned. On-demand testing allows you to test the location accuracy of clients and tags at a number of different locations. You generally use it to test the location accuracy for a small number of clients and tags.

To run an on-demand accuracy test, follow these steps:

Step 1
Choose Tools > Location Accuracy Tool.

Step 2
From the Select a command drop-down list, choose New On demand Accuracy Test.

Step 3
Enter a test name.

Step 4
Choose the area type from the drop-down list.

Step 5
Campus is configured as system campus by default. There is no need to change this setting.

Step 6
Select the building from the drop-down list.

Step 7
Select the floor from the drop-down list.

Step 8
View test results at the Accuracy Tests > Results page. Reports are in PDF format.

Step 9
Click Position Testpoints. The floor map appears with a red cross hair at the (0,0) coordinate.

Step 10
To test the location accuracy and RSSI of a location, choose either client or tag from the drop-down list on the left. A list of all MAC addresses for the chosen option (client or tag) appear in a drop-down list to its right.

Step 11
Choose a MAC address from the drop-down list, move the red cross hair to a map location, and click the mouse to place it.

Step 12
Click Start to begin collecting accuracy data.

Step 13
Click Stop to finish collecting data. You should allow the test to run for at least two minutes before clicking Stop.
Step 14  Repeat Step 10 to Step 13 for each testpoint that you want to plot on the map.

Step 15  Click Analyze when you are finished mapping the testpoints.

Step 16  Select the Results tab on the page that appears.

The on-demand accuracy report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges
- An error distance histogram
- A cumulative error distribution graph

Step 17  To download accuracy test logs from the Accuracy Tests summary page:

a. Select the listed test check box and choose either Download Logs or Download Logs for Last Run from the Select a command drop-down list.

b. Click Go.

The Download Logs option downloads the logs for all accuracy tests for the selected test(s).

The Download Logs for Last Run option downloads logs for only the most recent test run for the selected test(s).

Using Chokepoints to Enhance Tag Location Reporting

Installing chokepoints (also known as exciters) provides enhanced location information for active RFID tags. When an active Cisco CX version 1 compliant RFID tag enters the range of a chokepoint, it is stimulated by the chokepoint. The MAC address of this chokepoint is then included in the next beacon sent by the stimulated tag. All access points that detect this tag beacon then forward the information to the controller and mobility services engine.

Using chokepoints in conjunction with active Cisco CX compliant tags provides immediate location information on a tag and its asset. When a Cisco CX tag moves out of the range of a chokepoint, its subsequent beacon frames do not contain any identifying chokepoint information. Location determination of the tag defaults to the standard calculation methods based on RSSIs reported by access point associated with the tag.

Note  See the AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine Users Guide for chokepoint installation, configuration, and management details at the following URL: http://support.aeroscout.com

This section consists of the following topics:

- Adding Chokepoints to the WCS, page 7-13
- Removing Chokepoints from WCS, page 7-19

Adding Chokepoints to the WCS

After you install and configure the chokepoint using Aeroscout System Manager, you can add the chokepoint to the mse by positioning it on a WCS map.
To add a chokepoint to WCS, follow these steps:

**Step 1** Choose **Configure > Chokepoints** from the main menu. The Chokepoints summary page appears.

**Step 2** From the Select a command drop-down list, choose **Add Chokepoint** and click **Go**. The Add Chokepoint page appears (see Figure 7-7).

*Figure 7-7 Add Chokepoint Page*

**Step 3** Enter the MAC address, name, coverage range, and static IP address for the chokepoint.

*Note* The chokepoint range is product-specific and is supplied by the chokepoint vendor.

**Step 4** Select the **Entry/Exit Chokepoint** check box if you want the chokepoint to function as a perimeter chokepoint. Its function is to track the entry and exit of clients and tags from an area or floor.

*Tip* You generally enable a chokepoint that is placed near an exit to function as an entry/exit (perimeter) chokepoint. When a client or tag shows strong RSSIs on two floors, you can check for the last perimeter chokepoint that the tag or client passed to determine the current floor location of that client or tag.

**Step 5** Click **OK** to save the chokepoint entry to the database.
The Chokepoints summary page appears with the new chokepoint entry listed (see Figure 7-8).

**Figure 7-8 Chokepoints Summary Page**

![Image of Chokepoints Summary Page]

**Note** After you add the chokepoint to the database, you can place the chokepoint on the appropriate WCS floor map.

**Step 6** To add the chokepoint to a map, choose **Monitor > Maps** (see Figure 7-9).

**Figure 7-9 Monitor > Maps Page**

![Image of Monitor > Maps Page]
Step 7  At the Maps page, select the link (such as Build1 > Floor2) that corresponds to the floor location of the chokepoint. The floor map appears (Figure 7-10).

Figure 7-10 Selected Floor Map Page

![Selected Floor Map Page](image)

Step 8  From the Select a command drop-down list, choose Add Chokepoints and click Go.

The Add Chokepoints summary page appears (see Figure 7-11).

Note  The Add Chokepoints summary page lists all recently added chokepoints that are in the database but not yet mapped.

Figure 7-11 Add Chokepoints Summary Page

![Add Chokepoints Summary Page](image)

Step 9  Select the check box next to the chokepoint to be added to the map. Click OK.

A map appears with a chokepoint icon in the top-left corner. You can now place the chokepoint on the map.
**Step 10** Left-click the chokepoint icon and drag it to the proper location (see Figure 7-12).

*Figure 7-12 Chokepoint Icon is Positioned on the Floor Map*

![Chokepoint Icon Positioned on the Floor Map](image)

*Note* The MAC address, name, and coverage range of the chokepoint appear in the left panel when you click on the chokepoint icon for placement.

**Step 11** Click **Save** when the icon is correctly placed on the map.

The floor map reappears with the added chokepoint (see Figure 7-13).

*Note* If the chokepoint does not appear on the map, select the **Chokepoints** check box in the Floor Settings pane. Do not select **Save Settings** in the Floor Settings pane unless you want to save this display criteria for all maps.
**Figure 7-13  New Chokepoint Displayed on Floor Map**

*Note*  Name, range, entry/exit chokepoint: (*yes or no*), and static IP address of the chokepoint appear when you hover the mouse over its map icon.

*Note*  The rings around the chokepoint icon indicate the coverage area. When a Cisco CX tag and its asset pass within the coverage area, location details are broadcast and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and it is no longer mapped on the chokepoint rings.
Removing Chokepoints from WCS

You can remove one or more chokepoints at a time.

To delete a chokepoint, follow these steps:

**Step 1** Choose Configure > Chokepoints. The Chokepoints page appears.

**Step 2** Select the box next to the chokepoint to be deleted.

**Step 3** From the Select a command drop-down list, choose Remove Chokepoints and click Go (see Figure 7-14).

**Figure 7-14 Removing a Chokepoint**

**Step 4** To confirm chokepoint deletion, click OK in the dialog box that appears.

The Chokepoints page reappears and confirms deletion of the chokepoints. The deleted chokepoints are no longer listed in the page.

Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting

The Wi-Fi TDOA receiver is an external system designed to receive signals transmitted from a tagged, tracked asset. These signals are then forwarded to the mobility services engine for used in calculating location of a tagged asset. TDOA receivers use the Time Difference of Arrival (TDOA) method to calculate tag location. TDOA uses data from a minimum of three TDOA receivers to generate the location of a tagged asset.

**Note**

If a TDOA receiver is not in use, then the location calculations for tags are generated using RSSI readings from access points.

Before using a TDOA receiver within the Cisco Unified Wireless Network, you must:

1. Have a mobility services engine active in the network.
   
   Refer to Chapter 2, “Adding and Deleting Mobility Services Engines and Licenses,” for details on adding a mobility services engine.

2. Add the TDOA receiver to the WCS database and map.
   
   Refer to the “Adding Wi-Fi TDOA Receivers to WCS” section on page 7-20 for details on adding the TDOA receiver to WCS.
3. Synchronize WCS and mobility services engines.
   Refer to Chapter 3, “Synchronizing Mobility Services Engines,” for details on synchronization.

4. Set up the TDOA receiver using the AeroScout System Manager.

   **Note**  See the AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine Users Guide for configuration details at the following URL: http://support.aeroscout.com.

This section consists of the following topics:
- Adding Wi-Fi TDOA Receivers to WCS, page 7-20
- Removing Wi-Fi TDOA Receivers from WCS, page 7-22

### Adding Wi-Fi TDOA Receivers to WCS

After you add TDOA receivers to WCS maps and synchronize, use the AeroScout System Manager application rather than WCS to modify the TDOA receiver configuration.

   **Note** For more details on configuration options, refer to the AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine Users Guide at the following URL: http://support.aeroscout.com.

To add a TDOA receiver to the WCS database and appropriate map, follow these steps:

**Step 1** In WCS, choose **Configure > WiFi TDOA Receivers**. The WiFi TDOA Receivers summary page appears.

**Step 2** From the Select a command drop-down list, choose **Add WiFi TDOA Receivers** and click **Go**.

**Step 3** Enter the MAC Address, Name, and Static IP address of the TDOA receiver.

**Step 4** Click **OK** to save the TDOA receiver entry to the database. The WiFi TDOA Receivers summary page appears with the new TDOA receiver entry listed.

   **Note** After you add the TDOA receiver to the database, you can place the TDOA receiver on the appropriate WCS floor map. To do so, continue with **Step 5**.

**Step 5** To add the TDOA receiver to a map, choose **Monitor > Maps**.

**Step 6** At the Maps page, select the link that corresponds to the floor location of the TDOA receiver. The floor map appears.

**Step 7** Select the **WiFi TDOA Receivers** check box in the Floor Settings pane, if not already selected. This ensures that TDOA receivers display on the map (see Figure 7-15).

   **Note** Click **Save Settings** to display TDOA receivers in all maps (default setting).
Step 8 From the Select a command drop-down list, choose **Add WiFi TDOA receivers** and Click **Go**.
The Add WiFi TDOA Receivers summary page appears.

**Note** The WiFi TDOA Receivers summary page lists all recently added TDOA receivers that are in the database but not yet mapped.

Step 9 Select the check box next to each TDOA receiver to add it to the map. Click **OK**.
A map appears with a TDOA receiver icon in the top-left corner. You are now ready to place the TDOA receiver on the map (see **Figure 7-16**).

**Figure 7-16** Placing WiFi TDOA Receiver on the Map

Step 10 Left click the TDOA receiver icon and drag and place it in the proper location on the floor map.
Using Tracking Optimized Monitor Mode to Enhance Tag Location Reporting

To optimize monitoring and location calculation of tags, you can enable TOMM tracking optimized monitor mode on up to four channels within the 2.4-GHz band (802.11b/g radio) of an access point. This allows you to focus channel scans only on those channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

You must enable monitor mode at the access point level before you can enable TOMM and assign monitoring channels on the 802.11 b/g radio of the access point.

To optimize monitoring and location calculation of tags:
Step 1  Enable monitor mode on the access point, by following these steps:

a. Choose Configure > Access Point > AP Name.
b. Select Monitor as the AP Mode.

Note  For more details, see to the Cisco Wireless Control System Configuration Guide, Release 7.0 at the following URL:

Step 2  Enable TOMM and assign monitoring channels on the access point radio, by following these steps:

a. After enabling monitor mode at the access point level, choose Configure > Access Points.
b. At the Access Points summary page, select the 802.11 b/g Radio link for the access point on which monitor mode is enabled.
c. At the Radio details page, disable Admin Status by unselecting the check box. This disables the radio.
d. Select the Enable TOMM check box.
e. Select up to four channels (Channel 1, Channel 2, Channel 3, Channel 4) on which you want the access point to monitor tags.

Note  You can configure fewer than four channels for monitoring. To eliminate a monitoring channel, choose None from the channel drop-down list.

f. Click Save.
g. At the Radio parameters page, re-enable the radio by selecting the Admin Status check box.
h. Click Save. The access point is now configured as a TOMM access point.

The AP Mode appears as Monitor on the Monitor > Access Points page.

Defining Inclusion and Exclusion Regions on a Floor

To further refine location calculations on a floor, you can define the regions that are included (inclusion areas) in the calculations and those regions that are not included (exclusion regions).

For example, you might want to exclude regions such as an atrium or stairwell within a building but include a work area (such as cubicles, labs, or manufacturing floors).

Note  In WCS, inclusion and exclusion regions are calculated only for clients.

This section consists of the following topics:

- Guidelines, page 7-24
- Defining an Inclusion Region on a Floor, page 7-24
- Defining an Exclusion Region on a Floor, page 7-27
Guidelines

Consider the following when configuring exclusion and inclusion areas:

- Inclusion and exclusion areas can be any polygon shape and must have at least three points.
- You can define only one inclusion region on a floor. By default, an inclusion region is defined for each floor when it is added to WCS. The inclusion region is indicated by a solid aqua line and generally outlines the region.
- You can define multiple exclusion regions on a floor.
- Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.
  
  This might cause some of the devices to be located outside inclusion regions or inside exclusion regions till their location is calculated again.
- You must select the Location Regions option in the Floor Settings pane of the Monitor > Maps page for inclusion and exclusion regions to appear on the map.

Defining an Inclusion Region on a Floor

To define an inclusion region, follow these steps:

**Step 1** Choose Monitor > Maps.

**Step 2** Click the name of the appropriate floor.

**Step 3** From the Select a command drop-down list, choose Map Editor and click Go.

**Step 4** At the map, click the aqua box on the toolbar (see Figure 7-17).

A message box appears reminding you that only one inclusion region can be defined at a time. Defining a new inclusion region automatically removes the previously defined inclusion region. By default, an inclusion region is defined for each floor when it is added to WCS.
Step 5  Click **OK** in the message box that appears. A drawing icon appears to outline the inclusion area.

Step 6  To begin defining the inclusion area, move the drawing icon to a starting point on the map and click once.

Step 7  Move the cursor along the boundary of the area you want to include and click to end a border line. Click again to define the next boundary line.

Step 8  Repeat Step 7 until the area is outlined and then double-click the drawing icon. A solid aqua line defines the inclusion area (see Figure 7-18).
**Defining Inclusion and Exclusion Regions on a Floor**

**Figure 7-18**  
*Inclusion Area Defined*

**Step 9** Choose **Command > Save** or click the disk icon on the toolbar to save the inclusion region.

**Note** If you made an error in defining the inclusion area, click on the area. The selected area is outlined by a dashed aqua line. Next, click on the **X** icon on the toolbar. The area is removed from the floor map.

**Step 10** To return to the floor map to enable inclusion regions on heatmaps, choose **Command > Exit**.

**Step 11** Choose **Monitor > Maps > Floor**.

**Step 12** In the Floor Settings panel, select the **Location Regions** check box if it is not already selected. If you want it to apply to all floor maps, click **Save settings**.

The defined inclusion region appears on the map (see **Figure 7-19**).
To resynchronize the WCS and location databases, choose Services > Synchronize Services.

At the Synchronize WCS and MSE(s) page, select the Network Designs tab and click Synchronize. Look at the Sync. Status column to ensure that the synchronization is successful (two green arrows).

- If the floor was already assigned previously to a mobility services engine, the changes on the floor will be auto synchronized to the mobility services engine.
- For location calculation of an element, the rails and regions will take effect only after the location is recalculated.
- Inclusion region configurations do not apply to tags.

### Defining an Exclusion Region on a Floor

To further refine location calculations on a floor, you can define regions that are excluded (exclusion regions) in the calculations. Exclusion regions are generally defined within the borders of an inclusion region.

- Exclusion region configurations do not apply to tags.

To define an exclusion region, follow these steps:

- **Step 1** Choose Monitor > Maps.
- **Step 2** Click the name of the appropriate floor area.
- **Step 3** From the Select a command drop-down list, choose Map Editor and click Go.
Step 4  
At the map, click the purple box in the toolbar.

Step 5  
Click OK in the message box that appears. A drawing icon appears to outline the exclusion area.

Step 6  
To begin defining the exclusion area, move the drawing icon to the starting point on the map and click once.

Step 7  
Move the drawing icon along the boundary of the area you want to exclude and click once to start a boundary line and click again to end the boundary line.

Step 8  
Repeat Step 7 until the area is outlined and then double-click the drawing icon. The defined exclusion area is shaded in purple, when the area is completely defined. The excluded area is shaded in purple.

Step 9  
To define additional exclusion regions, repeat Step 4 to Step 8 (see Figure 7-20).

Figure 7-20  
Defining Exclusion Areas on Floor Map

To resize based on available browser space click here

Note: Please recomput RF prediction (Command -> Recompute Prediction) when Rails or Regions are modified for WCS Location.

Step 10  
When all exclusion areas are defined, select Save from the Command menu or the disk icon on the toolbar to save the exclusion region.

Note  
To delete an exclusion area, click on the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the X icon in the toolbar. The area is removed from the floor map.

Step 11  
To return to the floor map to enable exclusion regions on heatmaps, select Exit from the Command menu.

Step 12  
At the floor map, select the Location Regions check box if it is not already selected. The exclusion region is shown on the map (see Figure 7-21).
Step 13  To resynchronize the WCS and location databases, choose Services > Synchronize Services.

Step 14  At the Synchronize page, from the Synchronize drop-down list, choose Network Designs and then click Synchronize. View the Sync. Status column to ensure that the synchronization is successful (two green arrows).

**Note**

- Exclusion region auto synchronizes with mobility services engine if the floor was already synchronized to the mobility services engine.
- You can draw multiple exclusion regions within an inclusion region.
- For location calculation of an element, the rails and regions will take effect only after the location is recalculated.

---

### Defining a Rail Line on a Floor

You can define a rail line on a floor (such as a conveyor belt) that indicates an area where clients are expected to be.

**Note**

Rail line configurations do not apply to tags.

Additionally, you can define an area (east and west or north and south) of the rail that expands the area that clients are expected to populate. This expanded area is known as the snap-width and further assists location calculations. Any client located within the snap-width area is plotted on the rail line (majority) or just outside of the snap-width area (minority).

The snap-width area is defined in feet or meters (user-defined).

To define a rail on a floor, follow these steps:

**Step 1**  Choose Monitor > Maps.

**Step 2**  Click on the name of the appropriate floor area.
Step 3  From the Select a command drop-down list, choose Map Editor and click Go.

Step 4  Click the rail icon (to the right of the purple exclusion icon) in the toolbar (see Figure 7-22).

Figure 7-22  Rail Icon on Map Editor Toolbar

![Rail Icon on Map Editor Toolbar](image)

Step 5  In the message dialog that appears, enter a snap-width (feet or meters) for the rail and then click OK (see Figure 7-23).

Figure 7-23  Defining Rail Width

![Defining Rail Width](image)

Step 6  When the drawing icon appears, click the drawing icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.
Step 7  Click the drawing icon twice when the rail line is completely drawn on the floor map. The rail line appears on the map and is bordered on both sides by the defined snap-width region (see Figure 7-24).
Defining Rail Line on a Floor

Figure 7-24  Defining Rail Line in Map Editor

To delete a rail line, click on the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the X icon in the toolbar. The area is removed from the floor map.

**Step 8**  To return to the floor map to enable rails on heatmaps, select **Exit** from the Command menu.

**Step 9**  At the floor map, select the **Rails** check box in the Floor Setting panel if it is not already selected. The rail is shown on the map (see Figure 7-25).
Step 10 To resynchronize the WCS and mobility services engine, choose **Services > Synchronize Services**.

Step 11 At the Synchronize page, from the Synchronize drop-down list, choose **Network Designs** and then click **Synchronize**.

Look at the Sync. Status column to ensure that the synchronization is successful (two green arrows).

**Note**

- Rails auto synchronizes with mobility services engine if the floor was already synchronized to the mobility services engine.
- For location calculation of an element, the rails and regions will take effect only after the location is recalculated.

---

**Modifying Context-Aware Service Parameters**

You can specify the type and number of clients or tags that are tracked and whether or not locations are calculated for those clients or tags.

You can also modify parameters that affect the location calculation of clients and tags such as Receiver Signal Strength Indicator (RSSI) measurements.

**Note**

Licenses are required in order to retrieve contextual information on tags and clients from access points. The license of the client also includes tracking of rogue clients and rogue access points. Licenses for tags and clients are offered independently and are offered in a range of quantities, from 3,000 to 12,000...
units. For more information, see the *Cisco 3300 Series Mobility Services Engine Licensing and Ordering Guide* at the following URL:

This section consists of the following topics:

- Modifying Tracking Parameters, page 7-34
- Modifying Filtering Parameters, page 7-38
- Modifying History Parameters, page 7-41
- Enabling Location Presence, page 7-42
- Importing Asset Information, page 7-43
- Exporting Asset Information, page 7-43
- Modifying Location Parameters, page 7-44

### Modifying Tracking Parameters

The mobility services engine can track up to 18,000 clients (including rogue clients, rogue access points, wired clients, and interferers) and tags (combined count) with the proper license purchase and mobility services engine. Updates on the locations of tags, clients, and interferers being tracked are provided to the mobility services engine from the controller.

**Note**
Cisco 3350 Mobility Services Engine supports up to 18,000 clients and tags and the Cisco 3310 Mobility Services Engine supports up to 2,000 clients and tags.

Only those tags, clients and interferers that the controller is tracking are seen in WCS maps, queries and reports. No events and alarms are collected for non-tracked elements and none are used in calculating the 18,000 element limit for clients or tags.

You can modify the following tracking parameters using WCS:

- Enable and disable wired and wireless client stations, active asset tags, and rogue clients, interferers, and access points whose locations you actively track.
  
  Wired client location tracking enables servers in a data center to more easily find wired clients in the network. Servers are associated with wired switch ports in the network.

- Set limits on how many of a specific element you want to track.
  
  For example, given a client license of 12,000 trackable units, you could set a limit to track only 8,000 client stations (leaving 4,000 units available to allocate between rogue clients and rogue access points). Once the tracking limit is met for a given element, the number of elements not being tracked is summarized on the Tracking Parameters page.

- Disable tracking and reporting of ad hoc rogue clients and access points.

To configure tracking parameters for a mobility services engine, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In Cisco WCS, choose Services &gt; Mobility Services. The Mobility Services page appears.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the name of the mobility services engine whose properties you want to edit. The General Properties page appears.</td>
</tr>
</tbody>
</table>
Step 3  Choose **Context Aware Service > Administration > Tracking Parameters** to display the configuration options (see Figure 7-26).

**Figure 7-26  Context Aware Service > Administration > Tracking Parameters**

Step 4  Modify the tracking parameters as appropriate. Table 7-1 describes each parameter.
### Tracking Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Options</th>
</tr>
</thead>
</table>
| Wired Clients      | 1. Select the **Enable** check box to enable tracking of client stations by the mobility services engine.  
In 7.0, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, and interferers.  
The wired client limiting is supported from mobility services engine 7.0 and WCS 7.0 onwards. In other words, you can limit wired clients to a fixed number, say 500. This limit is set to ensure that the licenses are not taken up completely by wired clients and some licenses are available for wireless clients.  

**Caution**  
When upgrading mobility services engine from 6.0 to 7.0, if any limits have been set on wireless clients or rogues, they will get reset because of the wired client limit change in 7.0.  

**Note**  
Active Value (display only): Indicates the number of wired client stations currently being tracked.  

**Note**  
Not Tracked (display only): Indicates the number of wired client stations beyond the limit. |
| Wireless Clients    | 1. Select the **Enable** check box to enable tracking of client stations by the mobility services engine.  
2. Select the **Enable Limiting** check box to set a limit on the number of client stations to track.  
3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 18,000 which is the maximum number of clients that can be tracked by a mobility services engine.  

**Note**  
The actual number of tracked clients is determined by the license purchased.  

**Note**  
Active Value (display only): Indicates the number of client stations currently being tracked.  

**Note**  
Not Tracked (display only): Indicates the number of client stations beyond the limit. |
Chapter 7      Context-Aware Planning and Verification

Modifying Context-Aware Service Parameters

Table 7-1  Tracking Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue Clients and Access Points</td>
<td>1. Select the Enable check box to enable tracking of rogue clients and asset points by the mobility services engine.</td>
</tr>
<tr>
<td></td>
<td>2. Select the Enable Limiting check box to set a limit on the number of rogue clients and asset tags stations to track.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 18,000 which is the maximum number of rogue clients and access points that can be tracked by a mobility services engine.</td>
</tr>
<tr>
<td>Note</td>
<td>The actual number of tracked rogues (clients and access points) is driven by the client license purchased. The user must consider the number of clients that are being tracked in determining the available quantity to allocate to track rogue clients and access points because clients and rogue clients and access points are addressed by the same license.</td>
</tr>
<tr>
<td>Note</td>
<td>Active Value (display only): Indicates the number of rogue clients and access points currently being tracked.</td>
</tr>
<tr>
<td>Note</td>
<td>Not Tracked (display only): Indicates the number of rogue clients and access points beyond the limit.</td>
</tr>
<tr>
<td>Exclude Ad-Hoc Rogues</td>
<td>Select the check box to turn off the tracking and reporting of ad hoc rogues in the network. As a result, ad hoc rogues are not displayed on WCS maps or its events and alarms reported.</td>
</tr>
<tr>
<td>Interferers</td>
<td>1. Select the Enable check box to enable tracking of the interferers by the mobility services engine.</td>
</tr>
<tr>
<td></td>
<td>In 7.0, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, and interferers.</td>
</tr>
<tr>
<td>Note</td>
<td>Active Value (display only): Indicates the number of interferers currently being tracked.</td>
</tr>
<tr>
<td>Note</td>
<td>Not Tracked (display only): Indicates the number of interferers beyond the limit.</td>
</tr>
<tr>
<td>Asset Tracking Elements</td>
<td></td>
</tr>
<tr>
<td>Active RFID Tags</td>
<td>1. Select the Enable check box to enable tracking of active RFID tags by the mobility services engine.</td>
</tr>
<tr>
<td>Note</td>
<td>The actual number of tracked active RFID tags is determined by the license purchased.</td>
</tr>
<tr>
<td>Note</td>
<td>Active Value (display only): Indicates the number of active RFID tags currently being tracked.</td>
</tr>
<tr>
<td>Note</td>
<td>Not Tracked (display only): Indicates the number of active RFID tags beyond the limit.</td>
</tr>
</tbody>
</table>
Click **Save** to store the new settings in the mobility services engine database.

### Modifying Filtering Parameters

In addition to tracking parameters, you can use filtering to limit the number of clients, asset tags, wired clients, rogue clients, interferers, and access points whose locations are tracked. You can filter by MAC address and probing clients.

- **MAC addresses**
  
  Specific MAC addresses can be entered and labeled as allowed or disallowed from location tracking. You can import a file with the MAC addresses that are to be allowed or disallowed, or you can enter them individually from the WCS GUI window.
The format for entering MAC addresses is xx:xx:xx:xx:xx:xx. If a file of MAC addresses is imported, the file must follow a specific format:

- Each MAC address should be listed on a separate line.
- Allowed MAC addresses must be listed first and preceded by an “[Allowed]” line item. Disallowed MAC addresses must be preceded by “[Disallowed].”
- Wildcard listings can be used to represent a range of MAC addresses. For example, the first entry “00:11:22:33:*” in the Allowed listing below is a wildcard.

Note

Allowed MAC address formats are viewable from the Filtering Parameters configuration page. See Table 7-2 for details.

EXAMPLE file listing:

[Allowed]
00:11:22:33:*
22:cd:34:ae:56:45
02:23:23:34:*
[Disallowed]
00:10:*
ae:bc:de:ea:45:23

- Probing clients

Probing clients are clients that are associated with one controller but whose probing activity enables them to appear to another controller and count as an element for the probed controller as well as its primary controller.

Note

Excluding probing clients can free up the licenses for the associated clients.

To configure filtering parameters for a mobility services engine, follow these steps:

Step 1
In Cisco WCS, choose Services > Mobility Services. The Mobility Services page appears.

Step 2
Click the name of the mobility services engine whose properties you want to edit. The General Properties page appears.

Step 3
Choose Context Aware Service > Administration > Filtering Parameters to display the configuration options.

Step 4
Modify the filtering parameters as appropriate. Table 7-2 describes each parameter.
Chapter 7  Context-Aware Planning and Verification

Modifying Context-Aware Service Parameters

Table 7-2  Filtering Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude Probing Clients</td>
<td>Select the check box to prevent calculating location for probing clients.</td>
</tr>
<tr>
<td>Enable Location MAC Filtering</td>
<td>1. Select the check box to enable filtering of specific elements by their MAC addresses.</td>
</tr>
<tr>
<td></td>
<td>2. To import a file of MAC addresses (Upload a file for Location MAC Filtering text box),</td>
</tr>
<tr>
<td></td>
<td>browse for the file name and click Save to load the file. MAC addresses from the list</td>
</tr>
<tr>
<td></td>
<td>auto-populate the Allowed List and Disallowed List based on their designation in the file.</td>
</tr>
<tr>
<td>Note</td>
<td>To view allowed MAC address formats, click the red question mark next to the Upload a file for Location MAC Filtering text box.</td>
</tr>
<tr>
<td>Note</td>
<td>To add an individual MAC address, enter the MAC addresses (format is xx:xx:xx:xx:xx:xx)</td>
</tr>
<tr>
<td></td>
<td>and click either Allow or Disallow. The address appears in the appropriate column.</td>
</tr>
<tr>
<td>Note</td>
<td>To move an address between the Allow and Disallow columns, highlight the MAC address entry and click the button under the appropriate column.</td>
</tr>
<tr>
<td>Note</td>
<td>To move multiple addresses, click the first MAC address and then press Ctrl and click additional MAC addresses. Click Allow or Disallow to place an address in that column.</td>
</tr>
<tr>
<td>Note</td>
<td>If a MAC address is not listed in the Allow or Disallow column, it appears in the Blocked MACs column by default. If you click the Unblock button, the MAC address automatically moves to the Allow column. You can move it to the Disallow column by clicking the Disallow button under the Allow column.</td>
</tr>
</tbody>
</table>

Step 5  Click Save to store the new settings in the mobility services engine database.
Modifying History Parameters

You can use Cisco WCS to specify how long to store (archive) histories on client stations, asset tags, and rogue clients, wired clients, interferers and access points.

You can also program the mobility services engine to periodically prune (remove) duplicate data from its historical files, which increases the amount of memory available for storing the latest history information. This is important to prevent losing latest history information due to lack of disk space.

To configure mobility services engine history settings, follow these steps:

**Step 1** In Cisco WCS, choose Services > Mobility Services.

**Step 2** Click the name of the mobility services engine whose properties you want to edit.

**Step 3** Choose Context Aware Service > Administration > History Parameters.

**Step 4** Modify the following history parameters as appropriate. Table 7-3 describes each parameter.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive for</td>
<td>Enter the number of days for the location server to retain a history of each enabled category. Default value is 30. Allowed values are from 1 to 365.</td>
</tr>
<tr>
<td>Prune data starting at</td>
<td>Enter the number of hours and minutes at which the location server starts data pruning (between 0 and 23 hours, and between 1 and 59 minutes). Enter the interval in minutes after which data pruning starts again (between 1 and 99900000). Default start time is 23 hours and 50 minutes, and the default interval is 1440 minutes.</td>
</tr>
<tr>
<td>Client Stations</td>
<td>Select the <strong>Enable</strong> check box to turn on historical data collection for client stations.</td>
</tr>
<tr>
<td>Wired Stations</td>
<td>Select the <strong>Enable</strong> check box to turn on historical data collection for wired stations.</td>
</tr>
<tr>
<td>Asset Tags</td>
<td>Select the <strong>Enable</strong> check box to turn on historical data collection.</td>
</tr>
<tr>
<td>Note</td>
<td>Enter the default limits for better performance.</td>
</tr>
<tr>
<td>Rogue Clients and Access Points</td>
<td>Select the <strong>Enable</strong> check box to turn on historical data collection.</td>
</tr>
<tr>
<td>Interferers</td>
<td>Select the <strong>Enable</strong> check box to turn on historical data collection.</td>
</tr>
</tbody>
</table>

**Step 5** Click **Save** to store your selections in the mobility services engine database.
Enabling Location Presence

You can enable location presence on a mobility services engine in order to expand civic (city, state, postal code, country) and geographic (longitude, latitude) location information beyond the Cisco default settings (campus, building, floor, and X, Y coordinates). You can then request this information for wireless and wired clients on demand for use by location-based services and applications.

You can also import advanced location information such as the MAC address of a wired client and the wired switch slot and port to which the wired client is attached.

You can configure location presence when a new campus, building, floor or outdoor area is added or configure it at a later date.

Once enabled, the mobility services engine can provide any requesting Cisco CX v5 client its location.

**Note** For details on configuring location presence when adding a new campus, building, floor, or outdoor area, see the “Creating Maps” section in Chapter 5 of the Cisco Wireless Control System Configuration Guide, release 6.0 and later.

**Note** Before enabling this feature, synchronize the mobility services engine.

To enable and configure location presence on a mobility services engine, follow these steps:

**Step 1** Choose **Services > Mobility Services**. Select the mobility services engine to which the campus or building or floor is assigned.

**Step 2** Choose **Context Aware Service > Administration > Presence Parameters**. The Presence page displays.

**Step 3** Select the **Service Type On Demand** check box to enable location presence for Cisco CX clients v5.

**Step 4** Select one of the following Location Resolution options.

- **a.** When **Building** is selected, the mobility services engine can provide any requesting client its location by building.
  - For example, if a client requests its location and the client is located in Building A, the mobility services engine returns the client address as Building A.

- **b.** When **AP** is selected, the mobility services engine can provide any requesting client its location by its associated access point. The MAC address of the access point appears.
  - For example, if a client requests its location and the client is associated with an access point with a MAC address of 3034:00hh:0adg, the mobility services engine returns the client address of 3034:00hh:0adg.

- **c.** When **X,Y** is selected, the mobility services engine can provide any requesting client its location by its X and Y coordinates.
  - For example, if a client requests its location and the client is located at (50, 200) the mobility services engine returns the client address of 50, 200.

**Step 5** Select any or all of the location formats check boxes.

- **a.** Select the **Cisco** check box to provide location by campus, building, floor, and X and Y coordinates. This is the default setting.
b. Select the **Civic** check box to provide the name and address (street, city, state, postal code, country) of a campus, building, floor, or outdoor area.

c. Select the **GEO** check box to provide the longitude and latitude coordinates.

**Step 6**
By default, the Text check box for Location Response Encoding is selected. It indicates the format of the information when received by the client. There is no need to change this setting.

**Step 7**
Select the **Retransmission Rule Enable** check box to allow the receiving client to retransmit the received information to another party.

**Step 8**
Enter a Retention Expiration value in minutes. This determines how long the received information is stored by the client before it is overwritten. Default value is 24 hours (1440 minutes).

**Step 9**
Click **Save**.

---

**Importing Asset Information**

To import asset, chokepoint, and TDOA receiver information for the mobility services engine using WCS, follow these steps:

**Step 1**
In Cisco WCS, choose **Services > Mobility Services**.

**Step 2**
Click the name of the mobility services engine for which you want to import information.

**Step 3**
Choose **Context Aware Service > Administration > Import Asset Information**.

**Step 4**
Enter the name of the text file or browse for the filename.

Specify information in the imported file in the following formats:
- tag format: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname
- station format: #station, 00:00:00:00:00:00, categoryname, groupname, assetname

**Step 5**
Click **Import**.

---

**Exporting Asset Information**

To export asset, chokepoint, and TDOA receiver information from the mobility services engine to a file using WCS, follow these steps:

**Step 1**
In Cisco WCS, choose **Services > Mobility Services**.

**Step 2**
Click the name of the mobility services engine from which you want export information.

**Step 3**
Choose **Context Aware Service > Administration > Export Asset Information**.

Information in the exported file is in the following formats:
- tag format: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname
- station format: #station, 00:00:00:00:00:00, categoryname, groupname, assetname

**Step 4**
Click **Export**.

**Step 5**
Click **Open** (display to screen), **Save** (to external PC or server), or to **Cancel**.
Modifying Location Parameters

You can use WCS to modify parameters that affect location calculations such as Receiver Signal Strength Indicator (RSSI) measurements for clients.

You can also apply varying smoothing rates to manage location movement of a client.

**Note**
Location parameters apply only to clients.

To configure location parameters, follow these steps:

1. In Cisco WCS, choose Services > Mobility Services.
2. Click the name of the mobility services engine whose properties you want to modify.
3. Choose Context Aware Service > Advanced > Location Parameters. The configuration options appear.
4. Modify the location parameters as appropriate. Table 7-4 describes each parameter.

<table>
<thead>
<tr>
<th>Table 7-4</th>
<th>Location Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Configuration Options</td>
</tr>
</tbody>
</table>
| Calculation time | Select the Enable check box to initiate the calculation of the time required to compute location.  
**Note** This parameter applies only to clients, rogue access points, rogue clients, and interferers.  
**Caution** Enable this parameter only under Cisco TAC personnel guidance because it slows down the overall location calculations. |
| OW Location | Select the Enable check box to include Outer Wall (OW) calculation as part of location calculation.  
**Note** This parameter is ignored by the mobility services engine. |
| Relative discard RSSI time | Enter the number of minutes since the most recent RSSI sample after which RSSI measurement should be considered discarded. For example, if you set this parameter to 3 minutes and the mobility services engine receives two samples at 10 and 12 minutes, it keeps both samples. An additional sample received at 15 minutes is discarded. Default value is 3. Allowed values range from 0 to 99999. A value of less than 3 is not recommended.  
**Note** This parameter applies only to clients, rogue access points, rogue clients, and interferers. |
Chapter 7  Context-Aware Planning and Verification

Modifying Context-Aware Service Parameters

Table 7-4  Location Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absolute discard RSSI time</td>
<td>Enter the number of minutes after which RSSI measurement should be considered stale and discarded, regardless of the most recent sample. Default value is 60. Allowed values range from 0 to 99999. A value of less than 60 is not recommended.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>  This parameter applies only to clients.</td>
</tr>
<tr>
<td>RSSI Cutoff</td>
<td>Enter the RSSI cutoff value, in decibels (dBs) with respect to one (1) mW (dBm), above which the mobility services engine will always use the access point measurement. Default value is –75.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>  When 3 or more measurements are available above the RSSI cutoff value, the mobility services engine will discard any weaker values (lower than RSSI cutoff value) and use the 3 (or more) strongest measurements for calculation; however, when only weak measurements below the RSSI cutoff value are available, those values are used for calculation.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>  This parameter applies only to clients.</td>
</tr>
<tr>
<td>Location Filtering</td>
<td>Location filtering is used to smooth out the jitters in the calculated location. This prevents the located device from jumping between two discrete points on the floor map.</td>
</tr>
<tr>
<td>Chokepoint Usage</td>
<td>Select the Enable check box to enable chokepoints to track Cisco compatible tags.</td>
</tr>
<tr>
<td>Use Chokepoints for Interfloor conflicts</td>
<td>Perimeter chokepoints or weighted location readings can be used to locate Cisco compatible tags.</td>
</tr>
<tr>
<td>Options:</td>
<td>• Never: When selected, perimeter chokepoints are not used to locate Cisco compatible tags.</td>
</tr>
<tr>
<td></td>
<td>• Always: When selected, perimeter points are used to locate Cisco compatible tags.</td>
</tr>
<tr>
<td></td>
<td>• Floor Ambiguity: When selected, both weighted location readings and perimeter chokepoints are used to locate Cisco compatible tags. If similar locations are calculated by the two methods, the perimeter chokepoint value is used by default.</td>
</tr>
<tr>
<td>Chokepoint Out of Range timeout</td>
<td>When a Cisco compatible tag leaves a chokepoint range, the timeout period entered is the period that passes before RSSI values are again used for determining location.</td>
</tr>
<tr>
<td>Absent Data cleanup interval</td>
<td>Enter the number of minutes that data for absent mobile stations is kept. An absent mobile station is one that was discovered but does not appear in the network. Default value is 1440.</td>
</tr>
</tbody>
</table>

**Step 5**  Click Save.
Enabling Notifications and Configuring Notification Parameters

You can use WCS to enable notification and configure notification parameters.

This section consists of the following topics:

- Enabling Notifications, page 7-46
- Configuring Notification Parameters, page 7-46

Enabling Notifications

You can use WCS to define and enable user-configured conditional notifications and northbound notifications.

User-configured conditional notifications manage which notifications the mobility services engine sends to WCS or a third party destination compatible with the mobility services engine notifications. Refer to “Adding, Deleting, and Testing Event Definitions” section on page 6-3.

Northbound notifications define which tag notifications the mobility services engine sends to third-party applications. Client notifications are not forwarded. By enabling northbound notifications in WCS, the following five event notifications are sent: chokepoints, telemetry, emergency, battery, and vendor data. To send a tag location, you must enable that notification separately.

The mobility services engine sends all northbound notifications in a set format. Details are available on the Cisco developers support portal at the following URL: http://developer.cisco.com/web/cdc

Configuring Notification Parameters

You can limit the rate at which a mobility services engine generates notifications, set a maximum queue size for notifications, and set a retry limit for notifications with in a certain period.

Notification parameter settings apply to user-configurable conditional notifications and northbound notifications except as noted in Table 7-5.

Note

Modify notification parameters only when you expect the mobility services engine to send a large number of notifications or when notifications are not being received.

To enable northbound notifications and to configure notification parameters, follow these steps:

Step 1 In Cisco WCS, choose Services > Mobility Services.

Step 2 Click the name of the mobility services engine you want to configure.

Step 3 Choose Context Aware Service > Advanced > Notification Parameters to display the configuration options (see Figure 7-27).
Step 4 Select the **Enable Northbound Notifications** check box to enable the function.

Step 5 Select the **Notification Contents** check box to send notifications to third-party applications (northbound).

Step 6 Select one or more of the following Notification content options:
- Chokepoints
- Telemetry
- Emergency
- Battery Level
- Vendor Data
- Location

Step 7 Select the **Notification Triggers** check box.

Step 8 Select one or more of the following Notification trigger options:
- Chokepoints
- Telemetry
- Emergency
- Battery Level
- Vendor Data
- Location Recalculation

Step 9 Enter the IP address and port for the system that is to receive the northbound notifications.

Step 10 Choose the transport type from the drop-down list.
Step 11  Select HTTPS if you want to use HTTPS protocol for secure access to the destination system.

Step 12  To modify the notification parameter settings, enter the new value in the appropriate text box in the Advanced section of the page. Table 7-5 describes each parameter.

**Table 7-5  User-Configurable Conditional and Northbound Notifications Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Limit</td>
<td>Enter the rate in milliseconds at which the mobility services engine generates notifications. A value of 0 (default) means that the mobility services engine generates notifications as fast as possible (Northbound notifications only).</td>
</tr>
<tr>
<td>Queue Limit</td>
<td>Enter the event queue limit for sending notifications. The mobility services engine drops any event above this limit. Default values: Cisco 3350 (30000), Cisco 3310 (5,000), and Cisco 2710 (10,000).</td>
</tr>
</tbody>
</table>
| Retry Count                   | Enter the number of times to generate an event notification before the refresh time expires. This parameter can be used for asynchronous transport types which do not acknowledge the receipt of the notification and there is a possibility that the notification may be lost in transit. Default value is 1.  
**Note** The mobility services engine does not store events in its database. |
| Refresh Time                  | Enter the wait time in minutes that must pass before a notification is resent. For example, if a device is configured for In Coverage Area notification and it is constantly being detected within the Coverage Area. The notification will be sent once every refresh time. |
| Drop Oldest Entry on Queue Overflow | (Read only). The number of event notifications dropped from the queue since startup. |
| Serialize Events per Mac address per Destination | Select this option if you want the successive events for the same MAC address to be sent to a single destination in a serial manner. |

Step 13  Click **Save**.

**Viewing Notification Statistics**

You can view the notification statistics for a specific mobility services engine. To view the Notification Statistics for a specific mobility services engine:

Choose **Services > Mobility Services > MSE-name > Context Aware Service > Notification Statistics**.

where **MSE-name** is the name of a mobility services engine.

**Table 7-6** lists and describes the fields in the Notification statistics page.
Table 7-6 Notification Statistics Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>Total count of the destinations.</td>
</tr>
<tr>
<td>Unreachable</td>
<td>Count of unreachable destinations.</td>
</tr>
<tr>
<td>Track Definition Status</td>
<td>Status of the track definition. Track notification status could be either</td>
</tr>
<tr>
<td></td>
<td>Enabled or Disabled.</td>
</tr>
<tr>
<td>Track Definition</td>
<td>Track definition can be either Notbound or CAS event notification.</td>
</tr>
<tr>
<td>Destination IP Address</td>
<td>The destination IP Address to which the notifications are sent.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>The destination port to which the notifications are sent.</td>
</tr>
<tr>
<td>Destination Type</td>
<td>The type of the destination. Example: SOAP_XML</td>
</tr>
<tr>
<td>Destination Status</td>
<td>Status of the destination device. The status is either Up or Down.</td>
</tr>
<tr>
<td>Last Sent</td>
<td>The date and time at which the last notification was sent to the destination device.</td>
</tr>
<tr>
<td>Last Failed</td>
<td>The date and time at which the notification had failed.</td>
</tr>
<tr>
<td>Total Count</td>
<td>The total count of notifications sent to the destination. Click on the count link to view the notification statistics details of the destination device.</td>
</tr>
</tbody>
</table>

Configuring a Location Template

You can define a location template for the controller that you can download to multiple controllers.

You can set the following general and advanced parameters on the location template.

General parameters—Enable RFID tag collection, set the location path loss for calibrating or normal (non-calibrating) clients, measurement notification for clients, tags, and rogue access points, set the RSSI expiry timeout value for clients, tags, and rogue access points.

Advanced parameters—Set the RFID tag data timeout value and enable the location path loss configuration for calibrating client multi-band.
To configure a new location template for a controller, follow these steps:

**Step 1**  Choose Configure > Controller Template Launch Pad.

**Step 2**  Select the New (Location Configuration) link under the Location heading to create a new location template (see Figure 7-28).

**Figure 7-28  Configure > Controller Template Launch Pad Page**

**Step 3**  At the New template page, enter a name for the location template on the General tab (see Figure 7-29).

**Figure 7-29  Location Configuration > New > General Tab**

Footnote:
1. Synchronization to the MSE will be needed in order to see effects of changes.
### Step 4

On the General tab, modify parameters as necessary. Table 7-7 describes each of the parameters.

#### Table 7-7  General Location Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RFID tag calculation</strong></td>
<td>Select the <strong>Enabled</strong> check box to collect data on tags.</td>
</tr>
<tr>
<td><strong>Calibrating Client</strong></td>
<td>Select the <strong>Enabled</strong> check box to have a calibrating client. Controllers send regular S36 or S60 requests (depending on the client capability) by way of the access point to calibrating clients. Packets are transmitted on all channels. All access points irrespective of channel (and without a channel change) gather RSSI data from the client at each location. These additional transmissions and channel changes might degrade contemporaneous voice or video traffic. To use all radios (802.11a/b/g/n) available you must enable multiband on the Advanced panel.</td>
</tr>
<tr>
<td><strong>Normal Client</strong></td>
<td>Select the <strong>Enabled</strong> check box to have a non-calibrating client. No S36 or S60 requests are transmitted to the client.</td>
</tr>
<tr>
<td><strong>Measurement Notification Interval</strong></td>
<td>Enter a value to set the NMSP measurement notification interval for clients, tags, and rogue access points and clients. This value can be applied to selected controllers through the template. Setting this value on the controller generates out-of-sync notification which you can view on the Services &gt; Synchronize Services page. When a controller and the mobility services engine have two different measurement intervals, the largest interval setting of the two is adopted by the mobility services engine. Once this controller is synchronized with the mobility services engine, the new value is set on the mobility services engine.</td>
</tr>
<tr>
<td><strong>RSSI Expiry Timeout for Clients</strong></td>
<td>Enter a value to set the RSSI timeout value for normal (non-calibrating) clients.</td>
</tr>
<tr>
<td><strong>RSSI Expiry Timeout for Calibrating Clients</strong></td>
<td>Enter a value to set the RSSI timeout value for calibrating clients.</td>
</tr>
<tr>
<td><strong>RSSI Expiry Timeout for Tags</strong></td>
<td>Enter a value to set the RSSI timeout value for tags.</td>
</tr>
<tr>
<td><strong>RSSI Expiry Timeout for Rogue APs</strong></td>
<td>Enter a value to set the RSSI timeout value for rogue access points.</td>
</tr>
</tbody>
</table>
Enabling Location Services on Wired Switches and Wired Clients

You can import the location of wired Catalyst stackable switches (3750, 3750-E, 3560, 2960, IE-3000 switches), switch blades (3110, 3120, 3130, 3040, 3030, 3020), and switch ports into the mobility services engine.

The following Catalyst 4000 series are also supported:

Once you define a wired switch and synchronize it with a mobility services engine, details on wired clients connected to a wired switch are downloaded to the mobility services engine over the NMSP connection. You can then view wired switches and wired clients using WCS.
Import and display of civic and emergency location identification number (ELIN) meets specifications of RFC 4776, which is outlined at the following URL:

http://tools.ietf.org/html/rfc4776#section-3.4

**Note**

Catalyst stackable switches and switch blades must be operating at Cisco IOS Release 12.2(52) SG or later.

To support location services for wired clients and wired Catalyst switches, you must do the following:

1. Configure the Catalyst switch.
2. Add the Catalyst switch to the WCS.
3. Assign the Catalyst switch to the mobility services engine and synchronize.

This section consists of the following topics:

- Configuring a Catalyst Switch, page 7-53
- Adding a Catalyst Switch to WCS, page 7-55
- Assigning and Synchronizing a Catalyst Switches to a Mobility Services Engine, page 7-56

### Configuring a Catalyst Switch

To configure location service on a wired switch or wired client, and apply it to an interface, follow these steps:

**Note**

All commands are located in the privileged EXEC mode of the command-line interface.

**Step 1** Log into the command-line interface of the switch:

```
Switch > en
Switch#
Switch# configure terminal
```

**Step 2** Enable NMSP:

```
Switch(config)# nmsp
Switch(config-nmsp)# enable
```

**Step 3** Configure the SNMP community:

```
Switch(config)# snmp-server community wired-location
```

**Step 4** Enable IP device tracking in the switch:

```
Switch(config)# ip device tracking
```

**Step 5** Optional Configure a civic location for a switch.

**Note**

You can define a civic and emergency location identification number (ELIN) for a specific location. That identifier can then be assigned to a switch or multiple ports on a switch to represent that location. This location identifier is represented by a single number such as 6 (range 1 to 4095). This saves time when you are configuring multiple switches or ports that reside in the same location.
Enter configuration commands, one per line. End by pressing Ctrl-Z.

The following is an example of a civic location configuration:

Switch(config)# location civic-location identifier 6
Switch(config-civic)# name "switch-loc4"
Switch(config-civic)# seat "ws-3"
Switch(config-civic)# additional code "1e3f0034c092"
Switch(config-civic)# building "SJ-14"
Switch(config-civic)# floor "4"
Switch(config-civic)# street-group "Cisco Way"
Switch(config-civic)# number "3625"
Switch(config-civic)# type-of-place "Lab"
Switch(config-civic)# postal-community-name "Cisco Systems, Inc." 
Switch(config-civic)# postal-code "95134"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state "CA"
Switch(config-civic)# country "US"
Switch(config-civic)# end

Step 6 Configure the ELIN location for the switch.

**Note** The ELIN location length must be between 10 and 25 characters. In the following example, 4084084000 meets that specification. This number can also be entered as 408-408-4000. Additionally, a value with a mix of numerals and text can be entered such as 800-CISCO-WAY or 800CISCOWAY. However, if you place spaces between the numerals or text without hyphens, quotes should be used, such as “800 CISCO WAY.”

Switch(config)# location elin-location "4084084000" identifier 6
Switch(config)# end

Step 7 Configure the location for a port on the switch.

A switch has a specified number of switch ports, and clients and hosts are connected at these ports. When configuring location for a specific switch port, the client connected at that port is assumed to have the port location.

If a switch (switch2) is connected to a port (such as port1) on another switch (switch1) all the clients connected to switch2 are assigned the location that is configured on port1.

The syntax for defining the port is: interface {GigabitEthernet | FastEthernet} slot/module/port

Enter only one location definition on a line, and end the line by pressing Ctrl-Z.

Switch(config)# interface GigabitEthernet 1/0/10
Switch(config-if)# location civic-location-id 6
Switch(config-if)# location elin-location-id 6
Switch(config-if)# end

Step 8 Assign a location to the switch itself.

The following is configured on the FastEthernet network management port of the switch.

Enter configuration commands, one per line. End by pressing Ctrl-Z.

Switch(config)# interface FastEthernet 0
Switch(config-if)# location civic-location-id 6
Switch(config-if)# location elin-location-id 6
Switch(config-if)# end
Chapter 7 Context-Aware Planning and Verification

Enabling Location Services on Wired Switches and Wired Clients

Adding a Catalyst Switch to WCS

All Catalyst switches must be configured with location service before they are added to WCS. Refer to the “Configuring a Catalyst Switch” section on page 7-53.

To add a Catalyst switch configured for wired location service to WCS, follow these steps:

Step 1  Choose Configure > Ethernet Switches.

Step 2  From the Select a command drop-down list, choose Add Ethernet Switches. The Add Ethernet Switches page appears (see Figure 7-31).

Step 3  Choose Device Info or File from the Add Format Type drop-down list.

Note  Choose Device Info to manually enter one or more switch IP addresses. Choose File to import a file with multiple Catalyst switch IP addresses defined. When File is selected, a dialog box appears that defines the accepted format for the imported file.

Step 4  Enter one or more IP addresses.

Step 5  Select the Location Capable check box.

Step 6  From the drop-down list, choose the SNMP version if it is different from the default.

Step 7  No changes are required in the Retries and Timeout text boxes.

Step 8  Enter wired-location as the SNMP community string in the Community text box.

Note  The SNMP community string entered at this step must match that value assigned to the Catalyst switch in Step 3 of the “Configuring a Catalyst Switch” section on page 7-53.
Step 9  Click **OK**. A page confirming successful addition to WCS appears (see Figure 7-32).

![Figure 7-32 Add Switches Result Page](image)

Step 10 Click **OK** on the Add Switches Result page, and the newly added switch appears on the Ethernet Switches page (see Figure 7-33).

![Figure 7-33 Ethernet Switches Summary Page](image)

### Assigning and Synchronizing a Catalyst Switches to a Mobility Services Engine

After adding a Catalyst switch to WCS you need to assign it to a mobility services engine and then synchronize the two systems. Once they are synchronized, an NMSP connection between the controller and the mobility services engine is established.

All information on wired switches and wired clients connected to those switches downloads to the mobility services engine.

**Note** A switch can be synchronized only with one mobility services engine. However, a mobility services engine can have many switches connected to it.

To assign and synchronize Catalyst switches to a mobility services engine, follow these steps:

**Step 1** Choose **Services > Synchronize Services**.

**Step 2** Click the **Wired Switches** tab to assign a switch to a mobility services engine.

**Step 3** Choose one or more switches to be synchronized with the mobility services engine.
Step 4 Click **Change MSE Assignment**.

Step 5 Choose the mobility services engine to which the switches are to be synchronized.

Step 6 Click **Synchronize** to update the mobility services engine(s) database(s).

When items are synchronized, a green two-arrow icon appears in the Sync. Status column for each synchronized entry.

Step 7 To verify the NMSP connection between the switch and a mobility services engine, refer to **Verifying an NMSP Connection to a Mobility Services Engine**, page 7-57.

**Note** See the Chapter 8, “Monitoring the System and Services,” for information on monitoring wired switches.

---

### Verifying an NMSP Connection to a Mobility Services Engine

NMSP manages communication between the mobility services engine and a controller or a location-capable Catalyst switch. Transport of telemetry, emergency, and chokepoint information between the mobility services engine and the controller or location-capable Catalyst switch is managed by this protocol.

To verify a NMSP connection between a mobility services engine and a controller or a location-capable Catalyst switch, follow these steps:

**Step 1** Choose **Services > Mobility Services**.

**Step 2** At the Mobility Services page, click the device name link of the appropriate Catalyst switch or controller.

**Step 3** Choose **System > Status > NMSP Connection Status** (see Figure 7-34).

**Figure 7-34 NMSP Connection Status**

---

**Step 4** Verify that the NMSP Status is **ACTIVE**.

If not active, resynchronize the Catalyst switch or controller and the mobility services engine.
Verifying an NMSP Connection to a Mobility Services Engine

Note

On a Catalyst wired switch, enter the `sh nmsp status` command to verify NMSP connection.