Context-AwareServicePlanningandVerification

This chapter contains the following sections:

Licensing Requirement

Licenses are required 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 : http://www.cisco.com/en/US/products/ps9742/products_data_sheets_list.html

Planning Data, Voice, and Location Deployment

This section contains the following topics:

Guidelines and Limitations

- Access points, clients, and tags must be selected in the Floor Settings menu of the Monitor > Site MAPs page to appear on the map.
- Recommended calculations assume the need for consistently strong signals. In some cases, fewer access points may be required than recommended.
- You must select the Location Services to ensure that the recommended access points provide the true location of an element within seven meters at least 90% of the time.

Calculating the Placement of Access Points

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

Step 1 Choose **Monitor** > **Maps**.
The Site Map page appears.

Step 2 Click the appropriate map name link in the summary list that appears.
If you selected a building map, select a floor map in the Building View page.

A color-coded map appears showing placements of all installed elements (access points, clients, tags) and their relative signal strength.

Note The Access Points, Clients, and 802.11 Tags check boxes must be selected in the Floor Settings dialog box of the Monitor > Site Maps page to appear on the map.

Step 3 Choose **Planning Mode** from the Select a command drop-down list (top-right), and click **Go**.
A map appears with planning mode options at the top of the 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 is used on the floor. The 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 considers data/coverage, voice, and location in determining the number of access points required.

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

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.
- Guidelines and Limitations for Calibration Model, on page 3
- Creating and Applying Data Point and Calibration Models, on page 3

Guidelines and Limitations for Calibration Model

- 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
- We recommend a client device that supports both 802.11a/n and 802.11b/g/n radios to expedite the calibration process for both spectrums.
- Use a laptop or other wireless device to open Prime Infrastructure and perform the calibration process.
- Use only associated clients to collect calibration data.
- Rotate the calibrating client laptop during data collection so that the client is detected evenly by all access points in the vicinity.
- Do not stop data collection until you reach the endpoint even if the data collection bar indicates completion.
- It is generally observed that the point calibration gives more accurate calibration than line calibration.

Creating and Applying Data Point and Calibration Models

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

Step 1 Choose **Monitor** > **Site Maps**.

Step 2 From the Select a command drop-down list, choose **RF Calibration Models**. and then click **Go**.
The RF Calibration Models page displays a list of calibration models. The default calibration model is available in all the virtual domains.

Step 3 From the Select a command drop-down list, choose **Create New Model**. and then click **Go**.

Step 4 Assign a name to the model in the **Model Name** text box. 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 showing the details of the new model.
Note In this page, you can rename and delete the calibration model by choosing the proper option from the Select a command list drop-down 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**.
The campus, building, and floors displayed on this page are filtered based on the virtual domain.

Step 7 If you are performing this process from a mobile device connected to Prime Infrastructure 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 If this process is being performed from a mobile device connected to Prime Infrastructure through the Cisco Centralized architecture, the MAC address text box is automatically populated with the device address.

Step 8 Choose the appropriate campus, building, floor, or outdoor area where the calibration is to be performed. Click **Next**.
Note The calibration in Outdoor Area is supported in Release 7.0.200.x and later. You can use this option to add the calibration data points to the outdoor area. The data points can be added to the Outdoor Area using the same procedure for calibration.

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.

1 To perform a point collection, follow these steps:

a 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 menu appears on the map.

b Position the tip of the Calibration Point pop-up at a data point (+), and click **Go**. A page appears showing the progress of the data collection.

c 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. Information on color-coding is provided in legend on the left sidebar menu. 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.

d Repeat point collection Steps ai to aiii until the calibrations status bars 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.

2 To perform a linear collection, follow these steps:

a 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.

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

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

d Position yourself with your laptop at the starting data point, and click **Go**. Walk steadily towards the endpoint along the defined path. A dialog box appears to show that the data collection is in progress.

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

e Press the space bar (or press **Done** in the data collection page) when you reach the endpoint. The collection dialog box shows the number of samples taken before it closes to reveal the map. The map displays all the coverage areas where data was collected.

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.

Note 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).

f Repeat Steps bii to bv 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.

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). Choose **Monitor** > **Site 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.

Inspecting Location Readiness and Quality

This section contains the following topics:

Guidelines and Limitations

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

Inspecting Location Readiness Using Access Point Data

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

Step 1 Choose **Monitor** > **Site Maps.**

Step 2 Choose the appropriate floor location link from the list.
A map appears showing the 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 menu.

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 menu. Additionally, licenses for both clients and tags must be purchased for each of them to be tracked.

Note See 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 meet (indicated by Yes) and do not meet (indicated by No) the ten 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 data, follow these steps:

Step 1 Choose **Monitor** > **Site Maps**.

Step 2 From the Select a command drop-down list, choose **RF Calibration Model**, and then 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 Click the **Inspect Location Quality** link.
A color-coded map noting the 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 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 Location Accuracy Tool.

The Location 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.

There are two ways to test location accuracy using the Location Accuracy Tool:

- 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.

Note 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 page.

- Using Scheduled Accuracy Testing to Verify Current Location Accuracy, on page 7
- Using On-Demand Location Accuracy Testing, on page 8

Using Scheduled Accuracy Testing to Verify Current Location Accuracy

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**.

Note The campus, building, and floors displayed on this page are filtered based on virtual domain.

Step 3 Enter a test name.

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

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

Step 5 Choose the building from the drop-down list.

Step 6 Choose the floor from the drop-down list.

Step 7 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 8 Select the destination point for the test results. You can have the report e-mailed 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 e-mail option, an SMTP mail server must first be defined for the target e-mail address. Choose **Administrator** > **Settings** > **Mail Server Configuration** to enter the appropriate information.

Step 9 Click **Position Testpoints**. The floor map appears with a list of all clients and tags on that floor with their MAC addresses.

Step 10 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, 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 11 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 12 Click **Save** when all elements are positioned. A page appears confirming successful accuracy testing.

Step 13 Click **OK** to close the confirmation page. You are returned to the Accuracy Tests summary page.

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 14 To view the results of the location accuracy test, click **Test name** and then click **Download** in 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.

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

Step 5 Choose the building from the drop-down list.

Step 6 Choose the floor from the drop-down list.

Step 7 View the test results in the Accuracy Tests > Results page. Reports are in PDF format.

Step 8 Click **Position Testpoints**. The floor map appears with red cross hairs at the (0,0) coordinate.

Step 9 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) appears in a drop-down list to its right.

Step 10 Choose a MAC address from the drop-down list, move the red cross hairs to a map location, and click the mouse to place it.

Step 11 Click **Start** to begin collecting accuracy data.

Step 12 Click **Stop** to finish collecting data.

Note You should allow the test to run for at least two minutes before clicking Stop.

Step 13 Repeat Step 10 to Step 13 for each testpoint that you want to plot on the map.

Step 14 Click **Analyze** when you are finished mapping the testpoints.

Step 15 Click the **Results** tab in 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 16 To download accuracy test logs from the Accuracy Tests summary page:

- 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.
- 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 Optimized Monitor Mode to Enhance Tag Location Reporting

To optimize monitoring and location calculation of tags, you can enable Tracking Optimized Monitor Mode (TOMM) 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.

- Guidelines and Limitations, on page 10
- Optimizing Monitoring and Location Calculation of Tags, on page 10

Guidelines and Limitations

You can configure fewer than four channels for monitoring.

Optimizing Monitoring and Location Calculation of Tags

To optimize monitoring and location calculation of tags, follow these steps:

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.

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, click the **802.11 b/g Radio** link for the access point on which monitor mode is enabled.
c) In the Radio details page, disable **Admin Status** by deselecting 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 To eliminate a monitoring channel, choose **None** from the channel drop-down list.

f) Click **Save**.
g) In 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 in the Monitor > Access Points page.

Configuring Interferer Notification

You can configure this feature only from the campus, building, and floor view page. To configure interferer notification, follow these steps:

Step 1 Choose **Design** > **Site Maps**

Step 2 Click the name of the appropriate floor, building, or campus area.

Step 3 From the Select a command drop-down list, choose **Configure Interferer Notifications**, and click **Go**.
The Interferer CAS notification Configuration page appears. The following devices are displayed:

- Bluetooth Link
- Microwave Oven
- 802.11FH
- Bluetooth Discovery
- TDD Trasmitter
- Jammer
- Continous Transmitter
- DECT like Phone
- Video Camera
- 80.15.4
- WiFi Inverted
- WifI Invalid channel
- Super AG
- Radar
- Canopy
- Xbox
- WiMAX Mobile
- WiMAX Fixed

Step 4 Select the devices check box for which you want notifications to be generated.

Step 5 Click **Save**.

Modifying Context-Aware Service Parameters

You can also modify parameters that affect the location calculation of clients and tags such as Receiver Signal Strength Indicator (RSSI) measurements. Disable tracking and reporting of ad hoc rogue clients and access points.

Licensing Requirement

Licenses are required 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 : http://www.cisco.com/en/US/products/ps9742/products_data_sheets_list.html

Guidelines and Limitations

The Cisco 3315 Mobility Services Engine supports up to 2,000 clients and tags, and the Cisco 3350 Mobility Services Engine supports up to 18,000 clients and tags.

Modifying Tracking Parameters

The mobility services engine can track up to 25k for Cisco 3355 Mobility Service Engine and upto 50000 clients for Virtual Appliance (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.

Only those tags, clients, and interferers that the controller is tracking are seen in the Prime Infrastructure 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 Prime Infrastructure:

- 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 25,000 trackable units, you can set a limit to track only 10,000 client stations (leaving 15,000 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 in the Tracking Parameters page.

This section includes the following topics:

Guidelines and Limitations

- When upgrading mobility services engines from Release 6.0 to 7.0, if any limits have been set on wireless clients or rogues, they are reset because of the wired client limit change in Release 7.0.
- The actual number of tracked clients is determined by the license purchased.
- The actual number of tracked active RFID tags is determined by the license purchased.
- We recommend that you use a Release 4.2 or higher controller for better latency and accuracy.

Configuring Tracking Parameters for a Mobility Services Engine

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

Step 1 Choose **Services** > **Mobility Services**. The Mobility Services page appears.

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

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

Step 4 Modify the tracking parameters as appropriate. The following table lists the tracking parameters.

Table 1: Tracking Parameters

Field	Configuration Options
Tracking Parameters	

Field	Configuration Options
Wired Clients	1 Select the **Enable** check box to enable tracking of client stations by the MSE. In Release 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 MSE 7.0 and Prime Infrastructure Release 7.0 and later. In other words, you can limit wired clients to a fixed number such as 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 the MSE from Release 6.0, if any limits have been set on wireless clients or rogues, they are reset because of the wired client limit change in Release 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 MSE. 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 MSE. **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.
Rogue Access Points	1 Select the **Enable** check box to enable tracking of rogue access points by the MSE. 2 Select the **Enable Limiting** check box to set a limit on the number of rogue access points to track. 3 Enter a Limit Value if limiting is enabled. The limit entered can be any positive value up to18,000 which is the maximum number of rogue access points that can be tracked by a MSE. **Note** Active Value (Display only): Indicates the number of rogue access points currently being tracked. **Note** Not Tracked (Display only): Indicates the number of rogue access points beyond the limit.
Exclude Ad-Hoc Rogues	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 Prime Infrastructure maps or its events and alarms reported.

Field	Configuration Options
Rogue Clients	**1** Select the **Enable** check box to enable tracking of rogue clients by the MSE. **2** Select the **Enable Limiting** check box to set a limit on the number of rogue clients to track. **3** Enter a Limit Value if limiting is enabled. The limit entered can be any positive value. This limit varies based on the platform. The limit value is the maximum number of rogue clients that can be tracked by a MSE. **Note** Active Value (Display only): Indicates the number of rogue clients being tracked. **Note** Not Tracked (Display only): Indicates the number of rogue clients beyond the limit.
Interferers	**1** Select the **Enable** check box to enable tracking of the interferers by the MSE. **2** Select the **Enable Limiting** check box to set a limit on the number of interferers to track. **3** Enter a Limit Value if limiting is enabled. In Release 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. In Release 7.0.200.x, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, interferers, and guests. **Note** Active Value (Display only): Indicates the number of interferers currently being tracked. **Note** Not Tracked (Display only): Indicates the number of interferers beyond the limit.
Asset Tracking Elements	
Active RFID Tags	Select the **Enable** check box to enable tracking of active RFID tags by the MSE. **Note** The actual number of tracked active RFID tags is determined by the license purchased. **Note** Active Value (Display only): Indicates the number of active RFID tags currently being tracked. **Note** Not Tracked (Display only): Indicates the number of active RFID tags beyond the limit.
SNMP Retry Count	Enter the number of times to retry a polling cycle. The default value is 3. Allowed values are from 1 to 99999. (Configurable in controller Release 4.1 and earlier and location server Release 3.0 and earlier only).
SNMP Timeout	Enter the number of seconds before a polling cycle times out. The default value is 5. Allowed values are from 1 to 99999. (Configurable in controller Release 4.1 and earlier and location server Release 3.0 and earlier only).

Field	Configuration Options
Client Stations	Select the **Enable** check box to enable client station polling and enter the polling interval in seconds. The default value is 300. Allowed values are from 1 to 99999. (Configurable in controller Release 4.1 and earlier and location server Release 3.0 and earlier only).
Active RFID Tags	Select the **Enable** check box to enable active RFID tag polling and enter the polling interval in seconds. Allowed values are from 1 to 99999. **Note** Before the mobility service can collect asset tag data from Cisco WLCs, you must enable the detection of active RFID tags using the **config rfid status enable** command on the Cisco WLCs.
Rogue Clients and Access Points	Select the **Enable** check box to enable rogue access point polling and enter the polling interval in seconds. The default value is 600. Allowed values are from 1 to 99999 (Configurable in controller Release 4.1 and earlier and location server Release 3.0 and earlier only).
Statistics	Select the **Enable** check box to enable statistics polling for the mobility service, and enter the polling interval in seconds. Default value is 900. Allowed values are from 1 to 99999 (Configurable in controller Release 4.1 and earlier and location server Release 3.0 and earlier only).

Step 5 Click **Save** to store the new settings in the MSE database.

Modifying Filtering Parameters

- 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 in Prime Infrastructure.

  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 following allowed listing is a wildcard.

Note Allowed MAC address formats are viewable in the Filtering Parameters configuration page.

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.

Modifying Filtering Parameters contains the following topics:

Guidelines and Limitations

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

Configuring Filtering Parameters for a Mobility Services Engine

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

Step 1 Choose **Services** > **Mobility Services Engines**. 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. The following table lists filtering parameters.

Table 2: Filtering Parameters

Field	Configuration Options
Advanced Filtering Parameters	
Duty Cycle Cutoff Interferers	Enter the duty cycle cutoff value for interferers so that only those interferers whose duty cycle meets the specified limits are tracked and counted against the CAS license. The default value for the Duty Cycle Cutoff Interferers is 0% and the configurable range is from 0% to 100%. In order to better utilize the location license, you can choose to specify a filter for interferers based on the duty cycle of the interferer.

Field	Configuration Options
RSSI Cutoff for Probing Clients	Enter the RSSI cutoff value for probing clients so that those clients whose RSSI values are below the cutoff value is reported. The default value for the RSSI cutoff for probing clients 1 -128dB.
MAC Filtering Parameters	
Exclude Probing Clients	Select the check box to prevent calculating location for probing clients.
Enable Location MAC Filtering	1 Select the check box to enable filtering of specific elements by their MAC addresses. 2 To import a file of MAC addresses (Upload a file for Location MAC Filtering text box), browse for the file name and click **Save** to load the file. MAC addresses from the list auto-populate the Allowed List and Disallowed List based on their designation in the file. **Note** To view allowed MAC address formats, click the red question mark next to the Upload a file for Location MAC Filtering text box. 3 To add an individual MAC address, enter the MAC addresses (format is xx:xx:xx:xx:xx:xx) and click either **Allow** or **Disallow**. The address appears in the appropriate column. **Note** To move an address between the Allow and Disallow columns, highlight the MAC address entry and click the button under the appropriate column. **Note** 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. **Note** 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.

Step 5 Click **Save** to store the new settings in the mobility services engine database.

Modifying History Parameters

This section contains the following topics:

Guidelines and Limitations

Before enabling location presence, synchronize the mobility services engine.

Configuring Mobility Services Engine History Parameters

To configure mobility services engine history, follow these steps:

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

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. The following table lists history parameter.

Table 3: History Parameters

Field	Description
Archive for	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.
Prune data starting at	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. **Note** Enter the default limits for better performance.
Client Stations	Select the **Enable** check box to turn on historical data collection for client stations.
Wired Stations	Select the **Enable** check box to turn on historical data collection for wired stations.
Asset Tags	Select the **Enable** check box to turn on historical data collection. **Note** Before the mobility service can collect asset tag data from Cisco WLC, you must enable the detection of RFID tags using the **config rfid status enable** command.
Rogue Clients and Access Points	Select the **Enable** check box to turn on historical data collection.
Interferers	Select the **Enable** check box to turn on historical data collection.

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 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 Before enabling this feature, you have to synchronize the mobility services engine.

- Guidelines and Limitations, on page 19
- Enabling and Configuring Location Presence on a Mobility Services Engine, on page 20

Guidelines and Limitations

Before enabling location presence, synchronize the mobility services engine.

Enabling and Configuring Location Presence on a Mobility Services Engine

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

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

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 MSE 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 MSE returns the client address as *Building A*.

b) When AP is selected, the MSE 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 MSE returns the client address of *3034:00hh:0adg*.

c) When X,Y is selected, the MSE 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 MSE 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. The default value is 24 hours (1440 minutes).

Step 9 Click **Save**.

Importing and Exporting Asset Information

This section contains the following topics:

- Importing Asset Information, on page 21
- Exporting Asset Information, on page 22

Importing Asset Information

To import asset, chokepoint, and Time Difference Of Arrival (TDOA) receiver information for the mobility services engine using the Prime Infrastructure, follow these steps:

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

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 Time Difference Of Arrival (TDOA) receiver information from the mobility services engine to a file using Prime Infrastructure, follow these steps:

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

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 page), **Save** (to external PC or server), or **Cancel**.

Note If you click **Save**, you are asked to select the asset file destination and name. The file is named *assets.out* by default. Click **Close** in the dialog box when download is complete.

Modifying Location Parameters

This section contains the following topic:

- Configuring Location Parameters, on page 22

Configuring Location Parameters

To configure location parameters, follow these steps:

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

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

Step 3 Choose **Context Aware Service** > **Advanced** > **Location Parameters**. The configuration options appear.

Step 4 Modify the location parameters as appropriate. The following table lists location parameters.

Table 4: Location Parameters

Field	Configuration Options
Enable 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.
Enabled 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 MSE.
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 MSE receives two samples at 10 and 12 minutes, it keeps both samples. An additional sample received at 15 minutes is discarded. The 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.
Absolute discard RSSI time	Enter the number of minutes after which RSSI measurement should be considered stale and discarded, regardless of the most recent sample. The default value is 60. Allowed values range from 0 to 99999. A value of less than 60 is not recommended. **Note** This parameter applies only to clients.
RSSI Cutoff	Enter the RSSI cutoff value, in decibels (dBs) with respect to one (1) mW (dBm), above which the MSE will always use the access point measurement. The default value is –75. **Note** When 3 or more measurements are available above the RSSI cutoff value, the MSE discards 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. **Note** This parameter applies only to clients. **Caution** Modify only under Cisco TAC personnel guidance. Modifying this value can reduce the accuracy of location calculation.
Enable Location Filtering	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.

Field	Configuration Options
Chokepoint Usage	Select the **Enable** check box to enable chokepoints to track Cisco compatible tags.
Use Chokepoints for Interfloor conflicts	Perimeter chokepoints or weighted location readings can be used to locate Cisco compatible tags. Options: • Never: When selected, perimeter chokepoints are not used to locate Cisco compatible tags. • Always: When selected, perimeter points are used to locate Cisco compatible tags. • 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.
Chokepoint Out of Range timeout	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.
Absent Data cleanup interval	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.
Use Default Heatmaps for Non Cisco Antennas	Select this check box to enable the usage of default heatmaps for non-Cisco antennas during the Location Calculation. This option is disabled by default.
Movement Detection	
Individual RSSI change threshold	This parameter specifies the Individual RSSI movement recalculation trigger threshold. Enter a threshold value between 0-127 dBm. Modify only under Cisco TAC personnel guidance.
Aggregated RSSI change threshold	This parameter specifies the Aggregated RSSI movement recalculation trigger threshold. Enter a threshold value between 0-127 dBm. Modify only under Cisco TAC personnel guidance.
Many new RSSI change percentage threshold	This parameter specifies Many new RSSI movement recalculation trigger threshold in percentage. Modify only under Cisco TAC personnel guidance.

Step 5 Click **Save**.

Enabling Notifications and Configuring Notification Parameters

This section contains the following topics:

Enabling Notifications

User-configured conditional notifications manage which notifications the mobility services engine sends to Prime Infrastructure or a third-party destination compatible with the mobility services engine notifications.

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 Prime Infrastructure, 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 within a certain period.

Notification parameter settings apply to user-configurable conditional notifications and northbound notifications except as noted in Configuring Notification Parameters, on page 25.

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 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.

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 Contents check boxes:

- **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 Triggers check boxes:

- **Chokepoints**
- **Telemetry**
- **Emergency**
- **Battery Level**
- **Vendor Data**
- **Location Recalculation**

Step 9 Enter the IP address or hostname 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 the **HTTPS** check box 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 page. The following table describes the user-configurable conditional and northbound notifications fields.

Table 5: User-Configurable Conditional and Northbound Notifications Fields

Field	Configuration Options
Rate Limit	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).

Field	Configuration Options
Queue Limit	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).
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 re-sent. For example, if a device is configured for In Coverage Area notification and it is constantly being detected within the Coverage Area. The notification is sent once every refresh time. Default value is 0 minutes.
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 engine. To view notification statistics information for a specific mobility services engine, follow these steps:

Step 1 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 .
You can view the notification statistics for a specific mobility services engine. To view the Notification, choose **Services > Mobility Services >** *MSE-name* > **Context Aware Service** > **Notification Statistics**.

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

The following table lists fields in the Notification Statistics page.

Table 6: Notification Statistics Page

Field	Description
Summary	
Destinations	
Total	Destinations total count.
Unreachable	Unreachable destinations count.
Notification Statistics Summary	
Track Definition Status	Status of the track definition. Track notification status can be either Enabled or Disabled.
Track Definition	Track definition can be either Nothbound or CAS event notification.
Destination IP Address	The destination IP address to which the notifications are sent.
Destination Port	The destination port to which the notifications are sent.
Destination Type	The type of the destination. Example: SOAP_XML.
Destination Status	Status of the destination device. The status is either Up or Down.
Last Sent	The date and time at which the last notification was sent to the destination device.
Last Failed	The date and time at which the notification had failed.
Total Count	The total count of notifications sent to the destination. Click the count link to view the notification statistics details of the destination device.

Location Template for Cisco Wireless LAN Controllers

Currently WiFi clients are moving towards lesser probing to discover an AP. Smartphones do this to conserve battery power. The applications on a smartphone have difficulty generating probe request but can easily generate data packets and hence trigger enhanced location for the application. FastLocate feature enhances

the location performance via data packets RSSI reported through the WSSI module in monitor mode. The is accomplished by using the WSSI modules on the AP to monitor all traffic coming from a client. This not only increases the efficiency of monitoring such device packets to improve the location updates from the given client, but also does this with minimal impact on the client's battery life. Enabling this feature will increase the update rate of location of all associated clients, and will have limited improvement on the update rate of unassociated clients.

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 , enable the location path loss configuration for calibrating client multi-band and set the FastLocate configuration.

This section contains Configuring a New Location Template for a Wireless LAN Controller, on page 30

FastLocate Overview

Current generation of Wi-Fi clients probe less frequently to conserve battery power. It is often the case that probing behavior of a Wi-Fi client is device dependent. This poses a challenge for all W-Fi based location solution because they rely on RSSI measurements from probe frames that can be heard by multiple APs. With fewer probes from Wi-Fi clients, location updates become infrequent. Cisco has introduced FastLocate technology that addresses this problem. FastLocate makes it possible for multiple APs to hear the data packets at the same time. This is achieved with Wireless Security Module (WSM) to collect data packet RSSI sent by the associated Wi-Fi clients. Unlike probe request frames, applications on smartphone easily generate data traffic when they are connected to the Wi-Fi network. Enabling this feature will increase the update rate of location for all associated clients leading to a smoother blue dot experience. FastLocate increased the locate updates with minimal impact on clients battery life and is also device independent.

Deployment Considerations

- FastLocate technology does not require new hardware or AP. The existing WSM module with AP 3K can be used.
- FastLocate and advanced security monitoring can be simultaneously turned ON.
- MSE location algorithms can simultaneously calculate location from probes and data RSSI. There is no need to dedicate a new MSE for FastLocate.
- For best results, all APs in the RF environment will have WSM module. This is a 1:1 density of APs with WSM module. While a mix of APs with module and without modules is possible, this deployment needs to be carefully planned. This is not a recommended deployment at this time.
- Enabling FastLocate provides limited improvement on the update rate of unassociated clients.
- Since data packets are more frequent, using data packets for location increases the computation burden at the MSE Location engine. This has an impact on the total number of simultaneous active clients that can be tracked by the MSE.

- A rule of thumb is to reduce the maximum number of clients tracked by a factor of 5. For example, high end virtual MSE that can track up to 50,000 devices using probes can track up to 10,000 devices using Data packets.

Configuring a New Location Template for a Wireless LAN Controller

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.

Step 3 In the New Controller Template page, enter a name for the location template in the General tab

Step 4 In the General tab, modify parameters as necessary. The following table lists General tab fields.

Table 7: General Tab Fields

Parameter	Configuration Options
RFID tag calculation	Select the **Enabled** check box to collect data on tags.
Calibrating Client	Select the **Enabled** check box to have a calibrating client. Cisco WLCs 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 in the Advanced tab.
Normal Client	Select the **Enabled** check box to have a non-calibrating client. No S36 or S60 requests are transmitted to the client.
Measurement Notification Interval	Enter a value to set the Network Mobility Services Protocol (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 in the **Services > Synchronize Services** page. When a Cisco WLCs 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 Cisco WLCs is synchronized with the mobility services engine, the new value is set on the mobility services engine.
RSSI Expiry Timeout for Clients	Enter a value to set the RSSI timeout value for normal (non-calibrating) clients.
RSSI Expiry Timeout for Calibrating Clients	Enter a value to set the RSSI timeout value for calibrating clients.
RSSI Expiry Timeout for Tags	Enter a value to set the RSSI timeout value for tags.

Parameter	Configuration Options
RSSI Expiry Timeout for Rogue APs	Enter a value to set the RSSI timeout value for rogue access points.

Step 5 On the Advanced tab, modify parameters as necessary.
The following table describes each of the Advanced tab fields.

Table 8: Advanced Location Fields

Field	Configuration Options
RFID Tag Data Timeout	Enter an RFID tag data timeout value.
Calibrating Client Multiband	Select the **Enable** check box to send S36 and S60 packets (where applicable) on all channels. Calibrating clients must be enabled on the General tab.
FastLocate	Select the **Enable** check box.
FastLocate Threshold	Enter the threshold value. This parameter controls the frequency at which APs actively seek location measurements from the associated clients. Lower the value, higher is the frequency of APs seeking location measurements. The exact time interval between the location measurements depends on the number of channels that the AP will scan and the dwell time per channel.
FastLocate NTP IP Address	Enter the IP address of the NTP server that is reachable via the APs. Note that the cisco routers can act as NTP servers too. The only requirement is that all APs across all WLCs be on the same time (may be different NTP servers as long as the NTP servers are on the same time).

Step 6 Click **Save**.

Location Services on Wired Switches and Wired Clients

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 Prime Infrastructure.

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

- Prerequisites to Support Location Services for Wired Clients, on page 32
- Guidelines and Limitations, on page 32

Prerequisites to Support Location Services for Wired Clients

- Configure the Catalyst switch.
- Add the Catalyst switch to Prime Infrastructure.
- Catalyst stackable switches and switch blades must be running Cisco IOS Release 12.2(52) SG or later.
- Assign the Catalyst switch to the mobility services engine and synchronize.

Guidelines and Limitations

- WS-C4948, WS-C4948-10GE, ME-4924-10GE, WS-4928-10GE, WS-C4900M, WS-X4515, WS-X4516, WS-X4013+, WS-X4013+TS, WS-X4516-10GE, WS-X4013+10GE, WS-X45-SUP6-E, and WS-X45-SUP6-LE
- A switch can be synchronized only with one mobility services engine. However, a mobility services engine can have many switches connected to it.

Configuring a Catalyst Switch Using the CLI

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

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

Step 1 Log in to the command-line interface of the switch:

```
Switch > enable
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 timer 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 port location 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
```

Adding a Catalyst Switch to Prime Infrastructure

All Catalyst switches must be configured with location services before they are added to Prime Infrastructure. To add a Catalyst switch configured for wired location service to Prime Infrastructure, 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.

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.

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

Step 7 Enter **wired-location** as the SNMP community string in the Community text box.

Step 8 Click **Prime Infrastructure**. A page confirming the successful addition to Prime Infrastructure appears.

Step 9 Click **OK** in the Add Switches Result page. The newly added switch appears in the Ethernet Switches page.

Assigning and Synchronizing a Catalyst Switch to a Mobility Services Engine

After adding a Catalyst switch to the Prime Infrastructure, 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 MSE. However, a MSE can have many switches connected to it.

To assign and synchronize Catalyst switches to a MSE, follow these steps:

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

Step 2 Click the **Wired Switches** tab to assign a switch to a MSE.

Step 3 Choose one or more switches to be synchronized with the MSE.

Step 4 Click **Change MSE Assignment**.

Step 5 Choose the MSE to which the switches are to be synchronized.

Step 6 Click **Synchronize** to update the MSE(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 MSE, see the Verifying an NMSP Connection to a Mobility Services Engine, on page 35.

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 an NMSP connection between a MSE and a controller or a location-capable Catalyst switch, follow these steps:

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

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

Step 3 Choose **System** > **Status** > **NMSP Connection Status**.

Step 4 Verify that the NMSP Status is ACTIVE.
If not active, resynchronize the Catalyst switch or controller and the MSE.

Note On a Catalyst wired switch, enter the **show nmsp status** command to verify NMSP connection.