CHAPTER 7

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 7-18
- Using Tracking Optimized Monitor Mode to Enhance Tag Location Reporting, page 7-21
- Defining Inclusion and Exclusion Regions on a Floor, page 7-23
- Defining a Rail Line on a Floor, page 7-28
- Modifying Context-Aware Service Parameters, page 7-31
- Configuring a Location Template, page 7-46
- Enabling Location Services on Wired Switches and Wired Clients, page 7-49
- Verifying a NMSP Connection to a Mobility Services Engine, page 7-55

You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points. Licenses for tags and clients are offered separately. (The clients license also includes tracking of rogue clients and rogue access points).

Refer to the *Cisco 3300 Series Mobility Services Engine Licensing and Ordering Guide:*

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

For details on adding client and tag licenses to the mobility services engine, refer to Chapter 2.

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.

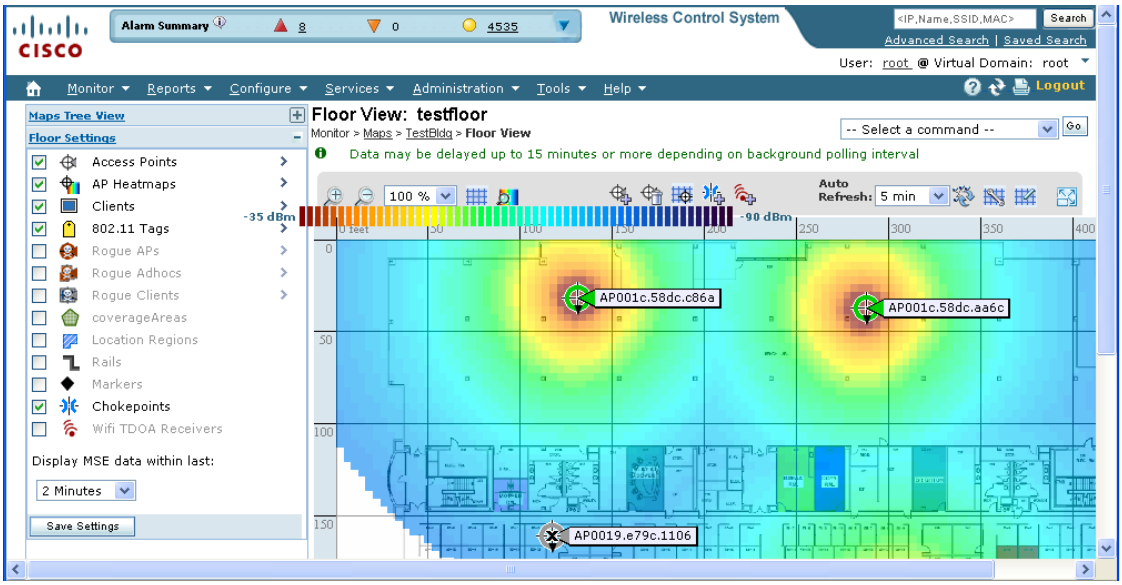
To calculate the recommended number and placement of access points on a floor, follow these steps:

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 window.

Figure 7-1 Monitor > Maps > Device Name Window



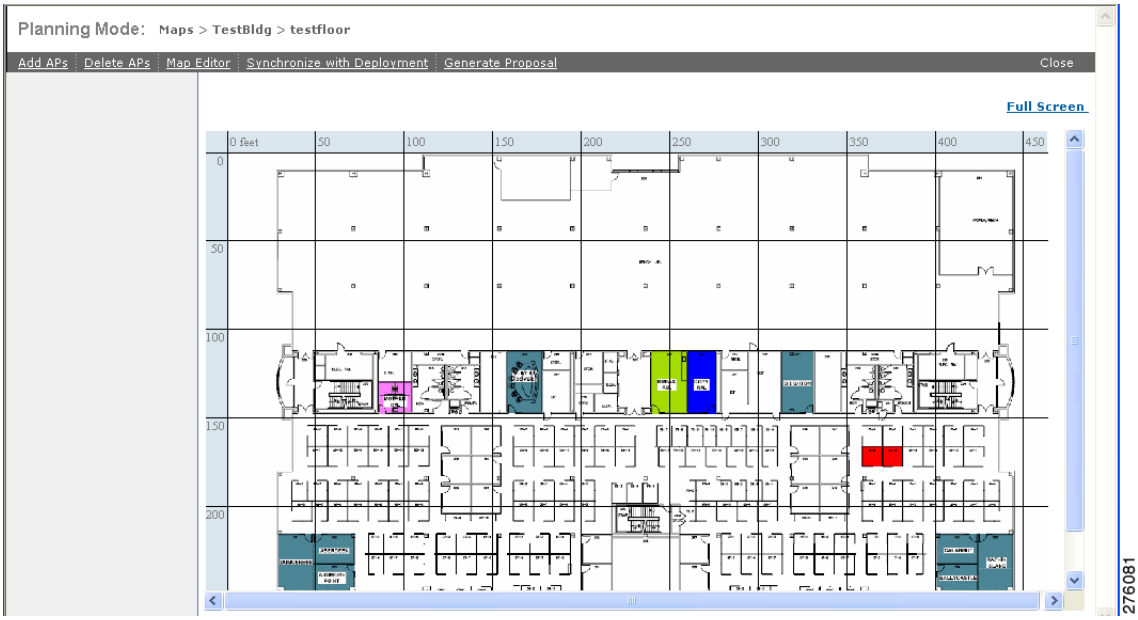
A map appears showing placement of all installed elements (access points, clients, tags) and their relative signal strength (RSSI). RSSI is indicated by the colored rings that surround the element. To identify the exact RSSI for that element, refer to the RSSI legend (color bar) at the top of the page.

Note Access points, clients, and tags must be selected (check boxes checked) in the Floor Settings panel of the Monitor > Maps window to appear on the map (see Figure 7-1).

Step 3 Select **Planning Mode** from the Select a command menu at the top-right of the window. Click **Go.**

A map appears with planning mode options at the top of the window (see Figure 7-2).

Figure 7-2 Planning Mode Window



Step 4 Click **Add APs**.

In the window 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 **Check** 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 of all services that are listed above it. For example, if you check 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** (left panel, bottom) to generate a map based on the recommended number of access points and their proposed placement in the selected area.

Note Check the Location services check box to ensure that the recommended access points provide the true location of an element within 10 meters at least 90% of the time.

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.

Note Calibration models can only be applied to clients, rogue clients, and rogue access points. Calibration for tags is done using the *Aeroscout System Manager*. Refer to the following link for details on tag calibration: http://support.aeroscout.com

Note 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 Cisco WCS and perform the calibration process.

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

Step 1 Navigate to **Monitor > Maps** and select **RF Calibration Models** from the Select a command drop-down menu. Click **Go**.

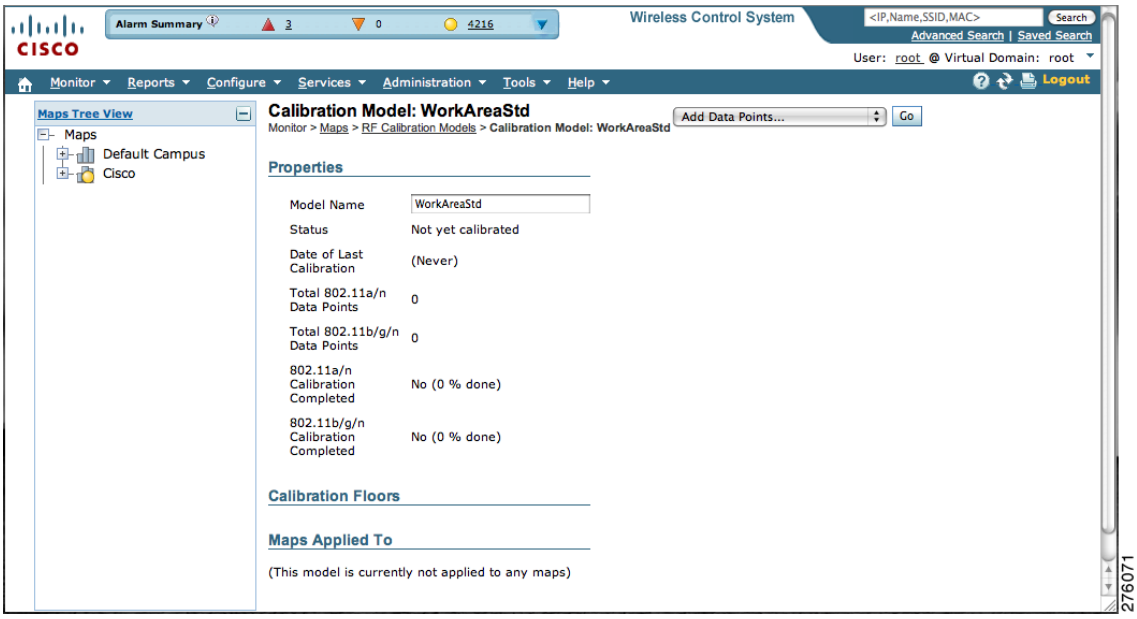
Step 2 Select **Create New Model** from the Select a command drop-down menu at the upper right. Click **Go**.

Step 3 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 4 To start the calibration process, click the **model name** link. A new window appears which showing the details of the new model (see Figure 7-3).

Figure 7-3 New Calibration Model Details Window



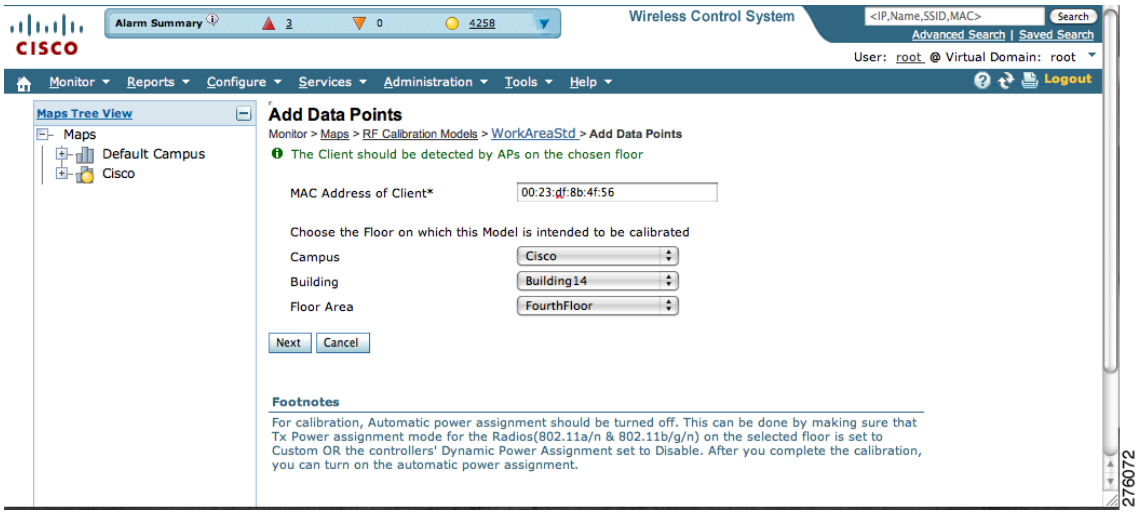
Note At this screen, you can rename and delete the calibration model by selecting the proper option from the Select a command menu. When renaming the model, enter the new name before selecting **Rename Model**.

Step 5 Select **Add Data Points** from the Select a command drop-down menu and click **Go**.

Step 6 If you are performing this process from a mobile device connected to WCS through the Cisco Centralized architecture, the MAC address field is automatically populated with the device's address. 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).

Step 7 Choose the appropriate campus, building, and floor where the calibration is to be performed (see Figure 7-4). Click **Next**.

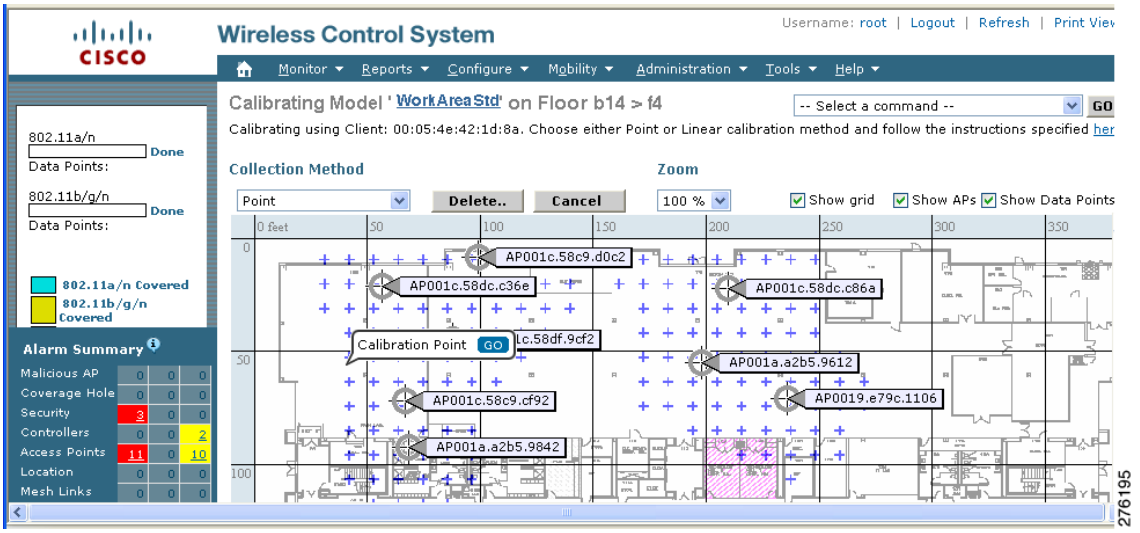
Figure 7-4 Starting to Calibrate



Step 8 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 window for a point calibration.

Figure 7-5 Positioning Calibration Points



a. To do a point collection, follow these steps:

1. Select **Point** from the Collection Method drop-down menu and check the Show Data Points check box if not already checked. 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.

Note Rotate the calibrating client laptop during data collection so that the client is detected evenly by all access points in the vicinity.

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 legend at left). 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 press and hold **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 roughly 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:

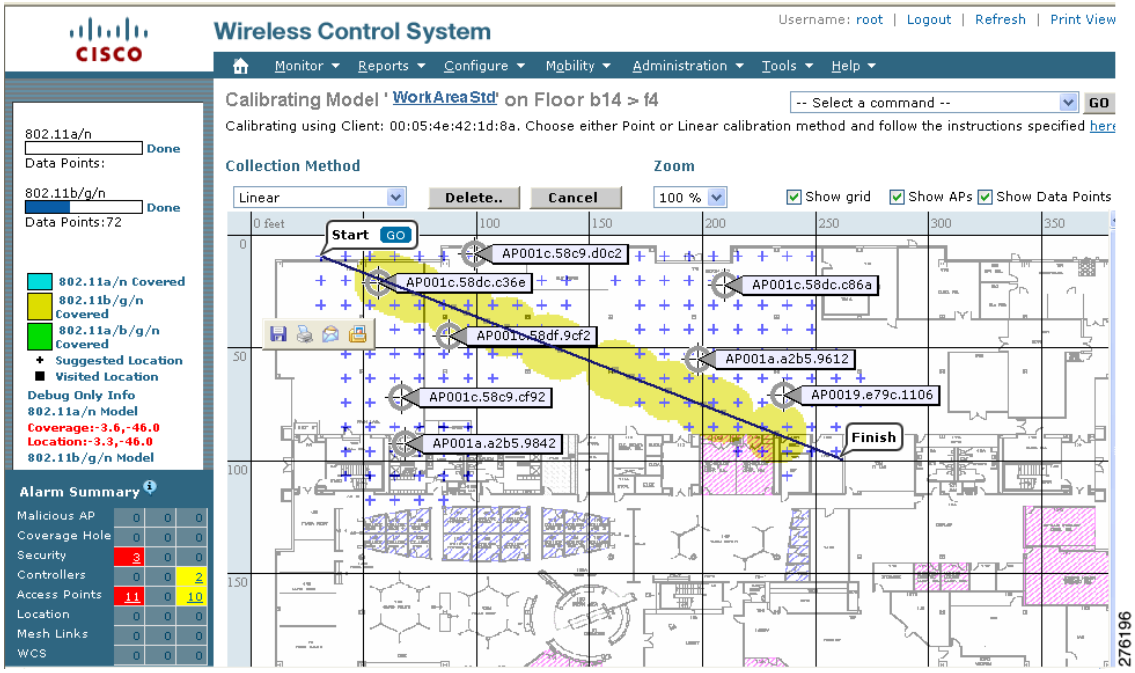
1. Select **Linear** from the Collection Method drop-down menu and check the **Show Data points** check box if not already checked. A line appears on the map with both Start and Finish pop-ups (see Figure 7-6).
2. Position the tip of the Start pop-up at the starting data point.
3. Position the Finish 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. A panel displays (left) showing that data collection is in progress.

Note Do not stop data collection until you reach the end point even if the data collection bar (left) 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.

Figure 7-6 Linear Data Collection



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 at left).

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 8 a.

Step 9 To calibrate the data points, click the name of the calibration model at the top of the window. The main screen for that model appears.

Step 10 Select **Calibrate** from the Select a command drop-down menu and click **Go**.

Step 11 Click **Inspect Location Quality** when calibration completes. A map appears showing RSSI readings displays.

Step 12 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 menu and click **Go**.

Step 13 From the Floor Type (RF Model) drop-down menu, 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

You can configure Cisco 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 10 meters at least 90% of the time. Location readiness calculation is determined the by 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 (10m, 90%).

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 on 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 on the Floor Settings panel (left).

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

Note Refer to Chapter 2 for details on installing client and tag licenses.

Step 3 Select **Inspect Location Readiness** from the Select a command menu at the top-right of the window. 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 Choose **RF Calibration Mode**l from the Select a command menu. 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 At the same window, 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 true location of an element within 10 meters at least 90% of the time.

You can analyze the location accuracy of non-rogue and rogue clients and asset tags 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 and tags at a number of different locations. It is generally used to test the location accuracy for a small number of clients and tags.

Both are configured and executed through a single window.

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 Select **New Scheduled Accuracy Test** from the Select a command drop-down menu.

Step 3 Enter a test name.

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

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

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

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

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 window. 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 Click the check box next to each client and tag for which you want to check the location accuracy.

When you check 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, check 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 window.

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 Select **New On demand Accuracy Test** from the Select a command drop-down menu.

Step 3 Enter a test name.

Step 4 Select the area type from the drop-down menu.

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

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

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

Step 8 View test results at the Accuracy Tests > Results window. 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, select either client or tag from the drop-down menu on the left. A list of all MAC addresses for the selected option (client or tag) appear in a drop-down menu to its right.

Step 11 Select a MAC address from the drop-down menu, 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 panel 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. Check the listed test check box and select either **Download Logs** or **Download Logs for Last Run** from the Select a command menu.

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 Refer to *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine Users Guide* for chokepoint installation, configuration, and management details: http://support.aeroscout.com

Adding Chokepoints to the Cisco WCS

After you install and configure the chokepoint using *Aeroscout System Manager,* you can add the chokepoint to the location database and position it on a Cisco WCS map.

To add a chokepoint to Cisco WCS, follow these steps:

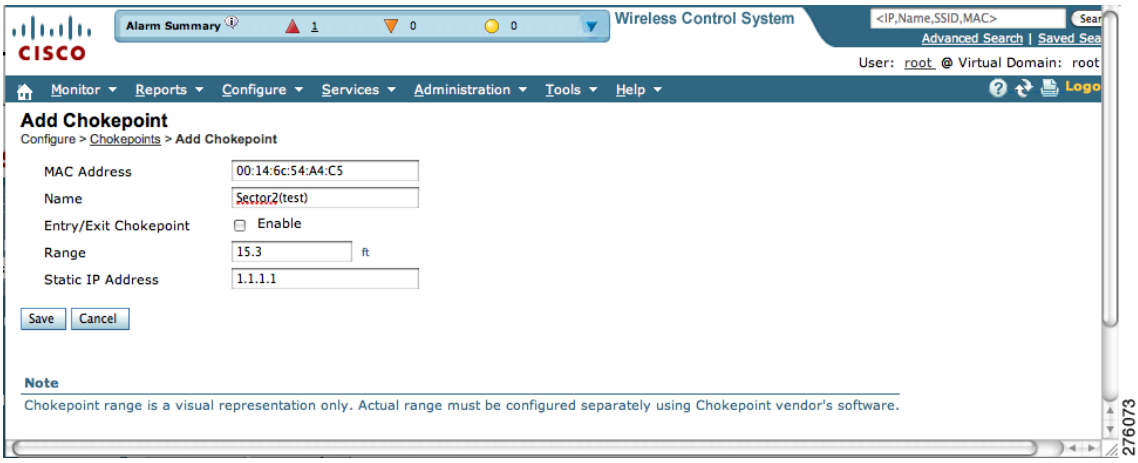
Step 1 Choose **Configure > Chokepoints** from the main menu (top).

The Chokepoints summary window appears.

Step 2 Select **Add Chokepoint** from the Select a command menu and click **Go.**

The Add Chokepoint entry screen appears (see Figure 7-7).

Figure 7-7 Add Chokepoint Window



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.

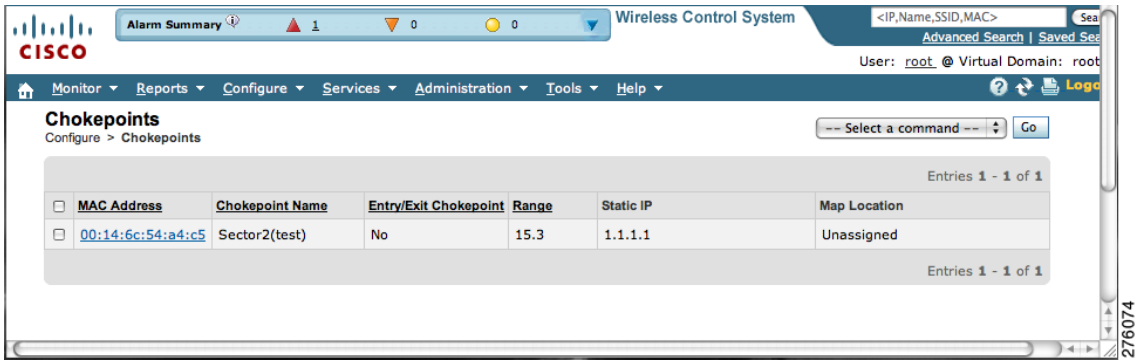
Step 4 Check the **Entry/Exit Chokepoint** check box if you want the chokepoint to function as a perimeter chokepoint. Its function is to track the entry and exit of clients and tags from an area or floor.

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 window appears with the new chokepoint entry listed (see Figure 7-8).

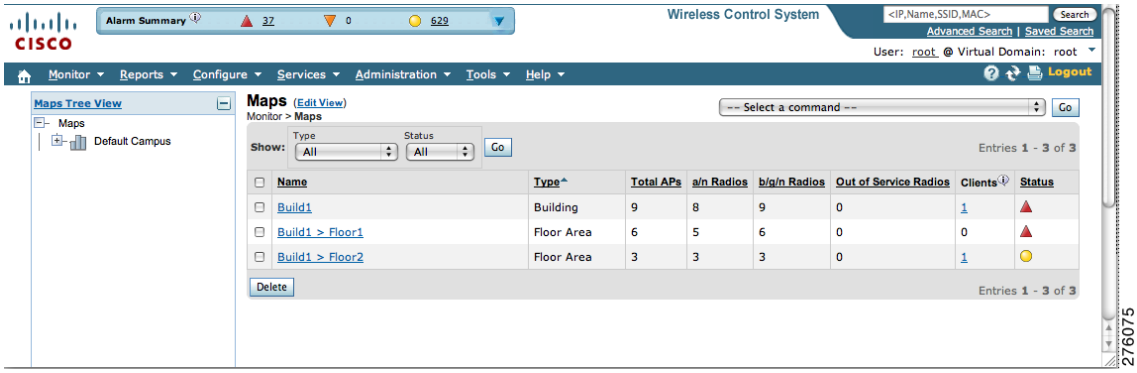
Figure 7-8 Chokepoints Summary Window



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

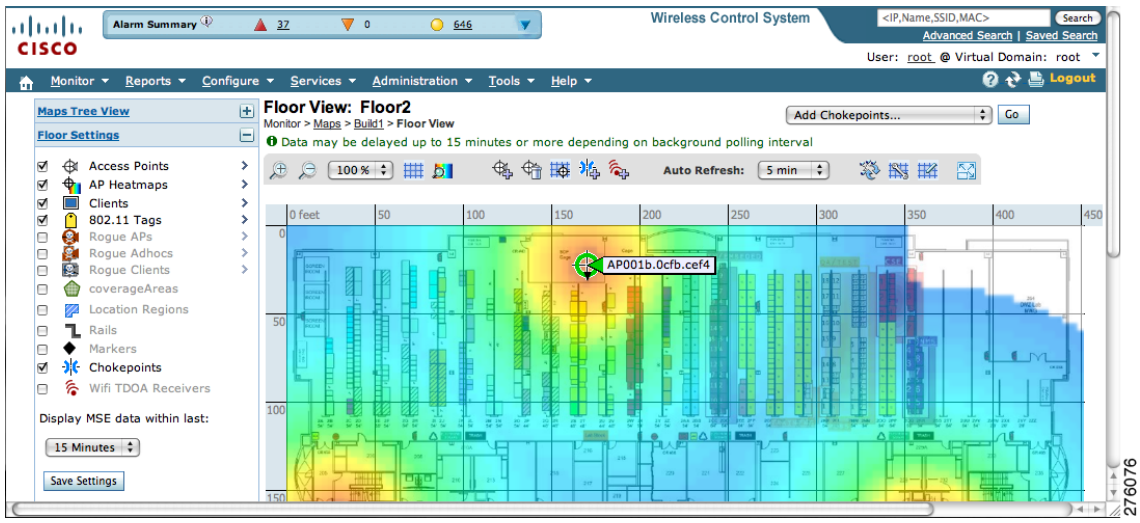
Step 6 To add the chokepoint to a map, choose **Monitor > Maps** (see Figure 7-9).

Figure 7-9 Monitor > Maps Window



Step 7 At the Maps window, 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 Window

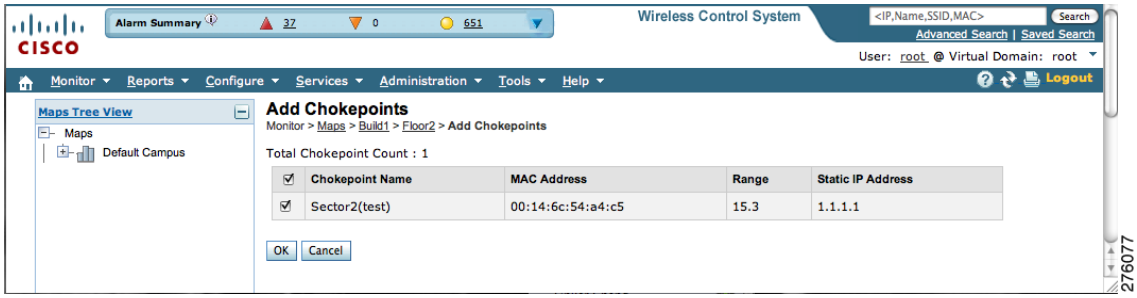


Step 8 Select **Add Chokepoints** from the Select a command menu. Click **Go**.

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

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

Figure 7-11 Add Chokepoints Summary Window

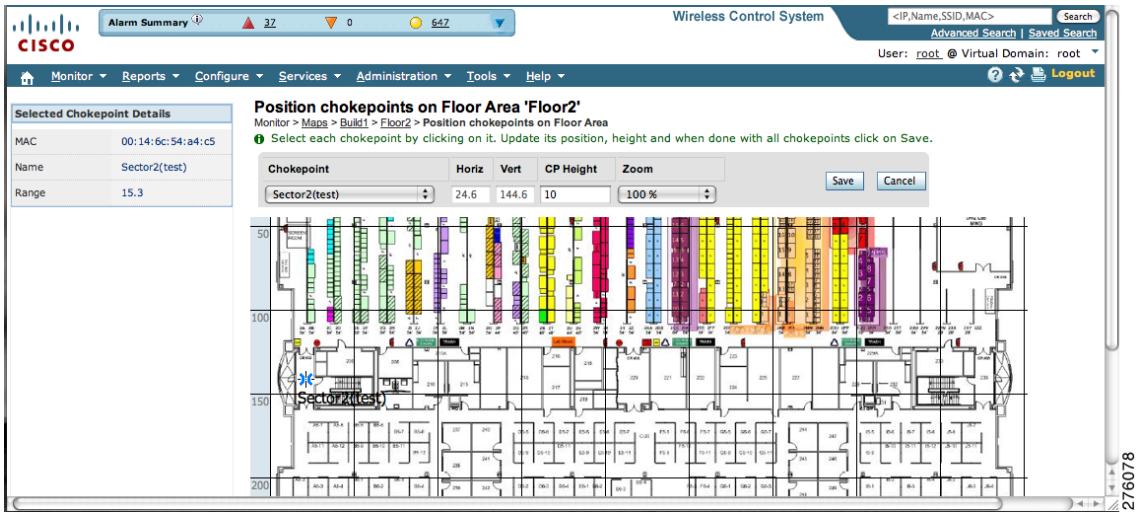


Step 9 Check the box next to the chokepoint to be added to the map. Click **OK** (bottom of screen).

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 on 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



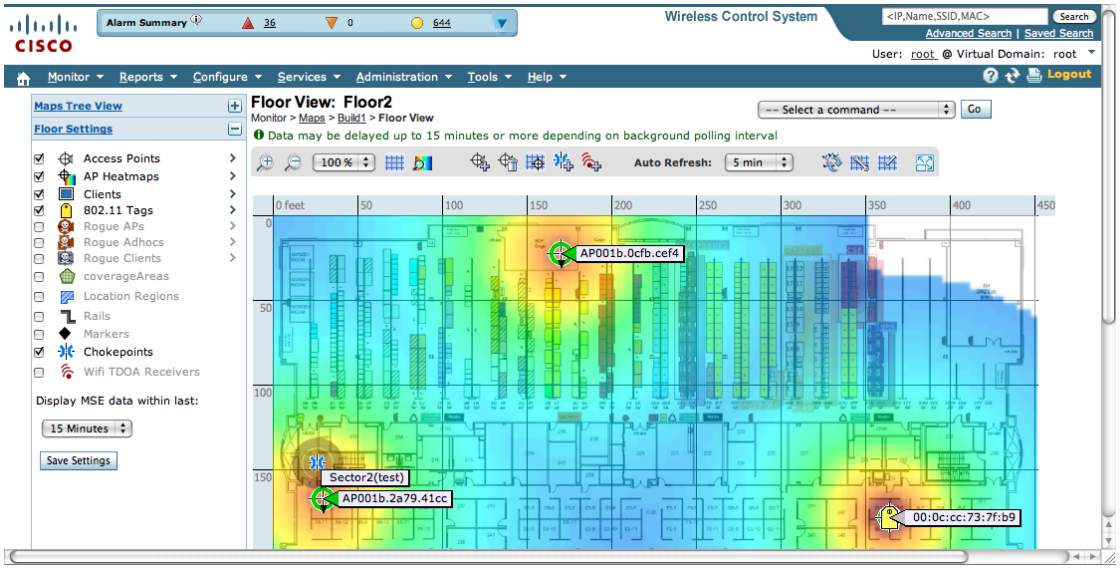
Note The MAC address, name, and coverage range of the chokepoint appear in the left panel when you click on the chokepoint icon for placement.

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, click the **Chokepoints** check box in the Floor Settings panel (left). Do not select **Save Settings** in the Floor Settings panel 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 pass a 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 Cisco WCS

You can remove one or more chokepoints at a time.

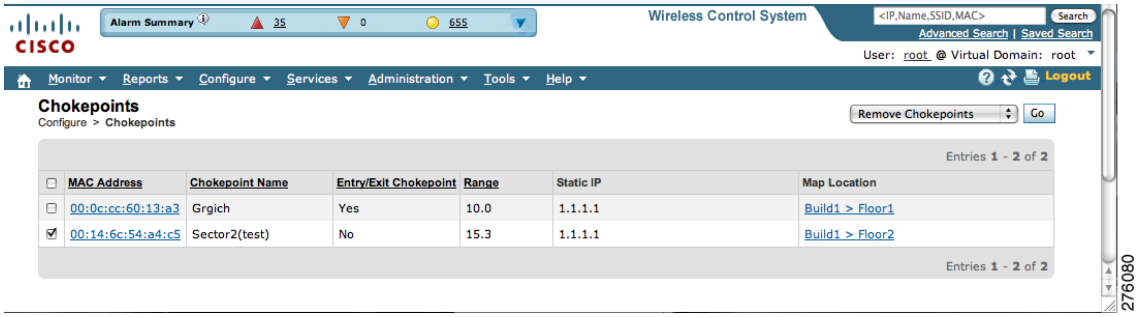
To delete a chokepoint, follow these steps:

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

Step 2 Check the box next to the chokepoint to be deleted.

Step 3 Select **Remove Chokepoints** from the Select a command drop-down menu. Click **Go** (see Figure 7-14).

Figure 7-14 Removing a Chokepoint



Step 4 To confirm chokepoint deletion, click **OK** in the pop-up window that appears.

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

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 a tagged asset's location.

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 Cisco WCS database and map.

   Refer to the "Adding Wi-Fi TDOA Receivers to Cisco WCS" section on page 7-19 for details on adding the TDOA receiver to Cisco WCS.

3. Synchronize Cisco WCS and mobility services engines.

   Refer to Chapter 3, "Synchronizing Mobility Services Engines," for details on synchronization.

4. Setup the TDOA receiver using the *AeroScout System Manager*.

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

Adding Wi-Fi TDOA Receivers to Cisco WCS

After you add TDOA receivers to Cisco WCS maps and synchronize, use the *AeroScout System Manager* application rather than Cisco 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 link: http://support.aeroscout.com.

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

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

Step 2 From the Select a command menu, select **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 window 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.

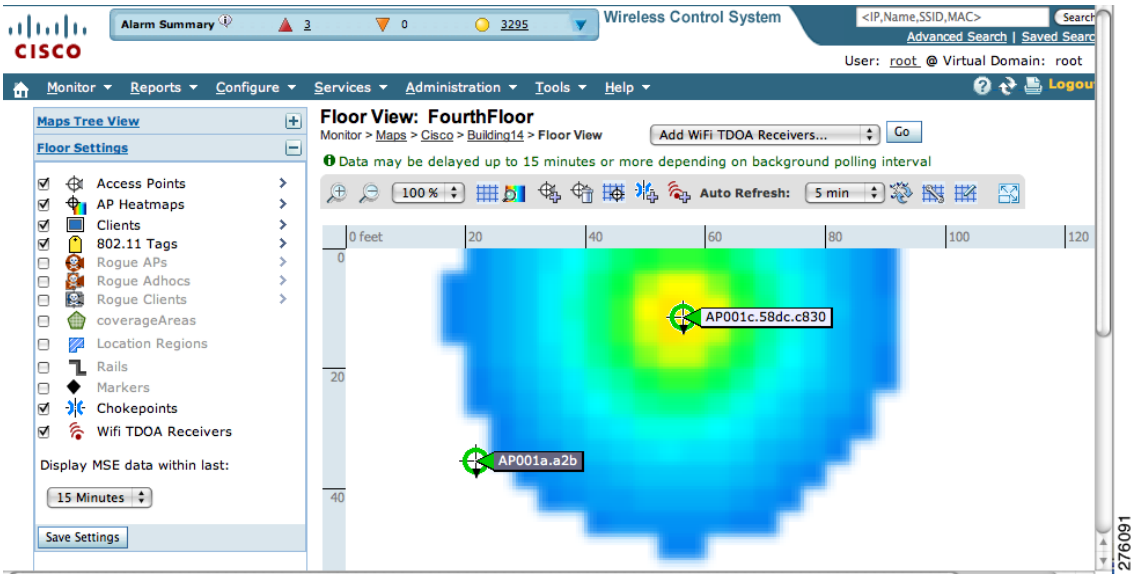
Step 5 To add the TDOA receiver to a map, choose **Monitor > Maps**.

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

Step 7 Check the **WiFi TDOA Receivers** check box in the Floor Settings panel (left), if not already checked. 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).

Figure 7-15 Monitor > Maps > Add WiFi TDOA Receivers Window



Step 8 Select **Add WiFi TDOA receivers** from the Select a command menu. Click **Go**.

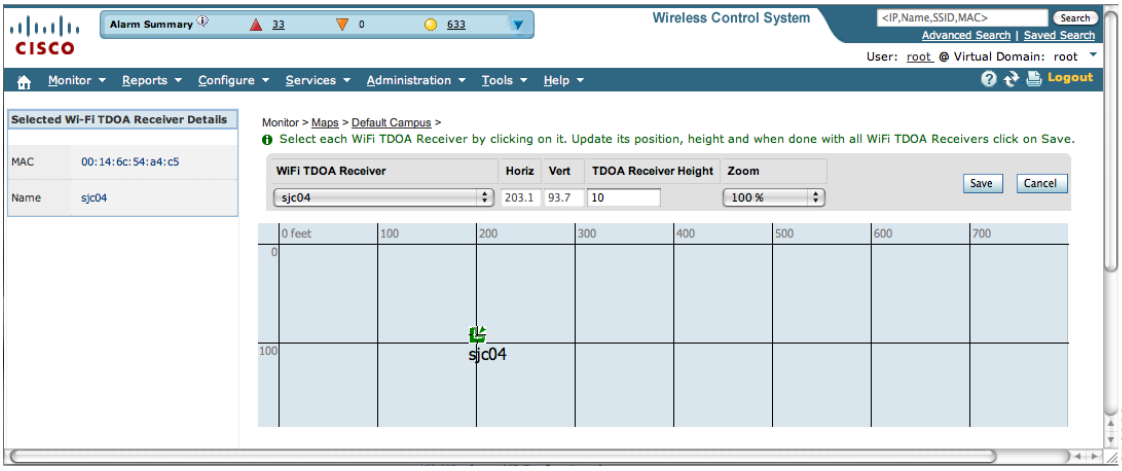
The Add WiFi TDOA Receivers summary window appears.

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

Step 9 Check 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.

Note You can also place the receiver by entering the horizontal (Horz), and vertical (Vert) coordinates of the target location.

Note The MAC address and name of the TDOA receiver appear in the left panel when you click the TDOA receiver icon for placement.

Step 11 After placing the TDOA receiver, enter the height of the receiver in the sensor height field.

Step 12 Click **Save** when the icon is placed correctly on the map.

The floor heat map reappears with the added TDOA receiver.

Note Update of the map might not be immediate as map updates are determined by the configured background polling interval.

Removing Wi-Fi TDOA Receivers from Cisco WCS

You can remove one or more Wi-Fi TDOA receivers at a time. If you remove a TDOA receiver from a map it remains in the WCS database but is labeled as unassigned.

To delete a TDOA receiver from WCS, follow these steps:

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

Step 2 Check the box next to each TDOA receiver to be deleted.

Step 3 Select **Remove WiFi TDOA Receivers** from the Select a command drop-down menu. Click **Go**.

Step 4 To confirm TDOA receiver deletion, click **OK** in the pop-up window that appears.

The **All WiFi TDOA Receivers** window. A message confirming deletion of the TDOA receiver appears. The deleted TDOA receiver is no longer listed in the window.

Using Tracking Optimized Monitor Mode to Enhance Tag Location Reporting

To optimize monitoring and location calculation of tags, you can enable 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.

Step 1 To enable monitor mode on the access point, follow these steps:

a. Choose **Configure > Access Point >** *AP Name*.

b. Select **Monitor** as the AP Mode.

Note For more details, refer to the *Cisco Wireless Control System Configuration Guide, Release 6.0* http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html

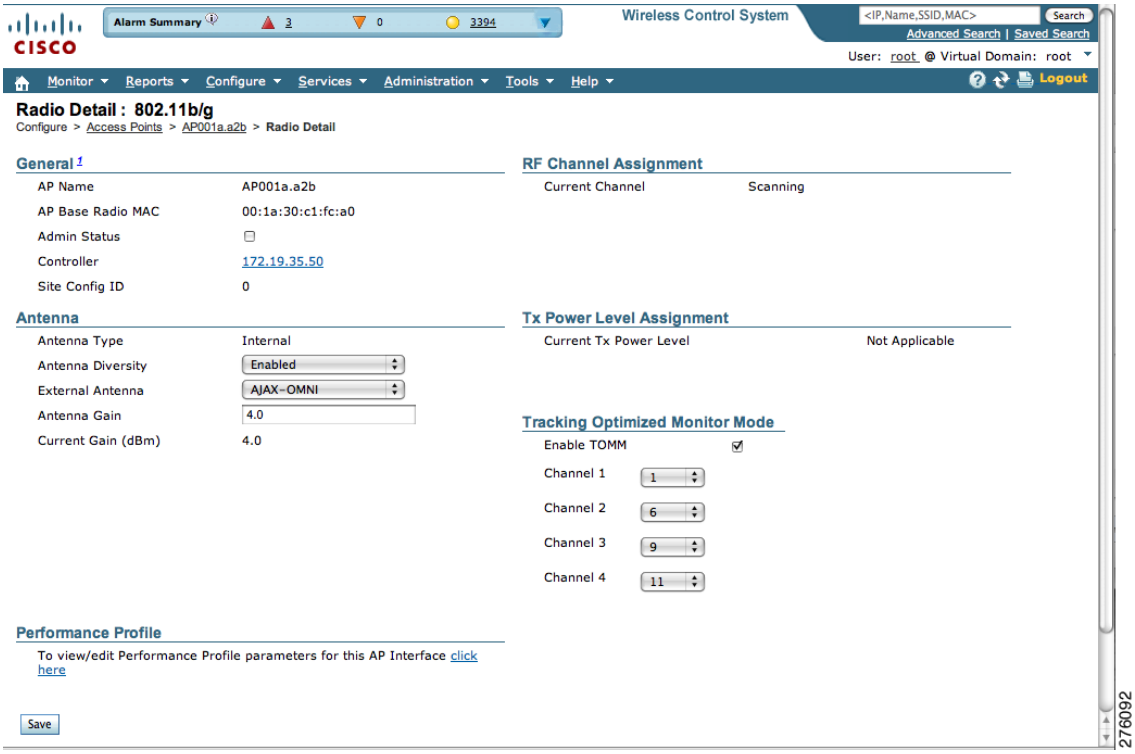
Step 2 To enable TOMM and assign monitoring channels on the access point radio, follow these steps:

a. After enabling monitor mode at the access point level, choose **Configure > Access Points**.

b. At the Access Points summary window, select the **802.11 b/g Radio** link for the access point on which monitor mode is enabled.

c. At the Radio details window, disable **Admin Status** by unchecking the check box. This disables the radio (see Figure 7-17).

Figure 7-17 Configure > Access Point > 802.11 b/g



d. Check the Enable TOMM (Tracking Optimized Monitor Mode) 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, select **None** from the channel drop-down menu.

f. Click **Save**.

g. At the Radio parameters window, re-enable the radio by checking 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** window.

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

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 Cisco 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.
- You must check the Location Regions option on the Floor Settings panel of the Monitor > Maps window 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**.

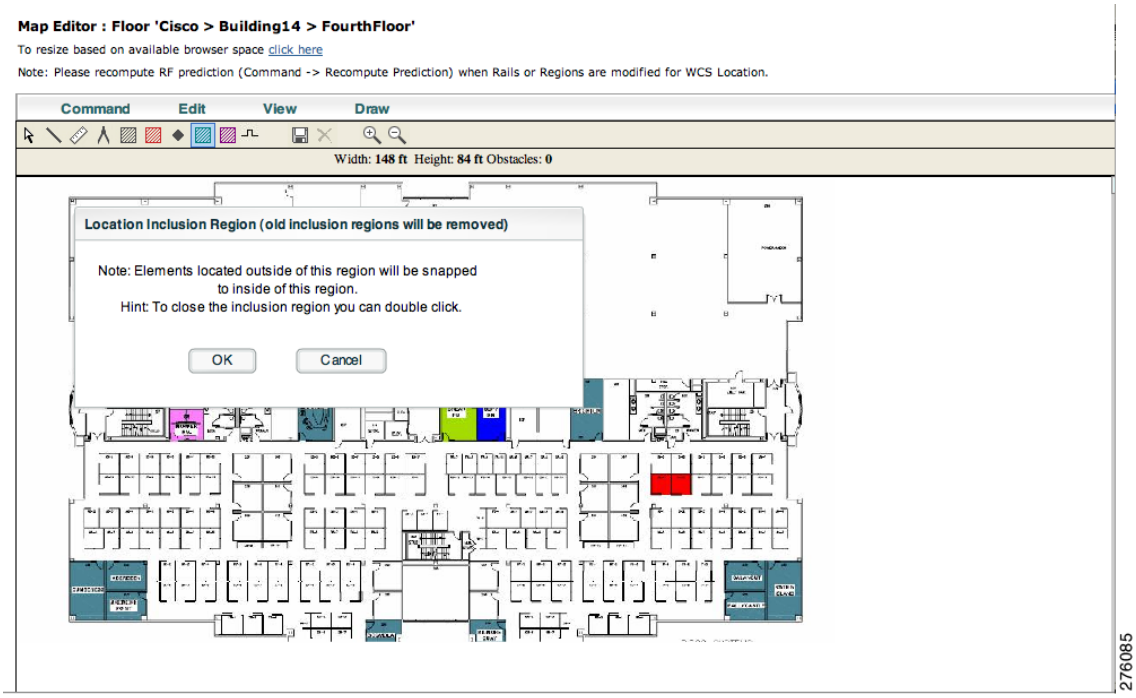
Step 2 Click the name of the appropriate floor.

Step 3 Select **Map Editor** from the Select a command drop-down menu. Click **Go**.

Step 4 At the map, click the aqua box in the tool bar (see Figure 7-18).

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 Cisco WCS.

Figure 7-18 Map Editor Window



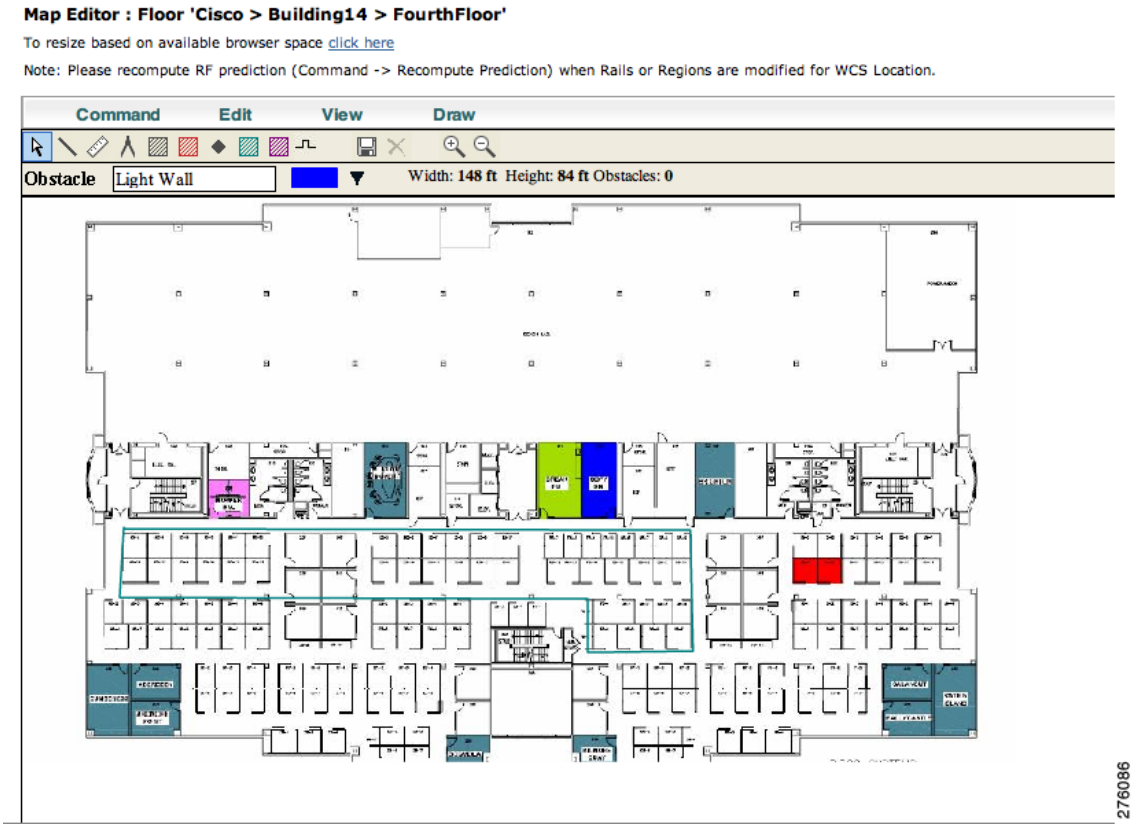
Step 5 Click **OK** in the message box that appears. A drawing icon appears to outline the inclusion area.

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 7-19).

Figure 7-19 Inclusion Area Defined



Step 9 Choose **Command > Save** or click the disk icon on the tool bar 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 in the tool bar. The area is removed from the floor map.

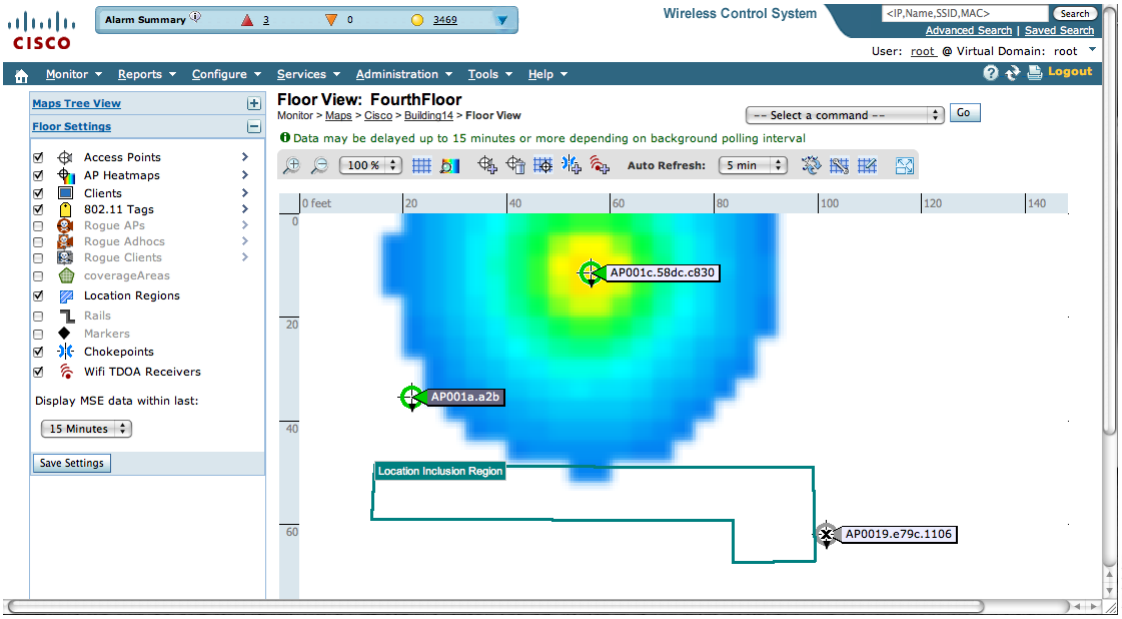
Step 10 To return to the floor map to enable inclusion regions on heatmaps, choose **Command > Exit**.

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

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

The defined inclusion region appears on the map (see Figure 7-20).

Figure 7-20 Monitor > Maps > Floor



Step 13 To resynchronize the Cisco WCS and location databases, choose **Services > Synchronize Services**.

Step 14 At the Synchronize WCS and MSE(s) window, select the **Network Designs** tab and click **Synchronize** (bottom).

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

Note Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.

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.

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 Select **Map Editor** from the Select a command drop-down menu.Click **Go**.

Step 4 At the map, click the purple box in the tool bar.

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 7-21).

Figure 7-21 Defining Exclusion Areas on Floor Map

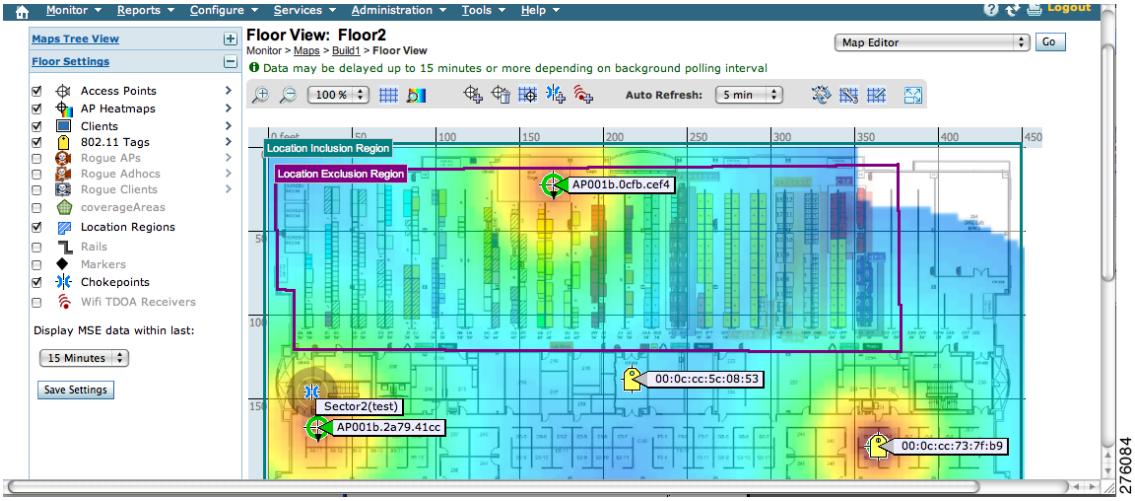
Step 10 When all exclusion areas are defined, select **Save** from the Command menu or the disk icon on the tool bar to save the exclusion region.

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 tool bar. 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, check the Location Regions check box if it is not already checked. The exclusion region is shown on the map (see Figure 7-22).

Figure 7-22 Location Exclusion Region



Step 13 To resynchronize the Cisco WCS and location databases, choose **Services > Synchronize Services**.

Step 14 At the Synchronize window, select **Network Designs** from the Synchronize drop-down menu and then click **Synchronize**.

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

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:

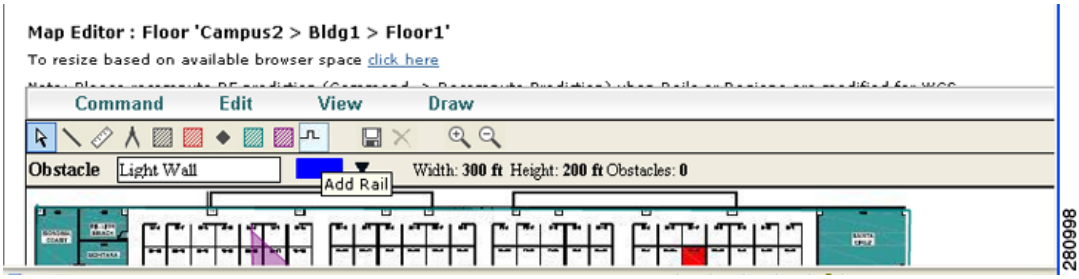
Step 1 Choose **Monitor > Maps**.

Step 2 Click on the name of the appropriate floor area.

Step 3 Select **Map Editor** from the Select a command drop-down menu. Click **Go**.

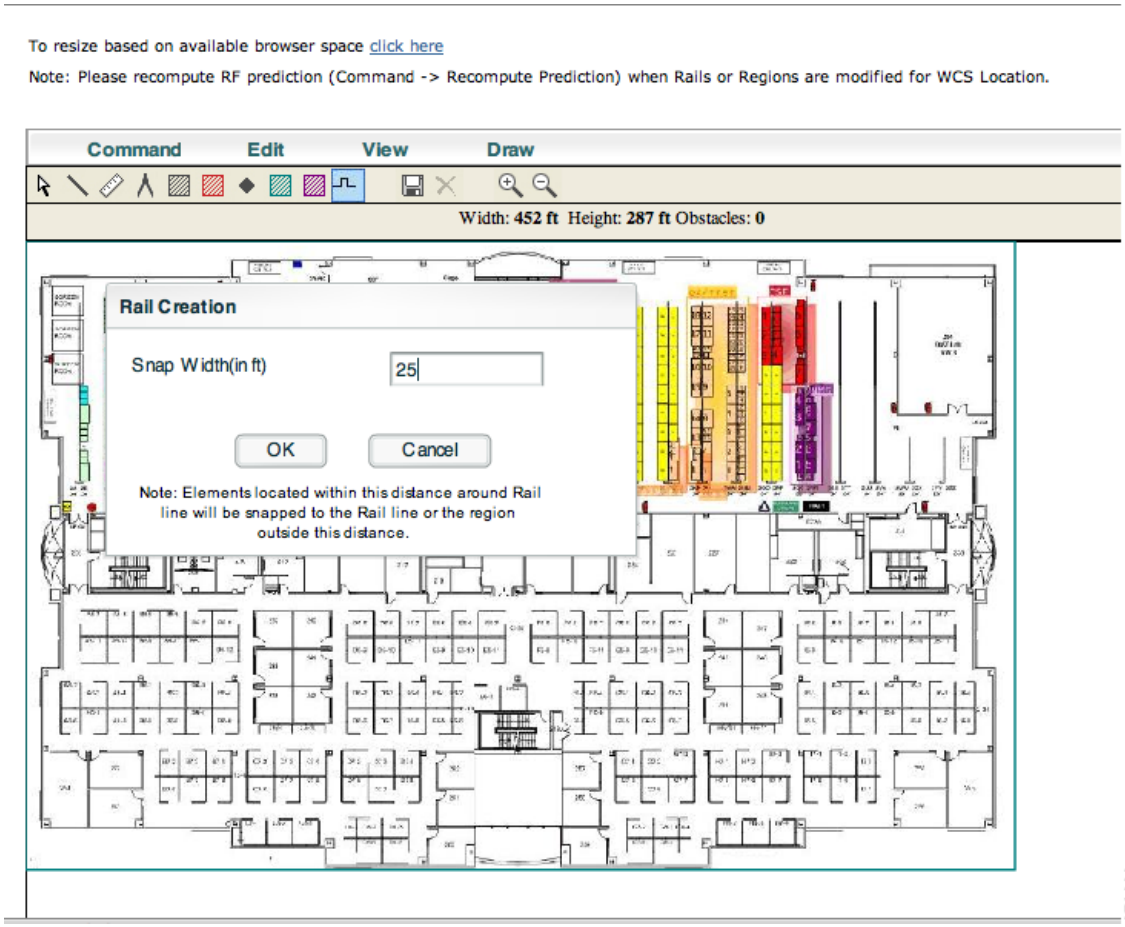
Step 4 Click the rail icon (to the right of the purple exclusion icon) in the tool bar (see Figure 7-23).

Figure 7-23 Rail Icon on Map Editor Tool Bar



Step 5 In the message panel that appears, enter a snap-width (feet or meters) for the rail and then click **OK** (see Figure 7-24).

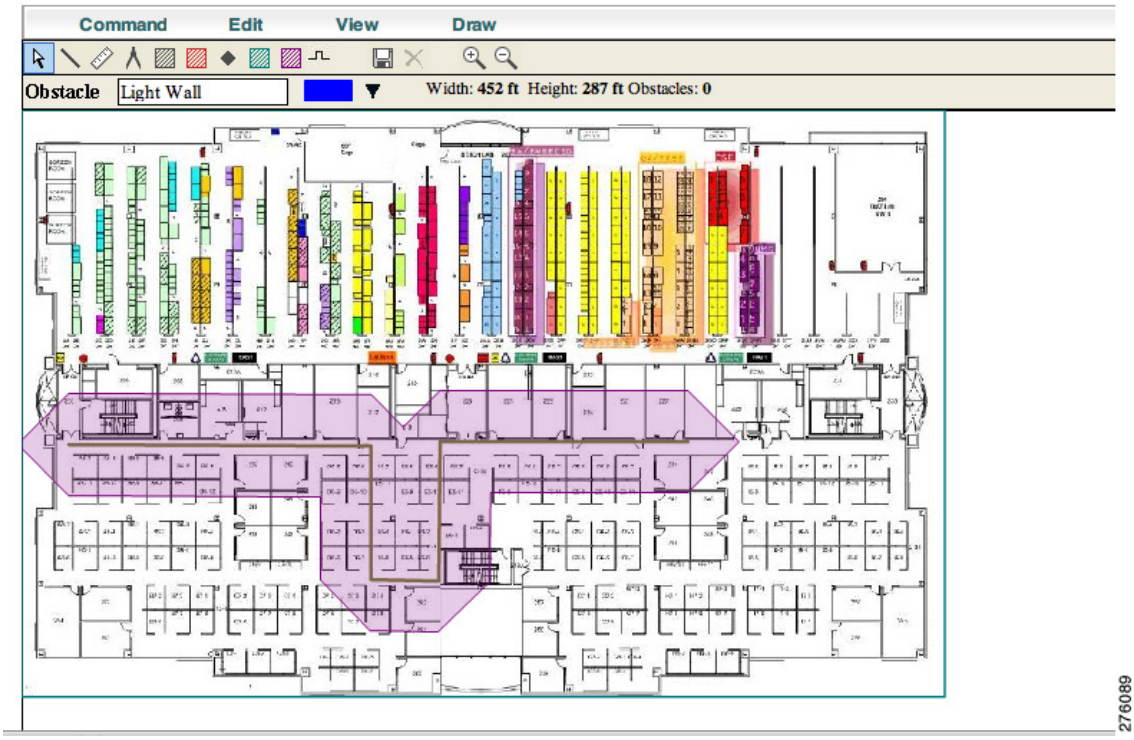
Figure 7-24 Defining Rail Width



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 7-25).

Figure 7-25 Defining Rail Line in Map Editor

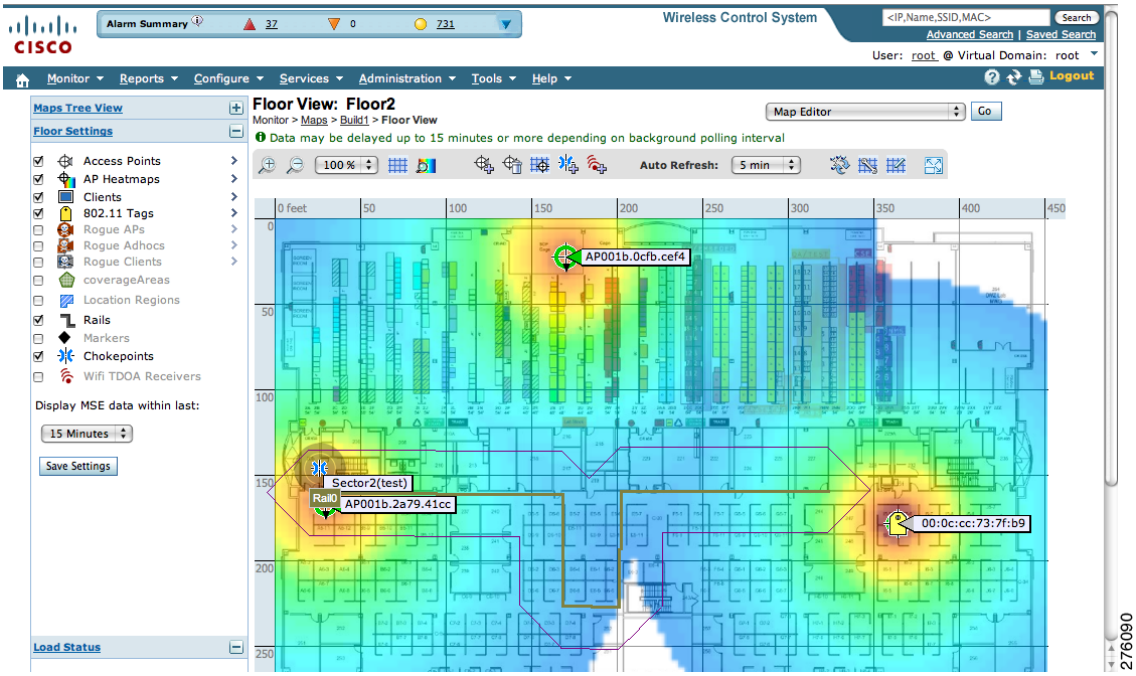


Note To delete a rail line, click on the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the ***X*** icon in the tool bar. The area is removed from the floor map.

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, check the **Rails** check box in the Floor Setting panel if it is not already checked. Rail is shown on the map (see Figure 7-26).

Figure 7-26 Rail Line on Heat Map



Step 10 To resynchronize the Cisco WCS and mobility services engine, choose **Services > Synchronize Services**.

Step 11 At the Synchronize window, select **Network Designs** from the Synchronize drop-down menu and then click **Synchronize**.

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

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 client's license 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. Refer to the *Cisco 3300 Series Mobility Services Engine Licensing and Ordering Guide*: http://www.cisco.com/en/US/products/ps9742/products_data_sheets_list.html

Modifying Tracking Parameters

The mobility services engine can track up to 18,000 clients (including rogue clients, rogue access points, and wired clients) and tags (combined count) with the proper license purchase and mobility services enigne. Updates on the locations of tags and clients 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 and clients that the controller is tracking are seen in Cisco 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 Cisco WCS:

- Enable and disable wired and wireless client stations, active asset tags, and rogue clients 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.

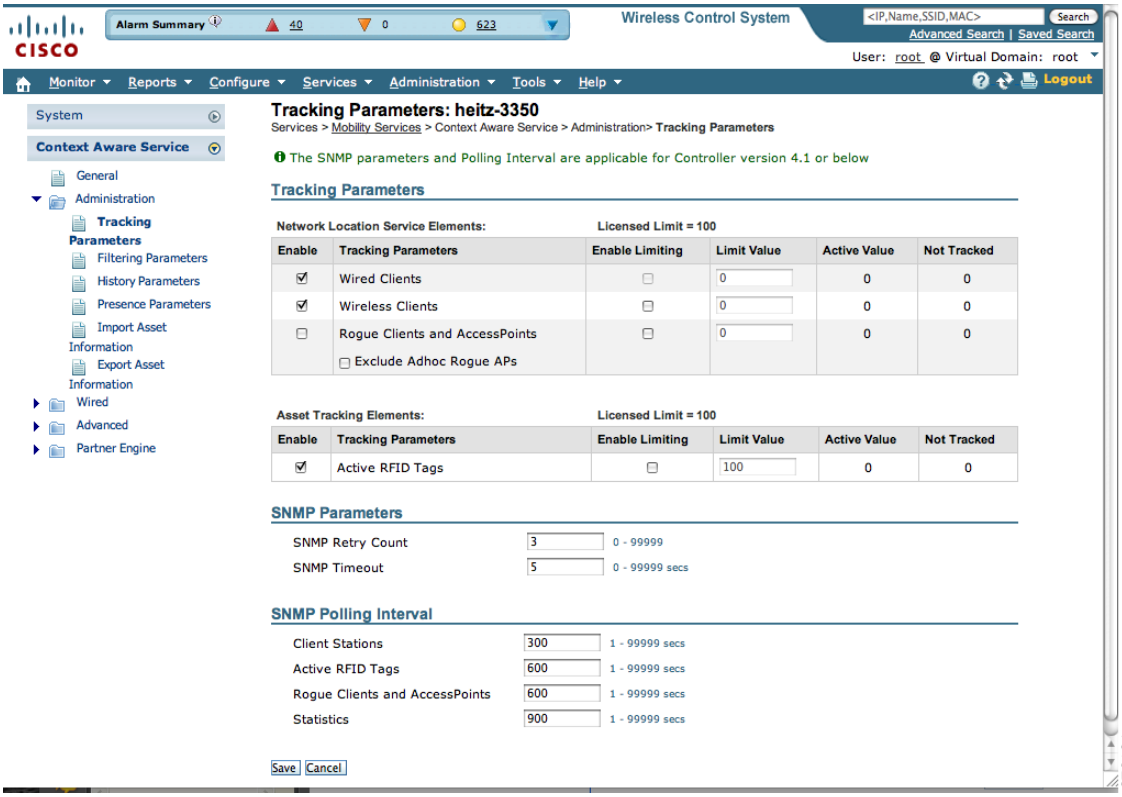
To configure tracking parameters for a mobility services engine, follow these steps:

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

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

Step 3 Choose **Context Aware Service > Administration > Tracking Parameters** to display the configuration options (see Figure 7-27).

Figure 7-27 Context Aware Service > Administration > Tracking Parameters



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

:

Table 7-1 Tracking Parameters

Parameter	Configuration Options
Tracking Parameters	
Wireless Clients	1. Check the **Enable** check box to track client stations. 2. Check 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** Licenses' purchased determine the actual number of tracked clients. **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.

Table 7-1 Tracking Parameters (continued)

Parameter	Configuration Options
Asset Tags	1. Check the **Enable** check box to track asset tags. 2. Check the **Enable Limiting** check box to set a limit on the number of asset tags 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 tags that can be tracked by a Cisco 3350 mobility services engine (Cisco 3310 mobility services engines can support up to 2,000 tags). **Note** Licenses' purchased determine the actual number of tracked tags. **Note** Active Value (display only): Indicates the number of asset tags currently being tracked. **Note** Not Tracked (display only): Indicates the number of asset tags beyond the set limit that are not being tracked.
Rogue Clients and Access Points	1. Check the **Enable** check box to track rogue clients and asset points. 2. Check the **Enable Limiting** check box to set a limit on the number of rogue clients and asset tags 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 rogue clients and access points that can be tracked by a mobility services engine. **Note** Cisco 3350 supports up to 18,000 clients and tags (combined count) and Cisco 3310 supports up to 2,000 clients and tags (combined count). **Note** Licenses' purchased determine the actual number of tracked rogues (clients and access points). 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. **Note** Active Value (display only): Indicates the number of rogue clients and access points currently being tracked. **Note** Not Tracked (display only): Indicates the number of rogue clients and asset tags beyond the set limit that are not being tracked.
Exclude Ad Hoc Rogues	Check 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 Cisco WCS maps or its events and alarms reported.
Wired Clients	1. Check the **Enable** check box to track wired client stations. **Note** **Enable Limiting** is not supported for wired clients. Wired clients are not included within the limit for tracking wireless clients. **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 set limit that are not being tracked.

Table 7-1 Tracking Parameters (continued)

Parameter	Configuration Options
SNMP Parameters are not applicable to mobility services engines.	
SNMP Retry Count	Enter the number of times to retry a polling cycle. Default value is 3. Allowed values are from 1 to 99999 (configurable in controller 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. 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).
Client Stations	Check the **Enable** check box to enable client station polling, and enter the polling interval in seconds. 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).
Asset Tags	Check the **Enable** check box to enable asset tag polling and enter the polling interval in seconds. 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). **Note** Before the location server can collect asset tag data from controllers, you must enable the detection of active RFID tags using the CLI command **config rfid status enable** on the controllers.
Rogue Clients and Access Points	Check the **Enable** check box to enable rogue access point polling and enter the polling interval in seconds. 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	Check the **Enable** check box to enable statistics polling for the location server, 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**.

Modifying Filtering Parameters

In addition to tracking parameters, you can use filtering to limit the number of clients, tags, and rogue clients 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 as noted below:

  – 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 window. 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.

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

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

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

Table 7-2 Filtering Parameters

Parameter	Configuration Options
Exclude Probing Clients	Check the check box to prevent calculating location for probing clients.
Enable Location MAC Filtering	1. Check 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* field), 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* field. 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

You can use Cisco WCS to specify how long to store (archive) histories on client stations, asset tags, and rogue clients and access points. Controllers associated with the mobility services engine send it histories.

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 other functions.

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 7-3 History Parameters

Parameter	Configuration Options
Archive for	Enter the number of days for the mobility services engine to retain a history of each enabled category. Default value is 30. Allowed values are from 1 to 99999.
Prune data starting at.	Enter the interval (hours, minutes) in which the mobility services engine starts data pruning. Allowed values are between 0 and 23 hours, and between 1 and 59 minutes.Default start time is 23 hours and 50 minutes.
...and also every	Enter the interval in minutes after which data pruning starts again. Allowed values are between 0, which means never, and 99900000. Default value is 1440 minutes.
Enable History Logging of Location Transitions for Client Stations, Asset Tags, Rogue Clients and Access Points	Check any or all of the element (client stations, asset tags, and rogue clients and access points) check boxes to log location transitions for the selected element types. When history logging is enabled for an element, a location transition event is logged each time the location of the selected element changes. You can download and review these log events, at the Systems > Log window of a given mobility services engine (Services > Mobility Services > Device Name).

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 an 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, refer to 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**.

Step 2 Select the mobility services engine to which the campus or building is assigned.

Step 3 Choose **Context Aware Service > Administration > Presence Parameters**. The Presence window displays.

Step 4 Check the **Service Type On Demand** check box to enable location presence for Cisco CX clients v5.

Step 5 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 6 Check any or all of the location formats check boxes.

a. Check the **Cisco** check box to provide location by campus, building, floor, and X and Y coordinates. This is the default setting.

b. Check 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. Check the **GEO** check box to provide the longitude and latitude coordinates.

Step 7 By default, the Text check box for Location Response Encoding is checked. It indicates the format of the information when received by the client. There is no need to change this setting.

Step 8 Check the **Retransmission Rule Enable** check box to allow the receiving client to retransmit the received information to another party.

Step 9 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 10 Click **Save**.

Importing Asset Information

To import asset, chokepoint, and TDOA receiver information for the mobility services engine using Cisco 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
- Wi-Fi TDOA receiver format: BuildingName, FloorName, LSMacAddress, LSName, IP Address, X,Y, Z

  X, *Y*, and *Z* represent map coordinates

  LS refers to the TDOA receiver
- chokepoint format: BuildingName, FloorName, CPMacAddress, CPName, IP Address, Range, X,Y, Z, IsPerimeter

  X, *Y*, and *Z* represent map coordinates.

  CP refers to the chokepoint

  IsPerimeter is only required if the chokepoint is a perimeter chokepoint

Step 5 Click **Import**.

Exporting Asset Information

To export asset, chokepoint, and TDOA receiver information from the mobility services engine to a file using Cisco 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
- Wi-Fi TDOA receiver format: BuildingName, FloorName, LSMacAddress, LSName, IP Address, X,Y, Z

  X, *Y*, and *Z* represent map coordinates

  LS refers to the TDOA receiver
- chokepoint format: BuildingName, FloorName, CPMacAddress, CPName, IP Address, Range, X,Y, Z, IsPerimeter

  X, *Y*, and *Z* represent map coordinates.

  IsPerimeter indicates that the chokepoint is a perimeter chokepoint.

  CP refers to the chokepoint.

Step 4 Click **Export**.

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

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

Modifying Location Parameters

You can use Cisco 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:

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

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. Table 7-4 describes each parameter.

Table 7-4 Location Parameters

Parameter	Configuration Options
Calculation time	Check the **Enable** check box to initiate the calculation of the time required to compute location. **Note** This parameter applies only to clients. **Caution** Enable this parameter only under Cisco TAC personnel guidance because it slows down the overall location calculations.
OW Location	Check 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.
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. 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 mobility services engine will always use the access point measurement. Default value is –75. **Note** 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. **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.
Location Filtering	Check the corresponding check box to enable the location filtering. Once enabled, you can set how set limits on how many asset tags, clients, and rogue clients and access points that have their locations tracked and filtered by MAC address and probing clients.
Chokepoint Usage	Check the Enable check box to enable chokepoints to track Cisco compatible tags.

Table 7-4 Location Parameters (continued)

Parameter	Configuration Options
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.

Step 5 Click **Save**.

Enabling Notifications and Configuring Notification Parameters

Enabling Notifications

You can use Cisco 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 Cisco WCS. Refer to "Adding, Deleting, and Testing Event Definitions" section on page 6-2.

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 Cisco 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:

http://www.cisco.com/en/US/products/svcs/ps3034/ps5408/ps5418/serv_home.html

Filtering Northbound Notifications

Filtering on northbound notifications is possible in release 6.0 and later. Similar to user-configured conditional notifications, you can limit which event notifications are forwarded.

You can use filtering to focus on specific notifications important to tag monitoring within your network and to limit the overall number of notifications sent. The latter might preserve processing and storage capacity on the northbound platform.

Note Cisco recommends defining northbound notification filters in the *aes-config.xml* file on the mobility services engine rather than Cisco WCS.

You can filter on six northbound parameters as summarized below:

```
<entry key="send-event-on-location-calc">true</entry>
<entry key="send-event-on-every-beacon">true</entry>
<entry key="send-event-on-vendor">true</entry>
<entry key="send-event-on-emergency">true</entry>
<entry key="send-event-on-chokepoint">true</entry>
<entry key="send-event-on-telemetry">true</entry>
```

To send all six northbound notifications with each beacon, ensure that the *send-event-on-location-calc* and *send-event-on-every-beacon* notification types are marked as true.

To limit the number of notifications, edit (but do not delete) the specific event entry in the *aes-config.xml* file by marking it as *false*.

For example, to send emergency and chokepoint notifications only change the other four notification types (location, beacon, vendor, and telemetry) to *false*.

The modified *aes-config.xml* file would read as:

```
<entry key="send-event-on-location-calc">false</entry>
<entry key="send-event-on-every-beacon">false</entry>
<entry key="send-event-on-vendor">false</entry>
<entry key="send-event-on-emergency">true</entry>
<entry key="send-event-on-chokepoint">true</entry>
<entry key="send-event-on-telemetry">false </entry>
```

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.

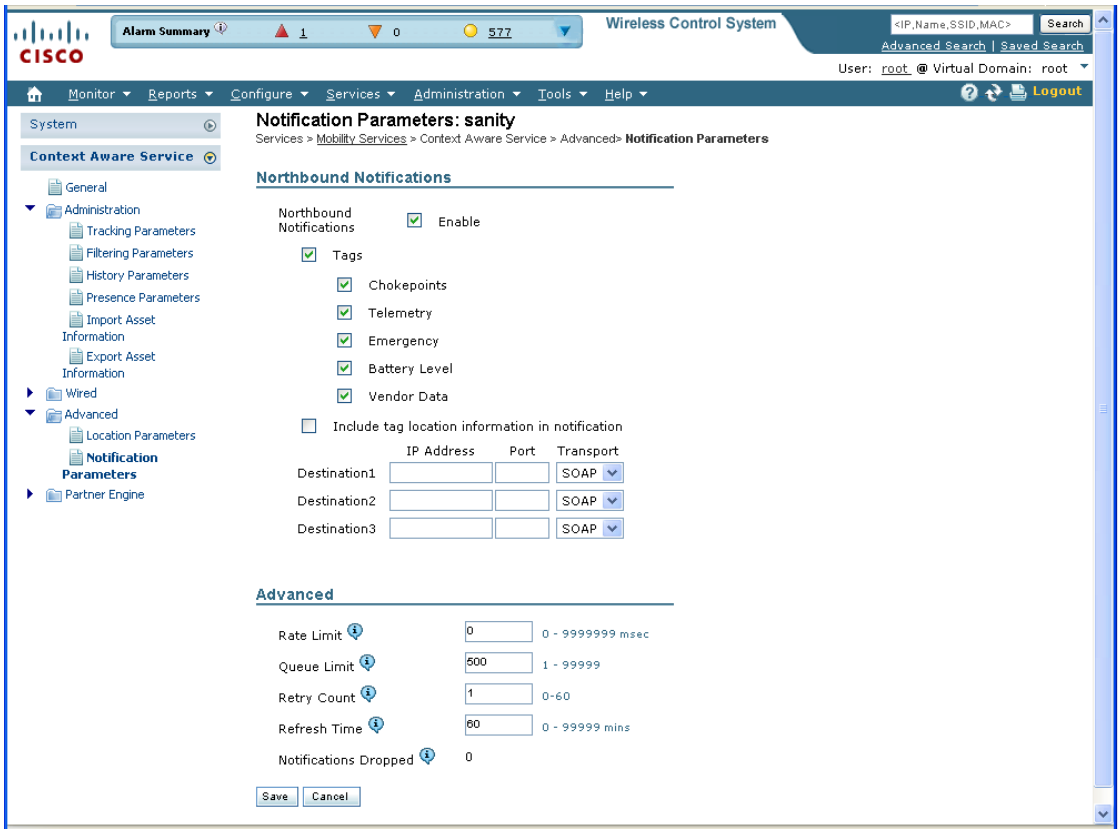
To enable northbound notifications and to configure notification parameters, follow these steps:

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 7-28).

Figure 7-28 Mobility Services Engine > Context Aware Service > Advanced > Notification Parameters



Step 4 Check the **Enable Northbound Notifications** check box to enable the function.

Step 5 Check the **Tags** check box to send tag notifications to third-party applications (northbound).

Note To limit the types of northbound notifications sent for tags, edit the *aes-config.xml* file. Refer to the "Filtering Northbound Notifications" section on page 7-43.

Step 6 Check the **Include tag location information in notification** check box to send the tag location.

Note You can define the type of location information to send for the tag. Options include building, X, Y map coordinates, civic (address, city, state), or GEO (longitude, latitude). Refer to the "Enabling Location Presence" section on page 7-38 section for configuration details.

Step 7 Enter the IP address and port for the system that is to receive the northbound notifications.

Step 8 Select the transport type from the drop-down menu.

Step 9 To modify the notification parameter settings, enter the new value in the appropriate field in the Advanced section of the window. Table 7-5 describes each parameter.

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

Parameter	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).
Queue Limit	Enter the event queue limit for sending notifications. The mobility services engine drops any event above this limit. Default values: Cisco 3350 (18000), Cisco 3310 (5,000), and Cisco 2710 (10,000).
Retry Limit	Enter the number of times to generate an event notification before the refresh time expires. This value ensures, to some extent, that the events that the mobility services engine generates eventually reach Cisco WCS. 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, suppose you enter 120 in this field. If a monitored element goes out of a specified area, the mobility services engine sends a notification. Then, until the notification is cleared, the mobility services engine resends a notification every 60 minutes.
Notifications Dropped	(Read only). The number of event notifications dropped from the queue since startup.

Step 10 Click **Save**.

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.

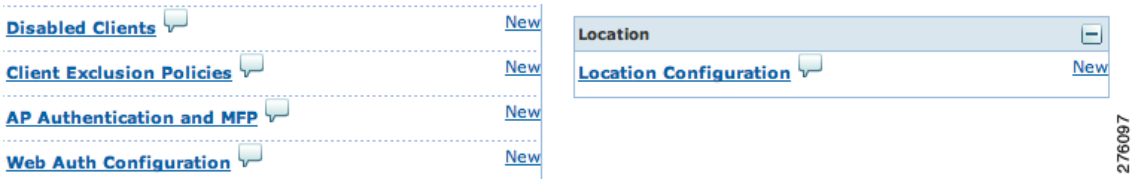
Advanced parameters–Set the RFID tag data timeout value and enable the location path loss configuration for calibrating client multi-band.

To configure a new location template for a controller, follow these steps:

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

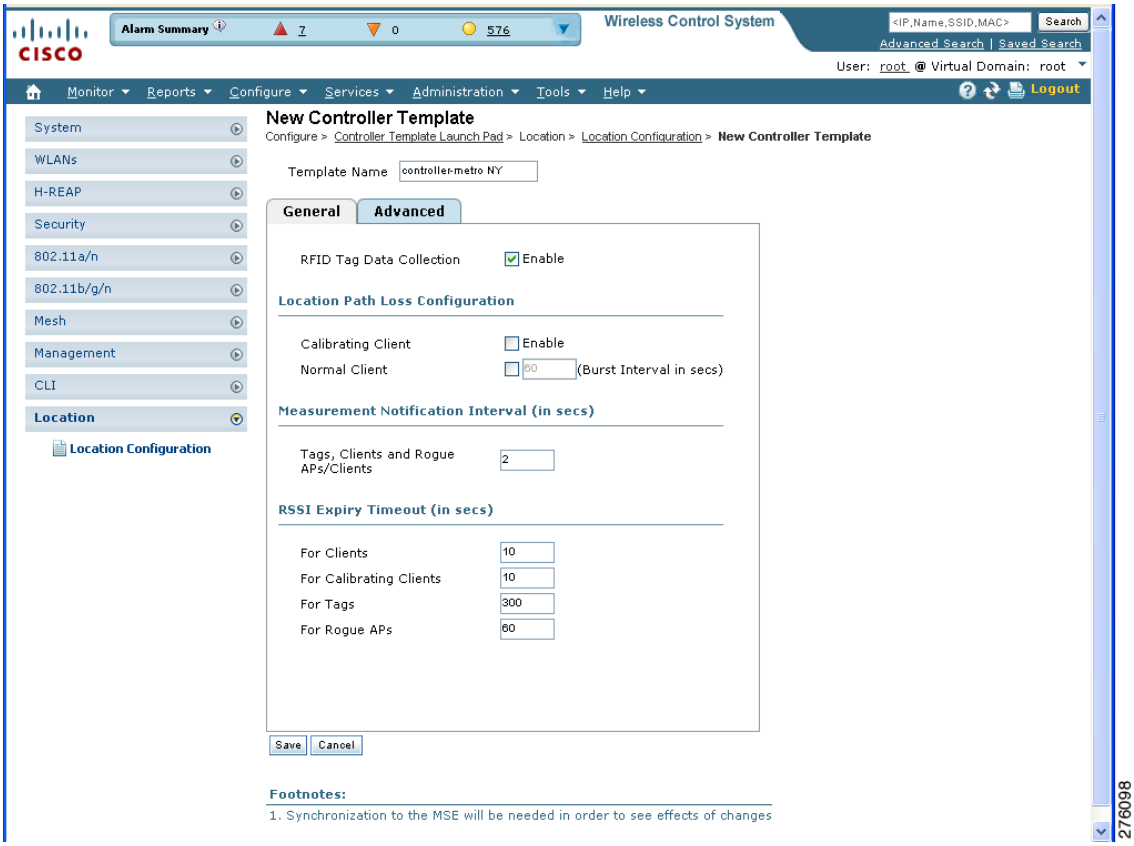
Step 2 Select the **New** (Location Configuration) link under the Location heading to create a new location template (see Figure 7-29).

Figure 7-29 Configure > Controller Template Launch Pad Window



Step 3 At the New template window, enter a name for the location template in the General panel (see Figure 7-30).

Figure 7-30 Location Configuration > New > General Panel



Step 4 At the General panel modify parameters as necessary. Table 7-6 describes each of the parameters.

Table 7-6 General Location Parameters

Parameter	Configuration Options
RFID tag calculation	Check the **Enabled** check box to collect data on tags.
Calibrating Client	Check the **Enabled** 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.
Normal Client	Check 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 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 > 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.
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.
RSSI Expiry Timeout for Rogue APs	Enter a value to set the RSSI timeout value for rogue access points.

Step 5 At the Advanced panel modify parameters as necessary (see Figure 7-31).

Table 7-7 describes each of the advanced parameters.

Figure 7-31 Location Configuration > New > Advanced Panel

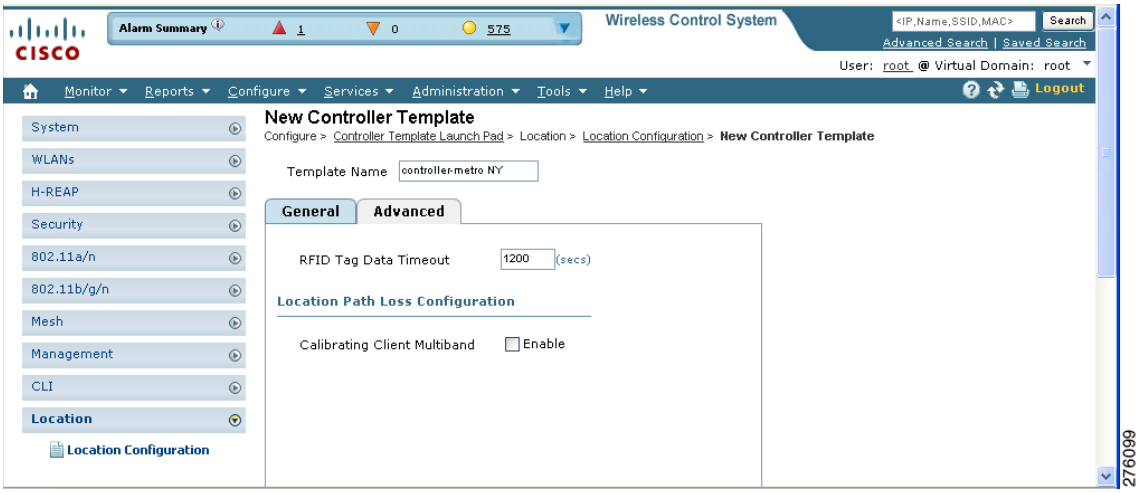


Table 7-7 Advanced Location Parameters

Parameter	Configuration Options
RFID Tag Data Timeout	Enter an RFID tag data timeout value.
Calibrating Client Multiband	Check the **Enabled** check box to send S36 and S60 packets (where applicable) on all channels. Calibrating clients must be enabled on the general panel.

Step 6 Click **Save**.

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:

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

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 Cisco WCS.

Import and display of civic and emergency location information (ELIN) meets specifications of RFC4776 which is outlined at:

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 Catalyst switch.
2. Add Catalyst switch to Cisco WCS
3. Assign Catalyst switch to mobility services engine and synchronize.

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 Configure a civic location for a switch (optional).

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 with **Ctrl-Z**.

Example civic location configuration is noted below.

```
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 switch.

Note The ELIN location length must be between 10 and 25 characters. In the example below, 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 hypens, quotes should be used such as "800 CISCO WAY."

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

Step 7 Configure 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*.

Format for defining port is: **interface {GigabitEthernet | FastEthernet} slot/module/port**

Enter only one location definition on a line, and end the line by entering **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 with **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 Cisco WCS

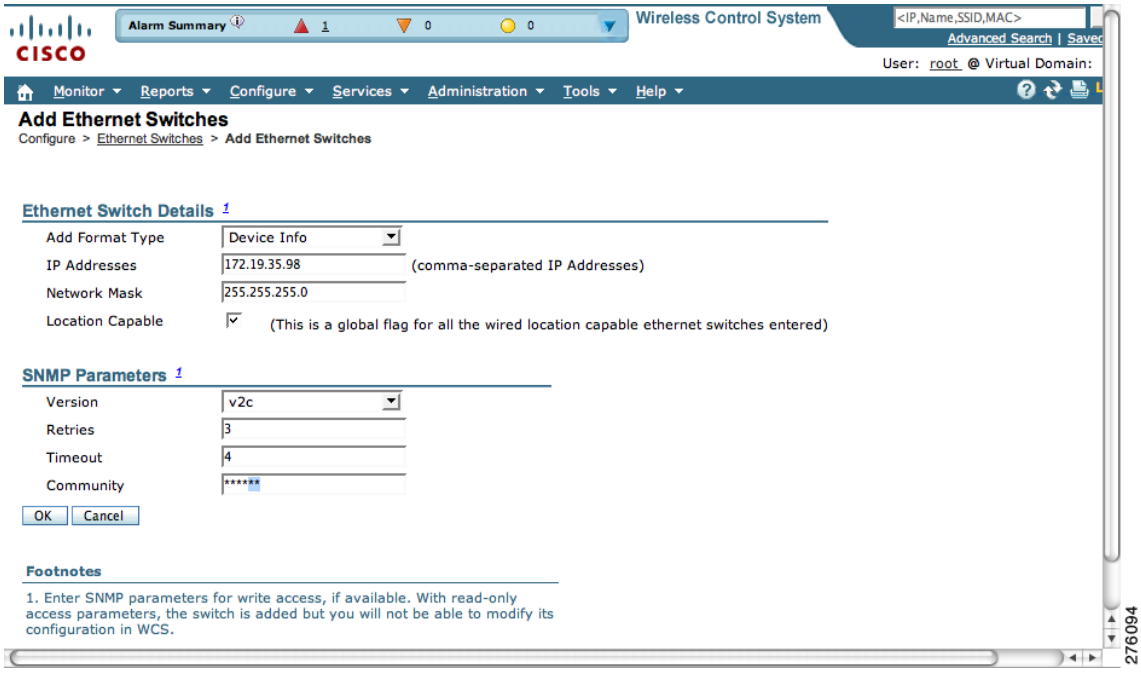
All Catalyst switches must be configured with location service before they are added to Cisco WCS. Refer to the "Configuring a Catalyst Switch" section on page 7-50.

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

Step 1 Choose **Configure > Ethernet Switches**.

Step 2 Select **Add Ethernet Switches** from the Select a command drop-down menu. The entry panel for the switch appears (see Figure 7-32).

Figure 7-32 Configure > Ethernet Switches > Add Ethernet Switches



Step 3 Select **Device Info** or **File** from the Add Format Type drop-down menu.

Note Select **Device Info** to manually enter one or more switch IP addresses. Select **File** to import a file with multiple Catalyst switch IP addresses defined. When File is selected, a pop-up panel appears that defines the accepted format for the imported file.

Step 4 Enter one or more IP addresses.

Step 5 Check the **Location Capable** check box.

Step 6 Select the SNMP version from the drop-down menu if it is different from the default.

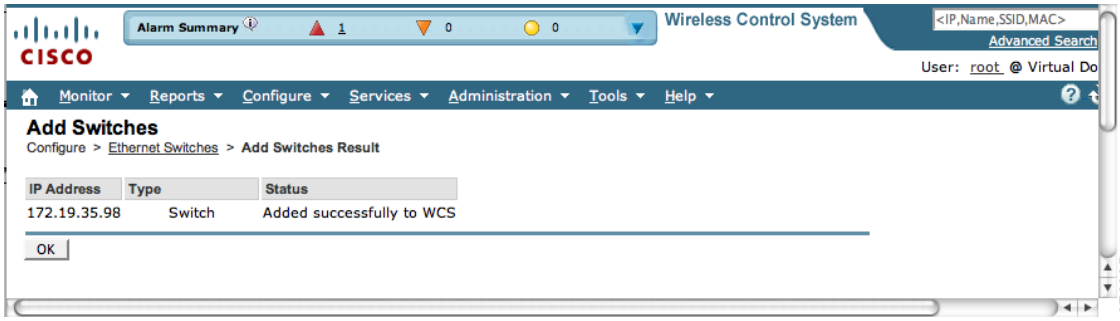
Step 7 No changes are required to the retries and timeout fields.

Step 8 Enter **wired-location** as the SNMP community string.

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 7-50.

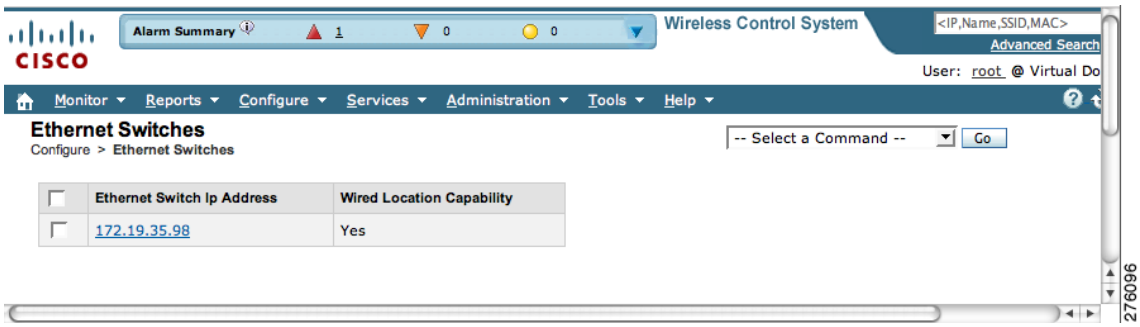
Step 9 Click **OK**. A window confirming successful addition to WCS displays (see Figure 7-33).

Figure 7-33 Add Switches Result Window



Step 10 Click **OK** on the Add Switches Result window, and the newly added switch appears on the Ethernet Switches window (see Figure 7-34).

Figure 7-34 Ethernet Switches Summary Window



Assigning and Synchronizing a Catalyst Switches to a Mobility Services Engine

After adding a Catalyst switch to Cisco 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.

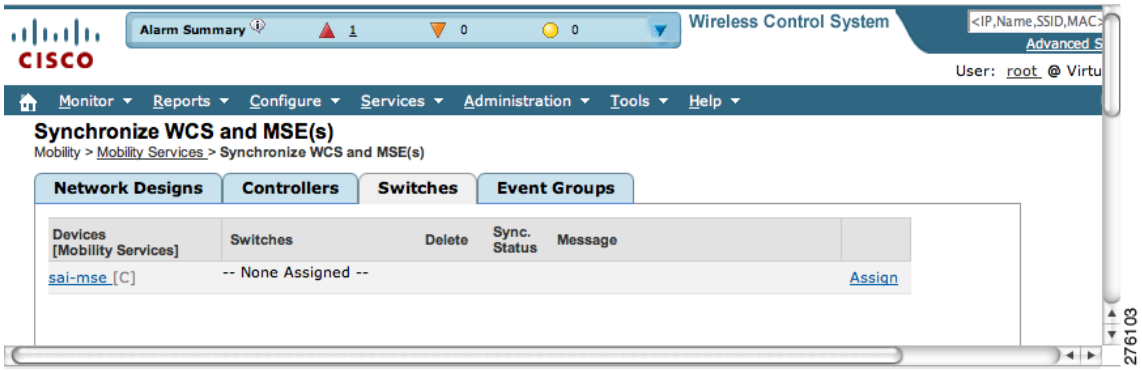
All information on wired switches and wired clients connected to those switches downloads to the mobility services engine.

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

Step 1 Choose **Services > Synchronize**.

Step 2 Select the **Switches** tab (see Figure 7-35).

Figure 7-35 Switches Assignment Tab

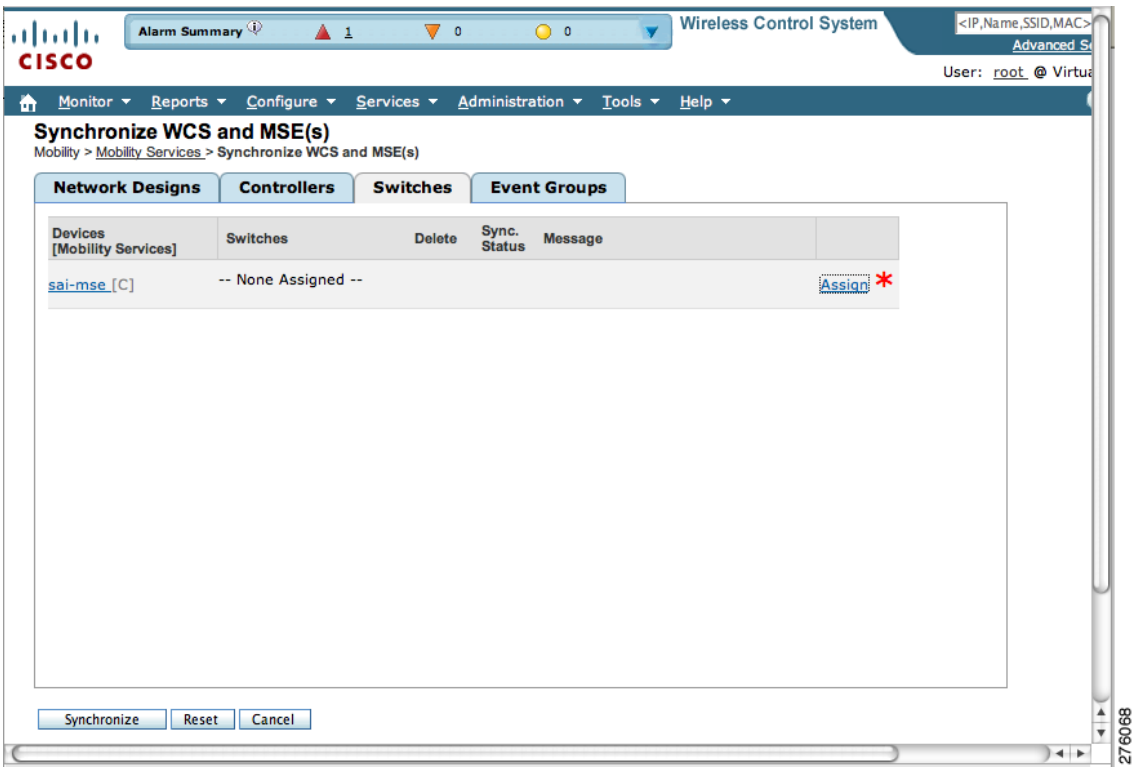


Step 3 Click the **Assign** link to assign a wired switch to a mobility services engine.

Step 4 In the window that appears, check the check box next to each wired switch to which you want the mobility services engine associated. Click **OK**.

An updated switches panel within the Synchronize WCS and MSE(s) window appears (see Figure 7-36). A red asterisk (*) appears next to the Assign link.

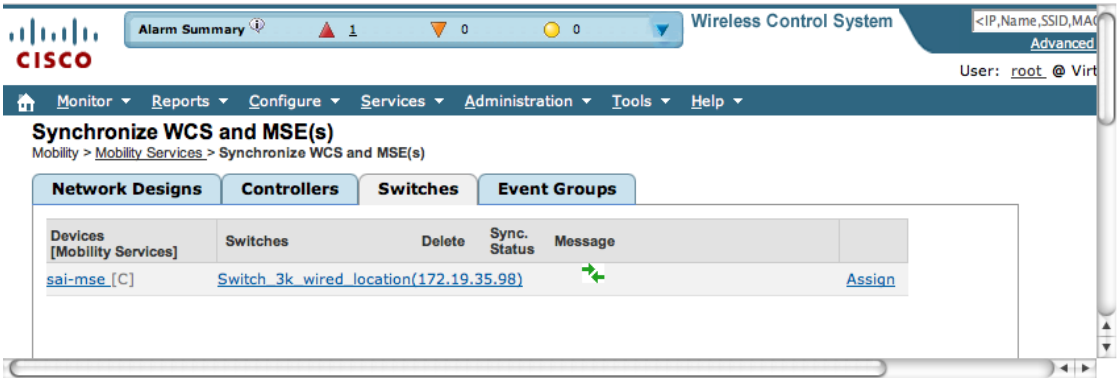
Figure 7-36 Updated Switches Panel Showing Pending Synchronization of Switch Assignment



Step 5 Click **Synchronize**. When synchronized, a screen displays showing two green arrows in the message area (see Figure 7-37).

To undo assignments prior to synchronization, click **Reset**. To go back to the Synchronize WCS and MSE(s) window without making any changes, click **Cancel**.

Figure 7-37 Updated Switches Panel Confirming Synchronization



Step 6 To verify the NMSP connection between the switch and a mobility services engine, refer to "Verifying a NMSP Connection to a Mobility Services Engine".

Note Refer to Chapter 8 for information on monitoring wired switches.

Verifying a 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 window, click the device name link of the appropriate Catalyst switch or controller.

Step 3 Choose **System > Status > NMSP Connection Status** (see Figure 7-38).

Figure 7-38 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.

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