Cisco Context-Aware Service Configuration Guide Release 6.0

June 11, 2009

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-19116-01

CONTENTS

CHAPTER 1

Overview

This chapter describes the role of the Cisco 3300 Series Mobility Services Engine (MSE), a component of the Cisco Context-Aware Mobility (CAM) Solution, within the overall Cisco Unified Wireless Network (CUWN).

Additionally, Context-Aware Software (CAS), a service supported on the mobility services engine and a component of the Context-Aware Mobility Solution, is addressed.

This chapter contains the following sections:

Cisco Context-Aware Mobility Solution Overview

The foundation of the Cisco Context-Aware Mobility Solution is the controller-based architecture of the CUWN. The CUWN includes the following primary components: access points, wireless LAN controllers, the Cisco Wireless Control System (WCS) management application, and the Cisco 3300 Series Mobility Services Engine.

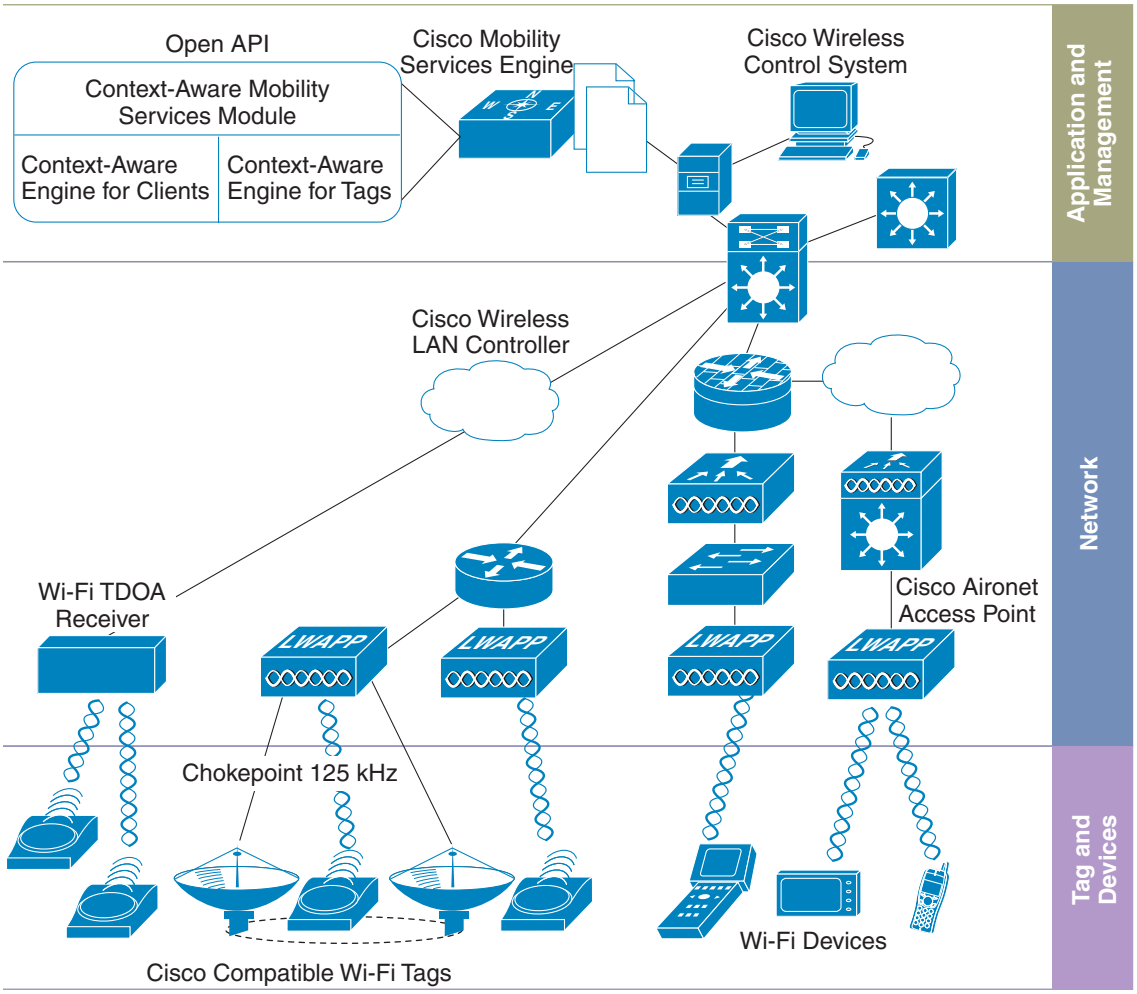
Cisco 3300 Series Mobility Services Engines

The Cisco 3300 Series Mobility Services Engine operates with CAS, which is a component of the Cisco Context-Aware Mobility Solution (see Figure 1-1).

There are two models of the mobility services engine:

- Cisco 3350 Mobility Services Engine
- Cisco 3310 Mobility Services Engine

Figure 1-1 Context-Aware Mobility Solution



CAS

CAS allows a mobility services engine to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as location, temperature, and availability from Cisco access points.

CAS relies on two engines for processing the contextual information it receives. The *Context-Aware Engine for Clients* processes data received from Wi-Fi clients and the *Context-Aware Engine for Tags* processes data received from Wi-Fi tags; these engines can be deployed together or separately depending on the business need.

Licensing for Clients and Tags

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, rogue access points and wired clients).
- For more information on tags, clients, rogue clients, and rogue access points, refer to Chapter 7, "Context-Aware Planning and Verification."
- Licenses for tags and clients are offered in various quantities, ranging from 1,000 to 12,000 units. Up to 18,000 Wi-Fi clients and Wi-Fi tags (combined count) are supported depending on the mobility services engine hardware.
  - Cisco 3350 mobility services engine supports up to 18,000 clients and tags (combined count).
  - Cisco 3310 mobility services engine supports up to 2,000 clients and tags (combined count).
- For details on tag and client licenses, refer to the *Cisco 3300 Series Mobility Services Engine Release Note, Release 6.0* at:

  http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html
- For details on adding client and tag licenses to the mobility services engine, refer to Chapter 2.

Viewing Contextual Information

The collected contextual information can be viewed in GUI format in the Cisco WCS, the centralized WLAN management platform.

Note However, before you can use Cisco WCS, initial configuration for the mobility services engine is required using a command-line (CLI) console session. Refer to *Cisco 3350 Mobility Services Engine Getting Started Guide* and the *Cisco 3100 Mobility Services Engine Getting Started Guide* at the following link: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html.

After its installation and initial configuration are complete, the mobility services engine can communicate with multiple Cisco wireless LAN controllers to collect operator-defined contextual information. You can then use the associated Cisco WCS to communicate with each mobility services engine to transfer and display selected data.

You can configure the mobility services engine to collect data for clients, rogue access points, rogue clients, mobile stations, and active RFID asset tags.

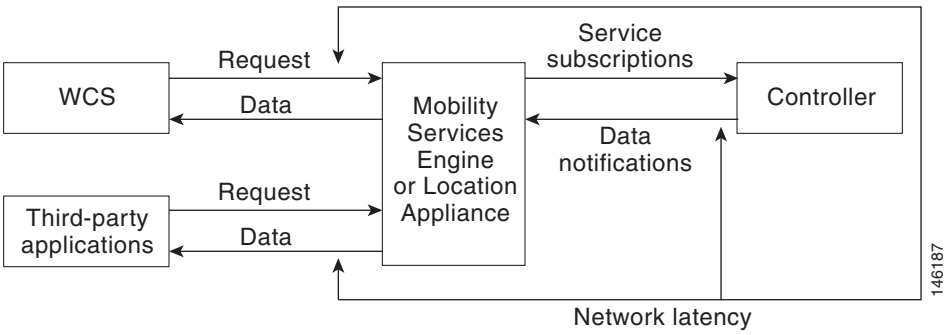
Event Notification

A mobility services engine sends event notifications to registered listeners over the following transport mechanisms:

- Simple Object Access Protocol (SOAP)
- Simple Mail Transfer Protocol (SMTP) mail
- Simple Network Management Protocol (SNMP)
- SysLog

Note Cisco WCS can act as a listener receiving event notifications over SNMP. Without event notification, Cisco WCS and third-party applications need to periodically request location information from location-based services see (see Figure 1-2).

Figure 1-2 Pull Communication Model



The pull communication model, however, is not suitable for applications that require more real-time updates to location information. For these applications, you can configure the mobility services engine push event notifications when certain conditions are met by the registered listeners.

Configuration and Administration

You can use Cisco WCS to perform different configuration and administrative tasks, including adding and removing a mobility services engine, configuring mobility services engine properties and managing users and groups as summarized below.

Adding and Deleting a Mobility Services Engine

You can use Cisco WCS to add and delete a mobility services engine within the network. You can also define the service supported on the mobility services engine. Refer to Chapter 2, "Adding and Deleting Mobility Services Engines and Licenses," for configuration details.

Editing Mobility Services Engine Properties

You can use Cisco WCS to configure the following parameters on the mobility services engine. Refer to the Chapter 4, "Configuring and Viewing System Properties," for configuration details.

- General Properties: Enables you to assign a contact name, username, password, and HTTP for the mobility services engine.
- NMSP Parameters: Enables you to modify Network Mobility Services Protocol (NMSP) parameters such as echo and neighbor dead intervals as well as response and retransmit periods. NMSP is the protocol that manages communication between the mobility services engine and the controller or a location-capable Catalyst switch. Transport of telemetry, emergency, and chokepoint information between the mobility services engine and the controller is managed by this protocol.
- Active Sessions: Enables you to view active user sessions on the mobility services engine.
- Trap Destinations: Enables you to specify which Cisco WCS or Cisco Security Monitoring, Analysis and Response System (CS-MARS) network management platform is the recipient of SNMP traps generated by the mobility services engine.
- Advanced Parameters: Enables you to set the number of days events are kept, set session time out values, set an absent data interval cleanup interval, and enable or disable Advanced Debug.

Editing CAS Properties

You can use Cisco WCS to configure the following parameters for CAS. Refer to Chapter 7, "Context-Aware Planning and Verification," for configuration details.

Location of an element (client, tag, rogue client or rogue access point) is one of the components that is retrieved from access points by the Context-Aware Software (CAS) installed on a mobility services engine. CAS also retrieves contextual information such as temperature and asset availability about a client or tagged asset from access points.

Note Context-Aware Software incorporates and expands the function of Cisco location-based services software.

- Tracking Parameters: Enables you to define the mobile assets (such as client stations, active asset tags; and rogue clients and access points) that you want to actively track, set limits on how many of a specific mobile asset you want to track, and disable tracking and reporting of ad hoc rogue clients and access points.
- Filtering Parameters: Enables you to define filters to exclude probing clients as well as tags and non-probing clients based on their MAC addresses.
  - Probing clients are clients that are associated to another controller but whose probing activity causes them to be seen by another controller and counted as a client by the *probed* controller as well as its *primary* controller.
- History Parameters: Enables you to specify how often the mobility services engine collects historical data on client station, rogue access point, and asset tags from controllers to manage the amount of data stored on the mobility services engine hard drive.
- Presence Parameters: Enables you to enable location presence on a mobility services engine to provide expanded Civic (city, state, postal code, country) and GEO (longitude, latitude) location information beyond the Cisco default setting (campus, building, floor, and X, Y coordinates). This information can then be requested by clients on a demand basis for use by location-based services and applications.
- Import and Export Asset Information: Enables you to import a file of formatted asset information from an external server and to export asset information to an external server.
- Import Civic Information: Enables you to import a file with civic information for use by the presence parameter for expanded location information.

- Location Parameters: Enables you to specify whether the mobility services engine retains its calculation times and how soon the mobility services engine deletes its collected RSSI measurement times. It also enables you to apply varying smoothing rates to manage location movement of an element.
- Notification Parameters: Enables you to define how often notifications are generated or resent by the mobility services engine. You can also enable forwarding of northbound notifications for tags to third-party applications.

Managing Users and Groups

You can use Cisco WCS to add, delete, and edit user session and user group parameters as well as add and delete host access records. Refer to Chapter 5, "Managing Users and Groups," for configuration details.

Mobility Services Engine Synchronization

Cisco WCS pushes network designs (logical maps of elements), controllers and event definitions to the mobility services engine to maintain accurate location information between the mobility services engine and controller. Cisco WCS provides you with two ways to synchronize: manual and automatic (auto-sync). Refer to Chapter 3, "Synchronizing Mobility Services Engines," for specifics.

Context-Aware Planning and Verification

To plan and optimize access point deployment, you can use Cisco WCS to calibrate linear or data points. Additionally, you can analyze the location accuracy of non-rogue and rogue clients and asset tags on an area or floor map using the accuracy tool, and you can use chokepoints to enhance location accuracy for tags. Refer to Chapter 7, "Context-Aware Planning and Verification," for specifics.

Monitoring Capability

You can use Cisco WCS to monitor alarms, events, and logs generated by mobility services engine. You can also monitor the status of mobility services engines, clients, and tagged assets. Additionally, you can generate a utilization report for the mobility services engine to determine CPU and memory utilization as well as counts for clients, tags and rogue access points and clients. Refer to Chapter 8, Chapter 8, "Monitoring the System and Services," for specifics.

Maintenance Operations

You can back up mobility services engine data to a predefined FTP folder on Cisco WCS at defined intervals, and restore the mobility services engine data from that Cisco WCS. Other mobility services engine maintenance operations that you can perform include: downloading new software images to all associated mobility services engines from any Cisco WCS station, defragmenting the mobility services engine database, restarting a mobility services engine, shutting down a mobility services engine and clearing mobility services engine configurations. Refer to Chapter 9, "Performing Maintenance Operations," for specifics.

Note Details on recovering GRUB and root passwords for the mobility seevices engine using the command-line interface (rather than Cisco WCS) is also addressed in Chapter 9.

System Compatibility

Note Refer to the *Cisco 3300 Mobility Services Engine Release Note* for the latest system (controller, WCS, mobility services engine) compatibility information, feature support, and operational notes for your current release at:
http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

CHAPTER 2

Adding and Deleting Mobility Services Engines and Licenses

This chapter describes how to add and delete a Cisco 3300 Series Mobility Services Engine from Cisco WCS.

This chapter contains the following sections:

Adding a Mobility Services Engine to Cisco WCS

To add a mobility services engine to Cisco WCS, log into WCS and follow these steps:

Step 1 Verify that you can ping the mobility service engine.

Step 2 Choose **Services > Mobility Services** to display the Mobility Services window.

Step 3 From the Select a command drop-down menu, select **Add Mobility Services Engine**. Click **Go**.

Step 4 In the Device Name field, enter a name for the mobility services engine.

Step 5 In the IP Address field, enter the mobility services engine's IP address.

Step 6 (Optional) In the Contact Name field, enter the name of the mobility services engine administrator.

Step 7 In the User Name and Password fields, enter the username and password for the mobility services engine.

The default username and password are both *admin*.

Note If you changed the username and password during the automatic installation script, enter those values here. If you did not change the default passwords, Cisco strongly recommends that you rerun the automatic installation script and change the username and password.

Step 8 Check the **Enable** HTTP check box to allow communication between the mobility services engine and third-party applications.

Step 9 Click **Next**. The Select Mobility Service window appears.

Step 10 To enable a service on the mobility services engine, check the check box next to that service.

Note A mobility services engine can support multiple services.

Step 11 Click **Save**.

Note After adding a new mobility services engine, you can synchronize network designs (campus, building, and outdoor maps), controllers, switches (specific Catalyst Series 3000 and 4000 only), and event groups for the mobility services engine and Cisco WCS. Refer to Chapter 3, "Synchronizing Mobility Services Engines".

Note For a list of Catalyst Series 3000 and 4000 switches that can operate with a mobility services engine, refer to the "Enabling Location Services on Wired Switches and Wired Clients" section on page 7-49.

Deleting a Mobility Services Engine from the Cisco WCS

To delete one or more mobility services engines from the Cisco WCS database, follow these steps:

Step 1 Choose **Services > Mobility Services** to display the Mobility Services window.

Step 2 Select the mobility services engine to be deleted by checking the corresponding check box.

Step 3 From the Select a command drop-down menu, select **Delete Service(s).** Click **Go**.

Step 4 Click **OK** to confirm that you want to delete the selected mobility services engine from the WCS database.

Step 5 Click **Cancel** to stop deletion.

Registering Client and wIPS Product Authorization Keys

You receive a product authorization key (PAK) when you order a client, wIPs, or tag license from Cisco. You must register the PAK to receive the license file for install on the mobility services engine. License files are emailed to you after successfully registering a PAK.

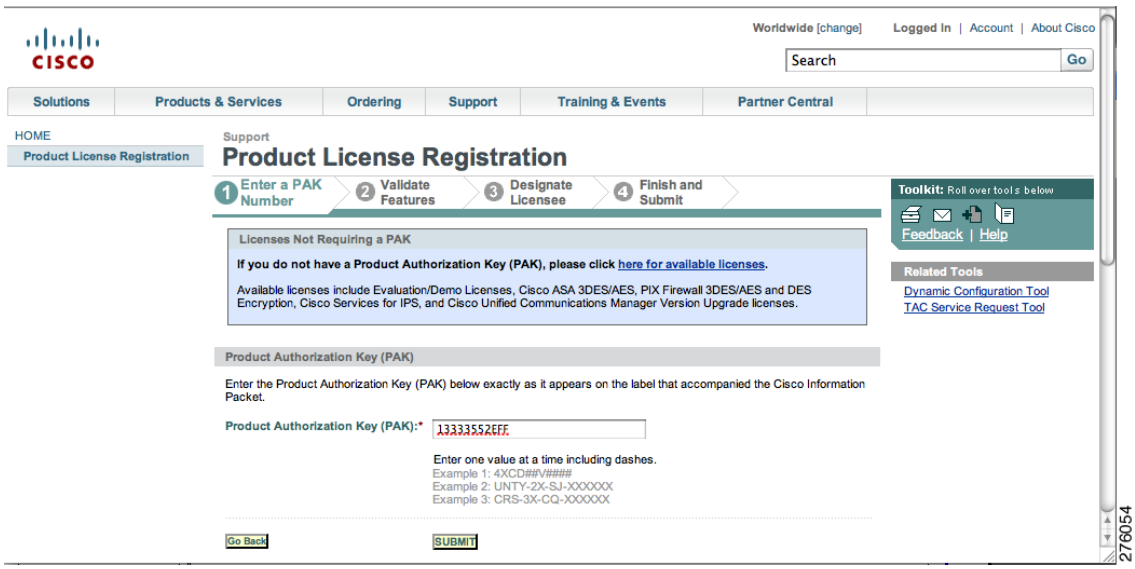
Client and wIPS PAKs are registered with Cisco.

Note Tag PAKs are registered with AeroScout. Refer to "Registering Tag PAKs" section on page 2-8.

To register a product authorization key (PAK) to obtain a license file for install, follow these steps:

Step 1 Open a browser window and enter www.cisco.com/go/license. Enter the PAK and click **SUBMIT** (see Figure 2-1).

Figure 2-1 Enter PAK Number Window



Step 2 Verify the license purchase. Click **Continue** if correct (see Figure 2-2). The licensee entry window appears (see Figure 2-3).

Note If the license is incorrect, click **TAC Service Request Tool** link (right) to report the problem.

Figure 2-2 Validate License Purchase Window

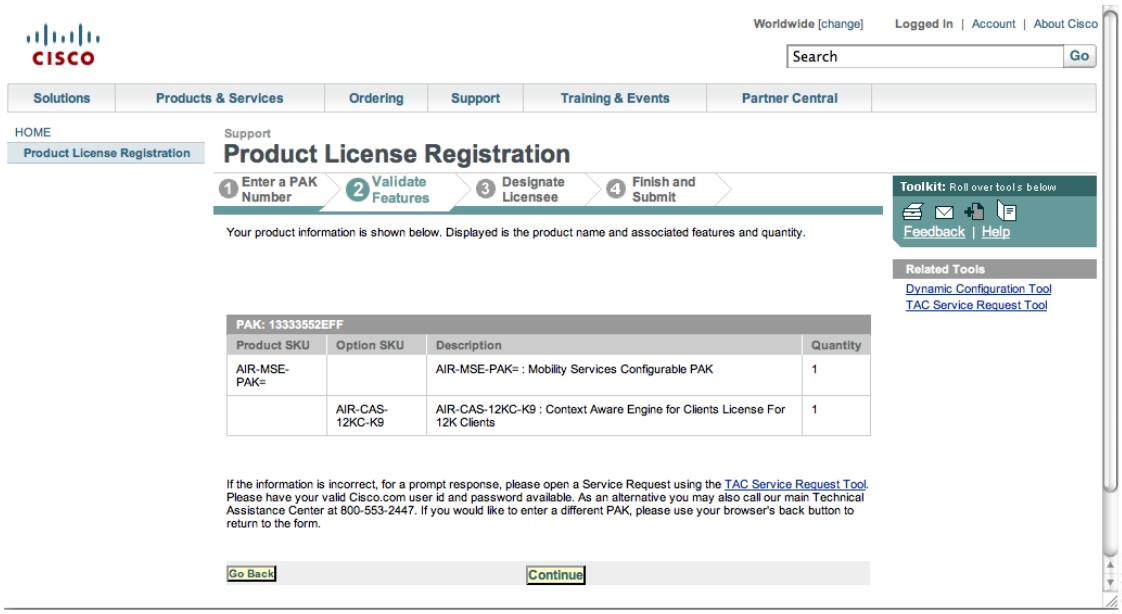
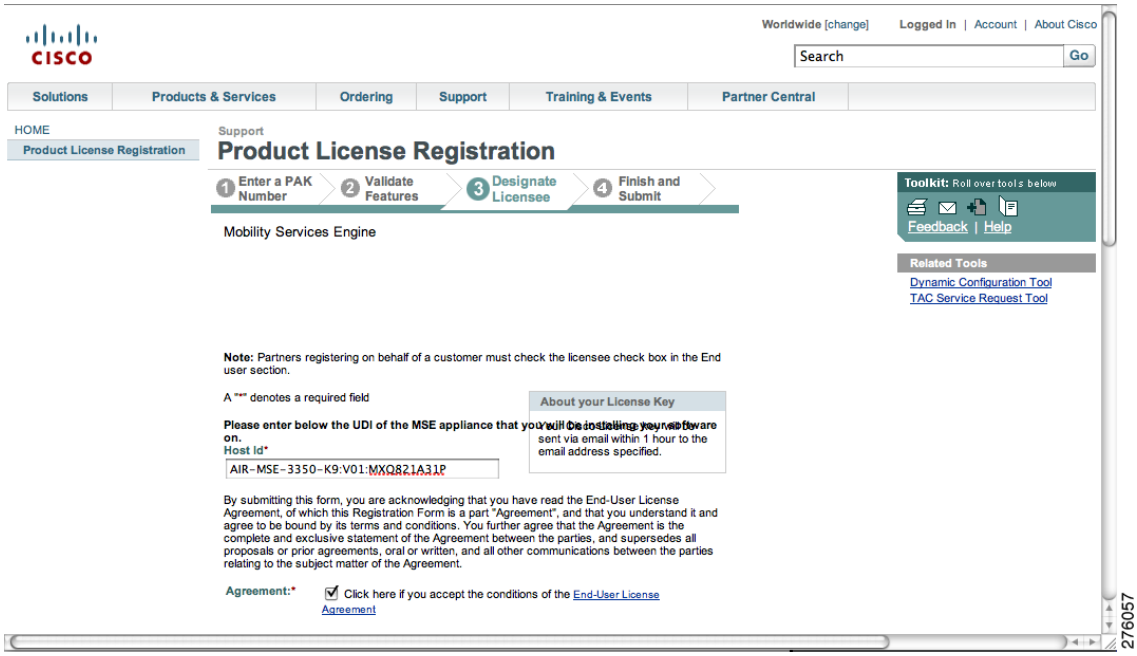


Figure 2-3 Designate Licensee Window, 1 of 2



Step 3 At the Designate Licensee window:

a. Enter the mobility service engine's UDI in the host ID field. This is the mobility services engine on which the license will be installed.

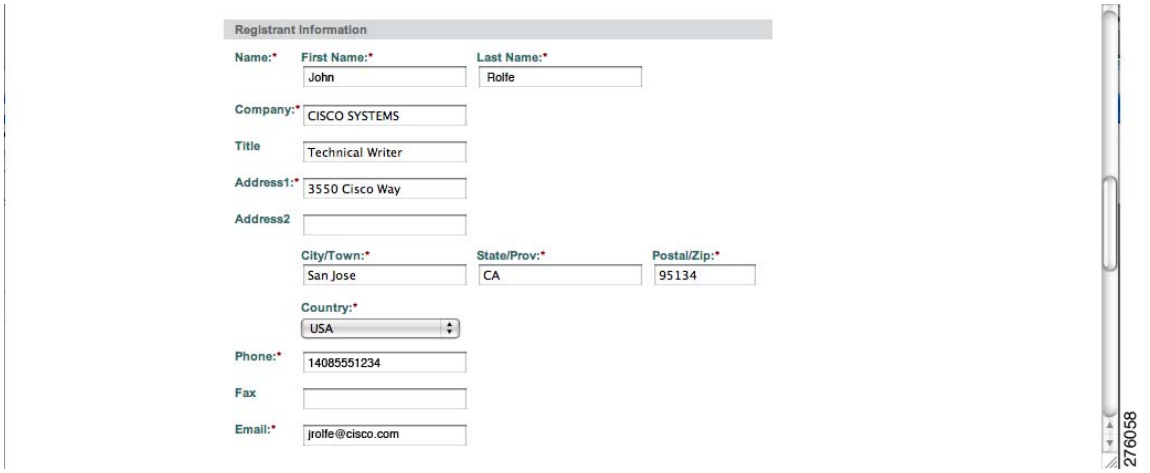
Note UDI information for a mobility services engine is found on the General Properties panel at Services > Mobility Services Engine > *Device Name* > *System*.

b. Check **Agreement** check box. Registrant information appears beneath the Agreement check box (see Figure 2-4).

Modify information as necessary.

Note Ensure that the phone number does not include any characters in the string for the registrant and end user. For example, enter 408 555 1212 rather than 408.555.1212 or 408-555-1212.

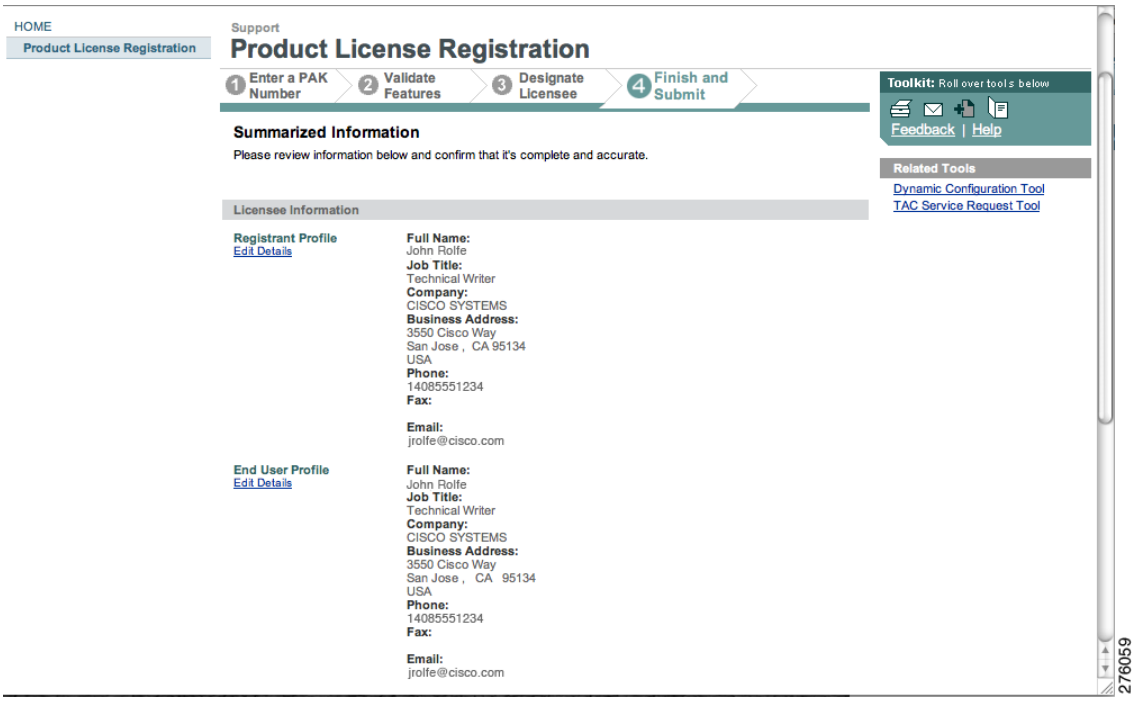
Figure 2-4 Designate Licensee Window, 2 of 2



c. If registrant and end user are not the same person, check **Licensee (End-User)** check box beneath registrant information and enter the end user's information.

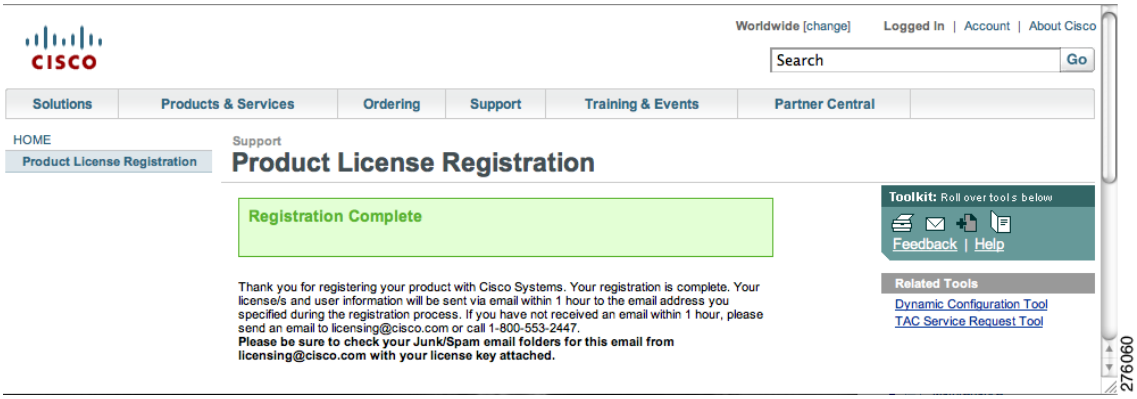
d. Click **Continue**. A summary of entered data appears (see Figure 2-5).

Figure 2-5 Finish and Submit Window



Step 4 At the Finish and Submit window, review registrant and end user data. Click **Edit Details** to correct information. Click **Submit**. A confirmation window appears (see Figure 2-6).

Figure 2-6 Registration Confirmation Window



Installing Client and wIPS License Files

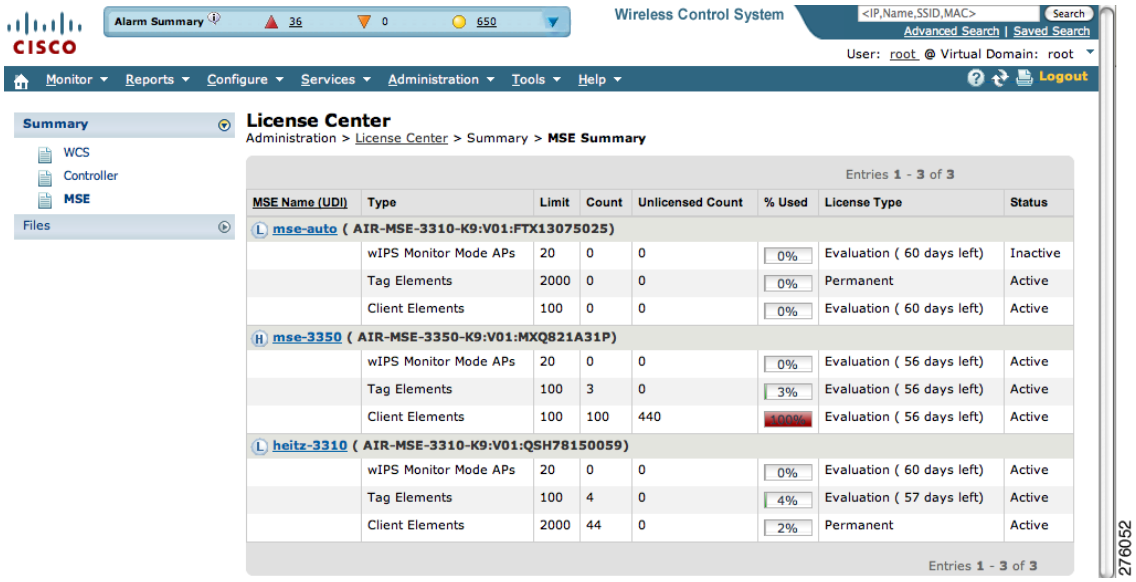
You can install client and wIPS licenses from Cisco WCS.

Tag licenses are installed using the AeroScout System Manager. Refer to "Installing Tag Licenses" section on page 2-8.

To add a client or wIPS license to Cisco WCS after registering the PAK, follow these steps:

Step 1 Choose **Administration > License Center** (see Figure 2-7).

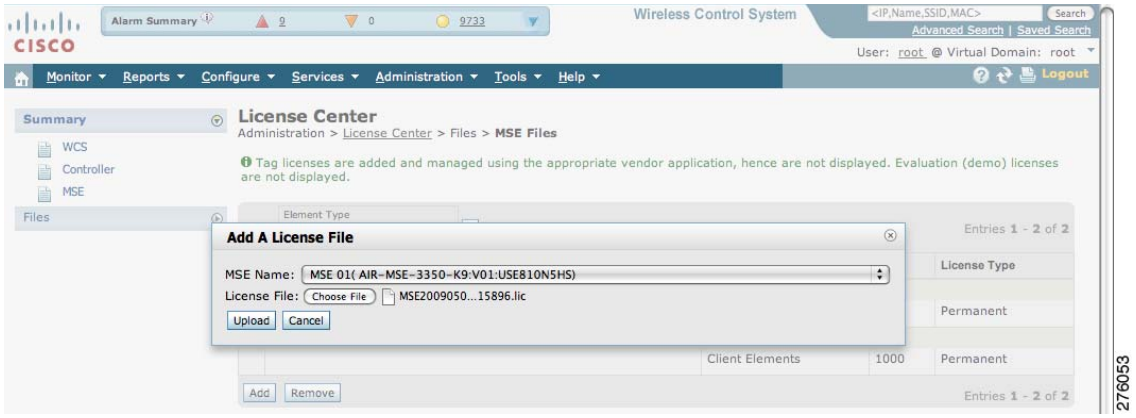
Figure 2-7 Administration > License Center Window



Step 2 Choose **Files > MSE Files** (left panel).

Step 3 Click **Add**. A pop-up entry panel appears (see Figure 2-8).

Figure 2-8 Add a License File Panel



Step 4 Select **MSE Name**.

Note Verify that the UDI of the selected mobility services engine matches the one you entered when registering the PAK.

Step 5 Click **Choose File** to browse and to select the license file.

Step 6 Click **Upload**. Newly added license appears in MSE license file list.

Registering Tag PAKs

To register tags at the AeroScout web site, follow these steps:

Step 1 Open a browser and enter http://www.aeroscout.com/content/support.

Step 2 Login if you have an existing account or click **Create New Account** to create a login a username and password.

If created a new account, you will receive a notification email with your username and password.

Step 3 After logging in, click **Register Products Purchased from Cisco** on the Home tab.

To register your product, you need the following information: PAK number, MSE ID (MSE serial number (S/N)) and Installation Type.

You will receive an email message from AeroScout that confirms registration.

Your PAK number is verified within 2 business days by email. If your PAK number is found to be invalid you must register again with a valid PAK number.

Installing Tag Licenses

After successfully registering your PAK, you will receive an email with your license key and instructions on how to download context-aware software and a copy of the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User's Guide*.

Refer to the users guide for details on installed your tag licenses.

http://support.aeroscout.com

CHAPTER 3

Synchronizing Mobility Services Engines

This chapter describes how to synchronize Cisco wireless LAN controllers and Cisco WCS with mobility services engines.

This chapter contains the following sections:

Synchronizing Cisco WCS and Mobility Services Engines

This section describes how to synchronize Cisco WCS and mobility services engines manually and automatically.

After adding a mobility services engine to Cisco WCS, you can synchronize network designs (campus, building, and outdoor maps), controllers (name and IP address), specific Catalyst Series 3000 and 4000 switches, and event groups with the mobility services engine.

- Network Design—is a logical mapping of the physical placement of access points throughout facilities. A hierarchy of a single campus, the buildings that comprise that campus, and the floors of each building constitute a single network design.
- Controller—is a selected controller that is associated and regularly exchanges location information with a mobility services engine. Regular synchronization ensures location accuracy.
- Switches (wired)—are wired Catalyst switches that provide an interface to wired clients on the network. Regular synchronization ensures that location tracking of wired clients in the network is accurate.
  - The mobility services engine can be synchronized with Catalyst stackable switches (3750, 3750-E, 3560, 2960, IE-3000 switches), switch blades (3110, 3120, 3130, 3040, 3030, 3020), and switch ports.
  - The mobility services engine can also be synchronized with the following Catalyst 4000 series: 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
- Event Groups—are a group of predefined events that define triggers that generate an event. Regular synchronization ensures that the latest defined events are tracked.

Note Be sure to verify software compatibility between the controller, Cisco WCS, and the mobility services engine before synchronizing. Refer to the latest mobility services engine release note at the following link: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html.

Note Communication between the mobility services engine and Cisco WCS and the controller is in universal time code (UTC). Configuring NTP on each system provides devices with the UTC time. The mobility services engine and its associated controllers must be mapped to the same NTP server and the same Cisco WCS server. An NTP server is required to automatically synchronize time between the controller, Cisco WCS, and the mobility services engine.

To synchronize network designs, a controller, a Catalyst switch, or event group with the mobility services engine, follow these steps:

Step 1 Choose **Services > Synchronize Services** to display the Mobility Services > Synchronize WCS and MSE(s) window.

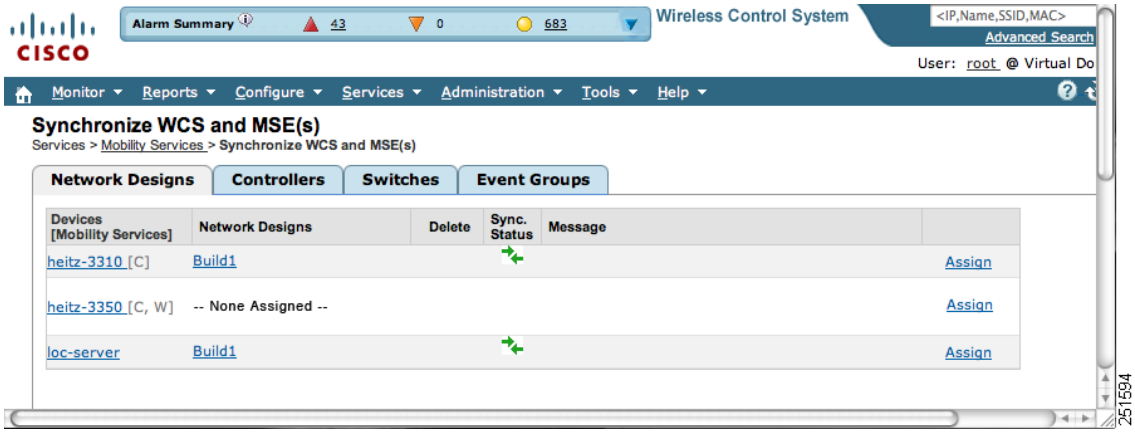
A four-tabbed panel appears with the following headings: Network Designs, Controllers, Switches, and Event Groups.

Note A Devices column appears on all four tabs and lists the name of the mobility services engine and the active services on that device. Services are noted in brackets next to the device name. Services supported are Context-Aware Software [C], and Wireless Intrusion Prevention System [W].

Step 2 Select the appropriate tab (network designs, controllers, switches, or event groups).

a. To assign a network design to a mobility services engine, click the **Network Designs** tab (see Figure 3-1).

Figure 3-1 Services > Synchronize Services > Network Designs Window



1. Click the **Assign** link for the appropriate network design.

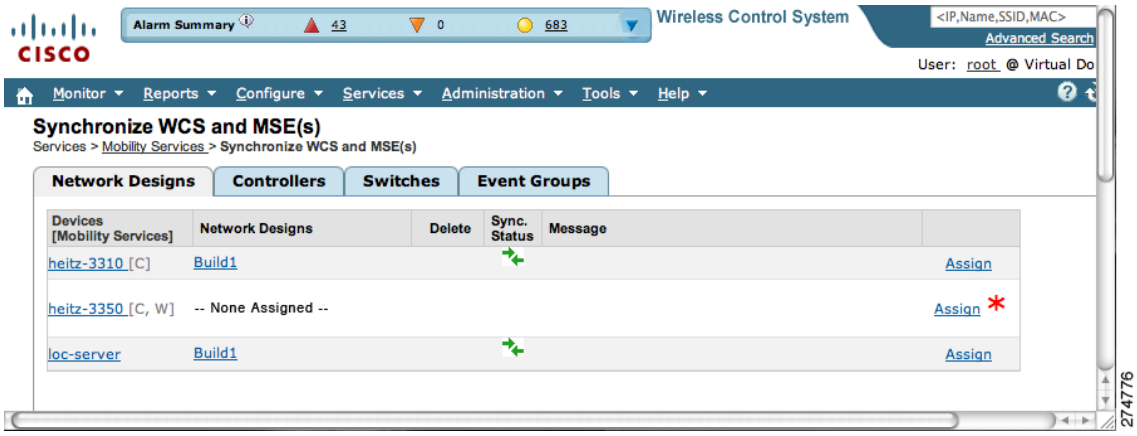
Note A network design might comprise a large campus with several buildings, each monitored by a different mobility services engine. Therefore, you might need to assign a single network design to multiple mobility services engines.

2. In the Network Designs window that appears, check the check box of each network design that you want to applyto the mobility services engine. Click **OK** when the selection is complete.

   A red asterisk (*) appears next to the Assign link (see Figure 3-2).

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

Figure 3-2 Services > Synchronize Services > Network Designs Window



3. Click **Synchronize** to update the mobility services database.

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

b. To associate a mobility services engine with a controller, click the **Controllers** tab.

1. In the Controllers window that appears click the **Assign** link for that mobility services engine.
2. In the window that appears (see Figure 3-3), check the check box next to the appropriate controller. Click **OK**.

   The window in Figure 3-4 appears. A red asterisk (*) appears next to the Assign link

Note The selected controller must support the service that is configured on the mobility services engine (as noted in the supported services column). If it does not, a warning message appears when you click **OK**.

Note Controller names must be unique for synchronizing with a mobility services engine. If you have two controllers with the same name, only one controller synchronizes.

Figure 3-3 Controller Selection Window

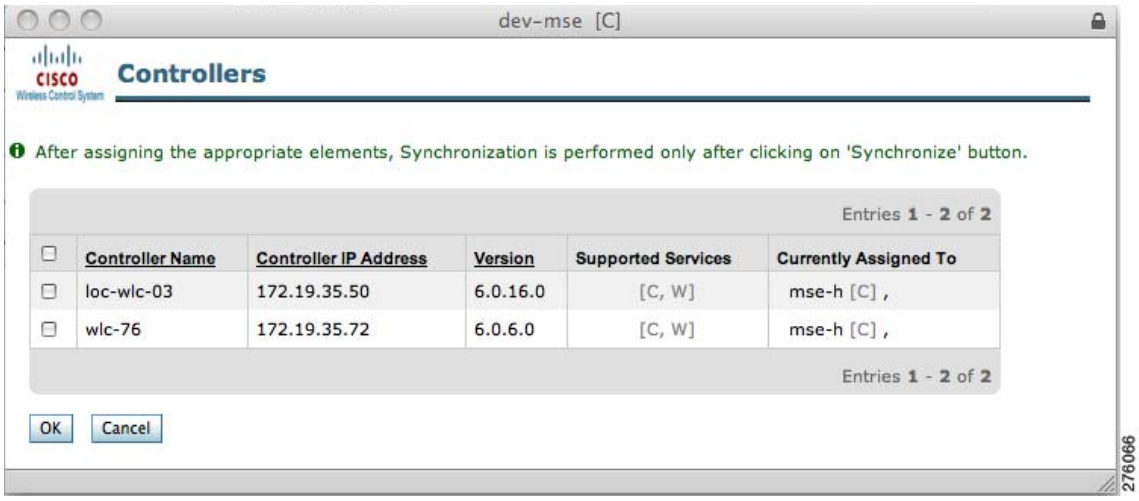
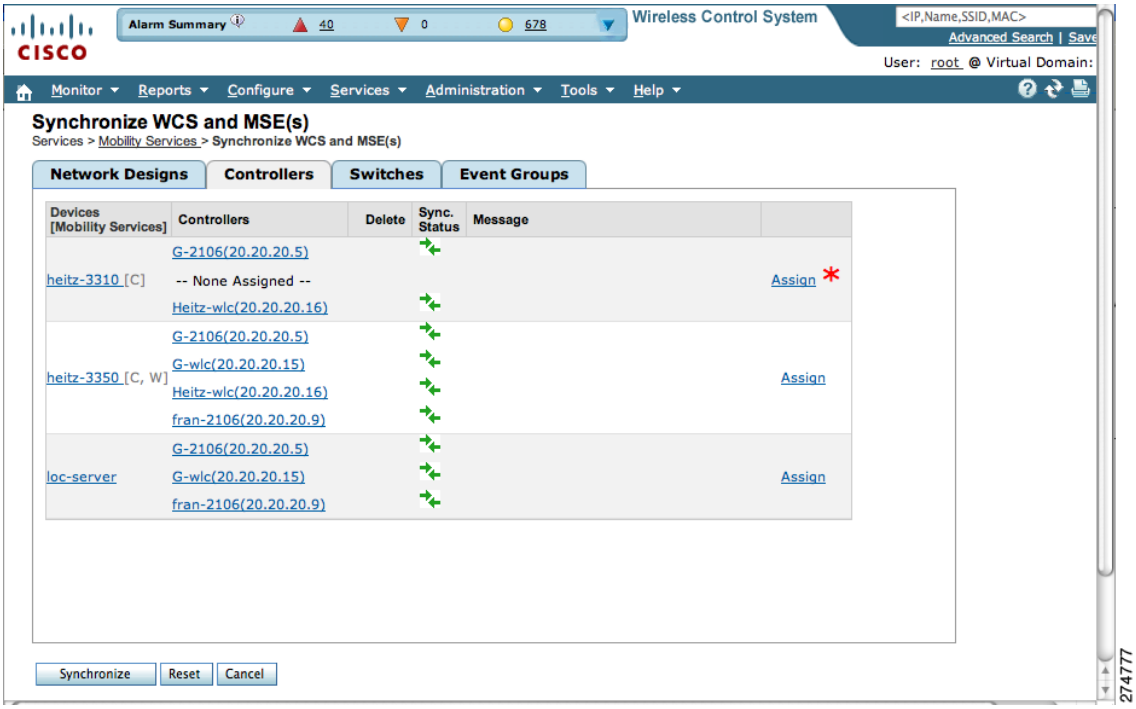


Figure 3-4 Services > Synchronize Services > Controllers Window



3. Click **Synchronize** to update the mobility services database.

   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**.

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

c. To assign a Catalyst switch to a mobility services engine, click the **Switches** tab (see Figure 3-5).

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 Cisco WCS and the mobility services engine is established.

All information (such as IP address, MAC, and civic address) on the wired switches and the wired clients connected to them downloads to the mobility services engine.

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

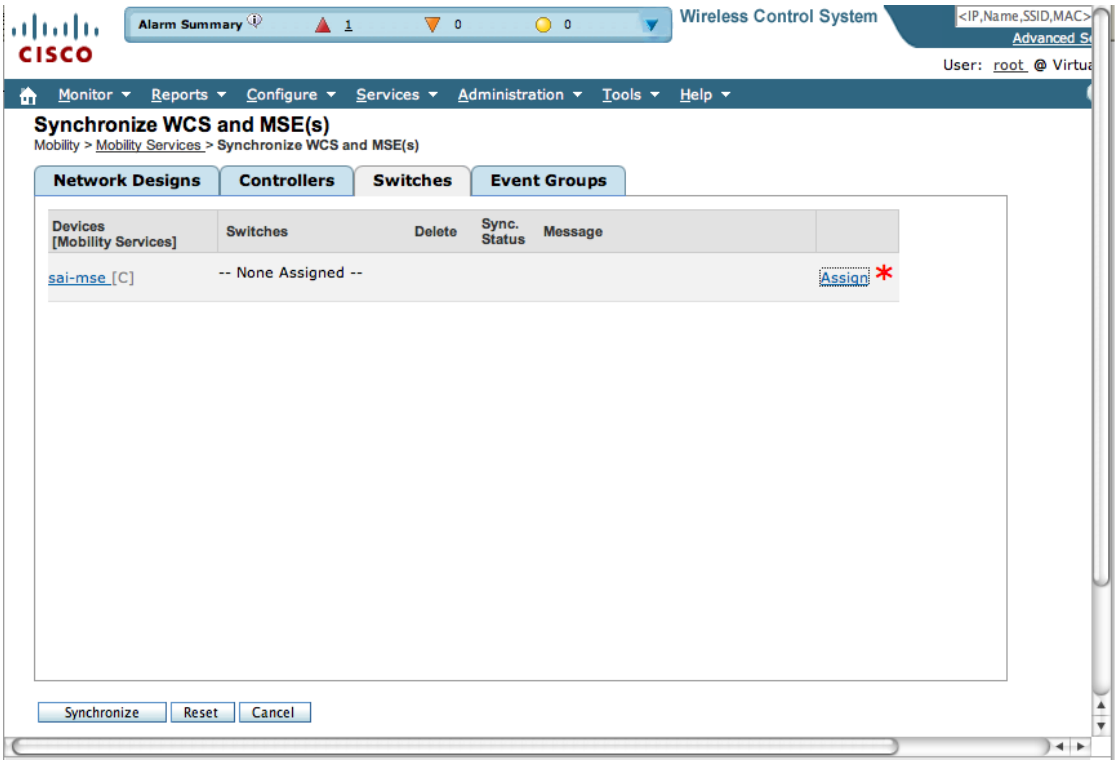
1. To assign a Catalyst switch to a mobility services engine, click its corresponding **Assign** link.

Figure 3-5 Services > Synchronize Services > Switches Window

2. In the Switch panel that appears, check the check box next to each wired switch to which you want the mobility services engine associated. Click **OK**.

   A red asterisk (*) appears next to the Assign link (see Figure 3-6).

Figure 3-6 Services > Synchronize Services > Switches Window

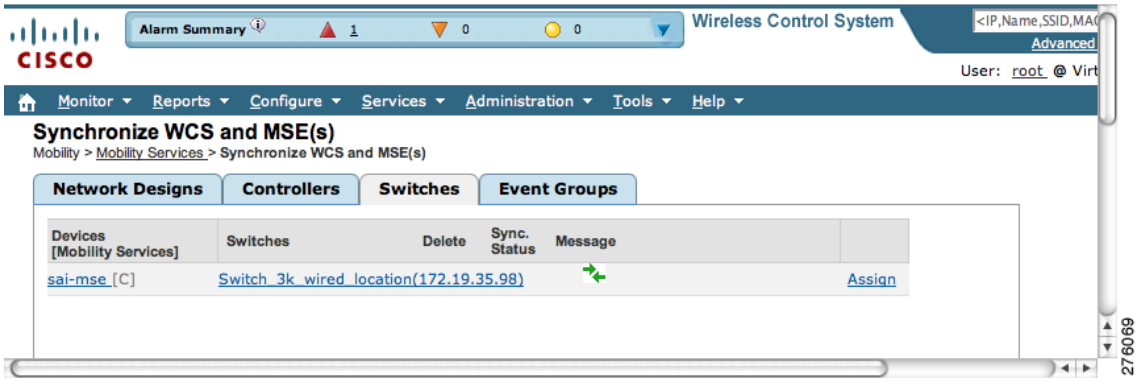


3. Click **Synchronize** to update the mobility services database.

   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**.

   When items are synchronized, a green two-arrow icon appears in the Sync. Status column for each synchronized entry (see Figure 3-7).

Figure 3-7 Synchronize WCS and MSE Confirmation Window



d. To assign an Event Group to a mobility services engine, click the **Event Groups** tab.

1. In the Event Groups panel that appears, check the check box for each event group that you want to assign to the mobility services engine. Click **OK**.

   A red asterisk (*) appears next to the Assign link. To undo assignments, click **Reset**. To go back to the Synchronize WCS and Server(s) window without making any changes, click **Cancel**.

2. Click **Synchronize** to update the mobility services database.

   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**.

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

Note To unassign a network design, controller, switch, or event group from a mobility services engine, click the **Assign** link next to the system. In the panel that appears, uncheck the check box for the corresponding network design, controller, switch, or event group. Click **OK.** Then, click **Synchronize**. The name of the removed network design, controller or event group is replaced with *None Assigned*.

Configuring Automatic Database Synchronization and Out of Sync Alerts

Manual synchronization of Cisco WCS and mobility services engine databases is immediate. However, future deployment changes (such as changes to maps and access point positions) can yield incorrect location calculations and asset tracking until resynchronization.

To prevent out-of-sync conditions, use Cisco WCS to enable automatic synchronization. This policy ensures that synchronization between Cisco WCS and mobility services engine databases is triggered periodically and any related alarms are cleared.

To configure automatic synchronization, follow these steps:

Step 1 In Cisco WCS, choose **Administration > Background Tasks**.

Step 2 Check the **Mobility Service Synchronization** check box. Select **Enable Task** from the Select a command drop-down menu if it is not already enabled. Click **Go**.

Step 3 Click the **Mobility Service Synchronization** link. The Task > Mobility Service Synchronization window appears.

Step 4 To set the mobility services engine to send out-of-sync alerts, check the Out of Sync Alerts **Enabled** check box. By default, out-of-sync alarms are enabled.

Note Uncheck the Out of Sync Alerts **Enabled** check box to disable forwarding of out-of-sync alarms.

Note For a summary of out of sync alerts that are sent, refer to the "Out-of-Sync Alarms" section on page 3-9.

Step 5 To enable automatic synchronization, check the Auto Synchronization **Enabled** check box.

Note Automatic synchronization does not apply to network designs, controllers, or event groups that are not assigned to a mobility services engine. However, out-of-sync alarms will still be generated for these unassigned elements. For automatic synchronization to apply to network designs, controllers, or event groups, you need to manually assign them to a mobility services engine.

Step 6 Enter the time interval in hours at which the automatic synchronization is to be occur.

By default, auto-sync is disabled.

Step 7 Click **Submit**. You are returned to the **Administration > Background Tasks** screen and the Mobility Service Synchronization task displays an enabled state.

Out-of-Sync Alarms

Out-of-sync alarms are of minor severity (yellow), and are raised in response to the following conditions:

- Elements are modified in Cisco WCS (the auto-sync policy pushes these elements)
- Elements are modified in the mobility services engine (the auto-sync policy pulls these elements)
- Elements other than controllers exist in the mobility services engine database but not in Cisco WCS (the auto-sync policy pulls these elements)
- Elements are not assigned to any mobility services engine (the auto-sync policy does not apply)

Out-of-sync alarms are cleared when the following occurs:

- Mobility services engine is deleted

Note When you delete a mobility services engine, the out-of-sync alarms for that system are also deleted. In addition, if you delete the last available mobility services engine, the alarms for the following event: *elements not assigned to any server* will also be deleted.

- Elements are synchronized manually or automatically
- User manually clears the alarms (although the alarms may reappear in the future when the scheduled task is next executed)

Viewing Mobility Services Engine Synchronization Status

You can use the Synchronize Services feature in Cisco WCS to view the status of network design, controller, switch, and event group synchronization with a mobility services engine.

To view synchronization status, follow these steps:

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

Step 2 Select either the **Network Designs**, **Controllers**, **Switches,** or **Event Groups** tab.

In the panel that appears, check the Sync. Status column for the synchronization status. A green two-arrow icon indicates that the mobility services engine is synchronized with the specified network design, controller, wired Catalyst switch, or event group. A gray two-arrow icon with a red circle indicates that its corresponding item is not synchronized with a given mobility services engine.

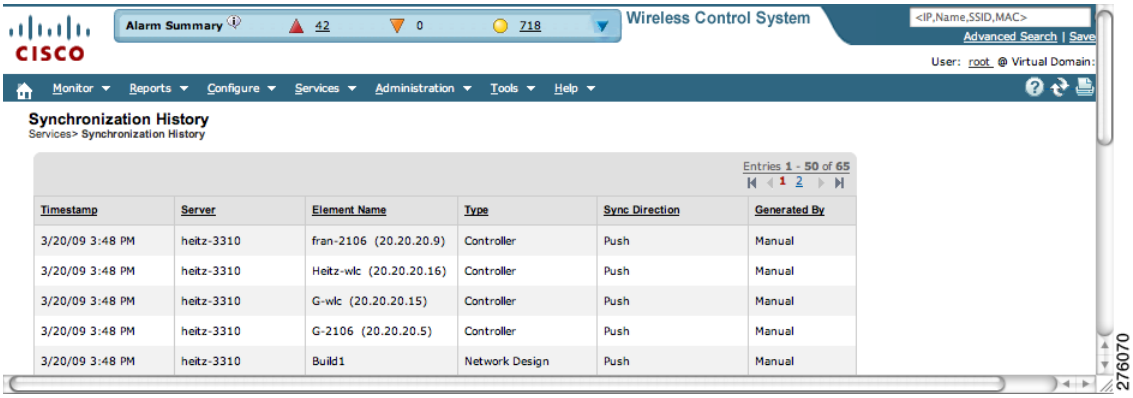
Viewing Synchronization History

You can view the synchronization history for the last 30 days for a mobility services engine. This is especially useful when automatic synchronization is enabled as alarms are automatically cleared. Synchronization history provides a summary of those cleared alarms.

To view synchronization history, follow these steps:

Step 1 In Cisco WCS, choose **Services > Synchronization History**. The Synchronization History window appears (see Figure 3-8).

Figure 3-8 Mobility > Synchronization History



Step 2 Click the column headers to sort the entries.

In the Synchronization History window, the Sync Direction column indicates whether information is pushed into the mobility services engine or pulled by the mobility services engine. The Generated By column indicates whether the synchronization was manual or automatic.

CHAPTER 4

Configuring and Viewing System Properties

This chapter describes how to configure and view system properties on the mobility services engine.

This chapter contains the following sections:

Editing General Properties and Viewing Performance

General Properties—You can use Cisco WCS to edit the general properties of a mobility services engine such as contact name, username, password, services enabled on the system, and the number of remaining units on each active license. Refer to the "Editing General Properties" section on page 4-2.

Note You would use the general properties to modify the username and password that you defined during initial setup of the mobility services engine.

Performance—You can use Cisco WCS to view CPU and memory use for a given mobility services engine. Refer to the "Viewing Performance Information" section on page 4-5.

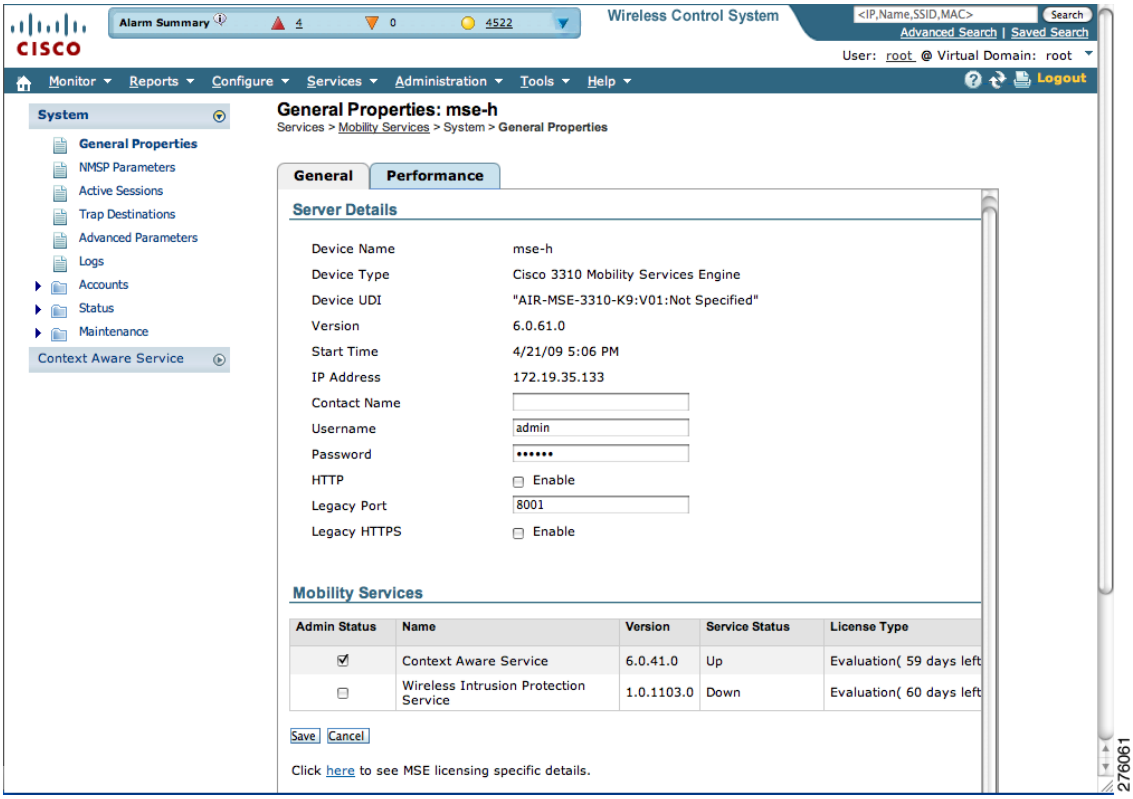
Editing General Properties

To edit the general properties of a mobility services engine, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services** to display the Mobility Services window.

Step 2 Click the name of the mobility services engine you want to edit. A two-tabbed panel appears with the following headings: General and Performance (see Figure 4-1).

Figure 4-1 Services > Mobility Services > General Properties



Note If the General Properties window does not appear by default, choose **System > General Properties** (left panel).

Step 3 Modify the parameters as appropriate in the General panel. Table 4-1 describes each parameter.

Table 4-1 General Properties

Parameter	Configuration Options
Contact Name	Enter a contact name for the mobility services engine.
Username	Enter the login username for the Cisco WCS server that manages the mobility services engine. This replaces any previously defined username including any set during initial setup.
Password	Enter the login password for the Cisco WCS server that manages the mobility services engine.This replaces any previously defined password including any set during initial setup.
Port	8001 **Note** The following ports are in use on a mobility services engine (MSE) in release 6.0: tcp 80: MSE HTTP port tcp 22: MSE SSH port tcp 443: MSE HTTPS port tcp 8001: Legacy port. Used for location APIs. Change in Cisco WCS. udp 123: NTPD port (open after NTP configuration) udp 32768: Location internal port tcp 4096: AeroScout notifications port tcp 1411: AeroScout SM tcp 1999: AeroScout internal port tcp 5900X: AeroScout (X could vary from 1 to 10) udp 32769: AeroScout internal port udp 37008: AeroScout internal port udp 162: AeroScout SNMP udp 12091: AeroScout devices (TDOA Wi-Fi Receivers, chokepoints) udp 12092: AeroScout devices (TDOA Wi-Fi Receivers, chokepoints) udp/tcp 4000X: AeroScout proxy (X could vary from 1 to 5)
HTTP	Check the **Enable** check box to enable HTTP. By default, HTTPS is enabled. **Note** HTTP is primarily enabled to allow third-party applications to communicate with the mobility services engine. **Note** Cisco WCS always communicates through HTTPS.

Table 4-1 General Properties (continued)

Parameter	Configuration Options
Legacy Port	Enter the mobility services port number that supports HTTPS communication. The Legacy HTTPS option must also be enabled.
Legacy HTTPS	This parameter does not apply to mobility services engines. It applies only to location appliances.
Mobility Services	To enable a service (CAS, wIPS) on a mobility services engine, check the **Admin Status** check box next to the service you want to enable. **Note** Once selected, the service displays as Up (active). All inactive services are noted as Down (inactive) on the selected (current) system and on the network. **Note** CAS and wIPS can operate on a mobility services engine at the same time. **Note** All mobility services engines are shipped with an evaluation license of CAS and wIPS. Evaluation copies are good for a period of 60 days (480 hours) and have preset device limits for each service. Licenses are usage-based (time is decremented by the number of days you use it rather than by calendar days passed). Click the **here** link (bottom) to see the time remaining on service licenses (evaluation or purchased) and the number of devices that can be assigned for the current system (see Figure 4-1). On the license summary page (see Figure 4-2), click **MSE** (left) to see details on licenses for all mobility services engines on the network (see Figure 4-3). **Note** For more information on purchasing and installing licenses, refer to: http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html

Figure 4-2 License Summary for Selected Mobility Services Engine

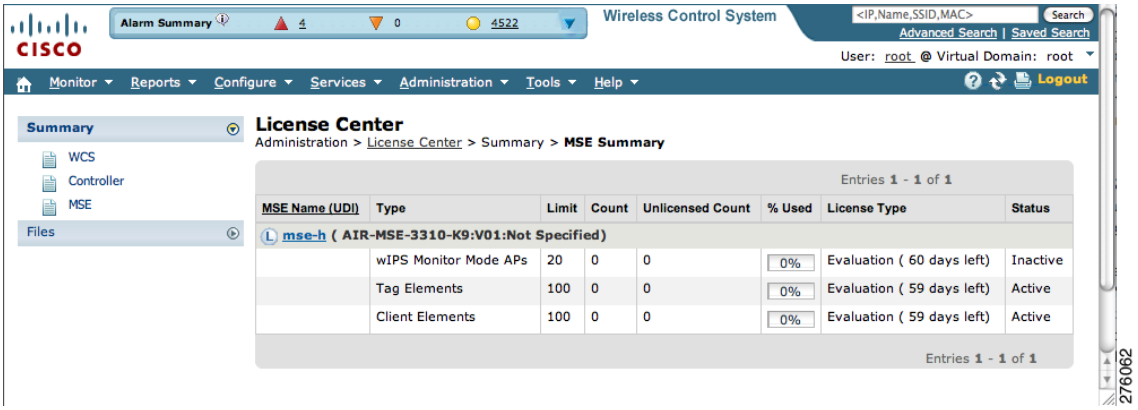
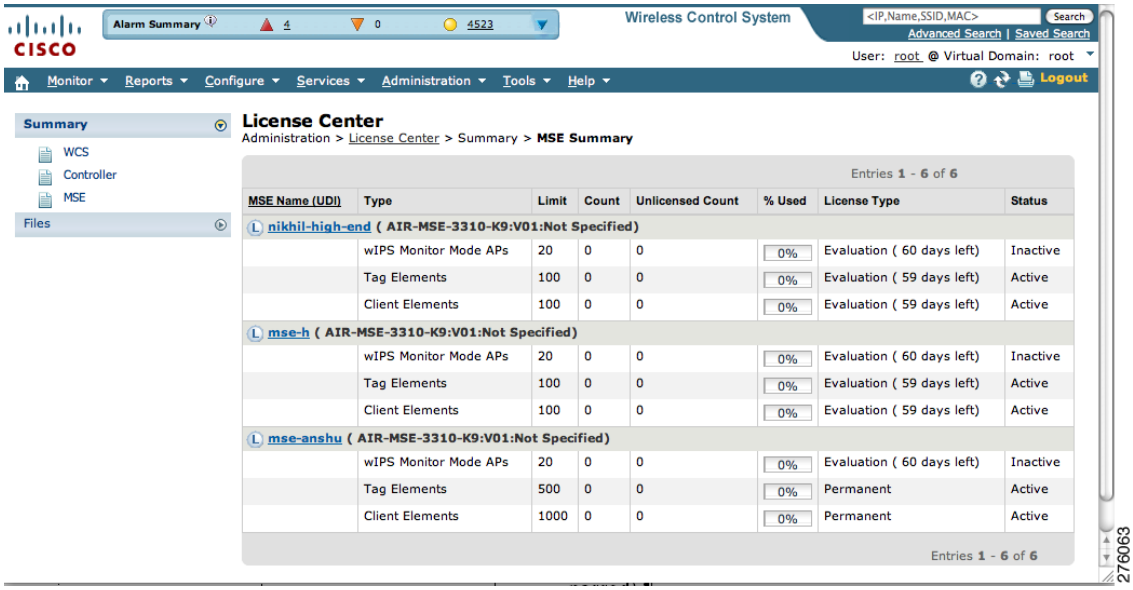


Figure 4-3 License Summary for All Mobility Services Engines



Step 4 Click **Save** to update the Cisco WCS and mobility services engine databases.

Viewing Performance Information

To view performance details, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services** to display the Mobility Services window.

Step 2 Click the name of the mobility services engine you want to view. A two-tabbed panel appears with the following headings: General and Performance.

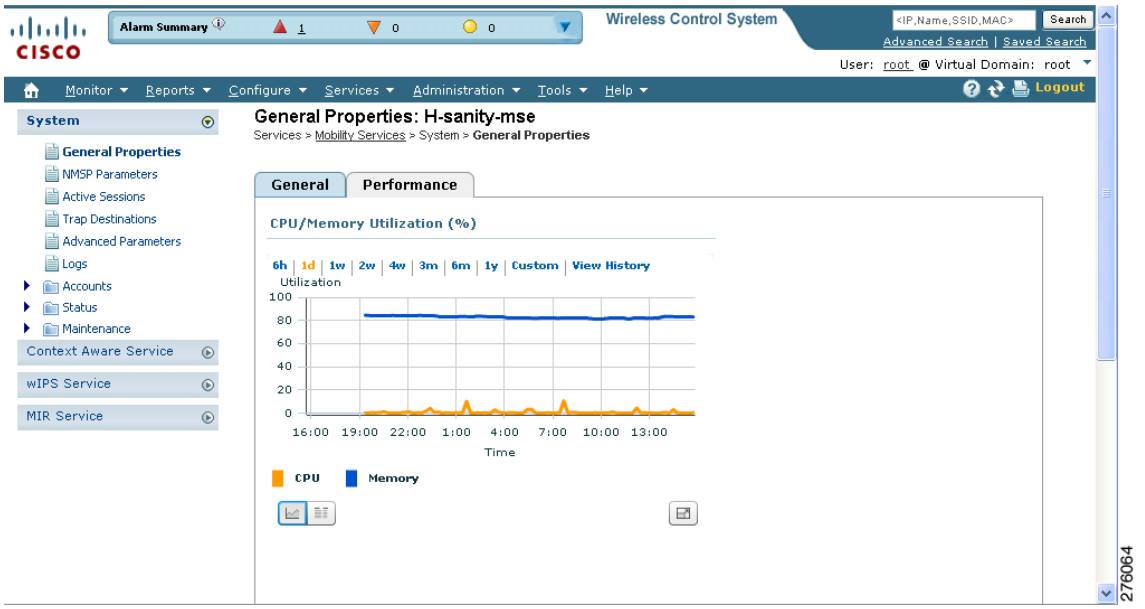
Step 3 Click **Performance** tab (see Figure 4-4).

Click a time period (such as *1w*) on the y-axis to see performance numbers for periods greater than one day.

To view a textual summary of performance, click the second icon under CPU.

To enlarge the screen, click the icon at the lower right.

Figure 4-4 CPU and Memory Performance



Modifying NMSP Parameters

Network Mobility Services Protocol (NMSP) is the protocol that manages communication between the mobility services engine and the controller. Transport of telemetry, emergency, and chokepoint information between the mobility services engine and the controller is managed by this protocol.

Note No change in the default parameter values is recommended unless the network is experiencing slow response or excessive latency.

- Telemetry, emergency and chokepoint information is only seen on controllers and Cisco WCS installed with release 4.1 software or later.
- The TCP port (16113) that the controller and mobility services engine communicate over MUST be open (not blocked) on any firewall that exists between the controller and mobility services engine.

To configure NMSP 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 edit.

Step 3 Choose **System > NMSP Parameters**. The configuration options appear.

Step 4 Modify the NMSP parameters as appropriate. Table 4-2 describes each parameter.

Table 4-2 NMSP Parameters

Parameter	Description
Echo Interval	How frequently an echo request is sent from a mobility services engine to a controller. The default value is 15 seconds. Allowed values range from 1 to 120 seconds. **Note** If a network is experiencing slow response, you can increase the values of the echo interval, neighbor dead interval, and the response timeout values to limit the number of failed echo acknowledgements.
Neighbor Dead Interval	The number of seconds that the mobility services engine waits for a successful echo response from the controller before declaring the neighbor dead. This timer begins when the echo request is sent. The default value is 30 seconds. Allowed values range from 1 to 240 seconds. **Note** This value must be at least two times the echo interval value.
Response Timeout	How long the mobility services engine waits before considering the pending request as timed out. The default value is 1 second. Minimum value is 1. There is no maximum value.
Retransmit Interval	Interval of time that the mobility services engine waits between notification of a response timeout and initiation of a request retransmission. The default setting is 3 seconds. Allowed values range from 1 to 120 seconds.
Maximum Retransmits	The maximum number of retransmits that are sent in the absence of a response to any request. The default setting is 5. Allowed minimum value is 0. There is no maximum value.

Step 5 Click **Save** to update the Cisco WCS and mobility services engine databases.

Viewing Active Sessions on a System

You can view active user sessions on the mobility services engine.

For every session, Cisco WCS displays the following information:

- Session identifier
- IP address from which the mobility services engine is accessed
- Username of the connected user
- Date and time when the session started
- Date and time when the mobility services engine was last accessed
- How long the session was idle since it was last accessed

To view active user sessions, 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 view active sessions.

Step 3 Choose **System > Active Sessions**.

Adding and Deleting Trap Destinations

You can specify which Cisco WCS or Cisco Security Monitoring, Analysis, and Response System (CS-MARS) network management platform is the recipient of SNMP traps generated by the mobility services engine.

When a user adds a mobility services engine using Cisco WCS, that WCS platform automatically establishes itself as the default trap destination. If a redundant Cisco WCS configuration exists, the backup WCS is not listed as the default trap destination unless the primary WCS fails and the backup system takes over. Only an active Cisco WCS is listed as a trap destination.

Adding Trap Destinations

To add a trap destination, 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 define a new SNMP trap destination server.

Step 3 Choose **System > Trap Destinations**.

Step 4 Select **Add Trap Destination** from the Select a command drop-down menu. Click **Go**.

Step 5 Enter IP address of destination SNMP server.

Step 6 Port number default of *162* is auto-populated. You can modify this as needed.

Step 7 Community default value of *public* is auto-populated. You can modify this as needed.

Step 8 Destination default value of *other* auto-populates.

Note All trap destinations are identified as *other* except for the automatically created *default* trap destination.

Step 9 Click **Save**.

You are returned to the trap destinations summary window and the newly defined trap is listed.

Deleting Trap Destinations

To delete a trap destination, 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 delete a SNMP trap destination server.

Step 3 Choose **System > Trap Destinations**.

Step 4 Check the check box next to the trap destination entry that you want to delete.

Step 5 Select **Delete Trap Destination** from the Select a command drop-down menu. Click **Go**.

Step 6 In the message box that appears, click **OK** to confirm deletion.

Viewing and Configuring Advanced Parameters

In Cisco WCS, at the Advanced Parameters window (see Figure 4-5) you can both view general system level settings of the mobility services engine and configure monitoring parameters.

- Refer to the "Viewing Advanced Parameters Settings" section on page 4-9 to view current system-level advanced parameters.
- Refer to the "Initiating Advanced Commands" section on page 4-11 to modify the current system-level advanced parameters or initiate advanced commands such as system reboot, system shutdown, clear a configuration file, or defragment the system database.

Viewing Advanced Parameters Settings

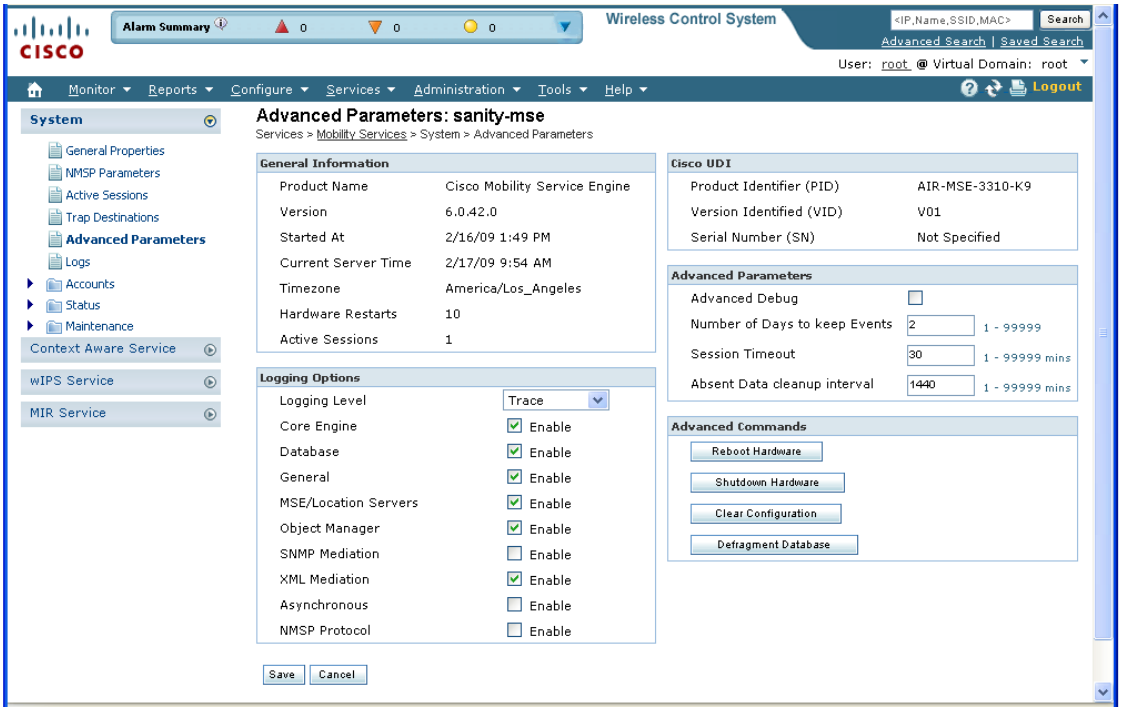
To view the advanced parameter settings of the mobility services engine, follow these steps:

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

Step 2 Click the name of a mobility services engine to view its status.

Step 3 Choose **System > Advanced Parameters** (see Figure 4-5).

Figure 4-5 Services > Mobility Services > System > Advanced Parameters



Configuring Advanced Parameters

On the Advanced Parameters window, you can use Cisco WCS:

- To specify the logging level and types of messages to log.

  Refer to the "Configuring Logging Options" section on page 4-10.
- To set how long events are kept, how long before a session time-outs, and the interval between data clean ups.

  Refer to the "Configuring Advanced Parameters" section on page 4-11.
- To enable or disable advanced debug level messages in the logs.

  Refer to the "Configuring Advanced Parameters" section on page 4-11.

Configuring Logging Options

You can use Cisco WCS to specify the logging level and types of messages to log.

To configure logging options, follow these steps:

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

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

Step 3 Choose **System > Advanced Parameters**. The advanced parameters for the selected mobility services engine appears.

Step 4 Scroll down to the Logging Options section and choose the appropriate option (Off, Error, Information, or Trace) from the Logging Level drop-down menu.

Caution Use **Error** and **Trace** only when directed to do so by Cisco Technical Assistance Center (TAC) personnel.

Step 5 Check the **Enabled** check box next to each item listed in that section to begin logging of its events.

Step 6 Click **Save**.

Configuring Advanced Parameters

To configure advanced parameters, follow these steps:

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

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

Step 3 Choose **System > Advanced Parameters**. The advanced parameters for the selected mobility services engine appears.

Step 4 Scroll down to the Advanced Parameters and make the appropriate changes. Table 4-3 describes the parameters.

Table 4-3 Advanced Parameters

Parameter	Configuration Options
Advanced debug	Check the check box to enable advanced debug. This enables reporting of advanced debug level messages to the log files.
Number of days to keep events	Enter the number of days that events are kept in the event table. Default value is 2.
Session time-out (minutes)	Enter the number of minutes a Cisco WCS or client session can remain inactive before it times out. Default value is 30.
Absent data cleanup interval (minutes)	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.

Initiating Advanced Commands

You can initiate a system reboot or shutdown, clear the system database, or defragment a database by clicking the appropriate button from the Advanced Parameters page.

Rebooting or Shutting Down a System

To reboot or shutdown a mobility services engine, follow these steps:

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

Step 2 Click the name of a mobility services engine you want to reboot or shutdown

Step 3 Click **System > Advanced Parameters** (see Figure 4-5).

Step 4 In the Advanced Commands section of the window (right), click the appropriate button (**Reboot Hardware** or **Shutdown Hardware**).

Click **OK** in the confirmation pop-up window to initiate either the reboot or shutdown process. Click **Cancel** to stop the process.

Clearing the System Database

To clear the database of a mobility services engine, follow these steps:

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

Step 2 Click the name of a mobility services engine whose configuration file you want to clear.

Step 3 Click **System > Advanced Parameters** (see Figure 4-5).

Step 4 In the Advanced Commands section of the window (right), click the **Clear Configuration** button.

Click **OK** in the confirmation pop-up window to initiate the process. Click **Cancel** to stop the process.

Defragment Database

To defragment the database of a mobility services engine, follow these steps:

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

Step 2 Click the name of a mobility services engine whose database you want to defragment.

Step 3 Choose **System > Advanced Parameters** (see Figure 4-5).

Step 4 In the Advanced Commands section of the window (right), click the **Defragment Database** button.

Click **OK** in the confirmation pop-up window to initiate the process. Click **Cancel** to stop the process.

CHAPTER 5

Managing Users and Groups

This chapter describes how to configure and manage users, groups, and host access on the mobility services engine.

This chapter contains the following sections:

Managing User Groups

This section describes how to add, delete, and edit user groups.

User groups allow you to assign different access privileges to users.

Caution Group permissions override individual user permissions. For example, if you give a user full access and add that user to a group with *read only* access, that user will not be able to configure mobility services engine settings.

Adding User Groups

To add a user group to a mobility services engine, follow these steps:

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

Step 2 Click the name of the mobility services engine to which you want to add a user group.

Step 3 Choose **System > Accounts > Groups**.

Step 4 Select **Add Group** from the Select a command drop-down menu and click **Go**.

Step 5 Enter the name of the group in the Group Name field.

Step 6 Select a permission level (read, write, or full) from the Permission drop-down menu.

Note Full Access is required for Cisco WCS to access mobility services engines.

Step 7 Click **Save**.

Deleting User Groups

To delete user groups from a mobility services engine, 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 to delete a user group.

Step 3 Choose **System > Accounts > Groups**.

Step 4 Check the check boxes of the groups that you want to delete.

Step 5 Select **Delete Group** from the Select a command drop-down menu and click **Go**.

Step 6 Click **OK**.

Changing User Group Permissions

Caution Group permissions override individual user permissions. For example, if you give a user *full* access and add that user to a group with only *read* access, that user will not be able to configure mobility services engine settings.

To change user group permissions, 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 edit.

Step 3 Choose **System > Accounts > Groups**.

Step 4 Click the name of the group you want to edit.

Step 5 Select a permission level (read, write, full) from the Permission drop-down menu.

Step 6 Choose **Save**.

Managing Users

This section describes how to add, delete, and edit users for a mobility services engine. It also describes how to view active user sessions.

Adding Users

Caution Group permissions override individual user permissions. For example, if you give a user *full* access and add that user to a group with only *read* access, that user will not be able to configure mobility services engine settings.

To add a users to a mobility services engine, follow these steps:

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

Step 2 Click the name of the mobility services engine to which you want to add users.

Step 3 Choose **System > Accounts > Users**.

Step 4 Select **Add User** from the Select a command drop-down menu and click **Go**.

Step 5 Enter the username in the Username field.

Step 6 Enter a password in the Password field.

Step 7 Enter the name of the group to which the user belongs in the Group Name field.

Step 8 Select a permission level (read, write, full) from the Permission drop-down menu.

Note Full access is required for Cisco WCS to access mobility services engines.

Step 9 Click **Save**.

Deleting Users

To delete a user from a mobility services engine, 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 to delete a user.

Step 3 Choose **System > Accounts > Users**.

Step 4 Check the check boxes of the users that you want to delete.

Step 5 Select **Delete User** from the Select a command drop-down menu and click **Go**.

Step 6 Click **OK**.

Changing User Properties

To change user properties, 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 edit.

Step 3 Choose **System > Accounts > Users**.

Step 4 Click the name of the group that you want to edit.

Step 5 Make the required changes to the Password, Group Name, and Permission fields.

Step 6 Click **Save**.

CHAPTER 6

Configuring Event Notifications

With Cisco WCS, you can define conditions that cause the mobility service engine to send notifications to specific listeners. This chapter describes how to define events and event groups and how to view event notification summaries.

This chapter contains the following sections:

Adding and Deleting Event Groups

This section describes how to add and delete event groups. Event groups help you organize your event notifications.

Adding Event Groups

To add an event group, follow these steps:

Step 1 In Cisco WCS, choose **Services > Context Aware Notifications**.

Step 2 Choose **Notification Settings** (left panel).

Step 3 From the Select a command drop-down menu, select **Add Event Group**. Click **Go**.

Step 4 Enter the name of the group in the Group Name field.

Step 5 Click **Save**.

The new event group appears in the Event Settings window.

Deleting Event Groups

To delete an event group, follow these steps:

Step 1 In Cisco WCS, choose **Services > Context Aware Notifications**.

Step 2 Choose **Notification Settings** (left panel).

Step 3 Select the event group to delete by checking its corresponding check box.

Step 4 From the Select a command drop-down menu, select **Delete Event Group(s)**. Click **Go**.

Step 5 In the panel that appears, click **OK** to confirm deletion.

Step 6 Click **Save**.

Adding, Deleting, and Testing Event Definitions

An event definition contains information about the condition that caused the event, the assets to which the event applies, and the event notification destination.

This section describes how to add, delete, and test event definitions.

Adding an Event Definition

Cisco WCS enables you to add an event definition to a group. An event definition must belong to a particular group.

To add an event definition, follow these steps:

Step 1 In Cisco WCS, choose **Services > Context Aware Notifications**.

Step 2 Choose **Notification Settings** (left panel).

Step 3 Click the name of the group to which you want to add an event definition. An event definition summary window appears showing existing event definitions for the event group.

Step 4 From the Select a command drop-down menu, select **Add Event Definition**. Click **Go**.

Step 5 At the Conditions tab, add one or more conditions. For each condition you add, specify the rules for triggering event notifications.

Tip For example, to keep track of heart monitors in a hospital, you might add rules to generate notifications when the following occur: (1) the heart monitor is missing for one hour, (2) the heart monitor moves off its assigned floor, or (3) the heart monitor enters a specific coverage area within a floor. In this example, we would add three separate rules to address these occurrences.

To add a condition, follow these steps:

a. Click **Add** to add a condition that triggers a notification.

b. In the Add/Edit Condition dialog box, follow these steps:

1. Choose a condition type from the Condition Type drop-down menu.

- If you chose **Missing** from the Condition Type drop-down menu, enter the number of minutes after which a missing asset generates a notification. For example, if you enter 10 in this field, the mobility service engine generates a missing asset notification if the mobility service engine has not located the asset for more than 10 minutes. Proceed to Step c.
- If you chose **In/Out** from the Condition Type drop-down menu, select **Inside of** or **Outside of**, then click **Select Area**. Entry and exit of assets from the selected area is then monitored. In the Select dialog box, choose the area to monitor, then click **Select**. The area to monitor could be an entire campus, building within a campus, a floor in a building, or a coverage area (you can define a coverage area using the map editor). For example, to monitor part of a floor in a building, choose a campus from the Campus drop-down menu, choose a building from the Building drop-down menu, and choose the area to monitor from the Floor Area drop-down menu. Then click **Select**. Proceed to Step c.
- If you chose **Distance** from the Condition Type drop-down menu, enter the distance in feet from a designated marker beyond which an asset triggers an event notification. Click **Select Marker**. In the Select dialog box, select the campus, building, floor, and marker from the corresponding drop-down menus and click **Select**. For example, if you add a marker to a floor plan and set the distance in the Trigger If field to 60 feet, an event notification will be generated if the monitored asset moves farther than 60 feet away from the marker. Proceed to Step c.

Note You can create markers and coverage areas using the Map Editor. When you create marker names, make sure they are unique across the entire system.

- If you chose **Battery Level** from the Condition Type drop-down menu, check the box next to the appropriate battery level (low, medium, normal) that will trigger a notification. Proceed to Step c.
- If you chose **Location Change** from the Condition Type drop-down menu, proceed to Step c.

- If you chose **Emergency** from the Condition Type drop-down menu, click the button next to the appropriate emergency (any, panic button, tampered, detached) that will trigger a notification. Proceed to Step c.
- If you chose **Chokepoint** from the Condition Type drop-down menu, proceed to Step c. There is only one trigger condition and it is displayed by default. No configuration required.

c. From the Apply To drop-down menu, choose the type of asset (Any, Clients, Tags, Rogue APs, Rogue Clients, or Interferers) for which a notification will be generated if the trigger condition is met.

Note If you select the *Any* option from the Apply to drop-down menu, the battery condition is applied to all tags, clients, and rogue access points, and rogue clients.

Note Emergency and chokepoint notifications apply only to Cisco compatible extension (CX) tags version 1 (or later).

d. For the Match By option there are three entries, left to right:

- Choose the matching criteria (MAC Address, Asset Name, Asset Group, or Asset Category) from the first drop-down menu.
- Choose the operator (Equals or Like) from the second drop-down menu.
- Enter the relevant text into the field base on the selected Match By element.

  Following are examples of asset matching criteria that you can specify:

  – If you choose **MAC Address** from the first drop-down menu, choose **Equals** from the second drop-down menu, and enter a MAC address (for example **12:12:12:12:12:12)** in the field, the event condition applies to the element whose MAC address is 12:12:12:12:12:12 (exact match).

  – If you choose **MAC Address** from the first drop-down menu, choose **Like** from the second drop-down menu, and enter **12:12** in the field, the event condition applies to elements whose MAC address starts with 12:12.

e. Click **Add** to add the condition you have just defined.

Note If you are defining a chokepoint, you must select the chokepoint after you add the condition.

To select a chokepoint, do the following:

1. Click **Select Chokepoint**. An entry panel appears.
2. Select Campus, Building, and Floor from the appropriate drop-down menus.
3. Select a Chokepoint from the menu that appears.

The Add/Edit Condition panel reappears and the location path (*Campus* > *Building* > *Floor*) for the chokepoint auto-populates the entry field next to the Select Checkpoint button.

Step 6 At the Destination and Transport tab, follow these steps to add one or more destinations to receive event notifications and to configure the transport settings:

a. To add a new destination, click **Add**. The Add/Edit Destination configuration panel appears.

b. Click **Add New**.

c. In the pop up that appears, enter the IP address of the system that will receive event notifications, and click **OK**.

The new entry is placed in the right column.

The recipient system must have an event listener running to process notifications. By default, when you create an event definition, Cisco WCS adds its IP address as the destination.

d. To select a destination for notifications, highlight one or more IP addresses in the box on the right, and click **Select** to add the IP addresses to the box on the left.

e. Select **XML** or **Plain Text** as the message format.

Note If you select WCS as the destination for notifications, you must select the XML format.

f. Choose one of the following transport types from the Transport Type drop-down menu:

- **SOAP**—Simple Object Access Protocol, a simple XML protocol. Use SOAP to send notifications over either HTTP (default) or HTTPS for process by web services at the destination.

  Be sure to select HTTPS in step g if you do not want to send notifications over HTTP.

  Also, enter a destination port number in step h if a value other than the auto-populated value is required.

- **Mail**—Use this option to send notifications by email.

  If you choose **Mail**, you need to choose the protocol for sending the mail from the Mail Type drop-down menu. You also need to enter the following information: username and password (if Authentication is enabled), name of the sender, prefix to add to the subject line, email address of recipient, and a port number if necessary.

- **SNMP**—Use Simple Network Management Protocol, a very common technology for network monitoring used to send notifications to SNMP-capable devices.

  If you choose **SNMP**, enter the SNMP community string in the SNMP Community field and the port number to send notifications to in the Port Number field.

- **SysLog**—Specifies the system log on the destination system as the recipient of event notifications.

  If you choose **SysLog**, enter the notification priority in the Priority field, the name of the facility in the Facility field, and the port number on the destination system in the Port Number field.

g. To enable HTTPS, check the **Enable** check box next to it.

h. **Port Number** auto-populates.

i. Click **Save**.

Step 7 At the General tab, follow these steps:

a. Check the Admin Status **Enabled** check box to enable event definition (disabled by default).

b. Set the event definition priority by choosing a number from the Priority drop-down menu. Zero is highest.

Note An event definition with higher priority is serviced before event definitions with lower priority.

c. Choose the frequency of notifications:
   1. Check the **All the Time** check box to continuously report events. Proceed to step g.
   2. Uncheck the **All the Time** check box to select the day and time of the week that you want event notifications sent. Days of the week and time fields appear for selection. Proceed to step d.

d. Check the check box next to each day that you want the event notification sent.

e. Choose a start time for the event notification by selecting the hour, minute, and AM or PM using the Apply From drop-down menus.

f. Choose an end time for the event notification by selecting the hour, minute, and AM or PM from the Apply Until drop-down menus.

g. Click **Save**.

Step 8 Verify that the new event definition is listed for the event group (Services > Context Aware Notifications > Notification Settings > *Group Name)*.

Deleting an Event Definition

To delete one or more event definitions from Cisco WCS, follow these steps:

Step 1 In Cisco WCS, choose **Services > Context Aware Notifications**.

Step 2 Choose **Notification Settings** (left panel).

Step 3 Click the name of the group from which you want to delete an event definition.

Step 4 Select the event definition that you want to delete by checking its corresponding check box.

Step 5 From the Select a command drop-down menu, choose **Delete Event Definition(s)**. Click **Go**.

Step 6 Click **OK** to confirm that you want to delete the selected event definition.

Testing Event Definitions

You can use Cisco WCS to verify that the mobility service engine is sending an event notification over the transport protocol you have specified in an event definition. The mobility service engine sends three fictitious event notifications (absence, containment, and distance) to the destination you have specified in the event definition. The messages contain dummy MAC addresses.

Note Emergency and chokepoint event notifications are not tested.

To test one or more event notifications of an event definition, follow these steps:

Step 1 In Cisco WCS, choose **Services > Context Aware Notifications**.

Step 2 Choose **Notification Settings** (left panel).

Step 3 Click the name of the group containing the event definitions that you want to test.

Step 4 Select the event definitions that you want to test by checking their corresponding check boxes.

Step 5 From the Select a command drop-down menu, choose **Test-Fire Event Definition(s)**. Click **Go**.

Step 6 Click **OK** to confirm that you want to test the event notifications.

Step 7 Ensure that notifications were sent to the designated recipient.

Viewing Event Notification Summary

The mobility services engine sends event notifications and does not store them. However, if WCS is a destination of notification events, it stores the notifications it receives and groups them into the following seven categories:

- Absence (Missing)—The mobility services engine generates an absence event when an asset goes missing. In other words, the mobility services engine cannot detect the asset in the WLAN for the specified time.
- In/Out Area (Containment)—The mobility services engine generates a containment event when an asset moves in or out of a designated area.

Note You define a containment area (campus, building, or floor) in the Maps section of Cisco WCS (**Monitor > Maps**). You can define a coverage area using the Map Editor.

- Movement from Marker (Movement/Distance)—The mobility services engine generates a movement event when an asset is moved beyond a specified distance from a designated marker you define on a map.
- Location Changes—The mobility services engine generates location change events when a client station, asset tag, rogue client and rogue access point changes its location.
- Battery Level—The mobility services engine generates battery level events for all tracked asset tags.
- Emergency—The mobility services engine generates an emergency event for a Cisco CX v.1 compliant asset tag when the tag's panic button is triggered or the tag becomes detached, is tampered with, becomes inactive, or reports an unknown state. This information is reported and displayed only for Cisco CX v.1 compliant tags.
- Chokepoint Notifications—The mobility services engine generates an event when a tag is stimulated by a chokepoint. This information is reported and displayed only for Cisco CX v.1 compliant tags.

Note All element events are summarized hourly and daily.

To view event notifications, follow these steps:

Step 1 In Cisco WCS, choose **Services > Context Aware Notifications**.

Cisco WCS displays a summary of event notifications for each of the seven event notification categories.

Note Emergency and chokepoint notifications are reported and displayed only for Cisco CX v.1 compliant tags.

Step 2 To view event notifications for a monitored asset, click one of its corresponding links.

For example, to view absence events for client stations generated in the last hour, click the link in the Last Hour column for the Client Stations entry in the Absence (Missing) list.

Clicking one of these links searches for location notifications of all severities.

Clearing Notifications

A mobility services engine sends event notifications when it clears an event condition in one of the following scenarios:

- **Missing (Absence)**—Elements (clients, tags, rogue access points, or rogue clients) reappear.
- **In/Out Area (Containment)**—Elements move back in to or out of the containment area.
- **Distance**—Elements move back within the specified distance from a marker.
- **Location Changes**—Clear state does not apply to this condition.
- **Battery Level**—Tags are detected again operating with normal battery level.

Note In Cisco WCS, the Notifications Summary window reflects whether notifications for cleared event conditions have been received.

Notification Message Formats

This section describes the notification message formats for XML and text.

Notification Formats in XML

This section describes the XML format of notification messages.

Note The XML format is part of a supported API, and Cisco will provide change notification as part of the Mobility Services Engine API program whenever the API is updated in the future.

Missing (Absence) Condition

Message format for element absence:

```
<AbsenceTrackEvent
missingFor="<time in secs entity has been missing>"
lastSeen="time last seen"
trackDefn="<name of track definition>"
entityType="Mobile Station | Tag | Rogue AP | Rogue Client"
entityID="<mac address"/>
```

Message format for the clear state:

```
<AbsenceTrackEvent
state="clear"
trackDefn="<name of track definition>"
entityType="Mobile Station | Tag | Rogue AP | Rogue Client"
entityID="<mac address"/>
```

Following are examples:

```
<AbsenceTrackEvent state="set" missingFor="34" lastSeen="15:00:20 08 Jun 2009"
trackDefn="absenceDef1" entityType="Mobile Station"
entityID="00:0c:f1:53:9e:c0"/>

<AbsenceTrackEvent state="clear" entityType="Tag"
trackDefn="absenceDef1" entityID="00:0c:cc:5b:fc:da"/>
```

In/Out (Containment) Condition

Message format for element containment:

```
<ContainmentTrackEvent
in="true | false"
trackDefn="<name of track definition>"
containerType="Floor | Area | Network Design | Building"
containerID="<fully quality name of container>"
entityType="Mobile Station | Tag | Rogue AP | Rogue Client"
entityID="<mac address"/>
```

Message format for the clear state:

```
<ContainmentTrackEvent
state="clear"
trackDefn="<name of track definition>"
entityType="Mobile Station | Tag | Rogue AP | Rogue Client"
entityID="<mac address"/>
```

Following are examples:

```
<ContainmentTrackEvent in="true" trackDefn="myContainerRule1"
containerType="Area"
containerID="nycTestArea,5th Floor,Bldg-A,Rochester_Group,Rochester,"
```

Note The `containerID` string represents a coverage area called `nycTestArea`, located in the 5th floor of Bldg-A of the campus *Rochester.*

```
entityType="Tag" entityID="00:0c:cc:5b:fa:44"/>

<ContainmentTrackEvent state="clear" entityType="Tag"
trackDefn="myContainerRule1" entityID="00:0c:cc:5b:f8:ab"/>
```

Distance Condition

Message format for elements on the same floor:

```
<MovementTrackEvent
distance="<distance in feet at which the element was located>"
triggerDistance="<the distance specified on the condition"
reference="<name of the marker specified on the condition>"
trackDefn="<name of event definition>"
entityType="Mobile Station | Tag | Rogue AP | Rogue Client"
entityID="<mac address"/>
```

Message format for elements located on a different floor:

```
<MovementTrackEvent optionMsg="has moved beyond original floor"
reference="<name of the marker specified on the condition>"
trackDefn="<name of event definition>"
entityType="Mobile Station | Tag | Rogue AP | Rogue Client"
entityID="<mac address"/>
```

Message format for clear state:

```
<MovementTrackEvent
state="clear"
trackDefn="<name of event definition>"
entityType="Mobile Station | Tag | Rogue AP | Rogue Client"
entityID="<mac address"/>
```

Following are examples:

```
<MovementTrackEvent distance="115.73819627990147" triggerDistance="60.0"
reference="marker2" trackDefn="distance2" entityType="Mobile Station"
entityID="00:0c:41:15:99:92"/>

<MovementTrackEvent optionMsg="has moved beyond original floor"
reference="marker2" entityType="Tag"
trackDefn="distance2"
entityID="00:0c:cc:5b:fa:4c"/>

<MovementTrackEvent state="clear" entityType="Tag"
```

Battery Level

An example:

```
<BatteryLifeTrackEvent lastSeen="10:28:52 08 Jun 2009" batteryStatus="medium"
trackDefn="defn1" entityType="Tag" entityID="00:01:02:03:04:06"/>
```

Location Change

An example:

```
<MovementTrackEvent distance="158.11388300841898" triggerDistance="5.0"
reference="marker1" referenceObjectID="1" trackDefn="defn1" entityType="Mobile Station"
entityID="00:01:02:03:04:05"/>
```

Chokepoint Condition

An example:

```
<ChokepointTrackEvent
lastSeen="11:10:08 PST 08 Jun 2009"
chokepointMac="00:0c:cc:60:13:a3"
chokepointName= "chokeA3"
trackDefn="choke"
entityType="Tag"
entityID="00:12:b8:00:20:4f"/>
```

An example for the clear state:

```
<ChokepointTrackEvent
state="clear"
entityType="Tag"
trackDefn="choke"
entityID="00:12:b8:00:20:4f"/>
```

Emergency Condition

An example for element location:

```
<ChokepointTrackEvent
lastSeen="11:36:46 PST June 08 2009"
emergencyReason= "detached"
trackDefn="emer"
entityType="Tag"
entityID="00:12:b8:00:20:50"/>
```

Note Emergency events are never cleared.

Notification Formats in Text

When you specify that notification be sent in text format, the mobility services engine uses a plain-text string to indicate the condition. Following are examples:

```
Tag 00:02:02:03:03:04 is in Floor <floorName>
Tag 00:02:02:03:03:04 is outside Floor <floorName>
Client 00:02:02:03:09:09 is in Area <areaName>
RogueClient 00:02:02:08:08:08 is outside Building <buildingName>
Tag 00:02:02:03:03:06 has moved 105 feet where the trigger distance was 90 feet.
Tag 00:02:02:03:03:20 missing for 14 mins, last seen <timestamp>.
```

Note Cisco maintains the right to modify the text notification format without notice.

Note XML is the recommended format for systems that need to parse or analyze notification contents.

Cisco WCS as a Notification Listener

Cisco WCS acts as a notification listener. Cisco WCS receives the notifications from the mobility services engine in the form of the trap `locationNotifyTrap` as part of the MIB file bsnwras.my. The mobility services engine stores the content of the notification message in XML format in the variable `locationNotifyContent` (see the "Notification Formats in XML" section on page 6-8).

```
locationNotifyTrap  NOTIFICATION-TYPE
    OBJECTS { locationNotifyContent}
    STATUS current
    DESCRIPTION
        "This trap will be generated by the mobility services engine
        for notifications of location events."
    ::= { bsnTraps 89 }

locationNotifyContent OBJECT-TYPE
    SYNTAX  OCTET STRING(SIZE(0..512))
    MAX-ACCESS  accessible-for-notify
    STATUS  current
    DESCRIPTION
        "This is the content of the notification."
    ::= { bsnTrapVariable 72 }
```

Cisco WCS translates the traps into UI alerts and displays them in the following formats:

- Missing (Absence)

  ```
  Absence of Tag with MAC 00:0c:cc:5b:e4:1b, last seen at 16:19:45 08 June 2009.
  ```

- In/Out (Containment)

  ```
  Tag with MAC 00:0c:cc:5b:fa:44 is In the Area 'Rochester > Rochester > 5th Floor >
  nycTestArea'
  ```

- Distance

  ```
  Tag with MAC 00:0c:cc:5b:fa:47 has moved beyond the distance configured for the marker
  'marker2'.
  Tag with MAC 00:0c:cc:5b:f9:b9 has moved beyond 46.0 ft. of marker 'marker2', located
  at a range of 136.74526528595058 ft.
  ```

- Battery Level

  ```
  Tag 00:01:02:03:04:06 has medium battery, last seen 11:06:01 08 June 2009
  ```

- Location Change

  ```
  Mobile Station 00:01:02:03:04:05 has moved
  158.11388300841898ft, where the trigger distance was 5.0
  ```

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:

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.

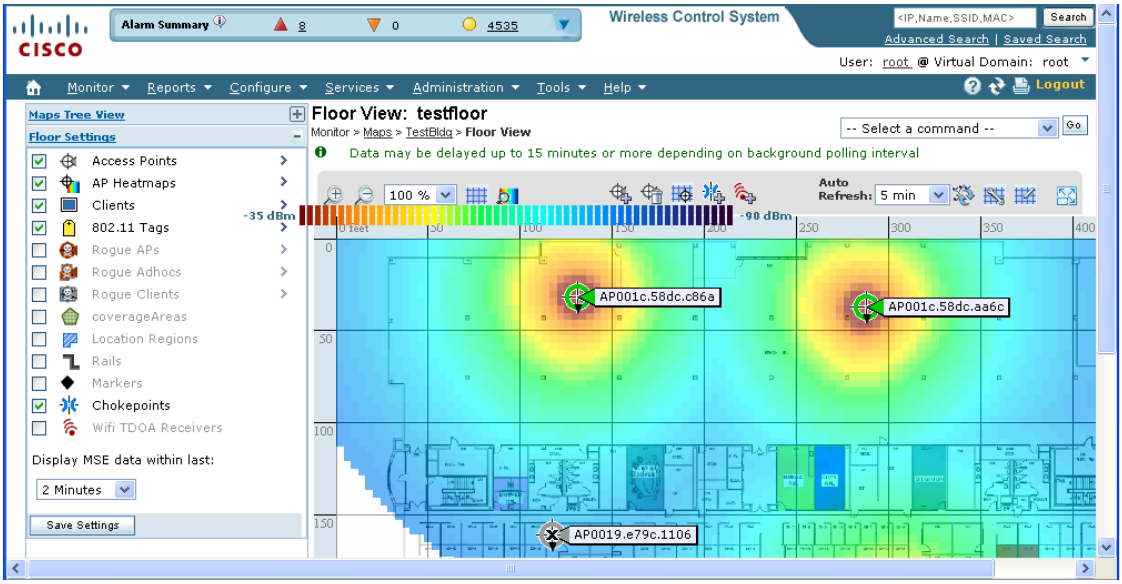
To calculate the recommended number and placement of access points on a floor, follow these steps:

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



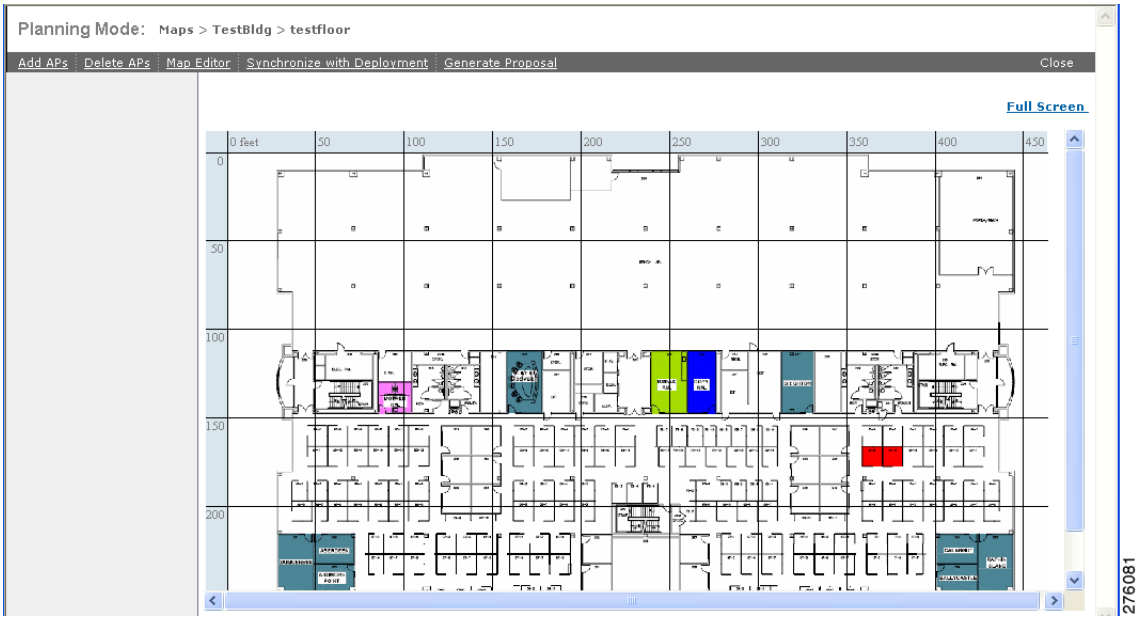
A map appears showing placement of all installed elements (access points, clients, tags) and their relative signal strength (RSSI). RSSI is indicated by the colored rings that surround the element. To identify the exact RSSI for that element, refer to the RSSI legend (color bar) at the top of the page.

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**.

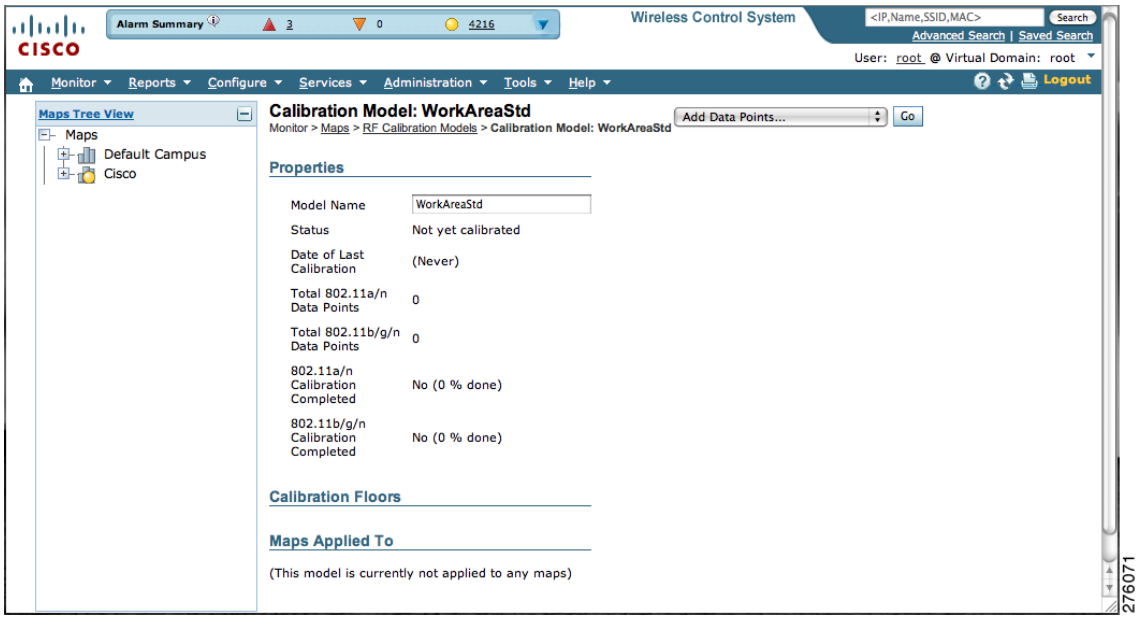
Step 2 Select **Create New Model** from the Select a command drop-down menu at the upper right. Click **Go**.

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



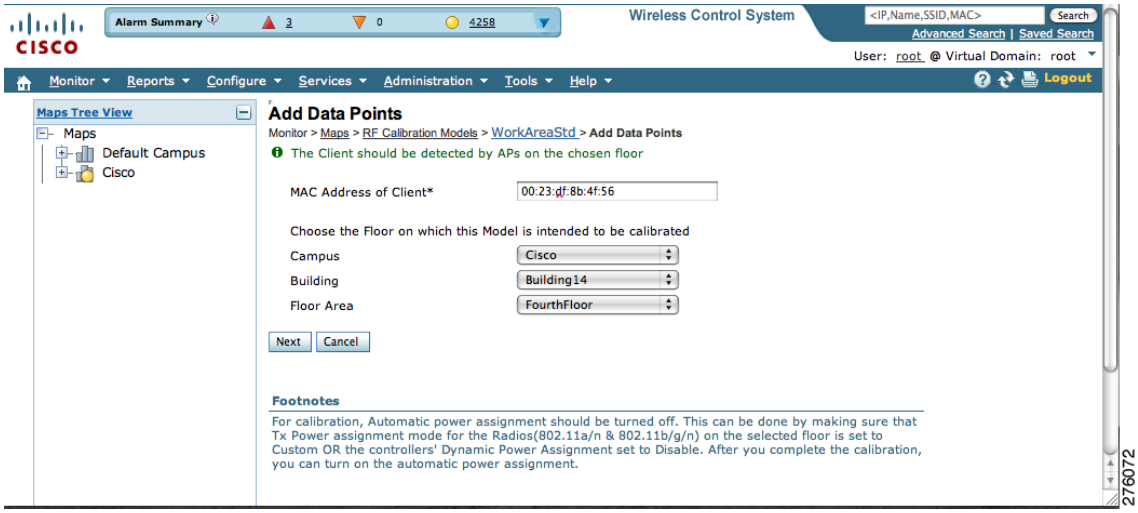
Note At this screen, you can rename and delete the calibration model by selecting the proper option from the Select a command menu. When renaming the model, enter the new name before selecting **Rename Model**.

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**.

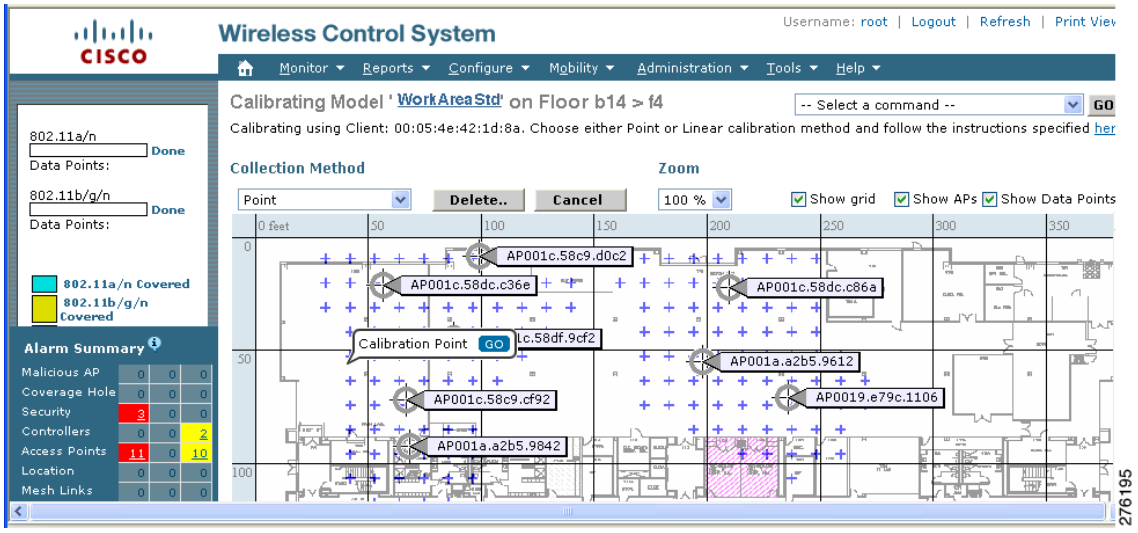
Figure 7-4 Starting to Calibrate



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:

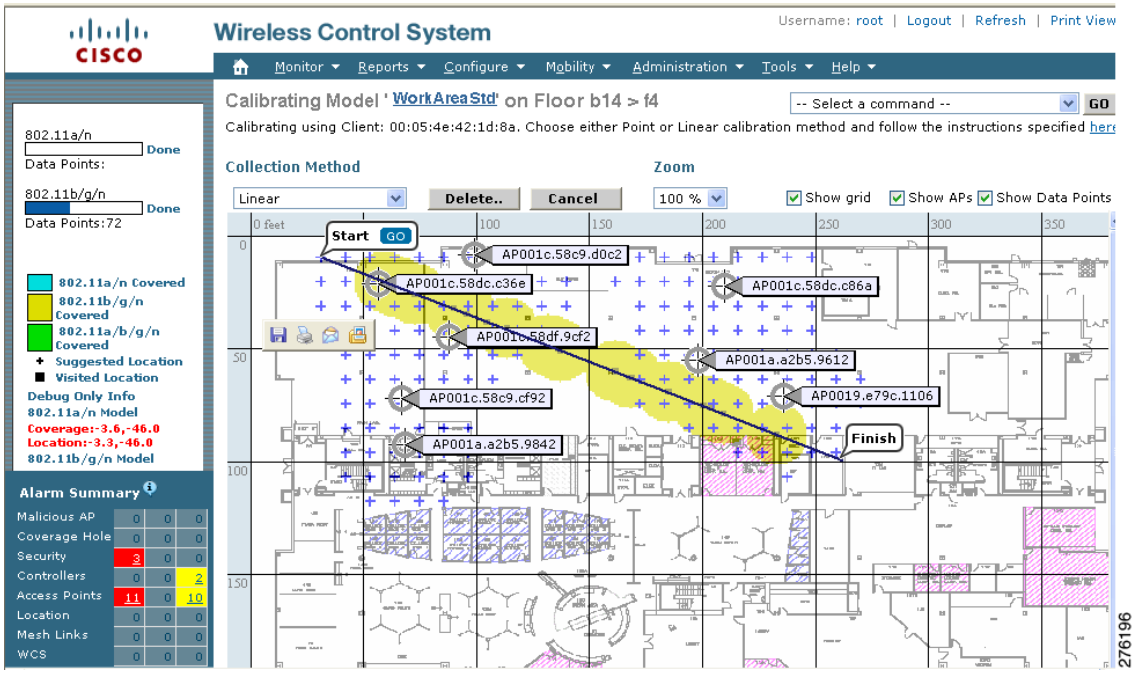
1. Select **Linear** from the Collection Method drop-down menu and check the **Show Data points** check box if not already checked. A line appears on the map with both Start and Finish pop-ups (see Figure 7-6).
2. Position the tip of the Start pop-up at the starting data point.
3. Position the Finish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

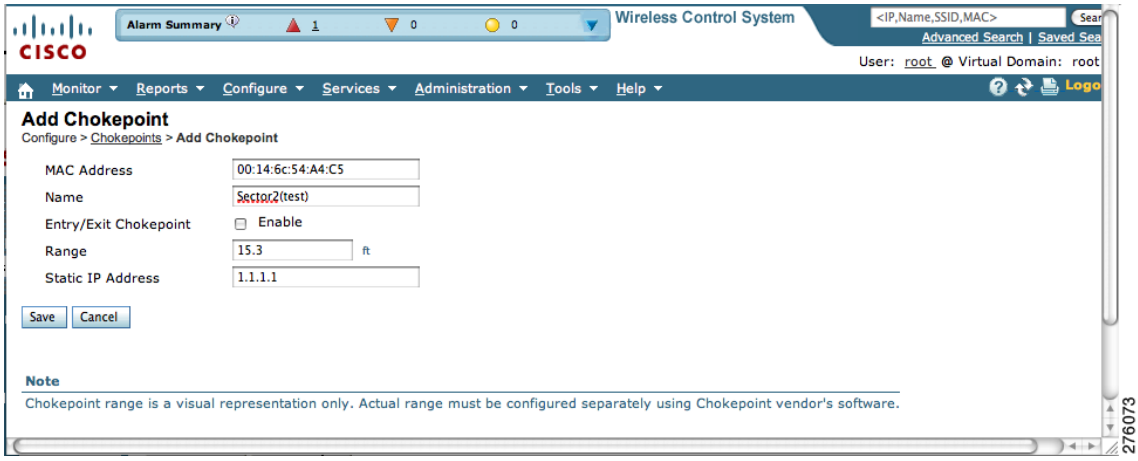
Step 1 Choose **Configure > Chokepoints** from the main menu (top).

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.

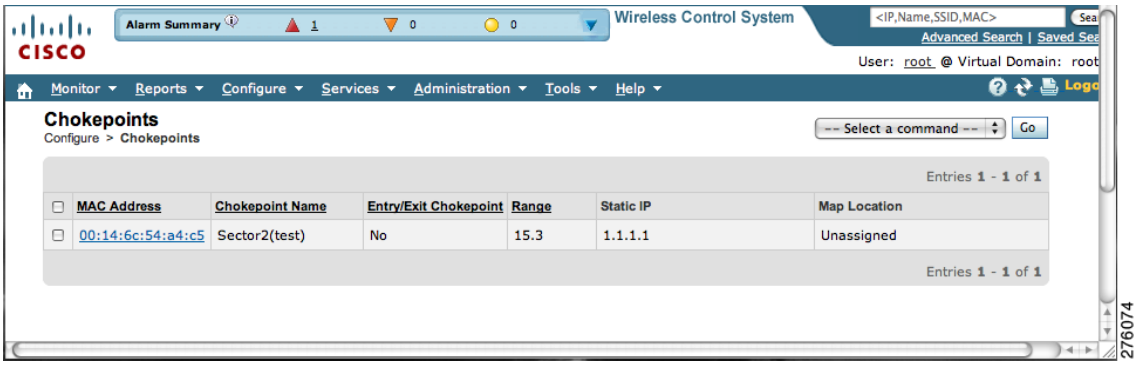
Step 4 Check the **Entry/Exit Chokepoint** check box if you want the chokepoint to function as a perimeter chokepoint. Its function is to track the entry and exit of clients and tags from an area or floor.

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).

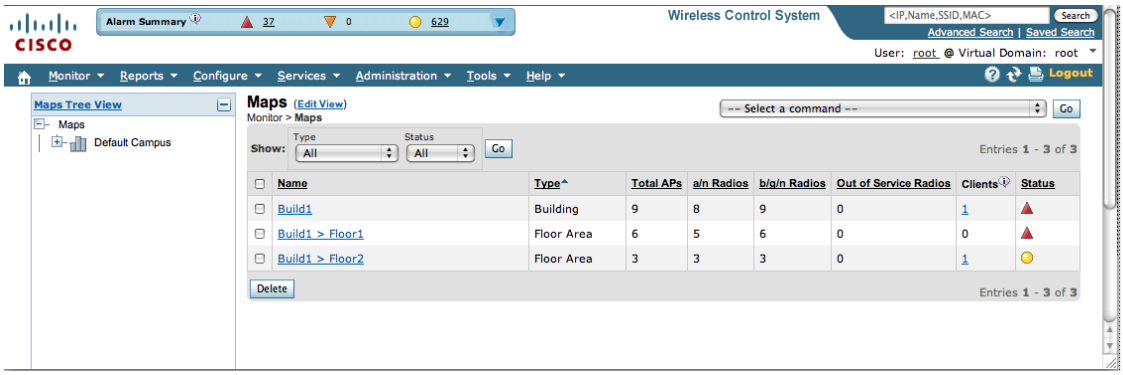
Figure 7-8 Chokepoints Summary Window



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

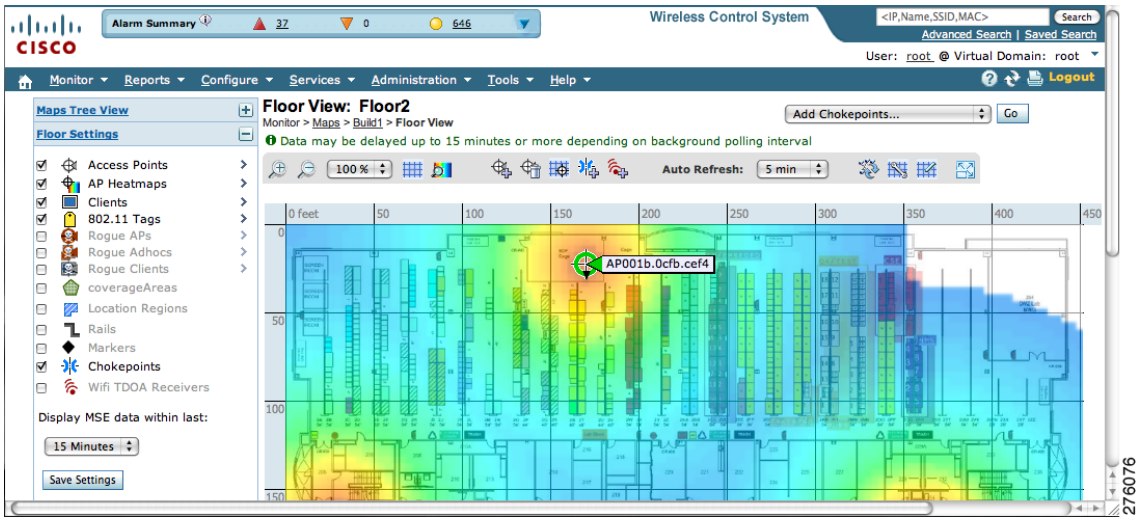
Step 6 To add the chokepoint to a map, choose **Monitor > Maps** (see Figure 7-9).

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

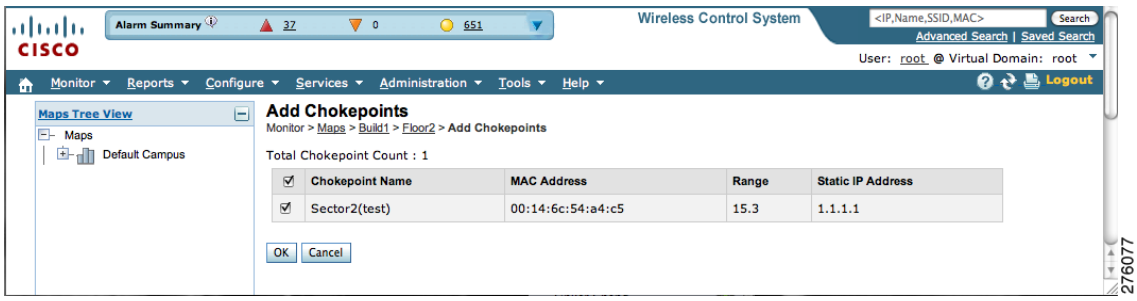


Step 8 Select **Add Chokepoints** from the Select a command menu. Click **Go**.

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

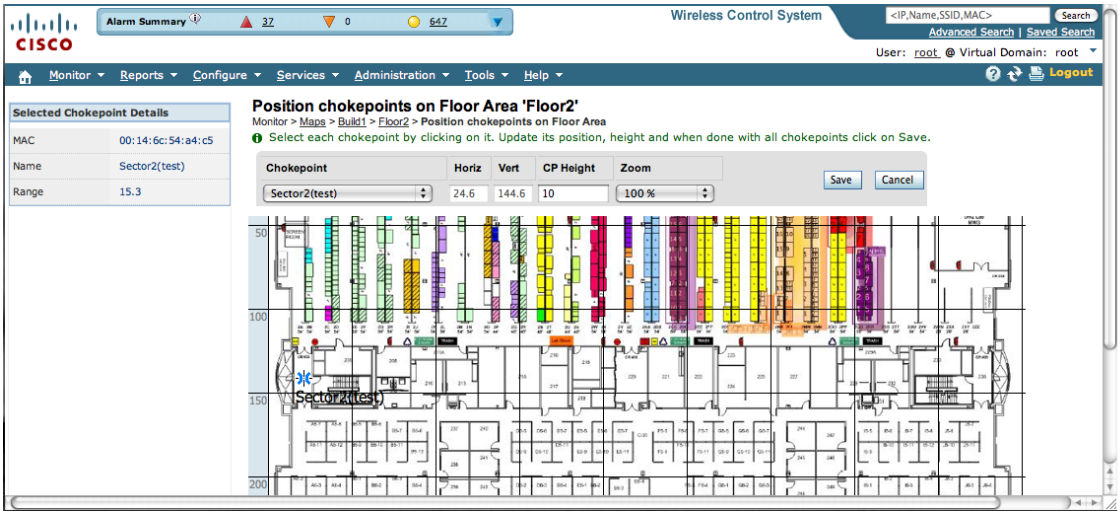


Step 9 Check the box next to the chokepoint to be added to the map. Click **OK** (bottom of screen).

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



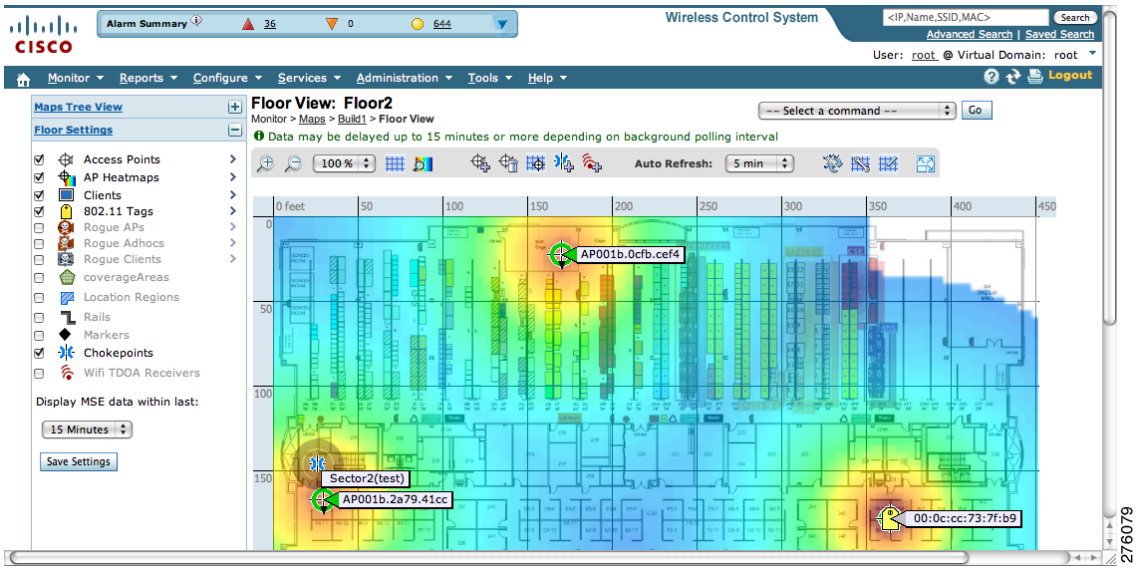
Note The MAC address, name, and coverage range of the chokepoint appear in the left panel when you click on the chokepoint icon for placement.

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.

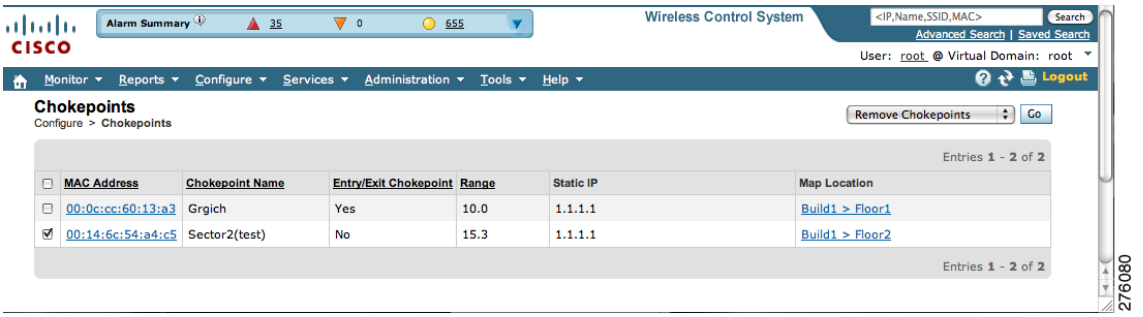
To delete a chokepoint, follow these steps:

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.

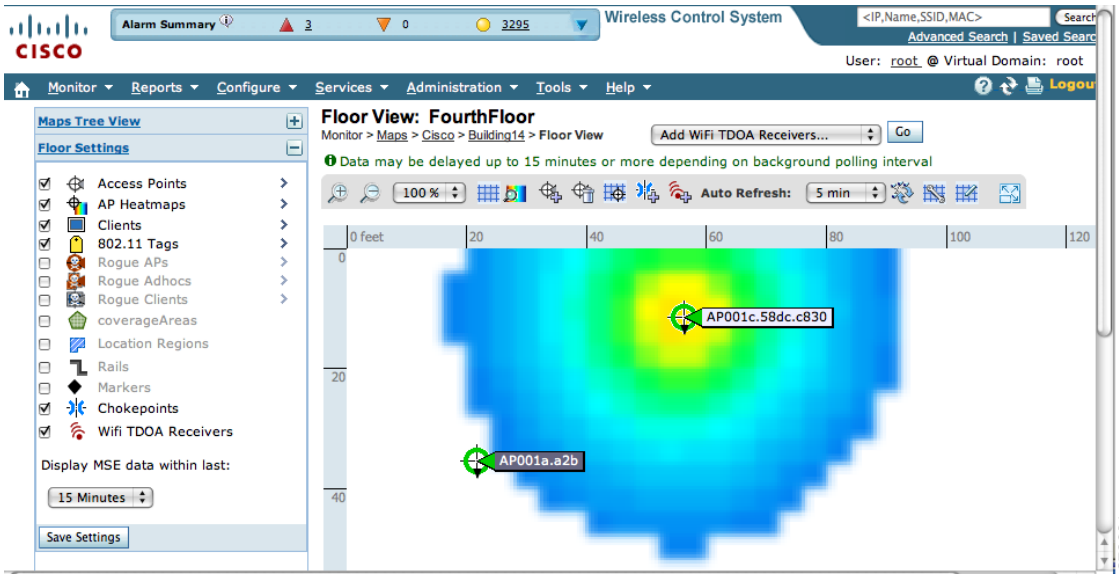
Step 5 To add the TDOA receiver to a map, choose **Monitor > Maps**.

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 > WiFi TDOA Receivers Window



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

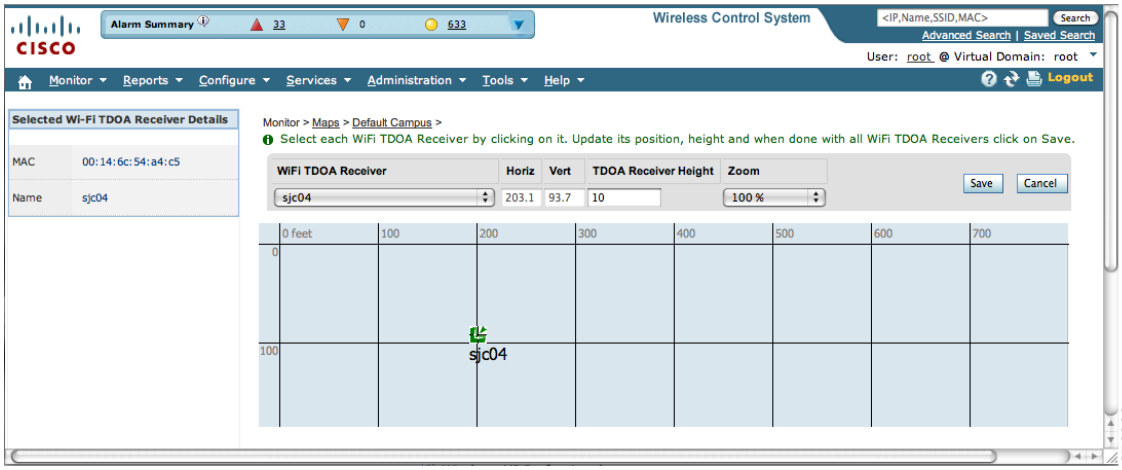
The Add WiFi TDOA Receivers summary window appears.

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

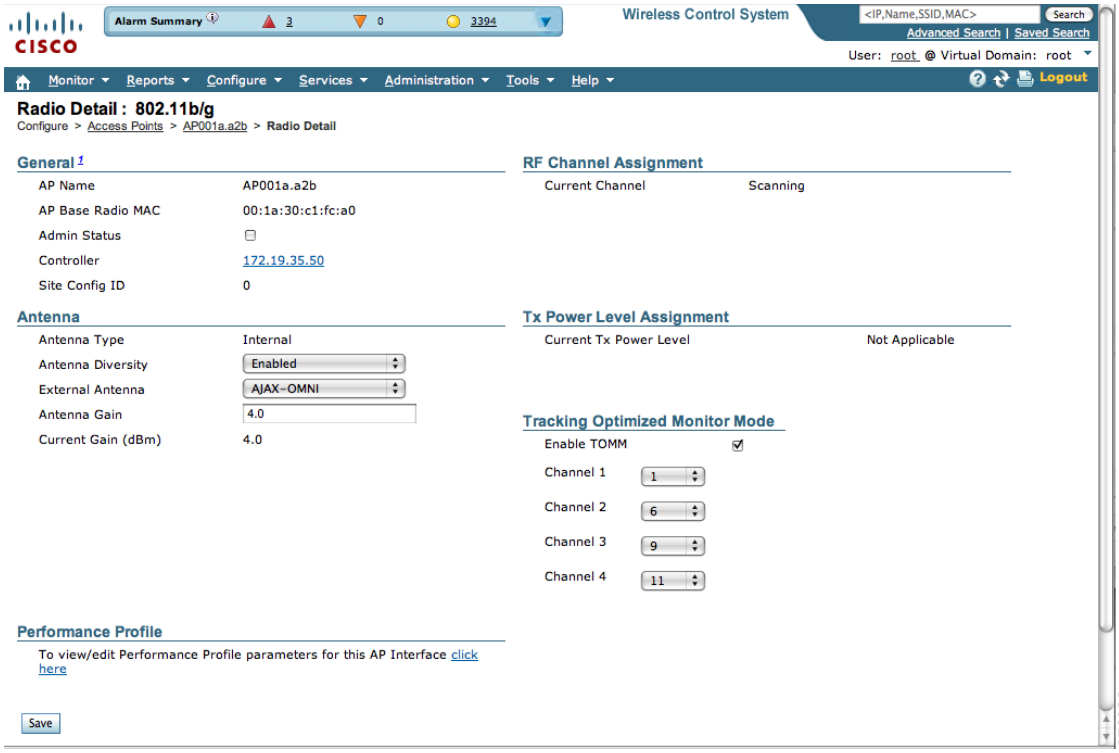
Step 2 To enable TOMM and assign monitoring channels on the access point radio, follow these steps:

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**.

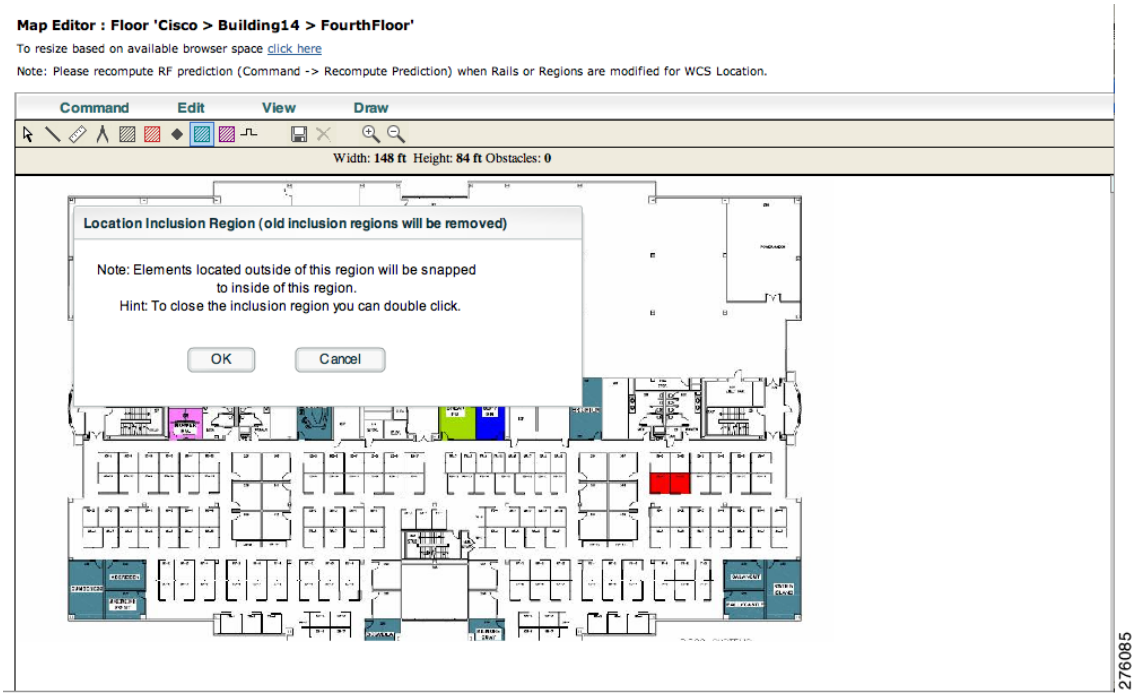
Step 2 Click the name of the appropriate floor.

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



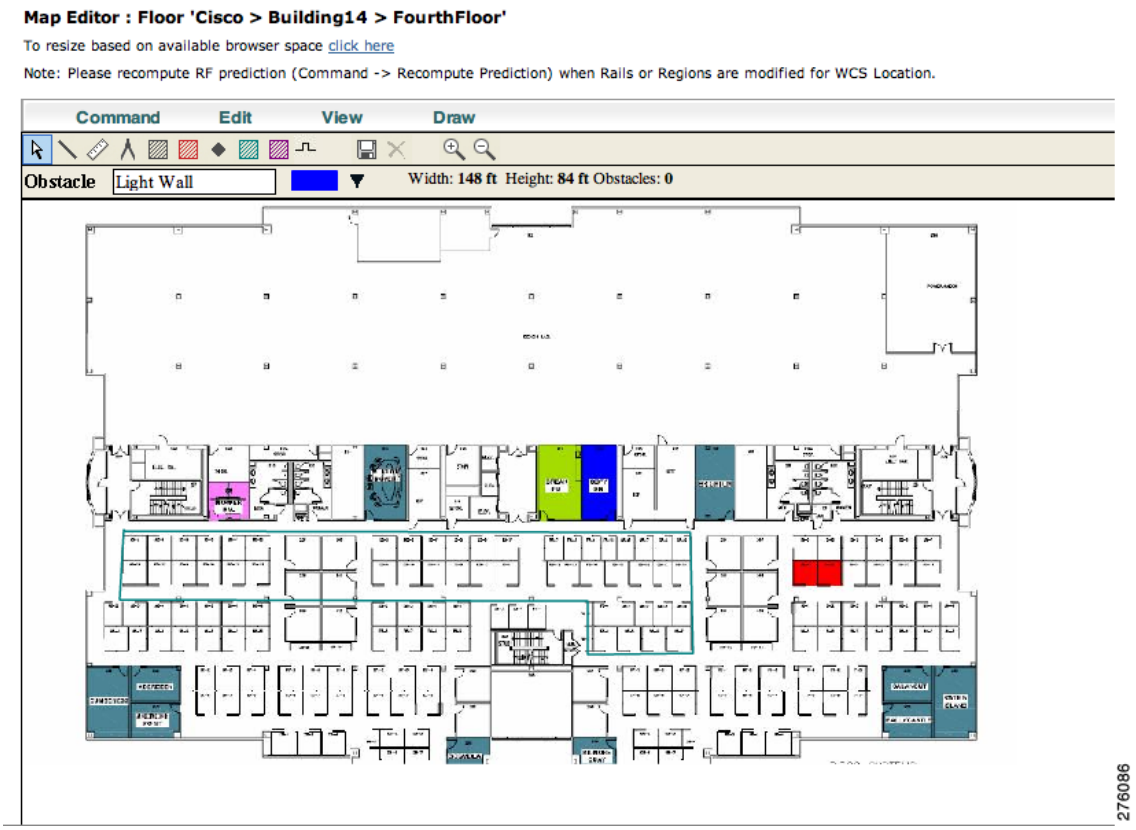
Step 5 Click **OK** in the message box that appears. A drawing icon appears to outline the inclusion area.

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.

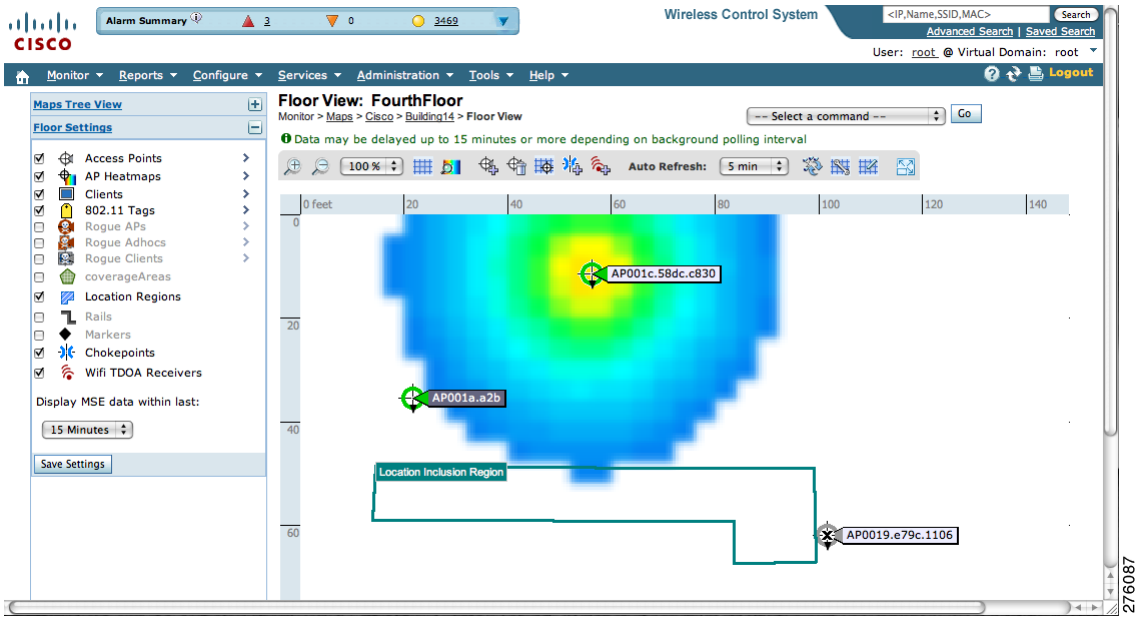
Step 10 To return to the floor map to enable inclusion regions on heatmaps, choose **Command > Exit**.

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

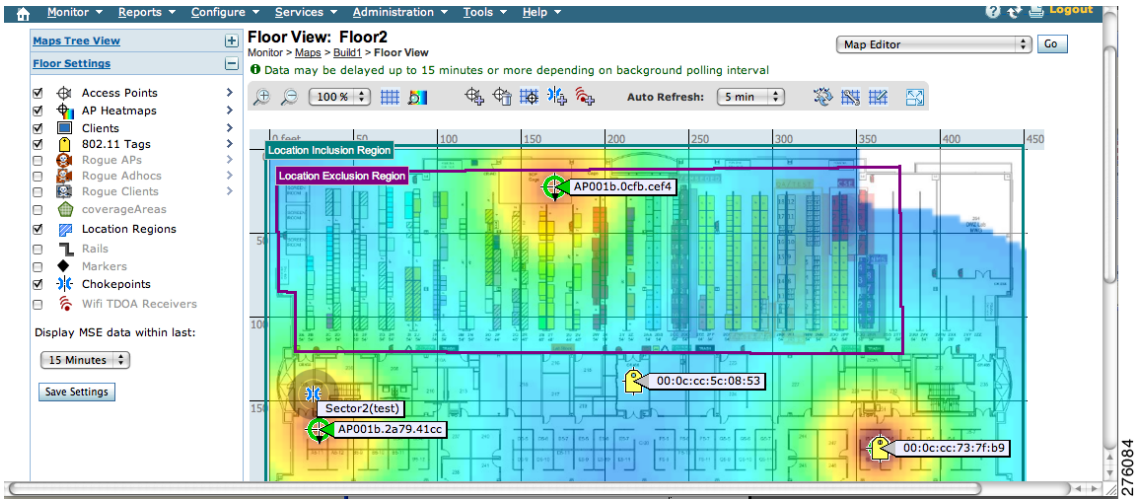
Step 10 When all exclusion areas are defined, select **Save** from the Command menu or the disk icon on the tool bar to save the exclusion region.

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:

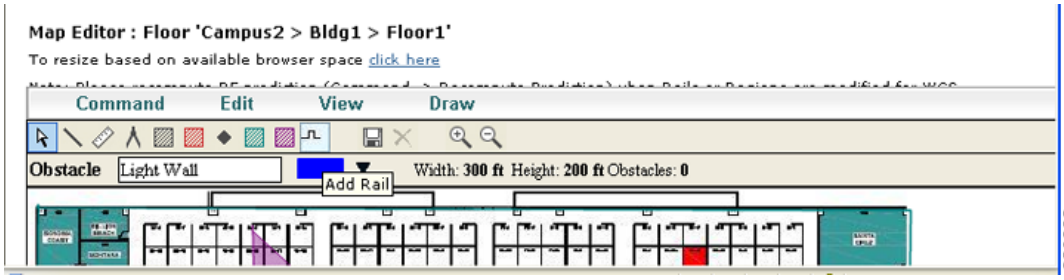
Step 1 Choose **Monitor > Maps**.

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**.

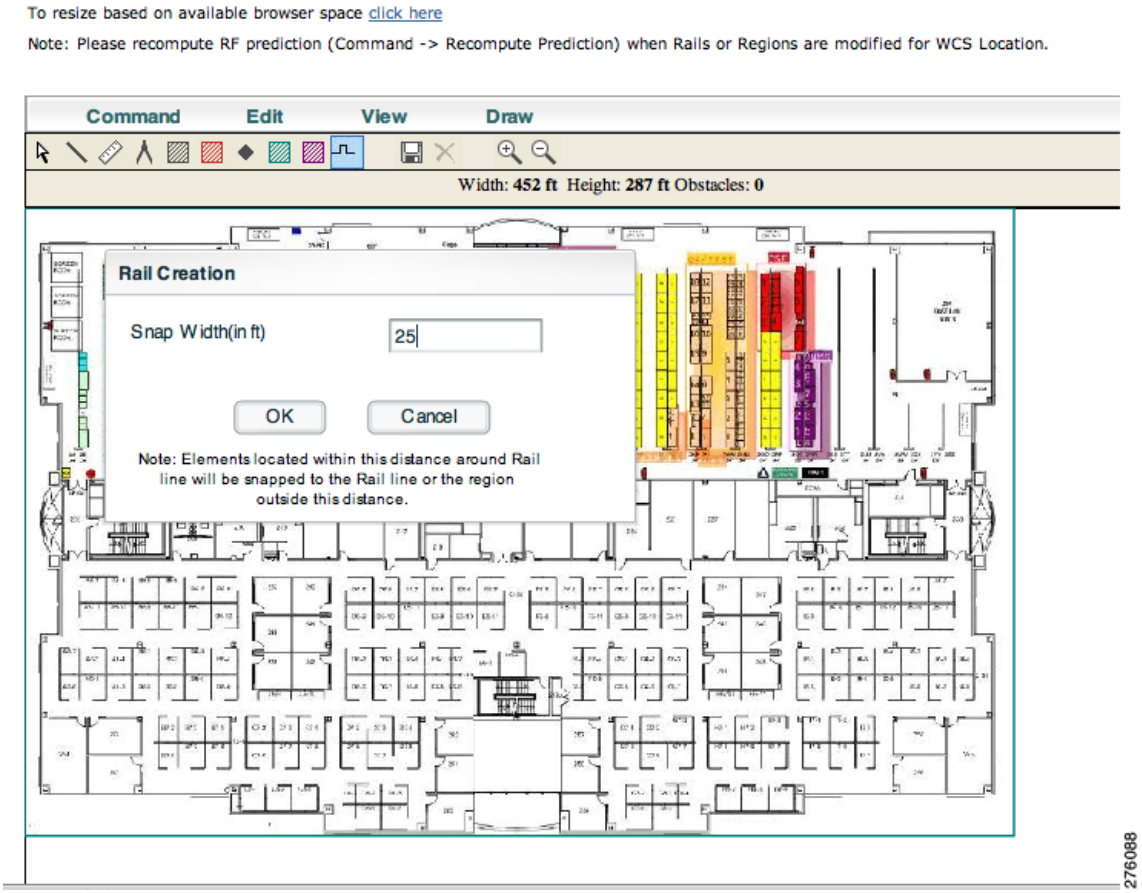
Step 4 Click the rail icon (to the right of the purple exclusion icon) in the tool bar (see Figure 7-23).

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).

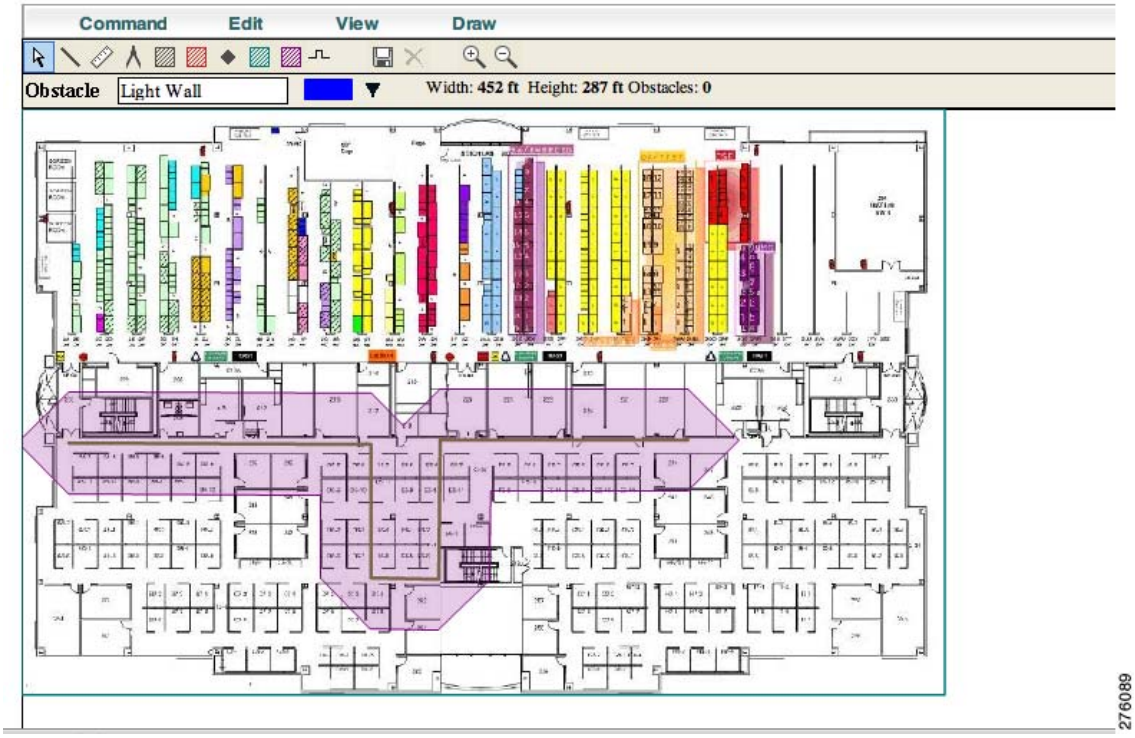
Figure 7-24 Defining Rail Width



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

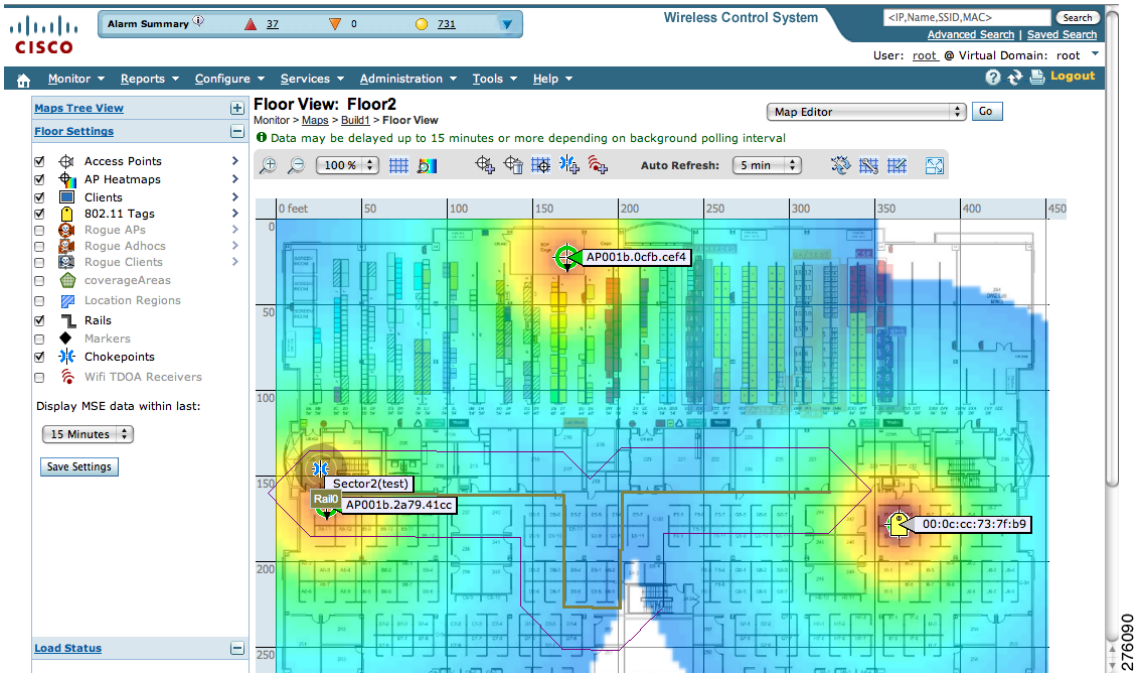


Note To delete a rail line, click on the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the ***X*** icon in the tool bar. The area is removed from the floor map.

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.

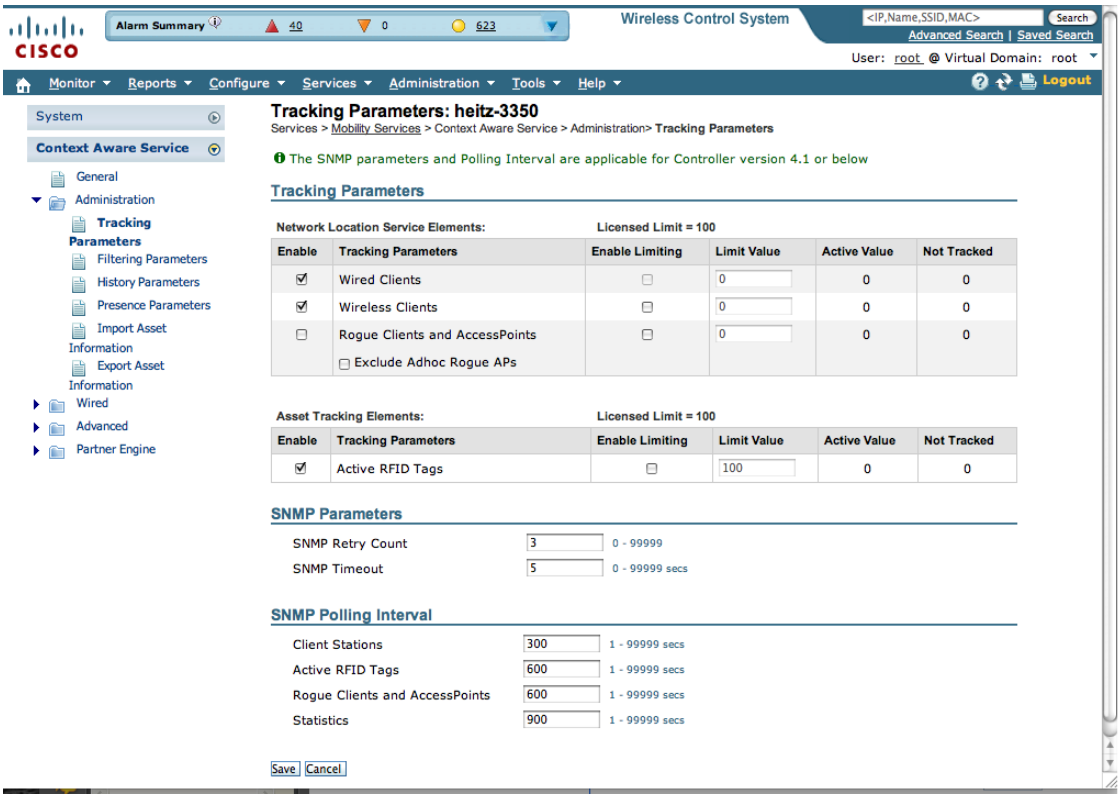
To configure tracking parameters for a mobility services engine, follow these steps:

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.

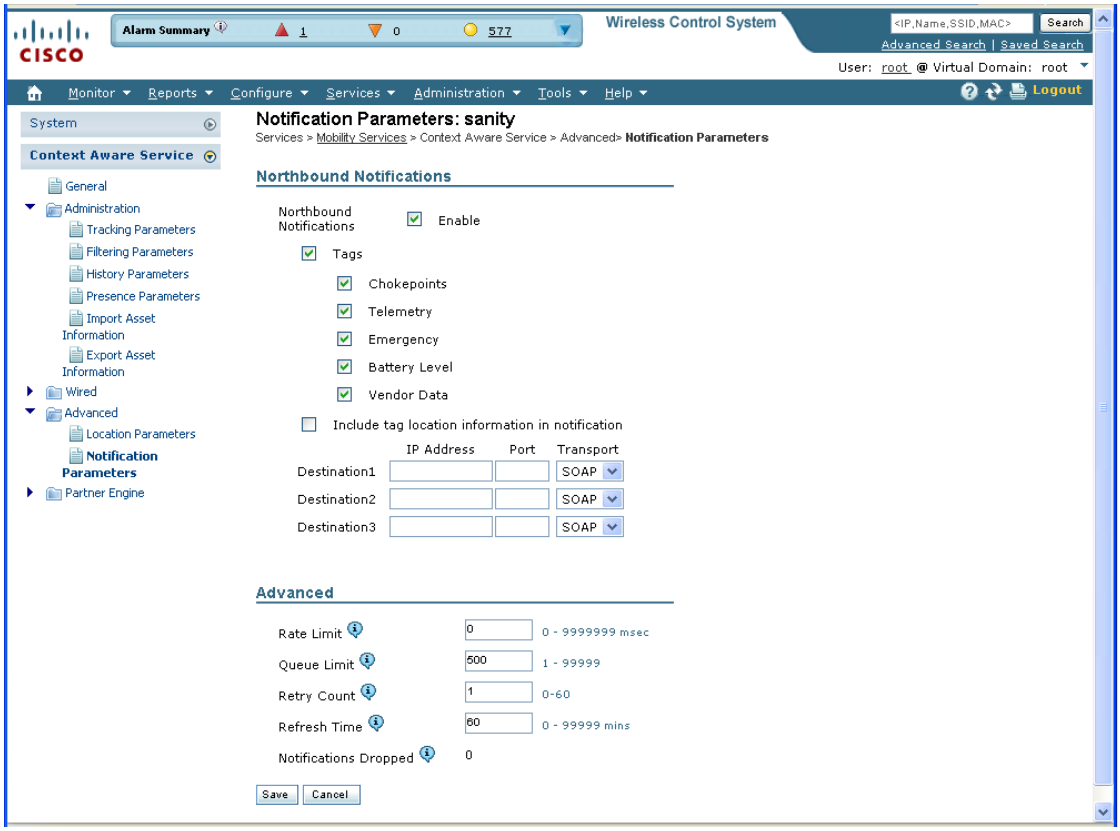
To enable northbound notifications and to configure notification parameters, follow these steps:

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.

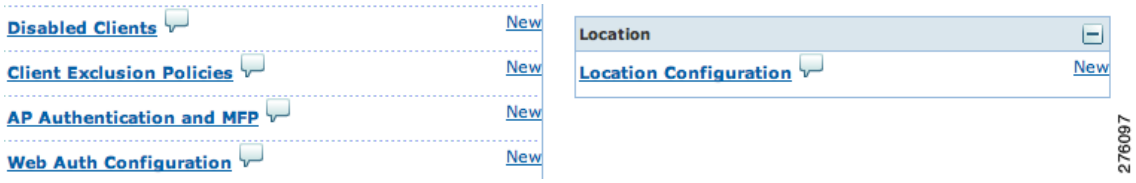
Advanced parameters–Set the RFID tag data timeout value and enable the location path loss configuration for calibrating client multi-band.

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

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

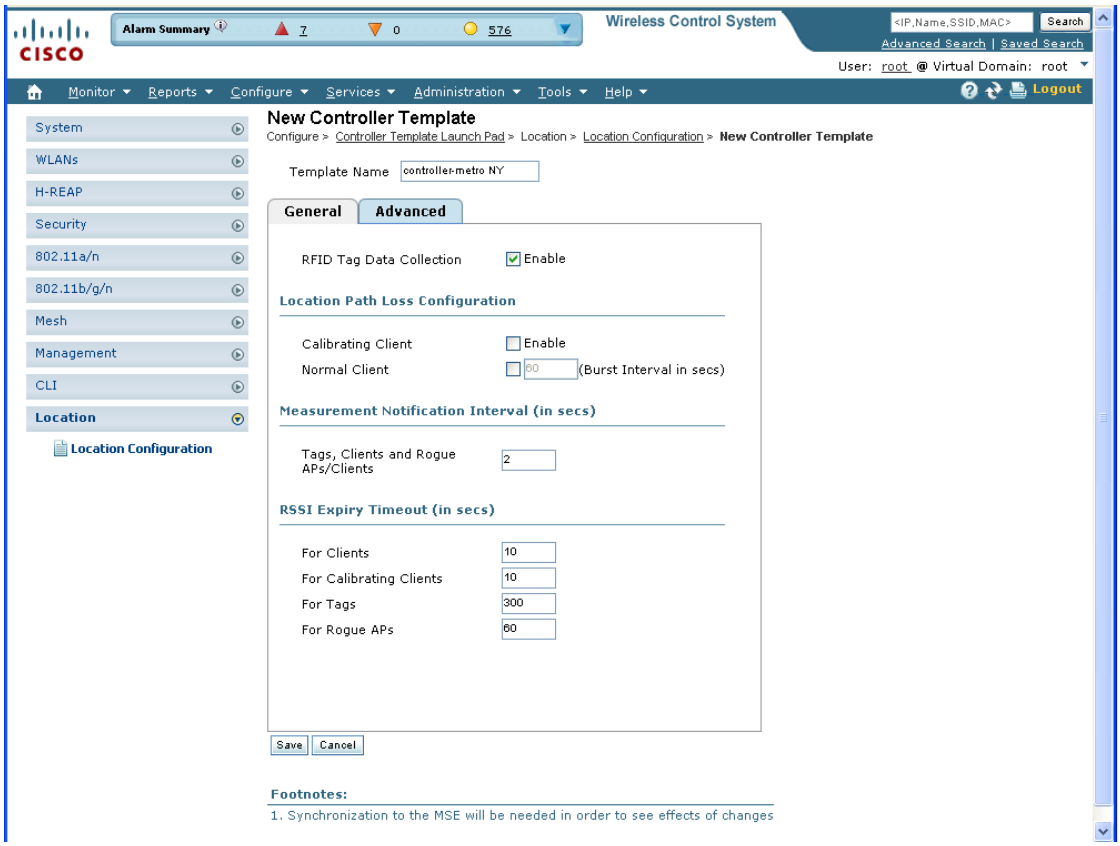
Step 2 Select the **New** (Location Configuration) link under the Location heading to create a new location template (see Figure 7-29).

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

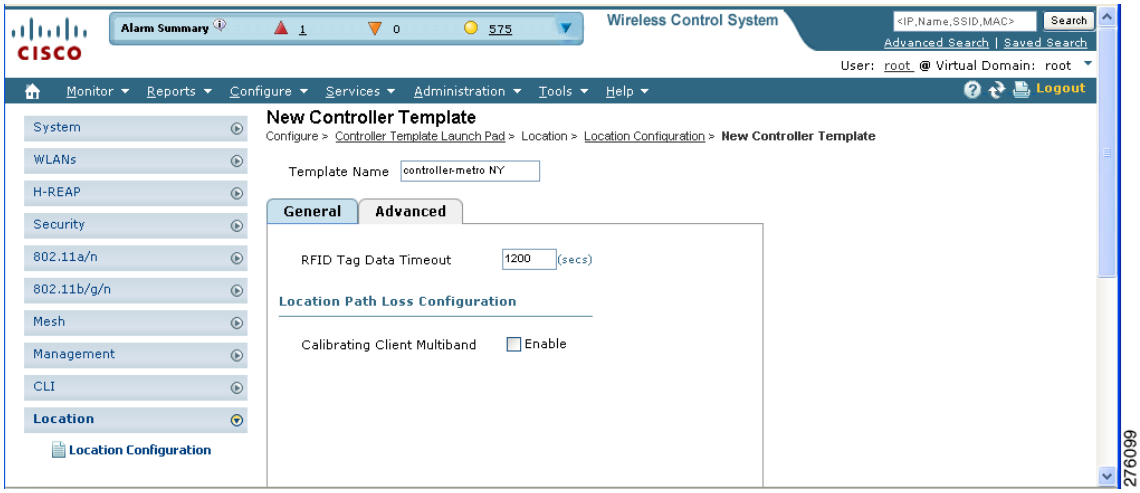


Table 7-7 Advanced Location Parameters

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

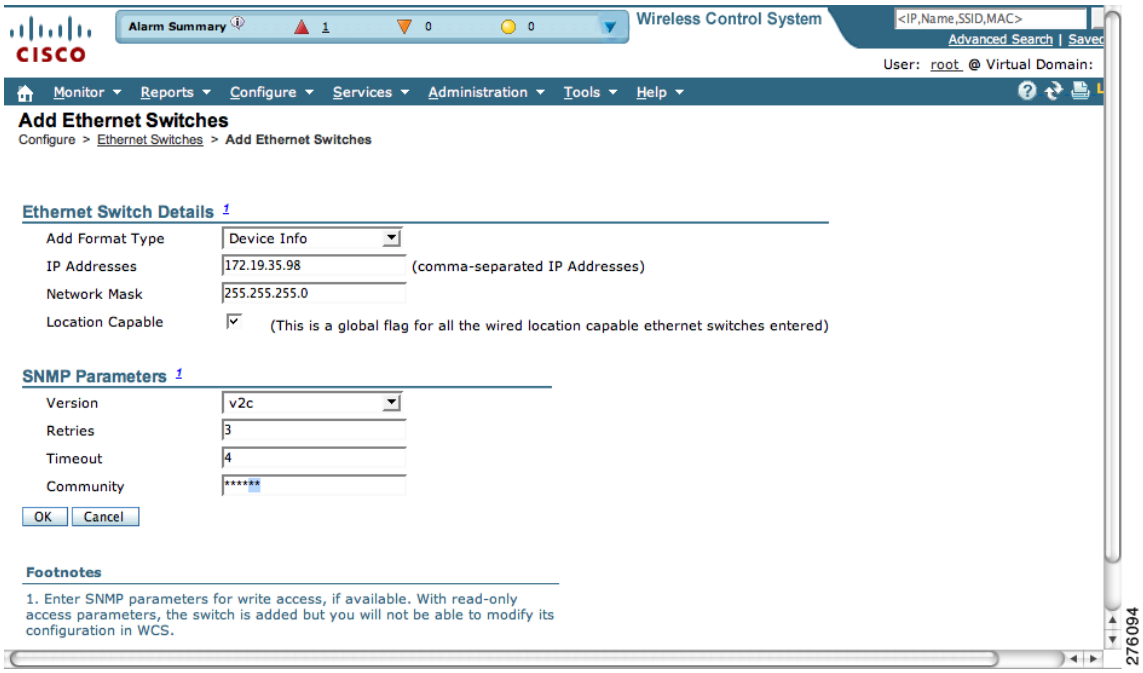
All Catalyst switches must be configured with location service before they are added to Cisco WCS. Refer to the "Configuring a Catalyst Switch" section on page 7-50.

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.

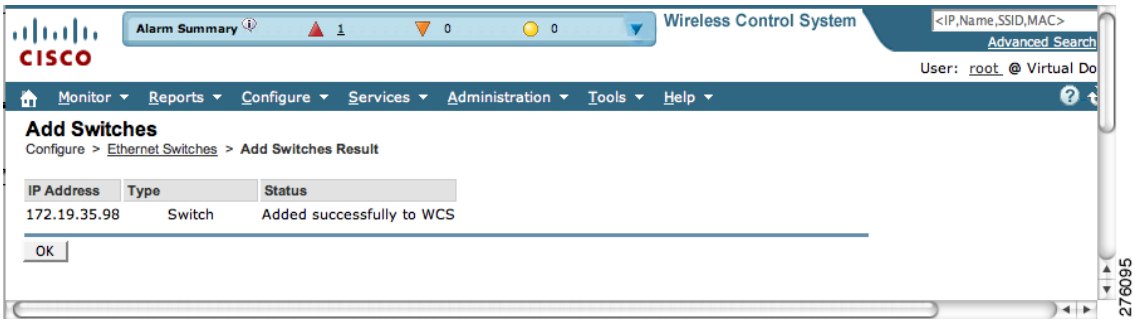
Step 7 No changes are required to the retries and timeout fields.

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.

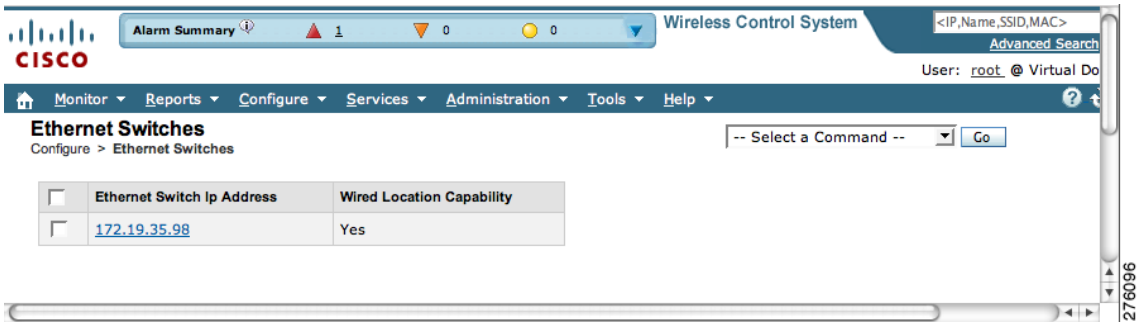
Step 9 Click **OK**. A window confirming successful addition to WCS displays (see Figure 7-33).

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.

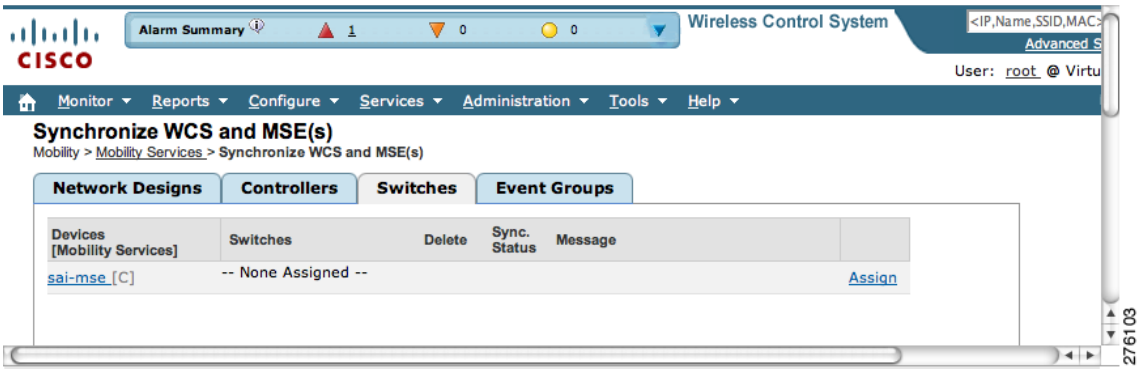
All information on wired switches and wired clients connected to those switches downloads to the mobility services engine.

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

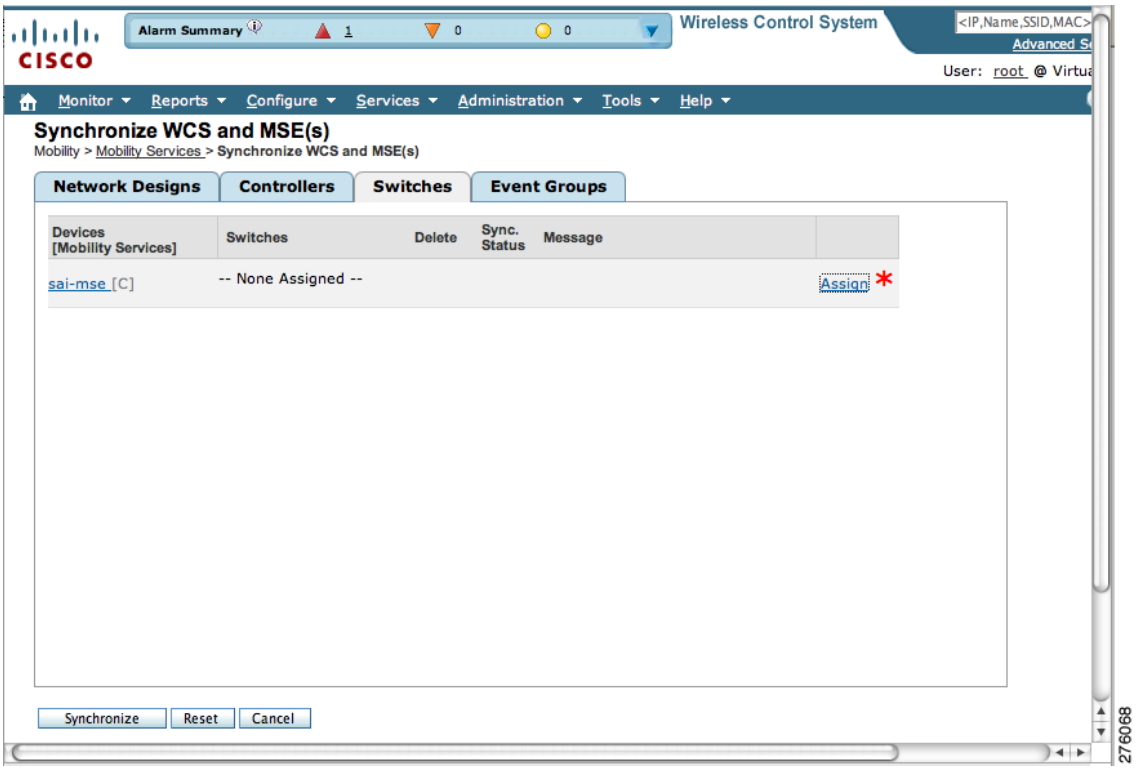


Step 3 Click the **Assign** link to assign a wired switch to a mobility services engine.

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.

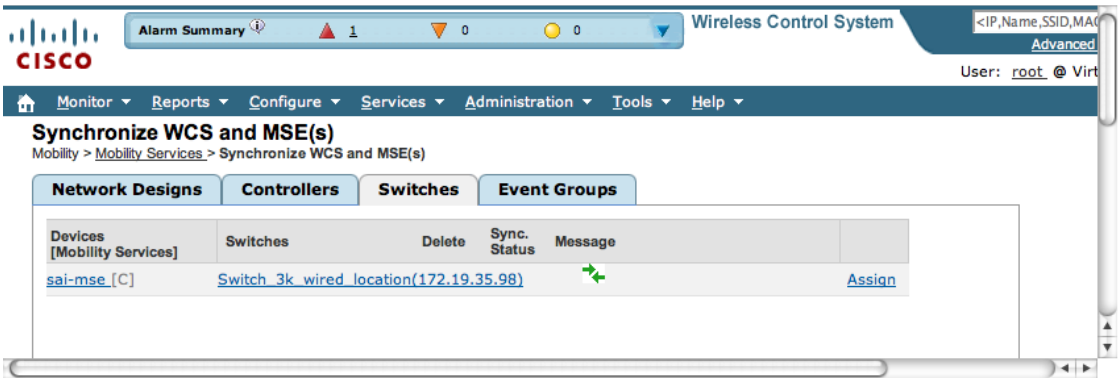
Figure 7-36 Updated Switches Panel Showing Pending Synchronization of Switch Assignment



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.

CHAPTER 8

Monitoring the System and Services

This chapter describes how to monitor the mobility services engine by configuring and viewing alarms, events, and logs as well as how to generate reports on system use and element counts (tags, clients, rogue clients, and access points).

It also describes how to use Cisco WCS to monitor clients (wired and wireless), tags, chokepoints, and Wi-Fi TDOA receivers.

This chapter contains the following sections:

Working with Alarms

This section describes how to view, assign, and clear alarms and events on a mobility services engine using Cisco WCS. It also describes how to define alarm notifications (all, critical, major, minor, warning) and detail how to email those alarm notifications.

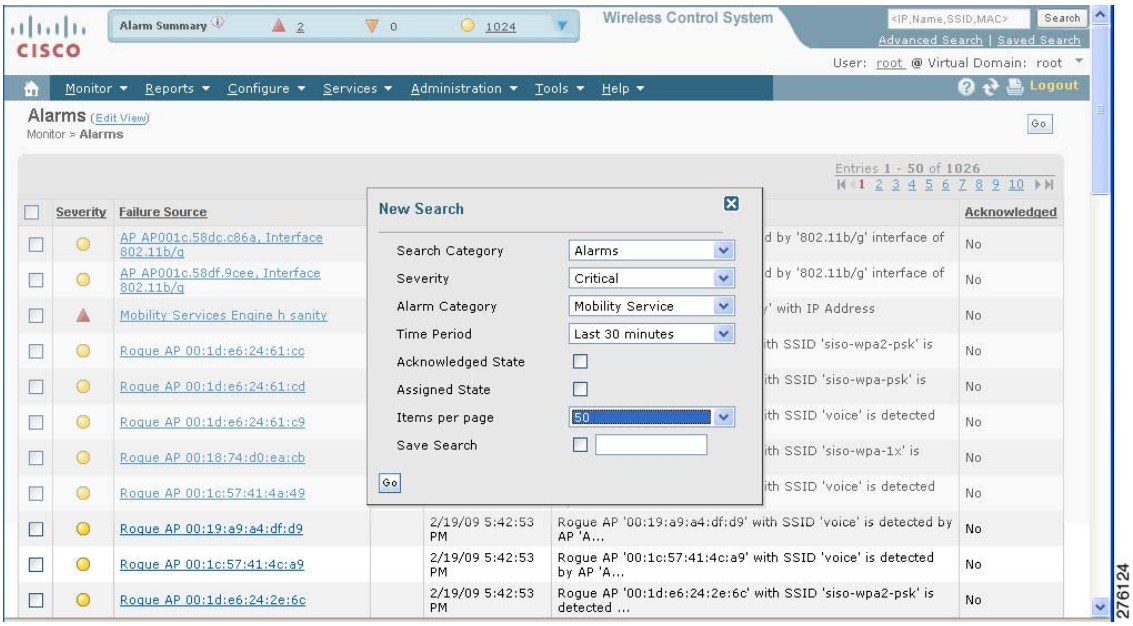
Viewing Alarms

To view mobility services engine alarms, follow these steps:

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

Step 2 Click the **Advanced Search** link in the navigation bar (top-right). A configurable search panel for alarms appears (see Figure 8-1).

Figure 8-1 Advanced Search Alarm Panel



Step 3 Select **Alarms** as the Search Category.

Step 4 Select the Severity of Alarms to display. Options are All Severities, Critical, Major, Minor, Warning or Clear.

Step 5 Select **Mobility Service** from the Alarm Category.

Step 6 Select the time frame for which you want to review alarms from the Time Period drop-down menu.

Options range from minutes (5, 15, and 30) to hours (1 and 8) to days (1 and 7). To display all, select **Any time**.

Step 7 Check the **Acknowledged State** check box to exclude the acknowledged alarms and their count from the Alarm Summary window.

Step 8 Check the **Assigned Stat**e check box to exclude the assigned alarms and their count from the Alarm Summary window.

Step 9 Select the number of alarms to display on each window from the Items per page drop-down menu.

Step 10 To save the search criteria for later use, check the **Save Search** box and enter a name for the search.

Note You can initiate the search thereafter, by clicking the Saved Searches link at the top-right of the navigation bar.

Step 11 Click **Go**. The alarms summary panel appears with search results.

Note Click the column headings (Severity, Failure Source, Owner, Date/Time, Message, and Acknowledged) to sort alarms.

Step 12 Repeat Step 2 to Step 11 to see Context-Aware notifications for the mobility services engine. Enter **Context Aware Notifications** as the alarm category in Step 5.

Assigning and Unassigning Alarms

To assign and unassign an alarm to yourself, follow these steps:

Step 1 Display the Alarms window as described in the "Viewing Alarms" section on page 8-2.

Step 2 Select the alarms that you want to assign to yourself by checking their corresponding check boxes.

Note To unassign an alarm assigned to you, uncheck the box next to the appropriate alarm. You cannot unassign alarms assigned to others.

Step 3 From the Select a command drop-down menu, choose **Assign to Me** (or **Unassign**). Click **Go**.

If you choose **Assign to Me**, your username appears in the Owner column. If you choose **Unassign**, the username column becomes empty.

Deleting and Clearing Alarms

If you delete an alarm, Cisco WCS removes it from its database. If you clear an alarm, it remains in the Cisco WCS database, but in the Clear state. You should clear an alarm when the condition that caused it no longer exists.

To delete or clear an alarm from a mobility services engine, follow these steps:

Step 1 Display the Alarms window as described in the "Viewing Alarms" section on page 8-2.

Step 2 Select the alarms that you want to delete or clear by checking their corresponding check boxes.

Step 3 From the Select a command drop-down menu, choose **Delete** or **Clear**. Click **Go**.

Emailing Alarm Notifications

Cisco WCS lets you send alarm notifications to a specific email address. Sending notifications through email enables you to take prompt action when needed.

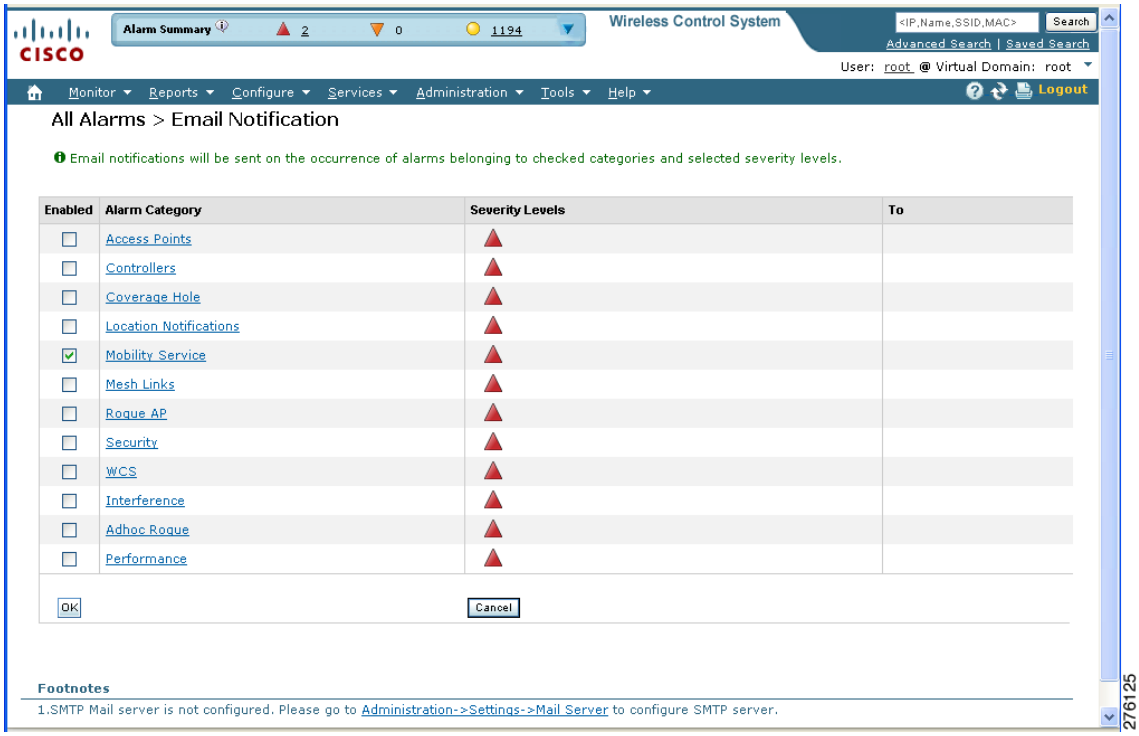
You can choose the alarm severity types (critical, major, minor, and warning) to have emailed to you.

To send alarm notifications, follow these steps:

Step 1 Choose **Monitor > Alarms**.

Step 2 From the Select a command drop-down menu, choose **Email Notification**. Click **Go**. The Email Notification window appears (see Figure 8-2).

Figure 8-2 All Alarms > Email Notification Window



Note A SMTP Mail Server must be defined before you enter target email addresses for email notification. Choose **Administration > Settings > Mail Server Configuration** to enter the appropriate information. You can also select the **Administration > Settings > Mail Server** link, if it is displayed at the bottom of the All Alarms > Email Notification Window noted above.

Step 3 Click the **Enabled** check box next to **Mobility Service**.

Note Enabling the **Mobility Service** alarm category sends all alarms related to mobility services engine and the location appliance to the defined email address.

Step 4 Click the **Mobility Service** link. The window for configuring the alarm severity types that are reported for the mobility services engine appears.

Step 5 Check the check box next to all the alarm severity types for which you want email notifications sent.

Step 6 In the To field, enter the email address or addresses to which you want the email notifications sent. Separate Email addresses by commas.

Step 7 Click **OK**.

You are returned to the Alarms > Notification window. The changes to the reported alarm severity levels and the recipient email address for email notifications are displayed.

Working with Events

You can use Cisco WCS to view mobility services engine and location notification events. You can search and display events based on their severity (critical, major, minor, warning, clear, and info) and event category.

You can search by the following event categories:

- By network coverage: coverage holes and interference
- By link: mesh links
- By notifications: location notifications
- By product type: access points (rogue and non-rogue), clients, controllers, or mobility service
- By security

Additionally, you can search for an element's events by its IP address, MAC address, or name.

A successful event search displays the event severity, failure object, date and time of the event, and any messages for each event.

To display events, follow these steps:

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

Step 2 In the Events window:

- If you want to display the events for a specific element, and you know its IP address, name, WLAN SSID, or MAC address, enter that value in the Search field of the navigation bar (top-right). Click **Search.**
- To display events by severity and category, click **Advanced Search** in the navigation bar and select the appropriate options from the Severity and Event Category drop-down menus. Click **Go**.

Step 3 If Cisco WCS finds events that match the search criteria, it displays a list of these events.

Note For more information about an event, click the failure source associated with the event. Additionally, you can sort the events summary by each of the column headings.

Working with Logs

This section describes how to configure logging options and how to download log files.

Configuring Logging Options

You can use Cisco WCS to specify the logging level and types of messages to log.

To configure logging options, follow these steps:

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

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

Step 3 Choose **System > Advanced**. The advanced parameters for the selected mobility services engine appear.

Step 4 Scroll down to the Logging Options section and choose the appropriate option (off, error, information, or trace) from the Logging Level drop-down menu.

Caution Use **Error** and **Trace** only when directed to do so by Cisco Technical Assistance Center (TAC) personnel.

Step 5 Check the **Enabled** check box next to each element listed in that section to begin logging its events.

Step 6 Click **Save**.

Downloading Log Files

If you need to analyze mobility services engine log files, you can use Cisco WCS to download them to your system. Cisco WCS downloads a zip file containing the log files.

To download a zip file containing the log files, follow these steps:

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

Step 2 Click the name of the mobility services engine to view its status.

Step 3 Choose **System > Logs**.

Step 4 Click **Download Logs**.

Step 5 Follow the instructions in the File Download dialog box to open the file or save the zip file to your system.

Generating Reports

In Cisco WCS, you can generate a device utilization and location utilization report for a mobility services engine. By default, reports are stored on the Cisco WCS server.

Once you define the report criteria, you can save the device and location utilization reports for future diagnostic use and run them on either an ad hoc or scheduled basis.

You can define the following criteria for a device utilization report:

- Which mobility services engine or engines to monitor
- How often the report is generated
- How the data is graphed on the charts
- Whether the report is emailed or exported to a file

You can view the following in a location utilization report:

- Chart 1 summarizes and graphs CPU and memory utilization
- Chart 2 summarizes and graphs client count, tag count, rogue client count, rogue access point count, and ad hoc rogue count

Creating a Device Utilization Report

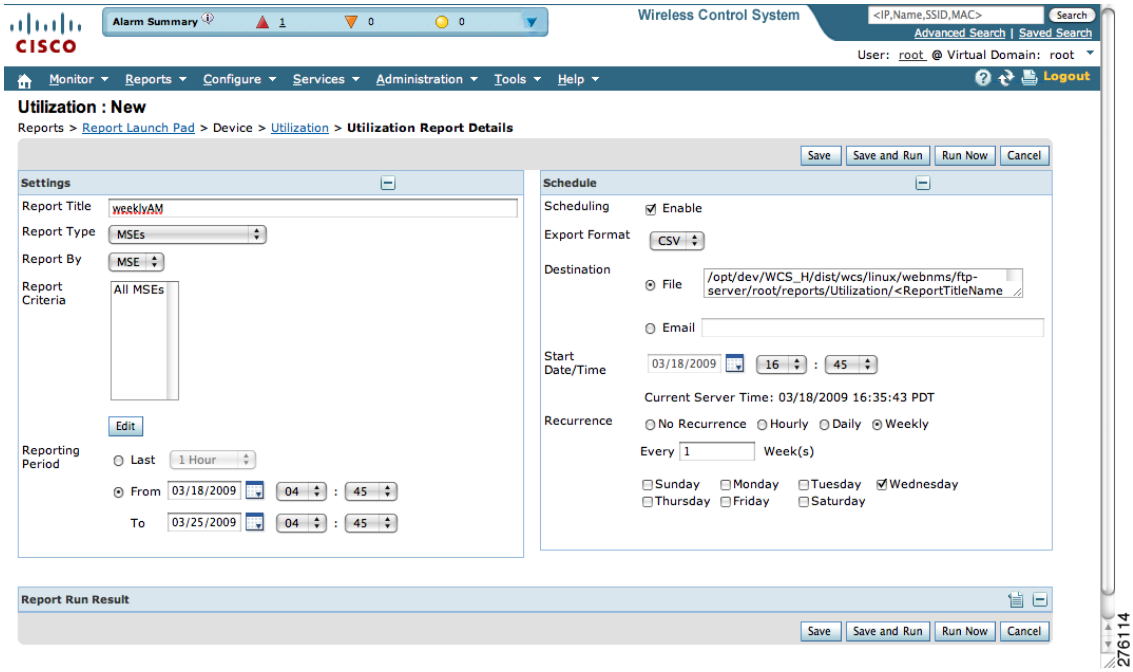
To create a device utilization report for the mobility services engine, follow these steps:

Step 1 In Cisco WCS, choose **Reports > Report Launch Pad**.

Step 2 Choose **Device > Utilization**.

Step 3 Click **New**. The Utilization: New window appears (see Figure 8-3).

Figure 8-3 Device > Utilization Window



Step 4 In the Settings panel (left), enter a report title.

Step 5 The Report Type and Report By selections are always MSE.

Step 6 Click **Edit** to select either a specific mobility services engine or **All MSEs** from the pop-up panel that appears.

Step 7 Enter the reporting period. You can define the report to collect data hourly, weekly, or at a specific date and time. The selected reporting period type will display on the x-axis.

Note The reporting period uses a 24-hour rather than a 12-hour clock. For example, select hour 13 for 1:00 p.m.

Step 8 In the Schedule panel (right), check the **Enable Schedule** check box.

Step 9 Select the report format (CSV or PDF) from the Export Report drop-down menu.

Step 10 Select either **File** or **Email** as the destination of the report.

- If you select the File option, a destination path must first be defined at the **Administration > Settings >** *Report* window. Enter the destination path for the files in the Repository Path field.
- If you select the Email option, an SMTP Mail Server must be defined prior to entry of target email address. Choose **Administrator > Settings >** *Mail Server Configuration* to enter the appropriate information.

Step 11 Enter a start date (MM:DD:YYYY) or click the calendar icon to select a date.

Step 12 Specify a start time using the hour and minute drop-down menus.

Step 13 Click one of the Recurrence buttons to select how often the report is run.

Note The days of the week appear on the screen only when the weekly option is chosen.

Step 14 When finished with all of the above steps, do one of the following:

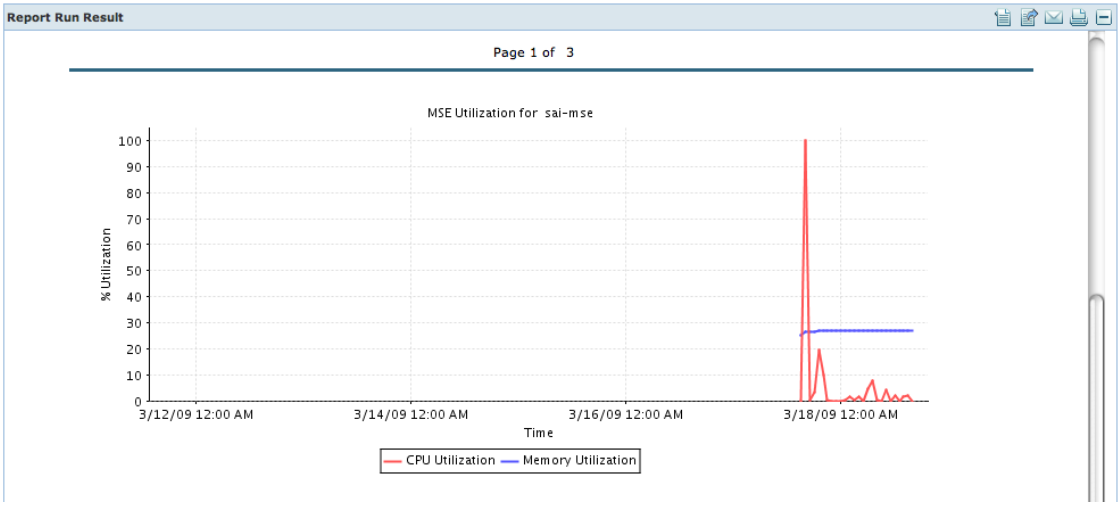
- Click **Save** to save edits. The report is run at the designated time and the results are either emailed or saved to a designated file as defined in the Schedule panel.
- Click **Save and Run** to save the changes and run the report now. The report runs regardless of any pending, scheduled run of that report. Results appear the bottom of the window. The report also runs at the designated time and the results are either emailed or saved to a designated file as defined in the Schedule panel.
  - At the results window, click **Cancel** to cancel the defined report.
- Click **Run Now** if you want to run the report immediately and review the results in the WCS window. The report runs regardless of any pending, scheduled run of that report. Results appear at the bottom of the window. Click **Save** if you want to save the report criteria you entered.

Note You can also use the **Run Now** command to check the defined report criteria before saving it or to run reports as necessary.

The results appear at the bottom of the window (see Figure 8-4).

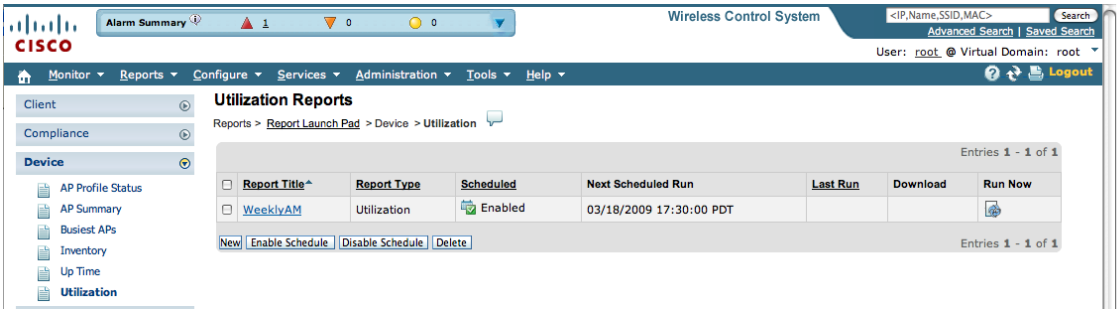
Note Only the CPU and memory utilization reports as shown in the example below (see Figure 8-4).

Figure 8-4 Devise > MSE Utilization > Results



Step 15 If you selected the Save or Save and Run option, click either **Reports > Saved Reports** (or **Reports > Scheduled Runs** if it has not yet run and is scheduled to run). The Utilization Reports summary window appears (see Figure 8-5).

Figure 8-5 Utilization Reports Summary Window



If the report is scheduled, it is shown as enabled and the next scheduled run date is noted.

If the report has run and is not scheduled to run again, it is shown as expired.

If the report has run and is scheduled to run again, it is shown as disabled.

Step 16 To enable, disable, or delete a report, check the check box next to the report title and click the appropriate option.

Viewing Saved Utilization Reports

To download a saved report, follow these steps:

Step 1 In Cisco WCS, choose **Reports > Saved Reports**.

Step 2 Click the **Download** icon for your report. It is downloaded and saved in the defined directory or emailed.

Viewing Scheduled Utilization Runs

To review status for a scheduled report, follow these steps:

Step 1 In Cisco WCS, choose **Reports > Scheduled Runs**.

Step 2 Click the **History** icon to see the date of the last report run.

Step 3 Click the **Download** icon for your report. It is downloaded and saved in the defined directory or emailed.

Monitoring Wireless Clients

Monitoring Wireless Clients Using Maps

On a Cisco WCS map, you can view the name of the access point that generated the signal for a client, its strength of signal, and when the location information was last updated for the client. Move the cursor over the client icon on the map to display this information.

You can also view the client details window, which provides statistics (such as client association, client RSSI, and client SNR), packets transmitted and received values, events, and security information for that client.

To determine a client's location status on a map and view its client details window using maps, follow these steps:

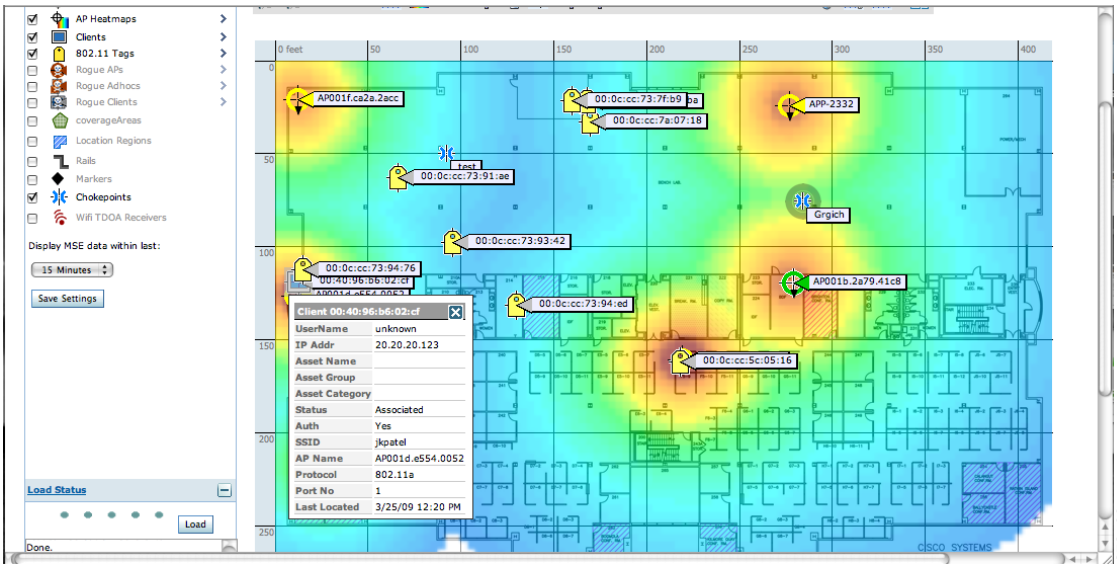
Step 1 In Cisco WCS, choose **Monitor > Maps**.

Step 2 Choose the building and floor on which the mobility services engine and its clients are located.

Step 3 Check the **Clients** check box in the Floor Settings panel (left), if it is not already checked (see Figure 8-6).

Note Do not click **Save Settings** unless you want to save changes made to the floor settings across all maps.

Figure 8-6 Monitor > Maps > Building > Floor Window



Step 4 Move the cursor over a client icon (blue square) and a summary of its configuration appears in a pop-up panel.

Step 5 Click the client icon to see client details (see Figure 8-7 and Figure 8-8).

Figure 8-7 Client Details Window (1 of 2)

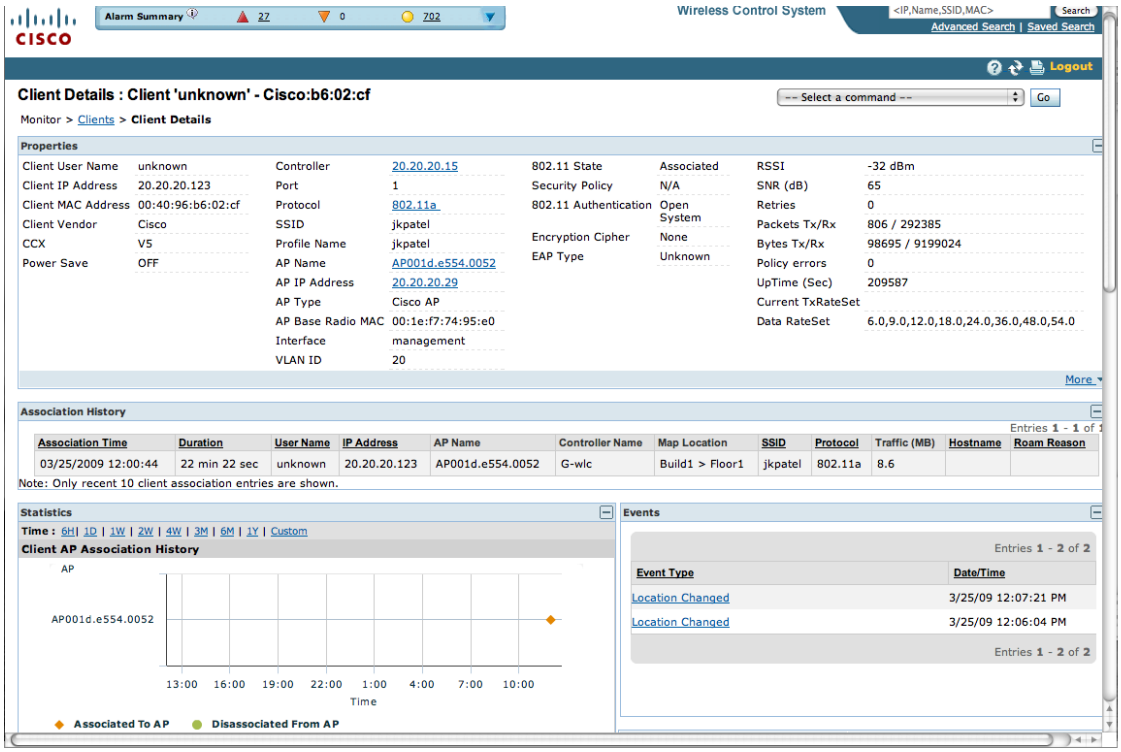
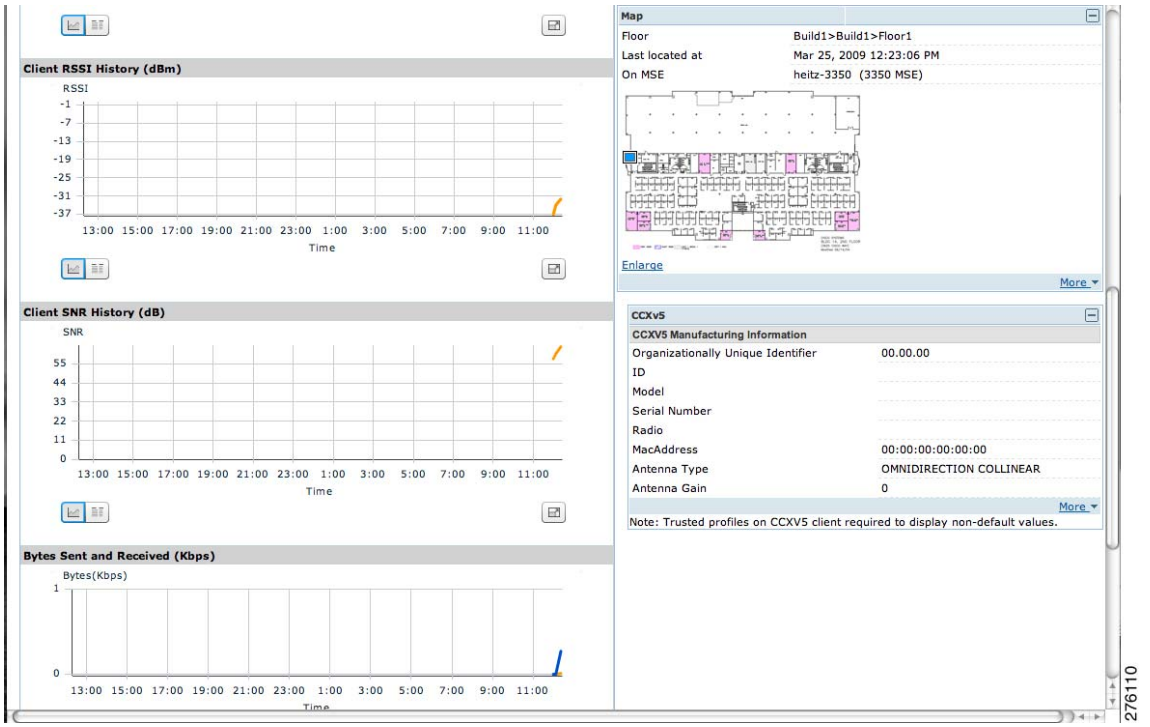


Figure 8-8 Client Details Window (2 of 2)



Monitoring Wireless Clients Using Search

You can view client information in summary and in detail at the **Monitor > Clients** window and on maps (Monitor > Maps).

To view client information, follow these steps:

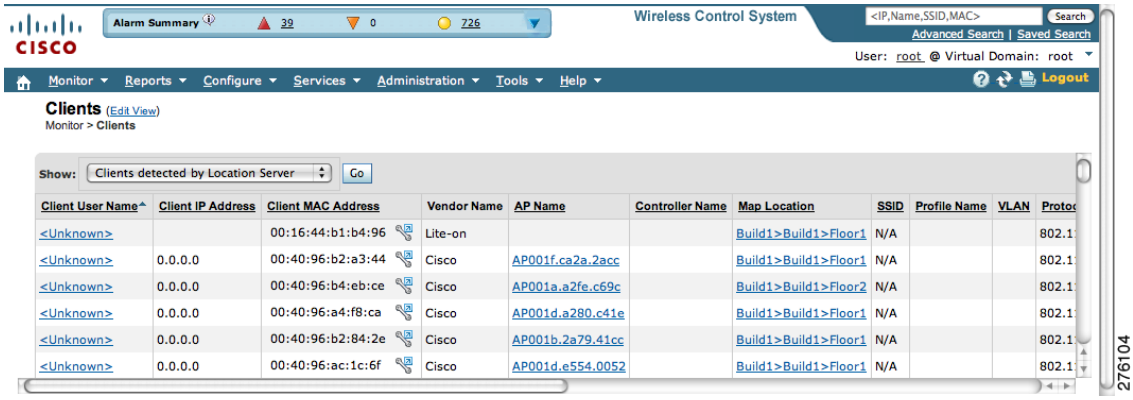
Step 1 In Cisco WCS, choose **Monitor > Clients**.

The Clients summary window appears.

Step 2 Select **Clients Detected by MSEs** from the Show drop-down menu. Click **Go**.

A summary of all clients detected by all mobility services engines and location appliances managed by Cisco WCS displays (see Figure 8-9).

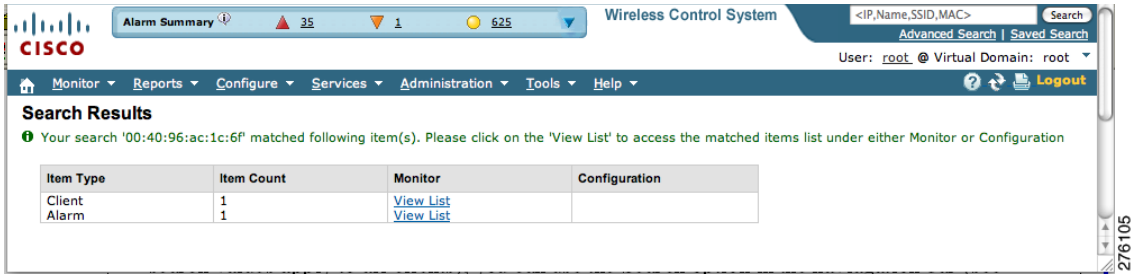
Figure 8-9 Monitor > Clients Window



a. To find a specific client by its IP address, name, SSID or MAC address, enter that value into the Search field in the navigation bar (not all search values apply to all clients).

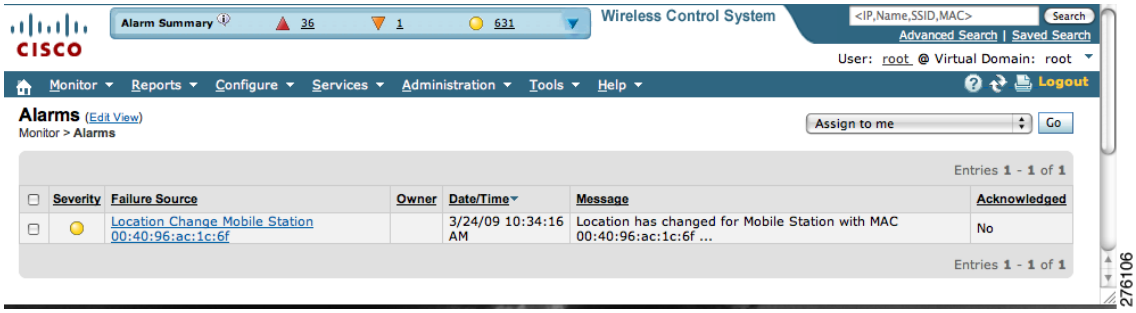
   For example, if you enter a MAC address in the search field, the following window appears (see Figure 8-10).

Figure 8-10 Search by MAC address Results



1. To see more configuration details about the client, click **View List** for the client item type. Details shown include associated devices (access point, controller), map location, VLAN, protocol, and authentication type.
2. To see alarms for the client, click **View List** for the alarm item type. A listing of all active alarms for that client noting severity, failure source (alarm description), owner of alarm (if assigned), date and time of the alarm, and whether or not alarm is acknowledged (see Figure 8-11).

Figure 8-11 Alarm Summary for Client

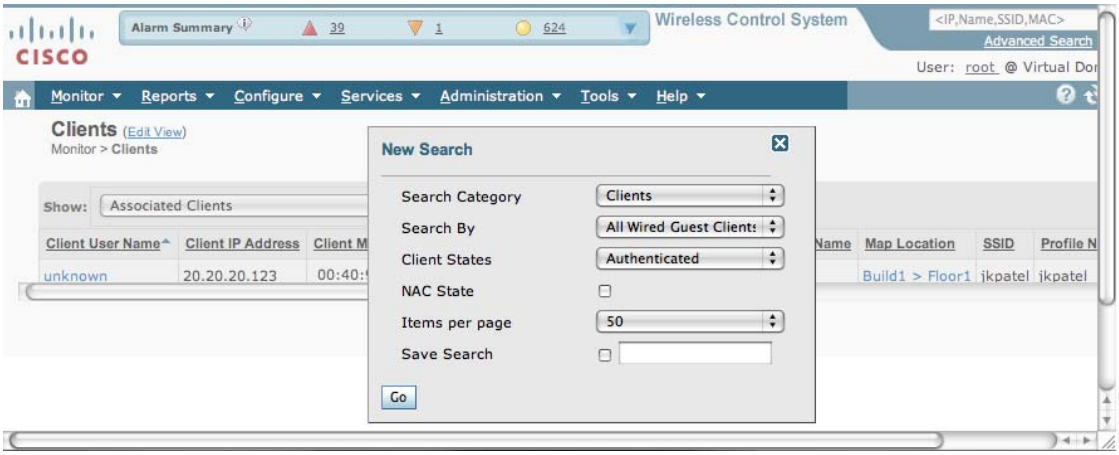


Note You can also assign or unassign the alarm, email it, delete or clear it, and acknowledge and unacknowledge it at this window by selecting the appropriate option from the Select a command drop-down menu.

b. To search for a client or multiple clients by device, network, map location and type of client (regular, rogue, or shunned), use Advanced search located in the navigation bar.

You can further define the client category by: all clients, all excluded clients, all wired guest clients, and all logged in clients using the Search By drop-down menu (see Figure 8-12).

Figure 8-12 Advanced Search Window



Step 3 Click on the appropriate client.

Monitoring Tags

You can monitor tag status and location on Cisco WCS maps as well as review tag details on the **Monitor > Tags** window. You can also use Advanced Search to monitor tags.

Monitoring Tags Using Maps

On a Cisco WCS map, you can view the name of the access point that generated the signal for a tagged asset, its strength of signal, and when the location information was last updated for the asset. Move the cursor over the tag icon on the map to display this information.

To enable tag location status on a map, follow these steps:

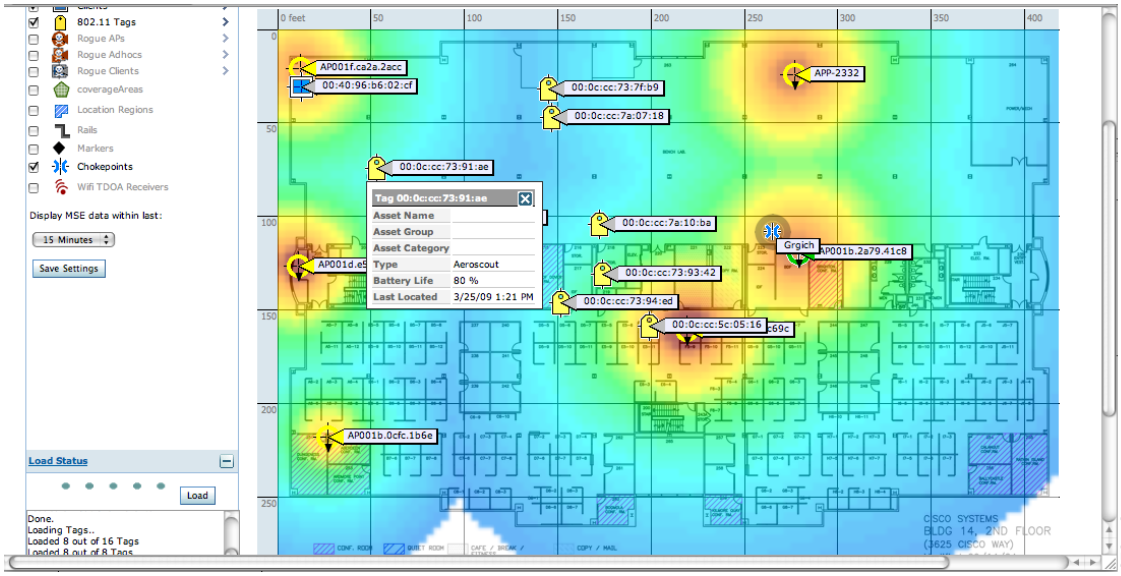
Step 1 In Cisco WCS, choose **Monitor > Maps**.

Step 2 Choose the building and floor on which the mobility services engine and tag are located.

Step 3 Check the **802.11 Tags** check box in the Floor Settings panel (left), if it is not already checked (see Figure 8-13).

Note Do not click **Save Settings** unless you want to save changes made to the floor settings across all maps.

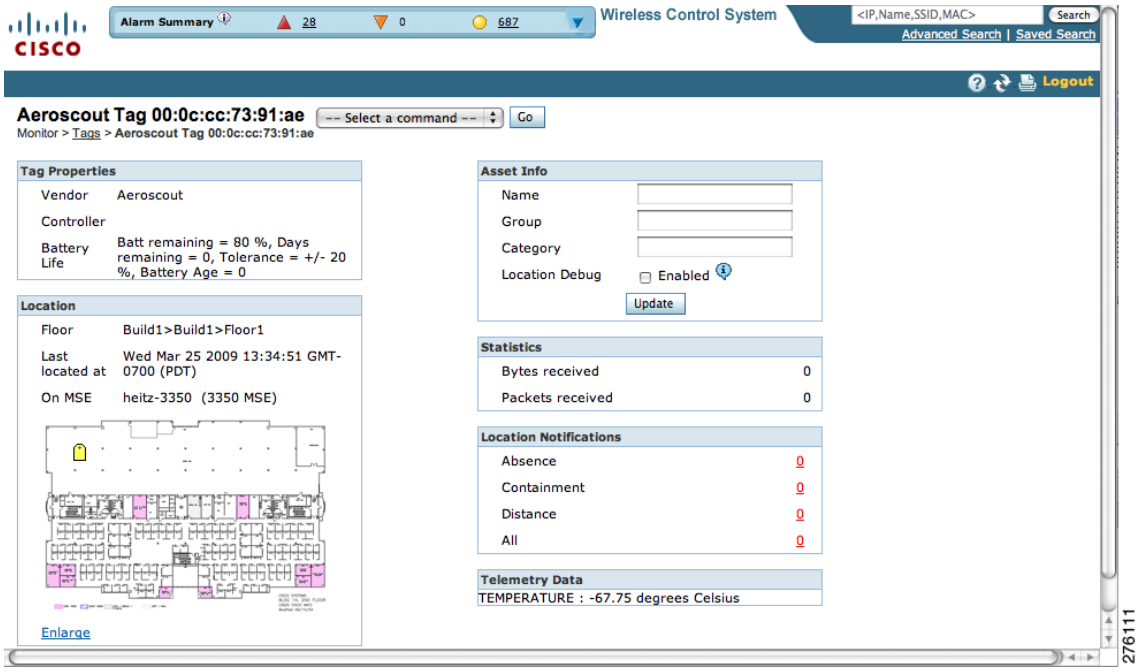
Figure 8-13 Monitor > Maps > Building > Floor > Tag Window



Step 4 Move the cursor over a tag icon (yellow tag) and a summary of its configuration appears in a pop-up panel.

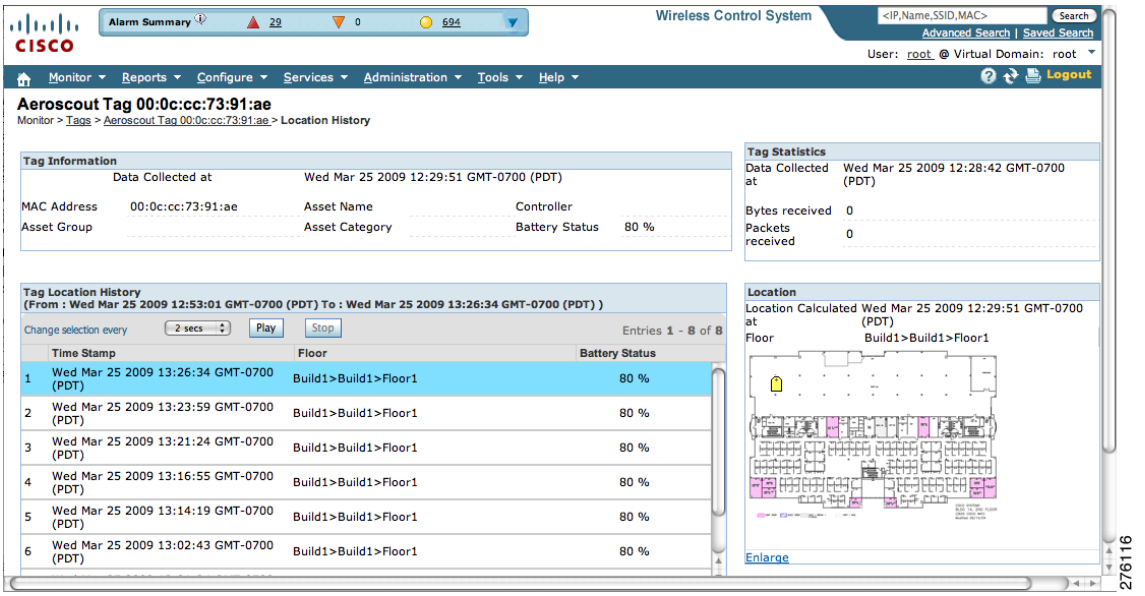
Step 5 Click the tag icon to see tag details (see Figure 8-14).

Figure 8-14 Tag Details Window



Step 6 To see location history for the tag, select **Location History** from the Select a command drop-down menu. Click **Go** (see Figure 8-15).

Figure 8-15 Tag Location History Window



Monitoring Tags Using Search

You can search for tags by asset type (name, category and group), by MAC address, by system (controller or MSE), and by area (floor area and outdoor area).

You can further refine your search using the Advanced search parameters and save the search criteria for future use. Choose **Saved Searches** located in the navigation bar to retrieve saved searches.

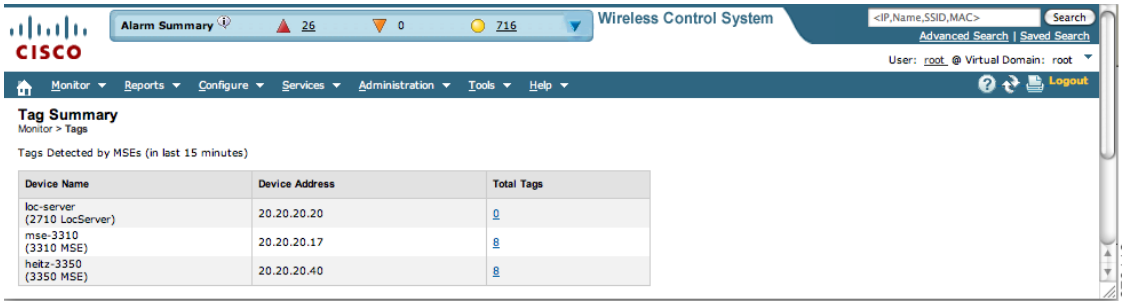
When you click on the MAC address of a tag location in a search results window, the following details appear for the tag:

- Tag vendor
- Controller to which tag is associated
- Telemetry data (CCX v1 compliant tags only)
  - Telemetry data displayed is vendor-specific; however, some commonly reported details are GPS location, battery extended information, pressure, temperature, humidity, motion, status, and emergency code.
- Asset Information (Name, Category, Group)
- Statistics (bytes and packets received)
- Location (Floor, Last Located, MSE, map)
- Location Notification (Absence, Containment, Distance, All)
- Emergency Data (CCX v1 compliant tags only)

To search for tags, follow these steps:

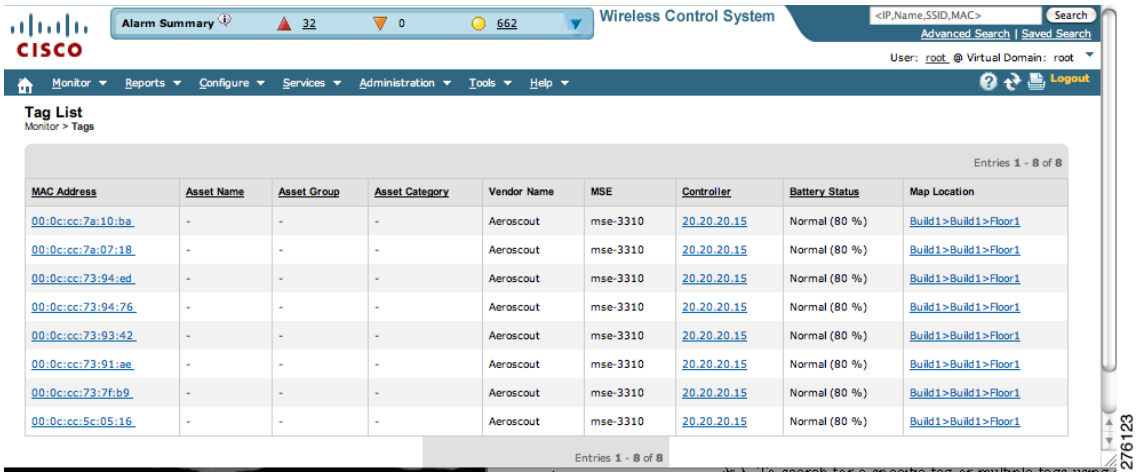
Step 1 Choose **Monitor > Tags**. The Tag Summary window appears (see Figure 8-16).

Figure 8-16 Monitor > Tags Window



a. To view a summary of tags associated with a specific mobility services engine, click the **Total Tags** link (see Figure 8-17).

Figure 8-17 Total Tags Listing by Mobility Services Engine



Note If the listing of mobility service engines or tags is lengthy, you can use Search or Advanced Search to isolate a specific tag.

b. To search for a specific tag, if you know its MAC address, name or VLAN ID (not all search values apply to all tags) use **Search** which is found in the navigation bar.

c. To search for a specific tag or multiple tags using a broader range of search categories such as device (MSE or controller), map location (floor or outdoor area), asset name or category, or tag vendor use **Advanced Search** which is found in the navigation bar (see Figure 8-18).

1. In the Advanced Search panel, select **Tags** as the search category.
2. Select the additional tag search criteria. Refer to Table 8-1 for a list of search criteria and their possible values.
3. Click **Go** when all advanced search parameters are selected. Results are shown in Figure 8-19.

Note If no tags are found based on the selected search criteria, a message appears noting this as well as the reason why the search was unsuccessful and possible actions.

Figure 8-18 Advanced Search Panel for Tags

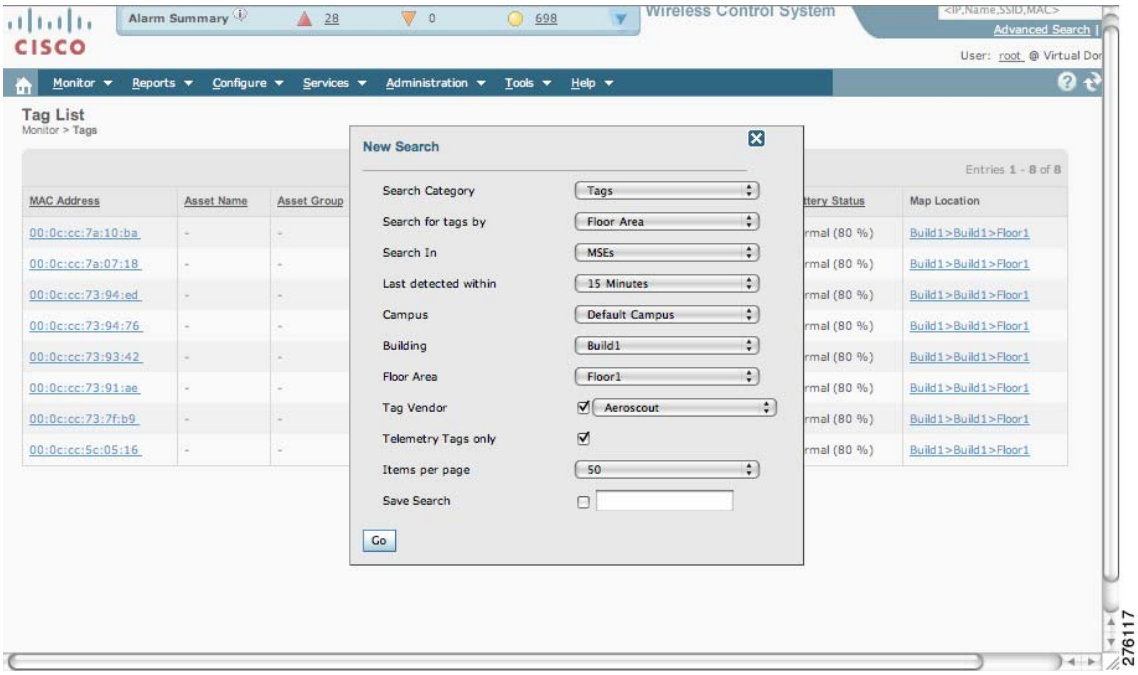
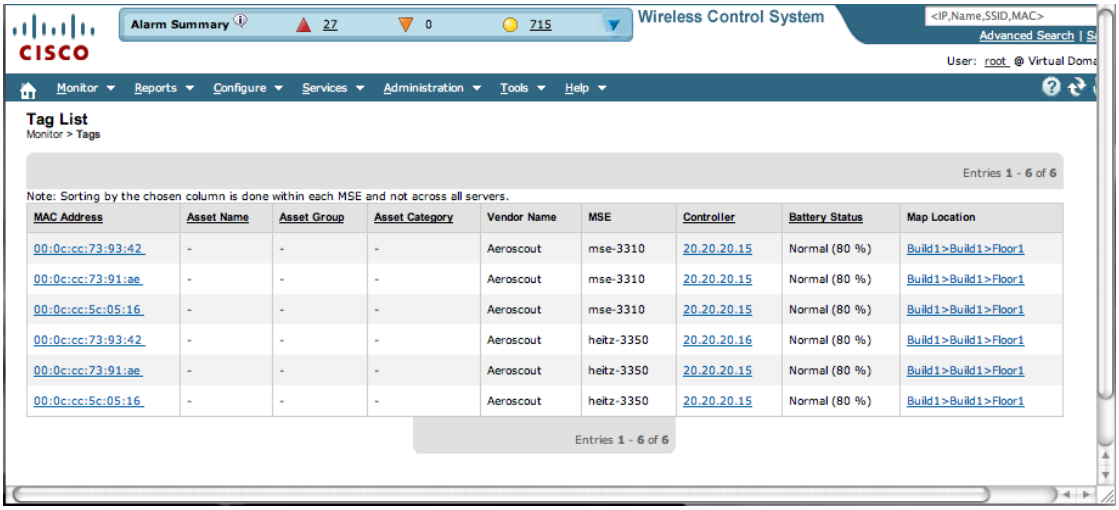


Figure 8-19 Advanced Search Results for Tag



Note If you click the MAC address of any of these tags, a Tag details window appears similar to that in Figure 8-14.

Table 8-1 Tag Search Criteria and Values

Search Criteria	Variable Search Criteria	Possible Values
Search for tags by (Tier 1 search criteria)	—	All Tags; Asset Name, Asset Category or Asset Group; MAC Address; Controller or MSEs; Floor Area or Outdoor Area. **Note** MSE search includes both location servers and mobility services engines.
Search in (Tier 2 search criteria)	—	MSEs or WCS Controllers. **Note** WCS Controller option indicates that the search for controllers is done within WCS. **Note** MSE search includes both location servers and mobility services engines.
Last detected within	—	Options are from 5 minutes to 24 hours.
Variable search criteria. (Tier 3 search criteria) **Note** Possible search criteria determined by the **Search for tabs by** (Tier 1 search) value.	If **Search for tags by** value is: 1. Asset Name, then enter tag asset name. 2. Asset Category, then enter tag asset category. 3. Asset Group, then enter tag asset group. 4. MAC Address, then enter tag MAC address. 5. Controller, then select controller IP address. 6. MSEs, then select an MSE IP address from drop-down menu. 7. Floor Area, then choose campus, building, and floor area. 8. Outdoor Area, then choose campus and outdoor area.	
Telemetry tags only	—	Check box to display telemetry tags. Leaving option unchecked displays all tags. **Note** Option only seen when the Search In option is MSE. **Note** Only those vendor tags that support telemetry appear.
Tag vendor	—	Check box to select tag vendor from drop-down menu. **Note** Option only seen when the Search In option is MSE.
Items per page	—	Select the number of tags to display per search request. Values range from 10 to 500.
Save search	—	Check box to name and save search criteria. Once saved, entry appears under Saved Searches heading (left-panel).

Overlapping Tags

When multiple tags are within close proximity of one another a summary tag is used to represent their location on a WCS map (**Monitor > Maps**). The summary tag is labeled with the number of tags at that location.

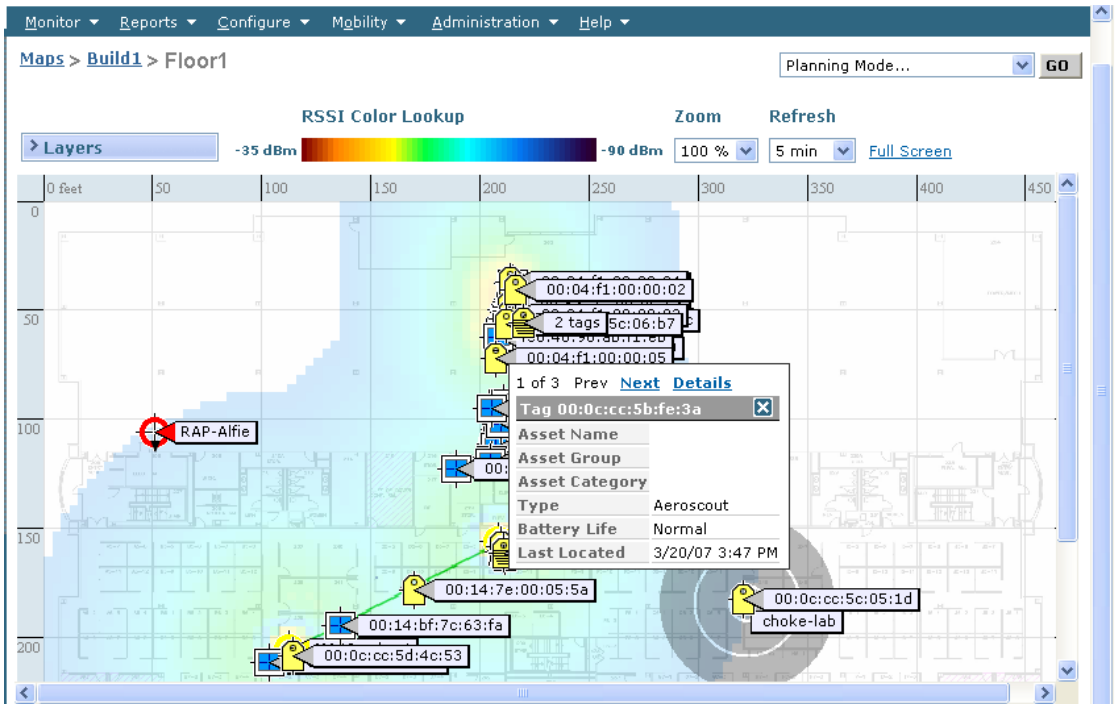
When you move the mouse over the overlapping tag on the map, a panel appears with summary information for the overlapping tags (see Figure 8-20).

Select the **Prev** and **Next** links to move between the individual tag summary panels. To see detailed information on a specific tag, select the **Details** link while viewing the tag's summary information.

Note

- Summary information for tags includes: Tag MAC address, Asset Name, Asset Group, Asset Category, Vendor (Type), Battery Life, and Last Located data (date and time). If the tag is Cisco CX v.1 compliant, telemetry information also appears.
- Detailed information for tags includes this additional information: IP address of associated controller, statistics, location notifications, location history, and whether the location debug feature is enabled.
  - To view location history for a tag, select that option from the Select a command drop-down menu and click **Go**.
  - To return to the details screen from the location history window, select the Tag Detail option and click **Go**.

Figure 8-20 Overlapping Tags Window



Monitoring Chokepoints

A chokepoint must be assigned to a map for its location to be monitored.

Refer to the "Adding Chokepoints to the Cisco WCS" section on page 7-13 of this configuration guide. After adding the TDOA receiver to a map, you must resynchronize the network designs (Services > Synchronize Services) with the mobility services engine for it to appear on the map.

If a chokepoint is not assigned to a map, you are not able to find that chokepoint using Search or Advanced Search.

All chokepoint setup is done 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.

To monitor chokepoints, follow these steps:

Step 1 Choose **Monitor > Chokepoints**. The Chokepoint summary window appears showing all mapped chokepoints.

Step 2 To refine the search criteria when an extensive list appears, search by MAC address or chokepoint name.

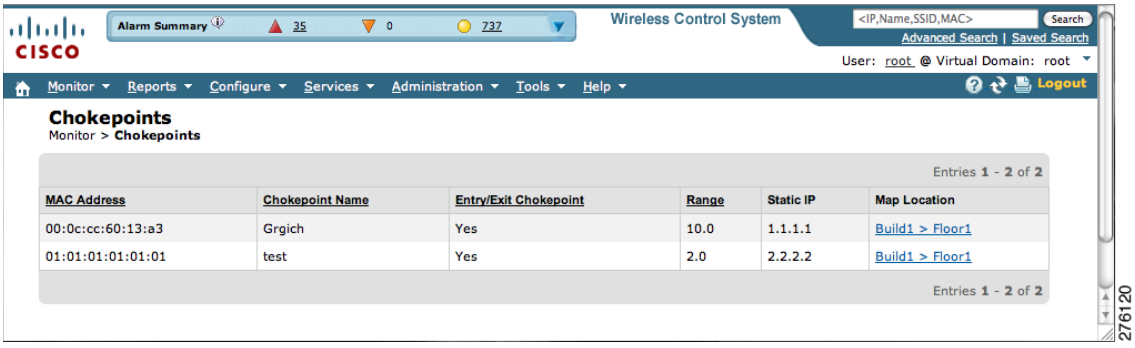
a. To initiate a search for a chokepoint by its MAC address or chokepoint name, enter that value in the Search field of the navigation bar. Click **Search** (see Figure 8-21).

Figure 8-21 Search for Chokepoint by MAC Address

This example show a search by MAC address (see Figure 8-22).

If no match exists, a message appears in the results window.

Figure 8-22 MAC Address Search Results for a Chokepoint Indicating a Match

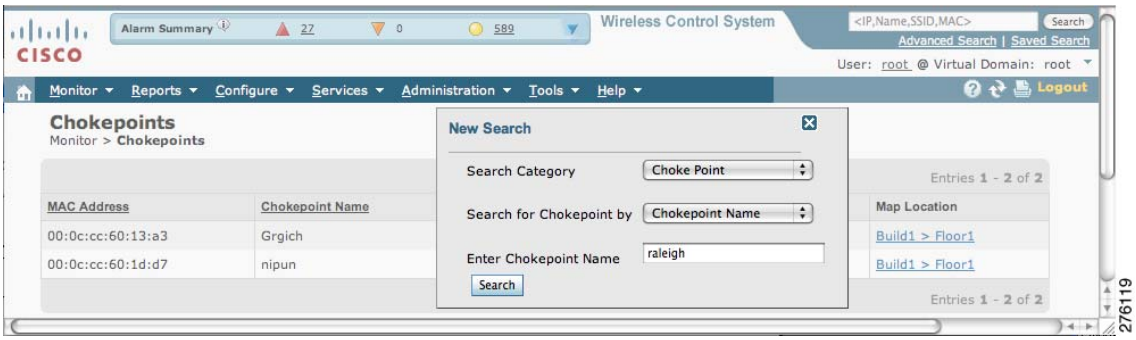


b. To initiate an advanced search for a chokepoint by its MAC address or name, click **Advanced Search** in the navigation bar.

1. Select **Chokepoint** as the search category.
2. Select either **Chokepoint Name** or **MAC Address** from the Search for Chokepoint by drop-down menu.
3. Enter either the chokepoint name or MAC address.
4. Click **Search**.

This example shows an advanced search using the chokepoint name (see Figure 8-23).

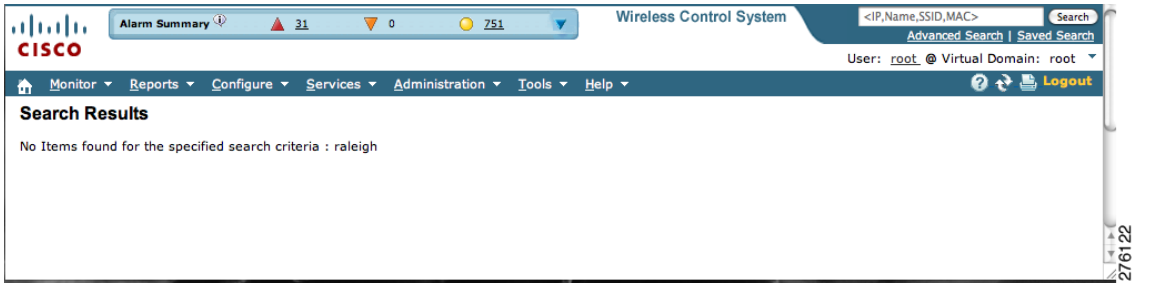
Figure 8-23 Chokepoint Name Advanced Search Panel



If no match exists, a message appears in the window (see Figure 8-24).

Otherwise the search result appears.

Figure 8-24 Chokepoint Advanced Search Results Indicating No Match



Monitoring Wi-Fi TDOA Receivers

A Wi-Fi TDOA receiver must be assigned to a map for its location to be monitored.

Refer to the "Adding Wi-Fi TDOA Receivers to Cisco WCS" section on page 7-19 of this configuration guide. After adding the TDOA receiver to a map, you must resynchronize network designs (Services > Synchronize Services) with the mobility services engine for it to appear on the map.

If a TDOA receiver is not assigned to a map, you cannot find it using Search or Advanced Search.

All TDOA receiver setup is done 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.

To monitor TDOA Receivers, follow these steps:

Step 1 Choose **Monitor > WiFi TDOA Receivers**. The WiFi TDOA Receivers summary window appears showing all mapped TDOA receivers.

Step 2 To refine the search criteria when an extensive list appears, search by MAC address or TDOA receiver name.

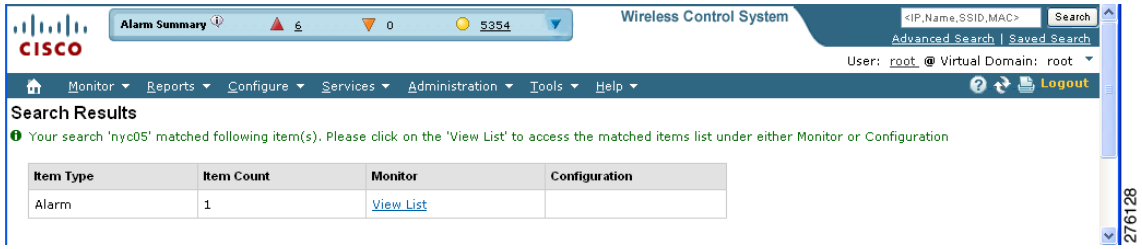
a. To initiate a search for a TDOA receiver by its MAC address or name, enter that value in the Search field of the navigation bar. Click **Search** (see Figure 8-25).

Figure 8-25 Monitor > WiFi TDOA Receivers Search Window

Figure 8-26 shows an example of advanced search using the TDOA Wi-Fi receiver name. Click **View List** to see a full list of Alarms.

If no match exists, a message appears in the results window.

Figure 8-26 Search Results Window



b. To initiate an advanced search for a TDOA receiver by its MAC address or name, click Advanced Search in the navigation bar.

1. Select **WiFi TDOA Receiver** as the search category.
2. Select either **WiFi TDOA Receivers Name** or **MAC Address** from the Search for WiFi TDOA Receiver by drop-down menu.
3. Enter either the TDOA receiver name or MAC address.
4. Click **Search**.

This example shows an advanced search using the MAC address (see Figure 8-27).

Figure 8-27 Advanced Search Panel

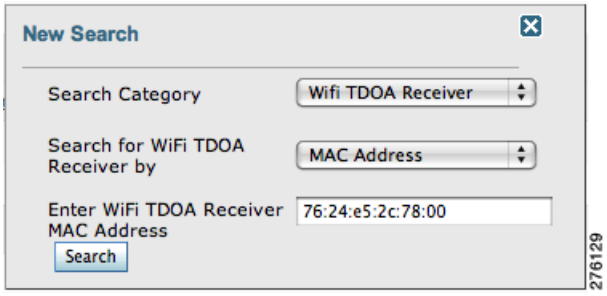
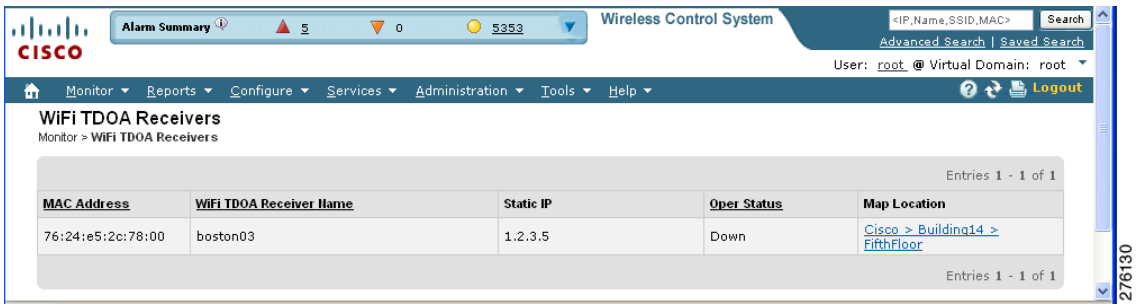


Figure 8-28 shows the search results.

If no match exists, a message appears in the results window.

Figure 8-28 WiFi TDOA Receivers Advanced Search Results Indicating a Match



Monitoring Wired Switches

You can review details on the wired switch (IP address, serial number, software version, and ELIN), its ports, its wired clients (count and status), and its civic information.

Wired switch data is downloaded to the mobility services engine through Cisco WCS when the Ethernet switch and the mobility services engine are synchronized (**Services > Synchronize Services > Switches**). Communications between a location-capable switch and a mobility services engine is over NMSP. Cisco WCS and the mobility services engine communicate over XML.

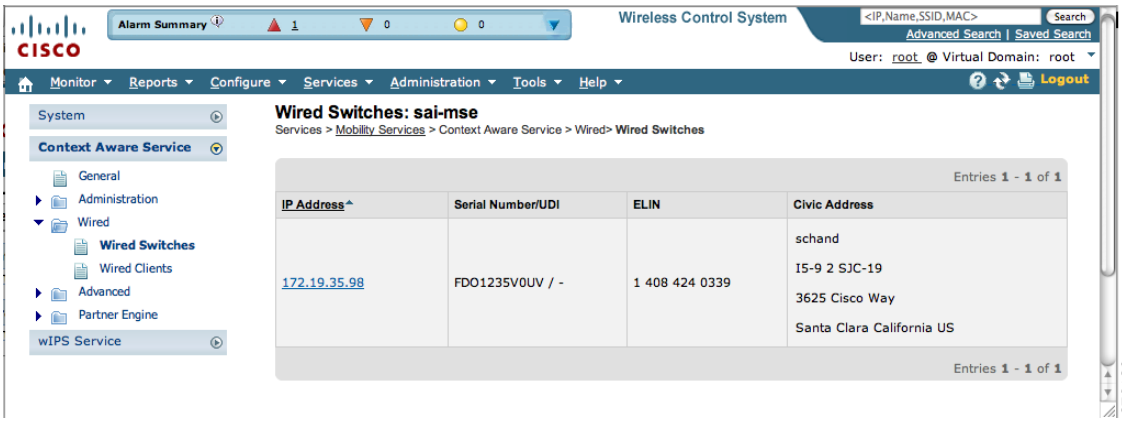
To view details on wired switches, follow these steps:

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

Step 2 At the Mobility Services window, click the device name link of the appropriate wired location switch.

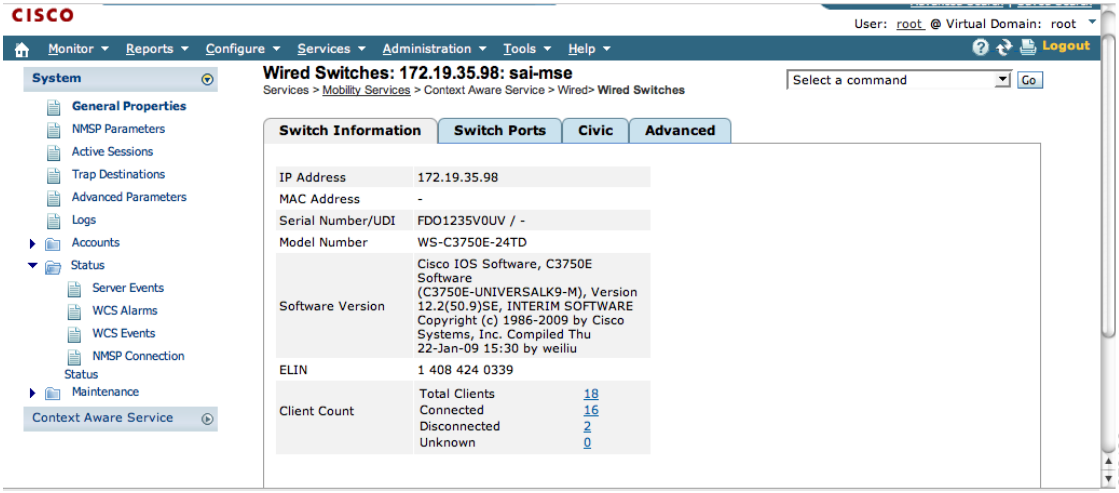
Step 3 Choose **Context Aware Service > Wired > Wired Switches** (see Figure 8-29). A summary of wired switches that are synchronized with the mobility services engine appears.

Figure 8-29 Context Aware Service > Wired Switches Window



Step 4 To see more details on the switch, its ports, its wired clients (count and status), and its civic information click the IP address link (see Figure 8-30).

Figure 8-30 Wired > Wired Switches > IP Address Window



Note You can export civic information from the switch by selecting that option from the Select a command drop-down menu. This option is available at all four sub-panels of the Wired Switches window.

On the Switch Information tab, a total count of wired clients connected to the switch is summarized along with their state (connected, disconnected, and unknown).

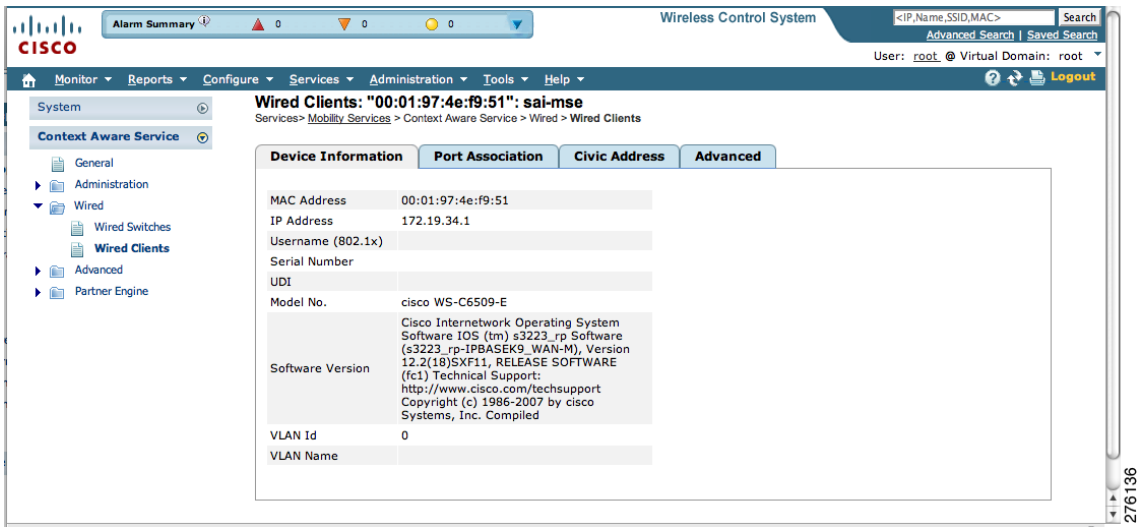
- Connected clients–Clients that are connected to the wired switch.
- Disconnected clients–Clients that are disconnected from the wired switch.
- Unknown clients–Clients are marked as unknown when the NMSP connection to the wired switch is lost.

You can view detailed wired client information by clicking on one of the client count links (total clients, connected, disconnected, and unknown). Refer to the "Monitoring Wired Clients" section on page 8-27 for details.

Step 5 Click the **Switch Ports** tab to see a detailed list of the ports on the switch (see Figure 8-31).

Note You can change the listing order (ascending, descending) of port IP addresses, slot numbers, module number, and port number by clicking on the respective column heading.

Figure 8-31 Wired Switches > Switch Ports Window

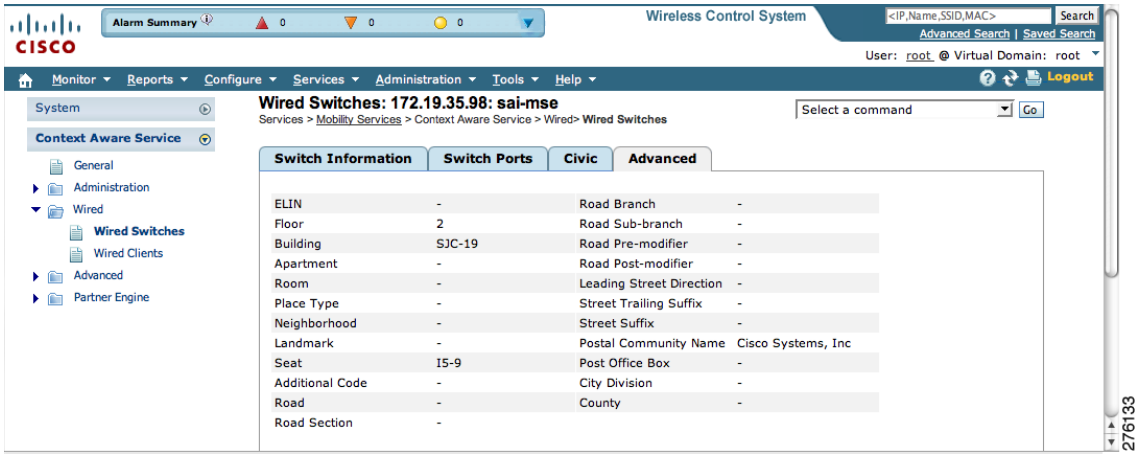


Step 6 Click the **Civic** tab to see a detailed list of the civic information for the wired switch (see Figure 8-32).

Figure 8-32 Wired Switches > Civic Window

Step 7 Click the **Advanced** tab to see a detailed list of the additional civic information for the wired switch (see Figure 8-33).

Figure 8-33 Wired Switches > Advanced Window



Monitoring Wired Clients

You can view details on a wired client (MAC address, IP address, username, serial number, UDI, model no., software version, VLAN ID, and VLAN ID), its port, and its civic information.

Wired client data is downloaded to the mobility services engine through Cisco WCS when the switch and the mobility services engine are synchronized (**Services > Synchronize Services > Switches**).

Communications between a location-capable switch and a mobility service engine is over NMSP. Cisco WCS and the mobility services engine communicate over XML.

You can view wired clients' details on either the wired switches window (**Context Aware Service > Wired > Wired Switches**) or wired clients window (**Context Aware Service > Wired > Wired Clients**).

- If you know the IP address, MAC address, VLAN ID, serial number, or username, you can use the search field on the wired clients window.
- If you want to examine wired clients as they relates to a specific switch, you can view that information on the wired switches window. Refer to the "Monitoring Wired Switches" section on page 8-24.

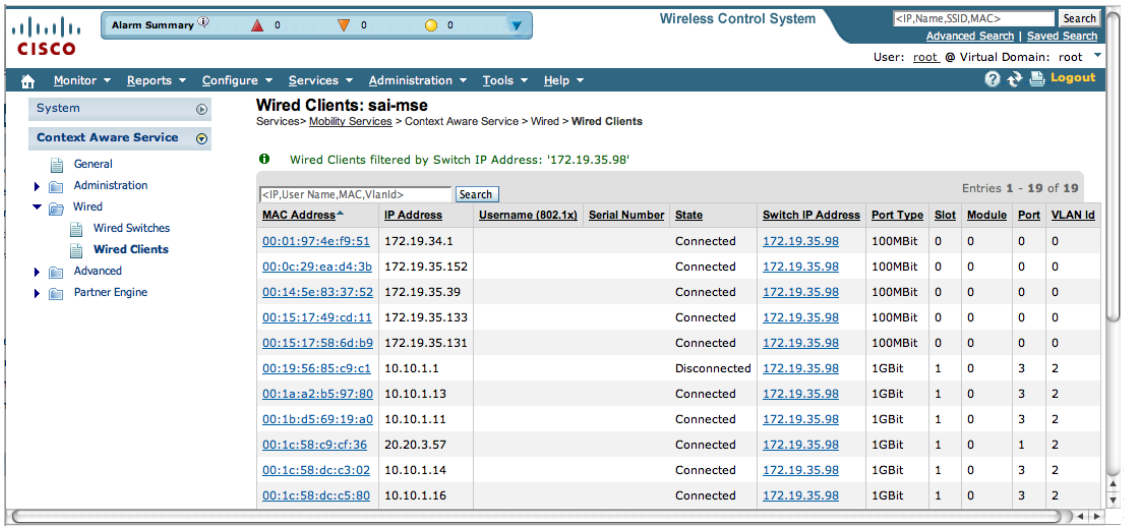
To view details on a wired client, follow these steps:

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

Step 2 Click the device name link of the appropriate wired location switch.

Step 3 Choose **Context Aware Service > Wired > Wired Clients**.

Figure 8-34 Wired > Wired Clients Window

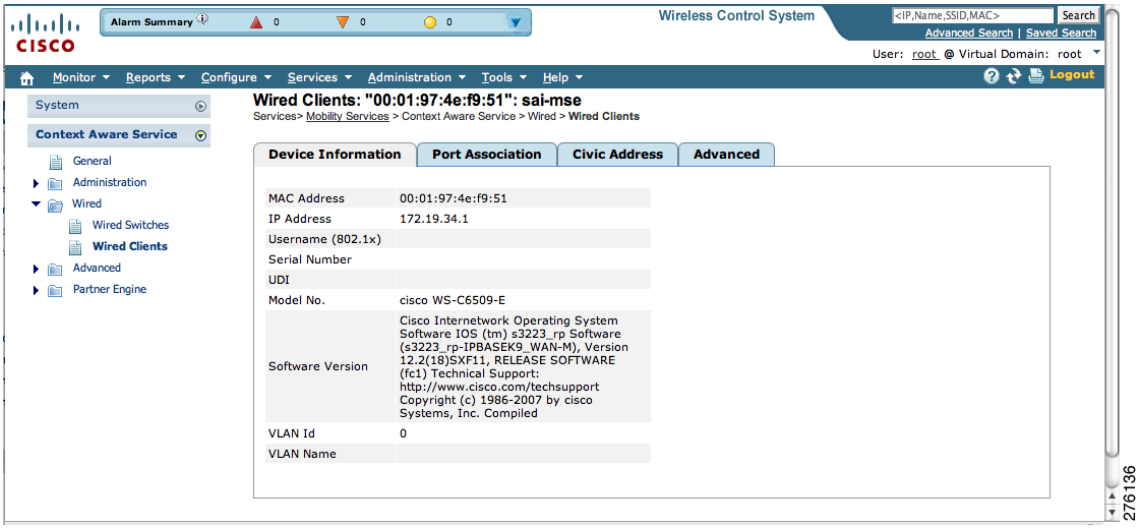


At the Wired Clients summary window, clients are grouped by their switch (see Figure 8-34).

A client's status is noted as connected, disconnected, or unknown. Definitions are summarized below:

- Connected clients–Clients that are active and connected to a wired switch.
- Disconnected clients–Clients that are disconnected from the wired switch.
- Unknown clients–Clients that are marked as unknown when the NMSP connection to the wired switch is lost.
- If you know the wired client's MAC address you can click on that link to reach the client's detail page (see Figure 8-35) or use the search field.
  - You can also search for a wired client by its IP address, username, or VLAN ID.
- If you click on the IP address of the switch, you are forwarded to the switch's detail window. Refer to the "Monitoring Wired Switches" section on page 8-24.

Figure 8-35 Wired Clients > Device Information Window



Step 4 Click the **Port Association** tab to show the physical location of the switch port/slot/module on which the wired client terminates, the client status (connected, disconnected, unknown), and the switch IP address (see Figure 8-36).

Figure 8-36 Wired Clients > Port Association Window

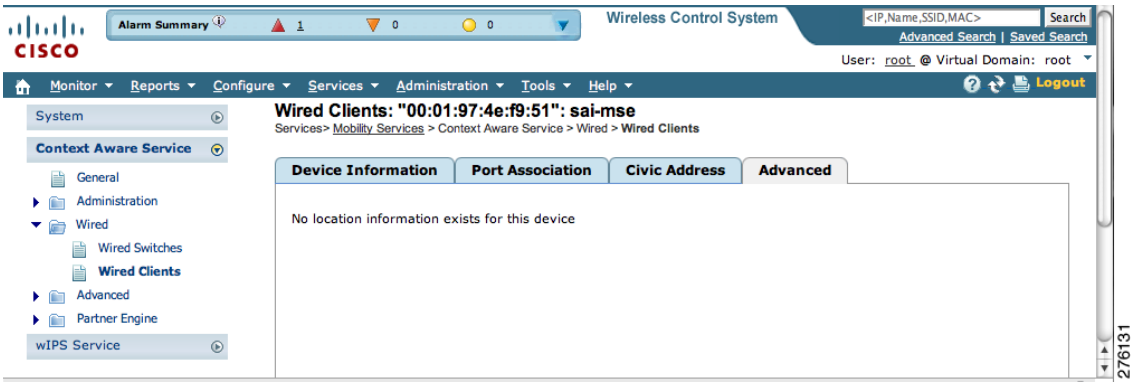
Step 5 Click the **Civic Address** tab to show any civic address information (see Figure 8-37).

Step 6 Click the **Advanced** tab to see any extended physical address details for the wired clients, if any (see Figure 8-38).

Note A client takes on the civic address and advanced location information that is configured for the port on which the client terminates. If no civic and advanced information is defined for the its port (port/slot/module) then no location data is displayed.

Figure 8-37 Wired Clients > Civic Address Window

Figure 8-38 Wired Clients > Advanced Window



CHAPTER 9

Performing Maintenance Operations

This chapter describes how to back up and restore mobility services engine data and how to update the mobility services engine software. It also describes other maintenance operations.

This chapter contains the following sections:

Recovering a Lost Password

To recover a lost or forgotten password for a mobility services engine, follow these steps:

Step 1 When the GRUB screen comes up, press **Esc** to enter the boot menu.

Step 2 Press **e** to edit.

Step 3 Navigate to the line beginning with *kernel* and press **e.**

At the end of the line put a space, followed by the number one (**1**). Press **Enter** to save this change.

Step 4 Press **b** to begin boot.

The boot sequence will commence and at the end the user will be given a shell prompt.

Step 5 The user may change the root password by invoking the **passwd** command.

Step 6 Enter and confirm the new password.

Step 7 Reboot the machine.

Recovering a Lost Root Password

To recover a lost or forgotten root password for a mobility services engine, follow these steps:

Step 1 When the GRUB screen comes up, press **Esc** to enter the boot menu.

Step 2 Press **e** to edit.

Step 3 Navigate to the line beginning with *kernel* and press **e.**

At the end of the line enter a space and the number one (**1**). Press **Enter** to save this change.

Step 4 Press **b** to begin boot sequence.

At the end of the boot sequence, a shell prompt appears.

Note The shell prompt does not appear if you have setup a single user mode password.

Step 5 You can change the root password by entering the **passwd** command.

Step 6 Enter and confirm the new password.

Step 7 Restart the machine.

Backing Up and Restoring Mobility Services Engine Data

This information describes how to back up and restore mobility services engine data. It also describes how to enable automatic backup.

Backing Up Mobility Services Engine Historical Data

Cisco WCS includes functionality for backing up mobility services engine data.

To back up mobility services engine data, follow these steps:

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

Step 2 Click the name of the mobility services engine that you want to back up.

Step 3 Choose **System > Maintenance**.

Step 4 Click **Backup**.

Step 5 Enter the name of the backup.

Step 6 Enter the time in seconds after which the backup times out.

Step 7 Click **Submit** to back up the historical data to the hard drive of the server running Cisco WCS.

Status of the backup can be seen on the screen while the backup is in process. Three items will display on the screen during the backup process: (1) Last Status field provides messages noting the status of the backup; (2) Progress field shows what percentage of the backup is complete; and (3) Started at field shows when the backup began noting date and time.

Note You can run the backup process in the background while working on other mobility services engine operations in other Cisco WCS windows.

Note Backups are stored in the FTP directory you specify during the Cisco WCS installation.

Restoring Mobility Services Engine Historical Data

You can use Cisco WCS to restore backed-up historical data.

To restore mobility services engine data, follow these steps:

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

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

Step 3 Choose **System > Maintenance**.

Step 4 Click **Restore**.

Step 5 Choose the file to restore from the drop-down menu.

Step 6 Enter the time in seconds after which restoration times out.

Step 7 Click **Submit** to start the restoration process.

Step 8 Click **OK** to confirm that you want to restore the data from the Cisco WCS server hard drive.

When restoration is completed, Cisco WCS displays a message to that effect.

Note You should not work on other mobility service engine operations when the restore process is running.

Enabling Automatic Location Data Backup

You can configure Cisco WCS to perform automatic backups of location data on a regular basis.

To enable automatic backup of location data on a mobility services engine, follow these steps:

Step 1 In Cisco WCS, choose **Administration > Background Tasks**.

Step 2 Check the **Mobility Service Backup** check box.

Step 3 Select **Enable Task** from the Select a command drop-down menu. Click **Go**.

The backups are stored in the FTP directory that you specify during the Cisco WCS installation.

Downloading Software to Mobility Services Engines

To download software to a mobility services engine, follow these steps:

Step 1 Verify that you can ping the mobility services engine from the Cisco WCS server or an external FTP server, whichever you are going to use for the application code download.

Step 2 In Cisco WCS, choose **Services > Mobility Services.**

Step 3 Click the name of the mobility services engine to which you want to download software.

Step 4 Choose **System > Maintenance**.

Step 5 Click **Download Software**.

Step 6 To download software, do one of the following:

- To download software listed in the Cisco WCS directory, select **Select from uploaded images to transfer into the Server**. Then, choose a binary image from the drop-down menu.

  Cisco WCS downloads the binary images listed in the drop-down menu into the FTP server directory you have specified during the Cisco WCS installation.
- To use downloaded software available locally or over the network, select the **Browse a new software image to transfer into the Server** and click **Browse**. Locate the file and click **Open**.

Step 7 Enter the time in seconds (between 1 and1800) after which software download times out.

Step 8 Click **Download** to send the software to the /opt/installers directory on the mobility services engine.

Step 9 After the image is transferred to the mobility services engine, log in to the mobility services engine CLI.

Step 10 Run the installer image from the */opt/installers* directory by entering the following command **./.bin** *mse image.* This installs the software.

Step 11 To run the software enter **/etc/init.d/msed start**.

Note To stop the software, enter **/etc/init.d/msed stop**, and to check status enter **/etc/init.d/msed status**.

Manually Downloading Software

If you do not want to automatically update the mobility services engine software using Cisco WCS, follow these steps to upgrade the software manually using a local (console) or remote (SSH) connection.

Step 1 Transfer the new mobility services engine image onto the hard drive.

a. Log in as root, and use the binary setting to send the image from an external FTP server root directory. The release note format is similar to the following and changes with each release: *CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz*.

Note The mobility services engine image is compressed at this point.

Note The default login name for the FTP server is *ftp-user*.

Your entries should look like this example:

```
# cd /opt/installers
# ftp <FTP Server IP address>
Name: <login>
Password: <password>
binary
get CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz
<CTRL-Z>
#
```

b. Verify that the image (*CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz*) is in the mobility services engine /opt/installers directory.

c. To decompress (unzip) the image file enter the following command:

gunzip *CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz*

The decompression yields a *bin* file.

d. Make sure that the *CISCO-MSE-L-K9-x-x-x-x.bin* file has execute permissions for the root user. If not, enter **chmod 755** *CISCO-MSE-L-K9-x-x-x-x.bin*.

Step 2 Manually stop the mobility services engine.

a. Log in as root and enter **/etc/init.d/msed stop**.

Step 3 Enter **/opt/installers/***CISCO-MSE-L-K9-x-x-x-x.bin* to install the new mobility services engine image.

Step 4 Start the new mobility services engine software by entering the following command:

/etc/init.d/msed start

Caution Only complete the next step that uninstalls the script files, if the system instructs you to do so. Removing the files unnecessarily erases your historical data.

Step 5 Enter **/opt/mse/uninstall** to uninstall the mobility services engine's script files.

Configuring NTP Server

You can configure NTP servers to set up the time and date of the mobility services engine.

Note

- You are automatically prompted to enable NTP and enter NTP server IP addresses as part of the automatic installation script for the mobility services engine. For more details on the automatic installation script, refer to the *Cisco 3350 Mobility Services Engine Getting Started Guide* or *Cisco 3310 Mobility Services Engine Getting Started Guide* at the following link:

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

- If you need to add or change an NTP server installation after a mobility services engine install, rerun the automatic installation script. You can configure the NTP server without adjusting the other values by just tabbing through the script.

Note For more information on NTP server configuration, consult the Linux configuration guides.

System Reset, Defragmenting Database and Clearing Configuration

For information on:

- Defragmenting the mobility services engine database
- Rebooting or shutting down the mobility services engine hardware
- Clearing the configuration file

Refer to the "Initiating Advanced Commands" section on page 4-11 of this configuration manual.