Cisco Context-Aware Software Configuration Guide Release 5.1

July 2008

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-19094-01

CONTENTS

Preface

This section describes the objectives, audience, organization, and conventions of the *Cisco Context-Aware Software Configuration Guide*.

Objectives

This publication explains the steps for using Cisco Wireless Control System (WCS) for configuring and managing the Cisco 3300 Series Mobility Services Engine and the Context-Aware Software which resides on the mobility services engine.

Audience

This publication is for the person configuring and managing Context-Aware Software. The user should be familiar with network structures, terms, and concepts.

Conventions

This publication uses the following conventions to convey instructions and information:

- Commands and keywords are in **boldface** type.

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix "Translated Safety Warnings.")**

Waarschuwing **Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel "Translated Safety Warnings" (Vertalingen van veiligheidsvoorschriften) raadplegen.)**

Varoitus **Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)**

Attention **Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).**

Warnung **Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)**

Avvertenza **Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).**

Advarsel **Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)**

Aviso **Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").**

¡Advertencia! **Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")**

Varning! **Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)**

Related Publications

Refer to the *Cisco 3350 Mobility Services Engine Getting Started Guide*, which describes how to install and set up mobility services engines.

This document is available on the Cisco.com website at the following URL:

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Overview

This chapter describes the role of the Cisco 3300 Series Mobility Services Engine, 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 (MSE) 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.

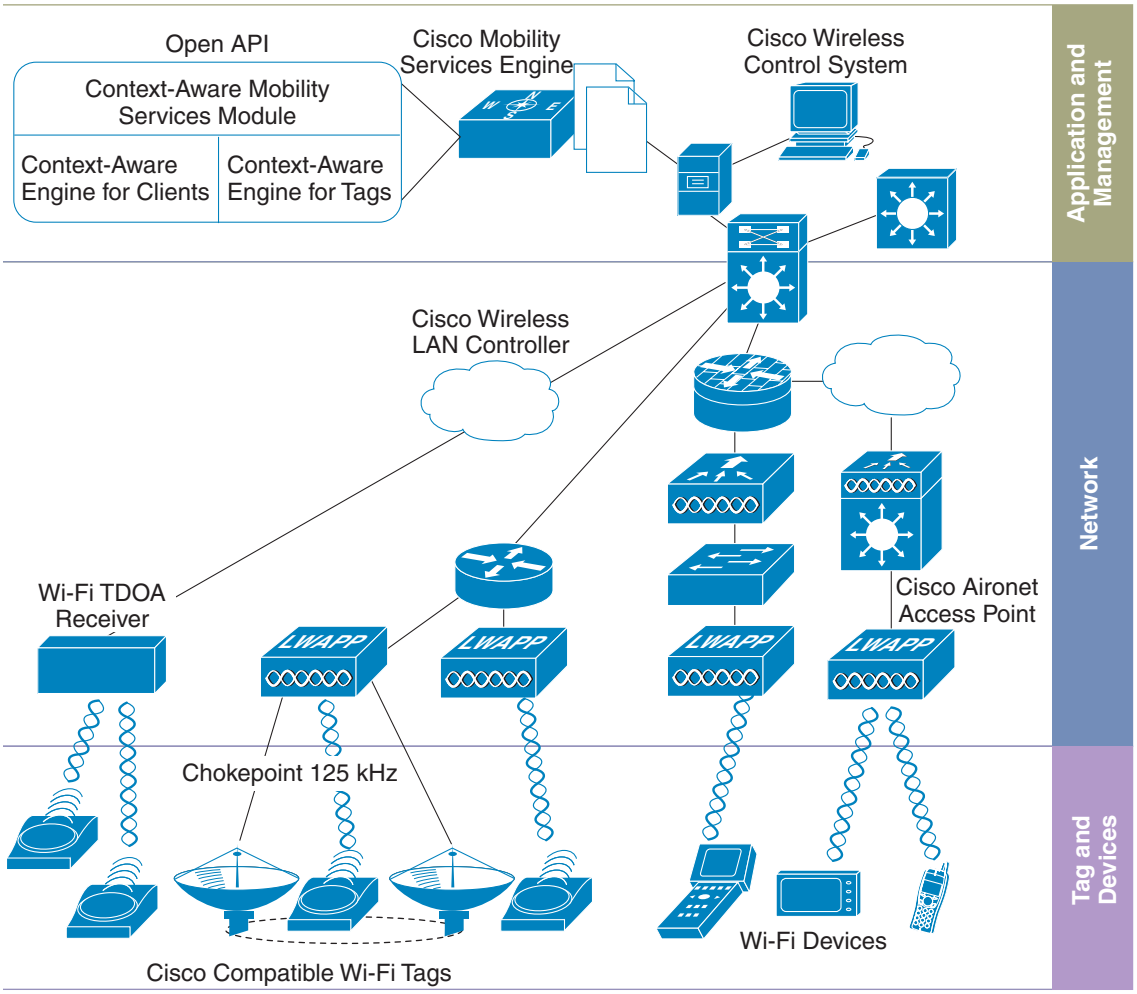
Cisco 3300 Series Mobility Services Engines

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

There are two models of the mobility services engine:

- Cisco 3350 Mobility Services Engine (supported in release 5.1 and later)
- Cisco 3310 Mobility Services Engine (supported in release 5.2 and later)

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; both of these engines can be deployed together or separately depending on the business need.

Note

- You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points.
- Licenses for tags and clients are offered independently. (The clients' license also includes tracking of rogue clients and rogue access points).
- Licenses for tags and clients are offered in various quantities, ranging from 1,000 to 12,000 units.

  For details on tag and client licenses, refer to the *Cisco 3300 Series Mobility Services Engine Release Note, Release 5.1* at:
  http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

Viewing Contextual Information

The collected contextual information can be viewed in GUI format in the Cisco Wireless Control System (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. Details are described in the *Cisco 3350 Mobility Services Engine Getting Started Guide* at the following link:
http://www.cisco.com/en/US/products/ps9742/tsd_products_support_install_and_upgrade.html

After its installation and initial configuration is 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.

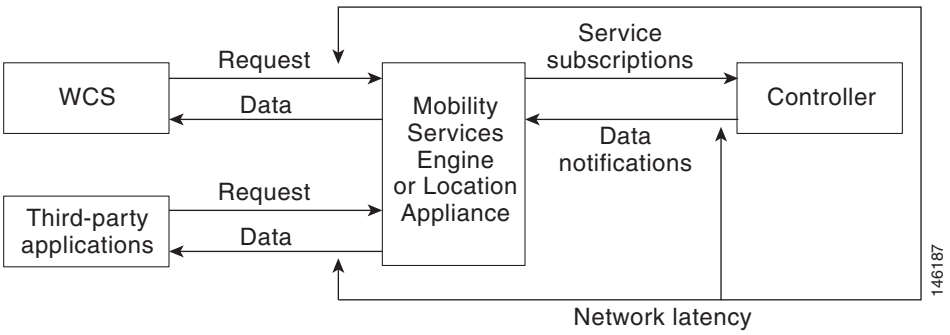
Event Notification

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 will need to periodically request location information from location-based services. (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 to send event notifications (push) 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 Mobility Services Engine

You can use Cisco WCS to add and delete mobility services engine within the network. You are also able to define the service supported on the mobility services engine. Refer to Chapter 2, "Adding and Deleting Systems" 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 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. 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 (clients, tags, rogue clients and rogue access points) is one of the components that is retrieved from access points by the Context-Aware Software (CAS) installed on a mobility services engine. CAS retrieves location as well as additional 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, "Monitoring the System and Services" for specifics.

Maintenance Operations

You can use Cisco WCS to recover a password, 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.

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 Systems

This chapter describes how to add and delete a mobility services engine from Cisco WCS.

This chapter contains the following sections:

Adding a Mobility Services Engine to Cisco WCS

To add a Cisco 3300 Series Mobility Services Engine to Cisco WCS, log into WCS and follow these steps:

Step 1 Verify that you can ping the mobility service engine that you want to add from Cisco WCS.

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

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

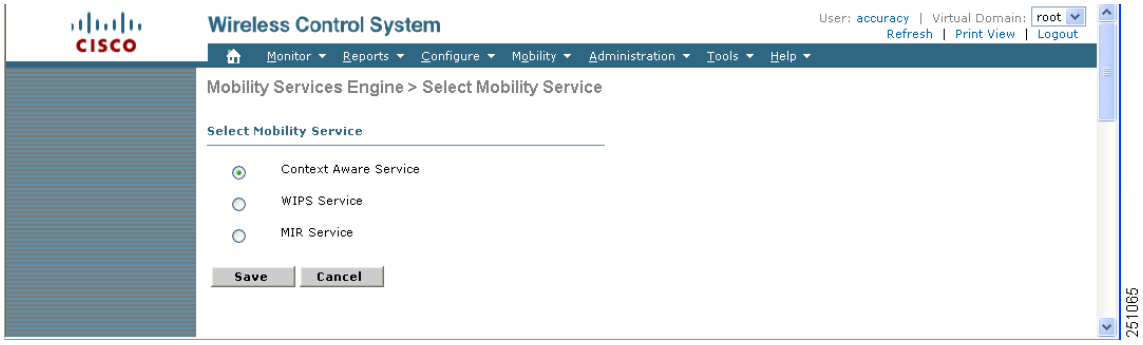
Step 7 In the User Name and Password fields, enter the username and password for the mobility services engine.

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 Click **Next**. The Select Mobility Service window appears (Figure 2-1).

Figure 2-1 Mobility Services Engine > Select Mobility Service



Step 9 To enable one service on the mobility services engine, click the circle next to that service.

Note A mobility services engine can only be configured to support a single service at a time.

Step 10 Click **Save**.

Note After adding a new mobility services engine, you can synchronize network designs (campus, building, and outdoor maps) and event groups on the local mobility services engine with Cisco WCS. You can also choose to synchronize the mobility services engine with a specific controller. You can do this synchronization immediately after adding a new mobility services engine or at a later time. To synchronize the local and Cisco WCS databases, continue to the "Synchronizing Cisco WCS and a Mobility Services Engine" section on page 3-2.

Deleting a Mobility Services Engine from the Cisco WCS

To delete a mobility services engine from the Cisco WCS database, follow these steps:

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

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

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

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:

Keeping Mobility Services Engines Synchronized

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), event groups or controller information (name and IP address) with the mobility services engine.

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.

Synchronizing Cisco WCS and a Mobility Services Engine

To synchronize Cisco WCS network designs, a controller or event groups with the mobility services engine, follow these steps:

Step 1 Click **Mobility > Synchronize Services** to display the Mobility Services > Synchronize WCS and MSE(s) window. A three-tabbed window appears.

Note The Devices column lists the system name of the mobility services engine and the active service on that device. Services are noted in parenthesis next to the device name. Services supported are Context-Aware Software (C), and Wireless Intrusion Protection Service (W).

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

a. To assign a network design to a mobility services engine, click its corresponding **Assign** link.

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.

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

A red asterisk (*) appears next to the Assign link (Figure 3-1). To undo assignments, click **Reset**. To go back to the Synchronize WCS and MSE(s) window without making any changes, click **Cancel**.

b. To associate a mobility services engine with a controller, click the **Assign** link for that mobility services engine.

In the Controllers panel that appears, check the check box next to each controller to which you want the mobility services engine associated. Click **OK** (Figure 3-2).

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

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.

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

c. To assign an event group to a mobility services engine, click its corresponding **Assign** link.

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**.

Figure 3-1 Synchronize > Network Designs

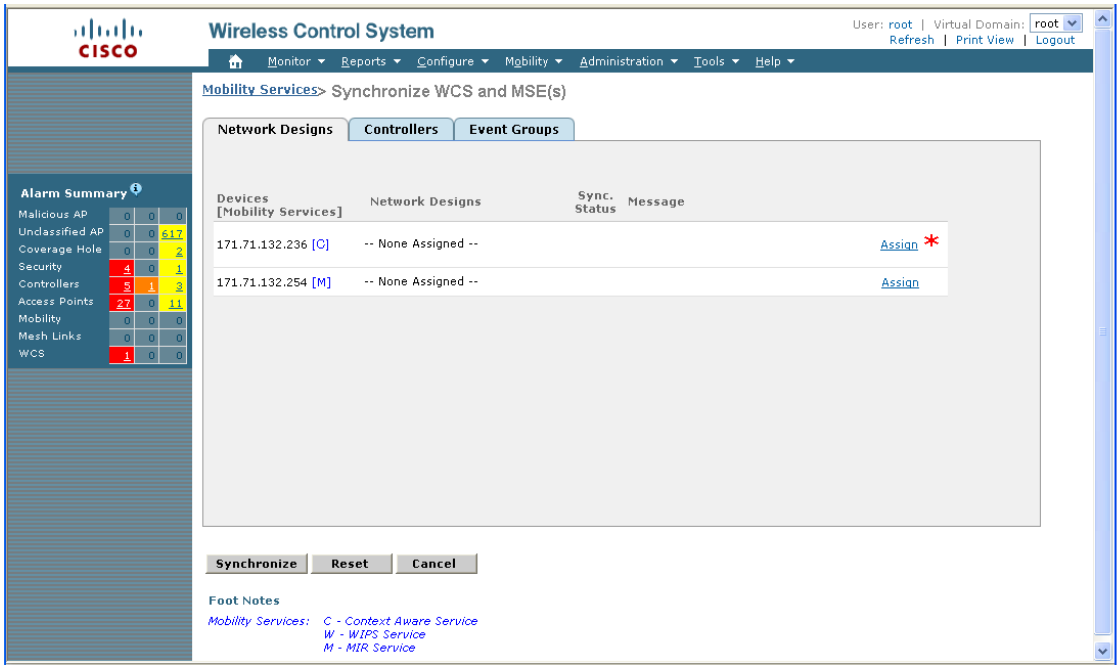


Figure 3-2 Assign > Controllers

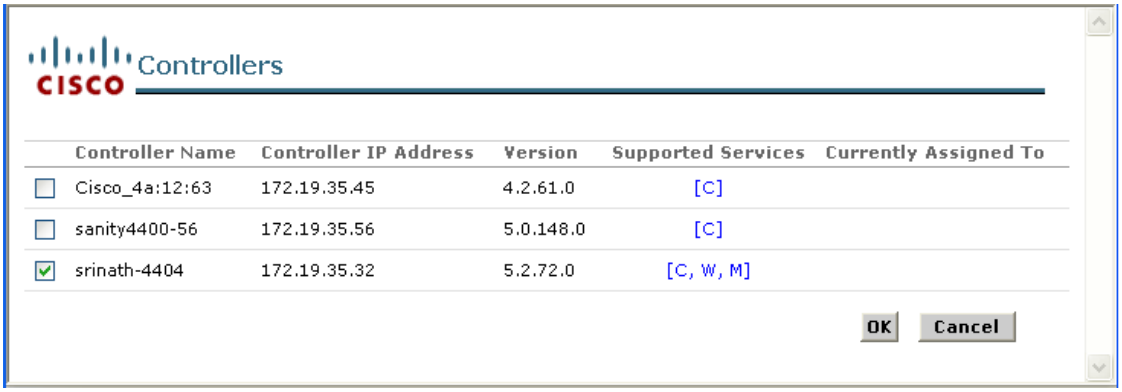
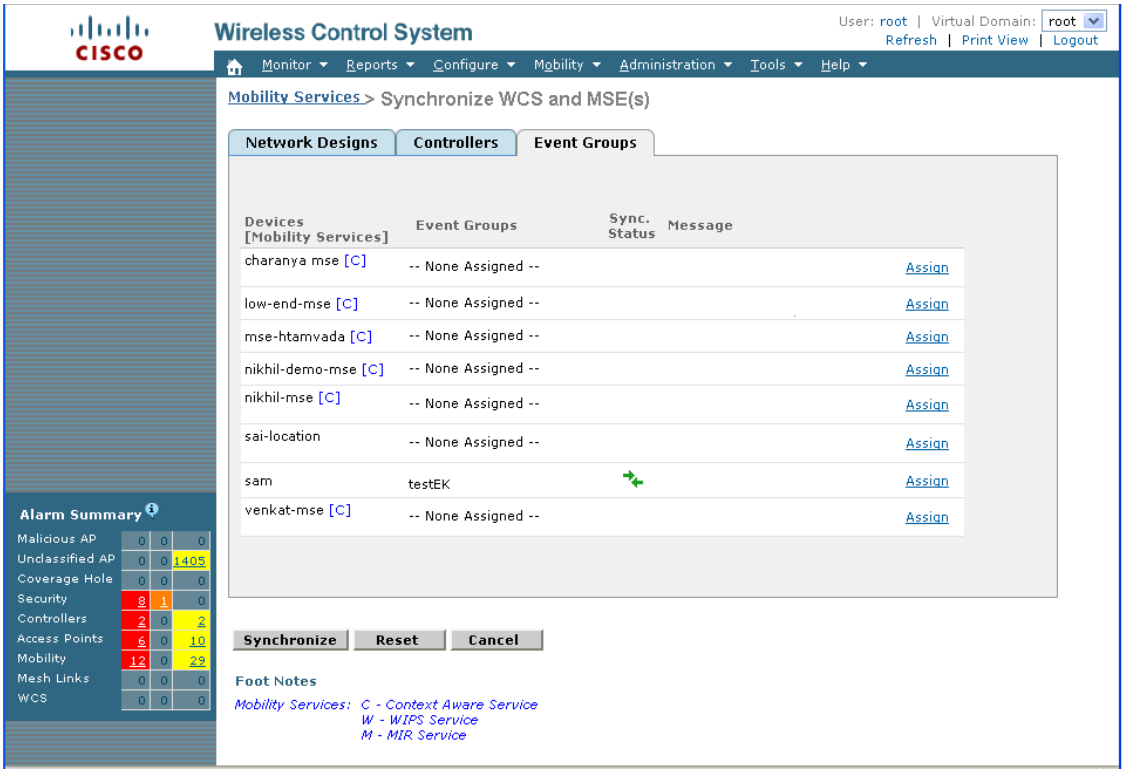


Figure 3-3 Synchronize > Event Groups



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

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 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 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 reoccurs.

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 not already enabled. Click **GO**.

Step 3 Click the **Mobility Service Synchronization** link and 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 3-6.

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 have not yet been 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 that the automatic synchronization is to be performed.

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 Synchronization Information

This section describes how to view synchronization status and history.

Viewing Mobility Services Engine Synchronization Status

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

To view synchronization status, follow these steps:

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

Step 2 Select either the **Network Designs**, **Controllers**, 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 or event group. A gray two-arrow icon with a red circle indicates that its corresponding item is not synchronized with a given server.

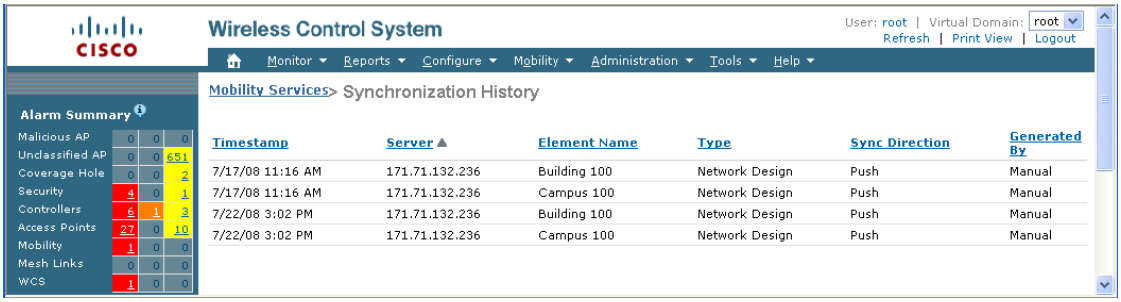
Viewing Synchronization History

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 **Mobility > Synchronization History**. The Synchronization History window appears (.

Figure 3-4 Mobility > Synchronization History



Step 2 Click the column headers to sort the entries. describes the column headings.

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:

Configuring General Properties

You can use Cisco WCS to edit the general properties of a mobility services engine such as contact name, user name, password, HTTP and HTTPS.

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

Step 1 In Cisco WCS, click **Mobility > 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 labeled with General and Performance appears.

Note If the General Properties window does not display by default, select **General Properties** from the **Systems** menu 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.
User Name	Enter the login user name for the Cisco WCS server that manages the mobility services engine.
Password	Enter the login password for the Cisco WCS server that manages the mobility services engine.
Port	8001
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.
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 on a mobility services engine, select the button next to the desired service. Once selected, the service displays as active (UP). **Note** Only one service can operate on a mobility services engine at a time. Operation of multiple services on a mobility services engine is not supported. All inactive services are noted as (DOWN) on the selected (current) system and on the network.

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

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 farewell that exists between the controller and mobility services engine for NMSP to function.

To configure NMSP parameters, follow these steps:

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

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

Step 3 From the **System** menu (left panel), select **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	Defines 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 values 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	Indicates how long the mobility services engine waits before considering the pending request as timed out. The default value is 1 second. Minimum value is one (1). There is no maximum value.

Table 4-2 NMSP Parameters (continued)

Parameter	Description
Retransmit Interval	Interval of time that the mobility services engine waits between notification of a response time out and initiation of a request retransmission. The default setting is 3 seconds. Allowed values range from 1 to 120 seconds.
Maximum Retransmits	Defines 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 zero (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
- Surname 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, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine on which you want to view active sessions.

Step 3 Click **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 back 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, click **Mobility > 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 Click **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** to save settings.

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, click **Mobility > 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 Click **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 (Figure 4-1) 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 4-6 to review current system level settings of the advanced parameters.

- Refer to the "Configuring Advanced Parameters" section on page 4-7 to modify the current system level settings of the advanced parameters.

Note You can also initiate advanced commands such as a system reboot, a system shutdown, clearing the configuration file, and defragment the system database. Refer to the "Initiating Advanced Commands" section on page 4-8 for information on these commands and when they should be used

Viewing Advanced Parameters Settings

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

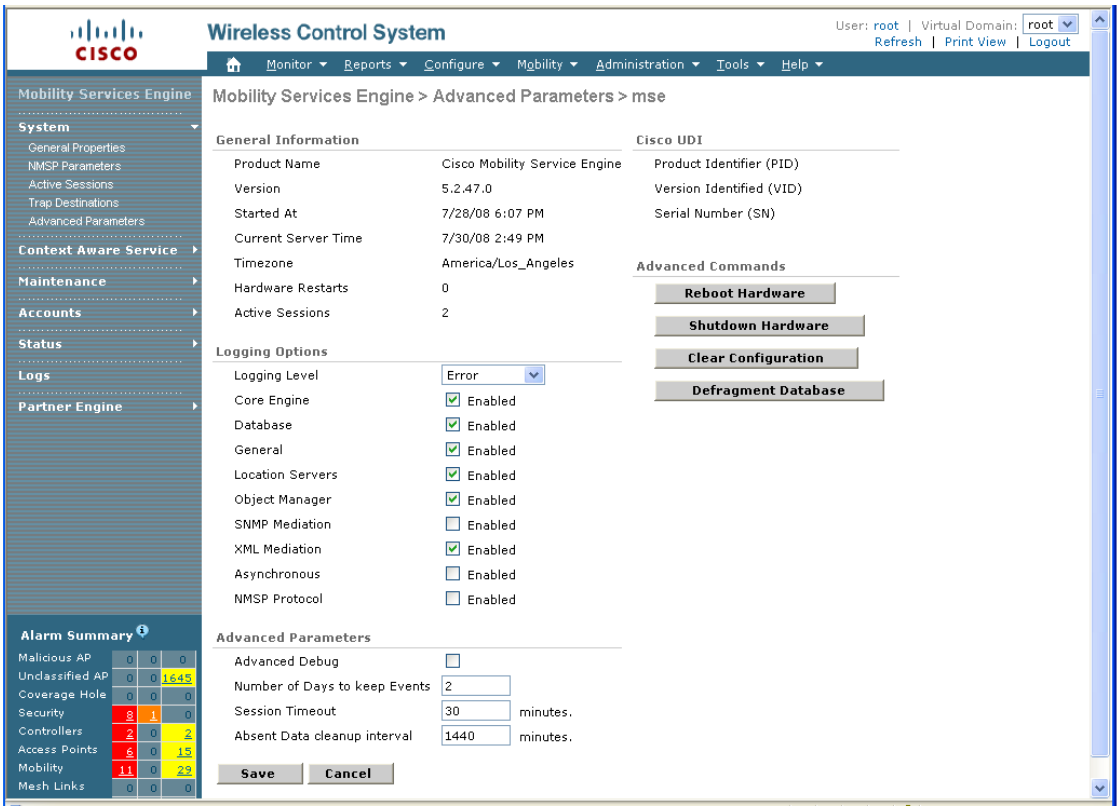
Step 1 In Cisco WCS, click **Mobility > Mobility Services.**

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

Step 3 Click **System** (left panel).

Step 4 Click **Advanced Parameters**.The following window appears (Figure 4-1).

Figure 4-1 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 4-7.
- To set how long events are kept, how long before a session time-outs, interval between data clean ups and enable or disable advanced debug level messages in the logs.

  Refer to the "Configuring Advanced Parameters" section on page 4-7.

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, click **Mobility > Mobility Services**.

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

Step 3 From the System menu (left panel) click **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 from the Logging Level drop-down menu.

There are four logging options: **Off**, **Error**, **Information**, and **Trace**.

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** to apply your changes.

Configuring Advanced Parameters

You can use Cisco WCS to set how long events are kept, how long before a session time-outs, interval between data clean ups and enable or disable advanced debug level messages in the logs.

To configure advanced parameters, follow these steps:

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

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

Step 3 From the System menu (left panel) click **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 configuration or defragment a database by clicking the appropriate button on the Advanced Parameters page.

Reboot or Shutdown a System

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

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

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

Step 3 Click **System** (left panel).

Step 4 Click **Advanced Parameters**.

Step 5 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.

Clear a Configuration File

To clear a configuration file of a mobility services engine, follow these steps:

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

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

Step 3 Click **System** (left panel).

Step 4 Click **Advanced Parameters**.

Step 5 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 clear a configuration file of a mobility services engine, follow these steps:

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

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

Step 3 Click **System** (left panel).

Step 4 Click **Advanced Parameters**.

Step 5 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.

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 Groups

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

User groups allow you to define and 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 access permission, 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, click **Mobility > Mobility Services**.

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

Step 3 Click **Accounts** (left).

Step 4 Click **Groups**.

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

Step 6 Enter the name of the group in the Group Name field.

Step 7 Select a permission level from the Permission drop-down menu.

There are three permissions levels to select from:

- Read Access
- Write Access
- Full Access (required for Cisco WCS to access mobility services engines)

Step 8 Click **Save** to add the new group to the mobility services engine.

Deleting User Groups

To delete user groups from a mobility services engine, follow these steps:

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

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

Step 3 Click **Accounts** (left).

Step 4 Click **Groups**.

Step 5 Check the check boxes of the groups that you want to delete.

Step 6 Select **Delete Group** from the Select a command drop-down menu and click **GO**.

Step 7 Click **OK** to confirm that you want to delete the selected groups.

Changing User Group Permissions

To change user group permissions, follow these steps:

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

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

Step 3 Click **Accounts** (left).

Step 4 Click **Groups**.

Step 5 Click the name of the group you want to edit.

Step 6 Select a permission level from the Permission drop-down menu.

Step 7 Click **Save** to apply your change.

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

Managing Users

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

Adding Users

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

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

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

Step 3 Click **Accounts** (left).

Step 4 Click **Users**.

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

Step 6 Enter the username in the Username field.

Step 7 Enter a password in the Password field.

Step 8 Enter the name of the group to which the user belongs in the Group Name field.

Step 9 Select a permission level from the Permission drop-down menu.

There are three permission levels to select from: Read Access, Write Access, and Full Access (required for Cisco WCS to access a mobility services engine).

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 access, that user will not be able to configure mobility services engine settings.

Step 10 Click **Save** to add the new user to the mobility services engine.

Deleting Users

To delete a user from a mobility services engine, follow these steps:

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

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

Step 3 Click **Accounts** (left).

Step 4 Click **Users**.

Step 5 Check the check boxes of the users that you want to delete.

Step 6 Select **Delete User** from the Select a command drop-down menu and click **GO**.

Step 7 Click **OK** to confirm that you want to delete the selected users.

Changing User Properties

To change user properties, follow these steps:

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

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

Step 3 Click **Accounts** (left).

Step 4 Click **Users**.

Step 5 Click the name of the group that you want to edit.

Step 6 Make the required changes to the Password, Group Name, and Permission fields.

Step 7 Click **Save** to apply your change.

CHAPTER 6

Configuring Event Notifications

Event notification enables you to define conditions that cause the mobility service engine to send notifications to the listeners that you have specified in Cisco WCS. 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 definitions.

Adding Event Groups

To add an event group, follow these steps:

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

Step 2 Click **Settings** (left- panel).

Step 3 From the Select a command drop-down menu, select **Add Event Group**, and 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, click **Mobility > Notifications**.

Step 2 Select the event group to delete by checking its corresponding check box.

Step 3 From the Select a command drop-down menu, select **Delete Event Group(s)**, and click **GO**.

Step 4 In the panel that appears, click **OK** to confirm deletion.

Step 5 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 definitions on a per-group basis. An event definition must belong to a particular group.

To add an event definition, follow these steps:

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

Step 2 Click **Settings** (left panel).

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

Step 4 From the Select a command drop-down menu, select **Add Event Definition** and click **GO**.

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

For example, to keep track of heart monitors in a hospital, you can add three rules to generate an event notification if the heart monitor is missing for two hours, if the heart monitor moves out of the second floor, or if the heart monitor enters a specific coverage area within a floor.

To add a condition, follow these steps:

a. Click **Add** to add a condition that triggers this event.

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

1. Choose a condition type from the Condition Type drop-down menu.
2. In the Trigger If field, follow these steps:

If you chose **Missing** from the Condition Type drop-down menu, enter the number of minutes after which a missing asset event is generated. For example, if you enter 10 in this field, the mobility service engine generates a missing asset event 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** to select the area to monitor for assets going into it or out of it. 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 that will trigger an event notification if the monitored asset moves beyond the specified distance from a designated marker, then 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 73 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 an event. 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 an event. 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, or Rogue Clients) for which an event will be generated if the trigger condition is met.

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

d. From the Match By drop-down menu, choose the matching criteria (Asset Name, Asset Group, Asset Category or MAC Address), the operator (**Equals** or **Like**) from the drop-down menu, and enter the relevant text for the selected Match By element.

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

- If you choose **MAC Address** from the Match By drop-down menu, choose **Equals** from the Operator drop-down menu, and enter **12:12:12:12:12:12**, 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 Match By drop-down menu, choose **Like** from the Operator drop-down menu, and enter **12:12**, 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.

You are returned to the Add/Edit Condition panel and the location path (*Campus* > *Building* > *Floor*) for the chokepoint auto-populates the 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 configure the transport settings:

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

b. Click **Add New**.

c. Enter the IP address of the system that will receive event notifications, and click **OK**.

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 to send event notifications to, 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** to specify the message format.

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

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

- **SOAP**—Specifies Simple Object Access Protocol, a simple XML protocol, as the transport type for sending event notifications. Use SOAP to send notifications over HTTP/HTTPS and to be processed by web services on the destination.

  If you choose **SOAP**, specify whether to send notifications over HTTPS by checking its corresponding check box. If you don't, HTTP is used. Also, enter the destination port number in the Port Number field.

- **Mail**—Use this option to send notifications via 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 **Enabled** check box for Admin Status to enable event generation (disabled by default).

b. Set the event 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. To select how often the event definitons are sent:

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 each day you want the event notification sent.

e. Select the time for starting the event notification by selecting the appropriate hour, minute and AM/PM options from the Apply From heading.

f. Select the time for ending the event notification by selecting the appropriate hour, minute and AM/PM options from the Apply Until heading.

g. Click **Save**.

Step 8 Verify that the new event definition is listed for the event group (Mobility > Notifications > Settings > *Event 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 **Mobility > Notifications**.

Step 2 Click **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)**, and click **GO**.

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

Testing Event Definitions

To verify that the mobility service engine is sending event definitions over the transport protocol you have specified in the event definition, use Cisco WCS to test the event notifications. The mobility service engine sends three fictitious event notifications (absence, containment, and distance) to the destinations 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 definitions, follow these steps:

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

Step 2 Click **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)**, and click **GO**.

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

Step 7 Check to make sure 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 absence events when the monitored assets go 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 containment events when an asset is moved inside or outside 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 movement events 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 client stations, asset tags, rogue clients and rogue access points move from their previous 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, tampered with, goes inactive or reports an unknown state. This information is only reported and displayed for Cisco CX v.1 compliant tags.
- Chokepoint Notifications—The mobility services engine generates an event when a tag is seen (stimulated) by a chokepoint. This information is only reported and displayed 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 **Mobility > Notifications**.

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

Note Emergency and chokepoint notifications are only reported and displayed 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.

Notifications Cleared

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

- **Missing (Absence)**—Elements reappear.
- **In/Out Area (Containment)**—Elements move back in or out of the containment area.
- **Distance**—Elements move back within the specified distance from a marker.

- **Location Changes**—Clear state is not applicable 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.

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 28 May 2006"
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,"
entityType="Tag" entityID="00:0c:cc:5b:fa:44"/>
```

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

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

Distance Condition

Message format for elements in 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 in 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 23 May 2006" 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

Message format for element location.

An example:

```
<ChokepointTrackEvent
lastSeen="11:10:08 PST 18 Jan 2007"
chokepointMac="00:0c:cc:60:13:a3"
chokepointName= "chokeA3"
trackDefn="choke"
entityType="Tag"
entityID="00:12:b8:00:20:4f"/>
```

Message format for the clear state.

An example:

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

Emergency Condition

Message format for element location.

An example:

```
<ChokepointTrackEvent
lastSeen=”11:36:46 PST Jan 18 2007"
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, at any time.

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 “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 13 Oct 2005.
  ```

- 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 23 May 2006
  ```

- 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 Software (CAS) installed on a mobility services engine retrieves location 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 Software was previously referred to as Cisco location-based services.

This chapter contains the following sections:

Note

- You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points. Licenses for tags and clients are offered independently. (The clients' license also includes tracking of rogue clients and rogue access points).
- For details on tag and client licenses, refer to the *Cisco 3350 Mobility Services Engine Release Note* at: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

Planning for Data, Voice, and Location Deployment

You can calculate the recommended number and location of access points based on whether data and/or voice traffic and/or location will be active.

To calculate recommended number and placement of access points for a given deployment, follow these steps:

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

Step 2 **Click** on the appropriate map name link in the list that displays.

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

Note If you select a building map, you then need to select a floor map from the window that appears.

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

A map appears with planning mode options at the top of the page.

Step 4 Click **Add APs** to open a window to enter data necessary to calculate the recommended number of access points.

Step 5 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 **Ctrl** key. Move the mouse as necessary to outline the targeted location.

Step 6 **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 given the services requested appears.

Note Each service option is inclusive 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 optimum 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 7 Click **Apply** (left panel, bottom) to generate a map based on the recommended number of access point and their proposed placement in the selected area.

Note Check the Location services option to ensure that the recommended access points will 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 the floor layout, you can create a calibration model that is applied to the floor and better represents the attenuation characteristics of that floor. In environments in which many floors share common attenuation characteristics (such as in a library), one calibration model can be created and then applied 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–Calibration points are selected and their coverage area is calculated one location at a time.
- Linear point collection–A series of linear paths are selected and then calculated as you traverse the path. This approach is generally faster than the data point collection. You can also employ data point collection to augment data collection for locations 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 at: http://support.aeroscout.com.

Note A client device that supports both 802.11a/n and 802.11b/g/n radios is recommended 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 manual models, follow these steps:

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

Step 2 Choose Create **New Model** from the Select a command drop-down menu in the upper right. Click **GO**.

Step 3 Assign a name to the model and click **OK**.

The new model appears along with the other RF calibration models, but its status is listed as *Not Yet Calibrated*.

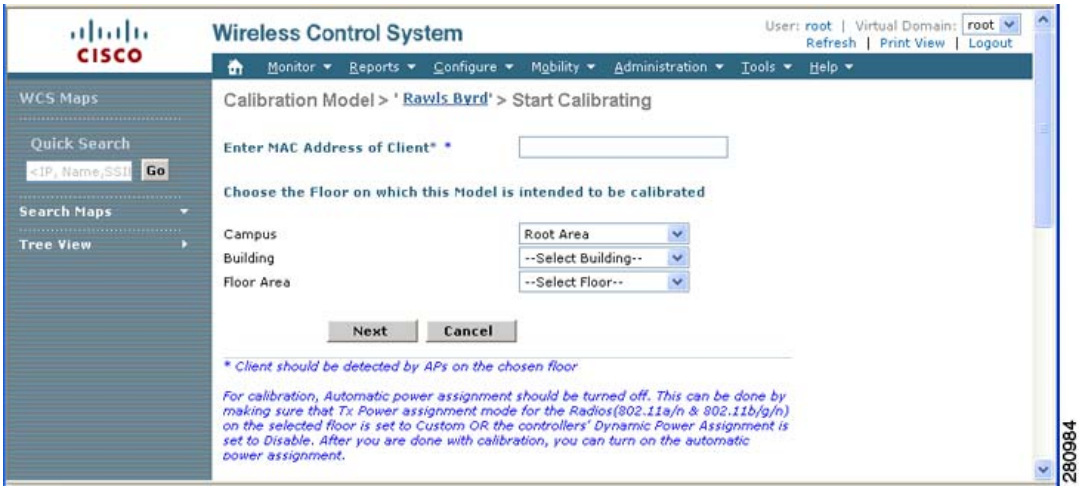
Step 4 To start the calibration process, click on the **model name** link. A new window appears which indicates the details of the new model.

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

Step 6 If this process is being performed 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 being used 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 7-1). Click **Next**.

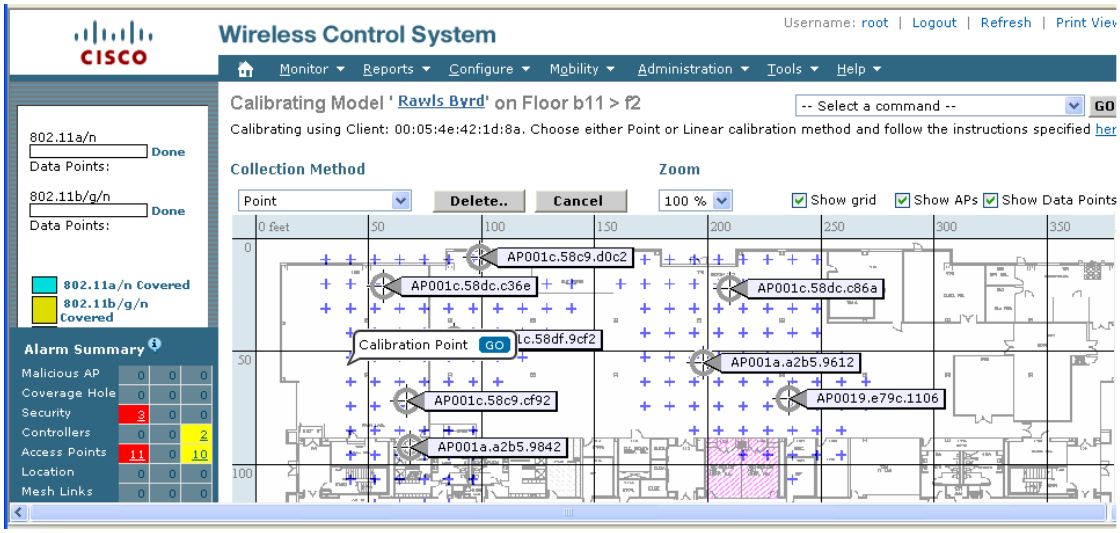
Figure 7-1 Starting to Calibrate



Step 8 When the chosen floor map and access point locations display, a grid of plus marks (+) indicates the locations where data collection for calibration is performed.

Using these locations as guidelines, you can perform either a point or linear collection of data by appropriate placement of either the Calibration Point pop-up (point) or the Start and Finish pop-ups (linear) that display on the map when the respective options are displayed. Figure 7-2 shows the starting window for a point calibration.

Figure 7-2 Positioning Calibration Points



a. If you want to do a point collection of data for the calibration, do the following:

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 displays 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 heard 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. Information on color-coding is provided in legend on the left-hand side of the window. 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 for locations 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.

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.’ b/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. If you want to do a linear collection of data for the calibration, do the following:

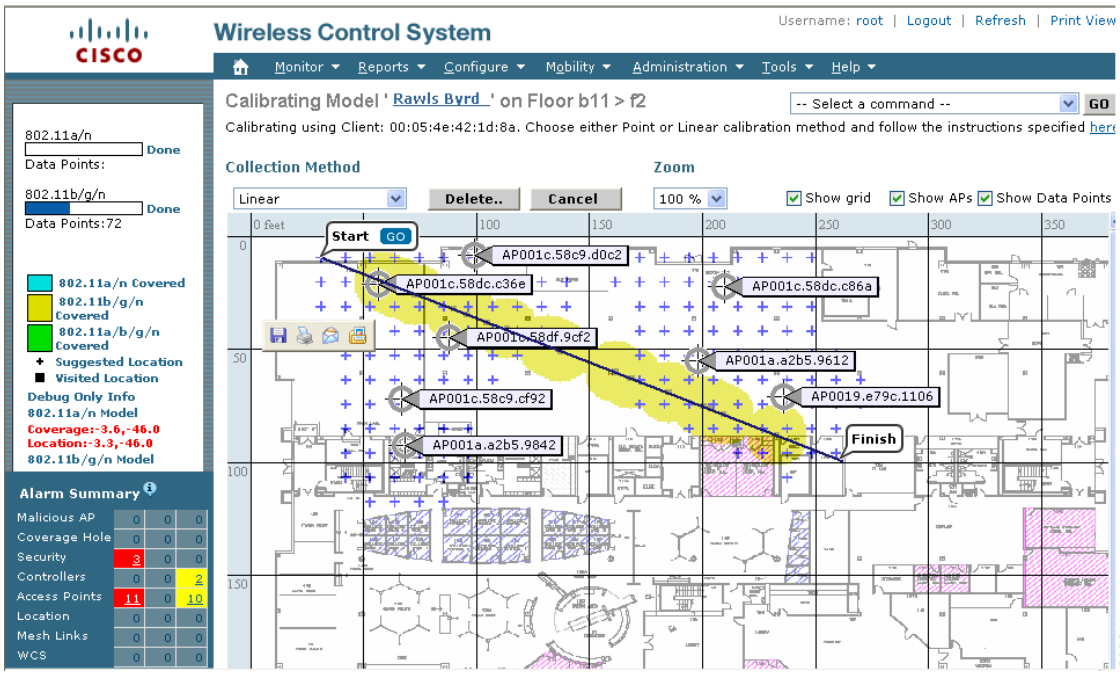
1. Select Linear from the Collection Method drop-down menu and check the Show Data points check box if not already checked. A line appears on the map with both Start and Finish pop-ups.
2. Position the tip of the Start pop-up at the starting data point.
3. Position the Finish pop-up at the ending data 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 to show that data collection is in process.

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

5. Press the space bar (or **Done** on the data collection panel) when you reach the end point. The collection panel displays the number of samples taken before it closes to reveal the map. The map displays all the coverage areas where data was collected. (see Figure 7-3).

Note To delete data points for locations 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 7-3 Linear Data Collection



Note The coverage area is color-coded and corresponds with the specific wireless LAN standard used to collect that data. Information on color-coding is provided in legend on the left-hand side of the window.

6. Repeat steps b2 to b5 until the status bar for the respective spectrum is filled in (done).

Note You can augment linear collection with data point collection to address missed coverage areas.

Step 9 Click on the name of the calibration model at the top of the window to return to the main screen for that model to calibrate the data points.

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

Step 11 Click the Inspect Location Quality link when calibration completes. A map displays 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 as well). Navigate to **Monitor > Maps** and find the specific floor to which the model is applied. 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 location determination performed on that floor is done 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 the 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. The location readiness calculation is based on the number and placement of access points.

You can also check the location quality and the ability of a given location to meet the location specification (10 m, 90%) based on data points gathered during a physical inspection and calibration.

Inspecting Location Readiness Using Access Point Data

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

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

Step 2 Click on the appropriate floor location link from the list that displays.

A map displays 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 under the Layer menu (top-left).

Note If clients, tags and access point are not displayed verify that their respective check boxes are checked in the Layers menu. Additionally, licenses for both clients and tags must be purchased for each of them to be tracked.

Step 3 Select **Inspect Location Readiness** from the Select a command menu found 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, click **Monitor > Maps.**

Step 2 Choose **RF Calibration Mode**l from the Select a command menu. Click **GO.**

A list of 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 checking for location accuracy, you are checking the ability of the existing access point deployment to 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 Conduct Accuracy Testing

There are two methods of conducting location accuracy testing:

- 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.

Note The **Advanced Debug** option must be enabled in Cisco WCS to allow use of both the Scheduled and On-demand location accuracy testing features. Additionally, the Location Accuracy Tool does not appear as an option under the Tools menu when the Advanced Debug option is not enabled.

To enable the advanced debug option in Cisco WCS, follow these steps:

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

Step 2 Select **Properties** from the Select a command drop-down menu and click **GO**.

Step 3 Select **Enabled** from the Advanced Debug drop-down menu. Click **OK**.

Note If Advanced Debug is already enabled, you do not need to do anything further. Click **Cancel**.

You can now run location accuracy tests on the mobility services engine using the Location Accuracy Tool.

Using Scheduled Accuracy Testing to Verify Accuracy of Current Location

To configure a scheduled accuracy test, follow these steps:

Step 1 Click **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 entered using a 24-hour clock.

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

Step 9 Select the Destination point for the test results. You can have the report emailed to you or 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. Click **Administrator > Settings > Mail Server** 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 a MAC address check box, two icons which overlay each other appear on the map.

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 displays in the left-most 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. 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 displays as Scheduled when the test is about to execute. A status of Running displays when the test is in process 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 the test name and then select the **Results** tab on the page that displays.

Step 16 At the Results panel, click the Download link under the Saved Report heading to view the report.

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 Accuracy Testing to Test Location Accuracy

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. It is generally used 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 Click **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 Tests results are viewed 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 particular 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) displays in a drop-down menu to its right.

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

Step 12 Click **Start** to begin collection of accuracy data.

Step 13 Click **Stop** to finish collection. 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

Note You can download logs for accuracy tests from the Accuracy Tests summary page.

- To do so, check the listed test check box and select either Download Logs or Download Logs for Last Run from the Select a command menu and 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 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 location appliance.

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.

Adding Chokepoints to the Cisco WCS

Chokepoints are installed and configured as recommended by the chokepoint vendor. When the chokepoint is installed and operational, you can add the chokepoint to the location database and positioned on a Cisco WCS map.

Note Chokepoints (also known as exciters) are managed by the chokepoint vendor's application. For details refer to the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User's Guide* for configuration details at the following link: http://support.aeroscout.com.

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

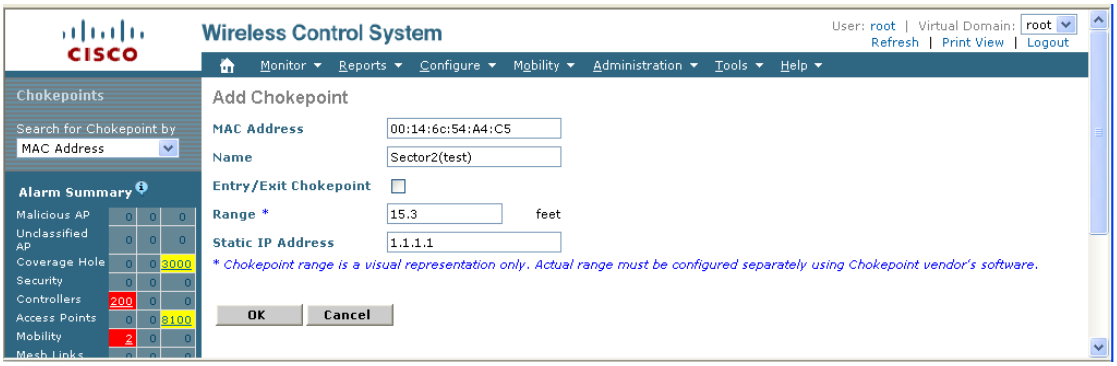
Step 1 Click **Configure > Chokepoints** from the main menu (top).

The All Chokepoints summary window appears.

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

The Add Chokepoint entry screen appears.

Figure 7-4 Add Chokepoint Window



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

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

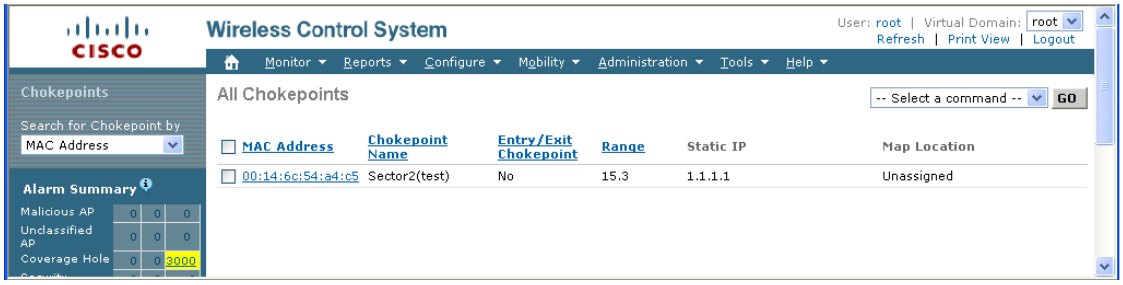
Step 4 Check the Entry/Exit Chokepoint check box if you want the chokepoint to function as an perimeter chokepoint. Its function is to track the entry and exit of clients and tags from an area or floor.

Note If a tag shows strong RSSIs on two floors, you can check for the last perimeter chokepoint the tag passed to determine its current floor.

Step 5 Click **OK** to save the chokepoint entry to the database.

The All Chokepoints summary window appears with the new chokepoint entry listed (Figure 7-5).

Figure 7-5 All Chokepoints Summary Window



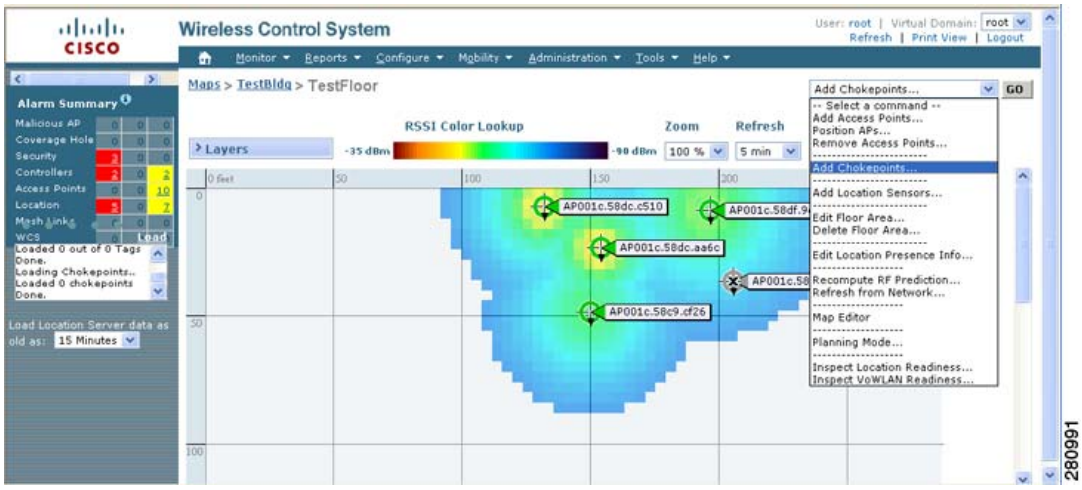
Note After you add the chokepoint to the database, you can place the chokepoint on the appropriate WCS floor map.

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

Figure 7-6 Monitor > Maps Window

Step 7 At the Maps window, select the link that corresponds to the floor location of the chokepoint. The floor map appears (Figure 7-7).

Figure 7-7 Selected Floor Map

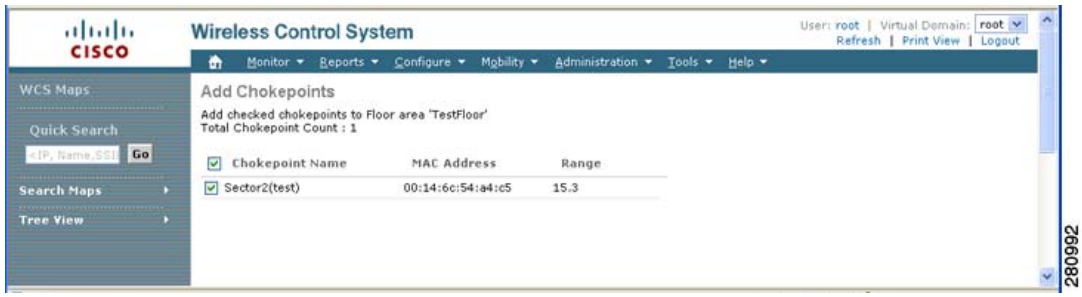


Step 8 Select **Add Chokepoints** from the Select a command menu. Click **GO**.

The Add Chokepoints summary window appears (Figure 7-8).

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

Figure 7-8 Add Chokepoints Summary Window

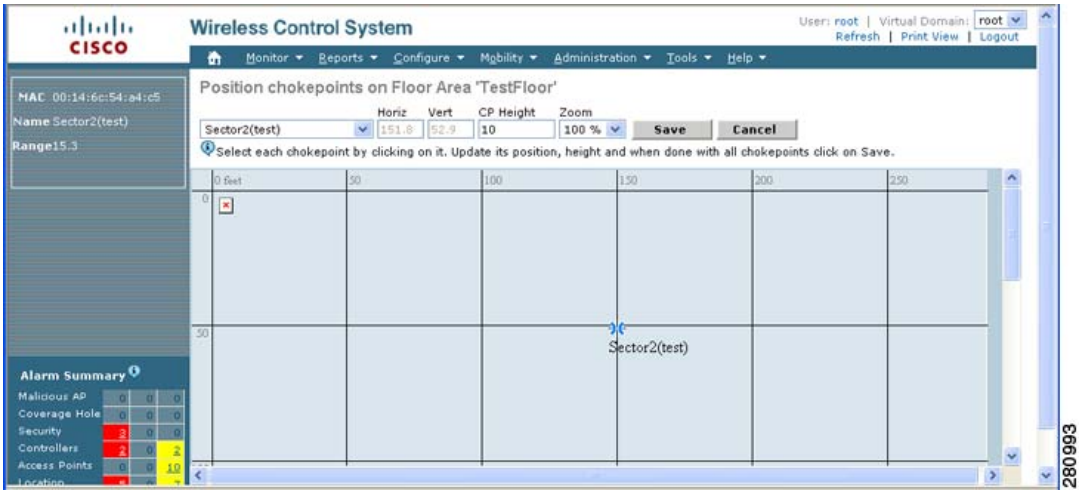


Step 9 Check the box next to the chokepoint to be added to the map. Click **OK** (bottom of screen).

A map appears with a chokepoint icon located in the top-left hand corner. You can now place the chokepoint on the map.

Step 10 Left click on the chokepoint icon and drag and place it in the proper location (Figure 7-9).

Figure 7-9 Chokepoint Icon is Positioned on the Floor Map



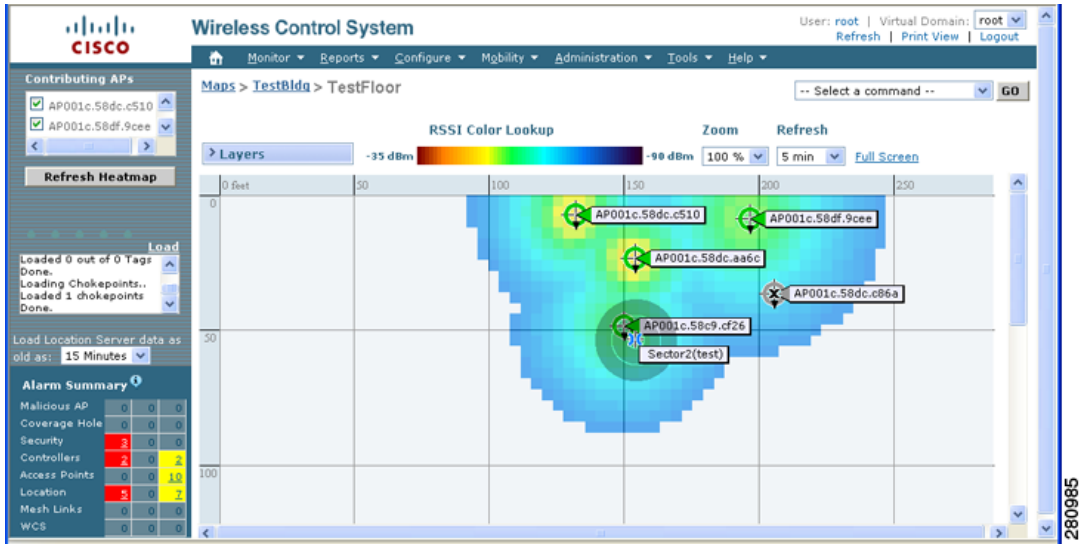
Note The MAC address, name, and coverage range of the chokepoint appear in the left panel when you click on the chokepoint icon for placement.

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

You are returned to the floor map and the added chokepoint appears on the map (Figure 7-10).

Note The icon for the newly added chokepoint may or may not appear on the map depending on the display settings for that floor. If the icon did not appear, proceed with Step 11.

Figure 7-10 New Chokepoint Displayed on Floor Map



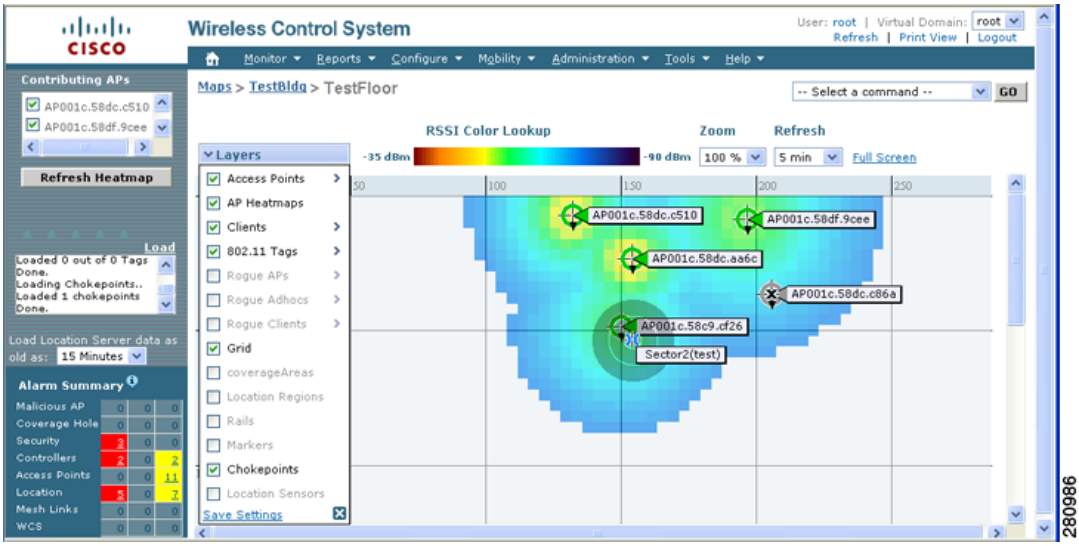
Note The rings around the chokepoint icon indicate the coverage area. When a Cisco CX tag and its asset passes within the coverage area, location details are broadcast and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is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

Note MAC address, name, and range of a chokepoint display when you pass a mouse over its map icon

Step 12 If the chokepoint does not appear on the map, click **Layers** to collapse a selection menu of possible elements to display on the map. Click the **Chokepoints** check box.

The chokepoint appears on the map (Figure 7-11).

Figure 7-11 Chokepoints Displayed on Map



Step 13 Click **X** to close the Layers window.

Note Do not select **Save Settings** unless you want to save this display criteria for all maps.

Removing Chokepoints from the WCS Database and Map

You can remove one or multiple chokepoints at a time.

To delete a chokepoint, follow these steps:

Step 1 Click **Configure > Chokepoints**. The All Chokepoints window appears.

Step 2 Check the box(es) next to the chokepoint(s) to be deleted.

Step 3 Select **Remove Chokepoints** from the Select a command drop-down menu. Click **GO** (Figure 7-12).

Figure 7-12 Removing a Chokepoint

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

You are returned to the All Chokepoints window. A message confirming deletion of the chokepoint appears. The deleted chokepoint(s) is 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 to aid in the location calculation of the asset. TDOA receivers use the method of Time Difference of Arrival (TDOA) to calculate tag location. This method 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 Systems" for details on adding a mobility services engine.

2. Add the TDOA receiver to the Cisco WCS database and map.

   Refer to "Adding Chokepoints to the Cisco WCS" section on page 7-13 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 User's Guide* for configuration details at the following link: http://support.aeroscout.com.

Adding Wi-Fi TDOA Receivers to Cisco WCS and Maps

After adding TDOA receivers to Cisco WCS maps and synchronizing, TDOA receiver configuration changes are done using the *AeroScout System Manager* application rather than Cisco WCS.

Note For more details on configuration options, refer to the AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User's 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, click **Configure > WiFi TDOA Receivers**. The All WiFi TDOA Receivers summary window appears.

Step 2 From the Select a command menu, choose **Add WiFi TDOA Receivers** and click **GO**.

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

Step 4 Click **OK** to save the TDOA receiver entry to the database. The All 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, click **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 Select **Add WiFi TDOA receivers** from the Select a command menu. Click **GO**.

The Add WiFi TDOA Receivers summary window appears.

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

Step 8 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 located in the top-left hand corner. You are now ready to place the TDOA receiver on the map.

Step 9 Left click on 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 on the TDOA receiver icon for placement.

Step 10 After placing the TDOA receiver, enter the height of the receiver in the sensor height field.

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

You are returned to the floor heat map and the added TDOA receiver appears on the map.

Note The icon for the newly added TDOA receiver may or may not appear on the map depending on the display settings for that floor. If the icon did not appear, proceed with Step 12.

Step 12 If the TDOA receiver does not appear on the map, click **Layers** to collapse a selection menu of possible elements to display on the map. Click the **WiFi TDOA Receivers** check box.

Step 13 The TDOA receiver appears on the map (Figure 7-13).

Note You can hover over (mouse over) a TDOA receiver on a map to see configuration details for that receiver.

Figure 7-13 WiFi TDOA Receiver Enabled on Layers Menu for Map Display

Step 14 Click **X** to close the Layers window.

Note Do not select **Save Settings** in the Layers menu unless you want to save this display criteria for all maps.

Removing Wi-Fi TDOA Receivers from Cisco WCS and Maps

You can remove one or multiple 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, click **Configure > WiFi TDOA Receivers**. The **All 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.

You are returned to 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 2.4GHz 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).

After enabling Monitor Mode at the access point level, you must then enable TOMM and assign monitoring channels on the 802.11 b/g radio of the access point.

Note For details on enabling Monitor Mode on an access point, refer to Step 5 in the "Configuring Access Points" section in Chapter 9 of the *Cisco Wireless Control System Configuration Guide*, Release 5.1.

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

Step 1 After enabling Monitor Mode at the access point level, click **Configure > Access Points**.

Step 2 At the All Access Points Summary window, select the 802.11 b/g Radio link for the appropriate access point.

Step 3 At the Radio parameters window, disable Admin Status by unchecking the check box. This disables the radio.

Step 4 Check the Location Optimized Channel Assignment check box. Drop-down menus for each of the four configurable channels display.

Step 5 Select the four channels 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.

Step 6 Click **Save**. Channel selection is saved.

Step 7 At the Radio parameters window, re-enable the radio by checking the Admin Status check box.

Step 8 Click **Save**. The access point is now configured as a TOMM access point.

The AP Mode displays as Monitor/TOMM 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 areas that are included (inclusion areas) in the calculations and those areas that are not included (exclusion areas).

For example, you might want to exclude areas 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 only calculated for clients.

Guidelines

Inclusion and exclusion areas can be any polygon shape and must have at least three points.

You can only define 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.

Defining an Inclusion Region on a Floor

To define an inclusion area, follow these steps:

Step 1 Click **Monitor > Maps**.

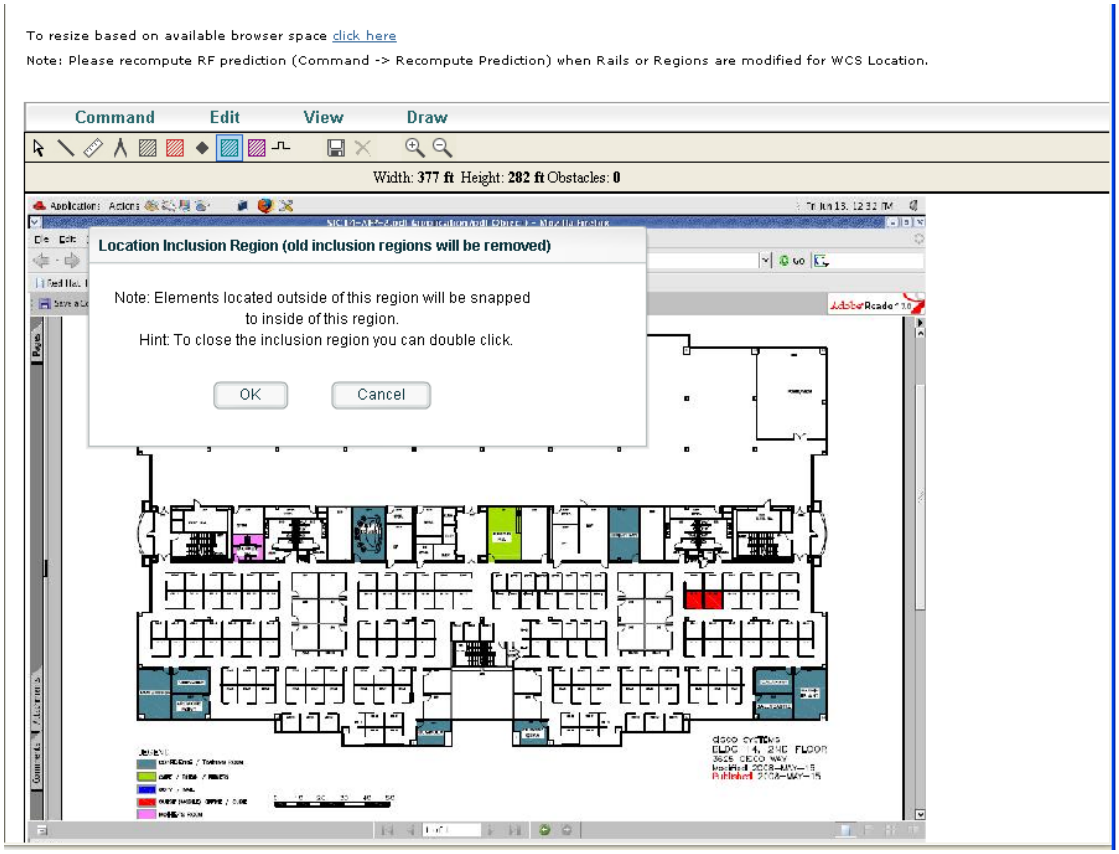
Step 2 Click on the name of the appropriate floor area.

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

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

Note A message box appears reminding you that only one inclusion area 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. The inclusion region is indicated by a solid aqua line and generally outlines the region (Figure 7-14).

Figure 7-14 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.

Step 9 Select **Save** from the Command menu 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, select **Exit** from the Command menu.

Step 11 At the floor map, click the **Layers** drop-down menu.

Step 12 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**. Close the Layers configuration panel.

Step 13 To resynchronize the Cisco WCS and location databases, click **Mobility > 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).

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 areas that are excluded (exclusion areas) in the calculations. For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion areas are generally defined within the borders of an inclusion area.

To define an exclusion area, follow these steps:

Step 1 Click **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 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.

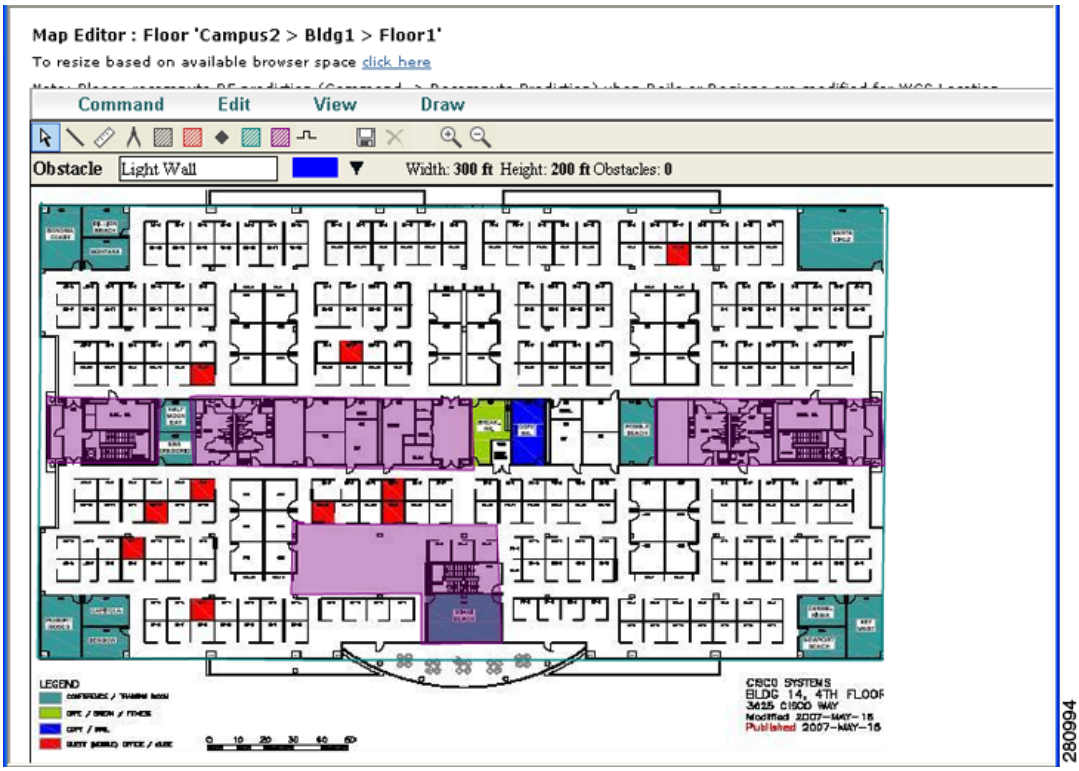
Step 6 To begin defining the exclusion area, move the drawing icon to the starting point on the map and click once.

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 7-15).

Figure 7-15 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 on 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, click the **Layers** drop-down menu.

Step 13 Check the Location Regions check box if it is not already checked and then click **Save setting**s and close the Layers configuration panel when complete.

Step 14 To resynchronize the Cisco WCS and location databases, click **Mobility > Synchronize Services**.

Step 15 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 that represents a conveyor belt. Additionally, you can define an area around the rail area known as the snap-width to further assist location calculations. This represents the area in which you expect clients to appear. Any client located within the snap-width area is plotted on the rail line (majority) or just outside of the snap-width area (minority).

Note Rail line configurations do not apply to tags.

The snap-width area is defined in feet or meters (user-defined) and represents the distance that is monitored on either side (east and west or north and south) of the rail.

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

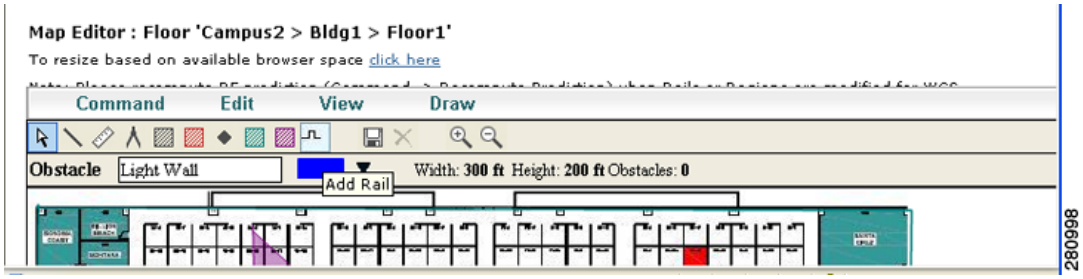
Step 1 Click **Monitor > Maps**.

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 At the map, click the rail icon (to the right of the purple exclusion icon) in the tool bar (see Figure 7-16).

Figure 7-16 Rail Icon on Map Editor Tool Bar



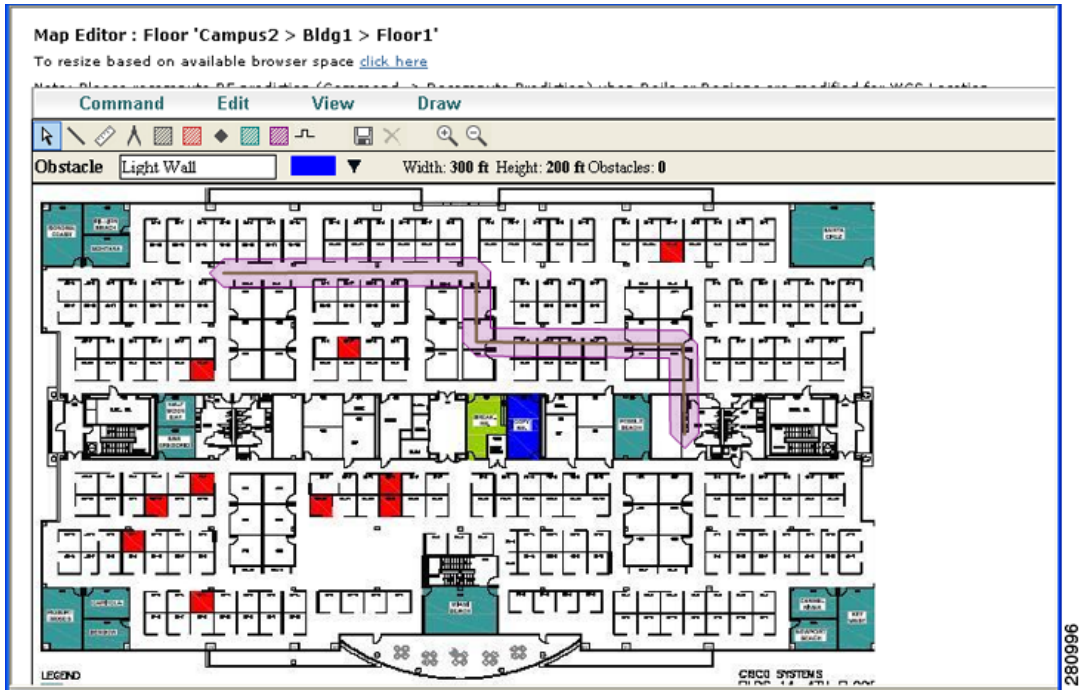
Step 5 In the message panel that appears, enter a snap-width (feet or meters) for the rail and then click **OK.** A drawing icon appears.

Note The snap-width is defined in feet or meters (as defined by the user) and represents the distance that is monitored on either side (left and right) of the rail.

Step 6 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 either side by the defined snap-width region (see Figure 7-17).

Figure 7-17 Rail Line



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 on 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, click the **Layers** drop-down menu.

Step 10 Check the Rails check box for if it is not already checked and then click **Save settings** and close the Layers configuration panel when complete.

Step 11 To resynchronize the Cisco WCS and mobility services engine, click **Mobility > Synchronize Services**.

Step 12 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).

Modifying Context-Aware Software Parameters

You can modify Context-Aware Software properties as to 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 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. Licenses for tags and clients are offered in a range of quantities, ranging from 3,000 to 12,000 units. Refer to the *Release Notes for Cisco 3300 Series Mobility Services Engine for Software Release 5.1.xx.0* at the following link for details: http://www.cisco.com/en/US/products/ps9742/prod_release_notes_list.html

Modifying Tracking Parameters

The mobility services engine can track up to18,000 clients and up to18,000 tags (with the proper license purchase). Updates on the locations of elements being tracked are provided to the mobility services engine from the Cisco wireless LAN controller.

Only those elements designated for tracking by the controller are viewable 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 element locations (client stations, active asset tags, and rogue clients and access points) you actively track.
- 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 track 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, click **Mobility > 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 In the Context-Aware Software menu (left panel), select **Tracking Parameters** from the Administration sub-heading to display the configuration options.

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

:

Table 7-1 Tracking Parameters

Parameter	Configuration Options
Tracking Parameters	
Client Stations	1. Check the **Enable** check box to enable tracking of client stations by the mobility services engine. 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** The actual number of tracked clients is determined by the license purchased. **Note** Active Value (display only): Indicates the number of client stations currently being tracked. **Note** Not Tracking (display only): Indicates the number of client stations beyond the limit.
Asset Tags	1. Check the **Enable** check box to enable tracking of asset tags by the mobility services engine. 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 mobility services engine. **Note** The actual number of tracked tags is determined by the license purchased. **Note** Active Value (display only): Indicates the number of asset tags currently being tracked. **Note** Not Tracking (display only): Indicates the number of asset tags beyond the limit.

Table 7-1 Tracking Parameters (continued)

Parameter	Configuration Options
Rogue Clients and Access Points	1. Check the **Enable** check box to enable tracking of rogue clients and asset points by the mobility services engine. 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 to18,000 which is the maximum number of rogue clients and access points that can be tracked by a mobility services engine. **Note** The actual number of tracked rogues (clients and access points) is driven by the client license purchased. The user must consider the number of clients that are being tracked in determining the available quantity to allocate to track rogue clients and access points because clients and rogue clients and access points are addressed by the same license. **Note** Active Value (display only): Indicates the number of rogue clients and access points currently being tracked. **Note** Not Tracking (display only): Indicates the number of rogue clients and asset tags beyond the limit.
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.
SNMP Parameters	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 release 4.1 and earlier and location server release 3.0 and earlier only).
SNMP Timeout	Enter the number of seconds before a polling cycle times out. 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.

Table 7-1 Tracking Parameters (continued)

Parameter	Configuration Options
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** to store the new settings in the mobility services engine database.

Modifying Filtering Parameters

In Cisco WCS, you can limit the number of asset tags, clients, and rogue clients and access points whose location is tracked by filtering on:

- 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 single 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 to another controller but whose probing activity causes them to be seen by another controller and counted as an element by 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, click **Mobility > 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 From the Context-Aware Software menu (left panel), select **Filtering Parameters** from the Administration sub-heading 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 location calculation of probing clients.
Enable Location MAC Filtering	1. Check the check box to enable MAC filtering of specific elements by their MAC address. 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. The imported list of MAC addresses auto-populates the Allowed List and Disallowed List based on their designation in the file. **Note** To view allowed MAC address formats, click on 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 depress the **Ctrl** to highlight additional MAC addresses. Click the **Allow** or **Disallow** button based on its desired destination. **Note** If a MAC address is not listed in the Allow or Disallow column, by default, it appears in the Blocked MACs column. If you click the **Unblock** button, the MAC address automatically moves to the Allow column. You can move it to the Disallow column by selecting 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 histories on client stations, rogue access points, and asset tags. These histories are received from those controllers associated with the mobility services engine.

You can also program the mobility services engine to periodically prune (remove) duplicate data from its historical files to reduce the amount of data stored on its hard drive.

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

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

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

Step 3 From the Context-Aware Software menu, select **History Parameters** from the Administration sub-heading.

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 of time in which the mobility services engine starts data pruning (between 0 and 23 hours, and between 1 and 59 minutes). Also enter the interval in minutes after which data pruning starts again (between 0, which means never, and 99900000). Default start time is 23 hours and 50 minutes, and the default interval is 1440 minutes.
Enable History Logging of Location Transitions for *Client Stations, Asset Tags* and *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 type(s). When history logging is enabled for an element, a location transition event is logged each time the location of the selected element changes.

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

Enabling Location Presence

You can enable location presence by 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.

Location Presence can be configured when a new Campus, Building, Floor or Outdoor Area is being added or configured at a later date.

Once enabled, the mobility services engine is capable of providing 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 5.1 and greater.

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 Click **Mobility > Mobility Services >** *Device Name*. Select the mobility services engine to which the campus or building is assigned.

Step 2 From the Context-Aware Software menu (left-panel), select **Presence Parameters** from the Administration sub-heading. The Presence window displays.

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

Step 4 Select one of the following Location Resolution options.

a. When Building is selected, the mobility services engine can provide any requesting client, its location by building.

- For example, if a client requests its location and the client is located in Building A, the mobility services engine returns the client address as *Building A*.

b. When AP is selected, the mobility services engine can provide any requesting client, its location by its associated access point. The MAC address of the access point displays.

- For example, if a client requests its location and the client is associated with an access point with a MAC address of 3034:00hh:0adg, the mobility services engine returns the client address of *3034:00hh:0adg*.

c. When X,Y is selected, the mobility services engine can provide any requesting client, its location by its X and Y coordinates.

- For example, if a client requests its location and the client is located at (50, 200) the mobility services engine returns the client address of *50, 200.*

Step 5 Check any or all of the location formats.

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

Note To import a file with multiple Civic listings, refer to the "Importing Civic Information" section on page 7-37.

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

Step 6 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 7 Check the Retransmission Rule Enable check box to allow the receiving client to retransmit the received information to another party.

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

Step 9 Click **Save**.

Importing Asset Information

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

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

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

Step 3 Click **Context Aware Software** (left panel).

Step 4 Click **Import Asset Information** from under the Administration sub-menu heading.

Step 5 Enter the name of the text file or browse for the file name.

Information in the imported file should be one of the following formats:

a. tag format: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname

b. station format: #station, 00:00:00:00:00:00, categoryname, groupname, assetname

c. 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

d. 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 6 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, click **Mobility > Mobility Services.**

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

Step 3 Click **Context Aware Software** (left panel).

Step 4 Click **Export Asset Information** from under the Administration sub-menu heading.

Information in the exported file is in one of the following formats:

a. tag format: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname

b. station format: #station, 00:00:00:00:00:00, categoryname, groupname, assetname

c. 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

d. chokepoint format: BuildingName, FloorName, CPMacAddress, CPName, IP Address, Range, X,Y, Z, IsPerimeter

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

IsPerimeter indicates the chokepoint is a perimeter chokepoint.

CP refers to the chokepoint

Step 5 Click **Export**.

You are prompted to **Open** (display to screen) or **Save** (to external PC or server) the asset file or to **Cancel** the request.

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.

Importing Civic Information

To import civic information for the mobility services engine using Cisco WCS, follow these steps:

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

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

Step 3 Click **Context Aware Software** (left panel).

Step 4 Click **Import Civic Information** from under the Administration sub-menu heading.

Step 5 Enter the name of the text file or browse for the file name.

Information in the imported file must be in the following format:

Switch IP Address, Slot Number, Port Number, Extended Parent Civic Address, X,Y, Floor ID, Building ID, Network Design ID, ELIN:"ELIN", PIDF-Lo-Tag:"Civic Address Element Value",...

Note Each entry must be on a separate line.

Step 6 Click **Import**.

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 Tag location is not managed or affected by location parameter settings. Only client location is affected.

To configure location parameters, follow these steps:

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

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

Step 3 From the Context Aware Software menu (left panel), select Location Parameters from under the Advanced sub-heading. 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 corresponding check box to enable the calculation of the time required to compute location. **Note** This parameter applies only to clients. **Caution** Enable only under Cisco TAC personnel guidance because enabling this parameter slows down overall location calculations.
OW Location	Check the corresponding check box to enable 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.

Table 7-4 Location Parameters (continued)

Parameter	Configuration Options
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 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.
Smooth Location Positions	Smoothing compares an element's prior location to its most recent reported location by applying a weighted average calculation to determine its current location. The specific weighted average calculation employed is tied to the given smoothing option selected. Default value is More Smoothing. Options: • Off (No smoothing): Elements assumed to be in location indicated by most recent polling. • Less smoothing: Prior location weighted at 25% and New location weighted at 75%. • Average smoothing: Prior location weighted at 50% and New location weighted at 50%. • More smoothing: Prior location weighted at 75% and New location weighted at 25%. • Maximum smoothing: Prior location weighted at 90% and New location weighted at 10%. **Note** This parameter applies only to clients.
Chokepoint Usage	Check the Enable check box to enable tracking of Cisco compatible tags by chokepoints. **Note** This parameter is ignored by the mobility services engine.

Table 7-4 Location Parameters (continued)

Parameter	Configuration Options
Use Chokepoints for Interfloor conflicts	Perimeter chokepoints or weighted location readings can be selected to determine the location of Cisco compatible tags. Options: • Never: When selected, perimeter chokepoints are not used to determine the location of Cisco compatible tags. • Always: When selected, perimeter points are used to determine the location of Cisco compatible tags. • Floor Ambiguity: When selected, both weighted location readings and perimeter chokepoints are used to generate location for Cisco compatible tags. If similar locations are calculated by the two methods, the perimeter chokepoint value is used by default. **Note** This parameter is ignored by the mobility services engine.
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. **Note** This parameter is ignored by the mobility services engine.
Allow Civic Address updates from Switches	Check the enable check box to receive civic address updates from the controller. When enabled, the civic address parameter provides city, state, postal code and country specifics for the mobility services engine. This capability is in addition to the Cisco default settings of campus, building, floor, and X, Y coordinates. This information can then be requested by clients on demand for use by location-based services and applications. **Note** For more details on civic addresses and other location options, refer to the "Enabling Location Presence" section on page 7-34.

Step 5 Click **Save** to store your selections in the Cisco WCS and mobility services engine databases.

Configuring Notification Parameters

You can use Cisco WCS to configure mobility services engine event notification parameters that define such items as how often the notifications are generated or resent by the mobility services engine.

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

You can also enable forwarding of northbound notifications for tags to be sent to third-party applications.

The format of northbound notifications sent by the mobility services engine is available on the Cisco developers support portal at:

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

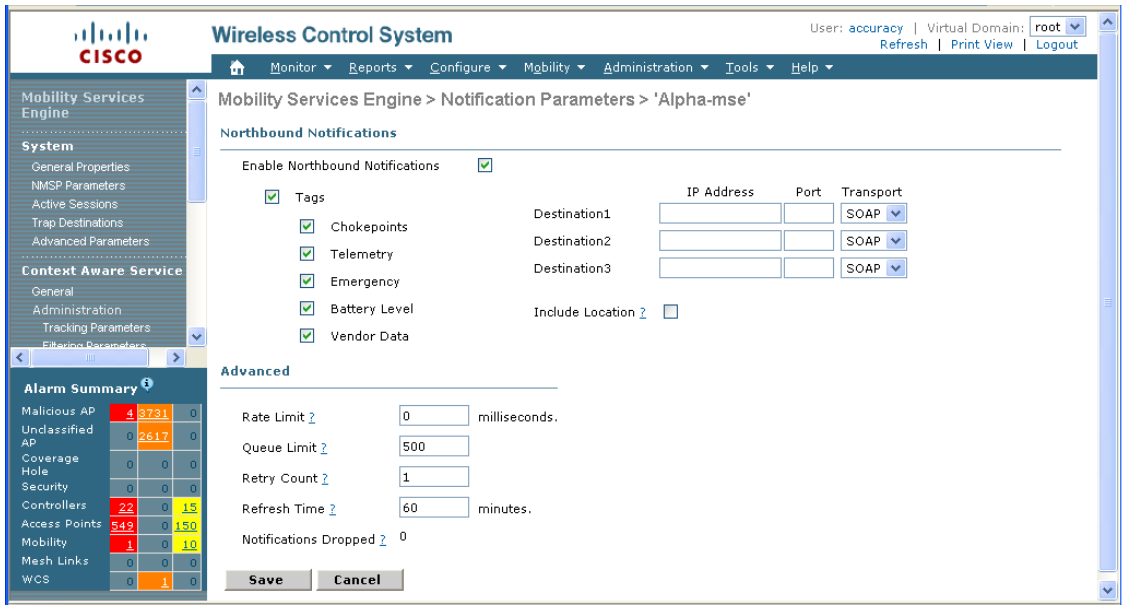
To configure notification parameters, follow these steps:

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

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

Step 3 From the **Context Aware Software** menu (left panel), select **Notification Parameters** from the Advanced sub-heading to display the configuration options.

Figure 7-18 Mobility Services Engine > Context Aware Software > 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.

Step 6 Check the check box for each of the tag notification event types (chokepoints, telemetry, emergency, battery level, vendor data) that you want sent.

Step 7 Check the **Include location** check box to send the tag location.

Note You can define what type of location information is sent for the tag. Options include building, X, Y map coordinates, civic (address), city, state) or GEO (longitude, latitude). Refer to the "Enabling Location Presence on a Mobility Services Engine" section in Chapter 7 for configuration details.

Step 8 Enter the IP address and port for the system that is to receive the northbound notifications.

Step 9 Select the transport type from the drop-down menu.

Step 10 To modify the notification parameter settings, enter the new value in the appropriate field in the Advanced section of the window. Definitions for each of the parameters is listed in Table 7-5.

Table 7-5 Notification Parameters:

Parameter	Configuration Options
Rate Limit	Enter the rate in milliseconds at which the mobility services engine will generate notifications. A value of 0 (default) means that the mobility services engine will generate event notifications as fast as possible.
Queue Limit	The event queue limit for sending notifications. The mobility services engine will drop any event above this limit. Default value is 500.
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 generated will 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 an event notification is resent. For example, suppose you enter 30 in this field. If a monitored element goes out of a specified area, the mobility services engine sends an event notification. Then, until the event is cleared, the mobility services engine resends an event notification every 30 minutes.
Notifications Dropped	(Read only). The number of event notifications dropped from the queue since startup.

Step 11 Click **Save** to store your updates in the Cisco WCS and mobility services engine databases.

Configuring a Location Template

You can define a location template for the controller for 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 notification parameters, follow these steps:

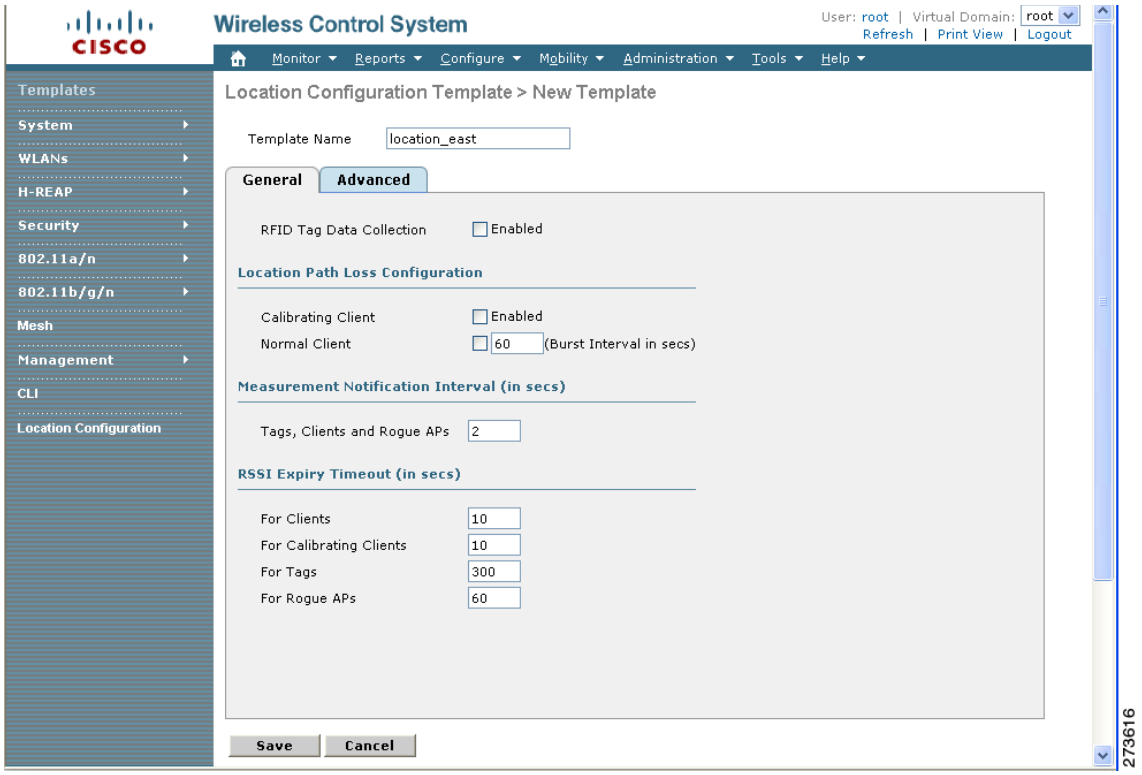
Step 1 Click **Configure > Controller**.

Step 2 Select **Location Configuration** (left panel).

Step 3 Select **Add Template** from the Select a command drop-down menu.

Step 4 At the New template window, enter a name for the location template (Figure 7-19).

Figure 7-19 New Template > General Panel



Step 5 At the General panel modify parameters as necessary. Definitions for each of the parameters is listed in Table 7-6.

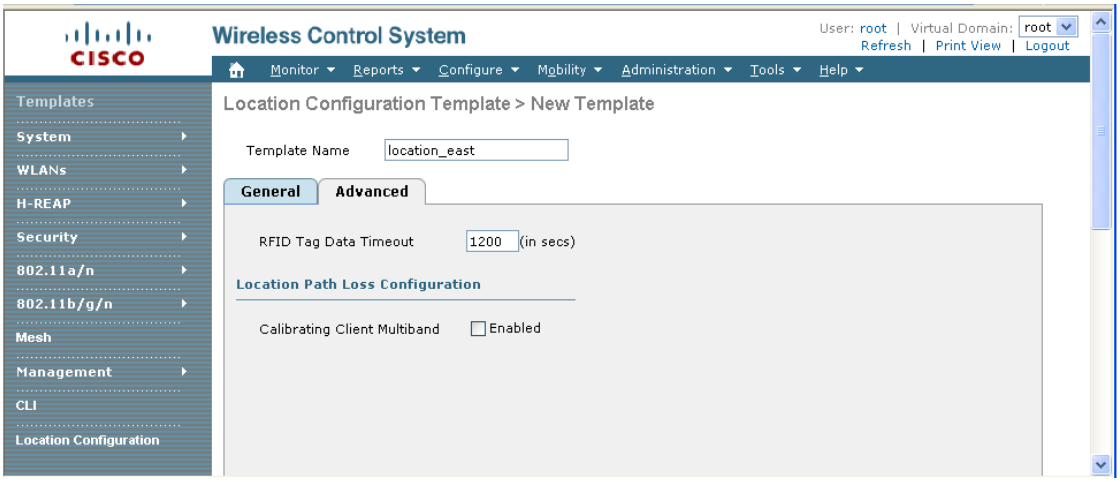
Table 7-6 General Location Parameters

Parameter	Configuration Options
RFID tag calculation	Check the **Enabled** check box to collect data on tags.
Calibrating Client	Check the **Enabled** check box to enable calibration for the 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.

Table 7-6 General Location Parameters (continued)

Parameter	Configuration Options
Measurement Notification Interval	Enter a value to set the NMSP measurement notification interval for clients, tags and rogues. This value can be applied to selected controllers via the template. Setting this value on the controller generates out-of-sync notification and the user is able to view this on the Synchronize Servers page. When different measurement intervals exists between a controller and the mobility services engine exist, 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.

Figure 7-20 New Template > Advanced Parameters Panel



Step 6 At the Advanced panel modify parameters as necessary (Figure 7-20). Definitions for each of the parameters is listed in Table 7-6.

Table 7-7 Advanced Location Parameters

Parameter	Configuration Options
RFID Tag Data Timeout	Enter a value to set the RFID tag data timeout setting.
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 7 Click **Save**.

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 utilization and element counts (tags, clients, rogue clients and access points).

It also describes how to use Cisco WCS to view system, client, and asset tag status as well as status on 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. Details on how to have email notifications for alarms sent to you is described as well as how to define those types (all, critical, major, minor, warning) of alarm notifications that are sent to you.

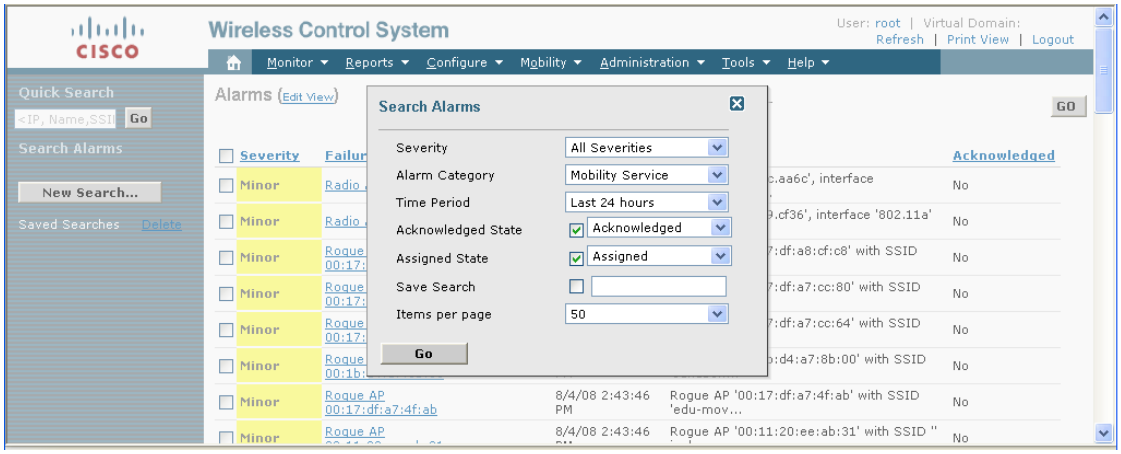
Viewing Alarms

To view mobility services engine alarms, follow these steps:

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

Step 2 Click **New Search**. A configurable search panel for alarms appears (Figure 8-1).

Figure 8-1 Search Alarm Panel



Step 3 Select the Severity of Alarms to display. Options are All Severities, Critical, Major, Minor or Warning.

Step 4 Select **Mobility Service** from the Alarm Category.

Options are: All Types, Access Points, Controller, Coverage Hole, Config Audit, Mobility Service Location Notifications, Interference, Mesh Links, Rogue AP, Rogue Adhoc**,** Security and WCS.

Step 5 Select the time frame for which you want to review alarms by selecting the appropriate option 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 6 Check the **Acknowledged State** check box to exclude the acknowledged alarms and their count from the Alarm Summary window.

Step 7 Check the **Assigned Stat**e check box to exclude the assigned alarms and their count from the Alarm Summary window.

Step 8 To save the search criteria for later use, check the **Save Search** box and enter a name for the search.

Note The search is then accessible from the Saved Searches drop-down menu (left-panel) of the Monitor > Alarms window.

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

Step 10 Click **GO**. Alarms summary panel appears with search results.

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

Step 11 Repeat Step 2 to Step 10 to see notifications for the mobility services engine by entering **Location Notifications** as the alarm category in Step 4.

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**) and 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

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.

Note 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 clear an alarm when the condition that caused it no longer exists.

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

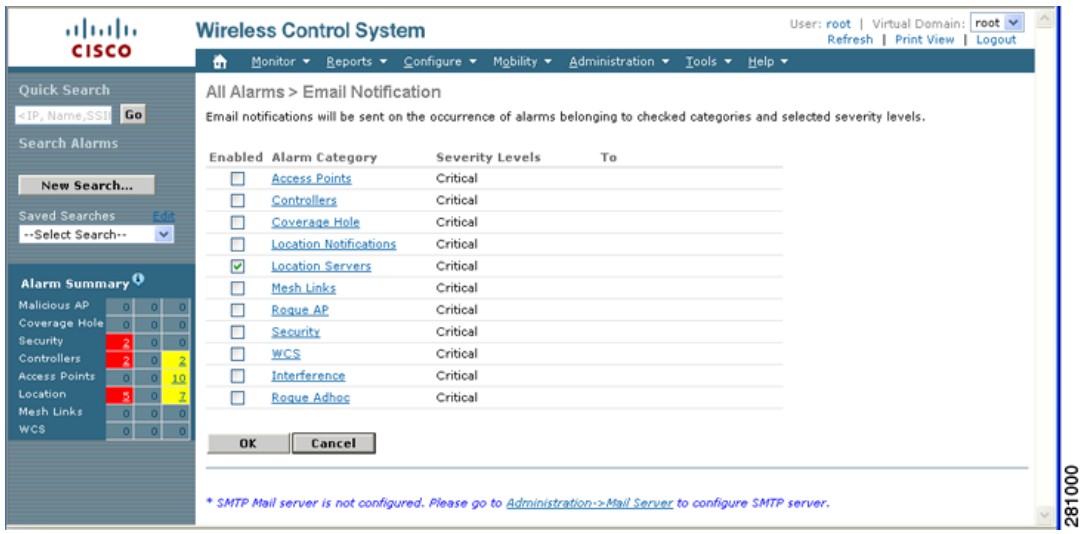
You can select the alarm severity types (critical, major, minor and warning) that are emailed to you.

To send alarm notifications, follow these steps:

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

Step 2 From the Select a commands drop-down menu, choose **Email Notification**, and click **GO**. The Email Notification window appears.

Figure 8-2 All Alarms > Email Notification Window



Note A SMTP Mail Server must be defined prior to entry of target email addresses for email notification. Choose **Administraton > Settings > Mail Server** to enter the appropriate information. You can also select the Administration > Mail Server link, if displayed, on the Email Notification window noted above.

Step 3 Click the **Enabled** box next to the **Location Servers**.

Note Enabling the Location Servers alarm category sends all alarms related to location services and the mobility services engine system to the defined email address.

Step 4 Click the **Location Servers** link. The panel for configuring the alarm severity types (critical, major, minor and warning) 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. Email addresess are separated 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, 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, and mobility service

Note The product type: mobility service reports events for mobility services engines.

- 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, click **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, MAC address, or Name, enter that value in the Quick Search field (left panel). Click **GO**.
- To display events by severity and category, select the appropriate options from the Severity and Event Category drop-down menus (left panel). Click **Search**.

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 object 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, click **Mobility > Mobility Services**.

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

Step 3 From the System menu (left panel) click **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 from the Logging Level drop-down menu.

There are four logging options: **Off**, **Error**, **Information**, and **Trace**.

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 of its events.

Step 6 Click **Save** to apply your changes.

Downloading Location Server 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, click **Mobility > Mobility Services**.

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

Step 3 Click **Logs** (left panel).

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 utilization report for a mobility services engine. By default, reports are stored on the Cisco WCS server.

The location utilization report summarizes and charts the following information in two separate charts for a prescribed period of time:

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

You can generate a utilization report for a mobility services engine. Once defined, the report can be saved for future diagnostic use and run on either an ad hoc or scheduled basis.

You can define the following in a utilization report:

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

Creating a System Utilization Report

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

Step 1 In Cisco WCS, click **Reports > Performance Reports.**

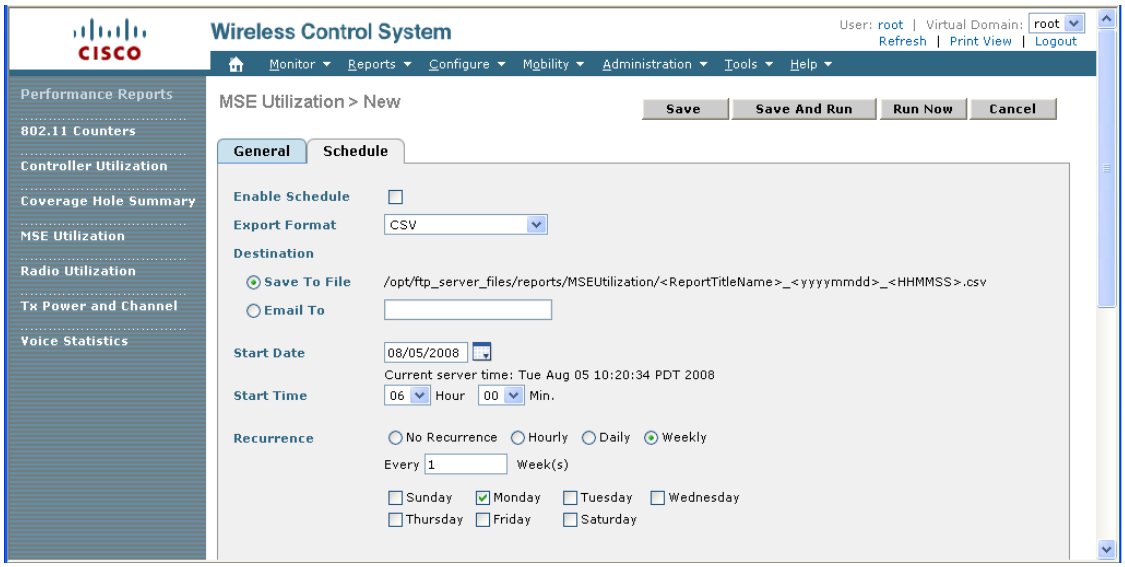
Step 2 Select **MSE Utilization** from the listing under the Performance Reports heading (left panel).

The MSE summary window appears.

Step 3 Select **New** from the Select a command drop-down menu. Click **GO**.

A tabbed panel appears (see Figure 8-3).

Figure 8-3 Reports > Performance Reports > MSE Utilization



Step 4 Enter a report title.

Step 5 The Report By selection is always MSE.

Step 6 Select either a specific mobility services engine or **All MSEs** from the drop-down MSE menu.

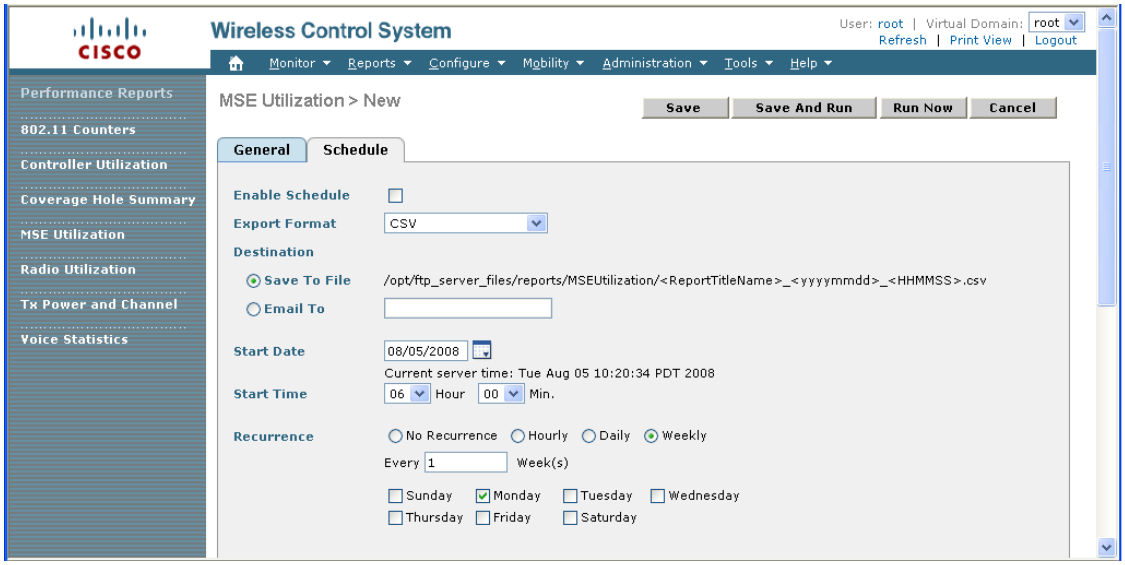
Step 7 Enter the reporting period for the report. You can define the report to collect data on either an hourly or weekly basis or at a specific date and time. The selected reporting period type will display on the x-axis. Select the **Schedule** tab when complete.

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

Step 8 At the Schedule window, check the **Enable Schedule** check box.

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

Figure 8-4 MSE Utilization > New > Schedule Tab



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

- If you select the Save To 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 To option, an SMTP Mail Server must be defined prior to entry of target email address. Choose **Administrator > Settings >** *Mail Server* 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 only on the screen when the weekly option is chosen.

Step 14 When complete 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 tab.
- Click **Save and Run** to save the changes and run the report now. The report runs regardless of any scheduled time associated with the report and is viewable in the **Results** tab. Additionally, 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 tab.
  - At the results window, you can cancel or delete the 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 scheduled time associated with the report and is viewable in the **Results** tab. If the report is too large to display in the WCS window, you are referred to the history tab to download the file for viewing. Click **Save** if you want to save the report scenario you entered.

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

Viewing a Defined System Utilization Report

To view results of a defined report, follow these steps:

Step 1 In Cisco WCS, click **Reports > Performance Reports**.

Step 2 Select **MSE Utilization** from the listing under the Performance Reports heading.

The MSE Utilization summary window appears. Any pre-defined reports, previously created and saved, are listed.

Note You can select one of the listed reports or you can define a new report. For details on creating a new report, see the "Creating a System Utilization Report" section on page 8-7.

Step 3 Click the listed report's link to review its settings. The two-tabbed window appears.

Step 4 Review or modify the report parameters on the General tab window. When finished, select the **Schedule** tab.

Step 5 Check the **Enable Schedule** check box to enable the report, if not already checked.

Step 6 Review and edit other parameters, as necessary. When you are finished with your review or edit, 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 tab.
- Click **Save and Run** to save the changes and run the report now. The report runs regardless of any scheduled time associated with the report and is viewable in the **Results** tab. Additionally, 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 tab.
  - At the results window, you can cancel or delete the 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 scheduled time associated with the report. If the report is too large to display in the WCS window, you are referred to the history tab to download the file for viewing. Click **Save** if you want to save the report scenario you entered. You can also delete or cancel the report.

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

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, click **Mobility > Mobility Services.**

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

Step 3 Click **Maintenance** (left).

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, click **Mobility > Mobility Services**.

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

Step 3 Click **Maintenance** (left panel).

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 can run the restore process in the background while working on other mobility service engine operations in other Cisco WCS windows.

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, click **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, click **Mobility > Mobility Services.**

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

Step 4 Click **Maintenance** (left panel).

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-K9-5-2-49-0-64bit.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* at the following link: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.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.

Defragmenting the Mobility Services Engine Database

Over time, the mobility services engine's database might get fragmented, which might lead to a decrease in the system's performance. To fix this problem, use Cisco WCS to defragment the database.

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

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

Step 2 Click the name of the mobility services engine that you want to defragment its database.

Step 3 Click **System** (left panel).

Step 4 Click **Advanced Parameters**.

Step 5 In the Advanced Commands section, click **Defragment Database**.

Step 6 Click **OK** to confirm that you want to defragment the mobility services engine's database.

Rebooting the Mobility Services Engine Hardware

If you need to restart a mobility services engine, follow these steps:

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

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

Step 3 Click **System** (left panel).

Step 4 Click **Advanced Parameters**.

Step 5 In the Advanced Commands section (right), click **Reboot Hardware**.

Step 6 Click **OK** to confirm that you want to reboot the mobility services engine hardware.

The rebooting process takes a few minutes to complete.

Shutting Down the Mobility Services Engine Hardware

If you need to shutdown a mobility services engine, follow these steps:

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

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

Step 3 Click **System** (left panel).

Step 4 Click **Advanced Parameters**.

Step 5 In the Advanced Commands section (right), click **Shutdown Hardware**.

Step 6 Click **OK** to confirm that you want to shutdown the mobility services engine.

Clearing Mobility Services Engine Configurations

To clear a mobility services engine configuration and restore its factory defaults, follow these steps:

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

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

Step 3 Click **System** (left panel).

Step 4 Click **Advanced Parameters**.

Step 5 In the Advanced Commands section (right), click **Clear Configuration**.

Note Using this command also clears the system's database.

Step 6 Click **OK** to clear the mobility services engine configurations.

INDEX

N

O

P

R

S

U