CISCO™

Cisco Location Appliance Configuration Guide, Release 5.2

Last revised: November 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

C O N T E N T S

Preface

This section describes the objectives, audience, organization, and conventions of the *Cisco Location Appliance Configuration Guide*.

Objectives

This publication explains the steps for using Cisco Wireless Control System (WCS) for configuring and managing location servers.

Audience

This publication is for the person configuring and managing location services. The user should be familiar with network structures, terms, and concepts.

Organization

This guide contains the following sections:

Chapter 1, "Overview," describes the major features of location servers that you can configure using Cisco WCS.

Chapter 2, "Adding and Deleting Location Servers," describes how to add and delete location servers.

Chapter 3, "Synchronizing Location Servers with Cisco Wireless LAN Controllers and Cisco WCS," describes how to synchronize Cisco WCS and locations servers.

Chapter 4, "Configuring and Viewing System Properties," describes how to configure location server properties.

Chapter 5, "Managing Location Server Users and Groups," describes how to configure and manage users, groups, and hot access.

Chapter 6, "Configuring Event Notifications," describes how to define events and event groups, and how to configure event notification parameters. It also describes how to view event notification summaries.

Chapter 7, "Location Planning and Verification," describes how to monitor locations servers by configuring and viewing alarms, events, and logs. It also describes how to view location server, client, and asset tag status. Achieving optimum AP placement and coverage is also addressed.

Chapter 8, "Monitoring Location Servers and Site," describes how to back up and restore location server data and how to update the location server software. It also describes other maintenance operations.

Chapter 9, "Performing Maintenance Operations," describes how to back up and restore location server data and how to update the location server software. It also describes other maintenance operations.

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

For more information about location appliances and related products, refer to the *Cisco Wireless Location Appliance Getting Started Guide*, which describes how to set up location appliances. This document is available on the Cisco.com website at the following URL:

http://www.cisco.com/en/US/products/ps6386/prod_installation_guides_list.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.

Overview

This chapter describes the role of the location appliance within the Cisco Unified Wireless Network and its overall functionality.

This chapter contains the following sections:

- "Location Appliance Functionality" section on page 1-2
- "Viewing Location Data" section on page 1-3
- "Event Notification" section on page 1-3
- "Configuration and Administration" section on page 1-4
- "Location Server Synchronization" section on page 1-5
- "Location Planning and Verification" section on page 1-5
- "Monitoring Capability" section on page 1-5
- "Maintenance Operations" section on page 1-5
- "System Compatibility" section on page 1-6

Location Appliance Functionality

The Cisco Wireless Location Appliance is a component of the Cisco Unified Wireless Network (CUWN).

The location appliance uses Cisco wireless LAN controllers and Cisco Aironet lightweight access points to simultaneously track the physical location of up to 2,500 802.11 wireless devices. For those areas requiring very high fidelity and deterministic location, chokepoint-based notifications are supported for Cisco Compatible Extensions Wi-Fi tags.

Figure 1-1 illustrates the relationship of the location appliance with other components of the CUWN.

Figure 1-1   ***Cisco Unified Wireless Network***
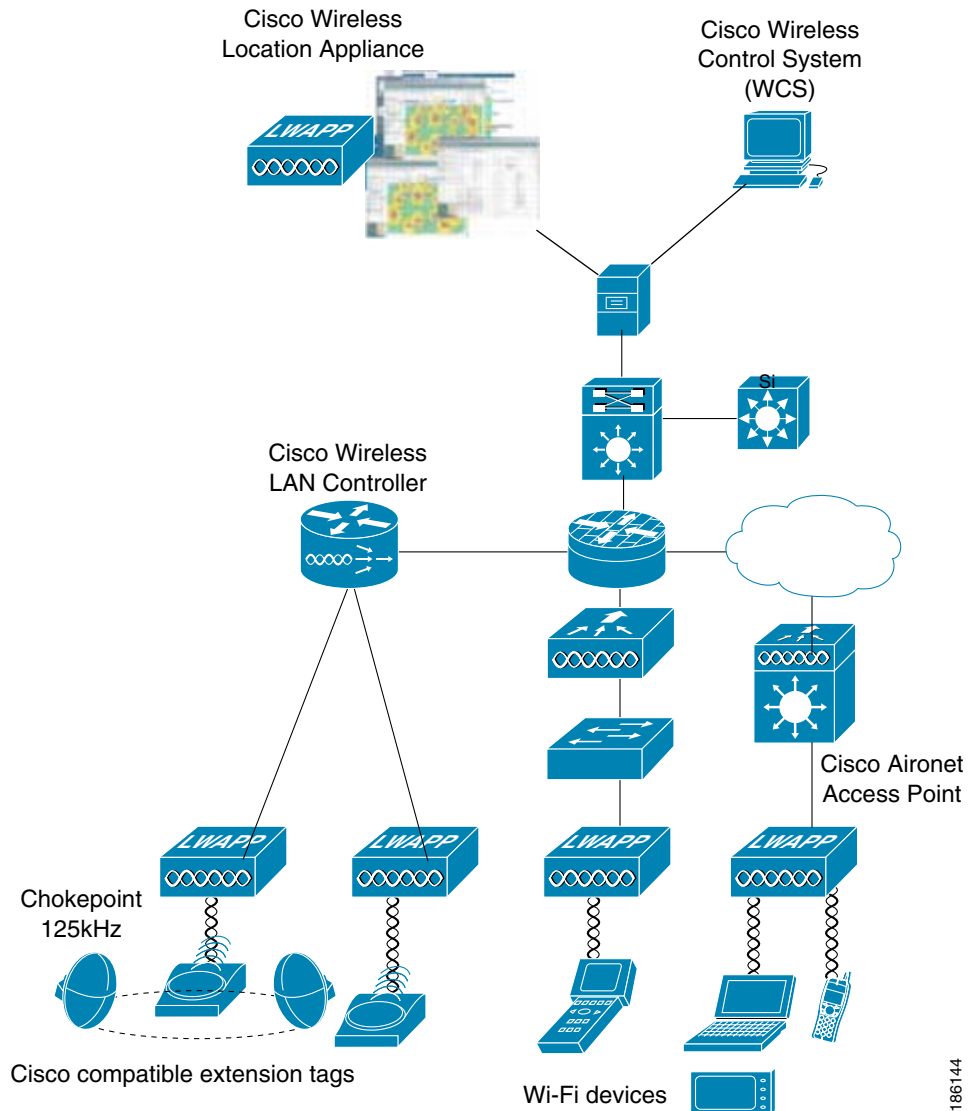
Viewing Location Data

The collected location data 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 location server is required using a command-line (CLI) console session. Details are described in the *Cisco Wireless Location Appliance Getting Started Guide* at:
http://www.cisco.com/en/US/products/ps6386/prod_installation_guides_list.html.

After its installation and initial configuration is complete, the location server communicates with the Cisco wireless LAN controller to which it was assigned to collect operator-defined location data. You can then use the associated Cisco WCS server to communicate with each location server to transfer and display selected data.

You can configure location appliances to collect data for Cisco Wireless LAN Solution clients, rogue access points, rogue clients, mobile stations, and RFID asset tags at separate intervals. The interval frequency is a user-configurable setting.

Event Notification

Location servers provide the functionality for sending 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 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 servers. (Figure 1-2).

Figure 1-2   *Pull Communication Model*
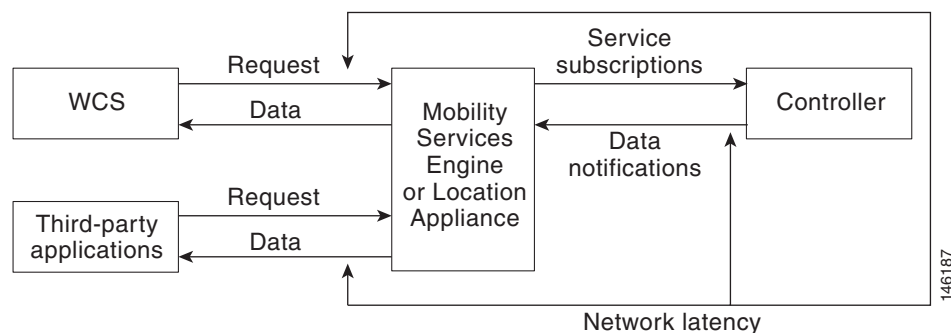
The pull communication model, however, is not suitable for applications that require more real-time updates to location information. For these applications, you can configure location servers to send event notifications (push) when certain conditions are met by the registered listeners.

Configuration and Administration

You can use Cisco WCS to perform different configuration and administrative tasks, including adding and removing location servers, configuring location server properties, and managing users and groups as summarized below.

Adding and Deleting Location Servers

You can use Cisco WCS to add and delete location servers within the network. Refer to Chapter 2, "Adding and Deleting Location Servers" for configuration details.

Editing Location Server Properties

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

- General Properties: Enables you to assign a contact name, user name, password and HTTPS for the location appliance.

- Tracking Parameters: Enables you define which element locations you want to actively track (client stations, active asset tags; and rogue clients and access points), set limits on how many of a specific element 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 and elements 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 an element by the "probed" controller as well as its primary controller.

- History Parameters: Enables you to specify how often the location appliance collects historical data on client station, rogue access point, and asset tags from controllers to manage the amount of data stored on the location appliance hard drive.

- 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.

- Location Parameters: Enables you to specify whether the location server retains its calculation times and how soon the location server deletes its collected RSSI measurement times. It also enables you to apply varying smoothing rates to manage location movement of an element.

- 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 location server and the controller. Transport of telemetry, emergency, and chokepoint information between the location server and the controller is managed by this protocol.

Managing Location Server 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 Location Server Users and Groups" for configuration details.

Location Server Synchronization

To maintain accurate location information, you can use Cisco WCS to configure location servers so that they are synchronized with network design, event group, and controller elements. Cisco WCS provides you with two ways to synchronize these elements and locations servers: manual and automatic (auto-sync). Additionally, you need to set the time zone for the associated controller to ensure continued synchronization. Refer to Chapter 3, "Synchronizing Location Servers with Cisco Wireless LAN Controllers and Cisco WCS"for specifics.

Location Planning and Verification

To plan and optimize access point deployment, you can use Cisco WCS to use either apply location readiness or calibration to examine location quality. Additionally, you can analyze the location accuracy of non-rogue and rogue clients and asset tags using testpoints on an area or floor map; and, use chokepoints to enhance location accuracy for tags.

To further refine location calculation, you can define those areas which should be included in location calculations (inclusion regions) and those areas that should not be included (exclusion regions). Rail areas which represent conveyors within a building can also be defined. Refer to Chapter 7, "Location Planning and Verification" for specifics.

Monitoring Capability

You can use Cisco WCS to monitor alarms, events and logs generated by location servers. You can also monitor the status of location servers, clients, and tagged asset status. Additionally, you can generate a location server utilization report to determine CPU and memory utilization as well as counts for clients, tags, and rogue elements (access points and clients). Refer to Chapter 8, "Monitoring Location Servers and Site"for specifics.

Maintenance Operations

You can use Cisco WCS to import and export asset location information, recover a password, back up the location server to a predefined FTP folder on any Cisco WCS server at defined intervals, and restore the location server data from that Cisco WCS Server. Other location server maintenance operations that you can perform include downloading new application code to all associated location server from any Cisco WCS server, a defragment the Cisco WCS database, restarting location servers, shutting down location servers, and clearing location server configurations. Refer to Chapter 9, "Performing Maintenance Operations" for specifics.

System Compatibility

> **Note** Refer to the location appliance release notes for the latest system (controller, WCS, location appliance) compatibility information, feature support and operational notes for your current release at:
> http://www.cisco.com/en/US/products/ps6386/prod_release_notes_list.html

Backwards Compatibility of Location Server Software

Location server software is backwards compatible with the previous two location server releases. Therefore, you can only upgrade two releases forward. For example, you can directly upgrade from release 3.1 to 5.2 but you cannot directly upgrade to release 5.2 from releases 1.1, 1.2, 2.0, 2.1 or 3.0.

> **Note** There is no release 3.2 or 5.0 for location appliances.

C H A P T E R 2

Adding and Deleting Location Servers

This chapter describes how to add and delete location servers.

This chapter contains the following sections:

Adding a Location Appliance to Cisco WCS

To add a location server to Cisco WCS, log into WCS and follow these steps:

Step 1 Verify that you can ping the location server that you want to add from the Cisco WCS server.

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

Step 3 From the Select a command drop-down menu (right-hand side), choose **Add Location Server** and click **GO**.

Step 4 In the Device Name field, enter a name for the location server.

Step 5 In the IP Address field, enter the location server's IP address.

Step 6 (Optional) In the Contact Name field, enter the name of the location server administrator.

Step 7 In the User Name and Password fields, enter the username and password for the location server.

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 run the automatic installation script and change the username and password.

Step 8 In the Port field, enter the port number used by the location server.

The default port is 8001.

Step 9 Check the Enable check box to enable HTTPS. Uncheck the check box to disable HTTPS.

HTTPS is disabled by default.

Step 10 Click **Save**.

Cisco WCS searches for the location server and adds it to the Cisco WCS database.

Step 11 Go back to the Mobility Services window and click **Refresh** (top right). Verify that the location server that you have just added appears in the window.

> **Note** Cisco WCS does not allow you to add a location server that already exists in the WCS database.

> **Note** After adding a new location server, you can synchronize network designs (campus, building, and outdoor maps) and event groups on the local location server with Cisco WCS. You can also choose to synchronize the location server with a specific controller, You can do this synchronization immediately after adding a new system or at a later time. To synchronize the local and Cisco WCS databases, continue to "Viewing Synchronization Information" section on page 3-6.

Deleting Location Servers from the Cisco WCS Database

To delete location servers from the Cisco WCS database, follow these steps:

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

Step 2   Select the server or servers to be deleted by checking the corresponding check box(es).

Step 3   From the Select a command drop-down menu (right-hand side), choose **Delete Service(s)** and click **GO**.

Step 4   Click **OK** to confirm that you want to delete the selected location server from the Cisco WCS database.

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

C H A P T E R 3

Synchronizing Location Servers with Cisco Wireless LAN Controllers and Cisco WCS

This chapter describes how to synchronize Cisco wireless LAN controllers and Cisco WCS with locations servers.

This chapter contains the following sections:

- "Keeping Location Servers Synchronized" section on page 3-2
- "Viewing Synchronization Information" section on page 3-6

Keeping Location Servers Synchronized

This section describes how to synchronize controllers, WCS and location servers manually and automatically.

Before a location server can collect any data, you must do two things:

1. Associate the server with a controller and synchronize them using Cisco WCS. Refer to the "Associating a Location Server with a Controller" section on page 3-2.

2. Verify that the timezone is set on the associated controller. Refer to the "Setting and Verifying Timezone on a Controller" section on page 3-3.

> **Note**   Be sure to verify software compatibility between the controller, Cisco WCS and the location server before synchronizing. Refer to the latest location server release note at the following link: http://www.cisco.com/en/US/products/ps6386/prod_release_notes_list.html

> **Note**   Communication between the location server and Cisco WCS and the controller is in universal time code (UTC). Configuring NTP on each system provides devices with the UTC time. The location server 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 location server.

Associating a Location Server with a Controller

Before a location server can collect any data, you must associate the server with a controller and synchronize them using Cisco WCS. After the initial synchronization, you can resynchronize the controllers and location servers at any time.

> **Note**   Controller names must be unique for synchronizing with location servers. If you have two controllers with the same name, only one will be synchronized.

To associate and synchronize a location server and a controller, follow these steps:

Step 1   Click **Mobility > Synchronize Services** to display the Synchronize Cisco WCS and Server(s) window.

Step 2   Select the **Controllers** tab.

Cisco WCS displays a list of possible controllers.

Step 3   To associate a location server with a controller, click the corresponding **Assign** link of that server.

Step 4   In the controllers dialog box that appears, check the check box of each controller that you want the location server to be associated. Click **OK** when selection is complete.

A red asterisk (*) appears next to the Assign link. To undo assignments, click **Reset**. To go back to the Mobility Services window without making any changes, click **Cancel**.

When the Cisco WCS and location server databases are synchronized, a green two-arrow icon appears in the Sync. Status column of every synchronized controller entry.

> **Note**   To disassociate a controller from a location server, click the Assign link next to the location
> server. In the controllers dialog box that appears, uncheck the appropriate check box for each
> controller. Click OK and then click **Synchronize**.

Setting and Verifying Timezone on a Controller

For controller releases 4.2 and greater, if a location server (release 3.1 or greater) is installed in your
network, it is mandatory that the time zone be set on the controller to ensure proper synchronization
between the two systems; and, a highly recommended setting in networks that do not have location
servers.

Universal Time Code (UTC) is used as the standard for setting the system time zone for the controller.

You can automatically set the time zone during initial system setup of the controller or manually set it
on a controller already installed in your network.

Follow these steps to manually set the time and time zone on an existing controller in your network using
the CLI:

Step 1   Configure the current local time in UTC on the controller by entering the following commands.

```
(Cisco Controller) >config time manual 09/07/07 16:00:00
(Cisco Controller) >config end
```

> **Note**   When setting the time, the current local time is entered in terms of UTC and as a value between
> 00:00 and 24:00. For example, if it is 8 AM Pacific Standard Time (PST) in the US, you enter
> 16:00 (4 PM PST) as the PST time zone is 8 hours behind UTC.

Step 2   Verify that the current local time is set in terms of UTC by entering the following command.

```
(Cisco Controller) >show time
Time......................................... Fri Sep 7 16:00:02 2007
Timezone delta................................... 0:0
```

Step 3   Set the local time zone for the system by entering the following commands.

> **Note**   When setting the time zone, you enter the time difference of the local current time zone with
> respect to UTC (+/-). For example, Pacific Standard Time (PST) in the United States (US) is 8
> hours behind UTC time. Therefore, it is entered as -8.

```
(Cisco Controller) >config time timezone -8
(Cisco Controller) >config end
```

Step 4   Verify that the controller displays the current local time with respect to the local time zone rather than
in UTC by entering the following command.

```
(Cisco Controller) >show time
Time......................................... Fri Sep 7 08:00:26 2007
Timezone delta................................... -8:0
```

> **Note** The time zone delta parameter in the **show time** command displays the difference in time between the local time zone and UTC (8 hours). Prior to configuration, the parameter setting is 0.0.

Synchronizing Cisco WCS and Location Servers

After adding a location server to Cisco WCS, you add network designs (campus, building, and outdoor maps), event groups or controller information (name and IP address) to the location server.

After the network designs are stored in the Cisco WCS and location server databases, you can re-synchronize the two databases at any time.

To synchronize Cisco WCS network designs with the location server, follow these steps:

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

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

    a.   To assign a network design to a location server, click its corresponding **Assign** link.

> **Note** A network design might comprise a large campus with several buildings, each monitored by a different location server. Therefore, you might need to assign a single network design to multiple location servers.

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

    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**.

    b.   To associate a location server with a controller, click the **Assign** link for that location server.

    In the Controllers panel that appears, check the check box next to each controller to which you want the location server associated. Click **OK**.

> **Note** Controller names must be unique for synchronizing with a location server. 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 location server, 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 location server. 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**.

Step 3   Click **Synchronize** to update the Cisco WCS and location server databases.

When the Cisco WCS and location server databases are synchronized, a green two-arrow icon appears in the Sync. Status column for each synchronized network design entry.

> **Note**   To unassign a network design from a location server, uncheck the server's check box in the Assign to servers dialog box and click **OK**. Then, click **Synchronize**. A two-arrow icon with a red circle appears in the Sync. Status column.

Configuring Automatic Location Service Database Synchronization

Manual synchronization of WCS and location server 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 WCS and location service databases is triggered periodically and any related alarms are cleared.

To configure automatic synchronization, follow these steps:

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

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

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

Step 4   To set the location server to send out-of-sync alerts, check the Out of Sync Alerts **Enabled** check box.

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

> **Note**   Automatic synchronization does not apply to elements (network designs, controllers, or event groups) that have not yet been assigned to a location server. However, out-of-sync alarms will still be generated for these unassigned elements. For automatic synchronization to apply to these elements, you need to manually assign them to a location server.

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**.

Out-of-Sync Alarms

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

- Elements have been modified in Cisco WCS (the auto-sync policy will push these elements)
- Elements have been modified in location servers (the auto-sync policy will pull these elements)
- Elements other than controllers exist in the location server but not in Cisco WCS (the auto-sync policy will pull these elements)

- Elements have not been assigned to any location server (the auto-sync policy doesn't apply)

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

- Location server is deleted

> **Note** When you delete a location server, the out-of-sync alarms for that server are also deleted. In addition, if you delete the last available location server, the following alarm, *Elements not assigned to any location server* is also 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)

> **Note** By default, out-of-sync alarms are enabled. You can disable them in Cisco WCS by choosing **Administration > Scheduled Tasks**, clicking the **Mobility Service Synchronization** link, unchecking the **Auto Synchronization** check box, and clicking **Submit**.

Viewing Synchronization Information

This section describes how to view location service synchronization status and history.

Viewing Location Service 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 location servers.

To view synchronization status, follow these steps:

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

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

Depending on the command you have chosen, Cisco WCS displays a list of elements (network designs, controllers, or event groups). In the list, the Sync. Status column shows the synchronization status. A green two-arrow icon indicates that its corresponding element is synchronized with the specified location server. A gray two-arrow icon with a red circle indicates that its corresponding item is not synchronized with the location server.

Viewing Location Service Synchronization History

You can view the location service synchronization history for the last 30 days. 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, click **Mobility > Synchronization History**

Step 2   Click the column headers to sort the entries.

In the Synchronization History window, the Sync Direction column indicates whether information is pushed to the location server or pulled by the location server. The Generated By column indicates whether the synchronization was manual or automatic.

C H A P T E R 4

Configuring and Viewing System Properties

This chapter describes how to configure and view system properties on the location server.

This chapter contains the following sections:

Configuring General Properties

You can use Cisco WCS to edit the general properties of a location server such as contact name, user name, password, and HTTPS.

To edit the general properties of a location server, 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 location server 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 location server.
User Name	Enter the login user name for the Cisco WCS server that manages the location server.
Password	Enter the login password for the Cisco WCS server that manages the location server.
Port	8001
HTTPS	Enable this check box to communicate with Cisco WCS.

Step 4   Click **Save** to update the Cisco WCS and location server databases.

.

Modifying NMSP Parameters

Network Mobility Services Protocol (NMSP) is the protocol that manages communication between the location server and the controller. Transport of telemetry, emergency, and chokepoint information between the location server 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 location server communicate over MUST be open (not blocked) on any farewell that exists between the controller and location server 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 location server 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 location server 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 location server 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 location server 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.
Retransmit Interval	Interval of time that the location server 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 location server databases.

Viewing Active Sessions on a System

You can view active user sessions on the location server.

For every session, Cisco WCS displays the following information:

- Session identifier
- IP address from which the location server is accessed
- Surname of the connected user

- Date and time when the session started

- Date and time when the location server 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 location server on which you want to view active sessions.

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

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 location server, and configure monitoring parameters.

- Refer to the"Viewing Advanced Parameters Settings" section on page 4-4 to review current system level settings of the advanced parameters.

- Refer to the "Configuring Advanced Parameters" section on page 4-5 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 4-6 for information on these commands and when they should be used

Viewing Advanced Parameters Settings

To view the advanced parameter settings of the location server, follow these steps:

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

Step 2   Click the name of a location server 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 4-5.

- 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 4-6.

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 location server that you want to configure.

Step 3   From the System menu (left panel) click **Advanced Parameters**. The advanced parameters for the selected location server 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 location server that you want to configure.

Step 3   From the System menu (left panel) click **Advanced Parameters**. The advanced parameters for the selected location server appears.

Step 4   Scroll down to the Advanced Parameters section 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 location server, follow these steps:

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

Step 2   Click the name of a location server 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 location server, follow these steps:

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

Step 2   Click the name of a location server 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 location server, follow these steps:

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

Step 2   Click the name of a location server 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 Location Server Users and Groups

This chapter describes how to configure and manage users, groups, and host access.

This chapter contains the following sections:

- "Managing Groups" section on page 5-2
- "Managing Users" section on page 5-3
- "Managing Host Access" section on page 5-5

Cisco Location Appliance Configuration Guide

OL-18503-01

5-1

Managing Groups

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

Adding User Groups

To add a user group to a location server, follow these steps:

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

Step 2   Click the name of the location server you want to edit.

Step 3   Click **Accounts** (left panel) to display the menu options.

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 choose from:

- Read Access

- Write Access

- Full Access (required for Cisco WCS to access location servers)

Step 8   Click **Save** to add the new group to the location server.

⚠
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 location server settings.

Deleting User Groups

To delete user groups from a location servers, follow these steps:

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

Step 2   Click the name of the location server you want to edit.

Step 3   Click **Accounts** (left panel) to display the menu options.

Step 4   Click **Groups**.

Step 5   Check the check box(es) of the group(s) 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 group(s).

Changing User Group Name, Password or Permission

To change user group permissions, follow these steps:

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

Step 2   Click the name of the location server you want to edit.

Step 3   Click **Accounts** (left panel) to display the menu options.

Step 4   Click **Groups**.

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

Step 6   Modify the group name, password or permission (access) level as appropriate.

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

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

Managing Users

This section describes how to add, delete, and edit users to location servers. It also describes how to view active user sessions.

Adding Users

To add a users to a location server, follow these steps:

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

Step 2   Click the name of the location server you want to edit.

Step 3   Click **Accounts** (left panel) to display the menu options.

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 choose from: Read Access, Write Access, and Full Access (required for Cisco WCS to access location servers).

⚠️

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

Step 10   Click **Save** to add the new user to the location server.

Deleting Users

To delete a user from a location server, follow these steps:

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

Step 2   Click the name of the location server you want to edit.

Step 3   Click **Accounts** (left panel) to display the menu options.

Step 4   Click **Users**.

Step 5   Check the check box(e)s of the user(s) 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 location server you want to edit.

Step 3   Click **Accounts** (left panel) to display the menu options.

Step 4   Click **Users**.

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

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

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

Viewing Active User Sessions

To view active user sessions, follow these steps:

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

Step 2   Click the name of the location server you want to edit.

Step 3   Click **System** (left panel) to display configuration options.

Step 4   Click **Active Sessions**.

Cisco WCS displays a list of active location server sessions. For every session, Cisco WCS displays the following information:

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

Managing Host Access

This section describes how to add, delete, and edit host access records.

Adding Host Access

You can use Cisco WCS to add host access records to the location server database. Using host access records, you can control which hosts have access to the location server and when. You can also control access preference by assigning priorities to host access.

To add a new host access record, follow these steps:

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

Step 2   Click the name of the location server you want to edit.

Step 3   Click **Accounts** (left panel) to display configuration options.

Step 4   Click **Host Access**.

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

Step 6   Enter the IP address and netmask of the host using the *ddd.ddd.ddd.ddd/dd* format.

Following are examples of IP address and netmask entries:

IP Address/Netmask	Description
120.10.0.0/8	Specifies hosts on a class A subnet (120.x.x.x).
120.10.0.0/16	Specifies hosts on a class B subnet (120.10.x.x).
120.10.223.0/16	Specifies hosts on a class C subnet (120.10.223.x).
120.10.223.10/32	Specifies one host (120.10.223.10).

Step 7   To allow host access, check the **Enable** check box of the Permit field.

To deny host access, do not check the **Enable** check box.

Step 8   Enter a priority number from 0 to 99999 in the Priority field.

Hosts with high priority have access preference over hosts with low priority.

Step 9   Enter the time of day when the host may access the location server in the Start Access fields.

In the Hrs. field, enter a value from 0 to 23. In the Mins. field, enter a value from 0 to 59.

Step 10   Enter the time of day when host access ends in the End Access fields.

In the Hrs. field, enter a value from 0 to 23. In the Mins. field, enter a value from 0 to 59.

Step 11   Click **Save** to add the new host access to the location server.

Deleting Host Access Records

To delete a host access record, follow these steps:

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

Step 2   Click the name of the location server you want to edit.

Step 3   Click **Accounts** (left panel) to display configuration options.

Step 4   Click **Host Access**.

Step 5   Check the check box(es) of the host access record(s) that you want to delete.

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

Step 7   Click **OK** to confirm that you want to delete the selected host access records.

Editing Host Access Records

To edit a host access record, follow these steps:

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

Step 2   Click the name of the location server you want to edit.

Step 3   Click **Accounts** (left panel) to display configuration options.

Step 4   Click **Host Access**.

Step 5   Click the IP and mask address of the host access record that you want to modify.

Step 6   Make the required changes to the Permit, Priority, Start Access, and End Access fields.

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

C H A P T E R 6

Configuring Event Notifications

Event notification is a feature that enables you to define conditions that cause the location server 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 configure event notification parameters. It also describes how to view event notification summaries.

This chapter contains the following sections:

Working with Event Groups

This section describes how to add and delete event groups.

Adding Event Groups

To manage events more efficiently, you can use Cisco WCS to create event groups. Event groups help you organize your event definitions.

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**.

Working with 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 destinations. 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. Any new 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 settings summary window appears for the specific event group listing all defined event definitions.

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

Step 5   Enter a name for the event definition and click **Save**.

Step 6   At the Conditions tab, add one or more conditions. For each condition you add, specify the rules for triggering an event notification.

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 location server generates a missing asset event if the location server 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 Chang**e 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, unknown) that will trigger an event. Proceed to Step c.

If you chose **Chokepoint** from the Condition Type drop-down menu. There is only one trigger condition and it is displayed by default. No configuration is required. Proceed to Step c.

> **Note**   For chokepoints you must select the chokepoint after you add the condition. See directions in the note after sub-step e.

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 tags (Cisco CX v.1 compliant).

d. From the Match By drop-down menu, choose the matching criteria (MAC Address, Asset Name, Asset Group, or Asset Category), 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 7   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 New**.

b. 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 a destination.

c. 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.

d. In the Message Format field, select **XML** or **Plain Text** to specify the message format.

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

e. 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.

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

g. **Port Number** auto-populates when HTTPS is enabled.

h. Click **Add**.

Step 8 Under the General tab, follow these steps:

a. Enable event generation (disabled by default) by checking the **Enabled** check box for the Admin Status field.

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. Select the day(s) of the week you want to activate event notification by checking the box next to the day(s).

> **Note** If you want to continuously report events, select the **All the Time** option. In this case, there is no need to set start and end ranges for event notification. These options are not displayed.

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

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

          f. Click **Save**.

Step 9   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, click **Mobility > Notifications**.

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

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

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).

> **Note**   Deleting event definitions as described above only removes them from the WCS database. You must also remove the definitions from the location server database.

To remove definitions from the location server, follow these steps:

Step 1   In Cisco WCS, click **Mobility > Synchronize Servers**.

Step 2   From the **Synchronize** drop-down menu, select **Event Groups**.

Step 3   To remove an event definition, click **Unassign** for the event group to which the event belongs.

> **Note**   The Unassign link only appears if the event group is linked. When a group is already unassigned, the assign link appears next to the event group.

Step 4   Click **Synchronize**.

Testing Event Definitions

To verify that the location server is sending event definitions over the transport protocol you have specified in the event definition, use Cisco WCS to test the event notifications. The location server 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, click **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, select **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 location server 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 location server generates absence events when the monitored assets go missing. In other words, the location server cannot detect the asset in the WLAN for the specified time.

- In/Out Area (Containment)—The location server 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 location server generates movement events when an asset is moved beyond a specified distance from a designated marker you define on a map.

- Location Changes—The location server generates location change events when client stations, asset tags, rogue clients and rogue access points move from their previous location.

- Battery Level—The location server generates battery level events for all tracked asset tags.

- Emergency—The location server generates an emergency event for a CCX 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 CCX v.1 compliant tags.

- Chokepoint Notifications—The location server generates an event when a tag is seen (stimulated) by a chokepoint. This information is only reported and displayed for CCX 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, click **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 compatible 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 location server 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.

Configuring Notification Parameters

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

> **Note** Modify notification parameters only if you expect the location server 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 location server 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, click **Mobility > Mobility Services**.

Step 2   Click the name of the location server you want to configure.

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

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 to send.

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 Location Server" 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.

The notification parameters and their definitions are listed in Table 6-1.

Table 6-1   Notification Parameters:

Parameter	Description
Rate Limit	Enter the rate in milliseconds at which the location server will generate notifications. A value of 0 (default) means that the server will generate event notifications as fast as possible.
Queue Limit	The event queue limit for sending notifications. The server 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 location server generated will eventually reach WCS. Default value is 1. **Note** The location server 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 location server sends an event notification. Then, until the event is cleared, the location server 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 location server databases.

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 Location Server 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 by location based services.

Notification Formats in Text

When you specify that notification be sent in Text format, the location server 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. WCS receives the notifications from location servers in the form of the trap `locationNotifyTrap` as part of the MIB file bsnwras.my. The location server stores the content of the notification message in XML format in the variable `locationNotifyContent` (see "Notification Formats in XML" section on page 6-10).

```
locationNotifyTrap  NOTIFICATION-TYPE
    OBJECTS { locationNotifyContent}
    STATUS current
    DESCRIPTION
        "This trap will be generated by the location server
        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 }
```

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
  ```

C H A P T E R 7

Location Planning and Verification

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

You can plan for new access point deployment based on applications employed.

You can check the ability of an existing access point deployment to estimate the true location of an element within 10 meters at least 90% of the time using a location readiness calculation based on the number and placement of access points.

You can use calibration data to examine location quality, as an alternative to using the location readiness calculation.

You can analyze the location accuracy of non-rogue and rogue clients and asset tags using testpoints on an area or floor map; or use chokepoints to enhance location accuracy for tags.

Additionally, you can specify areas to include or exclude in location calculations.

This chapter contains the following sections:

Deployment Planning for Data, Voice, and Location

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 from the list that displays.

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

Step 3   Select **Planning Mode** from the Select a command menu. Click **GO.**

Step 4   In the window that appears, click **Add AP**. A window appears with an access point entry panel (left) and map (right).

Step 5   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   In the access point entry panel on the left, check the check box next to the service (applications) 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 displays in the panel.

> **Note**   Each service option is inclusive of all services that are listed above it. For example, if you check the Location 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** to generate a map based on the recommendations to see recommended placement of the access points 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 radio frequency (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.

The calibration models are used as RF overlays with measured RF signal characteristics that can be applied to different floor areas. This enables the Cisco WLAN solution installation team to lay out one floor in a multi-floor area, use the RF calibration tool to measure, save the RF characteristics of that floor as a new calibration model, and apply that calibration model to all the other floors with the same physical layout.

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   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 the WCS server and perform the calibration process.

To create and apply calibration models, follow these steps:

Step 1   Click **Monitor > Maps** and choose **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 and click **GO**.

Step 3   Assign a name to the model and click **OK**. The new model name appears along with the other RF calibration models in the window that appears, but its status is listed as Not Yet Calibrated.

Step 4   To start the calibration process, click on the hyperlink associated with the new model name in the RF calibration model window.

Step 5   In the window that appears, which indicates the details of the new model, choose **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
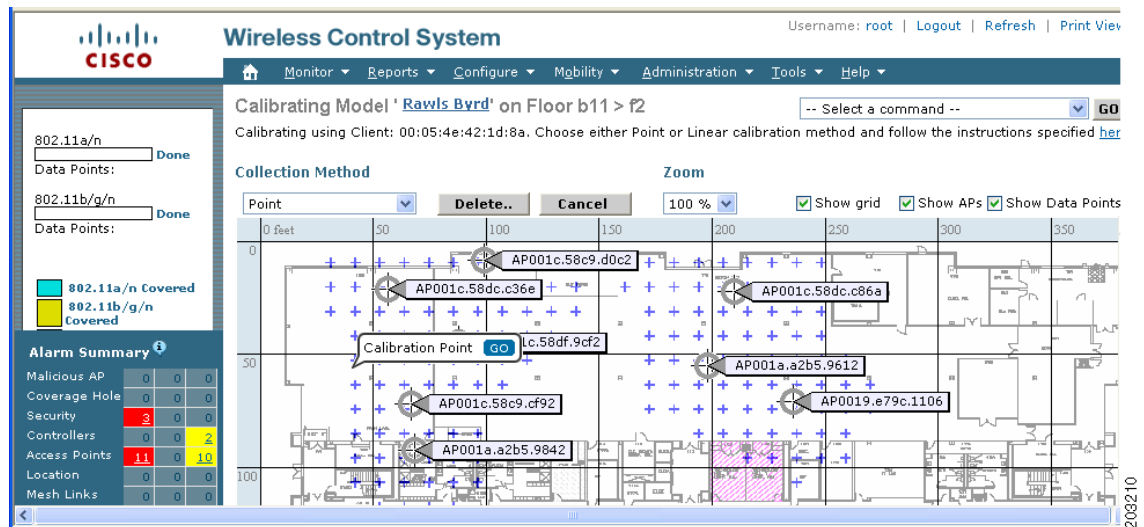
a.   If you want to do a point collection of data for the calibration, do the following:

    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 the 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 elements (access points, clients, tags) and their relative signal strength (RSSI).

Note   If RSSI is not displayed, you can enable AP Heatmaps under the Layer menu (top-left).

Step 3   Select **Inspect Location Readiness** from the Select a command menu. 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 Models** from the 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 using the location accuracy tool:

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

- On demand Accuracy Testing–Employed when elements are associated but not pre-positioned. On demand testing allows you to test the location accuracy of clients 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 Accuracy Tool does not appear as an option under the Tools menu when the Advanced Debug option is not enabled.

Follow these steps to enable the advanced debug option in Cisco WCS.

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

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

Step 3 Select Enabled from the Advanced Debug Mode 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 either scheduled or on-demand location accuracy tests on the location appliance using the Location Accuracy Tool.

Using Scheduled Accuracy Testing to Verify Accuracy of Current Location

To configure a scheduled accuracy test, do the following:

Step 1   In Cisco WCS, click **Tools > Location Accuracy Tool**.

Step 2   Select New Scheduled Accuracy Test from the Select a command drop-down menu. Click **GO**.

Step 3   In the window that appears, 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   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.

As you check a MAC address check box, two icons which overlay each other appear on the map.

One icon represents the actual location (shaded icon) and the other the reported (solid icon) location. Key for actual and reported icons are shown at the top of the floor map.

> **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 location server 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, do the following:

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 WCS Database and Map

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 the WCS database and appropriate map, 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 (Figure 7-4). 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
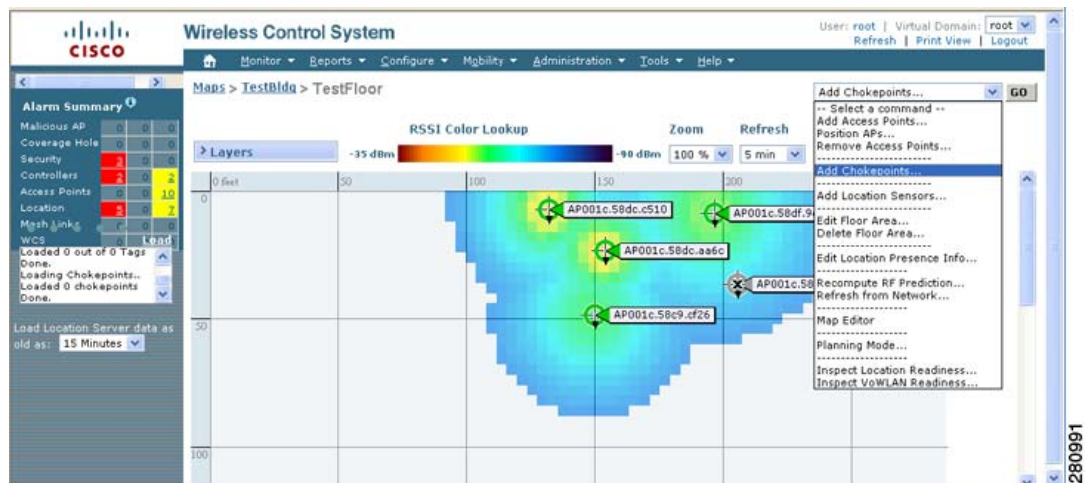
Step 8   Select **Add Chokepoints** from the Select a command menu. Click **GO**.

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**.

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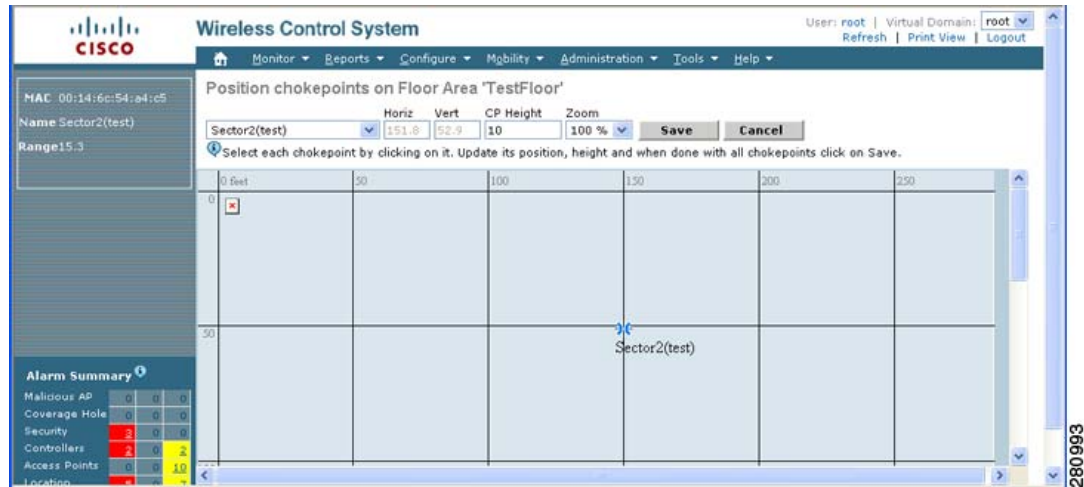
> **Note**   The MAC address, name, and coverage range of the chokepoint appear in the left panel when you click on the chokepoint icon for placement.

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 12.

Figure 7-10   New Chokepoint Displayed on Floor Map
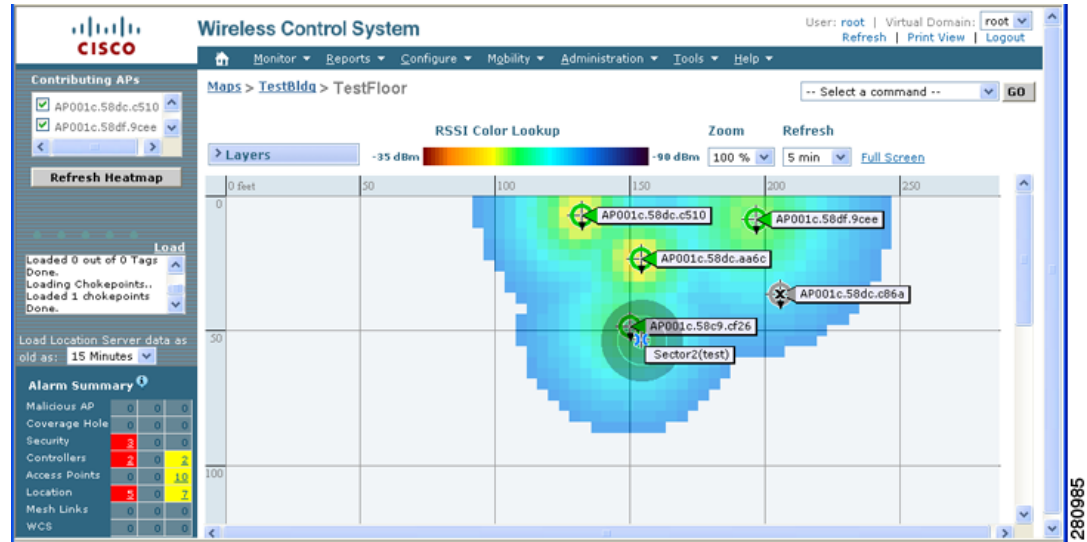
![Note]

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]

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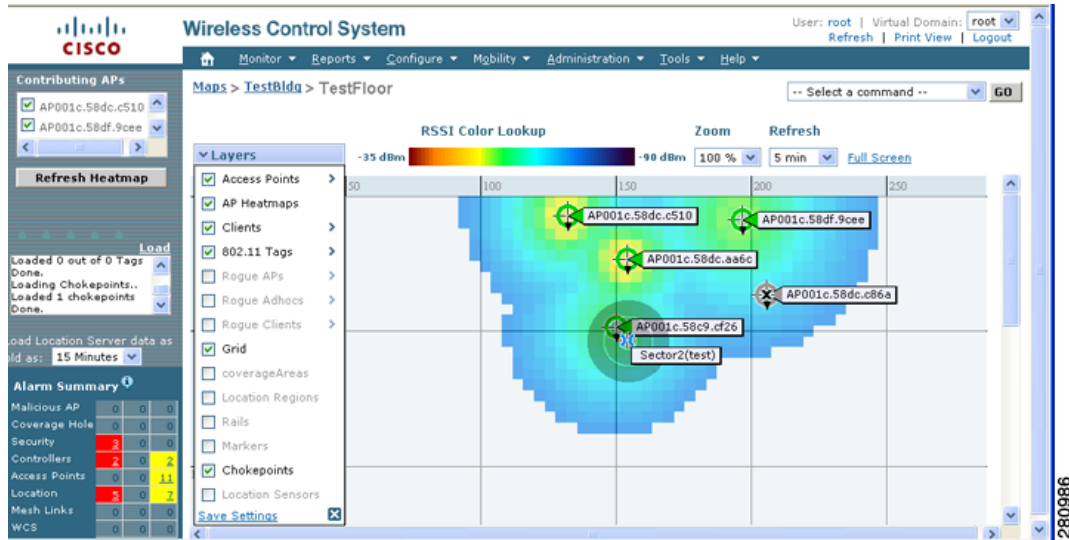
Step 13   Click **X** to close the Layers window.

✎

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.

Follow these steps to delete a chokepoint.

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 location appliance 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 location appliance active in the network.

   Refer to Chapter 2, "Adding and Deleting Systems" for details on adding a location appliance.

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

   Refer to for details on adding the TDOA receiver to Cisco WCS.

3. Synchronize Cisco WCS and location appliance.

   Refer to Chapter 3, "Synchronizing Location Servers with Cisco Wireless LAN Controllers and Cisco WCS" 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
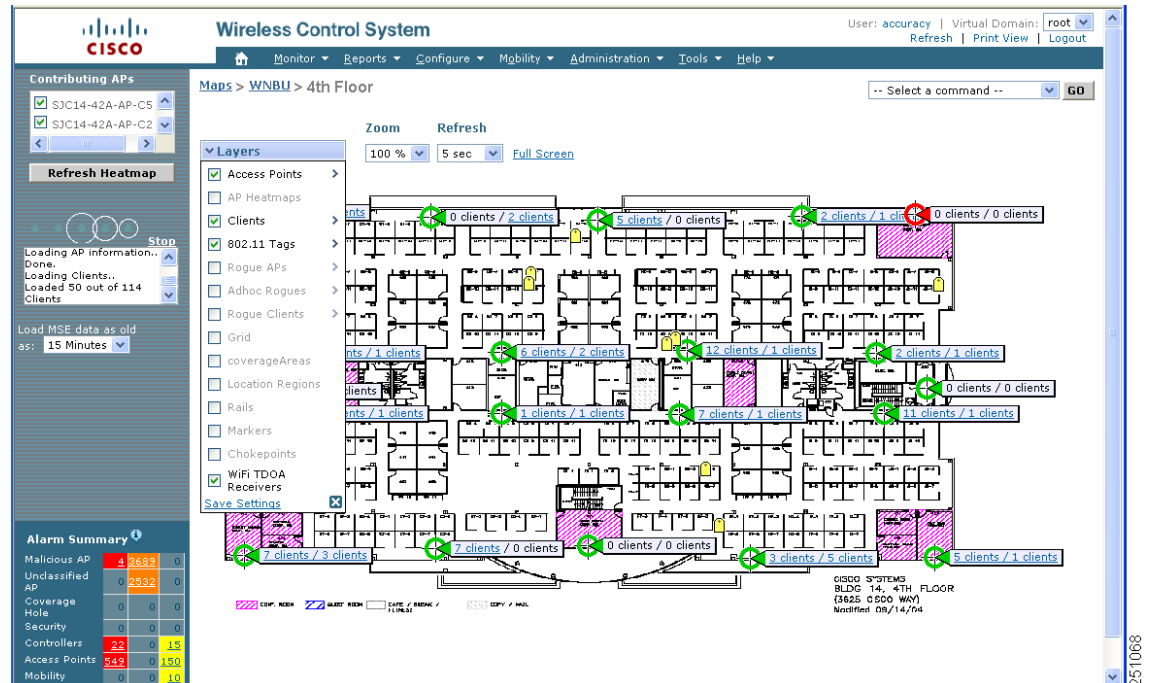
Step 14   Click **X** to close the Layers window.

> **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 LOMM 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 5.2.

Follow the steps below to set enable TOMM and assign monitoring channels on the access point radio.

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

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 display 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 location server recalculates location.

Defining an Inclusion Region on a Floor

Follow the steps below to define an inclusion area.

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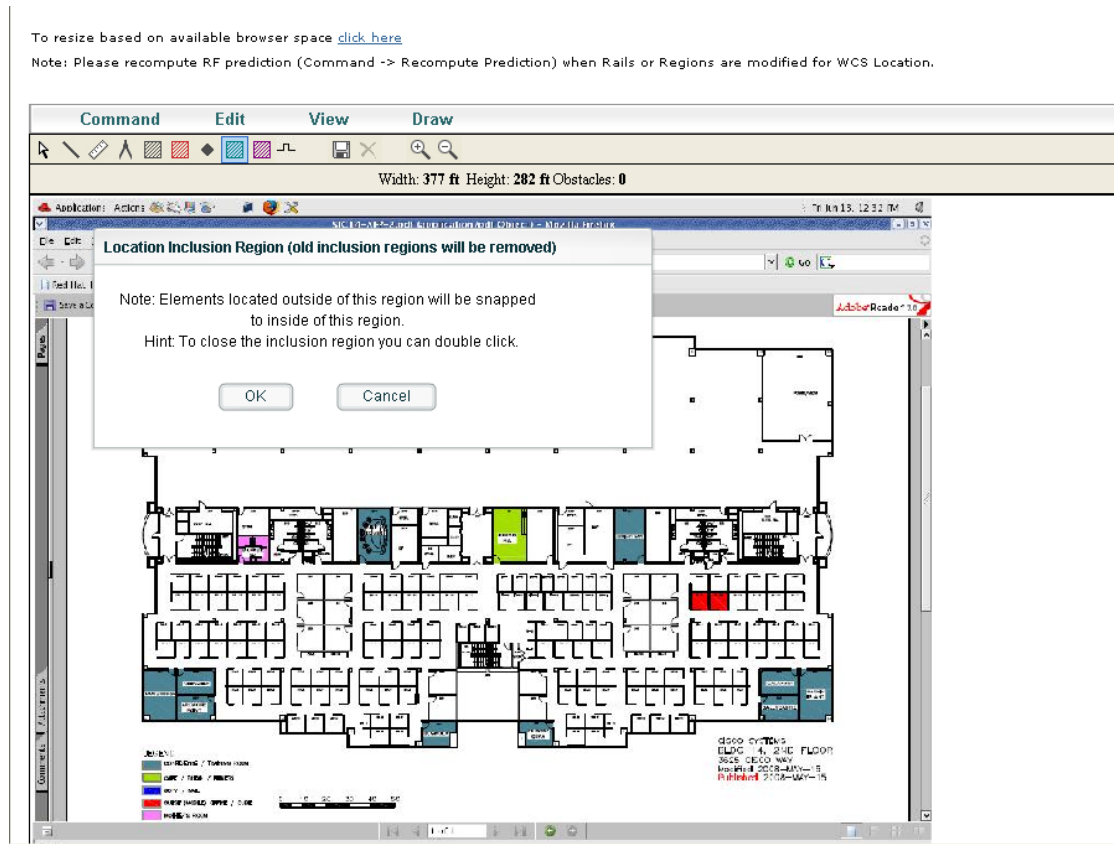
Step 5   Click **OK** in the message box that appears. A drawing icon appears to outline the inclusion area.

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 and then click **Save settings** and close the Layers configuration panel when complete.

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

Step 14   Select the **Network Designs** tab and then click **Synchronize**.

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

Note   Newly defined inclusion and exclusion regions appear on heatmaps only after the location server 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.

Follow the steps below to define an exclusion area.

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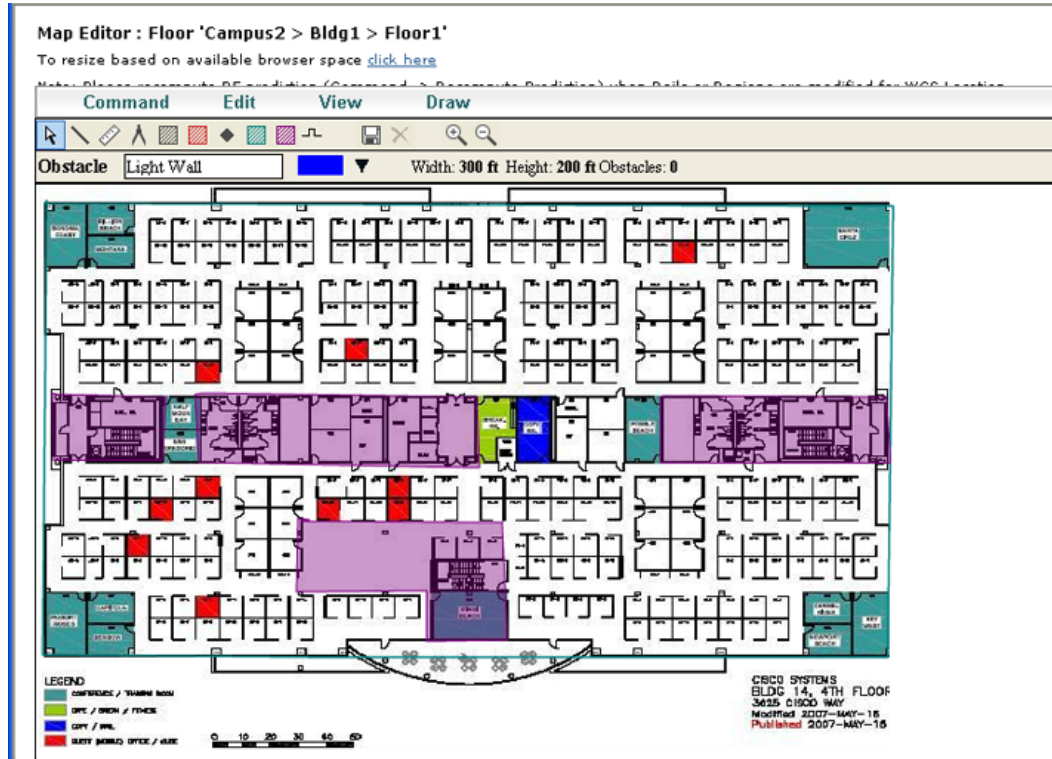
Step 10 When all exclusion areas are defined, select Save from the Command menu or the disk icon on the tool bar to save the exclusion region.

> **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 settings** and close the Layers configuration panel when complete.

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

Step 15 Select the **Network Designs** tab and then click Synchronize.

Check the Sync. Status column to ensure 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 certain inventory with asset tags to appear. Any asset tags located within the snap-width area are plotted on the rail line (majority) or just outside of the snap-width area (minority).

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

Follow the steps below to define a rail with a floor.

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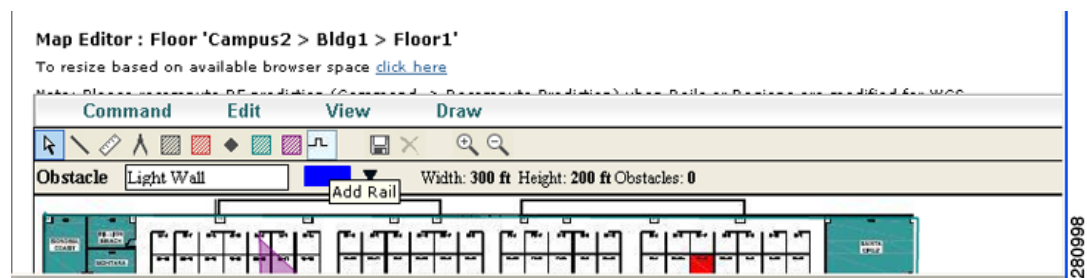
Step 5   In the message panel that appears, enter a snap-width (feet or meters) for the rail and then click **OK.** A drawing icon appears.

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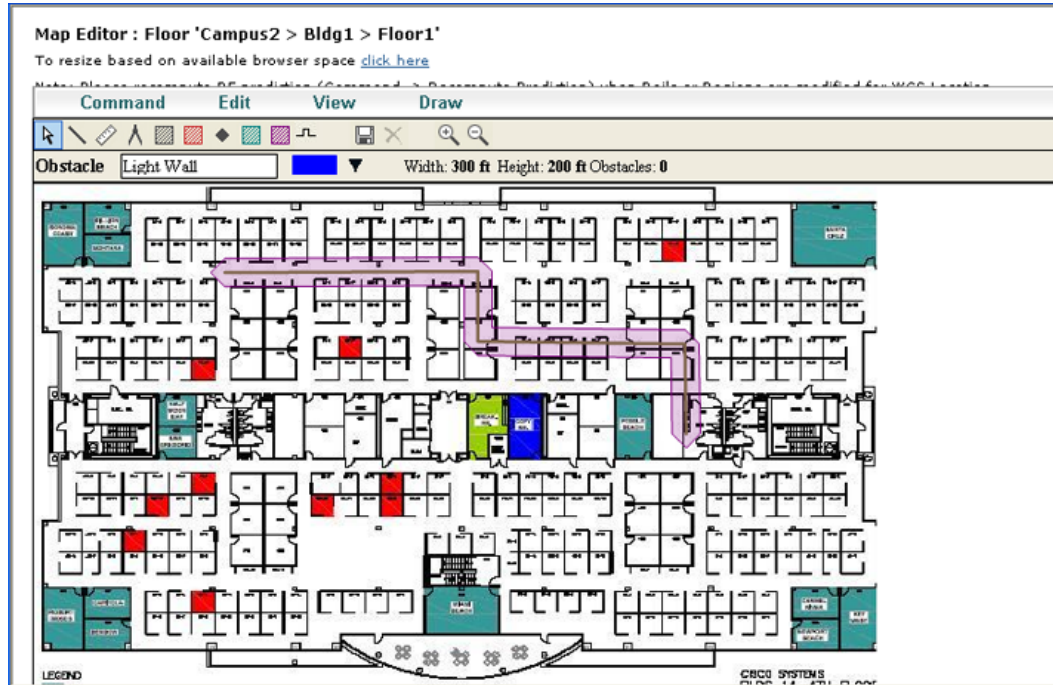
> **Note**   To delete a rail line, click on the area to be deleted. The selected area is outlined by a dashed purple line. Next, click on the *X* icon in the tool bar. The area is removed from the floor map.

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 location databases, click **Mobility > Synchronize Services**.

Step 12   Select the **Network Designs** tab and then click **Synchronize**.

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

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 7-18).

Figure 7-18   *New Template > General Panel*

Step 5   At the General panel modify parameters as necessary. Definitions for each of the parameters is listed in Table 7-1.

Table 7-1   *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.

Table 7-1   General Location Parameters (continued)

Parameter	Configuration Options
Normal Client	Check the **Enabled** check box to have a non-calibrating client. No S36 or S60 requests are transmitted to the client.
Measurement Notification Interval	Enter a value to set the NMSP measurement notification interval for clients, tags and 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 location appliance exist, the largest interval setting of the two is adopted by the location appliance. Once this controller is synchronized with the location appliance, the new value is set on the location appliance.
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.

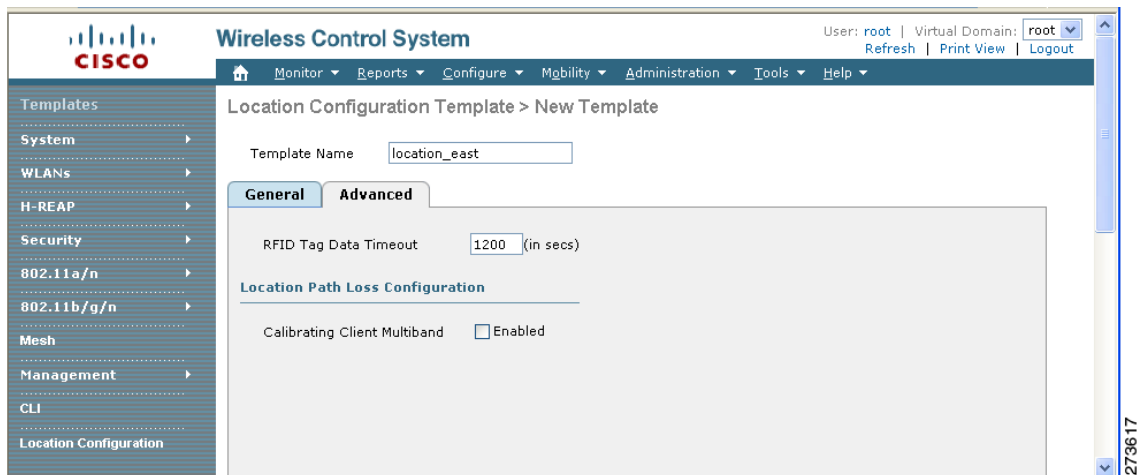*Figure 7-19   New Template > Advanced Parameters Panel*

Step 6   At the Advanced panel modify parameters as necessary (Figure 7-19). Definitions for each of the parameters is listed in Table 7-2.

Table 7-2   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**.

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   Context-Aware Software was previously referred to as location-based services.

Editing Tracking Parameters

The location appliance can track up to 2,500 elements. You can track the following elements: client stations, active asset tags and rogue clients and access points.Updates on the locations of elements being tracked are provided to the location server 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 they are not used in calculating the 2,500 element limit.

You can modify the following tracking parameters using Cisco WCS:

- Enable and disable which 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 limit of 2,500 trackable units, you could set a limit to track only 1,500 client stations. Once the tracking limit is met, 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 location appliance, follow these steps:

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

Step 2   Click the name of the location server whose properties you want to edit. The General Properties window appears.

Step 3 In the Context Aware Service 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 7-3 describes each parameter.

:

Table 7-3   Tracking and SNMP Parameters

Parameter	Configuration Options
Tracking Parameters	
Client Stations	1. Check the **Enable** check box to enable tracking of client stations by the location server.
	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 2,500 which is the maximum number of elements tracked by a location server.
	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 location server.
	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 2,500 which is the maximum number of elements tracked by a location server.
	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.
Rogue Clients and Access Points	1. Check the **Enable** check box to enable tracking of rogue clients and asset points by the location server.
	2. Check the **Enable Limiting** check box to set a limit on the number of rogue clients and asset tags stations to track.
	3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 2,500 which is the maximum number of elements tracked by a location server.
	Note Active Value (display only): Indicates the number of rogue clients and asset tags 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 WCS maps or its events and alarms reported.

Table 7-3   Tracking and SNMP Parameters (continued)

Parameter	Configuration Options
SNMP Parameters	
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.
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 location server database.

Editing 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 7-4 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 location appliance, follow these steps:

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

Step 2   Click the name of the location server whose properties you want to edit. The General Properties window appears.

Step 3   From the **Context Aware Service** 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 7-4 describes each parameter.

Table 7-4   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 column.
	Note To move multiple addresses, click the first MAC address and depress the **Ctrl** key to highlight additional MAC addresses. Click **Allow** or **Disallow** to transfer it to the MAC address to its 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 location server database.

Editing History Parameters

You can use Cisco WCS to specify how often to collect client station, rogue access point, and asset tag histories from the controllers associated with a location server.

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

To configure location server history settings, follow these steps:

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

Step 2   Click the name of the location server whose properties you want to edit.

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

Step 4   Modify the following history parameters as appropriate. Table 7-5 describes each parameter.

Table 7-5   History Parameters

Parameter	Configuration Options
Archive for	Enter the number of days for the location server to retain a history of each enabled category. Default value is 30. Allowed values are from 1 to 99999.
Prune data starting at	Enter the interval of time in which the location server 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 client stations, asset tags or rogue clients and access points check boxes to log location transitions. 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 location server database.

Enabling Location Presence on a Location Server

You can enable location presence by location server 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.

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 5.2 and greater.

Once enabled, the location server is capable of providing any requesting Cisco CX v5 client its location.

Note   Before enabling this feature, synchronize the location server.

To enable and configure location presence on a location server, follow these steps.

Step 1   Click **Mobility > Mobility Services** > *Device Name*. Select the location server to which the campus or building is assigned.

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

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

Step 4   Select one of the Location Resolution options.

    a.   When Building is selected, the location server 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 location server returns the client address as *Building A*.

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

    c.   When X,Y is selected, the location server 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 location server 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. Expanded location details can also be entered in the Advanced panel.

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 tag, station, and chokepoint information for the location server using Cisco WCS, follow these steps:

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

Step 2 Click the name of the location server 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. 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 tag, station, and chokepoint information from the location service 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 location server 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.   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.

Editing Location Parameters

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

To configure advanced location parameters, follow these steps:

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

Step 2   Click the name of the location server whose properties you want to edit.

Step 3   From the **Context Aware Service** 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 7-6 describes each parameter.

Table 7-6   Location Parameters

Parameter	Configuration Options
Calculation time	Check the corresponding check box to enable the calculation of the time required to compute location. ⚠ **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** The OW Location parameter is ignored by the location server.

Table 7-6   Location Parameters (continued)

Parameter	Configuration Options
Relative discard RSSI time	Enter the number of minutes since the most recent RSSI sample after which RSSI measurement should be considered stale and discarded. For example, if you set this parameter to 3 minutes and the location server 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.*
Absolute discard RSSI time	Enter the number of minutes after which RSSI measurement should be considered 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.*
RSSI Cutoff	Enter the RSSI cutoff value, in decibels (dBs) with respect to one (1) mW (dBm), above which the location server 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 location server 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.
	⚠
	Caution Modify only under Cisco TAC personnel guidance. Modifying this value can reduce the accuracy of location calculation.
Location Filtering	Check the corresponding check box to enable location filtering. Allows previous location calculations of a clients to be used in determining a client's current location to increase location accuracy.
Chokepoint Usage	Check the Enable check box to enable tracking of Cisco compatible tags by chokepoints.
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.
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.

Step 5   Click **Save** to store your selections in the Cisco WCS and location server databases.

C H A P T E R 8

Monitoring Location Servers and Site

This chapter describes how to monitor location servers by configuring and viewing alarms, events, and logs.

It also describes how to use Cisco WCS to view location server, client and asset tag status.

This chapter contains the following sections:

Working with Alarms

This section describes how to view, assign, and clear alarms and events on location servers 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 location server alarms, follow these steps:

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

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

Figure 8-1   *Search Alarm Panel*
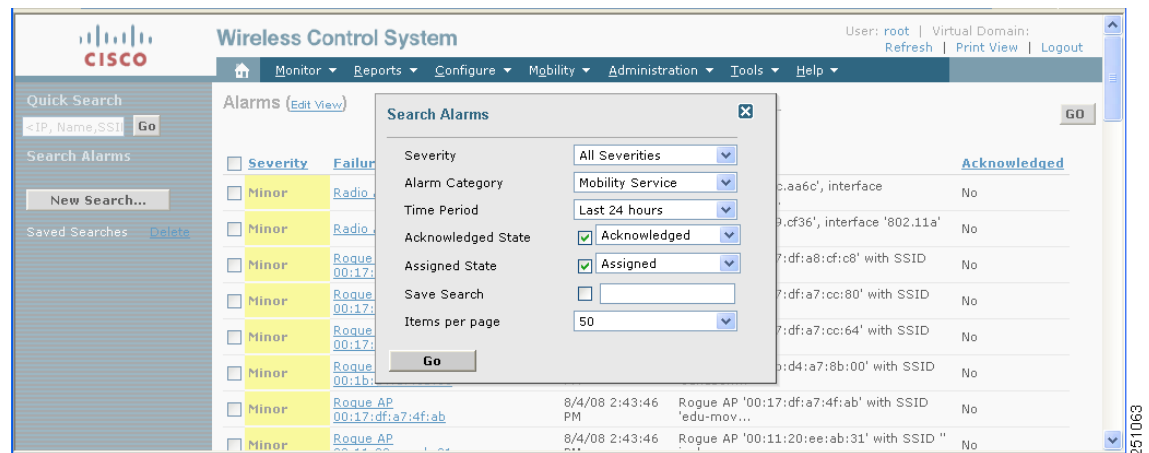
Step 3   Select the Severity of Alarms to display. Options are All Severities, Critical, Major, Minor or Warning.

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

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

Step 5   Select the time frame for which you want to review alarms by selection 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 Stat**e check box to exclude the acknowledged alarms and their count from the Alarm Summary window.

Step 7   Check the **Assigned State** 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.

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.

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 location appliance, 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.

> **Note**   A SMTP Mail Server must be defined prior to entry of target email addresses for email notification. Choose **Administrator > 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 **Context Aware Service**.

Step 4   Click the **Context Aware Service** link. The panel for configuring the alarm severity types (critical, major, minor and warning) that are reported for the location servers appears.

Step 5   Check box(es) 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. Each email address should be 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 location server 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 location servers
- By security

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

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

To display events, follow these steps:

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

Step 2 In the Events window:

- If you want to display the events for a specific element and you know its IP address, MAC address, or Name, enter that value in the Quick Search field (left-side). Click **GO**.

- To display events by severity and category, select the appropriate options from the Severity and Event Category drop-down menus. 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, choose **Mobility > Mobility Services**.

Step 2 Click the name of the location server that you want to configure.

Step 3 From the System menu (left panel) click **Advanced Parameters**. The advanced parameters for the selected location server 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 location server log files, you can use Cisco WCS to download them into your system. Cisco WCS downloads a zip file containing the log files.

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

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

Step 2   Click the name of the location server to view its status.

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

Step 4   Click **Download Logs**.

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

Generating Reports

In Cisco WCS, you can generate a utilization report for a location server. 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 the location server. 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 location server or servers 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 Location Server Utilization Report

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

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

The MSE Utilization summary window appears.

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

A tabbed panel appears (see Figure 8-2).

Step 4   Enter a report title.

Step 5   The Report By selection is always MSE.

Step 6   Select either a specific location server or **All MSEs** from the drop-down MSE menu.

> **Note**   Entering All MSEs reports location servers and mobility services engines.

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.

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

Step 8   To define how collected data is grouped and displayed (hourly, daily, weekly) on the report (x-axis), select an option from the Aggregation Frequency drop-down menu. Select the **Schedule** tab when complete.

For example, if you want to graph data daily on your report, you select **daily**. Additionally, you must select daily as the Recurrence value in the schedule tab.

> **Note**   The Recurrence parameter defines how often a report is generated.

Step 9   At the Schedule window, check the **Enable Schedule** check box to enable the report.

Figure 8-2   MSE Utilization > New > Schedule Tab

Step 10   Select the export format from the drop-down menu.

Step 11   Select either the **Save To File** or the **Email To** option.

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

Step 13   Specify a start time using the hour and minute drop-down menus.

Step 14   Click one of Recurrence buttons to select how often the report is run.

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

Step 15   When complete with all of the above steps, do one of the following:

- Click **Save** to save edits.

- Click **Save and Run** to save the changes and run the report now. The report is run and the results are either emailed or saved to a designated file as defined in the Schedule tab. The report runs again at the scheduled time.

- 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.

> ✎
> **Note**   You can also click **Run Now** to check a report scenario before saving it or to run reports as necessary.

Viewing an MSE Utilization Chart

To view results of a defined report, do the following:

Step 1   In Cisco WCS, choose **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 Location Server Utilization Report" section on page 8-6.

Step 3   Select a listed report.

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.

Step 6   Review and edit other parameters, as necessary. When finished with your review or edit, do one of the following:

- Click **Save** to save edits.

- Click **Save and Run** to save the changes and run the report now. The report is run and the results are either mailed or saved to a designated file as defined in the Schedule tab. The report runs again at the scheduled time.

- 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.

> **Note**   You can click **Run Now** to check a report scenario before saving it or to run reports as necessary.

Monitoring Location Server Status

This section describes how to view location server status and how to enable status information polling.

Viewing Location Server Current Information

To view the current status of a location server, follow these steps:

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

Step 2   Click the name of a location server to view its status.

Step 3   Click **System > Advanced Parameters** to display location server status.

> **Note**   For details on configuring advanced parameters, refer to Chapter 4.

Information for the selected location server found on the Advanced Parameters window is summarized in Table 8-1.

Table 8-1   Advanced Parameters for Location Servers

Page Heading	Description
General Information	Product name, version, time server started operation, time zone, hardware restarts, active sessions, number of tracked elements and tracked element limit.
	Note A major alert appears on the Advanced Parameter window if the tracked elements limit of 2,500 for the location server is reached.
Cisco UDI	Product identifier, version identifier, and serial number.
Logging Options	Types of occurrences and level (off, information, error, trace) being logged.
	Note Use **Error** and **Trace** only when directed to do so by Cisco Technical Assistance Center (TAC) personnel.

Table 8-1   Advanced Parameters for Location Servers (continued)

Page Heading	Description
Advanced Parameters	Number of days to keep events, Session Time out, Interval between data cleanup and enabled/disable status of Advanced Bug operation.
	Note To modify these values, refer to the "Viewing and Configuring Advanced Parameters" section on page 4-4.
Advanced Commands	Commands: Reboot Hardware, Shutdown Hardware, Clear Configuration and Defragment Database.

Monitoring Clients

You can configure Cisco WCS to display the name of the access point that generated the signal for a client, its strength of signal and how often the location information for that client is updated. This information is display by simply passing the cursor over the client icon on the map. Additionally, you can click on the icon to open the Client Properties window.

To provide this functionality, you must first enable location status for the client.

To enable client location status for a specific client, follow these steps:

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

The Clients Summary window displays.

Step 2   Click the Total Clients link for the appropriate location server listed under Clients Detected by Location Servers.

A summary of all clients for the chosen location server displays noting the user, vendor, IP address, MAC address, access point (AP), detecting controllers, port, system, 802.11 state, profile name, SSID, authenticated, protocol, map location launch link, link test launch link, and automated test ran (yes or no).

Note   To search for a client by a specific parameter such as by MAC address or controller, click New Search and select the appropriate search criteria. If you searched for the client by its MAC address, only one entry is listed.

Step 3   Click on the appropriate client.

Step 4   Click the **Location** tab.

Step 5   Check the **Enabled** check box for **Location Debug** under Asset Info.

Step 6   Click **Update** and close the window.

Step 7   At the map, click **Refresh Heatmap** to activate the feature on the map.

Note   At the **Monitor > Maps** window, both the Heatmaps and Clients check boxes in the Layers menu must be checked for the RSSI and client icons to display on the map.

Monitoring Tagged Assets

You can configure WCS to display the name of the access point that generated the signal for a tagged asset, its strength of signal and when the location information was last updated for the asset. This information is display by simply passing the cursor over the asset tag icon on the map. Additionally, you can click on the icon to open the Tag Properties window.

To provide this functionality, you must first enable location status for the tagged asset.

Enabling Tagged Asset Location Status

To enable tag location status, follow these steps:

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

The Tags Summary window appears.

Step 2   Click the **Total Tags** link for the appropriate location server.

A summary of all tags for the chosen location server appears noting MAC address, Asset Name, Asset Group, Asset Category, Vendor, Location server (labeled as MSE), Controller, Battery Status, and Map location for each of the tags.

> **Note**   You can also search for a specific tag by criteria such as MAC address, controller, or Tag Vendor. See the "Querying of Tags" section on page 8-11 for more details.

Step 3   Click the appropriate tag. The Tag Properties window appears.

Step 4   Check the **Enabled** check box for **Location Debug** under Asset Info

Step 5   Click **Update** and close the window.

Step 6   At the map, click **Refresh Heatmap** to activate the feature on the map.

> **Note**   At the **Monitor > Maps** window, both the Heatmaps and 802.11 Tags check boxes in the Layers menu must be checked for the RSSI and tag icons to display on the map.

Querying of Tags

You can query tags by asset type (name, category and group), by MAC address, by system (controller or location appliance), and by area (floor area and outdoor area).

You can further refine your search by tag vendor and type (telemetry) and save the search criteria for future use. Saved search criteria can be retrieved from the Saved Searches drop-down menu on the Tag Summary window (Monitor > Tags).

The following details are displayed on the Tag Properties window for each tag:

- Tag vendor
- Controller to which tag is associated
- Battery Life
- Asset Information (Name, Category, Group)

- Statistics (bytes and packets received)

- Location (Floor, Last Located, Location Server)

- Location Notifications

- Telemetry Data (CCX v1 compliant tags only)

✎ **Note**   Telemetry data displayed is vendor-specific; however, some commonly reported details are GPS location, battery extended information, pressure, temperature, humidity, motion, status, and emergency code.

- Emergency Data (CCX v1 compliant tags only)

To query tags, follow these steps:

Step 1   Choose **Monitor > Tags**. The Tag Summary window appears.

Step 2   To initiate a search for tags, click **New Search** (side panel) to open the tag search window (Figure 8-3).

Figure 8-3   Search Tags Panel
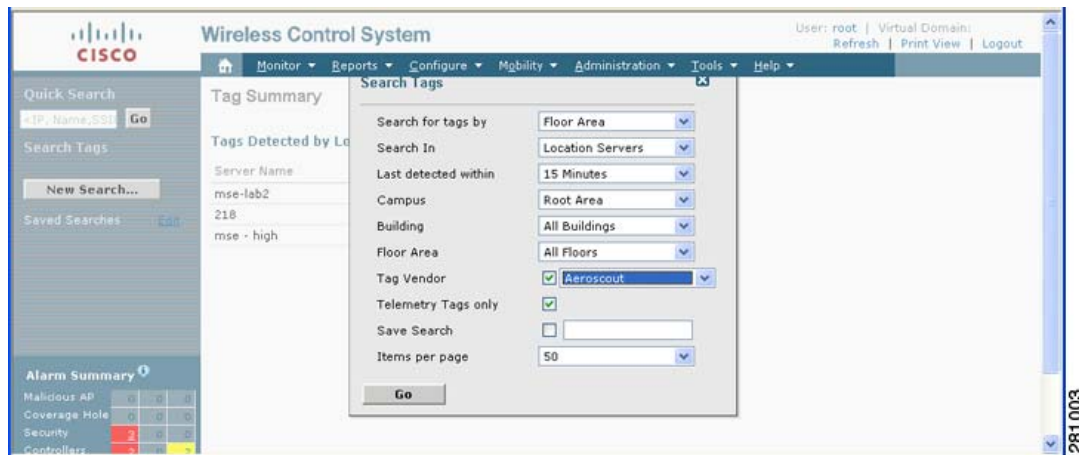
Step 3   Select the appropriate search criteria. Table 8-2 lists search criteria and their possible values.

Table 8-2   Tag Search Criteria and Values

Search Criteria	Variable Search Criteria	Possible Values
Search for tags by (Tier 1 search criteria)	—	All Tags; Asset Name, Asset Category or Asset Group; MAC Address; Controller or MSEs; Floor Area or Outdoor Area. **Note** MSE search includes both location servers and mobility services engines.
Search In (Tier 2 search criteria)	—	WCS Controllers or MSE. **Note** WCS Controller option indicates that the search for controllers is done within WCS. **Note** MSE search includes both location servers and mobility services engines.
Last detected within	—	Options are from 5 minutes to 24 hours.
Variable search criteria. (Tier 3 search criteria) **Note** Possible search criteria determined by the **Search for tabs by** (Tier 1 search) value.	If **Search for tags by** value is: 1. Asset Name, then enter Tag Asset Name. 2. Asset Category, then enter Tag Asset Category. 3. Asset Group, then enter Tag Asset Group. 4. MAC Address, then enter Tag MAC Address. 5. Controller, then select Controller IP address from drop-down menu. 6. MSE (when system is a location server), then choose a location server IP address from drop-down menu. 7. Floor Area, then choose Campus, Building and Floor Area. 8. Outdoor Area, then choose Campus and Outdoor Area.	
Show Telemetry Tags only	—	Check box to display telemetry tags. Leaving option unchecked displays all tags. **Note** Option only seen when MSE (select for location servers), Floor Area or Outdoor Area are selected as the Search for tags by option. **Note** Only those vendor tags that support telemetry appear.
Tag Vendor	—	Check box to select tag vendor from drop-down menu. **Note** Option does not display when Asset Name, Asset Category, Asset Group or MAC Address are the search criteria for tags.

Table 8-2   Tag Search Criteria and Values

Search Criteria	Variable Search Criteria	Possible Values
Save Search	—	Check box to name and save search criteria. Once saved, entry appears under Saved Searches heading (left-panel).
Items Per Page	—	Select the number of tags to display per search request. Values range from 10 to 500.

Step 4   Click **Go** when all search criteria are selected. A listing of all tags that match the search criteria appears.

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

Step 5   Select a MAC Address link to display details for a specific tag. The Tag Properties window appears (Figure 8-4).

Figure 8-4   Tag Properties Window (top)

Note   Scroll down to the bottom of the window to see Telemetry and Emergency details for the tag (Figure 8-5).

Figure 8-5   Tag Properties Window (bottom)
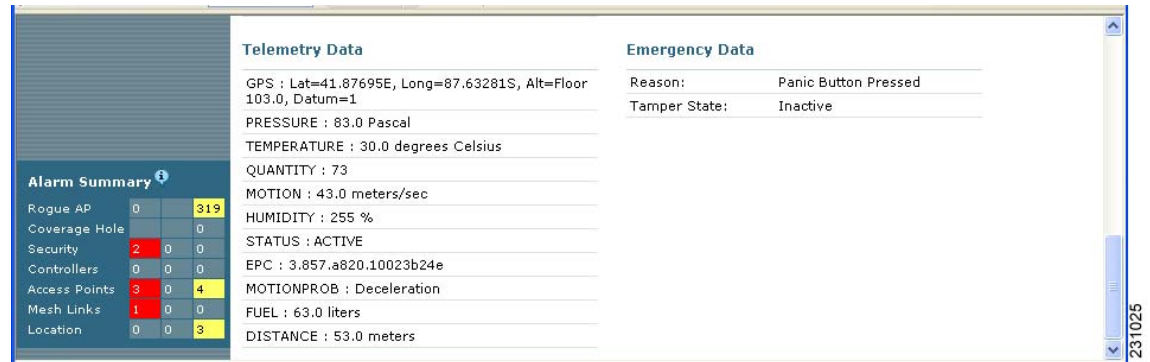
Overlapping Tags

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

When you move the mouse over the overlapping tag on the map, a panel appears with summary information for the overlapping tags (see Figure 8-6).

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

Note
- Summary information for tags includes: Tag MAC address, Asset Name, Asset Group, Asset Category, Vendor (Type), Battery life and Last Located data (date and time). If the tag is Cisco CX v.1 compliant, telemetry information also appears.

- Detailed information for tags includes this additional information: IP address of associated controller, statistics, location notifications, location history and whether the location debug feature is enabled.

  - To view location history for a tag, select that option from the Select a command drop-down menu and click **GO**.

  - To return to the details screen from the location history window, select the Tag Detail option and click **GO**.

Figure 8-6   *Overlapping Tags Window*
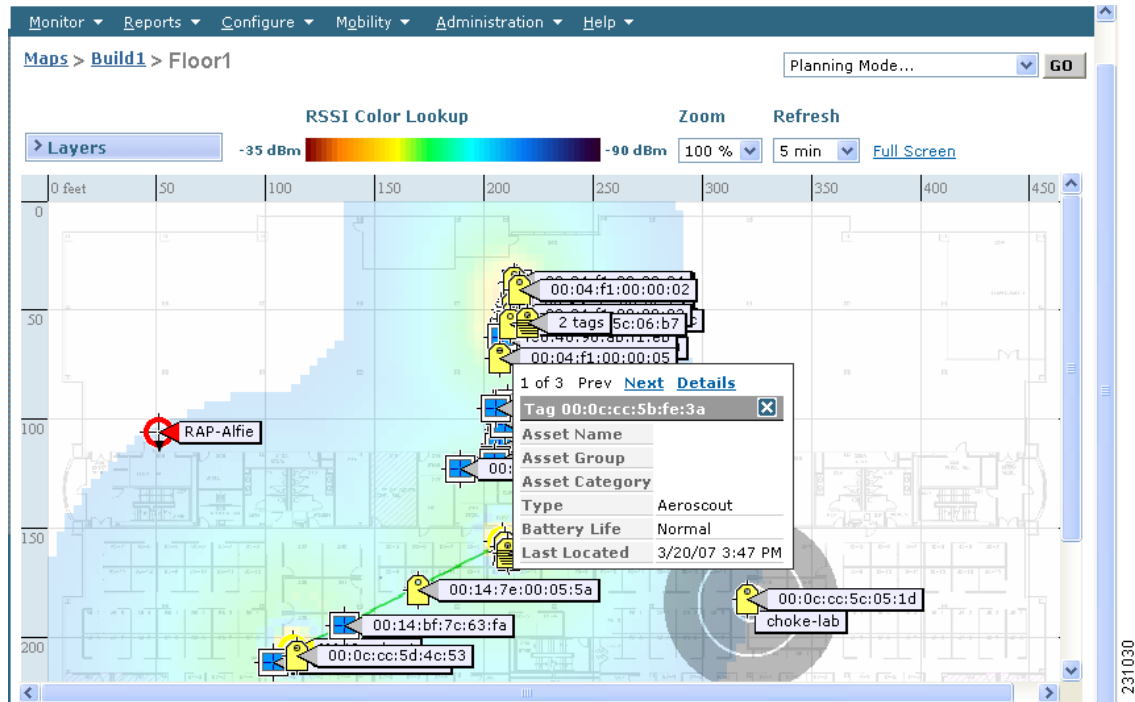
Monitoring Chokepoints

To monitor chokepoints, follow these steps:

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

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

    a.   To initiate a search for a chokepoint by its MAC address, select **MAC address** from the Search for Chokepoints by drop-down menu and enter the MAC address of the chokepoint in the field below. Click **Search**.

    b.   To initiate a search for a chokepoint by its name, select **Chokepoint Name** from the Search for Chokepoints by drop-down menu and enter the chokepoint name in the field below. Click **Search**.

If no match exists, then a message indicating that appears in the window. Otherwise the search result displays.

Monitoring Wi-Fi TDOA Receivers

To monitor location sensors, follow these steps:

Step 1   Click **Monitor > WiFi TDOA Receivers**. The WiFi TDOA Receiver **s**ummary window appears showing all mapped location sensors.

Step 2   To refine the search criteria when an extensive lists appears, you can search by MAC address or location sensor name.

    a.   To initiate a search for a TDOA receiver by its MAC address, select **MAC address** from the Search for WiFi TDOA Receiver by drop-down menu and enter the MAC address of the TDOA receiver in the field below. Click **Search**.

    b.   To initiate a search for a TDOA receiver by its name, select WiFi TDOA Receivers from the Search for WiFi TDOA Receiver by drop-down menu and enter the TDOA Receiver's name in the field below. Click **Search**.

If no match exists, then a message indicating that appears in the window. Otherwise the search result displays.

C H A P T E R 9

Performing Maintenance Operations

This chapter describes how to back up and restore location server data and how to update the location server software. It also describes other maintenance operations.

This chapter contains the following sections:

- "Recovering Lost Password" section on page 9-2
- "Recovering a Lost Root Password" section on page 9-2
- "Backing Up and Restoring Location Server Data" section on page 9-2
- "Downloading Software to Location Servers" section on page 9-4
- "Configuring NTP Server" section on page 9-6
- "Defragmenting the Location Server Database" section on page 9-7
- "Rebooting the Location Server Hardware" section on page 9-8
- "Shutting Down the Location Server Hardware" section on page 9-8
- "Clearing Location Server Configurations" section on page 9-8

Recovering Lost Password

To recover a lost or forgotten password for a location server, 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 location server, 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 Location Server Data

This information describes how to back up and restore location server data. It also describes how to enable automatic backup.

Backing Up Location Server Historical Data

Cisco WCS includes functionality for backing up location server data.

To back up location server data, follow these steps:

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

Step 2   Click the name of the server 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.

> **Note**   For location servers versions 2.1 or later, the timeout value is not required.

> **Note**   For location server versions 2.0 or later, the timeout indicates how long the full operation will take. The default value is 1800 seconds. For pre-2.0 versions of the location server, the timeout parameter refers only to the connection timeout value and a smaller value should be entered (120 seconds by default).

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 location server operations in other WCS windows.

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

Restoring Location Server Historical Data

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

To restore location server data, follow these steps:

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

Step 2   Click the name of the server that you want to restore.

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

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.

> ✎
> **Note**   For location servers versions 2.1 or later, the timeout value is not required.

> ✎
> **Note**   For location server versions 2.0 or later, the timeout represents how long the full operation will take (by default, the user interface suggest 1800 seconds). For older location servers, the timeout represents the connection timeout and you should use a small value (120 seconds by default).

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

Step 8   Click **OK** to confirm that you want to restore location server 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 location server operations in other WCS windows.

Enabling Automatic Location Server Backup

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

To enable automatic location server data backup, follow these steps:

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

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

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

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

Downloading Software to Location Servers

To download software to a location server, follow these steps:

Step 1   Verify that you can ping the location server 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 server to which you want to download the software.

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

Step 5 Click **Download Software**.

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

- To download software listed in the WCS directory, select **Select from uploaded images to transfer into the Location 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.

  > **Note** If upgrading a location server installed with a pre-2.0 version, you must first download and decompress the file (`gzip -d imageFilename`) **before** installing the image. After decompressing the file, run the resulting *.bin installer file.

  > **Note** If you have a 2.0 or later version of the location server image already installed, the software image automatically decompresses during its download from WCS.

- To use downloaded software available locally or over the network, select the **Browse a new software image to transfer into the Location Server** and click **Browse**. Locate the file and click **Open**.

Step 7 Enter the time in seconds (between 1 and 1800) after which software download times out.

Step 8 Click **Download** to send the software to the */opt/locserver/installers* directory on the location server.

Step 9 After the image is transferred to the location server, log into the location server CLI.

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

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

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

Manually Downloading Software

If you do not want to automatically update the location server 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 location server software 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-AIR-LOC2700-L-K9-x-x-x-x-64bit.bin.gz*.

> **Note** The location server software 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-AIR-LOC2700-L-K9-5-2-91-0-64bit.bin.gz
<CTRL-Z>
#
```

   b. Verify that the image (*CISCO-AIR-LOC2700-L-K9-x-x-x-x-64bit.bin.gz*) is in the location server's */opt/installers* directory.

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

   gunzip *CISCO-AIR-LOC2700-L-K9-x-x-x-x-64bit.bin.gz*

   The decompression yields a *bin* file.

   d. Make sure that the *CISCO-AIR-LOC2700-L-K9-x-x-x-x.bin* file has execute permissions for the root user. If not, enter **chmod 755** *CISCO-AIR-LOC2700-L-K9-x-x-x-x.bin*.

Step 2   Manually stop the location server.

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

Step 3   Enter **/opt/installers/***CISCO--AIR-LOC2700-L-K9-x-x-x-x.bin* to install the new location server image.

Step 4   Start the new location server software by entering the following command:

   /etc/init.d/locserverd 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/locserver/uninstall** to uninstall the location server's script files.

Configuring NTP Server

You can configure NTP servers to set up the time and date of the 2700 and 2710 location appliances.

> ✎
>
> **Note**   You are automatically prompted to enable NTP and enter NTP server IP addresses as part of the automatic installation script. You can rerun the automatic script at anytime to change settings. For more details on the automatic installation script, refer to the *Cisco Wireless Location Appliance Getting Started Guide* at the following link:
> http://www.cisco.com/en/US/products/ps6386/prod_installation_guides_list.html

The /etc/ntp.conf file is the main configuration file in which you place the IP addresses or DNS names of the NTP servers you want to use (see the following example).

```
server ntp.mydomain.com # my corporate NTP
server 192.168.2.5 # my second NTP
```

To get NTP configured to start at bootup, enter the following:

```
[root@loc-server1]# chkconfig ntpd on
```

To start, stop, and restart NTP after booting, follow these examples:

```
[root@loc-server1]# service ntpd start
[root@loc-server1]# service ntpd stop
[root@loc-server1]# service ntpd restart
```

After configuring and starting NTP, make sure it is working properly. To test whether the NTP process is running, use the following command:

```
[root@loc-server1]# pgrep ntpd
```

You should get a response of plain old process ID numbers.

Enter the *ntpdate -u serverIP* command to force your server to become instantly synchronized with its NTP servers before starting the NTP daemon for the first time (see the following example).

```
[root@loc-server1]# service ntpd stop
[root@loc-server1] ntpdate -u 192.168.1.100
Looking for host 192.168.1.100 and service ntp
host found: ntpl.my-site.com
12 Aug 08:03:38 ntpdate[2472]: step time server 192.168.1.100 offset 28993.084943 sec
[root@smallfry tmp]# service ntpd start
```

Note   For more information on the NTP configuration, consult a Linux configuration guide.

Defragmenting the Location Server Database

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

To defragment the location server database, follow these steps:

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

Step 2   Click the name of the location server that you want to defragment its database.

Step 3   Click **System** (left) to display its menu options.

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 location server's database.

Rebooting the Location Server Hardware

If you need to restart a location server, follow these steps:

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

Step 2   Click the name of the location server that you want to reboot.

Step 3   Click **System** (left-panel) to display its menu options.

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 location server hardware.

The rebooting process takes a few minutes to complete.

Shutting Down the Location Server Hardware

If you need to shutdown a location server, follow these steps:

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

Step 2   Click the name of the location server that you want to shutdown.

Step 3   Click **System** (left-panel) to display its menu options.

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 location server.

Clearing Location Server Configurations

To clear a location server 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 server you want to configure.

Step 3   Click **System** (left-panel) to display its menu options.

Step 4   Click **Advanced Parameters**.

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

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

I N D E X

A

active user sessions **5-5**

advanced debug **7-8**

alarm notifications

    emailing **8-4**

alarms

    assigning **8-3**

    clearing **8-3**

    deleting **8-3**

    unassigning **8-3**

    viewing **8-2**

applying calibration models **7-3**

assets

    battery level **8-11**

automatic synchronization **3-5**

C

calibration models **7-3**

calibration models, applying **7-3**

Cisco UDI **8-9**

client

    location debug **8-10, 8-11**

D

Database

    defragment **9-7**

E

event definition

    adding **6-3**

    deleting **6-6**

    testing **6-6**

event groups

    adding **6-2**

    deleting **6-2**

event notifications

    summary **6-7**

events

    viewing **8-4**

G

general properties

    editing **4-2**

groups

    adding **5-2**

    deleting **5-2**

    permissions **5-3**

H

history parameters

    editing **7-34**

host access

    adding **5-5**

    deleting **5-6**

    editing **5-7**

L

location parameters

    editing **7-29, 7-37**

W

warnings

    defined   **3-x to 3-xi**

Cisco Location Appliance Configuration Guide