



Cisco Location Appliance Configuration Guide, Release 6.0

Last revised: June 11, 2009

Americas Headquarters

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

Text Part Number: OL-20031-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Location Appliance Configuration Guide
© 2009 Cisco Systems, Inc. All rights reserved.

Customer Order Number:



CONTENTS

CHAPTER 1

Overview	1-1
Location Appliance Functionality	1-2
Viewing Location Data	1-3
Event Notification	1-3
Configuration and Administration	1-4
Adding and Deleting Location Servers	1-4
Editing Location Server Properties	1-4
Managing Location Server Users and Groups	1-5
Location Server Synchronization	1-5
Location Planning and Verification	1-5
Monitoring Capability	1-5
Maintenance Operations	1-5
System Compatibility	1-6
Backwards Compatibility of Location Server Software	1-6

CHAPTER 2

Adding and Deleting Location Servers	2-1
Adding a Location Appliance to Cisco WCS	2-2
Deleting Location Servers from the Cisco WCS Database	2-4

CHAPTER 3

Synchronizing Location Servers with Cisco Wireless LAN Controllers and Cisco WCS	3-1
Synchronizing Cisco WCS and Location Servers	3-2
Associating a Location Server with a Controller	3-2
Setting and Verifying Timezone on a Controller	3-3
Synchronizing Cisco WCS and Location Servers	3-4
Configuring Automatic Location Service Database Synchronization	3-5
Out-of-Sync Alarms	3-6
Viewing Synchronization Information	3-6
Viewing Location Service Synchronization Status	3-6
Viewing Location Service Synchronization History	3-7

CHAPTER 4

Configuring and Viewing System Properties	4-1
Configuring General Properties	4-2
Modifying NMSP Parameters	4-2

- Viewing Active Sessions on a System 4-4
- Viewing and Configuring Advanced Parameters 4-4
 - Viewing Advanced Parameters Settings 4-4
 - Configuring Advanced Parameters 4-5
 - Configuring Logging Options 4-5
 - Configuring Advanced Parameters 4-6
 - Initiating Advanced Commands 4-6
 - Rebooting or Shutting Down a System 4-6
 - Clearing the System Database 4-7
 - Defragmenting the Database 4-7

CHAPTER 5

Managing Location Server Users and Groups 5-1

- Managing Groups 5-2
 - Adding User Groups 5-2
 - Deleting User Groups 5-2
 - Changing User Group Name, Password or Permission 5-3
- Managing Users 5-3
 - Adding Users 5-3
 - Deleting Users 5-4
 - Changing User Properties 5-4
 - Viewing Active User Sessions 5-5
- Managing Host Access 5-5
 - Adding Host Access 5-5
 - Deleting Host Access Records 5-6
 - Editing Host Access Records 5-7

CHAPTER 6

Configuring Event Notifications 6-1

- Working with Event Groups 6-2
 - Adding Event Groups 6-2
 - Deleting Event Groups 6-2
- Adding, Deleting, and Testing Event Definitions 6-2
 - Adding an Event Definition 6-3
 - Deleting an Event Definition 6-6
 - Testing Event Definitions 6-6
- Viewing Event Notification Summary 6-7
- Notifications Cleared 6-8
- Enabling Notifications and Configuring Notification Parameters 6-8
 - Enabling Notifications 6-8

Filtering Northbound Notifications	6-9
Configuring Notification Parameters	6-9
Notification Message Formats	6-11
Notification Formats in XML	6-11
Missing (Absence) Condition	6-12
In/Out (Containment) Condition	6-12
Distance Condition	6-13
Battery Level	6-13
Location Change	6-13
Chokepoint Condition	6-14
Emergency Condition	6-14
Notification Formats in Text	6-14
Cisco WCS as a Notification Listener	6-15

CHAPTER 7**Location Planning and Verification 7-1**

Deployment Planning for Data, Voice, and Location	7-2
Creating and Applying Calibration Models	7-3
Inspecting Location Readiness and Quality	7-7
Inspecting Location Readiness Using Access Point Data	7-7
Inspecting Location Quality Using Calibration Data	7-7
Verifying Location Accuracy	7-8
Using the Location Accuracy Tool to Conduct Accuracy Testing	7-8
Using Scheduled Accuracy Testing to Verify Accuracy of Current Location	7-8
Using On-demand Accuracy Testing to Test Location Accuracy	7-10
Using Chokepoints to Enhance Tag Location Reporting	7-11
Adding Chokepoints to Cisco WCS	7-11
Removing Chokepoints from the WCS Database and Map	7-15
Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting	7-16
Adding Wi-Fi TDOA Receivers to Cisco WCS	7-17
Removing Wi-Fi TDOA Receivers from Cisco WCS and Maps	7-19
Using Tracking Optimized Monitor Mode to Enhance Tag Location Reporting	7-19
Defining Inclusion and Exclusion Regions on a Floor	7-21
Guidelines	7-21
Defining an Inclusion Region on a Floor	7-21
Defining an Exclusion Region on a Floor	7-24
Defining a Rail Line on a Floor	7-26
Configuring a Location Template	7-28
Verifying a NMSP Connection to a Location Server	7-31

- Modifying Context-Aware Software Parameters 7-32
 - Editing Tracking Parameters 7-32
 - Editing Filtering Parameters 7-36
 - Editing History Parameters 7-38
 - Enabling Location Presence on a Location Server 7-38
 - Importing Asset Information 7-40
 - Exporting Asset Information 7-40
- Editing Location Parameters 7-41

CHAPTER 8

Monitoring Location Servers and Site 8-1

- Working with Alarms 8-2
 - Viewing Alarms 8-2
 - Assigning and Unassigning Alarms 8-3
 - Deleting and Clearing Alarms 8-3
 - Emailing Alarm Notifications 8-4
- Working with Events 8-4
- Working with Logs 8-5
 - Configuring Logging Options 8-5
 - Downloading Location Server Log Files 8-6
- Generating Reports 8-6
 - Creating a Location Server Utilization Report 8-6
 - Viewing Saved Utilization Charts 8-9
 - Viewing Scheduled Utilization Runs 8-9
- Monitoring Location Server Status 8-9
 - Viewing Location Server Current Information 8-9
- Monitoring Wireless Clients 8-10
 - Monitoring Wireless Clients Using Maps 8-10
 - Monitoring Wireless Clients Using Search 8-12
- Monitoring Tags 8-14
 - Monitoring Tags Using Maps 8-14
 - Monitoring Tags Using Search 8-16
 - Overlapping Tags 8-20
- Monitoring Chokepoints 8-21
- Monitoring Wi-Fi TDOA Receivers 8-23

CHAPTER 9

Performing Maintenance Operations 9-1

- Recovering Lost Password 9-2
- Recovering a Lost Root Password 9-2

Backing Up and Restoring Location Server Data	9-2
Backing Up Location Server Historical Data	9-3
Restoring Location Server Historical Data	9-3
Enabling Automatic Location Data Backup	9-4
Downloading Software to Location Servers	9-4
Manually Downloading Software	9-5
Configuring NTP Server	9-6
Defragmenting the Location Server Database	9-7
Rebooting the Location Server Hardware	9-8
Shutting Down the Location Server Hardware	9-8
Clearing the System Database	9-8



CHAPTER 1

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, page 1-2](#)
- [Viewing Location Data, page 1-3](#)
- [Event Notification, page 1-3](#)
- [Configuration and Administration, page 1-4](#)
- [Location Server Synchronization, page 1-5](#)
- [Location Planning and Verification, page 1-5](#)
- [Monitoring Capability, page 1-5](#)
- [Maintenance Operations, page 1-5](#)
- [System Compatibility, page 1-6](#)

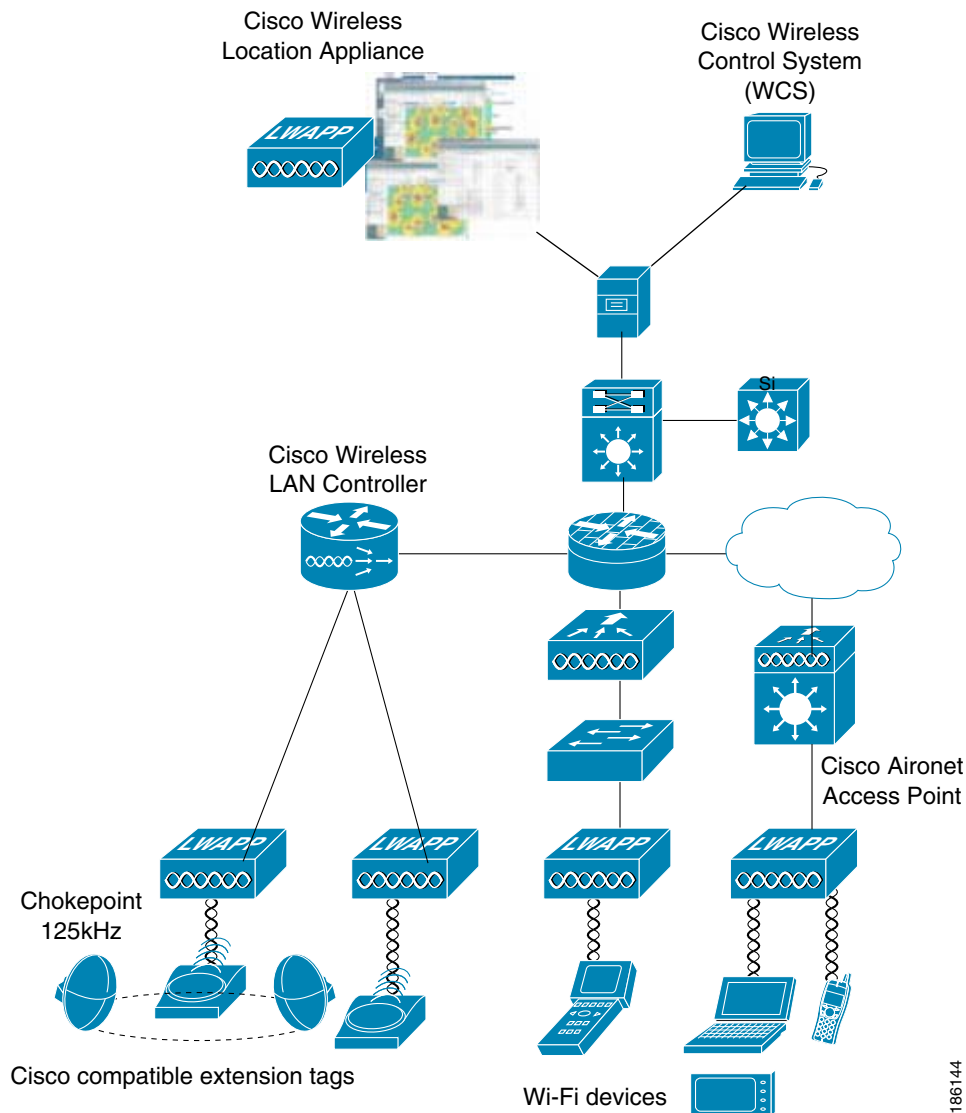
Location Appliance Functionality

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



186144

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:

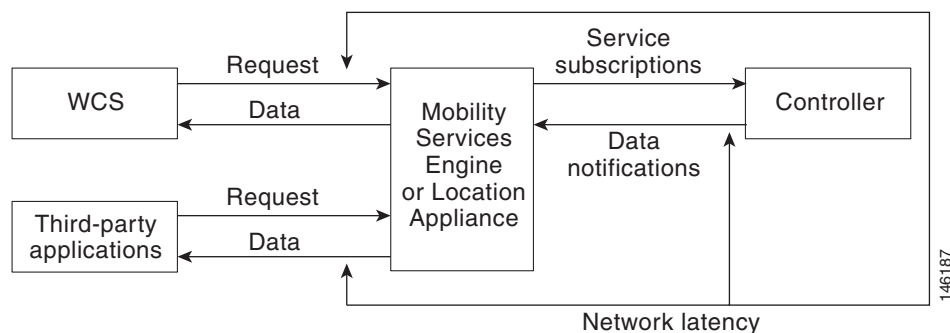
- Simple Object Access Protocol (SOAP)
- Simple Mail Transfer Protocol (SMTP) mail
- Simple Network Management Protocol (SNMP)
- SysLog



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, 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 5.1 to 6.0 but you cannot directly upgrade to release 6.0 from releases 1.1, 1.2, 2.0, 2.1, 3.0, 3.1 or 4.0.

**Note**

There is no release 3.2 or 5.0 for location appliances.



CHAPTER 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, page 2-2](#)
- [Deleting Location Servers from the Cisco WCS Database, page 2-4](#)

REVIEW DRAFT – CISCO CONFIDENTIAL

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 **Services > 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**. 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 Username 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.

The following ports are active on the location server:

- tcp 22: SSH port
- tcp 6100: Virtual frame buffer
- tcp 8001: Location server port
- udp 123: NTPD port (open after NTP configuration)
- udp 32768: Location internal port

- Step 9** Check the HTTPS enable check box to allow communication between the location server and Cisco WCS. Uncheck the check box to disable HTTPS.



Note Communication between the location server and third-party applications is done over HTTP. To operate over HTTP, leave the HTTPS enable check box unchecked.

- 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.

REVIEW DRAFT – CISCO CONFIDENTIAL**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](#).

REVIEW DRAFT – CISCO CONFIDENTIAL

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 **Services > 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)**. 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.
-



CHAPTER 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:

- [Synchronizing Cisco WCS and Location Servers, page 3-2](#)
- [Viewing Synchronization Information, page 3-6](#)

Synchronizing Cisco WCS and Location Servers

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** Choose **Services > 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**.
- Step 5** 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 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 09/07/09 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 2009
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 2009
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 Choose **Services > Synchronize Services** to display the Synchronize Cisco WCS and MSE(s) window.

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



Note The Switches tab is not supported for the location server.

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, choose **Administration > Background Tasks**.

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

Step 3 Click the **Mobility Service Synchronization** link and the Other Background Tasks > Mobility Service Synchronization window appears.

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

Step 5 To enable automatic synchronization, check the Auto Synchronization **Enable** 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, choose **Services > 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, choose **Services > 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.



CHAPTER 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, page 4-2](#)
- [Modifying NMSP Parameters, page 4-2](#)
- [Viewing Active Sessions on a System, page 4-4](#)
- [Viewing and Configuring Advanced Parameters, page 4-4](#)

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, choose **Services > 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.
Username	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 Note The following ports are in use on a location server in release 6.0: tcp 22: SSH port tcp 6100: Virtual frame buffer tcp 8001: Location server port udp 123: NTPD port (open after NTP configuration) udp 32768: Location internal port
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 the location server communicate over **MUST** be open (not blocked) on any firewall that exists between the controller and the location server.

To configure NMSP parameters, follow these steps:

- Step 1** In Cisco WCS, choose **Services > Mobility Services**.
- Step 2** Click the name of the location server whose properties you want to edit.
- Step 3** Choose **System > NMSP Parameters**. The configuration options appear.
- Step 4** Modify the NMSP parameters as appropriate. [Table 4-2](#) describes each parameter.

Table 4-2 NMSP Parameters

Parameter	Description
Echo Interval	How frequently an echo request is sent from a 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	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	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
- 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

To view active user sessions, follow these steps:

-
- Step 1** In Cisco WCS, choose **Services > Mobility Services**.
- Step 2** Click the name of the location server on which you want to view active sessions.
- Step 3** Choose **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**

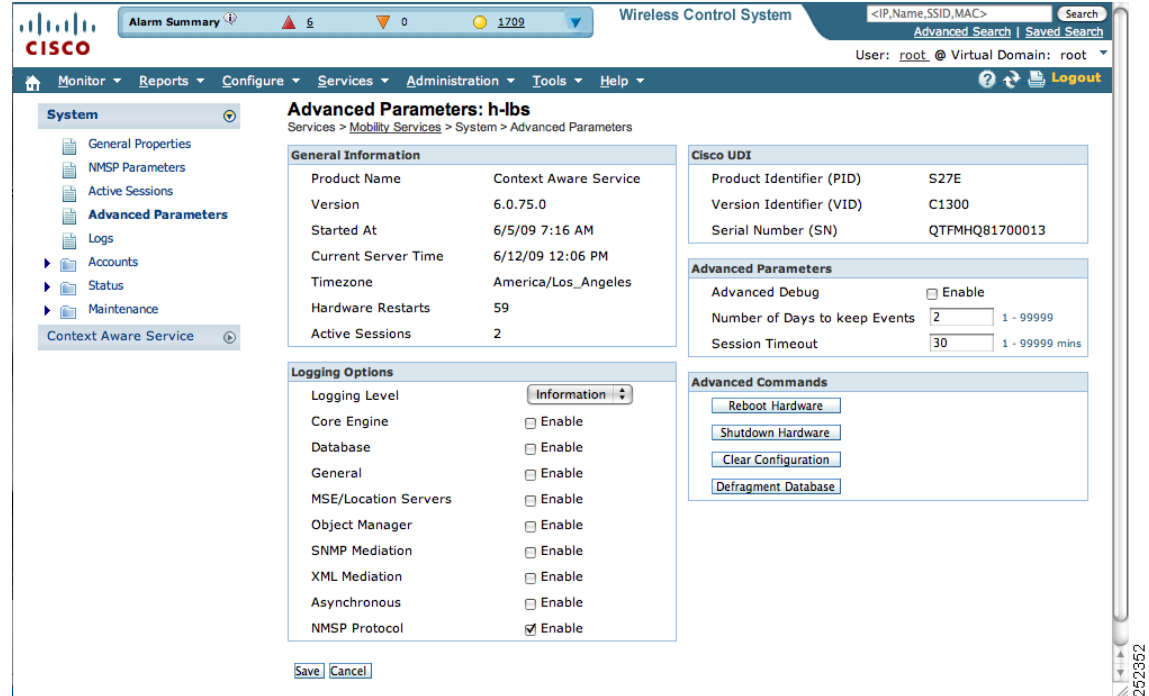
You can also initiate advanced commands such as a system reboot, a system shutdown, clearing the configuration file, and defragment the system database. Refer to the [“Initiating Advanced Commands” section on page 4-6](#) for information on these commands and when they should be used

Viewing Advanced Parameters Settings

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

-
- Step 1** In Cisco WCS, choose **Services > Mobility Services**.
- Step 2** Click the name of a location server to view its status.
- Step 3** Choose **System > 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, choose **Services > Mobility Services**.
- Step 2** Click the name of the location server that you want to configure.
- Step 3** Choose **System > 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, choose **Services > Mobility Services**.
- Step 2** Click the name of the location server that you want to configure.
- Step 3** Choose **System > Advanced Parameters**. The advanced parameters for the selected location server appears.
- Step 4** In the Advanced Parameters section, 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.

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.

Rebooting or Shutting Down a System

To reboot or shutdown a location server, follow these steps:

- Step 1** In Cisco WCS, choose **Services > Mobility Services**.
- Step 2** Click the name of a location server you want to reboot or shutdown.

- Step 3** Choose **System > Advanced Parameters**.
- Step 4** In the Advanced Commands section of the window (right), click the appropriate button (**Reboot Hardware** or **Shutdown Hardware**).
- Click **OK** in the confirmation pop-up window to initiate either the reboot or shutdown process. Click **Cancel** to stop the process.
-

Clearing the System Database

To clear the database of a location server, follow these steps:

- Step 1** In Cisco WCS, choose **Services > Mobility Services**.
- Step 2** Click the name of a location server for which you want to clear its database.
- Step 3** Choose **System > Advanced Parameters**.
- Step 4** In the Advanced Commands section of the window (right), click the **Clear Configuration** button.



Note The Clear Configuration command clears the database not the configuration file.

Click **OK** in the confirmation pop-up window to clear the location server database. Click **Cancel** to stop the process.

Defragmenting the Database

To defragment the location server database, follow these steps:

- Step 1** In Cisco WCS, choose **Services > Mobility Services**.
- Step 2** Click the name of a location server for which you want to defragment its database.
- Step 3** Choose **System > Advanced Parameters**.
- Step 4** In the Advanced Commands section of the window (right), click the **Defragment Database** button.
- Click **OK** in the confirmation pop-up window to initiate the process. Click **Cancel** to stop the process.
-



CHAPTER 5

Managing 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, page 5-2](#)
- [Managing Users, page 5-3](#)
- [Managing Host Access, page 5-5](#)

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, choose **Services > Mobility Services**.
 - Step 2** Click the name of the location server you want to edit.
 - Step 3** Choose **System > Accounts > Groups**.
 - Step 4** Select **Add Group** from the Select a command drop-down menu. Click **Go**.
 - Step 5** Enter the name of the group in the Group Name field.
 - Step 6** 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 7** 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, choose **Services > Mobility Services**.
 - Step 2** Click the name of the location server you want to edit.
 - Step 3** Choose **System > Accounts > Groups**.
 - Step 4** Check the check box(es) of the group(s) that you want to delete.
 - Step 5** Select **Delete Group** from the Select a command drop-down menu. Click **Go**.
 - Step 6** 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, choose **Services > Mobility Services**.
 - Step 2** Click the name of the location server you want to edit.
 - Step 3** Choose **System > Accounts > Groups**.
 - Step 4** Click the name of the group you want to edit.
 - Step 5** Modify the group name, password or permission (access) level as appropriate.
 - Step 6** 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, choose **Services > Mobility Services**.
 - Step 2** Click the name of the location server you want to edit.
 - Step 3** Choose **System > Accounts > Users**.
 - Step 4** Select **Add User** from the Select a command drop-down menu. Click **Go**.
 - Step 5** Enter the username in the Username field.
 - Step 6** Enter a password in the Password field.
 - Step 7** Enter the name of the group to which the user belongs in the Group Name field.

Step 8 Select a permission level 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 9 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, choose **Services > Mobility Services**.
 - Step 2** Click the name of the location server you want to edit.
 - Step 3** Click **System > Accounts > Users**.
 - Step 4** Check the check box(e)s of the user(s) that you want to delete.
 - Step 5** Select **Delete User** from the Select a command drop-down menu. Click **Go**.
 - Step 6** 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, choose **Services > Mobility Services**.
 - Step 2** Click the name of the location server you want to edit.
 - Step 3** Choose **System > Accounts > Users**.
 - Step 4** Click the name of the group that you want to edit.
 - Step 5** Make the desired changes to the Password, Group Name, and Permission fields.
 - Step 6** Click **Save** to apply your change.
-

Viewing Active User Sessions

To view active user sessions, follow these steps:

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

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

Step 3 Choose **System > 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, choose **Services > Mobility Services**.

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

Step 3 Choose **Accounts > Host Access**.

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

Step 5 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 6 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 7 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 8 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 9 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 10 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, choose **Services > Mobility Services**.

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

Step 3 Choose **Accounts > Host Access**.

Step 4 Check the check box(es) of the host access record(s) that you want to delete.

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

Step 6 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, choose **Services > Mobility Services**.
 - Step 2** Click the name of the location server you want to edit.
 - Step 3** Click **Accounts > Host Access**.
 - Step 4** Click the IP and mask address of the host access record that you want to modify.
 - Step 5** Make the required changes to the Permit, Priority, Start Access, and End Access fields.
 - Step 6** Click **Save** to apply your changes.
-



CHAPTER 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, page 6-2](#)
- [Adding, Deleting, and Testing Event Definitions, page 6-2](#)
- [Viewing Event Notification Summary, page 6-7](#)
- [Enabling Notifications and Configuring Notification Parameters, page 6-8](#)
- [Notification Message Formats, page 6-11](#)

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, choose **Services > Context Aware Notifications**.
 - Step 2** Choose **Notification Settings** (left- panel).
 - Step 3** From the Select a command drop-down menu, select **Add Event Group**, Click **Go**.
 - Step 4** Enter the name of the group in the Group Name field.
 - Step 5** Click **Save**.

The new event group appears in the Event Settings window.

Deleting Event Groups

To delete an event group, follow these steps:

-
- Step 1** In Cisco WCS, choose **Services > Context Aware Notifications**
 - Step 2** Select the event group to delete by checking its corresponding check box.
 - Step 3** From the Select a command drop-down menu, select **Delete Event Group(s)**, and click **Go**.
 - Step 4** In the panel that appears, click **OK** to confirm deletion.
 - Step 5** Click **Save**.
-

Adding, Deleting, and Testing Event Definitions

An event definition contains information about the condition that caused the event, the assets to which the event applies, and the event notification 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, choose **Services > Context Aware Notifications**.
 - Step 2** Choose **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 Change** from the Condition Type drop-down menu, proceed to Step c.

If you chose **Emergency** from the Condition Type drop-down menu, click the button next to the appropriate emergency (any, panic button, tampered, detached, 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 (Services > Notifications > Settings > *Event Group Name*).

Deleting an Event Definition

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

- Step 1** In Cisco WCS, choose **Services > Context Aware Notifications**.
 - Step 2** Choose **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, choose **Services > Synchronize Services**.
- 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, choose **Services > Context Aware Notifications**.
 - Step 2** Choose **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, choose **Services > Context Aware Notifications**.

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



Note Emergency and chokepoint notifications are 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.

Enabling Notifications and Configuring Notification Parameters

Enabling Notifications

You can use Cisco WCS to define and enable user-configured conditional notifications and northbound notifications.

User-configured conditional notifications manage which notifications the mobility services engine sends to Cisco WCS. Refer to the [“Adding, Deleting, and Testing Event Definitions”](#) section on page 6-2.

Northbound notifications define which tag notifications the mobility services engine sends to third-party applications. Client notifications are not forwarded. By enabling northbound notifications in Cisco WCS, the following five event notifications are sent: chokepoints, telemetry, emergency, battery, and vendor data. To send a tag location, you must enable that notification separately.

The mobility services engine sends all northbound notifications in a set format. Details are available on the Cisco developers support portal at:

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

Filtering Northbound Notifications

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

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



Note

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

You can filter on six northbound parameters as summarized below:

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

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

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

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

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

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

Configuring Notification Parameters

You can limit the rate at which a location server generates notifications, set a maximum queue size for notifications, and set a retry limit for notifications with in a certain period.

Notification parameter settings apply to user-configurable conditional notifications and northbound notifications except as noted in [Table 6-1](#).



Note

Modify notification parameters only when you expect the location server to send a large number of notifications or when notifications are not being received.

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

- Step 1** In Cisco WCS, choose **Services > Mobility Services**.
- Step 2** Click the name of the location server you want to configure.
- Step 3** Choose **Context Aware Service > Advanced > Notification Parameters** to display the configuration options (see [Figure 6-1](#)).

Figure 6-1 *Advanced > Notification Parameters Window*

The screenshot shows the Cisco WCS configuration interface for 'Notification Parameters: -lbs'. The breadcrumb trail is 'Services > Mobility Services > Context Aware Service > Advanced > Notification Parameters'. The left sidebar shows the navigation tree with 'Notification Parameters' selected. The main content area is divided into 'Northbound Notifications' and 'Advanced' sections.

Northbound Notifications

- Northbound Notifications: Enable
- Tags
 - Chokepoints
 - Telemetry
 - Emergency
 - Battery Level
 - Vendor Data
- Include tag location information in notification

Advanced

Field	Value	Range
Rate Limit	0	0 - 9999999 msec
Queue Limit	10000	1 - 99999
Retry Count	1	0-60
Refresh Time	60	0 - 99999 mins
Notifications Dropped	0	

At the bottom, there are 'Save' and 'Cancel' buttons.

- Step 4** Check the **Enable Northbound Notifications** check box to enable the function.
- Step 5** Check the **Tags** check box to send tag notifications to third-party applications (northbound).



Note To limit the types of northbound notifications sent for tags, edit the *aes-config.xml* file. Refer to the [“Filtering Northbound Notifications”](#) section on page 6-9.

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




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

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

- Step 8** Select the transport type from the drop-down menu.
- Step 9** To modify the notification parameter settings, enter the new value in the appropriate field in the Advanced section of the window.

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 generates notifications. A value of 0 (default) means that the mobility services engine generates notifications as fast as possible (Northbound notifications only).
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.
	 <p>Note The location server does not store events in its database.</p>
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 10** 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 qualified 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

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

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 6-11).

```
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



CHAPTER 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, page 7-2](#)
- [Creating and Applying Calibration Models, page 7-3](#)
- [Inspecting Location Readiness and Quality, page 7-7](#)
- [Verifying Location Accuracy, page 7-8](#)
- [Using Chokepoints to Enhance Tag Location Reporting, page 7-11](#)
- [Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting, page 7-16](#)
- [Using Tracking Optimized Monitor Mode to Enhance Tag Location Reporting, page 7-19](#)
- [Defining Inclusion and Exclusion Regions on a Floor, page 7-21](#)
- [Defining a Rail Line on a Floor, page 7-26](#)
- [Configuring a Location Template, page 7-28](#)
- [Modifying Context-Aware Software Parameters, page 7-32](#)
- [Editing Location Parameters, page 7-41](#)

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, choose **Monitor > Maps**.
- Step 2** **Click** the appropriate map name from the list that displays.
- If you selected a building map, select a floor map from the Building View window.
- A map appears showing placement of all installed elements (access points, clients, tags) and their relative signal strength (RSSI). RSSI is indicated by the colored rings that surround the element. To identify the exact RSSI for that element, refer to the RSSI legend (color bar) at the top of the page.
- 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 **Shift** 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 appears.



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** (left panel, bottom) 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 your floor layout, you can create and apply a calibration model to your floor that better represents its attenuation characteristics. In environments in which many floors share common attenuation characteristics (such as in a library), one calibration model can be created and then applied to floors with the same physical layout and same deployment.

You can collect data for a calibration using one of two methods:

- Data point collection—Selects calibration points and calculates their coverage area one location at a time.
- Linear point collection—Selects a series of linear paths and then calculates the coverage area as you traverse the path. This approach is generally faster than data point collection. You can also employ data point collection to augment location data missed by the linear paths.

**Note**

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

**Note**

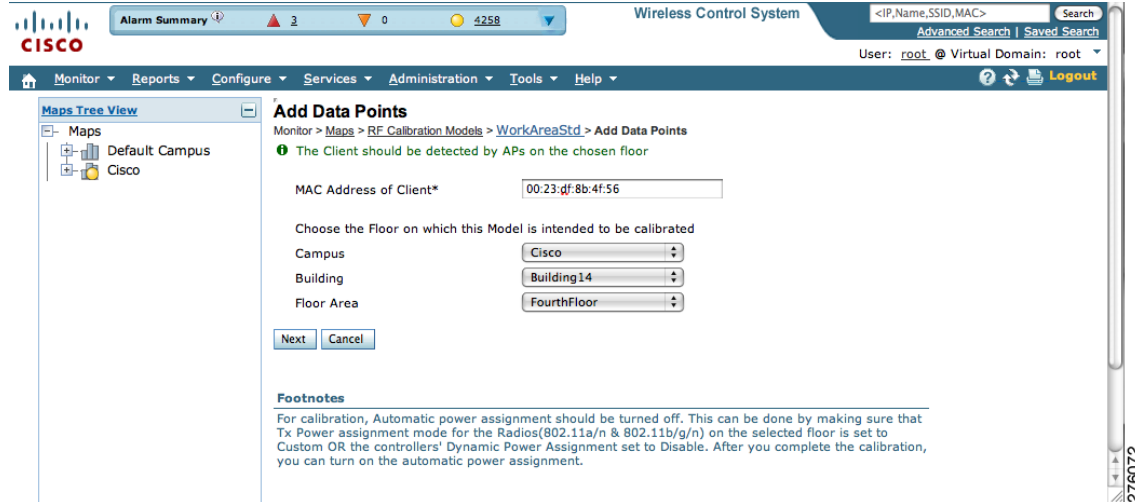
A client device that supports both 802.11a/n and 802.11b/g/n radios is recommended to expedite the calibration process for both spectrums.

Use a laptop or other wireless device to open a browser to Cisco WCS and perform the calibration process.

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

- Step 1** Choose **Monitor > Maps** and choose **RF Calibration Models** from the Select a command drop-down menu. Click **Go**.
- Step 2** Select **Create New Model** from the Select a command drop-down menu. Click **Go**.
- Step 3** Assign a name to the model. Click **OK**. The new model name appears along with the other RF calibration models, but its status is listed as *Not Yet Calibrated*.
- Step 4** To start the calibration process, click the **model name** link. A new window appears which showing the details of the new mode.
- Step 5** Select **Add Data Points** from the Select a command drop-down menu. Click **Go**.
- Step 6** If this process is being performed from a mobile device connected to WCS through the Cisco Centralized Architecture (CCA), 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**.

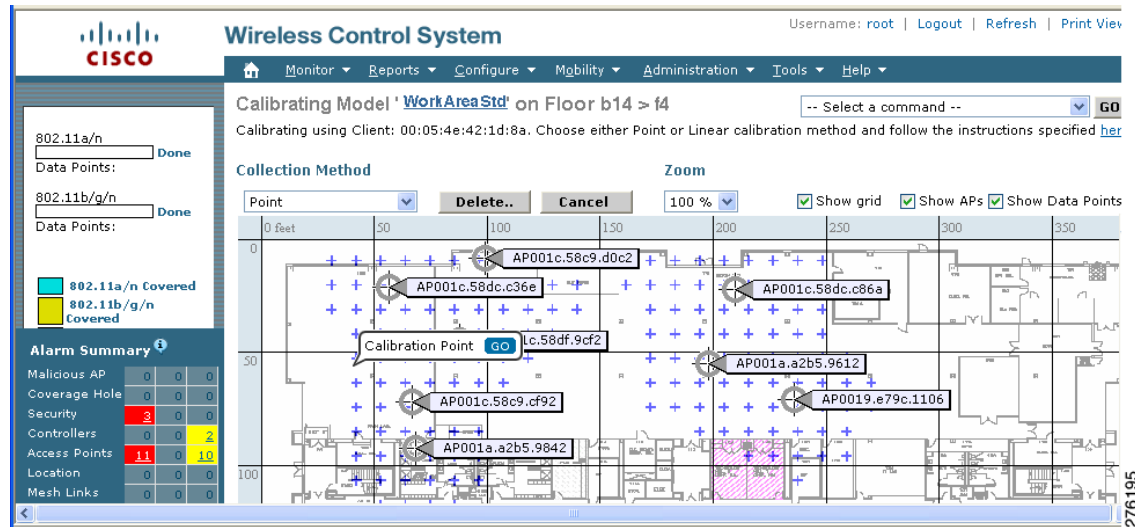
Figure 7-1 Starting to Calibrate



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

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

Figure 7-2 Positioning Calibration Points Window



- a. To do a point collection of data for the calibration, follow these steps:
 1. Select **Point** from the Collection Method drop-down menu and check the Show Data points check box if not already checked. A calibration point pop-up 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 detected evenly by all access points in the vicinity.

3. When the data collection is complete for a selected data point and the coverage area is plotted on the map, move the calibration point pop-up to another data point and click **Go**.



Note The coverage area plotted on the map is color-coded and corresponds with the specific wireless LAN standard used to collect that data (see legend at left). Additionally, the progress of the calibration process is indicated by two status bars above the legend, one for 802.11a/n and one for 802.11b/g/n.



Note To delete data points, click **Delete** and move the black square that appears over the appropriate data points. Resize the square as necessary by 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*.



Note The calibration status bar indicates data collection for the calibration as *done*, after roughly 50 distinct locations and 150 measurements have been gathered. For every location point saved in the calibration process, more than one data point is gathered. The progress of the calibration process is indicated by two status bars above the legend, one for 802.11b/g/n and one for 802.11a/n.

- b. To do a linear collection of data for the calibration, follow these steps:
 1. Select **Linear** from the Collection Method drop-down menu and check the **Show Data points** check box if not already checked. A line appears on the map with both Start and Finish pop-ups.
 2. Position the tip of the Start pop-up at the starting data point.
 3. Position the Finish pop-up at the ending data point.
 4. Position yourself with your laptop at the starting data point and click **Go**. Walk steadily towards the end point along the defined path. A panel displays (left) 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, click **Delete** and move the black square that appears over the appropriate data points. Resize the square as necessary by pressing **Ctrl** and moving the mouse.

Figure 7-3 Linear Data Collection Window

Wireless Control System Username: root | Logout | Refresh | Print View

Monitor Reports Configure Mobility Administration Tools Help

Calibrating Model 'WorkAreaStd' on Floor b14 > f4 -- Select a command -- GO

Calibrating using Client: 00:05:4e:42:1d:8a. Choose either Point or Linear calibration method and follow the instructions specified [here](#)

Collection Method Linear Zoom 100% Show grid Show APs Show Data Points

Start GO Finish

AP001c.58c9.d0c2
AP001c.58dc.c36e
AP001c.58df.9cf2
AP001c.58c9.cf92
AP001a.a2b5.9842
AP001c.58dc.c86a
AP001a.a2b5.9612
AP0019.e79c.1106

802.11a/n Done
Data Points: 0

802.11b/g/n Done
Data Points: 72

802.11a/n Covered
802.11b/g/n Covered
802.11a/b/g/n Covered
Suggested Location
Visited Location

Debug Only Info
802.11a/n Model
Coverage: 3.6, -46.0
Location: -3.3, -46.0
802.11b/g/n Model

Alarm Summary			
Malicious AP	0	0	0
Coverage Hole	0	0	0
Security	3	0	0
Controllers	0	0	2
Access Points	11	0	10
Location	0	0	0
Mesh Links	0	0	0
WCS	0	0	0

**Note**

The coverage area is color-coded and corresponds with the specific wireless LAN standard (802.11a/n, 802.11b/g/n, or 802.11a/b/g/n) used to collect that data (See legend at left).

- 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. Refer to [Step 8 a](#).

- Step 9** To calibrate the data points, click the name of the calibration model at the top of the window. The main screen for that model appears.
- Step 10** Select **Calibrate** from the Select a command drop-down menu and click **Go**.
- Step 11** Click **Inspect Location Quality** when calibration completes. A map 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 are determined using the specific collected attenuation data from the calibration model.

Inspecting Location Readiness and Quality

You can configure Cisco WCS to verify the ability of 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. 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, choose **Monitor > Maps**.

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

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

**Note**

If RSSI is not displayed, you can enable AP Heatmaps on the Floor Settings panel (left).

**Note**

If clients, 802.11 tags, and access points are not displayed, verify that their respective check boxes are checked in the Floor Settings panel.

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, choose **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 **Inspect Location Quality** found under the Calibration Floors heading.
A color-coded map noting percentage of location errors appears.



Note You can modify the distance selected to see the effect on the location errors.

Verifying Location Accuracy

By verifying for location accuracy, you are ensuring that the existing access point deployment can estimate the true location of an element within 10 meters at least 90% of the time.

You can analyze the location accuracy of non-rogue and rogue clients and asset tags by using the Accuracy Tool.

The Accuracy Tool enables you to run either a scheduled or on-demand location accuracy test. Both tests are configured and executed through a single window.

Using the Location Accuracy Tool to 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.

Using Scheduled Accuracy Testing to Verify Accuracy of Current Location

To configure a scheduled accuracy test, follow these steps:

-
- Step 1** In Cisco WCS, choose **Tools > Location Accuracy Tool**.
- Step 2** Select **New Scheduled Accuracy Test** from the Select a command drop-down menu. Click **Go**.
- Step 3** Enter a Test Name.
- Step 4** Select an area type from the drop-down menu.
- Step 5** Campus is configured as Root Area, by default. There is no need to change this setting.

- Step 6** Select the building from the drop-down menu.
- Step 7** Select the floor from the drop-down menu.
- Step 8** Select the begin and end time of the test by entering the days, hours, and minutes. Hours are entered using a 24-hour clock.
-  **Note** When entering the test start time, be sure to allow enough time to position testpoints on the map prior to the test start.
- Step 9** Select the destination point for the test results. You can have the report emailed to you or download the test results from the Accuracy Tests > Results window. Reports are in PDF format.
-  **Note** If you select the email option, a SMTP Mail Server must first be defined for the target email address. Choose **Administrator > Settings > Mail Server Configuration** to enter the appropriate information.
- Step 10** Click **Position Testpoints**. The floor map appears with a list of all clients and tags on that floor with their MAC addresses.
- Step 11** Click the check box next to each client and tag for which you want to check the location accuracy. When you check the MAC address check box, 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.
-  **Note** Only the actual location icon can be dragged.
- Step 13** Click **Save** when all elements are positioned. A panel appears confirming successful accuracy testing.
- Step 14** Click **OK** to close the confirmation panel. You are returned to the Accuracy Tests summary window.
-  **Note** The accuracy test status displays as *Scheduled* when the test is about to execute. A status of *In Progress* appears when the test is in running and *Idle* when the test is complete. A *Failure* status appears when the test is not successful.
- Step 15** To view the results of the location accuracy test, click the test name and then click **Download** on the page that appears.

The Scheduled Location Accuracy Report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges.
- An error distance histogram
- A cumulative error distribution graph
- An error distance over time graph
- A summary by each MAC address whose location accuracy was tested noting its actual location, error distance and a map showing its spatial accuracy (actual vs. calculated location) and error distance over time for each MAC.

Using On-demand Accuracy Testing to Test Location Accuracy

An On demand Accuracy Test is run when elements are associated but not pre-positioned. On demand testing allows you to test the location accuracy of clients and tags at a number of different locations. It is generally used to test the location accuracy for a small number of clients and tags.

To run an On-demand Accuracy Test, follow these steps:

- Step 1** Choose **Tools > Location Accuracy Tool**.
- Step 2** Select **New On demand Accuracy Test** from the Select a command drop-down menu.
- Step 3** Enter a test name.
- Step 4** Select the area type from the drop-down menu.
- Step 5** Campus is configured as Root Area, by default. There is no need to change this setting.
- Step 6** Select the building from the drop-down menu.
- Step 7** Select the floor from the drop-down menu.
- Step 8** 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 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 collecting accuracy data.
- Step 13** Click **Stop** to finish collecting accuracy data.



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

- Step 14** Repeat [Step 10](#) to [Step 13](#) for each testpoint that you want to plot on the map.
- Step 15** Click **Analyze** when you are finished mapping the testpoints.

Step 16 Select the **Results** tab on the panel that appears.

The On-demand Accuracy Report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges.
- An error distance histogram
- A cumulative error distribution graph

Step 17 To download accuracy test logs from the Accuracy Tests summary page:

- a. Check the listed test check box and select either **Download Logs** or **Download Logs for Last Run** from the Select a command menu.
- b. Click **Go**.

The Download Logs option downloads the logs for all accuracy tests for the selected test(s).

The Download Logs for Last Run option downloads logs for only the most recent test run for the selected test(s).

Using Chokepoints to Enhance Tag Location Reporting

Installing chokepoints (also known as *exciters*) provides enhanced location information for active RFID tags. When an active Cisco CX version 1 compliant RFID tag enters the range of a chokepoint, it is stimulated by the chokepoint. The MAC address of this chokepoint is then included in the next beacon sent by the stimulated tag. All access points that detect this tag beacon then forward the information to the controller and location server.

Using chokepoints in conjunction with active Cisco CX compliant tags provides immediate location information on a tag and its asset. When a Cisco CX tag moves out of the range of a chokepoint, its subsequent beacon frames do not contain any identifying chokepoint information. Location determination of the tag defaults to the standard calculation methods based on RSSIs reported by access point associated with the tag.



Note

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

Adding Chokepoints to Cisco WCS

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

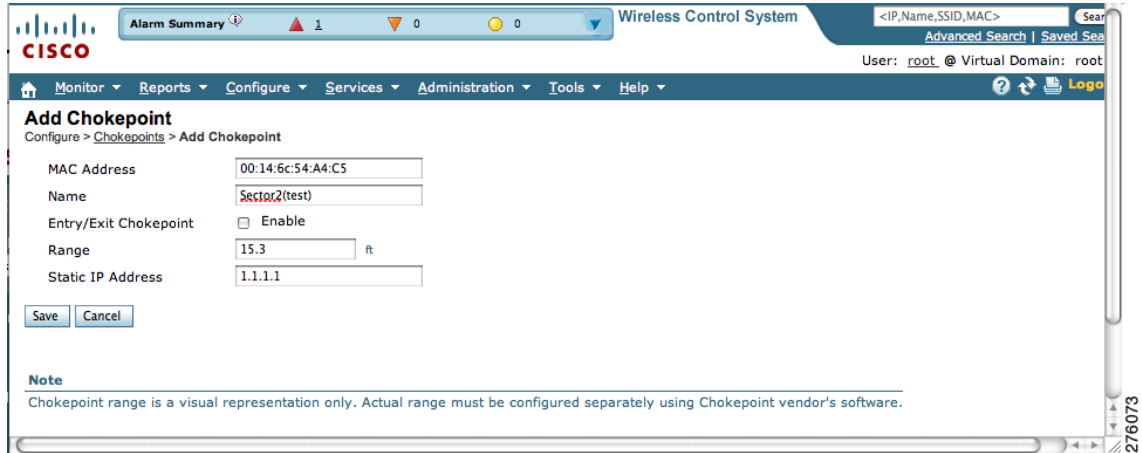
Step 1 Choose **Configure > Chokepoints** from the main menu (top).

The Chokepoints summary window appears.

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

The Add Chokepoint entry screen appears (Figure 7-4).

Figure 7-4 Add Chokepoint Window



Alarm Summary ▲ 1 ▼ 0 ● 0 Wireless Control System <IP,Name,SSID,MAC> Search
Advanced Search | Saved Searches
User: root @ Virtual Domain: root

Monitor Reports Configure Services Administration Tools Help

Add Chokepoint

Configure > Chokepoints > Add Chokepoint

MAC Address

Name

Entry/Exit Chokepoint Enable

Range ft

Static IP Address

Note
Chokepoint range is a visual representation only. Actual range must be configured separately using Chokepoint vendor's software.

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



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

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

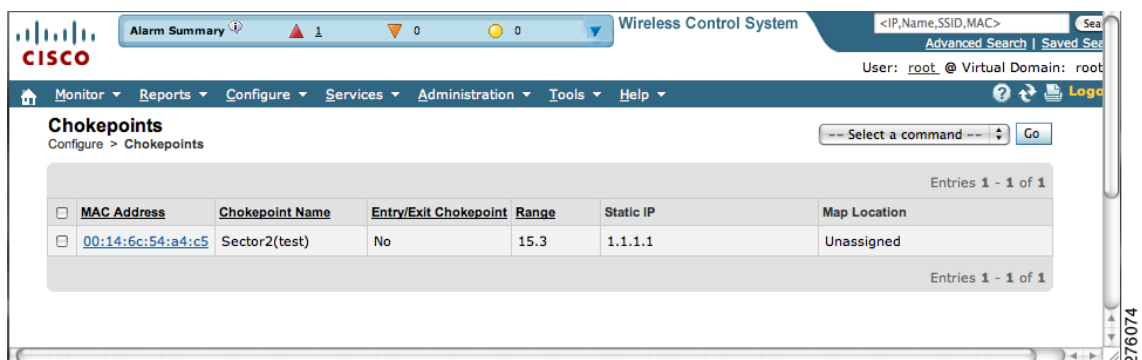


Tip You generally enable a chokepoint that is placed near an exit to function as an entry/exit (perimeter) chokepoint. When a client or tag shows strong RSSIs on two floors, you can check for the last perimeter chokepoint that the tag or client passed to determine the current floor location of that client or tag.

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

The Chokepoints summary window appears with the new chokepoint entry listed (see [Figure 7-5](#)).

Figure 7-5 Chokepoints Summary Window



Alarm Summary ▲ 1 ▼ 0 ● 0 Wireless Control System <IP,Name,SSID,MAC> Search
Advanced Search | Saved Searches
User: root @ Virtual Domain: root

Monitor Reports Configure Services Administration Tools Help

Chokepoints

Configure > Chokepoints

Entries 1 - 1 of 1

<input type="checkbox"/>	MAC Address	Chokepoint Name	Entry/Exit Chokepoint	Range	Static IP	Map Location
<input type="checkbox"/>	00:14:6c:54:a4:c5	Sector2(test)	No	15.3	1.1.1.1	Unassigned

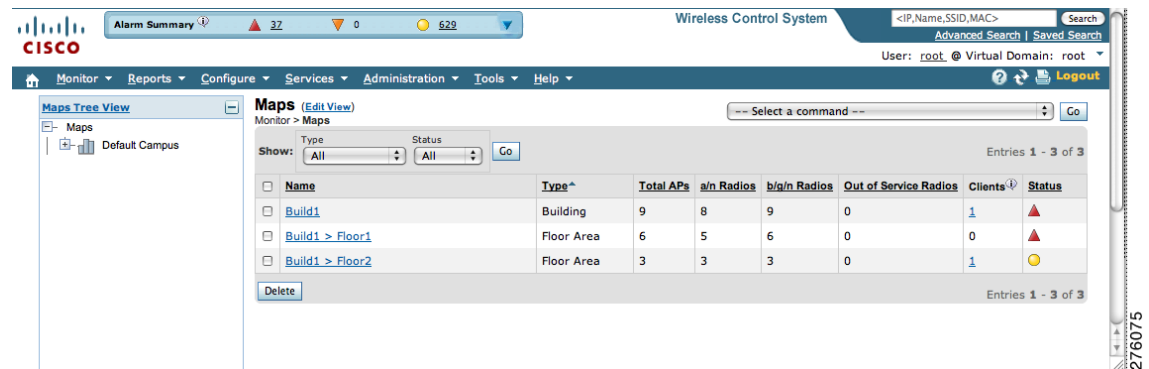
Entries 1 - 1 of 1



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

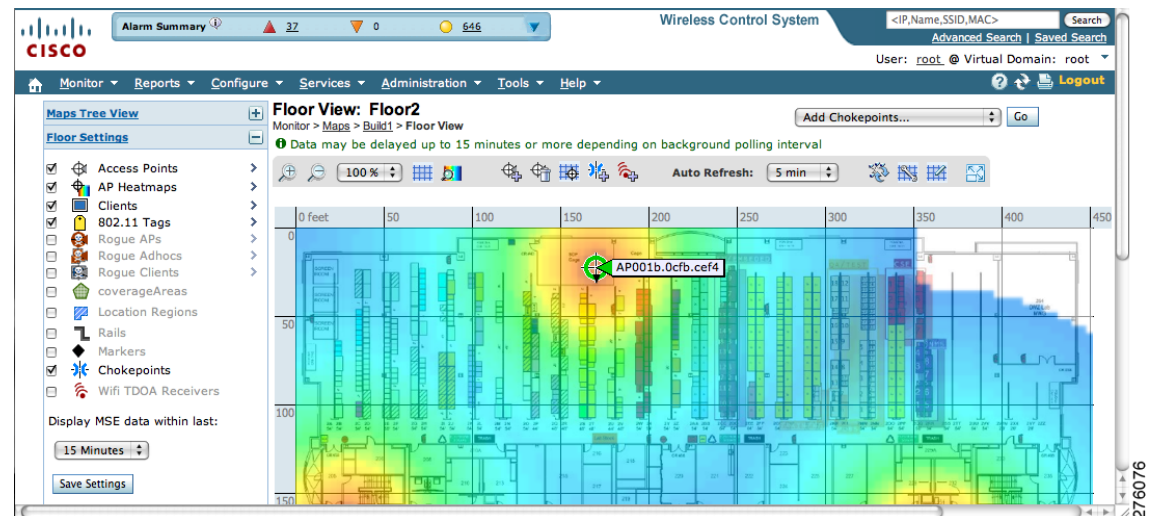
Step 6 To add the chokepoint to a map, choose **Monitor > Maps** (Figure 7-6).

Figure 7-6 Monitor > Maps Window



Step 7 At the Maps window, select the link (such as *Build1 > Floor2*) that corresponds to the floor location of the chokepoint. The floor map appears (see Figure 7-7).

Figure 7-7 Selected Floor Map



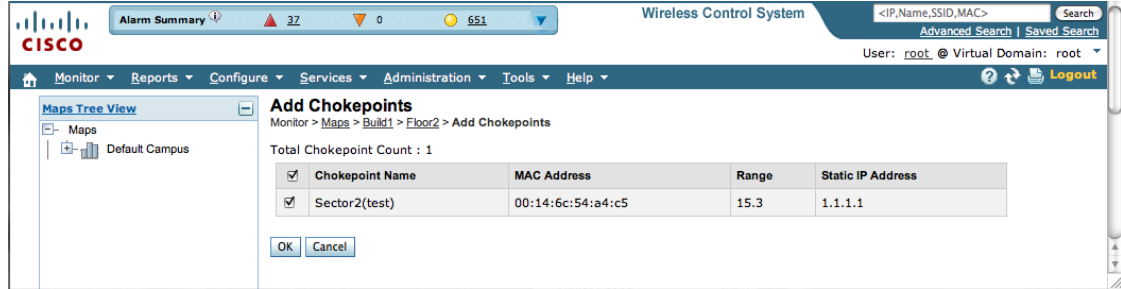
Step 8 Select **Add Chokepoints** from the Select a command menu. Click **Go**.

The Add Chokepoints summary window appears (see 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

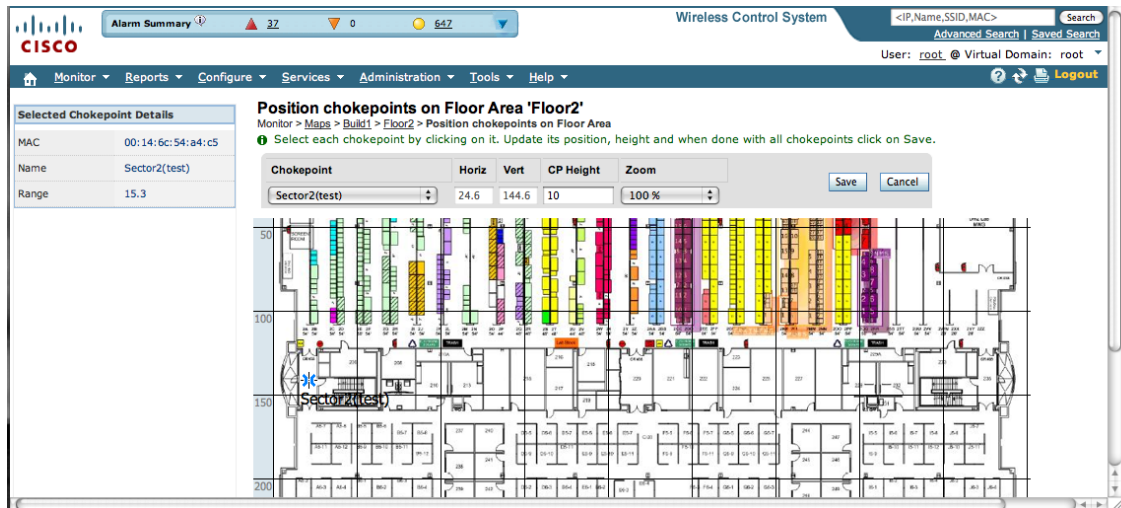


Step 9 Check the check box next to the chokepoint to be added to the map. Click **OK**.

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 (see 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.

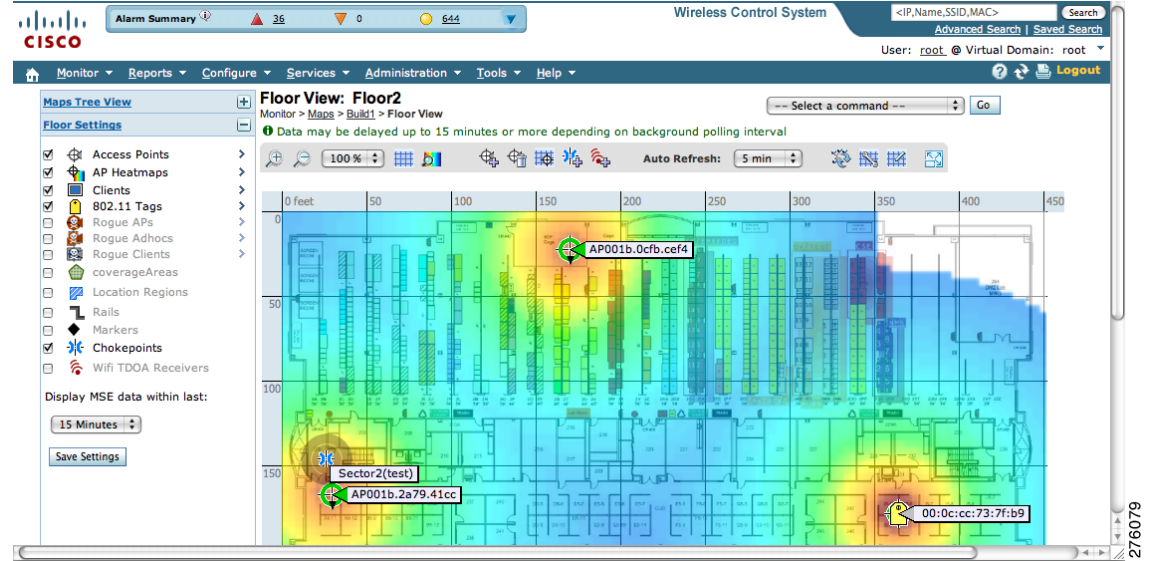
Step 11 Click **Save** when icon is correctly placed on the map.

The floor map reappears with the added chokepoint (see Figure 7-10).



Note If the chokepoint does not appear on the map, click the **Chokepoints** check box in the Floor Settings panel (left). Do not select **Save Settings** in the Floor Settings panel unless you want to save this display criteria for all maps.

Figure 7-10 New Chokepoint Displayed on Floor Map



Note Name, range, entry/exit chokepoint: (*yes* or *no*), and static IP address of the chokepoint appear when you pass a mouse over its map icon



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

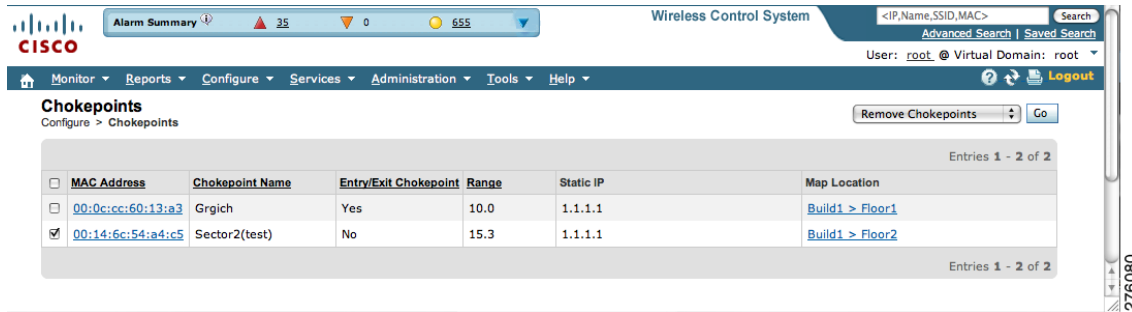
Removing Chokepoints from the WCS Database and Map

You can remove one or more chokepoints at a time.

To delete a chokepoint, follow these steps:

- Step 1** Choose **Configure > Chokepoints**. The Chokepoints window appears.
- Step 2** Check the check box next to the chokepoint(s) to be deleted.
- Step 3** Select **Remove Chokepoints** from the Select a command drop-down menu. Click **Go** (see Figure 7-11).

Figure 7-11 Removing a Chokepoint



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

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

Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting

The Wi-Fi TDOA receiver is an external system designed to receive signals transmitted from a tagged, tracked asset. These signals are then forwarded to the location server for used in calculating location of a tagged asset. TDOA receivers use the Time Difference of Arrival (TDOA) method to calculate tag location. TDOA uses data from a minimum of three TDOA receivers to generate a tagged asset's location.



Note

If a TDOA receiver is not in use, then the location calculations for tags are generated using RSSI readings from access points.

Before using a TDOA receiver within the Cisco Unified Wireless Network, you must:

1. Have a location appliance active in the network.
Refer to [Chapter 3, “Adding and Deleting Location Servers”](#) for details on adding a location appliance.
2. Add the TDOA receiver to the Cisco WCS database and map.
Refer to [Adding Chokepoints to Cisco WCS, page 7-11](#).
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

After you add TDOA receivers to Cisco WCS maps and synchronize, use the *AeroScout System Manager* application rather than Cisco WCS to modify the TDOA receiver configuration.

**Note**

For more details on configuration options, refer to the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine Users Guide* at the following link: <http://support.aeroscout.com>.

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

- Step 1** In Cisco WCS, choose **Configure > WiFi TDOA Receivers**. The WiFi TDOA Receivers summary window appears.
- Step 2** From the Select a command menu, 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 WiFi TDOA Receivers summary window appears with the new TDOA receiver entry listed.

**Note**

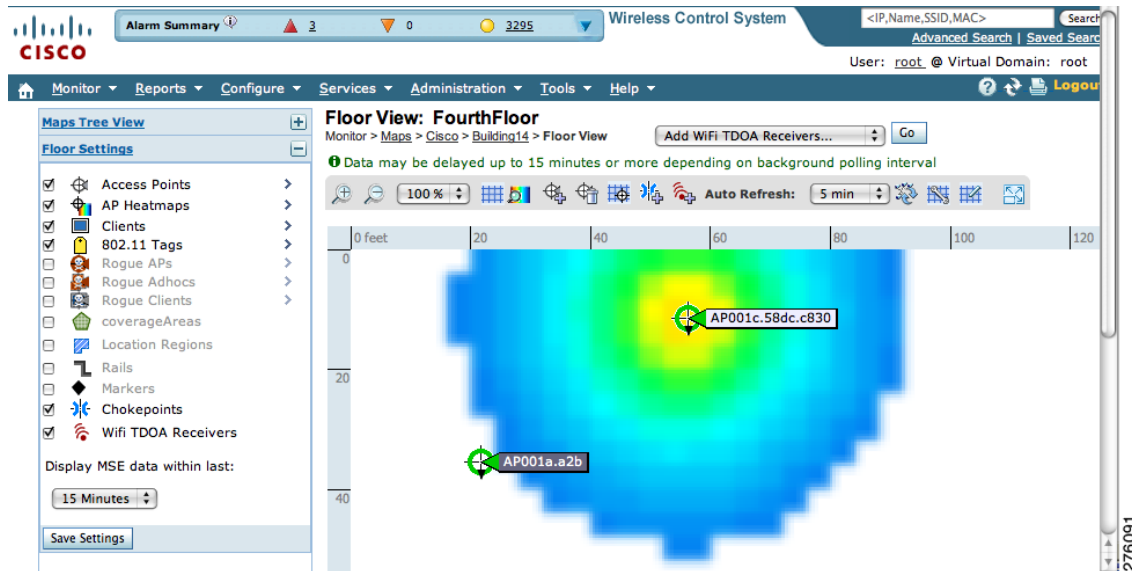
After you add the TDOA receiver to the database, you can place the TDOA receiver on the appropriate WCS floor map. To do so, continue with [Step 5](#).

- Step 5** To add the TDOA receiver to a map, choose **Monitor > Maps**.
- Step 6** At the Maps window, select the link that corresponds to the floor location of the TDOA receiver. The floor map appears.
- Step 7** Check the **WiFi TDOA Receivers** check box in the Floor Settings panel (left), if not already checked. This ensures that TDOA receivers display on the map (see [Figure 7-12](#)).

**Note**

Click **Save Settings** to display TDOA receivers in all maps (default setting).

Figure 7-12 Monitor > Maps > WiFi TDOA Receivers Window



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

The Add WiFi TDOA Receivers summary window appears.

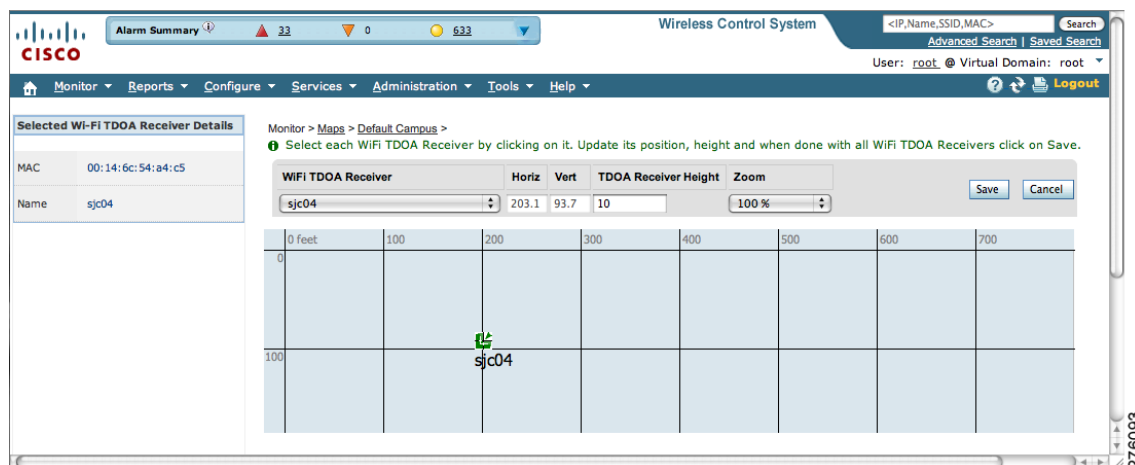


Note The WiFi TDOA Receivers summary window lists all recently added TDOA receivers that are in the database but not yet mapped.

Step 9 Check the check box next to each TDOA receiver to add it to the map. Click **OK**.

A map appears with a TDOA receiver icon in the top-left corner. You are now ready to place the TDOA receiver on the map (see Figure 7-13).

Figure 7-13 Placing WiFi TDOA Receiver on the Map



Step 10 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 11 After placing the TDOA receiver, enter the height of the receiver in the sensor height field.

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

The floor heat map reappears with the added TDOA receiver.



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

Removing Wi-Fi TDOA Receivers from Cisco WCS and Maps

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

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

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

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

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

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

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

Using Tracking Optimized Monitor Mode to Enhance Tag Location Reporting

To optimize monitoring and location calculation of tags, you can enable TOMM on up to four channels within the 2.4-GHz band (802.11b/g radio) of an access point. This allows you to focus channel scans only on those channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

You must enable monitor mode at the access point level before you can enable TOMM and assign monitoring channels on the 802.11 b/g radio of the access point.

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

- a. Choose **Configure > Access Point > AP Name**.
- b. Select **Monitor** as the AP Mode.



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

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

- a. After enabling monitor mode at the access point level, choose **Configure > Access Points**.
- b. At the Access Points summary window, select the **802.11 b/g Radio** link for the access point on which monitor mode is enabled.
- c. At the Radio details window, disable **Admin Status** by unchecking the check box. This disables the radio (see [Figure 7-14](#)).

Figure 7-14 *Configure > Access Point > 802.11b/g Window*

The screenshot displays the configuration page for a radio in the Cisco Wireless Control System. The breadcrumb trail is **Configure > Access Points > AP001a.a2b > Radio Detail**. The page is divided into several sections:

- General:** AP Name (AP001a.a2b), AP Base Radio MAC (00:1a:30:c1:fc:a0), Admin Status (unchecked), Controller (172.19.35.50), Site Config ID (0).
- Antenna:** Antenna Type (Internal), Antenna Diversity (Enabled), External Antenna (AJAX-OMNI), Antenna Gain (4.0), Current Gain (dBm) (4.0).
- RF Channel Assignment:** Current Channel (Scanning).
- Tx Power Level Assignment:** Current Tx Power Level (Not Applicable).
- Tracking Optimized Monitor Mode:** Enable TOMM (checked), Channel 1 (1), Channel 2 (6), Channel 3 (9), Channel 4 (11).
- Performance Profile:** A link to view/edit performance profile parameters.

A **Save** button is located at the bottom left of the configuration area.

- d. Check the Enable TOMM (Tracking Optimized Monitor Mode) check box.
- e. Select up to four channels (Channel 1, Channel 2, Channel 3, Channel 4) on which you want the access point to monitor tags.



Note You can configure fewer than four channels for monitoring. To eliminate a monitoring channel, select **None** from the channel drop-down menu.

- f. Click **Save**.
- g. At the Radio parameters window, re-enable the radio by checking the **Admin Status** check box.
- h. Click **Save**. The access point is now configured as a TOMM access point.
The AP Mode appears as Monitor on the **Monitor > Access Points** window.

Defining Inclusion and Exclusion Regions on a Floor

To further refine location calculations on a floor, you can define the 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

Consider the following when configuring exclusion and inclusion areas:

- Inclusion and exclusion areas can be any polygon shape and must have at least three points.
- You can define only one inclusion region on a floor. By default, an inclusion region is defined for each floor when it is added to Cisco WCS. The inclusion region is indicated by a solid aqua line and generally outlines the region.
- You can define multiple exclusion regions on a floor.
- Newly defined inclusion and exclusion regions appear on heatmaps only after the location server recalculates location.
- You must check the Location Regions option on the Floor Settings panel of the Monitor > Maps window for inclusion and exclusion regions to appear on the map.

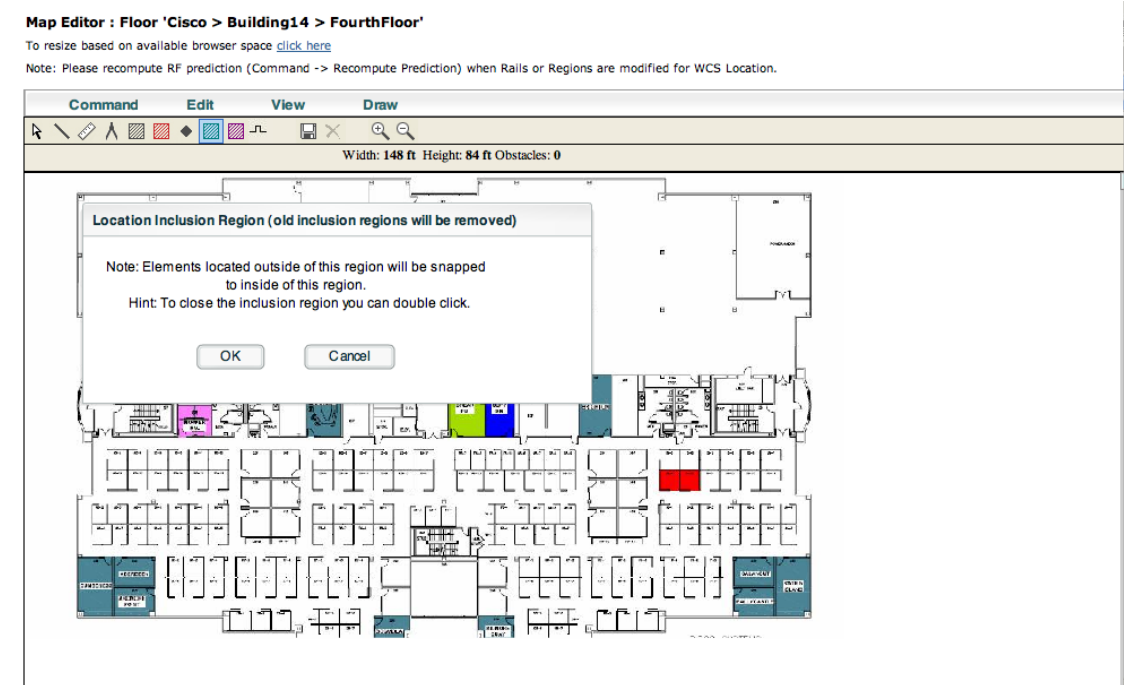
Defining an Inclusion Region on a Floor

To define an inclusion region, follow these steps:

- Step 1** Choose **Monitor > Maps**.
- Step 2** Click the name of the appropriate floor 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 (see [Figure 7-15](#)).

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 7-15 Map Editor Window



- Step 5** Click **OK** in the message box that appears. A drawing icon appears to outline the inclusion area.
- Step 6** To begin defining the inclusion area, move the drawing icon to a starting point on the map and click once.
- Step 7** Move the cursor along the boundary of the area you want to include and click to end a border line. Click again to define the next boundary line.
- Step 8** Repeat [Step 7](#) until the area is outlined and then double click the drawing icon. A solid aqua line defines the inclusion area (see [Figure 7-16](#)).

Figure 7-16 Inclusion Area Defined

Map Editor : Floor 'Cisco > Building14 > FourthFloor'

To resize based on available browser space [click here](#)

Note: Please recompute RF prediction (Command -> Recompute Prediction) when Rails or Regions are modified for WCS Location.



Step 9 Choose **Command > Save** or click the disk icon on the tool bar to save the inclusion region.



Note If you made an error in defining the inclusion area, click on the area. The selected area is outlined by a dashed aqua line. Next, click on the X icon in the tool bar. The area is removed from the floor map.

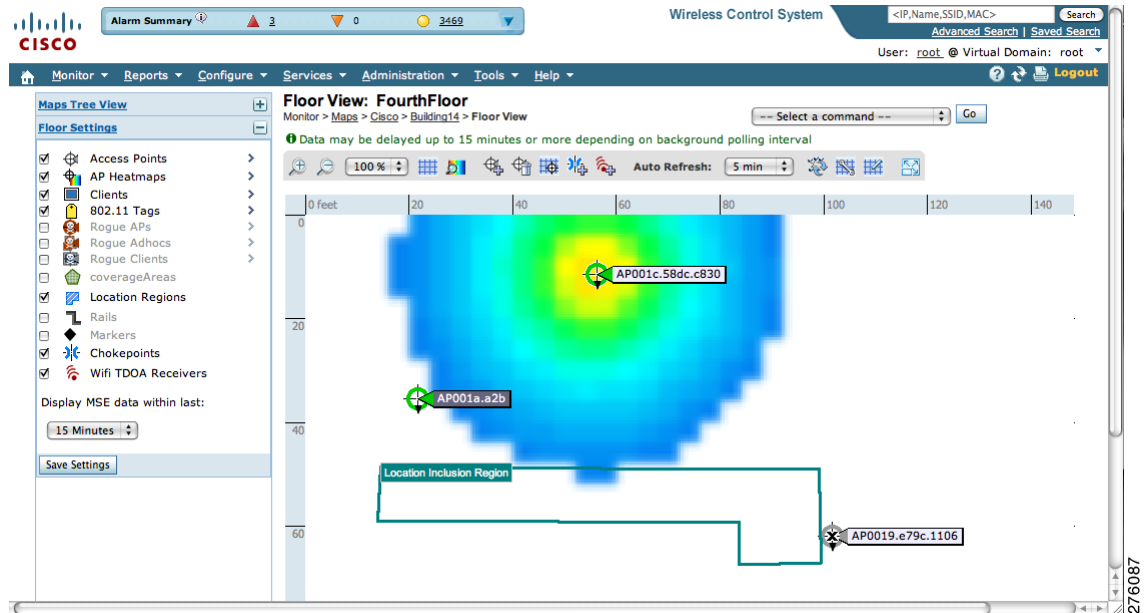
Step 10 To return to the floor map to enable inclusion regions on heatmaps, choose **Command > Exit**.

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

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

The defined inclusion region appears on the map (see [Figure 7-17](#)).

Figure 7-17 Monitor > Maps > Floor



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

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

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



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

To define an exclusion area, follow the steps:

Step 1 Choose **Monitor > Maps**.

Step 2 Click the name of the appropriate floor area.

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

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

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

- Step 6** To begin defining the exclusion area, move the drawing icon to the starting point on the map and click once.
- Step 7** Move the drawing icon along the boundary of the area you want to exclude and click once to start a boundary line and click again to end the boundary line.
- Step 8** Repeat [Step 7](#) until the area is outlined and then double click the drawing icon. The defined exclusion area is shaded in purple. when the area is completely defined. The excluded area is shaded in purple.
- Step 9** To define additional exclusion regions, repeat [Step 4](#) to [Step 8](#) (see [Figure 7-18](#)).

Figure 7-18 Defining Exclusion Areas on Floor Map

To resize based on available browser space [click here](#)

Note: Please recompute RF prediction (Command -> Recompute Prediction) when Rails or Regions are modified for WCS Location.



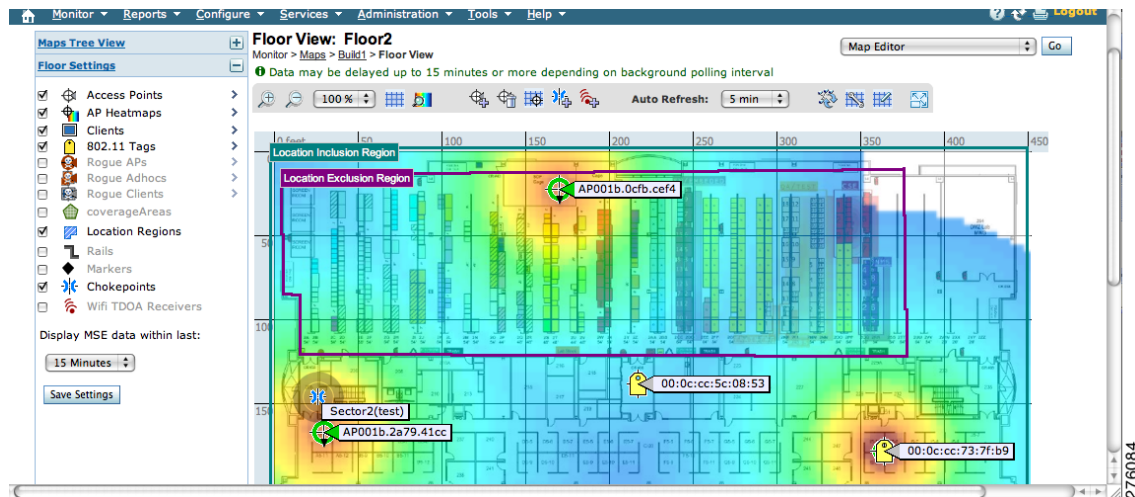
- Step 10** When all exclusion areas are defined, choose **Command > Save** or the disk icon in the tool bar to save the exclusion region.



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** In the Floor Settings panel, check the Location Regions check box if it is not already checked. The exclusion region is shown on the map (see [Figure 7-19](#)).

Figure 7-19 Location Exclusion Region



- Step 12** To synchronize the Cisco WCS and location databases, choose **Services > Synchronize Services**.
- Step 13** 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

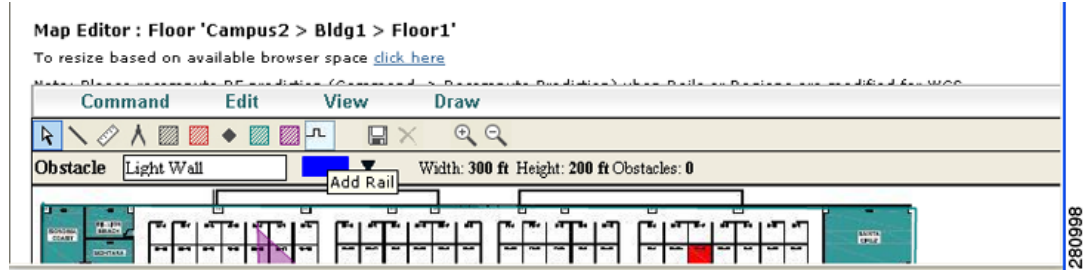
You can define a rail line on a floor that represents a conveyor belt. Additionally, you can define an area around the rail area known as the snap-width to further assist location calculations. This represents the area in which you expect certain inventory with asset tags to appear. Any asset tags located 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** Choose **Monitor > Maps**.
- Step 2** Click on the name of the appropriate floor area.
- Step 3** Select **Map Editor** from the Select a command drop-down menu. Click **Go**.
- Step 4** At the map, click the rail icon (to the right of the purple exclusion icon) in the tool bar (see [Figure 7-20](#)).

Figure 7-20 Rail Icon on Map Editor Tool Ba



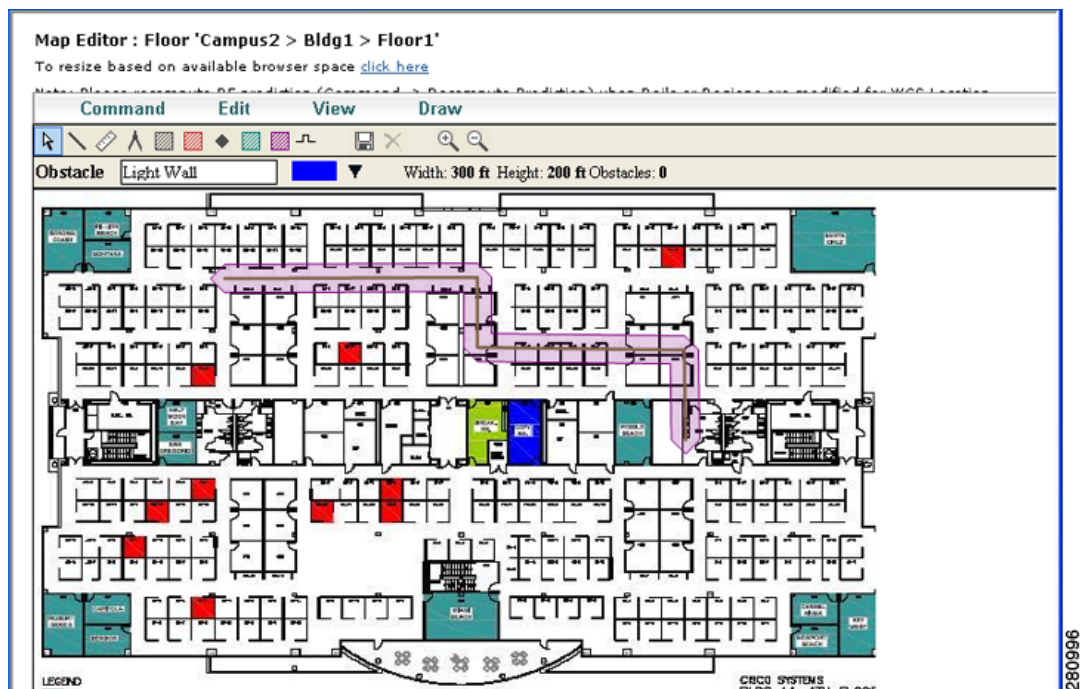
- Step 5** In the message panel that appears, enter a snap-width (feet or meters) for the rail and then click **OK**. A drawing icon appears.



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 both sides by the defined snap-width region (see Figure 7-21).

Figure 7-21 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, choose **Command > Exit**.

- Step 9** At the floor map, check the Location Regions check box if it is not already checked. The exclusion region is shown on the map.
- Step 10** To synchronize the Cisco WCS and location databases, choose **Services > Synchronize Services**.
- Step 11** 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 that you can download to multiple controllers.

You can set the following general and advanced parameters on the location template.

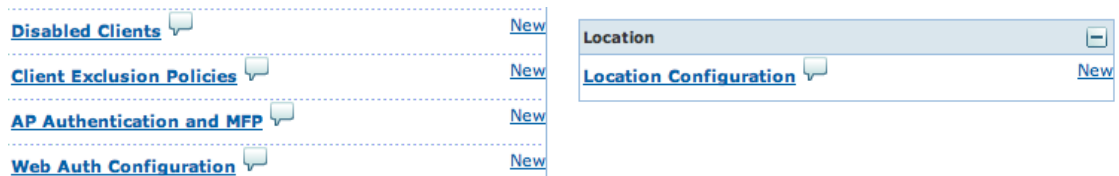
General parameters—Enable RFID tag collection, set the location path loss for calibrating or normal (non-calibrating) clients, measurement notification for clients, tags, and rogue access points, set the RSSI expiry timeout value for clients, tags, and rogue access points.

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

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

- Step 1** Choose **Configure > Controller Template Launch Pad**.
- Step 2** Select the **New** (Location Configuration) link under the Location heading to create a new location template (see [Figure 7-22](#)).

Figure 7-22 *Configure > Controller Template Launch Pad Window*



- Step 3** At the New template window, enter a name for the location template ([Figure 7-23](#)).

Figure 7-23 New Template > General Panel

New Controller Template
Configure > Controller Template Launch Pad > Location > Location Configuration > New Controller Template

Template Name:

General | **Advanced**

RFID Tag Data Collection Enable

Location Path Loss Configuration

Calibrating Client Enable
Normal Client (Burst Interval in secs)

Measurement Notification Interval (in secs)

Tags, Clients and Rogue APs/Clients

RSSI Expiry Timeout (in secs)

For Clients
For Calibrating Clients
For Tags
For Rogue APs

Footnotes:
1. Synchronization to the MSE will be needed in order to see effects of changes

Step 4 At the General panel modify parameters as necessary. [Table 7-1](#) describes each of these parameters.

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.
Normal Client	Check the Enabled check box to have a non-calibrating client. No S36 or S60 requests are transmitted to the client.

Table 7-1 General Location Parameters (continued)

Parameter	Configuration Options
Measurement Notification Interval	Enter a value to set the NMSP measurement notification interval for clients, tags, and rogues. This value can be applied to selected controllers via the template. Setting this value on the controller generates out-of-sync notification and the user is able to view this on the Synchronize Services window. When a controller and the location server have two different measurement intervals, the largest interval setting of the two is adopted by the location server. 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.

- Step 5** At the Advanced panel modify parameters as necessary (Figure 7-24).
Table 7-2 describes each of the advanced parameters.

Figure 7-24 New Template > Advanced Parameters Window

Table 7-2 Advanced Location Parameters

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

Step 6 Click **Save**.

Verifying a NMSP Connection to a Location Server

NMSP manages communication between the location server and a controller. Transport of telemetry, emergency, and chokepoint information between the location server and the controller is managed by this protocol.



Note NMSP also manages communication between a mobility services engine and a controller or a location-capable Catalyst switch. However, the location server does not communicate with location-capable Catalyst switches over NMSP.

To verify a NMSP connection between a location server and a controller, follow these steps:

- Step 1** Choose **Services > Mobility Services**.
- Step 2** At the Mobility Services window, click the device name link of the appropriate controller.
- Step 3** Choose **System > Status > NMSP Connection Status** (see [Figure 7-25](#)).

Figure 7-25 NMSP Connection Status

The screenshot shows the Cisco Wireless Control System interface. The main content area displays the **NMSP Connection Status: -lbs** page. The page includes a summary table and a detailed table of connection status.

Device	Total	Inactive
Controllers	4	0
Switches	0	0

IP Address	Target Type	Version	NMSP Status	Echo Request Count	Echo Response Count	Last Message Received
172.19.30.200	Controller	6.0.181.0	ACTIVE	360	360	Mon Jun 15 14:27:51 PDT 2009
172.19.35.48	Controller	5.1.151.0	ACTIVE	59277	59277	Mon Jun 15 14:27:50 PDT 2009
172.19.35.50	Controller	6.0.16.0	ACTIVE	34212	34207	Mon Jun 15 14:27:48 PDT 2009
172.19.35.72	Controller	5.2.183.0	ACTIVE	59278	59278	Mon Jun 15 14:27:44 PDT 2009

Step 4 Verify that the NMSP Status is **ACTIVE**.

If not active, synchronize the controller and the location server.

Modifying Context-Aware Software Parameters

You can specify the type and number of clients or tags that are tracked and whether or not locations are calculated for those clients or tags.

You can also modify parameters that affect the location calculation of clients and tags such as Receiver Signal Strength Indicator (RSSI) measurements.

**Note**

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

Editing Tracking Parameters

The location appliance can track up to 2,500 elements. You can track the following elements: client stations, active RFID 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 that the controller is tracking are seen in Cisco WCS maps, queries, and reports. No events and alarms are collected for non-tracked elements and none are used in calculating the 2,500 element limit.

You can modify the following tracking parameters using Cisco WCS:

- Enable and disable which element locations (client stations, active RFID tags, and rogue clients and access points) you actively track.
- Set limits on how many of a specific element you want to track.

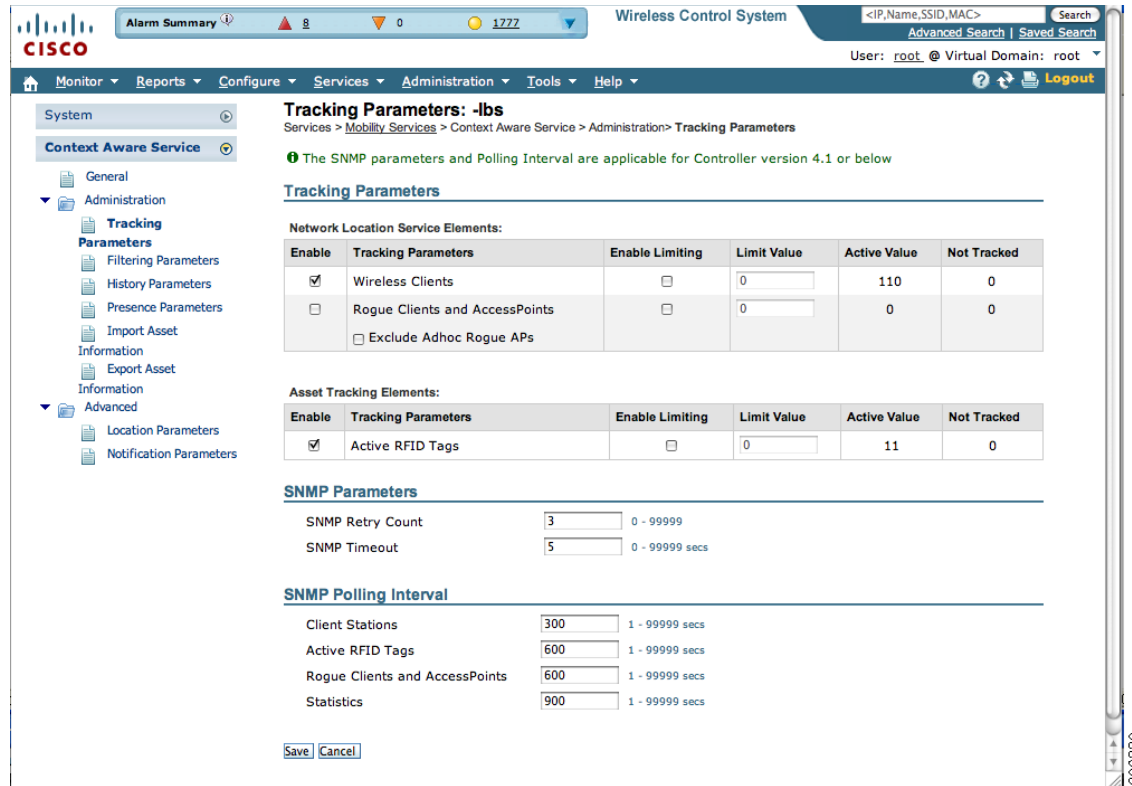
For example, given a limit of 2,500 trackable units, you could set a limit to track only 1,500 client stations. Once the tracking limit is met, the number of elements not being tracked is summarized on the Tracking Parameters page.

- 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, choose **Services > 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** Choose **Context Aware Service > Administration > Tracking Parameters** to display the configuration options (see [Figure 7-26](#)).

Figure 7-26 Context Aware Service > Administration > Tracking Parameters Window



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	
Wireless Clients	<ol style="list-style-type: none"> 1. Check the Enable check box to enable tracking of wireless client stations by the location server. 2. Check the Enable Limiting check box to set a limit on the number of wireless 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. <p>Note Active Value (display only): Indicates the number of wireless client stations currently being tracked.</p> <p>Note Not Tracking (display only): Indicates the number of wireless client stations beyond the limit.</p>

Table 7-3 Tracking and SNMP Parameters (continued)

Parameter	Configuration Options
Rogue Clients and Access Points	<ol style="list-style-type: none"> 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. <p>Note Active Value (display only): Indicates the number of rogue clients and asset tags currently being tracked.</p> <p>Note Not Tracking (display only): Indicates the number of rogue clients and asset tags beyond the limit.</p>
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.
Active RFID Tags	<ol style="list-style-type: none"> 1. Check the Enable check box to enable tracking of active RFID tags by the location server. 2. Check the Enable Limiting check box to set a limit on the number of active RFID 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. <p>Note Active Value (display only): Indicates the number of active RFID tags currently being tracked</p> <p>Note Not Tracking (display only): Indicates the number of active RFID tags beyond the limit.</p>

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).
SNMP Polling Interval	
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).
Active RFID Tags	Check the Enable check box to enable active RFID 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 active RFID 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 client and 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 addition to tracking parameters, you can use filtering to limit the number of clients, tags, and rogue clients, and access points whose locations are tracked.

You can filter by MAC address and probing clients.

- MAC addresses

Specific MAC addresses can be entered and labeled as allowed or disallowed from location tracking. You can import a file with the MAC addresses that are to be allowed or disallowed or you can enter them individually from the WCS GUI window.

The format for entering MAC addresses is `xx:xx:xx:xx:xx:xx`. If a file of MAC addresses is imported, the file must follow a specific format as noted below:

- Each MAC address should be listed on a 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, choose **Services > 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** Choose **Context Aware Service > Administration > Filtering Parameters** 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	<ol style="list-style-type: none"> 1. Check the check box to enable MAC filtering of specific elements by their MAC address. 2. To import a file of MAC addresses (<i>Upload a file for Location MAC Filtering</i> 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. <p>Note To view allowed MAC address formats, click on the red question mark next to the <i>Upload a file for Location MAC Filtering</i> field.</p> <ol style="list-style-type: none"> 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. <p>Note To move an address between the Allow and Disallow columns, highlight the MAC address entry and click the button under the column.</p> <p>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.</p> <p>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.</p>

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 long to store (archive) histories on client stations, asset tags, and rogue clients and access points. Controllers associated with the location server send it histories.

You can also program the location server to periodically prune (remove) duplicate data from its historical files, which increases the amount of memory available for other functions.

To configure location server history settings, follow these steps:

-
- Step 1** In Cisco WCS, choose **Services > Mobility Services**. The Mobility Services window appears.
 - Step 2** Click the name of the location server whose properties you want to edit.
 - Step 3** Choose **Context Aware Service > Administration > History Parameters** (left panel) 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. Allowed values are between 0 and 23 hours, and between 1 and 59 minutes. Default start time is 23 hours and 50 minutes,
...and also every	Enter the interval in minutes after which data pruning starts again. Allowed values are between 0, which means never, and 99900000. Default value is 1440 minutes.
Enable History Logging of Location Transitions for <i>Client Stations, Asset Tags and Rogue Clients and Access Points</i>	Check any or all of the elements (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 when an element moves at least 10 meters or 30 feet from its original site.

- Step 5** Click **Save**.
-

Enabling Location Presence on a Location Server

You can enable location presence by location server to expand 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 to Cisco WCS or configured at a later date.

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** Choose **Services > Mobility Services > Device Name**.
- Step 2** Select the location server to which the campus or building is assigned.
- Step 3** Choose **Context Aware Service > Administration > Presence Parameters** (left-panel). The Presence window displays.
- Step 4** Check the **On Demand** check box to enable location presence for Cisco CX clients v5.
- Step 5** 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 6** 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.
 - c. Check the **GEO** check box to provide the longitude and latitude coordinates.
- Step 7** By default the Text check box for Location Response Encoding is checked. It indicates the format of the information when received by the client. There is no need to change this setting.
- Step 8** Check the **Retransmission Rule Enable** check box to allow the receiving client to retransmit the received information to another party.

- Step 9** Enter a Retention Expiration value in minutes. This determines how long the received information is stored by the client before it is overwritten. Default value is 24 hours (1440 minutes).
- Step 10** Click **Save**.
-

Importing Asset Information

To import active RFID tag, station, chokepoint, and TDOA receiver information for the location server using Cisco WCS, follow these steps:

- Step 1** In Cisco WCS, choose **Services > Mobility Services**.
- Step 2** Click the name of the location server for which you want to import information.
- Step 3** Choose **Context Aware Software > Administration > Import Asset Information** (left panel).
- Step 4** 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
 - d. Wi-Fi TDOA receiver format: BuildingName, FloorName, LSMacAddress, LSName, IP Address, X, Y, Z
 X, Y, and Z represent map coordinates
 LS refers to the TDOA receiver
- Step 5** 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, choose **Services > Mobility Services**.
- Step 2** Click the name of the location server from which you want export information.
- Step 3** Choose **Context Aware Software > Administration > Export Asset Information** (left panel).
- 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
- d. Wi-Fi TDOA receiver format: BuildingName, FloorName, LSMacAddress, LSName, IP Address, X,Y, Z
X, Y, and Z represent map coordinates
LS refers to the TDOA receiver

Step 4 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, choose **Services > Mobility Services**.
- Step 2** Click the name of the location server whose properties you want to edit.
- Step 3** Choose **Context Aware Service > Advanced > Location Parameters** (left panel). 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 Enable check box to initiate 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.

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. <i>A value of less than 3 is not recommended.</i>
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. <i>A value of less than 60 is not recommended.</i>
RSSI Cutoff	<p>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.</p> <p>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.</p> <p> Caution Modify only under Cisco TAC personnel guidance. Modifying this value can reduce the accuracy of location calculation.</p>
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	<p>Perimeter chokepoints or weighted location readings can be selected to determine the location of Cisco compatible tags.</p> <p>Options:</p> <ul style="list-style-type: none"> • 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.
Absent Data cleanup interval	Enter the number of minutes that data for <i>absent</i> mobile stations is kept. An <i>absent</i> mobile station is one that was discovered but does not appear in the network. Default value is 1440.

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



CHAPTER 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, page 8-2](#)
- [Working with Events, page 8-4](#)
- [Working with Logs, page 8-5](#)
- [Generating Reports, page 8-6](#)
- [Monitoring Location Server Status, page 8-9](#)
- [Monitoring Wireless Clients, page 8-10](#)
- [Monitoring Wireless Clients Using Search, page 8-12](#)
- [Monitoring Chokepoints, page 8-21](#)

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 the **Advanced Search** link (top-right). A configurable search panel for alarms appears (see Figure 8-1).

Figure 8-1 Search Alarm Panel

Severity	Failure Source	Acknowledged
Warning	AP AP001c.58dc.c86a, Interface 802.11b/g	No
Warning	AP AP001c.58df.9cee, Interface 802.11b/g	No
Critical	Mobility Services Engine h sanity	No
Warning	Rogue AP 00:1d:e6:24:61:cc	No
Warning	Rogue AP 00:1d:e6:24:61:cd	No
Warning	Rogue AP 00:1d:e6:24:61:c9	No
Warning	Rogue AP 00:18:74:d0:ea:cb	No
Warning	Rogue AP 00:1c:57:41:4a:49	No
Warning	Rogue AP 00:19:a9:a4:df:d9	No
Warning	Rogue AP 00:1c:57:41:4c:a9	No
Warning	Rogue AP 00:1d:e6:24:2e:6c	No

- Step 3** Select **Alarms** as the Search Category.
- Step 4** Select the Severity of Alarms to display. Options are All Severities, Critical, Major, Minor, or Warning.
- Step 5** Select **Mobility Service** from the Alarm Category.
- Step 6** 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 7** Check the **Acknowledged State** check box to exclude the acknowledged alarms and their count from the Alarm Summary window.
- Step 8** Check the **Assigned State** check box to exclude the assigned alarms and their count from the Alarm Summary window.

- Step 9** Select the number of alarms to display on each window from the Items per Page drop-down menu.
- Step 10** To save the search criteria for later use, check the **Save Search** check box and enter a name for the search.
- Step 11** Click **Go**. Alarms summary panel appears with search results.



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

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

Assigning and Unassigning Alarms

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

- Step 1** Display the Alarms window as described in the [“Viewing Alarms” section on page 8-2](#).
- Step 2** Select the alarms that you want to assign to yourself by checking their corresponding check boxes.



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

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

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

To delete or clear an alarm from a 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 Configuration** 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 **Mobility Services**.
- Step 4** Click the **Mobility Services** 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 Email 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:
- To display the events for a specific element and you know its IP address, MAC address, or Name, enter that value in the Search field (top-right). Click **Go**.
 - To display events by severity and event category, click the **Advanced Search** link (top-right). Select **Events** as the Search Category and then select the appropriate options from the Severity and Event Category. Click **Go**.
- Step 3** If Cisco WCS finds events that match the search criteria, it displays a list of these events.



Note For more information about an event, click the failure 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 **Services > Mobility Services**.
- Step 2** Click the name of the location server that you want to configure.
- Step 3** Choose **System > Advanced Parameters** (left). 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 option listed in that section to begin logging of its events.
- Step 6** Click **Save**.
-

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 **Services > Mobility Services**.
 - Step 2** Click the name of the location server to view its status.
 - Step 3** Choose **System > 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 device utilization and location utilization report for a location server. By default, reports are stored on the Cisco WCS server.

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

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

- Which location server or servers to monitor
- How often the report is generated
- How the data is graphed on the charts
- Whether the report is emailed or exported to a file

You can view the following in a location utilization report:

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

Creating a Location Server Utilization Report

-
- Step 1** In Cisco WCS, choose **Reports > Report Launch Pad**.
 - Step 2** Choose **Device > Utilization**.
 - Step 3** Click **New**. The Utilization: New window appears (see [Figure 8-2](#)).

Figure 8-2 Device > Utilization Window

- Step 4** In the Settings panel (left), enter a report title.
- Step 5** The Report Type and Report By selections are always MSE (even when a location server).
- 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. You can define the report to collect data hourly, weekly basis, or at a specific date and time. The selected reporting period type will display on the x-axis.



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

- Step 8** In the Schedule panel (right), check the **Enable Schedule** check box.
- Step 9** Select the export format (CSV or PDF) from the Export Report drop-down menu.
- Step 10** Select either **File** or **Email** as the destination of the report.
- If you select the File option, a destination path must first be defined at the **Administration > Settings > Report** window. Enter the destination path for the files in the Repository Path field.
 - If you select the Email option, an SMTP Mail Server must be defined prior to entry of target email address. Choose **Administrator > Settings > Mail Server Configuration** to enter the appropriate information.
- Step 11** Enter a start date (MM:DD:YYYY) or click the calendar icon to select a date.
- Step 12** Specify a start time using the hour and minute drop-down menus.
- Step 13** Click one of Recurrence buttons to select how often the report is run.



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

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

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



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

Step 15 If you selected the Save or Save and Run option, click either **Reports > Saved Reports** (or **Reports > Scheduled Runs** if it has not yet run and is scheduled to run). The Utilization Reports summary window appears (see [Figure 8-3](#)).

Figure 8-3 Utilization Reports Summary Window

Report Title*	Report Type	Scheduled	Next Scheduled Run	Last Run	Download	Run Now
<input type="checkbox"/> WeeklyAM	Utilization	Enabled	03/18/2009 17:30:00 PDT			

Buttons: [New](#) [Enable Schedule](#) [Disable Schedule](#) [Delete](#)

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

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

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

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

Viewing Saved Utilization Charts

To download a saved report, follow these steps:

-
- Step 1** In Cisco WCS, choose **Reports > Saved Reports**.
 - Step 2** Click the **Download** icon for your report. It is downloaded and saved in the defined directory or emailed.
-

Viewing Scheduled Utilization Runs

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

-
- Step 1** In Cisco WCS, choose **Reports > Scheduled Runs**.
 - Step 2** Click the **History** icon to see the date of the last report run.
 - Step 3** Click the **Download** icon for your report. It is downloaded and saved in the defined directory or emailed.
-

Monitoring 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 **Services > 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 the [“Configuring Advanced Parameters”](#) section on page 4-5.

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.
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 Wireless Clients

Monitoring Wireless Clients Using Maps

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

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

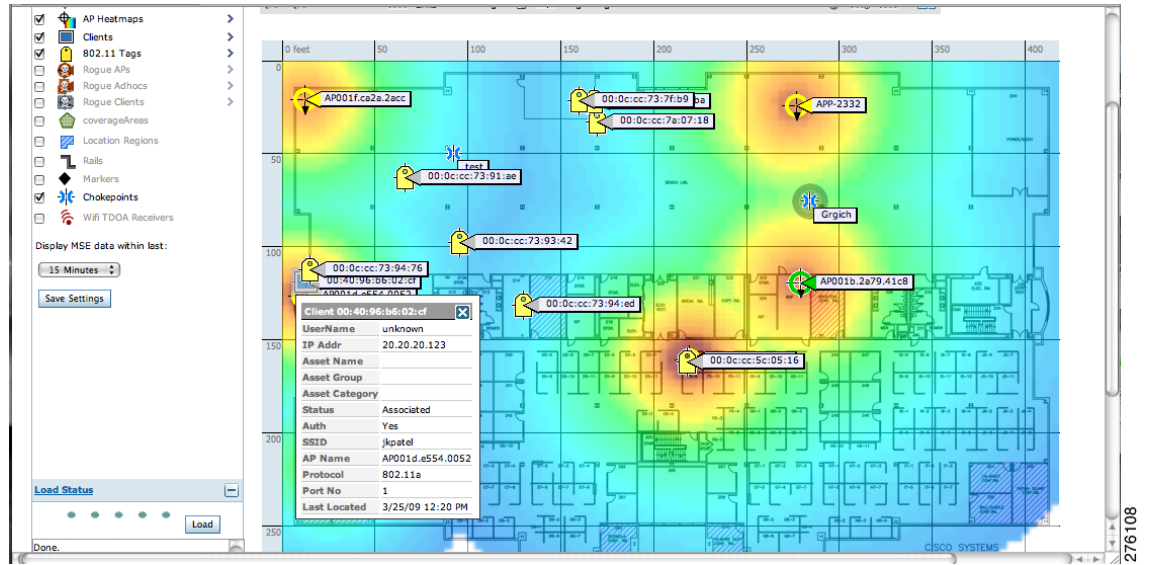
To determine a client’s location status on a map and view its client details window using maps, follow these steps:

-
- Step 1** In Cisco WCS, choose **Monitor > Maps**.
 - Step 2** Choose the building and floor on which the mobility services engine and its clients are located.
 - Step 3** Check the **Clients** check box in the Floor Settings panel (left), if it is not already checked (see [Figure 8-4](#)).



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

Figure 8-4 Monitor > Maps > Building > Floor Window



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

Step 5 Click the client icon to see client details (see Figure 8-5 and Figure 8-6).

Figure 8-5 Client Details Window (1 of 2)

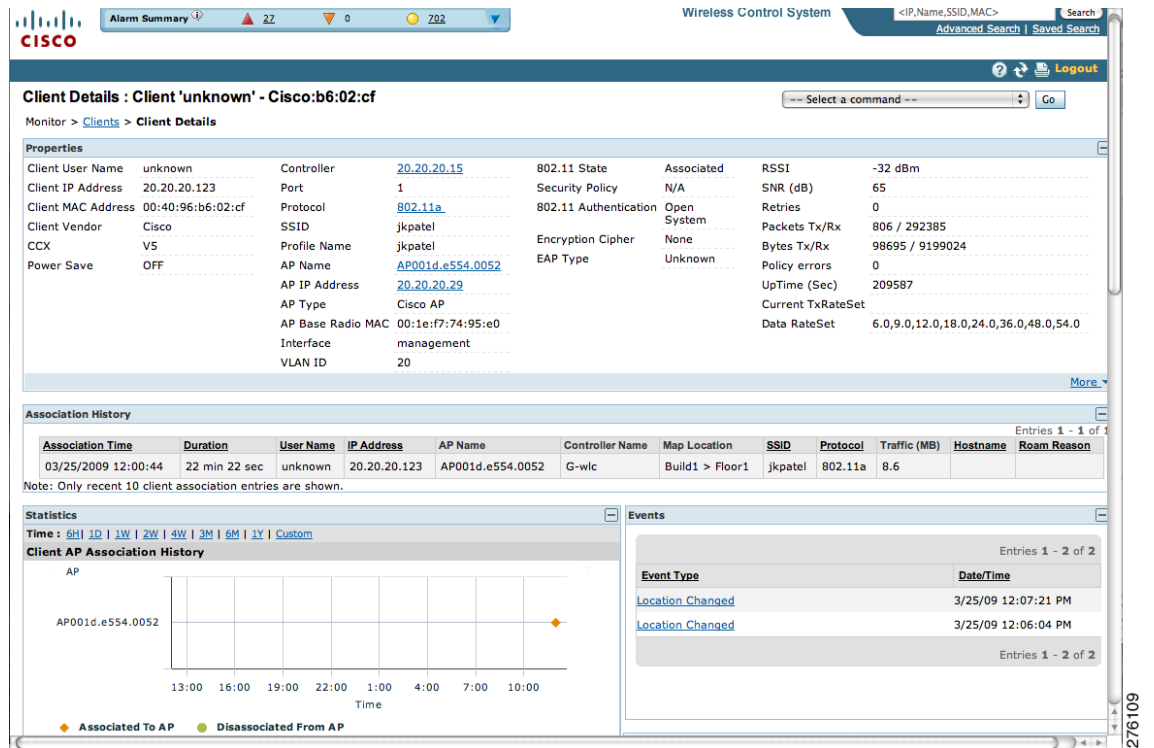
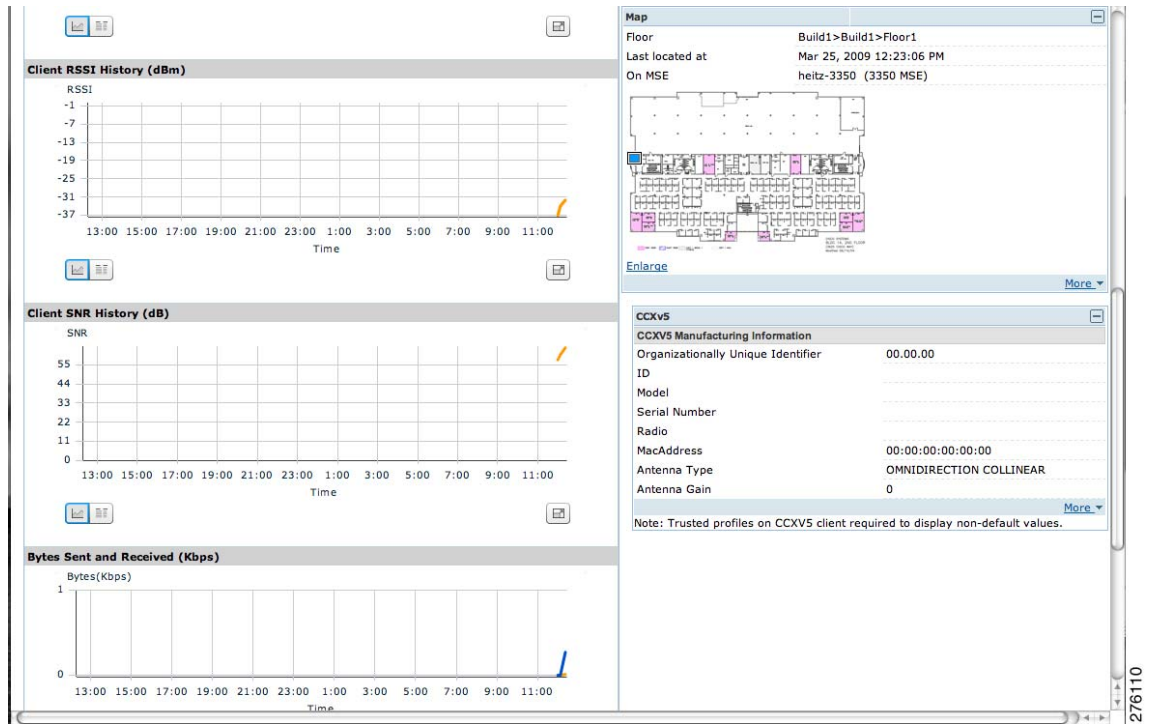


Figure 8-6 Client Details Window (2 of 2)



Monitoring Wireless Clients Using Search

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

To view client information, follow these steps:

-
- Step 1** In Cisco WCS, choose **Monitor > Clients**.
The Clients summary window appears.
- Step 2** Select **Clients Detected by MSEs** from the Show drop-down menu. Click **Go**.

A summary of all clients detected by all mobility services engines and location appliances managed by Cisco WCS displays (see Figure 8-7).

Figure 8-7 Monitor > Clients Window

Client User Name	Client IP Address	Client MAC Address	Vendor Name	AP Name	Controller Name	Map Location	SSID	Profile Name	VLAN	Protocol
<Unknown>		00:16:44:b1:b4:96	Lite-on			Build1>Build1>Floor1	N/A			802.1
<Unknown>	0.0.0.0	00:40:96:b2:a3:44	Cisco	AP001f.ca2a.2acc		Build1>Build1>Floor1	N/A			802.1
<Unknown>	0.0.0.0	00:40:96:b4:eb:ce	Cisco	AP001a.a2fe.c69c		Build1>Build1>Floor2	N/A			802.1
<Unknown>	0.0.0.0	00:40:96:a4:f8:ca	Cisco	AP001d.a280.c41e		Build1>Build1>Floor1	N/A			802.1
<Unknown>	0.0.0.0	00:40:96:b2:84:2e	Cisco	AP001b.2a79.41cc		Build1>Build1>Floor1	N/A			802.1
<Unknown>	0.0.0.0	00:40:96:ac:1c:6f	Cisco	AP001d.e554.0052		Build1>Build1>Floor1	N/A			802.1

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

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

Figure 8-8 Search by MAC address Results

Item Type	Item Count	Monitor	Configuration
Client	1	View List	
Alarm	1	View List	

- To see more configuration details about the client, click **View List** for the client item type. Details shown include associated devices (access point, controller), map location, VLAN, protocol, and authentication type.
- To see alarms for the client, click **View List** for the alarm item type. A listing of all active alarms for that client noting severity, failure source (alarm description), owner of alarm (if assigned), date and time of the alarm, and whether or not alarm is acknowledged (see Figure 8-9).

Figure 8-9 Alarm Summary for Client

Severity	Failure Source	Owner	Date/Time	Message	Acknowledged
Warning	Location Change Mobile Station 00:40:96:ac:1c:6f		3/24/09 10:34:16 AM	Location has changed for Mobile Station with MAC 00:40:96:ac:1c:6f ...	No

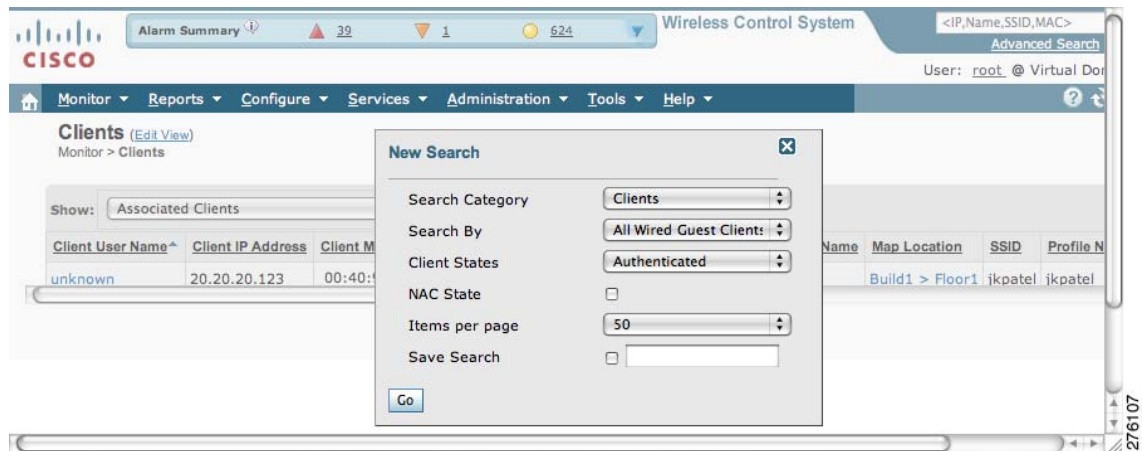


Note You can also assign or unassign the alarm, email it, delete or clear it, and acknowledge and unacknowledge it at this window by selecting the appropriate option from the Select a command drop-down menu.

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

You can further define the client category by: all clients, all excluded clients, all wired guest clients, and all logged in clients using the Search By drop-down menu (see [Figure 8-10](#)).

Figure 8-10 Advanced Search Window



Step 3 Click on the appropriate client.

Monitoring Tags

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

Monitoring Tags Using Maps

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

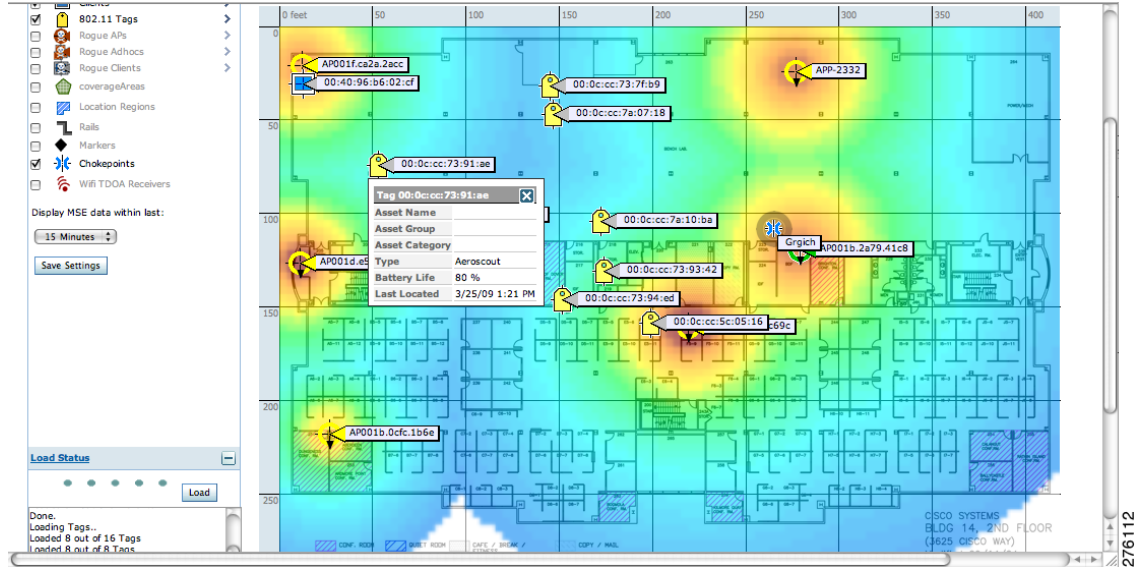
To enable tag location status on a map, follow these steps:

- Step 1** In Cisco WCS, choose **Monitor > Maps**.
- Step 2** Choose the building and floor on which the mobility services engine and tag are located.
- Step 3** Check the **802.11 Tags** check box in the Floor Settings panel (left), if it is not already checked (see [Figure 8-11](#)).



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

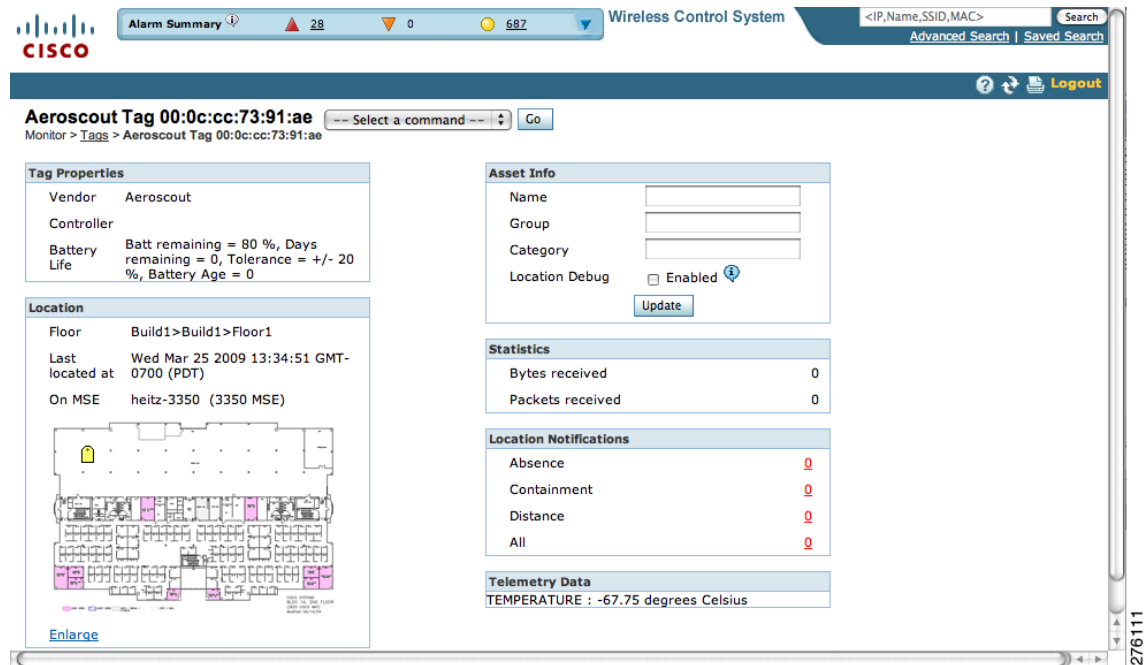
Figure 8-11 Monitor > Maps > Building > Floor > Tag Window



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

Step 5 Click the tag icon to see tag details (see Figure 8-12).

Figure 8-12 Tag Details Window



- Step 6** To see location history for the tag, select **Location History** from the Select a command drop-down menu. Click **Go** (see Figure 8-13).

Figure 8-13 Tag Location History Window

The screenshot shows the Cisco Wireless Control System interface. The main content area is titled "Aeroscout Tag 00:0c:cc:73:91:ae" and displays the "Location History" for this tag. The interface includes a navigation bar at the top with options like Monitor, Reports, Configure, Services, Administration, Tools, and Help. The "Tag Information" section shows data collected at Wed Mar 25 2009 12:29:51 GMT-0700 (PDT) with a battery status of 80%. The "Tag Statistics" section shows 0 bytes and 0 packets received. The "Tag Location History" table lists 6 entries, all from Wed Mar 25 2009, with a battery status of 80% and location "Build1>Build1>Floor1". A floor plan map is visible on the right side of the window.

Time Stamp	Floor	Battery Status
1 Wed Mar 25 2009 13:26:34 GMT-0700 (PDT)	Build1>Build1>Floor1	80 %
2 Wed Mar 25 2009 13:23:59 GMT-0700 (PDT)	Build1>Build1>Floor1	80 %
3 Wed Mar 25 2009 13:21:24 GMT-0700 (PDT)	Build1>Build1>Floor1	80 %
4 Wed Mar 25 2009 13:16:55 GMT-0700 (PDT)	Build1>Build1>Floor1	80 %
5 Wed Mar 25 2009 13:14:19 GMT-0700 (PDT)	Build1>Build1>Floor1	80 %
6 Wed Mar 25 2009 13:02:43 GMT-0700 (PDT)	Build1>Build1>Floor1	80 %

Monitoring Tags Using Search

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



Note Search by MSE includes location appliances.

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

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

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

To search for tags, follow these steps:

- Step 1** Choose **Monitor > Tags**. The Tag Summary window appears (see [Figure 8-14](#)).

Figure 8-14 Monitor > Tags Window

Device Name	Device Address	Total Tags
loc-server (2710 LocServer)	20.20.20.20	0
mse-3310 (3310 MSE)	20.20.20.17	8
heitz-3350 (3350 MSE)	20.20.20.40	8

- a. To view a summary of tags associated with a specific location appliance or mobility services engine, click the **Total Tags** link (see [Figure 8-15](#)).

Figure 8-15 Total Tags Listing by Mobility Services Engine and Location Appliance

MAC Address	Asset Name	Asset Group	Asset Category	Vendor Name	MSE	Controller	Battery Status	Map Location
00:0c:cc:7a:10:ba	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build 1 > Build 1 > Floor 1
00:0c:cc:7a:07:18	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build 1 > Build 1 > Floor 1
00:0c:cc:73:94:ed	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build 1 > Build 1 > Floor 1
00:0c:cc:73:94:76	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build 1 > Build 1 > Floor 1
00:0c:cc:73:93:42	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build 1 > Build 1 > Floor 1
00:0c:cc:73:91:ae	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build 1 > Build 1 > Floor 1
00:0c:cc:73:7f:b9	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build 1 > Build 1 > Floor 1
00:0c:cc:5c:05:16	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build 1 > Build 1 > Floor 1



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

- b. To search for a specific tag, if you know its MAC address, name or VLAN ID (not all search values apply to all tags) use **Search** which is found in the navigation bar.
- c. To search for a specific tag or multiple tags using a broader range of search categories such as device (MSE or controller), map location (floor or outdoor area), asset name or category, or tag vendor use **Advanced Search** which is found in the navigation bar (see [Figure 8-16](#)).
- In the Advanced Search panel, select **Tags** as the search category.
 - Select the additional tag search criteria. Refer to [Table 8-2](#) for a list of search criteria and their possible values.
 - Click **Go** when all advanced search parameters are selected. Results are shown in [Figure 8-17](#).



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

Figure 8-16 Advanced Search Panel for Tags

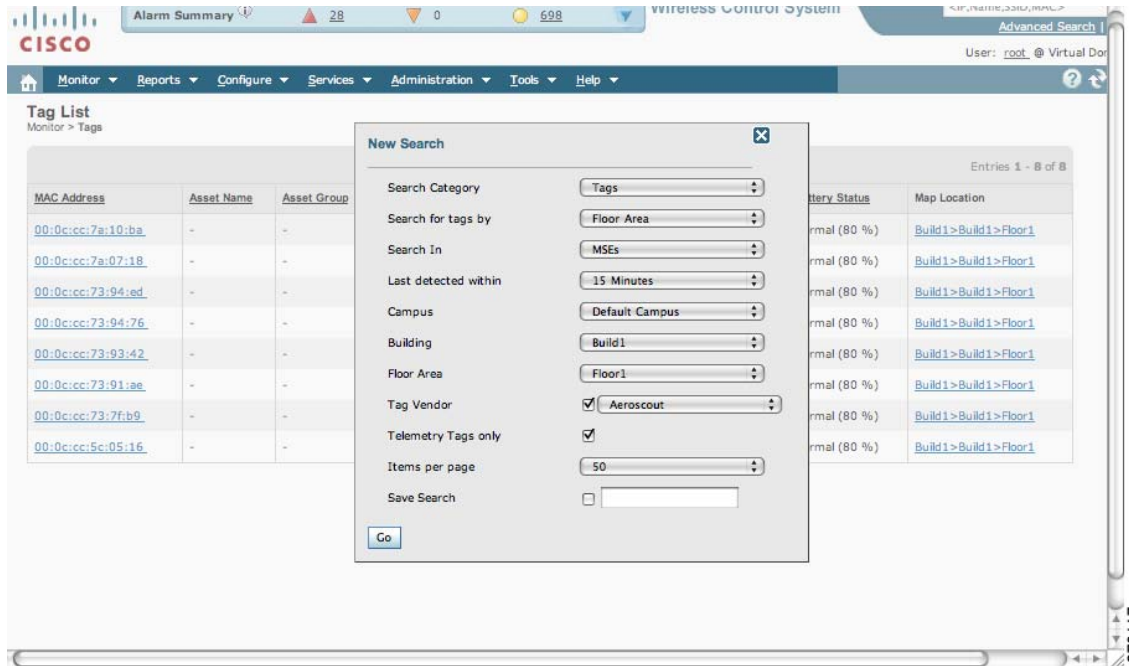
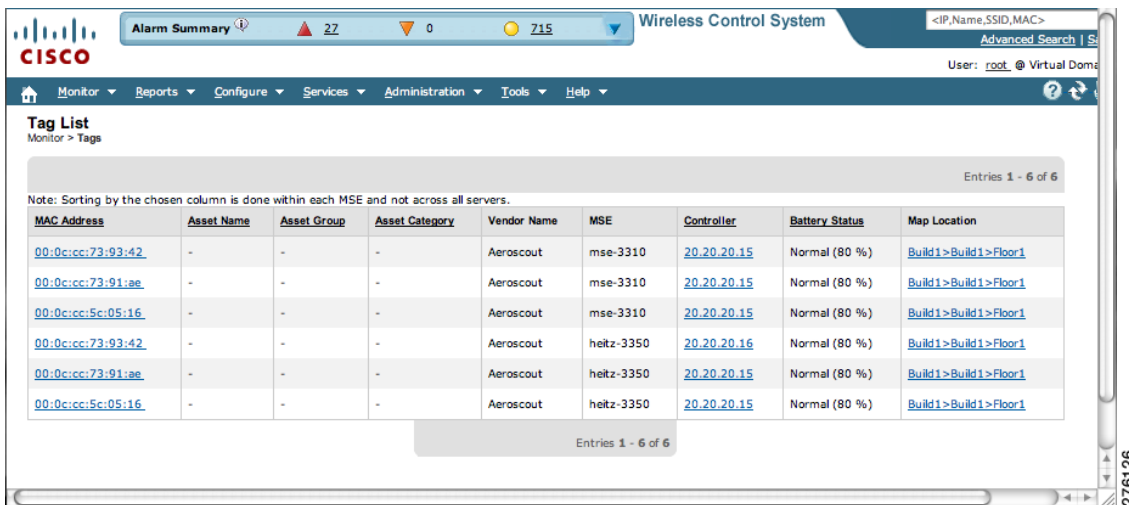


Figure 8-17 Advanced Search Results for Tag



Note If you click the MAC address of any of these tags, a Tag details window appears similar to that in Figure 8-12.

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 tags by (Tier 1 search) value.	If Search for tags by value is: <ol style="list-style-type: none"> 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.

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 8-18](#)).

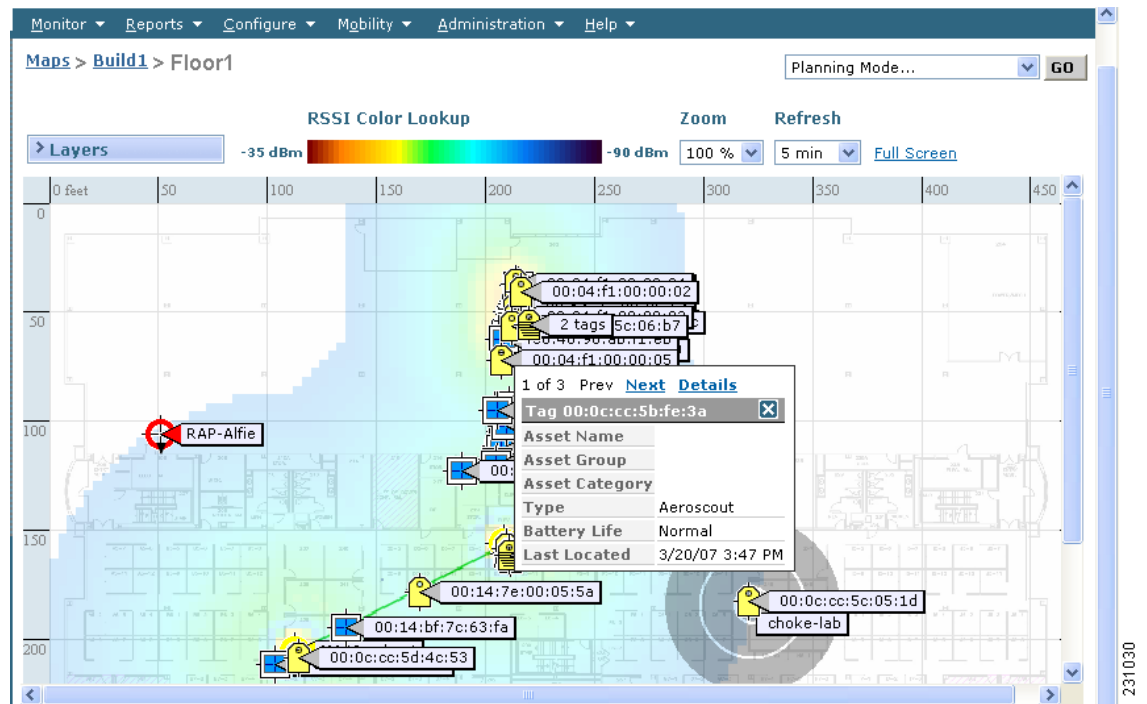
Select the Prev and Next links to move between the individual tag summary panels. To see detailed information on a specific tag, select the Details link while viewing the tag's summary information.



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 8-18 Overlapping Tags Window



Monitoring Chokepoints

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

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

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

All chokepoint setup is done using the *AeroScout System Manager*.



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

To monitor chokepoints, follow these steps:

- Step 1** Choose **Monitor > Chokepoints**. The Chokepoint summary window appears showing all mapped chokepoints.
- Step 2** To refine the search criteria when an extensive list appears, search by MAC address or chokepoint name.
 - a. To initiate a search for a chokepoint by its MAC address or chokepoint name, enter that value in the Search field of the navigation bar. Click **Search** (see [Figure 8-19](#)).

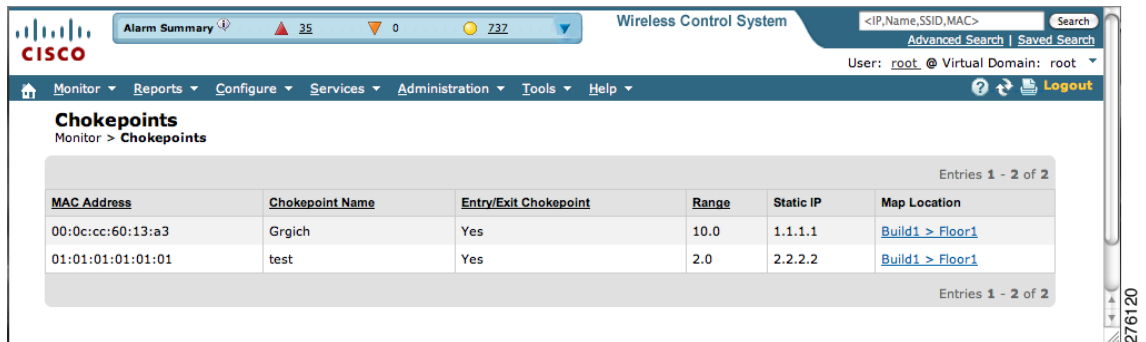
Figure 8-19 Search for Chokepoint by MAC Address



Figure 8-19 shows a search by MAC address. Figure 8-20 shows the results.

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

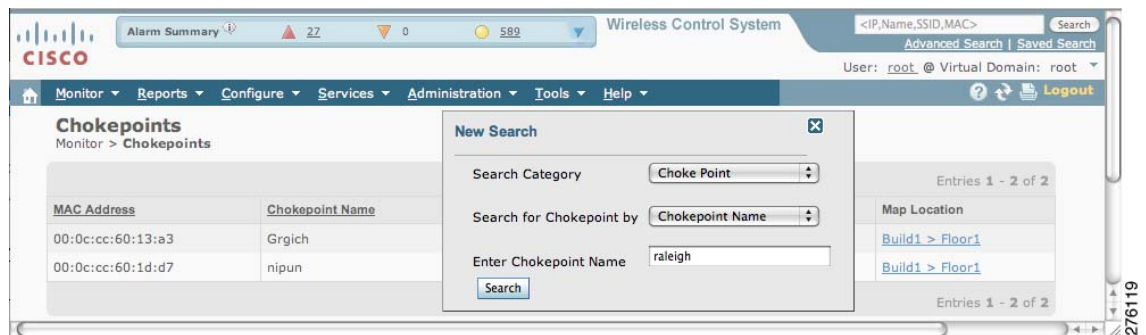
Figure 8-20 MAC Address Search Results for a Chokepoint Indicating a Match



- b. To initiate an advanced search for a chokepoint by its MAC address or name, click **Advanced Search** in the navigation bar.
 1. Select **Chokepoint** as the search category.
 2. Select either **Chokepoint Name** or **MAC Address** from the Search for Chokepoint by drop-down menu.
 3. Enter either the chokepoint name or MAC address.
 4. Click **Search**.

This example shows an advanced search using the chokepoint name (see Figure 8-21).

Figure 8-21 Chokepoint Name Advanced Search Panel



If no match exists, a message appears in the window (see Figure 8-22).

Otherwise the search result appears.

Figure 8-22 Chokepoint Advanced Search Results Indicating No Match

Monitoring Wi-Fi TDOA Receivers

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

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

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

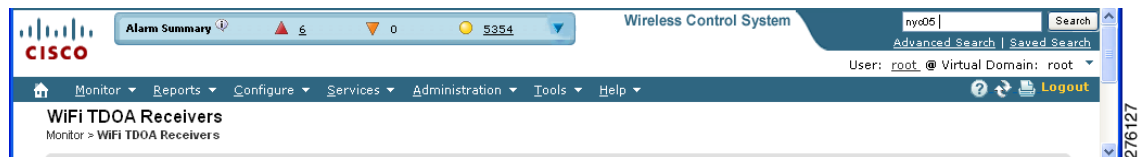
All TDOA receiver setup is done using the *AeroScout System Manager*.



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

To monitor TDOA Receivers, follow these steps:

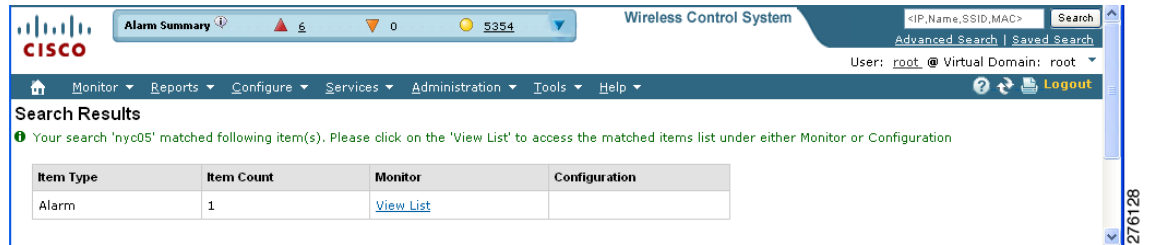
- Step 1** Choose **Monitor > WiFi TDOA Receivers**. The WiFi TDOA Receivers summary window appears showing all mapped TDOA receivers.
- Step 2** To refine the search criteria when an extensive list appears, search by MAC address or TDOA receiver name.
 - a. To initiate a search for a TDOA receiver by its MAC address or name, enter that value in the Search field of the navigation bar. Click **Search** (see [Figure 8-23](#)).

Figure 8-23 Monitor > WiFi TDOA Receivers Search Window

[Figure 8-24](#) shows an example of advanced search using the TDOA Wi-Fi receiver name. Click **View List** to see a full list of Alarms.

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

Figure 8-24 Search Results Window



- b. To initiate an advanced search for a TDOA receiver by its MAC address or name, click Advanced Search in the navigation bar.
 1. Select **WiFi TDOA Receiver** as the search category.
 2. Select either **WiFi TDOA Receivers Name** or **MAC Address** from the Search for WiFi TDOA Receiver by drop-down menu.
 3. Enter either the TDOA receiver name or MAC address.
 4. Click **Search**.

This example shows an advanced search using the MAC address (see Figure 8-25).

Figure 8-25 Advanced Search Panel

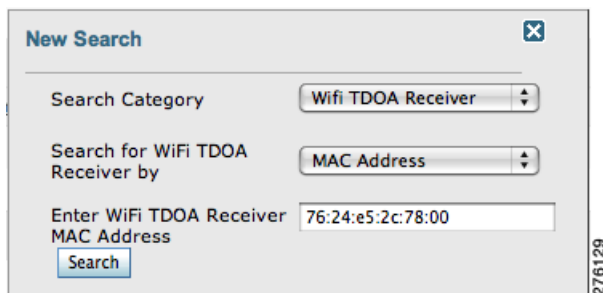
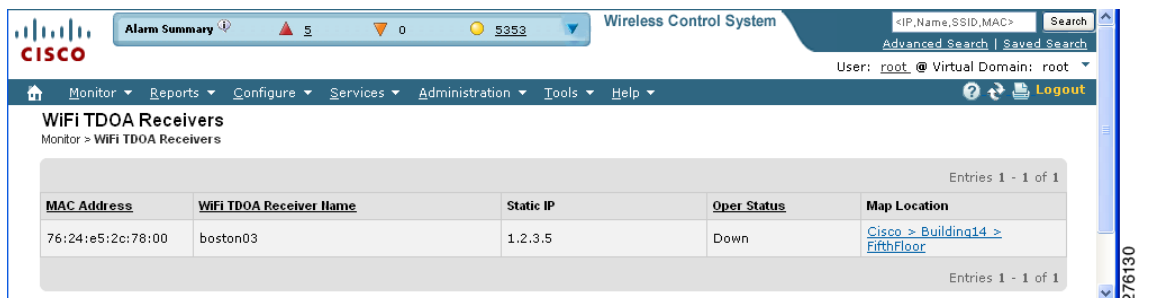


Figure 8-26 shows the search results.

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

Figure 8-26 WiFi TDOA Receivers Advanced Search Results Indicating a Match





CHAPTER 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, page 9-2](#)
- [Recovering a Lost Root Password, page 9-2](#)
- [Backing Up and Restoring Location Server Data, page 9-2](#)
- [Downloading Software to Location Servers, page 9-4](#)
- [Configuring NTP Server, page 9-6](#)
- [Defragmenting the Location Server Database, page 9-7](#)
- [Rebooting the Location Server Hardware, page 9-8](#)
- [Shutting Down the Location Server Hardware, page 9-8](#)
- [Clearing the System Database, 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, choose **Services > Mobility Services**.
 - Step 2** Click the name of the mobility services engine that you want to back up.
 - Step 3** Choose **System > Maintenance**.
 - Step 4** Click **Backup**.
 - Step 5** Enter the name of the backup.
 - Step 6** Enter the time in seconds after which the backup times out.



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 cannot run the backup process in the background while working on other location server operations in other Cisco 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, choose **Services > Mobility Services**.
 - Step 2** Click the name of the location server that you want to restore.
 - Step 3** Choose **System > Maintenance**.

- Step 4** Click **Restore**.
- Step 5** Choose the file to restore from the drop-down menu.
- Step 6** Enter the time in seconds after which restoration times out.



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 the data from the Cisco WCS server hard drive. When restoration is completed, Cisco WCS displays a message to that effect.
-

Enabling Automatic Location Data Backup

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

To enable automatic location 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, choose **Services > Mobility Services**.
 - Step 3** Click the name of the server to which you want to download the software.
 - Step 4** Choose **Maintenance > Download Software** (left).

Step 5 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 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 Server** and click **Browse**. Locate the file and click **Open**.

Step 6 Enter the time in seconds (between 1 and 1800) after which software download times out.

Step 7 Click **Download** to send the software to the `/opt/locserver/installers` directory on the location server.

Step 8 After the image is transferred to the location server, log into the location server CLI.

Step 9 Run the installer image from the `/opt/installers` directory by entering `./bin locserver image`. This installs the software.

Step 10 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.

- 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-x-x-x-x-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 bootstrap, 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, choose **Services > Mobility Services**.
 - Step 2** Click the name of the location server that you want to defragment its database.
 - Step 3** Choose **System > Advanced Parameters** (left).
 - Step 4** In the Advanced Commands section, click **Defragment Database**.
 - Step 5** 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, choose **Services > Mobility Services**.
 - Step 2** Click the name of the location server that you want to reboot.
 - Step 3** Choose **System > Advanced Parameters** (left).
 - Step 4** In the Advanced Commands section (right), click **Reboot Hardware**.
 - Step 5** 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, choose **Services > Mobility Services**.
 - Step 2** Click the name of the location server that you want to shutdown.
 - Step 3** Choose **System > Advanced Parameters** (left).
 - Step 4** In the Advanced Commands section (right), click **Shutdown Hardware**.
 - Step 5** Click **OK** to confirm that you want to shutdown the location server.
-

Clearing the System Database

To clear the database of a location server, follow these steps:

-
- Step 1** In Cisco WCS, choose **Services > Mobility Services**.
 - Step 2** Click the name of a location server for which you want to clear its database.
 - Step 3** Choose **System > Advanced Parameters**.
 - Step 4** In the Advanced Commands section of the window (right), click the **Clear Configuration** button.



Note The Clear Configuration command clears the database not the configuration file.

Click **OK** in the confirmation pop-up window to clear the location server database. Click **Cancel** to stop the process.
