Cisco Context-Aware Service Configuration Guide

Release 7.0

June 2010

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-21793-01
Contents

Preface vii

Objectives vii
Audience vii
Conventions vii
Related Documentation ix
Obtaining Documentation and Submitting a Service Request ix

Chapter 1

Overview 1-1
Cisco Context-Aware Mobility Solution Overview 1-2
Cisco 3300 Series Mobility Services Engines 1-2
CAS 1-3
Licensing for Clients and Tags 1-3
Viewing Contextual Information 1-3
Event Notification 1-4
Configuration and Administration 1-4
Adding and Deleting a Mobility Services Engine 1-5
Editing Mobility Services Engine Properties 1-5
Editing CAS Properties 1-5
Managing Users and Groups 1-6
Mobility Services Engine Synchronization 1-6
Context-Aware Planning and Verification 1-6
Monitoring Capability 1-6
Maintenance Operations 1-7
System Compatibility 1-7

Chapter 2

Adding and Deleting Mobility Services Engines and Licenses 2-1
Adding a Mobility Services Engine to WCS 2-2
Deleting a Mobility Services Engine from the WCS 2-3
Registering Client and wIPS Product Authorization Keys 2-3
Installing Client and wIPS License Files 2-7
Registering Tag PAKs 2-8
Installing Tag Licenses 2-8
CHAPTER 6 Configuring Event Notifications 6-1
   Adding and Deleting Event Groups 6-2
      Adding Event Groups 6-2
      Deleting Event Groups 6-2
   Adding, Deleting, and Testing Event Definitions 6-3
      Adding an Event Definition 6-3
      Deleting an Event Definition 6-6
      Testing Event Definitions 6-7
   Viewing Event Notification Summary 6-7
   Clearing Notifications 6-8
   Notification Message Formats 6-9
      Notification Formats in XML 6-9
         Missing (Absence) Condition 6-9
         In/Out (Containment) Condition 6-9
         Distance Condition 6-10
         Battery Level 6-11
         Location Change 6-11
         Chokepoint Condition 6-11
         Emergency Condition 6-11
      Notification Formats in Text 6-11
   WCS as a Notification Listener 6-12

CHAPTER 7 Context-Aware Planning and Verification 7-1
   Planning for Data, Voice, and Location Deployment 7-2
   Creating and Applying Calibration Models 7-4
   Inspecting Location Readiness and Quality 7-9
      Inspecting Location Readiness Using Access Point Data 7-9
      Inspecting Location Quality Using Calibration Data 7-10
   Verifying Location Accuracy 7-10
      Using the Location Accuracy Tool to Test Location Accuracy 7-10
      Using Scheduled Accuracy Testing to Verify Accuracy of Current Location 7-11
      Using On-Demand Location Accuracy Testing 7-12
   Using Chokepoints to Enhance Tag Location Reporting 7-13
      Adding Chokepoints to the WCS 7-13
      Removing Chokepoints from WCS 7-19
   Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting 7-19
      Adding Wi-Fi TDOA Receivers to WCS 7-20
      Removing Wi-Fi TDOA Receivers from WCS 7-22
Using Tracking Optimized Monitor Mode to Enhance Tag Location Reporting 7-22
Defining Inclusion and Exclusion Regions on a Floor 7-23
Guidelines 7-24
Defining an Inclusion Region on a Floor 7-24
Defining an Exclusion Region on a Floor 7-27
Defining a Rail Line on a Floor 7-29
Modifying Context-Aware Service Parameters 7-33
Modifying Tracking Parameters 7-34
Modifying Filtering Parameters 7-38
Modifying History Parameters 7-41
Enabling Location Presence 7-42
Importing Asset Information 7-43
Exporting Asset Information 7-43
Modifying Location Parameters 7-44
Enabling Notifications and Configuring Notification Parameters 7-46
Enabling Notifications 7-46
Configuring Notification Parameters 7-46
Viewing Notification Statistics 7-48
Configuring a Location Template 7-49
Enabling Location Services on Wired Switches and Wired Clients 7-52
Configuring a Catalyst Switch 7-53
Adding a Catalyst Switch to WCS 7-55
Assigning and Synchronizing a Catalyst Switches to a Mobility Services Engine 7-56
Verifying an NMSP Connection to a Mobility Services Engine 7-57

CHAPTER 8 Monitoring the System and Services 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 8-5
Working with Logs 8-5
Configuring Logging Options 8-6
MAC Address-based Logging 8-7
Downloading Log Files 8-7
Generating Reports 8-7
Creating a Device Utilization Report 8-8
Viewing Saved Utilization Reports 8-11
Viewing Scheduled Utilization Runs 8-11
Monitoring Wireless Clients 8-11
  Monitoring Wireless Clients Using Maps 8-11
  Monitoring Wireless Clients Using Search 8-13
Monitoring Tags 8-15
  Monitoring Tags Using Maps 8-15
  Monitoring Tags Using Search 8-18
  Overlapping Tags 8-22
Monitoring Chokepoints 8-23
Monitoring Wi-Fi TDOA Receivers 8-24
Monitoring Wired Switches 8-26
Monitoring Wired Clients 8-29
Monitoring Interferers 8-32
  Monitor > Interferers > AP Detected Interferers 8-32
  Monitor > Interferers > AP Detected Interferers > Interferer Details 8-33
  Monitor > Interferers > AP Detected Interferer Details > Interference Device ID > Location History 8-34
  Monitor > Interferers > Edit View 8-35

CHAPTER 9
Performing Maintenance Operations 9-1
  Recovering a Lost Password 9-1
  Recovering a Lost Root Password 9-2
  Backing Up and Restoring Mobility Services Engine Data 9-2
    Backing Up Mobility Services Engine Historical Data 9-2
    Restoring Mobility Services Engine Historical Data 9-3
    Enabling Automatic Location Data Backup 9-4
  Downloading Software to Mobility Services Engines 9-4
    Manually Downloading Software 9-5
  Configuring NTP Server 9-6
  Resetting the System 9-6
  Defragmenting the Database 9-6
  Clearing the Configuration File 9-6
Preface

This preface introduces the Cisco Context-Aware Service Configuration Guide and contains the following sections:

- Objectives, page vii
- Audience, page vii
- Conventions, page vii
- Related Documentation, page ix
- Obtaining Documentation and Submitting a Service Request, page ix

Objectives

This guide describes how to use the Cisco Wireless Control System (WCS) to configure and manage the Cisco 3300 Series Mobility Services Engine and the Context-Aware Service, which resides on the mobility services engine.

Audience

The purpose of this guide is to help you configure and manage the Context-Aware Service. Before you begin, you should be familiar with network structures, terms, and concepts.

Conventions

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

- Command and keywords appear in **boldface**.
- *Italics* indicate arguments for which you supply values.
- Series of menu options appear as `option > option`.

Examples use the following conventions:

- Examples depict screen displays and the command line in screen font.
- Information you need to enter in examples is shown in **bold screen** font.
- Variables for which you must supply a value are shown in *italic screen* font.
Note
Means reader take note. Notes contain helpful suggestions or references to materials not contained in the manual.

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

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

Related Documentation

See the Cisco 3350 Mobility Services Engine Getting Started Guide or Cisco 3310 Mobility Services Engine Getting Started Guide which describe how to install and set up mobility services engines.

These documents are available on the Cisco.com website at the following URL:


Obtaining Documentation and Submitting a Service Request

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


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

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

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

This chapter contains the following sections:

- Cisco Context-Aware Mobility Solution Overview, page 1-2
- Viewing Contextual Information, page 1-3
- Event Notification, page 1-4
- Configuration and Administration, page 1-4
- Mobility Services Engine Synchronization, page 1-6
- Context-Aware Planning and Verification, page 1-6
- Monitoring Capability, page 1-6
- Maintenance Operations, page 1-7
- System Compatibility, page 1-7
Cisco Context-Aware Mobility Solution Overview

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

This section contains the following topics:
- Cisco 3300 Series Mobility Services Engines, page 1-2
- CAS, page 1-3

Cisco 3300 Series Mobility Services Engines

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

There are two models of the mobility services engine:
- Cisco 3350 Mobility Services Engine
- Cisco 3310 Mobility Services Engine
CAS

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

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

Licensing for Clients and Tags

You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points.

- Licenses for tags and clients are offered separately. (The clients license also includes tracking of rogue clients, rogue access points, interferers, and wired clients).
- For more information on tags, clients, rogue clients, and rogue access points, see Chapter 7, “Context-Aware Planning and Verification”.
- Licenses for tags and clients are offered in various quantities, ranging from 1,000 to 12,000 units. Up to 18,000 Wi-Fi clients and Wi-Fi tags (combined count) are supported depending on the mobility services engine hardware.
  - Cisco 3350 mobility services engine supports up to 18,000 clients and tags (combined count).
  - Cisco 3310 mobility services engine supports up to 2,000 clients and tags (combined count).
- For details on tag and client licenses, see Cisco 3300 Series Mobility Services Engine Release Note, Release 6.0 at the following URL: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html
- For details on adding client and tag licenses to the mobility services engine, see Chapter 2, “Adding and Deleting Mobility Services Engines and Licenses”.

Viewing Contextual Information

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

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

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

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

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

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

**Note**

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

![Figure 1-2 Pull Communication Model](image)

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

Configuration and Administration

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

This section contains the following topics:

- Adding and Deleting a Mobility Services Engine, page 1-5
- Editing Mobility Services Engine Properties, page 1-5
- Editing CAS Properties, page 1-5
- Managing Users and Groups, page 1-6
Adding and Deleting a Mobility Services Engine

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

Editing Mobility Services Engine Properties

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

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

Editing CAS Properties

You can use WCS to configure the following parameters for CAS. See Chapter 7, “Context-Aware Planning and Verification,” for configuration details.

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

CAS incorporates and expands the function of Cisco location-based services software.

- Tracking Parameters: Enables you to define the mobile assets (such as client stations, active asset tags; rogue clients and access points, and interferers) that you want to actively track, set limits on how many of a specific mobile asset you want to track, and disable tracking and reporting of ad hoc rogue clients and access points.
- Filtering Parameters: Enables you to define filters to exclude probing clients as well as tags and non-probing clients based on their MAC addresses.
  - Probing clients are clients which are not associated to any access point but are being seen in the network because of their probing activity. They are counted as a client by the probed controller as well as its primary controller.
Mobility Services Engine Synchronization

- History Parameters: Enables you to log history of the devices located by the mobility services engine.
- Presence Parameters: Enables you to enable location presence on a mobility services engine to provide expanded Civic (city, state, postal code, country) and GEO (longitude, latitude) location information beyond the Cisco default setting (campus, building, floor, and X, Y coordinates). This information can then be requested by clients on a demand basis for use by location-based services and applications.
- Import and Export Asset Information: Enables you to import a file of formatted asset information from an external server and to export asset information to an external server.
- Import Civic Information: Enables you to import a file with civic information for use by the presence parameter for expanded location information.
- Location Parameters: Enables you to specify whether the mobility services engine retains its calculation times and how soon the mobility services engine deletes its collected RSSI measurement times. It also enables you to apply varying smoothing rates to manage location movement of an element.
- Notification Parameters: Enables you to define how often notifications are generated or resent by the mobility services engine. You can also enable forwarding of northbound notifications for tags to third-party applications.

Managing Users and Groups

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

Mobility Services Engine Synchronization

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

Context-Aware Planning and Verification

To plan and optimize access point deployment, you can use WCS to perform point or line calibration. Additionally, you can analyze the location accuracy of non-rogue clients, asset tags and interferers using the accuracy tool. See Chapter 7, “Context-Aware Planning and Verification,” for specifics.

Monitoring Capability

You can use WCS to monitor alarms, events, and logs generated by mobility services engine. You can also monitor the status of mobility services engines, clients, interferers, and tagged assets. Additionally, you can generate a utilization report for the mobility services engine to determine CPU and memory utilization as well as counts for clients, tags and rogue access points and clients. See Chapter 7, “Context-Aware Planning and Verification” and Chapter 8, “Monitoring the System and Services,” for more information.
Maintenance Operations

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

Note
Details on recovering GRUB and root passwords for the mobility services engine using the command-line interface (rather than WCS) are also addressed in Chapter 9, “Performing Maintenance Operations.”

System Compatibility

Note
Refer to the Cisco 3300 Mobility Services Engine Release Note for the latest system (controller, WCS, mobility services engine) compatibility information, feature support, and operational notes for your current release at the following URL:
Adding and Deleting Mobility Services Engines and Licenses

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

This chapter contains the following sections:

- Adding a Mobility Services Engine to WCS, page 2-2
- Deleting a Mobility Services Engine from the WCS, page 2-3
- Registering Client and wIPS Product Authorization Keys, page 2-3
- Installing Client and wIPS License Files, page 2-7
- Registering Tag PAKs, page 2-8
Adding a Mobility Services Engine to WCS

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

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

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

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

**Step 4**  In the Device Name text box, enter a name for the mobility services engine.

**Step 5**  In the IP Address text box, enter the IP address of the mobility services engine.

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

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

This refers to the WCS communication username and password created during the setup process.

If you have not specified username and password during the setup process, use defaults.

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, we recommend that you rerun the automatic installation script and change the username and password.

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

**Step 9**  Select the **Delete synchronized service assignments** check box if you want to permanently removes all service assignments from the mobility services engine.

This option is applicable for network designs, wired switches, controllers and event definitions. The existing location history data is retained, however you must use manual service assignments to do any future location calculations.

**Step 10**  Click **Next**. The Select Mobility Service page appears.

**Step 11**  To enable a service on the mobility services engine, select the check box next to that service.

**Note**  A mobility services engine can support multiple services.

**Step 12**  Click **Save**.

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

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

Step 1  Choose Services > Mobility Services to display the Mobility Services page.
Step 2  Select the mobility services engine to be deleted by selecting the corresponding check box.
Step 3  From the Select a command drop-down list, choose Delete Service(s). Click Go.
Step 4  Click OK to confirm that you want to delete the selected mobility services engine from the WCS database.
Step 5  Click Cancel to stop deletion.

Registering Client and wIPS Product Authorization Keys

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

Client and wIPS PAKs are registered with Cisco.

Note:  Tag PAKs are registered with AeroScout. Refer to the “Registering Tag PAKs” section on page 2-8.

To register a PAK to obtain a license file for install, follow these steps:

Step 1  Open a browser window and enter the following URL:
        www.cisco.com/go/license.
Step 2  Enter the PAK and click SUBMIT (see Figure 2-1).
Step 3   Verify the license purchase. Click **Continue** if correct (see Figure 2-2). The licensee entry page appears (see Figure 2-3).

*Note*   If the license is incorrect, click **TAC Service Request Tool** link (right) to report the problem.
Step 4  In the Designate Licensee page, enter the UDI of the mobility service engine in the host ID text box. This is the mobility services engine on which the license will be installed.

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

Step 5  Select the Agreement check box. Registrant information appears beneath the Agreement check box (see Figure 2-4).

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

Step 6  If registrant and end user are not the same person, select the **Licensee (End-User)** check box beneath registrant information and enter the information for the end user.

Step 7  Click **Continue**. A summary of entered data appears (see **Figure 2-5**).

**Figure 2-5**  Finish and Submit Page

Step 8  If the Finish and Submit page, review registrant, and end user data. Click **Edit Details** to correct information. Click **Submit**. A confirmation page appears (see **Figure 2-6**).

**Figure 2-6**  Registration Confirmation Page
Installing Client and wIPS License Files

You can install client and wIPS licenses from WCS.
Tag licenses are installed using the AeroScout System Manager. Refer to the “Installing Tag Licenses” section on page 2-8.

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

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

**Step 2** Choose Files > MSE Files from the left sidebar menu.

**Step 3** Click Add. The Add a License File dialog box appears (see Figure 2-8).

**Step 4** Choose the applicable MSE name from the MSE Name drop-down list.

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

To register tags at the AeroScout website, follow these steps:

**Step 1** Open a browser and enter [http://www.aeroscout.com/content/support](http://www.aeroscout.com/content/support).

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

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

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

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

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

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

Installing Tag Licenses

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

Refer to the users guide for details on installed your tag licenses at the following URL:

[http://support.aeroscout.com](http://support.aeroscout.com)
Synchronizing Mobility Services Engines

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

This chapter contains the following sections:

- Synchronizing WCS and Mobility Services Engines, page 3-2
- Synchronizing Controllers with Mobility Services Engine, page 3-5
- Configuring Automatic Database Synchronization and Out of Sync Alerts, page 3-6
- Viewing Mobility Services Engine Synchronization Status, page 3-8
Synchronizing WCS and Mobility Services Engines

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

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

- Network Design—Is a logical mapping of the physical placement of access points throughout facilities. A hierarchy of a single campus, the buildings that comprise that campus, and the floors of each building constitute a single network design.
- Controller—A selected controller that is associated and regularly exchanges location information with a mobility services engine. Regular synchronization ensures location accuracy.
- Switches (wired)—Wired Catalyst switches that provide an interface to wired clients on the network. Regular synchronization ensures that location tracking of wired clients in the network is accurate.
  - The mobility services engine can be synchronized with Catalyst stackable switches (3750, 3750-E, 3560, 2960, IE-3000 switches), switch blades (3110, 3120, 3130, 3040, 3030, 3020), and switch ports.
  - The mobility services engine can also be synchronized with the following Catalyst 4000 series: WS-C4948, WS-C4948-10GE, ME-4924-10GE, WS-4928-10GE, WS-C4900M, WS-X4515, WS-X4516, WS-X4013+, WS-X4013+TS, WS-X4516-10GE, WS-X4013+10GE, WS-X45-SUP6-E, and WS-X45-SUP6-LE
- Event Groups—A group of predefined events that define triggers that generate an event. Regular synchronization ensures that the latest defined events are tracked. Event groups can also be created by third-party applications. For more information on third-party application created event groups, see Configuring Automatic Database Synchronization and Out of Sync Alerts, page 3-6.

Note

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

Note

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

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

**Step 1** Choose Services > Synchronize Services.

Four menu items appear with the following headings: Network Designs, Controllers, Switches, and Event Groups.

**Step 2** Choose the appropriate menu option (network designs, controllers, wired switches, or event groups). See, Figure 3-1 for more information.
Step 3 To assign a network design to a mobility services engine, in the synchronization page, choose Network Designs from the the left sidebar menu.

Step 4 Choose all the maps to be synchronized with the mobility services engine.

Note Through Release 6.0, you can assign only up to a campus level to a mobility services engine. Starting with Release 7.0 this option is granular to a floor level. For example, you can choose to assign floor1 to MSE 1, floor2 to MSE 2, and floor3 to MSE 3.

Step 5 Click Change MSE Assignment.

Step 6 Select the mobility services engine to which the maps are to be synchronized. See Figure 3-2 for more information.

Step 7 Click either of the following in the MSE Assignment dialog box:

- Save—Saves the mobility services engine assignment. The following message appears in the Messages column of the Network Designs page with yellow arrows icon:
  
  To be assigned - Please synchronize.

- Cancel—Discards the changes to mobility services engine assignment and returns to the Network Designs page.

You can also click Reset to undo the mobility services engine assignments.
A network design may include a floor in a campus or a large campus with several buildings, each monitored by a different mobility services engine. Because of this, you may need to assign a single network design to multiple mobility services engines.

Network design assignments also automatically picks up the corresponding controller for synchronization.

**Step 8** Click **Synchronize** to update the mobility services engine(s) database(s).

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

You can use the same procedure to assign wired switches or event groups to a mobility services engine. To assign a controller to a mobility services engine, see *Synchronizing Controllers with Mobility Services Engine*, page 3-5 for more information.

### Working with Third Party Elements

When you synchronize elements with MSE, there might be event groups on the MSE that have been created by third party applications. You can either delete the unused elements or mark them as third party elements.

To delete the elements or mark them as third party elements:

**Step 1** In the synchronization page, choose **Third Party Elements** from the left sidebar menu.

The Third Party Elements page appears.

**Step 2** Select one or more elements.
Step 3  Click one of these buttons:
- Delete Event Groups—Deletes the selected event groups.
- Mark as 3rd Party Event Group(s)—Marks the selected event groups as third party event groups.

**Synchronizing Controllers with Mobility Services Engine**

You can assign an MSE to any wireless controller on a per-service (CAS or wIPS) basis. To associate a mobility services engine with a controller, follow these steps:

**Step 1**  In the Synchronization page, choose controller from the left sidebar menu.

**Step 2**  Choose the controllers to be assigned to the mobility services engine.

**Step 3**  Click **Change MSE Assignment**.

**Step 4**  Choose the mobility services engine to which the controllers have to be synchronized.

**Step 5**  Click either of the following in the Choose MSEs dialog box:
- Save—Saves the mobility services engine assignment. The following message appears in the Messages column of the Controllers page with yellow arrows icon:
  
  To be assigned - Please synchronize.

- Cancel—Discards the changes to mobility services engine assignment and returns to the Controllers page.

You can also click **Reset** to undo the mobility services engine assignments.

**Step 6**  Click **Synchronize** to complete the synchronization process.

**Step 7**  Check if the mobility services engine is communicating with each of the controller for only the chosen service. This can be done by clicking the NMSP status link on the status page.

**Note**
- After Synchronizing a controller, verify that the timezone is set on the associated controller.
- Controller names must be unique for synchronizing with a mobility services engine. If you have two controllers with the same name, only one will be synchronized.
- The smart controller assignment can be overridden by removing the assignment. This will be indicated in the Message field. In this case, any AP changes on the floor will not auto assign the controller and you have to manually assign the controller to remove the override.

You can use the same procedure to assign Catalyst switches or event groups to a mobility services engine.

**Note**
- A switch can only be synchronized with one mobility services engine. However, a mobility services engine can have many switches attached to it.
Chapter 3  Synchronizing Mobility Services Engines

To unassign a network design, controller, wired switch, or event group from a mobility services engine, follow these steps:

Step 1  On the respective tabs, choose one or more elements and click Change MSE Assignment. The choose mobility services engine dialog box appears.

Step 2  Unselect the mobility services engine if you do not want the elements to be associated with that mobility services engine.

Step 3  Click Save to save the changes to the assignments.

Step 4  Click Synchronize. Sync Status column appears blank.

Configuring Automatic Database Synchronization and Out of Sync Alerts

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

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

Any change to one or more of any synchronized component will be automatically synchronized with the mobility services engine. For example, if a floor with access points is synchronized with a particular mobility services engine and then one access point is moved to a new location on the same floor or another floor which is also synchronized with the mobility services engine, then the changed location of the access point will be automatically communicated.

To further ensure that WCS and MSE are in sync, Smart Synchronization happens in the background. This section includes the following topics:

- Configuring Automatic Database Synchronization, page 3-6
- Smart Controller Assignment and Selection Scenarios, page 3-7
- Out-of-Sync Alarms, page 3-8

Configuring Automatic Database Synchronization

To configure smart synchronization, follow these steps:

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

Step 2  Select the Mobility Service Synchronization check box.

Step 3  Click the Mobility Service Synchronization link.

Step 4  To set the mobility services engine to send out-of-sync alerts, select the Out of Sync Alerts Enabled check box.
Step 5 To enable smart synchronization, select the Smart Synchronization Enabled check box.

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

Note When a mobility services engine is added to a WCS, the data in the WCS is always treated as the primary copy that is synchronized with the mobility services engine. All synchronized network designs, controllers, event groups and wired switches that are present in the mobility services engine and not in the WCS are removed automatically from mobility services engine.

Step 6 Enter the time interval in minutes that the smart synchronization is to be performed.
By default, smart-sync is enabled.

Step 7 Click Submit.

For Smart controller assignment and selection scenarios, see Smart Controller Assignment and Selection Scenarios, page 3-7.

Smart Controller Assignment and Selection Scenarios

Scenario 1
If a floor having at least one access point from a controller is chosen to be synchronized with the mobility services engine from the Network Designs section of the Synchronization page, then the controller to which that access point is connected is automatically selected to be assigned to the mobility services engine for CAS service.

Scenario 2
When at least one access point from a controller is placed on a floor that is synchronized with mobility services engine, the controller to which the access point is connected is automatically assigned to the same mobility services engine for CAS service.

Scenario 3
An access point is added to a floor and is assigned to an mobility services engine. If that access point is moved from controller A to controller B, then controller B is automatically synchronized to the mobility services engine.

Scenario 4
If all access points placed on a floor which is synchronized to the MSE are deleted then that controller is automatically removed from mobility services engine assignment or unsynchronized.
Out-of-Sync Alarms

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

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

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

- Mobility services engine is deleted

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

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

Viewing Mobility Services Engine Synchronization Status

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

To view synchronization status, follow these steps:

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

**Step 2** Select the applicable menu option (Network Designs, Controllers, Wired Switches, or Event Groups).

For each of the elements, the Sync. Status column shows the synchronization status. A green two-arrow icon indicates that its corresponding element is synchronized with the specified server such as a mobility services engine. A gray two-arrow icon with a red circle indicates that its corresponding item is not synchronized with a given server.

The Message column displays the reason for failure if the elements are out of sync.

You can also view the synchronization status and assign or unassign from campus view and building view along with floor view.

To access this page, choose Monitor > Maps > System Campus > Building > Floor

where Building is the building within the Campus and Floor is a specific floor in that campus building.

On the left sidebar menu, there is an option MSE Assignment. This shows which mobility services engine the floor is currently assigned to. You can also change mobility services engine assignment from this page.
Viewing Synchronization History

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

To view synchronization history, follow these steps:

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

![Figure 3-3 Mobility > Synchronization History](image)

**Step 2** Table 3-1 lists and describes the text boxes that appear in the Synchronization History page.

<table>
<thead>
<tr>
<th>Text Box</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>The date and time at which the synchronization has happened.</td>
</tr>
<tr>
<td>Server</td>
<td>The mobility services engine server.</td>
</tr>
<tr>
<td>Element Name</td>
<td>The name of the element that was synchronized.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of the element that was synchronized.</td>
</tr>
<tr>
<td>Sync Operation</td>
<td>The sync operation that was performed. It could either be an Update or an Add or Delete.</td>
</tr>
<tr>
<td>Generated By</td>
<td>The method of synchronization. It could either be Manual or Automatic.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the synchronization. It could be either Success or Failed.</td>
</tr>
<tr>
<td>Message</td>
<td>Any additional message about the synchronization.</td>
</tr>
</tbody>
</table>
Click the column headers to sort the entries.
This chapter describes how to configure and view system properties on the mobility services engine. This chapter contains the following sections:

- Editing General Properties and Viewing Performance, page 4-1
- Modifying NMSP Parameters, page 4-5
- Viewing Active Sessions on a System, page 4-7
- Adding and Deleting Trap Destinations, page 4-7
- Viewing and Configuring Advanced Parameters, page 4-8
- Initiating Advanced Parameters, page 4-9

### Editing General Properties and Viewing Performance

General Properties—You can use WCS to edit the general properties of a mobility services engine such as contact name, username, password, services enabled on the system, enabling or disabling a service or enabling the mobility services engine for synchronization. See the “Editing General Properties” section on page 4-1.

Note

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

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

This section consists of the following topics:

- Editing General Properties, page 4-1
- Viewing Performance Information, page 4-5

### Editing General Properties

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

**Step 1**

In WCS, choose **Services > Mobility Services** to display the Mobility Services page.
Step 2  Click the name of the mobility services engine you want to edit. Two tabs appear with the following headings: General and Performance (see Figure 4-1).

Figure 4-1  Services > Mobility Services > General Properties

If the General Properties page does not appear by default, from the left sidebar menu, choose System > General Properties.

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

Table 4-1  General Properties

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Name</td>
<td>Enter a contact name for the mobility services engine.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the login username for the WCS server that manages the mobility services engine. This replaces any previously defined username including any set during initial setup.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the login password for the WCS server that manages the mobility services engine. This replaces any previously defined password including any set during initial setup.</td>
</tr>
<tr>
<td>Port</td>
<td>8001</td>
</tr>
<tr>
<td></td>
<td>This is a default value.</td>
</tr>
</tbody>
</table>
### Table 4-1 General Properties (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>Select the <strong>Enable</strong> check box to enable HTTP. By default, HTTPS is enabled.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>HTTP is primarily enabled to allow third-party applications to communicate with the mobility services engine.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>WCS always communicates through HTTPS.</td>
</tr>
<tr>
<td>Legacy Port</td>
<td>Enter the mobility services port number that supports HTTPS communication. The Legacy HTTPS option must also be enabled.</td>
</tr>
<tr>
<td>Legacy HTTPS</td>
<td>This parameter does not apply to mobility services engines. It applies only to location appliances.</td>
</tr>
<tr>
<td>Delete synchronized service assignments and enable synchronization</td>
<td>Select this check box if you want to permanently remove all service assignments from the mobility services engine. This option will show up only if the delete synchronized service assignments check box was unselected while adding an mobility services engine.</td>
</tr>
<tr>
<td>Mobility Services</td>
<td>To enable a service (CAS, wIPS) on a mobility services engine, select the <strong>Admin Status</strong> check box next to the service you want to enable.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Once selected, the service displays as Up (active). All inactive services are noted as Down (inactive) on the selected (current) system and on the network.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>CAS and wIPS can operate on a mobility services engine at the same time.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>All mobility services engines are shipped with an evaluation license of CAS and wIPS. Evaluation copies are good for a period of 60 days (480 hours) and have preset device limits for each service. Licenses are usage-based (time is decremented by the number of days you use it rather than by calendar days passed).</td>
</tr>
<tr>
<td>Click the <a href="http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html">here</a> link to see the number of devices that can be assigned for the current system (see Figure 4-1).</td>
<td></td>
</tr>
<tr>
<td>On the License Center page (see Figure 4-2), click <a href="http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html">MSE</a> sidebar menu option to see details on licenses for all mobility services engines on the network (see Figure 4-3).</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>For more information on purchasing and installing licenses, see the following URL:</td>
</tr>
</tbody>
</table>

**Note** The following tcp ports are in use on a mobility services engine (MSE) in Release 6.0: tcp 22: MSE SSH port, tcp 80: MSE HTTP port, tcp 443: MSE HTTPS port, tcp 1411: AeroScout, tcp 1999: AeroScout internal port, tcp 4096: AeroScout notifications port, tcp 5900X: AeroScout (X could vary from 1 to 10), and tcp 8001: Legacy port. Used for location APIs.
The following udp ports are in use on a mobility services engine (MSE) in release 6.0: udp 123: NTPD port (open after NTP configuration), udp 162: AeroScout SNMP, udp/tcp 4000X: AeroScout proxy (X could vary from 1 to 5), udp 12091: AeroScout devices (TDOA Wi-Fi Receivers, chokepoints), udp 12092: AeroScout devices (TDOA Wi-Fi Receivers, chokepoints), udp 32768: Location internal port, udp 32769: AeroScout internal port, and udp 37008: AeroScout internal port.

**Figure 4-2**  License Summary for Selected Mobility Services Engine

**Figure 4-3**  License Summary for All Mobility Services Engines

**Step 4**  Click Save to update the WCS and mobility services engine databases.
### Viewing Performance Information

To view performance details, follow these steps:

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

**Step 2** Click the name of the mobility services engine you want to view. Two tabs appear with the following headings: General and Performance.

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

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

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

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

### Figure 4-4  CPU and Memory Performance

![CPU and Memory Performance](image)

---

### Modifying NMSP Parameters

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

**Note**

- No change in the default parameter values is recommended unless the network is experiencing slow response or excessive latency.
- Telemetry, emergency and chokepoint information is only seen on controllers and WCS installed with Release 4.1 software or later.
Modifying NMSP Parameters

- The TCP port (16113) that the controller and mobility services engine communicate over must be open (not blocked) on any firewall that exists between the controller and mobility services engine for NMSP to function.

To configure NMSP parameters, follow these steps:

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

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

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

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

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

---

<table>
<thead>
<tr>
<th>Table 4-2</th>
<th>NMSP Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>Echo Interval</td>
<td>How frequently an echo request is sent from a mobility services engine to a controller. The default value is 15 seconds. Allowed values range from 1 to 120 seconds.</td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
</tr>
<tr>
<td>Neighbor Dead Interval</td>
<td>The number of seconds that the mobility services engine waits for a successful echo response from the controller before declaring the neighbor dead. This timer begins when the echo request is sent. The default value is 30 seconds. Allowed values range from 1 to 240 seconds.</td>
</tr>
<tr>
<td>Note</td>
<td>This value must be at least two times the echo interval value.</td>
</tr>
<tr>
<td>Response Timeout</td>
<td>How long the mobility services engine waits before considering the pending request as timed out. The default value is 1 second. Minimum value is 1. There is no maximum value.</td>
</tr>
<tr>
<td>Retransmit Interval</td>
<td>Interval of time that the mobility services engine waits between notification of a response timeout and initiation of a request retransmission. The default setting is 3 seconds. Allowed values range from 1 to 120 seconds.</td>
</tr>
<tr>
<td>Maximum Retransmits</td>
<td>The maximum number of retransmits that are sent in the absence of a response to any request. The default setting is 5. Allowed minimum value is 0. There is no maximum value.</td>
</tr>
</tbody>
</table>
Viewing Active Sessions on a System

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

For every session, WCS displays the following information:

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

To view active user sessions, follow these steps:

Step 1: In WCS, choose Services > Mobility Services.
Step 2: Click the name of the mobility services engine for which you want to view active sessions.
Step 3: Choose System > Active Sessions.

Adding and Deleting Trap Destinations

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

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

This section consists of the following topics:

- Adding Trap Destinations, page 4-7
- Deleting Trap Destinations, page 4-8

Adding Trap Destinations

To add a trap destination, follow these steps:

Step 1: In WCS, choose Services > Mobility Services.
Step 2: Click the name of the mobility services engine for which you want to define a new SNMP trap destination server.
Step 3: Choose System > Trap Destinations.
Step 4: From the Select a command drop-down list, choose Add Trap Destination. Click Go.
Step 5: Enter the IP address of the destination SNMP server.
Step 6: The Port number default of 162 is auto-populated. You can modify this as needed.
Viewing and Configuring Advanced Parameters

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

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

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

Step 9 Click Save.

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

Deleting Trap Destinations

To delete a trap destination, follow these steps;

Step 1 In WCS, choose Services > Mobility Services.
Step 2 Click the name of the mobility services engine for which you want to delete a SNMP trap destination server.
Step 3 Choose System > Trap Destinations.
Step 4 Select the check box next to the trap destination entry that you want to delete.
Step 5 From the Select a command drop-down list, choose Add Trap Destination. Click Go.
Step 6 In the message box that appears, click OK to confirm deletion.

Viewing and Configuring Advanced Parameters

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

- Refer to the “Viewing Advanced Parameters Settings” section on page 4-8 to view current system-level advanced parameters.
- Refer to the “Initiating Advanced Commands” section on page 4-10 to modify the current system-level advanced parameters or initiate advanced commands such as system reboot, system shutdown, clear a configuration file, or defragment the system database.

Viewing Advanced Parameters Settings

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

Step 1 In WCS, choose Services > Mobility Services.
Step 2 Click the name of a mobility services engine to view its status.
Step 3  Choose System > Advanced Parameters (see Figure 4-5).

![Figure 4-5 Services > Mobility Services > System > Advanced Parameters]

Initiating Advanced Parameters

The Advanced Parameters section of WCS enables you to set the number of days events are kept and set session time out values. It also enables you to initiate a system reboot or shutdown, clear the system database, or defragment a database.

**Note**

You can use WCS to modify troubleshooting parameters for a mobility services engine or a location appliance.

In the Advanced Parameters page, you can use WCS:

- To set how long events are kept and how long before a session times out.
  
  For more information, see the Configuring Advanced Parameters, page 4-10.

- To initiate a system reboot or shutdown, clear the system database, or defragment a database.
  
  For more information, see the Initiating Advanced Commands, page 4-10.
Configuring Advanced Parameters

To configure advanced parameters, follow these steps:

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

**Step 2** Click the name of the mobility service whose properties you want to edit.

**Step 3** From the left sidebar menu, choose System > Advanced Parameters.

**Step 4** View or modify the advanced parameters as necessary.

- **General Information**
- **Advanced Parameters**
  - Number of Days to keep Events—Enter the number of days to keep logs. Change this value as required for monitoring and troubleshooting.
  - Session Timeout—Enter the number of minutes before a session times out. Change this value as required for monitoring and troubleshooting. Currently this option is not configurable for the mobility services engine but configurable for location appliance.

- **Cisco UDI**
  - Product Identifier (PID)—The Product ID of the mobility services engine.
  - Version Identifier (VID)—The version number of the mobility services engine.
  - Serial Number (SN)—Serial number of the mobility services engine.

- **Advanced Commands**
  - Reboot Hardware—Click to reboot the mobility services hardware. See Rebooting or Shutting Down a System, page 4-11 for more information.
  - Shutdown Hardware—Click to turn off the mobility services hardware. See Rebooting or Shutting Down a System, page 4-11 for more information.
  - Clear Database—Click to clear the mobility services database. See Clearing the System Database, page 4-11 for more information. Unselect the Retain current service assignments in WCS check box to remove all existing service assignments from WCS and MSE. The resources have to be reassigned in the Services > Synchronize Services page. By default this option is selected.
  - Defragment Database—Click to initiate a defragmentation of the mobility services database. See Defragmenting The Database, page 4-11 for more information.

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

Initiating Advanced Commands

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

This section consists of the following topics:

- **Rebooting or Shutting Down a System, page 4-11**
- **Clearing the System Database, page 4-11**
Rebooting or Shutting Down a System

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

1. In WCS, choose Services > Mobility Services.
2. Click the name of a mobility services engine you want to reboot or shut down.
3. Choose System > Advanced Parameters (see Figure 4-5).
4. In the Advanced Commands section of the page, click the appropriate button (Reboot Hardware or Shutdown Hardware).

Click OK in the confirmation dialog box to initiate either the reboot or shutdown process. Click Cancel to stop the process.

Clearing the System Database

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

1. In WCS, click Services > Mobility Services.
2. Click the name of the mobility services engine you want to configure.
3. Choose System > Advanced Parameters.
4. In the Advanced Commands section, unselect the Retain current service assignments in WCS check box to remove all existing service assignments from WCS and MSE.

The resources have to be reassigned in the Services > Synchronize Services page. By default this option is selected.

5. In the Advanced Commands section, click Clear Database.
6. Click OK to clear the mobility services engine database.

Defragmenting The Database

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

1. In WCS, choose Services > Mobility Services.
2. Click the name of a mobility services engine whose database you want to defragment.
3. Choose System > Advanced Parameters (see Figure 4-5).
4. In the Advanced Commands section, click Defragment Database.

Click OK in the confirmation dialog box to initiate the process. Click Cancel to stop the process.
Managing Users and Groups

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

This chapter contains the following sections:
- Managing User Groups, page 5-1
- Managing Users, page 5-3

Managing User Groups

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

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

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

This section consists of the following topics:
- Adding User Groups, page 5-1
- Deleting User Groups, page 5-2
- Changing User Group Permissions, page 5-2

Adding User Groups

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

Step 1 In WCS, choose Services > Mobility Services.
Step 2 Click the name of the mobility services engine to which you want to add a user group.
Step 3 Choose System > Accounts > Groups.
Step 4 From the Select a command drop-down list, choose Add Group. Click Go.
Step 5 Enter the name of the group in the Group Name text box.
Step 6 Choose a permission level (read, write, or full) from the Permission drop-down list.
Managing User Groups

Chapter 5  Managing Users and Groups

Managing User Groups

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

Step 7  Click Save.

Deleting User Groups

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

Step 1  In WCS, choose Services > Mobility Services.
Step 2  Click the name of the mobility services engine from which you want to delete a user group.
Step 3  Choose System > Accounts > Groups.
Step 4  Select the check boxes of the groups that you want to delete.
Step 5  From the Select a command drop-down list, choose Delete Group. Click Go.
Step 6  Click OK.

Changing User Group Permissions

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

To change user group permissions, follow these steps:

Step 1  In WCS, choose Services > Mobility Services.
Step 2  Click the name of the mobility services engine you want to edit.
Step 3  Choose System > Accounts > Groups.
Step 4  Click the name of the group you want to edit.
Step 5  From the Permission drop-down list, choose a permission level (read, write, full).
Step 6  Choose Save.
Managing Users

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

This section consists of the following topics:
- Adding Users, page 5-3
- Deleting Users, page 5-3
- Changing User Properties, page 5-4

Adding Users

**Caution**

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

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

1. In WCS, choose **Services > Mobility Services**.
2. Click the name of the mobility services engine to which you want to add users.
3. Choose **System > Accounts > Users**.
4. From the Select a command drop-down list, choose **Add User**. Click **Go**.
5. Enter the username in the Username text box.
6. Enter a password in the Password text box.
7. Enter the name of the group to which the user belongs in the Group Name text box.
8. Click **Save**.

Deleting Users

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

1. In WCS, choose **Services > Mobility Services**.
2. Click the name of the mobility services engine from which you want to delete a user.
3. Choose **System > Accounts > Users**.
4. Select the check boxes of the users that you want to delete.
5. From the Select a command drop-down list, choose **Delete User**. Click **Go**.
6. Click **OK**.
Changing User Properties

To change user properties, follow these steps:

Step 1  In WCS, choose Services > Mobility Services.
Step 2  Click the name of the mobility services engine you want to edit.
Step 3  Choose System > Accounts > Users.
Step 4  Click the name of the group that you want to edit.
Step 5  Make the required changes to the Password and Group Name text boxes.
Step 6  Click Save.
Configuring Event Notifications

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

This chapter contains the following sections:

- Adding and Deleting Event Groups, page 6-2
- Adding, Deleting, and Testing Event Definitions, page 6-3
- Viewing Event Notification Summary, page 6-7
- Clearing Notifications, page 6-8
- Notification Message Formats, page 6-9
- WCS as a Notification Listener, page 6-12
Adding and Deleting Event Groups

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

This section consists of the following topics:
- Adding Event Groups, page 6-2
- Deleting Event Groups, page 6-2

Adding Event Groups

To add an event group, follow these steps:

Step 1  In WCS, choose Services > Context Aware Notifications.
Step 2  Choose Notification Settings.
Step 3  From the Select a command drop-down list, choose Add Event Group. Click Go.
Step 4  Enter the name of the group in the Group Name text box.
Step 5  Click Save.

The new event group appears in the Event Settings page.

Deleting Event Groups

To delete an event group, follow these steps:

Step 1  In WCS, choose Services > Context Aware Notifications.
Step 2  Choose Notification Settings.
Step 3  Select the event group to delete by selecting its corresponding check box.
Step 4  From the Select a command drop-down list, choose Delete Event Group(s). Click Go.
Step 5  In the panel that appears, click OK to confirm deletion.
Step 6  Click Save.
Adding, Deleting, and Testing Event Definitions

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

This section describes how to add, delete, and test event definitions and consists of the following topics:

- Adding an Event Definition, page 6-3
- Deleting an Event Definition, page 6-6
- Testing Event Definitions, page 6-7

Adding an Event Definition

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

To add an event definition, follow these steps:

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

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

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

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

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

**Tip**

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

To add a condition, follow these steps:

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

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

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

   - If you chose Missing from the Condition Type drop-down list, enter the number of minutes after which a missing asset generates a notification. For example, if you enter 10 in this text box, the mobility service engine generates a missing asset notification if the mobility service engine has not located the asset for more than 10 minutes after the devices has become inactive or is no longer in the system. This condition occurs when the controller detects its absence and informs mobility service engine about it or if the mobility service engine does not hear anything about this device from the controller for 60 minutes by default. This value is only configurable from the aes-config.xml file in the mobility service engine. Proceed to Step c.

   - If you chose In/Out from the Condition Type drop-down list, select Inside of or Outside of, then click Select Area. Entry and exit of assets from the selected area is then monitored. In the Select dialog box, choose the area to monitor, then click Select. The area to monitor could be an entire
Adding, Deleting, and Testing Event Definitions

Chapter 6 Configuring Event Notifications

 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 list, choose a building from the Building drop-down list, and choose the area to monitor from the Floor Area drop-down list. Then click Select. Proceed to Step c.

- If you chose Distance from the Condition Type drop-down list, enter the distance in feet from a designated marker beyond which an asset triggers an event notification. Click Select Marker. In the Select dialog box, select the campus, building, floor, and marker from the corresponding drop-down lists and click Select. For example, if you add a marker to a floor plan and set the distance in the Trigger If text box to 60 feet, an event notification will be generated if the monitored asset moves farther than 60 feet away from the marker. Proceed to Step c.

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

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

- If you chose Location Change from the Condition Type drop-down list, proceed to Step c.

- If you chose Emergency from the Condition Type drop-down list, click the button next to the appropriate emergency (any, panic button, tampered, detached) that will trigger a notification. Proceed to Step c.

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

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

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

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

d. For the Match By drop down list, there are three entries, left to right:

- Choose the matching criteria (MAC Address, Asset Name, Asset Group, or Asset Category) from the first drop-down list.

- Choose the operator (Equals or Like) from the second drop-down list.

- Enter the relevant text into the text box based on the Match By criteria you chose.

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

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

- If you choose MAC Address from the first drop-down list, choose Like from the second drop-down list, and enter 12:12 in the text box, the event condition applies to elements whose MAC address starts with 12:12.
Note: If the MAC address is a partial MAC it might cause a performance issue in WCS.

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 list boxes.
3. Select a Chokepoint from the menu that appears.

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

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

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

b. Click **Add New**.

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

The new entry is placed in the right column.

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

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

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

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

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

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

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

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

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

  If you choose **Mail**, you need to choose the protocol for sending the mail from the Mail Type drop-down list. 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.
Adding, Deleting, and Testing Event Definitions

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

- 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 text box, the name of the facility in the Facility text box, and the port number on the destination system in the Port Number text box.

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

h. The Port Number auto-populates.

i. Click Save.

Step 7 At the General tab, follow these steps:

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

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

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

c. Choose the frequency of notifications:

1. Select the All the Time check box to continuously report events. Proceed to Step g.

2. Unselect the All the Time check box to select the day and time of the week that you want event notifications sent. Days of the week and time text boxes appear for selection. Proceed to Step d.

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

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

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

g. Click Save.

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

Deleting an Event Definition

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

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

Step 2 Choose Notification Settings (left panel).

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

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

Step 5 From the Select a command drop-down list, choose Delete Event Definition(s). Click Go.
Click **OK** to confirm that you want to delete the selected event definition.

---

**Testing Event Definitions**

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

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

1. In WCS, choose **Services > Context Aware Notifications**.
2. Choose **Notification Settings** (left panel).
3. Click the name of the group containing the event definitions that you want to test.
4. Select the event definitions that you want to test by selecting their corresponding check boxes.
5. From the Select a command drop-down list, choose **Test-Fire Event Definition(s)**. Click **Go**.
6. Click **OK** to confirm that you want to test the event notifications.
7. Ensure that notifications were sent to the designated recipient.

---

**Viewing Event Notification Summary**

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

- **Absence (Missing)**—The mobility services engine generates an absence event when an asset goes missing. In other words, the mobility services engine cannot detect the asset in the WLAN for the specified time.
- **In/Out Area (Containment)**—The mobility services engine generates a containment event when an asset moves in or out of a designated area.
- **Movement from Marker (Movement/Distance)**—The mobility services engine generates a movement event when an asset is moved beyond a specified distance from a designated marker you define on a map.
- **Location Changes**—The mobility services engine generates location change events when a client station, asset tag, rogue client and rogue access point changes its location.
- **Battery Level**—The mobility services engine generates battery level events for all tracked asset tags.

---

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

- Emergency—The mobility services engine generates an emergency event for a Cisco CX v.1 compliant asset tag when the panic button of the tag is triggered or the tag becomes detached, is tampered with, becomes inactive, or reports an unknown state. This information is reported and displayed only for Cisco CX v.1 compliant tags.

- Chokepoint Notifications—The mobility services engine generates an event when a tag is stimulated by a chokepoint. This information is reported and displayed only for Cisco CX v.1 compliant tags.

Note
- All element events are summarized hourly and daily.
- The Track Group and events need to be synchronized with an mobility services engine for it to work.

To view event notifications, follow these steps:

Step 1
In WCS, choose Services > Context Aware Notifications.
WCS displays a summary of event notifications for each of the seven event notification categories.

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

Step 2
To view event notifications for a monitored asset, click one of its corresponding links.
For example, to view absence events for client stations generated in the last hour, click the link in the Last Hour column for the Client Stations entry in the Absence (Missing) list.
Clicking one of these links searches for location notifications of all severities.

Clearing Notifications

A mobility services engine sends event notifications when it clears an event condition in one of the following scenarios:
- Missing (Absence)—Elements (clients, tags, rogue access points, or rogue clients) reappear.
- In/Out Area (Containment)—Elements move back in to or out of the containment area.
- Distance—Elements move back within the specified distance from a marker.
- Location Changes—Clear state does not apply to this condition.
- Battery Level—Tags are detected again operating with normal battery level.

Note
In WCS, the Notifications Summary page reflects whether notifications for cleared event conditions have been received.
Notification Message Formats

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

Notification Formats in XML

This section describes the XML format of notification messages.

Note

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

Missing (Absence) Condition

Message format for element absence:

```xml
<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/>

For example:

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

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

In/Out (Containment) Condition

Message format for element containment:

```xml
<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>"
entityID="<mac address/>

For example:

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

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

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

<ContainmentTrackEvent state="clear" entityType="Tag"
trackDefn="myContainerRule1" entityID="00:0c:cc:5b:fa:44"/>

Distance Condition

Message format for elements on the same floor:

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

Message format for elements located on a different floor:

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

Message format for clear state:

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

For example:

<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

For example:

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

Location Change

For 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

For example:

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

An example for the clear state follows:

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

Emergency Condition

An example for element location follows:

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

Note

Emergency events are never cleared.

Notification Formats in Text

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

- 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 00:02:02:03:06 has moved 105 feet where the trigger distance was 90 feet.
WCS as a Notification Listener

WCS acts as a notification listener. WCS translates the traps into UI alerts and displays them in the following formats:

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

- **In/Out (Containment)**
  Tag with MAC 00:0c:cc:5b:fa:44 is In the Area 'Rochester > Rochester > 5th Floor > nycTestArea'

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

- **Battery Level**
  Tag 00:01:02:03:04:06 has medium battery, last seen 11:06:01 08 June 2009

- **Location Change**
  Mobile Station 00:01:02:03:04:05 has moved 158.11388300841898ft, where the trigger distance was 5.0
Context-Aware Planning and Verification

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

Context-Aware Service (CAS) installed on a mobility services engine retrieves location information as well as other contextual information such as temperature and asset availability about a client or tag (Cisco CX version 1 or later) from access points.

Note
Non-Cisco CX tags are not tracked or mapped by Cisco WCS.

Note
Context-Aware Service was previously referred to as Cisco location-based services.

This chapter contains the following sections:

- Planning for Data, Voice, and Location Deployment, page 7-2
- Creating and Applying Calibration Models, page 7-4
- Inspecting Location Readiness and Quality, page 7-9
- Verifying Location Accuracy, page 7-10
- Using Chokepoints to Enhance Tag Location Reporting, page 7-13
- Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting, page 7-19
- Using Tracking Optimized Monitor Mode to Enhance Tag Location Reporting, page 7-22
- Defining Inclusion and Exclusion Regions on a Floor, page 7-23
- Defining a Rail Line on a Floor, page 7-29
- Modifying Context-Aware Service Parameters, page 7-33
- Configuring a Location Template, page 7-49
- Enabling Location Services on Wired Switches and Wired Clients, page 7-52
- Verifying an NMSP Connection to a Mobility Services Engine, page 7-57
You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points. Licenses for tags and clients are offered separately. (The clients license also includes tracking of rogue clients and rogue access points).

For more information, see the *Cisco 3300 Series Mobility Services Engine Licensing and Ordering Guide* at the following URL:


For details on adding client and tag licenses to the mobility services engine, see Chapter 2, “Adding and Deleting Mobility Services Engines and Licenses”.

### Planning for Data, Voice, and Location Deployment

You can calculate the recommended number and location of access points based on the services (data, voice, location, or a combination) that are active.

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

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

**Step 2** Click the appropriate map name link in the summary list that appears.

If you selected a building map, select a floor map from the Building View page.

**Figure 7-1 Monitor > Maps > Device Name Page**

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

**Note** Access points, clients, and tags must be selected (check boxes selected) in the Floor Settings pane of the Monitor > Maps page to appear on the map (see Figure 7-1).
Step 3 From the Select a command drop-down list, choose the **Planning Mode**. Click **Go**.
A map appears with planning mode options at the top of the page (see Figure 7-2).

**Figure 7-2 Planning Mode page**

---

Step 4 Click **Add APs**.
In the page that appears, drag the dashed rectangle over the map location for which you want to calculate the recommended access points.

Note Adjust the size or placement of the rectangle by selecting the edge of the rectangle and holding down the **Shift** key. Move the mouse as necessary to outline the targeted location.

Step 5 **Select** the check box next to the service that will be used on the floor. Options are Data/Coverage (default), Voice, Location, and Location with Monitor Mode APs. Click **Calculate**.
The recommended number of access points appears.

Note Each service option includes all services that are listed above it. For example, if you select the Location check box, the calculation will consider data/coverage, voice, and location in determining the number of access points required.

Note Recommended calculations assume the need for consistently strong signals. In some cases, fewer access points may be required than recommended.

Step 6 Click **Apply** to generate a map based on the recommended number of access points and their proposed placement in the selected area.
Creating and Applying Calibration Models

If the provided RF models do not sufficiently characterize your floor layout, you can create and apply a calibration model to your floor that better represents its attenuation characteristics. In environments in which many floors share common attenuation characteristics (such as in a library), you can create one calibration model and apply it to floors with the same physical layout and same deployment.

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

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

**Note** Calibration models can only be applied to clients, rogue clients, and rogue access points. Calibration for tags is done using the **Aeroscout System Manager**. For more information on tag calibration, see the documentation available at the following URL: http://support.aeroscout.com

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

Use a laptop or other wireless device to open a browser to WCS and perform the calibration process. To create and apply data point and linear calibration models, follow these steps:

**Step 1** Choose Monitor > Maps

**Step 2** From the Select a command drop-down list, choose RF Calibration Models. Click Go.

**Step 3** From the Select a command drop-down list, choose Create New Model. Click Go.

**Step 4** Assign a name to the model. Click OK.

The new model appears along with the other RF calibration models, but its status is listed as *Not Yet Calibrated*. **
Step 5  
To start the calibration process, click the **model name** link. A new page appears which showing the details of the new model (see Figure 7-3).

**Figure 7-3  New Calibration Model Details page**

![New Calibration Model Details page](image)

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

Step 6  
From the Select a command drop-down list, choose **Add Data Points** and click **Go**.

Step 7  
If you are performing this process from a mobile device connected to WCS through the Cisco Centralized architecture, the MAC address text box is automatically populated with the address of the device. Otherwise, you can manually enter the MAC address of the device you are using to perform the calibration. MAC addresses that are manually entered must be delimited with colons (such as FF:FF:FF:FF:FF).

*Note*  
Use only associated clients to collect calibration data.

Step 8  
Choose the appropriate campus, building, and floor where the calibration is to be performed (see Figure 7-4). Click **Next**.
Step 9  When the chosen floor map and access point locations appear, a grid of plus marks (+) indicates the locations where data is collected for calibration.

Using these locations as guidelines, you can perform either a point or linear data collection by appropriate placement of either the Calibration Point pop-up (point) or the Start and Finish pop-ups (linear) that appear on the map when the respective options appear. Figure 7-5 shows the starting page for a point calibration.

Figure 7-5  Positioning Calibration Points

a. To perform a point collection, follow these steps:
   1. From the Collection Method drop-down list, choose **Point** and select the **Show Data Points** check box if not already selected. A calibration point pop-up appears on the map.
   2. Position the tip of the calibration point pop-up at a data point (+) and click **Go**. A panel appears showing the progress of the data collection.
Chapter 7  Context-Aware Planning and Verification

Creating and Applying Calibration Models

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 the left pane). 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 at least 50 distinct locations and 150 measurements have been gathered. For every location point saved in the calibration process, more than one data point is gathered. The progress of the calibration process is indicated by two status bars above the legend, one for 802.11b/g/n and one for 802.11a/n.

b. To do a linear collection, follow these steps:

1. From the Collection Method drop-down list, choose Linear and select the Show Data points check box if not already selected. A line appears on the map with both Start and Finish pop-ups (see Figure 7-6).

2. Position the tip of the Start pop-up at the starting data point.

3. Position the Finish pop-up at the ending data point.

4. Position yourself with your laptop at the starting data point and click Go. Walk steadily towards the end point along the defined path. The left pane appears indicating data collection is in progress.

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 7-6).

Note  
To delete data points selected in error, click Delete and move the black square that appears over the appropriate data points. Resize the square as necessary by pressing Ctrl and moving the mouse.
6. Repeat Steps b2 to b5 until the status bar for the respective spectrum is complete.

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 in the left pane).

Step 10
To calibrate the data points, click the name of the calibration model at the top of the page. The main page for that model appears.

Step 11
From the Select a command drop-down list, choose Calibrate and click Go.

Step 12
Click Inspect Location Quality when calibration completes. A map appears showing RSSI readings.

Step 13
To use the newly created calibration model, you must apply the model to the floor on which it was created (and on any other floors with similar attenuation characteristics). Navigate to Monitor > Maps and find the floor. At the floor map interface, choose Edit Floor Area from the drop-down list and click Go.

Step 14
From the Floor Type (RF Model) drop-down list, choose the newly created calibration model. Click OK to apply the model to the floor.

Note
This process can be repeated for as many models and floors as needed. After a model is applied to a floor, all locations are determined using the specific collected attenuation data from the calibration model.
Note

It is generally observed that the point calibration gives more accurate calibration than line calibration.

---

### Inspecting Location Readiness and Quality

You can configure WCS to verify the ability of an existing access point deployment to estimate the true location of a client, rogue client, rogue access point, or tag within 7 meters at least 90% of the time. Location readiness calculation is determined by the number and placement of access points.

Using data points gathered during a physical inspection and calibration you can verify that a location meets the location specification (7 meters, 90%).

This section consists of the following topics:

- Inspecting Location Readiness Using Access Point Data, page 7-9
- Inspecting Location Quality Using Calibration Data, page 7-10

### 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 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 in the Floor Settings pane.

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

**Note** Refer to Chapter 2, “Adding and Deleting Mobility Services Engines and Licenses,” for details on installing client and tag licenses.

**Step 3** From the Select a command drop-down list, choose Inspect Location Readiness and 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** From the Select a command drop-down list, choose RF Calibration Model Click Go.

A list of defined calibration models appears.

**Step 3** Click the appropriate calibration model.

Details on the calibration including date of last calibration, number of data points by signal type (802.11a, 802.11 b/g) used in the calibration, location, and coverage are displayed.

**Step 4** In the same page, click the Inspect Location Quality link found under the Calibration Floors heading.

A color-coded map noting percentage of location errors appears.

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

Verifying Location Accuracy

By verifying for location accuracy, you are ensuring that the existing access point deployment can estimate the location accuracy of the deployment.

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

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

Using the Location Accuracy Tool to Test Location Accuracy

There are two ways to test location accuracy:

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

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

Both are configured and executed through a single window.

This section consists of the following topics:

- Using Scheduled Accuracy Testing to Verify Accuracy of Current Location, page 7-11
- Using On-Demand Location Accuracy Testing, page 7-12
Using Scheduled Accuracy Testing to Verify Accuracy of Current Location

To configure a scheduled accuracy test, follow these steps:

**Step 1** Choose Tools > Location Accuracy Tool.

**Step 2** From the Select a command drop-down list, choose New Scheduled Accuracy Test.

**Step 3** Enter a test name.

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

**Step 5** Campus is configured as system campus by default. There is no need to change this setting.

**Step 6** Select the building from the drop-down list.

**Step 7** Select the floor from the drop-down list.

**Step 8** Select the begin and end time of the test by entering the days, hours, and minutes. Hours are represented using a 24-hour clock.

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

**Step 9** Select the destination point for the test results. You can have the report emailed to you or you can download the test results from the Accuracy Tests > Results page. 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** Select the check box next to each client and tag for which you want to check the location accuracy.

When you select the MAC address check box for a client or tag, two overlapping icons appear on the map for that element.

One icon represents the actual location and the other the reported location.

| Note | To enter a MAC address for a client or tag that is not listed, select the Add New MAC check box and enter the MAC address and click Go. An icon for the element appears on the map. If the newly added element is on the mobility services engine but on a different floor, the icon appears in the left corner (0,0) position. |

**Step 12** If the actual location for an element is not the same as the reported location, drag the actual location icon for that element to the correct position on the map.

| Note | Only the actual location icon can be dragged. |

**Step 13** Click Save when all elements are positioned. A panel appears confirming successful accuracy testing.

**Step 14** Click OK to close the confirmation panel. You are returned to the Accuracy Tests summary page.
Verifying Location Accuracy

Note
The accuracy test status appears as Scheduled when the test is about to execute. A status of In Progress appears when the test is running and Idle when the test is complete. A Failure status appears when the test is not successful.

Step 15
To view the results of the location accuracy test, click Test name and then click Download on the page that appears.

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

Using On-Demand Location Accuracy Testing

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

To run an on-demand accuracy test, follow these steps:

Step 1 Choose Tools > Location Accuracy Tool.
Step 2 From the Select a command drop-down list, choose New On demand Accuracy Test.
Step 3 Enter a test name.
Step 4 Choose the area type from the drop-down list.
Step 5 Campus is configured as system campus by default. There is no need to change this setting.
Step 6 Select the building from the drop-down list.
Step 7 Select the floor from the drop-down list.
Step 8 View test results at the Accuracy Tests > Results page. 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, choose either client or tag from the drop-down list on the left. A list of all MAC addresses for the chosen option (client or tag) appear in a drop-down list to its right.
Step 11 Choose a MAC address from the drop-down list, move the red cross hair to a map location, and click the mouse to place it.
Step 12 Click Start to begin collecting accuracy data.
Step 13 Click Stop to finish collecting data. You should allow the test to run for at least two minutes before clicking Stop.
Using Chokepoints to Enhance Tag Location Reporting

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

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

Note

See the AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine Users Guide for chokepoint installation, configuration, and management details at the following URL:

http://support.aeroscout.com

This section consists of the following topics:

- Adding Chokepoints to the WCS, page 7-13
- Removing Chokepoints from WCS, page 7-19

Adding Chokepoints to the WCS

After you install and configure the chokepoint using Aeroscout System Manager, you can add the chokepoint to the mse by positioning it on a WCS map.
To add a chokepoint to WCS, follow these steps:

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

The Chokepoints summary page appears.

**Step 2** From the Select a command drop-down list, choose **Add Chokepoint** and click **Go**.

The Add Chokepoint page appears (see Figure 7-7).

**Figure 7-7 Add Chokepoint Page**

![Add Chokepoint Page](image)

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

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

**Step 5** Click **OK** to save the chokepoint entry to the database.
The Chokepoints summary page appears with the new chokepoint entry listed (see Figure 7-8).

**Figure 7-8   Chokepoints Summary Page**

![Chokepoints Summary Page](image)

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

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

**Figure 7-9   Monitor > Maps Page**

![Monitor > Maps Page](image)
Step 7  At the Maps page, select the link (such as Build1 > Floor2) that corresponds to the floor location of the chokepoint. The floor map appears (Figure 7-10).

Figure 7-10  Selected Floor Map Page

Step 8  From the Select a command drop-down list, choose Add Chokepoints and click Go.

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

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

Figure 7-11  Add Chokepoints Summary Page

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

A map appears with a chokepoint icon in the top-left corner. You can now place the chokepoint on the map.
Step 10  Left-click the chokepoint icon and drag it to the proper location (see Figure 7-12).

*Figure 7-12  Chokepoint Icon is Positioned on the Floor Map*

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

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

The floor map reappears with the added chokepoint (see Figure 7-13).

Note  If the chokepoint does not appear on the map, select the Chokepoints check box in the Floor Settings pane. Do not select Save Settings in the Floor Settings pane unless you want to save this display criteria for all maps.
Figure 7-13 New Chokepoint Displayed on Floor Map

Note Name, range, entry/exit chokepoint: (yes or no), and static IP address of the chokepoint appear when you hover the 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 WCS

You can remove one or more chokepoints at a time.

To delete a chokepoint, follow these steps:

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

**Step 2** Select the box next to the chokepoint to be deleted.

**Step 3** From the Select a command drop-down list, choose Remove Chokepoints and click Go (see Figure 7-14).

**Figure 7-14 Removing a Chokepoint**

![Chokepoints page screenshot]

**Step 4** To confirm chokepoint deletion, click OK in the dialog box that appears.

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

Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting

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

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

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

1. Have a mobility services engine active in the network.
   
   Refer to Chapter 2, “Adding and Deleting Mobility Services Engines and Licenses,” for details on adding a mobility services engine.

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

   Refer to the “Adding Wi-Fi TDOA Receivers to WCS” section on page 7-20 for details on adding the TDOA receiver to WCS.
3. Synchronize WCS and mobility services engines.
   Refer to Chapter 3, “Synchronizing Mobility Services Engines,” for details on synchronization.

4. Set up the TDOA receiver using the AeroScout System Manager.

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

This section consists of the following topics:

- Adding Wi-Fi TDOA Receivers to WCS, page 7-20
- Removing Wi-Fi TDOA Receivers from WCS, page 7-22

### Adding Wi-Fi TDOA Receivers to WCS

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

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

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

**Step 2**  
From the Select a command drop-down list, 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 page 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 page, select the link that corresponds to the floor location of the TDOA receiver. The floor map appears.

**Step 7**  
Select the **WiFi TDOA Receivers** check box in the Floor Settings pane, if not already selected. This ensures that TDOA receivers display on the map (see **Figure 7-15**).

   **Note**  
   Click **Save Settings** to display TDOA receivers in all maps (default setting).
Step 8  From the Select a command drop-down list, choose **Add WiFi TDOA receivers** and Click **Go**.

The Add WiFi TDOA Receivers summary page appears.

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

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

A map appears with a TDOA receiver icon in the top-left corner. You are now ready to place the TDOA receiver on the map (see **Figure 7-16**).

**Figure 7-16  Placing WiFi TDOA Receiver on the Map**

Step 10  Left click the TDOA receiver icon and drag and place it in the proper location on the floor map.
Using Tracking Optimized Monitor Mode to Enhance Tag Location Reporting

To optimize monitoring and location calculation of tags, you can enable TOMM tracking optimized monitor mode 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.

To optimize monitoring and location calculation of tags:

---

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

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

**Step 11**
After placing the TDOA receiver, enter the height of the receiver in the sensor height text box.

**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 WCS**

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

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

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

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

**Step 3**
From the Select a command drop-down list, choose **Remove WiFi TDOA Receivers** and click **Go**.

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

The **All WiFi TDOA Receivers** page. A message confirming deletion of the TDOA receiver appears.

The deleted TDOA receiver is no longer listed in the page.

---

**Using Tracking Optimized Monitor Mode to Enhance Tag Location Reporting**

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 WCS, choose **Configure > WiFi TDOA Receivers**. The WiFi TDOA Receivers summary page appears.

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

**Step 3**
From the Select a command drop-down list, choose **Remove WiFi TDOA Receivers** and click **Go**.

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

The **All WiFi TDOA Receivers** page. A message confirming deletion of the TDOA receiver appears.

The deleted TDOA receiver is no longer listed in the page.

---
Step 1
Enable monitor mode on the access point, by following these steps:

a. Choose Configure > Access Point > AP Name.

b. Select Monitor as the AP Mode.

Note
For more details, see to the Cisco Wireless Control System Configuration Guide, Release 7.0 at the following URL:

Step 2
Enable TOMM and assign monitoring channels on the access point radio, by following these steps:

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

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

c. At the Radio details page, disable Admin Status by unselecting the check box. This disables the radio.

d. Select the Enable TOMM 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, choose None from the channel drop-down list.

f. Click Save.

g. At the Radio parameters page, re-enable the radio by selecting 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 page.

Defining Inclusion and Exclusion Regions on a Floor

To further refine location calculations on a floor, you can define the regions that are included (inclusion areas) in the calculations and those regions that are not included (exclusion regions).

For example, you might want to exclude regions such as an atrium or stairwell within a building but include a work area (such as cubicles, labs, or manufacturing floors).

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

This section consists of the following topics:

- Guidelines, page 7-24
- Defining an Inclusion Region on a Floor, page 7-24
- Defining an Exclusion Region on a Floor, page 7-27
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 WCS. The inclusion region is indicated by a solid aqua line and generally outlines the region.
- You can define multiple exclusion regions on a floor.
- Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.
  This might cause some of the devices to be located outside inclusion regions or inside exclusion regions till their location is calculated again.
- You must select the Location Regions option in the Floor Settings pane of the Monitor > Maps page 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Monitor &gt; Maps.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the name of the appropriate floor.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the Select a command drop-down list, choose Map Editor and click Go.</td>
</tr>
<tr>
<td>Step 4</td>
<td>At the map, click the aqua box on the toolbar (see Figure 7-17).</td>
</tr>
</tbody>
</table>

A message box appears reminding you that only one inclusion region can be defined at a time. Defining a new inclusion region automatically removes the previously defined inclusion region. By default, an inclusion region is defined for each floor when it is added to WCS.
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 7-18**).
Defining Inclusion and Exclusion Regions on a Floor

**Figure 7-18 Inclusion Area Defined**

*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 toolbar 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 on the toolbar. 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, select the **Location Regions** check box if it is not already selected. If you want it to apply to all floor maps, click **Save settings**.

The defined inclusion region appears on the map (see **Figure 7-19**).
Step 13 To resynchronize the WCS and location databases, choose Services > Synchronize Services.

Step 14 At the Synchronize WCS and MSE(s) page, select the Network Designs tab and click Synchronize. Look at the Sync. Status column to ensure that the synchronization is successful (two green arrows).

Note
- If the floor was already assigned previously to a mobility services engine, the changes on the floor will be auto synchronized to the mobility services engine.
- For location calculation of an element, the rails and regions will take effect only after the location is recalculated.
- Inclusion region configurations do not apply to tags.

Defining an Exclusion Region on a Floor

To further refine location calculations on a floor, you can define regions that are excluded (exclusion regions) in the calculations. Exclusion regions are generally defined within the borders of an inclusion region.

Note
Exclusion region configurations do not apply to tags.

To define an exclusion region, follow these steps:

Step 1 Choose Monitor > Maps.
Step 2 Click the name of the appropriate floor area.
Step 3 From the Select a command drop-down list, choose Map Editor and click Go.
Step 4  At the map, click the purple box in the toolbar.

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 7-20).

Figure 7-20  Defining Exclusion Areas on Floor Map

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

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

Step 11  To return to the floor map to enable exclusion regions on heatmaps, select Exit from the Command menu.

Step 12  At the floor map, select the Location Regions check box if it is not already selected. The exclusion region is shown on the map (see Figure 7-21).
To resynchronize the WCS and location databases, choose **Services > Synchronize Services**.

At the Synchronize page, from the Synchronize drop-down list, choose **Network Designs** and then click **Synchronize**.

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

---

**Note**

- Exclusion region auto synchronizes with mobility services engine if the floor was already synchronized to the mobility services engine.
- You can draw multiple exclusion regions within an inclusion region.
- For location calculation of an element, the rails and regions will take effect only after the location is recalculated.

---

### Defining a Rail Line on a Floor

You can define a rail line on a floor (such as a conveyor belt) that indicates an area where clients are expected to be.

**Note**

Rail line configurations do not apply to tags.

Additionally, you can define an area (east and west or north and south) of the rail that expands the area that clients are expected to populate. This expanded area is known as the *snap-width* and further assists location calculations. Any client located within the snap-width area is plotted on the rail line (majority) or just outside of the snap-width area (minority).

The snap-width area is defined in feet or meters (user-defined).

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

**Step 1** Choose **Monitor > Maps**.

**Step 2** Click on the name of the appropriate floor area.
Step 3  From the Select a command drop-down list, choose **Map Editor** and click **Go**.

Step 4  Click the rail icon (to the right of the purple exclusion icon) in the toolbar (see Figure 7-22).

**Figure 7-22  Rail Icon on Map Editor Toolbar**

Step 5  In the message dialog that appears, enter a snap-width (feet or meters) for the rail and then click **OK** (see Figure 7-23).

**Figure 7-23  Defining Rail Width**

Step 6  When the drawing icon appears, click the drawing icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.
Step 7  Click the drawing icon twice when the rail line is completely drawn on the floor map. The rail line appears on the map and is bordered on both sides by the defined snap-width region (see Figure 7-24).
Defining a Rail Line on a Floor

Figure 7-24  Defining Rail Line in Map Editor

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

Step 8  To return to the floor map to enable rails on heatmaps, select Exit from the Command menu.

Step 9  At the floor map, select the Rails check box in the Floor Setting panel if it is not already selected. The rail is shown on the map (see Figure 7-25).
Step 10  To resynchronize the WCS and mobility services engine, choose **Services > Synchronize Services**.

Step 11  At the Synchronize page, from the Synchronize drop-down list, choose **Network Designs** and then click **Synchronize**.

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

- Rails auto synchronizes with mobility services engine if the floor was already synchronized to the mobility services engine.
- For location calculation of an element, the rails and regions will take effect only after the location is recalculated.

**Modifying Context-Aware Service Parameters**

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

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

- Licenses are required in order to retrieve contextual information on tags and clients from access points. The license of the client also includes tracking of rogue clients and rogue access points. Licenses for tags and clients are offered independently and are offered in a range of quantities, from 3,000 to 12,000
Modifying Context-Aware Service Parameters

Modifying Tracking Parameters

The mobility services engine can track up to 18,000 clients (including rogue clients, rogue access points, wired clients, and interferers) and tags (combined count) with the proper license purchase and mobility services engine. Updates on the locations of tags, clients, and interferers being tracked are provided to the mobility services engine from the controller.

Note Cisco 3350 Mobility Services Engine supports up to 18,000 clients and tags and the Cisco 3310 Mobility Services Engine supports up to 2,000 clients and tags.

Only those tags, clients and interferers that the controller is tracking are seen in WCS maps, queries and reports. No events and alarms are collected for non-tracked elements and none are used in calculating the 18,000 element limit for clients or tags.

You can modify the following tracking parameters using WCS:

- Enable and disable wired and wireless client stations, active asset tags, and rogue clients, interferers, and access points whose locations you actively track.
  
  Wired client location tracking enables servers in a data center to more easily find wired clients in the network. Servers are associated with wired switch ports in the network.

- Set limits on how many of a specific element you want to track.
  
  For example, given a client license of 12,000 trackable units, you could set a limit to track only 8,000 client stations (leaving 4,000 units available to allocate between rogue clients and rogue access points). Once the tracking limit is met for a given element, the number of elements not being tracked is summarized on the Tracking Parameters page.

- Disable tracking and reporting of ad hoc rogue clients and access points.

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

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

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

Step 4  Modify the tracking parameters as appropriate. **Table 7-1** describes each parameter.
## Modifying Context-Aware Service Parameters

### Table 7-1 Tracking Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking Parameters</td>
<td></td>
</tr>
<tr>
<td>Wired Clients</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of client stations by the mobility services engine.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In 7.0, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, and interferers.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The wired client limiting is supported from mobility services engine 7.0 and WCS 7.0 onwards. In other words, you can limit wired clients to a fixed number, say 500. This limit is set to ensure that the licenses are not taken up completely by wired clients and some licenses are available for wireless clients.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong> When upgrading mobility services engine from 6.0 to 7.0, if any limits have been set on wireless clients or rogues, they will get reset because of the wired client limit change in 7.0.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (display only): Indicates the number of wired client stations currently being tracked.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (display only): Indicates the number of wired client stations beyond the limit.</td>
</tr>
<tr>
<td>Wireless Clients</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of client stations by the mobility services engine.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Enable Limiting</strong> check box to set a limit on the number of client stations to track.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 18,000 which is the maximum number of clients that can be tracked by a mobility services engine.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The actual number of tracked clients is determined by the license purchased.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (display only): Indicates the number of client stations currently being tracked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (display only): Indicates the number of client stations beyond the limit.</td>
</tr>
</tbody>
</table>
### Rogue Clients and Access Points

1. Select the **Enable** check box to enable tracking of rogue clients and asset points by the mobility services engine.

2. Select the **Enable Limiting** check box to set a limit on the number of rogue clients and asset tags stations to track.

3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 18,000 which is the maximum number of rogue clients and access points that can be tracked by a mobility services engine.

**Note** The actual number of tracked rogues (clients and access points) is driven by the client license purchased. The user must consider the number of clients that are being tracked in determining the available quantity to allocate to track rogue clients and access points because clients and rogue clients and access points are addressed by the same license.

**Note** Active Value (display only): Indicates the number of rogue clients and access points currently being tracked.

**Note** Not Tracked (display only): Indicates the number of rogue clients and access points beyond the limit.

### Exclude Ad-Hoc Rogues

Select 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.

### Interferers

1. Select the **Enable** check box to enable tracking of the interferers by the mobility services engine.

   In 7.0, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, and interferers.

**Note** Active Value (display only): Indicates the number of interferers currently being tracked.

**Note** Not Tracked (display only): Indicates the number of interferers beyond the limit.

### Asset Tracking Elements

#### Active RFID Tags

1. Select the **Enable** check box to enable tracking of active RFID tags by the mobility services engine.

**Note** The actual number of tracked active RFID tags is determined by the license purchased.

**Note** Active Value (display only): Indicates the number of active RFID tags currently being tracked.

**Note** Not Tracked (display only): Indicates the number of active RFID tags beyond the limit.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue Clients and Access Points</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of rogue clients and asset points by the mobility services engine.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Enable Limiting</strong> check box to set a limit on the number of rogue clients and asset tags stations to track.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 18,000 which is the maximum number of rogue clients and access points that can be tracked by a mobility services engine.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The actual number of tracked rogues (clients and access points) is driven by the client license purchased. The user must consider the number of clients that are being tracked in determining the available quantity to allocate to track rogue clients and access points because clients and rogue clients and access points are addressed by the same license.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (display only): Indicates the number of rogue clients and access points currently being tracked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (display only): Indicates the number of rogue clients and access points beyond the limit.</td>
</tr>
<tr>
<td>Exclude Ad-Hoc Rogues</td>
<td>Select 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.</td>
</tr>
<tr>
<td>Interferers</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of the interferers by the mobility services engine.</td>
</tr>
<tr>
<td></td>
<td>In 7.0, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, and interferers.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (display only): Indicates the number of interferers currently being tracked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (display only): Indicates the number of interferers beyond the limit.</td>
</tr>
<tr>
<td>Active RFID Tags</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of active RFID tags by the mobility services engine.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The actual number of tracked active RFID tags is determined by the license purchased.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (display only): Indicates the number of active RFID tags currently being tracked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (display only): Indicates the number of active RFID tags beyond the limit.</td>
</tr>
</tbody>
</table>
Modifying Context-Aware Service Parameters

Table 7-1  Tracking Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Parameters—Not applicable for Controllers less than 4.2 software version.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>We recommend to use a Controller 4.2 or higher for better latency and accuracy.</td>
</tr>
<tr>
<td>SNMP Retry Count</td>
<td>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).</td>
</tr>
<tr>
<td>SNMP Timeout</td>
<td>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).</td>
</tr>
<tr>
<td>SNMP Polling Interval</td>
<td></td>
</tr>
<tr>
<td>Client Stations</td>
<td>Select 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).</td>
</tr>
<tr>
<td>Active RFID Tags</td>
<td>Select the Enable check box to enable active RFID tag polling and enter the polling interval in seconds. Allowed values are from 1 to 99999.</td>
</tr>
<tr>
<td>Note</td>
<td>Before the mobility service can collect asset tag data from controllers, you must enable the detection of active RFID tags using the CLI command <code>config rfid status enable</code> on the controllers.</td>
</tr>
<tr>
<td>Rogue Clients and Access Points</td>
<td>Select the Enable check box to enable rogue access point polling and enter the polling interval in seconds. Default value is 600. Allowed values are from 1 to 99999 (Configurable in controller release 4.1 and earlier and location server release 3.0 and earlier only).</td>
</tr>
<tr>
<td>Statistics</td>
<td>Select the Enable check box to enable statistics polling for the mobility service, 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).</td>
</tr>
</tbody>
</table>

Step 5  Click Save to store the new settings in the mobility services engine database.

Modifying Filtering Parameters

In addition to tracking parameters, you can use filtering to limit the number of clients, asset tags, wired clients, rogue clients, interferers, 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:

- Each MAC address should be listed on a separate line.
- Allowed MAC addresses must be listed first and preceded by an “[Allowed]” line item. Disallowed MAC addresses must be preceded by “[Disallowed].”
- Wildcard listings can be used to represent a range of MAC addresses. For example, the first entry “00:11:22:33:*” in the Allowed listing below is a wildcard.

**Note**

Allowed MAC address formats are viewable from the Filtering Parameters configuration page. See Table 7-2 for details.

**EXAMPLE** file listing:

```
[Allowed]
00:11:22:33:*
22:cd:34:ae:56:45
02:23:23:34:*
[Disallowed]
00:10:*
ae:bc:de:ea:45:23
```

- Probing clients

Probing clients are clients that are associated with one controller but whose probing activity enables them to appear to another controller and count as an element for the probed controller as well as its primary controller.

**Note**

Excluding probing clients can free up the licenses for the associated clients.

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

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

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

**Step 3**
Choose Context Aware Service > Administration > Filtering Parameters to display the configuration options.

**Step 4**
Modify the filtering parameters as appropriate. Table 7-2 describes each parameter.
Table 7-2  Filtering Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude Probing Clients</td>
<td>Select the check box to prevent calculating location for probing clients.</td>
</tr>
<tr>
<td>Enable Location MAC Filtering</td>
<td>1. Select the check box to enable filtering of specific elements by their MAC addresses.</td>
</tr>
<tr>
<td></td>
<td>2. To import a file of MAC addresses (Upload a file for Location MAC Filtering text box), browse for the file name and click Save to load the file. MAC addresses from the list auto-populate the Allowed List and Disallowed List based on their designation in the file.</td>
</tr>
<tr>
<td></td>
<td>Note: To view allowed MAC address formats, click the red question mark next to the Upload a file for Location MAC Filtering text box.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Note: To move an address between the Allow and Disallow columns, highlight the MAC address entry and click the button under the appropriate column.</td>
</tr>
<tr>
<td></td>
<td>Note: To move multiple addresses, click the first MAC address and then press Ctrl and click additional MAC addresses. Click Allow or Disallow to place an address in that column.</td>
</tr>
<tr>
<td></td>
<td>Note: If a MAC address is not listed in the Allow or Disallow column, it appears in the Blocked MACs column by default. If you click the Unblock button, the MAC address automatically moves to the Allow column. You can move it to the Disallow column by clicking the Disallow button under the Allow column.</td>
</tr>
</tbody>
</table>

**Step 5**  Click Save to store the new settings in the mobility services engine database.
Modifying History Parameters

You can use Cisco WCS to specify how long to store (archive) histories on client stations, asset tags, and rogue clients, wired clients, interferers and access points.

You can also program the mobility services engine to periodically prune (remove) duplicate data from its historical files, which increases the amount of memory available for storing the latest history information. This is important to prevent losing latest history information due to lack of disk space.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In Cisco WCS, choose Services &gt; Mobility Services.</td>
</tr>
<tr>
<td>2</td>
<td>Click the name of the mobility services engine whose properties you want to edit.</td>
</tr>
<tr>
<td>3</td>
<td>Choose Context Aware Service &gt; Administration &gt; History Parameters.</td>
</tr>
<tr>
<td>4</td>
<td>Modify the following history parameters as appropriate. Table 7-3 describes each parameter.</td>
</tr>
<tr>
<td>5</td>
<td>Click Save to store your selections in the mobility services engine database.</td>
</tr>
</tbody>
</table>

### Table 7-3 History Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive for</td>
<td>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 365.</td>
</tr>
<tr>
<td>Prune data starting at</td>
<td>Enter the number of hours and minutes at which the location server starts data pruning (between 0 and 23 hours, and between 1 and 59 minutes). Enter the interval in minutes after which data pruning starts again (between 1 and 99900000). Default start time is 23 hours and 50 minutes, and the default interval is 1440 minutes.</td>
</tr>
<tr>
<td>Client Stations</td>
<td>Select the Enable check box to turn on historical data collection for client stations.</td>
</tr>
<tr>
<td>Wired Stations</td>
<td>Select the Enable check box to turn on historical data collection for wired stations.</td>
</tr>
<tr>
<td>Asset Tags</td>
<td>Select the Enable check box to turn on historical data collection.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Before the mobility service can collect asset tag data from controllers, you must enable the detection of RFID tags using the CLI command <strong>config rfid status enable</strong>.</td>
</tr>
<tr>
<td>Rogue Clients and Access Points</td>
<td>Select the Enable check box to turn on historical data collection.</td>
</tr>
<tr>
<td>Interferers</td>
<td>Select the Enable check box to turn on historical data collection.</td>
</tr>
</tbody>
</table>
Enabling Location Presence

You can enable location presence on a mobility services engine in order to expand civic (city, state, postal code, country) and geographic (longitude, latitude) location information beyond the Cisco default settings (campus, building, floor, and X, Y coordinates). You can then request this information for wireless and wired clients on demand for use by location-based services and applications.

You can also import advanced location information such as the MAC address of a wired client and the wired switch slot and port to which the wired client is attached.

You can configure location presence when a new campus, building, floor or outdoor area is added or configure it at a later date.

Once enabled, the mobility services engine can provide any requesting Cisco CX v5 client its location.

Note
For details on configuring location presence when adding a new campus, building, floor, or outdoor area, see the “Creating Maps” section in Chapter 5 of the Cisco Wireless Control System Configuration Guide, release 6.0 and later.

Note
Before enabling this feature, synchronize the mobility services engine.

To enable and configure location presence on a mobility services engine, follow these steps:

Step 1
Choose Services > Mobility Services. Select the mobility services engine to which the campus or building or floor is assigned.

Step 2
Choose Context Aware Service > Administration > Presence Parameters. The Presence page displays.

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

Step 4
Select one of the following Location Resolution options.

a. When Building is selected, the mobility services engine can provide any requesting client its location by building.
   - For example, if a client requests its location and the client is located in Building A, the mobility services engine returns the client address as Building A.

b. When AP is selected, the mobility services engine can provide any requesting client its location by its associated access point. The MAC address of the access point appears.
   - For example, if a client requests its location and the client is associated with an access point with a MAC address of 3034:00hh:0adg, the mobility services engine returns the client address of 3034:00hh:0adg.

c. When X,Y is selected, the mobility services engine can provide any requesting client its location by its X and Y coordinates.
   - For example, if a client requests its location and the client is located at (50, 200) the mobility services engine returns the client address of 50, 200.

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

a. Select the Cisco check box to provide location by campus, building, floor, and X and Y coordinates. This is the default setting.
b. Select the Civic check box to provide the name and address (street, city, state, postal code, country) of a campus, building, floor, or outdoor area.

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

**Step 6**
By default, the Text check box for Location Response Encoding is selected. It indicates the format of the information when received by the client. There is no need to change this setting.

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

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

**Step 9**
Click Save.

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

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

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

**Step 3**
Choose **Context Aware Service > Administration > Import Asset Information**.

**Step 4**
Enter the name of the text file or browse for the filename.

Specify information in the imported file in the following formats:

- **tag format**: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname
- **station format**: #station, 00:00:00:00:00:00, categoryname, groupname, assetname

**Step 5**
Click **Import**.

### Exporting Asset Information
To export asset, chokepoint, and TDOA receiver information from the mobility services engine to a file using WCS, follow these steps:

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

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

**Step 3**
Choose **Context Aware Service > Administration > Export Asset Information**.

Information in the exported file is in the following formats:

- **tag format**: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname
- **station format**: #station, 00:00:00:00:00:00, categoryname, groupname, assetname

**Step 4**
Click **Export**.

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

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

You can also apply varying smoothing rates to manage location movement of a client.

Note

Location parameters apply only to clients.

To configure location parameters, follow these steps:

Step 1

In Cisco WCS, choose Services > Mobility Services.

Step 2

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

Step 3

Choose Context Aware Service > Advanced > Location Parameters. The configuration options appear.

Step 4

Modify the location parameters as appropriate. Table 7-4 describes each parameter.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calculation time</td>
<td>Select the Enable check box to initiate the calculation of the time required to compute location.</td>
</tr>
<tr>
<td></td>
<td>Note: This parameter applies only to clients, rogue access points, rogue clients, and interferers.</td>
</tr>
<tr>
<td></td>
<td>Caution: Enable this parameter only under Cisco TAC personnel guidance because it slows down the overall location calculations.</td>
</tr>
<tr>
<td>OW Location</td>
<td>Select the Enable check box to include Outer Wall (OW) calculation as part of location calculation.</td>
</tr>
<tr>
<td></td>
<td>Note: This parameter is ignored by the mobility services engine.</td>
</tr>
<tr>
<td>Relative discard RSSI time</td>
<td>Enter the number of minutes since the most recent RSSI sample after which RSSI measurement should be considered discarded. For example, if you set this parameter to 3 minutes and the mobility services engine receives two samples at 10 and 12 minutes, it keeps both samples. An additional sample received at 15 minutes is discarded. Default value is 3. Allowed values range from 0 to 99999. A value of less than 3 is not recommended.</td>
</tr>
<tr>
<td></td>
<td>Note: This parameter applies only to clients, rogue access points, rogue clients, and interferers.</td>
</tr>
</tbody>
</table>
Chapter 7  Context-Aware Planning and Verification

## Table 7-4  Location Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absolute discard RSSI time</td>
<td>Enter the number of minutes after which RSSI measurement should be considered stale and discarded, regardless of the most recent sample. Default value is 60. Allowed values range from 0 to 99999. A value of less than 60 is not recommended.</td>
</tr>
<tr>
<td>Note</td>
<td>This parameter applies only to clients.</td>
</tr>
<tr>
<td>RSSI Cutoff</td>
<td>Enter the RSSI cutoff value, in decibels (dBs) with respect to one (1) mW (dBm), above which the mobility services engine will always use the access point measurement. Default value is –75.</td>
</tr>
<tr>
<td>Note</td>
<td>When 3 or more measurements are available above the RSSI cutoff value, the mobility services engine will discard any weaker values (lower than RSSI cutoff value) and use the 3 (or more) strongest measurements for calculation; however, when only weak measurements below the RSSI cutoff value are available, those values are used for calculation.</td>
</tr>
<tr>
<td>Note</td>
<td>This parameter applies only to clients.</td>
</tr>
<tr>
<td>Location Filtering</td>
<td>Location filtering is used to smooth out the jitters in the calculated location. This prevents the located device from jumping between two discrete points on the floor map.</td>
</tr>
<tr>
<td>Chokepoint Usage</td>
<td>Select the Enable check box to enable chokepoints to track Cisco compatible tags.</td>
</tr>
<tr>
<td>Use Chokepoints for Interfloor conflicts</td>
<td>Perimeter chokepoints or weighted location readings can be used to locate Cisco compatible tags. Options:</td>
</tr>
<tr>
<td>Never</td>
<td>When selected, perimeter chokepoints are not used to locate Cisco compatible tags.</td>
</tr>
<tr>
<td>Always</td>
<td>When selected, perimeter points are used to locate Cisco compatible tags.</td>
</tr>
<tr>
<td>Floor Ambiguity</td>
<td>When selected, both weighted location readings and perimeter chokepoints are used to locate Cisco compatible tags. If similar locations are calculated by the two methods, the perimeter chokepoint value is used by default.</td>
</tr>
<tr>
<td>Chokepoint Out of Range timeout</td>
<td>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.</td>
</tr>
<tr>
<td>Absent Data cleanup interval</td>
<td>Enter the number of minutes that data for absent mobile stations is kept. An absent mobile station is one that was discovered but does not appear in the network. Default value is 1440.</td>
</tr>
</tbody>
</table>

### Step 5  Click Save.
Enabling Notifications and Configuring Notification Parameters

You can use WCS to enable notification and configure notification parameters.

This section consists of the following topics:

- Enabling Notifications, page 7-46
- Configuring Notification Parameters, page 7-46
- Viewing Notification Statistics, page 7-48

Enabling Notifications

You can use 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 WCS or a third party destination compatible with the mobility services engine notifications. Refer to “Adding, Deleting, and Testing Event Definitions” section on page 6-3.

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 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 the following URL:


Configuring Notification Parameters

You can limit the rate at which a mobility services engine generates notifications, set a maximum queue size for notifications, and set a retry limit for notifications within a certain period.

Notification parameter settings apply to user-configurable conditional notifications and northbound notifications except as noted in Table 7-5.

Note

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

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

- **Step 1** In Cisco WCS, choose Services > Mobility Services.
- **Step 2** Click the name of the mobility services engine you want to configure.
- **Step 3** Choose Context Aware Service > Advanced > Notification Parameters to display the configuration options (see Figure 7-27).
Step 4 Select the Enable Northbound Notifications check box to enable the function.

Step 5 Select the Notification Contents check box to send notifications to third-party applications (northbound).

Step 6 Select one or more of the following Notification content options:
  - Chokepoints
  - Telemetry
  - Emergency
  - Battery Level
  - Vendor Data
  - Location

Step 7 Select the Notification Triggers check box.

Step 8 Select one or more of the following Notification trigger options:
  - Chokepoints
  - Telemetry
  - Emergency
  - Battery Level
  - Vendor Data
  - Location Recalculation

Step 9 Enter the IP address and port for the system that is to receive the northbound notifications.

Step 10 Choose the transport type from the drop-down list.
Step 11  Select HTTPS if you want to use HTTPS protocol for secure access to the destination system.

Step 12  To modify the notification parameter settings, enter the new value in the appropriate text box in the Advanced section of the page. Table 7-5 describes each parameter.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Limit</td>
<td>Enter the rate in milliseconds at which the mobility services engine generates</td>
</tr>
<tr>
<td></td>
<td>notifications. A value of 0 (default) means that the mobility services engine</td>
</tr>
<tr>
<td></td>
<td>generates notifications as fast as possible (Northbound notifications only).</td>
</tr>
<tr>
<td>Queue Limit</td>
<td>Enter the event queue limit for sending notifications. The mobility services engine</td>
</tr>
<tr>
<td></td>
<td>drops any event above this limit. Default values: Cisco 3350 (30000), Cisco 3310</td>
</tr>
<tr>
<td></td>
<td>(5,000), and Cisco 2710 (10,000).</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Enter the number of times to generate an event notification before the refresh time</td>
</tr>
<tr>
<td></td>
<td>expires. This parameter can be used for asynchronous transport types which do not</td>
</tr>
<tr>
<td></td>
<td>acknowledge the receipt of the notification and there is a possibility that the</td>
</tr>
<tr>
<td></td>
<td>notification may be lost in transit. Default value is 1.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>  The mobility services engine does not store events in its database.</td>
</tr>
<tr>
<td>Refresh Time</td>
<td>Enter the wait time in minutes that must pass before a notification is resent. For</td>
</tr>
<tr>
<td></td>
<td>example, if a device is configured for In Coverage Area notification and it is</td>
</tr>
<tr>
<td></td>
<td>constantly being detected within the Coverage Area. The notification will be sent</td>
</tr>
<tr>
<td></td>
<td>once every refresh time.</td>
</tr>
<tr>
<td>Drop Oldest Entry on Queue</td>
<td>(Read only). The number of event notifications dropped from the queue since startup.</td>
</tr>
<tr>
<td>Overflow</td>
<td></td>
</tr>
<tr>
<td>Serialize Events per Mac address</td>
<td>Select this option if you want the successive events for the same MAC address to</td>
</tr>
<tr>
<td>per Destination</td>
<td>be sent to a single destination in a serial manner.</td>
</tr>
</tbody>
</table>

Step 13  Click Save.

Viewing Notification Statistics

You can view the notification statistics for a specific mobility services engine. To view the Notification Statistics for a specific mobility services engine:

Choose Services > Mobility Services > MSE-name > Context Aware Service > Notification Statistics.

where MSE-name is the name of a mobility services engine.

Table 7-6 lists and describes the fields in the Notification statistics page.
Table 7-6 Notification Statistics Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Total count of the destinations.</td>
</tr>
<tr>
<td>Destinations</td>
<td>Count of unreachable destinations.</td>
</tr>
<tr>
<td>Total</td>
<td>Total count of the destinations.</td>
</tr>
<tr>
<td>Unreachable</td>
<td>Count of unreachable destinations.</td>
</tr>
<tr>
<td>Notification Statistics</td>
<td>Status of the track definition. Track notification status could be either</td>
</tr>
<tr>
<td>Summary</td>
<td>Enabled or Disabled.</td>
</tr>
<tr>
<td>Track Definition Status</td>
<td>Status of the track definition. Track notification status could be either</td>
</tr>
<tr>
<td>Track Definition</td>
<td>Enabled or Disabled.</td>
</tr>
<tr>
<td>Destination IP Address</td>
<td>The destination IP Address to which the notifications are sent.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>The destination port to which the notifications are sent.</td>
</tr>
<tr>
<td>Destination Type</td>
<td>The type of the destination. Example: SOAP_XML</td>
</tr>
<tr>
<td>Destination Status</td>
<td>Status of the destination device. The status is either Up or Down.</td>
</tr>
<tr>
<td>Last Sent</td>
<td>The date and time at which the last notification was sent to the destination device.</td>
</tr>
<tr>
<td>Last Failed</td>
<td>The date and time at which the notification had failed.</td>
</tr>
<tr>
<td>Total Count</td>
<td>The total count of notifications sent to the destination. Click on the count link to view the notification statistics details of the destination device.</td>
</tr>
</tbody>
</table>

**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 7-28).

**Figure 7-28** Configure > Controller Template Launch Pad Page

**Step 3** At the New template page, enter a name for the location template on the General tab (see Figure 7-29).

**Figure 7-29** Location Configuration > New > General Tab

Footnotes:
1. Synchronization to the MSE will be needed in order to see effects of changes.
Step 4  On the General tab, modify parameters as necessary. Table 7-7 describes each of the parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFID tag calculation</td>
<td>Select the Enabled check box to collect data on tags.</td>
</tr>
</tbody>
</table>
| Calibrating Client        | Select the Enabled check box to have a calibrating client. Controllers send regular S36 or S60 requests (depending on the client capability) by way of the access point to calibrating clients. Packets are transmitted on all channels. All access points irrespective of channel (and without a channel change) gather RSSI data from the client at each location. These additional transmissions and channel changes might degrade contemporaneous voice or video traffic.
|                            | To use all radios (802.11a/b/g/n) available you must enable multiband on the Advanced panel. |
| Normal Client             | Select the Enabled check box to have a non-calibrating client. No S36 or S60 requests are transmitted to the client. |
| Measurement Notification Interval | Enter a value to set the NMSP measurement notification interval for clients, tags, and rogue access points and clients. This value can be applied to selected controllers through the template. Setting this value on the controller generates out-of-sync notification which you can view on the Services > Synchronize Services page. When a controller and the mobility services engine have two different measurement intervals, the largest interval setting of the two is adopted by the mobility services engine.
|                            | Once this controller is synchronized with the mobility services engine, the new value is set on the mobility services engine. |
| RSSI Expiry Timeout for Clients | Enter a value to set the RSSI timeout value for normal (non-calibrating) clients. |
| RSSI Expiry Timeout for Calibrating Clients | Enter a value to set the RSSI timeout value for calibrating clients. |
| RSSI Expiry Timeout for Tags | Enter a value to set the RSSI timeout value for tags. |
| RSSI Expiry Timeout for Rogue APs | Enter a value to set the RSSI timeout value for rogue access points. |
Step 5  On the Advanced tab, modify parameters as necessary (see Figure 7-30). Table 7-8 describes each of the advanced parameters.

Figure 7-30  Location Configuration > New > Advanced Tab

Table 7-8  Advanced Location Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFID Tag Data Timeout</td>
<td>Enter an RFID tag data timeout value.</td>
</tr>
<tr>
<td>Calibrating Client Multiband</td>
<td>Select the Enabled check box to send S36 and S60 packets (where applicable) on all channels. Calibrating clients must be enabled on the general tab.</td>
</tr>
</tbody>
</table>

Step 6  Click Save.

Enabling Location Services on Wired Switches and Wired Clients

You can import the location of wired Catalyst stackable switches (3750, 3750-E, 3560, 2960, IE-3000 switches), switch blades (3110, 3120, 3130, 3040, 3030, 3020), and switch ports into the mobility services engine.

The following Catalyst 4000 series are also supported:

Once you define a wired switch and synchronize it with a mobility services engine, details on wired clients connected to a wired switch are downloaded to the mobility services engine over the NMSP connection. You can then view wired switches and wired clients using WCS.
Import and display of civic and emergency location identification number (ELIN) meets specifications of RFC 4776, which is outlined at the following URL:

http://tools.ietf.org/html/rfc4776#section-3.4

Note Catalyst stackable switches and switch blades must be operating at Cisco IOS Release 12.2(52) SG or later.

To support location services for wired clients and wired Catalyst switches, you must do the following:

1. Configure the Catalyst switch.
2. Add the Catalyst switch to the WCS.
3. Assign the Catalyst switch to the mobility services engine and synchronize.

This section consists of the following topics:

- Configuring a Catalyst Switch, page 7-53
- Adding a Catalyst Switch to WCS, page 7-55
- Assigning and Synchronizing a Catalyst Switches to a Mobility Services Engine, page 7-56

### Configuring a Catalyst Switch

To configure location service on a wired switch or wired client, and apply it to an interface, follow these steps:

Note All commands are located in the privileged EXEC mode of the command-line interface.

**Step 1** Log into the command-line interface of the switch:

```
Switch > en
Switch#
Switch# configure terminal
```

**Step 2** Enable NMSP:

```
Switch(config)# nmsp
Switch(config-nmsp)# enable
```

**Step 3** Configure the SNMP community:

```
Switch(config)# snmp-server community wired-location
```

**Step 4** Enable IP device tracking in the switch:

```
Switch(config)# ip device tracking
```

**Step 5** Optional Configure a civic location for a switch.

Note You can define a civic and emergency location identification number (ELIN) for a specific location. That identifier can then be assigned to a switch or multiple ports on a switch to represent that location. This location identifier is represented by a single number such as 6 (range 1 to 4095). This saves timer when you are configuring multiple switches or ports that reside in the same location.
Enter configuration commands, one per line. End by pressing Ctrl-Z.

The following is an example of a civic location configuration:

```
Switch(config)# location civic-location identifier 6
Switch(config-civic)# name "switch-loc4"
Switch(config-civic)# seat "ws-3"
Switch(config-civic)# additional code "1e3f0034c092"
Switch(config-civic)# building "SJ-14"
Switch(config-civic)# floor "4"
Switch(config-civic)# street-group "Cisco Way"
Switch(config-civic)# number "3625"
Switch(config-civic)# type-of-place "Lab"
Switch(config-civic)# postal-community-name "Cisco Systems, Inc."
Switch(config-civic)# postal-code "95134"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state "CA"
Switch(config-civic)# country "US"
Switch(config-civic)# end
```

**Step 6** Configure the ELIN location for the switch.

**Note** The ELIN location length must be between 10 and 25 characters. In the following example, 4084084000 meets that specification. This number can also be entered as 408-408-4000. Additionally, a value with a mix of numerals and text can be entered such as 800-CISCO-WAY or 800CISCOWAY. However, if you place spaces between the numerals or text without hypens, quotes should be used, such as “800 CISCO WAY.”

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

**Step 7** Configure the location for a port on the switch.

A switch has a specified number of switch ports, and clients and hosts are connected at these ports. When configuring location for a specific switch port, the client connected at that port is assumed to have the port location.

If a switch (switch2) is connected to a port (such as port1) on another switch (switch1) all the clients connected to switch2 are assigned the location that is configured on port1.

The syntax for defining the port is: `interface {GigabitEthernet | FastEthernet} slot/module/port`

Enter only one location definition on a line, and end the line by pressing Ctrl-Z.

```
Switch(config)# interface GigabitEthernet 1/0/10
Switch(config-if)# location civic-location-id 6
Switch(config-if)# location elin-location-id 6
Switch(config-if)# end
```

**Step 8** Assign a location to the switch itself.

The following is configured on the FastEthernet network management port of the switch.

Enter configuration commands, one per line. End by pressing Ctrl-Z.

```
Switch(config)# interface FastEthernet 0
Switch(config-if)# location civic-location-id 6
Switch(config-if)# location elin-location-id 6
Switch(config-if)# end
```
Adding a Catalyst Switch to WCS

All Catalyst switches must be configured with location service before they are added to WCS. Refer to the “Configuring a Catalyst Switch” section on page 7-53.

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

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

**Step 2** From the Select a command drop-down list, choose **Add Ethernet Switches**. The Add Ethernet Switches page appears (see Figure 7-31).

![Figure 7-31 Configure > Ethernet Switches > Add Ethernet Switches](image)

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

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

**Step 4** Enter one or more IP addresses.

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

**Step 6** From the drop-down list, choose the SNMP version if it is different from the default.

**Step 7** No changes are required in the Retries and Timeout text boxes.

**Step 8** Enter wired-location as the SNMP community string in the Community text box.

*Note* The SNMP community string entered at this step must match that value assigned to the Catalyst switch in Step 3 of the “Configuring a Catalyst Switch” section on page 7-53.
Step 9  Click OK. A page confirming successful addition to WCS appears (see Figure 7-32).

Figure 7-32  Add Switches Result Page

Step 10  Click OK on the Add Switches Result page, and the newly added switch appears on the Ethernet Switches page (see Figure 7-33).

Figure 7-33  Ethernet Switches Summary Page

Assigning and Synchronizing a Catalyst Switches to a Mobility Services Engine

After adding a Catalyst switch to WCS you need to assign it to a mobility services engine and then synchronize the two systems. Once they are synchronized, an NMSP connection between the controller and the mobility services engine is established.

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

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

To assign and synchronize Catalyst switches to a mobility services engine, follow these steps:

Step 1  Choose Services > Synchronize Services.

Step 2  Click the Wired Switches tab to assign a switch to a mobility services engine.

Step 3  Choose one or more switches to be synchronized with the mobility services engine.
Step 4 Click **Change MSE Assignment**.

Step 5 Choose the mobility services engine to which the switches are to be synchronized.

Step 6 Click **Synchronize** to update the mobility services engine(s) database(s).

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

Step 7 To verify the NMSP connection between the switch and a mobility services engine, refer to **Verifying an NMSP Connection to a Mobility Services Engine**, page 7-57.

**Note** See the **Chapter 8, “Monitoring the System and Services,”** for information on monitoring wired switches.

---

**Verifying an NMSP Connection to a Mobility Services Engine**

NMSP manages communication between the mobility services engine and a controller or a location-capable Catalyst switch. Transport of telemetry, emergency, and chokepoint information between the mobility services engine and the controller or location-capable Catalyst switch is managed by this protocol.

To verify a NMSP connection between a mobility services engine and a controller or a location-capable Catalyst switch, follow these steps:

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

Step 2 At the Mobility Services page, click the device name link of the appropriate Catalyst switch or controller.

Step 3 Choose **System > Status > NMSP Connection Status** (see **Figure 7-34**).

**Figure 7-34 NMSP Connection Status**

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

If not active, resynchronize the Catalyst switch or controller and the mobility services engine.
Verifying an NMSP Connection to a Mobility Services Engine

Note  On a Catalyst wired switch, enter the `sh nmsp status` command to verify NMSP connection.
CHAPTER 8

Monitoring the System and Services

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

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

This chapter contains the following sections:

- Working with Alarms, page 8-2
- Working with Events, page 8-5
- Working with Logs, page 8-5
- Generating Reports, page 8-7
- Monitoring Wireless Clients, page 8-11
- Monitoring Tags, page 8-15
- Monitoring Chokepoints, page 8-23
- Monitoring Wi-Fi TDOA Receivers, page 8-24
- Monitoring Wired Switches, page 8-26
- Monitoring Wired Clients, page 8-29
Working with Alarms

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

This section consists of the following topics:
- Viewing Alarms, page 8-2
- Assigning and Unassigning Alarms, page 8-3
- Deleting and Clearing Alarms, page 8-3
- Emailing Alarm Notifications, page 8-4

Viewing Alarms

To view mobility services engine alarms, follow these steps:

Step 1 In WCS, choose Monitor > Alarms.
Step 2 Click the Advanced Search link in the navigation bar. A configurable search dialog box for alarms appears (see Figure 8-1).

**Figure 8-1** Advanced Search Alarm Dialog Box

![Advanced Search Alarm Dialog Box]

Step 3 Select Alarms as the Search Category.
Step 4 Select the Severity of Alarms to display. Options are All Severities, Critical, Major, Minor, Warning or Clear.
Step 5 Select Mobility Service from the Alarm Category.
Step 6 From the Time Period drop-down list, choose the time frame for which you want to review alarms.
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** Select the Acknowledged State check box to exclude the acknowledged alarms and their count from the Alarm Summary page.

**Step 8** Select the Assigned State check box to exclude the assigned alarms and their count from the Alarm Summary page.

**Step 9** From the Items per page drop-down list, choose the number of alarms to display on each window.

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

**Note** You can initiate the search thereafter, by clicking the Saved Search link.

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

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

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

### Assigning and Unassigning Alarms

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

**Step 1** Choose Monitors > Alarms to display the Alarms page.

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

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

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

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

### Deleting and Clearing Alarms

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

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

Step 1 Choose Monitors > Alarms to display the Alarms page.
Step 2 Select the alarms that you want to delete or clear by selecting their corresponding check boxes.
Step 3 From the Select a command drop-down list, choose Delete or Clear. Click Go.

Emailing Alarm Notifications

Cisco WCS lets you send alarm notifications to a specific email address. Sending notifications through email enables you to take prompt action when needed.
You can choose the alarm severity types (critical, major, minor, and warning) to have emailed to you.
To send alarm notifications, follow these steps:

Step 1 Choose Monitor > Alarms.
Step 2 From the Select a command drop-down list, choose Email Notification. Click Go. The Email Notification page appears (see Figure 8-2).

Figure 8-2 All Alarms > Email Notification page

Note An SMTP Mail Server must be defined before you enter target email addresses for email notification. Choose Administration > Settings > Mail Server Configuration to enter the appropriate information. You can also choose the Administration > Settings > Mail Server link, if it is displayed at the bottom of the All Alarms > Email Notification page.
Working with Events

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

To display events, follow these steps:

Step 1 In WCS, choose Monitor > Events.

Step 2 In the Events page:

- If you want to display the events for a specific element, and you know its IP address, name, WLAN SSID, or MAC address, enter that value in the Search text box of the navigation bar. Click Search.
- To display events by severity and category, click Advanced Search in the navigation bar and choose the appropriate options from the Severity and Event Category drop-down list boxes. Click Go.

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

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

Working with Logs

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

This section includes the following topics:

- Configuring Logging Options, page 8-6
- Downloading Log Files, page 8-7
Configuring Logging Options

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

To configure logging options, follow these steps:

**Step 1**  In WCS, click Services > Mobility Services.
**Step 2**  Click the name of the mobility services engine that you want to configure.
**Step 3**  From the System menu, click Logs. The logging options for the selected mobility services engine appear.
**Step 4**  Choose the appropriate options from the Logging Level drop-down list.

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

All log records with a log level of Error or above are logged to a new error log file locserver-error-%u-%g.log. This is an additional log file maintained along with the location server locserver-%u-%g.log log file. The error log file consists of logs of Error level along with their context information. The contextual information consists of 25 log records prior to the error. You can maintain up to 10 error log files. The maximum size allowed for each log file is 10 MB.

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

**Step 5**  Select the Enabled check box next to each element listed in that section to begin logging of its events.
**Step 6**  Select the Enable check box under Advanced Parameters to enable advanced debugging. By default, this option is disabled.

**Caution**  Enable advanced debugging only under the guidance of TAC personnel because advanced debugging slows the mobility service down.

**Step 7**  To download log files from the server, click Download Logs. For more information, see Downloading Log Files, page 8-7.

**Step 8**  In the Log File Parameters section, enter the following:

- The number of log files to be maintained in the mobility services engine. You can maintain a minimum of 5 log files and a maximum of 20 log files in the mobility services engine.
- The maximum log file size in MB. The minimum log file size is 10 MB and the maximum is 50 MB.

**Step 9**  In the MAC Address Based Logging Parameters section, do the following:

- Select the Enable check box to enable MAC address logging. By default, this option is disabled.
- Add one or more MAC addresses for which you want to enable logging. You can also remove MAC addresses that you have already added by selecting the MAC address from the list and clicking Remove.

For more information on MAC Address-based logging, see MAC Address-based Logging, page 8-7.

**Step 10**  Click Save to apply your changes.
MAC Address-based Logging

This feature allows you to create log files that are specific to an entity whose MAC address is specified. The log files are created in the locserver directory under the following path:

```
/opt/mse/logs/locserver
```

A maximum of 5 MAC addresses can be logged at a time. The log file format for MAC address `aa:bb:cc:dd:ee:ff` is:

```
macaddress-debug-aa-bb-cc-dd-ee-ff.log
```

You can create a maximum of two log files for a MAC Address. The two log files may consist of one main and one backup or rollover log file.

The minimum size of a MAC log file is 10 MB. The maximum size allowed is 20 MB per MAC Address. The MAC log files which are not updated for more than 24 hours are pruned.

Downloading Log Files

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

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

1. In WCS, click **Services > Mobility Services**.
2. Click the name of the mobility services engine to view its status.
3. From the left sidebar menu, click **Logs**.
4. Click **Download Logs**.
5. Follow the instructions in the File Download dialog box to open the file or save the zip file to your system.

Generating Reports

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

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

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

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

You can view the following in a location utilization report:

- Chart 1 summarizes and graphs CPU and memory utilization
Chapter 8  Monitoring the System and Services

Creating a Device Utilization Report

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

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

**Step 2** Choose Device > Utilization.

**Step 3** Click New. The Utilization Report Details page appears (see Figure 8-3).

**Figure 8-3  Device > Utilization Details Page**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>In the Settings pane, enter a report title.</td>
</tr>
<tr>
<td>5</td>
<td>The Report Type and Report By selections are always MSE.</td>
</tr>
<tr>
<td>6</td>
<td>Click Edit to select either a specific mobility services engine or All MSEs from the pop-up panel that appears.</td>
</tr>
<tr>
<td>7</td>
<td>Enter the reporting period. You can define the report to collect data hourly, weekly, or at a specific date and time. The selected reporting period type will display on the x-axis.</td>
</tr>
</tbody>
</table>
Note The reporting period uses a 24-hour rather than a 12-hour clock. For example, select hour 13 for 1:00 p.m.

Step 8 In the Schedule pane, select the **Enable Schedule** check box.

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

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** page. Enter the destination path for the files in the Repository Path text box.
- 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 list boxes.

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

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

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

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

Note You can also click **Run Now** to check the defined report criteria before saving it or to run reports as necessary.
The results appear at the bottom of the page (see Figure 8-4).

**Note** Only the CPU and memory utilization reports are shown in the following example (see Figure 8-4).

**Figure 8-4** Devise > MSE Utilization > Results

![Graph showing MSE Utilization over time with CPU and Memory Utilization markers](image)

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

**Figure 8-5** Utilization Reports Summary Page

![Utilization Reports summary page with scheduled and run reports](image)

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, select the check box next to the report title and click the appropriate option.
Viewing Saved Utilization Reports

To download a saved report, follow these steps:

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

Viewing Scheduled Utilization Runs

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

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

Monitoring Wireless Clients

This section describes about monitoring wireless clients and consists of the following topics:

- Monitoring Wireless Clients Using Maps, page 8-11
- Monitoring Wireless Clients Using Search, page 8-13

Monitoring Wireless Clients Using Maps

On a Cisco WCS map, you can view the name of the access point that the client is associated with, the IP Address, Asset information, Authentication, SSID, 802.11 protocol, and when the location information was last updated for the client. Hover the cursor over the client icon on the map to display this information.

You can also view the client details page, 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 the location status of a client on a map and view its client details page using maps, follow these steps:

**Step 1**  In WCS, choose **Monitor > Maps.**  
**Step 2**  Choose the building and floor on which the mobility services engine and its clients are located.  
**Step 3**  Select the **Clients** check box in the Floor Settings pane, if it is not already selected (see **Figure 8-6**).  
Do not click **Save Settings** unless you want to save changes made to the floor settings across all maps.
Step 4  Move the cursor over a client icon (blue square) and a summary of its configuration appears in a pop-up dialog box.

Step 5  Click the client icon to see client details (see Figure 8-7 and Figure 8-8).
Step 6  Click on the More link to configure asset information for the client.

Monitoring Wireless Clients Using Search

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

To view client information, follow these steps:

Step 1  In WCS, choose Monitor > Clients.

The Clients summary page appears.

Step 2  From the Show drop-down list, choose Clients Detected by MSEs. Click Go.

A summary of all clients detected by all mobility services engines and location appliances managed by Cisco WCS are displayed (see Figure 8-9).
a. To find a specific client by its IP address, name, SSID or MAC address, enter that value into the Search text box in the navigation bar (not all search values apply to all clients).

For example, if you enter a MAC address in the Search text box, the following page appears (see Figure 8-10).

b. 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.

c. To see alarms for the client, click View List for the alarm item type. A listing of all active alarms for that client noting severity, failure source (alarm description), owner of alarm (if assigned), date and time of the alarm, and whether or not alarm is acknowledged (see Figure 8-11).
Note You can also assign or unassign the alarm, email it, delete or clear it, and acknowledge and unacknowledge it at this page by choosing the appropriate option from the Select a command drop-down list.

d. To search for a client or multiple clients by device, network, map location and type of client (regular, rogue, or shunned), Click the Advanced search link.

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 list (see Figure 8-12).

Figure 8-12 Advanced Search page

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 page. You can also use Advanced Search to monitor tags.

This section consists of the following topics:

- Monitoring Tags Using Maps, page 8-15
- Monitoring Tags Using Search, page 8-18
- Overlapping Tags, page 8-22

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. Hover the mouse 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 WCS, choose Monitor > Maps.

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

**Step 3** Select the **802.11 Tags** check box in the Floor Settings pane, if it is not already selected (see Figure 8-13).

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

**Step 4** Move the cursor over a tag icon (yellow tag) and a summary of its configuration appears in a Tag dialog box.
Step 5  
Click the **tag** icon to see tag details (see Figure 8-14).

You can also configure the asset information by entering the required information in the Asset Info pane.

**Figure 8-14  Tag Details Page**

![Tag Details Page](image)

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

**Figure 8-15  Tag Location History Page**

![Tag Location History Page](image)
Monitoring Tags Using Search

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

You can further refine your search using the Advanced search parameters and save the search criteria for future use. Click Saved Searches to retrieve saved searches.

When you click on the MAC address of a tag location in a search results page, 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 page appears (see Figure 8-16).

**Figure 8-16 Monitor > Tags Page**

**Step 2** To view a summary of tags associated with a specific mobility services engine, click the Total Tags link (see Figure 8-17).
Step 3  To search for a specific tag, if you know its MAC address, asset name (not all search values apply to all tags) click the Search link.

Step 4  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 click the Advanced Search link (see Figure 8-18).

a. In the Advanced Search pane, select Tags as the search category.

b. Select the additional tag search criteria. See Table 8-1 for a list of search criteria and their possible values.

c. Click Go when all advanced search parameters are selected. The results are shown in Figure 8-19.

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

Figure 8-18   Advanced Search Pane for Tags

[Image: Advanced Search Pane for Tags]

Figure 8-19   Advanced Search Results for Tag

[Image: Advanced Search Results for Tag]

Note If you click the MAC address of any of these tags, a Tag details page appears similar to that in Figure 8-14.
## Table 8-1  Tag Search Criteria and Values

<table>
<thead>
<tr>
<th>Search Criteria</th>
<th>Variable Search Criteria</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search for tags by (Tier 1 search criteria)</td>
<td>—</td>
<td>All Tags; Asset Name, Asset Category or Asset Group; MAC Address; Controller or MSEs; Floor Area or Outdoor Area.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note MSE search includes both location servers and mobility services engines.</td>
</tr>
<tr>
<td>Search in (Tier 2 search criteria)</td>
<td>—</td>
<td>MSEs or WCS Controllers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note WCS Controller option indicates that the search for controllers is done within WCS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note MSE search includes both location servers and mobility services engines.</td>
</tr>
<tr>
<td>Last detected within</td>
<td>—</td>
<td>Options are from 5 minutes to 24 hours.</td>
</tr>
<tr>
<td>Variable search criteria. (Tier 3 search criteria)</td>
<td>If the Search for tags by value is:</td>
<td></td>
</tr>
<tr>
<td>Note Possible search criteria determined by the Search for tabs by (Tier 1 search) value.</td>
<td>1. Asset Name, then enter tag asset name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Asset Category, then enter tag asset category.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Asset Group, then enter tag asset group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. MAC Address, then enter tag MAC address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Controller, then select controller IP address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. MSEs, then choose an MSE IP address from drop-down list.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. Floor Area, then choose campus, building, and floor area.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. Outdoor Area, then choose campus and outdoor area.</td>
<td></td>
</tr>
<tr>
<td>Telemetry tags only</td>
<td>—</td>
<td>Check box to display telemetry tags. Leaving option unselected displays all tags.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note Option only seen when the Search In option is MSE.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note Only those vendor tags that support telemetry appear.</td>
</tr>
<tr>
<td>Tag vendor</td>
<td>—</td>
<td>Check box to select tag vendor from drop-down list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note Option only seen when the Search In option is MSE.</td>
</tr>
<tr>
<td>Items per page</td>
<td>—</td>
<td>Select the number of tags to display per search request. Values range from 10 to 500.</td>
</tr>
<tr>
<td>Save search</td>
<td>—</td>
<td>Check box to name and save search criteria. Once saved, entry appears under Saved Searches heading.</td>
</tr>
</tbody>
</table>
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 hover the mouse over the overlapping tag on the map, a pane appears with summary information for the overlapping tags (see Figure 8-20).

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

Figure 8-20  Overlapping Tags Page

- 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, choose that option from the Select a command drop-down list and click Go.
  - To return to the details screen from the location history page, choose the Tag Detail option and click Go.
Monitoring Chokepoints

A chokepoint must be assigned to a map for its location to be monitored. See the “Adding Chokepoints to the WCS” section on page 7-13. After adding the TDOA receiver to a map, you must resynchronize the network designs (Services > Synchronize Services) with the mobility services engine for it to appear on the map.

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

All chokepoint setup is done using the AeroScout System Manager.

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

To monitor chokepoints, follow these steps:

**Step 1** Choose **Monitor > Chokepoints**. The Chokepoint summary page 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 text box of the navigation bar. Click **Search** (see Figure 8-21).

*Figure 8-21  Search for Chokepoint by MAC Address*

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

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

*Figure 8-22  MAC Address Search Results for a Chokepoint Indicating a Match*
b. To initiate an advanced search for a chokepoint by its MAC address or name, click the **Advanced Search** link.
   1. Select **Chokepoint** as the search category.
   2. From the Search for Chokepoint by drop-down list, choose either **Chokepoint Name** or **MAC Address**.
   3. Enter either the chokepoint name or MAC address.
   4. Click **Search**.

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

*Figure 8-23  Chokepoint Name Advanced Search Dialog Box*

If no match exists, a message appears in the page (see Figure 8-24). Otherwise the Search Result page appears.

*Figure 8-24  Chokepoint Advanced Search Results Indicating no Match*

---

**Monitoring Wi-Fi TDOA Receivers**

A Wi-Fi TDOA receiver must be assigned to a map for its location to be monitored. See the “Adding Wi-Fi TDOA Receivers to WCS” section on page 7-20. After adding the TDOA receiver to a map, you must resynchronize network designs (Services > Synchronize Services) with the mobility services engine for it to appear on the map.

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

All TDOA receiver setup is done using the AeroScout System Manager.
To monitor TDOA receivers, follow these steps:

**Step 1** Choose **Monitor > WiFi TDOA Receivers**. The WiFi TDOA Receivers summary page 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 text box. Click **Search** (see **Figure 8-25**).

**Figure 8-25**  **Monitor > WiFi TDOA Receivers Search Page**

![Figure 8-25 Monitor > WiFi TDOA Receivers Search Page](image)

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

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

**Figure 8-26**  **Search Results Page**

![Figure 8-26 Search Results Page](image)

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

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

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

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

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

To view details on wired switches, follow these steps:

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

**Step 2** In the Mobility Services page, click the device name link of the appropriate wired location switch.

**Step 3** Choose Context Aware Service > Wired > Wired Switches (see Figure 8-29). A summary of wired switches that are synchronized with the mobility services engine appears.
Step 4  To see more details on the switch, its ports, its wired clients (count and status), and its civic information click the **IP address** link (see Figure 8-30).

**Figure 8-30  Wired > Wired Switches > IP Address Page**

![IP address page](image)

---

**Note**  You can export civic information from the switch by choosing that option from the Select a command drop-down list. This option is available on all four tabs of the Wired Switches page.

- On the Switch Information tab, a total count of wired clients connected to the switch is summarized along with their state (connected, disconnected, and unknown).
- Connected clients—Clients that are connected to the wired switch.
- Disconnected clients—Clients that are disconnected from the wired switch.
- Unknown clients—Clients are marked as unknown when the NMSP connection to the wired switch is lost.

You can view detailed wired client information by clicking one of the client count links (total clients, connected, disconnected, and unknown). Refer to the “Monitoring Wired Clients” section on page 8-29 for details.

Step 5  Click the **Switch Ports** tab to see a detailed list of the ports on the switch (see Figure 8-31).
You can change the listing order (ascending, descending) of port IP addresses, slot numbers, module number, and port number by clicking the respective column heading.

**Figure 8-31  Wired Switches > Switch Ports Page**

![Wired Switches > Switch Ports Page](image1)

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

**Figure 8-32  Wired Switches > Civic Tab**

![Wired Switches > Civic Tab](image2)

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

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

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

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

You can view the details of the wired clients on either the Wired Switches page (Context Aware Service > Wired > Wired Switches) or wired clients page (Context Aware Service > Wired > Wired Clients).

- If you know the IP address, MAC address, VLAN ID, serial number, or username, you can use the Search text box on the Wired Clients page.
- If you want to examine wired clients as they relates to a specific switch, you can view that information on the Wired Switches page. See the “Monitoring Wired Switches” section on page 8-26.

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

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

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

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

At the Wired Clients summary page, clients are grouped by their switch.

The status of a client is noted as connected, disconnected, or unknown. Definitions are summarized as follows:

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

• If you know the MAC address of the wired client, then you can click on that link to reach the detail page of the client (see Figure 8-34) or use the Search text box.
  – You can also search for a wired client by its IP address, username, or VLAN ID.

• If you click on the IP address of the switch, you are forwarded to the detail page of the switch. See the “Monitoring Wired Switches” section on page 8-26.

*Figure 8-34  Wired Clients > Device Information Page*

Step 4  Click the Port Association tab to show the physical location of the switch port/slot/module on which the wired client terminates, the client status (connected, disconnected, unknown), and the switch IP address (see Figure 8-35).

*Figure 8-35  Wired Clients > Port Association Page*

Step 5  Click the Civic Address tab to show any civic address information (see Figure 8-36).

Step 6  Click the Advanced tab to see any extended physical address details for the wired clients, if any (see Figure 8-37).
Note

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

Figure 8-36  Wired Clients > Civic Address Page

Figure 8-37  Wired Clients > Advanced Page
Monitoring Interferers

The Monitor > Interferer page allows you to monitor interference devices detected by the CleanAir enabled access points.

This section provides information on the interferers detected by the CleanAir enabled access points. By default, the Monitor > Interferers > AP Detected Interferers, page 8-32 page is displayed.

This section includes the following topics:

- Monitor > Interferers > AP Detected Interferers, page 8-32
- Monitor > Interferers > AP Detected Interferers > Interferer Details, page 8-33
- Monitor > Interferers > Edit View, page 8-35

Monitor > Interferers > AP Detected Interferers

Choose Monitor > Interferers to view all the interfering devices detected by the CleanAir enabled access points on your wireless network. This page enables you to view a summary of the interfering devices including the following default information:

- Interferer ID—A unique identifier for the interferer. Click this link to learn more about the interferer.
- Type—Indicates the category of the interferer. Click to read more about the type of device. The pop-up dialog appears displaying more details. The categories include:
  - Bluetooth link—A Bluetooth link (802.11b/g/n only)
  - Microwave Oven—A microwave oven (802.11b/g/n only)
  - 802.11 FH—An 802.11 frequency-hopping device (802.11b/g/n only)
  - Bluetooth Discovery—A Bluetooth discovery (802.11b/g/n only)
  - TDD Transmitter—A time division duplex (TDD) transmitter
  - Jammer—A jamming device
  - Continuous Transmitter—A continuous transmitter
  - DECT-like Phone—A digital enhanced cordless communication (DECT)-compatible phone
  - Video—A video camera
  - 802.15.4—An 802.15.4 device (802.11b/g/n only)
  - WiFi Inverted—A device using spectrally inverted Wi-Fi signals
  - WiFi Invalid—A device using non-standard Wi-Fi channels
  - SuperAG—An 802.11 SuperAG device
  - Canopy—A Motorola Canopy device
  - Radar—A radar device (802.11a/n only)
  - XBox—A Microsoft Xbox (802.11b/g/n only)
  - WiMAX Mobile—A WiMAX mobile device (802.11a/n only)
  - WiMAX Fixed—A WiMAX fixed device (802.11a/n only)
- Status—Indicates the status of the interfering device.
  - Active—Indicates that the interferer is currently being detected by the CleanAir enabled access point.
Chapter 8 Monitoring the System and Services

Monitoring Interferers

- Inactive—Indicates that the interferer is no longer being detected by the CleanAir enabled access point or the CleanAir enabled access point saw the interferer no longer reachable by WCS.
- Severity—Displays the severity ranking of the interfering device.
- Affected Band—Displays the band in which this device is interfering.
- Affected Channels—Displays the affected channels.
- Duty Cycle (%)—The duty cycle of interfering device in percentage.
- Discovered—Displays the time at which it was discovered.
- Last Updated—The last time the interference was detected.
- Floor—The location where the interfering device is present.

Note
These devices appear only if the option to track Interferers is enabled in the Tracking Parameters page. This option is disabled by default. For more information on tracking parameters, see Modifying Tracking Parameters, page 7-34.

Monitor > Interferers > AP Detected Interferers > Interferer Details

Choose Monitor > Interferers > Interferer ID to view this page. This page enables you to view the details of the interfering devices detected by the access points. This page provides the following details about the interfering device.

- Interferer Properties
  - Type—Displays the type of the interfering device detected by the AP.
  - Status—The status of the interfering device. Indicates the status of the interfering device.
    - Active—Indicates that the interferer is currently being detected by the CleanAir enabled access point.
    - Inactive—Indicates that the interferer is no longer being detected by the CleanAir enabled access point or the CleanAir enabled access point saw the interferer no longer reachable by WCS.
  - Severity—Displays the severity ranking of the interfering device.
  - Duty Cycle (%)—The duty cycle of interfering device in percentage.
  - Affected Band—Displays the band in which this device is interfering.
  - Affected Channels—Displays the affected channels.
  - Discovered—Displays the time at which it was discovered.
  - Last Updated—The last time the interference was detected.

- Location
  - Floor—The location where this interfering device was detected.
  - Last Located At—The last time where the interfering device was located.
  - On MSE—The mobility services engine on which this interference device was located.

- Clustering Information
  - Clustered By—Displays the following:
    IP address of the controller if clustered by a controller.
Chapter 8      Monitoring the System and Services

Monitoring Interferers

IP address of the mobility services engine if clustered by a mobility services engine.

- Detecting APs—Displays the details of the access point that has detected the interfering device. The details include: Access Point Name (Mac), Severity, and Duty Cycle(%).

Note

The detecting access point information is available only for active devices. And even for some active devices, this information may not be available. This is because those interferers are in the process of being marked inactive and in the next refresh of the Monitor > Interferers page, those will appear inactive.

- Details—Displays a short description about the interfering type.

Select a Command

The Select a Command drop-down list provides access to the location history of the interfering device detected by the access point. See Monitor > Interferers > AP Detected Interferer Details > Interference Device ID > Location History.

Monitor > Interferers > AP Detected Interferer Details > Interference Device ID > Location History

Choose Monitor > Interferers > Interference Device ID and choose Location History from the Select a Command drop-down list, and click Go to view this page.

- Interferer Information—Displays the basic information about the interfering device.
  - Data Collected At—The time stamp at which the data was collected.
  - Type—The type of the interfering device.
  - Severity—The severity index of the interfering device.
  - Duty Cycle—The duty cycle (in percentage) of the interfering device.
  - Affected Channels—A comma-separated list of the channels affected.

- Interferer Location History—Displays the location history of the interfering devices.
  - Time Stamp
  - Floor

- Clustering Information
  - Clustered By

- Detecting APs
  - AP Name—The access point that detected the interfering device.
  - Severity—The severity index of the interfering device.
  - Duty Cycle(%)—The duty cycle (in percentage) of the interfering device.

- Location
  - Location Calculated At—Displays the time stamp at which this information was generated.
  - Floor—Displays location information of the interfering device.
  - A graphical view of the location of the interfering device is displayed in a map. Click the Enlarge link to view an enlarged image.
Monitor > Interferers > Edit View

The Edit View page allows you to add, remove, or reorder columns in the AP Detected Interferers Summary page. It also allows you to search for Interferers. By default only those interferers that are in Active state and with severity greater than or equal to 5 are displayed in the AP Detected Interferers page. For more information on editing search criteria, see Monitor > Interferers > Edit View > Edit Search, page 8-35.

To edit the columns in the AP Detected Interferers page, follow these steps:

Step 1 Choose Monitor > Interferers. The AP Detected Interferers page appears showing details of the interferers detected by the CleanAir enabled access points.

Step 2 Click the Edit View link in the AP Detected Interferers page.

Step 3 To add an additional column to the access points table, click to highlight the column heading in the left column. Click Show to move the heading to the right column. All items in the right column are displayed in the table.

Step 4 To remove a column from the access points table, click to highlight the column heading in the right column. Click Hide to move the heading to the left column. All items in the left column are not displayed in the table.

Step 5 Use the Up/Down buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click Up or Down to move it higher or lower in the current list.

Step 6 Click Reset to restore the default view.

Step 7 Click Submit to confirm the changes.

Monitor > Interferers > Edit View > Edit Search

You can search for interferers based on certain criteria. By default only those interferers that are in Active state and with severity greater than or equal to 5 are displayed in the AP Detected Interferers page. Use the Edit Search option to customize the interferer search.

To edit the search criteria, follow these steps:

Step 1 Choose Monitor > Interferers. The AP Detected Interferers page appears.

Step 2 Click Edit Search and complete the applicable parameters in the New Search dialog box (see Figure 8-38).
This option allows you to specify the following search criteria:

- **Search Category**—For interferer search, the search category is Interferers.
- **Detected By**—Select from the drop-down list if the interferer is detected by access points or interferer.
- **Search By**—Select one of the options from the list:
  - All Interferers
  - Interferer ID
  - Interferer Type
  - Severity
  - Duty Cycle
  - Location
- **Severity greater than**—Enter the severity level in the text box.
- **Detected within the last**—Choose one of the option from the drop-down list:
  - 5 Minutes
  - 15 Minutes
  - 30 Minutes
  - 1 Hour
  - 3 Hours
  - 6 Hours
  - 12 Hours
  - 24 Hours
  - All History
- **Interferer status**—Choose one of the option from the drop-down list:
  - Active
  - Inactive
  - All
• Restrict By Radio Band/Channels—Select this check box if you want to restrict certain radio frequencies or channels from the search. By default this check box is unselected. On selected this check box, a drop-down list appears with 2.4 GHz, 5 GHz and Individual Channel options. If you select Individual Channel, an Affected Channels text box appears. Specify the channel and select either Match All or Match Any radio button.

Step 3 Select the number of items per page that you want to view in the search results.
Step 4 Choose the Save Search check box if you want to save the search.
Step 5 After specifying the search criteria, click Go to view the search results.
Performing Maintenance Operations

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

This chapter contains the following sections:

- Recovering a Lost Password, page 9-1
- Recovering a Lost Root Password, page 9-2
- Backing Up and Restoring Mobility Services Engine Data, page 9-2
- Downloading Software to Mobility Services Engines, page 9-4
- Configuring NTP Server, page 9-6
- Resetting the System, page 9-6
- Defragmenting the Database, page 9-6
- Clearing the Configuration File, page 9-6

Recovering a Lost Password

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

---

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

**Step 2** Press e to edit.

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

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

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

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

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

**Step 6** Enter and confirm the new password.

**Step 7** Reboot the machine.

---
Recovering a Lost Root Password

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

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

**Step 2** Press `e` to edit.

**Step 3** Navigate to the line beginning with kernel and press `e`.
At the end of the line, enter a space, followed by 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 set up a single-user mode password.

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

**Step 6** Enter and confirm the new password.

**Step 7** Restart the machine.

Backing Up and Restoring Mobility Services Engine Data

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

This section consists of the following topics:
- Backing Up Mobility Services Engine Historical Data, page 9-2
- Restoring Mobility Services Engine Historical Data, page 9-3
- Enabling Automatic Location Data Backup, page 9-4

Backing Up Mobility Services Engine Historical Data

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

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

**Step 1** In 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** Click Submit to back up the historical data to the hard drive of the server running WCS.
The Status of the backup can be seen on the screen while the backup is in process. Three items will appear on the screen during the backup process: (1) Last Status text box, that provides messages noting the status of the backup; (2) Progress text box that shows what percentage of the backup is complete; and (3) Started at text box that shows when the backup began noting date and time.

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

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

---

**Restoring Mobility Services Engine Historical Data**

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

To restore mobility services engine data, follow these steps:

1. **Step 1** In WCS, choose **Services > Mobility Services**.
2. **Step 2** Click the name of the mobility services engine that you want to restore.
3. **Step 3** Choose **System > Maintenance**.
4. **Step 4** Click **Restore**.
5. **Step 5** Choose the file to restore from the drop-down list.
6. **Step 6** Select the **Delete synchronized service assignments** check box if you want to permanently remove all service assignments from the mobility services engine.

This option is applicable for network designs, wired switches, controllers, and event definitions. The existing location history data is retained, however, you must use manual service assignments to perform any future location calculations.

7. **Step 7** Click **Submit** to start the restoration process.
8. **Step 8** Click **OK** to confirm that you want to restore the data from the Cisco WCS server hard drive.

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

**Note** You should not work on other mobility service engine operations when the restore process is running.
Enabling Automatic Location Data Backup

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In WCS, choose Administration &gt; Background Tasks.</td>
</tr>
<tr>
<td>2</td>
<td>Select the Mobility Service Backup check box.</td>
</tr>
<tr>
<td>3</td>
<td>From the Select a command drop-down list, choose Enable Task and click Go. The backups are stored in the FTP directory that you specify during the Cisco WCS installation.</td>
</tr>
</tbody>
</table>

Downloading Software to Mobility Services Engines

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Verify that you can ping the mobility services engine from the Cisco WCS server or an external FTP server, whichever you are going to use for the application code download.</td>
</tr>
<tr>
<td>2</td>
<td>In WCS, choose Services &gt; Mobility Services.</td>
</tr>
<tr>
<td>3</td>
<td>Click the name of the mobility services engine to which you want to download software.</td>
</tr>
<tr>
<td>4</td>
<td>Choose System &gt; Maintenance.</td>
</tr>
<tr>
<td>5</td>
<td>Click Download Software.</td>
</tr>
<tr>
<td>6</td>
<td>To download software, do one of the following:</td>
</tr>
<tr>
<td></td>
<td>- 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 list. Cisco WCS downloads the binary images listed in the drop-down list into the FTP server directory you specified during the Cisco WCS installation.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td>7</td>
<td>Click Download to send the software to the /opt/installers directory on the mobility services engine.</td>
</tr>
<tr>
<td>8</td>
<td>After the image is transferred to the mobility services engine, log in to the mobility services engine CLI.</td>
</tr>
<tr>
<td>9</td>
<td>Run the installer image from the /opt/installers directory by entering ./bin mse image command. This installs the software.</td>
</tr>
<tr>
<td>10</td>
<td>To run the software, enter /etc/init.d/msed start.</td>
</tr>
</tbody>
</table>

Note: To stop the software, enter /etc/init.d/msed stop, and to check status, enter /etc/init.d/msed status.
Manually Downloading Software

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

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

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

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

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

   Your entries should look like this example:

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

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

3. To decompress (unzip) the image file, enter the following command:
   ```
   gunzip CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz
   ```
   The decompression yields a bin file.

4. Make sure that the CISCO-MSE-L-K9-x-x-x-x.bin file has execute permissions for the root user. If not, enter the following command:
   ```
   chmod 755 CISCO-MSE-L-K9-x-x-x-x.bin
   ```

### Step 2
Manually stop the mobility services engine.

### Step 3
Log in as root and enter:

```
/etc/init.d/msed stop.
```

### Step 4
To install the new mobility services engine image, enter the following command:

```
/opt/installers/CISCO-MSE-L-K9-x-x-x-x.bin.
```

### Step 5
Start the new mobility services engine software by entering the following command:

```
/etc/init.d/msed start
```

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

### Step 6
Enter the following command to uninstall the script files of the mobility services engine:
Configuring NTP Server

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

Note
- You are automatically prompted to enable NTP and enter NTP server IP addresses as part of the automatic installation script for the mobility services engine. For more details on the automatic installation script, see the Cisco 3350 Mobility Services Engine Getting Started Guide or Cisco 3310 Mobility Services Engine Getting Started Guide at the following link:
- If you need to add or change an NTP server installation after a mobility services engine install, rerun the automatic installation script. You can configure the NTP server without adjusting the other values by tabbing through the script.

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

Resetting the System

For information on rebooting or shutting down the mobility services engine hardware, see the Rebooting or Shutting Down a System, page 4-11.

Defragmenting the Database

For information on defragmenting the mobility services engine database, see the Defragmenting The Database, page 4-11

Clearing the Configuration File

For information on clearing the configuration file, see the Clearing the System Database, page 4-11
<table>
<thead>
<tr>
<th>A</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>alarm notifications</td>
<td></td>
</tr>
<tr>
<td>emailing</td>
<td>8-4</td>
</tr>
<tr>
<td>alarms</td>
<td></td>
</tr>
<tr>
<td>assigning</td>
<td>8-3</td>
</tr>
<tr>
<td>clearing</td>
<td>8-3</td>
</tr>
<tr>
<td>deleting</td>
<td>8-3</td>
</tr>
<tr>
<td>unassigning</td>
<td>8-3</td>
</tr>
<tr>
<td>viewing</td>
<td>8-2</td>
</tr>
<tr>
<td>applying calibration models</td>
<td>7-4</td>
</tr>
<tr>
<td>automatic synchronization</td>
<td>3-6</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
</tr>
<tr>
<td>calibration models</td>
<td>7-4</td>
</tr>
<tr>
<td>calibration models, applying</td>
<td>7-4</td>
</tr>
<tr>
<td>clearing</td>
<td>6-8</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
</tr>
<tr>
<td>event definition</td>
<td></td>
</tr>
<tr>
<td>adding</td>
<td>6-3</td>
</tr>
<tr>
<td>deleting</td>
<td>6-6</td>
</tr>
<tr>
<td>testing</td>
<td>6-7</td>
</tr>
<tr>
<td>event groups</td>
<td></td>
</tr>
<tr>
<td>adding</td>
<td>6-2</td>
</tr>
<tr>
<td>deleting</td>
<td>6-2</td>
</tr>
<tr>
<td>event notifications</td>
<td></td>
</tr>
<tr>
<td>summary</td>
<td>6-7</td>
</tr>
<tr>
<td>events</td>
<td></td>
</tr>
<tr>
<td>viewing</td>
<td>8-5</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td></td>
</tr>
<tr>
<td>general properties</td>
<td></td>
</tr>
<tr>
<td>editing</td>
<td>4-1</td>
</tr>
<tr>
<td>groups</td>
<td></td>
</tr>
<tr>
<td>adding</td>
<td>5-1</td>
</tr>
<tr>
<td>deleting</td>
<td>5-2</td>
</tr>
<tr>
<td>permissions</td>
<td>5-2</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>H</td>
<td></td>
</tr>
<tr>
<td>history parameters</td>
<td></td>
</tr>
<tr>
<td>editing</td>
<td>7-41</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>L</td>
<td></td>
</tr>
<tr>
<td>location parameters</td>
<td></td>
</tr>
<tr>
<td>editing</td>
<td>7-33</td>
</tr>
<tr>
<td>location readiness</td>
<td>7-9</td>
</tr>
<tr>
<td>location server</td>
<td></td>
</tr>
<tr>
<td>automatic backup</td>
<td>9-4</td>
</tr>
<tr>
<td>backup historical data</td>
<td>9-2</td>
</tr>
<tr>
<td>restore historical data</td>
<td>9-3</td>
</tr>
<tr>
<td>software download</td>
<td>9-4</td>
</tr>
<tr>
<td>location smoothing</td>
<td>7-44</td>
</tr>
<tr>
<td>log files</td>
<td></td>
</tr>
<tr>
<td>download</td>
<td>8-7</td>
</tr>
<tr>
<td>log options</td>
<td></td>
</tr>
<tr>
<td>configuring</td>
<td>8-6</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>M</td>
<td></td>
</tr>
<tr>
<td>monitoring</td>
<td>8-15</td>
</tr>
</tbody>
</table>
monitoring tags 8-15

N

network designs 3-2
notification
  statistics 7-48
NTP Server
  Configuring 9-6

O

out-of-sync 3-8

P

password
  recovering lost 9-1
polling parameters
  editing 7-34, 7-38
pull 1-4

R

RFID Asset Tags 1-3
rogue access points 1-3

S

scheduled tasks 3-6
Simple Mail Transfer Protocol 1-4
Simple Network Management Protocol 1-4
SMTP 1-4
SNMP 1-4
SOAP 1-4
Specifies Simple Object Access Protocol 1-4
Synchronization 3-8
synchronization history 3-9

synchronization status 3-8
SysLog 1-4

U

users
  adding 5-3
  deleting 5-3
  properties 5-4