CHAPTER 13

Mobility Services

This chapter briefly describes the CAS or wIPS services that Cisco WCS supports and gives steps for mobility procedures that are common across all services. You can refer to the Cisco Context-Aware Services documentation with the provided links for additional CAS and wIPS configuration and management details.

CAS

Context Aware Software (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.

Note You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points. Licenses for tags and clients are offered independently. For details on tag and client licenses, refer to the *Cisco 3350 Mobility Services Engine Release Note* at:

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

wIPS

The Cisco Adaptive Wireless IPS (wIPS) is an advanced approach to wireless threat detection and performance management. Cisco Adaptive wIPS combines network traffic analysis, network device and topology information, signature-based techniques and anomaly detection to deliver highly accurate and complete wireless threat prevention.

Note wIPS functionality is not supported for non-root partition users.

MSE Services Co-Existence

Starting from MSE Release 6.0, you can enable multiple services (Context Aware and wIPS) to run concurrently. Prior to version 6.0, mobility services engines could only support one active service at a time.

The following must be considered with co-existence of multiple services:

- Co-existence of services may be impacted by license enforcement. As long as the license is not expired, you can enable multiple services.

  Note Limits for individual services differ. For example, a low-end mobility services engine (MSE-3310) tracks a total of 2,000 CAS elements; a high-end mobility services engine (MSE-3350) tracks a total of 18,000 CAS elements.
  A low-end mobility services engine has a maximum limit of 2,000 wIPS elements; a high-end mobility services engine has a maximum limit of 3,000 wIPS elements. See the license order guide for the valid combination matrix.

- Expired evaluation licenses prevent the services from coming up.
- If a CAS license is added or removed, this process restarts all services on the mobility services engine including wIPS. If a wIPS license is added or removed, the process does not impact CAS; only wIPS restarts.
- Other services can be enabled in evaluation mode even if a permanent license for the maximum number of elements has been applied.

  Whenever one of the services has been enabled to run with its maximum license, another service can not be enabled to run concurrently because the capacity of the MSE would not be sufficient to support both services concurrently. For example, on MSE-3310, if you install a wIPS license of 2000, then you can not enable CAS to run concurrently. However, evaluation licenses are not subject to this limitation.

Note See the "MSE License Information" section on page 18-70 for more information on mobility services engine licensing.

Adding a Mobility Services Engine to Cisco WCS

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

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

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

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

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

Note An MSE is added only if a valid IP address is entered. The Device Name helps you distinguish between devices if you have multiple WCSs with multiple MSEs, but it is not considered when validating an MSE.

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

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.

The default username and password are both *admin*.

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

Step 8 Click **Next**. The Select Mobility Service page appears.

Note If you click **Cancel**, the MSE is not added. Any services that are already running on MSE are maintained, but if you want a change to a service to be accepted, you must complete Step 10.

Step 9 Click the circle next to the service(s) that you want to enable.

Step 10 Click **Save**.

Note After adding a new mobility services engine, you can synchronize network designs (floor, campus, building, and outdoor maps) and event groups on the local mobility services engine with Cisco WCS. You can also choose to synchronize the mobility services engine with a specific controller or with a wired switch. You can do this synchronization immediately after adding a new mobility services engine or at a later time. To synchronize the local and Cisco WCS databases, continue to the "Synchronizing Cisco WCS and a Mobility Services Engine" section on page 13-4.

Deleting a Mobility Services Engine from the Cisco WCS

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

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

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

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

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

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

Keeping the Mobility Services Engines Synchronized

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

After adding a mobility services engine to Cisco WCS, you can synchronize network designs (floor, campus, building, and outdoor maps), event groups, or controller information (name and IP address) with the mobility services engine.

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

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

Synchronizing Cisco WCS and a Mobility Services Engine

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

After adding a mobility services engine to Cisco 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.

Note Be sure to verify software compatibility between the controller, Cisco WCS, and the mobility services engine before synchronizing. See 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 Cisco 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 Cisco WCS server. An NTP server is required to automatically synchronize time between the controller, Cisco WCS, and the mobility services engine.

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

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

Four menu items appears 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).

To assign a network design to a mobility services engine:

a. On the synchronization page, choose Network Designs from the menu on the left side.

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

Note Through Release 6.0, you can assign only 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.

c. Click **Change MSE Assignment**.

d. Select the mobility services engine to which the maps are to be synchronized.

e. Click either of the following in the MSE Assignment dialog box:
   - OK—Saves the mobility services engine assignment. The following message appears in the Messages column of the Network Designs page.

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

You can also select one or more maps and click **Reset** to undo the yellow button assignments for those maps.

Note 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.

Step 3 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 Cisco WCS and a Mobility Services Engine, page 13-4 for more information.

Configuring Automatic Database Synchronization and Out of Sync Alerts

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

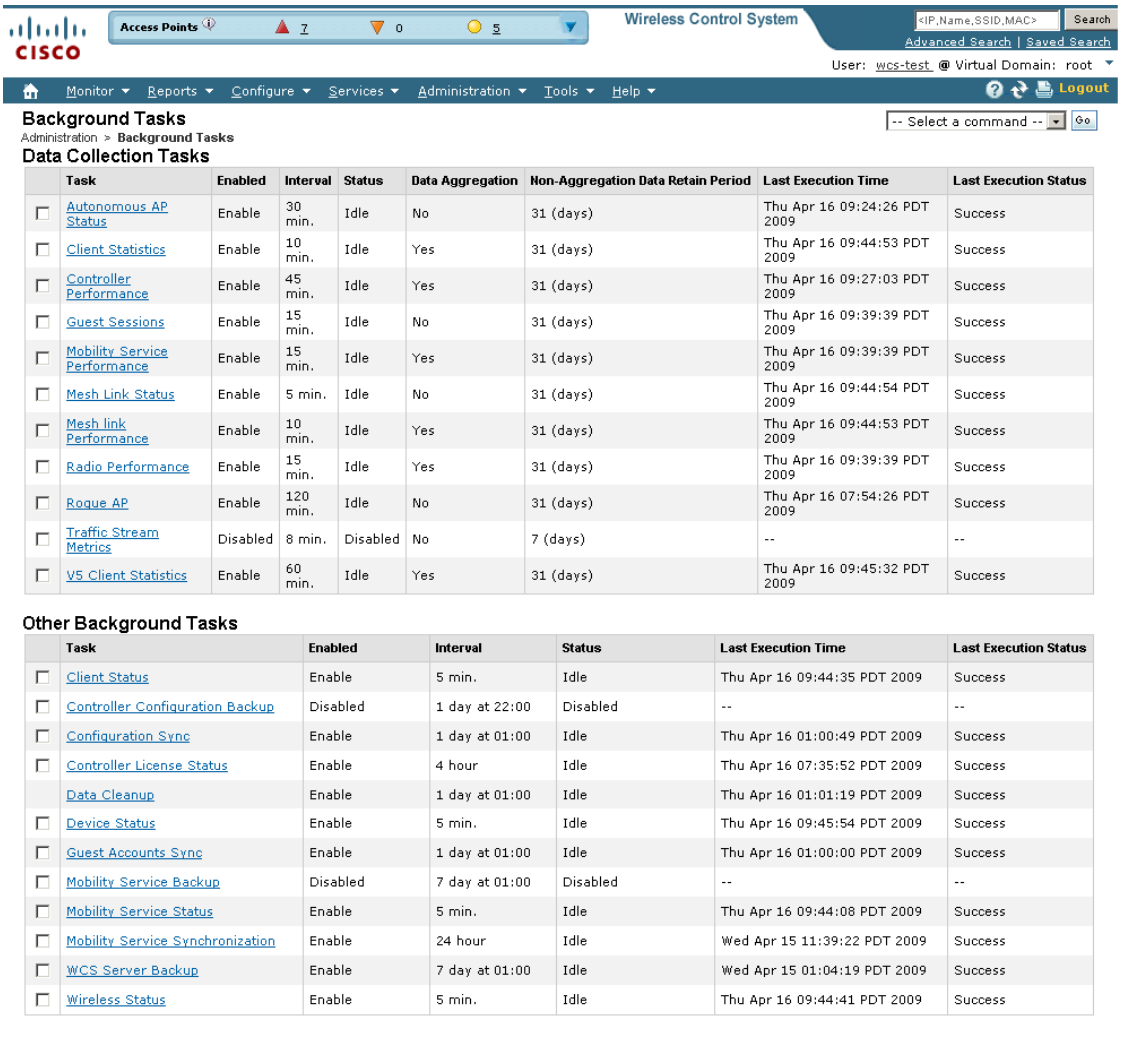
To prevent out-of-sync conditions, use Cisco WCS to enable smart synchronization. This policy ensures that synchronization between Cisco WCS and mobility services engine databases is triggered periodically and any related alarms are cleared.

To configure smart synchronization, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

The Background Tasks summary page appears (see Figure 13-1).

Figure 13-1 Administration > Background Tasks



Data Collection Tasks

Task	Enabled	Interval	Status	Data Aggregation	Non-Aggregation Data Retain Period	Last Execution Time	Last Execution Status
Autonomous AP Status	Enable	30 min.	Idle	No	31 (days)	Thu Apr 16 09:24:26 PDT 2009	Success
Client Statistics	Enable	10 min.	Idle	Yes	31 (days)	Thu Apr 16 09:44:53 PDT 2009	Success
Controller Performance	Enable	45 min.	Idle	Yes	31 (days)	Thu Apr 16 09:27:03 PDT 2009	Success
Guest Sessions	Enable	15 min.	Idle	No	31 (days)	Thu Apr 16 09:39:39 PDT 2009	Success
Mobility Service Performance	Enable	15 min.	Idle	Yes	31 (days)	Thu Apr 16 09:39:39 PDT 2009	Success
Mesh Link Status	Enable	5 min.	Idle	No	31 (days)	Thu Apr 16 09:44:54 PDT 2009	Success
Mesh link Performance	Enable	10 min.	Idle	Yes	31 (days)	Thu Apr 16 09:44:53 PDT 2009	Success
Radio Performance	Enable	15 min.	Idle	Yes	31 (days)	Thu Apr 16 09:39:39 PDT 2009	Success
Rogue AP	Enable	120 min.	Idle	No	31 (days)	Thu Apr 16 07:54:26 PDT 2009	Success
Traffic Stream Metrics	Disabled	8 min.	Disabled	No	7 (days)	--	--
V5 Client Statistics	Enable	60 min.	Idle	Yes	31 (days)	Thu Apr 16 09:45:32 PDT 2009	Success

Other Background Tasks

Task	Enabled	Interval	Status	Last Execution Time	Last Execution Status
Client Status	Enable	5 min.	Idle	Thu Apr 16 09:44:35 PDT 2009	Success
Controller Configuration Backup	Disabled	1 day at 22:00	Disabled	--	--
Configuration Sync	Enable	1 day at 01:00	Idle	Thu Apr 16 01:00:49 PDT 2009	Success
Controller License Status	Enable	4 hour	Idle	Thu Apr 16 07:35:52 PDT 2009	Success
Data Cleanup	Enable	1 day at 01:00	Idle	Thu Apr 16 01:01:19 PDT 2009	Success
Device Status	Enable	5 min.	Idle	Thu Apr 16 09:45:54 PDT 2009	Success
Guest Accounts Sync	Enable	1 day at 01:00	Idle	Thu Apr 16 01:00:00 PDT 2009	Success
Mobility Service Backup	Disabled	7 day at 01:00	Disabled	--	--
Mobility Service Status	Enable	5 min.	Idle	Thu Apr 16 09:44:08 PDT 2009	Success
Mobility Service Synchronization	Enable	24 hour	Idle	Wed Apr 15 11:39:22 PDT 2009	Success
WCS Server Backup	Enable	7 day at 01:00	Idle	Wed Apr 15 01:04:19 PDT 2009	Success
Wireless Status	Enable	5 min.	Idle	Thu Apr 16 09:44:41 PDT 2009	Success

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

Step 3 Click **Mobility Service Synchronization**. The Mobility Service Synchronization page appears.

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

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

Note For a summary of out of sync alerts that are sent, refer to the "Out-of-Sync Alarms" section on page 13-8.

Step 5 To enable smart synchronization, select the **Smart Synchronization** 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.
- 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 days and the time of day (xx:yy AM or PM) 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 Assigment and Selection Scenarios, page 13-8.

Smart Controller Assigment 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 MSE. If that access point changes its controller from controller A to controller B, then controller B is automatically synchronized to the mobility services engine.

Scenario 4

Delete all access points of controller A from a floor that is assigned to a mobility services engine. The controller A will be auto unassigned for that mobility services engine.

Out-of-Sync Alarms

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

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

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

- Mobility services engine is deleted

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

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

Viewing Synchronization Information

This section describes how to view synchronization status and history.

Viewing Mobility Services Engine Synchronization Status

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

To view synchronization status, follow these steps:

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

Step 2 Select 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 see the synchronization status of the floor to the mobility services engine on the Floor View page.

To access this page, go to **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 side there is a menu option called 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.

Step 2 Table 13-1 lists and describes the text boxes that appear in the Synchronization History page.

Table 13-1 Synchronization History

Text Box	Description
Timestamp	The date and time at which the synchronization has happened.
Server	The mobility services engine server.
Element Name	The name of the element that was synchronized.
Type	The type of the element that was synchronized.
Sync Operation	The sync operation that was performed. It could either be an Update or an Add or Delete.
Generated By	The method of synchronization. It could either be Manual or Automatic.
Status	The status of the synchronization. It could be either Success or Failed.
Message	Any additional message about the synchronization.

Click the column headers to sort the entries.

Adding and Deleting Event Groups

You can add and delete event groups. Event groups help you organize your event definitions.

Adding Event Groups

To add an event group, follow these steps:

Step 1 Click **Services > Context Aware Notifications**.

Step 2 Click **Notification Settings** from the left sidebar menu.

Step 3 From the Select a command drop-down list, click **Add Event Group**, and 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 Click **Services > Context Aware Notifications**.

Step 2 Click **Notification Settings** from the left sidebar menu.

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

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

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

Step 6 Click **Save**.

Adding 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.

Cisco WCS enables you to add definitions for each group. An event definition must belong to a group. See the *Cisco Content-Aware Software Configuration Guide* for information on deleting or testing event definitions.

To add an event definition, follow these steps:

Step 1 Choose **Services > Context Aware Notifications**.

Step 2 Click **Notification Settings** from the left sidebar menu.

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

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

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

Tip For example, to keep track of heart monitors in a hospital, you could add rules to generate event notifications when a heart monitor is missing for one hour, a heart monitor moves off its assigned floor, or a heart monitor enters a specific coverage area within a floor.

To add a condition, follow these steps:

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

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

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

   If you chose Missing from the Condition Type drop-down list, enter the number of minutes after which a missing asset event is generated. For example, if you enter 10 in this text box, the mobility service engine generates a missing asset event if the mobility service engine has not found the asset for more than 10 minutes. Proceed to Step c.

If you chose In/Out from the Condition Type drop-down list, select **Inside of** or **Outside of**, then select **Select Area** to select the area to monitor for assets going into it or out of it. In the Select dialog box, choose the area to monitor, then click **Select**. The area to monitor could be an entire campus, building within a campus, a floor in a building, or a coverage area (you can define a coverage area using the map editor). For example, to monitor part of a floor in a building, choose a campus from the Campus drop-down 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 that will trigger an event notification if the monitored asset moves beyond the specified distance from a designated marker, then click **Select Marker**. In the Select dialog box, select the campus, building, floor, and marker from the corresponding drop-down list 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 more 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, check the box next to the battery level (low, medium, normal) that will trigger an event. Proceed to Step c.

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

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

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

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

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

Some examples of asset matching criteria that you can specify:

- If you choose **MAC Address** from the Match By drop-down list, choose **Equals** from the Operator drop-down list, and enter a MAC address (for example 12:12:12:12:12:12), the event condition applies to the element whose MAC address is 12:12:12:12:12:12 (exact match).
- If you choose **MAC Address** from the Match By drop-down, choose **Like** from the Operator drop-down list, and enter **12:12**, the event condition applies to elements whose MAC address starts with 12:12.

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

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

To select a chokepoint, do the following:

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

You are returned to the Add/Edit Condition page, and the location path (Campus > Building > Floor) for the chokepoint auto-populates the field next to the Select Checkpoint button.

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

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

b. Click **Add New**.

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

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

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

e. Select **XML** or **Plain Text** to specify the message format.

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

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

  If you choose SOAP, specify whether to send notifications over HTTPS by checking its corresponding check box. If you do not, HTTP is used. Also, enter the destination port number in the Port Number text box.

- Mail—Use this option to send notifications via e-mail.

  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, e-mail address of recipient, and a port number if necessary.

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

  If you choose SNMP, enter the SNMP community string in the SNMP Community 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 of the destination system in the Port Number text box.

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

Port Number auto-populates.

h. Click **Save**.

Step 7 At the General tab, follow these steps:

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

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

Note An event notification with high priority is serviced before event definitions with lower priority.

c. To select how often the event notifications are sent:

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 fields appear for the selection. Proceed to Step d.

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

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

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

g. Click **Save**.

Step 8 Verify that the new event notification is listed for the event group (Mobility > Notifications > Settings > Event Group Name).

Planning for and Configuring Context-Aware Software

Context-Aware Software (CAS) resides on the mobility services engine. For more information on the CAS service, refer to the *Cisco Context-Aware Software Configuration Guide.*

Note If you have a location server, you can track or map non-Cisco CX tags.

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

Chapter 4 of the *Cisco Conxtext-Aware Software Configuration Guide* contains the following information on configuring and viewing system properties on the mobility services engine:

- Configuring general properties
- Modifying NMSP parameters
- Viewing active sessions on a system
- Adding and deleting trap destinations
- Viewing and configuring advanced parameters

Chapter 5 of the *Cisco Context-Aware Software Configuration Guide* contains information on configuring and managing users and groups on the mobility services engine.

Chapter 6 of the *Cisco Context-Aware Software Configuration Guide* contains the following information on event notifications:

- Adding and deleting event groups
- Adding, deleting, and testing event definitions
- Viewing event notification summary
- Notifications cleared
- Notification message formats

Chapter 7 of the *Cisco Context-Aware Software Configuration Guide* contains the following information on the tools and configurations that can be used to enhance the location accuracy of elements (clients, tags, rogue clients, interferers and rogue access points):

- Planning for data, voice, and location deployment
- Creating and applying calibration models
- Inspecting location readiness and quality
- Inspecting location quality using calibration data
- Verifying location accuracy
- Using chokepoints to enhance tag location reporting
- Using Wi-Fi TDOA receiver to enhance tag location reporting
- Using tracking optimized monitor mode to enhance tag location reporting
- Defining inclusion and exclusion regions on a floor
- Defining a rail line on a floor
- Modifying context aware software parameters
- Enabling Location Services on Wired Switches and Wired Clients.
- Assigning a Catalyst Switch to Mobility Services Engine and Synchronizing

Chapter 8 of the *Cisco Context-Aware Software Configuration Guide* contains the following information on how to monitor the mobility services engine by configuring and viewing alarms, events, and logs and how to generate reports on system utilization and element counts:

- Working with alarms
- Working with events
- Working with logs
- Generating reports
- Monitoring wireless clients
- Monitoring tagged assets
- Monitoring chokepoints
- Monitoring Wi-Fi TDOA receivers
- Monitoring Wired Switches
- Monitoring Wired Clients
- Monitoring Interferers

Chapter 9 of the *Cisco Context-Aware Software Configuration Guide* contains the following information on backing up and restoring mobility services engine data and updating the mobility services engine software:

- Recovering a lost password
- Recovering a lost root password
- Backing up and restoring mobility services engine data
- Downloading software to mobility services engines
- Configuring the NTP server
- Defragmenting the mobility services engine database
- Rebooting the mobility services engine hardware
- Shutting down the mobility services engine hardware
- Clearing mobility services engine configurations

wIPS Planning and Configuring

With a fully integrated solution, Cisco can continually monitor wireless traffic on both the wired and wireless networks and can use that network intelligence to analyze attacks from many different sources of information to more accurately pinpoint and proactively prevent attacks versus waiting until damage or exposure has occurred. See *Cisco Adaptive Wireless IPS* documentation for the following information:

- WCS and wIPS integration overview
- Mobility services engines
- wIPS profiles
- Configuring SSID group list
- Viewing wIPS alarms
- Viewing wIPS events
- Configuring access points and access point templates
- policy alarm encyclopedia
- WCS security vulnerability assessment
- Rogue management
- Radio resource management