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, 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

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

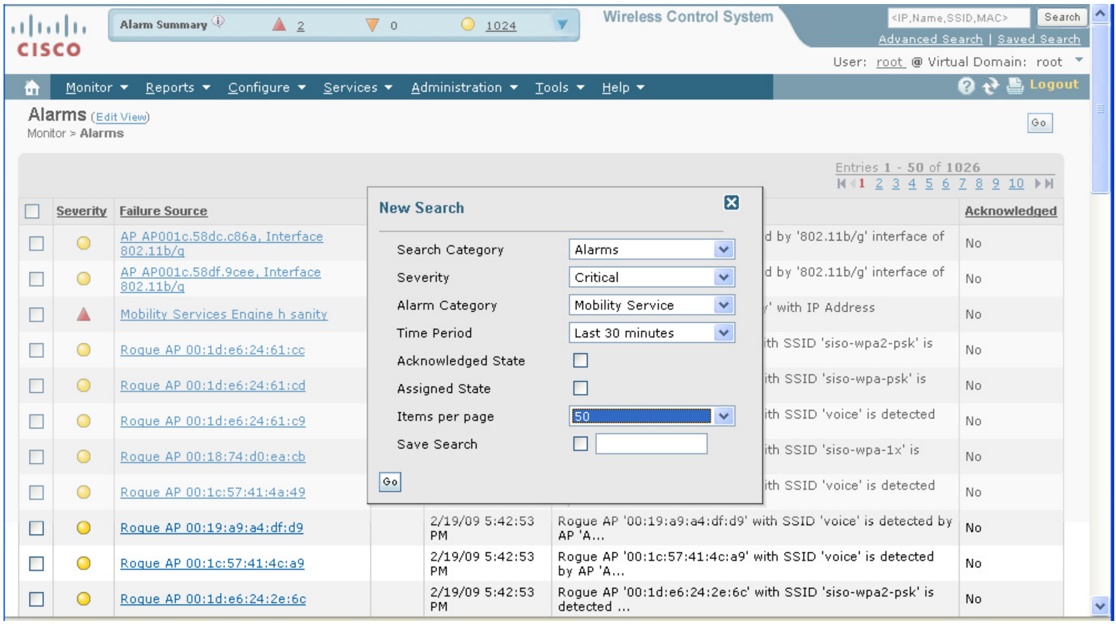
Viewing Alarms

To view mobility services engine alarms, follow these steps:

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

Step 2 Click the **Advanced Search** link in the navigation bar (top-right). A configurable search panel for alarms appears (see Figure 8-1).

Figure 8-1 Advanced Search Alarm Panel



New Search

Search Category	Alarms
Severity	Critical
Alarm Category	Mobility Service
Time Period	Last 30 minutes
Acknowledged State	□
Assigned State	□
Items per page	50
Save Search	□

Go

□	Severity	Failure Source			Acknowledged
□	●	AP AP001c.58dc.c86a, Interface 802.11b/g		d by '802.11b/g' interface of	No
□	●	AP AP001c.58df.9cee, Interface 802.11b/g		d by '802.11b/g' interface of	No
□	▲	Mobility Services Engine h sanity		' with IP Address	No
□	●	Rogue AP 00:1d:e6:24:61:cc		ith SSID 'siso-wpa2-psk' is	No
□	●	Rogue AP 00:1d:e6:24:61:cd		ith SSID 'siso-wpa-psk' is	No
□	●	Rogue AP 00:1d:e6:24:61:c9		ith SSID 'voice' is detected	No
□	●	Rogue AP 00:18:74:d0:ea:cb		ith SSID 'siso-wpa-1x' is	No
□	●	Rogue AP 00:1c:57:41:4a:49		ith SSID 'voice' is detected	No
□	●	Rogue AP 00:19:a9:a4:df:d9	2/19/09 5:42:53 PM	Rogue AP '00:19:a9:a4:df:d9' with SSID 'voice' is detected by AP 'A...	No
□	●	Rogue AP 00:1c:57:41:4c:a9	2/19/09 5:42:53 PM	Rogue AP '00:1c:57:41:4c:a9' with SSID 'voice' is detected by AP 'A...	No
□	●	Rogue AP 00:1d:e6:24:2e:6c	2/19/09 5:42:53 PM	Rogue AP '00:1d:e6:24:2e:6c' with SSID 'siso-wpa2-psk' is detected ...	No

Step 3 Select **Alarms** as the Search Category.

Step 4 Select the Severity of Alarms to display. Options are All Severities, Critical, Major, Minor, Warning or Clear.

Step 5 Select **Mobility Service** from the Alarm Category.

Step 6 Select the time frame for which you want to review alarms from the Time Period drop-down menu.

Options range from minutes (5, 15, and 30) to hours (1 and 8) to days (1 and 7). To display all, select **Any time**.

Step 7 Check the **Acknowledged State** check box to exclude the acknowledged alarms and their count from the Alarm Summary window.

Step 8 Check the **Assigned Stat**e check box to exclude the assigned alarms and their count from the Alarm Summary window.

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

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

Note You can initiate the search thereafter, by clicking the Saved Searches link at the top-right of the navigation bar.

Step 11 Click **Go**. The alarms summary panel 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 Display the Alarms window as described in the "Viewing Alarms" section on page 8-2.

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

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

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

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

Step 2 Select the alarms that you want to delete or clear by checking their corresponding check boxes.

Step 3 From the Select a command drop-down menu, 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.

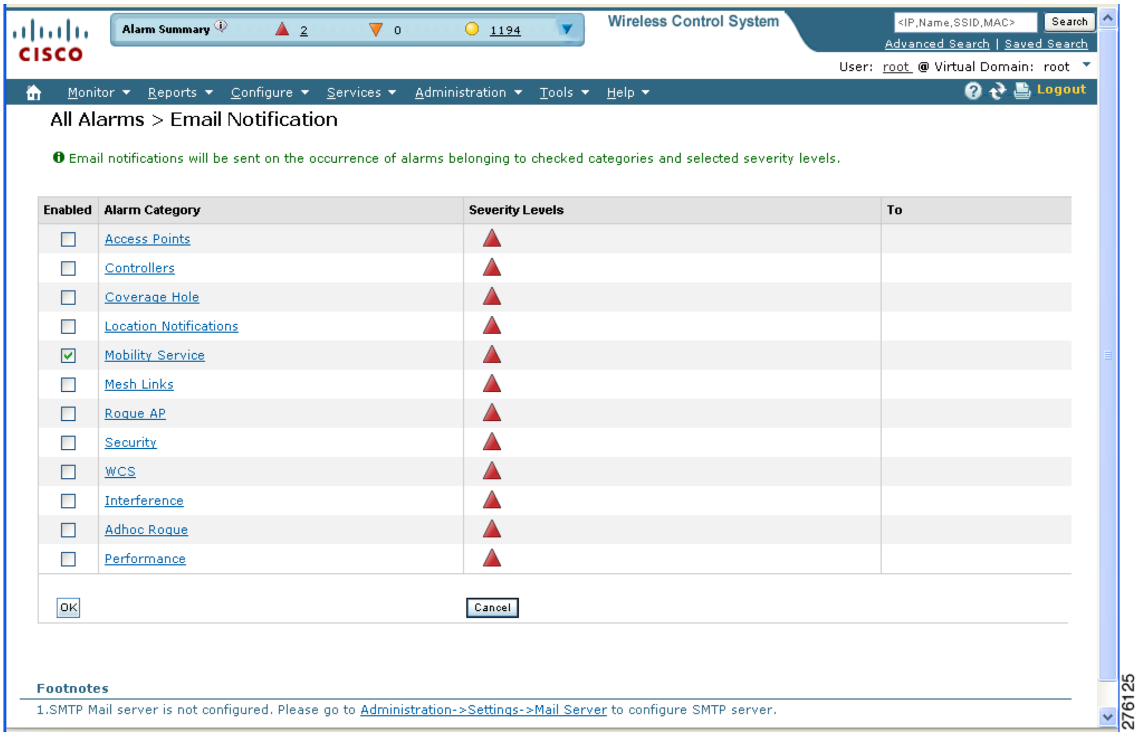
You can choose the alarm severity types (critical, major, minor, and warning) to have emailed to you.

To send alarm notifications, follow these steps:

Step 1 Choose **Monitor > Alarms**.

Step 2 From the Select a command drop-down menu, choose **Email Notification**. Click **Go**. The Email Notification window appears (see Figure 8-2).

Figure 8-2 All Alarms > Email Notification Window



All Alarms > Email Notification

Email notifications will be sent on the occurrence of alarms belonging to checked categories and selected severity levels.

Enabled	Alarm Category	Severity Levels	To
□	Access Points	▲	
□	Controllers	▲	
□	Coverage Hole	▲	
□	Location Notifications	▲	
☑	Mobility Service	▲	
□	Mesh Links	▲	
□	Rogue AP	▲	
□	Security	▲	
□	WCS	▲	
□	Interference	▲	
□	Adhoc Rogue	▲	
□	Performance	▲	

OK Cancel

Footnotes

1.SMTP Mail server is not configured. Please go to Administration->Settings->Mail Server to configure SMTP server.

Note A 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 select the **Administration > Settings > Mail Server** link, if it is displayed at the bottom of the All Alarms > Email Notification Window noted above.

Step 3 Click the **Enabled** check box next to **Mobility Service**.

Note Enabling the **Mobility Service** alarm category sends all alarms related to mobility services engine and the location appliance to the defined email address.

Step 4 Click the **Mobility Service** link. The window for configuring the alarm severity types that are reported for the mobility services engine appears.

Step 5 Check the check box next to all the alarm severity types for which you want email notifications sent.

Step 6 In the To field, enter the email address or addresses to which you want the email notifications sent. Separate Email addresses by commas.

Step 7 Click **OK**.

You are returned to the Alarms > Notification window. The changes to the reported alarm severity levels and the recipient email address for email notifications are displayed.

Working with Events

You can use Cisco WCS to view mobility services engine and location notification events. You can search and display events based on their severity (critical, major, minor, warning, clear, and info) and event category.

You can search by the following event categories:

- By network coverage: coverage holes and interference
- By link: mesh links
- By notifications: location notifications
- By product type: access points (rogue and non-rogue), clients, controllers, or mobility service
- By security

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

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

To display events, follow these steps:

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

Step 2 In the Events window:

- If you want to display the events for a specific element, and you know its IP address, name, WLAN SSID, or MAC address, enter that value in the Search field of the navigation bar (top-right). Click **Search.**
- To display events by severity and category, click **Advanced Search** in the navigation bar and select the appropriate options from the Severity and Event Category drop-down menus. 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.

Configuring Logging Options

You can use Cisco WCS to specify the logging level and types of messages to log.

To configure logging options, follow these steps:

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

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

Step 3 Choose **System > Advanced**. The advanced parameters for the selected mobility services engine appear.

Step 4 Scroll down to the Logging Options section and choose the appropriate option (off, error, information, or trace) from the Logging Level drop-down menu.

Caution Use **Error** and **Trace** only when directed to do so by Cisco Technical Assistance Center (TAC) personnel.

Step 5 Check the **Enabled** check box next to each element listed in that section to begin logging its events.

Step 6 Click **Save**.

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:

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

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

Step 3 Choose **System > Logs**.

Step 4 Click **Download Logs**.

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

Generating Reports

In Cisco WCS, you can generate a 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
- Chart 2 summarizes and graphs client count, tag count, rogue client count, rogue access point count, and ad hoc rogue count

Creating a Device Utilization Report

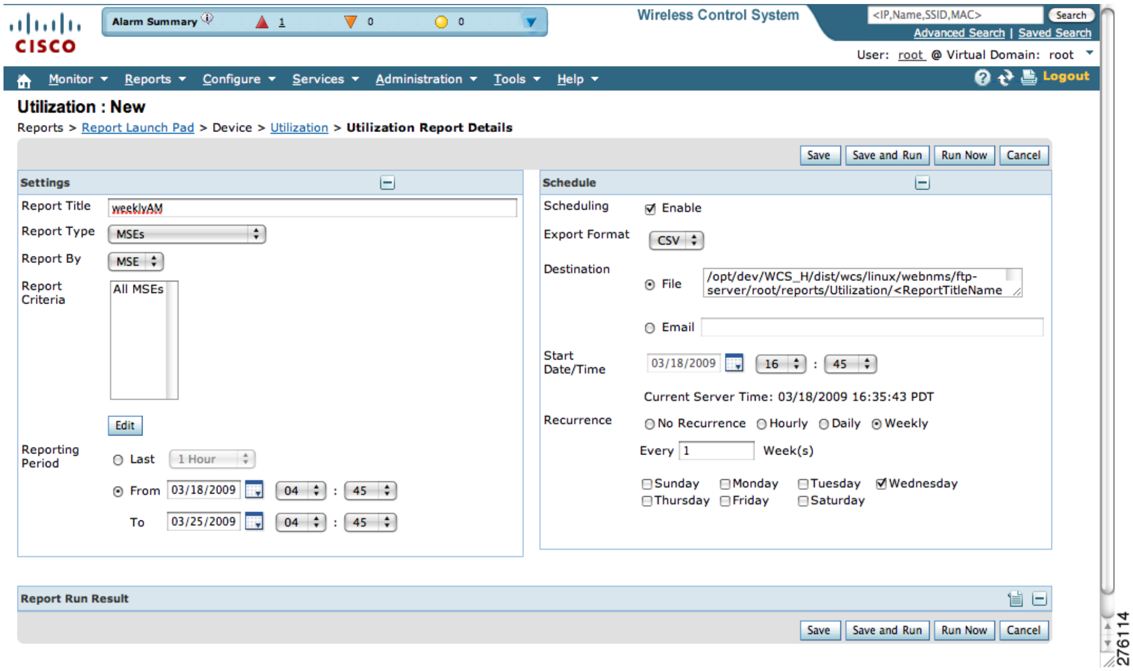
To create a device utilization report for the mobility services engine, follow these steps:

Step 1 In Cisco WCS, choose **Reports > Report Launch Pad**.

Step 2 Choose **Device > Utilization**.

Step 3 Click **New**. The Utilization: New window appears (see Figure 8-3).

Figure 8-3 Device > Utilization Window



User: root @ Virtual Domain: root

Utilization : New

Reports > Report Launch Pad > Device > Utilization > Utilization Report Details

Settings

Report Title: weeklyAM
Report Type: MSEs
Report By: MSE
Report Criteria: All MSEs
Reporting Period: ○ Last 1 Hour
● From 03/18/2009 04 : 45
To 03/25/2009 04 : 45

Schedule

Scheduling: ☑ Enable
Export Format: CSV
Destination: ● File /opt/dev/WCS_H/dist/wcs/linux/webnms/ftp-server/root/reports/Utilization/<ReportTitleName
○ Email
Start Date/Time: 03/18/2009 16 : 45
Current Server Time: 03/18/2009 16:35:43 PDT
Recurrence: ○ No Recurrence ○ Hourly ○ Daily ● Weekly
Every 1 Week(s)
□ Sunday □ Monday □ Tuesday ☑ Wednesday
□ Thursday □ Friday □ Saturday

Step 4 In the Settings panel (left), enter a report title.

Step 5 The Report Type and Report By selections are always MSE.

Step 6 Click **Edit** to select either a specific mobility services engine or **All MSEs** from the pop-up panel that appears.

Step 7 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.

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 panel (right), check the **Enable Schedule** check box.

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

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

- If you select the File option, a destination path must first be defined at the **Administration > Settings** > *Report* window. Enter the destination path for the files in the Repository Path field.
- If you select the Email option, an SMTP Mail Server must be defined prior to entry of target email address. Choose **Administrator > Settings >** *Mail Server Configuration* to enter the appropriate information.

Step 11 Enter a start date (MM:DD:YYYY) or click the calendar icon to select a date.

Step 12 Specify a start time using the hour and minute drop-down menus.

Step 13 Click one of 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:

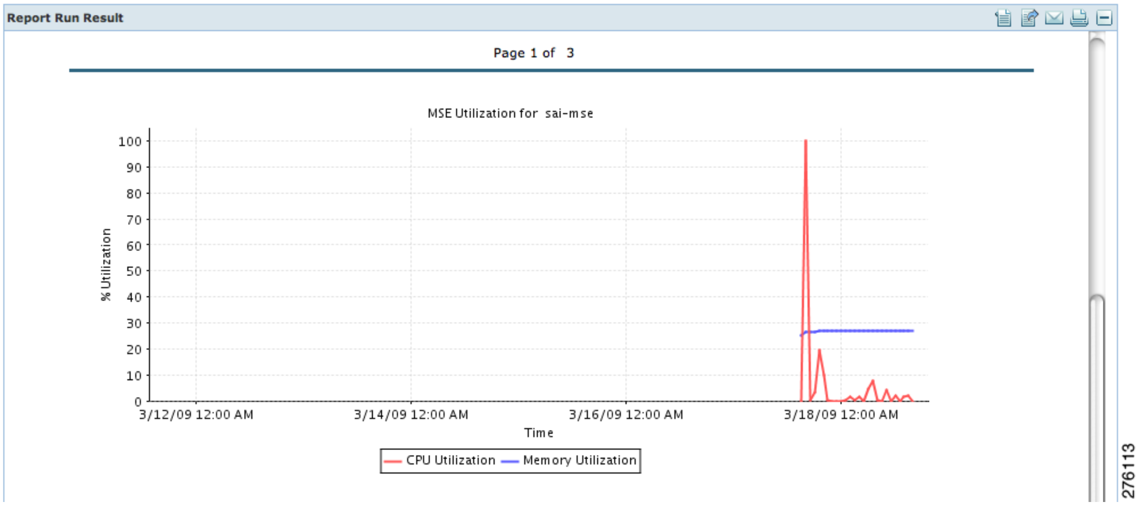
- Click **Save** to save edits. The report is run at the designated time and the results are either emailed or saved to a designated file as defined in the Schedule panel.
- Click **Save and Run** to save the changes and run the report now. The report runs regardless of any pending, scheduled run of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

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

The results appear at the bottom of the window (see Figure 8-4).

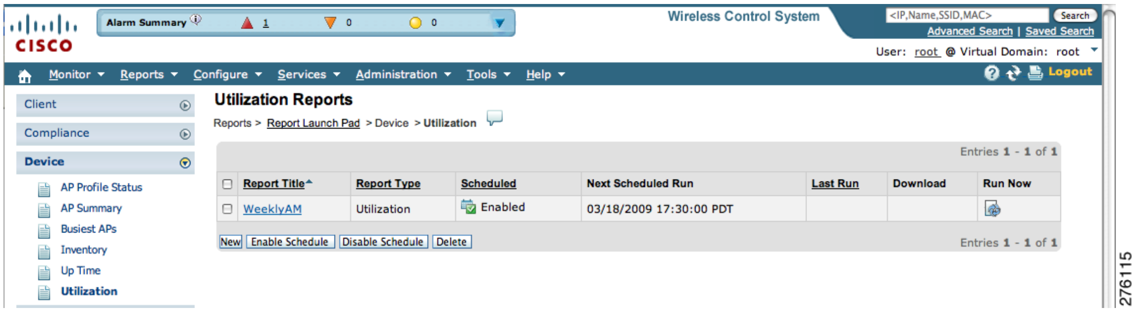
Note Only the CPU and memory utilization reports as shown in the example below (see Figure 8-4).

Figure 8-4 Devise > MSE Utilization > Results



Step 15 If you selected the Save or Save and Run option, click either **Reports > Saved Reports** (or **Reports > Scheduled Runs** if it has not yet run and is scheduled to run). The Utilization Reports summary window appears (see Figure 8-5).

Figure 8-5 Utilization Reports Summary Window



Utilization Reports

Reports > Report Launch Pad > Device > Utilization

Entries 1 - 1 of 1

☐	Report Title	Report Type	Scheduled	Next Scheduled Run	Last Run	Download	Run Now
☐	WeeklyAM	Utilization	Enabled	03/18/2009 17:30:00 PDT			

New | Enable Schedule | Disable Schedule | Delete

Entries 1 - 1 of 1

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

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

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

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

Monitoring Wireless Clients Using Maps

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

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

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

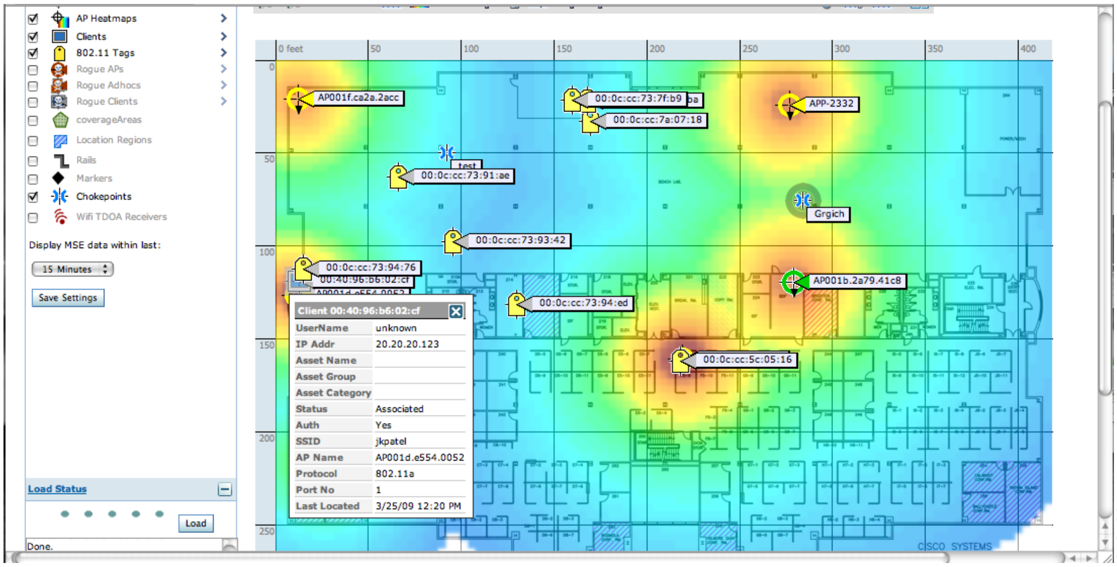
Step 1 In Cisco WCS, choose **Monitor > Maps**.

Step 2 Choose the building and floor on which the mobility services engine and its clients are located.

Step 3 Check the **Clients** check box in the Floor Settings panel (left), if it is not already checked (see Figure 8-6).

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

Figure 8-6 Monitor > Maps > Building > Floor Window



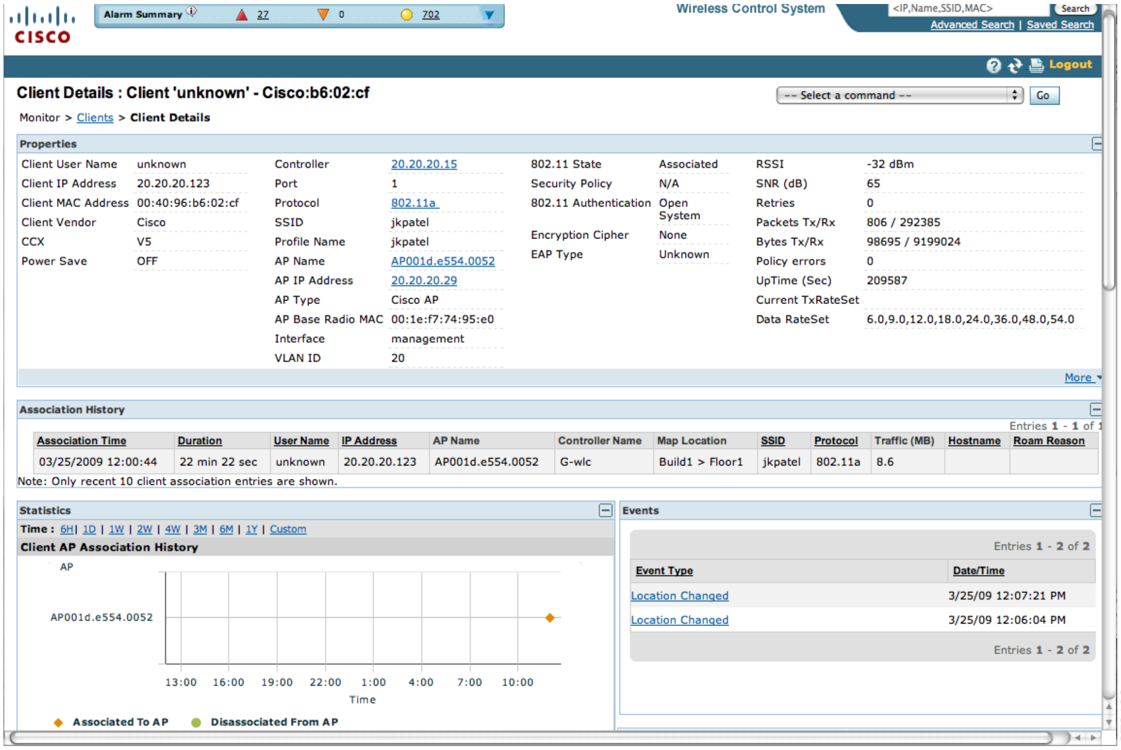
Client 00:40:96:b6:02:cf

UserName	unknown
IP Addr	20.20.20.123
Asset Name	
Asset Group	
Asset Category	
Status	Associated
Auth	Yes
SSID	jkpatel
AP Name	AP001d.e554.0052
Protocol	802.11a
Port No	1
Last Located	3/25/09 12:20 PM

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

Step 5 Click the client icon to see client details (see Figure 8-7 and Figure 8-8).

Figure 8-7 Client Details Window (1 of 2)



Client Details : Client 'unknown' - Cisco:b6:02:cf

Monitor > Clients > Client Details

Properties

Client User Name	unknown	Controller	20.20.20.15	802.11 State	Associated	RSSI	-32 dBm
Client IP Address	20.20.20.123	Port	1	Security Policy	N/A	SNR (dB)	65
Client MAC Address	00:40:96:b6:02:cf	Protocol	802.11a	802.11 Authentication	Open System	Retries	0
Client Vendor	Cisco	SSID	jkpatel	Encryption Cipher	None	Packets Tx/Rx	806 / 292385
CCX	V5	Profile Name	jkpatel	EAP Type	Unknown	Bytes Tx/Rx	98695 / 9199024
Power Save	OFF	AP Name	AP001d.e554.0052			Policy errors	0
		AP IP Address	20.20.20.29			UpTime (Sec)	209587
		AP Type	Cisco AP			Current TxRateSet	
		AP Base Radio MAC	00:1e:f7:74:95:e0			Data RateSet	6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0
		Interface	management				
		VLAN ID	20				

Association History

Entries 1 - 1 of 1

Association Time	Duration	User Name	IP Address	AP Name	Controller Name	Map Location	SSID	Protocol	Traffic (MB)	Hostname	Roam Reason
03/25/2009 12:00:44	22 min 22 sec	unknown	20.20.20.123	AP001d.e554.0052	G-wlc	Build1 > Floor1	jkpatel	802.11a	8.6		

Note: Only recent 10 client association entries are shown.

Statistics

Time : 6H | 1D | 1W | 2W | 4W | 3M | 6M | 1Y | Custom

Client AP Association History

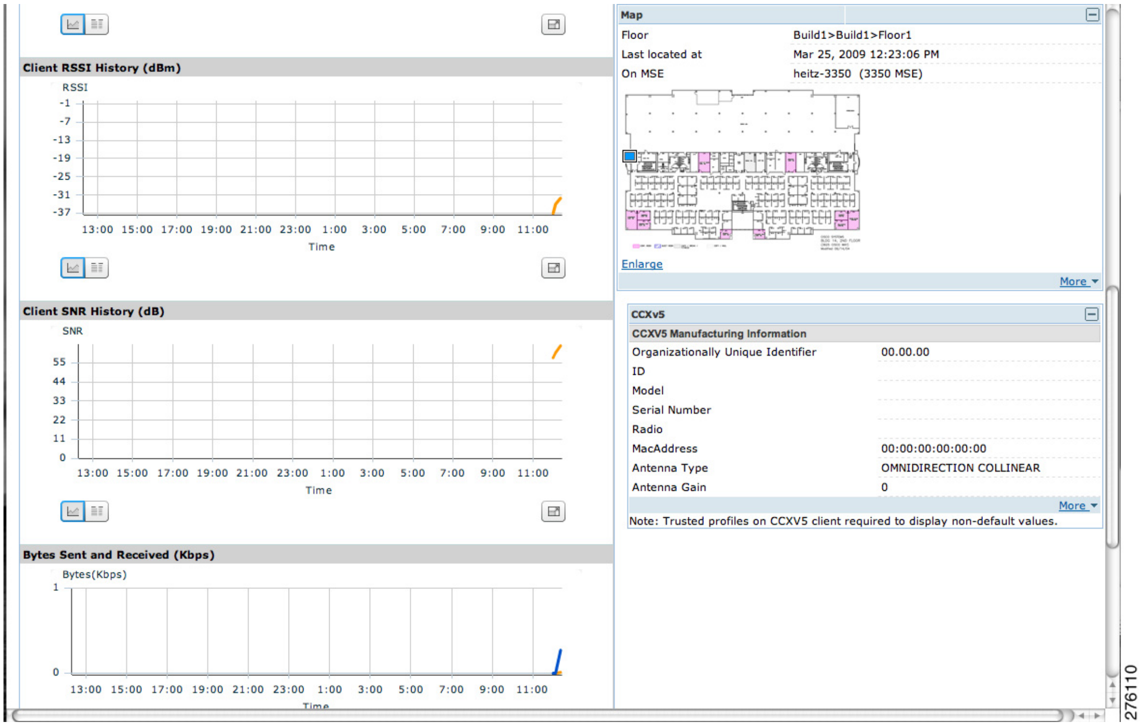
Events

Entries 1 - 2 of 2

Event Type	Date/Time
Location Changed	3/25/09 12:07:21 PM
Location Changed	3/25/09 12:06:04 PM

Entries 1 - 2 of 2

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



Map

Floor	Build1>Build1>Floor1
Last located at	Mar 25, 2009 12:23:06 PM
On MSE	heitz-3350 (3350 MSE)

CCXv5

CCXV5 Manufacturing Information

Organizationally Unique Identifier	00.00.00
ID	
Model	
Serial Number	
Radio	
MacAddress	00:00:00:00:00:00
Antenna Type	OMNIDIRECTION COLLINEAR
Antenna Gain	0

More

Note: Trusted profiles on CCXV5 client required to display non-default values.

Monitoring Wireless Clients Using Search

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

To view client information, follow these steps:

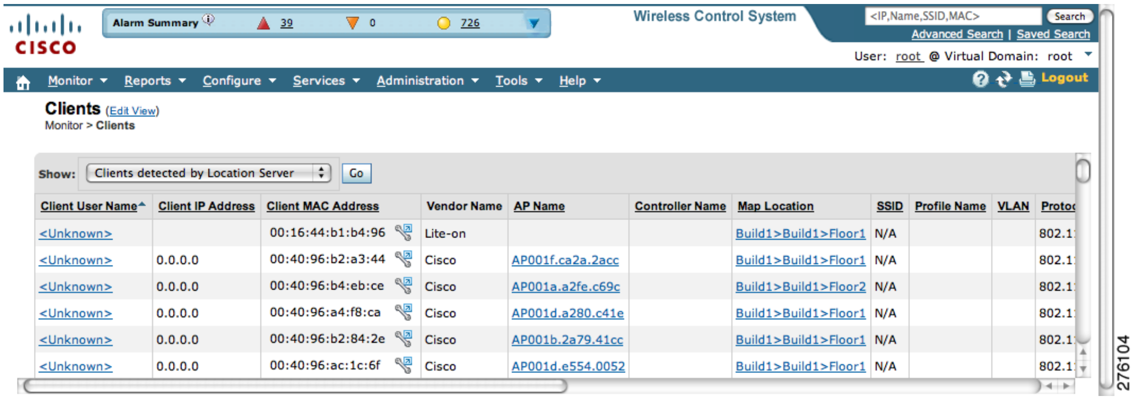
Step 1 In Cisco WCS, choose **Monitor > Clients**.

The Clients summary window appears.

Step 2 Select **Clients Detected by MSEs** from the Show drop-down menu. Click **Go**.

A summary of all clients detected by all mobility services engines and location appliances managed by Cisco WCS displays (see Figure 8-9).

Figure 8-9 Monitor > Clients Window



Clients (Edit View)
Monitor > Clients

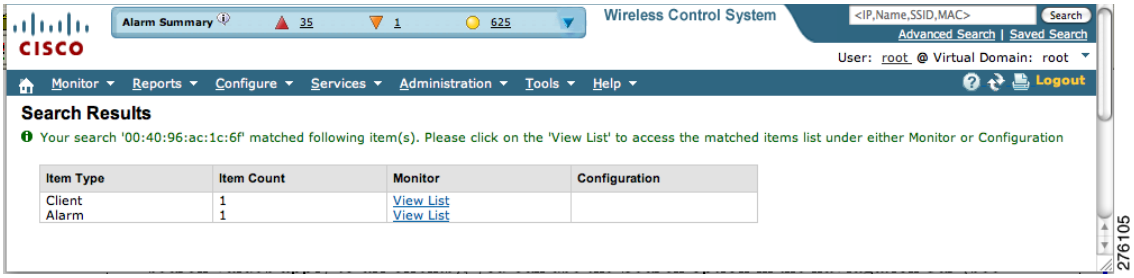
Show: Clients detected by Location Server Go

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

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

For example, if you enter a MAC address in the search field, the following window appears (see Figure 8-10).

Figure 8-10 Search by MAC address Results



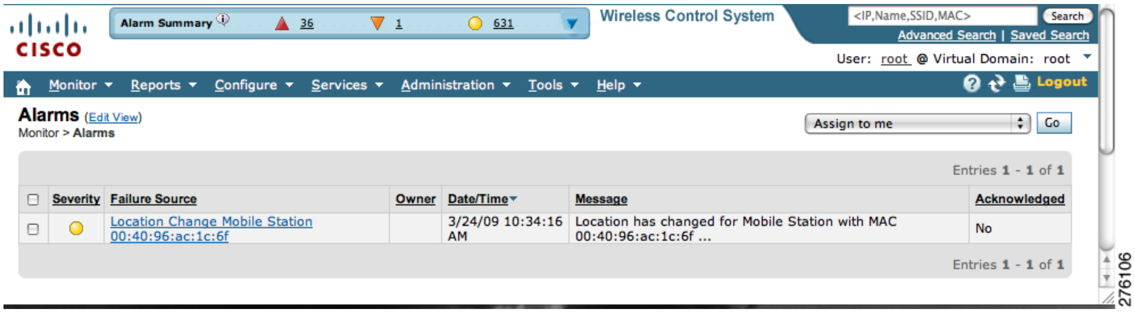
Search Results

Your search '00:40:96:ac:1c:6f' matched following item(s). Please click on the 'View List' to access the matched items list under either Monitor or Configuration

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

1. 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.
2. 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).

Figure 8-11 Alarm Summary for Client



Alarms (Edit View)
Monitor > Alarms

Assign to me Go

Entries 1 - 1 of 1

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

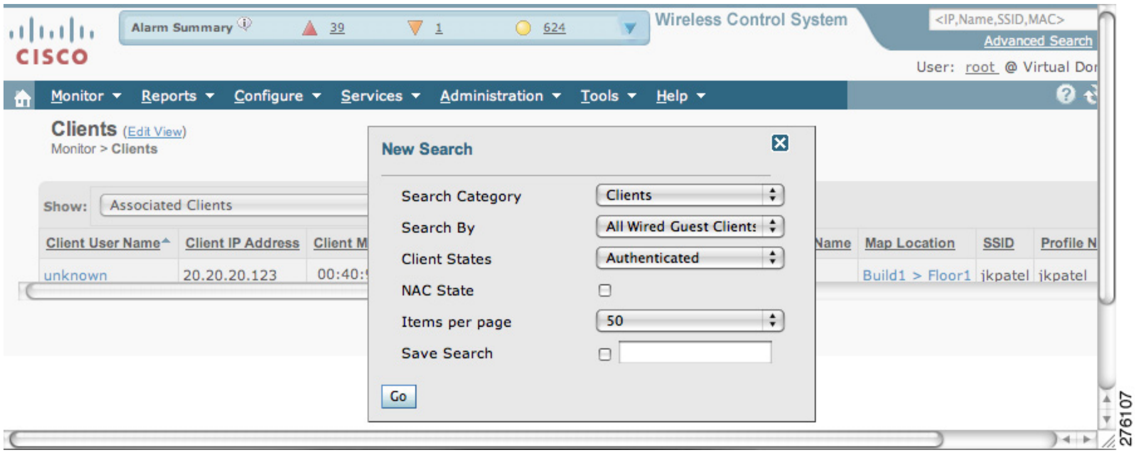
Entries 1 - 1 of 1

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

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

You can further define the client category by: all clients, all excluded clients, all wired guest clients, and all logged in clients using the Search By drop-down menu (see Figure 8-12).

Figure 8-12 Advanced Search Window



New Search

Search Category: Clients

Search By: All Wired Guest Client:

Client States: Authenticated

NAC State ☐

Items per page: 50

Save Search ☐

Step 3 Click on the appropriate client.

Monitoring Tags

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

Monitoring Tags Using Maps

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

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

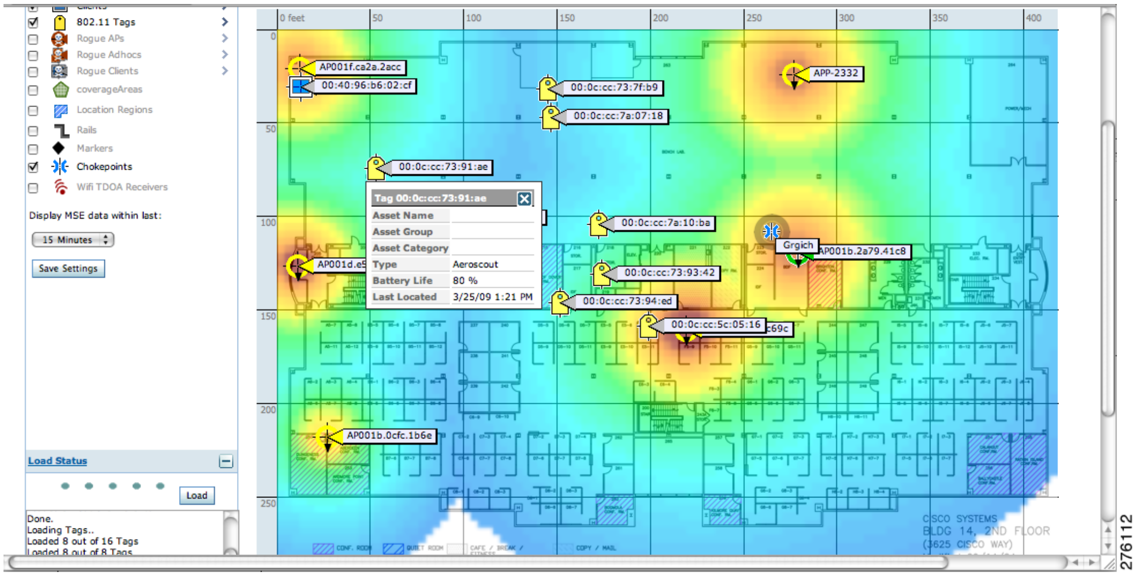
Step 1 In Cisco WCS, choose **Monitor > Maps**.

Step 2 Choose the building and floor on which the mobility services engine and tag are located.

Step 3 Check the **802.11 Tags** check box in the Floor Settings panel (left), if it is not already checked (see Figure 8-13).

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

Figure 8-13 Monitor > Maps > Building > Floor > Tag Window



- ☑ 802.11 Tags
- □ Rogue APs
- □ Rogue Adhocs
- □ Rogue Clients
- □ coverageAreas
- □ Location Regions
- □ Rails
- □ Markers
- ☑ Chokepoints
- □ Wifi TDOA Receivers

Display MSE data within last: 15 Minutes

Save Settings

Load Status

Load

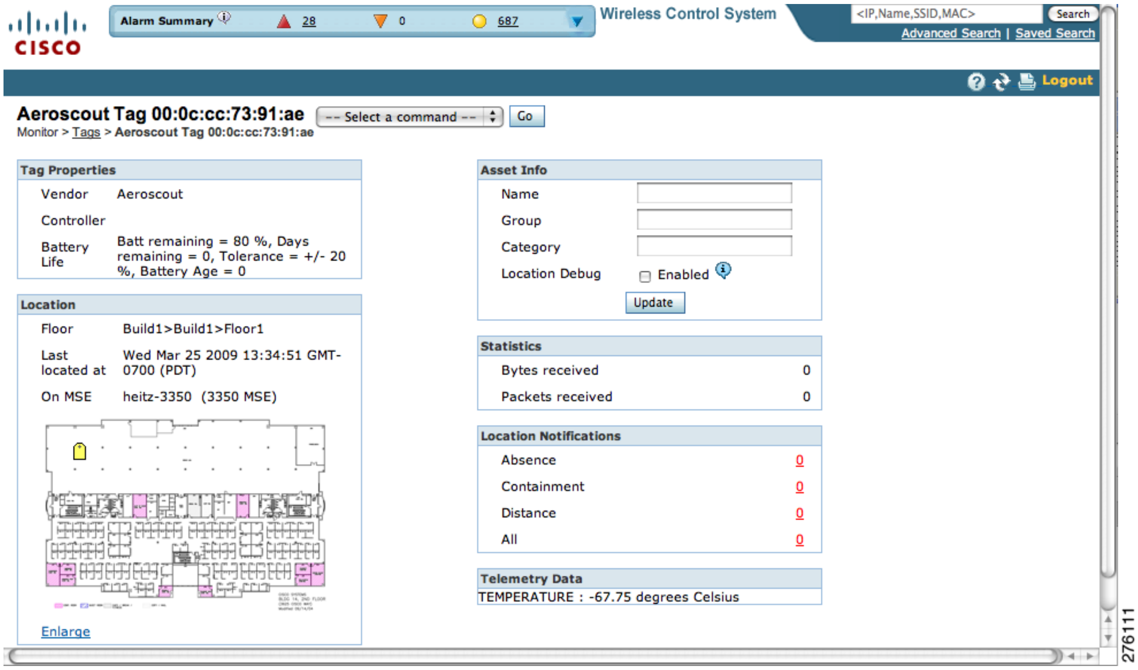
Done.
Loading Tags..
Loaded 8 out of 16 Tags
Loaded 8 out of 8 Tags

Tag 00:0c:cc:73:91:ae	
Asset Name	
Asset Group	
Asset Category	
Type	Aeroscout
Battery Life	80 %
Last Located	3/25/09 1:21 PM

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

Step 5 Click the tag icon to see tag details (see Figure 8-14).

Figure 8-14 Tag Details Window



Aeroscout Tag 00:0c:cc:73:91:ae -- Select a command -- Go

Monitor > Tags > Aeroscout Tag 00:0c:cc:73:91:ae

Tag Properties

Vendor	Aeroscout
Controller	
Battery Life	Batt remaining = 80 %, Days remaining = 0, Tolerance = +/- 20 %, Battery Age = 0

Location

Floor	Build1>Build1>Floor1
Last located at	Wed Mar 25 2009 13:34:51 GMT-0700 (PDT)
On MSE	heitz-3350 (3350 MSE)

Enlarge

Asset Info

Name	
Group	
Category	
Location Debug	□ Enabled

Update

Statistics

Bytes received	0
Packets received	0

Location Notifications

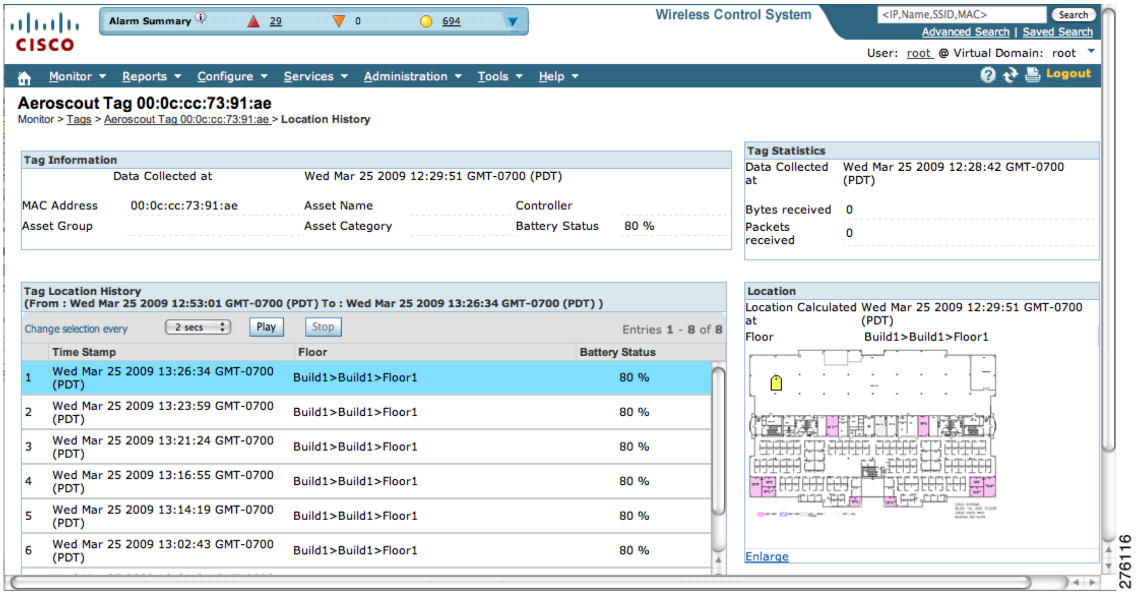
Absence	0
Containment	0
Distance	0
All	0

Telemetry Data

TEMPERATURE : -67.75 degrees Celsius

Step 6 To see location history for the tag, select **Location History** from the Select a command drop-down menu. Click **Go** (see Figure 8-15).

Figure 8-15 Tag Location History Window



Aeroscout Tag 00:0c:cc:73:91:ae

Monitor > Tags > Aeroscout Tag 00:0c:cc:73:91:ae > Location History

Tag Information

Data Collected at: Wed Mar 25 2009 12:29:51 GMT-0700 (PDT)

MAC Address	00:0c:cc:73:91:ae	Asset Name		Controller	
Asset Group		Asset Category		Battery Status	80 %

Tag Statistics

Data Collected at	Wed Mar 25 2009 12:28:42 GMT-0700 (PDT)
Bytes received	0
Packets received	0

Tag Location History
(From : Wed Mar 25 2009 12:53:01 GMT-0700 (PDT) To : Wed Mar 25 2009 13:26:34 GMT-0700 (PDT))

Change selection every 2 secs Play Stop Entries 1 - 8 of 8

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

Location

Location Calculated at	Wed Mar 25 2009 12:29:51 GMT-0700 (PDT)
Floor	Build1>Build1>Floor1

Monitoring Tags Using Search

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

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

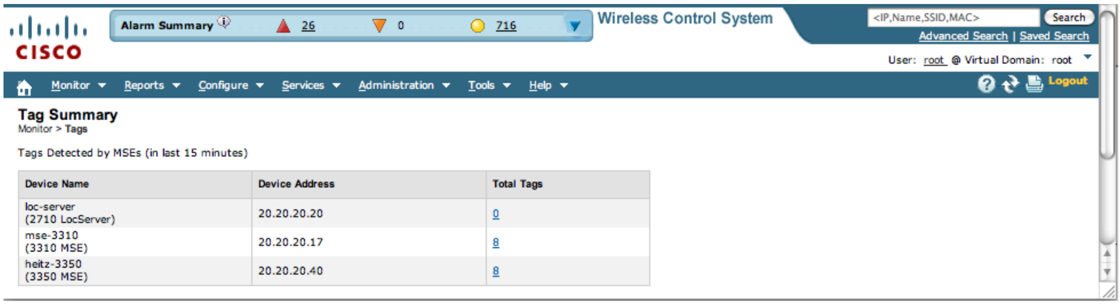
When you click on the MAC address of a tag location in a search results window, the following details appear for the tag:

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

To search for tags, follow these steps:

Step 1 Choose **Monitor > Tags**. The Tag Summary window appears (see Figure 8-16).

Figure 8-16 Monitor > Tags Window



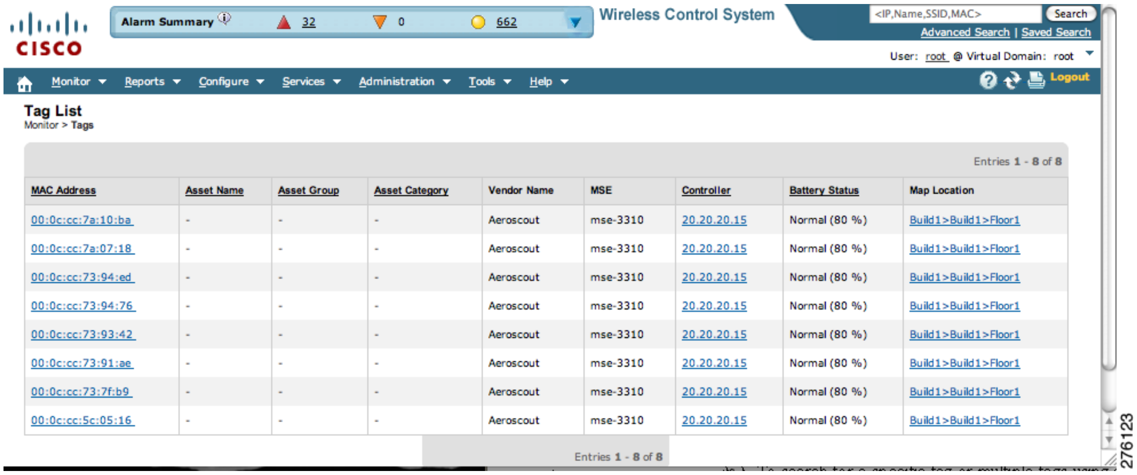
Tag Summary
Monitor > Tags

Tags Detected by MSEs (in last 15 minutes)

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

a. To view a summary of tags associated with a specific mobility services engine, click the **Total Tags** link (see Figure 8-17).

Figure 8-17 Total Tags Listing by Mobility Services Engine



Tag List
Monitor > Tags

Entries 1 - 8 of 8

MAC Address	Asset Name	Asset Group	Asset Category	Vendor Name	MSE	Controller	Battery Status	Map Location
00:0c:cc:7a:10:ba	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build1>Build1>Floor1
00:0c:cc:7a:07:18	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build1>Build1>Floor1
00:0c:cc:73:94:ed	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build1>Build1>Floor1
00:0c:cc:73:94:76	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build1>Build1>Floor1
00:0c:cc:73:93:42	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build1>Build1>Floor1
00:0c:cc:73:91:ae	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build1>Build1>Floor1
00:0c:cc:73:7f:b9	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build1>Build1>Floor1
00:0c:cc:5c:05:16	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build1>Build1>Floor1

Entries 1 - 8 of 8

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

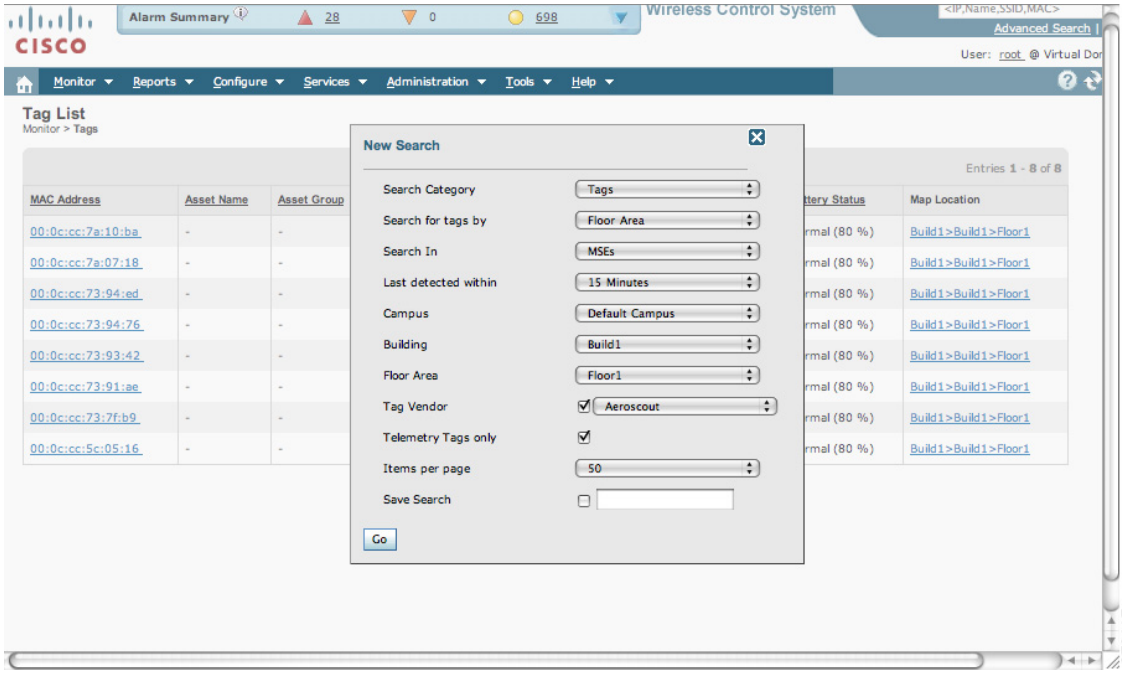
b. To search for a specific tag, if you know its MAC address, name or VLAN ID (not all search values apply to all tags) use **Search** which is found in the navigation bar.

c. To search for a specific tag or multiple tags using a broader range of search categories such as device (MSE or controller), map location (floor or outdoor area), asset name or category, or tag vendor use **Advanced Search** which is found in the navigation bar (see Figure 8-18).

1. In the Advanced Search panel, select **Tags** as the search category.
2. Select the additional tag search criteria. Refer to Table 8-1 for a list of search criteria and their possible values.
3. Click **Go** when all advanced search parameters are selected. 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.

Figure 8-18 Advanced Search Panel for Tags



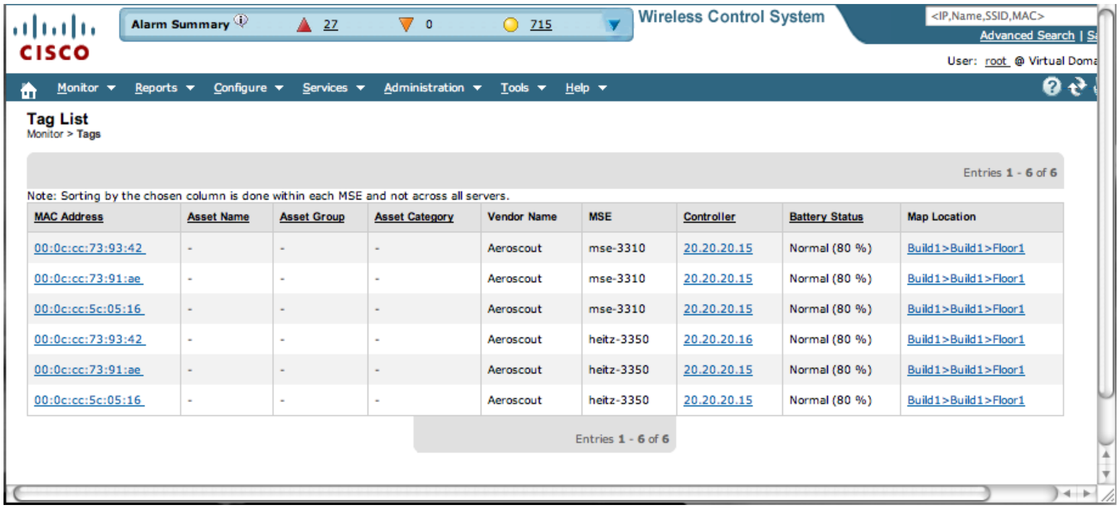
MAC Address	Asset Name	Asset Group	ttery Status	Map Location
00:0c:cc:7a:10:ba	-	-	rmal (80 %)	Build1>Build1>Floor1
00:0c:cc:7a:07:18	-	-	rmal (80 %)	Build1>Build1>Floor1
00:0c:cc:73:94:ed	-	-	rmal (80 %)	Build1>Build1>Floor1
00:0c:cc:73:94:76	-	-	rmal (80 %)	Build1>Build1>Floor1
00:0c:cc:73:93:42	-	-	rmal (80 %)	Build1>Build1>Floor1
00:0c:cc:73:91:ae	-	-	rmal (80 %)	Build1>Build1>Floor1
00:0c:cc:73:7f:b9	-	-	rmal (80 %)	Build1>Build1>Floor1
00:0c:cc:5c:05:16	-	-	rmal (80 %)	Build1>Build1>Floor1

New Search

Search Category	Tags
Search for tags by	Floor Area
Search In	MSEs
Last detected within	15 Minutes
Campus	Default Campus
Building	Build1
Floor Area	Floor1
Tag Vendor	☑ Aeroscout
Telemetry Tags only	☑
Items per page	50
Save Search	☐

Go

Figure 8-19 Advanced Search Results for Tag



Tag List
Monitor > Tags

Entries 1 - 6 of 6

Note: Sorting by the chosen column is done within each MSE and not across all servers.

MAC Address	Asset Name	Asset Group	Asset Category	Vendor Name	MSE	Controller	Battery Status	Map Location
00:0c:cc:73:93:42	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build1>Build1>Floor1
00:0c:cc:73:91:ae	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build1>Build1>Floor1
00:0c:cc:5c:05:16	-	-	-	Aeroscout	mse-3310	20.20.20.15	Normal (80 %)	Build1>Build1>Floor1
00:0c:cc:73:93:42	-	-	-	Aeroscout	heitz-3350	20.20.20.16	Normal (80 %)	Build1>Build1>Floor1
00:0c:cc:73:91:ae	-	-	-	Aeroscout	heitz-3350	20.20.20.15	Normal (80 %)	Build1>Build1>Floor1
00:0c:cc:5c:05:16	-	-	-	Aeroscout	heitz-3350	20.20.20.15	Normal (80 %)	Build1>Build1>Floor1

Entries 1 - 6 of 6

Note If you click the MAC address of any of these tags, a Tag details window appears similar to that in Figure 8-14.

Table 8-1 Tag Search Criteria and Values

Search Criteria	Variable Search Criteria	Possible Values
Search for tags by (Tier 1 search criteria)	—	All Tags; Asset Name, Asset Category or Asset Group; MAC Address; Controller or MSEs; Floor Area or Outdoor Area. **Note** MSE search includes both location servers and mobility services engines.
Search in (Tier 2 search criteria)	—	MSEs or WCS Controllers. **Note** WCS Controller option indicates that the search for controllers is done within WCS. **Note** MSE search includes both location servers and mobility services engines.
Last detected within	—	Options are from 5 minutes to 24 hours.
Variable search criteria. (Tier 3 search criteria) **Note** Possible search criteria determined by the **Search for tabs by** (Tier 1 search) value.	If **Search for tags by** value is: 1. Asset Name, then enter tag asset name. 2. Asset Category, then enter tag asset category. 3. Asset Group, then enter tag asset group. 4. MAC Address, then enter tag MAC address. 5. Controller, then select controller IP address. 6. MSEs, then select an MSE IP address from drop-down menu. 7. Floor Area, then choose campus, building, and floor area. 8. Outdoor Area, then choose campus and outdoor area.	
Telemetry tags only	—	Check box to display telemetry tags. Leaving option unchecked displays all tags. **Note** Option only seen when the Search In option is MSE. **Note** Only those vendor tags that support telemetry appear.
Tag vendor	—	Check box to select tag vendor from drop-down menu. **Note** Option only seen when the Search In option is MSE.
Items per page	—	Select the number of tags to display per search request. Values range from 10 to 500.
Save search	—	Check box to name and save search criteria. Once saved, entry appears under Saved Searches heading (left-panel).

Overlapping Tags

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

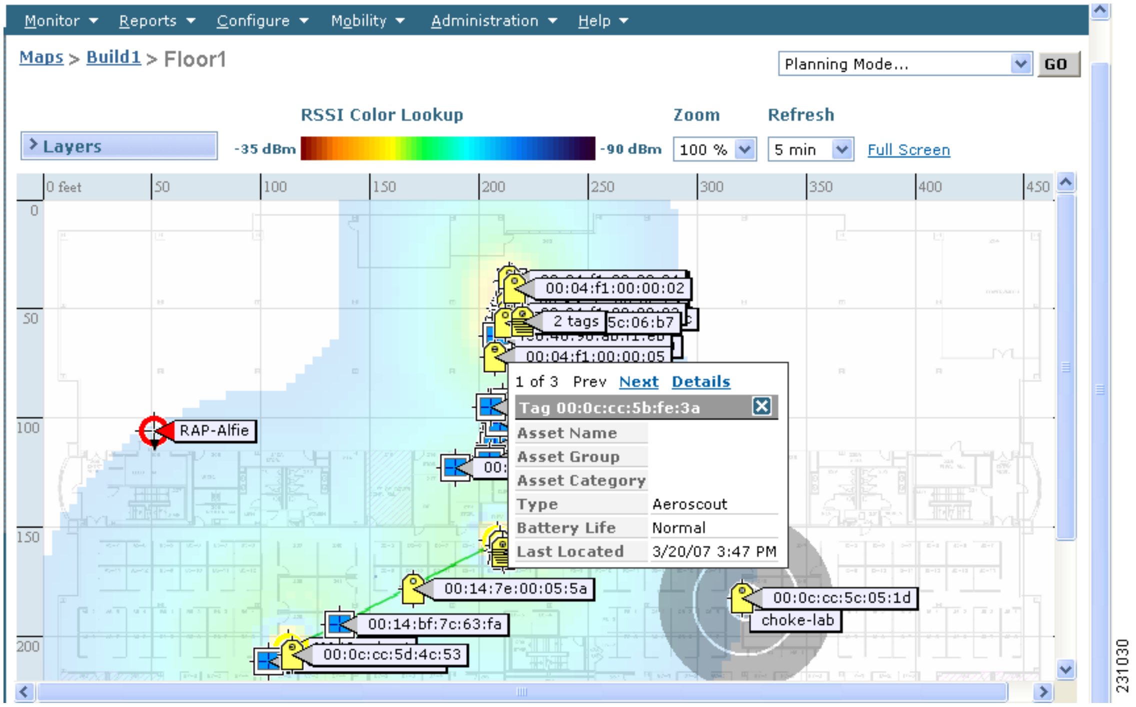
When you move the mouse over the overlapping tag on the map, a panel appears with summary information for the overlapping tags (see Figure 8-20).

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

Note

- Summary information for tags includes: Tag MAC address, Asset Name, Asset Group, Asset Category, Vendor (Type), Battery Life, and Last Located data (date and time). If the tag is Cisco CX v.1 compliant, telemetry information also appears.
- Detailed information for tags includes this additional information: IP address of associated controller, statistics, location notifications, location history, and whether the location debug feature is enabled.
  - To view location history for a tag, select that option from the Select a command drop-down menu and click **Go**.
  - To return to the details screen from the location history window, select the Tag Detail option and click **Go**.

Figure 8-20 Overlapping Tags Window



1 of 3 Prev Next Details

Tag 00:0c:cc:5b:fe:3a	
Asset Name	
Asset Group	
Asset Category	
Type	Aeroscout
Battery Life	Normal
Last Located	3/20/07 3:47 PM

Monitoring Chokepoints

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

Refer to the "Adding Chokepoints to the Cisco WCS" section on page 7-13 of this configuration guide. After adding the TDOA receiver to a map, you must 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.

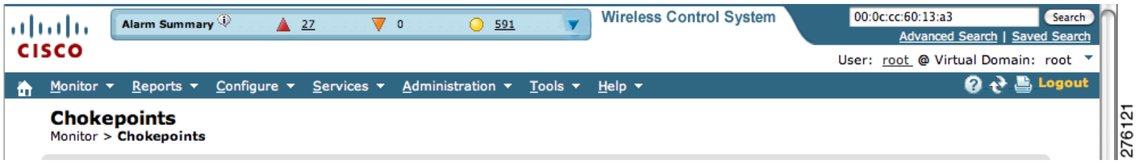
To monitor chokepoints, follow these steps:

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

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

a. To initiate a search for a chokepoint by its MAC address or chokepoint name, enter that value in the Search field of the navigation bar. Click **Search** (see Figure 8-21).

Figure 8-21 Search for Chokepoint by MAC Address

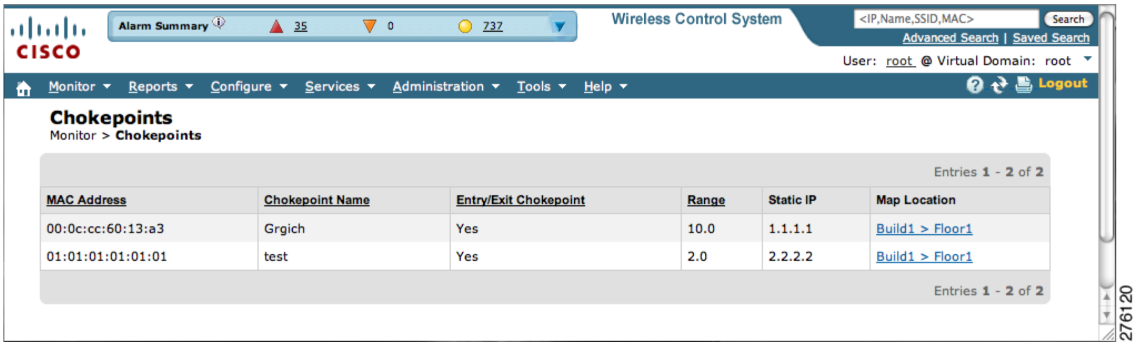


00:0c:cc:60:13:a3

This example show a search by MAC address (see Figure 8-22).

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

Figure 8-22 MAC Address Search Results for a Chokepoint Indicating a Match



Entries 1 - 2 of 2

MAC Address	Chokepoint Name	Entry/Exit Chokepoint	Range	Static IP	Map Location
00:0c:cc:60:13:a3	Grgich	Yes	10.0	1.1.1.1	Build1 > Floor1
01:01:01:01:01:01	test	Yes	2.0	2.2.2.2	Build1 > Floor1

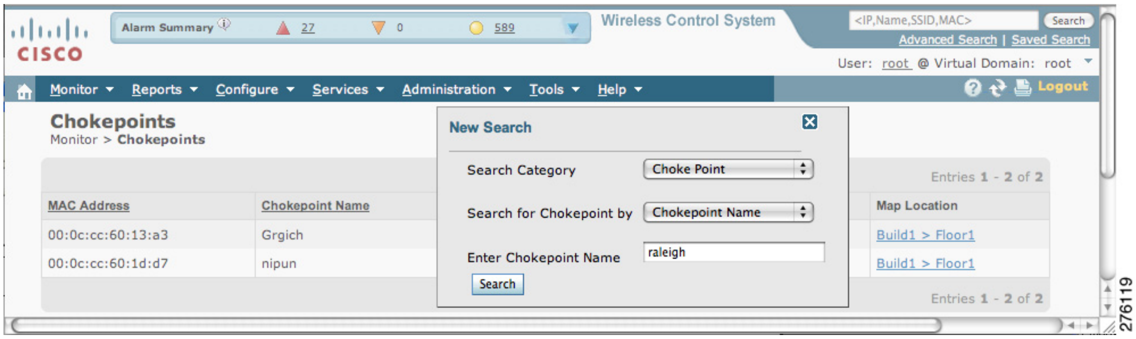
Entries 1 - 2 of 2

b. To initiate an advanced search for a chokepoint by its MAC address or name, click **Advanced Search** in the navigation bar.

1. Select **Chokepoint** as the search category.
2. Select either **Chokepoint Name** or **MAC Address** from the Search for Chokepoint by drop-down menu.
3. Enter either the chokepoint name or MAC address.
4. Click **Search**.

This example shows an advanced search using the chokepoint name (see Figure 8-23).

Figure 8-23 Chokepoint Name Advanced Search Panel



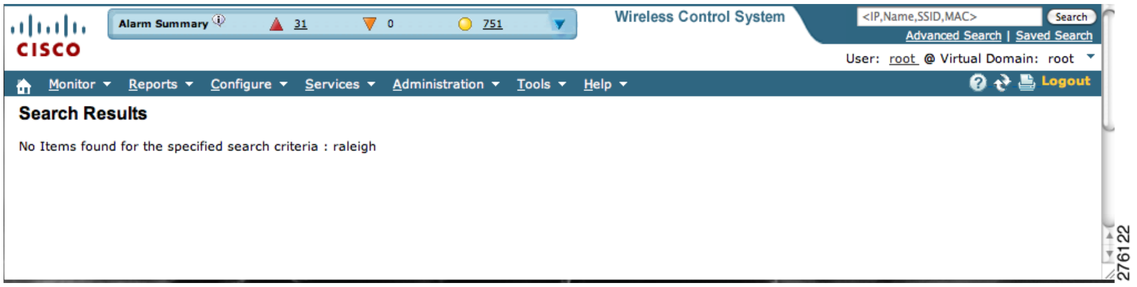
Search Category: Choke Point
Search for Chokepoint by: Chokepoint Name
Enter Chokepoint Name: raleigh

MAC Address	Chokepoint Name	Map Location
00:0c:cc:60:13:a3	Grgich	Build1 > Floor1
00:0c:cc:60:1d:d7	nipun	Build1 > Floor1

If no match exists, a message appears in the window (see Figure 8-24).

Otherwise the search result appears.

Figure 8-24 Chokepoint Advanced Search Results Indicating No Match



Search Results

No Items found for the specified search criteria : raleigh

Monitoring Wi-Fi TDOA Receivers

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

Refer to the "Adding Wi-Fi TDOA Receivers to Cisco WCS" section on page 7-19 of this configuration guide. After adding the TDOA receiver to a map, you must 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*.

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

To monitor TDOA Receivers, follow these steps:

Step 1 Choose **Monitor > WiFi TDOA Receivers**. The WiFi TDOA Receivers summary window appears showing all mapped TDOA receivers.

Step 2 To refine the search criteria when an extensive list appears, search by MAC address or TDOA receiver name.

a. To initiate a search for a TDOA receiver by its MAC address or name, enter that value in the Search field of the navigation bar. Click **Search** (see Figure 8-25).

Figure 8-25 Monitor > WiFi TDOA Receivers Search Window

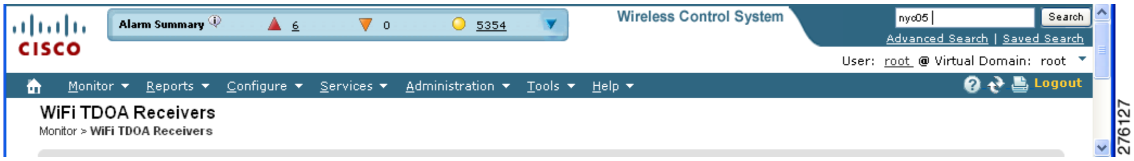
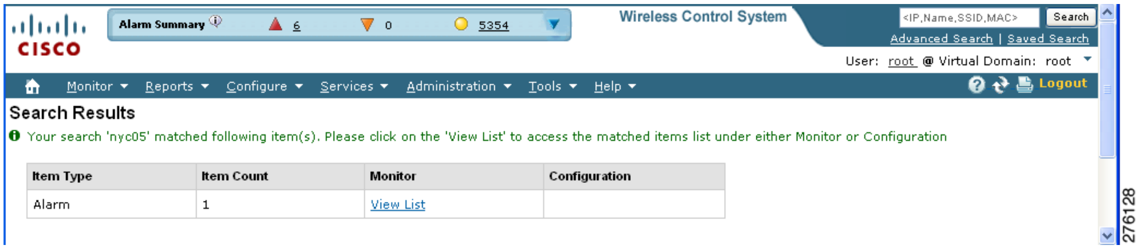


Figure 8-26 shows an example of advanced search using the TDOA Wi-Fi receiver name. Click **View List** to see a full list of Alarms.

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

Figure 8-26 Search Results Window



Search Results

Your search 'nyc05' matched following item(s). Please click on the 'View List' to access the matched items list under either Monitor or Configuration

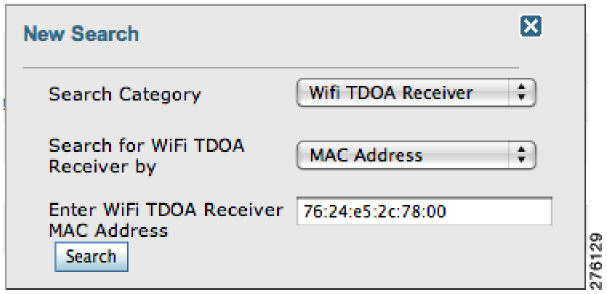
Item Type	Item Count	Monitor	Configuration
Alarm	1	View List	

b. To initiate an advanced search for a TDOA receiver by its MAC address or name, click Advanced Search in the navigation bar.

1. Select **WiFi TDOA Receiver** as the search category.
2. Select either **WiFi TDOA Receivers Name** or **MAC Address** from the Search for WiFi TDOA Receiver by drop-down menu.
3. Enter either the TDOA receiver name or MAC address.
4. Click **Search**.

This example shows an advanced search using the MAC address (see Figure 8-27).

Figure 8-27 Advanced Search Panel



New Search

Search Category: Wifi TDOA Receiver

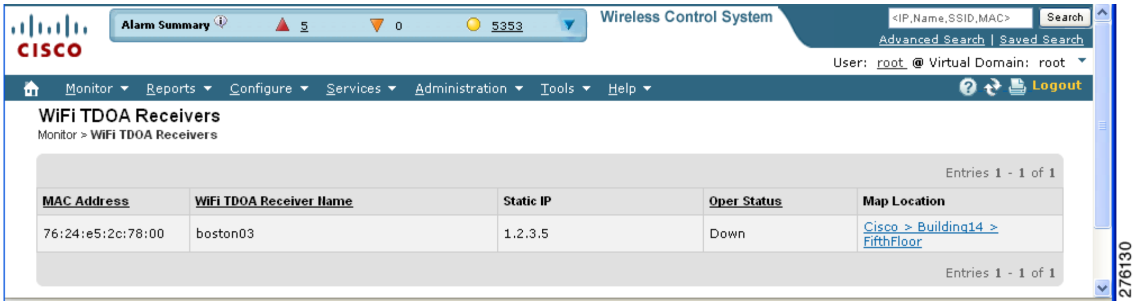
Search for WiFi TDOA Receiver by: MAC Address

Enter WiFi TDOA Receiver MAC Address: 76:24:e5:2c:78:00

Figure 8-28 shows the search results.

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

Figure 8-28 WiFi TDOA Receivers Advanced Search Results Indicating a Match



WiFi TDOA Receivers

Monitor > WiFi TDOA Receivers

Entries 1 - 1 of 1

MAC Address	WiFi TDOA Receiver Name	Static IP	Oper Status	Map Location
76:24:e5:2c:78:00	boston03	1.2.3.5	Down	Cisco > Building14 > FifthFloor

Entries 1 - 1 of 1

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.

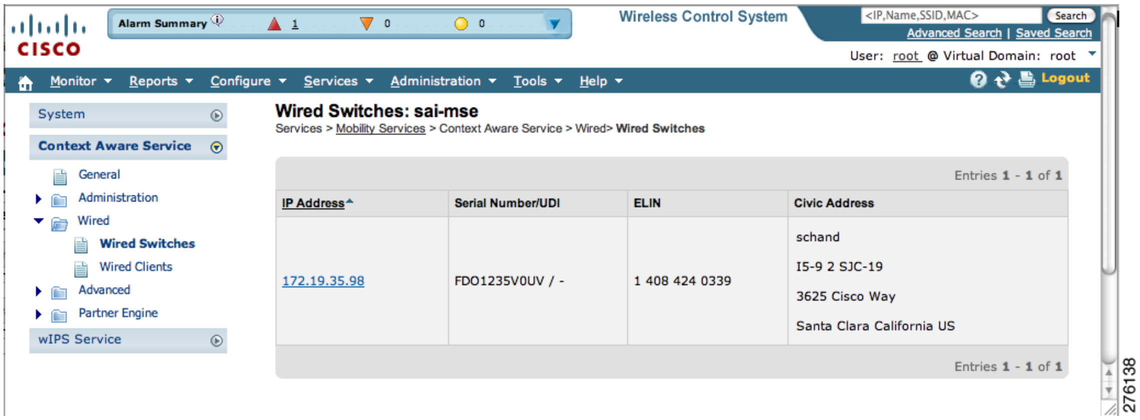
To view details on wired switches, follow these steps:

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

Step 2 At the Mobility Services window, 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.

Figure 8-29 Context Aware Service > Wired Switches Window



Wired Switches: sai-mse

Services > Mobility Services > Context Aware Service > Wired> **Wired Switches**

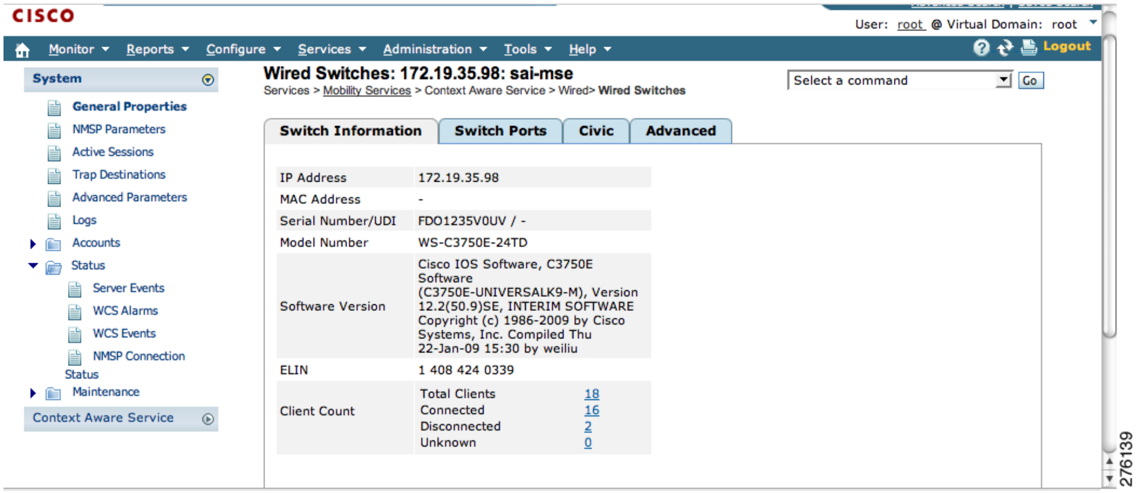
Entries 1 - 1 of 1

IP Address	Serial Number/UDI	ELIN	Civic Address
172.19.35.98	FDO1235V0UV / -	1 408 424 0339	schand I5-9 2 SJC-19 3625 Cisco Way Santa Clara California US

Entries 1 - 1 of 1

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 Window



Wired Switches: 172.19.35.98: sai-mse

Services > Mobility Services > Context Aware Service > Wired> **Wired Switches**

IP Address	172.19.35.98
MAC Address	-
Serial Number/UDI	FDO1235V0UV / -
Model Number	WS-C3750E-24TD
Software Version	Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Version 12.2(50.9)SE, INTERIM SOFTWARE Copyright (c) 1986-2009 by Cisco Systems, Inc. Compiled Thu 22-Jan-09 15:30 by weiliu
ELIN	1 408 424 0339
Client Count	Total Clients 18 Connected 16 Disconnected 2 Unknown 0

Note You can export civic information from the switch by selecting that option from the Select a command drop-down menu. This option is available at all four sub-panels of the Wired Switches window.

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).

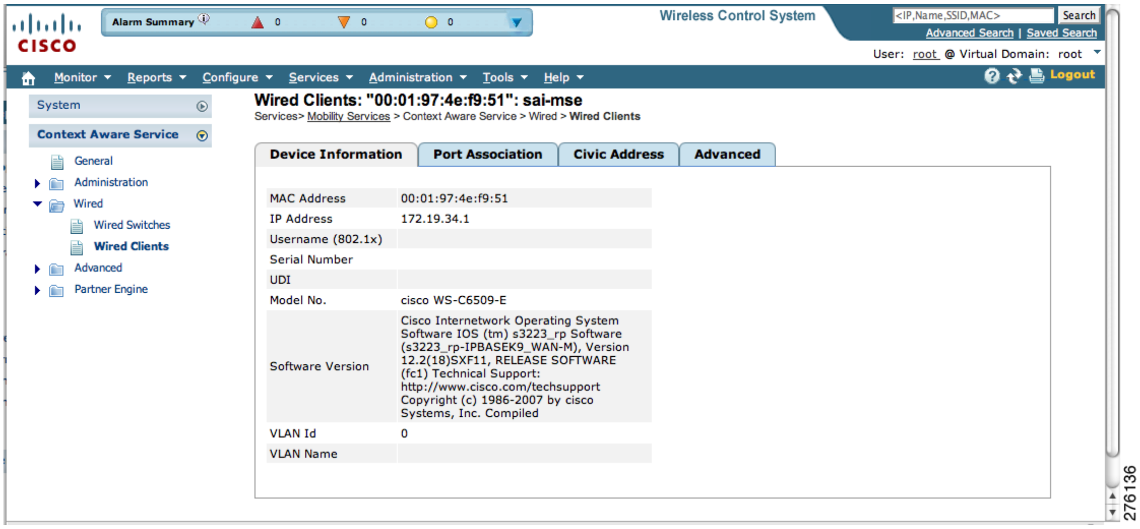
- Connected clients–Clients that are connected to the wired switch.
- Disconnected clients–Clients that are disconnected from the wired switch.
- Unknown clients–Clients are marked as unknown when the NMSP connection to the wired switch is lost.

You can view detailed wired client information by clicking on one of the client count links (total clients, connected, disconnected, and unknown). Refer to the "Monitoring Wired Clients" section on page 8-27 for details.

Step 5 Click the **Switch Ports** tab to see a detailed list of the ports on the switch (see Figure 8-31).

Note You can change the listing order (ascending, descending) of port IP addresses, slot numbers, module number, and port number by clicking on the respective column heading.

Figure 8-31 Wired Switches > Switch Ports Window



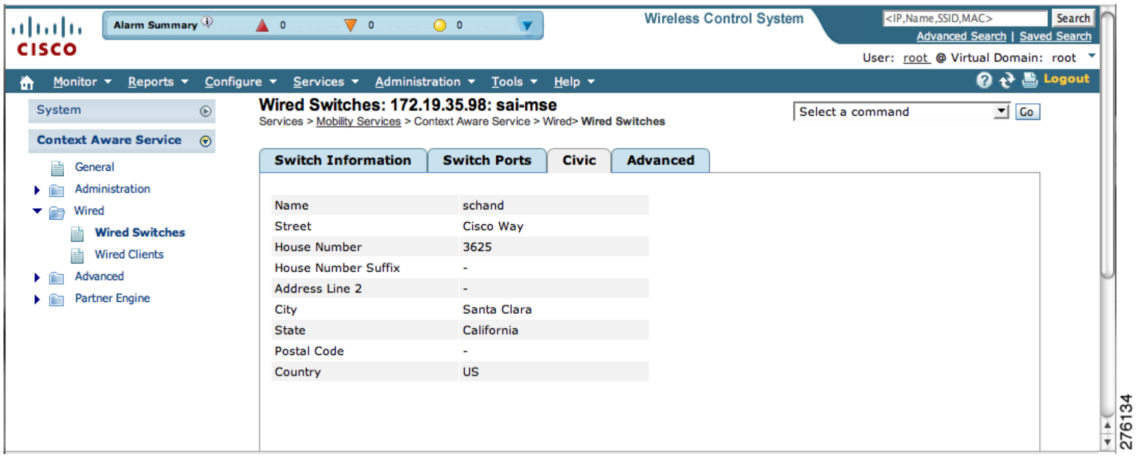
Wired Clients: "00:01:97:4e:f9:51": sai-mse

Services> Mobility Services > Context Aware Service > Wired > Wired Clients

MAC Address	00:01:97:4e:f9:51
IP Address	172.19.34.1
Username (802.1x)	
Serial Number	
UDI	
Model No.	cisco WS-C6509-E
Software Version	Cisco Internetwork Operating System Software IOS (tm) s3223_rp Software (s3223_rp-IPBASEK9_WAN-M), Version 12.2(18)SXF11, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2007 by cisco Systems, Inc. Compiled
VLAN Id	0
VLAN Name	

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 Window



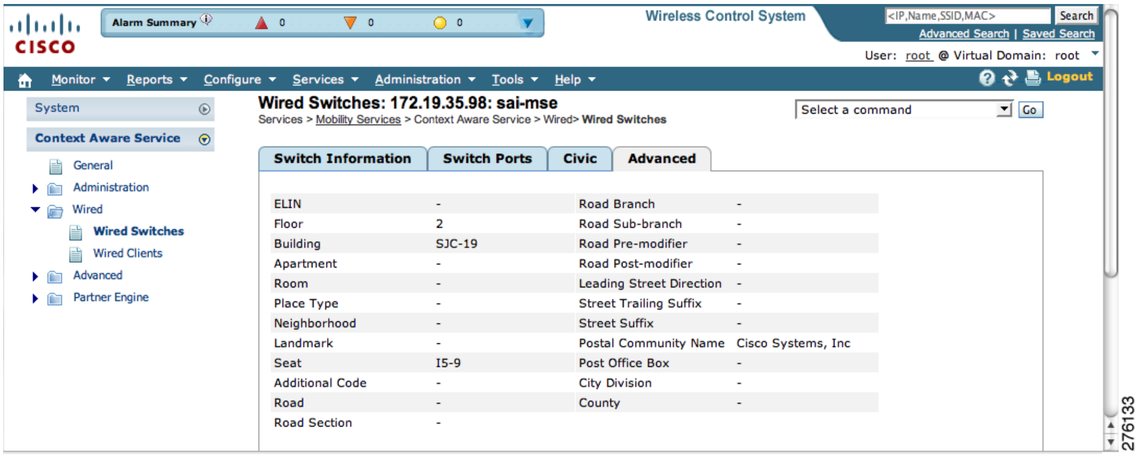
Wired Switches: 172.19.35.98: sai-mse

Services > Mobility Services > Context Aware Service > Wired> Wired Switches

Name	schand
Street	Cisco Way
House Number	3625
House Number Suffix	-
Address Line 2	-
City	Santa Clara
State	California
Postal Code	-
Country	US

Step 7 Click the **Advanced** tab to see a detailed list of the additional civic information for the wired switch (see Figure 8-33).

Figure 8-33 Wired Switches > Advanced Window



Wired Switches: 172.19.35.98: sai-mse

Services > Mobility Services > Context Aware Service > Wired> Wired Switches

ELIN	-	Road Branch	-
Floor	2	Road Sub-branch	-
Building	SJC-19	Road Pre-modifier	-
Apartment	-	Road Post-modifier	-
Room	-	Leading Street Direction	-
Place Type	-	Street Trailing Suffix	-
Neighborhood	-	Street Suffix	-
Landmark	-	Postal Community Name	Cisco Systems, Inc
Seat	I5-9	Post Office Box	-
Additional Code	-	City Division	-
Road	-	County	-
Road Section	-		

Monitoring Wired Clients

You can view details on a wired client (MAC address, IP address, username, serial number, UDI, model no., software version, VLAN ID, 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 wired clients' details on either the wired switches window (**Context Aware Service > Wired > Wired Switches**) or wired clients window (**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 field on the wired clients window.
- If you want to examine wired clients as they relates to a specific switch, you can view that information on the wired switches window. Refer to the "Monitoring Wired Switches" section on page 8-24.

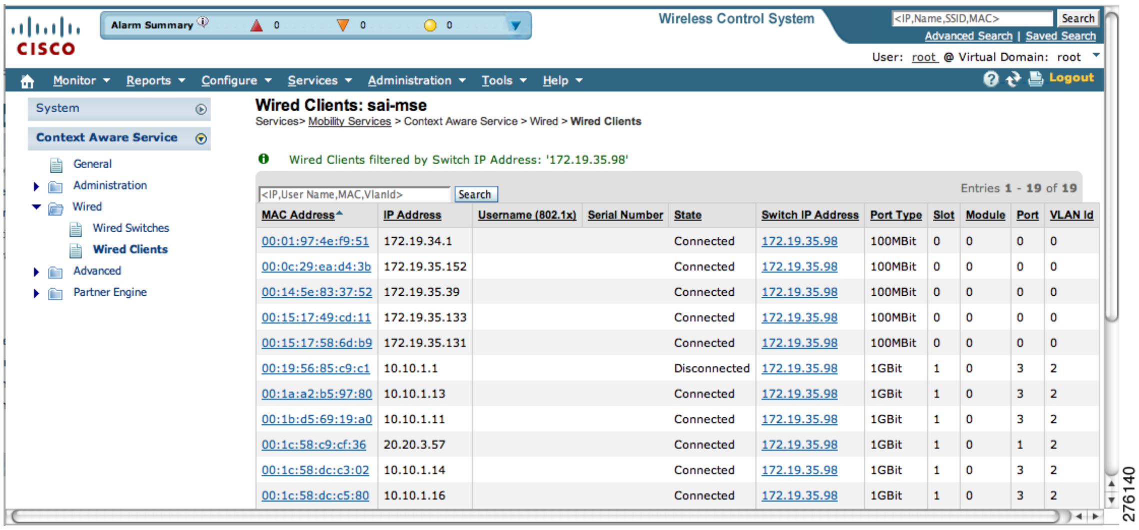
To view details on a wired client, follow these steps:

Step 1 Choose **Services > Mobility Services**. The Mobility Services window appears.

Step 2 Click the device name link of the appropriate wired location switch.

Step 3 Choose **Context Aware Service > Wired > Wired Clients**.

Figure 8-34 *Wired > Wired Clients Window*



Wired Clients: sai-mse

Services> Mobility Services > Context Aware Service > Wired > **Wired Clients**

Wired Clients filtered by Switch IP Address: '172.19.35.98'

<IP,User Name,MAC,VlanId> Search

Entries **1** - **19** of **19**

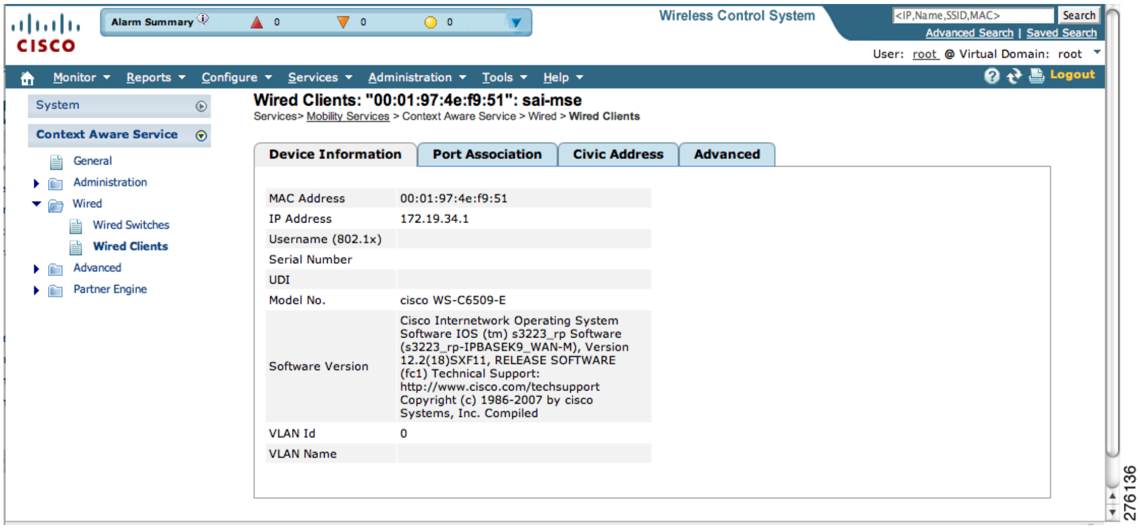
MAC Address	IP Address	Username (802.1x)	Serial Number	State	Switch IP Address	Port Type	Slot	Module	Port	VLAN Id
00:01:97:4e:f9:51	172.19.34.1			Connected	172.19.35.98	100MBit	0	0	0	0
00:0c:29:ea:d4:3b	172.19.35.152			Connected	172.19.35.98	100MBit	0	0	0	0
00:14:5e:83:37:52	172.19.35.39			Connected	172.19.35.98	100MBit	0	0	0	0
00:15:17:49:cd:11	172.19.35.133			Connected	172.19.35.98	100MBit	0	0	0	0
00:15:17:58:6d:b9	172.19.35.131			Connected	172.19.35.98	100MBit	0	0	0	0
00:19:56:85:c9:c1	10.10.1.1			Disconnected	172.19.35.98	1GBit	1	0	3	2
00:1a:a2:b5:97:80	10.10.1.13			Connected	172.19.35.98	1GBit	1	0	3	2
00:1b:d5:69:19:a0	10.10.1.11			Connected	172.19.35.98	1GBit	1	0	3	2
00:1c:58:c9:cf:36	20.20.3.57			Connected	172.19.35.98	1GBit	1	0	1	2
00:1c:58:dc:c3:02	10.10.1.14			Connected	172.19.35.98	1GBit	1	0	3	2
00:1c:58:dc:c5:80	10.10.1.16			Connected	172.19.35.98	1GBit	1	0	3	2

At the Wired Clients summary window, clients are grouped by their switch (see Figure 8-34).

A client's status is noted as connected, disconnected, or unknown. Definitions are summarized below:

- 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 wired client's MAC address you can click on that link to reach the client's detail page (see Figure 8-35) or use the search field.
  - 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 switch's detail window. Refer to the "Monitoring Wired Switches" section on page 8-24.

Figure 8-35 *Wired Clients > Device Information Window*



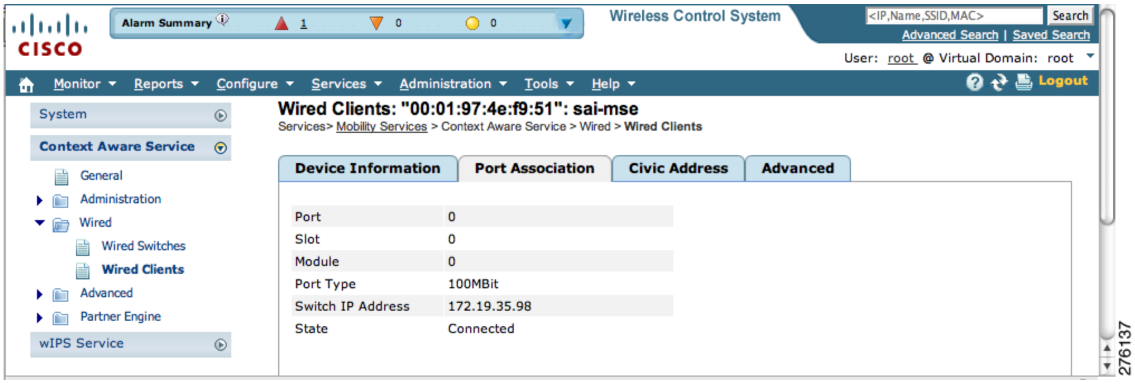
Wired Clients: "00:01:97:4e:f9:51": sai-mse

Services> Mobility Services > Context Aware Service > Wired > **Wired Clients**

MAC Address	00:01:97:4e:f9:51
IP Address	172.19.34.1
Username (802.1x)	
Serial Number	
UDI	
Model No.	cisco WS-C6509-E
Software Version	Cisco Internetwork Operating System Software IOS (tm) s3223_rp Software (s3223_rp-IPBASEK9_WAN-M), Version 12.2(18)SXF11, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2007 by cisco Systems, Inc. Compiled
VLAN Id	0
VLAN Name	

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 8-36).

Figure 8-36 Wired Clients > Port Association Window



Wired Clients: "00:01:97:4e:f9:51": sai-mse

Services> Mobility Services > Context Aware Service > Wired > Wired Clients

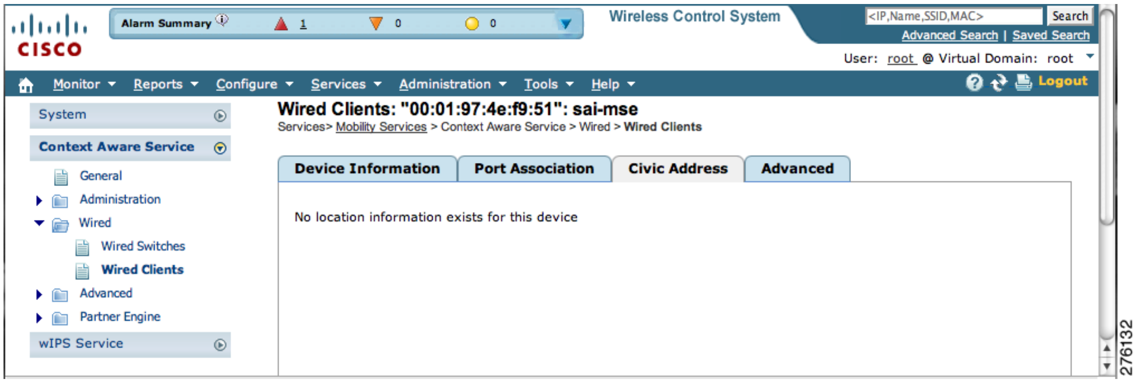
Port	0
Slot	0
Module	0
Port Type	100MBit
Switch IP Address	172.19.35.98
State	Connected

Step 5 Click the **Civic Address** tab to show any civic address information (see Figure 8-37).

Step 6 Click the **Advanced** tab to see any extended physical address details for the wired clients, if any (see Figure 8-38).

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 8-37 Wired Clients > Civic Address Window

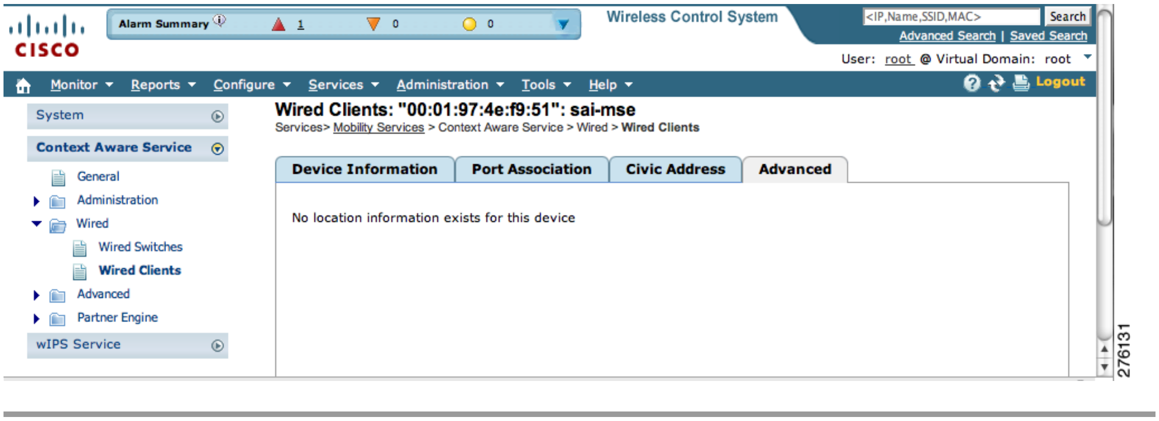


Wired Clients: "00:01:97:4e:f9:51": sai-mse

Services> Mobility Services > Context Aware Service > Wired > Wired Clients

No location information exists for this device

Figure 8-38 Wired Clients > Advanced Window



Wired Clients: "00:01:97:4e:f9:51": sai-mse

Services> Mobility Services > Context Aware Service > Wired > Wired Clients

No location information exists for this device