CHAPTER 7

# 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 WCS. It also describes how to have email notifications for alarms sent to you as well as how to define those types (all, critical, major, minor, warning) of alarm notifications.

This section contains the following topics:



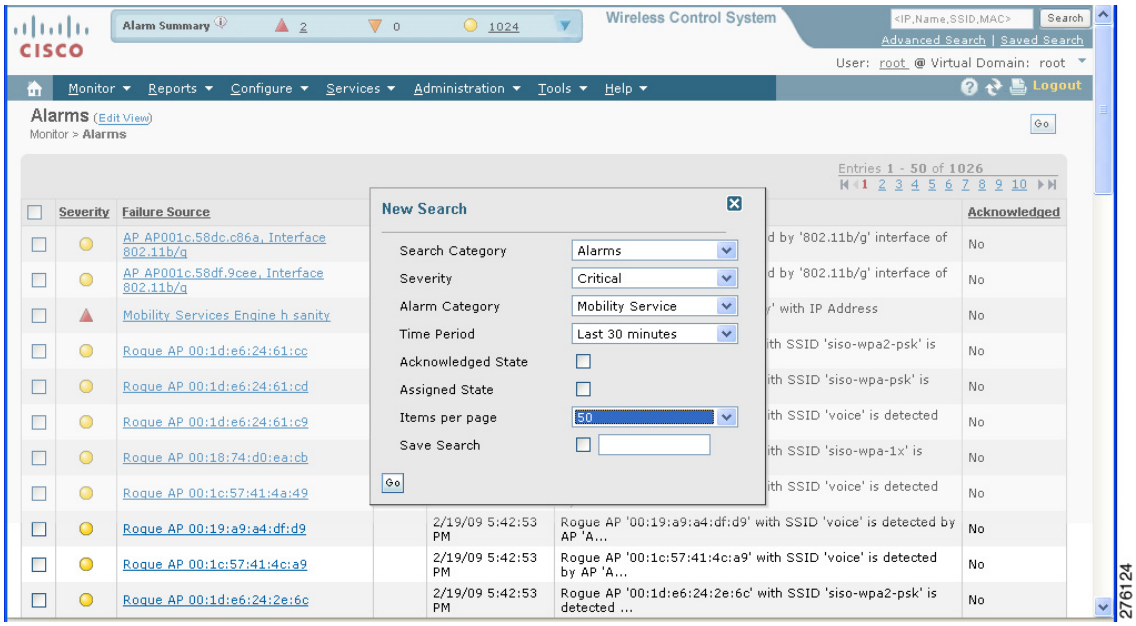
## Viewing Alarms

To view the 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. A configurable search dialog box for alarms appears (see Figure 7-1).

***Figure 7-1 New Search Alarm Dialog Box***




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

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

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

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

**Step 6** Choose the time frame for which you want to review alarms from the Time Period drop-down list.

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

**Step 7** Select the **Acknowledged State** check box to exclude the acknowledged alarms and their count in the Alarm Summary page.

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

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

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

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

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

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

**Step 12** Repeat Step 2 to Step 11 to see notifications for access points by entering **Access Points** as the alarm category in Step 5.

# Assigning and Unassigning Alarms

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

**Step 1** Choose **Monitors** > **Alarms** to display the Alarms page as described in the "Viewing Alarms" section on page 7-2.

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

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

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

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

# Deleting and Clearing Alarms

If you delete an alarm, WCS removes it from its database. If you clear an alarm, it remains in the 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** Choose **Monitors > Alarms** to display the Alarms page as described in the "Viewing Alarms" section on page 7-2.

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

**Step 3** From the Select a command drop-down list, choose **Delete** or **Clear**. Click **Go**.

# Emailing Alarm Notifications

WCS lets you send alarm notifications to a specific email address. Sending notifications through email enables you to take prompt action when needed.

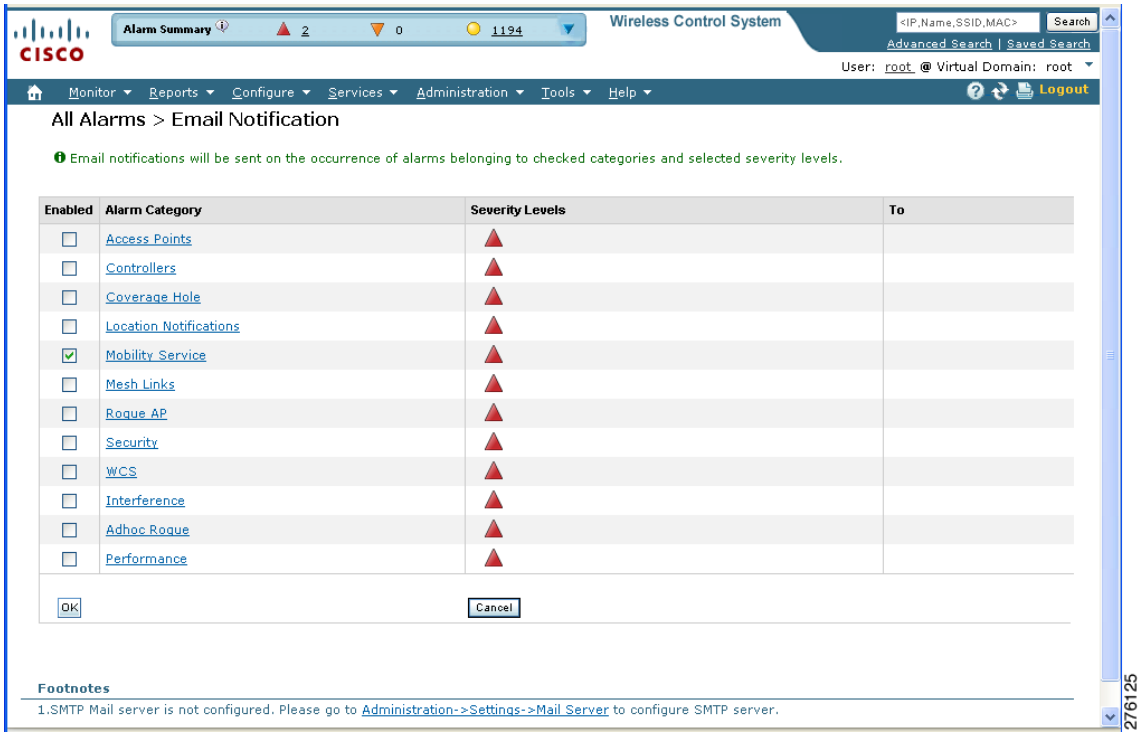
You can select the alarm severity types (critical, major, minor, and warning) you have emailed to you.

To send alarm notifications, follow these steps:

**Step 1** Choose **Monitor > Alarms**.

**Step 2** From the Select a commands drop-down list, choose **Email Notification**. Click **Go**. The Email Notification page appears (see Figure 7-2).

***Figure 7-2 All Alarms > Email Notification page***



**Note** An SMTP Mail Server must be defined prior to entry of 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 page.

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

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

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

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

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

**Step 7** Click **OK**.

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

# Working with Events

You can use 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, info) and event category.

You can search by the following event categories:

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

**Note** The product type: mobility service reports events for mobility services engines.

- By security

Additionally, you can search for events of an element 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 page:

- If you want to display the events for a specific element, and you know its IP address, name, WLAN SSID, or MAC address, enter that value in the Search text box. Click **Search**.
- To display events by severity and category, click **Advanced Search** in the navigation bar and choose the appropriate options from the Severity and Event Category drop-down lists. Click **Go**.

**Step 3** If WCS finds events that match the search criteria, it displays a list of these events.

**Note** For more information about an event, click the failure object associated with the event. Additionally, you can sort the events summary by each of the column headings.

# Working with Logs

This section describes how to configure logging options and how to download log files.

This section includes the following topics:



## Configuring Logging Options

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

To configure logging options, follow these steps:

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

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

**Step 3** From the System left sidebar menu click **Logs**. The advanced parameters for the selected mobility services engine appears.

**Step 4** In the Logging Options section, choose the appropriate option from the Logging Level drop-down list.

There are four logging options: Off, Error, Information, and Trace.

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

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

**Step 6** Select the **Enable** check box under Advanced Parameters to enable advanced debugging. By default, this option is disabled.

**Step 7** To download log files from the server, click **Download Logs**. For more information, see Downloading Log Files.

**Step 8** In the Log File Parameters section, enter the following:

- The number of log files to be maintained in the mobility services engine. You can maintain a minimum of 5 log files and a maximum of 20 log files in the mobility services engine.
- The maximum log file size in MB. The minimum log file size is 10 MB and the maximum is 50 MB.

**Step 9** In the MAC Address Based Logging Parameters section, do the following:

- Select the **Enable** check box to enable MAC address logging. By default, this option is disabled.
- Add one or more MAC addresses for which you want to enable logging. You can also remove MAC addresses that you have already added by selecting the MAC address from the list and clicking **Remove**.

For more information on MAC Address-based logging, see MAC Address Based Logging.

**Step 10** Click **Save** to apply your changes.

## MAC Address Based Logging

This feature allows you to create log files that are specific to an entity whose MAC address is specified. The log files are created in the locserver directory under the following path:

/opt/mse/logs/locserver

A maximum of 5 MAC addresses can be logged at a time. The Log file format for MAC address aa:bb:cc:dd:ee:ff is:

macaddress-debug-aa-bb-cc-dd-ee-ff.log

You can create a maximum of two log files for a MAC Address. The two log files may consist of one main and one backup or rollover log file.

- The minimum size of a MAC log file is 10 MB. The maximum size allowed is 20 MB per MAC Address. The MAC log files which are not updated for more than 24 hours are pruned.

**Step 11** Click **Save** to apply your changes.

# Downloading Log Files

If you need to analyze mobility services engine log files, you can use WCS to download them to your system. 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 WCS, you can generate a device utilization and location utilization report for a mobility services engine. By default, reports are stored on the 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

This section contains the following topics:



## Creating a Device Utilization Report

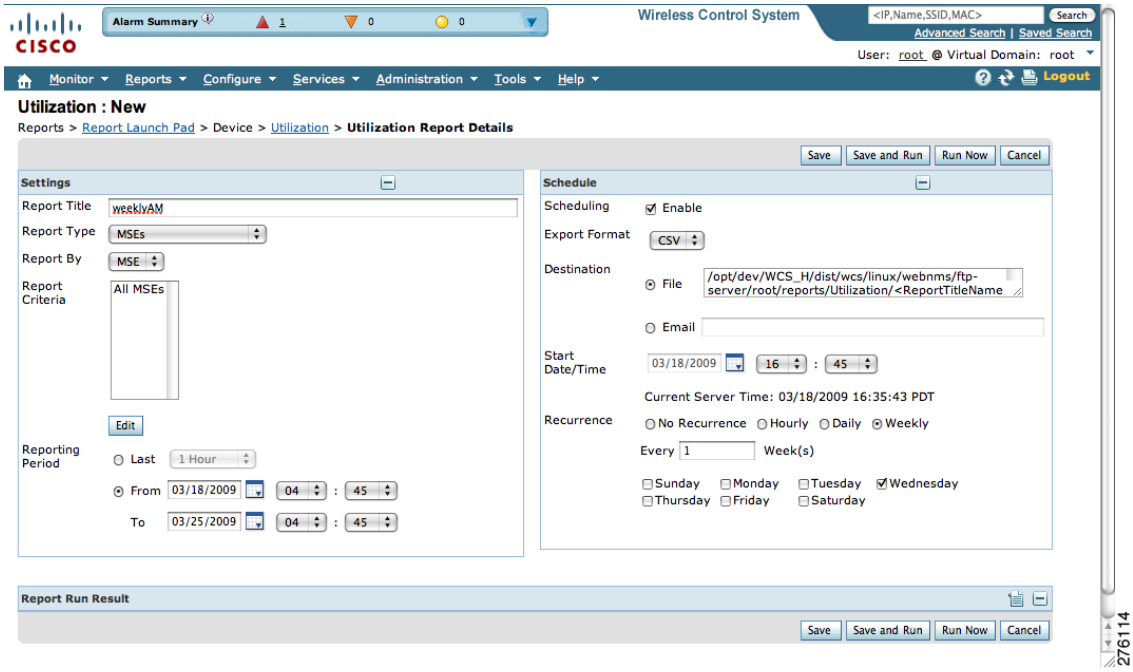
To create a utilization report for the mobility services engine, follow these steps:

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

**Step 2** Choose **Device > Utilization**.

**Step 3** Click **New**. The Utilization: New page appears (see Figure 7-3).

***Figure 7-3 Device > Utilization New Page***




**Step 4** In the Settings pane, 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** in the dialog box 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 pane, select the **Enable Schedule** check box.

**Step 9** Choose the report format (CSV or PDF) from the Export Report drop-down list.

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

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

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

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

**Step 13** Select any one of the Recurrence options to determine how often the report is to be run.

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

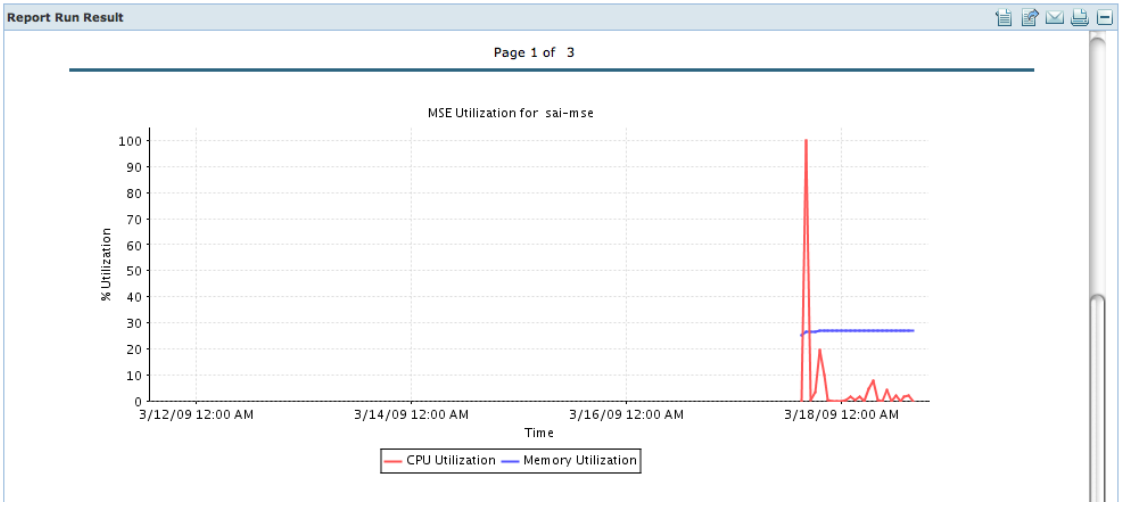
**Step 14** When finished with all of the above steps, do one of the following:

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

The results appear at the bottom of the page (see Figure 7-3).

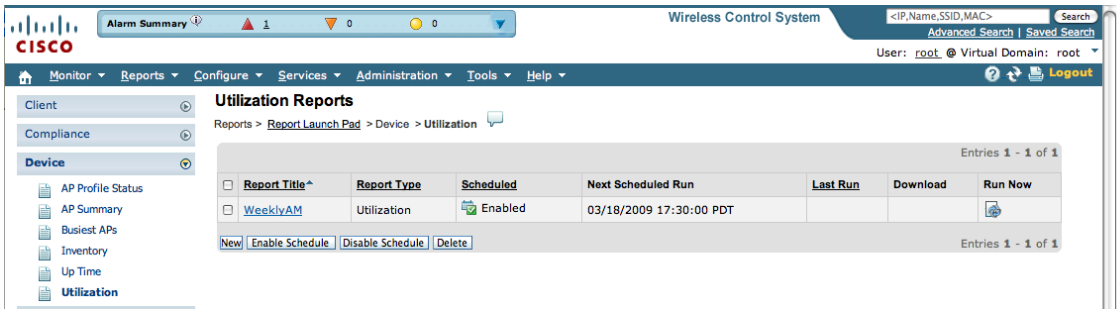
**Note** Only the CPU and memory utilization reports are shown (see Figure 7-4).

*Figure 7-4 Device > MSE Utilization > Results*



**Step 15** If you clicked Save or Save and Run, click either **Reports > Saved Reports** (or **Reports > Scheduled Runs** if the report has not yet run and is scheduled to run). The Utilization Reports summary page appears (see Figure 7-5).

***Figure 7-5 Utilization Reports Summary Page***




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

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

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

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

# Viewing Saved Utilization Report

To download a saved report, follow these steps:

**Step 1** In WCS, choose **Reports > Saved Reports**.

**Step 2** Click the **Download** icon for your request. 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 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.

# Security Reports and Alarms for wIPS

You can view, modify, or create a security report or alarm for wIPS.

**Note** Security reports do not show the status of autonomous access points.

The choices are as follows:

- Adaptive wIPS Alarms—Alarms reported for wIPS on monitor mode access points.
- Adaptive wIPS Top 10 AP—Lists the last 10 events reported for monitor access points.
- Adhoc Rogue Event—Displays all adhoc events that WCS has received in the selected timeframe.
- Adhoc Rogues—Displays all adhocs that have been updated in the selected timeframe.
- New Rogue APs—Displays, in tabular form, all rogues detected in a selected timeframe. It provides which new rogues were detected within a selected time. The created time indicates the time at which the rogue was first detected.
- New Rogue AP Count—Displays, in graphical form, all rogues detected in a selected timeframe.
- Rogue APs—Displays all rogues that are active in your network and have been updated in the selected timeframe. WCS receives updated events for rogues that are detected.
- Rogue APs Event—Displays all the events received by WCS. The controller sends updates of detected rogues if any of the attributes change or new rogues are detected.

**Note** This report was formally called the Rogue Detected by AP.

- Security Summary—Shows the number of association failures, rogues access points, ad hocs, and access point connections or disconnections over one month.
- Click **Save and Run** to save the changes and run the report now. The report runs regardless of any scheduled time associated with the report and is viewable on the Results tab. Additionally, the report is run at the designated time and the results are either emailed or saved to a designated file as defined on the Schedule tab.
  - In the results page, you can cancel or delete the report.

This section includes the following topics:

# Creating a New wIPS Security or Alarms Report

Security reports provide a number of details on access points and rogue access points for wIPS.

To create a new security report, follow these steps:

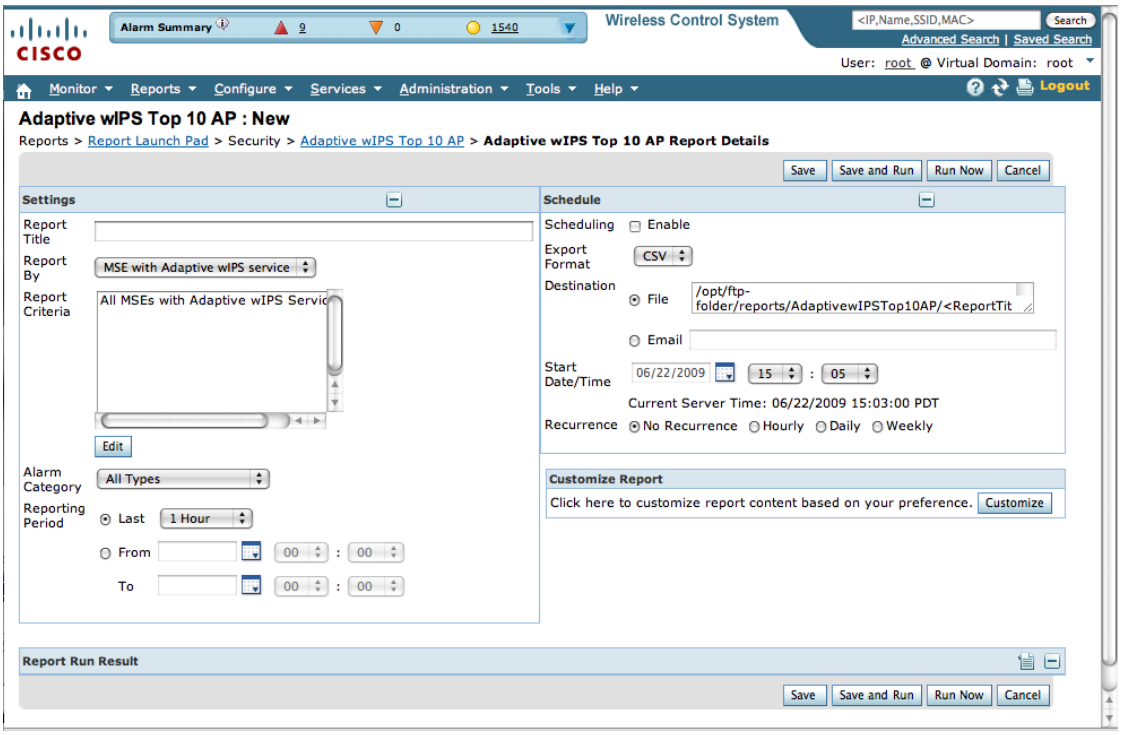
**Note** Some of these steps or options are not required for every report.

**Step 1** Choose **Reports > Report Launch Pad**. The Report Launch Pad page appears.

**Step 2** Choose **Security** and click on one of the report types in the left pane (such as Adaptive wIPS Top 10 Report Details).

**Step 3** Click **New**. The new report page appears (see Figure 7-6).

***Figure 7-6 New Report Page***




**Step 4** In the Settings pane, enter a report title.

**Step 5** The Report By is by default MSE with Adaptive wIPS Service.

**Step 6** The Report Criteria is always either a specific mobility services engine or All MSEs with Adaptive wIPS Service.

**Step 7** Click Edit to add or modify the Report Crieteria. The Filter Criteria dialog box appears.

**Step 8** 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 9** In the Schedule panel, select the **Enable Schedule** check box.

**Step 10** Choose the report format (CSV or PDF) from the Export Report drop-down list.

**Step 11** Select either **File** or **Email** as the destination of the report.

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

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

**Step 13** Choose a start time using the hour and minute drop-down lists.

**Step 14** Select any one of the Recurrence options to determine how often the report is to be run.

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

You can also use the Customize Report option to customize the report. Click **Customize** and provide the required information to generate the report.

**Step 15** When you have completed Step 1 to Step 14, 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 page. The report also runs at the designated time and the results are either emailed or saved to a designated file as defined in the Schedule panel.
  - In the results page, click **Cancel** to cancel the defined report.
- Click **Run Now** if you want to run the report immediately and review the results in the WCS page. The report runs regardless of any pending, scheduled run of that report. Results appear at the bottom of the page. Click **Save** if you want to save the report criteria you entered.

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

The results appear at the bottom of the page.

**Step 16** Repeat Step 2 to Step 15 for each wIPS report you want to create.

# Viewing Saved wIPS Report

To download a saved report, follow these steps:

**Step 1** In WCS, choose **Reports > Saved Reports**.

**Step 2** Click the **Download** icon for your request. It is downloaded and saved in the defined directory or emailed.

# Viewing Scheduled wIPS Report Runs

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

**Step 1** In 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.