Monitoring the System and Services

This chapter describes how to monitor the mobility services engine by configuring and viewing alarms, events, and logs and how to generate reports on system use and element counts (tags, clients, rogue clients, interferers, and access points). This chapter also describes how to use the Prime Infrastructure 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 on a mobility services engine using the Prime Infrastructure. It also describes how to define alarm notifications (all, critical, major, minor, warning) and how to e-mail those alarm notifications.

This section contains the following topics:

Guidelines and Limitations

Once the severity is cleared, the alarm is deleted from the Prime Infrastructure after 30 days.
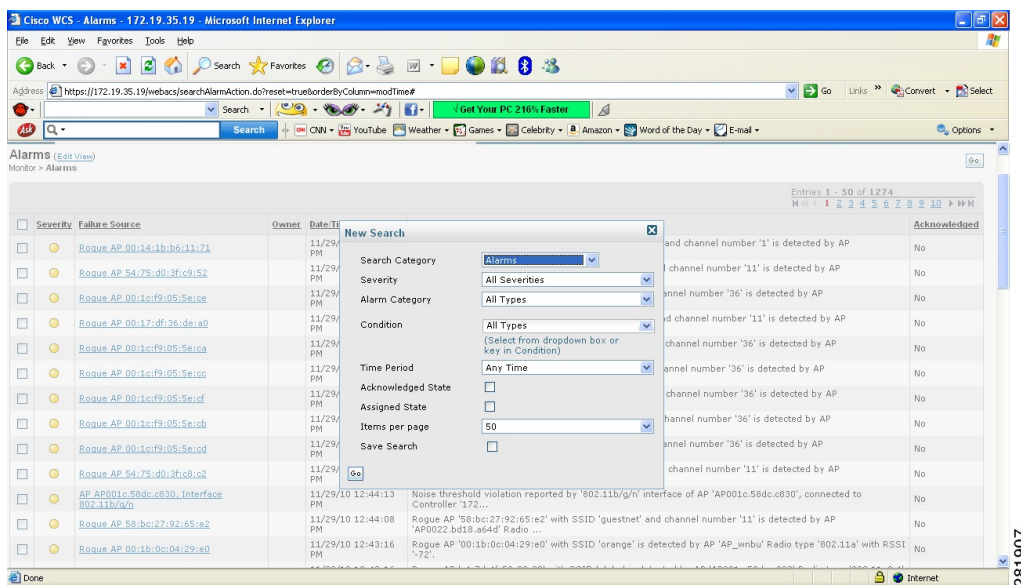
Viewing Alarms

To view mobility services engine alarms, follow these steps:

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

Step 2   Click the **Advanced Search** link in the navigation bar. A configurable search dialog box for alarms appears .

Figure 1: Advanced Search Alarm Dialog Box

Step 3   Choose **Alarms** from the Search Category drop-down list.

Step 4   Choose the severity of alarms from the Severity drop-down list. The options are All Severities, Critical, Major, Minor, Warning, or Clear.

Step 5   Choose **Mobility Service** from the Alarm Category drop-down list.

Step 6   Choose the **Condition** from the Condition combo box. Alternatively, you can enter the condition in the Condition text box.

Step 7   From the Time Period drop-down list, choose the time frame for which you want to review alarms.
The options range from minutes (5, 15, and 30) to hours (1 and 8) to days (1 and 7). To display all, choose **Any time**.

Step 8   Select the **Acknowledged State** check box to exclude the acknowledged alarms and their count in the Alarm Summary page.

Step 9   Select the **Assigned State** check box to exclude the assigned alarms and their count in the Alarm Summary page.

Step 10   From the Items per page drop-down list, choose the number of alarms to display in each page.

Step 11   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 12   Click **Go**. The alarms summary dialog box appears with search results.
     Note   Click the column headings (Severity, Failure Source, Owner, Date/Time, Message, and Acknowledged) to sort alarms.

Step 13   Repeat Step 2 to Step 12 to see Context-Aware Service notifications for the mobility services engine. Enter **Context Aware Notifications** as the alarm category in Step 5.

Viewing the MSE Alarm Details

To view MSE alarm details, follow these steps:

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

Step 2   Click an MSE in the Failure Source column to access the alarms details for a particular MSE.
Alternatively, you can choose the **Services** > *MSE Name* > **System** > **Status** > **Prime Infrastructure Alarms** page and click a particular MSE item in the Failure Source column to access the alarms details for a particular MSE.

Figure 2: MSE Alarm

The following table describes the various fields in the Alarm Detail page for an MSE.

Table 1: Alarm Detail Page Parameters

Field	Description
Failure Source	The MSE that generated the alarm.
Owner	Name of person to which this alarm is assigned, or blank.
Acknowledged	Shows whether or not the alarm is acknowledged by the user.
Category	The category of the alarm.The Alarm category is Mobility Services for MSEs.
Created	Month, day, year, hour, minute, second, AM or PM alarm created.
Modified	Month, day, year, hour, minute, second, AM or PM the alarm was last modified.
Generated By	This field displays the MSE.
Severity	Level of security: Critical, Major, Minor, Warning, Clear, Info, Color coded.
Previous Severity	Critical, Major, Minor, Warning, Clear, Info. Color coded.

Note The general information may vary depending on the type of alarm. For example, some alarm details may include location and switch port tracing information.

Assigning and Unassigning Alarms

To assign and unassign an alarms, follow these steps:

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

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

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

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

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

Deleting and Clearing Alarms

If you delete an alarm, the Prime Infrastructure removes it from its database. If you clear an alarm, it remains in the Prime Infrastructure 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.

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**.

E-mailing Alarm Notifications

The Prime Infrastructure lets you send alarm notifications to a specific e-mail address. Sending notifications through e-mail enables you to take prompt action when needed.
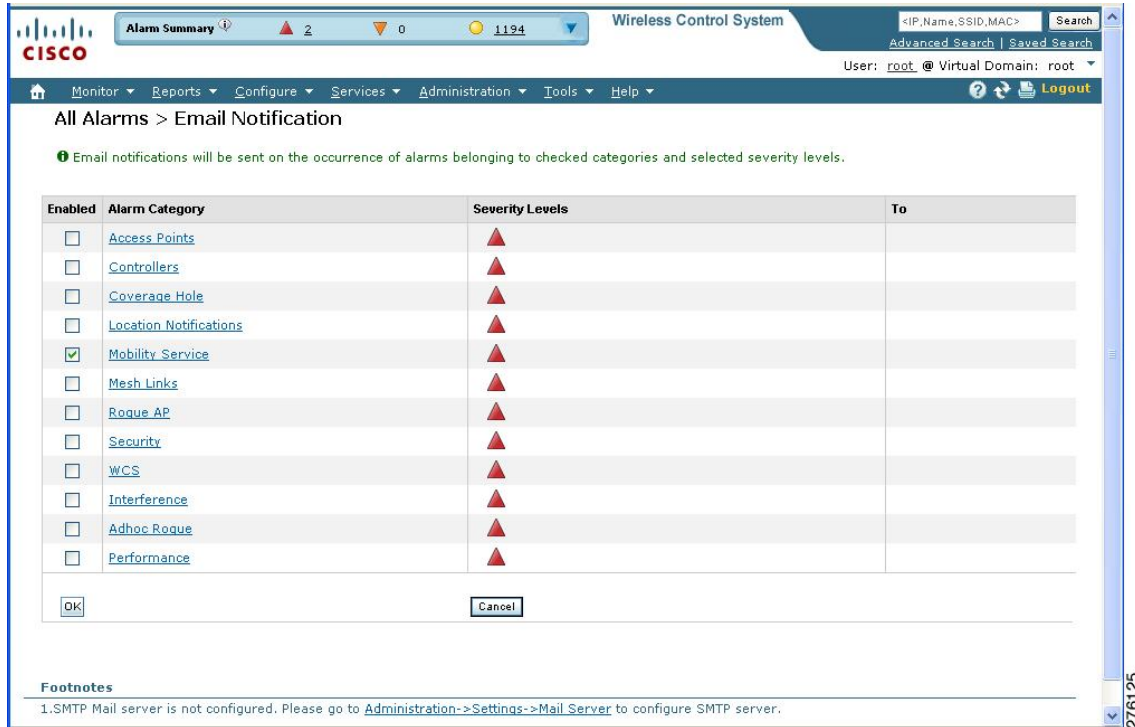
You can choose the alarm severity types (critical, major, minor, and warning) to have e-mailed to you.

To send alarm notifications to e-mail, follow these steps:

Step 1   Choose **Monitor > Alarms**.

Step 2   From the Select a command drop-down list, choose **Email Notification**. Click **Go**. The Email Notification page appears.

Figure 3: All Alarms > Email Notification Page

Note   An SMTP mail server must be defined before you enter target e-mail addresses for e-mail notification. Choose **Administration > Settings > Mail Server Configuration** to enter the appropriate information.

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

Note   Enabling the **Mobility Service** alarm category sends all alarms related to mobility services engine and the location appliance to the defined e-mail 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 e-mail notifications sent.

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

Step 7   Click **OK**.
You are returned to the Alarms > Notification page. The changes to the reported alarm severity levels and the recipient e-mail address for e-mail notifications are displayed.

Working with Events

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

This section contains the following topics:

Displaying Location Notification Events

To display location notification events, follow these steps:

Step 1   Choose **Monitor > Events**.

Step 2   In the Events page, you can perform the following:

- If you want to display the events for a specific element, and you know its IP address, name, WLAN SSID, or MAC address, enter that value in the Search text box of the navigation bar. Click **Search**.

- To display events by severity and category, click **Advanced Search** in the navigation bar and choose the appropriate options from the Severity and Event Category drop-down list boxes. Click **Go**.

Step 3   If Prime Infrastructure finds events that match the search criteria, it shows a list of these events.

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

Working with Logs

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

This section contains the following topics:

Guidelines and Limitations

- When you are selecting an appropriate option from the logging level, make sure you use Error and Trace only when directed to do so by Cisco TAC personnel.

- Enable advanced debugging only under the guidance of Cisco TAC personnel because advanced debugging slows the mobility service down.

Configuring Logging Options

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

To configure logging options, follow these steps:

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

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

Step 3   From the System menu, choose **Logs**. The logging options for the selected mobility services engine appear.

Step 4   Choose the appropriate options from the Logging Level drop-down list.
There are four logging options: **Off**, **Error**, **Information**, and **Trace**.

All log records with a log level of **Error** or above are logged to a new error log file locserver-error-%u-%g.log. This is an additional log file maintained along with the location server locserver-%u-%g.log log file. The error log file consists of logs of **Error** level along with their context information. The contextual information consists of 25 log records prior to the error. You can maintain up to 10 error log files. The maximum size allowed for each log file is 10 MB.

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

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

Step 6   Select the **Enable** check box under Advanced Parameters to enable advanced debugging. By default, this option is disabled.
Caution   Enable advanced debugging only under the guidance of Cisco TAC personnel because advanced debugging slows the mobility service down.

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

Step 8   In the Log File group box, 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 page, 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 back up or rollover log file.

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

Downloading Log Files

If you need to analyze mobility services engine log files, you can use Prime Infrastructure to download them to your system. The Prime Infrastructure downloads a .zip file containing the log files.

To download a .zip file containing the log files, follow these steps:

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

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

Step 3   From the left sidebar menu, choose **Logs**.

Step 4   Click **Download Logs**.

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

Generating Reports

In the Prime Infrastructure, you can generate various kinds of reports. This section explains how to generate Context Aware reports using the Prime Infrastructure Report Launch Pad. By default, reports are stored on the Prime Infrastructure server.

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

You can define the following criteria for the reports:

- 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 e-mailed or exported to a file

Report Launch Pad

The report launch pad provides access to all the Prime Infrastructure reports from a single page. In this page, you can view current reports, open specific types of reports, create and save new reports, and manage scheduled runs. You can access the ContextAware reports section in the Report Launch Pad to generate ContextAware reports.

$\mathcal{Q}$

Tip   Hover your mouse cursor over the tool tip next to the report type to view more report details.

This section contains the following topics:

Creating and Running a New Report

To create and run a new report, follow these steps:

Step 1   Choose **Reports** > **Report Launch Pad**.
The reports are listed by category in the main section of the page and on the left sidebar menu.

Step 2   Find the appropriate report in the main section of the Report Launch Pad.
Note   Click the report name from the Report Launch Pad or use the navigation on the left side of the Report Launch Pad page to view any currently saved reports for that report type.

Step 3   Click **New**. The Report Details page appears.

Step 4   In the Report Details page, enter the following Settings parameters:

Note Certain parameters may or may not appear depending on the report type.

- Report Title—If you plan to use this as a saved report, enter a report name.

- Report By—Choose the appropriate Report By category from the drop-down list.

- Report Criteria—Allows you to sort your results depending on the previous Report By selection made. Click Edit to open the Filter Criteria page.

  Note Click **Select to confirm your filter criteria** or Close to return to the previous page.

- Connection Protocol—All Clients, All Wired(802.3), All Wireless (802.11), All 11u Capable Clients, 802.11a/n, 802.11b/g/n, 802.11a, 802.11b, 802.11g, 802.11n (5 GHz), 802.11n (2.4 GHz).

- Reporting Period

  ◦ Select the reporting period from the Select a time period...drop-down list. The possible values are Today, Last 1 Hour, Last 6 Hours, Last 12 hours, Last 1 Day, Last 2 Days, Last 3 days, Last 4 Days, Last 5 Days, last 6 Days, Last 7 Days, Last 2 Weeks, Last 4 weeks, Previous Calendar Month, Last 8 Weeks, Last 12 Weeks, Last 6 Months, and Last 1 Year.

  ◦ From—Select the From radio button and enter the From and To dates and times. You can type a date in the text box, or click the Calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

  ◦ Show—Enter the number of records that you want to be displayed on each page.

  Note Leave the text box blank to display all records.

Step 5 If you plan to run this report at a later time or as a recurring report, enter the Schedule parameters. The Schedule parameters allow you to control when and how often the report runs.

- Scheduling—Select the Enable check box to run the report on the set schedule.

- Export Format—Choose your format for exported files (CSV or PDF).

- Destination—Select your destination type (File or E-mail). Enter the applicable file location or the e-mail address.

  Note The default file locations for CSV and PDF files are as follows:

  /localdisk/ftp/reports/Inventory/<ReportTitleName>_<yyyymmdd>_<HHMMSS>.csv

  /localdisk/ftp/reports/Inventory/,ReportTitleName>_<yyyymmdd>_<HHMMSS>.pdf

  Note To set the mail server setup for e-mails, choose Administration > Settings, then choose Mail Server from the left sidebar menu to view the Mail Server Configuration page. Enter the SMTP and other required information.

- Start Date/Time—Enter a date in the provided text box, or click the calendar icon to open a calendar from which you can choose a date. Choose the time from the hours and minutes drop-down lists. The report begins to run on this data and at this time.

- Recurrence—Enter the frequency of this report.

  ◦ No Recurrence—The report runs only once (at the time indicated for the Start Date/Time).

  ◦ Hourly—The report runs on the interval indicated by the number of hours you enter in the Entry text box.

◦ Daily—The report runs on the interval indicated by the number of days you enter in the Every text box.

◦ Weekly—The report runs on the interval indicated by the number of weeks you enter in the Every text box and on the days specified by the selected check boxes.

◦ Monthly—The report runs on the interval indicated by the number of months you enter in the Every text box.

The Create Custom Report page allows you to customize the report results. The following table specifies which reports are customizable, which have multiple sub-reports, and which report views are available. In future releases, all reports are customizable.

Table 2: Report Customization

Report	Customizable?	Multiple Sub-Reports?	Report Views	Data Field Sorting?
Air Quality vs Time	Yes	No	Tabular	No
Security Risk Interferers	Yes	No	Tabular	No
Worst Air Quality APs	Yes	No	Tabular	No
Worst Interferers	Yes	No	Tabular	No
Busiest Clients	Yes	No	Tabular	No
Client Count	Yes	No	Graphical	No
Client Session	Yes	No	Tabular	No
Client Summary	Yes	Yes	Various	Yes
Client Traffic	Yes	No	Graphical	No
Client Traffic Stream Metrics	Yes	No	Tabular	No
Throughput	No	No	Tabular	No
Unique Clients	Yes	No	Tabular	No
v5 Client Statistics	No	No	Tabular	No
Configuration Audit	Yes	No	Tabular	No
PCI DSS Detailed	Yes	No	Tabular	No
PCI DSS Summary	Yes	No	Graphical	No
AP Profile Status	Yes	No	Tabular	No

Report	Customizable?	Multiple Sub-Reports?	Report Views	Data Field Sorting?
Device Summary	Yes	No	Tabular	No
Busiest APs	Yes	No	Tabular	No
Inventory - Combined Inventory	Yes	Yes	Various	Yes
Inventory - APs	Yes	Yes	Various	Yes
Inventory - Controllers	Yes	Yes	Various	Yes
Inventory - MSEs	Yes	Yes	Various	Yes
Up Time	Yes	No	Tabular	No
Utilization - Controllers	No	No	Graphical	No
Utilization - MSEs	No	No	Graphical	No
Utilization - Radios	No	No	Graphical	No
Guest Account Status	Yes	No	Tabular	No
Guest Association	Yes	No	Tabular	No
Guest Count	No	No	Tabular	No
Guest User Sessions	Yes	No	Tabular	No
Prime Infrastructure Guest Operations	Yes	No	Tabular	No
Alternate Parent	Yes	No	Tabular	No
Link Stats - Link Stats	Yes	No	Tabular	No
Link Stats - Node Hops	Yes	No	Graphical	No
Nodes	Yes	No	Tabular	No
Packet Stats - Packet Stats	No	No	Graphical	No
Packet Stats - Packet Error Stats	No	No	Graphical	No
Packet Stats - Packet Queue Stats	No	No	Graphical	No

Report	Customizable?	Multiple Sub-Reports?	Report Views	Data Field Sorting?
Stranded APs	No	No	Tabular	No
Worst Node Hops - Worst Node Hop	Yes	Yes	Various	No
Worst Node Hops - Worst SNR Link	Yes	Yes	Various	No
802.11n Summary	No	Yes	Graphical	No
Executive Summary	No	Yes	Various	No
802.11 Counters	Yes	No	Both	Yes
Coverage Holes	Yes	No	Tabular	No
Network Utilization	Yes	Yes	Both	Yes
Traffic Stream Metrics	Yes	Yes	Both	Yes
Tx Power and Channel	No	No	Graphical	No
VoIP Calls Graph	No	No	Graphical	No
VoIP Calls Table	No	No	Tabular	No
Voice Statistics	No	No	Graphical	No
Adaptive wIPS Alarm	Yes	No	Tabular	No
Adaptive wIPS Alarm Summary	Yes	No	Both	No
Adaptive wIPS Top 10 APs	Yes	No	Tabular	No
Adhoc Rogue Count Summary	Yes	No	Both	No
Adhoc Rogues	Yes	No	Tabular	No
New Rogue AP Count Summary	Yes	No	Both	No
New Rogue APs	No	No	Graphical	No
Rogue AP Count Summary	Yes	No	Both	No

Report	Customizable?	Multiple Sub-Reports?	Report Views	Data Field Sorting?
Rogue APs	Yes	No	Tabular	No
Security Alarm Trending Summary	Yes	No	Graphical	No

Step 6 Click **Customize** to open a separate Create Custom Report page.

   a) From the Custom Report Name drop-down list, choose the report you intend to run. The Available and Selected column heading selections may change depending on the report selected.

   b) From the Report View drop-down list, specify if the report should appear in tabular, graphical, or combined form (both). This option is not available on every report.

   c) Use the Add > and < Remove buttons to move highlighted column headings between the two group boxes (Available data fields and Data fields to include).
   Note

   Column headings in blue are mandatory in the current sub report. They cannot be removed from the Selected Columns group box.

   d) Use the Change Order buttons (Move Up or Move Down) to determine the order of the columns in the results table. The higher the column heading appears in the Selected Columns list, the farther left it appears in the results table.

   e) In the Data field sorting group box, indicate your sorting preference (Ascending or Descending). Determine how the report data is sorted.

      • You can select four data fields for which you can specify sorting order. Use the Sort by and Then by drop-down lists to select each data field for sorting.

      • For each sorted data field, select whether you want it sorted in Ascending or Descending order.

      Note   Only reports in table form (rather than graphs or combined) can be sorted. Only fields that can be sorted appear in the Data field sorting drop-down lists.

   f) Click **Apply** to confirm the changes, **Reset** to return columns to the default, or **Cancel** to close this page with no changes made.
   Note   The changes made in the Create Custom Report page are not saved until you click Save in the Report Details page.

Step 7 When all report parameters have been set, choose one of the following:

   • Save—Click **Save** to save this report setup without immediately running the report. The report automatically runs at the scheduled time.

   • Save and Run—Click **Save and Run** to save this report setup and to immediately run the report.

   • Run Now—Click **Run Now** to run the report without saving the report setup.

   • Cancel—Click **Cancel** to return to the previous page without running nor saving this report.

Managing Current Reports

If a report has been saved for a specific report type, you can access the current reports from the Report Launch Pad.

To access current or saved reports from the Report Launch Pad, follow these steps:

When a new chokepoint is created, it is available in all the virtual domains. After placing it on a floor, it is updated so that it is available in the same virtual domain as that of a floor. When a chokepoint is removed from a floor, it will be available in all the virtual domains again.

Step 1   Choose **Reports** > **Report Launch Pad**

Step 2   Choose the specific report from the left sidebar menu or from the main section of the Report Launch Pad. The Report Launch Pad page displays a list of current reports for this report type.
To view a list of saved reports, choose **Reports** > **Saved Reports**.

Managing Scheduled Run Results

• Sorting Scheduled Run Results, page 10-18

Note   The list of scheduled runs can be sorted by report category, report type, and time frame.

Managing Saved Reports

In the Saved Reports page, you can create and manage saved reports. To open this page in the Prime Infrastructure, choose Reports > Saved Reports.

Note   The list of saved reports can be sorted by report category, report type, and scheduled status (enabled, disabled, or expired).

The Saved Reports page shows the following information:

• Report Title—Identifies the user-assigned report name.

Note   Click the report title to view the details for this report.

• Report Type—Identifies the specific report type.

• Scheduled—Indicates whether this report is enabled or disabled.

• Next Schedule On—Indicates the date and time of the next scheduled run for this report.

• Last Run—Indicates the date and time of the most recent scheduled run for this report.

• Download—Click the Download icon to open or save a .csv file of the report results.

• Run Now—Click the Run Now icon to immediately run the current report.

Generating MSE Analytics Reports

MSE analytics reports are generated based on location history data. This section lists and describes the various MSE analytics reports that you can generate through the Prime Infrastructure Report Launch Pad.

To generate an MSE analytics report, click New next to a type.

Click a report type to view currently saved reports. In this page, you can enable, disable, delete, or run currently saved reports.

This section describes the MSE Analytics report that you can create and contains the following topics:

Client Location

This report shows historical location information of a wireless client detected by an MSE.

Note The Client Location report is not filtered in non-root virtual domain.

This section contains the following topics:

Configuring a Client Location History Report

The client location history report results are available only in the root domain. To configure a client location history report, follow these steps:

Settings

• Report Title—If you plan to save this report, enter a report name.

• Report By—By default, Client MAC Address is selected.

• Report Criteria—Click Edit and enter a valid MAC address as the filter criteria.

Note In the Report Criteria page, click **Select to confirm your filter criteria** or click **Close** to return to the previous page.

Reporting Period

• Select the radio button and choose a period of time from the drop-down list.

or

- Select the From radio button and enter the From and To dates and times. You can type a date in the text box, or click the Calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

> **Note** The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the Managing Saved Reports, on page 16 for more information on scheduling a report.

Customize Report Form

The Customize Report form allows you to customize the report results. See the Managing Saved Reports, on page 16 for more information on customizing report results.

> **Note** Fixed columns appear in blue font and cannot be moved to the available columns.

Client Location Results

The results of the Client Location History report contain the following information:

- Last Located—The time when the client was located.
- Client Location—The position of the client at the located time.
- MSE—The name of the MSE that located this client.
- User—The username of the client.
- Detecting Controllers—The IP address of the detecting controller.
- 802.11 State—The state of 802.11. It can be either Probing or Associated.
- IP Address—The IP address of the client.
- AP MAC Address—The MAC address of the associated access point.
- Authenticated—Whether authenticated or not. This can be either Yes or No.
- SSID—The SSID used by the client.
- Protocol—The protocol used to retrieve the information from the client.

> **Note** The location field in this report is a hyperlink, and clicking the hyperlink shows the location of the client in the floor map at the located time.

Client Location Density

This report shows wireless clients and their locations detected by the MSEs based on your filtering criteria.

This section contains the following topics:

Configuring a Client Location Density Report

The client location history report results are available only in the root domain. To configure a Client Location History report, follow these steps:

Settings

- Report Title—If you plan to save this report, enter a report name.

- Report By

   ◦ MSE By Floor Area

   ◦ MSE By Outdoor Area

   ◦ MSE

- Report Criteria—The report criteria differ based on the Report By option selected. Click Edit and select the required filter criteria.

> **Note** In the Report Criteria page, click **Select** to confirm your filter criteria or click **Close** to return to the previous page.

- Reporting Period

   ◦ Select the radio button and choose a period of time from the drop-down list.

   or

   ◦ Select the From radio button and enter the From and To dates and times. You can type a date in the text box, or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

> **Note** The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Reporting Period

- Select the radio button and choose a period of time from the drop-down list.

   or

• Select the From radio button and enter the From and To dates and times. You can type a date in the text box, or click the Calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note   The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters.

Customize Report Form

The Customize Report form allows you to customize the report results.

Note   Fixed columns appear in blue font and cannot be moved to the available columns.

Client Location Density Results

The results of the Client Location Density report contain the following information:

• Last Located—The time when the client was last located during the selected Report Time criteria.

• MAC Address—The MAC address of the client.

• Client Location—The position of the client at the located time.

• MSE—The name of the MSE that located the client.

• User—The username of the client.

• Detecting Controllers—The IP address of the detecting controller.

• 802.11 State—The state of 802.11. It can be Probing or Associated.

• IP Address—The IP address of the client.

• SSID—The SSID used by the client

• Protocol—The protocol used to retrieve the information from the client.

Note   The location field in this report is a hyperlink, and clicking that hyperlink shows the location of the client in the floor map at the located time.

Guest Location Density

This report shows guest clients and their locations detected by the MSEs based on your filtering criteria.

This section contains the following topics:

Configuring Guest Location Tracking

This section contains the following topics:

Settings

• Report Title—If you plan to save this report, enter a report name.

• Report by

  ◦ MSE By Floor Area

  ◦ MSE By Outdoor Area

  ◦ MSE

• Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and select the required filter criteria.

> ✎
> **Note** In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

• Reporting Period

  ◦ Select the radio button and a period of time from the drop-down list.

  Or

  ◦ Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box, or click the **Calendar** icon to choose a date. Choose the hours and minutes from the drop-down lists.

  > ✎
  > **Note** The reporting period is based on the alarm last seen. The times are in the UTC time zone.

• **Schedule**

  If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the Managing Saved Reports, on page 16 for more information.

• **Customize Report Form**

  The Customize Report form allows you to customize the report results. See the Managing Saved Reports, on page 16 for more information on scheduling a report.

Guest Location Tracking Results

The results of the Guest Location Tracking report contains the following information:

- Last Located—The time when the guest client was last located during the selected Report Time criteria.

- Guest Username—The login name of the guest client user.

- MAC Address—The MAC address of the guest client.

- Guest Location—Position of the guest client at the located time.

- MSE—Name of the MSE that located this guest client.

- Detecting Controllers—The IP address of the detecting controller.

- IP Address—The IP address of the guest client.

- AP MAC Address—The MAC address of the access point to which the guest client is associated.

- SSID—The SSID used by the guest client.

- Protocol—The protocol used to retrieve the information from the guest client.

> **Note** The location field in this report is a hyperlink and clicking that hyperlink shows the location of the guest in the floor map at the located time.

Location Notifications by Zone

This report shows Context-Aware notifications generated by MSEs.

This section contains the following topics:

Configuring a Location Notification Report

This section describes how to configure a Rogue Client Location Tracking report.

`Settings`

- Report Title—If you plan to save this report, enter a report name.

- Report by
  - MSE By Floor Area
  - MSE By Outdoor Area
  - MSE

• Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and select the required filter criteria.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

• Reporting Period

  ◦ Select the radio button and a period of time from the drop-down list.

  Or

  ◦ Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box, or click the **calendar** icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the Managing Saved Reports, on page 16 for more information on scheduling a report.

Customize Report Form

The Customize Report form allows you to customize the report results. See the Managing Saved Reports, on page 16 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to the Available columns.

Location Notification Results

The results of Location Notification report contains the following information:

• Last Seen—The date and time when the device was last located.

• MAC Address—The MAC address of the device.

• Device Type—The type of the device.

• Asset Name—The name of the asset.

• Asset Group—The name of the asset group.

• Asset Category—The name of the asset category.

• Map Location—The map location where the device was located.

• serverName—The name of the server that sends the ContextAware notifications.

Rogue AP Location Density

This report shows Rogue APs and their locations detected by the MSEs based on your filtering criteria.

This section contains the following topics:

Configuring Rogue AP Location Density

This section describes how to configure a rogue AP location density report and contains the following topics

`Settings`

- Report Title—If you plan to save this report, enter a report name.

- Report By

    ◦ MSE By Floor Area

    ◦ MSE By Outdoor Area

- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and select the required filter criteria.

    Note   In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Device Type

    ◦ All

    ◦ Clinet

    ◦ Tags

    ◦ Rogue Clients

    ◦ Rogue APs

    ◦ Interferers

- `Reporting Period`

    ◦ Select the radio button and choose a period of time from the drop-down list.

    or

    ◦ Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box, or click the **Calendar** icon to choose a date. Choose the hours and minutes from the drop-down lists.

    Note   The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the Managing Saved Reports, on page 16 for more information on scheduling a report.

Customize Report Form

The Customize Report form allows you to customize the report results. See the Managing Saved Reports, on page 16 for more information on customizing report results.

> **Note**   Fixed columns appear in blue font and cannot be moved to the Available columns.

Rogue AP Location Density

This report shows Rogue APs and their locations detected by the MSEs based on your filtering criteria.

This section contains the following topics:

Rogue Client Location Density

This report shows Rogue Client APs and their locations detected by the MSEs based on your filtering criteria.

This section contains the following topics:

Configuring a Rogue Client Location Density

This section describes how to configure a Rogue Client Location Density and contains the following topics:

Settings

- Report Title—If you plan to save this report, enter a report name.
- Report by
    - MSE By Floor Area
    - MSE By Outdoor Area
    - MSE
- Report Criteria—The report criteria differs based on the Report By option selected. Click Edit and select the required filter criteria.

> **Note**   In the Report Criteria page, click Select to confirm your filter criteria or Close to return to the previous page.

- Reporting Period
    - Select the radio button and choose a period of time from the drop-down list.

      or

◦ Select the From radio button and enter the From and To dates and times. You can type a date in the text box, or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

> **Note** The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Reporting Period

• Select the radio button and choose a period of time from the drop-down list.

  or

• Select the From radio button and enter the From and To dates and times. You can type a date in the text box, or click the Calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

> **Note** The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the Managing Saved Reports, on page 16 for more information on scheduling a report.

Customize Report Form

The Customize Report form allows you to customize the report results. See the Managing Saved Reports, on page 16 for more information on customizing report results.

> **Note** Fixed columns appear in blue font and cannot be moved to the available columns.

Rogue Client Location Density

This report shows Rogue Client APs and their locations detected by the MSEs based on your filtering criteria.

This section contains the following topics:

Tag Location

This report shows the location history of a tag detected by an MSE.

This section contains the following topics:

Configuring Tag Location History

This section describes how to configure a tag location history and contains the following topics:

Settings

- Report Title—If you plan save this report, enter a report name.

- Report by

  ◦ MSE By Floor Area

  ◦ MSE By Outdoor Area

  ◦ MSE

- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and select the required filter criteria.

> **Note** In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period

  ◦ Select the radio button and a period of time from the drop-down list.

  Or

  ◦ Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box, or click the **calendar** icon to choose a date. Choose the hours and minutes from the drop-down lists.

> **Note** The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

- **Schedule**

  If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the Managing Saved Reports, on page 16 for more information on scheduling a report.

- **Customize Report Form**

  The Customize Report form allows you to customize the report results. See the Managing Saved Reports, on page 16 for more information on customizing report results.

> **Note** Fixed columns appear in blue font and cannot be moved to the Available columns.

Tag Location Tracking Results

The results of the Tag Location Tracking report contain the following information:

- Last Located—The time when the tag was last located during the selected Report Time criteria.

- Tag Location—The position of the tag at the located time.

- MSE—The name of the MSE that located this tag.

- Detecting Controller—The IP address of the detecting controller.

- Vendor—The name of the tag vendor.

- Battery Status—The status of the battery of that tag.

Note The location field in this report is a hyperlink and clicking that hyperlink shows the location of the tag in the floor map at the located time.

Tag Location Density

This report shows tags and their locations detected by the MSEs based on your filtering criteria.

This section contains the following topics:

Configuring a Tag Location Tracking

This section describes procedures to configure a Tag Location Tracking report and contains the following topics:

Settings

- Report Title—If you plan to save this report, enter a report name.

- Report by

  ◦ MSE By Floor Area.

  ◦ MSE By Outdoor Area

  ◦ MSE

- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and select the required filter criteria.

Note   In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

• Reporting Period

  ◦ Select the radio button and a period of time from the drop-down list.

  Or

  ◦ Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box, or click the **calendar** icon to choose a date. Select the hours and minutes from the drop-down lists.

Note   The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the Managing Saved Reports, on page 16 for more information on scheduling a report.

Customize Report Form

The Customize Report form allows you to customize the report results. See the Managing Saved Reports, on page 16 for more information on customizing report results.

Note   Fixed columns appear in blue font and cannot be moved to the Available columns.

Creating a Device Utilization Report

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

Step 1 Choose **Reports > Report Launch Pad**.

Step 2 Choose **Device > Utilization**.

Step 3 Click **New**. The Utilization Report Details page appears.

Figure 4: Device > Utilization Reports Details Page

Step 4 In the Reports Details page, enter the following Settings parameters:

Note   Certain parameters may or may not work depending on the report type.

- Report Title—If you plan to save this report, enter a report name.

- Report Type—By default, the report type is selected as MSE.

- Report By—Choose the appropriate Report By category from the drop-down list. The categories differ for each report. See specific report sections for Report By categories for each report.

- Report Criteria—The parameter allows you to sort your results depending on the previous Report By selection made. Click **Edit** to open the Filter Criteria page.

- Connection Protocol—Choose either of these protocols: **All Clients**, **All Wired (802.3)**, **All Wireless (802.11)**, **802.11a/n**, **802.11b/g/n**, **802.11a**, **802.11b**, **802.11g**, **802.11n (5-GHz)**, or **802.11n (2.4-GHz)**.

- SSID—All SSIDs is the default value.

- Reporting Period—You can define the report to collect data hourly, weekly, or at a specific date and time. The selected reporting period type is displayed on the x-axis.

Note   The reporting period uses a 24-hour rather than a 12-hour clock. For example, choose **hour 13** for 1:00 p.m.

Step 5   In the Schedule group box, select the **Enable Schedule** check box.

Step 6   Choose the report format (CSV or PDF) from the Export Report drop-down list.

Step 7   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 e-mail address. Choose **Administrator > Settings >** *Mail Server Configuration* to enter the appropriate information.

Step 8   Enter a start date (MM:DD:YYYY), or click the **calendar** icon to select a date.

Step 9   Specify a start time using the hour and minute drop-down list boxes.

Step 10   Select the **Recurrence** radio button to determine how often you want to run the report. The possible values are:

- No Recurrence

- Hourly

- Daily

- Weekly

- Monthly

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

Step 11   When finished with Step 1 to Creating a Device Utilization Report, do one of the following:

- Click **Save** to save edits. The report is run at the designated time and the results are either e-mailed or saved to a designated file as defined in the Schedule group box.

- 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 e-mailed or saved to a designated file as defined in the Schedule group box.

◦ 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 Prime Infrastructure 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 that you entered.

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

Note   Only the CPU and memory utilization reports are shown in the following example.

Figure 5: Devise > MSE Utilization > Results
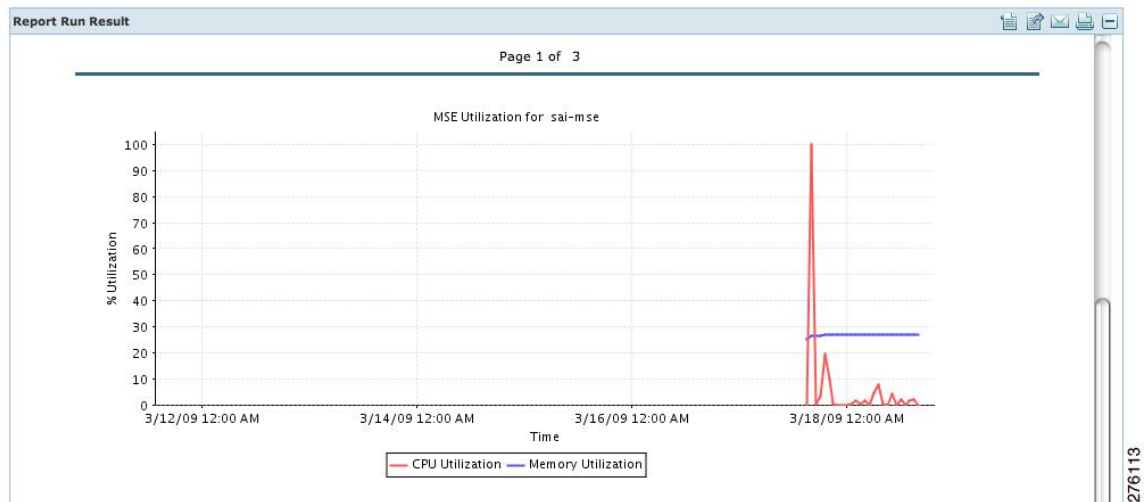
If the report is scheduled, it is shown as enabled and the next scheduled run date is noted.

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 12   To enable, disable, or delete a report, select the check box next to the report title and click the appropriate option.

Viewing Saved Utilization Reports

To download a saved report, follow these steps:

Step 1   Choose **Reports > Saved Reports**.

Step 2   Click the **Download** icon for your report. It is downloaded and saved in the defined directory or e-mailed.

Viewing Scheduled Utilization Runs

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

Step 1   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, e-mailed.

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—Shows all adhoc events that Prime Infrastructure has received in the selected timeframe.

- Adhoc Rogues—Shows all adhocs that have been updated in the selected timeframe.

- New Rogue APs—Shows 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—Shows in graphical form, all rogues detected in a selected timeframe.

    ◦ Rogue APs—Shows all rogues that are active in your network and have been updated in the selected timeframe. Prime Infrastructure receives updated events for rogues that are detected.

- Rogue APs Event—Shows all the events received by Prime Infrastructure. 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 e-mailed 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 contains the following topics:

- Creating a New wIPS Security or Alarms Report
- Viewing Saved wIPS Report
- Viewing Scheduled wIPS Report Runs

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 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.

Figure 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 Criteria. 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 page, 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 e-mail 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 e-mailed or saved to a designated file as defined in the Schedule page.

- 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 e-mailed or saved to a designated file as defined in the Schedule page.

  ◦ 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 Prime Infrastructure 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.

1 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 Prime Infrastructure, choose **Reports > Saved Reports**.

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

Viewing Scheduled wIPS Report Runs

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

Step 1 In Prime Infrastructure, 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, e-mailed.

Client Support on the MSE

You can use the Prime Infrastructure Advanced Search feature to narrow the client list based on specific categories and filters. You can also filter the current list using the Show drop-down list.

This section contains the following topics:

- Searching a Wireless Client from the Prime Infrastructure on the MSE by IPv6 Address
- Viewing the Clients Detected by the MSE

Searching a Wireless Client from the Prime Infrastructure on the MSE by IPv6 Address

To search for an MSE-located client using the Prime Infrastructure Advanced Search feature, follow these steps:

Step 1 Click **Advanced Search** located in the top right corner of the Prime Infrastructure UI.

Step 2 In the New Search dialog, choose **Clients** as the search category from the Search Category drop-down list.

Step 3 From the Media Type drop-down list, choose **Wireless Clients**.
Note The Wireless Type drop-down list appears only when you choose Wireless Clients as the media type.

Step 4 From the Wireless Type drop-down list, choose any of the following types: **All**, **Lightweight,** or **Autonomous Clients**.

Step 5 From the Search By drop-down list, choose **IP Address**.
Note Searching a client by IP address can contain either a full or partial IP address. Each client can have up to 16 IPv6 addresses and 4 IPv4 addresses.

Step 6 From the Clients Detected By drop-down list, choose **clients detected by MSE**.
This shows clients located by Context-Aware Service in the MSE by directly communicating with the controllers.

Step 7 From the Last detected within drop-down list, choose the time within which the client was detected.

Step 8 Enter the client IP address in the Client IP Address text box. You can enter wither a partial or full IPv6 address.

> **Note** If you are searching for the client from Prime Infrastructure on the MSE by IPV4 address, enter the IPV4 address in the Client IP Address text box.

Step 9 From the Client States drop-down list, choose the client states. The possible values for wireless clients are **All States**, **Idle**, **Authenticated**, **Associated**, **Probing**, or **Excused**. The possible values for wired clients are **All States**, **Authenticated**, and **Associated**.

Step 10 From the Posture Status drop-down list, choose the posture status to know if the devices are clean or not. The possible values are **All**, **unknown**, **Passed**, and **Failed**.

Step 11 Select the **CCX Compatible** check box to search for clients that are compatible with Cisco Client Extensions. The possible values are **All Versions**, **V1**, **V2**, **V3**, **V4**, **V5**, and **V6**.

Step 12 Select the **E2E Compatible** check box to search for clients that are End to End compatible. The possible values are **All Versions**, **V1**, and **V2**.

Step 13 Select the **NAC State** check box to search for clients identified by a certain Network Admission Control (NAC) state. The possible values are **Quarantine**, **Access**, **Invalid**, and **Not Applicable**.

Step 14 Select the **Include Disassociated** check box to include clients that are no longer on the network but for which Prime Infrastructure has historical records.

Step 15 From the **Items per page** drop-down list, choose the number of records to be displayed in the search results page.

Step 16 Select the **Save Search** check box to save the selected search option.

Step 17 Click **Go**.
The Clients and Users page appears with all the clients detected by the MSE.

Viewing the Clients Detected by the MSE

To view all the clients detected by MSE, follow these steps:

Step 1 Choose **Monitor** > **Clients and Users** to view both wired and wireless clients information.
The Client and Users page appears.

The Clients and Users table shows a few column by default. If you want to display the additional columns that are available, click ⚙ ▾, and then click **Columns**. The available columns appear. Select the columns that you want to show in the Clients and Users table. When you click anywhere in a row, the row is selected and the client details are shown.

Step 2 Filter the current list to choose all the clients that are detected by MSE by choosing **Clients detected by MSE** from the Show drop-down list.
All the clients detected by MSE including wired and wireless appear. All the clients detected by MSE including wired and wireless appear.

The following different parameters are available in the Clients Detected by MSE table:

- MAC Address—Client MAC address.

  - IP Address—Client IP address.

The IP address that appears in the IP Address column is determined by a predefined priority order. The first IP address available in the following order appears in the IP address text box:

- IPv4 address

  Note Only wireless clients have IPv6 addresses in this release. Each client can have up to 16 IPv6 addresses and 4 IPv4 addresses.

- IPv6 global unique address. If there are multiple addresses of this type, most recent IPv6 address that the client received is shown, because a user might have two Global IPv6 addresses but one might have been from an older Router Advertisement that is being aged out.

- IPv6 local unique address, if there are multiple then the most recent IPV6 local unique address is used by the client.

- IPv6 link local address. For an IPv6 address of the client which is self-assigned and used for communication before any other IPV6 address is assigned.

  The following are the different IPv6 address types:

- Link-local Unicast—The link-local addresses are designed to be used for addressing on a single link for purposes such as auto-address configuration, neighbor discovery, or when no routers are present.

- Site-local Unicast—The site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix.

- Aggregatable Global Unicast—The aggregatable global unicast address uniquely identifies the client in global network and equivalent to public IPv4 address. A client can have multiple aggregatable global unicast addresses.

- IP Type—The IP address type of the client. The possible options are IPv4, IPv6, or Dual-stack that signifies a client with both a IPV4 and IPV6 addresses.

  - Global Unique

  - Unique Local

  - Link Local

- User Name—Username based on 802.1x authentication. Unknown is displayed for client connected without a username.

- Type—Indicates the client type.

- Vendor—Device vendor derived from OUI.

- Device Name—Network authentication device name. For example, WLC and switch.

- Location—Map location of the connected device.

- VLAN—Indicates the access VLAN ID for this client.

- Status—Current client status.

  - Idle—Normal operation; no rejection of client association requests.

  - Auth Pending—Completing a AAA transaction.

  - Authenticated—802.11 authenticated complete.

- ◦ Associated—802.11 association complete. This is also used by wired clients to represent that a client is currently connected to the network.

- ◦ Disassociated—802.11 disassociation complete. This is also used by wired clients to represent that a client is currently not on the network.

- ◦ To Be Deleted—The client is deleted after disassociation.

- ◦ Excluded—Automatically disabled by the system due to perceived security threat.

- Interface—Controller interface (wireless) or switch interface (wired) that the client is connected to.

- Protocol

  - ◦ 802.11—Wireless

  - ◦ 802.3—Wired

- Association Time—Last association start time (for wireless client). For a wired client, this is the time when a client is connected to a switch port. This is blank for a client which is associated but has problems being on the network.

- CCX—Lightweight wireless only.

  - ◦ Select the radio button next to MAC Address in the Client and User page to view the associated client information. The following are the different client parameters that appear.

- Client attributes

- Client IPV6 Addresses

- Client Statistics

  Note   Client Statistics shows the statistics information after the client details are shown.

- Client Association History

- Client Event Information

- Client Location Information

- Wired Location History

- Client CCX Information

- Client Attributes

When you select a client from the Clients and Users list, the following client details are displayed. Clients are identified using the MAC address.

- General—Lists the following information:

  - ◦ User Name

  - ◦ IP Address

  - ◦ MAC address

  - ◦ Vendor

- ◦ Endpoint Type

- ◦ Client Type

- ◦ Media Type

- ◦ Mobility Role

- ◦ Hostname

- ◦ E2E

- ◦ Foundation Service

- ◦ Management Service

- ◦ Voice Service

- ◦ Location Service

- Session—Lists the following information:

  - ◦ Controller Name

  - ◦ AP Name

  - ◦ AP IP Address

  - ◦ AP Type

  - ◦ AP Base Radio MAC

  - ◦ Anchor Address

  - ◦ 802.11 State

  - ◦ Association ID

  - ◦ Port

  - ◦ Interface

  - ◦ SSID

  - ◦ Profile Name

  - ◦ Protocol

  - ◦ VLAN ID

  - ◦ AP Mode

- Security (wireless and Identity wired clients only)—Lists the following security information:

  - ◦ Security Policy Type

  - ◦ EAP Type

  - ◦ On Network

  - ◦ 802.11 Authentication

- ◦ Encryption Cipher

- ◦ SNMP NAC State

- ◦ RADIUS NAC State

- ◦ AAA Override ACL Name

- ◦ AAA Override ACL Applied Status

- ◦ Redirect URL

- ◦ ACL Name

- ◦ ACL Applied Status

- ◦ FlexConnect Local Authentication

- ◦ Policy Manager State

- ◦ Authentication ISE

- ◦ Authorization Profile Name

- ◦ Posture Status

- ◦ TrustSec Security Group

- ◦ Windows AD Domain

  Note   The identity clients are clients whose authentication type is 802.1x, MAC Auth Bypass or Web Auth. For non-identity clients, the authentication type is N/A.

  Note   The data that appears under the client attributes differs based on identity and non-identity clients. For identity clients, you can see the security information such as Authentication status, Audit Session ID, and so on.

- • Statistics (wireless only)

- • Traffic—Shows the client traffic information.

- • For wireless clients, client traffic information comes from the controller. For wired clients, the client traffic information comes from the ISE, and you must enable accounting information and other necessary functions on the switches.

  Statistics

The **Statistics** group box contains the following information for the selected client:

- • Client AP Association History.

- • Client RSSI History (dBm)—History of RSSI (Received Signal Strength Indicator) as detected by the access point with which the client is associated.

- • Client SNR History—History of SNR (signal-to-noise ratio of the client RF session) as detected by the access point with which the client is associated.

- • Bytes Sent and Received (Kbps)—Bytes sent and received with the associated access point.

- • Packets Sent and Received (per sec)—Packets sent and received with the associated access point.

- • Client Data rate

This information is presented in interactive graphs.

Client IPV6 Addresses

The Client IPv6 Address group box contains the following information for the selected client:

- IP Address—Shows the client IPv6 address.

- Scope—Contains 3 scope types: Global Unique, Local Unique, and Link Local.

- Address Type—Shows the address type.

- Discovery Time—Time when the IP was discovered.

  Association History

  The association history group box shows information regarding the last ten association times for the selected client. This information helps in troubleshooting the client.

  - Association Time

  - Duration

  - User Name

  - IP Address

  - IP Address Type

  - AP Name

  - Controller Name

  - SSID

  Events

The Events group box in the Client Details page displays all events for this client including the event type as well as the date and time of the event:

- Event Type

- Event Time

- Description

  Map

Click **View Location History** to view the location history details of wired and wireless clients.

The following location history information is displayed for a wired or wireless client:

- Timestamp

- State

- Port Type

- Slot

- Module

- Port

- User Name

- IP Address

- Switch IP

- Server Name

- Map Location Civic Location

Configuring Buildings

You can add buildings to the Prime Infrastructure database regardless of whether you have added campus maps to the database. This section describes how to add a building to a campus map or a standalone building (one that is not part of a campus) to the Prime Infrastructure database.

This section contains the following topics:

Adding a Building to a Campus Map

To add a building to a campus map in the Prime Infrastructure database, follow these steps:

Step 1   Choose **Monitor** > **Site Maps** to display the Maps page.

Step 2   Click the desired campus. The **Site Maps** > **Campus Name** page appears.

Step 3   From the Select a command drop-down list, choose **New Building** and click **Go**.

Step 4   In the Campus Name > New Building page, follow these steps to create a virtual building in which to organize related floor plan maps:

a)   Enter the building name.
b)   Enter the building contact name.
c)   Enter the number of floors and basements.
d)   Enter the horizontal position (distance from the corner of the building rectangle to the left edge of the campus map) and the vertical position (distance from the corner of the building rectangle to the top edge of the campus map) in feet.

> **Note** To change the unit of measurement (feet or meters), choose **Monitor** > **Site Maps** and choose **Properties** from the Select a command drop-down list.

e) Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet.
Note

The horizontal and vertical span should be larger than or the same size as any floors that you might add later.

> **Tip** You can also use **Ctrl-click** to resize the bounding area in the upper-left corner of the campus map. As you change the size of the bounding area, the Horizontal Span and Vertical Span parameters of the building change to match your actions.

f) Click **Place** to put the building on the campus map. The Prime Infrastructure creates a building rectangle scaled to the size of the campus map.

g) Click the building rectangle and drag it to the desired position on the campus map.
> **Note** After adding a new building, you can move it from one campus to another without having to recreate it.

h) Click **Save** to save this building and its campus location to the database. The Prime Infrastructure saves the building name in the building rectangle on the campus map.
> **Note** A hyperlink associated with the building takes you to the corresponding Map page.

Step 5 (Optional) To assign location presence information for the new outdoor area, do the following:

a) Choose **Edit Location Presence** Info from the Select a command drop-down list. Click **Go**. The Location Presence page appears.
> **Note** By default, the Presence Info check box of the Override Child Element is selected. This option should remain selected if you want to propagate the campus location to all buildings and floors on that campus. When adding buildings to the campus map, you can import the campus location information. The campus address cannot be imported to a building if the check box is unselected. This option should be unselected if you want to assign building-specific addresses to buildings on its campus rather than one campus address to all.

b) Click the **Civic Address**, or **Advanced** tab.

- Civic Address identifies the campus by name, street, house number, house number suffix, city (address line2), state, postal code, and country.

- Advanced identifies the campus with expanded civic information such as neighborhood, city division, country, and postal community name.

c) By default, the **Override Child's Presence Information** check box is selected. There is no need to alter this setting for standalone buildings.

Step 6 Click **Save**.

Adding a Standalone Building

To add a standalone building to the Prime Infrastructure database, follow these steps:

Step 1   Choose **Monitor** > **Site Maps** to display the Maps page.

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

Step 3   In the Maps > New Building page, follow these steps to create a virtual building in which to organize related floor plan maps:

a) Enter the building name.

b) Enter the building contact name.
   Note   After adding a new building, you can move it from one campus to another without having to recreate it.

c) Enter the number of floors and basements.

d) Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet.
   Note   To change the unit of measurement (feet or meters), choose **Monitor** > **Site Maps** and choose **Properties** from the Select a command drop-down list.
   Note   The horizontal and vertical span should be larger than or the same size as any floors that you might add later.

e) Click **OK** to save this building to the database.

Step 4   (Optional) To assign location presence information for the new building, do the following:

a) Choose **Location Presence** from the Select a command drop-down list. Click **Go**. The Location Presence page appears.

b) Click the **Civic**, **GPS Markers**, or**Advanced** tab.

   • Civic Address identifies the campus by name, street, house number, house number suffix, city (address line2), state, postal code, and country.

   • GPS Markers identify the campus by longitude and latitude.

   • Advanced identifies the campus with expanded civic information such as neighborhood, city division, country, and postal community name.

   Note   Each selected parameter is inclusive of all of those above it. For example, if you select Advanced, it can also provide GPS and Civic location information upon client demand. The selected setting must match what is set on the location server level (Services > Mobility Services).
   Note   If a client requests location information such as GPS Markers for a campus, building, floor, or outdoor area that is not configured for that parameter, an error message is returned.

c) By default, the Presence Info check box of the Override Child Element is selected. This option should remain selected if you want to propagate the campus location to all buildings and floors on that campus. When adding buildings to the campus map, you can import the location information. The campus address cannot be imported to a building if the check box is unselected. This option should be deselected if you want to assign building-specific addresses to buildings on its campus rather than one campus address to all.

Step 5   Click **Save**.
   Note   The standalone buildings are automatically placed in System Campus.

Viewing a Building

To view a current building map, follow these steps:

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

Step 2 Click the name of the building map to open its details page. The Building View page provides a list of floor maps and map details for each floor.

Note From the Building View page, you can click the Floor column heading to sort the list ascending or descending by floor.

The map details include the following:

- Floor area

- Floor index—Indicates the floor level. A negative number indicates a basement floor level

- Contact

- Status—Indicates the most serious level of alarm on an access point located on this map or one of its children.

- Number of total access points located on the map.

- Number of 802.11a/n and 802.11b/g/n radios located on the map.

- Number of out of service (OOS) radios.

- Number of clients—Click the number link to view the Monitor > Clients page.

Step 3 The Select a command drop-down list provides the following options:

- New Floor Area—See the Adding a Building to a Campus Map, on page 44for more information.

- Edit Building—See the Editing a Building, on page 47for more information.

- Delete Building—See the Deleting a Building, on page 48for more information.

Editing a Building

To edit a current building map, follow these steps:

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

Step 2 Click the name of the building map to open its details page.

Step 3 From the Select a command drop-down list, choose **Edit Building**.

Step 4 Make any necessary changes to Building Name, Contact, Number of Floors, Number of Basements, and Dimensions (feet).

Note To change the unit of measurement (feet or meters), choose **Monitor** > **Site Maps**, and choose **Properties** from the Select a command drop-down list.

Step 5 Click **OK**.

Deleting a Building

To delete a current building map, follow these steps:

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

Step 2 Select the check box for the building that you want to delete.

Step 3 Click **Delete** at the bottom of the map list (or choose **Delete Maps** from the Select a command drop-down list, and click **Go**).

Step 4 Click **OK** to confirm the deletion.

Note Deleting a building also deletes all of its container maps. The access points from all deleted maps are moved to an Unassigned state.

Moving a Building

To move a building to a different campus, follow these steps:

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

Step 2 Select the check box of the applicable building.

Step 3 From the Select a command drop-down list, choose **Move Buildings**.

Step 4 Click **Go**.

Step 5 Choose the **Target Campus** from the drop-down list.

Step 6 Select the buildings that you want to move. Unselect any buildings that remain in their current location.

Step 7 Click **OK**.

Monitoring Geo-Location

The MSE provides physical location of wired clients, wired endpoints, switches, controllers, and access points present in a wireless network deployment. Currently, MSE provides location information in geo-location format to the external entities through northbound and southbound entities.

To improve the accuracy of the geo-location information provided by MSE, this feature aims to transform the geometric location co-ordinates of a device to geo-location coordinates (latitude and longitude) and provides it to the external entities through northbound and southbound interfaces.

✎

| Note | At least three GPS markers are required for geo-location calculation. The maximum number of GPS markers that you can add is 20. |

This section contains the following topics:

Adding a GPS Marker to a Floor Map

To add a GPS marker to a floor map, follow these steps:

Step 1 Choose **Monitor** > **Site Maps** to display the Maps page.

Step 2 Choose **Campus Name** > **Building Name** > **Floor Name**.

Step 3 Choose the **Add/Edit GPS Markers** Information menu option on the top left menu to open the Add/Edit GPS page. A GPS Marker icon appears on the top left corner of the map (X=0 Y=0).

Step 4 You can drag the GPS Marker icon and place it in the desired location on the map or enter the X and Y position values in the GPS Marker Details table on the left sidebar menu to move the marker to the desired position.

    Note   If the markers added are too close, then the accuracy of geo-location information is less.

Step 5 Enter the Latitude and Longitude degrees for the selected GPS Marker icon in the left sidebar menu.

Step 6 Click **Save.** The GPS Marker information is saved to the database.

Step 7 Click **Apply to other Floors of Building** to copy GPS markers on one floor of a building to all the remaining floors of that building.

Editing a GPS Marker

To edit a GPS marker present on the floor, follow these steps:

Step 1 Choose **Monitor** > **Site Maps** to display the Maps page.

Step 2 Choose **Campus Name** > **Building Name** > **Floor Name**.

Step 3 Choose the **Add/Edit GPS Markers Information** menu option to open the Add/Edit GPS page.

Step 4 Select an existing GPS Marker which is present on the floor from the left sidebar menu.

Step 5 From the left sidebar menu, you can change the Latitude, Longitude, X Position, and Y Position which is associated with the GPS marker.

Step 6 Click **Save**.
The modified GPS marker information is now saved to the database.

Deleting a GPS Marker From theFloor

To delete a GPS marker from the floor, follow these steps:

Step 1 Choose **Monitor** > **Site Maps** to display the Maps page.

Step 2 Choose **Campus Name** > **Building Name** > **Floor Name**.

Step 3 Choose the **Add/Edit GPS Markers Information** menu option to open the Add/Edit GPS page.

Step 4 Select an existing GPS marker that is present on the floor from the left sidebar menu.
Note   You can delete multiple GPS markers present on a floor by selecting the **Multiple GPS Markers** check box.

Step 5 Click **Delete GPS Marker**.
The selected GPS marker is deleted from the database.

Ekahau Site Survey Integration

Ekahau Site Survey (ESS) tool is used for designing, deploying, maintaining, and troubleshooting high performance Wi-Fi networks. ESS works over any 802.11 network and is optimized for centrally managed 802.11n Wi-Fi networks.

You can use the ESS tool to import the existing floor maps from the Prime Infrastructure and export the project to the Prime Infrastructure. For more information, see the Cisco Prime Infrastructure Integration section on the ESS online help or access the user guide at: C:\Program Files\Ekahau\Ekahau Site Survey\doc.

Note The Prime Infrastructure site survey calibration requires that you have collected at least 150 survey data points at 50 distinct locations. If you do not have enough survey data points, a warning is given when trying to export the survey data.

Note If there are no access points in the Prime Infrastructure during the site survey, the site survey will not happen.

Note If the floor map scales are incorrect in the Prime Infrastructure, the visualizations in the ESS will be distorted.

AirMagnet Survey and Planner Integration

AirMagnet survey and AirMagnet planner is integrated with the Cisco Prime Infrastructure. This integration increases the operational efficiencies by eliminating the need to repeat the wireless planning and site survey tasks commonly associated with deployment and management of wireless LAN networks.

The AirMagnet survey tool allows you to export real world survey data to the Prime Infrastructure for calibrating planner modeling. With the AirMagnet planner, you can create and export planner projects directly to the Prime Infrastructure. This enables the Prime Infrastructure to create its own project directly from the imported AirMagnet Planner tool. For more information, see AirMagnet Survey and Planning documentation.