



## Monitoring the System and Services

---

This chapter describes how to monitor the Cisco 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.

- [Working with Alarms, page 2](#)
- [Working with Events, page 6](#)
- [Working with Logs, page 7](#)
- [Generating Reports, page 9](#)
- [Generating MSE Analytics Reports, page 15](#)
- [Creating a Device Utilization Report, page 32](#)
- [Managing OUI, page 34](#)
- [Monitoring Wireless Clients, page 35](#)
- [Client Support on the MSE, page 39](#)
- [Configuring Buildings, page 46](#)
- [Monitoring Tags, page 50](#)
- [Monitoring Geo-Location, page 54](#)
- [Monitoring Chokepoints, page 55](#)
- [Monitoring Wi-Fi TDOA Receivers, page 56](#)
- [Ekahau Site Survey Integration, page 57](#)
- [AirMagnet Survey and Planner Integration, page 58](#)
- [Monitoring Wired Clients, page 58](#)
- [Monitoring Wired Switches, page 59](#)
- [Monitoring Interferers, page 60](#)
- [Clustering of Monitor Mode APs Using MSE, page 62](#)

# 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.

- [Guidelines and Limitations](#), on page 2
- [Viewing Alarms](#), on page 2
- [Monitoring Cisco Adaptive wIPS Alarm Details](#), on page 3
- [Assigning and Unassigning Alarms](#), on page 5
- [Deleting and Clearing Alarms](#), on page 5
- [E-mailing Alarm Notifications](#), on page 6

## 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.
- 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](#).

## Monitoring Cisco Adaptive wIPS Alarm Details

To view MSE alarm details, follow these steps:

Choose **Monitor** > **Alarms** > *failure object* to view details of the selected Cisco wIPS alarm. The following alarm details are provided for Cisco Adaptive wIPS alarms:

- **General Properties**—The general information might vary depending on the type of alarm. For example, some alarm details might include location and switch port tracing information. The following table describes the general parameters associated with the MSE Alarm and wIPS Traps condition.
  - **Detected By wIPS AP**—The access point that detected the alarm.
  - **wIPS AP IP Address**—The IP address of the wIPS access point.
  - **Owner**—Name of person to which this alarm is assigned or left blank.
  - **Acknowledged**—Displays whether or not the alarm is acknowledged by the user.
  - **Category**—For wIPS, the alarm category is Security.
  - **Created**—Month, day, year, hour, minute, second, AM or PM that the alarm was created.
  - **Modified**—Month, day, year, hour, minute, second, AM or PM that the alarm was last modified.
  - **Generated By**—Indicates how the alarm event was generated (either NMS or from a trap).
    - NMS (Network Management System - Prime Infrastructure)—Generated through polling. Prime Infrastructure periodically polls the Cisco WLCs and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events. In this case, "Generated by" NMS.
    - Trap—Generated by the controller. Prime Infrastructure processes these traps and raises corresponding events for them. In this case, "Generated by" is controller.
  - **Severity**—Level of severity including critical, major, minor, warning, and clear.
  - **Last Disappeared**—The date and time that the potential attack last disappeared.
  - **Channel**—The channel on which the potential attack occurred.
  - **Attacker Client/AP MAC**—The MAC address of the client or access point that initiated the attack.
  - **Attacker Client/AP IP Address**—The IP address of the client or access point that initiated the attack.

- Target Client/AP IP Address—The IP address of the client or access point targeted by the attacker.
  - Controller IP Address—The IP address of the controller to which the access point is associated.
  - MSE—The IP address of the associated Mobility Services Engine.
  - Controller MAC address—The MAC address of the controller to which the access point is associated.
  - wIPS access point MAC address
  - Forensic File
  - Event History—Takes you to the Monitoring Alarms page to view all events for this alarm.
- Annotations—Enter any new notes in this text box and click **Add** to update the alarm. Notes appear in the "Annotations" display area.
  - Messages—Displays the alarm name.
  - Description—Displays the consolidated information about the alarm.
  - Mitigation Status—Displays what mitigation action was initiated against the attack.
  - Audit Report—Click to view config audit alarm details. This report is only available for Config Audit alarms.

Configuration audit alarms are generated when audit discrepancies are enforced on config groups.




---

**Note** If enforcement fails, a critical alarm is generated on the config group. If enforcement succeeds, a minor alarm is generated on the config group. The alarms have links to the audit report where you can view a list of discrepancies for each controller.

---

- Event History—Opens the MSE Alarm Events page to view events for this alarm. When there are multiple alarm pages, the page numbers appear at the top of the page with a scroll arrow on each side. Use these scroll arrows to view additional alarms.
- Rogue Clients—If the failure object is a rogue access point, information about rogue clients is displayed.
- Map Location—Displays the map location for the alarm.
  - Floor—The location where this attack was detected.
  - Last Located At—The last time where the attack was located.
  - On MSE—The mobility server engine in which this attack was located.
  - Location History—Click the Location History to see details on the current attacker and victim location.

**Note**

---

Out of all the alarms reported by wIPS, the following four alarms are detected at the wIPS server in the Mobility Services Engine (MSE) and not in the access point. For these alarms, currently there is no location information present. The list of alarms are:

- 124 Hotspotter tool detected
  - 133 Day-Zero attack by device security anomaly
  - 135 Day-Zero attack by WLAN security anomaly
  - 138 Unauthorized association by vendor list
- 

- Related Alarm List—Lists all the alarms related to a particular attack. This shows what consolidation rule was used to consolidate the alarms.
  - Alarm Name—Name of the alarm.
  - First Heard—Indicates the date and time when the attack first seen.
  - Last Heard—Indicates the date and time when the attack was last seen.
  - Status—Status of the attack.

## 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** Choose **Assign > Assign to Me (or Unassign)**.

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** Select the alarms by selecting their corresponding check boxes. Click **Email Notification**. The Email Notification page appears.
    - 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 [Displaying Location Notification Events](#) procedure.

## 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 lists box. 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.

- [Guidelines and Limitations](#), on page 7
- [Configuring Logging Options](#), on page 7
- [MAC address-based Logging](#), on page 8
- [Downloading Log Files](#), on page 9

## 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 Engines**.
- Step 2** Click the name of the MSE that you want to configure.
- Step 3** From the System menu, choose **Logs**. The logging options for the selected MSE 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 **Enable** 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 the [Downloading Log Files](#).
- Step 8** In the Log File group box, enter the following:
- The number of log files to be maintained in the MSE. You can maintain a minimum of 5 log files and a maximum of 20 log files in the MSE.
  - 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 the [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.

**Tip**

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

- [Creating and Running a New Report](#), on page 10
- [Managing Current Reports](#), on page 12
- [Managing Scheduled Run Results](#), on page 12
- [Managing Saved Reports](#), on page 13

## 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.

For the more information on the customizable reports, see *Cisco Prime Infrastructure User Guide*.

**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.

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.

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

**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



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

## Sorting Scheduled Run Results

You can use the Show drop-down list to sort the Scheduled Run Results by category, type, and time frame:

- **Report Category**—Choose the appropriate report category from the drop-down list or choose All.
- **Report Type**—Choose the appropriate report type from the drop-down list or choose All. The report Type selections change depending on the selected report category.
- **From/To**—Type the report start (From) and end (To) dates in the text boxes, or click the calendar icons to select the start and end dates.
- **Report Generation method**—Choose the appropriate report generation method from the drop-down list. The possible methods are Scheduled, On-demand Export, and On-demand Email.

Click Go to sort this list. Only reports that match your criteria appear.

## Viewing or Editing Scheduled Run Details

To view or edit a saved report, follow these steps:

- 
- Step 1** Choose **Report > Scheduled Run Results**.
  - Step 2** Click the **Report Title** link for the appropriate report to open the Report Details page.
  - Step 3** In this page, you can view or edit the details for the scheduled run.
  - Step 4** When all scheduled run parameters have been edited (if necessary), select from the following:
- 

- **Save**—Click **Save** to save this schedule run without immediately running the report. The report automatically runs at the scheduled time.
- **Save and Run**—Click **Save and Run** to save this scheduled run and to immediately run the report.
- **Cancel**—Click **Cancel** to return to the previous page without running nor saving this report.
- **Delete**—Click **Delete** to delete the current saved report.

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

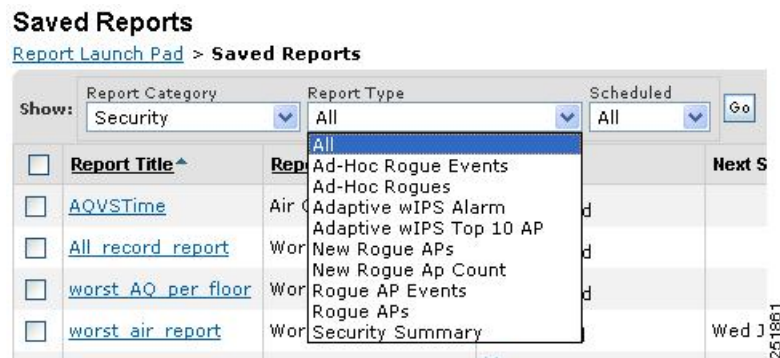
- Report Type—Identifies the specific report type.
- Scheduled—Indicates whether this report is enabled or disabled.
- Next Schedule On—Indicates the date and time of the next scheduled run for this report.
- Last Run—Indicates the date and time of the most recent scheduled run for this report.
- Download—Click 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.

## Sorting Saved Reports

You can use the Show drop-down lists to sort the Saved Reports list by category, type, and scheduled status.

- Report Category—Choose the appropriate report category from the drop-down list or choose **All**.
- Report Type—Choose the appropriate report type from the drop-down list or choose **All**. The Report Type selections change depending on the selected report category.
- Scheduled—Choose **All**, **Enabled**, **Disabled**, or **Expired** to sort the Saved Reports list by scheduled status.

**Figure 1: Sorting Saved Reports**



Click **Go** to sort this list. Only reports that match your criteria appear.

## Viewing or Editing Saved Report Details

To view or edit a saved report, follow these steps:

- Step 1** Choose **Report > Saved Reports**.
- Step 2** Click the **Report Title** link for the appropriate report to open the Report Details page.
- Step 3** In the Report Details page, you can view or edit the details for the saved report.
- Step 4** When all report parameters have been edited, 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.
  - **Delete**—Click **Delete** to delete the current saved 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:

- [Associated vs. Probing Clients by Selected Zone, on page 15](#)
- [Client Location, on page 16](#)
- [Client Location Density, on page 17](#)
- [Device Count by Zone, on page 19](#)
- [Device Dwell Time by Zone, on page 21](#)
- [Guest Location Density, on page 22](#)
- [Location Notifications by Zone, on page 24](#)
- [Mobile MAC Statistics, on page 25](#)
- [Rogue AP Location Density, on page 27](#)
- [Rogue Client Location Density, on page 28](#)
- [Tag Location Tracking, on page 30](#)

### Associated vs. Probing Clients by Selected Zone

This report provides counts for associated vs. probing clients in the selected time period on a selected zone. The first part of the report shows the count in a time series chart and the other part shows the distribution of the clients on the floor.

This section contains the following topics:

- [Configuring a associated vs. probing clients by selected zone report](#)

- Associated vs. Probing client report results

## 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 the non-root virtual domain.

---

This section contains the following topics:

- [Configuring a Client Location History Report, on page 16](#)
- [Client Location Results, on page 17](#)

## 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 13](#) 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 13 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 Cisco WLCs—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. If the previous and current client location calculation is greater than 20 feet which is a configurable parameter, then the location history report is updated. This calculation is done every 30 to 120 seconds depending on the client.

---

## 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](#), on page 18
- [Client Location Density Results](#), on page 19

## 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. 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.

---

### 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 Cisco WLCs—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.

---

## Device Count by Zone

This report provides the count of devices detected by an MSE in the selected zone.

This sections contains the following topics:

- [Configuring a Device Dwell by Zone Report](#), on page 19
- [Device Count by Zone Results](#), on page 21

## Configuring a Device Dwell by Zone Report

This section describes how to configure a Device Dwell Count Time by Zone report and contains the following topics:

### Settings

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

---

- 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 see. 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.

---

## Device Count by Zone Results

The results of the Device Count by Zone report contain the following information:

- MSE—The name of the MSE that located this client.
- Zone—Device count by zone results.
- Device Type—Type of the device.
- MSE Analytics Report Link—Link to get the MSE analytics report.

## Device Dwell Time by Zone

This report provides the Dwell Time Report for a device detected by an MSE.

- [Configuring a Device Dwell Time by Zone Report](#)
- [Device Count by Zone Results](#), on page 21

## Configuring a Device Dwell by Zone Report

This section describes how to configure a Device Dwell Count Time by Zone report and contains the following topics:

### Settings

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

---

- 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 see. 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.

---

## Device Count by Zone Results

The results of the Device Count by Zone report contain the following information:

- MSE—The name of the MSE that located this client.
- Zone—Device count by zone results.
- Device Type—Type of the device.
- MSE Analytics Report Link—Link to get the MSE analytics report.

## Guest Location Density

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

- [Configuring Guest Location Density](#), on page 22
- [Guest Location Density Results](#), on page 23

## Configuring Guest Location Density

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 13](#) for more information.

- **Customize Report Form**

The Customize Report form allows you to customize the report results. See the [Managing Saved Reports, on page 13](#) for more information on scheduling a report.

## Guest Location Density 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—The position of the guest client at the located time.
- MSE—The 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, on page 24](#)
- [Location Notification Results, on page 25](#)

## 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 13](#) 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 13](#) 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.

## Mobile MAC Statistics

This report shows the most active mobile Mac statistics based on click count by MSAP servers or by venues.

- [Configuring Mobile MAC Statistics, on page 26](#)
- [Mobile MAC Tracking Results, on page 27](#)

## Configuring Mobile MAC Statistics

This section describes how to configure a Mobile MAC Statistics 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 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.

---

### 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 13](#) 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 13](#) for more information on customizing report results.




---

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

---

## Mobile MAC Tracking Results

The results of the Mobile MAC Statistics report contain the following information:

- Venue
- Click Count
- Mobile MAC Address

**Note**

---

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

---

## 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, on page 27](#)

## 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 13](#) 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 13](#) 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 location density detected by the MSEs based on your filtering criteria.

- [Configuring Rogue Client Location Density, on page 28](#)
- [Rogue Client Location Tracking Results, on page 30](#)

### Configuring 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. 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.

---

### 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 13](#) 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 13](#) 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 Tracking Results

The results of Rogue Client Location Tracking report contains the following information:

- Last Located—The time when the rogue client was last located during the selected Report Time criteria.
- MAC Address—The MAC address of the rogue client.
- Rogue Client Location—Position of the rogue client at the located time.
- MSE—Name of the MSE that located this rogue client.
- Rogue AP—The rogue access point to which the rogue client is associated with.
- Detecting Cisco WLCs—The IP address of the detecting controller.
- State—State of the Rogue client.



---

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

---

## Tag Location Tracking

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

This section contains the following topics:

- [Configuring Tag Location Tracking, on page 30](#)
- [Tag Location Tracking Results, on page 31](#)

## Configuring 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 13](#) 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 13](#) 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.

---

# 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.
- 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 from 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 lists.
- Step 10** Select the **Recurrence** radio button to determine how often you want to run the report. The possible values follow:
- No Recurrence
  - Hourly
  - Daily
  - Weekly



- Monthly

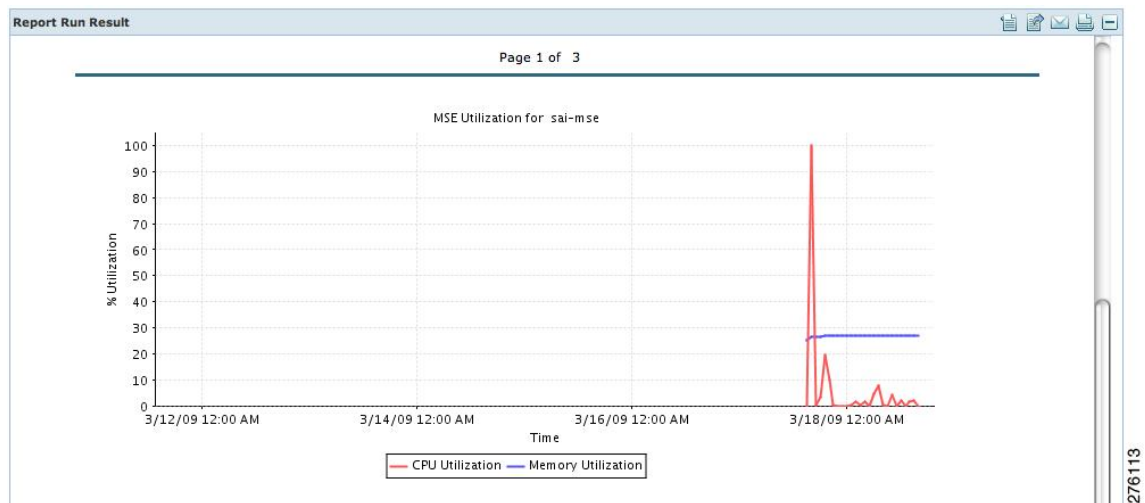
**Note** The days of the week appear on the page only when the weekly option is chosen.

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

**Figure 2: 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.
- 

## Managing OUI

The Prime Infrastructure relies on the IEEE Organizational Unique Identifier (OUI) database to identify the client vendor name mapping. Prime Infrastructure stores vendor OUI mappings in an XML file named vendorMacs.xml. With the OUI update, you can perform the following:

- Change the vendor display name for an existing OUI.
- Add new OUIs to Prime Infrastructure.
- Refresh the vendorMacs.xml file with new vendor OUI mappings and upload it to Prime Infrastructure.
- [Adding a New Vendor OUI Mapping, on page 34](#)
- [Uploading an Updated Vendor OUI Mapping File, on page 35](#)

## Adding a New Vendor OUI Mapping

The User Defined OUI List page displays a list of vendor OUI mappings that you created. This page allows you to add a new vendor OUI mapping, delete an OUI entry, and update the vendor name for an OUI that is existing in the vendorMacs.xml file.

When you add an OUI, Prime Infrastructure verifies the vendorMacs.xml file to see if the OUI exists. If the OUI exists, Prime Infrastructure updates the vendor name for the OUI. If the OUI does not exist, Prime Infrastructure adds a new OUI entry to the vendor OUI mapping.

To add a new vendor OUI mapping, follow these steps:

- 
- Step 1** Choose **Administration > System Settings**.
- Step 2** From the left sidebar menu, choose **User Defined OUI**. The User Defined OUI page appears.
- Step 3** From the Select a Command drop-down list, choose **Add OUI Entries**, and Click **Go**.
- Step 4** In the OUI field, enter a valid OUI. The format is aa:bb:cc.
- Step 5** Click **Check** to verify if the OUI exists in the vendor OUI mapping.
- Step 6** In the Name field, enter the display name of the vendor for the OUI.
- Step 7** Select the **Change Vendor Name** check box to update the display name of the vendor, if the OUI exists in the vendor OUI mapping.
- Step 8** Click **OK**.
- Step 9** After adding new OUIs, you must restart the Prime Infrastructure server to make changes into effect. You can use the following commands to shut down and restart the Prime Infrastructure server.
- Stop the services using the **ncs stop** command.
  - Restart the services using the **ncs start** command.
- 

## Uploading an Updated Vendor OUI Mapping File

You can download and save the vendorMacs.xml file posted on cisco.com to a local directory using the same filename, vendorMacs.xml. You can then, upload the file to Prime Infrastructure. Prime Infrastructure replaces the existing vendorMacs.xml file with the updated file and refreshes the vendor OUI mapping. However, it does not override the new vendor OUI mapping or the vendor name update that you made.

To upload the updated vendor OUI mapping file, follow these steps:

- 
- Step 1** Choose **Administration > System Settings**.
- Step 2** From the left sidebar menu, choose **Upload OUI**. The Upload OUI From File page appears.
- Step 3** Browse and select the vendorMacs.xml file that you downloaded from Cisco.com.
- Step 4** Click **OK**.
- 

## Monitoring Wireless Clients

This section describes about monitoring wireless clients and contains the following topics:

- [Monitoring Wireless Clients Using Maps](#), on page 36
- [Monitoring Wireless Clients Using Search](#), on page 38

## Monitoring Wireless Clients Using Maps

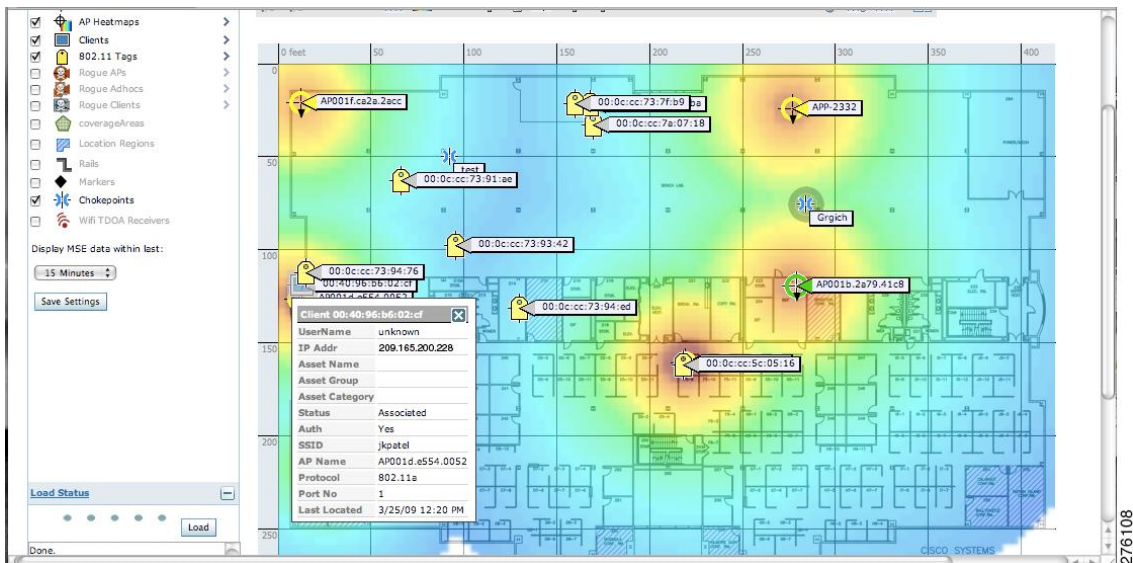
On a Prime Infrastructure map, you can view the name of the access point that the client is associated with, the IP Address, Asset information, Authentication, SSID, 802.11 protocol, and when the location information was last updated for the client. Hover mouse cursor over the client icon on the map to display this information.

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

To determine the location status of a client on a map and view its client details page using maps, follow these steps:

- Step 1** Choose **Monitor > Site Maps**.
- Step 2** Choose the building and floor on which the mobility services engine and its clients are located.
- Step 3** Select the **Clients** check box in the Floor Settings left sidebar menu if it is not already selected. Do not click **Save Settings** unless you want to save changes made to the floor settings across all maps.

**Figure 3: Monitor > Maps > Building > Floor Page**



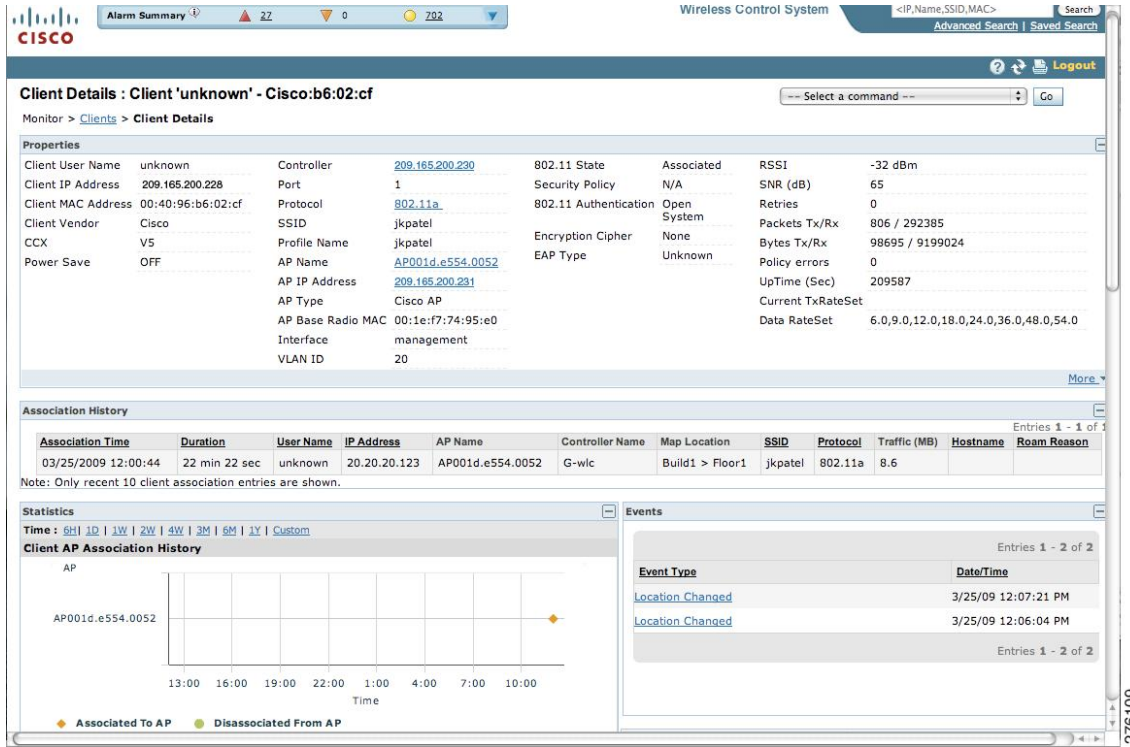
**Note** The map shows only associated clients by default. To see clients in all state, choose the **show all clients** option.

**Note** The map shows clients that was visible in the last 15 minutes. This value can be changed using the drop-down list in the left sidebar menu of the Maps page.

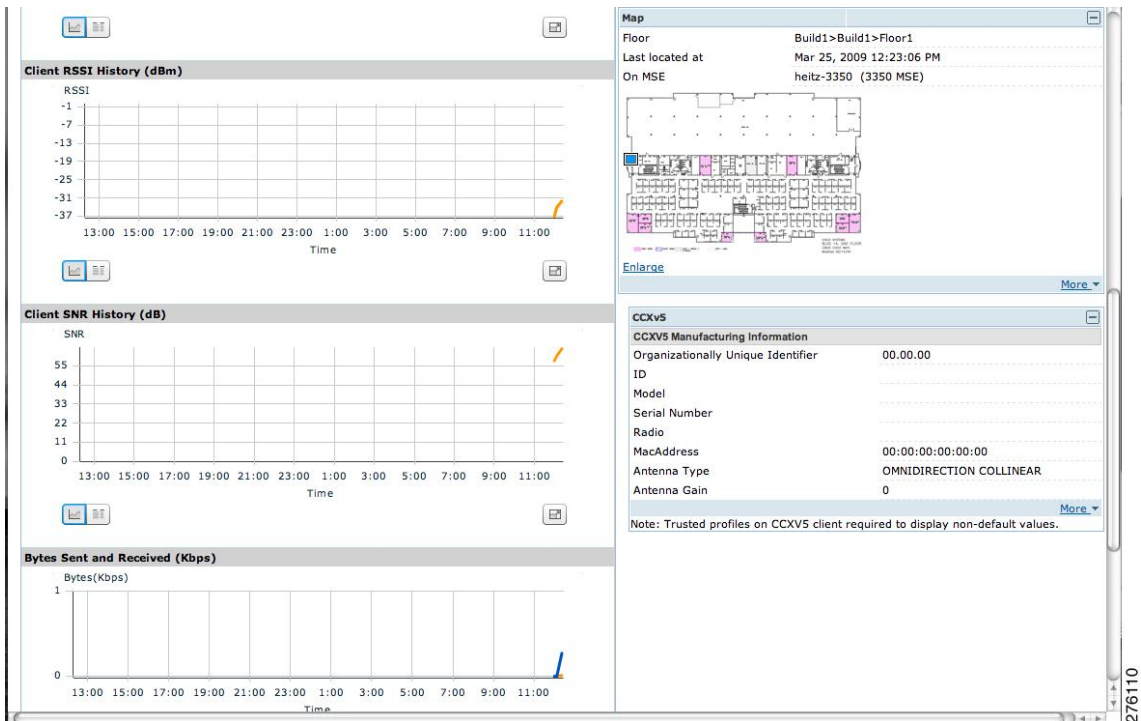
- Step 4** Hover mouse cursor over a client icon (blue square) and a summary of its configuration appears in a pop-up dialog box.
- Note** You can enter a custom note for a client in the summary dialog box. You can also edit it in the Client Details page.

**Step 5** Click the Client icon to see client details.

**Figure 4: Client Details Page (1 of 2)**



**Figure 5: Client Details Page (2 of 2)**



**Step 6** Click the **More** link to configure asset information for the client.

## Monitoring Wireless Clients Using Search

### Before You Begin

You can view client information in summary and in detail in the Monitor > Clients page and in the maps page (Monitor > Maps).

To view client information, follow these steps:

**Step 1** Choose **Monitor > Clients**.  
The Clients summary page appears.

**Step 2** From the Show drop-down list, choose Clients Detected by MSEs. Click Go.  
A summary of all clients detected by mobility services engines and location appliances managed by Prime Infrastructure is displayed (see Figure 11-6). The clients detected by MSE is a union of wired and wireless clients.

Location information is stored only for wireless clients in MSE but not for wired clients. Hence, in order to filter clients by virtual domain, switch ports must be assigned to floors in the given virtual domain in order to view the wired clients, otherwise only wireless clients are listed here.

**Note** The clients will only show one IP address when you hover your mouse over the client to see the information, even though there might be multiple IP addresses associated with this client. The details page will show all the IP addresses. Also the clients displayed can be filtered using any of the multiple IP addresses that a client can have (full or partial). the IP address displayed is the best matched string searched.

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

For example, if you enter a MAC address in the Search text box, the following page appears.

b) To see more configuration details about the client, click View List for the client item type. Details shown include associated devices (access point, controller), map location, VLAN, protocol, and authentication type.

c) To see alarms for the client, click View List for the alarm item type. A listing of all active alarms for that client noting severity, failure source (alarm description), owner of alarm (if assigned), date and time of the alarm, and whether or not alarm is acknowledged.

**Note** You can also assign or unassign the alarm, e-mail it, delete or clear it, and acknowledge and unacknowledge it in this page by choosing the appropriate option from the Select a command drop-down list.

d) To search for a client or multiple clients by device, network, map location and type of client (regular, rogue, or shunned), click the Advanced Search link.

You can further define the client category by all clients, all excluded clients, all wired guest clients, and all logged in clients using the Search By drop-down list.

Click the appropriate client.

---

## 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.

- [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 Cisco WLCs.
- 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 the 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—Cisco WLC 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 client parameters 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 choose 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 Cisco WLC. 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.

- [Adding a Building to a Campus Map, on page 46](#)
- [Viewing a Building](#)
- [Editing a Building](#)
- [Deleting a Building](#)
- [Moving a Building](#)

## 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:
- Enter the building name.
  - 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.
  - Enter the number of floors and basements.
  - 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.
  - Click **OK** to save this building to the database.
- Step 4** (Optional) To assign location presence information for the new building, do the following:
- Choose **Location Presence** from the Select a command drop-down list. Click **Go**. The Location Presence page appears.
  - 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.
  - 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 46 for more information.
  - Edit Building—See the [Editing a Building](#) for more information.
  - Delete Building—See the [Deleting a Building](#) for 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 Tags

You can monitor tag status and location on the Prime Infrastructure maps as well as review tag details in the Monitor > Tags page. You can also use the Advanced Search to monitor tags.

- [Monitoring Tags Using Maps](#), on page 51
- [Monitoring Tags Using Search](#), on page 51
- [Overlapping Tags](#), on page 53

## Monitoring Tags Using Maps

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

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

- 
- Step 1** Choose **Monitor > Maps**.
- Step 2** Choose the building and floor on which the mobility services engine and tag are located.
- Step 3** Select the **802.11 Tags** check box in the Floor Settings menu if it is not already selected.  
**Note** Do not click **Save Settings** unless you want to save changes made to the floor settings across all maps.
- Step 4** Hover your mouse cursor over a tag icon (yellow tag) and a summary of its configuration appears in a Tag dialog box.
- Step 5** Click the **tag** icon to see tag details.  
You can also configure the asset information by entering the required information in the Asset Info group box.
- Step 6** To see location history for the tag, choose **Location History** from the Select a command drop-down list. Click **Go**.
- 

## Monitoring Tags Using Search

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

You can further refine your search using the Advanced Search parameters and save the search criteria for future use. Click **Saved Searches** to retrieve saved searches.

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

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

To search for tags, follow these steps:

- Step 1** Choose **Monitor** > **Tags**. The Tag Summary page appears.
- Step 2** To view a summary of tags associated with a specific MSE, click the **Total Tags** link.  
**Note** If the listing of MSEs or tags is lengthy, you can use Search or Advanced Search to isolate a specific tag.
- Step 3** To search for a specific tag, if you know its MAC address and asset name (not all search values apply to all tags), click the **Search** link.
- Step 4** To search for a specific tag or multiple tags using a broader range of search criteria such as device (MSE or controller), map location (floor or outdoor area), asset name or category, or tag vendor, click the **Advanced Search** link.
- In the Advanced Search pane, select **Tags** as the search category.
  - Select the additional tag search criteria.
  - Click **Go** when all advanced search parameters are selected.
- Note** If no tags are found based on the selected search criteria, a message appears noting this as well as the reason why the search was unsuccessful and possible actions.

**Table 1: Tag Search Criteria and Values**

Search Criteria	Variable Search Criteria	Possible Values
Search for tags by (Tier 1 search criteria)	—	All Tags; Asset Name, Asset Category or Asset Group; MAC Address; Cisco WLC or MSEs; Floor Area, or Outdoor Area.  <b>Note</b> The MSE search includes both location servers and MSEs.
Search in (Tier 2 search criteria)	—	MSEs or Prime Infrastructure or Cisco WLCs.  <b>Note</b> The Prime Infrastructure controller option indicates that the search for Cisco WLC is done within the Prime Infrastructure.  <b>Note</b> The MSE search includes both location servers and MSEs.
Last detected within	—	Options are from 5 minutes to 24 hours.
Variable search criteria. (Tier 3 search criteria)  <b>Note</b> Possible search criteria determined by the Search for tabs by (Tier 1 search) value.	If the Search for tags by value is the following: Asset Name, then enter tag asset name. Asset Category, then enter tag asset category. Asset Group, then enter tag asset group. MAC Address, then enter tag MAC address. Controller, then select controller IP address. MSEs, then choose an MSE IP address from drop-down list. Floor Area, then choose campus, building, and floor area. Outdoor Area, then choose campus and outdoor area.	

Search Criteria	Variable Search Criteria	Possible Values
Telemetry tags only	—	<p>Check box to display telemetry tags. Leaving option unselected shows all tags.</p> <p><b>Note</b> Option only visible when the Search In option is MSE.</p> <p><b>Note</b> Only those vendor tags that support telemetry appear.</p>
Tag vendor	—	<p>Check box to select tag vendor from drop-down list.</p> <p><b>Note</b> Option only visible when the Search In option is MSE.</p>
Items per page	—	Select the number of tags to display per search request. Values range from 10 to 500.
Save search	—	Check box to name and save search criteria. Once saved, entry appears under Saved Searches heading.

## Overlapping Tags

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

When you hover your mouse cursor over the overlapping tag on the map, a dashlet appears with summary information for the overlapping tags.

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

Summary information for tags includes Tag MAC address, Asset Name, Asset Group, Asset Category, Vendor (Type), Battery Life, and Last Located data (date and time). If the tag is Cisco CX v.1 compliant, telemetry information also appears.

- Detailed information for tags also includes the IP address of the associated Cisco WLC, statistics, location notifications, location history, and whether the location debug feature is enabled.
  - To view location history for a tag, choose that option from the Select a command drop-down list, and click **Go**.
  - To return to the details page, choose Location History page from the Select a command drop-down list, and click **Go**.

# Monitoring Geo-Location

The MSE provides physical location of wired clients, wired endpoints, switches, Cisco WLCs, 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.

---

- [Adding a GPS Marker to a Floor Map, on page 54](#)
- [Editing a GPS Marker, on page 55](#)
- [Deleting a GPS Marker From the Floor, on page 55](#)

## 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 the Floor

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.
- 

## Monitoring Chokepoints

A chokepoint must be assigned to a map for its location to be monitored. After adding the TDOA receiver to a map, you must resynchronize the network designs (Services > Synchronize Services) with the mobility services engine for it to appear on the map.

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.

If the existing chokepoints are on a floor, then they all belong to the same virtual domain as the floor. If the chokepoints are not placed on a floor, then they are available in all virtual domains.

If a chokepoint is not assigned to a map, you are not able to find that chokepoint using Search or Advanced Search. All chokepoint setup is done using the AeroScout System Manager.



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

To monitor chokepoints, follow these steps:

- 
- Step 1** Choose **Monitor > Chokepoints**. The Chokepoint page appears showing all mapped chokepoints.
- Step 2** To refine the search criteria when an extensive list appears, search by MAC address or chokepoint name.
- a) To initiate a search for a chokepoint by its MAC address or chokepoint name, enter that value in the **Search** text box. Click **Search**. This example show a search by MAC address. If no match exists, a message appears in the Search Results page.
  - b) To initiate an advanced search for a chokepoint by its MAC address or name, click the **Advanced Search** link.
    - Choose **Chokepoint** as the search category.
    - From the Search for Chokepoint by drop-down list, choose either **Chokepoint Name** or **MAC Address**. This list should display chokepoints belonging to the current virtual domain. Chokepoints that are not placed on a floor belongs to all virtual domains. If a chokepoint is placed on a floor, it should be displayed in the same virtual domain as the floor on which it is placed.
    - Enter either the chokepoint name or MAC address.
    - Click **Search**. This example shows an advanced search using the chokepoint name. If no match exists, a message appears in the page. Otherwise the Search Results page appears.
- 

## Monitoring Wi-Fi TDOA Receivers

A Wi-Fi TDOA receiver must be assigned to a map for its location to be monitored. After adding the TDOA receiver to a map, you must resynchronize network designs (Services > Synchronize Services) with the mobility services engine for it to appear on the map.

If a TDOA receiver is not assigned to a map, you cannot find it using Search or Advanced Search.

All TDOA receiver setup is done using the AeroScout System Manager.

When a new TDOA receiver 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 the floor. When a TDOA receiver is removed from a floor, it will be available in all the virtual domains again.

If the existing TDOA receivers are on a floor, then they all belong to the same virtual domain as the floor. If the chokepoints are not placed on a floor, then they are available in all virtual domains.





---

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

---

To monitor TDOA receivers, follow these steps:

- 
- Step 1** Choose **Monitor > WiFi TDOA Receivers**. The WiFi TDOA Receivers summary page appears showing all mapped TDOA receivers.
- Step 2** To refine the search criteria when an extensive list appears, search by MAC address or TDOA receiver name.
- To initiate a search for a TDOA receiver by its MAC address or name, enter that value in the Search text box. Click **Search**.
  - Click **View List** to see a full list of alarms.  
If no match exists, a message appears in the Search Results page.
  - To initiate an advanced search for a TDOA receiver by its MAC address or name, click the **Advanced Search** link.
    - Choose **WiFi TDOA Receiver** as the search category from the Search Criteria drop-down list.
    - From the Search for WiFi TDOA Receiver by drop-down list, choose either **WiFi TDOA Receivers Name** or **MAC Address**.  
  
This list displays Wi-Fi TDoA receivers belonging to the current virtual domain. The Wi-Fi TDoA receivers that are not placed on a floor is belongs to all virtual domains. If a Wi-Fi TDoA receivers is placed on a floor, it should be displayed in the same virtual domain as the floor on which it is placed.
    - Enter either the TDOA receiver name or MAC address.
    - Click **Search**.  
If no match exists, a message appears in the Search Results page.
- 

## 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 in the ESS online help.



---

**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 the AirMagnet Survey and Planning documentation which is available at Fluke Networks website.

## Monitoring Wired Clients

You can view details on a wired client (MAC address, IP address, username, serial number, UDI, model no., software version, and VLAN ID), its port, and its civic information.

Wired client data is downloaded to the mobility services engine through the Prime Infrastructure when the switch and the mobility services engine are synchronized (Services > Synchronize Services > Switches).

You can view the details of the wired clients in either the Wired Switches page (Context Aware Service > Wired > Wired Switches) or wired clients page (Context Aware Service > Wired > Wired Clients).

- If you know the IP address, MAC address, VLAN ID, serial number, or username, you can use the Search text box in the Wired Clients page.
- If you want to examine wired clients as they relate to a specific switch, you can view that information in the Wired Switches page.

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

- 
- Step 1** Choose **Services > Mobility Services Engines**. The Mobility Services page appears.
- Step 2** Click the device name link of the appropriate wired location switch.
- Step 3** Choose **Context Aware Service > Wired > Wired Clients**.  
In the Wired Clients summary page, clients are grouped by their switch. The status of a client is noted as connected, disconnected, or unknown. Definitions are summarized as follows:
- Connected clients—Clients that are active and connected to a wired switch.

- Disconnected clients—Clients that are disconnected from the wired switch.
- Unknown clients—Clients that are marked as unknown when the NMSP connection to the wired switch is lost.
- If you know the MAC address of the wired client, then you can click that link to reach the detail page of the client or use the Search text box.
  - You can also search for a wired client by its IP address, username, or VLAN ID.
- If you click the IP address of the switch, you are forwarded to the detail page of the switch.

**Step 4** Click the **Port Association** tab to show the physical location of the switch port/slot/module on which the wired client terminates, the client status (connected, disconnected, unknown), and the switch IP address.

**Step 5** Click the **Civic Address** tab to show any civic address information.

**Step 6** Click the **Advanced** tab to see extended physical address details for the wired clients, if any.

**Note** A client takes on the civic address and advanced location information that is configured for the port on which the client terminates. If no civic and advanced information are defined for the port (port/slot/module), then no location data is displayed.

## Monitoring Wired Switches

You can review details on the wired switch (IP address, serial number, software version, and ELIN), its ports, its wired clients (count and status), and its civic information.

Wired switch data is downloaded to the mobility services engine through the Prime Infrastructure when the Ethernet switch and the mobility services engine are synchronized (Services > Synchronize Services > Switches). Communication between a location-capable switch and a mobility services engine occurs over NMSP. The Prime Infrastructure and the MSE communicate over XML.

To view details on wired switches, follow these steps:

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

**Step 2** In the Mobility Services page, click the device name link of the appropriate wired location switch.

**Step 3** Choose **Context Aware Service > Wired > Wired Switches**. A summary of wired switches that are synchronized with the MSE appears.

**Step 4** To see more details on the switch, its ports, its wired clients (count and status), and its civic information, click the **IP address** link.

**Note** You can export civic information from the switch by choosing that option from the Select a command drop-down list. This option is available on all four tabs in the Wired Switches page.

- On the Switch Information tab, a total count of wired clients connected to the switch is summarized along with their state (connected, disconnected, and unknown).
- Connected clients—Clients that are connected to the wired switch.
- Disconnected clients—Clients that are disconnected from the wired switch.

- Unknown clients—Clients are marked as unknown when the NMSP connection to the wired switch is lost.

You can view detailed wired client information by clicking one of the client count links (total clients, connected, disconnected, and unknown).

- Step 5** Click the **Switch Ports** tab to see a detailed list of the ports on the switch. You can change the listing order (ascending, descending) of port IP addresses, slot numbers, module number, and port number by clicking the respective column heading.
- Step 6** Click the **Civic** tab to see a detailed list of the civic information for the wired switch.
- Step 7** Click the **Advanced** tab to see a detailed list of the additional civic information for the wired switch
- 

## Monitoring Interferers

### Monitor > Interferers > AP Detected Interferers

Choose **Monitor > Interferers** to view all the interfering devices detected by the CleanAir-enabled access points on your wireless network. This page enables you to view a summary of the interfering devices including the following default information:

- Interferer ID—A unique identifier for the interferer. Click this link to learn more about the interferer.
- Type—Indicates the category of the interferer. Click to read more about the type of device. The pop-up dialog appears displaying more details. The categories include the following:
  - Bluetooth link—A Bluetooth link (802.11b/g/n only)
  - Microwave Oven—A **microwave oven** (802.11b/g/n only)
  - 802.11 FH—An 802.11 frequency-hopping device (802.11b/g/n only)
  - Bluetooth Discovery—A Bluetooth discovery (802.11b/g/n only)
  - TDD Transmitter—A time division duplex (TDD) transmitter
  - Jammer—A jamming device
  - Continuous Transmitter—A continuous transmitter
  - DECT-like Phone—A Digital Enhanced Cordless Telecommunication (DECT)-compatible phone
  - Video—A video camera
  - 802.15.4—An 802.15.4 device (802.11b/g/n only)
  - WiFi Inverted—A device using spectrally inverted Wi-Fi signals
  - WiFi Invalid—A device using non-standard Wi-Fi channels
  - SuperAG—An 802.11 SuperAG device
  - Canopy—A Motorola Canopy device

- Radar—A radar device (802.11a/n only)
- Xbox—A Microsoft Xbox (802.11b/g/n only)
- WiMAX Mobile—A WiMAX mobile device (802.11a/n only)
- WiMAX Fixed—A WiMAX fixed device (802.11a/n only)
- Status—Indicates the status of the interfering device.
  - Active—Indicates that the interferer is currently being detected by the CleanAir-enabled access point.
  - Inactive—Indicates that the interferer is no longer being detected by the CleanAir-enabled access point or the CleanAir-enabled access point detected that the interferer is no longer reachable by Prime Infrastructure.
- Severity—Shows the severity ranking of the interfering device.
- Affected Band—Shows the band in which this device is interfering.
- Affected Channels—Shows the affected channels.
- Duty Cycle (%)—The duty cycle of interfering device in percentage.
- Discovered—Shows the time at which it was discovered.
- Last Updated—The last time the interference was detected.
- Floor—The location where the interfering device is present.

**Note**

---

These devices appear only if the option to track Interferers is enabled in the Tracking Parameters page. This option is disabled by default. For more information on tracking parameters, see the [Modifying Tracking Parameters](#).

---

## Monitor > Interferers > Edit View

The Edit View page allows you to add, remove, or reorder columns in the AP Detected Interferers Summary page. It also allows you to search for Interferers. By default, only those interferers that are in Active state and with, severity greater than or equal to 5 are displayed in the AP Detected Interferers page.

To edit the columns in the AP Detected Interferers page, follow these steps:

- 
- Step 1** Choose **Monitor > Interferers**. The AP Detected Interferers page appears showing details of the interferers detected by the CleanAir-enabled access points.
  - Step 2** Click the **Edit View** link in the AP Detected Interferers page.
  - Step 3** To add an additional column to the access points table, click to highlight the column heading in the left column. Click **Show** to move the heading to the right column. All items in the right column are displayed in the table.
  - Step 4** To remove a column from the access points table, click to highlight the column heading in the right column. Click **Hide** to move the heading to the left column. All items in the left column are not displayed in the table.
  - Step 5** Use the **Up/Down** buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click **Up** or **Down** to move it higher or lower in the current list.
  - Step 6** Click **Reset** to restore the default view.
  - Step 7** Click **Submit** to confirm the changes.
- 

## Clustering of Monitor Mode APs Using MSE

Where *value* is the distance in feet for clustering. The default value is 150.