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

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.

• 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 Stat**e 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.

wIPS Alarm Consolidation

The wIPS alarm consolidation feature is introduced in Release 7.5. The wIPS alarm consolidation aggregates different wireless intrusion incidents reported by access points and provides a concise meaningful alarm. This helps you to quickly separate the potential security issues and concerns. Alarm consolidation is performed at wIPS services module in the MSE. After the consolidation rule is triggered in MSE, the MSE notifies the Prime Infrastructure by sending an SNMP trap.

The following three attack consolidation categories are created:

- Beacon flood—The system detects a number of out of sequence beacon frames sent from a device. By sending fake beacon frames, the hacker can advertise false access point configuration and settings such as supported data rate, SSID, and channel information. The following alarms are included in this alarm consolidation category:
  - Spoofed MAC Address Detected
  - DoS: Beacon Flood
- De-auth flood—This is a type of denial-of-service attack. The traffic pattern matches with the denial-of-service attack that uses spoofed de-authentication frames to break the association between an access point and its client stations.

  The following alarms are included in this alarm consolidation category:
  - Spoofed MAC address
  - DoS: De-Auth Flood
- MDK3-Destruction attack—This causes all clients that is associated or trying to associate with the AP to fail. The following alarms are included in this consolidation category:
  - DoS: De-Auth Broadcast Flood
  - DoS: Dis-Assoc Broadcast Flood
  - DoS: Unauthenticated Association
  - Dos: MDK3-Destruction Attack

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, hout, 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 process 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

- 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.

Monitoring Access Points Details

The Access Points Details page enables you to view access point information for a single AP.

Choose **Monitor > Access Points** and click an item in the AP Name column to access this page. Depending on the type of access point, the following tabs might be displayed. This section provides the detailed information regarding each Access Points Details page tab and contains the following topics:

- General Tab
- Interfaces Tab
- CDP Neighbors Tab

- Current Associated Clients Tab
- SSID Tab
- Clients Over Time Tab

General Tab

Note The General tab fields differ between lightweight and autonomous access points.

This section contains the following topics:

- General—Lightweight Access Points
- General—Autonomous

General—Lightweight Access Points

Table 5-47 lists the General (for Lightweight Access Points) Tab fields.

Table 1: General (for Lightweight Access Points) Tab Fields

Field	Description
General	
AP Name	Operator defined name of access point.
AP IP address, Ethernet MAC address, and Base Radio MAC address	IP address, Ethernet MAC address and Radio MAC address.
Country Code	The codes of the supported countries. Up to 20 countries can be supported per controller. **Note** Access points might not operate properly if they are not designed for use in your country of operation. For a complete list of country codes supported per product, see the following URL: http://www.cisco.com/en/US/docs/wireless/wcs/4.0/configuration/guide/wcscod.html.

Field	Description
Link Latency Settings	You can configure link latency on the controller to measure the link between an access point and the controller. See the Configuring Link Latency Settings for Access Points for more information. • Current Link Latency (in msec)—The current round-trip time (in milliseconds) of heartbeat packets from the access point to the controller and back. • Minimum Link Latency (in msec)—Because link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of heartbeat packets from the access point to the controller and back. • Maximum Link Latency (in msec)—Because link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of heartbeat packets from the access point to the controller and back.
LWAPP/CAPWAP Uptime	Displays how long the LWAPP/CAPWAP connection has been active.
LWAPP?CAPWAP Join Taken Time	Displays how long the LWAPP/CAPWAP connection has been joined.
Admin Status	The administration state of the access point as either enabled or disabled.
AP Mode	
Local	Default mode. Data clients are serviced while configured channels are scanned for noise and rogues. The access point goes off-channel for 50 ms and listens for rogues. It cycles through each channel for the period specified under the Auto RF configuration. **Note** To configure Local or FlexConnect access points for the Cisco Adaptive wIPS feature, choose Local or FlexConnect and select the **Enhanced wIPS Engine Enabled** check box.

Field	Description
Monitor	Radio receive only mode. The access point scans all configured channels every 12 seconds. Only deauthenticated packets are sent in the air with an access point configured this way. A monitor mode access point can connect as a client to a rogue access point. **Note** To configure access points for Cisco Adaptive wIPS feature, select **Monitor**. Select the **Enhanced wIPS Engine Enabled** check box and choose **wIPS** from the Monitor Mode Optimization drop-down list. Before you can enable an access point to be in wIPS mode, you must disable the access point radios. If you do not disable the access point radio, an error message appears. **Note** Once you have enabled the access point for wIPS, reenable the radios.
Rogue Detector	The access point radio is turned off and the access point listens to wired traffic only. The controllers that operate in this mode monitor the rogue access points. The controller sends all the rogue access point and client MAC address lists to the rogue detector, and the rogue detector forwards this information to the WLC. The MAC address list is compared to what the WLC access points heard over the network. If the MAC addresses match, you can determine which rogue access points are connected on the wired network.
Sniffer	The access point captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. These packets contain information such as timestamp, signal strength, packet size, and so on. This feature can only be enabled if you run AiroPeek, which is a third-party network analyzer software that supports the decoding of data packets.
FlexConnect	Enables FlexConnect for up to six access points. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. **Note** FlexConnect must be selected to configure an OfficeExtend access point. When the AP mode is FlexConnect, FlexConnect configuration options display including the option to enable OfficeExtend AP and to enable Least Latency Controller Join.

Field	Description
Bridge	This is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The bridge and its wired clients are listed as client in the Prime Infrastructure if the AP mode is set to Bridge, and the access point is bridge capable.
Spectrum Expert	This mode allows a CleanAir-enabled access point to be used extensively for interference detection on all monitored channels. All other functions such as IDS scanning and Wi-Fi are suspended.
Enhanced wIPs Engine	Enabled or Disabled, to enable the monitoring of the security attacks using Cisco Adaptive wIPS feature.
Operational Status	Registered or Not Registered, as determined by the controller.
Registered Controller	The controller to which the access point is registered. Click to display the registered controller details. See the "Monitoring System Summary" section on page 5-4 for more information.
Primary Controller	The name of the primary controller for this access point.
Port Number	The SNMP name of the access point primary controller. The access point attempts to associate with this controller first for all network operations and in the event of a hardware reset.
AP Uptime	Displays how long the access point has been active to receive and transmit.
Map Location	Customer-definable location name for the access point. Click to look at the actual location on a map. Choose **Monitor** > **Access Points** > *name* > **Map Location** for more information.
Google Earth Location	Indicates whether a Google Earth location is assigned.
Location	The physical location where the access point is placed (or Unassigned).
Statistics Timer	This counter sets the time in seconds that the access point sends its DOT11 statistics to the controller.

Field	Description
PoE Status	The power over ethernet status of the access point. The possible values include the following: • Low—The access point draws low power from the Ethernet. • Lower than 15.4 volts—The access point draws lower than 15.4 volts from the Ethernet. • Lower than 16.8 volts—The access point draws lower than 16.8 volts from the Ethernet. • Normal—The power is high enough for the operation of the access point. • Not Applicable—The power source is not from the Ethernet.
Rogue Detection	Indicates whether or not Rogue Detection is enabled. **Note** Rogue detection is disabled automatically for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. For more information regarding OfficeExtend access points, see the *Cisco Wireless LAN Controller Configuration Guide*.
OfficeExtend AP	Indicates whether or not the access point is enabled as an OfficeExtend access point. The default is Enabled.
Encryption	Indicates whether or not encryption is enabled. **Note** Enabling or disabling encryption functionality causes the access point to reboot which then causes a loss of connectivity for clients. **Note** DTLS data encryption is enabled automatically for OfficeExtend access points to maintain security. Encryption is only available if the access point is connected to a 5500 series controller with a Plus license.
Least Latency Join	The access point switches from a priority order search (primary, secondary, and then tertiary controller) to a search for the controller with the best latency measurement (least latency). The controller with the least latency provides the best performance.
Telnet Access	Indicates whether or not Telnet Access is enabled.

Field	Description
SSH Access	Indicates whether or not SSH is enabled. **Note** An OfficeExtend access point might be connected directly to the WAN which could allow external access if the default password is used by the access point. Because of this, Telnet and SSH access are disabled automatically for OfficeExtend access points.
Versions	
Software Version	The operating system release.version.dot.maintenance number of the code currently running on the controller.
Boot Version	The operating system bootloader version number.
Inventory Information	
AP Type	Type of Access Point
AP Model	Access point model number.
Cisco IOS Version	The Cisco IOS Release details.
AP Certificate Type	Either Self Signed or Manufacture Installed.
FlexConnect Mode Supported	Indicates if FlexConnect mode is supported or not.
wIPS Profile (when applicable)	
Profile Name	Click the user-assigned profile name to view wIPS profile details.
Profile Version	
Unique Device Identifier (UDI)	
Name	Name of the Cisco AP for access points.
Description	Description of the access point.
Product ID	Orderable product identifier.
Version ID	Version of product identifier.
Serial Number	Unique product serial number.

Field	Description
Run Ping Test Link— Click to ping the access point. The results are displayed in a pop-up dialog box. The below are the parameters associated: • Controller IP Address • Destination • Send Count • Received Count • Maximum Time Interval • Minimum Time Interval • Average Time Interval	
Alarms Link— Click to display alarms associated with this access point. • Severity • Message • Failure Source • Timestamp • Owner • Category • Condition	
Events Link— Click to display events associated with this access point. • Description • Failure Source • Timestamp • Severity • Category • Condition • Correlated	

General—Autonomous

Note For autonomous clients, the Prime Infrastructure *only* collects client counts. The client counts in the Monitor page and reports have autonomous clients included. Client search, client traffic graphs, or other client reports (such as Unique Clients, Busiest Clients, Client Association) do *not* include clients from autonomous access points.

Table 5-48 lists the General (for Autonomous Access Points) tab fields.

Table 2: General (for Autonomous Access Points) Tab Fields

Field	Description
AP Name	Operator defined name of access point.
AP IP address and Ethernet MAC address	IP address, Ethernet MAC address of the access point.
AP UpTime	Indicates how long the access point has been up in number of days, hours, minutes, and seconds.
Map Location	Customer-definable location name for the access point. Click to look at the actual location on a map.
WGB Mode	Indicates whether or not the access point is in work group bridge mode.
SNMP Info	
SysObjectId SysDescription SysLocation SysContact	System Object ID. The system device type and current version of firmware. The physical location of the device, such as a building name or room in which it is installed. The name of the system administrator responsible for the device.
Versions	
Software Version	The operating system release.version.dot.maintenance number of the code currently running on the controller.
CPU Utilization	Displays the maximum, average, and minimum CPU utilization over the specified amount of time.
Memory Utilization	Displays the maximum, average, and minimum memory utilization over the specified amount of time.

Field	Description
Inventory Information	
AP Type	Autonomous or lightweight.
AP Model	The Access Point model number.
AP Serial Number	Unique serial number for this access point.
FlexConnect Mode Supported	If FlexConnect mode is supported or not.
Unique Device Identifier (UDI)	
Name	Name of Cisco AP for access points.
Description	Description of access point.
Product ID	Orderable product identifier.
Version ID	Version of product identifier.
Serial Number	Unique product serial number.

Note Memory and CPU utilization charts are displayed.

Note Click **Alarms** to display the alarms associated with the access point. Click **Events** to display events associated with the access point.

Interfaces Tab

Table 5-49 lists the Interfaces tab fields.

Table 3: Interfaces Tab Fields

Field	Description
Interface	
Admin Status	Indicates whether the Ethernet interface is enabled.
Operational Status	Indicates whether the Ethernet interface is operational.
Rx Unicast Packets	Indicates the number of unicast packets received.

Field	Description
Tx Unicast Packets	Indicates the number of unicast packets sent.
Rx Non-Unicast Packets	Indicates the number of non-unicast packets received.
Tx Non-Unicast Packets	Indicates the number of non-unicast packets sent.
Radio Interface	
Protocol	802.11a/n or 802.11b/g/n.
Admin Status	Indicates whether the access point is enabled or disabled.
CleanAir Capable	Indicates whether the access point is able to use CleanAir.
CleanAir Status	Indicates the status of CleanAir.
Channel Number	Indicates the channel on which the Cisco Radio is broadcasting.
Extension Channel	Indicates the secondary channel on which Cisco radio is broadcasting.
Power Level	Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.
Channel Width	Indicates the channel bandwidth for this radio interface. See the Configuring 802.11a/n RRM Dynamic Channel Allocation for more information on configuring channel bandwidth. Minimum (default) setting is 20 MHz. Maximum setting is the maximum channel width supported by this radio.
Antenna Name	Identifies the type of antenna.

Click an interface name to view its properties (see Table 5-50).

Table 4: Interface Properties

Field	Description
AP Name	Name of the Access Point.
Link speed	Indicates the speed of the interface in Mbps.
RX Bytes	Indicates the total number of bytes in the error-free packets received on the interface.
RX Unicast Packets	Indicates the total number of unicast packets received on the interface.

Field	Description
RX Non-Unicast Packets	Indicates the total number of non-unicast or mulitcast packets received on the interface.
Input CRC	Indicates the total number of CRC error in packets received on the interface.
Input Errors	Indicates the sum of all errors in the packets while receiving on the interface.
Input Overrun	Indicates the number of times the receiver hardware was incapable of handing received data to a hardware buffer because the input rate exceeded the receiver capability to handle the data.
Input Resource	Indicates the total number of resource errors in packets received on the interface.
Runts	Indicates the number of packets that are discarded because they are smaller than the medium minimum packet size.
Throttle	Indicates the total number of times the interface advised a sending NIC that it was overwhelmed by packets being sent and to slow the pace of delivery.
Output Collision	Indicates the total number of packet retransmitted due to an Ethernet collision.
Output Resource	Indicates the total number of resource errors in packets transmitted on the interface.
Output Errors	Indicates the sum of all errors that prevented the final transmission of packets out of the interface.
Operational Status	Indicates the operational state of the physical Ethernet interface on the AP.
Duplex	Indicates the duplex mode of an interface.
TX Bytes	Indicates the total number of bytes in the error-free packets transmitted on the interface.
TX Unicast Packets	Indicates the total number of unicast packets transmitted on the interface.
TX Non-Unicast Packets	Indicates the total number of non-unicast or mulitcast packets transmitted on the interface.
Input Aborts	Indicates the total number of packet aborted while receiving on the interface.
Input Frames	Indicates the total number of packet received incorrectly having a CRC error and a non-integer number of octets on the interface.
Input Drops	Indicates the total number of packets dropped while receiving on the interface because the queue was full.

Field	Description
Unknown Protocol	Indicates the total number of packet discarded on the interface due to an unknown protocol.
Giants	Indicates the number of packets that are discarded because they exceed the maximum packet size of the medium.
Interface Resets	Indicates the number of times that an interface has been completely reset.
Output No Buffer	Indicates the total number of packets discarded because there was no buffer space.
Output Underrun	Indicates the number of times the transmitter has been running faster than the router can handle.
Output Total Drops	Indicates the total number of packets dropped while transmitting from the interface because the queue was full.

CDP Neighbors Tab

Table 5-51 lists the CDP Neighbors tab fields.

Note This tab is visible only when the CDP is enabled.

Table 5: CDP Neighbors Tab Fields

Field	Description
AP Name	The name assigned to the access point.
AP IP Address	IP address of the access point.
Port No	Port number connected or assigned to the access point.
Local Interface	Identifies the local interface.
Neighbor Name	Name of the neighboring Cisco device.
Neighbor Address	Network address of the neighboring Cisco device.
Neighbor Port	Port of the neighboring Cisco device.
Duplex	Indicates Full Duplex or Half Duplex.
Interface Speed	Speed at which the interface operates.

Current Associated Clients Tab

Table 5-52 lists the Current Associated Clients tab fields.

Note This tab is visible only when there are clients associated to the AP (CAPWAP or Autonomous AP).

Table 6: Current Associated Clients Tab Fields

Field	Description
Username	Click the username to view the Monitor Client Details page for this client. See the Monitoring Clients and Users for more information.
IP Address	IP address of the associated client.
Client MAC Address	Click the client MAC address to view the Monitor Client Details page for this client.
Association Time	Date and time of the association.
UpTime	Time duration of the association.
SSID	User-defined SSID name.
SNR (dB)	Signal to Noise Ratio in dB of the associated client.
RSSI	Received Signal Strength Indicator in dBm.
Bytes Tx	This indicates the total amount of data that has passed through the Ethernet interface either way.
Bytes Rx	This indicate the total amount of data that has been received through the Ethernet interface either way
When the access point is not associated with the controller, then the database is used to retrieve the data (rather than the controller itself). If the access point is not associated, the following fields appear.	
User Name	Username of the client.
IP Address	Local IP Address
Client MAC Address	Client MAC Address
Association Time	Timestamp of the client association.

Field	Description
Session Length	Time length of the session
SSID	User-defined SSID name.
Protocol	
Avg. Session Throughput	
Traffic (MB) as before	

Note Click the **Edit View** link to add, remove or reorder columns in the Current Associated Clients table. See the "Configuring the List of Access Points Display" section on page 5-47 for adding a new field using the Edit View.

SSID Tab

Table 5-53 lists the SSID tab fields.

Note This tab is visible only when the access point is Autonomous AP and there are SSIDs configured on the AP.

Table 7: SSID Tab

Field	Description
SSID	Service Set Identifier being broadcast by the access point radio.
SSID Vlan	SSID on an access point is configured to recognize a specific VLAN ID or name.
SSID Vlan Name	SSID on an access point is configured to recognize a specific VLAN ID or name.
MB SSID Broadcast	SSID broadcast disabled essentially makes your Access Point invisible unless a wireless client already knows the SSID, or is using tools that monitor or 'sniff' traffic from an AP's associated clients.
MB SSID Time Period	Within this specified time period, internal communication within the SSID continues to work.

Clients Over Time Tab

This tab displays the following charts:

- Client Count on AP—Displays the total number of clients currently associated with an access point over time.
- Client Traffic on AP—Displays the traffic generated by the client connected in the AP distribution over time.

Note The information that appears in the above charts is presented in a time-based graph. For graphs that are time-based, there is a link bar at the top of the graph page that displays 6h, 1d, 1w, 2w, 4w, 3m, 6m, 1y, and Custom. When selected, the data for that time frame is retrieved and the corresponding graph is displayed. See the "Time-Based Graphs" section on page 6-71 for more information.

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 25

• Managing Current Reports, on page 27
• Managing Scheduled Run Results, on page 27
• Managing Saved Reports, on page 27

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.

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.

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

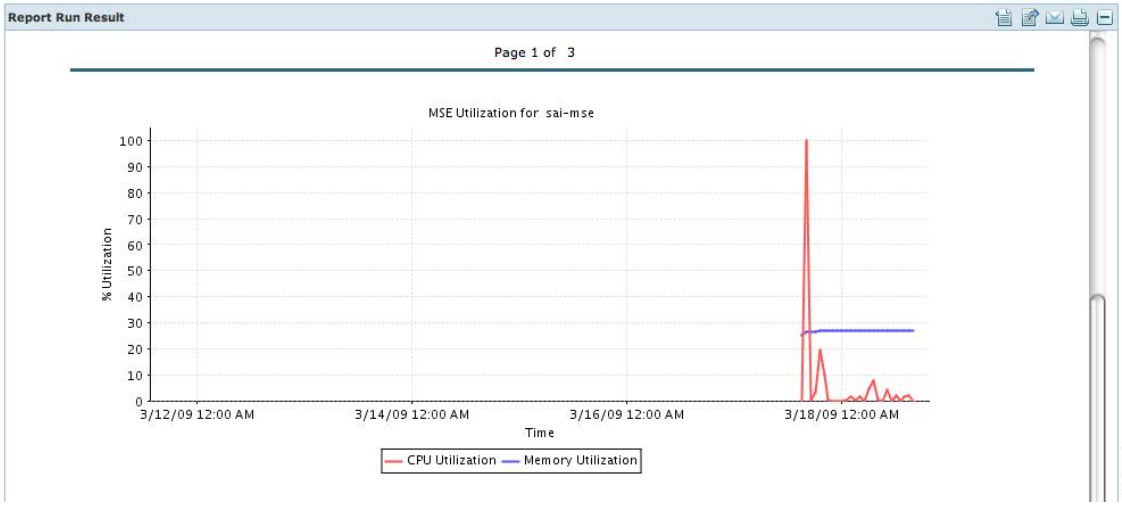
Note The days of the week appear on the page only when the weekly option is chosen.

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 1: 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.

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

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 38
- Editing a GPS Marker, on page 39
- Deleting a GPS Marker From the Floor, on page 39

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.

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.

Interpreting Security Dashboard

The Prime Infrastructure Security Dashboard have the following features added to it:

- Valid Client on Rogue AP
- Soft AP
- Good Guy Gone Bad (GGGB)

All the above features falls under the Client Classification table on the security dashboard. Hyperlinks are provided for the counts of Rogue APs. By clicking on the hyperlinks provided in the table, you will be able to view the details of Soft AP, GGGB and Valid Client on Rogue.

Viewing the Rogue APs

To view the Rogue Access Points (APs), perform the following steps:

SUMMARY STEPS

1. Click the **Valid Client connected to Rogue AP** number to view the clients who were previously associated with the enterprise network but are now associated with Rogue APs.
2. This page displays the following items:
3. Click the **Soft AP** number to view the clients who were previously probing but are now rogue APs.
4. This page displays the following items:
5. Click the **Good Guy Gone Bad** number to view the clients who were previously associated but are now Rogue APs.
6. This page displays the following items:

DETAILED STEPS

	Command or Action	Purpose
Step 1	Click the **Valid Client connected to Rogue AP** number to view the clients who were previously associated with the enterprise network but are now associated with Rogue APs.	
Step 2	This page displays the following items:	• Client Mac Address- Mac address of the client • Rogue AP Mac Address- Mac address of the rogue APs. • First Detected- Displays the date and time when a rogue AP was first detected • Last Detected- Displays the date and time when a rogue AP was last detected • Containment Start Time • Containment Stop Time • State- The state of the rogue AP when a Valid client is connected to rogue. The two states are, Alert and Threat
Step 3	Click the **Soft AP** number to view the clients who were previously probing but are now rogue APs.	
Step 4	This page displays the following items:	• Type- Displays the type of the client • Soft AP MAC Address- Mac address of the Soft AP • TimeStamp- Displays the exact date and time when a soft AP was detected
Step 5	Click the **Good Guy Gone Bad** number to view the clients who were previously associated but are now Rogue APs.	
Step 6	This page displays the following items:	• Type- Displays the type of the client

	Command or Action	Purpose
		• Good Guy Gone Bad Mac Address- Mac address of the Good Guy Gone Bad client • TimeStamp- Displays the exact date and time when a soft AP was detected

Client Classification

There are three clients:

Valid Client Connected to Rogue AP: When a client associates with rogue AP, MSE will check whether the client is a valid client. For valid clients, an entry is added to the Rogue AP table with the MAC addresses of both the devices. Depending on the containment action taken, containment fields are updated. The following scenarios needs to be considered:

- Client associates and then disappears
- Client dissociation information is available
- Incomplete Containment

Soft AP: A Soft Access Point (Soft AP) is set-up on a Wi-Fi adapter without the need of a physical Wi-Fi router. It is easy to set-up a Soft AP on the Windows 7 or Windows Vista Machine with Windows 7 virtual Wi-Fi capabilities. Once up and running, it is easy to share the network access available on a machine to other Wi-Fi users that will connect to the Soft AP. If an employee sets up a soft Access Point on his machine inside the corporate premises, and share the corporate network through it, then this soft AP behaves as Rogue AP. You can also turn on Wi-Fi tethering on your smartphone and act as a rogue AP. MSE detects this scenario of soft rogue AP and sends response to Controller for auto containment.

Good Guy Gone Bad: When a valid client turns into a Soft AP, it is a greater threat which need s immediate action. MSE detect s these scenarios and report s a good guy gone bad.