Monitoring Wireless Devices

You can monitor your wireless devices in your network on a daily basis, as well as perform other day-to-day or ad hoc operations related to wireless device inventory.

Monitoring Controllers

Choose **Monitor > Managed Elements > Network Devices**, then select **Device Type > Wireless Controller** to view all the wireless controllers.

Related Topic

- Monitoring System Parameters

Monitoring System Parameters

Choose **Monitor > Managed Elements > Network Devices**, then select **Device Type > Wireless Controller** to view all the wireless controllers. Click a Device name to view its details. You can monitor all the wireless controller details described in Table 9-1.

Table 9-1 Monitor > Network Devices > Wireless Controller Details

To View ...	Select This Menu ...
System Information	
Summary information such as IP address, device type, location, reachability status, description, etc.	**System > Summary** under **Device Details** tab
CLI session details	**System > CLI Sessions** under **Device Details** tab

Table 9-1 Monitor > Network Devices > Wireless Controller Details

To View ...	Select This Menu ...
DHCP statistics (for version 5.0.6.0 controllers or later) such as packets sent and received, DHCP server response information, and the last request time stamp	**System > DHCP Statistics** under **Device Details** tab
Multicast information	**System > Multicast** under **Configuration** tab
Stack information such as MAC address, role, state, etc.	**System > Stacks** under **Device Details** tab
STP statistics	**System > Spanning Tree Protocol** under **Configuration** tab
Information about any user-defined fields	**System > User Defined Field** under **Device Details** tab
Wireless local access networks (WLANs) configured on a controller	**System > WLANs** under **Device Details** tab
Mobility	
Statistics for mobility group events such as receive and transmit errors, handoff request, etc.	**Mobility > Mobility Stats** under **Device Details** tab
Ports	
Information regarding physical ports on the selected controller	**Ports > General** under **Configuration** tab
CDP Interfaces	**Ports > CDP Interface Neighbors** under **Configuration** tab
Security	
RADIUS accounting server information and statistics	**Security > RADIUS Accounting** under **Device Details** tab
RADIUS authentication server information	**Security > RADIUS Authentication** under **Device Details** tab
Information about network access control lists	**System > Security > Network Access Control**
Guest access deployment and network users	**Security > Guest Users** under **Device Details** tab
Management Frame Protection (MFP) summary information	**System > Security > Management Frame Protection** under **Device Details** tab
List of all rogue access point rules currently applied to a controller.	**System > Security > Rogue AP Rules** under **Device Details** tab
List of sleeping clients, which are clients with guest access that have had successful web authentication that are allowed to sleep and wake up without having to go through another authentication process through the login page	**Security > Sleeping Clients** under **Device Details** tab
IPv6	
Statistics for the number of messages exchanged between the host or client and the router to generate and acquire IPv6 addresses, link, MTU, etc.	**IPv6 > Neighbor Binding Timers** under **Configuration** tab
Redundancy	
Redundancy information	**System > Redundancy Summary** under **Device Details** tab
mDNS	
List of mDNS services and service provider information.	**mDNS > mDNS Service Provider** under **Device Details** tab

Related Topics

- Wireless Controller System Summary

- Spanning Tree Protocol
- Management Frame Protection
- Rogue AP Rules

Spanning Tree Protocol

The Spanning Tree Protocol (STP) is a link management protocol. Cisco WLAN Solution implements the IEEE 802.1D standard for media access control bridges.

The spanning tree algorithm provides redundancy while preventing undesirable loops in a network that are created by multiple active paths between stations. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail.

The following controllers do not support Spanning Tree Protocol: WISM, 2500, 5500, 7500 and SMWLC.

Related Topics

- Wireless Controller > System > Spanning Tree Protocol
- Monitoring Controllers

Management Frame Protection

Management Frame Protection (MFP) provides the authentication of 802.11 management frames. Management frames can be protected to detect adversaries who are invoking denial of service attacks, flooding the network with probes, interjecting as rogue access points, and affecting the network performance by attacking the QoS and radio measurement frames.

If one or more of the WLANs for the controller has MFP enabled, the controller sends each registered access point a unique key for each BSSID the access point uses for those WLANs. Management frames sent by the access point over the MFP enabled WLANs is signed with a Frame Protection Information Element (IE). Any attempt to alter the frame invalidates the message causing the receiving access point configured to detect MFP frames to report the discrepancy to the WLAN controller.

Related Topic

Monitoring Controllers

Rogue AP Rules

Rogue AP rules automatically classify rogue access points based on criteria such as authentication type, matching configured SSIDs, client count, and RSSI values. Prime Infrastructure applies the rogue access point classification rules to the controllers and respective access points.

These rules can limit a rogue appearance on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time).

Rogue AP Rules also help reduce false alarms.

Rogue classes include the following types:

- Malicious Rogue—A detected access point that matches the user-defined malicious rules or has been manually moved from the Friendly AP category.
- Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined friendly rules.
- Unclassified Rogue—A detected access point that does not match the malicious or friendly rules.

Related Topic

- Monitoring Controllers

Monitoring Third Party Controllers

Choose **Monitor > Managed Elements > Network Devices> Third Party Wireless Controllers** to view the detailed information about the third party (non-Cisco) controllers that are managed by Prime Infrastructure.

Monitoring Switches

Choose **Monitor > Managed Elements > Network Devices > Switches and Hubs** to view the following detailed information about the switches:

- Searching Switches

  Use the Prime Infrastructure search feature to find specific switches or to create and save custom searches.
- Viewing the Switches

Related topics

- Monitor > Switches > Search
- Monitor > Switches > View

Configuring the Switch List Page

The Edit View page allows you to add, remove, or reorder columns in the Switches table.

To edit the available columns in the table, follow these steps:

Step 1 Choose **Monitor > > Managed Elements > Network Devices > Switches and Hubs**.

Step 2 Click the **Edit View** link.

Step 3 To add an additional column to the 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 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.

Related topics

- Monitor > Switches > Search
- Monitor > Switches > View

Monitoring Switch System Parameters

Choose **Monitor > Managed Elements > Network Devices > Switches and Hubs**, then click on a Device Name to view the following detailed information about the switch:

- Viewing Switch Memory Information
- Viewing Switch Environment Information
- Viewing Switch Module Information
- Viewing Switch VLAN Information
- Viewing Switch VTP Information
- Viewing Switch Physical Ports Information
- Viewing Switch Sensor Information
- Viewing Switch Spanning Tree Information
- Viewing Spanning Tree Details
- Viewing Switch Stacks Information
- Viewing Switch NMSP and Location Information

Related Topics

- Viewing Switch Information

Viewing Switch Information

To view switch information, follow these steps:

Step 1 Choose **Monitor > Managed Elements > Network Devices > Switches and Hubs**.

Step 2 Click an Device Name in the Device Name column to view details about the switch.

Step 3 Click one of the following from the **System** menu to view the relevant information:

- Environment
- Modules
- VLANs
- VTP
- Physical Ports
- Sensors
- Spanning Tree

- Stacks
- NMSP and Location

Related Topic

- Monitoring Switch Interfaces
- Monitor > Switches > IP Address
- Monitor > Switches > Memory
- Monitor > Switches > Environment
- Monitor > Switches > Modules
- Monitor > Switches > VLANs
- Monitor > Switches > VTP
- Monitor > Switches > Physical Ports
- Monitor > Switches > Sensors
- Monitor > Switches > Spanning Tree
- Monitor > Switches > Spanning Tree Details
- Monitor > Switches > Stacks

Monitoring Switch Interfaces

Step 1 Choose **Monitor > Managed Elements > Network Devices > Switches and Hubs**.

Step 2 Click an Device Name in the Device Name column to view details about the switch.

Step 3 Click **Interfaces** to view the following information:

- Monitoring Switch Ethernet Interfaces
- Monitoring Switch Ethernet Interface Details
- Monitoring Switch IP Interfaces
- Monitoring Switch VLAN Interfaces
- Monitoring Switch EtherChannel Interfaces

Related Topics

- Viewing Switch Interface Information

Viewing Switch Interface Information

To view switch interface information, follow these steps:

Step 1 Choose **Monitor > Managed Elements > Network Devices > Switches and Hubs**.

Step 2 Click an Device Name in the Device Name column to view details about the switch.

Step 3 Click **Interfaces**.

Step 4 Click one of the following to view the relevant information:

- Ethernet Interfaces
- Ethernet Interface Name
- IP Interfaces
- VLAN Interfaces
- EtherChannel Interfaces

Related Topics

- Monitor > Switches > Interfaces > Ethernet Interfaces
- Monitor > Switches > Interfaces > Ethernet Interface Name
- Monitor > Switches > Interfaces > IP Interface
- Monitor > Switches > Interfaces > VLAN Interface
- Monitor > Switches > Interfaces > EtherChannel Interface

Monitoring Switch Clients

To view switch interface information, follow these steps:

Step 1 Choose **Monitor > Managed Elements > Network Devices > Switches and Hubs**.

Step 2 Click an Device Name in the Device Name column to view details about the switch.

Step 3 Choose **Clients** from the System Menu to monitor switch clients.

Monitoring Access Points

This section describes access to the controller access points summary details. Use the main date area to access the respective access point details.

Choose **Monitor > Wireless Technologies> Access Point Radios** to access this page.

Related Topics

- Searching for Access Points
- Viewing a List of Access Points
- Types of Reports for Access Points
- Monitoring Access Points Details

Searching for Access Points

Use the Prime Infrastructure Search feature to find specific access points or to create and save custom searches.

Related Topics

- Viewing a List of Access Points
- Types of Reports for Access Points
- Monitoring Access Points
- Monitoring Access Points Details
- Search Methods

Viewing a List of Access Points

Choose **Monitor > Wireless Technologies> Access Point Radios** or perform an access point search to view the summary of access points including the default information.

Related Topics

- Searching for Access Points
- Types of Reports for Access Points
- Monitoring Access Points
- Monitoring Access Points Details
- Viewing a List of Access Points

Configuring the List of Access Points Display

The **Edit View** page allows you to add, remove, or reorder columns in the Access Points table.

To edit the available columns in the alarms table:

Step 1 Choose **Monitor > Wireless Technologies > Access Point Radios**.

Step 2 Click the **Edit View** link.

Step 3 To add an additional column to the access points table, highlight the column heading in the left column and click **Show** to move the heading to the right column. An additional column will be added to the left of the highlighted column.

Step 4 To remove a column from the access points table, highlight the column heading of the column on the right of the column you want to remove and click **Hide**.

All items in the left column will be removed from the table.

Step 5 Use the **Up/Down** buttons to specify the order in which the information appears in the table. Highlight the desired row 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.

Related Topics

- Monitoring Access Points
- Searching for Access Points
- Viewing a List of Access Points
- Monitoring Access Points Details

Types of Reports for Access Points

The following reports can be generated for Access Points. These reports cannot be customized.

- Load—Generates a report with load information.
- Dynamic Power Control—Generates a report with Dynamic Power Control information.
- Noise—Generates a report with Noise information.
- Interference—Generates a report with Interference information.
- Coverage (RSSI)—Generates a report with Coverage (RSSI) information.
- Coverage (SNR)—Generates a report with Coverage (SNR) information.
- Up/Down Statistics—Time in days, hours and minutes since the last reboot. Generates a report with Up Time information.
- Network Airtime Fairness Statistics—Tabular representation of Average Airtime used across different WLAN profiles in the selected interval of time.
- Voice Statistics—Generates a report for selected access points showing radio utilization by voice traffic.
- Voice TSM Table—Generates a report for selected access points and radio, organized by client device showing QoS status, PLR, and latency of its voice traffic stream.
- Voice TSM Reports—Graphical representation of the TSM table except that metrics from the clients are averaged together on the graphs.
- 802.11 Counters—Displays counters for access points at the MAC layer. Statistics such as error frames, fragment counts, RTS/CTS frame count, and retried frames are generated based on the filtering criteria and can help interpret performance (and problems, if any) at the MAC layer.
- AP Profile Status—Displays access point load, noise, interference, and coverage profile status.
- Air Quality vs. Time—Displays the air quality index of the wireless network during the configured time duration.
- Traffic Stream Metrics—Determines the current and historical quality of service (QoS) for given clients at the radio level. It also displays uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.
- Tx Power and Channel—Displays the channel plan assignment and transmit power level trends of devices based on the filtering criteria used when the report was generated. It can help identify unexpected behavior or issues with network performance.

- VoIP Calls Graph—Helps analyze wireless network usage from a voice perspective by providing details such as the number and duration of VoIP calls (per radio) on the network over time. VoIP snooping must be enabled on the WLAN to be able to gather useful data from this report. This report displays information in a graph.
- VoIP Calls Table—Provides the same information as the VoIP Calls Graph report but in table form.
- Voice Statistics—Helps analyze wireless network usage from a voice perspective by providing details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, and rejected calls (per radio) on the network. To be able to gather useful data from this report, make sure call admission control (CAC) is supported on voice clients.
- Worst Air Quality APs—Provides a high-level, easy-to- understand metric to facilitate understanding of where interference problems are impacting the network. Air Quality (AQ) is reported at a channel, floor, and system level and it supports AQ alerts, so that you can be automatically notified when AQ falls below a desired threshold.

Note Tx Power and Channel report and AP Profile Status report in Cisco Prime Infrastructure may not show data for all the polling instances. This is because of a mechanism in the database that compresses the identical rows in a table.

- TX Power and Channel report and AP Profile Status report fetches data from "**lradifstats**" table in the database, which contains the following information:
  - Channel number
  - Tx Power level
  - Operational status
  - Load profile state
  - Noise Profile state
  - Interference profile state
  - Coverage profile state

  The compression logic is applied to all the above columns in the table. If values in all the columns are the same, then the entry is compressed. For example, consider that the polling happened at interval t1, t2, t3, t4, and t5. If the values at interval t1 to t4 are the same and changes at t5, then Prime Infrastructure keeps t1, t4, and t5 entries in the database.
- The compression logic applies to Preferred Calls report also. But this report gets data from a different table "**lradifprefvoicecallstats**", which has the columns: Number of calls received and Number of calls accepted.

Related Topics

- Monitoring Traffic Load
- Monitoring Dynamic Power Control
- Monitoring Access Points Noise
- Monitoring Access Points Interference
- Monitoring Access Points Coverage (RSSI)
- Monitoring Access Points Coverage (SNR)
- Monitoring Access Points Up/Down Statistics
- Monitoring the Access Points Voice Statistics

- Monitoring the Access Points Voice TSM Table
- Monitoring the Access Points Voice TSM Reports
- Monitoring Access Points 802.11 Counters
- Monitoring Access Points AP Profile Status
- Monitoring Air Quality
- Monitoring Access Points Traffic Stream Metrics
- Monitoring Access Points Tx Power and Channel
- Monitoring VoIP Calls
- Monitoring Voice Statistics
- Monitoring Air Quality

Generating Reports for Access Points

To generate a report for access points:

Step 1 Choose **Monitor > Wireless Technologies > Access Point Radios.**

Step 2 Click to select the access point(s) for which you want to run a report.

Step 3 Choose the applicable report from the Select a report drop-down list.

Step 4 Click **Go**.

Related Topics

- Types of Reports for Access Points

Monitoring Traffic Load

Traffic Load is the total amount of bandwidth used for transmitting and receiving traffic. This enables WLAN managers to track network growth and plan network growth ahead of client demand.

To generate the access point load report:

Step 1 Choose **Monitor > Wireless Technologies > Access Point Radios.**

Step 2 Select the check box(es) of the applicable access point(s).

Step 3 From the Generate a report for selected APs drop-down list, choose **Load**.

Step 4 Click **Go**. The Load report displays for the selected access points.

Related Topics

- Types of Reports for Access Points
- Monitor > Access Points > Load

Monitoring Dynamic Power Control

To generate the Access Point Load report:

Step 1 Choose **Monitor > Wireless Technologies > Access Point Radios**.

Step 2 Select the check box(es) of the applicable access point(s).

Step 3 From the Generate a report for selected APs drop-down list, choose **Dynamic Power Control**.

Step 4 Click **Go**. The Dynamic Power Control report displays the selected access points.

Related Topics

- Types of Reports for Access Points
- Monitor > Access Points > Dynamic Power Control

Monitoring Access Points Noise

To generate the Access Point Noise report:

Step 1 Choose **Monitor > Wireless Technologies > Access Point Radios**.

Step 2 Select the check box(es) of the applicable access point(s).

If multiple access points are selected, they must have the same radio type.

Step 3 Choose **Noise** from the **Generate a report selected APs** drop-down list,.

Step 4 Click **Go**.

The Noise report displays a bar graph of noise (RSSI in dBm) for each channel for the selected access points.

Related Topics

- Types of Reports for Access Points

Monitoring Access Points Interference

To generate the Access Point Interference report:

Step 1 Choose **Monitor > Wireless Technologies > Access Point Radios**.

Step 2 Select the check box(es) of the applicable access point(s).

If multiple access points are selected, they must have the same radio type.

Step 3 Choose **Interference** from the **Generate a report for selected APs** drop-down list, then click **Go**.

The Interference report displays a bar graph of interference (RSSI in dBm) for each channel:

- High interference -40 to 0 dBm.
- Marginal interference -100 to -40 dBm.

- Low interference -110 to -100 dBm.

Related Topics

- Types of Reports for Access Points

Monitoring Access Points Coverage (RSSI)

To generate the Access Point Coverage (RSSI) report:

Step 1 Choose **Monitor > Wireless Technologies > Access Point Radios**

Step 2 Select the check box(es) of the applicable access point(s).

Step 3 Choose **Coverage (RSSI)** from the Generate a report for selected APs drop-down list.

Step 4 Click **Go**.

The Coverage (RSSI) report displays a bar graph of client distribution by received signal strength showing the number of clients versus RSSI in dBm.

Related Topics

- Types of Reports for Access Points

Monitoring Access Points Coverage (SNR)

To generate the Access Point Coverage (SNR) report:

Step 1 Choose **Monitor > Wireless Technologies > Access Point Radios**.

Step 2 Select the check box(es) of the applicable access point(s).

Step 3 Choose **Coverage (SNR)** from the **Generate a report for selected APs** drop-down list, then click **Go**.

The Access Points Coverage (SNR) report displays a bar graph of client distribution by signal-to-noise ratio showing the number of clients versus SNR.

Related Topics

- Types of Reports for Access Points

Monitoring Access Points Up/Down Statistics

To generate the Access Point Up/Down Statistics report:

Step 1 Choose **Monitor > Wireless Technologies > Access Point Radios.**

Step 2 Select the check box of the applicable access point.

Step 3 Choose **Up/Down Statistics** from the **Generate a report for selected APs** drop-down list.

Click **Go**.

The Up/Down Statistics report displays a line graph of access point up time graphed against time.

Related Topics

- Types of Reports for Access Points

Monitoring the Access Points Voice Statistics

To generate the Access Point Voice Statistics report:

Step 1 Choose **Monitor > Wireless Technologies > Access Point Radios**.

Step 2 Select the check box(es) of the applicable access point(s).

Step 3 Choose **Voice Statistics** from the **Generate a report for selected APs** drop-down list, then click **Go**.

The Voice Statistics report displays the following radio utilization statistics by voice traffic:

- AP Name.
- Radio.
- Calls in Progress
- Roaming Calls in Progress
- Bandwidth in Use

Voice Statistics reports are only applicable for CAC/WMM clients.

Related Topics

- Types of Reports for Access Points

Monitoring the Access Points Voice TSM Table

To access the Access Point Voice TSM Table report:

Step 1 Choose **Monitor > Wireless Technologies > Access Point Radios.**

Step 2 Select the check box of the applicable access point.

Step 3 Choose **Voice TSM Table** from the **Generate a report for selected APs** drop-down list.

Step 4 Click **Go**.

The Voice Traffic Stream Metrics Table is generated for the selected access points and radio, organized by client device showing QoS status, PLR, and latency of its voice traffic stream.

Related Topics

- Types of Reports for Access Points
- Monitor > Wireless Technologies > Access Point Radios > Voice TSM Table

Monitoring the Access Points Voice TSM Reports

To access the access point Voice Traffic Stream Metrics Table report:

Step 1 Choose **Monitor > Wireless Technologies > Access Point Radios**.

Step 2 Select the check box of the applicable access point.

Step 3 Choose **Voice TSM Reports** from the **Generate a report for selected APs** drop-down list.

Step 4 Click **Go**.

The Voice Traffic Stream Metrics Table report displays a graphical representation of the Voice Traffic Stream Metrics Table except that metrics from the clients that are averaged together on the graphs for the selected access point.

Related Topics

- Types of Reports for Access Points
- Monitor > Wireless Technologies > Access Point Radios > Voice TSM Reports

Monitoring Access Points 802.11 Counters

The 8o2.11 Counters report displays counters for access points at the MAC layer. Statistics such as error frames, fragment counts, RTS/CTS frame count, and retried frames are generated based on the filtering criteria and can help interpret performance (and problems, if any) at the MAC layer.

Related Topics

- Types of Reports for Access Points
- Managing Reports

Monitoring Access Points AP Profile Status

The AP Profile Status Report displays access point load, noise, interference, and coverage profile status.

Related Topics

- Types of Reports for Access Points
- Managing Reports

Monitoring Access Points Radio Utilization

The Radio Utilization Report displays the utilization trends of the access point radios based on the filtering criteria used when the report was generated. It helps to identify current network performance and capacity planning for future scalability needs.

Related Topics

- Types of Reports for Access Points
- Managing Reports

Monitoring Access Points Traffic Stream Metrics

The Traffic Stream Metrics Report is useful in determining the current and historical quality of service (QoS) for given clients at the radio level. It also displays uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.

Related Topics

- Types of Reports for Access Points
- Managing Reports

Monitoring Access Points Tx Power and Channel

The Tx Power and Channel report displays the channel plan assignment and transmits power level trends of devices based on the filtering criteria used when the report was generated. It can help identify unexpected behavior or issues with network performance.

The Current Tx Power Level setting controls the maximum conducted transmit power. The maximum available transmit power varies according to the configured channel, individual country regulation, and access point capability. See the *Product Guide* or data sheet at for each specific model to determine the access point capability.

The Current Tx Power Level setting of 1 represents the maximum conducted power setting for the access point. Each subsequent power level (for example. 2, 3, 4, and so on.) represents approximately a 50% (or 3dBm) reduction in transmit power from the previous power level. The actual power reduction might vary slightly for different models of access points.

Based on the configured antenna gain, the configured channel, and the configured power level, the actual transmit power at the access point can be reduced so that the specific country regulations are not exceeded.

Irrespective of whether you choose Global or Custom assignment method, the actual conducted transmit power at the access point is verified such that country specific regulations are not exceeded.

The following command buttons are available to configure the transmission levels:

- Save—Save the current settings.
- Audit—Discover the present status of this access point.

Related Topics

- Types of Reports for Access Points
- Managing Reports

Monitoring VoIP Calls

VoIP Calls Report helps analyze wireless network usage from a voice perspective by providing details such as the number and duration of VoIP calls (per radio) on the network over time. To be able to gather useful data from this report, VoIP snooping must be enabled on the WLAN. This report displays information in a graph.

Click **VoIP Calls Graph** from the Report Launch Pad to open the VoIP Calls Graph Reports page. From this page, you can enable, disable, delete, or run currently saved report templates.

Related Topics

- Types of Reports for Access Points
- Managing Reports

Monitoring Voice Statistics

Voice Statistics report helps analyze wireless network usage from a voice perspective by providing details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, and rejected calls (per radio) on the network.

To be able to gather useful data from this report, make sure Call Admission Control (CAC) is supported on voice clients.

Related Topics

- Types of Reports for Access Points
- Managing Reports

Monitoring Air Quality

To facilitate an easy understanding of where interference problems are impacting the network, Prime Infrastructure rolls up the detailed information into a high-level, easy-to- understand metric referred to as Air Quality (AQ). AQ is reported at a channel, floor, and system level and it supports AQ alerts, so that you can be automatically notified when AQ falls below a desired threshold.

Related Topics

- Types of Reports for Access Points
- Managing Reports

Monitoring Access Points Details

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

Choose **Monitor > Wireless Technologies > Access Point Radios** and click the access point name in the **AP Name** column to access this page. Depending on the type of access point, the following tabs are displayed:

- General Tab

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

For autonomous clients, 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.

- Interfaces Tab
- CDP Neighbors Tab

  This tab is visible only when CDP is enabled.
- Current Associated Clients Tab

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

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

  The information that appears in these charts is presented in a time-based graph. Time-based graphs have 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.

Related Topics

- Types of Reports for Access Points
- Monitor > Wireless Technologies > Access Point Radios> General
- Monitor > Wireless Technologies > Access Point Radios> Interfaces
- Monitor > Wireless Technologies > Access Point Radios > CDP Neighbors
- Monitor > Wireless Technologies > Access Point Radios > Current Associated Clients
- Monitor > Wireless Technologies > Access Point Radios> SSID

Monitoring Rogue Access Points

A rogue device is an unknown access point or client that is detected by managed access points in your network. Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain-text or other denial of service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as usernames and passwords. The hacker can then transmit a series of clear-to-send (CTS) frames. This action mimics an access point informing a particular client to transmit and instructing all others to wait, which results in legitimate clients being unable to access network resources. Therefore, wireless LAN service providers have a strong interest in banning rogue access points from the air space.

Since rogue access points are inexpensive and readily available, employees sometimes plug unauthorized rogue access points into existing LANs and build ad-hoc wireless networks without IT department knowledge or consent. These rogue access points can be a serious breach of network security as they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. Even more alarming, wireless users frequently publish insecure access point locations, increasing the odds of having enterprise security breached.

Related Topics

- Detecting Rogue Devices
- Classifying Rogue Access Points
- Monitoring Rogue AP Alarms
- Monitoring Ad hoc Rogues
- Searching Rogue Clients Using Advanced Search
- Monitoring Rogue Access Point Location, Tagging, and Containment

Detecting Rogue Devices

Controllers continuously monitor all nearby access points and automatically discover and collect information on rogue access points and clients. When a controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) to determine if the rogue is attached to your network. Prime Infrastructure consolidates all of the controllers rogue access point data.

You can configure controllers to use RLDP on all access points or only on access points configured for monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded RF space, allowing monitoring without creating unnecessary interference and without affecting regular data access point functionality. If you configure a controller to use RLDP on all access points, the controller always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to either manually or automatically contain the detected rogue.

Rogue access point partitions are associated with one of the detecting access points (the one with the latest or strongest RSSI value). If there is detecting access point information, Prime Infrastructure uses the detecting controller. If the rogue access point is detected by two controllers which are in different partitions, the rogue access point partition might be changed at any time.

Related Topics

- Configuring Rogue Policies
- Monitoring Rogue Access Points
- Classifying Rogue Access Points
- Monitoring Rogue AP Alarms
- Monitoring Ad hoc Rogue Alarms

Classifying Rogue Access Points

Classification and reporting of rogue access points occurs through the use of rogue states and user-defined classification rules that enable rogues to automatically move between states. You can create rules that enable the controller to organize and display rogue access points as Friendly, Malicious, or Unclassified.

By default, none of the classification rules are enabled. Therefore, all unknown access points are categorized as Unclassified. When you create a rule, configure conditions for it, and enable the rule, the unclassified access points are reclassified. Whenever you change a rule, it is applied to all access points (friendly, malicious, and unclassified) in the Alert state only.Rule-based rogue classification does not apply to ad-hoc rogues and rogue clients.

The 5500 series controllers support up to 2000 rogues (including acknowledged rogues); the 4400 series controllers, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch support up to 625 rogues; and the 2100 series controllers and Controller Network Module for Integrated Services Routers support up to 125 rogues. Each controller limits the number of rogue containments to three per radio (or six per radio for access points in monitor mode).

When the controller receives a rogue report from one of its managed access points, it responds as follows:

1. The controller verifies whether the unknown access point is in the friendly MAC address list. If it is, the controller classifies the access point as Friendly.
2. If the unknown access point is not in the friendly MAC address list, the controller starts applying rogue classification rules.
3. If the rogue is already classified as Malicious, Alert or Friendly, Internal or External, the controller does not reclassify it automatically. If the rogue is classified differently, the controller reclassifies it automatically only if the rogue is in the Alert state.
4. The controller applies the first rule based on priority. If the rogue access point matches the criteria specified by the rule, the controller classifies the rogue according to the classification type configured for the rule.
5. If the rogue access point does not match any of the configured rules, the controller classifies the rogue as Unclassified.
6. The controller repeats the previous steps for all rogue access points.
7. If RLDP determines that the rogue access point is on the network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if no rules are configured. You can then manually contain the rogue (unless you have configured RLDP to automatically contain the rogue), which would change the rogue state to Contained. If the rogue access point is not on the network, the controller marks the rogue state as Alert, and you can manually contain the rogue.
8. If desired, you can manually move the access point to a different classification type and rogue state.

As mentioned previously, the controller can automatically change the classification type and rogue state of an unknown access point based on user-defined rules, or you can manually move the unknown access point to a different classification type and rogue state.

The following table shows the allowable classification types and rogue states from and to which an unknown access point can be configured.

Table 9-2 Allowable Classification Type and Rogue State Transitions

From	To
Friendly (Internal, External, Alert)	Malicious (Alert)
Friendly (Internal, External, Alert)	Unclassified (Alert)
Friendly (Alert)	Friendly (Internal, External)
Malicious (Alert, Threat)	Friendly (Internal, External)
Malicious (Contained, Contained Pending)	Malicious (Alert)
Unclassified (Alert, Threat)	Friendly (Internal, External)
Unclassified (Contained, Contained Pending)	Unclassified (Alert)
Unclassified (Alert)	Malicious (Alert)

If the rogue state is Contained, you have to uncontain the rogue access point before you can change the classification type. If you want to move a rogue access point from Malicious to Unclassified, you must delete the access point and allow the controller to reclassify it.

Malicious Rogue APs

Malicious rogue access points are detected but untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification.

The Security dashboard of Prime Infrastructure home page displays the number of malicious rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active malicious rogue access points.

Malicious rogue access point states include:

- Alert—Indicates that the access point is not on the neighbor list or part of the user-configured Friendly AP list.
- Contained—The unknown access point is contained.
- Threat—The unknown access point is found to be on the network and poses a threat to WLAN security.
- Contained Pending—Indicates that the containment action is delayed due to unavailable resources.
- Removed—This unknown access point was seen earlier but is not seen now.

Click an underlined number in any of the time period categories for detailed information regarding the malicious rogue access points.

Friendly Rogue APs

Friendly rogue access points are known, acknowledged or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained.

Only users can add a rogue access point MAC address to the Friendly AP list. Prime Infrastructure does not apply the Friendly AP MAC address to controllers.

The Security dashboard of Prime Infrastructure home page displays the number of friendly rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active friendly rogue access points.

Friendly rogue access point states include the following:

- Internal—If the unknown access point is inside the network and poses no threat to WLAN security, you would manually configure it as Friendly, Internal. For example, the access points in your lab network.
- External—If the unknown access point is outside the network and poses no threat to WLAN security, you would manually configure it as Friendly, External. For example, the access points belonging to a neighboring coffee shop.
- Alert—The unknown access point is not on the neighbor list or part of the user-configured Friendly AP list.

Click an underlined number in any of the time period categories for detailed information regarding the friendly rogue access points.

To delete a rogue access point from the Friendly AP list, ensure that both Prime Infrastructure and controller remove the rogue access point from the Friendly AP list. Change the rogue access point from Friendly AP Internal or External to Unclassified or Malicious Alert.

Unclassified Rogue APs

A rogue access point is called unclassified, if it is not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list.

The Security dashboard of the Prime Infrastructure home page displays the number of unclassified rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active unclassified rogue access points.

Unclassified rogue access point states include:

- Pending—On first detection, the unknown access point is put in the Pending state for 3 minutes. During this time, the managed access points determine if the unknown access point is a neighbor access point.
- Alert—The unknown access point is not on the neighbor list or part of the user-configured Friendly AP list.
- Contained—The unknown access point is contained.
- Contained Pending—The unknown access point is marked Contained, but the action is delayed due to unavailable resources.

Click an underlined number in any of the time period categories for further information.

Related Topics

- Monitoring Rogue Access Points
- Detecting Rogue Devices

Monitoring Rogue AP Alarms

Rogue access point radios are unauthorized access points detected by one or more Cisco 1000 series lightweight access points. To open the Rogue AP Alarms page, do one of the following:

- Search for rogue APs.

- Navigate to **Dashboard > Wireless > Security**. This page displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
- Click the **AP number** link in the Alarm Summary.

If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use it to view additional alarms.

Rogue access point partitions are associated with one of the detecting access points (the one with the latest or strongest RSSI value). If there is detecting access point information, Prime Infrastructure uses the detecting controller. If the rogue access point is detected by two controllers which are in different partitions, the rogue access point partition might be changed at any time.

When Prime Infrastructure polls, some data might change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

Related Topic

- Rogue AP Alarms Page
- Alarm Severity Icons
- Selecting Commands for Rogue AP Alarms

Viewing Rogue AP Alarm Details

Rogue access point radios are unauthorized access points detected by Cisco 1000 Series Lightweight APs. Alarm event details for each rogue access point are available in the Rogue AP Alarms list page.

To view alarm events for a rogue access point radio, select **Monitor > Monitoring Tools > Alarms and Events**, and click the arrow icon in a row to view Rogue AP Alarm Details page.

All Alarm Details page fields (except No. of Rogue Clients) are populated through polling and are updated every two hours. The number of rogue clients is a real-time number and is updated each time you access the Alarm Details page for a rogue access point alarm.

When a controller (version 7.4 or 7.5) sends custom rogue AP alarm, Prime Infrastructure shows it as unclassified rogue alarm. This is because Prime Infrastructure does not support custom rogue AP alarm.

When Prime Infrastructure polls, some data might change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

Related Topics

- Monitoring Rogue Access Points
- Monitoring Ad hoc Rogue Alarms
- Viewing Ad hoc Rogue Alarm Details
- Selecting Commands for Rogue AP Alarms

Viewing Rogue Client Details

You can view a list of rogue clients in several ways:

- Perform a search for rogue clients using Prime Infrastructure Search feature.

- View the list of rogue clients for a specific rogue access point from the Alarm Details page for the applicable rogue access point. Click the Rogue MAC address for the applicable rogue client to view the Rogue Client details page.
- In the Alarms Details page of a rogue access point, choose **Rogue Clients** from the Select a command drop-down list.

The Rogue Clients page displays the Client MAC address, when it was last heard, its current status, its controller, and the associated rogue access point.

Rogue client statuses include: Contained (the controller contains the offending device so that its signals no longer interfere with authorized clients); Alert (the controller forwards an immediate alert to the system administrator for further action); and Threat (the rogue is a known threat).The higher the threat of the rogue access point, the higher the containment required.

Click the Client MAC Address for the rogue client to view the Rogue Client details page. T

Related Topics

- Monitoring Rogue Access Points
- Monitoring Rogue AP Alarms
- Monitoring Ad hoc Rogue Alarms
- Monitoring Ad hoc Rogue Events
- Viewing Ad hoc Rogue Alarm Details
- Selecting Commands for Rogue AP Alarms

Viewing Rogue AP History Details

To view the history of a rogue AP alarms, click the **Rogue AP History** link in the Rogue AP Alarm page. Click the Rogue MAC address to view the specific rogue AP history details page.

Related Topics

- Rogue AP History Details Page
- Rogue AP Event History Details Page

Viewing Rogue AP Event History Details

To view the event details of a rogue AP, click the **Event History** link in the Rogue AP Alarm page.

Related Topics

- Monitoring Rogue Access Points
- Monitoring Rogue AP Alarms
- Monitoring Ad hoc Rogue Alarms
- Monitoring Rogue Alarm Events
- Rogue AP History Details Page
- Rogue AP Event History Details Page

Monitoring Ad hoc Rogues

If the MAC address of a mobile client operating in a ad hoc network is not in the authorized MAC address list, then it is identified as an ad hoc rogue.

Related Topics

- Viewing Rogue AP Alarm Details
- Viewing Rogue Client Details
- Viewing Rogue AP History Details
- Monitoring Ad hoc Rogue Alarms
- Viewing Ad hoc Rogue Alarm Details

Monitoring Ad hoc Rogue Alarms

The Adhoc Rogue Alarms page displays alarm events for ad hoc rogues.To access the Adhoc Rogue Alarms page, do one of the following:

- Perform a search for ad hoc rogue alarms.
- Navigate to **Dashboard > Wireless > Security**. This page displays all the ad hoc rogues detected in the past hour and the past 24 hours. Click the ad hoc rogue number to view the ad hoc rogue alarms.

If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

When Prime Infrastructure polls, some data might change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

Related Topics

- Viewing Rogue AP History Details
- Viewing Ad hoc Rogue Alarm Details
- Selecting Commands for Rogue AP Alarms

Viewing Ad hoc Rogue Alarm Details

Alarm event details for each ad hoc rogue is available on the Adhoc Rogue Alarms page. Rogue access point radios are unauthorized access points detected by Cisco 1000 Series Lightweight APs

To view alarm events for an ad hoc rogue radio, click the applicable Rogue MAC address in the Adhoc Rogue Alarms page.

When Prime Infrastructure polls, some data might change or get updated. Hence some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

Alarms will not be triggered if a rogue is discovered using switch port tracing as switch port tracing does not update any of the rogue attributes such as severity, state, and so on.

Related Topics

- Searching Rogue Clients Using Advanced Search

- Viewing Ad hoc Rogue Alarm Details
- Selecting Commands for Rogue AP Alarms

Searching Rogue Clients Using Advanced Search

When the access points on your WLAN are powered up and associated with controllers, Prime Infrastructure immediately starts listening for rogue access points. When a controller detects a rogue access point, it immediately notifies Prime Infrastructure, which creates a rogue access point alarm.

To find rogue access point alarms using Advanced Search, follow these steps:

Step 1 Click **Advanced Search** in the top right-hand corner of the Prime Infrastructure main page.

Step 2 Choose **Rogue Client** from the Search Category drop-down list.

You can filter the search even further with the other search criteria if desired.

Step 3 Click **Search**. The list of rogue clients appears.

Step 4 Choose a rogue client by clicking a client MAC address. The Rogue Client detail page appears.

Step 5 To modify the alarm, choose one of these commands from the **Select a Command** drop-down list, and click **Go**.

- Set State to 'Unknown-Alert'—Tags the ad hoc rogue as the lowest threat, continues to monitor the ad hoc rogue, and turns off containment.
- 1 AP Containment through 4 AP Containment—Indicates the number of access points (1-4) in the vicinity of the rogue unit that send deauthenticate and disassociate messages to the client devices that are associated to the rogue unit.
- Map (High Resolution)—Displays the current calculated rogue location in the Maps > Building Name > Floor Name page.
- Location History—Displays the history of the rogue client location based on RF fingerprinting. The client must be detected by an MSE for the location history to appear.

Related Topics

- Viewing Rogue AP Alarm Details
- Monitoring Rogue Access Point Location, Tagging, and Containment

Monitoring Rogue Access Point Location, Tagging, and Containment

Prime Infrastructure generates the flags as rogue access point traps and displays the known rogue access points by MAC address Cisco Unified Network Solution is monitoring it.

The operator displays a map showing the location of the access points closest to each rogue access point. These access points are classified as:

- Known or Acknowledged rogue access points (no further action)
- Alert rogue access points (watch for and notify when active)
- Contained rogue access points

This built-in detection, tagging, monitoring, and containment capability enables system administrators to take appropriate action:

- Locate rogue access points.
- Receive new rogue access point notifications, eliminating hallway scans.
- Monitor unknown rogue access points until they are eliminated or acknowledged.
- Determine the closest authorized access point, making directed scans faster and more effective.
- Contain rogue access points by sending their clients deauthenticate and disassociate messages from one to four access points. This containment can be done for individual rogue access points by MAC address or can be mandated for all rogue access points connected to the enterprise subnet.
- Tag rogue access points:
  - Acknowledge rogue access points when they are outside of the LAN and do not compromise the LAN or WLAN security
  - Accept rogue access points when they do not compromise the LAN or WLAN security
  - Tag rogue access points as unknown until they are eliminated or acknowledged
- Tag rogue access points as contained and discourage clients from associating with the rogue access points by having between one and four access points transmit deauthenticate and disassociate messages to all rogue access point clients. This function applies to all active channels on the same rogue access point.

Related Topics

- Detecting Access Points
- Monitoring Rogue Alarm Events

Detecting Access Points

Use the Detecting Access Points feature to view information about the Cisco Lightweight APs that are detecting a rogue access point.

To access the Rogue AP Alarms details page, follow these steps:

Step 1 To display the Rogue AP Alarms page, do one of the following:

- Perform a search for rogue APs.
- Navigate to **Dashboard > Wireless > Security**. This dashboard displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
- Click the **Malicious AP** number link in the Alarm Summary box.

Step 2 In the Rogue AP Alarms page, click the Rogue MAC Address for the applicable rogue access point. The Rogue AP Alarms details page appears.

Step 3 From the Select a command drop-down list, choose **Detecting APs**.

Step 4 Click **Go**.

Click a list item to display data about that item.

Related Topics

- Monitoring Rogue Access Point Location, Tagging, and Containment
- Monitoring Rogue Alarm Events

Monitoring Rogue Alarm Events

The Events page enables you to review information about rogue alarm events. Prime Infrastructure generates an event when a rogue access point is detected or if you make manual changes to a rogue access point (such as changing its state). The Rogue AP Events list page displays all rogue access point events.

To access the Rogue AP Events list page, follow these steps:

Step 1 Do one of the following:

- Perform a search for rogue access point events using the Advanced Search feature of Prime Infrastructure.
- In the Rogue AP Alarms details page, click **Event History** link.

Related Topics

- Detecting Access Points
- Viewing Rogue AP Event Details
- Rogue AP Event History Details Page

Viewing Rogue AP Event Details

To view rogue access point event details, in the Rogue AP Events list page, click the **Rogue MAC Address** link.

Related Topics

- Monitoring Rogue Alarm Events
- Monitoring Ad hoc Rogue Events
- Rogue AP Event History Details Page
- Selecting Commands for Rogue AP Alarms

Monitoring Ad hoc Rogue Events

The Events page enables you to review information about ad hoc rogue events. Prime Infrastructure generates an event when an ad hoc rogue is detected or if you make manual changes to an ad hoc rogue (such as changing its state). The Adhoc Rogue Events list page displays all ad hoc rogue events.

To access the Rogue AP Events list page, either perform a search for ad hoc rogues events using the Advanced Search feature of Prime Infrastructure or in the Adhoc Rogue Alarms details page, click **Event History** from the **Select a Command** drop-down list.

Related Topics

- Viewing Rogue AP Event Details
- Viewing Ad hoc Rogue Event Details

Viewing Ad hoc Rogue Event Details

To view rogue access point event details, in the Rogue AP Events list page, click the **Rogue MAC Address** link.

Related Topics

- Viewing Rogue AP Event Details
- Monitoring Ad hoc Rogue Events
- Rogue AP Event History Details Page

Troubleshooting Unjoined Access Points

When a lightweight access point initially starts up, it attempts to discover and join a WLAN controller. After joining the wireless controller, the access point updates its software image if needed and receives all the configuration details for the device and network. After successfully joining the wireless controller, the access point can be discovered and managed by Prime Infrastructure. Until the access point successfully joins a wireless controller the access point cannot be managed by Prime Infrastructure and does not contain the proper configuration settings to allow client access.

Prime Infrastructure provides you with a tool that diagnoses why an access point cannot join a controller and lists corrective actions.

The Unjoined AP page displays a list of access points that have not joined any wireless controllers. All gathered information about the unjoined access point is included in the page. This includes name, MAC address, IP address, controller name and IP address, switch and port that the access point is attached to, and any join failure reason if known.

To troubleshoot unjoined access points, do the following:

Step 1 Choose **Monitor > Wireless Technologies > Unjoined Access Points**. The Unjoined APs page appears containing a list of access points that have not been able to join a wireless controller.

Step 2 Select the access point that you wish to diagnose, then click **Troubleshoot**.

An analysis is run on the access point to determine the reason why the access point was not able to join a wireless controller. After performing the analysis, the Unjoined APs page displays the results. The middle pane, you can view what the problem is. It will also list error messages and controller log information.

Step 3 Select a controller.

If the access point has tried to join multiple wireless controllers and has been unsuccessful, the controllers are listed in the left pane.

Step 4 Perform one of the recommended actions from the list of recommendations for solving the problems listed in the right pane.

Step 5 Run RTTS through the Unjoined AP page to further diagnose a problem. This allows you to see the debug messages from all the wireless controllers that the access point tried to join at one time.

To run RTTS, click the RTTS icon ( ) located to the right of the table. The debug messages appear in the table. You can then examine the messages to see if you can determine a cause for the access point not being able to join the controllers.

Related Topics

- Monitoring Rogue Access Points
- Monitoring Ad hoc Rogues

Monitoring Spectrum Experts

A Spectrum Expert client acts as a remote interference sensor and sends dynamic interference data to Prime Infrastructure. This feature allows Prime Infrastructure to collect, archive and monitor detailed interferer and air quality data from Spectrum Experts in the network.

To access the Monitor Spectrum Experts page, follow these steps:

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

From the left sidebar menu, you can access the Spectrum Experts Summary page.

Related Topics

- Field Reference guide for Spectrum Experts Summary
- Field Reference guide for Interferer's Summary
- Field Reference guide for Spectrum Experts Details
- Searching Interferers

Monitoring WiFi TDOA Receivers

The WiFi TDOA receiver is an external system designed to receive signals transmitted from a tagged, tracked asset. These signals are then forwarded to the mobility services engine to aid in the location calculation of the asset.

To view WiFi TDOA receiver information:

Step 1 Choose **Monitor > Wireless Technologies > WiFi TDOA Receivers**.

Related Topics

- Searching WiFi TDOA Receivers

Searching WiFi TDOA Receivers

To refine the search criteria for WiFi TDOA receivers:

Step 1 Click the **Advanced Search** in the Prime Infrastructure user interface.

Step 2 Choose **WiFi TDOA Receiver** from the Search Category drop-down list.

- To initiate a search for a Wi-Fi TDOA receiver by its MAC address, choose **MAC Address** from the Search drop-down list and enter the MAC address of the Wi-Fi TDOA receiver in the available text box, and click **Search**.
- To initiate a search for a Wi-Fi TDOA receiver by its name, choose **WiFi TDOA Receivers** from the Search by drop-down list and enter the name of the Wi-Fi TDOA receiver in the available text box, and click **Search**.

Related Topics

- Monitoring WiFi TDOA Receivers

Monitoring Media Streams

To view all the media streams configured across controllers:

Step 1 Choose **Monitor > Wireless Technologies > Media Streams**.

Related Topics

- Viewing Media Stream Details

Viewing Media Stream Details

To view media stream details:

Step 1 Choose **Monitor > Wireless Technologies > Media Streams**.

Step 2 Click the **Stream Name** link.

Related Topics

- Monitoring Media Streams
- Monitoring WiFi TDOA Receivers

Radio Resource Management

The Radio Resource Management (RRM), built into the Cisco Unified Wireless Network, monitors and dynamically corrects performance issues found in the RF environment. Prime Infrastructure receives traps whenever a change in the transmit power in the access point or channel occurred. These trap events or similar events such as RF regrouping are logged into Prime Infrastructure and are maintained by the event dispatcher.

RRM automatically detects and configures new controllers and lightweight access points as they are added to the network. It automatically adjusts associated and nearby lightweight access points to optimize coverage and capacity. Lightweight access points can simultaneously scan all valid 802.11b/g channels for the country of operation as well as for channels available in other locations. The access points go off-channel for a period not greater than 60 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points.

The following notifications are sent to RRM dashboard:

- Channel change notifications are sent when a channel change occurs. Channel change depends on the Dynamic Channel Assignment (DCA) configuration.
- Transmission power change notifications are sent when transmission power changes occur. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur.
- RF grouping notifications are sent when there is a RF grouping content change and automatic grouping is enabled.

Related Topics

- Viewing the RRM Dashboard

Viewing the RRM Dashboard

To view the RRM dashboard information:

Step 1 Choose **Monitor > Wireless Technologies > Radio Resource Management**.

Related Topics

- Radio Resource Management

Monitoring Access Point Alarms

To monitor the Access Point (AP) alarms on your network:

Step 1 Perform an advanced search for **AP** alarms.

The **Search Results** page contains the following information for AP alarms. You can select the check box next to the alarm and modify the required fields in the **Alarm Browser** toolbar.

- Severity
- Failure Source
- Owner
- Time
- Message
- Category
- Condition

- Acknowledged

Step 2 Select the check box next to the alarm and modify the required fields in the **Alarm Browser** toolbar.

Monitoring Air Quality Alarms

To monitor air quality alarms on your network:

Step 1 Perform an advanced search for **Performance** alarms.

The **Search Results** page contains the following information for air quality alarms.

- Severity
- Failure Source
- Owner
- Time
- Message
- Category
- Condition
- Acknowledged

Step 2 Select the check box next to the alarm and modify the required fields in the **Alarm Browser** toolbar.

Monitoring CleanAir Security Alarms

To monitor CleanAir security alarms:

Step 1 Perform an advanced search for **Security** alarms.

The **Search Results** page contains the following information for CleanAir Security alarms.

- Severity
- Failure Source
- Owner
- Date/Time
- Message
- Acknowledged

Step 2 Select the check box next to the alarm and modify the required fields in the **Alarm Browser** toolbar.

Monitoring Cisco Adaptive wIPS Alarms

Alarms from Cisco Adaptive wIPS DoS (denial of service) and security penetration attacks are classified as security alarms.

To view a list of wIPS DoS and security penetration attack alarms:

Step 1 Perform an advanced search for **wIPS DoS** alarms.

The **Search Results** page contains the following information.

- Severity
- Failure Object
- Date/Time
- Message
- Acknowledged
- Category
- Condition
- When there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

Step 2 Select the check box next to the alarm and modify the required fields in the **Alarm Browser** toolbar.

Monitoring Cisco Adaptive wIPS Alarm Details

To monitor Cisco Adaptive wIPS alarm details:

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

- General
  - 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 controllers and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events.

    Trap—Generated by the controller. Prime Infrastructure process these traps and raises corresponding events for them.

  - Severity—Level of severity including critical, major, info, 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—Displays any annotations that you have entered.
- Messages—Displays information about the alarm.
- Audit Report—Click to view configuration audit alarms details. This report is only available for Configuration Audit alarms.

  Configuration audit alarms are generated when audit discrepancies are enforced on configuration groups.
- Rogue Clients—If the failure object is a rogue access point, information about rogue clients is displayed.

Related Topics

- Monitoring Cisco Adaptive wIPS Alarms

Monitoring Failure Objects

To monitor failure objects, follow these steps:

Step 1 Choose **Monitor > Monitoring Tools > Alarms and Events**, then click the **Events** tab.

Step 2 Click the expand icon to the left of the Description column. Depending on the type of event you selected, the associated details vary.

- General Info
  - Failure Source—Indicates the source of the event (including name and/or MAC address).
  - Category—Type of alarm such as Security or AP.
  - Generated—Date and time that the event was generated.
  - 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 controllers and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events.

Trap—Generated by the controller. Prime Infrastructure process these traps and raises corresponding events for them.

- Device IP Address—IP address of the alarm-generating device.
- Severity—Level of severity including critical, major, info, warning, and clear.

- Messages—Message explaining why the event occurred.

Monitoring Events for Rogue Access Points

To monitor events for rogue access points:

Step 1 Choose **Monitor > Monitoring Tools > Alarms and Events**, then click the **Events** tab.

Step 2 Use the Quick Filter or Advanced Filter feature to monitor the Rogue APs.

Step 3 Click the expand icon to view alarm events for a rogue access point radio.

The following fields appear:

General

- Rogue MAC Address
- Vendor
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Owner—Name of person to which this alarm is assigned, or (blank).
- State—State of this radio relative to the network or Port. Rogue access point radios appear as “Alert” when first scanned by the Port, or as “Pending” when operating system identification is still underway.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Containment Level—An access point which is being contained is either unable to provide service at all, or provides exceedingly slow service. There is a level associated with the containment activity which indicates how many Cisco 1000 series lightweight access points to use in containing the threat. This service must be initiated and halted by the administrator. Containment Type - Contained if the rogue access point clients have been contained at Level 1 through Level 4 under Update Status, otherwise Unassigned.
- Channel—Indicates the band at which the ad hoc rogue is broadcasting.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Created—Date and time that the event occurred.
- 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 controllers and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events.
  - Trap—Generated by the controller. Prime Infrastructure process these traps and raises corresponding events for them.
- Device IP Address—IP address of the alarm-generating device.
- Severity—Level of severity, Critical, Major, Minor, Warning, and Clear, Info.

Message—Displays descriptive information about the alarm.

Help—Displays information about the alarm.

Related Topics

- Monitoring Rogue Access Points

Monitoring Events for Ad hoc Rogues

To monitor events for ad hoc rogues:

Step 1 Choose **Monitor > Monitoring Tools > Alarms and Events**, then click the **Events** tab.

Step 2 Use the Quick Filter or Advanced Filter feature to monitor the events for Ad hoc Rogue APs.

Step 3 Click the expand icon to view alarm events for an ad hoc rogue access point. The following fields are displayed:

General

- Rogue MAC Address
- Vendor
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Owner—Name of person to which this alarm is assigned, or (blank).
- State—State of this radio relative to the network or Port. Rogue access point radios appear as “Alert” when first scanned by the Port, or as “Pending” when operating system identification is still underway.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Containment Level—An access point which is being contained is either unable to provide service at all, or provides exceedingly slow service. There is a level associated with the containment activity which indicates how many Cisco 1000 series lightweight access points to use in containing the threat. This service must be initiated and halted by the administrator. Containment Type - Contained if the rogue access point clients have been contained at Level 1 through Level 4 under Update Status, otherwise Unassigned.

- Channel—Indicates the band at which the ad hoc rogue is broadcasting.
- Created—Date and time that the event occurred.
- 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 controllers and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events.
  - Trap—Generated by the controller. Prime Infrastructure process these traps and raises corresponding events for them.
  - Device IP Address—IP address of the alarm-generating device.
- Severity—Level of severity, Critical, Major, Minor, Warning, and Clear, Info.

Message—Displays descriptive information about the alarm.

Step 4 Help—Displays information about the alarm.

Related Topics

- Monitoring Rogue Access Points

Monitoring Cisco Adaptive wIPS Events

To monitor Cisco adaptive wIPS events:

Step 1 Choose **Monitor > Monitoring Tools > Alarms and Events**, then click the Events tab.

Step 2 Use the Quick Filter or Advanced Filter feature to narrow down the search results to monitor wIPS events. One or more events might generate an abnormal state or alarm. The alarm can be cleared, but the event remains.

Monitoring CleanAir Air Quality Events

To view the events generated on CleanAir air quality of the wireless network:

Step 1 Perform an advanced search for **Performance** event.

The **Search Results** page contains the following CleanAir air quality events information:

- Severity—Indicates the severity of the alarm.
- Failure Source—Device that generated the alarm.
- Date/Time—The time at which the alarm was generated.

Related Topics

- Viewing Air Quality Event Details

Viewing Air Quality Event Details

To view air quality event details:

Step 1 From the Air Quality Events page, click an expand icon adjacent to **Severity** column to access the alarm details page.

Step 2 The air quality event page displays the following information:

- Failure Source—Device that generated the alarm.
- Category—The category this event comes under. In this case, Performance.
- Created—The time stamp at which the event was generated.
- Generated by—The device that generated the event.
- Device IP Address—The IP address of the device that generated the event.
- Severity—The severity of the event.
- Alarm Details—A link to the related alarms associated with this event. Click the link to learn more about the alarm details.
- Message—Describes the air quality index on this access point.

Monitoring Interferer Security Risk Events

To monitor interferer security risk events:

Step 1 To view the security risk event generated on your wireless network, perform an advanced search for **Security** event.

The **Search Results** page contains the following interferer security events information:

- Severity—Indicates the severity of the alarm.
- Failure Source—Device that generated the alarm.
- Date/Time—The time at which the alarm was generated.

Related Topics

- Viewing Interferer Security Risk Event Details

Viewing Interferer Security Risk Event Details

To view interferer security event details:

Step 1 In the Interferer Security Event details page, click an expand icon adjacent to **Severity** column to access the alarm details page.

Step 2 The air quality event page displays the following information:

- Failure Source—Device that generated the alarm.
- Category—The category this event comes under. In this case, Security.

- Created—The time stamp at which the event was generated.
- Generated by—The device that generated the event.
- Device IP Address—The IP address of the device that generated the event.
- Severity—The severity of the event.
- Alarm Details—A link to the related alarms associated with this event. Click the link to know more about the alarm details.
- Message—Describes the interferer device affecting the access point.

Related Topics

- Monitoring Interferer Security Risk Events

Monitoring Health Monitor Events

To view the health monitor events:

Step 1 Perform an advanced search for **Prime Infrastructure** event.

The **Search Results** page contains the following health monitor events related information:

- Severity—Indicates the severity of the alarm.
- Failure Source—Device that generated the alarm.
- Date/Time—The time at which the alarm was generated.
- Message—Describes the health details.

Related Topics

- Viewing Health Monitor Event Details

Viewing Health Monitor Event Details

To view health monitor event details:

Step 1 In the Health Monitor Events page, click an expand icon adjacent to **Severity** column to access the alarm details page.

Step 2 The Health Monitor Events page displays the following information:

- Failure Source—Device that generated the alarm.
- Category—The category this event comes under.
- Created—The time stamp at which the event was generated.
- Generated by—The device that generated the event.
- Device IP Address—The IP address of the device that generated the event.
- Severity—The severity of the event.

- Alarm Details—A link to the related alarms associated with this event. Click the link to know more about the alarm details.
- Message—Describes the event through a message.

Related Topics

- Monitoring Health Monitor Events