Monitor Wireless Devices

- Monitor Controllers, on page 1
- View Access Point Radio Air Time Fairness Information, on page 8
- What is a Rogue Access Point, on page 8
- What is an Ad hoc Rogue, on page 14
- View Access Points Interference Information from Spectrum Experts, on page 16
- Monitor WiFi TDOA Receivers, on page 16
- View RF Performance Using Radio Resource Management Dashboard, on page 16
- View Access Points Alarms and Events, on page 17
- Using Telemetry, on page 19

Monitor Controllers

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

Related Topics

Monitor System Parameters, on page 1

Monitor 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.

From Release 3.2 onwards, for the following Monitor pages under **Device Details** > **System**, by default the data is fetched from the Prime Infrastructure database. There is an option to refresh from device by clicking the **Refresh from Device** link in the upper right corner of the page. It also shows the date and time when the data was last refreshed on the Prime Infrastructure.

- Summary
- CDP Neighbors
- WLANs

From Release 3.2 onwards, for the following Monitor pages under **Device Details** > **System**, the data is fetched directly from the device.

- CLI Sessions
- DHCP Statistics

Table 1: Monitor Network Devices Wireless Controller Details

To View ...	Select This Menu ...
System Information	**System > Summary** under **Device Details tab**
Summary information such as IP address, device type, location, reachability status, description, and total device count	
CLI session details	**System > CLI Sessions** under **Device Details tab**
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, and state	**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	**Mobility > Mobility Stats** under **Device Details tab**
Statistics for mobility group events such as receive and transmit errors, and handoff request	
Ports	**Ports > General** under **Configuration tab**
Information regarding physical ports on the selected controller	
CDP Interfaces	**Ports > CDP Interface Neighbors** under **Configuration tab**
Security	**Security > RADIUS Accounting** under **Device Details tab**
RADIUS accounting server information and statistics	
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**

To View ...	Select This Menu ...
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	**IPv6** > **Neighbor Binding Timers** under **Configuration tab**
Statistics for the number of messages exchanged between the host or client and the router to generate and acquire IPv6 addresses, link, and MTU	
Redundancy	**System** > **Redundancy Summary** under **Device Details tab**
Redundancy information	
mDNS	**mDNS** > **mDNS Service Provider** under **Device Details tab**
List of mDNS services and service provider information	

Related Topics

What is Spanning Tree Protocol, on page 3
What is Management Frame Protection, on page 3
What are Rogue Access Points Rules, on page 4

What is 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.

What is 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.

What are Rogue Access Points Rules

Rogue Access Points 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 Access Points 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 Access Points 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 Topics

Monitor System Parameters, on page 1

View System Details About 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.

View System Details About Switch Controllers and Configure the Switch List

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

Configure 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.

Monitor 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

View Access Points, on page 5
View System Details About Access Points, on page 7

View 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

Types of Reports for Access Points, on page 5
View System Details About Switch Controllers and Configure the Switch List, on page 4

Types of Reports for Access Points

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

- 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.
- Dynamic Power Control—Generates a report with Dynamic Power Control information.
- Noise—Generates a report with Noise information. The Noise report displays a bar graph of noise (RSSI in dBm) for each channel for the selected access points.
- Interference—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
- Coverage (RSSI)—The Coverage (RSSI) report displays a bar graph of client distribution by received signal strength showing the number of clients versus RSSI in dBm.
- Coverage (SNR)—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.
- Up/Down Statistics—The Up/Down Statistics report displays a line graph of access point up time graphed against time. Time in days, hours and minutes since the last reboot.

- Network Airtime Fairness Statistics—Network Airtime Fairness Statistics is a 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. The Voice Statistics report displays the following radio utilization statistics by voice traffic:
  - Access Points Name
  - Radio
  - Calls in Progress
  - Roaming Calls in Progress
  - Bandwidth in Use

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

- Voice TSM Table—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.
- Voice TSM Reports—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.
- 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.
- Access Points Profile Status—The Access Points Profile Status displays access point load, noise, interference, and coverage profile status.
- Air Quality vs. Time—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. The Radio Utilization Report displays the air quality index of the wireless network during the configured time duration.
- 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.
- Tx Power and Channel—The Tx Power and Channel report 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.

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.
- VoIP Calls Graph—VoIP Calls Graph analyzes 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—VoIP Calls Table provides the same information as the VoIP Calls Graph report but in table form.
- Voice Statistics—Voice Statistics Report analyzes 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.

View System Details About Access Points

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

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 Access Point (CAPWAP or Autonomous Access Point).

- SSID Tab

This tab is visible only when the access point is an Autonomous Access Point and there are SSIDs configured on the Access Point

- Clients Over Time Tab

This tab displays the following charts:

- Client Count on Access Point—Displays the total number of clients currently associated with an access point over time.
- Client Traffic on Access Point—Displays the traffic generated by the client connected in the Access Point 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, on page 5

View Access Point Radio Air Time Fairness Information

Cisco Air Time Fairness (ATF) for High Density Experience (HDX) allows network administrators to group devices of a defined category and enables some groups to receive traffic from the WLAN more frequently than other groups. Therefore, some groups are entitled to more air time than other groups.

Cisco ATF has the following capabilities:

- Allocates Wi-Fi air time for user groups or device categories
- Air time fairness is defined by the network administrator and not by the network
- Provides a simplified mechanism for allocating air time
- Dynamically adapts to changing conditions in a WLAN
- Enables a more efficient fulfillment of service-level agreements
- Augments standards-based Wi-Fi QoS mechanisms

To monitor the ATF Statistics:

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

Step 2 Click the desired radio name in the **Radio** column.

Depending on the type of access point, different tabs are displayed.

Step 3 In the **Access Point Radio Details**, choose the **Air Time Fairness** tab.

The following charts are displayed:

- **Air Time Usage Absolute**—This chart represents the percent Air Time Usage by a WLAN on a Radio during the measured interval of time.
  - Click the calendar icon to choose the start date and year and end date and year or choose a preset value. The presets available are 1h, 6h, 1d, 1w, 2w, 4w, 3m, 6m, and 1y.
- **Air Time Usage Relative**—This chart displays the percent Air Time usage by a WLAN across all WLAN s on a radio.
- Click the calendar icon to choose the start date and year and end date and year or choose a preset value. The presets available are 1h, 6h, 1d, 1w, 2w, 4w, 3m, 6m, and 1y.

What is a Rogue Access Point

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

How Cisco Prime Infrastructure Detects Rogue Access Points, on page 9
How Rogue Access Point States Are Determined, on page 10
View Rogue Access Point Alarms, on page 12
What is an Ad hoc Rogue, on page 14
View Rogue Access Point Clients , on page 13
How Prime Infrastructure Locates, Tags, and Contains Rogue Access Points , on page 14

How Cisco Prime Infrastructure Detects Rogue Access Points

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

What is a Rogue Access Point, on page 8
How Rogue Access Point States Are Determined, on page 10
View Rogue Access Point Alarms, on page 12
View Ad Hoc Rogue Access Point Alarms, on page 14

How Rogue Access Point States Are Determined

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.

Related Topics

What is a Rogue Access Point, on page 8
How Cisco Prime Infrastructure Detects Rogue Access Points, on page 9
How Rogue Access Points are Classified, on page 10

How Rogue Access Points are Classified

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

Table 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 Access Point 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 Access Point list. Prime Infrastructure does not apply the Friendly Access Point 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 Access Point 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 Access Point list, ensure that both Prime Infrastructure and controller remove the rogue access point from the Friendly Access Point list. Change the rogue access point from Friendly Access Point 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 Access Point 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

What is a Rogue Access Point, on page 8
How Cisco Prime Infrastructure Detects Rogue Access Points, on page 9

View Rogue Access Point Alarms

Rogue access point radios are unauthorized access points detected by one or more Cisco 1000 series lightweight access points. To open the Rogue Access Point 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.

Alarm event details for each rogue access point are available in the Rogue Access Point 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 Access Point 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 Access Point alarm, Prime Infrastructure shows it as unclassified rogue alarm. This is because Prime Infrastructure does not support custom rogue Access Point 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.

View Rogue Access Point Clients

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

- Perform a search for rogue clients using Prime Infrastructure 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.

Related Topics

What is a Rogue Access Point, on page 8
View Rogue Access Point Alarms, on page 12
View Ad Hoc Rogue Access Point Alarms, on page 14

What is an Ad hoc Rogue

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

View Ad Hoc Rogue Access Point Alarms, on page 14
View Rogue Access Point Clients , on page 13

View Ad Hoc Rogue Access Point 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.

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.

How Prime Infrastructure Locates, Tags, and Contains Rogue Access Points

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

Identify the Lightweight Access Points That Detect Rogue Access Points, on page 15

Identify the Lightweight Access Points That Detect Rogue 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 Access Point Alarms details page, follow these steps:

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

- Perform a search for rogue Access Points
- 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 Access Point Alarms page, click the Rogue MAC Address for the applicable rogue access point. The Rogue Access Point 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

How Prime Infrastructure Locates, Tags, and Contains Rogue Access Points , on page 14

View Access Points Interference Information from 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:

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

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

Monitor 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.

Related Topics

Enhance Tag Location Reporting with WiFi TDOA Receivers
Add WiFi TDOA Receivers to Prime Infrastructure and Maps

View RF Performance Using Radio Resource Management Dashboard

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.

To view the RRM dashboard information choose **Monitor > Wireless Technologies > Radio Resource Management**.

View Access Points Alarms and Events

To monitor the Access Point alarms on your network:

Step 1 Perform an advanced search for the following:
a) Performance alarms
b) CleanAir Security alarms
c) wIPS DoS alarms

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

View Access Points 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.

View Access Points 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.

View Access Points Ad Hoc Rogues

To monitor events for ad hoc rogues:

Procedure

	Command or Action	Purpose
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.	

Related Topics

What is a Rogue Access Point, on page 8

View Access Points 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.

View Access Points CleanAir Air Quality Events

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

Perform an advanced search for Performance event.

The Search Results page contains information about severity, failure Source, and date and time.

What to do next

To view air quality event details click an expand icon adjacent to **Severity column** in the Air Quality Events page.

View Access Points Interferer Security Risk Events

To monitor interferer security risk events:

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 CleanAir air quality events information about severity, failure Source, and date and time.

What to do next

To view interferer security event details, click an expand icon adjacent to **Severity column** to access the alarm details page.

View Access Points Health Monitor Events

To view the health monitor events:

Perform an advanced search for Prime Infrastructure event.

The Search Results page contains information about severity, failure Source, messages and date and time.

View Health Monitor Event Details

To view health monitor event details click an expand icon adjacent to **Severity column** to access the alarm details page.

Related Topics

View Access Points Health Monitor Events, on page 19

Using Telemetry

This section describes how telemetry is used in Cisco Prime Infrastructure.

Devices that Support Telemetry

In Cisco Prime Infrastructure, telemetry supports the following devices:

- Cisco Catalyst 9800-40 Wireless Controller
- Cisco Catalyst 9800-80 Wireless Controller
- Cisco Catalyst 9800-L-F Wireless Controller
- Cisco Catalyst 9800-CL Wireless Controller for Cloud

Prerequisites for Using Telemetry

- You must enable NETCONF configuration on the Catalyst 9800 WLC.
- You must integrate Coral with the Cisco Prime Infrastructure server.

About Telemetry

Telemetry polls the device and collects telemetry data such as any change on the device like addition or removal of APs and clients.

Ports Used by Telemetry

- Prime Infrastructure to WLC: TCP port 830

  This is used by Cisco Prime Infrastructure to push the telemetry configuration to the 9800 devices using NETCONF.

- WLC to Prime Infrastructure: TCP port 20828 (for IOS-XE 16.10 and 16.11, Cisco PI 3.5 to 3.7).

  or

  TCP port 20830 (for IOS-XE 16.12,17.x and later, Cisco PI 3.8 onwards).

Note In case there is a firewall between Cisco Prime Infrastructure and Catalyst 9800, be sure to open these ports to establish communication

Difference Between Telemetry and SNMP in Cisco Prime Infrastructure

In SNMP, Cisco PI fetches the data from the device. It will also use SNMP to push configuration templates as well as support traps for AP and client events.

In telemetry, Cisco PI registers itself as a receiver to receive telemetry data and PI keeps listening to the device. The device is responsible for sending data such as discovery data and association and disassociation data of APs and clients. Telemetry does not fetch configuration data as in SNMP.

Verify Telemetry Status

To verify the telemetry connection to Prime from the C9800, use the **show telemetry internal connection** command.

```
#show telemetry internal connection
Telemetry connection

Address Port Transport State Profile
------------------------------------------------------------------
x.x.x.x 20828 cntp-tcp Active
```

If you have any issues with telemetry, you must collect the prime coral logs such as “Prime_TDL_collector_R0-”* logs.

For more information on telemetry on Cisco PI, see Managing Catalyst 9800 Wireless Controller Series with Prime Infrastructure using SNMP v2 and SNMP v3 and NetCONF.