



Field Reference for Monitor Pages

This section provides descriptions of the fields found under the **Monitor** tab in Cisco Prime Infrastructure.

- [Monitor > Switches > Physical Ports](#), on page 2
- [Monitor > Switches > Sensors](#), on page 2
- [Monitor > Switches > Spanning Tree](#), on page 3
- [Monitor > Switches > Spanning > Tree > STP instance ID](#) , on page 3
- [Monitor > Switches > Stacks](#) , on page 4
- [Monitor > Switches > Interfaces > Ethernet Interfaces](#), on page 4
- [Monitor > Switches > Interfaces > Ethernet Interface Name](#), on page 5
- [Monitor > Switches > Interfaces > IP Interface](#), on page 6
- [Monitor > Switches > Interfaces > VLAN Interface](#), on page 6
- [Monitor > Switches > Interfaces > EtherChannel Interface](#), on page 6
- [Monitor > Switches > Client](#), on page 7
- [Monitor > Wireless Technologies > Access Point Radios](#), on page 7
- [Monitor > Wireless Technologies > Access Point Radios > Edit View](#), on page 8
- [Monitor > Wireless Technologies > Access Point Radios > Load](#), on page 10
- [Monitor > Wireless Technologies > Access Point Radios > Dynamic Power Control](#), on page 10
- [Monitor > Wireless Technologies > Access Point Radios > Voice TSM Table](#), on page 11
- [Monitor > Wireless Technologies > Access Point Radios > Voice TSM Reports](#), on page 12
- [Monitor > Wireless Technologies > Access Point Radios > General](#), on page 13
- [Monitor > Wireless Technologies > Access Point Radios > Interfaces](#), on page 18
- [Monitor > Wireless Technologies > Access Point Radios > CDP Neighbors](#), on page 20
- [Monitor > Wireless Technologies > Access Point Radios > Current Associated Clients](#) , on page 21
- [Monitor > Wireless Technologies > Access Point Radios > SSID](#), on page 22
- [Rogue AP Alarms Page](#), on page 22
- [Alarm Severity Indicator Icons](#), on page 23
- [Selecting Commands for Rogue AP Alarms](#) , on page 24
- [Drop-Down Menus in Rogue AP Alarm Details Page](#), on page 25
- [Ad hoc Rogue Alarm Details](#), on page 26
- [Rogue AP History Details Page](#), on page 28
- [Rogue AP Event History Details Page](#), on page 29
- [Ad hoc Rogue Alarms Page](#), on page 30
- [Select Commands for Ad hoc Rogue AP Alarms](#), on page 31
- [View Ad hoc Rogue Alarm Details](#), on page 32

- [Chokepoints Page](#), on page 33
- [AP Detected Interferers Page](#), on page 34
- [AP Detected Interferer Details Page](#), on page 35
- [Monitor > Interferers > Interference Device ID > Location History](#), on page 36
- [Spectrum Experts > Summary](#), on page 37
- [Interferers > Summary](#), on page 37
- [Spectrum Experts Details Page](#), on page 38
- [Monitor > Network Devices > Unified AP](#), on page 39
- [Monitor > Network Devices > Wireless Controller > System Summary](#), on page 45
- [Wireless Controller System Spanning Tree Protocol](#), on page 47
- [Wireless Controller > System > CLI Sessions](#), on page 48
- [Wireless Controller > System > DHCP Statistics](#), on page 48
- [Wireless Controller > WLANs](#), on page 49
- [Wireless Controller > Ports](#), on page 50
- [Wireless Controller > CDP Neighbors](#), on page 50
- [Wireless Controller > Security > RADIUS Authentication](#), on page 51
- [Wireless Controller > Security > RADIUS Accounting](#), on page 52
- [Wireless Controller > Security > Management Frame Protection](#), on page 53
- [Wireless Controller > Security > Rogue AP Rules](#), on page 54
- [Wireless Controller Security Guest Users](#), on page 55
- [Wireless Controller > Mobility > Mobility Stats](#), on page 55
- [Wireless Controller > Redundancy > Redundancy Summary](#), on page 57
- [Monitor Tools](#), on page 58
- [Media Streams](#), on page 66

Monitor > Switches > Physical Ports

The following table describes the switch physical ports information:

Table 1: View Switches Physical Ports Information

Physical Ports	
Port Name	Name of the physical port.
Port Description	Description of the physical port.
Residing Module	Module on which the physical port resides.
Vendor Equipment Type	Description of vendor equipment type.

Monitor > Switches > Sensors

The following table describes the switch sensor information:

Table 2: View Switches Sensors Information

Sensors	
Sensor Name	Name of the sensor.
Sensor Description	Description of the sensor.
Type	Type of sensor.
Vendor Sensor Type	Description of vendor sensor type.
Equipment Name	Name of equipment.
Precision	When in the range 1 to 9, precision is the number of decimal places in the fractional part of a Sensor Value fixed-point number. When in the range -8 to -1, Sensor Precision is the number of accurate digits in a SensorValue fixed-point number.
Status	Operational status of the sensor.

Monitor > Switches > Spanning Tree

The following table describes the spanning tree information:

Table 3: View Switches Spanning Tree Information

Spanning Tree	
STP Instance ID	ID of the STP. Click an STP Instance ID to see the spanning tree details.
VLAN ID	ID of the VLAN.
Root Path Cost	Root cost of the path.
Designated Root	Forwarding port.
Bridge Priority	Priority of the bridge.
Root Bridge Priority	Priority number of the root bridge.
Max Age (sec)	STP timer value for maximum age (in seconds).
Hello Interval (sec)	STP timer value (in seconds).

Monitor > Switches > Spanning > Tree > STP instance ID

The following table describes the fields in the spanning tree details page:

Table 4: View Spanning Tree Details

Spanning Tree	
STP Port	Name of the STP port.
Port Role	Role of the port.
Port Priority	Priority number of the port.
Path Cost	Cost of the path.
Port State	State of the port.
Port Type	Type of port.

Monitor > Switches > Stacks

The following table describes the fields in switch stacks information page:

Table 5: View Switches Stacks Information

Stacks	
MAC Address	MAC address of the stack.
Role	Role of the stack: <ul style="list-style-type: none"> • Primary—Stack primary • Member—Active member of the stack • Not Member—Non-active stack member
Switch Priority	Priority number of the switch.
State	Current state of the stack.
Software Version	Software image running on the switch.

Monitor > Switches > Interfaces > Ethernet Interfaces

The following table describes the fields in the switch Ethernet interfaces page:

Table 6: View Switch Ethernet Interfaces

Ethernet Interfaces	
----------------------------	--

Name	Name of the Ethernet interface. Click an Ethernet interface name to see details.
MAC Address	MAC address of the Ethernet interface.
Speed (Mbps)	Estimate of the current bandwidth of the Ethernet interface in bits per second.
Operational Status	Current operational state of the Ethernet interface.
MTU	Size of the largest packet that can be sent/received on the interface.
Desired VLAN Mode	VLAN mode.
Access VLAN	VLAN on which the port is configured.

Monitor > Switches > Interfaces > Ethernet Interface Name

The following table describes the fields in the switch Ethernet interface details page:

Table 7: View Switch Ethernet Interface Details

Ethernet Interfaces	
Name	Name of the Ethernet interface.
Admin Status	Administration status of the interface.
Duplex Mode	Duplex mode configured on the interface.
VLAN Switch Port	
Operational VLAN Mode	Specifies the operational mode of the VLAN switch port, which can be either an access port or a trunk port.
Desired VLAN Mode	VLAN mode, which can be truck, access, dynamic, or desirable.
Access VLAN	VLAN on which the port is configured.
Operational Truck Encapsulation	Trunk encapsulation, which can be <i>802.1Q</i> or <i>none</i> .
VLAN Trunk	
Native VLAN	Untagged VLAN on the trunk switch port.
Prune Eligible	Specifies whether VLANs on the trunk port can be pruned.
Allows VLANs	List of allowed VLANs on the trunk port.
Desired Trunking Encapsulation	Trunk encapsulation.

Ethernet Interfaces	
Trunking Encapsulation Negotiation	Specifies that the interface negotiate with the neighboring interface to become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring interface.

Monitor > Switches > Interfaces > IP Interface

The following table describes the fields in the switch IP interfaces page:

Table 8: View Switch IP Interfaces

Interface	Name of the interface.
IP Address	IP address of the interface.
Address Type	Type of address (IPv4 or IPv6).

Monitor > Switches > Interfaces > VLAN Interface

The following table describes the fields in the switch VLAN interfaces page:

Table 9: View Switch VLAN Interfaces

Port Name	Name of the VLAN port.
VLAN ID	ID of the VLAN port.
Operational Status	Current operational state of the VLAN interface.
Admin Status	Current administrative state of the VLAN interface.
Port Type	Type of VLAN port.
Maximum Speed (Mbps)	Maximum supported speed for the VLAN interface.
MTU	Size of the largest packet that can be sent/received on the VLAN interface.

Monitor > Switches > Interfaces > EtherChannel Interface

The following table describes the fields in the switch EtherChannel interfaces page:

Table 10: View Switch EtherChannel Interfaces

Name	Name of the EtherChannel interface.
Channel Group ID	Numeric identifier for the EtherChannel.

Control Method	Protocol for managing the EtherChannel either LACP or TAGP.
Actor Admin Key	Channel Identifier.
Number of (LAG) Members	Number of ports configured.

Monitor > Switches > Client

The following table describes the fields in the switch clients page:

Table 11: View Current Associated Client

IP Address	IP address of the client.
MAC Address	MAC address of the client.
User Name	Username of the client.
Vendor Name	Vendor Name of the client.
Map Location	Location of the client.
VLAN	VLAN on which the client is configured.
Interface	Interface on which the client is configured.
Association Time	Timestamp of the client association.
Authorization Profile Name	Authorization Profile Name stored.

Monitor > Wireless Technologies > Access Point Radios

The following table describes the **Monitor > Wireless Technologies > Access Point Radios** fields.

Table 12: Access Point Search Results Fields

Field	Description
AP Name	The name assigned to the access point.
Ethernet MAC	AP Ethernet MAC address.
IP Address	Local IP address of the access point.
Radio	Protocol of the rogue access point is 802.11a, 802.11b or 802.11g. Click a list item to view access point radio details.
Map Location	Click a list item to go to the location indicated on the list.
Controller	Click a list item to display a graphic and information about the controller.
Client Count	Displays the total number of clients currently associated with the controller.

Field	Description
Admin Status	Displays the administration state of the access point as either enabled or disabled.
AP Mode	Displays the operational mode of the access point.
Oper Status	Displays the operational status of the Cisco WLAN Solution device, either Up or Down. If the admin status is disabled, the operation status is labeled as down and there are no alarms.
Alarm Status	Alarms are color coded as follows: <ul style="list-style-type: none"> • Clear-No Alarm • Red-Critical Alarm • Orange-Major Alarm • Yellow-Minor Alarm

Monitor > Wireless Technologies > Access Point Radios > Edit View

The following table describes the **Monitor > Wireless Technologies > Access Point Radios > Edit View** fields.

Table 13: Edit View Search Results Fields

Field	Description
AP Type	Displays the type of access point (unified or autonomous).
Antenna Azim. Angle	Displays the horizontal angle of the antenna.
Antenna Diversity	Displays if antenna diversity is enabled or disabled. Antenna diversity refers to the access point sampling the radio signal from two integrated antenna ports to choose the preferred antenna.
Antenna Elev. Angle	Displays the elevation angle of the antenna.
Antenna Gain	The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means $4 \times 0.5 = 2$ dBm of gain.
Antenna Mode	Displays the antenna mode such as omni, directional, or non-applicable.
Antenna Name	Displays the antenna name or type.

Field	Description
Audit Status	Displays one of the following audit statuses: <ul style="list-style-type: none"> • Mismatch-Configuration differences were found between Prime Infrastructure and controller during the last audit. • Identical-No configuration differences were found during the last audit. • Not Available-Audit status is unavailable.
Base Radio MAC	Displays the MAC address of the base radio.
Bridge Group Name	Displays the name of the bridge group used to group the access points, if applicable.
CDP Neighbors	Displays all directly connected Cisco devices.
Channel Control	Displays whether the channel control is automatic or custom.
Channel Number	Displays the channel on which the Cisco Radio is broadcasting.
Channel Width	Displays the channel bandwidth for this radio. The Channel Width field is supported only for 11n APs. Displays "N/A" for other APs.
Controller Port	Displays the number of controller ports.
Google Earth Location	Displays whether or not a Google Earth location is assigned and Displays the location.
Location	Displays the physical location of the access point.
Node Hops	Displays the number of hops between access points.
OfficeExtend AP	Specifies whether or not OfficeExtend access is enabled. If it is disabled, the access point is remotely deployed which increases the security risk.
PoE Status	Displays the power over Ethernet status of the access point. The possible values include the following: <ul style="list-style-type: none"> • Low-The access point draws low power from the Ethernet. • Lower than 15.4 volts-The access point draws lower than 15.4 volts from the Ethernet. • Lower than 16.8 volts-The access point draws lower than 16.8 volts from the Ethernet. • Normal-The power is high enough for the operation of the access point. • Not Applicable-The power source is not from the Ethernet.
Primary Controller	Displays the name of the primary controller for this access point.
Radio MAC	Displays the radio MAC address.
Reg. Domain Supported	Displays whether or not the regulatory domain is supported.
Serial Number	Displays the access point serial number.
Slot	Displays the slot number.

Field	Description
Tx Power Control	Displays whether the transmission power control is automatic or custom.
Tx Power Level	Displays the transmission power level.
Up Time	Displays how long the access point has been up in days, hours, minutes and seconds.
WLAN Override Names	Displays the WLAN override profile names.
WLAN Override	Displays whether WLAN Override is enabled or disabled.

Monitor > Wireless Technologies > Access Point Radios > Load

The following table describes the **Monitor > Wireless Technologies > Access Point Radios > Load** fields.

Table 14: Traffic Load Page Fields

Field	Description
AP Name	Displays the name of the access point.
Radio	Displays the protocol of the rogue access point. It is either 802.11a, 802.11b or 802.11g. Click the radio to view On-Demand Statistics for this access point.
Attached Client Count	Displays the number of clients attached (Actual and Threshold.)
Channel Utilization	Displays the 802.11a RF utilization threshold between 0 and 100 percent (Actual and Threshold).
Receive Utilization	Displays the 802.11a or 802.11b/g RF receive utilization threshold between 0 and 100 percent.
Transmit Utilization	Displays the 802.11a or 802.11b/g RF transmit utilization threshold between 0 and 100 percent.
Status	Displays the status of the client connection.

Monitor > Wireless Technologies > Access Point Radios > Dynamic Power Control

The following table describes the **Monitor > Wireless Technologies > Access Point Radios > Dynamic Power Control** fields.

Table 15: Dynamic Power Control Page Fields

Field	Description
AP Name	Displays the name of the AP.

Field	Description
Radio	Displays the protocol of the rogue access point. It is either 802.11a, 802.11b or 802.11g. Click the radio to view On-Demand Statistics for this access point.
Current Power Level	<p>Displays the operating transmit power level from the transmit power table.</p> <p>The power levels and available channels are defined by the Country Code Setting, and are regulated on a country by country basis.</p> <p>The AP transmit power level are:</p> <ul style="list-style-type: none"> • 1—Maximum power allowed per Country Code setting • 2—50% power • 3—25% power • 4—6.25 to 12.5% power • 5—0.195 to 6.25% power
Power Assignment Mode	<p>Displays the dynamic transmit power assignment. The three available modes are:</p> <ul style="list-style-type: none"> • Automatic—The transmit power is periodically updated for all Cisco 1000 Series lightweight access points that permit this operation. • On Demand—Transmit power is updated when the Assign Now button is selected. • Fixed—No dynamic transmit power assignments occur and value are set to their global default. The default is Automatic.

Monitor > Wireless Technologies > Access Point Radios > Voice TSM Table

The following table describes the **Monitor > Wireless Technologies > Access Point Radios > Voice TSM Table** fields.

Table 16: Voice Traffic Stream Metrics Table Page Fields

Field	Description
Time	Time that the statistics were gathered from the access point(s).
Client MAC	MAC address of the client. This shows a list of the clients evaluated during the most recent 90 second interval. The client could be a VoIP phone, laptop, PDA and refers to any client attached to the access point collecting measurements.
QoS	QoS values (packet latency, packet jitter, packet loss, roaming time) which can affect the WLAN are monitored. Access points and clients measure the metrics, access points collect the measurements and send them to the controller. The access points update the controller with traffic stream metric information every 90 seconds and 10 minutes of data is stored at one time.

Field	Description
% PLR (Downlink)	Percentage of packets lost on the downlink (access point to client) during the 90 second interval.
% PLR (Uplink)	Percentage of packets lost on the uplink (client to access point) during the 90 second interval.
Avg Queuing Delay (ms) (Downlink)	Average queuing delay in milliseconds for the downlink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.
Avg Queuing Delay (ms) (Uplink)	Average queuing delay in milliseconds for the uplink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.
% Packets > 40 ms Queuing Delay	Percentage of queuing delay packets greater than 40 ms.
% Packets > 20 ms Queuing Delay	Percentage of queuing delay packets greater than 20 ms.
Roaming Delay	Roaming delay in milliseconds. Roaming delay, which is measured by clients, is measured beginning when the last packet is received from the old access point and ending when the first packet is received from the new access point after a successful roam.

Monitor > Wireless Technologies > Access Point Radios > Voice TSM Reports

The following table describes the **Monitor > Wireless Technologies > Access Point Radios > Voice TSM Reports** fields.

Table 17: Voice Traffic Stream Metrics Table Reports Page Fields

Field	Description
Average Queuing Delay (ms)	Average queuing delay in milliseconds. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.
% Packet with less than 10 ms delay	Percentage of packets with less than 10 milliseconds delay.
% Packet with more than 10 < 20 ms delay	Percentage of packets with more than 10 milliseconds delay but less than 20 milliseconds delay.
% Packet with more than 20 < 40 ms delay	Percentage of packets with more than 20 milliseconds delay but less than 40 milliseconds delay.
% Packet with more than 40 ms delay	Percentage of packets with more than 40 milliseconds delay.

Field	Description
Packet Loss Ratio	Ratio of lost packets.
Total Packet Count	Number of total packets.
Roaming Count	Number of packets exchanged for roaming negotiations in this 90 seconds metrics page.
Roaming Delay	Roaming delay in milliseconds.

Monitor > Wireless Technologies > Access Point Radios > General

The following table describes the **Monitor > Wireless Technologies > Access Point Radios > General** fields for Lightweight Access Points.

Table 18: General Tab Fields for Lightweight Access Points

Field	Description
General	
AP Name	Operator defined name of the AP.
AP IP address, Ethernet MAC address, and Base Radio MAC address	IP address, Ethernet MAC address and Radio MAC address.
Country Code	The codes of the supported countries. Up to 20 countries can be supported per controller. Access points might not operate properly if they are not designed for use in your country of operation. See http://www.cisco.com/en/US/docs/wireless/wcs/4.0/configuration/guide/wcscod.html for a complete list of country codes supported per product.
Link Latency Settings	The link latency settings. The link latencies available are: <ul style="list-style-type: none"> • Current Link Latency—The current round-trip time in milliseconds of heartbeat packets from the access point to the controller and back. • Minimum Link Latency—The minimum round-trip time in milliseconds of heartbeat packets from the access point to the controller and back when link latency has been enabled or reset. • Maximum Link Latency—The maximum round-trip time in milliseconds of heartbeat packets from the access point to the controller and back when link latency has been enabled or reset.
LWAPP/CAPWAP Uptime	Displays how long the LWAPP/CAPWAP connection has been active.
LWAPP?CAPWAP Join Taken Time	Displays how long the LWAPP/CAPWAP connection has been joined.

Field	Description
Admin Status	The administration state of the access point as either enabled or disabled.
AP Mode	
Local	<p>Default mode. Data clients are serviced while configured channels are scanned for noise and rogues. The access point goes off-channel for 50 ms and listens for rogues. It cycles through each channel for the period specified under the Auto RF configuration.</p> <p>To configure Local or FlexConnect access points for the Cisco Adaptive wIPS feature, choose Local or FlexConnect and select the Enhanced wIPS Engine Enabled check box.</p>
Monitor	<p>Radio receive only mode. The access point scans all configured channels every 12 seconds. Only deauthenticated packets are sent in the air with an access point configured this way. A monitor mode access point can connect as a client to a rogue access point.</p> <p>To configure access points for Cisco Adaptive wIPS feature, select Monitor. Select the Enhanced wIPS Engine Enabled check box and choose wIPS from the Monitor Mode Optimization drop-down list.</p> <p>Before you can enable an access point to be in wIPS mode, you must disable the access point radios. If you do not disable the access point radio, an error message appears.</p> <p>Once you have re-enable the radios after you enable wIPS on the access point.</p>
Rogue Detector	The access point radio is turned off and the access point listens to wired traffic only. The controllers that operate in this mode monitor the rogue access points. The controller sends all the rogue access point and client MAC address lists to the rogue detector, and the rogue detector forwards this information to the WLC. The MAC address list is compared to what the WLC access points heard over the network. If the MAC addresses match, you can determine which rogue access points are connected on the wired network.
Sniffer	The access point captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. These packets contain information such as timestamp, signal strength, packet size, and so on. This feature can only be enabled if you run AiroPeek, which is a third-party network analyzer software that supports the decoding of data packets.
FlexConnect	<p>Enables FlexConnect for up to six access points. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost.</p> <p>FlexConnect must be selected to configure an OfficeExtend access point. In the FlexConnect mode, the configuration options display the option to enable OfficeExtend AP and allows the Least Latency Controller to join it.</p>
Bridge	This is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The bridge and its wired clients are listed as client in the Prime Infrastructure if the AP mode is set to Bridge, and the access point is bridge capable.
Spectrum Expert	This mode allows a CleanAir-enabled access point to be used extensively for interference detection on all monitored channels. All other functions such as IDS scanning and Wi-Fi are suspended.
Enhanced wIPs Engine	Enabled or Disabled, to enable the monitoring of the security attacks using Cisco Adaptive wIPS feature.

Field	Description
Operational Status	Registered or Not Registered, as determined by the controller.
Registered Controller	The controller to which the access point is registered. Click to display the registered controller details.
Primary Controller	The name of the primary controller for this access point.
Port Number	The SNMP name of the access point primary controller. The access point attempts to associate with this controller first for all network operations and in the event of a hardware reset.
AP Uptime	Displays how long the access point has been active to receive and transmit.
Map Location	Customer-definable location name for the access point. Click to look at the actual location on a map. Choose Monitor > Access Points > name > Map Location for more information.
Google Earth Location	Indicates whether a Google Earth location is assigned.
Location	The physical location where the access point is placed (or Unassigned).
Statistics Timer	This counter sets the time in seconds that the access point sends its DOT11 statistics to the controller.
PoE Status	The power over Ethernet status of the access point. The possible values are: <ul style="list-style-type: none"> • Low—The access point draws low power from the Ethernet. • Lower than 15.4 volts—The access point draws lower than 15.4 volts from the Ethernet. • Lower than 16.8 volts—The access point draws lower than 16.8 volts from the Ethernet. • Normal—The power is high enough for the operation of the access point. • Not Applicable—The power source is not from the Ethernet.
Rogue Detection	Indicates whether or not Rogue Detection is enabled. Rogue detection is disabled automatically for OfficeExtend access points because these access points are deployed in a home environment and are likely to detect a large number of rogue devices.
OfficeExtend AP	Indicates whether or not the access point is enabled as an OfficeExtend access point. The AP is enabled by default.
Encryption	Indicates whether or not encryption is enabled. Enabling or disabling encryption functionality causes the access point to reboot which then leads to a loss of connectivity for clients. DTLS data encryption is enabled automatically for OfficeExtend access points to maintain security. Encryption is only available if the access point is connected to a 5500 series controller with a Plus license.
Least Latency Join	The access point switches from a priority order search (primary, secondary, and then tertiary controller) to a search for the controller with the best latency measurement (least latency). The controller with the least latency provides the best performance.
Telnet Access	Indicates whether or not Telnet Access is enabled.

Field	Description
SSH Access	Indicates whether or not SSH is enabled. An OfficeExtend access point might be connected directly to the WAN which could allow external access if the default password is used by the access point. Hence Telnet and SSH access are disabled automatically for OfficeExtend access points.
Versions	
Software Version	The operating system release version number of the code currently running on the controller.
Boot Version	The operating system bootloader version number.
Inventory Information	
AP Type	Type of Access Point
AP Model	Access point model number.
Cisco IOS Version	The Cisco IOS Release details.
AP Certificate Type	Self Signed or Manufacture Installed certificate.
FlexConnect Mode Supported	Indicates if FlexConnect mode is supported or not.
wIPS Profile (when applicable)	
Profile Name	The wIPS profile details.
Profile Version	The zIPS profile version.
Unique Device Identifier (UDI)	
Name	Name of the Cisco AP for access points.
Description	Description of the access point.
Product ID	Orderable product identifier.
Version ID	Version of product identifier.
Serial Number	Unique product serial number.
Run Ping Test Link	Click to ping the access point. The results are displayed in a pop-up dialog box.
Alarms Link	Click to display alarms associated with this access point.
Events Link	Click to display events associated with this access point.

The following table describes the **Monitor > Wireless Technologies > Access Point Radios > General** fields for Autonomous Access Points.

Table 19: General Tab Fields for Autonomous Access Points

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

Field	Description
Version ID	Version of product identifier.
Serial Number	Unique product serial number.

Monitor > Wireless Technologies > Access Point Radios > Interfaces

The following table describes the **Monitor > Wireless Technologies > Access Point Radios > Interface** fields.

Table 20: Interfaces Tab Fields

Field	Description
Interface	
Admin Status	Indicates whether the Ethernet interface is enabled.
Operational Status	Indicates whether the Ethernet interface is operational.
Rx Unicast Packets	Indicates the number of unicast packets received.
Tx Unicast Packets	Indicates the number of unicast packets sent.
Rx Non-Unicast Packets	Indicates the number of non-unicast packets received.
Tx Non-Unicast Packets	Indicates the number of non-unicast packets sent.
Radio Interfaces	
Protocol	802.11a/n or 802.11b/g/n, XOR(2.4GHz), XOR(5GHz), or XOR (Monitor Mode).
Admin Status	Indicates whether the access point is enabled or disabled.
CleanAir Capable	Indicates whether the access point is able to use CleanAir.
CleanAir Status	Indicates the status of CleanAir.
Channel Number	Indicates the channel on which the Cisco Radio is broadcasting.
Extension Channel	Indicates the secondary channel on which Cisco radio is broadcasting.
Power Level	Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.
Channel Width	Indicates the channel bandwidth for this radio interface. The default setting is 20 MHz. This is also the minimum value. The maximum setting is the maximum channel width supported by this radio.
Antenna Name	Identifies the type of antenna.

The following table describes the Interface properties fields.

Table 21: Interface Properties Fields

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

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

Monitor > Wireless Technologies > Access Point Radios > CDP Neighbors

The following table describes the **Monitor > Wireless Technologies > Access Point Radios > CDP Neighbors** fields.

Table 22: CDP Neighbors Tab Fields

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

Monitor > Wireless Technologies > Access Point Radios > Current Associated Clients

The following table describes the **Monitor > Wireless Technologies > Access Point Radios > Current Associated Clients** fields.



Note The IP address in the Current Associated Clients will be displayed only if the current switch (where the Current Associated Clients is launched) knows the IP address of the clients.

Table 23: Current Associated Clients Tab Fields

Field	Description
Username	Username of the associated client.
IP Address	IP address of the associated client.
Client MAC Address	MAC address of the associated client.
Association Time	Date and time of the association.
UpTime	Time duration of the association.
SSID	User-defined SSID name.
SNR (dB)	Signal to Noise Ratio in dB of the associated client.
RSSI	Received Signal Strength Indicator in dBm.
Bytes Tx	Total amount of data that has passed through the Ethernet interface either way.
Bytes Rx	Total amount of data that has been received through the Ethernet interface either way.
When the access point is not associated with the controller, then the database is used to retrieve the data (rather than the controller itself). If the access point is not associated, the following fields appear.	
User Name	Username of the client.
IP Address	Local IP Address.
Client MAC Address	Client MAC Address.
Association Time	Time stamp of the client association.
Session Length	Time length of the session.

Field	Description
SSID	User-defined SSID name.
Protocol	Protocol of the associated client.

Monitor > Wireless Technologies > Access Point Radios > SSID

The following table describes the **Monitor > Wireless Technologies > Access Point Radios > SSID** fields.

Table 24: SSID Tab Fields

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

Rogue AP Alarms Page

The following table describes fields in the Rogue AP Alarms page:





Table 25: Rogue AP Alarms Page Fields




Field	Description
Severity	Indicates the severity of the alarm using icons. You can use the Severity Configuration feature to determine the level of severity for the following rogue access point alarm types: <ul style="list-style-type: none"> • Rogue detected • Rogue detected contained • Rogue detected on network
Rogue MAC Address	Indicates the MAC address of the rogue access points.
Vendor	Rogue access point vendor name or Unknown.
Classification Type	Pending, Malicious, Friendly, or Unclassified.
Radio Type	Lists all radio types applicable to this rogue access point.

Field	Description
Strongest AP RSSI	Displays the strongest AP RSSI for this rogue access point across the life of the rogue. The strongest AP RSSI over the life of the rogue displays to indicate the nearest distance that existed between the rogue access point and your building or location. The higher the RSSI, the closer the location.
No. of Rogue Clients	Indicates the number of rogue clients associated to this rogue access point. This number comes from the Prime Infrastructure database. It is updated every two hours. This number is a real-time number and it is updated each time you open the Alarm Details page for this rogue access point.
Owner	Name of person to which this alarm is assigned, or (blank).
Last Seen Time	Indicates the date and time that the rogue access point was last seen.
State	Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point. <ul style="list-style-type: none"> • Malicious rogue states include: Alert, Contained, Threat, Contained Pending, and Removed. • Friendly rogue states include: Internal, External, and Alert. • Unclassified rogue states include: Pending, Alert, Contained, and Contained Pending.
SSID	Indicates the service set identifier being broadcast by the rogue access point radio. It is blank if the SSID is not being broadcast.
Map Location	Indicates the map location for this rogue access point.
Acknowledged	Displays whether or not the alarm is acknowledged by the user. You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality.

Alarm Severity Indicator Icons

Table 26: Alarm Severity Indicator Icons

Icon	Meaning
	Critical
	Major
	Minor
	Warning

Icon	Meaning
	Information
	Unknown Note When the controller goes down, the controller inventory dashlet shown the controller status as critical. But the radio inventory dashlet, retains the last known status. In Monitor > AP page, the AP alarm status is shown as “Unknown”.
	Clear—Appears if the rogue is no longer detected by any access point. Note Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. Note Once the severity of a rogue is Clear, the alarm is deleted from the Prime Infrastructure after 30 days.

Selecting Commands for Rogue AP Alarms

Select one or more alarms by selecting their respective check boxes, choose one of the commands from the following drop-down lists.

Table 27: Command drop-down Menus for Rouge AP alarms

Field	Description
Change Status	<ul style="list-style-type: none"> • Acknowledge—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality. • Unacknowledge—Unacknowledge an already acknowledged alarm. • Clear—Clear the selected alarm(s). Indicates that the alarm is no longer detected by any access point. Once the severity is Clear, the alarm is deleted from the Prime Infrastructure after 30 days.
Change State	<ul style="list-style-type: none"> • Unclassified-Alert —Choose this command to tag the rogue access point as the lowest threat, continue monitoring the rogue access point, and to turn off Containment. Indicates the MAC address of the rogue access points. • Malicious-Alert —Choose this command to tag the rogue access point as ‘Malicious’. • Friendly-Internal —Choose this command to tag the rogue access point as internal, add it to the Known Rogue APs list, and to turn off Containment. • Friendly-External —Choose this command to tag the rogue access point as external, add it to the Known Rogue APs list, and to turn off Containment. • Refresh from Network —Refresh the network.

Field	Description
Assign	<ul style="list-style-type: none"> • Assign to me—Assign the selected alarm(s) to the current user. • Unassign—Unassign the selected alarm(s). • Select Owner— Assign the selected alarm to a particular user.
Annotation	Type the note and click Post to save and display the note or Close to close the page without saving the note.
Email Notification	Takes you to the Monitor > Monitoring Tools > Alarms and Events > Email Notification page to view and configure email notifications.

Drop-Down Menus in Rogue AP Alarm Details Page

Table 28: Menus in Rogue AP Alarm Details Page

Field	Description
Change Status	<ul style="list-style-type: none"> • Acknowledge—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality. • Unacknowledge—Unacknowledge an already acknowledged alarm. • Clear—Clear the selected alarm(s). Indicates that the alarm is no longer detected by any access point. Once the severity is Clear, the alarm is deleted from the Prime Infrastructure after 30 days. • Set State to ‘Unclassified - Alert’—Choose this command to tag the rogue access point as the lowest threat, continue monitoring the rogue access point, and to turn off Containment. • Set State to ‘Malicious - Alert’—Choose this command to tag the rogue access point as ‘Malicious’. • Set State to ‘Friendly - Internal’—Choose this command to tag the rogue access point as internal, add it to the Known Rogue APs list, and to turn off Containment. • Set State to ‘Friendly - External’—Choose this command to tag the rogue access point as external, add it to the Known Rogue APs list, and to turn off Containment. • Refresh from Network—Refresh the alarm details.
Assign	<ul style="list-style-type: none"> • Assign to me—Assign the selected alarm(s) to the current user. • Unassign—Unassign the selected alarm(s). • Select Owner— Assign an owner.
View	<ul style="list-style-type: none"> • View Detecting AP on Network • View Details by Controller

Field	Description
AP Containment	<ul style="list-style-type: none"> • 1 AP Containment—Target the rogue access point for containment by one access point. (Lowest containment level.) • 2 AP Containment—Target the rogue access point for containment by two Cisco 1000 Series lightweight access points. • 3 AP Containment—Target the rogue access point for containment by three Cisco 1000 Series lightweight access points. • 4 AP Containment—Target the rogue access point for containment by four Cisco 1000 Series lightweight access points. (Highest containment level.) <p>The higher the threat of the rogue access point, the higher the containment required.</p> <p>Attempting to contain a rogue access point might lead to legal consequences. When you select any of the AP Containment commands, a message “Containing a Rogue AP may have legal consequences. Do you want to continue?” appears. Click OK if you are sure or click Cancel if you do not wish to contain any access points.</p>

Ad hoc Rogue Alarm Details

The following table describes the fields on the Ad hoc Rogue Alarm Details page:

Table 29: Ad hoc Rogue Alarm Fields

Field	Description
General	
Rogue MAC Address	Displays the MAC address of the rogue access points.
Vendor	Displays the Rogue access point vendor name or Unknown. An Airlink rogue access point alarm is displayed as Alpha instead of Airlink.
Rogue Type	Displays the rogue type such as AP.
On Network	Displays how the rogue detection occurred.
Controller	Displays the name of the controller that detected the rogue (Yes or No).
Switch Port Trace	Displays the switch port trace that detected the rogue. The switch port trace is one of the following types: <ul style="list-style-type: none"> • Traced but not found • Traced and found • Not traced
Owner	Displays the name of the owner. It may be left blank in some cases.

Field	Description
Acknowledged	Displays whether or not the alarm is acknowledged by the user. You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the Prime Infrastructure and you can search for all acknowledged alarms using the alarm search functionality.
Classification Type	Displays the classification type of the rogue access point. The classifications are: <ul style="list-style-type: none"> • Malicious • Friendly • Unclassified.
State	Displays the state of the alarm. The possible states vary depending on the classification type of rogue access point.
SSID	Displays the Service Set Identifier being broadcast by the rogue access point radio. This field is left blank if SSID is not broadcast.
Channel Number	Displays the channel of the rogue access point.
Containment Level	Displays the containment level of the rogue access point.
Radio Type	Lists all radio types applicable to this rogue access point.
Strongest AP RSSI	Displays the strongest AP RSSI for this rogue access point across the life of the rogue. The strongest AP RSSI over the life of the rogue displays to indicate the nearest distance that existed between the rogue access point and your building or location. The higher the RSSI, the closer the location.
No. of Rogue Clients	Displays the number of rogue clients associated to this rogue access point. This is the only real-time field. It updates each time you open the Alarm Details page for this rogue access point. All other fields on the Alarm Details page are populated through polling and are updated every two hours.
First Seen Time	Displays the date and time when the rogue access point was first detected. This information is populated from the controller.
Last Seen Time	Displays the date and time when the rogue access point was last detected. This information is populated from the controller.
Modified	Displays when the alarm event was modified.
Generated By	Displays how the alarm event was generated (either NMS or from a trap). <ul style="list-style-type: none"> • 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. In this case, Generated by is displayed as NMS. • Trap—Generated by the controller. Prime Infrastructure process these traps and raises corresponding events for them. In this case, “Generated by” is Controller.
Severity	Displays the severity of the alarm.

Field	Description
Previous Severity	Displays the previous severity of the alarm: <ul style="list-style-type: none"> • Critical • Major • Minor • Clear.
Event Details	Displays the event details.
Rogue AP History	Displays the historical Rogue AP Alarm details.
Switch Port Trace Status	Displays the switch port trace status. Switch port trace status may include: <ul style="list-style-type: none"> • Traced, but not found • Traced and found, Not traced • Failed.
Rogue Clients	Displays the rogue clients for this access point including the client MAC address, the last date and time the client was heard, and the current client status.
Message	Displays the most recent message regarding this rogue access point. A message is sent for the following: <ul style="list-style-type: none"> • The rogue access point that is first detected • Any trap sent • Any changed state.
Annotations	Displays the current notes regarding this rogue access point. To add a new note, click New Annotation . Type the note and click Post to save and display the note or Cancel to close the page without saving the note.
Location Notifications	Displays the number of location notifications logged against the client.
Location	Displays the location information, if available.

Rogue AP History Details Page

The following table describes the fields in Rouge AP History Details page.

Table 30: Rogue AP History Details

Field	Description
Severity	The severity of the alarm.

Field	Description
Rogue MAC Address	MAC address of the rogue access points.
Classification Type	Malicious, Friendly, or Unclassified.
Radio Type	Lists all radio types applicable to this rogue access point.
Strongest AP RSSI	Displays the strongest AP RSSI for this rogue access point across the life of the rogue. The strongest AP RSSI over the life of the rogue displays to indicate the nearest distance that existed between the rogue access point and your building or location. The higher the RSSI, the closer the location.
No. of Rogue Clients	Indicates the number of rogue clients associated to this rogue access point.
First Seen Time	Indicates the date and time when the rogue access point was first detected. This information is populated from the controller.
Last Seen Time	Indicates the date and time when the rogue access point was last detected. This information is populated from the controller.
State	Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point.
SSID	Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
Category	Indicates the category of this alarm such as Security or Prime Infrastructure.
On Network	Indicates how the rogue detection occurred. <ul style="list-style-type: none"> • 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.
Channel Number	Indicates the channel of the ad hoc rogue.
Containment Level	Indicates the containment level of the ad hoc rogue or Unassigned.
Switch Port Trace Status	Indicates the switch port trace status. Switch port trace status might include: Traced, but not found, Traced and found, Not traced, Failed.

Rogue AP Event History Details Page

The following table describes the fields in Rouge AP Events History Details Page.

Table 31: Rogue AP Event History Details

Field	Description
Severity	The severity of the alarm.
Rogue MAC Address	MAC address of the rogue access points.

Field	Description
Vendor	Rogue access point vendor name or Unknown.
Classification Type	Malicious, Friendly, or Unclassified.
On Network	Indicates whether the rogue detection occurred. The controller detected the rogue (Yes or No).
Radio Type	Lists all radio types applicable to this rogue access point.
Date/Time	The date and time that the event was generated.
State	Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point.
SSID	Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

Ad hoc Rogue Alarms Page

The following table describes fields in the Ad hoc Rogue alarms page.

Table 32: Ad hoc Rogue Alarms Details

Field	Description
Severity	Indicates the severity of the alarm using icons. You can use the Severity Configuration feature to determine the level of severity for the following rogue access point alarm types: <ul style="list-style-type: none"> • Rogue detected • Rogue detected contained • Rogue detected on network
Rogue MAC Address	Indicates the MAC address of the rogue.
Vendor	Indicates ad hoc rogue vendor name, or Unknown.
Radio Type	Lists all radio types applicable to this rogue access point.
Strongest AP RSSI	Displays the strongest AP RSSI for this rogue across the life of the rogue. The strongest AP RSSI over the life of the rogue displays to indicate the nearest distance that existed between the rogue and your building or location. The higher the RSSI, the closer the location.
No. of Rogue Clients	Indicates the number of rogue clients associated to this rogue access point. The number of rogue clients is the only real-time field in the Alarm Details page. It updates each time you open the Alarm Details page for this rogue access point. All other fields in the Alarm Details page are populated through polling and are updated every two hours.
Owner	Indicates the owner or is left blank.
Last Seen Time	Indicates the date and time that the rogue access point was last seen.

Field	Description
State	Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
SSID	The Service Set Identifier that is being broadcast by the rogue ad hoc radio. It is blank if there is no broadcast.
Map Location	Indicates the map location for this ad hoc rogue.
Acknowledged	Displays whether or not the alarm is acknowledged by the user. You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality.

Select Commands for Ad hoc Rogue AP Alarms

Select one or more alarms by selecting their respective check boxes, choose one of the commands from the following drop-down lists.

Table 33: Commands for Ad hoc Rogue AP Alarms

Field	Description
Change Status	<ul style="list-style-type: none"> • Acknowledge—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality. • Unacknowledge—Unacknowledge an already acknowledged alarm. • Clear—Clear the selected alarm(s). Indicates that the alarm is no longer detected by any access point. Once the severity is Clear, the alarm is deleted from the Prime Infrastructure after 30 days. • Clear all of this Condition
Change State	<ul style="list-style-type: none"> • Unclassified - Alert—Choose this command to tag the rogue access point as the lowest threat, continue monitoring the rogue access point, and to turn off Containment. Indicates the MAC address of the rogue access points. • Malicious - Alert—Choose this command to tag the rogue access point as ‘Malicious’. • Friendly - Internal—Choose this command to tag the rogue access point as internal, add it to the Known Rogue APs list, and to turn off Containment. • Friendly - External—Choose this command to tag the rogue access point as external, add it to the Known Rogue APs list, and to turn off Containment. • Refresh from Network

Field	Description
Assign	<ul style="list-style-type: none"> • Assign to me—Assign the selected alarm(s) to the current user. • Unassign—Unassign the selected alarm(s). • Select Owner
Annotation	Type the note and click Post to save and display the note or Close to close the page without saving the note.
Delete	Delete the selected alarm(s).
Email Notification	Takes you to the Monitor > Alarms and Events > Email Notification page to view and configure email notifications.

View Ad hoc Rogue Alarm Details

Table 34: Ad hoc Rogue Alarm Details Page Descriptions

Field	Description
Rogue MAC Address	Indicates the MAC address of the rogue.
Vendor	Indicates ad hoc rogue vendor name, or Unknown.
On Network	Indicates how the rogue detection occurred (controller or switch port trace). The switch port tracing does not update any of the rogue attributes such as severity, state, and so on. As the rogue attributes are not updated by switch port tracing, alarms would not be triggered if a rogue is discovered to be 'on network' using switch port tracing.
Owner	Indicates the owner or is left blank.
Acknowledged	Indicates whether or not the alarm is acknowledged by the user. Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality.
State	Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
SSID	The Service Set Identifier that is being broadcast by the rogue ad hoc radio. It is blank if there is no broadcast.
Channel Number	Indicates the channel of the ad hoc rogue.
Containment Level	Indicates the containment level of the ad hoc rogue or Unassigned.
Radio Type	Lists all radio types applicable to this rogue access point.
Strongest AP RSSI	Displays the strongest AP RSSI for this rogue across the life of the rogue. The strongest AP RSSI over the life of the rogue displays to indicate the nearest distance that existed between the rogue and your building or location. The higher the RSSI, the closer the location.

Field	Description
No. of Rogue Clients	Indicates the number of rogue clients associated to this rogue access point. The number of rogue clients is the only real-time field in the Alarm Details page. It updates each time you open the Alarm Details page for this rogue access point. All other fields in the Alarm Details page are populated through polling and are updated every two hours.
Created	Indicates when the alarm event was created.
Modified	Indicates when the alarm event was modified.
Generated By	Indicates how the alarm event was generated (either NMS or from a trap).
Severity	Indicates the severity of the alarm.
Previous Severity	The previous severity of the alarm: Critical, Major, Minor, Clear. Color coded.
Last Seen Time	Indicates the date and time that the rogue access point was last seen.
Location Notification	Displays the number of location notifications logged against the client. Clicking a link displays the notifications.
Map Location	Indicates the map location for this ad hoc rogue.
Rogue Clients Details	Lists rogue clients for this access point including the client MAC address, the last date and time the client was heard, and the current client status.
Message	Indicates descriptive information about the alarm.
Help	Indicates the latest information about the alarm.
Event History	Displays the event history.
Annotations	Lists existing notes for selected alarm.f

Chokepoints Page

The following table displays the Fields in the page displaying Chokepoints.

Table 35: Chokepoints field descriptions

Field	Description
MAC Address	The MAC address of the chokepoint.
Chokepoint Name	The user-defined name of the chokepoint.
Entry/Exit Chokepoint	Indicates whether or not the chokepoint is an entry/exit chokepoint.
Static IP	The static IP address of the chokepoint.
Map Location	A link to a map showing the location of the chokepoint.

AP Detected Interferers Page

Table 36: AP Detected Interferers Page Fields

Field	Description
Interferer ID	A unique identifier for the interferer. This is a pseudo-randomly generated ID. Though it is similar to a to a MAC address, it is not a real address, such as the one used by a Bluetooth headset.
Type	<p>Indicates the category of the interferer. Click to read more about the type of device. A pop-up window appears displaying more details. The categories include the following:</p> <ul style="list-style-type: none"> • Bluetooth link—A Bluetooth link (802.11b/g/n only) • Microwave Oven—A microwave oven (802.11b/g/n only) • 802.11 FH—An 802.11 frequency-hopping device (802.11b/g/n only) • Bluetooth Discovery—A Bluetooth discovery (802.11b/g/n only) • TDD Transmitter—A time division duplex (TDD) transmitter • Jammer—A jamming device • Continuous Transmitter—A continuous transmitter • DECT-like Phone—A digital enhanced cordless communication (DECT)-compatible phone • Video Camera—A video camera • 802.15.4—An 802.15.4 device (802.11b/g/n only) • WiFi Inverted—A device using spectrally inverted Wi-Fi signals • WiFi Invalid Channel—A device using non-standard Wi-Fi channels • SuperAG—An 802.11 SuperAG device • Canopy—A Motorola Canopy device • Radar—A radar device (802.11a/n only) • XBox—A Microsoft Xbox (802.11b/g/n only) • WiMAX Mobile—A WiMAX mobile device (802.11a/n only) • WiMAX Fixed—A WiMAX fixed device (802.11a/n only) • WiFi AOCI—A WiFi device with AOCI • Unclassified
Status	<p>Indicates the status of the interfering device.</p> <ul style="list-style-type: none"> • Active—Indicates that the interferer is currently being detected by the CleanAir capable access point. • Inactive—Indicates that the interferer is no longer being detected by the CleanAir capable access point or no longer reachable by the Prime Infrastructure.

Field	Description
Severity	Displays the severity ranking of the interfering device.
Affected Band	Displays the band in which this device is interfering.
Affected Channels	Displays the affected channels.
Duty Cycle (%)	The duty cycle of interfering device in percentage.
Discovered	Displays the time at which it was discovered.
Last Updated	The last time the interference was detected.
Floor	The location where the interfering device is present.

AP Detected Interferer Details Page

Table 37: AP Detected Interferer Details Page Fields

Field	Description
Interferer Properties	Type—Displays the type of the interfering device detected by the AP.
Status	<p>The status of the interfering device. Indicates the status of the interfering device.</p> <ul style="list-style-type: none"> • Active—Indicates that the interferer is currently being detected by the CleanAir capable access point. • Inactive—Indicates that the interferer is no longer being detected by the CleanAir capable access point or no longer reachable by the Prime Infrastructure. • Severity—Displays the severity ranking of the interfering device. • Duty Cycle (%)—The duty cycle of interfering device in percentage. • Affected Band—Displays the band in which this device is interfering. • Affected Channels—Displays the affected channels. • Discovered—Displays the time at which it was discovered. • Last Updated—The last time the interference was detected.
Status	<p>Indicates the status of the interfering device.</p> <ul style="list-style-type: none"> • Active—Indicates that the interferer is currently being detected by the CleanAir capable access point. • Inactive—Indicates that the interferer is no longer being detected by the CleanAir capable access point or no longer reachable by the Prime Infrastructure.

Field	Description
Location	<ul style="list-style-type: none"> • Floor—The location where this interfering device was detected. • Last Located At—The last time where the interfering device was located. • On MSE—The mobility server engine on which this interference device was located.
Clustering Information	<ul style="list-style-type: none"> • Clustered By—Displays the IP address of the controller or the MSE that clustered the interferer information from the access point. • Detecting APs—Displays the details of the access point that has detected the interfering device. The details include: Access Point Name (Mac), Severity, and Duty Cycle(%).
Details	Displays a short description about the interfering type.

Monitor > Interferers > Interference Device ID > Location History

Choose **Monitor > Interferers > Interference Device ID**, then choose **Location History** from the Select a command drop-down list, and click **Go** to view this page.

Table 38: AP Detected Interferer Details Location History Page Fields

Field	Description
Interferer Information	Displays the basic information about the interfering device. <ul style="list-style-type: none"> • Data Collected At—The time stamp at which the data was collected. • Type—The type of the interfering device. • Severity—The severity index of the interfering device. • Duty Cycle—The duty cycle (in percentage) of the interfering device. • Affected Channels—A comma separated list of the channels affected.
Interferer Location History	Displays the location history of the interfering devices. <ul style="list-style-type: none"> • Time Stamp • Floor
Clustering Information	Clustered By—Displays the IP address of the controller or the MSE that clustered the interferer information from the access point.
Detecting APs	<ul style="list-style-type: none"> • AP Name—The access point that detected the interfering device. • Severity—The severity index of the interfering device. • Duty Cycle(%)—The duty cycle (in percentage) of the interfering device.

Field	Description
Location	<ul style="list-style-type: none"> • Location Calculated At—Displays the time stamp at which this information was generated. • Floor—Displays location information of the interfering device. • A graphical view of the location of the interfering device is displayed in a map. Click the Enlarge link to view an enlarged image.

Spectrum Experts > Summary

The Spectrum Experts > Summary page is the default page and provides a table of the Spectrum Experts added to the system. The table provides the following Spectrum Expert information:

Table 39: Spectrum Experts Summary Page Fields

Field	Description
Host Name	Displays the hostname or IP Address depending on how it was added. Click the hostname to access the Spectrum Experts Details Page.
Active Interferers	Indicates the current number of interferes being detected by the Spectrum Experts.
Affected APs	The number of access points seen by the Spectrum Expert that are potentially affected by detected interferers.
Alarms	The number of active interference traps sent by the Spectrum Expert. Click to access the Alarm page that is filtered to the active alarms for this Spectrum Expert.
Reachability Status	Indicates “Reachable” in green if the Spectrum Expert is running and sending data to the Prime Infrastructure; otherwise indicates “Unreachable” in red.
Location	When the Spectrum is a wireless client, a link is available that displays the location of the Spectrum Expert. A red box around the Spectrum Expert indicates the effective range. Click to access the nearest mapped access point.

Interferers > Summary

The Interferers > Summary page displays a list of all the Interferers detected over a 30 day interval. The table provides the following Interferers information:

Table 40: Interferes Summary Page Fields

Field	Description
Interferer ID	An identifier that is unique across different spectrum experts. This is a pseudo-randomly generated ID. Though it is similar to a MAC address, it is not a real address, which you can use to find the interfering device.

Field	Description
Category	Indicates the category of the interferer. Categories include: Bluetooth, Cordless Phones, Microwave Ovens, 802.11 FH, Generic - Fixed-Frequency, Jammers, Generic - Frequency-Hopped, Generic - Continuous.
Type	Indicates the type of Interferer. Click to access a pop-up description of the type.
Status	Indicates Active or Inactive. <ul style="list-style-type: none"> • Active—Indicates that the interferer is currently being detected by a spectrum expert. • Inactive—Indicates that the interferer is no longer detected by a spectrum expert or the spectrum expert that saw the interferer is no longer reachable by the Prime Infrastructure.
Discover Time	Indicates the time of discovery.
Affected Channels	Identifies affected channels.
Number of APs Affected	An access point is listed as Affected if the following conditions are met: <ul style="list-style-type: none"> • The access point is managed by the Prime Infrastructure. • The spectrum expert detects the access point. • The spectrum expert detects an interferer on the serving channel of the access point.
Power	Indicated in dBm.
Duty Cycle	Indicated in percentage. 100% indicates the worst value.
Severity	Indicates the severity ranking of the Interferer. 100% indicates the worst value where 0 indicates no interference.

Spectrum Experts Details Page

The Spectrum Expert Details page provides all interference details from a single Spectrum Expert. This page updates every 20 seconds providing a real-time look at what is happening on the remote Spectrum Expert and includes the following items:

Table 41: Spectrum Expert Details Fields

Field	Description
Total Interferer Count	As seen by the specific Spectrum Expert.
Active Interferers Count Chart	Displays a pie chart that groups interferes by category.
Active Interferer Count Per Channel	Displays the number of interferes grouped by category on different channels.
AP List	Provides a list of access points detected by the Spectrum Expert that are on channels that have active interferers detected by the Spectrum Expert on those channels.

Field	Description
Affected Clients List	Provides a list of clients that are currently authenticated/associated to the radio of one of the access points listed in the access point list.

Monitor > Network Devices > Unified AP

The following table describes the **Monitor > Network Devices > Unified AP > AP Name > Configuration** tab.

Table 42: General Tab Fields for Unified Access Points

Field	Description
General	
AP Name	Operator defined name of the AP.
APIP address, Ethernet MAC address, and Base Radio MAC address	IP address, Ethernet MAC address and Radio MAC address.
Country Code	The codes of the supported countries. Up to 20 countries can be supported per controller. Access points might not operate properly if they are not designed for use in your country of operation. See Cisco Wireless Control System Configuration Guide, Release 4.0 for a complete list of country codes supported per product.
Link Latency Settings	The link latency settings. The link latencies available are: <ul style="list-style-type: none"> • Current Link Latency—The current round-trip time in milliseconds of heartbeat packets from the access point to the controller and back. • Minimum Link Latency—The minimum round-trip time in milliseconds of heartbeat packets from the access point to the controller and back when link latency has been enabled or reset, • Maximum Link Latency—The maximum round-trip time in milliseconds of heartbeat packets from the access point to the controller and back when link latency has been enabled or reset.
LWAPP/CAPWAP Uptime	Displays how long the LWAPP/CAPWAP connection has been active.
LWAPP/CAPWAP Join Taken Time	Displays how long the LWAPP/CAPWAP connection has been joined.
Admin Status	The administration state of the access point as either enabled or disabled.

Field	Description
<p>AP Mode</p> <p>Note Only Local, FlexConnect, and Sniffer modes are supported on Cisco 1815I Series Unified Access Points and Cisco Aironet 1810W Series Access Points.</p>	
Local	<p>Default mode. Data clients are serviced while configured channels are scanned for noise and rogues. The access point goes off-channel for 50 ms and listens for rogues. It cycles through each channel for the period specified under the Auto RF configuration.</p> <p>To configure Local or FlexConnect access points for the Cisco Adaptive wIPS feature, choose Local or FlexConnect and select the Enhanced wIPS Engine Enabled check box.</p>
Monitor	<p>Radio receive only mode. The access point scans all configured channels every 12 seconds. Only deauthenticated packets are sent in the air with an access point configured this way. A monitor mode access point can connect as a client to a rogue access point.</p> <p>To configure access points for Cisco Adaptive wIPS feature, select Monitor. Select the Enhanced wIPS Engine Enabled check box and choose wIPS from the Monitor Mode Optimization drop-down list.</p> <p>Before you can enable an access point to be in wIPS mode, you must disable the access point radios. If you do not disable the access point radio, an error message appears.</p> <p>Once you have re-enable the radios after you enable wIPS on the access point.</p>
Rogue Detector	<p>The access point radio is turned off and the access point listens to wired traffic only. The controllers that operate in this mode monitor the rogue access points. The controller sends all the rogue access point and client MAC address lists to the rogue detector, and the rogue detector forwards this information to the WLC. The MAC address list is compared to what the WLC access points heard over the network. If the MAC addresses match, you can determine which rogue access points are connected on the wired network.</p>
Sniffer	<p>The access point captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. These packets contain information such as timestamp, signal strength, packet size, and so on. This feature can only be enabled if you run AiroPeek, which is a third-party network analyzer software that supports the decoding of data packets.</p>
FlexConnect	<p>Enables FlexConnect for up to six access points. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost.</p> <p>FlexConnect must be selected to configure an OfficeExtend access point. In the FlexConnect mode, the configuration options display the option to enable OfficeExtend AP and allows the Least Latency Controller to join it.</p>
Bridge	<p>This is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The bridge and its wired clients are listed as client in the Prime Infrastructure if the AP mode is set to Bridge, and the access point is bridge capable.</p>

Field	Description
Spectrum Expert	This mode allows a CleanAir-enabled access point to be used extensively for interference detection on all monitored channels. All other functions such as IDS scanning and Wi-Fi are suspended.
Versions	
Software Version	The operating system release version number of the code currently running on the controller.
Enhanced wIPs Engine	Enabled or Disabled, to enable the monitoring of the security attacks using Cisco Adaptive wIPS feature.
Operational Status	Registered or Not Registered, as determined by the controller.
Registered Controller	The controller to which the access point is registered. Click to display the registered controller details.
Primary Controller	The name of the primary controller for this access point.
Port Number	The SNMP name of the access point primary controller. The access point attempts to associate with this controller first for all network operations and in the event of a hardware reset.
AP Uptime	Displays how long the access point has been active to receive and transmit.
Map Location	Customer-definable location name for the access point. Click to look at the actual location on a map. Choose Monitor > Access Points > name > Map Location for more information.
Google Earth Location	Indicates whether a Google Earth location is assigned.
Location	The physical location where the access point is placed (or Unassigned).
Statistics Timer	This counter sets the time in seconds that the access point sends its DOT11 statistics to the controller.
PoE Status	The power over Ethernet status of the access point. The possible values are: <ul style="list-style-type: none"> • Low—The access point draws low power from the Ethernet. • Lower than 15.4 volts—The access point draws lower than 15.4 volts from the Ethernet. • Lower than 16.8 volts—The access point draws lower than 16.8 volts from the Ethernet. • Normal—The power is high enough for the operation of the access point. • External—The power source is from a power injector. • Not Applicable—The power source is not from the Ethernet.
Rogue Detection	Indicates whether or not Rogue Detection is enabled. Rogue detection is disabled automatically for OfficeExtend access points because these access points are deployed in a home environment and are likely to detect a large number of rogue devices.
OfficeExtend AP	Indicates whether or not the access point is enabled as an OfficeExtend access point. The AP is enabled by default.

Field	Description
Encryption	Indicates whether or not encryption is enabled. Enabling or disabling encryption functionality causes the access point to reboot which then leads to a loss of connectivity for clients. DTLS data encryption is enabled automatically for OfficeExtend access points to maintain security. Encryption is only available if the access point is connected to a 5500 series controller with a Plus license.
Least Latency Join	The access point switches from a priority order search (primary, secondary, and then tertiary controller) to a search for the controller with the best latency measurement (least latency). The controller with the least latency provides the best performance.
Telnet Access	Indicates whether or not Telnet Access is enabled.
SSH Access	Indicates whether or not SSH is enabled. An OfficeExtend access point might be connected directly to the WAN which could allow external access if the default password is used by the access point. Hence Telnet and SSH access are disabled automatically for OfficeExtend access points.
Inventory Information	
AP Type	Type of Access Point
AP Model	Access point model number.
Cisco IOS Version	The Cisco IOS Release details.
AP Certificate Type	Self Signed or Manufacture Installed certificate.
FlexConnect Mode Supported	Indicates if FlexConnect mode is supported or not.
wIPS Profile (when applicable)	
Profile Name	The wIPS profile details.
Profile Version	The zIPS profile version.
Unique Device Identifier (UDI)	
Name	Name of the Cisco AP for access points.
Description	Description of the access point.
Product ID	Orderable product identifier.
Version ID	Version of product identifier.
Serial Number	Unique product serial number.
Run Ping Test Link	Click to ping the access point. The results are displayed in a pop-up dialog box.
Alarms Link	Click to display alarms associated with this access point.
Events Link	Click to display events associated with this access point.

Field	Description
Global Username Password Configuration	
Override Global Username Password	Select the check box to enable an override for the global username/password. Enter and confirm the new access point username and password in the appropriate text boxes.
Supplicant Credentials Configuration	
Override Supplicant Credentials	Select the Override Supplicant Credentials check box to prevent this access point from inheriting the authentication username and password from the controller. The default value is unselected. The Override Supplicant Credentials option is supported in controller Release 6.0 and later. In the Username, Password, and Confirm Password text boxes, enter the unique username and password that you want to assign to this access point.
USB Settings	USB Module Type - Type of the USB Module selected.
Note This section/option is available only for the AP's that supports the USB module.	USB Operational State - Displays Detected or Not Detected to indicating if any USB is plugged in or not. USB Override - Enable the checkbox to override the AP's. For Aries OS you can override group level status and for EWLC to override profile level status. USB Module State - Enable the checkbox if you want to turn on/off the operational state. The below mentioned inventory data will be provided only if the USB module is connected to the AP: <ul style="list-style-type: none"> • USB Product ID • USB Description • USB Serial Number • USB Max Power
Controller Configuration	
Controllers Configuration	Select the check box to enable the drop-down lists for the primary, secondary, and tertiary controller names. <ul style="list-style-type: none"> • Primary, Secondary, and Tertiary Controller Name—The Primary/Secondary/Tertiary Controller names. • Primary, Secondary, and Tertiary Controller IP—The Primary/Secondary/Tertiary Controller IP is the Management IP of the controller.
Venue Configuration	<ul style="list-style-type: none"> • Venue Group • Venue Type • Secondary Venue Name • Language

Field	Description
Power Over Ethernet Settings	
Pre-Standard 802.3af Switches	Pre-Standard 802.3af Switches.
Power Injector State	When enabled, this allows you to manipulate power injector settings through Prime Infrastructure without having to go directly to the controllers. If the Enable Power Injector State is selected, power injector options appear.
Power Injector Selection	Choose installed or override from the drop-down list.
AP Transmit Config Parameters	
AP Transmit Count	Enter the AP Retransmit Count and Intervals. The AP Retransmit Count default value is 5 and the range is from 3 to 8.
AP Retransmit Interval	The AP Retransmit Interval default value is 3. The range is from 2 to 5.
BLE Beacon Configuration	Enable the BLE Beacon Configuration check box and configure the following: <ul style="list-style-type: none"> • Beacon Id • Major Field • Minor Field • Tx Power (dBm)
AP LAN Port Configuration	
Note This configuration is applicable only for Cisco Aironet 702W Series APs and Cisco 1810W Series APs.	
AP LAN Override	Select the check box to enable the LAN Override on the access point.
Port	Displays the port number.
State	Select the check box to enable the port status.
POE Status	The first LAN port contains a POE through which you can configure the POE status. Select the check box to enable the POE status.
VLAN ID	Enter the VLAN ID.
Ethernet Interfaces	The group box provides information such as interface name, slot Id, and administration status of the interface. Select the appropriate interface and specify its mode.

Field	Description
Radio Interfaces	<ul style="list-style-type: none"> • Protocol—802.11a/n or 802.11b/g/n, XOR(2.4GHz), XOR(5GHz), or XOR (Monitor Mode). • Admin Status—Indicates whether the access point is enabled or disabled. • Channel Number—Indicates the channel on which the Cisco Radio is broadcasting. • Power Level —Access Point transmit power level: 1 = Maximum power allowed per Country Code Setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power. • Antenna Diversity—Displays if antenna diversity is enabled or disabled. Antenna diversity refers to the access point sampling the radio signal from two integrated antenna ports to choose the preferred antenna. • Antenna Type—Indicate an external or internal antenna. • Sub Band • Antenna Name—Identifies the type of antenna.

Monitor > Network Devices > Wireless Controller > System Summary

The following table describes the **Monitor > Network Devices > Wireless Controller > System Summary** fields.

Table 43: Monitor System Summary Page Fields

Field	Description
General	
IP Address	Local network IP address of the controller management interface.
Name	User-defined name of the controller.
Device Type	Type of controller.
UP Time	Time in days, hours and minutes since the last reboot.
System Time	Time used by the controller.
Location	User-defined physical location of the controller.
Contact	Contact person or the owner of the controller.
Total Client Count	Displays the total number of clients currently associated with the controller excluding anchored clients.

Field	Description
Current CAPWAP Transport Mode	Control and Provisioning of Wireless Access Points (CAPWAP) protocol transport mode. Communications between controllers and access points. Choose Layer 2 or Layer 3 .
Power Supply One	If the power supply is available and operation. This is only for 4400 series controller.
Power Supply Two	If the power supply is available and operation. This is only for 4400 series controller.
Inventory	
Software Version	The operating system release.version.dot.maintenance number of the code currently running on the controller.
Emergency Image Version	An image version of the controller.
Description	Description of the inventory item.
Model No	Specifies the machine model as defined by the Vital Product Data.
Serial No	Unique serial number for this controller.
Burned-in MAC Address	The burned-in MAC address for this controller.
Number of APs Supported	The maximum number of access points supported by the controller.
Gig Ethernet/Fiber Card	Displays the presence or absence of the optional 1000BASE-T/1000BASE-SX GigE card.
Crypto Card One	<p>Displays the presence or absence of an enhanced security module which enables IPsec security and provides enhanced processing power.</p> <p>Note By default, the enhanced security module is not installed on a controller.</p> <p>Maximum number of crypto cards that can be installed on a Cisco Wireless LAN controller:</p> <ul style="list-style-type: none"> • Cisco 2000 Series—None • Cisco 4100 Series—One • Cisco 4400 Series—Two
Crypto Card Two	Displays the presence or absence of a second enhanced security module.
GIGE Port(s) Status	Up or Down. Click to review the status of the port.
Unique Device Identifier (UDI)	
Name	Product type. Chassis for controller and Cisco AP for access points.
Description	Description of controller and might include number of access points.
Product ID	Orderable product identifier.
Version ID	Version of product identifier.
Serial No	Unique product serial number.

Field	Description
Utilization	
CPU Utilization	Displays a graph of the maximum, average, and minimum CPU utilization over the specified amount of time.
Memory Utilization	Displays a graph of the maximum, average, and minimum memory utilization over the specified amount of time.
Peer Memory Utilization	Displays a graph of the maximum, average, and minimum peer memory utilization over the specified time.
Peer CPU Usage for Standby Controller	Displays a graph of the maximum, average, and minimum peer CPU utilization over the specified amount of time.

Wireless Controller System Spanning Tree Protocol

The following table describes the **Monitor > Network Devices > Wireless Controller > Spanning Tree Protocol** fields.

Table 44: Monitor Network Devices Wireless Controller Spanning Tree Protocol Fields

Field	Description
General	
Spanning Tree Specification	An indication of what version of the Spanning Tree Protocol is being run. IEEE 802.1D implementations return 'IEEE 802.1D'. If future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version, a new value is defined.
Spanning Tree Algorithm	Specifies if this controller participates in the Spanning Tree Protocol. Might be enabled or disabled by choosing the corresponding line in the drop-down list. The factory default is disabled.
Priority	The value of the writable portion of the Bridge ID, that is, the first two octets of the (8 octet long) Bridge ID. The other (last) 6 octets of the Bridge ID are given by the value of Bridge MAC Address. The value might be specified as a number between 0 and 65535. The factory default is 32768.
STP Statistics	
Topology Change Count	The total number of topology changes detected by this bridge since the management entity was last reset or initialized.
Time Since Topology Changed	Time (in days, hours, minutes, and seconds) since a topology change was detected by the bridge.
Designated Root	The bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol as executed by this node. This value is used as the Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
Root Cost	The cost of the path to the root as seen from this bridge.
Root Port	The port number of the port which offers the lowest cost path from this bridge to the root bridge.

Field	Description
Maximum Age (seconds)	The value that all bridges use for MaxAge when this bridge is acting as the root. Note The 802.1D-1990 specifies that the range for this parameter is related to the value of Stp Bridge Hello Time. The granularity of this timer is specified by 802.1D-1990 to be 1 second. Valid values are 6 through 40 seconds. The factory default is 20.
Hello Time (seconds)	The value that all bridges use for HelloTime when this bridge is acting as the root. The granularity of this timer is specified by 802.1D-1990 to be 1 second. Valid values are 1 through 10 seconds. The factory default is 2.
Forward Delay (seconds)	The value that all bridges use for ForwardDelay when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of Stp Bridge Maximum Age. The granularity of this timer is specified by 802.1D-1990 to be 1 second. An agent might return a badValue error if a set is attempted to a value which is not a whole number of seconds. Valid values are 4 through 30 seconds. The factory default is 15.
Hold Time (seconds)	The minimum time period to elapse between the transmission of Configuration BPDUs through a given LAN Port: at most one Configuration BPDU shall be transmitted in any Hold Time period.

Wireless Controller > System > CLI Sessions

The following table describes the **Monitor > Network Devices > Wireless Controller > CLI Sessions** fields.

Table 45: Monitor > Network Devices > Wireless Controller > CLI Sessions Fields

Field	Description
Session Index	Session identification.
Username	Login username.
Connection Type	Telnet or serial session.
Connection From	IP address of the client computer system.
Session Time	Elapsed active session time.
Idle Time	Elapsed inactive session time.

Wireless Controller > System > DHCP Statistics

The following table describes the **Monitor > Network Devices > Wireless Controller > DHCP Statistics** fields.

Table 46: Monitor > Network Devices > Wireless Controller > DHCP Statistics Fields

Field	Description
Server IP	Identifies the IP address of the server.
Is Proxy	Identifies whether or not this server is proxy.
Discover Packets Sent	Identifies the total number of packets sent intended to locate available servers.
Request Packets Sent	Identifies the total number of packets sent from the client requesting parameters from the server or confirming the correctness of an address.
Decline Packets	Identifies the number of packets indicating that the network address is already in use.
Inform Packets	Identifies the number of client requests to the DHCP server for local configuration parameters because the client already has an externally configured network address.
Release Packets	Identifies the number of packets that release the network address and cancel the remaining lease.
Reply Packets	Identifies the number of reply packets.
Offer Packets	Identifies the number of packets that respond to the discover packets with an offer of configuration parameters.
Ack Packets	Identifies the number of packets that acknowledge successful transmission.
Nak Packets	Identifies the number of packets that indicate that the transmission occurred with errors.
Tx Failures	Identifies the number of transfer failures that occurred.
Last Response Received	Provides a timestamp of the last response received.
Last Request Sent	Provides a timestamp of the last request sent.

Wireless Controller > WLANs

The following table describes the fields on the **Monitor > Network Devices > Wireless Controller > WLAN** page.

Table 47: Monitor > Network Devices > Wireless Controller > WLAN Fields

Field	Description
WLAN ID	Identification number of the WLAN.
Profile Name	User-defined profile name specified when initially creating the WLAN. Profile Name is the WLAN name.
SSID	User-defined SSID name.
Security Policies	Security policies enabled on the WLAN.
No of Mobility Anchors	Mobility anchors are a subset of a mobility group specified as the anchor controllers for a WLAN.

Field	Description
Admin Status	Status of the WLAN is either enabled or disabled.
No. of Clients	Current number of clients currently associated with this WLAN.

Wireless Controller > Ports

The following table describes the fields on the **Monitor > Network Devices > Wireless Controller > Physical Ports** page.

Table 48: Monitor > Network Devices > Wireless Controller > Physical Ports Fields

Field	Description
Port	Click the port number to view port details.
Physical Mode	Displays the physical mode of all ports. The choices include the following: <ul style="list-style-type: none"> • 100 Mbps Full Duplex • 100 Mbps Half Duplex • 10 Mbps Full Duplex • 10 Mbps Half Duplex
Admin Status	Displays the port state as either Enable or Disable.
STP State	Displays the STP state of the port as either Forwarding or Disabled.
Physical Status	Displays the actual port physical interface: <ul style="list-style-type: none"> • Auto Negotiate • Half Duplex 10 Mbps • Full Duplex 10 Mbps • Half Duplex 100 Mbps • Full Duplex 100 Mbps • Full Duplex 1 Gbps
Link Status	Red (down/failure), Yellow (alarm), Green (up/normal).

Wireless Controller > CDP Neighbors

The following table describes the fields on the **Monitor > Network Devices > Wireless Controller > CDP Neighbors** page.

Table 49: Monitor > Network Devices > Wireless Controller > CDP Neighbors Fields

Field	Description
Local Interface	Local Port information.
Neighbor Name	The name of each CDP neighbor.
Neighbor Address	The IP address of each CDP neighbor.
Neighbor Port	The port used by each CDP neighbor for transmitting CDP packets.
Capability	The functional capability of each CDP neighbor.
Platform	The hardware platform of each CDP neighbor device.
Duplex	Displays Full Duplex or Half Duplex.
Software Version	The software running on the CDP neighbor.

Wireless Controller > Security > RADIUS Authentication

The following table describes the fields on the **Monitor > Network Devices > Wireless Controller > Security > RADIUS Authentication** page.

Table 50: Monitor > Network Devices > Wireless Controller > Security > RADIUS Authentication Fields

Field	Description
RADIUS Authentication Servers	
Server Index	Access priority number for RADIUS servers. Up to four servers can be configured, and controller polling of the servers starts with Index 1, Index 2 second, and so forth. The index number is based on when the RADIUS server is added to the controller.
IP Address	The IP address of the RADIUS server.
Ping	Click the icon to ping the RADIUS server from the controller to verify the link.
Port	Controller port number for the interface protocols.
Admin Status	Indicates whether the server is enabled or disabled.
Authentication Server Statistics	
Msg Round Trip Time	The time interval (in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
First Requests	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.

Field	Description
Retry Requests	The number of RADIUS Authentication-Request packets retransmitted to this RADIUS authentication server.
Accept Responses	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
Reject Responses	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
Challenge Responses	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
Malformed Msgs	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or unknown types are not included as malformed access responses.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout, or retransmission.
Bad Authentication Msgs	The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.
Timeouts Requests	The number of authentication timeouts to this server. After a timeout the client might retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
Unknown Type Msgs	The number of RADIUS packets of unknown type which were received from this server on the authentication port.
Other Drops	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

Wireless Controller > Security > RADIUS Accounting

The following table describes the fields on the **Monitor > Network Devices > Wireless Controller > Security > RADIUS Accounting** page.

Table 51: Monitor > Network Devices > Wireless Controller > Security > RADIUS Accounting Fields

Field	Description
RADIUS Accounting Server	
Server Index	Access priority number for RADIUS servers. Up to four servers can be configured, and controller polling of the servers starts with Index 1, Index 2 second, and so forth. Index number is based on when the RADIUS server is added to the controller.
IP Address	The IP address of the RADIUS server.
Ping	Click the icon to ping the RADIUS Server from the controller to verify the link.

Field	Description
Port	The port of the RADIUS server.
Admin Status	Indicates whether the server is enabled or disabled.
Accounting Statistics	
Msg Round Trip Time	The time interval (in milliseconds) between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
First Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Retry Requests	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Accounting Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Msgs	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authentication Msgs	The number of RADIUS Accounting-Response packets which contained invalid authenticators received from this server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.
Timeouts Requests	The number of accounting timeouts to this server. After a timeout the client might retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
Unknown Type Msgs	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
Other Drops	The number of RADIUS packets which were received from this server on the accounting port and dropped for some other reason.

Wireless Controller > Security > Management Frame Protection

Table 1-60 describes the fields on the **Monitor > Network Devices > Wireless Controller > Security > Management Frame Protection** page.

Table 52: Monitor > Network Devices > Wireless Controller > Security Management Frame Protection Fields

Field	Description
General	

Field	Description
Management Frame Protection	Indicates if the infrastructure MFP is enabled globally for the controller.
Controller Time Source Valid	The Controller Time Source Valid field indicates whether the controller time is set locally (by manually entering the time) or through an external source (such as NTP server). If the time is set by an external source, the value of this field is “True.” If the time is set locally, the value is “False.” The time source is used for validating the timestamp on management frames between access points of different controllers within a mobility group.
WLAN Details	
WLAN ID	The WLAN ID, 1 through 17.
WLAN Name	User-defined profile name when initially creating the WLAN. Both the SSID name and profile name are user-defined. The WLAN name is same as the profile name.
MFP Protection	Management Frame Protection is either enabled or disabled.
Status	Status of the WLAN is either enabled or disabled.
AP Details	
AP Name	Operator-defined name of access point.
MFP Validation	Management Frame Protection is enabled or disabled.
Radio	802.11 a or 802.11b/g.
Operation Status	Displays the operational status: either UP or DOWN.
Protection	Full (All Frames).
Validation	Full (All Frames).

Wireless Controller > Security > Rogue AP Rules

The following table describes the fields on the **Monitor > Network Devices > Wireless Controller > Security > Rogue AP Rules** page.

Table 53: Monitor > Network Devices > Wireless Controller > Security > Rogue AP Rules Fields

Field	Description
Rule Name	Name of the rule.
Rule Type	Malicious or Friendly <ul style="list-style-type: none"> 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.

Field	Description
Match Type	Match any or match all conditions.
Enabled Rule Conditions	Indicates all enabled rule conditions including: <ul style="list-style-type: none"> • Open Authentication • Match Managed AP SSID • Match User Configured SSID • Minimum RSSI • Time Duration • Minimum Number Rogue Clients

Wireless Controller Security Guest Users

The following table describes the fields on the **Monitor > Network Devices > Wireless Controller > Security > Guest Users** page.

Table 54: Monitor > Network Devices > Wireless Controller > Security > Guest Users Fields

Field	Description
Guest User Name	Indicates the guest user login name.
Profile	Indicates the profile to which the guest user is connected.
Lifetime	Indicates the length of time that the guest user account is active. Length of time appears in days, hours, and minutes or as Never Expires.
Start Time	Indicates when the guest user account was activated.
Remaining Lifetime	Indicates the remaining time for the guest user account.
Role	Indicates the designated user role.
First Logged in at	Indicates the date and time of the user first login.
Number of logins	Indicates the total number of logins for this guest user.
Description	User-defined description of the guest user account for identification purposes.

Wireless Controller > Mobility > Mobility Stats

The following table describes the fields on the **Monitor > Network Devices > Wireless Controller > Mobility > Mobility Stats** page.

Table 55: Monitor > Network Devices > Wireless Controller > Mobility > Mobility Stats Fields

Field	Description
Global Mobility Statistics	
Rx Errors	Generic protocol packet receive errors, such as packet too short or format incorrect.
Tx Errors	Generic protocol packet transmit errors, such as packet transmission fail.
Responses Retransmitted	The Mobility protocol uses UDP and it resends requests several times if it does not receive a response. Because of network or processing delays, the responder might receive one or more retry requests after it initially responds to a request. This is a count of the response resends.
Handoff Requests Received	Total number of handoff requests received, ignored or responded to.
Handoff End Requests	Total number of handoff end requests received. These are sent by the Anchor or the Foreign to notify the other about the close of a client session.
State Transitions Disallowed	PEM (policy enforcement module) has denied a client state transition, usually resulting in the handoff being aborted.
Resource Unavailable	A necessary resource, such as a buffer, was unavailable, resulting in the handoff being aborted.
Mobility Responder Statistics	
Handoff Requests Ignored	Number of handoff requests/client announces that were ignored. The controller simply had no knowledge of that client.
Ping Pong Handoff Requests Dropped	Number of handoff requests that were denied because the handoff period was too short (3 sec).
Handoff Requests Dropped	Number of handoff requests that were dropped due to a either an incomplete knowledge of the client or a problem with the packet.
Handoff Requests Denied	Number of handoff requests that were actively denied.
Client Handoff as Local	Number of handoffs responses sent while in the local role.
Client Handoff as Foreign	Number of handoffs responses sent while in the foreign role.
Anchor Requests Received	Number of anchor requests received.
Anchor Requests Denied	Number of anchor requests denied.
Anchor Requests Granted	Number of anchor requests granted.
Anchor Transferred	Number of anchors transferred because the client has moved from a foreign controller to controller on the same subnet as the current anchor.
Mobility Initiator Statistics	
Handoff Requests Sent	Number of clients that have associated with controller and have been announced to the mobility group.

Field	Description
Handoff Replies Received	Number of handoff replies that have been received in response to the requests sent.
Handoff as Local Received	Number of handoffs in which the entire client session has been transferred.
Handoff as Foreign Received	Number of handoffs in which the client session was anchored elsewhere.
Handoff Denies Received	Number of handoffs that were denied.
Anchor Request Sent	Number of anchor requests that were sent for a three party (foreign to foreign) handoff. Handoff was received from another foreign and the new controller is requesting the anchor to move the client.
Anchor Deny Received	Number of anchor requests that were denied by the current anchor.
Anchor Grant Received	Number of anchor requests that were approved by the current anchor.
Anchor Transfer Received	Number of anchor transfers that were received by the current anchor.

Wireless Controller > Redundancy > Redundancy Summary

The following table describes the fields on the **Monitor > Network Devices > Wireless Controller > Redundancy > Redundancy Summary** page.

Table 56: Monitor > Network Devices > Wireless Controller > Redundancy > Redundancy Summary Fields

Field	Description
Local State	Displays the status.
Peer State	Displays the peer state information.
Active Controller	Displays whether the active controller is a Primary or Secondary controller.
Unit Mac	Displays the unit MAC address.
Redundancy State	Displays the redundancy state.
Mobility MAC	Mobility MAC address.
Redundancy-Management IP	Redundancy management IP address
Peer Redundancy-Management IP	Peer redundancy management IP address information.
Redundancy port IP	Redundancy port IP address.
Peer Redundancy port IP	Peer redundancy port IP address.
Peer Service Port IP	Peer service port IP address.
Average Redundancy Peer Reachability Latency (Micro seconds)	Displays the average redundancy peer reachability latency in micro seconds.

Field	Description
Average Management Gateway Reachability Latency (Micro seconds)	Displays the average latency to reach the management gateway in micro seconds.
Primary to Standby BulkSync Status	Displays status of configuration sync from primary to standby controller.
Serial Number	Displays the serial number of the unit. Note Available for controllers with version 8.7 onwards.
Fan Status	Displays status of the unit's fan. Note Available for controllers with version 8.7 onwards.

Monitor Tools

The following topics contain field descriptions for Monitor Tools:

- [Packet Capture > Capture Sessions](#)
- [Monitor > Wireless Technologies Tools](#)

Packet Capture > Capture Sessions

The following table describes the fields on **Monitor > Tools > Packet Capture > Capture Sessions**.

Table 57: Monitor > Tools > Packet Capture

Field	Description
Name	Enter a unique name for this capture session.
Packet Slice Size (bytes)	To capture the full packet, enter 0.
File Size (MB)	The total size of the capture file.
Rotate Files	If this option is enabled, the capture will be continuous until it is explicitly stopped. For NAM, the results are stored in round robin sequence by the “number of files” parameter. For example, if “rotate” is true and “number of files” is 2, two capture files will be used to store content. Packets will be saved in the first file until it is full, then the process is repeated in the next file. For ASR, the packet file is circular (the same file is used; the contents are overwritten).
For ASR devices only:	<ul style="list-style-type: none"> • Packet-to-Sample: Which n th packet to capture. For example, “3” means every third packet. • Packet-Rate: Number of packets to be captured per second. (minimum: 1; valid entries: 0-9). • Duration: How long to capture. • Packets: The total number of packets to capture.

Field	Description
Number of files	The number of files used to store content. For NAM devices only.

Monitor > Wireless Technologies Tools

The following sections contain field descriptions for pages found in **Monitor > Wireless Technologies Tools**.

Voice Audit Field Descriptions

The following topics describe the fields on the **Monitor > Tools > Wireless Voice Audit** page.

- [Voice Audit Controller Tab](#)
- [Voice Audit Rules Tab](#)
- [Voice Audit Report Tab](#)

Voice Audit Controller Tab

The following table describes the fields on **Monitor > Tools > Wireless Voice Audit > Controllers**.

Table 58: Wireless Voice Audit > Controller Tab Field Descriptions

Field	Description
Run audit on	Choose one of the following options: <ul style="list-style-type: none"> • All Controllers—No additional Controller information is necessary. • A Floor Area—From the drop-down lists, choose the applicable campus, building, floor, and controller. • A Single Controller—Choose the applicable controller from the drop-down list.

Voice Audit Rules Tab

The following table describes the fields on **Monitor > Tools > Wireless Voice Audit > Rules**.

Table 59: Wireless Voice Audit > Rules Tab Field Descriptions

Rule	Rule Details
VoWLAN SSID	Description—Checks whether or not the VoWLAN SSID exists. Rule validity—User-defined VoWLAN SSID.
CAC: 7920	Description—Checks whether or not 7920 AP CAC is enabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.
CAC: 7920 Clients	Description—Checks whether or not the 7920 Client CAC is disabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.

Rule	Rule Details
DHCP Assignment	Description—Checks whether or not DHCP assignment is disabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.
MFP Client	Description—Checks whether or not MFP Client protection is not set to Required for VoWLAN. Rule validity—User-defined VoWLAN SSID.
Platinum QoS	Description—Checks whether or not QoS is set to Platinum (Voice) for VoWLAN. Rule validity—User-defined VoWLAN SSID.
Non Platinum QoS	Description—Checks that QoS is not set to Platinum for non-VoWLAN. Rule validity—User-defined VoWLAN SSID.
WMM	Description—Checks whether or not WMM is enabled for VoWLAN. Rule data—Choose Allowed or Required from the drop-down list. Rule validity—User-defined VoWLAN SSID.
CCKM	Description—Checks whether or not CCKM is enabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.
CCKM With No AES- for 792x phones	Description—Check that AES encryption is not enabled with Cisco Centralized Key Management (CCKM) for VoWLAN. This rule is only for 792x phones. Rule validity—User-defined VoWLAN SSID.
TSM	Description—Check that Traffic Stream Metrics (TSM) is Enabled. Rule data—Select 802.11a/n TSM , 802.11b/g/n TSM , or both check boxes. Rule validity—At least one band must be selected.
DFS	Description—Checks whether the Channel Announcement and Channel Quiet Mode are Enabled for Dynamic Frequency Selection (DFS).
ACM	Description—Checks whether or not Admission Control is enabled. Rule data—Select 802.11a/n ACM , 802.11b/g/n ACM , or both check boxes. Rule validity—At least one band must be selected.
DTPC	Description—Checks whether or not Dynamic Transmit Power Control is enabled. Rule data—Select 802.11a/n DTPC , 802.11b/g/n DTPC , or both check boxes. Rule validity—At least one band must be selected.
Expedited Bandwidth	Description—Checks whether or not Expedited Bandwidth is enabled. Rule data—Select 802.11a/n Expedited Bandwidth , 802.11b/g/n Expedited Bandwidth , or both check boxes. Rule validity—At least one band must be selected.

Rule	Rule Details
Load Based CAC	<p>Description—Checks whether or not Load Based Admission Control (CAC) is enabled.</p> <p>Rule data—Select 802.11a/n Load Based CAC, 802.11b/g/n Load Based CAC (LBCAC), or both check boxes.</p> <p>Rule validity—At least one band must be selected.</p>
CAC: Max Bandwidth	<p>Description—Checks whether or not Maximum RF Bandwidth for Call Admission Control is configured properly.</p> <p>Rule data—Enter percentages in the text boxes for Maximum Allowed Bandwidth for 802.11a/n and 802.11b/g/n.</p> <p>Rule validity—Data for at least one band must be provided. The valid range is 0 to 100%.</p>
CAC: Reserved Roaming Bandwidth	<p>Description—Checks whether or not Reserved Roaming Bandwidth for Call Admission Control is configured properly.</p> <p>Rule data—Enter percentages in the text boxes for Maximum Reserved Roaming Bandwidth for 802.11a/n and 802.11b/g/n.</p> <p>Rule validity—Data for at least one band must be provided. The valid range is 0 to 100%.</p>
Pico Cell mode	<p>Description—Checks whether or not Pico Cell mode is disabled.</p> <p>Rule data—Select 802.11a/n Pico Cell mode, 802.11b/g/n Pico Cell mode, or both check boxes.</p> <p>Rule validity—At least one band must be selected.</p>
Beacon Period	<p>Description—Checks whether or not Beacon Period is configured properly.</p> <p>Rule data—Enter the time (ms) in the text boxes for Beacon Period for 11a/n and 11b/g/n.</p> <p>Rule validity—Data for at least one band must be provided. The valid range is 20 to 1000. Enter 0 or keep it empty if a band should not be checked.</p>
Short Preamble	<p>Description—Checks whether or not Short Preamble is enabled for 11b/g.</p>
Fragmentation Threshold	<p>Description—Checks whether or not Fragmentation Threshold is configured properly.</p> <p>Rule data—Enter the threshold amount (bytes) in the text boxes for Fragmentation Threshold for 11a/n and 11b/g/n.</p> <p>Rule validity—Data for at least one band must be provided. The valid range is 256 to 2346. Enter 0 or keep it empty if a band should not be checked.</p>
Data Rate	<p>Description—Checks whether or not Data Rates are configured properly.</p> <p>Data Rate configuration for 11b/g—Select Disabled, Supported, or Mandatory for each Mbps category.</p> <p>Data Rate configuration for 11a—Select Disabled, Supported, or Mandatory for each Mbps category.</p>
Aggressive Load Balancing	<p>Description—Checks whether or not Aggressive Load Balancing is disable.</p>
QoS Profile	<p>Description—Checks that QoS Profiles are not altered from default values.</p>

Rule	Rule Details
EAP Request Timeout	Description—Checks whether or not EAP Request Timeout is configured properly. Rule data—Enter the time limit (sec) for the EAP Request Timeout. Rule validity—Data cannot be left blank or as zero. The valid range is 1 to 120.
ARP Unicast	Description—Checks whether or not ARP Unicast is disabled.

Voice Audit Report Tab

The following table describes the fields on **Monitor > Tools > Wireless Voice Audit > Report**.

Table 60: Wireless Voice Audit > Report Tab Field Descriptions

Field	Description
Audit Status	Indicates whether or not the audit is complete.
Start Time and End Time	Indicates the time at which the voice audit starts and ends.
# Total Devices	Indicates the number of devices involved in the voice audit.
# Completed Devices	Indicates the number of devices the tool attempted to audit. Note If a controller is unreachable, the audit skips it. The Voice Audit does not complete any rule checks for that controller.
# Rules	Indicates the number of rules selected for the voice audit.
Report Results	
IP Address	Indicates the IP address for the controller involved in the voice audit.
Rule	Indicates the rule that was applied for this controller.
Result	Indicates the result (Skipped, Violation, Unreachable) of the applied rule. Note If there is no mismatch between the current configuration and a rule value, no results are displayed for that rule.
Details	Defines an explanation for the rule results. Note If the applied rule results in a Violation, the Details link provides additional information including Name, the Device Value, and the Rule Value. Hover your mouse cursor over the link to view the additional details.
Time	Provides a timestamp for the voice audit.

Voice Diagnostic Field Descriptions

The following topics describe the fields on the **Monitor > Tools > Wireless Voice Diagnostic** page.

- [Voice Diagnostic Test List Page](#)

- [Voice Diagnostic Test Report Page](#)

Voice Diagnostic Test List Page

The following table describes the fields on **Monitor > Tools > Wireless Voice Diagnostic**.

Table 61: Voice Diagnostic Test List Page Field Descriptions

Field	Description
Test Name	Name of the test.
Duration of Test (Minutes)	The duration for which the test is performed. The duration can be either 10, 20, 30, 40, 50, or 60 minutes. The default selection is 10 minutes.
First Client	Displays the First Client details such as the Client MAC address and all the controllers provisioned for the client and if the controllers are not reachable then the failed provisioned controllers are also listed.
Second Client	Displays the Second Client details (if any) such as the Client MAC address and all the controllers provisioned for the client and if the controllers are not reachable then the failed provisioned controllers are also listed.
Start Time	The time when the test was started.
Remaining Time	The time remaining for the test.
State	The state of the test. It can be one of the four states, Running, Completed, Stopped or Aborted.
Problem	The status of the test. Red indicates a problem was discovered in the test. Green indicates the voice diagnostic test that no problems were discovered during the call.

Voice Diagnostic Test Report Page

The following table describes the tabs on **Monitor > Tools > Wireless Voice Diagnostic Test Report**.

Table 62: Voice Diagnostic Test Report Page Tab Descriptions

Tab	Description
Summary This tab is divided into three areas where top area displays the test and client details, the middle area displays the problems, and the bottom area displays the corresponding log messages.	

Tab	Description
Test and Client Details	<p>The test status displays the test details like the Test Name, First Client MAC address, Second Client MAC address, device type, test status, start time, remaining time and the duration of the test. Restart if the test was stopped or completed the test. A stop button is provided to Stop the running test. The Refresh Status Tab and Refresh Client Tab buttons is used to refresh the status and client details. The client details such as the client user name, IP address, MAC address, Vendor, CCX Version, 802.11 state, protocol, SSID, profile-name, and AP details are displayed. You can click the Client MAC address for more client details.</p>
Problems	<p>The Problems pane appears below the test and client status details pane, This pane displays all the problems regarding the current diagnosis. This pane is updated every 5 seconds independently. There is no need to refresh the whole page. You can sort the information in this pane by clicking on any of the pane columns. A pop-up dialog box appears with the Problem detailed description and Suggested action when you click any row of the Problems pane.</p> <p>Note In some cases of inter controller roaming failure, the MAC address in the From AP information is incorrect and may appear as “00:00:00:00:00:00”.</p>
Logs	<p>The Logs pane appears below the Problems pane. This pane displays all the messages exchanged between the controller and the WCS during this diagnosis. You can sort the information in this pane by clicking on any of the pane columns. This pane is updated every 5 sec independently without refreshing the whole page.</p>
<p>Charts</p> <p>This tab displays the charts for each client's uplink and downlink traffic. The charts are updated every 10 secs.</p>	
Client Uplink and DownLink TSM Chart with Roaming	<p>The Client Uplink Traffic Stream Metric (TSM) chart shows the clients which support CCX V4 and above. The TSM data is plotted for every 10 sec. The TSM Chart displays the metrics for a set of series, that can be enabled or disabled using the Select Series button in the chart.</p>
Client Uplink and DownLink QoS Chart	<p>For each interval, QoS will be calculated and shown on the chart. represents the Client Uplink QoS chart. This pie chart provides the total QoS Chart counts and its distribution in three categories. These categories generally indicate the quality of a voice call.</p>
Average Uplink and Downlink AC Queue	<p>The AC Queue displays the type of packets and the number of packets for a series. You can enable or disable the series using the Select Series button.</p>

Tab	Description
<p>Roam History</p> <p>This tab shows the roaming history information in the Roaming Table. This Roaming table displays both the successful and the failed roaming history. The roaming table provides the following information:</p> <ul style="list-style-type: none"> • Time at which the roaming of the client happened • The name of the AP from which the client moved • The type of Radio from which the client moved • The IP address of the controller from which the client moved • The name of the AP to which the client moved • The IP address of the controller to which the client moved • The type of radio to which the client moved • The roaming result, whether it was successful or a failure • If it was a failure it also provides the reason to the failure 	
<p>Events</p> <p>The Event tab shows the event history related to client and AP during a voice call in a list. It will show last 10 events. There is two Event tables available, Client Events and AP Events. Client Specific events during the voice call is shown in the Client Events table and AP Specific events in shown in the AP Event table.</p>	

Monitor > WiFi TDOA Receivers

The following table describes the fields on **Monitor > TDOA Receivers** page.

Table 63: Monitor > TDOA Receivers Fields

Fields	Description
MAC Address	MAC address of the WiFi TDOA receiver.
WiFi TDOA Receiver Name	TDOA receiver name.
Static IP	Static IP address of the WiFi TDOA receiver.
Oper Status	Shows whether the status is Up or Down.

Fields	Description
Map Location	Click the Map Location link to view the floor map for the WiFi TDOA receiver.

Media Streams

The following topics contain field description for Media Streams:

- [Monitor > Media Streams](#)
- [Monitor > Media Streams > Media Stream Details](#)

Monitor > Media Streams

The following table describes the fields on **Monitor > Media Streams** page.

Table 64: Monitor > Media Streams Fields

Field	Description
Stream Name	Media stream name. Click the Stream Name to view the media stream details.
Start IP	Starting IP address of the media stream for which the multicast direct feature is enabled.
End IP	Ending IP address of the media stream for which the multicast direct feature is enabled.
State	Operational state for the media stream.
Max Bandwidth	Maximum bandwidth that is assigned to the media stream.
Priority	Priority bit set in the media stream. The priority can be any number from 1 to 8. A lower value indicates a higher priority. For example, a priority of 1 is highest and a value of 8 is the lowest.
Violation	Action to be performed in case of a violation. The possible values are as follows: <ul style="list-style-type: none"> • Drop—Indicates that a stream is dropped on periodic reevaluation. • Best Effort—Indicates that a stream is demoted to best-effort class on periodic reevaluations.
Policy	Media stream policy. The possible values are Admit or Deny.
Controllers	Number of controllers that use the specified media stream.
Clients	Number of clients that use the specified media stream.

Monitor > Media Streams > Media Stream Details

The following table describes the fields on **Monitor > Media Streams > Media Stream Details** page.

Table 65: Monitor > Media Streams > Media Stream Details Fields

Fields	Description
Media Stream Details	<p>Displays the following media stream configuration information:</p> <ul style="list-style-type: none"> • Media Stream Name • Multicast Destination Start IP • Multicast Destination End IP • Maximum Expected Bandwidth (1 to 35000 kbps) • Operational Status • Average Packet Size(100-1500 bytes) • RRC Periodic • RRC Priority(1-8) • Traffic Profile Violation • Policy
Statistics	Displays the number of controllers and number of clients that use the selected media stream. Click the controller count to access the list of controllers that use the selected media stream.
Error	Displays the error and corresponding floor map for that AP.
Client Counts	Displays the number of clients for each period. The client information is presented in a time-based graph. For graphs that are time-based, there is a link bar at the top of the graph page that displays 6h, 1d, 1w, 2w, 4w, 3m, 6m, 1y, and Custom. When selected, the data for that time frame is retrieved and the corresponding graph is displayed.
Failed Client Counts	Displays the number of clients that failed for each period.

For more information see the section *Add, Position, and Delete WiFi TDOA Receivers* in the latest [Cisco Prime Infrastructure User Guide](#).

Monitor > Radio Resource Management

The following table describes the fields on **Monitor > Radio Resource Management** page.

Table 66: Monitor > Radio Resource Management Fields

Fields	Description
RRM Statistics	<p>Displays the following network-wide RRM performance statistics and predicts reasons for channel changes based on grouping the events together:</p> <ul style="list-style-type: none"> • Number of RF Groups—Shows the total number of RF groups currently managed by Prime Infrastructure. • APs at maximum power (a/n/ac)—Shows what percentage of time, the access points with 802.11 a/n radios were at maximum power and gives the location of those access points. • APs at maximum power (b/g/n)—Shows what percentage of time, the access points with 802.11 a/n radios were at maximum power and gives the location of those access points. • Total Configuration Mismatches—Shows the total number of configuration mismatches detected over a 24-hour period. • Total Channel Changes—Shows the sum total of channel changes across 802.11 a/b/g/n radios, irrespective of whether the channel was updated or revised. The count is split over a 24-hour and 7-day period. If you click the percentages link or the link under the 24-hour column, a page with details for that access point only appears. • CleanAir Initiated Channel Changes—Shows the CleanAir initiated channel change information. • Total Coverage Hole Events—Shows the total number of coverage hole events over a 24-hour and 7-day period.
Channel Change Reason	<p>Displays reason why the channels changed for all 802.11 a/b/g/n radios and contains the following parameters:</p> <ul style="list-style-type: none"> • Signal—The channel changed because it improved the channel quality for some other neighbor radio(s). Improving the channel quality for some other neighbor radio (s) improved the channel plan of the system as evaluated by the algorithm. • Wifi Interference • Load • Radar • Noise • Persistent Non-Wifi interference • Major Air Quality Event • Other
Channel Change Causes	<p>Displays a graphical bar chart for 802.11 a/n radios. The chart is factored based on the reason for channel change. The chart is divided into two parts, each depicting the percentage of weighted reasons causing the event to occur over a 24-hour and 7-day period. Each event for channel change can be caused by multiple reasons, and the weight is equally divided across these reasons. The net reason code is factored and equated to one irrespective of the number of reasons for the event to occur.</p>

Fields	Description
Channel Change - APs with channel changes	Displays channel change information. Each event for channel change includes the MAC address of the lightweight access point. For each reason code, you are given the most channel changes that occurred for the 802.11a/n access point based on the weighted reason for channel events. This count is split over a 24-hour and 7-day period.
Configuration Mismatch - RF Groups with Configuration Mismatches	Displays the configuration mismatch over a 24-hour period by RF group details.
Coverage Hole - APs reporting coverage holes	Displays the top five access points filtered by IF Type 11 a/n, which triggered a coverage hole event (threshold based).
APs at Maximum Power	Displays a graphical progressive chart of the total percentage of 802.11a/n lightweight access points which are operating at maximum power to accommodate coverage holes events. The count is split over a 24-hour and 7-day period.

Alarms and Events

The following topics contain field description for Alarms and Events:

- [Monitoring Tools > Alarms and Events Alarms Tab](#)
- [Monitor > Monitoring Tools > Clients and Users](#)

Monitoring Tools > Alarms and Events Alarms Tab

The following table describes the fields on **Monitor > Monitoring Tools > Alarms and Events > Alarms** tab.

Table 67: Monitor > Monitoring Tools > Alarms and Events > Alarms Tab Fields

Fields	Description
Severity	Severity of the alarm which can be: <ul style="list-style-type: none"> • Critical • Major • Minor • Warning • Informational
Message	Messages about the alarm.
Status	Status of the alarm.
Failure Source	Indicates the source of the event (including name and/or MAC address).

Fields	Description
Timestamp	Date and time that the alarm occurred.
Owner	Name of the person to whom this alarm is assigned, if one was entered.
Category	Category assigned to the alarm such as rogue AP, controller, switch, and security.
Condition	Condition that caused the alarm.
Alarm Browser Toolbar	
Change Status	<p>Changes the alarm status to one of the following:</p> <ul style="list-style-type: none"> • Acknowledge—You can acknowledge the alarm. By default, acknowledged alarms are not displayed in the Alarm Browser page. Acknowledged alarms remain in Prime Infrastructure and you can search for all acknowledged alarms using the alarm search functionality. • Unacknowledge—You can choose to Unacknowledge an already acknowledged alarm. • Clear—Clear the selected alarm(s). The alarm is removed from the Alarm Browser. Cleared alarms remain in the Prime Infrastructure and you can search for all cleared alarms using the alarm search functionality.
Assign	<p>For the selected alarm, you can do the following:</p> <ul style="list-style-type: none"> • Assign to me—To assign the alarm to yourself. • Select Owner—To assigns the alarm to a specified user. • Unassign—To remove the specified owner from the alarm.
Annotation	Enter an annotation for the selected alarm, then click Post . The annotation you entered appears when you view the alarm details.
Delete	Delete the selected alarm(s). Indicates that the alarm is no longer detected by any device.
Email Notification	Set up email notifications for alarms based on the alarm category and severity level. Prime Infrastructure sends email notifications when alarms for the categories you specified occur.

Fields	Description
Show	<p>Show drop-down list has the following options:</p> <ul style="list-style-type: none"> • Quick Filter—Enter text in any of the boxes to display alarms that contain the text you enter. • Advanced Filter—This filter provides an advanced alarm search capability. It provides ability to search on specific fields with various conditions like contains, does not contain, starts with, ends with and so on. • All—Displays all alarms. • Manage Preset Filter—Displays any previously saved filters and allows you to edit and delete previously saved filters. • Assigned to Me—Displays all alarms assigned to you. • Unassigned Alarms—Displays all unassigned alarms. • Alarms in Last 5 Minutes • Alarms in Last 15 Minutes • Alarms in Last 30 Minutes • Alarms in the last hour • Alarms in the last 8 hours • Alarms in the last 24 hours • Alarms in last 7 days • All wired alarms—Displays all alarms for wired devices. • All wireless alarms—Displays all alarms for wireless devices.

Monitor > Monitoring Tools > Alarms and Events > Events

The following table describes the fields on **Monitor > Monitoring Tools > Alarms and Events > Events** tab.

Table 68: Monitor > Monitoring Tools > Alarms and Events > Events Tab Fields

Field	Description
Description	Describes the event details.
Time	Indicates the date and time when the event was generated.
Severity	Indicates the event severities. The possible options are: Critical, Major, Minor, Warning, Cleared, or Information.
Failure Source	Indicates the source of the event (including name and/or MAC address).
Category	Type of event such as Rogue AP, Security, or AP.

Field	Description
Mesh Links	Mesh link information.
Clients	Clients information.
Context Aware Notifications	Displays context aware notifications.
Coverage Hole Event	
Access Point Name	Access point name.
Failed Clients	Number of clients that failed due to the coverage hole.
Total Clients	Total number of clients affected by the coverage hole.
Radio Type	The radio type (802.11b/g or 802.11a) of the applicable access point.
Coverage Threshold	Displays coverage threshold information.
Rogue AP Events	
Vendor	Rogue access point vendor name or Unknown.
Classification Type	Indicates the type of rogue access point including Malicious, Friendly, or Unclassified.
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.
Radio Type	Lists all radio types applicable to this rogue access point.
State	Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
SSID	Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
Adhoc Rogue Events	
Vendor	Rogue access point vendor name or Unknown.
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.
Radio Type	Lists all radio types applicable to this rogue access point.
State	Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.

Field	Description
SSID	Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
Interference	
Detected By	IP address of the device that detected the interference.
ID	ID of the device that detected the interference.
Pre Coverage Hole	
Client MAC Address	MAC address of the client affected by the Pre Coverage Hole.
AP MAC Address	MAC address of the applicable access point.
Radio Type	The radio type (802.11b/g or 802.11a) of the applicable access point.
Power Level	Access Point transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, 5 = 0.195 to 6.25% power).
Client Type	Client type can be laptop(0), pc(1), pda(2), dot11mobilephone(3), dualmodephone(4), wgb(5), scanner(6), tabletpc(7), printer(8), projector(9), videoconfsystem(10), camera(11), gamingsystem(12), dot11deskphone(13), cashregister(14), radiotag(15), rfidsensor(16), server(17).
WLAN Coverage Hole Status	Displays coverage hole status.

Monitor > Monitoring Tools > Clients and Users


The following table describes the preset filters that are available in the Clients and Users page and the results when you choose these filters from the Show drop-down list.

Table 69: Client List Filters

Filter	Results
All	All clients including inactive clients. Note Generally, “All” filter means no filters. All SSID returns all clients connected to all controllers such as PMIP, WGB, or wired guest clients.
2.4 GHz Clients	All clients using 2.4 GHz radio band.
5 GHz Clients	All clients using 5.0 GHz radio band.
All Lightweight Clients	All clients connected to lightweight APs.
All Autonomous Clients	All clients connected to autonomous APs.
All Wired Clients	All clients directly connected to a switch managed by Prime Infrastructure.
Associated Clients	All clients connected to the network regardless of whether they are authenticated or not.

Filter	Results
Clients detected by MSE	All clients detected by MSE including wired and wireless clients.
Clients detected in last 24 hours	All clients detected in the last 24 hours.
Clients Known by ISE	Shows all the clients that are authenticated by ISE.
Clients with Problems	Clients that are associated, but have not yet completed policy.
Excluded Clients	All lightweight wireless clients excluded by the controller.
FlexConnect Locally Authenticated	Clients connected to FlexConnect APs and authenticated locally.
New Clients detected in last 24 hours	New Clients detected in the last 24 hours.
On Network Clients	Clients that have gone through authentication/authorization and are able to send and receive data. This means the clients that have completed all set policies and are on the network. The clients are not Identity clients and are always appear as 'On Network'.
WGB Clients	All WGB clients. Note If an access point is bridge capable, and the AP mode is set to Bridge, you can view clients identified as WGBs. WGB clients bridge wireless to wired. Any Cisco IOS access point can take on the role of a WGB, acting as a wireless client with a wired client connected to it. The information about this WGB is propagated to the controller and appears as a client in both Prime Infrastructure and WLC.

The following table shows the columns that are available in the Clients and Users table:

Tab	Description
Client Attributes	<p>When you select a client from the Clients and Users list, the client attributes appear in the Clients and Users list. Clients are identified using the MAC address.</p> <p>The details that appear in the Client Attributes group box are from the device, whereas the details that appear in the Clients and Users list are from the database. Therefore, there can be some discrepancy between the details that appear in the Clients and Users list and the Client Attributes group box.</p> <p>For wired clients, the information comes from the switch. Also, the data that appears in the details page is live data collected on demand from the controller/switch/ISE.</p> <p>These details include the following client details:</p> <ul style="list-style-type: none"> • General—Lists the generation information such as User Name, MAC address, and so on. <p></p> <ul style="list-style-type: none"> • Session—Lists the client session information. <p>Security (wireless and Identity wired clients only)—Lists Security policy, authentication information, and EAP type.</p> <p>The identity clients are the clients whose authentication types are 802.1x, MAC Auth Bypass or Web Auth. For non-identity clients, the authentication type is N/A.</p> <p>The data that appears in the Client Attributes group box differs depending on the type of client: identity and non-identity clients. For identity clients, you can see the security information such as Authentication status, Audit Session ID, and so on.</p> <ul style="list-style-type: none"> • Statistics (wireless only) • Traffic—Shows the client traffic information. <p>For wireless clients, client traffic information comes from controller. For wired clients, the client traffic information comes from the ISE, therefore you must enable accounting information and other necessary functions on the switches.</p> <p>Click Refresh from Device to see client statistics.</p>
Client Attributes Summary	Click any of the client, access point and switch topology icons, to view the respective Device 360° view.

Tab	Description
Client IPv6 Addresses	<p>When you select an IPv6 client from the Clients and Users list, the client IPv6 address details appear. These details come from the controller directly.</p> <p>For the wired clients that have IPv6 addresses, Prime Infrastructure discovers the client addresses from the IPv6 neighbors table on the switch.</p> <p>These details include the following information:</p> <ul style="list-style-type: none"> • IP Address—Client IPv6 address. • Scope • Address Type • Discovery Time
Client Statistics	<p>The Client Statistics includes the following information for the selected client:</p> <ul style="list-style-type: none"> • Client AP Association History. • RSSI (dBm)—RSSI (Received Signal Strength Indicator) as detected by the access point with which the client is associated. • SNR — SNR (signal-to-noise ratio of the client RF session) as detected by the access point with which the client is associated. <p>The default values of RSSI and SNR (-128 and 0 respectively) are denoted as N/A (Not Applicable).</p> <ul style="list-style-type: none"> • Bytes Sent and Received (Kbps)—Bytes sent and received with the associated access point. • Packets Sent and Received (per second)—Packets sent and received with the associated access point. • Data rate over time. <p>Hover your mouse cursor over points on the graph for additional statistical information. This information is presented in interactive graphs. See the Interactive Graphs section in Related Topics for more information.</p>

Tab	Description
Client Association History	

Tab	Description
	<p>The Association History dashlet displays information regarding the last ten association times for the selected client. This information can help in troubleshooting the client. This section remains blank when the clients are not successfully authenticated.</p> <p>For a selected period (for example, 6h, 1d and 1w etc.), the Client Association History chart may not be displayed properly due to the following reasons:</p> <ul style="list-style-type: none"> • If the number of access points (plotted in Y-axis) to which the client was associated while roaming, exceeds five. • If the number of association and disassociation points (plotted in X-axis) exceeds 120. • Client Association History (for wireless clients) includes the following information: <ul style="list-style-type: none"> • Date and time of association • Duration of association • Username • IP address • Access point name (for wireless clients only) • Access point and controller name (for wired clients only) • Map Location (for wired clients only) • Controller name (for wireless clients only) • SSID • Protocol • Amount of traffic (MB) • Hostname • Roam reason (such as <i>No longer seen from controller</i> or <i>New association detected</i>) <p>Click the settings icon to add, remove or reorder columns in the Current Associated Clients table. See the Configure the List of Access Points Display section in Related Topics for adding new parameters than can be added through settings icon.</p> <p>Prime Infrastructure reports the reassociations of an access point as separate sessions. This is because of the following reasons:</p> <ul style="list-style-type: none"> • Session timeout on WLAN • Low power level because of interference in setup • Client is roaming • Client driver implementation

Tab	Description
	Data decrypt errors on the client driver
Client Event Information	<p>The Client Event dashlet of the Client Details page displays all events for this client including the event type as well as the date and time of the event.</p> <p>Click an event type to view its details. See the Monitoring Failure Objects section in Related Topics for more information.</p>
Client Location Information	<p>The following location parameters appear (if available) for the selected client:</p> <ul style="list-style-type: none"> • Map Area—The map area in which the client was last located. • ELIN—The Emergency Location Identification Number. This is applicable only to the wired clients that are located by MSE. • Civic Address—The fields on the Civic Address tab are populated if a civic address is imported for a client. This is applicable only to the wired clients that are located by MSE. • Advanced—Detailed information about the client. The fields on this tab are populated if a civic address is imported for a client. <p>For more information on importing Civic information for the client, see the Configure a Switch Location section in Related Topics.</p>
Wired Location History	<p>You can view the Location History for wired clients.</p> <p>The wired clients must be located by MSE and the history for wired clients must be enabled on the MSE.</p> <p>The following Location History information is displayed for a client:</p> <ul style="list-style-type: none"> • Timestamp • State • Port Type • Slot • Module • Port • User Name • IP Address • Switch IP • Server Name • Map Location • Civic Location

Tab	Description
Wireless Location History	<p>You can view the Location History for wireless clients.</p> <p>The wireless clients must be located by MSE and the history for wired clients must be enabled on the MSE.</p>
Client CCXv5 Information	<p>CCXv5 clients are client devices that support Cisco-compatible Extensions Version 5 (CCXv5). Reports specific to CCXv5 clients provide client details that enhance client diagnostics and troubleshooting.</p> <p>The CCXv5 manufacturing information is displayed for CCXv5 clients only.</p> <ul style="list-style-type: none"> • Organizational Unique Identifier—The IEEE assigned organizational unique identifier, for example, the first 3 bytes of the MAC address of the wireless network connected device. • ID—The manufacturer identifier of the wireless network adapter. • Model—Model of the wireless network adapter. • Serial Number—Serial number of the wireless network adapter. • Radio—Radio type of the client. • MAC Address—MAC address assigned to the client. • Antenna Type—Type of antenna connected to the wireless network adapter. • Antenna Gain—The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means $4 \times 0.5 = 2$ dBm of gain. • Automated Troubleshooting Report—If the automated test runs, this report displays the location of automated troubleshooting log AUTO_TS_LOG<ClientMac>.txt. If no automated test runs, Not Exists appears. n • Power (dBm).

Tab	Description
Client CCXv5 Information	<p>Radio Receiver Sensitivity—Displays receiver sensitivity of the wireless network adapter including the following:</p> <ul style="list-style-type: none"> • Radio • Data Rate • Minimum and Maximum RSSI <p>CCXV5 Capability Information—Displays the Capability Information parameters for CCXv5 clients only.</p> <ul style="list-style-type: none"> • Radio • Client Status—Success or failure. • Service Capability—Service capabilities such as voice, streaming (uni-directional) video, interactive (bi-directional) video. <p>Radio Channels—Identifies the channels for each applicable radio.</p> <p>Transmit Data Rates—Identifies the transmission data rates (Mbps) for each radio.</p> <p>Transmit Power Values—Identifies the transmission power values including:</p> <ul style="list-style-type: none"> • Power mode • Radio

The following table describes the fields on Network Client Radio Measurement results:

Table 70: Network Client Radio Measurement results

Measurement Parameter	Description
Channel	The channel number for this measurement.
BSSID	6-byte BSSID of the station that sent the beacon or probe response.
PHY	Physical Medium Type (FH, DSS, OFDM, high rate DSS or ERP).
Received Signal Power	The strength of the beacon or probe response frame in dBm.
Parent TSF	The lower 4 bytes of serving access point TSF value.
Target TSF	The 8-byte TSF value contained in the beacon or probe response.
Beacon Interval	The 2-byte beacon interval in the received beacon or probe response.
Capability information	As found in the beacon or probe response.
Number of frames	Number of frames received from the transmit address.
Received Signal Power	The signal strength of 802.11 frames in dBm.

Measurement Parameter	Description
CCA busy fraction	The fractional duration over which CCA indicated the channel was busy during the measurement duration defined as ceiling (255 times the duration the CCA indicated channel was busy divided by measurement duration).
RPI	RPI density in each of the eight power ranges.