

Troubleshoot Wireless Issues with Catalyst Center

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Collect Data from Catalyst Center](#)

[Issue with Catalyst 9800 Series Wireless Controller](#)

[Reviewing Controller Health with Device 360](#)

[Issue with an Access Point](#)

[Intelligent Captures for Access Point](#)

[AP Statistics Capture](#)

[OTA Sniffer Capture](#)

[Anomaly Detection](#)

[Issue with Wireless Client Connectivity](#)

[Intelligent Captures for Wireless Clients](#)

[Onboarding Packet Capture](#)

[Full Packet Capture](#)

[Isolate Network Service Issues \(AAA, DHCP, DNS\)](#)

[Network Reasoner](#)

[Technical References](#)

Introduction

This document describes troubleshooting Catalyst 9800 Wireless LAN Controller (WLC), AP, and client connectivity issues using Cisco Catalyst Center.

Prerequisites

- The Wireless LAN Controller must be added to Catalyst Center and show a **Managed** state in inventory.
- **Telemetry status** on the WLC must show **Up**.

Requirements

Cisco recommends that you have the knowledge of these topics:

- Command Line Interface (CLI) or Graphic User Interface (GUI) access to Wireless LAN Controller
- Command Line Interface (CLI) or Graphic User Interface (GUI) access to Catalyst Center

Components Used

The information in this document is based on these software and hardware versions:

- 9800 Model WLC
- Cisco IOS XE 17.15.5 version
- Catalyst Center 2.3.7 version

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Collect Data from Catalyst Center

Once a Catalyst 9800 Series WLC is added to Catalyst Center for Assurance, the platform pulls data through multiple collection methods — SNMP polling, streaming telemetry, NetFlow, Syslog, CLI-based collection, APIs, and IP SLA. Each mechanism serves a different purpose: some report basic device health (CPU, memory, KPIs), while others deliver granular detail (PoE status, client sessions, wireless performance).

1. **Device/Inventory Health (SNMP + CLI):** Reachability, CPU, memory, interface stats, and software version — collected via standard SNMP polling and CLI.
2. **Syslog:** System and operational log messages sent to Catalyst Center, which acts as the configured syslog server.
3. **Wireless Telemetry (NETCONF/YANG streaming):** The core Assurance feed. It streams AP and client-level data in near real time — client onboarding and roaming events, RSSI/SNR, AP radio/RF statistics, and WLC internal health counters.

To receive this data, the Wireless LAN Controller must be in managed state on Catalyst Center, with the telemetry status showing as up between the 9800 Controller and Catalyst Center.

The screenshot shows the Catalyst Center Provision / Inventory page. The 'Wireless Controllers' tab is selected. A table lists the devices, with one device highlighted: 'WLC Hostname' with IP 'WLC IP', Vendor 'Cisco', Reachability 'Reachable', 4 alerts, Managed status, and Non-Compliant compliance. The site is '.../CampusControllers/West' and the image version is '17.15.4d'. The last updated time is '8 hours 54 minutes ago'.

Tags	Device Name	IP Address	Vendor	Reachability	ExX Status	Manageability	Compliance	Site	Image Version	Last Updated
	WLC Hostname	WLC IP	Cisco	Reachable	4 alerts	Managed	Non-Compliant	.../CampusControllers/West	17.15.4d	8 hours 54 minutes ago

Wireless LAN Controller Status on Catalyst Center

<#root>

WLC#

```
show telemetry connection all
```

Telemetry connections

Index	Peer Address	Port	VRF	Source Address	State	State Description
0	CATC_IP	25103	0	WLC_IP	Active	Connection up

By default, Cisco Catalyst Center is configured with health, issue, and event settings that include specific thresholds and priorities for Wireless Controllers, Access Points, Wireless Clients, and Applications. Catalyst Center generates events and alerts based on the data it receives from these managed devices and the configured event settings. Additionally, custom profiles can be created to tailor these settings according to specific network requirements, allowing for more precise monitoring and alerting based on the unique needs of the network environment.

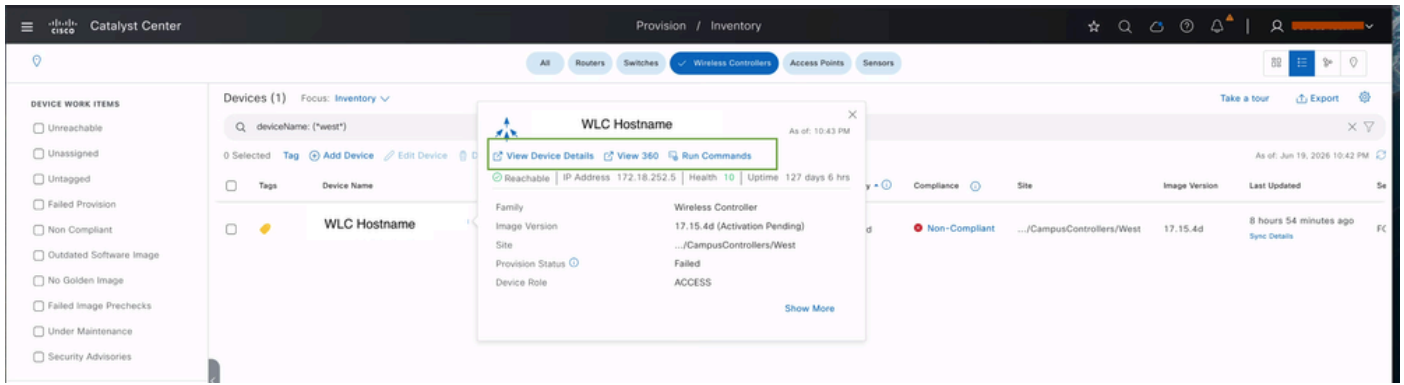
Issue with Catalyst 9800 Series Wireless Controller

When a Wireless LAN Controller (WLC) experiences problems such as reachability loss, slow performance, accessibility errors, an outage, or degradation in a specific service, Cisco Catalyst Center provides built-in visibility that lets you reconstruct what was happening on the controller at the exact time of the issue — without needing to log in to the device directly.

Reviewing Controller Health with Device 360

The Device 360 view consolidates a controllers reachability, telemetry status, historical issues, generated events, and performance statistics into a single timeline-driven dashboard, making it the first place to look when investigating a reported WLC problem.

Navigate to **Provision > Inventory > Wireless Controller > [search for the controller] > click the device name > Device 360**



View 360 for Wireless LAN Controller



Note: The same view can also be reached from Assurance > Health > Network, then clicking the device name in the Network Devices table.

Device 360 lets you move the health timeline slider back to any point within the supported historical window (Catalyst Center Assurance data is retained for up to 30 days) to see exactly what the controller status looked like at the time of the incident. For that selected window, the view surfaces:

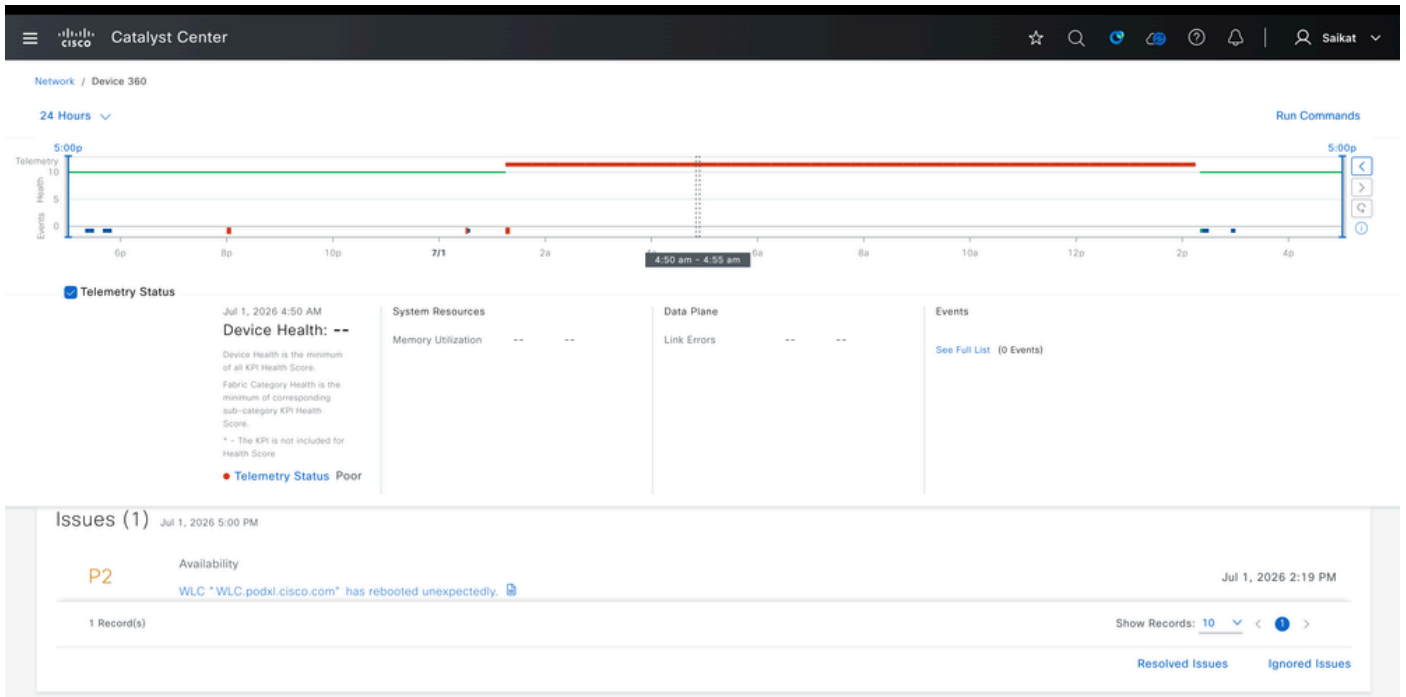
Device reachability — whether the controller was reachable and managed.

Telemetry status — health of the SNMP/Syslog/NETCONF telemetry feeding Assurance.



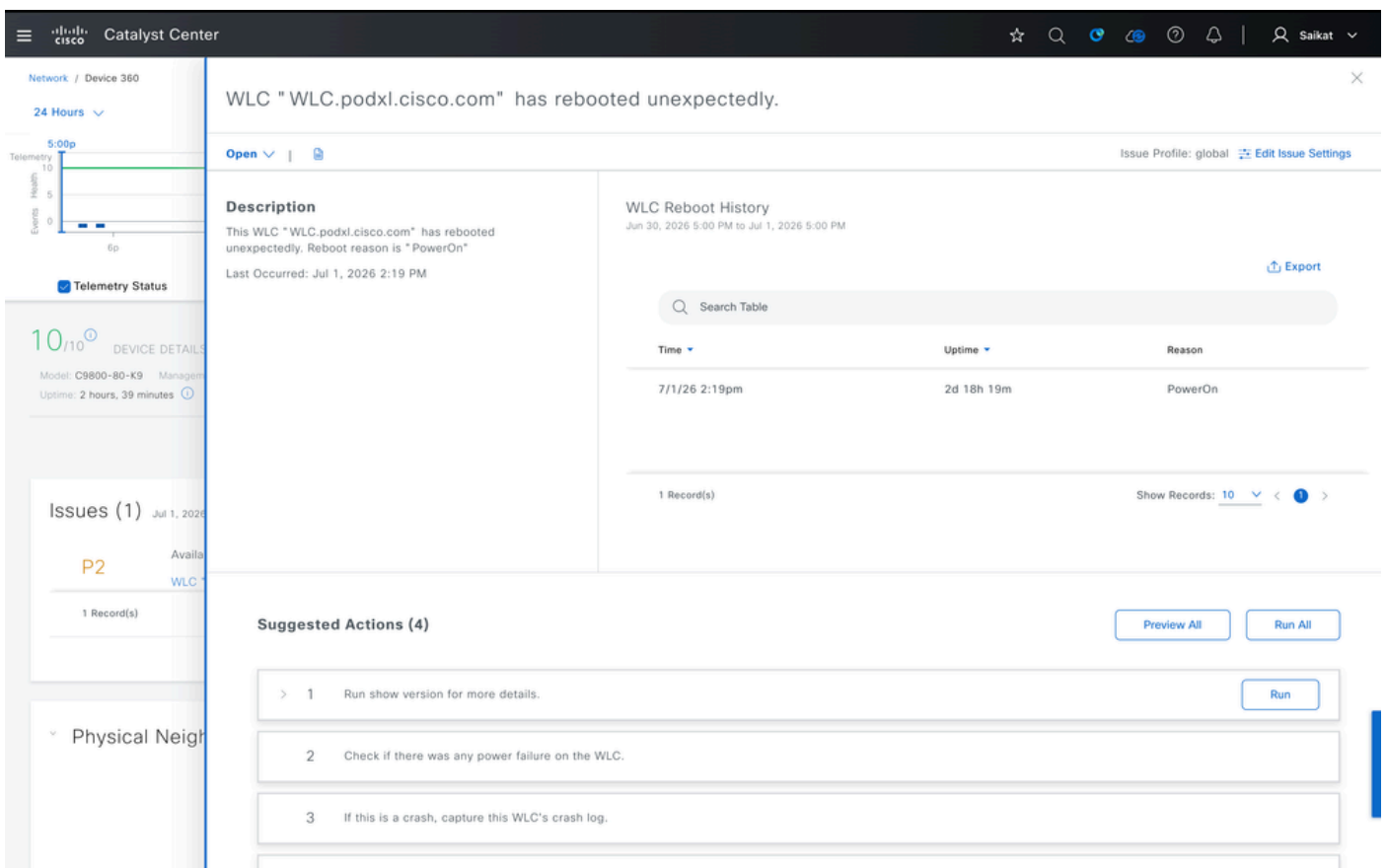
Telemetry Status of Wireless LAN Controller

Issues observed — Assurance-detected problems on the device during that period.



Issues Reported for Wireless LAN Controller

By clicking a specific issue you can see detailed information about it, along with suggested actions to resolve it or investigate further.



Suggested Action for Issue Reported on WLC

Event Viewer

Go to Global Event Viewer Export Full Screen

Search Table

Severity	Details	Message Type	Time
Jun 19, 2026			
Alert	MM_NODE_LOG:KEEP_ALIVE	Syslog	2:44:51.867 PM
Alert	MM_NODE_LOG:ANCHORS_DOWN	Syslog	2:44:31.673 PM
Alert	MM_NODE_LOG:KEEP_ALIVE	Syslog	2:44:31.672 PM
Notice	CAPWAPAC_SMGR_TRACE_MESSAGE:AP_JOIN_DISJOIN	Syslog	12:49:30.457 PM
Notice	CAPWAPAC_SMGR_TRACE_MESSAGE:AP_JOIN_DISJOIN	Syslog	12:47:20.893 PM
Notice	CAPWAPAC_SMGR_TRACE_MESSAGE:AP_JOIN_DISJOIN	Syslog	6:19:51.230 AM

10 records Show Records: 25 1 - 11

MM_NODE_LOG_A... Jun 19, 2026 2:44:31 PM [Create an Issue](#)

Detailed Information

Severity	Alert
Mnemonic	ANCHORS_DOWN
Facility	MM_NODE_LOG
Message Text	77554901: wlc-200-wlc0-9k: Jun 19 19:14:31.360 AEST: %MM_NODE_LOG-1-ANCHORS_DOWN: Chassis 1 RRD: mobility: All Export-Anchors are down.
Message Type	Syslog

Event Viewer for Wireless LAN Controller - Example2

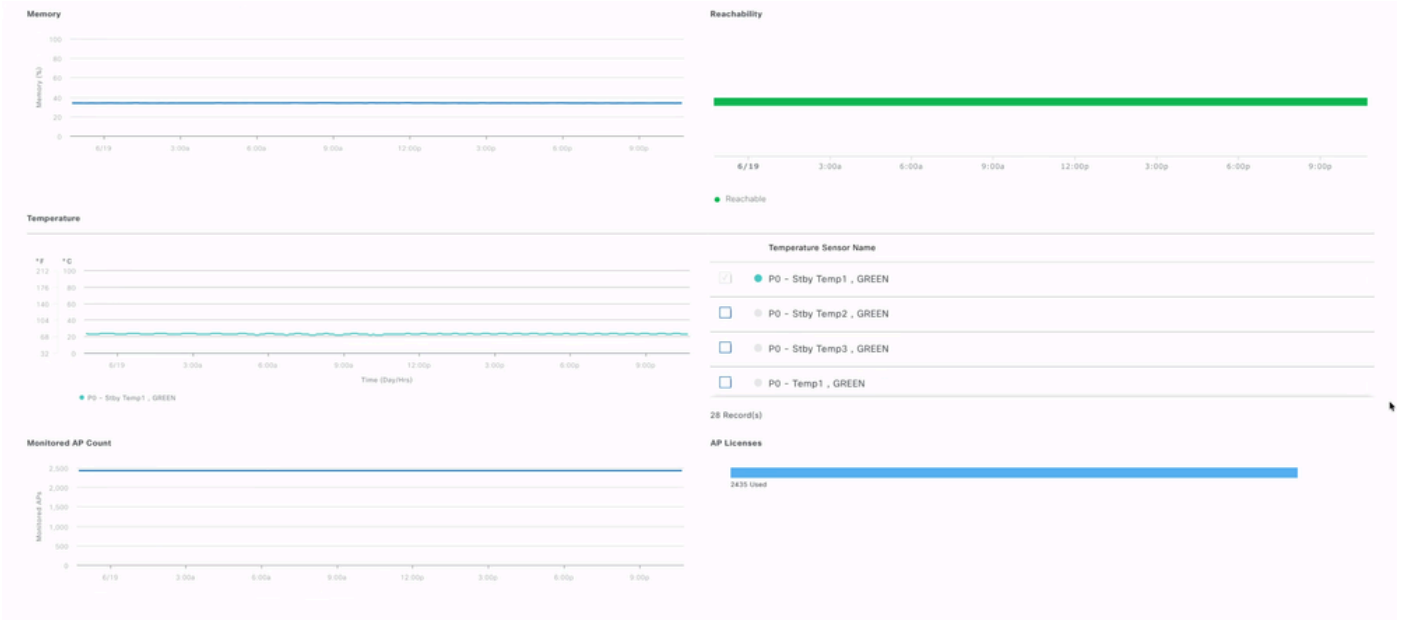
Performance statistics — CPU and memory utilization, temperature, uptime, HA state, and last reload reason.

Connected clients — including breakdowns by local, foreign, anchor, and idle client counts.

AP status — the join/health state of access points associated with the controller.

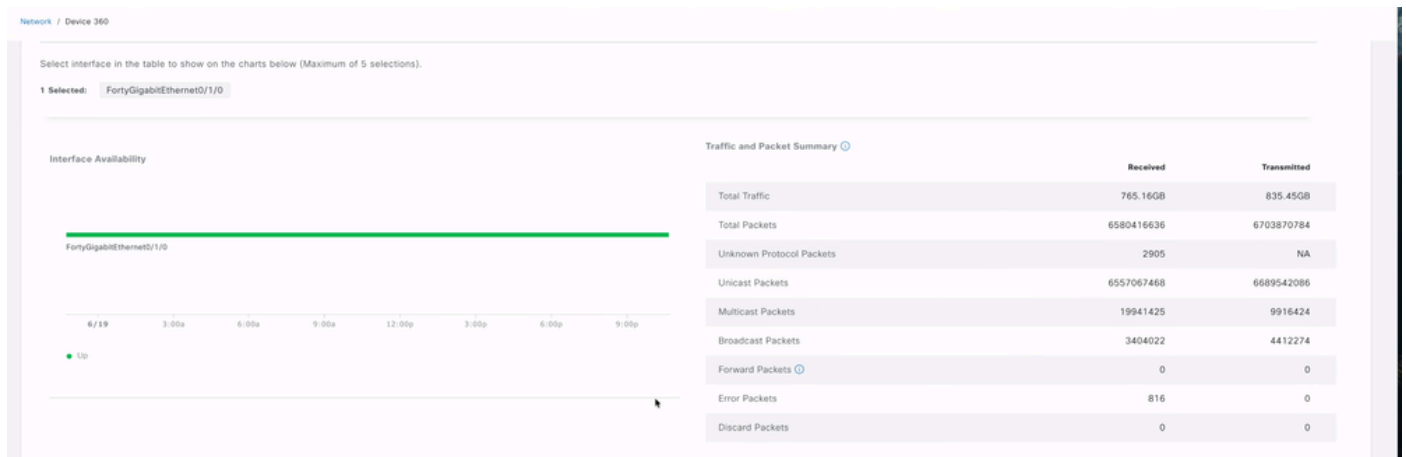


WLC Statistics on Catalyst Center



WLC Statistics on Catalyst Center

Interface statistics — per-interface status, RX/TX packet counts, utilization, discards, and errors.



WLC Statistics on Catalyst Center

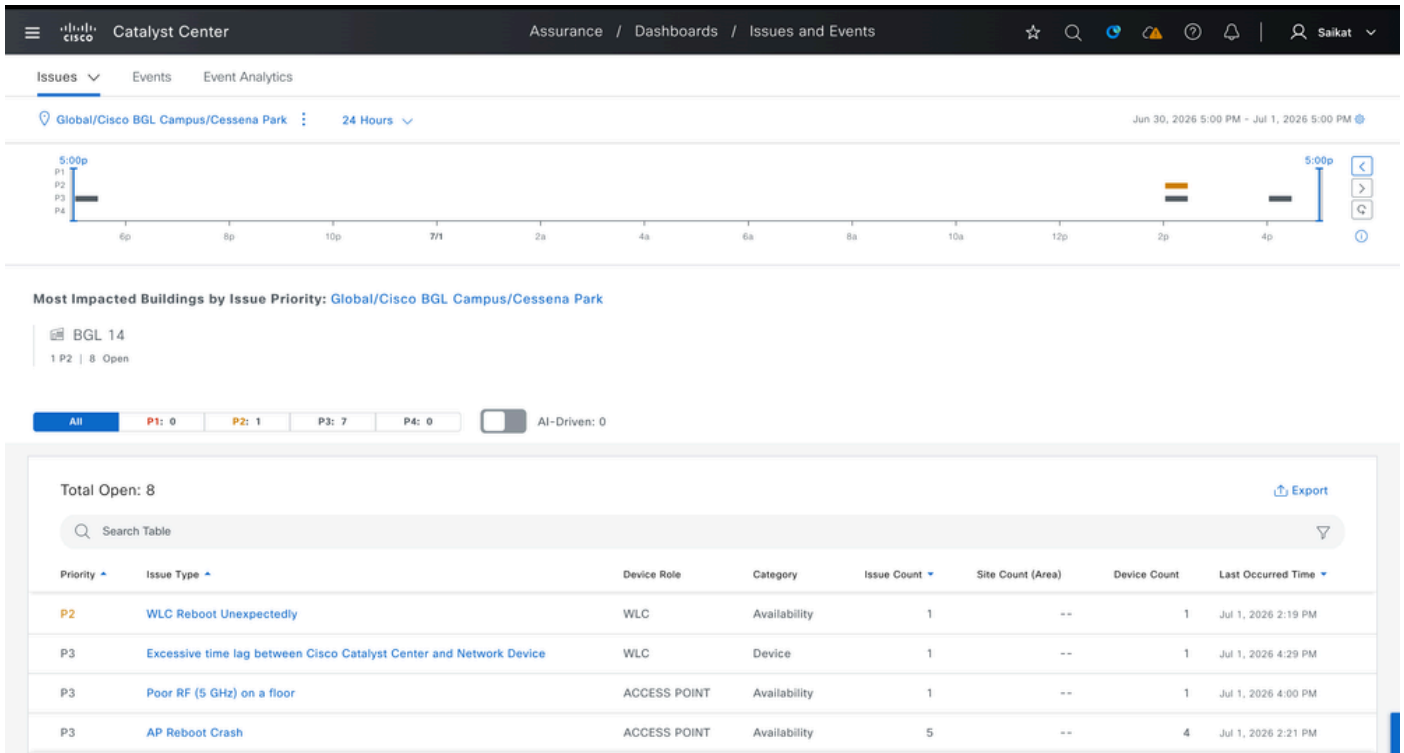


WLC Statistics on Catalyst Center

Because all of this is correlated, you can correlate multiple related factors during the time of issue and get the clear understanding. With these statistics you can not exactly get the root cause of the issue but we can rule out all the potential causes that can help us to troubleshoot further and setup the type of logs required to be collected real-time.

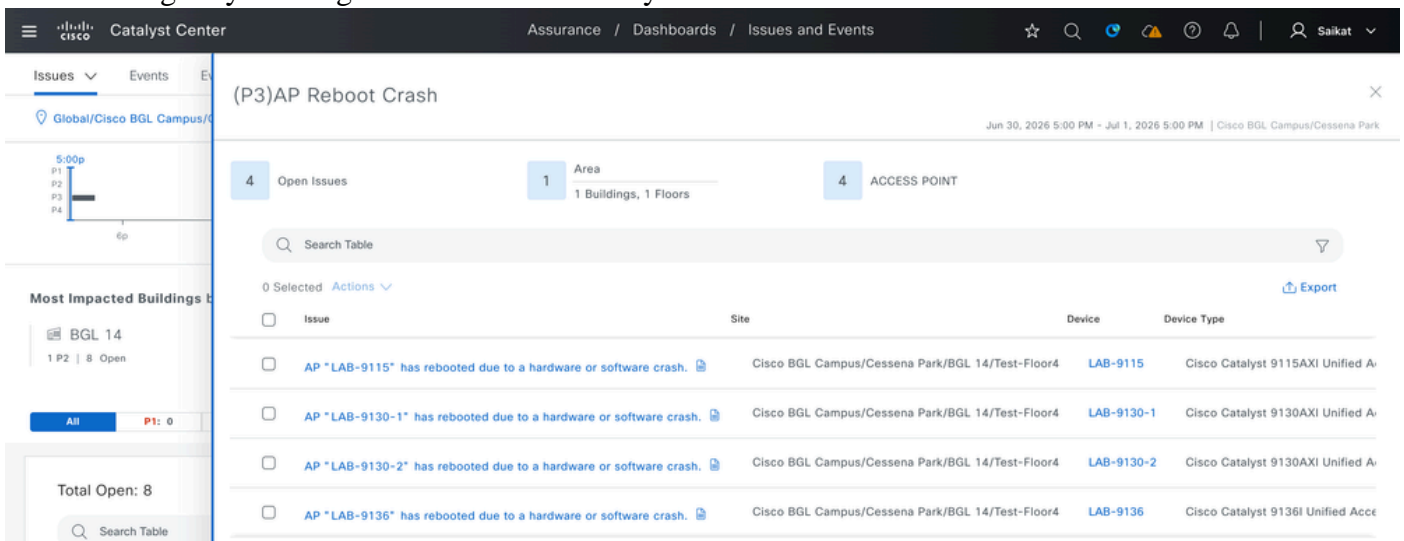
Issue with an Access Point

When a Cisco Access Point encounters issues such as disconnect events, radio status anomalies, reboots, crashes, poor RF conditions, high channel utilization, or inactivity, Catalyst Center generates alerts with appropriate priority levels. You can view these alerts by navigating to **Assurance > Issues and Health Settings**.



Issues Reported Generates an Alerts with Respective Priority

This section displays all open issues in your environment. By clicking individual events, you can get the detailed insight by clicking each event individually:



Detailed Overview of Issue Reported

By clicking a specific issue you can see detailed information about it, along with suggested actions to resolve it or investigate further.

Catalyst Center Assurance / Dashboards / Issues and Events

AP Reboot Crash / Issue Instance

Global/Cisco BGL Campus/...

AP "LAB-9115" has rebooted due to a hardware or software crash.

Open | Issue Profile: global | Edit Issue Settings

Description
 This AP "LAB-9115" has rebooted due to a hardware or software crash.
 Last Occurred: Jul 1, 2026 2:21 PM
 Jul 1, 2026 2:16 PM - 2:21 PM

AP Last Reboot Crash Logs
 Jun 30, 2026 4:59 PM to Jul 1, 2026 4:59 PM

Time	Up time	Down time
7/1/26 2:21pm	7h 4m	13h 53m

1 Record(s) Show Records: 25 < 1 >

Impacted Client Table

Suggested Actions (2)

- 1 Capture this AP's crash log.
- > 2 If you are unable to resolve the issue, contact Cisco TAC for support.

Suggestion Action for Issue Reported on AP

Additionally, you can access the **Event Viewer**, which contains all events received by Catalyst Center as syslog. This is useful for tracking all events such as AP join/disjoin activity, channel changes, TX power modifications, and reboots. These events are captured for both the wireless controller and individual APs.

Catalyst Center Assurance / Dashboards / Issues and Events

Issues ▾ Events Event Analytics

Global/Cisco BGL Campus/Cessena Park 24 Hours Jun 30, 2026 5:00 PM - Jul 1, 2026 5:00 PM

Events (142)

Category Type: **Devices** Endpoints Router: 0 Switch: 0 Wireless Controller: 74 **AP: 68** Third Party Device: 0

Filter Table

0 Selected

<input type="checkbox"/>	Event Name	Status	Timestamp	Device Name	Event Type	Device IP
<input type="checkbox"/>	AP is connected to WLC. CAPWAP channel is up	●	Jun 30, 2026 5:28:01.534 PM	LAB-9115	Device Event	10.127.197.180
<input type="checkbox"/>	AP is disconnected from WLC. CAPWAP channel is down	●	Jul 1, 2026 12:30:30.273 AM	LAB-9115	Device Event	10.127.197.180
<input type="checkbox"/>	AP is connected to WLC. CAPWAP channel is up	●	Jul 1, 2026 2:24:00.118 PM	LAB-9115	Device Event	10.127.197.180
<input type="checkbox"/>	Channel Change	●	Jul 1, 2026 3:21:57.015 PM	LAB-9115	Device Event	10.127.197.180
<input type="checkbox"/>	Channel Change	●	Jul 1, 2026 3:11:38.998 PM	LAB-9115	Device Event	10.127.197.180
<input type="checkbox"/>	Channel Change	●	Jul 1, 2026 3:42:39.052 PM	LAB-9115	Device Event	10.127.197.180
<input type="checkbox"/>	AP is connected to WLC. CAPWAP channel is up	●	Jun 30, 2026 5:25:48.921 PM	LAB-9130-2	Device Event	10.127.197.182
<input type="checkbox"/>	AP is disconnected from WLC. CAPWAP channel is down	●	Jul 1, 2026 12:30:28.273 AM	LAB-9130-2	Device Event	10.127.197.182

Events Viewer for APs on Catalyst Center

Catalyst Center Assurance / Dashboards / Issues and Events

Issues ▾ Events Event Analytics

Global/Cisco BGL Campus/Cessena Park 24 Hours

Events (142)

Category Type: **Devices** Endpoints Router: 0 Switch: 0 Wireless Controller: 74 **AP: 68** Third Party Device: 0

Filter Table

0 Selected

Event Name

AP is disconnected from WLC. CAPWAP channel is down
Jul 1, 2026 12:30:30.273 AM

Additional Info: AP Disconnect - Heartbeat not heard from AP

Event Type: Device Event

Device Name: LAB-9115

Device IP: 10.127.197.180

Location: Global/Cisco BGL Campus/Cessena Park/BGL 14/Test-Floor4

Wireless Controller: WLC.podxl.cisco.com

AP Base Radio Mac: 5C:E1:76:6A:D2:C0

Reason: AP Disconnect - Heartbeat not heard from AP

Connected Device Events (1)
Jul 1, 2026 12:15 AM - 12:45 AM

Wireless Controller: WLC.podxl.cisco.com Wireless Endpoints Switch: BGL14-1-C16-2960-1.esl.cisco.com

Show Events (+15 mins)

Catalyst Center Assurance / Dashboards / Issues and Events

Issues Events Event Analytics

Global/Cisco BGL Campus/Cessena Park

Events (142)

Category Type: Devices Endpoints

Filter Table

0 Selected

Event Name

AP is connected to WLC. CAPWAP channel is up

Tx Power Change
Jul 1, 2026 3:21:59.016 PM

Additional Info: Radio Slot : 1 (5.0GHz) | Power: 11 dBm -> 8 dBm | System Driven

Event Type: Device Event

Device Name: LAB-9130-2

Device IP: 10.127.197.182

Location: Global/Cisco BGL Campus/Cessena Park/BGL 14/Test-Floor4

Wireless Controller: WLC.podxl.cisco.com

AP Base Radio Mac: 88:9C:AD:E7:9F:C0

Radio: 1

Frequency: 5.0GHz

Reason: System Driven : Tx Power change due to running TPC Algo.

Current Power Level: 8 dBm

Previous Power Level: 11 dBm

Connected Device Events
Jul 1, 2026 3:06 PM - 3:36 PM

Wireless Controller: WLC.podxl.cisco.com Wireless Endpoints Switch: BGL14-1-C16-2960-1.esl.cisco.com

Detailed Overview of Event Reported (Notice)

Catalyst Center Assurance / Dashboards / Issues and Events

Issues Events Event Analytics

Global/Cisco BGL Campus/Cessena Park

Events (142)

Category Type: Devices Endpoints

Filter Table

0 Selected

Event Name

AP is connected to WLC. CAPWAP channel is up

AP is disconnected from WLC. CAPWAP channel is

Channel Change
Jul 1, 2026 3:21:57.015 PM

Additional Info: Radio Slot : 1 (5.0GHz) | Primary Channel: 157->64 | System Driven

Event Type: Device Event

Device Name: LAB-9115

Device IP: 10.127.197.180

Location: Global/Cisco BGL Campus/Cessena Park/BGL 14/Test-Floor4

Wireless Controller: WLC.podxl.cisco.com

AP Base Radio Mac: 5C:E1:76:6A:D2:C0

Radio: 1

Frequency: 5.0GHz

New Channel List: [64, 60]

Old Channel List: [157, 161]

Interference: -56 dBm -> -121 dBm

Noise: -86 dBm -> -84 dBm

Reason: System Driven : Dynamic Channel Assignment(DCA) run by controller attributing Channel Change due to following factors - Signal Interference

Connected Device Events
Jul 1, 2026 3:06 PM - 3:36 PM

Wireless Controller: WLC.podxl.cisco.com Wireless Endpoints Switch: BGL14-1-C16-2960-1.esl.cisco.com

Detailed Overview of Event Reported (Notice)

Catalyst Center Assurance / Dashboards / Issues and Events

Issues Events Event Analytics

Global/Cisco BGL Campus/Cessena Park

Events (142)

Category Type: Devices Endpoints

Filter Table

0 Selected

Event Name

AP is connected to WLC. CAPWAP channel is up
Jun 30, 2026 5:25:48.921 PM

Additional Info: Last Reset Type - Configuration Changes

Event Type: Device Event

Device Name: LAB-9130-2

Device IP: 10.127.197.182

Location: Global/Cisco BGL Campus/Cessena Park/BGL 14/Test-Floor4

Wireless Controller: WLC.podxl.cisco.com

AP Base Radio Mac: 88:9C:AD:E7:9F:C0

Last Reset Type: Configuration Changes

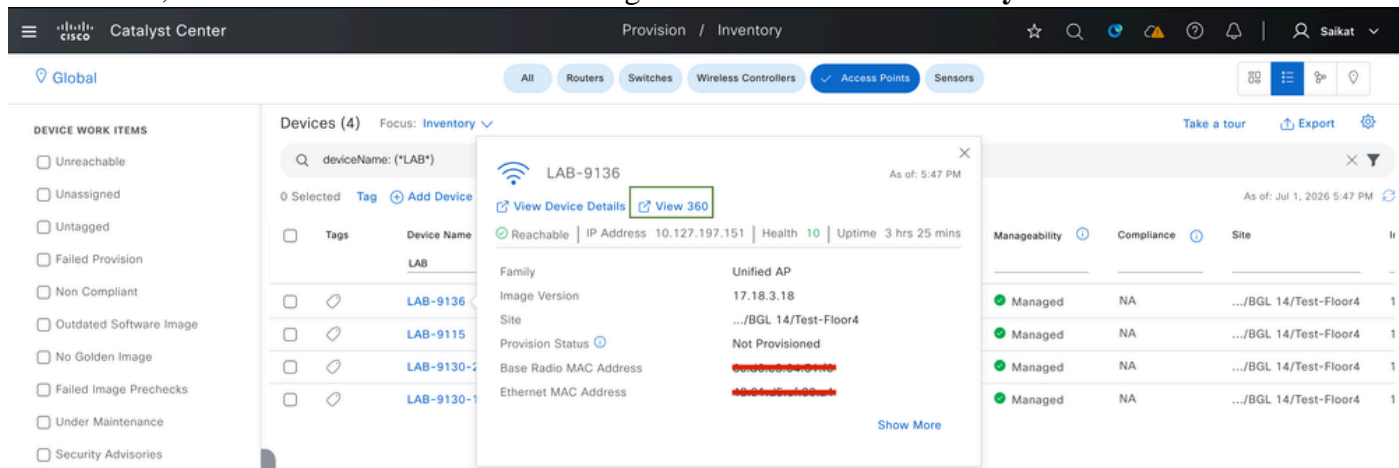
Connected Device Events
Jun 30, 2026 5:10 PM - 5:40 PM

Wireless Controller: WLC.podxl.cisco.com Wireless Endpoints Switch: --

Show Events (±15 mins)

Detailed Overview of Event Reported (Info)

For issues specific to an individual AP, you can check the **360 Health** view for that device. Here you can see the reachability status, reported events and issues, along with the health score for that AP at a given point in time. The health score is calculated based on memory utilization, channel utilization, air quality, interference, and traffic utilization. For this navigate to **Provision > Inventory > Access Point > Click AP:**



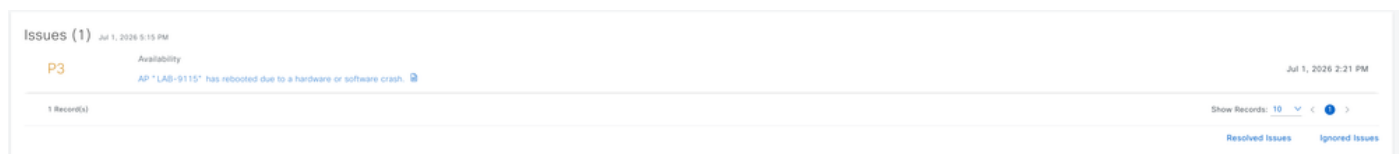
View 360 for Individual AP

Device 360 Telemetry Summary: Here you can see the APs overall health score timeline, system resource utilization (memory, CPU), data plane link errors, and radio-specific stats (noise, channel utilization, interference, traffic utilization) for both radios. Device 360 lets you move the health timeline slider back to any point within the supported historical window (30 days).



View 360 : AP Telemetry Status and Health

Issues - Here you can see the list of open issues for the AP, along with severity (P1-P4), issue category, description, and timestamps.



Issue Reported for AP

Event Viewer - You can see a chronological log of AP events (example channel changes, CAPWAP status) along with detailed event information such as WLC name, radio, frequency, reason, and old/new channel lists.

The screenshot shows the 'Event Viewer' interface. On the left, there is a table of events for July 1, 2026. The table has columns for 'Event Type', 'Details', and 'Time'. The events listed are:

Event Type	Details	Time
Channel Change	Radio Slot : 1 (5.0GHz) Primary Channel: 64->140 System Driven	3:42:39.052 PM
Channel Change	Radio Slot : 1 (5.0GHz) Primary Channel: 157->64 System Driven	3:21:57.015 PM
Channel Change	Radio Slot : 1 (5.0GHz) Primary Channel: 36->157 System Driven	3:11:38.998 PM
AP is connected to WLC. CAPWAP channel is up	Last Reset Type - Crash	2:24:00.118 PM

On the right, a detailed view of a 'Channel Change' event is shown for July 1, 2026, 3:42:39 PM. The 'Detailed Information' section includes:

- WLC Name: WLC.pool.cisco.com
- AP Base Radio Mac: 50:61:76:6A:02:00
- Radio: 1
- Frequency: 5.8GHz
- Event Type: Channel Change
- Reason: System Driven - Dynamic Channel Assignment(DCA) run by controller distributing Channel Change due to following factors - Signal Interference
- New Channel List: [140, 144]
- Old Channel List: [84, 80]

Event Viewer of Individual AP

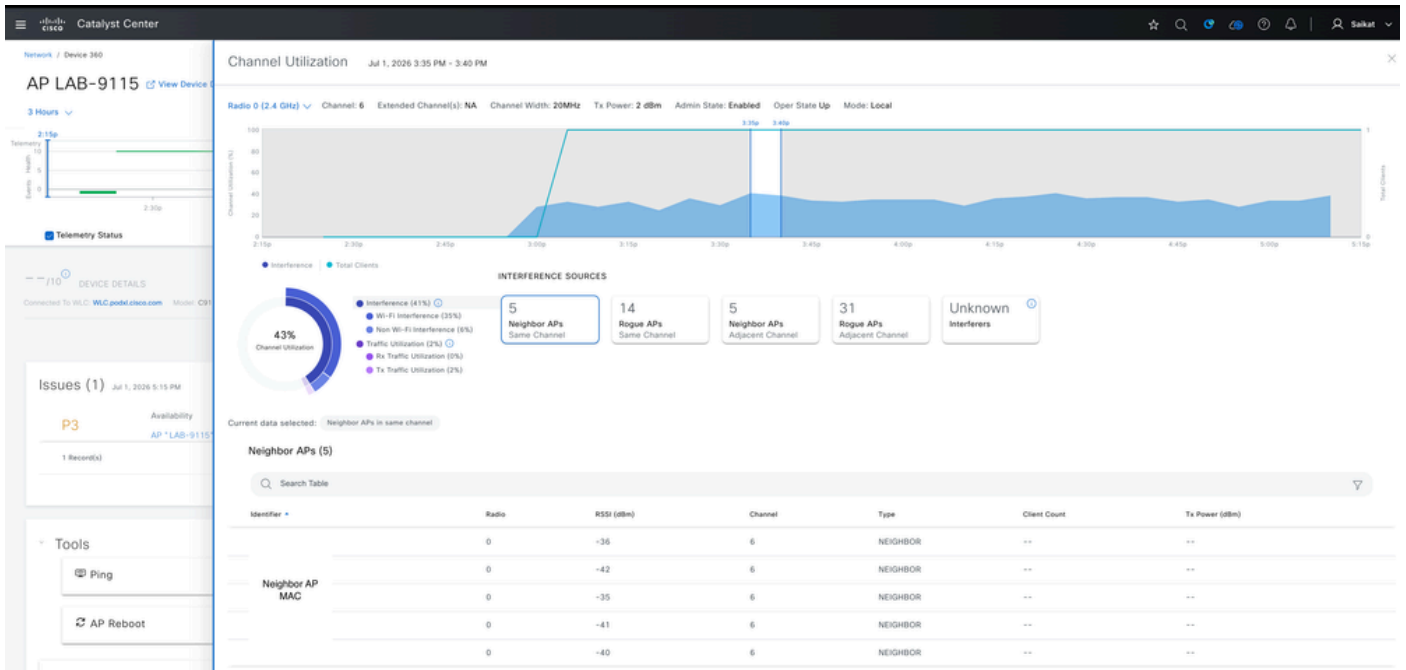
Physical Neighbor Topology with Client List - This view displays the physical topology connecting the WLC, AP, and connected clients, along with additional client details like device name, health score and MLO

The screenshot shows the 'Physical Neighbor Topology' view. It features a network diagram with a central WLC (WLC.a.pool) connected to an AP (AP1). The AP is connected to a client (cxLabs-WIN11). Below the diagram, there are statistics: 2 APs Clients, 1 Non-MLO Client, 0 MLO Link, 1 Non-MLO Client, and 0 MLO Link. A 'View Client List' button is present. On the right, a popup window titled '1 Client (2.4 GHz)' shows details for the client 'cxLabs-WIN11':

Device	Health Score	IPv4 Address	IPv6
cxLabs-WIN11	10	10.127.197.177	fe80

Physical Topology of AP

Channel Utilization - You can see the APs channel utilization trend, interference sources (neighbor APs, rogue APs, unknown interferers), and a detailed neighbor AP table with RSSI, channel, and type.



Channel Utilization for Individual AP

Detail Information (Device Tab) - This section shows device information (AP name, IP, model, MAC addresses, software version), availability details (uptime, controller join time, last reset reason), CPU/memory utilization graphs, and the AP-to-WLC connectivity chart.



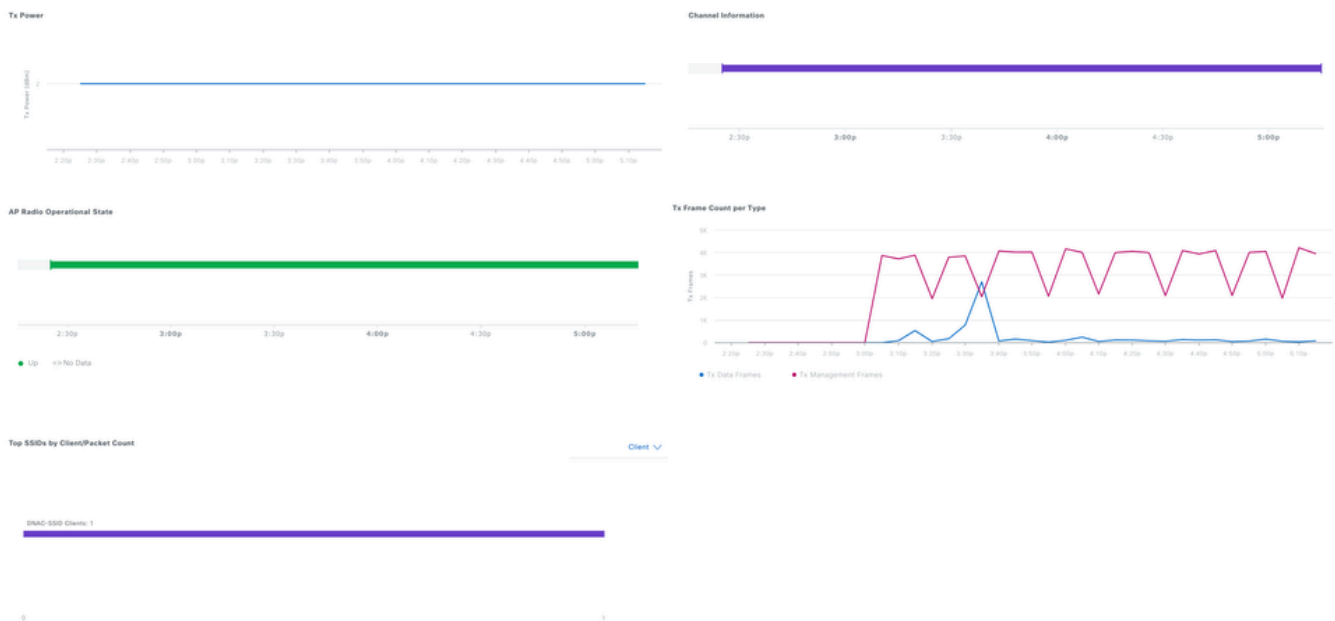
Device Details for AP

Radio Specific KPIs: Here you can view radio-level KPIs including channel utilization, client count, throughput (Rx/Tx rate), retries, noise, and air quality for the selected radio.



RF Statistics for Individual AP

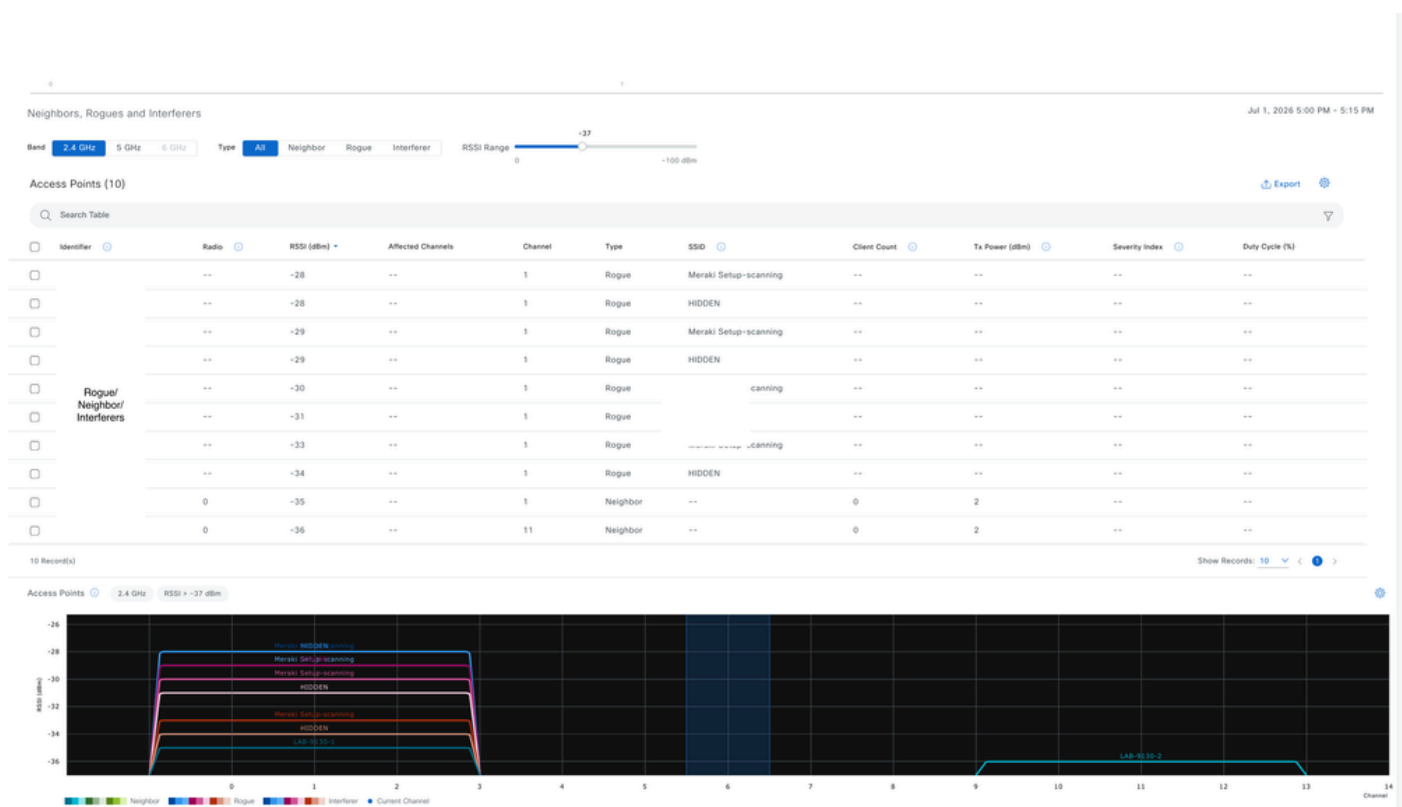
Tx Power, Channel Information & Frame Stats: On this screen, you can see Tx power trends, channel assignment history, AP radio operational state, Tx frame counts by type (data vs. management), and top SSIDs by client/packet count.



RF Statistics for Individual AP

Neighbors, Rogues and Interferers: This view lets you see all nearby neighbor, rogue, and interferer devices with their RSSI, affected channels, SSID, client count, Tx power, and severity index, along with a visual

RSSI-vs-channel plot.



Rogue, Neighbor and Interferers Reported for Individual AP

The Device 360 dashboard brings together RF details like channel usage, interference, noise, and retries, along with nearby neighbor, rogue, and interferer information — helping you figure out if an AP problem is caused by RF congestion, channel conflicts, or rogue devices. Device health data like CPU, memory, reboot history, and connectivity status, along with the Event Viewer and Issues panel, help you understand hardware crashes, connection drops, and unexpected channel changes. Combined with the topology and client views, this gives a complete picture for troubleshooting — from RF issues down to individual client problems — with suggested actions built in to help resolve them

Intelligent Captures for Access Point

Intelligent Capture for the access point offers two main features: always-on real-time RF monitoring, anomaly detection and on-demand over the air capture, spectrum analysis.

AP Statistics Capture

You can enable and manage AP Statistics data collection for one or more access points — including AP radio statistics, WLAN statistics, and AP client statistics — with support for up to 1000 APs.

To enable AP Stats Capture, navigate to **Assurance > Settings > Intelligent Capture Settings > Access Point > AP Stats Capture**. From here, you have the flexibility to either:

- Enable it for specific APs (up to 1000), or
- Enable it globally for all APs managed under a particular WLC.

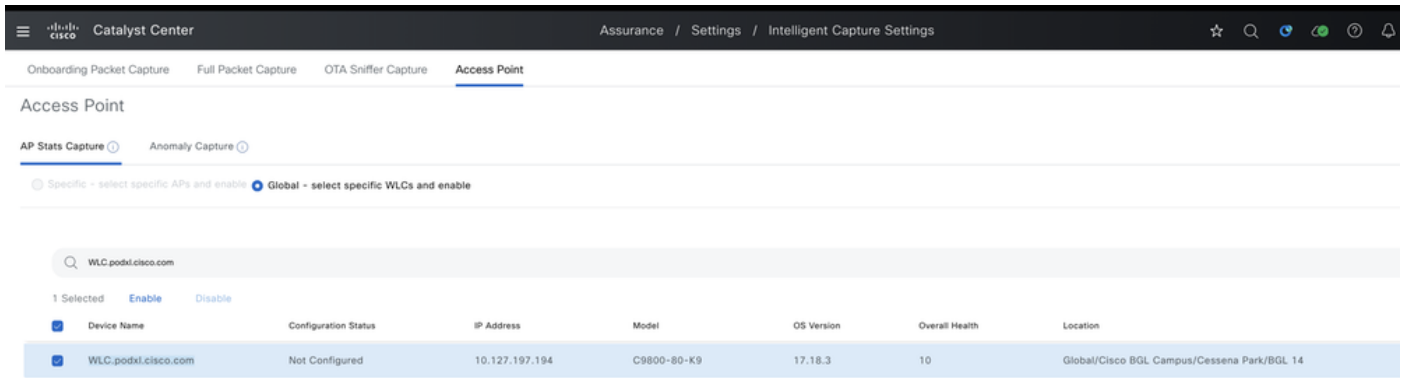
The screenshot shows the 'Intelligent Capture Settings' page for an 'Access Point'. The breadcrumb trail is 'Assurance / Settings / Intelligent Capture Settings'. Under 'Access Point', there are two tabs: 'AP Stats Capture' (selected) and 'Anomaly Capture'. A central graphic shows a blue cube with a white top, surrounded by a light blue circle. Below it, the text reads 'Configure AP Enablement' with two radio button options: 'Specific - select specific APs and enable' (selected) and 'Global - enable or disable capable WLCs'. A 'Get Started' button is located at the bottom.

AP Stats Capture Option

This screenshot shows the configuration details for an 'Access Point' under 'AP Stats Capture'. The breadcrumb trail is 'Assurance / Settings / Intelligent Capture Settings'. The 'Specific - select specific APs and enable or disable' option is selected. A message states: '1 APs are individually configured out of an allowed total of 1000.' On the left, a 'Find Hierarchy' search box is visible with a tree view showing 'Global', '9800-CL', 'BGL SDA', 'Guru', and 'Karnataka'. The main area shows a table with columns: 'Access Point', 'Device Type', 'OS Version', 'Overall Health Score', 'Client Count', and 'Configuration Status'. One AP is selected and its status is 'Enable'. The table contains one row with the following data:

Access Point	Device Type	OS Version	Overall Health Score	Client Count	Configuration Status
AP_NAME	C9130AXI-D	17.15.4.160	Down	--	--

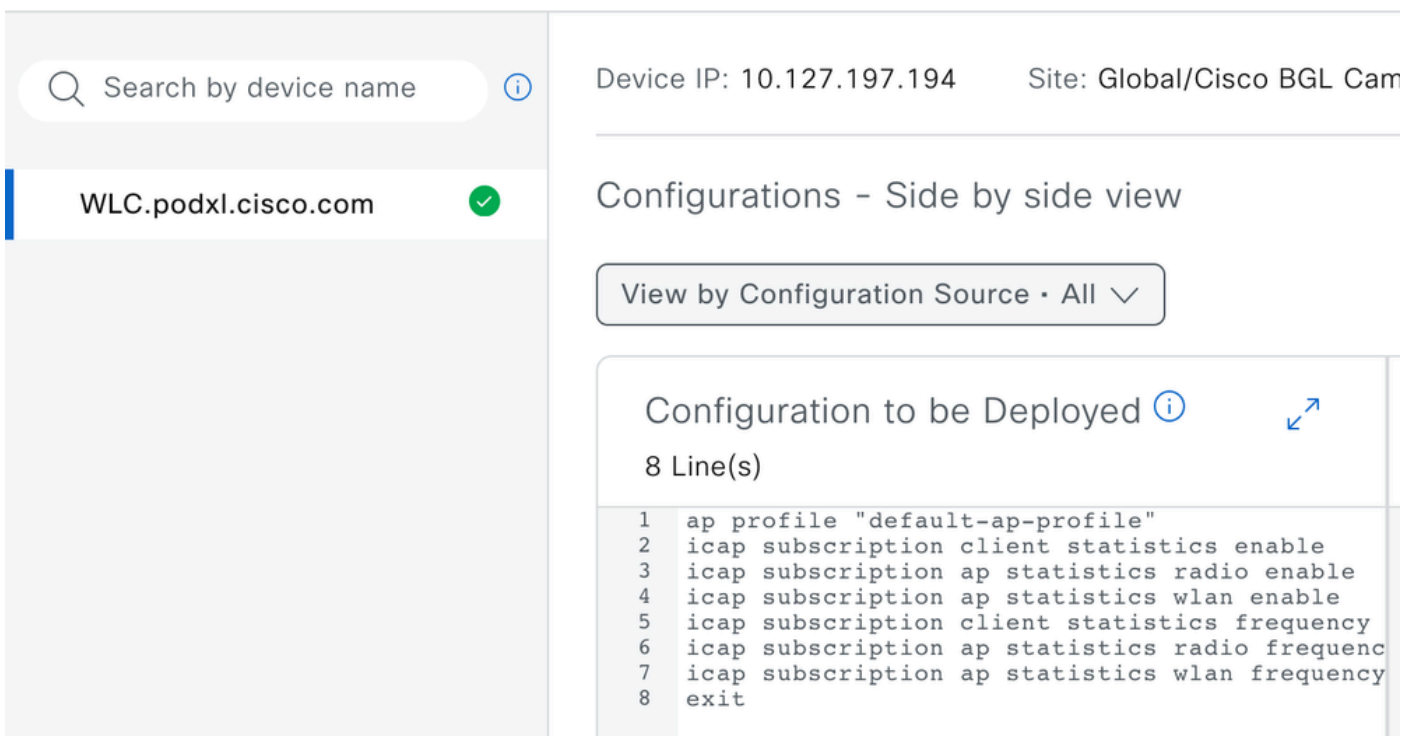
Enable AP Stats Intelligent Captures on Specific AP



Enable AP Stats Intelligent Capture Globally

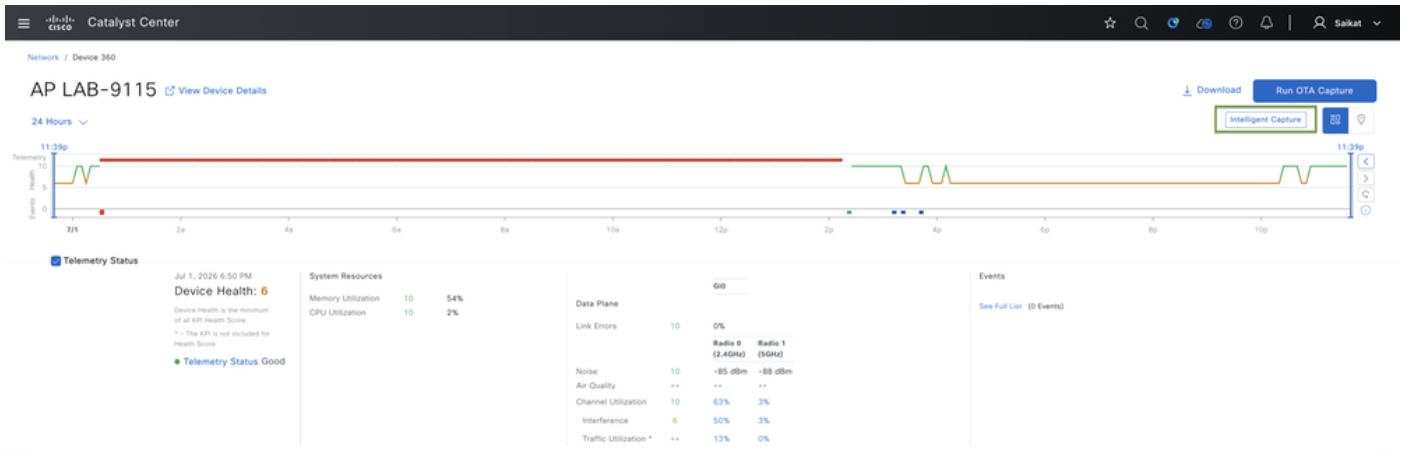
Once AP Stats Capture is enabled, Catalyst Center pushes the corresponding configuration to the WLC — either for the specific AP(s) selected or for all APs, depending on whether it was enabled at the individual AP level or globally at the WLC level.

Task Details / Work Item Details

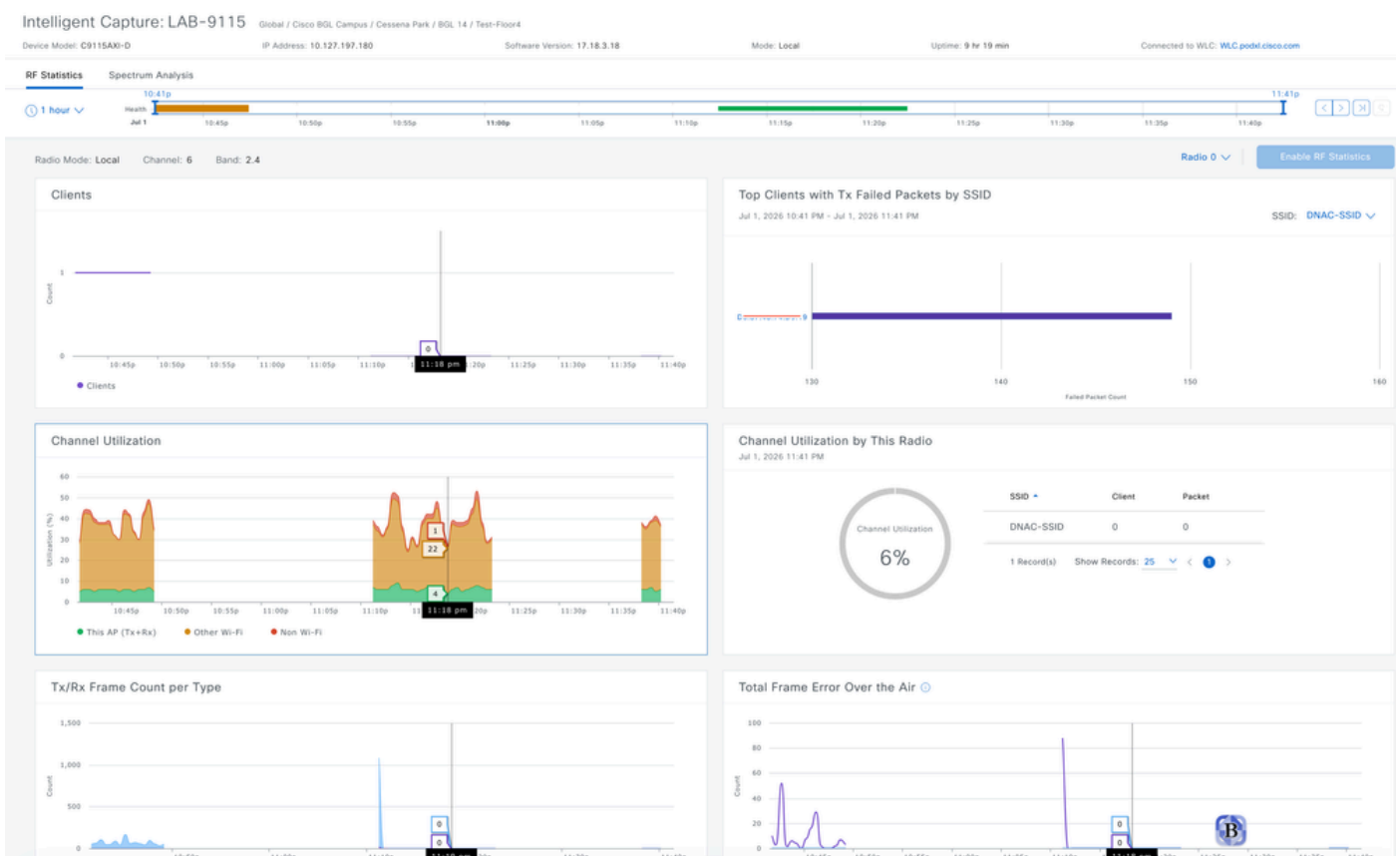


Configuration to be Pushed when AP Stats Capture is Enabled

After enabling this capture, you can view the real-time data collected through Intelligent Capture directly from the **Device 360** page. Additionally, you can run **Spectrum Analysis** on demand as needed to further investigate RF conditions.



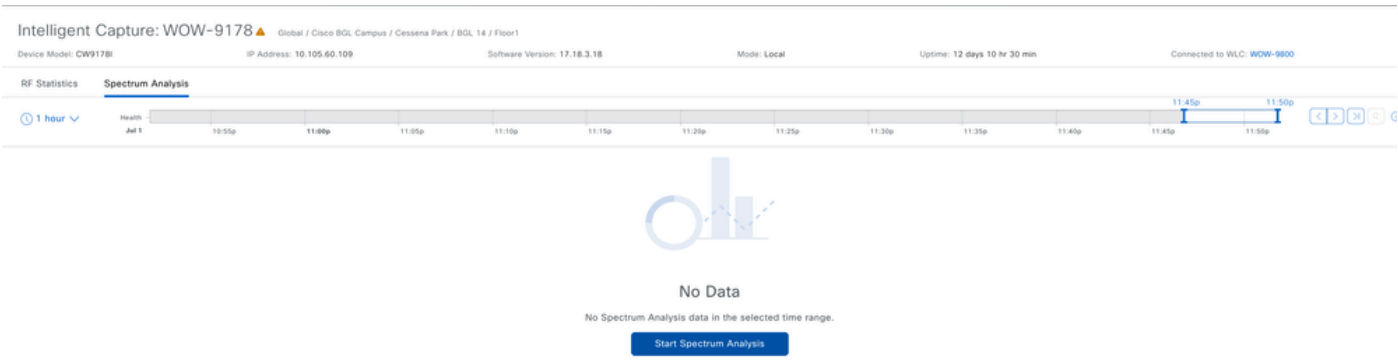
Intelligent Capture for AP in Device 360



AP Stats Captured using Intelligent Capture on Catalyst Center

Here you can see real-time statistics covering Tx/Rx frame count per type, total frame errors over the air, multicast/broadcast counters, Tx power and noise floor, channel utilization, top clients with failed Tx packets by SSID, and client data captured for specific AP using Intelligent capture.

You can also run on-demand spectrum analysis for an individual AP whenever needed to inspect RF conditions. However, this feature requires the AP model to support it.



On Demand Spectrum Analysis

Enable Spectrum on WOW-9178

Step 3 of 3: Preview Configuration

Review the device configuration provided below by clicking on each device. When you are done reviewing, click Deploy. Click [Exit and Preview Later](#) to

Deploy

Now Later

Task Name*
Enable Spectrum on WOW-9178

Once submitted, the progress and relevant information can be tracked from the [Activities > Tasks](#) window.

Search by device name

WOW-9800 ●

Device IP: 10.105.60.100 Site: Global/Cisco BGL Campus/Ce...

Configurations - Side by side view

View by Configuration Source - All

Configuration to be Deployed

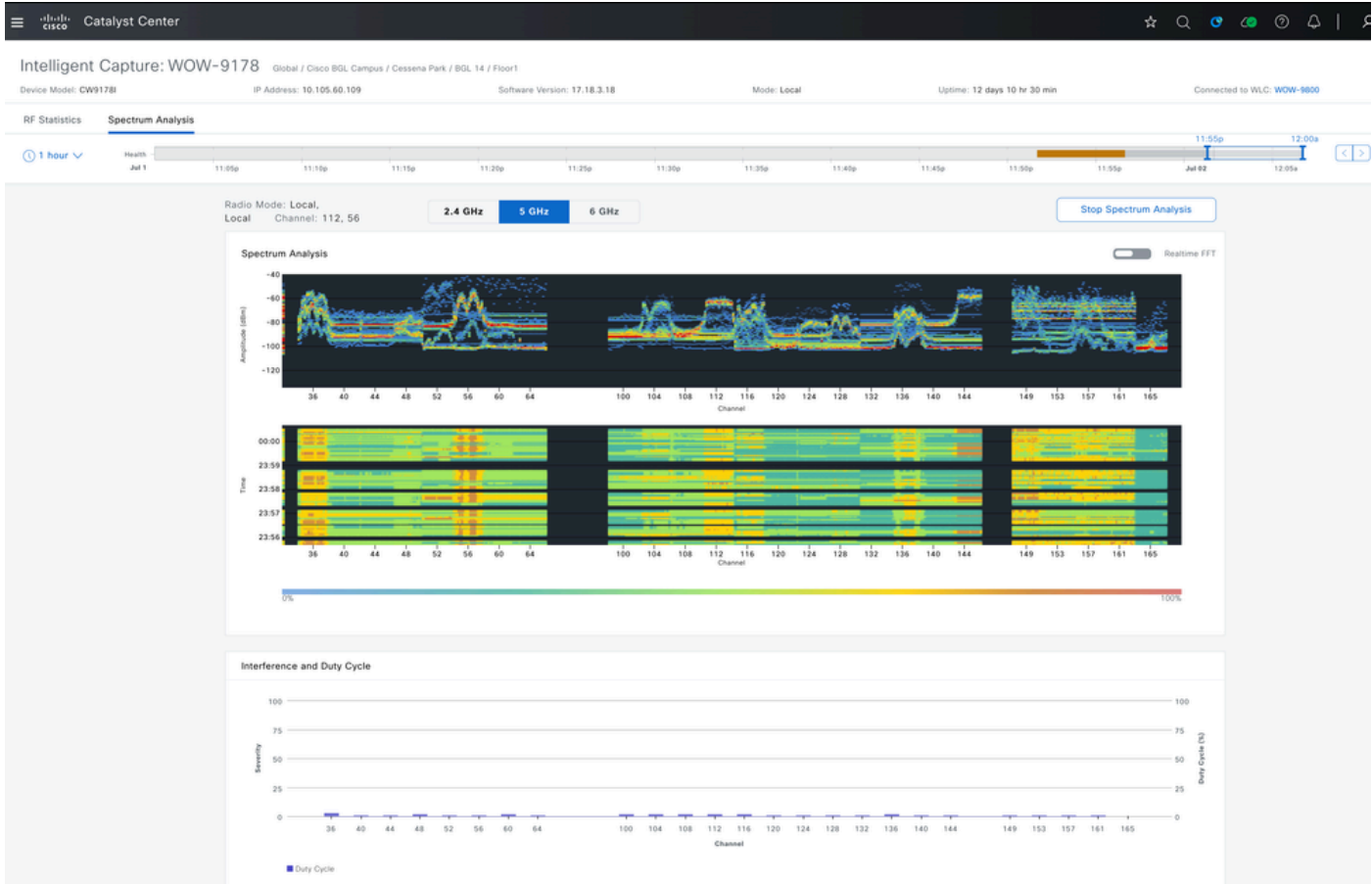
5 Line(s)

```

1 do ap name WOW-9178 leap subscription ap rf spectrum enable
2 do ap name WOW-9178 leap subscription ap rf spectrum slot 5
3 do ap name WOW-9178 leap subscription ap rf spectrum slot 1
4 do ap name WOW-9178 leap subscription ap rf spectrum slot 2
5 do ap name WOW-9178 leap subscription ap rf spectrum slot 3

```

Configuration Applied for Spectrum Analysis

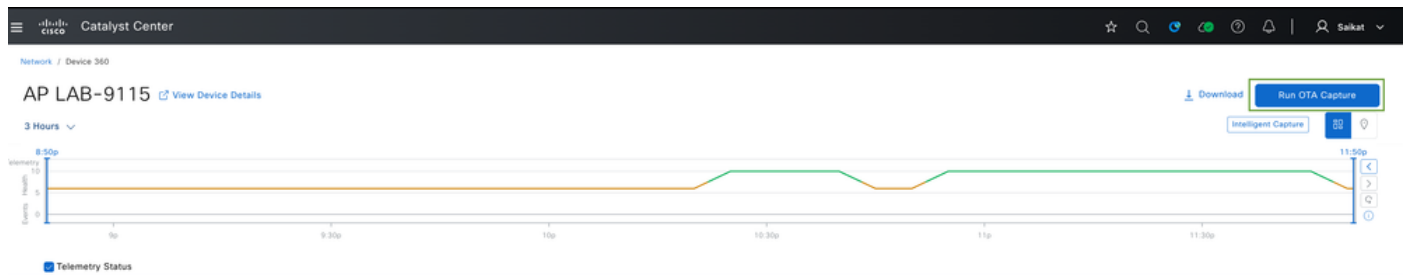


Spectrum Analysis Result

OTA Sniffer Capture

Catalyst Center lets you enable OTA Sniffer Capture on a specific radio, bandwidth, and channel. Once enabled, all Wi-Fi data packets traveling on that radio and channel are captured. You can select up to 2 APs to perform the sniffing. Keep in mind that the 2 APs configured for traffic sniffing can switch to sniffer mode on their respective radio/slot for as long as OTA Capture is enabled.

To enable this, navigate to **Provision > Inventory > Access Points**, click the AP for which you want to collect OTA data, then select **Run OTA Capture**. You can choose up to 2 nearby access points to sniff the traffic.



Run OTA Capture on Target AP

Run OTA Capture




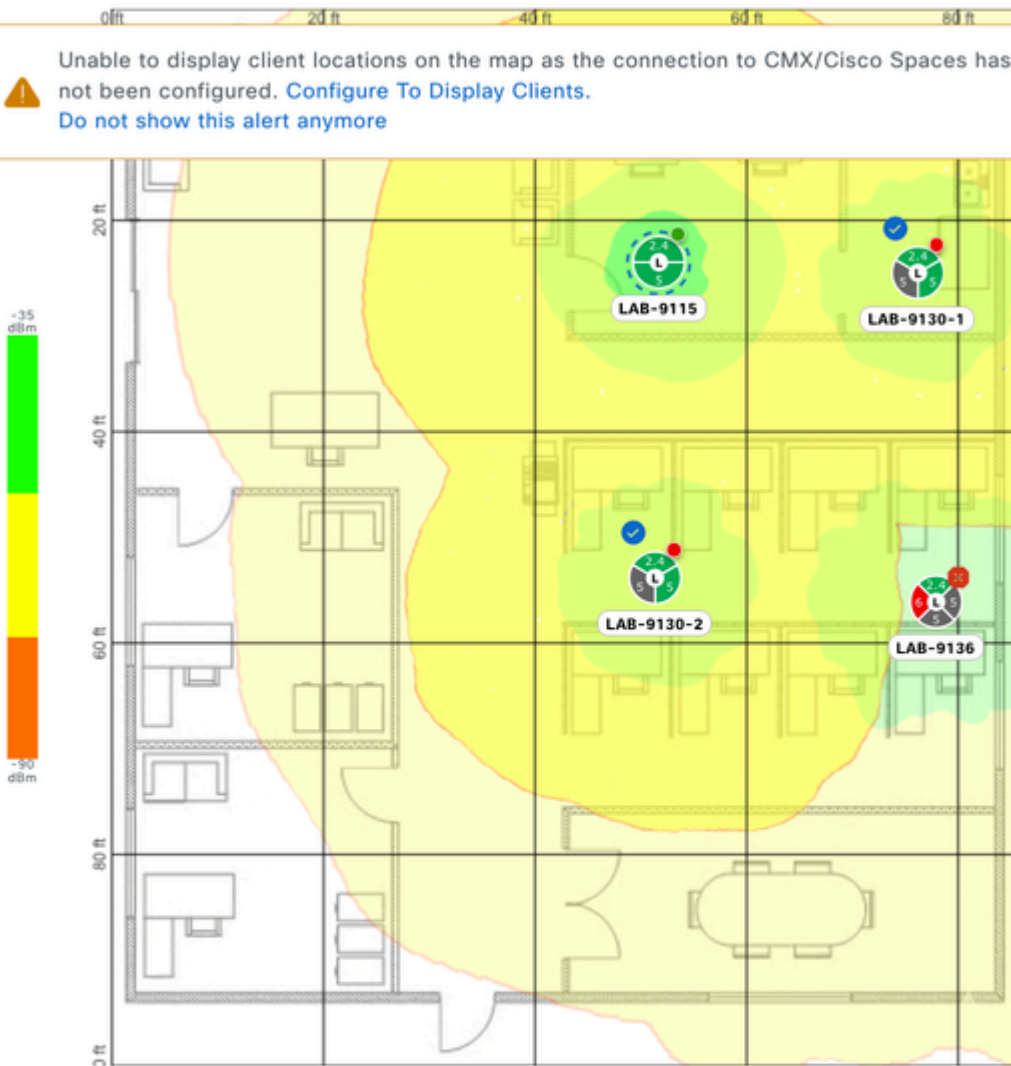
Select Access Points

This is the Over the Air Sniffer, you can select up to 2 access points. These Access Points will promiscuously sniff the environment.



Global/Cisco BGL Campus/Cessena Park/BGL 14 Test-Floor4 ⌵ ⓘ

 Unable to display client locations on the map as the connection to CMX/Cisco Spaces has not been configured. [Configure To Display Clients.](#) ✕
Do not show this alert anymore



LAB-9130-1 ✕

Radios: 0 (2.4 GHz),
1 (5 GHz), 2 (5 GHz)
IP Address:
10.127.197.184
Floor: Test-Floor4
RSSI: -36 dBm
Device 360

LAB-9130-2 ✕

Radios: 0 (2.4 GHz),
1 (5 GHz), 2 (5 GHz)
IP Address:
10.127.197.182
Floor: Test-Floor4
RSSI: -36 dBm
Device 360

Cancel

Next

Selection of Neighbor APs (Upto 2) to Sniff the Traffic

Select OTA Sniffer Band, Radio, Channel Width & Channel

LAB-9130-1

MAC Address: 88:9C:AD:1E:19:40

AP LAB-9130-1 supports capturing packets at the radio level.

Select Band

5  

Select Radio

1 (Client Count: 0) 

Select Channel Width

40 

Select Channel


36 

LAB-9130-2

MAC Address: 88:9C:AD:E7:9F:C0

AP LAB-9130-2 supports capturing packets at the radio level.

Select Band

5  

Select Radio

1 (Client Count: 0) 

Select Channel Width

40 

Select Channel

40 

back

Next

Select Radio, Channel-Width, Channel to Sniff the Traffic

The screenshot shows the Catalyst Center interface for configuring a Wireless LAN Controller (WLC). The top navigation bar includes 'Activities / Tasks', a search icon, and the user name 'Salkat'. The main content area is titled 'Configurations - Side by side view' and shows a comparison between the 'Configuration to be Deployed' and the 'Running Configuration'.

Configuration to be Deployed (12 Line(s))

```
1 do ap name LAB-9130-1 dot11 5ghz slot 1 shutdown
2 do ap name LAB-9130-1 dot11 5ghz slot 1 radio role manual sniffer
3 do ap name LAB-9130-1 no dot11 5ghz slot 1 shutdown
4 do ap name LAB-9130-1 icap subscription client packet-trace sniff
5 do ap name LAB-9130-1 dot11 5ghz slot 1 channel width 40
6 do ap name LAB-9130-1 dot11 5ghz slot 1 sniff 36 127.0.0.1
7 do ap name LAB-9130-2 dot11 5ghz slot 1 shutdown
8 do ap name LAB-9130-2 dot11 5ghz slot 1 radio role manual sniffer
9 do ap name LAB-9130-2 no dot11 5ghz slot 1 shutdown
10 do ap name LAB-9130-2 icap subscription client packet-trace sniff
11 do ap name LAB-9130-2 dot11 5ghz slot 1 channel width 40
12 do ap name LAB-9130-2 dot11 5ghz slot 1 sniff 40 127.0.0.1
```

Running Configuration (2221 Line(s))

```
1 Building configuration...
2
3 Current configuration : 83781 bytes
4
5 ! Last configuration change at 18:07:48 UTC Wed Jul 1 2026 by ad
6
7 version 17.18
8 service timestamps debug datetime msec
9 service timestamps log datetime msec
10 service internal
11 platform qfp utilization monitor load 80
12
13 hostname WLC
14
15 boot-start-marker
16 boot system bootflash:packages.conf
17 boot system bootflash:/packages.conf
18 boot-end-marker
19
20 !
```

Config Preview for Enabling OTA Capture

The screenshot displays the 'Audit Logs' section in Catalyst Center. The left sidebar shows filters for 'SUMMARY', 'Type (2)', 'Status (7)', 'Review Status (1)', and 'Last Updated (3)'. The main area shows a list of tasks with the following details:

- ICAP disable: OTA LAB-9130-1 WLC.podxl.cisco.com**
 - Task: system · ASSURANCE_ICAP
 - Status: Upcoming
 - Start: Jul 2, 2026 12:21 AM
 - Update: Jul 2, 2026 12:06 AM
- Start OTA Capture for AP LAB-9115**
 - Task: salkat · ASSURANCE_ICAP
 - Status: Success
 - Start: Jul 2, 2026 12:05 AM
 - Update: Jul 2, 2026 12:06 AM
 - End: Jul 2, 2026 12:06 AM

Task Scheduled when OTA Capture is Enabled

Cisco Catalyst 9800-80 Wireless Controller

Welcome admin

Search APs and Clients

Feedback

Configuration > Wireless > Access Points

All Access Points

Misconfigured APs

Tag : 0 Country Code : 0 LSC Fallback : 0 URWB : 0 Select an Action

Multiple APs can be configured at once from Bulk AP Provisioning feature

AP Name	AP Model	Slots	Admin Status	Up Time	WLC Association Uptime	IP Address	AP Mode	Power Derate Capable	Operation Status	Configuration Status	Configuration Misc
LAB-9115	C9115AXI-D	2	✓	0 days 9 hrs 54 mins 10 secs	0 days 9 hrs 51 mins 59 secs	10.127.197.180	Local	Yes	Registered	Healthy	No
LAB-9136	C9136I-ROW	4	✓	0 days 9 hrs 54 mins 19 secs	0 days 9 hrs 52 mins 5 secs	10.127.197.151	Local	Yes	Registered	Healthy	No
LAB-9130-1	C9130AXI-D	3	✓	0 days 9 hrs 54 mins 13 secs	0 days 9 hrs 52 mins 31 secs	10.127.197.184	Local	Yes	Registered	Healthy	No
LAB-9130-2	C9130AXI-D	3	✓	0 days 9 hrs 54 mins 13 secs	0 days 9 hrs 52 mins 30 secs	10.127.197.182	Local	Yes	Registered	Healthy	No

1 - 4 of 4 access points

6 GHz Radios

5 GHz Radios

Total 5 GHz radios : 3

Operation Status "Is equal to" Up

AP Name	Slot No	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Radio Role (Radio Mode)	Channel Width	Channel	Punct
LAB-9115	1	✓	✓	Filter-Policy-Tag	Filter-Site-tag	Filter-RF-Tag	Automatic (local)	40 MHz	(140,144)*	N/A
LAB-9130-1	1	✓	✓	Filter-Policy-Tag	Filter-Site-tag	Filter-RF-Tag	Sniffer (sniffer)	40 MHz	N/A (Sniffer)	N/A
LAB-9130-2	1	✓	✓	Filter-Policy-Tag	Filter-Site-tag	Filter-RF-Tag	Sniffer (sniffer)	40 MHz	N/A (Sniffer)	N/A

Slot 1 in Sniffer Mode for the AP Enabled to Sniff the Traffic

To check the status of running OTA capture by navigate to **Assurance > Settings > Intelligent Capture Settings > OTA Sniffer Capture**:

Catalyst Center

Onboarding Packet Capture Full Packet Capture **OTA Sniffer Capture** Access Point

OTA Sniffer Capture

2 In-progress Captures 1 Completed Captures

Search Table

2 Selected Stop Capture

Sniff Target AP	Wireless Controllers	Start Time	End Time	Duration
LAB-9115	WLC.podxl.cisco.com	Jul 2, 2026 12:05 AM	Jul 2, 2026 12:20 AM	15 min
LAB-9115	WLC.podxl.cisco.com	Jul 2, 2026 12:05 AM	Jul 2, 2026 12:20 AM	15 min

Status of OTA Capture



Note: By default, Catalyst Center runs this task for 15 minutes before automatically disabling it, though it can also be stopped manually at any time.

Once the OTA capture is completed, it appears in the **Completed Captures** section, from where you can download the file.

Sniff Target AP	Wireless Controllers	Start Time	End Time	Download	Duration
LAB-9136	WLC.podx1.cisco.com	Jul 1, 2026 06:32 PM	Jul 1, 2026 06:47 PM	↓	15 min
LAB-9115	WLC.podx1.cisco.com	Jul 2, 2026 12:05 AM	Jul 2, 2026 12:20 AM	↓	15 min
LAB-9115	WLC.podx1.cisco.com	Jul 2, 2026 12:05 AM	Jul 2, 2026 12:20 AM	↓	15 min

Completed Capture - OTA Sniffer Capture

Anomaly Detection

This feature allows Cisco APs to detect possible irregularities in the behavior of wireless clients associated with them. It includes:

- Anomaly Detection
- Anomaly Packet Capture
- Anomaly Individual Reports
- Anomaly Summary Reports

To enable AP Anomaly Capture navigate to **Assurance > Settings > Intelligent Capture Settings > Access Point > Anomaly Capture**. From here, you have the flexibility to either:

- Enable it for specific APs (up to 1000), or
- Enable it globally for all APs managed under a particular WLC.

Once enabled, Intelligent Capture automatically collects and presents anomalous behavior for clients associated with those APs, and this data can be viewed on the Client Intelligent Capture page.

Configure Anomaly Capture

Assurance / Settings / Intelligent Capture Settings

Onboarding Packet Capture Full Packet Capture OTA Sniffer Capture **Access Point**

Access Point

AP Stats Capture **Anomaly Capture**

Specific - select specific APs and enable or disable Global - enable or disable capable WLCs

0 APs are individually configured out of an allowed total of 1000.

Find Hierarchy Search Help

- Global
 - Cisco BGL Campus
 - 9800-Site-2
 - CALO
 - Cessena Park
 - Mesh
 - Malaysia
 - UK

Enabled APs (0) **Disabled APs (4)** Not-Ready APs (0)

Search Table

1 Selected **Enable**

Access Point	Device Type	OS Version	Overall Health Score	Client Count	Configuration Status
<input type="checkbox"/> LAB-9130-1	C9130AXI-D	17.18.3.18	1	0	--
<input type="checkbox"/> LAB-9130-2	C9130AXI-D	17.18.3.18	1	0	--
<input type="checkbox"/> LAB-9136	C9136I-ROW	17.18.3.18	6	0	--
<input checked="" type="checkbox"/> LAB-9115	C9115AXI-D	17.18.3.18	10	1	--

Enable Anomaly Capture for Specific AP

Assurance / Settings / Intelligent Capture Settings

Onboarding Packet Capture Full Packet Capture OTA Sniffer Capture **Access Point**

Access Point

AP Stats Capture **Anomaly Capture**

Specific - select specific APs and enable Global - select specific WLCs and enable

WLC.podxl.cisco.com

1 Selected **Enable** **Disable**

Device Name	Configuration Status	IP Address	Model	OS Version	Overall Health	Location
<input checked="" type="checkbox"/> WLC.podxl.cisco.com	Not Configured	10.127.197.194	C9800-80-K9	17.18.3	10	Global/Cisco BGL Campus/Cessena Park/BGL 14

Enable Anomaly Capture Globally for Specific WLC

Activities / Tasks

Task Details / Work Item Details

Search by device name

WLC.podxl.cisco.com

Device IP: 10.127.197.194 Site: Global/Cisco BGL Campus/Ce...

← Back to workflow progress

Configurations - Side by side view

View by Configuration Source · All

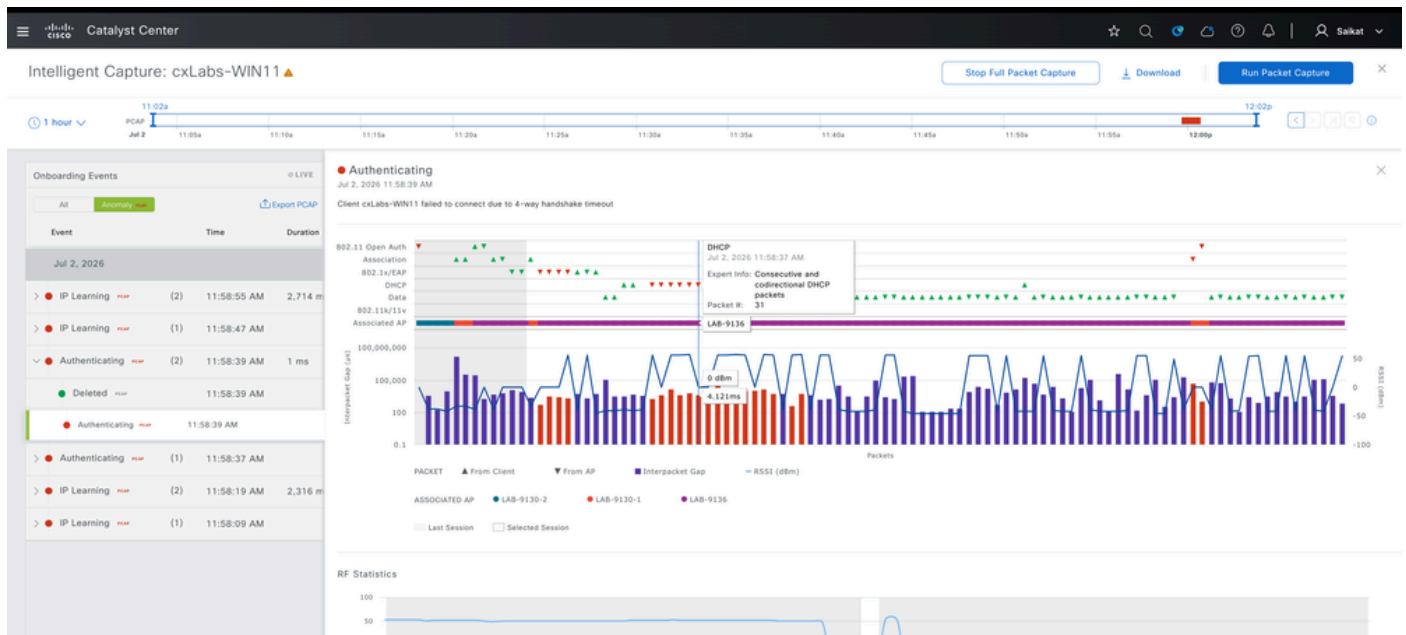
Search configuration

Configuration to be Deployed	Running Configuration
6 Line(s)	2243 Line(s)
<pre> 1 do ap name LAB-9115 icap subscription client anomaly-detection ena 2 do ap name LAB-9115 icap subscription client anomaly-detection reg 3 do ap name LAB-9115 icap subscription client anomaly-detection reg 4 do ap name LAB-9115 icap subscription client anomaly-detection pac 5 do ap name LAB-9115 icap subscription client anomaly-detection reg 6 do ap name LAB-9115 icap subscription client anomaly-detection reg </pre>	<pre> 1 Building configuration... 2 3 Current configuration : 85499 bytes 4 ! 5 ! Last configuration change at 06:16:02 UTC Thu Jul 2 2026 by ad 6 ! 7 version 17.18 8 service timestamps debug datetime msec 9 service timestamps log datetime msec 10 service internal 11 platform qfp utilization monitor load 80 12 ! 13 hostname WLC 14 ! 15 boot-start-marker 16 boot system bootflash:packages.conf 17 boot system bootflash:/packages.conf </pre>

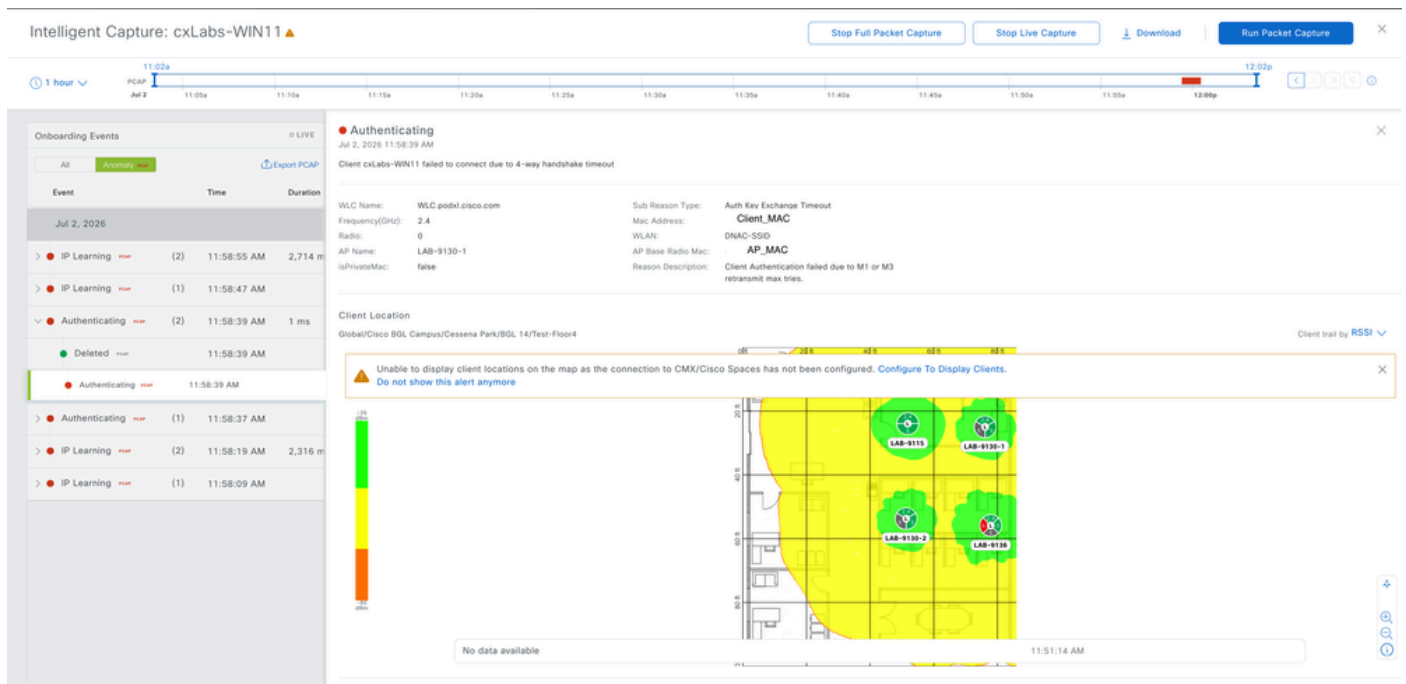
Config Preview for Anomaly Capture

Once enabled, it continuously collect anomaly behaviors for clients associated with the AP, and these can be

viewed within the Intelligent Captures (Onboarding and Full) taken for specific client IDs.



Anomaly Capture View for Client



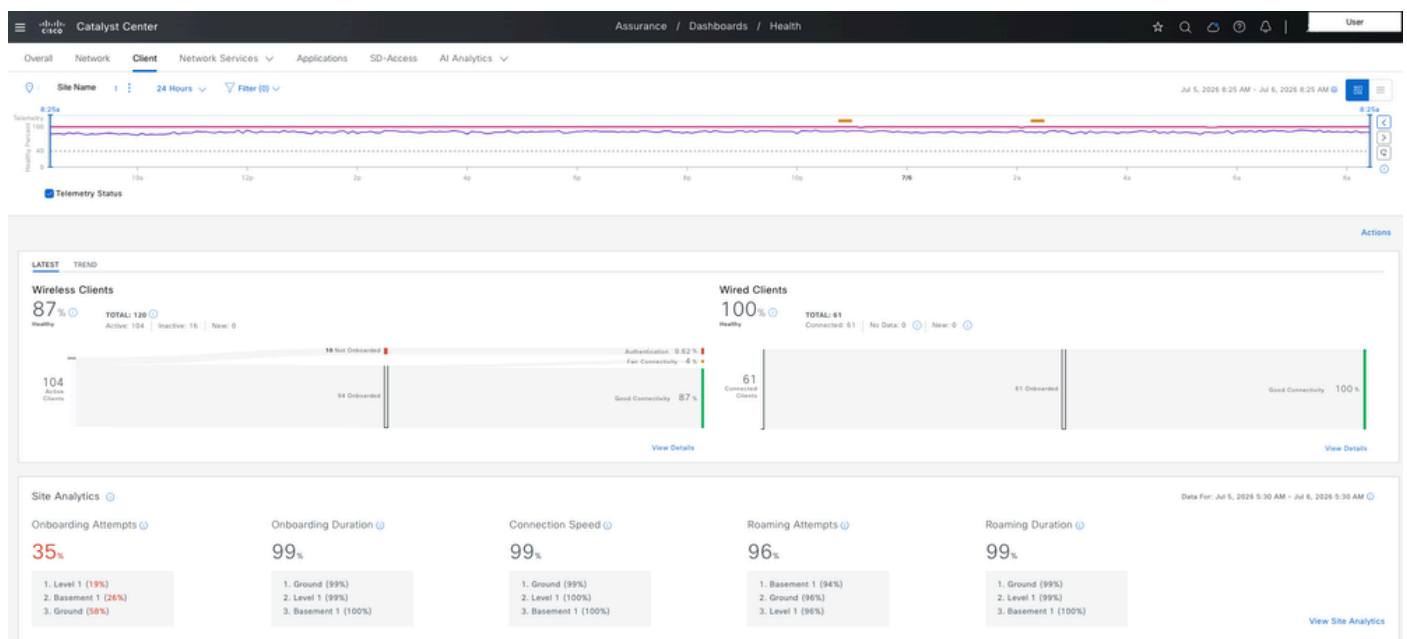
Anomaly Capture Details for Client

With this we can troubleshoot irregular or unexpected client behavior — such as failed onboarding, authentication issues, or abnormal association patterns — by automatically detecting and flagging these events for APs where it is enabled. Combined with onboarding and full packet captures for specific client IDs, it allows administrators to trace the exact sequence of events leading up to an anomaly, making it easier to pinpoint root causes of recurring client connectivity or performance issues without manually monitoring every client session.

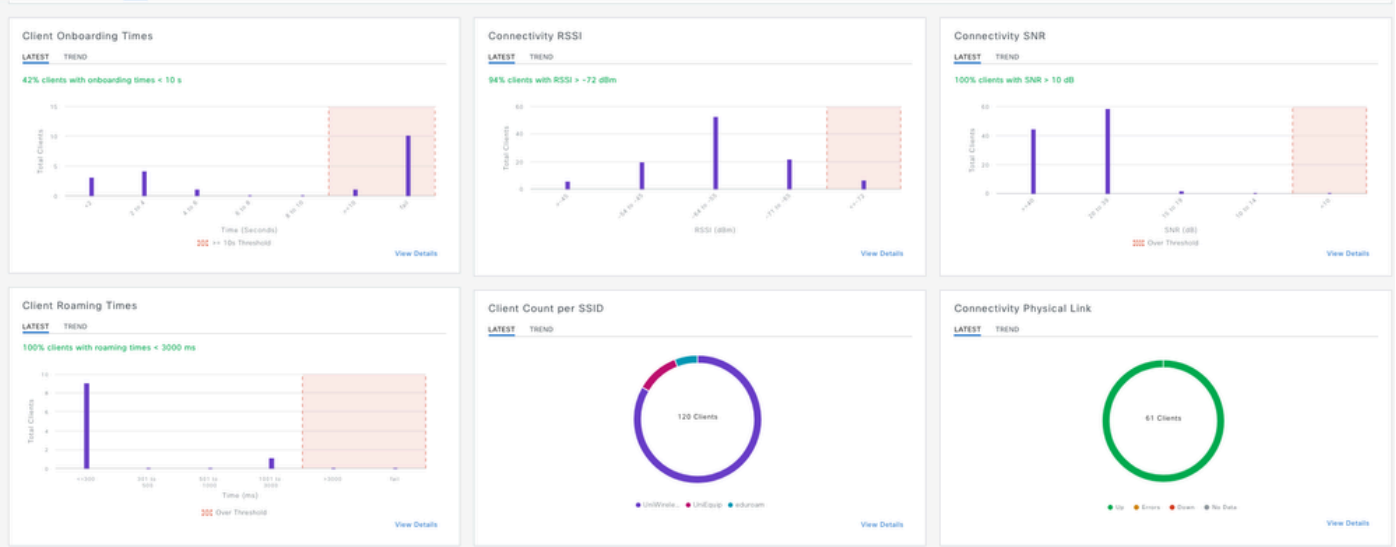
Issue with Wireless Client Connectivity

Wireless client issues — onboarding failures, roaming drops, RF interference, or intermittent connectivity — are often transient and difficult to reproduce, making traditional polling-based monitoring insufficient for troubleshooting. Cisco Catalyst Center addresses this gap through continuous, sub-second telemetry collected directly from access points and wireless controllers, correlated across Device 360, Client 360, and Intelligent Capture workflows. This telemetry-driven architecture enables to reconstruct the exact RF and protocol-level conditions at the time of failure — from channel utilization and interference to 802.11 onboarding frames.

The Client Health section provides a comprehensive, global overview of wireless client statistics across all sites. This includes key metrics such as onboarding performance, RSSI, SNR, roaming activity, per-SSID and per-radio distribution, data rates, and physical connectivity status. You can filter this data by a specific site and view historical trends going back up to the last 30 days, giving you both a network-wide perspective and site-level granularity. Navigate to **Assurance > Dashboard > Health > Client**



Wireless Client Statistics on Catalyst Center



Wireless Client Statistics on Catalyst Center

Client Devices (120)

LATEST TREND

TYPE: **Wireless** | Wired | OVERALL HEALTH: **All** | Poor | Fair | Good | Inactive | No Data

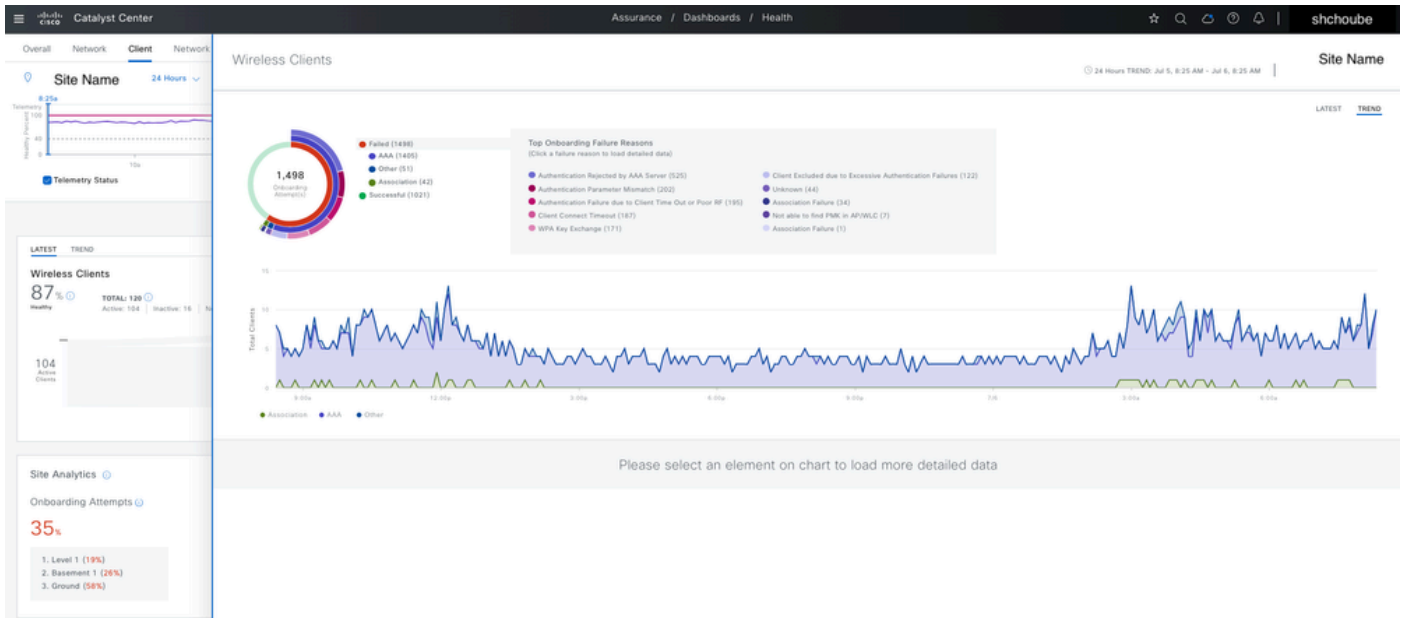
DATA: Onboarding Time >= 10s | Association >= 5s | DHCP >= 5s | Authentication >= 5s | RSSI <= -72 dBm | SNR <= 9 dB

Search by name, MAC address, or IPv4/IPv6 address

Identifier	MAC Address	IPv4 Address	Device Type	Tracked	AP Name	WLC Name	Connection Status	Band	RSSI	Last Seen	Auth Type	Roaming Time	Capability
			Murata-Manufacturing-Device	No			CONNECTED	5 GHz	-63 dBm	Jul 6, 8:21 AM	WPA2/WPA3+802.1x/802.1x-SHA256	7.695 s	11ac
			Murata-Manufacturing-Device	No			CONNECTED	5 GHz	-66 dBm	Jul 6, 8:21 AM	WPA2/WPA3+802.1x/802.1x-SHA256	7.116 s	11ac
			UNKNOWN	No			CONNECTED	2.4 GHz	-78 dBm	Jul 6, 8:23 AM	WPA2/WPA3+802.1x/802.1x-SHA256	5.263 s	Wi-Fi 6
			MacBook Pro (13-inch, M2, 2022)	No			CONNECTED	2.4 GHz	-69 dBm	Jul 6, 8:21 AM	WPA2/WPA3+802.1x/802.1x-SHA256	4.144 s	Wi-Fi 6
			Murata-Manufacturing-Device	No			CONNECTED	2.4 GHz	-68 dBm	Jul 6, 8:22 AM	WPA2/WPA3+802.1x/802.1x-SHA256	3.166 s	11n
			UNKNOWN	No			CONNECTED	2.4 GHz	--	Jul 6, 8:25 AM	WPA2/WPA3+802.1x/802.1x-SHA256	2.666 s	Unclassified
			Apple-iPhone	No			CONNECTED	5 GHz	-50 dBm	Jul 6, 8:24 AM	WPA2/WPA3+802.1x/802.1x-SHA256	2.389 s	Wi-Fi 6E
			Murata-Manufacturing-Device	No			CONNECTED	5 GHz	-74 dBm	Jul 6, 8:21 AM	WPA2/WPA3+802.1x/802.1x-SHA256	1.142 s	11ac
			Murata-Manufacturing-Device	No			CONNECTED	5 GHz	-51 dBm	Jul 6, 8:23 AM	WPA2/WPA3+802.1x/802.1x-SHA256	1.122 s	11ac
			Apple-iPhone	No			CONNECTED	5 GHz	-51 dBm	Jul 6, 8:21 AM	WPA2/WPA3+802.1x/802.1x-SHA256	1.028 s	Wi-Fi 6
			UNKNOWN	No			CONNECTED	2.4 GHz	--	Jul 6, 8:21 AM	WPA2/WPA3+802.1x/802.1x-SHA256	0.754 s	Wi-Fi 6
			Un-Classified Device	No			CONNECTED	5 GHz	-57 dBm	Jul 6, 8:25 AM	WPA2+802.1x	0.753 s	Wi-Fi 6E

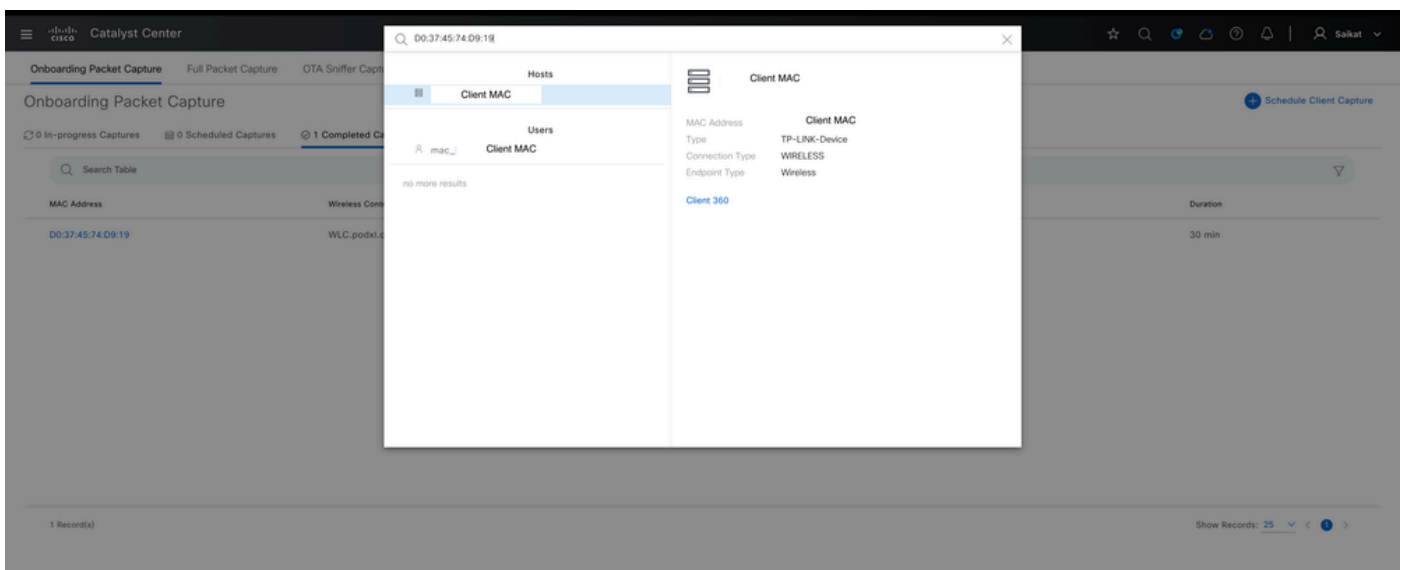
120 Record(s) | Show Records: 50 | 1 - 50 | < 2 3 >

Wireless Client Statistics on Catalyst Center

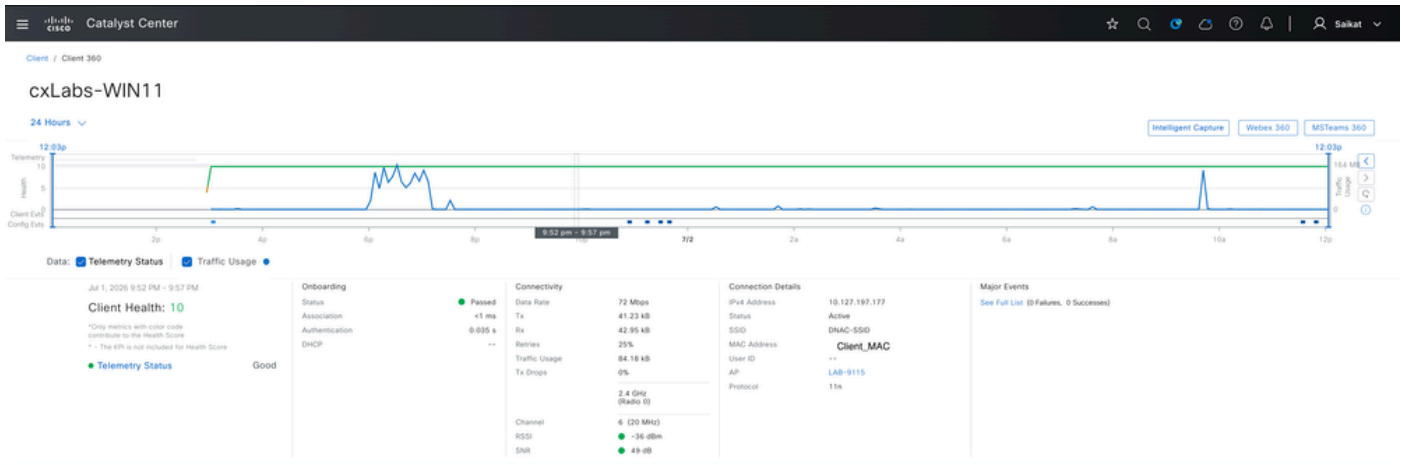


Wireless Client Statistics on Catalyst Center

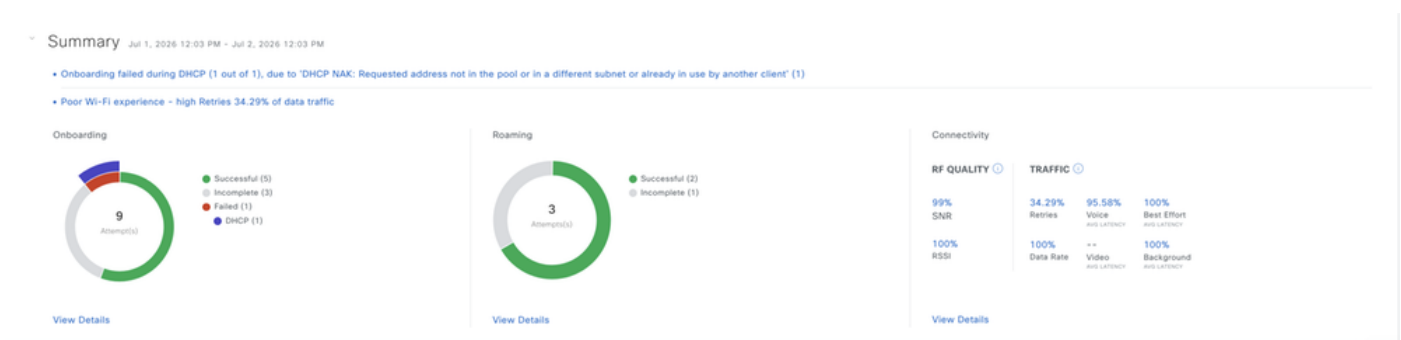
For troubleshooting a specific client, you can search using the clients MAC address, which takes you to the Client 360 view. This page presents detailed, client-specific statistics — including onboarding history, connectivity events, RF metrics, and session details — scoped exclusively to that individual client, allowing for precise root cause analysis of individual client issues.



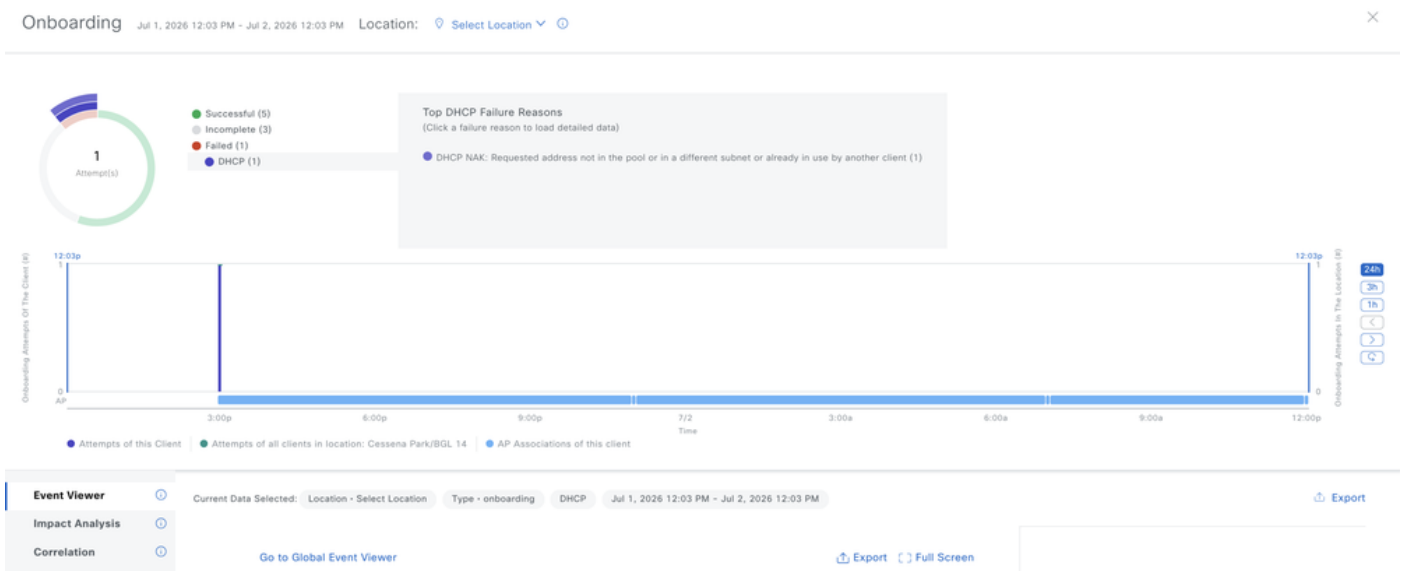
Specific Client Mac Address Device 360



Telemetry + Health Status of Client



Overall Summary for Client



Event Reported for Client in Detail

Detail Information Jul 2, 2026 12:03 PM

Device Info Connectivity RF

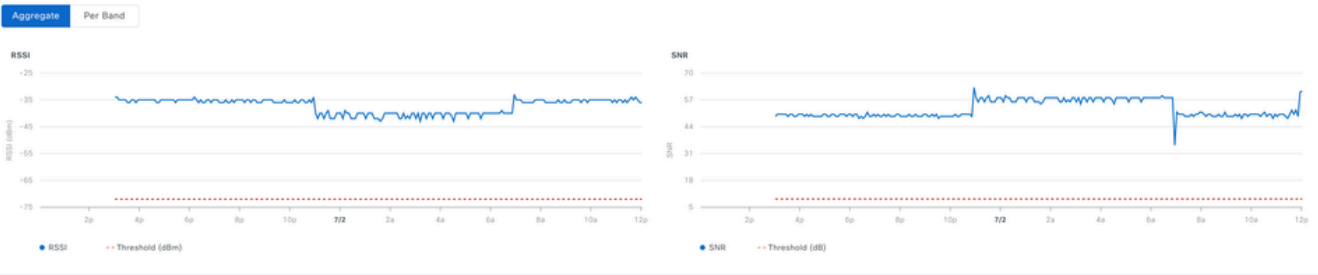
Information		Connection Information	
Device Type	TP-LINK-Device	WMM	--
Operating System	--	U-APSD	--
User ID	--	Band	
Host Name	cxLabs-WN11	Radio	
MAC Address		Spatial Streams	
IPv4 Address	10.127.197.177	Channel	
IPv6 Address	fe80::85d:3e54:8b7b:7bc6 (1 more)		
Status	Disconnected		
Hardware Manufacturer	--		
Endpoint Type	--		
VLAN ID	97		
Association Protocol	11n		
Protocol Capability	11n		
L3 Virtual Network	--		
L2 Virtual Network	--		
Tracked	No		
Exclusion	No		
Bridge-Network Virtual Network	NA		

⚠ You haven't subscribed to the client notification yet. [Set up Subscription](#) X

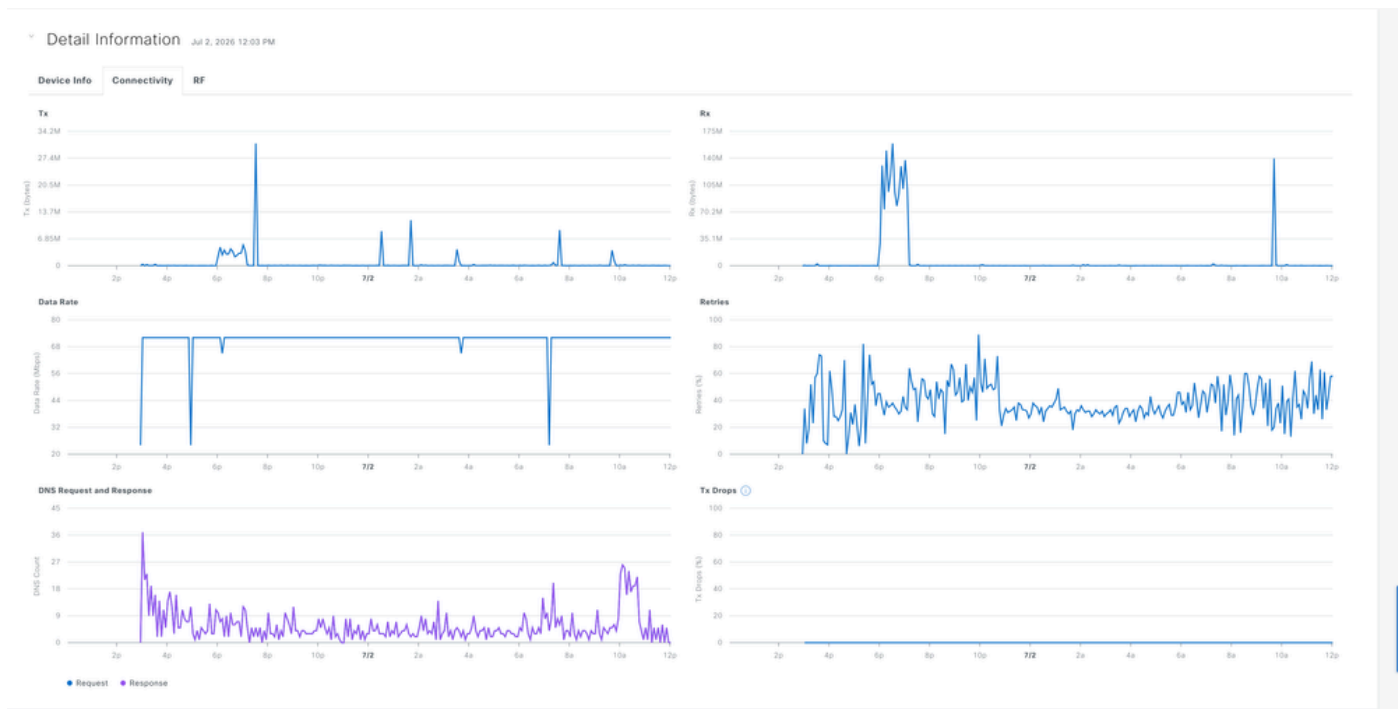
Client Device Details

Detail Information Jul 2, 2026 12:03 PM

Device Info Connectivity RF



RF Statistics for Client



Connectivity Statistics for Client

Intelligent Captures for Wireless Clients

Intelligent Capture (iCAP) helps troubleshoot wireless client connectivity issues by capturing real packet-level data directly from Catalyst Center. It can capture 802.11 management, DHCP, and EAP frames to pinpoint where a connection attempt fails, unencrypted data and management packets for a specific client to troubleshoot onboarding, accessibility and application issues. You can also schedule intelligent captures to run at a later time as per the requirement. The default duration of the session is 30 minutes and can be set up to eight hours.

Onboarding Packet Capture

Onboarding Packet Capture records the sequence of packets a client device exchanges while attempting to join the wireless network, including 802.11 management frames (such as association and authentication requests), DHCP packets, and EAP packets used during 802.1X authentication. Alongside this, it collects the clients RF statistics giving visibility into signal conditions at the exact moment of onboarding. These captures are useful for troubleshooting a scenario when a client fails to connect and helps to pinpoint the precise stage — whether during association, authentication, or IP address assignment — where the failure occurs. By default, Onboarding Packet Capture is enabled on the last client-connected wireless controller. You can select up to three wireless controllers to cover the client roaming scenario.

To enable **Onboarding Packet capture** navigate to **Assurance > Settings > Intelligent Capture Settings > Onboarding Capture > Schedule Client Capture (on the Top Right Corner) > Search for Client Identifier (Mac address)**

The screenshot shows the 'Intelligent Capture Settings' page in Catalyst Center. The left panel, 'Onboarding Packet Capture', shows 0 In-progress Captures, 0 Scheduled Captures, and 0 Completed Captures. The right panel, 'Schedule Client Capture', shows a table of wireless controllers with columns for Device Name, IP Address, MAC Address, and Reachability. The controller 'WLC.podxl.cisco.com' is selected.

Device Name	IP Address	MAC Address	Reachability
WLC-Saikat	10.105.60.89		Reachable
itsmewlc	10.105.193.79		Reachable
WLC.podxl.cisco.com	10.127.197.194	WLC_MAC_Address	Reachable
wlc3504-saikat	10.105.60.87		Reachable
WOW-9800	10.105.60.100		Reachable

The screenshot shows the 'Onboarding Packet Capture' panel with 1 In-progress Capture, 0 Scheduled Captures, and 0 Completed Captures. A table shows a single record for 'Client-MAC' on 'WLC.podxl.cisco.com' with a duration of 30 min and a status of 'Success'.

MAC Address	Wireless Controller	Start Time	End Time	Configuration Status	Duration
Client-MAC	WLC.podxl.cisco.com	Jul 2, 2026 11:32 AM	Jul 2, 2026 12:02 PM	Success	30 min

Scheduled Onboarding Capture

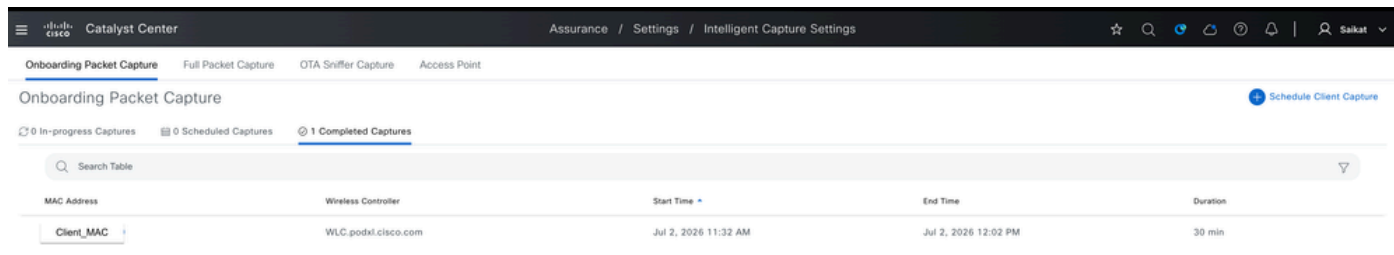
The screenshot shows the 'Start Live Capture for D0:37:45:74:D9:19' dialog box. It includes a 'Work Item' for 'ASSURANCE_ICAP' and a 'Completed' status. The start and end times are both 'Jul 1, 2026 6:12 PM'. The device IP is '10.127.197.194' and the site is 'Global/Cisco BGL Campus/Ce...'. The dialog shows a side-by-side view of configurations for 'WLC.podxl.cisco.com'.

Configuration to be Deployed	Running Configuration
10 Line(s)	2221 Line(s)
<pre> 1 ap profile "default-ap-profile" 2 icap subscription client packet-trace partial enable 3 icap subscription client packet-trace partial filter protocol type 4 icap subscription client packet-trace partial filter protocol type 5 icap subscription client packet-trace partial filter protocol all 6 icap subscription client statistics filter enable 7 icap subscription client statistics filter frequency 5 8 icap subscription client packet-trace partial filter client d0:37:45:74:d9:19 9 icap subscription client statistics filter d0:37:45:74:d9:19 10 exit </pre>	<pre> 1 Building configuration... 2 3 Current configuration : 83781 bytes 4 5 Last configuration change at 18:50:08 UTC Wed Jul 1 2026 by ad 6 7 version 17.18 8 service timestamps debug datetime msec 9 service timestamps log datetime msec 10 service internal 11 platform qfp utilization monitor load 80 12 13 hostname WLC 14 15 boot-start-marker 16 boot system bootflash:packages.conf 17 boot system bootflash:/packages.conf 18 boot-end-marker 19 20 </pre>

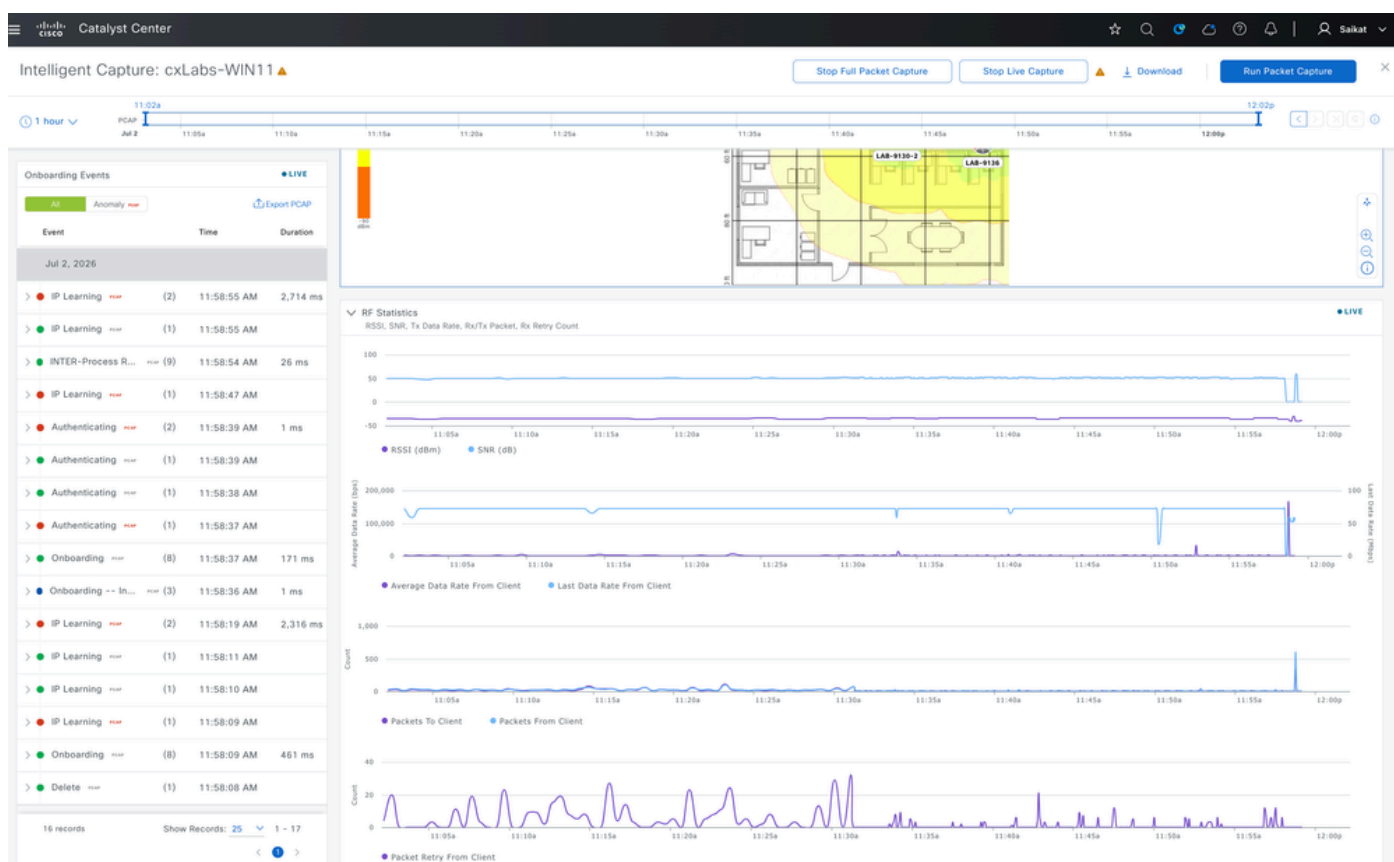
Config Preview for Onboarding Capture

The onboarding capture can either be stopped manually or automatically disabled once the scheduled

duration (ranging from 30 minutes to 8 hours) elapses. Once stopped, the capture appears under Completed Captures, where you can click the clients MAC address to view the detailed capture data, and export the file in PCAP format for further analysis.



Completed Onboarding Capture

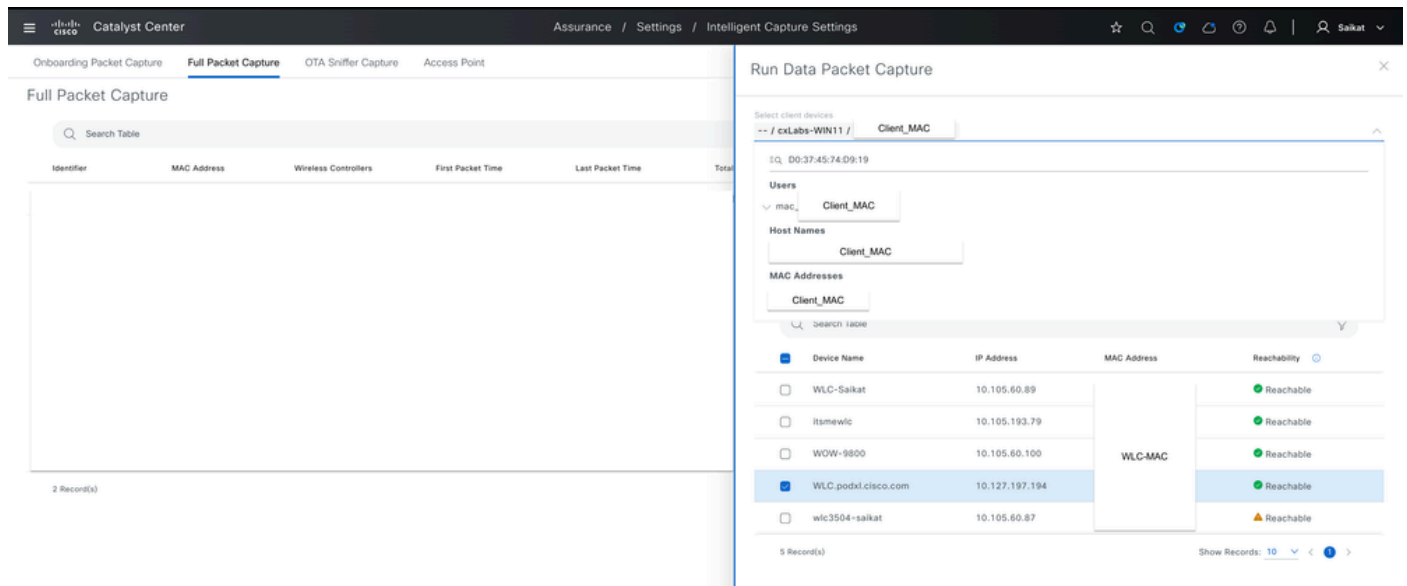


Example of Complete Onboarding Capture

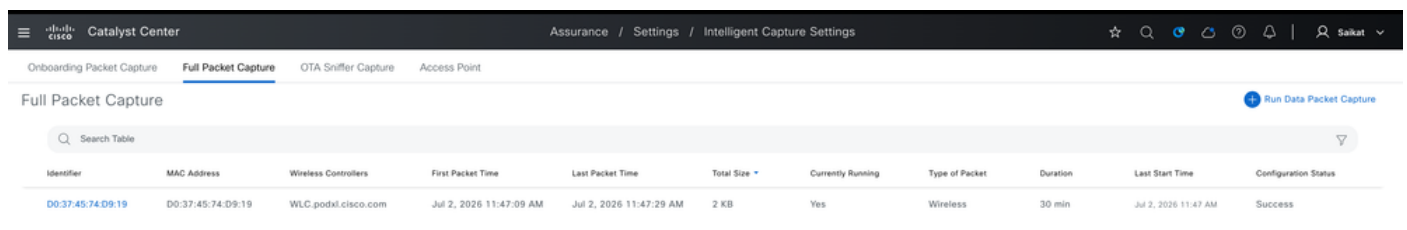
Full Packet Capture

Full Packet Capture session can capture complete data for a specific client, providing deep, packet-level visibility into that clients ongoing wireless traffic which allows us to inspect both data and management packets in detail to troubleshoot access issues, application performance problems, or other connectivity anomalies that go beyond what standard RF statistics can reveal. It can capture up to 1 GB of rolling data for a specific client and continuously retains the most recent data up to the limit.

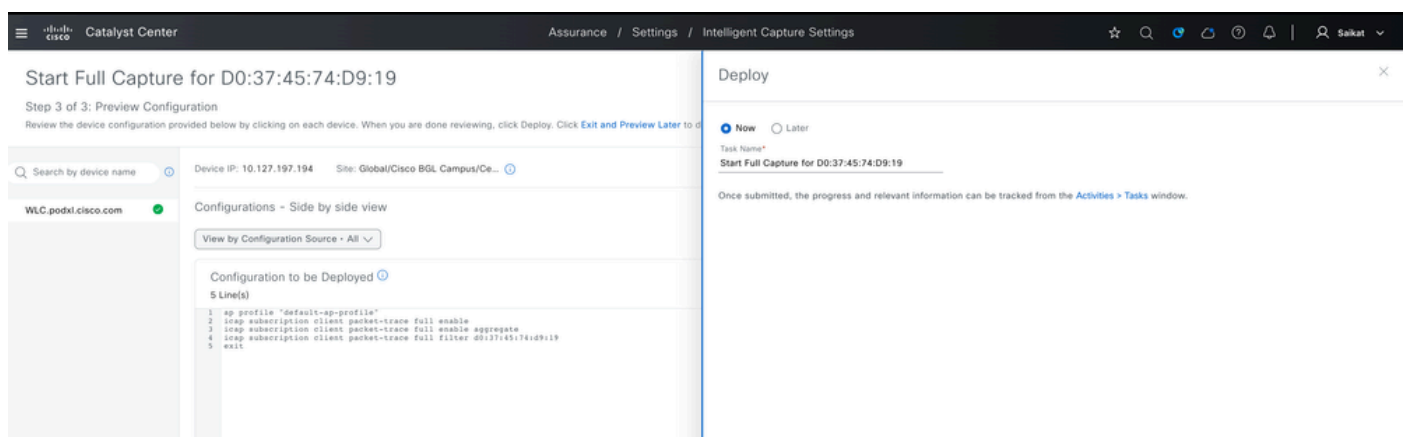
To enable **Full Packet Capture** navigate to **Assurance > Settings > Intelligent Capture Settings > Onboarding Capture > Run Data Capture (on the Top Right Corner) > Search for Client Identifier (Mac address)**:



Full Packet Capture for Client



Scheduled Full Packet Capture for Client



Config Preview for Full Packet Capture

The full Packet capture can either be stopped manually or automatically disabled once the scheduled duration (ranging from 30 minutes to 8 hours) elapses. Once stopped, the capture appears under completed captures, where you can click the clients MAC address to view the detailed capture data, and export the file in PCAP format for further analysis.

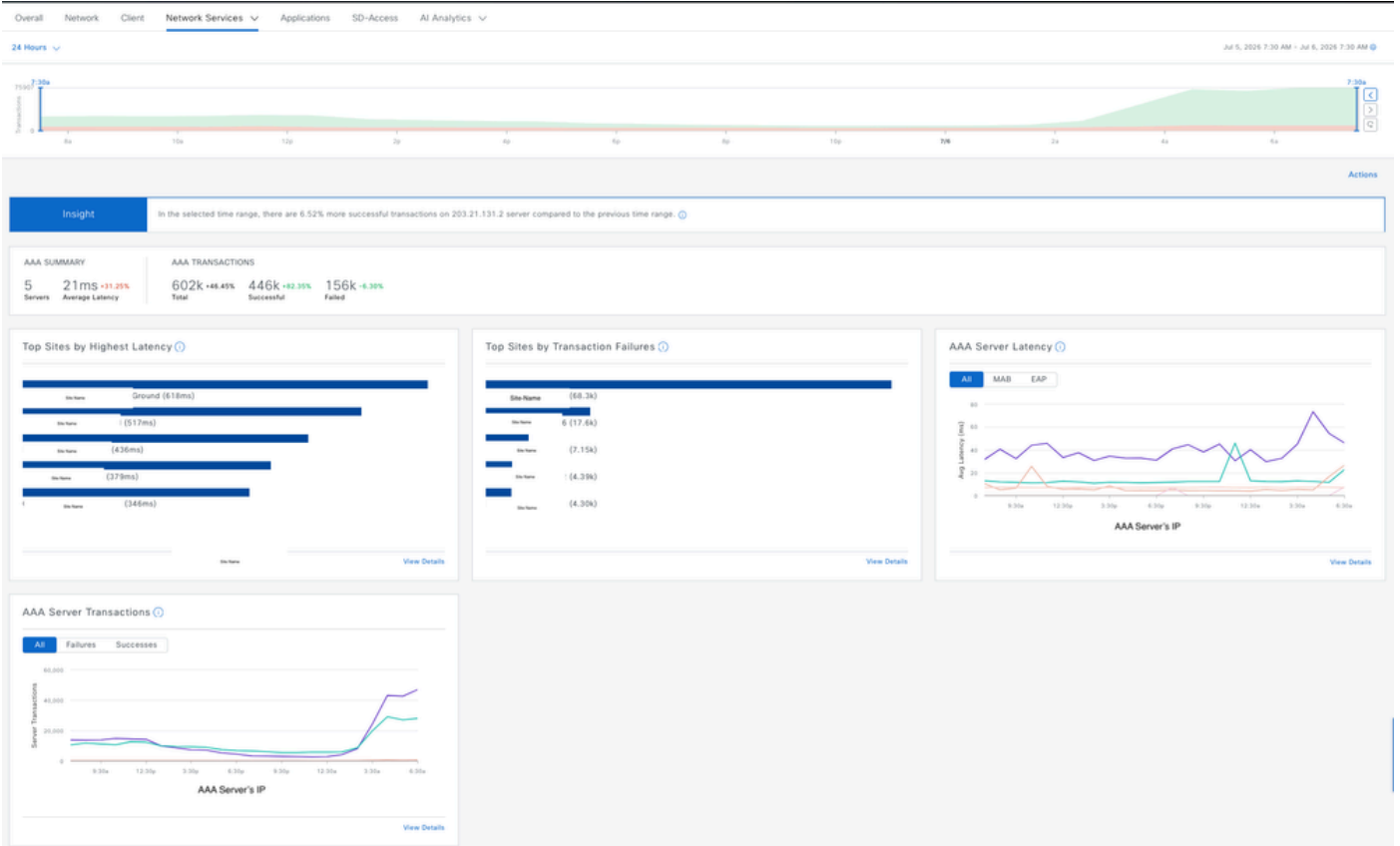


Example of Full Capture Collected for Client

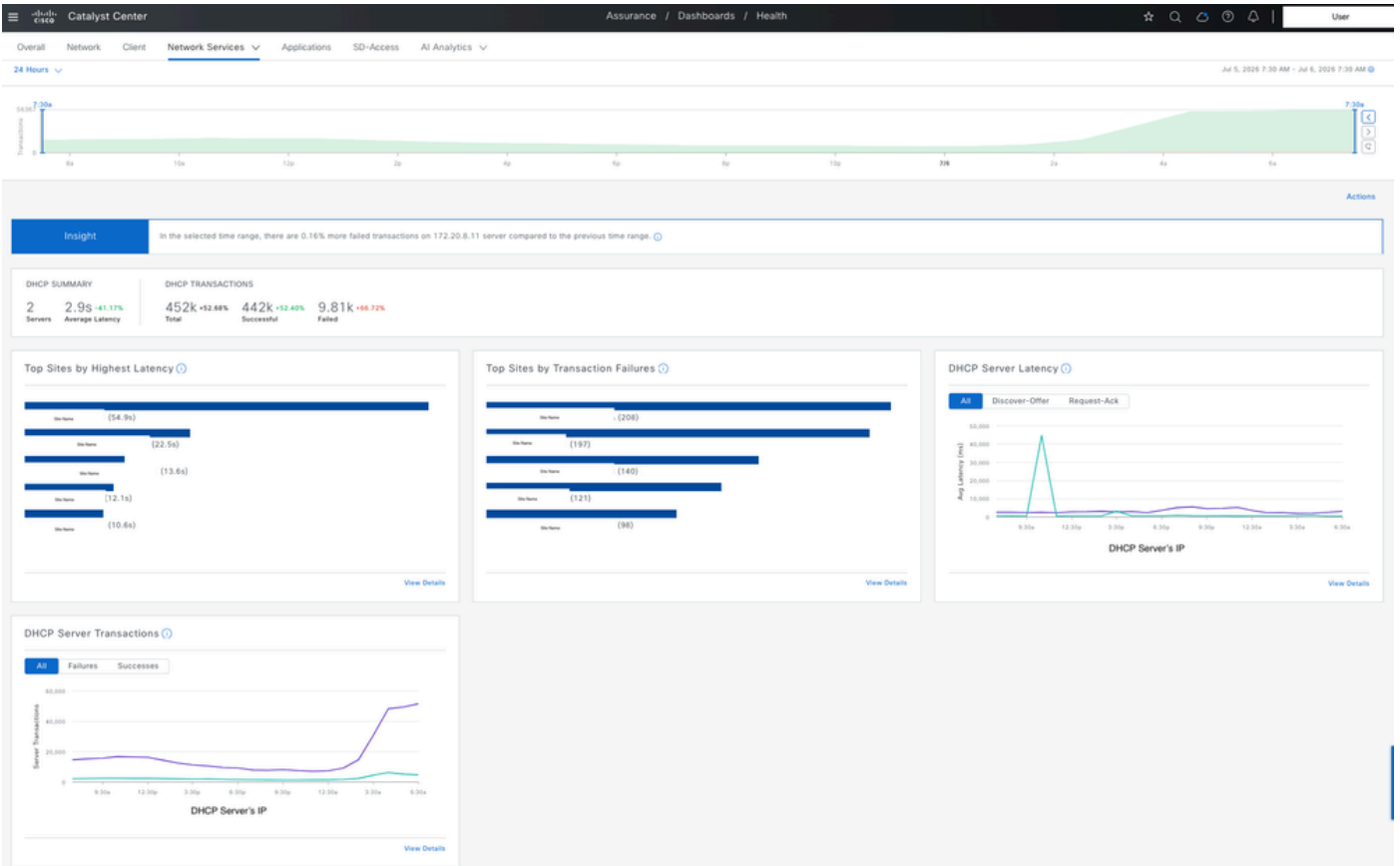
Isolate Network Service Issues (AAA, DHCP, DNS)

If the reported symptom points to a specific network service rather than the controller itself — for example, clients failing authentication, not receiving an IP address, or failing name resolution — Catalyst Center Network Services dashboard under Assurance gives you visibility into those transactions as reported by the WLC.

Navigate to **Assurance > Dashboard > Health > Network services > AAA/DHCP/DNS:**



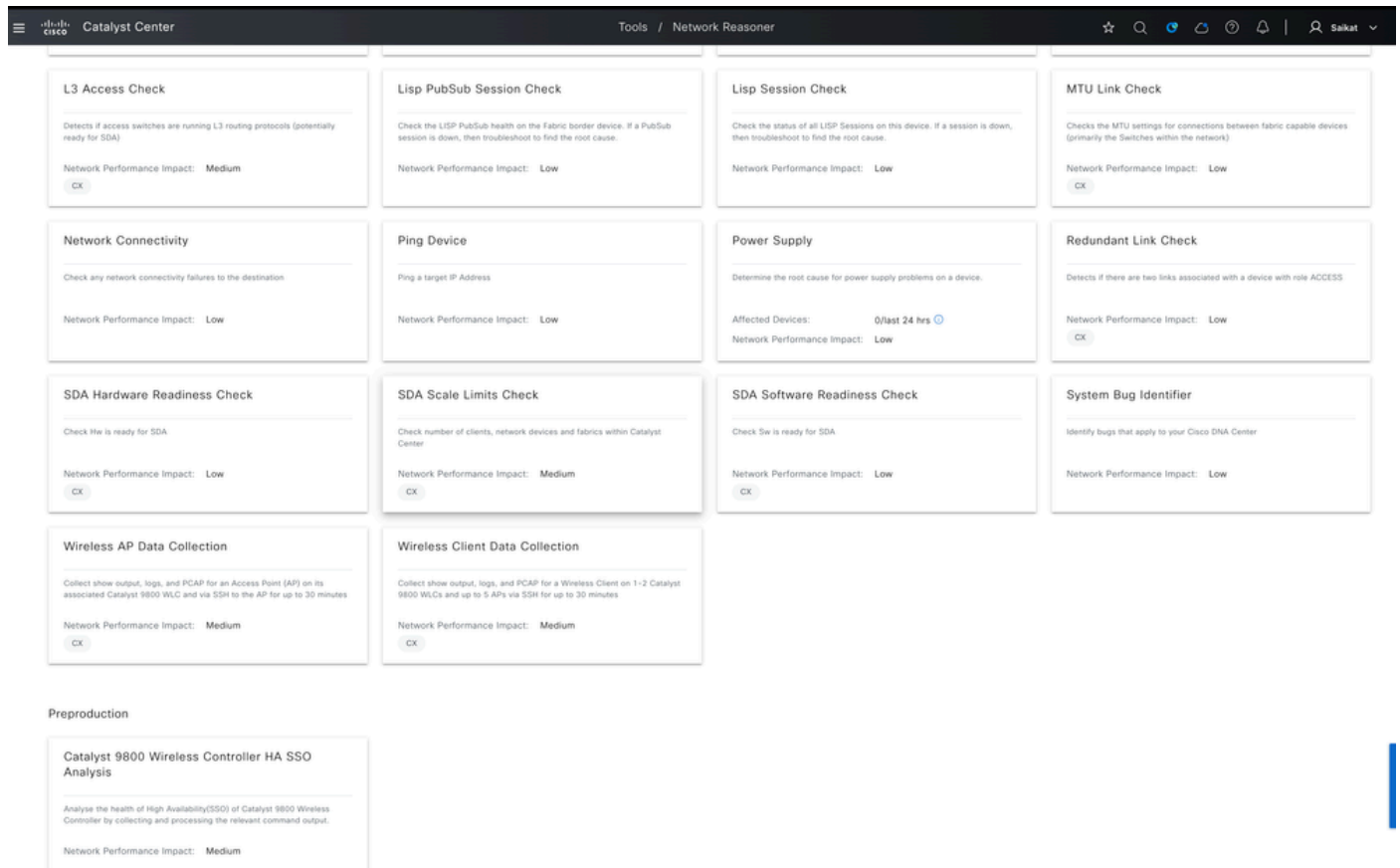
Wireless Client AAA Statistics on Catalyst Center



Wireless Client DHCP Statistics on Catalyst Center

Network Reasoner

Network Reasoner is a built-in tool in Catalyst Center that automatically investigates network problems for you — you do not have to dig through logs manually. You can find it under **Tools > Network Reasoner**. Each troubleshooting option (called a workflow) shows you a short description, how many devices were affected in the last 24 hours, and what happens if you run it. It can only detect issues on devices that are either added to Catalyst Center for Assurance monitoring or provisioned through Catalyst Center.



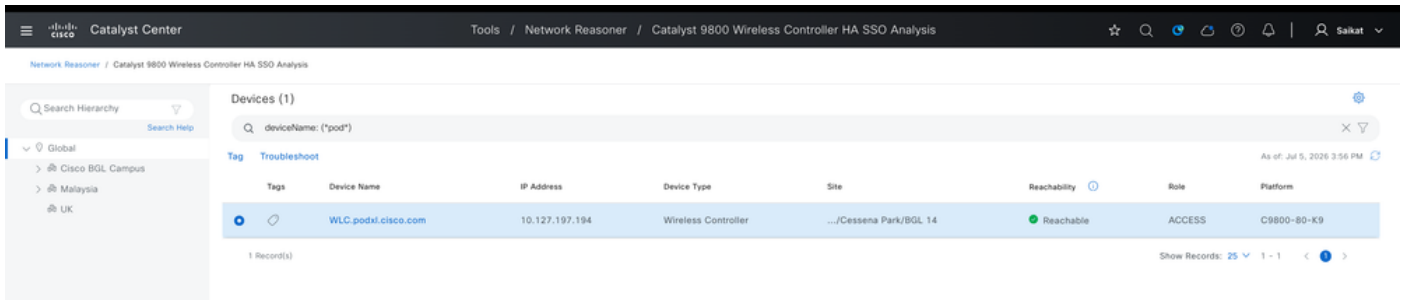
Various Network Troubleshooting Options Available on Network Reasoner

For wireless networks, there are three main things you can troubleshoot:

1. For controller problems — especially with High Availability (HA) setups — Network Reasoner checks things like:

- Is the controller reachable?
- Is HA set up correctly?
- Are the active and standby controllers in sync?
- Is the connection between them working?

If it finds an issue, it tells you exactly what is wrong and suggests how to fix it. There is also a separate option for troubleshooting devices that are not sending any monitoring data at all.

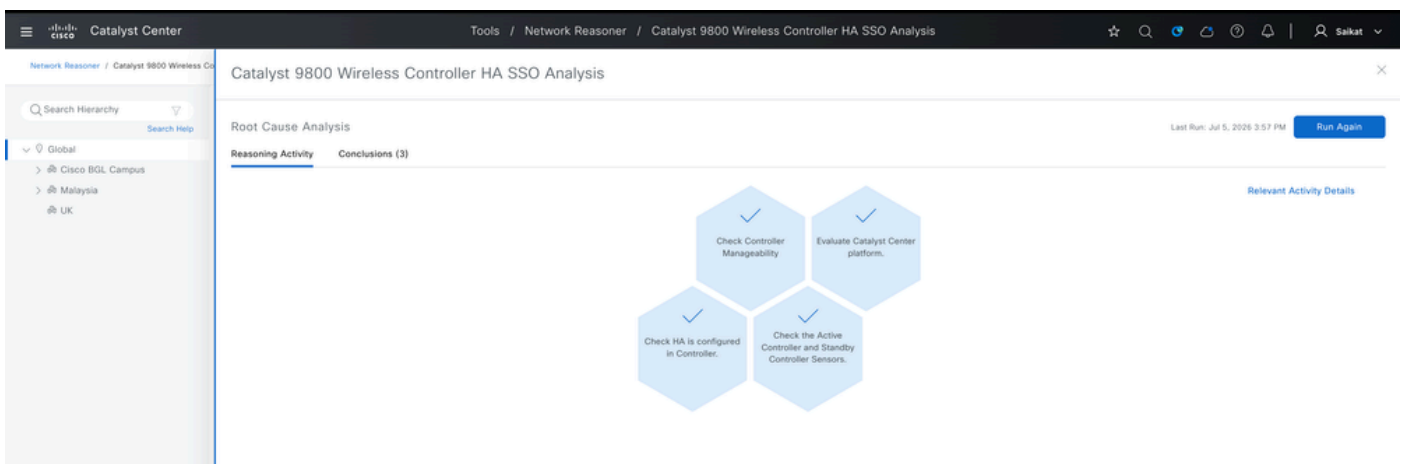


Troubleshooting HA using Network Reasoner

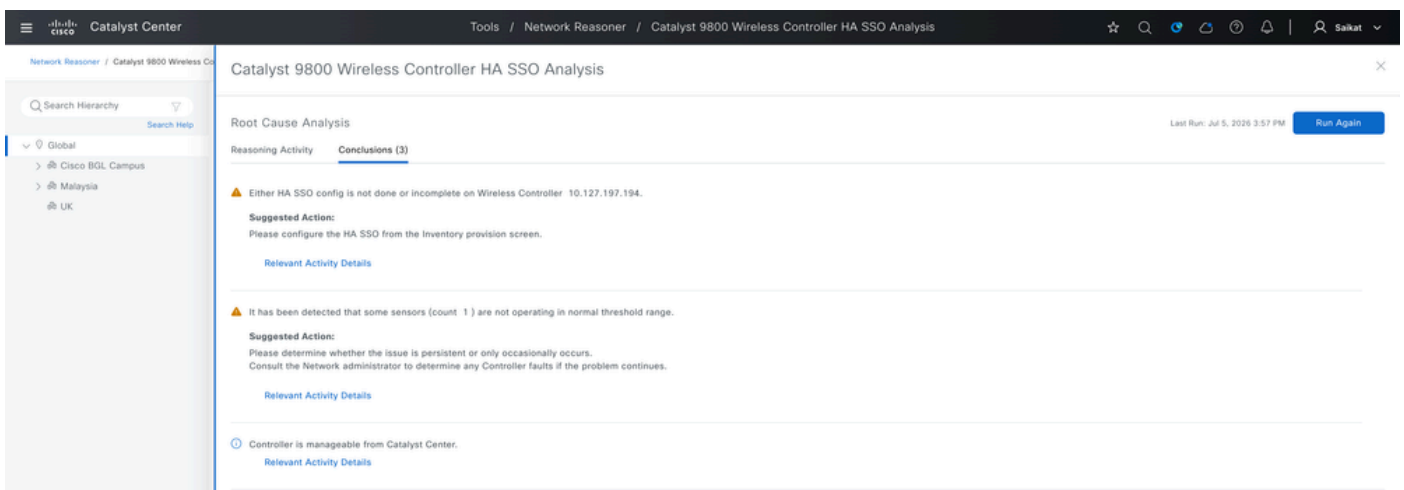
When you enable the troubleshoot feature for HA SSO analysis on the 9800 WLC using Network Reasoner, it performs several checks and provides a conclusion based on the results. If any issues are found with HA SSO, it also suggests corrective actions to resolve them.

!! Task Workflow !!

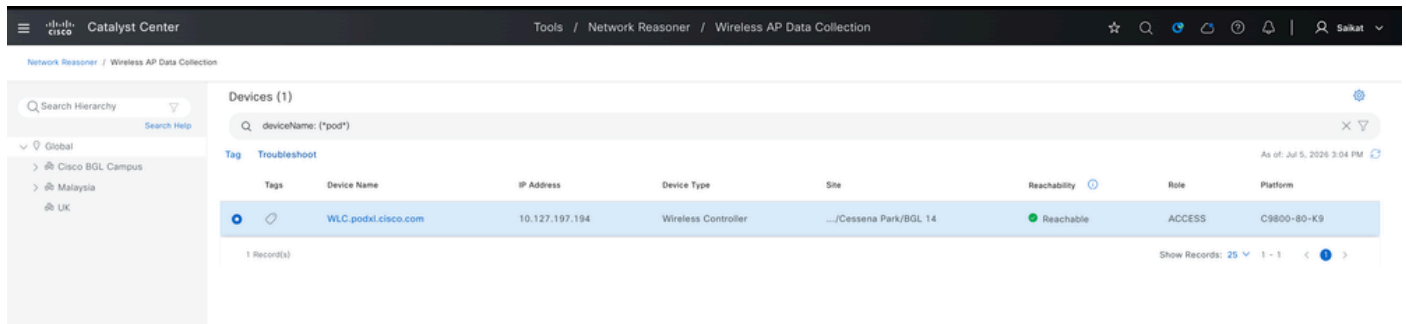
- Check Controller Manageability
- Evaluate Catalyst Center platform.
- Check HA is configured in Controller.
- Check the Active Controller and Standby Controller Sensors.



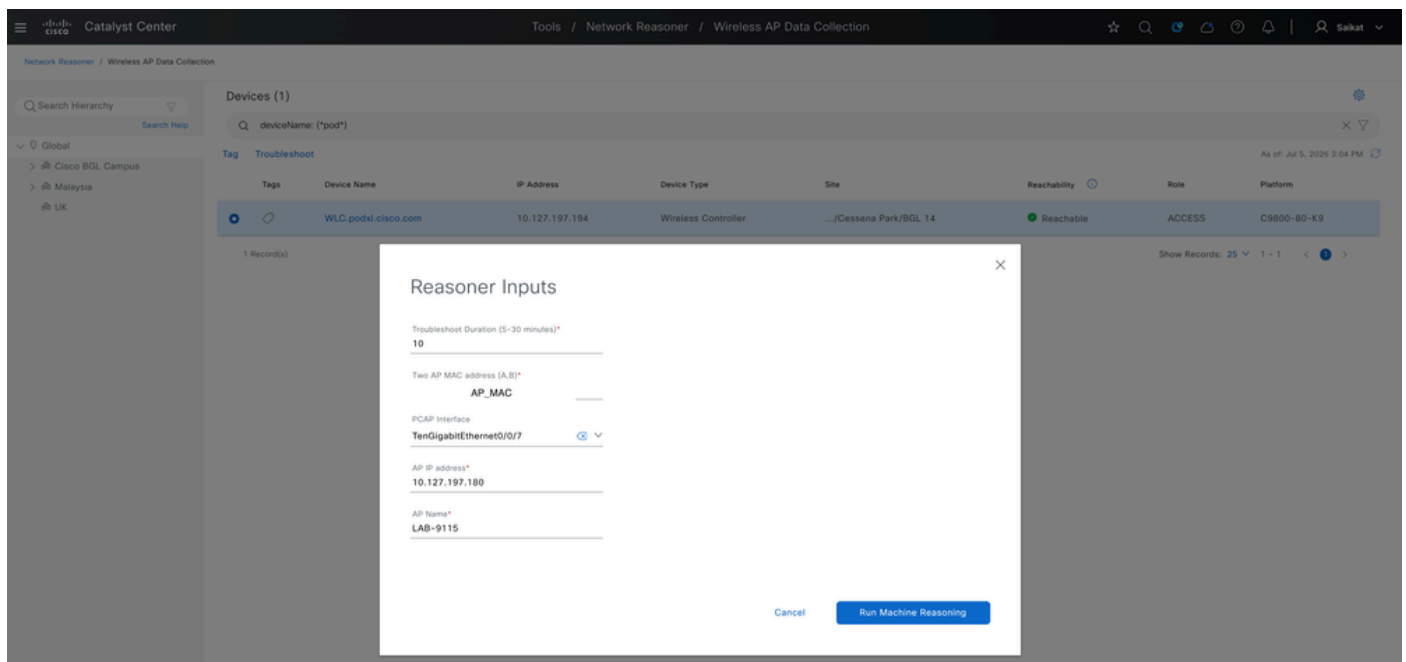
Tasks Performed by CATC for HA SSO Analysis



2. Access Points - If an AP is experiencing issues, select the controller that manages it, then enter the APs MAC address, set the duration for the check to run. It enables logs and packet capture from the WLC and AP, for deeper visibility. Here is the workflow for enabling Network Reasoner for an AP, along with the corresponding results:



Select Managed AP AP WLC to Troubleshoot



Provide AP Details to Troubleshoot

Wireless AP Data Collection

Root Cause Analysis

Reasoning Activity Conclusions (0)

Get Current Time ✓

Check AP SSH Credentials ✓

Get AP Type ✓

Check device reachability ✓

Check device controllability ✓

Evaluate device capabilities ✓

Check Device Site ✓

Relevant Activity Details Hide Details

Get Current Time
Jul 5, 2026 3:22:49 PM

Check if AP with IP address 10.127.197.180 has SSH credentials configured in Catalyst Center
Jul 5, 2026 3:22:50 PM

Get type of AP with IP address 10.127.197.180
Jul 5, 2026 3:22:51 PM

Check device controllability
Jul 5, 2026 3:22:51 PM

Determine if device is reachable
Jul 5, 2026 3:22:51 PM

Determine if the network features are supported on the given wireless platform
Jul 5, 2026 3:22:52 PM

Tasks Running to Troubleshoot AP Issue

Wireless AP Data Collection

Root Cause Analysis

Reasoning Activity Conclusions (1)

Download the troubleshooting files here:

- ap-1783245169513.log
- WLC.podx1.cisco.com-1783245169513.log
- WLC.podx1.cisco.com-1783245169513.pcap
- WLC.podx1.cisco.com-1783245169513.txt
- WLC.podx1.cisco.com-1783245169513.log
- Workflow Parameters

Viewing Relevant Activity Details...

Relevant Activity Details Hide Details

Get Current Time
Jul 5, 2026 3:22:49 PM

Check if AP with IP address 10.127.197.180 has SSH credentials configured in Catalyst Center
Jul 5, 2026 3:22:50 PM

Get type of AP with IP address 10.127.197.180
Jul 5, 2026 3:22:51 PM

Check device controllability
Jul 5, 2026 3:22:51 PM

Determine if device is reachable
Jul 5, 2026 3:22:51 PM

Determine if the network features are supported on the given wireless platform
Jul 5, 2026 3:22:52 PM

Captures Collected from WLC and AP for AP issue

!! Task Workflow !!

Get Current Time

Jul 5, 2026 5:04:39 PM

Check if AP with IP address 10.127.197.180 has SSH credentials configured in Catalyst Center

Jul 5, 2026 5:04:40 PM

Get type of AP with IP address 10.127.197.180

Jul 5, 2026 5:04:40 PM

Check device controllability

Jul 5, 2026 5:04:41 PM

Determine if device is reachable

Jul 5, 2026 5:04:41 PM

Determine if the network features are supported on the given wireless platform

Jul 5, 2026 5:04:41 PM

Check if the device <device> is provisioned or assigned to a site.

Jul 5, 2026 5:04:42 PM

Start RA Trace

Jul 5, 2026 5:04:49 PM

Get Current Time

Jul 5, 2026 5:04:54 PM

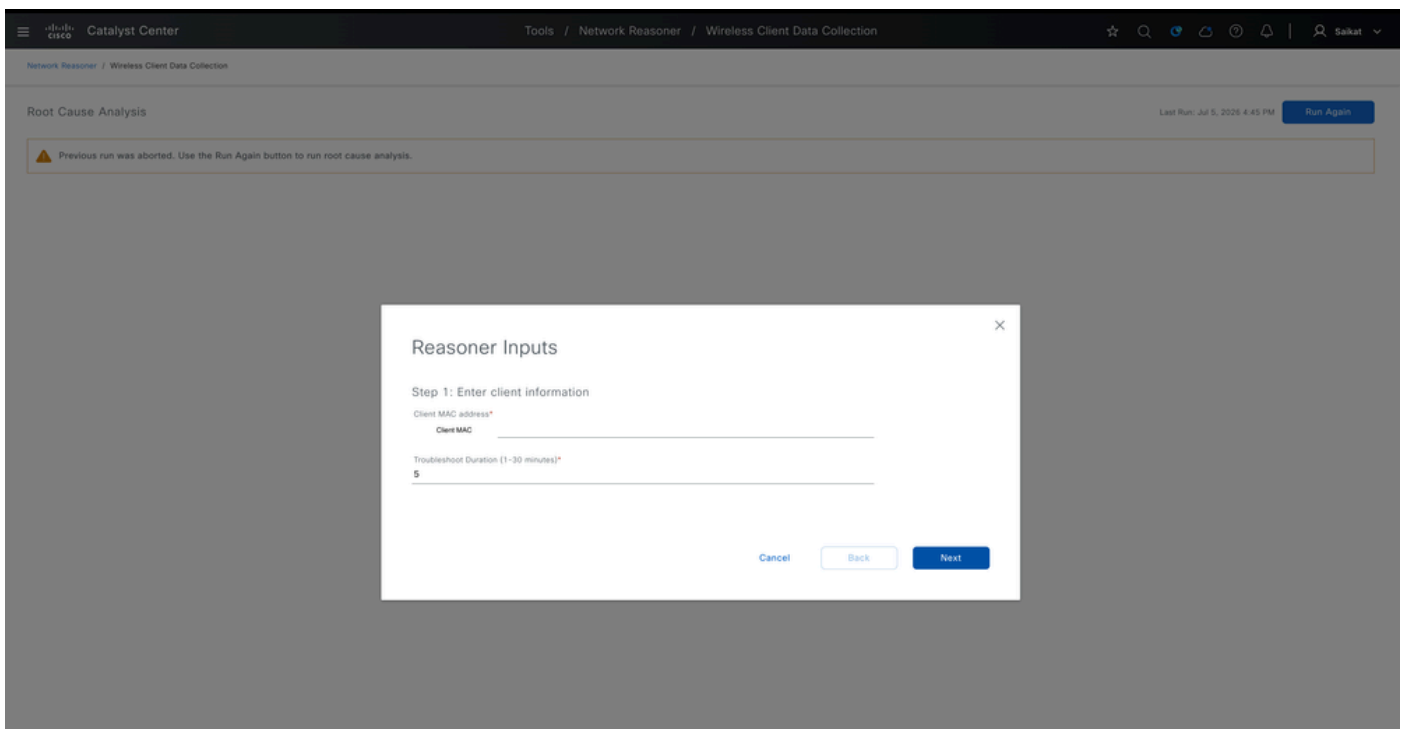
Starting AP PCAP session <file-name> with filter 10.127.197.180 on interface TenGigabitEthernet0/0/7

Jul 5, 2026 5:04:55 PM

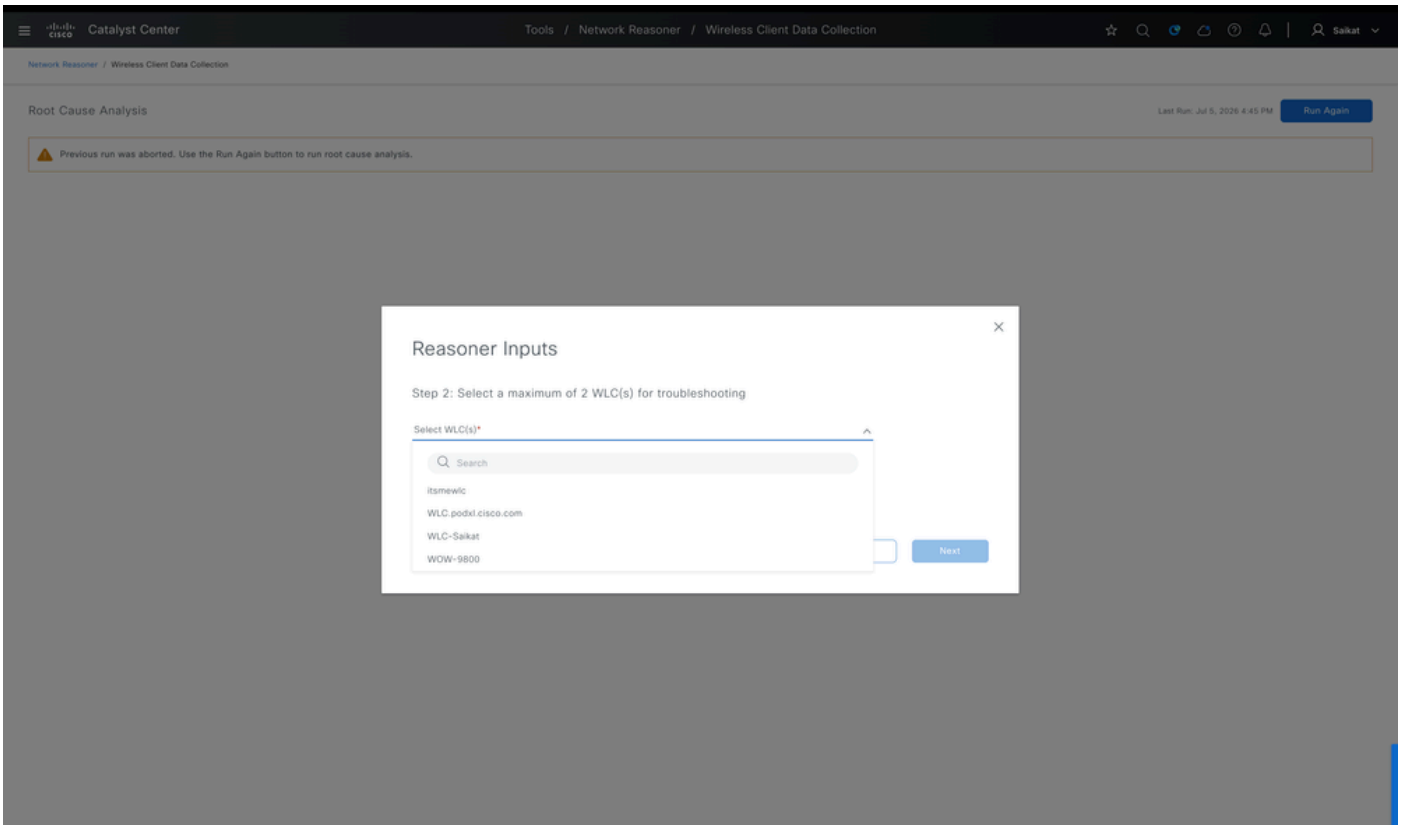
Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127.197.194
Jul 5, 2026 5:04:57 PM
Start AP statistics collection on WLC with IP address 10.127.197.194 and wait for data collection for 30 seconds
Jul 5, 2026 5:04:58 PM
Start logging on COS AP with IP address 10.127.197.180 over SSH for feature set apDataCollection, saved into file bootflash:
Jul 5, 2026 5:04:59 PM
Stop AP statistics collection on WLC with IP address 10.127.197.194 with data saved into file bootflash:
Jul 5, 2026 5:10:00 PM
Stop data collection on COS AP with IP address 10.127.197.180 over SSH for feature set apDataCollection
Jul 5, 2026 5:10:01 PM
Start AP show-tech wireless collection on WLC with IP address 10.127.197.194 for AP name LAB-9115 and save to file
Jul 5, 2026 5:10:02 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194
Jul 5, 2026 5:10:07 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194
Jul 5, 2026 5:10:15 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194
Jul 5, 2026 5:10:20 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194
Jul 5, 2026 5:10:27 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194
Jul 5, 2026 5:10:34 PM
Stop AP show-tech wireless collection on WLC with IP address 10.127.197.194 with data saved into file bootflash:
Jul 5, 2026 5:10:35 PM
Start to upload file bootflash:<file-name> from WLC with IP address 10.127.197.194 to https://10.105.197.194
Jul 5, 2026 5:10:36 PM
Check if file bootflash:<file-name> has been uploaded successfully from WLC with IP address 10.127.197.194 to https://10.105.197.194
Jul 5, 2026 5:10:41 PM
File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to https://10.105.197.194
Jul 5, 2026 5:10:41 PM
Delete the file bootflash:<file-name> from WLC with IP address 10.127.197.194
Jul 5, 2026 5:10:41 PM
Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127.197.194
Jul 5, 2026 5:10:43 PM
Stop RA Trace for AP: <MAC>
Jul 5, 2026 5:10:46 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194
Jul 5, 2026 5:10:49 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194
Jul 5, 2026 5:10:53 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194
Jul 5, 2026 5:10:57 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194
Jul 5, 2026 5:11:02 PM
Start to upload file bootflash:<file-name> from WLC with IP address 10.127.197.194 to https://10.105.197.194
Jul 5, 2026 5:11:03 PM
Check if file bootflash:<file-name> log has been uploaded successfully from WLC with IP address 10.127.197.194 to https://10.105.197.194
Jul 5, 2026 5:11:08 PM
File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to https://10.105.197.194
Jul 5, 2026 5:11:08 PM
Delete the file bootflash:<file-name> from WLC with IP address 10.127.197.194
Jul 5, 2026 5:11:08 PM
Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127.197.194
Jul 5, 2026 5:11:10 PM
Stop RA Trace for AP: <MAC>
Jul 5, 2026 5:11:13 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194
Jul 5, 2026 5:11:15 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194
Jul 5, 2026 5:11:19 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194
Jul 5, 2026 5:11:22 PM

Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194
Jul 5, 2026 5:11:27 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194
Jul 5, 2026 5:11:30 PM
Start to upload file bootflash:<file-name> from WLC with IP address 10.127.197.194 to https://10.105.197.194
Jul 5, 2026 5:11:32 PM
Check if file bootflash:<file-name> has been uploaded successfully from WLC with IP address 10.127.197.194
Jul 5, 2026 5:11:37 PM
File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to https://10.105.197.194
Jul 5, 2026 5:11:37 PM
Delete the file bootflash:<file-name> from WLC with IP address 10.127.197.194
Jul 5, 2026 5:11:39 PM
Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127.197.194
Jul 5, 2026 5:11:41 PM
Stopping PCAP <file-name> session with <AP-MAC> filter on TenGigabitEthernet0/0/7 interface.
Jul 5, 2026 5:11:41 PM
Start to upload file bootflash:<file-name> from WLC with IP address 10.127.197.194 to https://10.105.197.194
Jul 5, 2026 5:11:41 PM
Check if file bootflash:<file-name> has been uploaded successfully from WLC with IP address 10.127.197.194
Jul 5, 2026 5:11:46 PM
File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to https://10.105.197.194
Jul 5, 2026 5:11:53 PM
Delete the file bootflash:<file-name> from WLC with IP address 10.127.197.194
Jul 5, 2026 5:11:56 PM

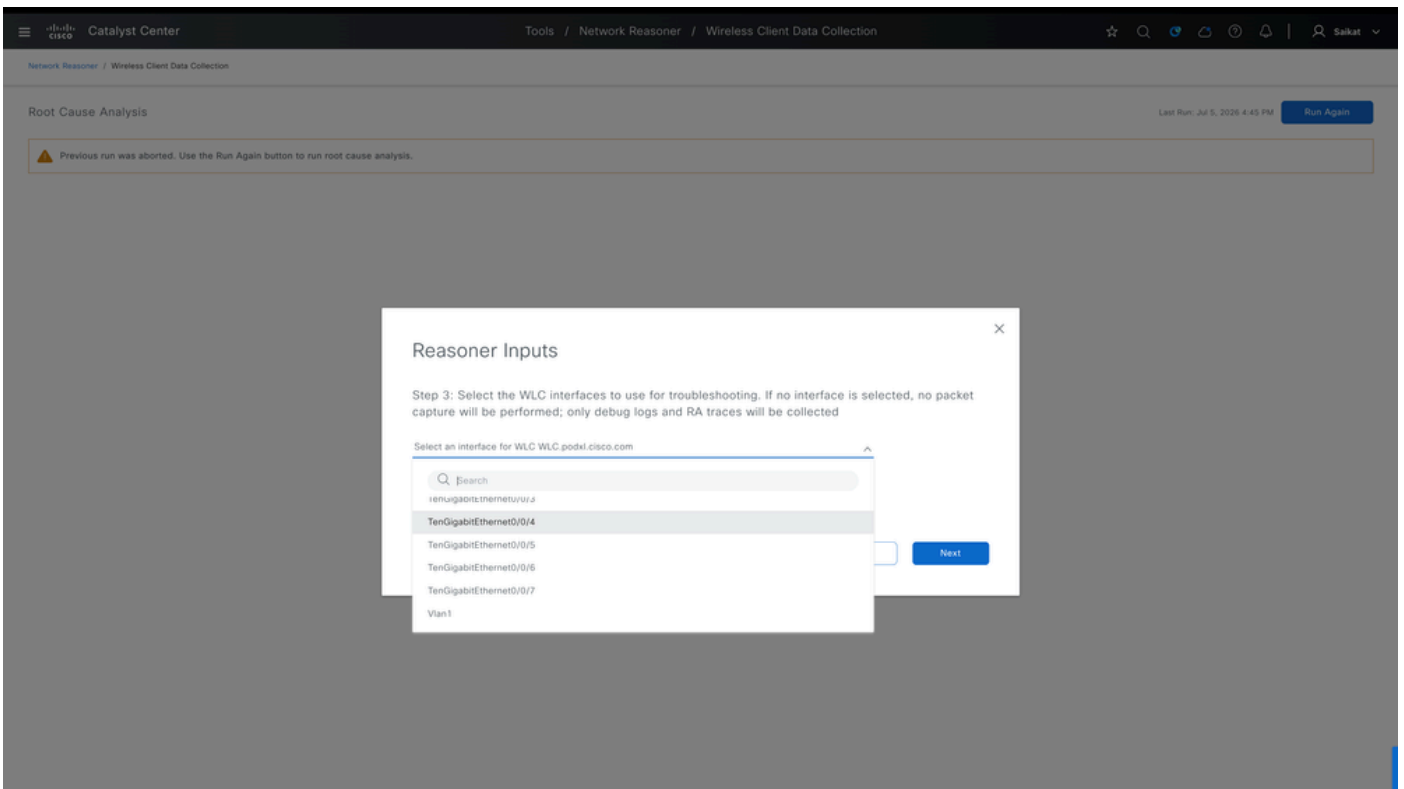
3. Wireless Clients - If a user is having Wi-Fi problems, pick the wireless controller they are connected to, enter their device MAC address, and choose how long you want the tool to monitor. It enables statistics logs, RA traces and packet capture to see the actual data exchanged. Here is the workflow for enabling Network Reasoner for wireless client, along with the corresponding results:



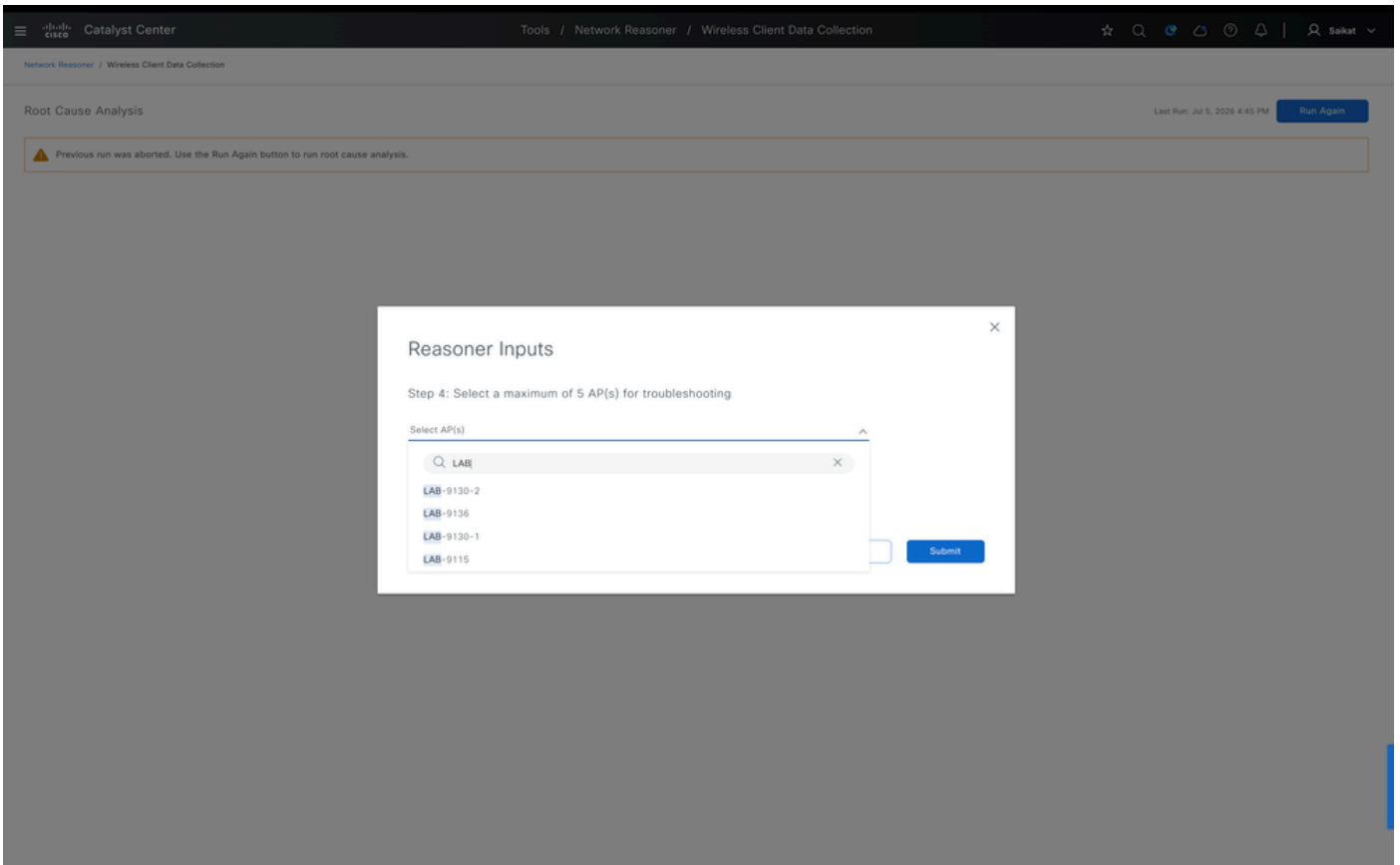
Provide Client Details to Troubleshoot



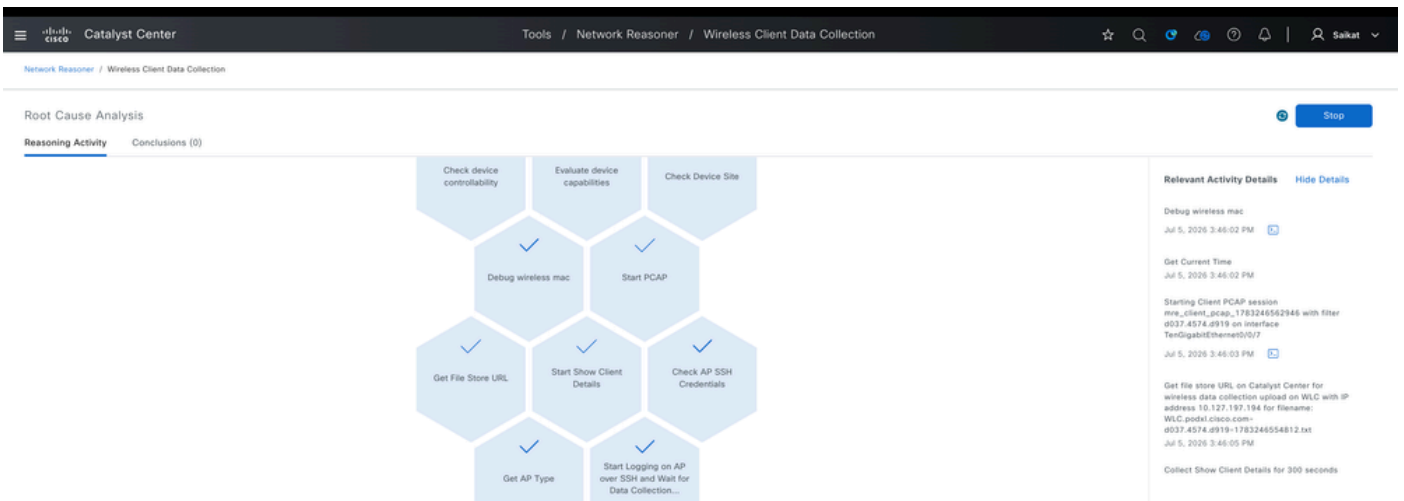
Select WLC to Troubleshoot Wireless Client MAC



Select Interface on WLC to Troubleshoot Wireless Client



Select APs (Max 4) to Troubleshoot Wireless Client



Tasks Running to Troubleshoot Wireless Client Issue

Catalyst Center Tools / Network Reasoner / Wireless Client Data Collection

Root Cause Analysis Last Run: Jul 5, 2026 3:45 PM [Run Again](#)

Reasoning Activity **Conclusions (1)**

- Download the troubleshooting files here:
 - WLC pod1.cisco.com client-mac 783246554812.txt
 - ap-10.127.197.151-1783246554812.log
 - WLC pod1.cisco.com client-mac 1783246554812.log
 - WLC pod1.cisco.com client-mac 1783246554812.pcap
 - ap-10.127.197.180-1783246554812.log
 - Workflow Parameters

[Relevant Activity Details](#)

Was this automated root cause analysis helpful? [👍](#) [👎](#)

Captures Collected from WLC and AP for Wireless Client Issue

!! Task Workflow !!

Get Current Time

Jul 5, 2026 5:53:11 PM

Check device controllability

Jul 5, 2026 5:53:11 PM

Determine if device is reachable

Jul 5, 2026 5:53:11 PM

Determine if the network features are supported on the given wireless platform

Jul 5, 2026 5:53:11 PM

Check if the device <device> is provisioned or assigned to a site.

Jul 5, 2026 5:53:12 PM

Debug wireless mac

Jul 5, 2026 5:53:18 PM

Get Current Time

Jul 5, 2026 5:53:19 PM

Starting Client PCAP session <file-name> with filter <clien-mac> on interface TenGigabitEthernet0/0/7

Jul 5, 2026 5:53:20 PM

Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127

Jul 5, 2026 5:53:21 PM

Collect Show Client Details for 300 seconds

Jul 5, 2026 5:53:22 PM

Check if AP with IP address 10.127.197.180 has SSH credentials configured in Catalyst Center

Jul 5, 2026 5:53:24 PM

Get type of AP with IP address 10.127.197.180

Jul 5, 2026 5:53:25 PM

Start logging on COS AP with IP address 10.127.197.180 over SSH for Client MAC <client-mac> feature set

Jul 5, 2026 5:53:28 PM

End Show Client Details

Jul 5, 2026 5:58:35 PM

Stop data collection on COS AP with IP address 10.127.197.180 over SSH for Client MAC <client-mac> feat

Jul 5, 2026 5:58:36 PM

Stop data collection on COS AP with IP address 10.127.197.151 over SSH for Client MAC <client-mac> feat

Jul 5, 2026 5:58:38 PM

Check File Size: <file-name>

Jul 5, 2026 5:58:38 PM

Start to upload file <file-name> from WLC with IP address 10.127.197.194 to <https://10.105.193.40/api/v>

Jul 5, 2026 5:58:40 PM

Check if file <file-name> has been uploaded successfully from WLC with IP address 10.127.197.194 to [htt](https://10.105.193.40/api/v)

Jul 5, 2026 5:58:45 PM

File <file-name> uploaded successfully from WLC with IP address 10.127.197.194 to [https://10.105.193.40](https://10.105.193.40/api/v)

Jul 5, 2026 5:58:45 PM

Delete the file <file-name> from WLC with IP address 10.127.197.194

Jul 5, 2026 5:58:45 PM

Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127

Jul 5, 2026 5:58:47 PM

No debug wireless mac

Jul 5, 2026 5:58:49 PM

Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.

Jul 5, 2026 5:58:52 PM

Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.

Jul 5, 2026 5:58:56 PM

Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.

Jul 5, 2026 5:58:59 PM

Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.

Jul 5, 2026 5:59:03 PM

Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.

Jul 5, 2026 5:59:07 PM

Start to upload file bootflash:<file-name> from WLC with IP address 10.127.197.194 to <https://10.105.19>

Jul 5, 2026 5:59:09 PM

Check if file bootflash:<file-name> has been uploaded successfully from WLC with IP address 10.127.197.

Jul 5, 2026 5:59:14 PM

File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to <https://10.>

Jul 5, 2026 5:59:14 PM

Delete the file bootflash:<file-name> from WLC with IP address 10.127.197.194

Jul 5, 2026 5:59:14 PM

Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127.

Jul 5, 2026 5:59:16 PM

Stopping PCAP <file-name> session with d037.4574.d919 filter on TenGigabitEthernet0/0/7 interface.

Jul 5, 2026 5:59:16 PM

Check File Size:bootflash:<file-name>

Jul 5, 2026 5:59:16 PM

Start to upload file bootflash:<file-name> from WLC with IP address 10.127.197.194 to <https://10.105.19>

Jul 5, 2026 5:59:18 PM

Check if file bootflash:<file-name> has been uploaded successfully from WLC with IP address 10.127.197.

Jul 5, 2026 5:59:23 PM

File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to

Jul 5, 2026 5:59:23 PM

Delete the file bootflash:<file-name> from WLC with IP address 10.127.197.194

Jul 5, 2026 5:59:23 PM

Technical References

- [Cisco Intelligent Capture Deployment Guide](#)
- [Manage Intelligent captures](#)
- [Cisco Catalyst Assurance User Guide, Release 2.3.7.x](#)
- [Troubleshoot Network Device using Network Reasoner - HA on Wireless LAN Controller using MRE Workflow](#)