

Risoluzione dei problemi wireless con Catalyst Center

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Raccolta dati da Catalyst Center](#)

[Problema con Catalyst serie 9800 Wireless Controller](#)

[Verifica dello stato del controller con Device 360](#)

[Problema con un punto di accesso](#)

[Acquisizioni intelligenti per access point](#)

[Acquisizione statistiche AP](#)

[OTA Sniffer Capture](#)

[Rilevamento anomalie](#)

[Problema di connettività client wireless](#)

[Acquisizioni intelligenti per client wireless](#)

[Acquisizione pacchetti in entrata](#)

[Acquisizione completa dei pacchetti](#)

[Isolamento dei problemi dei servizi di rete \(AAA, DHCP, DNS\)](#)

[Motivo rete](#)

[Riferimenti tecnici](#)

Introduzione

Questo documento descrive la risoluzione dei problemi di connettività di Catalyst 9800 Wireless LAN Controller (WLC), AP e client con Cisco Catalyst Center.

Prerequisiti

- Il controller LAN wireless deve essere aggiunto al Catalyst Center e deve essere visualizzato nell'inventario uno stato gestito.
- Lo stato della telemetria sul WLC deve essere visualizzato.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso da CLI (Command Line Interface) o GUI (Graphic User Interface) al controller LAN wireless
- Accesso da CLI (Command Line Interface) o GUI (Graphic User Interface) a Catalyst Center

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 9800 modello WLC
- Cisco IOS XE versione 17.15.5
- Versione di Catalyst Center 2.3.7

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

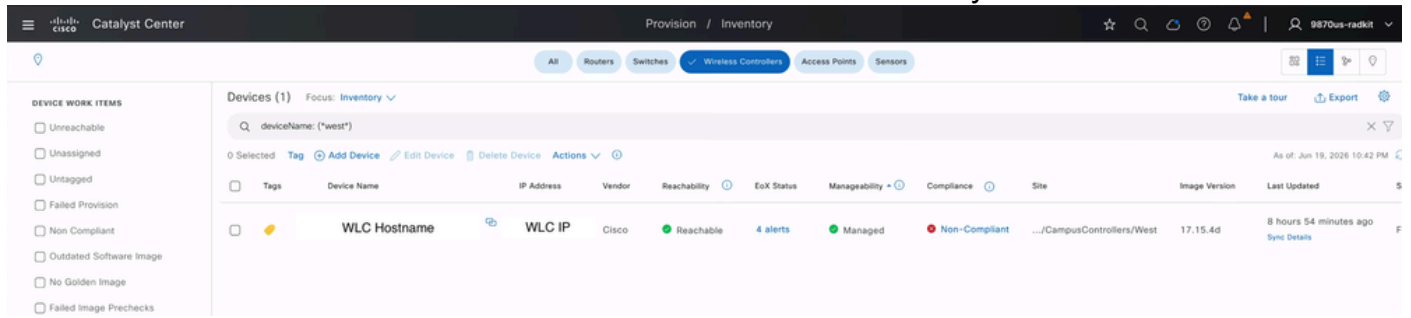
Raccolta dati da Catalyst Center

Dopo aver aggiunto un WLC Catalyst serie 9800 a Catalyst Center for Assurance, la piattaforma recupera i dati tramite diversi metodi di raccolta, tra cui polling SNMP, telemetria in streaming, NetFlow, Syslog, raccolta basata su CLI, API e SLA IP. Ciascun meccanismo ha una finalità diversa: alcuni segnalano lo stato di base dei dispositivi (CPU, memoria, indicatori KPI), mentre altri forniscono dettagli granulari (stato PoE, sessioni client, prestazioni wireless).

1. Integrità dispositivo/inventario (SNMP + CLI): Raggiungibilità, CPU, memoria, statistiche dell'interfaccia e versione del software: raccolte tramite il polling SNMP e la CLI standard.
2. Syslog: Messaggi di log operativi e di sistema inviati al Catalyst Center, che funge da server syslog configurato.
3. Telemetria wireless (streaming NETCONF/YANG): Il feed Assurance di base. Trasmette dati a livello di client e AP quasi in tempo reale: eventi di caricamento e roaming dei client, RSSI/SNR, statistiche radio/RF AP e contatori interni dello stato WLC.

Per ricevere questi dati, il controller LAN wireless deve essere in stato gestito su Catalyst Center,

con lo stato della telemetria visualizzato tra il controller 9800 e Catalyst Center.



Stato del controller LAN wireless su 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

Per impostazione predefinita, Cisco Catalyst Center è configurato con impostazioni relative a stato, problemi ed eventi che includono soglie e priorità specifiche per controller wireless, punti di accesso, client wireless e applicazioni. Catalyst Center genera eventi e avvisi in base ai dati ricevuti da questi dispositivi gestiti e alle impostazioni degli eventi configurate. Inoltre, è possibile creare profili personalizzati per adattare le impostazioni alle esigenze specifiche della rete, consentendo un monitoraggio più preciso e l'invio di avvisi in base alle esigenze specifiche dell'ambiente di rete.

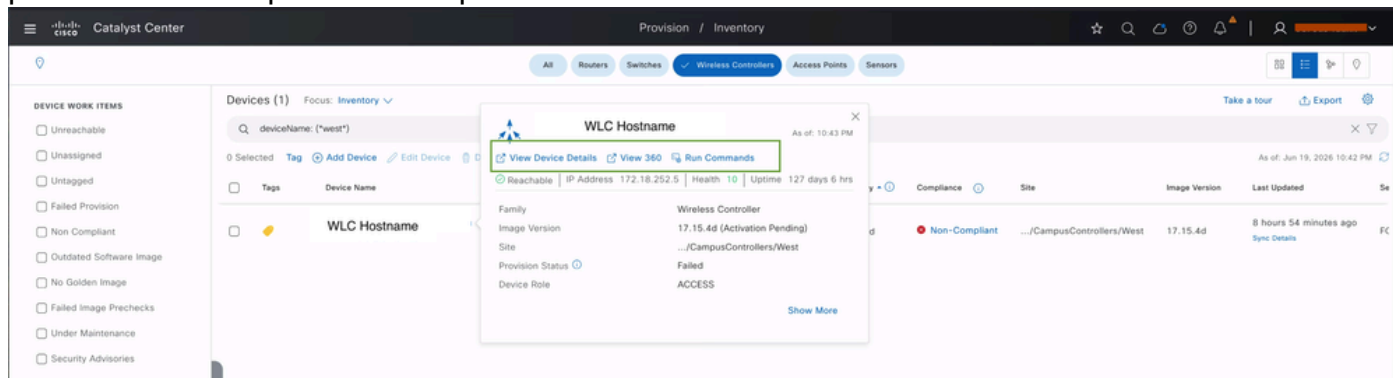
Problema con Catalyst serie 9800 Wireless Controller

Quando un controller WLC (Wireless LAN Controller) incontra problemi come la perdita di raggiungibilità, le prestazioni lente, gli errori di accessibilità, un'interruzione o un peggioramento in un servizio specifico, Cisco Catalyst Center offre una visibilità integrata che consente di ricostruire quanto stava accadendo sul controller nel momento esatto in cui si è verificato il problema, senza dover accedere direttamente al dispositivo.

Verifica dello stato del controller con Device 360

La vista di Device 360 consolida in un unico dashboard basato su timeline la raggiungibilità dei controller, lo stato della telemetria, i problemi storici, gli eventi generati e le statistiche delle prestazioni, rendendolo il primo punto da esaminare quando si analizza un problema WLC segnalato.

Selezionare Provisioning > Inventory > Wireless Controller > [cerca il controller] > fare clic sul pulsante nome dispositivo > Dispositivo 360



View 360 per controller LAN wireless

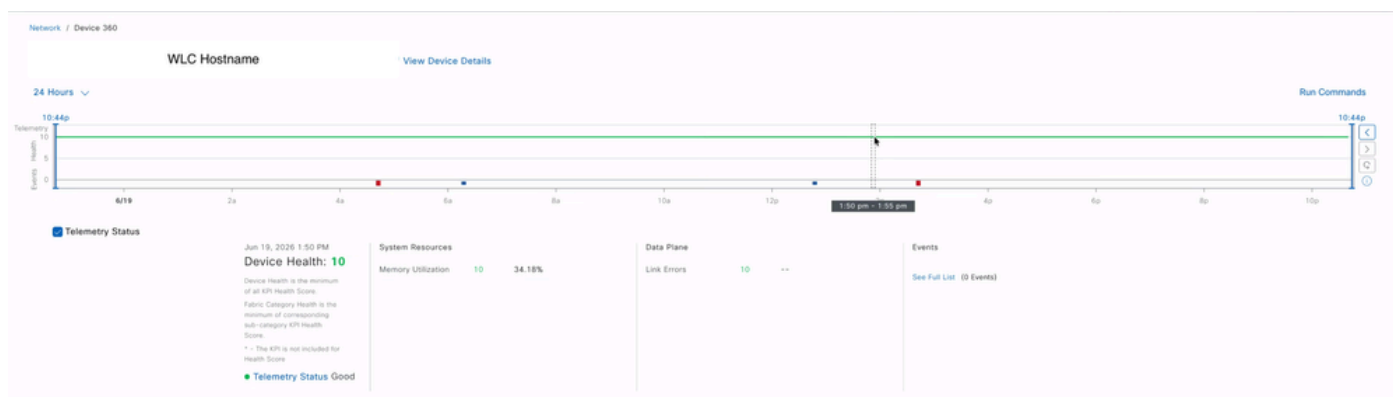


Nota: La stessa vista può essere raggiunta anche da Assurance > Integrità > Rete, quindi facendo clic sul nome del dispositivo nella tabella Dispositivi di rete.

Device 360 consente di spostare il dispositivo di scorrimento della cronologia dello stato di salute in un punto qualsiasi all'interno della finestra cronologica supportata (i dati di Catalyst Center Assurance vengono conservati per un massimo di 30 giorni) per verificare esattamente l'aspetto dello stato del controller al momento dell'incidente. Per la finestra selezionata, la vista viene visualizzata come segue:

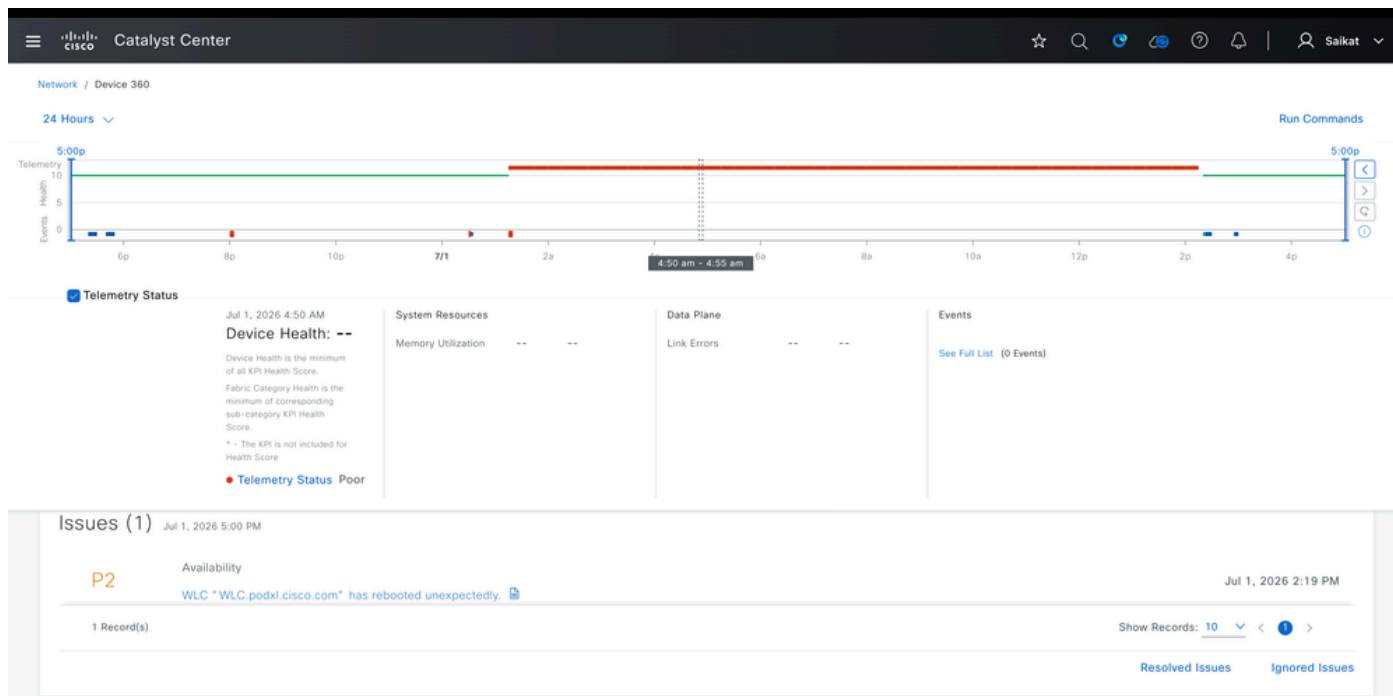
Raggiungibilità del dispositivo: indica se il controller è raggiungibile e gestito.

Stato della telemetria: stato di SNMP/Syslog/NETCONF telemetry feed Assurance.



Stato telemetria del controller LAN wireless

Problemi osservati: i problemi rilevati con la garanzia sul dispositivo durante tale periodo.



Problemi segnalati per il controller LAN wireless

Facendo clic su un problema specifico è possibile visualizzare informazioni dettagliate su di esso, insieme alle azioni suggerite per risolverlo o indagare ulteriormente.

Catalyst Center

Network / Device 360

24 Hours

Telemetry Health

5:00p

Events Health

6p

Telemetry Status

10/10

DEVICE DETAILS

Model: C9800-80-K9 Management

Uptime: 2 hours, 39 minutes

Issues (1) Jul 1, 2026

P2 Available

WLC

1 Record(s)

Physical Neigh

WLC "WLC.podxl.cisco.com" has rebooted unexpectedly.

Open |

Issue Profile: global Edit Issue Settings

Description

This WLC "WLC.podxl.cisco.com" has rebooted unexpectedly. Reboot reason is "PowerOn"

Last Occurred: Jul 1, 2026 2:19 PM

WLC Reboot History

Jun 30, 2026 5:00 PM to Jul 1, 2026 5:00 PM

Export

Search Table

Time	Uptime	Reason
7/1/26 2:19pm	2d 18h 19m	PowerOn

1 Record(s) Show Records: 10 < 1 >

Suggested Actions (4)

Preview All Run All

- Run show version for more details. Run
- Check if there was any power failure on the WLC.
- If this is a crash, capture this WLC's crash log.

Azione consigliata per il problema segnalato sul WLC

Catalyst Center

Network / Device 360

24 Hours

Telemetry Health

5:00p

Events Health

6p

Telemetry Status

10/10

DEVICE DETAILS

Model: C9800-80-K9 Management

Uptime: 2 hours, 39 minutes

Issues (1) Jul 1, 2026

P2 Available

WLC

1 Record(s)

Physical Neigh

WLC "WLC.podxl.cisco.com" has rebooted unexpectedly.

Open |

Issue Profile: global Edit Issue Settings

Description

This WLC "WLC.podxl.cisco.com" has rebooted unexpectedly. Reboot reason is "PowerOn"

Last Occurred: Jul 1, 2026 2:19 PM

WLC Reboot History

Jun 30, 2026 5:00 PM to Jul 1, 2026 5:00 PM

Export

Search Table

Time	Uptime	Reason
7/1/26 2:19pm	2d 18h 19m	PowerOn

1 Record(s) Show Records: 10 < 1 >

Suggested Actions (4)

Preview All Run All

- Run show version for more details.
 - show version


```
show version
Cisco IOS XE Software, Version 17.18.03
Cisco IOS Software [IOSXE], C9800 Software (C9800_IOSXE-K9), Version 17.18.3, RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2026 by Cisco Systems, Inc.
Compiled Tue 14-Apr-26 08:56 by mcpre
```

 Success
- Check if there was any power failure on the WLC.
- If this is a crash, capture this WLC's crash log.

Azione consigliata per il problema segnalato sul WLC

Eventi generati: in base ai messaggi syslog e alle trap SNMP ricevute dal controller:

The screenshot shows the 'Event Viewer' interface. At the top, there are links for 'Go to Global Event Viewer', 'Export', and 'Full Screen'. A search bar labeled 'Search Table' is present. Below is a table with columns: Severity, Details, Message Type, and Time. The table shows several events from June 19, 2026. One event is selected, and its details are shown in a sidebar on the right. The selected event is a Notice with the message type 'Syslog' and time '12:49:30.457 PM'. The detailed information sidebar shows: Severity: Notice, Mnemonic: AP_JOIN_DISJOIN, Facility: CAPWAPAC_SMGR_TRACE_MESSAGE, Message Text: 77536189: wlc-200-wlc0-0n, Jun 19 17:19:30.208 AEST: %CAPWAPAC_SMGR_TRACE_MESSAGE-9-AP_JOIN_DISJOIN: Chassis 1 R0/0: wlc0d: AP Event: AP Name: AP_Name, AP_MAC and IP Details: Joined, Message Type: Syslog.

Visualizzatore eventi per controller LAN wireless - Esempio 1

The screenshot shows the 'Event Viewer' interface. At the top, there are links for 'Go to Global Event Viewer', 'Export', and 'Full Screen'. A search bar labeled 'Search Table' is present. Below is a table with columns: Severity, Details, Message Type, and Time. The table shows several events from June 19, 2026. One event is selected, and its details are shown in a sidebar on the right. The selected event is an Alert with the message type 'Syslog' and time '2:44:31.673 PM'. The detailed information sidebar shows: Severity: Alert, Mnemonic: ANCHORS_DOWN, Facility: MM_NODE_LOG, Message Text: 77536901: wlc-200-wlc0-0n, Jun 19 19:14:31.360 AEST: %MM_NODE_LOG-1-ANCHORS_DOWN: Chassis 1 R0/0: mobilityd: All Export-Anchors are down, Message Type: Syslog.

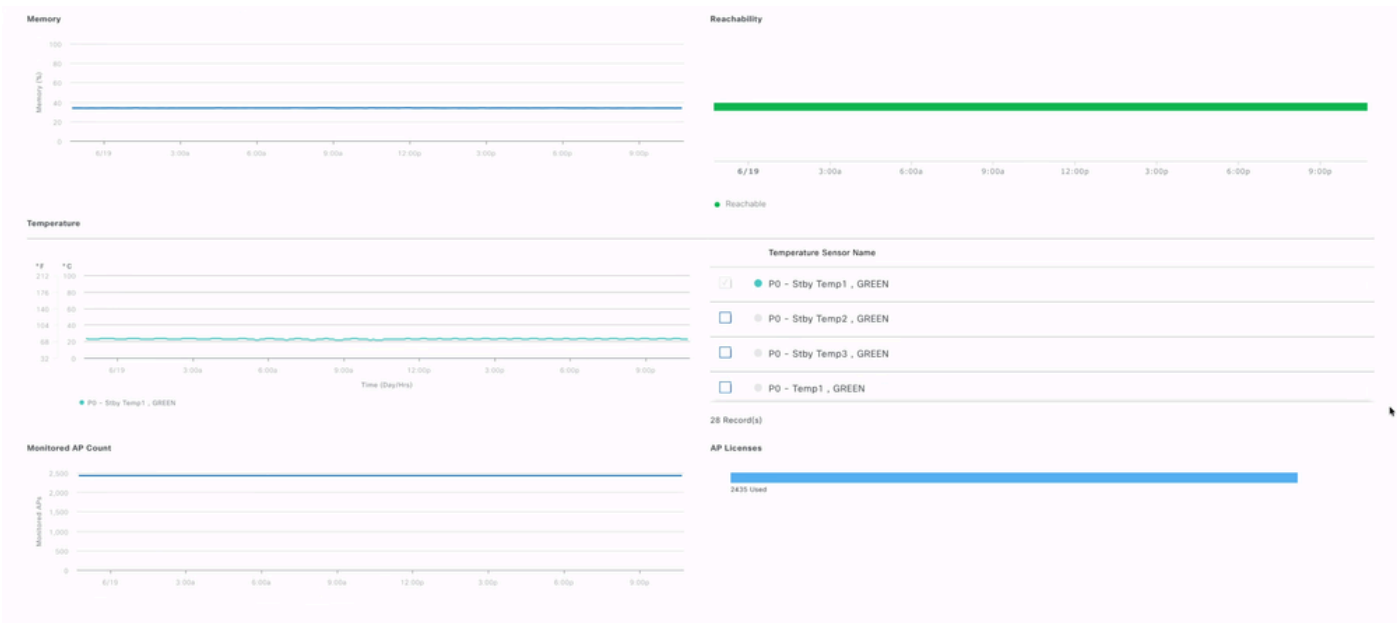
Visualizzatore eventi per controller LAN wireless - Esempio 2

Statistiche relative alle prestazioni: utilizzo di CPU e memoria, temperatura, tempo di attività, stato HA e motivo dell'ultimo ricaricamento.

Client connessi, incluse le suddivisioni per conteggi di client locali, esteri, di ancoraggio e inattivi. Stato AP — lo stato di join/integrità dei punti di accesso associati al controller.



Statistiche WLC su Catalyst Center



Statistiche WLC su Catalyst Center

Statistiche interfaccia: stato per interfaccia, conteggi pacchetti RX/TX, utilizzo, scarti ed errori.

Select interface in the table to show on the charts below (Maximum of 5 selections).

1 Selected: FortyGigabitEthernet0/1/0

Interface Availability

FortyGigabitEthernet0/1/0

100

Traffic and Packet Summary

	Received	Transmitted
Total Traffic	765.16GB	835.45GB
Total Packets	6580416636	6703870784
Unknown Protocol Packets	2905	NA
Unicast Packets	6557067468	6689542086
Multicast Packets	19941425	9916424
Broadcast Packets	3404022	4412274
Forward Packets	0	0
Error Packets	816	0
Discard Packets	0	0

Statistiche WLC su Catalyst Center

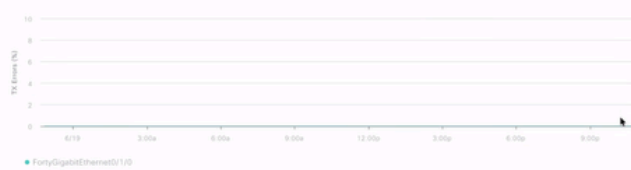
Utilization

TX Utilization



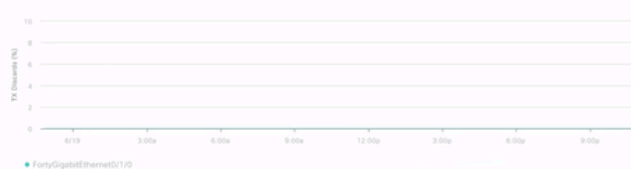
Error

TX Errors



Discard

TX Discards



RX Utilization



Error

RX Errors



Discard

RX Discards



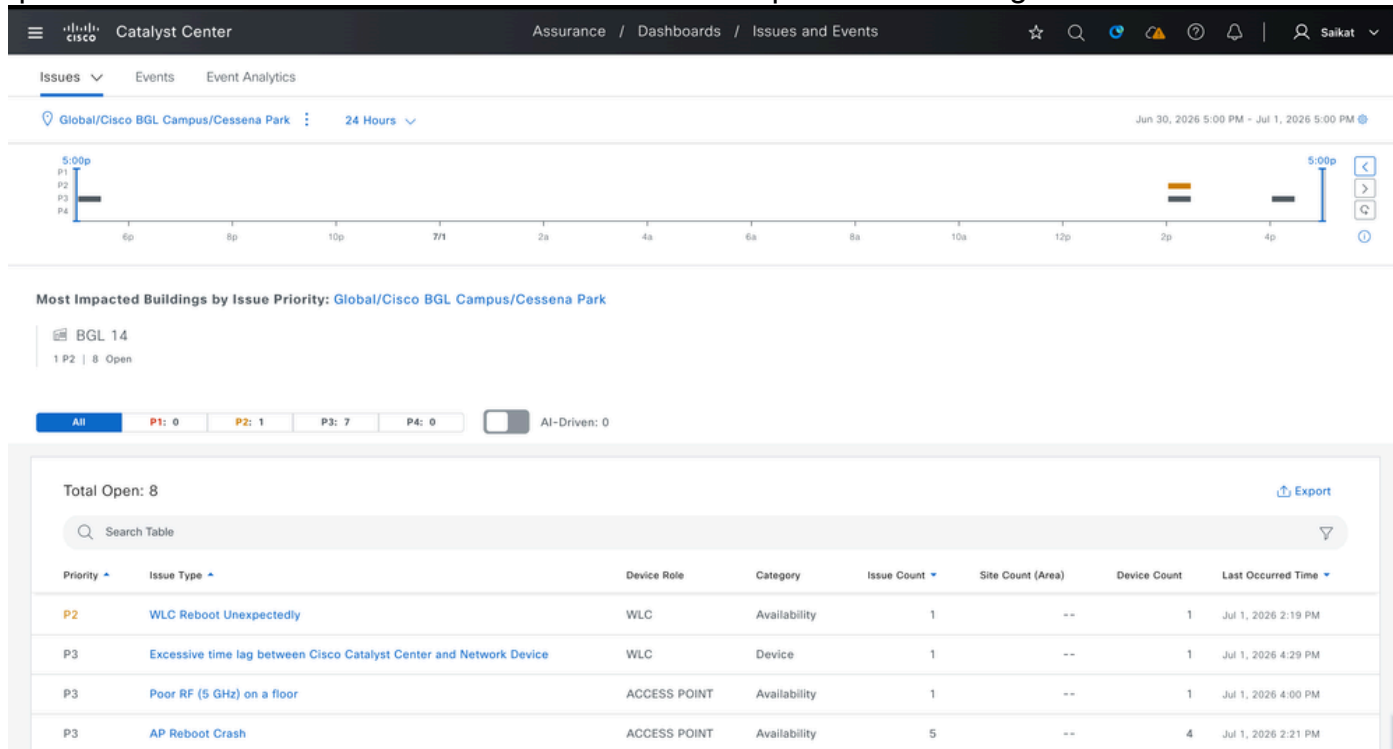
Statistiche WLC su Catalyst Center

Poiché tutto ciò è correlato, è possibile correlare più fattori correlati durante il tempo di emissione e ottenere una chiara comprensione. Con queste statistiche non è possibile ottenere esattamente la causa principale del problema, ma possiamo escludere tutte le potenziali cause che possono aiutarci a risolvere ulteriormente il problema e impostare il tipo di log richiesto per essere raccolti in tempo reale.

Problema con un punto di accesso

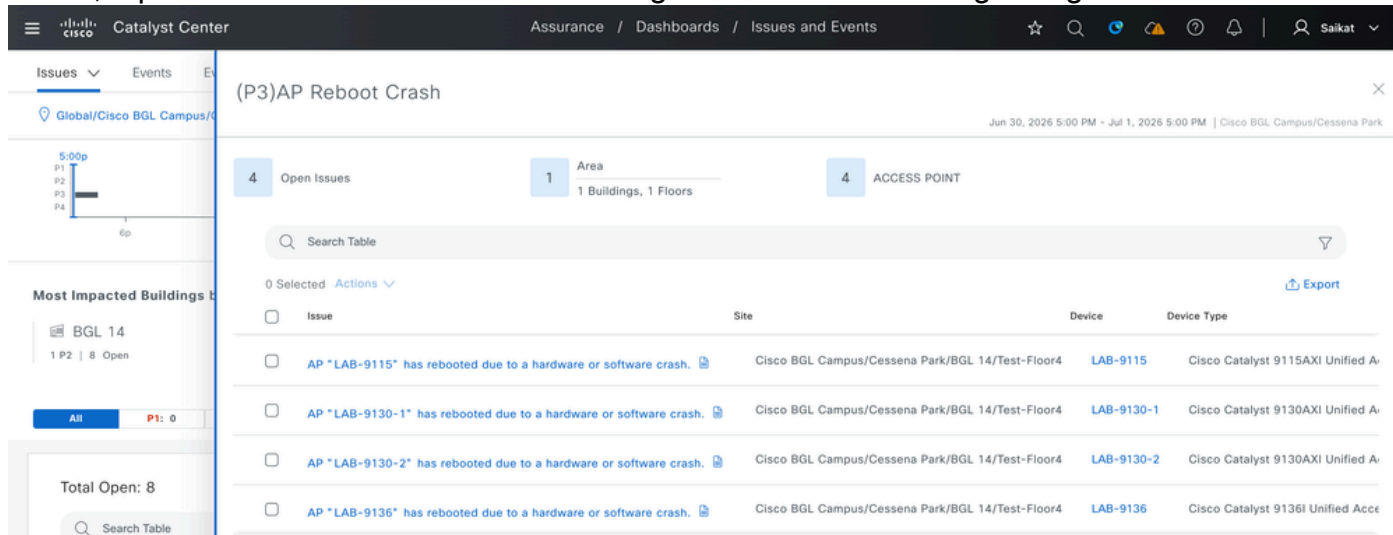
Quando un Cisco Access Point incontra problemi come eventi di disconnessione, anomalie dello stato della radio, riavvii, arresti anomali, condizioni RF scadenti, elevato utilizzo dei canali o inattività, Catalyst Center genera avvisi con livelli di priorità appropriati. È possibile visualizzare

questi avvisi selezionando Assurance > Problemi e impostazioni di integrità.



Problemi segnalati Genera un avviso con la priorità corrispondente

In questa sezione vengono visualizzati tutti i problemi aperti dell'ambiente. Facendo clic sui singoli eventi, è possibile ottenere informazioni dettagliate facendo clic su ogni singolo evento:



Panoramica dettagliata del problema segnalato

Facendo clic su un problema specifico è possibile visualizzare informazioni dettagliate su di esso, insieme alle azioni suggerite per risolverlo o indagare ulteriormente.

Catalyst Center Assurance / Dashboards / Issues and Events

AP Reboot Crash / Issue Instance

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

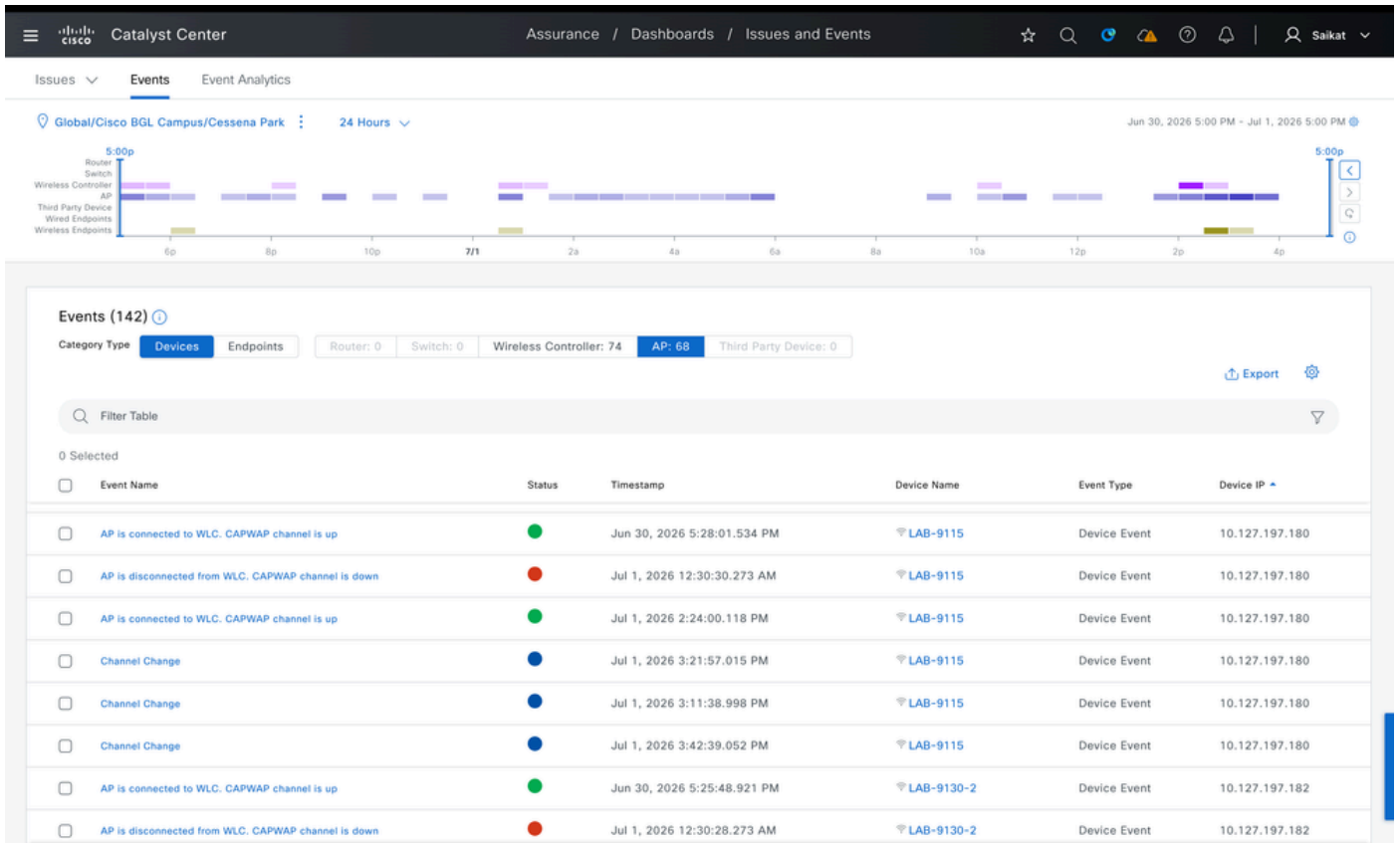
1 Record(s) Show Records: 25 < 1 >

Suggested Actions (2)

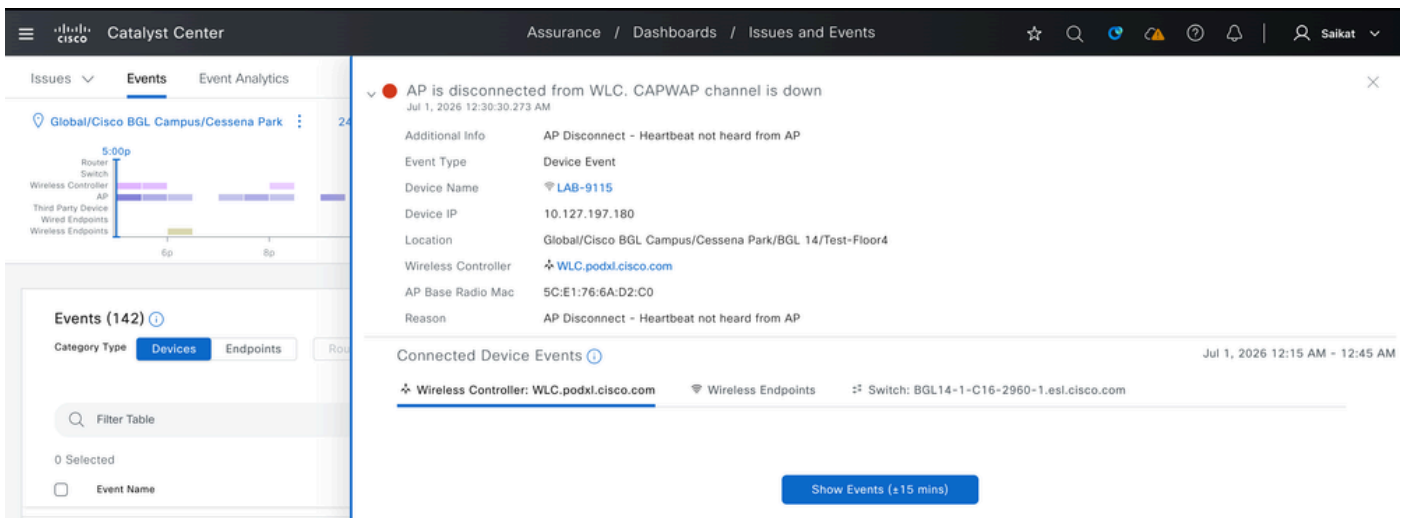
- 1 Capture this AP's crash log.
- > 2 If you are unable to resolve the issue, contact Cisco TAC for support.

Azione suggerita per il problema segnalato in AP

È inoltre possibile accedere al Visualizzatore eventi, che contiene tutti gli eventi ricevuti da Catalyst Center come syslog. Ciò è utile per tenere traccia di tutti gli eventi quali l'attività di aggiunta/disconnessione di un punto di accesso, le modifiche dei canali, le modifiche dell'alimentazione TX e i riavvii. Questi eventi vengono acquisiti sia per il controller wireless che per i singoli access point.



Visualizzatore eventi per access point su Catalyst Center



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

Panoramica dettagliata dell'evento segnalato (avviso)

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 up

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

Panoramica dettagliata dell'evento segnalato (avviso)

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

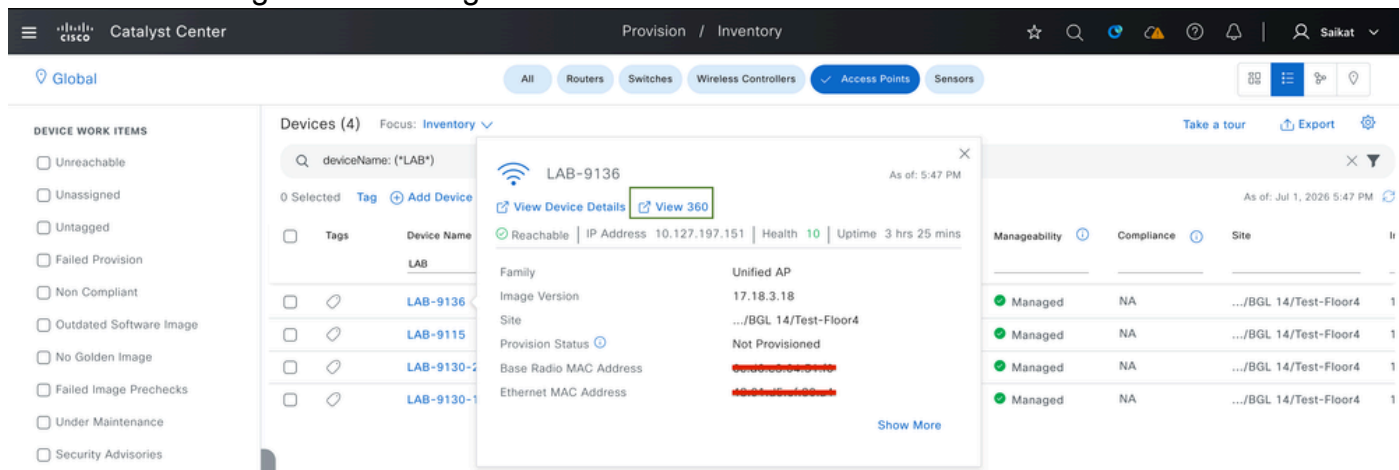
Connected Device Events
Jun 30, 2026 5:10 PM - 5:40 PM

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

Show Events (±15 mins)

Panoramica dettagliata dell'evento segnalato (Info)

Per i problemi specifici di un singolo access point, è possibile controllare la visualizzazione Integrità 360 del dispositivo. In questa schermata è possibile visualizzare lo stato di raggiungibilità, gli eventi e i problemi segnalati, oltre al punteggio di integrità relativo all'access point in un determinato momento. Il livello di integrità viene calcolato in base all'utilizzo della memoria, del canale, della qualità dell'aria, delle interferenze e del traffico. Per eseguire questa operazione, selezionare Assegnazione > Magazzino > Access Point > Fare clic su AP:



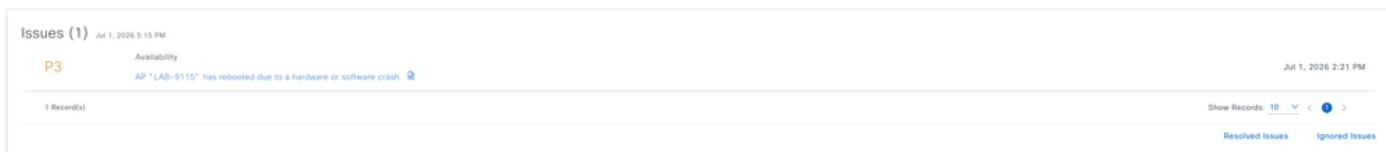
Vista 360 per access point individuale

Riepilogo telemetria dispositivo 360: Qui è possibile visualizzare la cronologia del punteggio di integrità complessivo dei punti di accesso, l'utilizzo delle risorse di sistema (memoria, CPU), gli errori di collegamento al piano dati e le statistiche specifiche della radio (rumore, utilizzo dei canali, interferenze, utilizzo del traffico) per entrambe le radio. La periferica 360 consente di spostare il dispositivo di scorrimento della cronologia di stato in qualsiasi punto all'interno della finestra cronologica supportata (30 giorni).



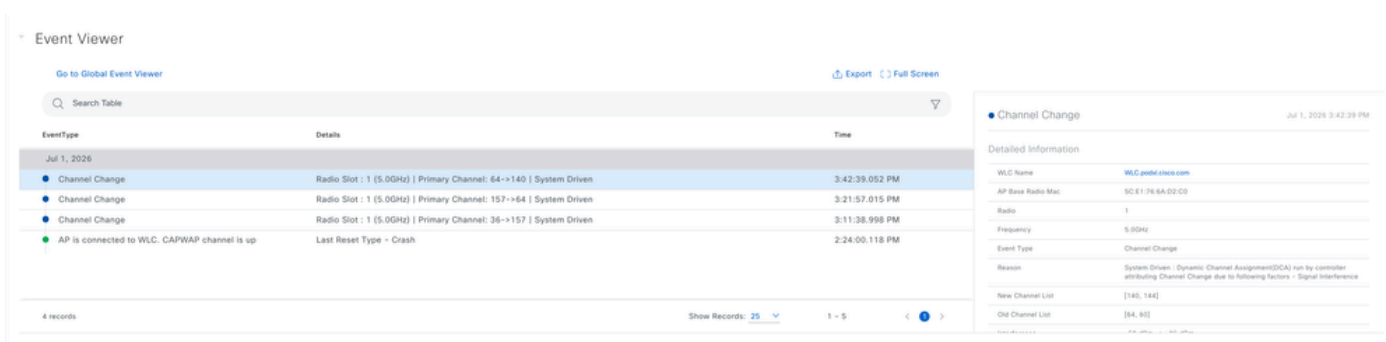
Visualizzazione 360: Stato e integrità telemetria AP

Problemi - Qui è possibile vedere l'elenco dei problemi aperti per l'access point, insieme alla gravità (P1-P4), la categoria del problema, la descrizione e i timestamp.



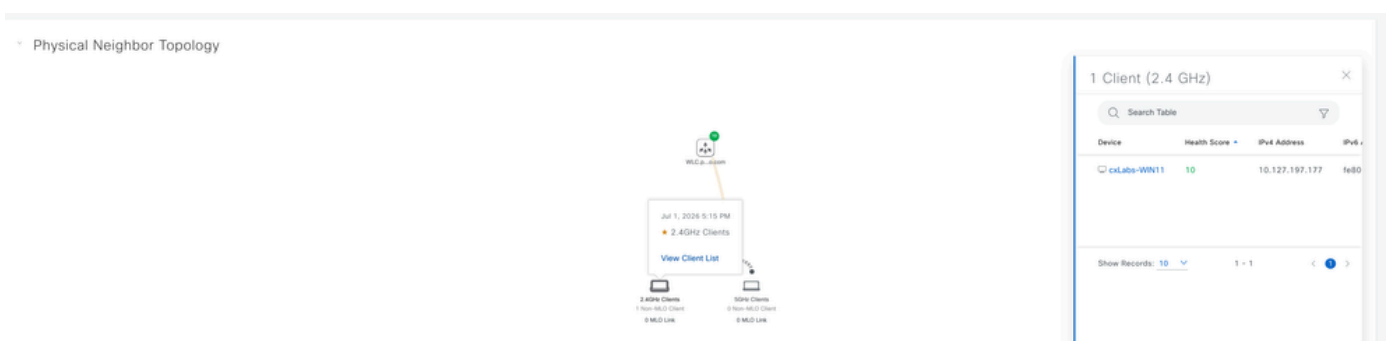
Problema segnalato per il punto di accesso

Visualizzatore eventi: è possibile visualizzare un registro cronologico degli eventi AP (ad esempio, modifiche dei canali, stato CAPWAP) insieme a informazioni dettagliate sugli eventi quali il nome WLC, la radio, la frequenza, il motivo e gli elenchi dei canali vecchi/nuovi.



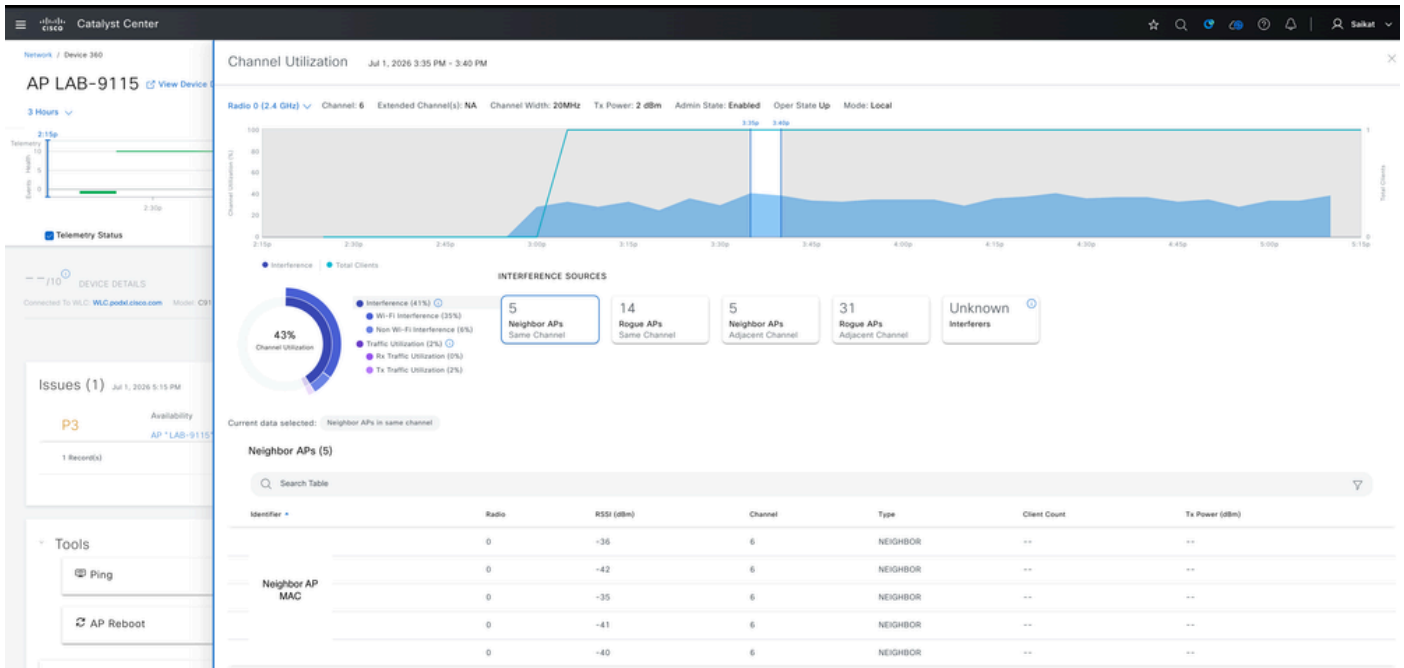
Visualizzatore eventi di singoli access point

Physical Neighbor Topology with Client List: questa vista mostra la topologia fisica che connette il WLC, l'access point e i client connessi, oltre a ulteriori dettagli sul client come il nome del dispositivo, il punteggio di integrità e MLO



Topologia fisica del punto di accesso

Utilizzo del canale: è possibile visualizzare la tendenza di utilizzo del canale dei punti di accesso, le origini delle interferenze (punti di accesso adiacenti, punti di accesso non autorizzati, interferenze sconosciute) e una tabella dettagliata dei punti di accesso adiacenti con RSSI, canale e tipo.



Utilizzo dei canali per singoli access point

Informazioni dettagliate (scheda Periferica) - Questa sezione mostra le informazioni sul dispositivo (nome AP, IP, modello, indirizzi MAC, versione del software), i dettagli sulla disponibilità (uptime, tempo di collegamento al controller, motivo dell'ultimo reset), i grafici sull'utilizzo della CPU e della memoria e il grafico della connettività da AP a WLC.



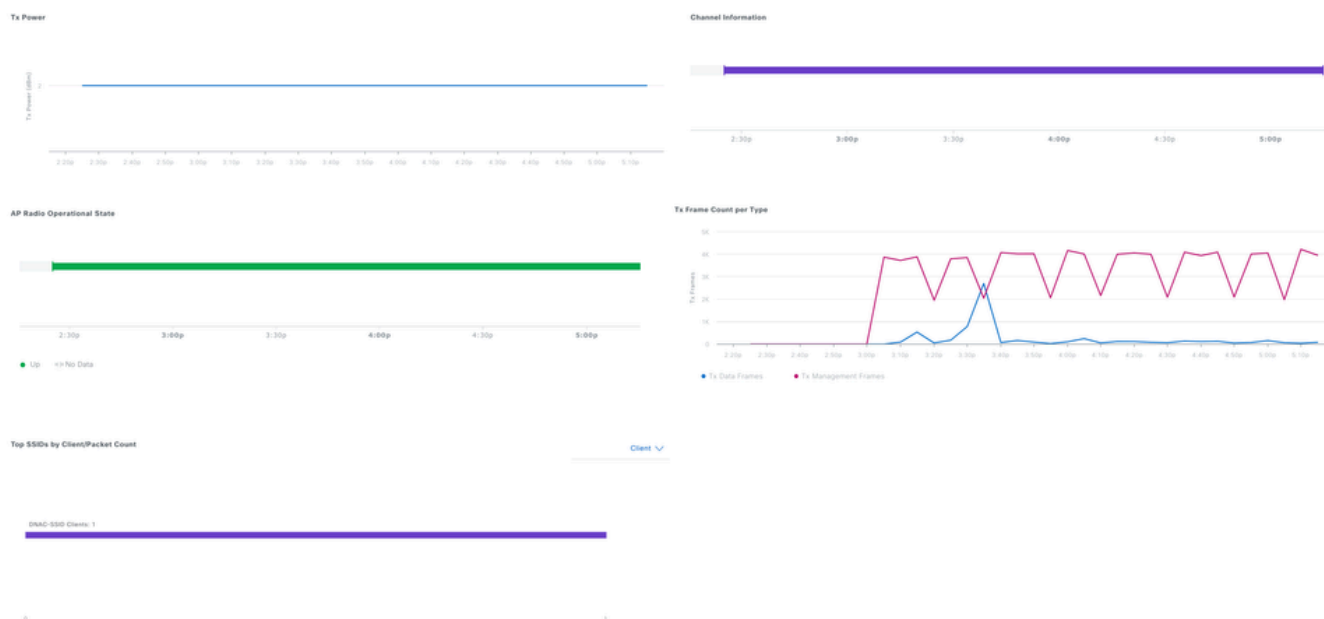
Dettagli dispositivo per AP

Indicatori KPI specifici per la radio: In questa finestra è possibile visualizzare gli indicatori KPI a livello di radio, tra cui l'utilizzo del canale, il numero di client, la velocità effettiva (frequenza Rx/Tx), i tentativi, il rumore e la qualità dell'aria per la radio selezionata.



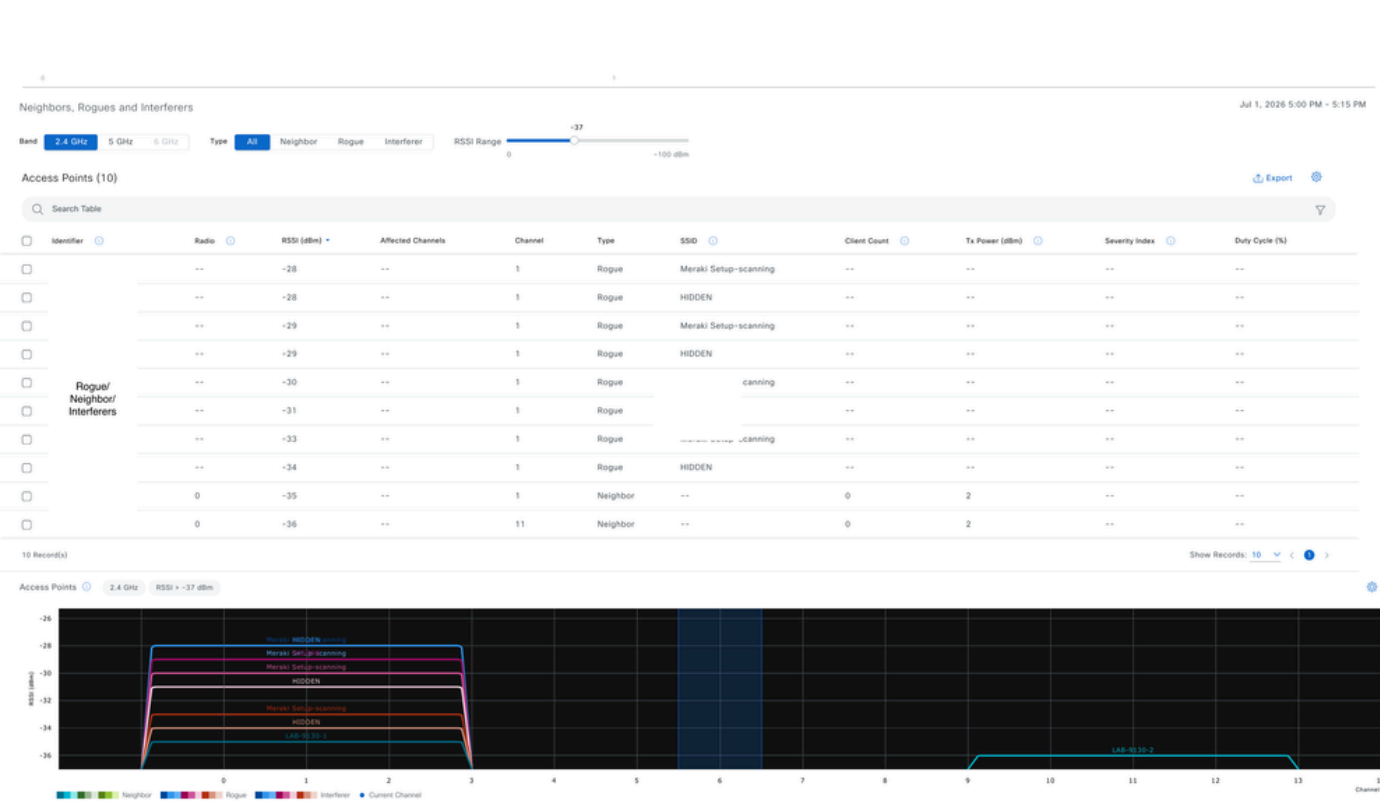
Statistiche RF per singolo access point

Alimentazione Tx, informazioni sul canale e stato del frame: in questa schermata è possibile visualizzare le tendenze dell'alimentazione Tx, la cronologia delle assegnazioni dei canali, lo stato operativo della radio AP, il numero di frame Tx per tipo (dati rispetto alla gestione) e i primi SSID per client/numero di pacchetti.



Statistiche RF per singolo access point

Vicini, nemici e interferenti: Questa vista consente di vedere tutti i dispositivi vicini, non autorizzati e interferenti con i relativi RSSI, canali interessati, SSID, conteggio client, potenza Tx e indice di gravità, oltre a un plottaggio visivo RSSI-vs-channel.



Segnalati server non autorizzati, adiacenti e interferenti per singolo access point

Il dashboard di Device 360 riunisce i dettagli relativi alla radiofrequenza, ad esempio l'utilizzo, l'interferenza, il rumore e i tentativi di connessione, oltre alle informazioni sugli elementi adiacenti, i dispositivi non autorizzati e gli interferenti, in modo da determinare se un problema del punto di accesso è causato da congestione della radiofrequenza, conflitti di canale o dispositivi non autorizzati. I dati sullo stato del dispositivo, quali CPU, memoria, cronologia dei riavvii e stato della connettività, insieme al Visualizzatore eventi e al pannello Problemi, consentono di comprendere arresti anomali dell'hardware, interruzioni di connessione e modifiche impreviste dei canali. In combinazione con la topologia e le visualizzazioni dei client, questo fornisce un quadro completo per la risoluzione dei problemi, dai problemi di RF a quelli dei singoli client, con le azioni consigliate incorporate per risolverli

Acquisizioni intelligenti per access point

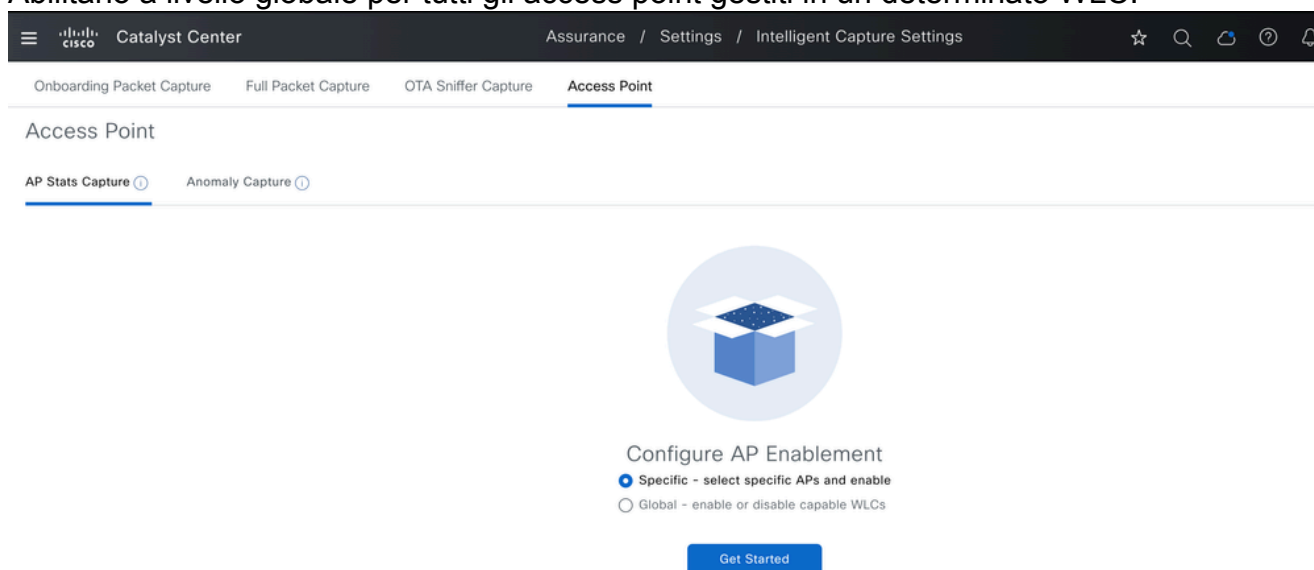
L'acquisizione intelligente dei dati per il punto di accesso offre due funzioni principali: monitoraggio RF in tempo reale sempre attivo, rilevamento di anomalie e acquisizione via etere on demand, analisi dello spettro.

Acquisizione statistiche AP

È possibile abilitare e gestire la raccolta dei dati delle statistiche AP per uno o più punti di accesso, incluse le statistiche radio AP, le statistiche WLAN e le statistiche client AP, con il supporto per un massimo di 1000 punti di accesso.

Per abilitare l'acquisizione delle statistiche AP, selezionare Assurance > Settings > Intelligent Capture Settings > Access Point > AP Stats Capture (Assurance > Impostazioni > Impostazioni di acquisizione intelligente > Punto di accesso > Acquisizione statistiche AP). Da qui, è possibile:

- Abilitarlo per punti di accesso specifici (fino a 1000) oppure
- Abilitarlo a livello globale per tutti gli access point gestiti in un determinato WLC.



Opzione di acquisizione statistiche AP

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

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

Find Hierarchy [Search Help](#)

- Global
 - 9800-CL
 - BGL SDA
 - Guru
 - Karnataka

Enabled APs (1) **Disabled APs (11)** Not-Ready APs (0)

AP_NAME

1 Selected **Enable**

<input checked="" type="checkbox"/>	Access Point	Device Type	OS Version	Overall Health Score	Client Count	Configuration Status
<input checked="" type="checkbox"/>	AP_NAME	C9130AXI-D	17.15.4.160	Down	--	--

Abilita acquisizioni intelligenti delle statistiche AP in un punto di accesso specifico

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**

<input checked="" type="checkbox"/>	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

Abilita acquisizione intelligente delle statistiche AP a livello globale

Dopo aver abilitato l'acquisizione delle statistiche dell'access point, Catalyst Center invia la configurazione corrispondente al WLC, sia per gli access point specifici selezionati che per tutti, a seconda che sia stata abilitata a livello di singolo access point o a livello globale al WLC.

WLC.podxl.cisco.com

Device IP: 10.127.197.194 Site: Global/Cisco BGL Cam

Configurations - Side by side view

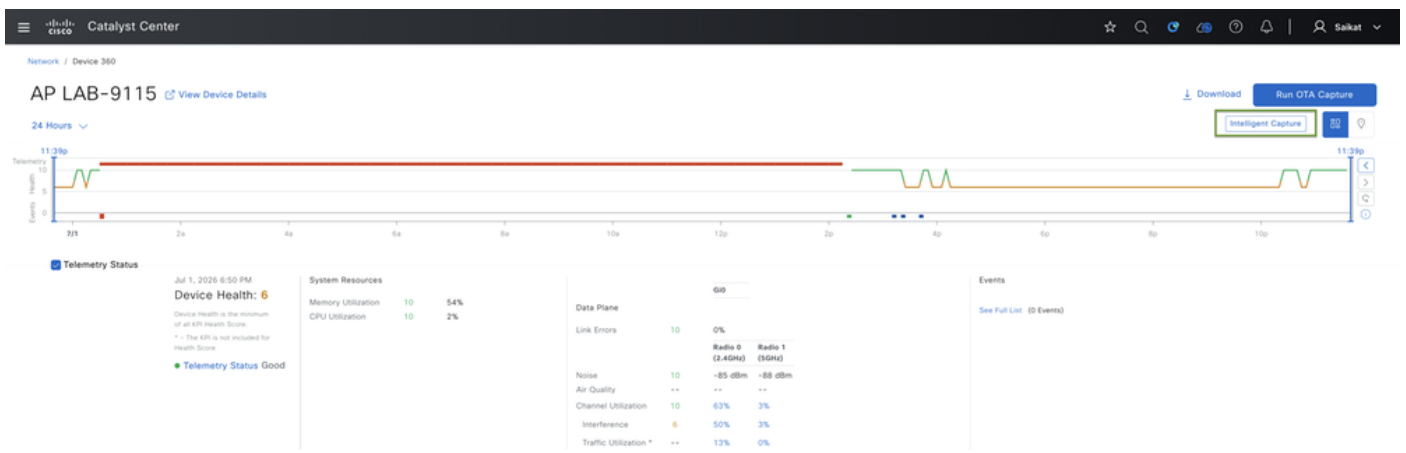
View by Configuration Source • All

Configuration to be Deployed 8 Line(s)

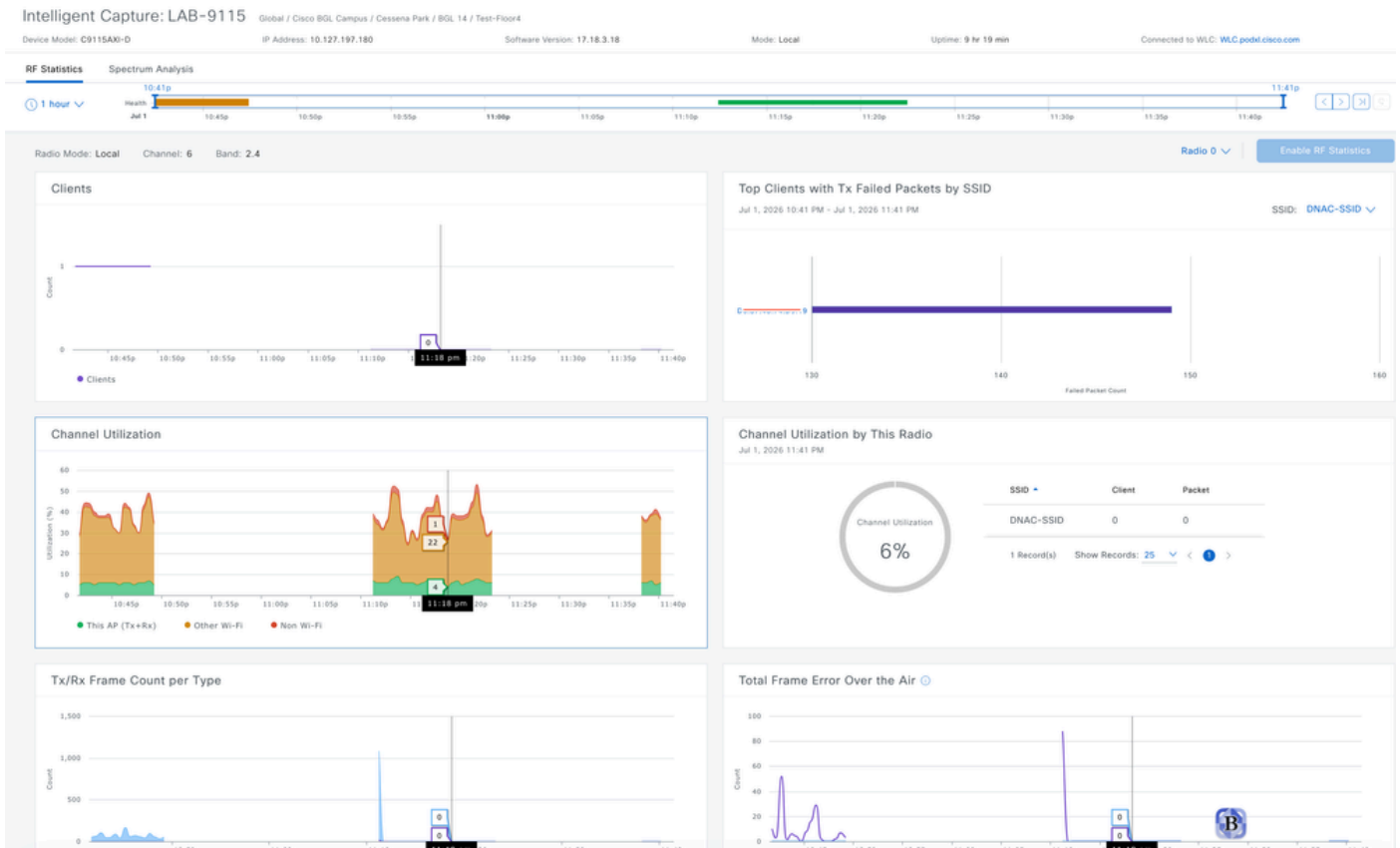
```
1 ap profile "default-ap-profile"
2 icap subscription client statistics enable
3 icap subscription ap statistics radio enable
4 icap subscription ap statistics wlan enable
5 icap subscription client statistics frequency
6 icap subscription ap statistics radio frequenc
7 icap subscription ap statistics wlan frequency
8 exit
```

Configurazione da sottoporre a push quando è abilitata l'acquisizione dello stato del punto di accesso

Dopo aver abilitato l'acquisizione, è possibile visualizzare i dati in tempo reale raccolti tramite Intelligent Capture direttamente dalla pagina Device 360. Inoltre, è possibile eseguire l'analisi dello spettro su richiesta per analizzare ulteriormente le condizioni RF.



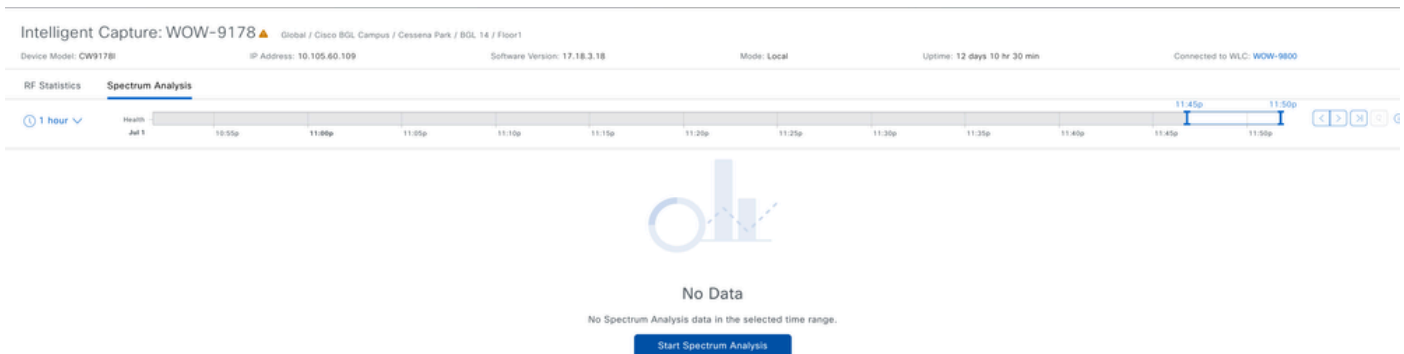
Acquisizione intelligente per AP nella periferica 360



Statistiche AP acquisite con Intelligent Capture su Catalyst Center

Qui è possibile vedere le statistiche in tempo reale che coprono il numero di frame Tx/Rx per tipo, il totale degli errori di frame via etere, i contatori multicast/broadcast, l'alimentazione Tx e la soglia del rumore, l'utilizzo dei canali, i primi client con pacchetti Tx guasti tramite SSID e i dati dei client acquisiti per un punto di accesso specifico tramite l'acquisizione intelligente.

È inoltre possibile eseguire analisi dello spettro su richiesta per un singolo punto di accesso ogni volta che è necessario ispezionare le condizioni RF. Tuttavia, questa funzionalità richiede il supporto del modello AP.



Analisi dello spettro su richiesta

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

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 icap subscription ap rf spectrum enable
2 do ap name WOW-9178 icap subscription ap rf spectrum slot 0
3 do ap name WOW-9178 icap subscription ap rf spectrum slot 1
4 do ap name WOW-9178 icap subscription ap rf spectrum slot 2
5 do ap name WOW-9178 icap subscription ap rf spectrum slot 3
```

Deploy

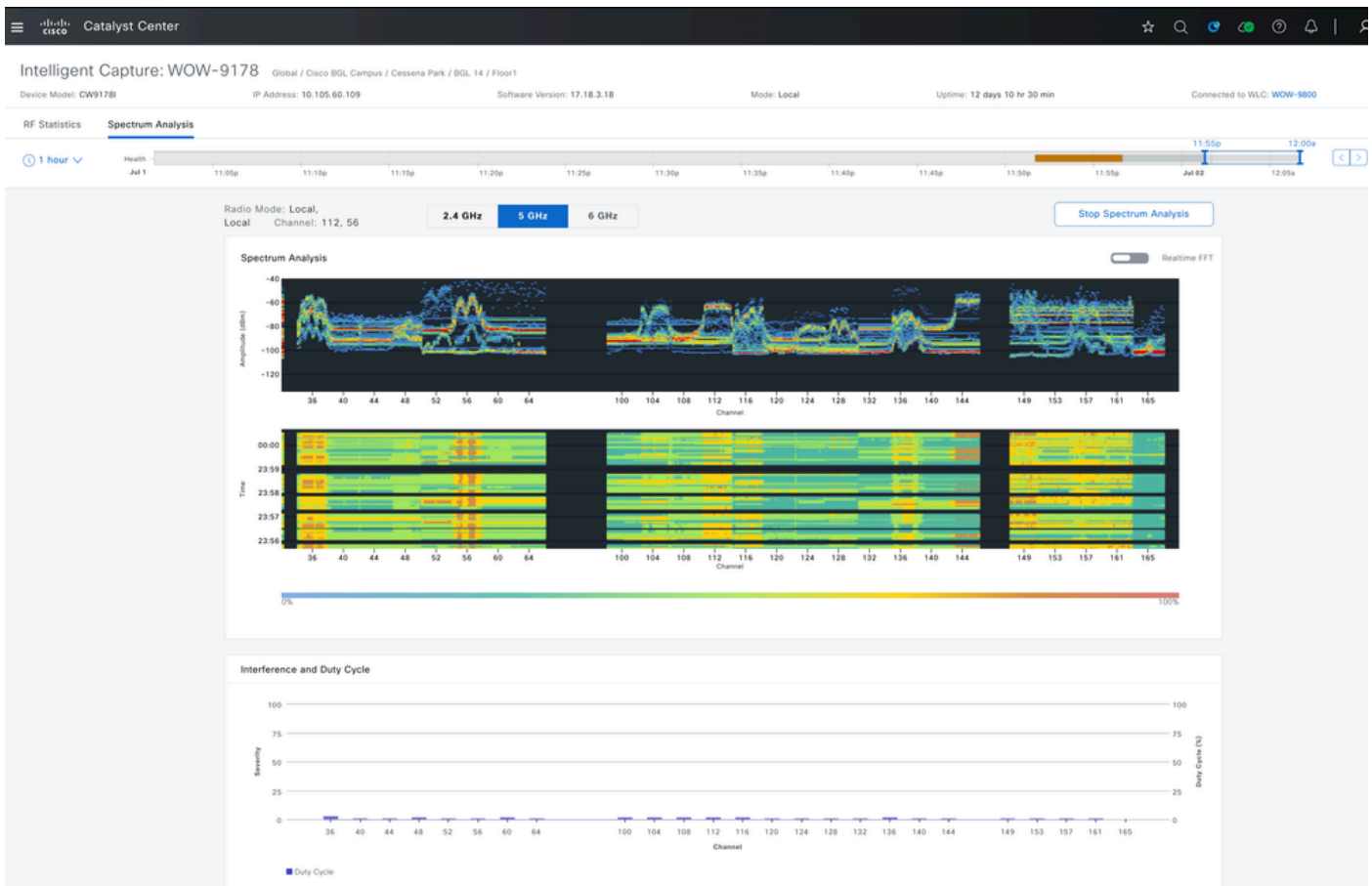
Now Later

Task Name*

Enable Spectrum on WOW-9178

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

Configurazione applicata per l'analisi dello spettro



Risultato analisi multicolore

OTA Sniffer Capture

Catalyst Center consente di abilitare l'acquisizione OTA Sniffer su una radio, una larghezza di banda e un canale specifici. Una volta abilitati, tutti i pacchetti di dati Wi-Fi che viaggiano su quella radio e canale vengono catturati. È possibile selezionare fino a 2 punti di accesso per eseguire l'analisi. Tenere presente che i due access point configurati per l'analisi del traffico possono passare alla modalità sniffer sulla rispettiva radio/slot finché è abilitata l'acquisizione OTA.

Per abilitare questa funzione, selezionare Provisioning > Inventario > Access Point, fare clic

sull'access point per il quale si desidera raccogliere i dati OTA, quindi selezionare Esegui acquisizione OTA. È possibile scegliere fino a 2 access point vicini per analizzare il traffico.



Esegui acquisizione OTA su access point di destinazione

Run OTA Capture




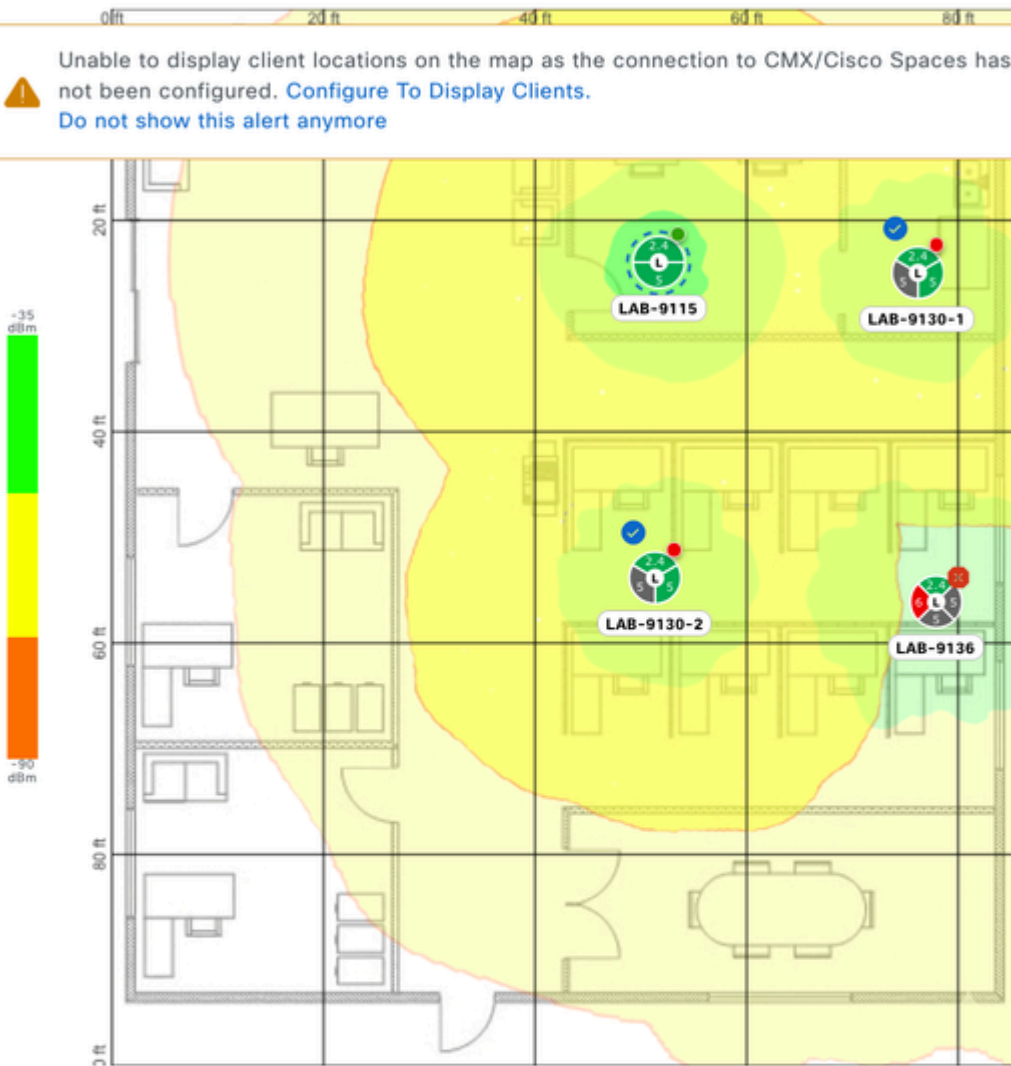
Select Access Points

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

Selezione dei punti di accesso adiacenti (fino a 2) per l'analisi del traffico

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

Seleziona radio, larghezza canale, canale per sniffare il traffico

The screenshot shows the Catalyst Center configuration interface for a device with IP 10.127.197.194. The interface is split into two main sections: 'Configuration to be Deployed' and 'Running Configuration'. The left sidebar shows the device name 'WLC.podxl.cisco.com'. The top navigation bar includes 'Activities / Tasks' and a search bar. The 'Configuration to be Deployed' section shows 12 lines of configuration, including commands for shutting down radios, setting channel widths, and enabling sniffing on specific channels. The 'Running Configuration' section shows 2221 lines of configuration, including system settings, boot system commands, and platform qfp utilization monitoring.

Anteprima di configurazione per l'attivazione dell'acquisizione OTA

The screenshot shows the Catalyst Center Audit Logs interface. The top navigation bar includes 'Activities / Tasks' and a search bar. The left sidebar shows a summary of tasks, including 'Type (2)', 'Status (7)', 'Review Status (1)', and 'Last Updated (3)'. The main content area displays a list of tasks. The first task is 'ICAP disable: OTA LAB-9130-1 WLC.podxl.cisco.com', which is currently 'Upcoming'. The second task is 'Start OTA Capture for AP LAB-9115', which is 'Completed' with a 'Success' status. The interface includes a search bar and a filter for 'Update - Latest first'.

Attività pianificata quando l'acquisizione OTA è abilitata

Cisco Catalyst 9800-80 Wireless Controller

Welcome admin

Search APs and Clients

Feedback

Configuration > Wireless > Access Points

All Access Points

Total APs : 4

Misconfigured APs: Tag : 0, Country Code : 0, LSC Fallback : 0, URWB : 0

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	Con...
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

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 modalità sniffer per l'access point abilitato per l'analisi del traffico

Per controllare lo stato di esecuzione dell'acquisizione OTA, selezionare 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

Selected	Sniff Target AP	Wireless Controllers	Start Time	End Time	Duration
<input checked="" type="checkbox"/>	LAB-9115	WLC.podxl.cisco.com	Jul 2, 2026 12:05 AM	Jul 2, 2026 12:20 AM	15 min
<input checked="" type="checkbox"/>	LAB-9115	WLC.podxl.cisco.com	Jul 2, 2026 12:05 AM	Jul 2, 2026 12:20 AM	15 min

Stato dell'acquisizione OTA



Nota: Per impostazione predefinita, Catalyst Center esegue questa attività per 15 minuti prima di disattivarla automaticamente, ma può anche essere interrotta manualmente in qualsiasi momento.

Una volta completata l'acquisizione OTA, questa viene visualizzata nella sezione Acquisizioni completate, da cui è possibile scaricare il file.

Sniff Target AP	Wireless Controllers	Start Time	End Time	Download	Duration
LAB-9136	WLC.podxl.cisco.com	Jul 1, 2026 06:32 PM	Jul 1, 2026 06:47 PM	↓	15 min
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

Acquisizione completata - Acquisizione Sniffer OTA

Rilevamento anomalie

Questa funzione consente agli access point Cisco di rilevare possibili irregolarità nel comportamento dei client wireless ad essi associati. Esso comprende:

- Rilevamento anomalie
- Anomaly Packet Capture
- Report singoli anomali
- Report di riepilogo delle anomalie

Per abilitare l'acquisizione anomala AP, selezionare Assurance > Settings > Intelligent Capture Settings > Access Point > Anomaly Capture. Da qui, è possibile:

- Abilitarlo per punti di accesso specifici (fino a 1000) oppure
- Abilitarlo a livello globale per tutti gli access point gestiti in un determinato WLC.

Una volta abilitata, Intelligent Capture raccoglie e presenta automaticamente un comportamento anomalo per i client associati a tali punti di accesso. I dati possono essere visualizzati nella pagina Client Intelligent Capture.

The screenshot shows the 'Intelligent Capture Settings' page in the Cisco Catalyst Center. Under the 'Access Point' section, the 'Anomaly Capture' option is selected. A text box explains that Intelligent Capture automatically collects and presents anomalous behavior for clients associated with enabled Access Points. Below this, there is a 'Configure AP Enablement' section with two radio button options: 'Specific - select specific APs and enable' (which is selected) and 'Global - enable or disable capable WLCs'. A 'Get Started' button is located at the bottom of this section.

Configura acquisizione anomalie

The screenshot shows the 'Access Point' configuration page in Catalyst Center. The 'Anomaly Capture' tab is active, and the 'Specific - select specific APs and enable or disable' radio button is selected. A search hierarchy on the left shows the path: Global > Cisco BGL Campus > 9800-Site-2 > CALD > Cessena Park > Mesh > Malaysia > UK. The main table displays a list of access points with columns for Access Point, Device Type, OS Version, Overall Health Score, Client Count, and Configuration Status. The AP LAB-9115 is selected and highlighted in blue.

Access Point	Device Type	OS Version	Overall Health Score	Client Count	Configuration Status
LAB-9130-1	C9130AXI-D	17.18.3.18	1	0	--
LAB-9130-2	C9130AXI-D	17.18.3.18	1	0	--
LAB-9136	C9136I-ROW	17.18.3.18	6	0	--
LAB-9115	C9115AXI-D	17.18.3.18	10	1	--

Abilita acquisizione anomalie per punto di accesso specifico

The screenshot shows the 'Access Point' configuration page in Catalyst Center. The 'Global - select specific WLCs and enable' radio button is selected. A search bar contains 'WLC.podxl.cisco.com'. The main table displays a list of WLCs with columns for Device Name, Configuration Status, IP Address, Model, OS Version, Overall Health, and Location. The WLC WLC.podxl.cisco.com is selected and highlighted in blue.

Device Name	Configuration Status	IP Address	Model	OS Version	Overall Health	Location
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

Abilita acquisizione anomalie a livello globale per WLC specifici

The screenshot shows the 'Activities / Tasks' page in Catalyst Center. The 'Task Details / Work Item Details' section is active, showing the configuration for the WLC WLC.podxl.cisco.com. The 'Configurations - Side by side view' section displays the configuration to be deployed and the running configuration. The configuration to be deployed is a 6-line configuration snippet for anomaly detection on AP LAB-9115. The running configuration is a 17-line configuration snippet showing the current configuration for the WLC.

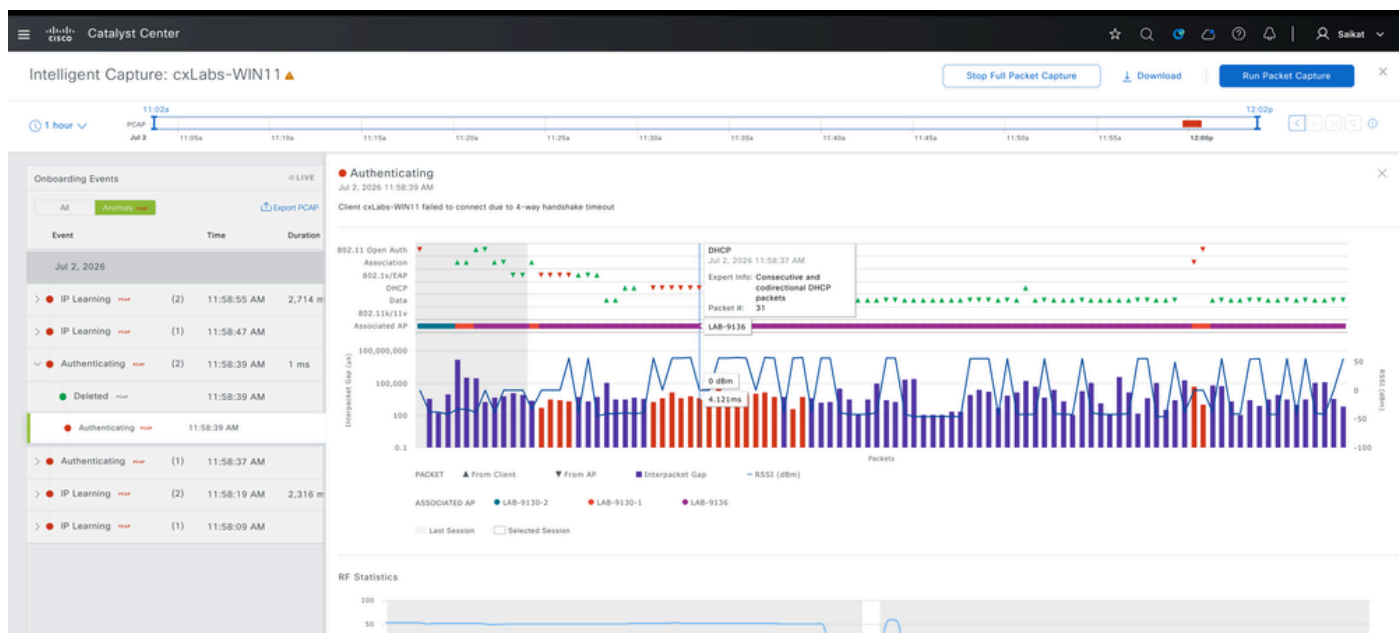
```

Configuration to be Deployed
6 Line(s)
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

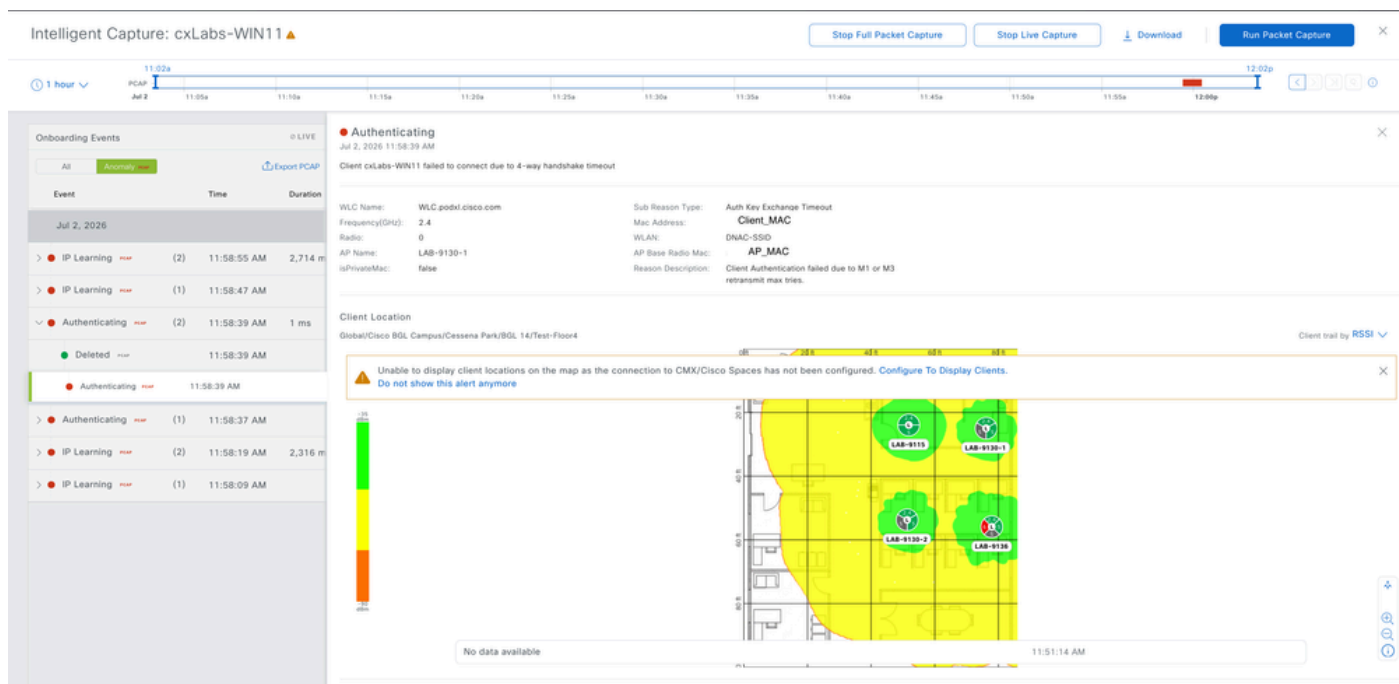
Running Configuration
2243 Line(s)
1 Building configuration...
2
3 Current configuration : 85499 bytes
4 !
5 Last configuration change at 06:16:02 UTC Thu Jul 2 2026 by ad
6 !
7 version 17.18
8 service timestamps debug datetime msec
9 service timestamps log datetime msec
10 service internal
11 platform 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
    
```

Anteprima configurazione per acquisizione anomalie

Una volta abilitato, raccoglie continuamente comportamenti anomali per i client associati all'access point, che possono essere visualizzati all'interno delle acquisizioni intelligenti (onboarding e complete) prese per gli ID client specifici.



Visualizzazione acquisizione anomalie per il client



Dettagli acquisizione anomalie per il client

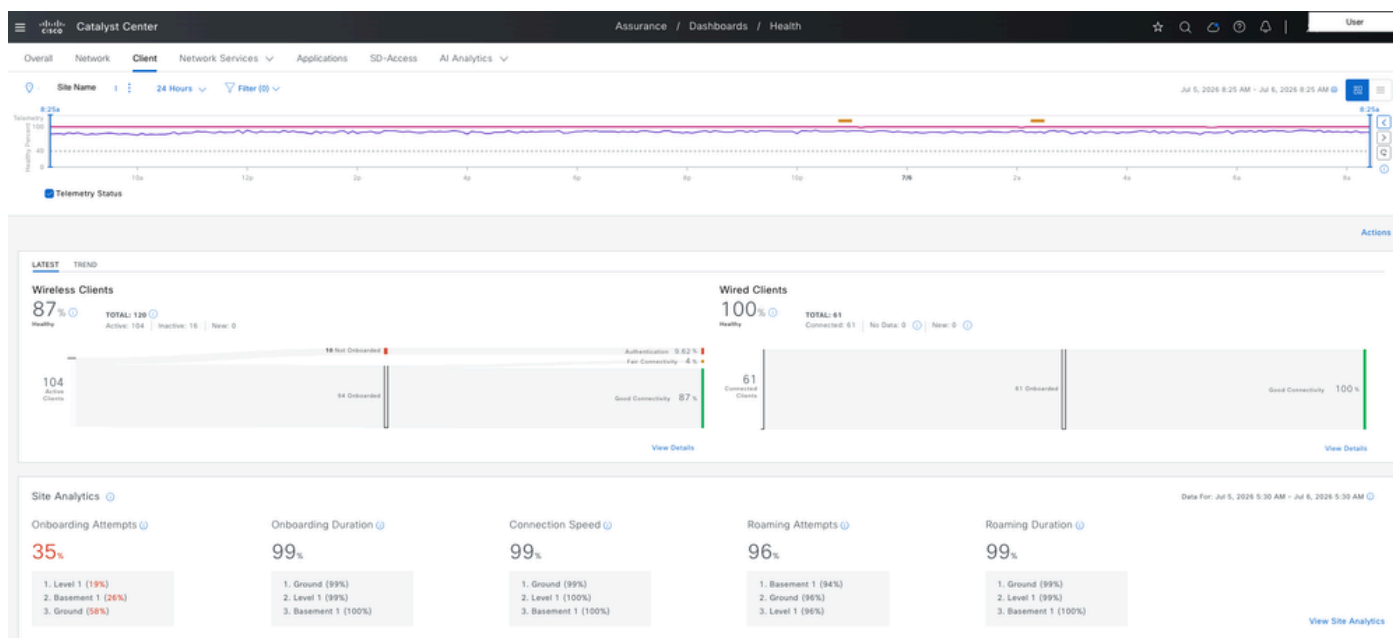
In questo modo è possibile risolvere i problemi relativi a comportamenti client irregolari o imprevisti, ad esempio errori di caricamento, problemi di autenticazione o modelli di associazione anomali, rilevando e contrassegnando automaticamente questi eventi per i punti di accesso in cui sono attivati. In combinazione con l'onboarding e l'acquisizione di pacchetti completi per ID client

specifici, consente agli amministratori di tracciare l'esatta sequenza di eventi che portano a un'anomalia, rendendo più facile individuare le cause principali dei problemi ricorrenti di connettività o prestazioni dei client senza dover monitorare manualmente ogni sessione client.

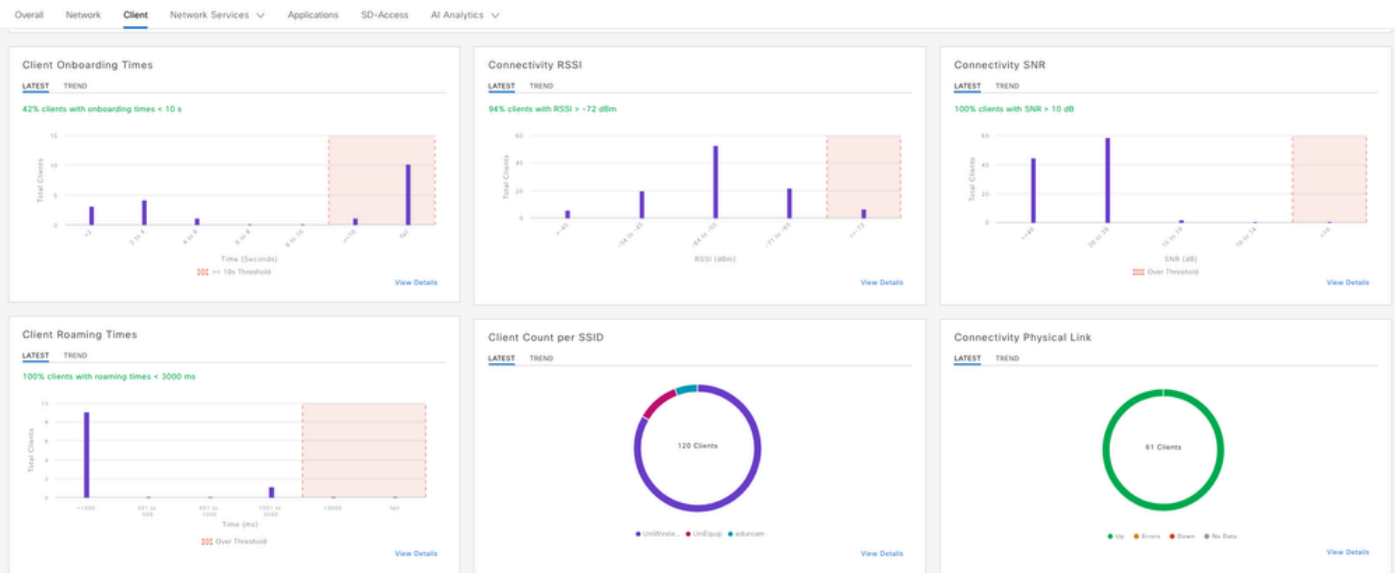
Problema di connettività client wireless

I problemi dei client wireless (errori di caricamento, cali di roaming, interferenze RF o connettività intermittente) sono spesso transitori e difficili da riprodurre, il che rende il monitoraggio tradizionale basato sul polling insufficiente per la risoluzione dei problemi di Cisco Catalyst Center colma questa lacuna tramite la telemetria continua di un secondo (al secondo) raccolta direttamente dai punti di accesso e dai controller wireless, correlata nei flussi di lavoro di Device 360, Client 360 e Acquisizione intelligente. Questa architettura basata sulla telemetria consente di ricostruire le esatte condizioni RF e a livello di protocollo al momento del guasto, dall'utilizzo e dall'interferenza dei canali ai frame di caricamento 802.11.

La sezione Integrità client fornisce una panoramica completa e globale delle statistiche client wireless in tutti i siti. Questo include metriche chiave quali prestazioni di caricamento, RSSI, SNR, attività di roaming, distribuzione per SSID e per radio, velocità di trasferimento dati e stato della connettività fisica. È possibile filtrare questi dati in base a un sito specifico e visualizzare le tendenze cronologiche fino agli ultimi 30 giorni, offrendo una prospettiva a livello di rete e una granularità a livello di sito. Selezionare Assurance > Dashboard > Integrità > Client



Statistiche client wireless su Catalyst Center



Statistiche client wireless su 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

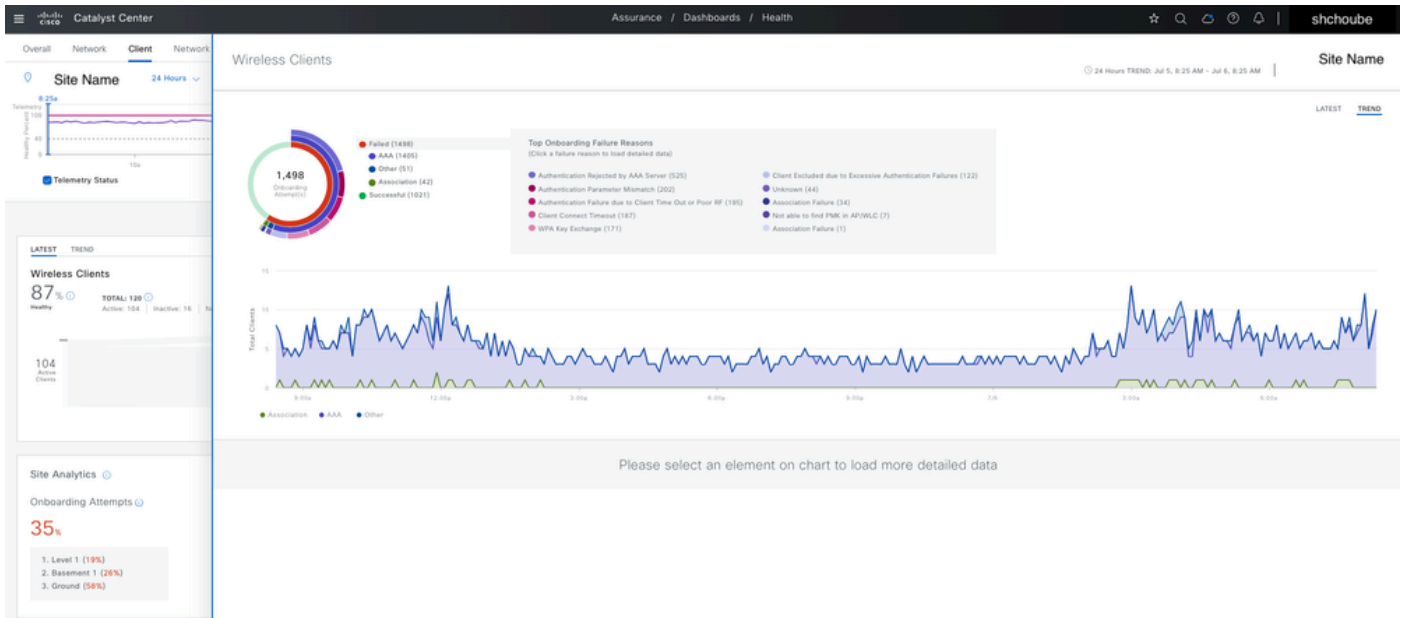
Search by name, MAC address, or IPv4/IPv6 address

0 Selected Actions

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	-68 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	3.146 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

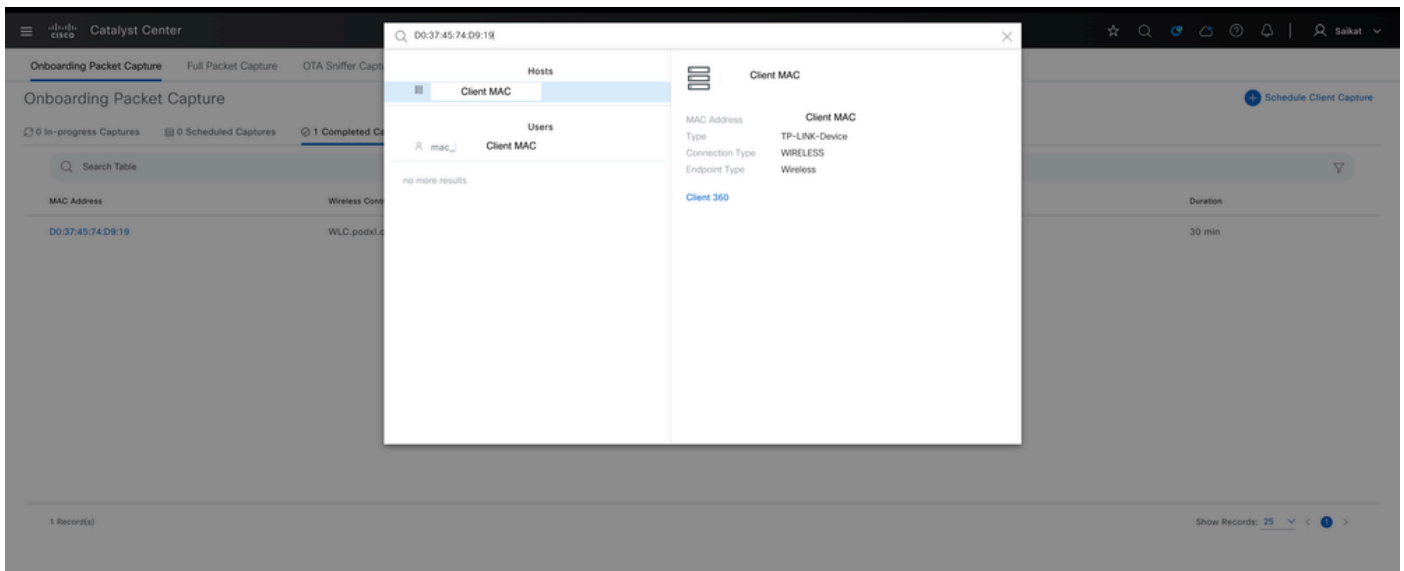
120 Record(s) Show Records: 50 1 - 50

Statistiche client wireless su Catalyst Center

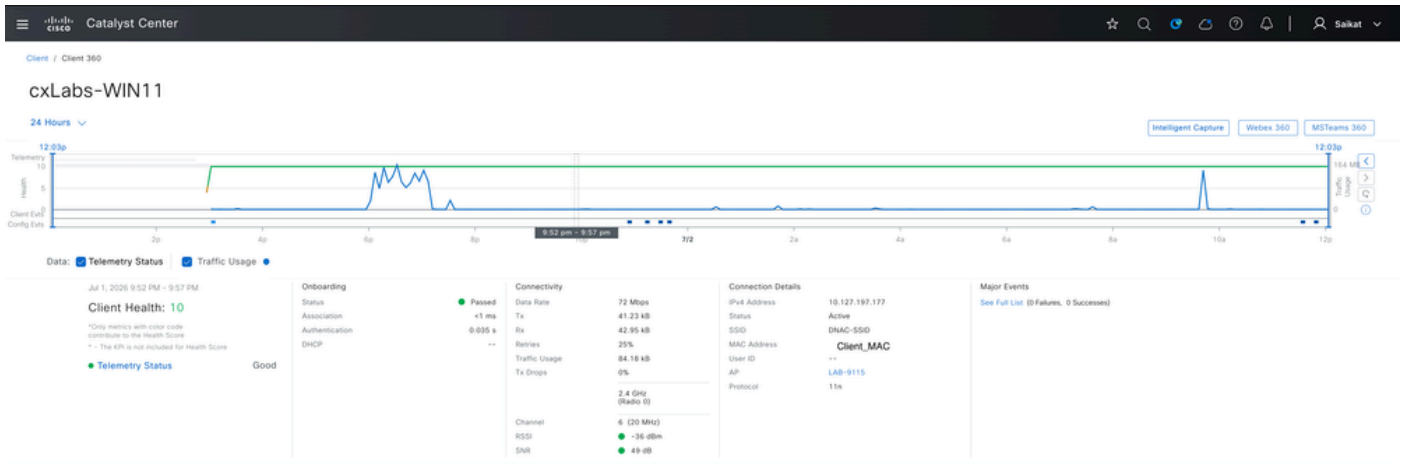


Statistiche client wireless su Catalyst Center

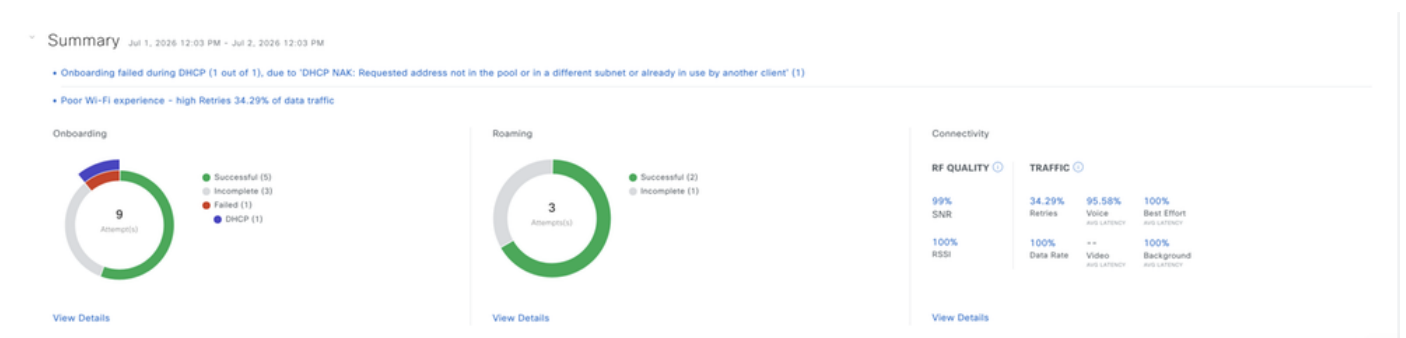
Per la risoluzione dei problemi di un client specifico, è possibile eseguire la ricerca utilizzando l'indirizzo MAC del client, che consente di passare alla visualizzazione Client 360. Questa pagina presenta statistiche dettagliate specifiche del client, tra cui la cronologia di caricamento, gli eventi di connettività, le metriche RF e i dettagli della sessione, con ambito esclusivo per il singolo client, consentendo l'analisi precisa della root cause dei singoli problemi del client.



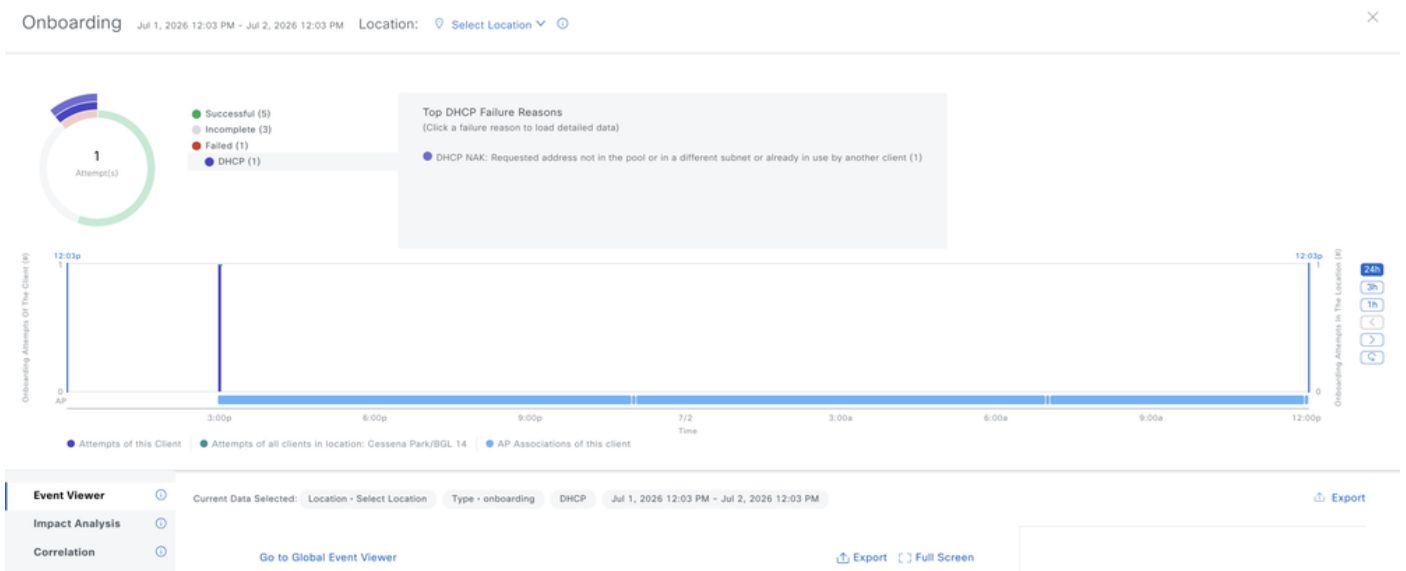
Dispositivo indirizzo Mac client specifico 360



Telemetria + stato del client



Riepilogo generale per il client



Evento riportato in dettaglio per il client

Detail Information Jul 2, 2026 12:03 PM

Device Info Connectivity RF

Information

Device Type	TP-LINK-Device
Operating System	--
User ID	--
Host Name	cxLabs-WN11
MAC Address	
IPv4 Address	10.127.197.177
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

Connection Information

WMM	--
U-APSD	--
Band	
Radio	
Spatial Streams	
Channel	

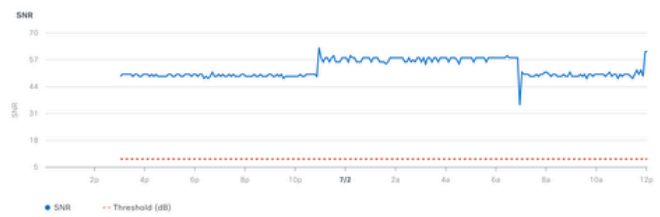
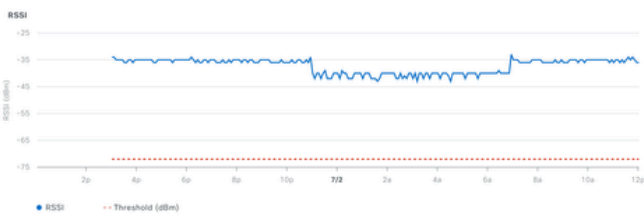
⚠ You haven't subscribed to the client notification yet. [Set up Subscription](#)

Dettagli dispositivo client

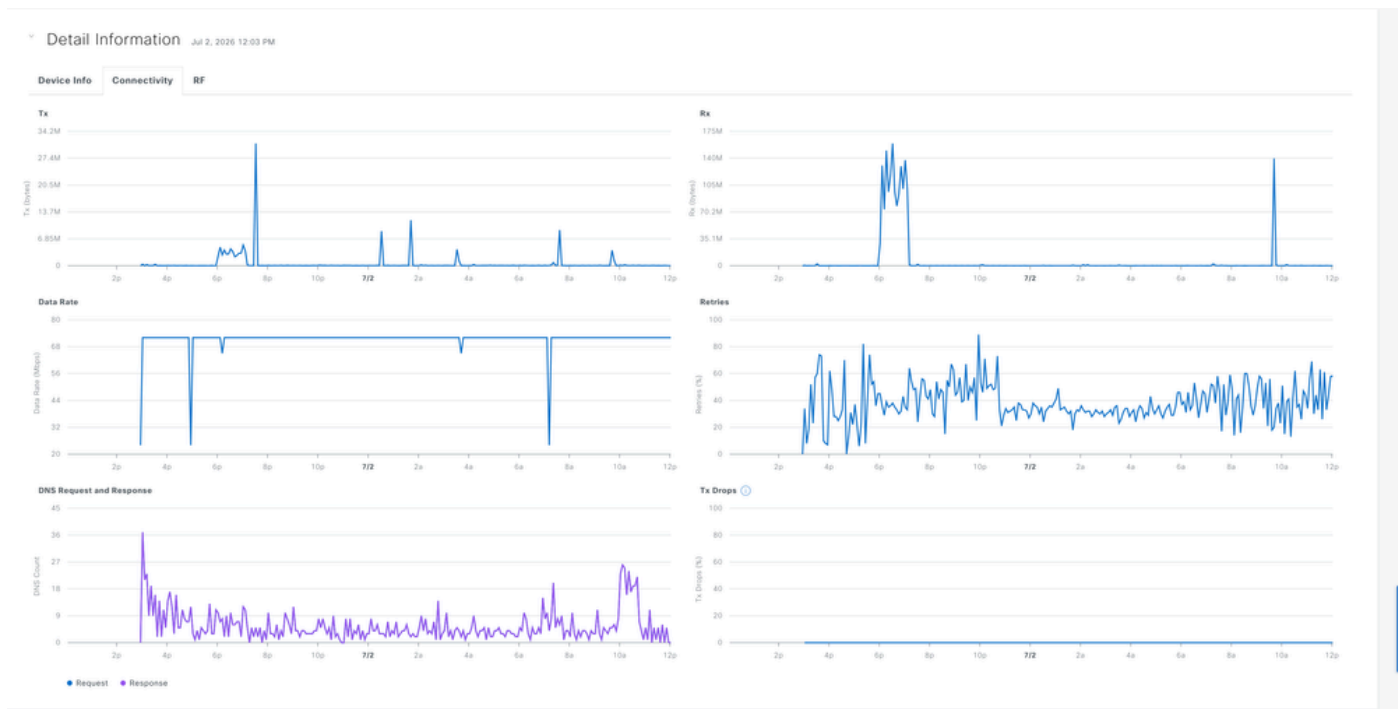
Detail Information Jul 2, 2026 12:03 PM

Device Info Connectivity RF

Aggregate Per Band



Statistiche RF per il client



Statistiche di connettività per client

Acquisizioni intelligenti per client wireless

Intelligent Capture (iCAP) aiuta a risolvere i problemi di connettività dei client wireless acquisendo dati reali a livello di pacchetto direttamente da Catalyst Center. Può acquisire frame di gestione 802.11, DHCP e EAP per individuare il punto in cui un tentativo di connessione non riesce, dati non crittografati e pacchetti di gestione per un client specifico per risolvere problemi di caricamento, accessibilità e applicazioni. È inoltre possibile pianificare l'esecuzione delle acquisizioni intelligenti in un secondo momento in base al requisito. La durata predefinita della sessione è di 30 minuti e può essere impostata fino a otto ore.

Acquisizione pacchetti in entrata

L'acquisizione dei pacchetti in entrata registra la sequenza di pacchetti scambiati da un dispositivo client durante il tentativo di connessione alla rete wireless, inclusi i frame di gestione 802.11 (come le richieste di associazione e autenticazione), i pacchetti DHCP e i pacchetti EAP utilizzati durante l'autenticazione 802.1X. Inoltre, raccoglie le statistiche RF dei client, dando visibilità alle condizioni del segnale nel momento esatto dell'imbarco. Queste acquisizioni sono utili per la risoluzione dei problemi di uno scenario in cui un client non riesce a connettersi e consentono di individuare con precisione la fase in cui si è verificato l'errore, durante l'associazione, l'autenticazione o l'assegnazione dell'indirizzo IP. Per impostazione predefinita, l'acquisizione pacchetti in entrata è abilitata sull'ultimo controller wireless connesso al client. È possibile selezionare fino a tre controller wireless per coprire lo scenario di roaming dei client.

Per abilitare l'acquisizione dei pacchetti in entrata, selezionare Assurance > Settings > Intelligent

Capture > Onboarding Capture > Schedule Client Capture (nell'angolo in alto a destra) > Search for Client Identifier (indirizzo Mac)

Schedule Client Capture

Select client devices: / cxLabs-WIN11 / Client_MAC

Host Names: cxLabs-WIN11, Client_MAC

MAC Addresses: Client_MAC

Device Name	IP Address	MAC Address	Reachability
<input type="checkbox"/> WLC-Saikat	10.105.60.89		Reachable
<input type="checkbox"/> itsmewlc	10.105.193.79		Reachable
<input checked="" type="checkbox"/> WLC.podxl.cisco.com	10.127.197.194	WLC_MAC_Address	Reachable
<input type="checkbox"/> wlc3504-saikat	10.105.60.87		Reachable
<input type="checkbox"/> WOW-9800	10.105.60.100		Reachable

Onboarding Packet Capture

1 In-progress Captures | 0 Scheduled Captures | 0 Completed Captures

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

Acquisizione di caricamento pianificata

Start Live Capture for D0:37:45:74:D9:19

Work Item · ASSURANCE_ICAP

Completed · Ready | Pending Review

Start: Jul 1, 2026 6:12 PM | End: Jul 1, 2026 6:12 PM | As of: 11:31:42 AM | Refresh

Device IP: 10.127.197.194 | Site: Global/Cisco BGL Campus/Ce... | Back to workflow progress

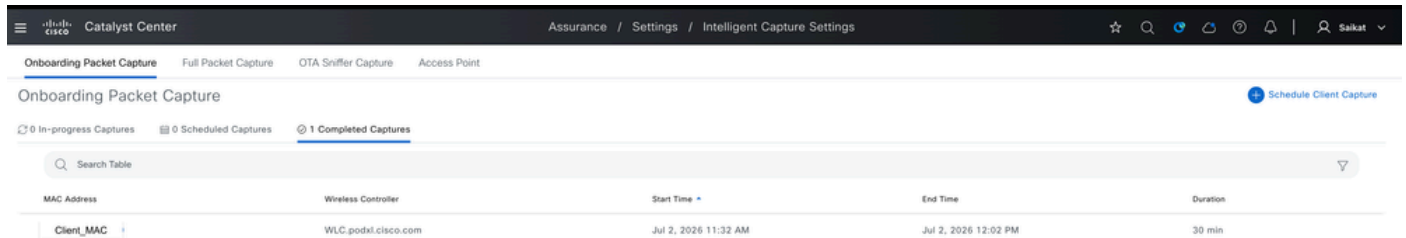
Configurations - Side by side view

View by Configuration Source · All

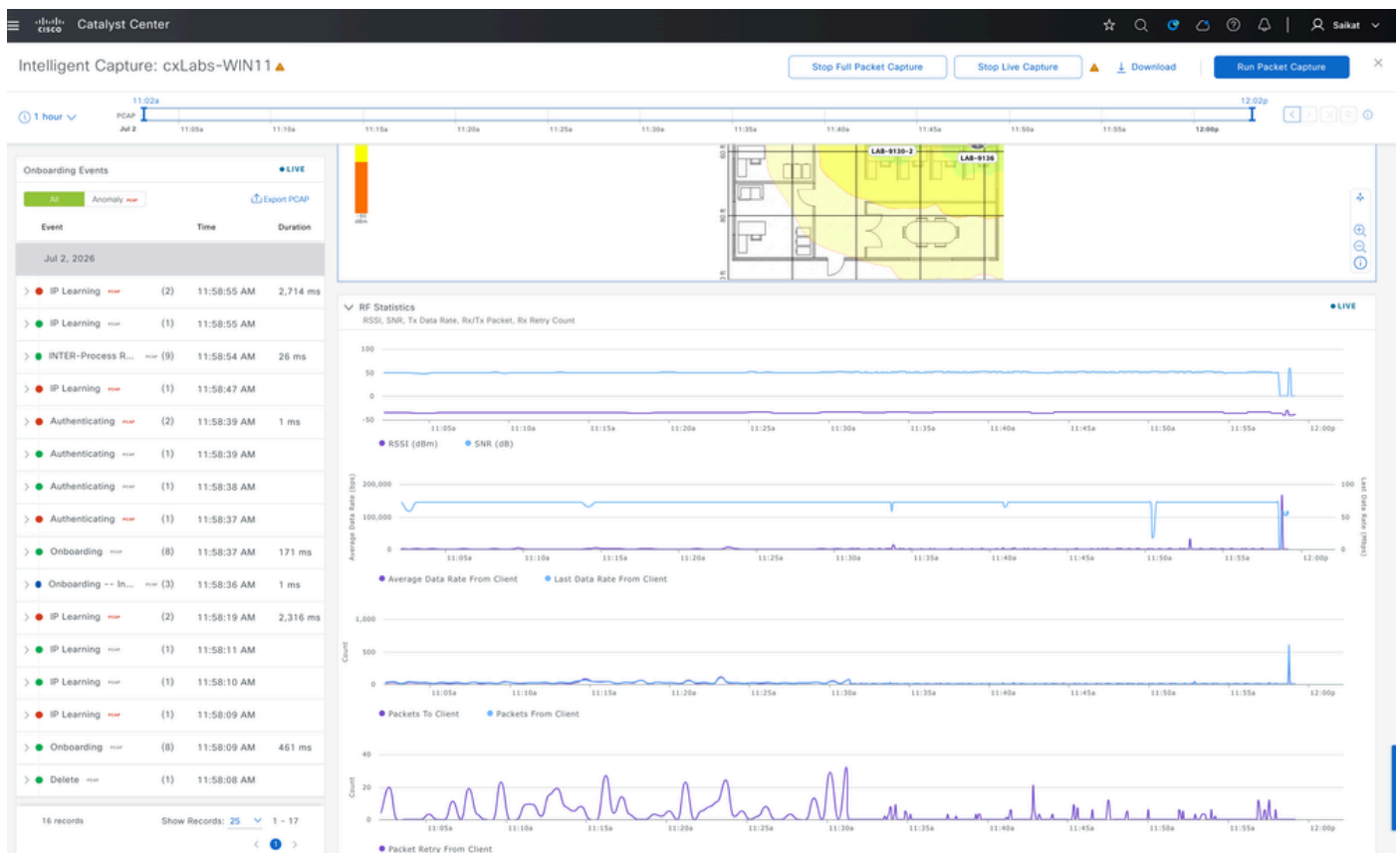
Configuration to be Deployed (10 Line(s))	Running Configuration (2221 Line(s))
<pre> 1 ap profile "default-ap-profile" 2 icap subscription client packet-trace partial enable 3 icap subscription client packet-trace partial filter protocol type all 4 icap subscription client packet-trace partial filter protocol type all 5 icap subscription client packet-trace partial filter protocol type 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 admin 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>

Anteprima configurazione per acquisizione incorporata

L'acquisizione di caricamento può essere interrotta manualmente o automaticamente una volta trascorsa la durata programmata (da 30 minuti a 8 ore). Una volta interrotta, l'acquisizione viene visualizzata in Acquisizioni completate, dove è possibile fare clic sull'indirizzo MAC dei clienti per visualizzare i dati di acquisizione dettagliati ed esportare il file in formato PCAP per ulteriori analisi.



Acquisizione di caricamento completata



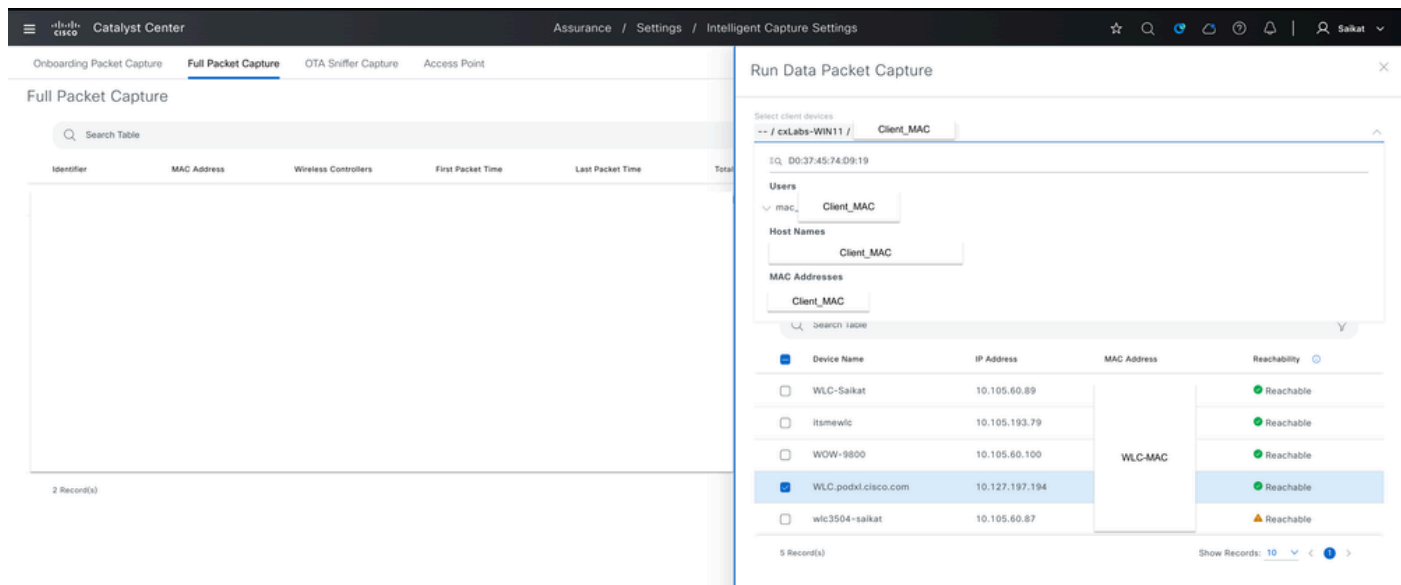
Esempio di acquisizione integrata completa

Acquisizione completa dei pacchetti

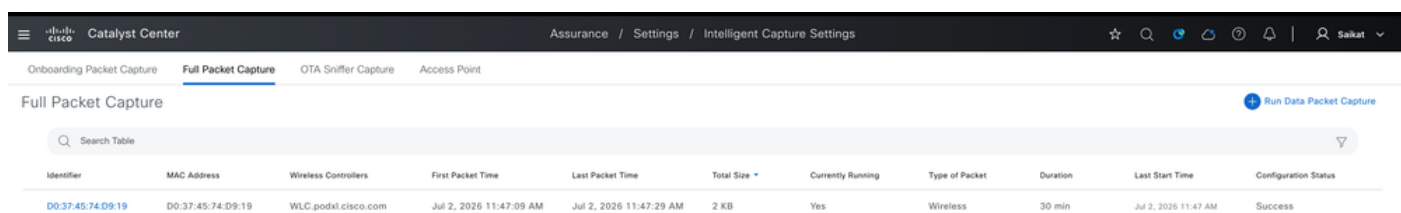
La sessione Full Packet Capture è in grado di acquisire dati completi per un client specifico, fornendo una visibilità completa a livello di pacchetto nel traffico wireless continuo del client, che

consente di ispezionare in dettaglio i pacchetti di dati e di gestione per risolvere problemi di accesso, problemi di prestazioni delle applicazioni o altre anomalie di connettività che vanno al di là di quanto possono rivelare le statistiche RF standard. È in grado di acquisire fino a 1 GB di dati in sequenza per un client specifico e di conservare in modo continuo fino al limite i dati più recenti.

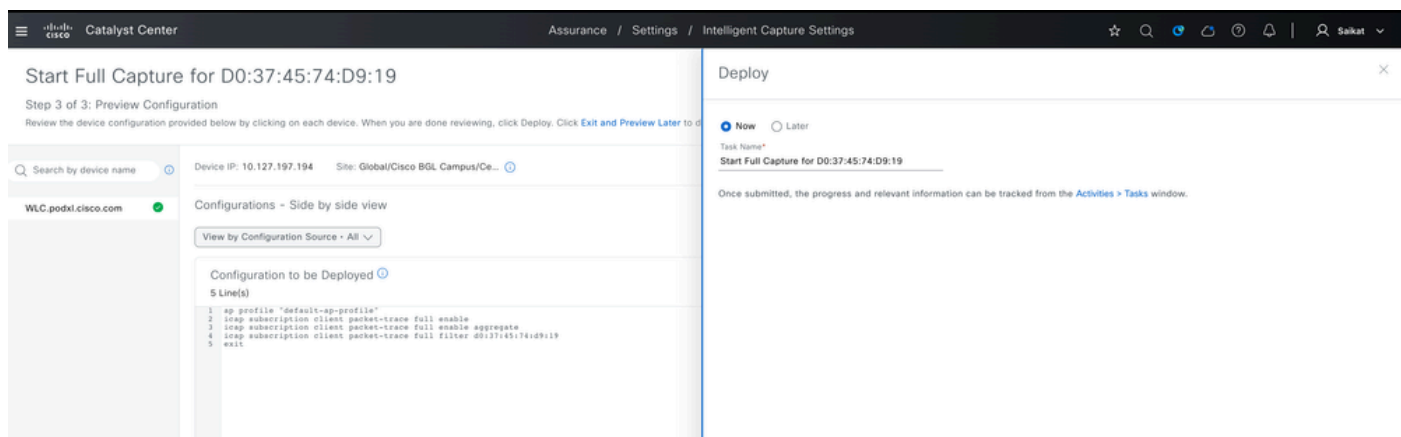
Per abilitare Full Packet Capture navigate to Assurance > Settings > Intelligent Capture Settings > Onboarding Capture > Run Data Capture (nell'angolo in alto a destra) > Search for Client Identifier (indirizzo Mac):



Acquisizione completa pacchetti per il client



Pianificazione dell'acquisizione completa dei pacchetti per il client



Anteprima di configurazione per l'acquisizione di pacchetti completi

L'acquisizione completa del pacchetto può essere interrotta manualmente o automaticamente una volta trascorsa la durata programmata (da 30 minuti a 8 ore). Una volta interrotta, l'acquisizione viene visualizzata sotto acquisizioni completate, dove è possibile fare clic sull'indirizzo MAC dei client per visualizzare i dati di acquisizione dettagliati ed esportare il file in formato PCAP per ulteriori analisi.

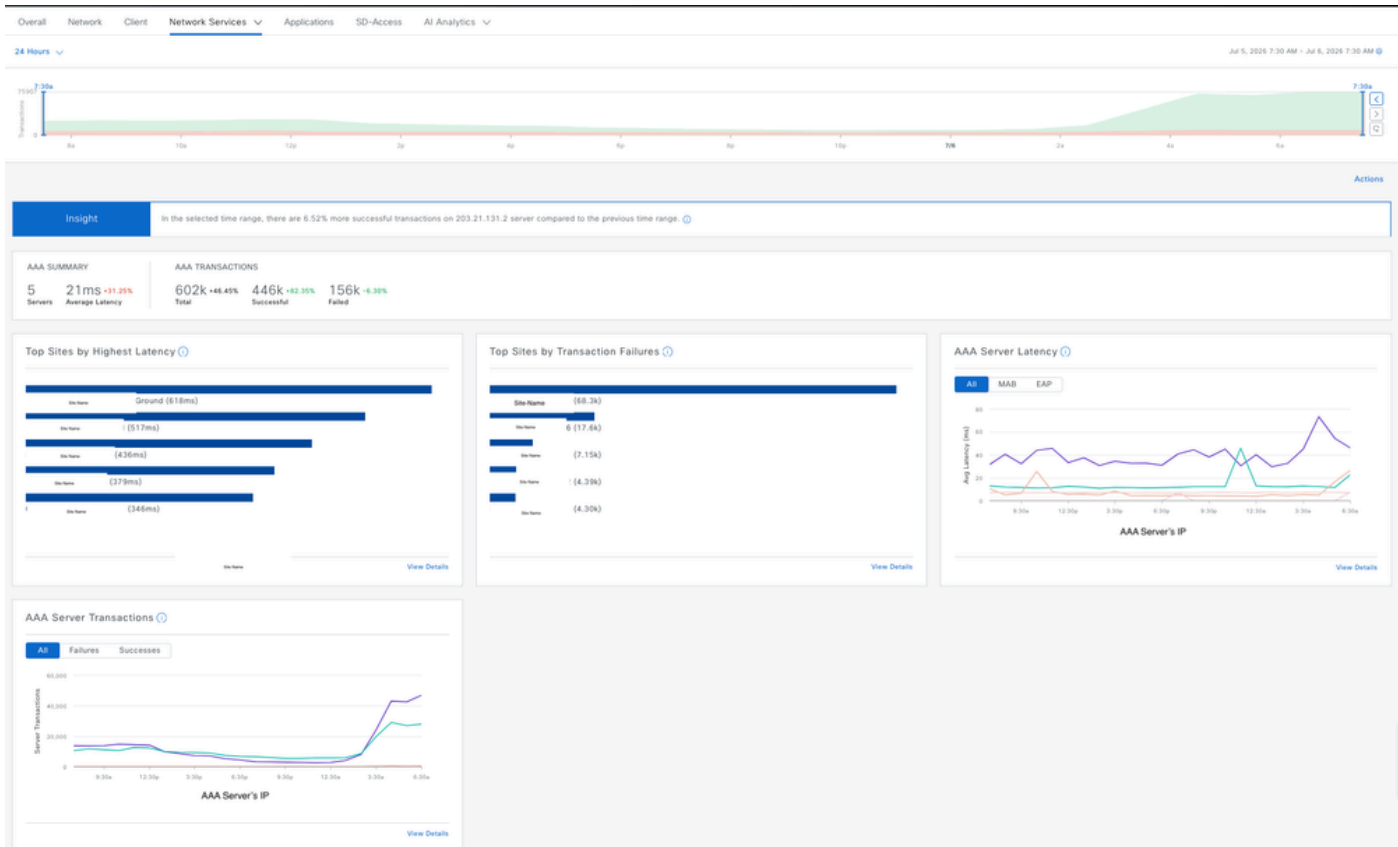


Esempio di acquisizione completa raccolta per il client

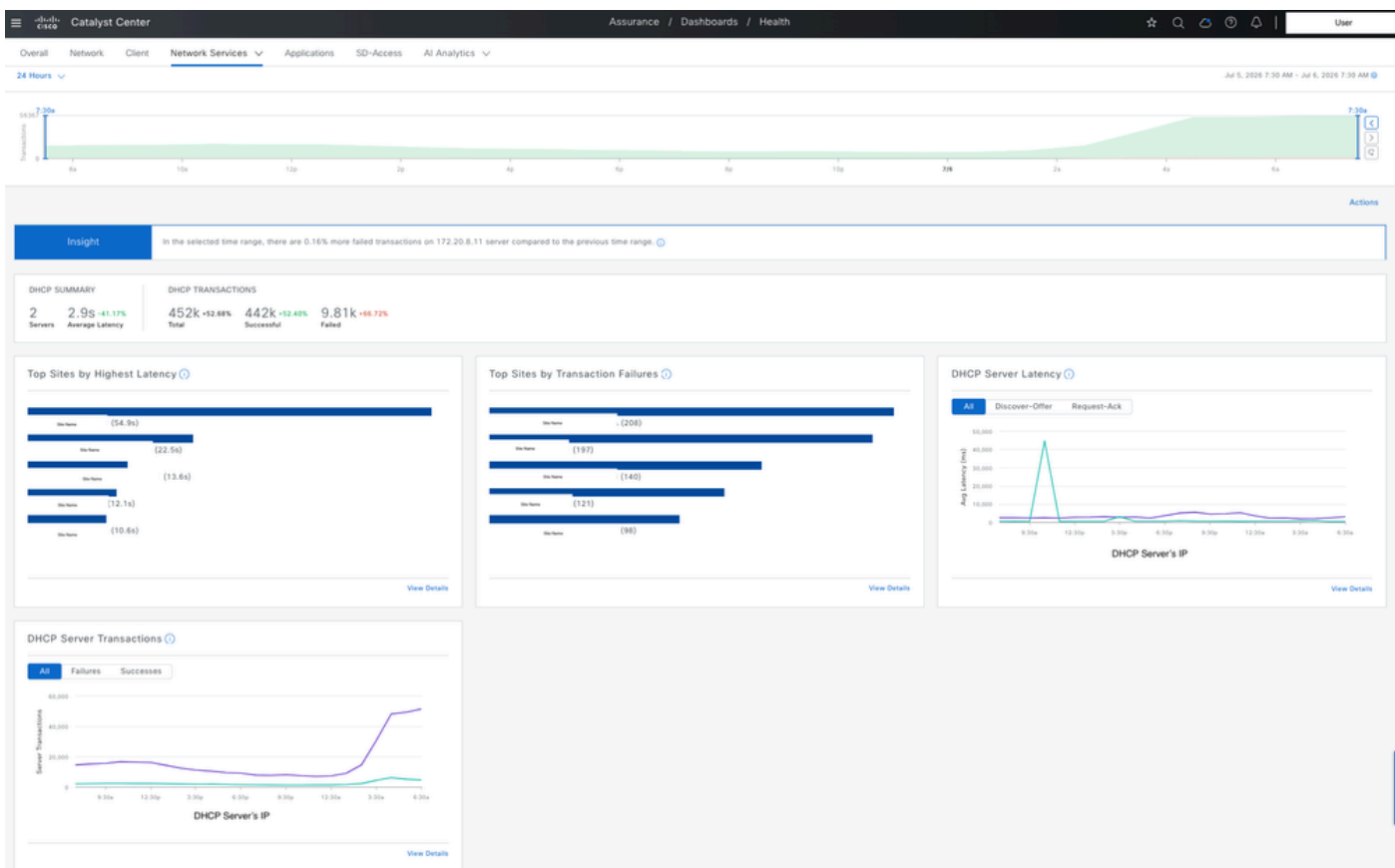
Isolamento dei problemi dei servizi di rete (AAA, DHCP, DNS)

Se il sintomo segnalato fa riferimento a un servizio di rete specifico anziché al controller stesso, ad esempio se i client non riescono a eseguire l'autenticazione, non ricevono un indirizzo IP o non riescono a risolvere il nome, il dashboard dei servizi di rete di Catalyst Center in Assurance fornisce la visibilità di tali transazioni come segnalato dal WLC.

Selezionare Assurance > Dashboard > Integrità > Servizi di rete > AAA/DHCP/DNS:



Statistiche AAA client wireless su Catalyst Center



Statistiche DHCP client wireless su Catalyst Center

Motivo rete

Network Reasoner è uno strumento integrato in Catalyst Center che consente di individuare automaticamente i problemi di rete, senza doverli esaminare manualmente. È possibile trovarlo in Strumenti > Motore di rete. Ogni opzione di risoluzione dei problemi (denominata flusso di lavoro) mostra una breve descrizione, il numero di dispositivi interessati nelle ultime 24 ore e cosa accade se viene eseguita. Può rilevare solo problemi su dispositivi aggiunti al Catalyst Center for Assurance Monitoring o attivati tramite Catalyst Center.

The screenshot displays the Catalyst Center Network Reasoner interface. The top navigation bar includes the Cisco logo, 'Catalyst Center', and 'Tools / Network Reasoner'. The main area is a grid of 16 tool cards, each with a title, description, and network performance impact. The tools are:

- L3 Access Check**: Detects if access switches are running L3 routing protocols (potentially ready for SDA). Network Performance Impact: Medium.
- Lisp PubSub Session Check**: Check the LISP PubSub health on the Fabric border device. If a PubSub session is down, then troubleshoot to find the root cause. Network Performance Impact: Low.
- Lisp Session Check**: Check the status of all LISP Sessions on this device. If a session is down, then troubleshoot to find the root cause. Network Performance Impact: Low.
- MTU Link Check**: Checks the MTU settings for connections between fabric capable devices (primarily the Switches within the network). Network Performance Impact: Low.
- Network Connectivity**: Check any network connectivity failures to the destination. Network Performance Impact: Low.
- Ping Device**: Ping a target IP Address. Network Performance Impact: Low.
- Power Supply**: Determine the root cause for power supply problems on a device. Affected Devices: 0/last 24 hrs. Network Performance Impact: Low.
- Redundant Link Check**: Detects if there are two links associated with a device with role ACCESS. Network Performance Impact: Low.
- SDA Hardware Readiness Check**: Check Hw is ready for SDA. Network Performance Impact: Low.
- SDA Scale Limits Check**: Check number of clients, network devices and fabrics within Catalyst Center. Network Performance Impact: Medium.
- SDA Software Readiness Check**: Check Sw is ready for SDA. Network Performance Impact: Low.
- System Bug Identifier**: Identify bugs that apply to your Cisco DNA Center. Network Performance Impact: Low.
- Wireless AP Data Collection**: Collect show output, logs, and PCAP for an Access Point (AP) on its associated Catalyst 9800 WLC and via SSH to the AP for up to 30 minutes. Network Performance Impact: Medium.
- Wireless Client Data Collection**: Collect show output, logs, and PCAP for a Wireless Client on 1-2 Catalyst 9800 WLCs and up to 5 APs via SSH for up to 30 minutes. Network Performance Impact: Medium.

Below the grid, there is a 'Preproduction' section with one tool card:

- Catalyst 9800 Wireless Controller HA SSO Analysis**: Analyse the health of High Availability(SSO) of Catalyst 9800 Wireless Controller by collecting and processing the relevant command output. Network Performance Impact: Medium.

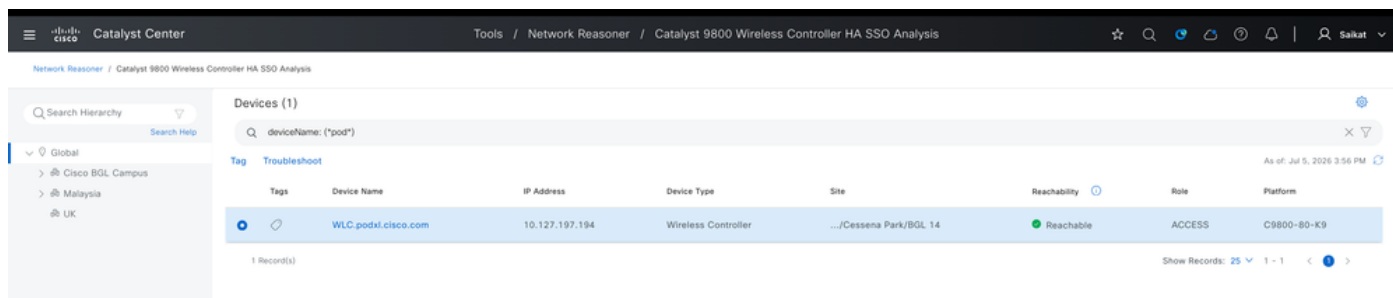
Varie opzioni di risoluzione dei problemi di rete disponibili in Motivo rete

Per le reti wireless, è possibile risolvere i problemi in tre modi:

1. Per i problemi dei controller, in particolare con le impostazioni di alta disponibilità (HA), Network Reasoner controlla aspetti quali:

- Il controller è raggiungibile?
- Ha è impostato correttamente?
- I controller attivo e di standby sono sincronizzati?
- La connessione tra di loro funziona?

Se rileva un problema, indica esattamente cosa è sbagliato e suggerisce come risolverlo. Esiste inoltre un'opzione separata per i dispositivi di risoluzione dei problemi che non inviano alcun dato di monitoraggio.



Risoluzione dei problemi di elevata disponibilità mediante il Motore di rete

Quando si abilita la funzione di risoluzione dei problemi per l'analisi HA SSO sul WLC 9800 utilizzando Network Reasoner, vengono eseguiti diversi controlli e viene fornita una conclusione basata sui risultati. Se vengono rilevati problemi con SSO HA, vengono suggerite anche azioni correttive per risolverli.

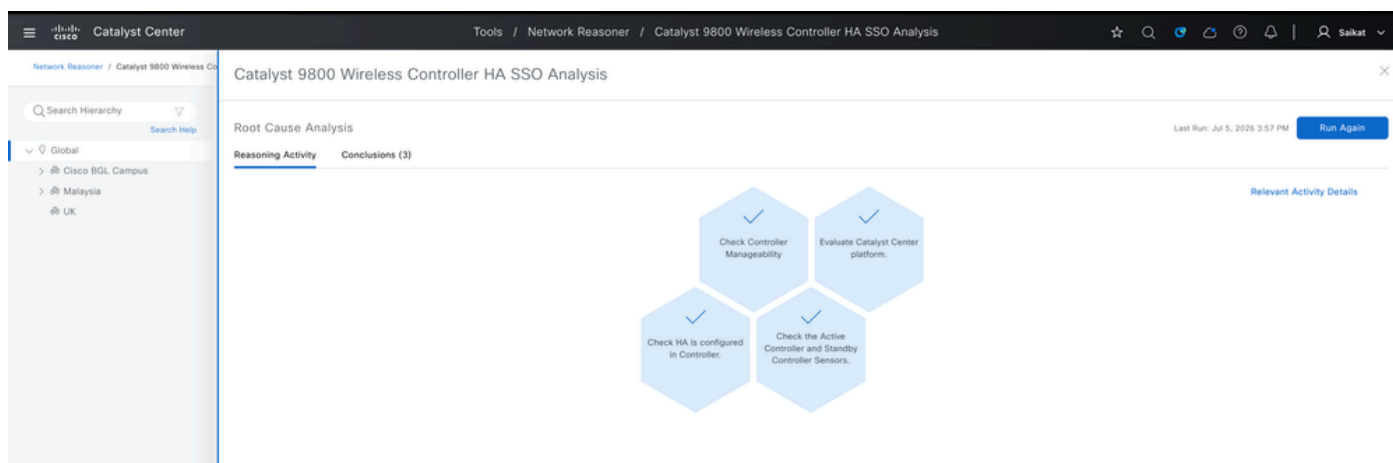
!! Task Workflow !!

Check Controller Manageability

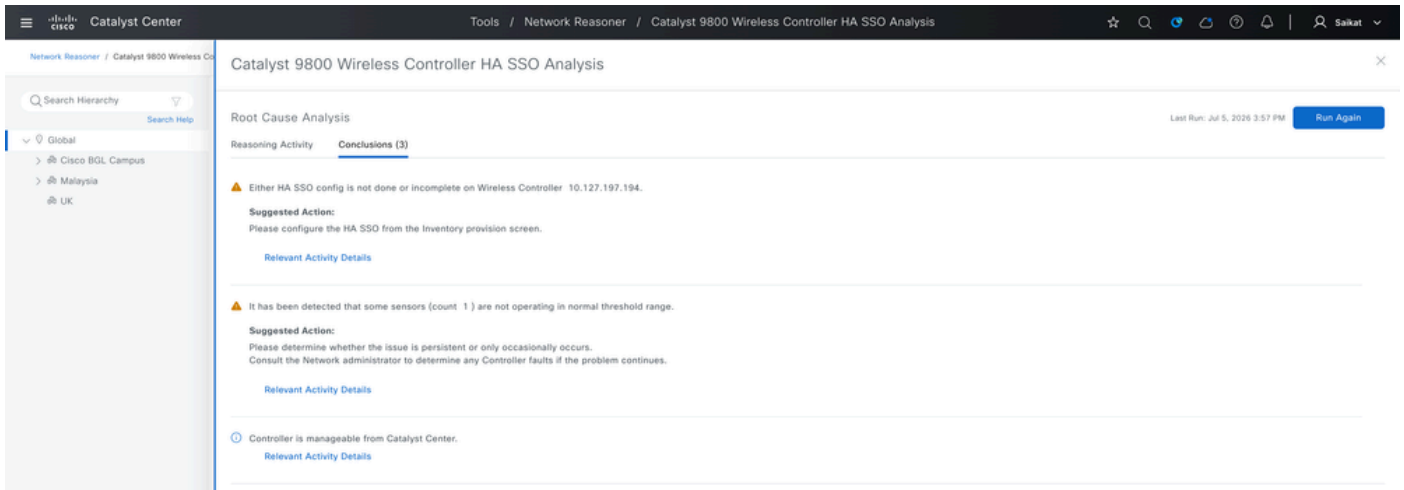
Evaluate Catalyst Center platform.

Check HA is configured in Controller.

Check the Active Controller and Standby Controller Sensors.

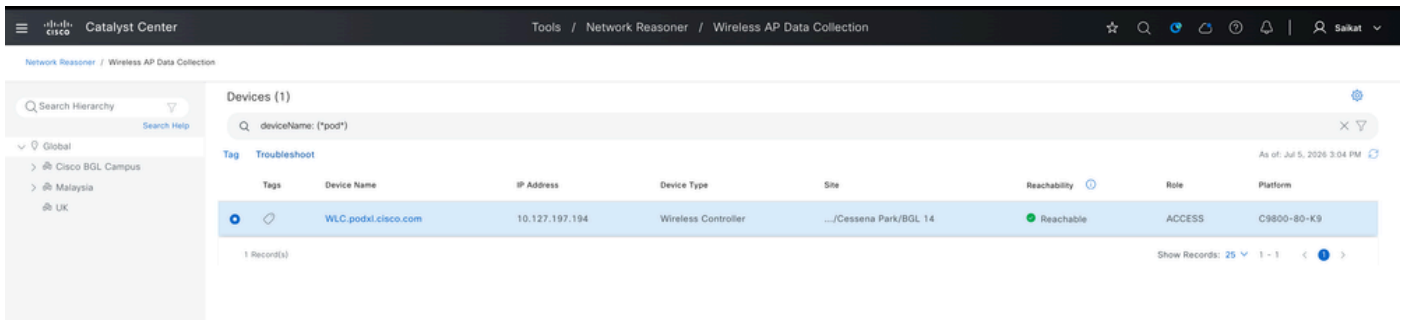


Attività eseguite da CATC per l'analisi HA SSO

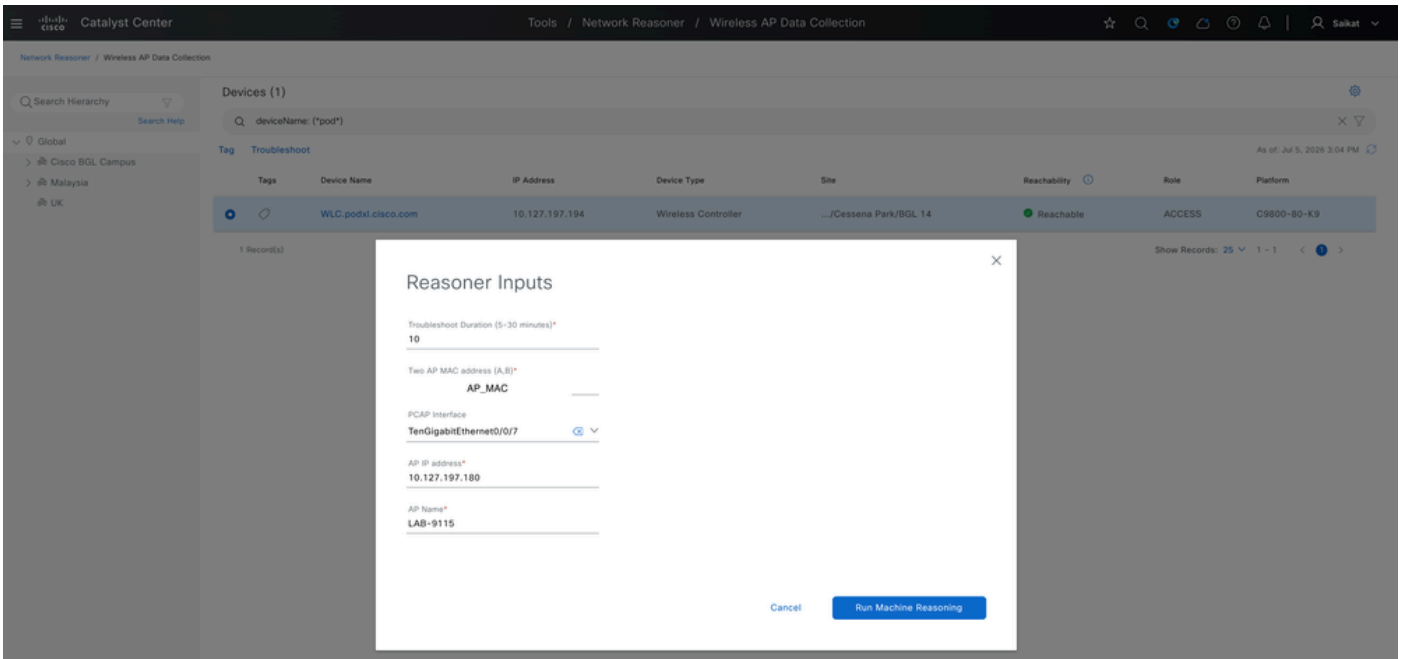


Esempio di conclusione per la risoluzione dei problemi di SSO HA utilizzando il Motore di rete

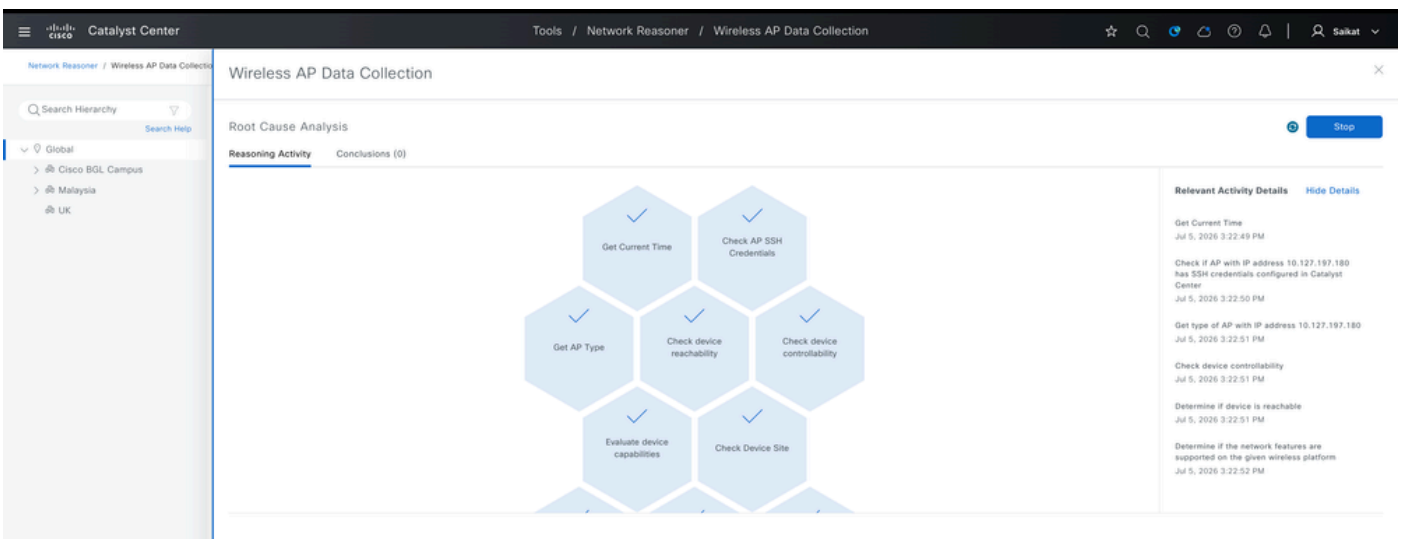
2. Access point: se in un access point si verificano problemi, selezionare il controller che lo gestisce, quindi immettere l'indirizzo MAC dell'access point e impostare la durata per l'esecuzione del controllo. Consente l'acquisizione di registri e pacchetti dal WLC e dall'access point, per una maggiore visibilità. Di seguito viene riportato il flusso di lavoro per l'abilitazione di Network Reasoner per un punto di accesso con i risultati corrispondenti:



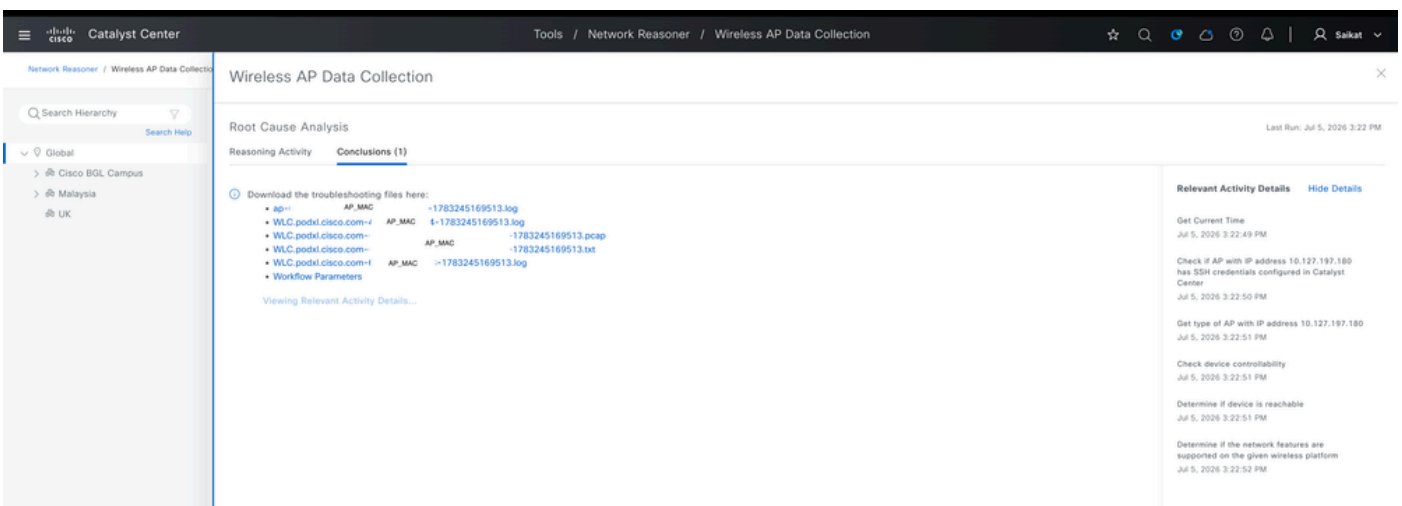
Selezionare il WLC dell'access point gestito per la risoluzione dei problemi



Fornire i dettagli dell'access point per la risoluzione dei problemi



Attività in esecuzione per la risoluzione dei problemi relativi al punto di accesso



!! 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:<file-name>

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:<file-name>

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, saved into file bootflash:<file-name>

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 into file bootflash:<file-name>

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:<file-name>

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

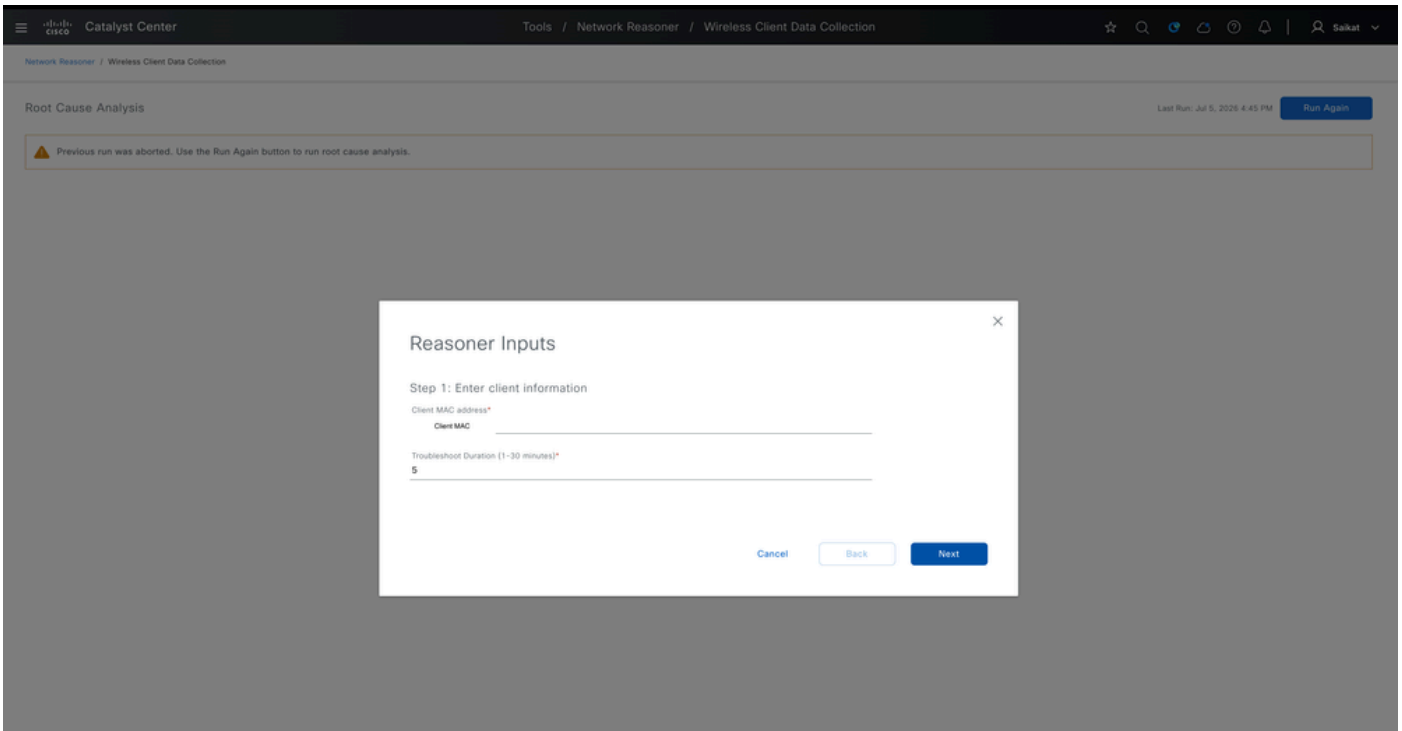
Stop RA Trace for AP: <MAC>

Jul 5, 2026 5:10:46 PM

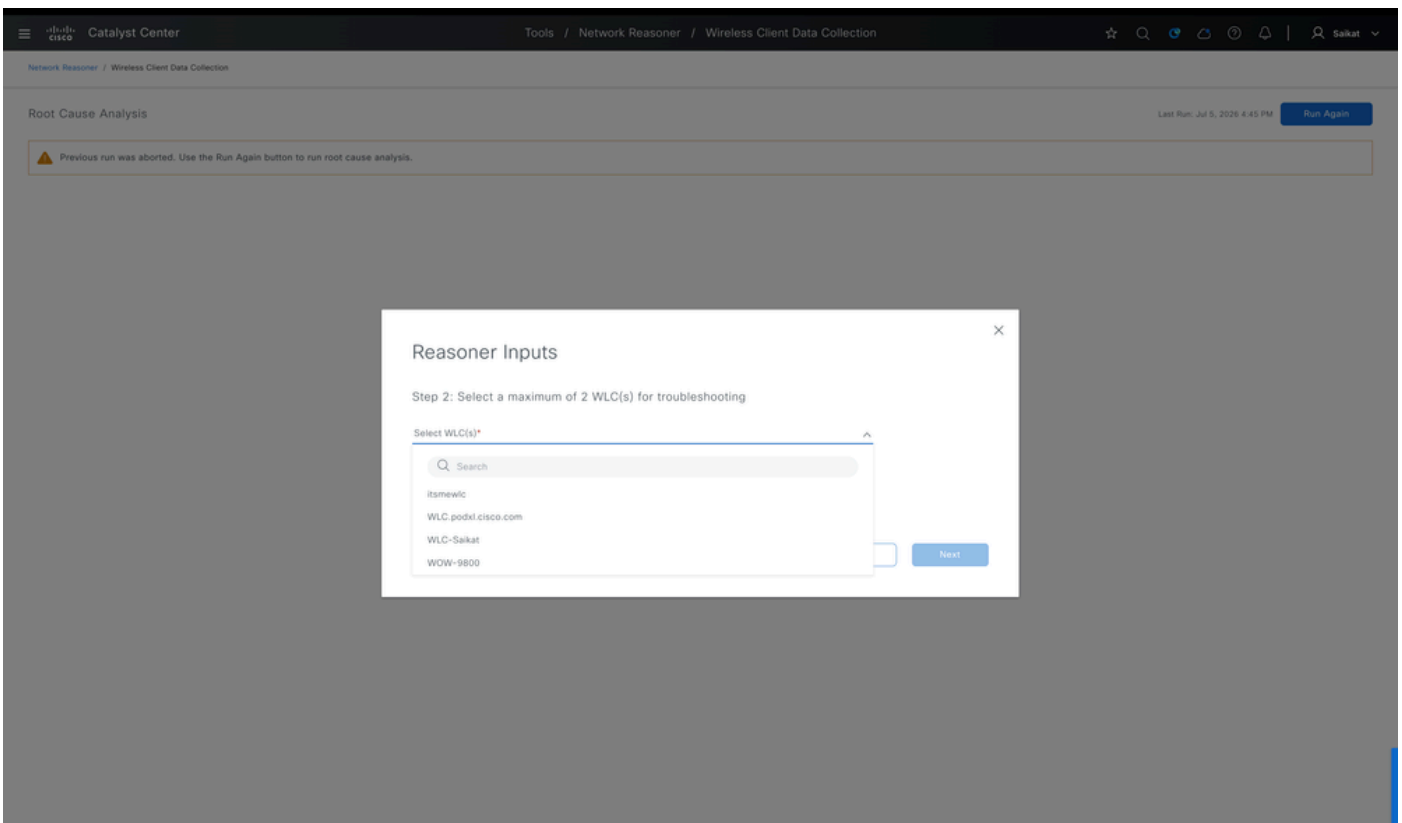
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194

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.
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.
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.
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://10.105.19.
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.
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.
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.
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.
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.
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.
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.
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.
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://10.105.19.
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.
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.
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.
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://10.105.19.
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.
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.
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

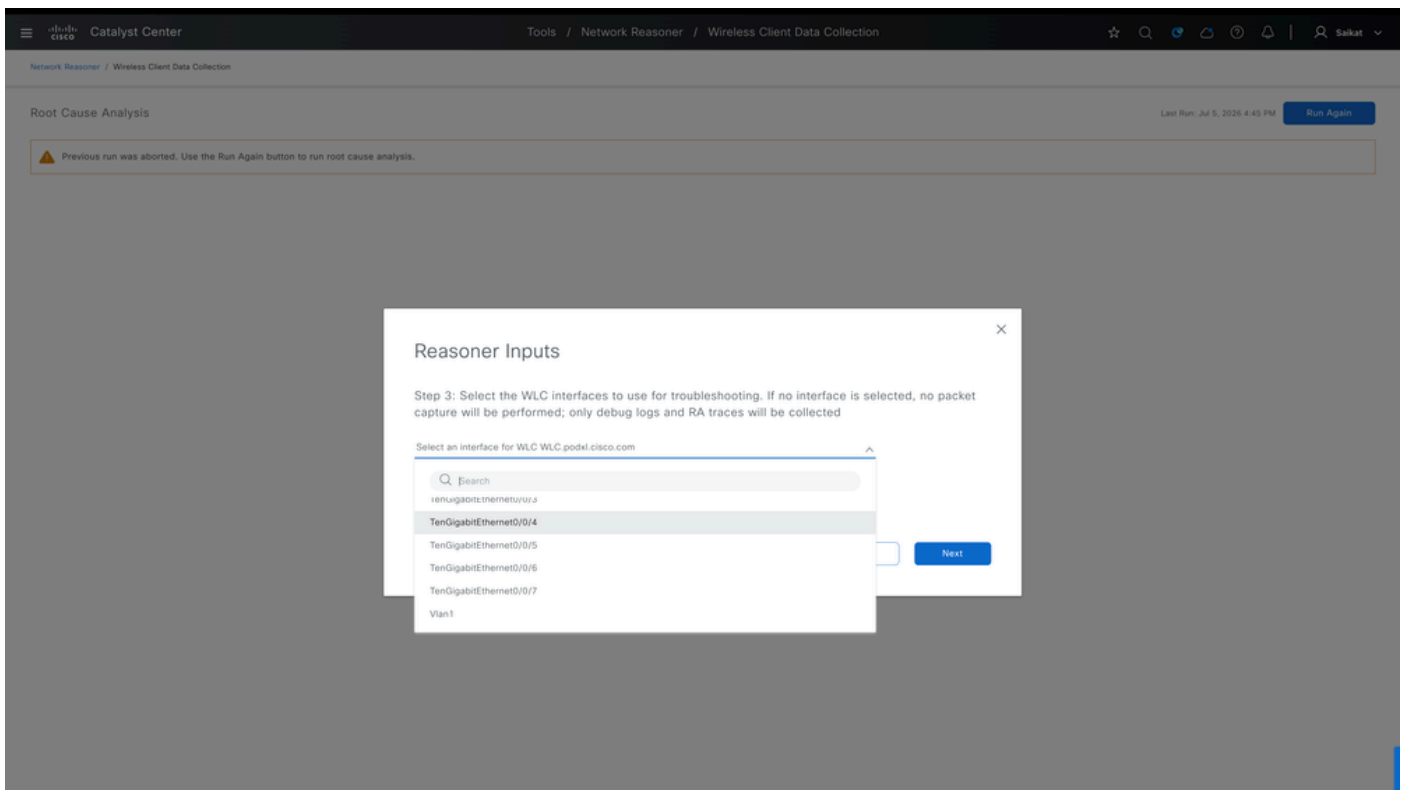
3. Client wireless - Se un utente ha problemi Wi-Fi, seleziona il controller wireless a cui è connesso, immetti l'indirizzo MAC del dispositivo e scegli per quanto tempo desideri che lo strumento controlli. Consente inoltre di registrare statistiche, eseguire le tracce RA e acquisire pacchetti per visualizzare i dati effettivamente scambiati. Di seguito è riportato il flusso di lavoro per l'attivazione di Network Reasoner per client wireless con i risultati corrispondenti:



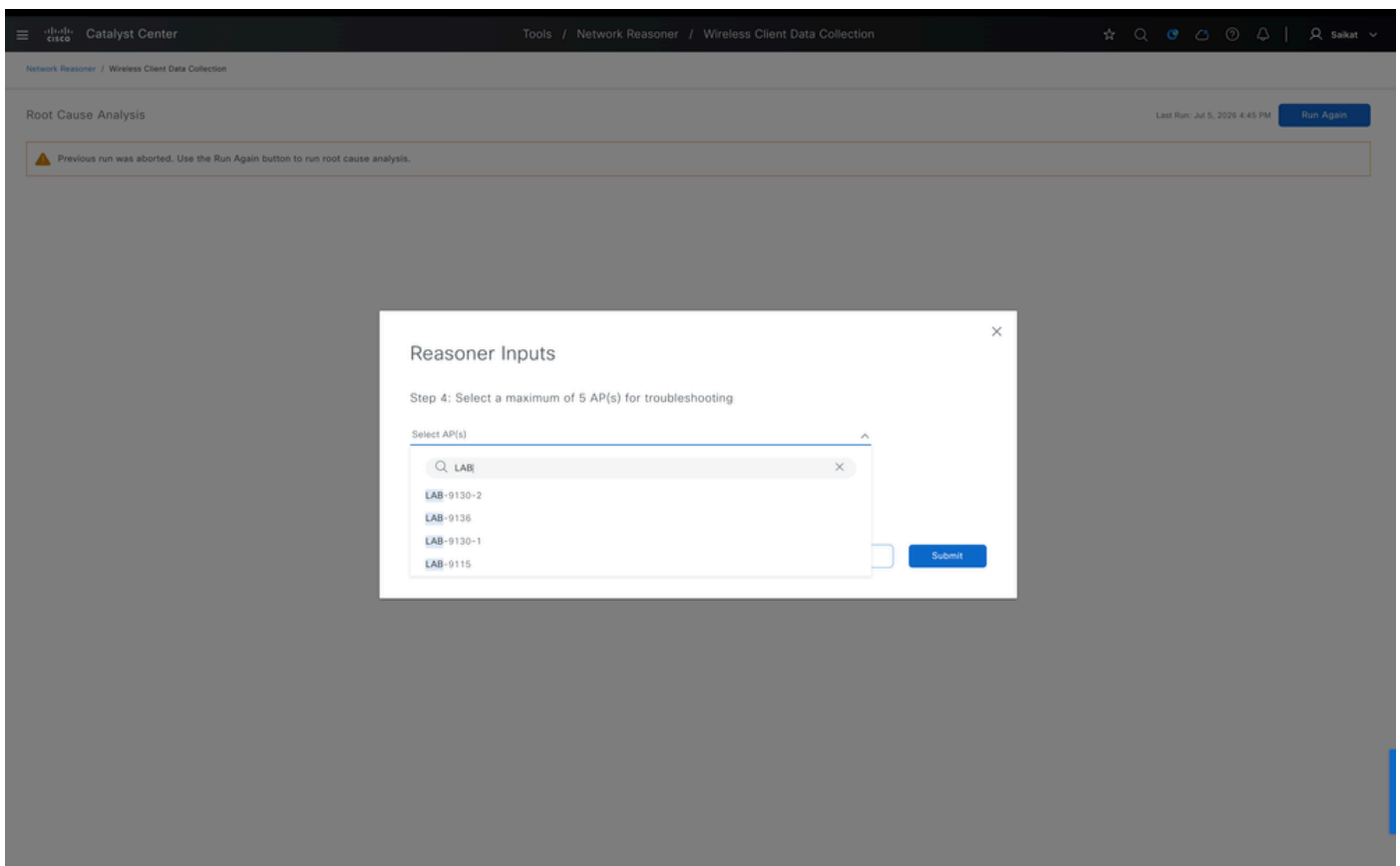
Fornire i dettagli del client per la risoluzione dei problemi



Selezionare WLC per risolvere i problemi relativi all'indirizzo MAC del client wireless



Selezionare Interface on WLC per risolvere i problemi del client wireless



Selezionare i punti di accesso (massimo 4) per la risoluzione dei problemi dei client wireless

Root Cause Analysis

Reasoning Activity | Conclusions (0)

Check device controllability ✓

Evaluate device capabilities ✓

Check Device Site ✓

Debug wireless mac ✓

Start PCAP ✓

Get File Store URL ✓

Start Show Client Details ✓

Check AP SSH Credentials ✓

Get AP Type ✓

Start Logging on AP over SSH and Wait for Data Collection... ✓

Relevant Activity Details | Hide Details

Debug wireless mac
Jul 5, 2026 3:46:02 PM

Get Current Time
Jul 5, 2026 3:46:02 PM

Starting Client PCAP session mve_client_pcap_1783246554812 with filter 0037.4574.d919 on interface TenGigabitEthernet0/0/7
Jul 5, 2026 3:46:03 PM

Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127.197.194 for filename: WLC.podkl.cisco.com-0037.4574.d919-1783246554812.txt
Jul 5, 2026 3:46:05 PM

Collect Show Client Details for 300 seconds

Attività in esecuzione per la risoluzione dei problemi del client wireless

Root Cause Analysis

Reasoning Activity | Conclusions (1)

Last Run: Jul 5, 2026 3:45 PM | Run Again

Download the troubleshooting files here:

- WLC.podkl.cisco.com client-mac 783246554812.txt
- ap-10.127.197.151-1783246554812.log
- WLC.podkl.cisco.com client-mac 1783246554812.log
- WLC.podkl.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?

Acquisizioni raccolte da WLC e AP per problemi del client wireless

!! 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 [https://10.105.193.40](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 10.127.197.194
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 10.127.197.194
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 10.127.197.194
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 10.127.197.194
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 10.127.197.194
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 10.127.197.194
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://10.105.193.40](https://10.105.193.40/api/v)
Jul 5, 2026 5:59:09 PM
Check if file bootflash:<file-name> has been uploaded successfully from WLC with IP address 10.127.197.194
Jul 5, 2026 5:59:14 PM
File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to [https://10.105.193.40](https://10.105.193.40/api/v)
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 10.127.197.194

05 lug 2026 5:59:16

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

05 lug 2026 5:59:16

Check File Size:bootflash:<file-name>

05 lug 2026 5:59:16

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

05 lug 2026 5:59:18

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

05 lug 2026 5:59:23

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

05 lug 2026 5:59:23

Eliminare il file bootflash:<nome-file> dal WLC con indirizzo IP 10.127.197.194

05 lug 2026 5:59:23

Riferimenti tecnici

- [Guida all'implementazione di Cisco Intelligent Capture](#)
- [Gestisci acquisizioni intelligenti](#)
- [Guida per l'utente di Cisco Catalyst Assurance, versione 2.3.7.x](#)
- [Risoluzione dei problemi relativi ai dispositivi di rete mediante il Motore di rete - HA su controller LAN wireless con flusso di lavoro MRE](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).