使用Catalyst Center解決無線問題

目錄

簡介

本檔案介紹使用Cisco Catalyst Center疑難排解Catalyst 9800無線LAN控制器(WLC)、AP和使用者端連線問題。

必要條件

- 必須將無線LAN控制器新增到Catalyst Center並在清單中顯示Managed狀態。
- WLC上的遙測狀態必須顯示為Up。

需求

思科建議您瞭解以下主題：

- 對無線區域網控制器的命令列介面(CLI)或圖形使用者介面(GUI)訪問
- 命令列介面(CLI)或圖形使用者介面(GUI)訪問Catalyst Center

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 9800型號WLC
- Cisco IOS XE 17.15.5版本
- Catalyst Center 2.3.7版本

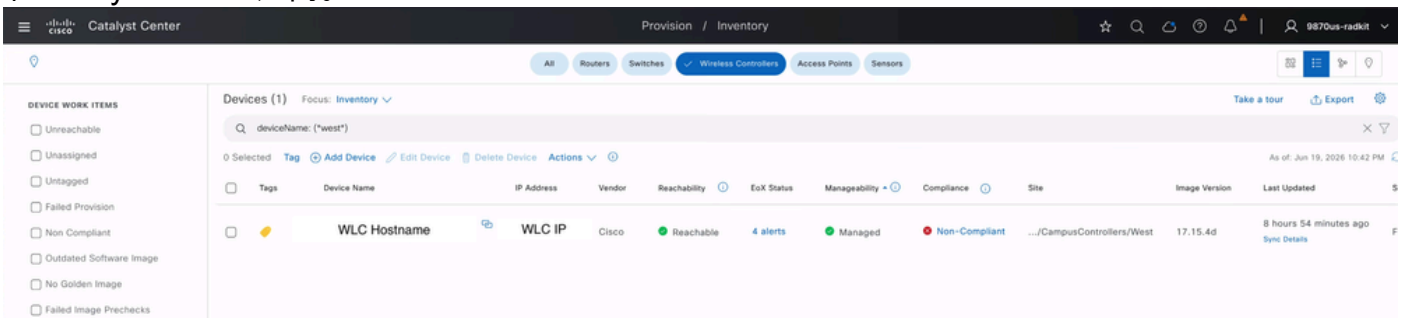
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

從Catalyst Center收集資料

將Catalyst 9800系列WLC新增到Catalyst Center for Assurance後，該平台將通過多種收集方法提取資料：SNMP輪詢、流遙測、NetFlow、系統日誌、基於CLI的收集、API和IP SLA。每種機制都有不同的用途：一些報告基本裝置運行狀況（CPU、記憶體、KPI），而另一些報告提供精細的細節（PoE狀態、客戶端會話和無線效能）。

1. 裝置/清單運行狀況(SNMP + CLI):可訪問性、CPU、記憶體、介面統計資料和軟體版本 — 通過標準SNMP輪詢和CLI收集。
2. 系統日誌：將系統和操作日誌消息傳送到Catalyst Center（充當已配置的系統日誌伺服器）。
3. 無線遙測（NETCONF/YANG串流）：核心保證源。它以接近即時的方式流傳輸AP和客戶端級別的資料 — 客戶端登入和漫遊事件、RSSI/SNR、AP無線電/RF統計資訊和WLC內部運行狀況計數器。

要接收此資料，無線LAN控制器必須處於Catalyst Center的管理狀態，遙測狀態顯示在9800控制器和Catalyst Center之間。



```
<#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
```

預設情況下，Cisco Catalyst Center配置為運行狀況、問題和事件設定，包括無線控制器、接入點、無線客戶端和應用程式的特定閾值和優先順序。Catalyst Center根據它從這些受管裝置接收的資料和配置的事件設定來生成事件和警報。此外，可以建立自定義配置檔案，以根據特定網路要求定製這些設定，從而根據網路環境的獨特需求進行更精確的監控和警報。

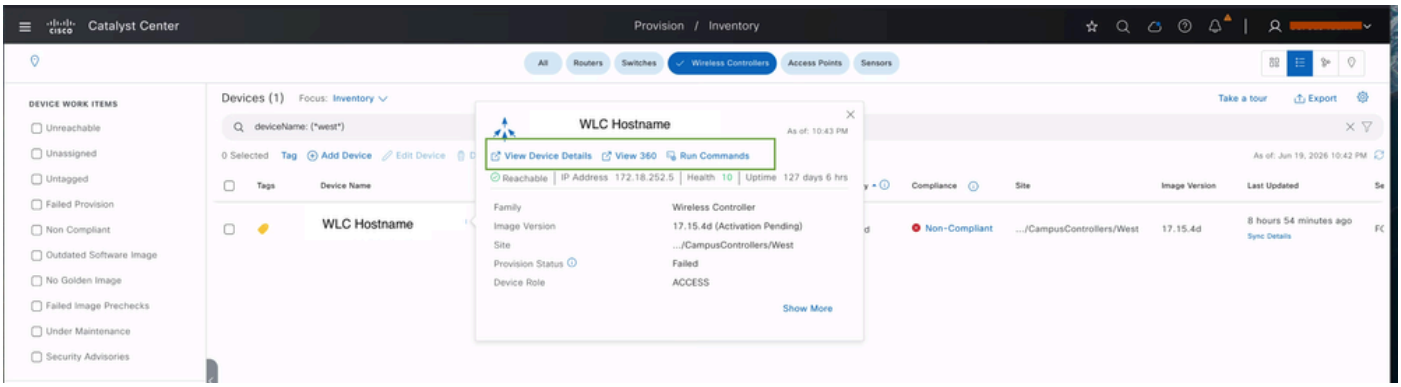
Catalyst 9800系列無線控制器問題

當無線LAN控制器(WLC)遇到諸如特定服務中的連線能力喪失、效能下降、存取錯誤、中斷或退化等問題時，Cisco Catalyst Center提供內建的可視性，允許您在問題發生時重新設定控制器上發生的情況，而無需直接登入裝置。

使用裝置360檢視控制器運行狀況

裝置360檢視將控制器的可達性、遙測狀態、歷史問題、生成的事件和效能統計資訊整合到單個時間軸驅動的儀表板中，使其成為調查所報告的WLC問題時首先檢視的內容。

導覽至Provision > Inventory > Wireless Controller > [search for the controller] > 按一下 裝置名稱 >裝置360

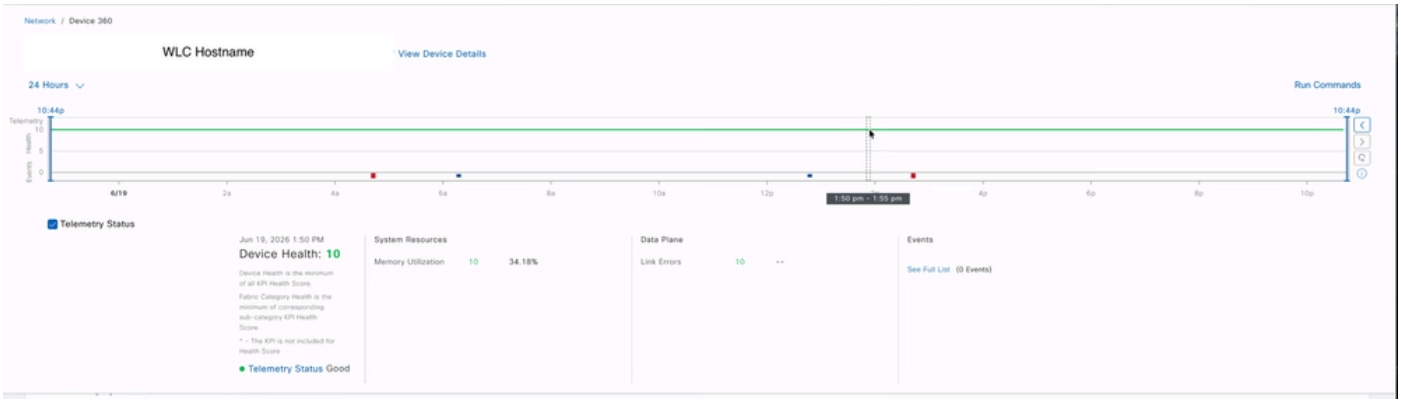


適用於無線LAN控制器的View 360

附註：也可以從Assurance > Health > Network訪問相同的檢視，然後按一下Network Devices表中的裝置名稱。

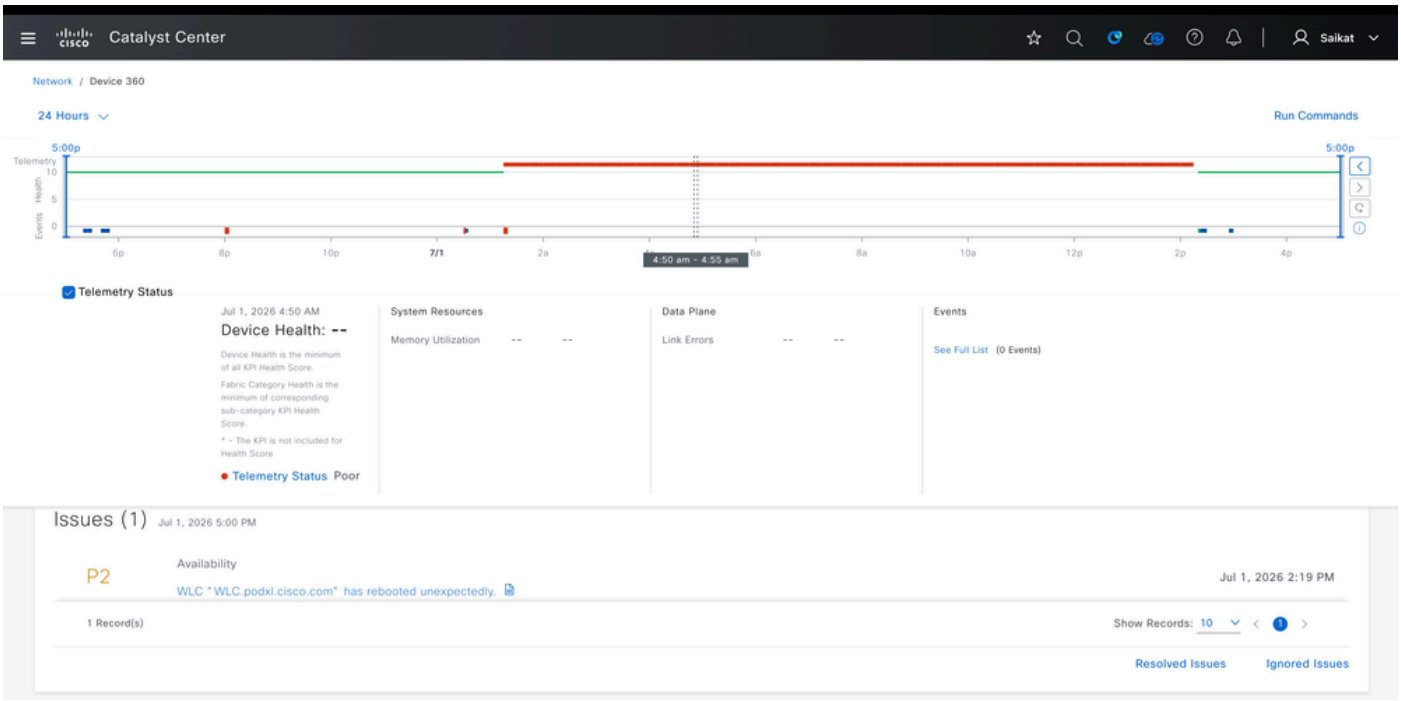
使用裝置360，您可以將健康時間線滑塊移回支援的歷史視窗內的任意點（Catalyst Center Assurance資料最多保留30天），以檢視發生事故時控制器狀態的準確外觀。對於該選定的視窗，檢視曲面：

裝置可連線 — 控制器是否可連線和管理。
遙測狀態 — SNMP/Syslog/NETCONF遙測饋送保證的運行狀況。



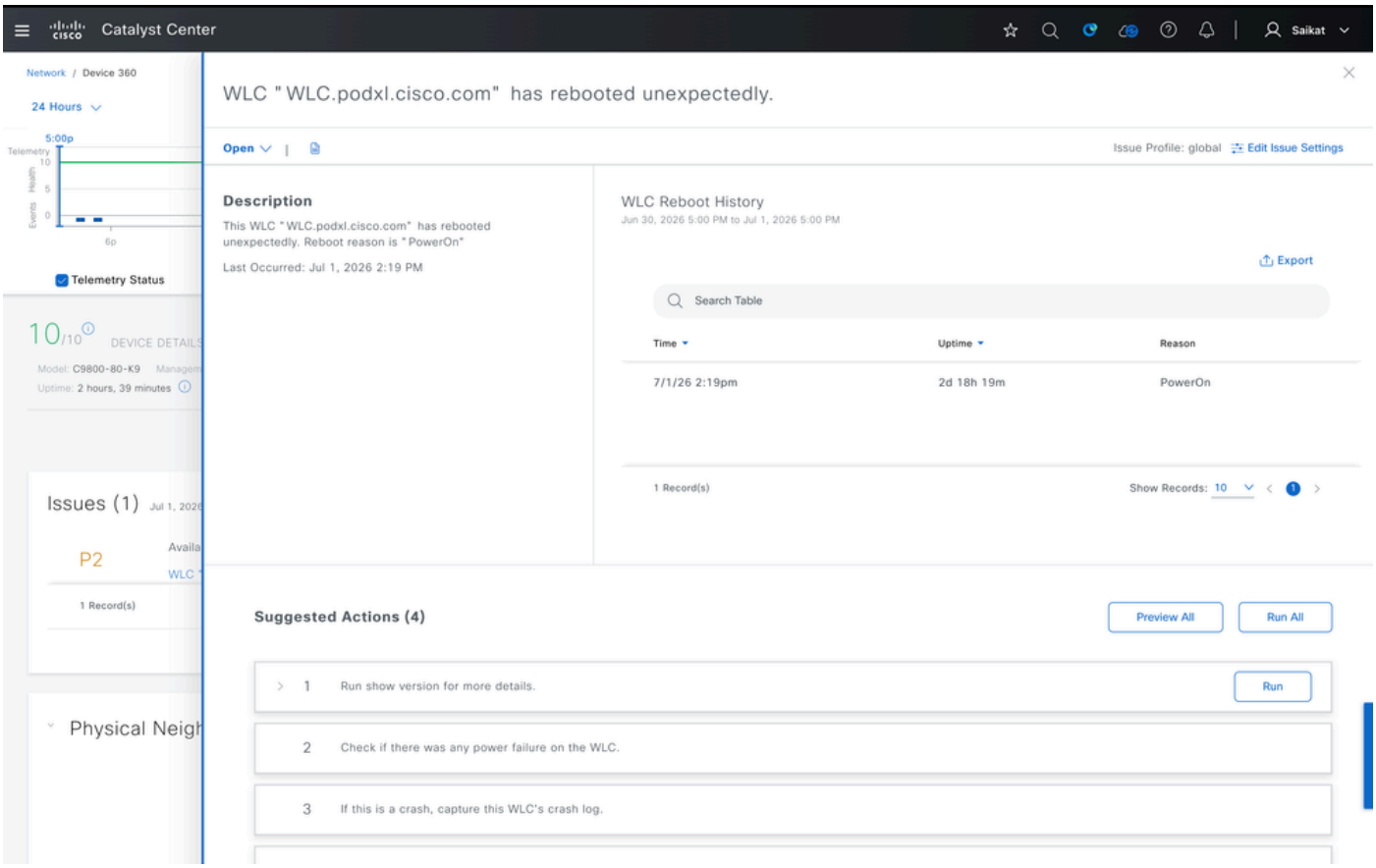
無線LAN控制器的遙測狀態

觀察到的問題 — 保證在該期間在裝置上檢測到問題。

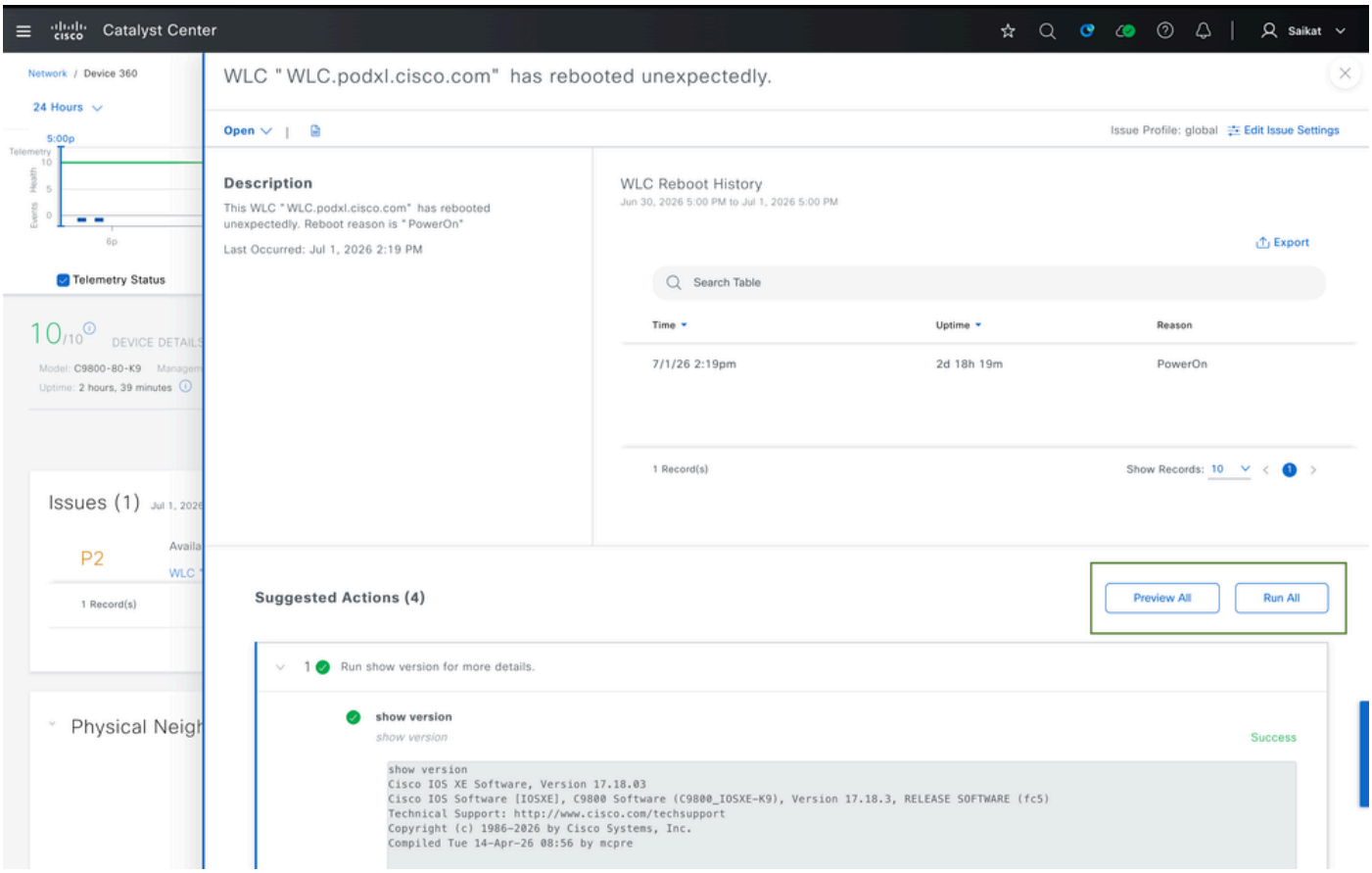


無線LAN控制器報告的問題

按一下特定問題，可以檢視有關該問題的詳細資訊，以及用於解決問題或進一步調查的建議操作。

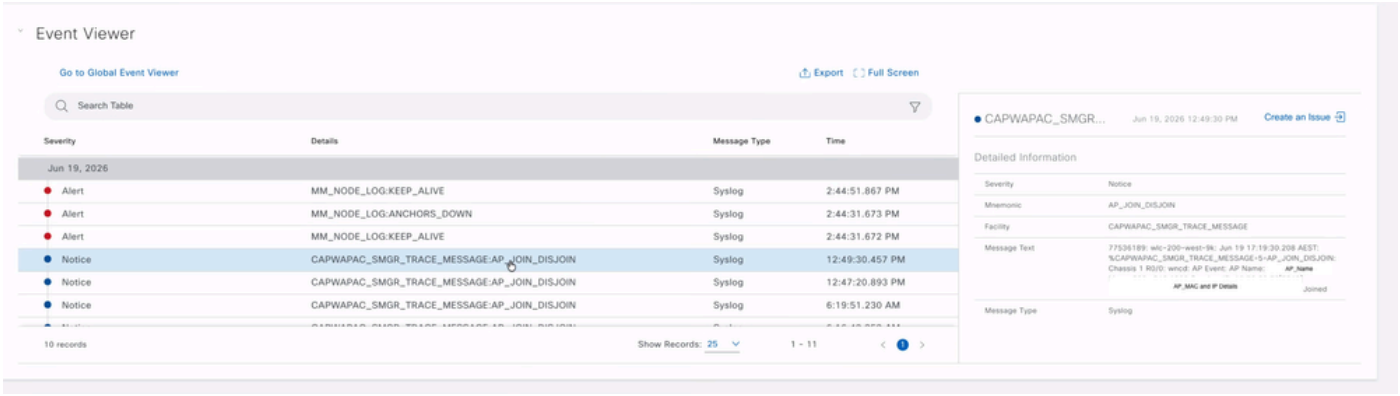


針對WLC上報告的問題建議的操作

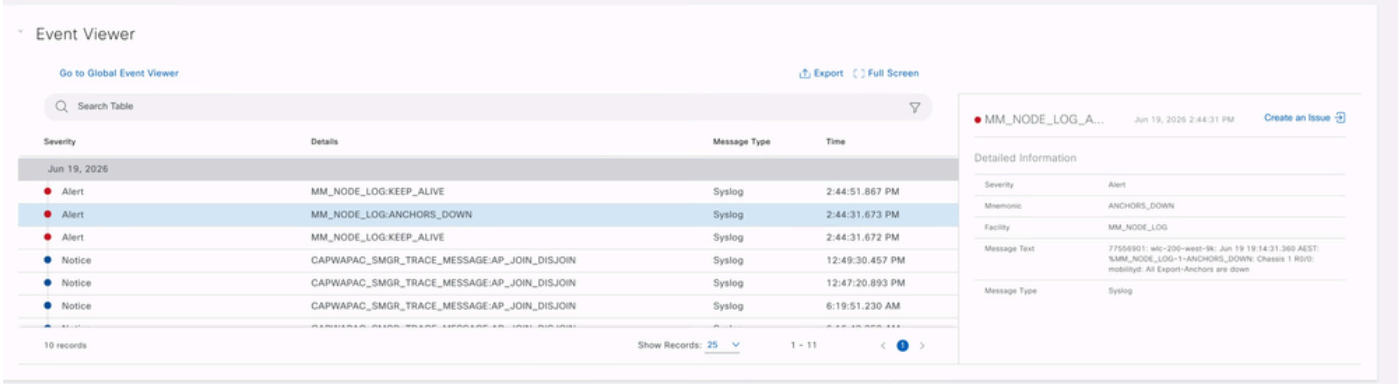


針對WLC上報告的問題建議的操作

生成的事件 — 基於從控制器接收的系統日誌消息和SNMP陷阱：



無線LAN控制器的事件檢視器 — 範例1

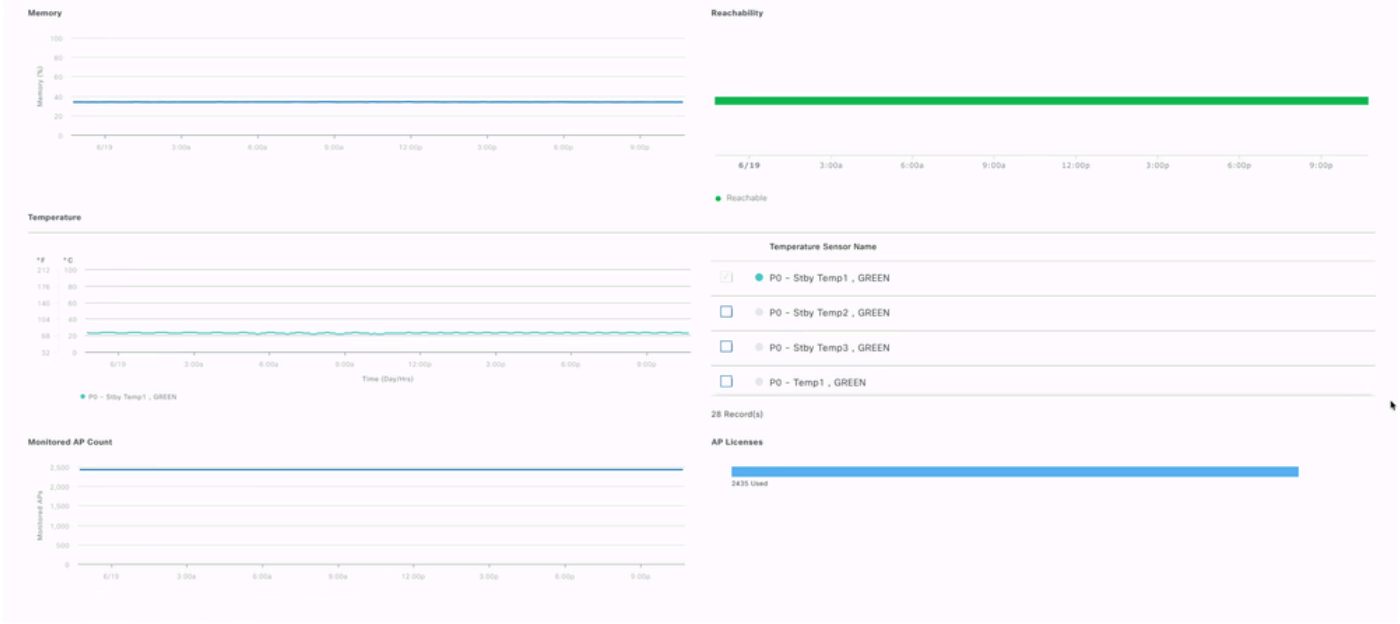


無線LAN控制器的事件檢視器 — 範例2

效能統計資訊 — CPU和記憶體利用率、溫度、正常運行時間、HA狀態和上次重新載入原因。

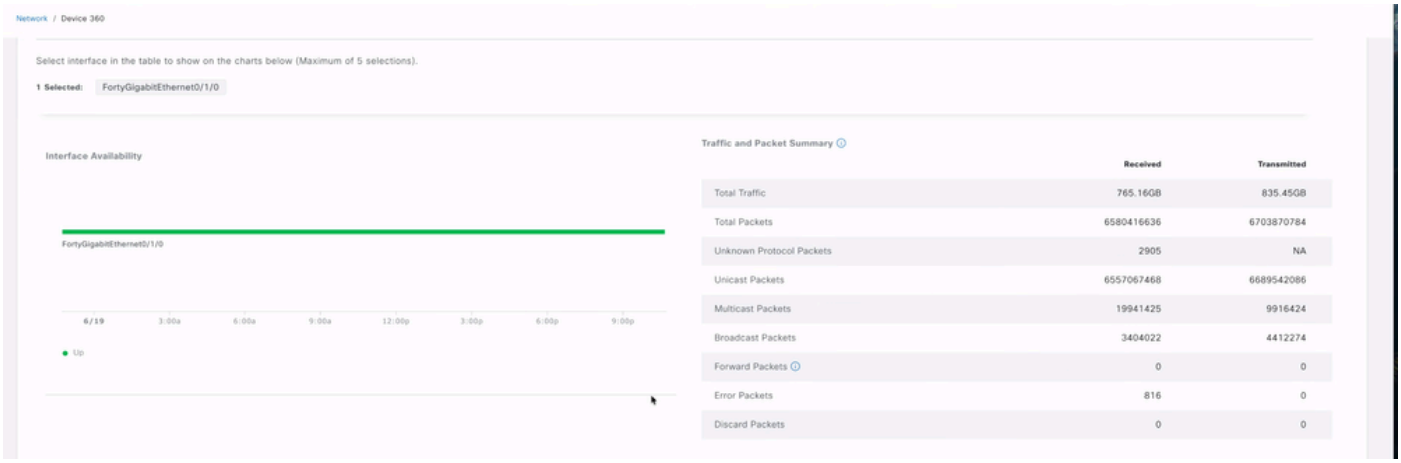
連線的客戶端 — 包括按本地、外部、錨點和空閒客戶端計數細分的資料。
AP狀態 — 與控制器關聯的接入點的加入/運行狀況狀態。

Catalyst Center上的WLC統計資訊



Catalyst Center上的WLC統計資訊

介面統計資訊 — 每個介面的狀態、RX/TX資料包計數、利用率、丟棄和錯誤。



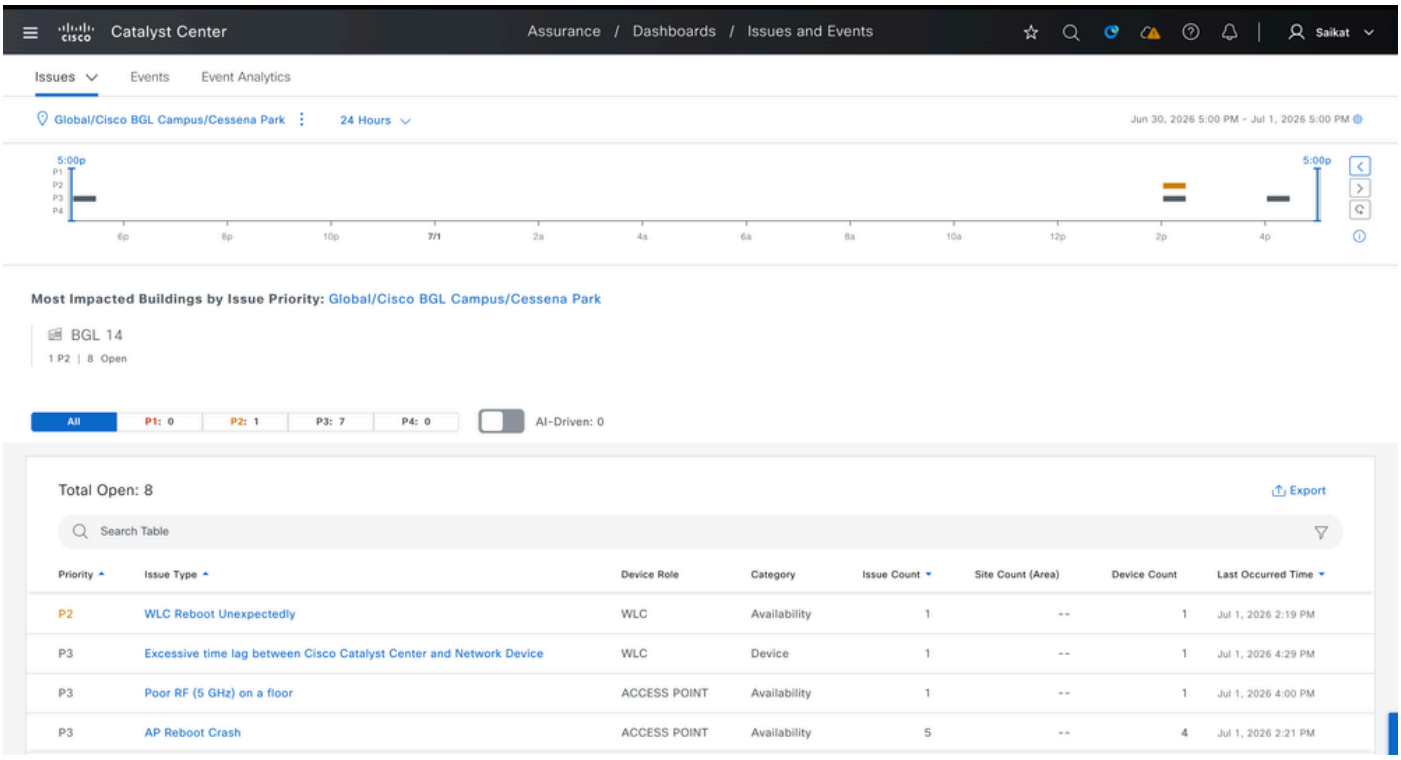
Catalyst Center上的WLC統計資訊

Catalyst Center上的WLC統計資訊

由於所有這些都是相互關聯的，因此您可以在發佈期間關聯多個相關因素並獲得清晰的瞭解。使用這些統計資料，您並不能準確地找到問題的根本原因，但是我們可以排除所有可能的原因，幫助我們進一步排除故障，設定需要即時收集的日誌型別。

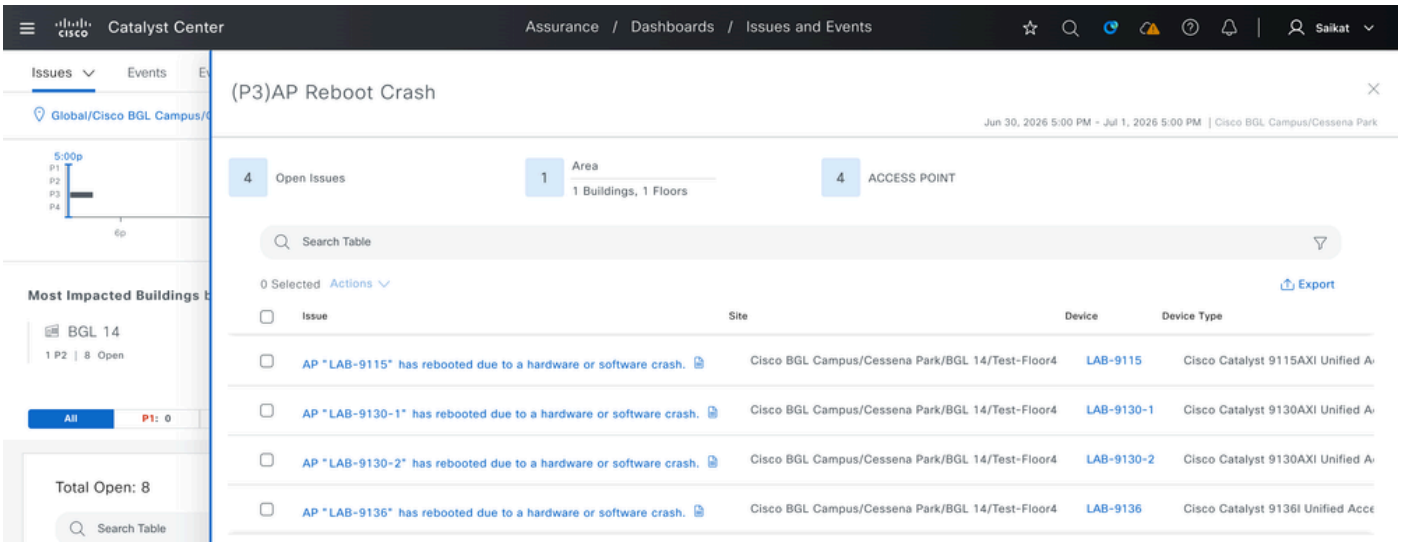
接入點問題

當Cisco接入點遇到諸如斷開連線事件、無線電狀態異常、重新啟動、崩潰、RF條件差、通道利用率高或處於非活動狀態等問題時，Catalyst Center會生成具有適當優先順序級別的警報。您可以通過導航到保證>問題和健康狀況設定來檢視這些警報。



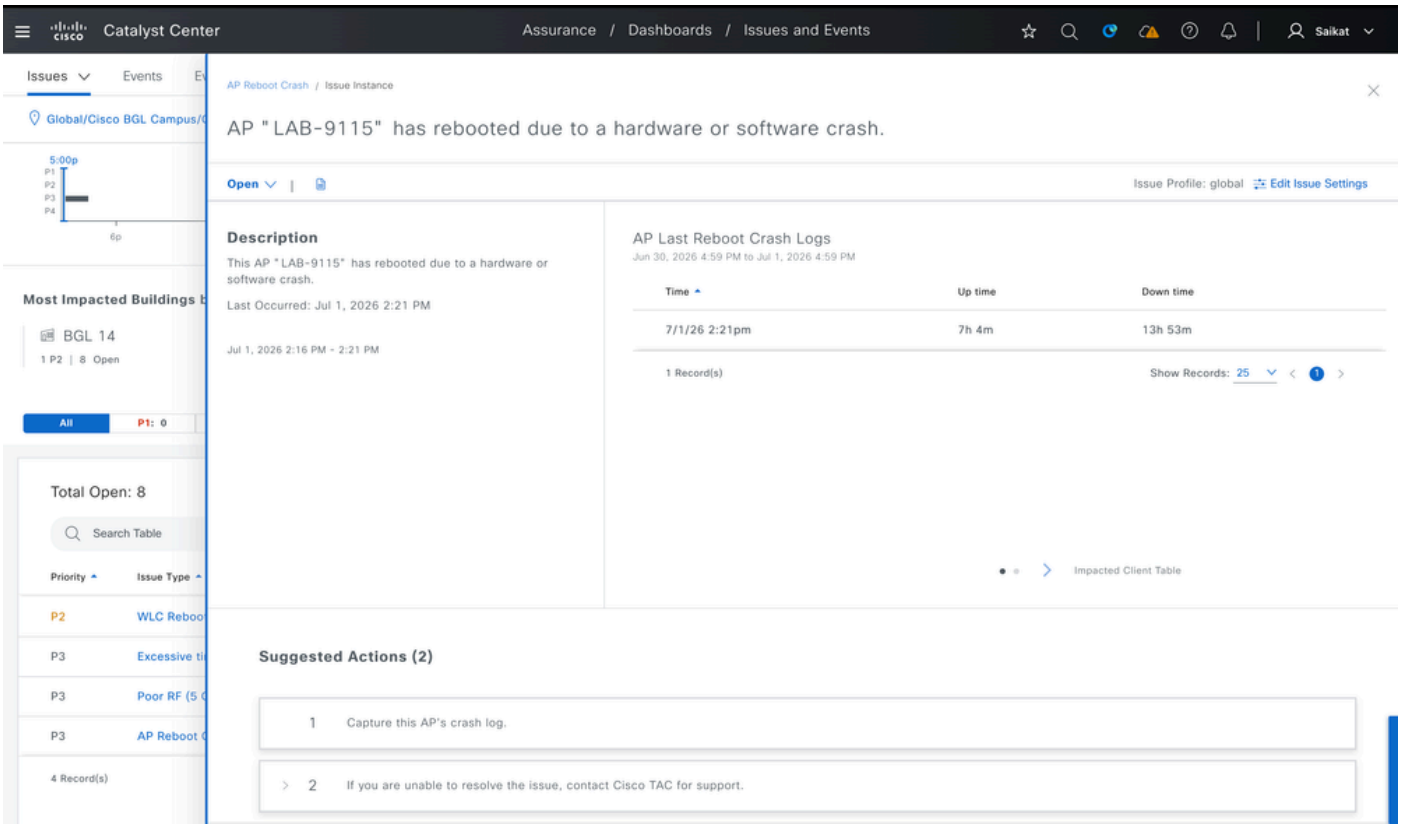
報告的問題生成具有相應優先順序的警報

此部分顯示環境中所有未解決的問題。通過按一下各個事件，您可以通過單獨按一下每個事件來獲得詳細的見解：



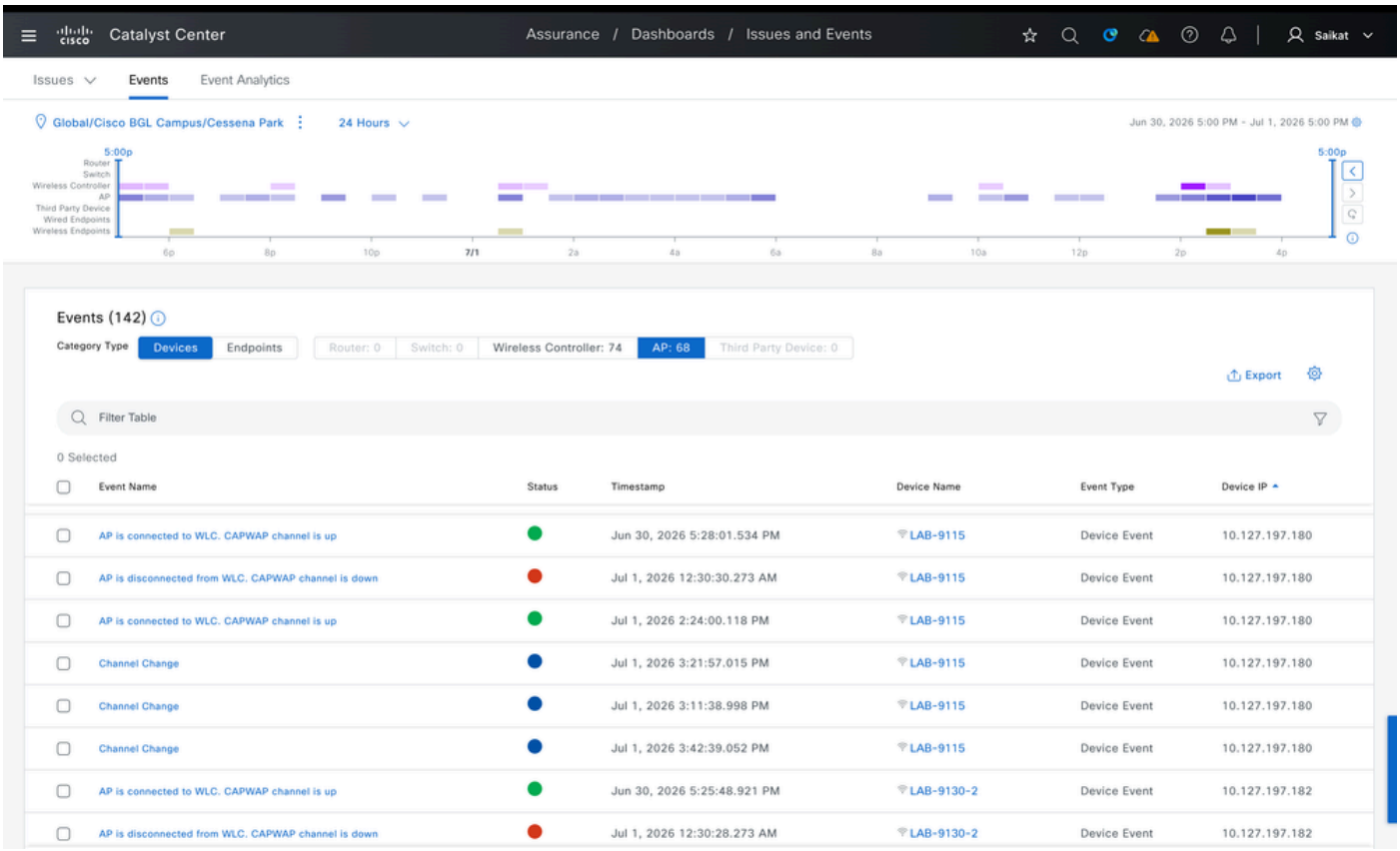
所報告問題的詳細概述

按一下特定問題，可以檢視有關該問題的詳細資訊，以及用於解決問題或進一步調查的建議操作。

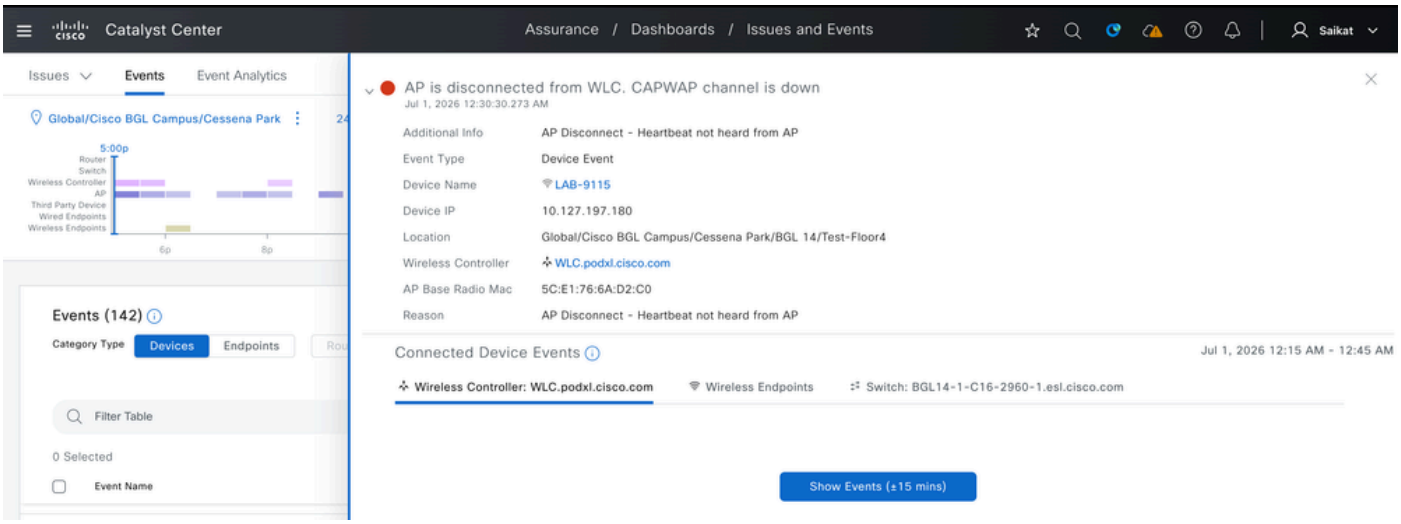


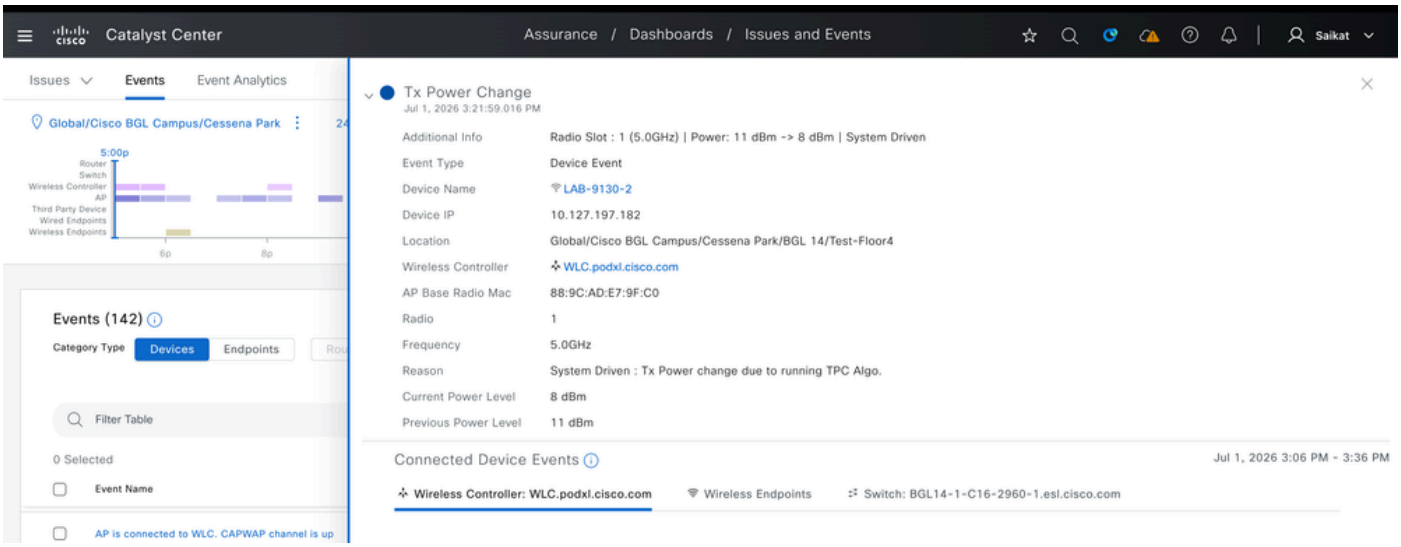
針對AP上報告問題的建議操作

此外，您還可以訪問事件檢視器，其中包含由Catalyst Center作為系統日誌接收的所有事件。這對於跟蹤所有事件（例如AP加入/退出活動、通道更改、TX電源修改和重新引導）非常有用。無線控制器和單個AP都會捕獲這些事件。

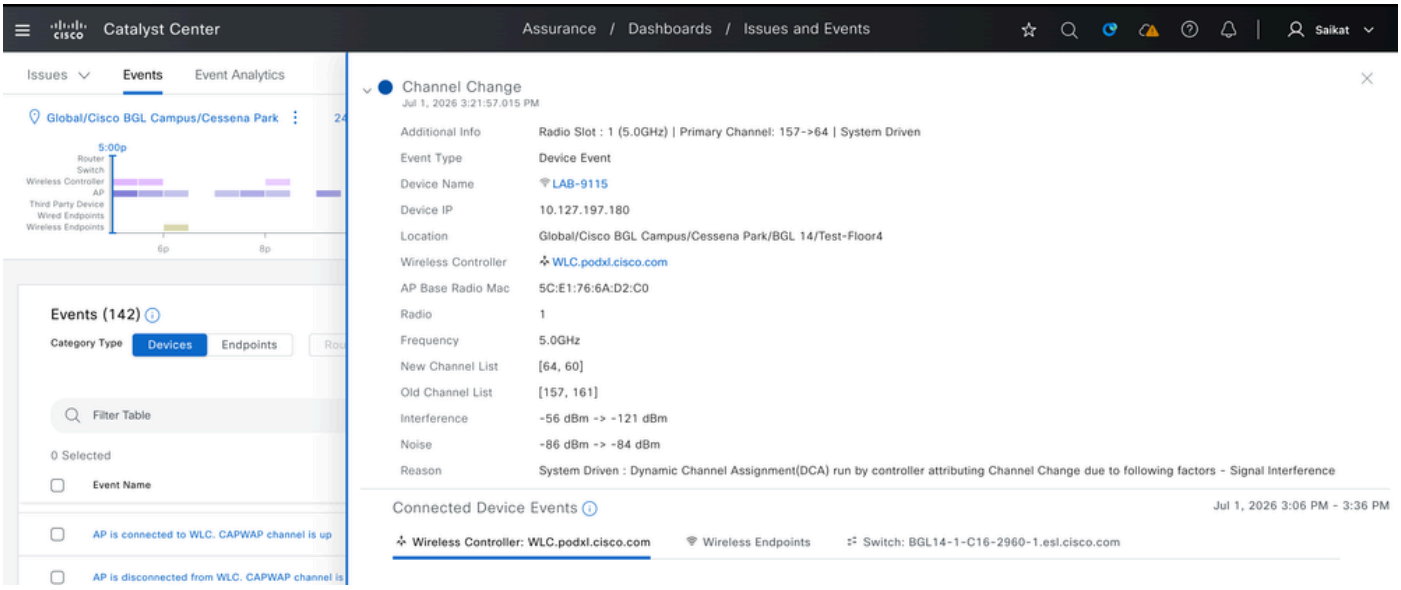


Catalyst Center上AP事件檢視器

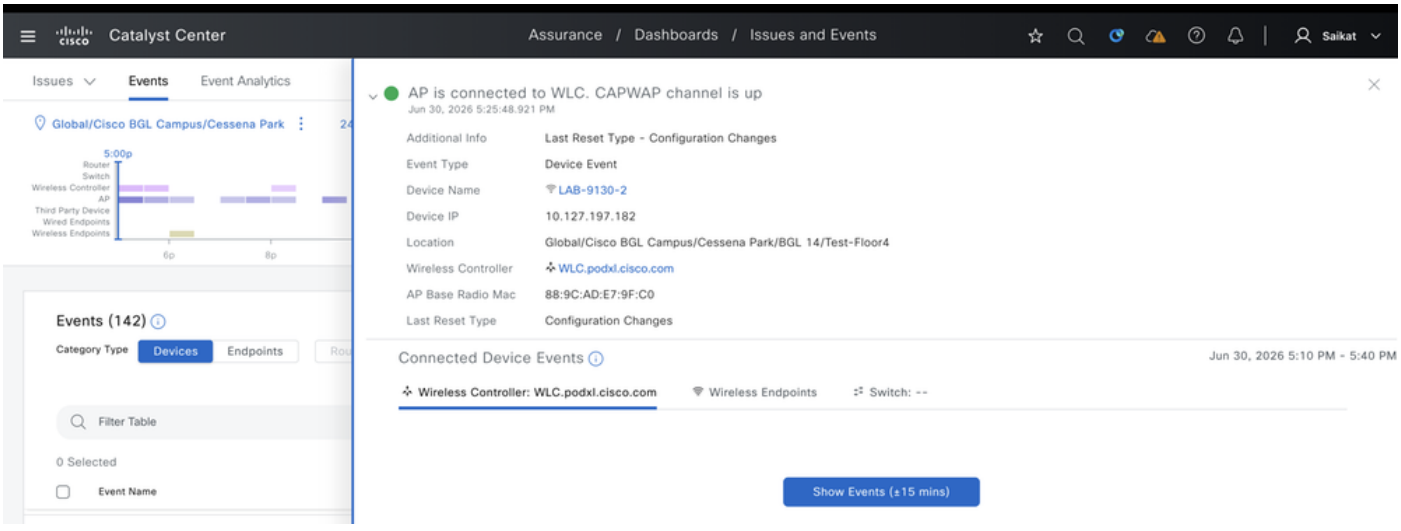




所報告事件的詳細概述（通知）

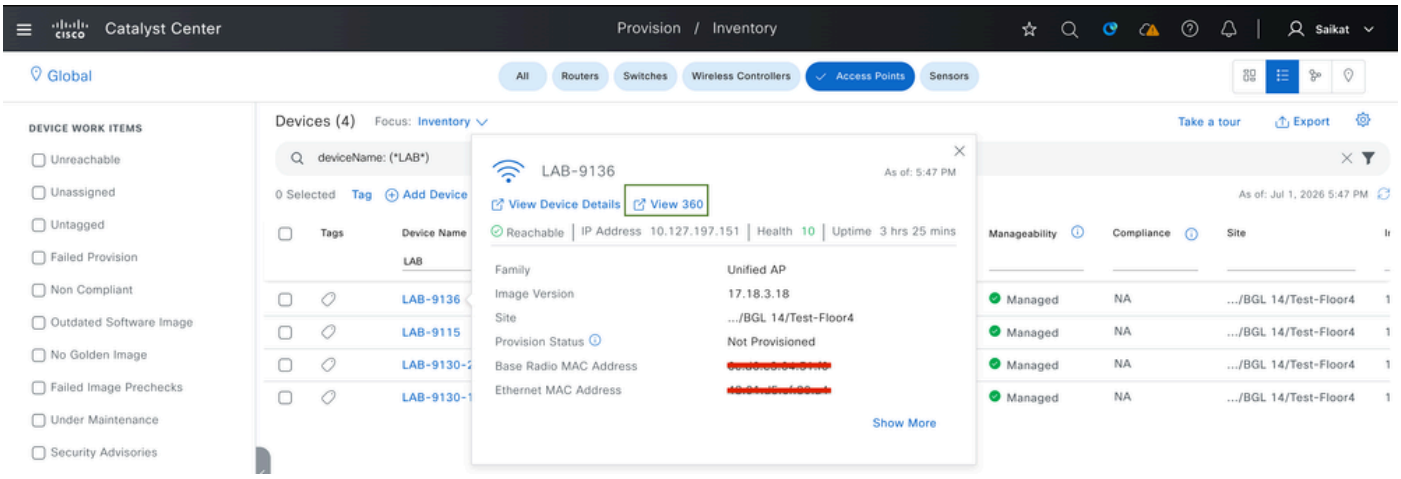


所報告事件的詳細概述（通知）



所報告事件的詳細概述（資訊）

對於特定AP的問題，您可以檢查該裝置的360 Health檢視。在這裡，您可以看到可達性狀態、報告的事件和問題，以及該AP在給定時間點的運行狀況得分。運行狀況得分根據記憶體利用率、通道利用率、空氣品質、干擾和流量利用率來計算。為此，請導航到Provision > Inventory > Access Point > Click AP:

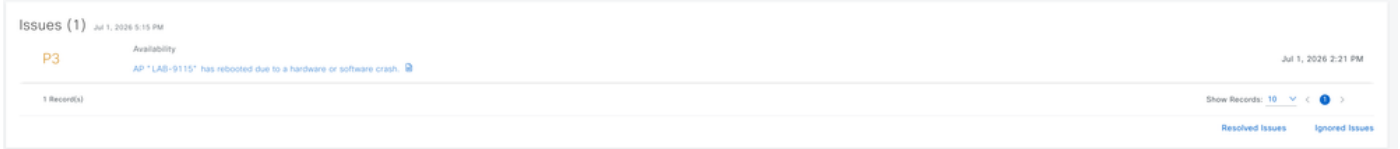


檢視單個AP的360

裝置360遙測摘要：在這裡，您可以看到兩個無線電的AP整體運行狀況得分時間線、系統資源利用率（記憶體、CPU）、資料平面連結錯誤和無線電特定統計資訊（雜訊、通道利用率、干擾、流量利用率）。通過裝置360，您可以將運行狀況時間表滑塊移回支援的歷史視窗內的任何點（30天）。

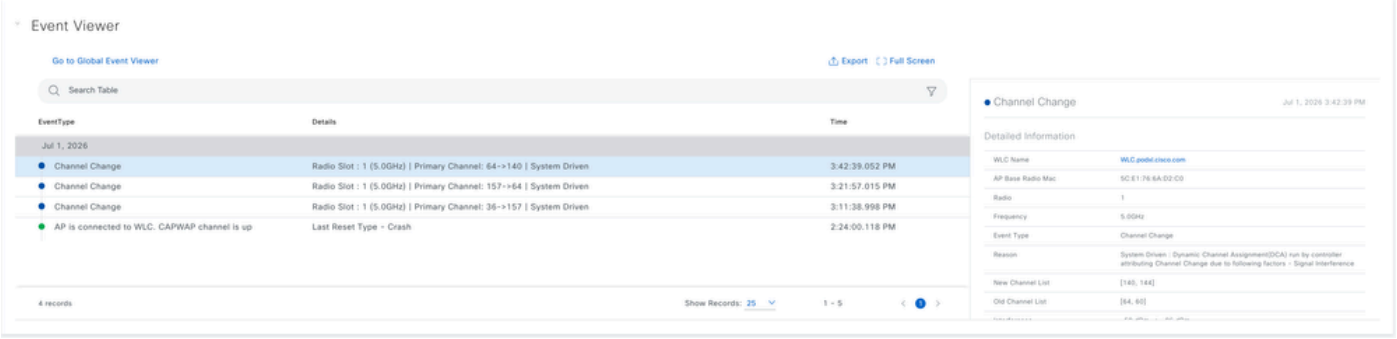
檢視360:AP遙測狀態和運行狀況

問題 — 在這裡，您可以看到AP的未解決問題清單以及嚴重性(P1-P4)、問題類別、說明和時間戳。



為AP報告的問題

事件檢視器 — 您可以檢視AP事件按時間順序排列的日誌（例如，通道更改、CAPWAP狀態）以及詳細的事件資訊，如WLC名稱、射頻、頻率、原因和舊/新通道清單。

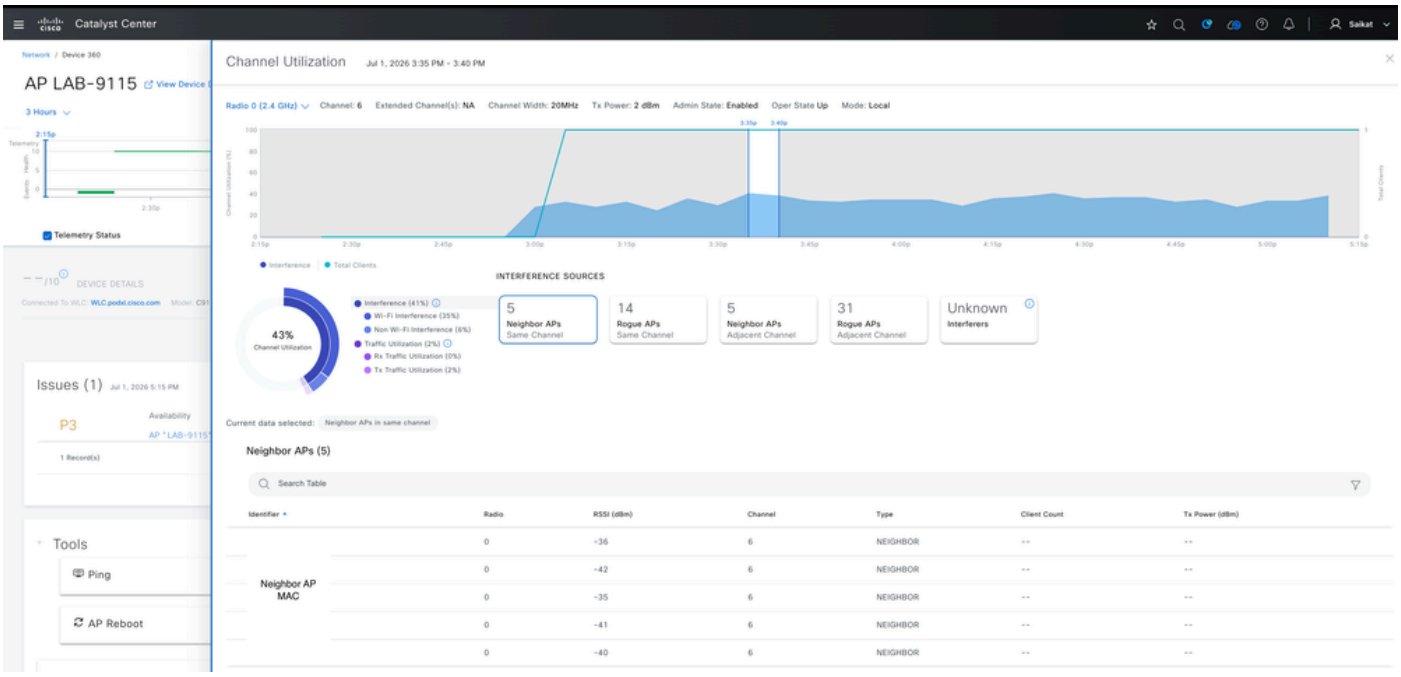


單個AP的事件檢視器

包含客戶端清單的物理鄰居拓撲 — 此檢視顯示連線WLC、AP和已連線客戶端的物理拓撲，以及其他客戶端詳細資訊，如裝置名稱、運行狀況得分和MLO

AP的物理拓撲

通道利用率 — 您可以檢視AP通道利用率趨勢、干擾源（鄰居AP、欺詐AP、未知干擾源）以及包含RSSI、通道和型別的詳細鄰居AP表。



單個AP的通道利用率

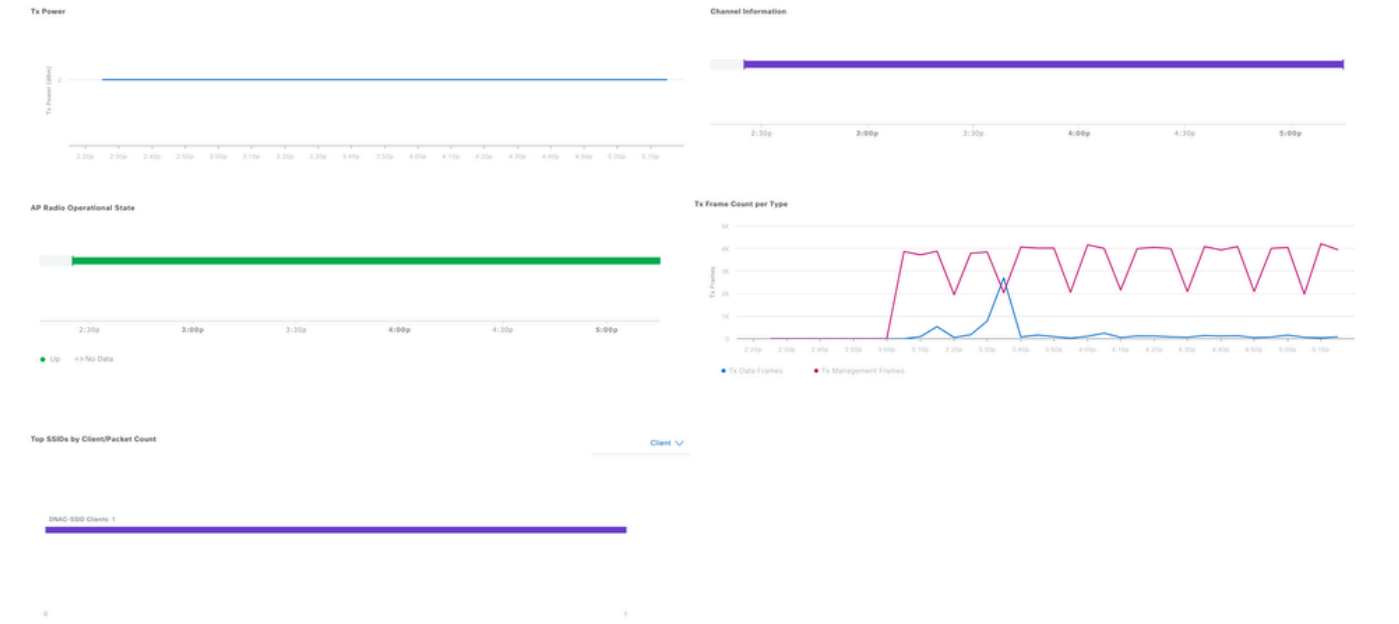
詳細資訊（裝置頁籤）— 此部分顯示裝置資訊（AP名稱、IP、型號、MAC地址、軟體版本）、可用性詳細資訊（正常運行時間、控制器加入時間、上次重置原因）、CPU/記憶體利用率圖形以及AP到WLC的連線圖表。

AP的裝置詳細資訊

無線電特定KPI:在此您可以檢視無線電級別的KPI，包括所選無線電的通道利用率、客戶端計數、吞吐量（Rx/Tx速率）、重試次數、雜訊和空氣品質。

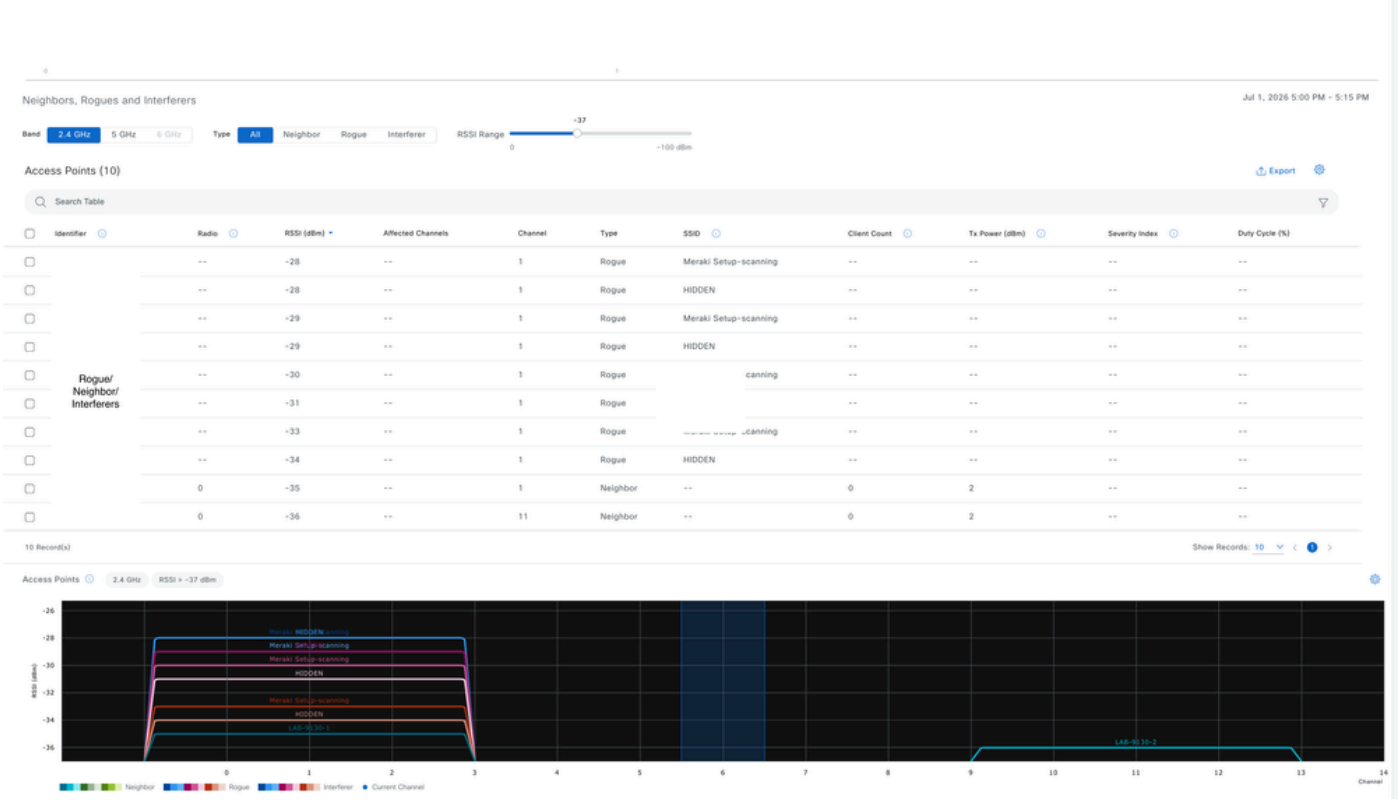
單個AP的RF統計資訊

Tx功率、通道資訊和幀統計資訊:在此螢幕上，您可以檢視Tx功率趨勢、通道分配歷史記錄、AP無線電運行狀態、Tx幀計數（資料與管理）以及按客戶端/資料包計數排在前的SSID。



單個AP的RF統計資訊

鄰居、流氓和干擾者：通過此檢視，您可以檢視所有鄰近的鄰居、欺詐裝置和干擾裝置及其RSSI、受影響的通道、SSID、客戶端計數、發射功率和嚴重性指數，以及可視RSSI與通道圖。



報告單個AP的惡意、鄰居和干擾源

Device 360控制面板彙集了射頻詳細資訊（如通道使用、干擾、雜訊和重試）以及附近的鄰居、欺詐和干擾資訊 — 幫助您確定AP問題是由射頻擁塞、通道衝突還是欺詐裝置引起的。裝置運行狀況資料（如CPU、記憶體、重新啟動歷史記錄和連線狀態）以及Event Viewer and Issues（事件檢視器和問題）面板，可幫助您瞭解硬體崩潰、連線丟失和意外的通道更改。結合拓撲和客戶端檢視，可全面瞭解從RF問題到單個客戶端問題的故障排除過程，並內建建議操作以幫助解決這些問題

接入點的智慧捕獲

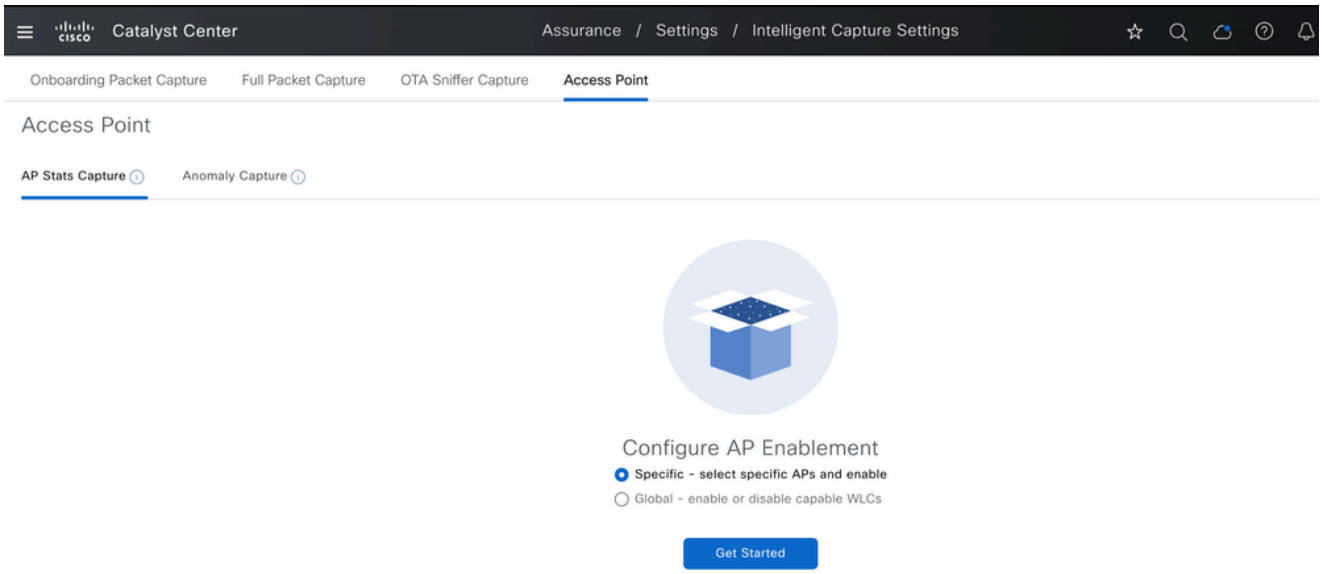
適用於存取點的智慧擷取提供兩個主要功能：不間斷即時射頻監控、異常檢測和空中按需捕獲、頻譜分析。

AP統計資訊捕獲

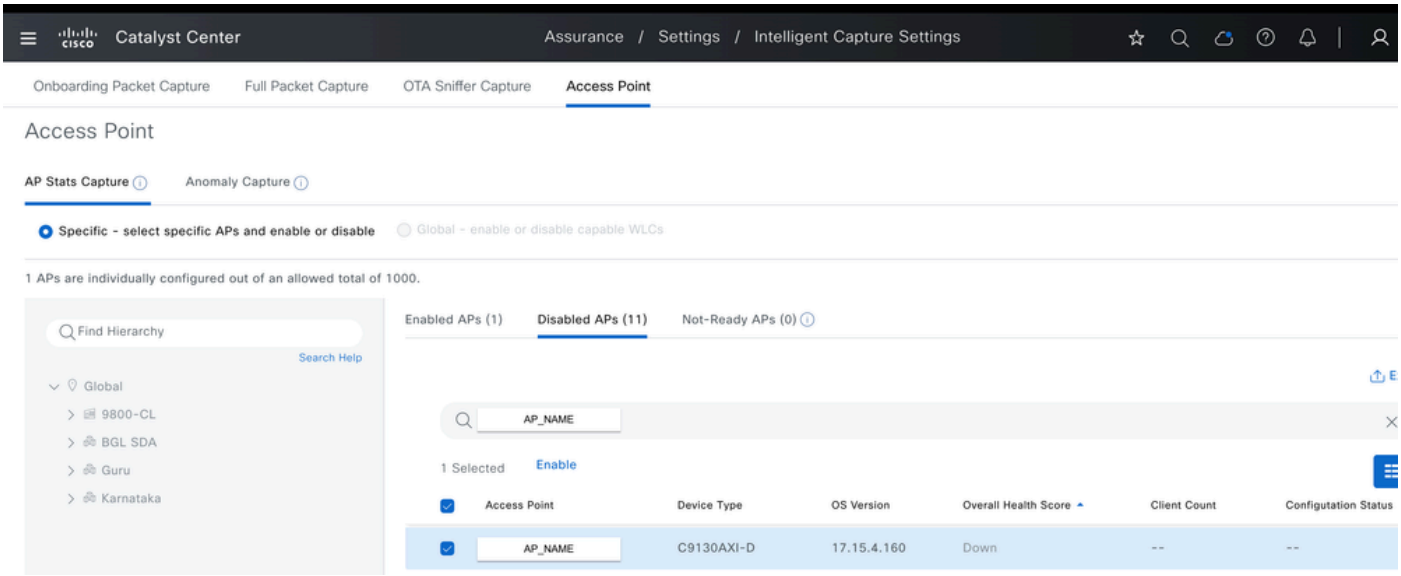
您可以啟用和管理一個或多個接入點的AP統計資訊資料收集（包括AP無線電統計、WLAN統計和AP客戶端統計），最多可支援1000個AP。

要啟用AP狀態捕獲，請導航到保證>設定>智慧捕獲設定>接入點> AP狀態捕獲。從這裡開始，您可以靈活選擇：

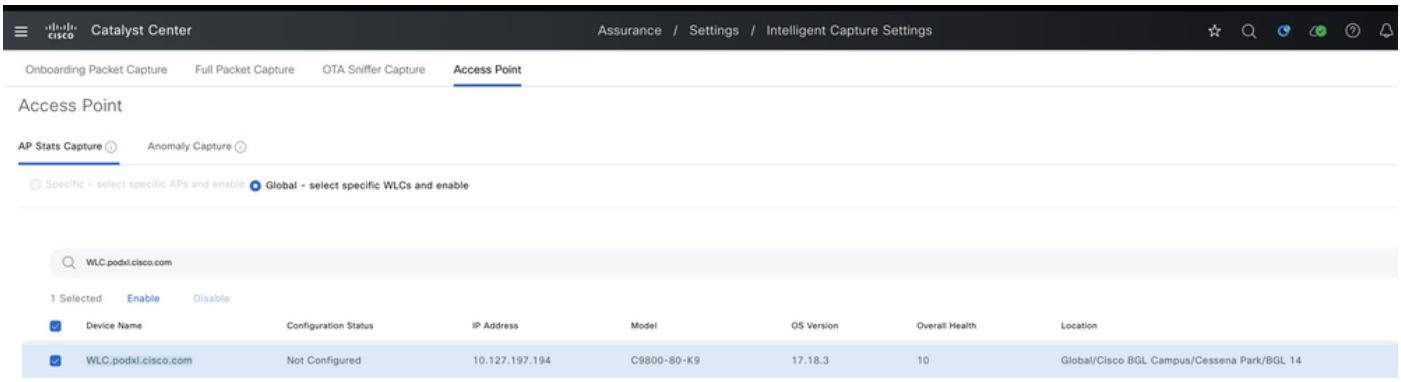
- 為特定AP（最多1000個）啟用它，或
- 為特定WLC下管理的所有AP全域性啟用此功能。



AP統計資訊捕獲選項

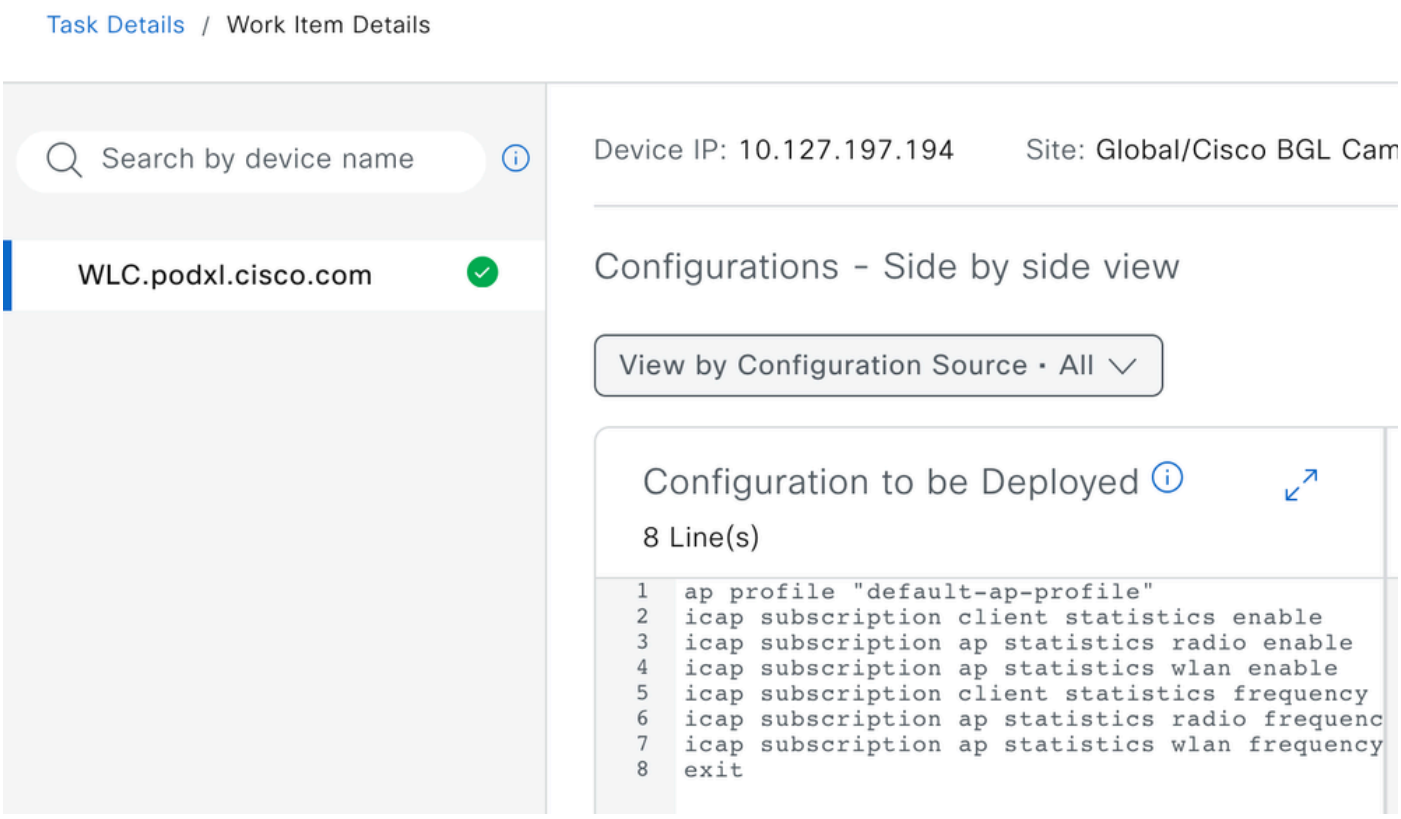


在特定AP上啟用AP狀態智慧捕獲



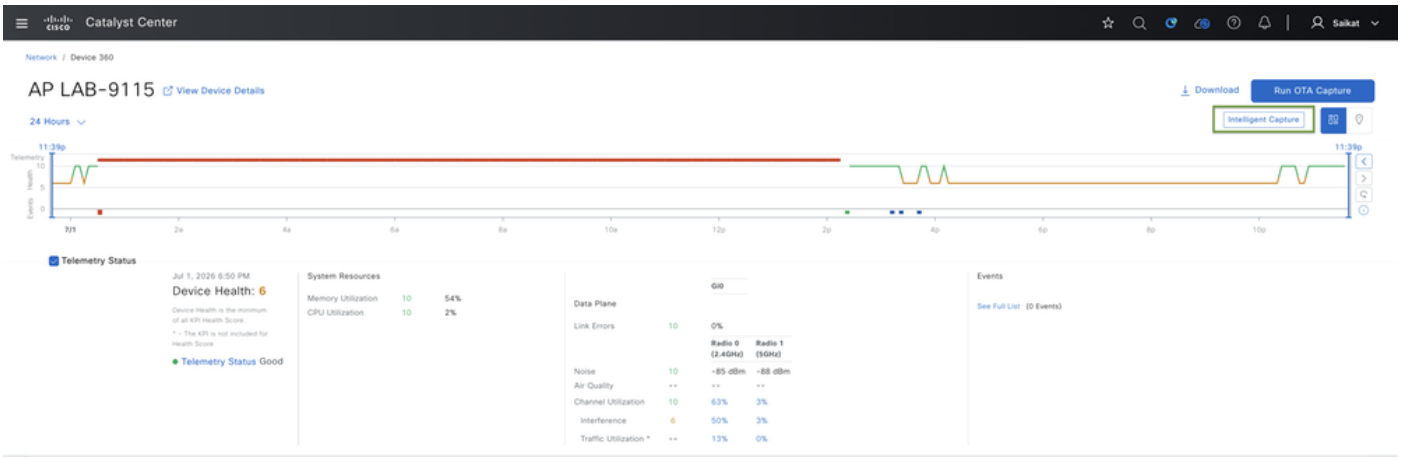
全域性啟用AP統計資訊智慧捕獲

啟用AP Stats Capture後，Catalyst Center會將相應的配置推送到WLC — 適用於選定的特定AP或所有AP，具體取決於它是在單個AP級別啟用還是在WLC級別全域性啟用。

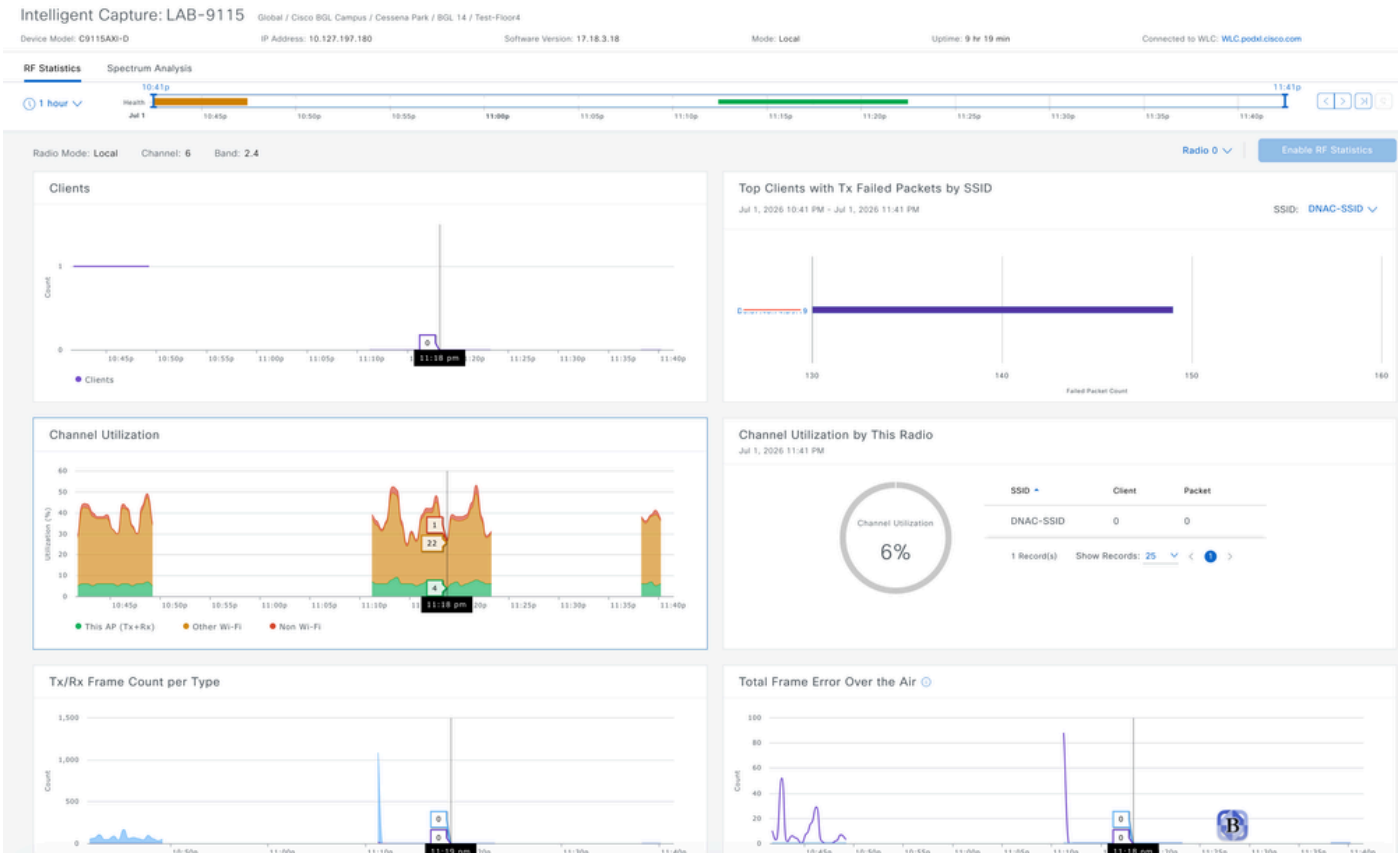


啟用AP統計資訊捕獲時要推送的配置

啟用此捕獲後，您可以直接從Device 360頁檢視通過智慧捕獲收集的即時資料。此外，您可以根據需要運行頻譜分析，以進一步調查RF情況。



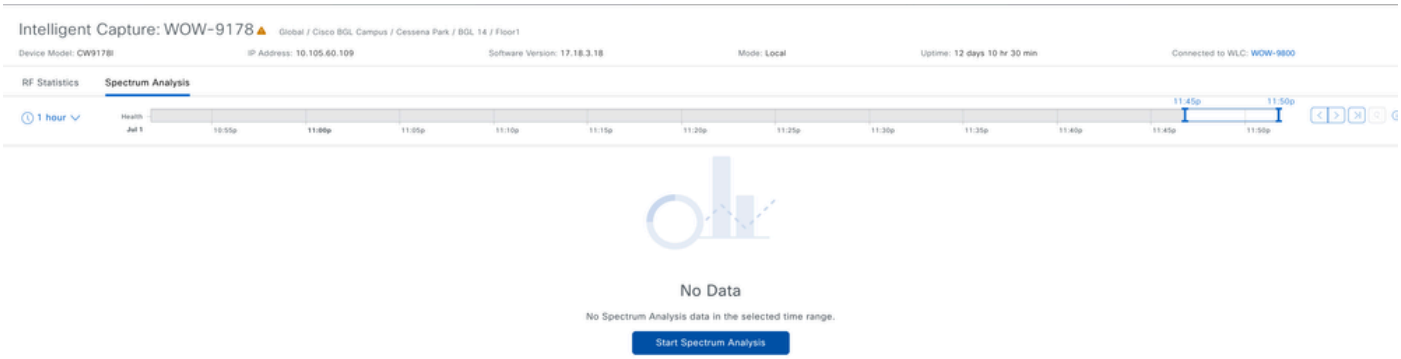
裝置360中AP的智慧捕獲



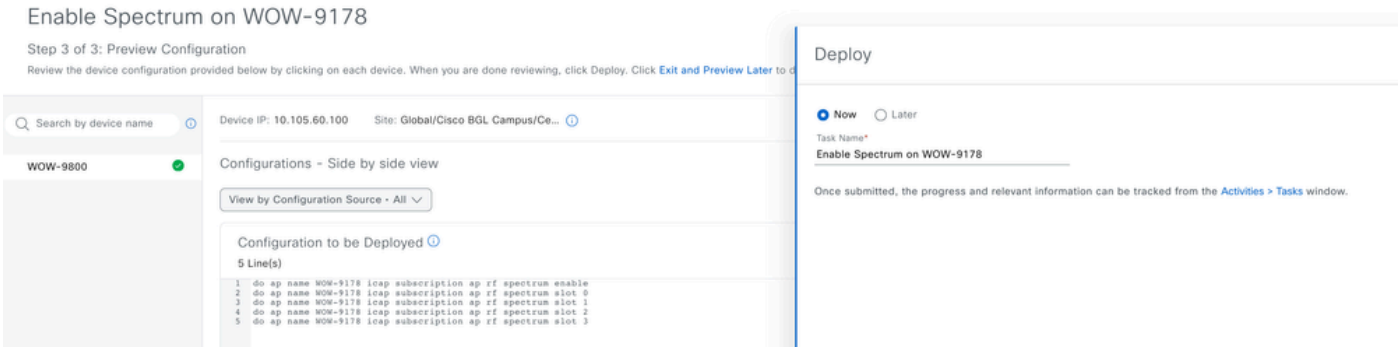
在Catalyst Center上使用智慧捕獲捕獲AP統計資訊

在這裡，您可以看到即時統計資訊，包括每種型別的Tx/Rx幀計數、空中幀錯誤總數、組播/廣播計數器、Tx功率和雜訊最低限、通道利用率、按SSID顯示失敗的Tx資料包的頂級客戶端，以及使用智慧捕獲為特定AP捕獲的客戶端資料。

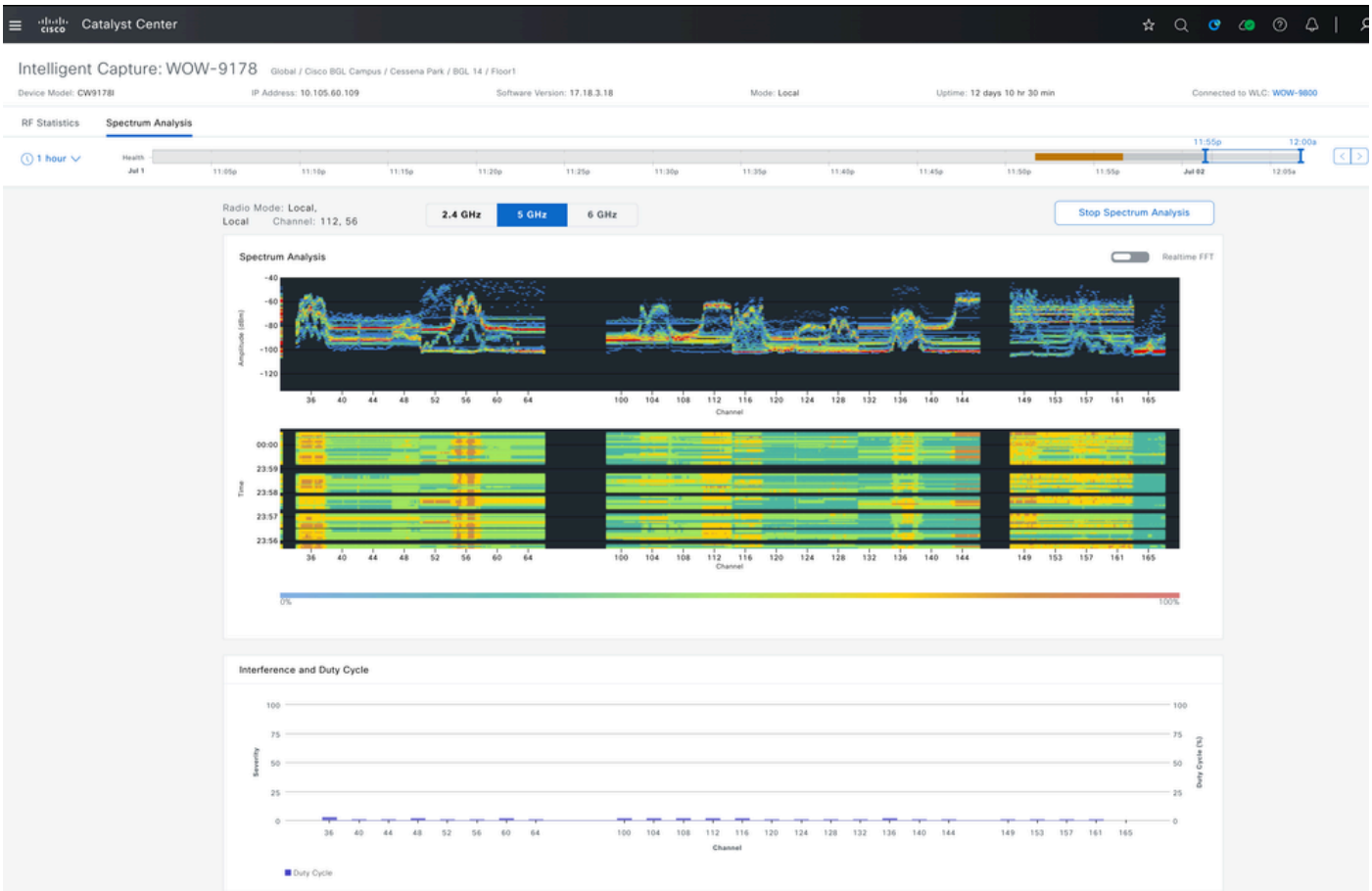
在需要檢查RF條件時，還可以對單個AP運行按需頻譜分析。但是，此功能需要AP型號支援它。



按需頻譜分析



配置在頻譜分析中的應用

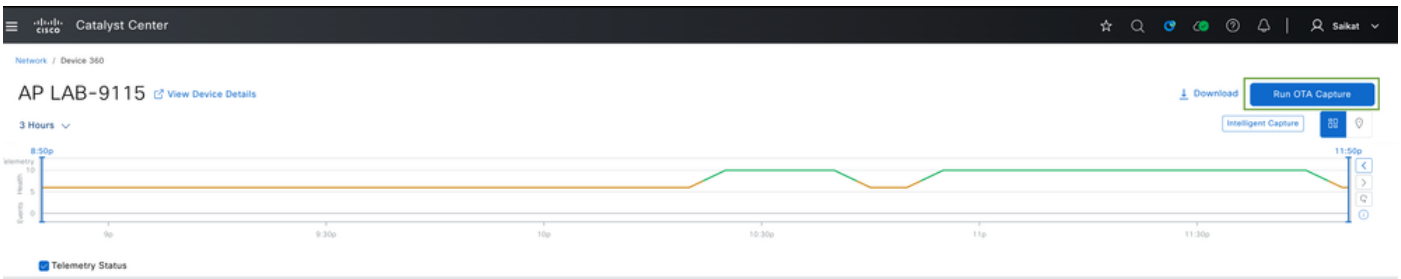


頻譜分析結果

OTA監聽器擷取

Catalyst Center允許您在特定無線電、頻寬和通道上啟用OTA監聽器捕獲。一旦啟用，在該無線電和通道上傳輸的所有Wi-Fi資料包都會被捕獲。您最多可以選擇2個AP來執行嗅探。請記住，只要啟用OTA捕獲，為流量監聽配置的2個AP即可在其各自的無線電/插槽上切換到監聽器模式。

要啟用此功能，請導航到Provision > Inventory > Access Points，按一下要為其收集OTA資料的AP，然後選擇Run OTA Capture。最多可以選擇兩個附近的接入點來嗅探流量。

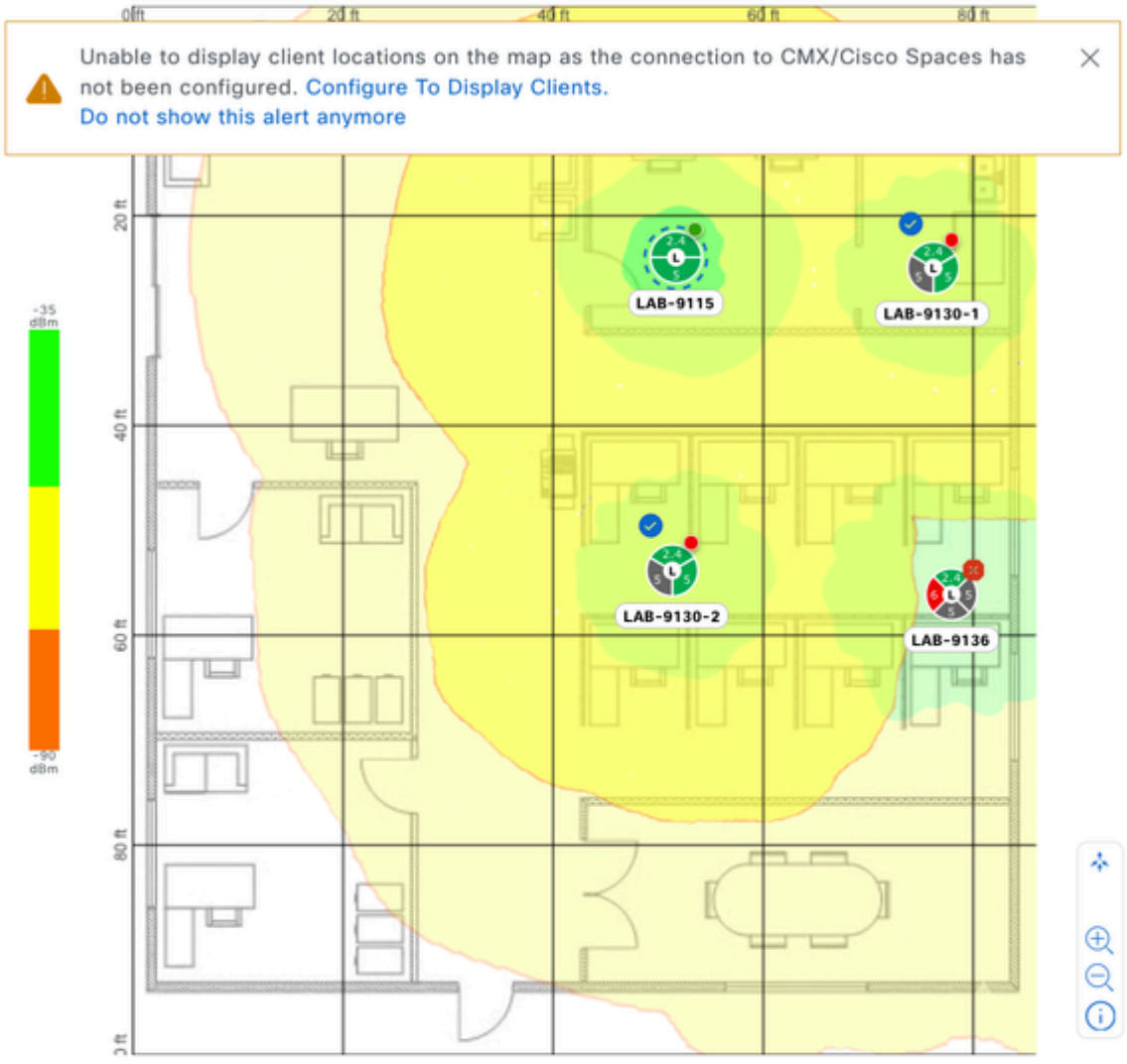


對目標AP運行OTA捕獲

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



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

選擇鄰居AP（最多2個）以嗅探流量

Run OTA Capture

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

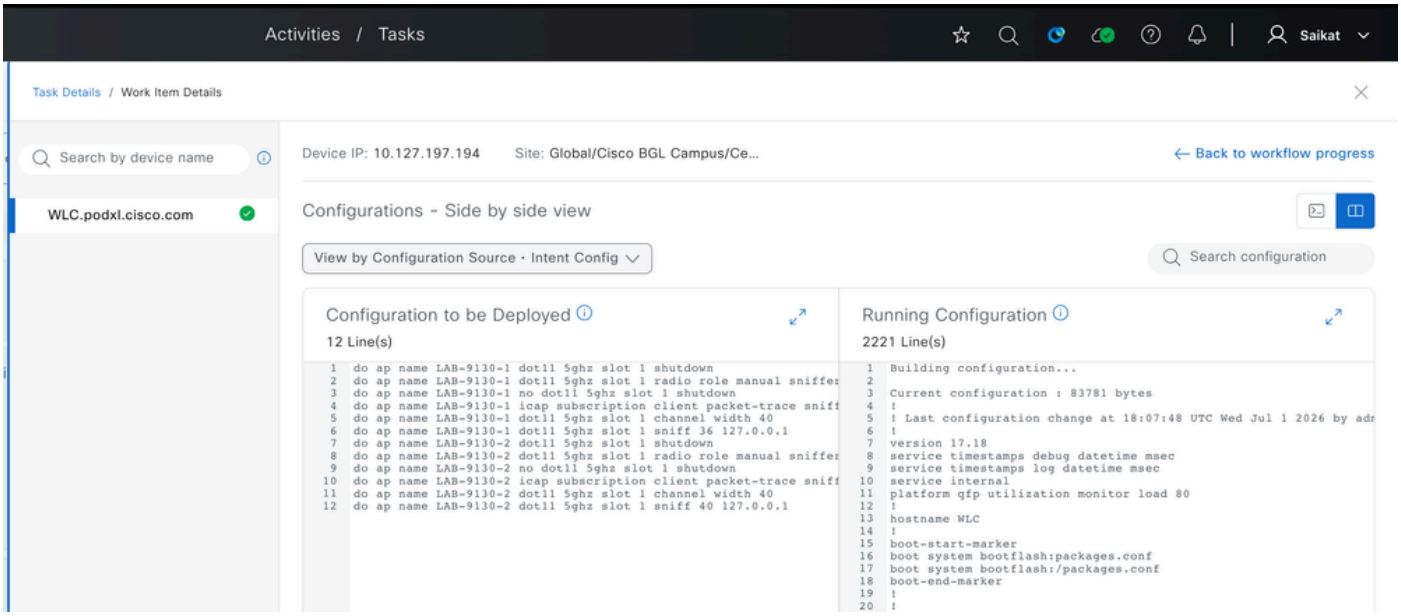
Select Radio
1 (Client Count: 0)

Select Channel Width
40

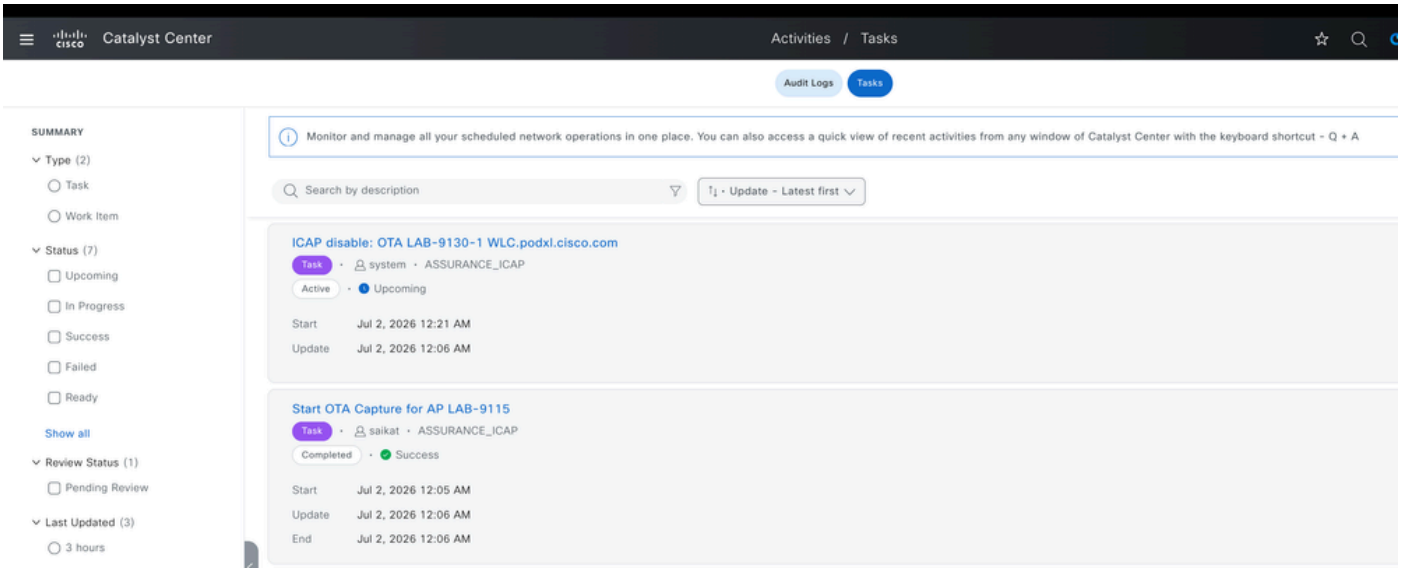
Select Channel
40

back Next

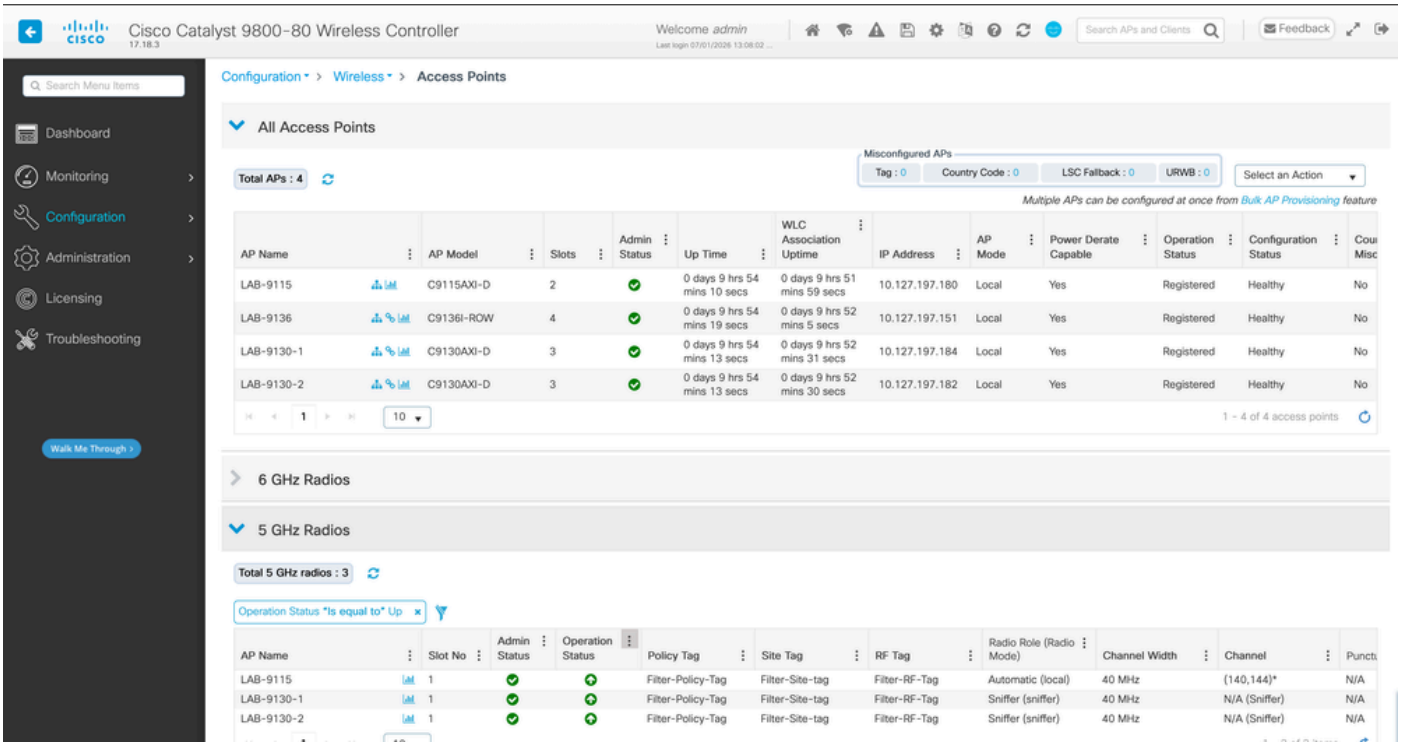
選擇Radio、Channel-Width、Channel以監聽流量



啟用OTA捕獲的配置預覽

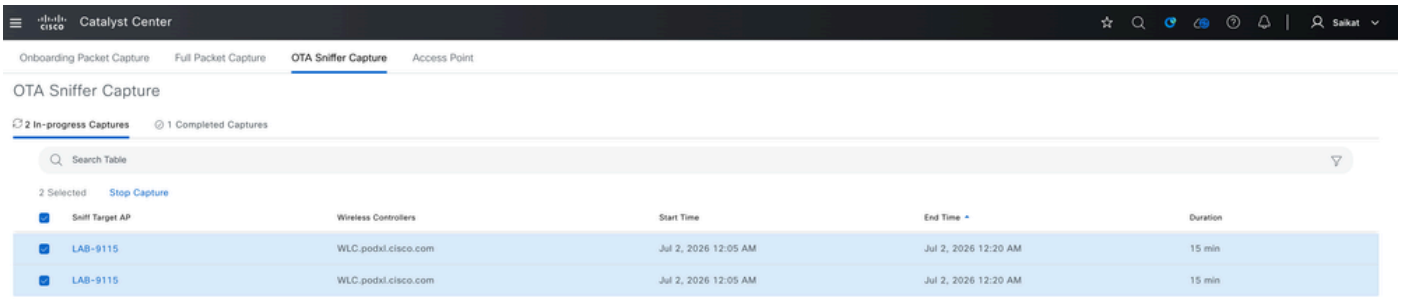


啟用OTA捕獲時計畫任務



已啟用的AP在監聽器模式下用於監聽流量的插槽1

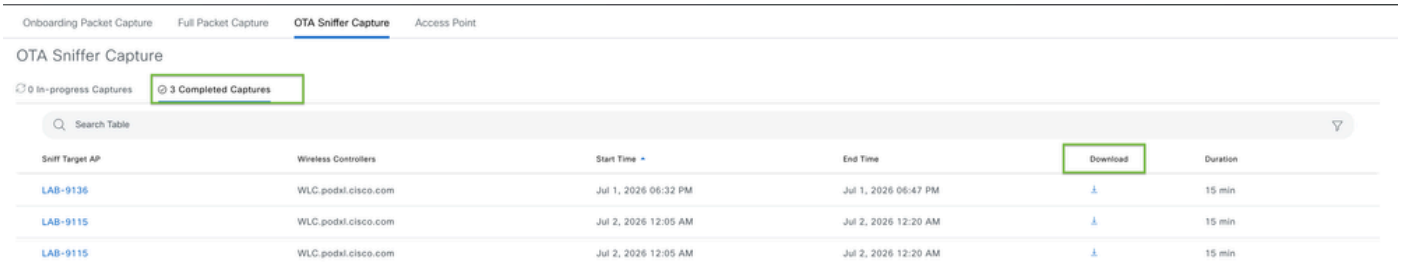
要檢查運行OTA捕獲的狀態，請導航到保證>設定>智慧捕獲設定> OTA監聽器捕獲:



OTA捕獲的狀態

附註：預設情況下，Catalyst Center在自動禁用此任務之前運行該任務15分鐘，但也可以隨時手動停止該任務。

完成OTA捕獲後，該捕獲將顯示在完成的捕獲部分，您可以從那裡下載檔案。



已完成捕獲 — OTA監聽器捕獲

異常檢測

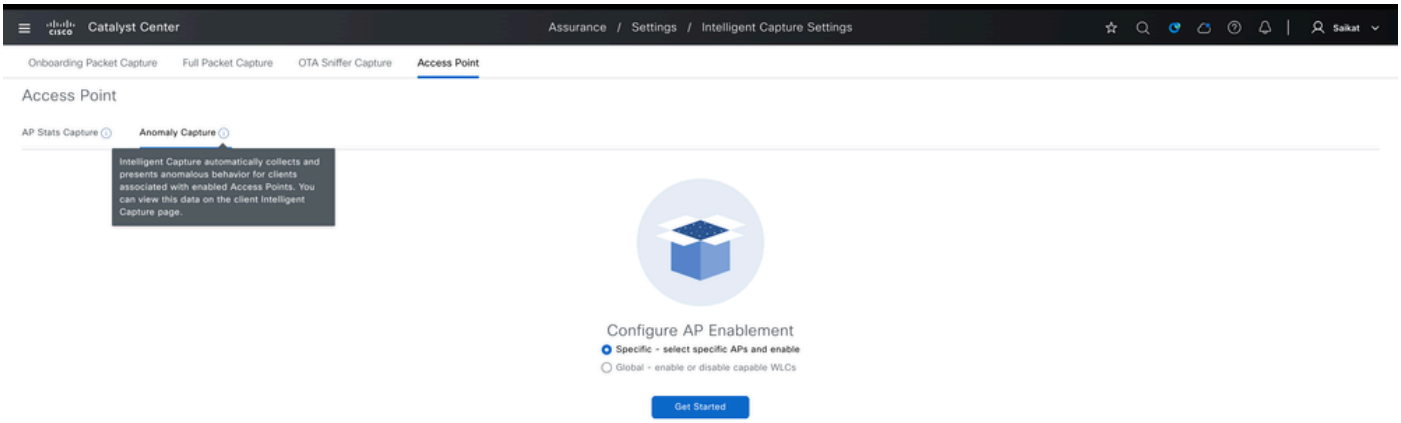
此功能允許思科AP檢測與其關聯的無線客戶端的行為中可能的不規則行為。它包括：

- 異常檢測
- 異常資料包捕獲
- 異常個體報告
- 異常摘要報告

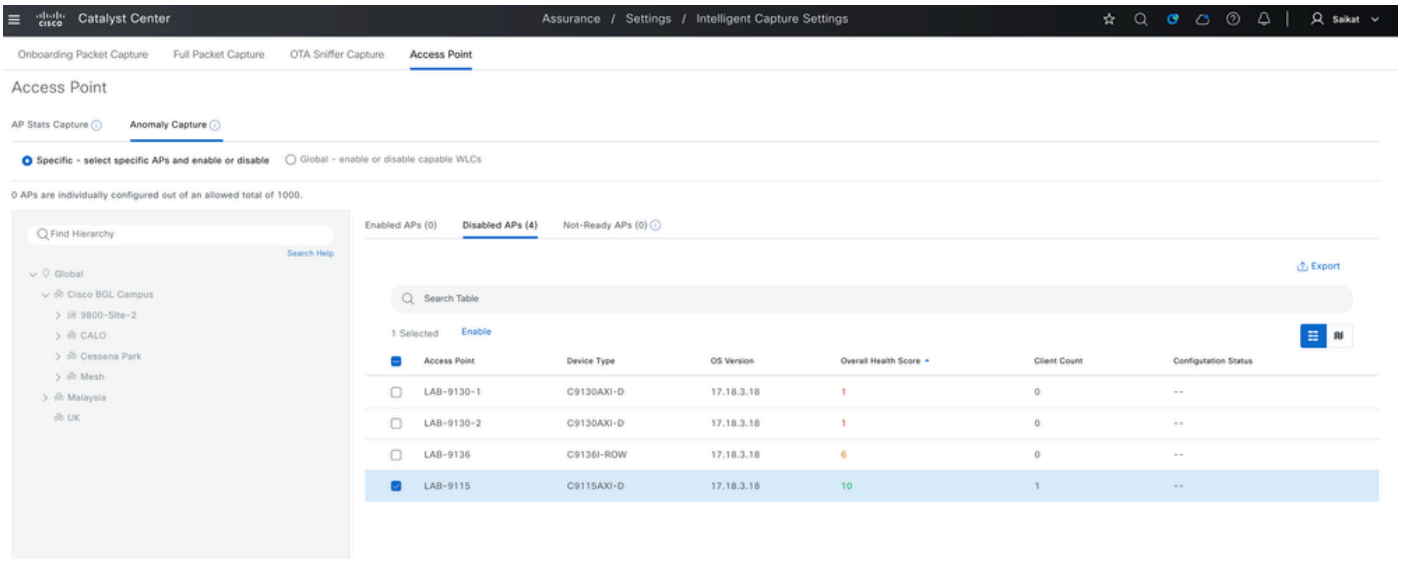
要啟用AP異常捕獲，請導航到保證>設定>智慧捕獲設定>接入點>異常捕獲。在此處，您可以靈活地執行以下操作：

- 為特定AP（最多1000個）啟用它，或
- 為特定WLC下管理的所有AP全域性啟用此功能。

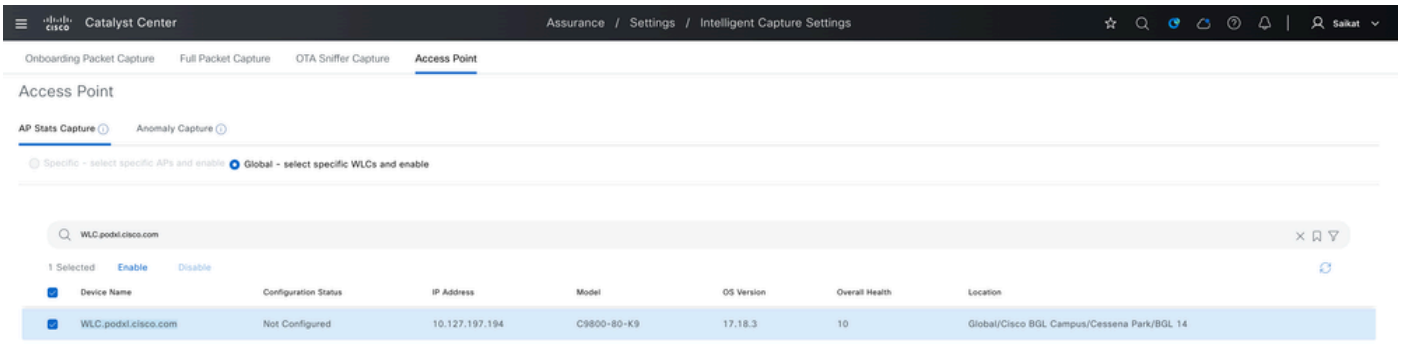
啟用後，智慧捕獲將自動收集與這些AP關聯的客戶端並顯示異常行為，並且可以在「客戶端智慧捕獲」頁面檢視此資料。



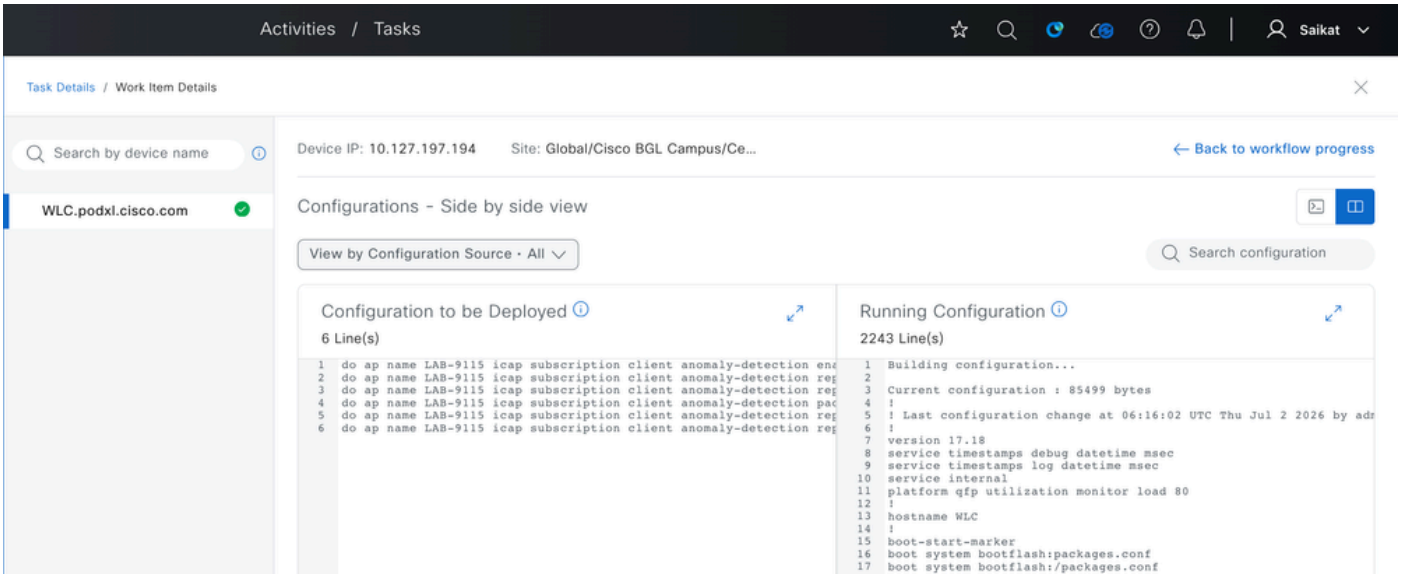
配置異常捕獲



為特定AP啟用異常捕獲

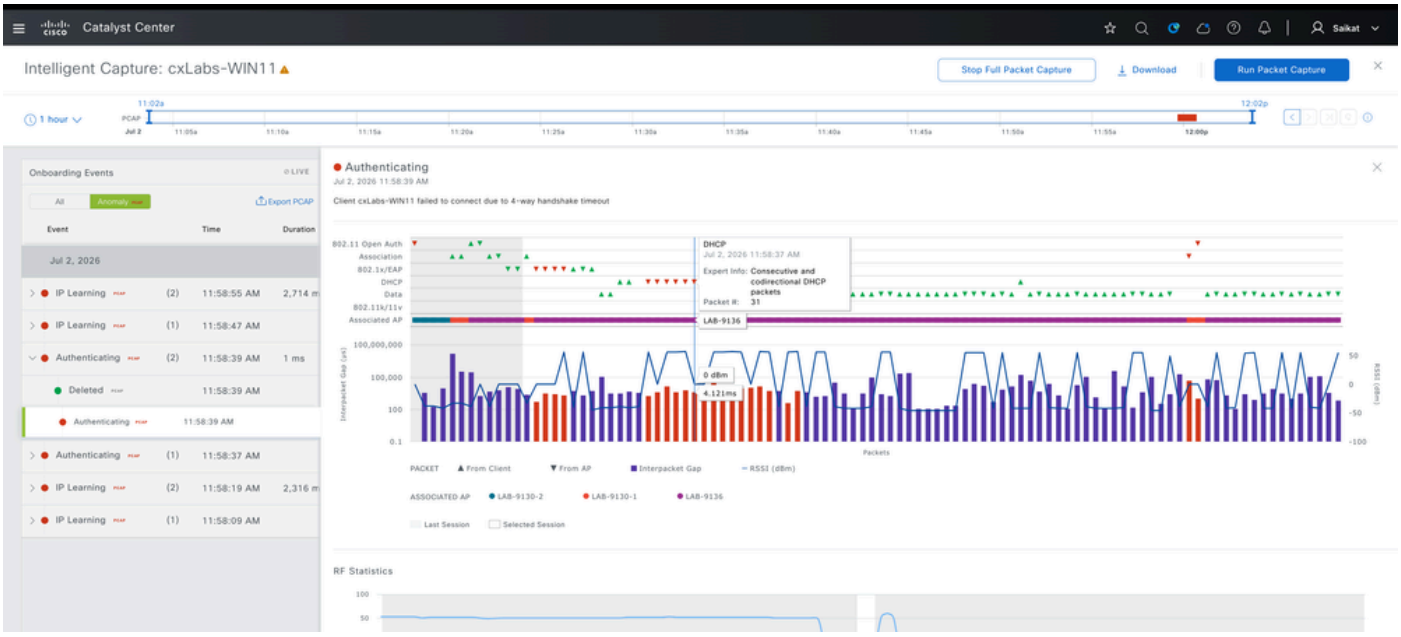


為特定WLC全域性啟用異常捕獲

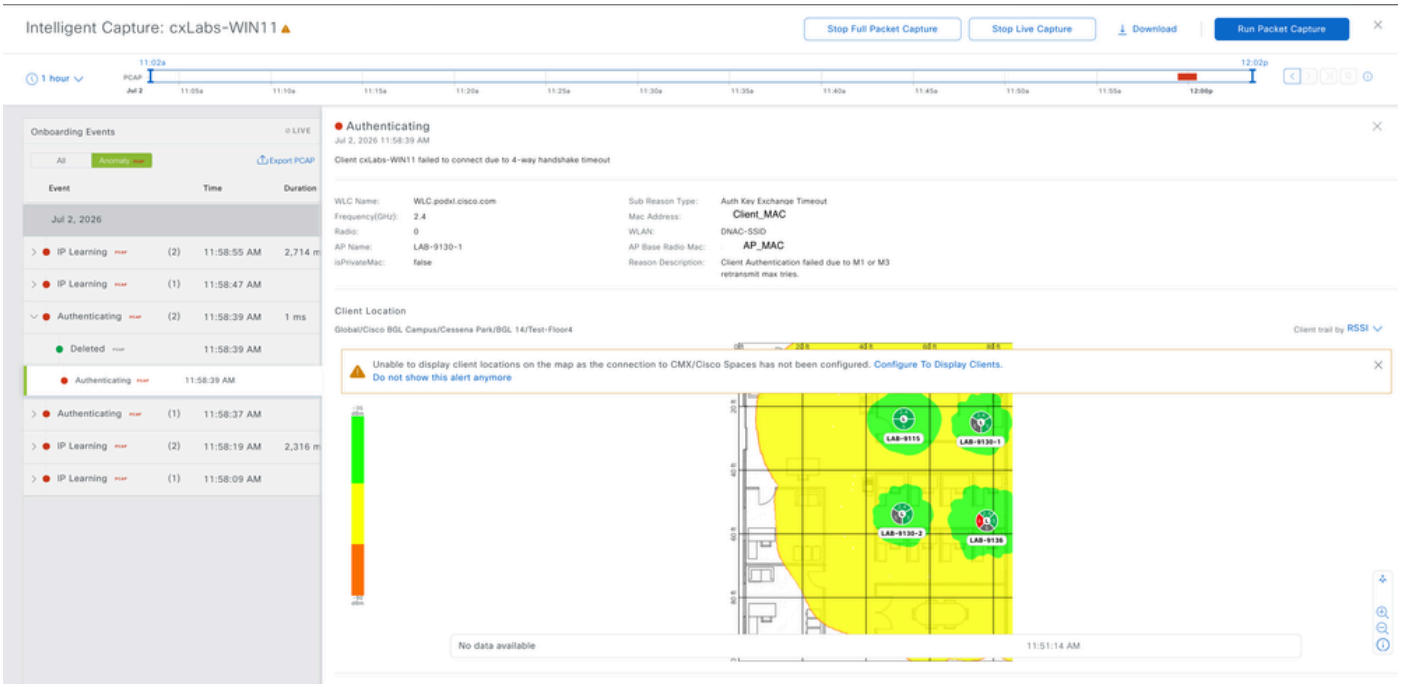


異常捕獲的配置預覽

啟用後，它會持續收集與AP關聯的客戶端的異常行為，並且可以在針對特定客戶端ID進行的智慧捕獲（載入和完整）中檢視這些異常行為。



客戶端的異常捕獲檢視



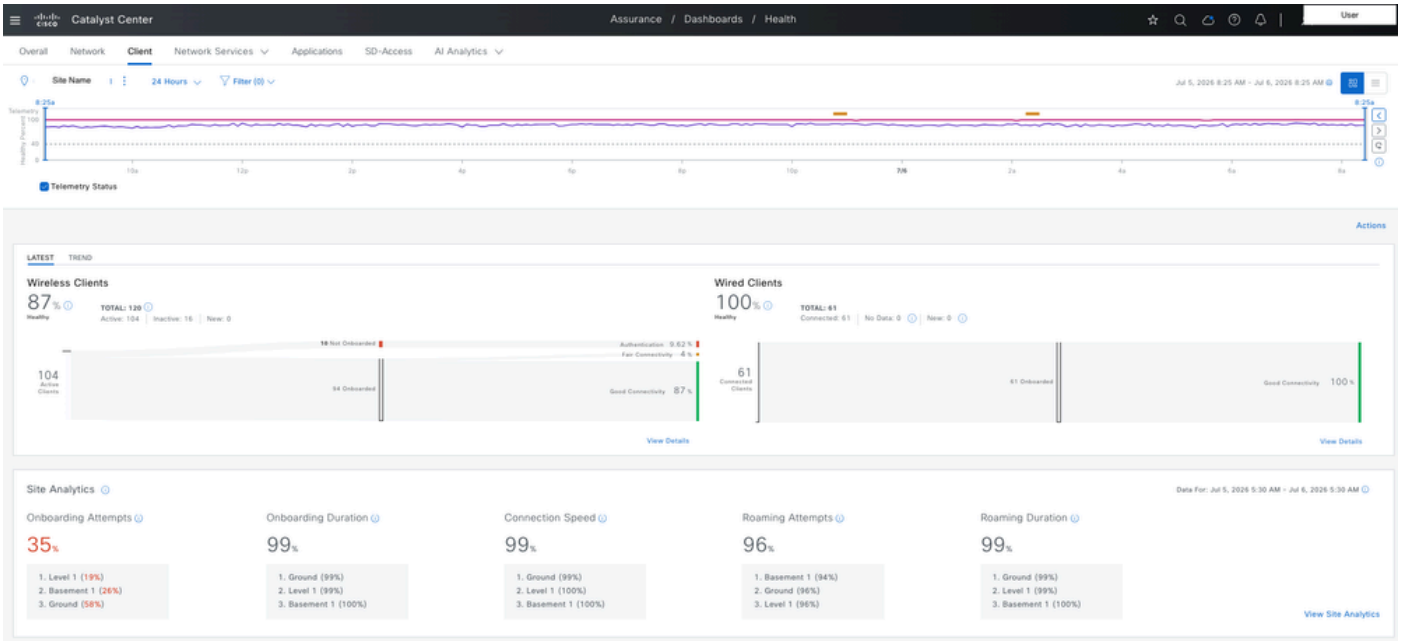
客戶端的異常捕獲詳細資訊

利用此功能，我們可以自動檢測和標籤處於啟用狀態的AP的這些事件，從而排除不規則或意外的客戶端行為（例如登入失敗、身份驗證問題或異常關聯模式）。結合針對特定客戶端ID的載入和完整資料包捕獲，管理員可以跟蹤導致異常的事件的確切順序，從而更輕鬆地查明反複出現的客戶端連線或效能問題的根本原因，而無需手動監控每個客戶端會話。

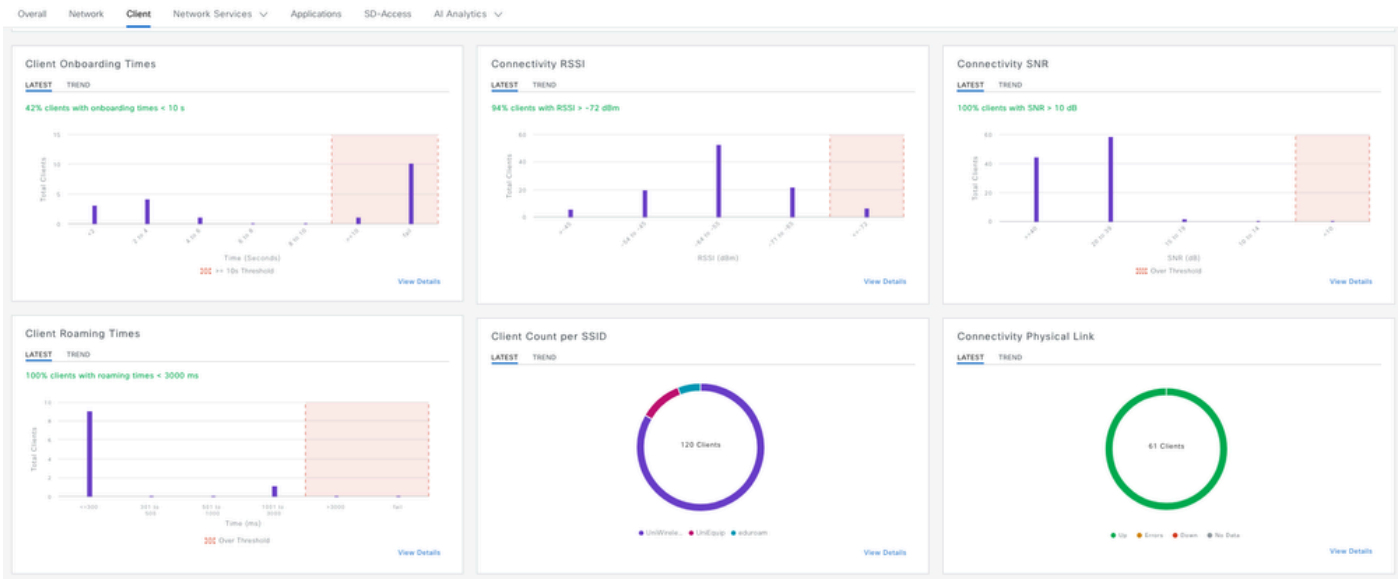
無線客戶端連線問題

無線客戶端問題（自註冊故障、漫遊掉線、射頻干擾或間歇性連線）通常是暫時的，難以複製，使得傳統的基於輪詢的監控不足以對Cisco Catalyst中心進行故障排除，無法通過連續的、次秒級遙測直接從接入點和無線控制器收集、跨裝置360、客戶端360和智慧捕獲工作流程進行關聯，從而解決此缺陷。這種遙測驅動架構能夠在發生故障時（從通道利用和干擾到802.11自註冊幀）重建準確的射頻和協定級條件。

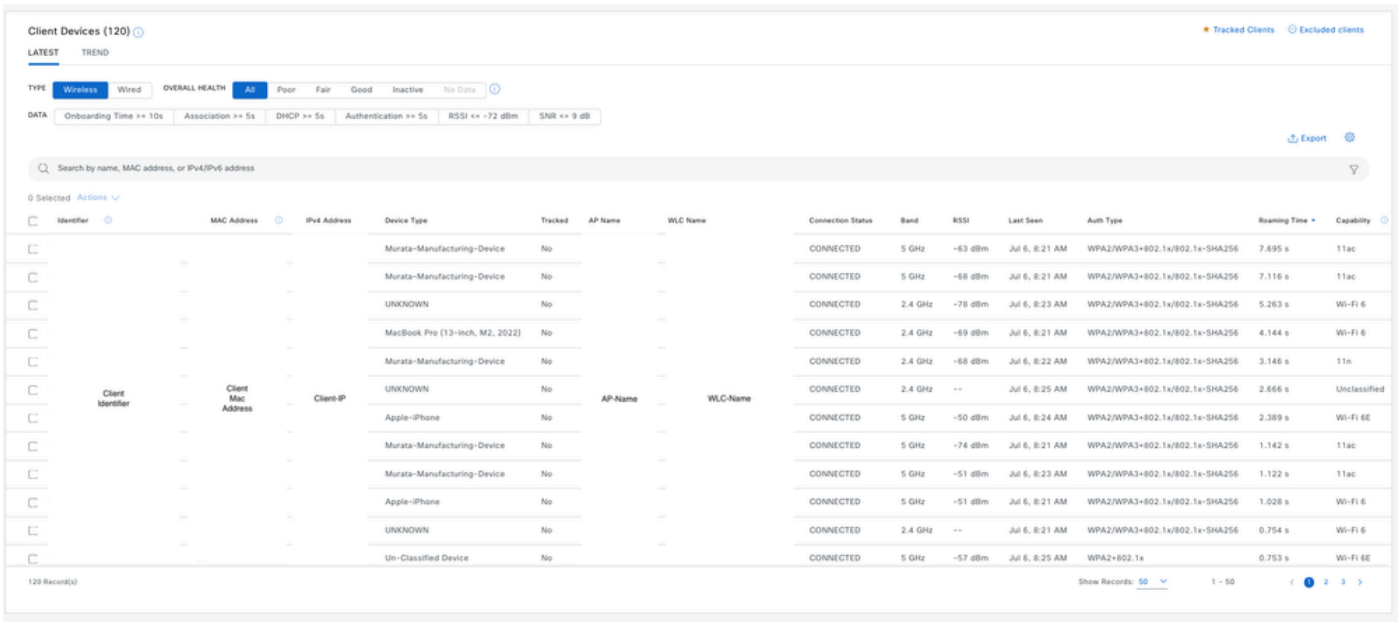
「客戶端運行狀況」部分提供所有站點的無線客戶端統計資訊的全面全域性概述。這包括關鍵指標，如入網效能、RSSI、SNR、漫遊活動、每SSID和每無線電分佈、資料速率和物理連線狀態。您可以按特定站點過濾此資料，並檢視過去30天的歷史趨勢，從而獲得網路範圍的視角和站點級別的細分度。導航至保證>控制面板>運行狀況>客戶端



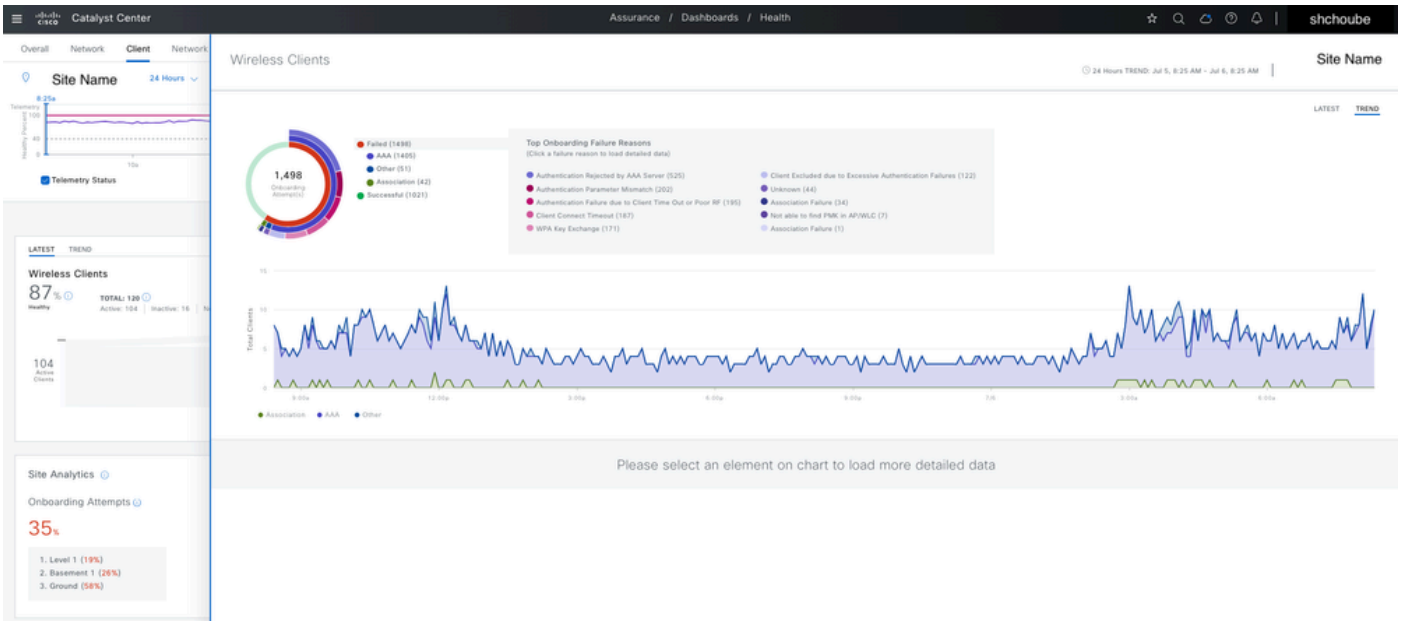
Catalyst Center上的無線客戶端統計資訊



Catalyst Center上的無線客戶端統計資訊

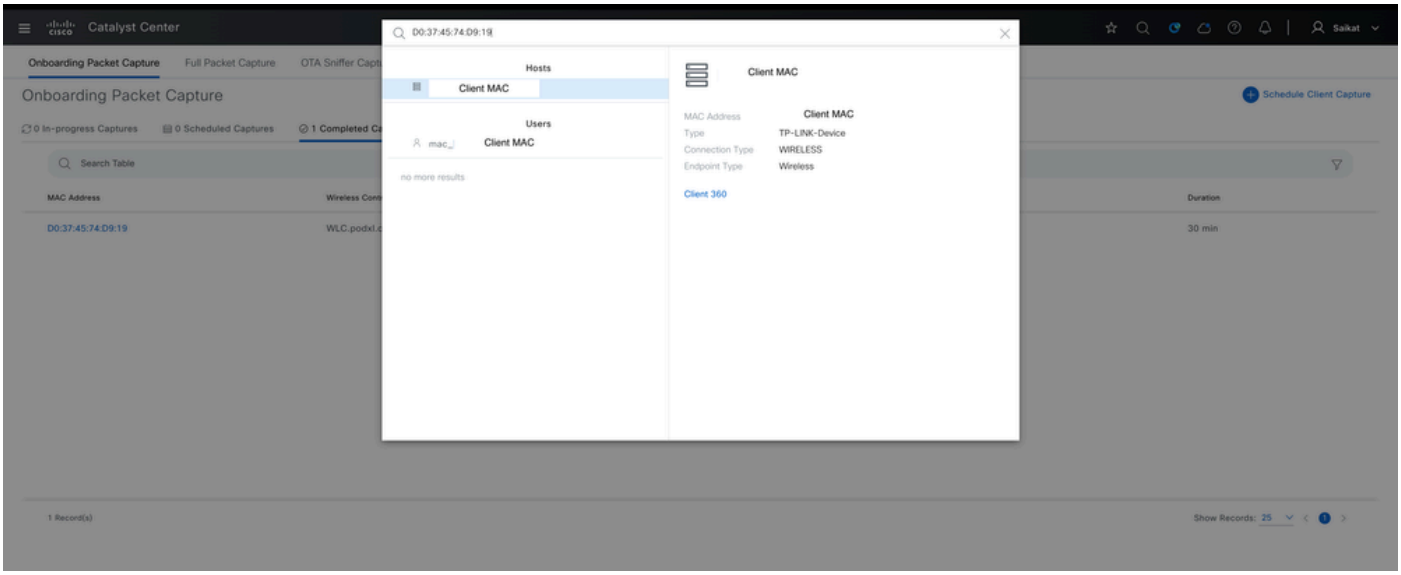


Catalyst Center上的無線客戶端統計資訊

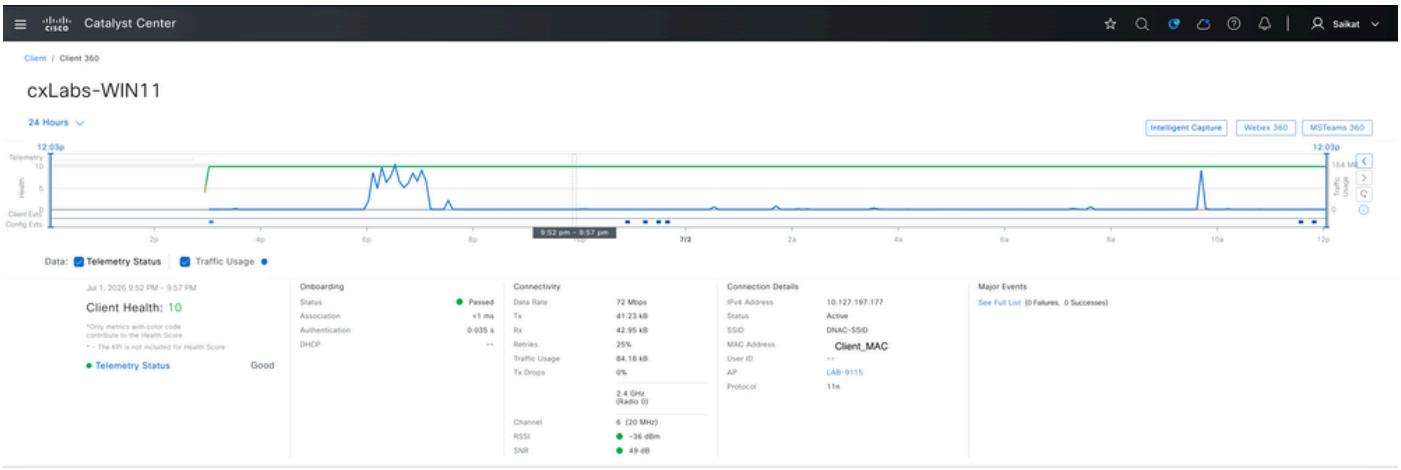


Catalyst Center上的無線客戶端統計資訊

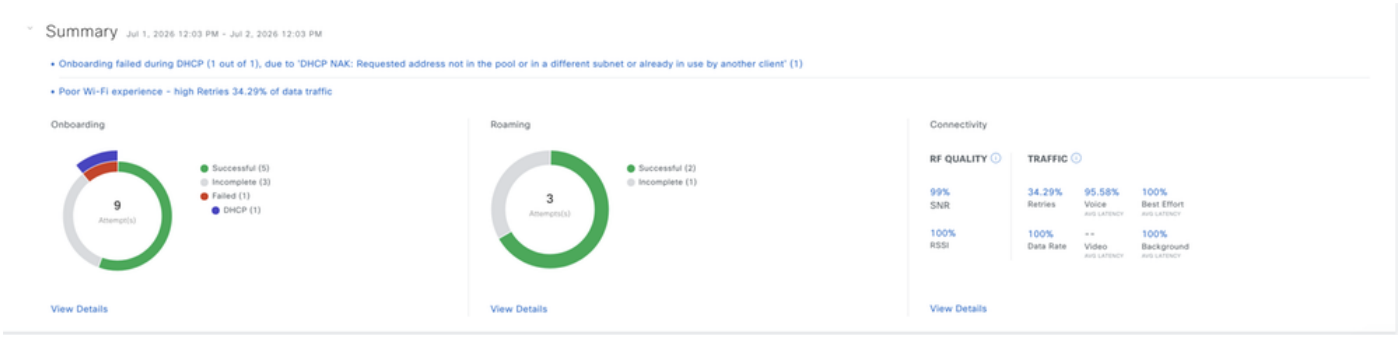
對於特定客戶端的故障排除，您可以使用客戶端MAC地址進行搜尋，該地址會將您帶到「客戶端360」檢視。此頁面顯示特定於客戶端的詳細統計資訊（包括自註冊歷史記錄、連線事件、RF指標和會話詳細資訊），這些統計資訊僅針對該單個客戶端，從而可以對單個客戶端問題進行精確的根本原因分析。



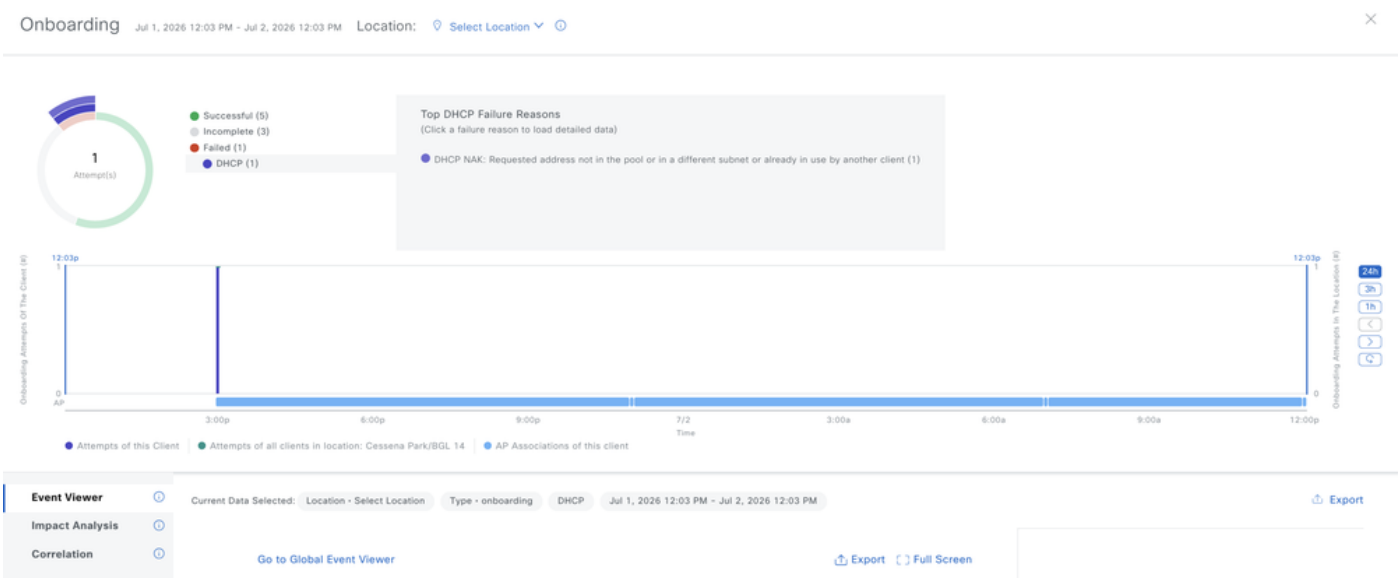
特定客戶端Mac地址裝置360



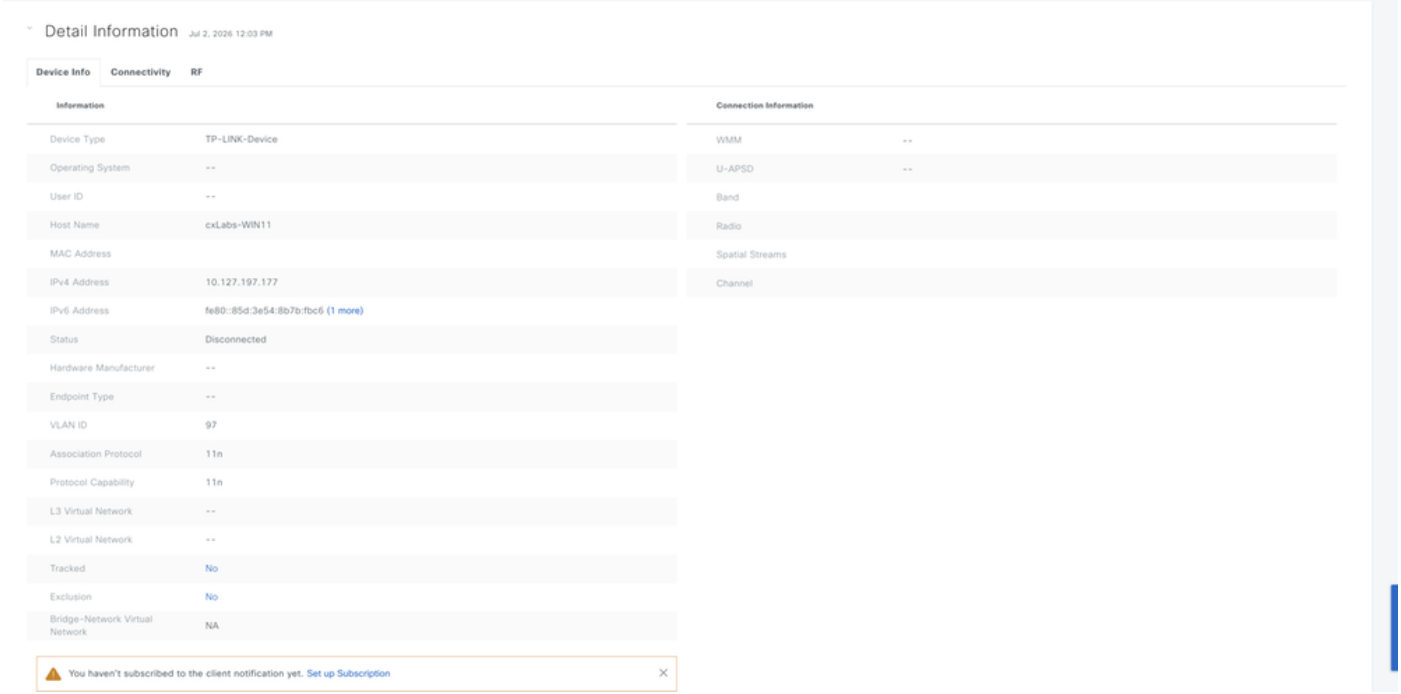
客戶端的遙測+運行狀況狀態



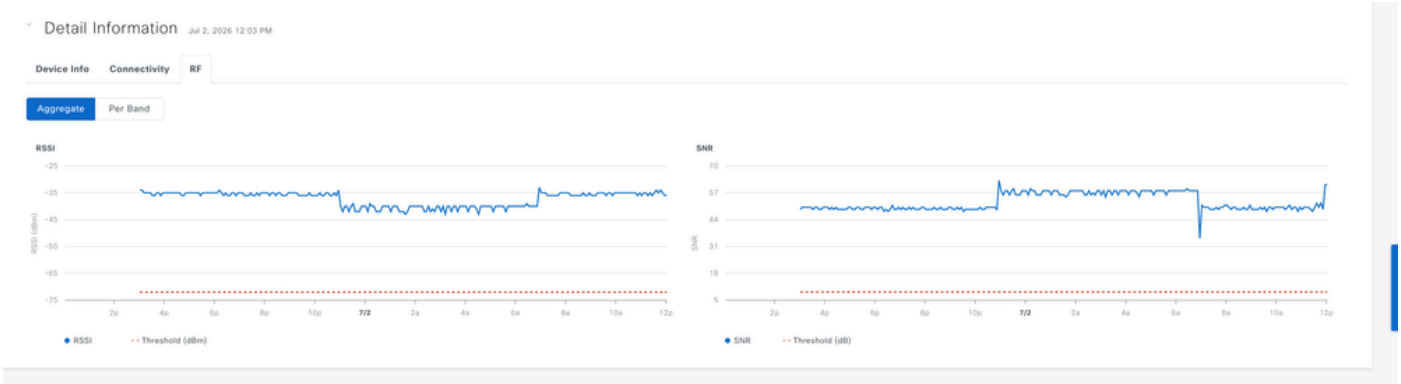
客戶端總體摘要



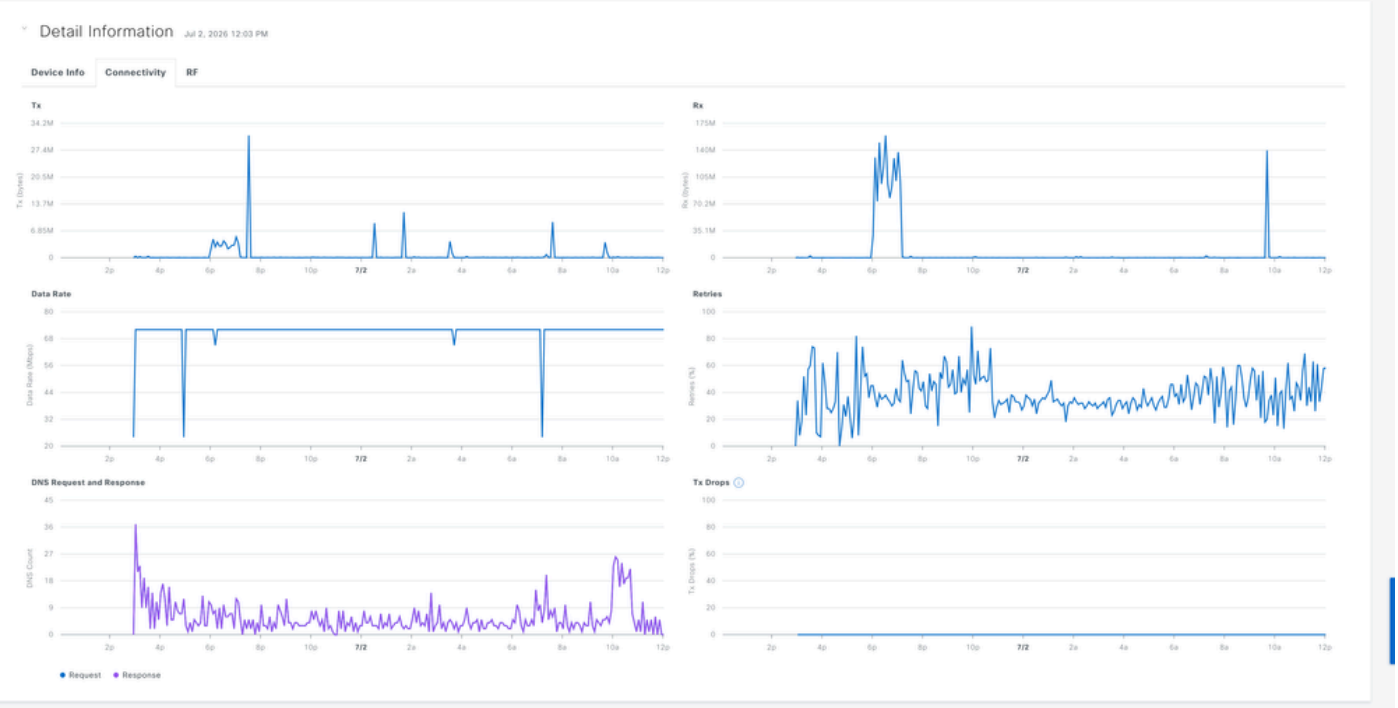
針對客戶端報告的事件詳細資訊



客戶端裝置詳細資訊



客戶端的RF統計資訊



客戶端的連線統計資訊

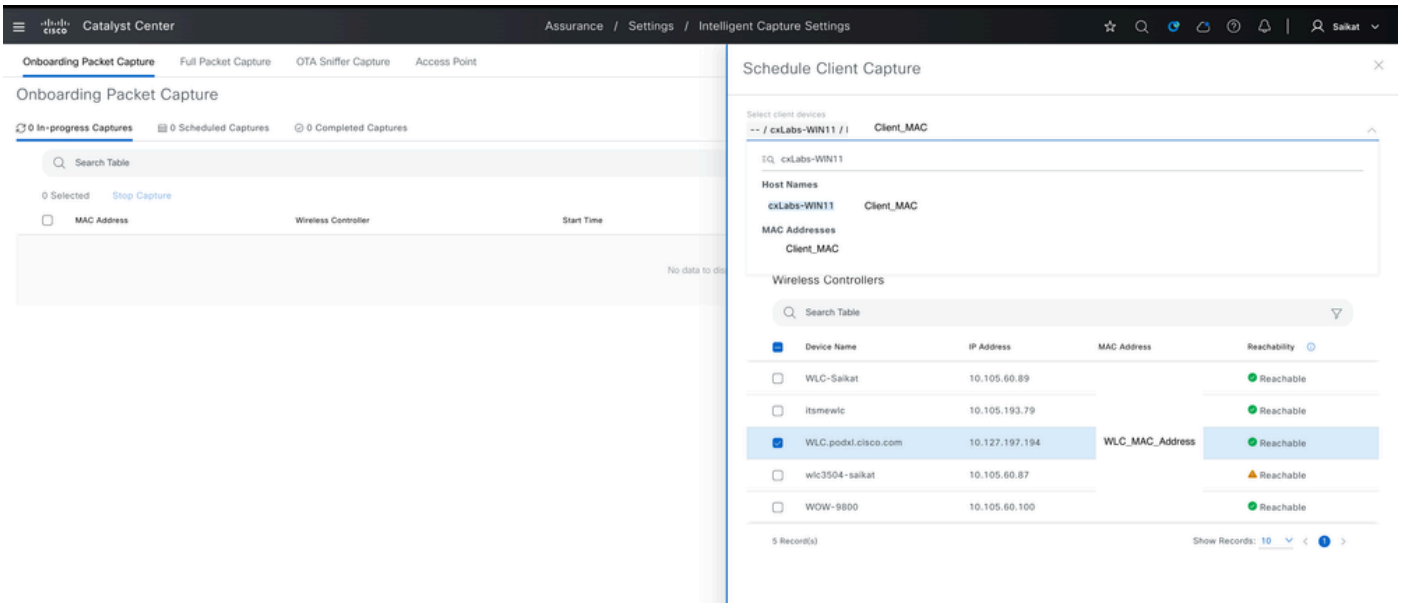
無線客戶端的智慧捕獲

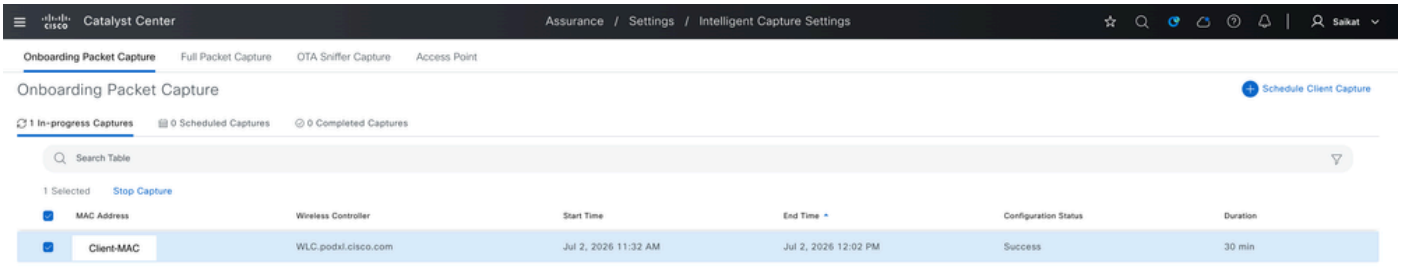
智慧捕獲(iCAP)通過直接從Catalyst Center捕獲實際的資料包級資料，幫助排除無線客戶端連線問題。它可以捕獲802.11管理、DHCP和EAP幀，以查明連線嘗試失敗的位置、特定客戶端的未加密資料和管理資料包，從而對自註冊、可訪問性和應用問題進行故障排除。您還可以根據要求安排智慧捕獲在以後運行。會話的預設持續時間是30分鐘，最大可以設定為八小時。

載入封包擷取

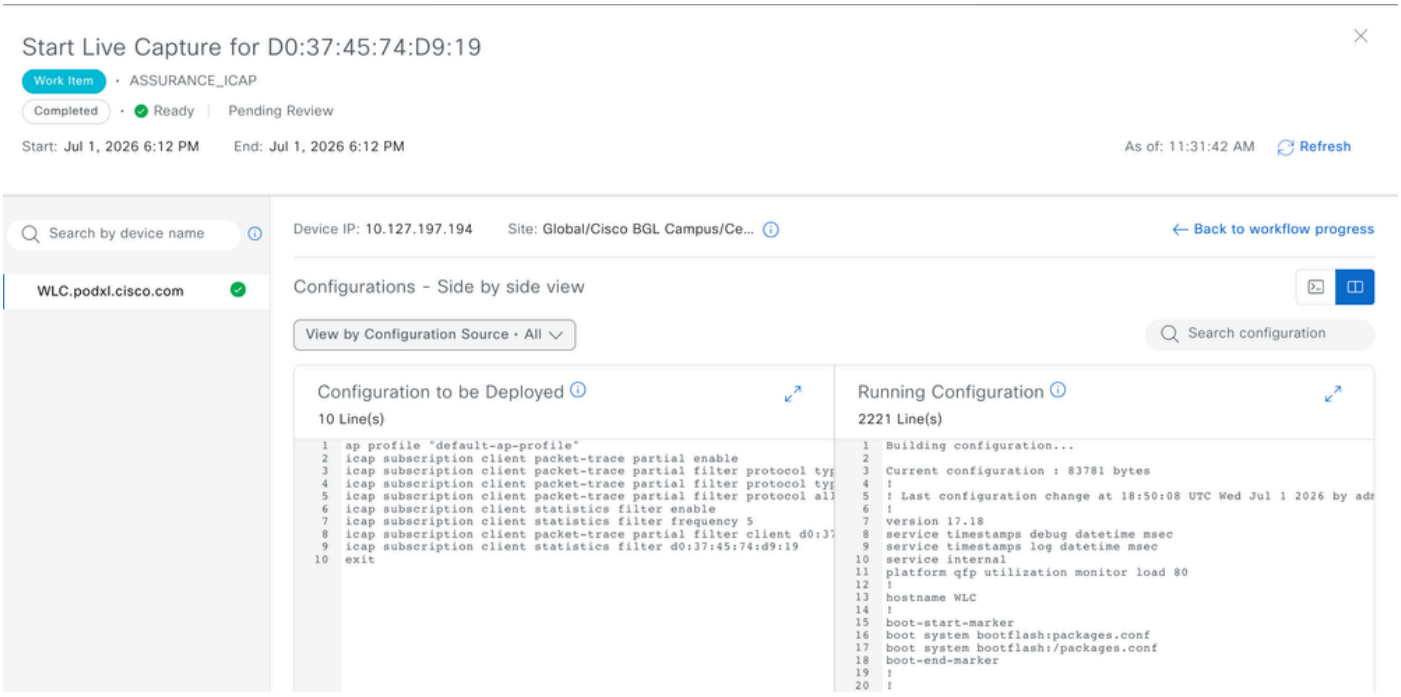
Onboarding Packet Capture記錄客戶端裝置在嘗試加入無線網路時交換的資料包序列，包括802.11管理幀（如關聯和身份驗證請求）、DHCP資料包和802.1X身份驗證期間使用的EAP資料包。此外，它還會收集客戶端射頻統計資料，以便檢視入網時刻的訊號狀況。這些捕獲對於客戶端無法連線時的場景故障排除很有用，有助於查明故障發生的確切階段（無論是在關聯、身份驗證或IP地址分配期間）。預設情況下，在最後一個客戶端連線的無線控制器上啟用自註冊資料包捕獲。最多可以選擇三個無線控制器以涵蓋客戶端漫遊場景。

要啟用Onboarding Packet capture，請導航到Assurance > Settings > Intelligent Capture Settings > Onboarding Capture > Schedule Client Capture（在右上角）> Search for Client Identifier(Mac address)





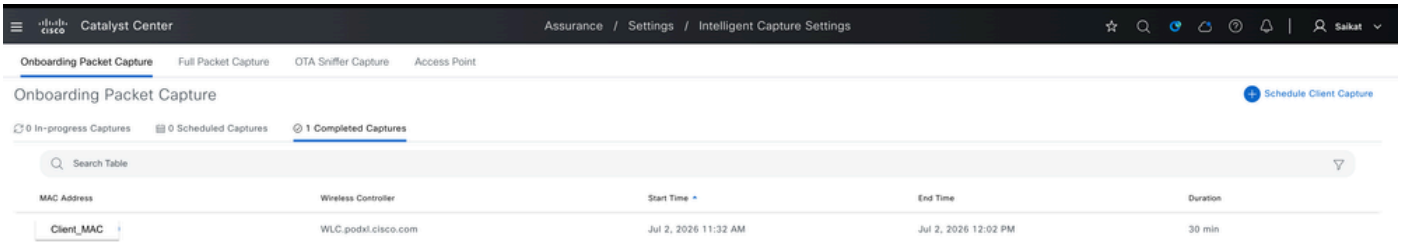
計畫的入職捕獲



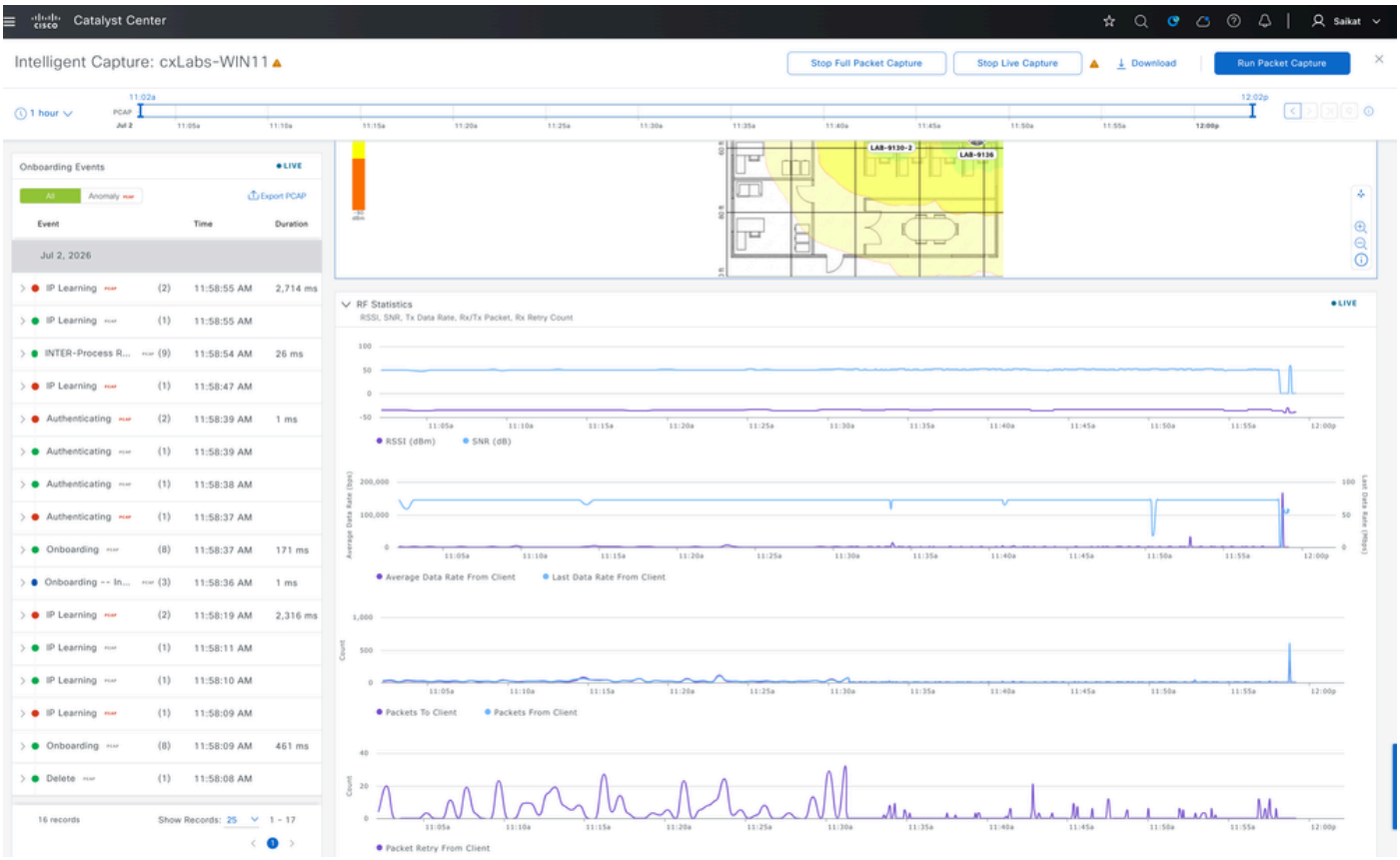
Onboarding Capture配置預覽

在計畫持續時間（從30分鐘到8小時不等）過後，可以手動停止或自動禁用入職捕獲。一旦停止

，捕獲將顯示在「完成的捕獲」下，您可以在其中按一下客戶端MAC地址檢視詳細的捕獲資料，然後以PCAP格式匯出檔案以供進一步分析。



已完成的入職捕獲

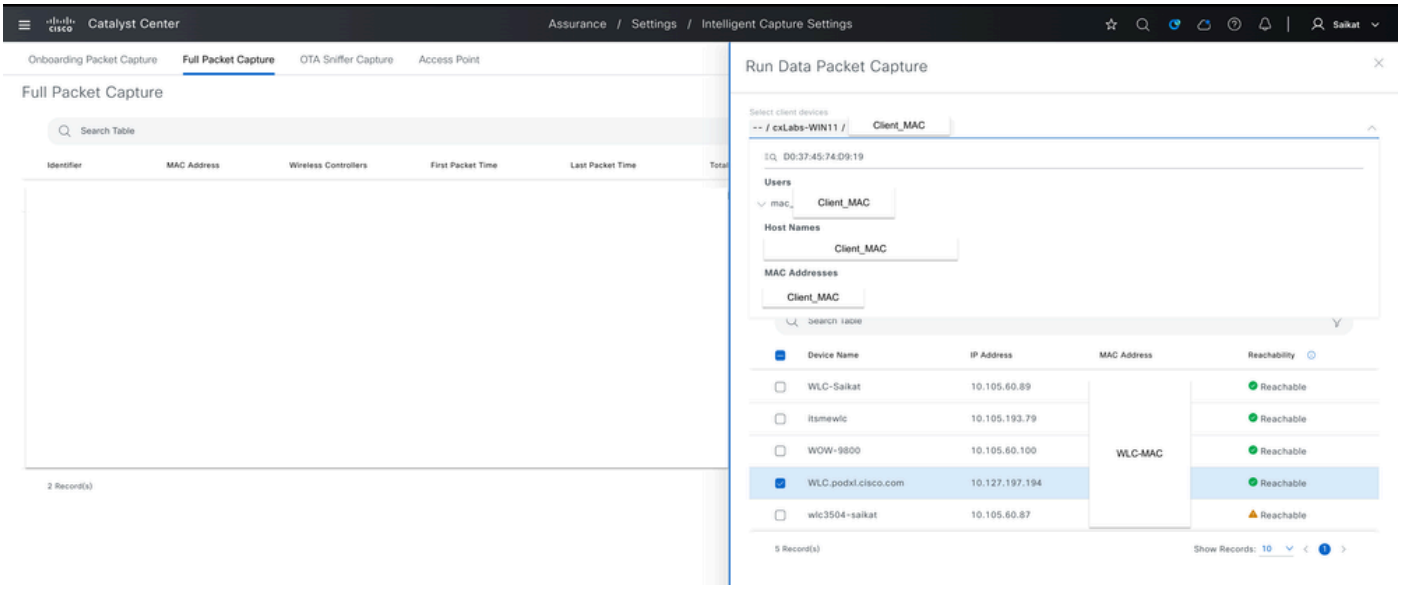


完整自註冊捕獲示例

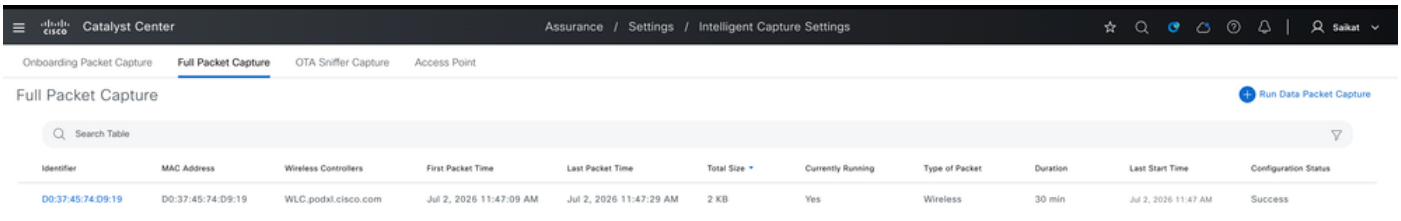
完整資料包捕獲

完整資料包捕獲會話可以捕獲特定客戶端的完整資料，提供對客戶端持續無線流量的深度資料包級可視性，這允許我們仔細檢查資料和管理資料包，以解決超出標準RF統計資訊所揭示範圍的訪問問題、應用效能問題或其他連線異常問題。它可以捕獲特定客戶端最多1 GB的滾動資料，並持續保留最新資料（最大限度）。

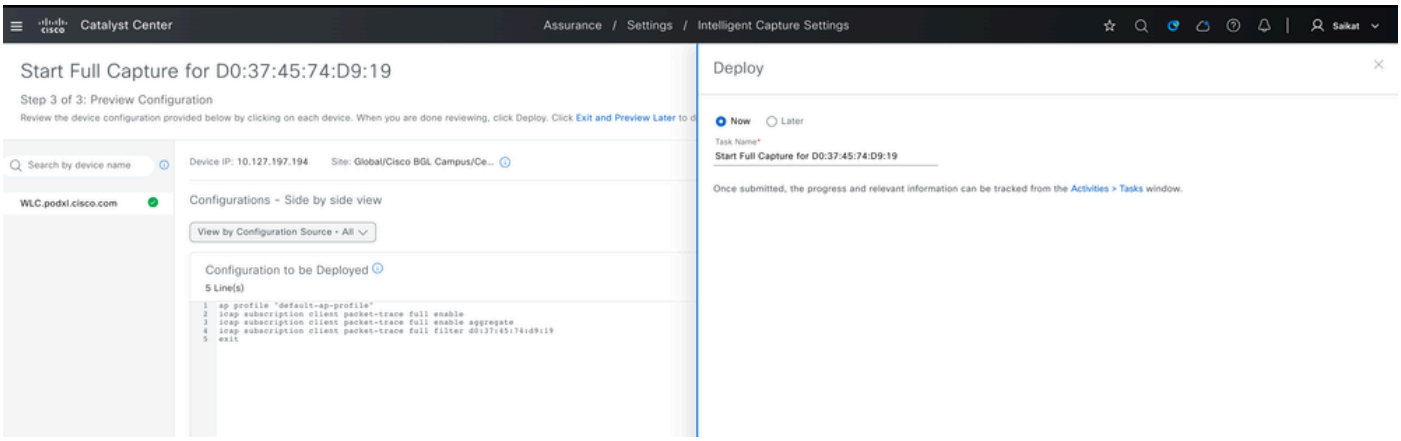
要啟用Full Packet Capturenavigate to Assurance > Settings > Intelligent Capture Settings > Onboarding Capture > Run Data Capture（在右上角）> Search for Client Identifier(Mac address):



使用者端的完整封包擷取



使用者端的排程式完整封包擷取



完整資料包捕獲的配置預覽

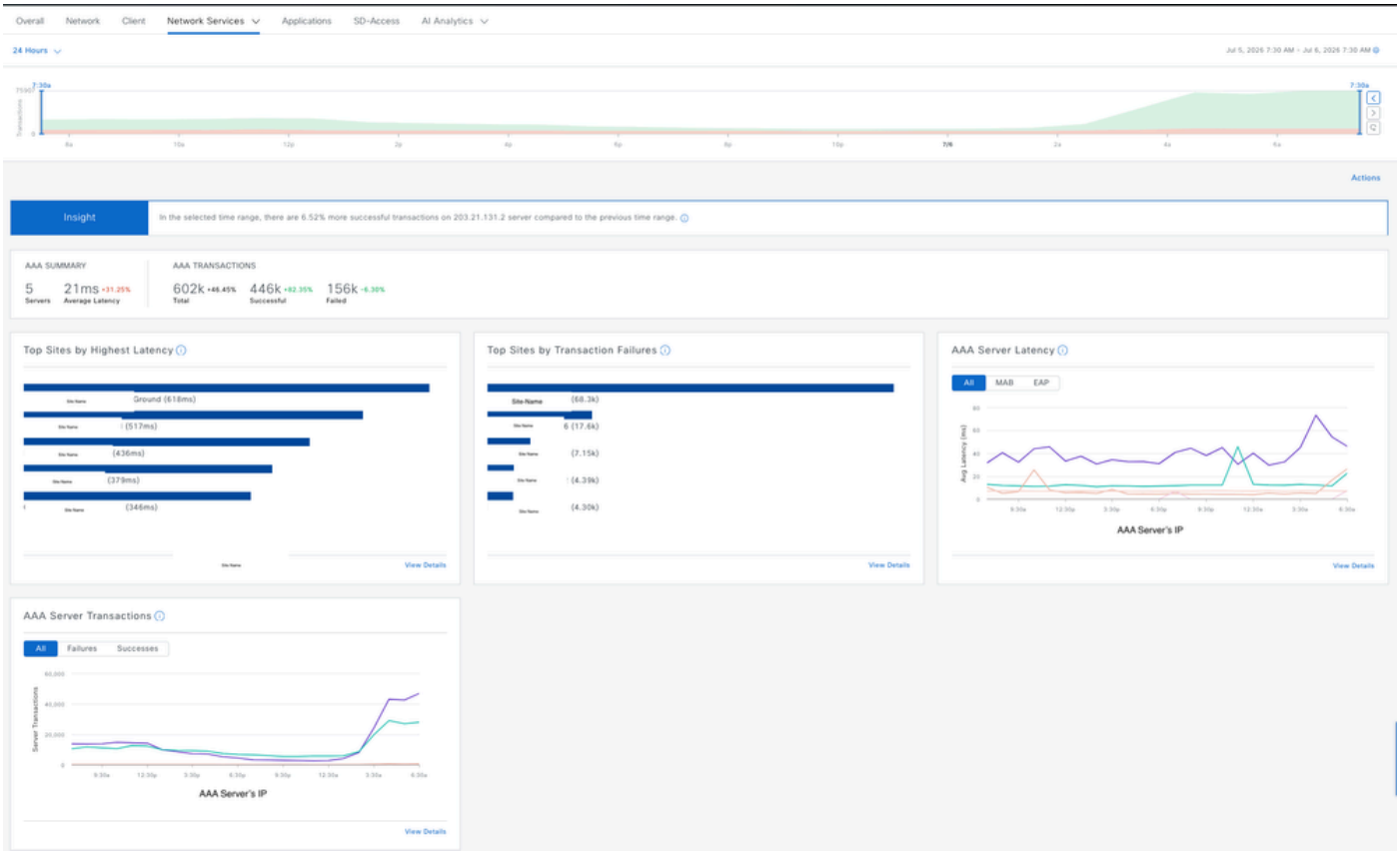
在計畫的持續時間（從30分鐘到8小時不等）過後，可以手動停止或自動禁用完整的資料包捕獲。一旦停止，捕獲將顯示在完成的捕獲下，您可以在其中按一下客戶端MAC地址檢視詳細的捕獲資料，然後以PCAP格式匯出檔案以供進一步分析。

為客戶端收集完全捕獲的示例

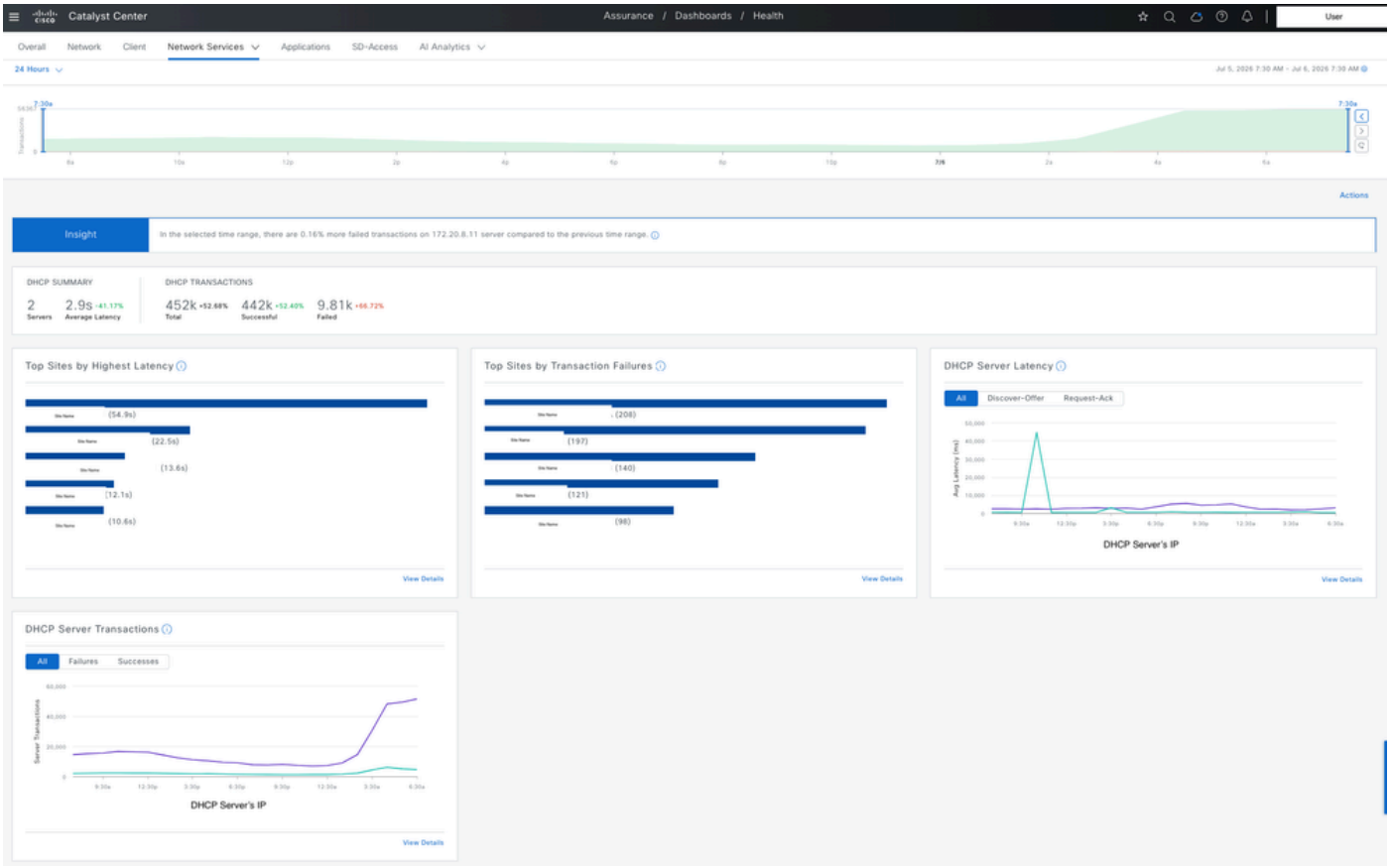
隔離網路服務問題(AAA、DHCP、DNS)

如果報告的症狀指向特定網路服務而不是控制器本身（例如，客戶端身份驗證失敗、未接收IP地址或名稱解析失敗），則「保證」下的Catalyst Center Network Services（Catalyst Center網路服務）控制面板可讓您檢視WLC報告的那些事務。

導航到Assurance > Dashboard > Health > Network services > AAA/DHCP/DNS:



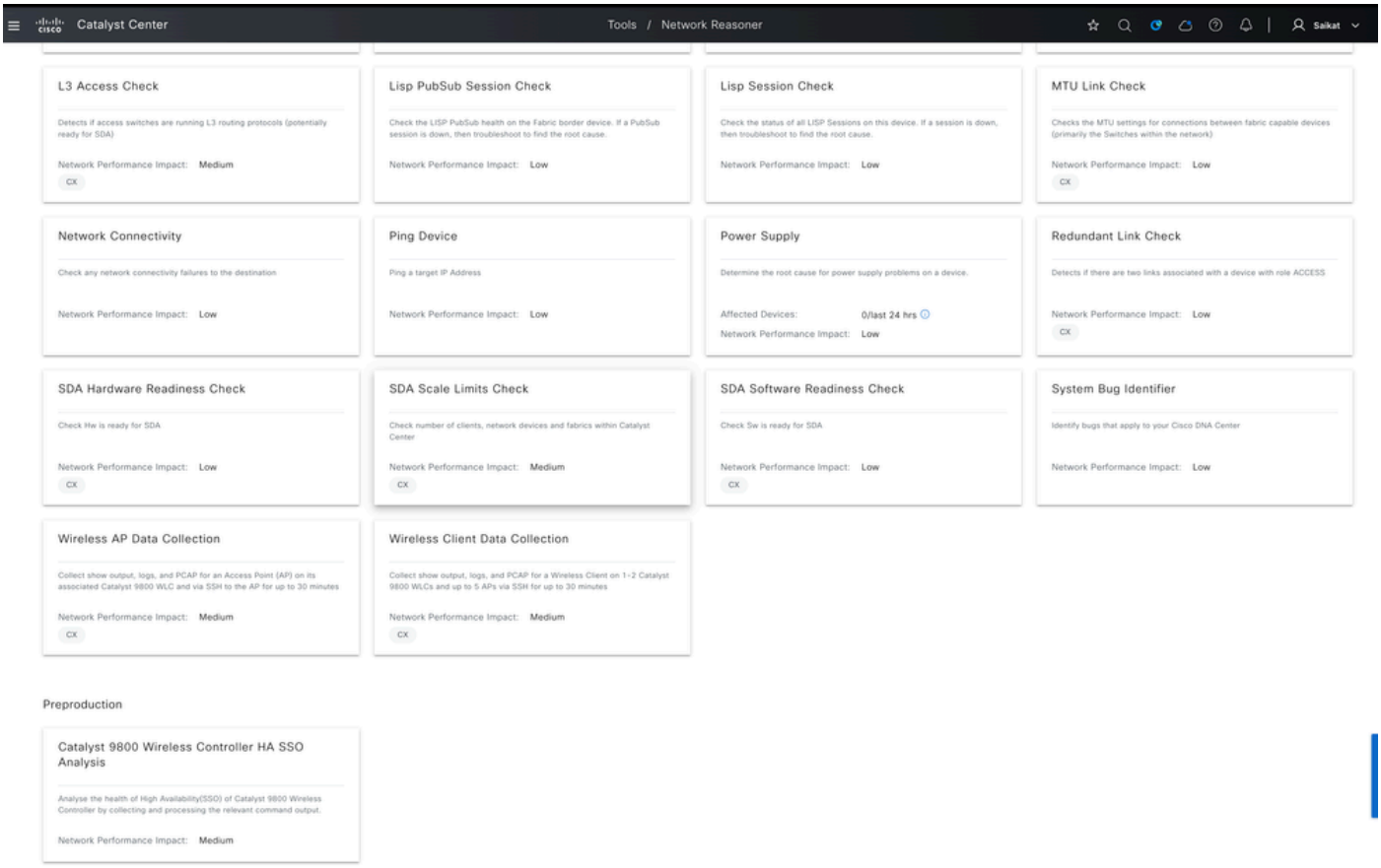
Catalyst Center上的無線客戶端AAA統計資訊



Catalyst Center上的無線客戶端DHCP統計資訊

網路說明員

Network Reasoner是Catalyst Center中的內建工具，可自動為您調查網路問題 — 您不必手動挖掘日誌。您可以在Tools > Network Reasoner下找到它。每個故障排除選項（稱為工作流）都會向您顯示簡短說明、過去24小時內受影響的裝置數量，以及運行該選項會發生的情況。它只能檢測新增到Catalyst Center for Assurance監控或通過Catalyst Center調配的裝置的問題。



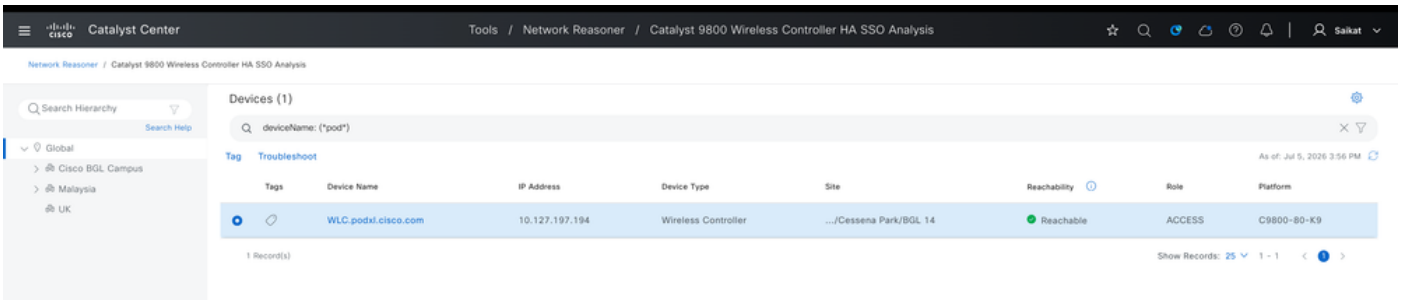
Network Reasoner上提供的各種網路故障排除選項

對於無線網路，有三種主要問題可以排除：

1.對於控制器問題(尤其是高可用性(HA)設定問題),Network Reasoner檢查以下內容：

- 控制器可達嗎？
- HA是否設定正確？
- 活動和備用控制器是否同步？
- 它們之間的聯絡是否有效？

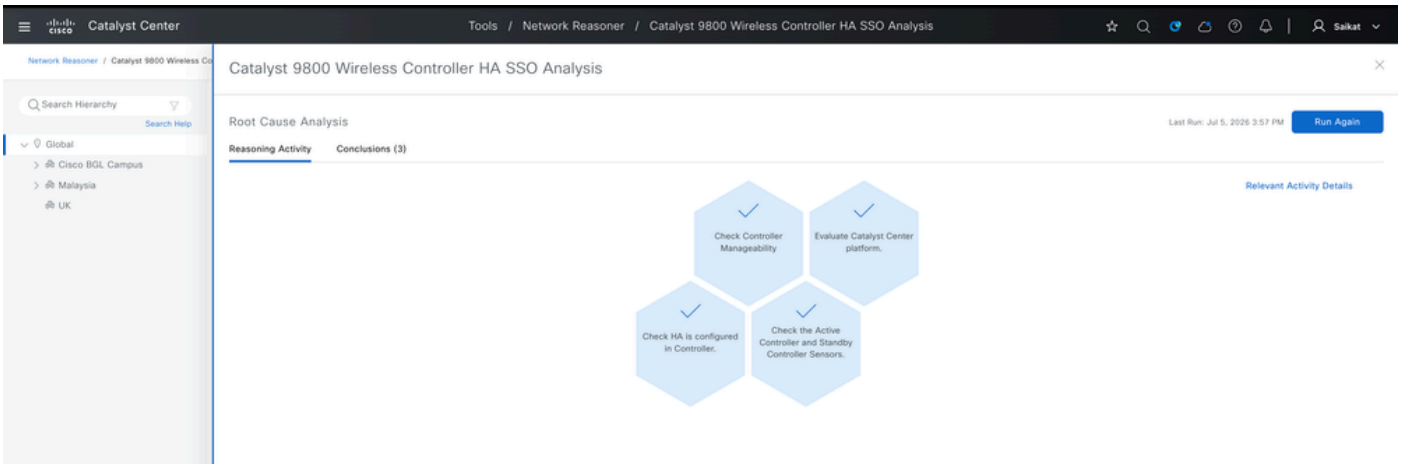
如果它發現問題，它會準確地告訴你問題所在，並建議如何解決。對於根本未傳送任何監控資料的裝置，還有單獨的故障排除選項。



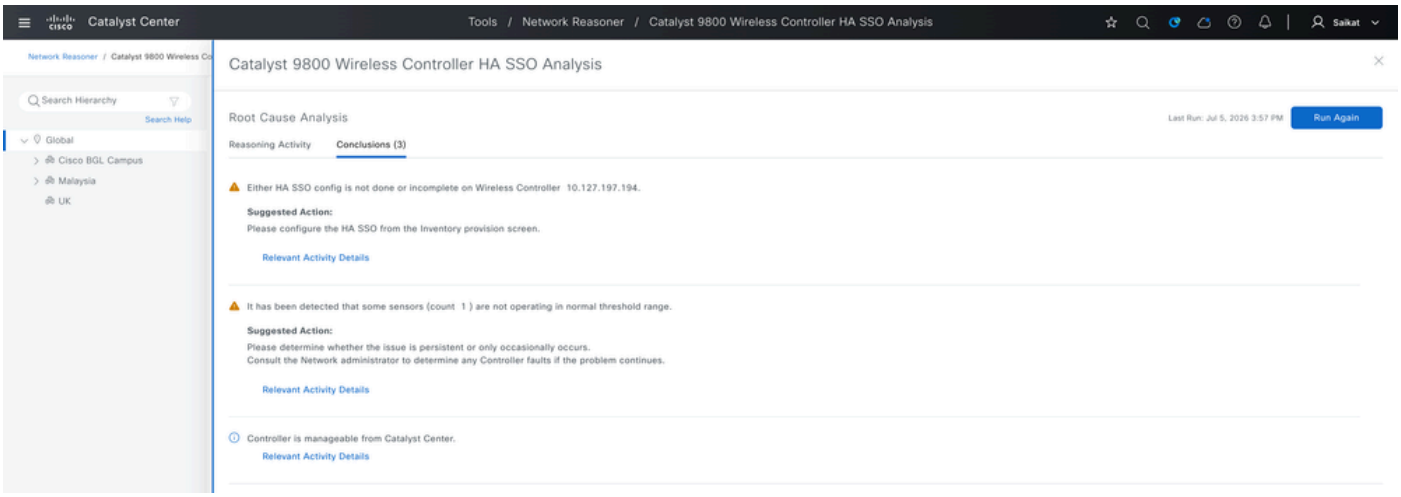
使用網路說明器對HA進行故障排除

在9800 WLC上使用網路論證器啟用HA SSO分析的疑難排解功能時，會執行多項檢查，並根據結果提供結論。如果發現HA SSO有任何問題，也建議採取糾正措施來解決這些問題。

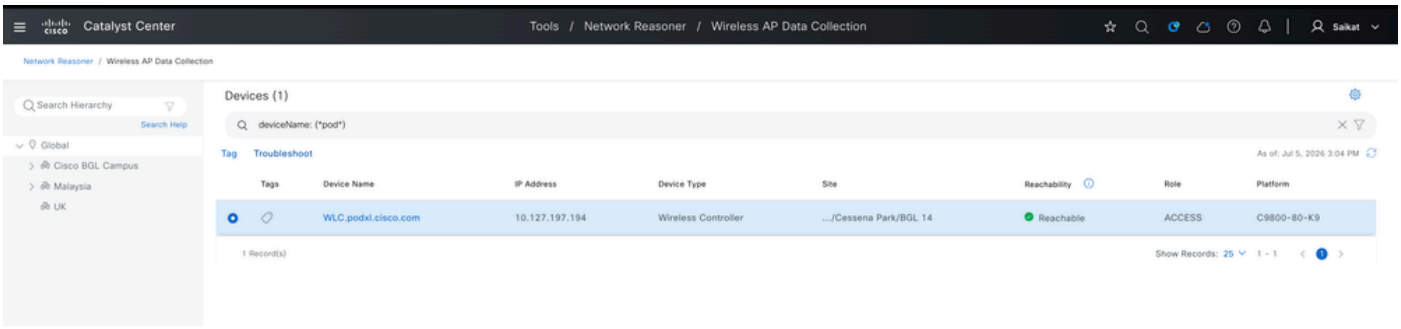
```
!! Task Workflow !!
Check Controller Manageability
Evaluate Catalyst Center platform.
Check HA is configured in Controller.
Check the Active Controller and Standby Controller Sensors.
```



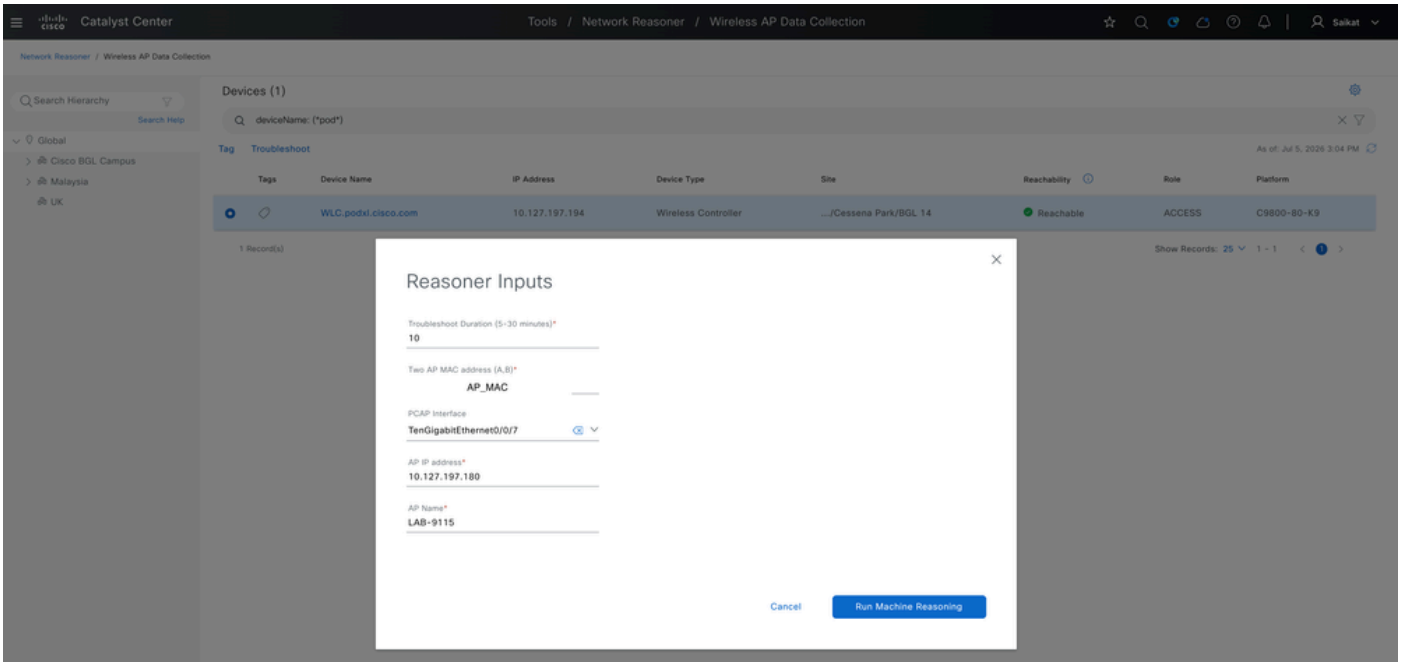
CATC為HA SSO分析執行的任務



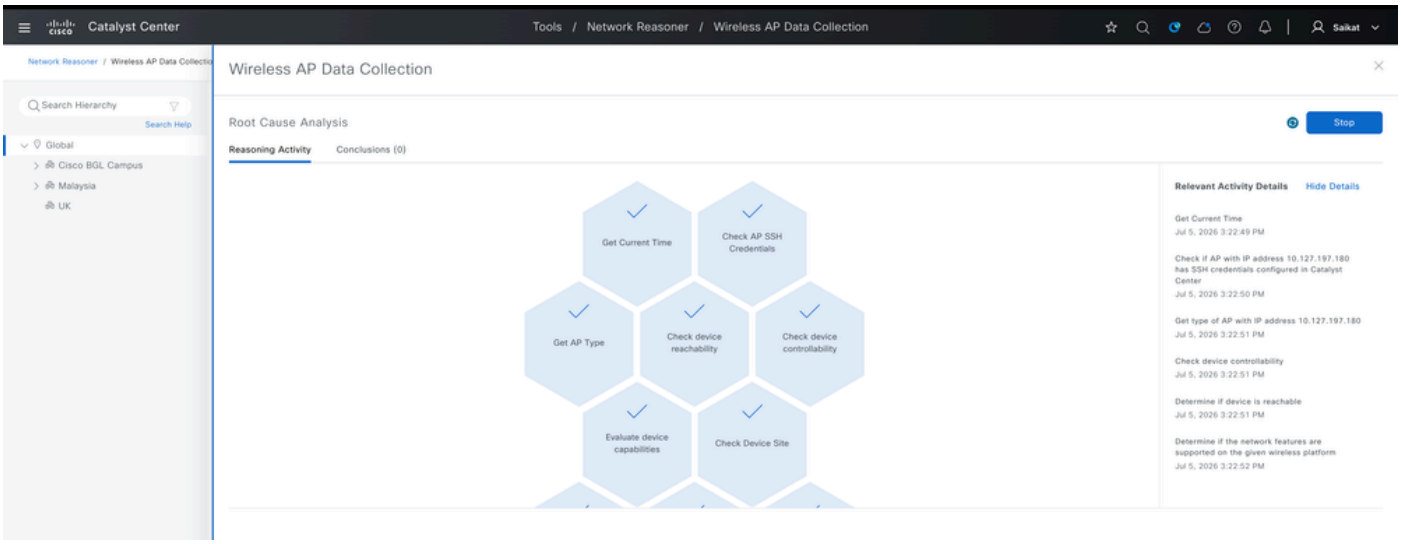
2.接入點 — 如果AP遇到問題，請選擇管理它的控制器，然後輸入AP的MAC地址，設定運行檢查的持續時間。它支援從WLC和AP捕獲日誌和資料包，以實現更深入的可視性。以下是為AP啟用Network Reasoner的工作流程以及相應的結果：



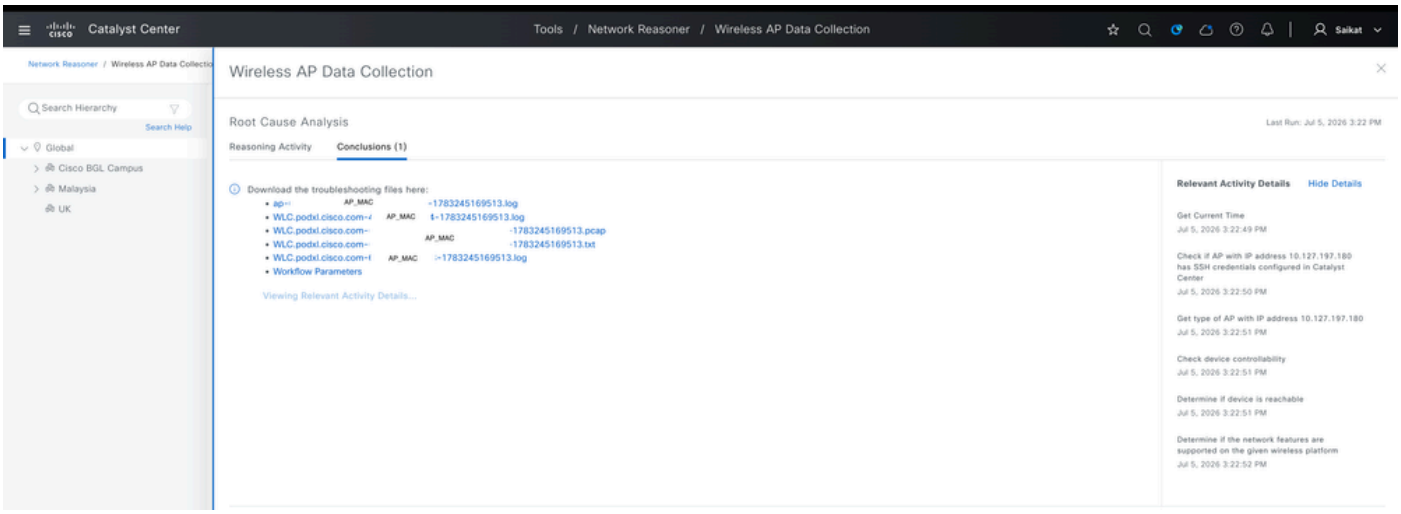
選擇要故障排除的託管AP AP WLC



提供AP詳細資訊以進行故障排除



正在運行以排除AP問題的任務



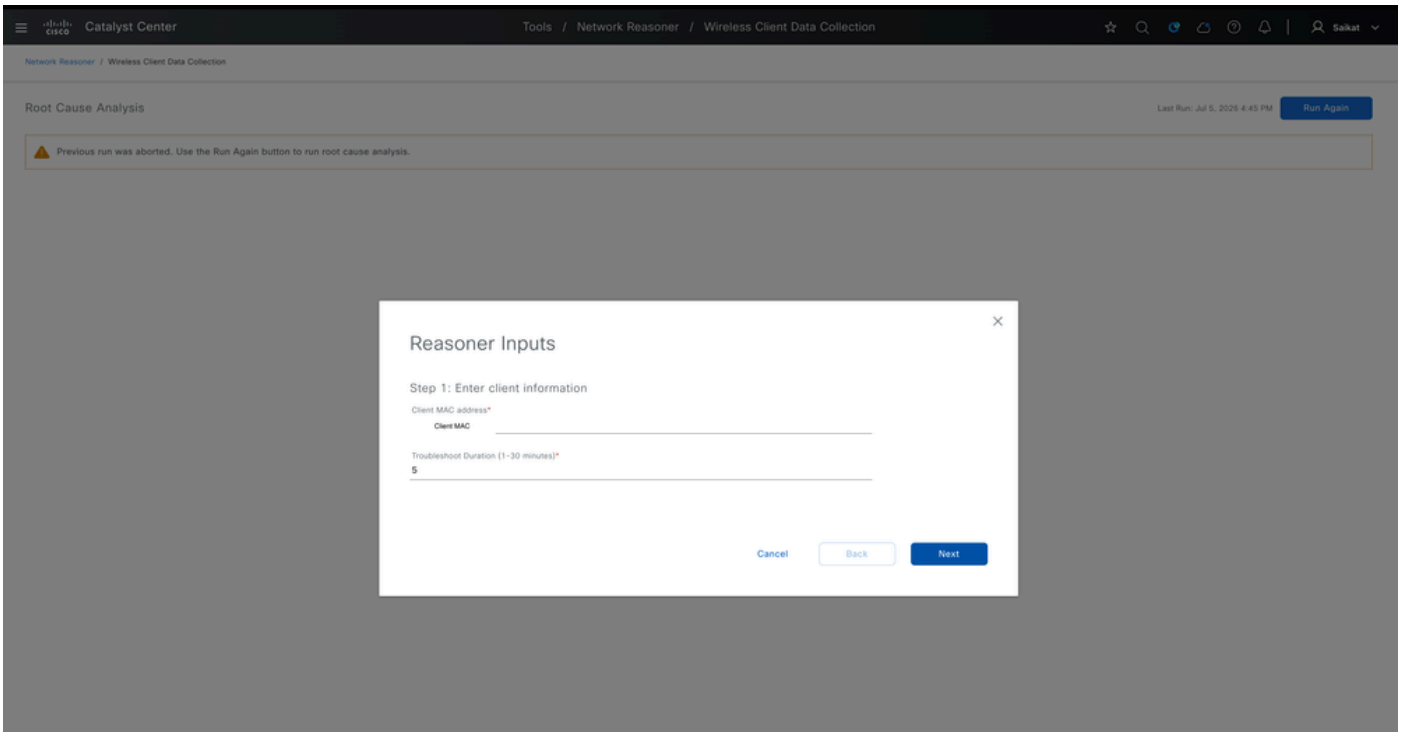
捕獲從WLC和AP收集的無線接入點問題

```
!! 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
```

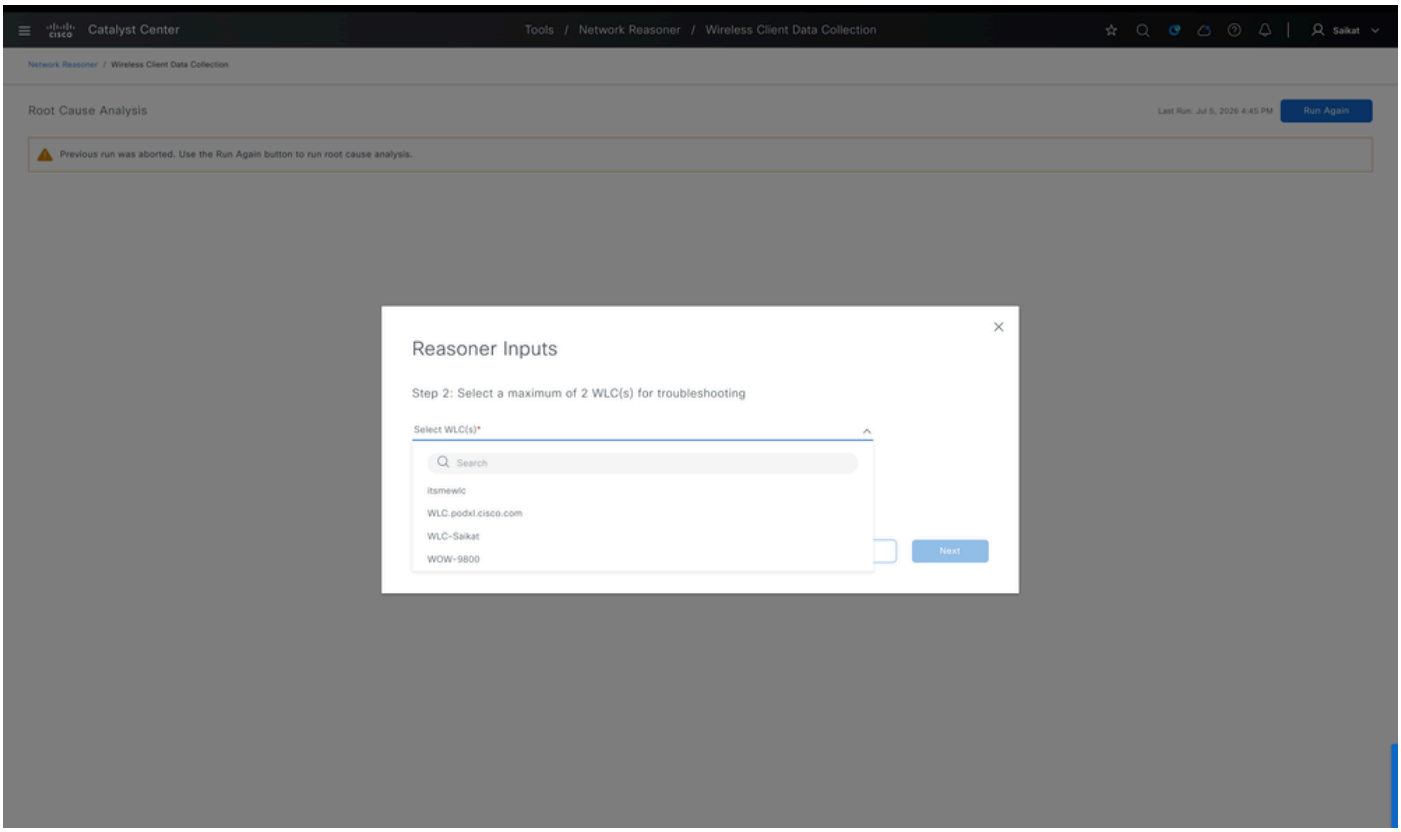
Jul 5, 2026 5:04:55 PM
Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127
Jul 5, 2026 5:04:57 PM
Start AP statistics collection on WLC with IP address 10.127.197.194 and wait for data collection for 3
Jul 5, 2026 5:04:58 PM
Start logging on COS AP with IP address 10.127.197.180 over SSH for feature set apDataCollection, saved
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 s
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
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.
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
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
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.
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 b
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://10.105.19
Jul 5, 2026 5:10:36 PM
Check if file bootflash:<file-name>has been uploaded successfully from WLC with IP address 10.127.197.1
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.
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
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
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
```

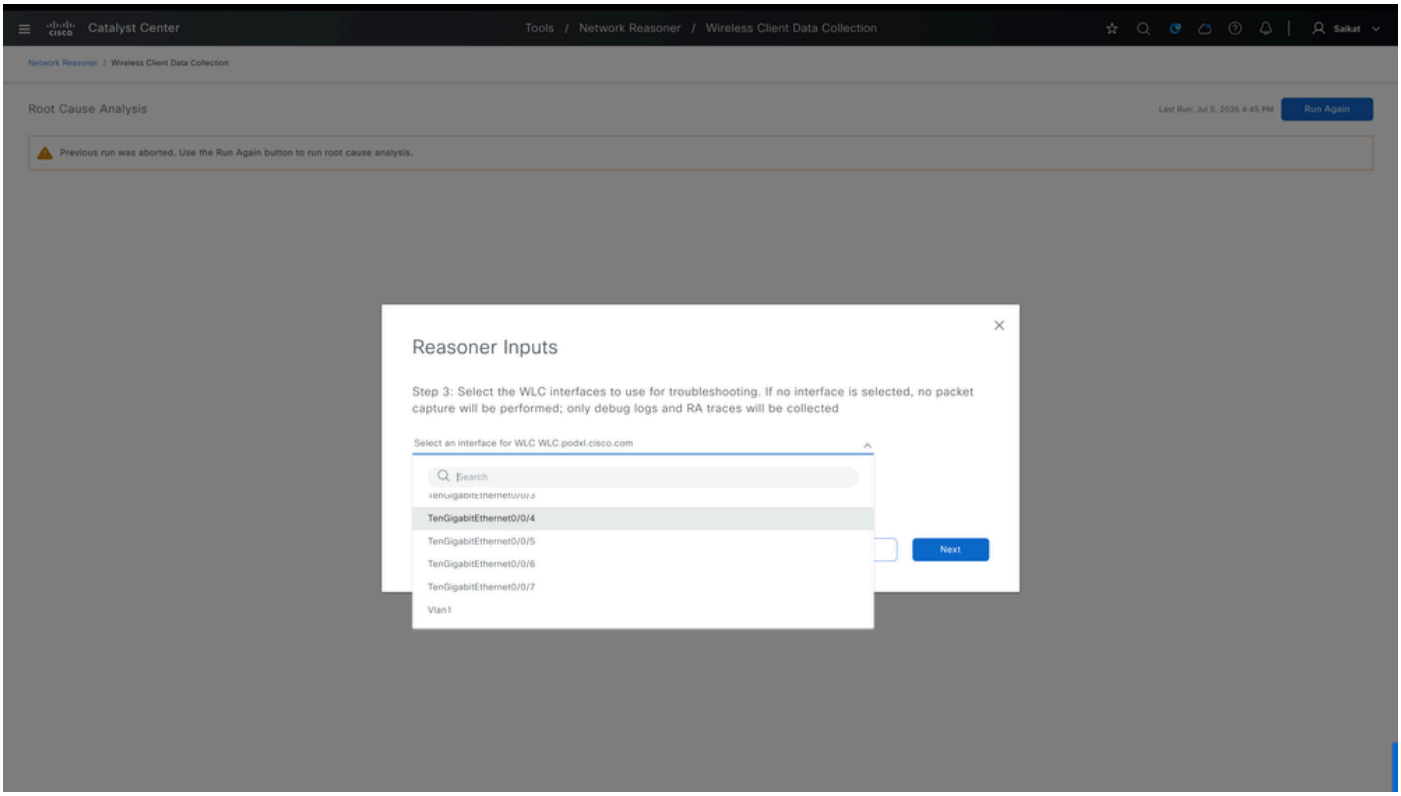
3.無線客戶端 — 如果使用者存在Wi-Fi問題，請選擇使用者所連線的無線控制器，輸入其裝置MAC地址，然後選擇您希望該工具監控的時間。它支援統計日誌、RA跟蹤和資料包捕獲，以檢視實際交換的資料。以下是為無線客戶端啟用Network Reasoner的工作流程以及相應的結果：



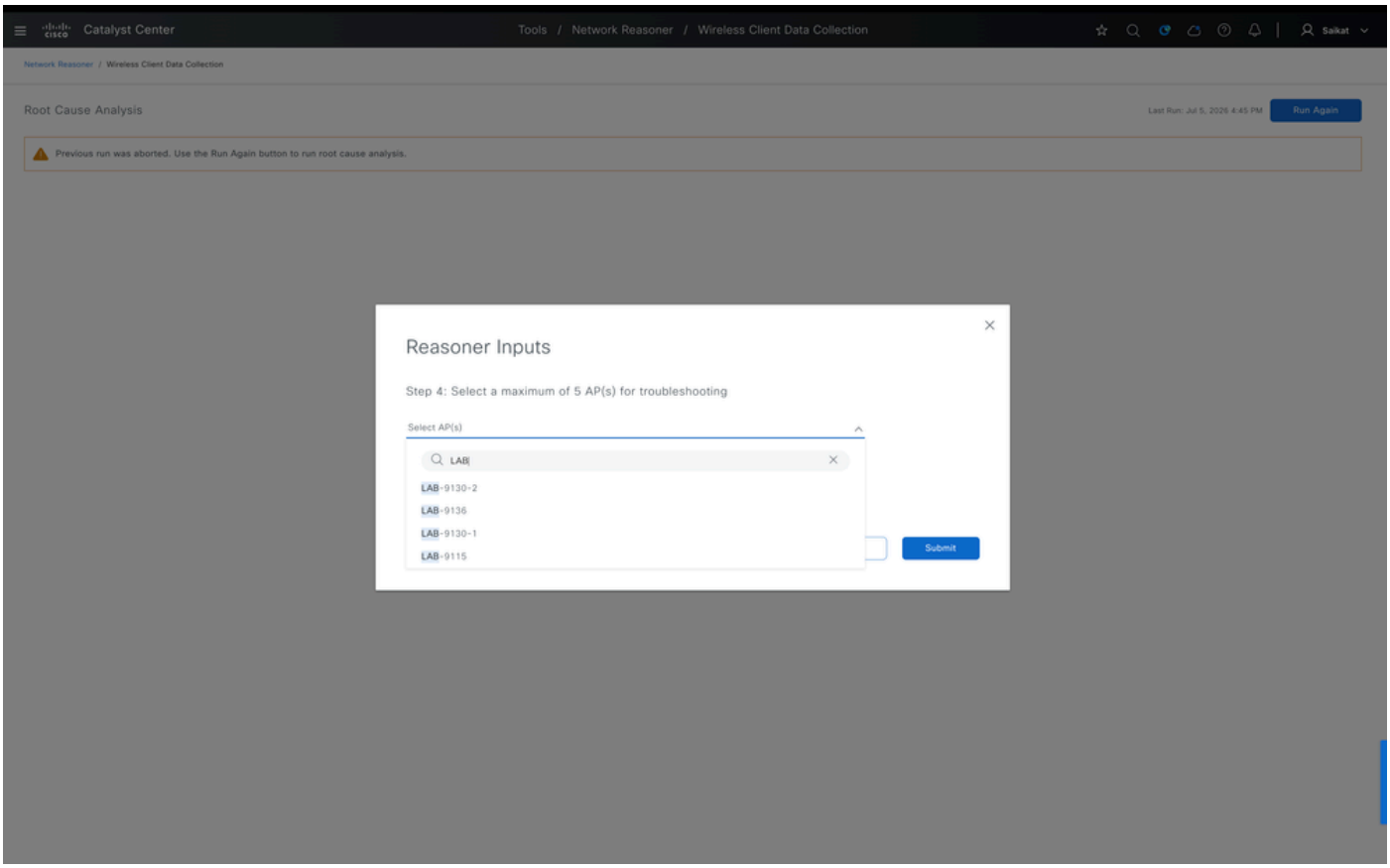
提供客戶端詳細資訊以進行故障排除



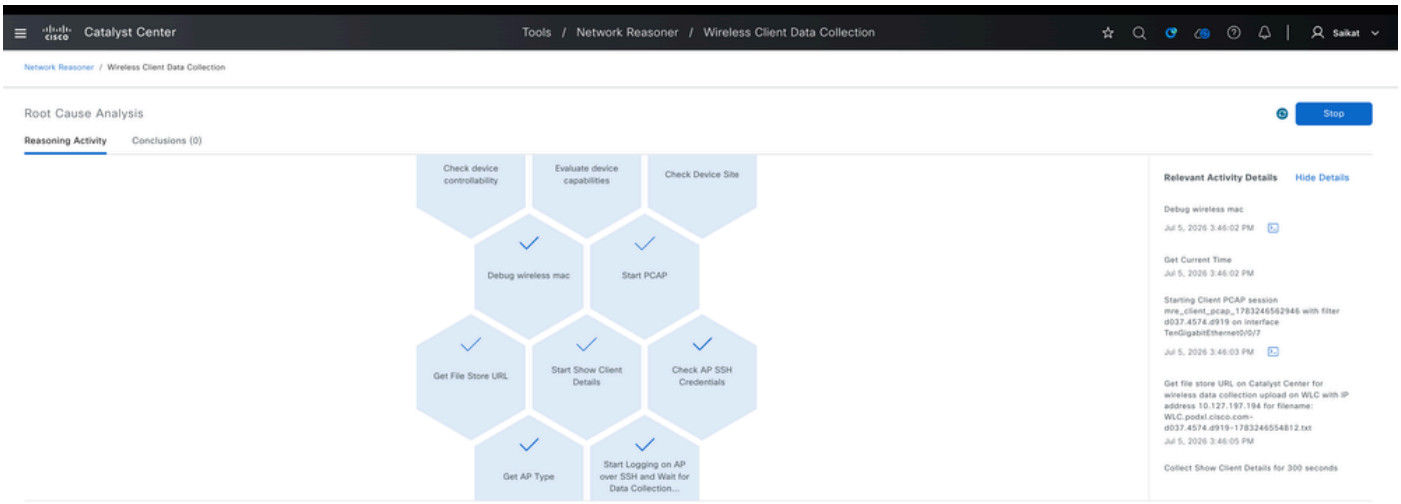
選擇WLC對無線客戶端MAC進行故障排除



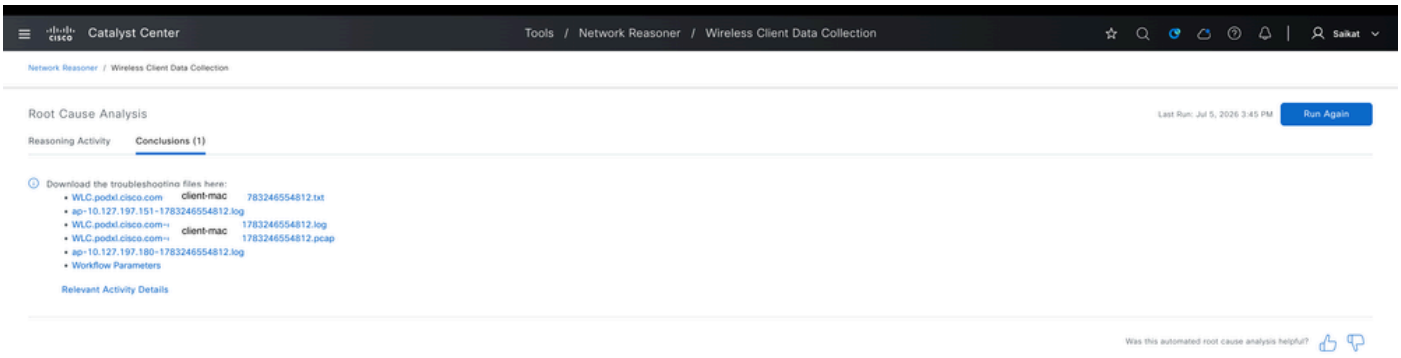
選擇WLC上的介面以排解無線使用者端疑難問題



選擇AP（最多4個）對無線客戶端進行故障排除



正在運行以排除無線客戶端問題的任務



從WLC和AP收集的捕獲無線客戶端問題

```
!! 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> featu
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> featu
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
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
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

2026年7月5日下午5:59:16

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

2026年7月5日下午5:59:16

Check File Size:bootflash:<file-name>

2026年7月5日下午5:59:16

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

2026年7月5日下午5:59:18

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

2026年7月5日下午5:59:23

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

2026年7月5日下午5:59:23
從IP地址為10.127.197.194的WLC中刪除bootflash:<file-name>
2026年7月5日下午5:59:23

技術參考

- 思科智慧捕獲部署指南
- 管理智慧捕獲
- Cisco Catalyst保證使用手冊，版本2.3.7.x
- 使用Network Reasoner排除網路裝置故障 — 使用MRE工作流程對無線LAN控制器上的HA進行故障排除

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。