使用Catalyst Center解决无线问题

目录

简介

本文档介绍使用Cisco Catalyst Center对Catalyst 9800无线局域网控制器(WLC)、AP和客户端连接问题进行故障排除。

先决条件

- 无线LAN控制器必须添加到Catalyst Center并在资产中显示Managed状态。
- WLC上的遥测状态必须显示为Up。

要求

思科建议您了解以下主题：

- 无线局域网控制器的命令行界面(CLI)或图形用户界面(GUI)访问
- 命令行界面(CLI)或图形用户界面(GUI)访问Catalyst Center

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

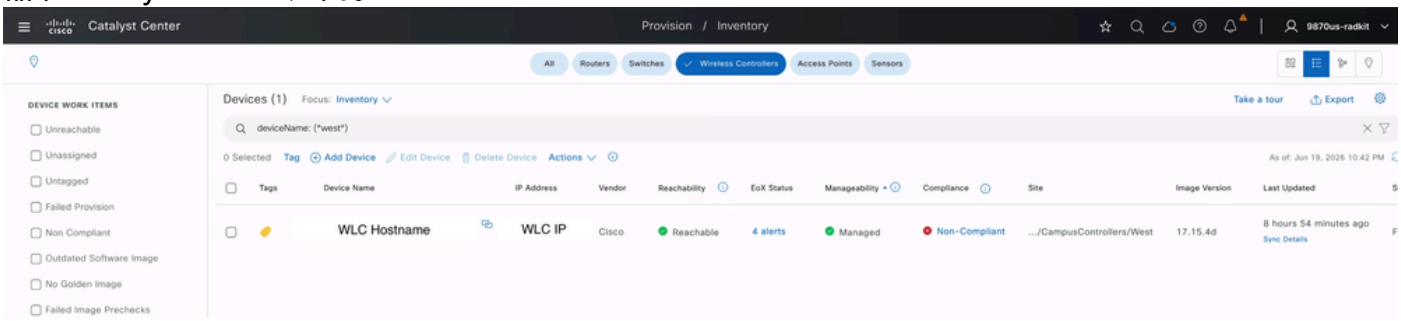
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

从Catalyst Center收集数据

将Catalyst 9800系列WLC添加到Catalyst Center for Assurance后，该平台将通过多种收集方法提取数据：SNMP轮询、流遥测、NetFlow、系统日志、基于CLI的收集、API和IP SLA。每种机制都有不同的用途：一些报告基本设备运行状况（CPU、内存、KPI），而另一些报告提供精细的详细信息（PoE状态、客户端会话、无线性能）。

1. 设备/资产运行状况(SNMP + CLI):可达性、CPU、内存、接口统计信息和软件版本 — 通过标准SNMP轮询和CLI收集。
2. 系统日志:发送到Catalyst Center（充当已配置的系统日志服务器）的系统和操作日志消息。
3. 无线遥测（NETCONF/YANG流）：核心保障源。它以接近实时的方式流传输AP和客户端级别的数据 — 客户端登录和漫游事件、RSSI/SNR、AP无线电/RF统计信息和WLC内部运行状况计数器。

要接收此数据，无线LAN控制器必须处于Catalyst Center上的管理状态，遥测状态显示在9800控制器和Catalyst Center之间。



<#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

默认情况下，Cisco Catalyst Center配置有运行状况、问题和事件设置，包括无线控制器、接入点、无线客户端和应用的特定阈值和优先级。Catalyst Center根据它从这些受管设备接收的数据和配置的事件设置来生成事件和警报。此外，可以创建自定义配置文件来根据特定网络要求定制这些设置，从而根据网络环境的独特需求进行更精确的监控和警报。

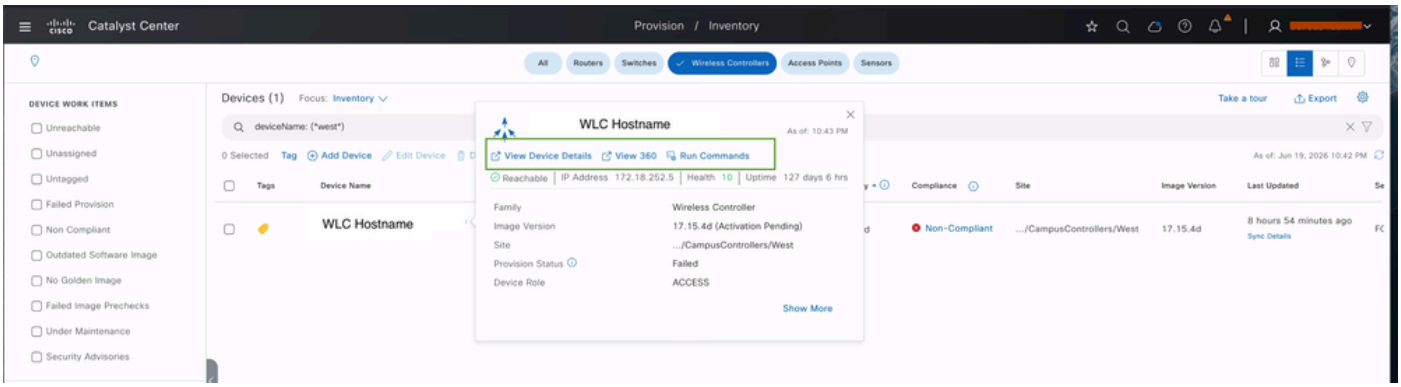
Catalyst 9800系列无线控制器问题

当无线LAN控制器(WLC)遇到诸如可达性丢失、性能缓慢、访问错误、中断或特定服务降级等问题时，Cisco Catalyst Center提供内置可视性，使您能够在问题发生时重新构建控制器上发生的情况，而无需直接登录设备。

查看设备360的控制器运行状况

设备360视图将控制器可达性、遥测状态、历史问题、生成的事件和性能统计信息整合到单个时间轴驱动的控制面板中，使其成为调查报告的WLC问题时首先查看的位置。

导航到Provision > Inventory > Wireless Controller > [search for the controller] > 单击 device name > Device 360

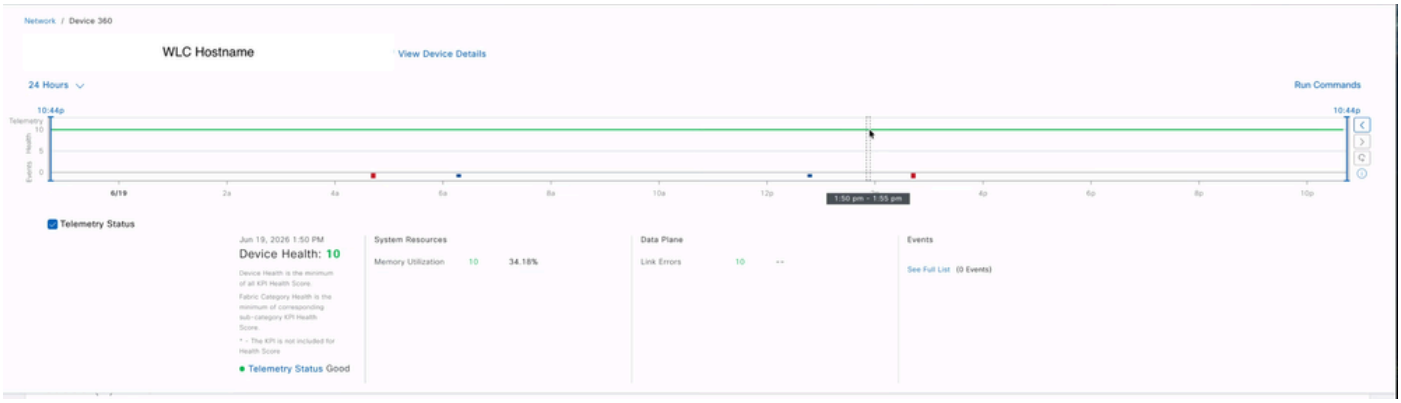


无线LAN控制器的View 360

注意：也可以从Assurance > Health > Network访问同一视图，然后单击Network Devices表中的设备名称。

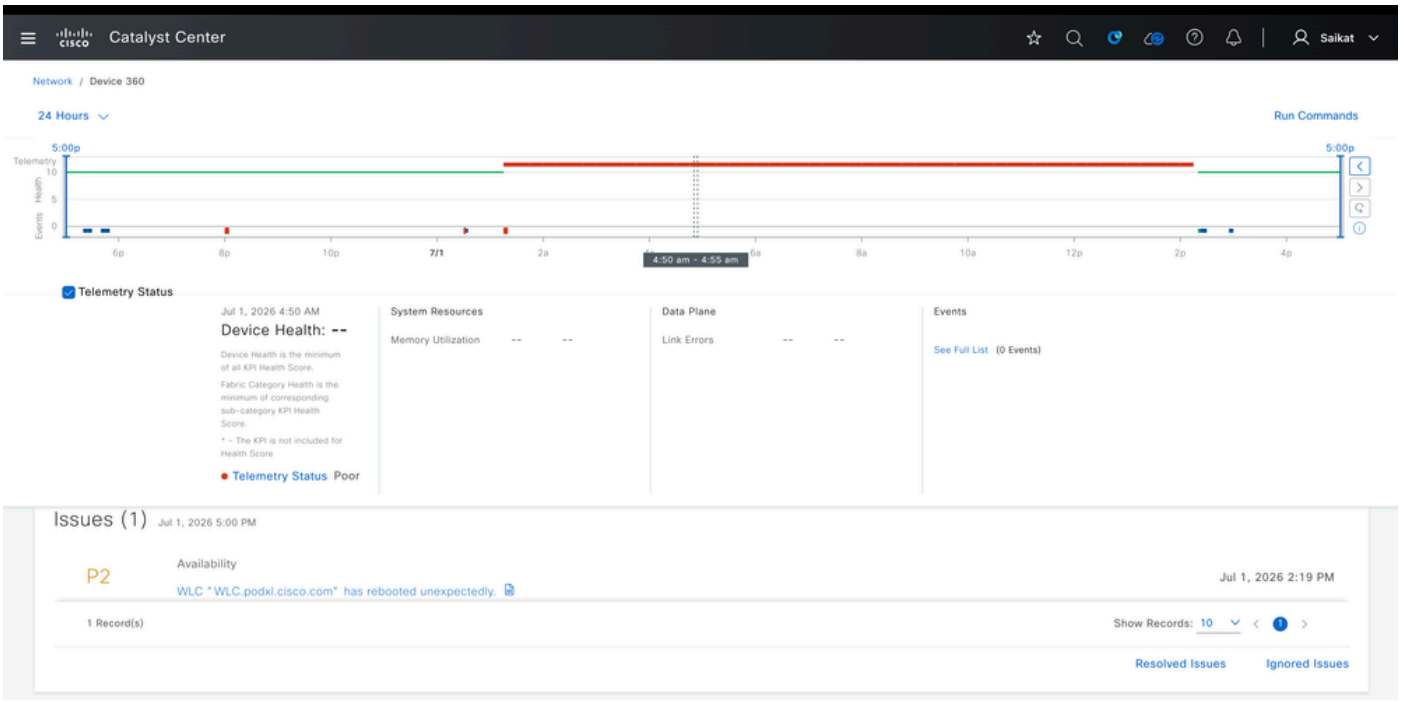
通过设备360，您可以将健康时间线滑块移回支持的历史窗口内的任意点（Catalyst Center Assurance数据最多保留30天），以查看发生事故时控制器状态的准确状态。对于该选定窗口，视图曲面：

设备可达性 — 控制器是否可访问和管理。
遥测状态 — SNMP/Syslog/NETCONF遥测馈送保证的运行状况。



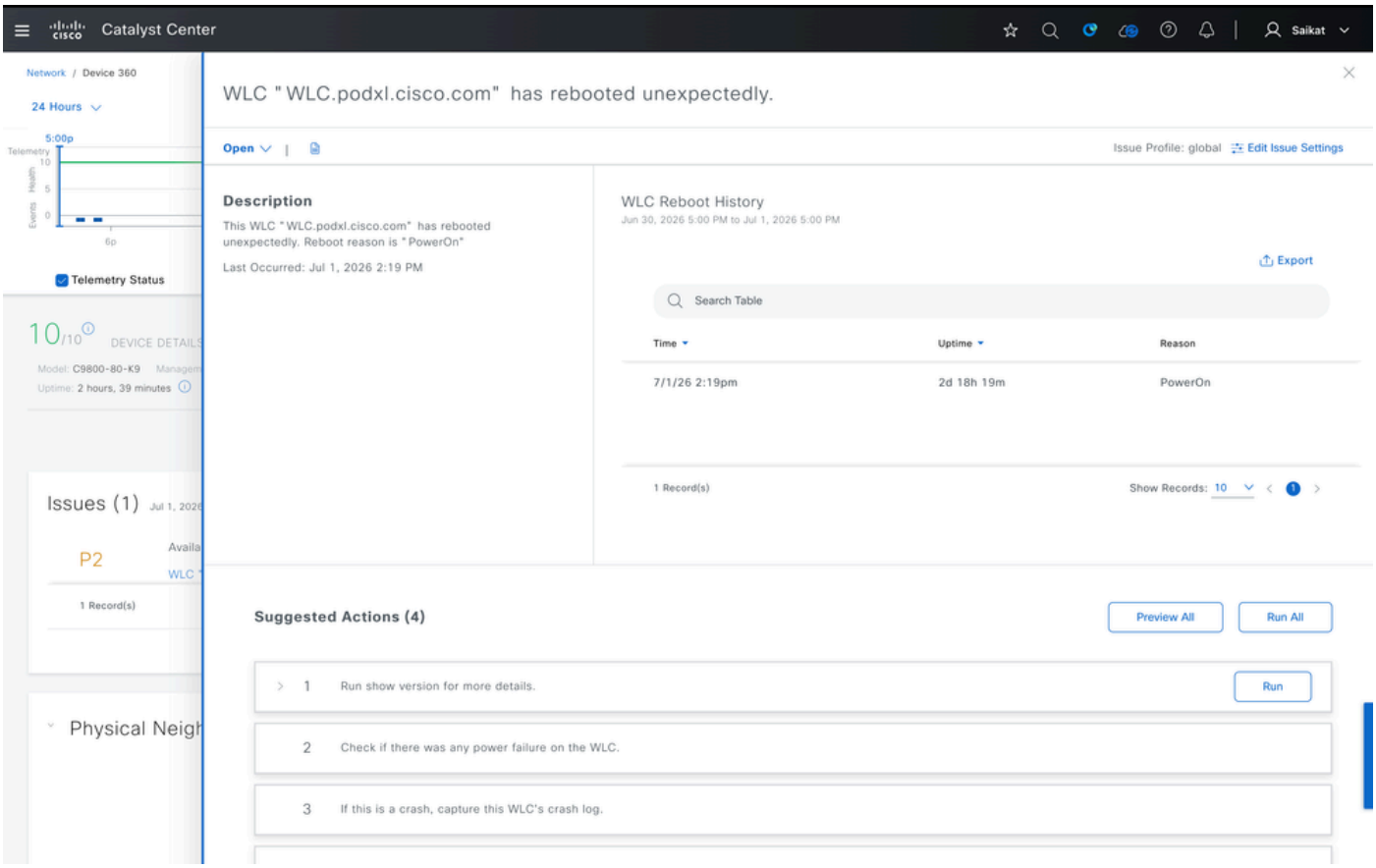
无线LAN控制器的遥测状态

观察到的问题 — 保证在该期间检测到设备上的问题。

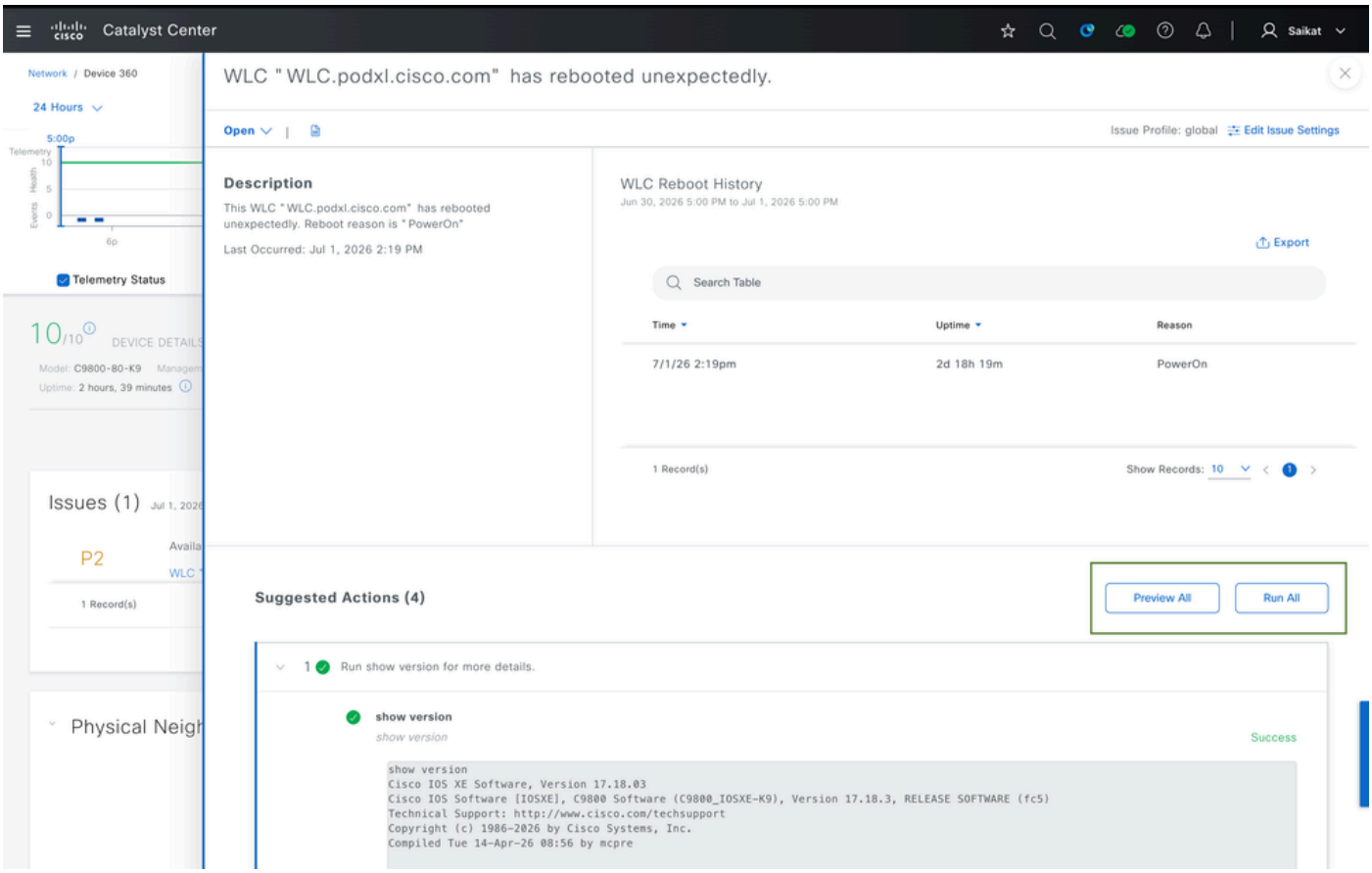


无线LAN控制器报告的问题

单击特定问题，您可以查看有关它的详细信息，以及解决问题或进一步调查的建议操作。

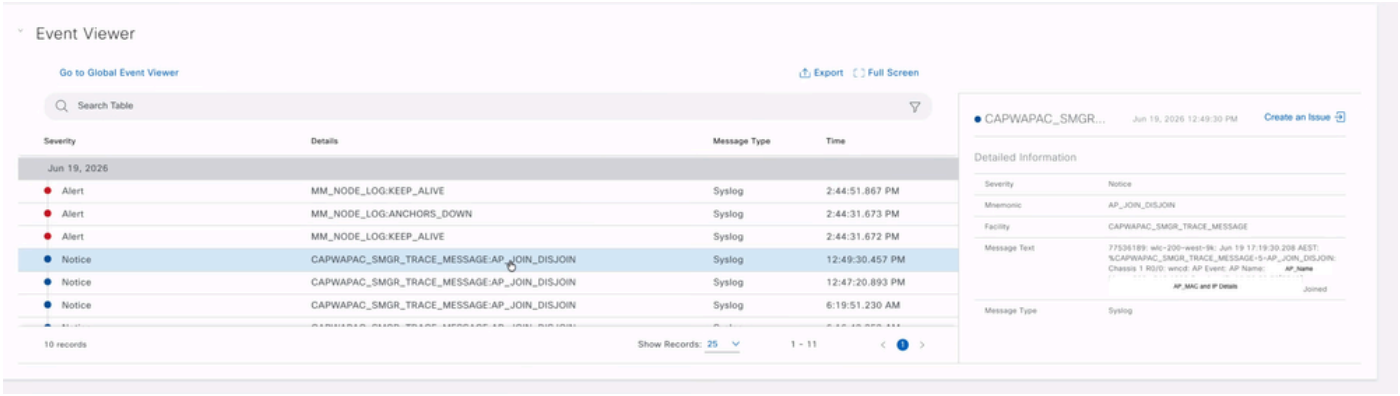


针对WLC上报告的问题建议的操作

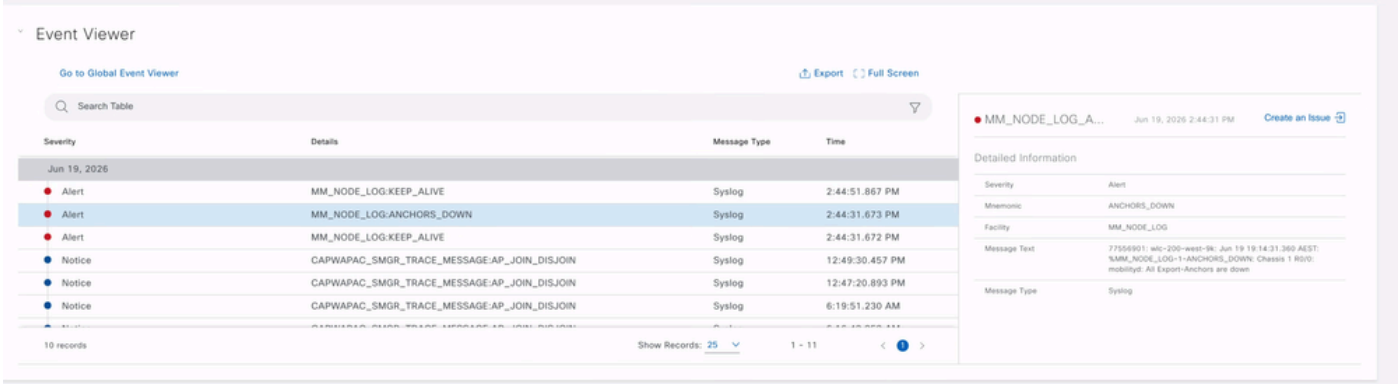


针对WLC上报告的问题建议的操作

生成的事件 — 基于从控制器接收的系统日志消息和SNMP陷阱：



无线LAN控制器的事件查看器 — 示例1

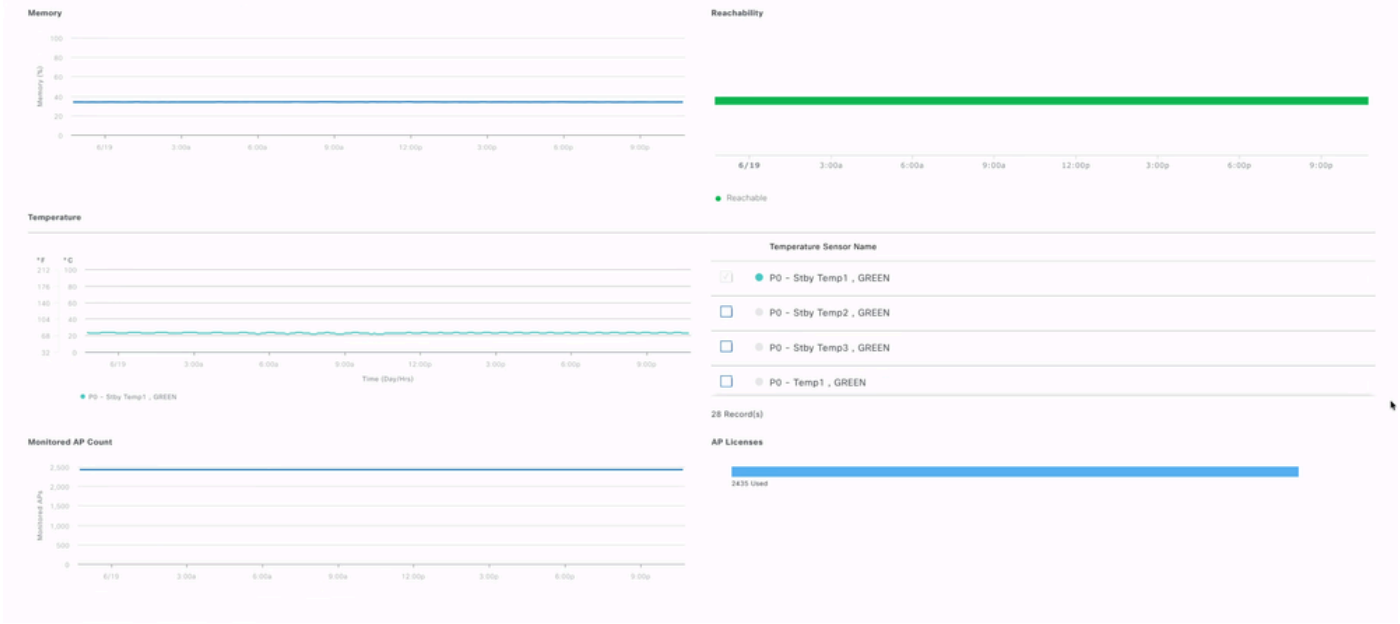


无线LAN控制器的事件查看器 — 示例2

性能统计信息 — CPU和内存利用率、温度、正常运行时间、高可用性状态和上次重新加载原因。

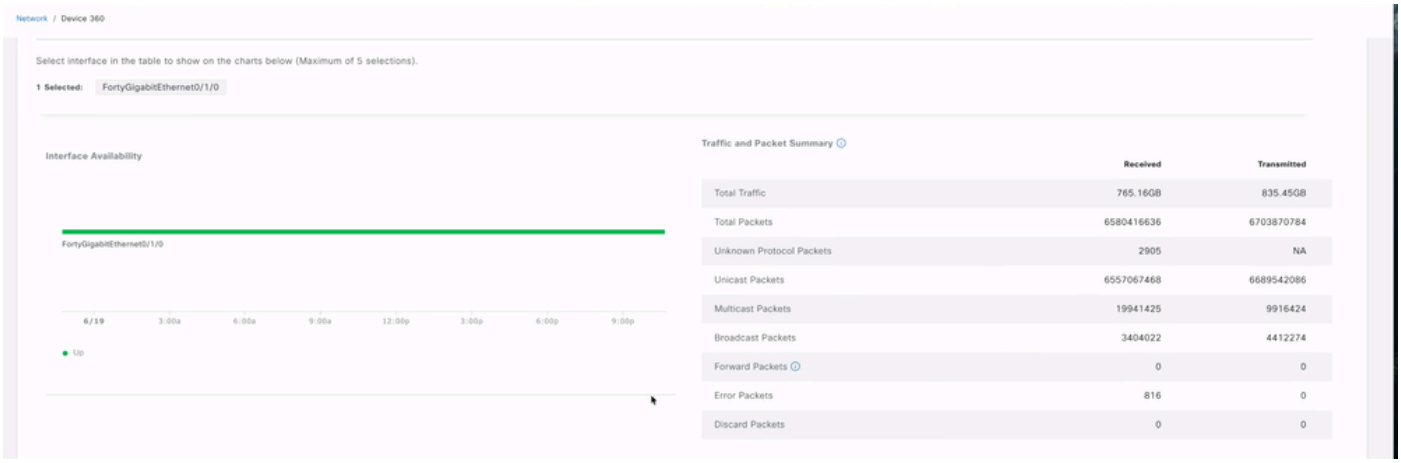
连接的客户端 — 包括按本地、外部、锚点和空闲客户端计数细分的客户端。
AP状态 — 与控制器关联的接入点的加入/运行状态。

Catalyst Center上的WLC统计信息



Catalyst Center上的WLC统计信息

接口统计信息 — 每个接口的状态、RX/TX数据包计数、利用率、丢弃和错误。



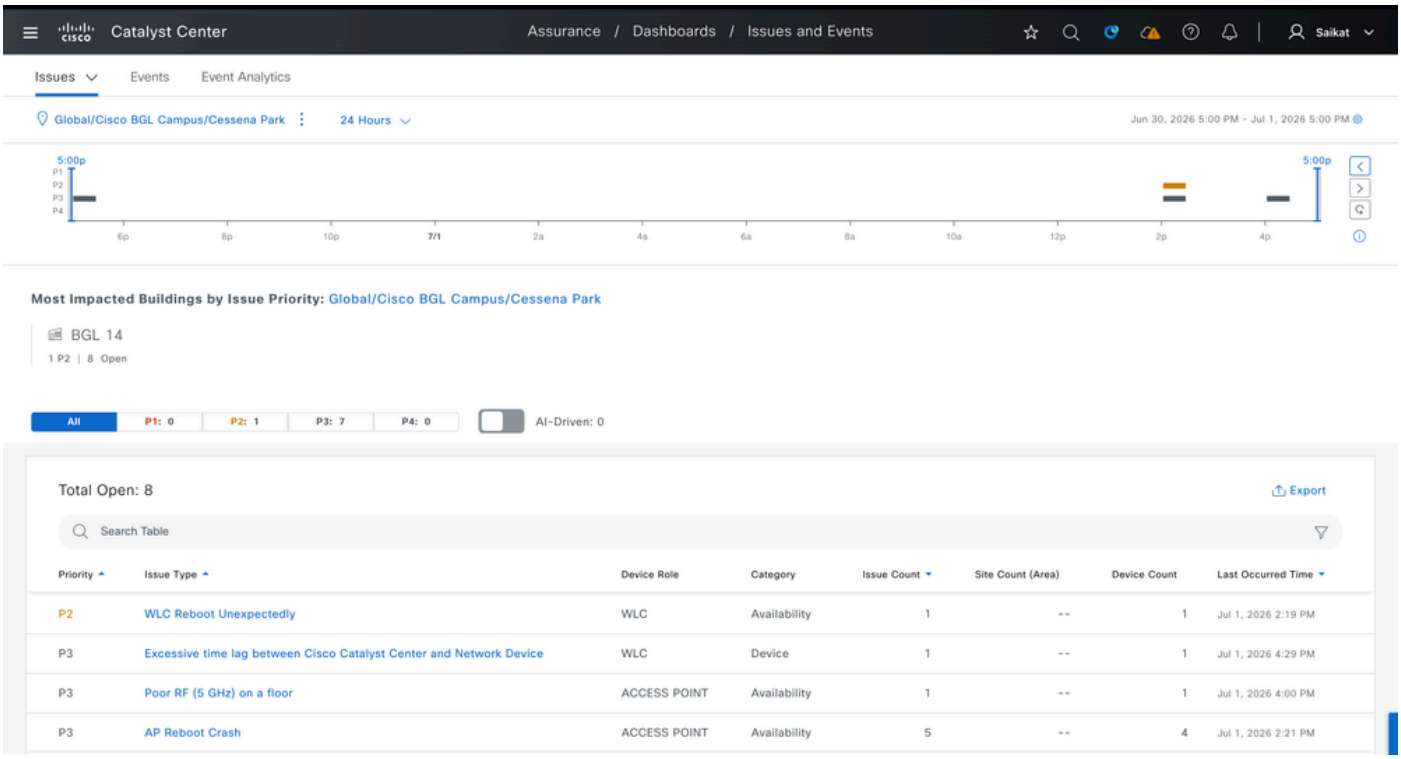
Catalyst Center上的WLC统计信息

Catalyst Center上的WLC统计信息

由于所有这一切都是相互关联的，因此您可以在发布期间关联多个相关因素并获得清晰的了解。使用这些统计数据，您无法确切了解问题的根本原因，但我们可以排除所有可能的原因，帮助我们进一步排除故障并设置需要实时收集的日志类型。

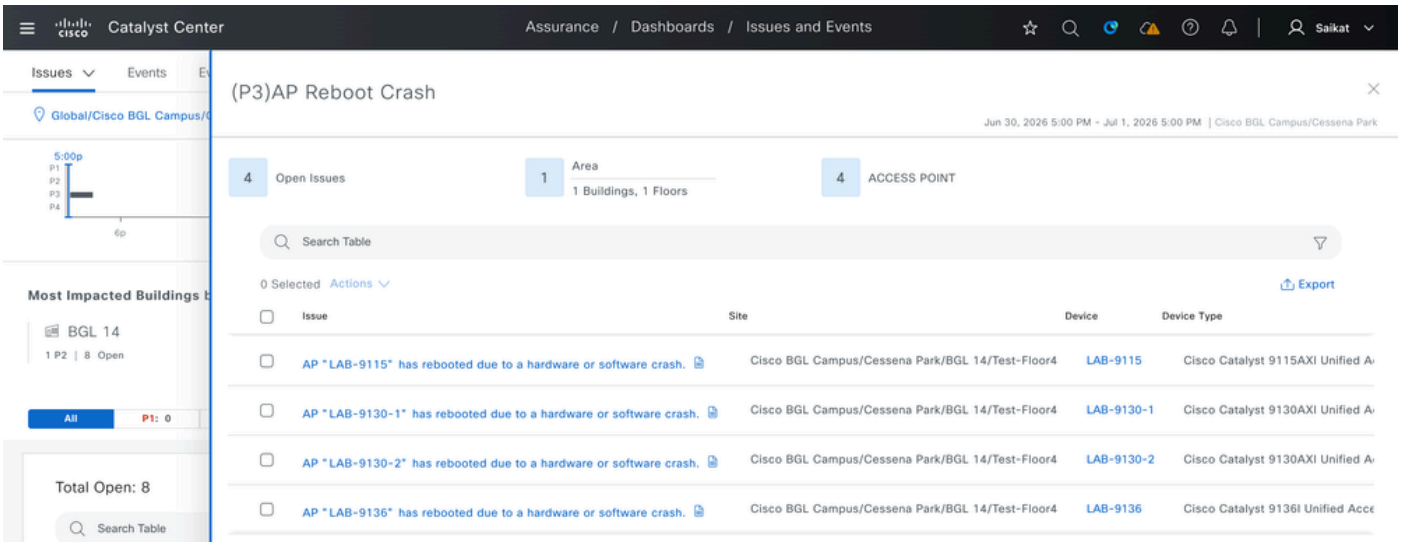
接入点问题

当Cisco接入点遇到诸如断开事件、无线电状态异常、重新启动、崩溃、RF条件差、信道利用率高或处于非活动状态等问题时，Catalyst Center会生成具有适当优先级级别的警报。您可以通过导航到保证>问题和运行状况设置来查看这些警报。



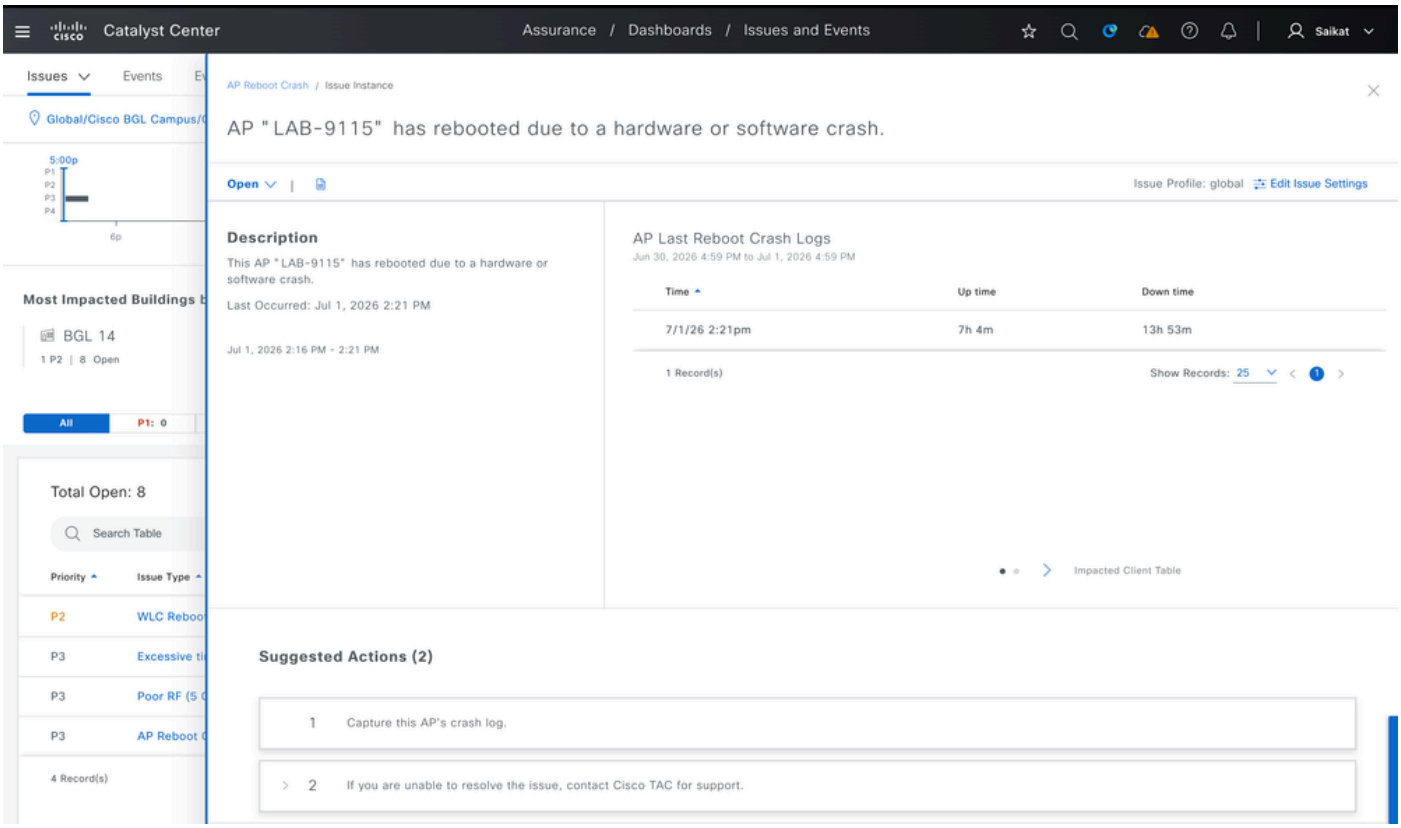
报告的问题生成具有相应优先级的警报

此部分显示您的环境中所有未解决的问题。通过点击单个事件，您可以通过单独点击每个事件获得详细见解：



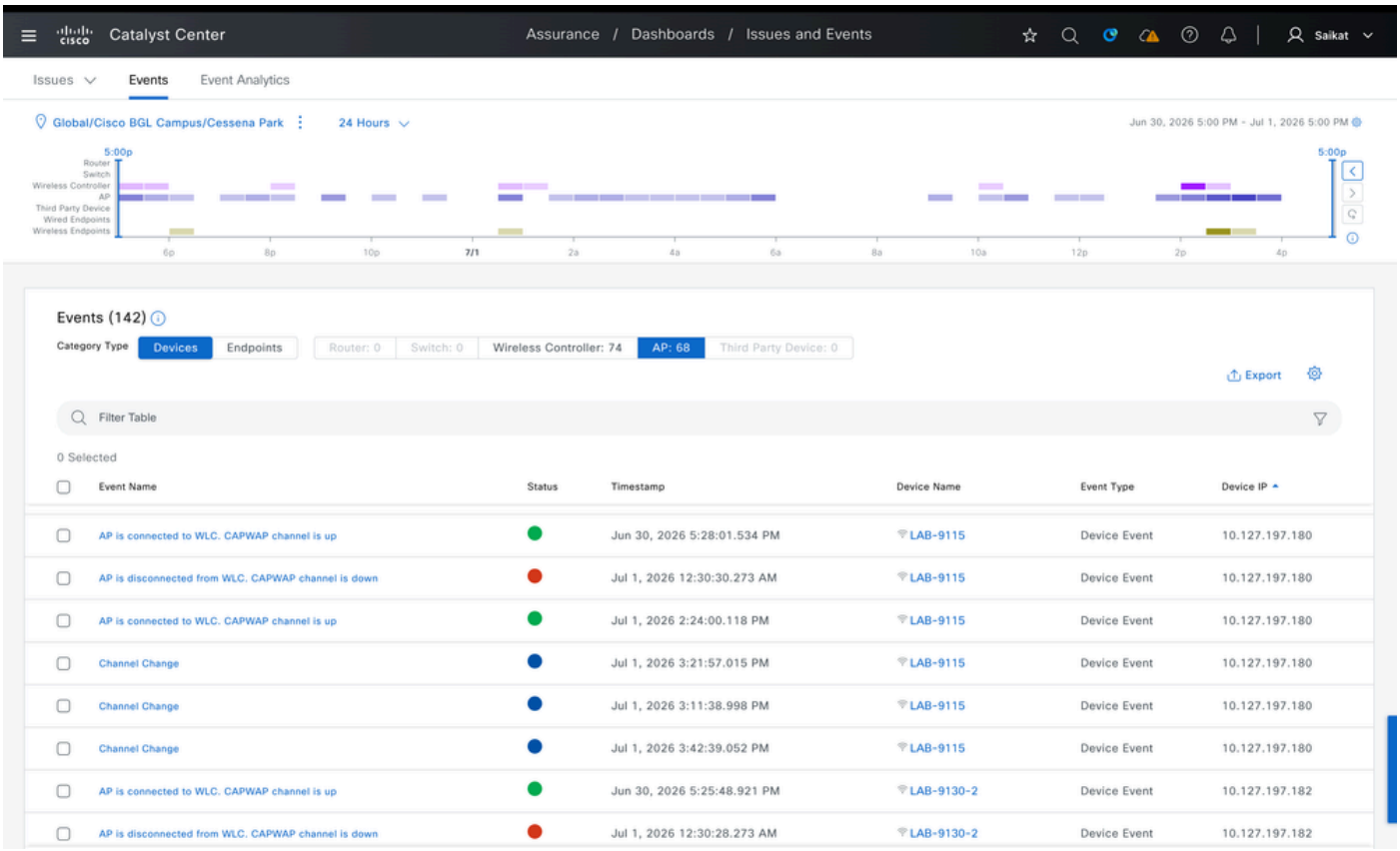
已报告问题的详细概述

单击特定问题，您可以查看有关它的详细信息，以及解决问题或进一步调查的建议操作。

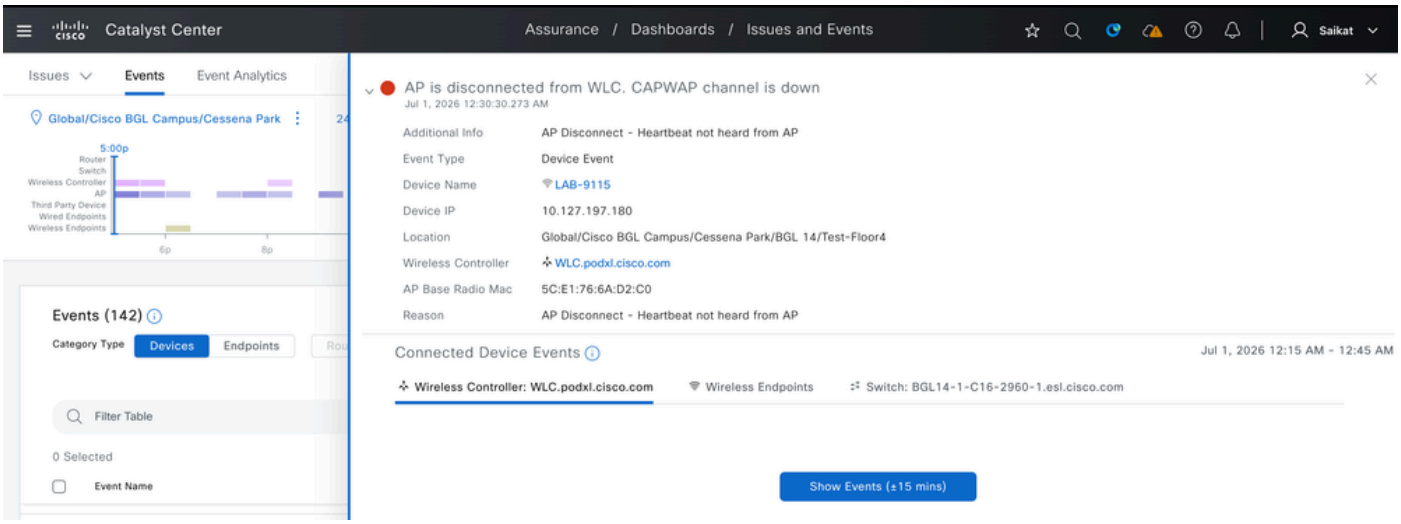


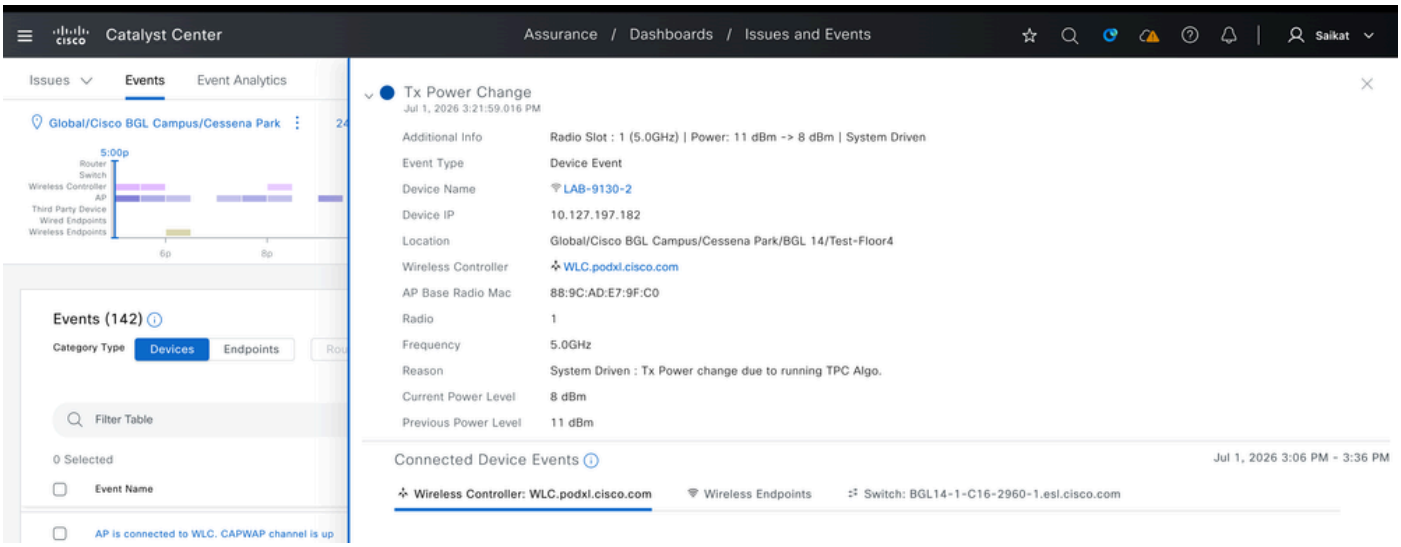
针对AP上报告问题的建议操作

此外，还可以访问事件查看器，其中包含由Catalyst Center作为系统日志接收的所有事件。这对于跟踪所有事件（例如AP加入/退出活动、信道更改、TX功率修改和重新启动）非常有用。为无线控制器和单个AP捕获这些事件。

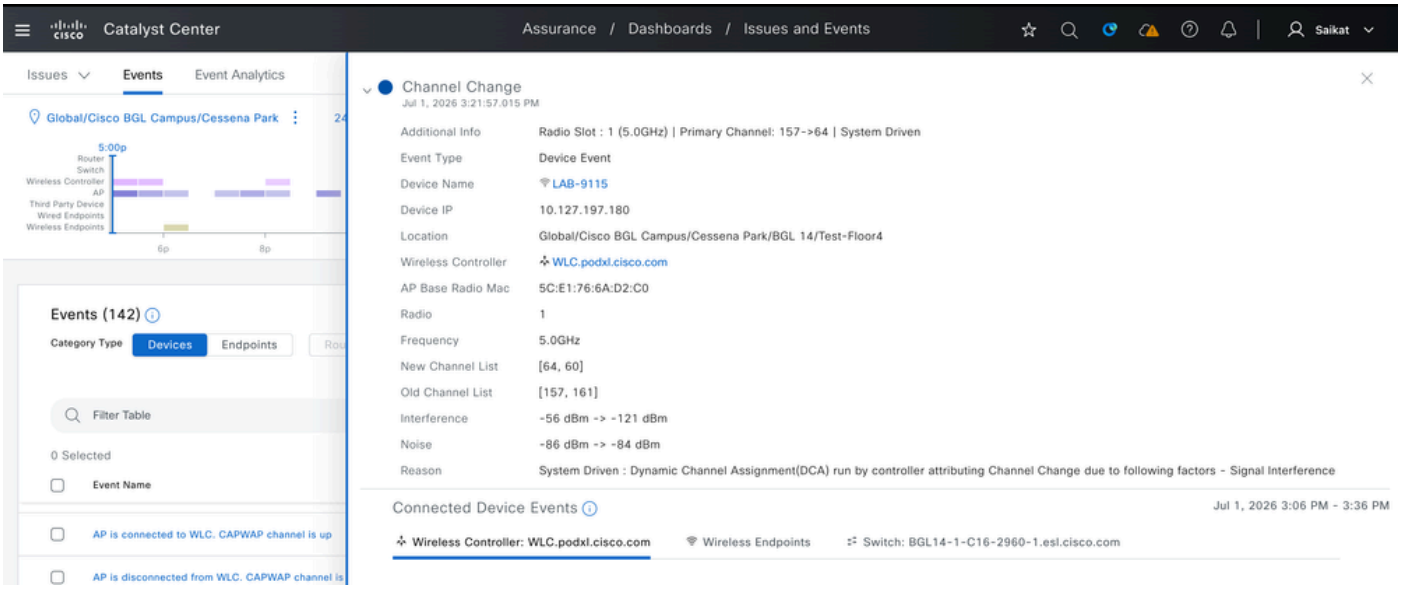


Catalyst Center上的AP事件查看器

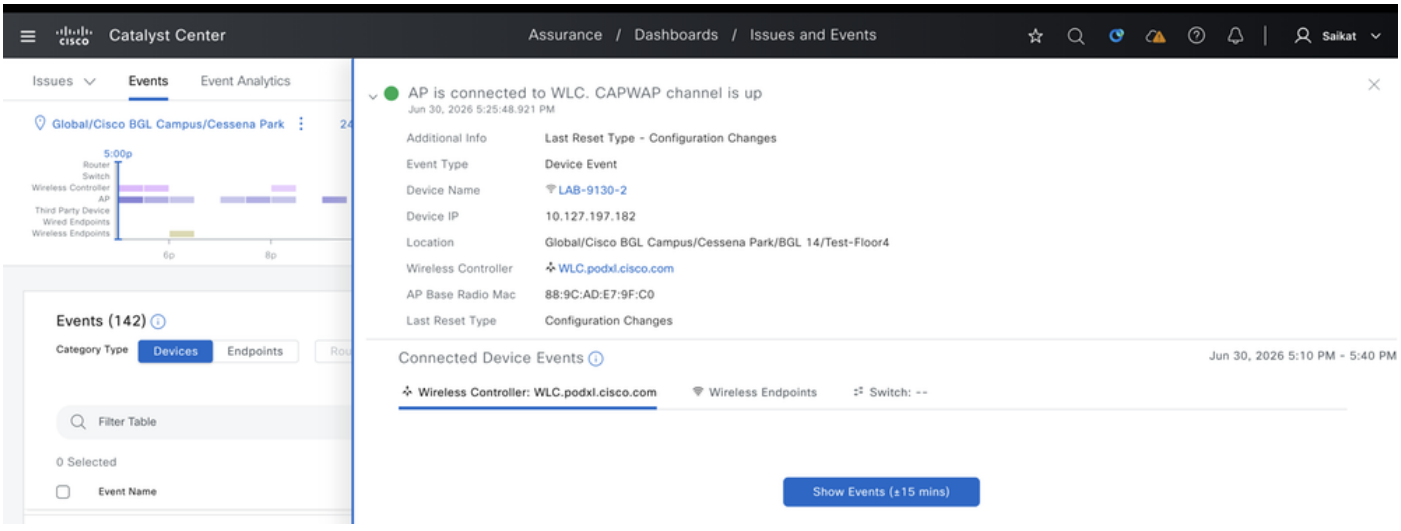




已报告事件的详细概述（通知）

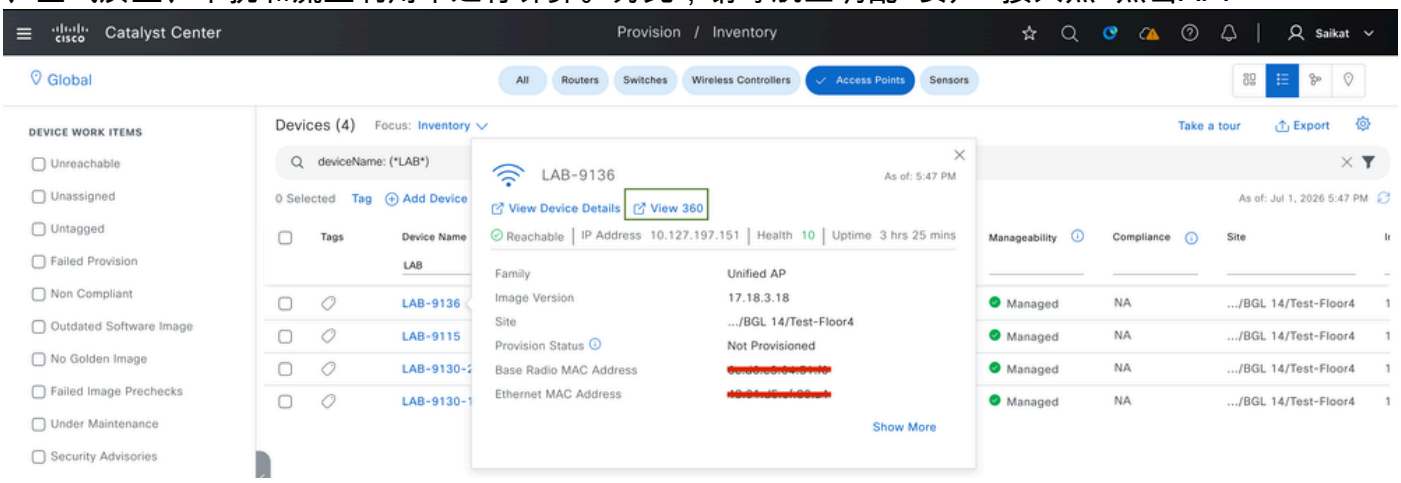


已报告事件的详细概述（通知）



所报告事件的详细概述（信息）

对于特定AP的问题，您可以检查该设备的360 Health视图。在这里，您可以看到可达性状态、报告的事件和问题，以及给定时间点该AP的运行状况得分。运行状况得分根据内存利用率、信道利用率、空气质量、干扰和流量利用率进行计算。为此，请导航至调配>资产>接入点>点击AP:

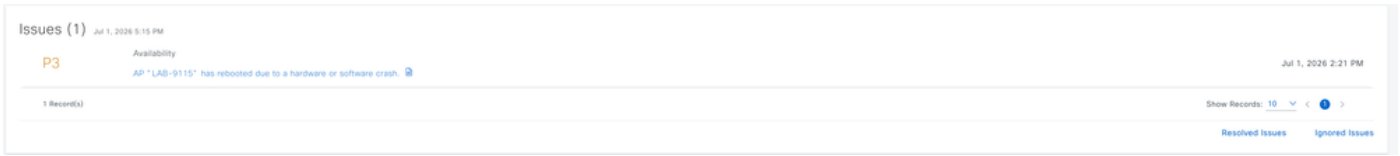


查看单个AP的360

设备360遥测摘要：在此，您可以看到两个无线电的AP整体运行状况得分时间线、系统资源利用率（内存、CPU）、数据平面链路错误和无线电特定统计信息（噪声、信道利用率、干扰、流量利用率）。设备360允许您将运行状况时间表滑块移回支持的历史窗口内的任意点（30天）。

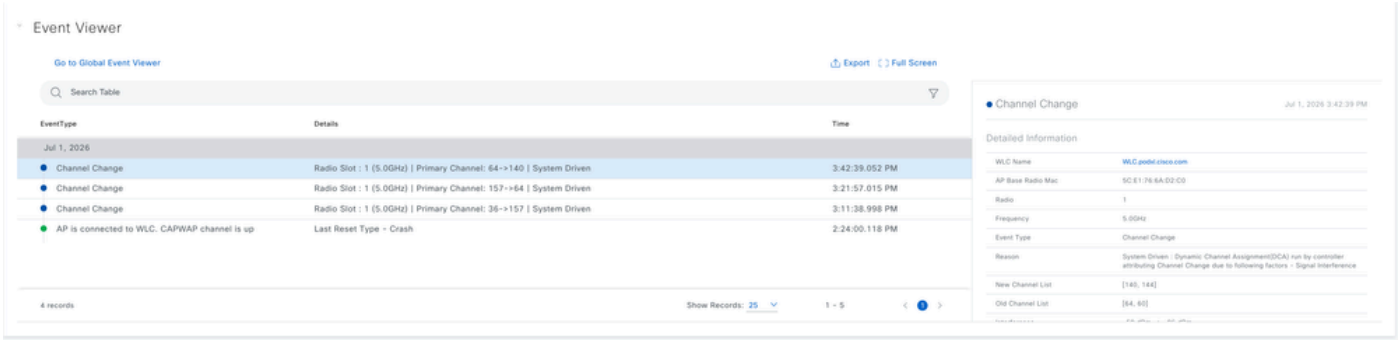
查看360:AP遥测状态和运行状况

问题 — 在此，您可以看到AP的未决问题列表以及严重性(P1-P4)、问题类别、说明和时间戳。



为AP报告的问题

事件查看器 — 您可以查看AP事件按时间顺序排列的日志（例如信道更改、CAPWAP状态）以及详细的事件信息，如WLC名称、射频、频率、原因和旧/新信道列表。

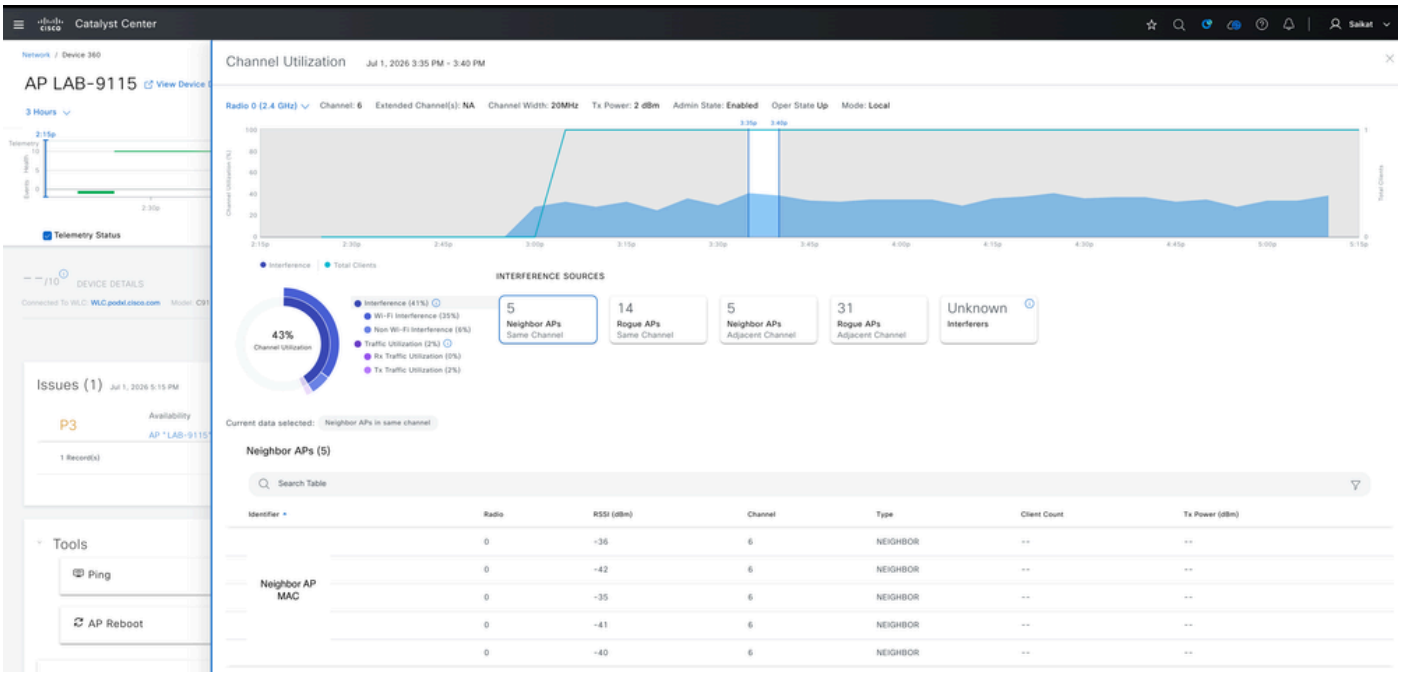


单个AP的事件查看器

带客户端列表的物理邻居拓扑 — 此视图显示连接WLC、AP和已连接客户端的物理拓扑，以及其他客户端详细信息，如设备名称、运行状况得分和MLO

AP的物理拓扑

信道利用率 — 您可以看到AP信道利用率趋势、干扰源（邻居AP、欺诈AP、未知干扰源）以及包含RSSI、信道和类型的详细邻居AP表。



单个AP的信道利用率

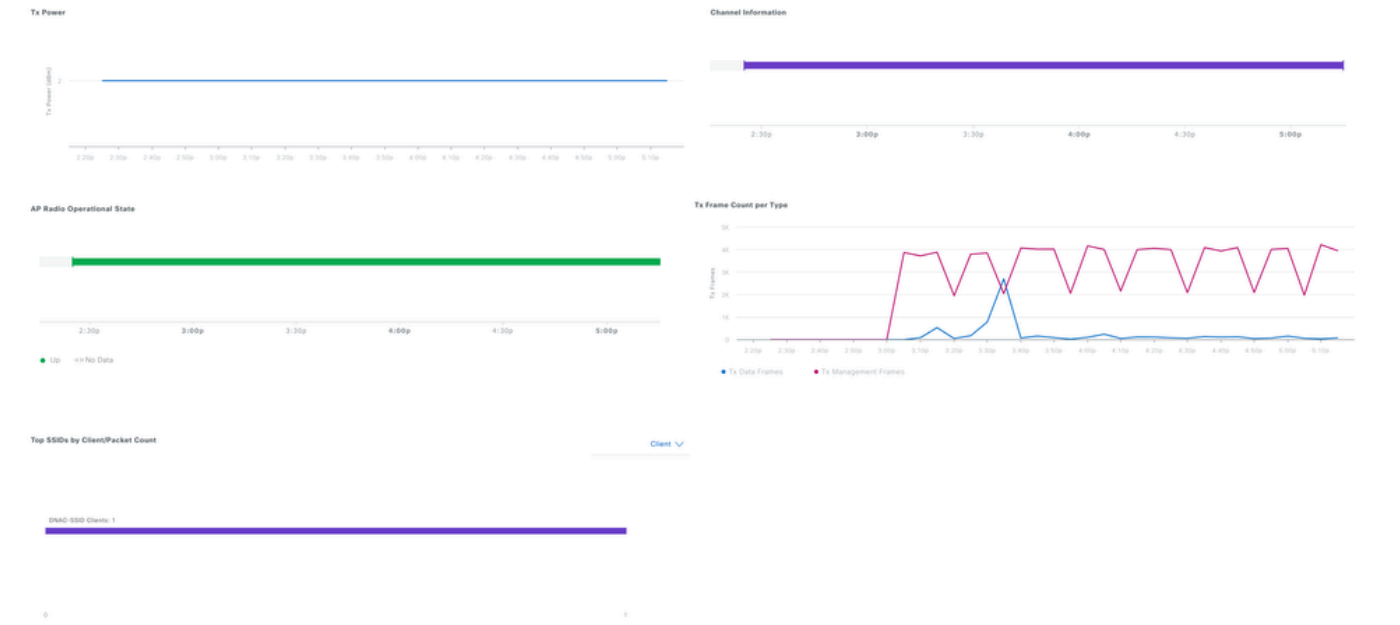
详细信息（设备选项卡）— 此部分显示设备信息（AP名称、IP、型号、MAC地址、软件版本）、可用性详细信息（正常运行时间、控制器加入时间、上次重置原因）、CPU/内存利用率图表以及AP到WLC连接图。

AP的设备详细信息

无线电特定KPI:您可以在此处查看无线电级别KPI，包括所选无线电的信道利用率、客户端计数、吞吐量（Rx/Tx速率）、重试、噪声和空气质量。

单个AP的RF统计信息

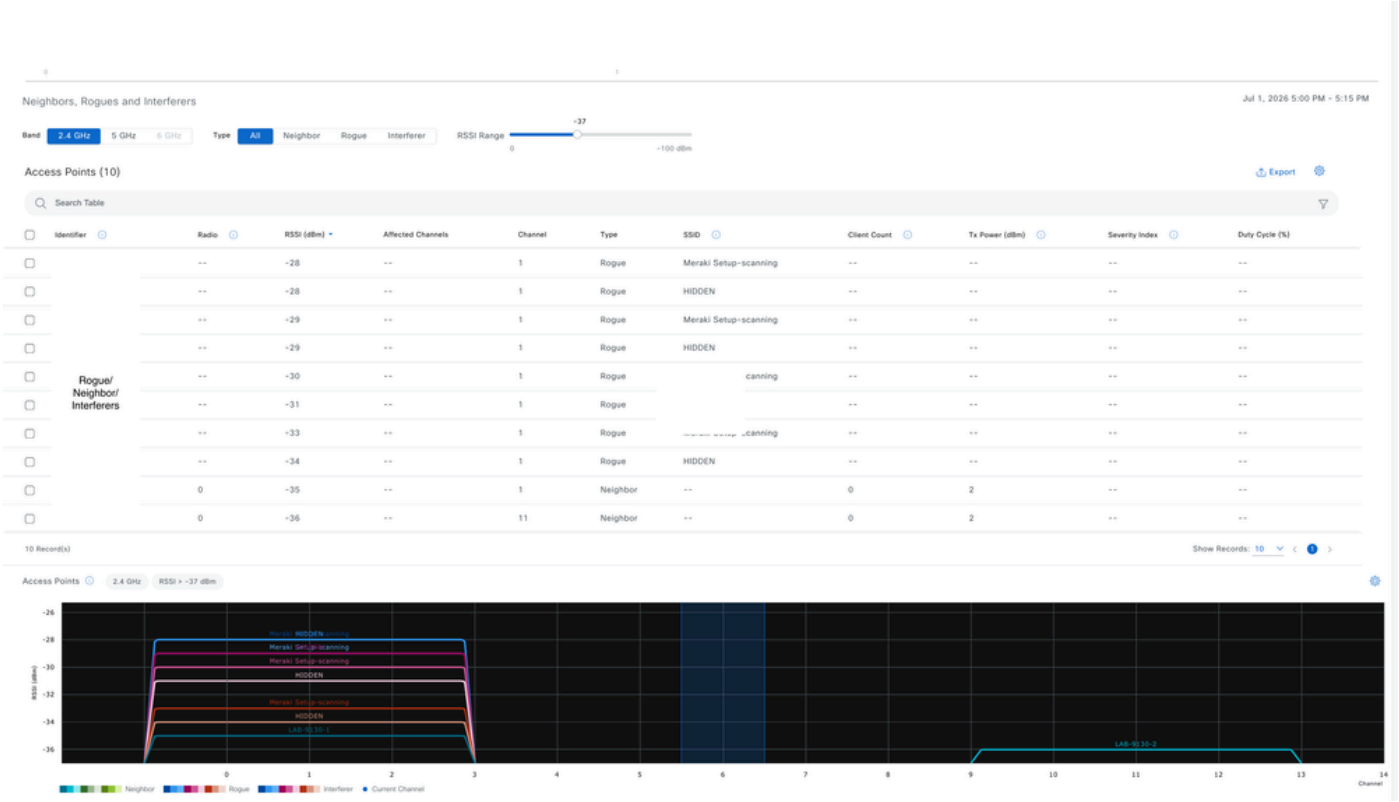
Tx Power、Channel Information & Frame Stats：在此屏幕上，您可以查看Tx power trends、channel assignment history、AP radio operational state、Tx frame counts by type(data vs. management)，以及top SSID s by client/packet count。



单个AP的RF统计信息

邻居、恶意程序和干扰源：通过此视图，您可以看到所有附近的邻居、欺诈设备和干扰设备及其

RSSI、受影响的信道、SSID、客户端计数、发射功率和严重性指数，以及可视RSSI-vs-channel图
。



为单个AP报告的欺诈、邻居和干扰源

设备360控制面板汇集了射频详细信息（如信道使用、干扰、噪声和重试）以及附近的邻居、欺诈和干扰信息 — 帮助您确定AP问题是由射频拥塞、信道冲突还是欺诈设备引起的。设备运行状况数据（如CPU、内存、重新启动历史记录和连接状态）以及Event Viewer and Issues（事件查看器和问题）面板，可帮助您了解硬件崩溃、连接断开和意外的通道更改。结合拓扑和客户端视图，可全面了解从射频问题到单个客户端问题的故障排除过程，以及内置的建议操作以帮助解决这些问题

接入点的智能捕获

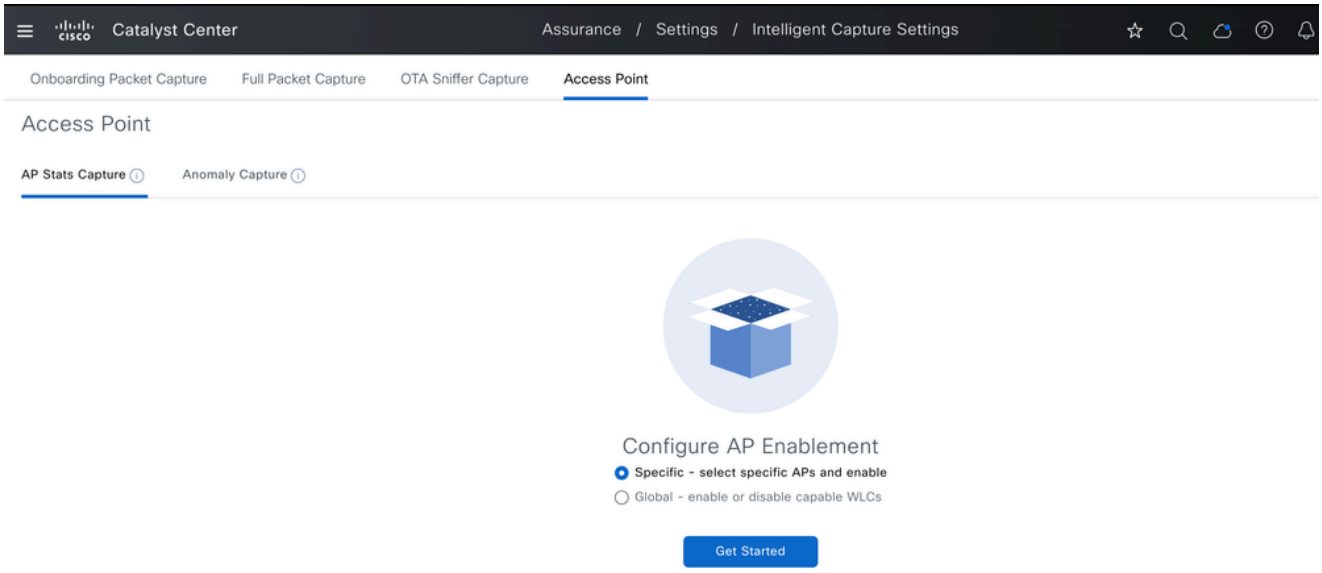
接入点的智能捕获提供两个主要功能：不间断的实时RF监控、异常检测和按需空中捕获、频谱分析
。

AP统计信息捕获

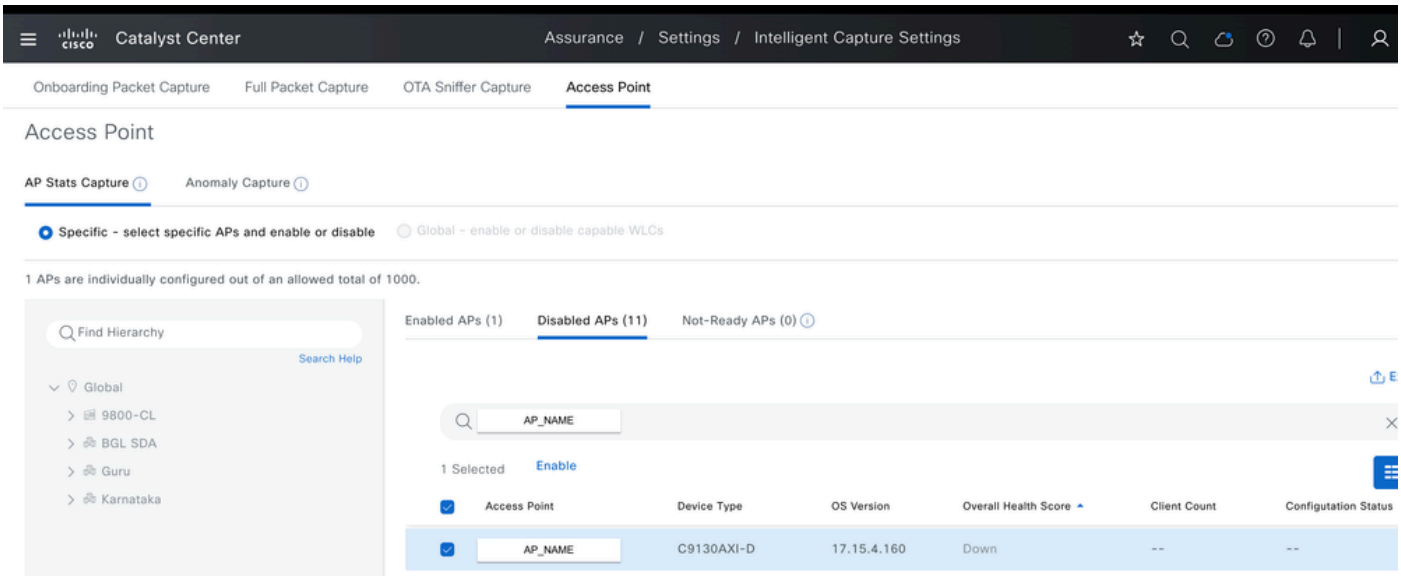
您可以启用和管理一个或多个接入点的AP统计信息数据收集（包括AP无线电统计信息、WLAN统计信息和AP客户端统计信息），最多可支持1000个AP。

要启用AP统计信息捕获，请导航到保证>设置>智能捕获设置>接入点> AP统计信息捕获。从这里，您可以灵活选择：

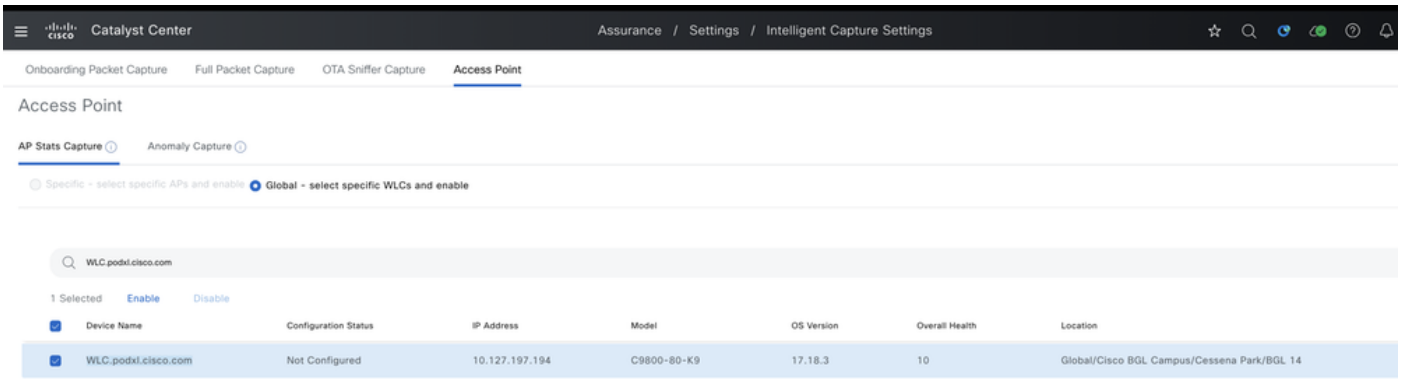
- 为特定AP（最多1000个）启用它，或
- 为特定WLC下管理的所有AP全局启用此功能。



AP统计信息捕获选项

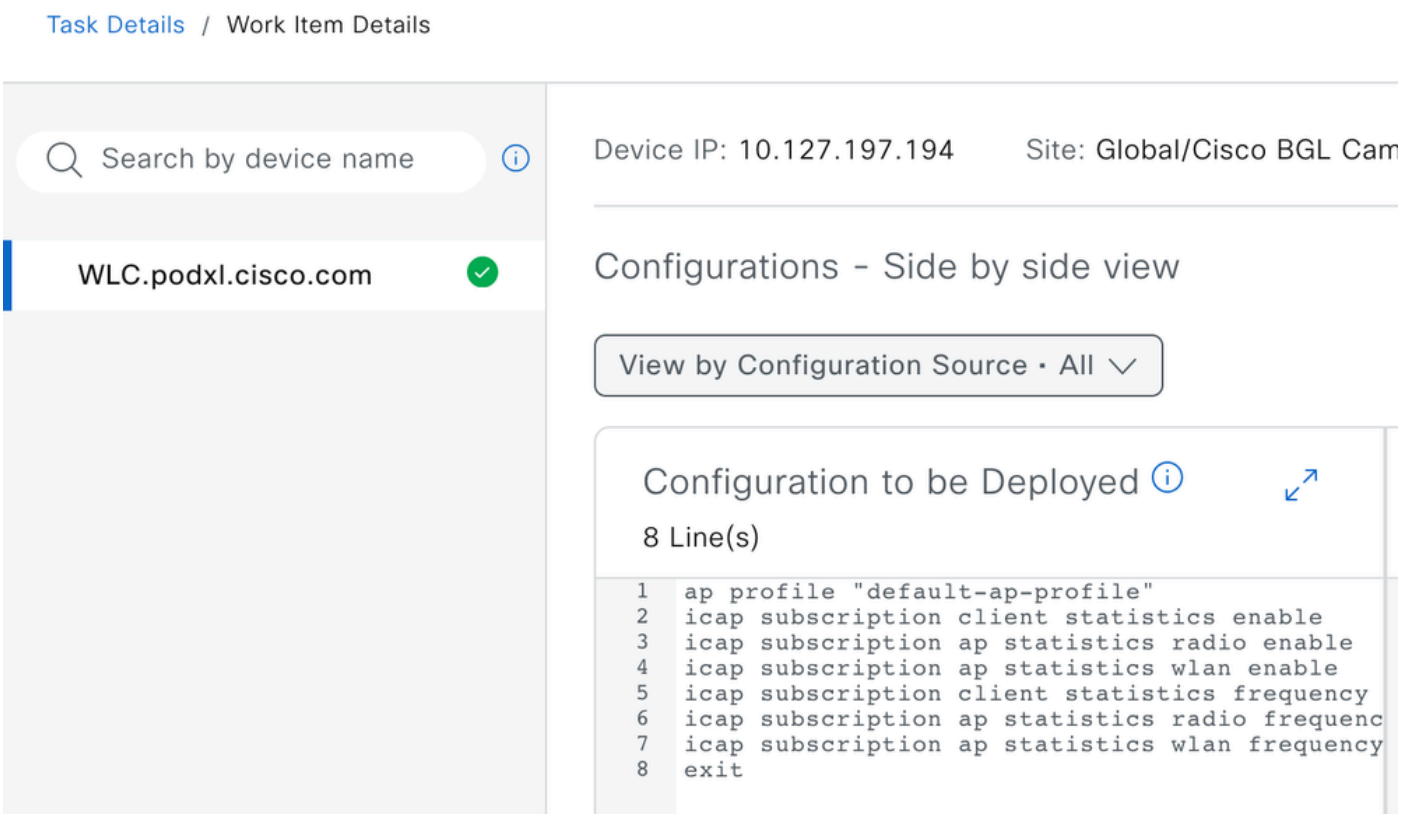


在特定AP上启用AP统计信息智能捕获



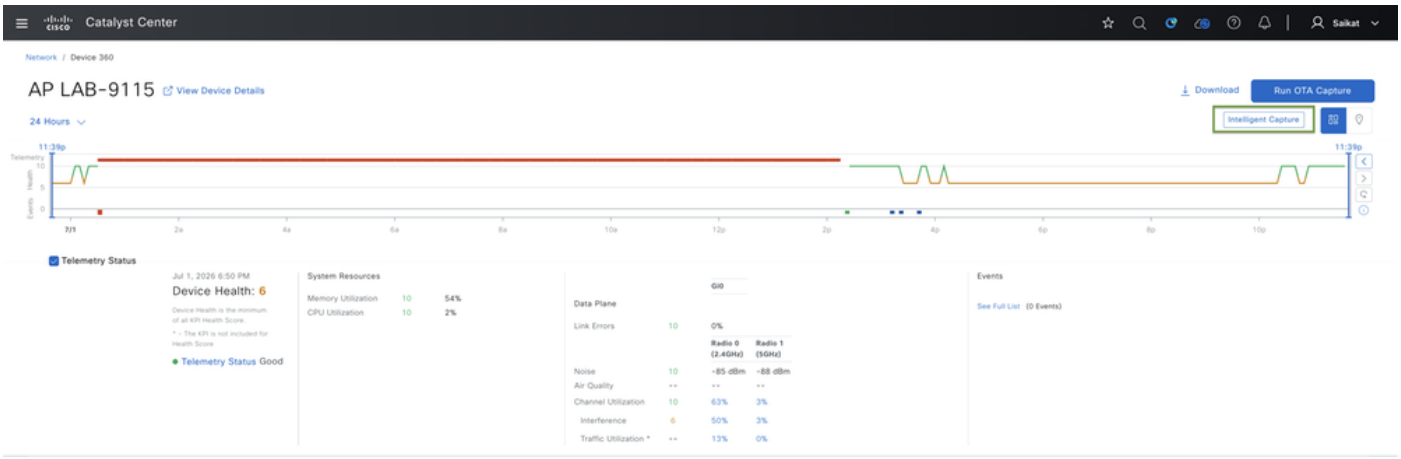
全局启用AP统计信息智能捕获

启用AP统计信息捕获后，Catalyst Center会将相应的配置推送到WLC — 适用于所选的特定AP或所有AP，具体取决于它是在单个AP级别启用还是在WLC级别全局启用。

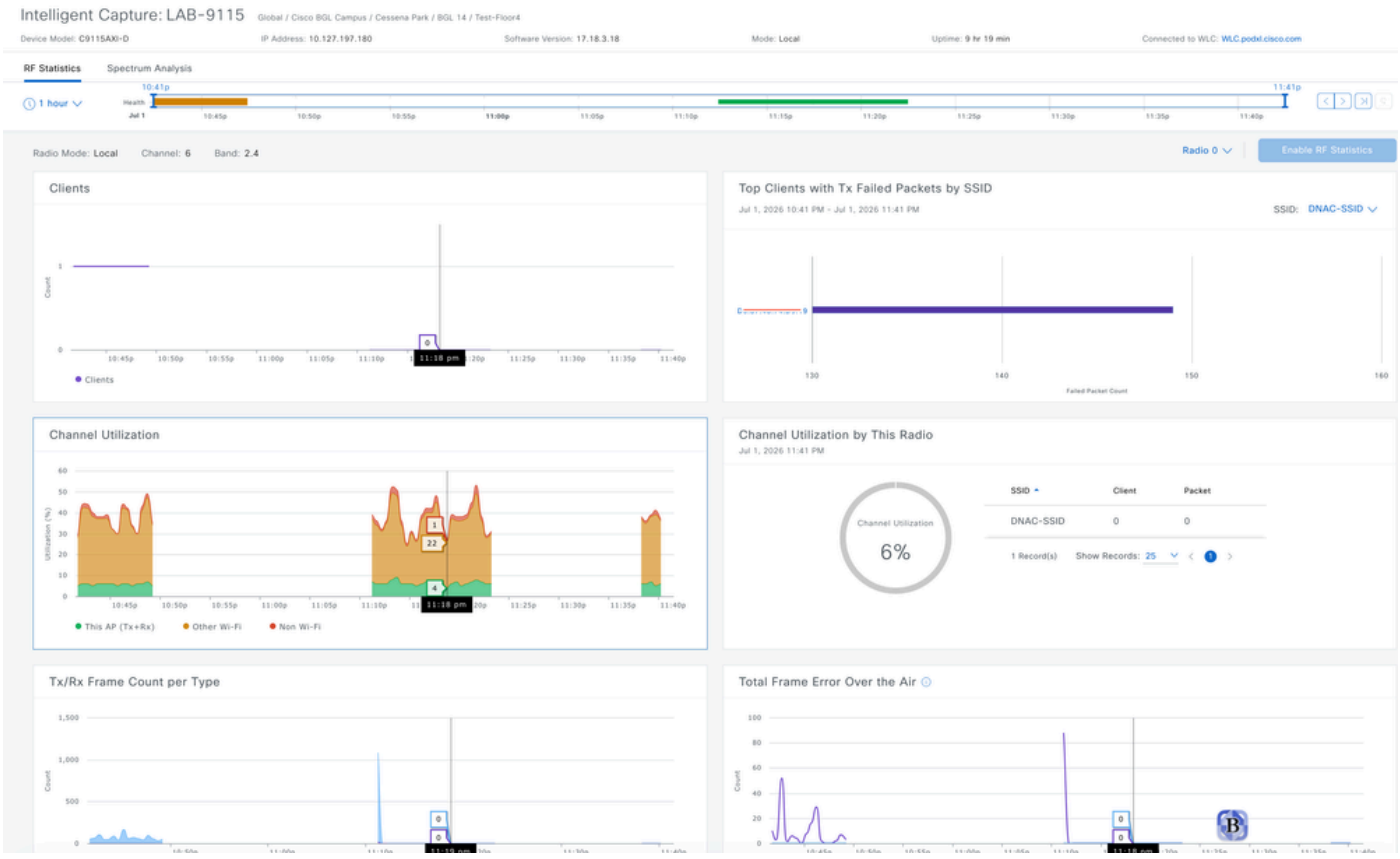


启用AP统计信息捕获时要推送的配置

启用此捕获后，您可以直接从Device 360（设备360）页面查看通过智能捕获收集的实时数据。此外，您可以根据需要运行Spectrum Analysis，以进一步调查RF情况。



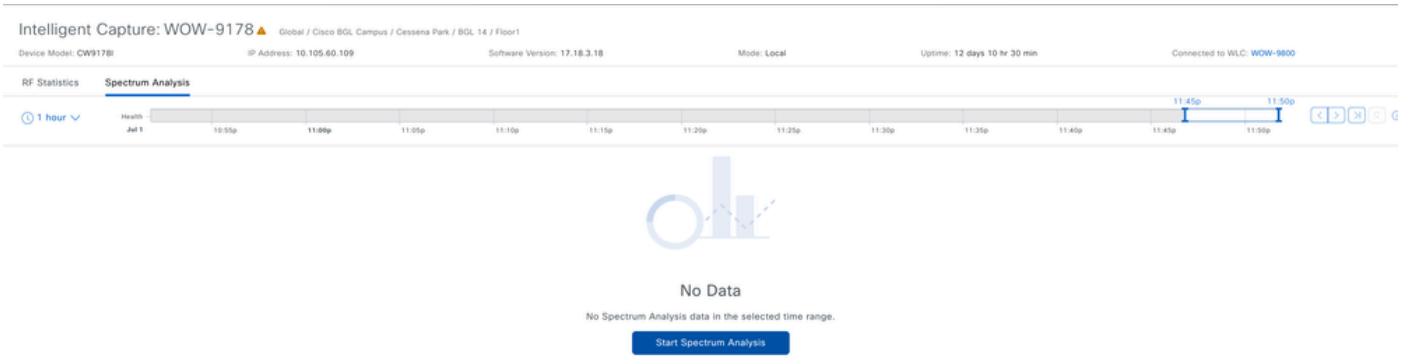
设备360中AP的智能捕获



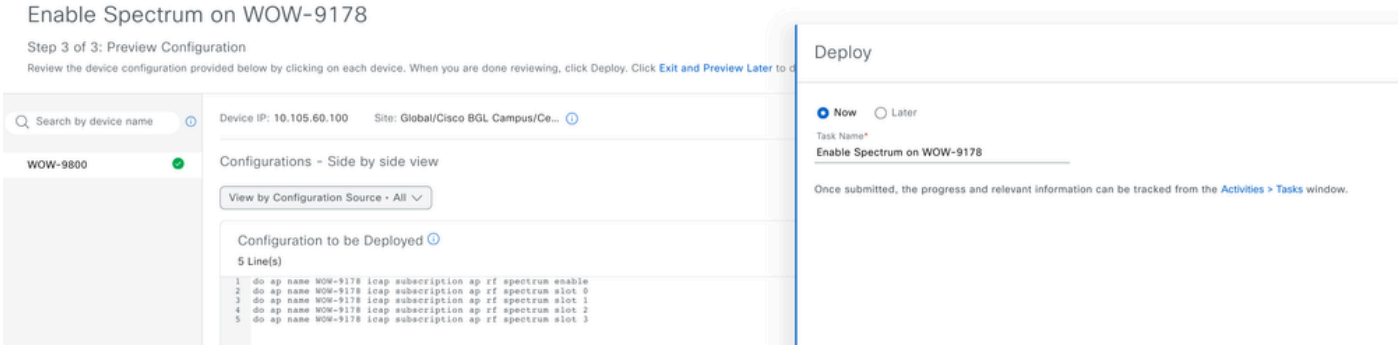
在Catalyst Center上使用智能捕获捕获AP统计信息

在这里，您可以看到实时统计信息，包括每种类型的Tx/Rx帧计数、空中帧错误总数、组播/广播计数器、Tx功率和噪声本底、信道利用率、按SSID显示的Tx数据包发生故障的排名靠前的客户端，以及使用智能捕获为特定AP捕获的客户端数据。

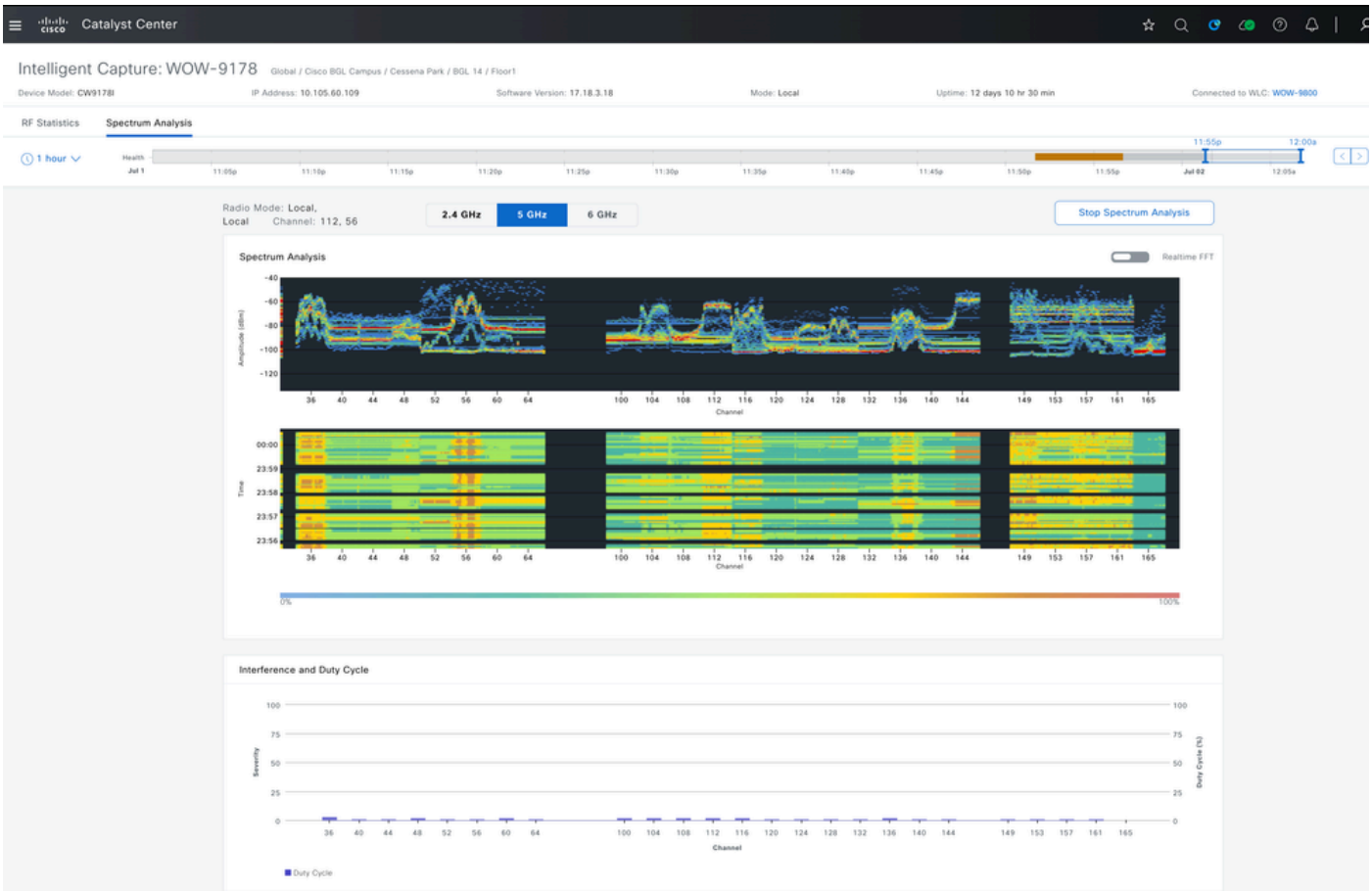
在需要检查RF条件时，您还可以对单个AP运行按需频谱分析。但是，此功能需要AP型号才能支持。



按需频谱分析



应用于频谱分析的配置

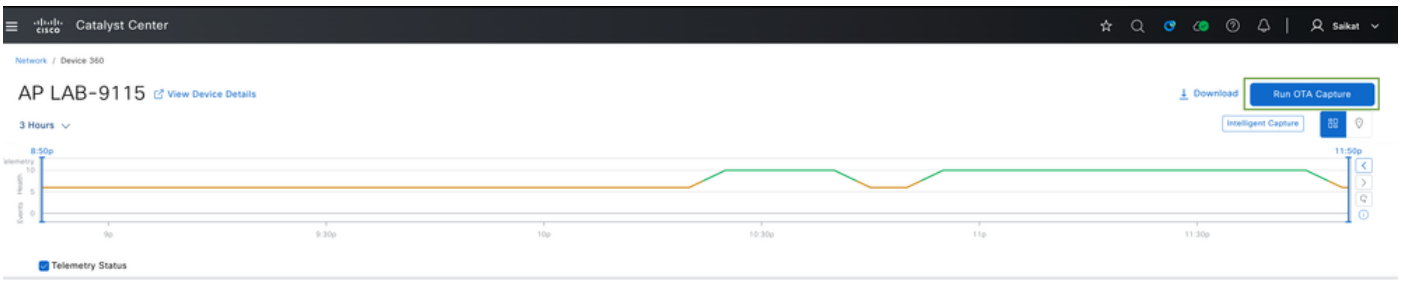


频谱分析结果

OTA嗅探器捕获

Catalyst Center允许您在特定无线电、带宽和信道上启用OTA嗅探器捕获。启用后，会捕获在该无线电和信道上传输的所有Wi-Fi数据包。您最多可以选择2个AP来执行嗅探。请记住，只要启用OTA捕获，为流量嗅探配置的2个AP即可在其各自的无线电/插槽上切换到嗅探器模式。

要启用此功能，请导航到调配>库存>接入点，单击要为其收集OTA数据的AP，然后选择运行OTA捕获。最多可以选择两个附近的接入点嗅探流量。

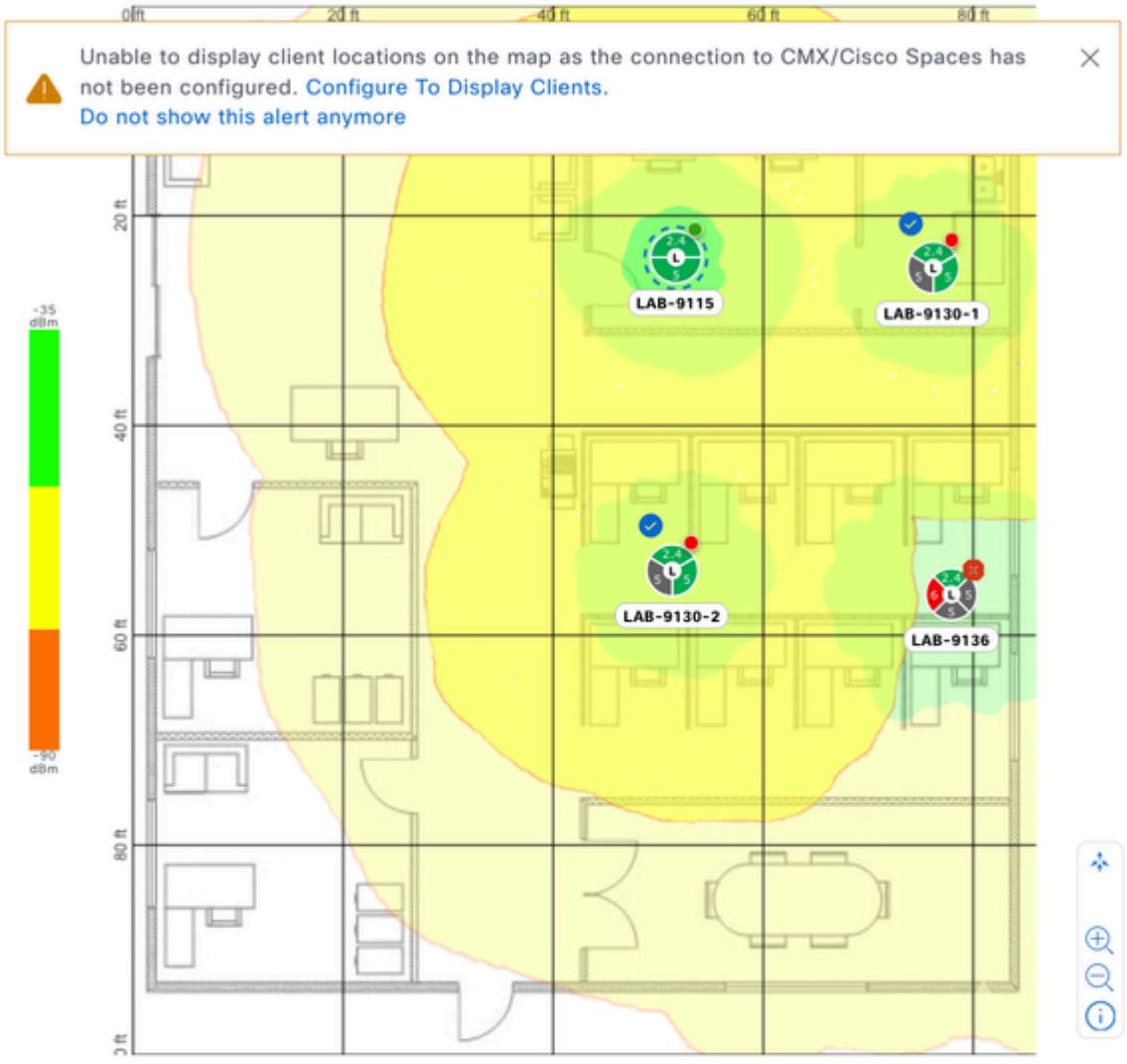


对目标AP运行OTA捕获

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

选择邻居AP（最多2个）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

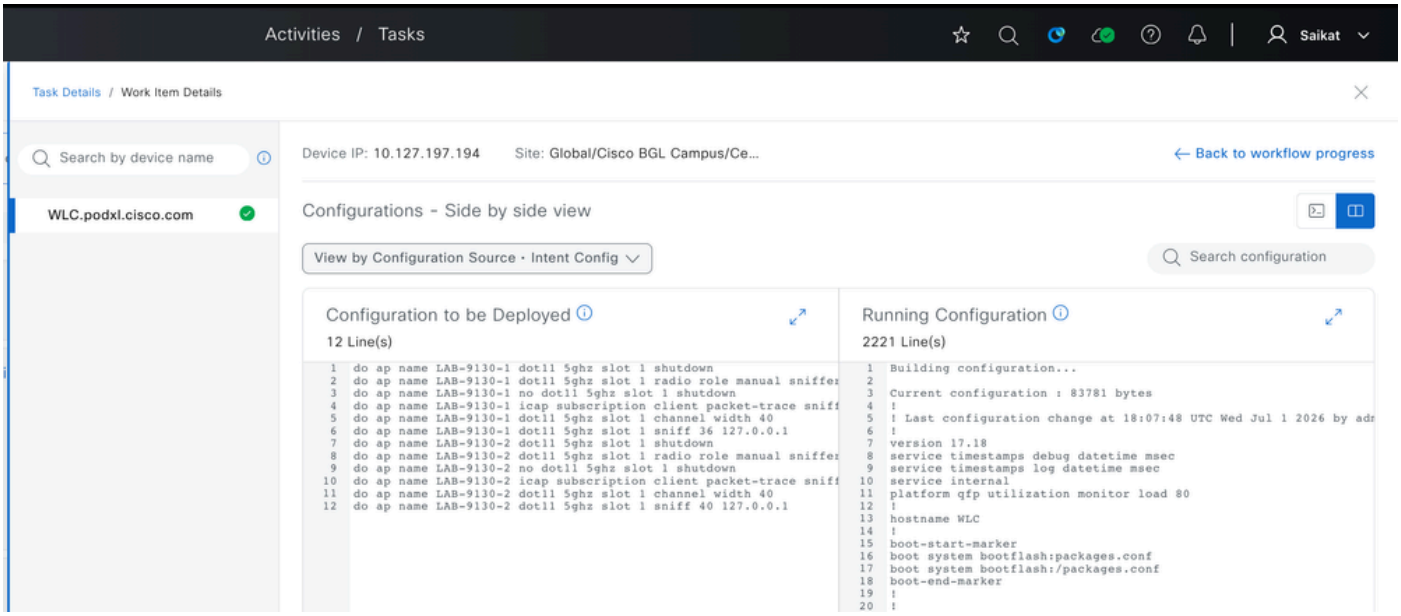
Select Radio
1 (Client Count: 0)

Select Channel Width
40

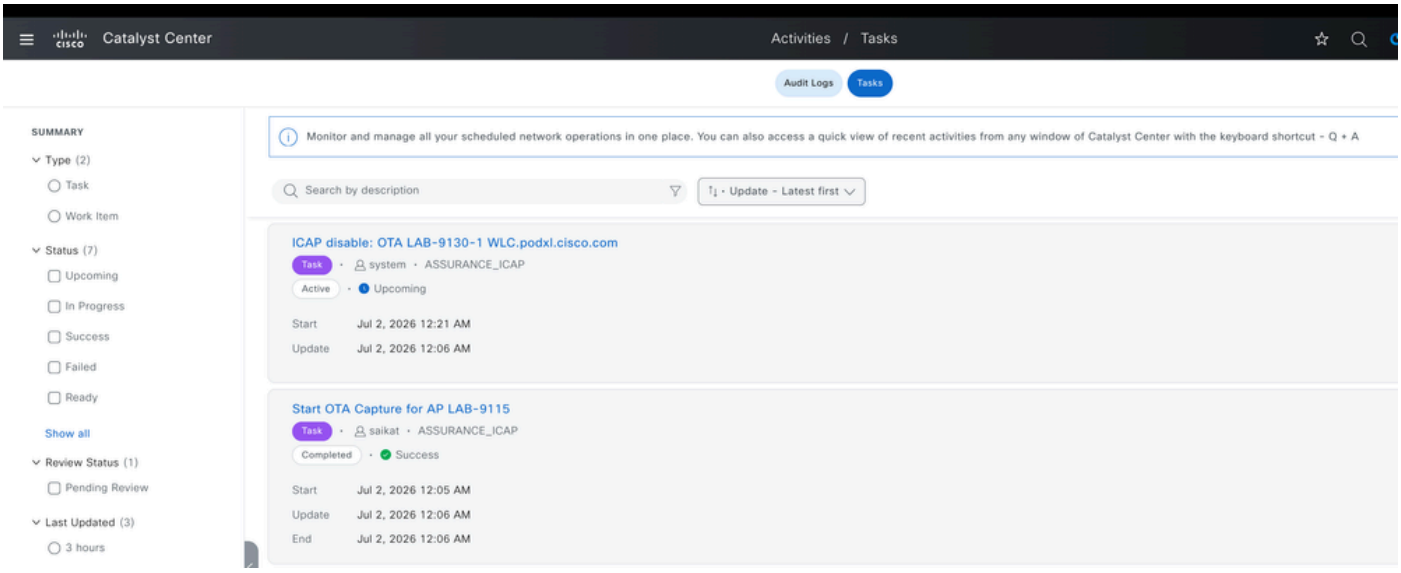
Select Channel
40

back Next

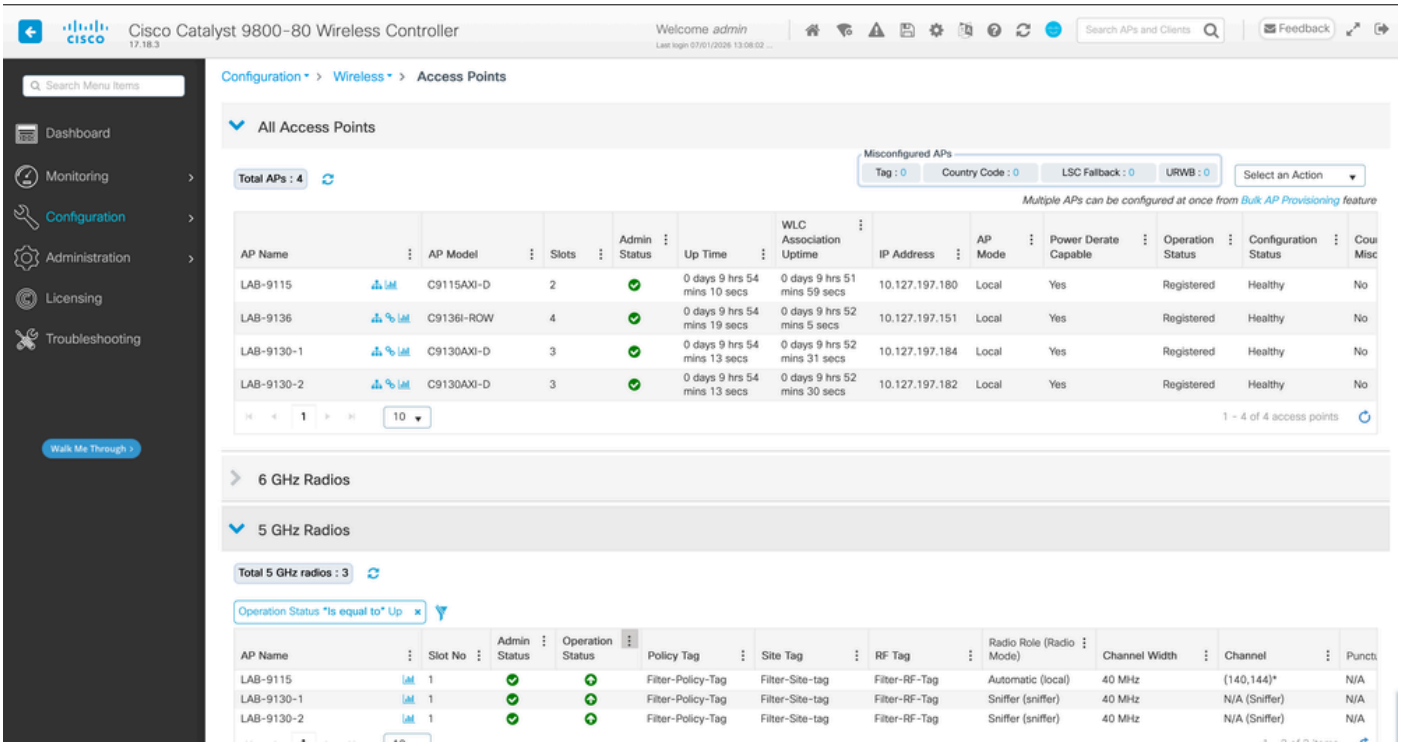
选择Radio、Channel-Width、Channel以嗅探流量



启用OTA捕获的配置预览

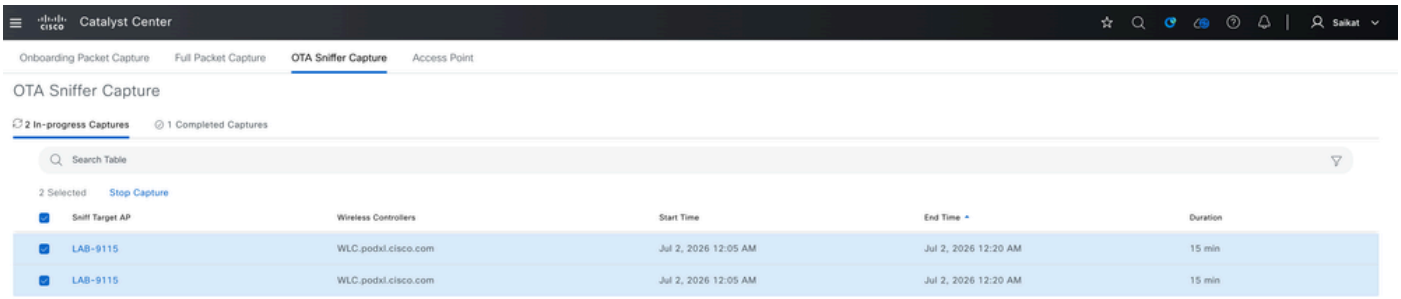


启用OTA捕获时安排的任务



插槽1处于侦听器模式，用于已启用AP以侦听流量

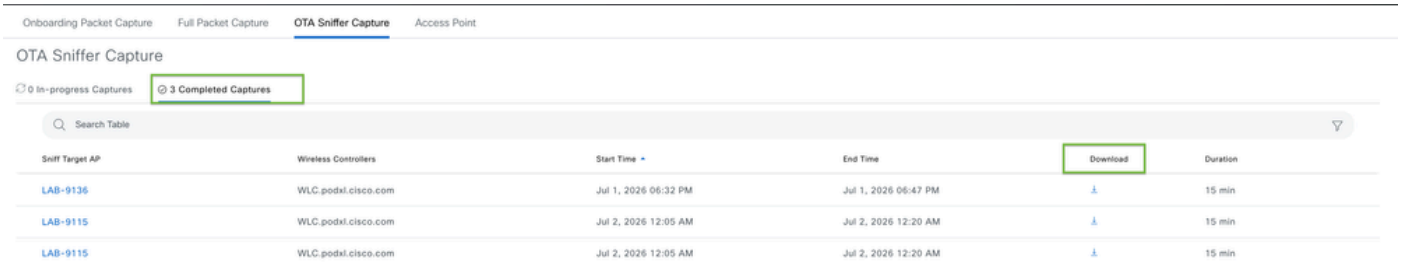
要通过导航到保证>设置>智能捕获设置> OTA嗅探器捕获检查运行OTA捕获的状态：



OTA捕获的状态

注意：默认情况下，Catalyst Center在自动禁用此任务之前运行该任务15分钟，但也可以随时手动将其停止。

完成OTA捕获后，它将显示在Completed Captures部分中，您可以从其中下载文件。



已完成的捕获 — OTA嗅探器捕获

异常检测

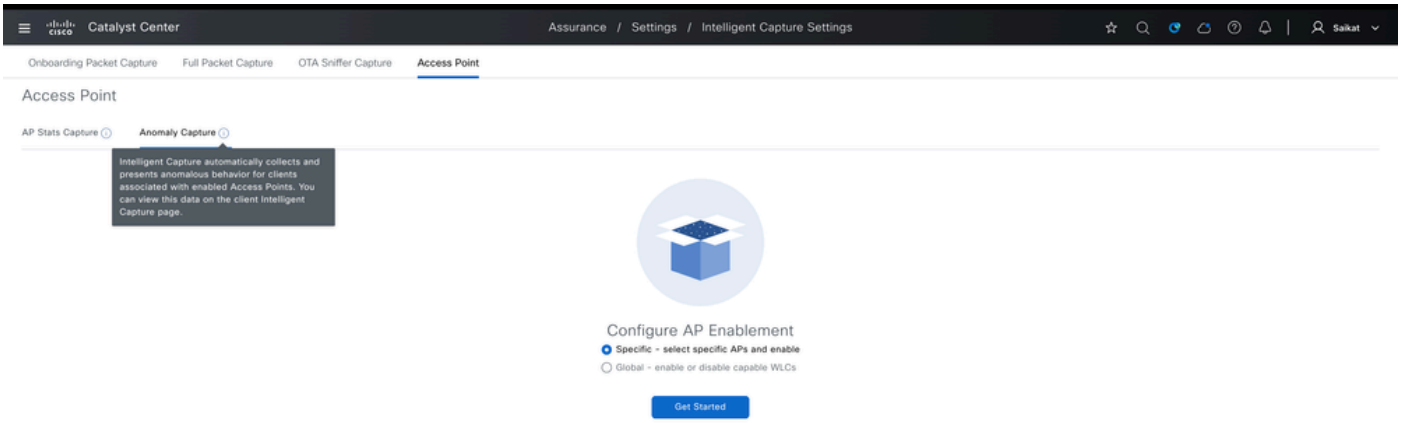
此功能允许思科AP检测与其关联的无线客户端行为中可能的不规则行为。此命令包括：

- 异常检测
- 异常数据包捕获
- 异常独立报告
- 异常情况摘要报告

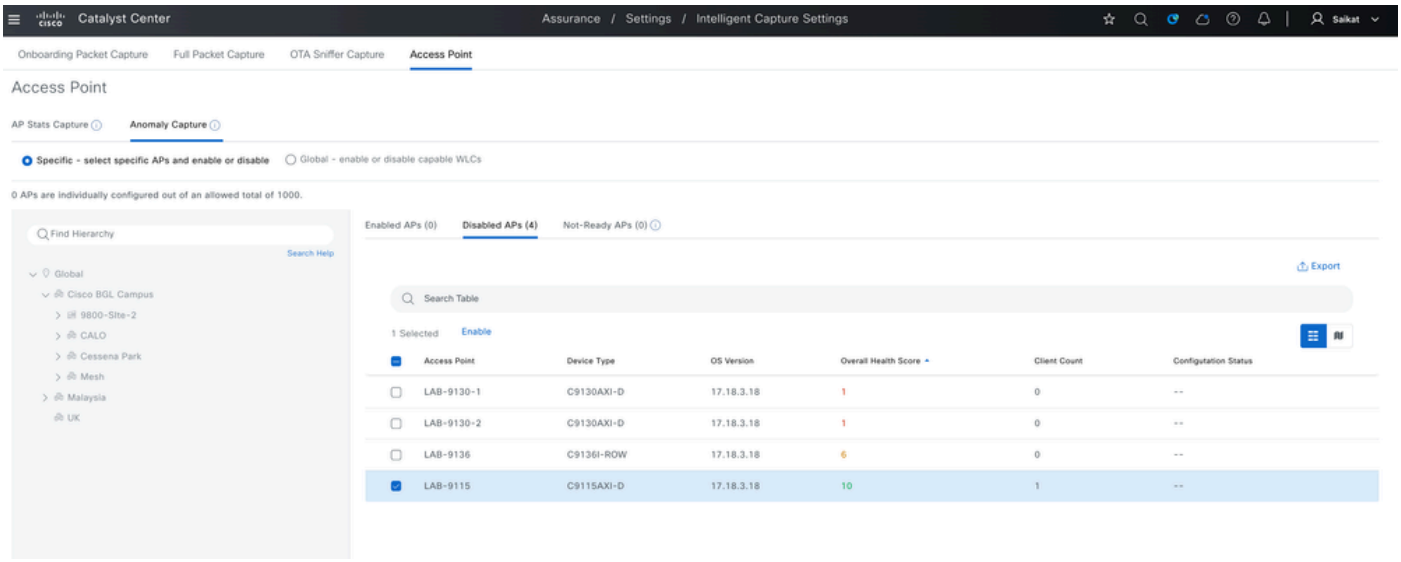
要启用AP异常捕获，请导航到保证>设置>智能捕获设置>接入点>异常捕获。在此处，您可以灵活地进行以下操作：

- 为特定AP（最多1000个）启用它，或
- 为特定WLC下管理的所有AP全局启用此功能。

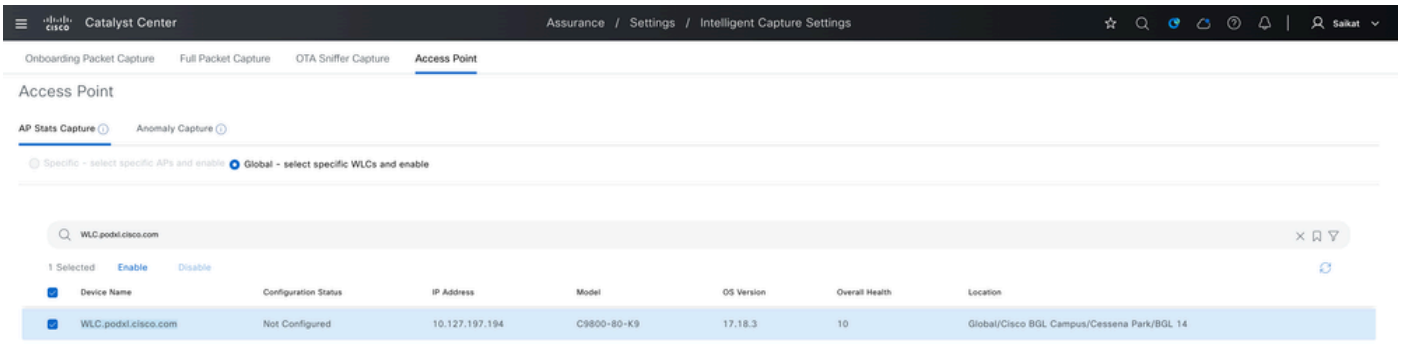
启用后，智能捕获将自动收集与这些AP关联的客户端并显示异常行为，这些数据可在“客户端智能捕获”页面上查看。



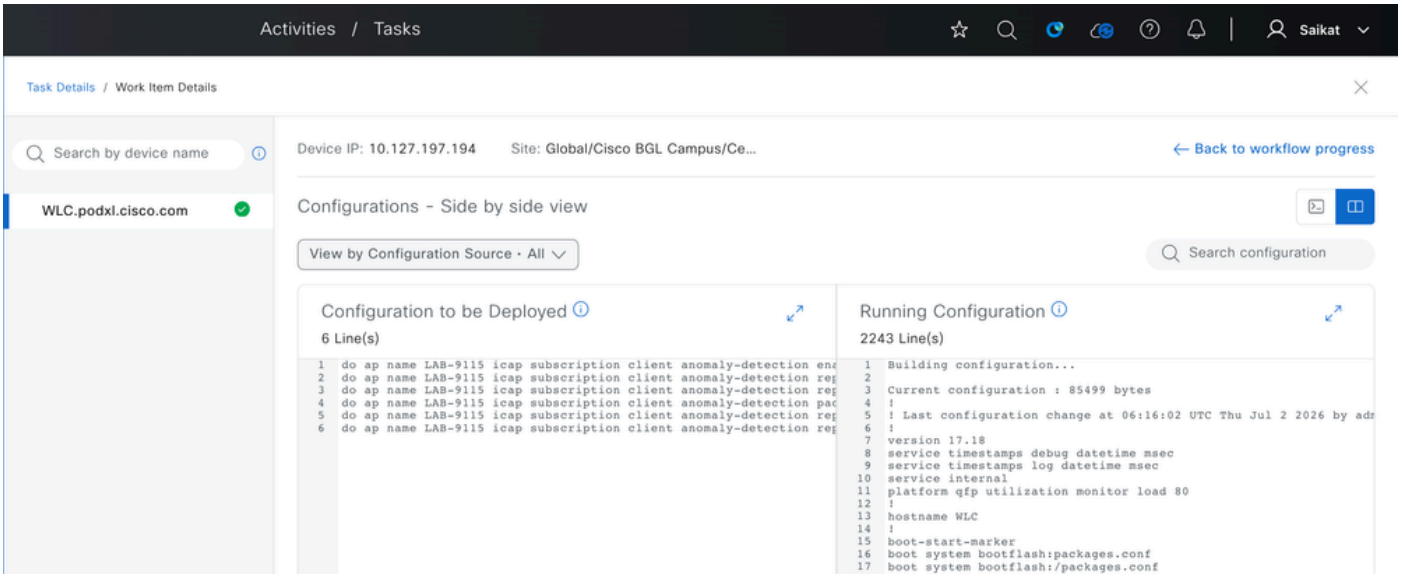
配置异常捕获



为特定AP启用异常捕获

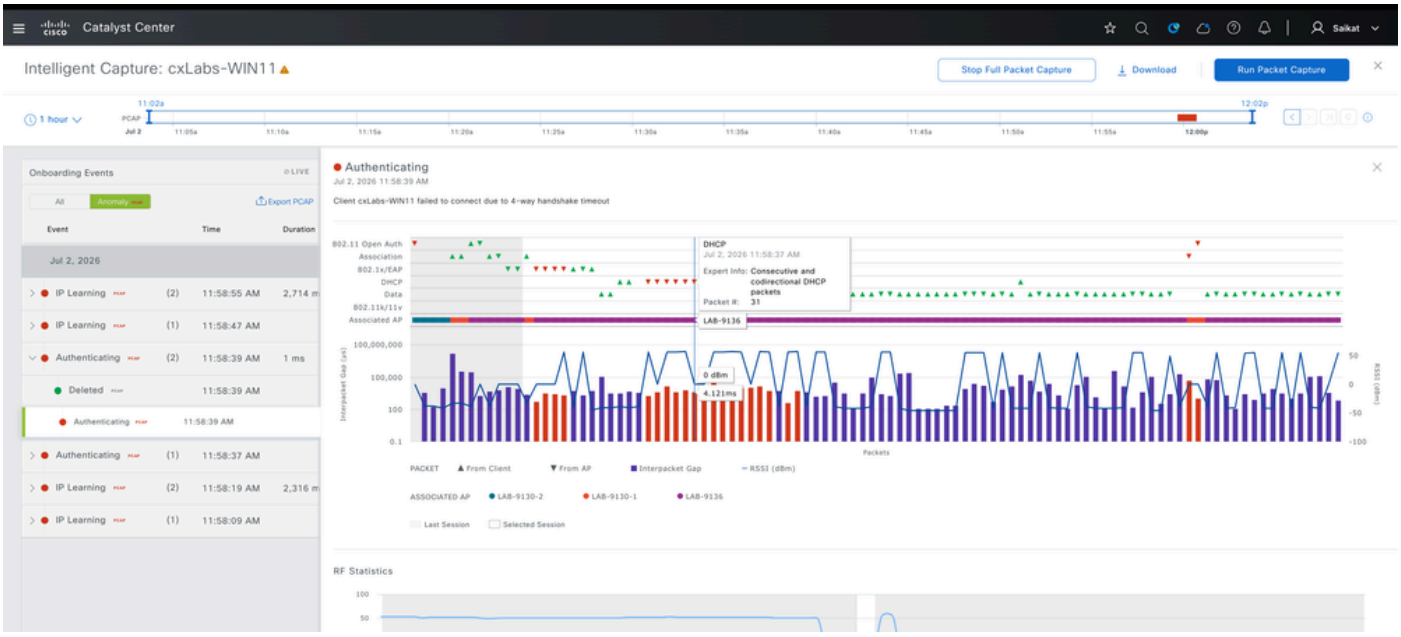


为特定WLC全局启用异常捕获

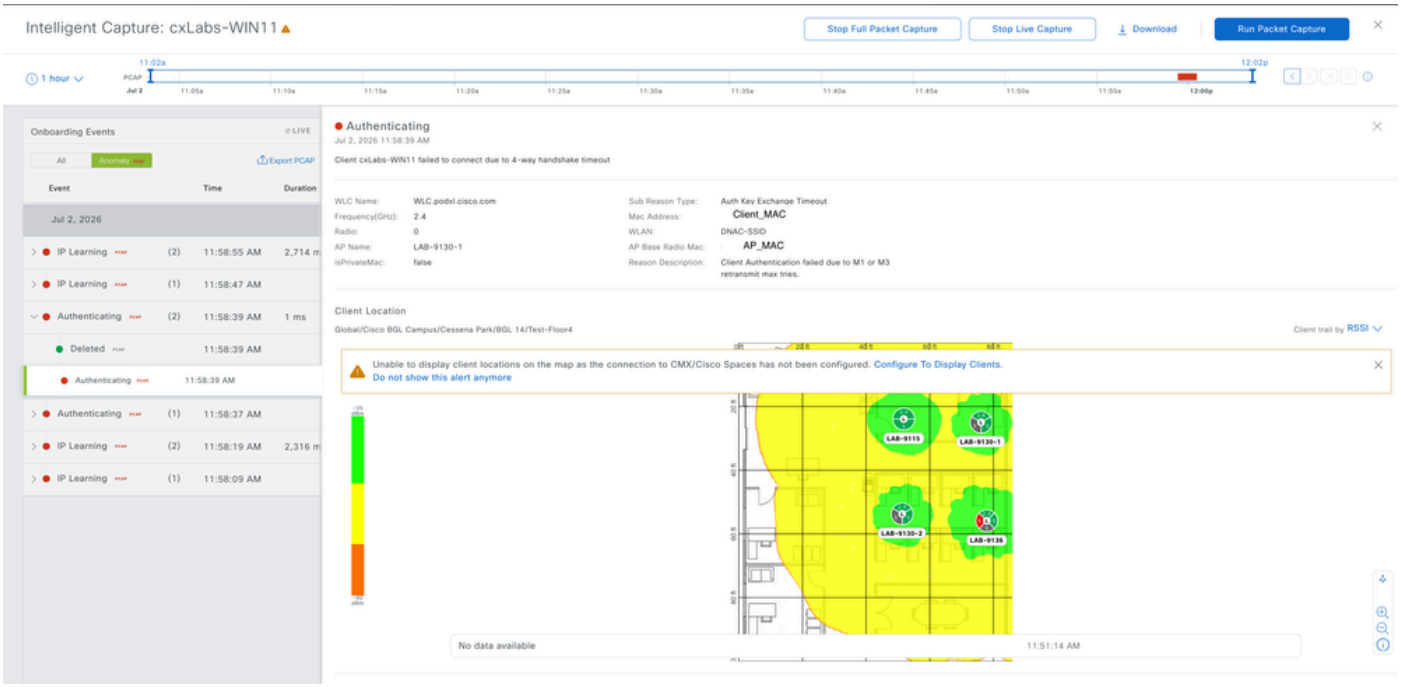


异常捕获配置预览

启用后，它会持续收集与AP关联的客户端的异常行为，并且可以在特定客户端ID的智能捕获（入网和完整）中查看这些行为。



客户端的异常捕获视图



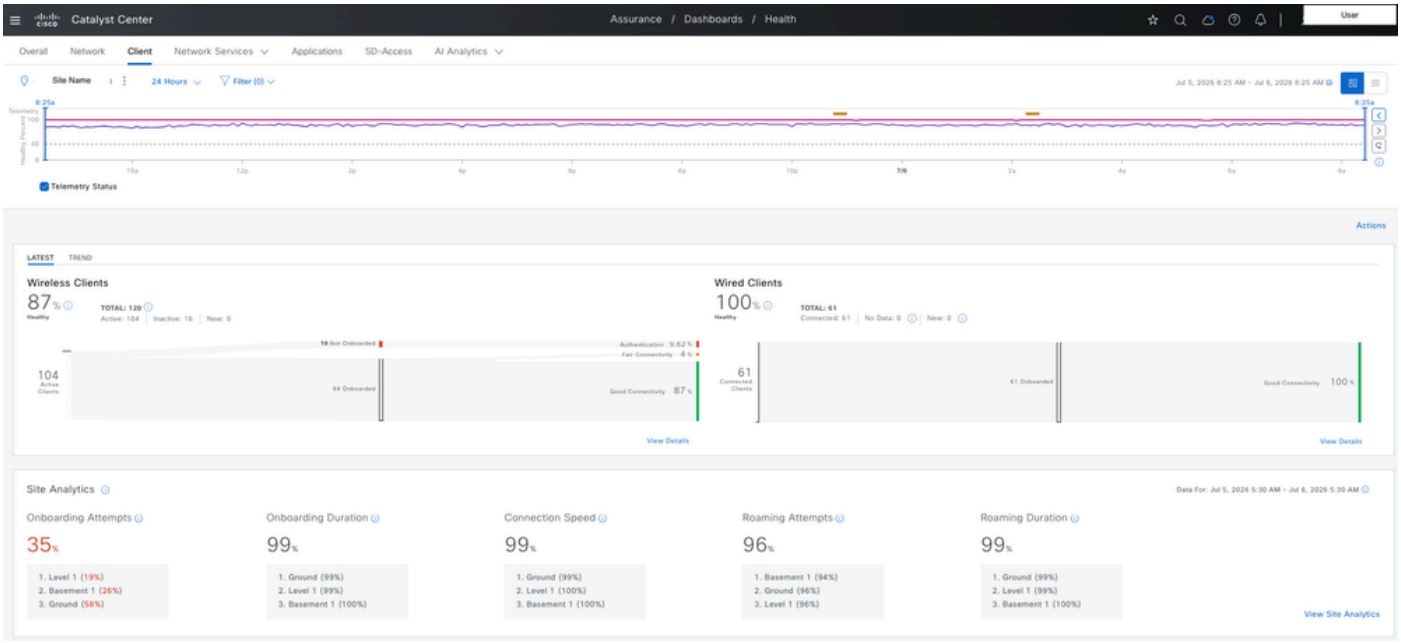
客户端的异常捕获详细信息

利用此功能，我们可以通过自动检测和标记已启用的AP的这些事件，对不规则或意外客户端行为（例如登录失败、身份验证问题或异常关联模式）进行故障排除。结合特定客户端ID的入网和完整数据包捕获，管理员可以跟踪导致异常事件的确切顺序，从而更轻松地查明客户端连接或性能问题反复出现的根本原因，而无需手动监控每个客户端会话。

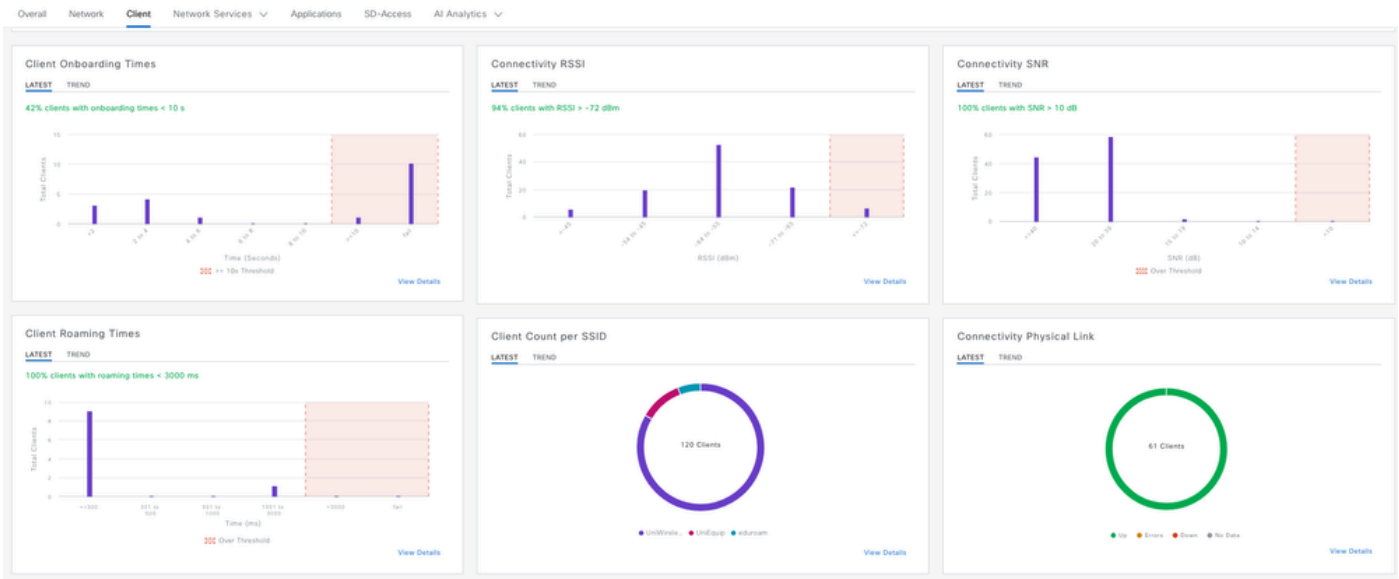
无线客户端连接问题

无线客户端问题（自注册故障、漫游丢弃、射频干扰或间歇连接）通常是暂时的，难以复制，因此传统的基于轮询的监控不足以对Cisco Catalyst Center进行故障排除，它通过连续、亚秒级遥测直接从接入点和无线控制器收集，并在设备360、客户端360和智能捕获工作流程之间关联，从而解决这一差距。这种遥测驱动的架构能够在发生故障时（从信道利用率和干扰到802.11自注册帧）重新构建准确的射频和协议级条件。

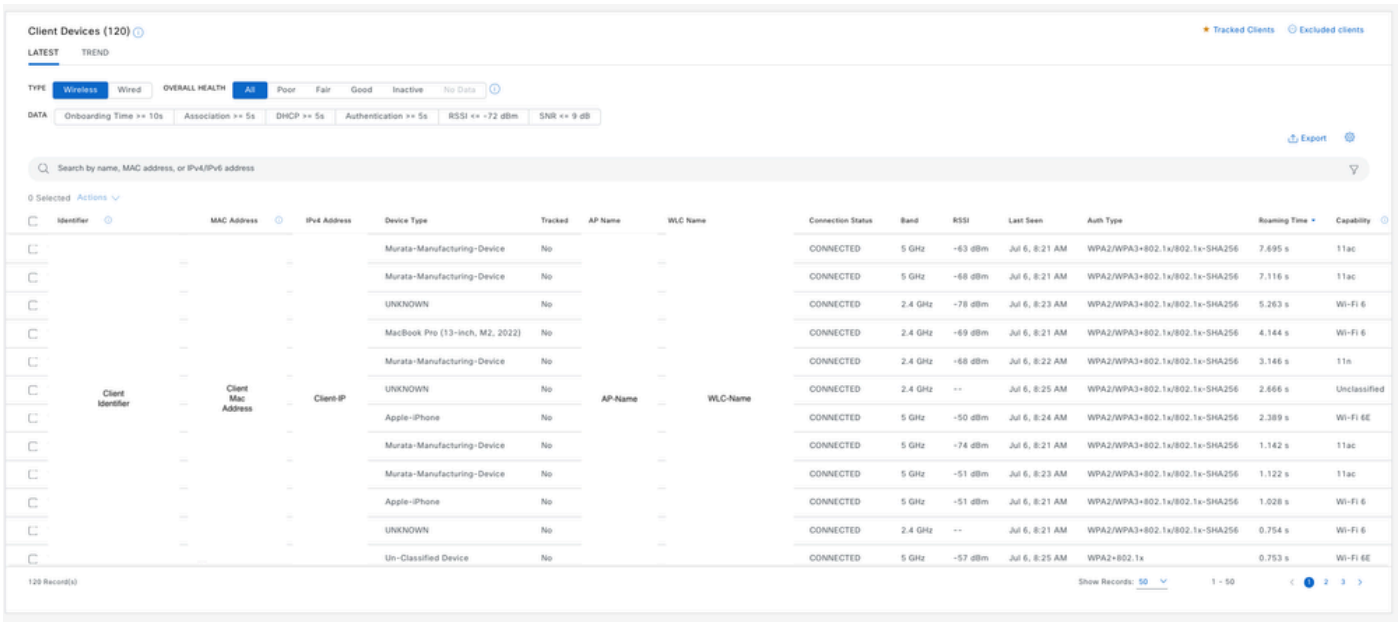
“客户端运行状况”(Client Health)部分提供所有站点的无线客户端统计信息的全面全局概述。这包括关键指标，例如自注册性能、RSSI、SNR、漫游活动、每SSID和每无线电分布、数据速率和物理连接状态。您可以按特定站点过滤此数据，并查看过去30天的历史趋势，从而获得网络范围的视角和站点级别的细分度。导航到保证>控制面板>运行状况>客户端



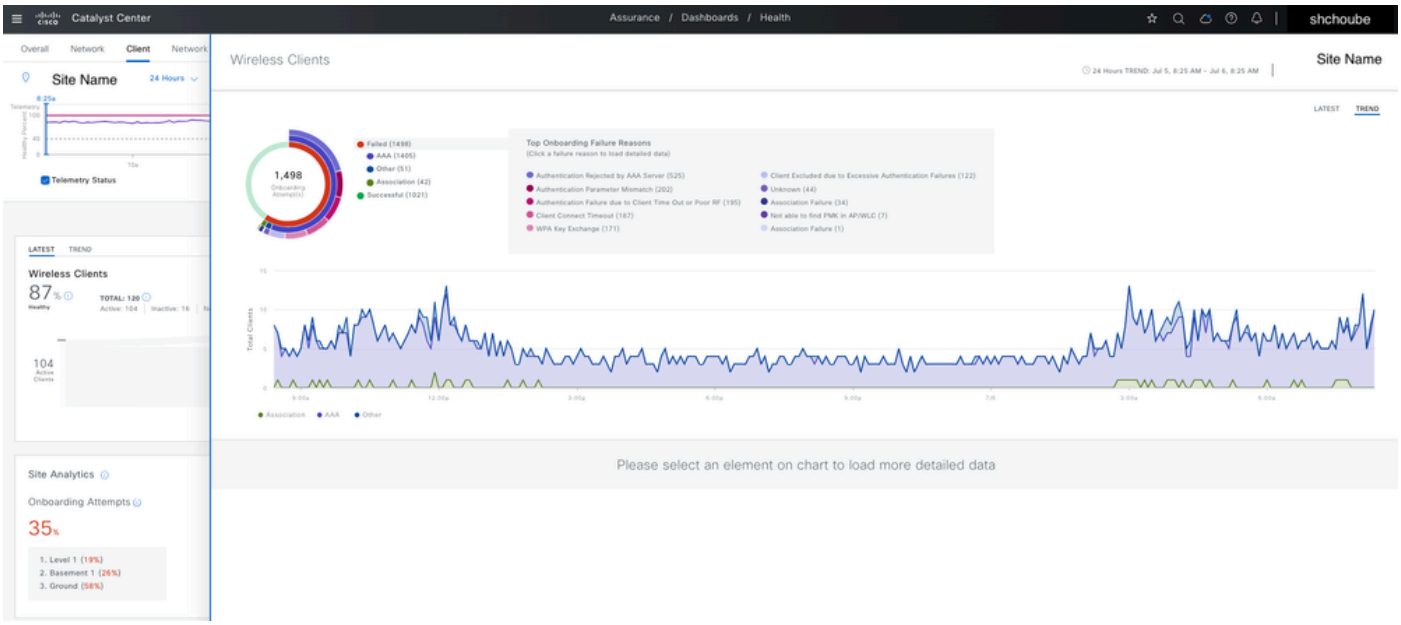
Catalyst Center上的无线客户端统计信息



Catalyst Center上的无线客户端统计信息

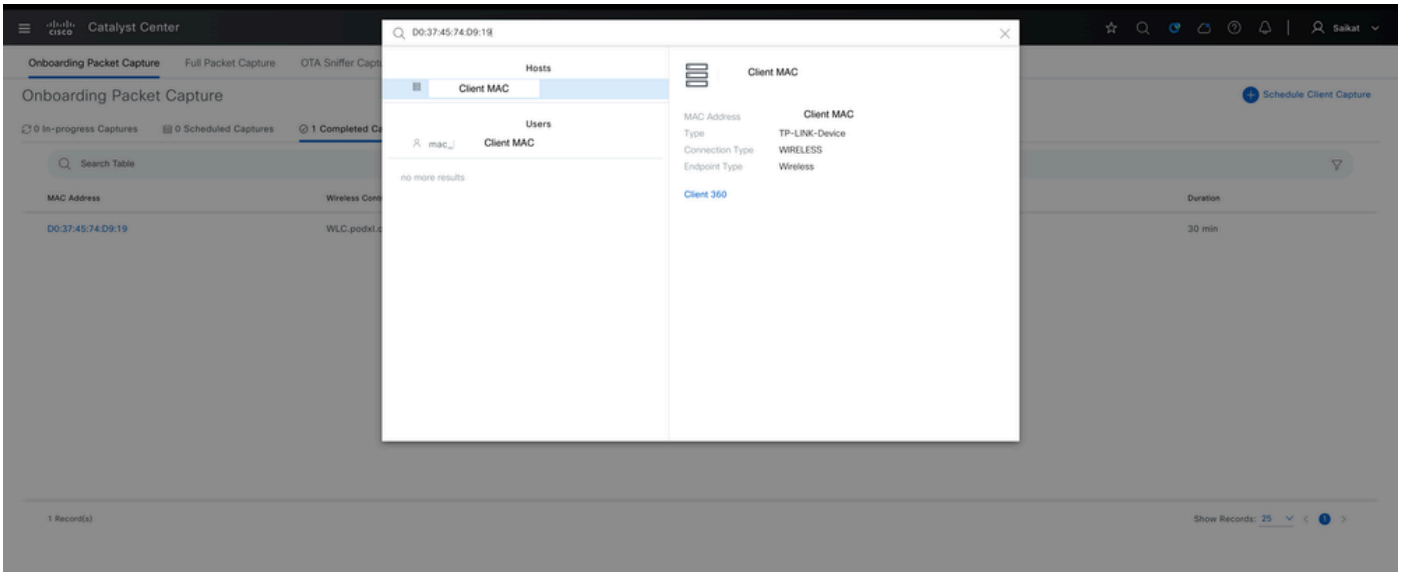


Catalyst Center上的无线客户端统计信息

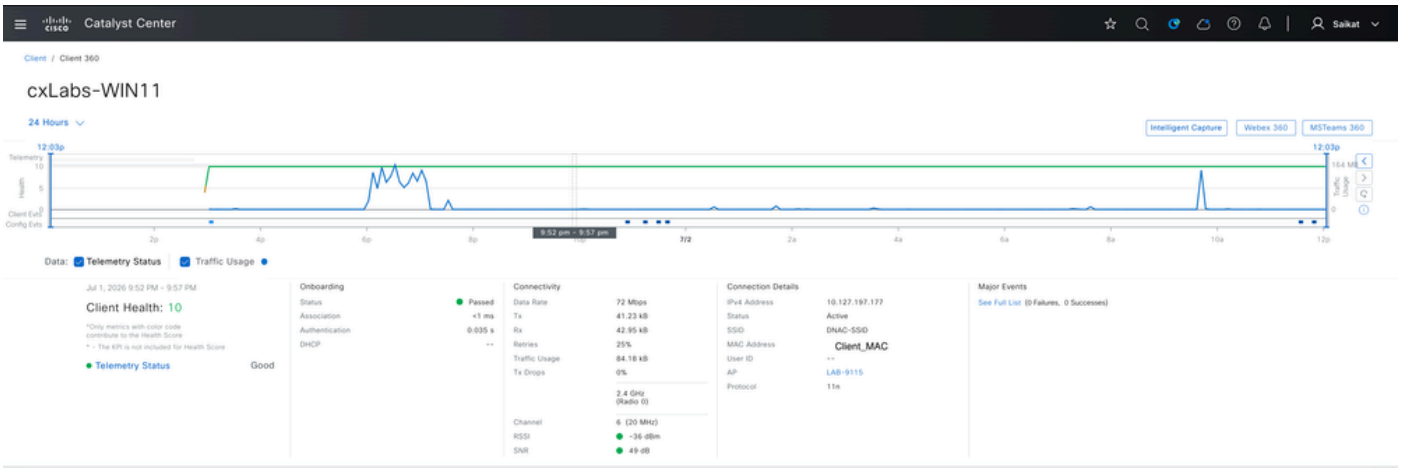


Catalyst Center上的无线客户端统计信息

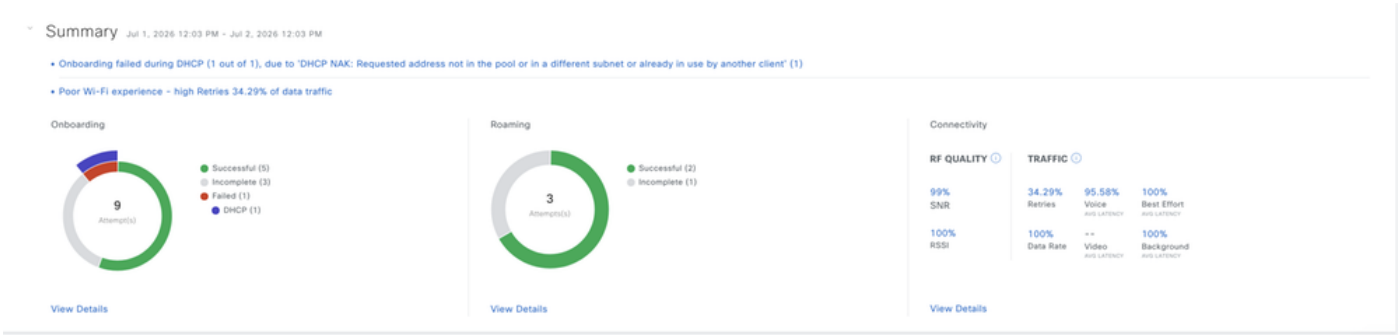
对于特定客户端的故障排除，可以使用客户端MAC地址进行搜索，这会使您进入客户端360视图。此页面提供特定于客户端的详细统计信息（包括自注册历史记录、连接事件、RF指标和会话详细信息），这些统计信息仅针对该单个客户端，从而可以对单个客户端问题进行精确的根本原因分析。



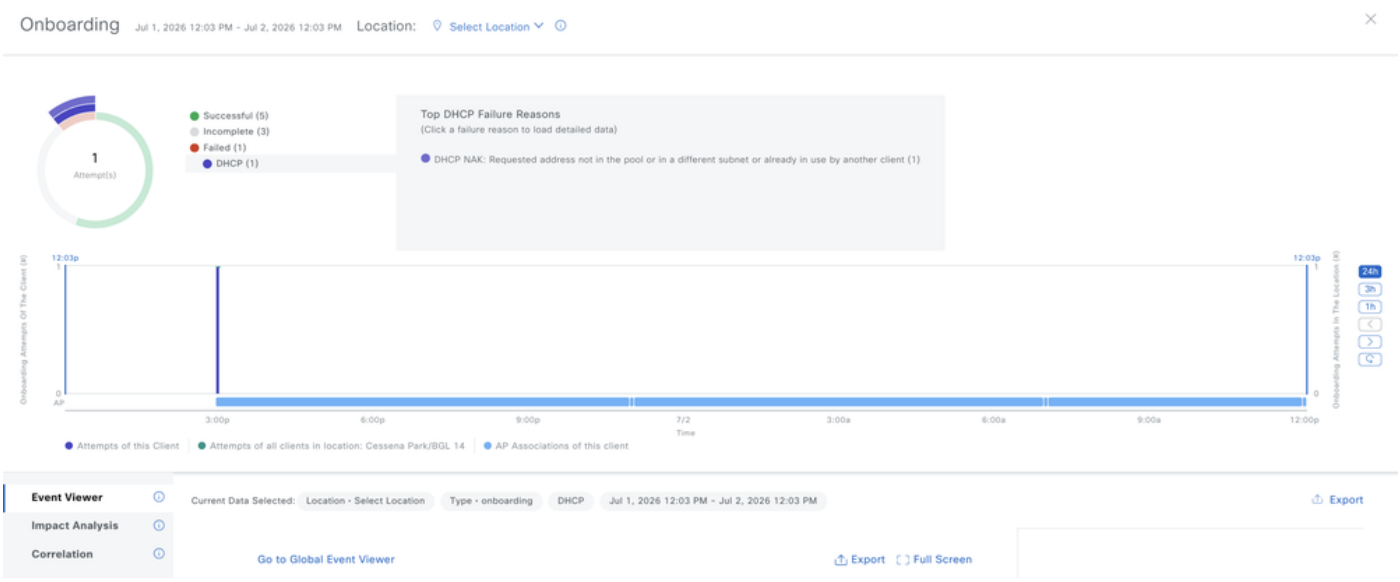
特定客户端Mac地址设备360



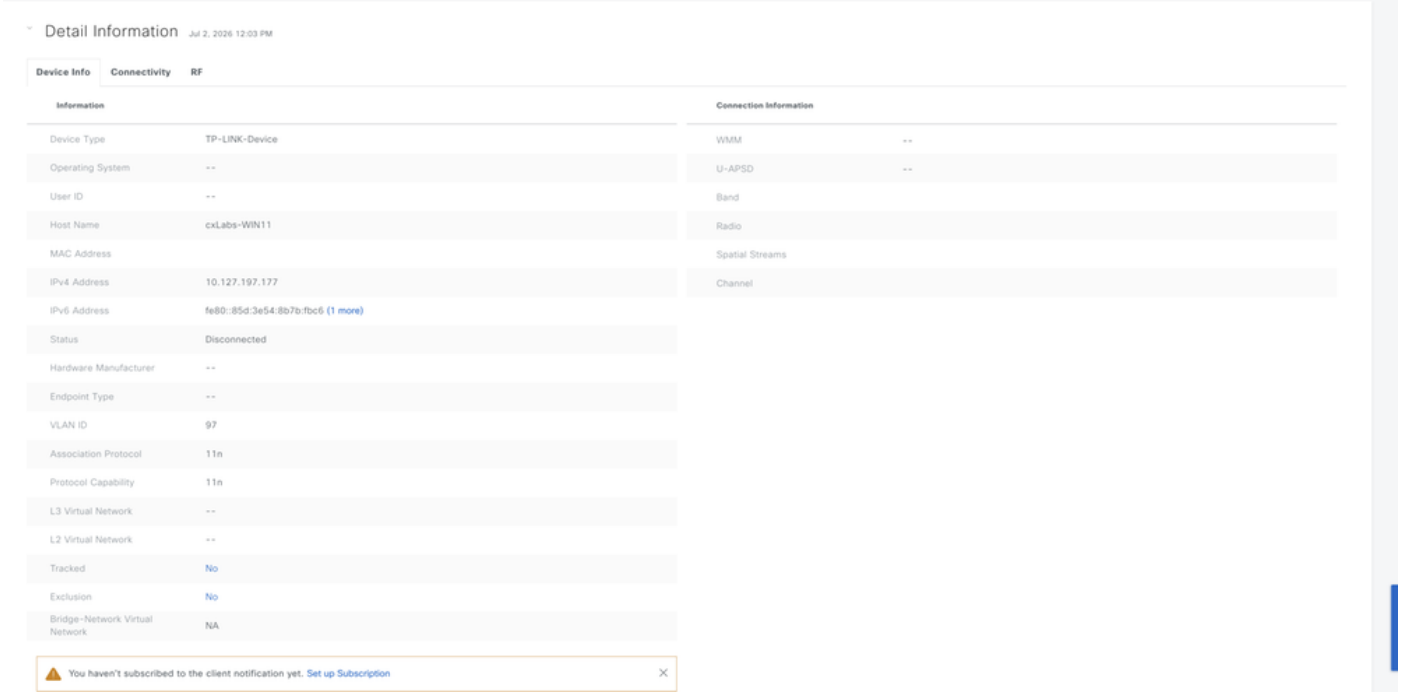
客户端的遥感勘测+运行状况



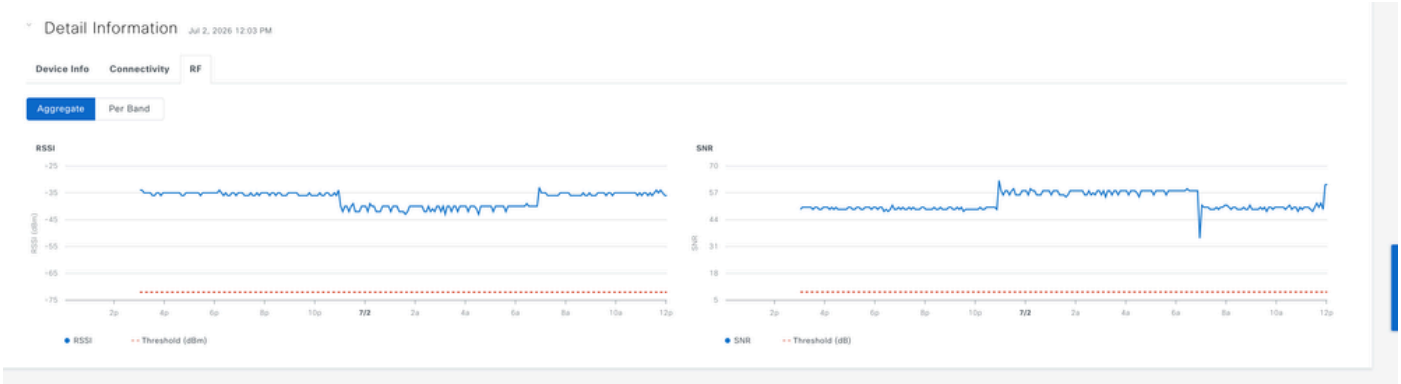
客户端总体摘要



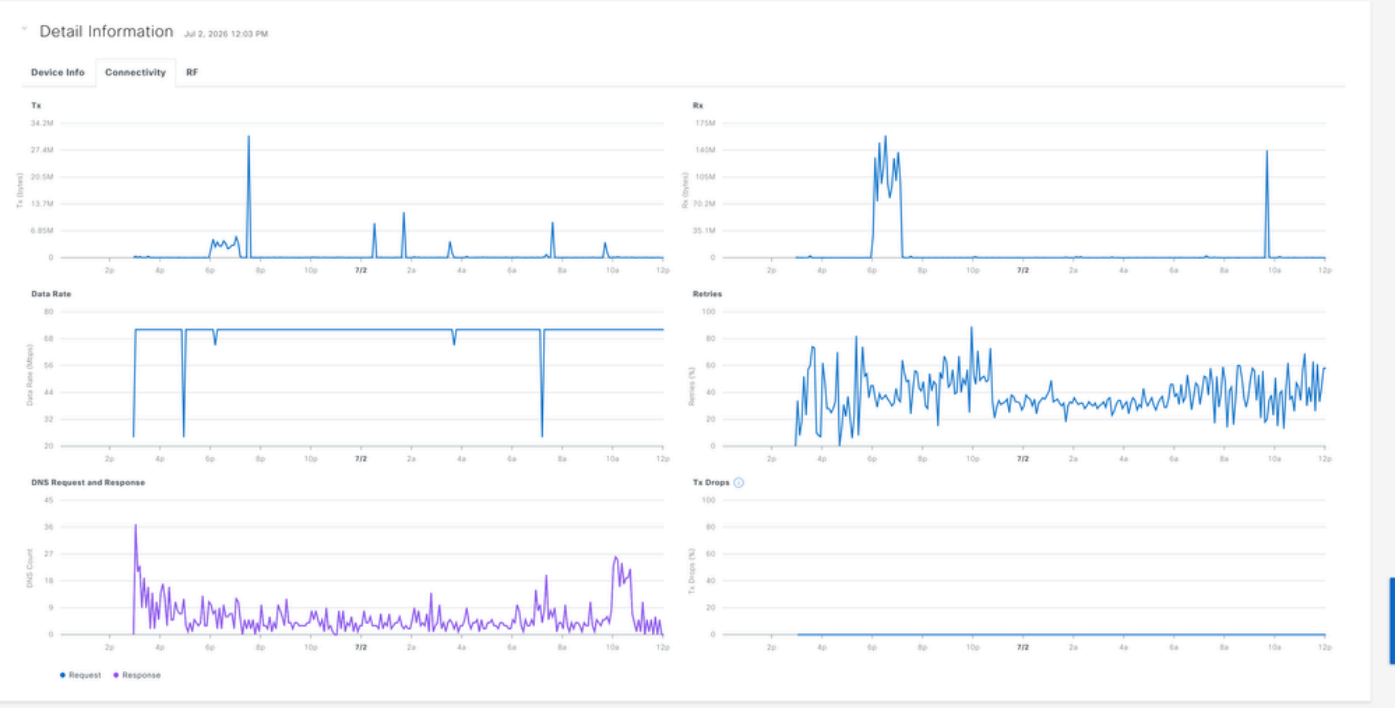
为客户端报告的事件详细信息



客户端设备详细信息



客户端的RF统计信息



客户端的连接统计信息

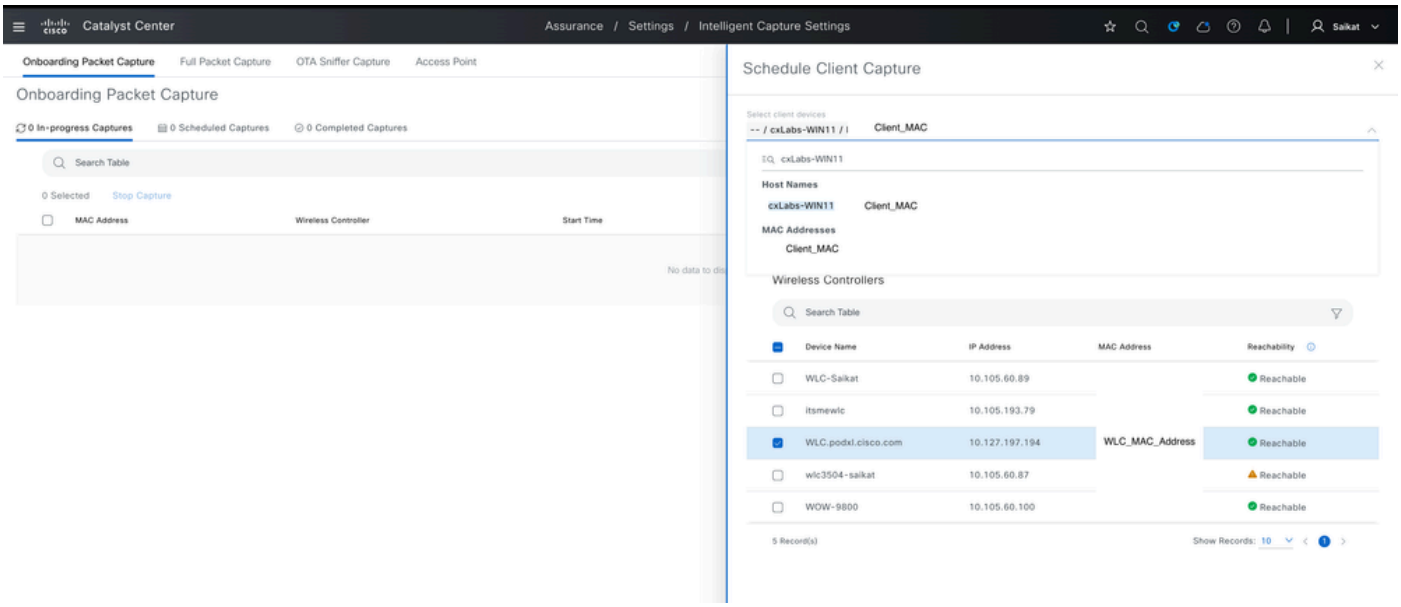
无线客户端智能捕获

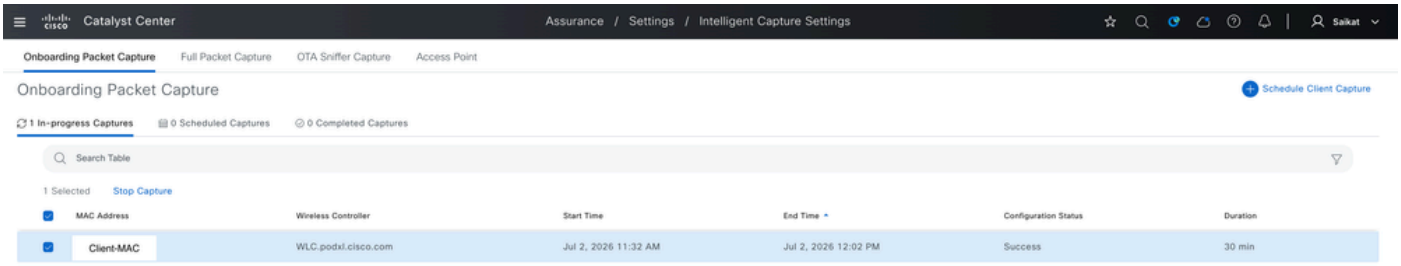
智能捕获(iCAP)通过直接从Catalyst Center捕获实际的数据包级数据，帮助解决无线客户端连接问题。它可以捕获802.11管理、DHCP和EAP帧，以查明连接尝试失败的位置、特定客户端的未加密数据和管理数据包，从而对自注册、可访问性和应用问题进行故障排除。您还可以安排智能捕获按照要求在以后运行。会话的默认持续时间是30分钟，最大可以设置为八小时。

自注册数据包捕获

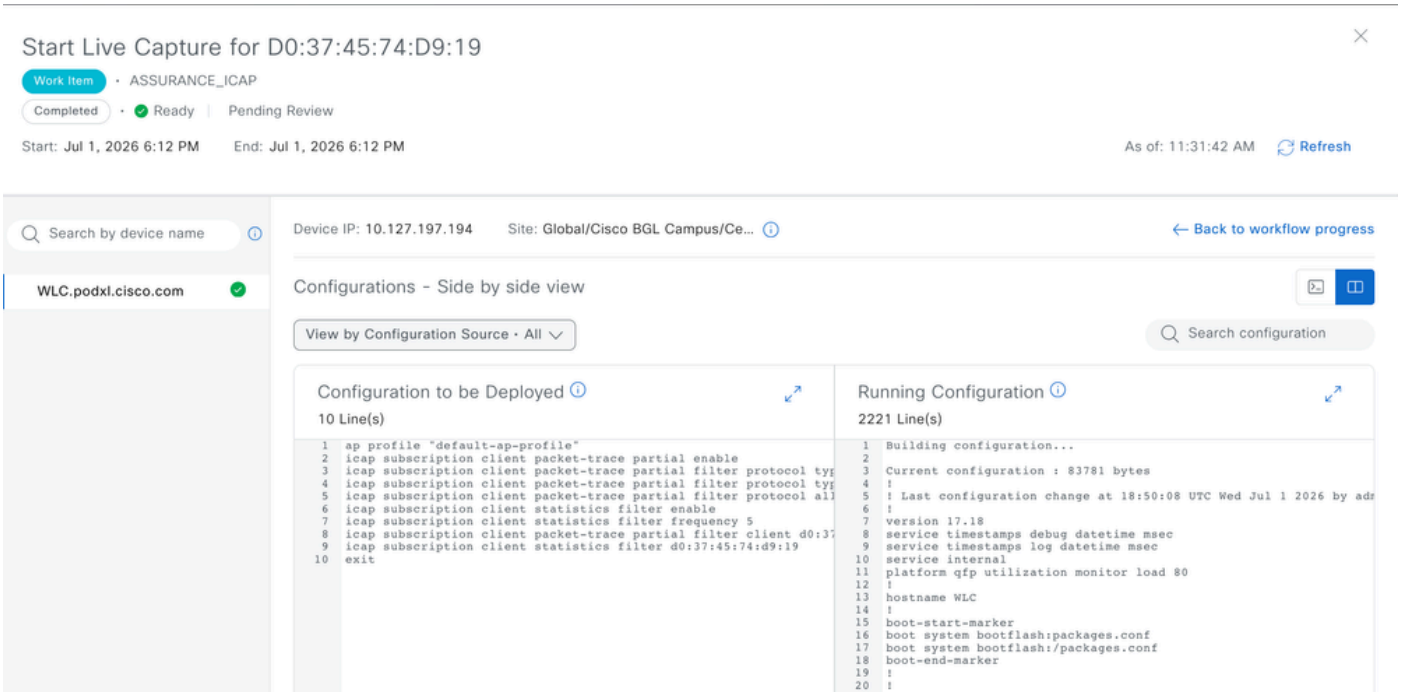
自注册数据包捕获记录客户端设备在尝试加入无线网络时交换的数据包的顺序，包括802.11管理帧（例如关联和身份验证请求）、DHCP数据包和802.1X身份验证期间使用的EAP数据包。此外，它还可以收集客户端射频统计信息，以便查看入网时的确切信号状况。这些捕获对于排除客户端无法连接的故障方案非常有用，有助于确定故障发生的准确阶段（无论是在关联、身份验证还是IP地址分配期间）。默认情况下，在最后一个客户端连接的无线控制器上启用自注册数据包捕获。您可以选择最多三个无线控制器以涵盖客户端漫游场景。

要启用Onboarding Packet capture，请导航到Assurance > Settings > Intelligent Capture Settings > Onboarding Capture > Schedule Client Capture（在右上角）> Search for Client Identifier(Mac address)





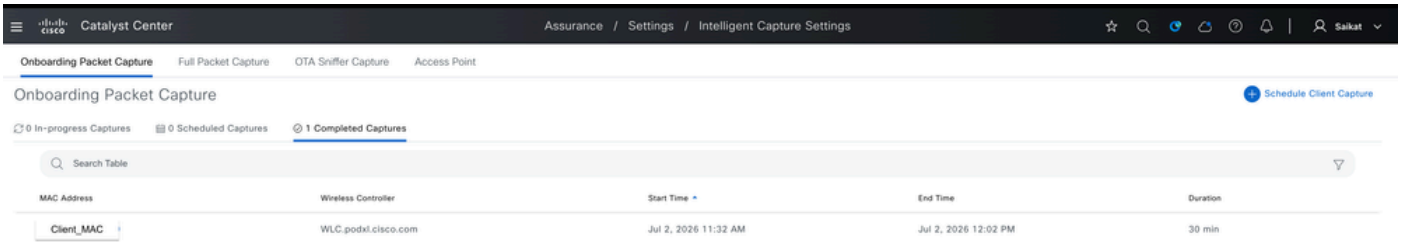
计划入职捕获



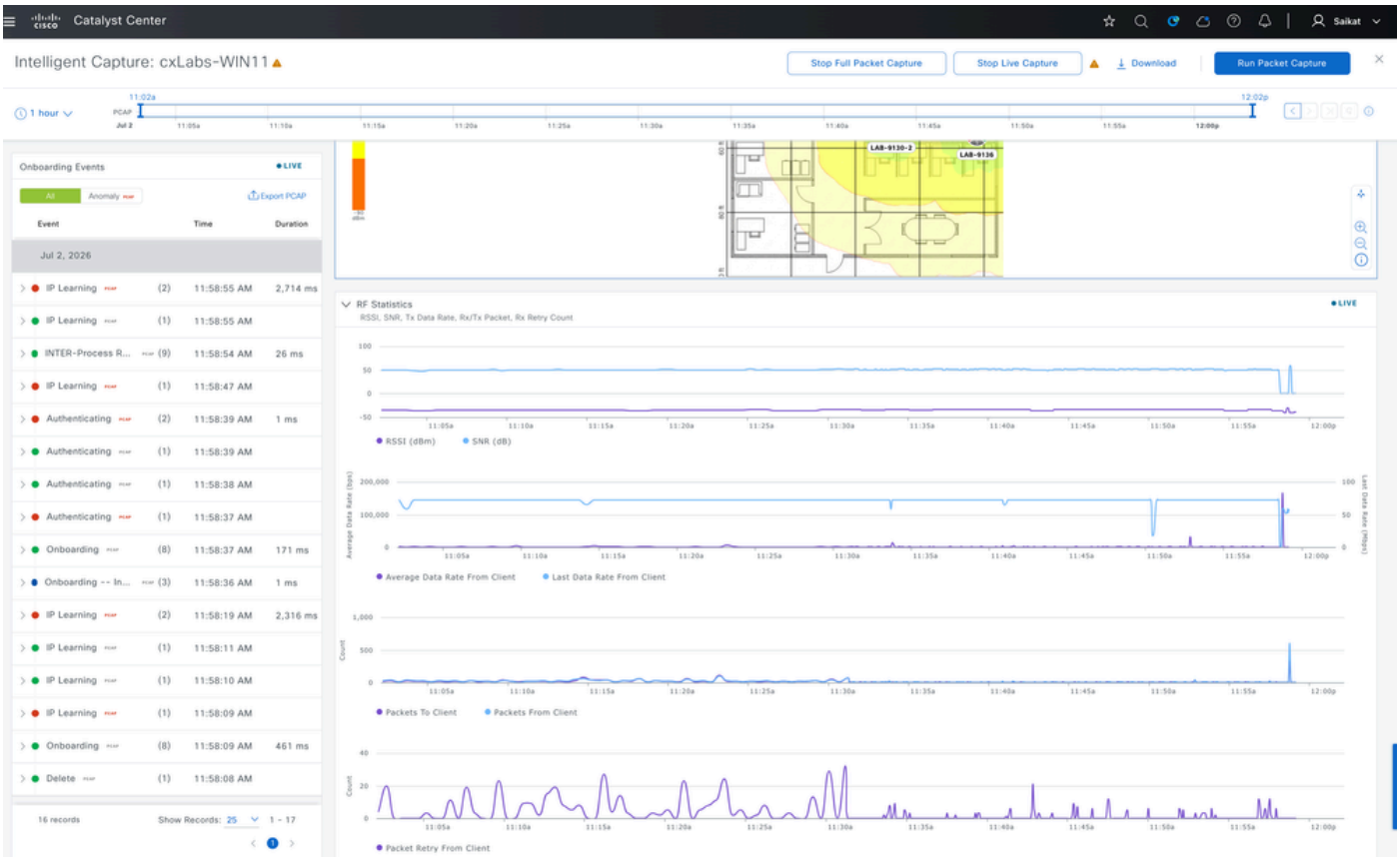
自注册捕获配置预览

在计划持续时间（从30分钟到8小时不等）过后，可以手动停止或自动禁用入职捕获功能。一旦停

止，捕获将显示在Completed Captures下，您可以在其中单击客户端MAC地址查看详细的捕获数据，并以PCAP格式导出文件以供进一步分析。



已完成的入职捕获

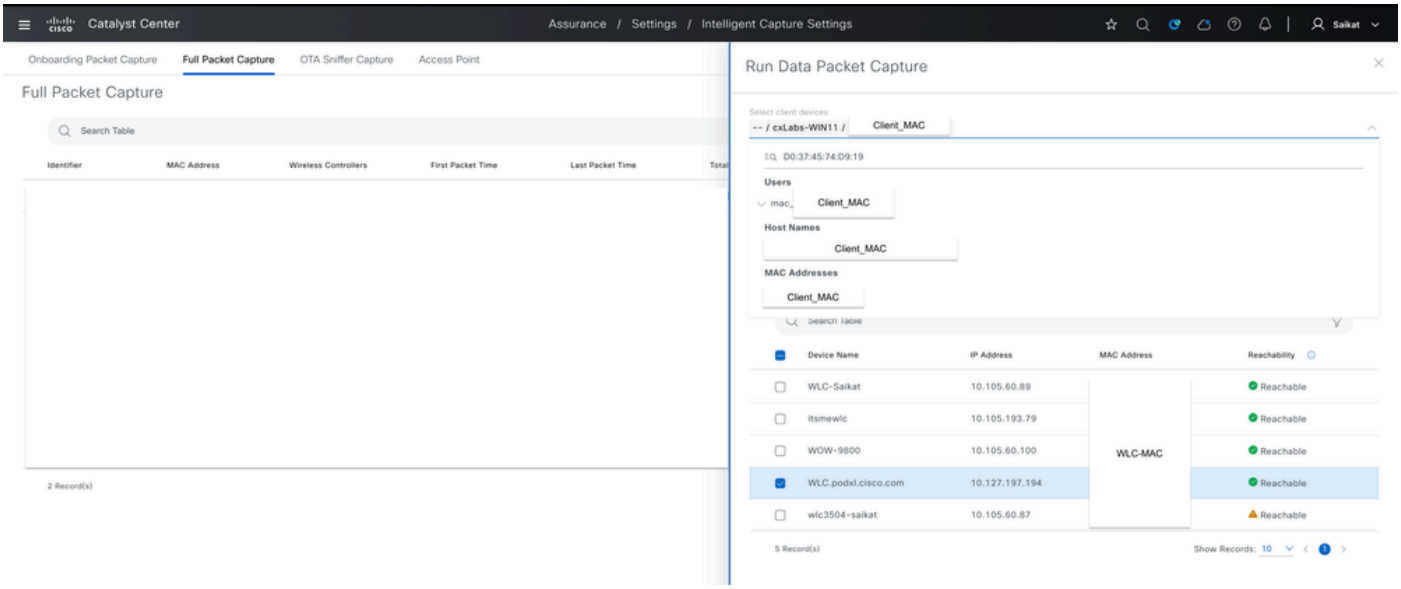


完全自注册捕获示例

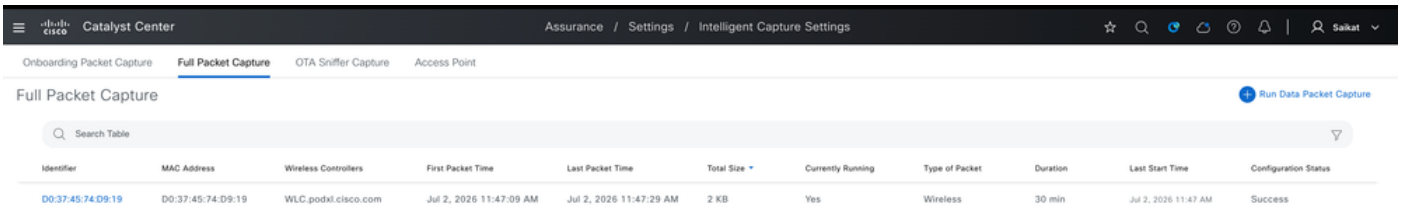
完整数据包捕获

完整数据包捕获会话可以捕获特定客户端的完整数据，从而提供深入的数据包级可视性，了解客户端的持续无线流量，允许我们详细检查数据和管理数据包，以排除超出标准RF统计信息所显示的访问问题、应用性能问题或其他连接异常故障。它可以捕获特定客户端最多1 GB的滚动数据，并持续保留最新数据（最大值不超过限制）。

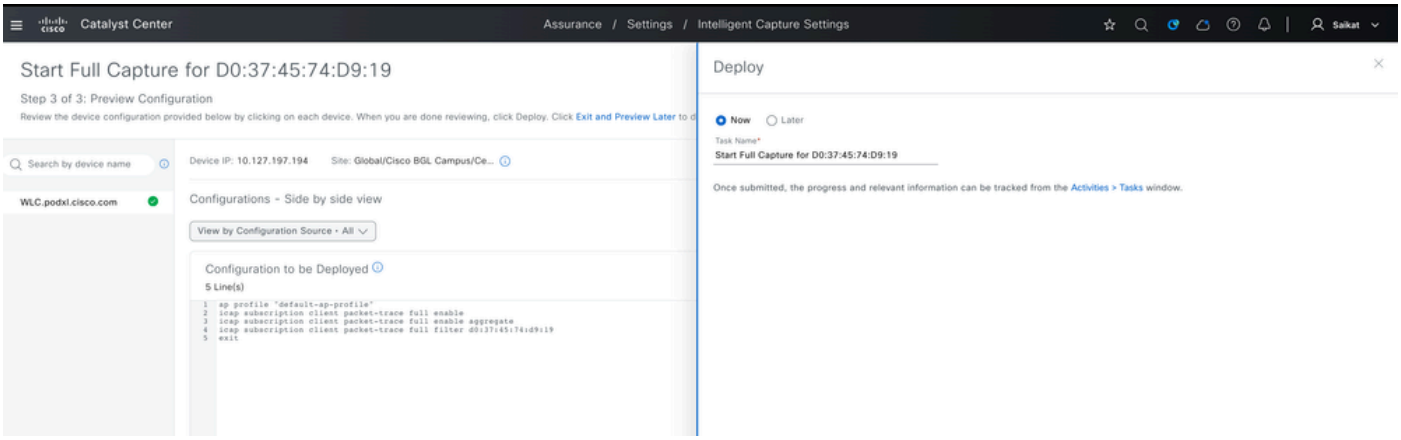
要启用Full Packet Capturenavigate to Assurance > Settings > Intelligent Capture Settings > Onboarding Capture > Run Data Capture（在右上角）> Search for Client Identifier(Mac address):



客户端的完整数据包捕获



客户端的预定完整数据包捕获



完整数据包捕获的配置预览

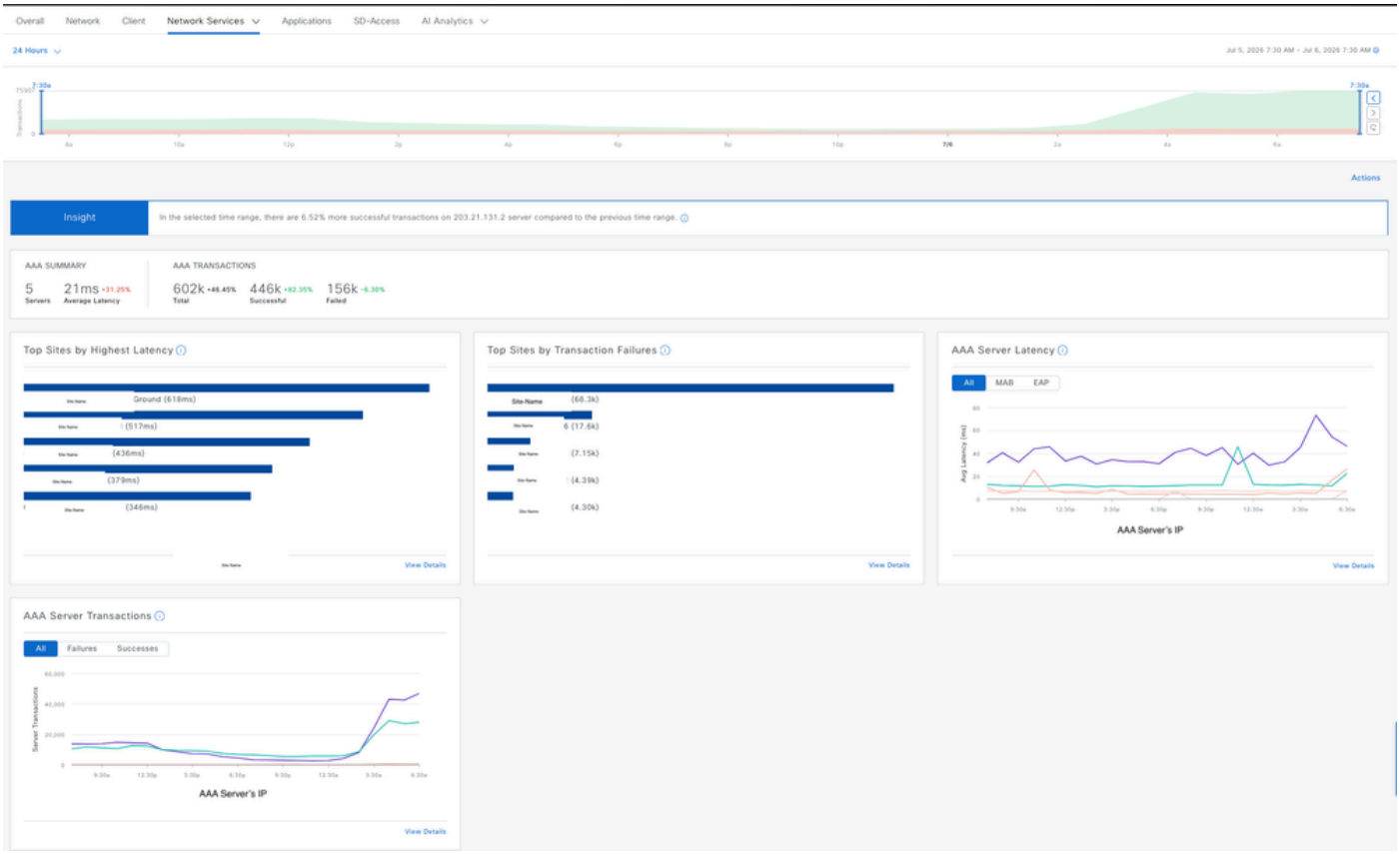
在计划的持续时间（从30分钟到8小时不等）过后，可以手动停止或自动禁用完整数据包捕获。一旦停止，捕获将显示在完成的捕获下，您可以在其中单击客户端MAC地址查看详细的捕获数据，然后以PCAP格式导出文件以供进一步分析。

为客户端收集的完全捕获示例

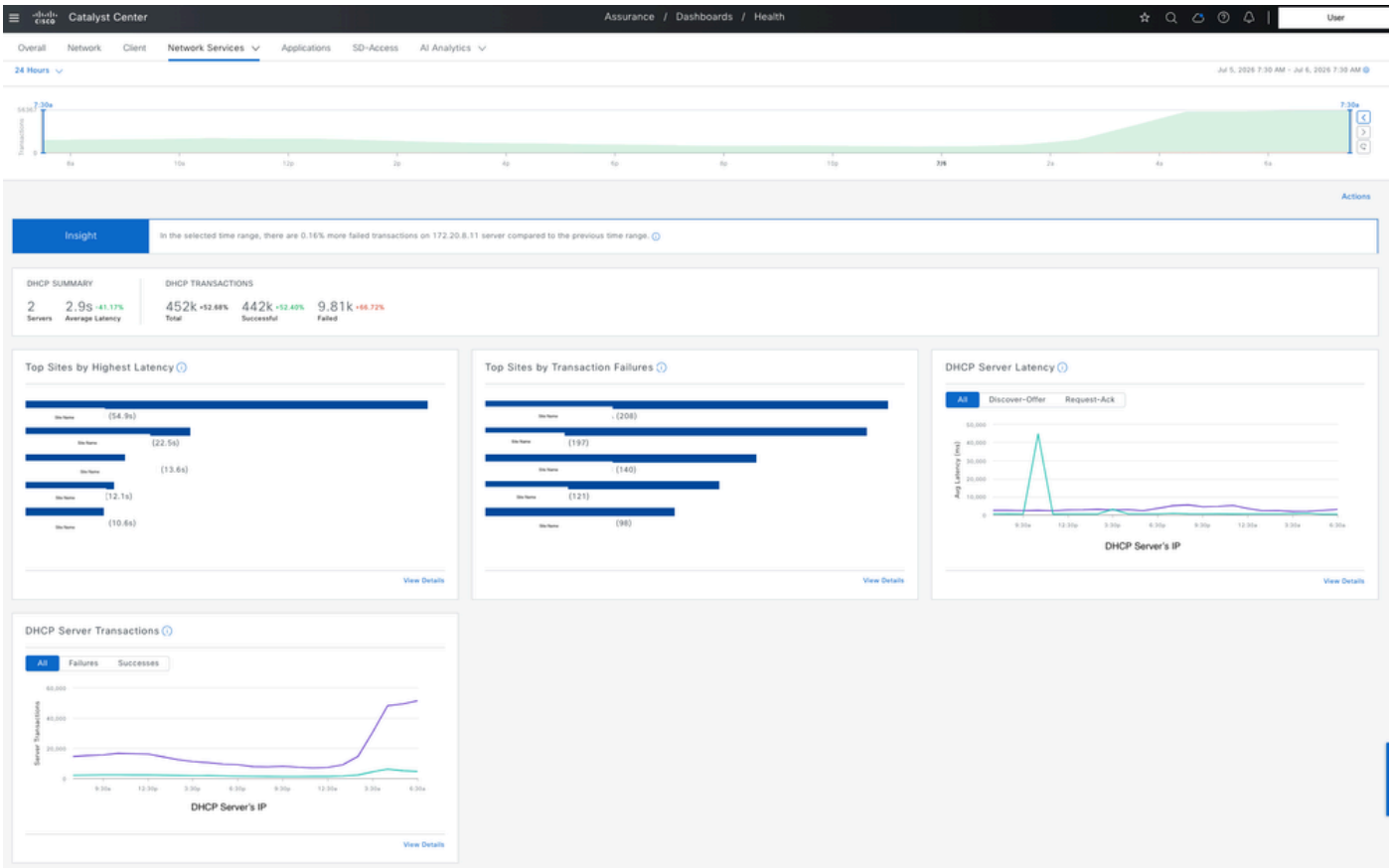
隔离网络服务问题(AAA、DHCP、DNS)

如果报告的症状指向特定网络服务而不是控制器本身（例如，客户端身份验证失败、未接收IP地址或名称解析失败），则“保证”下的Catalyst Center网络服务控制面板可让您查看WLC报告的这些事务。

导航到保证>控制面板>运行状况>网络服务> AAA/DHCP/DNS:



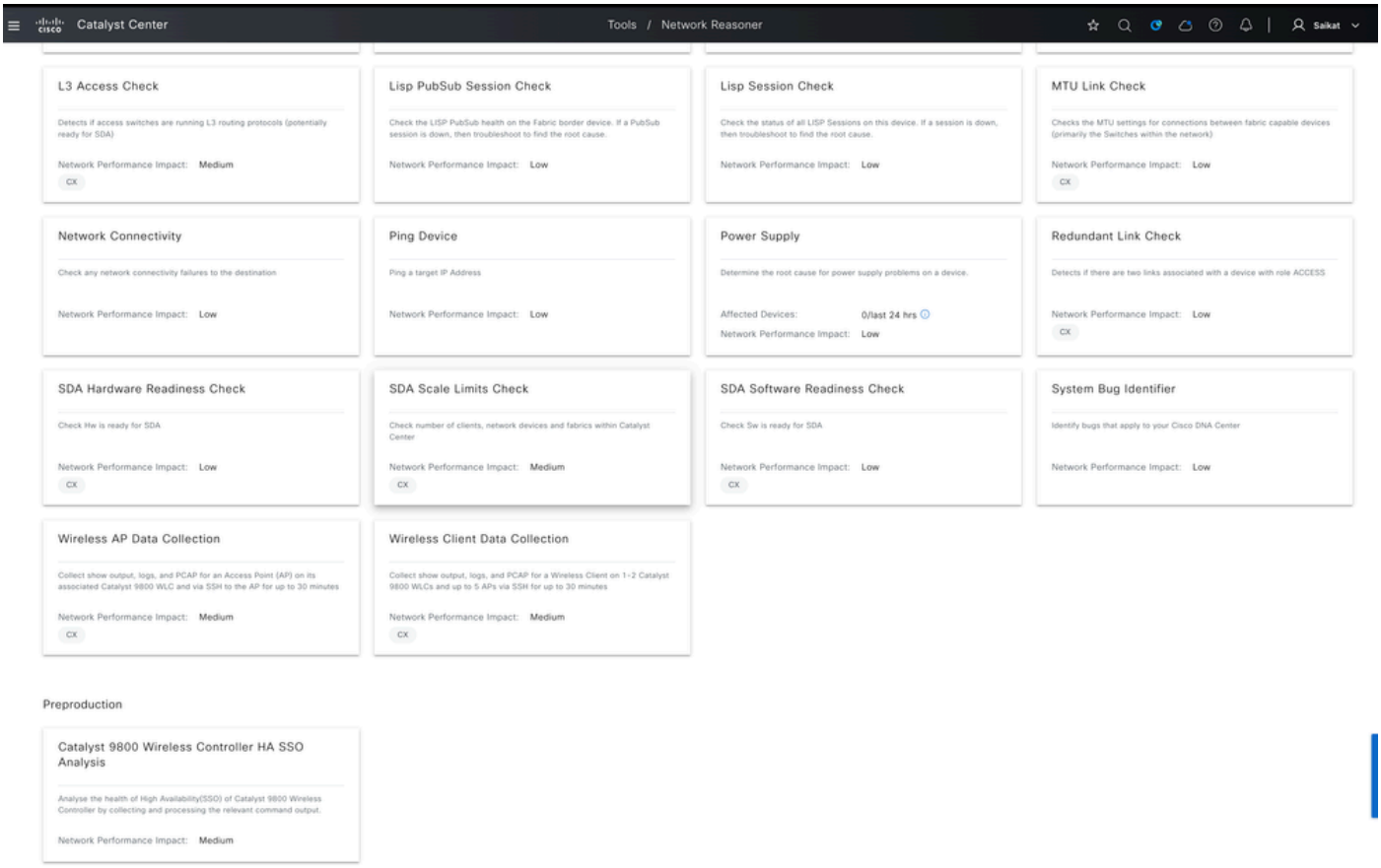
Catalyst Center上的无线客户端AAA统计信息



Catalyst Center上的无线客户端DHCP统计信息

网络设计师

Network Reasoner是Catalyst Center中的内置工具，可自动为您调查网络问题，您无需手动挖掘日志。您可以在Tools > Network Reasoner下找到它。每个故障排除选项（称为工作流）都会显示一个简短说明、过去24小时内受影响的设备数以及运行该操作会发生什么情况。它只能检测已添加到Catalyst Center for Assurance监控或通过Catalyst Center调配的设备上的问题。



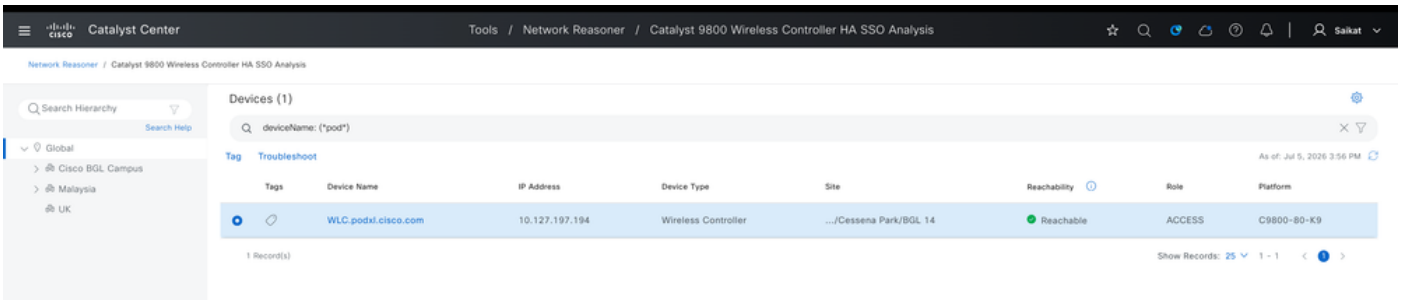
Network Reasoner上提供的各种网络故障排除选项

对于无线网络，有三个主要问题可以排除故障：

1.对于控制器问题(尤其是高可用性(HA)设置问题)，网络论证会检查以下内容：

- 控制器是否可达？
- HA是否设置正确？
- 主用和备用控制器是否同步？
- 它们之间的连接是否有效？

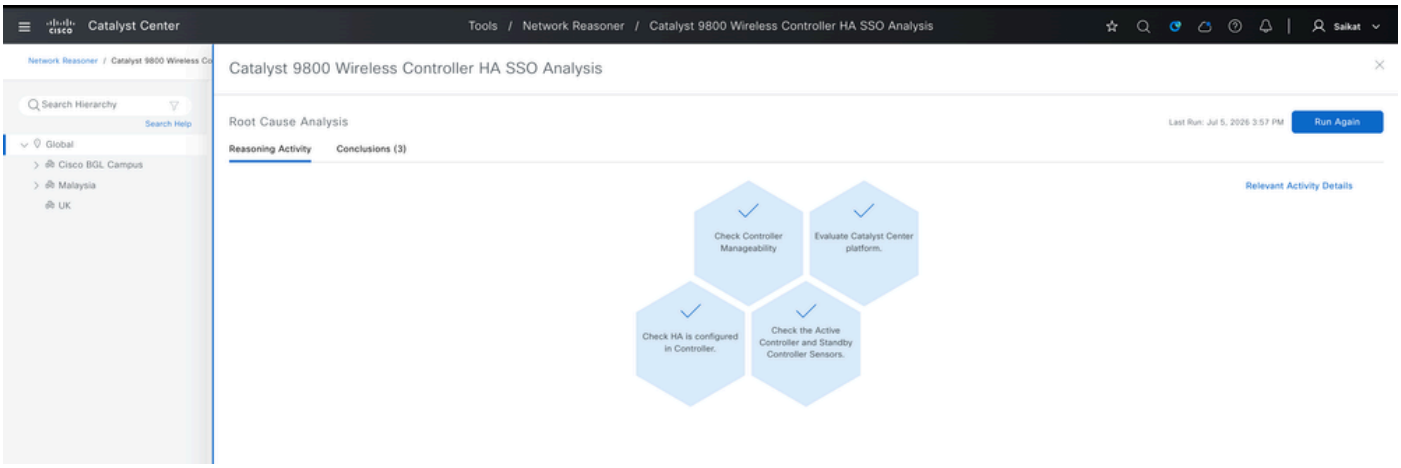
如果发现问题，它会确切地告诉您问题所在并建议如何解决。对于根本未发送任何监控数据的设备，还有单独的故障排除选项。



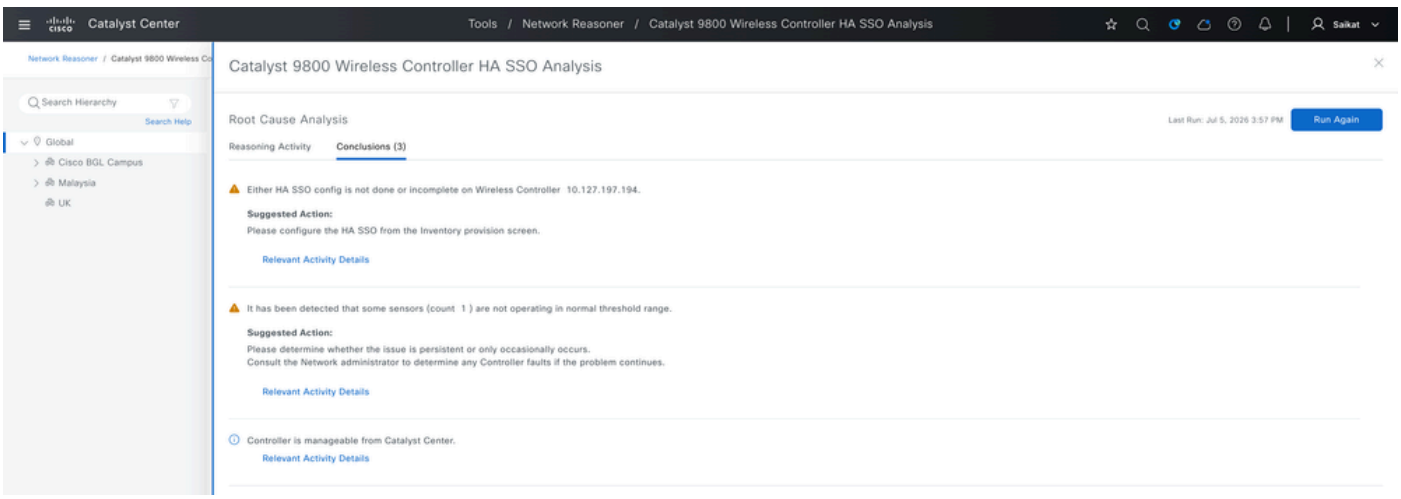
使用网络说明程序对HA进行故障排除

当您在9800 WLC上使用Network Reasoner启用HA SSO分析的故障排除功能时，它会执行多次检查并根据结果提供结论。如果发现HA SSO存在任何问题，也会建议纠正措施来解决这些问题。

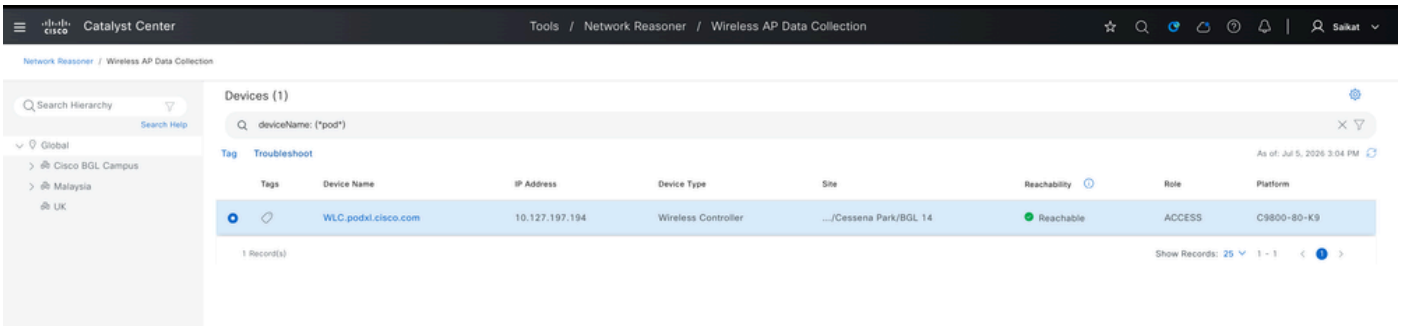
```
!! Task Workflow !!
Check Controller Manageability
Evaluate Catalyst Center platform.
Check HA is configured in Controller.
Check the Active Controller and Standby Controller Sensors.
```



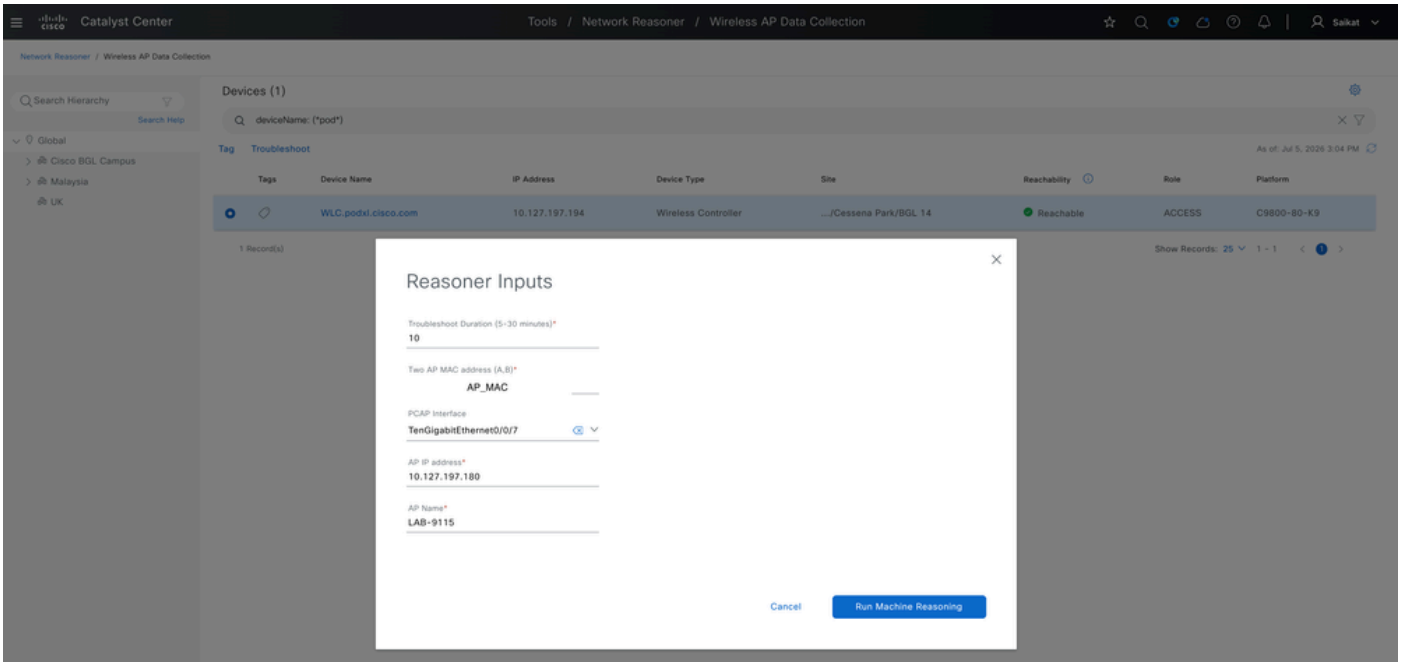
CATC为HA SSO分析执行的任务



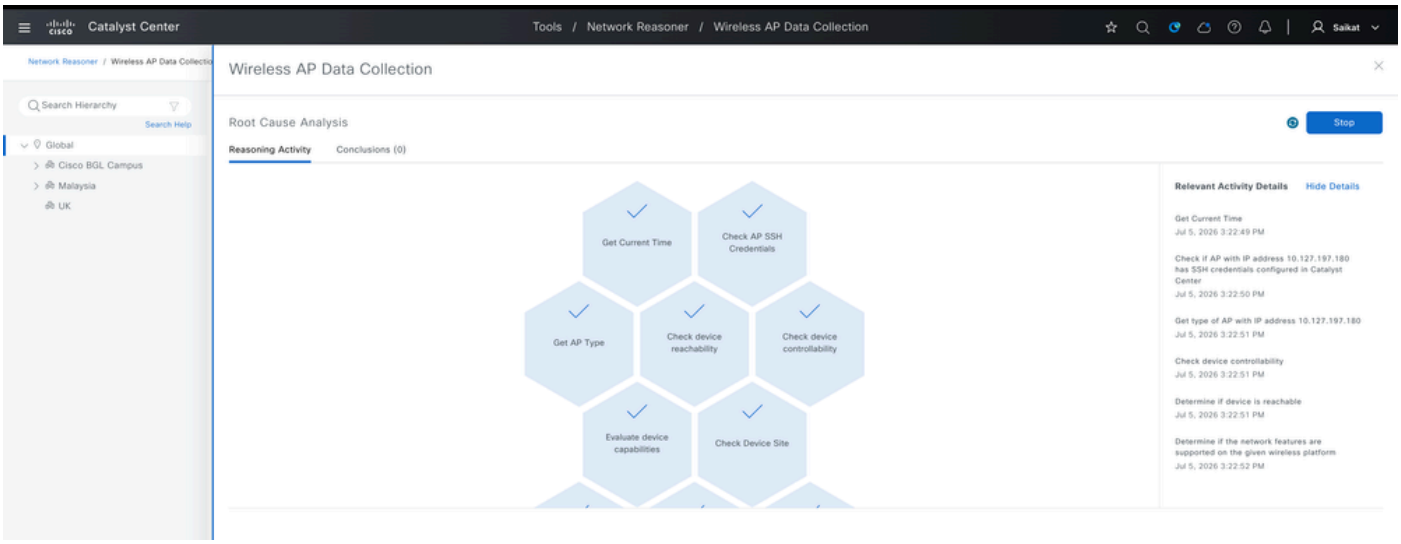
2.接入点 — 如果AP遇到问题，请选择管理它的控制器，然后输入AP的MAC地址，设置检查运行的持续时间。它支持从WLC和AP捕获日志和数据包，以实现更深入的可视性。以下是为AP启用Network Reasoner的工作流程以及相应的结果：



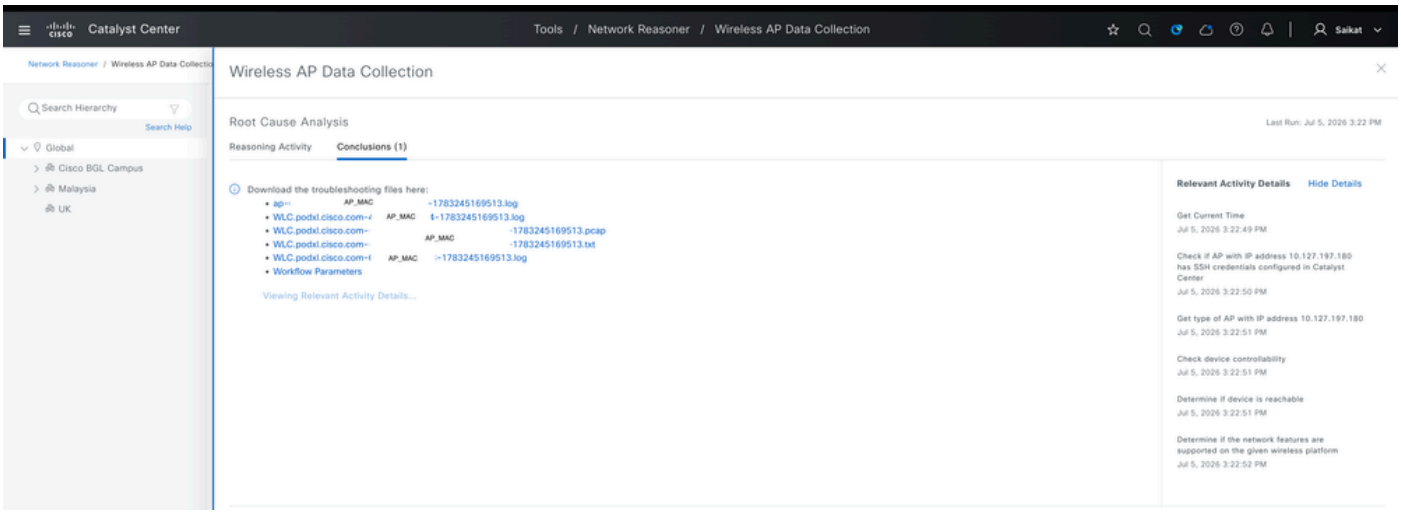
选择要进行故障排除的托管AP AP WLC



提供AP详细信息以进行故障排除



正在运行以排除AP问题的任务



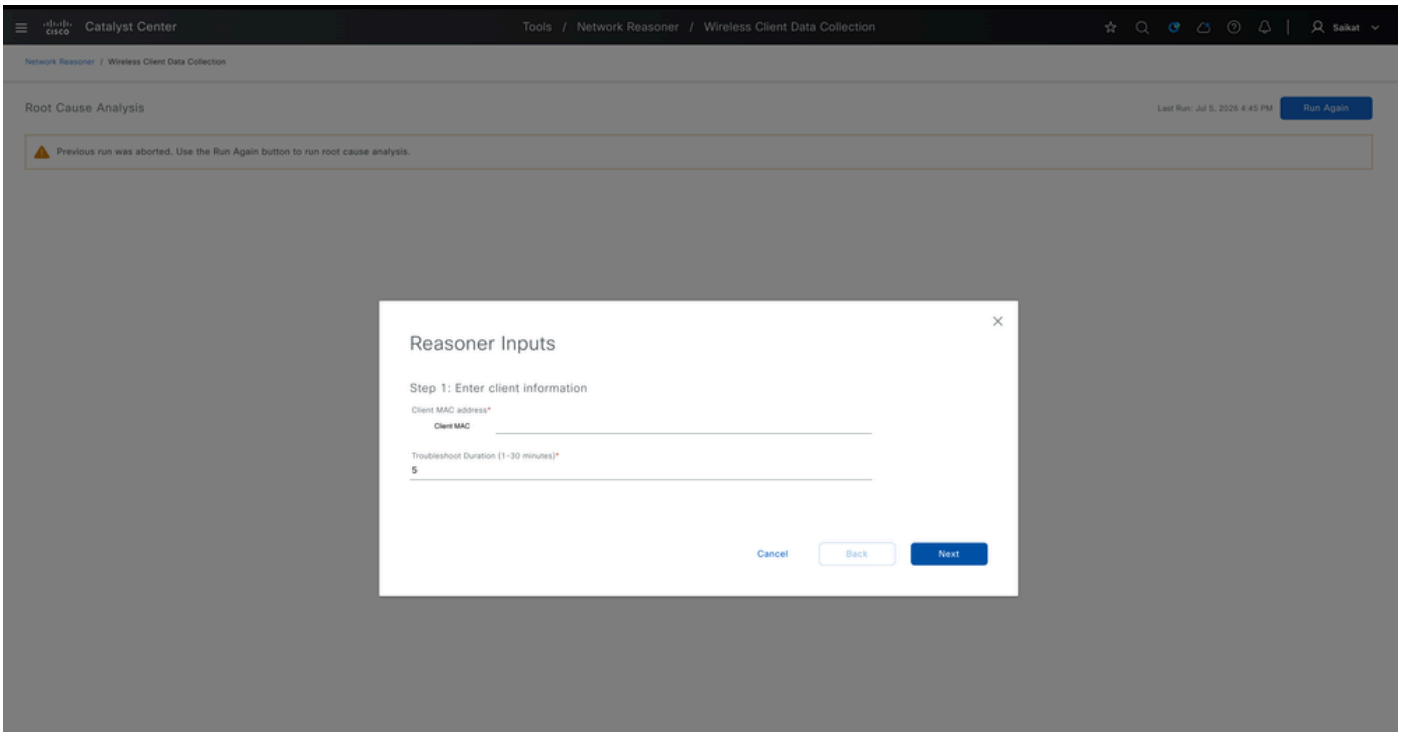
从WLC和AP收集的捕获以解决AP问题

```
!! 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
```

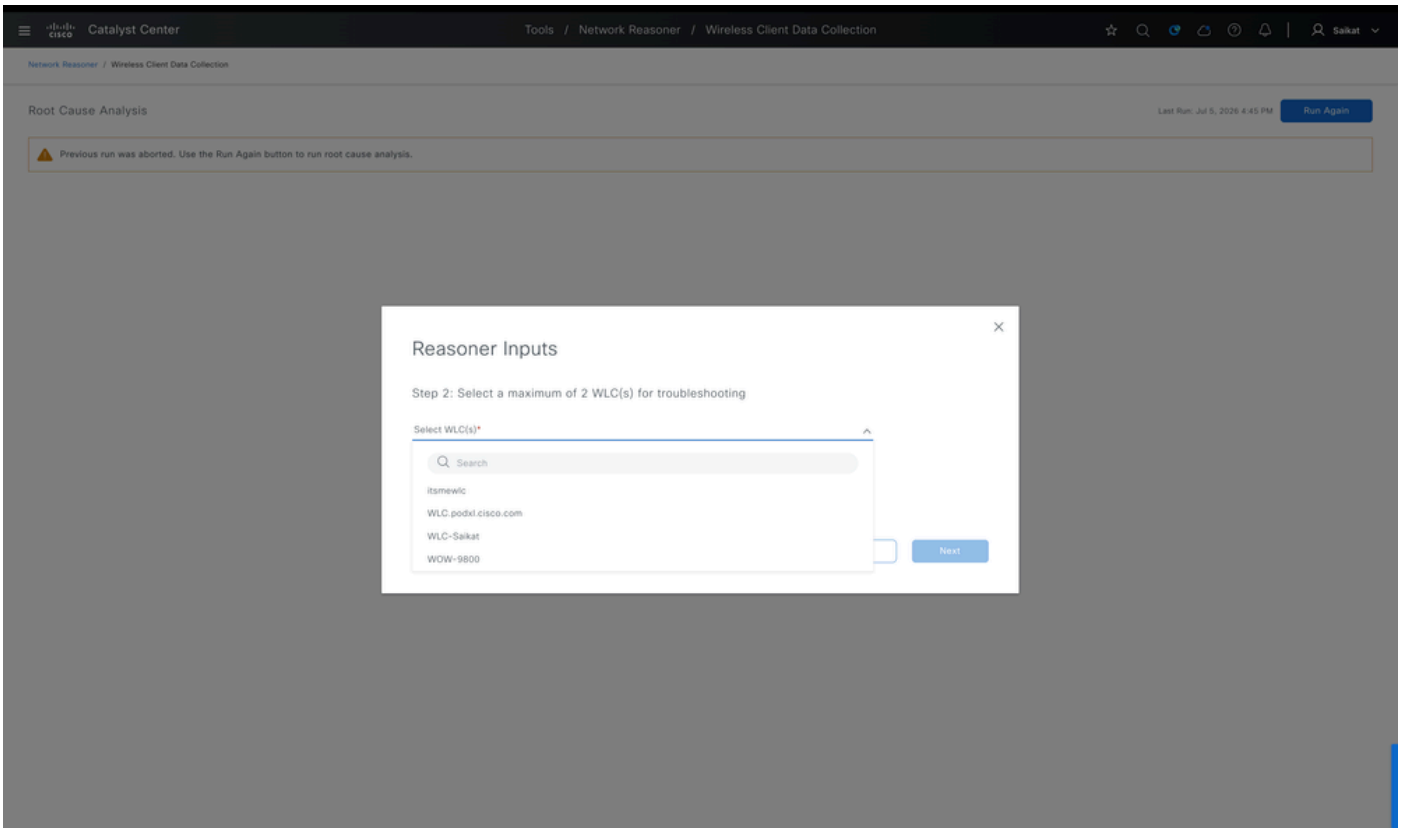
Jul 5, 2026 5:04:55 PM
Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127
Jul 5, 2026 5:04:57 PM
Start AP statistics collection on WLC with IP address 10.127.197.194 and wait for data collection for 3
Jul 5, 2026 5:04:58 PM
Start logging on COS AP 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
```

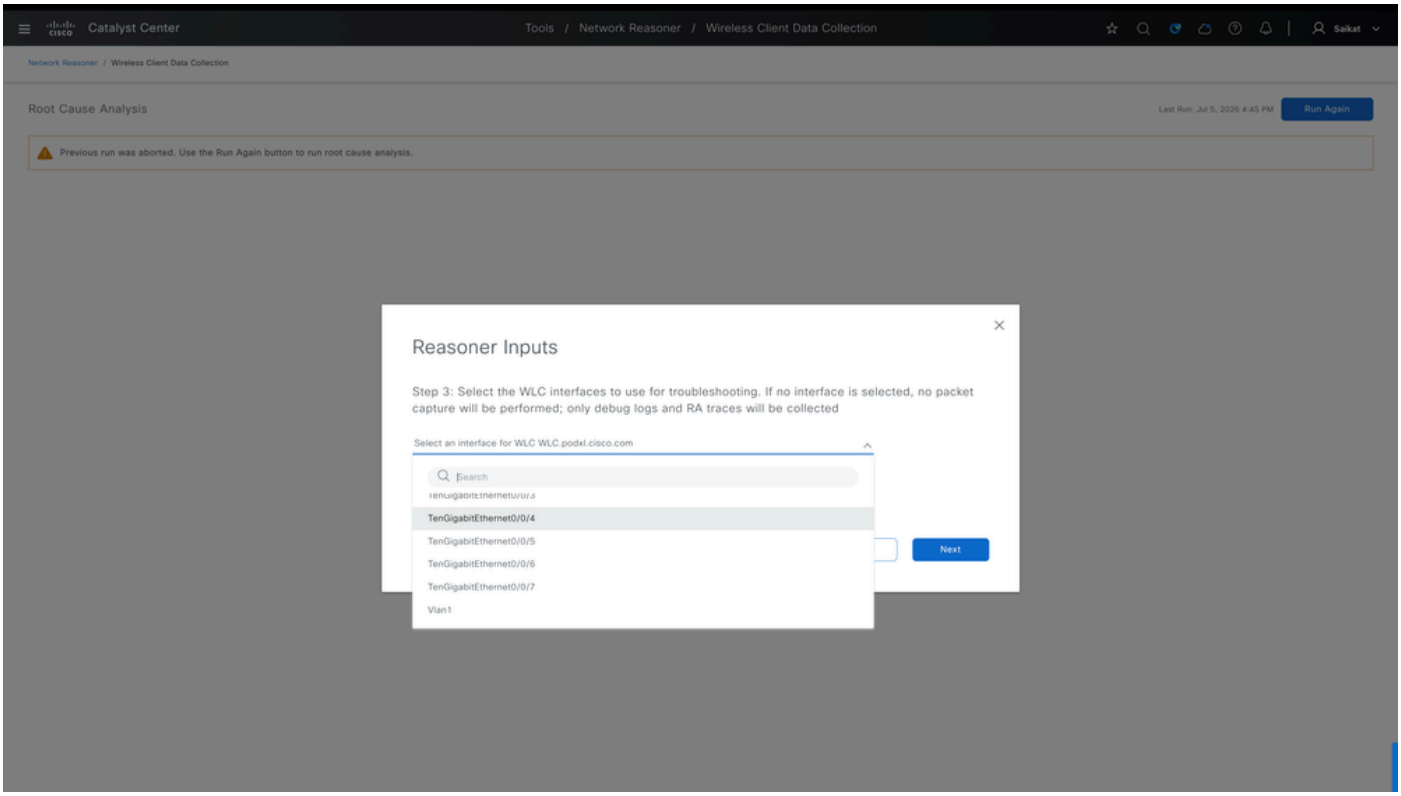
3.无线客户端 — 如果用户存在Wi-Fi问题，请选择用户所连接的无线控制器，输入其设备MAC地址，然后选择您希望该工具监控的时间。它支持统计日志、RA跟踪和数据包捕获，以查看交换的实际数据。下面是为无线客户端启用Network Reasoner的工作流程以及相应的结果：



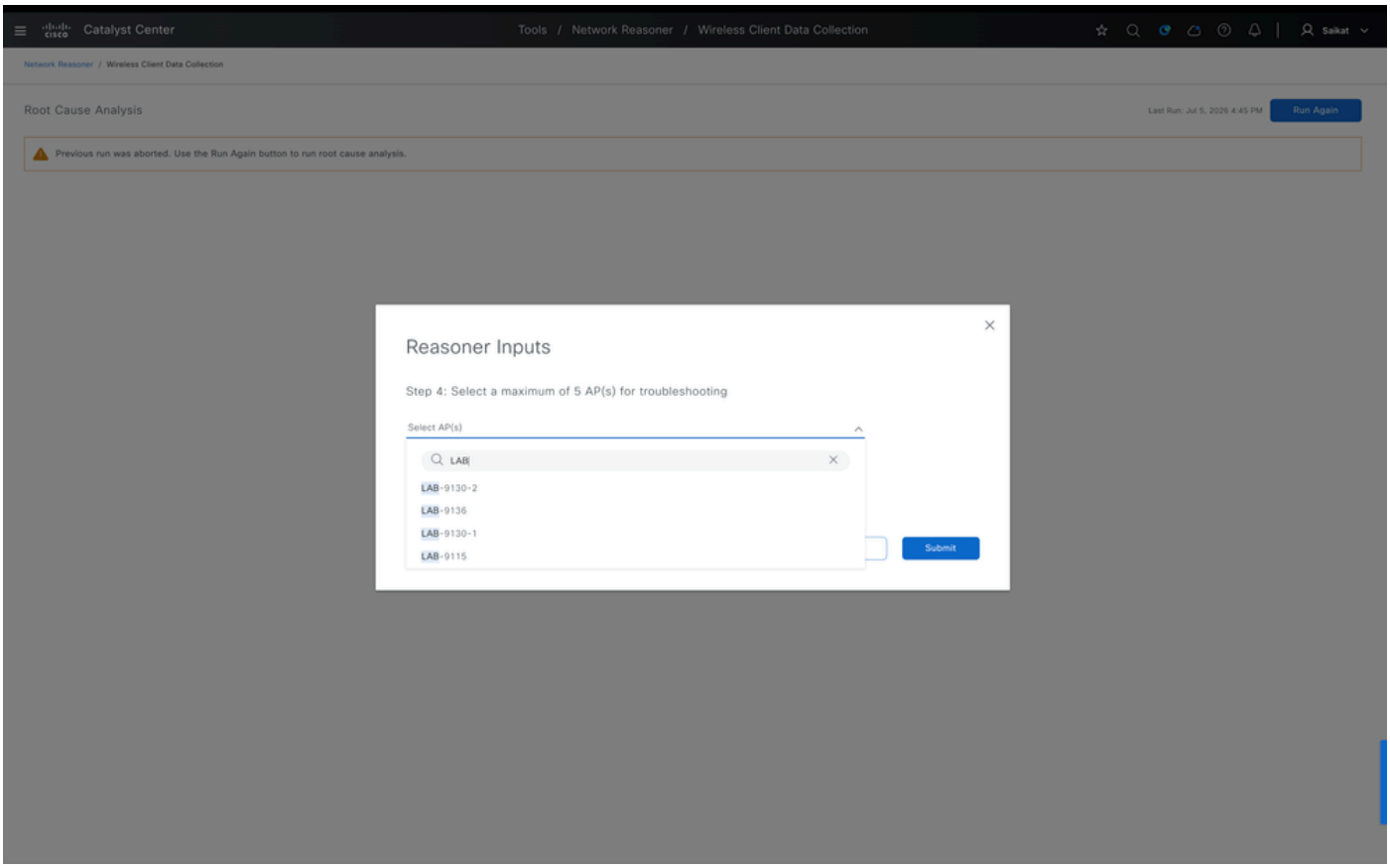
提供客户端详细信息以进行故障排除



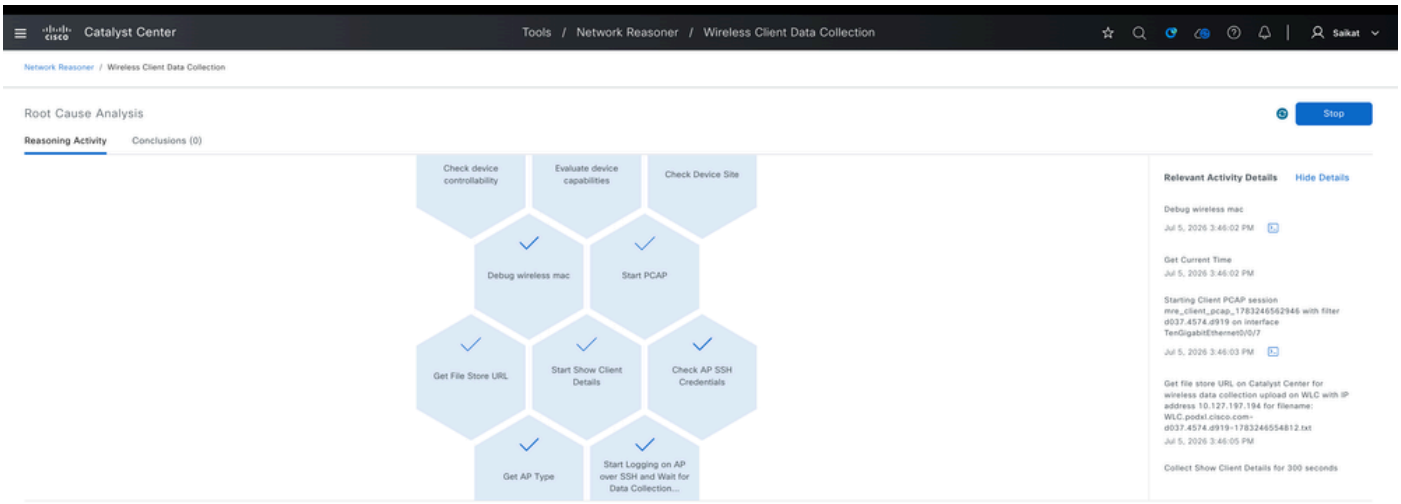
选择WLC排除无线客户端MAC故障



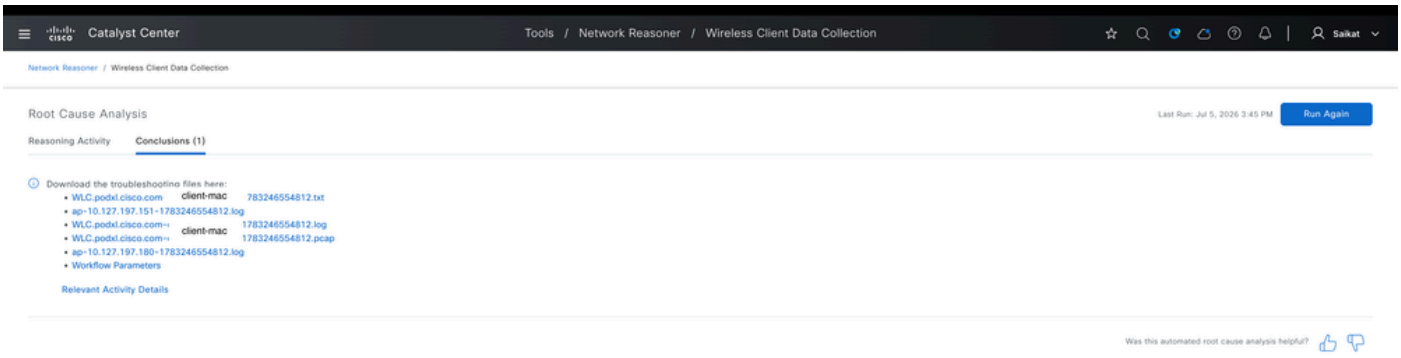
选择WLC上的接口排除无线客户端故障



选择AP（最多4个）对无线客户端进行故障排除



正在运行以排除无线客户端问题的任务



从WLC和AP收集的捕获用于无线客户端问题

```
!! 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
从IP地址为10.127.197.194的WLC中删除文件bootflash:<file-name>
2026年7月5日下午5:59:23

技术参考

- 思科智能捕获部署指南
- 管理智能捕获
- Cisco Catalyst保证用户指南，版本2.3.7.x
- 使用网络说明器排除网络设备故障 — 使用MRE工作流程在无线LAN控制器上使用HA

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。