Fehlerbehebung bei Wireless-Problemen mit Catalyst Center

Inhalt

Einleitung

In diesem Dokument wird die Behebung von Verbindungsproblemen mit Catalyst 9800 Wireless LAN Controller (WLC), APs und Clients unter Verwendung von Cisco Catalyst Center beschrieben.

Voraussetzungen

- Der Wireless LAN Controller muss zu Catalyst Center hinzugefügt werden und einen verwalteten Status im Bestand anzeigen.
- Der Telemetriestatus auf dem WLC muss "Up" (Aufwärts) lauten.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

- Zugriff auf den Wireless LAN Controller über eine Kommandozeile oder eine grafische Benutzeroberfläche
- Zugriff auf das Catalyst Center über eine Kommandozeile oder eine grafische Benutzeroberfläche

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Modell WLC 9800
- Cisco IOS XE 17.15.5
- Catalyst Center Version 2.3.7

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

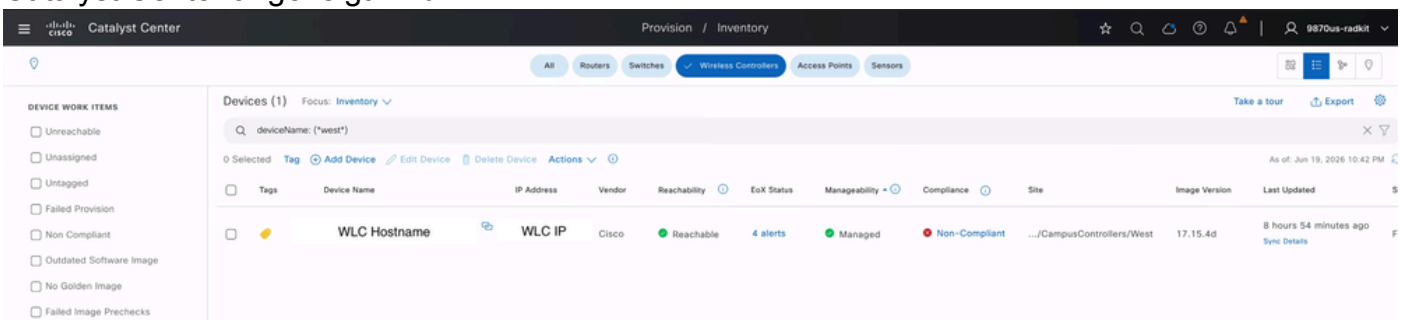
Erfassung von Daten aus Catalyst Center

Sobald ein Catalyst 9800 WLC zu Catalyst Center for Assurance hinzugefügt wurde, ruft die Plattform Daten über mehrere Erfassungsmethoden ab - SNMP Polling, Streaming-Telemetrie, NetFlow, Syslog, CLI-basierte Erfassung, APIs und IP SLA. Jeder Mechanismus erfüllt einen anderen Zweck: Einige berichten über den grundlegenden Gerätezustand (CPU, Arbeitsspeicher, Leistungsindikatoren), während andere detaillierte Informationen liefern (PoE-Status, Client-Sitzungen, Wireless-Leistung).

1. Geräte-/Bestandsüberwachung (SNMP + CLI): Erreichbarkeit, CPU, Arbeitsspeicher, Schnittstellenstatistiken und Softwareversion, erfasst durch Standard-SNMP Polling und CLI.
2. Syslog: System- und Betriebsprotokollmeldungen werden an Catalyst Center gesendet, das als konfigurierter Syslog-Server fungiert.
3. Wireless-Telemetrie (NETCONF/YANG-Streaming): Der zentrale Assurance-Feed. Es streamt Daten auf AP- und Client-Ebene nahezu in Echtzeit - Client-Onboarding- und

Roaming-Ereignisse, RSSI/SNR, AP-Funk-/RF-Statistiken und interne WLC-Integritätszähler.

Um diese Daten zu empfangen, muss sich der Wireless LAN Controller im verwalteten Zustand von Catalyst Center befinden, wobei der Telemetriestatus zwischen dem Controller 9800 und Catalyst Center angezeigt wird.



Status des Wireless LAN-Controllers in 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

Cisco Catalyst Center wird standardmäßig mit Integritäts-, Problem- und Ereigniseinstellungen konfiguriert, die spezifische Schwellenwerte und Prioritäten für Wireless Controller, Access Points, Wireless Clients und Anwendungen enthalten. Catalyst Center generiert Ereignisse und Warnungen auf Basis der Daten, die es von diesen verwalteten Geräten erhält, und der konfigurierten Ereigniseinstellungen. Darüber hinaus können benutzerdefinierte Profile erstellt werden, um diese Einstellungen an die spezifischen Netzwerkanforderungen anzupassen. Dies ermöglicht eine präzisere Überwachung und Warnmeldungen auf Basis der individuellen Anforderungen der Netzwerkumgebung.

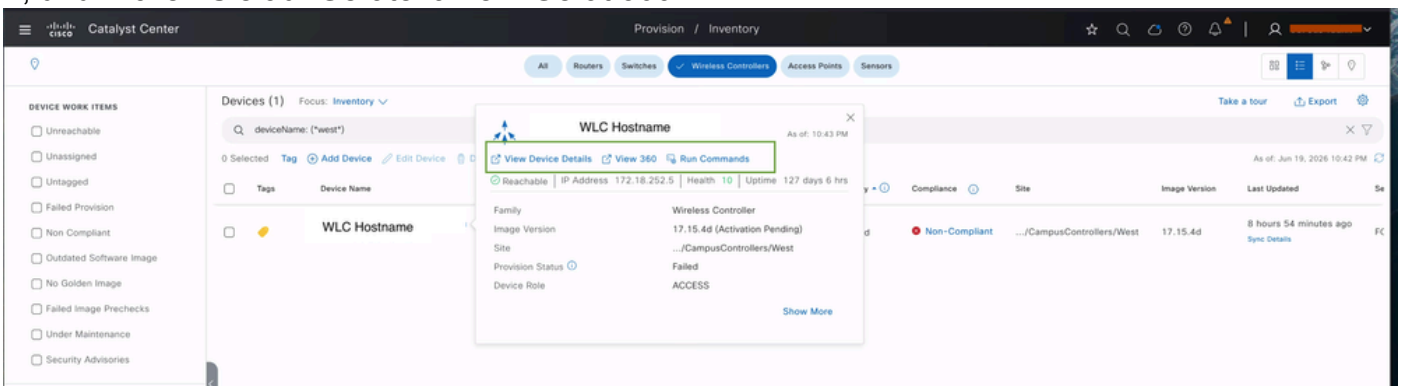
Problem mit Catalyst Wireless Controller der Serie 9800

Wenn bei einem Wireless LAN Controller (WLC) Probleme auftreten, wie z. B. Verlust der Erreichbarkeit, langsame Leistung, Zugriffsfehler, ein Ausfall oder eine Verschlechterung eines bestimmten Services, bietet Cisco Catalyst Center integrierte Transparenz, mit der Sie die Vorgänge auf dem Controller genau zum Zeitpunkt des Problems rekonstruieren können, ohne sich direkt beim Gerät anmelden zu müssen.

Überprüfen des Controller-Status mit Gerät 360

Die Ansicht "Gerät 360" fasst die Erreichbarkeit von Controllern, den Telemetriestatus, Verlaufsprobleme, generierte Ereignisse und Leistungsstatistiken in einem einzigen zeitgesteuerten Dashboard zusammen und ist damit der erste Ort, an dem ein gemeldetes WLC-Problem untersucht werden kann.

Navigieren Sie zu Bereitstellung > Bestand > Wireless Controller > [Nach dem Controller suchen] >, und klicken Sie auf Gerätename > Gerät 360

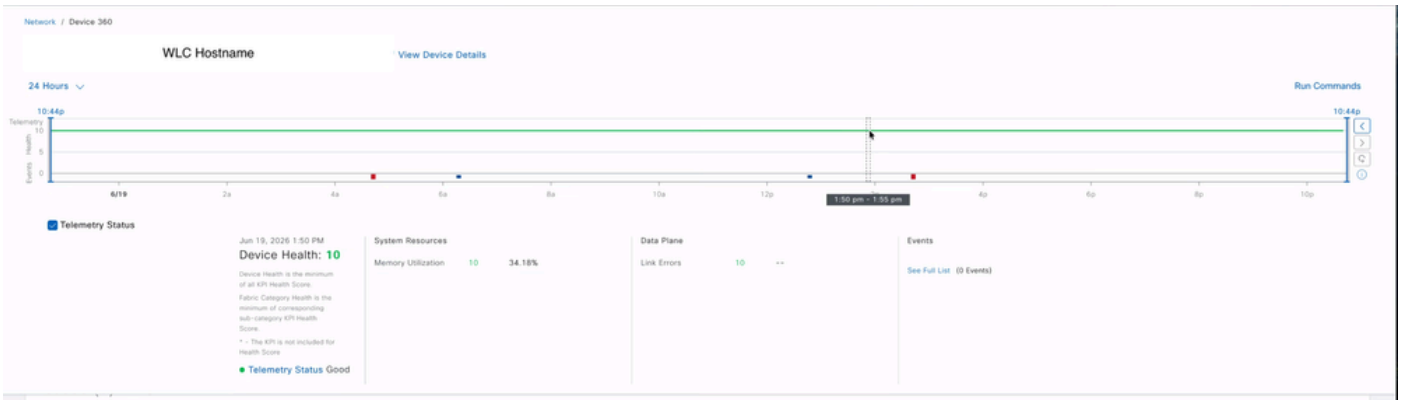


View 360 für Wireless LAN-Controller

Anmerkung: Dieselbe Ansicht können Sie auch über Assurance > Health > Network (Sicherheit > Gesundheit > Netzwerk) aufrufen und dann in der Tabelle Network Devices (Netzwerkgeräte) auf den Gerätenamen klicken.

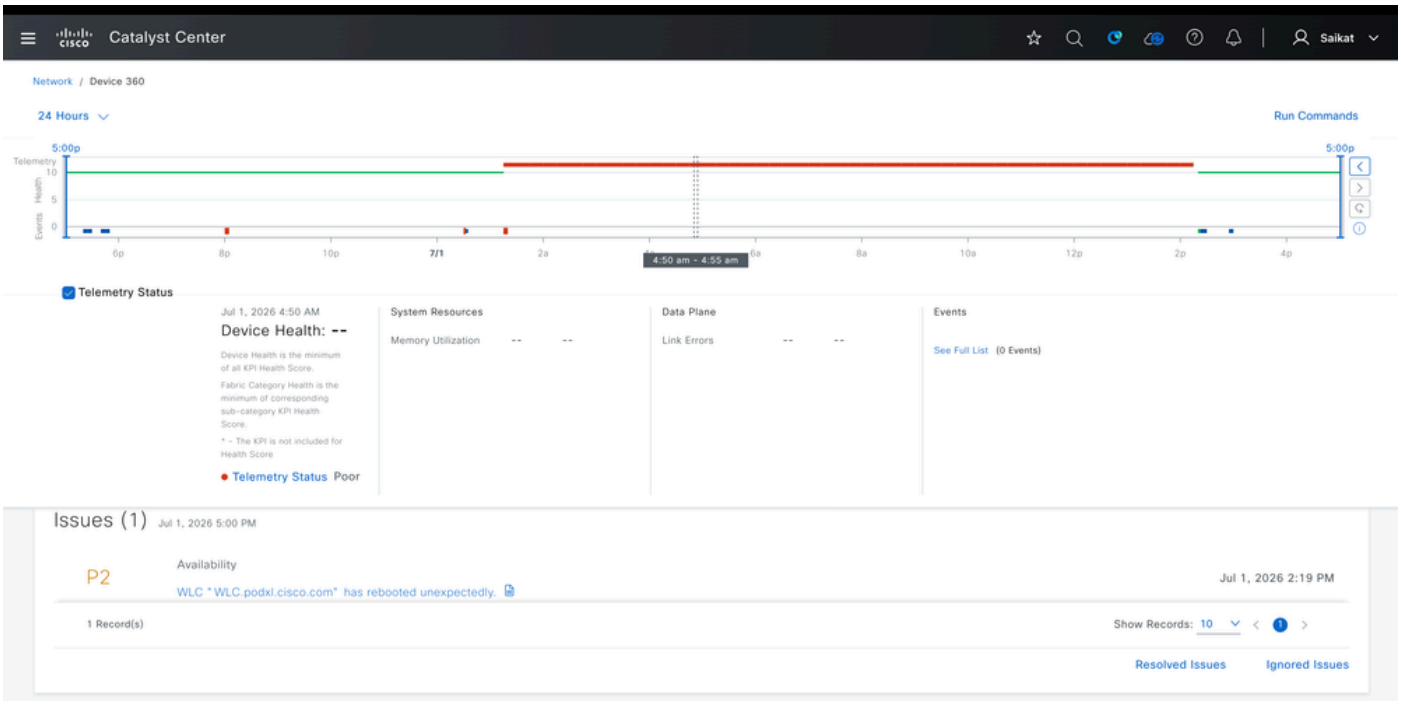
Mit Gerät 360 können Sie den Schieberegler für die Integritätszeitleiste auf einen beliebigen Punkt innerhalb des unterstützten Verlaufsfensters verschieben (die Catalyst Center Assurance-Daten werden bis zu 30 Tage gespeichert), um den Controller-Status zum Zeitpunkt des Vorfalls genau zu überprüfen. Die Ansichtsflächen für dieses ausgewählte Fenster:

Erreichbarkeit von Geräten - ob der Controller erreichbar war und verwaltet wurde
Telemetriestatus - Zustand der SNMP/Syslog/NETCONF-Telemetrieförderung Assurance.



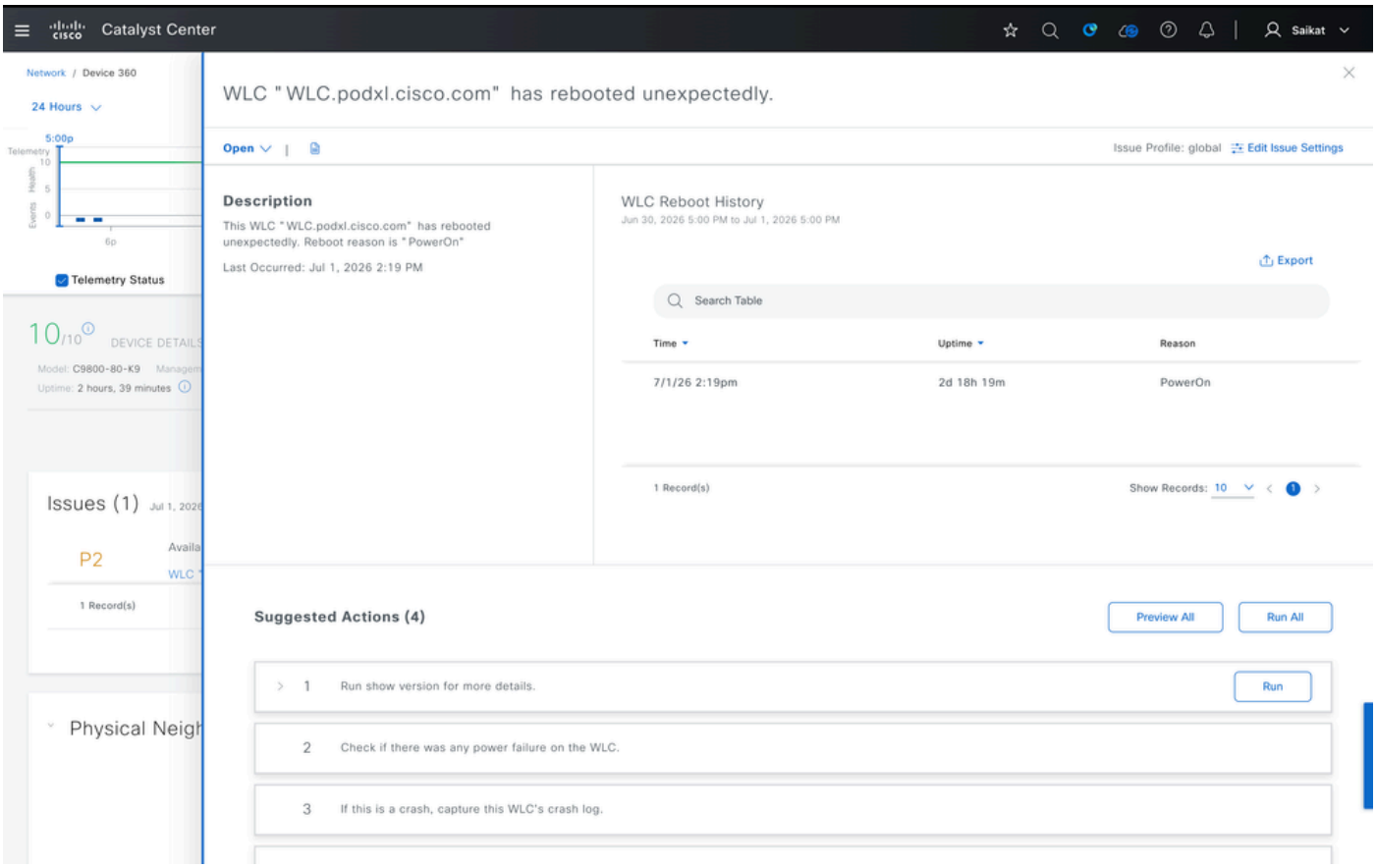
Telemetriestatus des Wireless LAN-Controllers

Beobachtete Probleme - Von der Garantie erkannte Probleme auf dem Gerät in diesem Zeitraum.

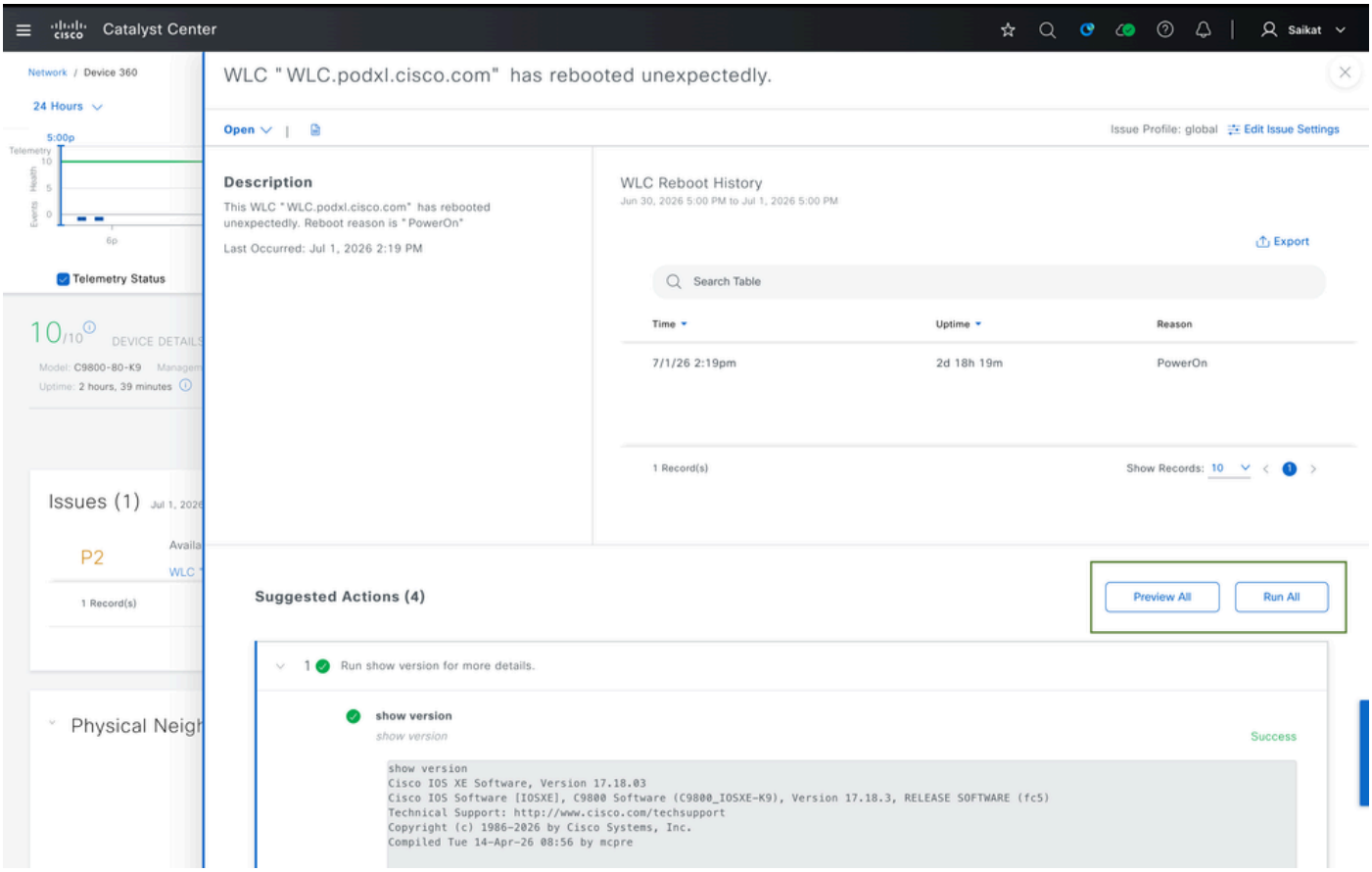


Für den Wireless LAN-Controller gemeldete Probleme

Wenn Sie auf ein bestimmtes Problem klicken, werden detaillierte Informationen sowie Vorschläge zur Behebung des Problems oder zur weiteren Untersuchung angezeigt.

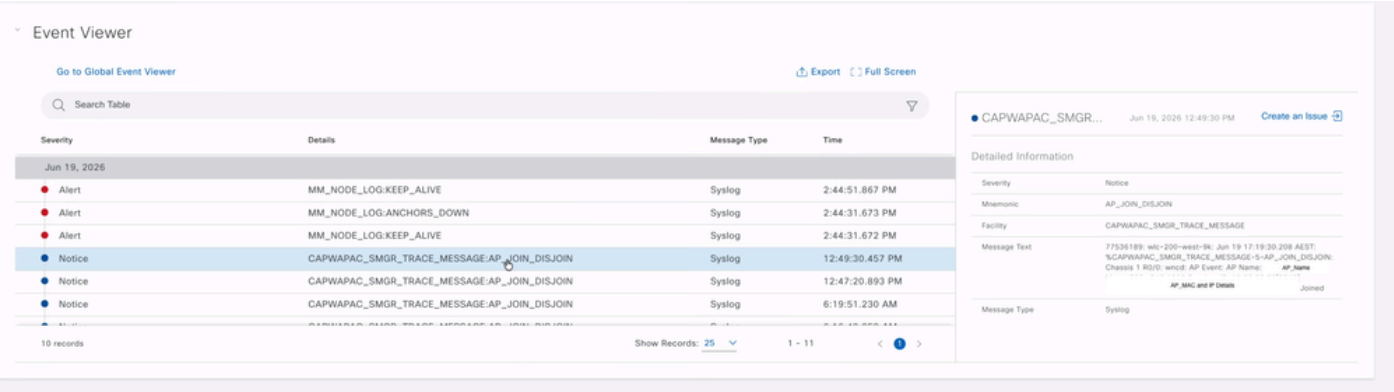


Vorgeschlagene Aktion für Problem gemeldet auf WLC

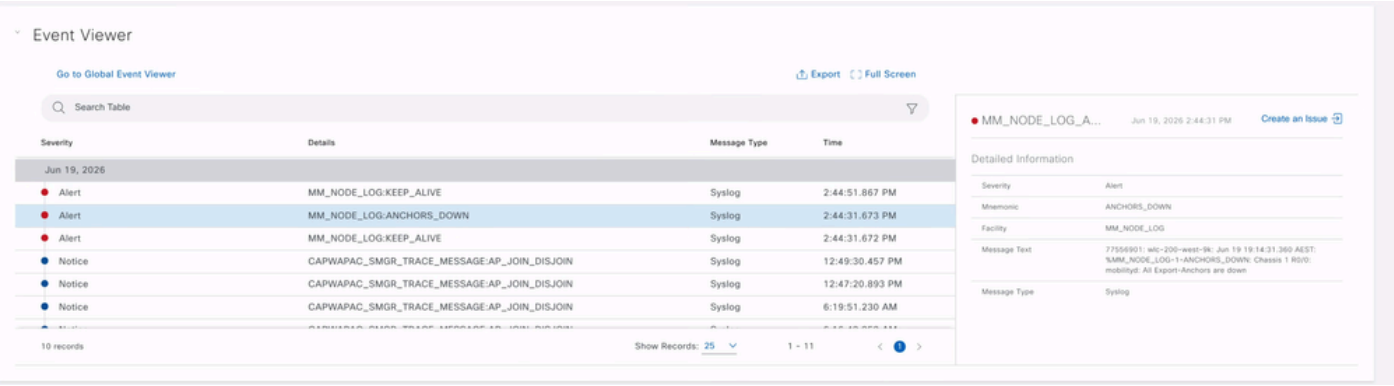


Vorgeschlagene Aktion für Problem gemeldet auf WLC

Generierte Ereignisse - basierend auf Syslog-Meldungen und SNMP-Traps, die vom Controller empfangen wurden:



Ereignisanzeige für Wireless LAN-Controller - Beispiel 1

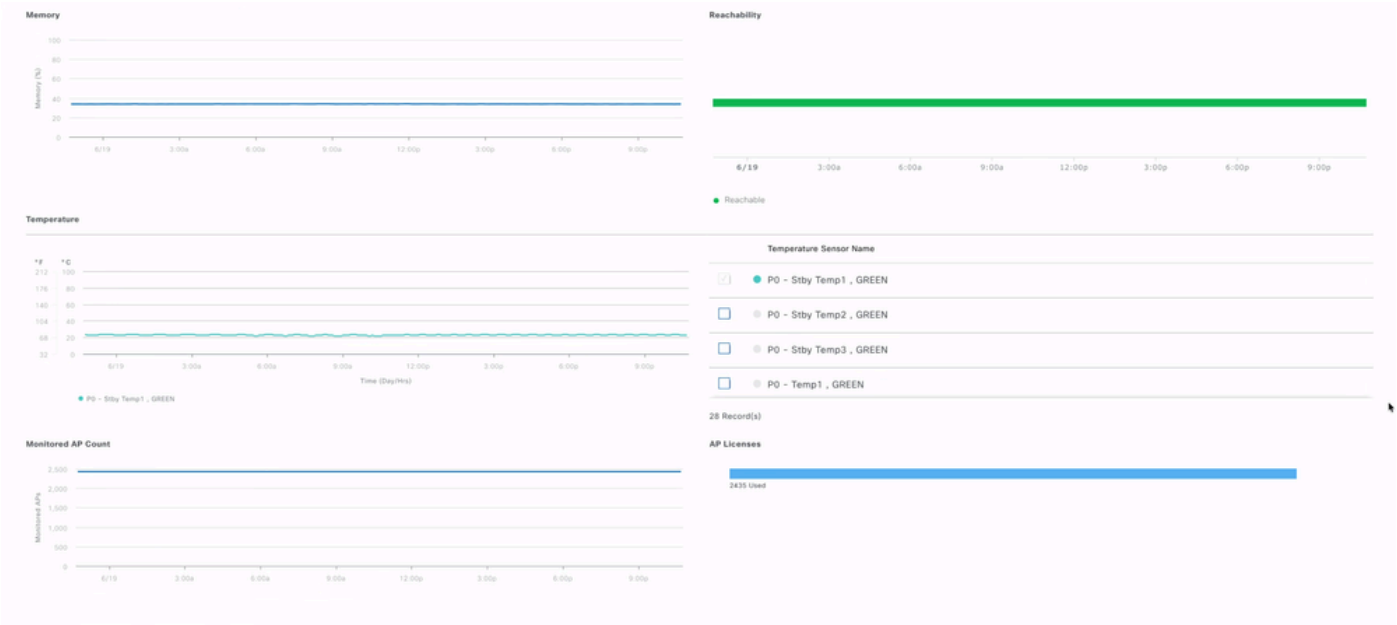


Ereignisanzeige für Wireless LAN-Controller - Beispiel 2

Leistungsstatistiken - CPU- und Speichernutzung, Temperatur, Betriebszeit, HA-Status und Grund für das letzte Neuladen.

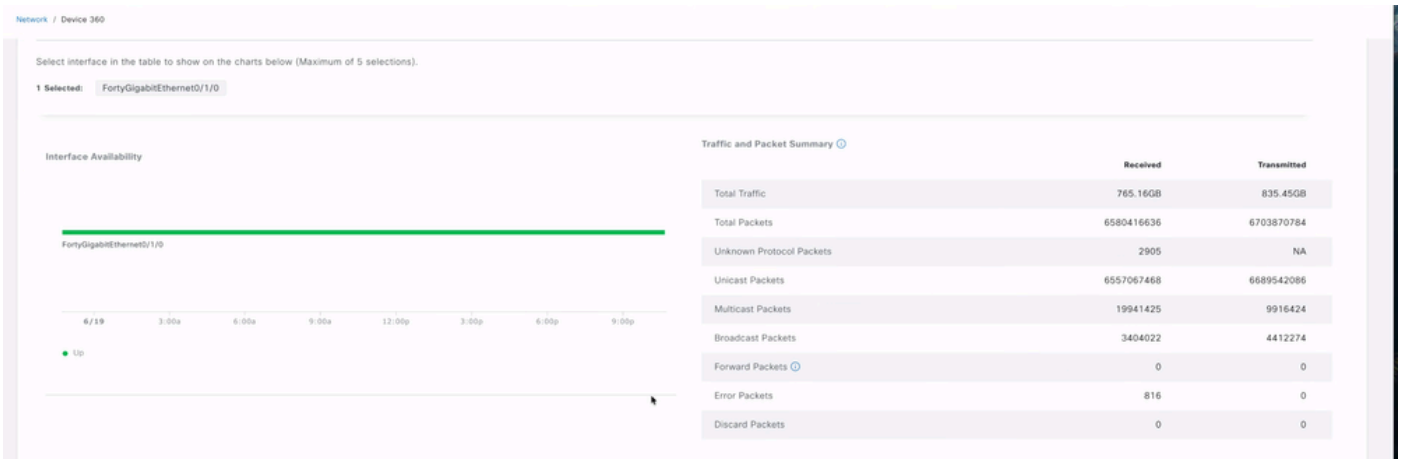
Verbundene Clients - einschließlich Aufschlüsselung nach lokaler, ausländischer, Anker- und Inaktivitätszahl der Clients
AP-Status - Der Verbindungs-/Integritätsstatus der Access Points, die dem Controller zugeordnet sind.

WLC-Statistiken zu Catalyst Center



WLC-Statistiken zu Catalyst Center

Schnittstellenstatistiken - Schnittstellenstatus, RX-/TX-Paketanzahl, Auslastung, Verwerfungen und Fehler.



WLC-Statistiken zu Catalyst Center

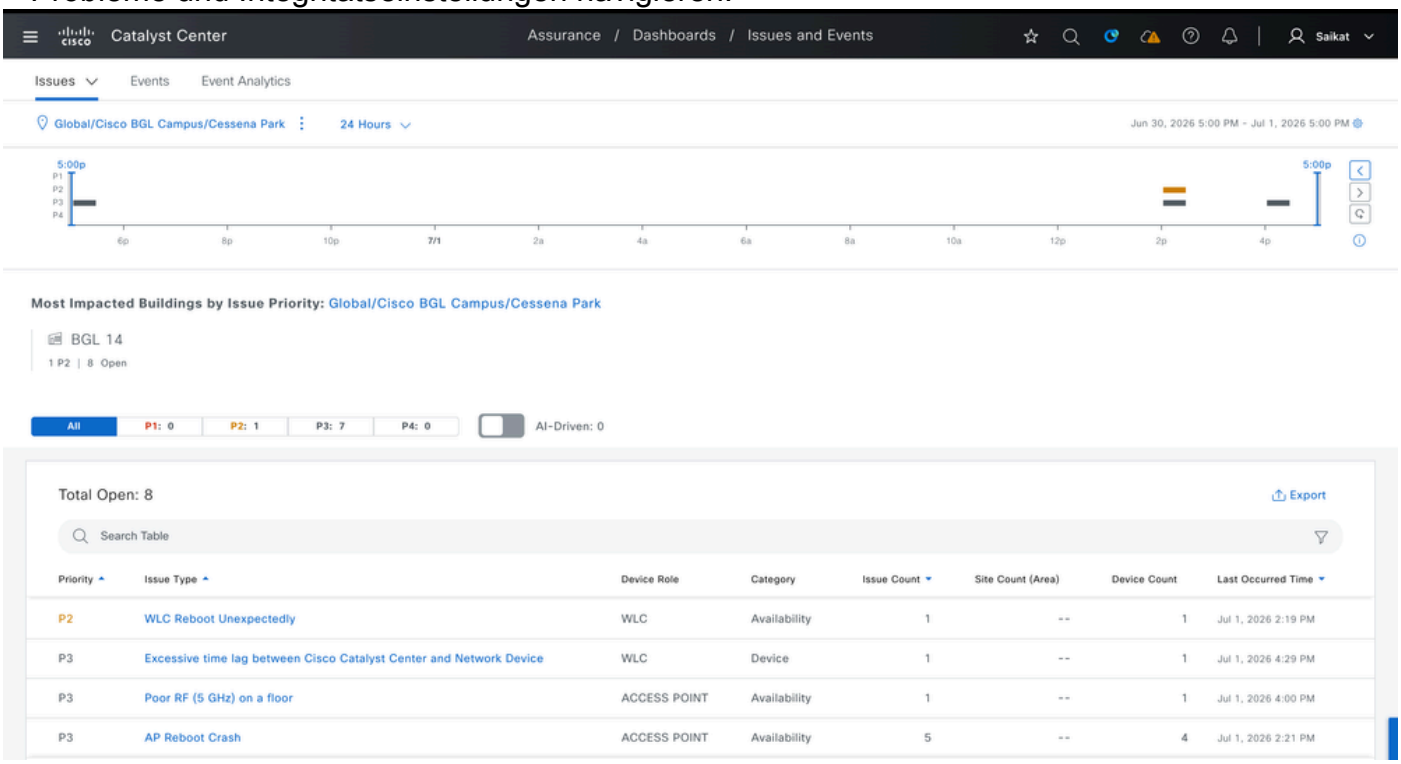
WLC-Statistiken zu Catalyst Center

Da all dies miteinander korreliert ist, können Sie während der Zeit der Ausgabe mehrere verwandte Faktoren korrelieren und ein klares Verständnis dafür erhalten. Mit diesen Statistiken können Sie die Ursache des Problems nicht genau ermitteln, aber wir können alle möglichen Ursachen ausschließen, die uns bei der weiteren Fehlerbehebung und der Einrichtung der Protokolltypen helfen können, die in Echtzeit erfasst werden müssen.

Problem mit einem Access Point

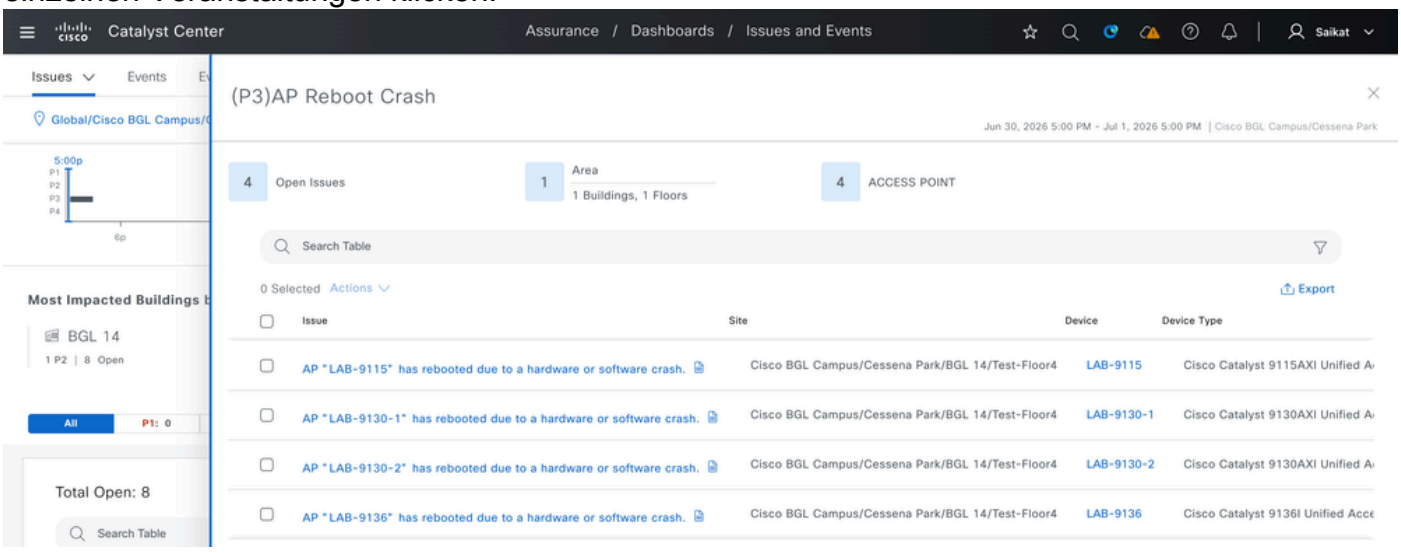
Wenn ein Cisco Access Point auf Probleme wie Verbindungsunterbrechungen, Funkstatusanomalien, Neustarts, Abstürze, unzureichende Funkfrequenzbedingungen, hohe Kanalauslastung oder Inaktivität stößt, generiert Catalyst Center Warnungen mit den

entsprechenden Prioritätsstufen. Sie können diese Warnungen anzeigen, indem Sie zu Sicherheit > Probleme und Integritätseinstellungen navigieren.



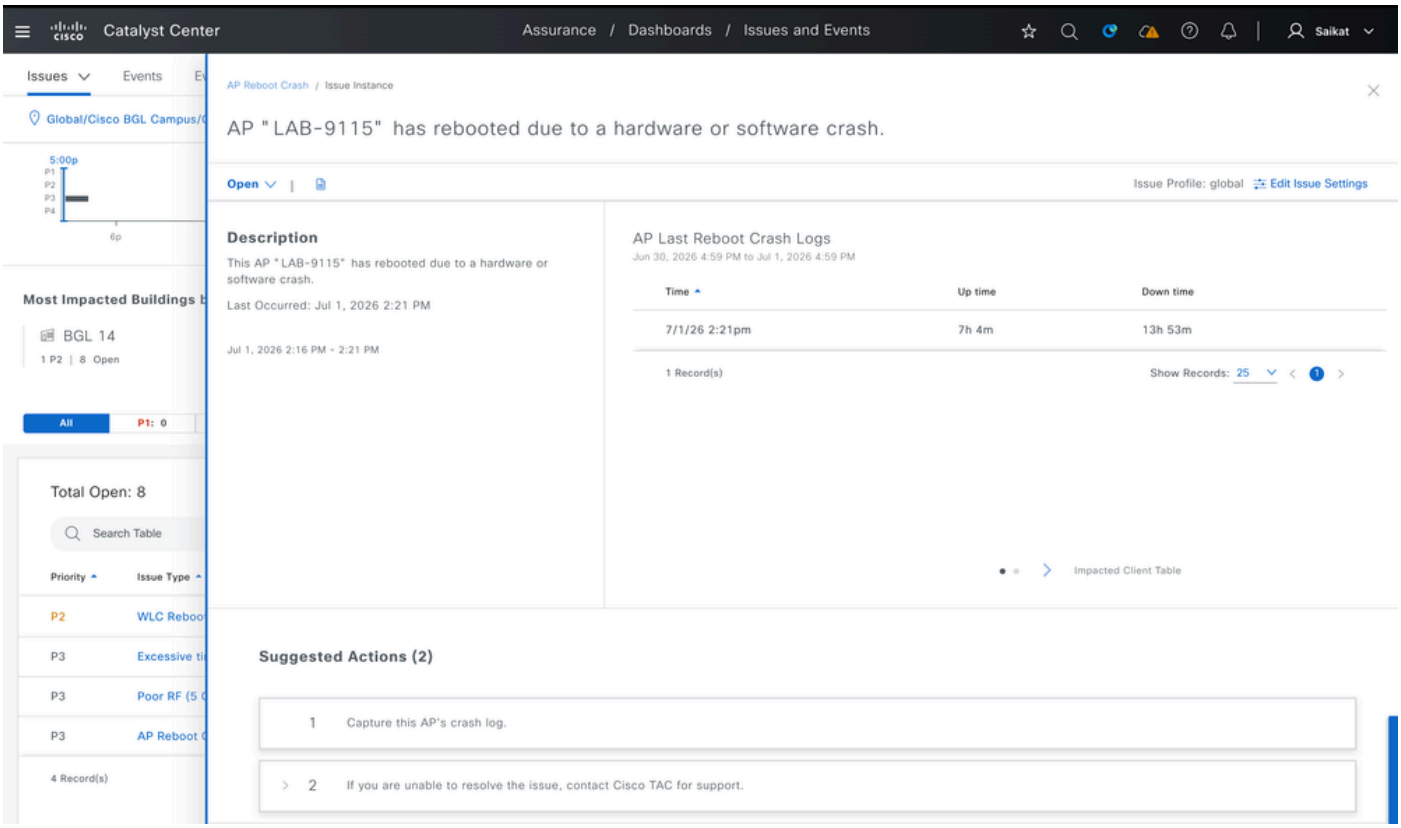
Berichtete Probleme werden mit der entsprechenden Priorität generiert und ausgegeben

In diesem Abschnitt werden alle offenen Probleme in Ihrer Umgebung angezeigt. Wenn Sie auf die einzelnen Veranstaltungen klicken, erhalten Sie detaillierte Informationen, indem Sie auf die einzelnen Veranstaltungen klicken:



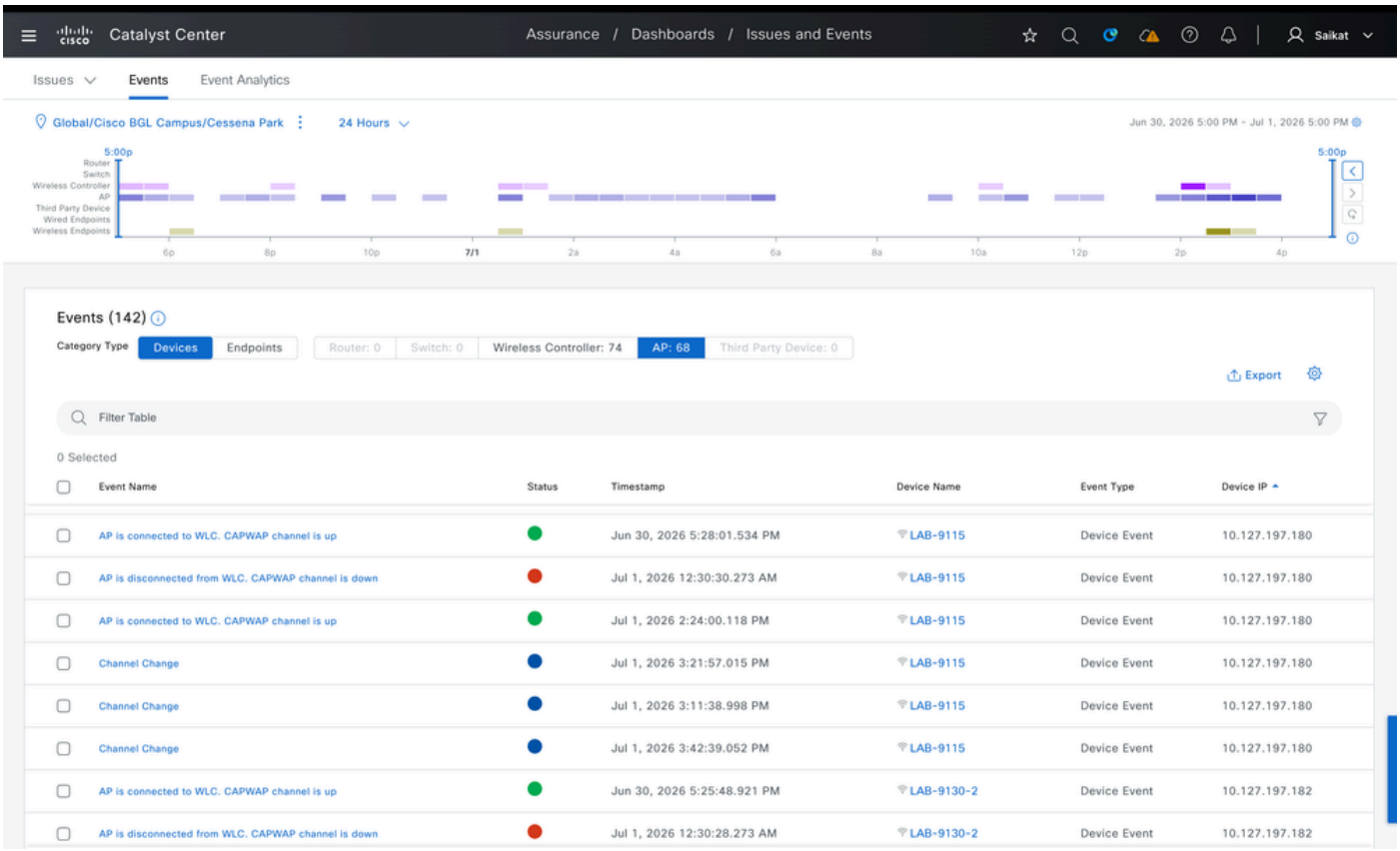
Detaillierte Übersicht über das gemeldete Problem

Wenn Sie auf ein bestimmtes Problem klicken, werden detaillierte Informationen sowie Vorschläge zur Behebung des Problems oder zur weiteren Untersuchung angezeigt.

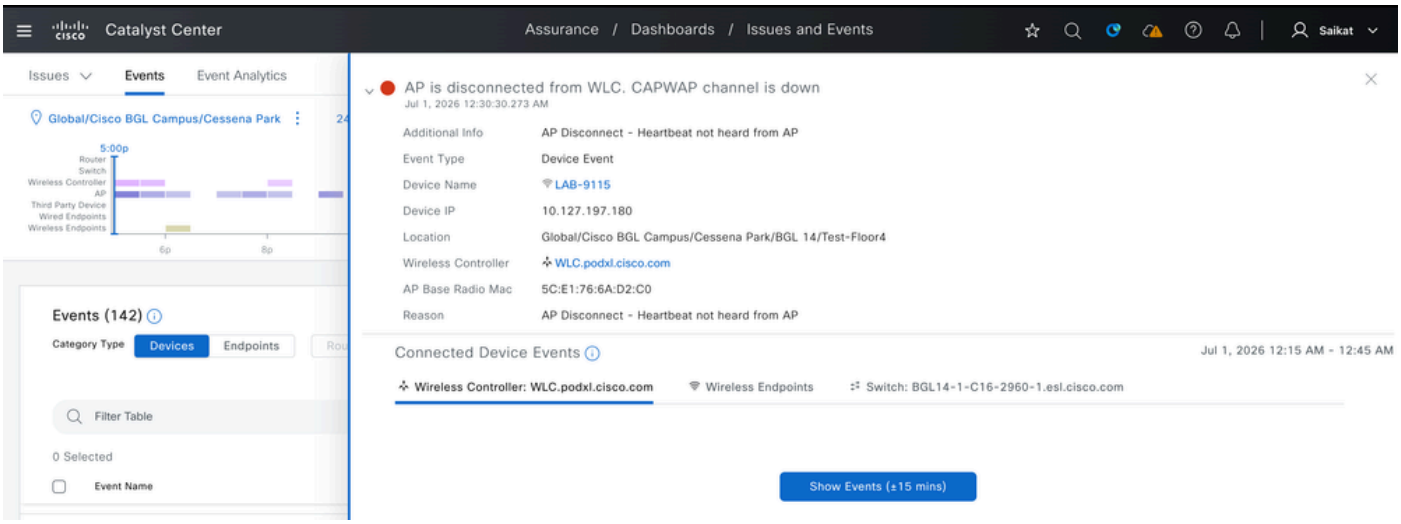


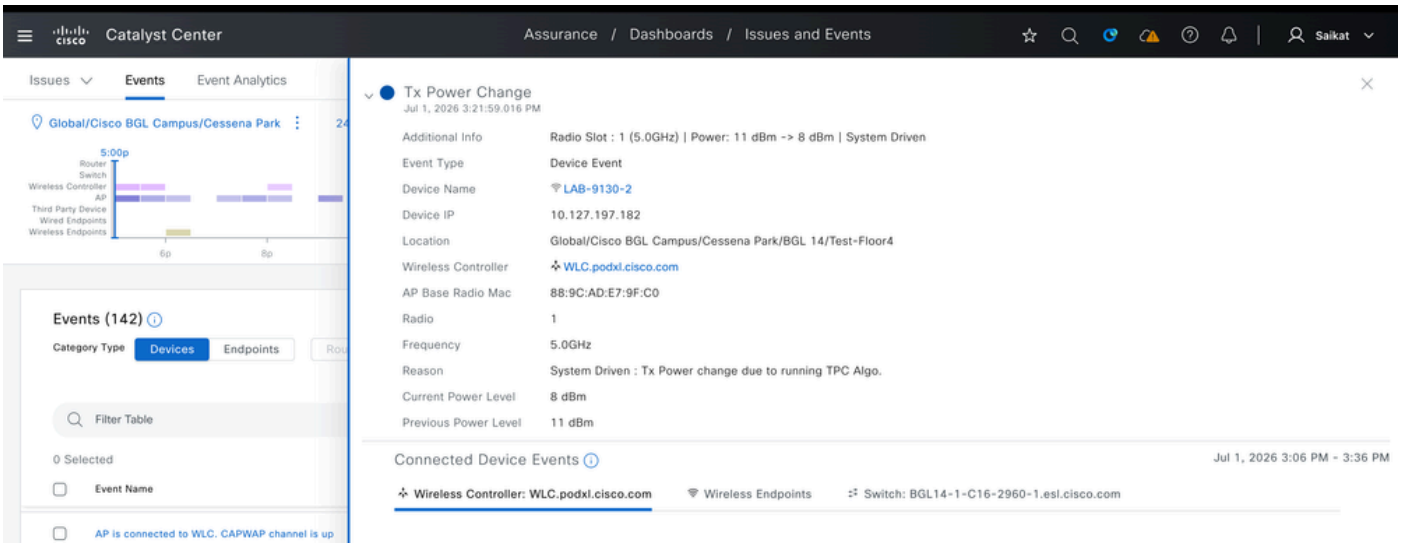
Vorgeschlagene Aktion für Problem am Access Point gemeldet

Darüber hinaus können Sie auf die Ereignisanzeige zugreifen, die alle von Catalyst Center empfangenen Ereignisse als Syslogs enthält. Dies ist nützlich, um alle Ereignisse zu verfolgen, z. B. die Join/Disjoin-Aktivität des Access Points, Kanaländerungen, Änderungen am TX-Strom und Neustarts. Diese Ereignisse werden sowohl für den Wireless-Controller als auch für einzelne APs erfasst.

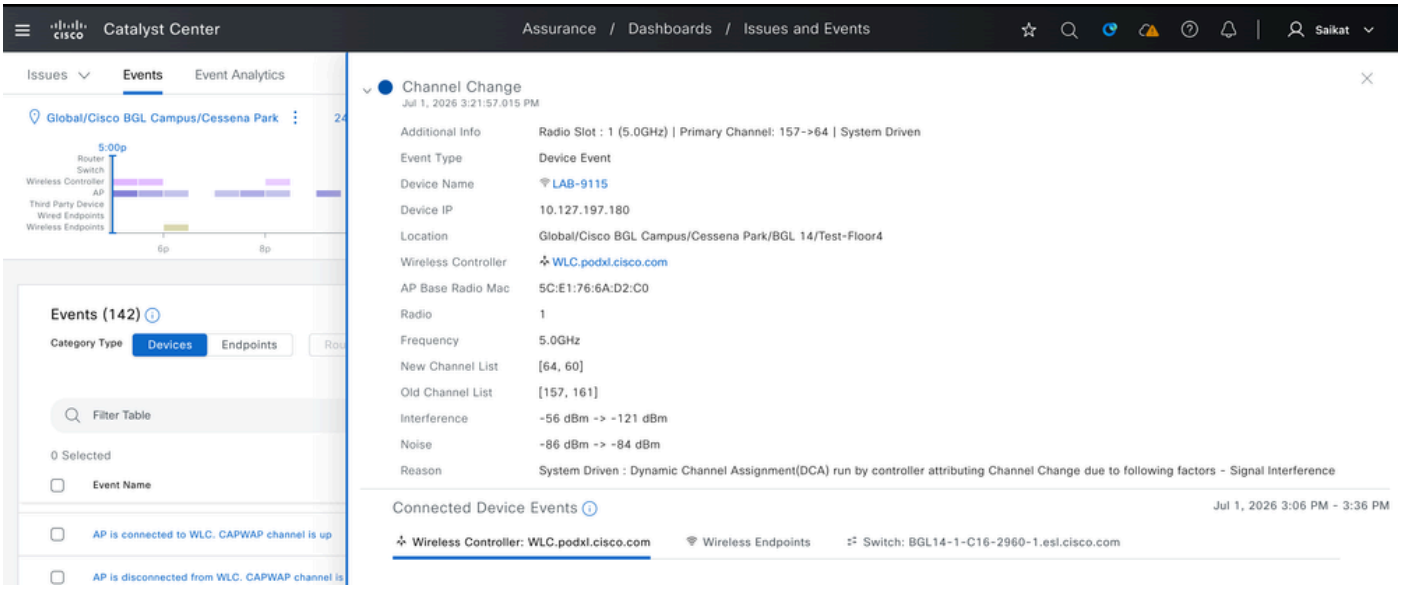


Ereignisanzeige für APs in Catalyst Center

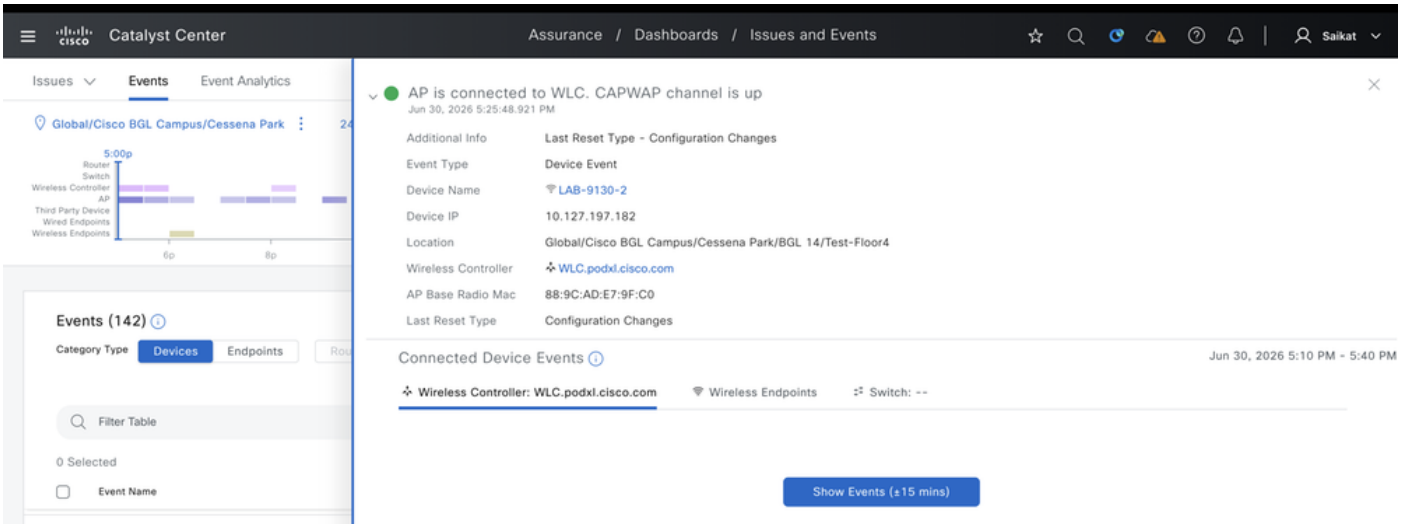




Detaillierte Übersicht über die gemeldeten Ereignisse (Hinweis)

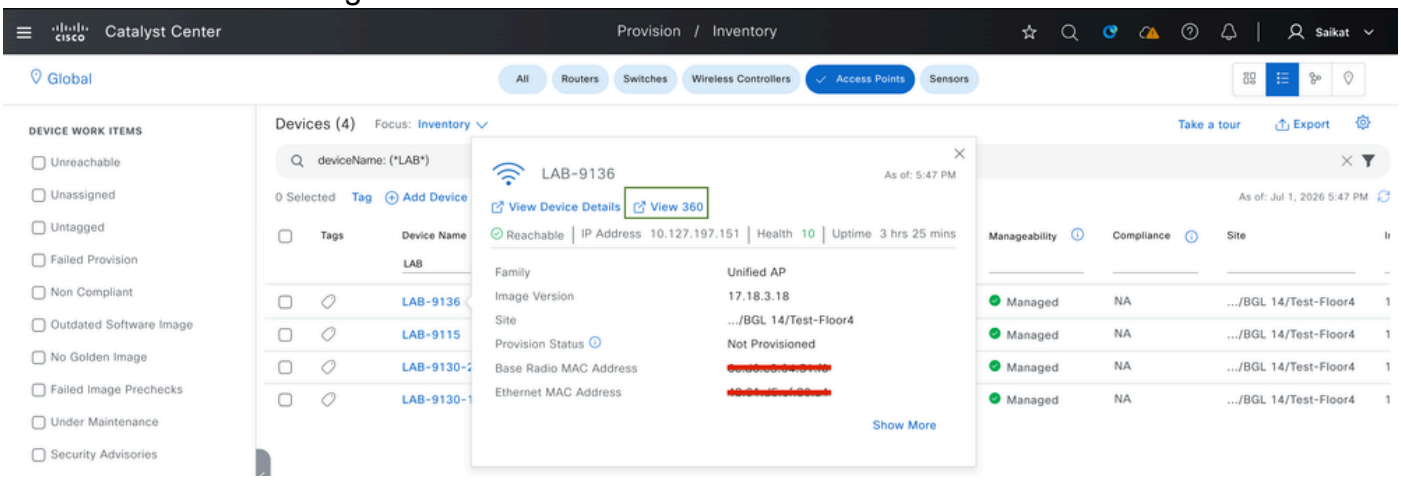


Detaillierte Übersicht über die gemeldeten Ereignisse (Hinweis)



Detaillierte Übersicht über das gemeldete Ereignis (Info)

Bei spezifischen Problemen mit einem einzelnen Access Point können Sie die 360-Systemzustandsansicht für das Gerät überprüfen. Hier sehen Sie den Erreichbarkeitsstatus, gemeldete Ereignisse und Probleme sowie die Integritätsbewertung für diesen Access Point zu einem bestimmten Zeitpunkt. Die Integritätsbewertung wird basierend auf Speichernutzung, Kanalnutzung, Funkqualität, Interferenz und Datenverkehrsnutzung berechnet. Navigieren Sie hierzu zu Provisionierung > Bestand > Access Point > Klicken Sie auf AP:

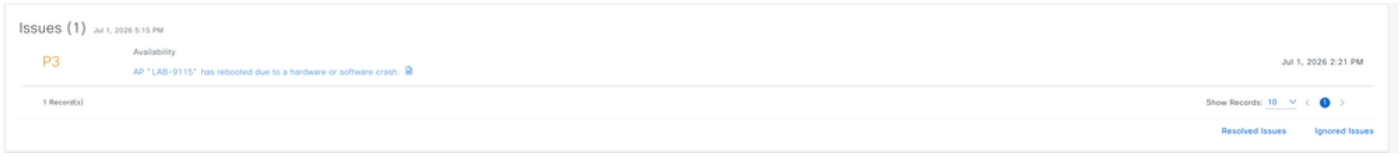


View 360 für individuellen AP

Telemetrie-Übersicht für Gerät 360: Hier sehen Sie die Timeline für den Gesamtzustand der Access Points, die Systemressourcennutzung (Speicher, CPU), Verbindungsfehler auf Datenebene und funkspezifische Statistiken (Rauschen, Kanalnutzung, Interferenz, Datenverkehrsnutzung) für beide Funkmodule. Mit Gerät 360 können Sie den Schieberegler für den Zustand der Timeline zu einem beliebigen Punkt innerhalb des unterstützten Verlaufsfensters (30 Tage) zurückbewegen.

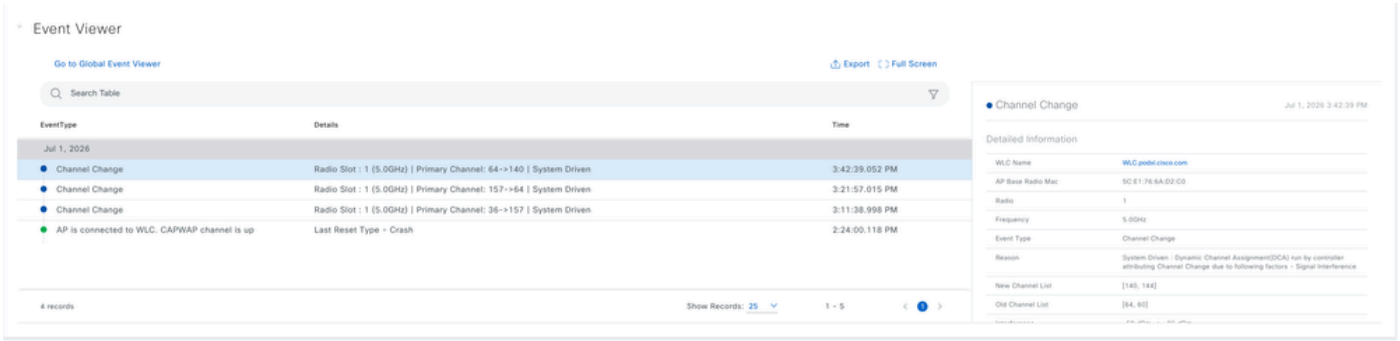
View 360: AP-Telemetriestatus und Zustand

Probleme - Hier sehen Sie die Liste der offenen Probleme für den Access Point, zusammen mit Schweregrad (P1-P4), Problemkategorie, Beschreibung und Zeitstempeln.



Problem für AP gemeldet

Ereignisanzeige - Sie können ein chronologisches Protokoll der AP-Ereignisse (z. B. Kanaländerungen, CAPWAP-Status) zusammen mit detaillierten Ereignisinformationen wie WLC-Name, Funkfrequenz, Grund und alte/neue Kanallisten anzeigen.

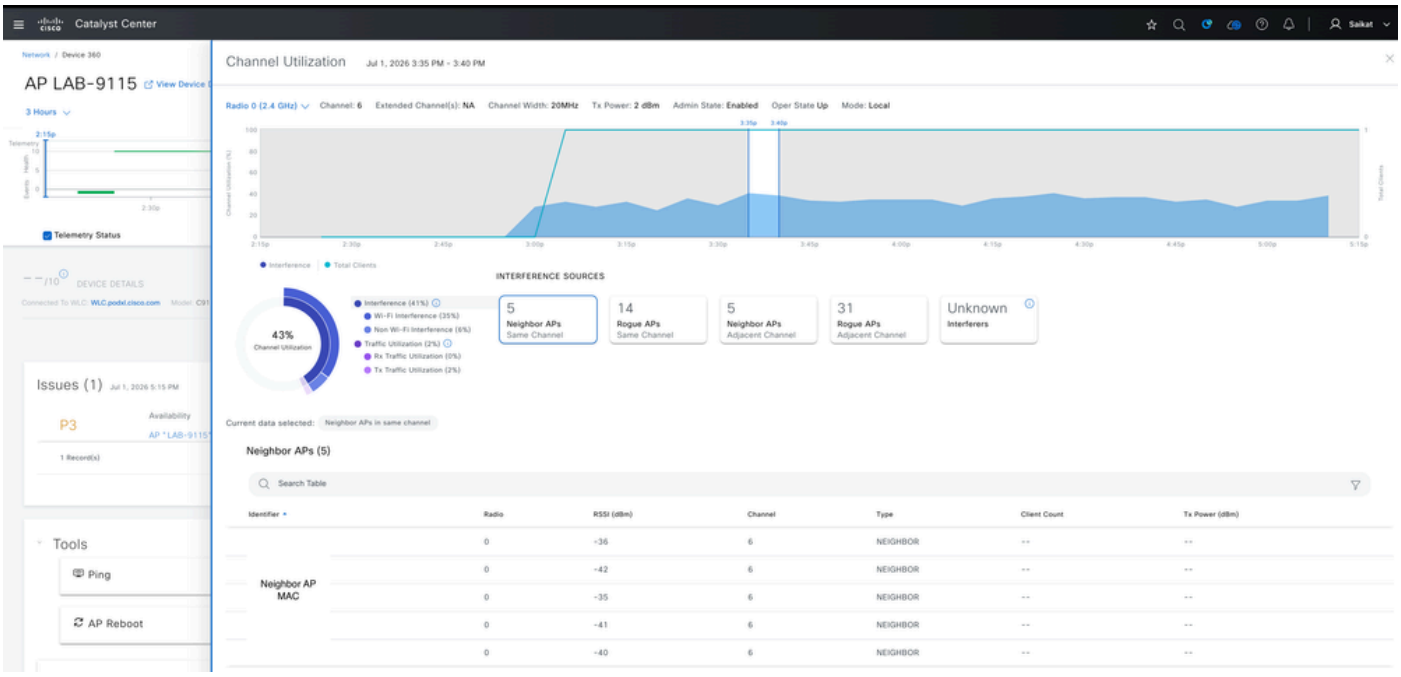


Ereignisanzeige einzelner APs

Physische Nachbartopologie mit Client-Liste - Diese Ansicht zeigt die physische Topologie, die den WLC, AP und die verbundenen Clients verbindet, sowie weitere Client-Details wie Gerätename, Integritätsbewertung und MLO.

Physische Topologie des Access Points

Kanalauslastung - Hier sehen Sie den Trend zur Kanalauslastung der APs, Störungsquellen (benachbarte APs, nicht autorisierte APs, unbekannte Störungsquellen) und eine detaillierte Tabelle der benachbarten APs mit RSSI, Kanal und Typ.



Kanalnutzung für einzelnen AP

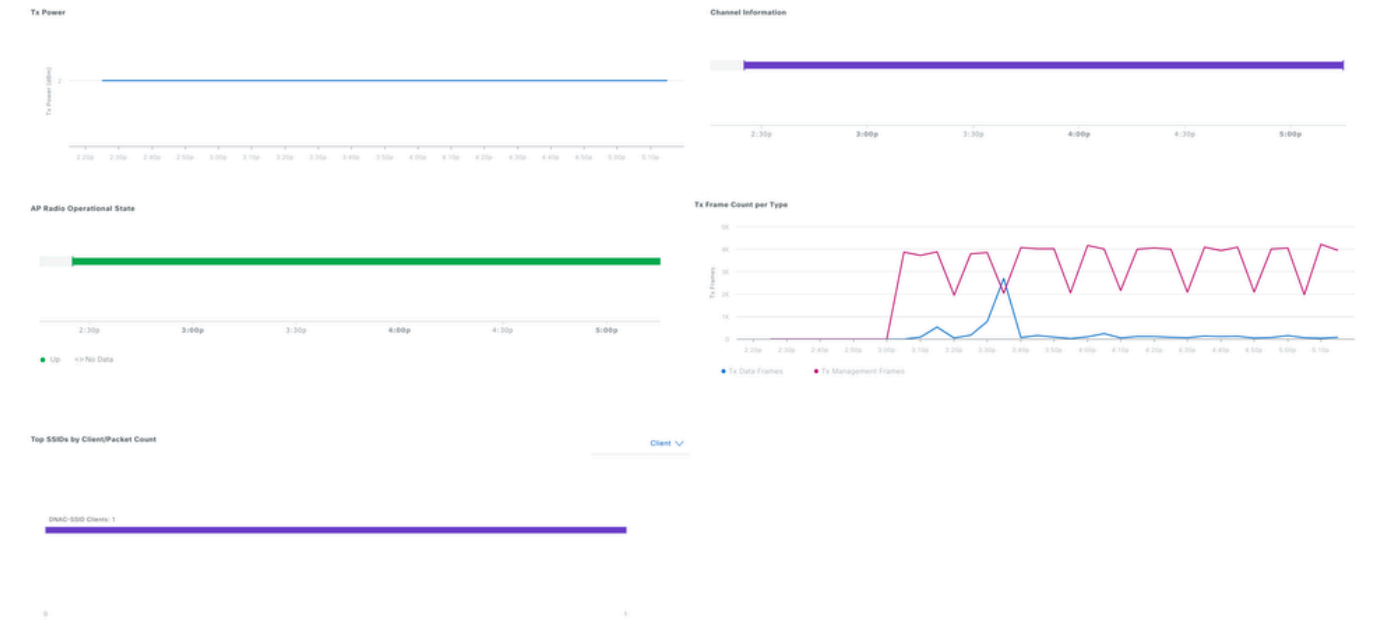
Detailinformationen (Registerkarte "Gerät") - Dieser Abschnitt zeigt Geräteinformationen (AP-Name, IP-Adresse, Modell, MAC-Adressen, Softwareversion), Verfügbarkeitsdetails (Betriebszeit, Controller-Beitrittszeit, Grund für das letzte Zurücksetzen), CPU-/Speichernutzungsdiagramme und das Verbindungsdiagramm von AP zu WLC.

Gerätedetails für AP

Funkspezifische KPIs: Hier können Sie Kennzahlen für den Funkpegel anzeigen, einschließlich Kanalnutzung, Client-Anzahl, Durchsatz (Rx/Tx-Rate), Wiederholungsversuche, Rauschen und Funkqualität für die ausgewählte Funkeinheit.

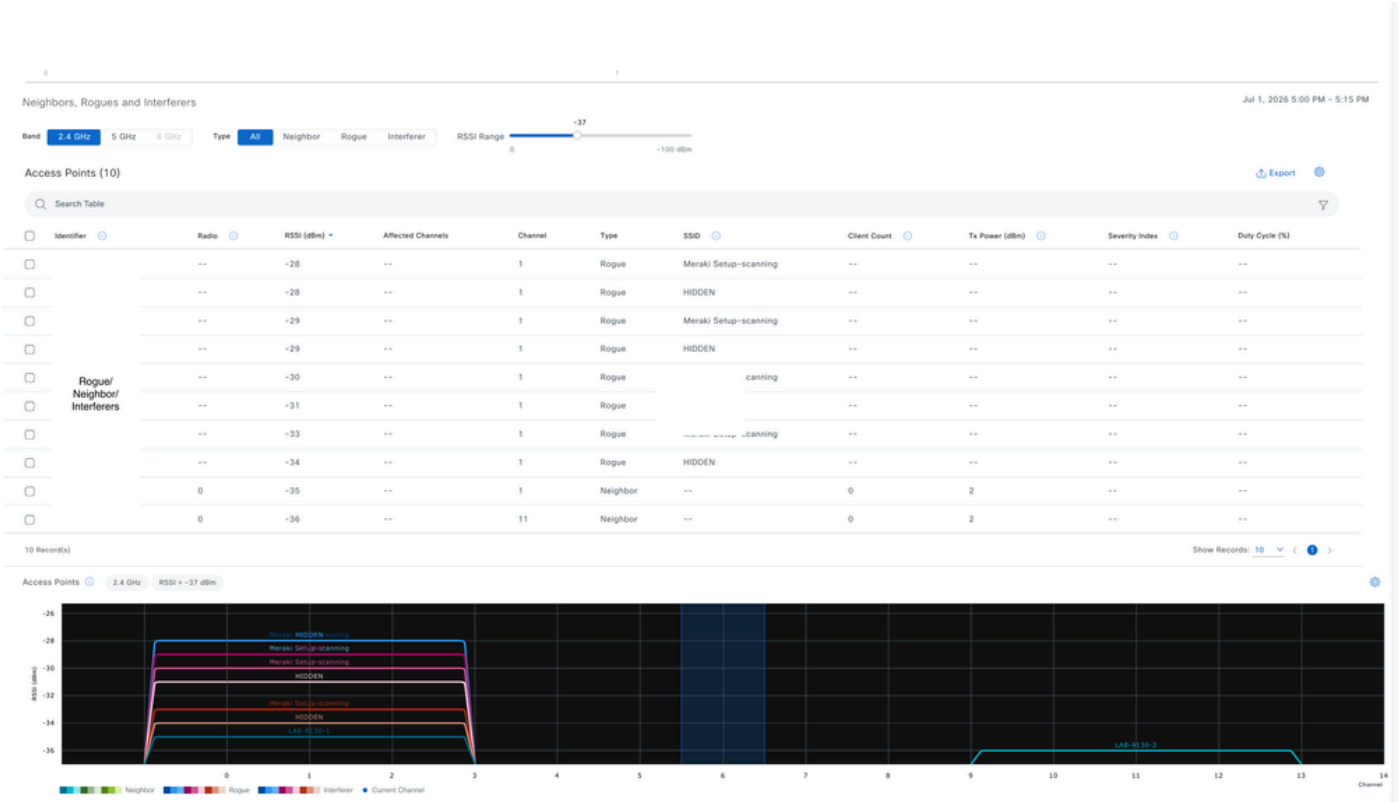
RF-Statistik für einzelnen AP

Tx Power, Channel Information & Frame Stats (Übertragungsleistung, Kanalinformationen und Frame-Statistiken): Auf diesem Bildschirm werden Trends zur Übertragungsleistung, der Verlauf der Kanalzuweisung, der Betriebsstatus des AP-Funkmoduls, die Anzahl der Tx-Frames nach Typ (Daten vs. Verwaltung) und die höchsten SSIDs nach Client-/Paketanzahl angezeigt.



RF-Statistik für einzelnen AP

Nachbarn, Schurken und Störenfriede: In dieser Ansicht sehen Sie alle benachbarten Geräte, nicht autorisierte Geräte und Störungsquellen mit ihrer RSSI, den betroffenen Kanälen, der SSID, der Client-Anzahl, der Sendeleistung und dem Schweregrad sowie eine visuelle Darstellung der RSSI-vs-Channel.



Nicht autorisierte, Nachbarn und Störer für einzelnen AP gemeldet

Das Dashboard für die Geräte 360 vereint Informationen zur Funkumgebung wie Kanalnutzung, Interferenz, Rauschen und Wiederholungen sowie Informationen zu benachbarten Geräten, unberechtigten Geräten und Störquellen. So können Sie leichter herausfinden, ob ein AP-Problem durch Funküberlastung, Kanalkonflikte oder unberechtigte Geräte verursacht wird. Gerätezustandsdaten wie CPU, Arbeitsspeicher, Neustartverlauf und Verbindungsstatus helfen Ihnen zusammen mit der Ereignisanzeige und dem Bedienfeld "Probleme" dabei, Hardwareabstürze, Verbindungsunterbrechungen und unerwartete Kanaländerungen zu erkennen. In Kombination mit der Topologie und den Client-Ansichten ergibt sich so ein umfassendes Bild für die Fehlerbehebung - von RF-Problemen bis hin zu individuellen Client-Problemen - mit integrierten Lösungsvorschlägen

Intelligente Erfassung für Access Point

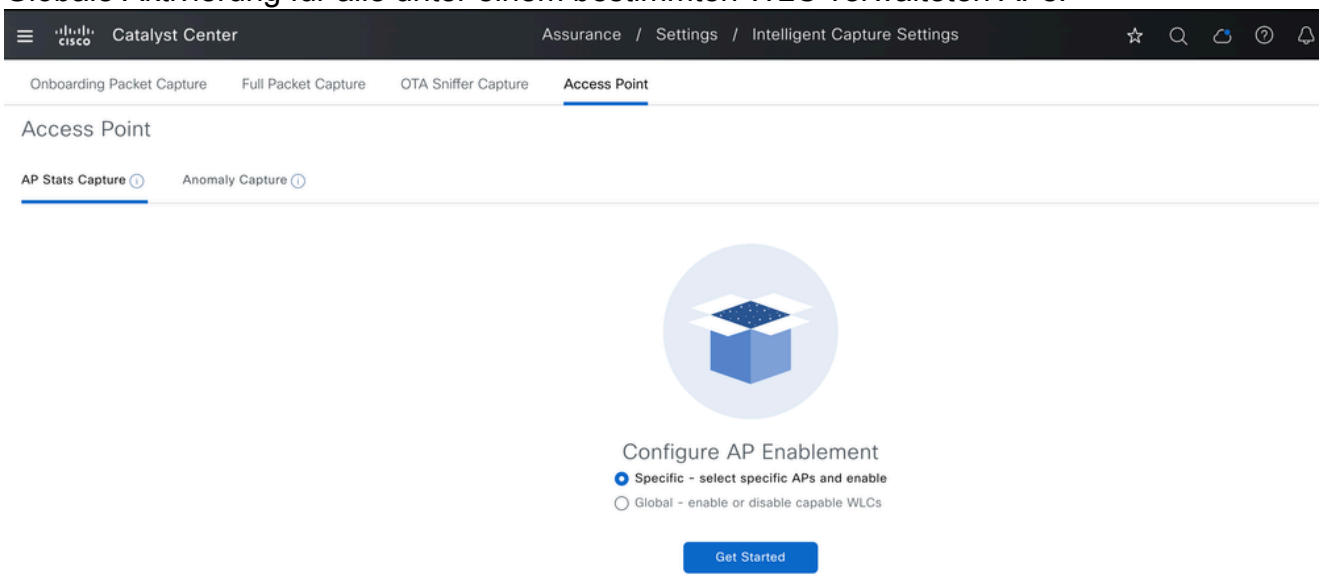
Die intelligente Erfassung für den Access Point bietet zwei Hauptfunktionen: stets verfügbare RF-Überwachung in Echtzeit, Erkennung von Anomalien und On-Demand-Übertragung über die Lufterfassung, Spektrumanalyse.

Erfassung von AP-Statistiken

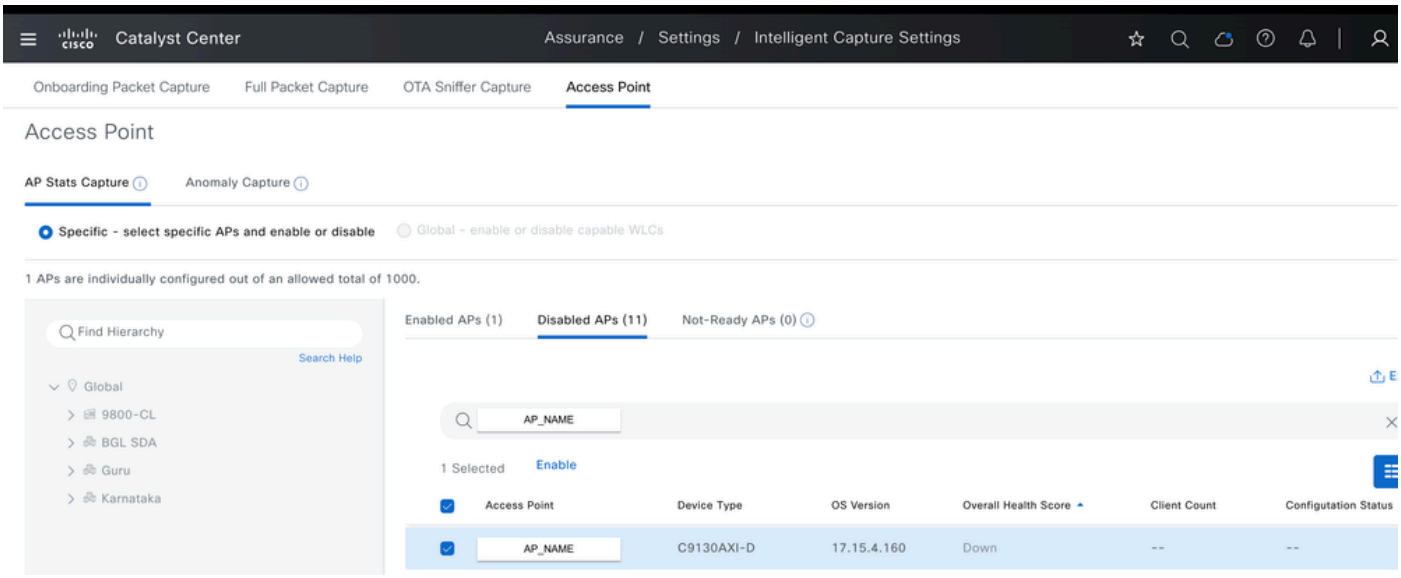
Sie können die AP-Statistikdatensammlung für einen oder mehrere Access Points aktivieren und verwalten, einschließlich AP-Funkstatistiken, WLAN-Statistiken und AP-Client-Statistiken, wobei bis zu 1.000 APs unterstützt werden.

Um die AP-Statistikerfassung zu aktivieren, navigieren Sie zu Assurance > Settings > Intelligent Capture Settings > Access Point > AP Stats Capture. Hier haben Sie die Flexibilität:

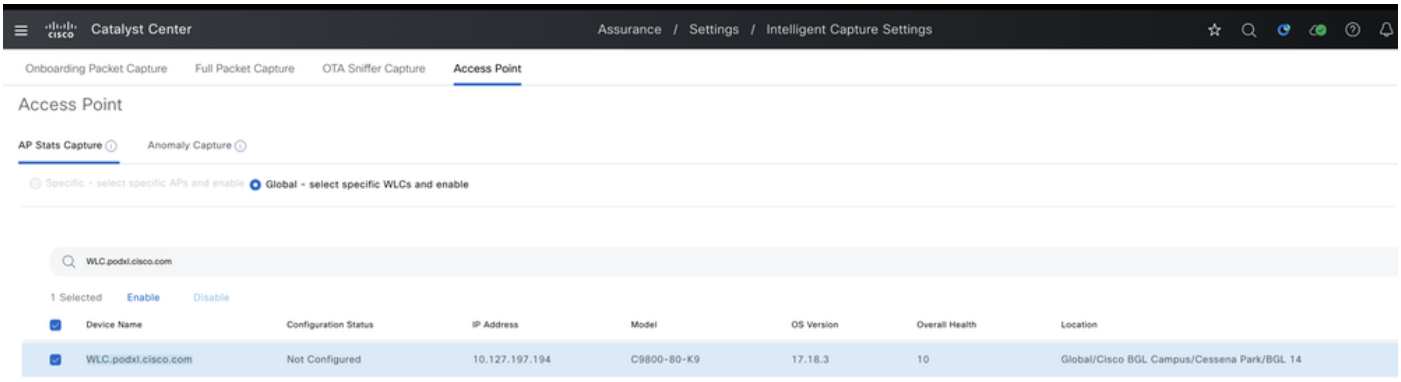
- Aktivierung für bestimmte APs (bis zu 1000) oder
- Globale Aktivierung für alle unter einem bestimmten WLC verwalteten APs.



AP-Statistikerfassungsoption

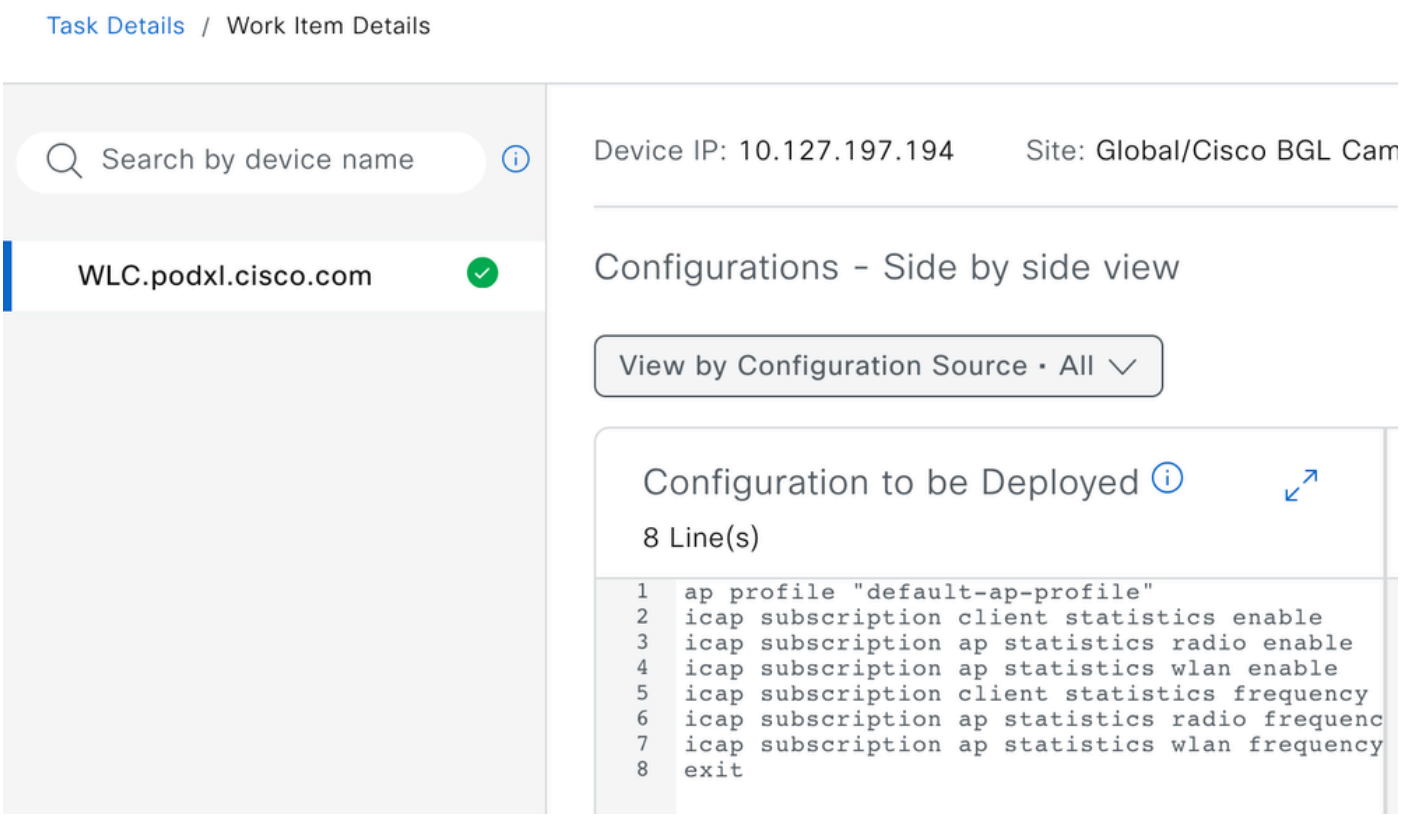


Aktivieren von AP-Statistiken Intelligente Erfassung auf bestimmten APs



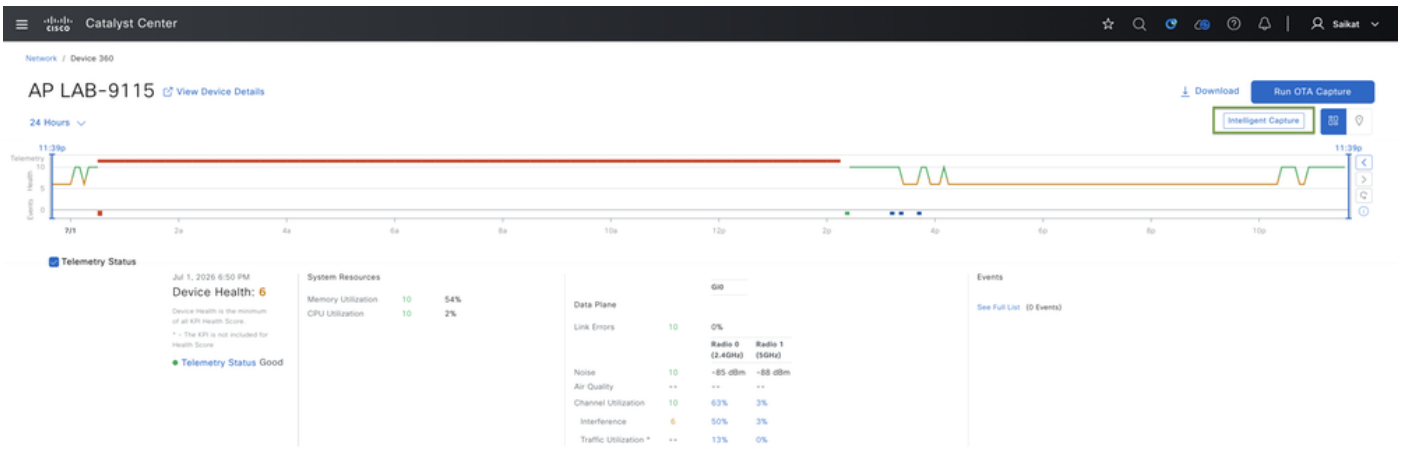
Globale intelligente Erfassung von AP-Statistiken aktivieren

Sobald die Erfassung der AP-Statistiken aktiviert ist, überträgt Catalyst Center die entsprechende Konfiguration an den WLC - entweder für die ausgewählten AP(s) oder für alle APs, je nachdem, ob sie auf der einzelnen AP-Ebene oder global auf der WLC-Ebene aktiviert wurde.

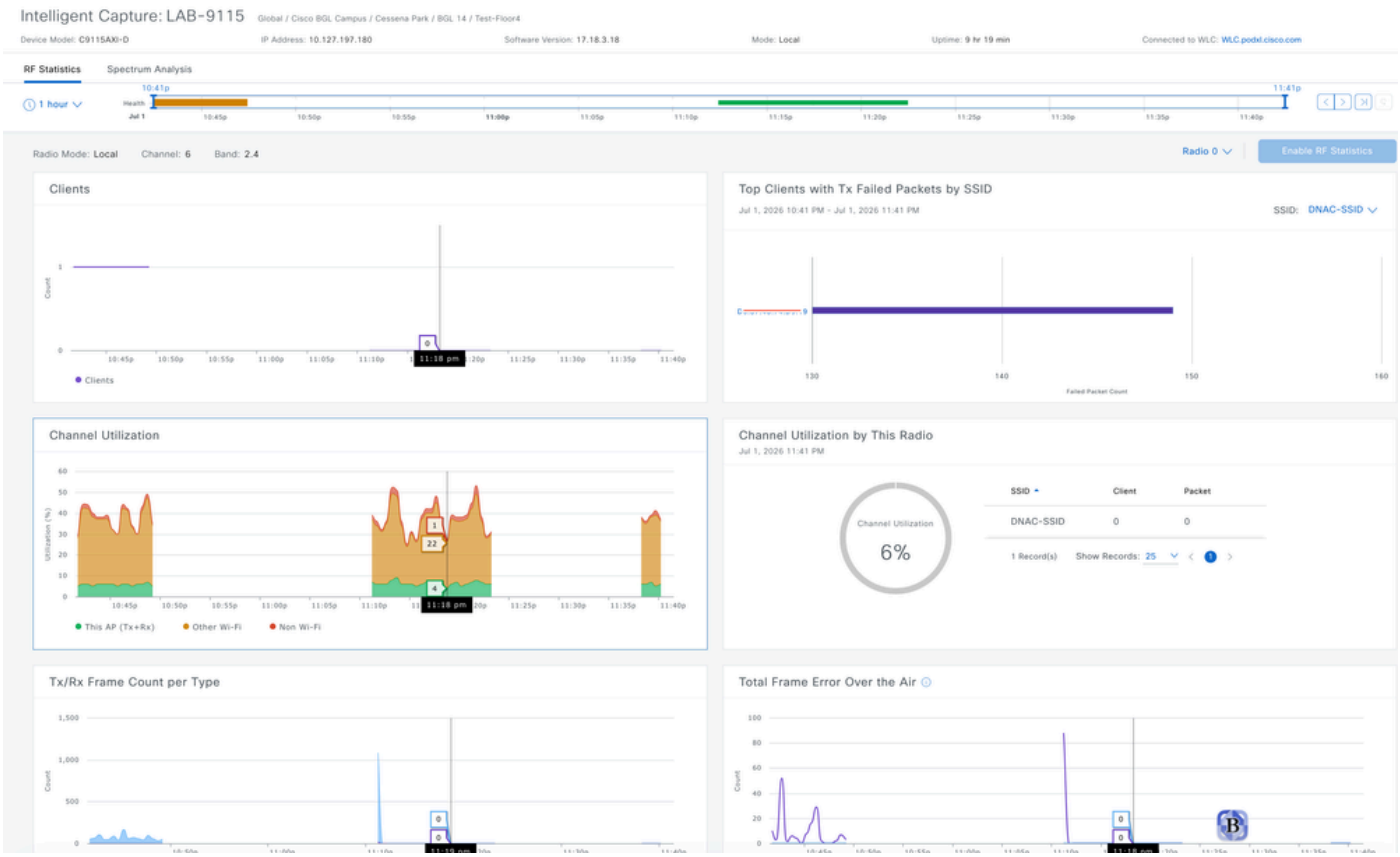


Konfiguration für Pushübertragung bei aktivierter AP-Statistikerfassung

Nachdem Sie diese Erfassung aktiviert haben, können Sie die mithilfe der intelligenten Erfassung erfassten Echtzeitdaten direkt auf der Seite Device 360 (Gerät 360) anzeigen. Darüber hinaus können Sie bei Bedarf Spektrumanalysen durchführen, um HF-Bedingungen genauer zu untersuchen.



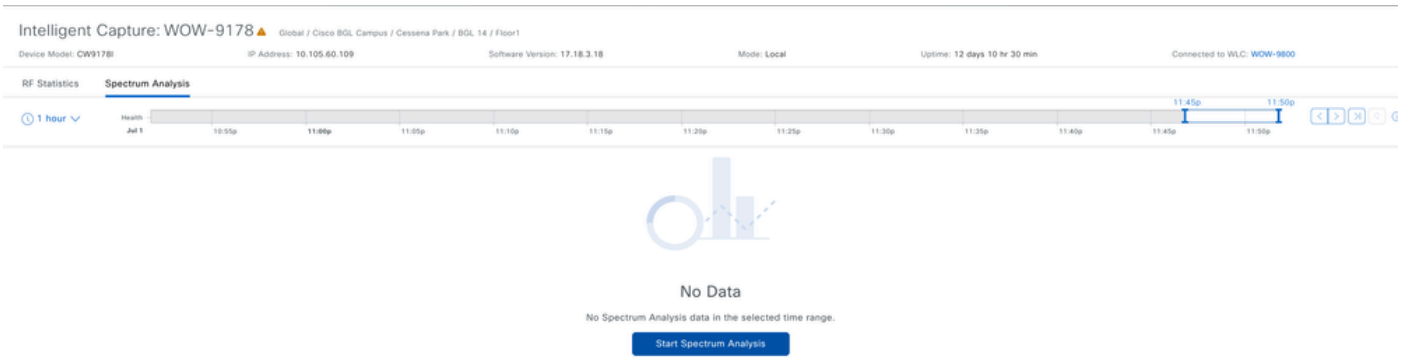
Intelligente Erfassung für AP im Gerät 360



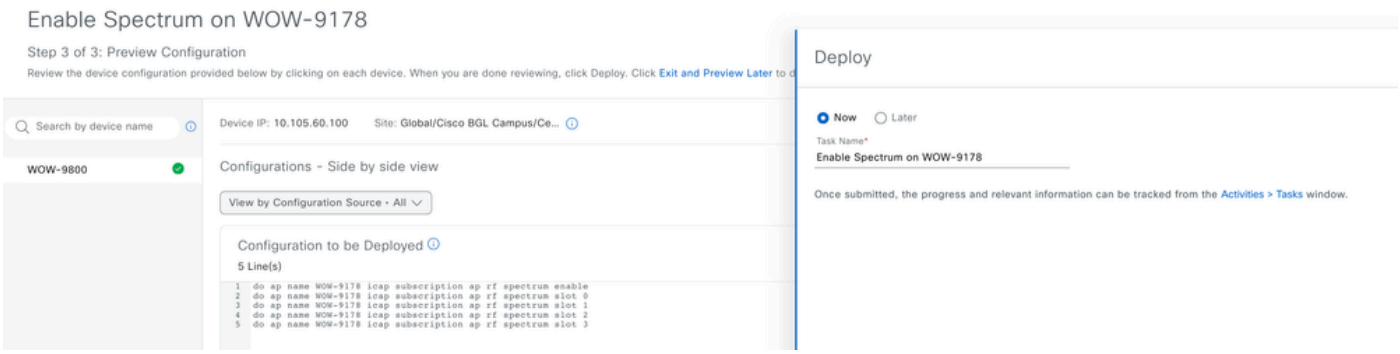
AP-Statistiken erfasst mit intelligenter Erfassung in Catalyst Center

Hier sehen Sie Echtzeitstatistiken zur Tx/Rx-Frame-Anzahl pro Typ, zur Gesamtzahl der Frame-Fehler über Funk, zu Multicast-/Broadcast-Zählern, zur Tx-Leistung und zur Geräuschkulisse, zur Kanalnutzung, zu den Top-Clients mit fehlerhaften Tx-Paketen durch SSID sowie zu Client-Daten, die mithilfe der intelligenten Erfassung für bestimmte APs erfasst wurden.

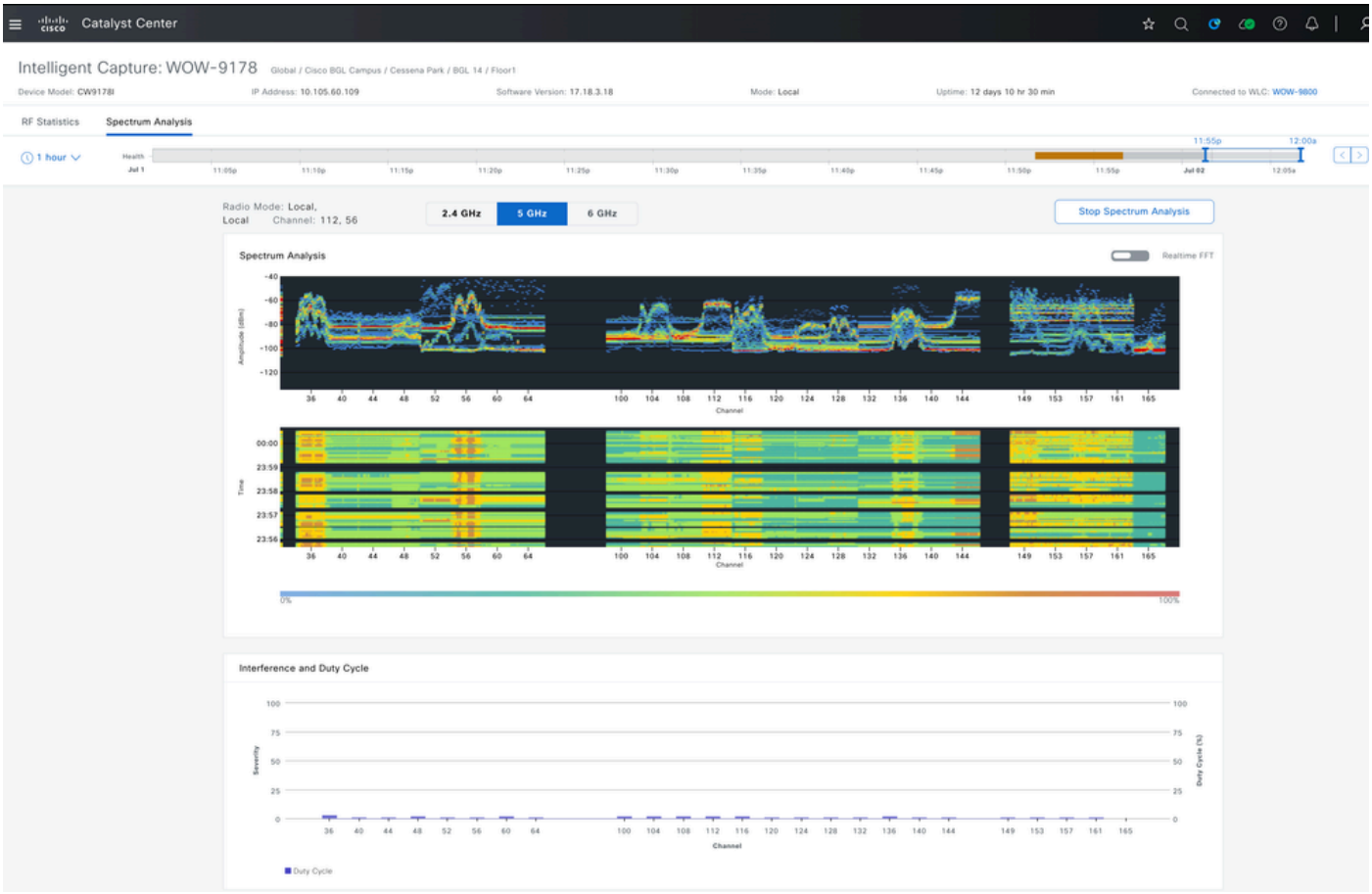
Sie können auch bei Bedarf eine Spektrumanalyse für einen einzelnen Access Point durchführen, wenn dies zur Überprüfung der Funkbedingungen erforderlich ist. Für diese Funktion ist jedoch das AP-Modell erforderlich.



Analyse des On-Demand-Spektrums



Konfiguration für Spektrumanalyse angewendet

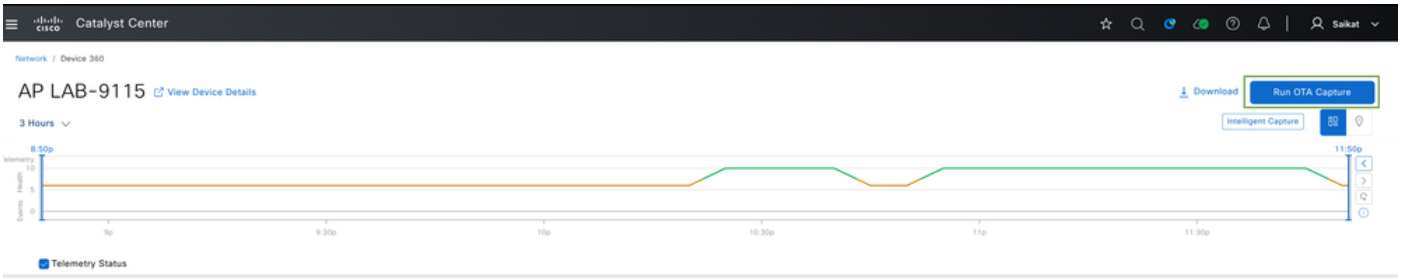


Ergebnis der Spektrumanalyse

OTA Sniffer-Erfassung

Mit Catalyst Center können Sie OTA Sniffer Capture für ein bestimmtes Funkmodul, eine bestimmte Bandbreite und einen bestimmten Kanal aktivieren. Nach der Aktivierung werden alle Wi-Fi-Datenpakete erfasst, die über diesen Funk- und Kanal übertragen werden. Sie können bis zu 2 APs auswählen, um den Sniffing durchzuführen. Beachten Sie, dass die beiden für Traffic Sniffing konfigurierten APs auf ihrem jeweiligen Funkmodul/Steckplatz in den Sniffer-Modus wechseln können, solange OTA Capture aktiviert ist.

Um dies zu aktivieren, navigieren Sie zu Bereitstellung > Bestand > Access Points, klicken Sie auf den Access Point, für den Sie OTA-Daten sammeln möchten, und wählen Sie dann OTA-Erfassung ausführen. Sie können bis zu 2 Access Points in der Nähe auswählen, um den Datenverkehr zu erfassen.

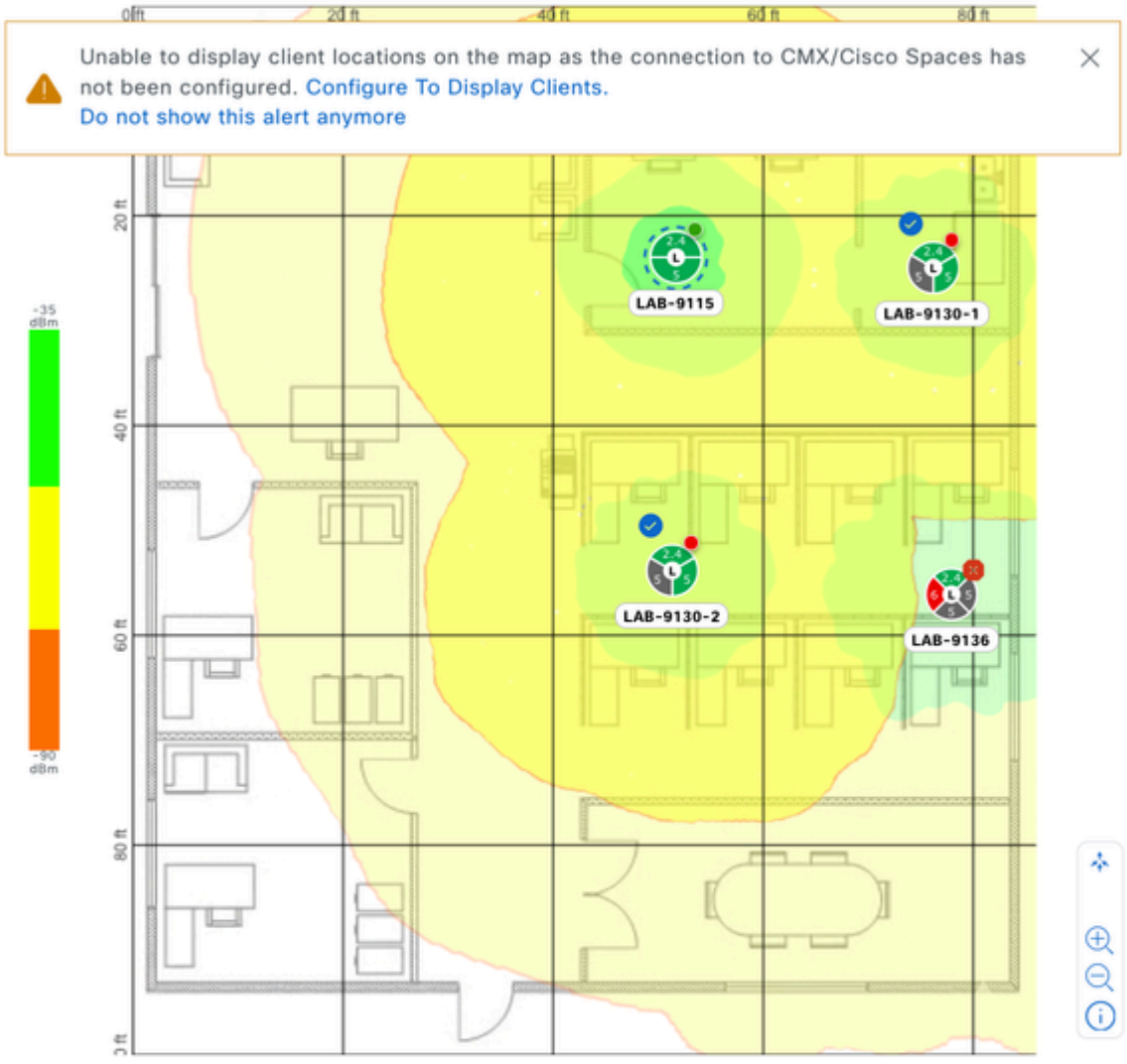


Ausführung der OTA-Erfassung auf dem Ziel-AP

Run OTA Capture

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

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



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

Auswahl benachbarter APs (bis zu 2) zum Abfangen des Datenverkehrs

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

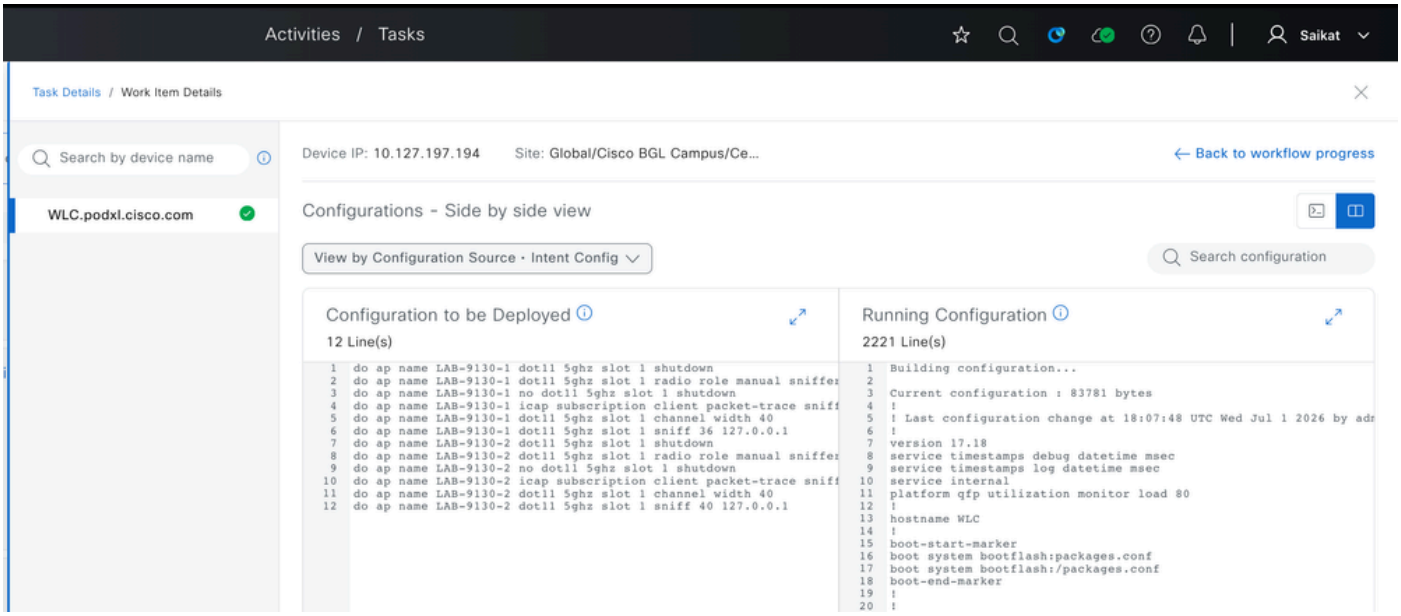
Select Radio
1 (Client Count: 0)

Select Channel Width
40

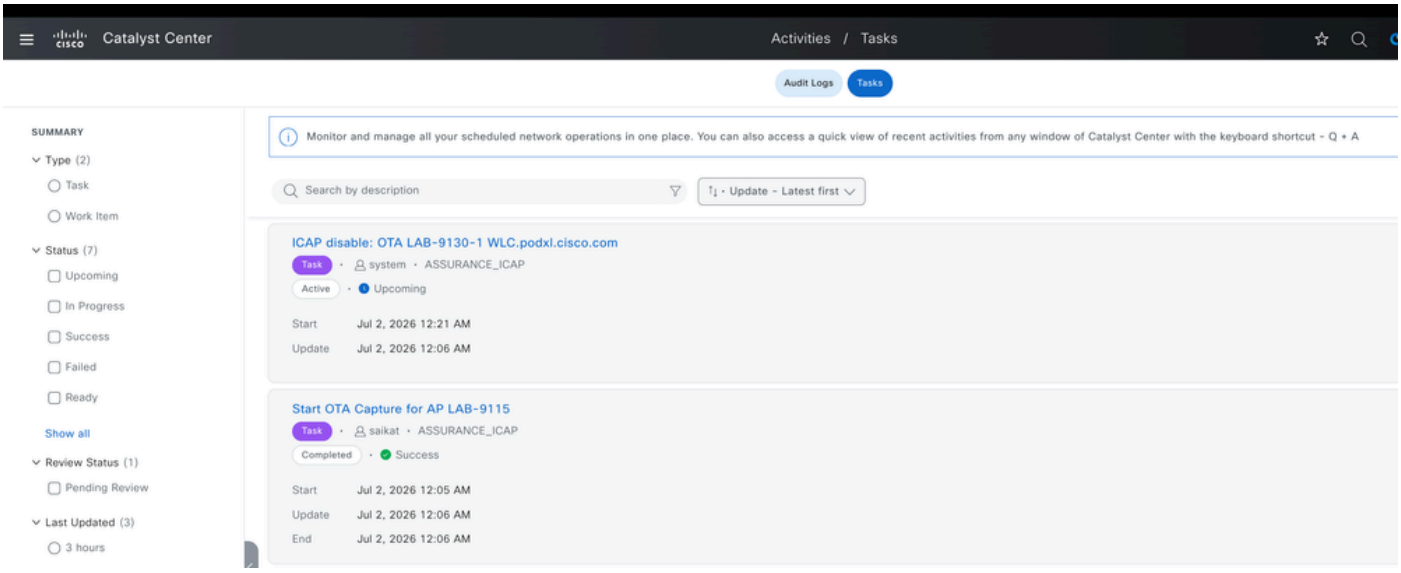
Select Channel
40

back Next

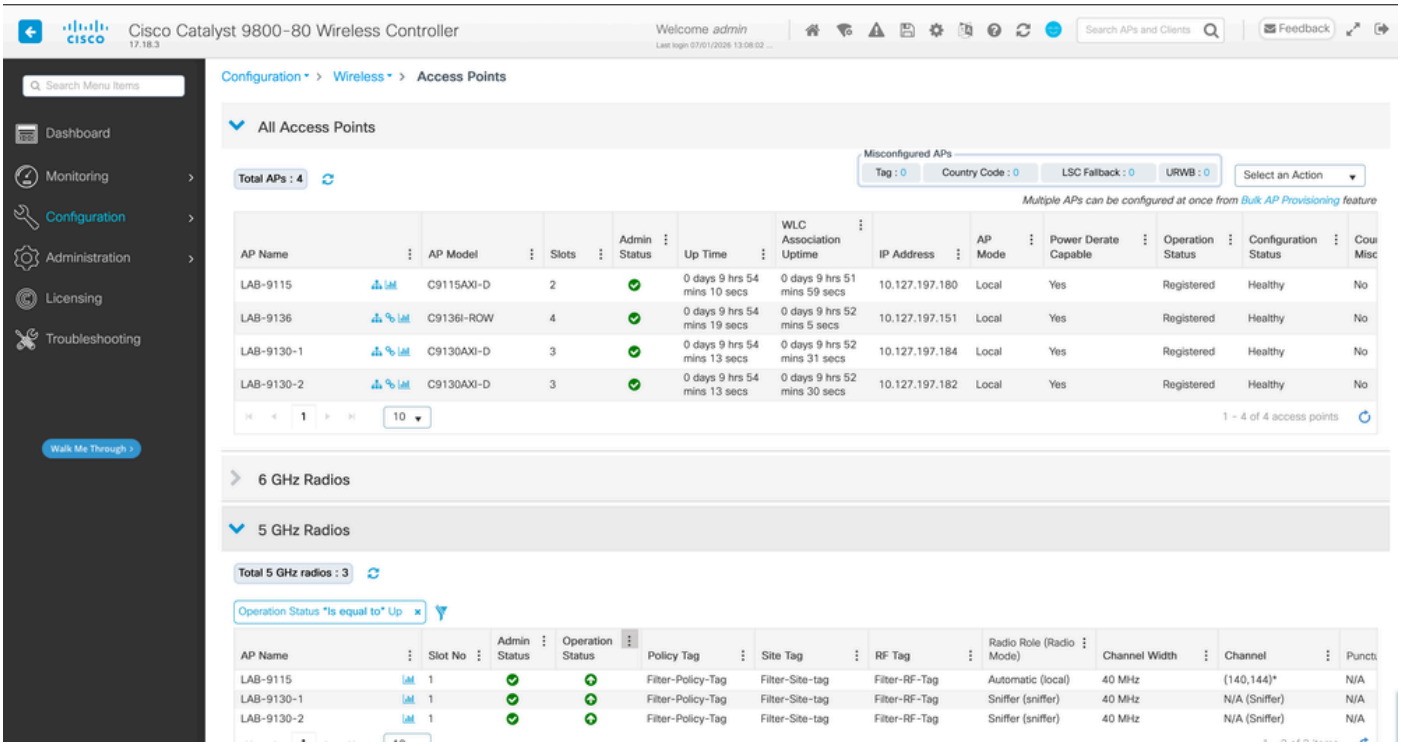
Wählen Sie "Radio", "Channel-Width" und "Channel" aus, um den Datenverkehr abzufangen.



Konfigurationsvorschau zur Aktivierung der OTA-Erfassung

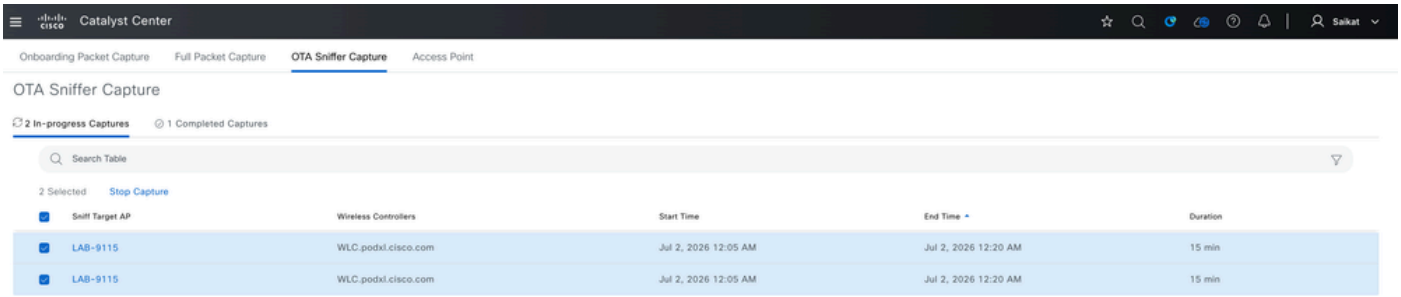


Geplante Aufgabe bei aktivierter OTA-Erfassung



Steckplatz 1 im Sniffer-Modus, damit der AP den Datenverkehr abfangen kann

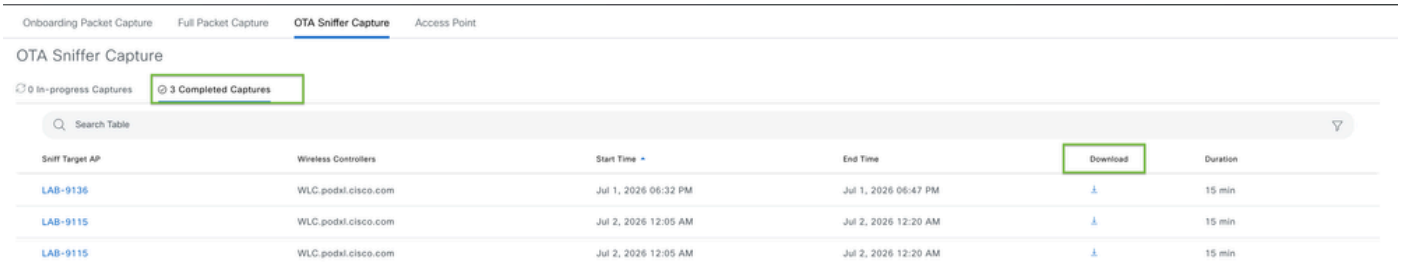
Um den Status der laufenden OTA-Erfassung zu überprüfen, navigieren Sie zu Assurance > Settings > Intelligent Capture Settings > OTA Sniffer Capture:



Status der OTA-Erfassung

Anmerkung: Catalyst Center führt diese Aufgabe standardmäßig 15 Minuten lang aus, bevor sie automatisch deaktiviert wird. Sie kann jedoch auch jederzeit manuell beendet werden.

Sobald die OTA-Erfassung abgeschlossen ist, wird sie im Abschnitt Abgeschlossene Erfassungen angezeigt, von dem Sie die Datei herunterladen können.



Abgeschlossene Erfassung - OTA Sniffer-Erfassung

Erkennung von Anomalien

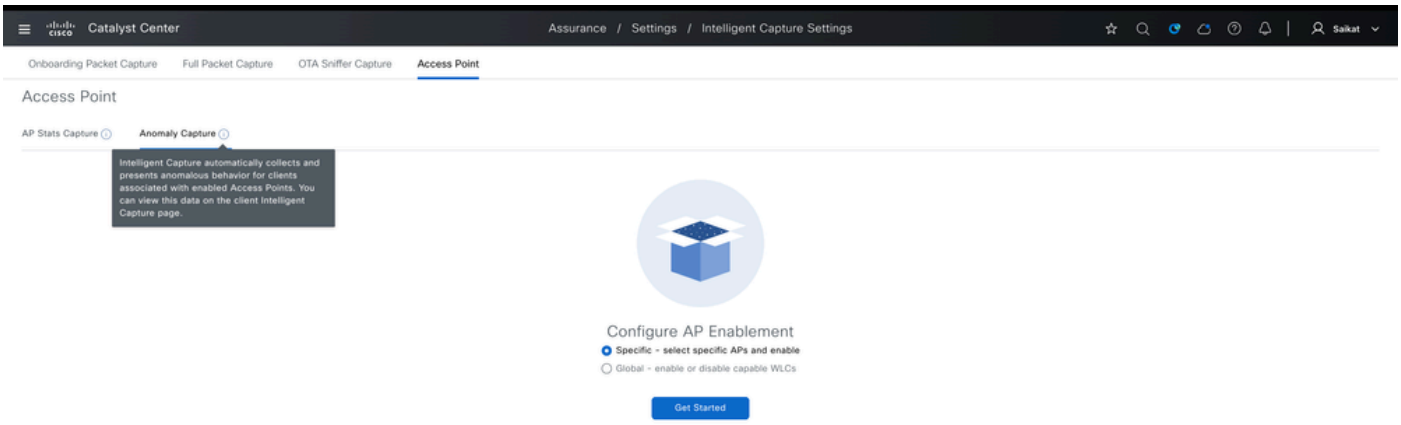
Mit dieser Funktion können Cisco APs mögliche Unregelmäßigkeiten im Verhalten der ihnen zugeordneten Wireless-Clients erkennen. Sie umfasst:

- Erkennung von Anomalien
- Anomalie-Paketerfassung
- Anomalie Individuelle Berichte
- Übersichtsberichte zu Anomalien

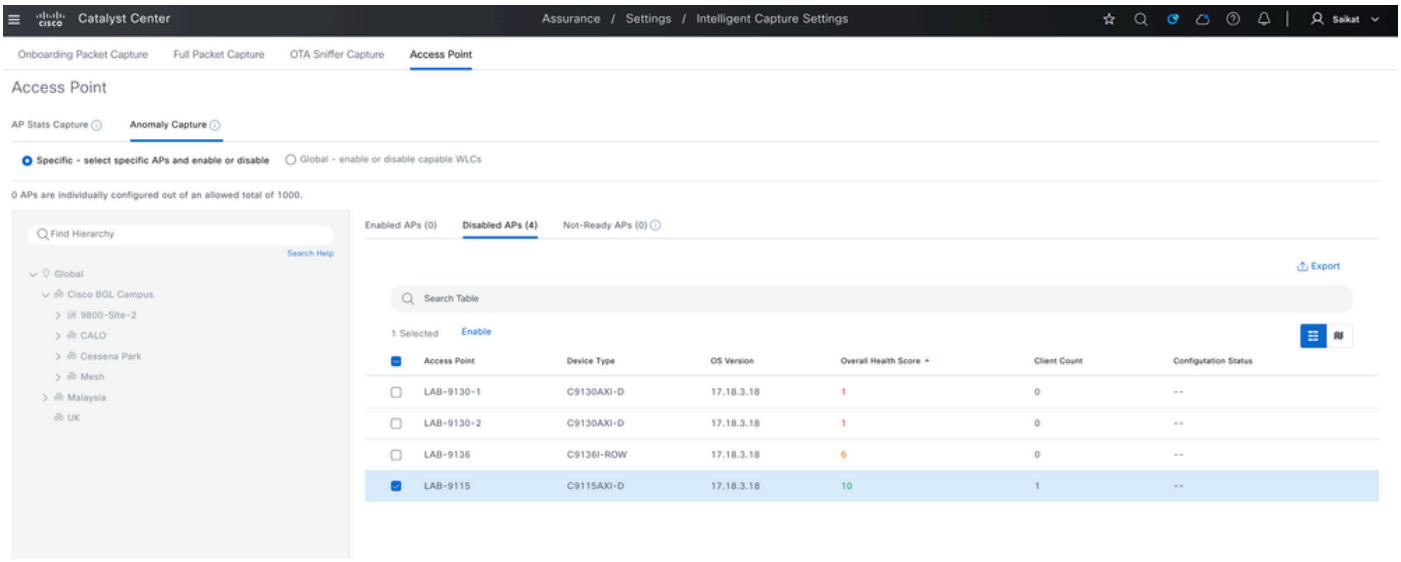
Um die AP Anomaly Capture zu aktivieren, navigieren Sie zu Assurance > Settings > Intelligent Capture Settings > Access Point > Anomaly Capture. Von hier aus können Sie zwischen folgenden Optionen wählen:

- Aktivierung für bestimmte APs (bis zu 1000) oder
- Globale Aktivierung für alle unter einem bestimmten WLC verwalteten APs.

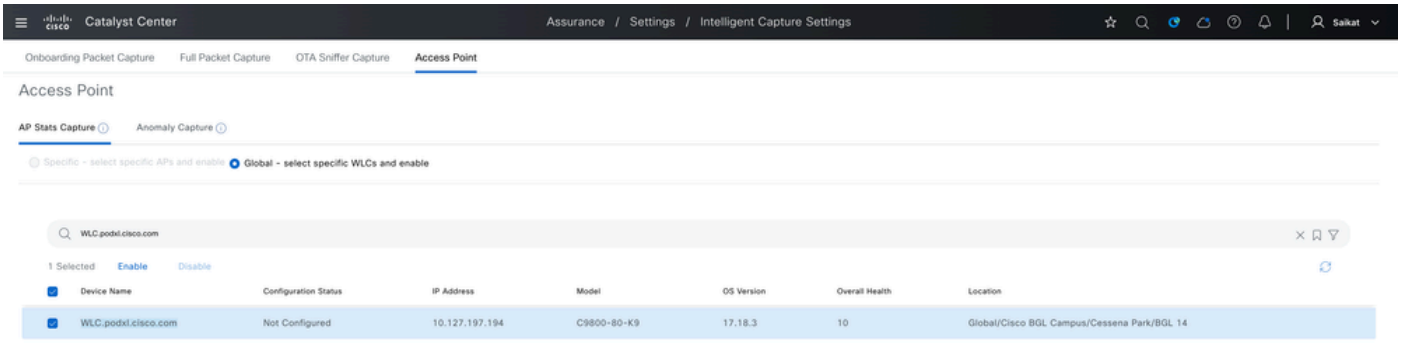
Sobald Intelligent Capture aktiviert ist, erfasst und präsentiert es automatisch ungewöhnliches Verhalten für Clients, die diesen APs zugeordnet sind. Diese Daten können auf der Seite "Client Intelligent Capture" (Client Intelligente Erfassung) angezeigt werden.



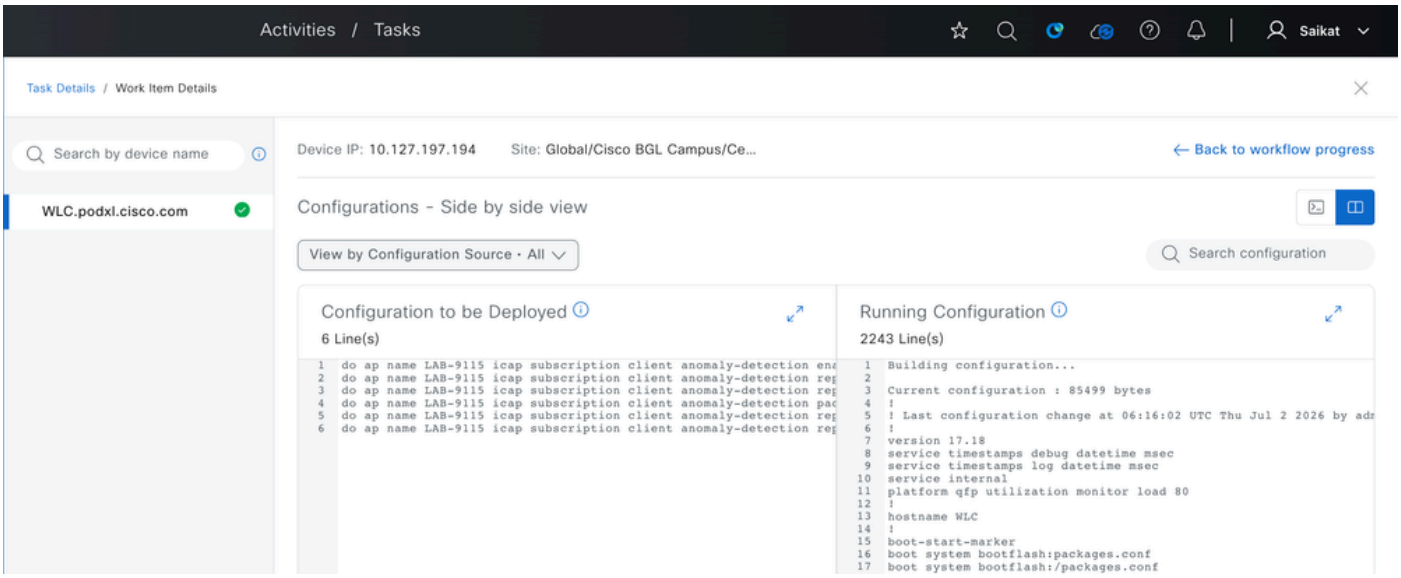
Anomalie-Erfassung konfigurieren



Anomalie-Erfassung für bestimmten AP aktivieren

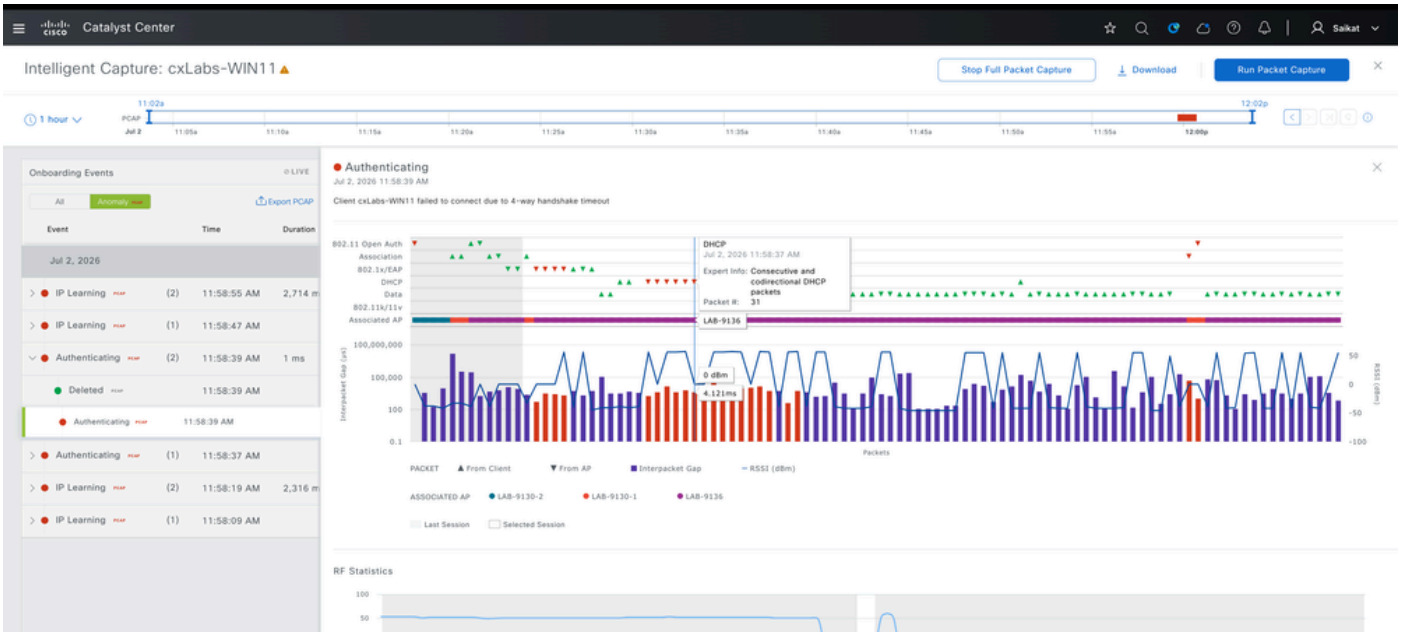


Globale Anomalie-Erfassung für bestimmten WLC aktivieren

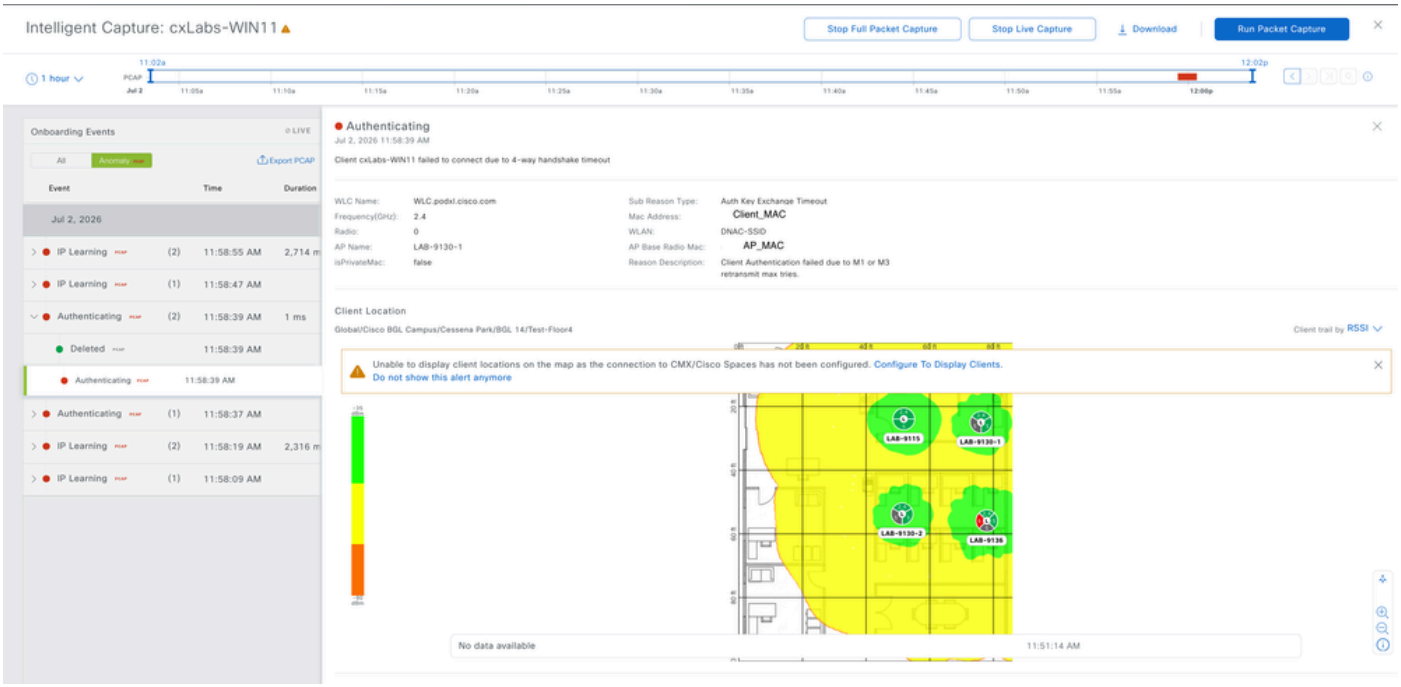


Konfigurationsvorschau für die Erfassung ungewöhnlicher Ereignisse

Nach der Aktivierung erfasst das Programm laufend ungewöhnliche Verhaltensweisen von Clients, die mit dem Access Point verbunden sind. Diese Verhaltensweisen können in den intelligenten Erfassungen (Onboarding und vollständige Erfassung) für bestimmte Client-IDs angezeigt werden.



Anomalie-Erfassungsansicht für Client



Anomalie-Erfassungsdetails für Client

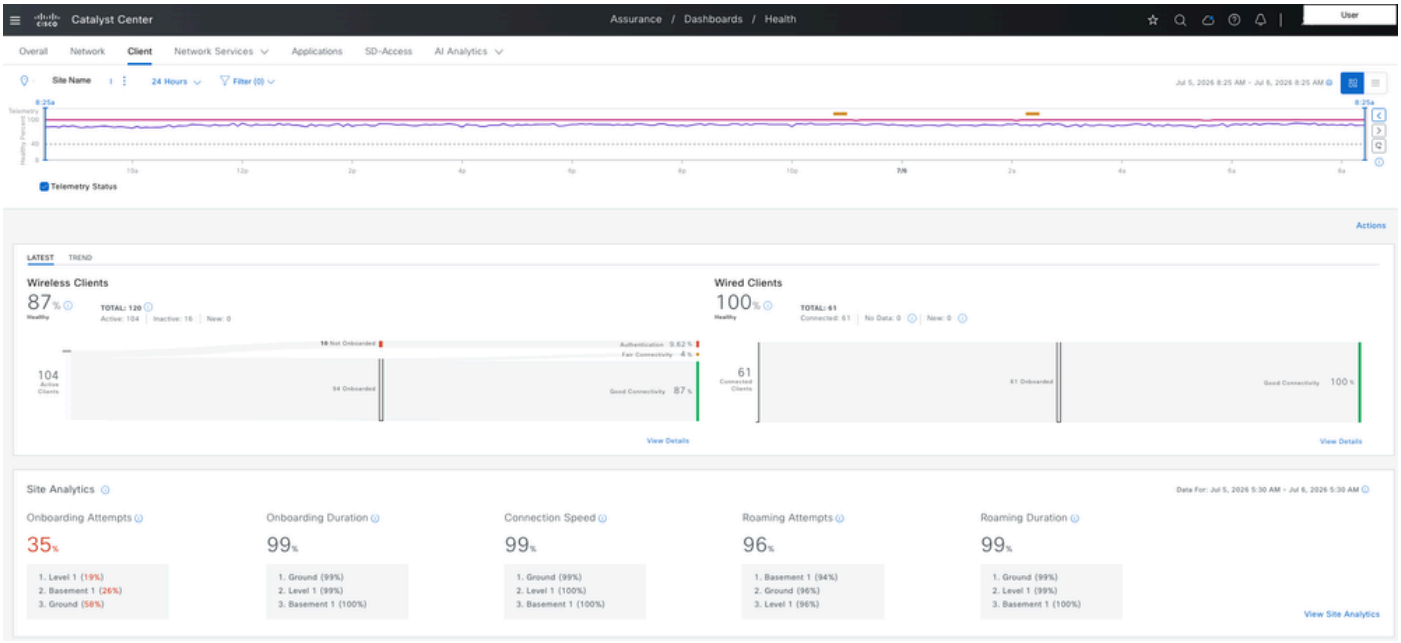
Auf diese Weise können wir unregelmäßiges oder unerwartetes Client-Verhalten (z. B. fehlgeschlagene Einbindung, Authentifizierungsprobleme oder abnorme Zuordnungsmuster) beheben, indem wir diese Ereignisse automatisch erkennen und für die APs markieren, für die sie aktiviert sind. In Kombination mit der Integration und der vollständigen Paketerfassung für bestimmte Client-IDs können Administratoren die genaue Abfolge von Ereignissen verfolgen, die zu einer Anomalie führen, sodass die Ursachen von wiederkehrenden Client-Verbindungs- oder Leistungsproblemen leichter ermittelt werden können, ohne jede Client-Sitzung manuell überwachen zu müssen.

Problem mit der Wireless-Client-Verbindung

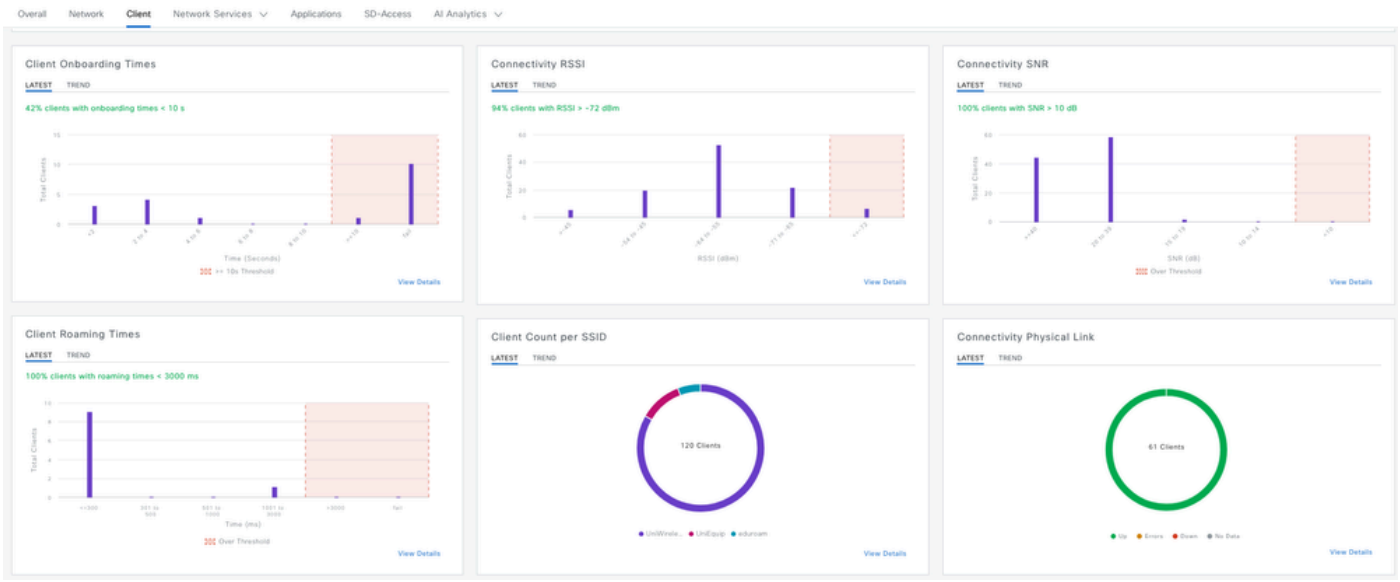
Probleme mit Wireless-Clients - Onboarding-Fehler, Roaming-Abbrüche, Funkinterferenzen oder intermittierende Verbindungen - sind häufig nur vorübergehend und schwer zu reproduzieren. Die herkömmliche abfragebasierte Überwachung ist daher für die Fehlerbehebung nicht ausreichend. Cisco Catalyst Center schließt diese Lücke durch kontinuierliche Telemetrie in Sekundenbruchteilen, die direkt von Access Points und Wireless Controllern erfasst und mit den Workflows von Gerät 360, Client 360 und intelligenter Erfassung korreliert wird. Diese telemetriegestützte Architektur ermöglicht die Wiederherstellung der genauen HF- und Protokollbedingungen zum Zeitpunkt des Ausfalls - von der Kanalnutzung und Interferenz bis hin zu 802.11-Onboarding-Frames.

Der Abschnitt "Client Health" bietet einen umfassenden, globalen Überblick über Statistiken zu Wireless-Clients an allen Standorten. Dazu gehören wichtige Metriken wie Onboarding-Leistung, RSSI, SNR, Roaming-Aktivität, SSID- und Funkverteilung, Datenraten und physischer Verbindungsstatus. Sie können diese Daten nach einem bestimmten Standort filtern und

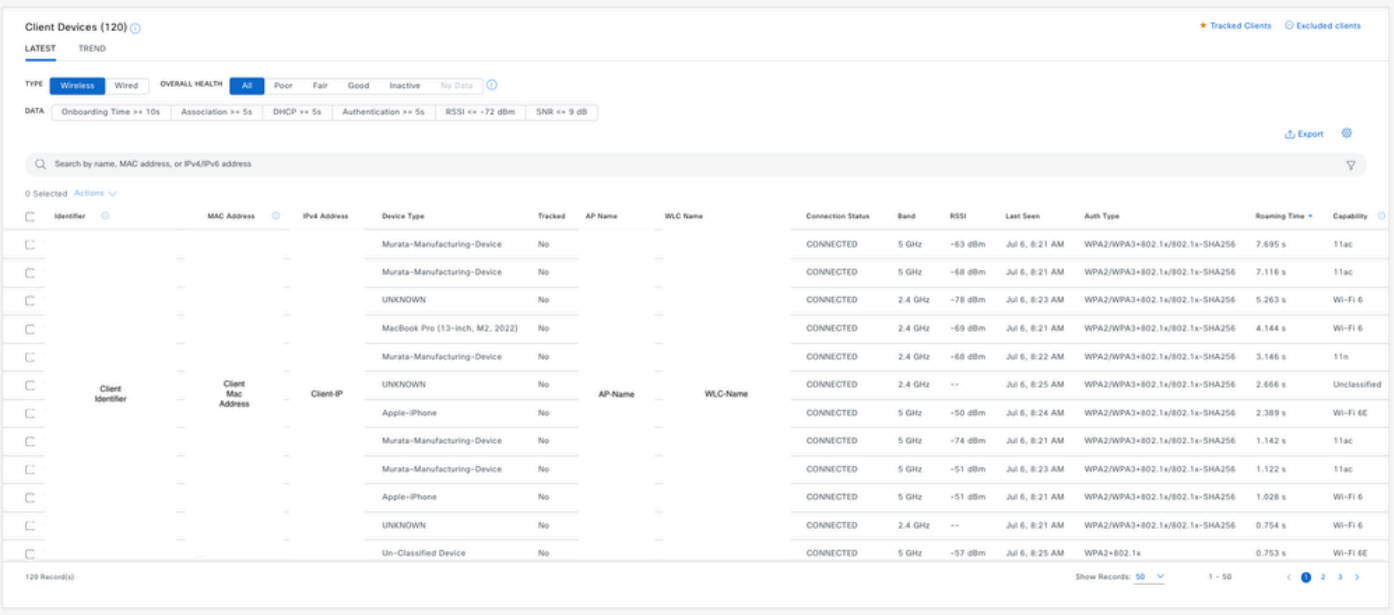
historische Trends aus den letzten 30 Tagen anzeigen. So erhalten Sie eine netzwerkweite Perspektive und Detailgenauigkeit auf Standortebene. Navigieren Sie zu Assurance > Dashboard > Health > Client.



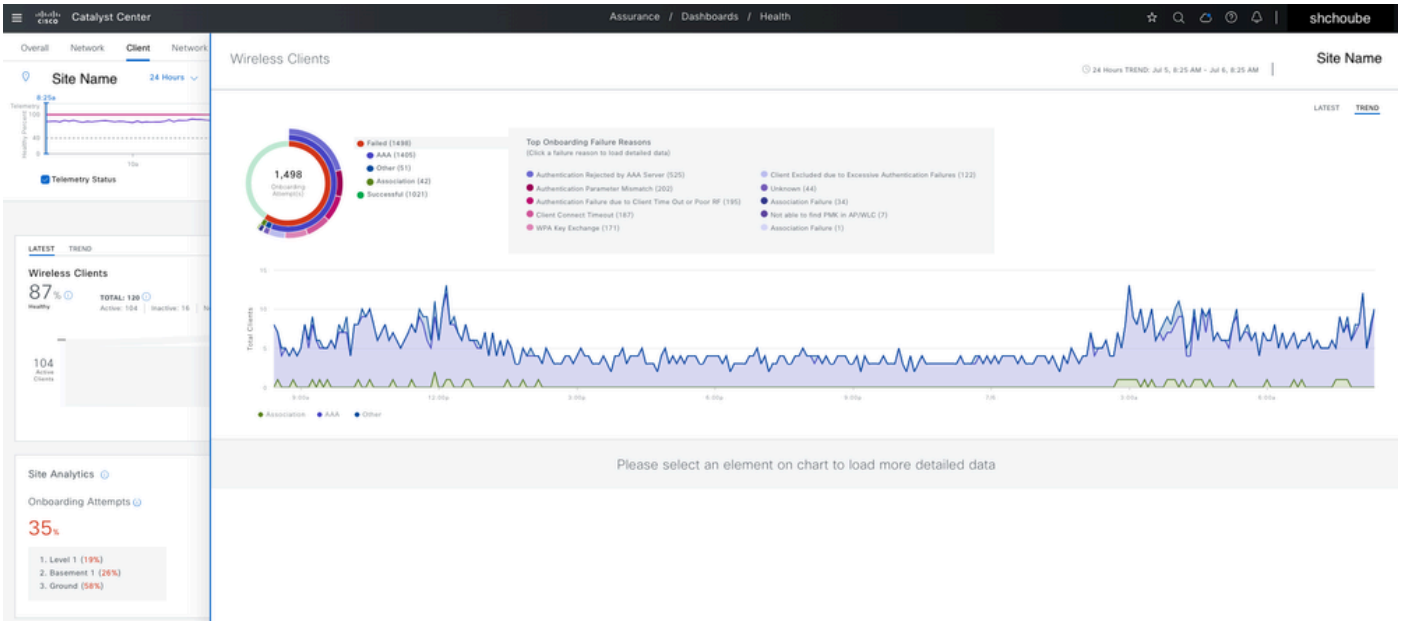
Wireless-Client - Statistiken zu Catalyst Center



Wireless-Client - Statistiken zu Catalyst Center

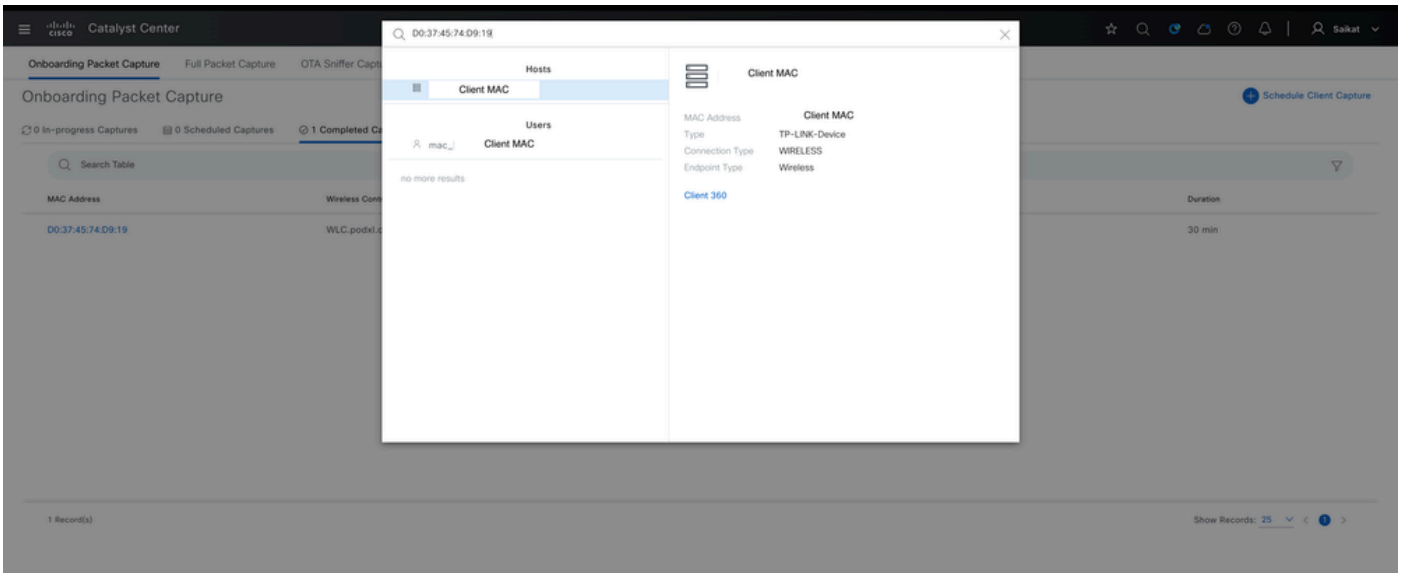


Wireless-Client - Statistiken zu Catalyst Center

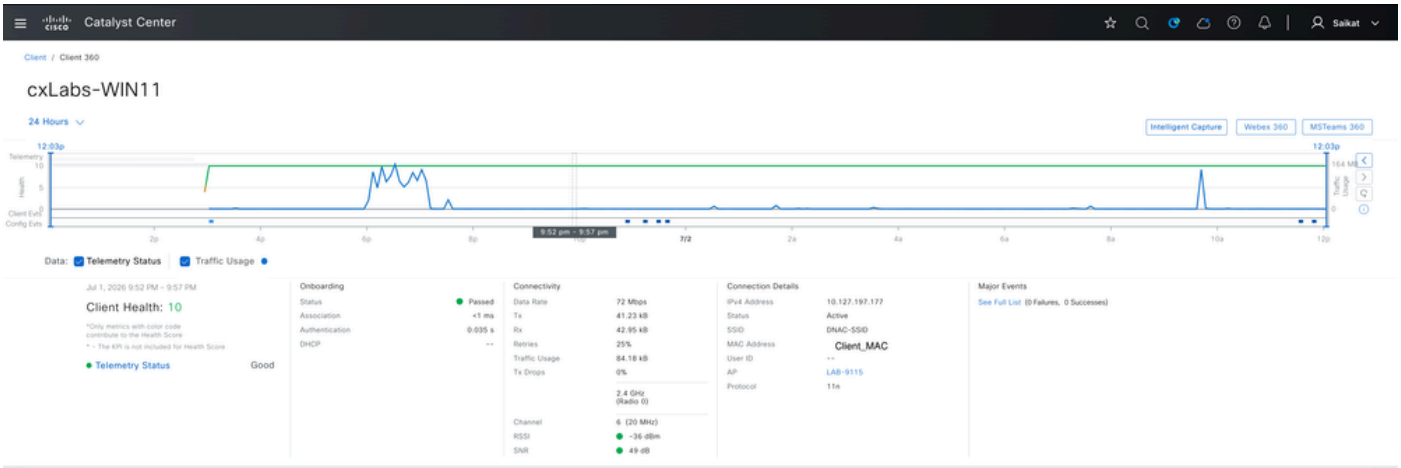


Wireless-Client - Statistiken zu Catalyst Center

Zur Fehlerbehebung bei einem bestimmten Client können Sie anhand der MAC-Adresse des Clients suchen, über die Sie zur Client 360-Ansicht gelangen. Diese Seite enthält detaillierte, kundenspezifische Statistiken, einschließlich Onboarding-Verlauf, Anbindungsereignisse, RF-Metriken und Sitzungsdetails, die sich exklusiv auf den jeweiligen Client beziehen und eine präzise Ursachenanalyse einzelner Client-Probleme ermöglichen.

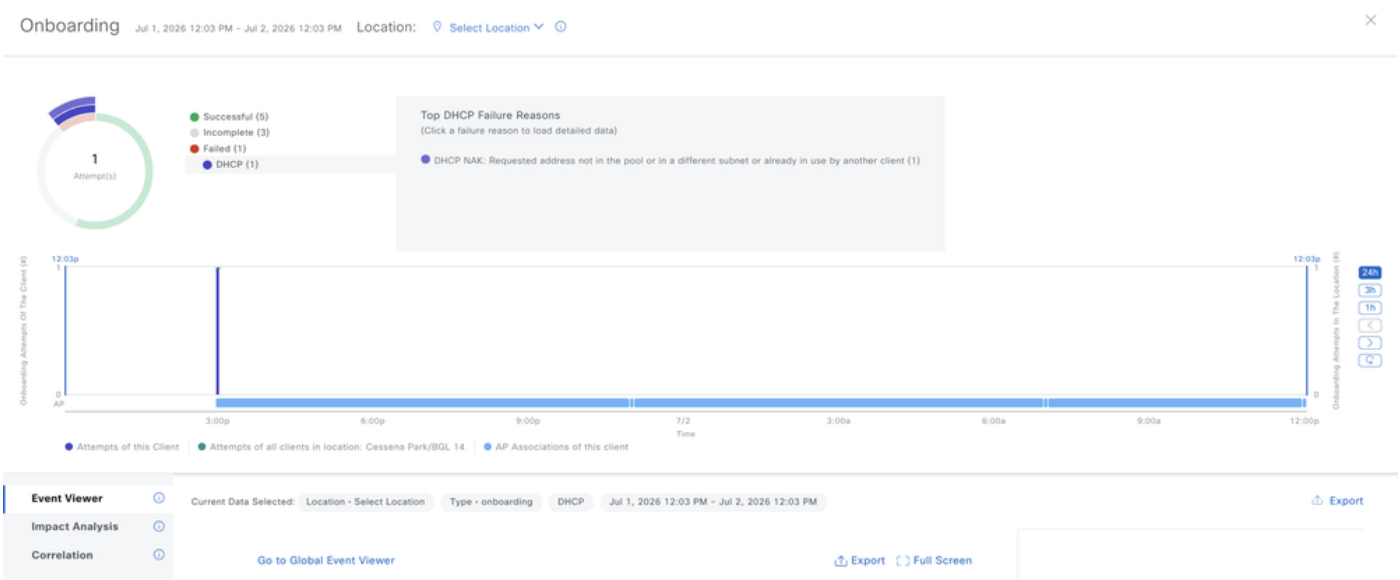


Spezifischer Client für MAC-Adressgerät 360

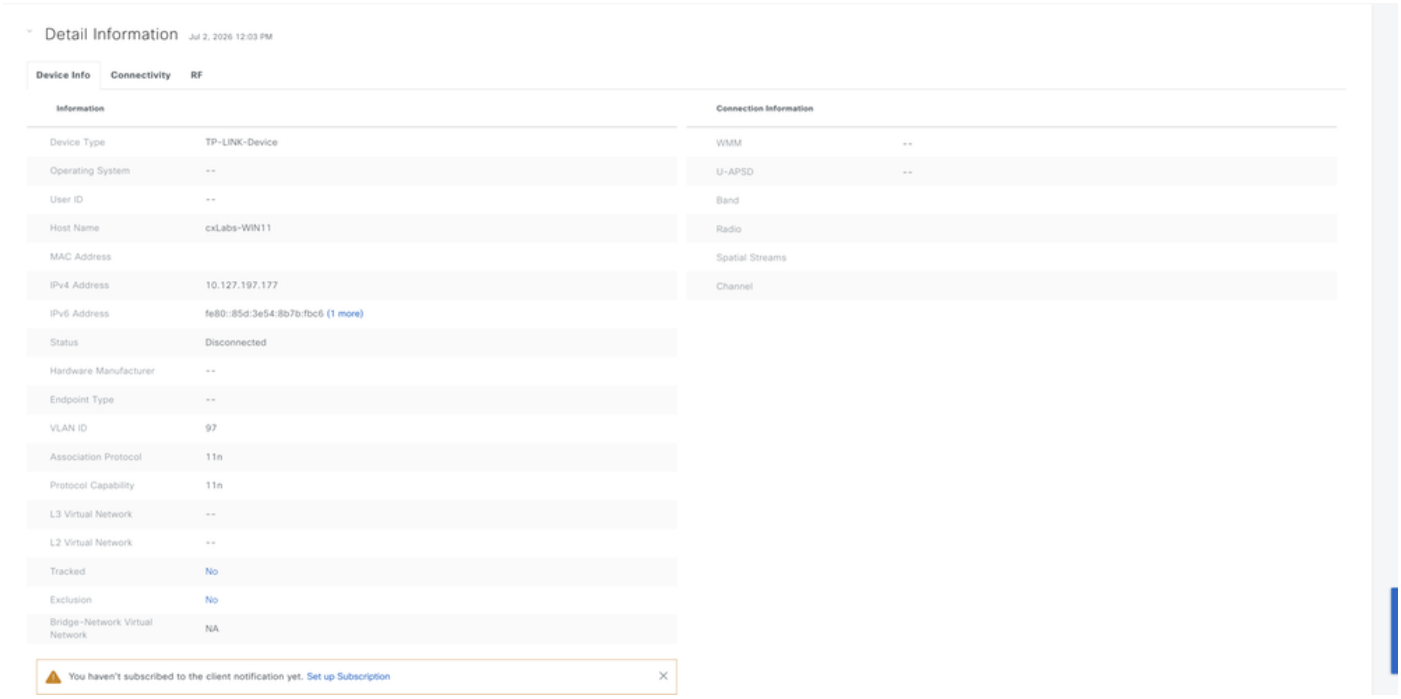


Telemetrie + Zustandsstatus des Clients

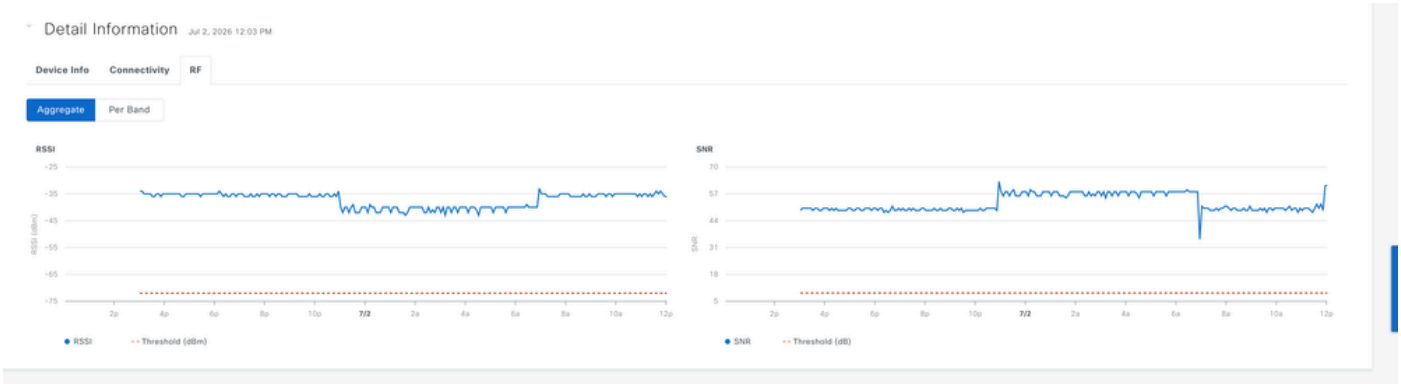
Gesamtübersicht für Client



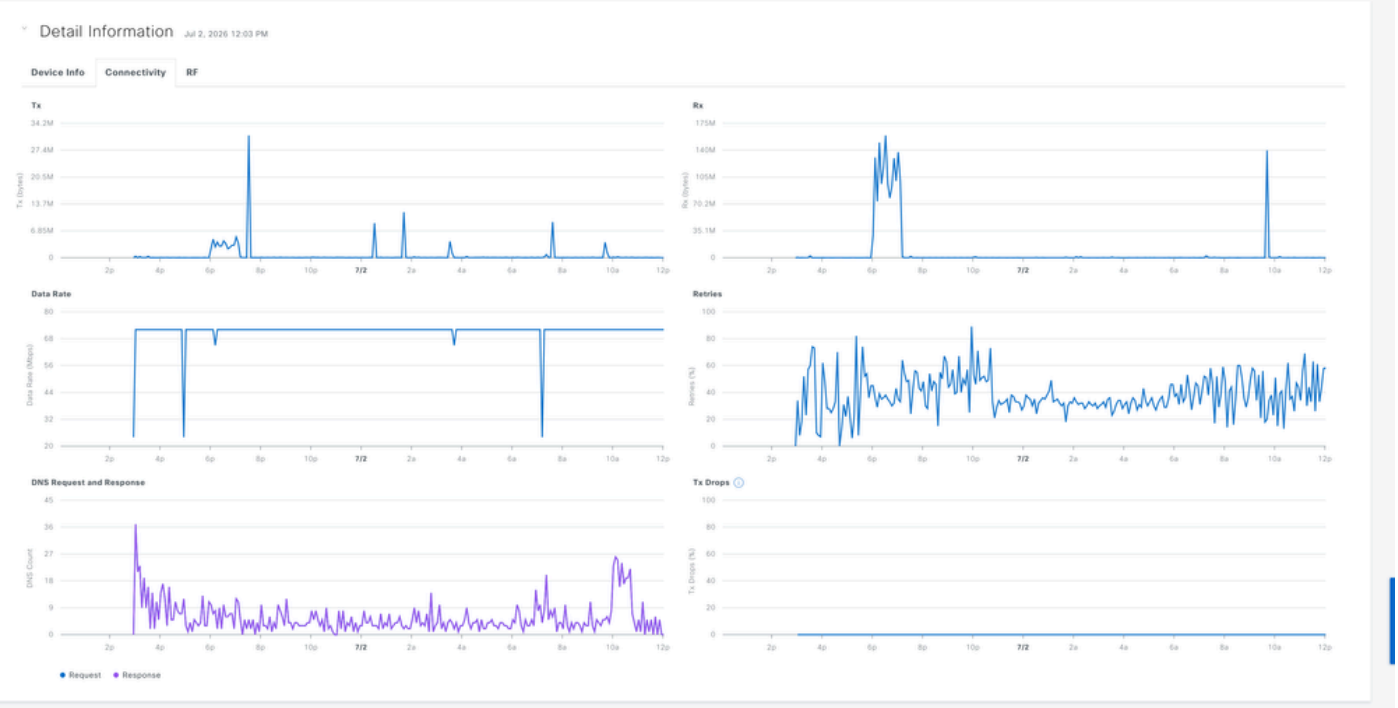
Für den Client gemeldetes Ereignis im Detail



Details zum Client-Gerät



RF-Statistik für Client



Verbindungsstatistiken für Client

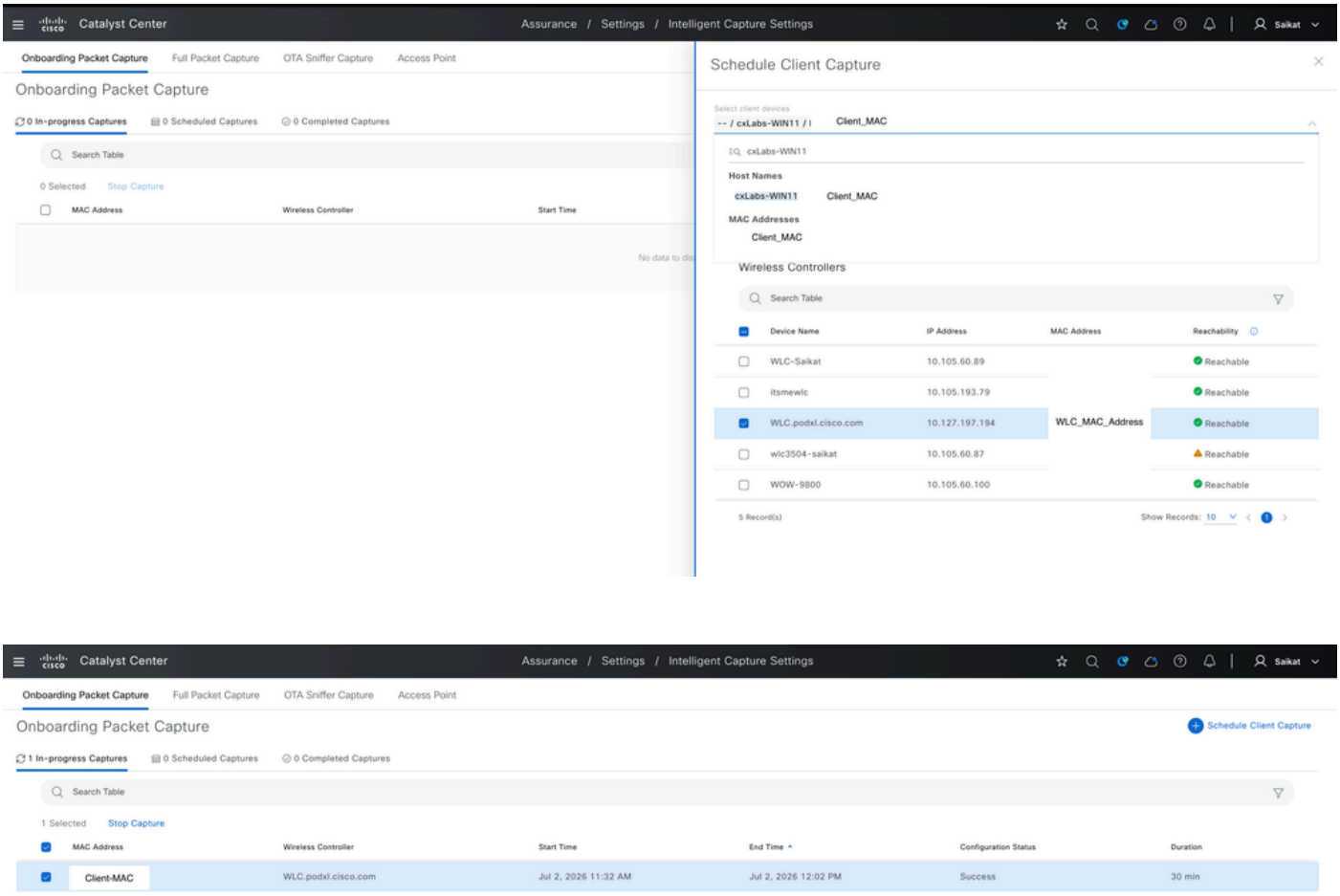
Intelligente Erfassung für Wireless-Clients

Intelligent Capture (iCAP) unterstützt die Behebung von Verbindungsproblemen bei Wireless-Clients, indem reale Daten auf Paketebene direkt aus Catalyst Center erfasst werden. Er kann 802.11-Management-, DHCP- und EAP-Frames erfassen, um festzustellen, wo ein Verbindungsversuch fehlschlägt, und unverschlüsselte Daten und Managementpakete für einen bestimmten Client erfassen, um Fehler beim Onboarding, bei Zugänglichkeits- und Anwendungsproblemen zu beheben. Sie können auch festlegen, dass intelligente Aufzeichnungen zu einem späteren Zeitpunkt ausgeführt werden. Die Standarddauer der Sitzung beträgt 30 Minuten und kann auf acht Stunden festgelegt werden.

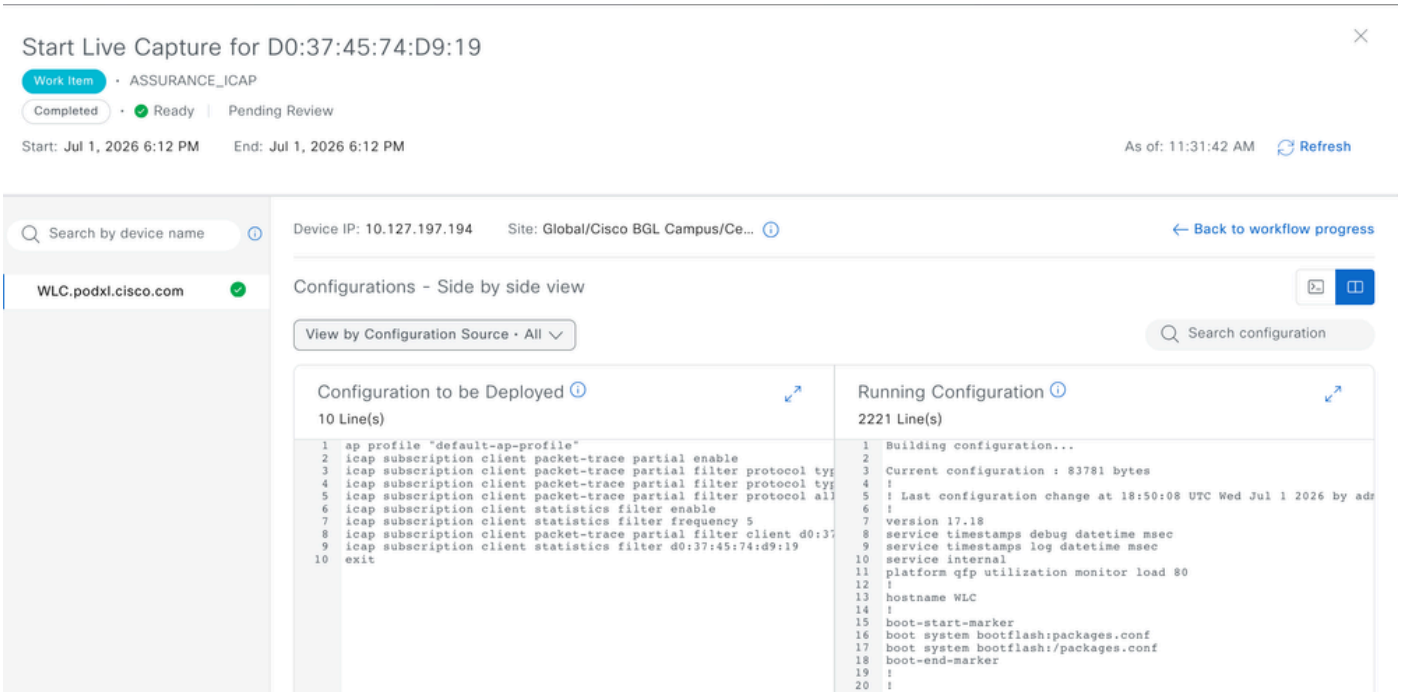
Onboarding-Paketerfassung

Onboarding Packet Capture zeichnet die Reihenfolge der Pakete auf, die ein Client-Gerät austauscht, wenn es versucht, dem Wireless-Netzwerk beizutreten, einschließlich 802.11-Management-Frames (wie Assoziierungs- und Authentifizierungsanforderungen), DHCP-Pakete und EAP-Pakete, die während der 802.1X-Authentifizierung verwendet werden. Darüber hinaus erfasst es die RF-Statistiken der Clients und gibt Einblick in die Signalbedingungen zum genauen Zeitpunkt des Onboarding. Diese Erfassungen sind nützlich für die Fehlerbehebung in einem Szenario, in dem ein Client keine Verbindung herstellen kann, und helfen, den genauen Punkt zu bestimmen, in dem der Fehler auftritt - ob während der Zuordnung, Authentifizierung oder IP-Adresszuweisung. Standardmäßig ist die Onboarding-Paketerfassung auf dem letzten mit dem Client verbundenen Wireless Controller aktiviert. Sie können bis zu drei Wireless-Controller auswählen, um das Client-Roaming-Szenario abzudecken.

Um die Onboarding-Paketerfassung zu aktivieren, navigieren Sie zu Assurance > Settings > Intelligent Capture Settings > Onboarding Capture > Schedule Client Capture (oben rechts) > Search for Client Identifier (MAC-Adresse).

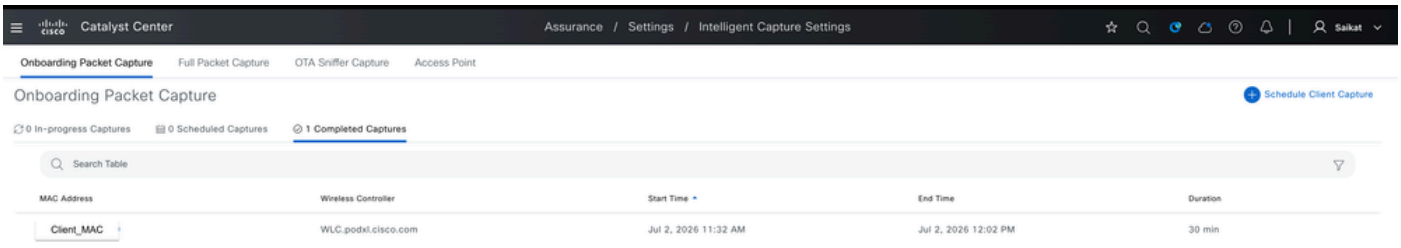


Geplante Erfassung des Onboarding

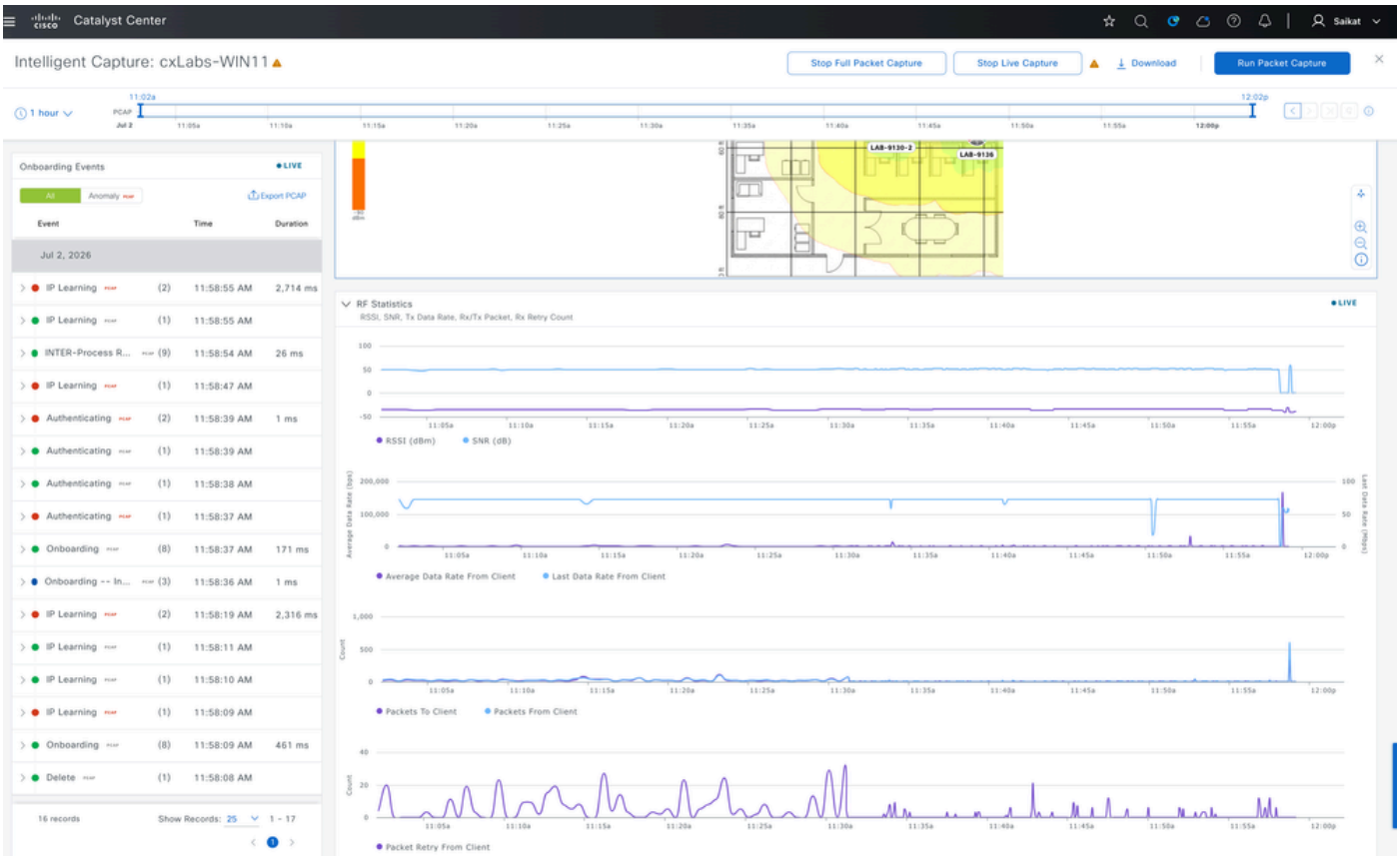


Konfigurationsvorschau für Onboarding-Erfassung

Die Onboarding-Erfassung kann manuell gestoppt oder automatisch deaktiviert werden, sobald die geplante Dauer (von 30 Minuten bis 8 Stunden) abgelaufen ist. Sobald die Erfassung beendet ist, wird sie unter "Abgeschlossene Erfassungen" angezeigt. Dort können Sie auf die MAC-Adresse des Clients klicken, um die detaillierten Erfassungsdaten anzuzeigen und die Datei zur weiteren Analyse im PCAP-Format zu exportieren.



Abgeschlossene Onboarding-Erfassung

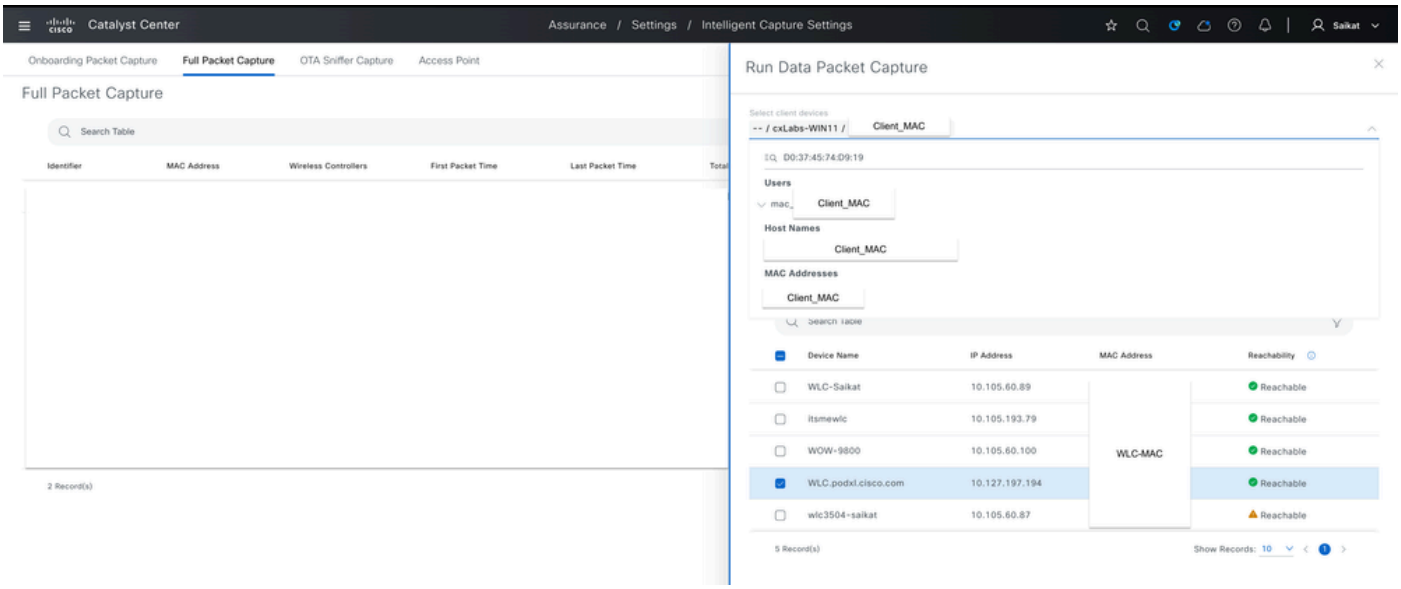


Beispiel für eine vollständige Erfassung des Onboarding-Prozesses

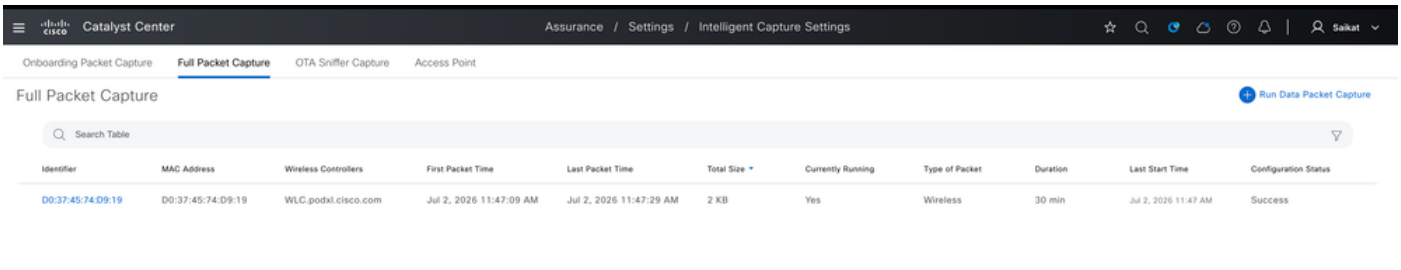
Vollständige Paketerfassung

Vollständige Packet Capture-Sitzung kann vollständige Daten für einen bestimmten Client erfassen und bietet eine umfassende Transparenz auf Paketebene des laufenden Wireless-Datenverkehrs der Clients. So können wir sowohl Daten als auch Verwaltungspakete eingehend untersuchen, um Zugriffsprobleme, Probleme mit der Anwendungsleistung oder andere Verbindungsanomalien zu beheben, die über die üblichen RF-Statistiken hinausgehen. Es kann bis zu 1 GB an rollenden Daten für einen bestimmten Client erfassen und behält die neuesten Daten bis zum Maximum bei.

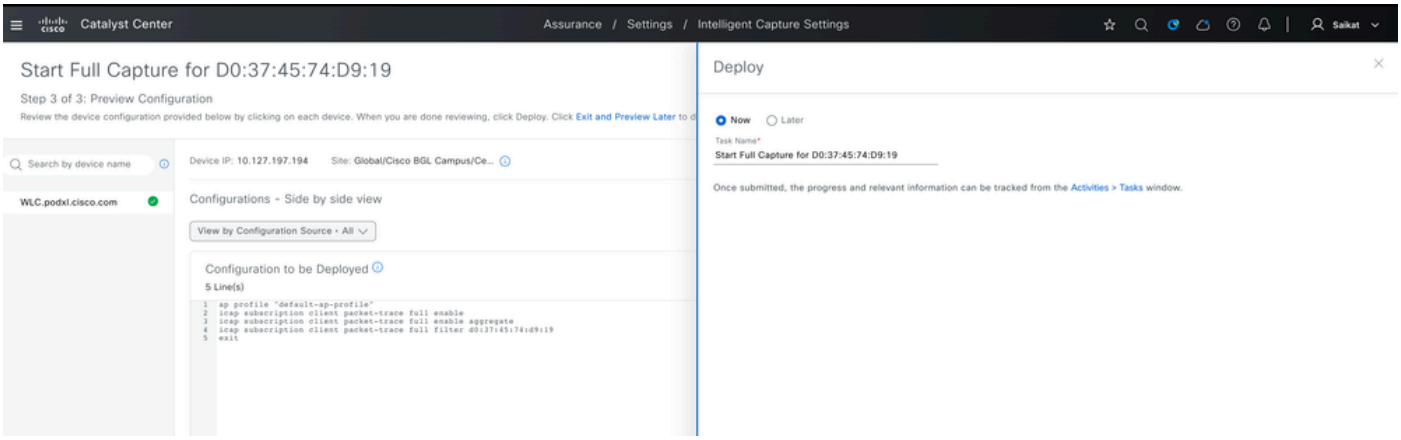
So aktivieren Sie Full Packet CaptureNavigate to Assurance > Settings > Intelligent Capture Settings > Onboarding Capture > Run Data Capture (in der oberen rechten Ecke) > Search for Client Identifier (MAC-Adresse):



Vollständige Paketerfassung für Client



Geplante vollständige Paketerfassung für Client



Konfigurationsvorschau für vollständige Paketerfassung

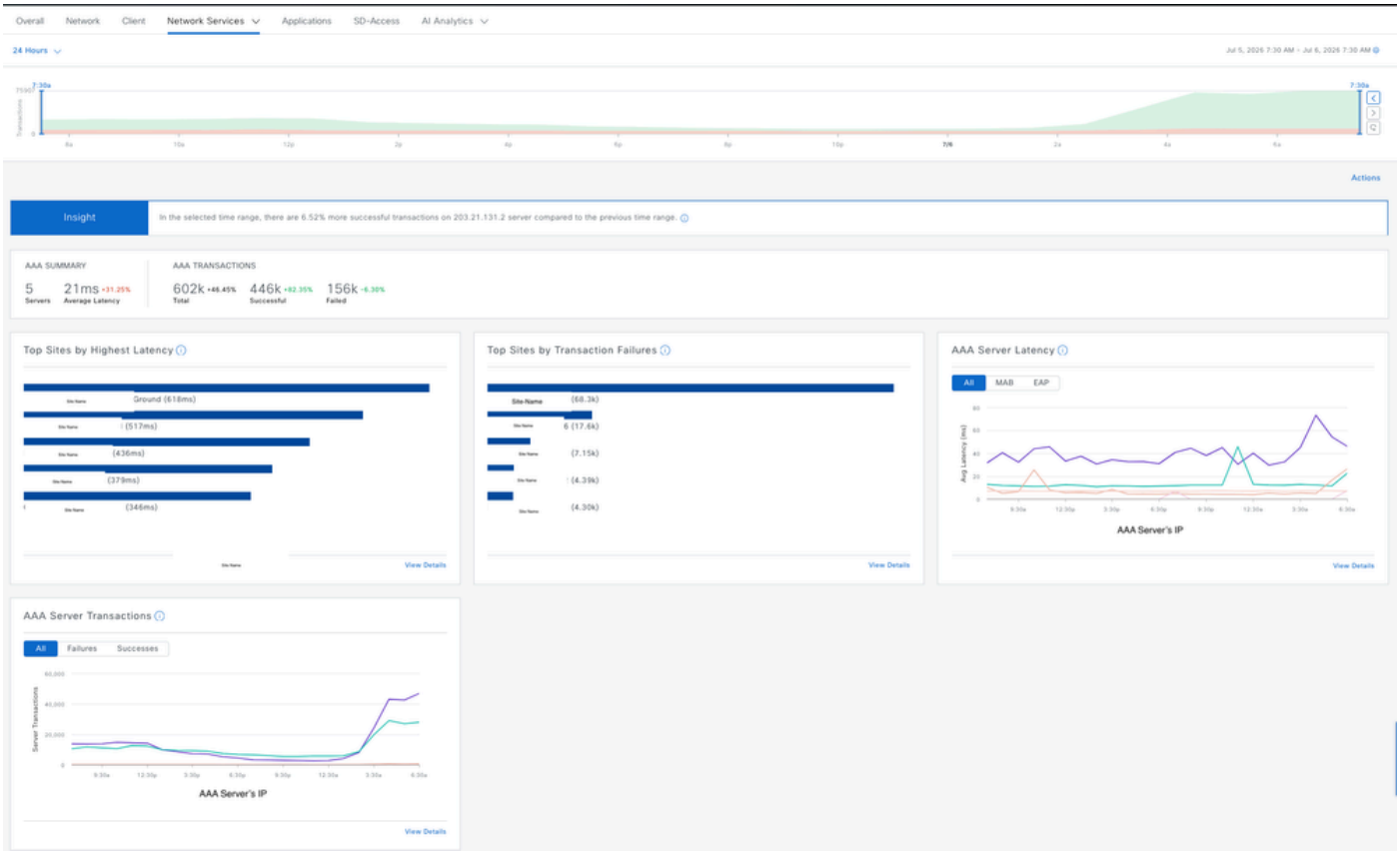
Die vollständige Paketerfassung kann entweder manuell gestoppt oder automatisch deaktiviert werden, wenn der geplante Zeitraum (von 30 Minuten bis 8 Stunden) abgelaufen ist. Sobald die Erfassung beendet ist, wird sie unter "Abgeschlossene Erfassungen" angezeigt. Dort können Sie auf die MAC-Adresse des Clients klicken, um die detaillierten Erfassungsdaten anzuzeigen und die Datei zur weiteren Analyse im PCAP-Format zu exportieren.

Beispiel für vollständige Erfassung für Client erfasst

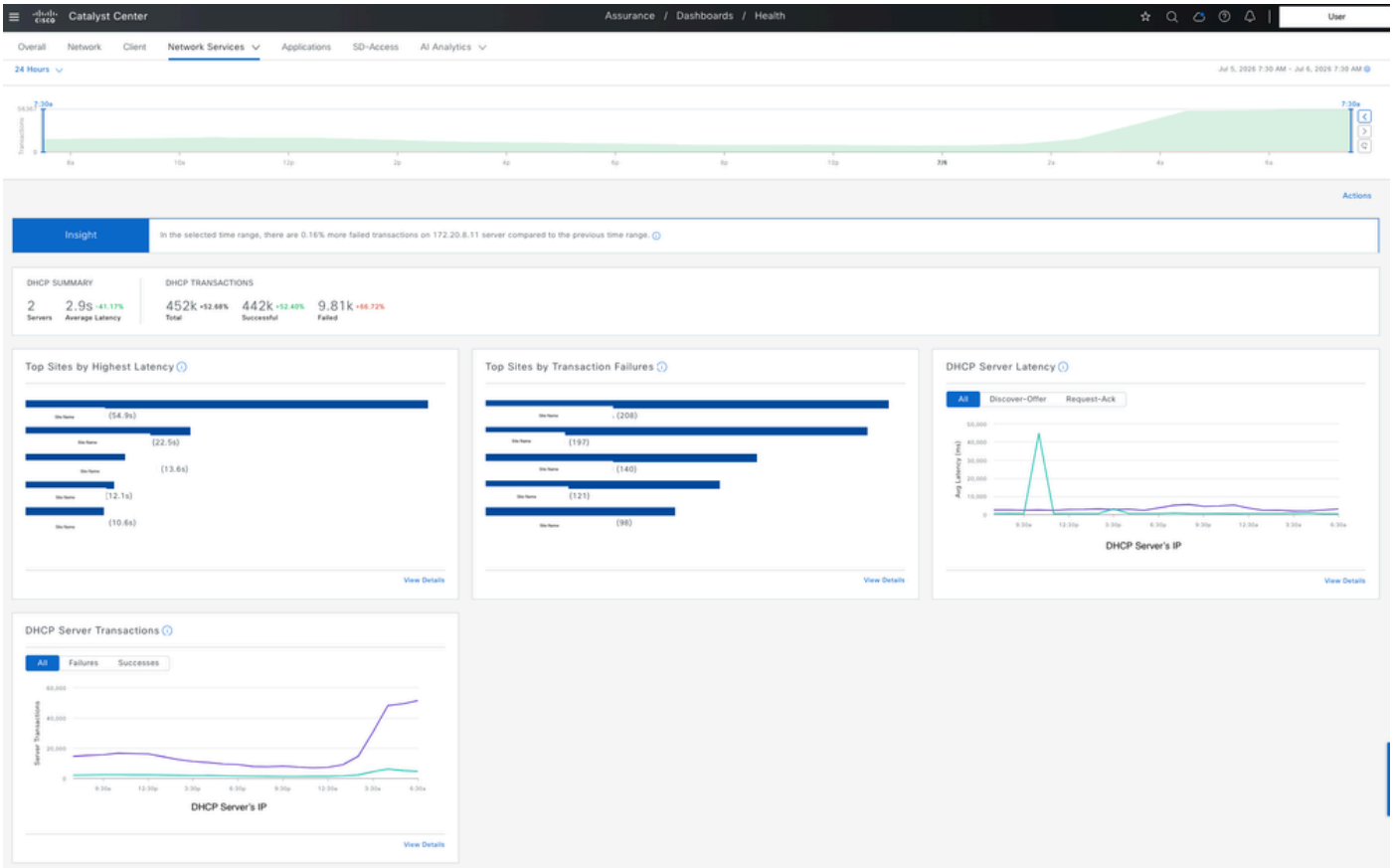
Isolierung von Netzwerkserviceproblemen (AAA, DHCP, DNS)

Wenn das gemeldete Symptom auf einen bestimmten Netzwerkdienst und nicht auf den Controller selbst verweist (z. B. Clients, die nicht authentifiziert werden konnten, keine IP-Adresse erhielten oder Probleme mit der Namensauflösung), bietet Ihnen das Catalyst Center Network Services-Dashboard unter "Assurance" Einsicht in die Transaktionen, die vom WLC gemeldet wurden.

Navigieren Sie zu Assurance > Dashboard > Health > Network services > AAA/DHCP/DNS:



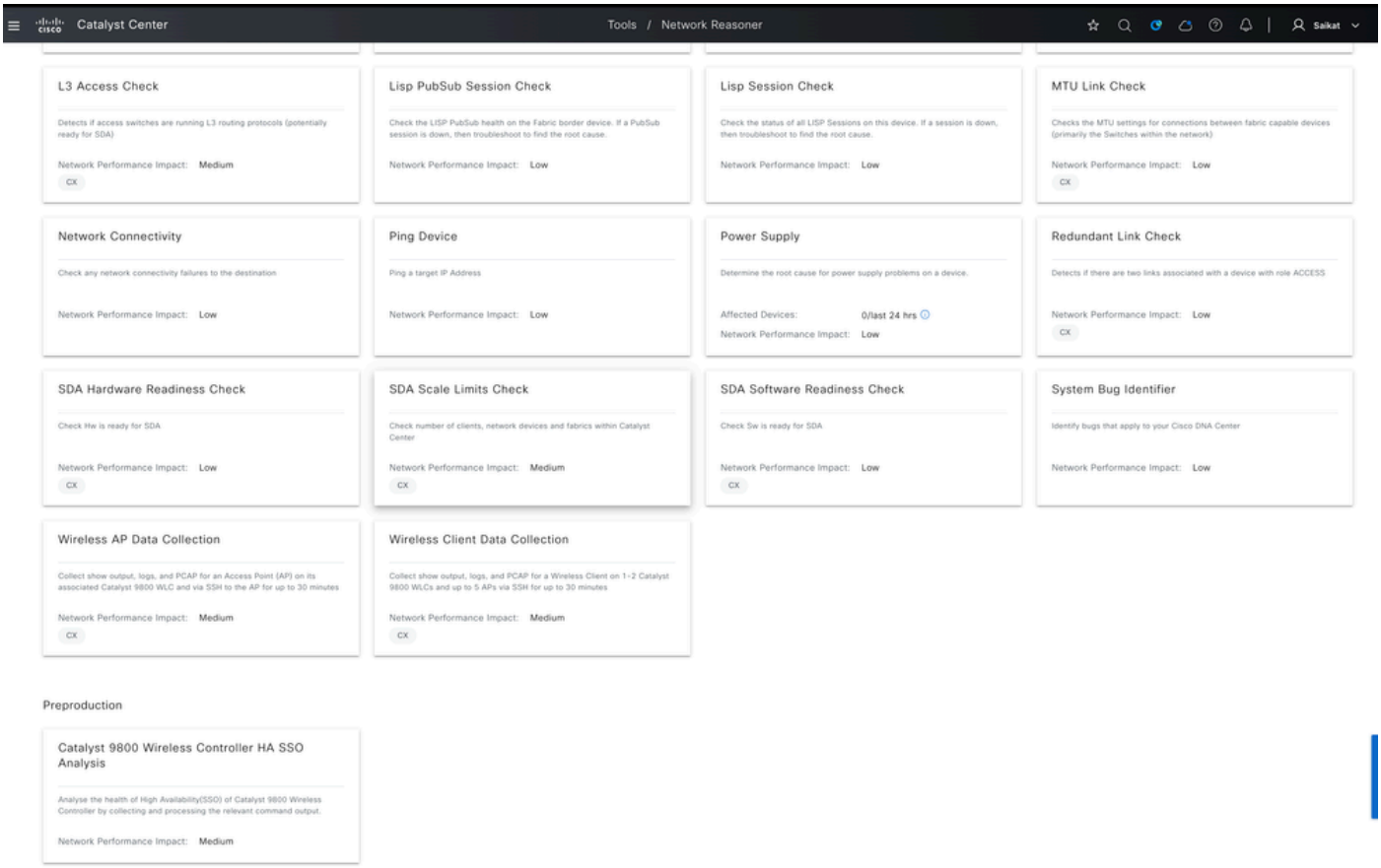
Wireless-Client - AAA-Statistiken zu Catalyst Center



DHCP-Statistiken des Wireless-Clients zu Catalyst Center

Gründe für das Netzwerk

Network Reasoner ist ein integriertes Tool im Catalyst Center, das Netzwerkprobleme automatisch für Sie untersucht. Sie müssen die Protokolle nicht manuell durchsuchen. Sie finden es unter Tools > Network Reasoner. Jede Fehlerbehebungsoption (Workflow genannt) zeigt Ihnen eine kurze Beschreibung, wie viele Geräte in den letzten 24 Stunden betroffen waren und was passiert, wenn Sie sie ausführen. Es kann nur Probleme auf Geräten erkennen, die entweder zur Garantieüberwachung zu Catalyst Center hinzugefügt oder über Catalyst Center bereitgestellt werden.



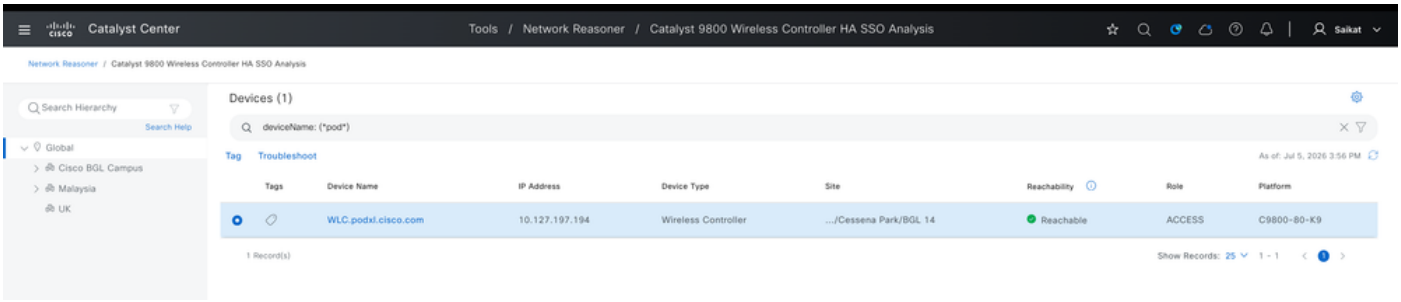
Verschiedene Optionen zur Behebung von Netzwerkfehlern im Network Reasoner

Für Wireless-Netzwerke gibt es drei Hauptaspekte, die Sie beheben können:

1. Bei Controller-Problemen, insbesondere bei HA-Konfigurationen (High Availability), überprüft der Network Reasoner z. B. Folgendes:

- Ist der Controller erreichbar?
- Ist HA korrekt eingerichtet?
- Sind die aktiven und Standby-Controller synchronisiert?
- Funktioniert die Verbindung zwischen ihnen?

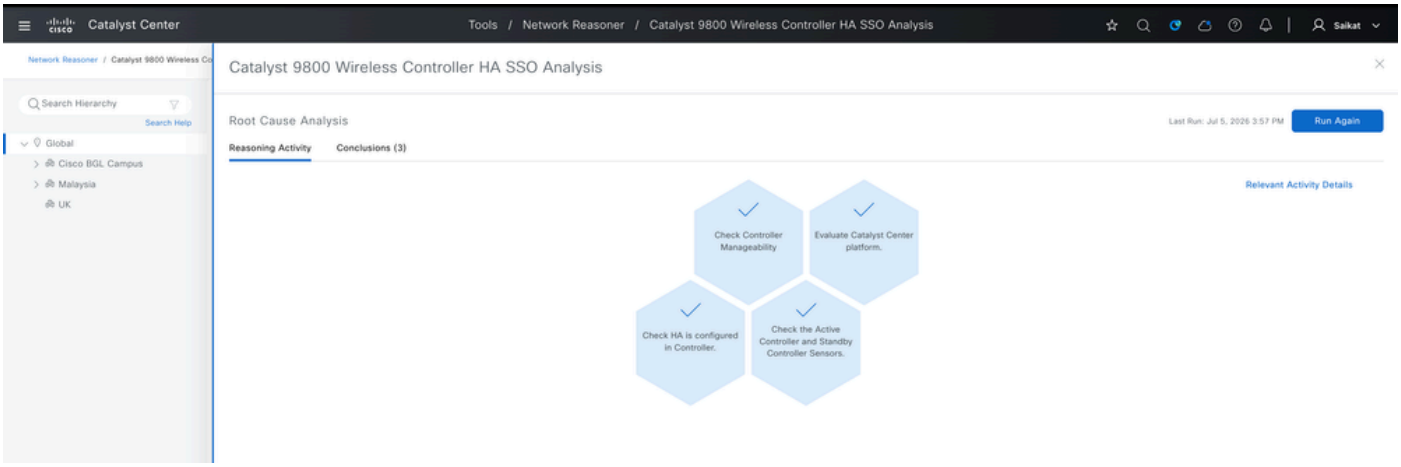
Wenn es ein Problem findet, sagt es Ihnen genau, was falsch ist und schlägt vor, wie es zu beheben. Es gibt auch eine separate Option für die Fehlerbehebung von Geräten, die überhaupt keine Überwachungsdaten senden.



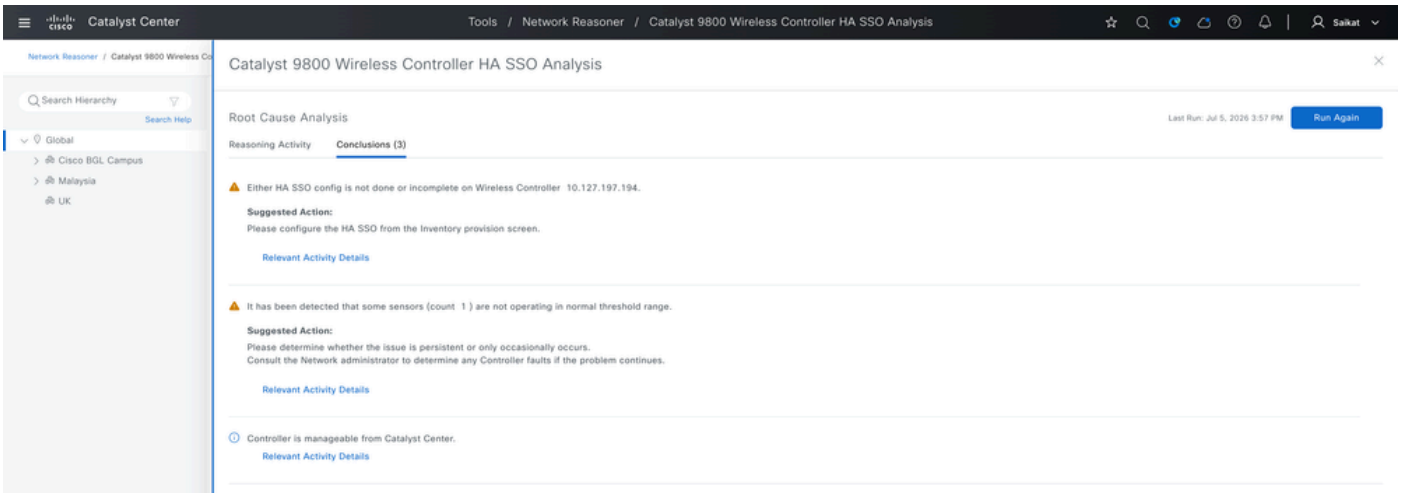
Fehlerbehebung bei HA mit Network Reasoner

Wenn Sie die Fehlerbehebungsfunktion für HA SSO-Analysen auf dem 9800 WLC mit Network Reasoner aktivieren, führt sie mehrere Prüfungen durch und liefert basierend auf den Ergebnissen eine Schlussfolgerung. Wenn Probleme mit HA SSO festgestellt werden, werden auch Korrekturmaßnahmen vorgeschlagen, um diese zu beheben.

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

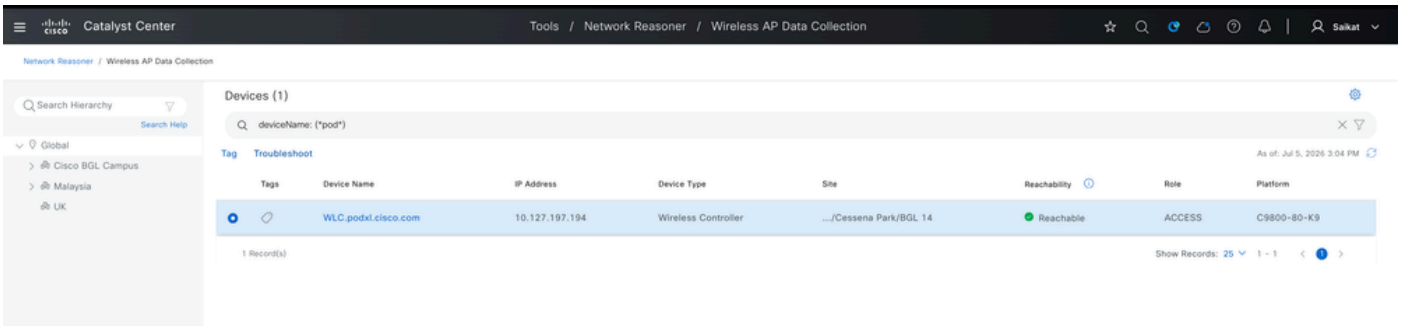


Von CATC für HA SSO-Analyse durchgeführte Aufgaben

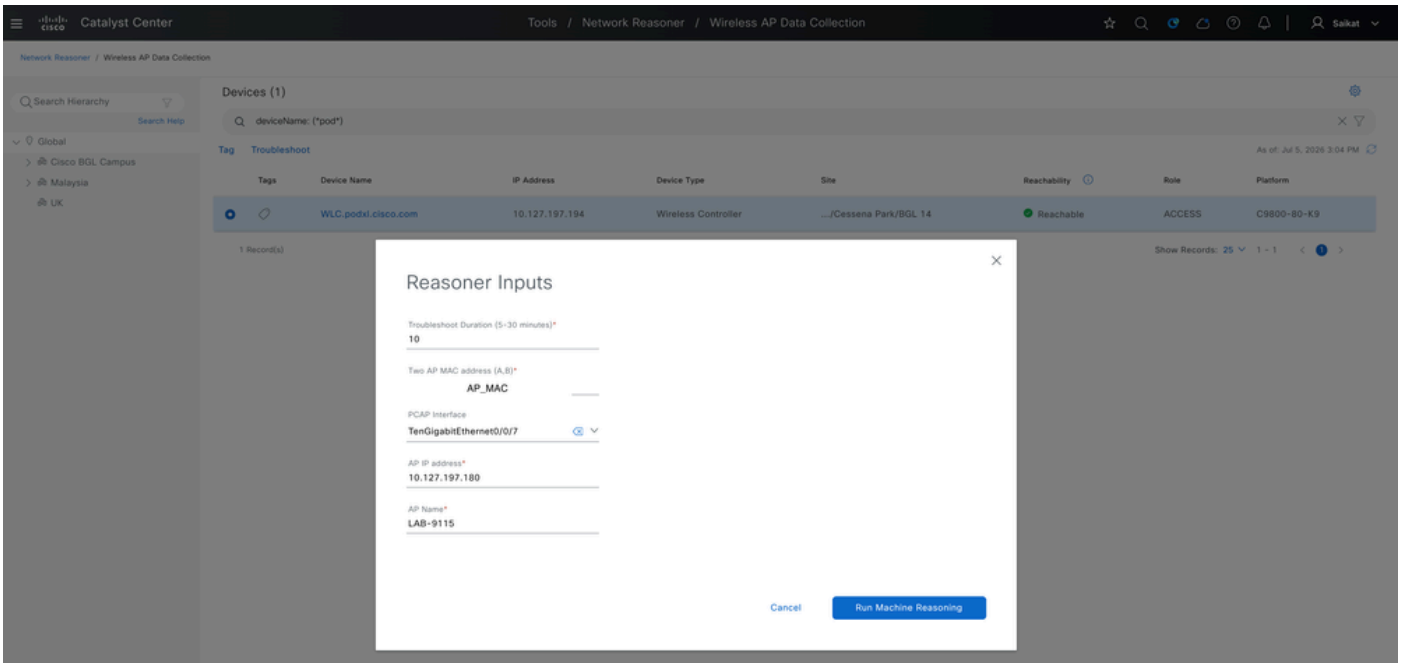


Fazit-Beispiel für HA SSO-Fehlerbehebung mit Network Reasoner

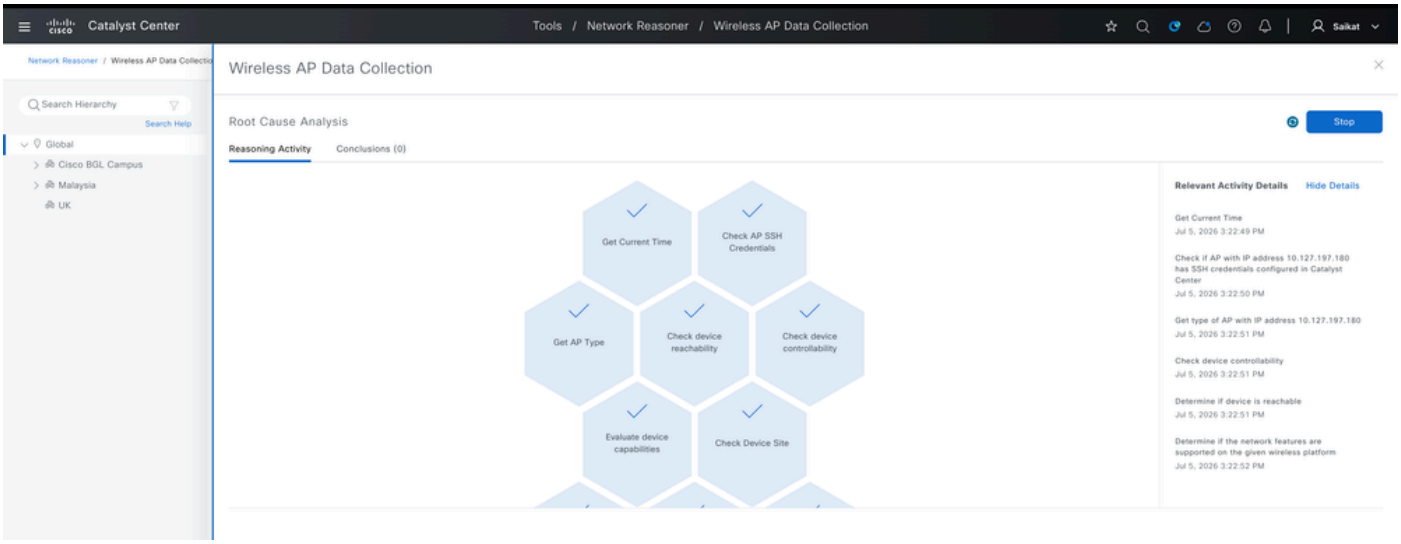
2. Access Points - Wenn bei einem Access Point Probleme auftreten, wählen Sie den Controller aus, der den Access Point verwaltet, und geben Sie dann die MAC-Adresse des Access Points ein. Legen Sie die Dauer für die Prüfung fest. Sie ermöglicht die Protokollierung und Paketerfassung vom WLC und AP und sorgt so für eine bessere Transparenz. Nachfolgend finden Sie den Workflow zum Aktivieren der Network Reasoner-Funktion für einen Access Point sowie die entsprechenden Ergebnisse:



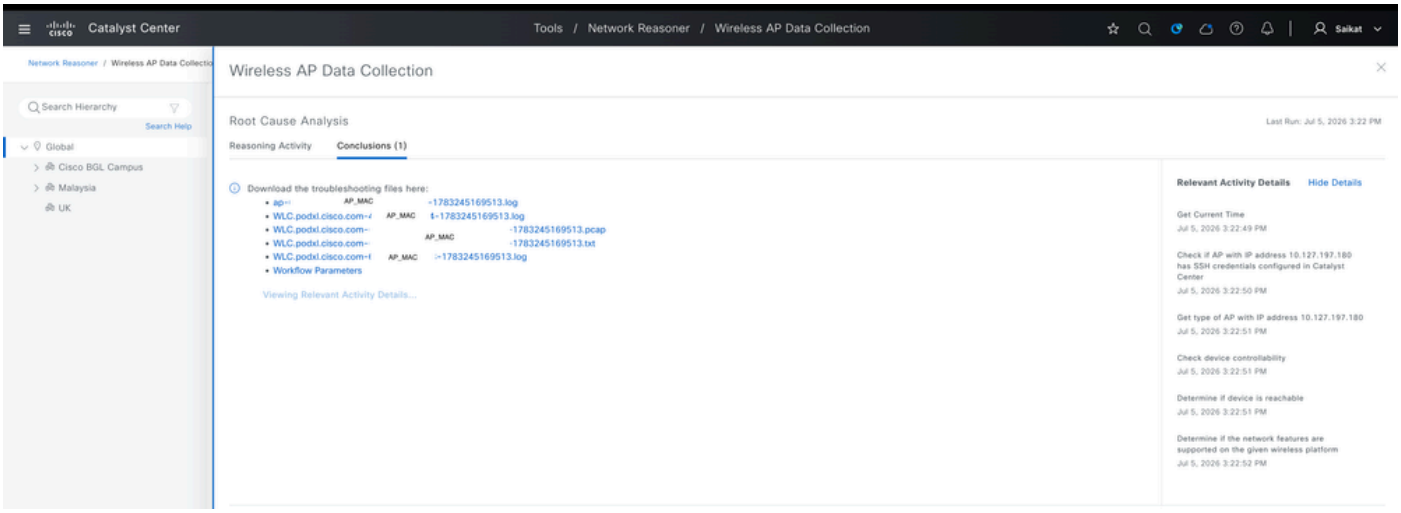
Verwalteten AP WLC zur Fehlerbehebung auswählen



Bereitstellung von AP-Details zur Fehlerbehebung



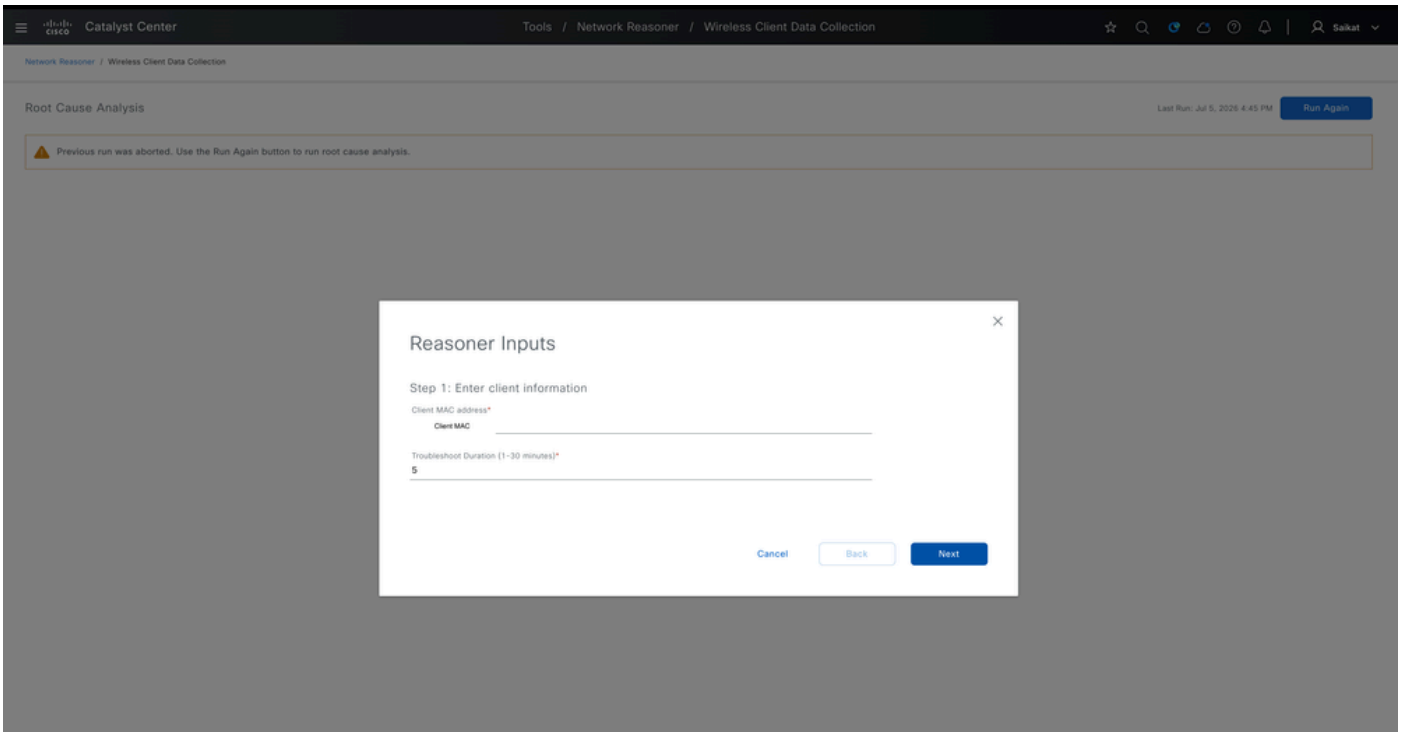
Aufgaben zur Behebung von AP-Problemen



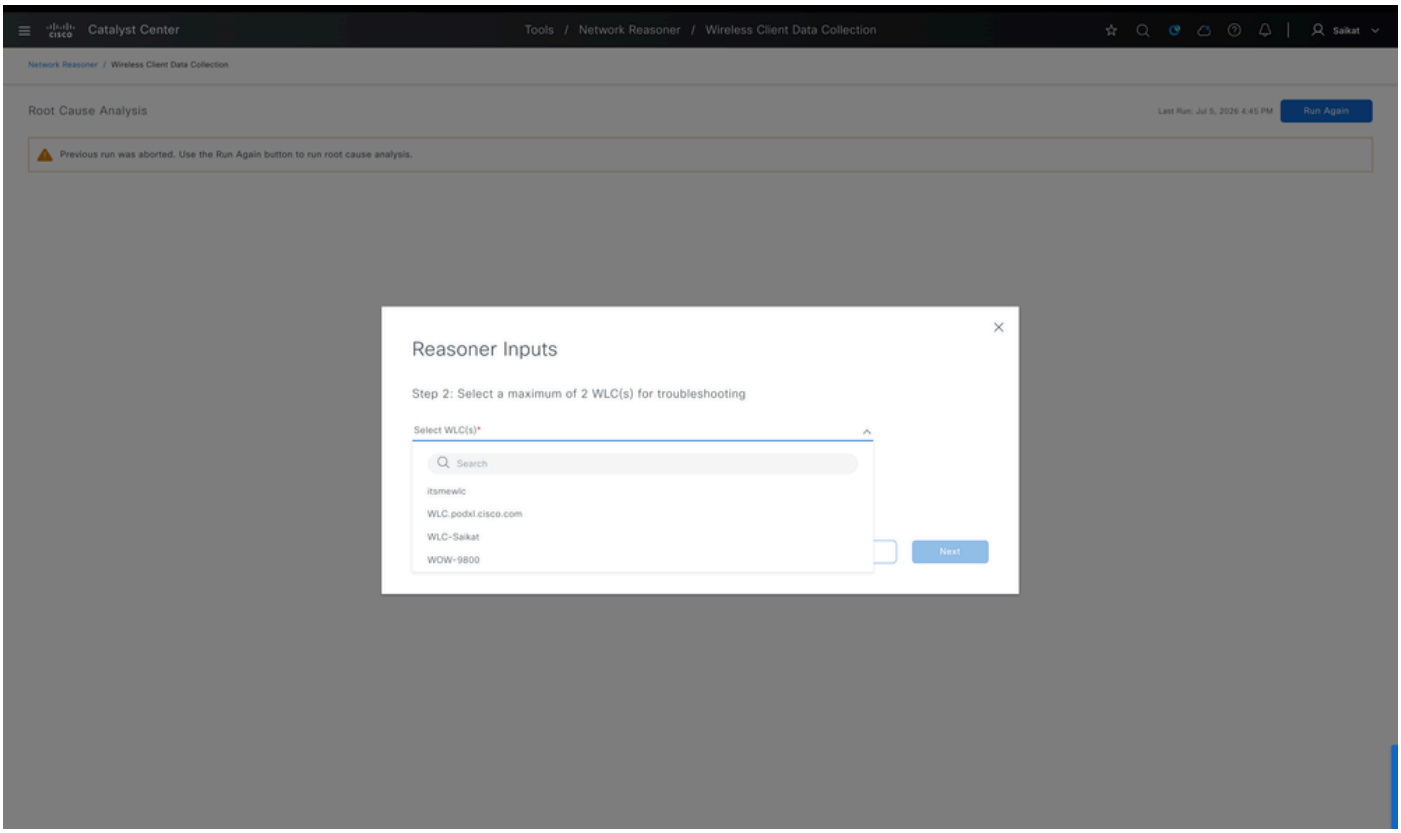
```
!! Task Workflow !!
Get Current Time
Jul 5, 2026 5:04:39 PM
Check if AP with IP address 10.127.197.180 has SSH credentials configured in Catalyst Center
Jul 5, 2026 5:04:40 PM
Get type of AP with IP address 10.127.197.180
Jul 5, 2026 5:04:40 PM
Check device controllability
Jul 5, 2026 5:04:41 PM
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
```

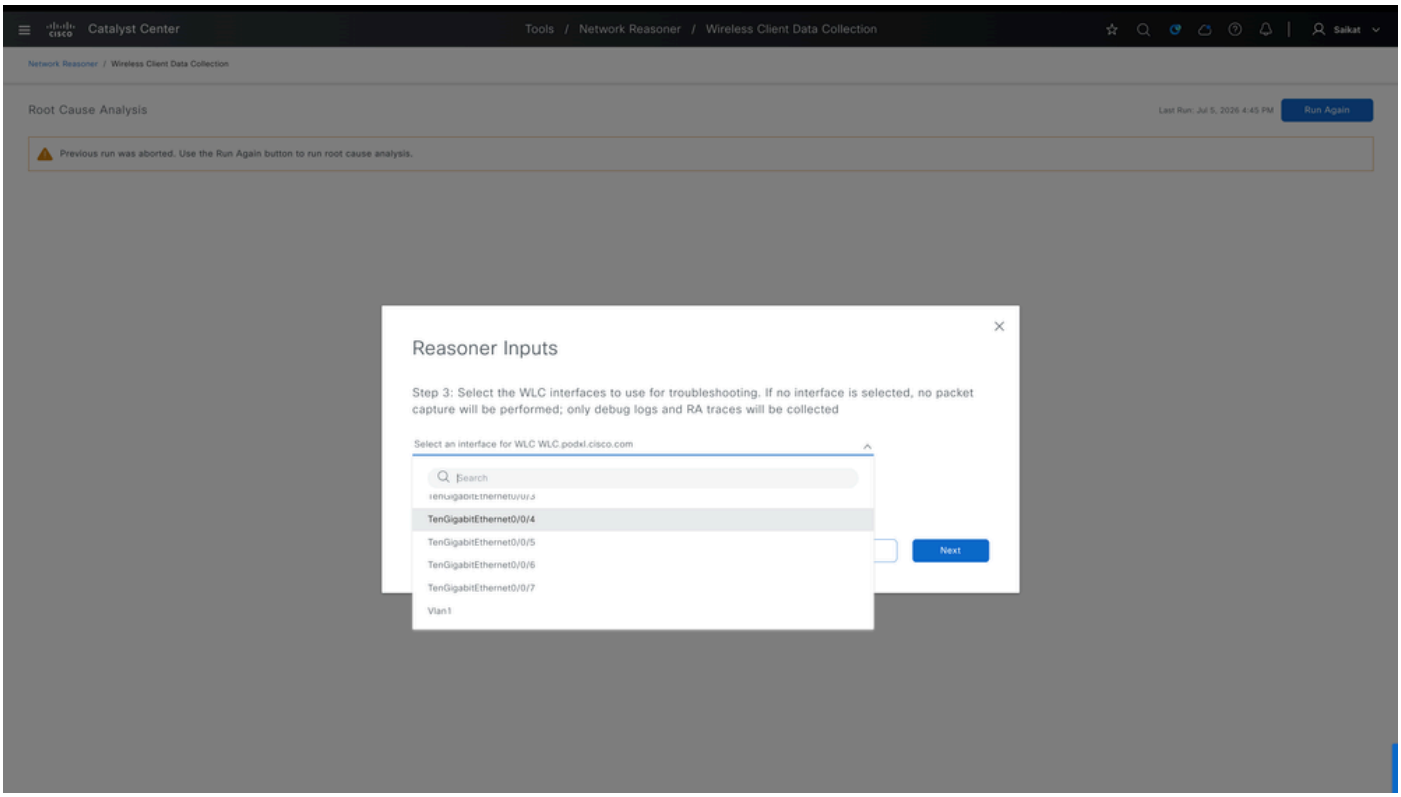
3. Wireless-Clients - Wenn ein Benutzer Wi-Fi-Probleme hat, wählen Sie den Wireless-Controller aus, mit dem er verbunden ist, geben Sie die MAC-Adresse des Geräts ein, und wählen Sie aus, wie lange das Tool überwachen soll. Es ermöglicht Statistikprotokolle, RA-Ablaufverfolgungen und Paketerfassung, um die tatsächlich ausgetauschten Daten zu sehen. Nachfolgend finden Sie den Workflow zum Aktivieren des Network Reasoners für den Wireless-Client sowie die entsprechenden Ergebnisse:



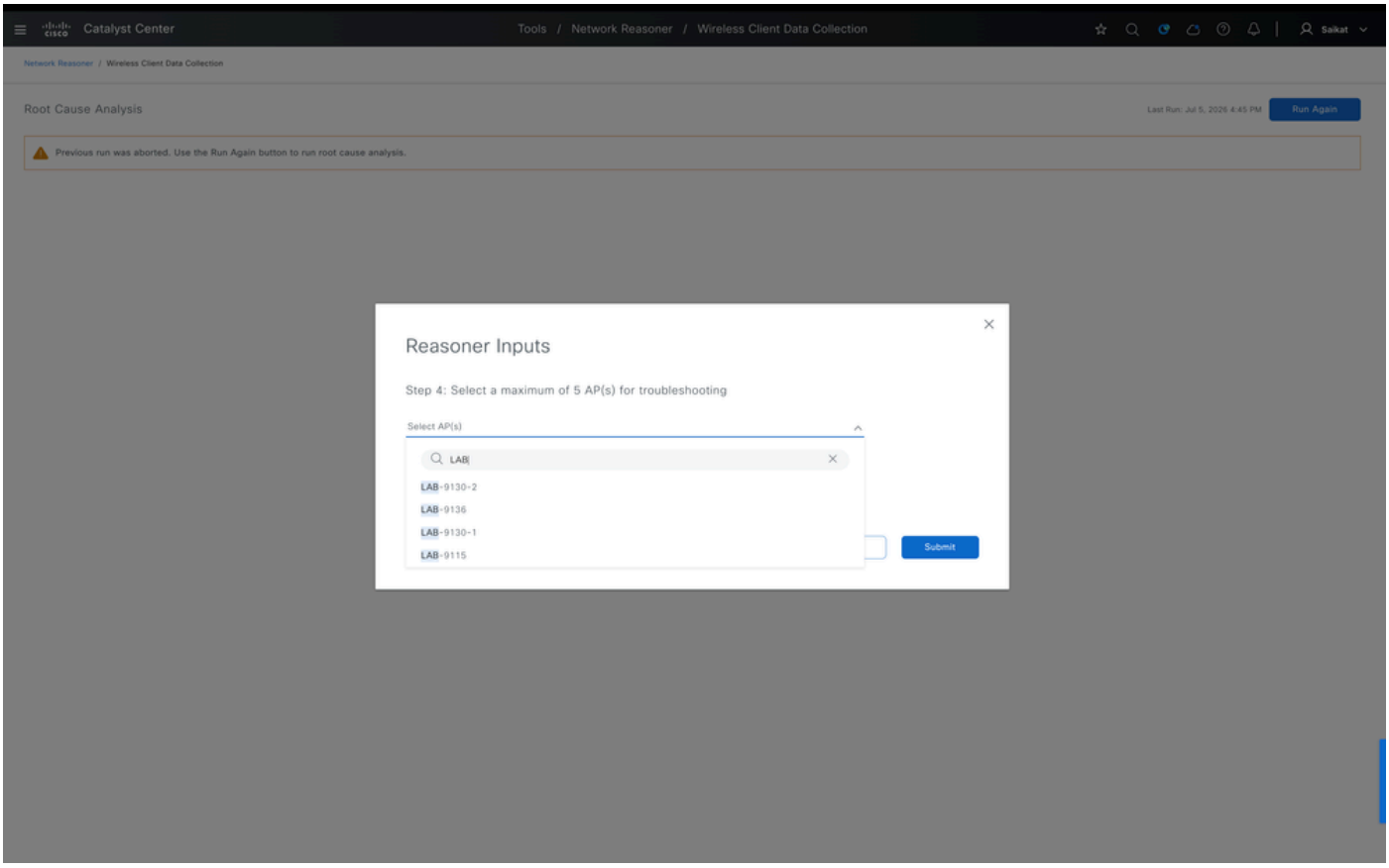
Bereitstellen von Client-Details zur Fehlerbehebung



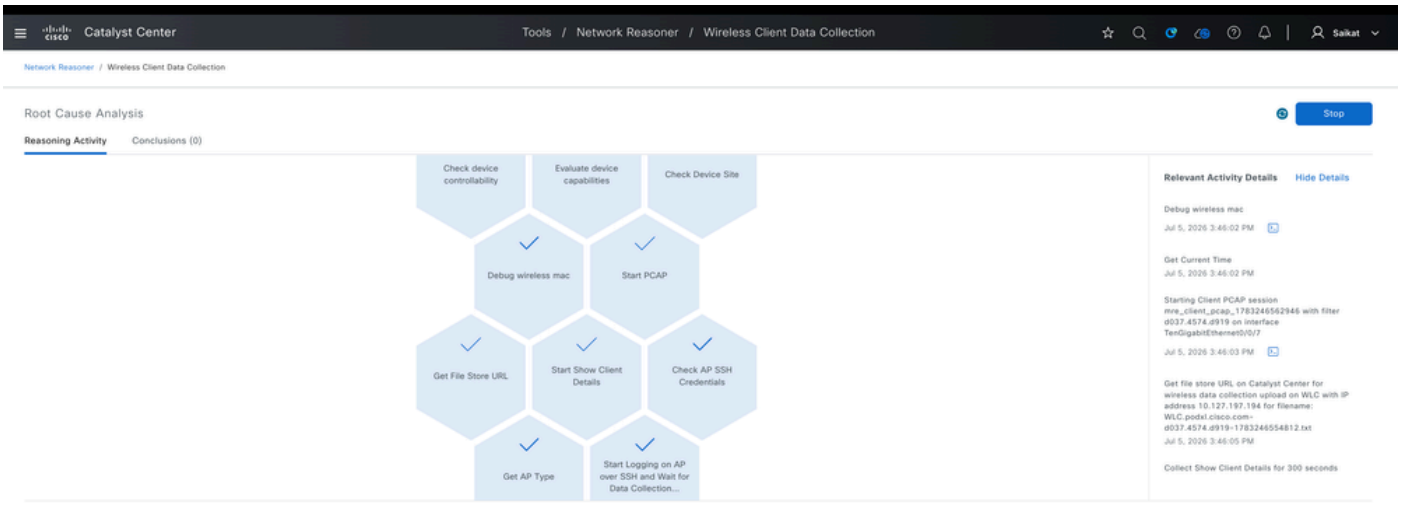
WLC zur Fehlerbehebung bei MAC des Wireless-Clients auswählen



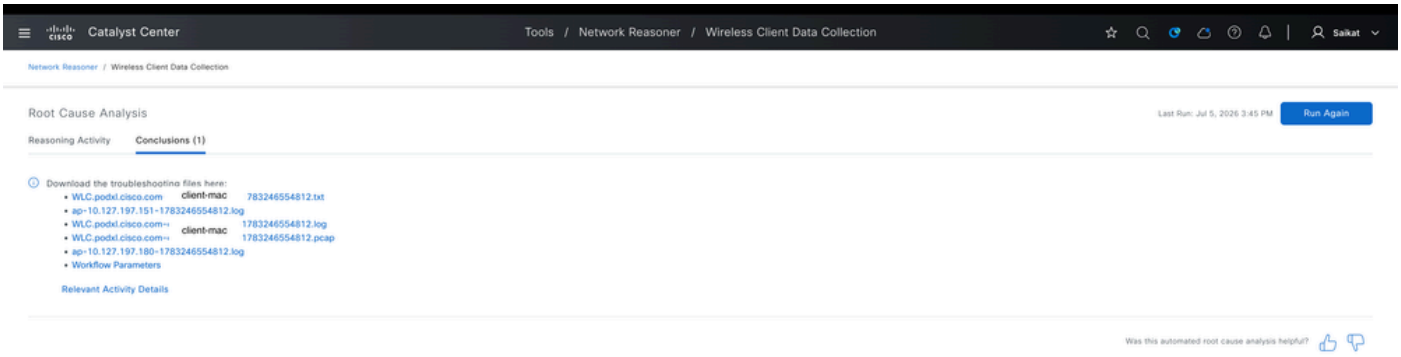
Wählen Sie die Schnittstelle auf dem WLC zur Fehlerbehebung beim Wireless-Client aus.



Auswahl von APs (max. 4) zur Fehlerbehebung beim Wireless-Client



Aufgaben zur Fehlerbehebung bei Problemen mit Wireless-Clients



Erfassung von WLC und AP bei Wireless-Client-Problemen

```
!! 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/v1
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 http
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

05.07.2026 17:59:16

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

05.07.2026 17:59:16

Check File Size:bootflash:<file-name>

05.07.2026 17:59:16

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

05.07.2026 17:59:18

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

05.07.2026 17:59:23

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

05.07.2026 17:59:23
Löschen Sie die Datei bootflash:<Dateiname> vom WLC mit der IP-Adresse 10.127.197.194.
05.07.2026 17:59:23

Technische Referenzen

- Cisco Intelligent Capture - Implementierungsleitfaden
- Verwalten intelligenter Erfassungen
- Cisco Catalyst Assurance-Benutzerhandbuch, Version 2.3.7.x
- Fehlerbehebung bei Netzwerkgeräten mit Network Reasoner - hohe Verfügbarkeit am Wireless LAN-Controller mit MRE-Workflow

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.