

# Fehlerbehebung bei Wireless-Problemen mit Catalyst Center

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Erfassung von Daten aus Catalyst Center](#)

[Problem mit Catalyst Wireless Controller der Serie 9800](#)

[Überprüfen des Controller-Status mit Gerät 360](#)

[Problem mit einem Access Point](#)

[Intelligente Erfassung für Access Point](#)

[Erfassung von AP-Statistiken](#)

[OTA Sniffer-Erfassung](#)

[Erkennung von Anomalien](#)

[Problem mit der Wireless-Client-Verbindung](#)

[Intelligente Erfassung für Wireless-Clients](#)

[Onboarding-Paketerfassung](#)

[Vollständige Paketerfassung](#)

[Isolierung von Netzwerkserviceproblemen \(AAA, DHCP, DNS\)](#)

[Gründe für das Netzwerk](#)

[Technische Referenzen](#)

---

## 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.

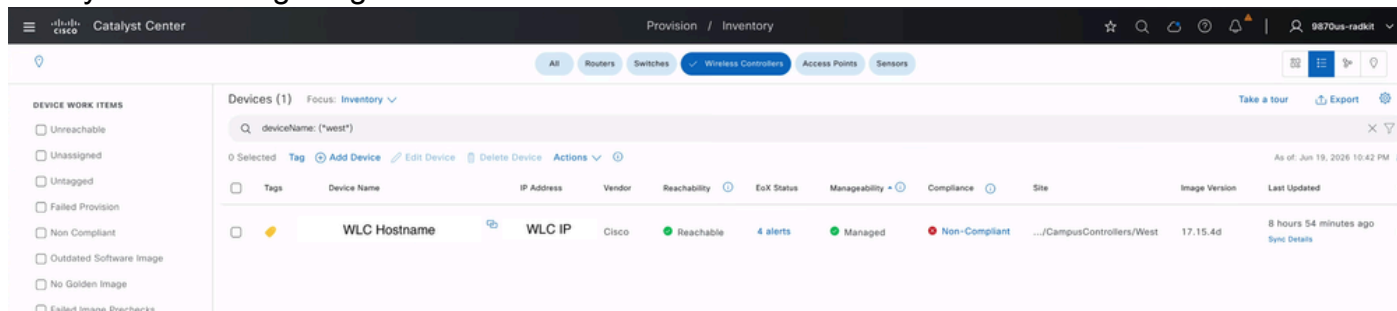
## Erfassung von Daten aus Catalyst Center

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.

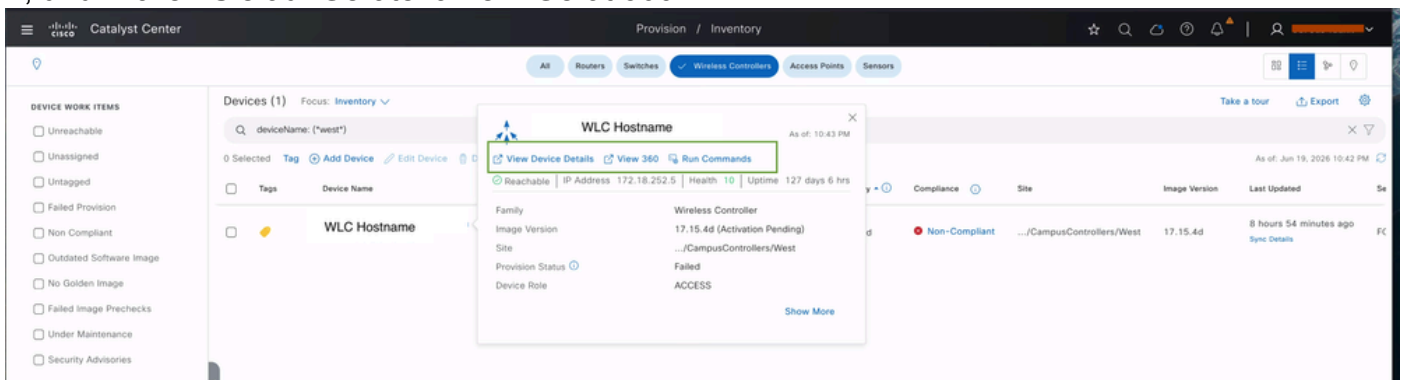
## Problem mit Catalyst Wireless Controller der Serie 9800

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



The screenshot shows the Cisco Catalyst Center interface. The main navigation bar includes 'Provision / Inventory'. The left sidebar lists 'DEVICE WORK ITEMS' such as 'Unreachable', 'Unassigned', 'Untagged', 'Failed Provision', 'Non Compliant', 'Outdated Software Image', 'No Golden Image', 'Failed Image Prechecks', 'Under Maintenance', and 'Security Advisories'. The main content area shows a list of devices with a search filter 'deviceName: (\*west\*)'. A modal window titled 'WLC Hostname' is open, displaying details for a specific device. The 'View 360' button is highlighted with a green box. The details shown in the modal window are:

Property	Value
Family	Wireless Controller
Image Version	17.15.4d (Activation Pending)
Site	.../CampusControllers/West
Provision Status	Failed
Device Role	ACCESS

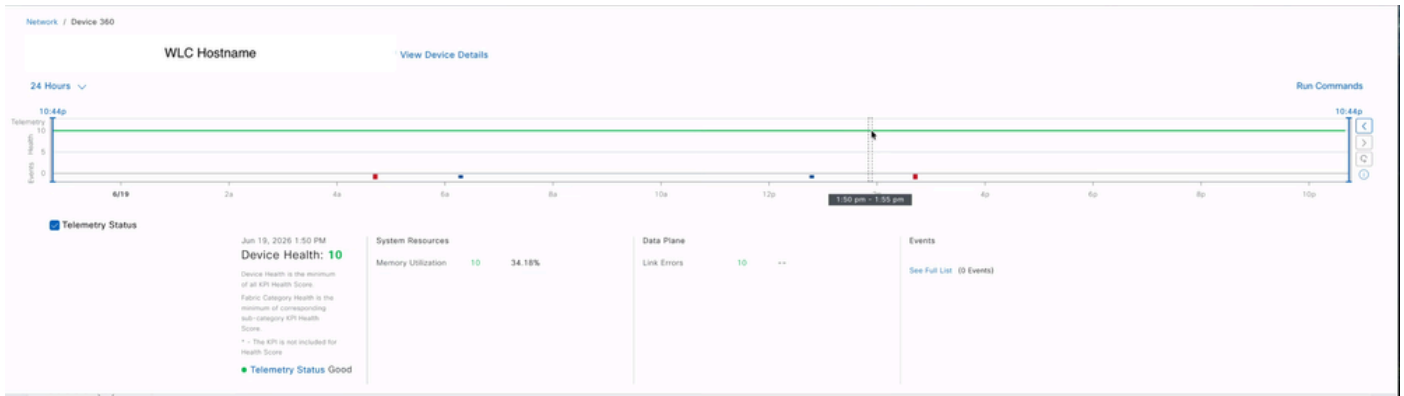
View 360 für Wireless LAN-Controller



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.

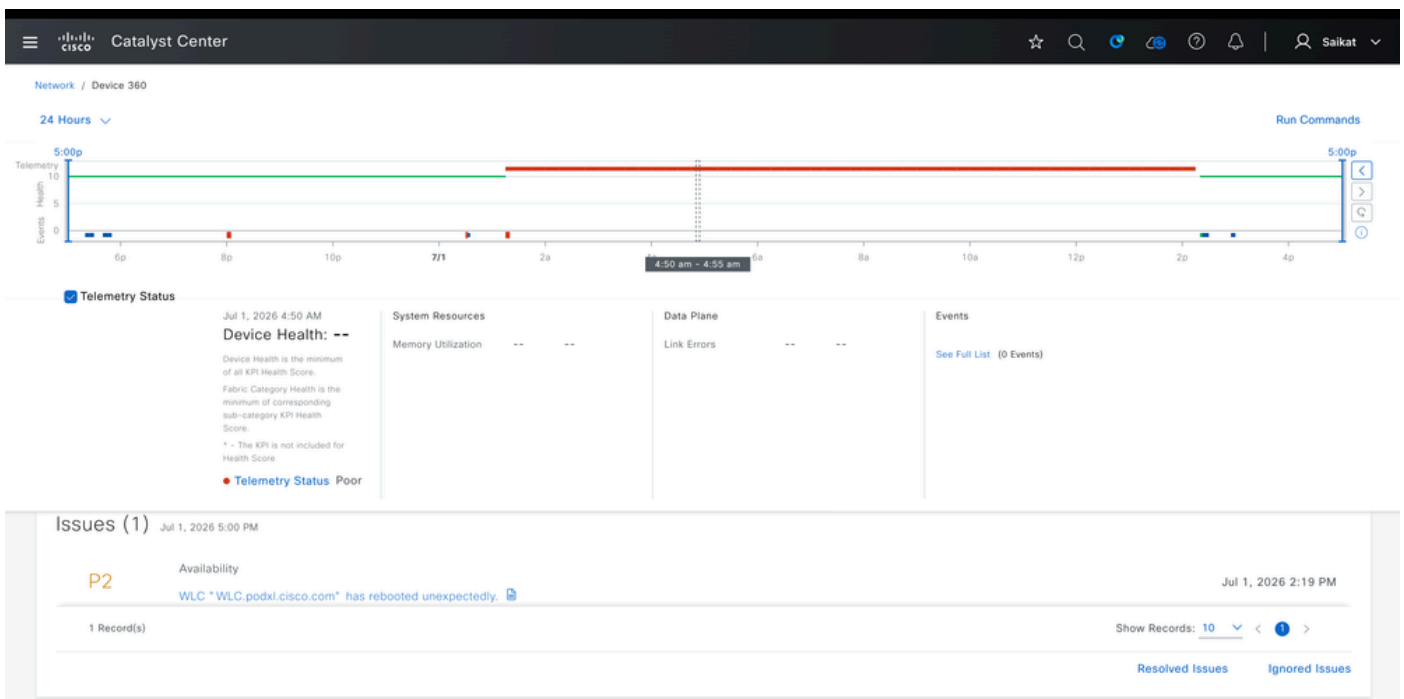
Mit Gerät 360 können Sie den Schieberegler für die Integritätszeitleiste auf einen beliebigen Punkt innerhalb des unterstützten Verlaufs Fensters verschieben (die Catalyst Center Assurance-Daten werden bis zu 30 Tage gespeichert), um den Controller-Status zum Zeitpunkt des Vorfalls genau zu überprüfen.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

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

Open | Issue Profile: global | Edit Issue Settings

**Description**  
 This WLC "WLC.podxl.cisco.com" has rebooted unexpectedly. Reboot reason is "PowerOn"  
 Last Occurred: Jul 1, 2026 2:19 PM

**WLC Reboot History**  
 Jun 30, 2026 5:00 PM to Jul 1, 2026 5:00 PM

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

1 Record(s) | Show Records: 10 | 1

**Suggested Actions (4)** | Preview All | Run All

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

Vorgeschlagene Aktion für Problem gemeldet auf WLC

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

Open | Issue Profile: global | Edit Issue Settings

**Description**  
 This WLC "WLC.podxl.cisco.com" has rebooted unexpectedly. Reboot reason is "PowerOn"  
 Last Occurred: Jul 1, 2026 2:19 PM

**WLC Reboot History**  
 Jun 30, 2026 5:00 PM to Jul 1, 2026 5:00 PM

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

1 Record(s) | Show Records: 10 | 1

**Suggested Actions (4)** | Preview All | Run All

- Run show version for more details.
  - show version  
 show version Success

```

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

Vorgeschlagene Aktion für Problem gemeldet auf WLC

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

The screenshot shows the 'Event Viewer' interface. At the top, there are links for 'Go to Global Event Viewer', 'Export', and 'Full Screen'. A search bar is labeled 'Search Table'. Below this is a table with columns for Severity, Details, Message Type, and Time. The table lists several events, with the one selected being a Notice event: CAPWAPAC\_SMGR\_TRACE\_MESSAGE:AP\_JOIN\_DISJOIN, Syslog, 12:49:30.457 PM. To the right of the table is a 'Detailed Information' panel for the selected event, showing fields like Severity (Notice), Mnemonic (AP\_JOIN\_DISJOIN), Facility (CAPWAPAC\_SMGR\_TRACE\_MESSAGE), and Message Text.

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

Ereignisanzeige für Wireless LAN-Controller - Beispiel 1

This screenshot shows the 'Event Viewer' interface with a different event selected. The table lists several events, with the selected one being an Alert event: MM\_NODE\_LOG:ANCHORS\_DOWN, Syslog, 2:44:31.673 PM. The 'Detailed Information' panel on the right shows fields like Severity (Alert), Mnemonic (ANCHORS\_DOWN), Facility (MM\_NODE\_LOG), and Message Text.

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

Ereignisanzeige für Wireless LAN-Controller - Beispiel 2

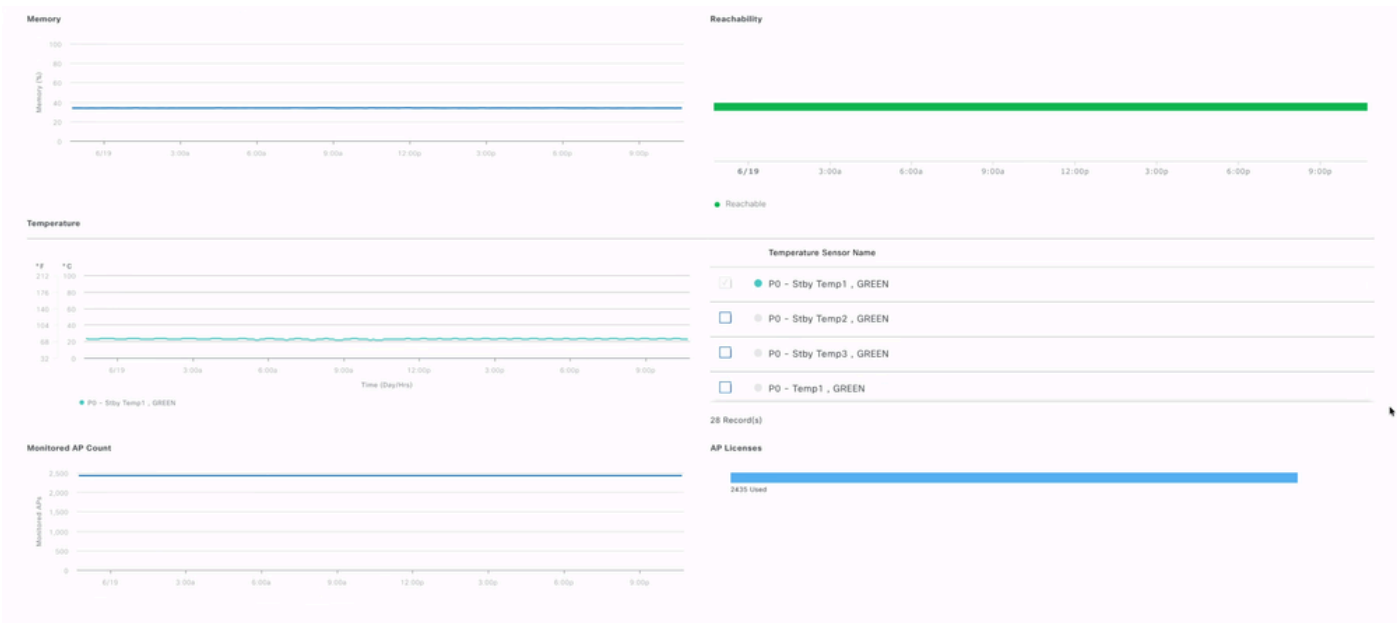
Leistungsstatistiken - CPU- und Speichernutzung, Temperatur, Betriebszeit, HA-Status und Grund für das letzte Neuladen.

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.

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

1 Selected: FortyGigabitEthernet0/1/0

## Interface Availability

FortyGigabitEthernet0/1/0

100

## Traffic and Packet Summary

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

## WLC-Statistiken zu Catalyst Center

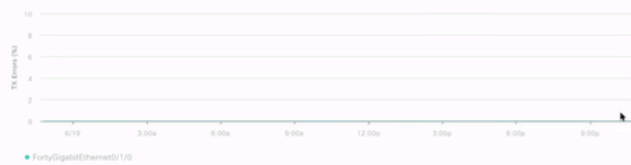
## Utilization

## TX Utilization



## Error

## TX Errors



## Discard

## TX Discards



## RX Utilization



## Error



## Discard



## 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.

Catalyst Center Assurance / Dashboards / Issues and Events

AP Reboot Crash / Issue Instance

Global/Cisco BGL Campus/...

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

Issue Profile: global [Edit Issue Settings](#)

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

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

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

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

**Suggested Actions (2)**

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

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.

Catalyst Center Assurance / Dashboards / Issues and Events

Issues ▾ Events Event Analytics

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

Events (142)

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

Filter Table

0 Selected

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

Ereignisanzeige für APs in Catalyst Center

Catalyst Center Assurance / Dashboards / Issues and Events

Issues ▾ Events Event Analytics

Global/Cisco BGL Campus/Cessena Park 24 Hours

Events (142)

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

Filter Table

0 Selected

Event Name

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

Additional Info: AP Disconnect - Heartbeat not heard from AP

Event Type: Device Event

Device Name: LAB-9115

Device IP: 10.127.197.180

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

Wireless Controller: WLC.podxl.cisco.com

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

Reason: AP Disconnect - Heartbeat not heard from AP

---

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

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

Show Events (±15 mins)

**Catalyst Center** Assurance / Dashboards / Issues and Events

Issues ▾ **Events** Event Analytics

Global/Cisco BGL Campus/Cessena Park

**Events (142)**  
Category Type: **Devices** Endpoints

Filter Table

0 Selected

Event Name

AP is connected to WLC. CAPWAP channel is up

---

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

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

Event Type: Device Event

Device Name: LAB-9130-2

Device IP: 10.127.197.182

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

Wireless Controller: WLC.podxl.cisco.com

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

Radio: 1

Frequency: 5.0GHz

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

Current Power Level: 8 dBm

Previous Power Level: 11 dBm

---

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

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

Detaillierte Übersicht über die gemeldeten Ereignisse (Hinweis)

**Catalyst Center** Assurance / Dashboards / Issues and Events

Issues ▾ **Events** Event Analytics

Global/Cisco BGL Campus/Cessena Park

**Events (142)**  
Category Type: **Devices** Endpoints

Filter Table

0 Selected

Event Name

AP is connected to WLC. CAPWAP channel is up

AP is disconnected from WLC. CAPWAP channel is

---

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

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

Event Type: Device Event

Device Name: LAB-9115

Device IP: 10.127.197.180

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

Wireless Controller: WLC.podxl.cisco.com

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

Radio: 1

Frequency: 5.0GHz

New Channel List: [64, 60]

Old Channel List: [157, 161]

Interference: -56 dBm -> -121 dBm

Noise: -86 dBm -> -84 dBm

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

---

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

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

Detaillierte Übersicht über die gemeldeten Ereignisse (Hinweis)

**Catalyst Center** Assurance / Dashboards / Issues and Events

Issues ▾ **Events** Event Analytics

Global/Cisco BGL Campus/Cessena Park

**Events (142)**  
Category Type: **Devices** Endpoints

Filter Table

0 Selected

Event Name

---

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

Additional Info: Last Reset Type - Configuration Changes

Event Type: Device Event

Device Name: LAB-9130-2

Device IP: 10.127.197.182

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

Wireless Controller: WLC.podxl.cisco.com

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

Last Reset Type: Configuration Changes

---

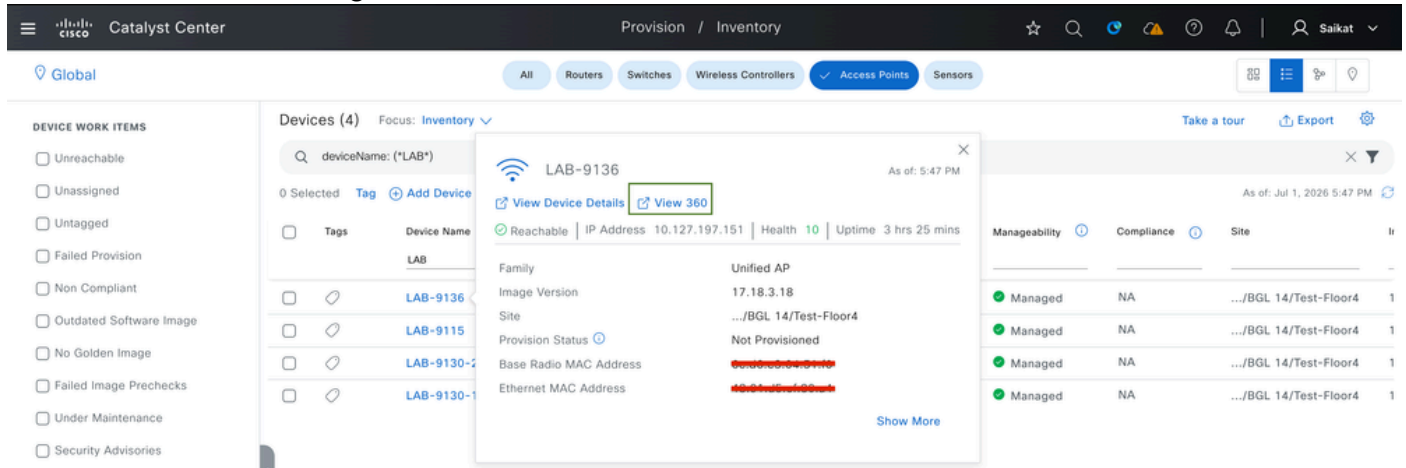
Connected Device Events  
Jun 30, 2026 5:10 PM - 5:40 PM

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

Show Events (±15 mins)

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 Verlaufs Fensters (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.

Issues (1) Jul 1, 2026 5:15 PM

**P3** Availability  
AP "LAB-9115" has rebooted due to a hardware or software crash.

1 Record(s)

Show Records: 10 < >

Resolved Issues Ignored Issues

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.

Event Viewer

Go to Global Event Viewer Export Full Screen

Search Table

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

4 records Show Records: 25 1 - 5 < >

**Channel Change** Jul 1, 2026 3:42:39 PM

Detailed Information

WLC Name: WLC.peddl.cisco.com

AP Base Radio Mac: 5C:E1:76:6A:02:00

Radio: 1

Frequency: 5.0GHz

Event Type: Channel Change

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

New Channel List: [140, 144]

Old Channel List: [64, 68]

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 Geräte-Name, Integritätsbewertung und MLO.

Physical Neighbor Topology

1 Client (2.4 GHz)

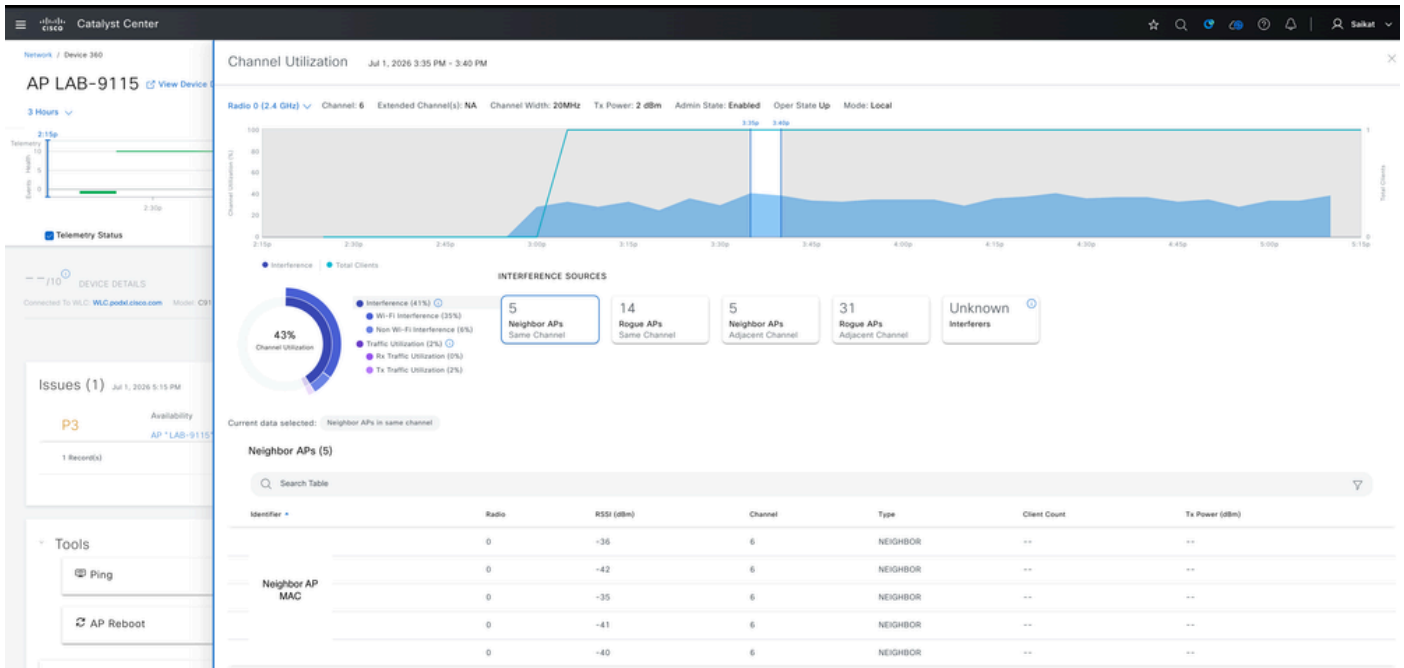
Search Table

Device	Health Score	IPv4 Address	IPv6
cx-Labs-WIN11	10	10.127.197.177	fe80

Show Records: 10 1 - 1 < >

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.



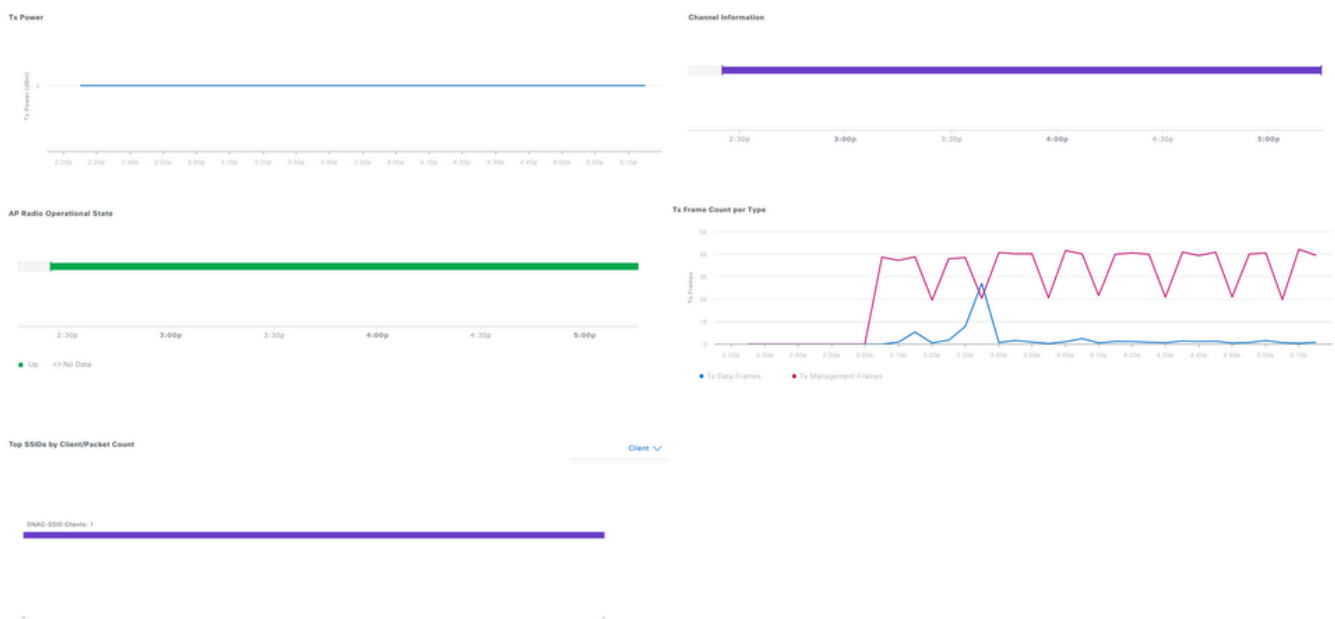
Gerätedetails für AP

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.



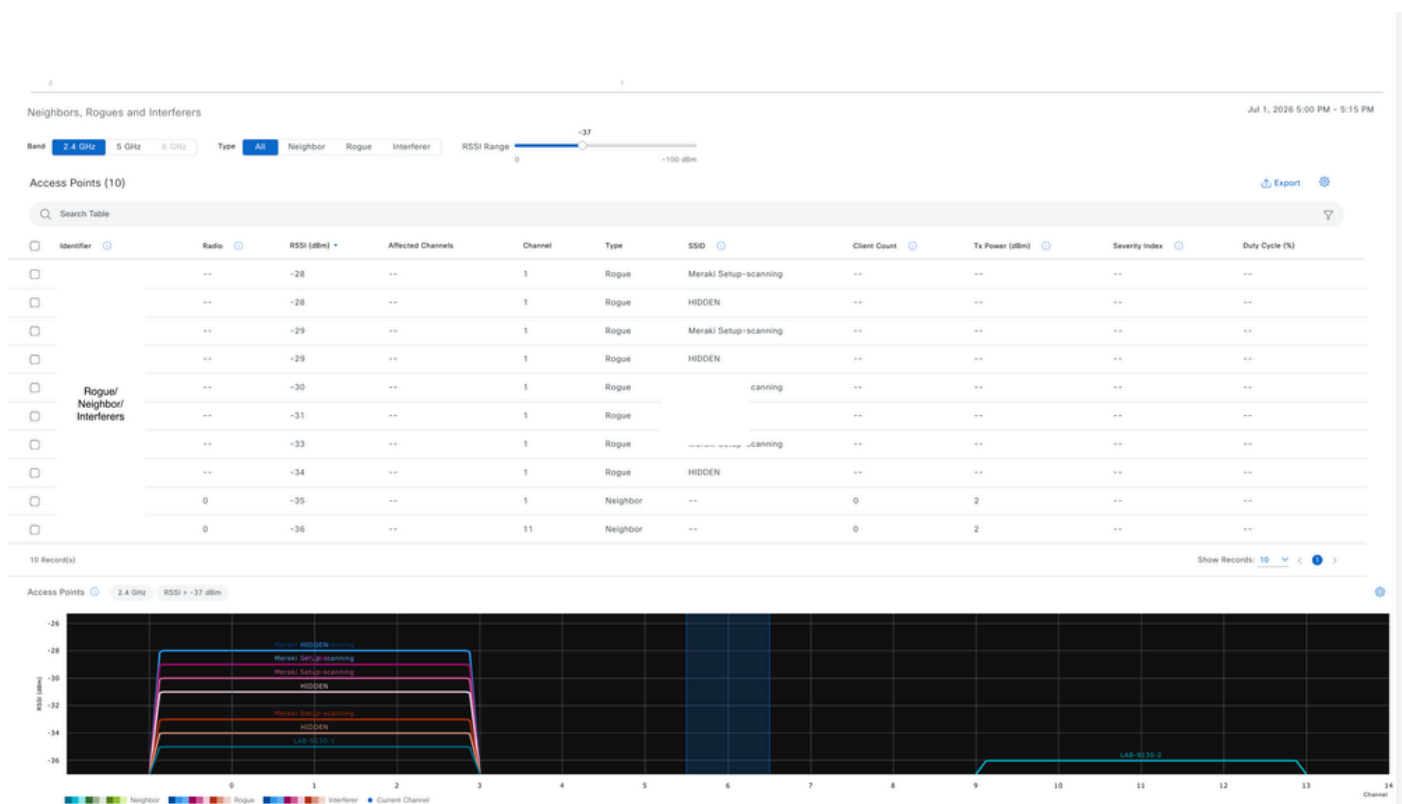
RF-Statistik für einzelnen AP

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

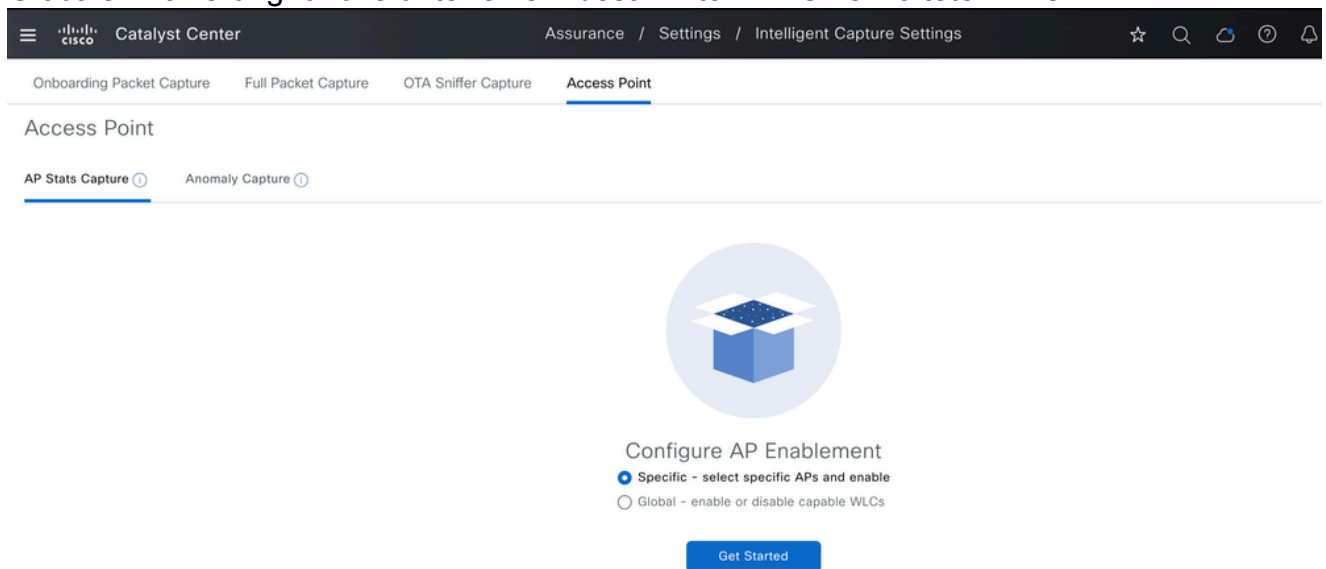
Die intelligente Erfassung für den Access Point bietet zwei Hauptfunktionen: stets verfügbare RF-Überwachung in Echtzeit, Erkennung von Anomalien und On-Demand-Übertragung über die Luftefassung, Spektrumanalyse.

## 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.



The screenshot shows the Cisco Catalyst Center web interface. The breadcrumb navigation is Assurance / Settings / Intelligent Capture Settings. The main menu includes Onboarding Packet Capture, Full Packet Capture, OTA Sniffer Capture, and Access Point. Under the 'Access Point' section, there are two tabs: 'AP Stats Capture' (selected) and 'Anomaly Capture'. The main content area features a large blue icon of an open box. Below the icon, the heading is 'Configure AP Enablement'. There are two radio button options: 'Specific - select specific APs and enable' (selected) and 'Global - enable or disable capable WLCs'. A blue 'Get Started' button is located at the bottom of the configuration area.

AP-Statistikerfassungsoption

Catalyst Center Assurance / Settings / Intelligent Capture Settings

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

### Access Point

AP Stats Capture  Anomaly Capture

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

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

Find Hierarchy

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

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

AP\_NAME

1 Selected **Enable**

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

Aktivieren von AP-Statistiken Intelligente Erfassung auf bestimmten APs

Catalyst Center Assurance / Settings / Intelligent Capture Settings

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

### Access Point

AP Stats Capture  Anomaly Capture

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

WLC.podxl.cisco.com

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

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

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.

Search by device name (i)

---

**WLC.podxl.cisco.com** ✓

Device IP: 10.127.197.194      Site: Global/Cisco BGL Cam

---

Configurations - Side by side view

View by Configuration Source • All ▾

Configuration to be Deployed (i) ↗

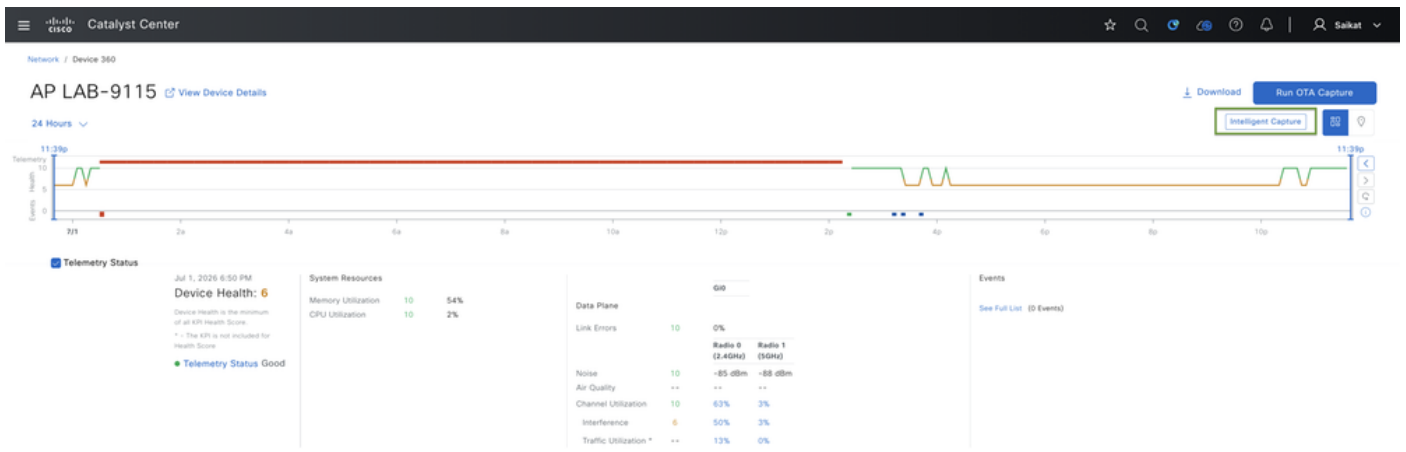
8 Line(s)

```

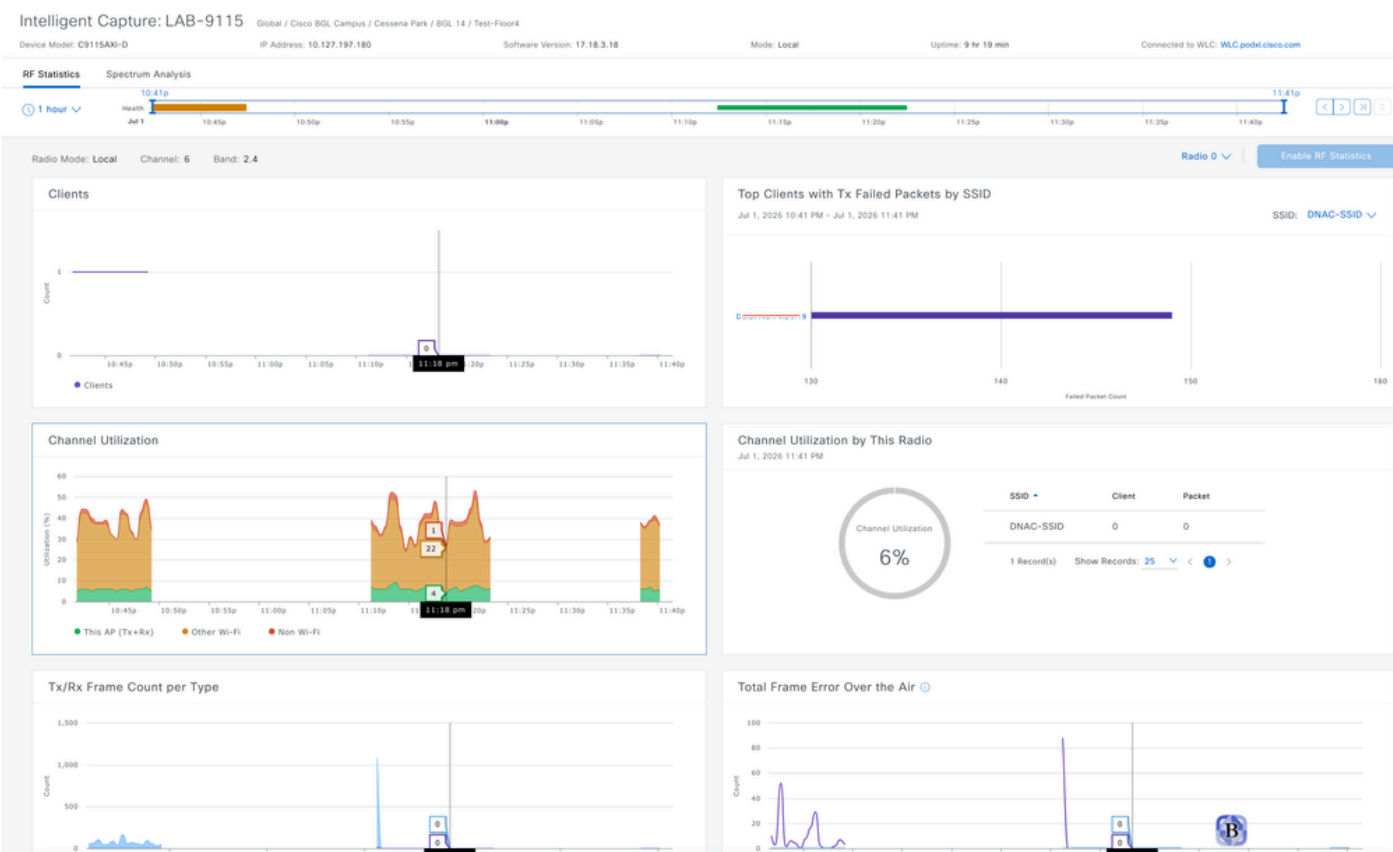
1 ap profile "default-ap-profile"
2 icap subscription client statistics enable
3 icap subscription ap statistics radio enable
4 icap subscription ap statistics wlan enable
5 icap subscription client statistics frequency
6 icap subscription ap statistics radio frequenc
7 icap subscription ap statistics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

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.



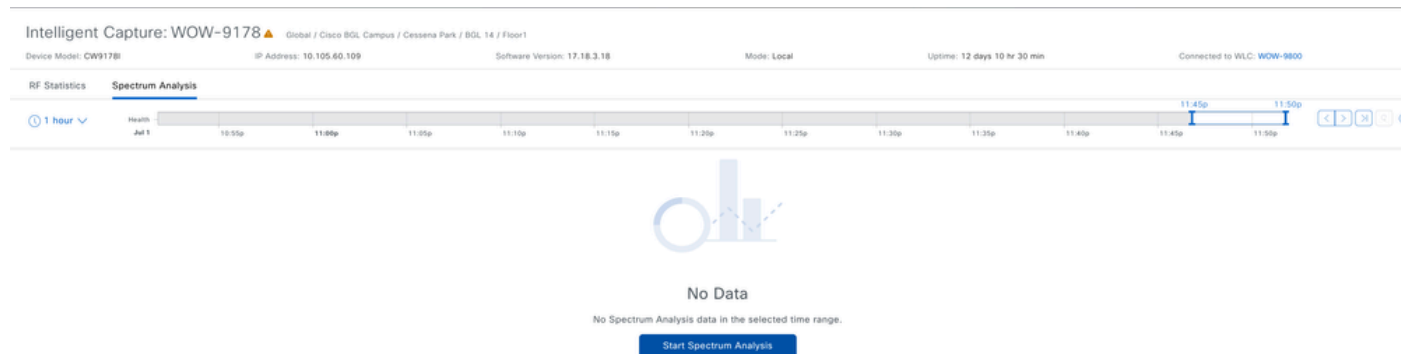
Intelligente Erfassung für AP im Gerät 360



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

## Enable Spectrum on WOW-9178

### Step 3 of 3: Preview Configuration

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

Search by device name

WOW-9800

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

Configurations - Side by side view

View by Configuration Source - All

Configuration to be Deployed

5 Line(s)

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

## Deploy

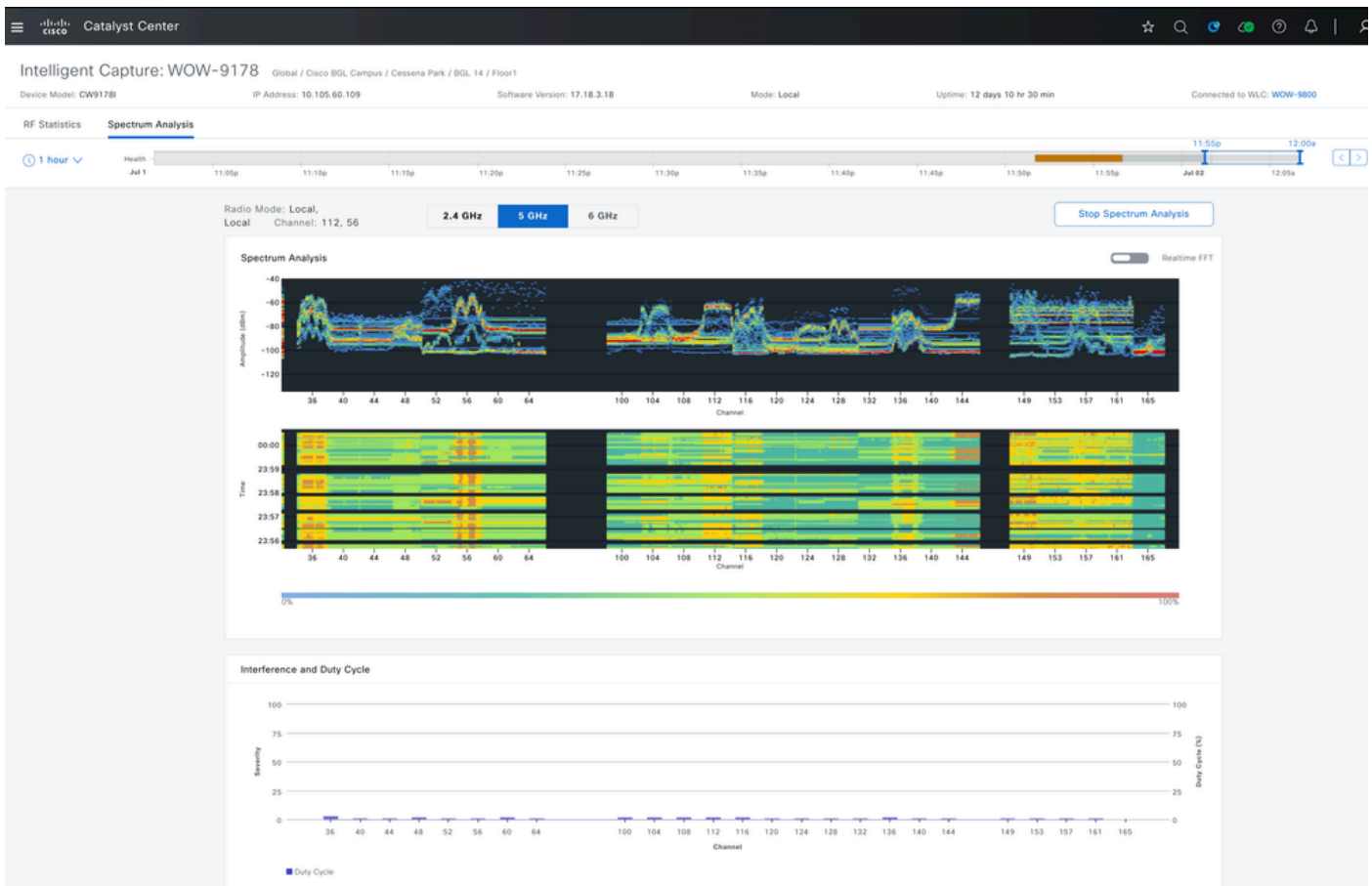
Now  Later

Task Name\*

Enable Spectrum on WOW-9178

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

Konfiguration für Spektrumanalyse angewendet

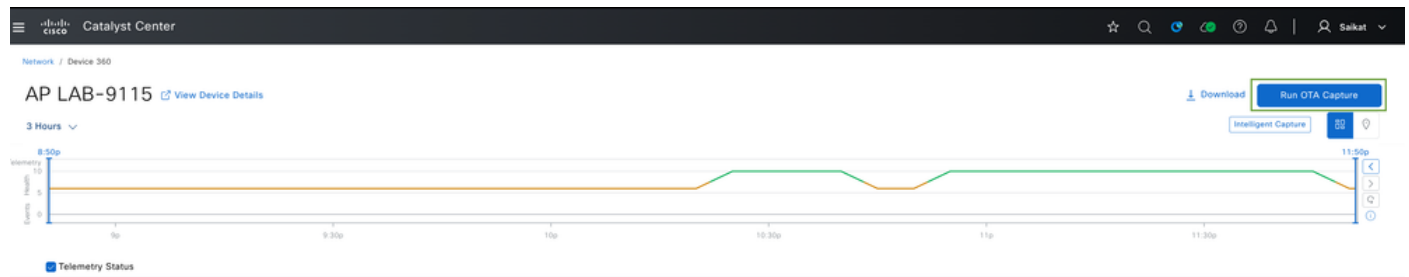


Ergebnis der Spektrumanalyse

## 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




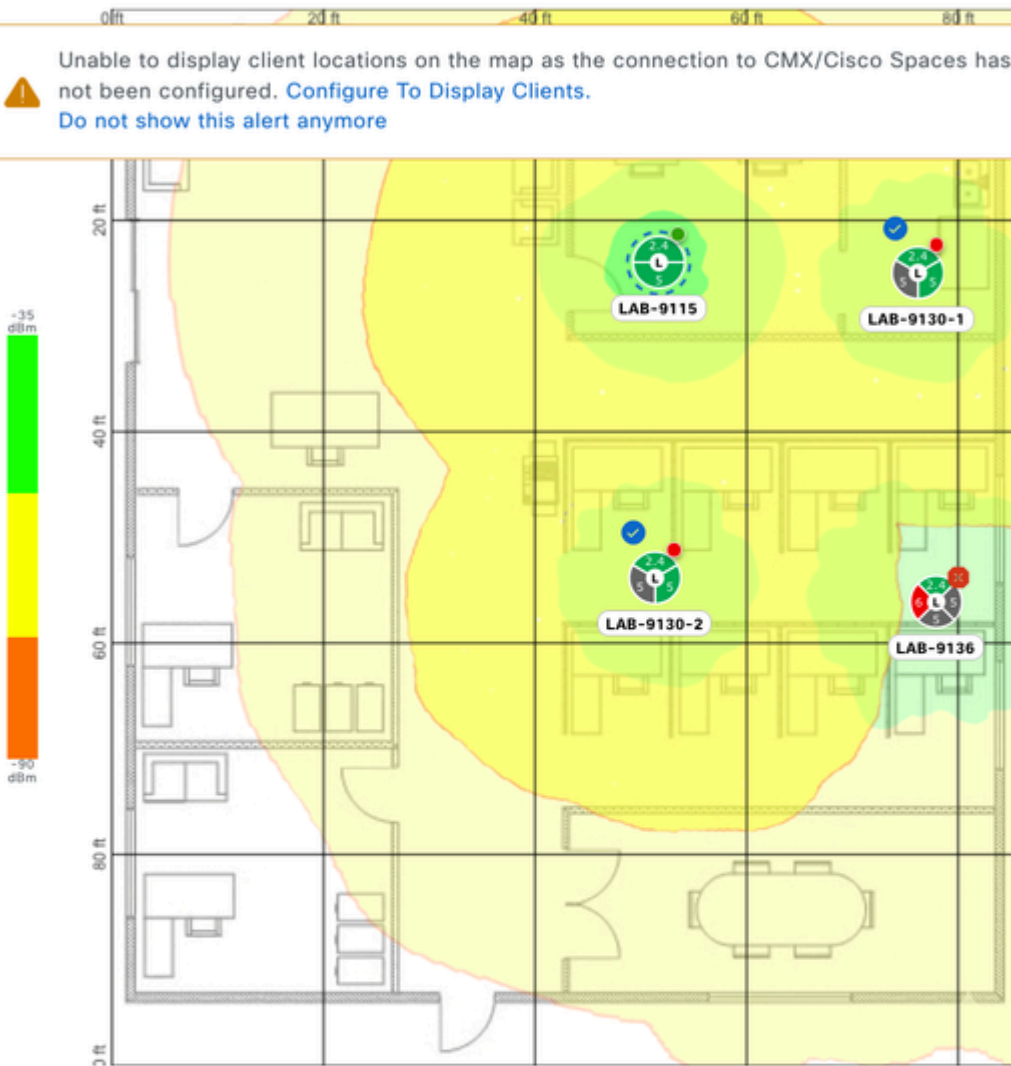
## Select Access Points

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 ⌵ ⓘ

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



LAB-9130-1 ✕

Radios: 0 (2.4 GHz),  
1 (5 GHz), 2 (5 GHz)

IP Address:  
10.127.197.184

Floor: Test-Floor4

RSSI: -36 dBm

Device 360

LAB-9130-2 ✕

Radios: 0 (2.4 GHz),  
1 (5 GHz), 2 (5 GHz)

IP Address:  
10.127.197.182

Floor: Test-Floor4

RSSI: -36 dBm

Device 360

Cancel

Next

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

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.

The screenshot shows the 'Configurations - Side by side view' in Cisco Catalyst Center. The left pane shows the 'Configuration to be Deployed' with 12 lines of configuration for two APs (LAB-9130-1 and LAB-9130-2). The right pane shows the 'Running Configuration' with 2221 lines. The configuration includes commands for shutting down radios, enabling sniffing on channels 40 and 127.0.0.1, and setting up various services like timestamps and platform qfp utilization monitoring.

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

Running Configuration (2221 Line(s))
1 Building configuration...
2
3 Current configuration : 83781 bytes
4 !
5 ! Last configuration change at 18:07:48 UTC Wed Jul 1 2026 by ad
6 !
7 version 17.18
8 service timestamps debug datetime msec
9 service timestamps log datetime msec
10 service internal
11 platform qfp utilization monitor load 80
12 !
13 hostname WLC
14 !
15 boot-start-marker
16 boot system bootflash:packages.conf
17 boot system bootflash:/packages.conf
18 boot-end-marker
19 !
20 !
```

Konfigurationsvorschau zur Aktivierung der OTA-Erfassung

The screenshot shows the 'Tasks' page in Cisco Catalyst Center. The left sidebar has filters for 'Type' (Task, Work Item) and 'Status' (Upcoming, In Progress, Success, Failed, Ready). The main area displays a list of tasks. One task, 'ICAP disable: OTA LAB-9130-1 WLC.podxl.cisco.com', is currently 'Upcoming' and scheduled for July 2, 2026, at 12:21 AM. Another task, 'Start OTA Capture for AP LAB-9115', is 'Completed' and successful, also scheduled for July 2, 2026, at 12:05 AM.

**SUMMARY**

- Type (2)
  - Task
  - Work Item
- Status (7)
  - Upcoming
  - In Progress
  - Success
  - Failed
  - Ready
- Show all
- Review Status (1)
  - Pending Review
- Last Updated (3)
  - 3 hours

**Tasks**

Monitor and manage all your scheduled network operations in one place. You can also access a quick view of recent activities from any window of Catalyst Center with the keyboard shortcut - Q + A

Search by description | 1 | Update - Latest first

**ICAP disable: OTA LAB-9130-1 WLC.podxl.cisco.com**

- Task
- system
- ASSURANCE\_ICAP
- Active
- Upcoming

Start Jul 2, 2026 12:21 AM  
Update Jul 2, 2026 12:06 AM

**Start OTA Capture for AP LAB-9115**

- Task
- saikat
- ASSURANCE\_ICAP
- Completed
- Success

Start Jul 2, 2026 12:05 AM  
Update Jul 2, 2026 12:06 AM  
End Jul 2, 2026 12:06 AM

Geplante Aufgabe bei aktivierter OTA-Erfassung

Cisco Catalyst 9800-80 Wireless Controller

Welcome admin

Search APs and Clients

Feedback

Configuration > Wireless > Access Points

All Access Points

Total APs : 4

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

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

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

1 - 4 of 4 access points

6 GHz Radios

5 GHz Radios

Total 5 GHz radios : 3

Operation Status "Is equal to" Up

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

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:

Catalyst Center

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

OTA Sniffer Capture

2 In-progress Captures 1 Completed Captures

Search Table

2 Selected Stop Capture

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

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.

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

OTA Sniffer Capture

0 In-progress Captures   **3 Completed Captures**

Search Table

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

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.


Catalyst Center Assurance / Settings / Intelligent Capture Settings

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

Access Point

AP Stats Capture **Anomaly Capture**

Intelligent Capture automatically collects and presents anomalous behavior for clients associated with enabled Access Points. You can view this data on the client Intelligent Capture page.



**Configure AP Enablement**

Specific - select specific APs and enable

Global - enable or disable capable WLCs

[Get Started](#)

## Anomalie-Erfassung konfigurieren

Catalyst Center Assurance / Settings / Intelligent Capture Settings

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

Access Point

AP Stats Capture **Anomaly Capture**

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

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

Find Hierarchy Search Help

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

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

Search Table

1 Selected **Enable**

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

[Export](#)

## Anomalie-Erfassung für bestimmten AP aktivieren

Catalyst Center Assurance / Settings / Intelligent Capture Settings

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

Access Point

AP Stats Capture **Anomaly Capture**

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

WLC.pod1.cisco.com

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

Device Name	Configuration Status	IP Address	Model	OS Version	Overall Health	Location
<input checked="" type="checkbox"/> WLC.pod1.cisco.com	Not Configured	10.127.197.194	C9800-80-K9	17.18.3	10	Global/Cisco BGL Campus/Cessena Park/BGL 14

## Globale Anomalie-Erfassung für bestimmten WLC aktivieren

Activities / Tasks ☆ 🔍 🔄 📄 ? 🔔 | 👤 Saikat ▾

Task Details / Work Item Details ✕

Search by device name 🔍

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

WLC.podxl.cisco.com ✓

Configurations - Side by side view 📄 📄

View by Configuration Source · All ▾ 🔍 Search configuration

Configuration to be Deployed ⓘ

6 Line(s)

```

1 do ap name LAB-9115 icap subscription client anomaly-detection end
2 do ap name LAB-9115 icap subscription client anomaly-detection reg
3 do ap name LAB-9115 icap subscription client anomaly-detection reg
4 do ap name LAB-9115 icap subscription client anomaly-detection pac
5 do ap name LAB-9115 icap subscription client anomaly-detection reg
6 do ap name LAB-9115 icap subscription client anomaly-detection reg

```

Running Configuration ⓘ

2243 Line(s)

```

1 Building configuration...
2
3 Current configuration : 85499 bytes
4 !
5 ! Last configuration change at 06:16:02 UTC Thu Jul 2 2026 by ad
6 !
7 version 17.18
8 service timestamps debug datetime msec
9 service timestamps log datetime msec
10 service internal
11 platform qfp utilization monitor load 80
12 !
13 hostname WLC
14 !
15 boot-start-marker
16 boot system bootflash:packages.conf
17 boot system bootflash:/packages.conf

```

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.

Catalyst Center ☆ 🔍 🔄 📄 ? 🔔 | 👤 Saikat ▾

Intelligent Capture: cxLabs-WIN11 📄

Stop Full Packet Capture 📄 Download 📄 Run Packet Capture ✕

1 hour ▾ PCAP Jul 2 11:02a 11:05a 11:10a 11:15a 11:20a 11:25a 11:30a 11:35a 11:40a 11:45a 11:50a 11:55a 12:00p

Onboarding Events 📄 LIVE

All Anomaly 📄 Export PCAP

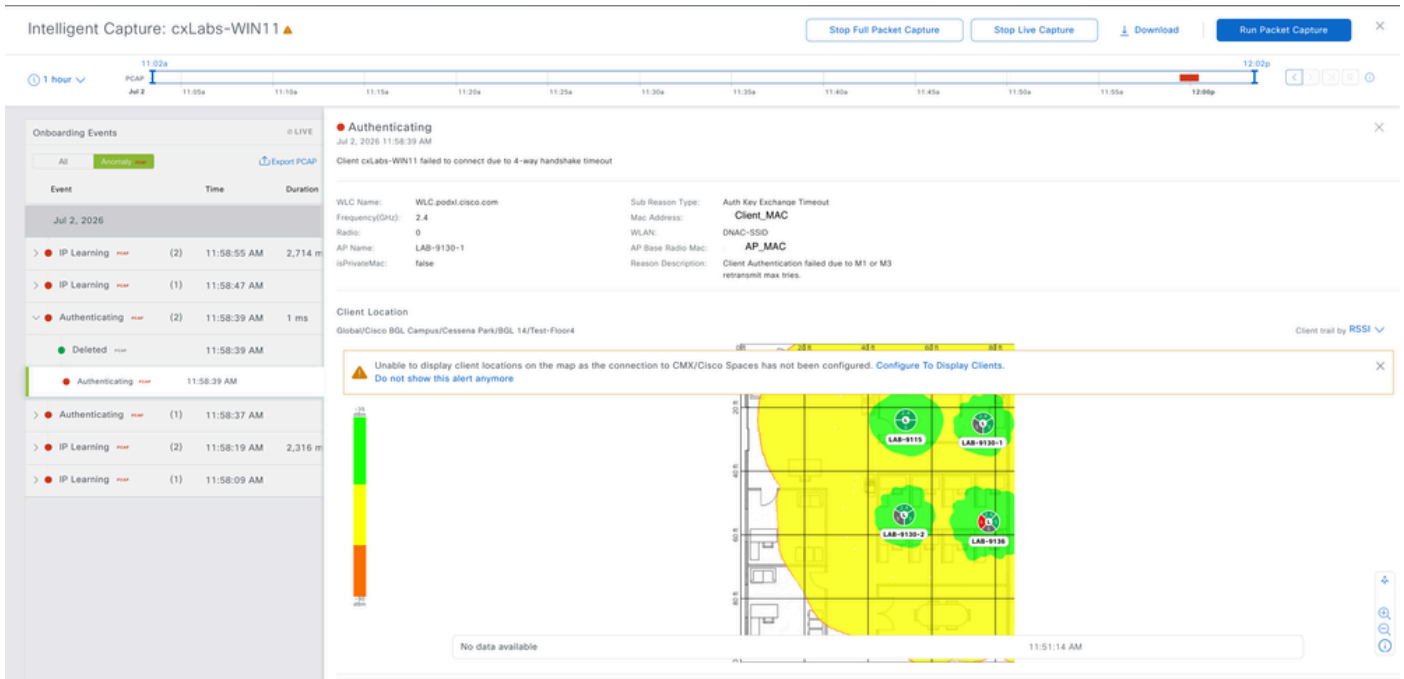
Event	Time	Duration
Jul 2, 2026		
IP Learning	(2) 11:58:55 AM	2,714 m
IP Learning	(1) 11:58:47 AM	
Authenticating	(2) 11:58:39 AM	1 ms
Deleted	11:58:39 AM	
Authenticating	11:58:39 AM	
Authenticating	(1) 11:58:37 AM	
IP Learning	(2) 11:58:19 AM	2,316 m
IP Learning	(1) 11:58:09 AM	

Authenticating Jul 2, 2026 11:58:39 AM

Client cxLabs-WIN11 failed to connect due to 4-way handshake timeout

RF Statistics

Anomalie-Erfassungsansicht für Client



Anomalie-Erfassungsdetails für Client

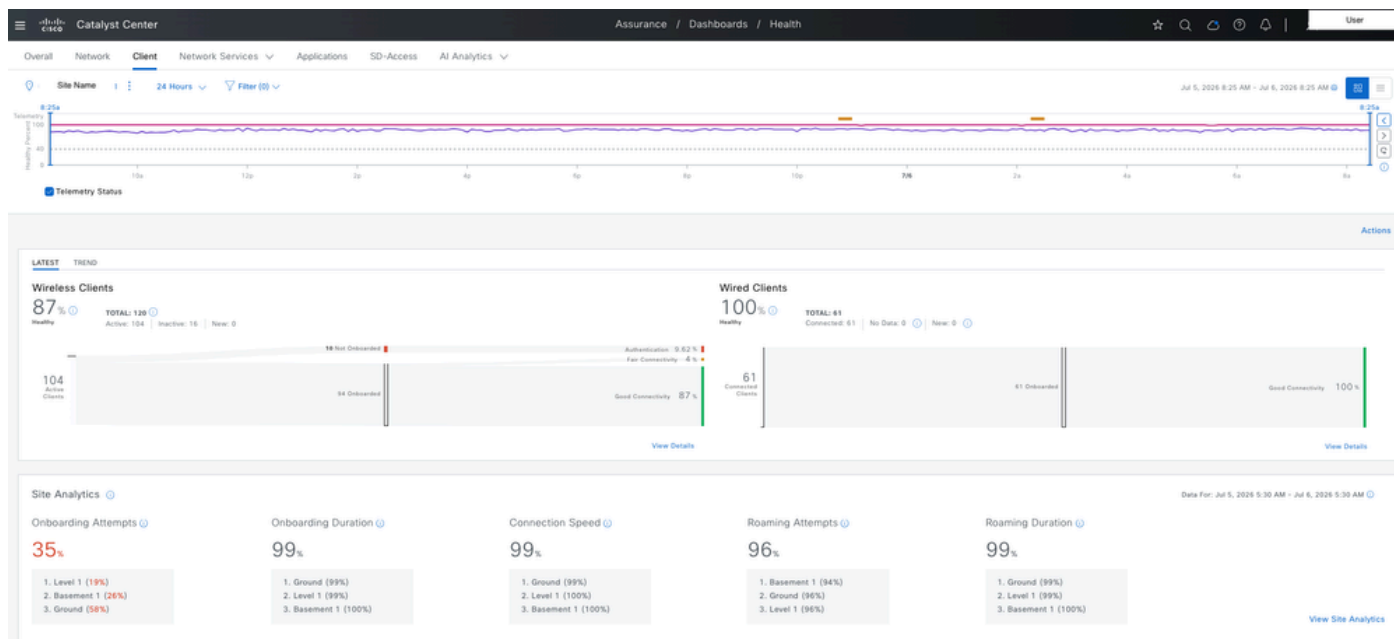
Auf diese Weise können wir unregelmäßiges oder unerwartetes Client-Verhalten (z. B. fehlgeschlagene Einbindung, Authentifizierungsprobleme oder abnorme Zuordnungsmuster) beheben, indem wir diese Ereignisse automatisch erkennen und für die APs markieren, für die sie aktiviert sind. In Kombination mit 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

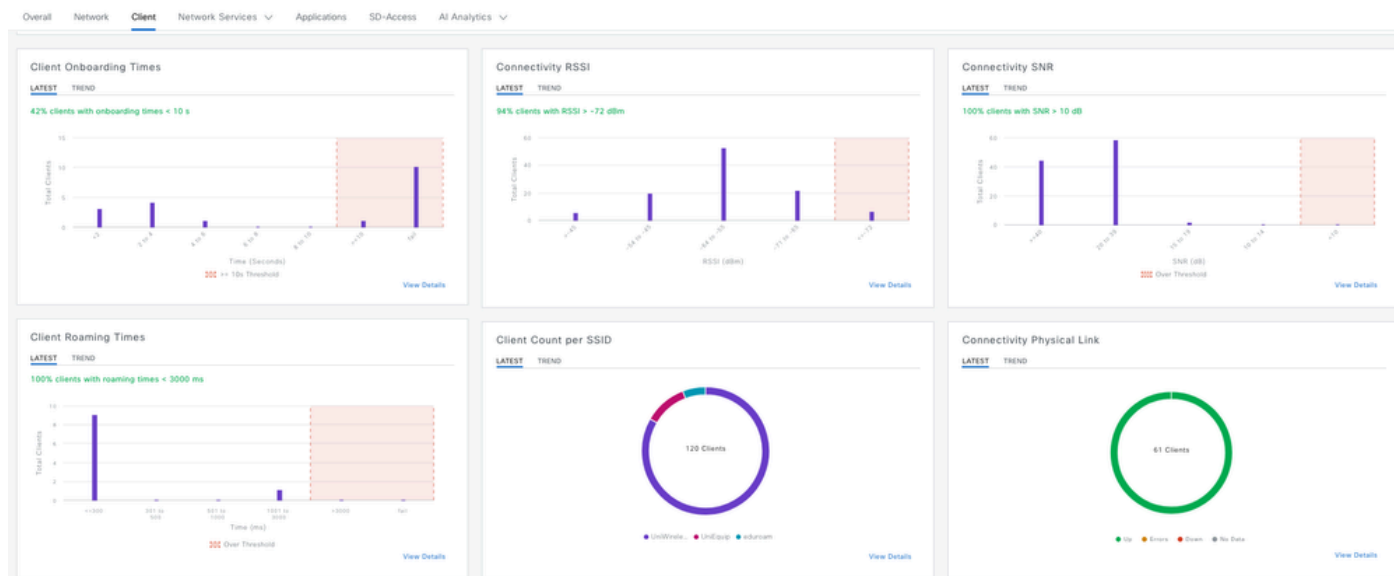
Probleme mit Wireless-Clients - Onboarding-Fehler, Roaming-Abbrüche, Funkinterferenzen oder intermittierende Verbindungen - sind häufig nur vorübergehend und schwer zu reproduzieren. Die herkömmliche abfragebasierte Überwachung ist daher für die Fehlerbehebung nicht ausreichend. Cisco Catalyst Center 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

Client Devices (120)

LATEST TREND

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

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

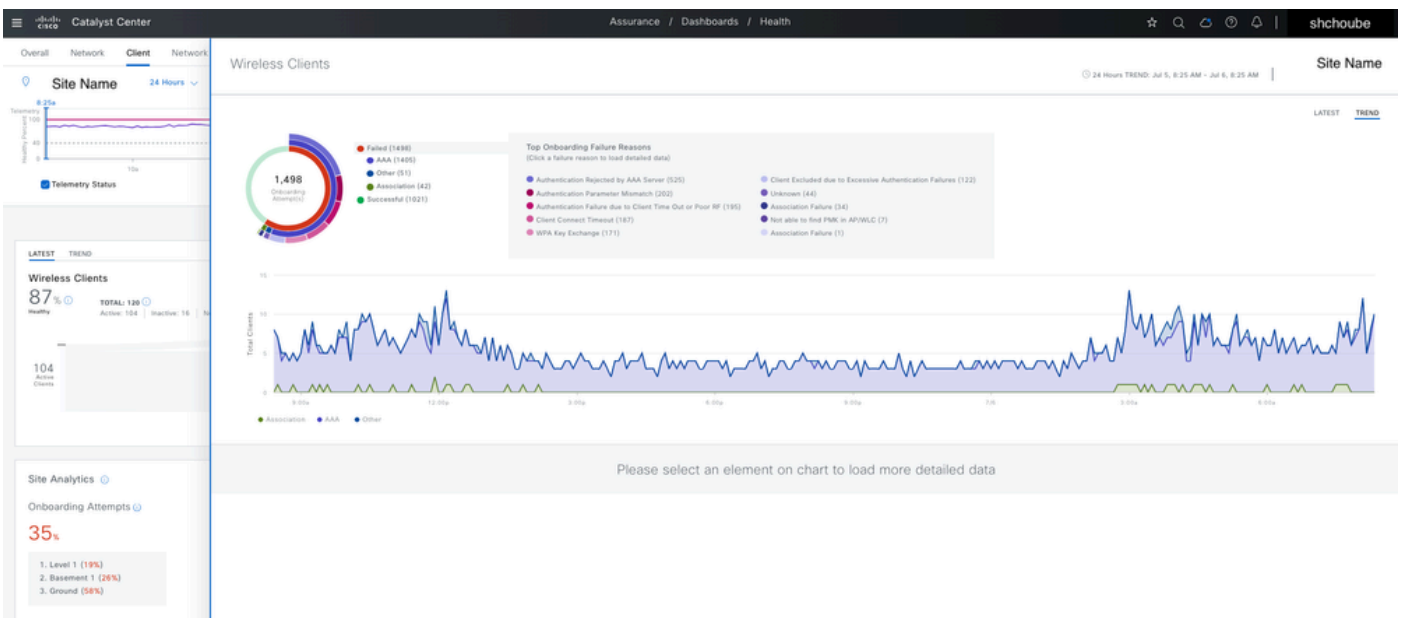
Search by name, MAC address, or IPv4/IPv6 address

0 Selected Actions

Identifier	MAC Address	IPv4 Address	Device Type	Tracked	AP Name	WLC Name	Connection Status	Band	RSSI	Last Seen	Auth Type	Roaming Time	Capability
			Murata-Manufacturing-Device	No			CONNECTED	5 GHz	-63 dBm	Jul 6, 8:21 AM	WPA2/WPA3-802.1x/802.1x-SHA256	7.695 s	11ac
			Murata-Manufacturing-Device	No			CONNECTED	5 GHz	-68 dBm	Jul 6, 8:21 AM	WPA2/WPA3-802.1x/802.1x-SHA256	7.116 s	11ac
			UNKNOWN	No			CONNECTED	2.4 GHz	-78 dBm	Jul 6, 8:23 AM	WPA2/WPA3-802.1x/802.1x-SHA256	5.263 s	Wi-Fi 6
			MacBook Pro (13-inch, M2, 2022)	No			CONNECTED	2.4 GHz	-69 dBm	Jul 6, 8:21 AM	WPA2/WPA3-802.1x/802.1x-SHA256	4.144 s	Wi-Fi 6
			Murata-Manufacturing-Device	No			CONNECTED	2.4 GHz	-68 dBm	Jul 6, 8:22 AM	WPA2/WPA3-802.1x/802.1x-SHA256	3.146 s	11n
Client Identifier	Client Mac Address	Client IP	UNKNOWN	No	AP-Name	WLC-Name	CONNECTED	2.4 GHz	--	Jul 6, 8:25 AM	WPA2/WPA3-802.1x/802.1x-SHA256	2.656 s	Unclassified
			Apple-iPhone	No			CONNECTED	5 GHz	-50 dBm	Jul 6, 8:24 AM	WPA2/WPA3-802.1x/802.1x-SHA256	2.389 s	Wi-Fi 6E
			Murata-Manufacturing-Device	No			CONNECTED	5 GHz	-74 dBm	Jul 6, 8:21 AM	WPA2/WPA3-802.1x/802.1x-SHA256	1.142 s	11ac
			Murata-Manufacturing-Device	No			CONNECTED	5 GHz	-51 dBm	Jul 6, 8:23 AM	WPA2/WPA3-802.1x/802.1x-SHA256	1.122 s	11ac
			Apple-iPhone	No			CONNECTED	5 GHz	-51 dBm	Jul 6, 8:21 AM	WPA2/WPA3-802.1x/802.1x-SHA256	1.028 s	Wi-Fi 6
			UNKNOWN	No			CONNECTED	2.4 GHz	--	Jul 6, 8:21 AM	WPA2/WPA3-802.1x/802.1x-SHA256	0.754 s	Wi-Fi 6
			Un-Classified Device	No			CONNECTED	5 GHz	-57 dBm	Jul 6, 8:25 AM	WPA2-802.1x	0.753 s	Wi-Fi 6E

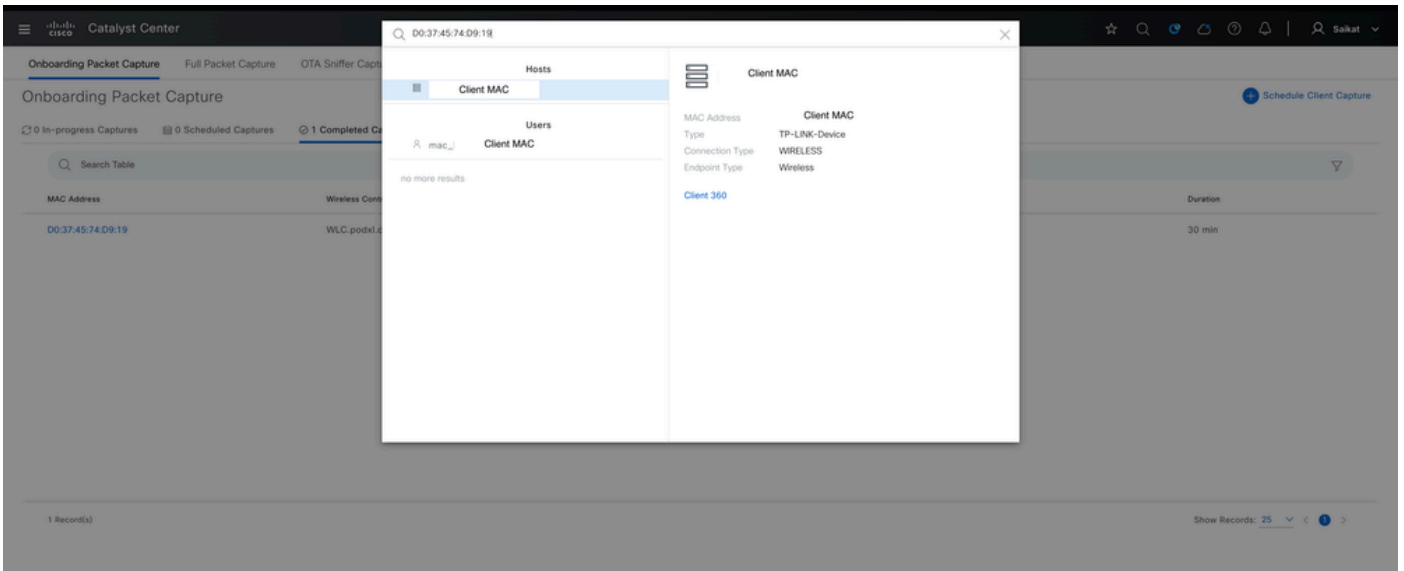
120 Record(s) Show Records: 50 1 - 50

### Wireless-Client - Statistiken zu Catalyst Center

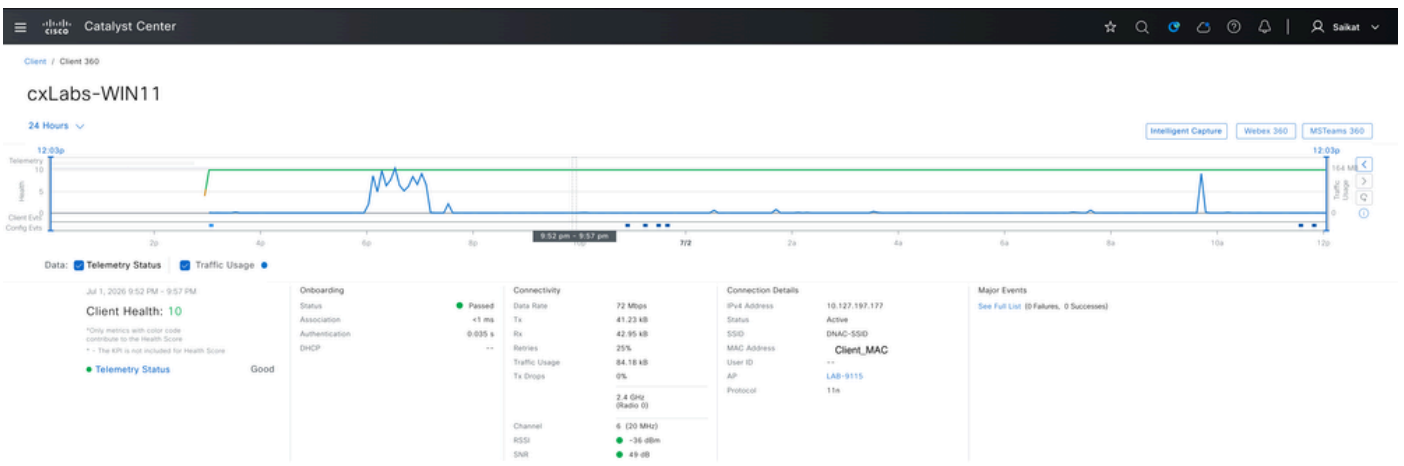


### Wireless-Client - Statistiken zu Catalyst Center

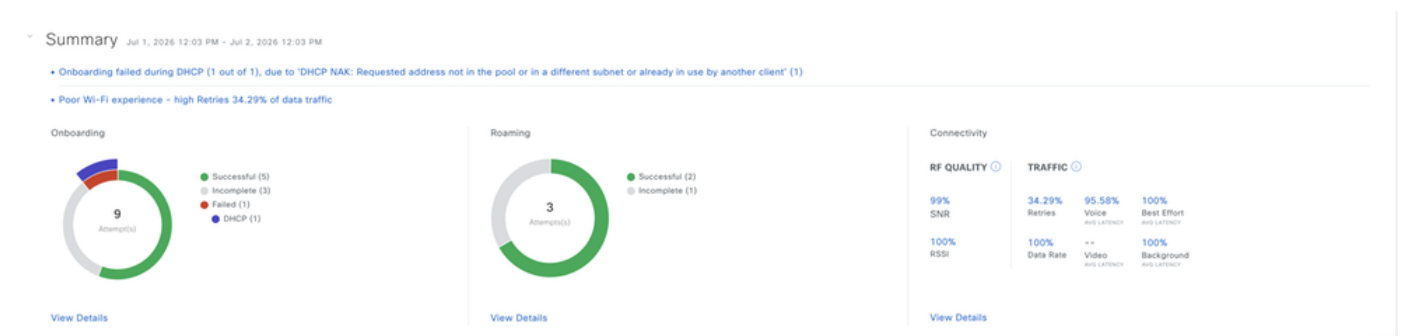
Zur Fehlerbehebung bei einem bestimmten Client können Sie anhand der MAC-Adresse des Clients suchen, über die Sie zur Client 360-Ansicht gelangen. Diese Seite enthält detaillierte, kundenspezifische Statistiken, einschließlich Onboarding-Verlauf, Anbindungsereignisse, RF-Metriken und Sitzungsdetails, 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



**Event Viewer** | Current Data Selected: [Location - Select Location](#) | [Type - onboarding](#) | [DHCP](#) | [Jul 1, 2026 12:03 PM - Jul 2, 2026 12:03 PM](#) | [Export](#)

**Impact Analysis** | [Go to Global Event Viewer](#) | [Export](#) | [Full Screen](#)

**Correlation**

Für den Client gemeldetes Ereignis im Detail

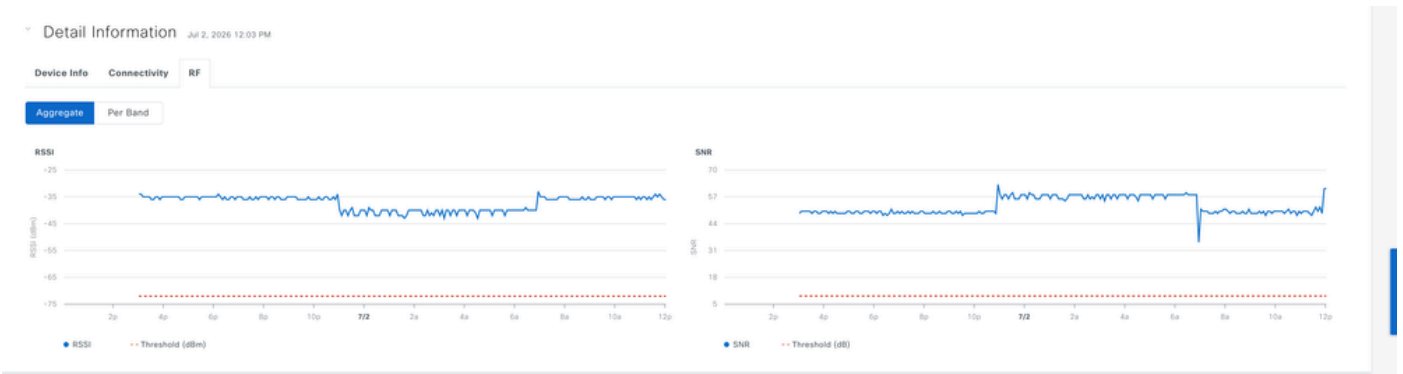
**Detail Information** Jul 2, 2026 12:03 PM

Device Info | Connectivity | RF

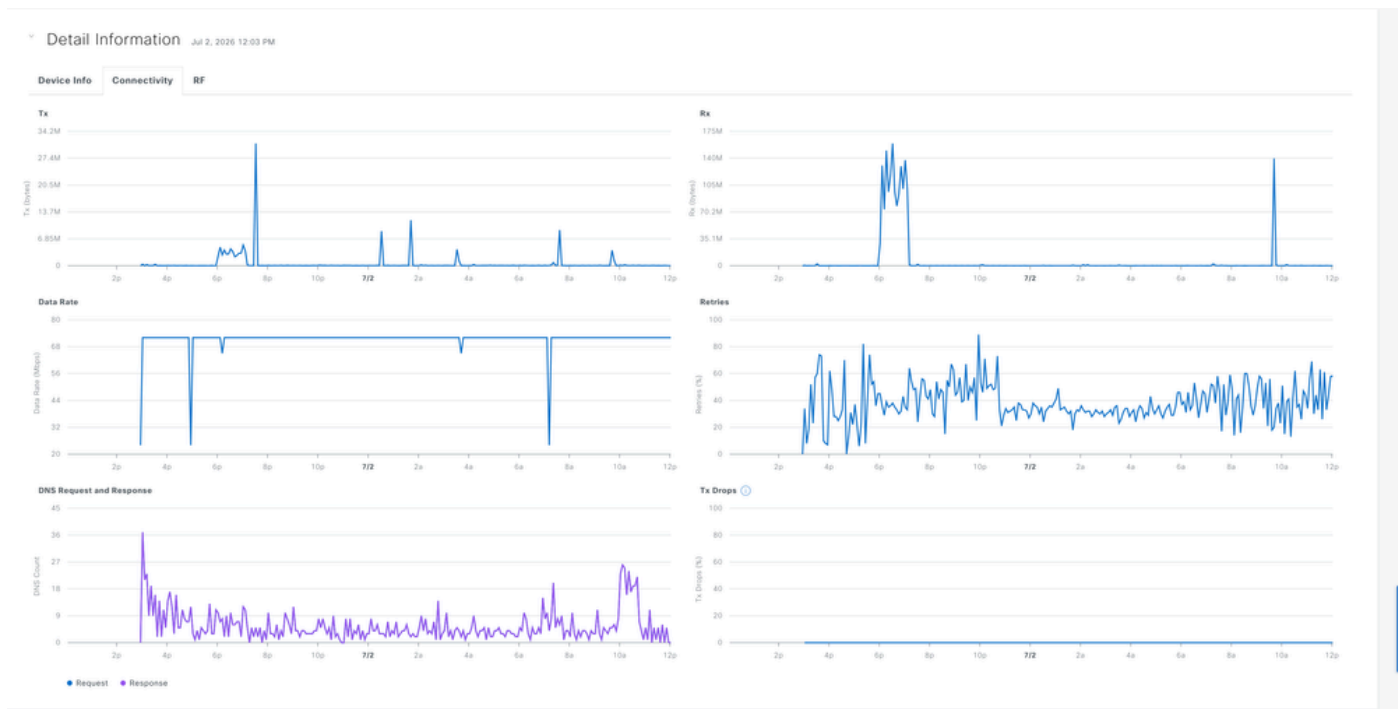
Information		Connection Information	
Device Type	TP-LINK-Device	WMM	--
Operating System	--	U-APSD	--
User ID	--	Band	--
Host Name	cxLabs-WIN11	Radio	--
MAC Address	--	Spatial Streams	--
IPv4 Address	10.127.197.177	Channel	--
IPv6 Address	fe80::85d3e54:8b7b:fb66 (1 more)		
Status	Disconnected		
Hardware Manufacturer	--		
Endpoint Type	--		
VLAN ID	97		
Association Protocol	11n		
Protocol Capability	11n		
L3 Virtual Network	--		
L2 Virtual Network	--		
Tracked	No		
Exclusion	No		
Bridge-Network Virtual Network	NA		

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

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).

The screenshot shows the 'Schedule Client Capture' configuration window in Cisco Catalyst Center. The window title is 'Schedule Client Capture'. It displays a search for client devices with the following table:

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

The 'WLC.podxi.cisco.com' device is selected, and its configuration is shown in the 'Wireless Controllers' section below the table.

The screenshot shows the 'Onboarding Packet Capture' window in Cisco Catalyst Center. It displays a table with the following data:

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

The 'Client-MAC' entry is selected, and a 'Schedule Client Capture' button is visible in the top right corner.

Geplante Erfassung des Onboarding

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



Work Item · ASSURANCE\_ICAP

Completed · Ready | Pending Review

Start: Jul 1, 2026 6:12 PM End: Jul 1, 2026 6:12 PM

As of: 11:31:42 AM [Refresh](#)

Search by device name

Device IP: 10.127.197.194 Site: Global/Cisco BGL Campus/Ce... [Back to workflow progress](#)

WLC.podxl.cisco.com

### Configurations - Side by side view

View by Configuration Source · All

Search configuration

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

## 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.

Catalyst Center Assurance / Settings / Intelligent Capture Settings

Onboarding Packet Capture Full Packet Capture OTA Sniffer Capture Access Point

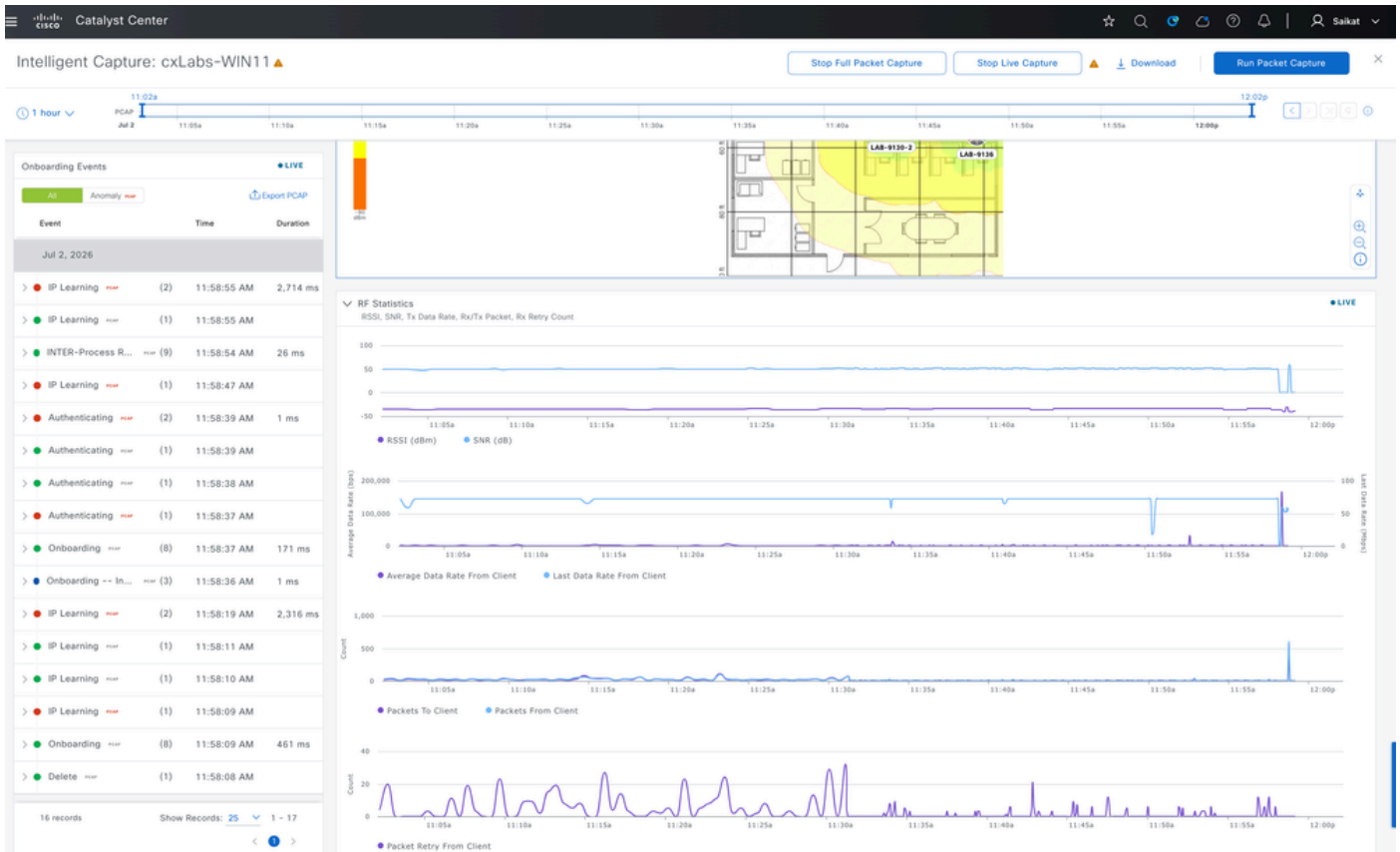
### Onboarding Packet Capture

0 In-progress Captures 0 Scheduled Captures 1 Completed Captures [Schedule Client Capture](#)

Search Table

MAC Address	Wireless Controller	Start Time	End Time	Duration
<a href="#">Client_MAC</a>	WLC.podxl.cisco.com	Jul 2, 2026 11:32 AM	Jul 2, 2026 12:02 PM	30 min

## Abgeschlossene Onboarding-Erfassung

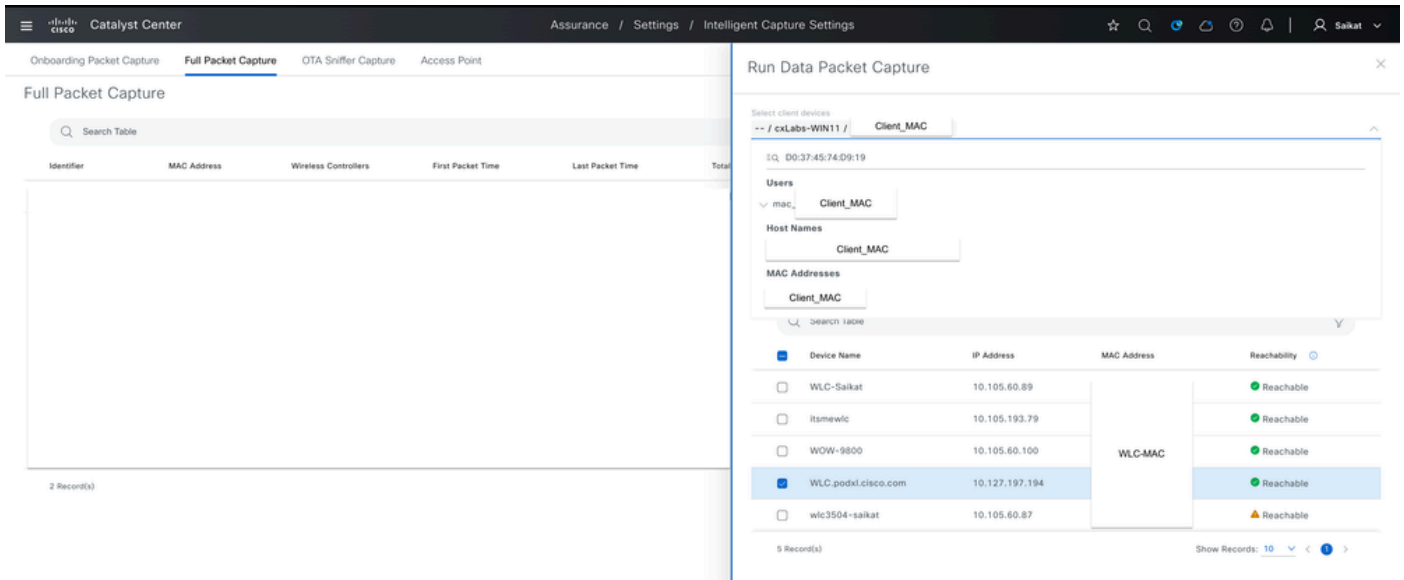


Beispiel für eine vollständige Erfassung des Onboarding-Prozesses

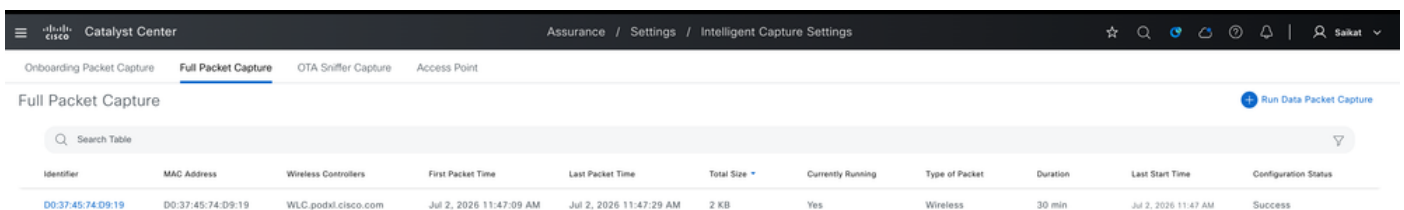
## Vollständige Paketerfassung

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.

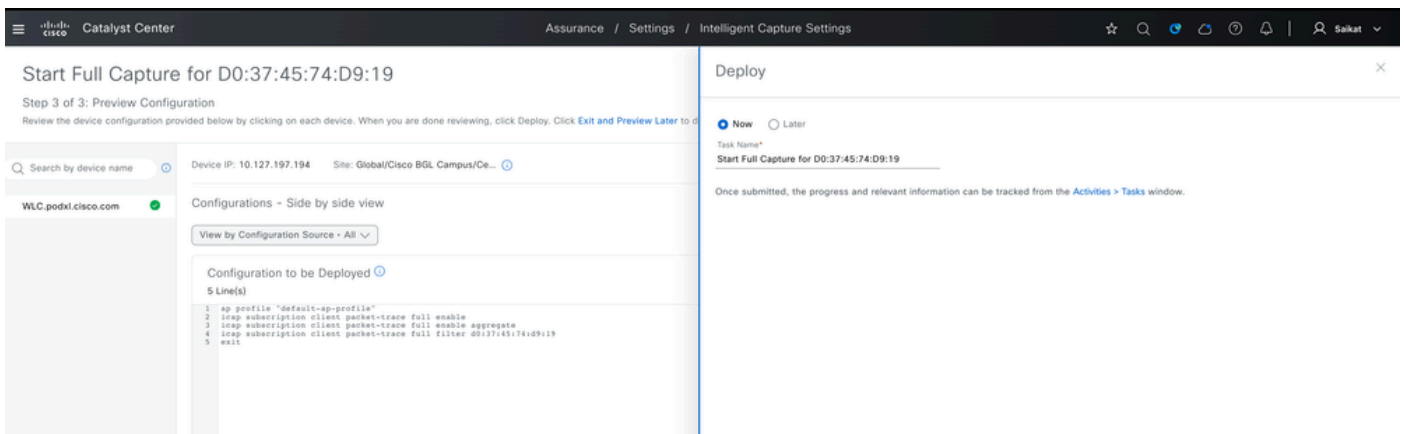
So aktivieren Sie Full Packet Capture: [Navigate to Assurance > Settings > Intelligent Capture Settings > Onboarding Capture > Run Data Capture](#) (in der oberen rechten Ecke) > [Search for Client Identifier \(MAC-Adresse\):](#)



Vollständige Paketerfassung für Client

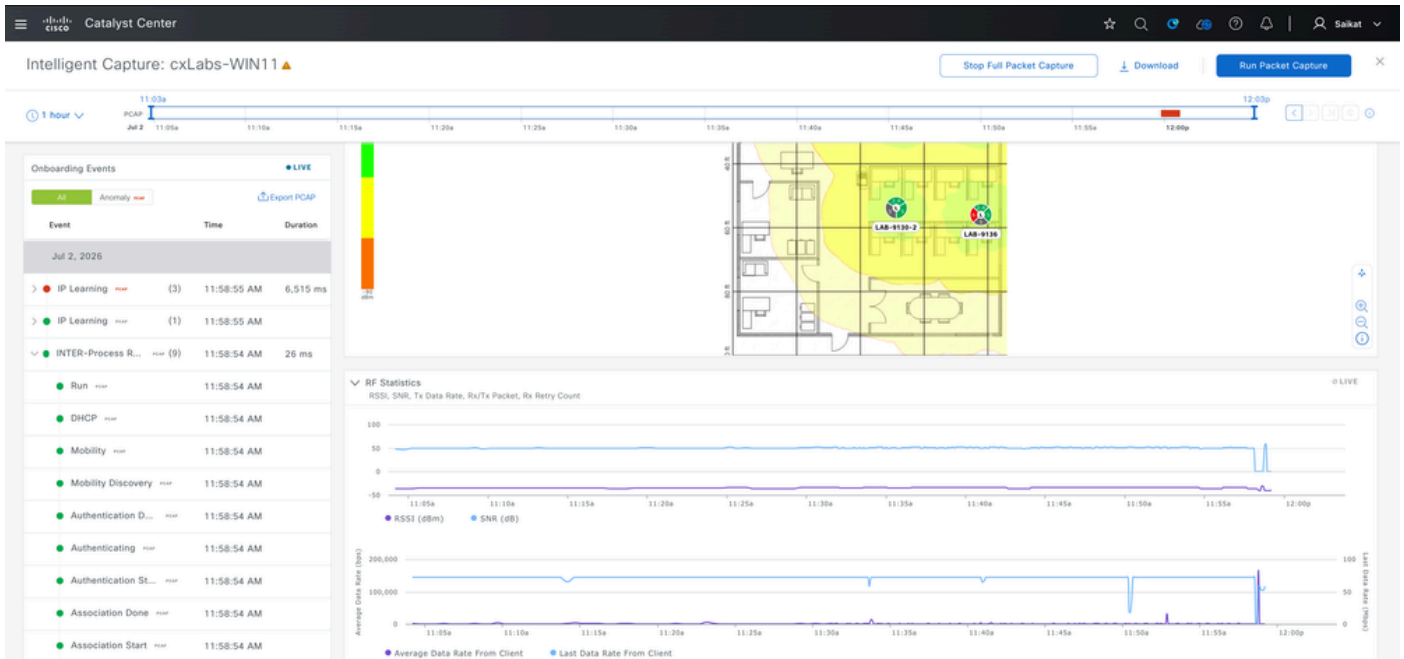


Geplante vollständige Paketerfassung für Client



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.

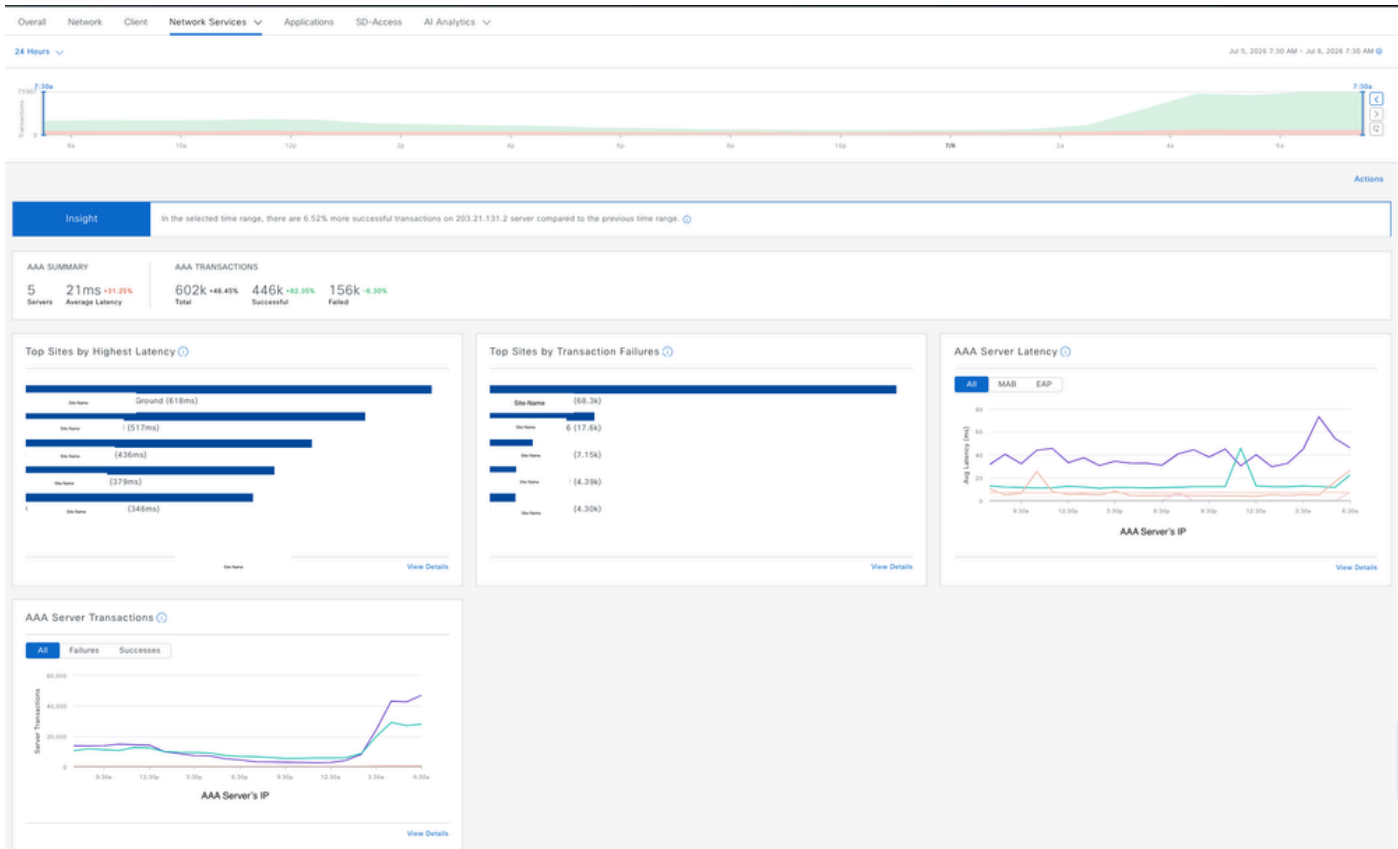


Beispiel für vollständige Erfassung für Client erfasst

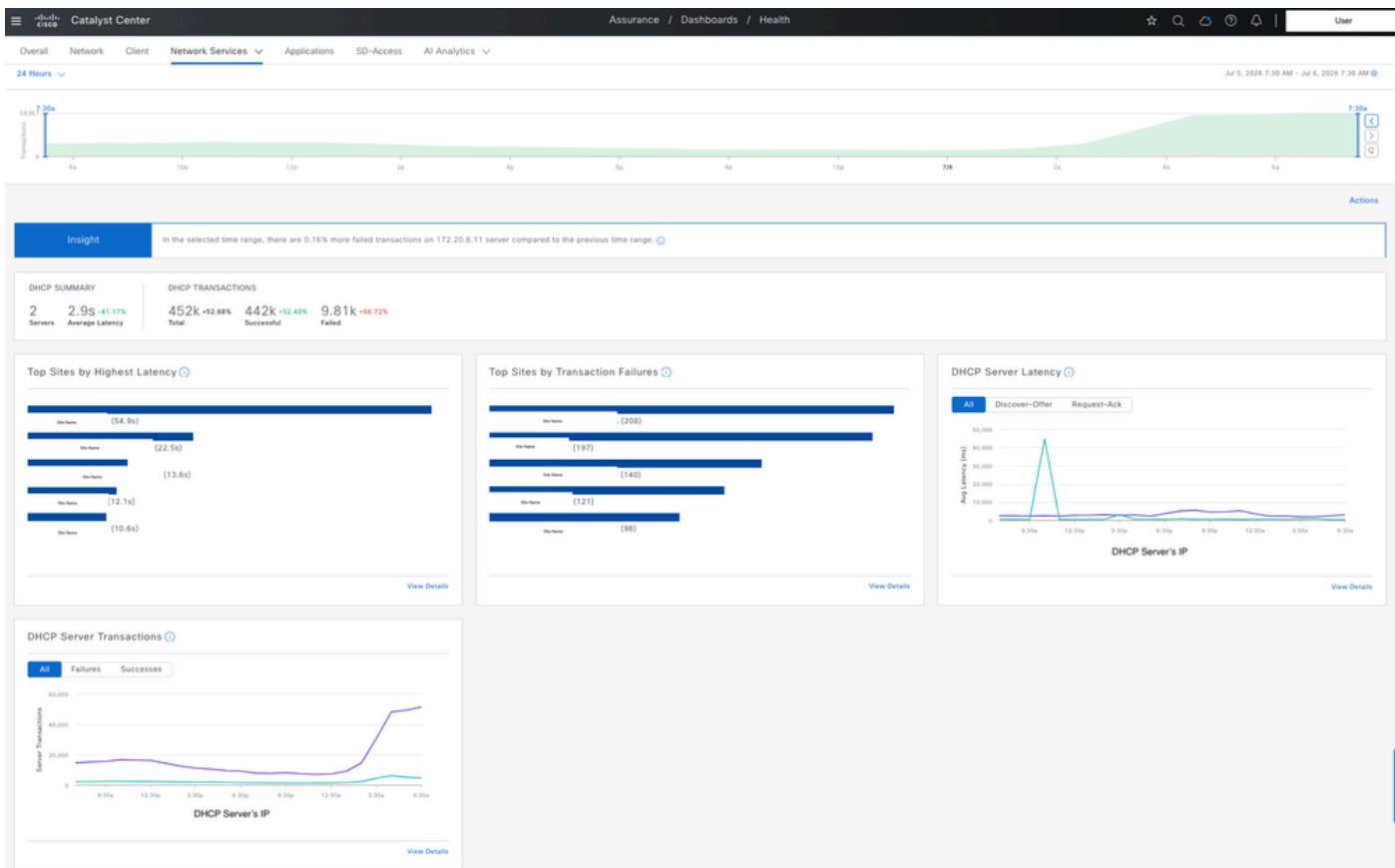
## Isolierung von Netzwerkeserviceproblemen (AAA, DHCP, DNS)

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:



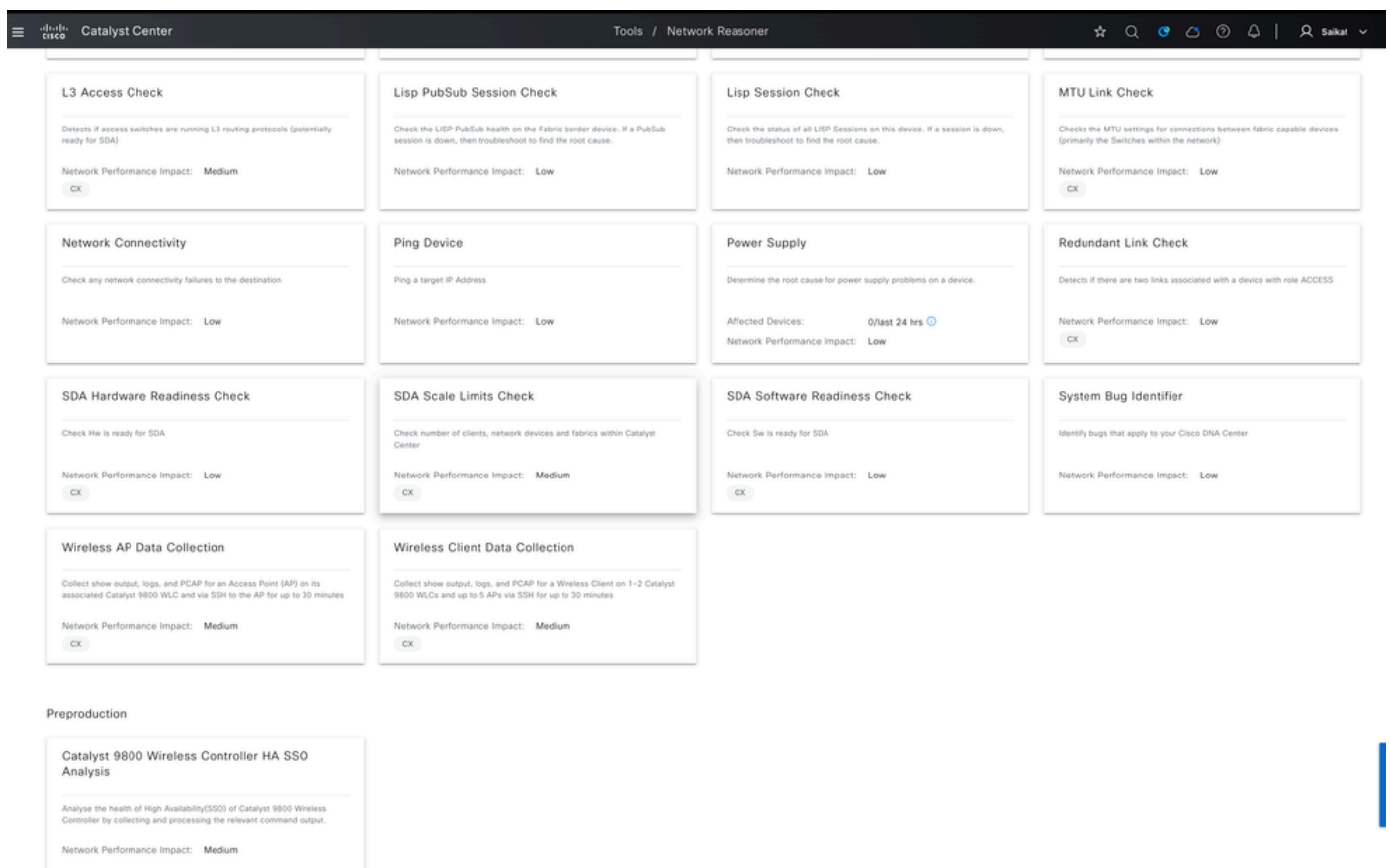
Wireless-Client - AAA-Statistiken zu Catalyst Center



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.



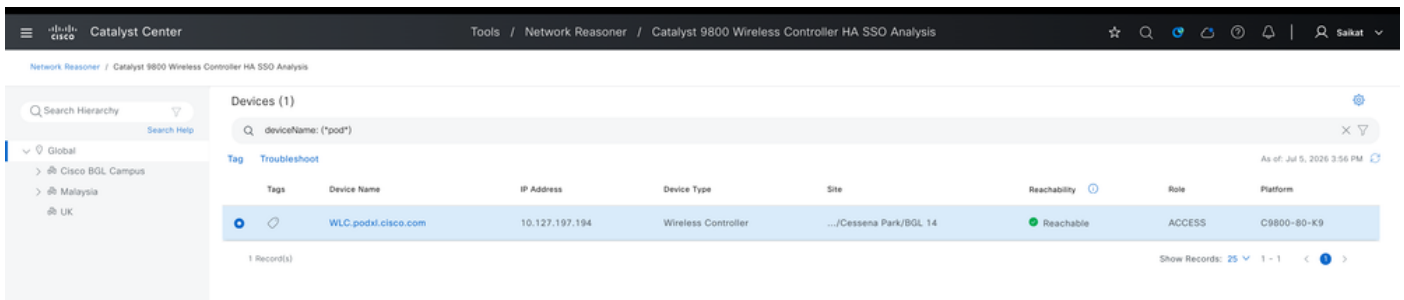
Verschiedene Optionen zur Behebung von Netzwerkfehlern im Network Reasoner

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?

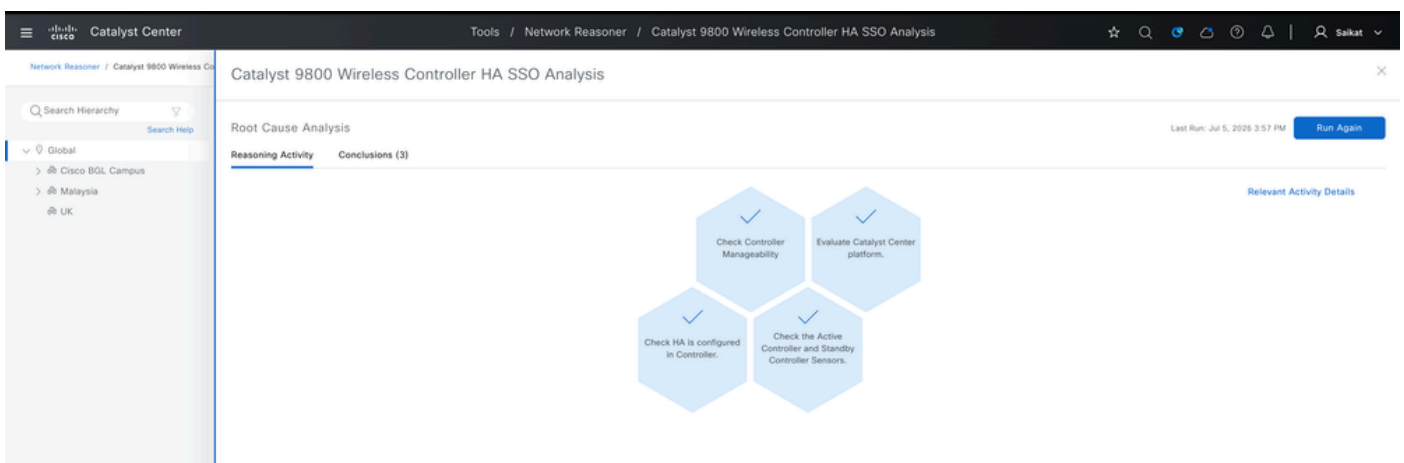
Wenn es ein Problem findet, sagt es Ihnen genau, was falsch ist und schlägt vor, wie es zu beheben. Es gibt auch eine separate Option für die Fehlerbehebung von Geräten, die überhaupt keine Überwachungsdaten senden.



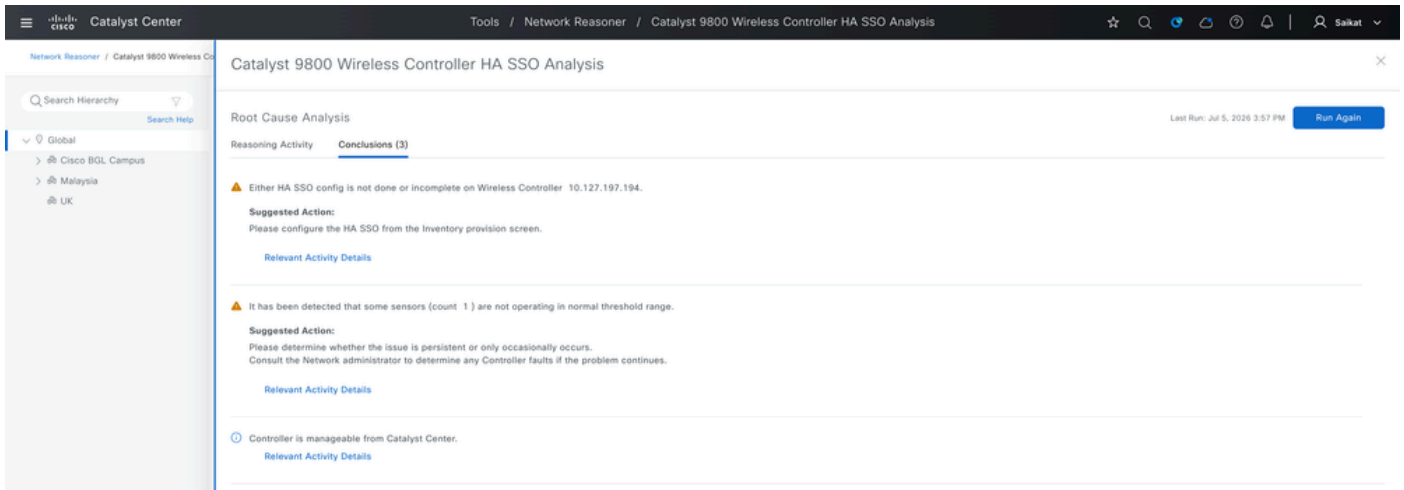
Fehlerbehebung bei HA mit Network Reasoner

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.

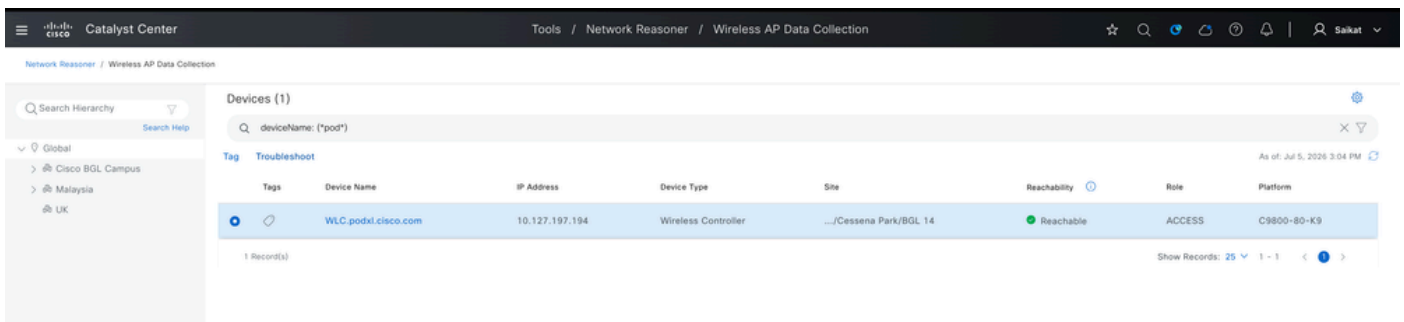


Von CATC für HA SSO-Analyse durchgeführte Aufgaben

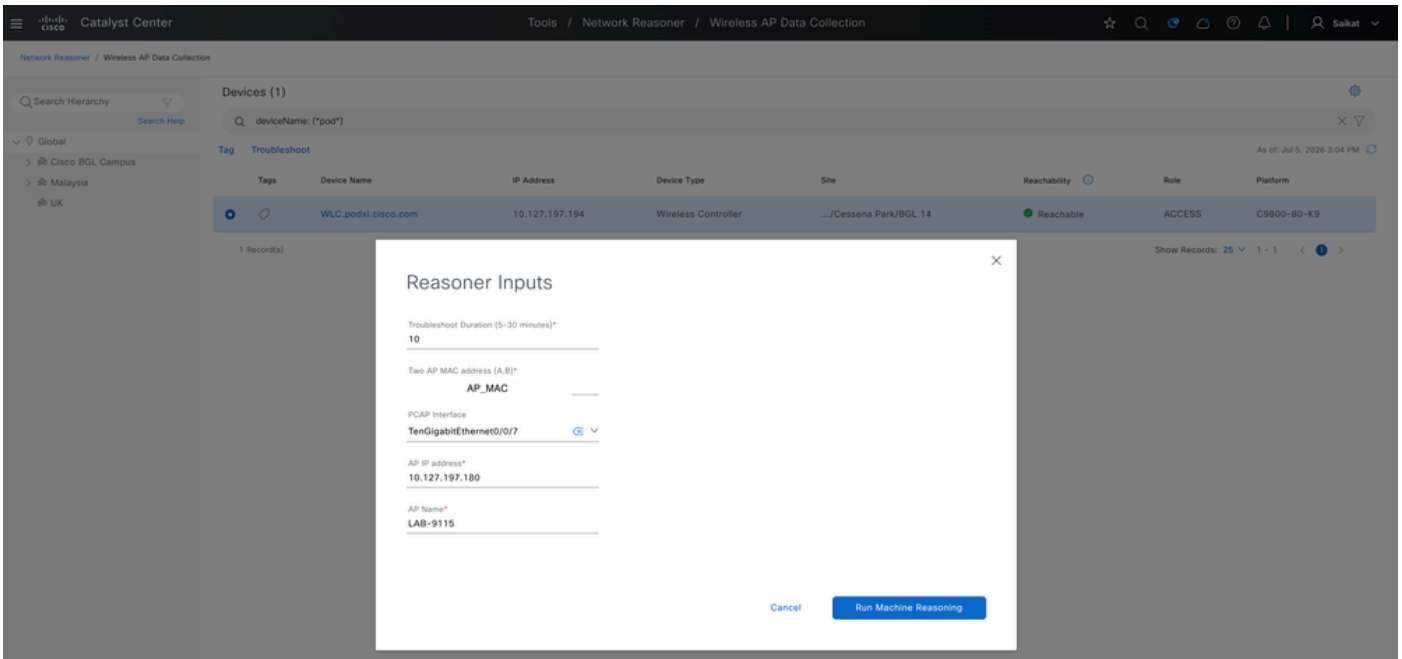


Fazit-Beispiel für HA SSO-Fehlerbehebung mit Network Reasoner

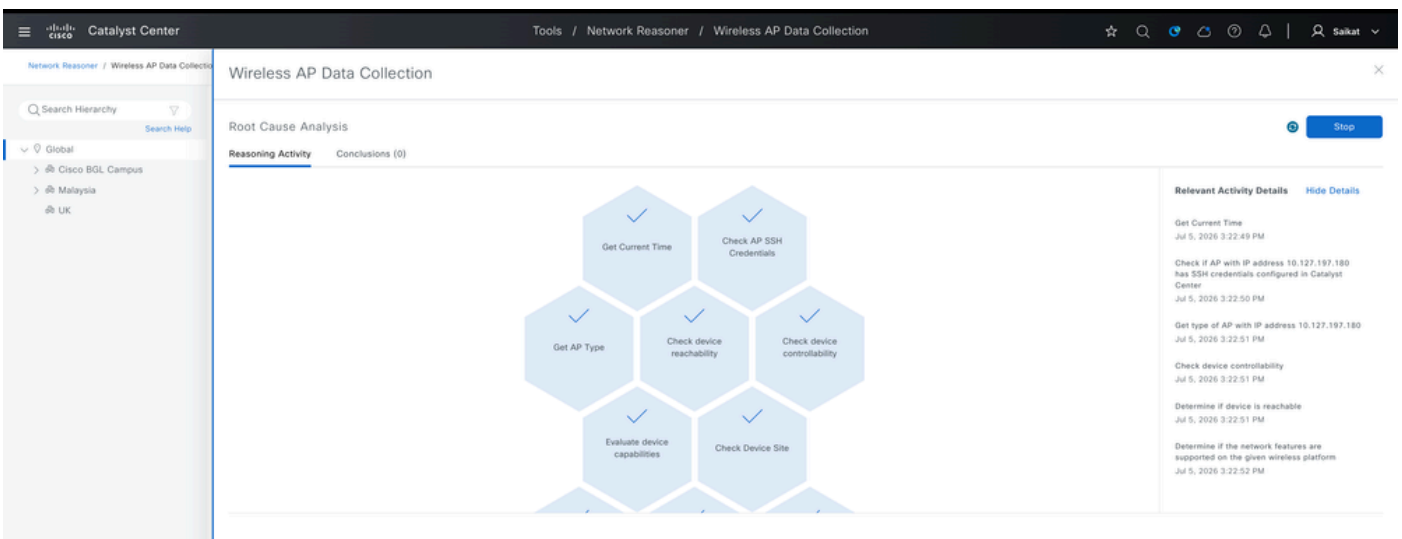
2. Access Points - Wenn bei einem Access Point Probleme auftreten, wählen Sie den Controller aus, der den Access Point verwaltet, und geben Sie dann die MAC-Adresse des Access Points ein. Legen Sie die Dauer für die Prüfung fest. Sie ermöglicht die Protokollierung und Paketerfassung vom WLC und AP und 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:



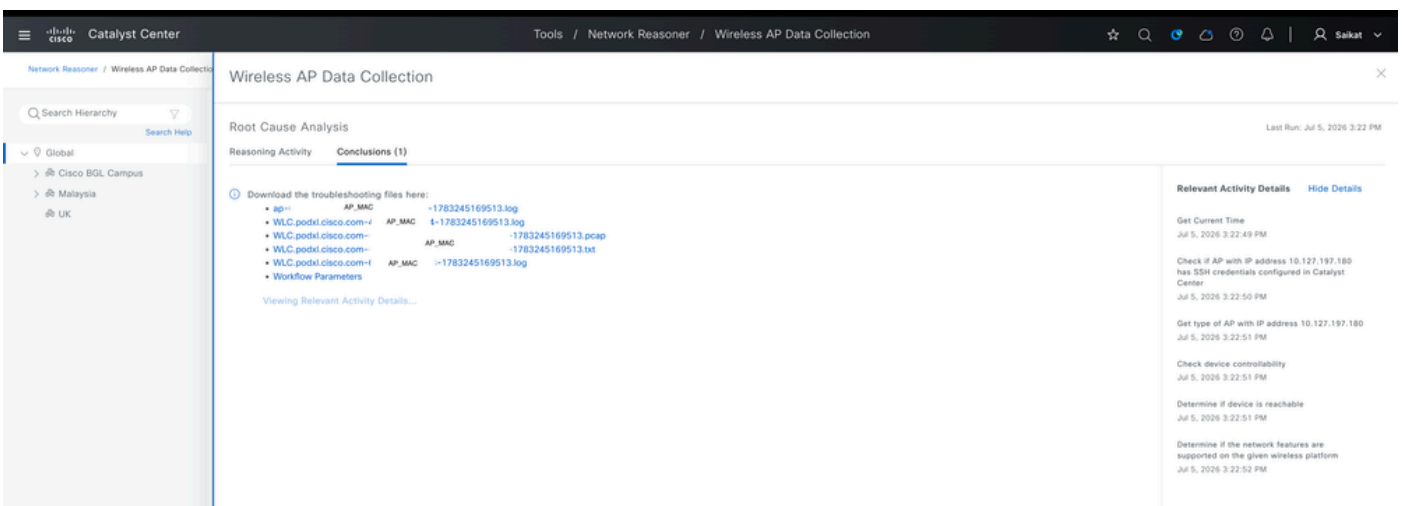
Verwalteten AP WLC zur Fehlerbehebung auswählen



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 10.127.197.194

Jul 5, 2026 5:04:57 PM

Start AP statistics collection on WLC with IP address 10.127.197.194 and wait for data collection for 30 seconds

Jul 5, 2026 5:04:58 PM

Start logging on COS AP with IP address 10.127.197.180 over SSH for feature set apDataCollection, saved into file bootflash:<file-name>

Jul 5, 2026 5:04:59 PM

Stop AP statistics collection on WLC with IP address 10.127.197.194 with data saved into file bootflash:<file-name>

Jul 5, 2026 5:10:00 PM

Stop data collection on COS AP with IP address 10.127.197.180 over SSH for feature set apDataCollection, saved into file bootflash:<file-name>

Jul 5, 2026 5:10:01 PM

Start AP show-tech wireless collection on WLC with IP address 10.127.197.194 for AP name LAB-9115 and save into file bootflash:<file-name>

Jul 5, 2026 5:10:02 PM

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

Jul 5, 2026 5:10:07 PM

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

Jul 5, 2026 5:10:15 PM

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

Jul 5, 2026 5:10:20 PM

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

Jul 5, 2026 5:10:27 PM

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

Jul 5, 2026 5:10:34 PM

Stop AP show-tech wireless collection on WLC with IP address 10.127.197.194 with data saved into file bootflash:<file-name>

Jul 5, 2026 5:10:35 PM

Start to upload file bootflash:<file-name> from WLC with IP address 10.127.197.194 to https://10.105.197.194/<file-name>

Jul 5, 2026 5:10:36 PM

Check if file bootflash:<file-name> has been uploaded successfully from WLC with IP address 10.127.197.194 to https://10.105.197.194/<file-name>

Jul 5, 2026 5:10:41 PM

File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to https://10.105.197.194/<file-name>

Jul 5, 2026 5:10:41 PM

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

Jul 5, 2026 5:10:41 PM

Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127.197.194

Jul 5, 2026 5:10:43 PM

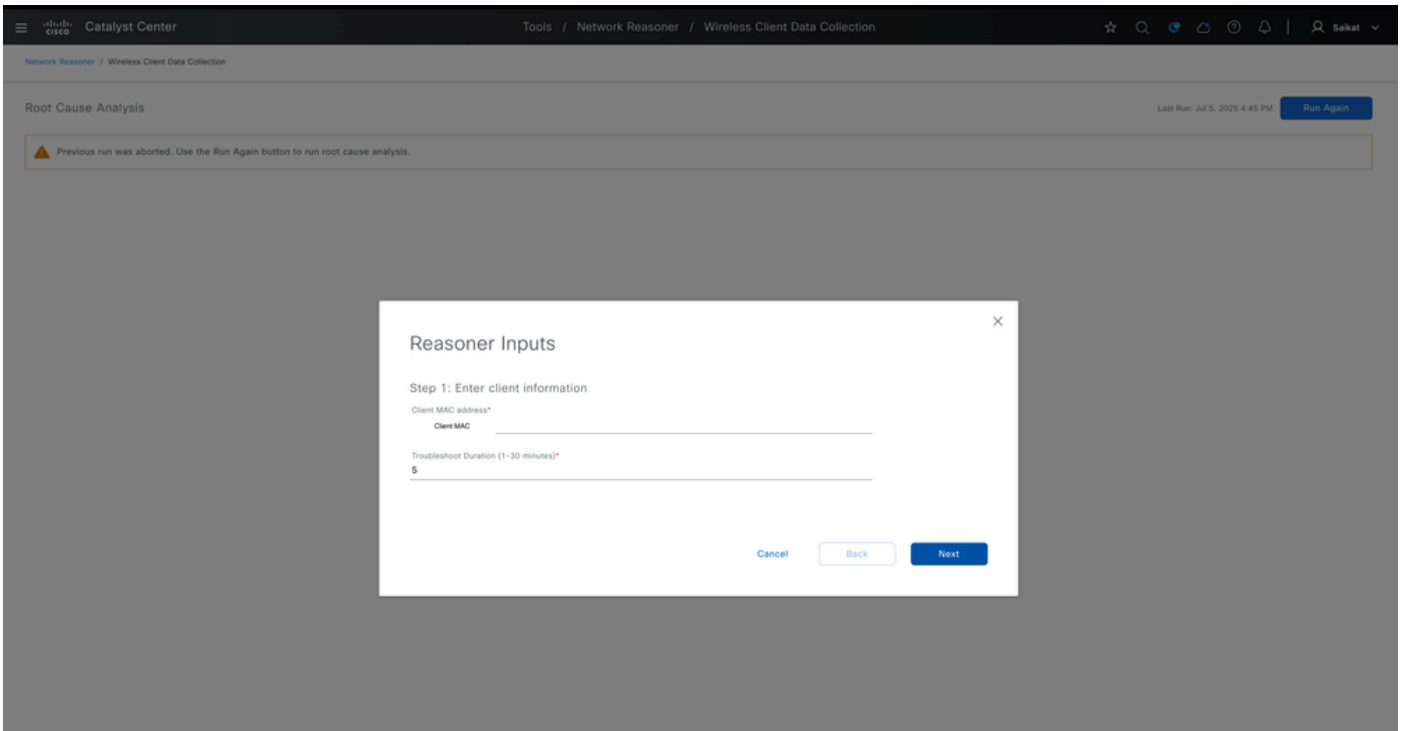
Stop RA Trace for AP: <MAC>

Jul 5, 2026 5:10:46 PM

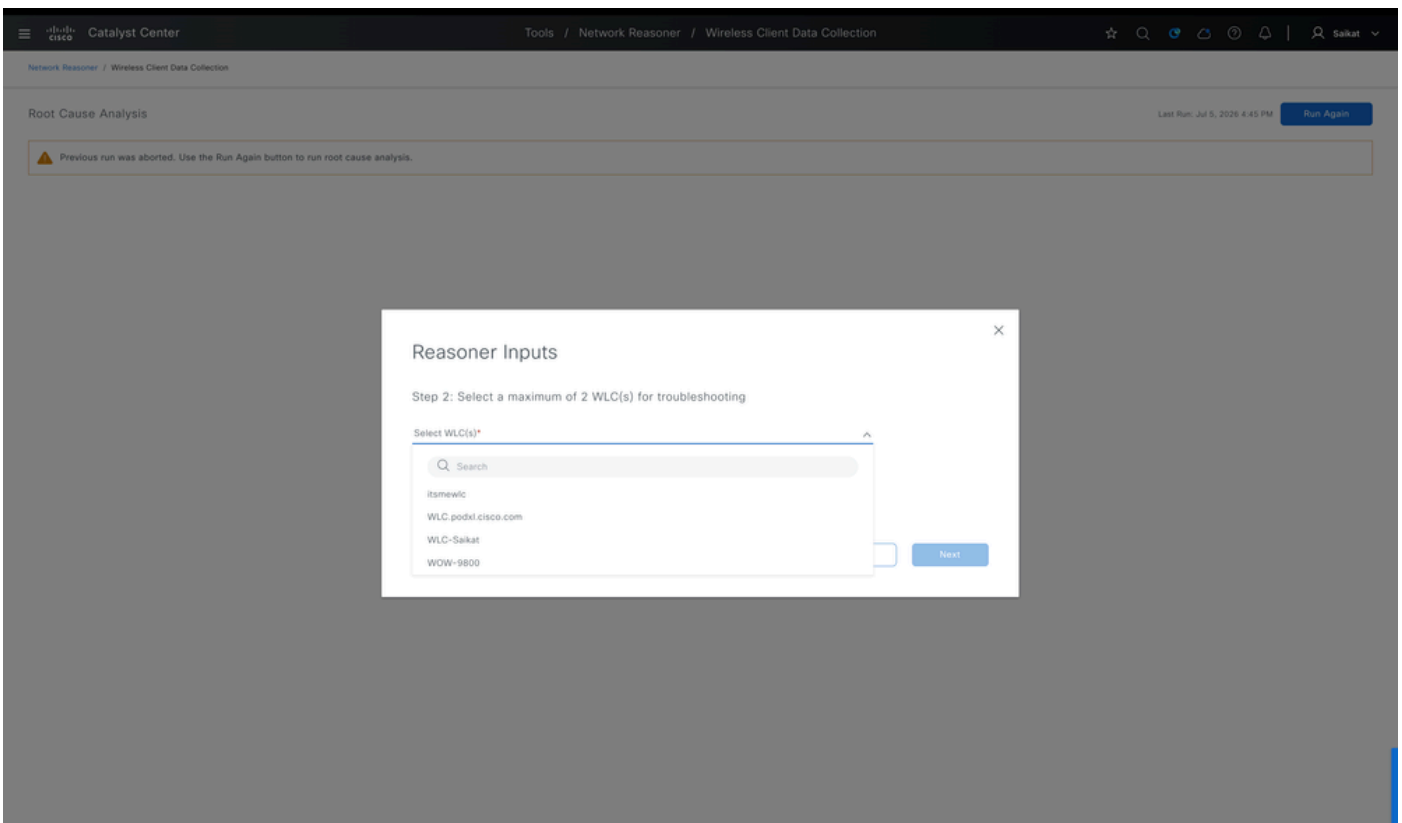
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194

Jul 5, 2026 5:10:49 PM  
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.  
Jul 5, 2026 5:10:53 PM  
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.  
Jul 5, 2026 5:10:57 PM  
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.  
Jul 5, 2026 5:11:02 PM  
Start to upload file bootflash:<file-name> from WLC with IP address 10.127.197.194 to https://10.105.19.  
Jul 5, 2026 5:11:03 PM  
Check if file bootflash:<file-name> log has been uploaded successfully from WLC with IP address 10.127.  
Jul 5, 2026 5:11:08 PM  
File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to https://10.  
Jul 5, 2026 5:11:08 PM  
Delete the file bootflash:<file-name> from WLC with IP address 10.127.197.194  
Jul 5, 2026 5:11:08 PM  
Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127.  
Jul 5, 2026 5:11:10 PM  
Stop RA Trace for AP: <MAC>  
Jul 5, 2026 5:11:13 PM  
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.  
Jul 5, 2026 5:11:15 PM  
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.  
Jul 5, 2026 5:11:19 PM  
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.  
Jul 5, 2026 5:11:22 PM  
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.  
Jul 5, 2026 5:11:27 PM  
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.  
Jul 5, 2026 5:11:30 PM  
Start to upload file bootflash:<file-name> from WLC with IP address 10.127.197.194 to https://10.105.19.  
Jul 5, 2026 5:11:32 PM  
Check if file bootflash:<file-name> has been uploaded successfully from WLC with IP address 10.127.197.  
Jul 5, 2026 5:11:37 PM  
File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to https://10.  
Jul 5, 2026 5:11:37 PM  
Delete the file bootflash:<file-name> from WLC with IP address 10.127.197.194  
Jul 5, 2026 5:11:39 PM  
Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127.  
Jul 5, 2026 5:11:41 PM  
Stopping PCAP <file-name> session with <AP-MAC> filter on TenGigabitEthernet0/0/7 interface.  
Jul 5, 2026 5:11:41 PM  
Start to upload file bootflash:<file-name> from WLC with IP address 10.127.197.194 to https://10.105.19.  
Jul 5, 2026 5:11:41 PM  
Check if file bootflash:<file-name> has been uploaded successfully from WLC with IP address 10.127.197.  
Jul 5, 2026 5:11:46 PM  
File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to https://10.  
Jul 5, 2026 5:11:53 PM  
Delete the file bootflash:<file-name> from WLC with IP address 10.127.197.194  
Jul 5, 2026 5:11:56 PM

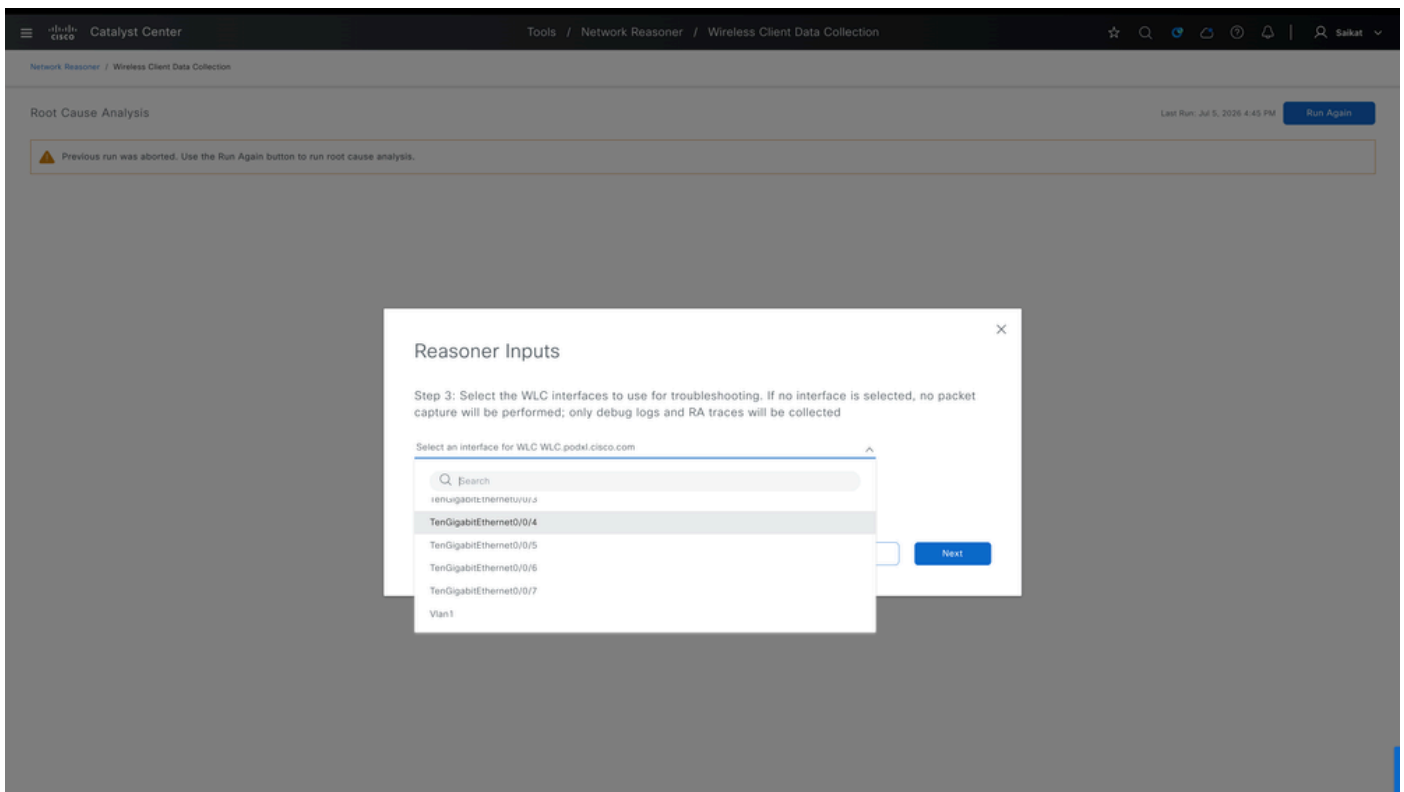
3. Wireless-Clients - Wenn ein Benutzer Wi-Fi-Probleme hat, wählen Sie den Wireless-Controller aus, mit dem er verbunden ist, geben Sie die MAC-Adresse des Geräts ein, und wählen Sie aus, wie lange das Tool überwachen soll. Es ermöglicht Statistikprotokolle, RA-Ablaufverfolgungen und Paketerfassung, 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:



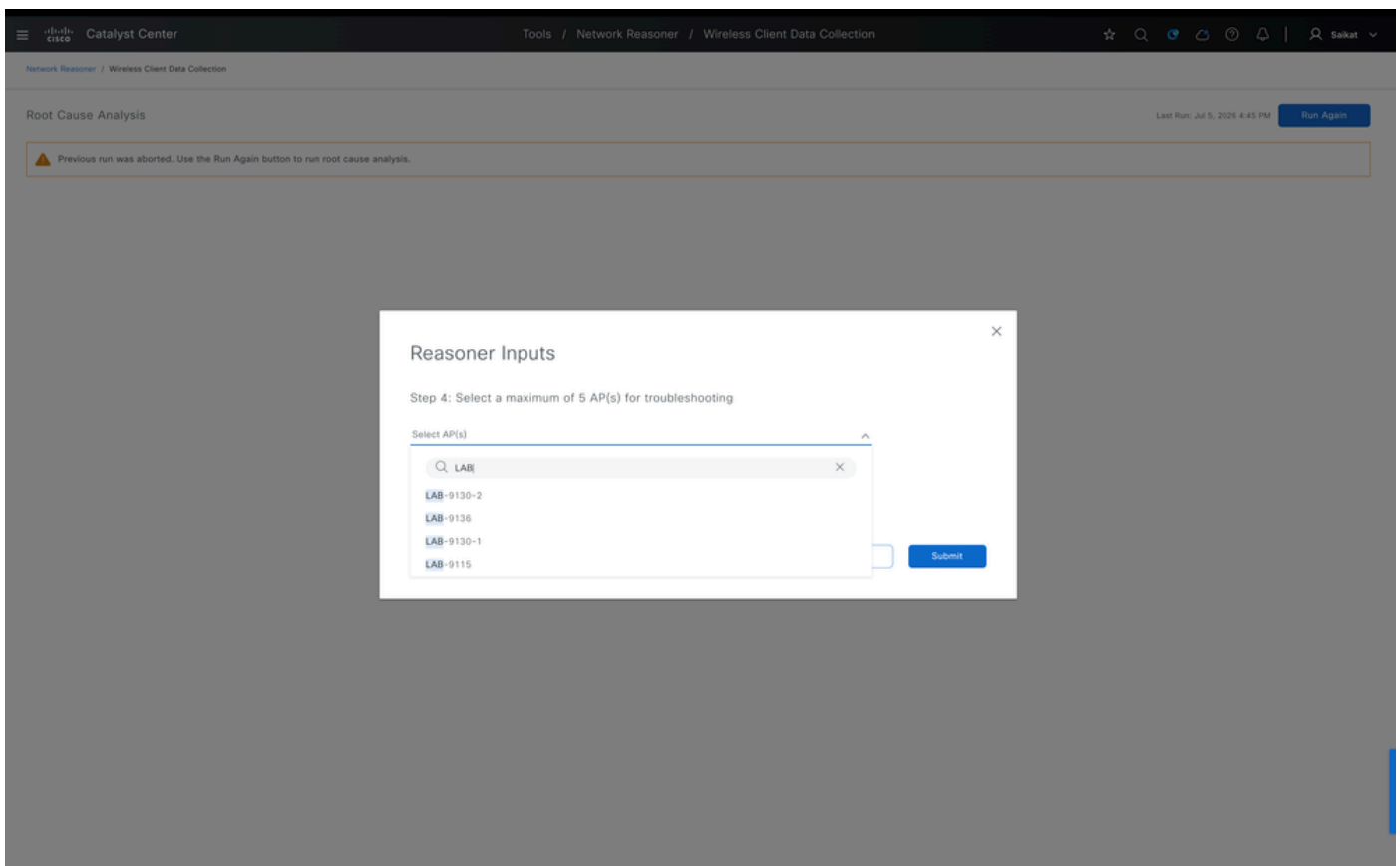
Bereitstellen von Client-Details zur Fehlerbehebung



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

The screenshot shows the 'Root Cause Analysis' section in Catalyst Center. It features a central workflow diagram with ten steps, each in a blue hexagonal box with a checkmark: 'Check device controllability', 'Evaluate device capabilities', 'Check Device Site', 'Debug wireless mac', 'Start PCAP', 'Get File Store URL', 'Start Show Client Details', 'Check AP SSH Credentials', 'Get AP Type', and 'Start Logging on AP over SSH and Wait for Data Collection...'. To the right, the 'Relevant Activity Details' panel shows a list of actions performed, including 'Debug wireless mac', 'Get Current Time', 'Starting Client PCAP session', and 'Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127.197.180-1783246554812.txt'.

### Aufgaben zur Fehlerbehebung bei Problemen mit Wireless-Clients

This screenshot shows the 'Conclusions (1)' tab in the Root Cause Analysis section. It lists several downloaded files for troubleshooting, such as 'WLC.podkl.cisco.com client-mac 783246554812.txt' and 'ap-10.127.197.151-1783246554812.log'. A 'Run Again' button is visible in the top right corner.

### 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 10.127.197.180-1783246554812.txt  
Jul 5, 2026 5:53:21 PM
  - Collect Show Client Details for 300 seconds  
Jul 5, 2026 5:53:22 PM
  - Check if AP with IP address 10.127.197.180 has SSH credentials configured in Catalyst Center

Jul 5, 2026 5:53:24 PM  
Get type of AP with IP address 10.127.197.180  
Jul 5, 2026 5:53:25 PM  
Start logging on COS AP with IP address 10.127.197.180 over SSH for Client MAC <client-mac> feature set  
Jul 5, 2026 5:53:28 PM  
End Show Client Details  
Jul 5, 2026 5:58:35 PM  
Stop data collection on COS AP with IP address 10.127.197.180 over SSH for Client MAC <client-mac> feat  
Jul 5, 2026 5:58:36 PM  
Stop data collection on COS AP with IP address 10.127.197.151 over SSH for Client MAC <client-mac> feat  
Jul 5, 2026 5:58:38 PM  
Check File Size: <file-name>  
Jul 5, 2026 5:58:38 PM  
Start to upload file <file-name> from WLC with IP address 10.127.197.194 to <https://10.105.193.40/api/v>  
Jul 5, 2026 5:58:40 PM  
Check if file <file-name> has been uploaded successfully from WLC with IP address 10.127.197.194 to [https://10.105.193.40](https://10.105.193.40/api/v)  
Jul 5, 2026 5:58:45 PM  
File <file-name> uploaded successfully from WLC with IP address 10.127.197.194 to [https://10.105.193.40](https://10.105.193.40/api/v)  
Jul 5, 2026 5:58:45 PM  
Delete the file <file-name> from WLC with IP address 10.127.197.194  
Jul 5, 2026 5:58:45 PM  
Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127.197.194  
Jul 5, 2026 5:58:47 PM  
No debug wireless mac  
Jul 5, 2026 5:58:49 PM  
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194  
Jul 5, 2026 5:58:52 PM  
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194  
Jul 5, 2026 5:58:56 PM  
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194  
Jul 5, 2026 5:58:59 PM  
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194  
Jul 5, 2026 5:59:03 PM  
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10.127.197.194  
Jul 5, 2026 5:59:07 PM  
Start to upload file bootflash:<file-name> from WLC with IP address 10.127.197.194 to [https://10.105.193.40](https://10.105.193.40/api/v)  
Jul 5, 2026 5:59:09 PM  
Check if file bootflash:<file-name> has been uploaded successfully from WLC with IP address 10.127.197.194  
Jul 5, 2026 5:59:14 PM  
File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to [https://10.105.193.40](https://10.105.193.40/api/v)  
Jul 5, 2026 5:59:14 PM  
Delete the file bootflash:<file-name> from WLC with IP address 10.127.197.194  
Jul 5, 2026 5:59:14 PM  
Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127.197.194

05.07.2026 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.