

Accelerating TAC Case Resolution with Innovative Cisco Wireless Tools and Solutions

cisco Live !

Madhuri C
Principal Engineer, [Linkedin-Madhuri](#)

Cisco Webex App

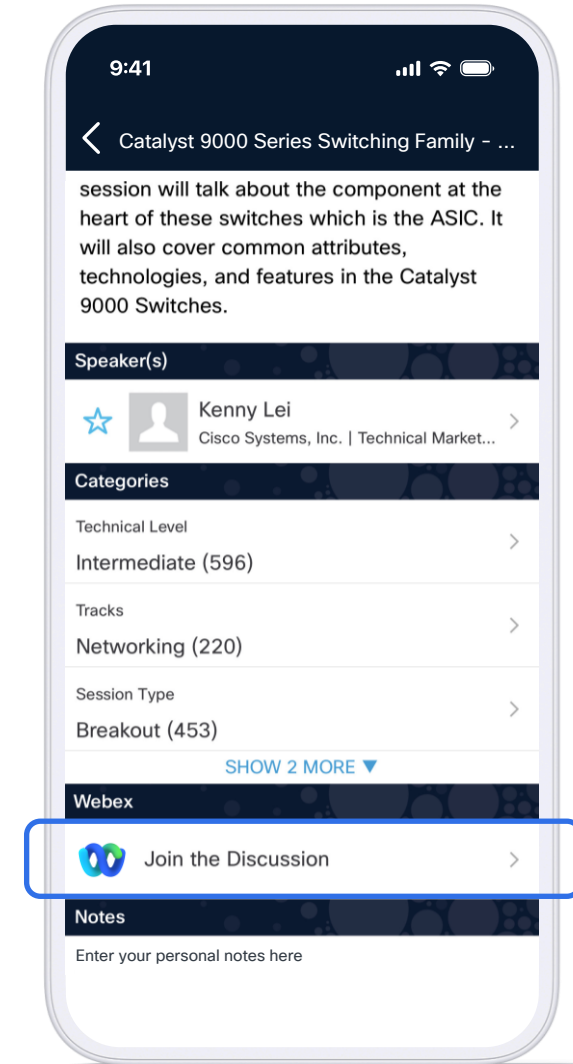
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEWN-2430>

About Madhuri



Started in 2008 & currently working as Principal Engineer



Leo & his Family



CL Melbourne



CCIE 10 Years



First Patent



Industry Recognition (Asia pacific Stevie, Pinnacle, NASSCOM Finalist & featured in NASSCOM coffee table book, Times of India)

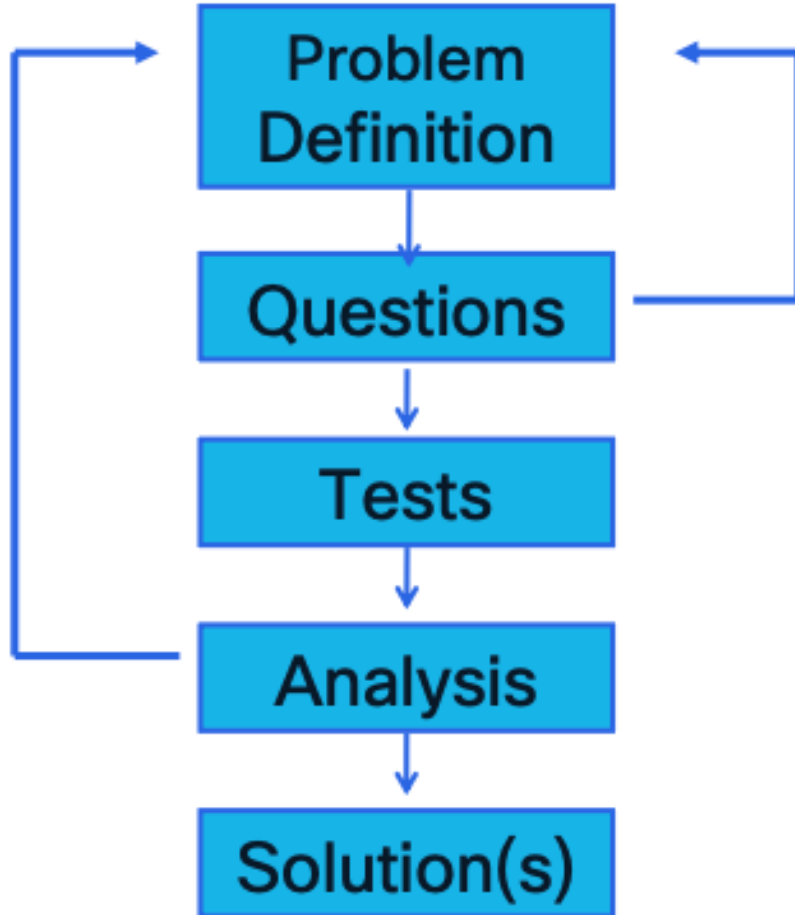


My Family

Agenda

- 01 Troubleshooting Basics
- 02 Flexible Options Overview
- 03 Proactive Engagement
- 04 In-Product Assistance
- 05 Diagnostic Tools
- 06 Dashboards
 - Catalyst Center, Meraki
- 07 Advanced Scripts
- 08 RADKit
- 09 Cisco AI Assistant

Troubleshooting Basics



Approach

- Clearly define the problem
 - Understand any possible triggers
 - Question & seek clarity
 - Know the expected behaviour
 - Reproducibility - Intermittent/Consistent ?
- Test various scenarios & combinations
- Analysis
- Arrive at the solution

Flexible Options to Self-Serve & Accelerate Case Resolution

Proactive Engagement

- Log Advisor
- Vulnerability Checker
- Talk to cisco.com

DignosticTools

- AP, WLC Debugs
- Wireless Config Analyzer Express
- Debug Analyzer
- WiFi Hawk-Over the air

Advanced Scripts

- EEMs
- Guest Shell
- WLAN Poller

Cloud Like Tool

- RADKit

Monitoring Dashboards

- Catalyst Center
- Meraki Dashboard

In-Product Assistance

- WalkMe
- Cisco Support Assistant Extension

Case Closure

Case Open

1. Prevent TAC case

2. Gather and Analyze Data

3. KPI Monitoring, Workarounds, TAC Handoff

Proactive Engagement

Flexible Options to Self-Serve & Accelerate Case Resolution

Proactive Engagement

- Log Advisor
- Vulnerability Checker
- Talk to cisco.com

Case Open



DignosticTools

- AP, WLC Debugs
- Wireless Config Analyzer Express
- Debug Analyzer
- WiFi Hawk-Over the air

Advanced Scripts

- EEMs
- Guest Shell
- WLAN Poller

Case Closure



In-Product Assistance

- WalkMe
- Cisco Support Assistant Extension

Monitoring Dashboards

- Catalyst Center
- Meraki Dashboard

Cloud Like Tool

- RADKit

1. Prevent TAC case

2. Gather and Analyze Data

3. KPI Monitoring, Workarounds, TAC Handoff

Proactive Engagement



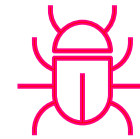
Scenario : Engage before case open or perhaps prevent a case ?

1. Log Advisor



- Gather **insights on right data** to be gathered before opening TAC Case
- Helps resolve TAC case faster

2. Check Vulnerability



- Verify if your hardware and software is impacted.
- Get additional details on **CVE**, Bug, Workarounds, Fix
- Prevent TAC case

3. Talk to Cisco.com



- Talk to virtual assistance to understand **compatibility** on hardware, software, **Field Notice Applicability**
- Prevent TAC case

1. Log Advisor - Log Collection Insights

← → ↻ mycase.cloudapps.cisco.com/create/problem

Bypass ReasonAS Entitlement

Severity ⓘ

Critical Impact (S1)

High Impact (S2)

Moderate Impact (S3)

Ask

TitleAP WLC Compatibility20/240 characters

Description

M↕BBI“↵⋮⋮⋮⋮Headings ▼Code

AP WLC Compatibility

20/32000 characters

Note: Files can be uploaded after case is created.

TechnologySuggested Technologies ⓘ

Wireless > 91xx Series Access Points (with Embedded Wireless Controller)

Wireless > 5520 Series Wireless LAN Controller (AIR-CT5520)

Wireless > Catalyst 9800 Wireless LAN Controller 40 Gbps (C9800-40)

OR

Manually Select A Technology

Problem AreaChoose Problem Area

Device Name, SW Version, Customer Reference # & PICA ID ▼

Need help with Cat 9800 Wireless LAN Controllers?

Your Cat 9800 Service Request can move a lot faster if you can help upload logs requested from the log advisor tool organized based on various wireless problem buckets.

At a minimum, please try to collect and upload the < show tech wireless > output from the C9800 WLC.

What logs to collect from Catalyst 9800 WLC for various scenarios?

Did you know? If you are using Chrome or Edge browser, you can upload your logs or open a case directly from the C9800 WebUI using the Cisco Support Assistant(CSA) Extension . This is the fastest way to engage with TAC. Learn more about the CSA Extension.

Cat 9800 Configuration Analyzer

Close

<https://logadvisor.cisco.com/>

Menu of Scenarios



Wireless and Mobility

Catalyst 9800 Controllers

 Search for an issue

 Solutions

- General Logs To Collect For Any 9800 WLC Issue
- Logs to Collect for AP Join/Connectivity Issues
- Logs to Collect for Client Connectivity Issues for 9800
- Logs for RF or RRM (Radio Resource Management) Issue
- Logs to Collect for WebAuth (LWA,CWA) Issues
- Logs to Collect for High Availability(HA) Issues
- Logs to Collect for Smart Licensing Issues
- Logs to Collect for Web User Interface or GUI Issues
- Logs to Collect for WLC Platform Issues(Crash, Performance)
- Advanced Information on AP/Client Debugs from 9800 V
- Wireless Config Analyzer Express

In SCM (Support Case Manager)

Log Collection Insights – Log Advisor

[Home](#) / [Wireless and Mobility](#) / [Catalyst 9800 Controllers](#) / **Logs to Collect for Client Connectivity Issues for 9800**

Self-service and validation

This scenario will cover client connectivity issues, association issues, authentication issues, disconnections, roaming issues.

Outputs to check key performance indicators KPIs to identify if there could be client connectivity issues:

Check for client delete reasons, identify top delete reason and see if counters are increasing

```
show wireless stats client delete reasons | ex 0
```

Additional logs to collect for client connectivity issues.

Always-On Tracing:

```
show logging profile wireless filter mac <Client_MAC> to-file always-on-<FILENAME.txt>
```

RadioActive Tracing:

```
debug wireless mac <Client_MAC>
```

Embedded Captures filtered by client MAC:

```
monitor capture MYCAP clear
```

```
monitor capture MYCAP interface Po1 both
```

```
monitor capture MYCAP buffer size 100
```

```
monitor capture MYCAP match any
```

```
monitor capture MYCAP mac <Client_MAC>
```

```
monitor capture MYCAP start
```

!!Reproduce

```
monitor capture MYCAP stop
```

```
monitor capture export flash:|tftp:|http:../filename.pcap
```

Data to be gathered for
Client connectivity issues

2. Vulnerability – Check Applicability

← → ↺ mycase.cloudapps.cisco.com/create/problem

20/240 characters

Description

M B I S “ ” ↵ ☰ ☷ ☲ ☳ ☴ ☵ ☶ ☷

CVE-2022-20683

14/32000 characters

Note: Files can be uploaded after case is created.

Technology

Suggested Technologies

☐ Wireless > 91xx Series Access Points (with Embedded Wireless Controller)

☐ Wireless > Catalyst 9800 Wireless LAN Controller for On-Premise Cloud (C9800-CL)

☐ Wireless > Catalyst 9800 Wireless LAN Controller 10 Gbps (C9800-L)

OR

☒ Wireless > Catalyst 9800 Wireless LAN Controller 40 Gbps (C9800-40)

Change

Problem Area

Installation > Interoperability

Change

Was this helpful?

🔒 Common Potential Vulnerabilities and Exposures

SCM has identified the following CVE(s)/Advisory ID(s) in the text provided. Please use the "Check Applicability on Software" to validate the impact on specific software or visit the **Security Portal** or **Cisco Vulnerability Repository (CVR)** to find all the information related to the CVE(s)/Advisory ID(s).

Check Associated Bugs

• CVE-2022-20683

Security Portal

CVR

Check Applicability on Software

Continue Case Creation

Security Portal

Vulnerability Applicability



Impacted in 17.3.2

Common Potential Vulnerabilities and Exposures

Please provide the following details to check a specific software version affected:

Software Type

IOS-XE

Software Version

17.3.2

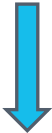
Sample Input Format: 17.3.5a, 16.10.1

3

Fill in Hardware & Software

Back to CVE/Advisory List

Check Applicability on Software



Run the Check

Common Potential Vulnerabilities and Exposures

The following CVE(s)/Advisory ID(s) affect **IOS-XE ver 17.3.2**

CVE(s)	Advisory ID(s)			
CVE-2022-20683	cisco-sa-c9800-fn...	Security Portal	CVR	CSCvx21714

Visit the **Security Portal** or **Cisco Vulnerability Repository (CVR)** to find all the information related to the CVE(s)/Advisory ID(s).

Continue Case Creation

Security Portal

Vulnerability Applicability

Common Potential Vulnerabilities and Exposures

Please provide the following details to check a specific software version affected:

Software Type

IOS-XE

Software Version

17.3.2

Sample Input Format: 17.3.5a, 16.10.1

Back to CVE/Advisory List

Check Applicability on Software

3
Fill in Hardware & Software

Run the Check



Common Potential Vulnerabilities and Exposures



The following CVE(s)/Advisory ID(s) affect **IOS-XE ver 17.3.2** ✎:

CVE(s)

Advisory ID(s)

CVE-2022-20683

cisco-sa-c9800-fn...

Security Portal

CVR

CSCvx21714

Visit the **Security Portal** or **Cisco Vulnerability Repository (CVR)** to find all the information related to the CVE(s)/Advisory ID(s).

Continue Case Creation

Security Portal



Common Potential Vulnerabilities and Exposures



No matching potential vulnerabilities found for CVE(s)/Advisory ID(s) affecting **IOS-XE ver 17.18.1** ✎:

- CVE-2022-20683 Security Portal CVR CSCvx21714

Visit the **Security Portal**, **Cisco Software Checker** or **Cisco Vulnerability Repository (CVR)** to find all the information related to the CVE(s)/Advisory ID(s).



Not Impacted in 17.18.1

3. Check Compatibility: Virtual Assistance in Cisco.com

Talk to Virtual Assistance in Cisco.com

... / Cisco Wireless LAN Controller Software / Compatibility Information /

Cisco Wireless Solutions Software Compatibility Matrix

Updated: July 22, 2025

Save

Download

Print

Bias-Free Language

Contents

Cisco Wireless Solutions Software Compatibility Matrix

Conventions

Cisco Catalyst 9800 Series Wireless Controller Matrix

Cisco Catalyst 9800 Wireless Controller Specific Software Release Support

Cisco Embedded Wireless Controller Matrix

Cisco Access Points Supported in Cisco Wireless Controller Platform Software Releases

Supported Access Points in Cisco Catalyst 9800 Series Wireless Controller Software Releases

Supported Access Points in Cisco Catalyst 9800 Embedded Wireless Controller

Supported Access Points in Cisco AireOS Wireless Software Releases

Supported Cisco Integrated Service Router 1100 Series and Embedded AP Models

Related Information

Access Point Specific Wireless Controller Software Support

Cisco AireOS Wireless Controller Specific Software Release Support

Cisco Aironet 1800s Active Sensor Compatibility Matrix

Inter Release Compatibility Matrix within Platforms

Inter Release Compatibility Matrix between IOS-XE Software Releases

Inter Release Compatibility Matrix between AireOS Releases

Cisco Spaces Compatibility Matrix

Cisco Connected Mobile Experiences Compatibility Matrix

Important Notes for Connected Mobile Experiences Platform

Cisco CMX Compatibility Matrix

Was this Document Helpful?

Yes

No

Feedback

Customers Also Viewed

Recommended Cisco IOS XE Releases for Catalyst 9800 Wireless LAN Controllers

Troubleshoot a Lightweight AP that Fails to Join a WLC

Contact Cisco

Open a Support Case

(Requires a Cisco Service Contract)

This Document Applies to These Products

2500 Series Wireless Controllers

Unleash the Power of TAC's Virtual Assistance

Login to enable assistance

8500 Series Wireless Controllers

Aironet Active Sensor

+ Show All 15 Products

Login Here for Virtual Assistance

Compatibility Check

Cisco Support Assistant
Knowledge Scope: Cisco Wireless AI Assistant

22:55:51

Select the hardware from list below OR enter your question in chat below.

Select WLC HW Model

CW9800H1

Select AP Models

CW9172I-x CW9176I-x

Chat with Cisco Support Assistant AI

22:55:56

Welcome to the Cisco Wireless AI Assistant! I can assist with your WLC and AP queries. Please type a brief question to get started!

I need a recommended release for this combination?

I need to understand whether the selected models are compatible?

I have a wireless feature question?

Select WLC,
AP models

- Select :
- 1. Recommended Release
 - 2. Compatibility
 - 3. Feature Qn

Cisco Support Assistant
Knowledge Scope: Cisco Wireless AI Assistant

For the combination of CW9800H1 controller with CW9172I-x and CW9176I-x access points, the recommended release is as follows:

The recommended release for any WLC controller platform supporting Cisco Wireless APs CW9176 or CW9172 is Cisco IOS XE 17.15.3 with APSP and SMU.

Summary Table

Controller Model	AP Models Supported	Recommended Release	Notes
CW9800H1	CW9172I-x, CW9176I-x	IOS XE 17.15.3 with APSP and SMU	Both APs supported in 17.15.3

Additional Notes

APSPs (Access Point Service Packs) and SMUs (Software Maintenance Upgrades) require a Network Advantage License. If you have a Network Essentials license, an Escalation Image can be requested from Cisco TAC, but this requires downtime. Always apply the latest APSP and SMU for your deployment.

17.15.3 is the recommended release for all deployments with CW9800 WLC appliances or with CW9176 and CW9172 Wi-Fi 7 APs.

Reference Citation

Reference: [Recommended Cisco IOS XE Releases for Catalyst 9800 Wireless LAN Controllers - Cisco](#)

References:
<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214749-tac-recommended-ios-xe-builds-for-wirele.html>

Recommendation - Emailed

Wireless compatibility result - Chat with Cisco Support Assistant AI



Saturday, 9 August 2025 at 10:58 PM

 **no-reply@cisco.com** <no-reply@cisco.com>
To: Madhuri C (madc)

Summary mail

For the combination of CW9800H1 controller with CW9172I-x and CW9176I-x access points, the recommended release is as follows:

The recommended release for any WLC controller platform supporting Cisco Wireless APs CW9176 or CW9172 is Cisco IOS XE 17.15.3 with APSP and SMU.

Summary Table

Controller Model	AP Models Supported	Recommended Release	Notes
CW9800H1	CW9172I-x, CW9176I-x	IOS XE 17.15.3 with APSP and SMU	Both APs supported in 17.15.3

Additional Notes

- APSPs (Access Point Service Packs) and SMUs (Software Maintenance Upgrades) require a Network Advantage License. If you have a Network Essentials license, an Escalation Image can be requested from Cisco TAC, but this requires downtime.
- Always apply the latest APSP and SMU for your deployment.
- 17.15.3 is the recommended release for all deployments with CW9800 WLC appliances or with CW9176 and CW9172 Wi-Fi 7 APs.

Reference Citation

Reference: [Recommended Cisco IOS XE Releases for Catalyst 9800 Wireless LAN Controllers - Cisco](#)

References:

1. <https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214749-tac-recommended-ios-xe-builds-for-wirele.html>
2. <https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-12/release-notes/rn-17-12-9800.html>
3. <https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-13/release-notes/rn-17-13-9800.html>
4. <https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-9/release-notes/rn-17-9-9800.html>

Source links:

1. <https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214749-tac-recommended-ios-xe-builds-for-wirele.html>
2. <https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-12/release-notes/rn-17-12-9800.html>
3. <https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-13/release-notes/rn-17-13-9800.html>
4. <https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-9/release-notes/rn-17-9-9800.html>

Summary Table &
Reference Citation

Field Notice - SN Validation:

Field Notice: FN74160 - A Limited Subset of Memory Modules in Cisco Catalyst 9800-L Wireless Controllers May Fail Prematurely - Hardware Upgrade Available

Products Affected

Problem Description

Problem Symptom

Workaround/Solution

Save

Translations

Print

Updated: September 13, 2024

Document ID: FN74160

Bias-Free Language

High

Impact Rating: High

First Published: 2024-Sep-13

Last Published: 2024-Sep-13

Revision: 1.0

Cisco Bug IDs: CSCwb84008

Notice

THIS FIELD NOTICE IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTY OF MERCHANTABILITY. YOUR USE OF THE INFORMATION ON THE FIELD NOTICE OR MATERIALS LINKED FROM THE FIELD NOTICE IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS FIELD NOTICE AT ANY TIME.

Products Affected

Affected Product Name	Description	Comments
C9800-L-C-CA-K9	Cisco Catalyst 9800-L-C Wireless Controller	

Was this Document Helpful?

Yes No

Feedback

Customers Also Viewed

Field Notice: FN74222 - Full or Partial Cisco 9800 Series Wireless Controller Configuration Loss after High-Availability Stateful Switchover Failover - Software Upgrade Recommended

Recommended Cisco IOS XE Releases for Catalyst 9800 Wireless LAN Controllers

Configure High Availability SSO on Catalyst 9800 | Quick Start Guide

Hello! I can help you validate if you're impacted by this Field Notice

Hello! I can help you validate if you're impacted by this Field Notice

Cisco AI Assistant for Support

Knowledge Scope: Field Notices

Hi there! I'm Cisco AI Assistant for Support

00:58:42

I can help validate if your device Serial Number is impacted by a Field Notice.

00:58:43

Enter SN(s) of your device to check if they're impacted by any Field Notices

You can provide max 100 SN values - comma separated

Serial Number(s)

SCXXXXIN

Upload file

Validate SN

00:58:45

Enter Serial Number

Field Notice: SN Validation (continued)

Field Notice: FN74160 – A Limited Subset of Memory Modules in Cisco Catalyst 9800-L Wireless Controllers May Fail Prematurely – Hardware Upgrade Available

Products Affected

Updated: September 1

High

Notice

THIS FIELD NOTICE IS YOUR USE OF THE INF OR UPDATE THIS FIEL

Products Affected

Affected Product Name

C9800-L-C-CA-K9

C9800-L-C-K9

C9800-L-C-K9-RF

C9800-L-F-CA-K9

Cisco Support Assistant

Knowledge Scope: Field Notices

3

Provide SNs

Upload file

Validate SN

01:16:12

Please wait while we process your data. This will only take a few seconds.

01:16:19

We have processed 3 serial numbers, out of which 1 is impacted and 2 are not.

FN ID	Title	Family	Impacted Serial(s) Numbers
74160 (Create the RMA here)	FN74160 - A Limited Subset of Memory Modules in Cisco Catalyst 9800-L Wireless Controllers May Fail Prematurely - Hardware Upgrade Available	E9800L	FCL24520054

Following Serial Number(s) are not impacted by any field notice: FCL250800KM, FCL250800ES

2 SNs : Not Impacted

Proactive Engagement : Summary



1. Use Log Advisor



- Leverage **Log Collection Modules (Log Advisor)** to gather **insights on logs** needed in SCM during case open.
- Helps **resolve** TAC case **faster**

2. Vulnerability Check



- Know if your hardware and software is **impacted by CVE**, Workarounds, Fix.
- **Prevent TAC case**

3. Talk to Cisco.com



- Talk to virtual assistance to get **compatibility** of hardware, software, **recommended code**, Field Notice(FN) **Applicability**
- **Prevent TAC case**

Option A : In-Product Insights

Flexible Options to Self-Serve & Accelerate Case Resolution

Proactive Engagement

- Log Advisor
- Vulnerability Checker
- Talk to cisco.com



Case Open



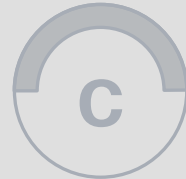
In-Product Insights

- WalkMe
- Cisco Support Assistant Extension



DignosticTools

- AP, WLC Debugs
- Wireless Config Analyzer Express
- Debug Analyzer
- WiFi Hawk-Over the air



Monitoring Dashboards

- Catalyst Center
- Meraki Dashboard



Advanced Scripts

- EEMs
- Guest Shell
- WLAN Poller



Cloud Like Tool

- RADKit

Case Closure



1. Prevent TAC case

2. Gather and Analyze Data

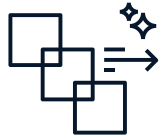
3. KPI Monitoring, Workarounds, TAC Handoff

In-Product Insights



Scenario : How to get insights in product and upload data from box directly ?

1. WalkMe (Guided Assistance)



- Provide insights or resources in product at **right time** and only **if impacted**
- Helps **prevent issues** and guide or walk you through config

2. Cisco Support Assistant Extension



- CSAE helps **record screen, upload data, open TAC case etc** directly.
- 17.18.2- Natively supported and **integrated in product.**

In-Product Insights

Proactive, Predictive and Preemptive



Detect

- Find relevant catastrophic defects, applicable insights



Assess

- Assess via automated, interactive multi-conditional check



Notify

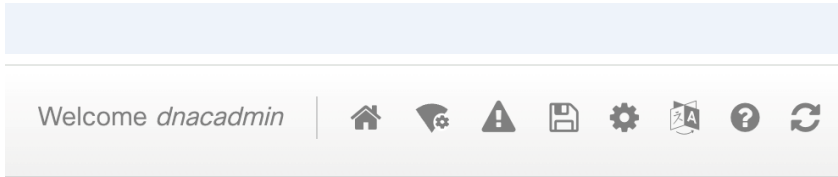
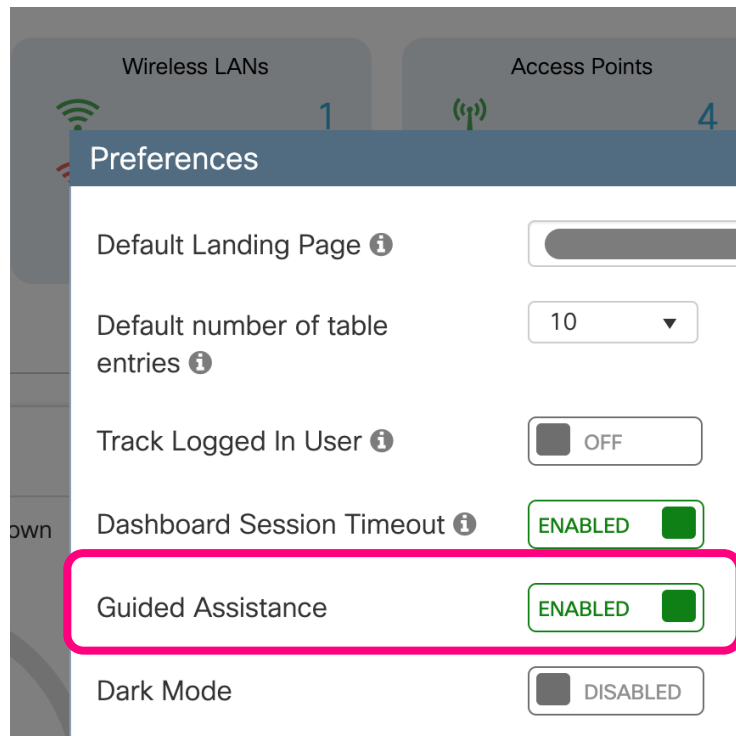
- Real-time notification within product for user to take action



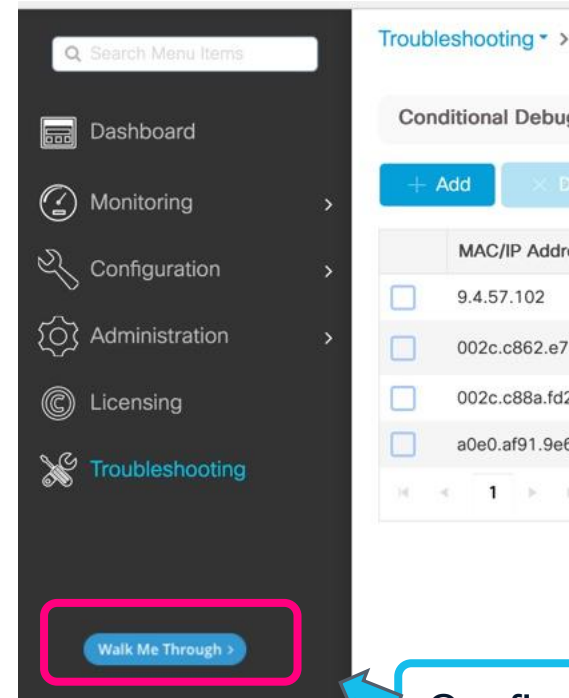
Outcome

- Prevent Outages, Save time, Deflect Cases, Self-Serve

WalkMe or Guided Assistance



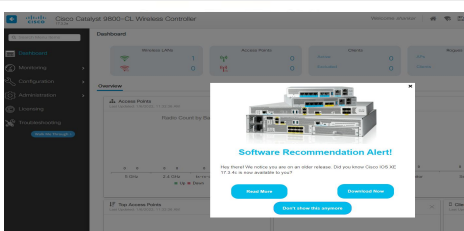
On by default



Config Walkthroughs

WalkMe In-Product Insights

Steering to Latest Software



Software Recommendation Alert!

Hey there! We notice you are on an older release. Did you know Cisco IOS XE 17.3.5a + SMU is now available to you?

[Read More](#) [Download Now](#)

[Don't show this anymore](#)

Alerting on Catastrophic Defects

Detected AP name >=32 characters. Please be aware of (

wpa-agent11234567891234567890124	AIR-AP2802I-2
	D-K9

Configuration Tips

ENABLED 

RMI IP must be in the same subnet as Wireless Management Interface (WMI). For more information, see [here](#).

10.201.234.155 

Shoutouts

 Need help on what logs to collect for various scenarios?

 Onboarding newer 9105/9120/9130 APs? [Click here.](#)

Relevant Warning !!

TCP MSS Configuration

Adjust MSS Enable 

Adjust MSS* 1250

Warning! Potential for client throughput issues owing to [CSCwd37092](#) . Please upgrade [APSP patch](#) or refer [workaround](#) to prevent this issue.

Self Serve Tools

 Licensing

 Troubleshooting

[Walk Me Through >](#)

Wireless Debug Analyzer

Last Run Result

Field Notice

 Cisco is aware of an issue affecting image validation at software upgrades or downgrades in the Cisco 1702, 2702, 3702, 1572, IW3702 Wave 1/IOS Access Points. We recommend following the workarounds mentioned in the bug [CSCwd80290](#).

Intelligent Software Steering

Match Hardware + Software

Cisco Catalyst 9800-CL Wireless Controller
17.3.2a

Welcome shankar

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Walk Me Through

Dashboard

Wireless LANs

Access Points

Clients

Rogues

Overview

Access Points

Radio Count by Ba

Top Access Points

Hey there! We notice you are on an older release. Did you know Cisco IOS XE is now available to you?

Read More

Download Now

Don't show this anymore

Thousands of customers downloaded recommended software

Multipage Conditional Check of a Catastrophic Defect

←

Cisco Catalyst 9800-CL Wireless Controller

17.5.20210126

Welcome cisco

🏠

📶

💾

⚙️

🔧

❓

🔄

Search APs and Clients 🔍

🔍 Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Configuration > Tags & Profiles > WLANs

+ Add

✖ Delete

Enable WLAN

Disable WLAN

Number of WLANs selected : 0

☐	Status	Name	ID	SSID	Security
☐	🟢	docwlan	1	docwlan	[WPA2][AES] [Enabled]
☐	🟢	test	2	test	[WPA2][AES]
☐	🔴	test2sd	3	test	[WPA2][AES]
☐	🟢	sdfds	4	sdfds	[WPA2][AES]
☐	🟢	dsds	5	dsds	[WPA2][AES]

10

Items per page

1

👤

Click on warning icon to trigger validation

⚠️

←

Cisco Catalyst 9800-CL Wireless Controller

17.5.20210126

🔍 Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Accounting

+ Add

✖ Delete

☐	Name	Type
☐	test	exec

10

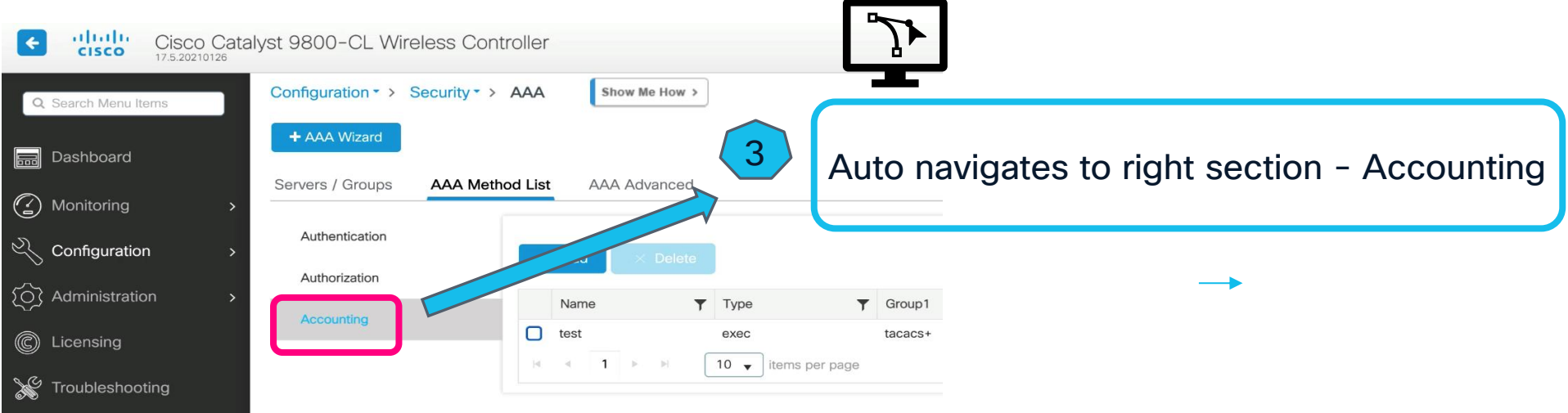
items per p

2

🖥️

Auto navigation to AAA in Security Page

Multipage Conditional Check of a Catastrophic Defect (Contd)



Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

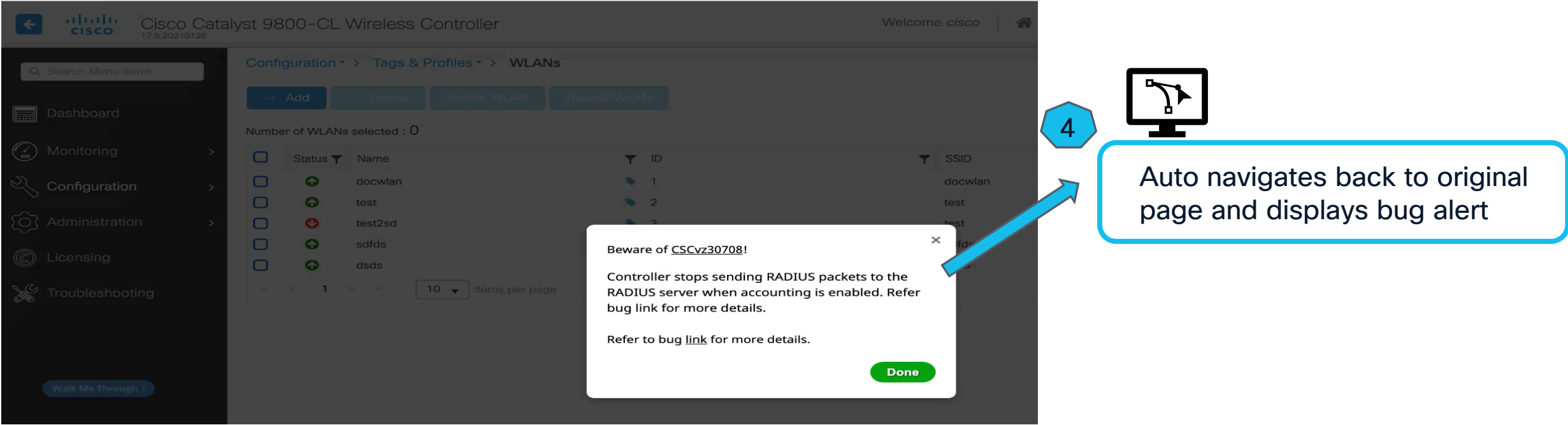
Authentication

Authorization

Accounting

Auto navigates to right section - Accounting

Name	Type	Group1
test	exec	tacacs+



Configuration > Tags & Profiles > WLANs

+ Add Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

Status	Name	ID	SSID
✓	docwlan	1	docwlan
✓	test	2	test
✗	test2sd	3	test
✓	sdfds		
✓	dsds		

Beware of [CSCvz30708](#)!

Controller stops sending RADIUS packets to the RADIUS server when accounting is enabled. Refer bug link for more details.

Refer to bug [link](#) for more details.

Done

Auto navigates back to original page and displays bug alert

Alerting a Defect – Prevent Outage

←

Cisco

Cisco Catalyst 9800-40 Wireless Controller
17.3.3

Welcome admin

🏠

📶

💾

⚙️

📄

❓

🔄

Search APs and Clients 🔍

🔍 Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Configuration > Wireless > Access Points

▼ All Access Points

Number of AP(s): 1

AP

Admin

IP

Base Radio

AP

Operation

Configuration

Policy

AddressMACModeStatusStatusTag

Detected AP name >=32 characters. Please be aware of CSCvy11981

wpa-agent11234567891234567890124

AIR-AP2802I-D-K9

2

✓

10.106.37.168

b811.4b5f.84a0

Local

Registered

Healthy

default-policy-tag

1 - 1 of 1 access points

5 GHz Radios

2.4 GHz Radios

Dual-Band Radios

Country

LSC Provision

Matching a defect where AP name >32 characters would crash WLC in 17.3.3

Detected AP name >=32 characters. Please be aware of CSCvy11981

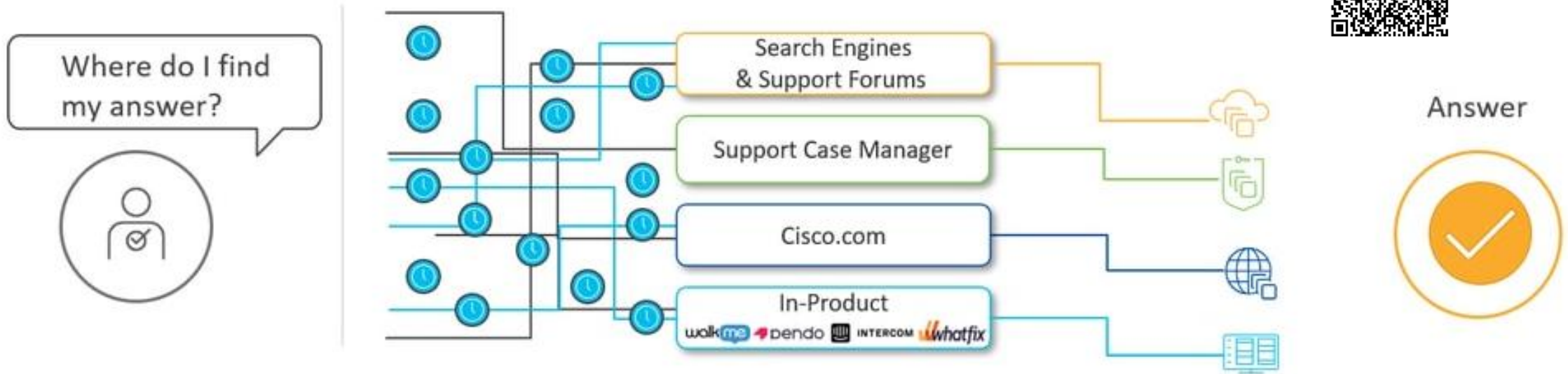
wpa-agent11234567891234567890124

AIR-AP2802I-D-K9

2

✓

2. Cisco Support Assistant Extension (CSAE) :



CSAE Availability

1. Browser Extension

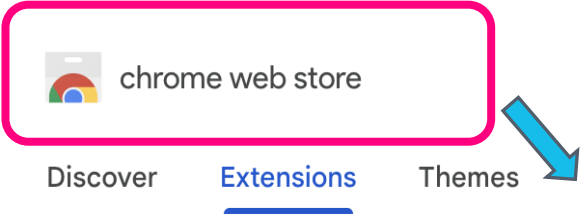
- Prior to 17.18.2
- Supported on Chrome, Microsoft Edge

2. Native Product Integration

- 17.18.2- Natively supported and integrated in 9800 WLC.

Install CSAE

Download from chrome web store



Cisco In Product Support

5.0 ★ (33 ratings) [Share](#)

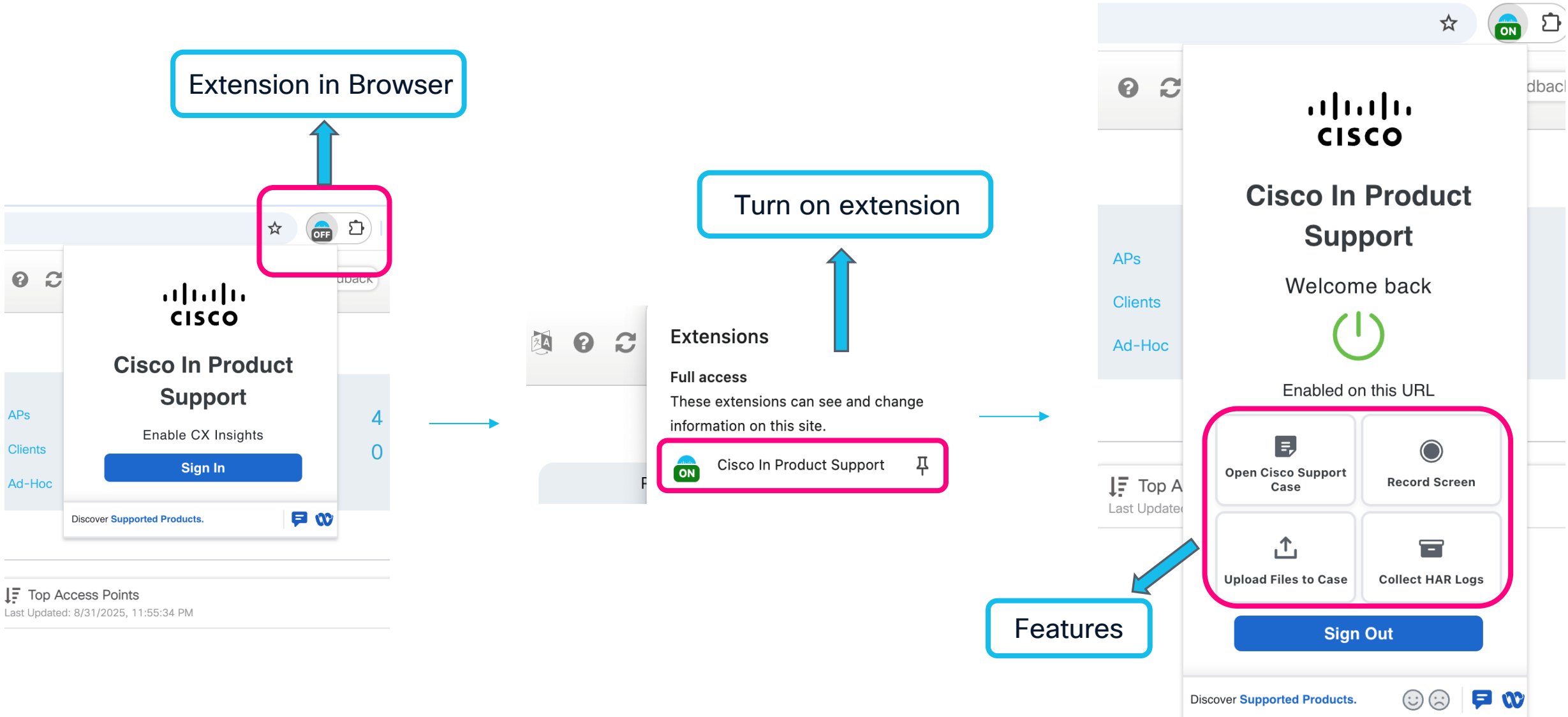
Extension

Workflow & Planning

3,000 users

More info : [CSAE](#)

CSAE – Install & Enable



CSAE View

← → ↺

Not Secure https://[redacted]webui/#/dashboard

☆

ON

←

CISCO

Cisco Catalyst 9800-40 Wireless Controller

17.15.3

Welcome admin

🏠

📶

⚠️

💾

⚙️

📄

❓

↺

🔍 Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Walk Me Through

Dashboard

Network

6 GHz 3

5 GHz 3

2.4 GHz 3

Wireless LANs

3

3

Access Points

2

0

0

Not Joined

0

Clients

0

0

0

Active

Excluded

Sleeping

APs

0

0

0

Clients

Ad-Hoc

Overview

Radios

Last Updated: 11/2/2025, 3:49:41 PM

Up

Down

Client Serving

Monitoring

Sniffer

Radio Role Show

2

6 GHz

2

2

2

5 GHz

2

2

2

2.4 GHz

1

1

1

1

Top A

Last Update

Sort by: A

AP N

✓

👤

On

Through

136 bps

CISCO

Cisco In Product Support

Welcome back Madhuri C

🔌

Enabled on this URL

Open Cisco Support Case

Record Screen

Upload Files to Case

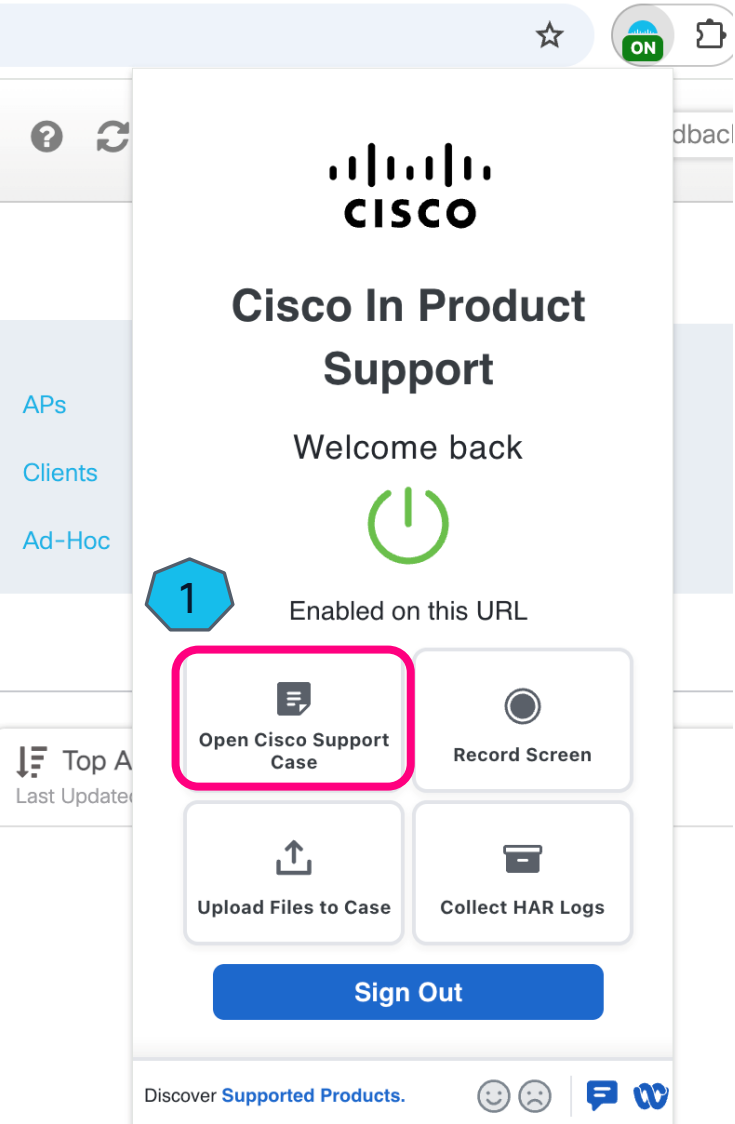
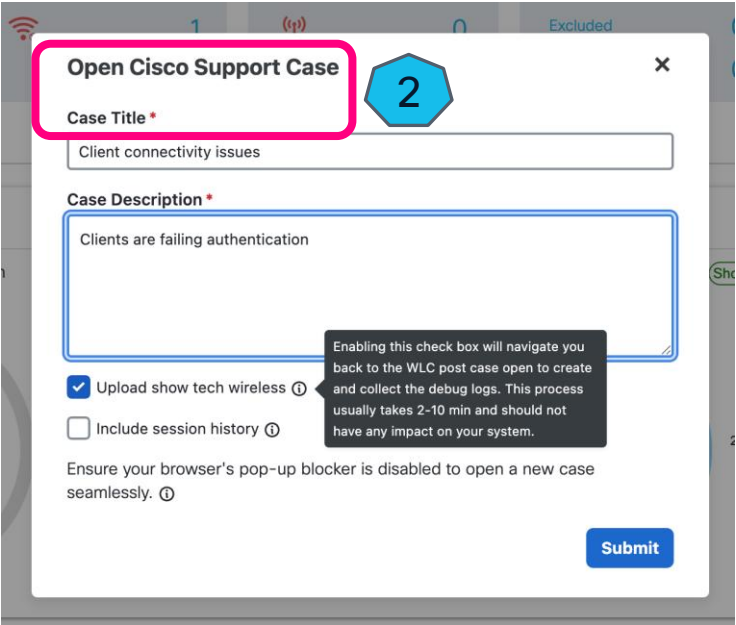
Collect HAR Logs

Sign Out

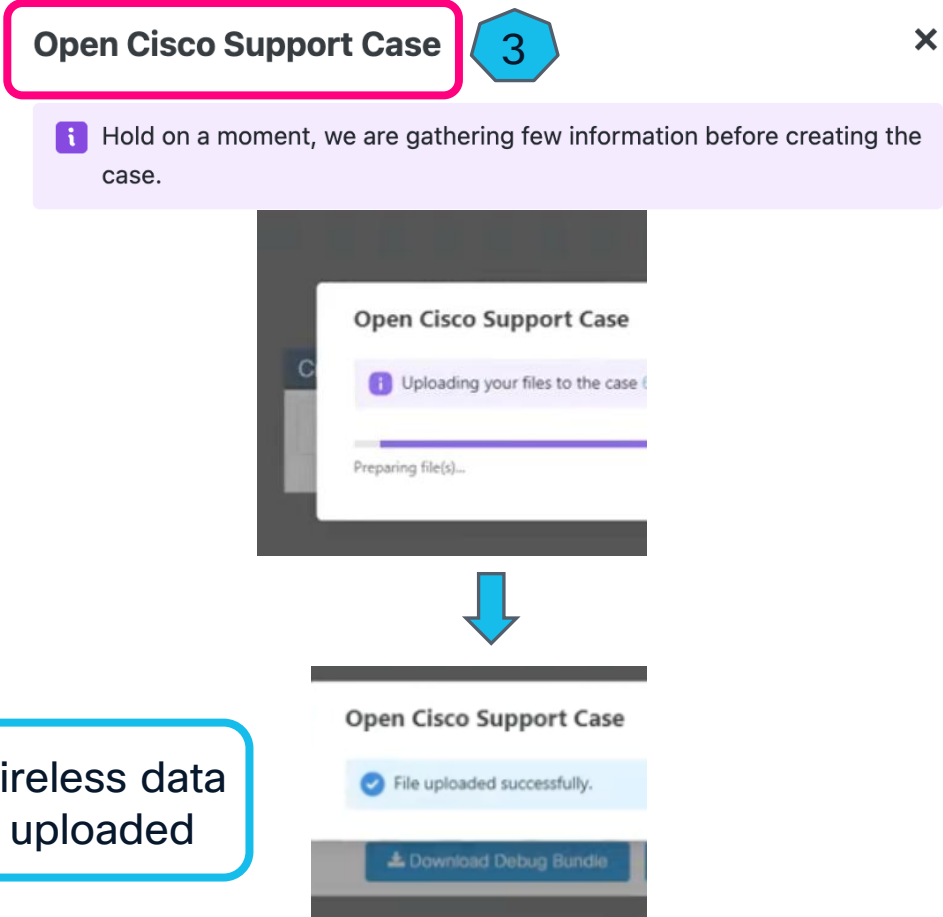
Discover Supported Products.

😊 😞 💬

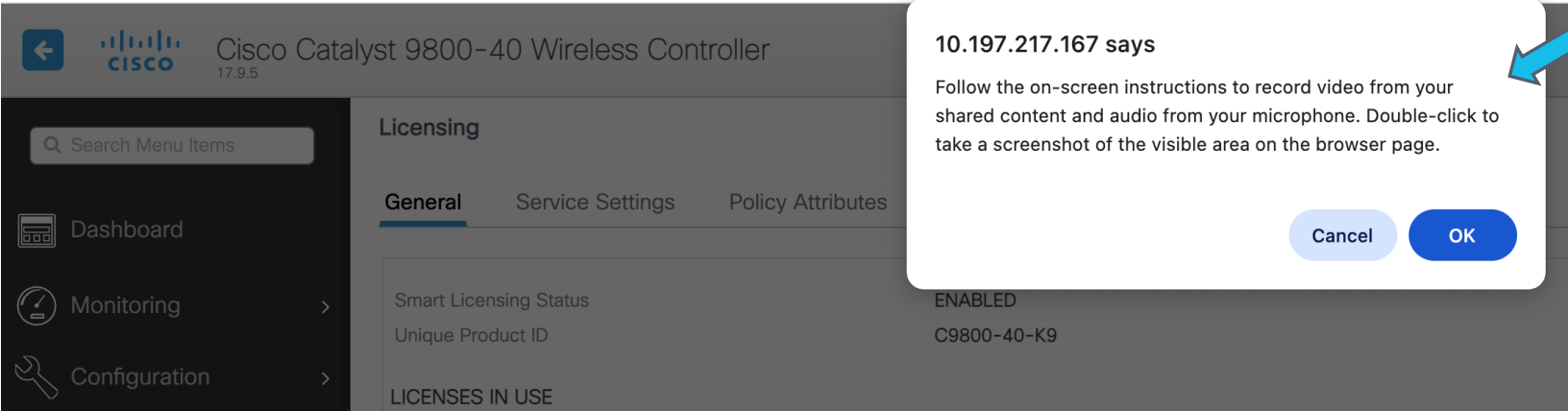
CSAE – Open TAC SR from WLC



Show tech wireless data collected & uploaded



CSAE – Upload Recording (Screen & Audio)



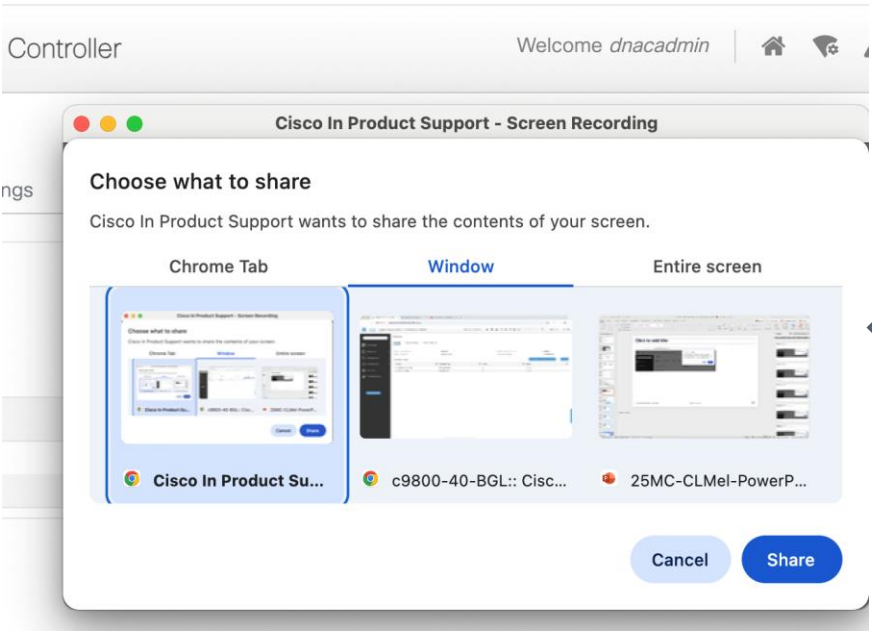
10.197.217.167 says

Follow the on-screen instructions to record video from your shared content and audio from your microphone. Double-click to take a screenshot of the visible area on the browser page.

Cancel OK

Pop up on selecting record option

1



Controller

Welcome dnacadmin

Cisco In Product Support - Screen Recording

Choose what to share

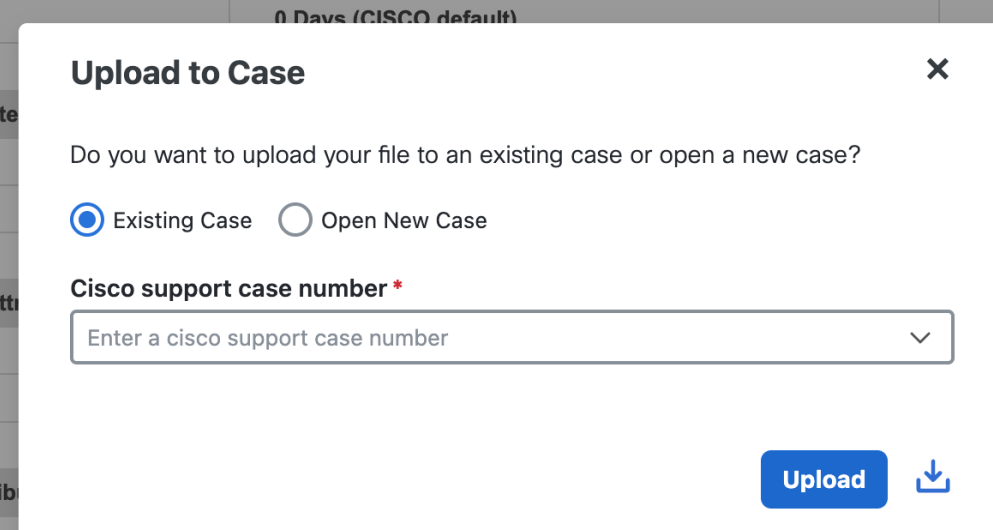
Cisco In Product Support wants to share the contents of your screen.

Chrome Tab Window Entire screen

Cancel Share

2

- Select Screen
- Allow audio
- Upload to SR



0 Days (CISCO default)

Upload to Case

Do you want to upload your file to an existing case or open a new case?

☒ Existing Case ☐ Open New Case

Cisco support case number *

Enter a cisco support case number

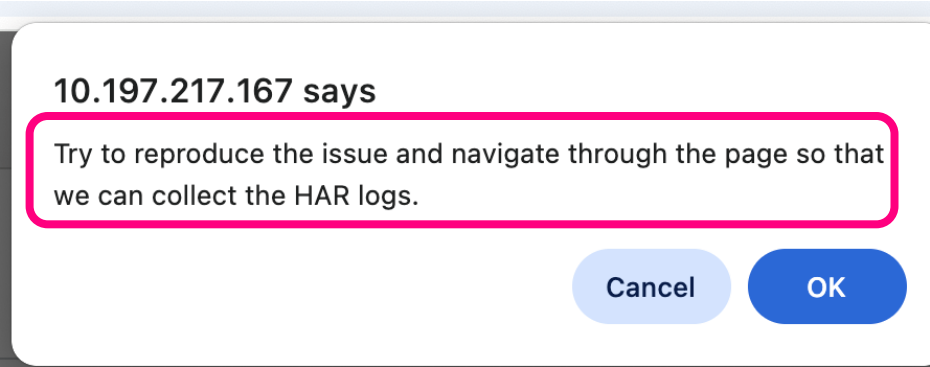
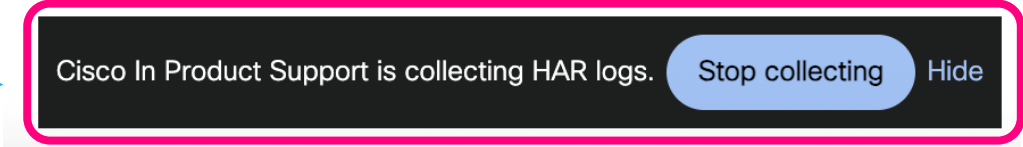
Upload

CSAE – Collect HAR Logs, Upload Debug Files

1

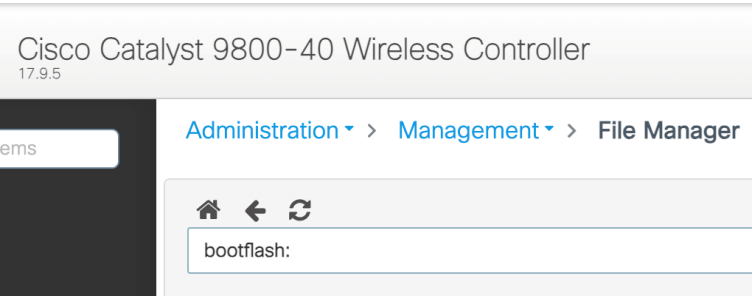
Collect Har Logs for GUI Issues

Pop up on selecting record option

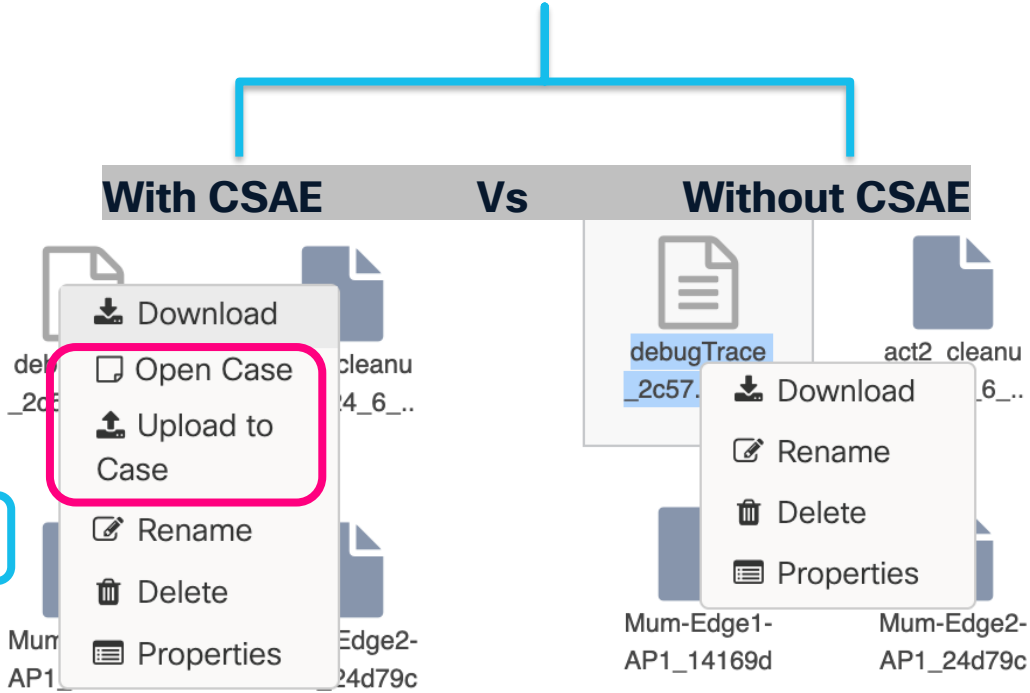


2

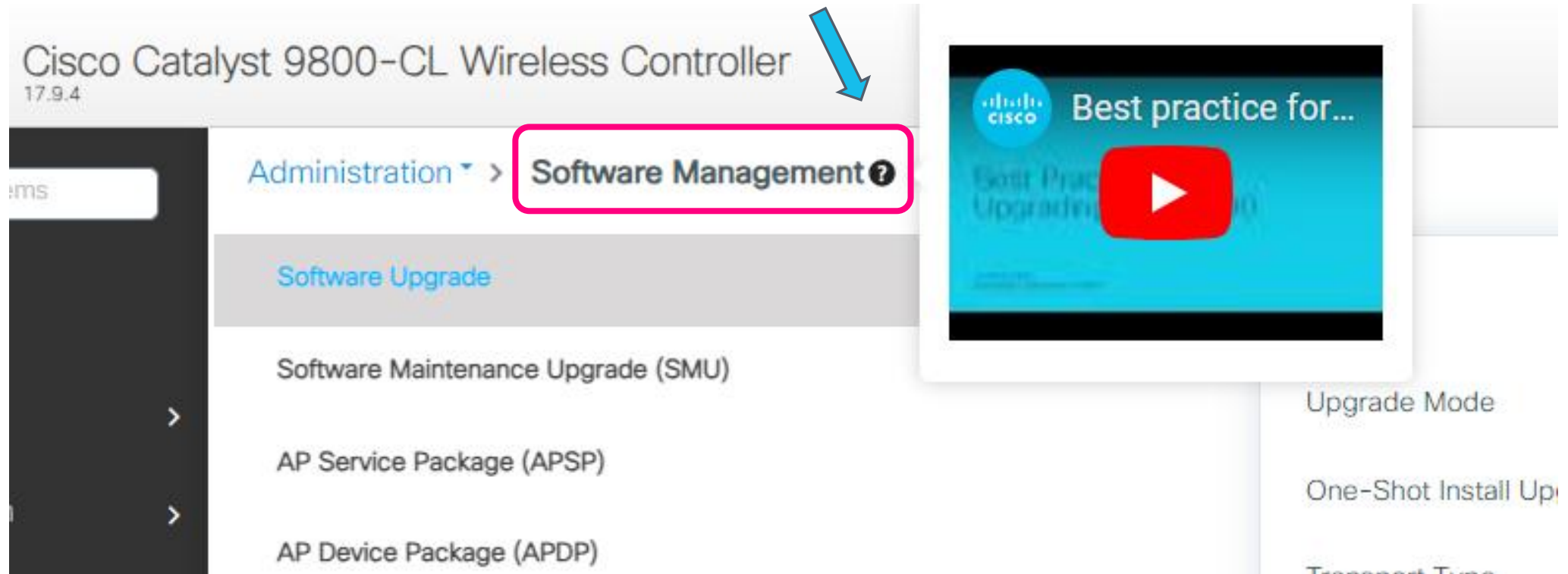
Uploading Debug File



2 New Options

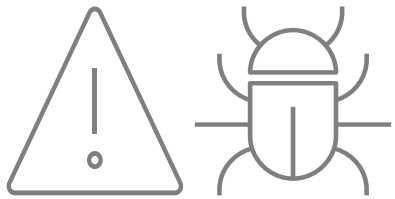


Play video in product

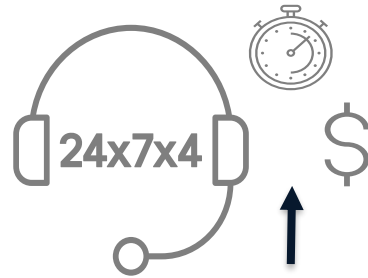


The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The title bar at the top reads "Cisco Catalyst 9800-CL Wireless Controller" with the version "17.9.4" below it. A blue arrow points to the "Software Management ?" link in the top navigation bar, which is highlighted with a pink rectangle. Below this, the "Software Upgrade" section is visible, containing links for "Software Maintenance Upgrade (SMU)", "AP Service Package (APSP)", and "AP Device Package (APDP)". A video overlay is positioned on the right side of the screen, featuring the Cisco logo and the text "Best practice for..." above a large red play button icon. The video title "Best Practice Upgrade" is partially visible. To the right of the video, a list of upgrade modes is shown: "Upgrade Mode", "One-Shot Install Up", and "Tentative Time".

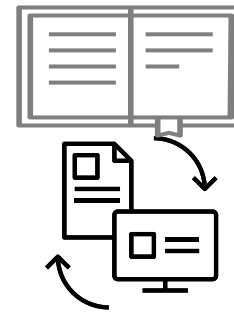
In-Product Insights Benefits



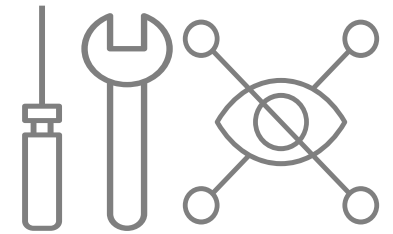
**Prevent Network
Outages due to
Known Issues**



**Prevent time
consuming TAC
Cases**



**Better consumption of
Documentation**



**Better tools
Adoption**

Option B : Diagnostic Tools

Flexible Options to Self-Serve & Accelerate Case Resolution

Proactive Engagement

- Log Advisor
- Vulnerability Checker
- Talk to cisco.com



DignosticTools

- AP, WLC Debugs
- Wireless Config Analyzer Express
- Debug Analyzer
- WiFi Hawk-Over the air

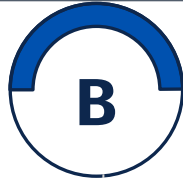
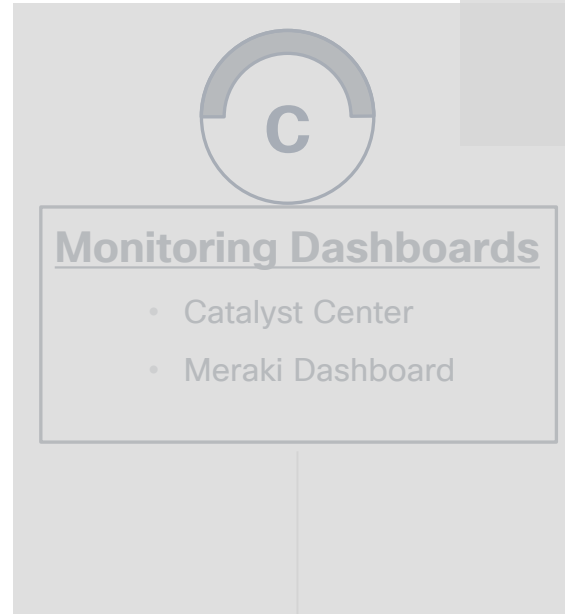
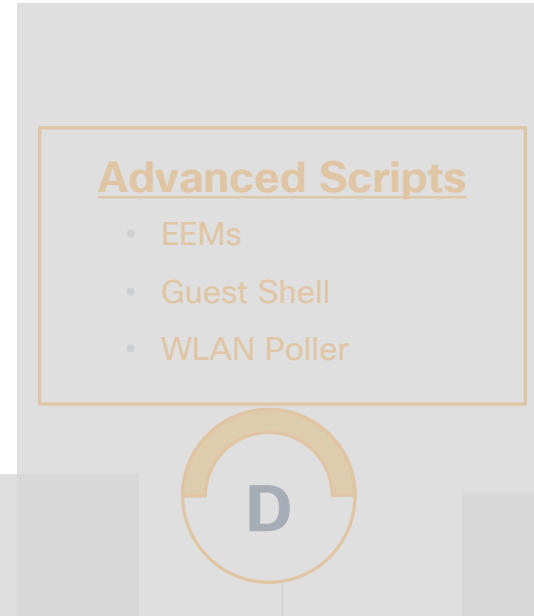
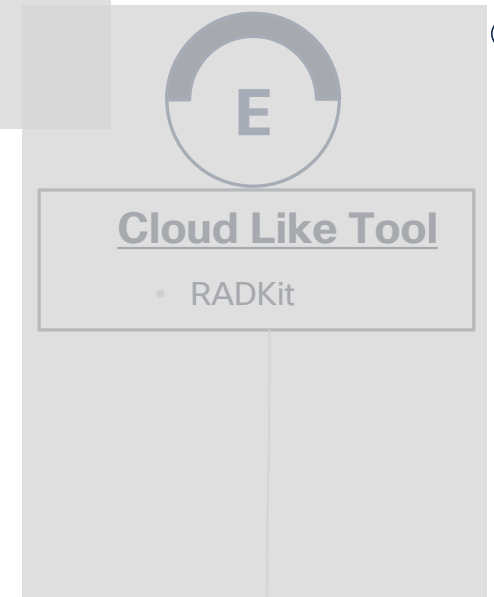


Case Open



In-Product Assistance

- WalkMe
- Cisco Support Assistant Extension



Case Closure



1. Prevent TAC case

2. Gather and Analyze Data

3. KPI Monitoring, Workarounds, TAC Handoff

Diagnostic Tools



Scenario : Troubleshooting AP Join, Best Practices, Client Connectivity, PCAPs

AP/WLC Debugs

- Correlating AP and WLC side of debugs
- Example : AP join issues

WCAE

- Gain insights on best practices, warnings, RF, performance issues
- Example : Checking WLC Performance and High WNCd CPU Issues

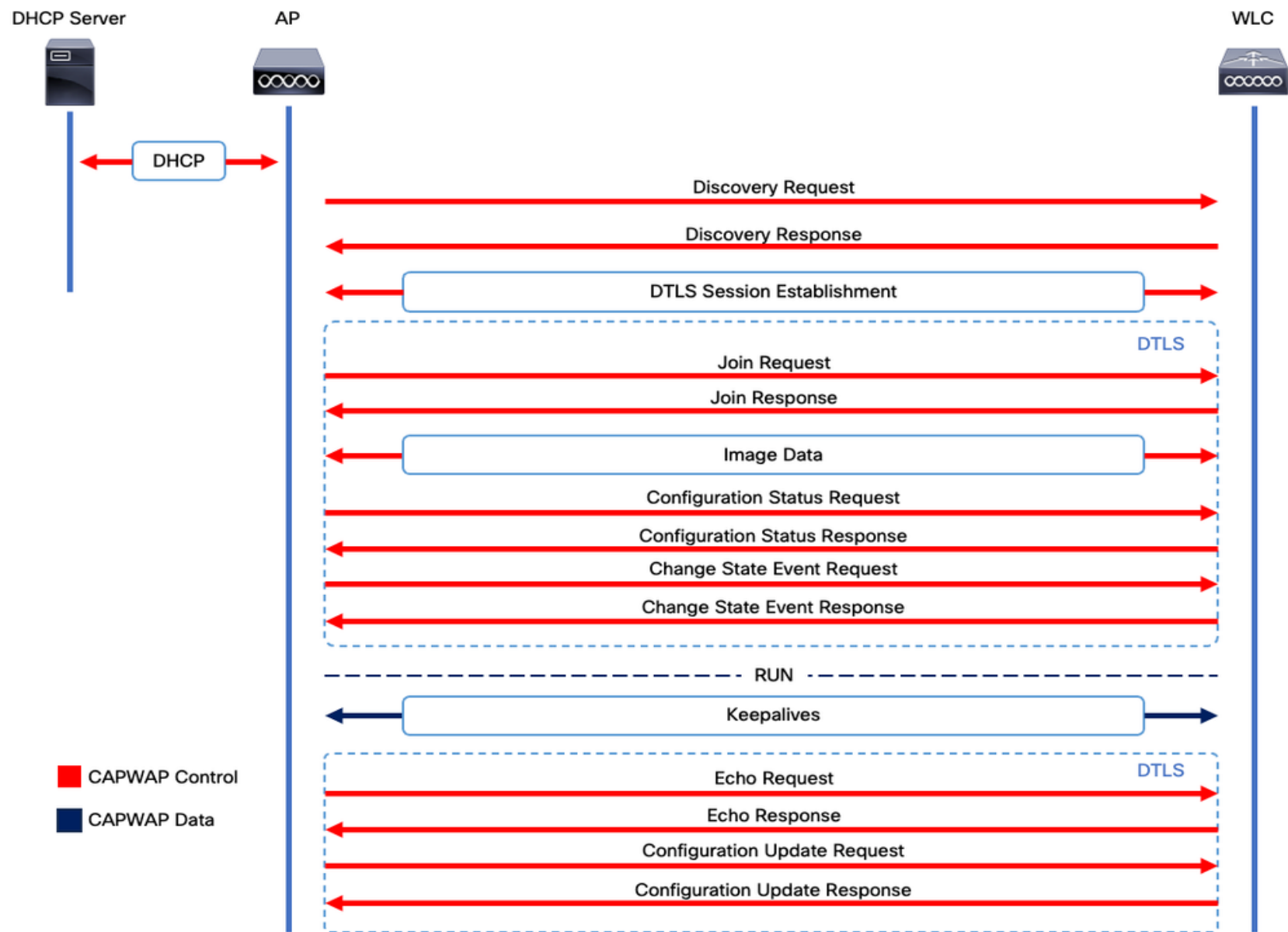
Debug Analyzer

- Analyze client RA traces in table, graphical format for quick and easy consumption with various statistics
- Example : Client connectivity

WiFi-Hawk (OTA)

- Get insights on over the air packet capture, outputs from AP
- Example : Debugging an RF Issue

Quick Look : AP Join Flow



Correlating AP Debugs & WLC Traces

- **AP side debugs** : In AP CLI : “**debug capwap client events**” and “**debug capwap client error**”
- **WLC side** : In WLC : **RA trace** for AP mac address from WLC : **Troubleshooting > RA trace**

1. Discovery Phase

AP Debugs :

Sep 7 12:57:46 kernel: [*09/07/2025 12:57:46.1638] CAPWAP State: Discovery

Sep 7 12:57:46 kernel: [*09/07/2025 12:57:46.1666] **Discovery Request sent to 10.127.84.20**, discovery type STATIC_CONFIG(1)

Sep 7 12:57:46 kernel: [*09/07/2025 12:57:46.1877] **Discovery Response from 10.127.84.20**

Sep 7 12:57:46 kernel: [*09/07/2025 12:57:46.1879] Found Configured MWAR 'c9800-40-BGL' (respIdx 0).

WLC RA Trace :

2025/09/07 12:57:47.156982498 {wncmard_R0-0}{1}: [capwapac-discovery] [14867]: (note): MAC: 1416.9d2a.bf80
IP:10.127.85.77[5256], Discovery Request received

2025/09/07 12:57:47.157593433 {wncmgrd_R0-0}{1}: [capwapac-discovery] [14867]: (note): MAC: 1416.9d2a.bf80
IP:10.127.85.77[5256], Discovery Response sent

Correlating AP Debugs & WLC Traces

2. DTLS Phase

AP Debugs :

Sep 7 12:57:47 kernel: [*09/07/2025 12:57:47.0099] CAPWAP State: DTLS Setup

Sep 7 12:57:47 kernel: [*09/07/2025 12:57:47.0240] DTLS connection created sucessfully local_ip: 10.127.85.77
local_port: 5256 peer_ip: 10.127.84.20 peer_port: 5246, app_tag: 2C5741582524 CN:Cisco Manufacturing CA III

Sep 7 12:57:47 kernel: [*09/07/2025 12:57:47.0649] dtls_verify_server_cert: Controller certificate verification
successful

Sep 7 12:57:47 kernel: [*09/07/2025 12:57:47.4022] Dtls Session Established with the AC 10.127.84.20, port 5246

WLC RA Trace :

2025/09/07 12:57:47.222608830 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [15069]: (note): MAC: 1416.9d2a.bf80
DTLS session create callback received.

2025/09/07 12:57:47.284328730 {wncd_x_R0-0}{1}: [ewlc-dtls-sessmgr] [15069]: (info): Remote Host:
10.127.85.77[5256] MAC: 1416.9d2a.bf80 Completed cert verification, status: CERT_VALIDATE_SUCCESS

Correlating AP Debugs & WLC Traces

3. Join Phase

AP Debugs :

Sep 7 12:57:47 kernel: [*09/07/2025 12:57:47.4135] CAPWAP State: Join

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.3521] Sending Join request to 10.127.84.20 through port 5256, packet size 1376

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.3565] Join Response from 10.127.84.20 packet size 1397

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.3873] Starting Post Join timer

WLC RA Trace :

2025/09/07 12:57:48.550108207 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [15069]: (note): MAC: 1416.9d2a.bf80

Received CAPWAP join request

2025/09/07 12:57:48.553214349 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [15069]: (note): MAC: 1416.9d2a.bf80
Successfully processed Join request. AP name: BGL-Edge1-AP1, Model: C9130AXE-D, radio slots: 3, rlan slots: 0, site tag name: ST_Banga_BGL18_caba6_0, policy tag name: PT_Banga_BGL18_BGL18-Se_52ab9, rf tag name: TYPICAL

2025/09/07 12:57:48.553368425 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [15069]: (info): MAC: 1416.9d2a.bf80
Join Response generated with MTU 1485 as per MTU payload, update flag: 0

2025/09/07 12:57:48.553386207 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [15069]: (note): MAC: 1416.9d2a.bf80
Join processing complete. AP in joined state

Correlating AP Debugs & WLC Traces

4. Image

AP Debugs :

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.3962] CAPWAP State: Image Data

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.3968] AP image version 17.9.5.47 backup 17.9.3.50, Controller 17.9.5.47

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.3969] CAPWAP Image Data: MWAR Controller image running version 17.9.5.47 is accepted.

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.3969] Version is the same, do not need update.

WLC RA Trace :

2025/09/07 12:57:48.554127571 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [15069]: (info): 1416.9d2a.bf80 Retrieved AP SW version: 17.9.5.47, for AP model: C9130AXE-D, AP image type: ap1g6a, site-tag: ST_Banga_BGL18_caba6_0

Correlating AP Debugs & WLC Traces

5. Configure & Run

AP Debugs :

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.5007] CAPWAP State: Configure

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.8400] Configuration Status sent to 10.127.84.20 (part 0)

Sep 7 12:57:48 kernel: [*09/07/2025 12:57:48.8434] Configuration Status Response from 10.127.84.20

Sep 7 12:57:49 kernel: [*09/07/2025 12:57:49.3048] CAPWAP State: Run

Sep 7 12:57:49 kernel: [*09/07/2025 12:57:49.3395] CAPWAP data tunnel ADD to forwarding SUCCEEDED

Sep 7 12:57:49 kernel: [*09/07/2025 12:57:49.3543] AP has joined controller c9800-40-BGL

WLC RA Trace :

2025/09/07 12:57:49.038381077 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [15069]: (note): MAC: 1416.9d2a.bf80

Received CAPWAP config status request

2025/09/07 12:57:49.038455973 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [15069]: (note): MAC: 1416.9d2a.bf80
Successfully handled Config status request.

2025/09/07 12:57:49.040192648 {wncd_x_R0-0}{1}: [lisp-agent-api] [15069]: (info): AP Join Successful for MAC: 1416.9d2a.bf80

Wireless Config Analyzer Express (WCAE)

- How to leverage WCAE
- Using WCAE to troubleshoot WNCd utilization

WCAE – Cloud Version

 [Download Full Report](#)

Wireless Analyzer Results

- WLC Messages
- AP Message Summary
- RF Stats WLC Level Summary
- RF Stats AP Site Summary
- RF Stats Flex Profile Summary
- RF Health WLC Level Summary
- RF Health AP Site Summary
- RF Health Flex Profile Summary
- AP Models Summary
- AP Modes Summary
- WLC Logs Summary
- Show All
- Hide All

RF Health WLC Level Summary

Total Unique Messages

Message Type	Count
Error	4
Warning	28
Info	16
Parsing Errors	0
Processing Errors	0

230038	Management: To prevent WebUI issues while using some large GUI options (VLANs for example), it is advisable to increase the VTY count to 50 Action: Use the command 'line vty 0 50' to increase the VTY count
230044	Security: Management over Wireless is enabled, this is not recommended from a security point of view Action: Management over wireless should be used with care, only enable if absolutely required. Check 9800 Best practices guide for more information
230056	Management: Service tcp-keepalive in/out, should be enabled to reduce lingering inactive connections to management points Action: Add: service tcp-keepalives in/service tcp-keepalives out to configuration
60020	RF: WLC has 80.0% of APs with failed Interference Profile for 2.4GHz Band Action: None

		2.4GHz Band			5GHz Band		
Stats	Total Radios	15			74		
	Health Assessment						
	Lowest Metric Average	0			0		
		Low	Medium	High	Low	Medium	High
AP Radio Count per RF Health Metrics	Co-Channel Neighbor Utilization	0	0	15	0	2	72
	Co-Channel Overlapping	0	1	14	16	2	56
	Side Channel Overlapping	0	0	15	0	0	74
	Noise Same Channel	0	0	15	0	0	74
	Noise Side Channel	0	0	15	0	0	74
	Interference Same Channel	0	0	15	0	0	74

WCAE –Excel Download

Table of contents

Generated: 2025-09-12 12:28
WCAE Version: 0.41

Total Message Counts

Errors: 12
Warnings: 39
Informational: 23
Program Execution
Parsing Errors: 4
Processing Errors: 680

[Debug Data](#)

	A	B	C	D	E
1					
2	Type	Count	Log Signature	Back to Content Tab	Explanation
3	Client 8021x Fail(ed/ures)	348223	CO_CLIENT_DELETE_REASON_CLIENT_8021X_FAILURE	May happen during Normal Onboarding	Client reported authentication error on deauth frame
4	Inter Instance Roam Success	251715	CO_CLIENT_DELETE_REASON_INTER_WNCD_ROAM_SUCCESS	May happen during Normal Onboarding	Client roamed across WNCD instances. This is normal scenario for default tag, or roaming across tags
5	Incorrect Credentials	121346	CO_CLIENT_DELETE_REASON_CLIENT_CREDENTIAL_FAILURE	May need validation	Wrong username or password
6	Client Eap Timeout	114699	CO_CLIENT_DELETE_REASON_CLIENT_EAP_TIMEOUT_FAILURE	May happen during Normal Onboarding	Client reported EAP error on deauth frame
7	L2-auth Connection Timeout	104621	CO_CLIENT_DELETE_REASON_L2AUTH_CONNECT_TIMEOUT	May happen during Normal Onboarding	Client did not complete L2 auth like PSK or 802.1x, in time. Could be normal if client roamed or went out of coverage
8	Mic Validation Fail(ed/ures)	60916	CO_CLIENT_DELETE_REASON_KEY_MGMT_MIC_VALIDATION	May need validation	if WLAN is PSK, possible invalid password. For 802.1x, this is client side supplicant issue
9	L3 Authentication Fail(ed/ures)	59426	CO_CLIENT_DELETE_REASON_L3AUTH_FAIL	May need validation	Security processing for a L3 Auth failed (Webauth/guest)
10	Inter Controller Roam Success	50018	CO_CLIENT_DELETE_REASON_INTER_CTRL_ROAM_SUCCESS	May happen during Normal Onboarding	Successful inter controller client roam
11	Due To Mobility Fail(ed/ures)	18204	CO_CLIENT_DELETE_REASON_MOBILITY_FAILURE	May happen during Normal Onboarding	Client delete, either due to roaming while on IP learning state, or due to policy configuration mismatch
12	Client Miscellaneous Reason	12607	CO_CLIENT_DELETE_REASON_CLIENT_MISC_REASON	May happen during Normal Onboarding	Client reported generic reason in deauth frame
13	Wpa Group Key Update Timeout	10186	CO_CLIENT_DELETE_REASON_GROUP_KEY_UPDATE_TIMEOUT	May need validation	Client did not complete Broadcast key rotation. This may happen if client was sleeping or out of coverage
14	Supplicant Request(s)	10084	CO_CLIENT_DELETE_REASON_USER_REQUEST	May happen during Normal Onboarding	Client deleted due to supplicant sending EAP Logoff. This may happen during machine authentication
15	Due To Ssid Change	8476	CO_CLIENT_DELETE_REASON_WLAN_CHANGE	May happen during Normal Onboarding	Client changed WLANs/SSID
16	Ip-learn Connection Timeout	8163	CO_CLIENT_DELETE_REASON_IPLEARN_CONNECT_TIMEOUT	May happen during Normal Onboarding	Controller did not learn client IP address in the allowed time
17	Dot11r Pre-authentication Fail(ed/ures)	5454	CO_CLIENT_DELETE_REASON_FT_AUTH_RESPONSE	May happen during Normal Onboarding	Client failed pre-authentication during FT roaming
18	Mac Authentication Fail(ed/ures)	5074	CO_CLIENT_DELETE_REASON_MAB_FAILED	May happen during Normal Onboarding	Client failed Mac Authentication Bypass
19	Wpa Key Exchange Timeout	4599	CO_CLIENT_DELETE_REASON_KEY_XCHNG_TIMEOUT	May happen during Normal Onboarding	This can happen during normal scenarios. Client deleted due to EAPoL M1 retries. Possible client side issue, or it roamed during
20	Wrong Psk	3528	CO_CLIENT_DELETE_REASON_EXCLUDE_WRONG_PSK	Possible defect or config error	Client excluded due to wrong PSK password

Back to Content tab

Configuration Checks:

[Controller Checks Results](#)
[APs Checks Results](#)

Controller: 9800WLC

[Data Summary](#)
[Log Summary](#)
[Upgrade Advisor](#)
[Best Practices](#)
[WLAN Summary](#)
[Interface Summary](#)
[RF Profiles 2.4 GHz](#)
[RF Profiles 5 GHz](#)
[RF Profiles 6 GHz](#)
[Site Tags](#)
[Hardware State](#)
[Resources](#)
[Client Stats](#)

[WNCD Load Distribution](#)
[Client Delete Reasons](#)
[Tag/Policy Usage](#)
[RF Stats 2.4GHz](#)
[RF Stats 5GHz](#)
[RF Stats 6GHz](#)
[RF Health 2.4GHz](#)
[RF Health 5GHz](#)
[RF Health 6GHz](#)
[Channel Stats 2.4GHz](#)
[Channel Stats 5GHz](#)
[Channel Stats 6GHz](#)
[Rogue Report](#)
[RF Neighborhood 2.4GHz](#)
[RF Neighborhood 5GHz](#)
[RF Neighborhood 6GHz](#)

Client delete reasons breakup

Client Audit

[Apple IOS](#)
[Cisco 8821](#)
[Drager](#)
[Spectralink](#)
[Vocera](#)

AP Information

[APs Configuration](#)
[APs Slot Configuration](#)
[APs Interface Status](#)
[APs RF Summary 2.4GHz](#)
[APs RF Summary 5GHz](#)
[APs RF Summary 6GHz](#)
[APs RF Health Details](#)
[APs NDP Summarization 2.4GHz](#)
[APs NDP Summarization 5GHz](#)
[APs NDP Summarization 6GHz](#)
[APs RF Neighbors 2.4GHz](#)
[APs RF Neighbors 5GHz](#)
[APs RF Neighbors 6GHz](#)

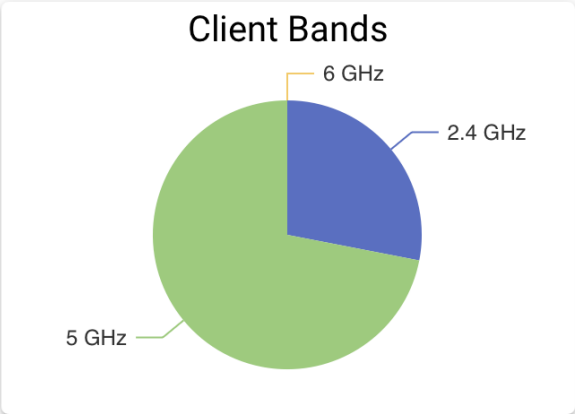
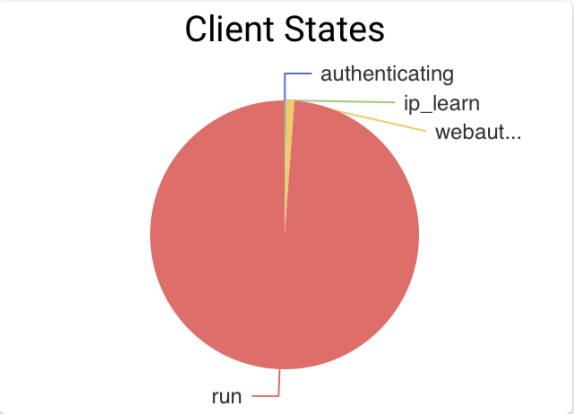
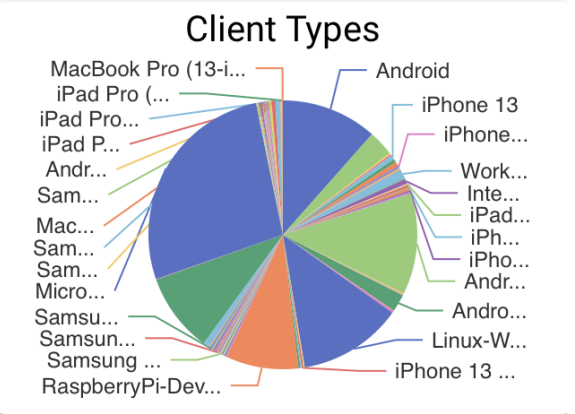
Wireless Config Analyzer Express (WCAE) – Summary



☰

➡

- Summary
- Checks
- Access Points
- Controller
- Site Tags
- Policy Tags
- RF Profiles
- WLANs Summary
- AP RF View
- Channel View
- RF Stats
- RF Health
- Rogue Report
- Performance
- Clients
- Export
- WCAE Logs

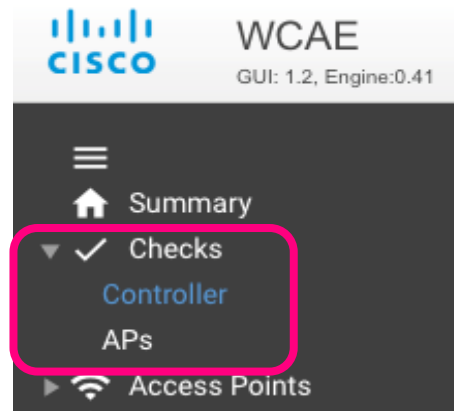


Total Messages	Count
Controller Messages	44
APs Messages	31
Processing Errors	4967
Parsing Errors	4
AP Missing Config	0
AP Missing RF Data	0

Controller Information	
Model	C9800-80-K9
Serial	FOX2803P0TQ
Version	17.15.3
Rommon Version	17.12(2r)
Days Uptime	1
System Name	9800_WLC

General Info	
AP Count	1577
Active Clients	5103
Site Tags	16
Policy Tags	147
Redundancy	Duplex
Multicast/Broadcast	Disabled/Disabled

WCAE – WLC and AP Checks



WLC Checks

Level	Category	Feature	Message	Action
Error	Operational	HW	Controller has a ROMMON version lower than the recommended for the platform	Check ROMMON Software section for your controller, in the Cisco Software Download page, and upgrade to latest version available, otherwise this may prevent future IOS-XE upgrade scenarios
Warning	Operational	RF	WLC has 13.0% of APs with high channel utilization for 2.4GHz Band	
Warning	Operational	RF	WLC has 32.1% of APs with failed Interference Profile for 2.4GHz Band	
Info	Config Error	Tags	More than 100 Site tags detected. Large counts are supported, but they may have a performance impact on some conditions	

AP Checks

60029 Warning Operational RF

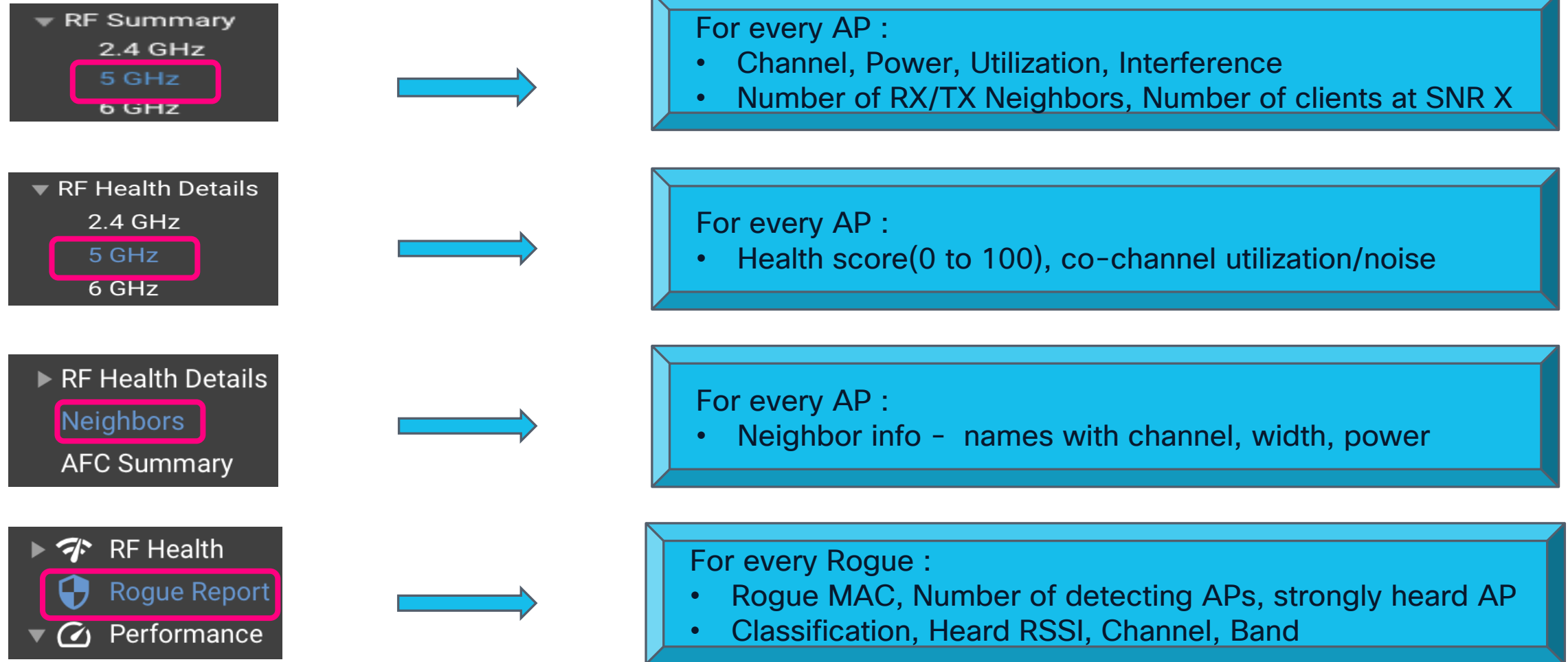
Low coverage detected, action on AP placement recommended

AP shows low coverage (all neighbors < -75 dBm) on 5GHz band. This could affect roaming and be indication of poor RF design or NDP issues

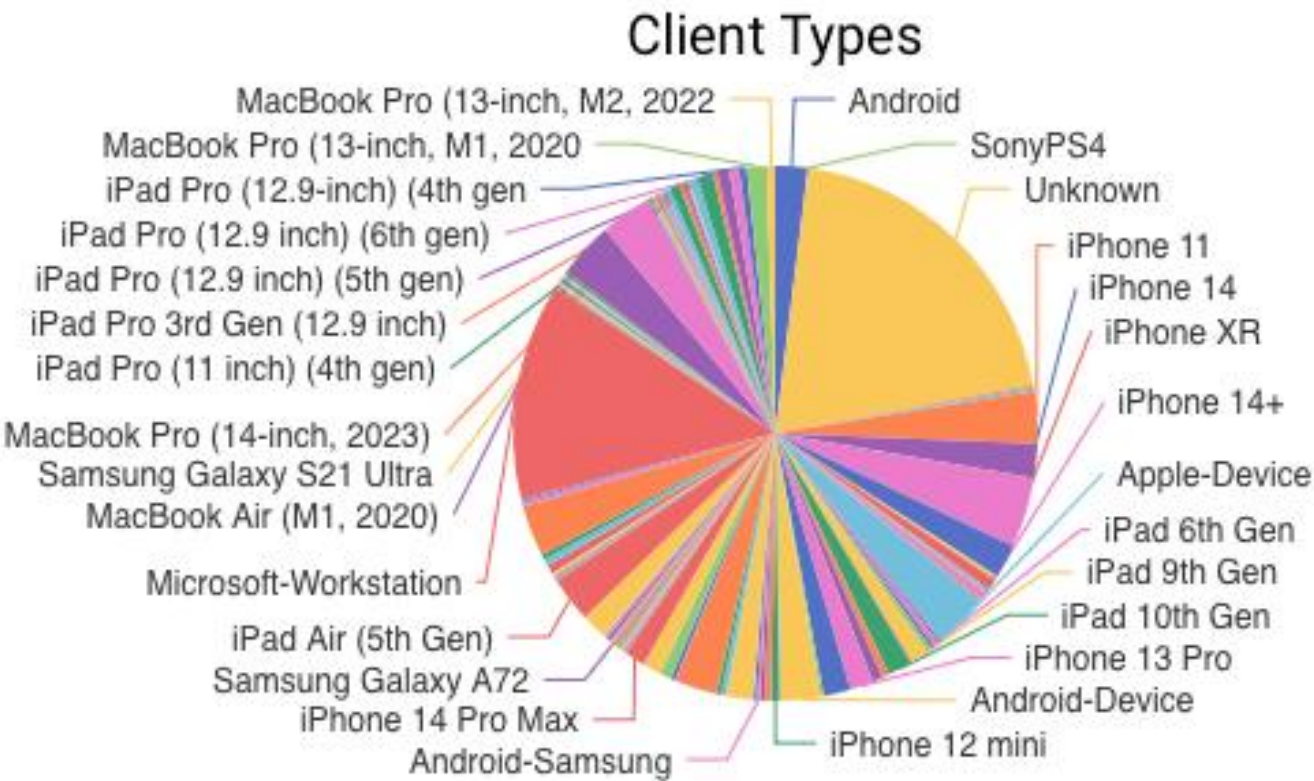
This message is intended to flag APs that don't have a smooth coverage transition to other APs. This may be result of AP physical placement

RF Summarization

Path : Access Points > RF Summary/ RF Health Details/Neighbors or Rogue Report in home page



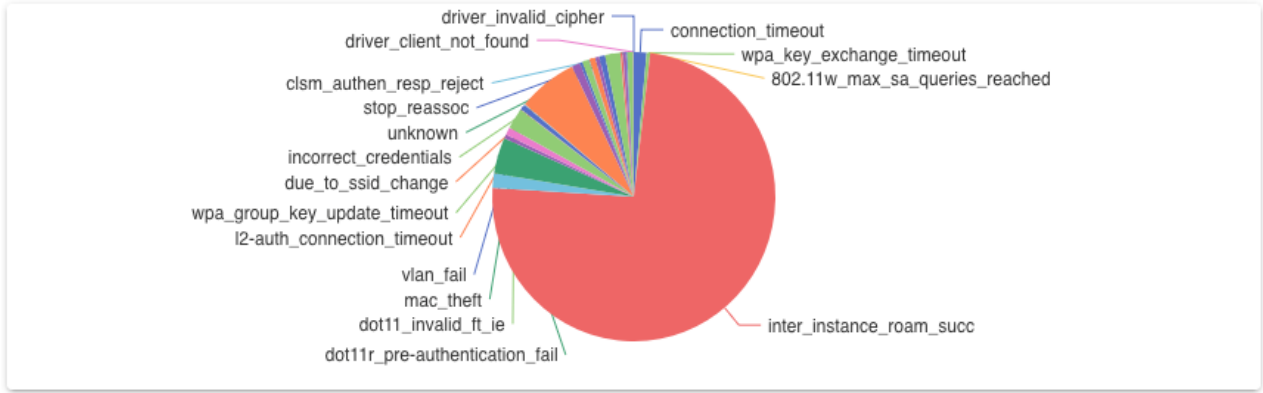
Client Types And Count



Client Type	Count
Android	297
SonyPS4	2
Unknown	3005
iPhone 7	20
iPhone 8	29
HP-Device	1
iPhone 11	467
iPhone 12	310
iPhone 13	634
iPhone 14	304
iPhone 7+	10
iPhone 8+	23
iPhone XR	108
iPhone XS	28

Client Delete Reasons

Client Delete Reasons

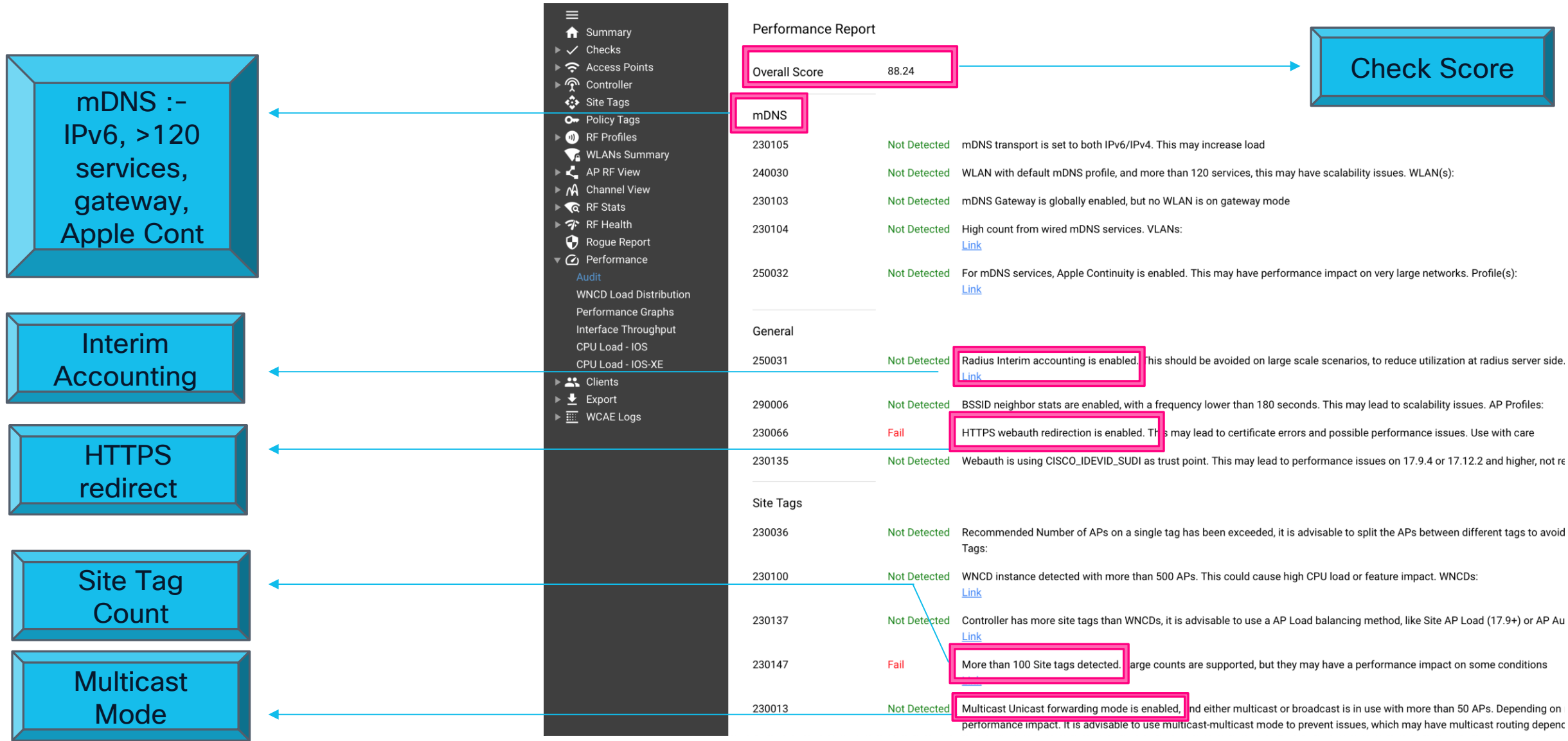


- Count per delete reason
- Reason
- Explanation



Delete Reason	Count	Log Signature	Level	Explanation
Connection Timeout	3314	CO_CLIENT_DELETE_REASON_CONNECT_TIMEOUT	May need validation	Client associated to Flex AP, and did not complete onboarding process, may be triggered if client v
Wpa Key Exchange Timeout	942	CO_CLIENT_DELETE_REASON_KEY_XCHNG_TIMEOUT	May happen during Normal Onboarding	This can happen during normal scenarios. Client deleted due to EAPoL M1 retries. Possible client
802.11w Max Sa Queries Reached	2	CO_CLIENT_DELETE_REASON_MAX_SAQUERIES	May happen during Normal Onboarding	For PMF clients, triggered when client did not reply to SA queries and reached max retries. Could l
Inter Instance Roam Success	169437	CO_CLIENT_DELETE_REASON_INTER_WNCD_ROAM_SUCCESS	May happen during Normal Onboarding	Client roamed across WNCD instances. This is normal scenario for default tag, or roaming across
Due To Mobility Fail(ed/ures)	3699	CO_CLIENT_DELETE_REASON_MOBILITY_FAILURE	May happen during Normal Onboarding	Client delete, either due to roaming while on IP learning state, or due to policy configuration mism
Dot11r Pre-authentication Fail(ed/ures)	9219	CO_CLIENT_DELETE_REASON_FT_AUTH_RESPONSE	May happen during Normal Onboarding	Client failed pre-authentication during FT roaming
Dot11 Fail(ed/ures)	2	CO_CLIENT_DELETE_REASON_DOT11_UNSPECIFIED_FAILURE	May need validation	Association response creation fail, possible due to client malformed request
Dot11 Invalid Akm	1030	CO_CLIENT_DELETE_REASON_DOT11_AKMP_INVALID	Possible defect or config error	Client requested invalid Authentication Key Management during association
Dot11 Received Invalid Pmkid In The Received Rsn le	1950	CO_CLIENT_DELETE_REASON_DOT11_INVALID_PMKID	Possible defect or config error	Controller could not validate PMKID provided by client. This may have different triggers
Dot11 Invalid Mdie	1	CO_CLIENT_DELETE_REASON_DOT11_INVALID_MDIE	May need validation	802.11r(FT) client sent invalid mobility domain
Dot11 Invalid Ft le	5353	CO_CLIENT_DELETE_REASON_DOT11_INVALID_FTIE	May need validation	Failure during FT processing for client. This may have different triggers
Client Eap Id Timeout	55	CO_CLIENT_DELETE_REASON_CLIENT_EAP_ID_TIMEOUT	May happen during Normal Onboarding	Client did not reply to EAP requests in the specified retries/time
Wrong Replay Counter	44	CO_CLIENT_DELETE_REASON_MN_AP_WRONG_REPLAY_COUNTER	May need validation	Invalid replay counter received during EAPoL negotiation. Client should recover on new attempt
Mic Validation Fail(ed/ures)	4	CO_CLIENT_DELETE_REASON_KEY_MGMT_MIC_VALIDATION	May need validation	if WLAN is PSK, possible invalid password. For 802.1x, this is client side supplicant issue

Usecase : Troubleshooting High WNCd Utilization



Troubleshooting High WNCd Utilization (Continued..)

WNCd - AP count

Site Tags		
230036	Not Detected	Recommended Number of APs on a single tag has been exceeded, it is advisable to split the APs between different tags to avoid CPU load issues, and use an AP balancing method. Tags:
230100	Not Detected	WNCd instance detected with more than 500 APs. This could cause high CPU load or feature impact. WNCds: Link

Load Balancing

230137	Not Detected	Controller has more site tags than WNCds, it is advisable to use a AP Load balancing method, like Site AP Load (17.9+) or AP Auto RF balancing (17.12+) Link
230147	Fail	More than 100 Site tags detected. Large counts are supported, but they may have a performance impact on some conditions Link

GUI Latency

230013	Not Detected	Multicast Unicast forwarding mode is enabled, and either multicast or broadcast is in use with more than 50 APs. Depending on network traffic characteristics, this could have large performance impact. It is advisable to use multicast-multicast mode to prevent issues, which may have multicast routing dependencies on your infrastructure
230038	Not Detected	To prevent WebUI issues while using some large GUI options (VLANs for example), it is advisable to increase the VTY count to 50

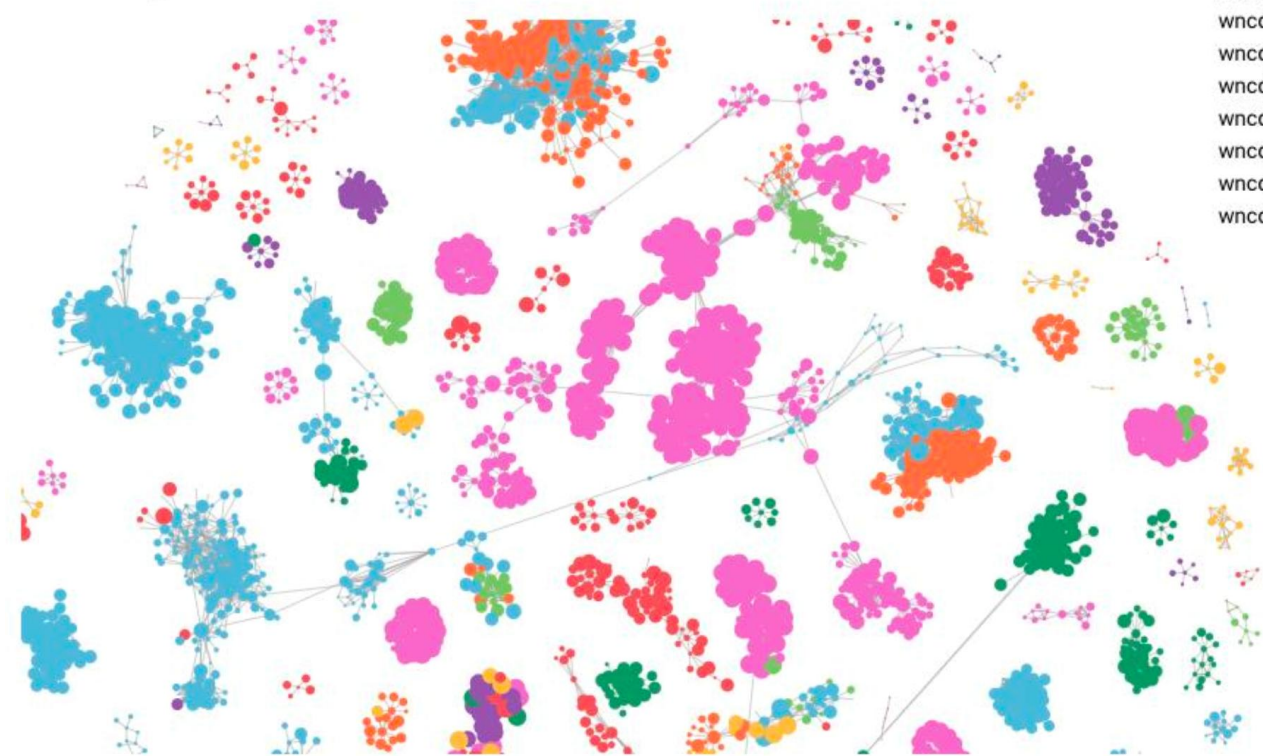
Data Plane Util

CPU		
230148	Not Detected	Process detected with sustained high CPU, please validate if this may be a problem: Link
230149	Not Detected	High Data plane utilization (5 min higher than 80%) Link

WNCd view

RF View - Band: 5 GHz

AP Classified per : WNCd. NDP RSSI: -85



Radio Count:3498		
Link Count: 14740		
WNCd	AP Count	Client Count
wncd0	278	1262
wncd1	700	1843
wncd2	119	1800
wncd3	194	2210
wncd4	682	11152
wncd5	241	461
wncd6	270	1132
wncd7	481	1576

☐ Show Legend | View Type: WNCd | Link RSSI Filter: -85

High Inter WNCd expected(expensive)



Fairly balanced WNCds



WNCd Load Balancing Options

17.3.X:

- The controller load balances the site-tags across the WNCds in a **round robin fashion**
- not always optimal for large networks.

17.9.3 and higher:

- To prevent unbalanced site-tag assignment to WNCds, the **site load command** was introduced in 17.9.3 and higher.
- This allows administrators to predefine the expected load of each site tag.

17.12.X and higher:

- The RF based **Automatic AP Load Balancing** feature uses **Radio Resource Management (RRM)** neighbor report-based AP grouping and load-balancing across WNCd instances.
- When this feature is enabled, it forms AP clusters based on the RSSI received from AP neighbor reports. These clusters or neighborhoods are further split into sub-neighborhoods and smaller areas.
- The resulting groups of APs are then distributed evenly across the WNCd processes

Debug Analyzer

- RA Trace Analyzer
- Obtain quick insights

Simplified Data Collection - Debug Bundle

Log collection in a single command :

RA Traces & Client Tech Support

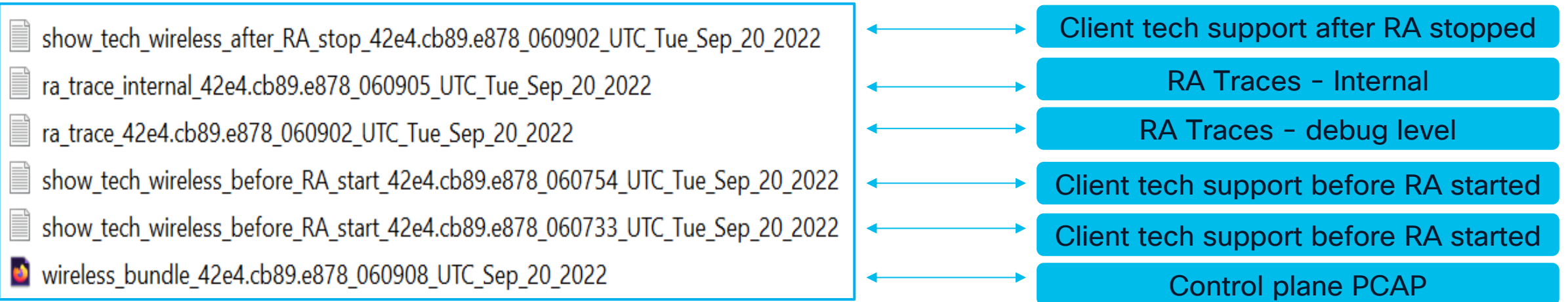
- This collects and captures both RA traces(debug level) and internal RA for the configured clients
- Show tech wireless client MAC of two instances, one before RA trace is enabled and once after RA trace is stopped are captured
- C9800# `debug wireless bundle client <client_mac1 ...client_mac5>`

Packet Capture

- Packet captures at the WLC control plane is collected for the clients
- C9800# `debug wireless bundle include epc client <client_mac1 ...client_mac5>`

Bundle Contents

- i. Two sets of RA traces for all the clients
- ii. Two sets of clients tech support
- iii. WLC control plane captures



RA Trace – Raw File

```
~\Downloads/debugTrace_ec63.d7fc.f729 (2).txt
1 Logging display requested on 2025/06/23 12:00:04 (IST) for Hostname: [c9800-40-SJC], Model: [C9800-40-K9], Version: [17.09.05], SN: [JAE271507TK], MD_SN: [TTM265101FM]
2 2025/06/20 18:28:15.073514051 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729 Association received. BSSID 889c.ade7.9281, WLAN SJ_Corp_SSID_profile, Slot 0 AP 889c.ade7.9280, SJ-E
3 2025/06/20 18:28:15.073746134 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729 Client state transition: S_CO_INIT -> S_CO_ASSOCIATING
4 2025/06/20 18:28:15.074469577 {wncd_x_R0-0}{1}: [dot11] [15082]: (note): MAC: ec63.d7fc.f729 Association success. AID 1, Roaming = False, WGB = False, 11r = False, 11w = False Fast roam = False
5 2025/06/20 18:28:15.074852467 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729 Client state transition: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS
6 2025/06/20 18:28:15.075299006 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729 ADD MOBILE sent. Client state flags: 0x41 BSSID: MAC: 889c.ade7.9281 capwap IFID: 0x90000003, Add mobil
7 2025/06/20 18:28:15.079588340 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729 L2 Authentication initiated. method DOT1X, Policy VLAN 1, AAA override = 1, NAC = 0
8 2025/06/20 18:28:15.080450179 {wncd_x_R0-0}{1}: [site-manager-ap] [15082]: (ERR): Failed to get flex interface name vlan table root
9 2025/06/20 18:28:15.081349113 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [15082]: (note): Authentication Success. Resolved Policy bitmap:11 for client ec63.d7fc.f729
10 2025/06/20 18:29:45.082253726 {wncd_x_R0-0}{1}: [errmsg] [15082]: (note): %DOT1X-5-FAIL: R0/0: wncd: Authentication failed for client (ec63.d7fc.f729) with reason (No Response from Client) on Interface ca
11 2025/06/20 18:29:45.082531498 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [15082]: (ERR): SANET_AUTHC_FAILURE - No Response from Client, audit session id 15547F0A0000005A806B16A7
12 2025/06/20 18:29:45.082550762 {wncd_x_R0-0}{1}: [errmsg] [15082]: (note): %SESSION_MGR-5-FAIL: R0/0: wncd: Authorization failed or unapplied for client (ec63.d7fc.f729) on Interface capwap_90000003 AuditS
13 2025/06/20 18:29:55.083275604 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729 Co client reap timer callback. Co client reap timer triggering E_CO_CLIENT_CONNECT_TIMEOUT event, cli
14 2025/06/20 18:29:55.083342500 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [15082]: (ERR): ec63.d7fc.f729CLIENT_STAGE_TIMEOUT State = AUTHENTICATING, WLAN profile = SJ_Corp_SSID_profile, Policy profile = SJ_Corp_SS
15 2025/06/20 18:29:55.083369294 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729 Client delete initiated. Reason: CO_CLIENT_DELETE_REASON_L2AUTH_CONNECT_TIMEOUT, details: , fsm-state
16 2025/06/20 18:29:55.083519937 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729 Delete mobile payload sent for BSSID: 889c.ade7.9281 WTP mac: 889c.ade7.9280 slot id: 0
17 2025/06/20 18:29:55.083699299 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729 Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_DELETE_IN_PROGRESS
18 2025/06/20 18:29:55.084613832 {wncd_x_R0-0}{1}: [sanet-shim-translate] [15082]: (note): MAC: ec63.d7fc.f729 Session manager disconnect event called, session label: 0x34000050
19 2025/06/20 18:29:55.085742854 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729 Client state transition: S_CO_DELETE_IN_PROGRESS -> S_CO_DELETED
20 2025/06/23 06:41:02.209724436 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729 Association received. BSSID 889c.ade7.9280, WLAN EEC_Exp, Slot 0 AP 889c.ade7.9280, SJ-Edge2-AP1, Sit
21 2025/06/23 06:41:02.209964796 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729 Client state transition: S_CO_INIT -> S_CO_ASSOCIATING
22 2025/06/23 06:41:02.210705345 {wncd_x_R0-0}{1}: [dot11] [15082]: (note): MAC: ec63.d7fc.f729 Association success. AID 1, Roaming = False, WGB = False, 11r = False, 11w = False Fast roam = False
23 2025/06/23 06:41:02.211068931 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729 Client state transition: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS
24 2025/06/23 06:41:02.211353370 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729 L2 Authentication initiated. method PSK, Policy VLAN 352, AAA override = 0, NAC = 0
25 2025/06/23 06:41:02.213391451 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [15082]: (note): Authentication Success. Resolved Policy bitmap:11 for client ec63.d7fc.f729
26 2025/06/23 06:41:02.213614721 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729 ADD MOBILE sent. Client state flags: 0x71 BSSID: MAC: 889c.ade7.9280 capwap IFID: 0x90000003, Add mobil
27 2025/06/23 06:41:02.253665212 {wncd_x_R0-0}{1}: [client-keymgmt] [15082]: (note): MAC: ec63.d7fc.f729 EAP Key management successful. AKM:PSK Cipher:CCMP WPA Version: WPA2
28 2025/06/23 06:41:02.253808853 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729 L2 PSK Authentication Success. EAP type: NA, Resolved VLAN: 352, Audit Session id: 15547F0A000000A59A56B
29 2025/06/23 06:41:02.254249467 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729 Mobility discovery triggered. Client mode: Local
30 2025/06/23 06:41:02.254254623 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729 Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS
31 2025/06/23 06:41:02.255433129 {wncd_x_R0-0}{1}: [mm-client] [15082]: (note): MAC: ec63.d7fc.f729 Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Client IFID: 0xa0000003, Client R
32 2025/06/23 06:41:02.255590673 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729 ADD MOBILE sent. Client state flags: 0x72 BSSID: MAC: 889c.ade7.9280 capwap IFID: 0x90000003, Add mobil
33 2025/06/23 06:41:02.255766465 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729 Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS
34 2025/06/23 06:41:02.255888594 {wncd_x_R0-0}{1}: [dot11] [15082]: (note): MAC: ec63.d7fc.f729 Client datapath entry params - ssid:EEC_Exp,slot_id:0 bssid ifid: 0x0, radio_ifid: 0x9000000a, wlan_ifid: 0xf0
35 2025/06/23 06:41:02.256196600 {wncd_x_R0-0}{1}: [dpath_svc] [15082]: (note): MAC: ec63.d7fc.f729 Client datapath entry created for ifid 0xa0000003
36 2025/06/23 06:41:02.256476894 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729 Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
37 2025/06/23 06:41:02.404022207 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (ERR): MAC: 0000.0000.0000 vlan_mode_api: fsm_ctxt not found
38 2025/06/23 06:41:05.778682535 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (ERR): MAC: 0000.0000.0000 vlan_mode_api: fsm_ctxt not found
39 2025/06/23 07:17:22.705798404 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729 Re-Association received. BSSID 889c.ade7.9880, WLAN EEC_Exp, Slot 0 AP 889c.ade7.9880, SJ-Edge2-AP2,
40 2025/06/23 07:17:22.705935348 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729 Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
41 2025/06/23 07:17:22.706466185 {wncd_x_R0-0}{1}: [dot11] [15082]: (note): MAC: ec63.d7fc.f729 Association success. AID 2, Roaming = True, WGB = False, 11r = False, 11w = False Fast roam = False
42 2025/06/23 07:17:22.706695241 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729 Delete mobile payload sent for BSSID: 889c.ade7.9280 WTP mac: 889c.ade7.9280 slot id: 0
43 2025/06/23 07:17:22.707108086 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729 Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L2_AUTH_IN_PROGRESS
44 2025/06/23 07:17:22.708088849 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729 ADD MOBILE sent. Client state flags: 0x71 BSSID: MAC: 889c.ade7.9880 capwap IFID: 0x9000000c, Add mobil
45 2025/06/23 07:17:22.744876468 {wncd_x_R0-0}{1}: [client-keymgmt] [15082]: (note): MAC: ec63.d7fc.f729 EAP Key management successful. AKM:PSK Cipher:CCMP WPA Version: WPA2
46 2025/06/23 07:17:22.745019080 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729 L2 PSK Authentication Success. EAP type: NA, Resolved VLAN: 352, Audit Session id: 15547F0A000000A59A56B
47 2025/06/23 07:17:22.745433966 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729 Mobility discovery triggered. Client mode: Local
48 2025/06/23 07:17:22.745438686 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729 Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS
49 2025/06/23 07:17:22.745697077 {wncd_x_R0-0}{1}: [mm-client] [15082]: (note): MAC: ec63.d7fc.f729 Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_INTRA_INSTANCE, Previous BSSID MAC: 889
50 2025/06/23 07:17:22.745932349 {wncd_x_R0-0}{1}: [client-auth] [15082]: (note): MAC: ec63.d7fc.f729 ADD MOBILE sent. Client state flags: 0x76 BSSID: MAC: 889c.ade7.9880 capwap IFID: 0x9000000c, Add mobil
51 2025/06/23 07:17:22.746104443 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729 Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS
52 2025/06/23 07:17:22.746429588 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729 Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
53 2025/06/23 07:17:39.142919647 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729 Re-Association received. BSSID 2c57.4158.71a0, WLAN EEC_Exp, Slot 0 AP 2c57.4158.71a0, SJ-Edge1-AP2,
54 2025/06/23 07:17:39.143042319 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729 Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
55 2025/06/23 07:17:39.143657454 {wncd_x_R0-0}{1}: [dot11] [15082]: (note): MAC: ec63.d7fc.f729 Association success. AID 1, Roaming = True, WGB = False, 11r = False, 11w = False Fast roam = False
56 2025/06/23 07:17:39.143943419 {wncd_x_R0-0}{1}: [client-orch-sm] [15082]: (note): MAC: ec63.d7fc.f729 Delete mobile payload sent for BSSID: 889c.ade7.9880 WTP mac: 889c.ade7.9880 slot id: 0
57 2025/06/23 07:17:39.144396513 {wncd_x_R0-0}{1}: [client-orch-state] [15082]: (note): MAC: ec63.d7fc.f729 Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L2_AUTH_IN_PROGRESS
```



Debug Analyzer - Home Page

Show Advanced Debug Insights

NEW!!

Select a client MAC Address and connection to see logs.



[Download CSV](#)

ec63.d7fc.f729

Connection 10 of 10 < 1 ... 9 10 >

- ☒ Show Time
- ☒ Show Task
- ☒ Show Translated
- ☐ Show Original
- ☐ Show Prior First Connection
- ☐ Show All

Time	Task	Translated
2025/06/23 12:08:05.797	client-orch-sm	Client made a new Association to an AP/BSSID: BSSID 889c.ade7.9881, WLAN SJ_Corp_SSID_profile, Slot 0 AP 889c.ade7.9880, SJ-Edge2-AP2, Site tag ST_SanJo_Corporat_9248f_0, Policy tag PT_SanJo_Corpo_Corporat_78519, Policy profile SJ_Corp_SSID_profile, Switching Local, old BSSID 889c.ade7.9881, Socket delay 0ms
2025/06/23 12:08:05.798	dot11	Association success for client, assigned AID is: 2
2025/06/23 12:08:32.420	client-auth	Starting EAPOL 4-Way Handshake
2025/06/23 12:08:32.436	client-keymgmt	Negotiated the following encryption mechanism: AKM:DOT1X Cipher:CCMP WPA Version: WPA2
2025/06/23 12:08:32.436	client-orch-state	Starting Mobility Anchor discovery for client
2025/06/23 12:08:32.439	client-orch-state	Entering IP learn state
2025/06/23 12:08:32.493	client-iplearn	Client got IP: 10.127.85.54, discovered through: IP Snooping

Advanced Debug Insights

of success/failed sessions, start/end timestamp per client

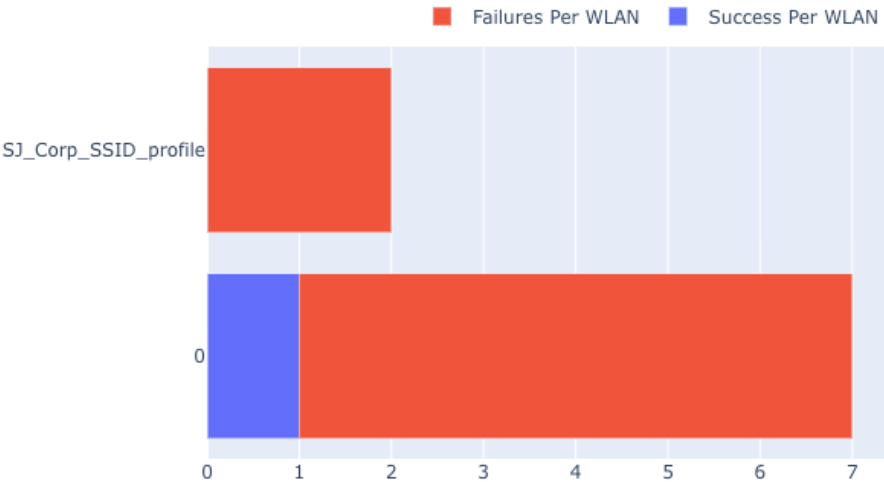


Advanced Debug Insights

9800 WLC Advanced Debug Insights [\(Help\)](#)

Client MAC Address	Success Sessions	Failed Sessions	Start Time	End Time
ec63.d7fc.f729	1	8	June 23, 2025 11:50:4...	June 23, 2025 12:08:05...

Success/Failure stats per WLAN



Advanced Debug Insights

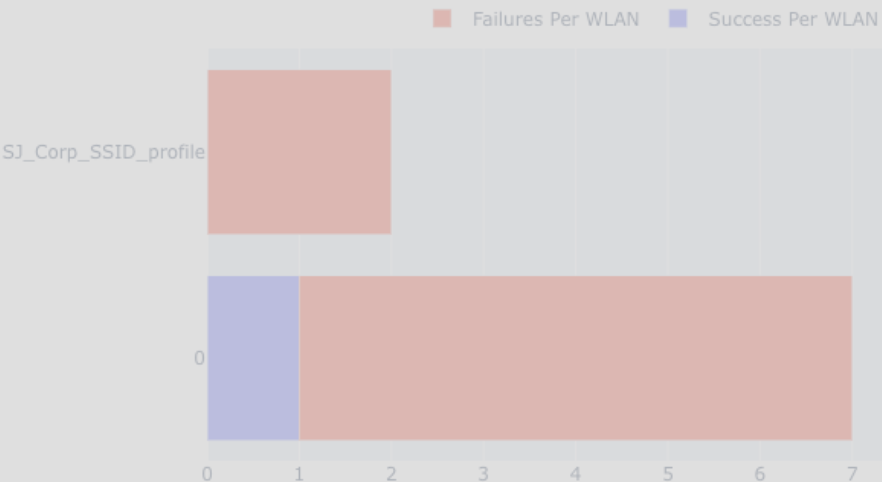
of success/failed sessions, start/end timestamp per client

Advanced Debug Insights

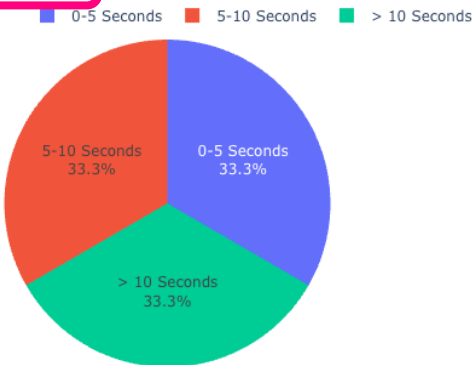
9800 WLC Advanced Debug Insights (Help)

Client MAC Address	Success Sessions	Failed Sessions	Start Time	End Time
ec63.d7fc.f729	1	8	June 23, 2025 11:50:4...	June 23, 2025 12:08:05...

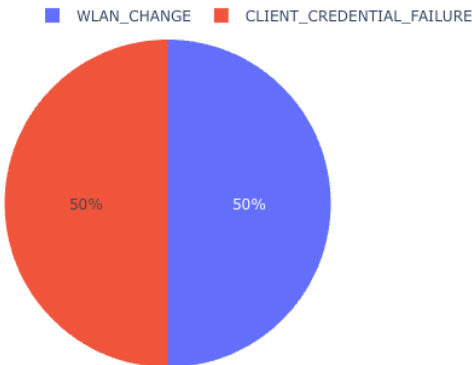
Success/Failure stats per WLAN



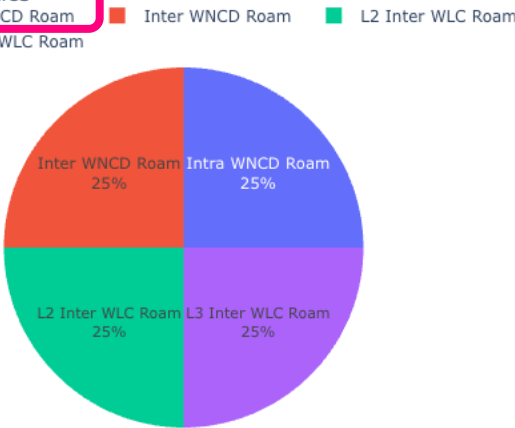
Client Onboarding Time



Delete Reasons



Client Roam Statistics



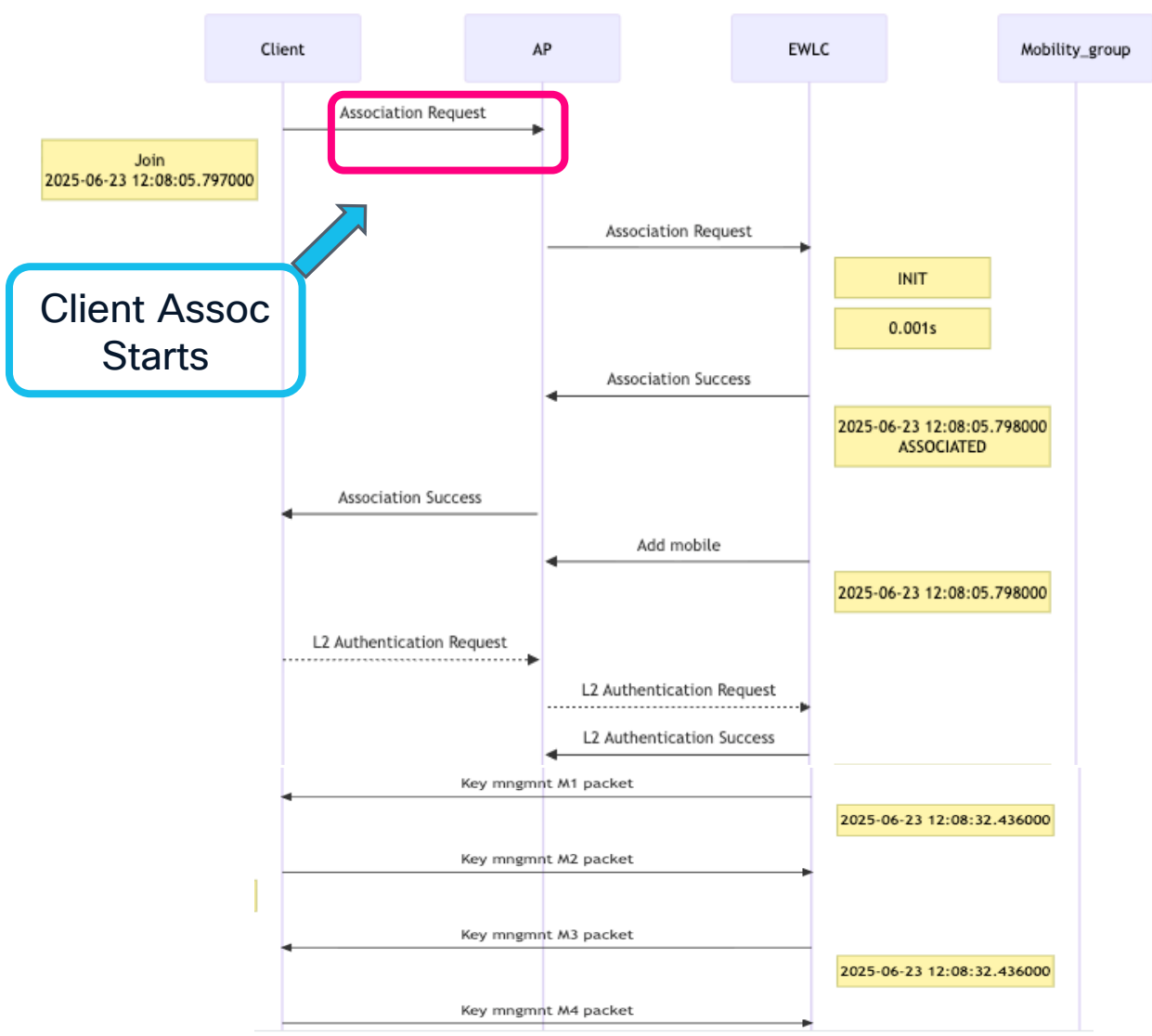
Client Onboarding time for 0-5/10 secs, Delete Reasons, Roam (Intra/inter WNCd/WLC stats)

Client Session Table

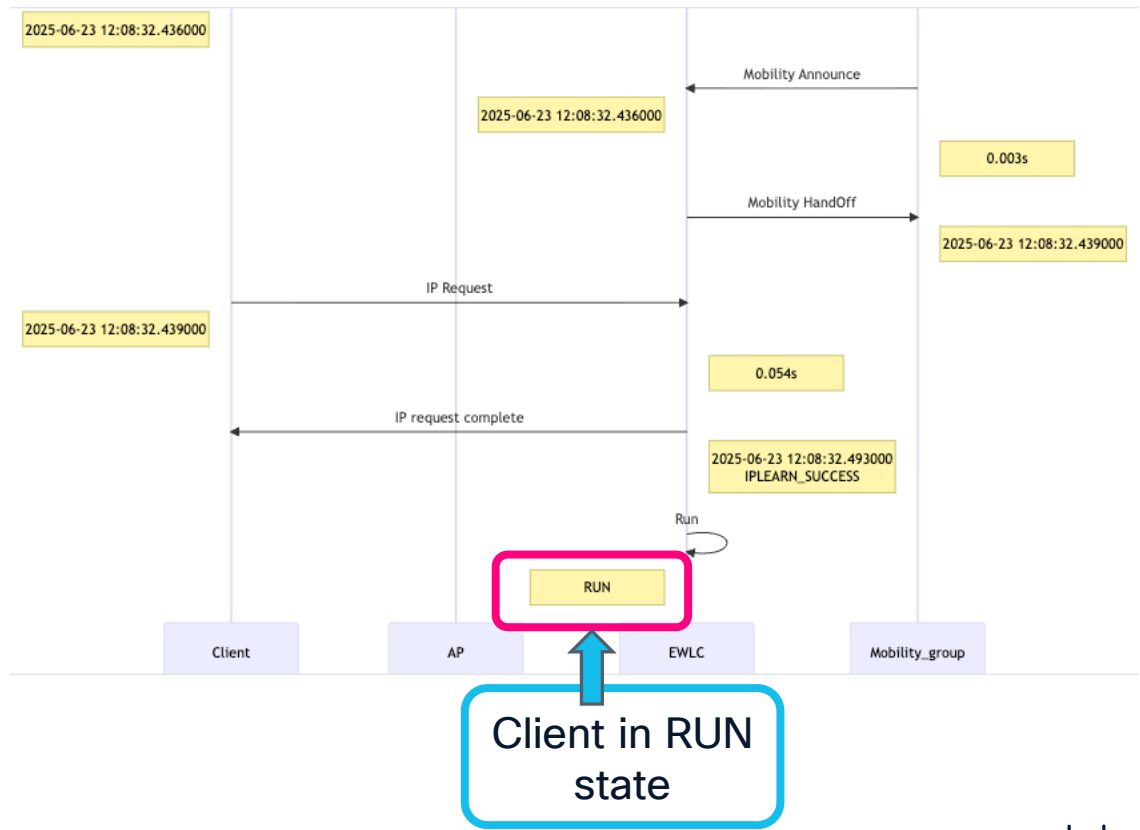
Client MAC: Ec63.D7fc.F729

Session	State	Auth Method	AP	WLAN	Mobility Role	IP Address	Onboarding Time	Start/Run Time	Delete Reason	Delete Time
1		IPLEARN	UNKNOWN	Site tag ST_SanJo_Corporat_9248f_0	0	Local-None		0 ms	11:50:47:555 /	
2		INIT	UNKNOWN	Site tag ST_SanJo_Corporat_9248f_0	0	NONE-NONE		0 ms	12:04:28:337 /	WLAN_CHANGE 12:04:28:000
3		L2AUTH	DOT1X	889c.ade7.9280	SJ_Corp_SSID_profile	NONE-NONE		0 ms	12:04:28:340 /	
4		L2AUTH	DOT1X	Site tag ST_SanJo_Corporat_9248f_0	0	NONE-NONE		0 ms	12:04:29:900 /	CLIENT_CREDENTIAL_FAILURE 12:04:43:000
5		L2AUTH	DOT1X	889c.ade7.9880	SJ_Corp_SSID_profile	NONE-NONE		0 ms	12:07:12:867 /	
6		L2AUTH	DOT1X	Site tag ST_SanJo_Corporat_9248f_0	0	NONE-NONE		0 ms	12:07:14:325 /	
7		L2AUTH	DOT1X	Site tag ST_SanJo_Corporat_9248f_0	0	NONE-NONE		0 ms	12:07:15:568 /	
8		L2AUTH	DOT1X	Site tag ST_SanJo_Corporat_9248f_0	0	NONE-NONE		0 ms	12:07:36:743 /	
9		RUN	DOT1X	Site tag ST_SanJo_Corporat_9248f_0	0	Local-None	10.127.85.54	26698 ms	12:08:05:797 / 12:08:32:495	

Packet Flow Between Client, AP, WLC



← → Transaction seen in the log file
←...→ Transaction not seen in log file. (Doesn't mean this is expected or needed always)



WiFi-HAWK

- Over the air capture analyzer

WiFi-Hawk

- Expert system to **identify problems** over from a wireless capture
 - Hard to see issues found in huge files
 - Low level protocol analysis
 - Interoperability problems
- Generate a **summary of events** per client and AP WLANs
- Create **expert reports**



WiFi Hawk

How to use?



- Upload file
- View Excel Analysis

▶▶▶▶▶▶▶▶	Auth request	Info	2727	FT BSS Transition
◀◀◀◀◀◀◀◀	Auth resp-fail	Error	2729	Failed, Status code:Invalid pairwise master key identifier
-----	General Warning	Warning	2731	Deauth sent from client, not to current AP. Reason:1 (Unspecified)
▶▶▶▶▶▶▶▶	Auth request	Info	3367	FT BSS Transition
◀◀◀◀◀◀◀◀	Auth resp-fail	Error	3370	Failed, Status code:Invalid pairwise master key identifier
-----	General Warning	Warning	3372	Deauth sent from client, not to current AP. Reason:1 (Unspecified)

Quick Index view

- List of **BSSIDs** (APs) and **clients** active during the capture
- **Quick glance** on who is having problems
- **Last known state** for each client (probing, auth, full traffic, etc)
- **Click** on each item for **full details**

Table of contents

Generated:

2022-03-11 10:28

Wireless Consultant Version:

0.7

Total Frames:

82685

File Type:

Radio Tap

Processing time:

131.21 seconds

Total BSSIDs seen:

76

Total Clients seen:

175

Processing Errors:

Invalid Frames

0

Exceptions

75

Non Parsed Frames

0

Filtered Frames

0

FCS Errors

0

AP BSSIDs

SSID	Events	Errors	Warnings
e0:10:7f:65:61:53	146	0	145
58:1d:91:6b:2d:10	58	0	57
58:bf:ea:bb:c0:66	57	0	56
58:bf:ea:bb:c0:61	53	0	52
58:bf:ea:bb:c0:67	50	0	49
58:bf:ea:bb:c0:60	49	0	48
58:bf:ea:bb:c0:6d	43	0	40

Clients

Last State	Events	Errors	Warnings
EAPoL 4-WAY completed	555	0	0
Deauthenticated	476	0	476
Association failed	445	0	0
Probing	441	0	0
Probing	402	0	0
Bidirectional Traffic	250	2	0
Probing	228	0	0

Event Flow

- Color coded events registered per device
- Summary of repeated items for a more concise view
- Quick location in capture of important issues (frame/time)
- Added information for better understanding
- Translation of reason codes, failures, EAP types, etc

Event Flow:										
Direction	Type	Severity	BSSID	Frame	Time	Info				
>>>>>>	Probe requests	Info	NA	28669	NA	Consecutive requests:48				
<<<<<<	Probe responses	Info	NA	28617	NA	Consecutive responses:223				
>>>>>>	Auth request	Info	64:f6:9d:55:5c:f4	28688	Thu, 12 May 2016 11:22:33 CEST	Auth Open System				
<<<<<<	Auth resp success	Info	64:f6:9d:55:5c:f4	28690	Thu, 12 May 2016 11:22:33 CEST	Auth Open System				
>>>>>>	Assoc request	Info	64:f6:9d:55:5c:f4	28693	Thu, 12 May 2016 11:22:33 CEST	Type: 802.1x . To SSID:Jio_AKA-Ahmedabad				
<<<<<<	EAP ID request	Info	64:f6:9d:55:5c:f4	28701	Thu, 12 May 2016 11:22:33 CEST	Identity request				
>>>>>>	EAP ID response	Info	64:f6:9d:55:5c:f4	28715	Thu, 12 May 2016 11:22:33 CEST	Identity response				
<<<<<<	EAP request	Info	64:f6:9d:55:5c:f4	28802	Thu, 12 May 2016 11:22:33 CEST	EAP-AKA				
>>>>>>	EAP response	Info	64:f6:9d:55:5c:f4	28880	Thu, 12 May 2016 11:22:33 CEST	EAP-AKA				
>>>>>>	EAP response	Info	64:f6:9d:55:5c:f4	28883	Thu, 12 May 2016 11:22:33 CEST	EAP-AKA				
<<<<<<	EAP Success	Info	64:f6:9d:55:5c:f4	29201	Thu, 12 May 2016 11:22:34 CEST	Dot1x Auth success				
<<<<<<	EAP KEY RX	Info	64:f6:9d:55:5c:f4	29203	Thu, 12 May 2016 11:22:34 CEST	EAPoL M1				
<<<<<<	EAP Start	Info	64:f6:9d:55:5c:f4	29214	Thu, 12 May 2016 11:22:34 CEST	EAP START				
<<<<<<	EAP Start	Info	64:f6:9d:55:5c:f4	29219	Thu, 12 May 2016 11:22:34 CEST	EAP START				
<<<<<<	EAP ID request	Info	64:f6:9d:55:5c:f4	29221	Thu, 12 May 2016 11:22:34 CEST	Identity request				
<<<<<<	EAP ID request	Info	64:f6:9d:55:5c:f4	29223	Thu, 12 May 2016 11:22:34 CEST	Identity request				
>>>>>>	Client going to sleep	Info	64:f6:9d:55:5c:f4	39809	Thu, 12 May 2016 11:22:53 CEST	Signaling AP that is going to sleep				
>>>>>>	Sleep Time	Warning	NA	48017	NA	Client slept for more than 0:00:12 seconds				
>>>>>>	Sleep Time	Warning	NA	49805	NA	Client slept for more than 0:00:03 seconds				
>>>>>>	Sleep Cycles	Info	NA		NA	Consecutive sleep-awake cycles:2				
>>>>>>	Client awake	Info	64:f6:9d:55:5c:f4	49805	Thu, 12 May 2016 11:23:08 CEST	Signaling AP that is going to sleep				

Detecting easy to miss problems

Simplify finding issues across large captures

- Unencrypted traffic leak (client/AP)
- Beacon loss
- High co-channel
- Incorrect data rates

Event Flow									
Direction	Type	Severity	Frame	Time		Info			
-----	High Channel Utilization	Warning	1	Fri, 15 Mar 2019 21:05:05 CET		Current Channel utilization: 94			
>>>>>>	First Beacon	Info	1	Fri, 15 Mar 2019 21:05:05 CET					
>>>>>>	Beacon loss	Warning	2	Fri, 15 Mar 2019 21:05:06 CET		Beacon loss detected, Time delta:0.824816			
-----	High Channel Utilization	Warning	2	Fri, 15 Mar 2019 21:05:06 CET		Current Channel utilization: 95			
>>>>>>	Beacon loss	Warning	3	Fri, 15 Mar 2019 21:05:08 CET		Beacon loss detected, Time delta:1.427207			
-----	High Channel Utilization	Warning	3	Fri, 15 Mar 2019 21:05:08 CET		Current Channel utilization: 95			
>>>>>>	Beacon loss	Warning	9	Fri, 15 Mar 2019 21:05:11 CET		Beacon loss detected, Time delta:3.523894			
-----	High Channel Utilization	Warning	9	Fri, 15 Mar 2019 21:05:11 CET		Current Channel utilization: 94			
>>>>>>	Beacon loss	Warning	13	Fri, 15 Mar 2019 21:05:16 CET		Beacon loss detected, Time delta:4.612270			

<<<<<<	EAP KEY RX	Info	6c:8b:d3:3b:8a:a0	1271	Thu, 21 Jan 2021 00:51:56 CET	EAPoL M1			
<<<<<<	EAP KEY RX	Info	6c:8b:d3:3b:8a:a0	1273	Thu, 21 Jan 2021 00:51:56 CET	EAPoL M1			
>>>>>>	EAP KEY TX	Info	6c:8b:d3:3b:8a:a0	1330	Thu, 21 Jan 2021 00:51:56 CET	EAPoL M2			
<<<<<<	Unencrypted AP TX Traffic	Error	6c:8b:d3:3b:8a:a0	1333	Thu, 21 Jan 2021 00:51:56 CET	AP defect, traffic sent without encryption			
<<<<<<	EAP KEY RX	Info	6c:8b:d3:3b:8a:a0	1334	Thu, 21 Jan 2021 00:51:56 CET	EAPoL M3			

Diagnostic Tools - Takeaways



Scenario : Troubleshooting Client Connectivity, AP Join, Best Practice miss etc

AP/WLC Debugs

- **Correlating** AP and WLC side of debugs, outputs
- Example : **AP join issues**

WCAE

- **Gain insights** on best practices, warnings, RF, performance issues
- Example : Checking WLC Performance and **High WNCd CPU Issues**

Debug Analyzer

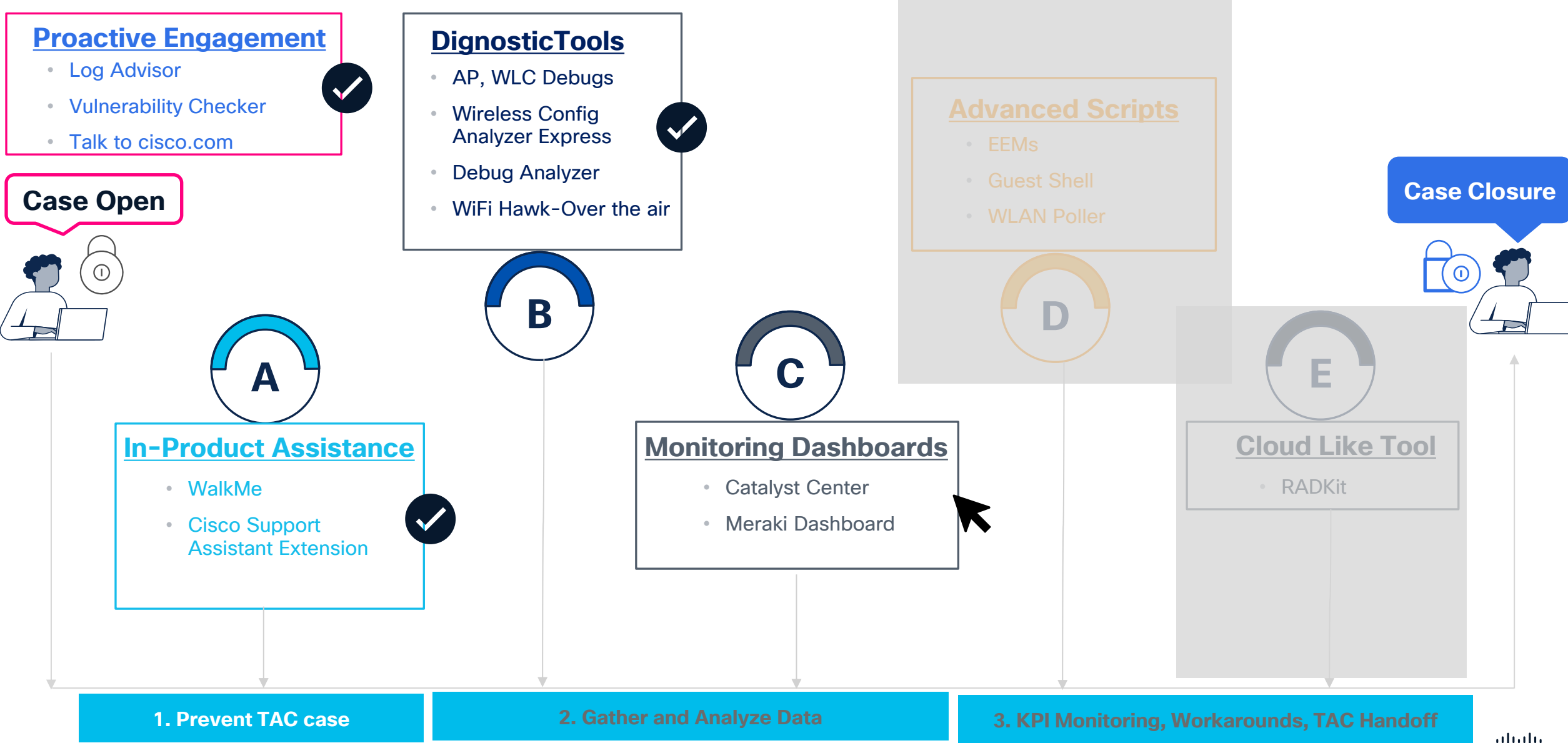
- **Analyze client RA traces** in table, graphical format for quick and easy consumption with various statistics
- Example : **Client connectivity**

WiFi-Hawk (OTA)

- Get **insights on over the air** packet capture
- Example : **Debugging an RF Issue/AP/Client issue**

C-Monitoring Dashboards

Flexible Options to Self-Serve & Accelerate Case Resolution



Monitoring Catalyst Center, Meraki Dashboard



Scenario : Obtain insights, assurance information, various reports

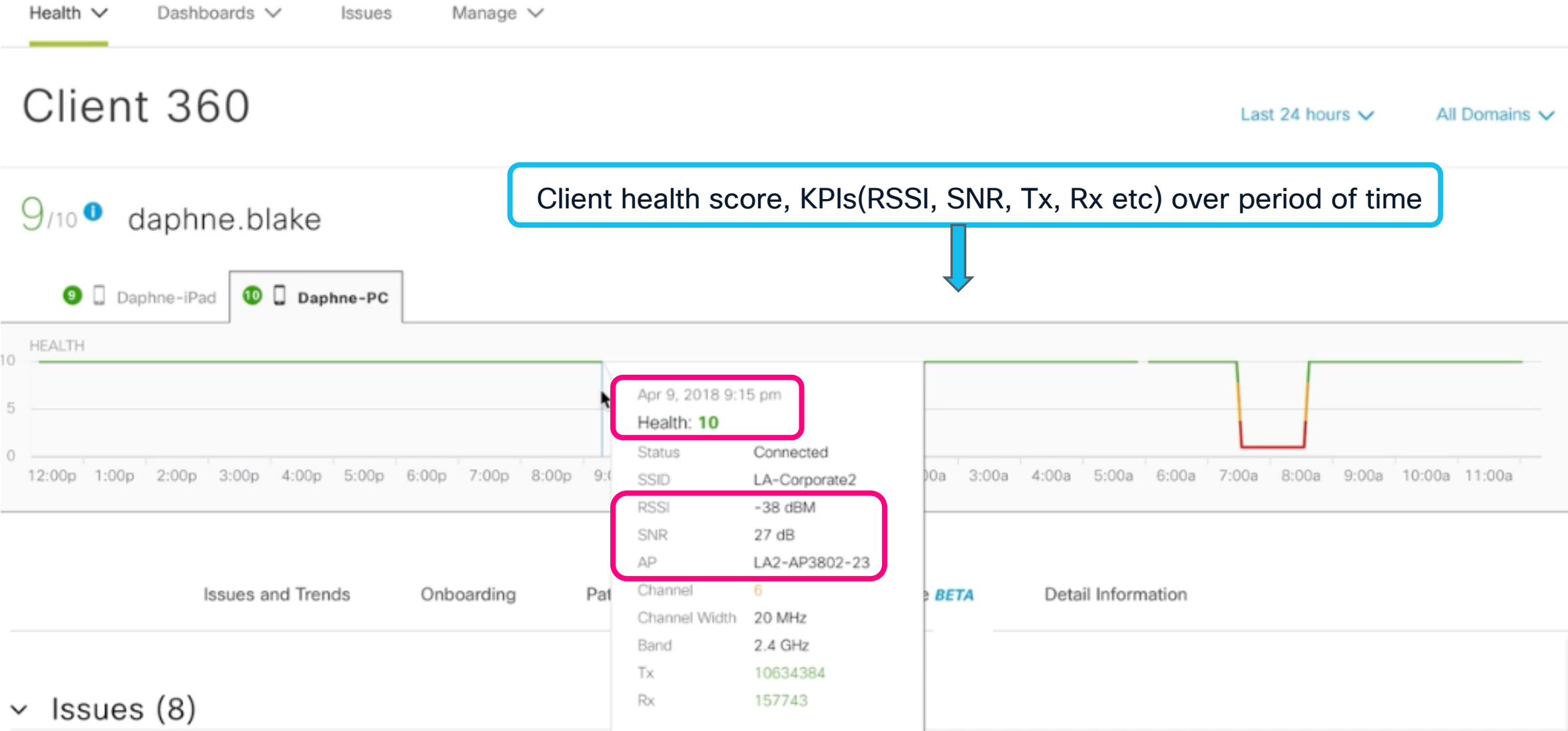
Catalyst Centre

- Leverage [CatC for 360](#) troubleshooting of networks and clients.
- Example : [Network Reasoner](#), [Reports](#), [Assurance](#)

Meraki Dashboard

- [Manage Catalyst Products](#) from Meraki Dashboard (Hybrid)
- Example : [AP Live Tools](#), [PCAPs](#), [WLC CLI & UI](#)

Client 360



Client health score, KPIs(RSSI, SNR, Tx, Rx etc) over period of time



Client 360 - Issues Insights



- Client A took longer to authenticate due to network delay.
- Network latency for Netflix application above 387ms.
- Client B connectivity issue due to RF at AP location B.

Issues (4)

Onboarding

Wireless client took a long time to connect (SSID: LA-Corporate2, AP: LA2-AP3802-23, Band: 2.4 GHz) - Excessive time for Authentication due to AAA server or Network delays

Total occurrences: 9

Application

Network Latency for Application 'netflix' is Above the Threshold Value of 387ms.

Total occurrences: 16

Application

Network Latency for Application 'disney-web-portal' is Above the Threshold Value of 262ms.

Total occurrences: 11

Onboarding

Wireless client took a long time to connect (SSID: LA-Corporate2, AP: LA2-AP3802-23, Band: 2.4 GHz, Site: Global/USA/SM/Level1) - Excessive time due to RF issues

Total occurrences: 4

Detailed insights of the issue

Wireless client took a long time to connect

Total occurrences: 9

Application

Network Latency for Application

Total occurrences: 16

Application

Network Latency for Application

Total occurrences: 11

Onboarding

Wireless client took a long time to connect

Total occurrences: 4

Status: Open

Description

This client is taking longer than expected time to connect to 'LA-Corporate2' SSID due to excessive authentication time.

- Onboarding took 36.4 seconds (expected time should be less than 10.0 seconds).
- Association took less than a second (expected time should be less than 2.0 seconds)
- Authentication and Key Exchange took 30.8 seconds (expected time should be less than 3.0 seconds)
- IP Addressing took 0 seconds (expected time should be less than 5.0 seconds)

Onboarding Transaction Log

EQ Find

Event	Reason	Date / Duration
> Failure	4 Way Key Timeout	5.55 sec
> Success		30.85 sec

Event

Reason

Failure

4 Way Key Timeout

Auth Start

PMK Cache Expired

Auth Done

dot1x Full Auth

L2Key Done

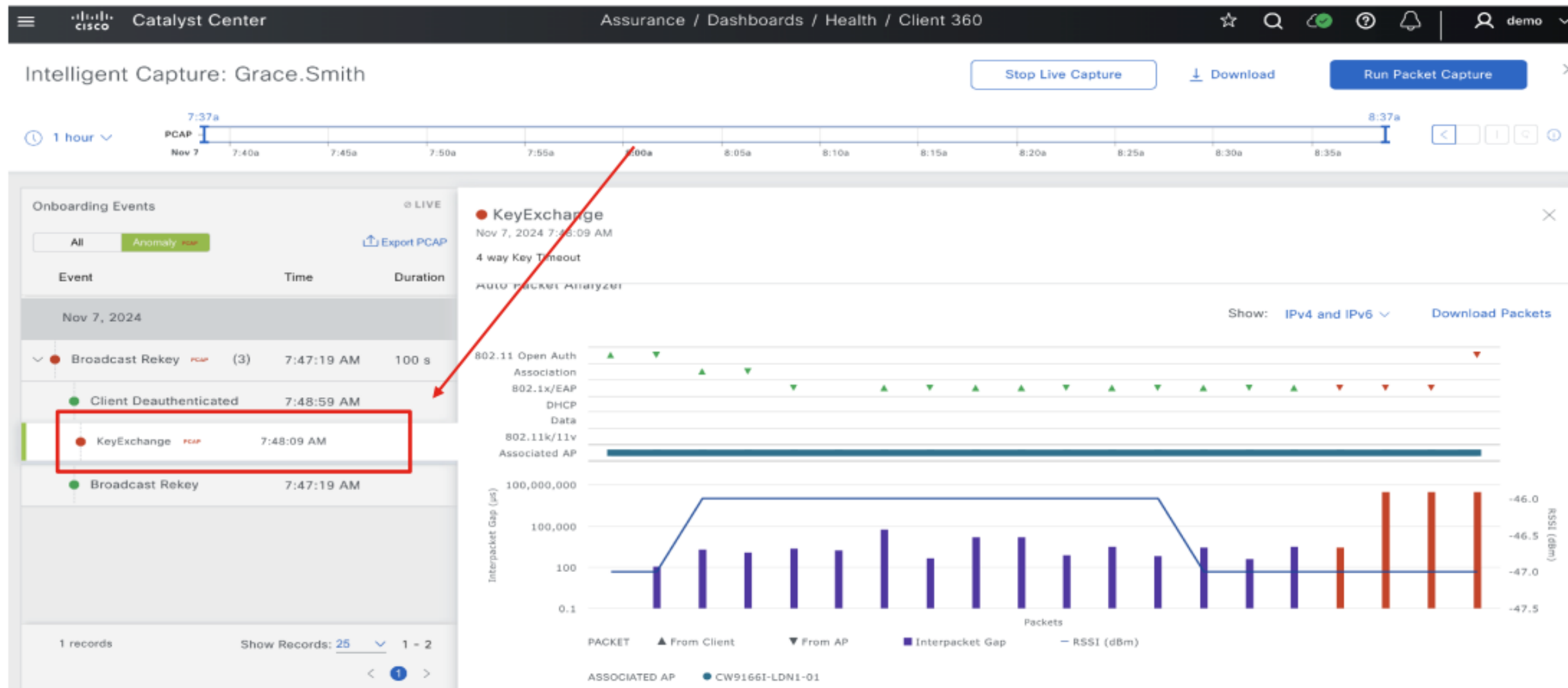
4 Way Key Timeout

Send Deauth

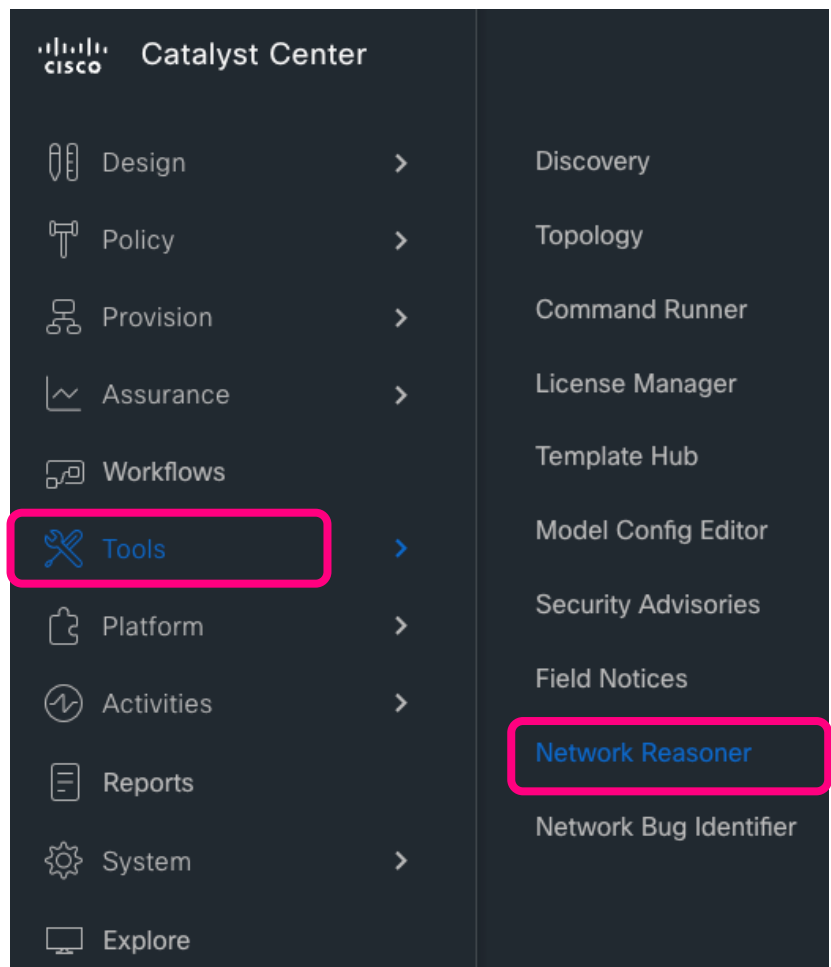
Failure due to - 4 way handshake key timeout



ICAP (Intelligent Capture) in Catalyst Center – Client 360



Network Reasoner



1

Wireless AP Data Collection

Collect show output, logs, and PCAP for an Access Point (AP) on its associated Catalyst 9800 WLC and via SSH to the AP for up to 30 minutes

Network Performance Impact: Medium

CX

2

Wireless Client Data Collection

Collect show output, logs, and PCAP for a Wireless Client on 1-2 Catalyst 9800 WLCs and up to 5 APs via SSH for up to 30 minutes

Network Performance Impact: Medium

CX

Running Machine Reasoning – AP Data Collection

Reasoner Inputs

Troubleshoot Duration (5-30 minutes)*

5

Two AP MAC address (A,B)*

a49b.cd5a.b160,a49b.cd47.f474

PCAP Interface

GigabitEthernet0

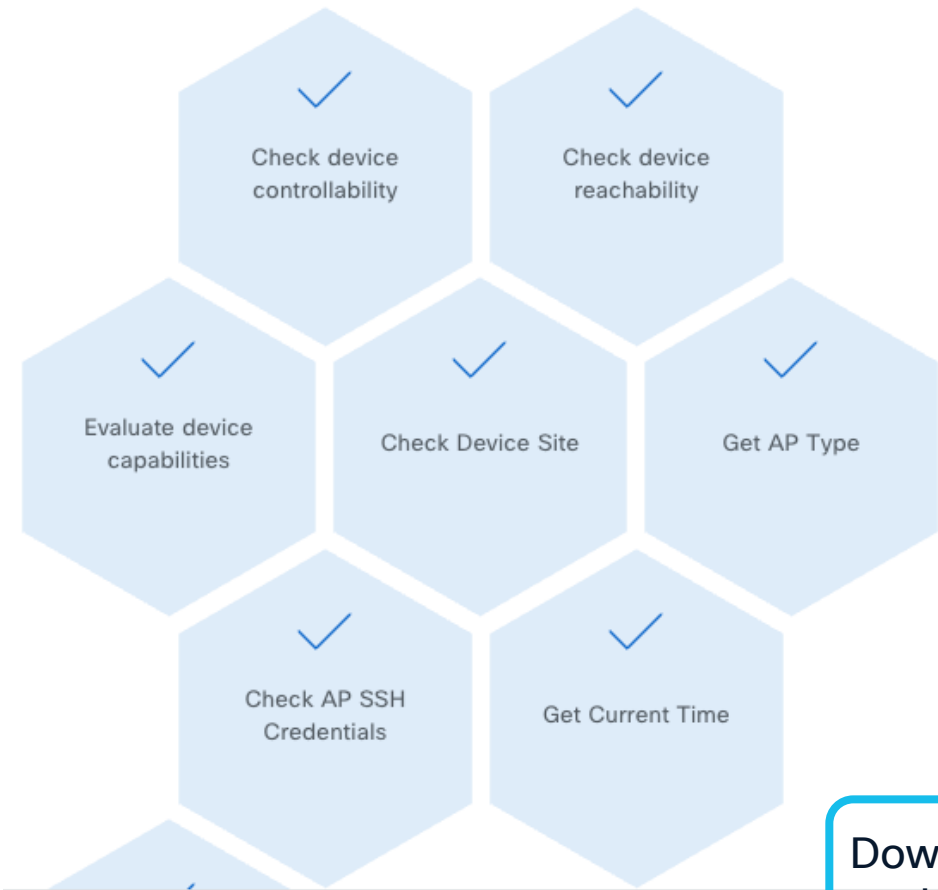
AP IP address*

10.107.79.18

AP Name*

9120AP

Run Machine Reasoning



Download the bundle

Reasoning Activity

Conclusions (1)



Download the command outputs file here: [cmd_output_9f7962c3-c54a-4a76-9642-05ddf0ca23ae.tar.gz](#)

[View Relevant Activities](#)

Network Reasoner Activity - Client

Network Reasoner / Wireless Client Data Collection



Detailed insights
of activities



Relevant Activity Details [Hide Details](#)

Check if the device f45a3cc3-d96c-46d1-a33d-7ecc147e6fe9 is provisioned or assigned to a site.

Sep 13, 2025 11:32:38 PM

Debug wireless mac

Sep 13, 2025 11:32:44 PM [View](#)

Get Current Time

Sep 13, 2025 11:32:44 PM

Starting Client PCAP session

mre_client_pcap_1757786564883 with filter ec63.d7fc.f729 on interface GigabitEthernet0

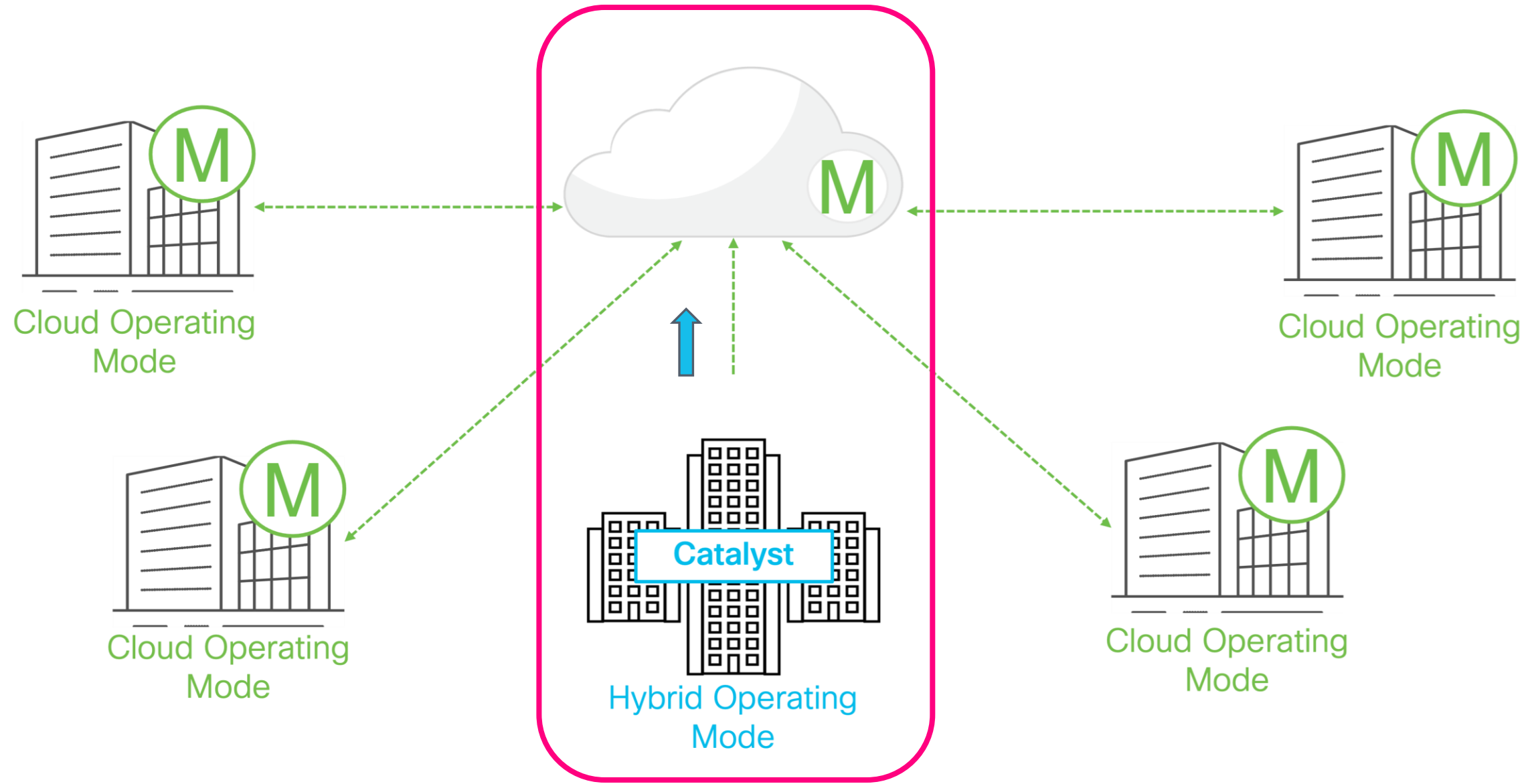
Sep 13, 2025 11:32:45 PM [View](#)

Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127.84.21 for filename: c9800-40-SJC.cisco.com-ec63.d7fc.f729-1757786555655.txt

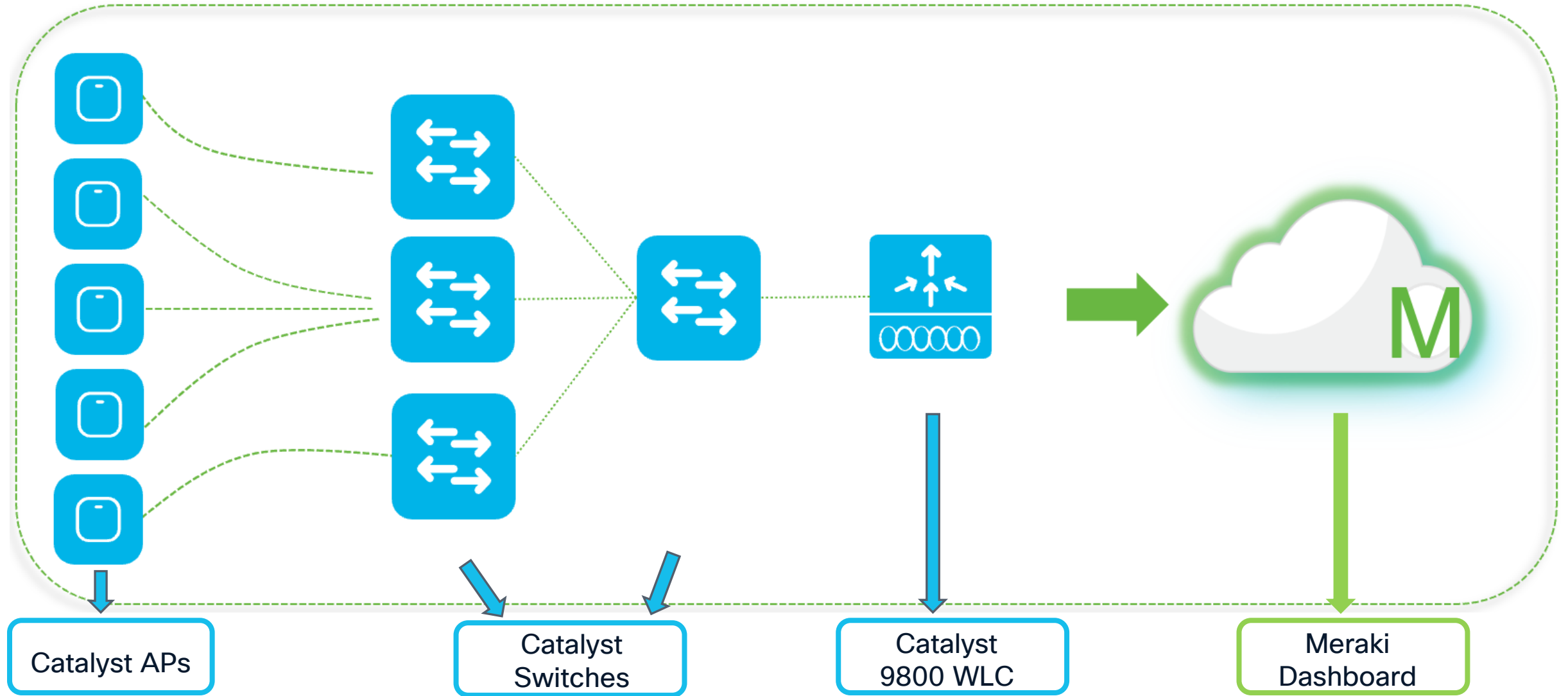
Meraki Dashboard for Catalyst Devices

- Cloud management - Catalyst devices
- Assurance and Packet Captures

Unified Architecture



Hybrid Operating Mode



Assurance in Meraki Dashboard

Alerts : AP stopped communicating with WLC

OverviewLast week

Network Calo141

Network-wide

Assurance

Wireless

Organization

Access ManagerNew

Network health score

Good

100/100

0 pts last week

Does the score feel right?

Learn about scores

Network health score on 100

Organization CiscoTAC

Two-factor Authentication is not currently enabled on your Meraki Dashboard account. For an extra layer of security, we recommend enabling it at yo

Alerts0Started last week

Alerts triggered over time

of alerts

2025-09-09 05:302025-09-10 05:302025-09-11 05:302025-09-12 05:302025-09-13 05:30

ActiveDismissedResolvedAlert Type

0Critical

Active alerts

Severity	Alert type
----------	------------

Alert Counts

2025-09-10 20:06 - 2025-09-11 00:17

Critical

Current Period 3

AP stopped communicating with WLC2

Unreachable device1

Previous Week 0

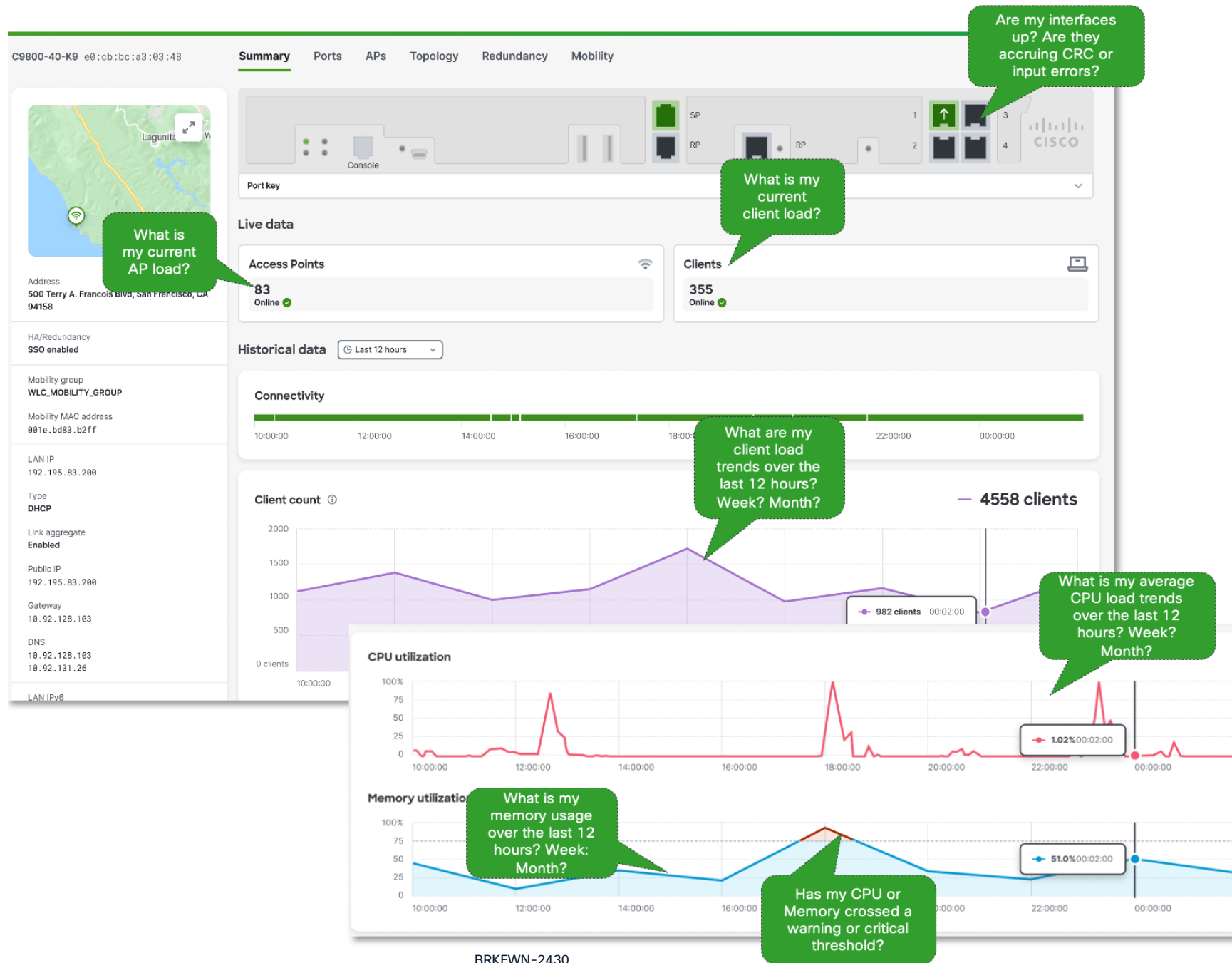
Warning

Current Period 1

SSH error connection1

Previous Week 0

WLC KPIs



KPIs Per AP

68:49:92:59:0a:a0 CW9164I



Summary

Performance for the last month

SSID: All SSIDs BAND: All bands

AP CW9164I Performance

Clients

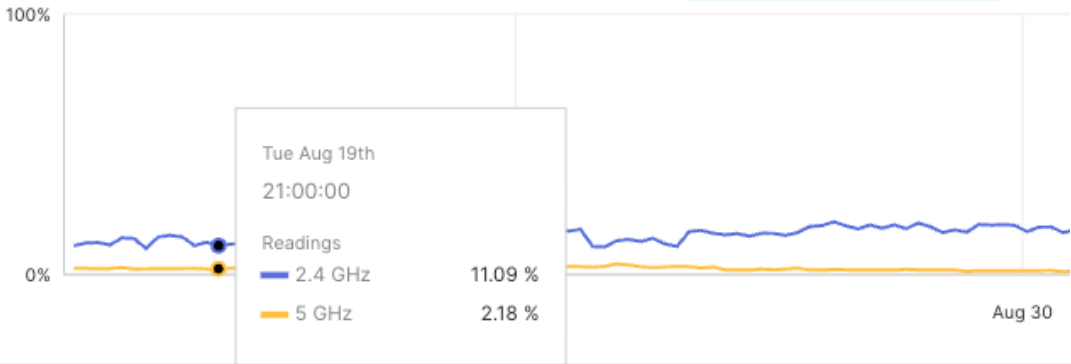
Number of clients on this AP on 21st Aug



Channel utilization

802.11 and interference

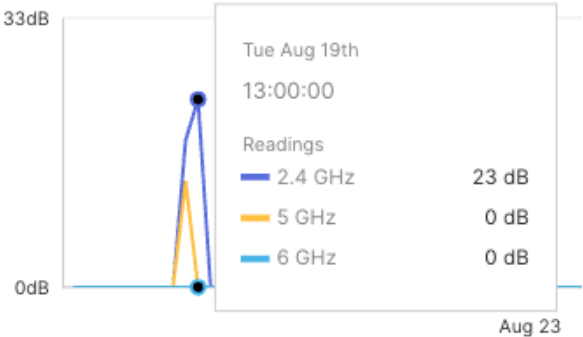
Channel util on both radios



Avg signal quality and latency in ms for all 3 radios

Average signal quality

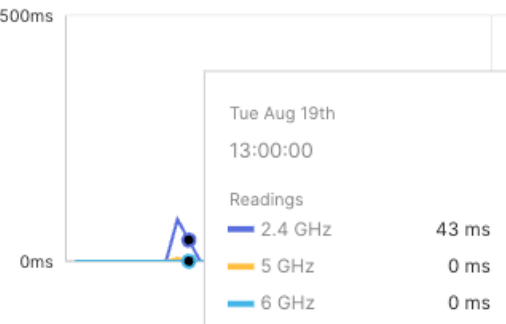
in SNR



Average wireless latency

All traffic

Slowest Clients



Data rates

All traffic

Data rates per radio in Mbps



KPIs Per AP

Utilization on current channels



Channel 11 (2.4 GHz)

Acceptable (25%)

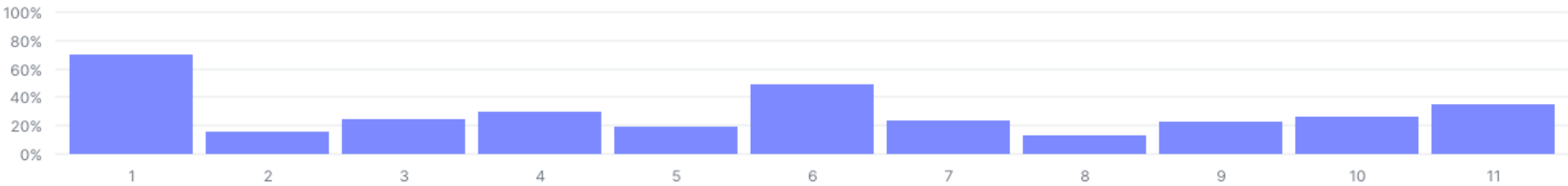


802.11 Utilization
across 2.4GHz

Utilization on all channels

2.4 GHz

802.11 Traffic



Historical device data

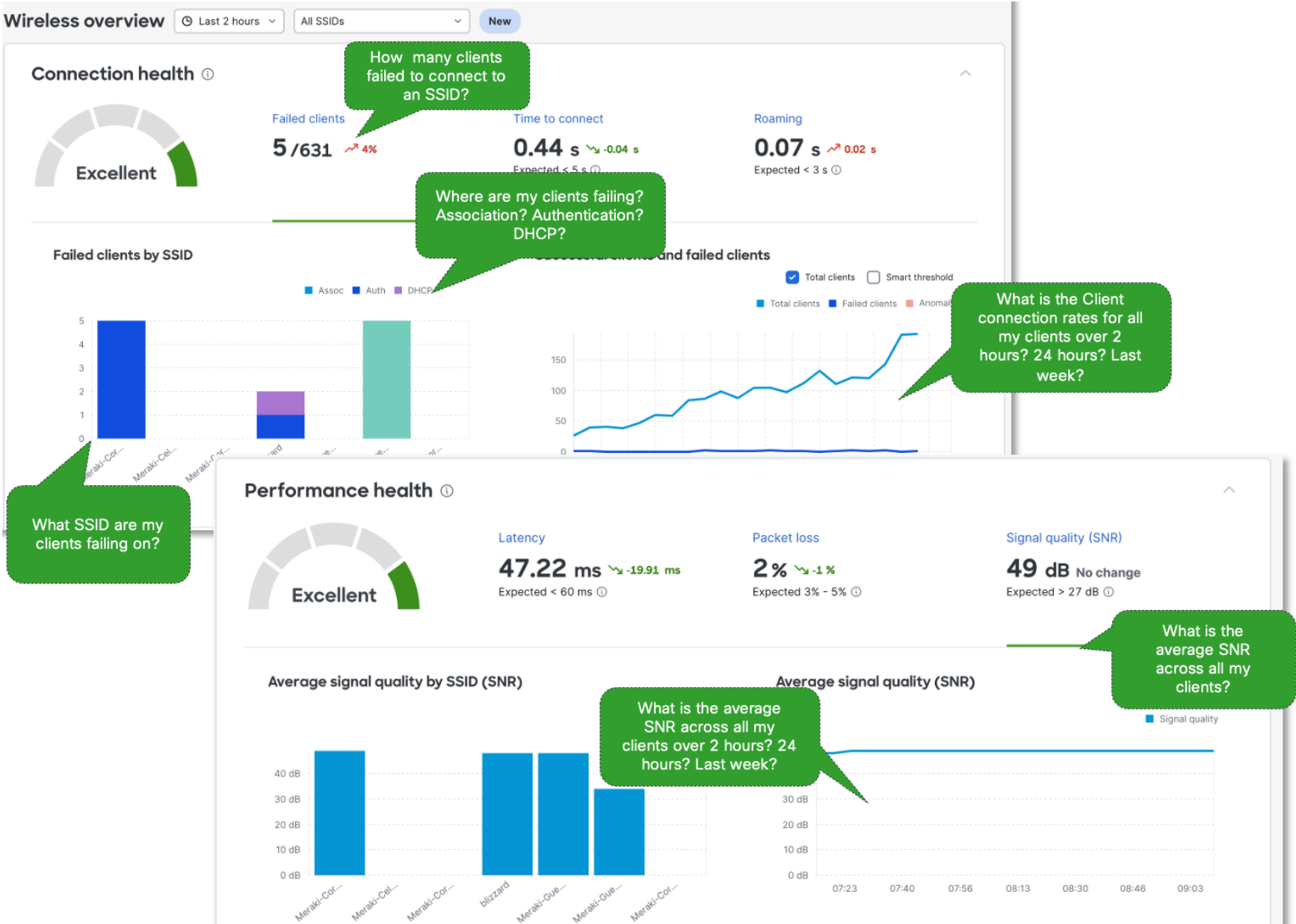
Last month

Historical clients

2 clients 40 KB

Description	Usage	IP Address	MAC Address
Samsung Galaxy S21	22 KB	192.168.1.16	62:ff:4e:16:30:12
Unknown Device	18 KB	—	06:fe:43:f4:12:10

Client KPIs



New Cloud CLI

Summary

Ports

Cloud CLI

APs

CLI terminal

Close terminal

Detach terminal

Welcome to the interactive CLI IOS XE terminal

Verifying your device configuration. Please wait...Done

You are in Configuration Mode

All configuration commands are logged as user madc@cisco.com

Establishing connection to your device. Please wait...

Connection established successfully

EEC-Aurora#sh ap summary

Number of APs: 2

CC = Country Code

RD = Regulatory Domain

AP Name

State

Location

Slots

AP Model

Odissi_AP_2

3

CW9164I-ROW

Automated show commands

Select command

Show CDP Details

Select port

TenGigabitEthernet0/0/0

Outputs CDP neighbor details on an interface

Run

Show CDP Details for Port num TenGigabitEthernet0/0/0

EEC-Aurora# show cdp neighbors TenGigabitEthernet 0/0/0 detail

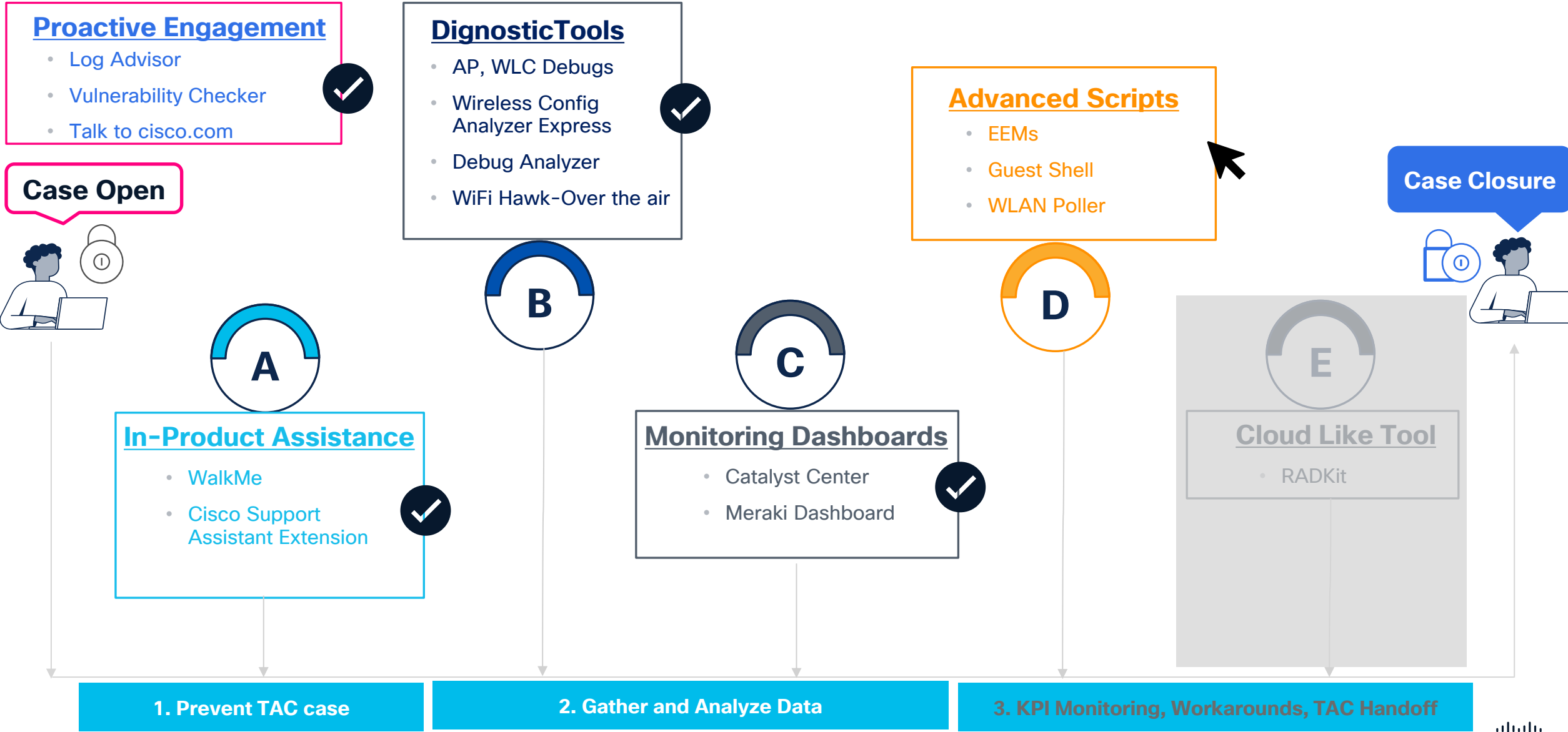
Device ID: Fusion-C9300-1.ciscolab.com

Session History

Start time (UTC)	Complete time (UTC)	User	Session type	Session log
Aug 12, 2025 12:15:46	Aug 12, 2025 12:15:50	MerakiSupport_leOA7d	Configuration	Download
Aug 12, 2025 12:15:34	Aug 12, 2025 12:16:17	MerakiSupport_leOA7d	Configuration	Download
Aug 12, 2025 11:55:08	Aug 12, 2025 11:58:55	MerakiSupport_leOA7d	Configuration	Download

Option D - Advanced Scripts

Flexible Options to Self-Serve & Accelerate Case Resolution



Option D : Advanced Scripts (KPI Monitoring/Workaround)



Scenario : KPI monitoring, Apply workarounds, Bulk data collection

EEMs

- Match condition and recover from tricky issues or prevent outages.
- Example : HA SSO failure recovery or AP radio shutdown

Guest Shell Scripts

- Host guest shell scripts for scheduled activities
- Example : KPI monitoring, rollover packet captures

WLAN Poller

- Bulk data collection or push workaround to APs and WLCs
- Ex : Flash corruption recovery, AP migration

EEM - Embedded Event Manager

- Available in switches/routers and now in 9800 WLCs, they are [trigger-based](#) TCL(Tool Command Language) scripts.
 - Match a [trigger](#) and [take an action](#) accordingly. [Ex : Apply workarounds](#) automatically
 - Automate [data-collection](#)
 - Combine outputs or create commands.
- Documentation:

General
Information



IOS-XE
EEM



Best
Practices



EEM Script : Example 1

Issue :

- WLC stuck in Standby recovery due to the ports going into **Remote fault**.
- **Reboot** of controller is **needed to recover** the device from remote fault/ recovery mode.

Challenge :

Manual intervention needed to identify the issue and reboot the WLC

EEM Solution :

EEM script to match remote fault and execute reload of WLC to recover without human intervention.

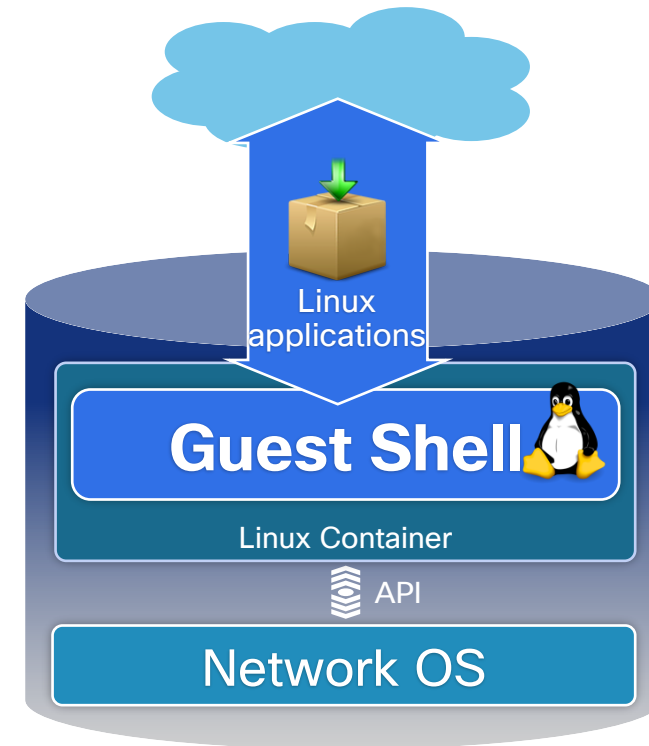
```
event manager applet AutoReload
event syslog pattern "Interface TenGigabitEthernet0/0/1, link down due to remote fault"
action 100 syslog msg "Reloading to recover from port in Remote fault"
action 101 reload
```

Guestshell

- Virtualized Linux-based environment, designed to run Python scripts for automated control and management.
- Python 3.6 supported from 17.1 onwards and is default after 17.3.1.
- Supported on 9800-40, 9800-80 or 9800-L running 16.12 or later (Not supported on 9800-CL or EWC APs)
- Enable guestshell in config.
- Copy python scripts in the /bootflash/guest-share folder

Guestshell Sample Scripts for following use cases:

- Efficient Client Troubleshooting
- Automated Archive request and export
- Continuous Embedded Packet Capture
- KPI Collector



How to setup Guestshell – KPI Collector

Reference & Script



Enable
Guestshell

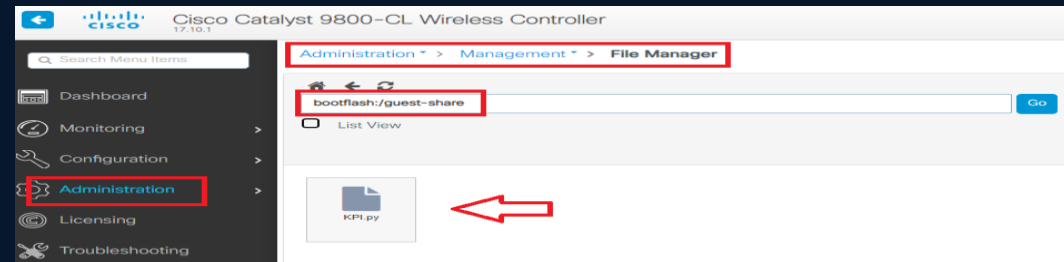


Copy Script to
9800



Execute script

```
conf t
iox
  app-hosting appid guestshell
  app-vnic management guest-interface 0
end
wr
```



```
Gladius1#guestshell run python3 /bootflash//guest-share/KPI.py
Starting datacollection
Exported files WLC-Sep-10-2025.txt to destination
tftp://192.168.0.45/wlc/
```

KPI Script

Actions done:

- Run a set of commands.
- Store info in a file.
- Can collect logs several times using for loop.

```
[guestshell@guestshell guest-share]$ cat KPI.py
```

```
import cli
```

```
import time
```

```
from datetime import datetime
```

```
#Configure tftp server and directory
```

```
dst="tftp://192.168.0.45/wlc/"
```

```
#List of commands
```

```
cmd_list=[
```

```
"sh ver | i uptime|Installation mode|Cisco IOS Software",
```

```
"sh redundancy | i ptime|Location|Current Software state",
```

```
"sh processes cpu platform sorted | i wncd",
```

```
"sh platform resources",
```

```
"show process memory platform sorted",
```

```
.....
```

```
"show wireless mobility sum",
```

```
"sh nmsp status"
```

```
]
```

Add the needed
commands

Combine Guestshell & EEM – Continuous PCAP Ex

- Combine EEM with Guestshell using EEM trigger-based scripts
- Create Scripts to automate data-collection
- Run script periodically or On-Demand

Script to capture continuous PCAP from WLC

```
event manager applet Continuous_packet_capture
event timer watchdog name timer time 120
action 0.5 cli command "enable"
action 1.0 cli command "guestshell run python3 /bootflash//guest-
share/Continuous_packet_capture.py"
```

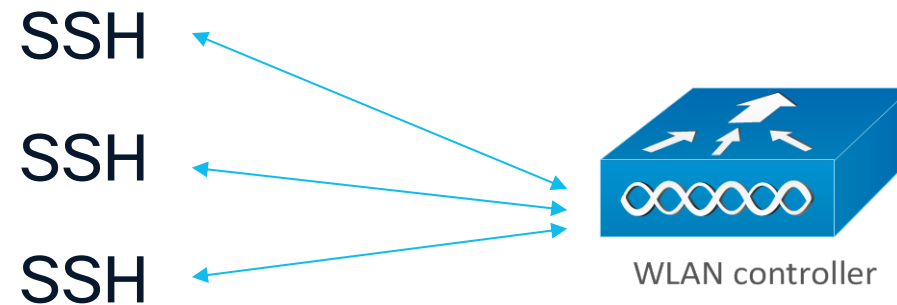
WLAN Poller

- Gather bulk data from AP/WLC

WLAN Poller – For AP Side Data Collection



- **Bulk data** collection from controllers and APs, **execute commands** on **regular intervals**. Ex : IOS AP Flash health check and recovery, AP Image download & AP Reload options
- Task automation against Controller/APs
- Python bundle: No install required
- Aggregate AP crashfiles (taken from WLC), radio events and coredumps (taken from APs) to a common TFTP repository



WLAN Poller GUI

WLAN Poller

WLAN Poller

General

* Indicates required fields

Wireless LAN Controller Information

* WLC Type:

AireOs

C9800

* IP Address:

10.104.172.194

Connection Mode

* WLC:

SSH

TELNET

AP:

SSH

TELNET

Credentials

WLC:

* Username:

Test

* Password:

••••••••

Enable Secret:

Please wait!

Connecting to the WLAN Controller 10.104.172.194...

Password:

Enable Secret:

Connect

WLAN Poller – GUI (Command List)

WLAN Poller Gui

WLAN Poller Config Wizard

Step1:Configure Device Details

Step2:Select Feature/s

WLC Operations

CustomTemplate

Enter 9800 Custom CLI cmd list in the text editor below.

WLC Custom Cli list

show ap summary

show ap uptime

show version | i 17.

show clock

SAVE

AP Operations

Enter AP CLI cmd list in the text editor below.

AP Custom Cli list

show clock

show inventory

show version | i ptime

show capwap client rcb | i Mgr

capwap ap primary-base pbglad 9.12.88.30

%confirm% test capwap restart

REVIEW

EXECUTE

Launch Wlan Poller & proceed to Monitor Page.

START WLANPOLLER

BACK

Check Summary and Download

Wlanpoller
GUI: 0.6, Engine:0.22

Summary
Status
Wlanpoller Logs

WLC Summary



Profile: WLC & AP Operations IP: 10.104.172.100 User: Test

Controller Information	
Model	C9800-80-K9
Version	FXS2200
System Name	9800-1
Ip Address	10.104.172.100
Uptime	21 hours, 24 minutes
AP Count	1
Client Count	0

WLAN Poller Gui
Wlanpoller
GUI: 0.6, Engine:0.22

Summary
Status
Wlanpoller Logs
Poller Logs
Data Logs

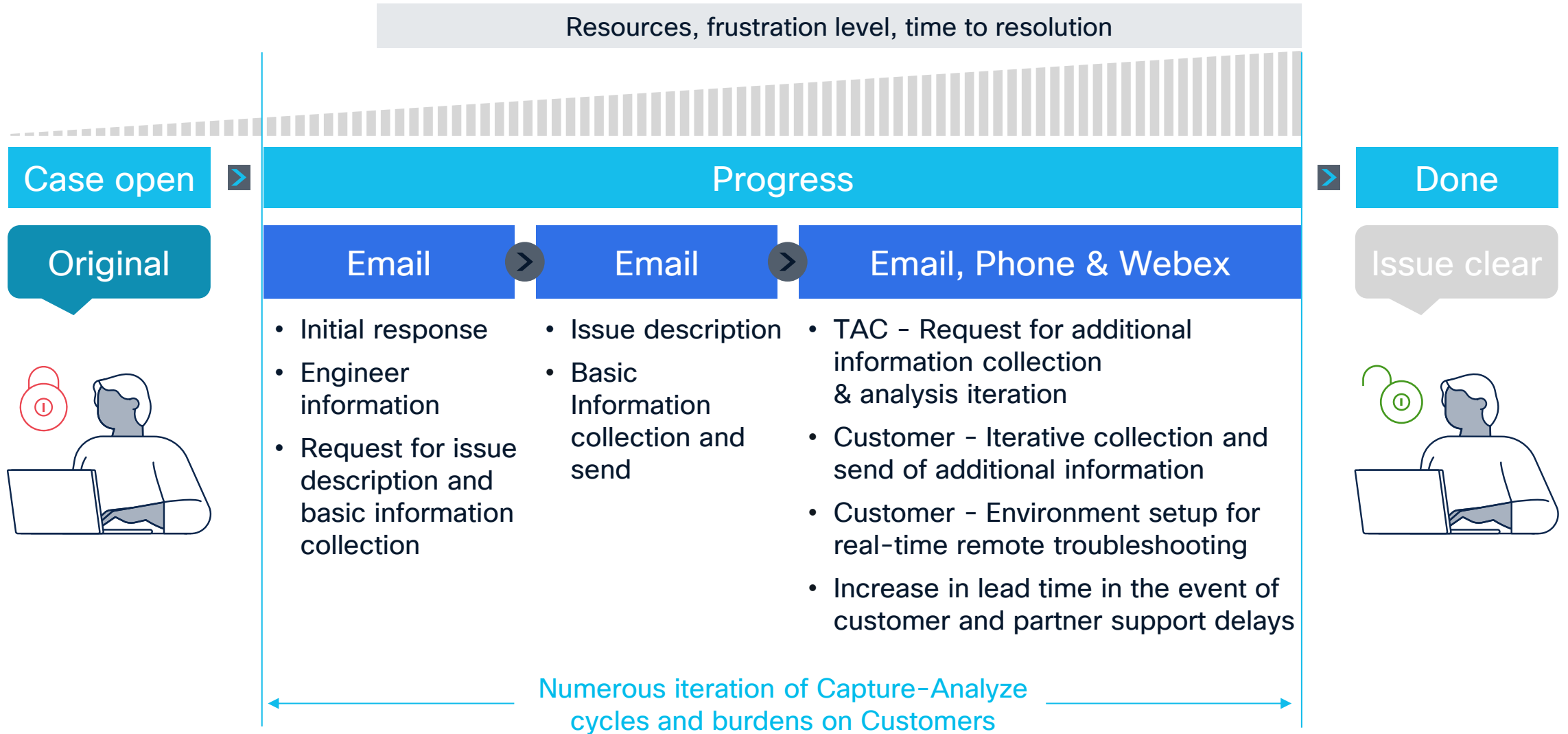
WLAN POLLER run complete, please check below Data logs.

DOWNLOAD

- Check summary & status
- Download logs

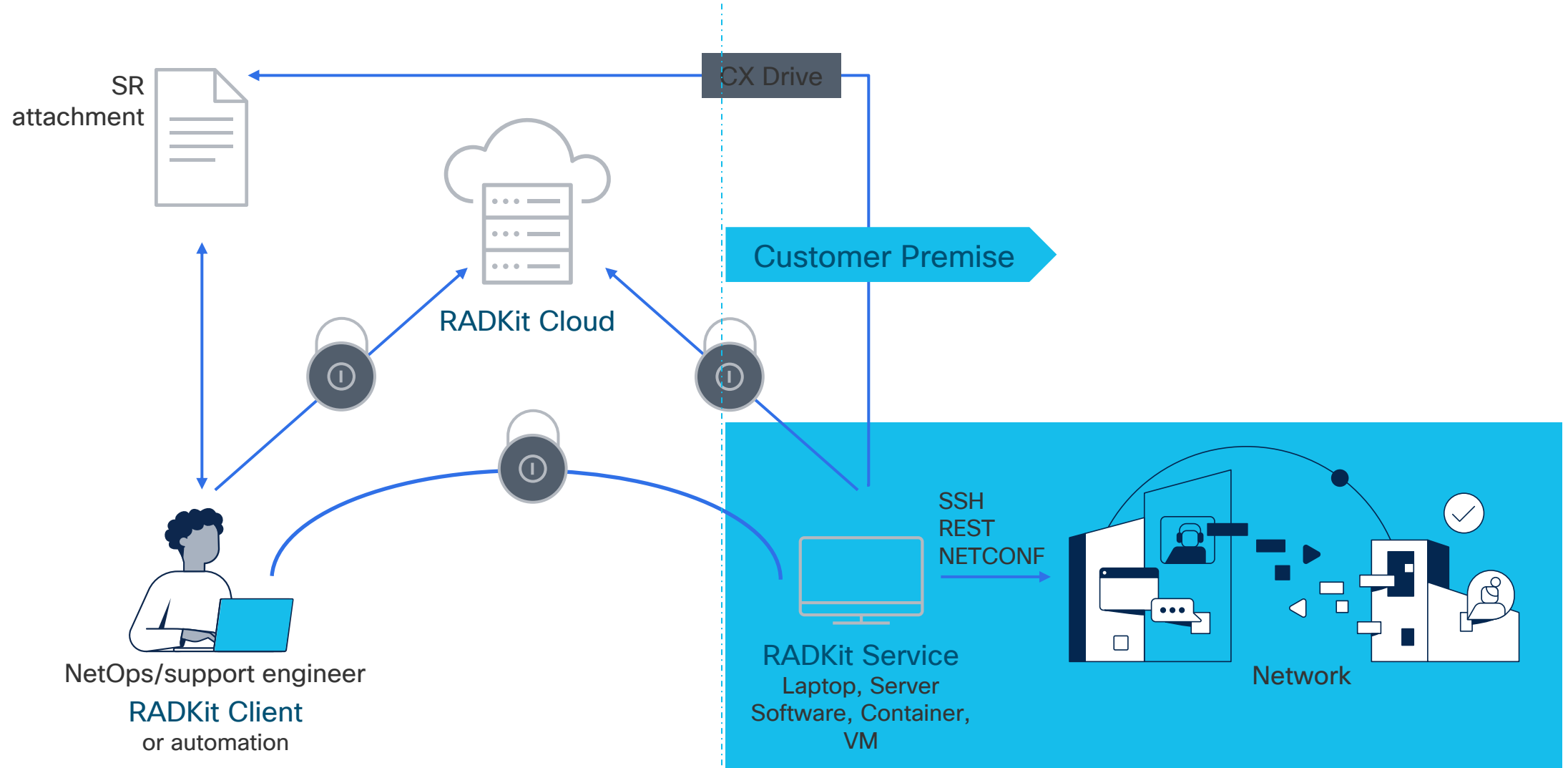
E - RADKit

Current troubleshooting method



RADKit accelerates case resolution

More info at radkit.cisco.com



RADKit Security & Capabilities

More at radkit.cisco.com – FAQ section

- RADKit is CSDL compliant, meets all stringent security, and data privacy criterias
- All data is [encrypted at rest and in-transit](#). End to end encryption. [Remote procedure call \(RPC\) over TLS1.3](#)
- RADKit [does not store](#) any user data in the cloud. All [data remains the customer property](#).
- Only customer [authorized users](#) can connect
- Capabilities :
 - Exec data collection
 - Interactive CLI troubleshooting
 - GUI Live troubleshooting
 - SR file attachment

Customer View : RADKit Service Inventory

All
Devices

← → ↻

Not secure | https://localhost:8081

🔖 ☆ 🏠 👤 ⋮

Remote Automation Development Kit
Cisco RADKit Service

Domain: PROD Service ID: Igno-8tqf-gz5d

📄 5

RBAC DISABLED

CONNECTED

⚙️

📶

Connectivity

📱

Devices

👤

Remote Users

⚙️

Admin Users

🏷️

RBAC Labels

🖥️

Monitoring

?

Help

+ Add Device

📧

🔍

🗑️

0 🛒 Edit Cart

+ 🛒

- 🛒

× 🛒

🔍 Search

☐	Active	Device Name	Hostname or IP Address	Device Type	In cart	Description	Labels	Actions
☐	☒	en-dnac		CiscoDNACenter		Enterprise DNAC		🔗 🗑️ ⋮
☐	☒	c9800-40-1-sda-com		IOS		Imported from: en-dnac		🔗 🗑️ ↻
☐	☒	c9800-40-2-sda-com		IOS		Imported from: en-dnac		🔗 🗑️ ↻
☐	☒	fusion-c9300-1-cisco-com		IOS		Imported from: en-dnac		🔗 🗑️ ↻
☐	☒	mum-bdr1-sda-com		IOS		Imported from: en-dnac		🔗 🗑️ ↻
☐	☒	mum-bdr2-sda-com		IOS		Imported from: en-dnac		🔗 🗑️ ↻
☐	☒	mum-edge1-ap1		UNKNOWN		Imported from: en-dnac		🔗 🗑️ ↻
☐	☒	mum-edge1-sda-com		IOS		Imported from: en-dnac		🔗 🗑️ ↻
☐	☒	mum-edge2-ap1		UNKNOWN		Imported from: en-dnac		🔗 🗑️ ↻
☐	☒	mum-edge2-sda-com		IOS		Imported from: en-dnac		🔗 🗑️ ↻
☐	☒	pun-bdr1-sda-com		IOS		Imported from: en-dnac		🔗 🗑️ ↻
☐	☒	pun-bdr2-sda-com		IOS		Imported from: en-dnac		🔗 🗑️ ↻
☐	☒	pune-edge1-ap1		UNKNOWN		Imported from: en-dnac		🔗 🗑️ ↻
☐	☒	pune-edge1-sda-com		IOS		Imported from: en-dnac		🔗 🗑️ ↻
☐	☒	pune-edge2-ap1		UNKNOWN		Imported from: en-dnac		🔗 🗑️ ↻
☐	☒	pune-edge2-sda-com		IOS		Imported from: en-dnac		🔗 🗑️ ↻
☐	☒	pun-in1-sda-com		IOS		Imported from: en-dnac		🔗 🗑️ ↻
☐	☒	pun-in2-sda-com		IOS		Imported from: en-dnac		🔗 🗑️ ↻

Showing 1 to 18 of 18 entries. | Selected: 0.

Page size: 15 | 25 | 50 | 100 | 250

RADKit Users & Session Logs

localhost

RADKit

+

🔍 | ...

⏪ ⏩ ↺

⚠ Not secure | https://localhost:8081/users

🔗 ☆ 🖨 👤 ⋮

Remote Automation Development Kit

Cisco RADKit Service

Domain: PROD Service ID: Igno-8tqf-gz5d 📄

5

RBAC DISABLED

CONNECTED 📶

⚙ ▾

📶

Connectivity

📶

Devices

👤

Remote

+ Add User

☑

⊗

🗑

TAC Engineer

🔍 Search ?

☐	Active	Remaining Time	User Email	Full Name	Description	Labels	Actions
☐	☒	Never expires	ag2@cisco.com	Anand G	RADKit Engineer		🔗 🗑
☐	☒	Never expires	madc@cisco.com	Madhuri		③ Router Switch Wireless	🔗 🗑
☐	☒	Never expires	maib@cisco.com				🔗 🗑

Remote Automation Development Kit

Cisco RADKit Service

Domain: PROD Service ID: Igno-8tqf-gz5d 📄

📶

Connectivity

📶

Devices

👤

Remote Users

⚙

Admin Users

/ session-logs

Search...

0 directories and 672 files.

Filename	Date
..	
20240205-085646-SSH-pune-edge2-sda-com.log	2/5/2024, 8:57:52 AM
20240205-085647-SSH-eec-oddisi-demo-2.log	2/5/2024, 8:57:58 AM
20240205-085647-SSH-mum-edge2-sda-com.log	2/5/2024, 8:56:47 AM
20240205-085647-SSH-pun-in2-sda-com.log	2/5/2024, 8:57:52 AM
20240205-085647-SSH-vmanage.log	2/5/2024, 8:57:51 AM
20240205-085701-SSH-ccc8800-ula-log	2/5/2024, 9:07:05 AM

Sessions logs in RADKit Service

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKEWN-2430

CISCO

Cisco Confidential

Session logs accessed by
TAC can we viewed



© 2025 Cisco and/or its affiliates. All rights reserved.

TAC View : Inventory and Device Login

RADKit Network Console

[madc@lgn0-8tqf-gz5d] 696976857> show inventory

<radkit_client.sync.device.DeviceDict object at 0x23b1d4ad1f0>

name	host	device_type	Terminal	Netconf	SNMP	Swagger	HTTP	description	failed
c9800-40-1-sda-com		IOS_XE	True	False	False	False	False	Imported from: en-dnac	False
c9800-40-2-sda-com		IOS_XE	True	False	False	False	True	Imported from: en-dnac	False
eec-oddisi-demo-2		IOS_XE	True	False	False	False	False		False
eec9800wlc		IOS_XE	True	False	False	False	True		False
en-dnac		CISCO_DNA_CENTER	False	False	False	False	True	Enterprise DNAC	False
fusion-c9300-1-cisco-com		IOS_XE	True	False	False	False	False	Imported from: en-dnac	False
mum-bdr1-sda-com		IOS_XE	True	False	False	False	False	Imported from: en-dnac	False
mum-bdr2-sda-com		IOS_XE	True	False	False	False	False	Imported from: en-dnac	False
mum-edge1-ap1		GENERIC	True	False	False	False	False	Imported from: en-dnac	False
mum-edge1-sda-com		IOS_XE	True	False	False	False	False	Imported from: en-dnac	False
mum-edge2-ap1		GENERIC	True	False	False	False	False	Imported from: en-dnac	False
mum-edge2-sda-com		IOS_XE	True	False	False	False	False	Imported from: en-dnac	False
pun-bdr1-sda-com		IOS_XE	True	False	False	False	False	Imported from: en-dnac	False
pun-bdr2-sda-com		IOS_XE	True	False	False	False	False	Imported from: en-dnac	False
pun-in1-sda-com		IOS_XE	True	False	False	False	False	Imported from: en-dnac	False
pun-in2-sda-com		IOS_XE	True	False	False	False	False	Imported from: en-dnac	False
pune-edge1-ap1		GENERIC	True	False	False	False	False	Imported from: en-dnac	False
pune-edge1-sda-com		IOS_XE	True	False	False	False	False	Imported from: en-dnac	False
pune-edge2-ap1		GENERIC	True	False	False	False	False	Imported from: en-dnac	False
pune-edge2-sda-com		IOS_XE	True	False	False	False	False	Imported from: en-dnac	False
vmanage		VMANAGE	True	False	False	False	True		False

Untouched inventory from service lgn0-8tqf-gz5d.

[madc@lgn0-8tqf-gz5d] 696976857>

[madc@lgn0-8tqf-gz5d] 696976857>

[madc@lgn0-8tqf-gz5d] 696976857> interactive c9800-40-2-sda-com

Attaching to c9800-40-2-sda-com ...

Type: ~, to detach.

~? for other shortcuts.

When using nested SSH sessions, add an extra ~ per level of nesting.

Warning: all sessions are logged. Never type passwords or other secrets, except at an echo-less password prompt.

C9800-40-2#

C9800-40-2#

C9800-40-2#

C9800-40-2#

C9800-40-2#sh version

Cisco IOS_XE Software, Version 17.09.03

Cisco IOS Software [Cupertino], C9800 Software (C9800_IOSXE-K9), Version 17.9.3, RELEASE SOFTWARE (fc6)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2023 by Cisco Systems, Inc.

Compiled Tue 14-Mar-23 18:14 by mcpre

Login to device

Execute commands

RADKit Console – Upload to SR

Auto uploads session logs to SR

RADKit Network Console

```
> login madc@cisco.com
```

```
Logging in as: madc@cisco.com on domain PROD
```

```
A browser window was opened to continue the authentication process. Please follow the instructions there.
```

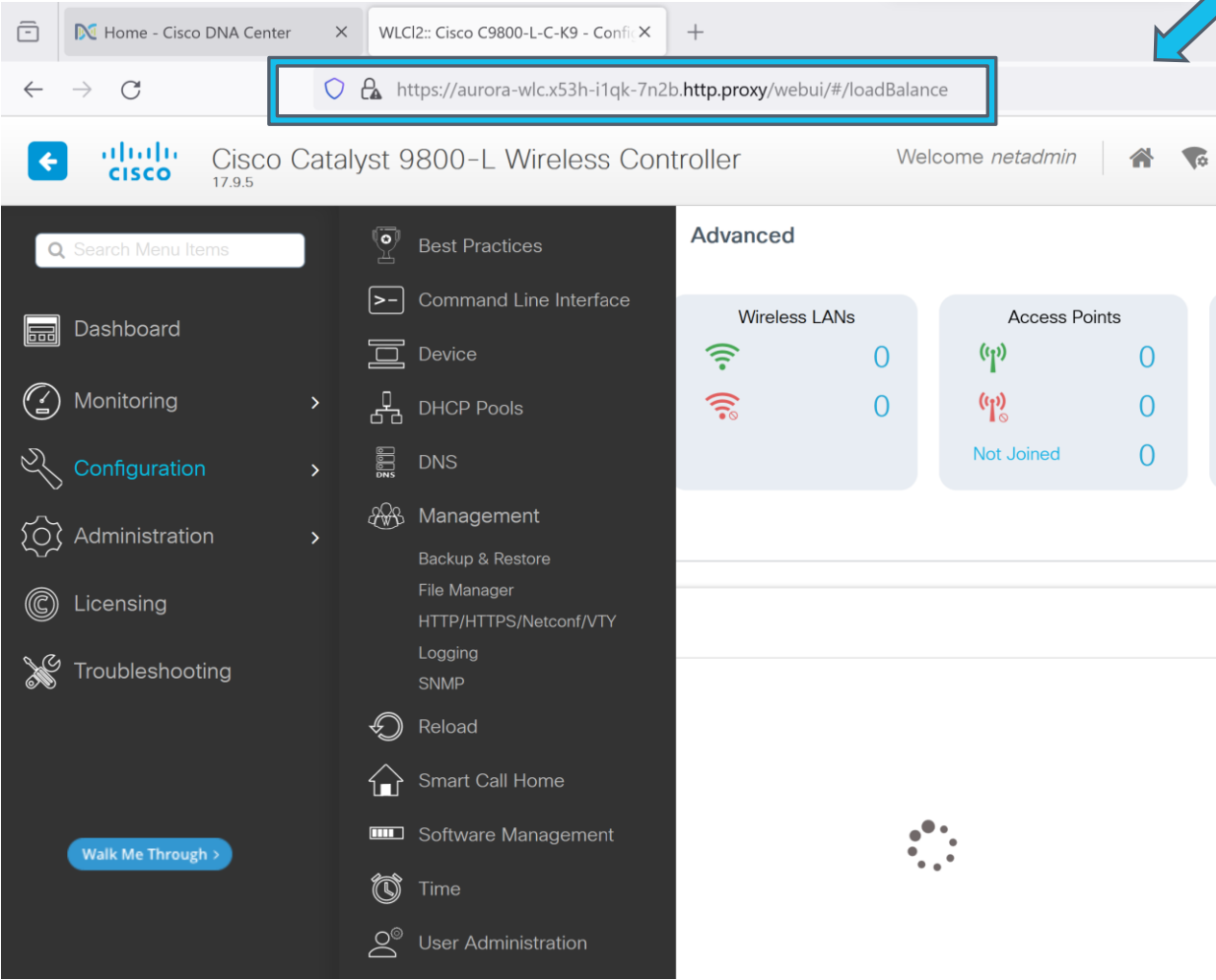
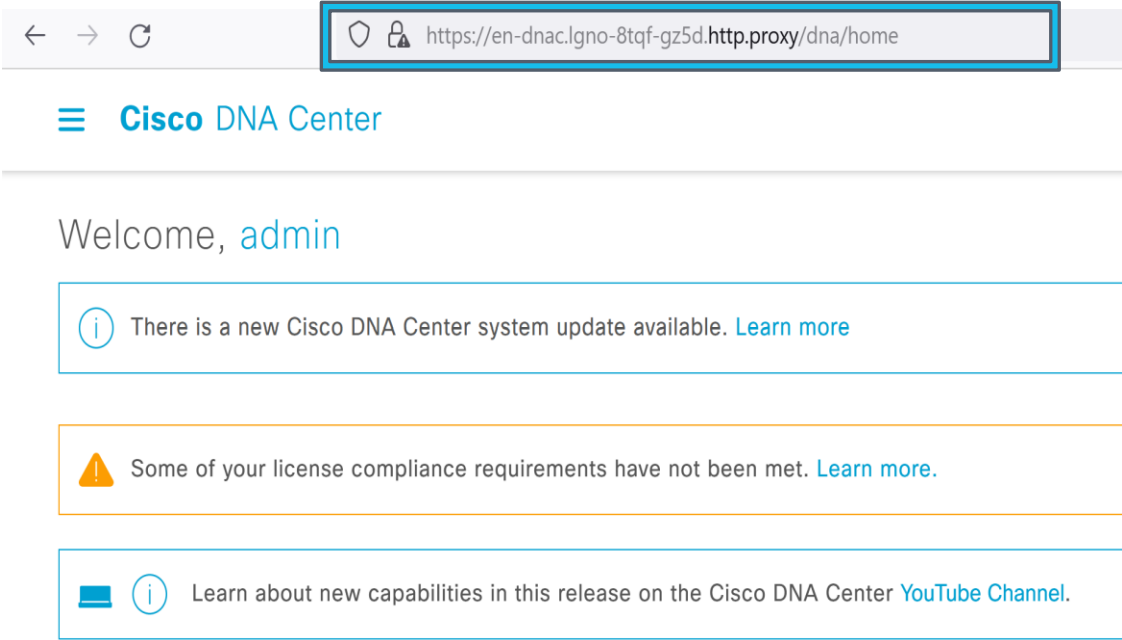
```
Authentication result received.
```

```
[madc] > service lgn0-8tqf-gz5d sr 696976857 auto_upload
```

```
Connecting to Service: lgn0-8tqf-gz5d in context of SR 696976857 with automatic log upload
```

Passwordless GUI Login

Proxy in the URL



Benefits of RADKit



On call time : No or minimal on call/webex time



Data Collection Ownership: Ownership of data collection with TAC



File Upload : File uploaded to TAC case automatically via Radkit without delay



Reduced Email Exchange : No back and forth emails for additional data collection



Faster Resolution : Reduces meeting conflicts delay and Timezone challenges between TAC & Customers

RADKit Success Story – A Sample

Problem

- A bug triggered during specific condition of channel and power changes together triggered via RRM on 9166 APs would have N/A as country code(Regulatory Domain), resulting in [CAPWAP resets](#) impacting random 100s of APs out of ~1800 APs.

Challenge

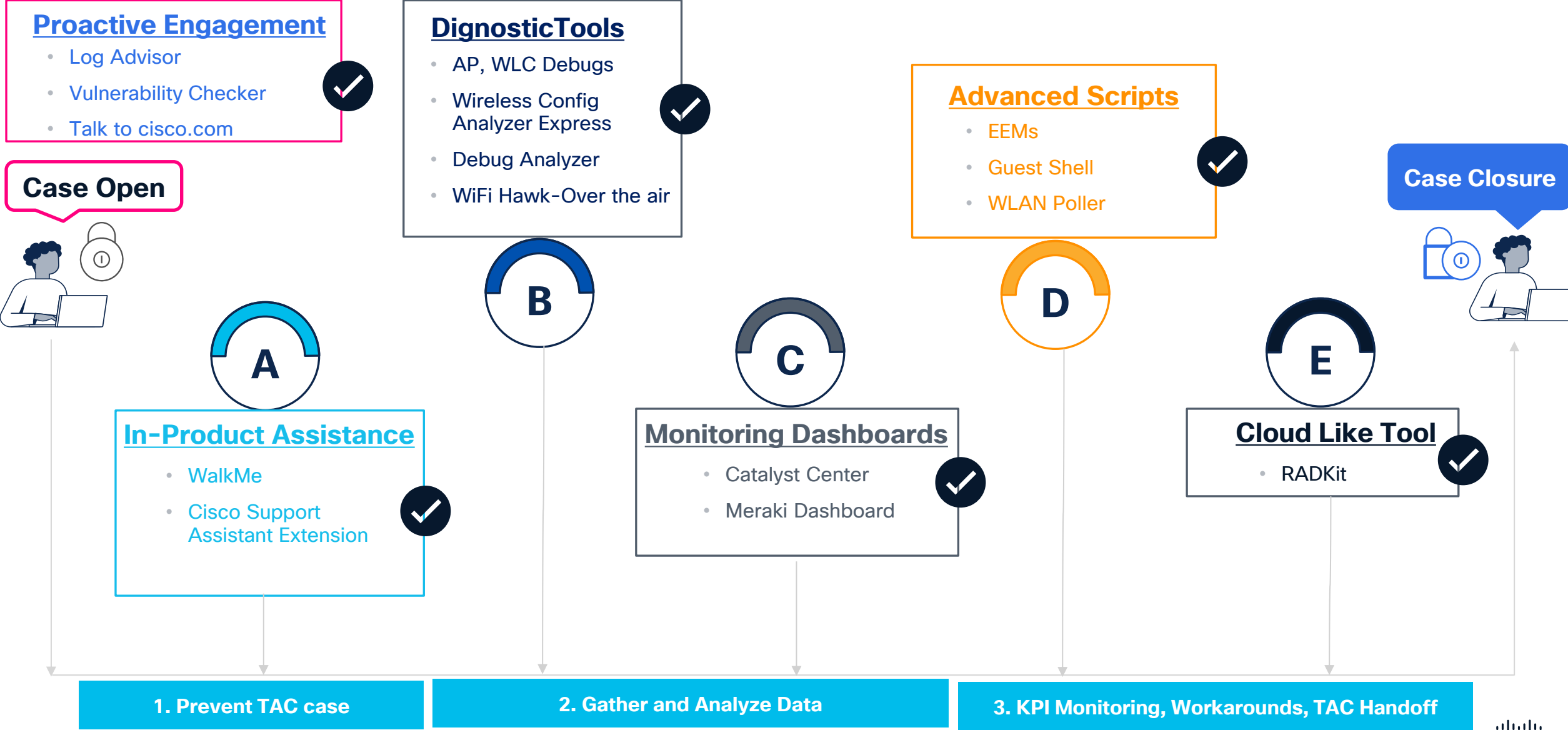
- [Identify](#) the impacted AP radios out of 1800 APs.
- [Recover](#) the AP radio by manually entering the [devshell](#)/present challenge of each AP, remove the config/wireless file, and reboot the AP.

How did RADKit help

- [Identification Script](#) : To run “show controllers dot11radio 0 | in country”, match for regex ‘NA’ and write the AP names to a text file.
- [Recovery Script](#) : To login to every AP that is in affected.txt file, get into devshell prompt, present challenge, perform recovery by re-building config file

This saved [100+](#) hours together for TAC and customer

Flexible Options to Self-Serve & Accelerate Case Resolution



Cisco AI Assistant for Support

How to **escalate** a technical support case

If you have opened a service request and are not satisfied with the progress, use the following procedure to escalate and connect directly to a resolution owner



- ▶ Escalate using **Cisco AI Assistant for Support** at <https://supportassistant.cisco.com/escalate>, via Webex App, on [Support Case Manager](#) or Virtual Spaces
- ▶ Enter case number
- ▶ Provide escalation reason
- ▶ Choose “Escalate to TAC Manager”
- ▶ Provide phone number for S1/S2 case or email address for S3/4 case

Severity Definitions

Severity 1

Critical impact on business operations. Cisco hardware, software, or as-a-service product is down.

Severity 2

Substantial impact on business operations. Cisco hardware, software, or as-a-service product is degraded.

Severity 3

Minimal impact on business operations. Cisco hardware, software or as a service product is partially degraded.

Severity 4

No impact on business operations. Features, implementation, or configuration assistance.

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a CiscoLive T-Shirt.



Earn 800 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

The background of the slide is an abstract design featuring flowing, wavy lines in various shades of blue and white. A large, solid white rectangular box is positioned on the left side of the slide, serving as a backdrop for the main text.

Thank You

