

The Cisco Live! logo features the word "CISCO" in a dark blue, sans-serif font, followed by "Live!" in a dark blue, cursive script font. The background of the entire image is a vibrant, multi-colored abstract pattern of overlapping, wavy lines and geometric shapes, transitioning from dark blue on the left to bright yellow and white in the center, and then to various shades of blue and green on the right.

CISCO *Live!*

Let's go



The bridge to possible

Cisco Wireless supercharged by Catalyst Center

The Ultimate Guide to Bring Your Wireless Operation
to the Next Level

Ignacio Fité, Solutions Engineer

CISCO *Live!*

BRKEWN-2667


Agenda


- Introduction
- Get insights with AIOps
- Operate efficiently with NetOps
- Expand usage with DevOps
- Conclusion

About me

Ignacio Fité



 Solutions Engineer – Ent. Networking

 5 years experience
with Cisco gear

 Network Management Focus

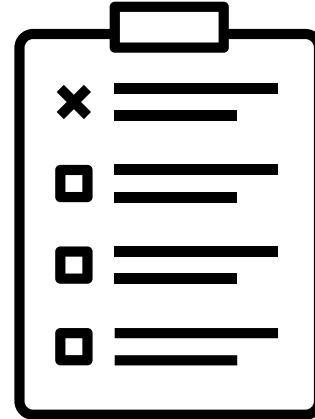


Agenda

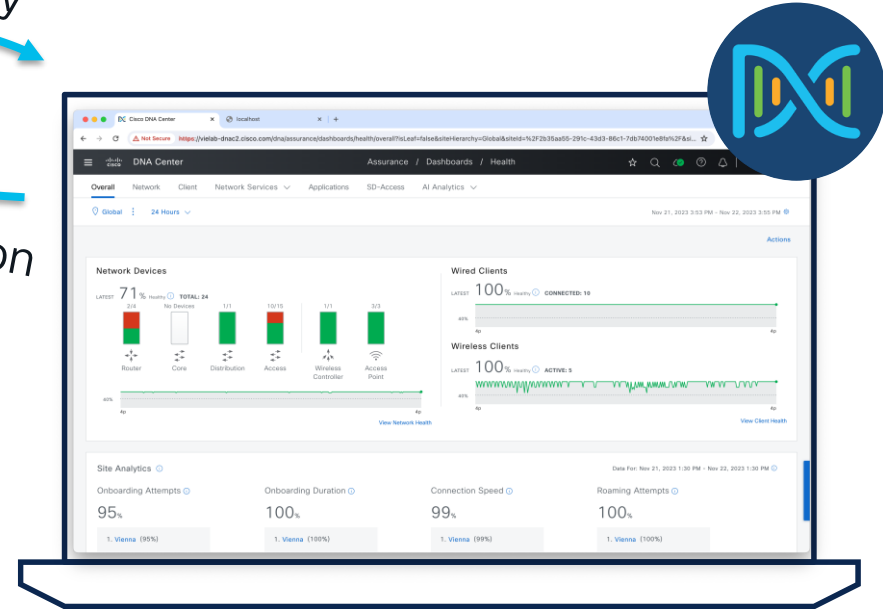
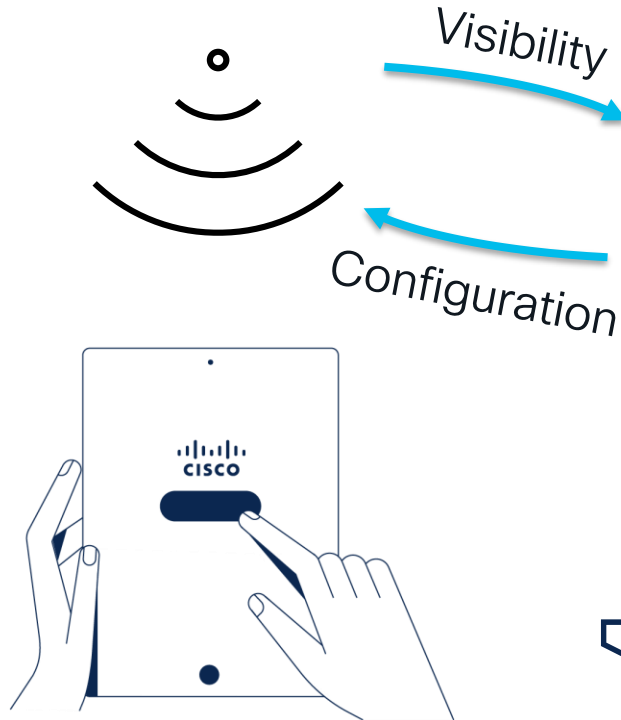
CISCO *Live!*

- Introduction
- Get insights with AIOps
- Operate efficiently with NetOps
- Expand usage with DevOps
- Conclusion

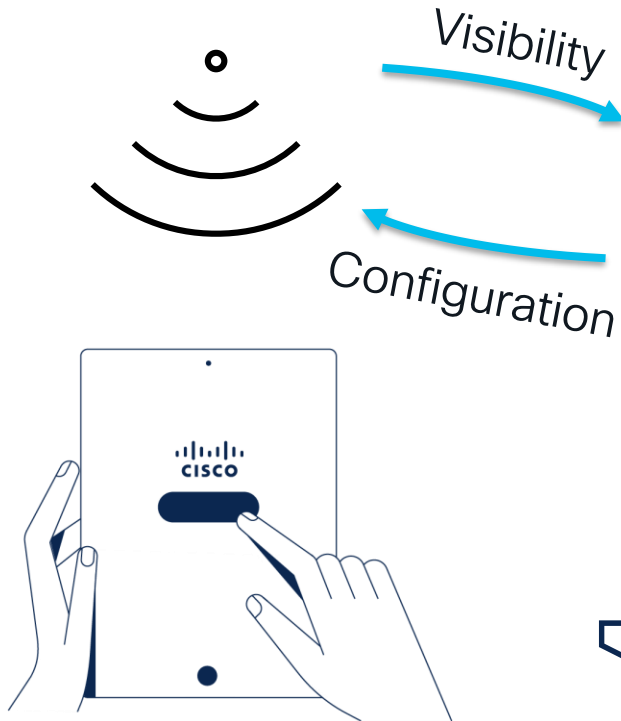
Why this session?



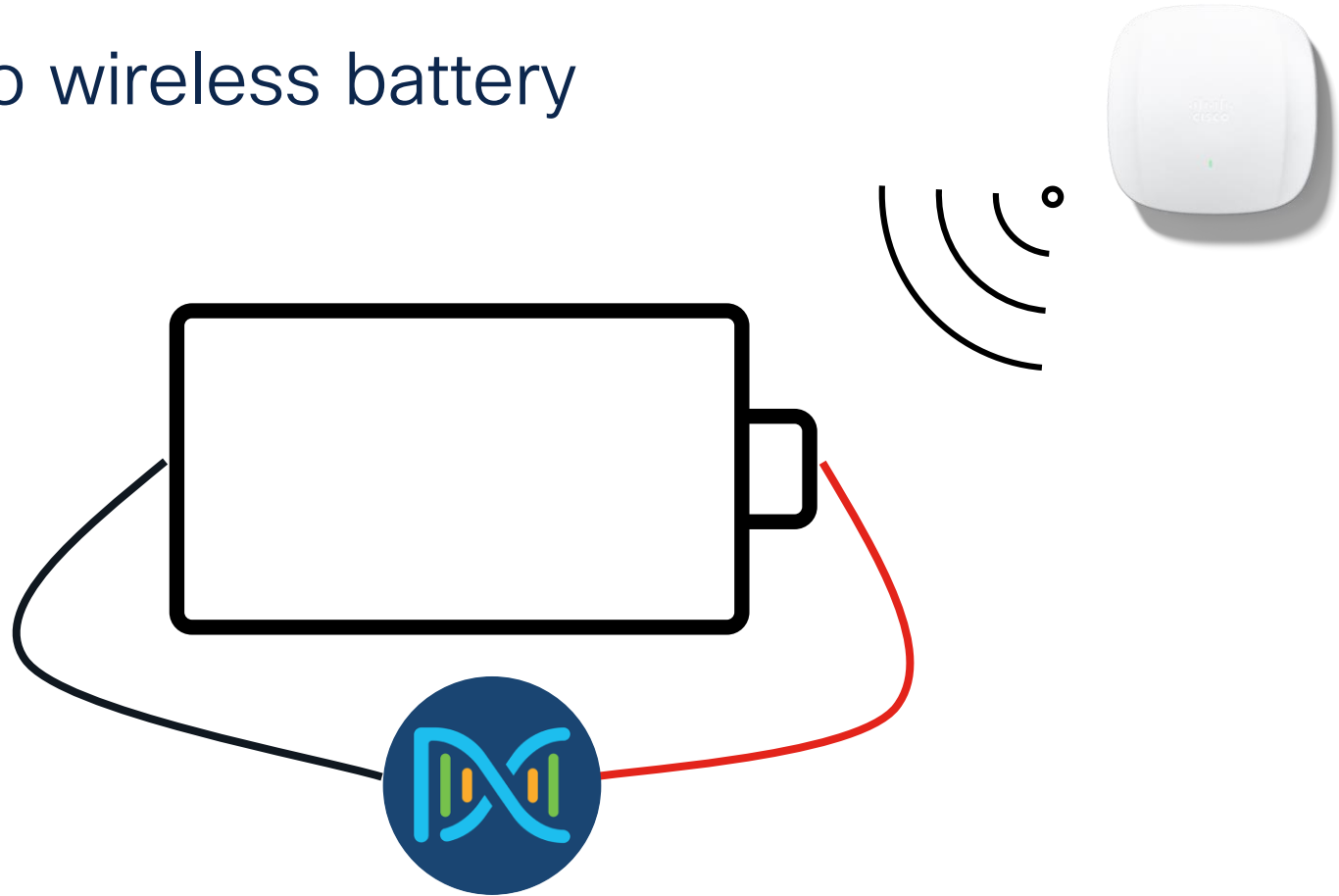
Why this session?



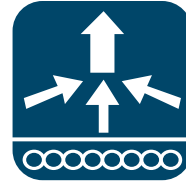
Why this session?



Your Cisco wireless battery



Components



C9800*
17.9/17.12



C91xx
CW916x



Cisco Catalyst Center
2.3.7

*Local Mode / FlexConnect Mode (Central/Local Switching)

What's NOT covered in this session



Setup of Catalyst Center / Wireless Controller



Tuning / T-Shoot of Catalyst Center / Wireless Controller itself



BRKEWN-2339, BRKEWN-3628, BRKEWN-2094, BRKEWN-2926

Cisco Live EMEA Catalyst Center Learning Map

Monday 5th

TECOPS-2001

The Ultimate Guide to Install, Onboard, Operate your Campus Network with Catalyst Center

TECOPS-2002

How to leverage Catalyst Center to build a Zero Trust Campus Network

TECOPS-2158

Catalyst Center Out-of-the-Box and Custom Integrations

TECOPS-2823

How to leverage Catalyst Center to its greatest potential

Tuesday 6th

LTREWN-2511

Automating wireless deployments at scale using Catalyst Center

BRKOPS-2032 ★

3 Catalyst Center and ITSM Workflows: CMDB, Incident Management and SWIM

BRKOPS-2416

7 Habits for success with Cisco Catalyst Center

BRKOPS-1183

Introduction to Infrastructure as Code for Catalyst Center with Terraform

LTRSEC-2005

Building Cisco SD-Access with Cisco Catalyst Center & ISE

Wednesday 7th

BRKOPS-2540

Best Practice for Prime to Catalyst Center Migration

BRKOPS-2683

Let Catalyst Center be your guide to a Zero-Trust Workplace

★ BRKOPS-2375

Everything that you need to be aware of Licensing for Catalyst Center

LTROPS-2977

Cross-Domain Automation with Catalyst Center and ACI using CI/CD Pipelines

BRKCOC-2465

Inside Cisco IT - automating the network with Catalyst Center

BRKOPS-1110 ★

Unleash Your Network Potential: Catalyst Center's MIB2/SNMP Empowerment for 3rd Party Devices

BRKOPS-2357

Taking Infrastructure as Code for Catalyst Center with GitLab CI/CD to the Next Level

Thursday 8th

BRKOPS-2077

Tips and Tricks for Prime Infrastructure to Catalyst Center Migration

BRKEWN-2667

Catalyst Wireless Supercharged by Catalyst Center

BRKOPS-2038

The Flow of Things: Navigating and Properly Enabling NetFlow-based Solutions through Catalyst Center

BRKOPS-2402

Automate the Deployment of a Wireless Network with the Help of Catalyst Center

★ BRKOPS-2471

Custom Workflows for the Cisco DNA Center Integration with ServiceNow

Friday 9th

★ BRKOPS-2521

Revolutionize Your Network Management with Cisco Catalyst Center: Physical or Virtual on AWS or VMware ESXi

Capture The Flag

@Hub All week long

Catalyst Center 2.3.7

Catalyst Center 2.3.5

Prime Migration

Catalyst Center

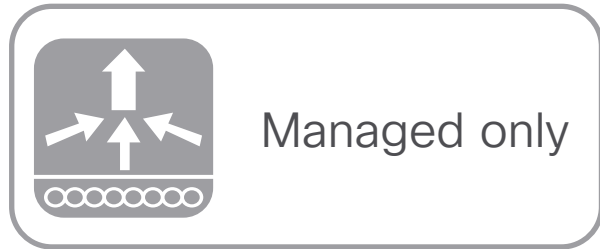
#CiscoLive

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

★ BU led sessions

CISCO Live!

Clarification



For most of the presentation the Wireless LAN Controller (WLC) only needs to be managed by Catalyst Center, not configured. Wireless configuration is done directly on the WLC.



For some of the NetOps parts, Catalyst Center must be managing & configuring the Wireless settings on the WLC. In those parts, this icon will be shown.

For your reference

- There are slides in your PDF that will not be presented, or quickly presented.
- They are valuable, but included only “For your reference”.



For your
reference

Agenda

- Introduction
- Get insights with AIOps
- Operate efficiently with NetOps
- Expand usage with DevOps
- Conclusion

Agenda

CISCO *Live!*

- Get insights with AIOps
 - Basics you should configure
 - Add-Ons you can leverage
 - On-Demand Tools that ease your life
 - The platform advantage

Overall **Network** Client Network Services Applications SD-Access AI Analytics

Global 24 Hours

Jan 22, 2024 9:57 PM - Jan 23, 2024 10:27 PM



Actions

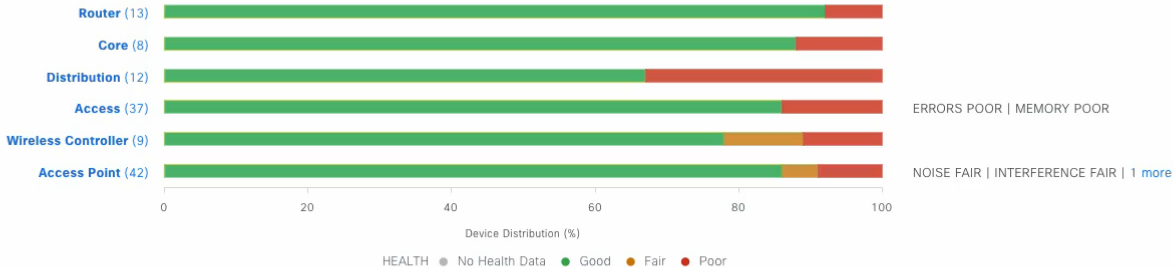
LATEST TREND

Network Devices

83 %

Healthy Network Devices

TOTAL DEVICES	121
Good Health	85
Fair Health	4
Poor Health	32
No Health Data	--



View Details

WAN Link Utilization

LATEST TREND

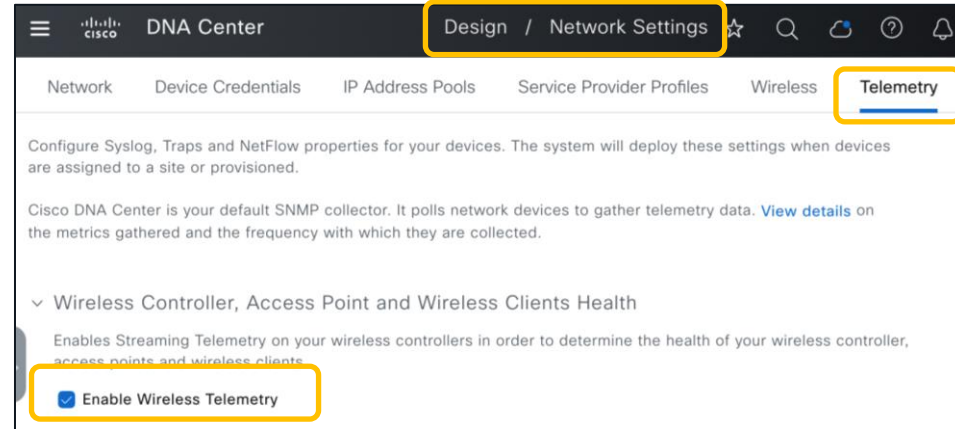
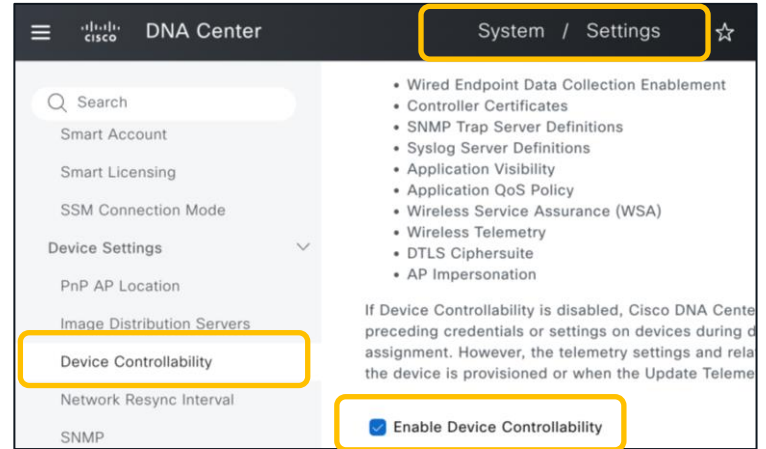
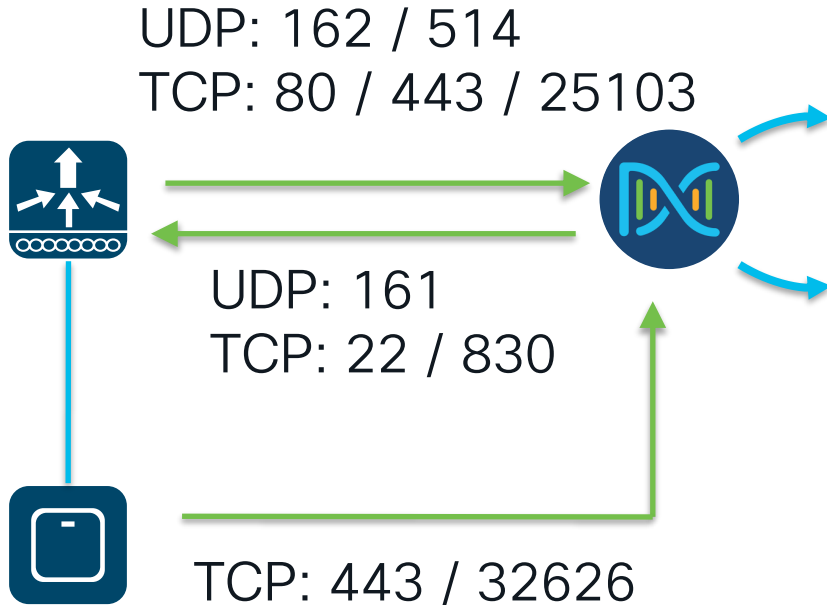
Top N APs by Client Count

LATEST TREND

WAN Link Availability

LATEST TREND

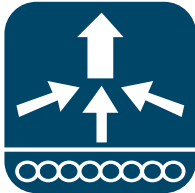
Prerequisites for Assurance



How to configure? – Wireless Assurance

Tools | Discovery

Discover WLC
with Netconf

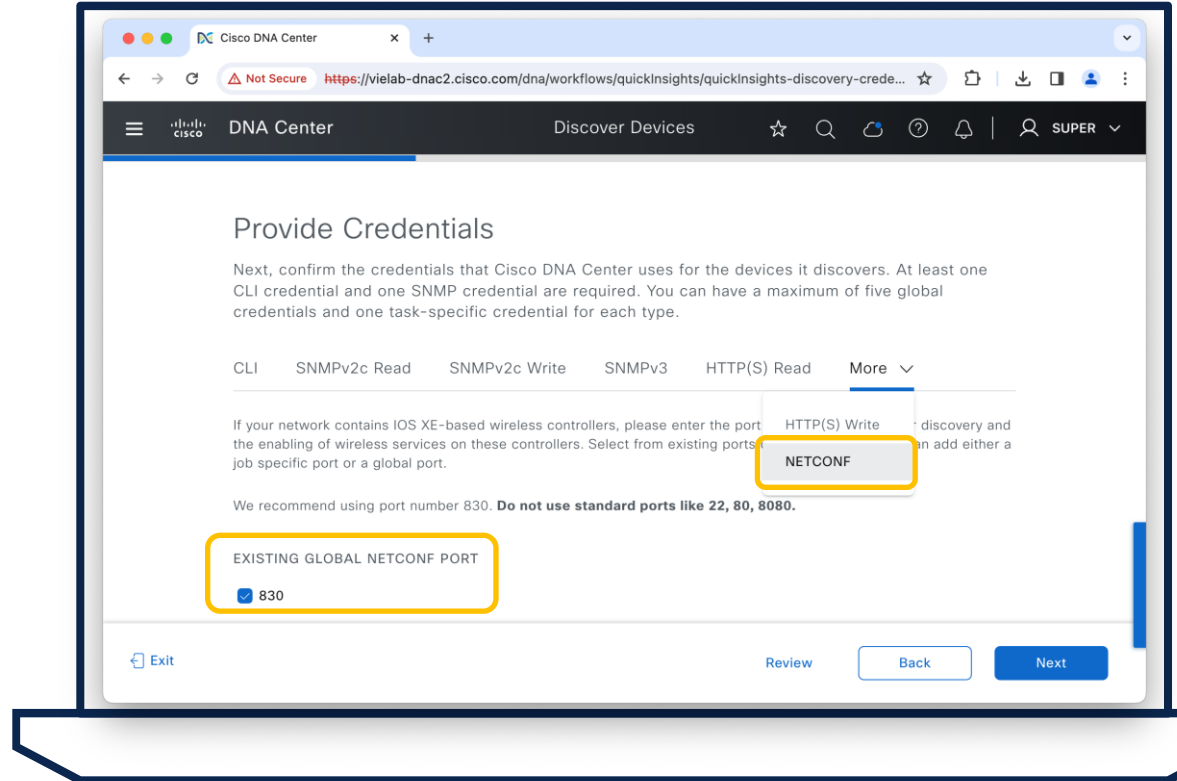
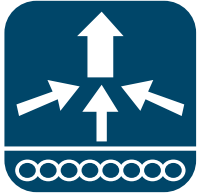


The screenshot shows the Cisco DNA Center Discovery dashboard. The left sidebar has 'Tools' highlighted. The top navigation bar has 'Discovery' highlighted. A table of discovered devices is visible on the right.

IP Address	Reachable Devices	Actions
10.51.77.130	1	...
10.51.75.200	1	...
10.51.75.143	1	...
10.10.47.14-10.2.31.2-10.2.31.2	3	...

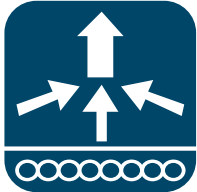
How to configure? – Wireless Assurance

Discover WLC
with Netconf

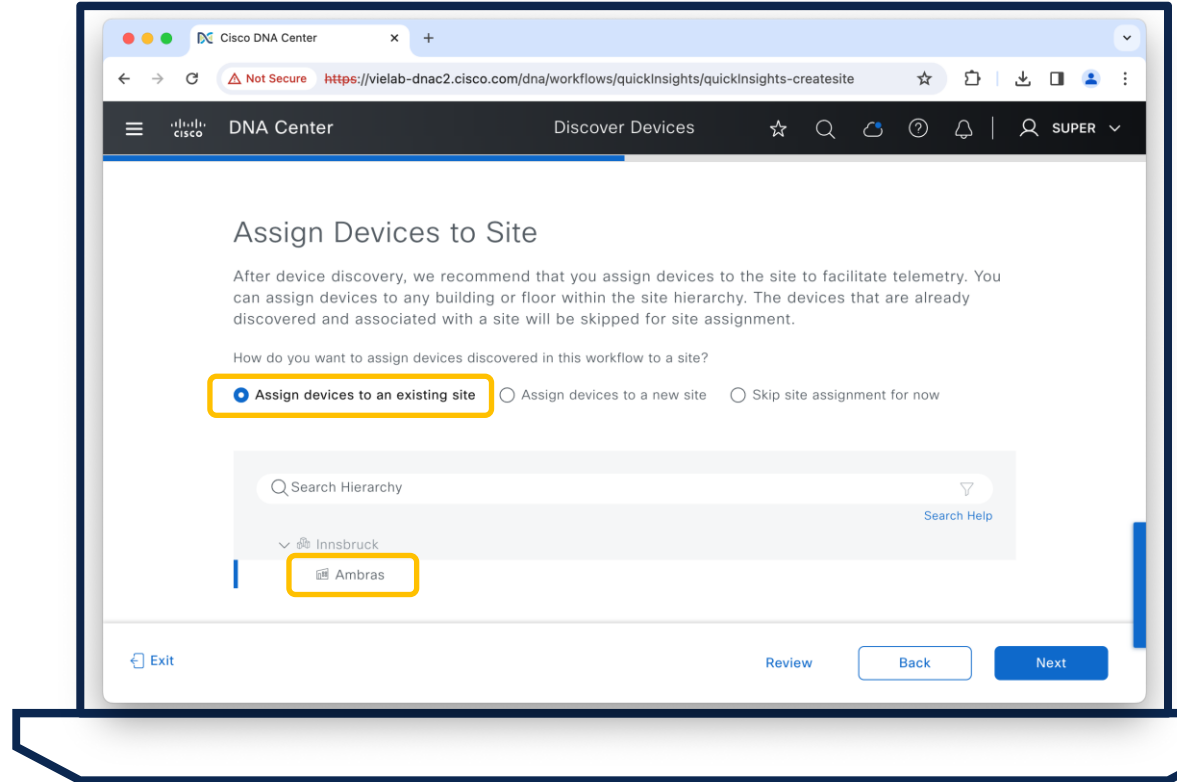


How to configure? – Wireless Assurance

Discover WLC
with Netconf



Assign WLC
to Building



How to configure? – Wireless Assurance

Provision | Inventory



Assign APs
to Floors

The screenshot displays the Cisco DNA Center web interface. The left-hand navigation menu is visible, with 'Provision' highlighted in a yellow box. The 'Inventory' option under 'NETWORK DEVICES' is also highlighted in a yellow box. The main content area shows a table of wireless controllers. The 'Actions' column for the selected controller is expanded, showing options like 'Inventory', 'Software Image', 'Provision', 'Telemetry', 'Device Replacement', 'Compliance', and 'More'. The 'Provision' option is highlighted in a yellow box. Below the table, the 'Assign Device to Site' option is also highlighted in a yellow box. The browser address bar shows the URL: <https://vielab-dnac2.cisco.com/dna/provision/devices/inventory/list>. The user's name 'SUPER' is visible in the top right corner.

How to configure? – Wireless Assurance



Assign APs
to Floors

A screenshot of the Cisco DNA Center web interface. The browser address bar shows 'https://vielab-dnac2.cisco.com/dna/provision/devices/inventory/list'. The page title is 'DNA Center' and the breadcrumb is 'Provision / Inventory'. A modal dialog titled 'Assign Device to Site' is open. On the left, a list of three devices is shown, all selected with blue checkmarks. The devices are: AP548A.BA7C.6270 AP, AP00A2.8902.4910 AP, and AP00A2.8902.1988 AP. On the right, a table shows the assignment of these devices to a site. The table has columns for 'Serial Number', 'Devices', and a site icon with the path '/Vienna/Belvedere/Tower'. The rows show: KWC25060 assigned to AP548A.BA7C.6270, KWC20300 assigned to AP00A2.8902, and KWC20300 assigned to AP00A2.8902. At the bottom of the dialog, it says 'Device Controllability is Enabled. Learn More | Disable' and has 'Cancel' and 'Next' buttons.

Serial Number	Devices	Site
KWC25060	AP548A.BA7C.6270	.../Vienna/Belvedere/Tower
KWC20300	AP00A2.8902	.../Vienna/Belvedere/Tower
KWC20300	AP00A2.8902	.../Vienna/Belvedere/Tower

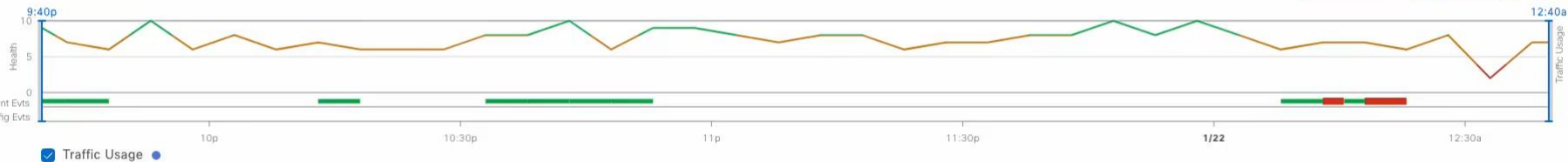
Client / User 360

Grace.Smith-iPad

- 7 Grace.Smith-iPad
- 4 Grace.Smith-iPhone
- 8 Grace.Smith-PC
- 9 Grace.Smith-Galaxy-S20

3 Hours

Intelligent Capture Webex 360 MSTeams 360



7/10 CLIENT DETAILS

Jan 21, 2024 9:40 PM - Jan 22, 2024 12:40 AM

Device: Apple-iPad OS: Apple-iPad MAC: 6C:19:C0:BD:87:C9 IPv4: 10.30.100.27 IPv6: 2001:420:81:450::4ade:cfa5 L3 Virtual Network: -- L2 Virtual Network: -- VLAN ID: 100 Status: Connected Capability: 11ac Last seen: Jan 22, 2024 12:47:01 AM

Connected Network Device: SJC01_9136_1 SSID: @CorpSSID [View All Details](#)

- Issues
- Onboarding
- Path Trace
- Application Experience
- Device Info
- Connectivity
- RF
- iOS Analytics
- User Defined Network
- Event Viewer

Summary Jan 21, 2024 9:40 PM - Jan 22, 2024 12:40 AM

- Onboarding failed during Authentication (1 out of 1), due to 'Auth Key Exchange Timeout' (1)
- Roaming failed during Authentication (4 out of 4), mostly due to 'Auth Key Exchange Timeout' (3)

Onboarding



Roaming



Connectivity

RF QUALITY

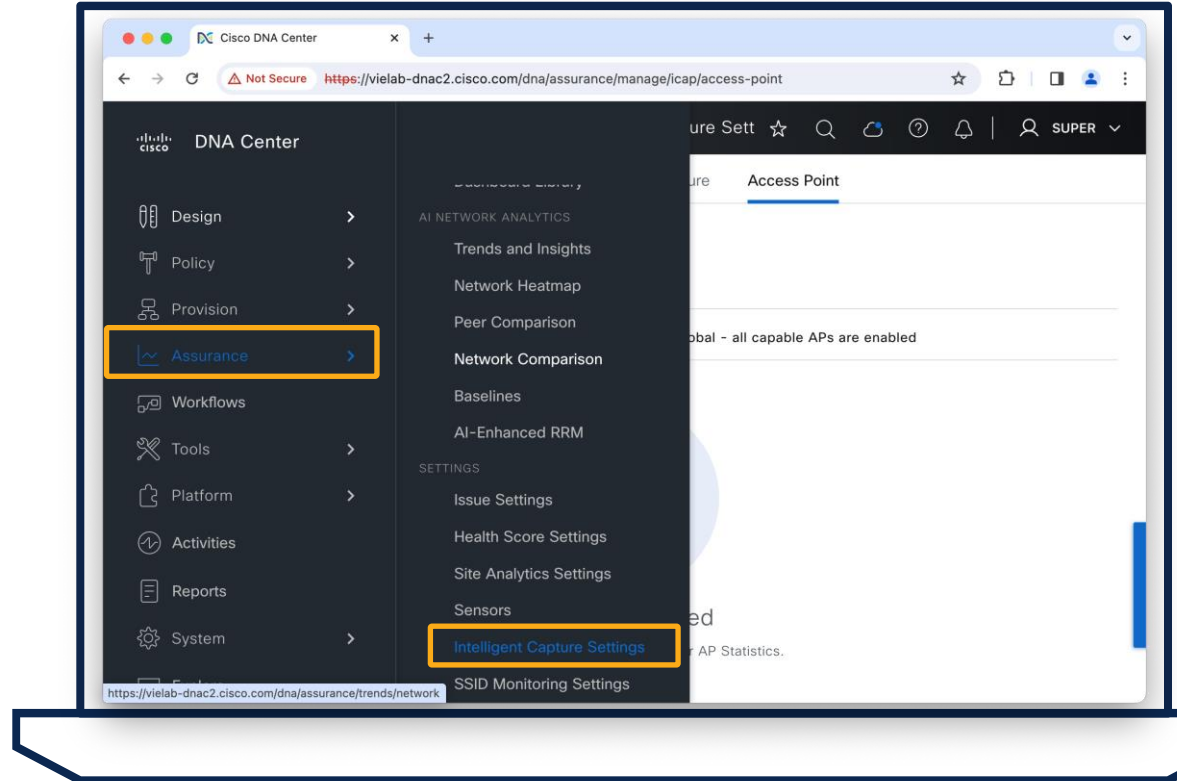
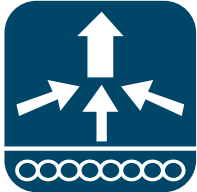
RSSI 94% of the time is Good

TRAFFIC

Retries 8% of the data traffic

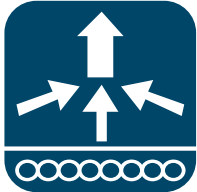
How to configure? – Intelligent Capture

Enable Anomaly & AP Stats Capture

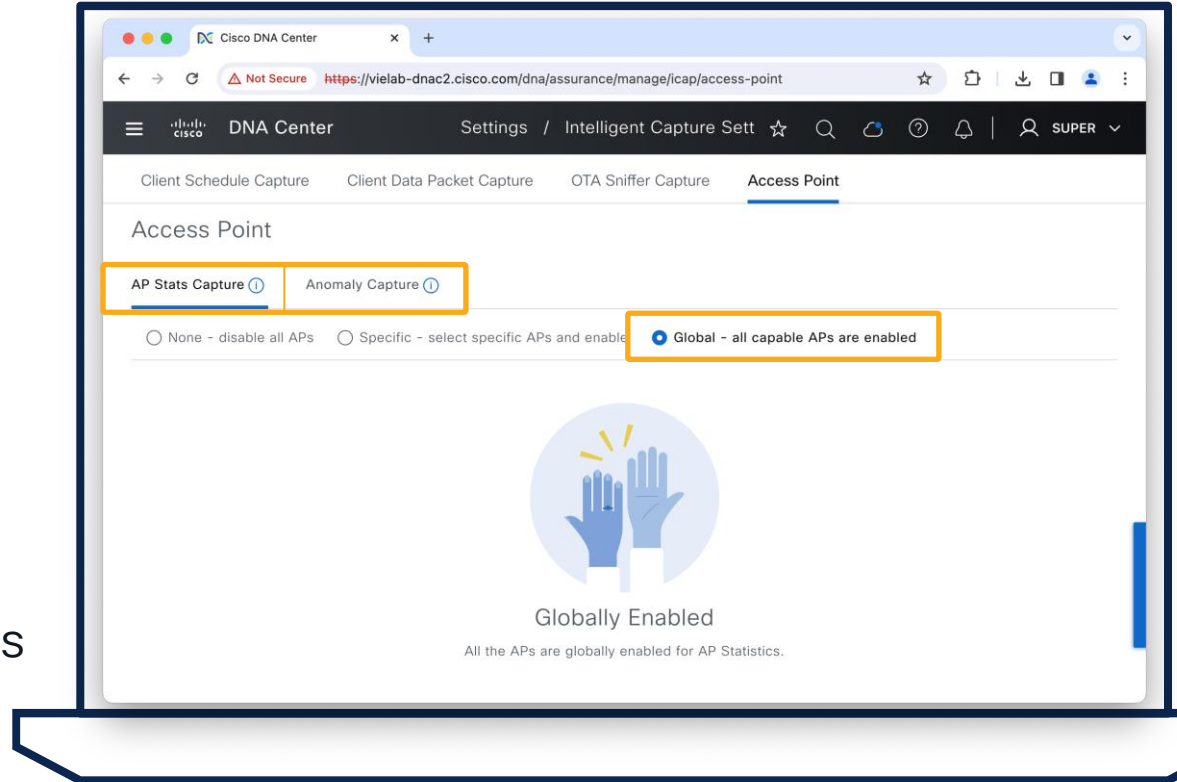


How to configure? – Intelligent Capture

Enable Anomaly & AP Stats Capture



AP Stats limited to 1000 APs



Data Frequency and Scale

Operation	Feature Data	Data Frequency	Max Concurrent Session
Global or per AP	Anomaly Packet Capture	Whenever an anomaly occurs	Unlimited
	Client RF Stats	30 seconds	All clients associated to up to 1000 enabled APs
	AP RF Stats	30 seconds	
On-Demand or Scheduled	Live Capture's Filtered Client RF Stats	5 seconds	16 Clients
	Live Capture's Filtered Onboarding Events	2 seconds	
	Live Capture's Onboarding Packet Capture	Whenever packets are sent	
On-Demand Only	Data Packet Capture ¹⁾	Whenever packets are sent	1 Client
	Spectrum Analysis ²⁾	Continuous for 10min	10 APs

Site: Global

Jan 23, 2024 7:38 PM - Jan 23, 2024 10:38 PM Last 3 hours Refresh Actions

TOTAL ROGUE THREATS

73

TOTAL AWIPS THREATS

0

TOTAL UNIQUE ROGUE CLIENTS

6

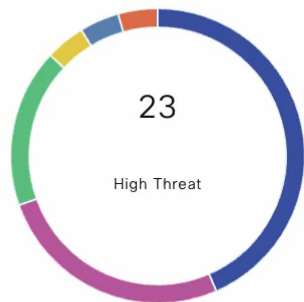
ROGUES CONTAINED

0

High Threats Summary

Active High Threats (23)

By Threat Type Top 10 All



- Honeypot (10)
- Deauthentication broadcast (6)
- Association flood (4)
- Authentication flood (1)
- Rogue on wire (1)
- Deauthentication flood (1)

Top Locations Affected

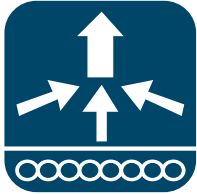


High Threats Over Time

View Threats

How to configure? – Rogue/aWIPS

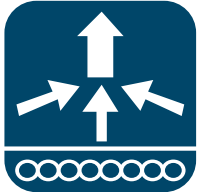
Enable
Rogue / aWIPS



The screenshot shows the Cisco DNA Center interface. In the left sidebar, the 'Assurance' menu item is highlighted with a yellow box. In the main dashboard area, the 'Rogue and aWIPS' link is highlighted with a yellow box. A context menu is open over the 'Rogue and aWIPS' link, with the 'Enable' option highlighted with a yellow box. The context menu also includes options for 'Disable', 'Status', 'Rogue', 'aWIPS', and 'Reports'. The dashboard title is 'and aWIP'. The top navigation bar shows 'DNA Center' and 'SUPER' user. The browser address bar shows 'https://vielab-dnac2.cisco.com/dna/assurance/dashboards/roguemgmtDashboard/overview'.

How to configure? – Rogue/aWIPS

Configuration | AP Join



Enable aWIPS /
Rogue Detection
@AP Join Profile
on WLC

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller web interface. The browser address bar shows <https://localhost:6445/webui/#/apJoin>. The page title is "Cisco Catalyst 9800-CL Wireless Controller" with version 17.9.4. The user is logged in as "admin". The navigation menu on the left includes Dashboard, Monitoring, Configuration (highlighted with an orange box), Administration, Licensing, and Troubleshooting. The main content area is titled "Edit AP Join Profile" and has tabs for General, Client, CAPWAP, AP, Management, Security (active), ICap, and QoS. Under the "Security" tab, there are two sections highlighted with orange boxes: "Rogues" and "aWIPS". The "Rogues" section has a "Rogue Detection" checkbox checked. The "aWIPS" section has "aWIPS Enable" and "Forensic Enable" checkboxes checked. The "Rogue Detection Minimum RSSI" is set to -90, "Rogue Detection Transient Interval (seconds)" is 0, and "Rogue Detection Report Interval (seconds)" is 10. The "Rogue Containment Automatic Rate Selection" and "Auto Containment on FlexConnect Standalone" checkboxes are unchecked. At the bottom right, there is an "Update & Apply to Device" button.

Tips and Tricks – Wireless Assurance



Netconf authentication and authorization uses the default group (configurable 17.9 or higher)

```
C9800#show run | sec aaa
...
aaa new-model

aaa authentication login default myAuth
aaa authorization exec default myAuthZ
```

Tips and Tricks – Wireless Assurance



Netconf authentication and authorization uses the default group (configurable 17.9 or higher)

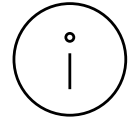
```
C9800#show version
Cisco IOS XE Software, Version 17.09.01
...
C9800#show run | sec yang

yang-interfaces aaa authentication ...
yang-interfaces aaa authorization ...
```


Tips and Tricks – Wireless Assurance



Netconf authentication and authorization uses the default group (configurable 17.9 or higher)



Verify telemetry connection from WLC if you don't receive data

```
C9800#show telemetry connection all
```

```
Telemetry connections
```

Index	Peer Add	Port	Source Address	State
1	10.51.77.181	25103	10.51.77.173	Active

Active – All good

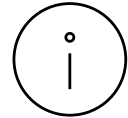
Connecting – Cert/FW issue

N/A – Telemetry config missing

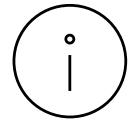
Tips and Tricks – Wireless Assurance



Netconf authentication and authorization uses the default group (configurable 17.9 or higher)



Verify telemetry connection from WLC if you don't receive data



Intelligent capture troubleshoot: check gRPC tunnel status on AP

```
CW9166-01#show ap icap connection
```

```
Connection Status:  READY  
Connection URL:    10.51.77.181:32626  
Certificate Failures:  0
```

Ready – **All good**

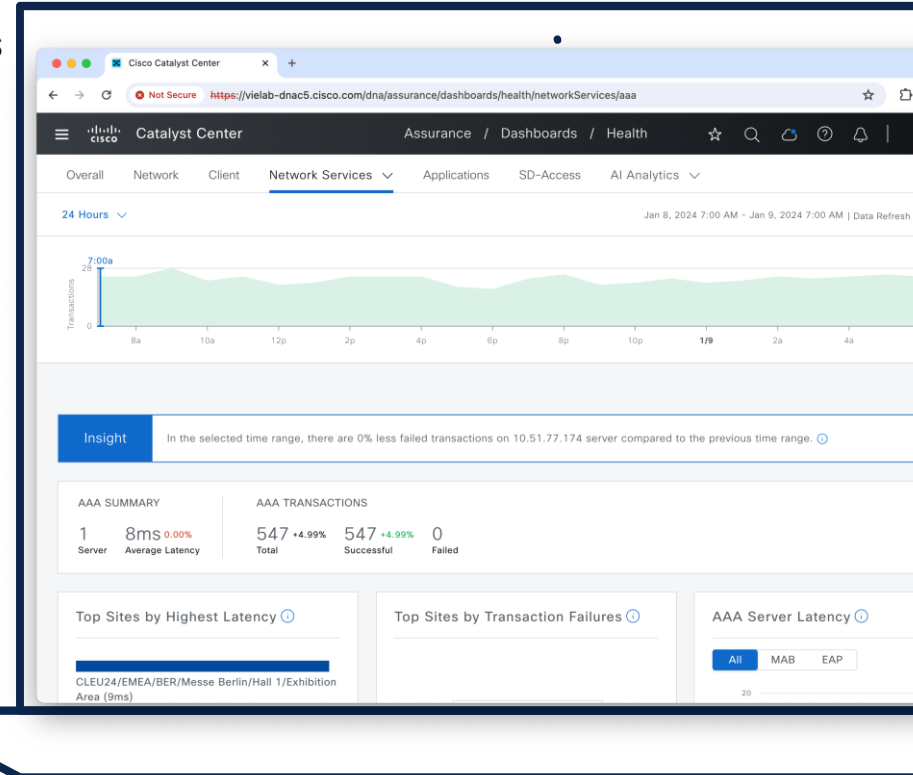
Not Connected – **Cert/FW issue**

N/A – **iCap config missing**

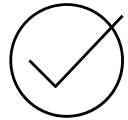
Tips and Tricks – Wireless Assurance



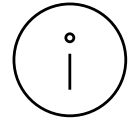
Network Services (DHCP/AAA) requires traffic to cross WLC (Local Mode/Flex Central Switching)



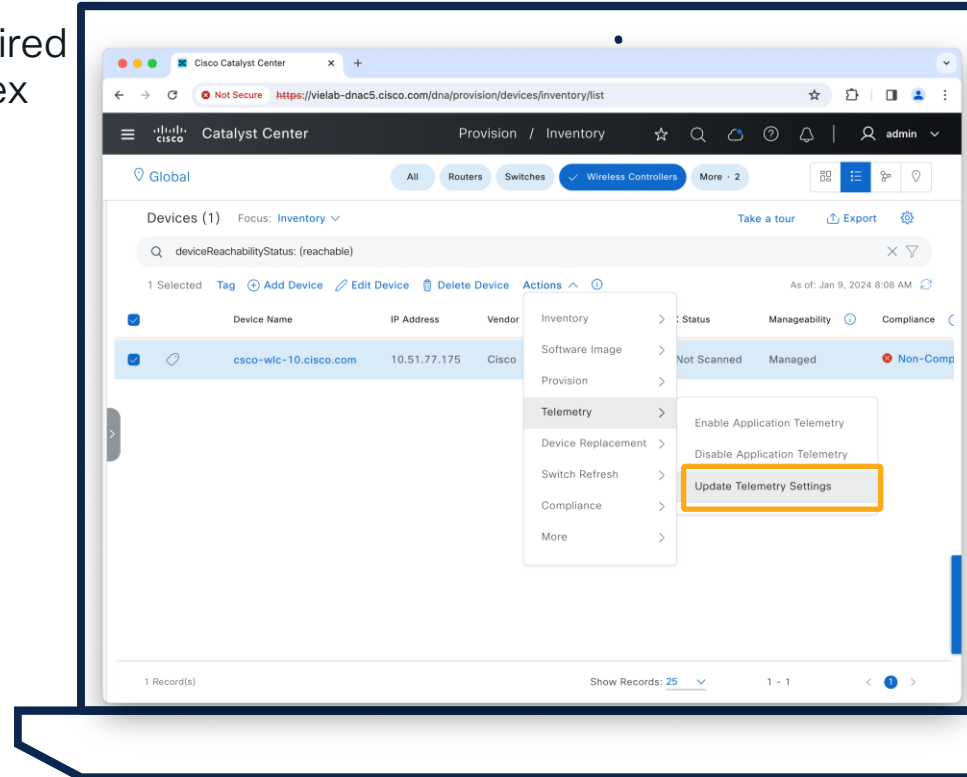
Tips and Tricks – Wireless Assurance



Network Services (DHCP/AAA) required traffic to cross WLC (Local Mode/Flex Central Switching)



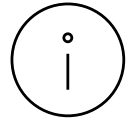
Use 'Update Telemetry Settings' (Force Push) for reprovisioning



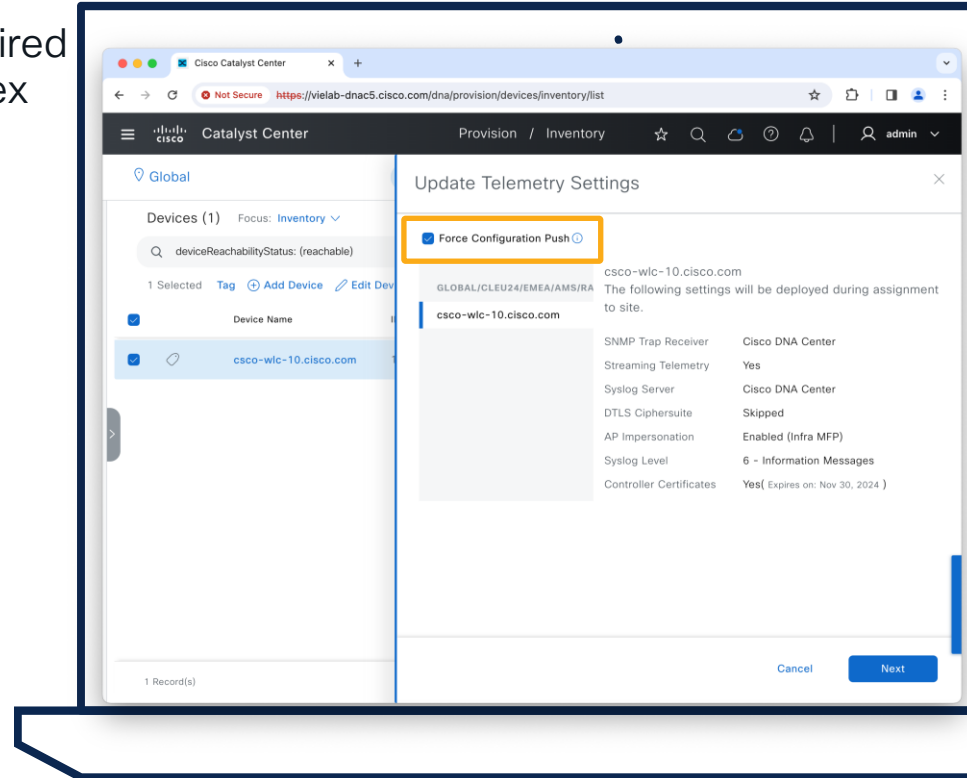
Tips and Tricks – Wireless Assurance



Network Services (DHCP/AAA) required traffic to cross WLC (Local Mode/Flex Central Switching)



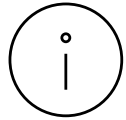
Use 'Update Telemetry Settings' (Force Push) for reprovisioning



Tips and Tricks – Wireless Assurance



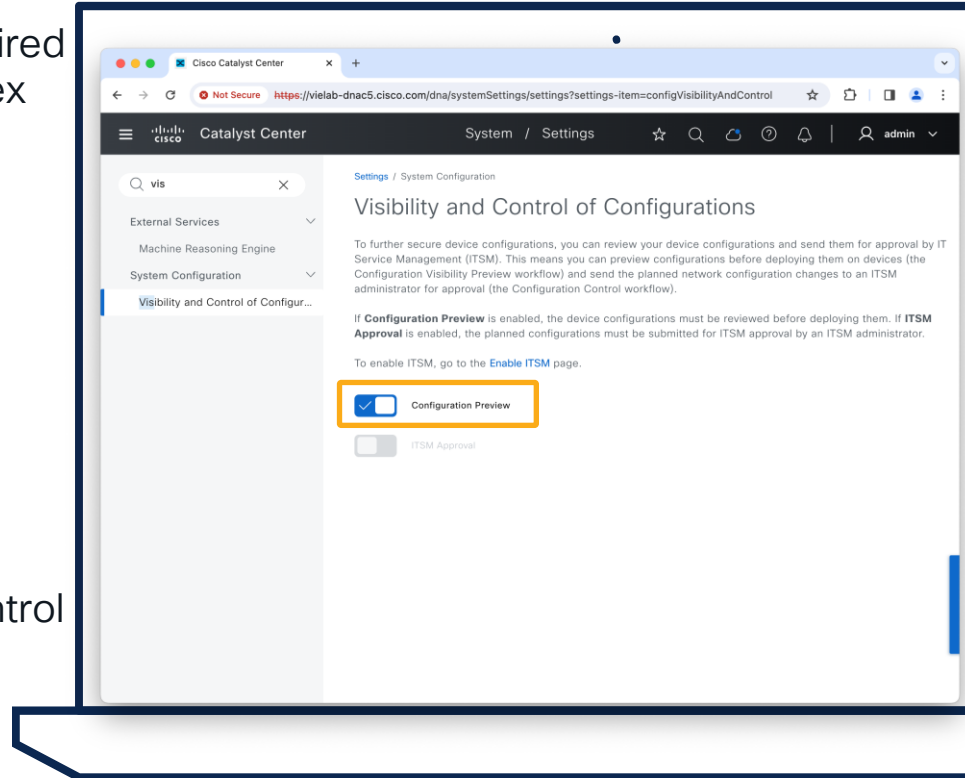
Network Services (DHCP/AAA) required traffic to cross WLC (Local Mode/Flex Central Switching)



Use 'Update Telemetry Settings' (Force Push) for reprovisioning



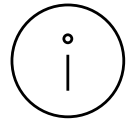
For better control, enable 'Configuration Preview' under System | Settings | Visibility and Control



Tips and Tricks – Wireless Assurance



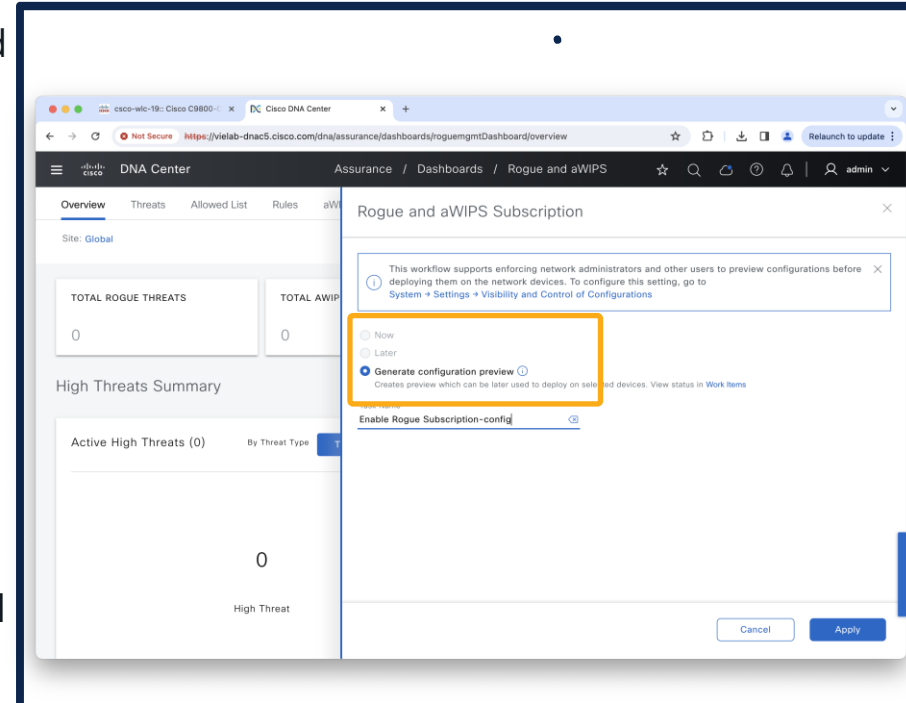
Network Services (DHCP/AAA) required traffic to cross WLC (Local Mode/Flex Central Switching)



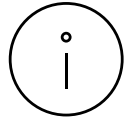
Use 'Update Telemetry Settings' (Force Push) for reprovisioning



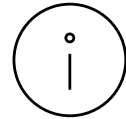
For better control, enable 'Configuration Preview' under System | Settings | Visibility and Control



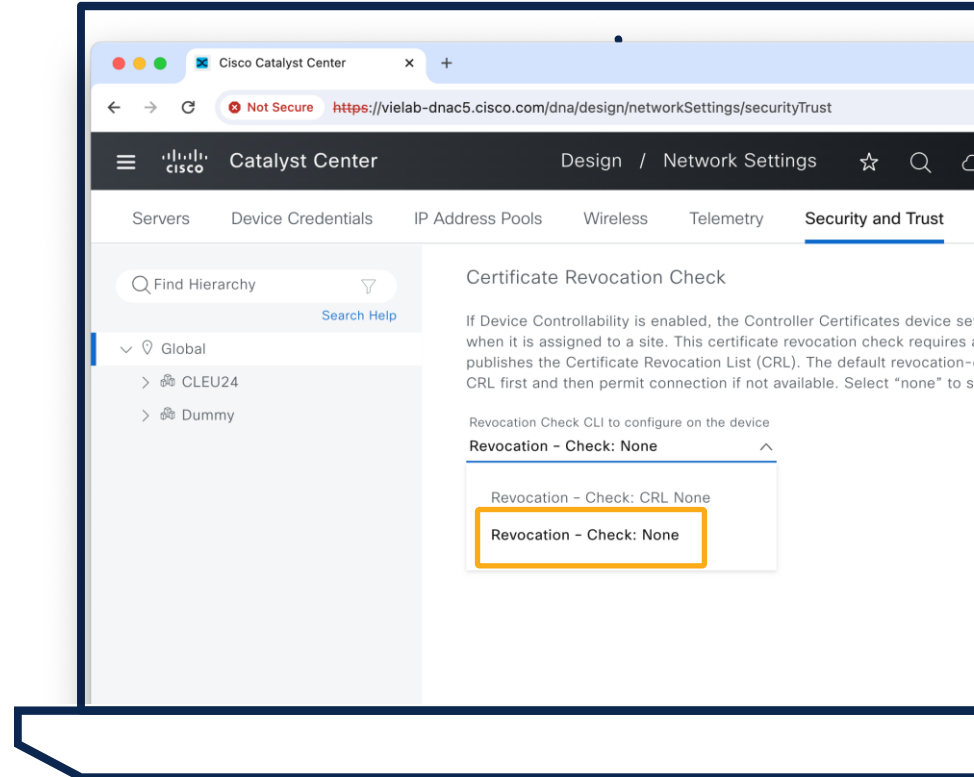
Tips and Tricks – Wireless Assurance



Disable Revocation Check in Design Settings



iCap configuration is not pushed automatically to newly added AP Join profiles on C9800, either manually configure it or disable/enable iCap





Manual iCap Statistic/Anomaly Configuration

```
C9800#
```

```
! Configuration @ AP Join Profile
```

```
ap profile APJoin4CSCO
```

```
icap subscription ap statistics radio enable
```

```
icap subscription ap statistics wlan enable
```

```
icap subscription client anomaly-detection enable
```

```
icap subscription client anomaly-detection packet-trace trigger ap
```

```
icap subscription client anomaly-detection report-individual throttle 100
```

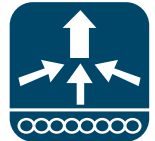
```
icap subscription client anomaly-detection report-summary enable
```

```
icap subscription client statistics enable
```

Certificates



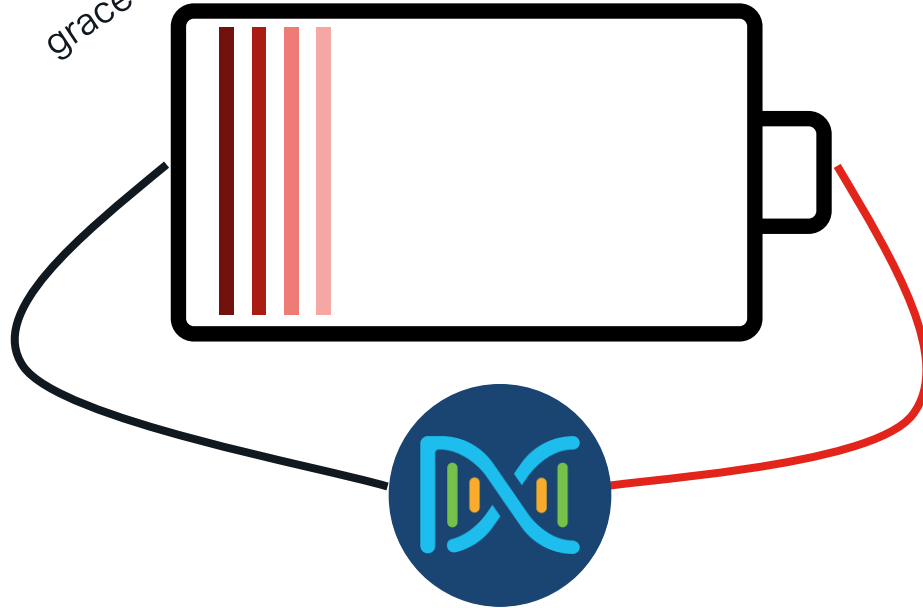
- Catalyst Center System (GUI) Certificate
 - If custom required, replace before adding devices
 - Stick to documentation for cert SAN field and option keys
 - Trustpoint on device: DNAC-CA
- Device certificate is created with internal CA of Catalyst Center
 - Can be Sub CA of corporate CA
 - Can query external CA with SCEP
 - Trustpoint on device: sdn-network-infra-iwan



Your Cisco wireless battery

network dashboard
grace

intelligent capture



Agenda

CISCO *Live!*

- Get insights with AIOps
 - Basics you should configure
 - Add-Ons you can leverage
 - On-Demand Tools that ease your life
 - The platform advantage

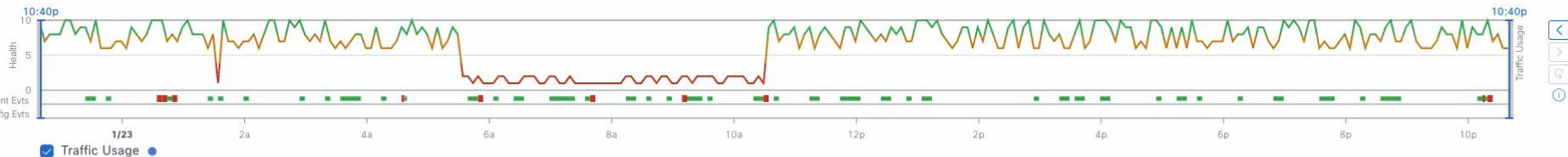
Client / User 360

Grace.Smith-iPad

7 Grace.Smith-iPad 8 Grace.Smith-iPhone 8 Grace.Smith-PC 9 Grace.Smith-Galaxy-S20

24 Hours

Intelligent Capture Webex 360 MSTeams 360



7/10 CLIENT DETAILS

Jan 22, 2024 10:40 PM - Jan 23, 2024 10:40 PM

Device: Apple-iPad OS: Apple-iPad MAC: 6C:19:C0:BD:87:C9 IPv4: 10.30.100.27 IPv6: 2001:420:81:450::4ade:cfa5 L3 Virtual Network: -- L2 Virtual Network: -- VLAN ID: 100 Status: Connected Capability: 11ac Last seen: Jan 23, 2024 10:40:12 PM

Connected Network Device: SJC01_9136_1 SSID: @CorpSSID [View All Details](#)

Issues Onboarding Path Trace Application Experience Device Info Connectivity RF iOS Analytics User Defined Network Event Viewer

Summary Jan 22, 2024 10:40 PM - Jan 23, 2024 10:40 PM

- Onboarding failed during Authentication (1 out of 1), due to 'Auth Key Exchange Timeout' (1)
- Roaming failed during Authentication (4 out of 4), mostly due to 'Auth Key Exchange Timeout' (3)

Onboarding



Roaming



Connectivity

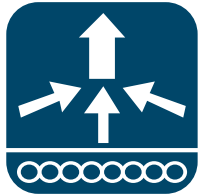
RF QUALITY

RSSI 100% of the time is Good

TRAFFIC

Retries 5% of the data traffic

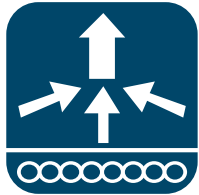
How to configure Application Assurance?



A screenshot of the Cisco DNA Center web interface. The browser address bar shows the URL: https://vielab-dnac2.cisco.com/dna/design/networkSettings/telemetry. The page title is "DNA Center" and the breadcrumb is "Design / Network Settings". The "Telemetry" tab is selected in the navigation menu. The main content area has a heading "Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned." Below this is a paragraph: "Cisco DNA Center is your default SNMP collector. It polls network devices to gather telemetry data. View details on the metrics gathered and the frequency with which they are collected." The "Application Visibility" section is expanded and highlighted with an orange rounded rectangle. It contains the following text: "Enable Netflow Application Telemetry and Controller Based Application Recognition (CBAR) by default upon network device site assignment". There are two radio button options: "Enable by default on supported wired access devices" (which is selected) and "Use Cisco DNA Center as the Netflow Collector" (which is also selected). Below these are two more radio button options: "Use Cisco Telemetry Broker (CTB) or ODF Director" and "Use Cisco Telemetry Broker (CTB) or ODF Director". At the bottom right of the configuration area are "Reset" and "Save" buttons.

How to configure Application Assurance?

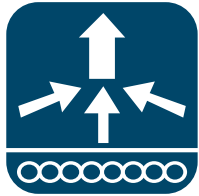
Enable Application Telemetry

A screenshot of the Cisco DNA Center web interface. The browser address bar shows the URL: https://vielab-dnac2.cisco.com/dna/provision/devices/inventory/list. The page title is "DNA Center" and the breadcrumb is "Provision / Inventory". The user is logged in as "SUPER". The interface shows a list of devices under the "Wireless Controllers" filter. One device, "vielab-wlc2 WLC", is selected. The "Actions" menu is open, and the "Telemetry" option is highlighted. A sub-menu is displayed, showing "Enable Application Telemetry" as the selected option. Other options in the sub-menu include "Disable Application Telemetry" and "Update Telemetry Settings".

Device Name	IP Address	Vendor	Re	Inventory	Manageability	Compliance
vielab-wlc2 WLC	10.51.77.130	Cisco		Inventory	Managed	Compliant

How to configure Application Assurance?

Enable Application Telemetry

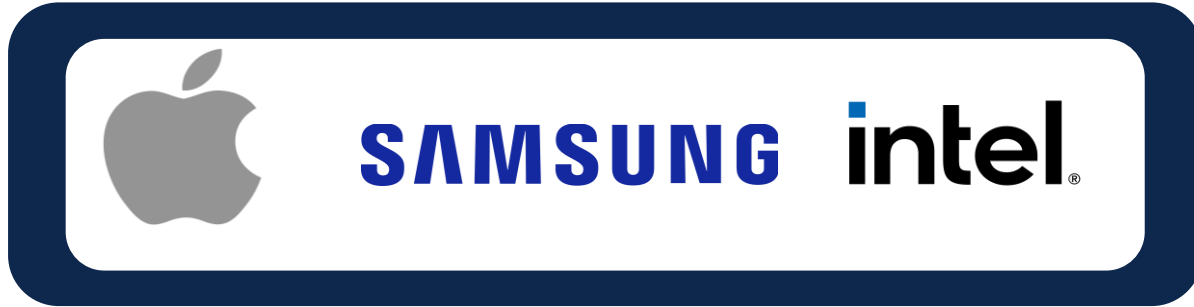


The screenshot shows the Cisco DNA Center web interface. The main page displays a table of devices with one device selected: 'vielab-wlc2' (WLC) with IP address 10.51.3. The 'Enable Application Telemetry' dialog is open, showing a warning about network service disruption and a note about disabling and re-enabling the feature. The configuration options for 'vielab-wlc2' are: Local, Flex/Fabric, Include Guest SSIDs, and Telemetry Source: **NetFlow**. The dialog has 'Cancel' and 'Enable' buttons.

Client Analytics



BRKEWN-2926



iOS Analytics, Fastlane and Fastlane+

Neighbor AP Table

BSSID	AP Name	Channel	SSID (only)	Location	Time	Disassociation Reason
88:95:60:0D:48:7F	LAR-HP45P-0802-0786	149	-55	GlobalPorch-AmericaUS004	May 8, 2022 9:58 PM	User triggered disassociation
88:95:60:0D:48:7F	AP8887-CASA-3002	149	-76	GlobalPorch-AmericaUS004	May 8, 2022 9:53 PM	Client site
88:95:60:0D:48:7F	SGE11_1P10_1	141	-58	GlobalPorch-AmericaUS004	May 8, 2022 9:43 PM	User triggered disassociation

Disassociation Details

Neighbor AP Visual

SAMSUNG Analytics

Event Viewer

Event	Time	Details
RTT4-WLC Reaming	5:51:05:581 PM - 5:51:05:581 PM	
Client Sent Disassociation	5:47:30:581 PM	101-01 Device Turned Off
Client Sent Disassociation	5:47:30:581 PM	
Disassociation - Incomplete	5:43:30:581 PM - 5:43:30:581 PM	AP:AP4802 WLAN:WLAN@Corp0502
Client Sent Disassociation	5:39:30:581 PM	AP:AP4802 WLAN:WLAN@Corp0502
Client Sent Disassociation	5:39:30:581 PM	Airplane Mode Turned On
ENKP	5:39:05:581 PM - 5:39:05:581 PM	
Bluetooth Relay	5:31:05:581 PM - 5:31:05:581 PM	

intel Connectivity Analytics

Detail Information

Reported Errors

- Jan 2, 2022 3:05 PM
- Jan 2, 2022 2:08 PM



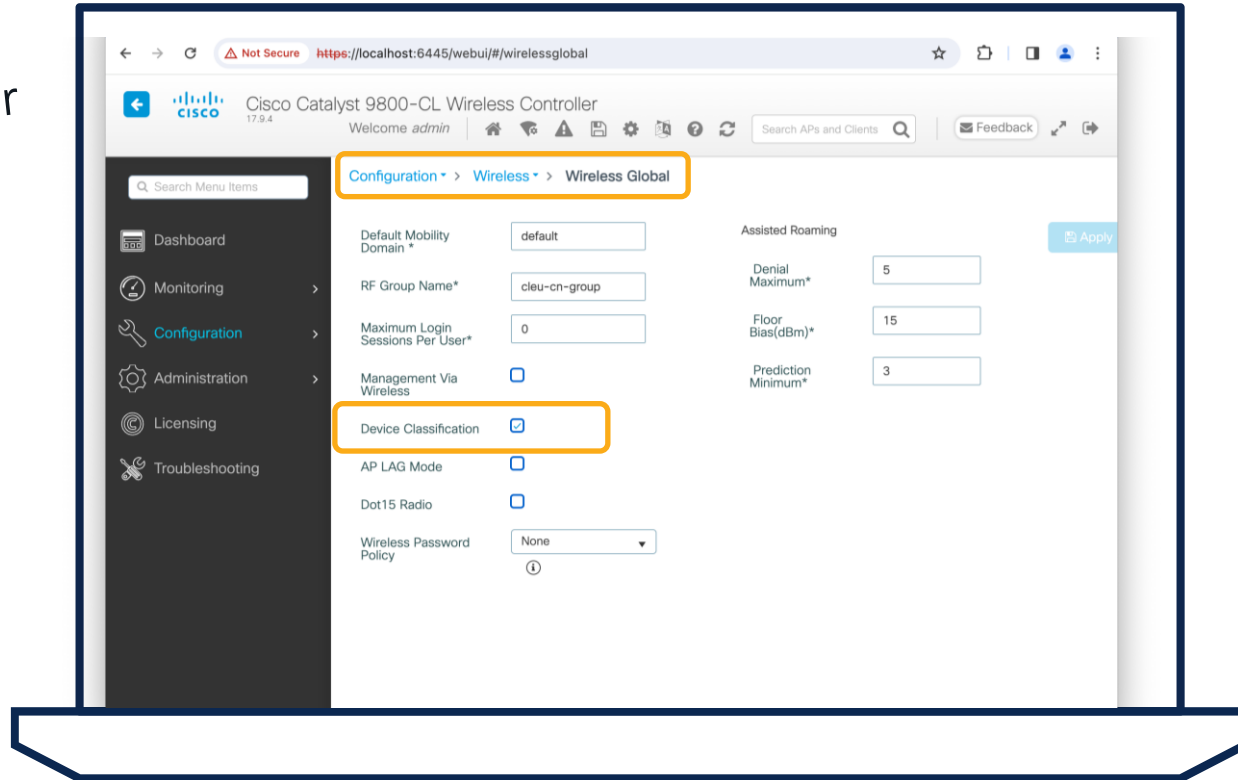
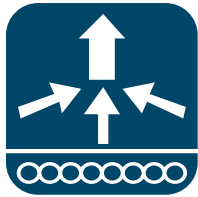
Intel Connectivity, Apple, Samsung Analytics

	Driver Version Device Type	Catalyst Center	IOS-XE Release
Intel Connectivity Analytics	Intel 22.50.1 or newer on AX1650/1675 AC8561/9560 AX200/201/210/211/411	2.3.3	17.6.1
Apple Analytics	iOS 11 on iPhone 7 or later	2.2.1	16.12.1s
Samsung Analytics	Android 9 or later on Galaxy S10 or newer	2.2.1	17.1.1

How to configure Client Analytics?

Wireless Global

Configure Device Classifier

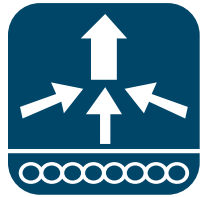


The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller configuration page for the Wireless Global settings. The breadcrumb navigation is Configuration > Wireless > Wireless Global. The left sidebar contains menu items: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area displays various configuration options:

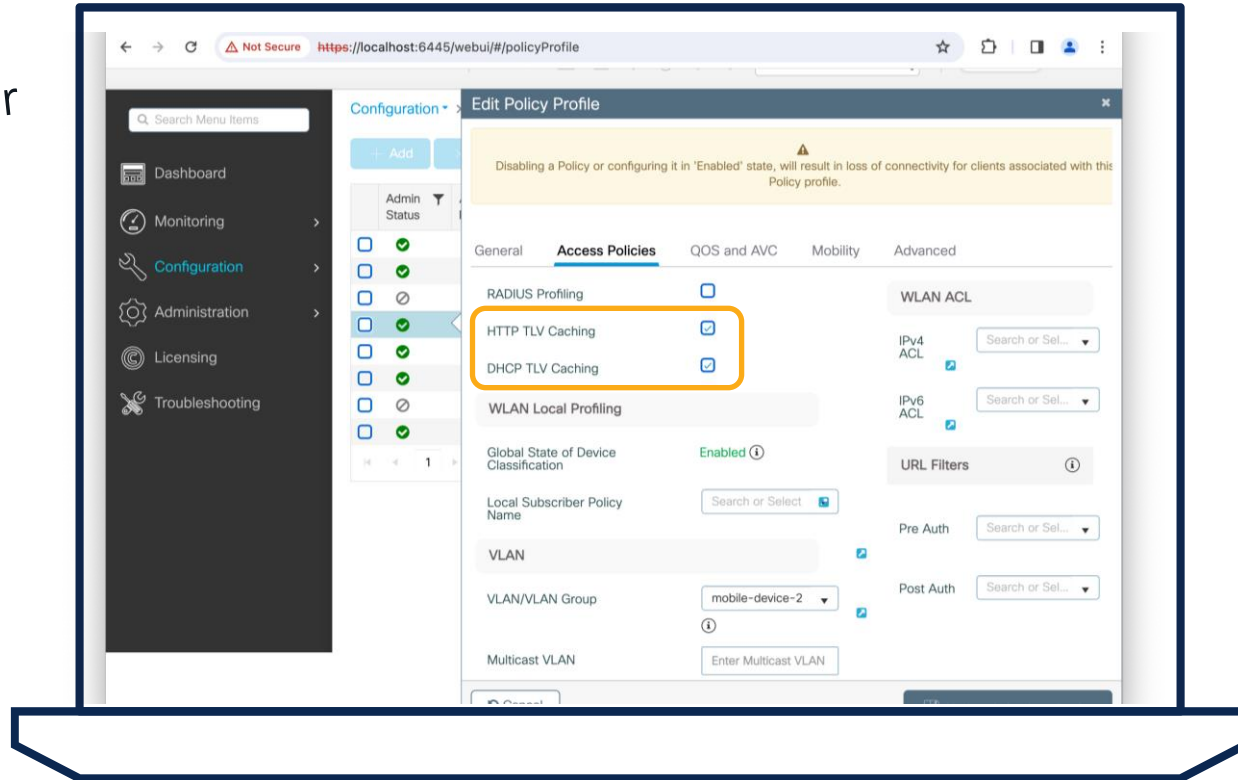
- Default Mobility Domain: default
- RF Group Name: cleu-cn-group
- Maximum Login Sessions Per User: 0
- Management Via Wireless:
- Device Classification: (highlighted with an orange box)
- AP LAG Mode:
- Dot15 Radio:
- Wireless Password Policy: None
- Assisted Roaming: (Apply button)
- Denial Maximum: 5
- Floor Bias(dBm): 15
- Prediction Minimum: 3

How to configure Client Analytics?

Policy Profile | Access Policies



Configure Device Classifier

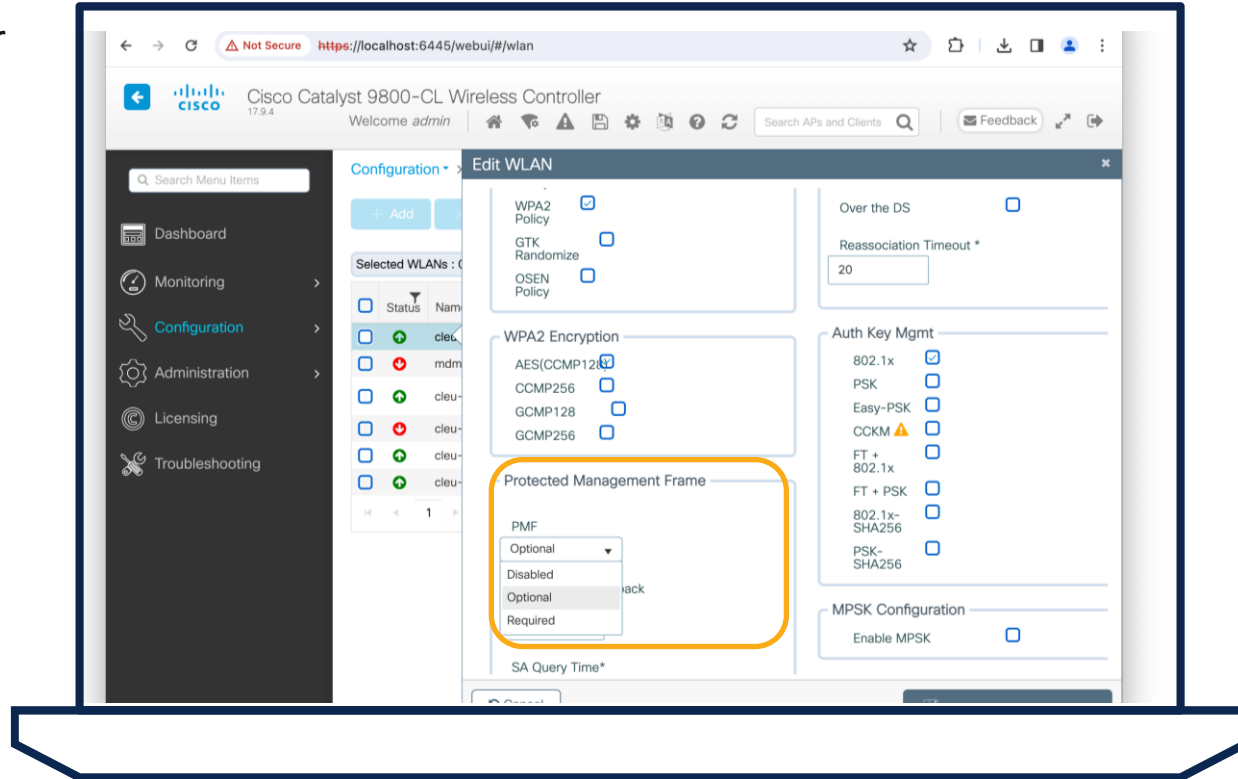
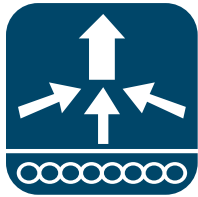


The screenshot shows the 'Edit Policy Profile' configuration page in a web browser. The browser address bar shows 'https://localhost:6445/webui/#/policyProfile'. The page has a dark sidebar on the left with a search bar and menu items: Dashboard, Monitoring, Configuration (highlighted), Administration, Licensing, and Troubleshooting. The main content area is titled 'Edit Policy Profile' and has a warning banner at the top: 'Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.' Below the banner are tabs for 'General', 'Access Policies', 'QoS and AVC', 'Mobility', and 'Advanced'. The 'Access Policies' tab is active. Under 'Access Policies', there are sections for 'RADIUS Profiling' (with checkboxes for 'HTTP TLV Caching' and 'DHCP TLV Caching', both checked and highlighted with an orange box), 'WLAN Local Profiling', 'Global State of Device Classification' (set to 'Enabled'), 'Local Subscriber Policy Name', 'VLAN' (with 'VLAN/VLAN Group' set to 'mobile-device-2'), and 'Multicast VLAN'. On the right side, there are sections for 'WLAN ACL' (with 'IPv4 ACL' and 'IPv6 ACL' search fields), and 'URL Filters' (with 'Pre Auth' and 'Post Auth' search fields).

How to configure Client Analytics?

WLANs | Security | Layer 2

PMF Optional or Required



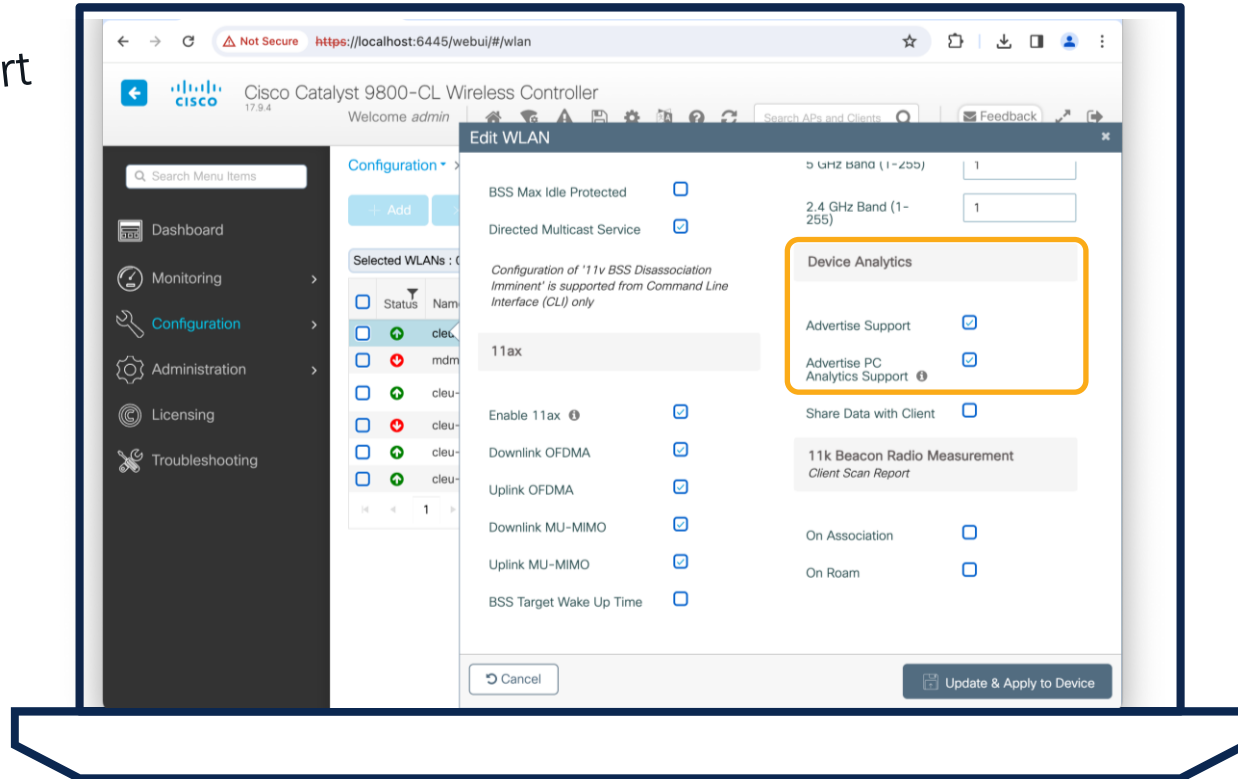
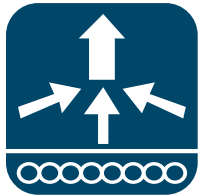
The screenshot displays the Cisco Catalyst 9800-CL Wireless Controller configuration interface. The main content area is titled "Edit WLAN" and contains several configuration sections:

- WPA2 Policy:** Includes checkboxes for WPA2 Policy, GTK Randomize, and OSEN Policy.
- Over the DS:** Includes a checkbox for "Over the DS" and a "Reassociation Timeout *" field set to 20.
- WPA2 Encryption:** Includes checkboxes for AES(CCMP128), CCMP256, GCMP128, and GCMP256.
- Protected Management Frame:** This section is highlighted with a yellow box. It contains a dropdown menu for "PMF" with the following options: "Optional" (selected), "Disabled", "Optional", and "Required".
- Auth Key Mgmt:** Includes checkboxes for 802.1x, PSK, Easy-PSK, CCKM, FT + 802.1x, FT + PSK, 802.1x-SHA256, and PSK-SHA256.
- MPSK Configuration:** Includes a checkbox for "Enable MPSK".

How to configure Client Analytics?

WLANs | Advanced

Advertise Support



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller configuration interface. The 'Edit WLAN' window is open, displaying various configuration options. The 'Device Analytics' section is highlighted with a yellow box, showing the following settings:

- Advertise Support:
- Advertise PC Analytics Support:
- Share Data with Client:

Other visible settings include:

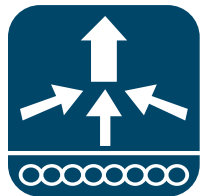
- BSS Max Idle Protected:
- Directed Multicast Service:
- 11ax:
- Enable 11ax:
- Downlink OFDMA:
- Uplink OFDMA:
- Downlink MU-MIMO:
- Uplink MU-MIMO:
- BSS Target Wake Up Time:

The interface also shows a sidebar with navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The 'Update & Apply to Device' button is visible at the bottom right of the configuration window.



How to support the Clients? - optional

WLANs | Advanced 802.11k/v and 'Share Data' with client



The screenshot displays the 'Edit WLAN' configuration page in the Cisco Catalyst 9800-CL Wireless Controller. The page is divided into several sections:

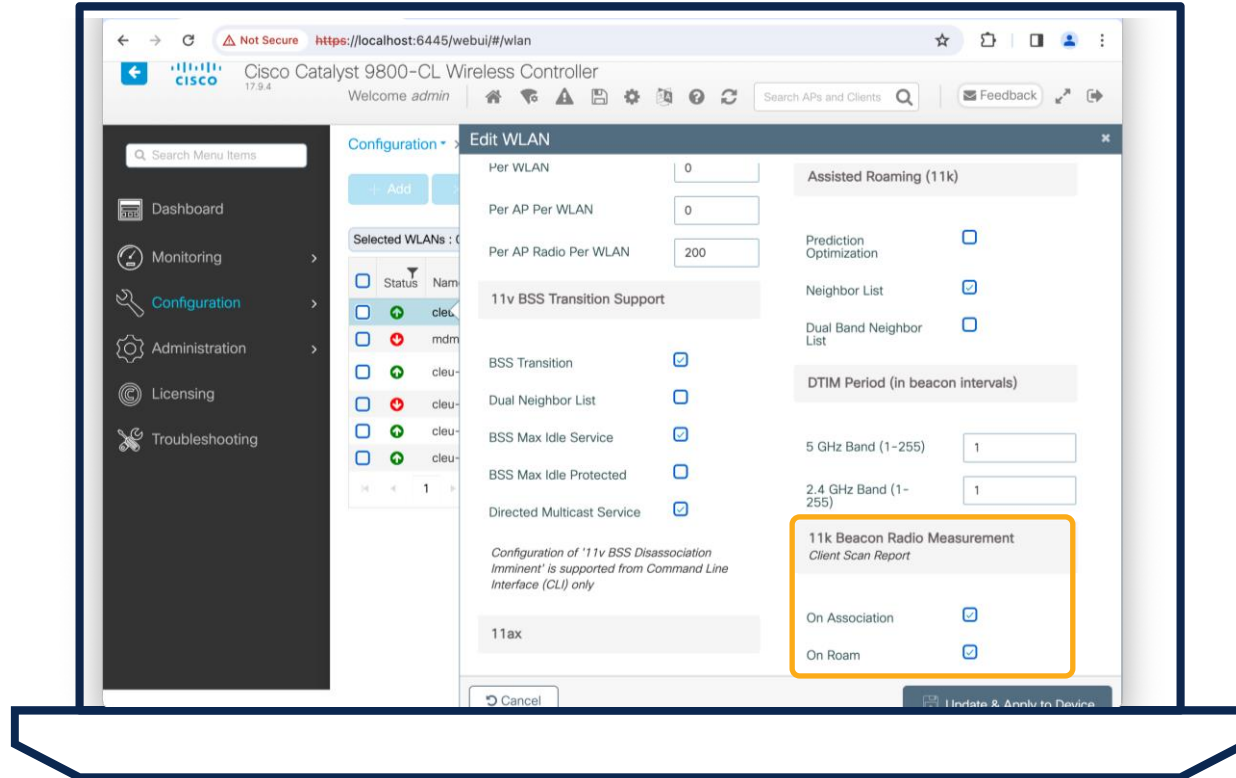
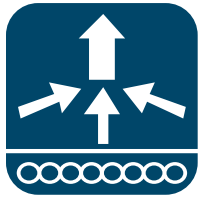
- Configuration:** Includes fields for 'Per WLAN' (0), 'Per AP Per WLAN' (0), and 'Per AP Radio Per WLAN' (200).
- 11v BSS Transition Support:** A section highlighted with an orange box, containing the following options:
 - BSS Transition:
 - Dual Neighbor List:
 - BSS Max Idle Service:
 - BSS Max Idle Protected:
 - Directed Multicast Service:
- Assisted Roaming (11k):** A section highlighted with an orange box, containing the following options:
 - Prediction Optimization:
 - Neighbor List:
 - Dual Band Neighbor List:
- Device Analytics:** Contains options for 'Advertise Support' (checked), 'Advertise PC Analytics Support' (checked), and 'Share Data with Client' (checked, highlighted with an orange box).
- 11k Beacon Radio Measurement Client Scan Report:** A section at the bottom right.

At the bottom of the page, there is a '11ax' label and an 'Update & Apply to Device' button.

How to get the Client view? – optional

WLANs | Advanced

Receive Radio Measurement



The screenshot displays the Cisco Catalyst 9800-CL Wireless Controller web interface. The main content area is titled "Edit WLAN" and shows various configuration options for a WLAN. A table lists "Selected WLANs" with columns for "Status" and "Name". The "11k Beacon Radio Measurement Client Scan Report" section is highlighted with an orange box, showing the following options:

- On Association
- On Roam



How to get the Client view? - optional

```
C9800#
```

```
! Required Config
```

```
network-assurance enable
```

```
wlan ciscolive 24 ciscolive
```

```
shutdown
```

```
mbo
```

```
no shutdown
```

```
! How to request Client report
```

```
wireless client mac-address H.H.H scan-report once mode ...
```

```
! Display Result
```

```
show wireless client mac-address H.H.H detail | sec Scan
```

Tips and Tricks – Application Assurance / Client Analytics



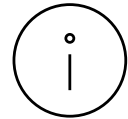
Application Assurance configuration temporarily shuts the policy profiles

```
C9800(config)#wireless profile policy xxx
shutdown
ipv4 flow monitor avc_ipv4_assurance input
ipv4 flow monitor avc_ipv4_assurance_dns input
ipv4 flow monitor avc_ipv4_assurance_rtp input
...
no shutdown
```

Tips and Tricks – Application Assurance / Client Analytics



Application Assurance configuration temporarily shuts the policy profiles



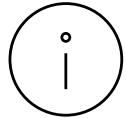
Application Assurance also enables DNS Service monitoring (on Local Mode with 17.10 or higher)

```
C9800(config)#wireless profile policy xxx
shutdown
ipv4 flow monitor avc_ipv4_assurance input
ipv4 flow monitor avc_ipv4_assurance_dns input
ipv4 flow monitor avc_ipv4_assurance_rtp input
...
no shutdown
```

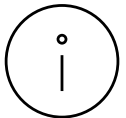
Tips and Tricks – Application Assurance / Client Analytics



Application Assurance configuration temporarily shuts the policy profiles



Application Assurance also enables DNS Service monitoring (on Local Mode with 17.10 or higher)



Flex Connect supports now Application Experience (Loss, Jitter, Delay)

```
C9800(config)#wireless profile policy PP4IoT
no central association
no central dhcp
no central switching
ipv4 flow monitor avc_ipv4_assurance_v9 input
ipv4 flow monitor avc_ipv4_assurance_rtp_v9 i
...
```

Agenda

CISCO *Live!*

- Get insights with AIOps
 - Basics you should configure
 - Add-Ons you can leverage
 - On-Demand Tools that ease your life
 - The platform advantage

Network / Device 360

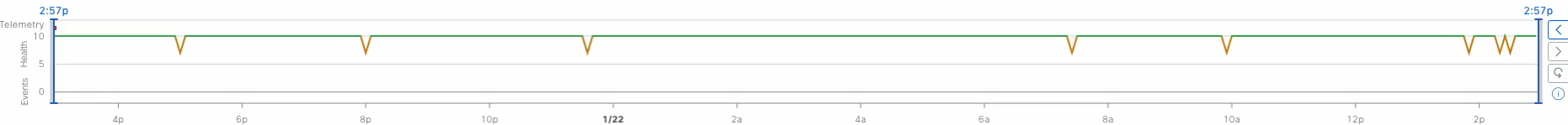
AP ap-cleu-ams1 [View Device Details](#)

Download

Run OTA Capture

24 Hours

Intelligent Capture



Telemetry Status

Jan 21, 2024 2:57 PM - Jan 22, 2024 2:57 PM

10/10⁰ DEVICE DETAILS

Connected To WLC: [cisco-wlc-10.cisco.com](#) Model: CW9166I-E Software: 17.9.4.206 Management IP: 10.0.110.212 Location: Global / CLEU24 / EMEA / AMS / RAI / 1st Floor Mode: Local Uptime: 12 days, 20 hours, 35 minutes Capability: Wi-Fi 6E Operational Status: Up

Power Save Mode Capability: Supported [View All Details](#)

- Issues
- Tools
- Physical Neighbor Topology
- Event Viewer
- Device
- RF
- Ethernet

Issues (0) Jan 22, 2024 2:57 PM

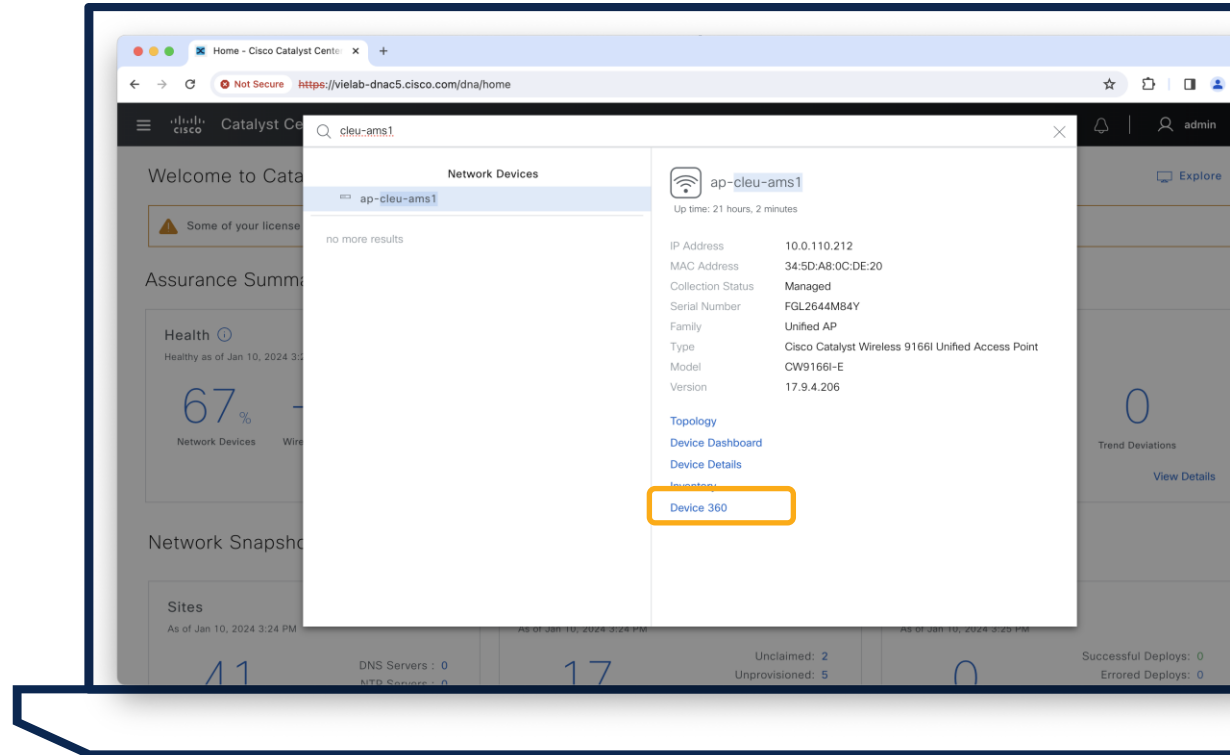
No data to display

Resolved Issues

Ignored Issues

How to enable Spectrum Analysis?

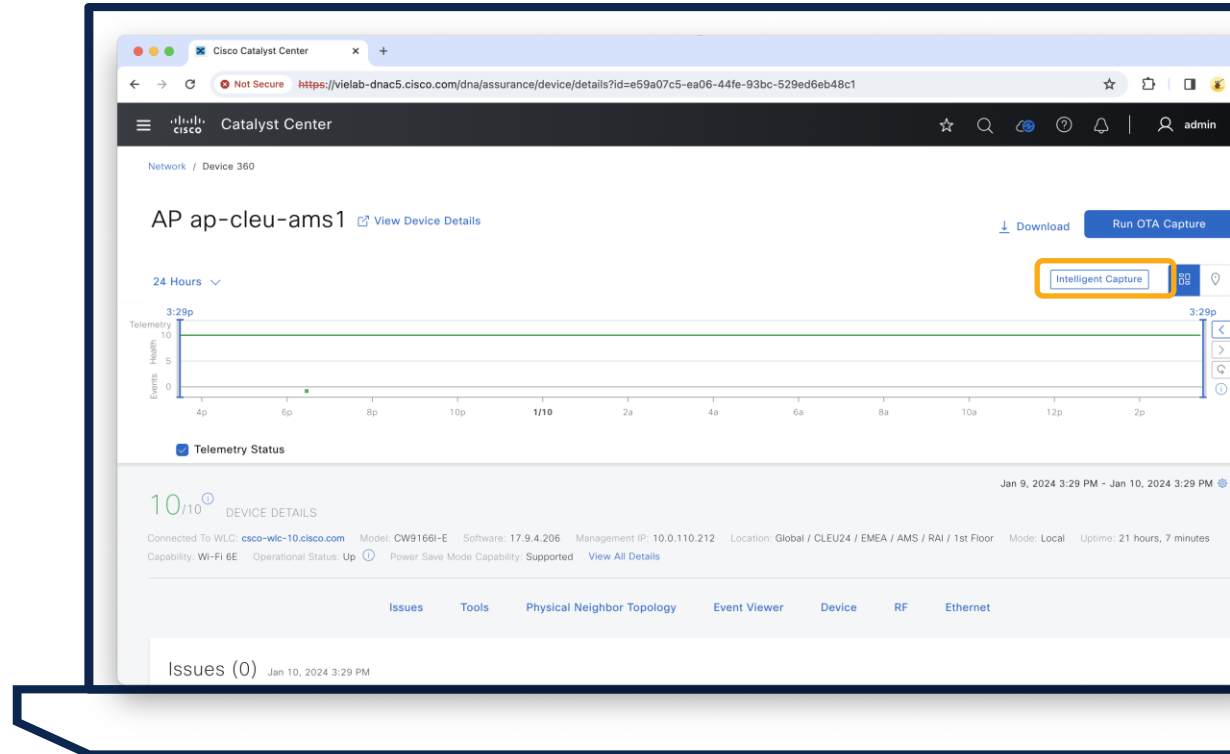
- Go to Accesspoint Device 360 View



The screenshot displays the Cisco Catalyst Center interface. A search bar at the top contains 'cleu-ams1'. Below the search bar, a 'Network Devices' panel shows a list with 'ap-cleu-ams1' selected. To the right, a detailed view for 'ap-cleu-ams1' is shown, including fields for IP Address (10.0.110.212), MAC Address (34:5D:A8:0C:DE:20), Collection Status (Managed), Serial Number (FGL2644M84Y), Family (Unified AP), Type (Cisco Catalyst Wireless 9166I Unified Access Point), Model (CW9166I-E), and Version (17.9.4.206). A yellow box highlights the 'Device 360' link in the 'Inventory' section.

How to enable Spectrum Analysis?

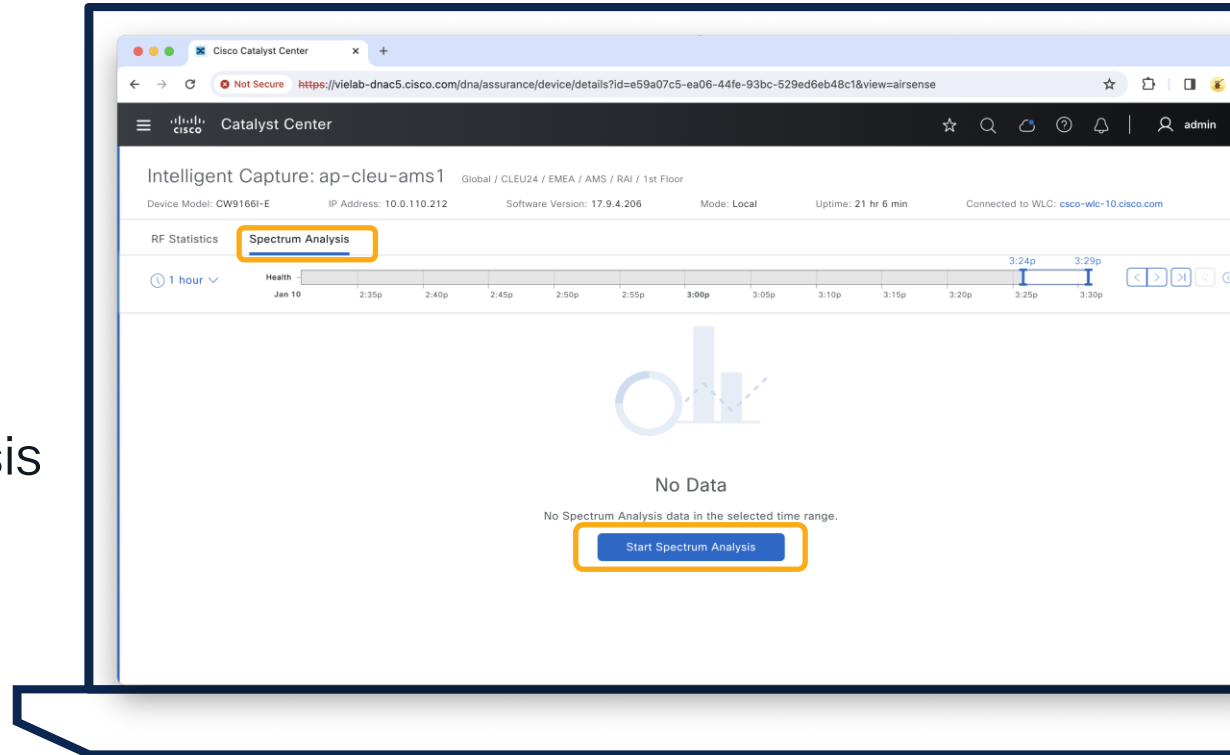
- Go to Accesspoint Device 360 View
- Intelligent Capture



The screenshot displays the Cisco Catalyst Center interface for an Access Point (AP) named 'ap-cleu-ams1'. The page is titled 'Catalyst Center' and shows the 'Device 360' view. A '24 Hours' time range is selected, and a graph shows 'Telemetry Health' over time. A red box highlights the 'Intelligent Capture' button in the top right corner. Below the graph, the 'Telemetry Status' is checked. The 'DEVICE DETAILS' section shows the AP is connected to the WLC 'cisco-wlc-10.cisco.com' and is operational. The 'Issues (0)' section is visible at the bottom.

How to enable Spectrum Analysis?

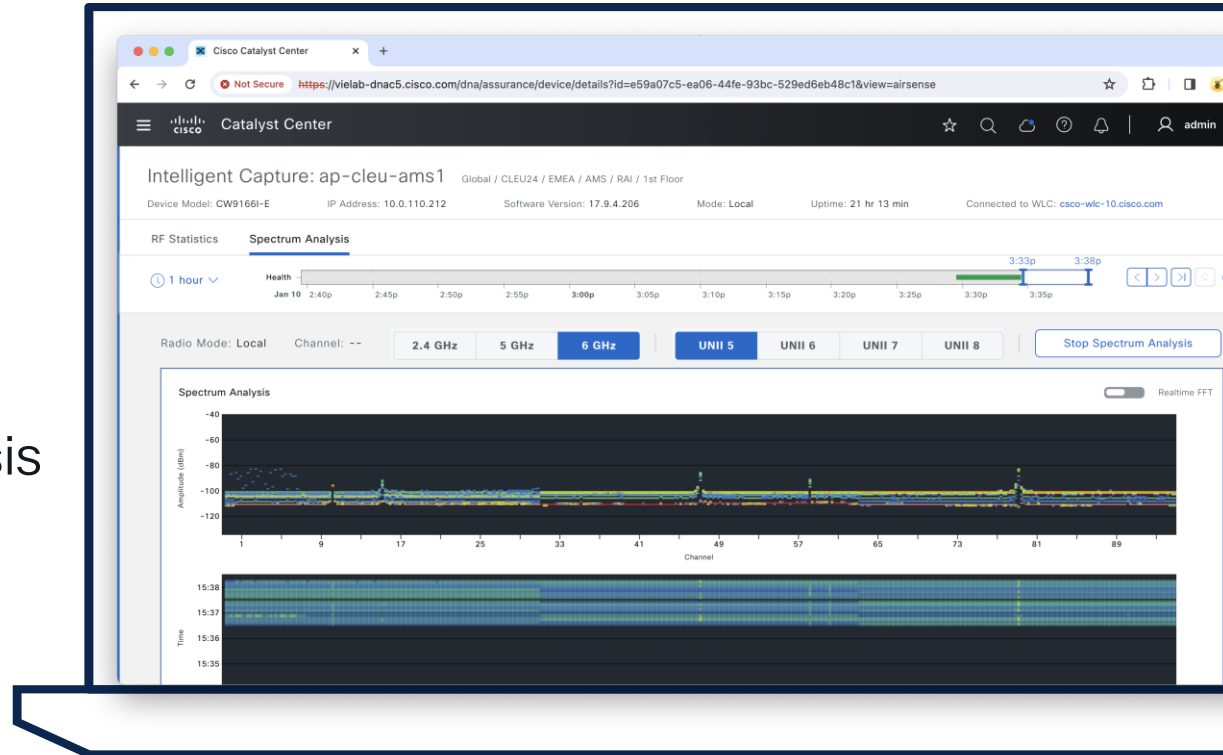
- Go to Accesspoint Device 360 View
- Intelligent Captures
- Start Spectrum Analysis



The screenshot displays the Cisco Catalyst Center web interface. The browser address bar shows the URL: <https://vielab-dnac5.cisco.com/dna/assurance/device/details?id=e59a07c5-aa06-44fe-93bc-529ed6eb48c1&view=airsense>. The page title is "Intelligent Capture: ap-cleu-ams1". Below the title, there is a navigation bar with "RF Statistics" and "Spectrum Analysis" tabs. The "Spectrum Analysis" tab is selected and highlighted with an orange box. Below the tabs, there is a timeline for "Health" on "Jan 10" with a "1 hour" filter. The timeline shows a time range from 2:35p to 3:30p. A blue bar highlights the time range from 3:24p to 3:29p. Below the timeline, there is a "No Data" message: "No Spectrum Analysis data in the selected time range." A blue button labeled "Start Spectrum Analysis" is highlighted with an orange box.

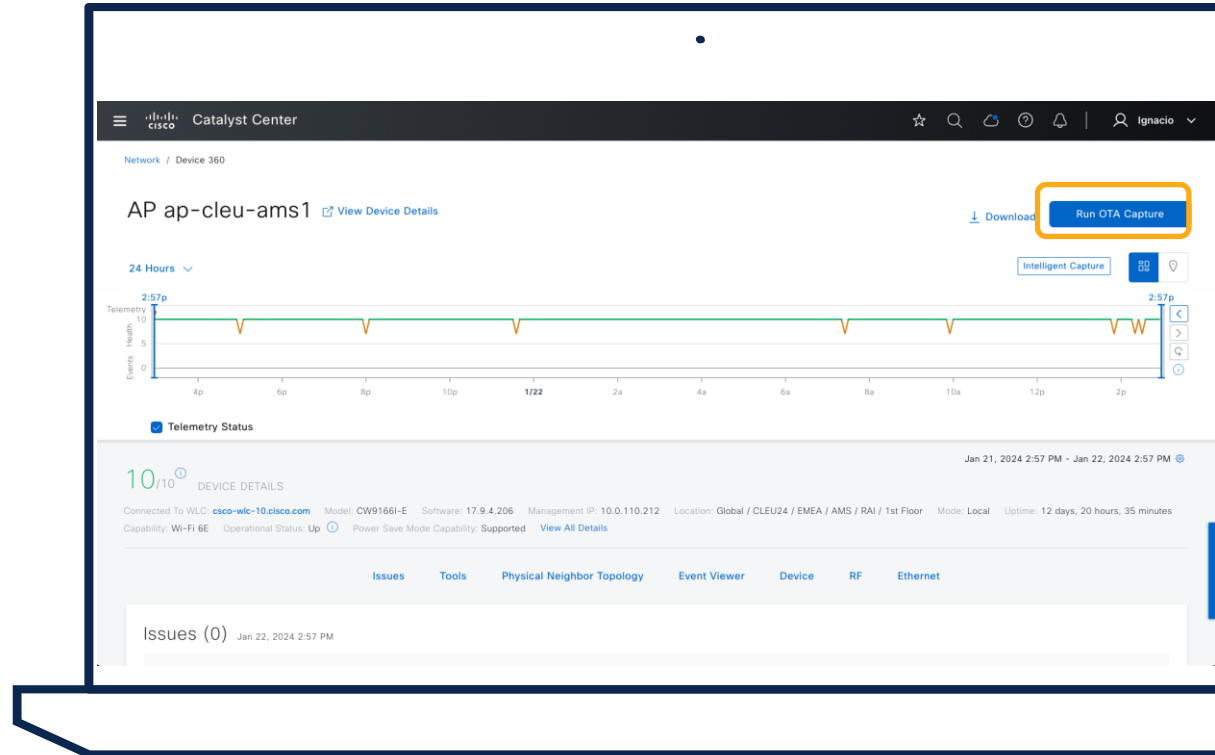
How to enable Spectrum Analysis?

- Go to Accesspoint Device 360 View
- Intelligent Capture
- Start Spectrum Analysis



How to run over the air (OTA) capture?

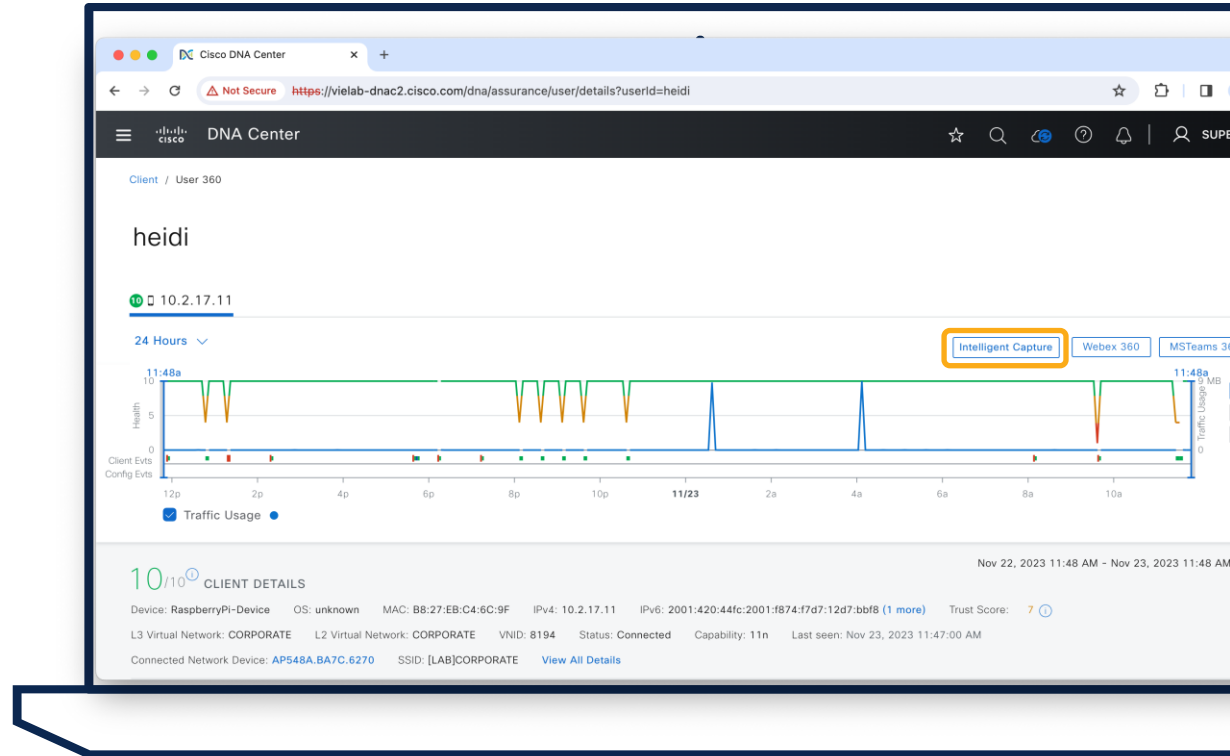
- Go to Accesspoint Device 360 View
- Run OTA Capture
- Select band, radio, channel width and channel



The screenshot displays the Cisco Catalyst Center interface for an Access Point (AP) named 'ap-cleu-ams1'. The 'Run OTA Capture' button is highlighted with an orange box. Below the button, there is a '24 Hours' time range selector and an 'Intelligent Capture' button. A line graph shows the Telemetry Status over time, with a green line indicating a healthy status and a red line indicating a degraded status. The graph shows several instances of degraded status, with the most recent one occurring at 2:57 PM on Jan 22, 2024. Below the graph, the 'DEVICE DETAILS' section shows the AP's status as 'Up' and provides various technical specifications such as Model (CW91661-E), Software (17.9.4.206), and Location (Global / CLEU24 / EMEA / AMS / RAI / 1st Floor). The 'Issues (0)' section is also visible at the bottom of the interface.

How to run client Live Packet Capture?

- Go to Client 360 View
> Intelligent Capture



How to run client Live Packet Capture?

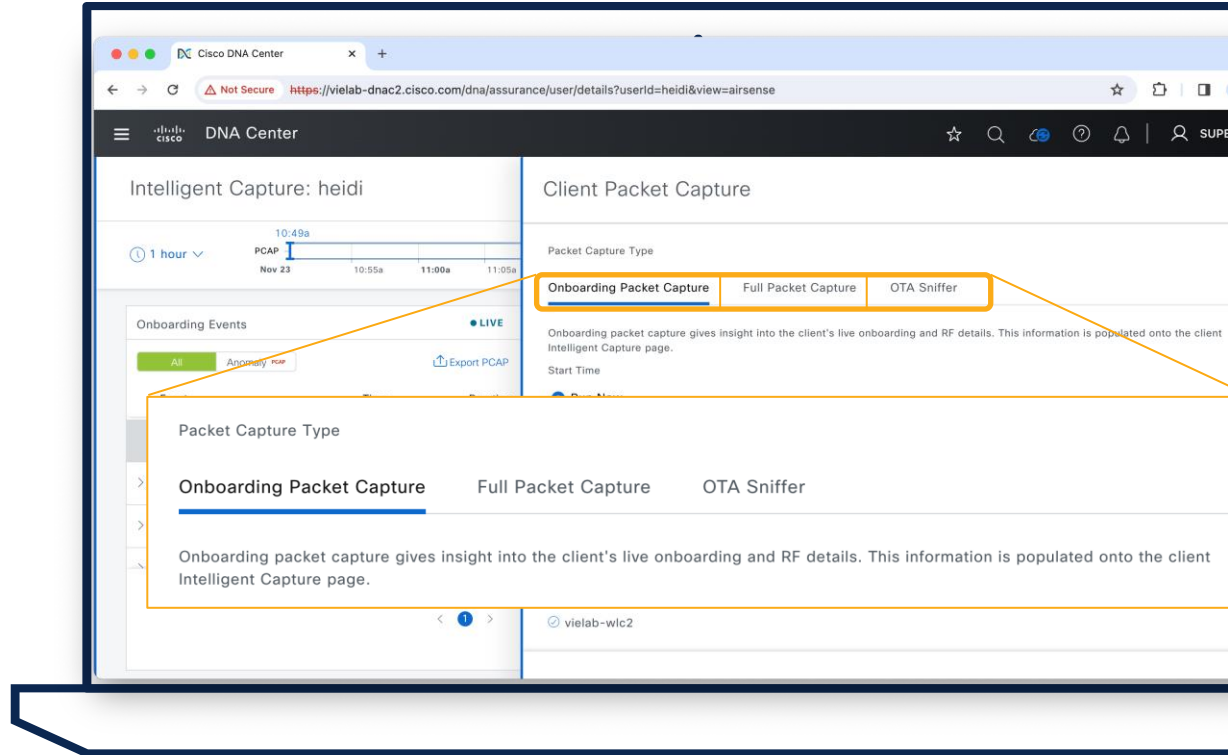
- Go to Client 360 View > Intelligent Capture
- Run Packet Capture

The screenshot displays the Cisco DNA Center web interface for Intelligent Capture. The browser address bar shows the URL: <https://vielab-dnac2.cisco.com/dna/assurance/user/details?userId=heidi&view=airsense>. The page title is "Intelligent Capture: heidi". A "Run Packet Capture" button is visible in the top right corner. Below the title, there is a timeline for the capture session, currently set to "1 hour" and showing a range from 10:49a to 11:49a on Nov 23. The main content area is divided into two panels. The left panel, titled "Onboarding Events", shows a table of events with columns for "Event", "Time", and "Duration". The right panel, titled "Client Location", shows a floor plan map with a heatmap overlay and two access points labeled "AP00A2.8902.4910" and "AP548A.BA7C.6270". A tooltip over the map indicates "Live track not available".

Event	Time	Duration
Onboarding (8)	11:33:00 AM	3,142 ms
Onboarding (1)	11:31:58 AM	
Onboarding (1)	11:31:49 AM	

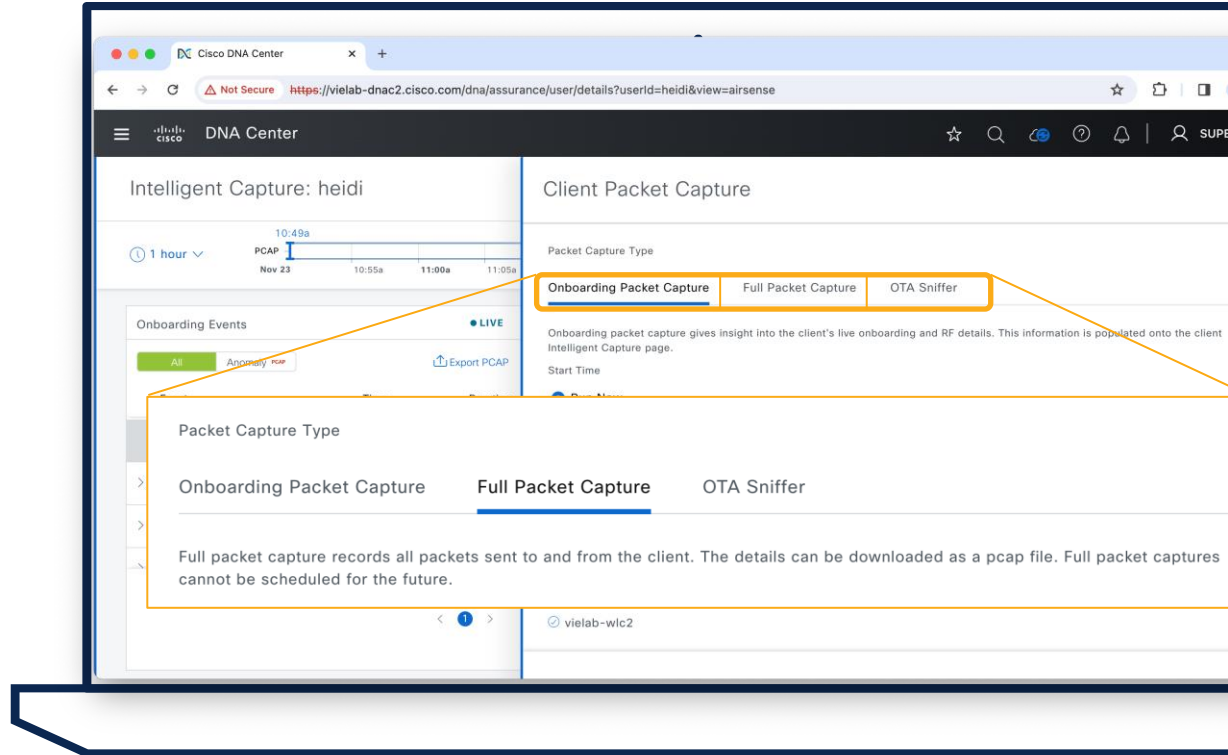
How to run client Live Packet Capture?

- Go to Client 360 View > Intelligent Capture
- Run Packet Capture
- Select Packet Capture Type



How to run client Live Packet Capture?

- Go to Client 360 View > Intelligent Capture
- Run Packet Capture
- Select Packet Capture Type



How to run client Live Packet Capture?

- Go to Client 360 View > Intelligent Capture
- Run Packet Capture
- Select Packet Capture Type

The screenshot displays the Cisco DNA Center interface for configuring a Client Packet Capture. The main heading is 'Client Packet Capture'. Under the 'Packet Capture Type' section, three options are available: 'Onboarding Packet Capture', 'Full Packet Capture', and 'OTA Sniffer'. The 'OTA Sniffer' option is currently selected. Below this, a descriptive text states: 'Over The Air Capture records all radio signals heard on a specified channel. The details can be downloaded from a pcap file.' A 'Select Access Points' section is visible at the bottom, showing a search bar and a list of access points, with 'vielab-wlc2' being one of the entries. The interface also includes a timeline for 'Intelligent Capture: heidi' and a 'Start Time' field.



Packet Capture Types

- Onboarding Packet Capture
 - At AP radio level
 - No client impact
 - Onboarding Packets for a client (EAP, ICMP, DNS,...)

91	10.0.120.40	10.0.120.254	ICMP	2023-12-20 1
92	Cisco_05:74:4f	ca:e2:16:ad:5f:13	802.11	2023-12-20 1
93	ca:e2:16:ad:5f:13	Cisco_05:74:4f	802.11	2023-12-20 1
94	10.0.120.40	144.254.71.184	DNS	2023-12-20 1
95	10.0.120.40	144.254.71.184	DNS	2023-12-20 1
96	10.0.120.254	10.0.120.40	ICMP	2023-12-20 1
97	10.0.120.36	10.0.120.40	ICMP	2023-12-20 1
98	10.0.120.40	10.0.120.36	ICMP	2023-12-20 1
99	10.0.120.36	10.0.120.40	ICMP	2023-12-20 1
100	10.0.120.40	10.0.120.36	ICMP	2023-12-20 1

```
> Frame 96: 1440 bytes on wire (11520 bits), 1440 bytes captured (11520) on interface 0
> Radiotap Header v0, Length 38
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .....F.
> Logical-Link Control
> Internet Protocol Version 4, Src: 10.0.120.254, Dst: 10.0.120.40
> Internet Control Message Protocol
```

Packet Capture Types

- Onboarding Packet Capture
 - At AP radio level
 - No client impact
 - Onboarding Packets for a client (EAP, ICMP, DNS,...)
- Full Packet Capture
 - At AP radio level
 - No client impact
 - All data packets for a client
 - APs: C9130/C9136/CW9166

7597	74.125.100.234	10.0.120.40	TCP	QoS Data
7598	74.125.100.234	10.0.120.40	TCP	QoS Data
7599	74.125.100.234	10.0.120.40	TCP	QoS Data
7600	74.125.100.234	10.0.120.40	TCP	QoS Data
7601	74.125.100.234	10.0.120.40	TCP	QoS Data
7602	74.125.100.234	10.0.120.40	TCP	QoS Data
7603	ca:e2:16:ad:5f:1...	Cisco_05:74:4f (...	802.11	802.11 Block Ack
7604	74.125.100.234	10.0.120.40	TLSv1.2	QoS Data
7605	ca:e2:16:ad:5f:1...	Cisco_05:74:4f (...	802.11	802.11 Block Ack
7606	ca:e2:16:ad:5f:1...	Cisco_05:74:4f (...	802.11	Request-to-send
7607		ca:e2:16:ad:5f:1...	802.11	Clear-to-send
7608	ca:e2:16:ad:5f:13	Cisco_f3:d7:9f	802.11	QoS Data
7609	Cisco_05:74:4f (...	ca:e2:16:ad:5f:1...	802.11	802.11 Block Ack
7610	74.125.100.234	10.0.120.40	TCP	QoS Data

```

> Frame 7604: 1362 bytes on wire (10896 bits), 1362 bytes captured (10896 bits)
> Radiotap Header v0, Length 38
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .....F.
> Logical-Link Control
> Internet Protocol Version 4, Src: 74.125.100.234, Dst: 10.0.120.40
> Transmission Control Protocol, Src Port: 443, Dst Port: 65159, Seq: 3481122, Ack: 65159
> [14 Reassembled TCP Segments (16406 bytes): #7589(1233), #7590(1238), #7591(1233), #7592(1238), #7593(1233), #7594(1238), #7595(1233), #7596(1238), #7597(1233), #7598(1238), #7599(1233), #7600(1238), #7601(1233), #7602(1238)]
> Transport Layer Security
  
```

Packet Capture Types

- OTA Sniffer
 - At AP radio level
 - Turns radio into Sniffer mode, no client serving capability
 - Captures all packets on specific channel
 - Requires 17.11 and 2.3.7

29637	Cisco_2f:dd:e2	Broadcast	802.11	Beacon frame
29638	Cisco_b3:e6:99	PVST+	802.11	Data
29639	Apple_3d:39:07	ca:e2:16:ad:5f:13	802.11	QoS Data
29640	ca:e2:16:ad:5f:1...	Cisco_05:74:40 (...)	802.11	802.11 Block Ack
29641	ca:e2:16:ad:5f:1...	Cisco_05:74:40 (...)	802.11	Request-to-send
29642		ca:e2:16:ad:5f:1...	802.11	Clear-to-send
29643	ca:e2:16:ad:5f:13	Apple_3d:39:07	802.11	QoS Data
29644	Cisco_05:74:40 (...)	ca:e2:16:ad:5f:1...	802.11	802.11 Block Ack
29645	Cisco_30:0c:e2	Cisco_e3:58:66	802.11	Probe Response
29646		Cisco_30:0c:e2 (...)	802.11	Acknowledgement
29647	Cisco_2f:dd:e2	Cisco_e3:58:66	802.11	Probe Response
29648	Cisco_2f:dd:e2	Cisco_e3:58:66	802.11	Probe Response
29649	Cisco_2f:dd:e2	Cisco_e3:58:66	802.11	Probe Response

```

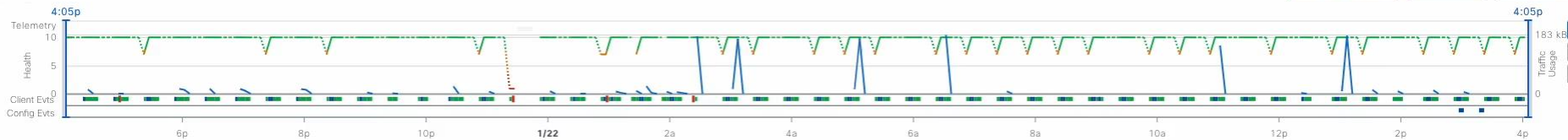
> Frame 29643: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .p.....T
> Data (100 bytes)
  
```

Client / Client 360

sen-cleu-001

24 Hours ▾

Intelligent Capture Webex 360 MSTeams 360



Data: Telemetry Status Traffic Usage

10/10 CLIENT DETAILS

Jan 21, 2024 4:05 PM - Jan 22, 2024 4:05 PM

Device: Cisco-Device OS: -- MAC: 0C:75:BD:0D:78:B1 IPv4: 10.0.120.43 IPv6: fe80::e75:bdf:fe0d:78b1 Trust Score: -- L3 Virtual Network: -- L2 Virtual Network: -- VLAN ID: 120 Status: Connected Capability: 11ac Last seen: Jan 22, 2024 4:02:00 PM

Connected Network Device: [ap-cleu-ams1](#) SSID: cleu-iot [View All Details](#)

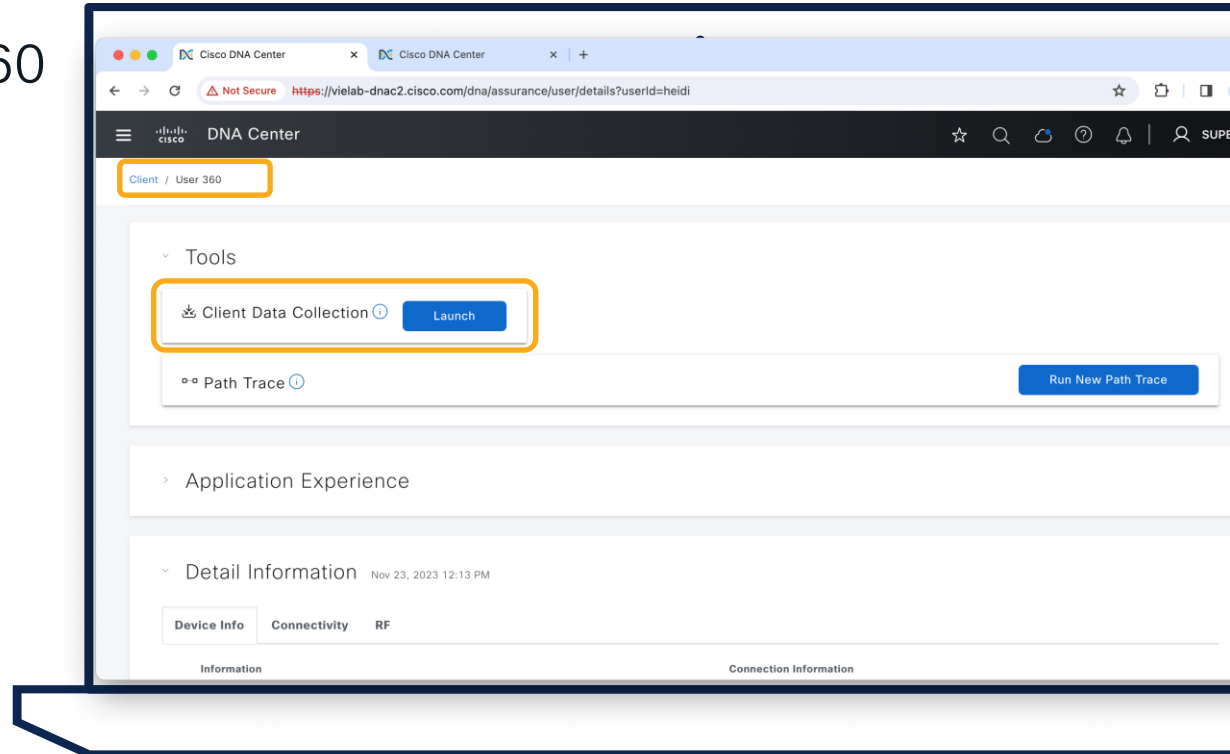
[Issues](#) [Onboarding](#) [Event Viewer](#) [Tools](#) [Application Experience](#) [Device Info](#) [Connectivity](#) [RF](#)

Summary Jan 21, 2024 4:05 PM - Jan 22, 2024 4:05 PM

- Onboarding failed during Authentication (2 out of 4) with multiple failure reasons
- Onboarding failed during Association (1 out of 4), due to 'WLAN Change' (1)
- Onboarding failed during DHCP (1 out of 4), due to 'Client Connect Timeout' (1)
- Poor Wi-Fi experience - low SNR 80.0% of times

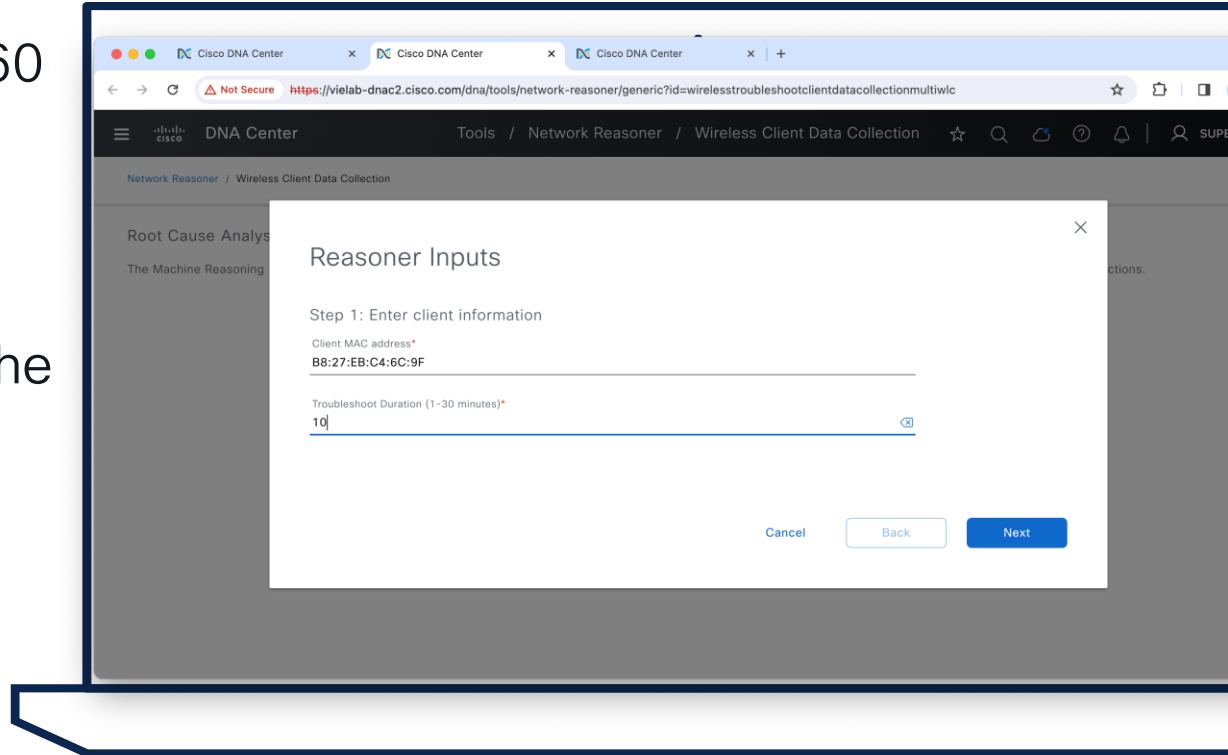
How to collect AP/Client Wireless data?

- Go to Device/Client 360 Tools section



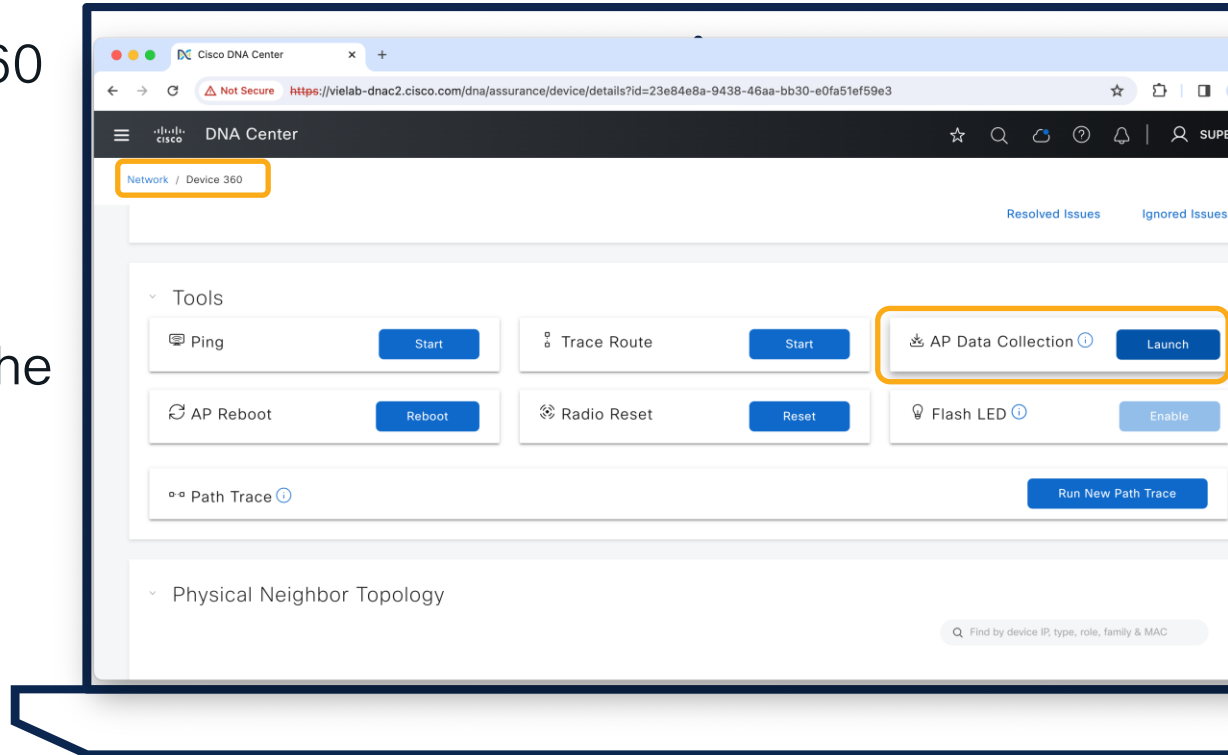
How to collect AP/Client Wireless data?

- Go to Device/Client 360 Tools section
- Launch the MRE workflow and collect the data



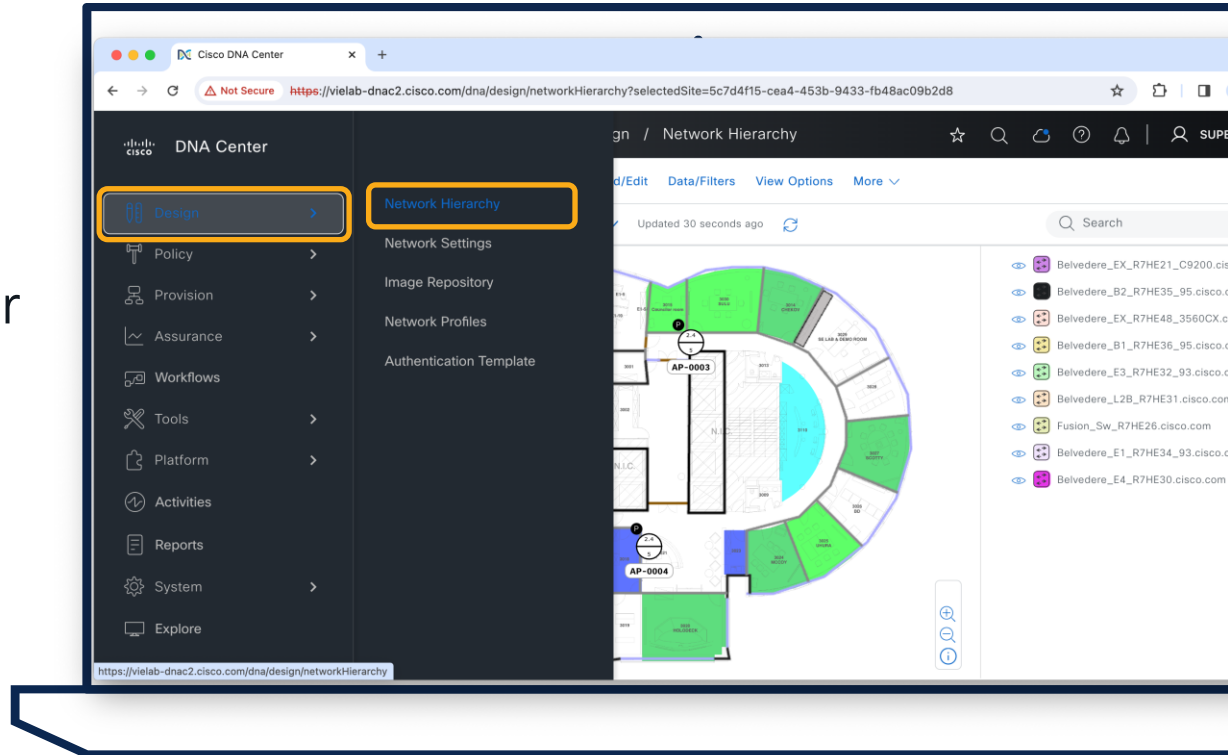
How to collect AP/Client Wireless data?

- Go to Device/Client 360 Tools section
- Launch the MRE workflow and collect the data



How to plan Wireless Coverage?

- Go to Design Network Hierarchy
- Select the proper Floor and Add/Edit



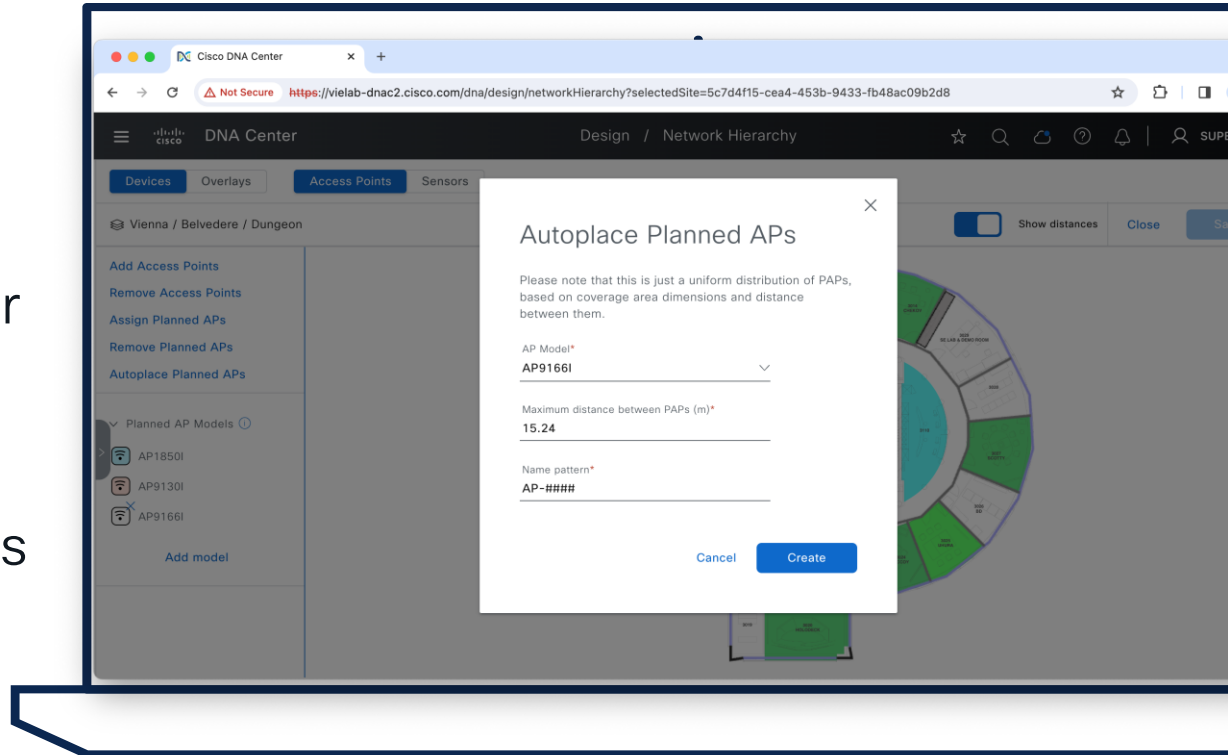
How to plan Wireless Coverage?

- Go to Design Network Hierarchy
- Select the proper Floor and Add/Edit
- Autoplace Planned APs

The screenshot displays the Cisco DNA Center web interface. The browser address bar shows the URL: <https://vielab-dnac2.cisco.com/dna/design/networkHierarchy?selectedSite=5c7d4f15-cea4-453b-9433-fb48ac09b2d8>. The page title is "Design / Network Hierarchy". The navigation bar includes "Devices", "Overlays", "Access Points", and "Sensors". The main content area shows a floor plan for "Vienna / Belvedere / Dungeon" with several APs placed on it, labeled "AP-0002", "AP-0003", and "AP-0004". A callout box explains the "Autoplace Planned APs" feature: "Automates Access Points placement to provide optimum Wi-Fi coverage. This feature uses a predictive survey to gather information about the coverage area. Then, using the AP type, antenna pattern, and coverage area information, it calculates the optimum number and placement of the APs and displays them on the floor map." The left sidebar shows a list of "Planned AP Models" including AP1850I, AP9130I, and AP9166I, with the "Autoplace Planned APs" option highlighted in orange.

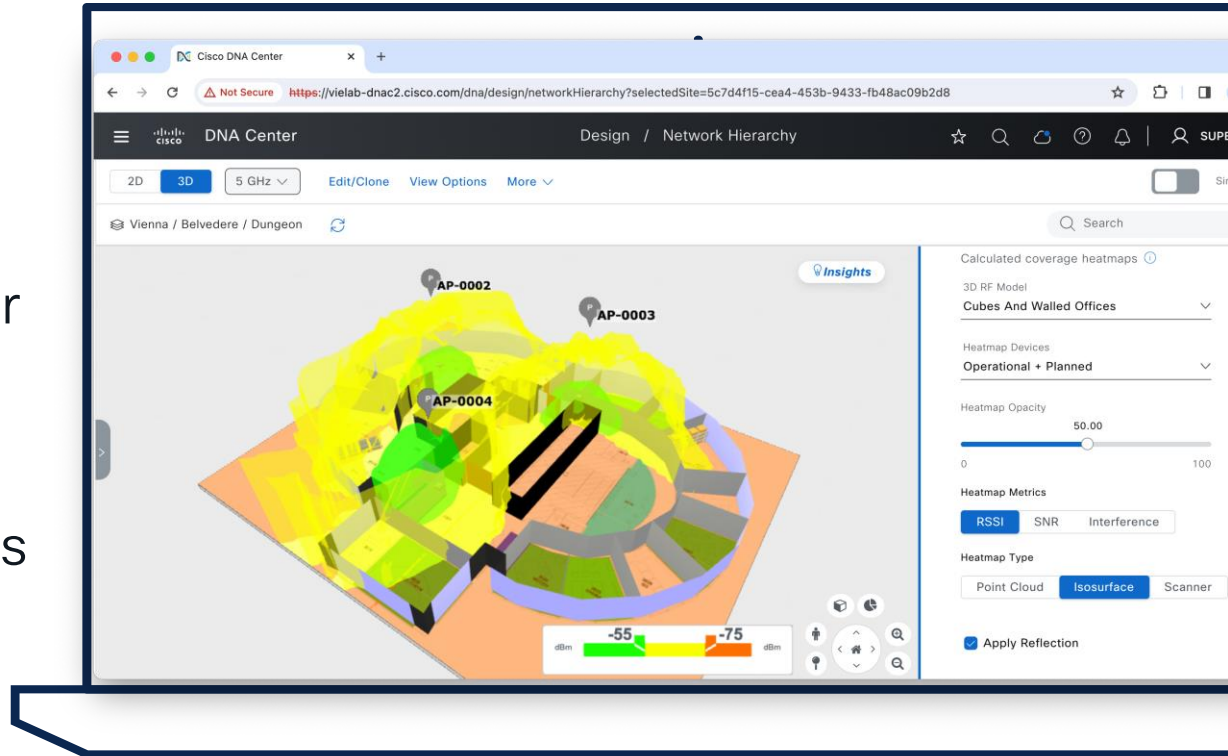
How to plan Wireless Coverage?

- Go to Design Network Hierarchy
- Select the proper Floor and Add/Edit
- Autoplace Planned APs



How to plan Wireless Coverage?

- Go to Design Network Hierarchy
- Select the proper Floor and Add/Edit
- Autoplace Planned APs



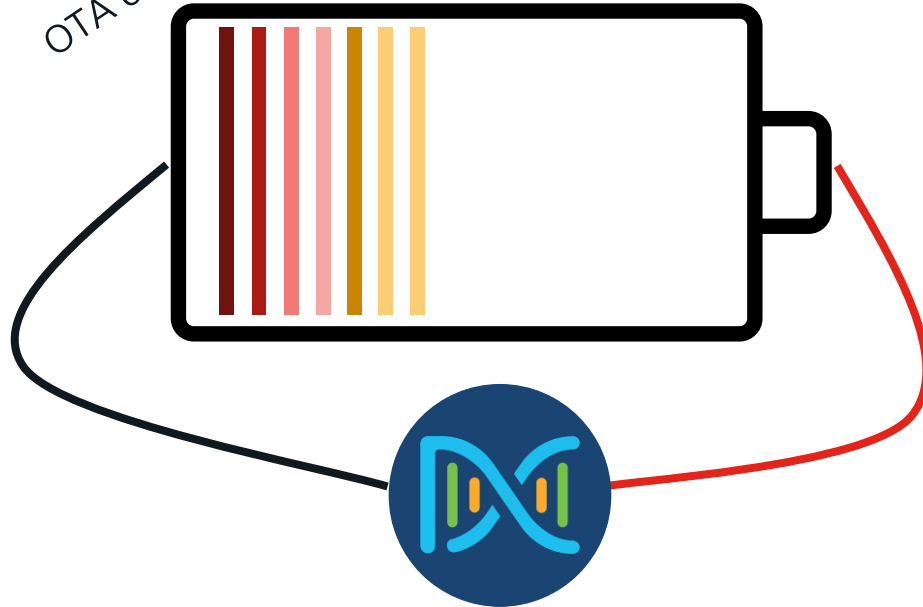
Your Cisco wireless battery

application experience

OTA capture

client analytics

spectrum analysis



Agenda

CISCO *Live!*

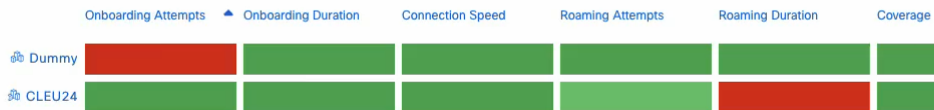
- Get insights with AIOps
 - Basics you should configure
 - Add-Ons you can leverage
 - On-Demand Tools that ease your life
 - The platform advantage

⚠️ The Site Analytics dashboard shows data up to the last 3 hours which is the time needed to process and aggregate the data.

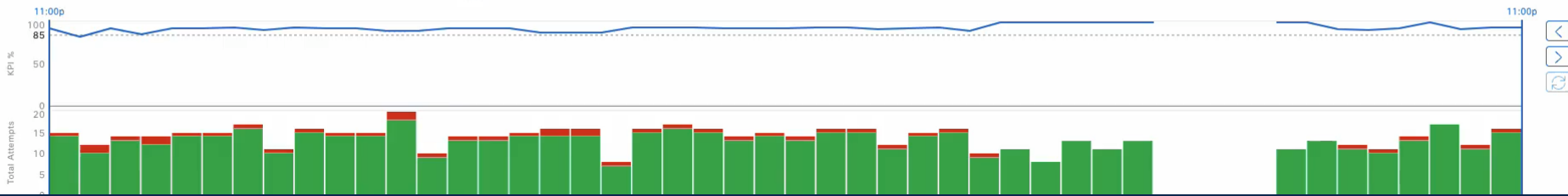
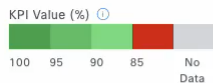
Onboarding Attempts 93% Dummy (3%)	Onboarding Duration 100% CLEU24 (100%)	Connection Speed 99% Dummy (98%)	Roaming Attempts 92% CLEU24 (91%)	Roaming Duration 77% CLEU24 (71%)	Coverage 100% CLEU24 (100%)
---	---	---	--	--	--

Sites (2)

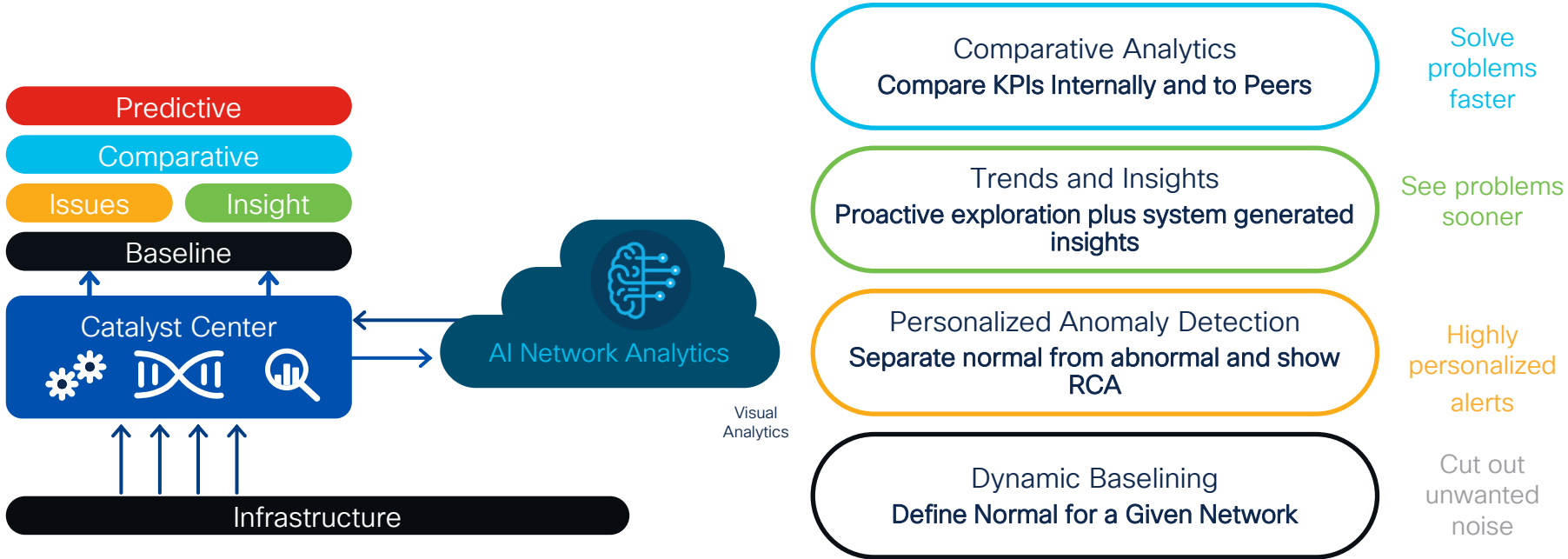
Hierarchical Site View



2 Record(s) 1 - 2



Cisco AI Network Analytics



How to enable Cisco AI Network Analytics?

Enable
Cisco AI Analytics



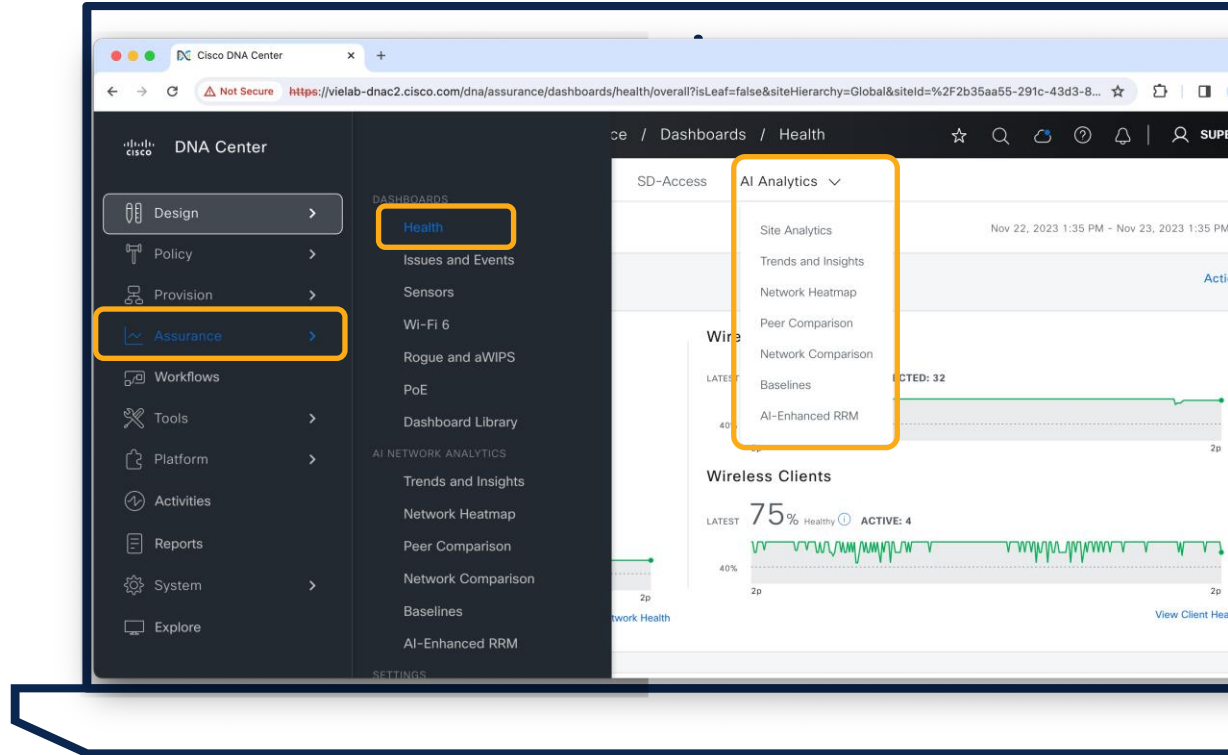
Data Storage

- US East
- Europe (Germany)

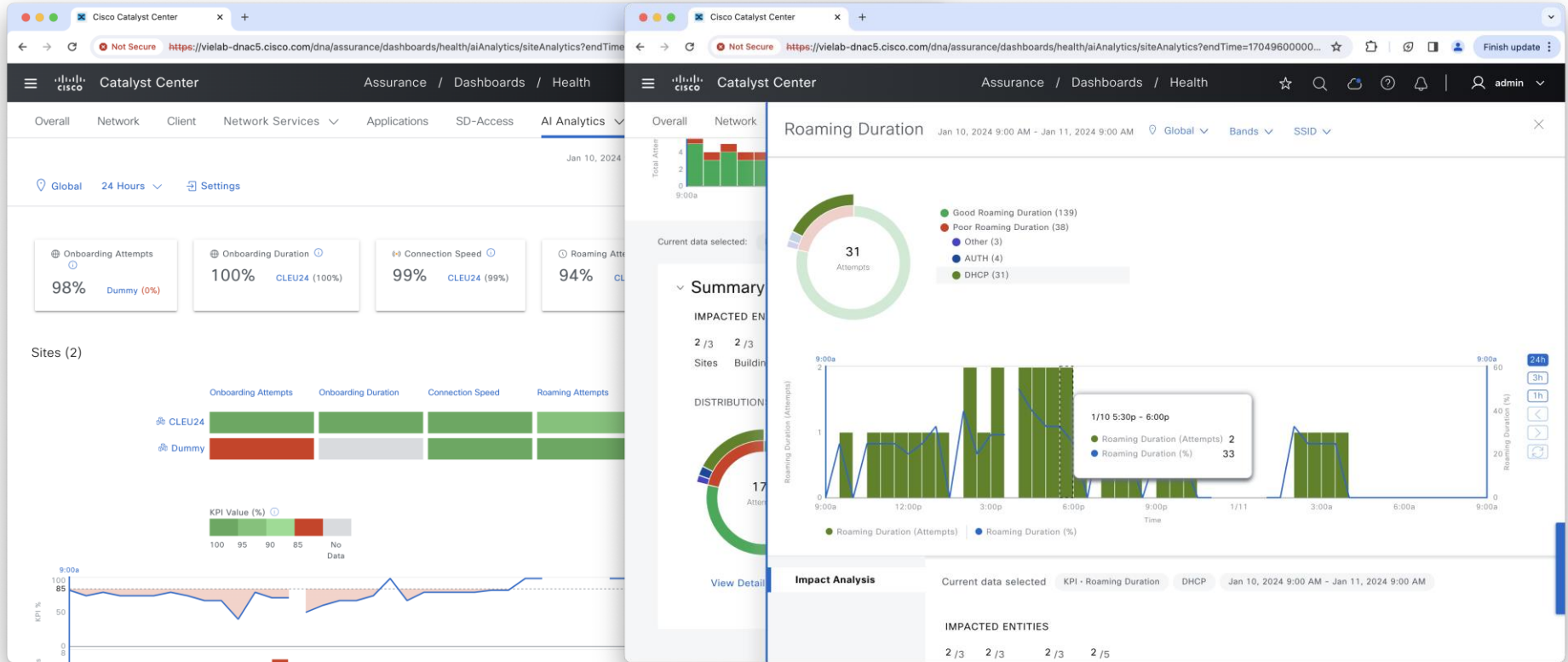
The screenshot shows the Cisco DNA Center interface. The breadcrumb navigation at the top right is 'System / Settings', with 'Settings' highlighted in orange. The left sidebar contains a search bar and a list of navigation items: Cisco Accounts, Device Settings, External Services, Umbrella, Authentication and Policy Servers, Integrity Verification, VManage, IP Address Manager, Cloud Access Login, Cisco AI Analytics (highlighted in orange), Stealthwatch, Talos IP Reputation, Destinations, Cisco Spaces/CMX Servers, and Machine Reasoning Engine. The main content area is titled 'Cisco AI Analytics' and includes a sub-section 'AI Network Analytics' with a description. Below this, there are two toggle switches: 'Enable AI Network Analytics' (checked and highlighted in orange) and 'Enable AI-Enhanced RRM' (checked). At the bottom, there is a section for 'EVENTS ANALYTICS PREVIEW' with a note about Syslog message exports.

How to use Cisco AI Network Analytics?

- Assurance > Health AI Analytics



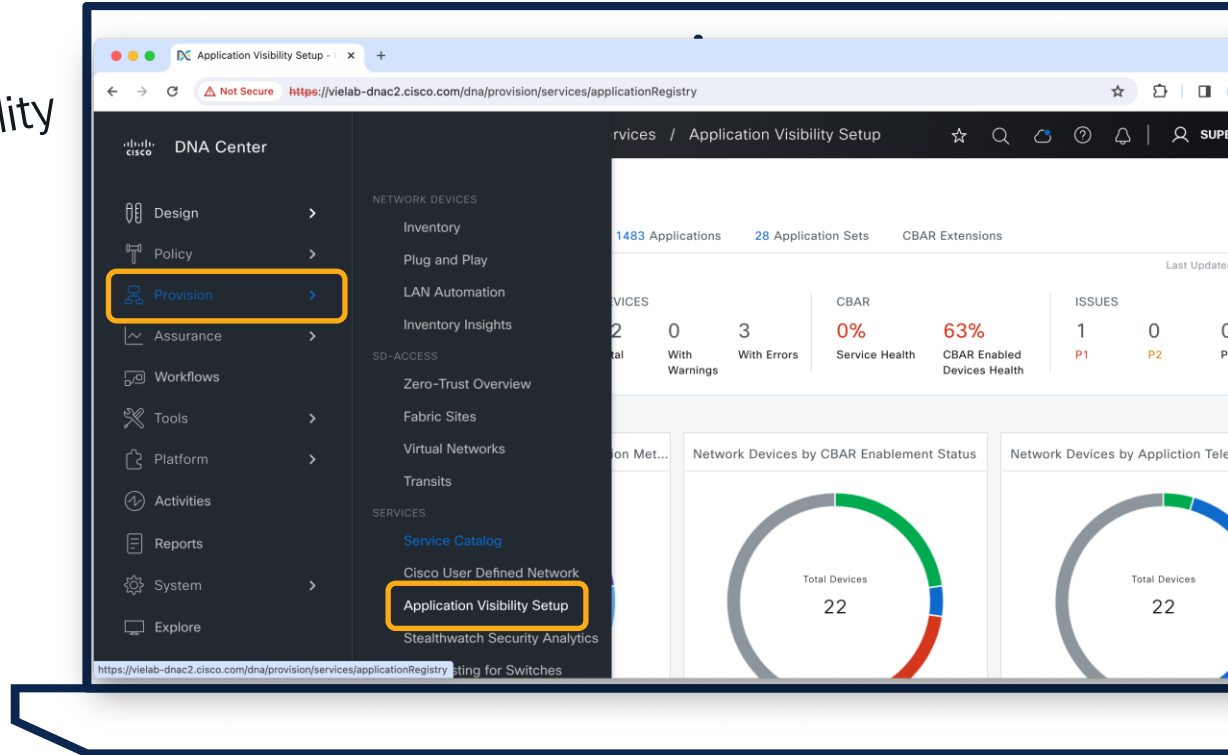
Site Analytics to monitor critical KPIs



How to enable AI Endpoint Analytics?



Configure Application Visibility
aka CBAR

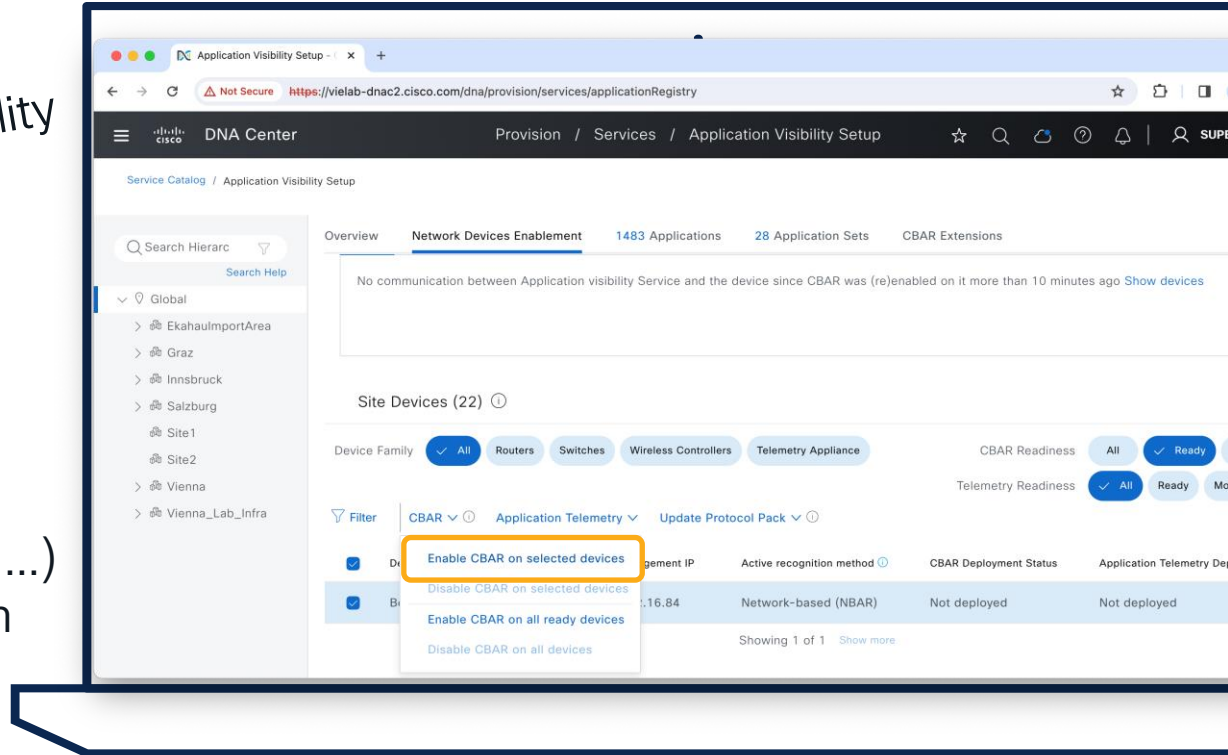


How to enable AI Endpoint Analytics?



Configure Application Visibility
aka CBAR

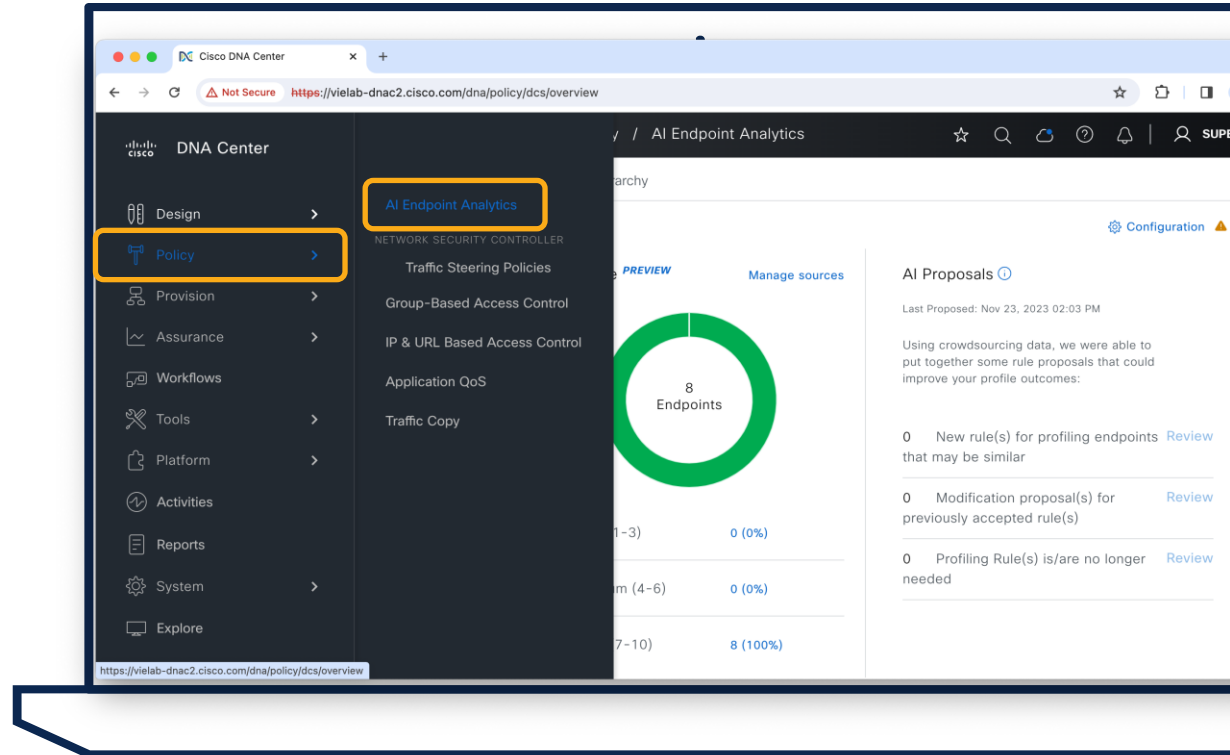
To leverage this workflow for C9800, Wireless (SSIDs,...) need to be *provisioned* from Catalyst Center





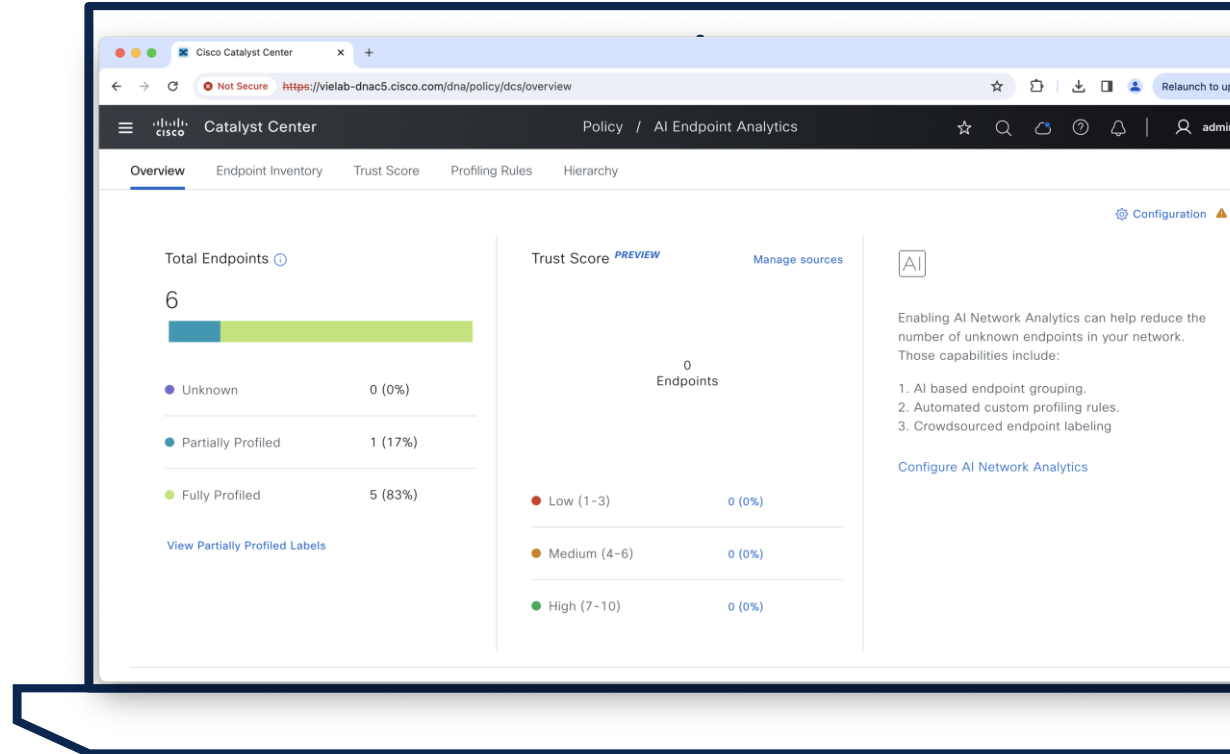
How to use AI Endpoint Analytics?

- Policy > AI Endpoint Analytics



How to use AI Endpoint Analytics?

- Policy > AI Endpoint Analytics
- Verify Endpoints in Overview



The screenshot shows the Cisco Catalyst Center interface for AI Endpoint Analytics. The page is titled "Policy / AI Endpoint Analytics" and has a navigation bar with "Overview", "Endpoint Inventory", "Trust Score", "Profiling Rules", and "Hierarchy". The "Overview" tab is active, showing a "Total Endpoints" section with a bar chart and a table of endpoint statuses. The "Trust Score" section shows "0 Endpoints" and a table of score ranges. A right-hand panel contains an "AI" icon and text explaining the benefits of AI Network Analytics.

Endpoint Status	Count	Percentage
Unknown	0	0%
Partially Profiled	1	17%
Fully Profiled	5	83%

Trust Score Range	Count	Percentage
Low (1-3)	0	0%
Medium (4-6)	0	0%
High (7-10)	0	0%

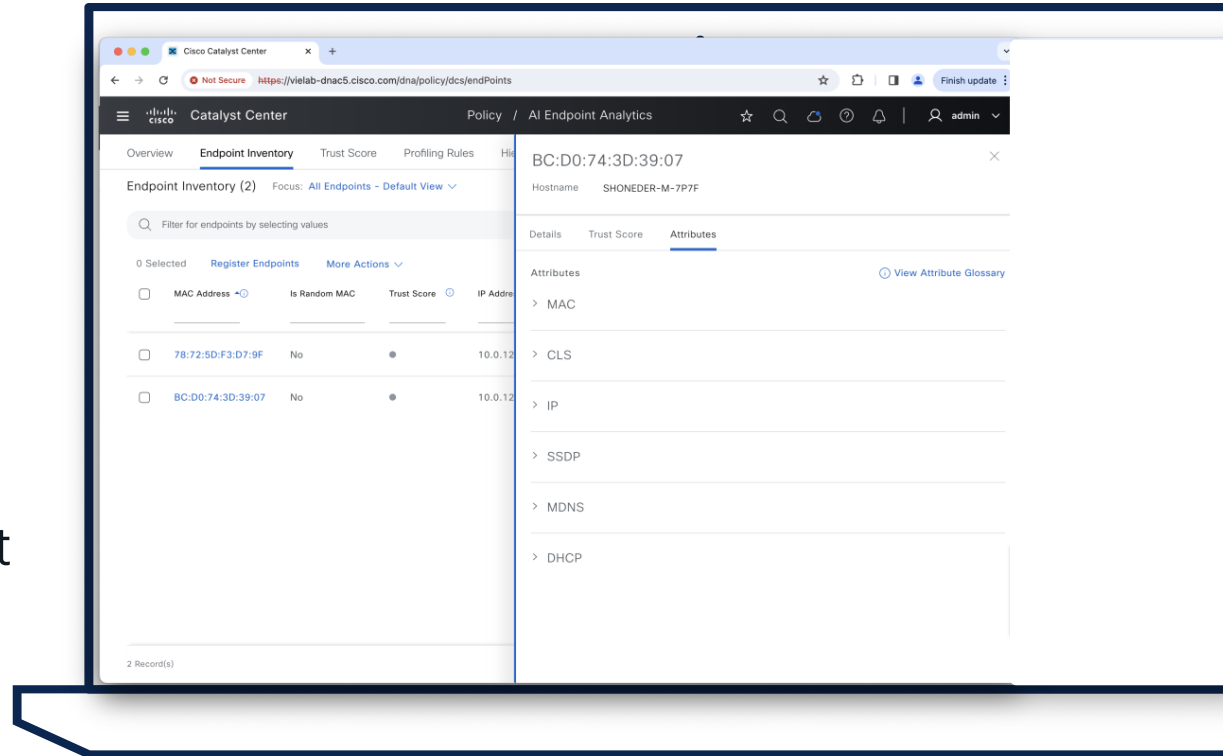
Enabling AI Network Analytics can help reduce the number of unknown endpoints in your network. Those capabilities include:

1. AI based endpoint grouping.
2. Automated custom profiling rules.
3. Crowdsourced endpoint labeling

[Configure AI Network Analytics](#)

How to use AI Endpoint Analytics?

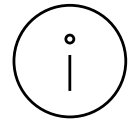
- Policy > AI Endpoint Analytics
- Verify Endpoints in Overview
- Get Details in Endpoint Inventory



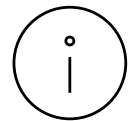
Tips and Tricks – CBAR / AI Endpoint Analytics



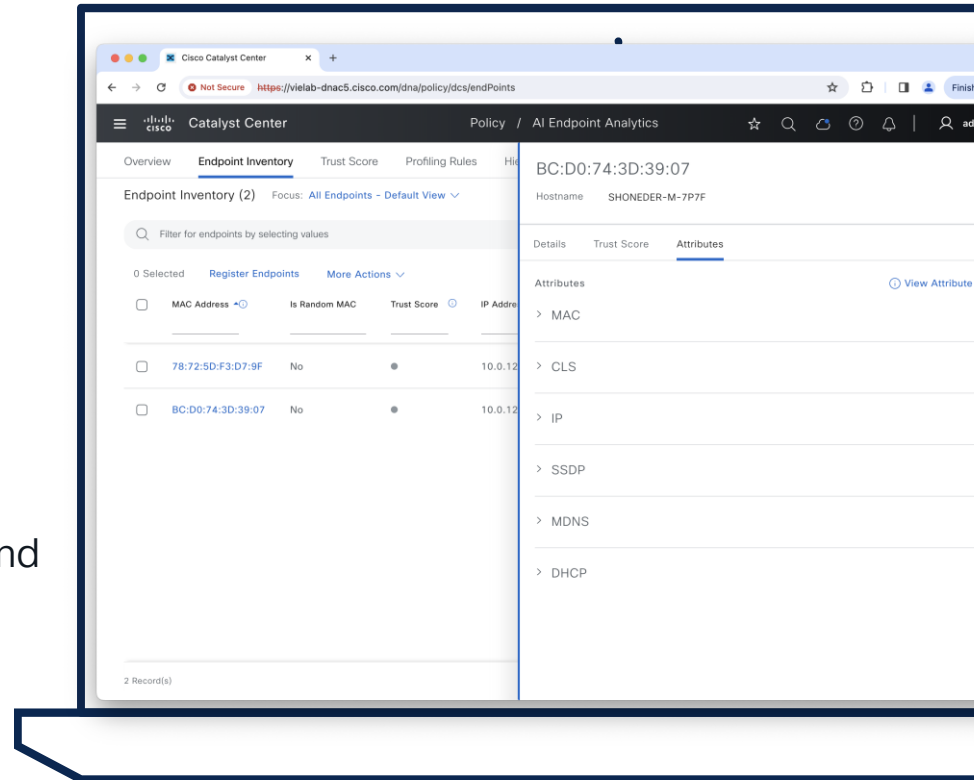
Integration with ISE optional



Application Visibility configuration temporarily shuts the policy profiles



Supported Modes are Local Mode and FlexConnect Mode (>17.6)



Have you heard of AI-RRM (radio resource management)?

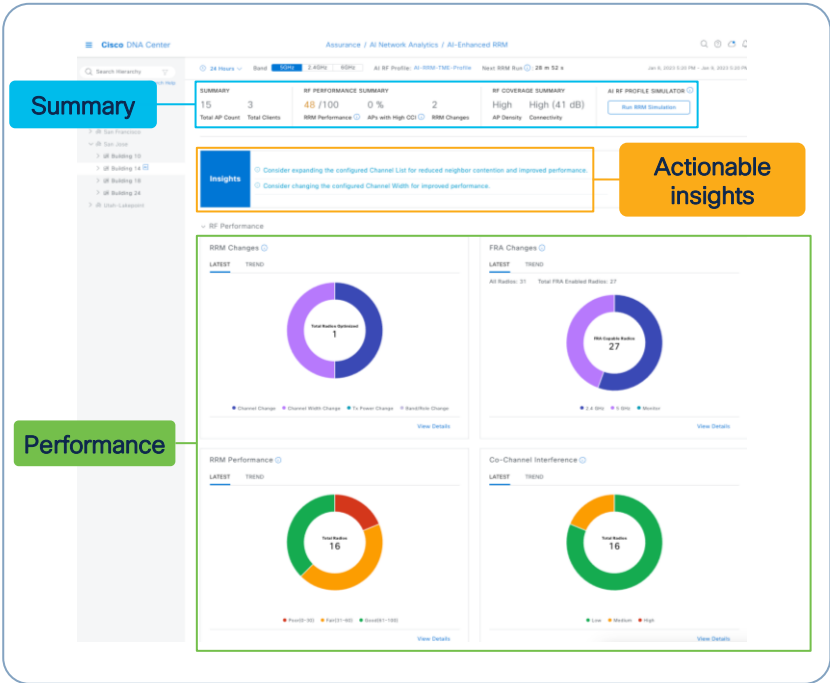
 **Managed & provisioned**

Available today

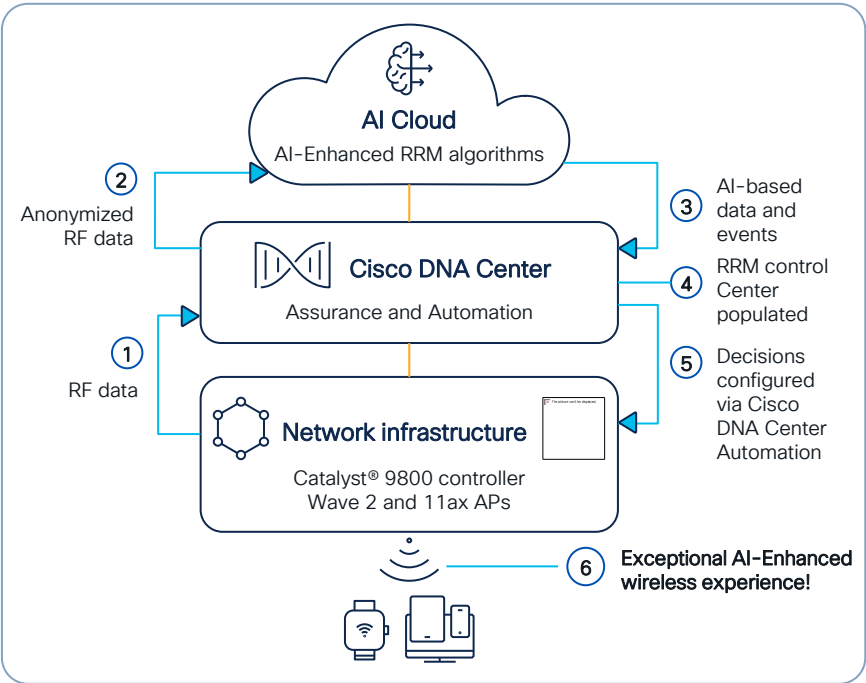
 **Managed only**

Coming in 2.3.7.4

Instantaneous visibility



Proactive optimizations



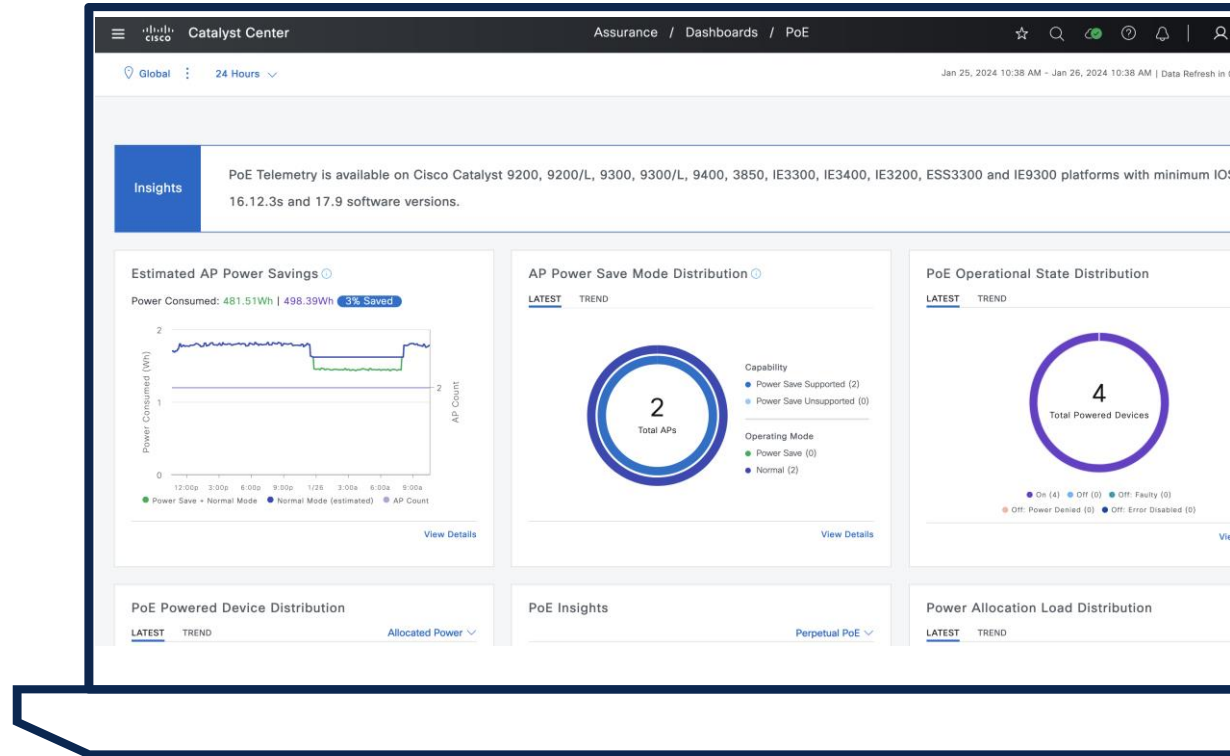
If you want to learn more about AI-RRM...



Advanced RF Tuning for Wi-Fi 6E with Cisco Catalyst Wireless:
Become an Expert While Getting a Little Help from AI
BRKEWN-3413

Observe the AP Power Save mode distribution

- Assurance > PoE
- Requires 17.10
- Switches that power APs must be added in the inventory

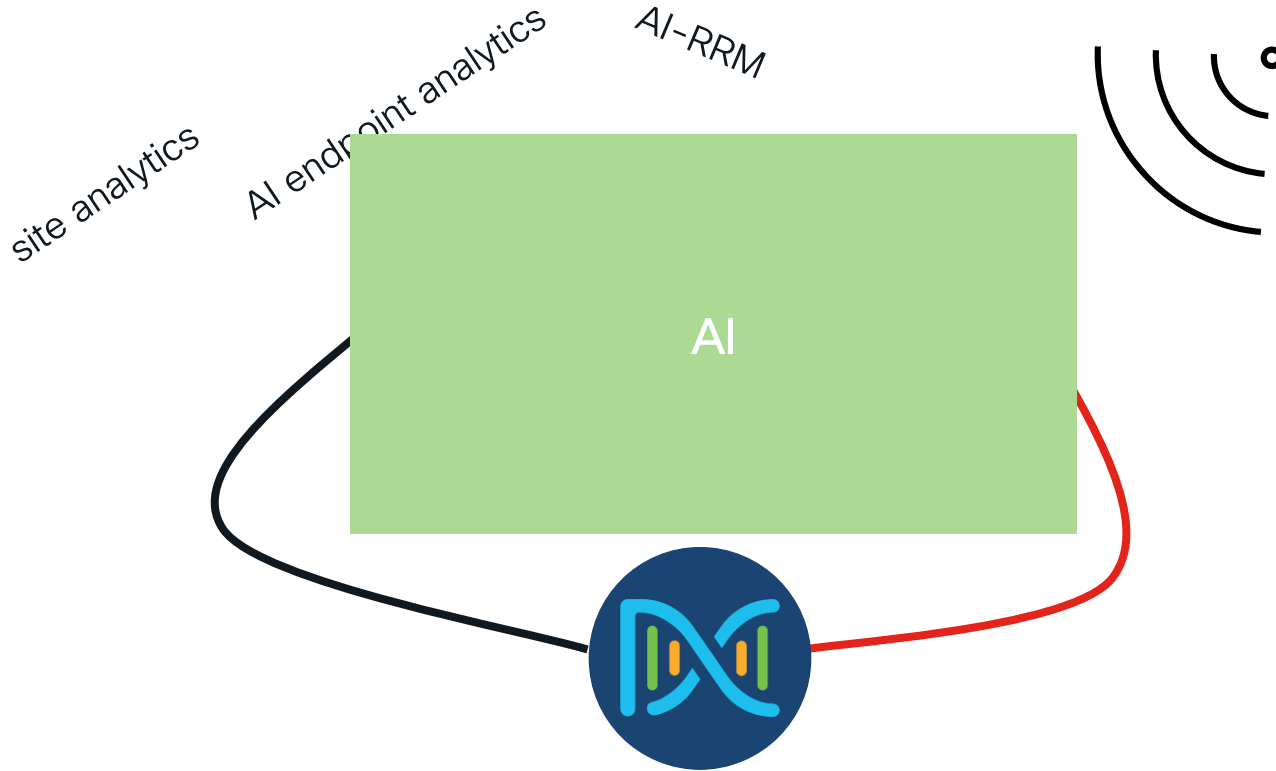


Agenda

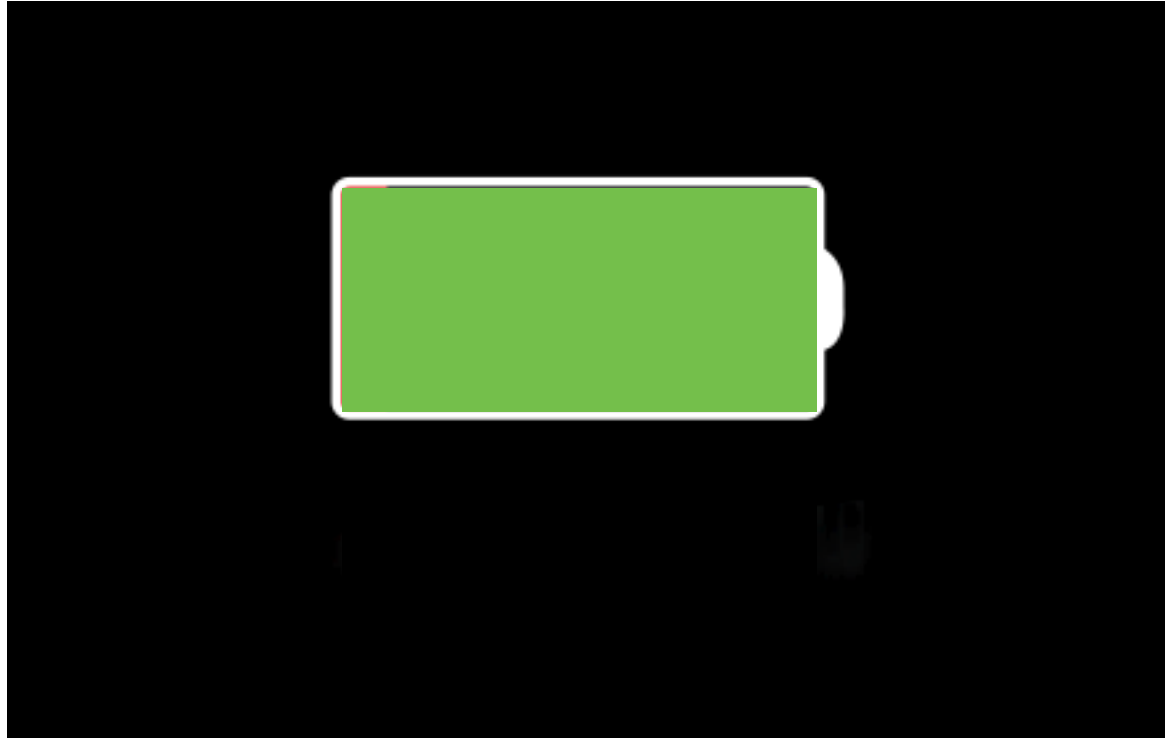
CISCO *Live!*

- Introduction
- Get insights with AIOps
- Operate efficiently with NetOps
- Expand usage with DevOps
- Conclusion

Your Cisco wireless battery



Your Cisco speaker status



Agenda

- Introduction
- Get insights with AIOps
- Operate efficiently with NetOps
- Expand usage with DevOps
- Conclusion

Agenda

- Operate efficiently with NetOps
 - The NetOps 101
 - Ease your life with NetOps
 - Advanced NetOps topics

Software Image Management

The screenshot shows the Cisco DNA Center interface for managing software images. The page title is "Provision / Inventory". The user is logged in as "admin". The current view is "Global" and the device type is "All". The "Devices (6)" section is focused on "Software Images". A search bar is present with the text "Click here to apply basic or advanced filters or view recently applied filters". The table below shows a list of devices with columns for "Device Name", "IP Address", "Device Family", "Software Image", "OS Update Status", and "Site". The device "cisco-wlc-19.cisco.com" is selected, and the "Actions" menu is open, showing options like "Inventory", "Software Image", "Provision", "Telemetry", "Device Replacement", "Compliance", and "More". The "Software Image" sub-menu is also open, showing options like "Image Update", "Image Update Status", "Download Update Readiness Report", and "Check Image Update Readiness".

Device Name	IP Address	Device Family	Software Image	OS Update Status	Site
ap-cleu-ams1	10.0.110.201	Unified AP			.../RAI/1st Flo
sen-cleu-001	10.0.111.4	Wireless Senso		Ice Uptodate	.../Millenium T
cisco-wlc-19.cisco.com	10.10.10.19	Wireless Contro		tribution Pending	.../AMS/RAI
ap-cleu-ams3	10.0.110.31	Unified AP	NA	NA	.../RAI/1st Flo
ap-cleu-ams4	10.0.110.38	Unified AP	NA	NA	.../RAI/1st Flo
ap-cleu-ams2	10.0.110.59	Unified AP	Reachable	NA	.../RAI/1st Flo

Tips and Tricks – SWIM



Tagged AddOns (SMU, APSP, ...) are part of the upgrade

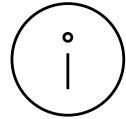
The screenshot displays the Cisco DNA Center interface for an 'Image Update Readiness Check'. The left pane shows a list of devices, and the right pane shows the details for the selected device, 'cisco-wlc-19.cisco.com'. The 'Golden Image' field is highlighted with an orange box, showing the path: 'C9800-CL-universalk9.17.09.04.CSCwh87343.SPA.smu.bin, C9800-CL-universalk9.17.09.04.CSCwh93727.SPA.apsp.bin'. Below this, a table of 'Readiness Checks Results' is shown.

Check Type	Description	Status	Last Ch
Image Version Support	The golden image is applicable to the device	Success (Green)	Dec 12, 12:00 PM
Flash check	Flash check: SUCCESS Expected: 1210 MB Available Free space is: 9173 MB	Success (Green)	Dec 12, 12:00 PM
Service Entitlement Check	Could not validate license service contract	Warning (Yellow Triangle)	Dec 12, 12:00 PM
Startup config check	Startup configuration exist for this device	Success (Green)	Dec 12, 12:00 PM
Config-register	Config-register verified successfully	Success (Green)	Dec 12, 12:00 PM

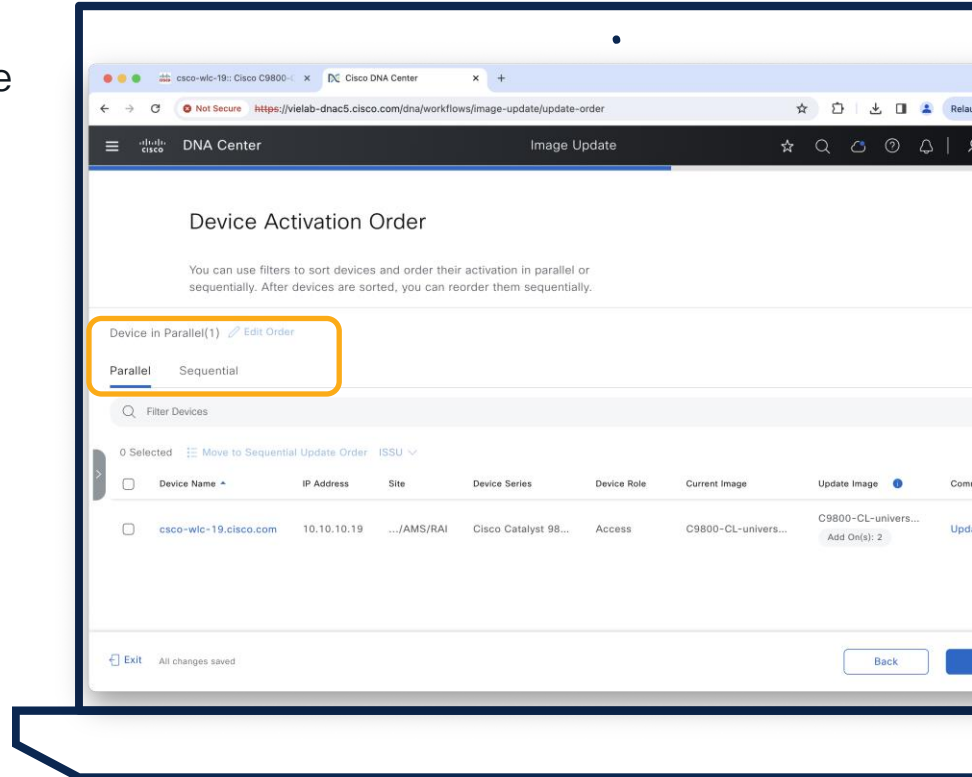
Tips and Tricks – SWIM



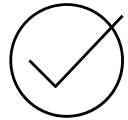
Tagged AddOns (SMU, APSP, ...) are part of the upgrade



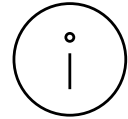
2.3.7 introduced Device Activation Order (Parallel/Sequential)



Tips and Tricks – SWIM



Tagged AddOns (SMU, APSP, ...) are part of the upgrade



2.3.7 introduced Device Activation Order (Parallel/Sequential)

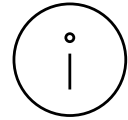


Image Update Status shows also AP Pre-image download progress

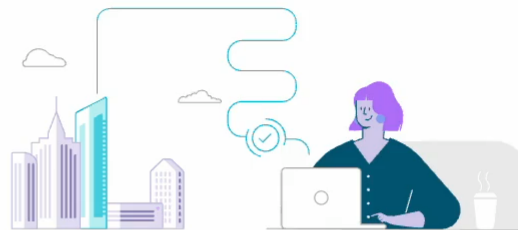
The screenshot shows the Cisco DNA Center interface for an image update. The main heading is "cisco-wlc-19.cisco.com (10.10.10.19) Image Update". Below this, there is a progress bar and a summary of the update: Date: Dec 12, 2023 6:57 PM, Duration: 13 minutes 47 seconds, Status: In Progress. The page is divided into several sections: SUMMARY, Devices Updates, Operations, and Checks. The Operations section is expanded, showing a list of tasks. The "AP Pre-Image Download" task is highlighted with a yellow box. The task details are as follows:

Task Name	Task Status
AP Pre-Image Download	In Progress (AP download image status: Total number of APs = 4, initiated = 0, downloading = 0, predownloading = 0, completed predownloading = 0, not supported = 0, failed to predownload = 0.)



Build and maintain your network more efficiently with Workflows.

Let us guide you through end-to-end workflows tailored to make your job easier.



Library [Choose An Intent ▾](#)



Configure Cisco UDN

Configure Cisco User Defined Network which enables users to define their own personal network in a shared Wireless network

Wireless



Site to Site VPN

Create VPN configuration between two sites

Wired



Create Sensor Test

Build a wireless test template for monitoring real-world client experiences.

Wireless



Replace Device

Replace your device in a few quick easy steps

Wired

Wireless



Switch Refresh

Refresh network devices at your sites with new models.

Wired



Access Point Refresh

Replace Your Access Points with New ones

Wireless



Create a Remote Support Authorization

Grant the Cisco specialist temporary access to Cisco DNA Center to triage the managed



Smart License Compliance

Explore capabilities for Smart License Enabled devices



Configure REP Ring (Non-Fabric)

Configure a REP Ring to enable redundancy on the Extended Nodes

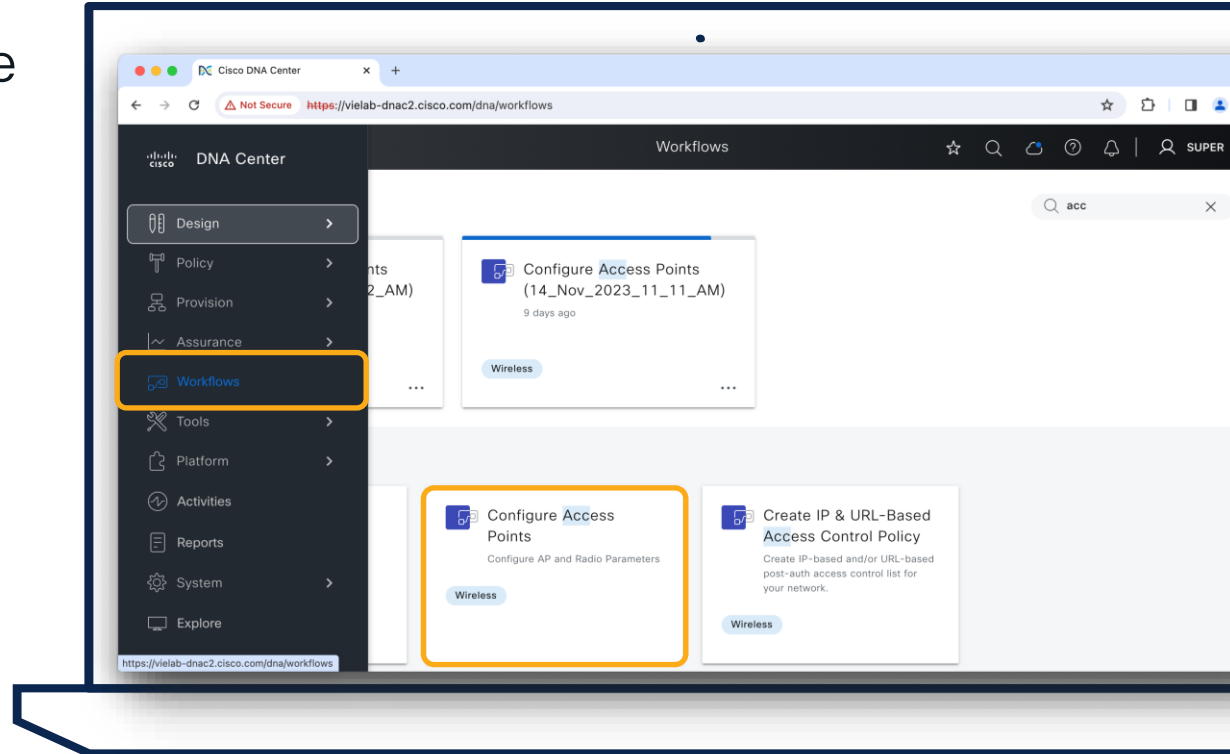


Configure REP Ring (Fabric)

Configure a REP Ring to enable redundancy on the Extended Nodes

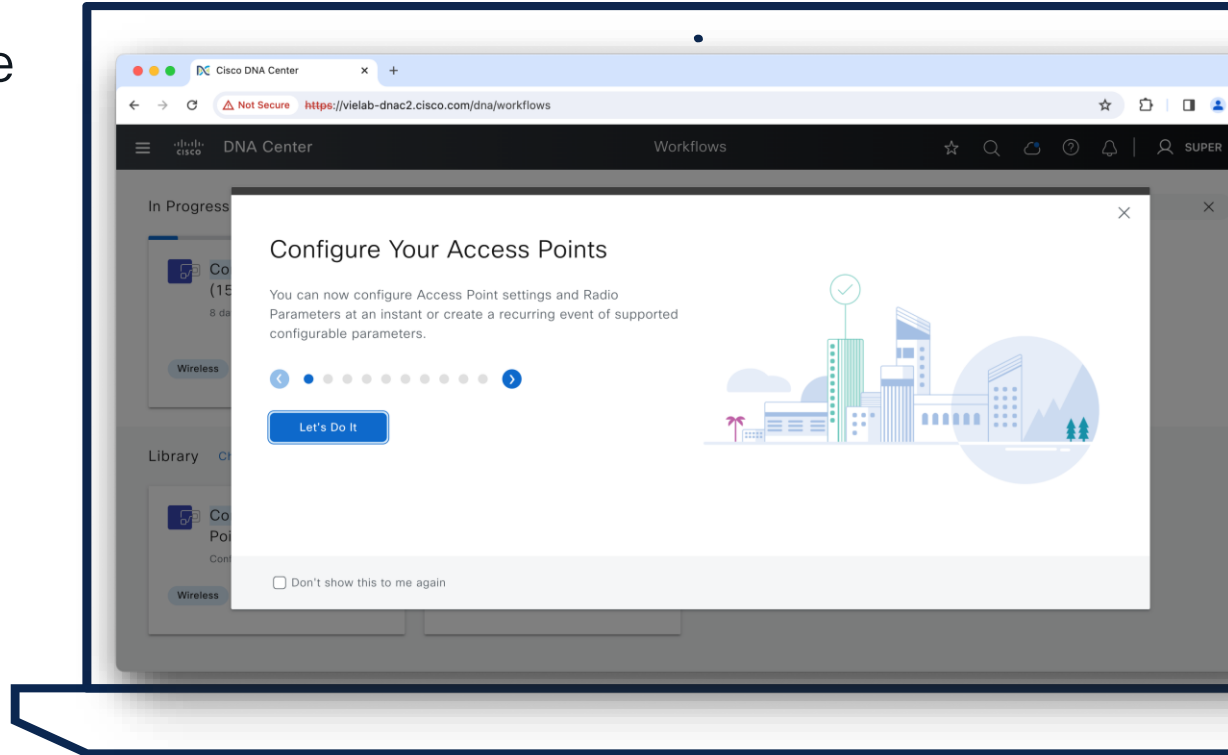
AP Configuration Workflow

- Workflows > Configure Access Points



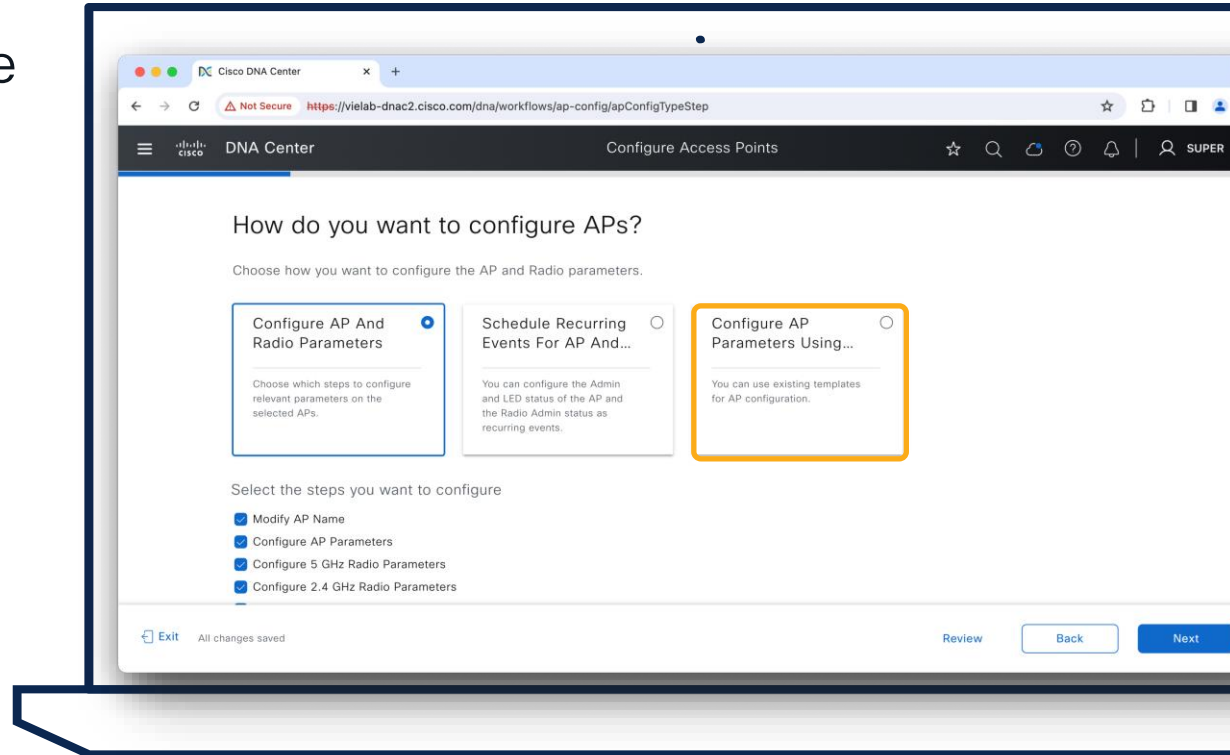
AP Configuration Workflow

- Workflows > Configure Access Points



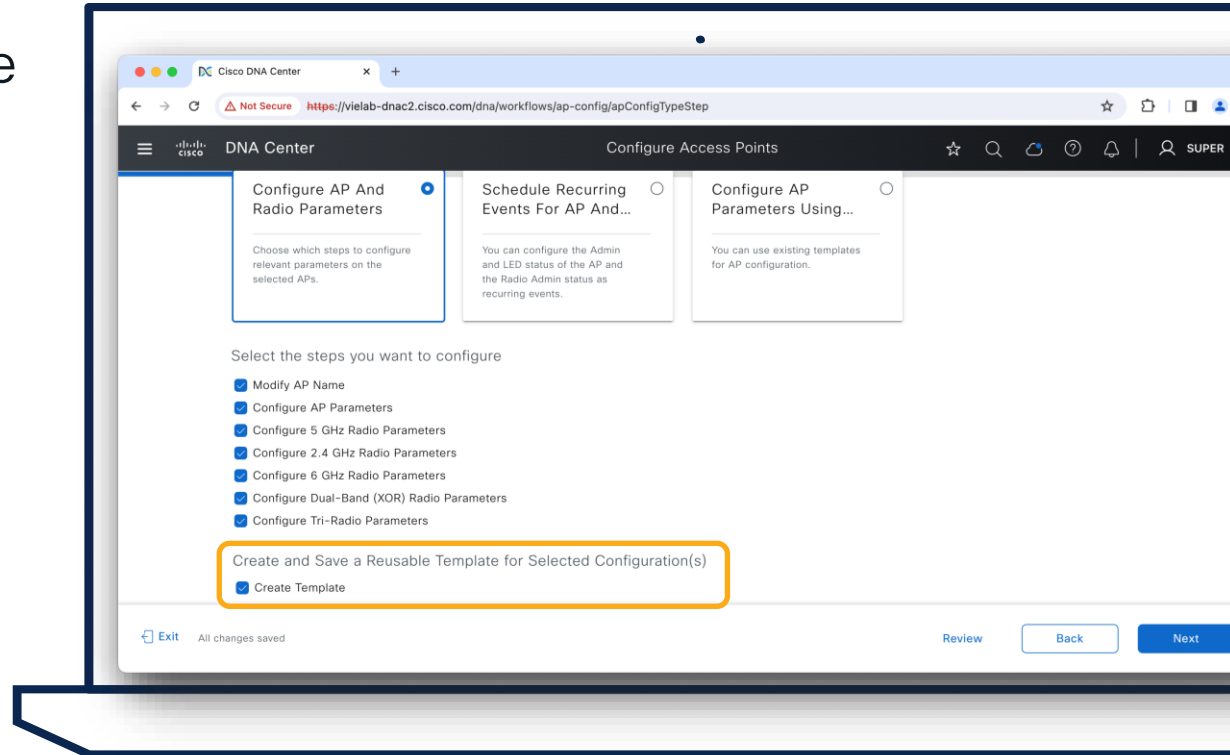
AP Configuration Workflow

- Workflows > Configure Access Points
- Select Configure / Recurring / *Template*



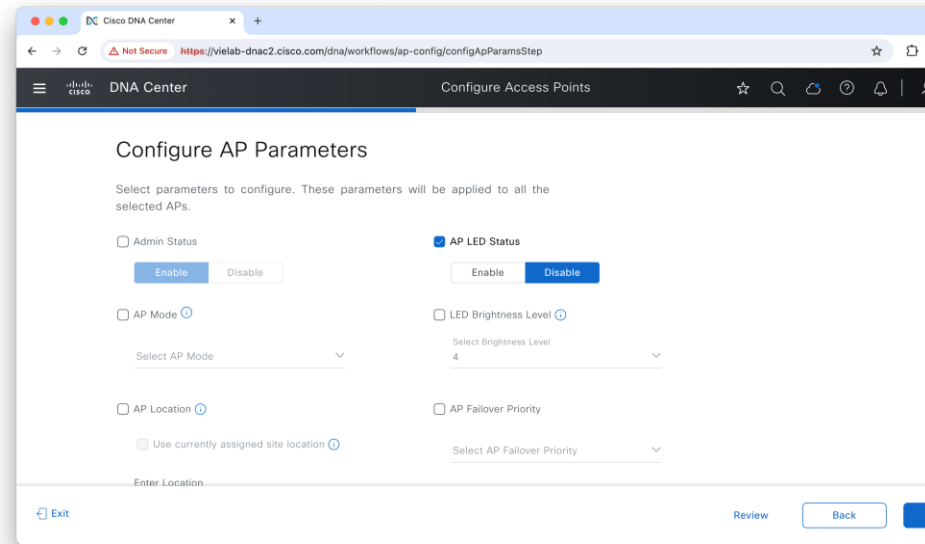
AP Configuration Workflow

- Workflows > Configure Access Points
- Select Configure / Recurring / *Template*



What to expect? AP Configuration Workflow

- AP Name Change
- AP Parameters
 - WLC Change (Primary/Secondary/Tertiary)
 - Admin Status
 - Location
 - LED
- Radio Parameters (2.4GHz/5GHz/6GHz/XOR)
 - Admin Status
 - Antenna
 - Channel
 - Power



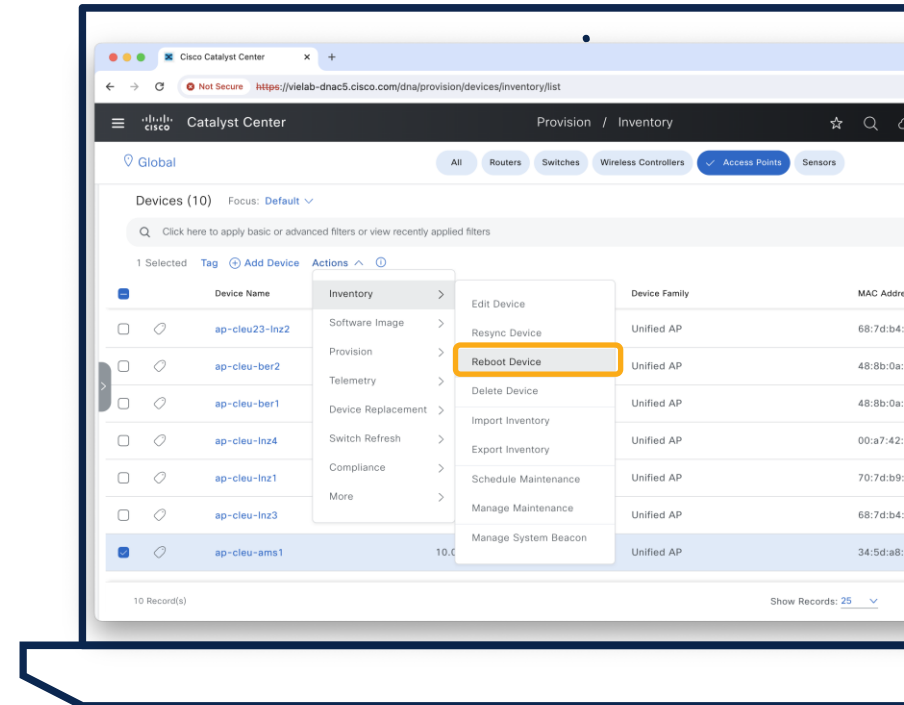
Tips and Tricks for AP Configuration Workflow



WLC only needs to be Reachable/Managed state





AP Reboot/LED can be managed through Inventory

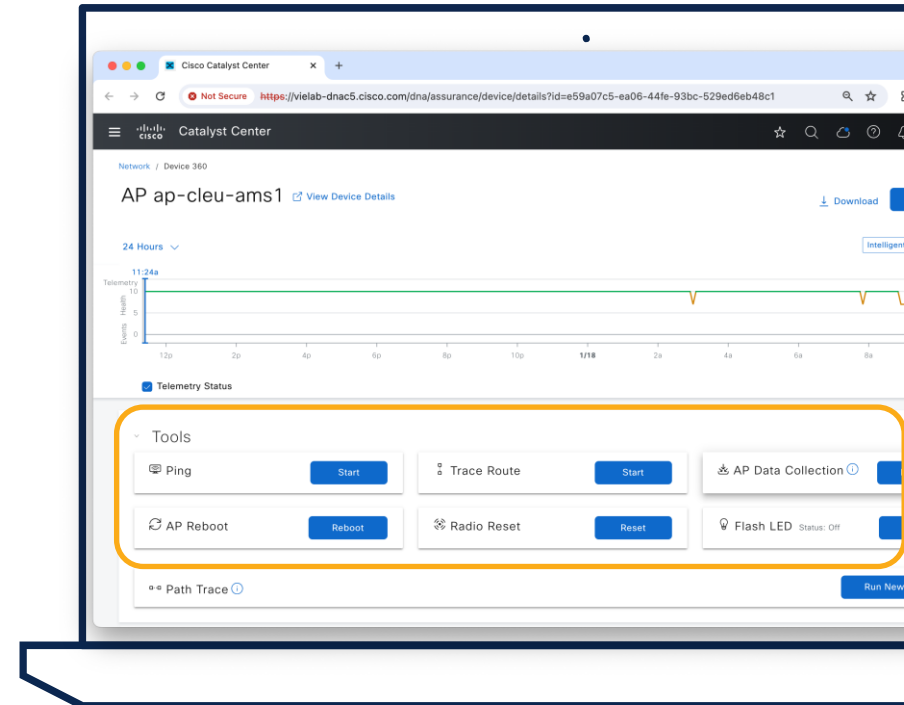


Tips and Tricks for AP Configuration Workflow

 WLC only needs to be Reachable/Managed state

 AP Reboot/LED can be managed through Inventory

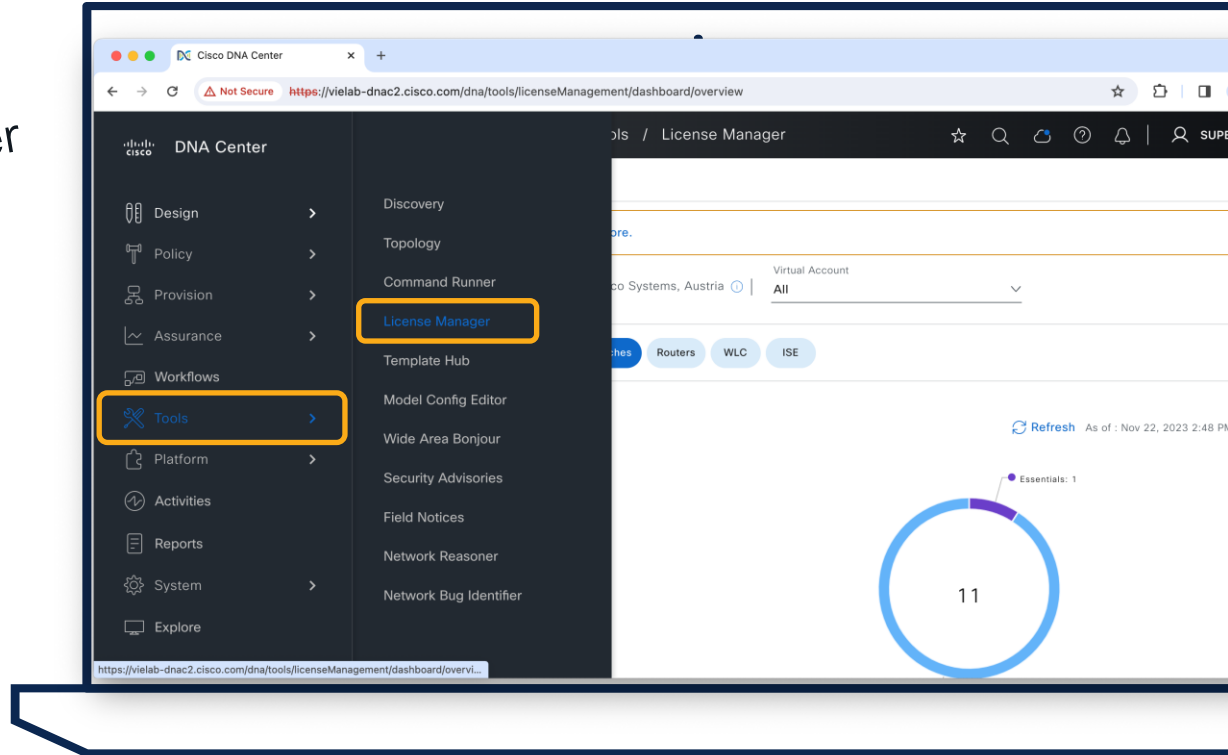
 Tools at Device 360 view also available for frequently used activities



How to report License Usage of C9800?



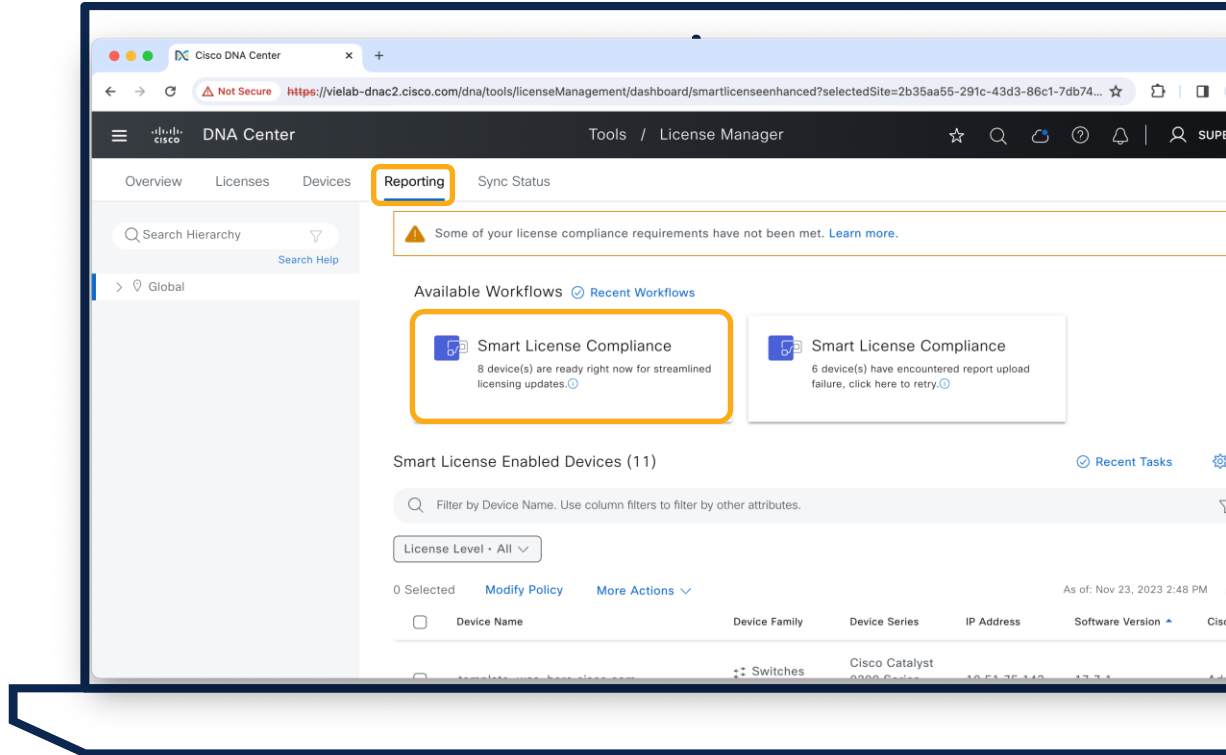
Tools
License Manager



How to report License Usage of C9800?



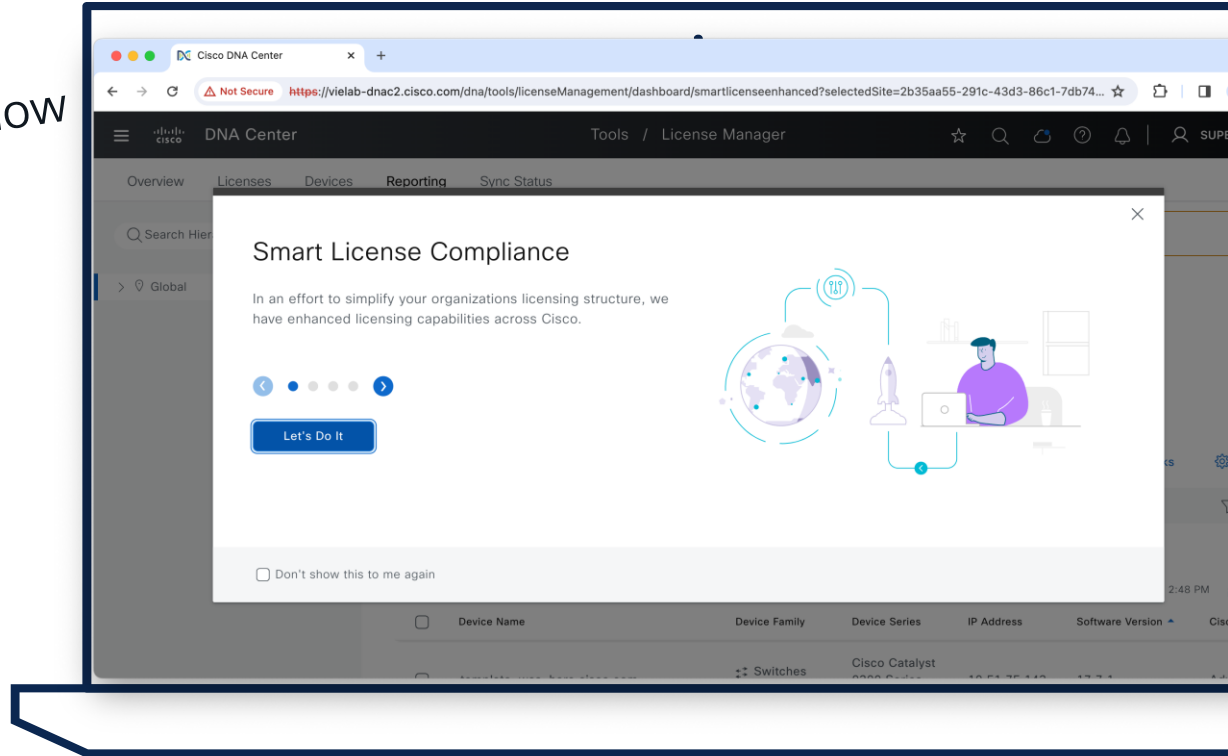
Reporting



How to report License Usage of C9800?



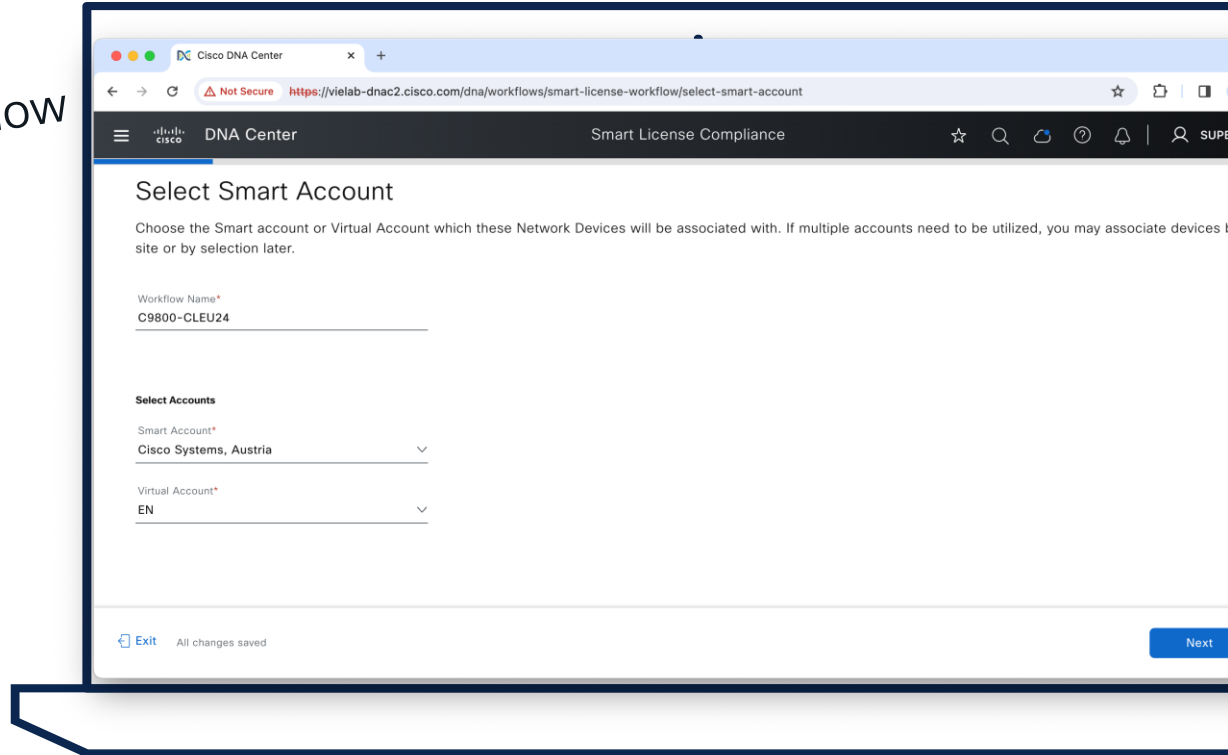
Go Through Workflow



How to report License Usage of C9800?

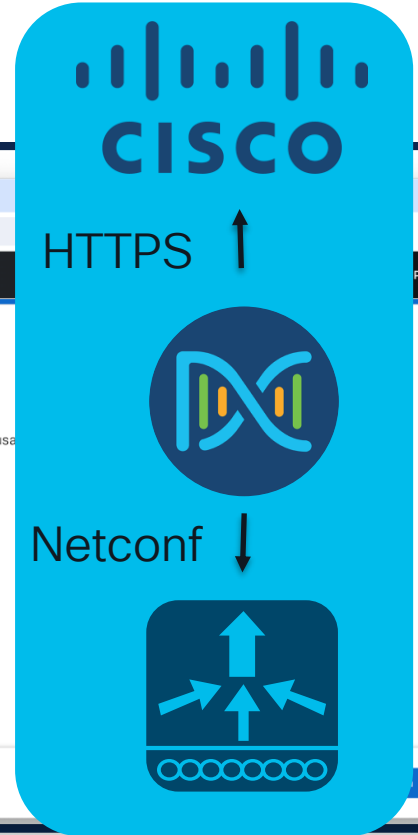
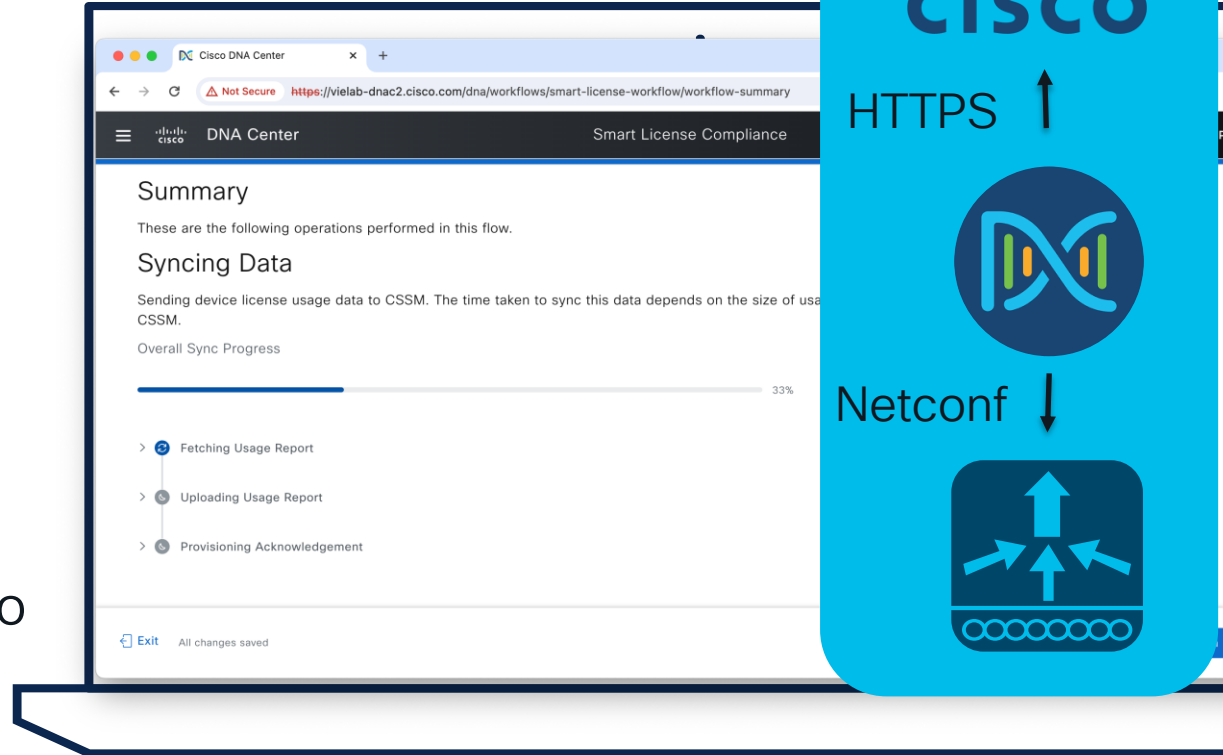


Go Through Workflow



How does it work in the background?

- Catalyst Center pulls Usage Report from WLC with Netconf
- Uploads it to Cisco with HTTPS
- Provisions ACK back to WLC with Netconf



Tips and Tricks for License Reporting



On-Prem CSSM is currently NOT supported in combination with Catalyst Center Smart Licensing using Policy reporting workflow

The screenshot shows the Cisco Catalyst Center web interface. The browser address bar displays the URL: <https://vielab-dnac5.cisco.com/dna/systemSettings/settings?settings-item=connectionMode>. The page title is "Catalyst Center" and the breadcrumb is "System / Settings". The left sidebar contains a search bar and a menu with items: Certificates, Cisco Accounts, PnP Connect, Cisco.com Credentials, Smart Account, Smart Licensing, SSM Connection Mode (highlighted), Device Settings, External Services, System Configuration, Terms and Conditions, and Trust & Privacy. The main content area is titled "SSM Connection Mode" and shows three radio buttons: "Direct" (selected), "On-Prem CSSM", and "Smart proxy". Below the radio buttons is the "Smart Call Home Server URL" field with the value <https://tools.cisco.com/its/service/oddce/services/DDCEService> and a "Save" button. A red text box is overlaid on the "Direct" radio button with the text: "Relevant for devices running 17.3.2 or earlier".

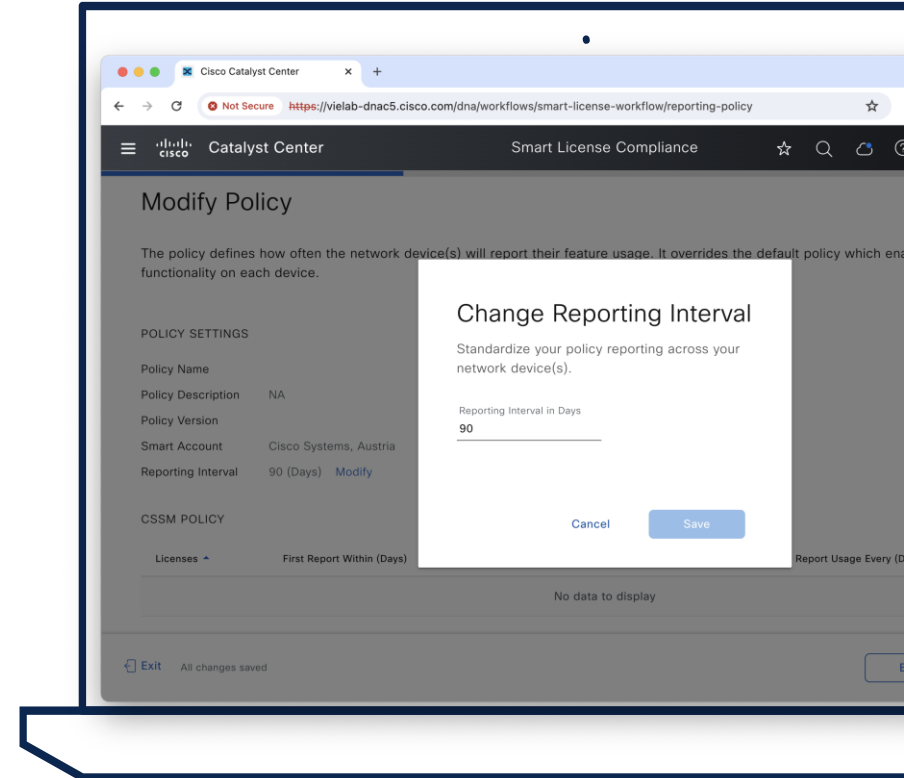
Tips and Tricks for License Reporting



On-Prem CSSM is currently NOT supported in combination with Catalyst Center Smart Licensing using Policy reporting workflow

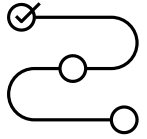


Workflow runs automatically in the defined reporting interval



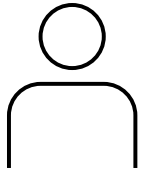
Agenda

- Operate efficiently with NetOps
 - The NetOps 101
 - Ease your life with NetOps
 - Advanced NetOps topics

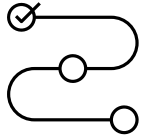


How to use CLI Template based AP PnP?

Generate AP PnP Onboarding Template

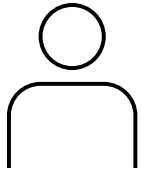


Project	Type	Version	Commit State	Provision Status	Network Profiles	Act
Onboarding Configuration	Regular	1	07 Sep 2023 07:11 PM	Not Provisioned	Attach	...
Onboarding Configuration	Regular	1	07 Sep 2023 07:11 PM	Not Provisioned	Attach	...
Onboarding Configuration	Regular	1	07 Sep 2023 07:11 PM	Not Provisioned	Attach	...
Onboarding Configuration	Regular	1	12 Sep 2023 12:28 PM	Not Provisioned	1	...



How to use CLI Template based AP PnP?

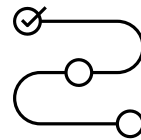
Generate AP PnP Onboarding Template



Project Name:
Onboarding Configuration
Device Family:
Wireless Controller

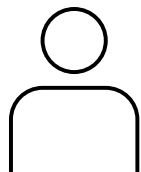
The screenshot displays the Cisco DNA Center interface for managing templates. The main area shows a list of 12 templates, all filtered by 'Onboarding Configuration'. The 'Add New Template' sidebar is active, showing the 'Template Details' section. The 'Project Name' is set to 'Onboarding Configuration', the 'Template Type' is 'Regular Template', and the 'Template Language' is 'JINJA'. The 'Software Type' is set to 'IOS-XE'. The interface includes a search bar, a table of templates, and various action buttons like 'Export', 'Import', and 'Delete'.

Name	Project	Type
Ambras_switch_onboarding	Onboarding Configuration	Regular
DMVPN Hub for Cloud Router...	Onboarding Configuration	Regular
Hohenzalzburg_switch_onboar...	Onboarding Configuration	Regular
IPsec 1 Branch for Cloud Ro...	Onboarding Configuration	Regular
IPsec 2 Branch for Cloud Ro...	Onboarding Configuration	Regular
pnp-demo2-2SW_stack_peguchs	Onboarding Configuration	Regular



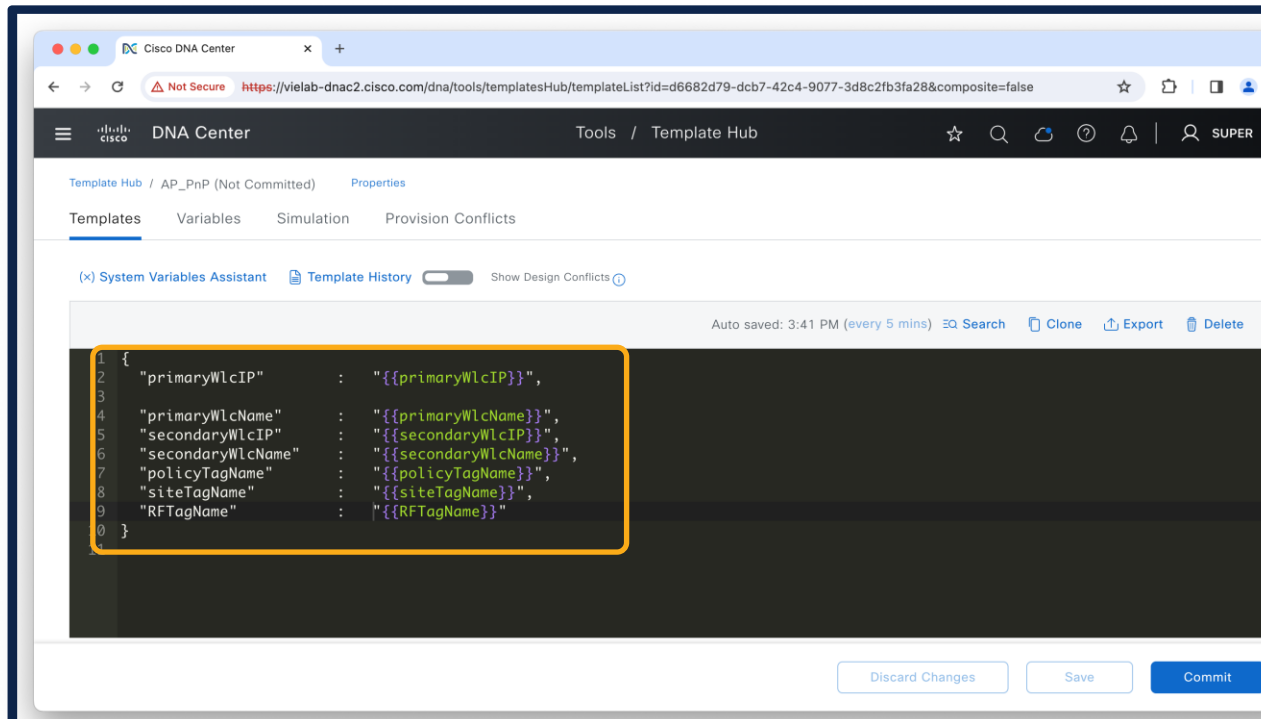
How to use CLI Template based AP PnP?

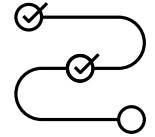
Generate AP PnP Onboarding Template



Parameter bare minimum:
primaryWlcIP

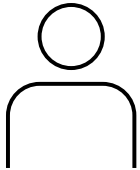
Rest is optional!





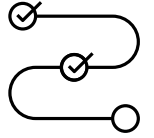
How to use CLI Template based AP PnP?

Provision > Plug and Play



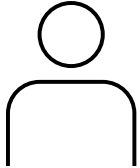
The screenshot shows the Cisco DNA Center interface. The left sidebar contains a navigation menu with 'Provision' highlighted. The main content area shows a 'Plug and Play' section with a table of network devices. The table has columns for Product ID, Last Contact, State, and Onboarding Progress. All devices shown are in a 'Provisioned' state.

Product ID	Last Contact	State	Onboarding Progress
D9500-24Y4C	Apr 07, 2021 1:54:50 PM	Provisioned	Provisioned
D9300-48P	Apr 07, 2021 1:57:51 PM	Provisioned	Provisioned
D9300-48U	Apr 07, 2021 2:15:54 PM	Provisioned	Provisioned



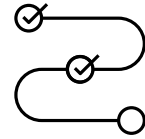
How to use CLI Template based AP PnP?

Add Device



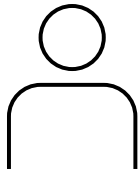
The screenshot shows the Cisco DNA Center interface for adding devices. The main content area is titled 'Network Plug and Play Overview' and displays a table of devices. The 'Add Devices' button in the table is highlighted with an orange box. To the right, a sidebar titled 'Add Devices' offers three methods: 'Single Add', 'Bulk Add', and 'Smart Account Add'. The 'Single Add' method is highlighted with an orange box.

#	Device Name	Serial Number	Product
1	R7HE35_B2-2	CAT2248L06X	C95
2	R7HE34-E1	FCW2244DHY3	C93
3	R7HE32-E3	FOC2244Q1D1	C93



How to use CLI Template based AP PnP?

Add+Claim

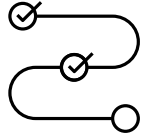


The screenshot shows the Cisco DNA Center interface for adding a device. The main content area is titled 'Add a Single Device' and contains the following fields:

- Serial Number*: FOC12312312
- Product ID*: CW9166I
- Device Name: ap::cleu24::ams1

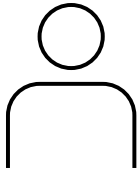
Below the form, there is a checkbox for 'Enable SUDI Authorization' which is currently unchecked. At the bottom right of the form, there is a blue 'Add Device' button and a white 'Add + Claim' button with a blue border, which is highlighted with an orange box.

#	Device Name	Serial Number	Product ID
1	R7HE35_B2-2	CAT2248L06X	C95...
2	R7HE34-E1	FCW2244DHY3	C93...
3	R7HE32-E3	FOC2244Q1D1	C92...



How to use CLI Template based AP PnP?

Go to Step 2
WITHOUT
Site assignment



1 Assign Site 2 Assign Configuration 3 Provision Templates 4 Summary

Assign Site

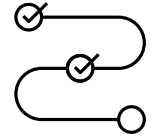
Devices (1) [Clear Sites](#)

Search Table

Device Name	Serial Number	Product ID	Device Type	Site (Recommended)	Actions
ap-cleu24-ams1	FOC12312312	CW9166I	AP	Assign	...

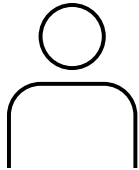
Do NOT 'Assign' a Site

Success
1 devices successfully added



How to use CLI Template based AP PnP?

Assign Template



Assign Configuration

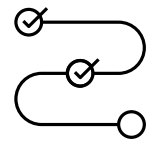
There are total of 1 devices missing required configuration. [Show devices.](#)

AP Location will **not be configured** as the assigned site during the claim process. To change this setting, go to [System -> Settings -> PnP AP Location.](#) [↗](#)
After the setting is updated, click [Refresh](#) [↻](#)

Devices (1) [Clear Configuration](#) [v](#)

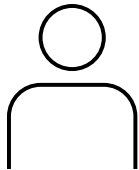
Search Table [v](#)

Device Name	Serial Number	Product ID	Assigned Site	Configuration	Actions
ap-cleu24-ams1	FOC12312312	CW91661	-	Template: Assign*	...



How to use CLI Template based AP PnP?

Assign Template



Configuration for device name: ap-cleu24-ams1

Serial Number: FOC12312312
Product ID: CW91661
Assigned Site:
Device Name: Device Name
ap-cleu24-ams1

Failed to retrieve a device-specific template. Below are all the available onboarding templates:

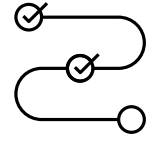
Select a Template
AP_PnP
Ex: Template Name (Profile Type)

Copy running configuration to startup configuration

Template: AP_PnP

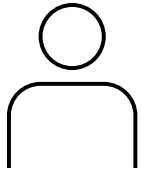
Cancel Save

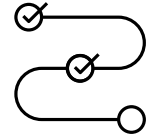
Device Name	Serial Number	Product ID
ap-cleu24-ams1	FOC12312312	CW91661



How to use CLI Template based AP PnP?

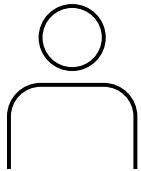
Fill Variables
if required





How to use CLI Template based AP PnP?

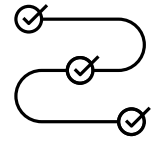
Finish Workflow



Summary

Devices (1)

Device Name	Serial Number	Product ID	Assigned Site	Configuration	Device Configuration
ap-cleu24-ams1	FOC12312312	CW91661	-	Template: AP_PnP	Preview Configuration



How to use CLI Template based AP PnP?



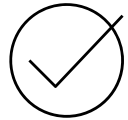
Get AP
Online



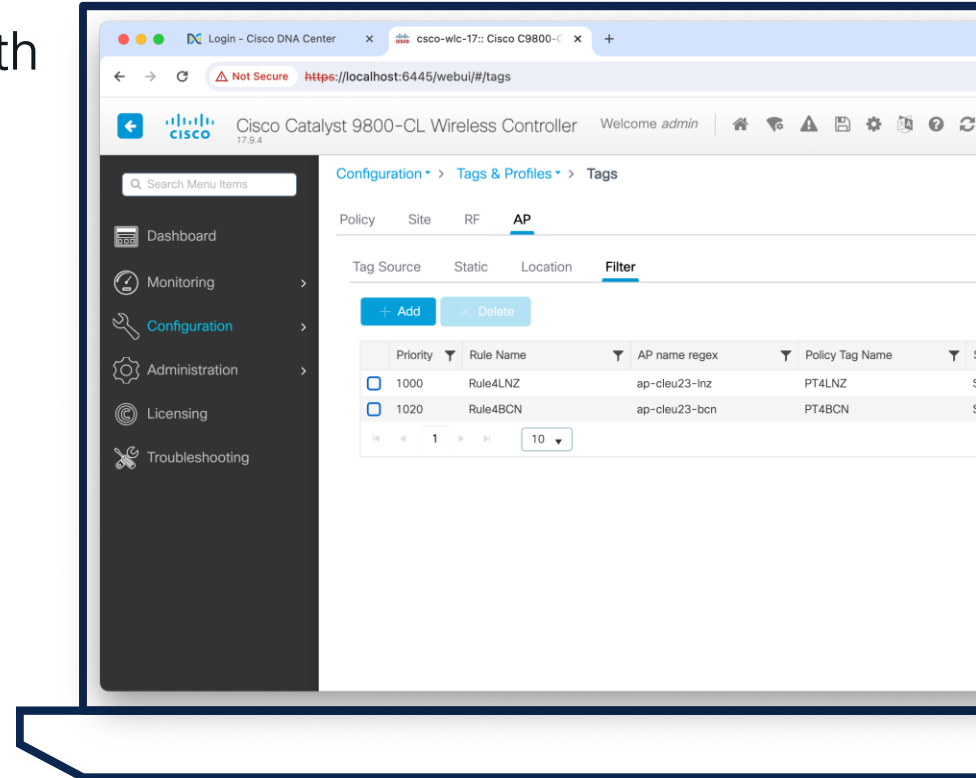
DHCP Option 43
pointing to
Catalyst Center
(PnP Options)

```
ip dhcp pool ap-pool
option 42 ip <NTP Server IP>
option 43 ascii
                "5A1D;B2;K4;I<DNAC IP>;J80"
```

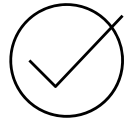

Tips and Tricks – AP PnP Template Based



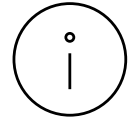
Powerful in combination with Filter (Regex) based Tag assignment on C9800



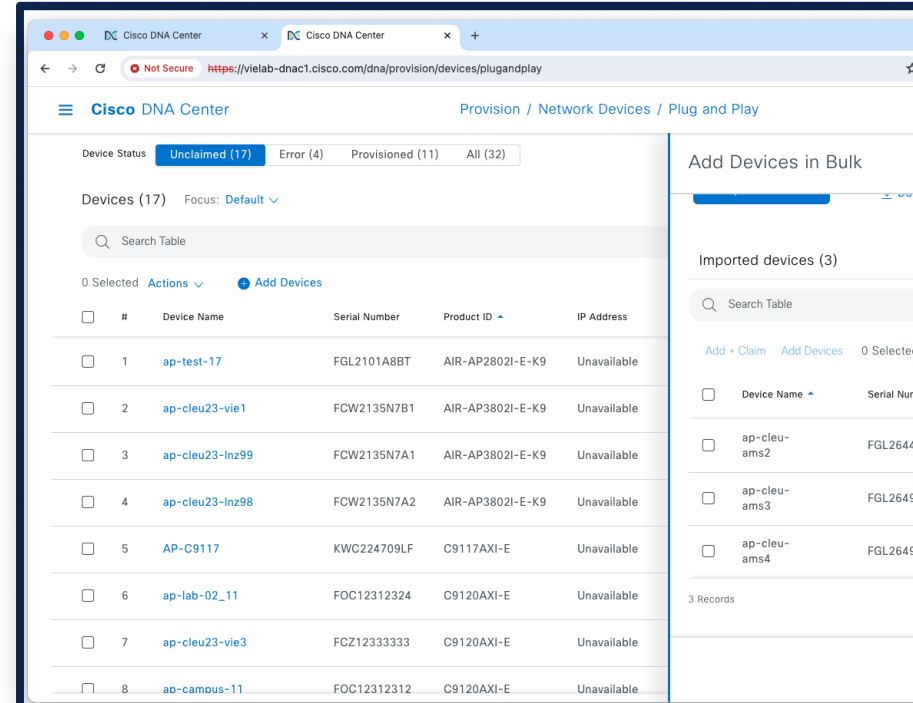
Tips and Tricks – AP PnP Template Based



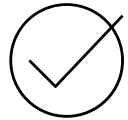
Powerful in combination with Filter (Regex) based Tag assignment on C9800



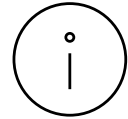
Can be used with CSV import to add multiple APs at once



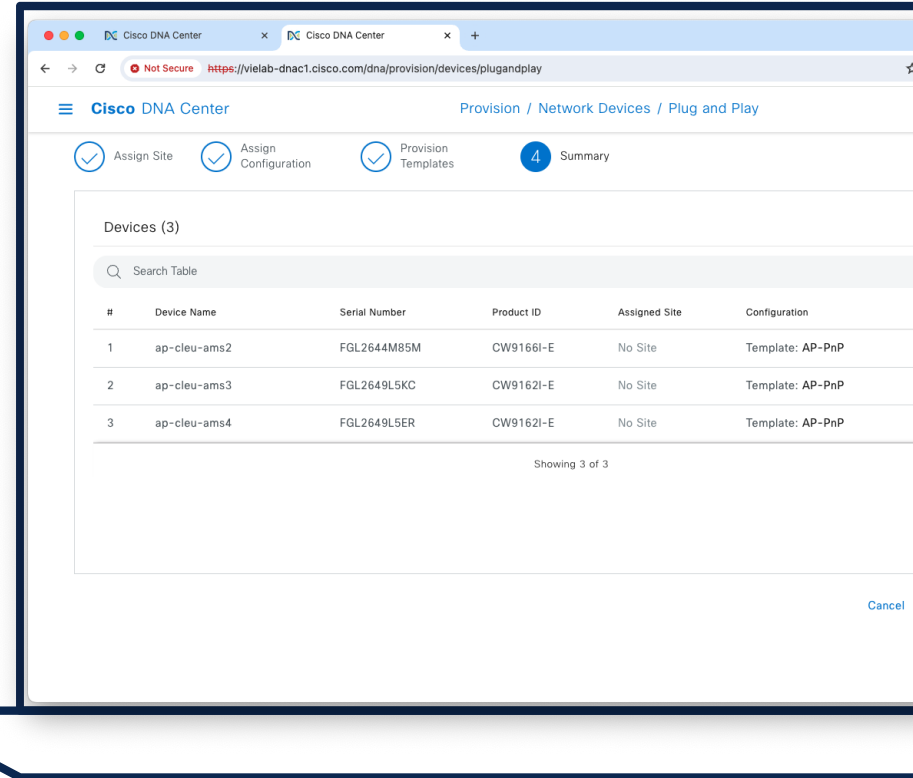
Tips and Tricks – AP PnP Template Based



Powerful in combination with Filter (Regex) based Tag assignment on C9800



Can be used with CSV import to add multiple APs at once

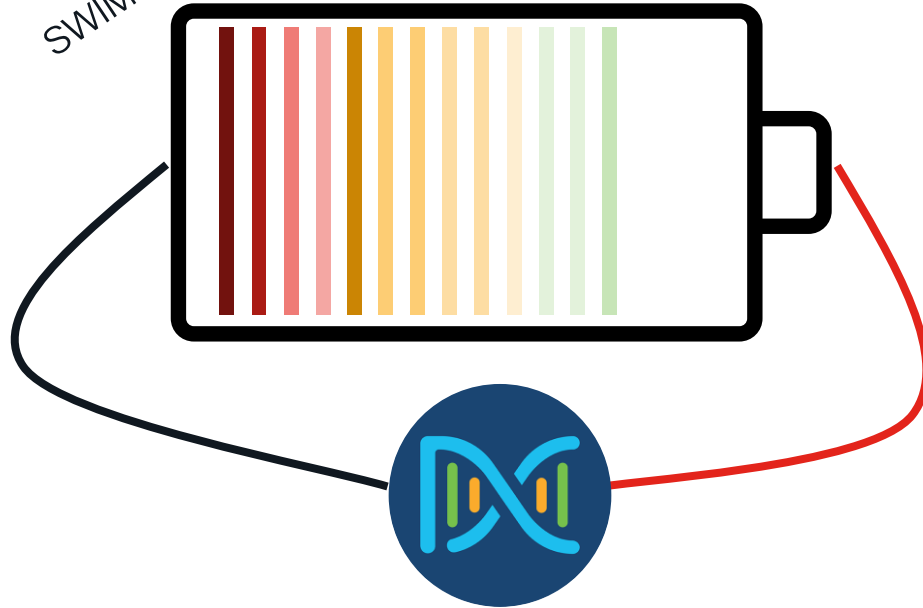


Your Cisco wireless battery

AP configuration workflow

PnP

SWIM

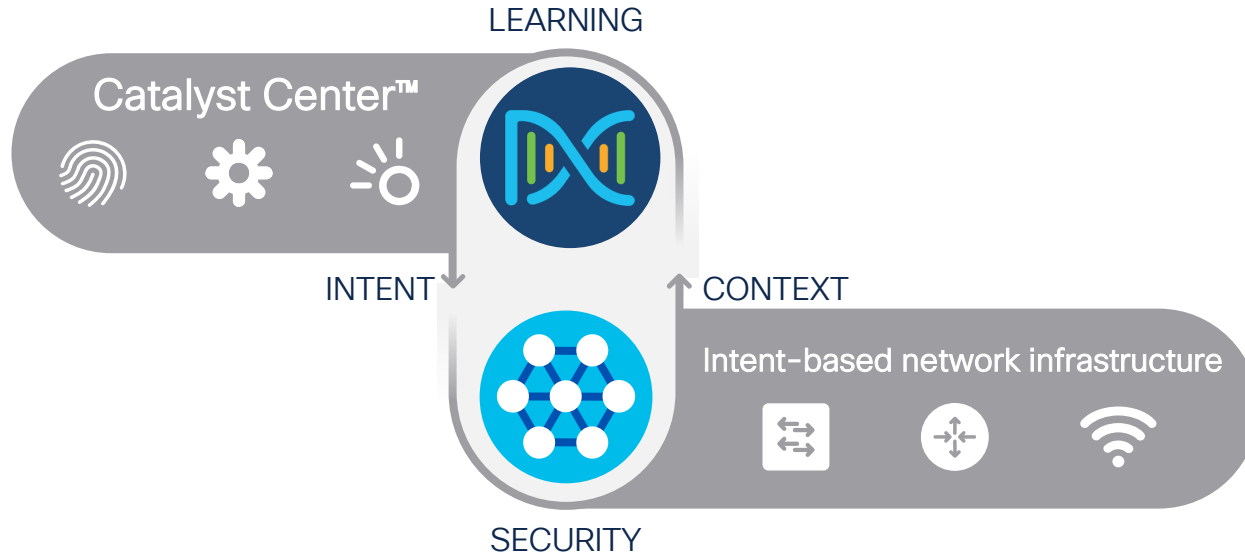


Agenda

CISCO *Live!*

- Operate efficiently with NetOps
 - The NetOps 101
 - Ease your life with NetOps
 - Advanced NetOps topics

Clarify your intent: Design your Network



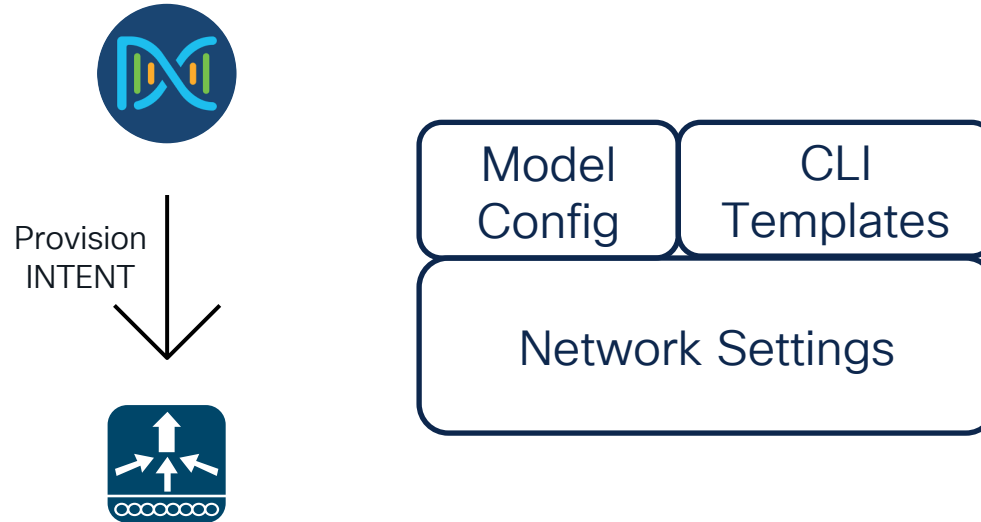
Clarify your intent: Design your Network

Automate the Deployment of a Wireless Network with the Help of
Cisco Catalyst Center

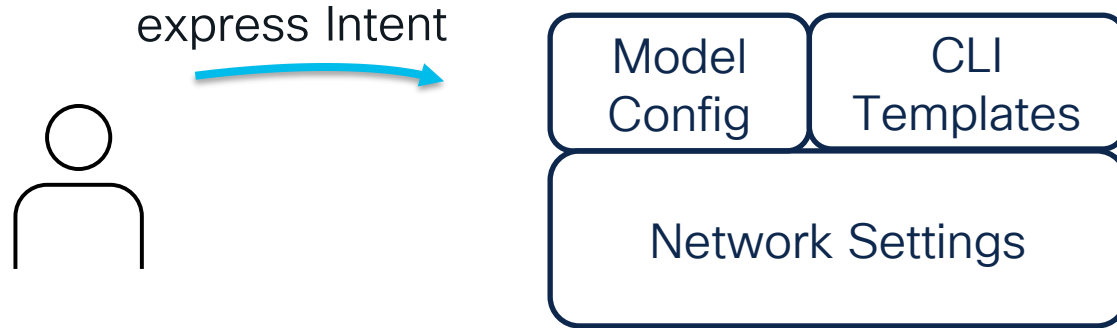


BRKOPS-2402

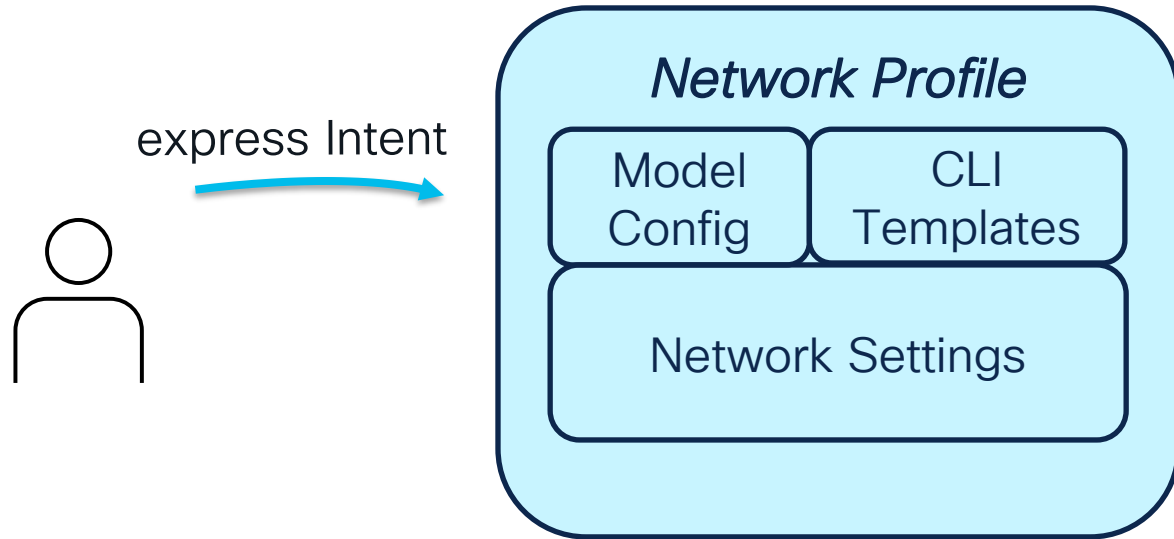
Clarify your intent: Design your Network



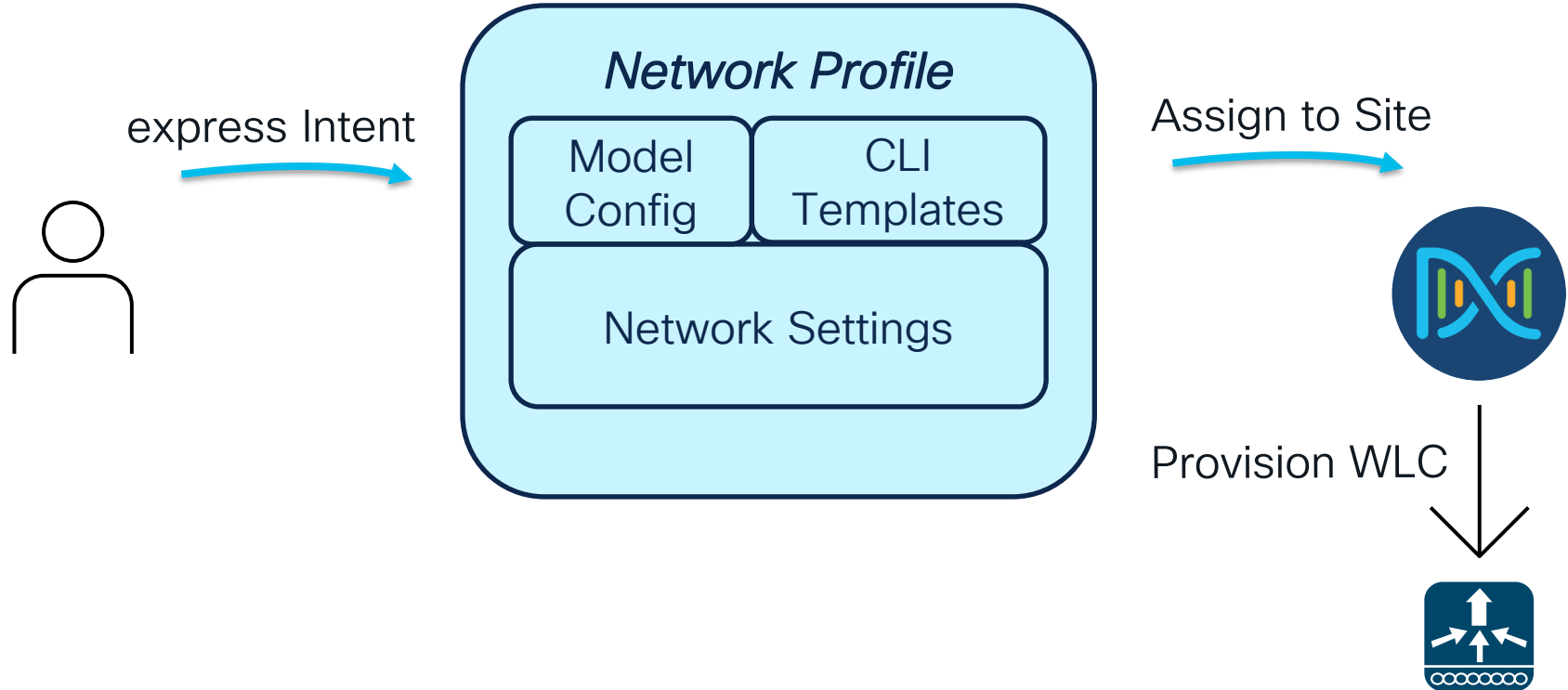
How to define the Intent



How to define the Intent

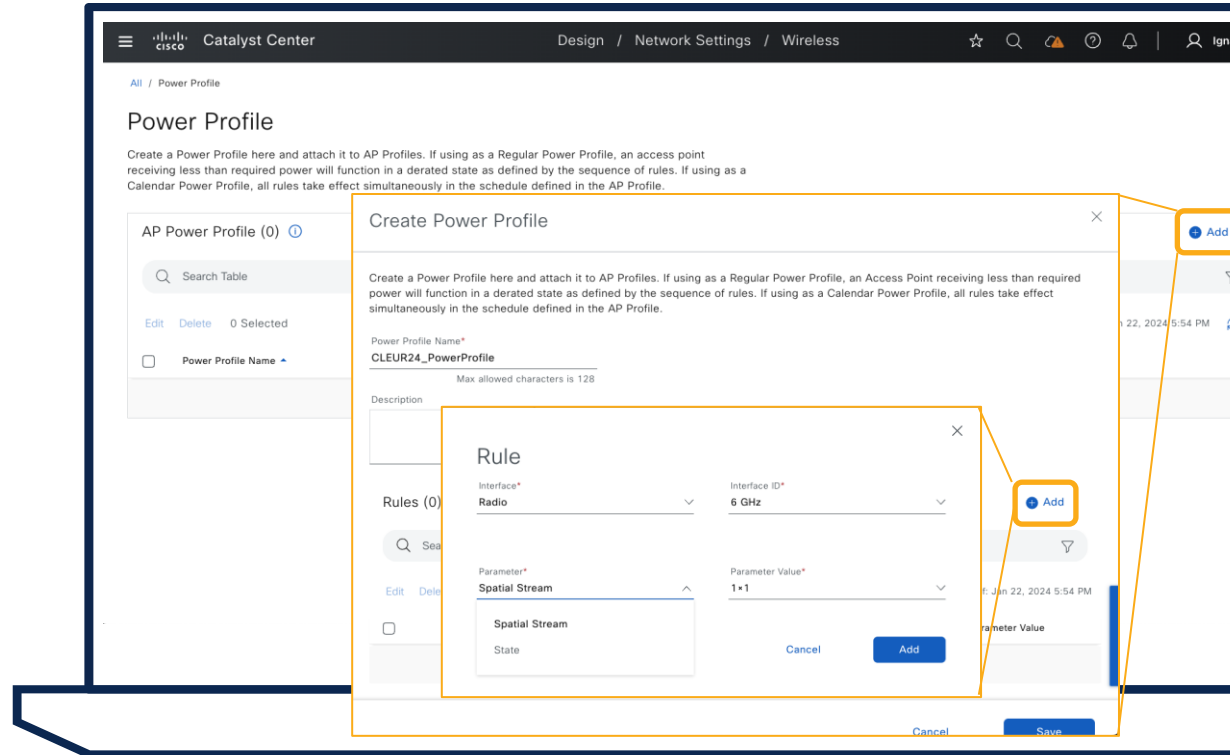


How to define the Intent



Do you want to save power? AP Power Profile is there to help you

- Design > Network Settings > Wireless > Create Power Profile



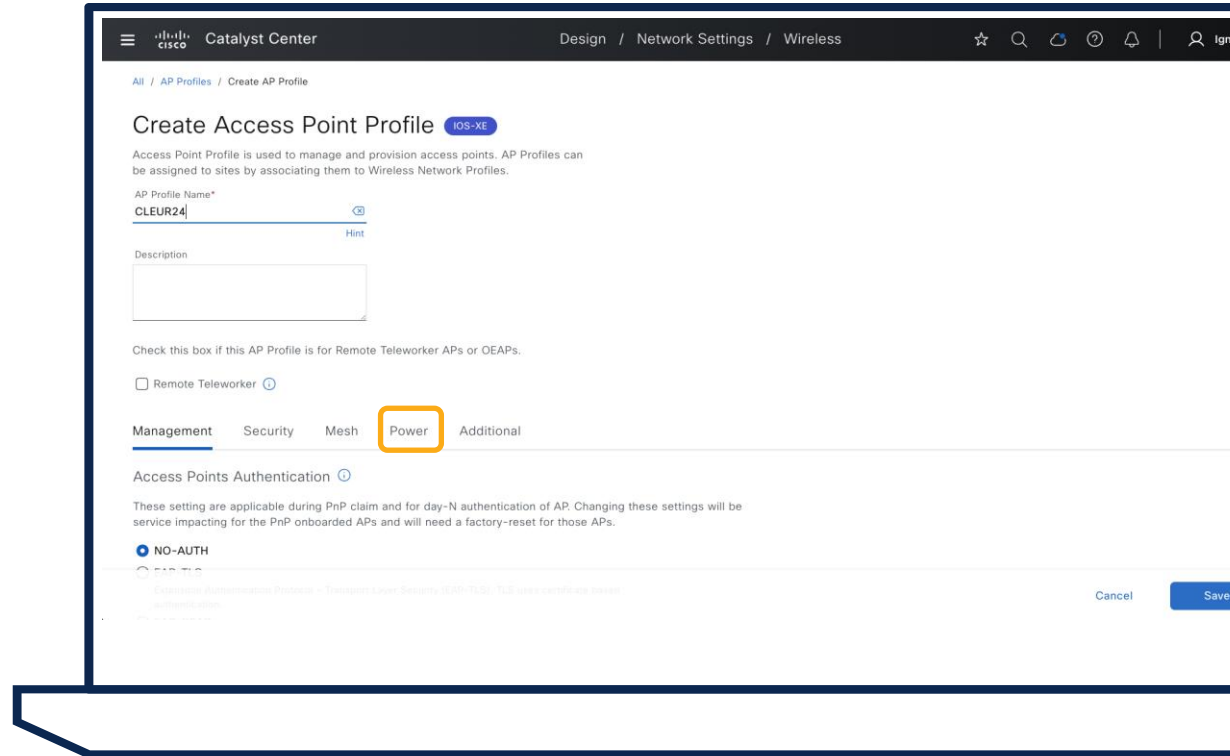
The screenshot displays the Cisco Catalyst Center interface for configuring a Power Profile. The main window is titled "Power Profile" and contains a table for "AP Power Profile (0)". A "Create Power Profile" dialog box is open, showing the following configuration:

- Power Profile Name:** CLEUR24_PowerProfile
- Description:** (Empty field)
- Rules (0):**
 - Interface:** Radio
 - Interface ID:** 6 GHz
 - Parameter:** Spatial Stream
 - Parameter Value:** 1x1

The dialog box includes "Add", "Cancel", and "Save" buttons. A "Rule" configuration sub-dialog is also visible, showing the same parameters as the main dialog.

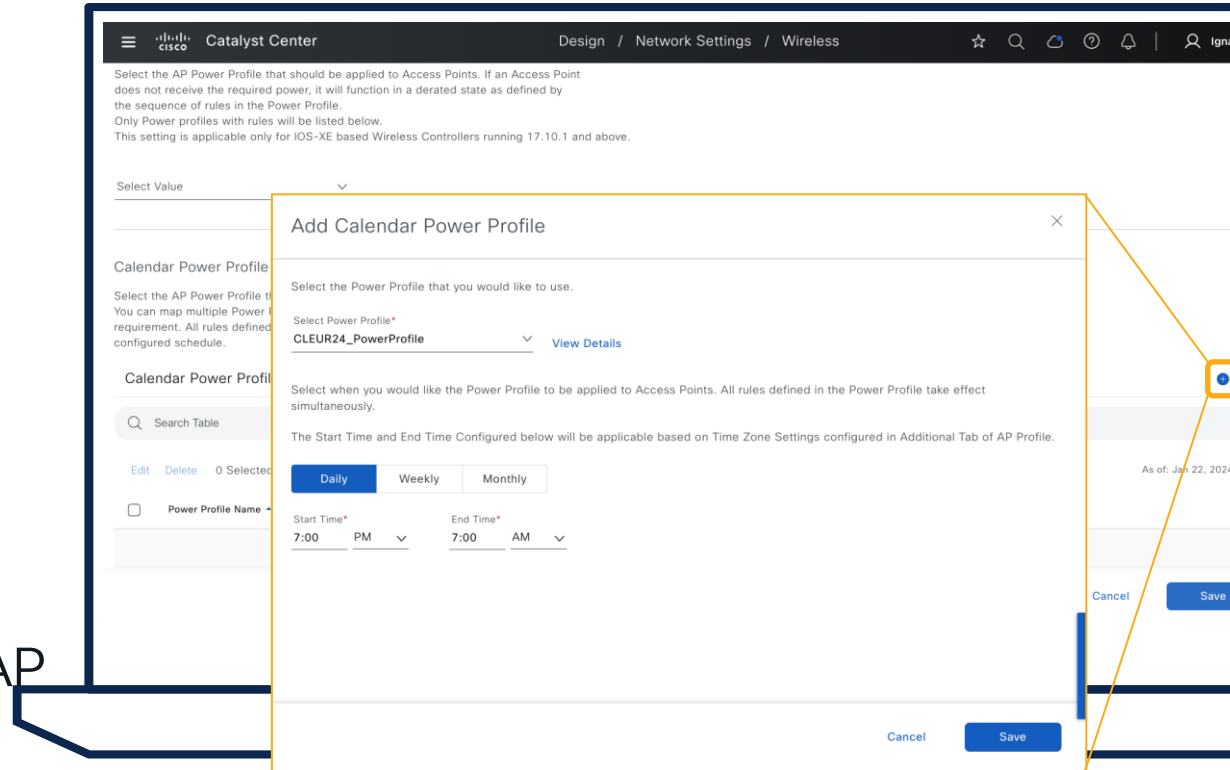
Do you want to save power? AP Power Profile is there to help you

- Design > Network Settings > Wireless > Create Power Profile
- Design > Network Settings > Wireless > Create/Edit AP Profile



Do you want to save power? AP Power Profile is there to help you

- Design > Network Settings > Wireless > Create Power Profile
- Design > Network Settings > Wireless > Create/Edit AP Profile
- Add power profile to AP Profile



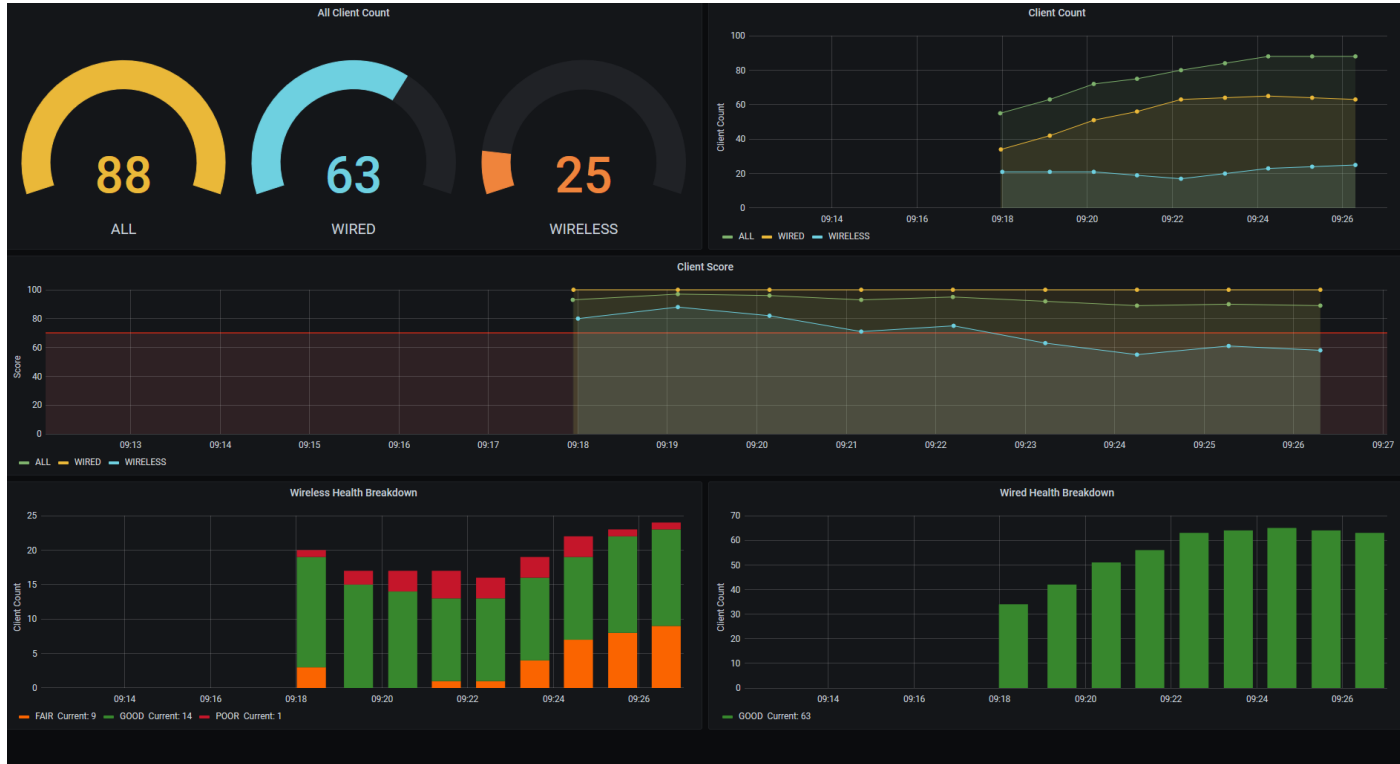
Agenda

- Introduction
- Get insights with AIOps
- Operate efficiently with NetOps
- Expand usage with DevOps
- Conclusion

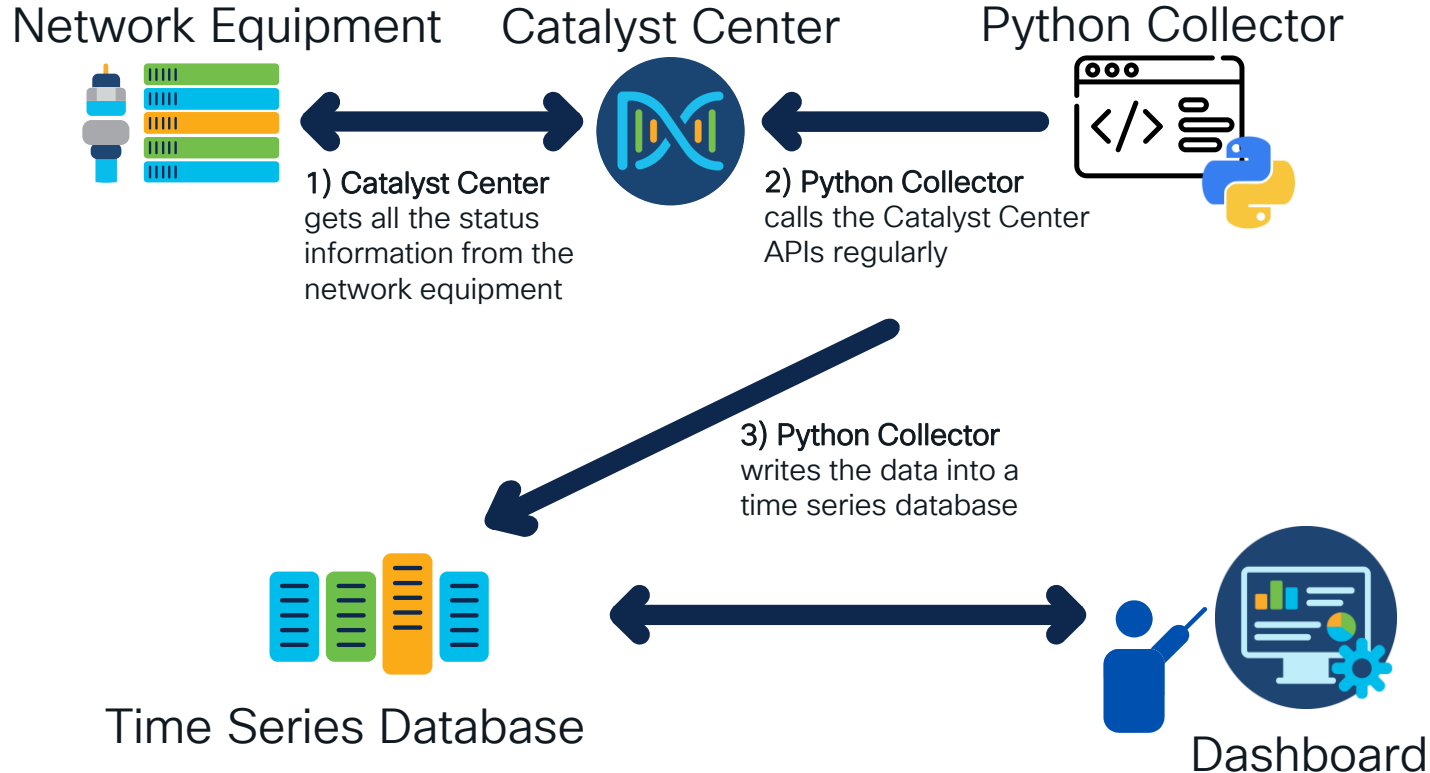
Agenda

- Expand usage with DevOps
 - Scripting
 - Remote Support Authorization

Customized dashboard with Catalyst Center telemetry



Customized dashboard with Catalyst Center telemetry

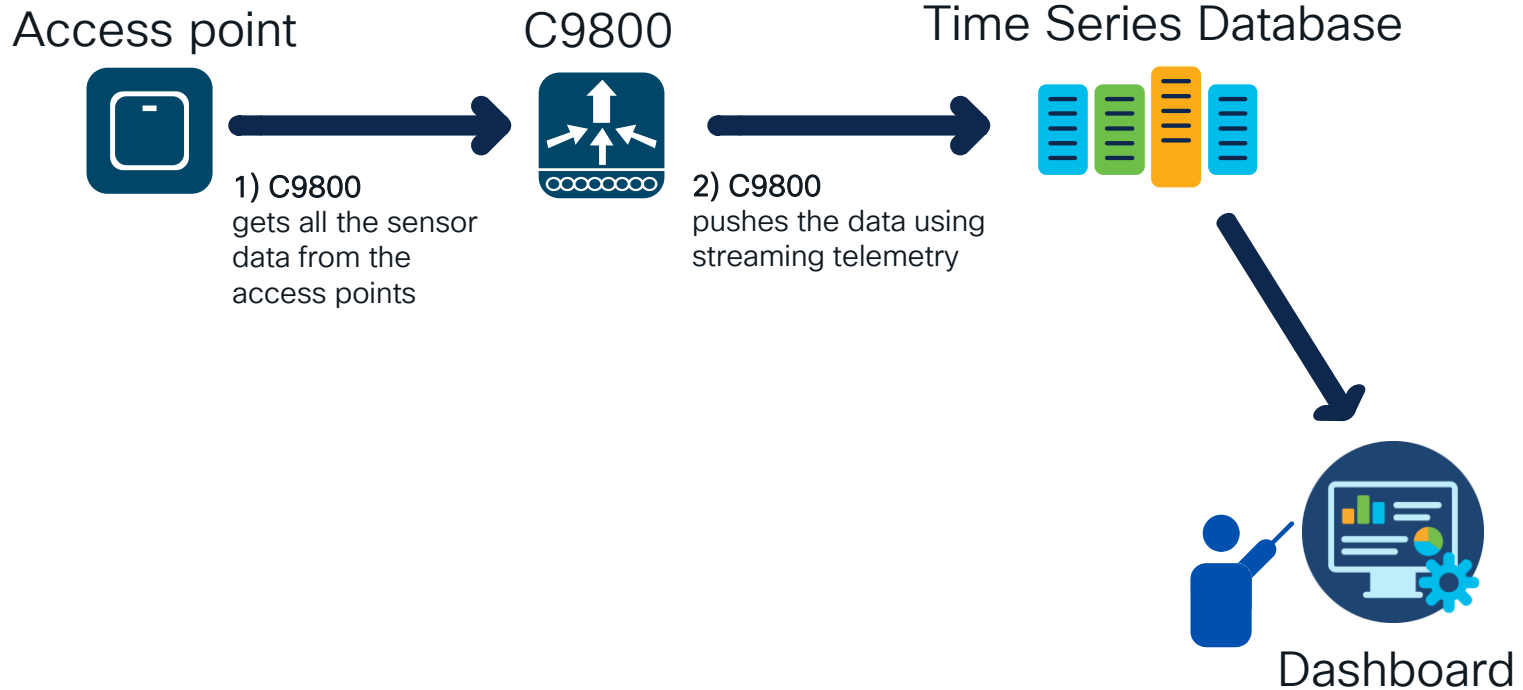


<https://github.com/CiscoSE/Catalyst-Telemetry>

AP sensor data in a customized dashboard (TIG stack)



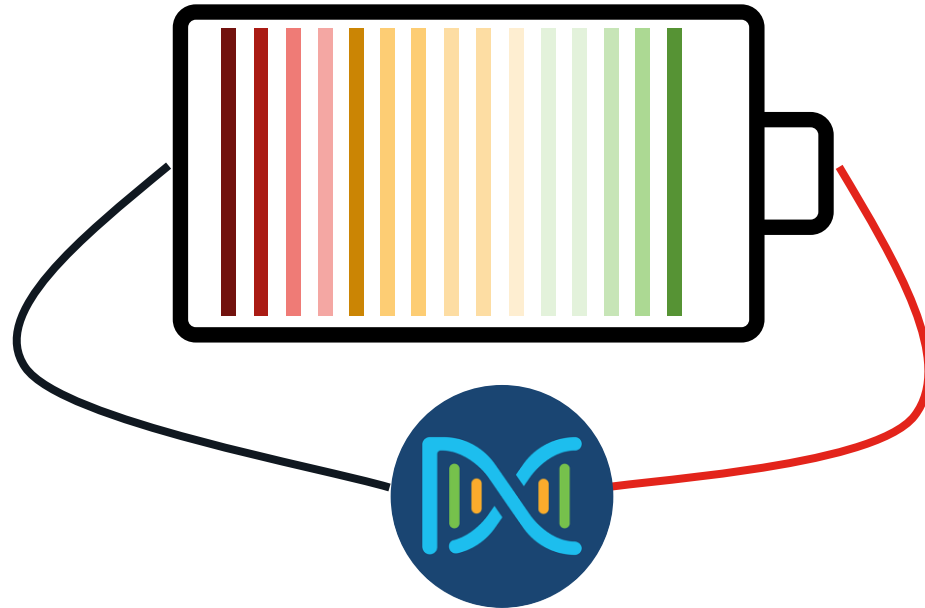
AP sensor data in a customized dashboard (TIG stack)



Your Cisco wireless battery

intent-based networking

DevOps



Agenda

CISCO *Live!*

- Expand usage with DevOps
 - Scripting
 - Remote Support Authorization

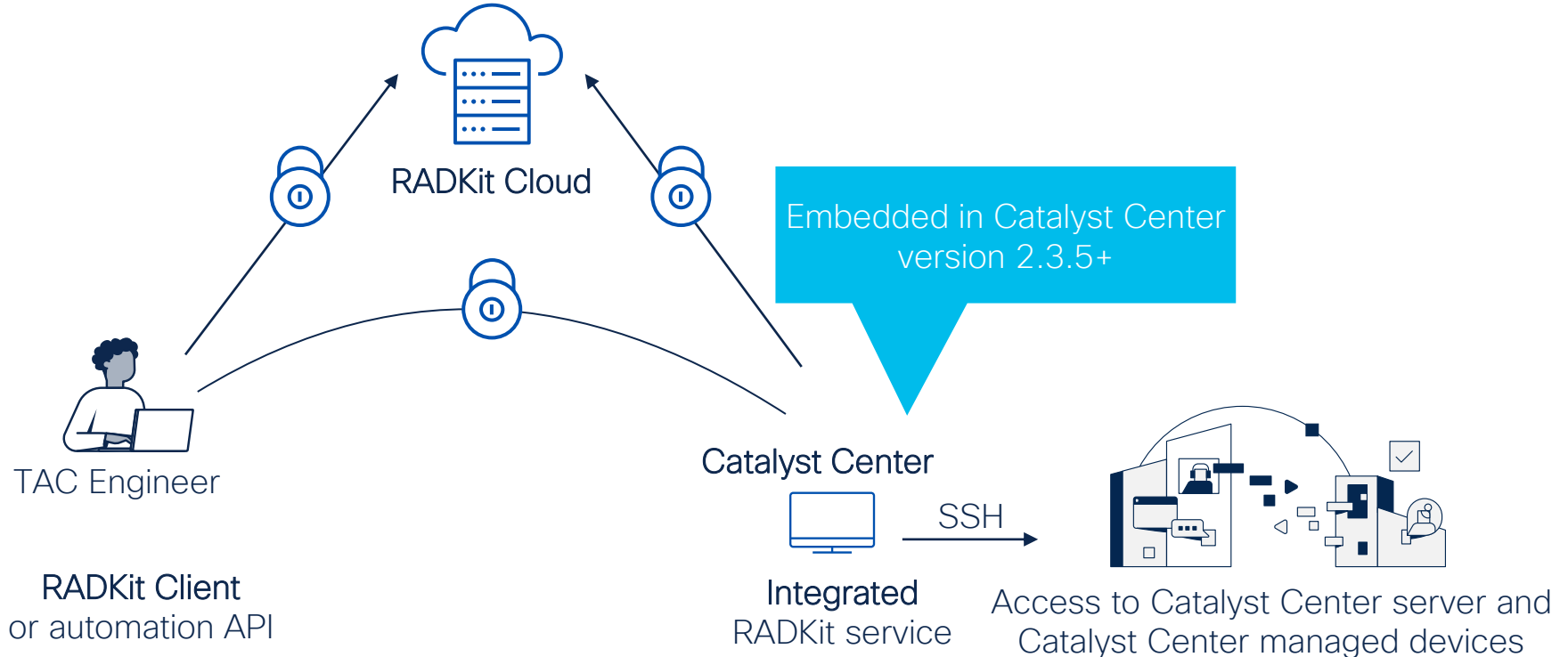
Current troubleshooting method

Resources, frustration level, time to resolution

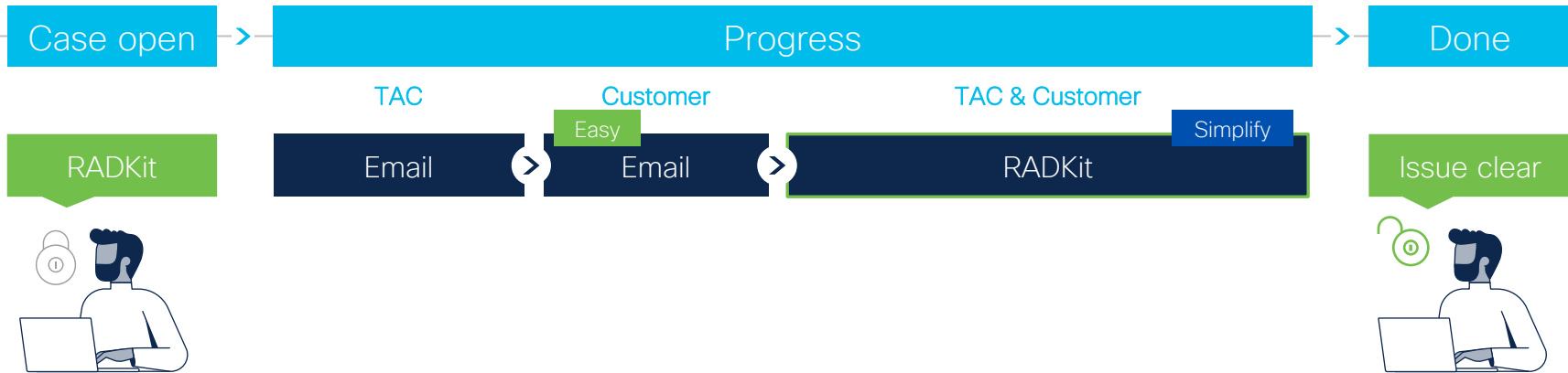


Remote Support Authorization aka RADKit

Get easily help when needed



RADKit Problem resolution life cycle



Welcome to Catalyst Center!

⚠️ Some of your license compliance requirements have not been met. [Learn more.](#)

🖥️ Explore

Assurance Summary

Health ⓘ

Healthy as of Jan 16, 2024 8:44 PM

67%

Network Devices

100%

Wireless Clients

--%

Wired Clients

[View Details](#)

Critical Issues

Last 24 Hours

3

P1

43

P2

[View Details](#)

- About
- Cisco DNA Sense
- API Reference [↗](#)
- Developer Resources [↗](#)
- Contact Support [↗](#)
- Remote Support Authorization
- Help [↗](#)
- Interactive Help
- Compatibility Information [↗](#)
- Keyboard Shortcuts [⌘ + /](#)
- Make a Wish

0

Trend Deviations

[View Details](#)

Network Snapshot

Sites

As of Jan 16, 2024 8:44 PM

41

DNS Servers : 0

NTP Servers : 0

[Add Sites](#)

Network Devices

As of Jan 16, 2024 8:44 PM

17

Unclaimed: 2

Unprovisioned: 5

Unreachable: 3

[Find New Devices](#)

Application QoS Policies

As of Jan 16, 2024 8:46 PM

0

Successful Deploys: 0

Errored Deploys: 0

Stale Policies: 0

[Add New Policy](#)

Prerequisites for Remote Support Authorization



Install Package
'Support Services'



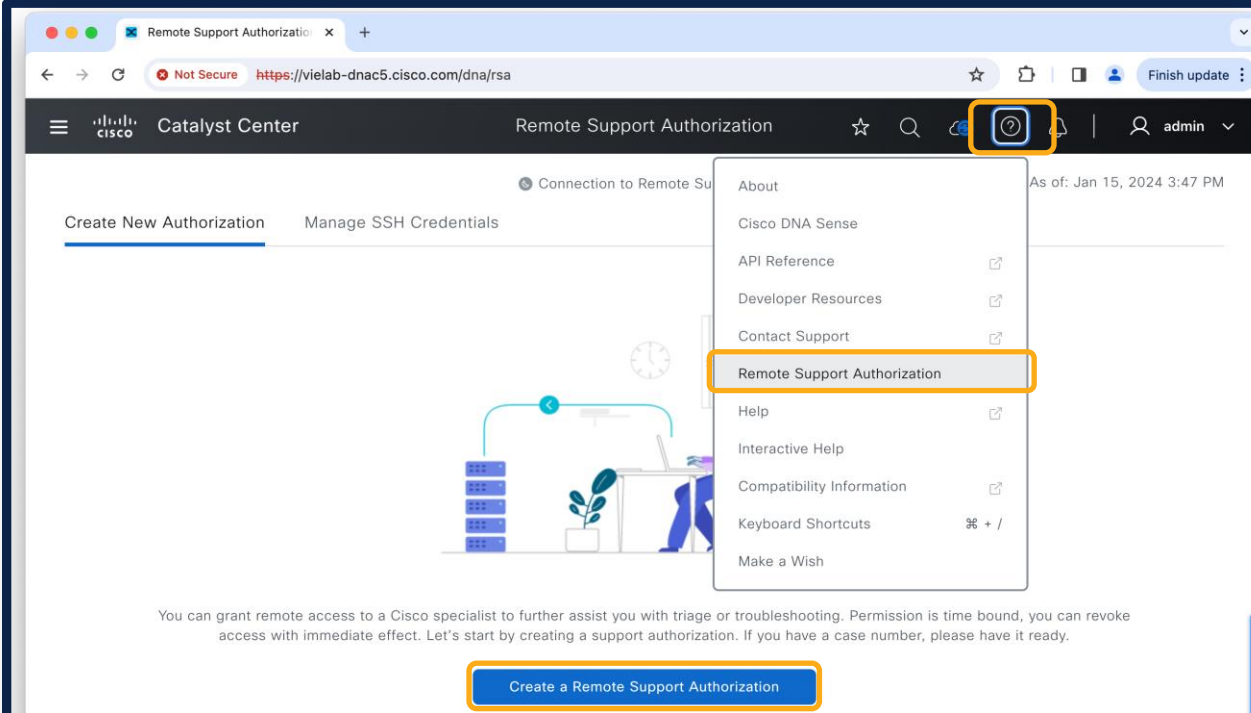
Have access to the RADKit
cloud through firewall or proxy
wss://prod.radkit-cloud.cisco.com:443

The screenshot shows the Cisco Catalyst Center web interface for software management. The page title is "Available applications for 2.3.7.4-70424". Below the title, there is a note: "The software packages below are available to install. During installation, we automatically check for dependencies and install them as well." A "Select All" link is present. There are four application cards displayed in a grid:

- Cisco Umbrella**: Cisco Umbrella is a service within Cisco DNA Center that provides a workflow to enable Cisco Umbrell... [View Details](#)
- Cloud Device Provisioning Application**: Cloud Device Provisioning is a workflow to on-board cloud hosted (AWS) CSR router or a Catalyst 9800... [View Details](#)
- Support Services**: Cisco Support personnel assigned to your open support cases can interact with and troubleshoot your ... [View Details](#) (This card is highlighted with an orange border and has a blue checkmark in the top right corner.)
- SD Access**: Cisco DNA Center automates SD Access, through provisioning of campus fabric overlay and user access ... [View Details](#)

How to use Remote Support Authorization?

- Create New Authorization



The screenshot displays the Cisco Catalyst Center interface for Remote Support Authorization. The browser address bar shows the URL <https://vielab-dnac5.cisco.com/dna/rsa>. The page title is 'Remote Support Authorization'. The navigation menu includes 'About', 'Cisco DNA Sense', 'API Reference', 'Developer Resources', 'Contact Support', 'Remote Support Authorization' (highlighted), 'Help', 'Interactive Help', 'Compatibility Information', 'Keyboard Shortcuts', and 'Make a Wish'. The main content area features a 'Create New Authorization' tab and a 'Manage SSH Credentials' tab. Below the tabs is an illustration of a person at a desk with a computer and server racks. At the bottom, there is a blue button labeled 'Create a Remote Support Authorization'.

How to use Remote Support Authorization?

- Create New Authorization
- Workflow defines What (Catalyst Center and/or Devices), Who (cisco.com user) and for How long it is enabled

Catalyst Center Create a Remote Support Authorization admin

Step 4 of 4: Summary

Review your selections. To make any changes, click **Edit** and make the necessary updates. When you are happy with your selections, click **Create**.

- ✓ Access Permission Agreement
 - Agreed to provide access to network devices.
 - Agreed to provide access to Cisco DNA Center.
- ✓ Set Up the Authorization [Edit](#)
 - Cisco Specialist Email Address shoneder@cisco.com
- ✓ Schedule the Access [Edit](#)

Scheduled For	Now
Duration	24 hours

Maximum 24 hours

[Exit](#) All changes saved [Back](#) [Create](#)

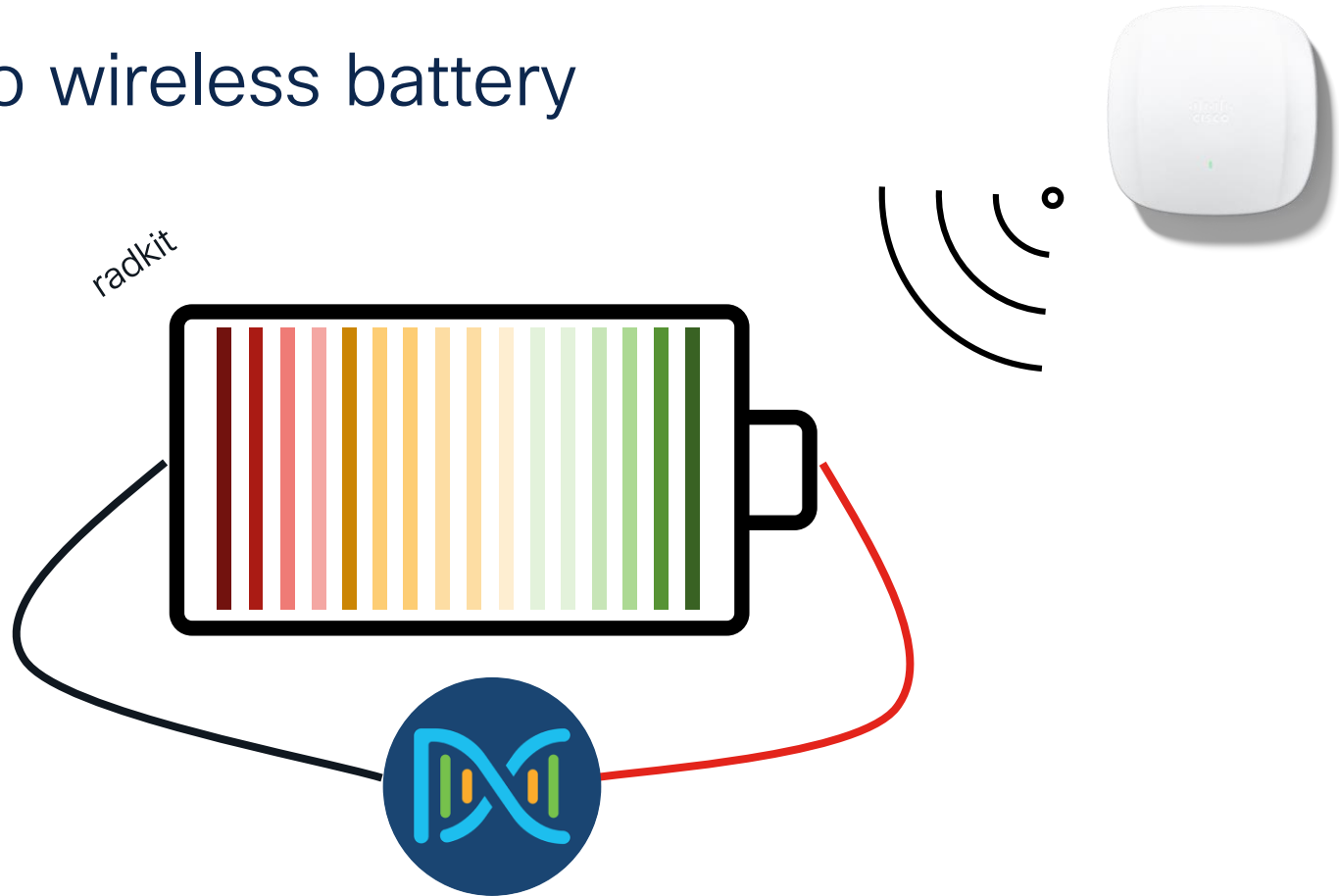
How to use Remote Support Authorization?

- Create New Authorization
- Workflow defines What (Catalyst Center and/or Devices), Who (cisco.com user) and for How long it is enabled
- Audit Logs show Activity

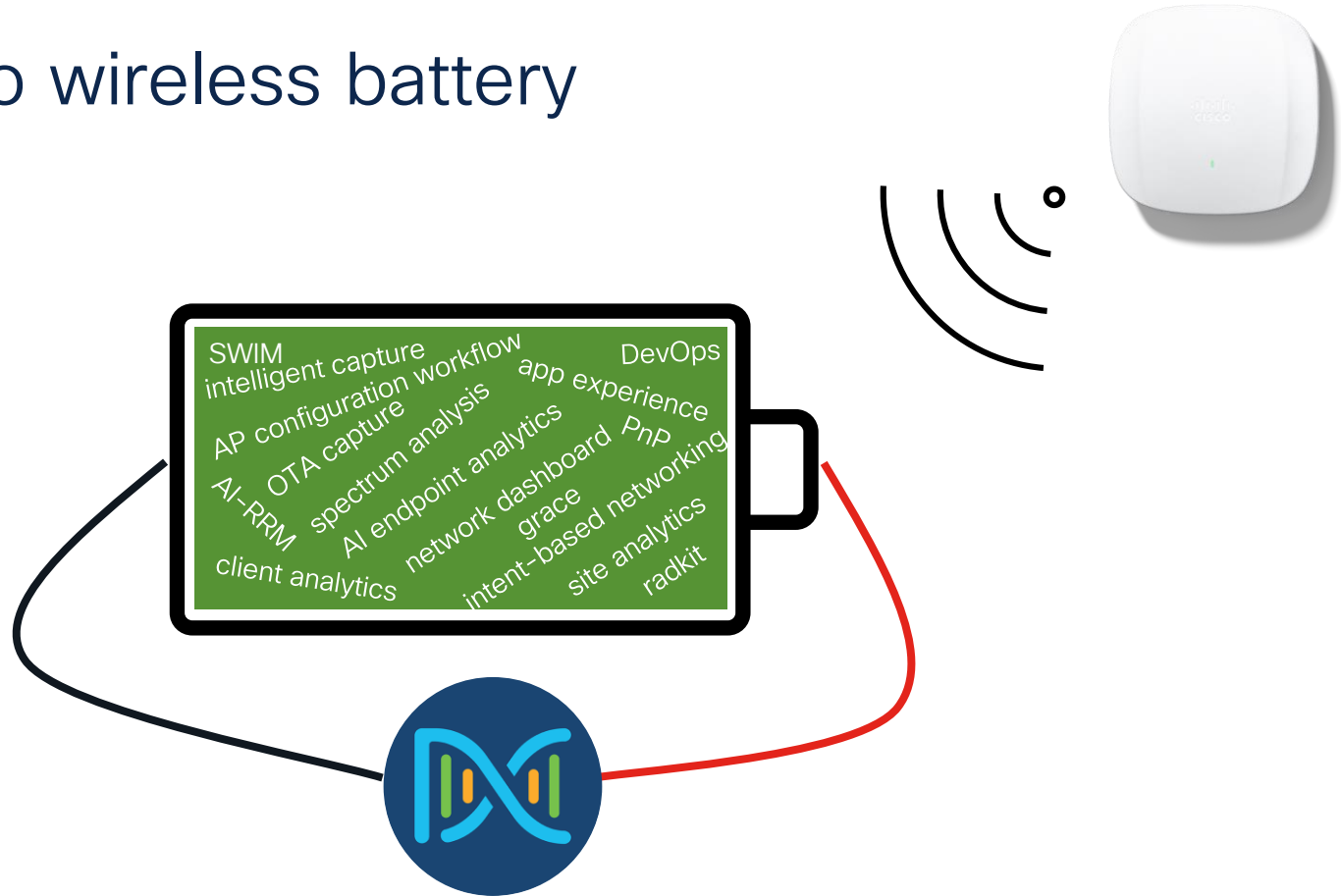
The screenshot displays the Cisco Catalyst Center interface, specifically the Audit Logs section. The page title is 'Catalyst Center' and the breadcrumb is 'Activities / Audit Logs'. The user 'admin' is logged in. The logs are filtered by date from 'Jan 16, 2023 04:23 PM' to 'Jan 15, 2024 04:23 PM'. A 'SUMMARY' section on the left shows 'Severity (3)' with options for Critical, Warning, and Info. A timeline view shows a log entry at 4:23p. Two log entries are highlighted with orange boxes:

- Log 1:** Jan 15, 2024 15:53 PM (CET) Log Id. Description: Login was successful for Remote Support User [shoneder@cisco.com]. User: system, Interface: API, Destination: SYSTEM, Source: NA.
- Log 2:** Jan 16, 2024 21:12 PM (CET) Log Id. Description: Executing command [maglev-config certs info] on the device [1.1.1.1]. User: system, Interface: API, Destination: SYSTEM, Source: NA.

Your Cisco wireless battery



Your Cisco wireless battery

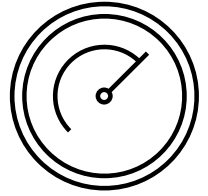




Agenda

- Introduction
- Get insights with AIOps
- Operate efficiently with NetOps
- Expand usage with DevOps
- Conclusion

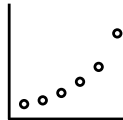
Conclusion



Catalyst Center brings your
Cisco Wireless to the next level!



Giving an unprecedented visibility



Ability to scale your work

Continue
your education

CISCO *Live!*



CTF booth at World of Solutions

Test your skills and earn
Cisco CE Credits*

CTF is gamified Hands-On
Cisco Technologies Labs!

* Ask at the booth for the qualifying missions

Next steps

If you don't have Catalyst Center and you are interested, contact your Cisco partner or the Cisco account team for help!

If you have Catalyst Center and you discovered something new:

Adopt it!



The bridge to possible

Thank you

CISCO *Live!*

The Cisco Live! logo features the word "CISCO" in a bold, black, sans-serif font, followed by "Live!" in a black, cursive script font. The background of the entire image is a vibrant, multi-colored abstract pattern of overlapping, wavy bands in shades of red, orange, yellow, green, and blue, radiating from a bright white point on the right side.

CISCO *Live!*

Let's go