

The background features a vibrant, abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, cyan, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

7 Habits for success with Cisco Catalyst Center

Jeff Lee
Technical Solutions Architect
CCIE#25598 (R&S)
BRKOPS-2416

CISCO *Live!*

#CiscoLiveAPJC

Who am I?

- Over 20 years IT/networking experience
- 4 years in Cisco as Enterprise Networking Specialist
- Avid cyclist (used to be good)
- Keen (if not very good) skier



Habit ...

... a thing that you do often and almost without thinking, especially something that is hard to stop doing.

Cisco Webex App

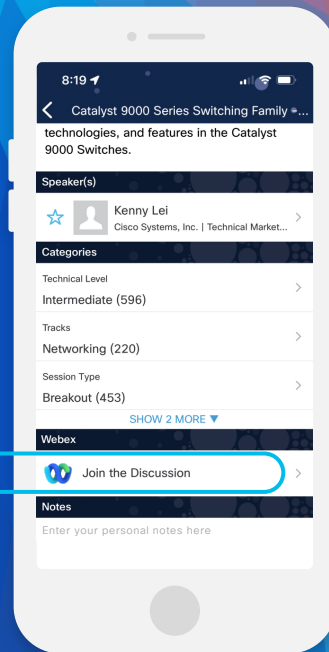
Questions?

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

How

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

Webex spaces will be moderated by the speaker until December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKOPS-2416>

Agenda

Habit #1 - Understanding and embracing Device Controllability

Habit #2 - Find issues before your users with telemetry

Habit #3 - Leverage Compliance and Configuration management

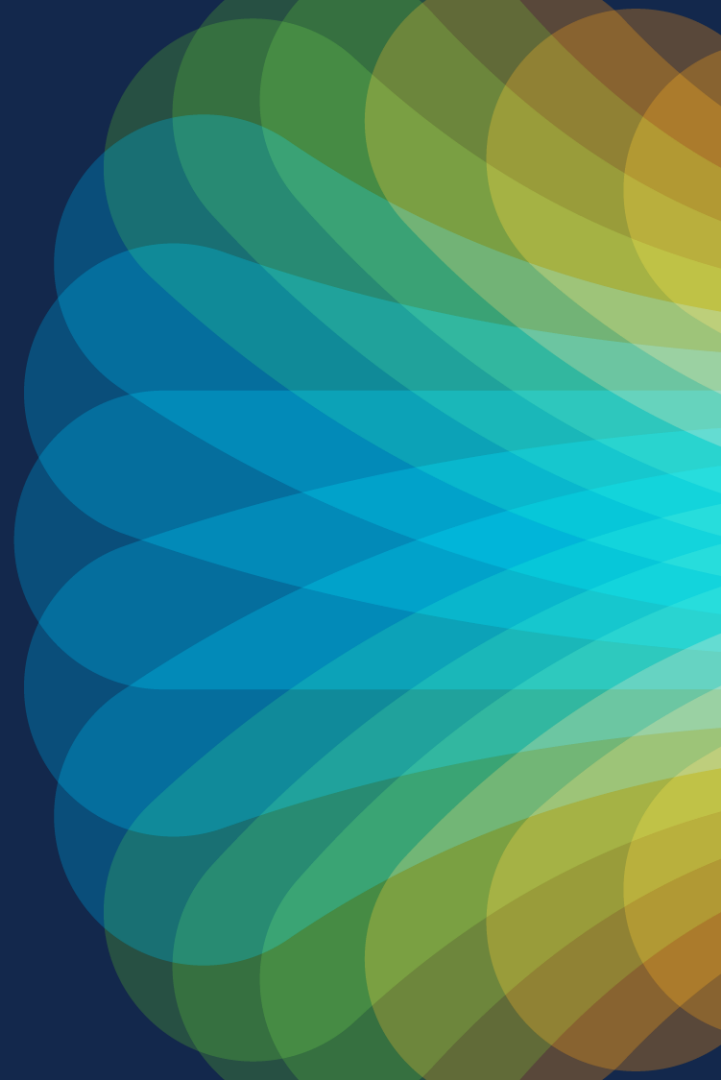
Habit #4 - Keep your infrastructure code up to date with software image management

Habit #5 - Explore Proactive insights with AI/ML

Habit #6 - Ease your remote support with RADKit

Habit #7 - Up your automation game with APIs and other integrations

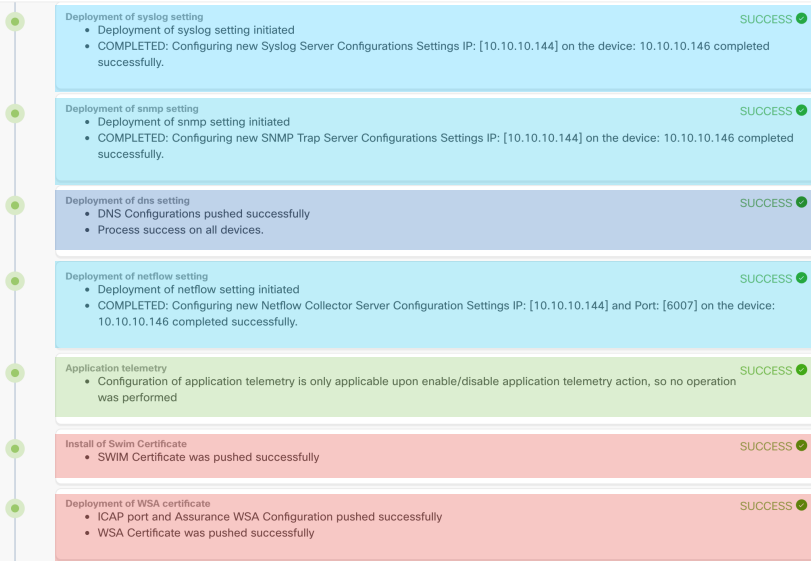
Habit #1 – Understanding (and embracing) device controllability



Device Controllability

reallylongName2.adamlab.cisco.com

Management IP 10.10.10.146
Device Type Cisco Catalyst 9800-CL Wireless Controller for Cloud
Device Role ACCESS



A vertical timeline showing the sequence of configuration steps for Device Controllability. Each step is represented by a colored box with a green dot on the left and a 'SUCCESS' status with a green checkmark on the right.

- Deployment of syslog setting** (Light Blue)
 - Deployment of syslog setting initiated
 - COMPLETED: Configuring new Syslog Server Configurations Settings IP: [10.10.10.144] on the device: 10.10.10.146 completed successfully.
- Deployment of snmp setting** (Light Blue)
 - Deployment of snmp setting initiated
 - COMPLETED: Configuring new SNMP Trap Server Configurations Settings IP: [10.10.10.144] on the device: 10.10.10.146 completed successfully.
- Deployment of dns setting** (Light Blue)
 - DNS Configurations pushed successfully
 - Process success on all devices.
- Deployment of netflow setting** (Light Blue)
 - Deployment of netflow setting initiated
 - COMPLETED: Configuring new Netflow Collector Server Configuration Settings IP: [10.10.10.144] and Port: [6007] on the device: 10.10.10.146 completed successfully.
- Application telemetry** (Light Green)
 - Configuration of application telemetry is only applicable upon enable/disable application telemetry action, so no operation was performed
- Install of Swin Certificate** (Light Red)
 - SWIM Certificate was pushed successfully
- Deployment of WSA certificate** (Light Red)
 - ICAP port and Assurance WSA Configuration pushed successfully
 - WSA Certificate was pushed successfully

Monitoring

Settings

Telemetry

Trust

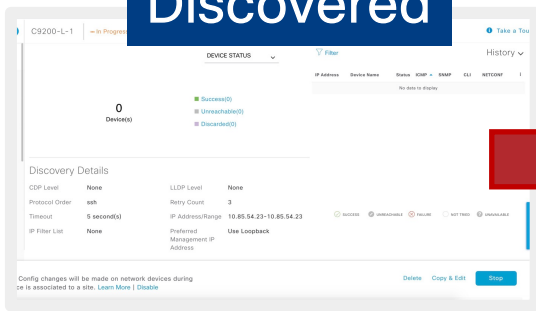


A vertical timeline showing the sequence of configuration steps for Monitoring, Settings, Telemetry, and Trust. Each step is represented by a colored box with a green dot on the left and a 'SUCCESS' status with a green checkmark on the right.

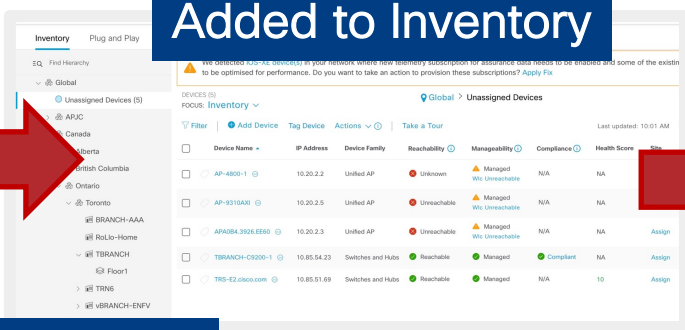
- Deployment of Wireless AP Join Certificate** (Light Red)
 - Certificate already exists on the device.
 - Deployment of Wireless AP Join Certificate setting initiated
- Deployment of PKCS12 certificate** (Light Red)
 - Started process: Pkcs12 Internal Certificate Configure
 - Reachable DNAC IP: 10.10.10.144
 - PKI Configurations pushed successfully
 - PKCS12 Certificate was pushed successfully
- Deployment of IOS WLC NA Certificate configuration** (Light Red)
 - Setting does not apply to device, so no operation was performed
- Deployment of IOS Telemetry Subscriptions configuration** (Light Green)
 - Configuring Assurance Telemetry Receiver Information
 - Configuring Assurance Telemetry Subscriptions
 - Configured Telemetry Subscription Receiver on the device with Receiver as 10.10.10.144
 - Assurance Telemetry Subscriptions Configuration Success
 - App Based Telemetry Subscriptions Configuration Success
 - Telemetry Subscriptions was pushed successfully
 - App Based Telemetry Subscriptions Configuration Success
- Deployment of AP Impersonation configuration** (Light Blue)
 - AP Impersonation pushed successfully
 - Deployment of AP Impersonation setting initiated
- Deployment of Terminal Width** (Light Blue)
 - Setting does not apply to device, so no operation was performed
- Deployment of IPDT** (Light Blue)
 - Cannot push IPDT Configuration on the device with IpAddress: 10.10.10.146 for Product Family: wireless controller (Not Applicable)

Brownfield device on-boarding and config automation process into Catalyst Center

Discovered



Added to Inventory

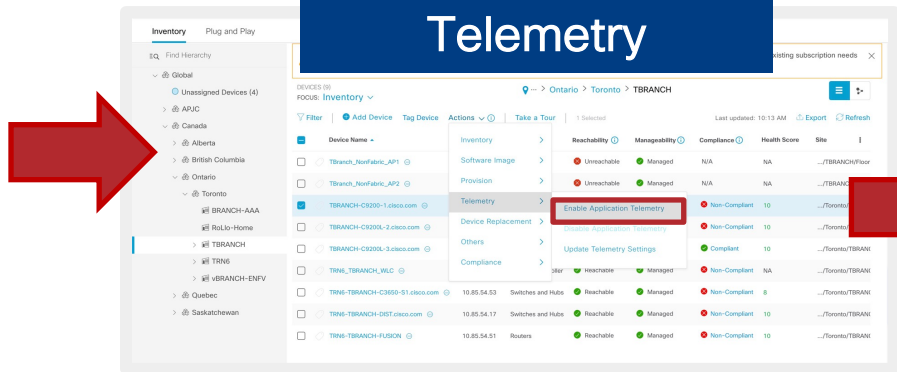


Assigned to Site

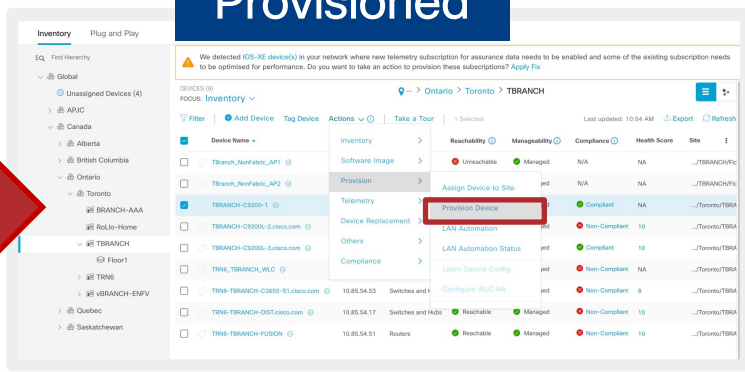
Device
Controllability
happens here



Enabled for Telemetry



Provisioned



Adding a device to Catalyst Center – Assign to Site

The screenshot shows the Cisco DNA Center interface with the 'Assign Device to Site' dialog box open. The dialog displays the following settings for device TBRANCH-C9200-1:

Setting	Value
Syslog Server	Cisco DNA Center
Netflow Collector	Cisco DNA Center
IP Device Tracking	Yes
SNMP Trap Receiver	Cisco DNA Center, 10.10.10.10
Cisco TrustSec (CTS) Credentials	No
Syslog Level	6 - Information Messages
Controller Certificates	Yes

At the bottom of the dialog, the 'Device Controllability' status is shown as 'Enabled'. A red box highlights the 'Device Controllability is Enabled. Learn More | Disable' text.

The background shows the 'Inventory' page with a list of devices. The device TBRANCH-C9200-1 is selected in the list.

Adding a device to Catalyst Center – Assign to Site

Cisco DNA Center Provision / Network Devices / Inventory

Preview New Page 🔍 ⓘ 🔔

Inventory Plug and Play Inventory Insights

Find Hierarchy 🔍

Global

- Unassigned Devices (7)
- APJC
- Canada
- Alberta

DEVICES (41) FOCUS: Inventory ▾

Filter | Add Device Tag D

Device Name ▾

Assign Device to Site ✕

☐ Now ☐ Later ☒ **Generate configuration preview**
Creates preview which can be later used to deploy on selected devices.

Task Name*

Activities / Work Items 🔍 ⓘ 🔄 🔔

SITE ASSIGNMENT ✕

Configuration preview: Assign/Unassign 1 Device(s) to/from Site

Dec 23, 2022 11:46 AM | Status: ✔ Success | Last updated: 11:47:08 AM [Refresh](#)

Search by description 🔍

SITE ASSIGNMENT	
lila	
Configuration preview: Assign/Unassign 1 Device(s) to/from Site	
Dec 23, 2022 11:40 AM	Sta
SITE ASSIGNMENT	
lila	
Configuration preview: Assign/Unassign 1 Device(s) to/from Site	
Dec 23, 2022 11:38 AM	Sta
SITE ASSIGNMENT	
lila	
Configuration preview: Assign/Unassign 1 Device(s) to/from Site	
Dec 23, 2022 11:46 AM	Sta

DEVICES

TBRANCH-C9200L-2

Configuration Preview 🔍 ⓘ 🔄 🔔

Device IP : 10.85.54.24

```
1 !SysloglistConfigs
2 logging host 10.85.54.177 transport udp port 514
3 logging source-interface Vlan419
4 logging trap 6
5 !done
6 !SysloglistConfigs
7 !done
8 snmp-server enable traps
9 snmp-server host 10.85.54.177 traps version 2c ***** udp-port 162
10 snmp-server source-interface traps Vlan419
11 !NetflowConfigs
12 flow exporter 10.85.54.177
13 destination 10.85.54.177
14 transport udp 6007
15 exit
16 !done
17 !NetflowConfigs
18 !done
19 no crypto pki trustpoint DNAC-CA
20 crypto key ***** rsa DNAC-CA
21 <mdt-config-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-mdt-cfg">
22   <mdt-subscription nc:operation="remove">
23     <subscription-id>
24       <![CDATA[553]]>
25     </subscription-id>
26   </mdt-subscription>
27 </mdt-config-data>
28 <mdt-config-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-mdt-cfg">
```

Device Controllability

Site-level customization

Cisco DNA Center Design / Network Settings

Network Device Credentials IP Address Pools SP Profiles Wireless **Telemetry** Security and Trust

aaa Search Help

Global Canada Ontario Toronto BRANCH-AAA

Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings are assigned to a site or provisioned.

Cisco DNA Center is your default SNMP collector. It polls network devices to gather telemetry data. View metrics gathered and the frequency with which they are collected.

SNMP Traps

Choose Cisco DNA Center to be your SNMP trap server, and/or add any external SNMP trap servers. These are the destination servers for SNMP traps and messages from network devices.

☒ Use Cisco DNA Center as SNMP trap server

☒ Add an external SNMP trap server

IP Address

10.10.10.10 +

Syslogs

Choose Cisco DNA Center to be your syslog server, and/or add any external syslog servers. Devices will be provisioned with syslog severity level 6 (information messages) when they are assigned to a site and/or provisioned.

☒ Use Cisco DNA Center as syslog server

☐ Add an external syslog server

Telemetry Configuration:

- SYSLOG Server
- SNMP Trap Server
- SNMP Polling
- NetFlow
- Wired Client Data Collection

Cisco Catalyst Center is configured as Syslog server, SNMP Trap Server and Netflow collector server by default

Device Controllability

Site-level customization

The screenshot shows the Cisco DNA Center interface with the 'Telemetry' tab selected. The left sidebar shows a hierarchy: Global > Canada > Ontario > Toronto > BRANCH-AAA. The main content area is titled 'Design / Network Settings' and contains the following text:

Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned.

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.

NetFlow

Choose Cisco DNA Center to be your NetFlow collector server, and/or add any external NetFlow collector server. This is the destination server for NetFlow export from network devices. Cisco DNA Center will only push the first NetFlow collector server for Wireless Controller as it has a restriction on the number of flow exporters.

☒ Use Cisco DNA Center as NetFlow collector server

INTERFACES FOR APPLICATION TELEMETRY

To enable telemetry on a device, select the device from the Provision table and choose "Actions->Enable Application Telemetry". By default, All access interfaces on a switch OR all LAN-facing interfaces on a router will be provisioned. To override this default behavior, tag specific interfaces to be designated as LAN interface, by putting the keyword "lan" in the interface description.

Once specific interfaces are tagged those interfaces will be monitored.

☐ Add Cisco Telemetry Broker (CTB)

Cisco DNA Center should be configured as a destination in CTB to receive Netflow records.

The screenshot shows the Cisco DNA Center interface with the 'Telemetry' tab selected. The left sidebar shows a hierarchy: Global > Canada > Ontario > Toronto > BRANCH-AAA. The main content area is titled 'Design / Network Settings' and contains the following text:

Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned.

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.

Wired Endpoint Data Collection

The primary function of this feature is to track the presence, location, and movement of wired endpoints in the network. Traffic received from endpoints is used to extract and store their identity information (MAC address and IP address). Other features, such as IEEE 802.1X, web authentication, Cisco Security Groups (formerly TrustSec), SD-Access, and Assurance, depend on this identity information to operate properly.

Wired Endpoint Data Collection enables Device Tracking policies on devices assigned to the Access role in Inventory.

☒ Enable Cisco DNA Center Wired Endpoint Data Collection At This Site

☐ Disable Cisco DNA Center Wired Endpoint Data Collection At This Site

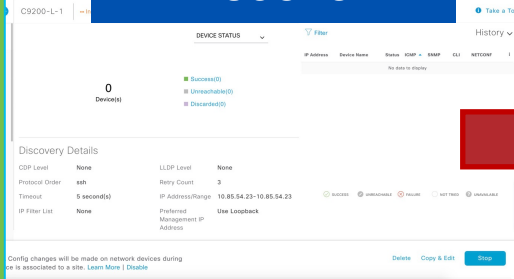
Wireless Controller, Access Point and Wireless Clients Health

Enables Streaming Telemetry on your wireless controllers in order to determine the health of your wireless controller, access points and wireless clients.

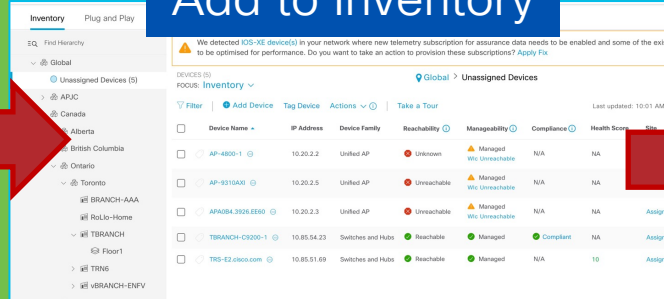
☒ Enable Wireless Telemetry

Brownfield device on-boarding and config automation process into Catalyst Center

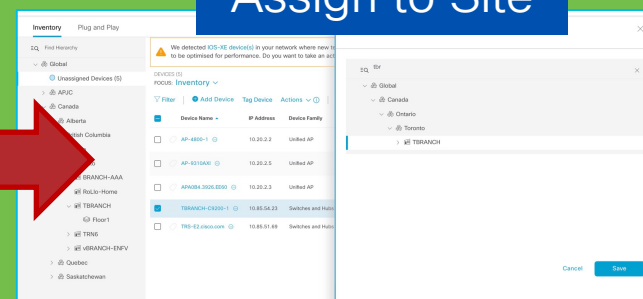
Discover



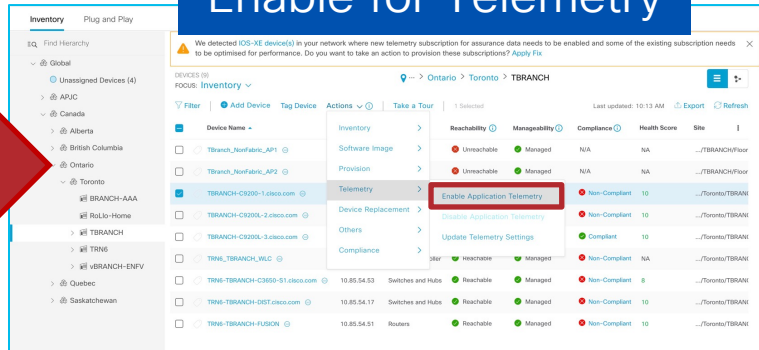
Add to Inventory



Assign to Site



Enable for Telemetry



Green steps can be done in a single discovery workflow

Discovery Workflow



For your
reference

Discovery

Discover Devices

Begin by naming this discovery job. Then, select your preferred type of discovery. Discovered devices will be assigned to a site later in this workflow. Access Points associated with discovered wireless controllers will be automatically added to Inventory()

Discovery Job Name*

DISCOVERY TYPE

☐ CDP ☒ IP Address Range ☐ LLDP ☐ CDG

Add ranges for the network device, not endpoints. No need to add for APs or sensors as they will be auto-discovered via WLC's. Check out the list of Discoverable Devices

IP ADDRESS RANGE

Starting P Address* 10.85.54.25 Ending P Address* 10.85.54.25

PREFERRED MANAGEMENT IP ADDRESS

☒ None ☐ Use (Loopback If Applicable)

Back Next

Credentials

Provide Credentials

Next, enter the following credentials that Cisco DNA Center will configure for the devices it discovers. At least one CLI credential and one SNMP credential are required. You can have a maximum of five global credentials and one job specific credential for each type.

CLI SNMPv2c Read SNMPv2c Write SNMPv3 HTTP(S) Read HTTP(S) Write NETCONF

Select from existing credentials or add new ones. You can add either a job specific credential or a global credential.

EXISTING GLOBAL CLI CREDENTIALS

☒ netadmin ☐ admin ☐ Lila ☐ NFVIS netadmin ☐ francis ☐ prabhjit-device-creds

+ Add CLI Credentials

Assign to Site

Assign Devices to Site

After device discovery, we recommend that you assign devices to the site to facilitate telemetry. You can assign devices to any building or floor within the site hierarchy. The devices that are already discovered and associated with a site will be skipped for site assignment.

How do you want to assign devices discovered in this workflow to a site?

☒ Assign devices to an existing site ☐ Assign devices to a new site ☐ Skip site assignment for now

Search tbr

Global

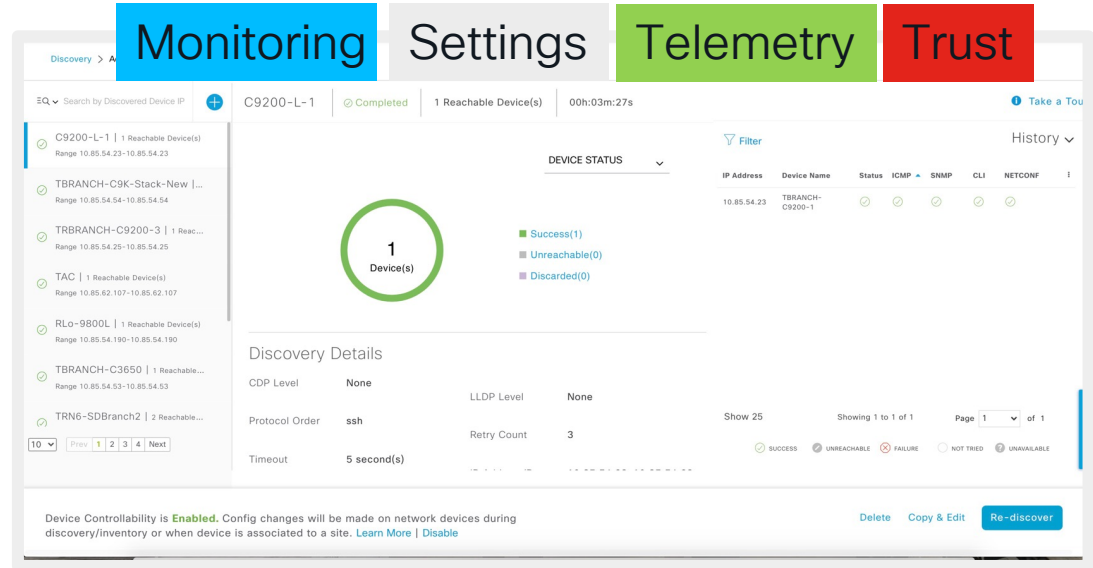
Canada

Ontario

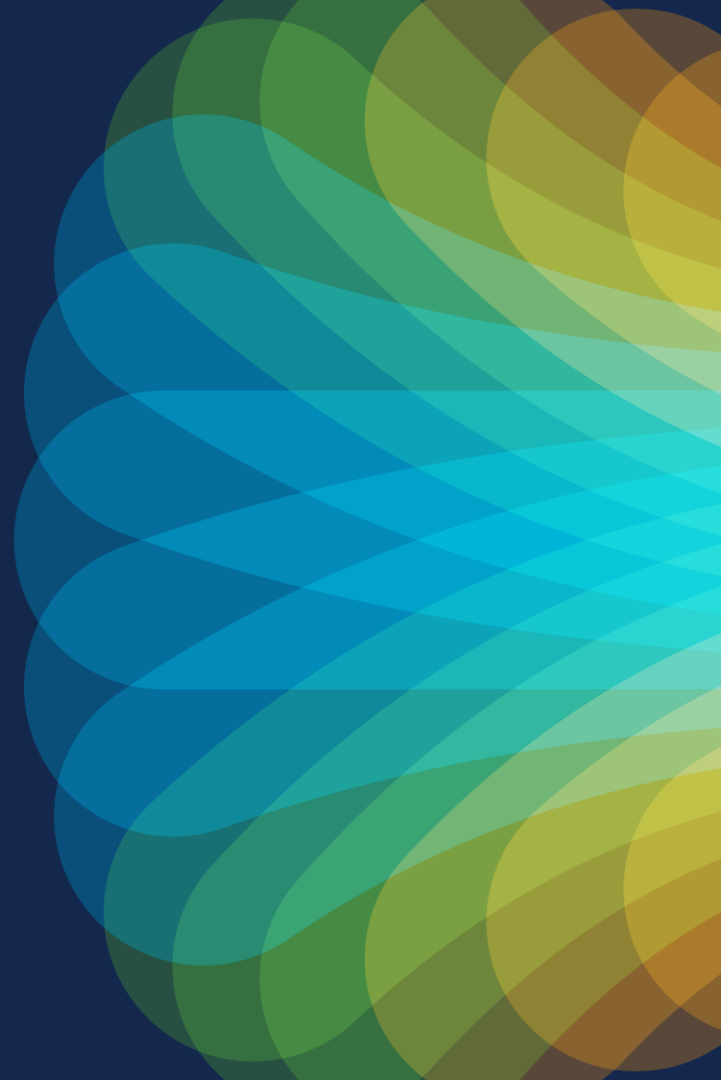
Toronto

TBRANCH

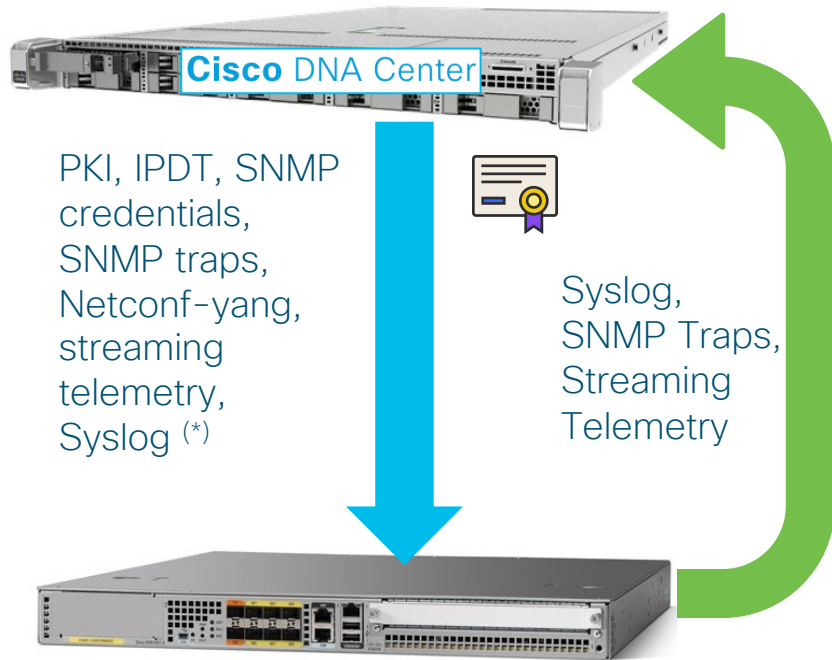
- Device Controllability allows **devices to interact with Catalyst Center efficiently**
- Recommended to **keep Device Controllability enabled** and send configs to Catalyst Center
- Controllability is **safe and easy to troubleshoot**
- Cisco Catalyst Center now provides **comprehensive visibility and customizations** into Device Controllability configurations



Habit #2 – Find issues **before** your users with telemetry



Benefits of Telemetry data captured via Catalyst Center



- Network Network and Client Health
- Application Health
- Network Services (AAA, DHCP, DNS)
- View and Manage Issues
- Visibility into Wi-Fi 6/6E Readiness
- Monitor Power over Ethernet
- EoX Insights
- Inventory Insights
- Network Trends and Insights

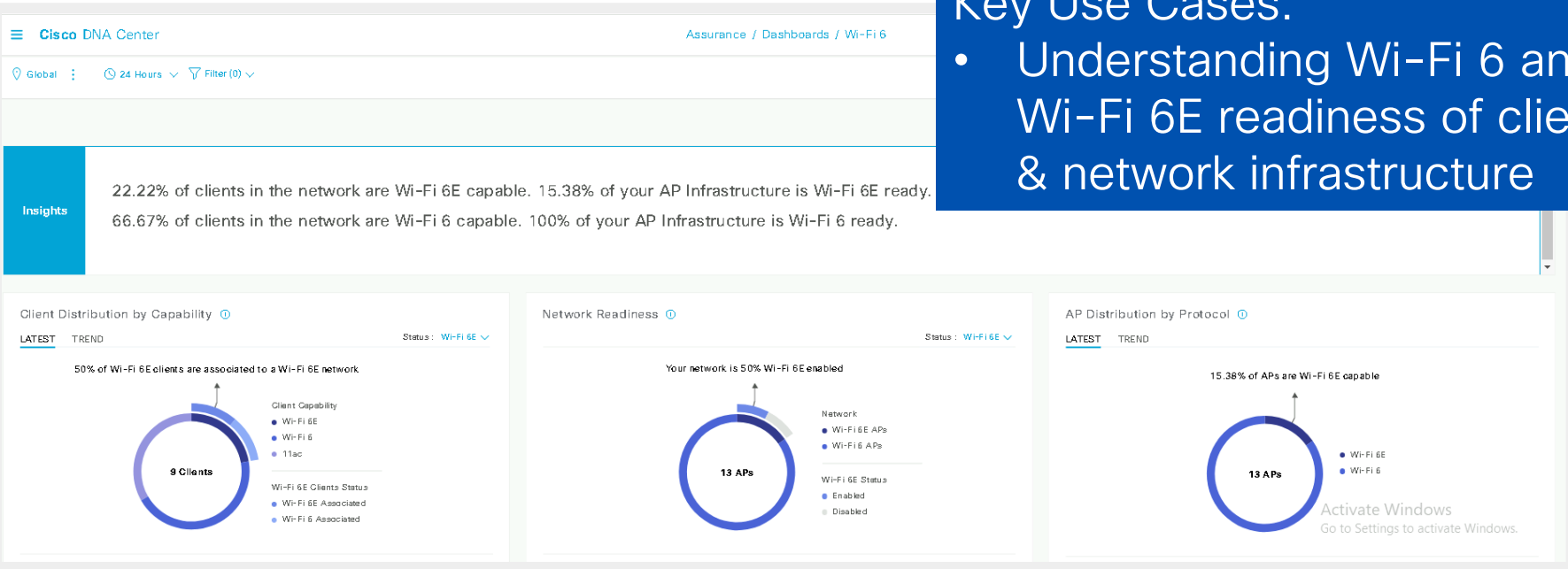


Demo

Wi-Fi 6 Readiness Dashboard

Key Use Cases:

- Understanding Wi-Fi 6 and Wi-Fi 6E readiness of clients & network infrastructure



Wi-Fi 6 Readiness Dashboard

Key Use Cases:

- Visualizing the benefits of an existing Wi-Fi 6 and Wi-Fi 6E Network

Cisco DNA Center

Assurance / Dashboards / Wi-Fi 6

Global 24 Hours Filter (0)

Insights

22.22% of clients in the network are Wi-Fi 6E capable. 15.38% of your AP Infrastructure is Wi-Fi 6E ready.
66.67% of clients in the network are Wi-Fi 6 capable. 100% of your AP Infrastructure is Wi-Fi 6 ready.

Client Distribution by Capability

LATEST TREND Status: Wi-Fi 6E

50% of Wi-Fi 6E clients are associated to a Wi-Fi 6E network.



Client Capability

Wi-Fi 6E Clients Status

Network Readiness

LATEST TREND Status: Wi-Fi 6E

Your network is 50% Wi-Fi 6E enabled



Network

AP Distribution by Protocol

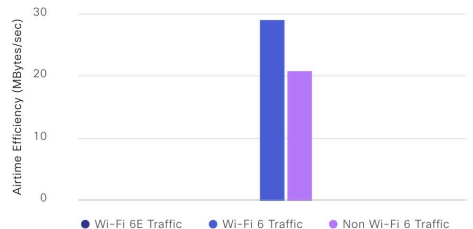
LATEST TREND Status: Wi-Fi 6E

15.38% of APs are Wi-Fi 6E capable



Wireless Airtime Efficiency BETA

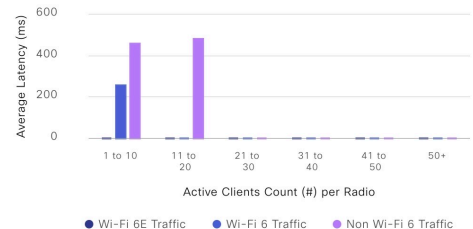
LATEST TREND View: Voice



View Details

Wireless Latency by Client Count BETA

LATEST TREND View: Voice



View Details

Wi-Fi 6 Readiness Dashboard



For your
reference

Wi-Fi 6 clients
associated with
Wi-Fi 6 network

Client Distribution by Capability ⓘ

LATEST TREND

84% of Wi-Fi 6 clients are associated to a Wi-Fi 6 network

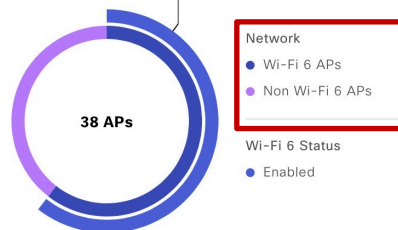


[View Details](#)

Percentage of APs
Wi-Fi 6 enabled

Wi-Fi 6 Network Readiness ⓘ

Your network is 60.53% Wi-Fi 6 enabled

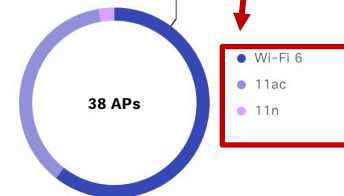


Percentage of
APs Wi-Fi 6
capable

AP Distribution by Protocol ⓘ

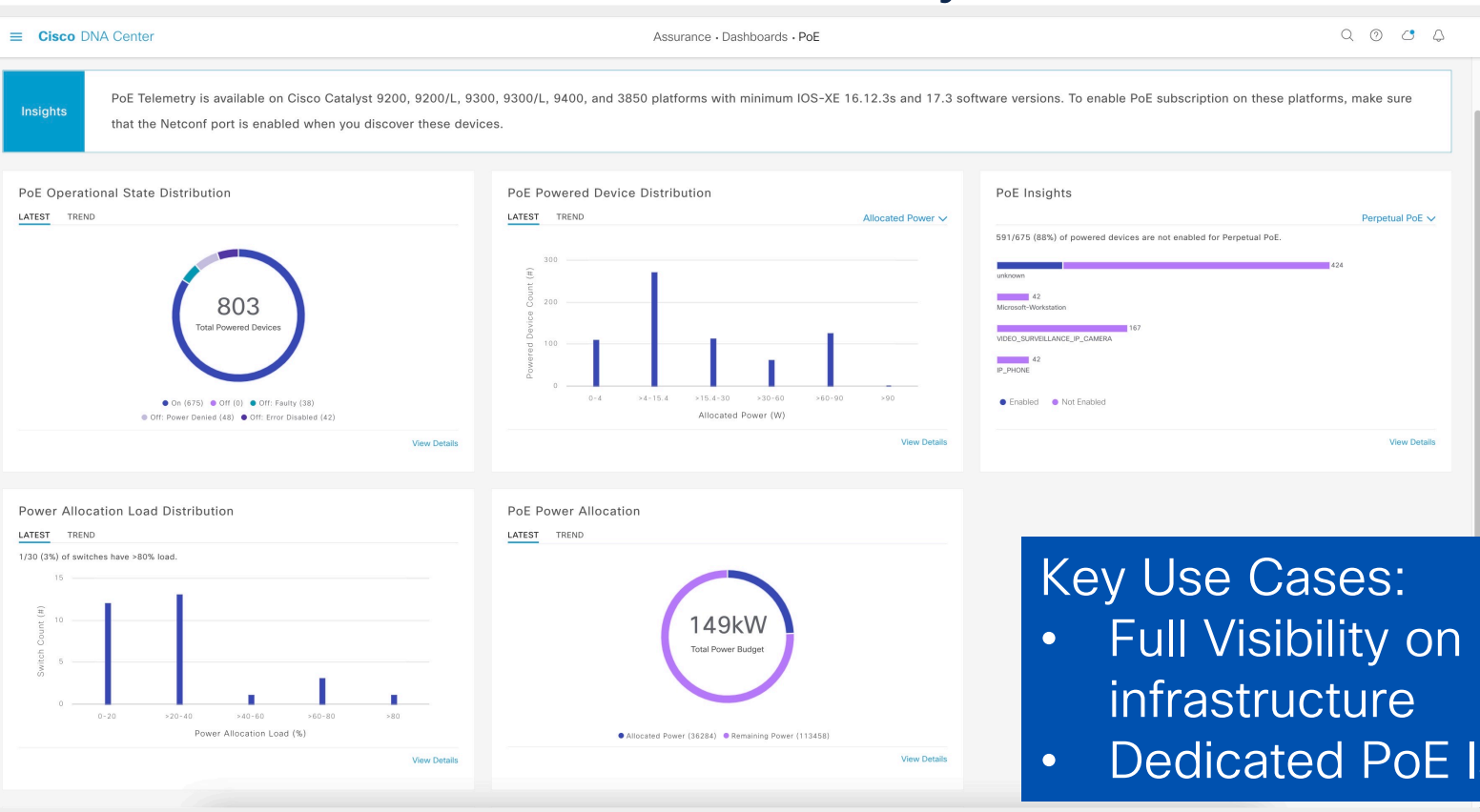
LATEST TREND

60.53% of APs are Wi-Fi 6 capable



[View Details](#)

Power over Ethernet Analytics



- ## Key Use Cases:
- Full Visibility on PoE infrastructure
 - Dedicated PoE Issue Types

Power over Ethernet Analytics

Percentage of the devices using PoE and configured with: Perpetual PoE, Fast PoE, IEEE Compliant or UPOE+

PoE Insights

IEEE Compliant ▾

0/25 (0%) of powered devices are not IEEE Compliant.



● Yes ● No

Perpetual PoE

- Uninterrupted PoE power during control plane reboot

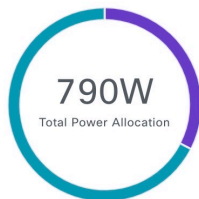
Allocated & Remaining Power

Power Usage

LATEST

TREND

Allocation ▾



● PoE Power Allocation (257W)

● System Power Allocation (0W)

Fast PoE

- Bypasses Cisco IOS® control plane boot
- Restores power to Powered Device (PD) within 30 seconds of power resumption

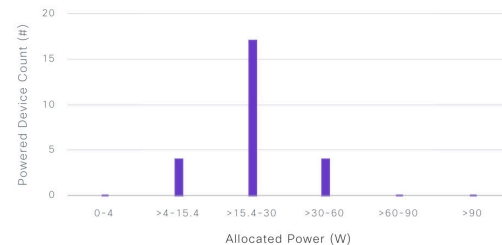
Type type of devices and their power consumption.

PoE Powered Device Distribution

LATEST

TREND

Allocated Power ▾



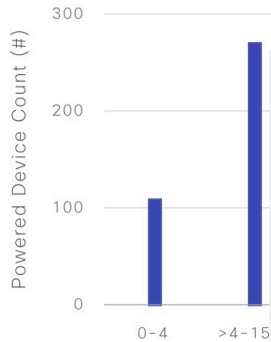
[View Details](#)

Power over Ethernet Analytics

PoE Powered Device Distribution

LATEST

TREND



PoE Powered Device Distribution

24 hours: Apr 26, 1:03 PM - Apr 27, 1:03 PM | Global

Allocated Power



PoE Powered Device Distribution

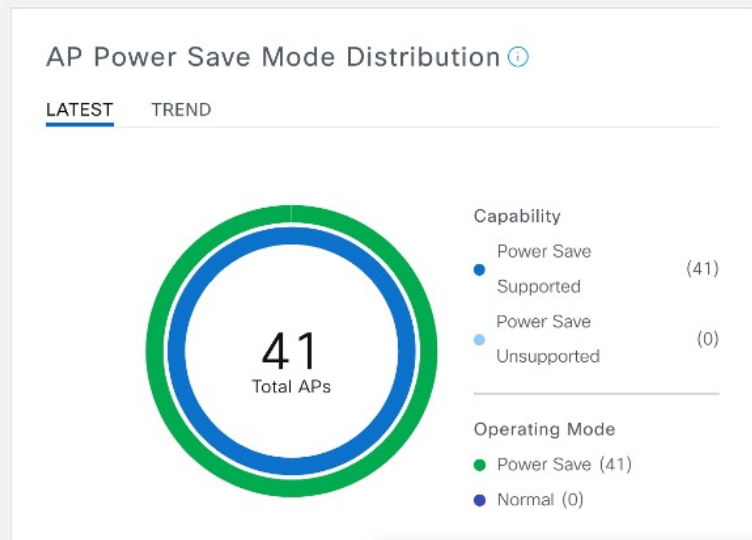
24 hours: Apr 26, 1:03 PM - Apr 27, 1:03 PM | Global

Search Table

Identifier	Powered Device Model	Powered Device Type	Connected Switch	Switch Interface	IEEE Compliant	Location	Allocated Power
--	AIR-AP3802I-B-K9	unknown	p1.edge1-sda1.local	GigabitEthernet1/0/15	Yes	Global/North America/USA/California/San Jose/SJC01	90
--	IP Phone 6961	unknown	SJC06-C9300-01	GigabitEthernet1/0/1	Yes	Global/North America/USA/California/San Jose/SJC06	90
--	IP Phone 6961	unknown	SJC06-C9300-01	GigabitEthernet1/0/3	Yes	Global/North America/USA/California/San Jose/SJC06	90
--	IEEE PD	unknown	SJC06-C9300-01	GigabitEthernet1/0/16	Yes	Global/North America/USA/California/San Jose/SJC06	90
--	AIR-AP2802I-B-K9	unknown	SJC06-C9300-02	GigabitEthernet1/0/3	Yes	Global/North America/USA/California/San Jose/SJC06	90
--	IP Phone 6961	unknown	SJC06-C9300-02	GigabitEthernet1/0/24	Yes	Global/North America/USA/California/San Jose/SJC06	90

AP Power Savings Insights

Visualize Your Power Savings!



AP Power Save Mode Distribution

- Outer Ring: Depicts # of APs in Power Save or Normal Mode
- Inner Ring: Depicts APs that support Power Save mode as only higher-end APs support Power Save mode

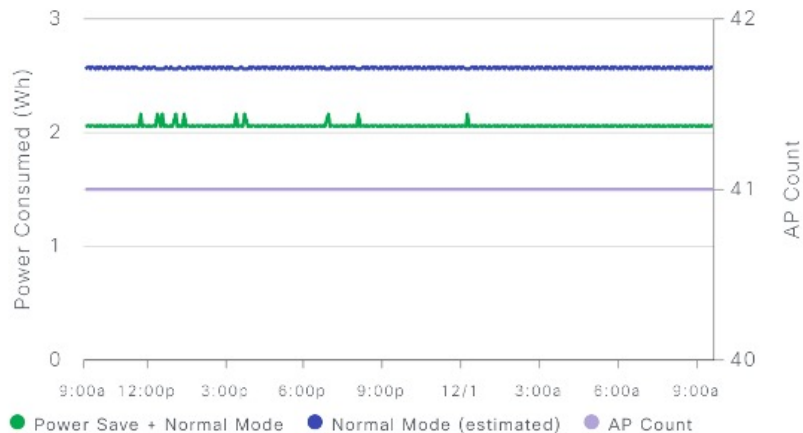
Search Table					
Identifier	Device Type	Switch Name	Switch Port	Power Consumed	Power Savings
assur-br1-ap3-1	Cisco Catalyst 9115AXI Unified Access Point	assur-br1-sw-3.cisco.com	GigabitEthernet1/0/11	6.35W	0.06W
assur-br1-ap3-2	Cisco Catalyst 9120AXI Unified Access Point	assur-br1-sw-3.cisco.com	TwoGigabitEthernet2/0/12	9.51W	0.00W
2 Records					
Show Records: 10 1 - 2					

AP Power Savings Insights

Visualize Your Power Savings!

AP Power Savings ⓘ

Power Consumed: 594.57Wh | 743.21Wh **20% Saved**



[View Details](#)

AP Power Savings

- Depicts power savings when AP Power Save Mode is enabled
- Savings are calculated by comparing resources consumed when AP Power Save mode is enabled to if it was disabled

PoE Analytics

Under the Hood



For your
reference

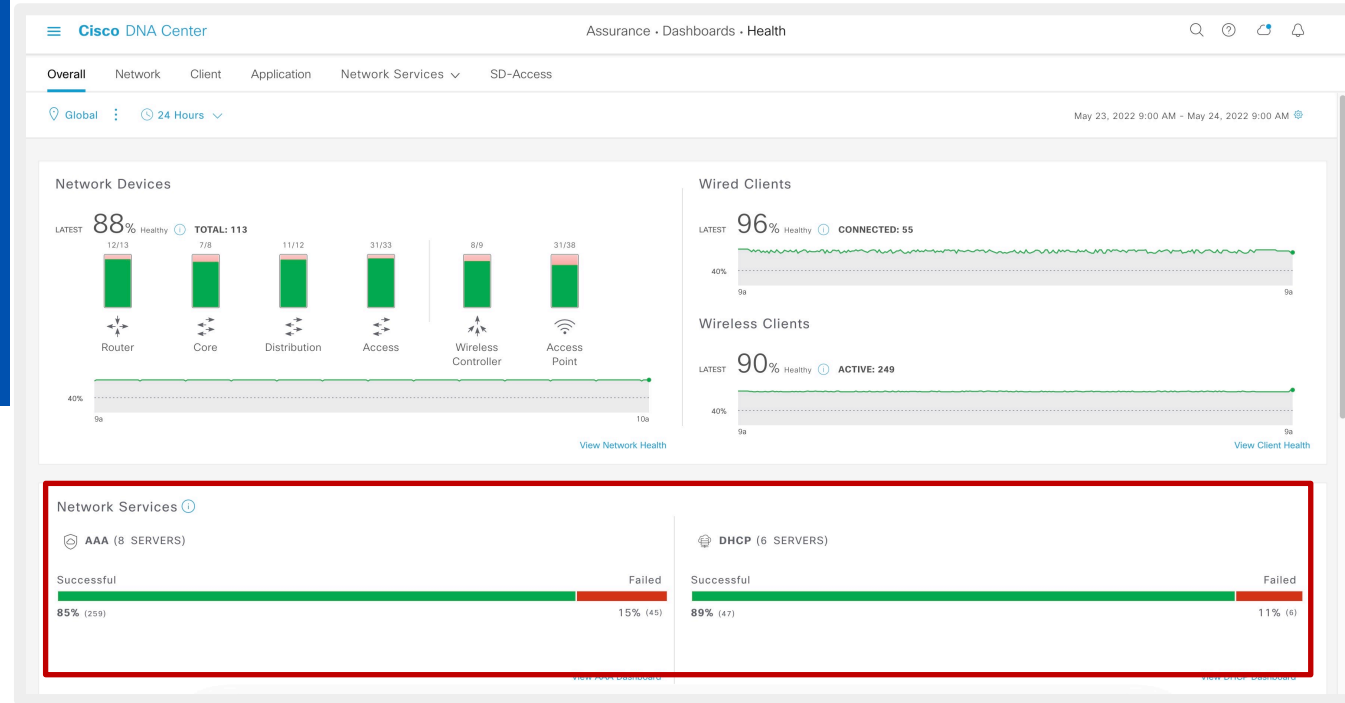
```
!  
telemetry ietf subscription 500  
  encoding encode-tdl  
  filter tdl-uri  
/services;serviceName=ios_oper/poe_port_detail  
  receiver-type protocol  
  source-address 10.85.54.24  
  stream native  
  update-policy periodic 60000  
  receiver name DNAC_ASSURANCE_RECEIVER  
telemetry ietf subscription 501  
  encoding encode-tdl  
  filter tdl-uri  
/services;serviceName=ios_oper/poe_module  
  receiver-type protocol  
  source-address 10.85.54.24  
  stream native  
  update-policy periodic 60000  
  receiver name DNAC_ASSURANCE_RECEIVER
```

```
telemetry ietf subscription 502  
  encoding encode-tdl  
  filter tdl-uri  
/services;serviceName=ios_oper/poe_stack  
  receiver-type protocol  
  source-address 10.85.54.24  
  stream native  
  update-policy periodic 60000  
  receiver name DNAC_ASSURANCE_RECEIVER  
telemetry ietf subscription 503  
  encoding encode-tdl  
  filter tdl-uri  
/services;serviceName=ios_oper/poe_switch  
  receiver-type protocol  
  source-address 10.85.54.24  
  stream native  
  update-policy periodic 60000  
  receiver name DNAC_ASSURANCE_RECEIVER
```

Subscriptions automatically configured as
part of “Device Controllability”

Network Services Analytics

- Help improve user Onboarding experience
- Identify sites with potential AAA/DHCP issues



Network Services Analytics - DHCP

DHCP SUMMARY

6 Servers
210ms Average Latency -11.11%

DHCP TRANSACTIONS

53 Total +54.55%
47 Successful +54.55%
6 Failed

Top Sites by Highest Latency ⓘ

San Francisco/SFO10/Fir-SFO10-1 (9ms)
San Jose/SJC01/Fir-SJC1-1 (8ms)
San Jose/SJC22/Fir-SJC22-1 (7ms)

[View Details](#)

Top Sites by Transaction Failures ⓘ

San Jose/SJC01/Fir-SJC1-1 (9)
San Francisco/SFO10/Fir-SFO10-1 (8)
San Jose/SJC22/Fir-SJC22-1 (6)

[View Details](#)

DHCP Server Latency ⓘ



[View Details](#)

DHCP Server Transactions ⓘ



- Dashlet details for highest latency and highest number of transaction failures

Network Services Analytics

Mapping of WLCs to corresponding AAA/DHCP servers

AAA Servers By WLC (8)

[Export](#)

Search Table

AAA Server IP	WLC Name	WLC Location	Transactions	Failures	Avg Latency (ms)	MAC Auth Latency (ms)	EAP Latency (ms)	MAC Auth Transactions	EAP Transactions	MAC Auth Failures	EAP Failures
106.235.200.202	WLC-9800	Global/North America/USA/California/San Jose/SJC01	238	28	150	--	150	0	238	0	28
109.7.150.69	SWLC-FABRIC-01	Global/North America/USA/California/San Jose/SJC01	13	4	5	--	5	0	13	0	4
14.10.181.87	SJC06-vWLC-9800	Global/North America/USA/California/San Jose/SJC06	9	2	6	--	6	0	9	0	2
140.102.148.249	Campus_WLC3	Global/North America/USA/California/San Jose/SJC05	6	2	4	--	4	0	6	0	2
158.128.154.123	Campus_WLC4	Global/North America/USA/Washington/Seattle/SE1	8	4	6	--	6	0	8	0	4

DHCP Servers By WLC (6)

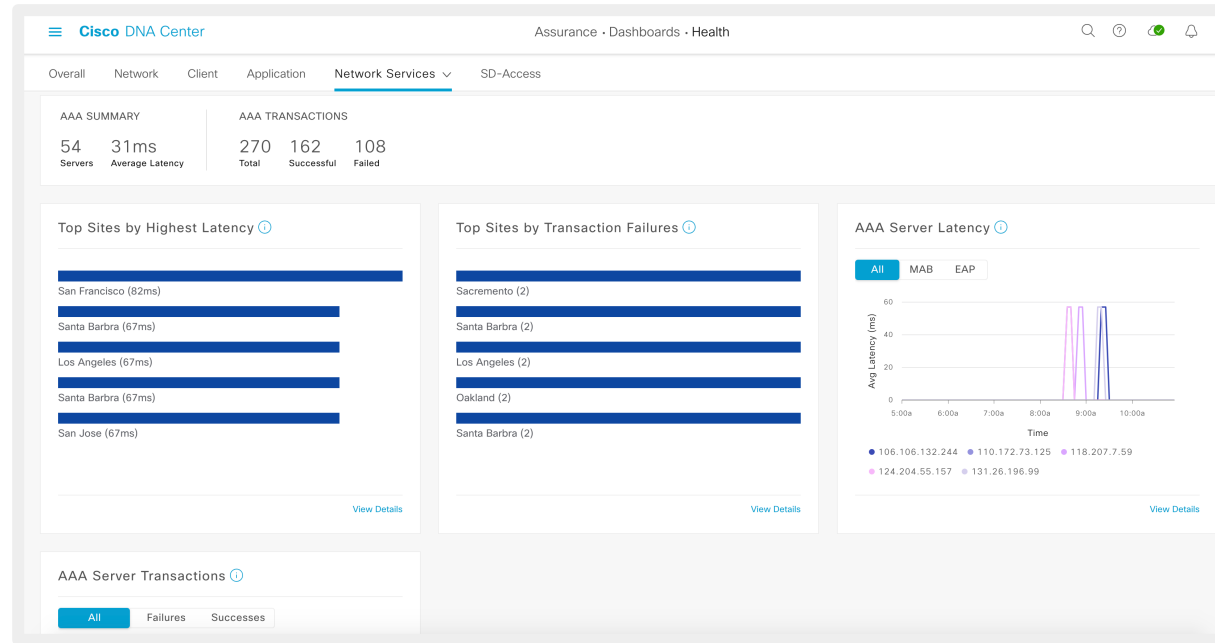
[Exp](#)

Search Table

DHCP Server IP	WLC Name	WLC Location	Transactions	Failures	Avg Latency (ms)	Discover-Offer Latency (ms)	Request-Ack Latency (ms)
192.168.152.1	WLC-9800	Global/North America/USA/California/San Jose/SJC01	14	0	45	45	1
100.30.189.51	SWLC-FABRIC-01	Global/North America/USA/California/San Jose/SJC01	7	1	36	36	9
104.194.73.167	SJC06-vWLC-9800	Global/North America/USA/California/San Jose/SJC06	15	2	28	28	4
140.102.148.249	Campus_WLC3	Global/North America/USA/California/San Jose/SJC05	10	1	43	43	6
116.140.161.52	Campus_WLC4	Global/North America/USA/Washington/Seattle/SE1	3	0	54	54	7
118.130.12.121	SJC06-WLC-ISSU	Global/North America/USA/California/San Jose/SJC06	4	2	4	4	3

Network Services Analytics

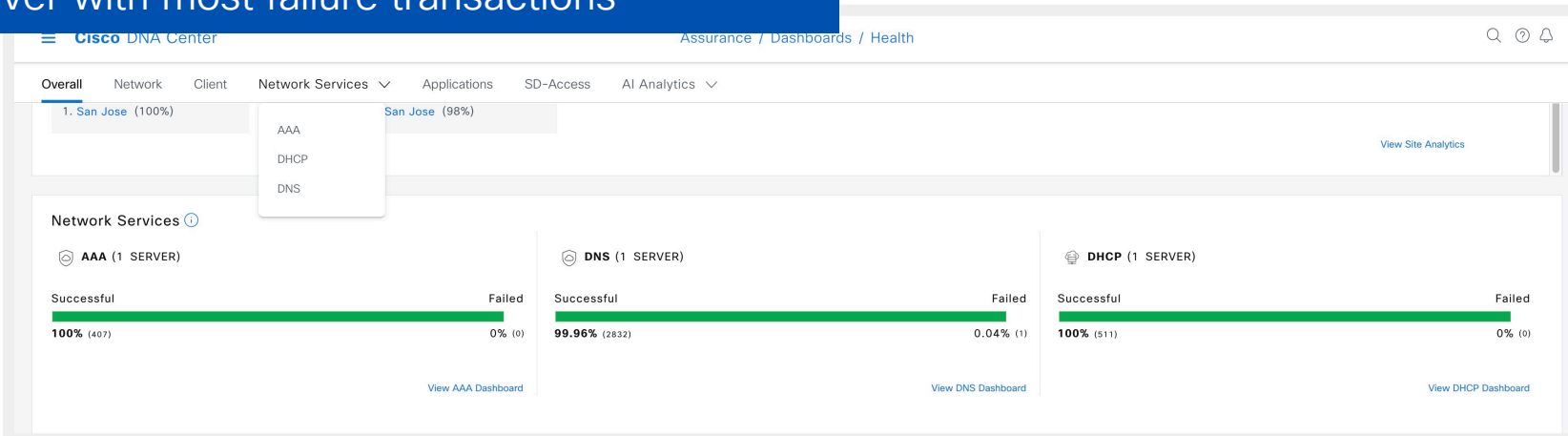
- Supported for wireless only
- IOS-XE 17.6.1+
- Not supported for AireOS controllers
- Local DHCP on 9800 not supported
- All transaction and server information is provided by the WLC directly
- WLC TDL subscriptions:
 - AAA -> 4321
 - DHCP -> 4322



Network Services Analytics – DNS

Catalyst Center 2.3.5+

- View success and failed transactions in timeline
- Insights into DNS performance
- View Top DNS failure reasons
- Find servers with highest DNS latency
- Find server with most failure transactions



Network Services – DNS Dashboard

- Find DNS servers by device
- Displays total transactions, failures and average latency per server

DNS Servers By Device (4) Export Settings

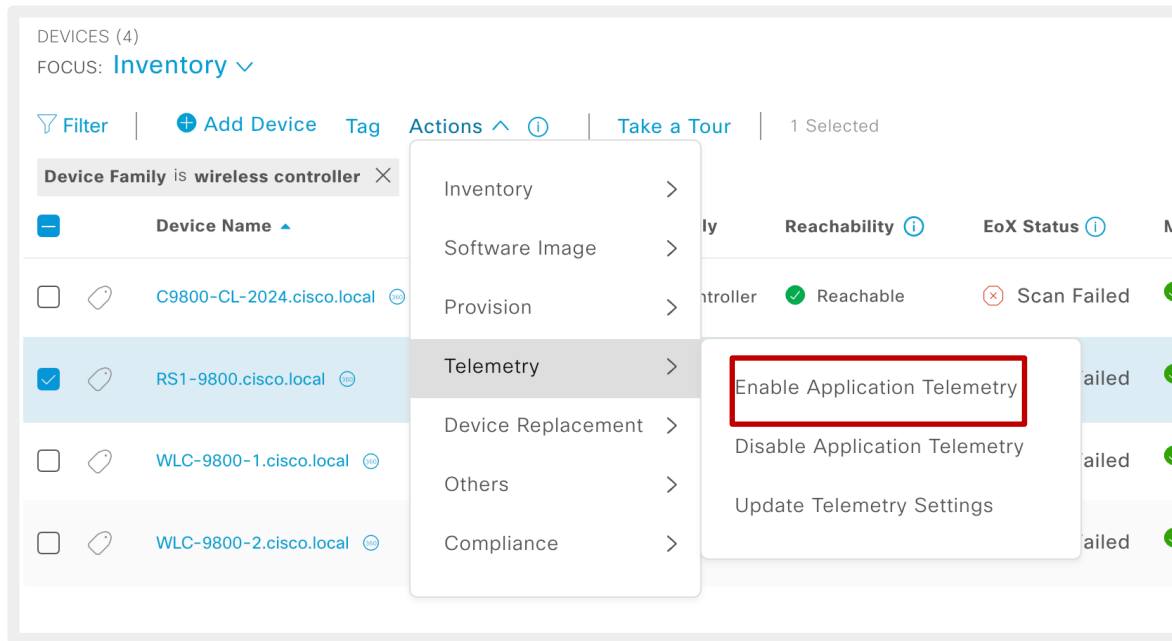
Search Table Filter

DNS Server IP	Device Name	Device Location	Device Family	Transactions	Failures	Avg Latency (ms)
10.85.48.6	C9K-STACK	Global/Canada/Ontario/Toronto/TBRANCH	Switches and Hubs	14310	14310	0
10.85.48.5	C9K-STACK	Global/Canada/Ontario/Toronto/TBRANCH	Switches and Hubs	14298	14298	0
64.102.6.247	TBRANCH-C9200L-2	Global/Canada/Ontario/Toronto/TBRANCH	Switches and Hubs	139	7	111
64.102.6.247	C9K-STACK	Global/Canada/Ontario/Toronto/TBRANCH	Switches and Hubs	1	0	244

Network Services Analytics - DNS

Catalyst Center 2.3.5+

- Supported in switches, routers and eWLCs.
- No support on AireOS WLC
- IOS-XE 17.10+
- Enabled via Application Telemetry



Network Services – DNS Dashboard



For your
reference

```
flow record dnacrecord_dns
 match ipv4 version
 match ipv4 protocol
 match connection client ipv4 address
 match connection server ipv4 address
 match flow observation point
 match application dns qtype
 match application dns rcode
 collect datalink mac source address input
 collect timestamp absolute first
 collect timestamp absolute last
 collect connection client counter packets long
 collect connection client counter bytes network long
 collect connection server counter packets long
 collect connection server counter bytes network long
 collect application dns requests
 collect application dns delay response sum
!
<snip>
!
flow monitor dnacmonitor_dns
 exporter dnacexporter
 cache timeout inactive 10
 cache timeout active 60
 record dnacrecord_dns
!
```

C9200L-24T-4G

C9300-24P

IOS-XE: 17.11.01

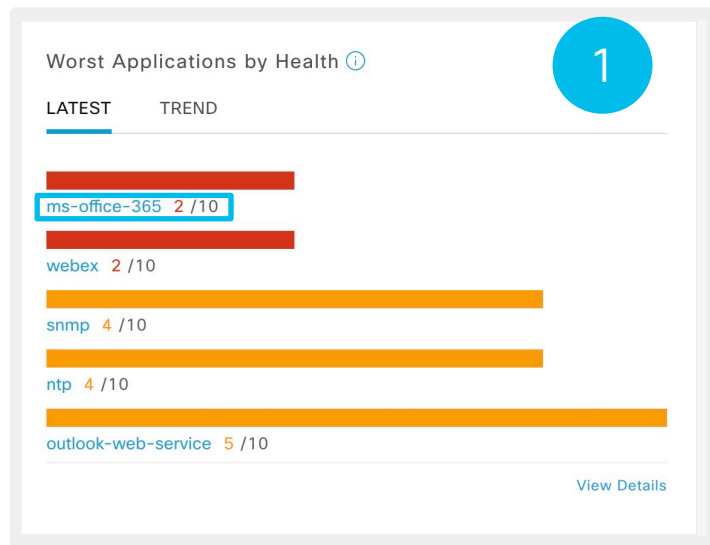
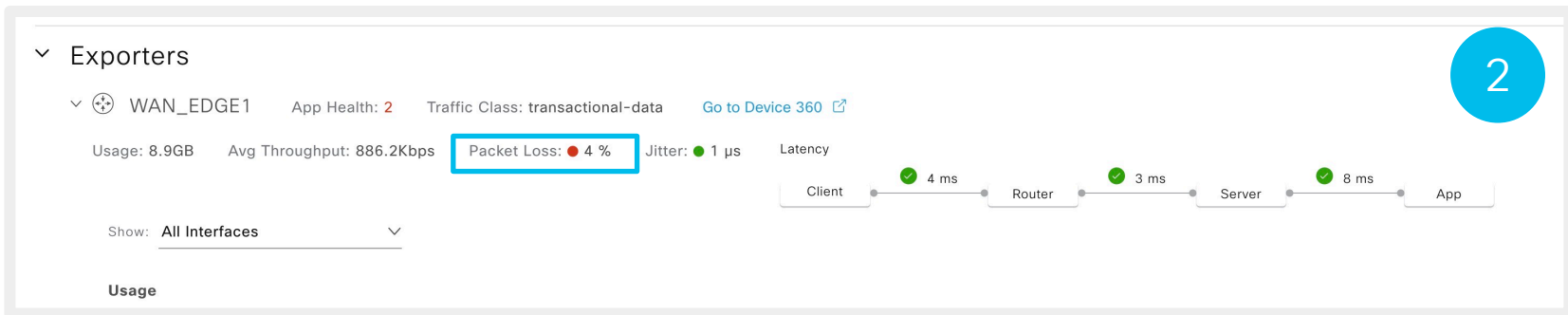
Cisco DNA Center

Version 2.3.5.3-70194

```
interface GigabitEthernet1/0/8
 description Description pushed by Catalyst Center
Template -- lan
 switchport access vlan 420
 switchport mode access
 device-tracking attach-policy IPDT_POLICY
 ip flow monitor dnacmonitor input
 ip flow monitor dnacmonitor_dns input
 ip flow monitor dnacmonitor output
 ip flow monitor dnacmonitor_dns output
 service-policy input DNA-MARKING_IN
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
 ip nbar protocol-discovery
```

Application Visibility

- Metrics on application usage and health
- Identify issues with applications



Application Visibility vs Application Experience

How Much = quantitative (usage)

- Supported on C9K switches
 - 17.3.1 supported with ETA
- AireOS WLC

How Good = qualitative (health)

- Supported on routers IOS-XE
- 9800 WLC- local
- 9800 WLC - flex (*), fabric(*)

Top Applications by Throughput

LATEST

TREND

MedicalRecords 412.9Mbps
microsoft-teams 134.5Mbps
ms-office-365 127.6Mbps
binary-over-http 92.6Mbps
ssh 40.7Mbps

Top Endpoints by Throughput

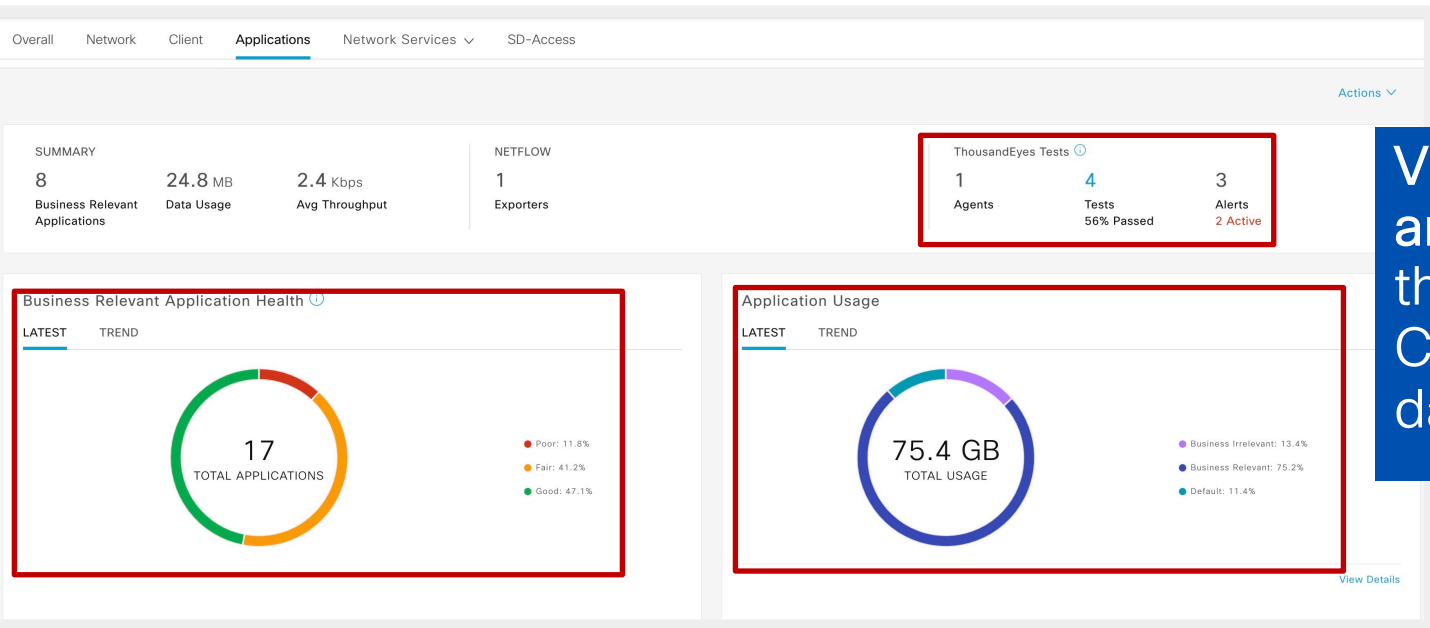
LATEST

Grace.Smith 11.2Kbps
DR.Dogood 10.1Kbps
john.zoldberg 1.6Kbps
Gordon.Thomson 1.3Kbps
shaggy.rogers 1.1Kbps

Name	Health	Business Relevance	Usage	Average Throughput	Packet Loss (%)	Network Latency	Jitter
MedicalRecords	8	Business Relevant	307.7MB	2.9Mbps	20	200 ms	2 μs
> microsoft-teams	8	Business Relevant	100.2MB	934.2Kbps	1	19 ms	24.9 ms
ms-office-365	2	Business Relevant	95.1MB	886.2Kbps	2	200 ms	1 μs
ssh	9	Business Relevant	30.3MB	282.7Kbps	4	1 ms	1 μs
outlook-web-service	5	Business Relevant	29.9MB	279Kbps	4	1 ms	1 μs
s	4	Business Relevant	5MB	46.8Kbps	1	1 ms	1 μs
control	--	Business Relevant	246.1B	2bps	1	1 ms	1 μs

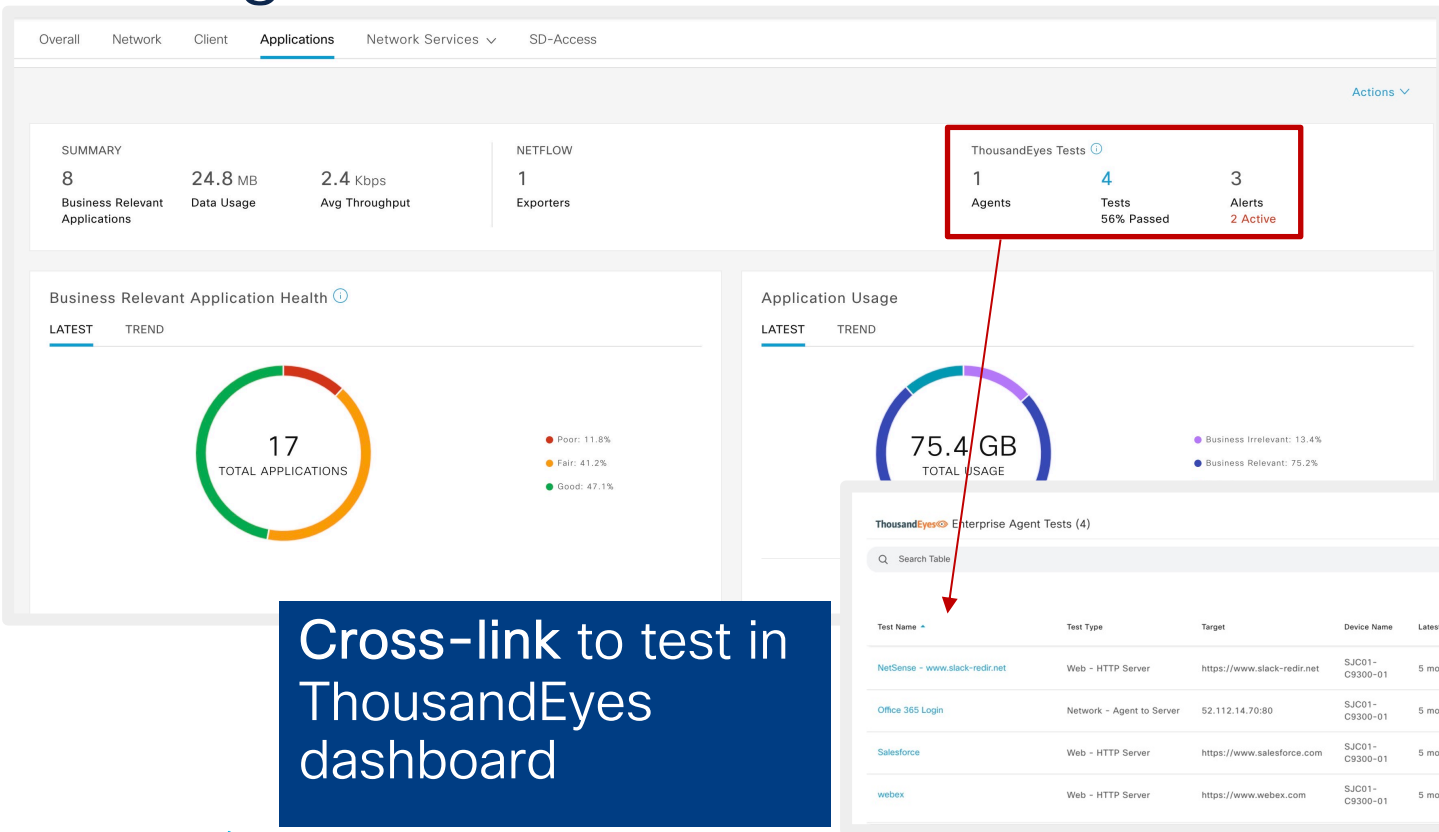
*Catalyst Center 2.3.5+ and IOS-XE 17.10.1+ with C91xx APs

Application Health Dashboard: ThousandEyes Integration



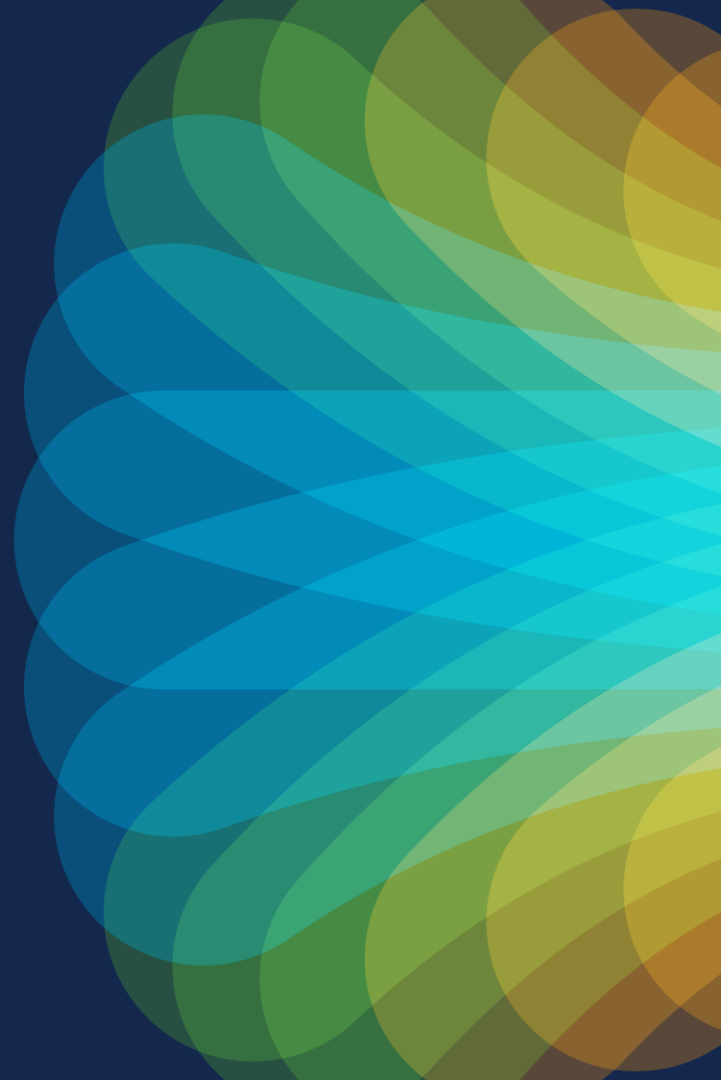
View agent, test, and alert data on the Catalyst Center Application dashboard

Application Health Dashboard: ThousandEyes Integration



Cross-link to test in
ThousandEyes
dashboard

Habit #3 - Leverage Compliance and Configuration management



Cisco Catalyst Center Compliance Landscape

The screenshot displays the Cisco Catalyst Center Compliance Landscape for a device named C9300-48-Stack-R8. The interface includes a sidebar with navigation options like 'All Devices', 'Config Drift', 'SECURITY', and 'Fabric'. The main content area shows a 'Compliance Summary' with a 'Run Compliance Check' button. Below this, there are several compliance cards: 'Network Settings' (Compliant), 'EoX - End of Life' (Compliant), 'Startup vs Running Configuration' (9 mins out of sync), 'Network Profiles' (Non-Compliant), 'Fabric BETA' (Compliant), 'Application Visibility' (Non-Compliant), 'Software Image' (Compliant), and 'Critical Security Advisories' (Compliant). Annotations with red arrows point to specific features: 'End of Sale & End of Life alerts' points to the EoX card; 'Identify whether the startup and running configurations of a device are in sync.' points to the Startup vs Running Configuration card; 'Violation of intent provisioned to a device through Catalyst Center' points to the Network Profiles card; 'Difference in network settings compared to "Network Settings" in Design' points to the Network Settings card; 'Check whether configuration matches Fabric design intent' points to the Fabric BETA card; 'Violation of application visibility intent provisioned to a device through CBAR and NBAR' points to the Application Visibility card; 'See if the tagged golden image is running on the device.' points to the Software Image card; and 'Check whether the devices are running without critical security vulnerabilities.' points to the Critical Security Advisories card.

End of Sale & End of Life alerts

Identify whether the startup and running configurations of a device are in sync.

Violation of intent provisioned to a device through Catalyst Center

Difference in network settings compared to "Network Settings" in Design

Check whether configuration matches Fabric design intent

Violation of application visibility intent provisioned to a device through CBAR and NBAR

See if the tagged golden image is running on the device.

Check whether the devices are running without critical security vulnerabilities.

Compliance: Software Image - Switches

Stack SW version mismatch

Detect SW version mismatch among switch stack

Compare image version between master and members

C9300-24P Run Commands View 360 Last updated: 12:52 PM Refresh

Reachable Managed IP Address: 8.18.19.13 Device Model: Cisco Catalyst 9300 Switch Role: ACCESS Uptime: 2 days 19 hrs 38 mins Site: -

DETAILS

Interfaces

Ethernet Ports

Native VLANs

Hardware & Software

Configuration

Power

Fans

SFP Modules

User Defined Fields

Compliance Summary

No events detected to trigger compliance check Run Compliance Check

Startup vs Running Configuration

Compliance last run on: Feb 16th, 2022, 08:20:53 PM

1 day since in sync

Lines added: 0

Lines removed: 0

Lines modified: 0

Software Image

Non-Compliant since Feb 16th, 2022, 03:17:16 PM

Compliance last run on: Feb 16th, 2022, 08:20:53 PM

17.06.03 Golden Image Version

Running Version: 17.6.1

Stack Member Status: Mismatch

Critical Security Advisories

Compliance last run on: Feb 16th, 2022, 08:20:53 PM

NA

Device was either added after the last scan or was not reachable during the...

Compliance Summary / Software Image

GOLDEN IMAGE		DEVICE IMAGE	
Image Name	cat9k_iosxe.17.07.01.SPA.bin	Image Name	cat9k_iosxe.17.07.01.SPA.bin
Version	17.07.01.0.82	Version	17.07.01.0.82
Role	MEMBER	Role	MASTER
Version	Version Mismatch	Version	17.07.01
Stack Member Number	3	Stack Member Number	2
Role	STANDBY	Role	STANDBY
Version	17.07.01	Version	17.07.01
Stack Member Number	1	Stack Member Number	1

Compliance: Network Profiles - Switches

The screenshot shows the Cisco DNA Center interface for a switch named **C9K-BRANCH-STACK**. The breadcrumb navigation at the top indicates the path: **All Devices / C9K-BRANCH-STACK**. Below this, the switch's status is shown as **Reachable** and **Managed**, along with its IP address, device model (Cisco Catalyst 9300 Switch), role (ACCESS), uptime (122 days 23 hrs 9 mins), and site (Global/Canada/Ontario/Toronto/TBRANCH).

The left sidebar contains a **DETAILS** section with the following options: **Interfaces** (with a dropdown arrow), **Ethernet Ports**, **Native VLANs**, **Hardware & Software**, **Configuration**, **Power**, **Fans**, **SFP Modules**, **User Defined Fields**, **Config Drift**, **Stack**, **SECURITY**, and **Advisories**.

The main content area is titled **Compliance Summary** and states: **No events detected to trigger compliance check**. A **Run Compliance Check** link is available. The summary consists of four cards:

- Startup vs Running Configuration**: Shows a red status icon, a last run time of Sep 2nd, 2022, 03:01:30 PM, and a **4 mins** out of sync. It also lists **Lines added: 0**, **Lines removed: 1**, and **Lines modified: 0**.
- Network Profiles**: Shows a red status icon, a last run time of Sep 2nd, 2022, 03:01:45 PM, and is **Non-Compliant**. It shows **1** change for the **CLI Template: 1**.
- Software Image**: Shows a green status icon, a last run time of Sep 2nd, 2022, 03:01:30 PM, and is **Compliant**. It shows the **Golden Image Version: 17.08.01** and the **Running Version: 17.8.1**.
- Critical Security Advisories**: Shows a green status icon, a last run time of Sep 2nd, 2022, 03:01:30 PM, and is **Compliant**. It shows **0** advisories.

Compliance: Network Profiles - Switches

Config pushed by Catalyst Center via templates:

```
interface GigabitEthernet1/0/7
  description Description pushed by Catalyst Center Template --
lan
!
interface GigabitEthernet1/0/8
  description Description pushed by Catalyst Center Template --
lan
```

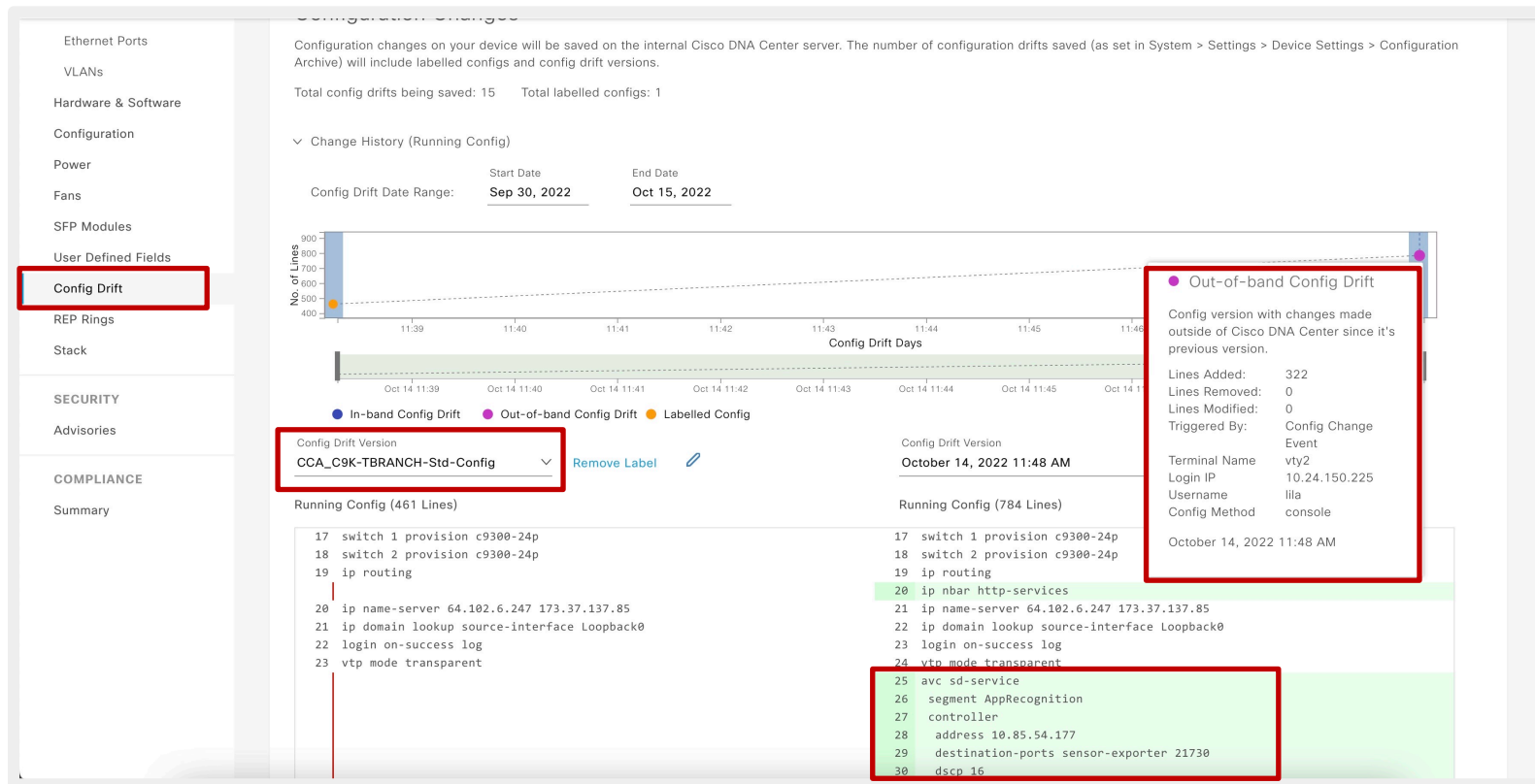
Out of band changes:

```
C9K-BRANCH-STACK#conf t
Enter configuration comm
C9K-BRANCH-STACK(config)
C9K-BRANCH-STACK(config-
```

The screenshot shows the Cisco Catalyst Center interface for the C9K-BRANCH-STACK network profile. The left sidebar lists various configuration categories, and the main area displays the 'CLI Template (1)' section. A table titled 'CLI Deviations' shows the current state of the network profile as of May 26, 2022, at 2:25 PM. The table has columns for line numbers, CLI commands, and descriptions. A callout box points to the highlighted text in red, indicating that these are missing CLIs.

Line	CLI	Description
2	late -- lan	description Description pushed by DNAC Temp
3		
4		interface GigabitEthernet1/0/8
5	late -- lan	description Description pushed by DNAC Temp
6		
7		
8		alias exec showntp show nto status

Config Drift



Compliance: Network Profiles – Wireless

The screenshot displays the Cisco DNA Center interface for a specific device, **STL01-C9800-CL.dlab.local**. The interface is divided into a left sidebar with navigation options and a main content area showing compliance details.

Navigation Sidebar:

- DETAILS
 - Interfaces
 - Ethernet Ports
 - Virtual Ports
 - Hardware & Software
 - User Defined Fields
 - Config Drift
 - Wireless Info
 - Mobility
- SECURITY
 - Advisories
- COMPLIANCE
 - Summary

Device Information:

- Device: STL01-C9800-CL.dlab.local
- Status: Reachable, Managed
- IP Address: 172.16.255.35
- Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud
- Role: ACCESS
- Uptime: 22 hrs 56 mins
- Site: Global/Canada/Quebec/Saint-Lambert/STL01

Compliance Summary:

No events detected to trigger compliance check. [Run Compliance Check](#)

Compliance Items:

- Startup vs Running Configuration:** Compliance last run on: Apr 2nd, 2022, 11:16:36 AM. 1 hr since out of sync. Lines added: 2, Lines removed: 2, Lines modified: 0.
- Network Profiles:** Non-Compliant since Feb 9th, 2022, 02:38:20 AM. Compliance last run on: Apr 2nd, 2022, 11:16:36 AM. 3 Changes. Model Config: 1, Wireless: 1. [+1 more](#).
- Application Visibility:** Compliant since Apr 2nd, 2022, 11:16:54 AM. Compliance last run on: Apr 2nd, 2022, 11:16:54 AM. 0 Changes.
- Software Image:** Compliant since Feb 3rd, 2022, 05:10:45 PM. Compliance last run on: Apr 2nd, 2022, 11:16:36 AM. 17.07.01 Golden Image Version. Running Version: 17.7.1.
- Critical Security Advisories:** Compliant since Feb 8th, 2022, 07:00:11 PM. Compliance last run on: Apr 2nd, 2022, 11:16:36 AM. 0.

Compliance: Network Profiles – Wireless

Cisco DNA Center

STL01-C9800-CL.dlab.local

Run Commands View 360

Last updated: 11:16 AM Refresh

Reachable Managed IP Address: 172.16.255.35 Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud Role: ACCESS Uptime: 22 hrs 56 mins Site: Global/Canada/Quebec/Saint-Lambert/STL01

DETAILS

- Interfaces
 - Ethernet Ports
 - Virtual Ports
 - Hardware & Software
 - User Defined Fields
 - Config Drift
 - Wireless Info
 - Mobility

SECURITY

- Advisories

COMPLIANCE

- Summary

Compliance Summary / Network Profiles

CLI Template (1) Model Config (1) Wireless (1)

CLI Deviations As of: Apr 2, 2022 11:18 AM

Search Table

Template

- Enabling SI

1 Records Show Records: 10 1 - 1

Realize Template: Enabling SI

1	1	ap dot11 24ghz SI
2		ap dot11 5ghz SI

Compliance: Network Profiles – Wireless

The screenshot displays the Cisco DNA Center interface. At the top, the breadcrumb navigation shows 'All Devices / STL01-C9800-CL.dlab.local'. Below this, the device name 'STL01-C9800-CL.dlab.local' is shown with links for 'Run Commands' and 'View 360'. The status bar indicates the device is 'Reachable' and 'Managed', with an IP address of 172.16.255.35, a device model of 'Cisco Catalyst 9800-CL Wireless Controller for Cloud', a role of 'ACCESS', an uptime of '22 hrs 56 mins', and a site of 'Global/Canada/Quebec/Saint-Lambert/STL01'.

The left sidebar contains a 'DETAILS' section with a dropdown menu. The 'Interfaces' option is selected, showing a list of categories: Ethernet Ports, Virtual Ports, Hardware & Software, User Defined Fields, Config Drift, Wireless Info, and Mobility. Below this, the 'SECURITY' section includes 'Advisories', and the 'COMPLIANCE' section includes 'Summary'.

The main content area is titled 'Compliance Summary / Network Profiles'. It features three tabs: 'CLI Template (1)', 'Model Config (1)', and 'Wireless (1)'. The 'Wireless (1)' tab is highlighted with a red box. Below the tabs is a search bar labeled 'Search Table'. A table displays the network profile details:

Model Name	Attribute	Status	Intended Value	Actual Value
Wlan/BestCorpWi_Global_NF_e5f0c407	FT Adaptive	Changed	Adaptive	Disabled

At the bottom of the table, it says 'Showing 1 of 1'.

Compliance: Network Profiles – Wireless

Cisco DNA Center

All Devices / STL01-C9800-CL.dlab.local

STL01-C9800-CL.dlab.local [Run Commands](#) [View 360](#) Last updated: 11:16 AM [Refresh](#)

Reachable Managed IP Address: 172.16.255.35 Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud Role: ACCESS Uptime: 22 hrs 56 mins Site: Global/Canada/Quebec/Saint-Lambert/STL01

DETAILS

- Interfaces
 - Ethernet Ports
 - Virtual Ports
- Hardware & Software
- User Defined Fields
- Config Drift
- Wireless Info
- Mobility

SECURITY

- Advisories

COMPLIANCE

- Summary

Compliance Summary / Network Profiles

CLI Template (1) **Model Config (1)** Wireless (1)

Search Table

Model Name	Attribute	Status	Intended Value	Actual Value
Policy_Profile/BestCorpWi_Global_NF_e5f0c407	IPv4 DHCP Required	Changed	YES	NO

Showing 1 of 1

Catalyst Center 2.3.5+

Fix Config Compliance Issues

Mail - Lila Rousseau (trousse... X) Cisco DNA Center X Cisco DNA Center X +

Not Secure | https://10.85.54.180/dna/provision/devices/inventory/device-details?deviceId=82a8469c-a262-4c9c-af33-a7f3e524d97e

Cisco DNA Center

All Devices / C9K-STACK

C9K-STACK Run Commands View 360

PORT_SECURITY

Reachable Managed IP Address: 10.85.54.54 Device Model: Cisco Catalyst 9300 Switch Device Role: ACCESS Uptime: 61 days 2 hrs 17 mins Site: Global/Canada

DETAILS

Interfaces >

Hardware & Software

Configuration

Power

Fans

SFP Modules

User Defined Fields

Config Drift

REP Rings

Stack

SECURITY

Advisories

COMPLIANCE

Summary

You can now fix all configuration compliance issues on this device. You will be able to review before the fix is applied. [Fix All Configuration Compliance Issues](#)

Compliance Summary View Pref

Next Compliance check is scheduled on Jan 17, 2023 02:50 PM [Run Compliance Check](#)

EoX - End of Life Compliance last run on: Jan 17th, 2023, 02:55:23 PM
Module : **Compliant**
Software : **Compliant**
Hardware : **Compliant**

Network Settings Non-Compliant since Jan 17th, 2023, 02:55:23 PM
Compliance last run on: Jan 17th, 2023, 02:55:23 PM
2 General: 2
Open Violations

Startup vs Running Configuration Compliance last run on: Jan 17th, 2023, 02:55:23 PM
71 days since in sync
Lines added: 0
Lines removed: 0
Lines modified: 0

Network Profiles Non-Compliant since Oct 14th, 2022, 01:23:01 PM
Compliance last run on: Jan 17th, 2023, 02:55:24 PM
1 CLI Template: 1
Open Violations

Application Visibility Compliant since Jan 17th, 2023, 02:56:06 PM
Compliance last run on: Jan 17th, 2023, 02:56:06 PM
0 Open Violations

Software Image Compliant since Nov 17th, 2022, 12:35:00 PM
Compliance last run on: Jan 17th, 2023, 02:55:23 PM
17.09.02 Golden Image Version
Running Version: 17.9.2
Stack Member Status: Up to Date

Fix Configuration Compliance Issues

3 compliance issues are listed to be fixed. Review and schedule the fix.

Note: Routing, HA Remediation, Software Image, Securities Advisories and Workflow related compliance issues will not be addressed in this fix. You can address these separately by following the actions in their respective sections.

Summary of Issues to be Fixed

Following are the different violations selected to be fixed. Click on the issues identified to view details in the respective compliance sections.

Compliance Type	Issues Identified
Network Profiles	1
Network Settings	2

Schedule the Fix

When would you like to apply the fix?

☒ Now

☐ Later

☐ Generate Preview

Creates preview which can be later used to deploy on selected devices. View status in [Work Items](#)

Task Name*

C9K-STACK - Compliance Fix

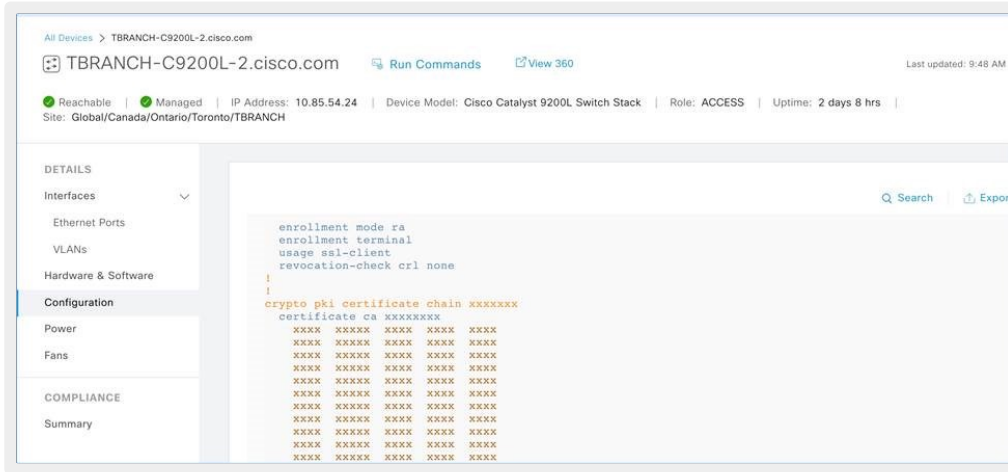
Cancel

Apply

Compliance Tips

- Event-based archive takes at least 5 minutes to update after traps are received. For accurate results, we recommend that you **wait for at least 5 minutes before running compliance manually** after a configuration change.
- **Network Profile** and **Network Settings**
 - Device must be provisioned by Cisco Catalyst Center

Device Configuration Management



- Catalyst Center stores device configurations in the Catalyst Center DB
- Device configurations are available via the UI
- For security reasons, sensitive data is masked
- CLI output can be exported from this same window, but it will be done using the masked config as well. What this means is that we don't expose sensitive data via the UI or UI export.
- But it also means that we can't directly use this device config to restore a device.

APIs to retrieve device configuration

-
- A screenshot of a macOS desktop environment. In the background, there's a blurred view of a room with a desk and chair. The foreground shows a macOS interface. At the top, there's a menu bar with various icons like volume, network, and battery. Below it, a dock contains several application icons including Finder, Safari, and Mail. A File Explorer window is open, displaying a folder named "Downloads". Inside this folder, there are two files: "03_Oct_2020_20_33_12__RUNNINGCONFIG(1).cfg" and "03_Oct_2020_20_33_12_684_RUNNINGCONFIG(1).cfg". The second file is selected and its contents are displayed in a preview pane on the right. The preview pane shows a Cisco IOS configuration script. The script includes commands for setting timestamps, service passwords, hostname, boot system, VRF definition, logging console, enable password, username, switch provision, IP routing, device tracking, queue settings, access-session, crypto pki trustpoint, and enrollment selfsigned. The script ends with a comment "# End of Configuration" and a timestamp "2020-10-03 13:51:05 UTC Sat Oct 3 2020 by cisco".
- Back/forward Downloads New Folder View Action Group Share Add Tags Delete Path
- Name Date Modified Date Created Size
- 03_Oct_2020_20_33_12__RUNNINGCONFIG(1).cfg Today at 9:53 AM Today at 9:53 AM
- 03_Oct_2020_20_33_12_684_RUNNINGCONFIG(1).cfg
- ```
! Last configuration change at 13:51:05 UTC Sat Oct 3 2020 by cisco
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec show-timezone year
service password-encryption
service internal
service compress-config
!
hostname CAMPUS-access1
!
boot-start-marker
boot system switch all flash:cat3k_caa-universalk9.SPA.03.06.04.E.152-2.E4.bin
boot-end-marker
!
vrf definition Mgmt-vrf
 address-family ipv4
 exit-address-family
 address-family ipv6
 exit-address-family
!
no logging console
enable password 7 1S11021R0725
!
username cisco privilege 15 password 7 094F471A1A0A
no aaa new-model
switch 1 provision ws-c3850-48u
!
!
!
ip routing
ip host test 100.100.100.100
!
ip device tracking probe auto-source override
ip device tracking probe delay 60
qos queue-software-multiplier 100
access-session mac-move deny
crypto pki trustpoint TP-self-signed-4149926277
enrollment selfsigned
End of Configuration
2020-10-03 13:51:05 UTC Sat Oct 3 2020 by cisco
```

# Device Configuration Management

## Configuration Archive

☰ Cisco DNA Center

System / Settings

🔍 ⓘ ⌂

🔍 Search Settings

Cisco Accounts

▼

PnP Connect

Cisco.com Credentials

Smart Account

Smart Licensing

SSM Connection Mode

Device Settings

▼

Device Controllability

Network Resync Interval

SNMP

ICMP Ping

Image Distribution Servers

Device EULA Acceptance

PnP Device Authorization

Device Prompts

Configuration Archive

Settings / Device Settings

Configuration Archive

Cisco DNA Center internal server will periodically back up your device's running configuration. You can select the day and time for the backup and select the total number of config drifts being backed up (note: total config drifts being saved included all the labelled configs for the device). To archive all the device's running configurations, you can configure an external server.

Internal

External

External Repository

As of: Feb 10, 2022 2:03 PM

🔄

🔍 Search Table

⌵

| Host         | Protocol | User Name | Backup Format | Backup Cycle                                | Connectivity | Action |
|--------------|----------|-----------|---------------|---------------------------------------------|--------------|--------|
| 10.85.54.179 | SFTP     | netadmin  | RAW           | <div>📅 Daily</div> <div>Time 01:04 PM</div> | 🟢 Connected  | 🗑️ ✎️  |

SFTP server can be configured to export raw configs to an external repository

# Device Configuration Management

## Configuration Archive

**Archive Utility**

Please enter the password for  
"Export\_Configs-10\_Feb\_2022\_18\_04\_00\_353-oWF.zip".

Password:

Cancel OK

**Downloads**

Back/Forward New Folder View Action Group Share Search

Name Date Modified

Export\_Configs-10\_Feb\_2022\_18\_04\_00\_353-oWF.zip

**Export\_Configs-10...**

Back/Forward New Folder View Action Group Share Search

Name Date Modified Date Created

|                                               |                  |                  |
|-----------------------------------------------|------------------|------------------|
| > 10.85.51.69-TRS-E2.cisco.com                | Today at 2:07 PM | Today at 2:07 PM |
| > 10.85.54.17-TRN6-TBRANCH-DIST.cisco.com     | Today at 2:07 PM | Today at 2:07 PM |
| > 10.85.54.20-TRN6-TBRANCH-WLC                | Today at 2:07 PM | Today at 2:07 PM |
| > 10.85.54.23-TBRANCH-C9200-1.lila.com        | Today at 2:07 PM | Today at 2:07 PM |
| > 10.85.54.24-TBRANCH-C9200L-2.cisco.com      | Today at 2:07 PM | Today at 2:07 PM |
| > 10.85.54.25-TBRANCH-C9200L-3.cisco.com      | Today at 2:07 PM | Today at 2:07 PM |
| > 10.85.54.51-TRN6-TBRANCH-FUSION             | Today at 2:07 PM | Today at 2:07 PM |
| > 10.85.54.53-TRN6-TBRANCH-C3650-S1.cisco.com | Today at 2:07 PM | Today at 2:07 PM |
| > 10.85.54.54-C9K-BRANCH-STACK                | Today at 2:07 PM | Today at 2:07 PM |
| > 10.85.54.99-wlc01                           | Today at 2:07 PM | Today at 2:07 PM |
| > 10.85.54.102-wlc02                          | Today at 2:07 PM | Today at 2:07 PM |
| > .TCP                                        | Today at 2:07 PM | Today at 2:07 PM |
| > .Fabric_WLC                                 | Today at 2:07 PM | Today at 2:07 PM |
| > IPUS-FUSION.cirrus.cloud                    | Today at 2:07 PM | Today at 2:07 PM |
| > IPUS-B1.cirrus.cloud                        | Today at 2:07 PM | Today at 2:07 PM |

**10.85.54.54-C9K-...**

Back/Forward New Folder View Action Group Share Search

Name Date Modified Date Created

|                                            |                  |                  |
|--------------------------------------------|------------------|------------------|
| 10_Feb_2022_18_04_00_353_RUNNINGCONFIG.cfg | Today at 6:04 PM | Today at 2:07 PM |
| 10_Feb_2022_18_04_00_353_STARTUPCONFIG.cfg | Today at 6:04 PM | Today at 2:07 PM |
| 10_Feb_2022_18_04_00_353_vlan.dat.bat      | Today at 6:04 PM | Today at 2:07 PM |

# Device Configuration Management

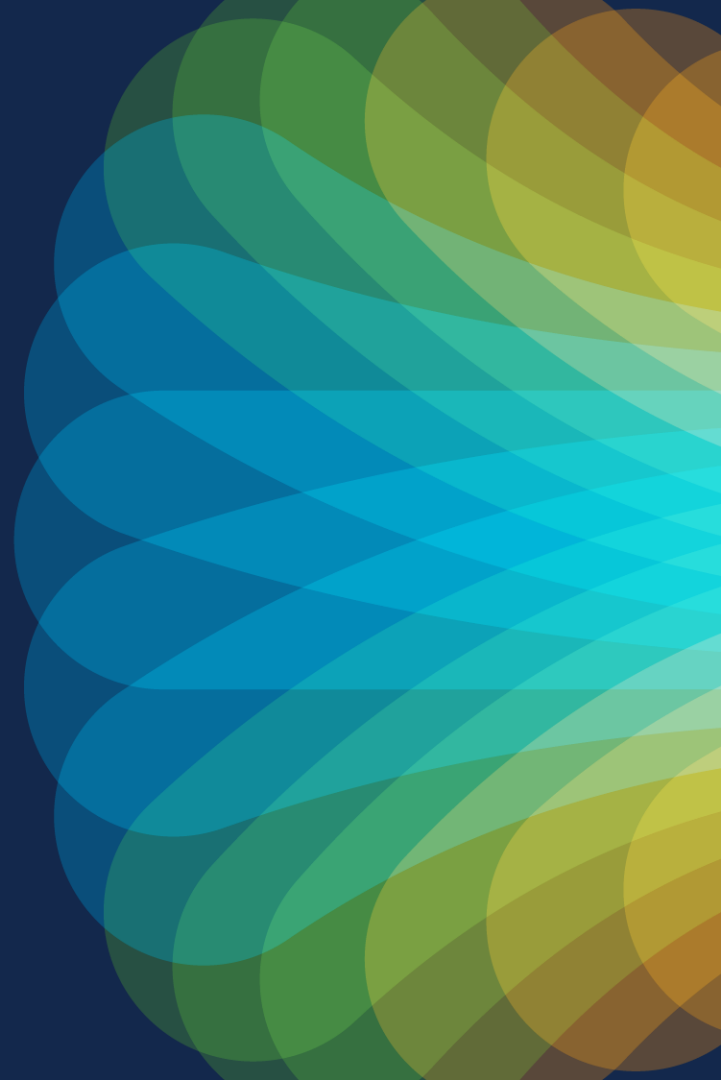
## Configuration Archive

10\_Feb\_2022\_18\_04\_00\_353\_RUNNINGCONFIG.cfg

10\_Feb\_2022\_18\_04\_00\_353\_RUNNINGCONFIG.cfg

```
! Last configuration change at 21:55:47 UTC Mon Feb 7 2022 by netadmin
! NVRAM config last updated at 21:55:49 UTC Mon Feb 7 2022 by netadmin
version 17.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
! Call-home is enabled by Smart-Licensing.
service call-home
platform punt-keepalive disable-kernel-core
hostname C9K-BRANCH-STACK
!
!
vrf definition Mgmt-vrf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
enable secret 9 9slJ/gvcAL9GF0$uk6/kumGDPS/A8btHwK8xzqGeVEVVM3idf83ZIm4zH92
no aaa new-model
boot system switch all flash:packages.conf
switch 1 provision c9300-24p
switch 2 provision c9300-24p
!
!
ip routing
!
!
ip nbar attribute-map BR2
attribute business-relevance default
ip nbar attribute-map TC3
attribute traffic-class multimedia-streaming
! ip nbar attribute-map TCF 001
```

Habit #4 - Keep your  
infrastructure **code**  
**up to date** with  
software image  
management





# SWIM Demo

# Software Upgrade Recommendations

- To reduce the network downtime, it's recommended to perform **distribution and activation job separately**
- **Maintenance window** is required for activation
- Wireless
  - Start with **ISSU, AP Pre-Image Download, Staggered Upgrade**
  - Use **Rolling AP upgrades** where ISSU not available
- Consider **external file servers** for remote sites
- **Install Mode** is recommended mode
  - “Bundle”/”Install” mode **conversion is not supported**

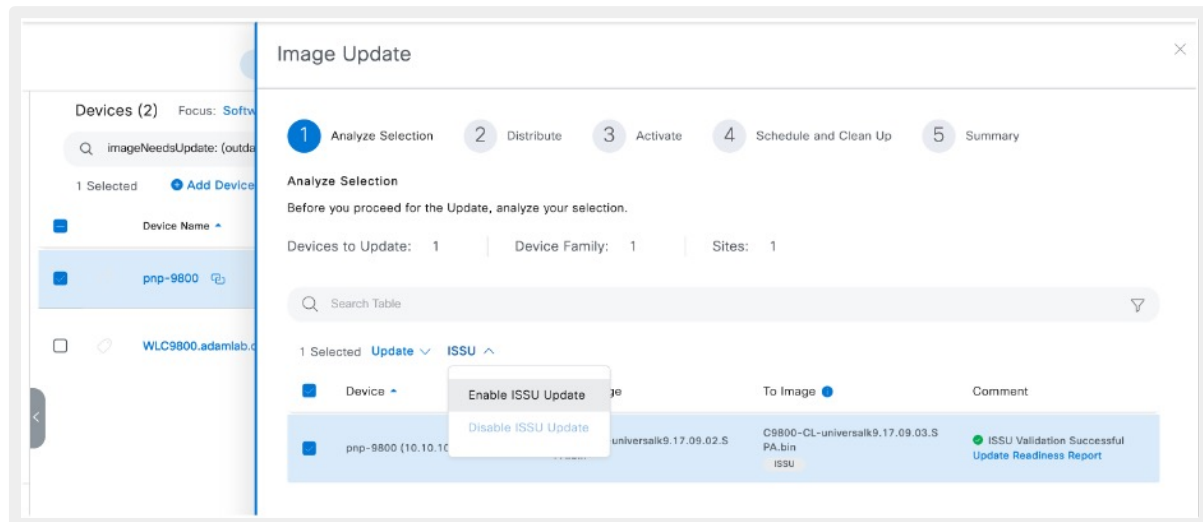
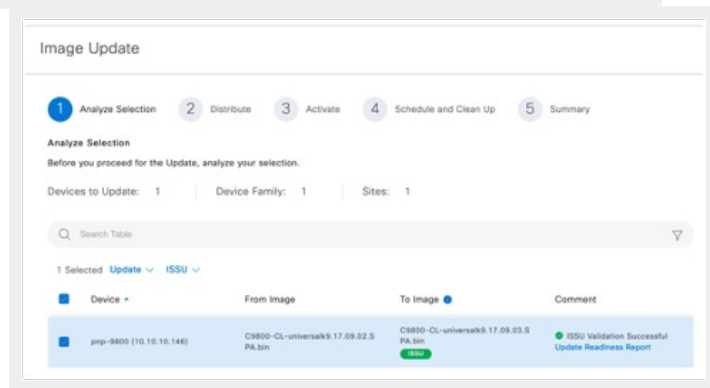
# Control over SWIM- ISSU

ISSU supports both Wired & Wireless devices

ISSU support for C9800 controller starting 17.3

Helps reduce downtime for wireless Infrastructure

ISSU requires controllers in HA SSO



# Ready to go ISSU

Provision / Inventory

Image Update

Analyze Selection

Distribute

Activate

Schedule and Clean Up

5 Summary

Summary

Review your entry and make changes if you wish to do

Devices to Update: 1

Device Family: 1

Sites: 1

| Device                  | From Image                                | To Image                                          | Update Support             |
|-------------------------|-------------------------------------------|---------------------------------------------------|----------------------------|
| pnp-9800 (10.10.10.146) | C9800-CL-universalk9.17.09.02.SP<br>A.bin | C9800-CL-universalk9.17.09.03.SP<br>A.bin<br>ISSU | ISSU Validation Successful |

# Control SWIM- AP Pre-Image Download/Rolling AP Upgrade

ISSU together with AP Pre-Image Download and Rolling AP Upgrade helps reduce network downtime

Controllers needs to be provisioned for Rolling AP Upgrade

AP Pre-image download by default available starting Catalyst Center 2.3.3.x

**Cisco DNA Center** Provision / Inventory / Image Update Status

**9800\_SWIM (172.100.1.54) Image Update**  
Date: Sep 27, 2022 4:20 PM Duration: 27 minutes 7 seconds Status: ● Successfully Activated C9800-CL-universalk9.16.12.05.SPA.bin

**SUMMARY**  
> Task Names (4)  
> Image Versions (7)

**Devices Updates**  
0 Selected Retry Upcoming T

| Device Name                               | Device Type |
|-------------------------------------------|-------------|
| 100.100.100.100                           | Uni         |
| New-Cat9300-Stack-Switch (192.168.120.20) | Dev Fan     |
| 9800_SWIM (172.100.1.54)                  | Wir Cor     |
| New-Cat9300-Stack-Switch (192.168.120.20) | Swi and     |
| 9800_SWIM (172.100.1.54)                  | Wir Cor     |

15 Records

**Operations** **Checks**

- > ● Image Checksum Verification On Device  
40 seconds
- > ● Unpack Images  
2 minutes 30 seconds
- > ● **AP Pre-Image Download**  
8 minutes 6 seconds

Task Name AP Pre-Image Download

Task Status Success ( AP Image Predownload Status : Total number of APs = 1, initiated = 0, downloading = 0, predownloading = 0, completed predownloading = 1, not supported = 0, failed to predownload = 0.)

> ● Activation 13 minutes 15 seconds

# Activation for Normal Wireless vs ISSU Wireless

Provision / Inventory / Image Update Status

pnp-9800 (10.10.10.146) Image Update

Date: May 30, 2023 12:09 PM Duration: 26 minutes 37 seconds Status: ● Successfully Activated C9800-CL-universalk9.17.09.02.SPA.bin

Operations Checks

- > ● Distribution 17 minutes 15 seconds
- ▼ ● Activation 9 minutes 22 seconds
  - NETCONF Activation of image: C9800-CL-universalk9.17.09.02.SPA.bin on device: 10.10.10.146 completed successfully.
  - > ● Pre Activation Operation 2 seconds
  - > ● Image Activation 8 minutes 44 seconds
  - > ● Install Commit 17 seconds
  - > ● Remove Inactive Images 6 seconds
  - > ● Collect Running Image Details 5 seconds
  - > ● Verify Image Activation 1 second
  - > ● Post Activation Operation 5 seconds

Normal Activation

Provision / Inventory / Image Update Status

pnp-9800 (10.10.10.146) Image Update

Date: May 30, 2023 2:09 PM Duration: 56 minutes 54 seconds Status: ● Successfully Activated C9800-CL-universalk9.17.09.03.SPA.bin

Operations Checks

- > ● Distribution 17 minutes 3 seconds
- ▼ ● Activation 39 minutes 51 seconds
  - ISSU Activation of image: C9800-CL-universalk9.17.09.03.SPA.bin on device: 10.10.10.146 completed successfully.
  - > ● Pre Activation Operation 2 seconds
  - > ● Image Activation 30 minutes 19 seconds
  - > ● Staggered AP Upgrade 6 minutes
  - > ● Install Commit 3 minutes 5 seconds
  - > ● Remove Inactive Images 6 seconds
  - > ● Collect Running Image Details 10 seconds
  - > ● Verify Image Activation 1 second
  - > ● Post Activation Operation 4 seconds

Task Name Staggered AP Upgrade

Task Status Success ( Staggered AP Upgrade Status: Completed, Total number of APs = 1, Upgraded = 1, In Progress = 0, Remaining = 0, APS not handled by Rolling AP Upgrade = 0 )

ISSU Activation

# Staggered Upgrade



For your  
reference

```
pnp-9800#show ap upgrade
Status: In progress
From version: 17.9.2.52
To version: 17.9.3.50
Started at: 05/30/2023 04:56:51 UTC
Configured percentage: 15
Percentage complete: 0
Expected time of completion: 05/30/2023 05:04:51 UTC

Client steering: Enabled
Accounting percentage: 90%
Iteration expiry time: 9 minutes

Progress Report

Iterations

Iteration Start time End time AP count

0 05/30/2023 04:56:51 UTC 05/30/2023 04:56:51 UTC 0

Upgraded

Number of APs: 0
AP Name Radio MAC Iteration Status Site

In Progress

Number of APs: 1
AP Name Radio MAC

thirdwheel_9100 f4bd.9e9f.3f00

Remaining

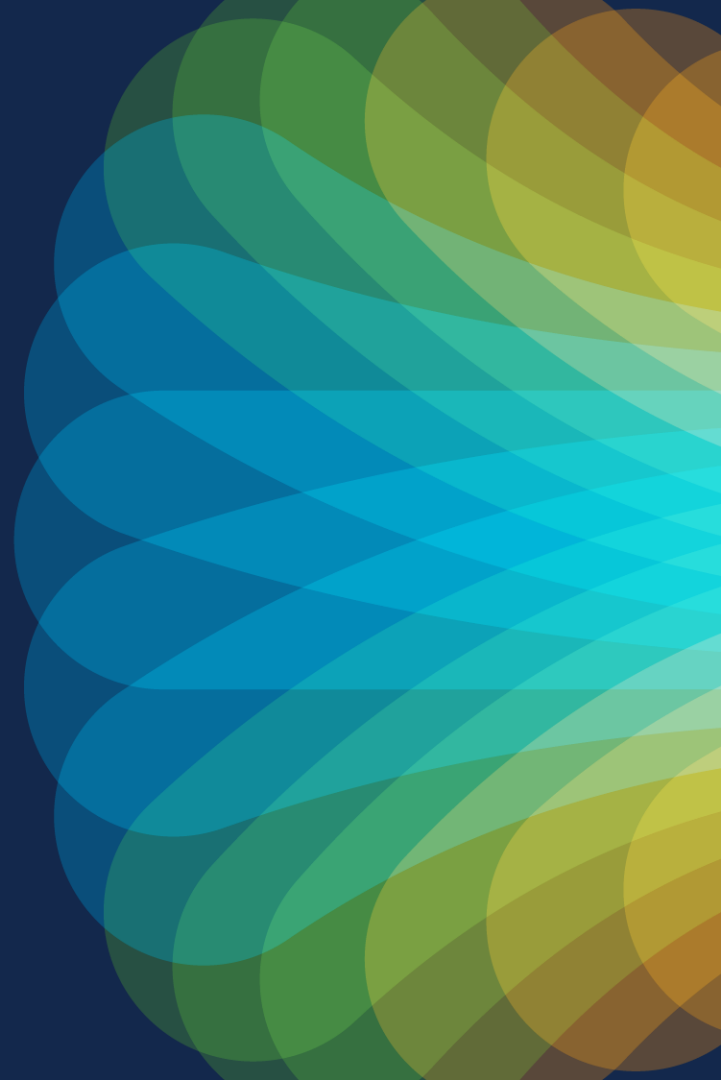
Number of APs: 0
AP Name Radio MAC

APs not handled by Rolling AP Upgrade

AP Name Radio MAC Status Reason for not handling by Rolling AP Upgrade

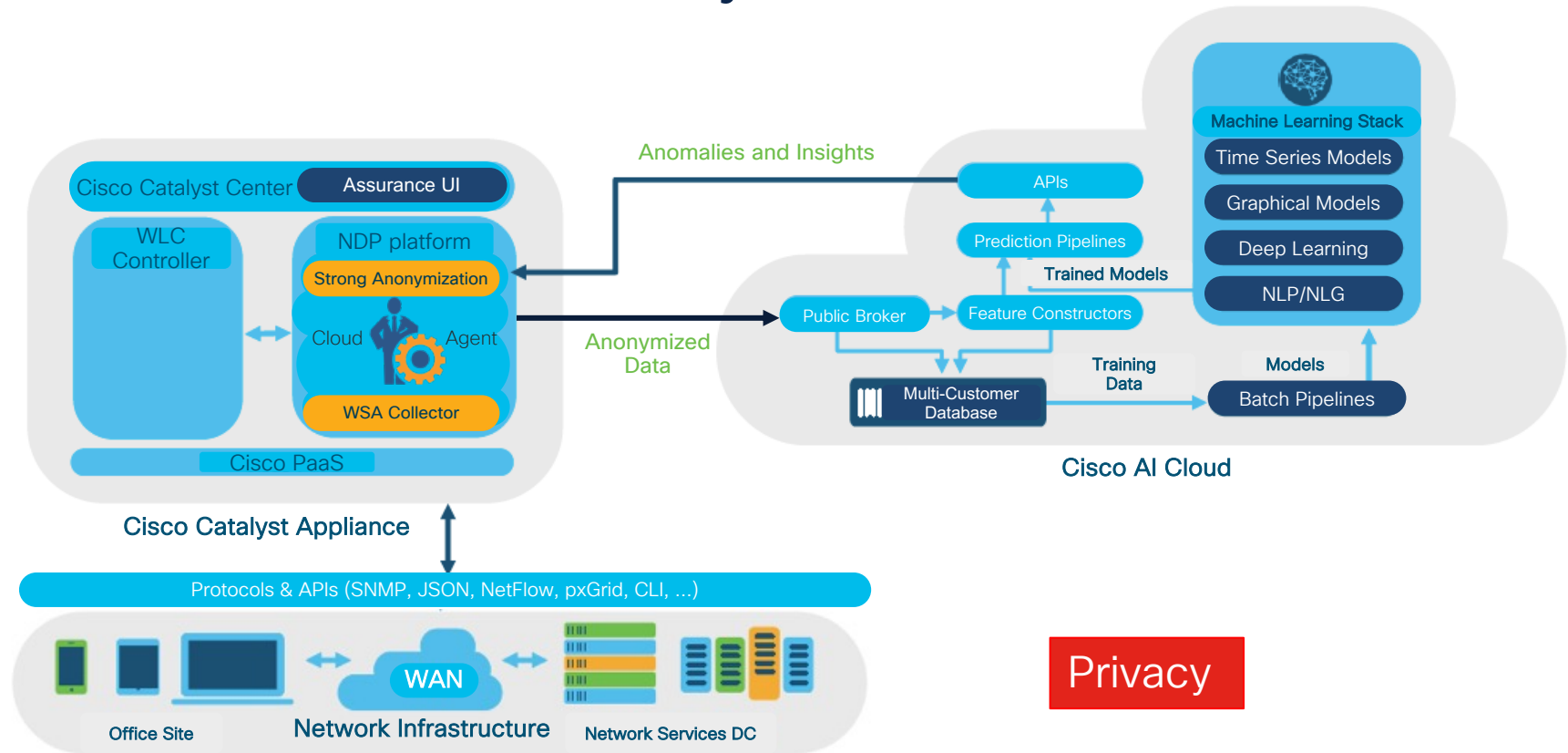
```

# Habit #5 - Explore Proactive insights with AI/ML





# Cisco AI Network Analytics Architecture

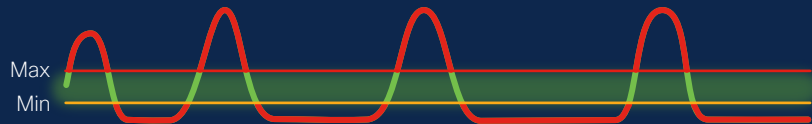


# AI-Driven Dynamic Baselining

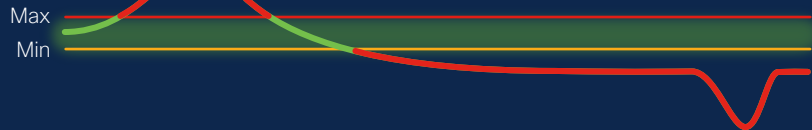
Learn About the Issues that Really Matter

Custom Thresholds = False Positives

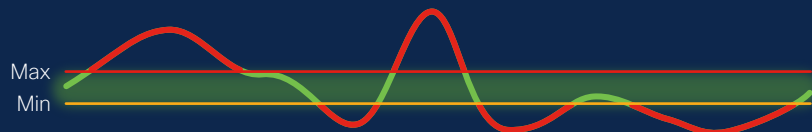
Environment 1



Environment 2

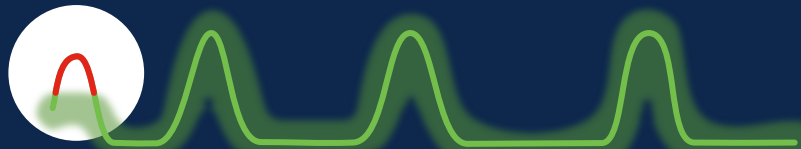


Environment 3

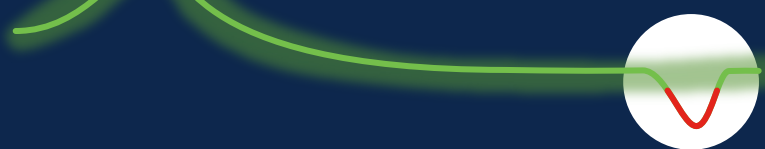


AI-Driven Dynamic Baselines = Relevant Anomalies

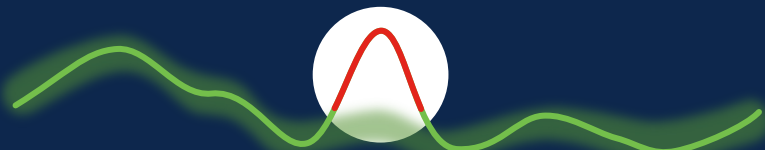
Environment 1



Environment 2



Environment 3



# AI Driven Baseline Issues

## Use case:

What are the expected KPI performance across APs and SSIDs? How can I effectively identify, isolate and mitigate deviations from the baseline performance.

## Key Benefits:



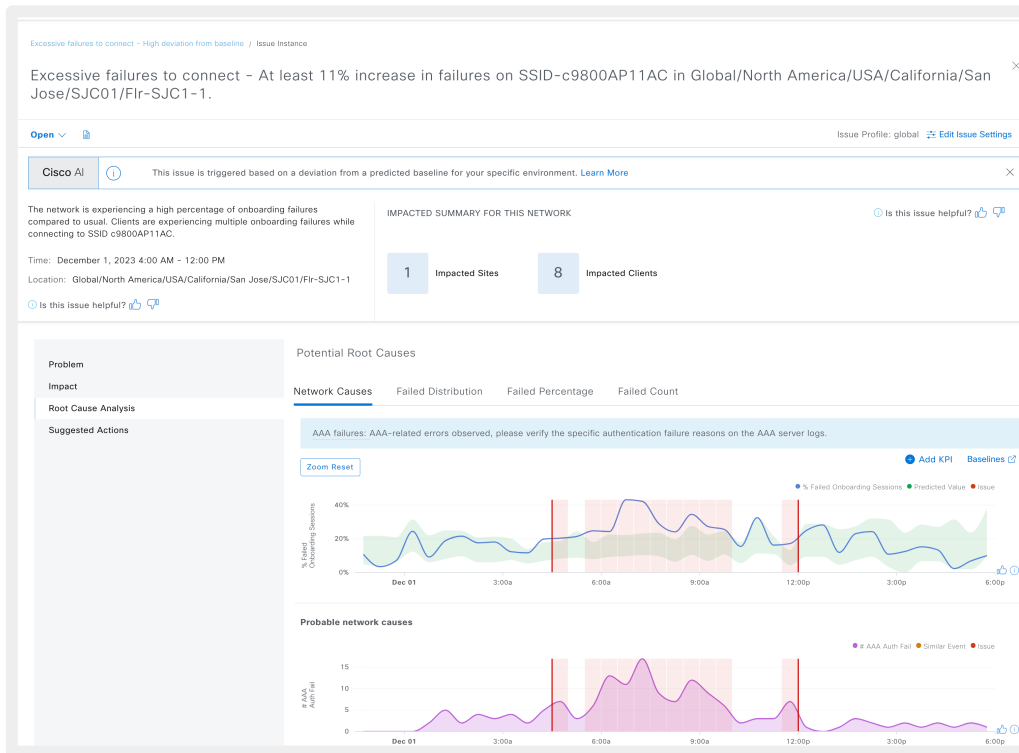
View Dynamic baselines and deviations for 12 (onboarding + throughput) KPIs



Accelerated troubleshooting with end-to-end workflow complete with impact and potential root cause details



Active feedback loop (thumps up/down) to integrate SME expertise to further refine baselines over period of time



# AI Analytics – AP Family & Endpoint Comparison

## Use case:

View and evaluate AP and client performance across different sites through dynamic performance clusters identified based on selected KPI

## Key Benefits:



Compare AP performance across traffic classes



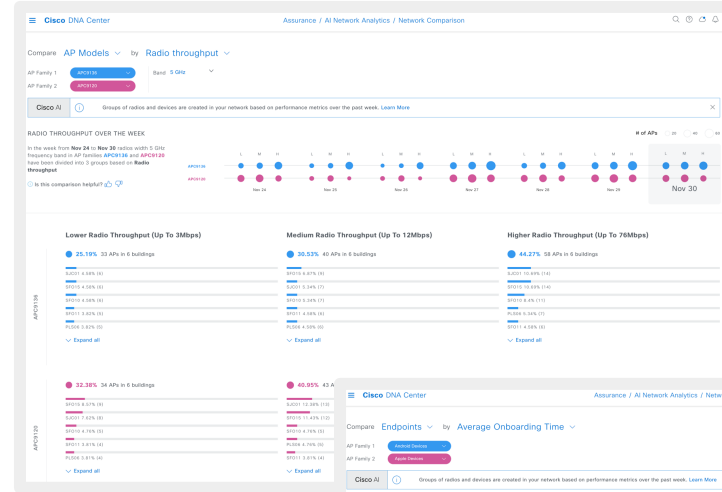
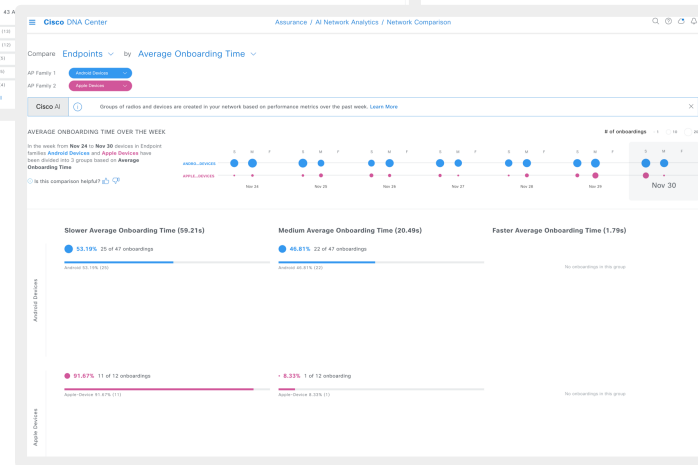
Flexibility to compare both on-boarding and throughput KPIs



View and compare dynamic performance clusters for a selected KPI and AP families

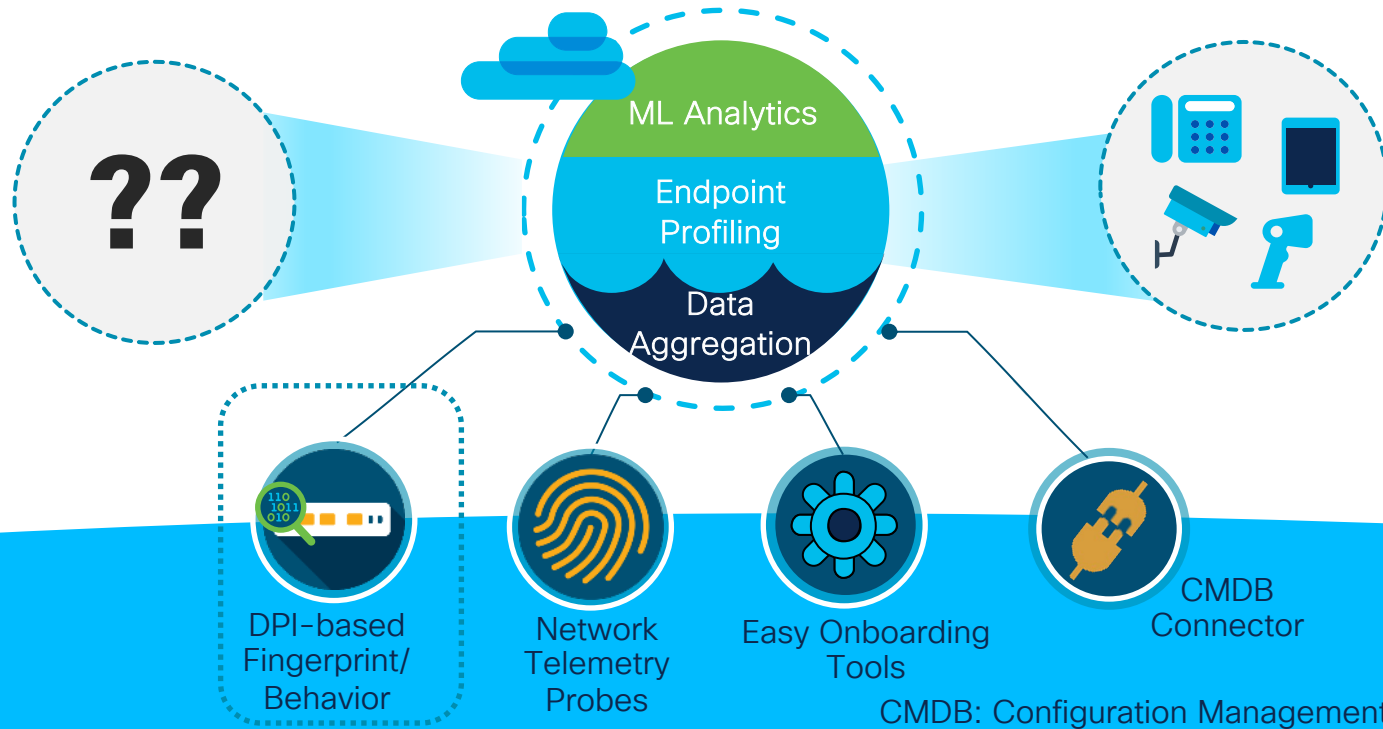


View and compare onboarding KPIs for specific device types for days of a week

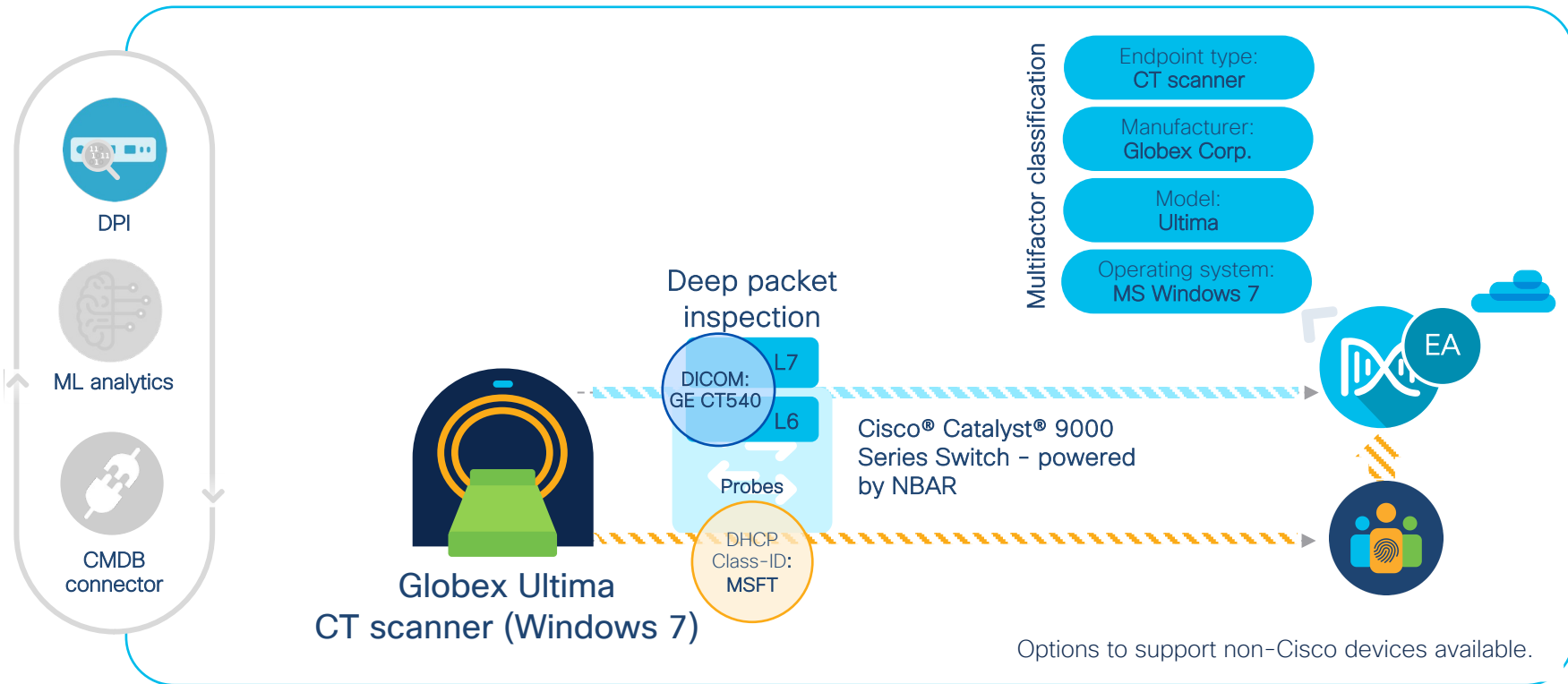


# AI Endpoint Analytics on Cisco Catalyst Center

Rapidly reducing the unknowns by aggregating data from different sources



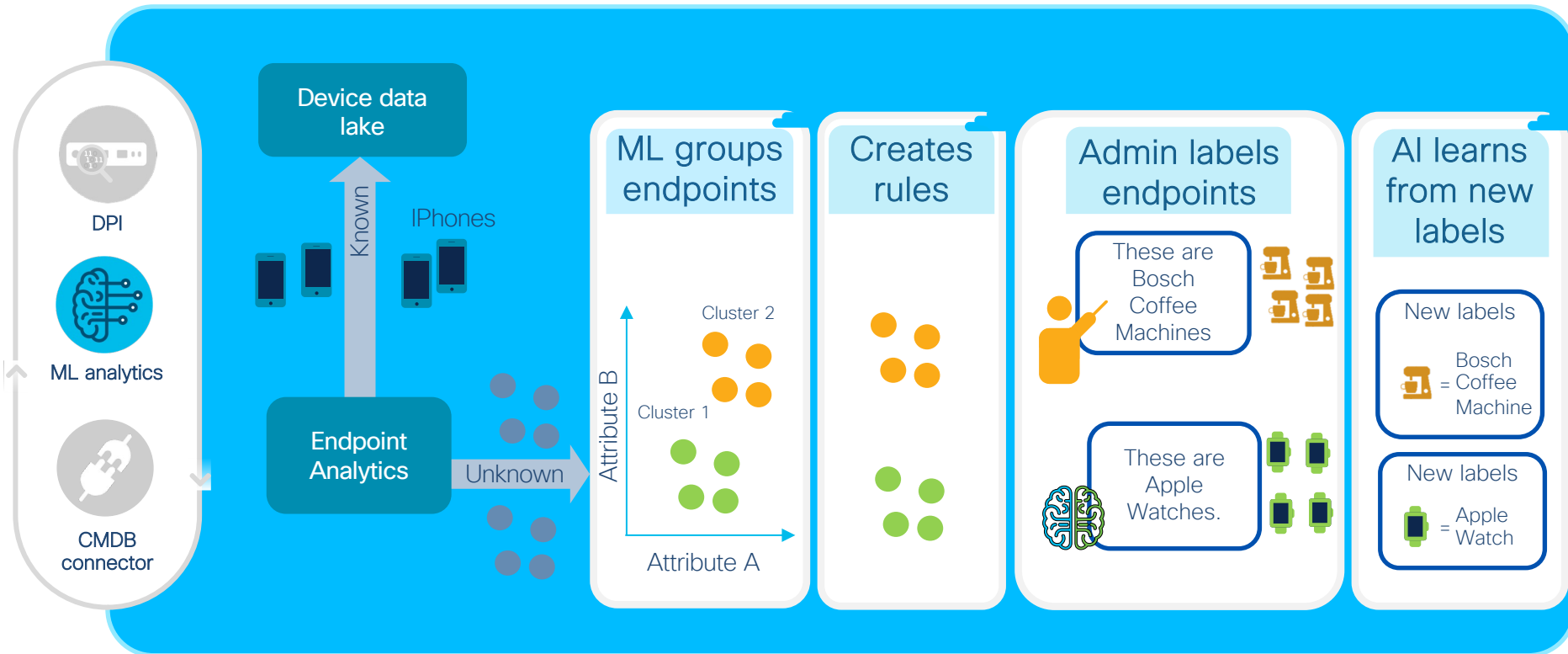
# Classification based on Deep Packet Inspection (DPI)



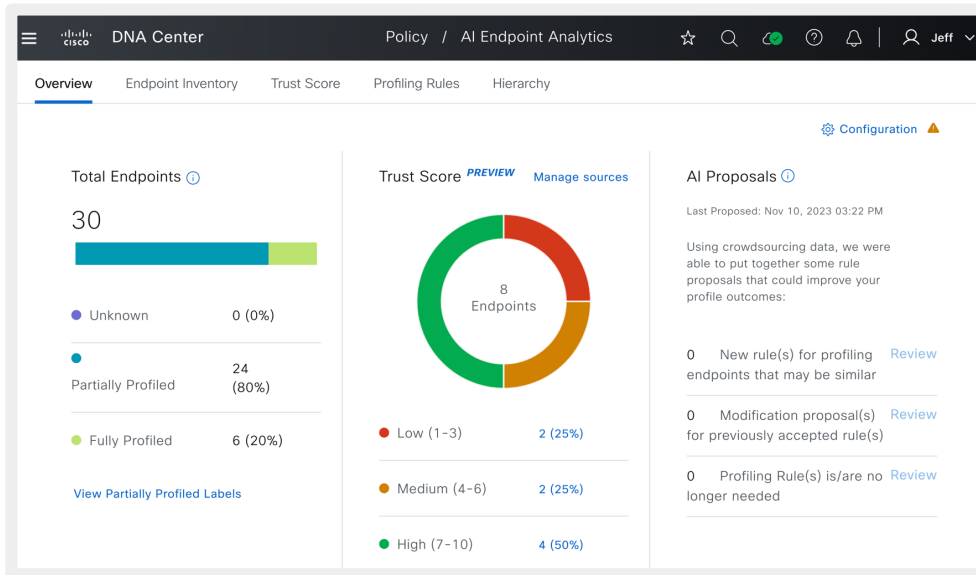
# Reducing Unknowns with Machine Learning



For your  
reference

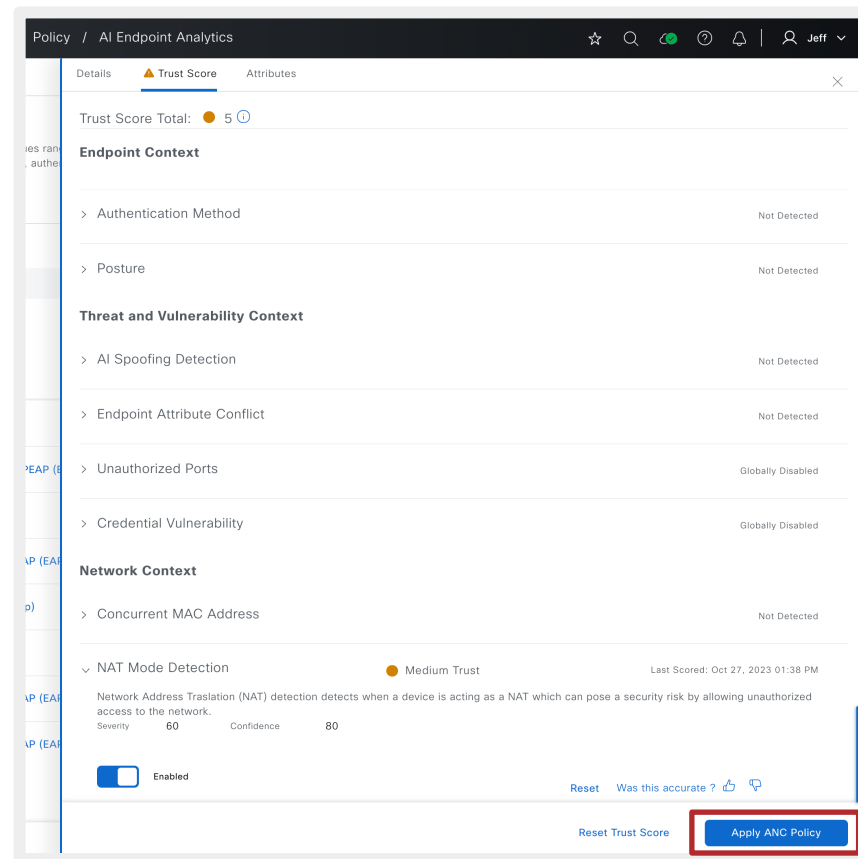


# Trust Scores and Remediation



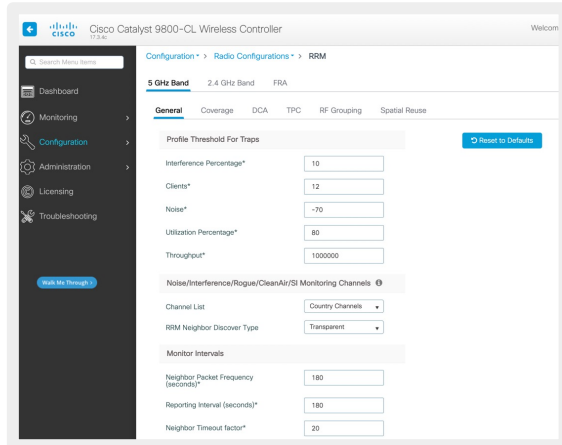
## Adaptive Network Control - ANC

Remediate the host via Identity Services Engine - ISE

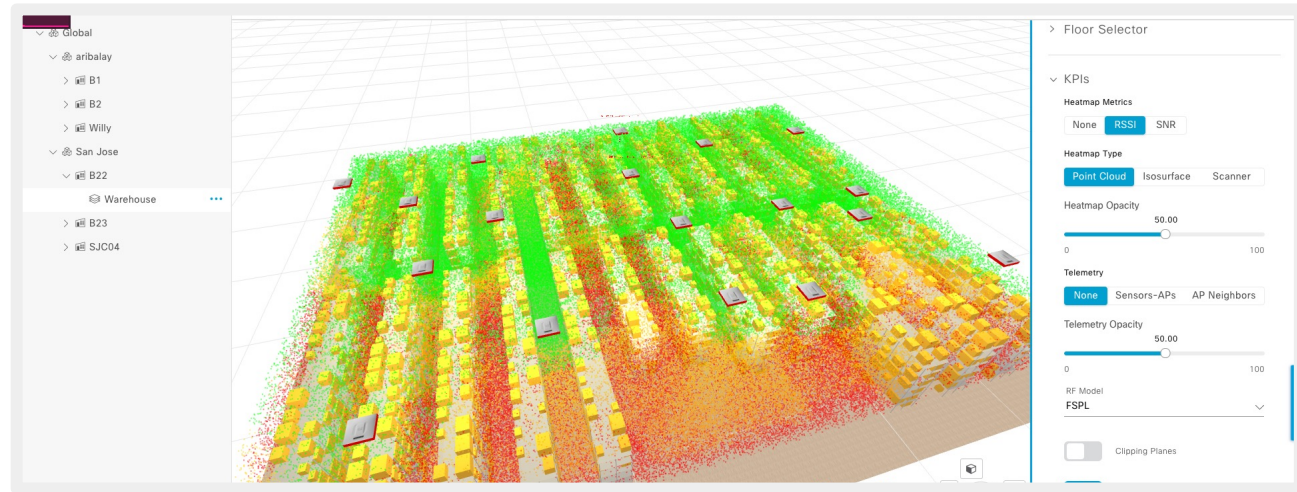




# Why Radio Resource Management



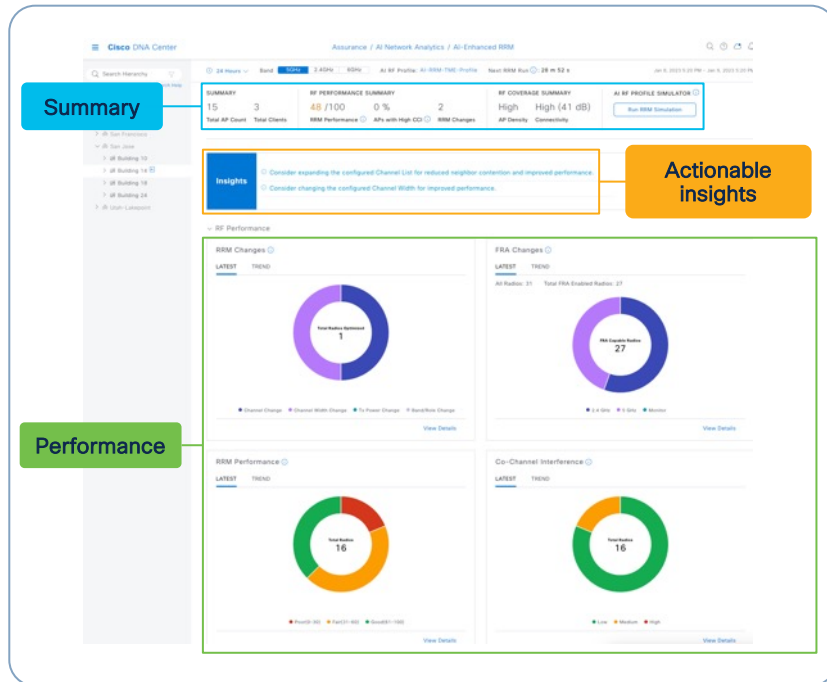
- 10min worth of data
- No "busy hour(s)"
- No building segmentation
- No visibility
- Lots of tuning knobs
- No simulation mode \*\*



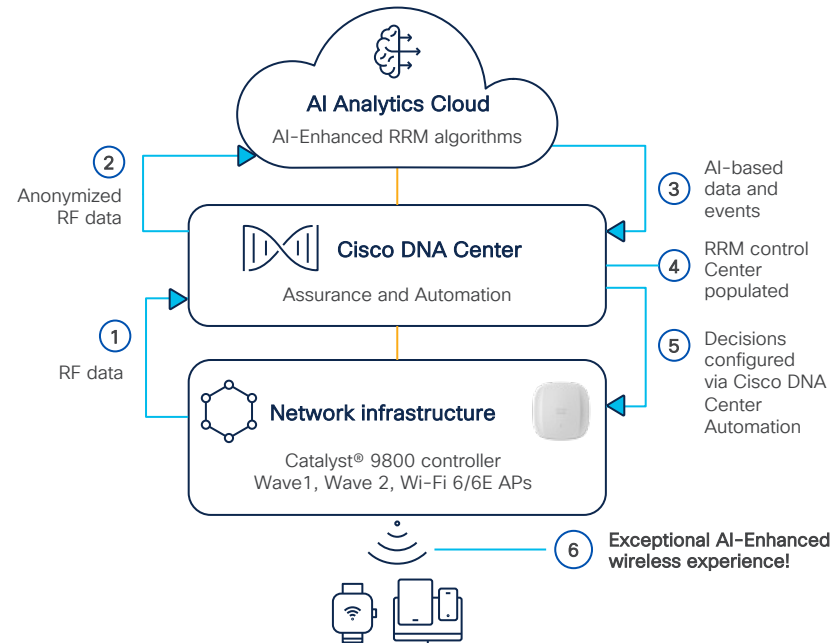
# AI powers your network with AI-Enhanced RRM

Smarter RF = Better user experience, reduced operational costs & time IOS XE 17.9.3+ DNAC v2.3.3.7+

## Instantaneous visibility



## Proactive optimizations



# Easy Three-Step Deployment Workflow

Reap the Benefits of AI-Enhanced RRM Within Minutes!



For your  
reference

1

Give AI-Enhanced RRM  
Cloud Access in Settings.

The screenshot shows the Cisco DNA Center Settings page. The left sidebar contains navigation links: Search Settings, Accounts, Connect, Credentials, Account, Licensing, Connection Mode, Settings, Distribution Servers, Controllability, Resync Interval, IP, Ping, EULA Acceptance, Device Authorization, Prompts, Configuration Archive, Services, Preload, Identification and Policy Services, Integrity Verification, and Page. The main content area is titled 'Settings / External Services' and 'Cisco AI Analytics'. Under 'AI Network Analytics', there is a checkbox 'Enable AI Network Analytics' which is checked. Below this, under 'AI-ENHANCED RRM', there is a checkbox 'Enables AI-Enhanced RRM' which is also checked. At the bottom, under 'EVENTS ANALYTICS PREVIEW', there is a checkbox 'Enable log export' which is unchecked.

2

Create an AI RF Profile.

The screenshot shows the 'Edit AI Radio Frequency Profile' page in Cisco DNA Center. The page title is 'Wireless / Edit AI RF Profile'. The 'Profile Name' is 'AI-RRM-TME-Profile'. Under 'Basic Settings', the 'Radio Frequency Settings' section has three checkboxes: '2.4 GHz' (checked), '5 GHz' (checked), and '6 GHz' (checked). The 'Busy Hours' section has a 'Start Time' of '9:00' and an 'End Time' of '17:00'. The 'Busy Hour Sensitivity' is set to 'High'. The 'Enable RF Settings' section has three checkboxes: '2.4 GHz' (checked), '5 GHz' (checked), and '6 GHz' (checked). The 'Flexible Radio Assignment' checkbox is unchecked. The 'Dynamic Channel Assignment' checkbox is unchecked. The 'Dynamic Bandwidth Selection' checkbox is unchecked. The 'Transmit Power Control' checkbox is unchecked.

3

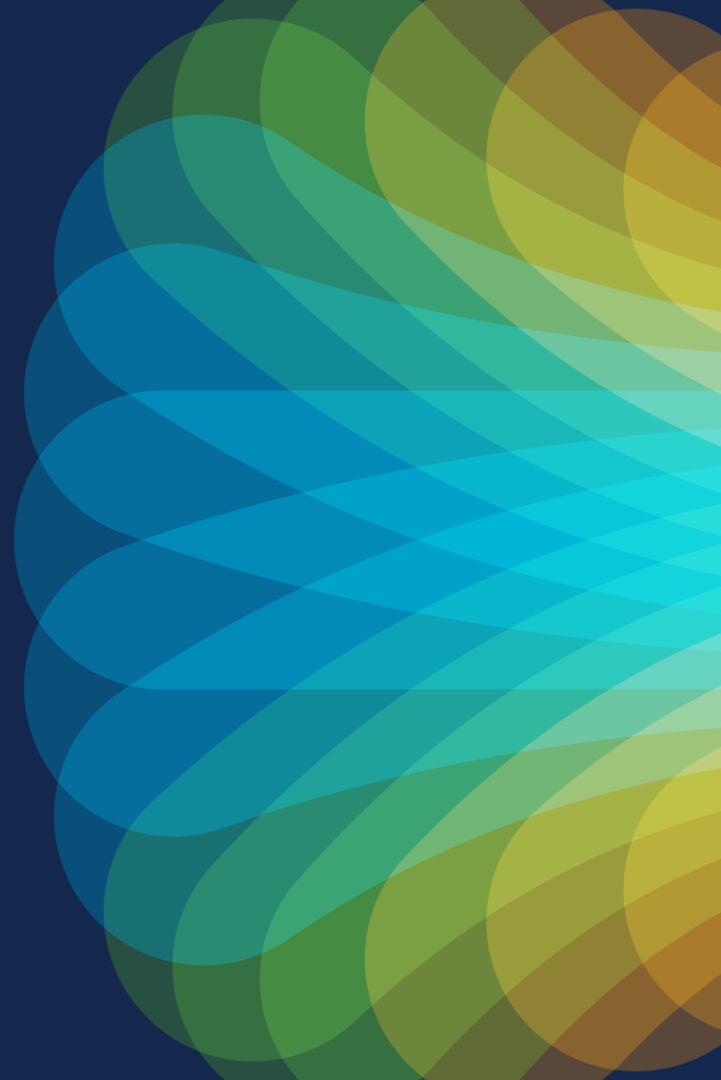
Assign AI RF Profile to a building,  
and provision your C9800 & APs.

The screenshot shows the 'Assign Locations to AI RF-Profile: AI\_RF\_Profile' page in Cisco DNA Center. The page title is 'Assign Locations to AI RF-Profile: AI\_RF\_Profile'. A message at the top states: 'Below selected and impacted locations will be upgraded with AI RF Profile and APs will be provisioned with new AI RF Tags.' The 'Site selection summary' table shows the following data:

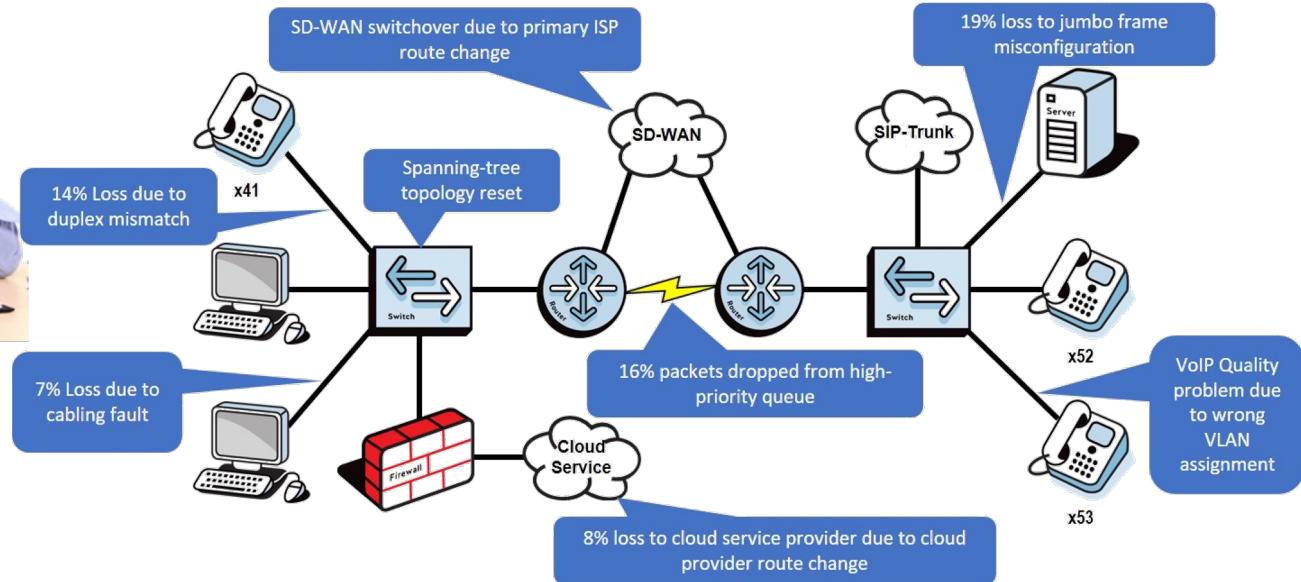
| Selected Location | Impacted Location               |
|-------------------|---------------------------------|
| Building 14       | No impacted locations available |

The 'Search Hierarchy' section shows a list of locations: San Jose, Building 10, Building 14 (selected), Building 18, Building 24, and Utah-Lakepoint.

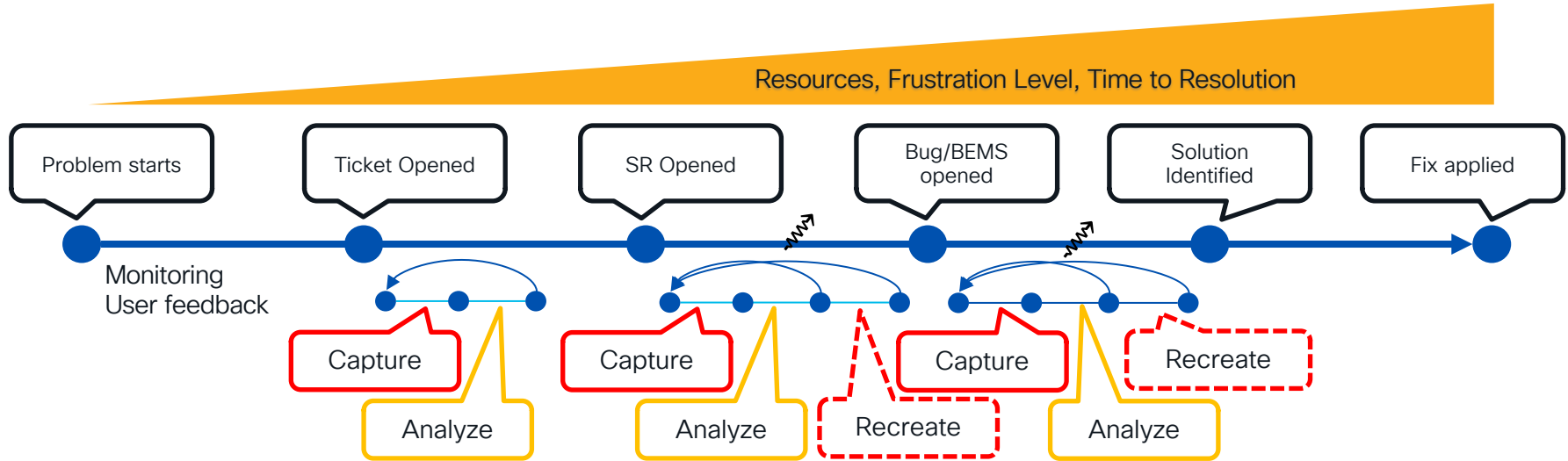
# Habit #6 – Ease your Remote Support with RADKit



# How painful is this?



# Current Troubleshooting Method



## With RADKit

- TAC Engineer is autonomous
- Immediate data transfer to SR
- API for complex data capture
- Effortless for our customers



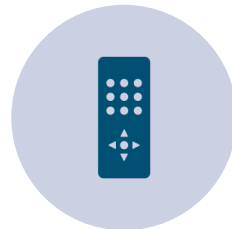
## Without RADKit

- Customer laptop tied up in Webex
- Repetitive requests to customer
- Delays in data request turnaround
- Complex requests met with hostility

# What is Remote Automation Development Kit (RADKit)?



RADKit is a Software Development Kit. It frees you from CVE monitoring of dozens of opensource packages.



The included tools allow your NetOps staff to interactively connect to remote terminals, WebUIs or desktops.



Use our powerful and easy to use our efficient and scalable APIs for remote and local automations.

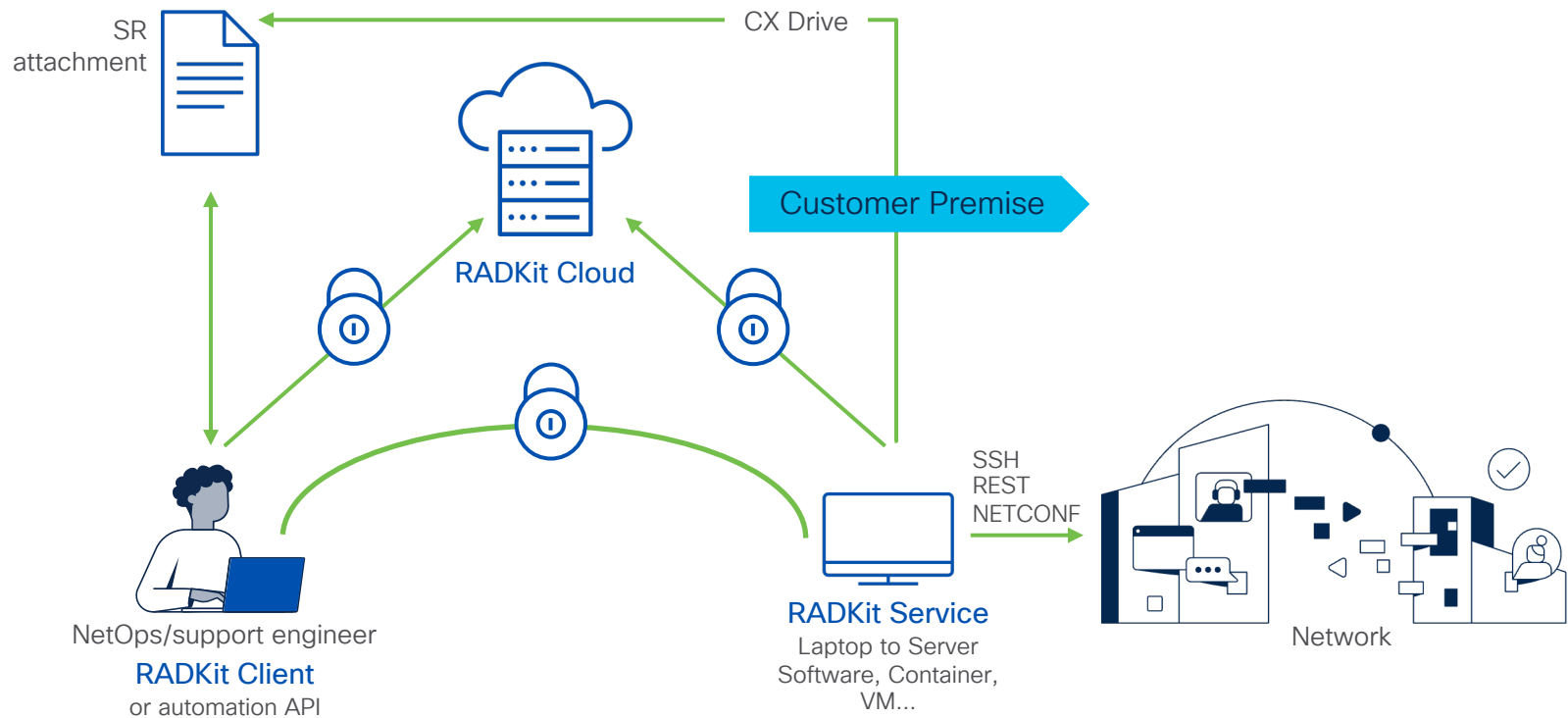


Full-on security with SSO, Certificates, data encryption at rest and in transit, exhaustive audit-logs,...

RADKit enhances all NetOps activities, streamlines incident escalation processes, and more!

# RADKit General Architecture

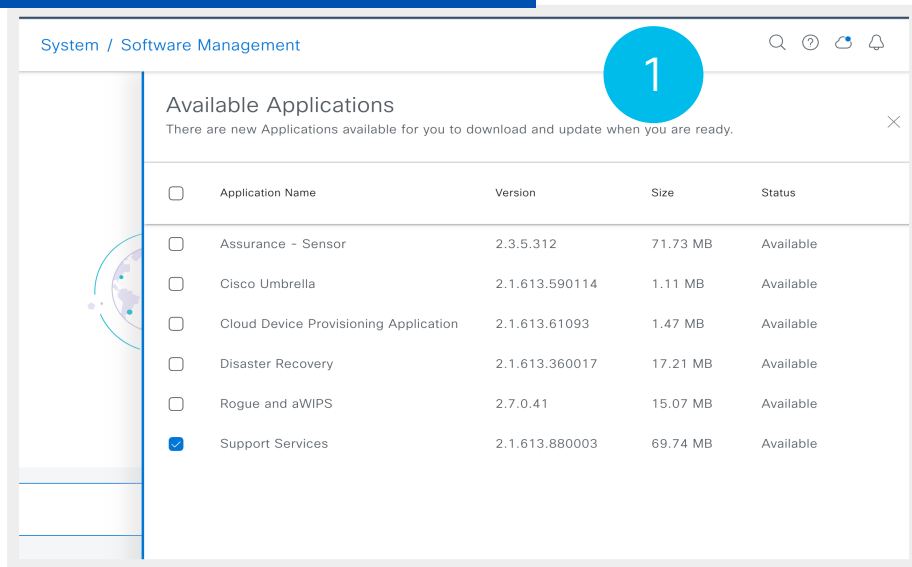
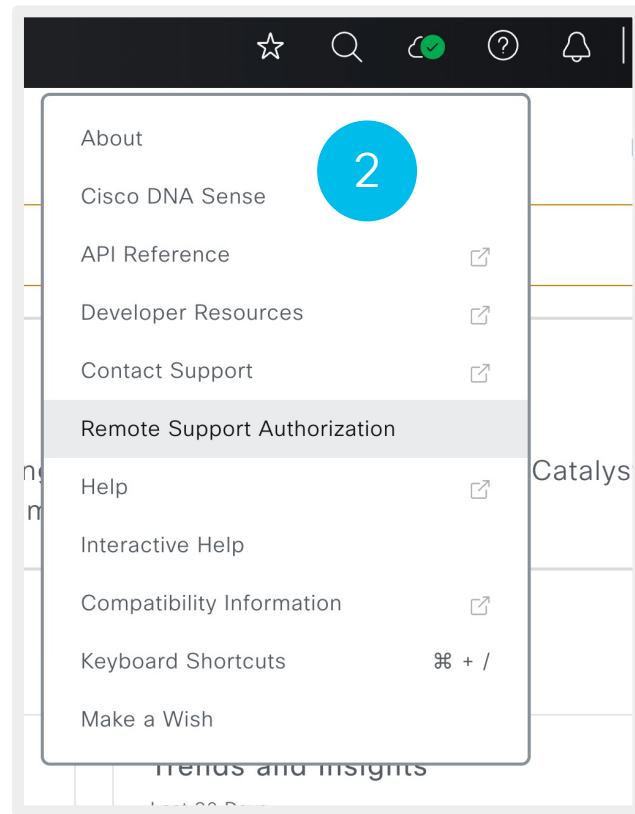
<https://radkit.cisco.com>





# Install RADKit Service in Catalyst Center

- Install Support Services in Catalyst Center
- Under '?' create a Remote Support Authorization



# RADKit Demo

# Cisco-RADKit Intro – RADKit examples

- <https://github.com/Cisco-RADKit/Intro>
- Full documentation at [radkit.cisco.com](https://radkit.cisco.com)

Cisco-RADKit / Intro (Public)

<> Code Issues Pull requests Actions Projects Security Insights

main 1 branch 0 tags Go to file

mstanczy create\_devices fixed intendation ac4ca43 1 hour ago 38 commits

|             |                                        |             |
|-------------|----------------------------------------|-------------|
| Advanced    | Update README.md                       | 5 hours ago |
| Control-API | create_devices fixed intendation       | 1 hour ago  |
| Intro RPC   | updated the Service ID in dCloud setup | 2 hours ago |
| SNMP        | Adding simple snmp example             | yesterday   |
| .gitignore  | Initial commit                         | last week   |
| LICENSE     | Initial commit                         | last week   |
| README.md   | Update README.md                       | last week   |

README.md

## Intro to RADKit

This repository contains examples meant as an introduction to the RADKit API.

The examples are split into multiple sections:

- RADKit RPC API basics - execute CLI on multiple devices, use REST, Swagger, SNMP,... from the REPL
- Simple standalone scripts - wrap your REPL into a script without complex Python setup
- Advanced standalone scripts - how to write fully standalone scripts that do not rely on the RADKit REPL
- Control API - Control RADKit Service by API. Manage the inventory, users, etc. programmatically

Example codes to get started with Cisco RADKit

Readme

Unlicense license

Activity

0 stars

0 watching

1 fork

Report repository

Releases

No releases published

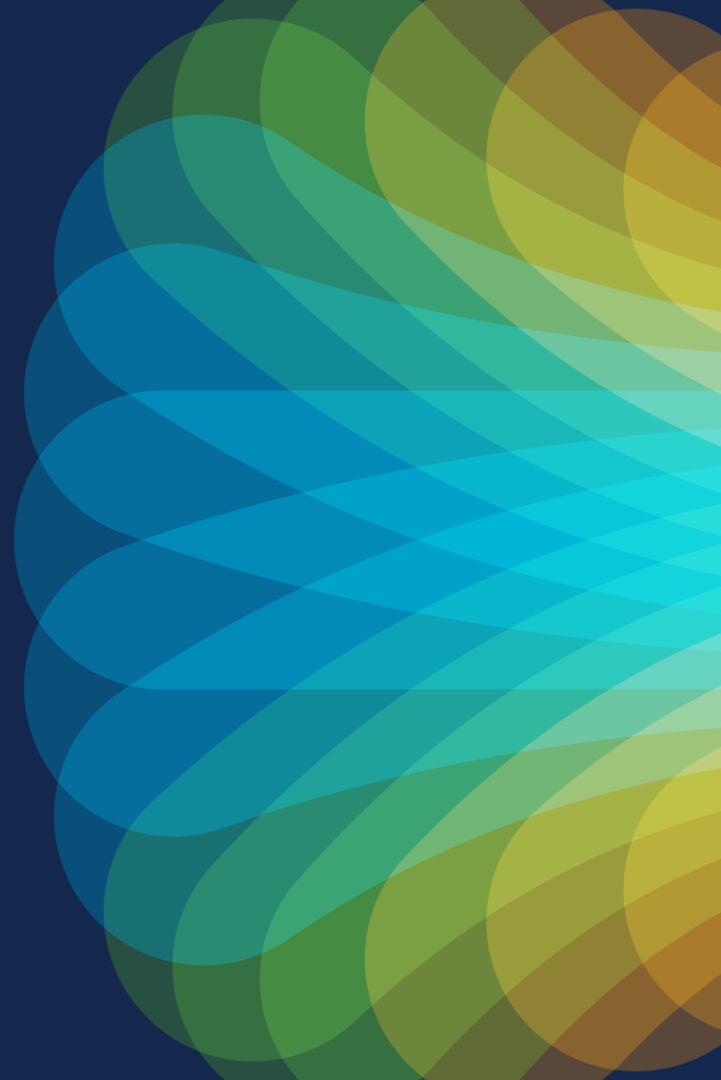
Packages

No packages published

Languages

Python 100.0%

# Habit #7 - Up your automation game with APIs and other integrations



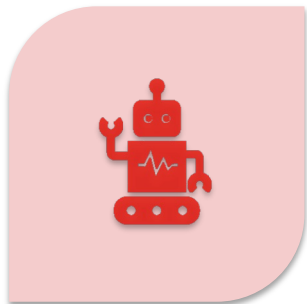


**DRIVE FOR  
SHOW  
AND  
PUTT FOR  
DOUGH**



**GUI FOR  
SHOW  
AND  
API FOR  
DOUGH**

# Why API?



AUTOMATION



INTEGRATION



INNOVATION

# APIs Directly From Catalyst Center

Platform → Developer Toolkit

The screenshot shows the Cisco DNA Center Platform Developer Toolkit interface. The left sidebar contains navigation links for APIs, Integration Flows, and Event Notifications. The main content area is titled 'Connectivity' and includes a search bar and a table of connectivity APIs. A blue circle with the number '1' is overlaid on the 'Connectivity' section.

| Method | Name                                             | Description                    | URL                                      | Action |
|--------|--------------------------------------------------|--------------------------------|------------------------------------------|--------|
| DELETE | Remove WLC from Fabric Domain <sup>Client</sup>  | Remove WLC from Fabric Domain  | /business/sda/wireless-controller        | ...    |
| POST   | Add SSID to IP Pool Mapping <sup>Client</sup>    | Add SSID to IP Pool Mapping    | /business/sda/hostonboarding/ssid-ippool | ...    |
| PUT    | Update SSID to IP Pool Mapping <sup>Client</sup> | Update SSID to IP Pool Mapping | /business/sda/hostonboarding/ssid-ippool | ...    |
| GET    | Get SSID to IP Pool Mapping <sup>Client</sup>    | Get SSID to IP Pool Mapping    | /business/sda/hostonboarding/ssid-ippool | ...    |
| POST   | Add WLC to Fabric Domain <sup>Client</sup>       | Add WLC to Fabric Domain       | /business/sda/wireless-controller        | ...    |

The screenshot shows the 'Get Client Detail' API page in the Cisco DNA Center Platform Developer Toolkit. The page includes a 'Parameters' section with a 'Request Query Parameters' table. A blue circle with the number '2' is overlaid on the 'Request Query Parameters' table.

| Name       | Description                                                         | DataType | Required | Default Value |
|------------|---------------------------------------------------------------------|----------|----------|---------------|
| macAddress | MAC Address of the client                                           | string   | Yes      |               |
| timestamp  | Epoch time(in milliseconds) when the Client health data is required | number   | No       |               |

The screenshot shows the 'Try 'Get Client Detail'' API page in the Cisco DNA Center Platform Developer Toolkit. The page includes a 'Parameters' section with a 'Request Query Parameters' table. A blue circle with the number '3' is overlaid on the 'Response' section.

Method: **GET** Public URL :https://10.67.27.75/dna/intent/api/v1/client-detail

PARAMETERS

QUERY PARAMETERS

macAddress\* <sup>Client</sup>  
a0:36:9f:bc:ec:fa

timestamp <sup>Client</sup>

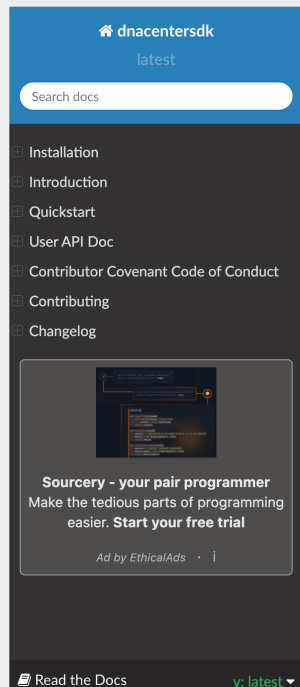
Response Headers Status Code: 200

```
1 - {
2 - "detail": {
3 - "id": "A0_36_9F_BC_EC_FA",
4 - "connectionStatus": "DISCONNECTED",
5 - "tracked": "No",
6 - "hostType": "WIRED",
7 - "userId": null,
8 - "duid": "",
9 - "identifier": "PC-Client7",
10 - "hostName": "PC-Client7",
11 - "hostOs": "Windows",
12 - "hostVersion": null,
13 - "subType": "Intel-Device",
14 - "firmwareVersion": null,
15 - "deviceVendor": "Intel Corporation",
16 - "deviceForm": "Workstation",
17 - "salesCode": null,
18 - "countryCode": null,
19 - "lastUpdated": 1700978820000,
20 - "healthScore": [
21 - {
22 - "healthType": "OVERALL",
23 - "reason": "",
24 - "score": 1
25 - },
26 - {
27 - "healthType": "ONBOARDED",
28 - "reason": "",
29 - "score": 1
30 - },
31 - {
32 - "healthType": "CONNECTED",
33 - "reason": "",
34 - "score": 0
35 - }
36 -],
37 - "hostMac": "A0:36:9F:BC:EC:FA",
38 - }
39 - }
```

# SDK

```
>>> from dnacentersdk import DNACenterAPI
```

```
>>> api = DNACenterAPI()
```



🏠 / dnacentersdk

[Edit on GitHub](#)

## dnacentersdk

*Simple, lightweight, scalable Python API wrapper for the DNA Center APIs*

Welcome to the docs! dnacentersdk is a *community developed* Pythonic wrapping of the DNA Center APIs (for API versions: 1.2.10, 1.3.0, 1.3.1, 1.3.3, 2.1.1, 2.1.2, 2.2.1, 2.2.2.3, 2.2.3.3, 2.3.3.0 and 2.3.5.3). The package represents all of the Cisco DNA Center API interactions via native Python tools. Making working with the Cisco DNA Center APIs in Python a *native* and *natural* experience.

**dnacentersdk helps you get things done faster.** We take care of the API semantics, and you can focus on writing your code.

With dnacentersdk, you can easily:

- Interact with the DNA Center APIs in an interactive Python session
- Quickly create code that enables you get something done in DNA Center
- Leverage the API wrapper to cleanly add DNA Center functionality to your project without having to write the boilerplate code for working with the DNA Center APIs

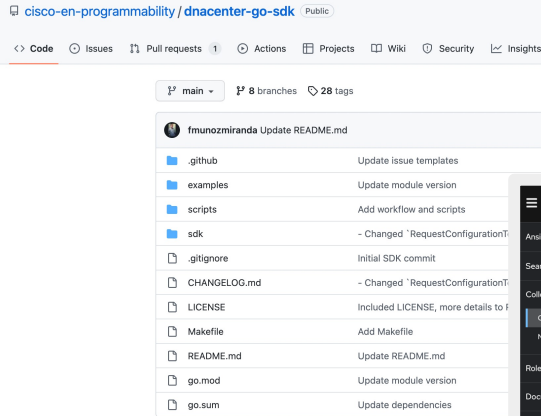
To *dive in* and see how dnacentersdk makes your life better, check out the [Quickstart!](#)

## The User Guide

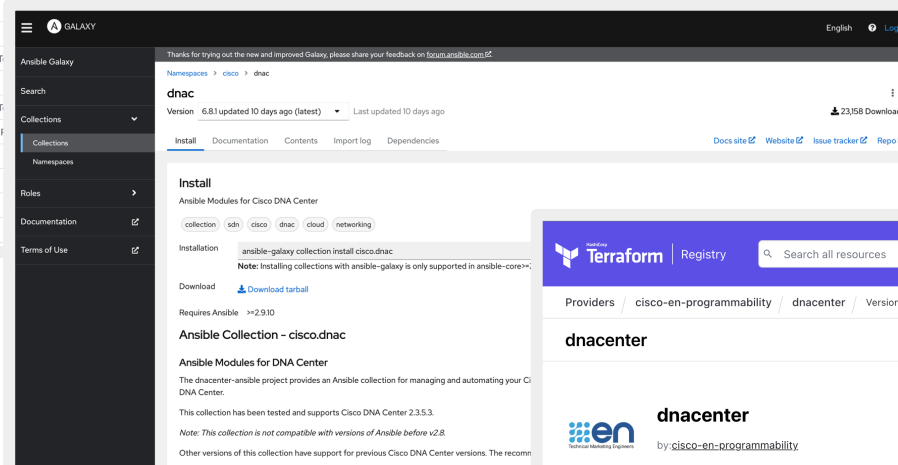
<https://dnacentersdk.readthedocs.io/en/latest/>



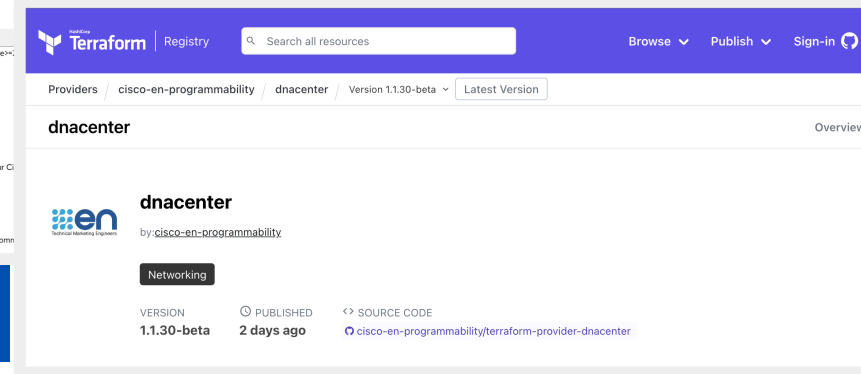
# Go/Ansible/Terraform



<https://github.com/cisco-en-programmability/dnacenter-go-sdk>



<https://galaxy.ansible.com/ui/repo/published/cisco/dnac/>



<https://registry.terraform.io/providers/cisco-en-programmability/dnacenter/latest>

# Native Webex Issue Integration



Catalyst Center Notification Bot 8:22 am

## Cisco DNA Center Notification

**Source DNA** 10.67.27.75  
**Center IP:**  
**Severity:** 3  
**Category:** TASK\_COMPLETE  
**Timestamp:** 2023-10-29 21:22:41  
**Issue Name:** Security-Advisory-New-Update-Available-For-Scan  
**Issue Description:** Security Advisory updates available  
We recommend that you perform a network scan.

Cisco DNA Center Issue Details



Catalyst Center Notification Bot Yesterday, 7:57 pm

## Cisco DNA Center Notification

**Source DNA** 10.67.27.75  
**Center IP:**  
**Severity:** 3  
**Category:** WARN  
**Timestamp:** 2023-10-29 08:57:19  
**Issue Name:** High input/output error on interface GigabitEthernet1/0/18 (Interface description: 9300-48 L2 g1/0/2)  
**Issue Description:** High Input/Output error Rx 2.27% Tx 0.0% on interface GigabitEthernet1/0/18 (Interface description: 9300-48 L2 g1/0/2), Device Infra-3850-R8.dcloud.cisco.com  
**Issue Status:** active

Cisco DNA Center Issue Details



Catalyst Center Notification Bot Monday, 9:05 am

## Cisco DNA Center Notification

**Source DNA** 10.67.27.75  
**Center IP:**  
**Severity:** 3  
**Category:** WARN  
**Timestamp:** 2023-11-26 22:05:00  
**Issue Name:** The 5GHz radio on AP AP002c.c899.1b3c is experiencing high utilization  
**Issue Description:** The 5GHz radio on the AP AP002c.c899.1b3c has exceeded the 70% threshold and is currently experiencing 76% utilization. This is impacting 0 client(s).  
**Issue Status:** active

Cisco DNA Center Issue Details

# Take aways



 Device Controllability to maximize value

 Telemetry for network/application/user insights

 Software Image management to keep code up to date

 Compliance and Configuration management for NetOps

 AI/ML for AIOps

 Utilise RADKit to aid in remote support

 API for automation/integration/innovation



# Did you know?

You can have a  
one-on-one session with  
a technical expert!

Visit Meet the Expert in The HUB  
to meet, greet, whiteboard & gain  
insights about your unique questions  
with the best of the best.



## Meet the Expert Opening Hours:

|                  |                         |
|------------------|-------------------------|
| <b>Tuesday</b>   | <b>3:00pm – 7:00pm</b>  |
| <b>Wednesday</b> | <b>11:15am – 7:00pm</b> |
| <b>Thursday</b>  | <b>9:30am – 4:00pm</b>  |
| <b>Friday</b>    | <b>10:30am – 1:30pm</b> |

# Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



# Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](https://www.CiscoLive.com/on-demand)

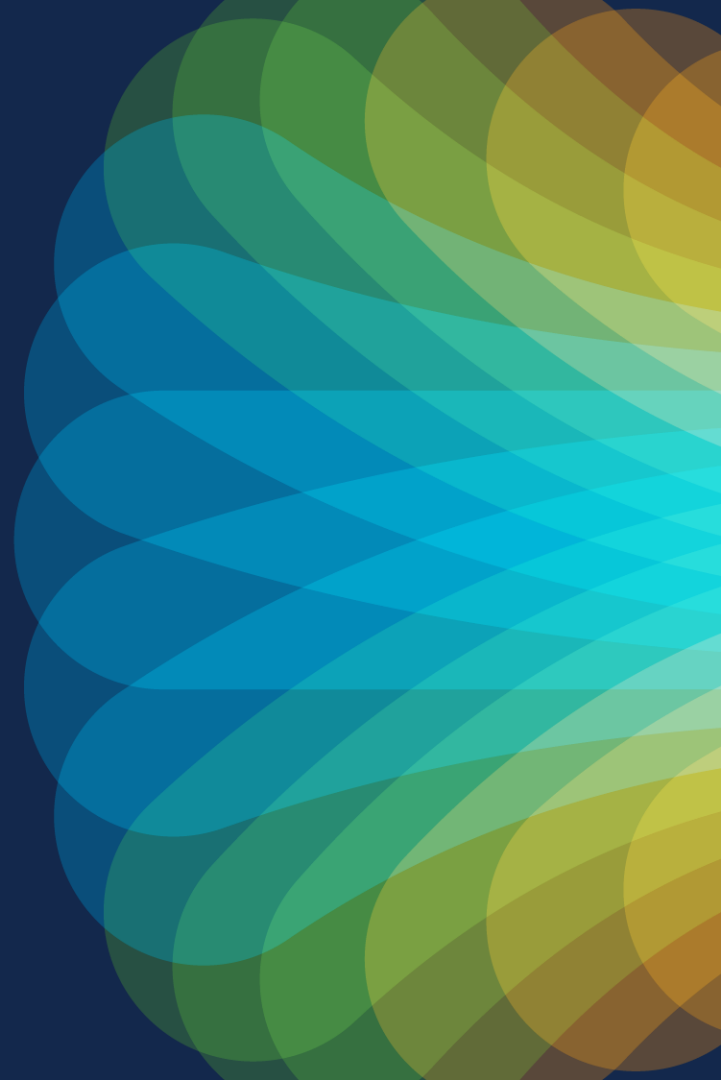


The bridge to possible

# Thank you

CISCO *Live!*

#CiscoLiveAPJC



The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC