

# 7 Habits for a successful Cisco DNA Center deployment

Adam Radford, Distinguished Architect @adamradford123  
Lila Rousseaux, Principal Architect @lila\_rousseau

# Cisco Webex App

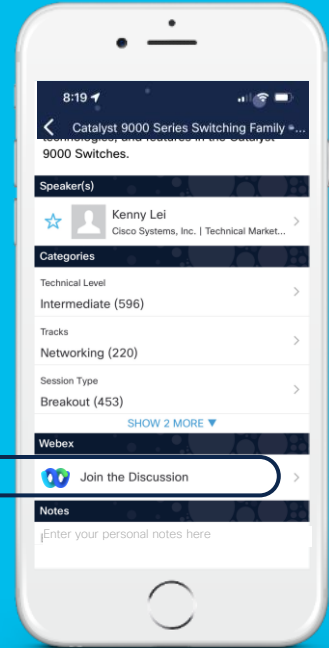
## Questions?

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 until February 24, 2023.



*Habit ...*

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

# Agenda

- Habit #1 – Understanding device controllability
- Habit #2 – Find issues before your users with telemetry
- Habit #3 – Compliance and Configuration management
- Habit #4 – Agile operations with software image management
- Habit #5 – Proactive insights with AI/ML
- Habit #6 – APIs and other integrations
- Habit #7 – Minimizing upgrade risk with AURA tool

# 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

Deployment of syslog setting SUCCESS

- 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 SUCCESS

- 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 SUCCESS

- DNS Configurations pushed successfully
- Process success on all devices.

Deployment of netflow setting SUCCESS

- 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 SUCCESS

- Configuration of application telemetry is only applicable upon enable/disable application telemetry action, so no operation was performed

Install of Swim Certificate SUCCESS

- SWIM Certificate was pushed successfully

Deployment of WSA certificate SUCCESS

- ICAP port and Assurance WSA Configuration pushed successfully
- WSA Certificate was pushed successfully

Monitoring

Settings

Telemetry

Trust

Deployment of Wireless AP Join Certificate SUCCESS

- Certificate already exists on the device.
- Deployment of Wireless AP Join Certificate setting initiated

Deployment of PKCS12 certificate SUCCESS

- 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 SUCCESS

- Setting does not apply to device, so no operation was performed

Deployment of IOS Telemetry Subscriptions configuration SUCCESS

- 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 SUCCESS

- AP Impersonation pushed successfully
- Deployment of AP Impersonation setting initiated

Deployment of Terminal Width SUCCESS

- Setting does not apply to device, so no operation was performed

Deployment of IPDT SUCCESS

- Cannot push IPDT Configuration on the device with IpAddress: 10.10.10.146 for Product Family: wireless controller (Not Applicable)

# What happens when a C9K switch is added to Cisco DNA Center?



Push PKI,  
IPDT, HTTP  
Server, SNMP  
configuration,  
Netconf-yang,  
telemetry

SNMP Poll  
and CLI  
telemetry  
collection

Syslog,  
SNMP Trap  
Streaming  
Telemetry

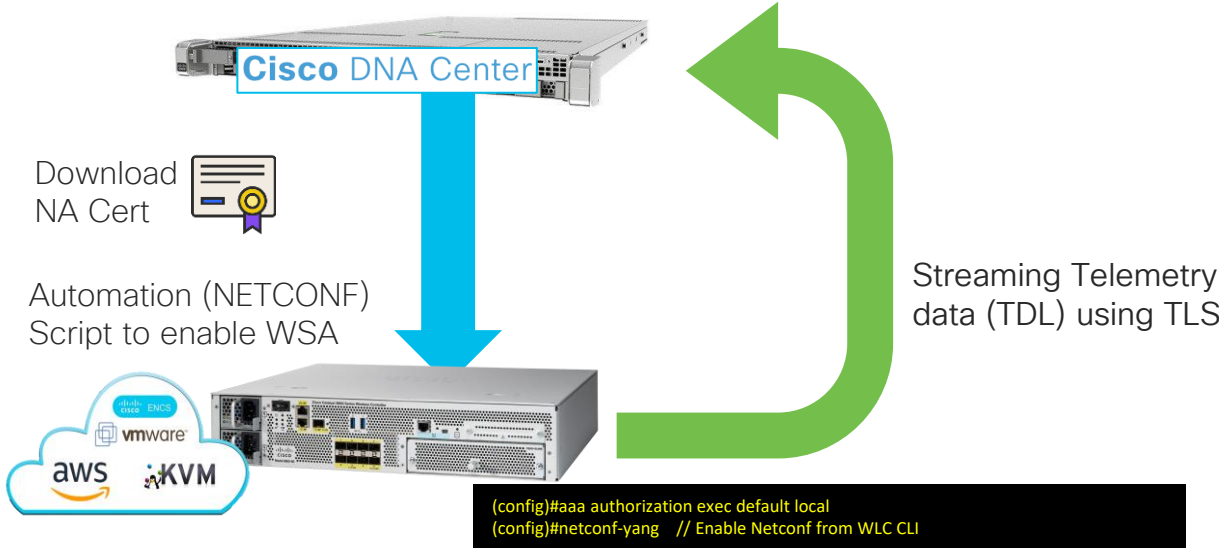
```
crypto pki trustpoint DNAC-CA
  enrollment mode ra
  enrollment terminal
  usage ssl-client
  revocation-check crl
crypto pki certificate chain DNAC-CA
  <snip>
quit

device-tracking tracking
!
device-tracking policy IPDT_MAX_10
  limit address-count 10
  no protocol udp
  tracking enable
!
interface <ACCESS-INTERFACES>
  device-tracking attach-policy IPDT_MAX_10

ip http client source-interface Loopback0

snmp-server community <RO-COMMUNITY> RO
snmp-server community <RW-COMMUNITY> RW
```

# What happens when an C9800 WLC is added to Cisco DNA Center?





# Full device on-boarding process into DNA Center

Discovered

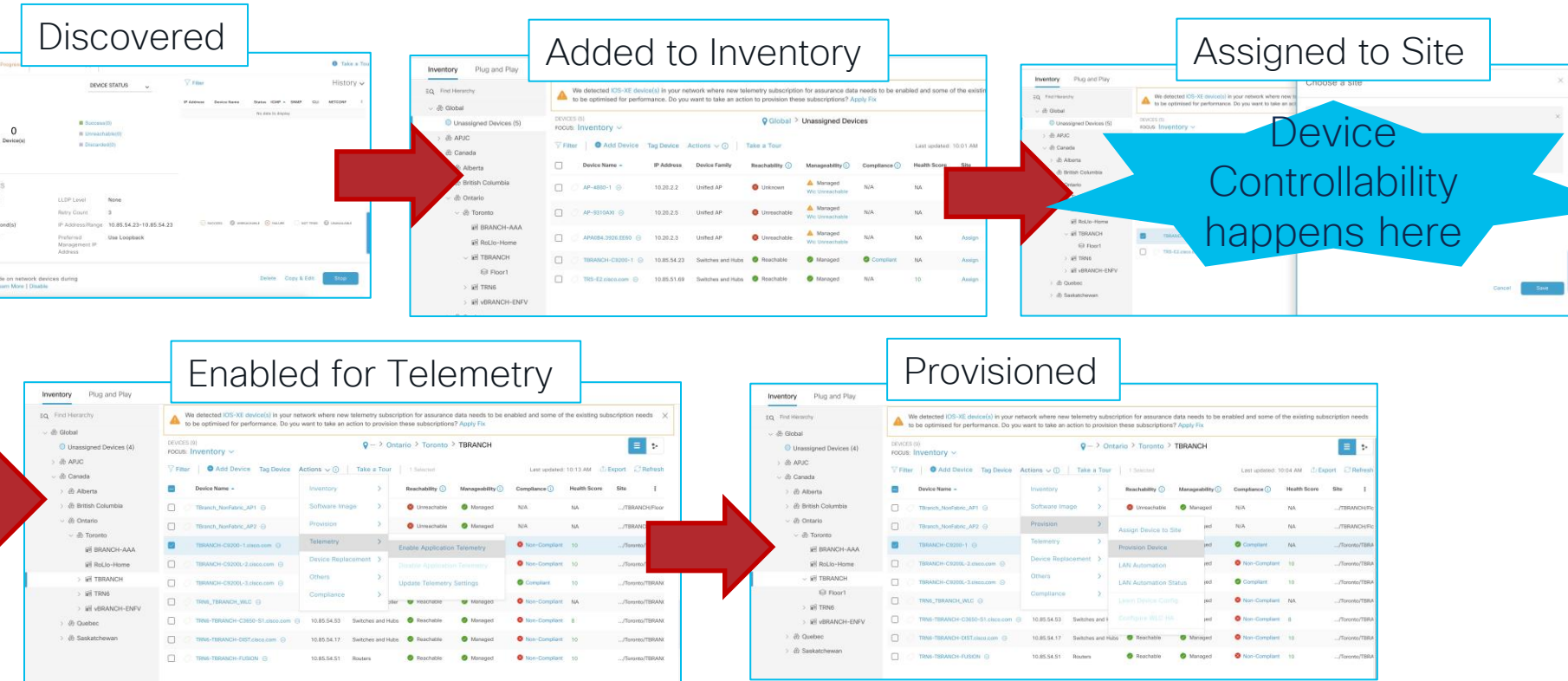
Added to Inventory

Assigned to Site

Device Controllability happens here

Enabled for Telemetry

Provisioned



# Adding a switch to DNA 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, a message states: "Device Controllability is Enabled. Learn More | Disable".

# Adding a switch to DNA Center – Assign to Site

The screenshot displays the Cisco DNA Center interface. The top navigation bar shows 'Cisco DNA Center' and 'Provision / Network Devices / Inventory'. The main content area is split into two panels. The left panel shows the 'Inventory' section with a search bar and a list of devices under 'Global'. The right panel is titled 'Assign Device to Site' and contains a dialog box with three radio buttons: 'Now', 'Later', and 'Generate configuration preview'. The 'Generate configuration preview' option is selected and highlighted with a red box. Below the radio buttons, there is a 'Task Name\*' field and a 'Configuration preview: Assign 1 Device(s) to 5' label. The bottom panel shows the 'Activities / Work Items' section with a search bar and a list of activities. The selected activity is 'Configuration preview: Assign/Unassign 1 Device(s) to/from Site', which is also highlighted with a red box. The activity details show the device name 'TBRANCH-C9200L-2' and a 'Configuration Preview' section containing the following configuration code:

```
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 nco:operation="remove" >
23-     <subscription-id>
24       <![CDATA[5531]]>
25     </subscription-id>
26   </mdt-subscription>
27- </mdt-config-data >
```

# 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

Global

Canada

Ontario

Toronto

BRANCH-AAA

Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when they 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 for 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 DNA 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 for configuring Telemetry settings at the site level. The breadcrumb navigation is "Design / Network Settings". The main navigation tabs include Network, Device Credentials, IP Address Pools, SP Profiles, Wireless, **Telemetry**, and Security and Trust. The left sidebar shows a search bar with "aaa" and a tree view with "Global", "Canada", "Ontario", "Toronto", and "BRANCH-AAA". The main content area has a description of Syslog, Traps, and NetFlow properties. A "NetFlow" section is expanded, showing a radio button option "Use Cisco DNA Center as NetFlow collector server" which is selected. Below this is a section for "INTERFACES FOR APPLICATION TELEMETRY" with instructions on enabling it and a radio button option "Add Cisco Telemetry Broker (CTB)".

**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 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

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.

# Device Controllability

## Site-level customization

The screenshot shows the Cisco DNA Center interface for configuring Telemetry settings at a site level. The breadcrumb navigation is "Design / Network Settings". The "Telemetry" tab is selected and highlighted with a red box. The left sidebar shows a search bar with "aaa" and a tree view with "Global", "Canada", "Ontario", and "Toronto" expanded, with "BRANCH-AAA" selected. The main content area is divided into sections:

- Telemetry** (highlighted with a red box):
  - 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** (highlighted with a red box):
  - 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** (highlighted with a red box):
  - 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**

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

The screenshot shows the Cisco DNA Center interface for monitoring device discoverability. The top navigation bar includes tabs for Monitoring, Settings, Telemetry, and Trust. The main content area is titled 'Discovery > Add' and shows a search for 'C9200-L-1' with a status of 'Completed' and '1 Reachable Device(s)'. A central summary card displays '1 Device(s)' in a green circle. To the right, a table lists the discovered device with the following details:

IP Address	Device Name	Status	ICMP	SNMP	CLI	NETCONF
10.85.54.23	TBRANCH-C9200-1	Success	Success	Success	Success	Success

Discovery Details:

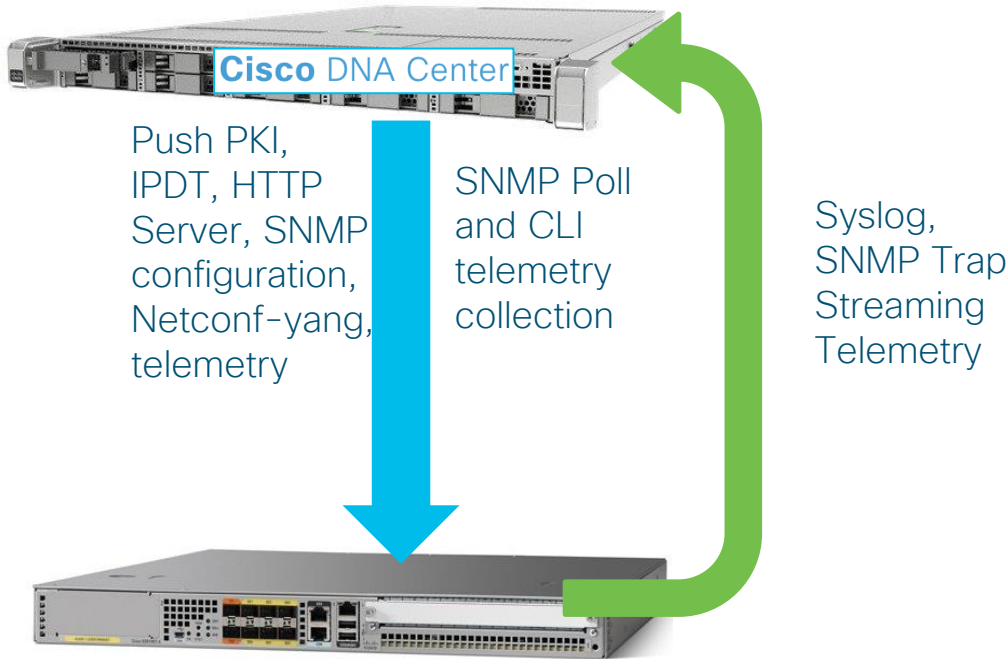
- CDP Level: None
- LLDP Level: None
- Protocol Order: ssh
- Retry Count: 3
- Timeout: 5 second(s)

At the bottom, a status bar indicates 'Device Controllability is Enabled' and provides buttons for 'Delete', 'Copy & Edit', and 'Re-discover'.

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

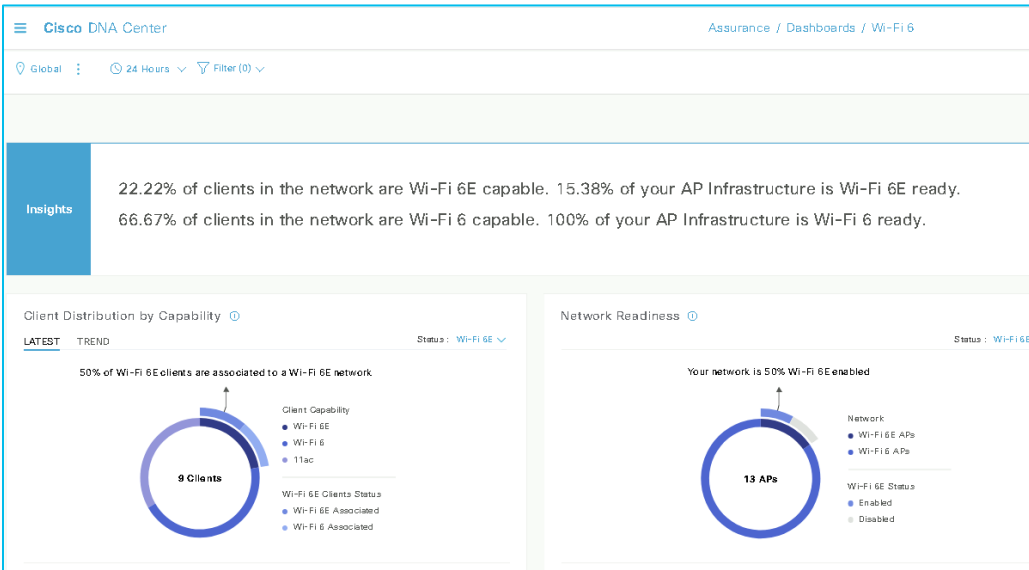


# Benefits of Telemetry data captured via DNA Center



- Monitor Network Network and Client Health
- Monitor Application Health
- Monitor Network Services
- View and Manage Issues
- Monitor Wi-Fi 6 Readiness
- Monitor Power over Ethernet
- EoX Insights
- Observe Network Trends and Gain Insights

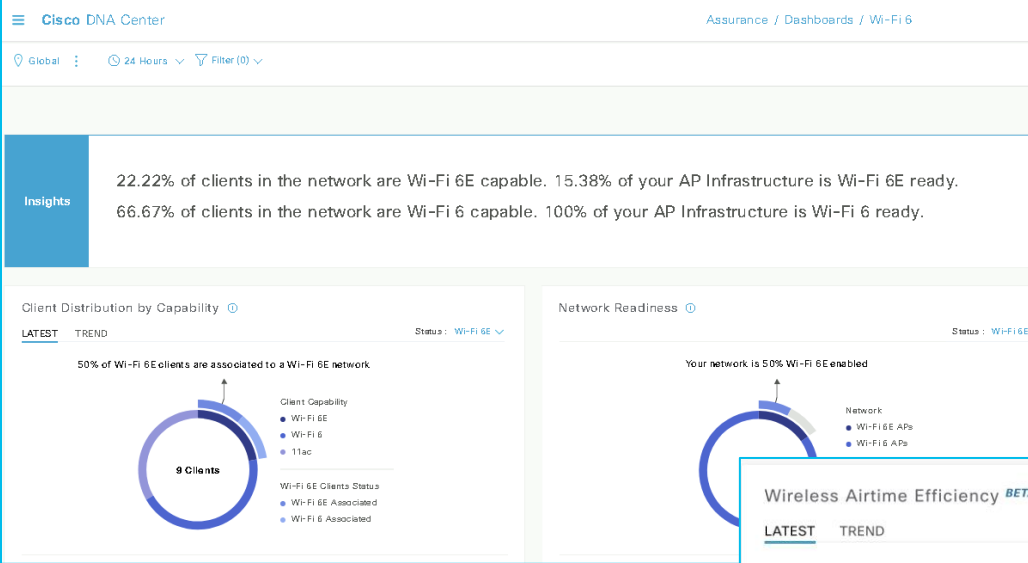
# Wi-Fi 6 Readiness Dashboard



## Key Use Cases:

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

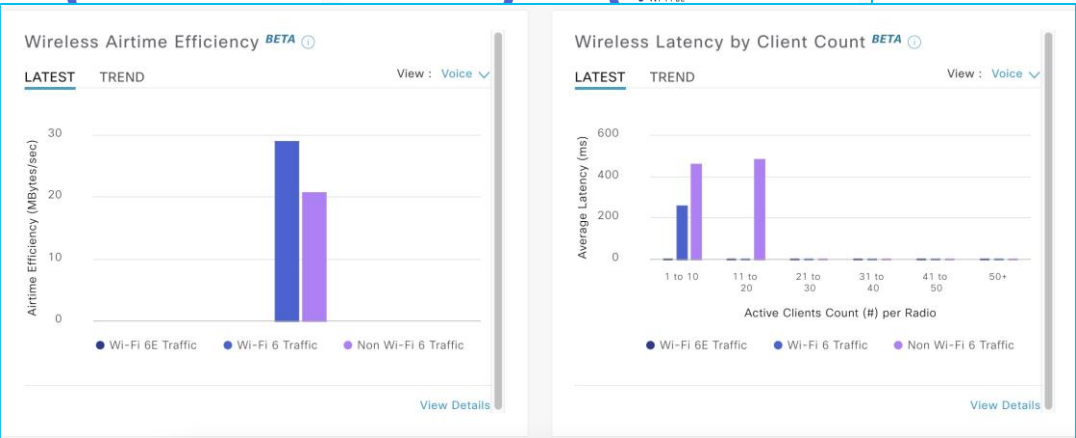
# Wi-Fi 6 Readiness Dashboard



**Key Use Cases:**

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

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



# Wi-Fi 6 Readiness Dashboard



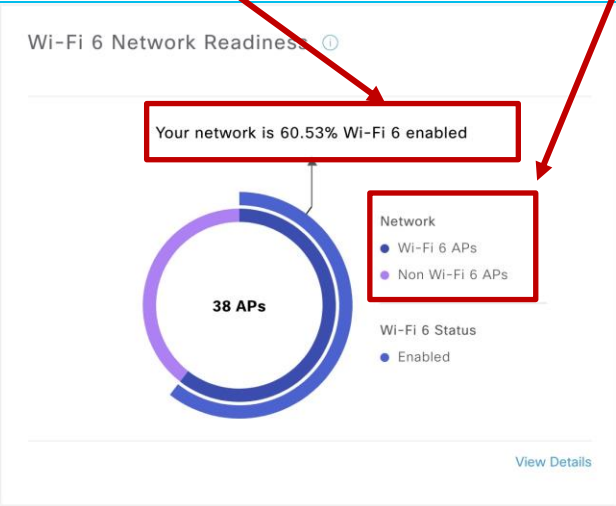
For your reference

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

Percentage of AP's Wi-Fi 6 enabled

Percentage of AP's Wi-Fi 6 capable

Wi-Fi version distribution



# Power over Ethernet Analytics

Insights

PoE Telemetry is available on Cisco Catalyst 9200, 9200/L, 9300, 9300/L, 9400, and 3850 platforms with minimum IOS-XE 16.12.3s and 17.3 software versions. To enable PoE subscription on these platforms, make sure that the Netconf port is enabled when you discover these devices.

### PoE Operational State Distribution

LATEST TREND

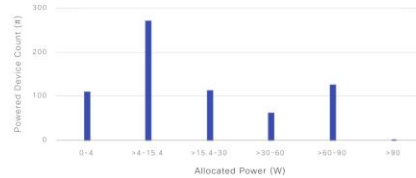


View Details

### PoE Powered Device Distribution

LATEST TREND

Allocated Power



View Details

### PoE Insights

Perpetual PoE

591/675 (88%) of powered devices are not enabled for Perpetual PoE.

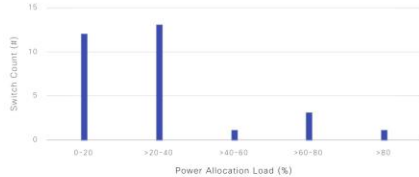


View Details

### Power Allocation Load Distribution

LATEST TREND

1/30 (3%) of switches have >80% load.



View Details

### PoE Power Allocation

LATEST TREND



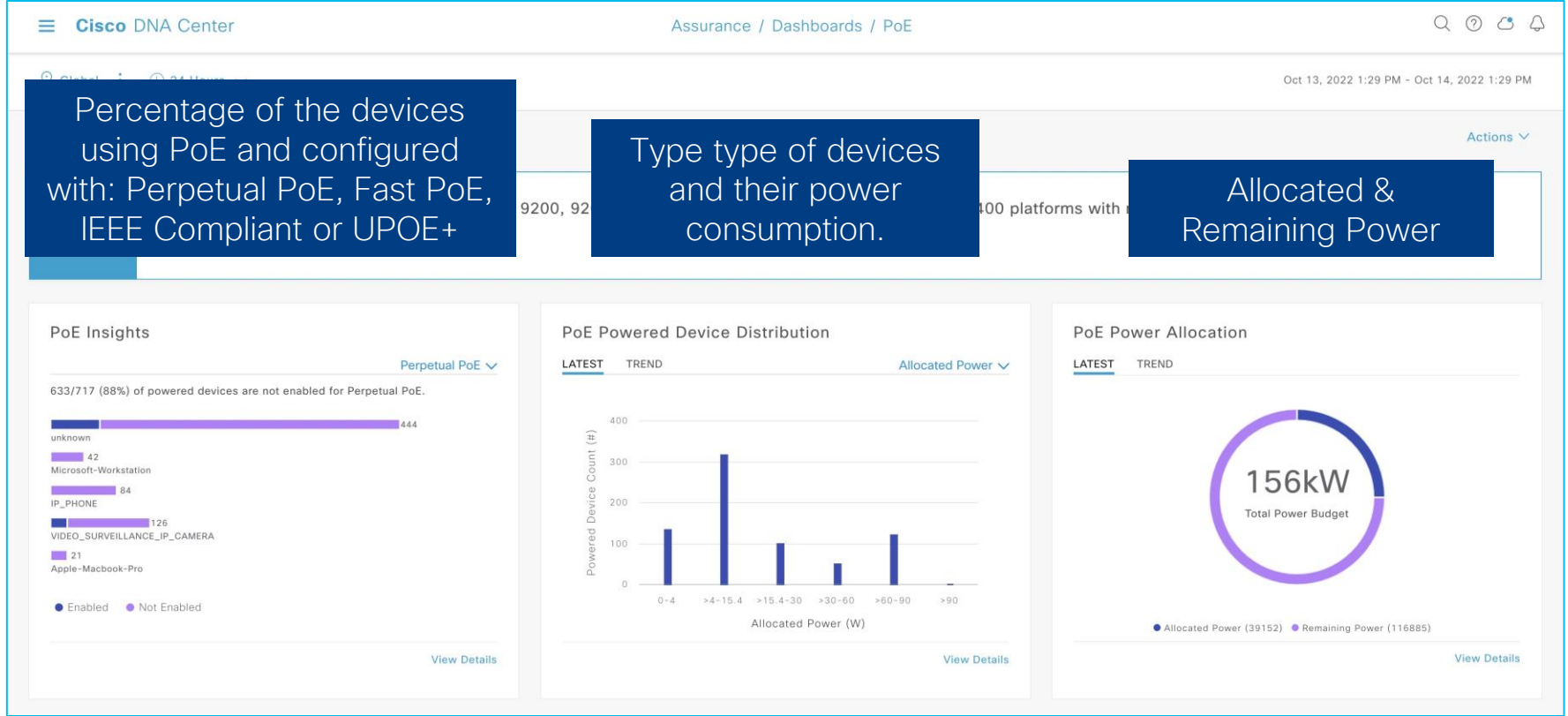
View Details

## Key Use Cases:

Full Visibility on PoE infrastructure

Dedicated PoE Issue Types

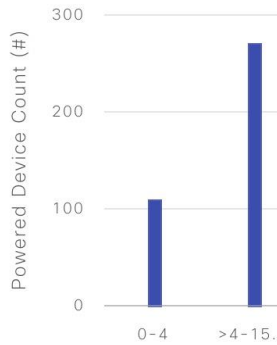
# Power over Ethernet Analytics



# 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

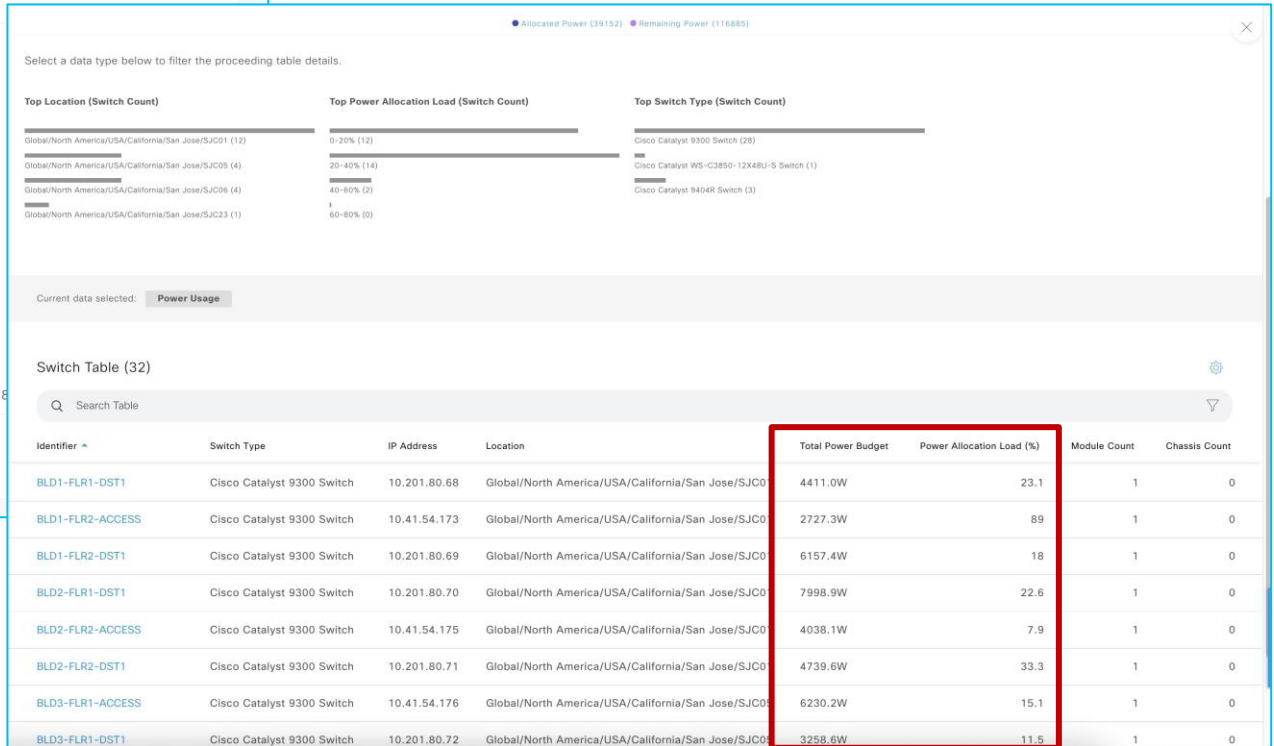
Search Table

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

# Power over Ethernet Analytics

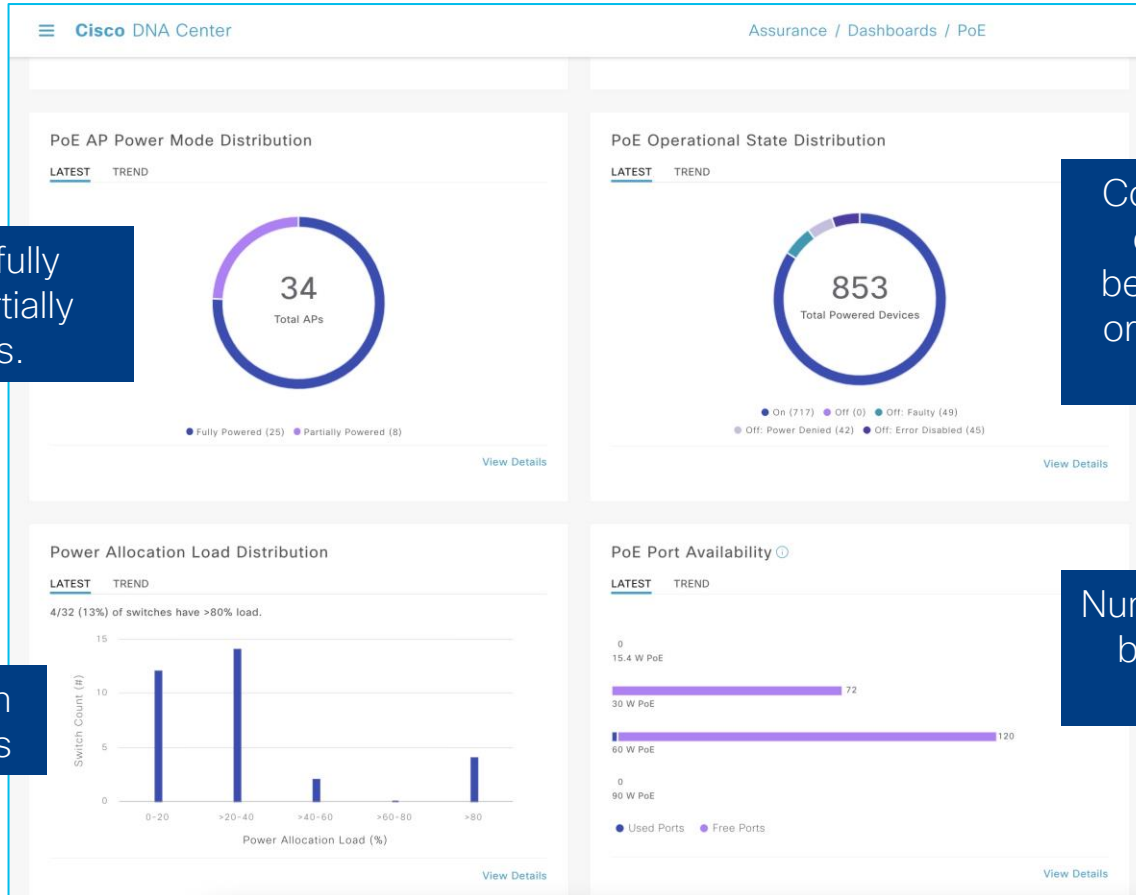
## PoE Power Allocation

LATEST TREND





# Power over Ethernet Analytics



Distribution of fully powered vs partially powered APs.

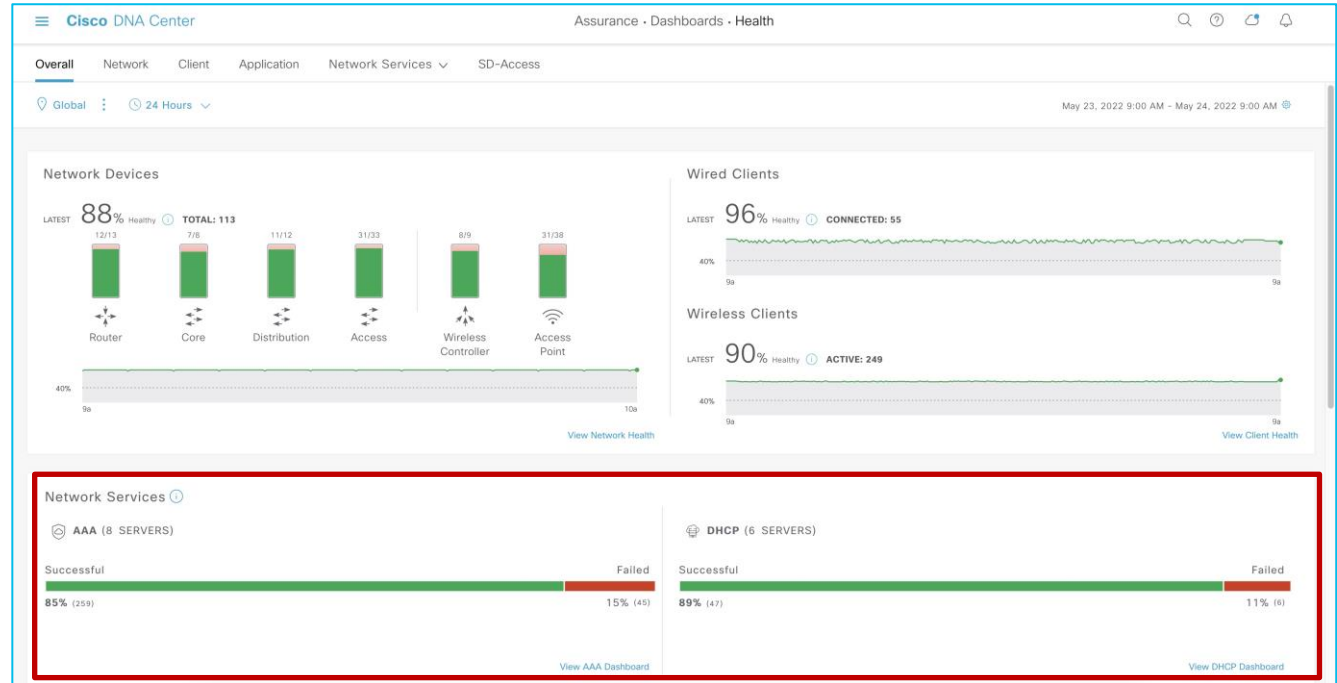
Count of devices based on whether they are being supplied with PoE or not. If not, a reason is provided

Power Allocation load and insights

Number of ports available based on their power load for PoE.

# Network Services Analytics

- Network Services Analytics to improve user Onboarding experience
- Quickly view and monitor AAA and DHCP transactions



# Network Services Analytics

DHCP SUMMARY		DHCP TRANSACTIONS		
6	210ms <small>-11.11%</small>	53 <small>+54.55%</small>	47 <small>+54.55%</small>	6
Servers	Average Latency	Total	Successful	Failed

## Top Sites by Highest Latency



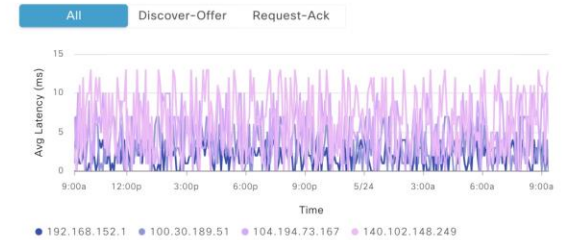
[View Details](#)

## Top Sites by Transaction Failures



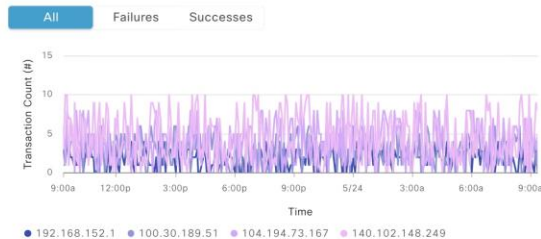
[View Details](#)

## DHCP Server Latency



[View Details](#)

## DHCP Server Transactions



Identify sites with potential AAA/DHCP issues using dashlets' details for **highest latency** and **highest number of transaction failures**

# Network Services Analytics

- See 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

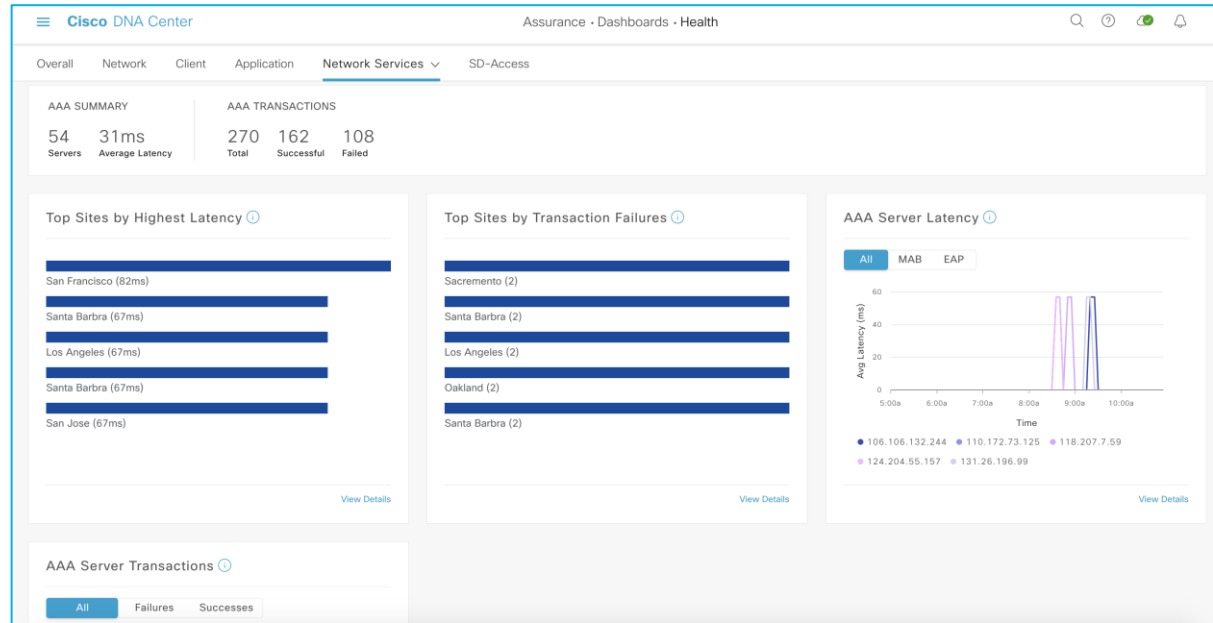
## DHCP Servers By WLC (6)

Search Table Export

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

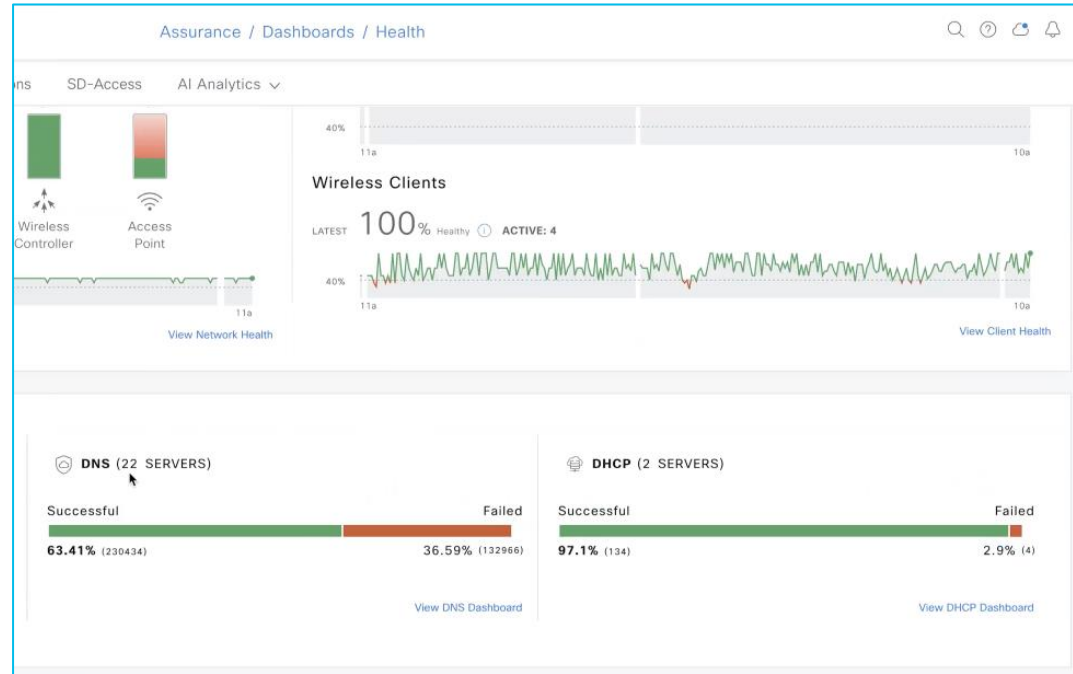
- Supported for wireless only
- IOS-XE 17.6.1 version or higher
- Not supported for AireOs controllers
- Local DHCP on 9800 not supported
- All transaction and server information is provided by the WLC directly
- WLC TDL subscriptions:
  - AAA -> 4321
  - DHCP -> 4322



# New in 2.3.5: Network Services DNS

- Monitor DNS server transactions reported by wireless controllers, switches, and routers
- Servers and Average Latency
- View all Successful and Failed Transactions
- Enable via Application Telemetry

```
flow monitor avc_ipv4_assurance_dns |
exporter avc_exporter |
exporter avc_local_exporter |
cache timeout active 60
record wireless avc_ipv4_assurance-dns
!
flow monitor avc_ipv6_assurance_dns
exporter avc_exporter
exporter avc_local_exporter
cache timeout active 60
record wireless avc_ipv4_assurance-dns
!
flow exporter avc_exporter
destination 10.79.59.28
source Vlan13
transport udp 6007
export-protocol ipfix
option vrf-table timeout 300
option ssid-table timeout 300
option application-table timeout 300
option application-attributes timeout 300
!
```



# Network Services DNS



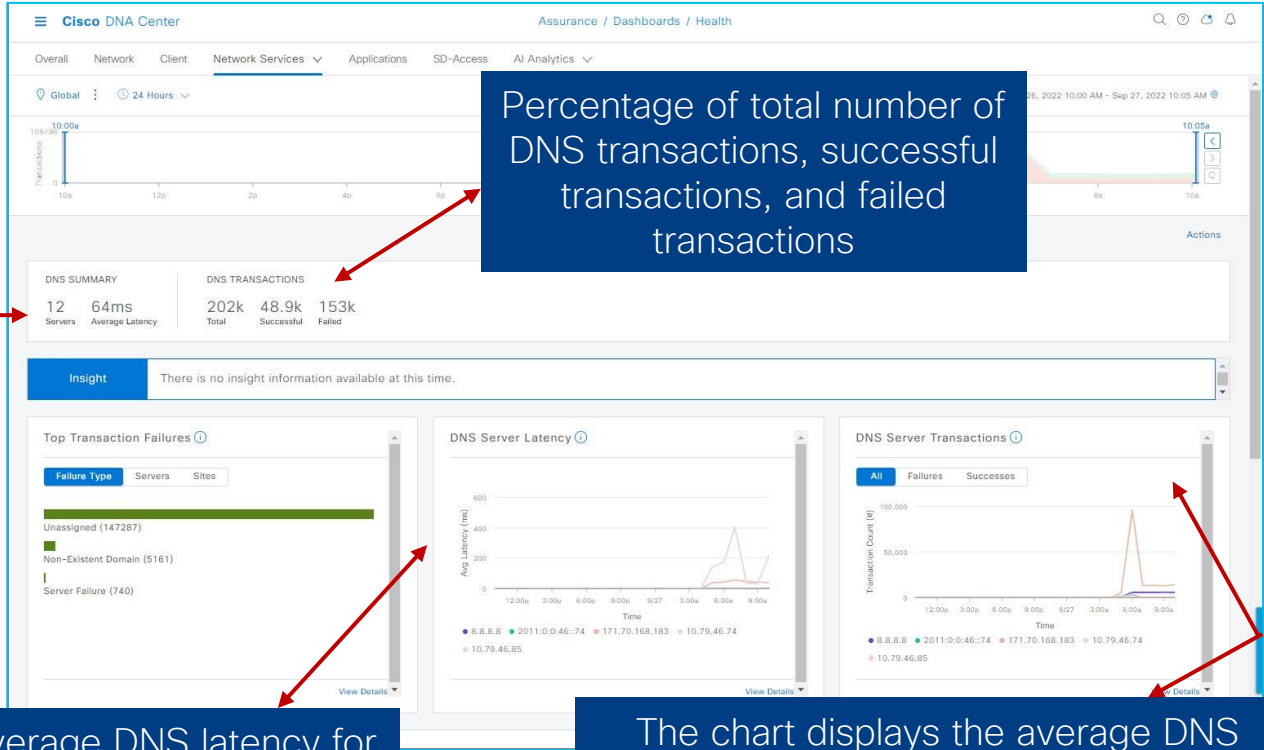
Count of DNS servers and average latency (in ms) of your network.

Top DNS server transaction failure types, servers, and sites

Average DNS latency for each DNS server.

Percentage of total number of DNS transactions, successful transactions, and failed transactions

The chart displays the average DNS server transactions status for each DNS server reported by wireless controllers.



# Network Services – DNS Dashboard



DNS Servers By Device (28) Export

Search Table

DNS Server IP	Device Name	Device Location	Device Family	Transactions	Failures	Avg Latency (ms)
8.8.8.8	C9300-79-59-5.assurance.com	Global/San Jose/BLD10/2F	Switches and Hubs	99808	99808	0.00
10.79.46.85	C9300-79-59-5.assurance.com	Global/San Jose/BLD10/2F	Switches and Hubs	12412	12412	0.00
1.14.61.51	eWLC-179.assurance.com	Global/eWLC-Area/eWLC-Building/eWLC-Floor	Wireless Controller	1	0	0.00
8.8.4.4	eWLC-1181303	Global/Shanghai/SHN15/4F	Wireless Controller	3	0	0.00
114.114.114.114	eWLC-179.assurance.com	Global/eWLC-Area/eWLC-Building/eWLC-Floor	Wireless Controller	36	0	0.00
114.67.102.75	eWLC-179.assurance.com	Global/eWLC-Area/eWLC-Building/eWLC-Floor	Wireless Controller	1	0	0.00
202.12.97.45	eWLC-179.assurance.com	Global/eWLC-Area/eWLC-Building/eWLC-Floor	Wireless Controller	1	0	0.00

View DNS servers by location, failures, and latency for a specific device.



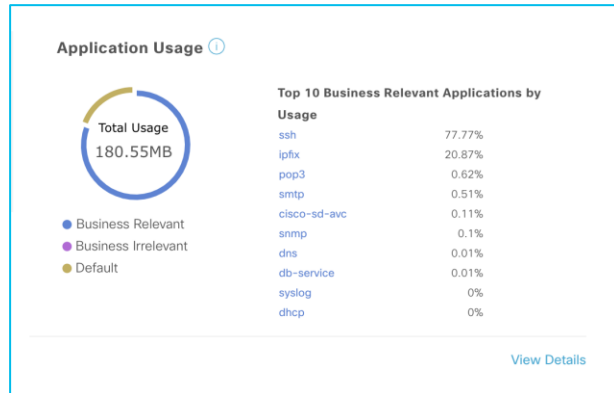
# Application Visibility vs Application Experience

## How Much = quantitative

- Supported on C9k switches
- 17.3.1 supported with ETA
- AirOS WLC
- 9800 WLC – flex

## How Good = qualitative (health)

- Supported on routers IOS-XE
- 9800 WLC– local mode



Application (18) Feb 20, 2021 6:55 AM

Filter: Business Relevant, Business Irrelevant, Default, HTTP, FTP, POP, SMTP, Unknown

Name	Health	Business Relevance	Usage	Average Throughput	Packet Loss (%)	Network Latency	jitter
ssh	10	Business Relevant	113.32MB	3.17Mbps	0	18 ms	---
ssh-afac.adam@cc.com	10	Default	33.15MB	927.02Kbps	0	3 ms	---
ipfix	---	Business Relevant	30.41MB	801.48Kbps	---	---	---
pop3	10	Business Relevant	616.05KB	12.54Kbps	0	1 ms	---
ftp-data	10	Default	893.7KB	24.4Kbps	0	0 ms	---
smtp	10	Business Relevant	708.01KB	20.97Kbps	0	1 ms	---
ftp	10	Default	496.46KB	13.59Kbps	0	2 ms	---

DNA Center 2.1.2 supports auto interface/WLAN selection

# Telemetry cheat sheet



For your  
reference

## How Much = quantitative

APV – application performance visibility

Switches 16.10 or 17.3 for ETA+

AireOS WLC 8.8.114 – central

9800 WLC 16.12.1 – central

## How Good = qualitative (health)

APM – application performance monitor

Routers. 17.3 optimized APM

Appliance 17.3 optimized APM

9800 WLC 17.3 optimized APM central  
(with DNAC 2.1.2)

Note: Optimized APM increases performance. no DSCP marking – observed and expected values

#3 SWIM to do software upgrades

# Configuration pushed (1/2)



For your  
reference

```
flow exporter avc_exporter
destination 10.10.10.181
source Vlan10
transport udp 6007
export-protocol ipfix
option vrf-table timeout 300
option ssid-table timeout 300
option application-table timeout 300
option application-attributes timeout 300
exit
```

```
flow exporter avc_local_exporter
destination local wlc
exit
```

```
flow monitor avc_ipv4_assurance
exporter avc_exporter
exporter avc_local_exporter
cache timeout active 60
default cache entries
record wireless avc ipv4 assurance
exit
```

```
flow monitor avc_ipv6_assurance
exporter avc_exporter
exporter avc_local_exporter
cache timeout active 60
default cache entries
record wireless avc ipv6 assurance
exit
```

```
flow monitor avc_ipv4_assurance_rtp
exporter avc_exporter
cache timeout active 60
default cache entries
record wireless avc ipv4 assurance-rtp
exit
```

```
flow monitor avc_ipv6_assurance_rtp
exporter avc_exporter
cache timeout active 60
default cache entries
record wireless avc ipv6 assurance-rtp
exit
```

# Configuration pushed (2/2)



For your  
reference

```
wireless profile policy hk_Global_NF_a38f71c1
shutdown
ipv4 flow monitor avc_ipv4_assurance input
ipv4 flow monitor avc_ipv4_assurance output
ipv4 flow monitor avc_ipv4_assurance_rtp input
ipv4 flow monitor avc_ipv4_assurance_rtp output
ipv6 flow monitor avc_ipv6_assurance input
ipv6 flow monitor avc_ipv6_assurance output
ipv6 flow monitor avc_ipv6_assurance_rtp input
ipv6 flow monitor avc_ipv6_assurance_rtp output
no shutdown
exit
```

```
wireless profile policy default-policy-profile
shutdown
ipv4 flow monitor avc_ipv4_assurance input
ipv4 flow monitor avc_ipv4_assurance output
ipv4 flow monitor avc_ipv4_assurance_rtp input
ipv4 flow monitor avc_ipv4_assurance_rtp output
ipv6 flow monitor avc_ipv6_assurance input
ipv6 flow monitor avc_ipv6_assurance output
ipv6 flow monitor avc_ipv6_assurance_rtp input
ipv6 flow monitor avc_ipv6_assurance_rtp output
no shutdown
exit
```

# Habit #3 – Compliance and Configuration management

# Cisco DNA Center Compliance Landscape

The screenshot shows the Cisco DNA Center interface for a device named C9K-STACK. The main area displays a 'Compliance Summary' with several violation cards:

- Network Settings:** Non-Compliant since Dec 13th, 2022, 09:33:23 AM. Compliance last run on: Dec 13th, 2022, 09:33:23 AM. 2 Open Violations.
- EoX - End of Life:** Compliance last run on: Dec 13th, 2022, 09:33:23 AM. Module: Compliant, Software: Compliant, Hardware: Compliant.
- Startup vs Running Configuration:** Compliance last run on: Dec 13th, 2022, 09:33:22 AM. 36 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: Dec 13th, 2022, 09:33:23 AM. 2 Open Violations.
- Application Visibility:** Compliant since Dec 13th, 2022, 09:33:40 AM. Compliance last run on: Dec 13th, 2022, 09:33:40 AM. 0 Open Violations.
- Software Image:** Compliant since Nov 17th, 2022, 12:35:00 PM. Compliance last run on: Dec 13th, 2022, 09:33:22 AM. 17.09.02 Golden Image Version. Running Version: 17.9.2. Stack Member Status: Up to Date.
- Critical Security Advisories:** Compliant since Oct 14th, 2022, 11:38:16 AM. Compliance last run on: Dec 13th, 2022, 09:33:22 AM. 0 Open Violations.

Annotations in blue boxes with red arrows point to specific features:

- End of Sale & End of Life alerts:** Points to the EoX - End of Life 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 DNA Center:** Points to the Network Profiles card.
- Difference in network settings compared to "Network Settings" in Design:** Points to the Network Settings 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.
- Check whether the devices are running without critical security vulnerabilities:** Points to the Critical Security Advisories card.

# 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

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  
Golden Image Version: 17.06.03  
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
		Version	Version Mismatch
		Stack Member Number	3
		Role	MASTER
		Version	17.07.01
		Stack Member Number	2
		Role	STANDBY
		Version	17.07.01
		Stack Member Number	1

# Compliance: Network Profiles - Switches

The screenshot displays the Cisco DNA Center interface for a switch named 'C9K-BRANCH-STACK'. The top navigation bar shows the device name and a 'Run Commands' button. Below this, the device's status is shown as 'Reachable' and 'Managed', along with its IP address (10.85.54.54), device model (Cisco Catalyst 9300 Switch), role (ACCESS), uptime (122 days 23 hrs 9 mins), and site (Global/Canada/Ontario/Toronto/TBRANCH).

The main content area is titled 'Compliance Summary' and includes a 'Run Compliance Check' button. It displays four compliance cards:

- Startup vs Running Configuration:** Shows a 4-minute sync delay with 0 lines added, 1 removed, and 0 modified.
- Network Profiles:** Highlighted with a red box, it shows a non-compliant state with 1 change in the CLI Template.
- Software Image:** Shows the device is compliant with the 17.08.01 Golden Image Version and the running version is 17.8.1.
- Critical Security Advisories:** Shows the device is compliant with 0 advisories.

A left-hand sidebar contains navigation options for 'DETAILS' (Interfaces, Ethernet Ports, Native VLANs, Hardware & Software, Configuration, Power, Fans, SFP Modules, User Defined Fields, Config Drift, Stack) and 'SECURITY' (Advisories).



# Compliance: Network Profiles - Switches

Config pushed by DNA Center via templates:

```
interface GigabitEthernet1/0/7
  description Description pushed by DNAC Template -- lan
!
interface GigabitEthernet1/0/8
  description Description pushed by DNAC 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 DNA Center interface for a device named C9K-BRANCH-STACK. The device status is Reachable and Managed. The interface shows a Compliance Summary for Network Profiles, specifically for a CLI Template (1). The table below shows the CLI deviations, with some rows highlighted in red to indicate missing CLIs.

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

# Config Drift

The screenshot displays the 'Configuration Changes' page in Cisco DNA Center. On the left is a navigation menu with 'Config Drift' highlighted. The main content area shows configuration changes saved on the internal Cisco DNA Center server. It indicates that 15 config drifts and 1 labelled config will be saved. A 'Change History' section shows a date range from Sep 30, 2022, to Oct 15, 2022. A line graph plots the number of lines over time, with a legend for In-band Config Drift (blue), Out-of-band Config Drift (purple), and Labelled Config (orange). A dropdown menu shows the selected 'Config Drift Version' as 'CCA\_C9K-TBRANCH-Std-Config'. Below this, two columns of configuration lines are shown: 'Running Config (461 Lines)' and 'Running Config (784 Lines)'. A red box highlights a specific configuration change in the second column, labeled as an 'Out-of-band Config Drift'. A callout box provides details for this drift, including the number of lines added (322), removed (0), and modified (0), along with the triggered event and terminal information.

Ethernet Ports  
VLANs  
Hardware & Software  
Configuration  
Power  
Fans  
SFP Modules  
User Defined Fields  
**Config Drift**  
REP Rings  
Stack  
SECURITY  
Advisories  
COMPLIANCE  
Summary

Configuration changes on your device will be saved on the internal Cisco DNA Center server. The number of configuration drifts saved (as set in System > Settings > Device Settings > Configuration Archive) will include labelled configs and config drift versions.

Total config drifts being saved: 15    Total labelled configs: 1

Change History (Running Config)

Config Drift Date Range:    Start Date    End Date  
                                         Sep 30, 2022    Oct 15, 2022

No. of Lines

Config Drift Days

● In-band Config Drift    ● Out-of-band Config Drift    ● Labelled Config

Config Drift Version  
CCA\_C9K-TBRANCH-Std-Config    Remove Label    Edit

Running Config (461 Lines)

```
17 switch 1 provision c9300-24p
18 switch 2 provision c9300-24p
19 ip routing
20 ip name-server 64.102.6.247 173.37.137.85
21 ip domain lookup source-interface Loopback0
22 login on-success log
23 vtp mode transparent
```

Running Config (784 Lines)

```
17 switch 1 provision c9300-24p
18 switch 2 provision c9300-24p
19 ip routing
20 ip nbar http-services
21 ip name-server 64.102.6.247 173.37.137.85
22 ip domain lookup source-interface Loopback0
23 login on-success log
24 vtp mode transparent
25 avc sd-service
26 segment AppRecognition
27 controller
28 address 10.85.54.177
29 destination-ports sensor-exporter 21730
30 ustp 16
```

Out-of-band Config Drift

Config version with changes made outside of Cisco DNA Center since it's previous version.

Lines Added: 322  
Lines Removed: 0  
Lines Modified: 0  
Triggered By: Config Change Event  
Terminal Name: vty2  
Login IP: 10.24.150.225  
Username: lila  
Config Method: console

October 14, 2022 11:48 AM

# 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**

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

- Startup vs Running Configuration** (Info)
  - 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** (Info) Non-Compliant since Feb 9th, 2022, 02:38:20 AM
  - Compliance last run on: Apr 2nd, 2022, 11:16:36 AM
  - 3 Changes [+1 more](#)
  - Model Config: 1
  - Wireless: 1
- Application Visibility** (Info)
  - Compliant since Apr 2nd, 2022, 11:16:54 AM
  - Compliance last run on: Apr 2nd, 2022, 11:16:54 AM
  - 0 Changes
- Software Image** (Info)
  - 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** (Info)
  - 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

The screenshot displays the Cisco DNA Center interface for a specific device, STL01-C9800-CL.dlab.local. The breadcrumb navigation shows 'All Devices / STL01-C9800-CL.dlab.local'. The device status is 'Reachable' and 'Managed', with an IP address of 172.16.255.35 and a role of 'ACCESS'. The device model is 'Cisco Catalyst 9800-CL Wireless Controller for Cloud'. The left sidebar shows navigation options under 'DETAILS', 'SECURITY', and 'COMPLIANCE', with 'Summary' selected under 'COMPLIANCE'. The main content area is titled 'Compliance Summary / Network Profiles' and shows 'CLI Template (1)', 'Model Config (1)', and 'Wireless (1)'. A red box highlights the 'CLI Template (1)' link. Below this, the 'CLI Deviations' section shows a table with one record: 'Enabling SI'. The 'Realize Template: Enabling SI' section shows a table with two records: 'ap dot11 24ghz SI' and 'ap dot11 5ghz SI'.

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)

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

**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
Wlan/BestCorpWi_Global_NF_e5f0c407	FT Adaptive	Changed	Adaptive	Disabled

Showing 1 of 1

# Compliance: Network Profiles - Wireless

The screenshot displays the Cisco DNA Center interface for a device named 'STL01-C9800-CL.dlab.local'. The breadcrumb navigation shows 'Compliance Summary / Network Profiles'. A red box highlights the 'Model Config (1)' link. Below this, a table lists compliance violations. The table has columns for Model Name, Attribute, Status, Intended Value, and Actual Value. One violation is shown: 'Policy\_Profile/BestCorpWi\_Global\_NF\_e5f0c407' with the attribute 'IPv4 DHCP Required', a status of 'Changed', an intended value of 'YES', and an actual value of 'NO'. The table footer indicates 'Showing 1 of 1'.

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

# New in DNA Center 2.3.5

## Network Setting Compliance

```
[C9K-STACK#show run | i name-server
ip name-server 64.102.6.247 173.37.137.85
[C9K-STACK#conf t
Enter configuration commands, one per line. End with CNTL/Z.
[C9K-STACK(config)#no ip name-server 64.102.6.247 173.37.137.85
```

All Devices / C9K-STACK

C9K-STACK Run Comm

Reachable Managed IP Address

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 / Network Settings [View Preference for Acknowledged Violations](#)

General (2)

Search Table

Open Violations (2) Acknowledged Violations (0)

0 Selected [Acknowledge](#)

<input type="checkbox"/>	Model Name	Attribute	Status	Intended Value	Actual Value	Action
<input type="checkbox"/>	DNS NR Settings	nameServers	Changed	64.102.6.247	-	<a href="#">Acknowledge</a>
<input type="checkbox"/>	DNS NR Settings	nameServers	Changed	173.37.137.85	-	<a href="#">Acknowledge</a>

Showing 2 of 2

# New in 2.3.5

## Fix Config Compliance Issues

The screenshot shows the Cisco DNA Center interface for a device named C9K-STACK. The left sidebar contains navigation options: DETAILS, Interfaces, Hardware & Software, Configuration, Power, Fans, SFP Modules, User Defined Fields, Config Drift, REP Rings, Stack, SECURITY, Advisories, and COMPLIANCE. The COMPLIANCE section is expanded to show a 'Summary' view. The main content area displays a 'Compliance Summary' for the device, indicating that the next compliance check is scheduled for Jan 17, 2023, at 02:50 PM. Below this, there are four compliance issue cards: 'EoX - End of Life' (Compliant), 'Network Settings' (2 violations), 'Network Profiles' (1 violation), and 'Application Visibility' (Compliant). Each card shows the last run time and a link to 'Open Violations'.

The dialog box titled 'Fix Configuration Compliance Issues' provides instructions and options for fixing compliance issues. It states that 3 compliance issues are listed to be fixed and includes a note that Routing, HA Remediation, Software Image, Securities Advisories, and Workflow related issues will not be addressed. A 'Summary of Issues to be Fixed' section lists the following violations:

Compliance Type	Issues Identified
Network Profiles	1
Network Settings	2

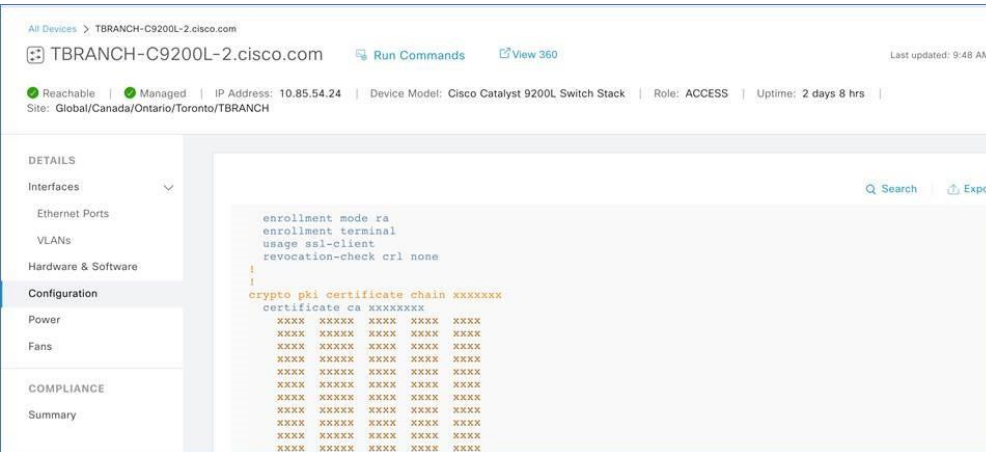
The 'Schedule the Fix' section asks 'When would you like to apply the fix?' with three radio button options: 'Now' (selected), 'Later', and 'Generate Preview'. The 'Generate Preview' option includes a sub-note: 'Creates preview which can be later used to deploy on selected devices. View status in Work Items'. Below this is a 'Task Name\*' field with the value 'C9K-STACK - Compliance Fix'. At the bottom right, there are 'Cancel' and 'Apply' buttons.



# 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 has to be provisioned by Cisco DNA Center

# Device Configuration Management



The screenshot shows the Cisco DNA Center interface for a specific device. The breadcrumb navigation is 'All Devices > TBRANCH-C9200L-2.cisco.com'. The device name is 'TBRANCH-C9200L-2.cisco.com' and it was last updated at 9:48 AM. Status indicators show it is 'Reachable' and 'Managed'. Key details include IP Address: 10.85.54.24, Device Model: Cisco Catalyst 9200L Switch Stack, Role: ACCESS, and Uptime: 2 days 8 hrs. The left sidebar shows navigation options like 'DETAILS', 'Interfaces', 'Ethernet Ports', 'VLANs', 'Hardware & Software', 'Configuration', 'Power', 'Fans', 'COMPLIANCE', and 'Summary'. The main content area displays the configuration for the 'crypto pki certificate chain' section, which is mostly masked with 'XXXX' characters. The visible configuration lines are:

```
enrollment mode ra
enrollment terminal
usage ssl-client
revocation-check crl none
!
crypto pki certificate chain XXXXXXXX
certificate ca XXXXXXXX
XXXX XXXXX XXXX XXXX XXXX
XXXX XXXXX XXXX XXXX XXXX
XXXX XXXXX XXXX XXXX XXXX
XXXX XXXXX XXXX XXXX XXXX
XXXX XXXXX XXXX XXXX XXXX
XXXX XXXXX XXXX XXXX XXXX
XXXX XXXXX XXXX XXXX XXXX
XXXX XXXXX XXXX XXXX XXXX
XXXX XXXXX XXXX XXXX XXXX
```

- DNA Center stores device configurations in the DNAC 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.

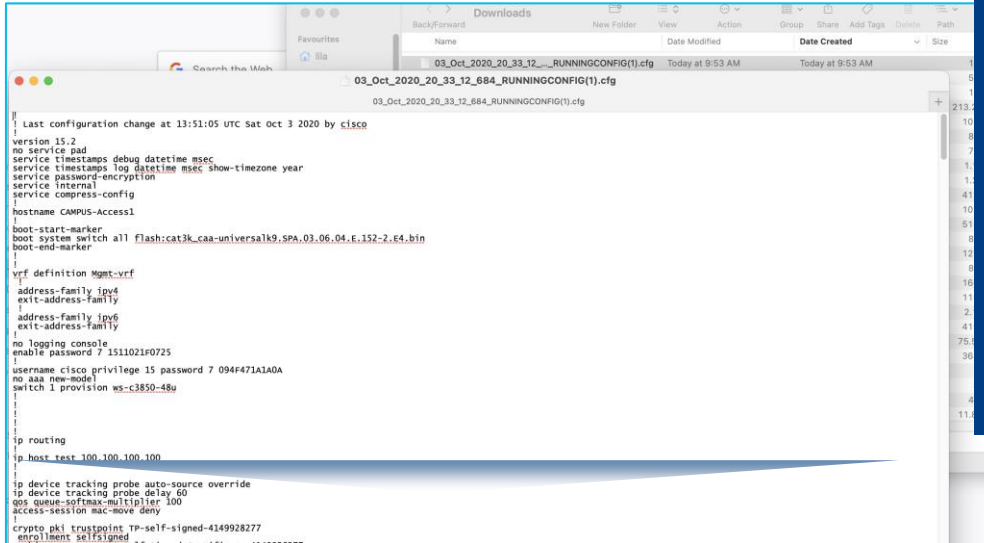
# Device Configuration Management

## API's to retrieve device configuration

- The API's available in DNAC allows you to retrieve raw startup, running configs and VLAN DB.

- API details:

- POST /network-device-archive/cleartext
- A zip file is generated which contains raw running-config, startup-config and VLAN DB



```
! 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 1511021f0725
!
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-softmax-multiplier 100
access-session mac-move deny
!
crypto pki trustpoint TP-self-signed-4149928277
enrollment selfsigned
```

# Device Configuration Management

## Configuration Archive

System / Settings

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	Daily Time 01:04 PM	Connected	

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

# Device Configuration Management

## Configuration Archive

The screenshots illustrate the workflow of archiving and extracting device configurations:

- Top-Left:** A file named "Export\_Configs-10\_Feb\_2022\_18\_04\_00\_353-oWF.zip" is selected in the Downloads folder.
- Top-Right:** The contents of the "Export\_Configs-10..." folder are shown, listing various configuration files such as "10.85.51.69-TRS-E2.cisco.com" and "10.85.54.17-TRN6-TBRANCH-DIST.cisco.com".
- Bottom-Left:** A dialog box prompts for a password to extract the zip file: "Please enter the password for 'Export\_Configs-10\_Feb\_2022\_18\_04\_00\_353-oWF.zip'." The password field is filled with dots.
- Bottom-Right:** The extracted files are shown in a folder named "10.85.54.54-C9K-...", including "10\_Feb\_2022\_18\_04\_00\_353\_RUNNINGCONFIG.cfg", "10\_Feb\_2022\_18\_04\_00\_353\_STARTUPCONFIG.cfg", and "10\_Feb\_2022\_18\_04\_00\_353\_vlan.dat.bat".

# 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 $9$slj/gvcAL9GF0U$k6/kumGDPS/ABbtHwK8xzqGeVEVvM3idf83ZIm4zH92
!
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 TC6-801
```

Habit #4 – Maintain network  
infrastructure code up to  
date with SWIM

# SWIM Demo



# What you need to know about SWIM

## Intent Based Network Upgrades



Golden-image driven to automate process and drive consistency

## Streamlined Upgrade Process



Upgrade base image, patches, ROMMON in one single flow. ISSU supported

## Trustworthiness Integration



Assures that device images are not compromised in any way.

## Upgrade Checks



Pre/Post check ensures updates do not have adverse effects on network

# Uncover software potential security vulnerabilities

The screenshot displays the Cisco DNA Center interface for Security Advisories. The main content area shows details for device TRN6\_C9800CL\_Fabric.cirrus.cloud (10.85.54.170), which is Reachable and has an uptime of 412 days 13 hrs 41 mins. A table lists 101 advisories, with three highlighted as Critical:

Advisory ID	Advisory Title	CVSS Score	Impact	Fixed Versions	CVE
<a href="#">cisco-sa-ewlc-capwap-rce-LYgj8Kf</a>	Cisco IOS XE Software for Catalyst 9000 Family Wireless Controllers CAPWAP Remote Code Execution Vulnerability	10	Critical	16.12.1w 16.12.5	CVE-2021-34770
<a href="#">cisco-sa-ioxPE-KgGvCAf9</a>	Cisco IOx for IOS XE Software Privilege Escalation Vulnerability	9.8	Critical	N/A	CVE-2020-3227
<a href="#">cisco-sa-aaa-Yx47ZT8Q</a>	Cisco IOS XE Software NETCONF and RESTCONF Authentication Bvoass	9.8	Critical	16.12.6 16.12.1z2	CVE-2021-1619

# Golden Images & Security Advisories

Find Hierarchy

Global

- APJC
- Canada
- RBC-Canada-Ontario
- US

Import | Update Devices | Show Tasks | Take a Tour

Physical | Virtual

Filter | Refresh | Last updated: 12:36 PM

Cisco.com ID: Iroussea@cisco.com (Not me?)

Family	Image Name	Device(s)	Version	Advisory	Golden Image	Device Role	Action
> Cisco 3504 Wireless LAN ...	AIR-CT3504-K9-S-10-105-0.aes Verified	1	5.0 (Latest) Add On (N/A)	0 Critical 0 High	★	ALL ★	
▼ Cisco Catalyst 9300 Switch	cat9k_iosxe.17.03.03.SPA.bin Verified	0	17.03.03 (Suggested) Add On (N/A)	5 High 2 Medi...	★	ALL ★	
	cat9k_iosxe.17.02.01.SPA.bin Verified	2	17.02.01 (Latest) Add On (N/A)	2 Critical 32 High	☆		<a href="#">View Advisory Details</a>
	Install Mode (16.9.2s.0.18)	2	16.9.2s Add On (N/A)	3 Critical 40 High	↓	ⓘ	
	Install Mode (16.12.1s.0.639)	1	16.12.1s Add On (N/A)	2 Critical 50 High	↓	ⓘ	
			16.11.1				

# Golden Images Recommendations

The screenshot displays the Cisco Prime Network Manager interface. The main window shows an 'Image Advisory' for 'Cisco Catalyst 9300 Switch' with version '17.02.01'. It lists 22 advisories: 2 Critical, 32 High, 22 Medium, 0 Low, and 0 Informational. A dialog box titled 'Image Update' is open, showing a table of advisories for the selected image 'cat9k\_iosxe\_npe.17.03.0...'. The table indicates 0 Critical, 5 High, 2 Medium, and 0 Low advisories. A 'Download / Mark Golden' button is highlighted in red. Another 'Fix Advisories' button is also highlighted in red in the background window.

Advisory Level	Count
Critical	2
High	32
Medium	22
Low	0
Informational	0

Advisory Level	Count
Critical	0
High	5
Medium	2
Low	0

Image Recommendations based on published PSIRT advisory

# Golden Image Tagging

The screenshot displays the Cisco Catalyst 9300 Switch image repository interface. The main content is a table of images with columns for Image Name, Version, Devices, and Advisories. A modal titled "Assign Device Roles & Tags" is open on the right, showing the selected image name and options for roles and tags. The modal is divided into two sections: "SELECTED DEVICE ROLES (0)" and "SELECTED DEVICE TAGS (0)".

**Table Data:**

Image Name	Version	Devices	Advisories
cat9k_iosxe.17.06.04.SPA.bin	(Suggested) Add On (1)	0	Critical High
cat9k_iosxe.17.08.01.SPA.bin Verified	17.08.01.0.1490 Add On (N/A)	0	0 Critical High
cat9k_iosxe.17.09.02.SPA.bin Verified	17.09.02.0.3040 (Latest) Add On (N/A)	0	0 Critical High
cat9k_iosxe_npe.16.12.08.SPA.bin	Gibraltar-16.12.8 (Latest) Add On (N/A)	0	3 High 1 Med
cat9k_iosxe_npe.17.03.05.SPA.bin	Amsterdam-17.3.5 (Suggested) Add On (N/A)	0	0 Critical High
cat9k_iosxe_npe.17.03.06.SPA.bin	Amsterdam-17.3.6 (Latest) Add On (1)	0	0 Critical High

**Assign Device Roles & Tags Modal:**

Image Name: cat9k\_iosxe.17.08.01.SPA.bin

In the following, manage the assignments of roles and tags for the selected image.

**SELECTED DEVICE ROLES (0)**  
Select the roles to assign below.

- Role: Unknown
- Role: Access
- Role: Border Router
- Role: Core
- Role: Distribution
- Role: All

**SELECTED DEVICE TAGS (0)**

Note: If any 'Device-tag' is selected for an image, it would take precedence over 'Role' across image versions for the same role.

Select from Available Tags

Select from Available Tags

- FabricBorder
- FabricEdge
- MyNewTag
- PORT\_SECURITY
- RBC
- Stack priority

# Outdated Software Images

**FILTERED BY**

Outdated Software Im... x

**DEVICE WORK ITEMS**

- Unreachable
- Unassigned
- Failed Provision
- Non Compliant
- Outdated Software Image**
- No Golden Image
- Under Maintenance
- Security Advisories
- Marked for Replacement
- System Beacon Enabled

**Devices (18)** Focus: Select v

Go to old page Take a tour Export

Filter devices

0 Selected Add Device Tag Actions v

As of: Dec 8, 2022 10:42

Device Name	IP Address	Device Family	Site	Software Image	Image Version
<input type="checkbox"/> TRN6-SDA-CAMPUS-B1.cirrus.cloud FabricBorder	10.85.62.102	Switches and Hubs	.../TRN6/TRN6-28-SELab	cat9k_iosxe.16.09.... Needs Update	16.9.2s
<input type="checkbox"/> TRN6-SDA-CAMPUS-B2.cirrus.cloud FabricBorder	10.85.62.103	Switches and Hubs	.../TRN6/TRN6-28-SELab	cat9k_iosxe.16.09.... Needs Update	16.9.2s
<input type="checkbox"/> TRN6-SDA-CAMPUS-E1.cirrus.cloud FabricEdge	10.85.62.106	Switches and Hubs (WLC Capable)	.../TRN6/TRN6-28-SELab	cat9k_iosxe.16.12.... Needs Update	16.12.3a
<input type="checkbox"/> CLG2-SDABRANCH-B.cirrus.cloud	10.85.62.186	Switches and Hubs (WLC Capable)	.../CLG2/CLG2-3	cat9k_iosxe.16.12.... Needs Update	16.12.1s
<input type="checkbox"/> CLG2-SDABRANCH-E.cirrus.cloud	10.85.62.187	Switches and Hubs	.../CLG2/CLG2-3	cat3k_caa-univers... Needs Update	16.9.4
<input type="checkbox"/> EDM02-SDABRANCH-B.cirrus.cloud	10.85.58.215	Switches and Hubs (WLC Capable)	.../EDM02/EDM02-8	cat9k_iosxe.17.02.... Needs Update	17.2.1

# Visibility into Non-Compliant Devices Inventory

- Device Dashboard helps in creating a filter for “Outdated Software Images”
- Inventory provides a filter to show devices which are Non-compliant

The screenshot displays the Cisco Inventory Management interface. At the top, there is a navigation bar with a menu icon, 'Global' location, and 'Provision / Inventory' page title. A notification banner at the top right states: 'To provision subscriptions on devices that have not been discovered with NETCONF, rediscover the devices with NETCONF, and update the Telemetry Settings with the Force Configuration Push option.' Below this, there are filter tabs for 'All', 'Routers', 'Switches', 'Wireless Controllers', 'Access Points', and 'Sensors'. The main content area is titled 'Devices (1) Focus: Inventory'. It features a search bar 'Filter devices' and a table of devices. The table has columns for 'Device Name', 'IP Address', 'Device Family', 'Reachability', 'EoX Status', 'Manageability', 'Compliance', and 'Health Score'. One device is listed: 'Cat9300-Stack-Switch' with IP '192.168.120.10', family 'Switches and Hubs (WLC Capable)', 'Reachable' status, '1 alert', 'Managed' status, and 'Non-Compliant' compliance status. On the left sidebar, under 'FILTERED BY', there are two active filters: 'Outdated Software Images' and 'Security Advisories'. Under 'DEVICE WORK ITEMS', there are several checkboxes, with 'Outdated Software Image' and 'Security Advisories' also checked and highlighted with a purple box.

# Control SWIM- Golden Image Tagging

- Image Repository provides options to mark devices as golden based on
  - Device Role
  - Device Tags
  - Sites
- Image Repository also provides visibility into advisories impacting a particular software version

The screenshot shows the Cisco Catalyst 9300 Switch Image Repository interface. The breadcrumb navigation is Design / Image Repository / Image Family. The page title is Cisco Catalyst 9300 Switch. The left sidebar shows a SUMMARY section with links to Roles & Tags (6), Major Versions (9), and Golden Images (2). The main content area displays a table of 16 images. The table has columns for Image Name, Version, Devices, Advisories, and Golden Image. A 'Device Roles & Tags' button is highlighted in a purple box. The table data is as follows:

Image Name	Version	Devices	Advisories	Golden Image
cat9k_iosxe.16.12.03a.SPA.bin Verified	16.12.3a.0.4 Add On (N/A)	0	1 Critical 30 High	☆
cat9k_iosxe.16.12.08.SPA.bin	Gibraltar-16.12.8 (Latest) Add On (N/A)	0	3 High 1 Medi...	↓
cat9k_iosxe.17.03.05.SPA.bin Verified	17.03.05.0.6600 (Suggested) Add On (1)	0	0 Critical 0 High	★
cat9k_iosxe.17.03.06.SPA.bin	Amsterdam-17.3.6 (Latest)	0	0 Critical 0 High	↓



# Define relevant pre & post checks

Update Image  
1 device(s)

Distribute Activate **3 Checks** 4 Confirm

Following are a set of available validators or checks to run for each stages of operation represented in each tab. You may un-check the validators you would not like to run for the current workflow.

Distribution (1) Activation (5)

Flash check  SYSTEM PRE

Update Image  
1 device(s)

Add a New Custom Check

Name\* show route When\* Pre X Post X

You can add commands in the below text area. You can invoke command runner to check if the commands are supported by Cisco DNA Center before adding to the list below, Use Q+T command to toggle the visibility of the Command Runner.

Select a Test Device\* C9K-STACK.cisco.com

Test commands show route

Update Image  
1 device(s)

Distribute Activate **3 Checks** 4 Confirm

Following are a set of available validators or checks to run for each stages of operation represented in each tab. You may un-check the validators you would not like to run for the current workflow.

Distribution (2) Activation (6)

Flash check  SYSTEM PRE

show route  CUSTOM PRE POST

Not able to see the check you would like to run? You can add a new check.

TBRANCH-C9200L-3.cisco.com (10.85.54.25) Image Update  
Date: May 2, 2022 3:34 PM Duration: 13 minutes 22 seconds Status: Successfully Activated cat9k\_lite\_iosxe.17.08.01.SPA.bin

Operations Checks

Search Table

Scripts	Operation	Pre Check	Post Check	Differences
Spanning Tree Summary Check	Activate	✓	✓	2 Differences
CDP neighbors Check	Activate	✓	✓	2 Differences
Interface Check	Activate	✓	✓	No Differences
Fabric Device Upgrade Check	Activate	✓	N/A	No Differences
Config register check	Activate	✓	N/A	No Differences
ShowPlntBrief	Activate	✓	✓	No Differences
ShowIntf	Activate	✓	✓	No Differences

# 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](#)
  - 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 or N+1

The screenshot displays the 'Image Update' interface. At the top, a progress bar shows five steps: 1. Analyze Selection (active), 2. Distribute, 3. Activate, 4. Schedule and Clean Up, and 5. Summary. Below the progress bar, the 'Analyze Selection' section is active, with the instruction: 'Before you proceed for the Update, analyze your selection.' The summary shows: 'Devices to Update: 1 | Device Family: 1 | Sites: 1'. A search bar labeled 'Search Table' is present. Below it, a table lists the selected device. A context menu is open over the first row, showing 'Enable ISSU Update' and 'Disable ISSU Update' options.

Device	Device Family	To Image	Comment
WLC1 (172.100.1.5)	CL-universalk9.17.06.03.SP	C9800-CL-universalk9.17.06.04.SP A.bin ISSU	ISSU Validation Successful <a href="#">Update Readiness Report</a>

# 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 DNAC 2.3.3.x

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

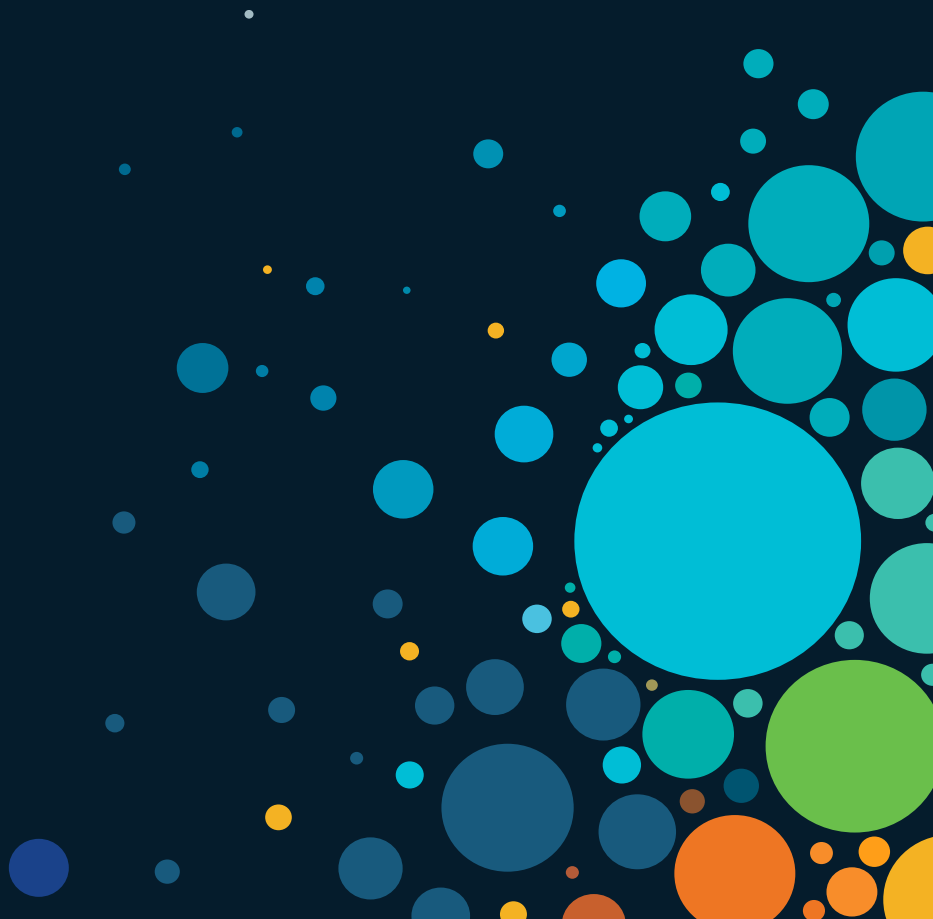
### 9800\_SWIM (172.100.1.54) Image Update

Date: Sep 27, 2022 4:20 PM Duration: 27 minutes 7 seconds Status: ✔ Successfully Activated C9800-CL-universalk9.16.12.05.SPA.bin

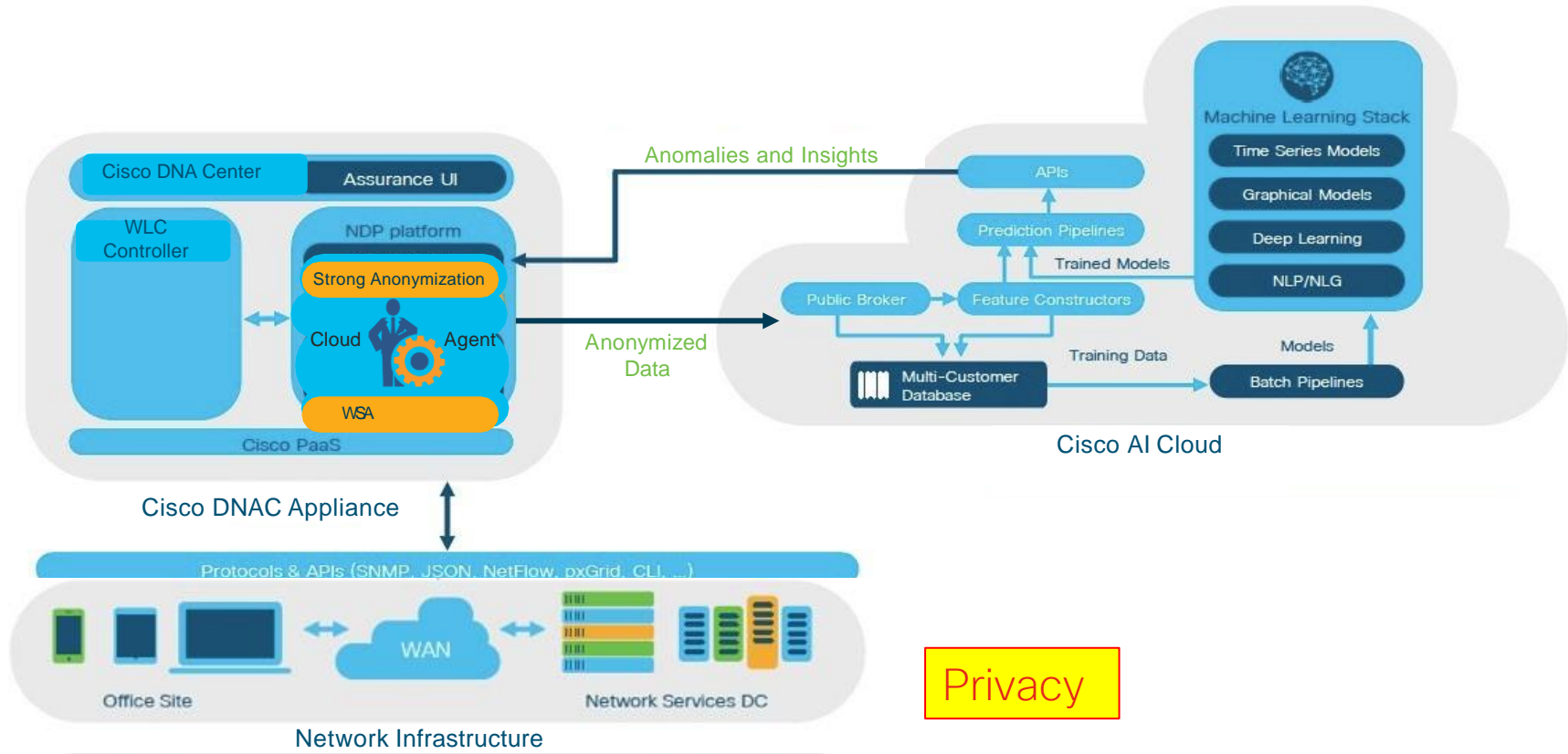
Task Names (4)	Devices Updates	Operations	Checks												
> Image Versions (7)	0 Selected <span style="color: blue;">Retry</span> <span style="color: blue;">Upcoming T</span>	<span style="color: green;">✔</span> Image Checksum Verification On Device 40 seconds													
	<table border="1"><thead><tr><th>Device Name</th><th>Dev</th></tr></thead><tbody><tr><td><a href="#">172.100.1.54</a></td><td>Una</td></tr><tr><td><a href="#">New-Cat9300-Stack-Switch (192.168.120.20)</a></td><td>Dev Fan Una</td></tr><tr><td><a href="#">9800_SWIM (172.100.1.54)</a></td><td>Wir Cor</td></tr><tr><td><a href="#">New-Cat9300-Stack-Switch (192.168.120.20)</a></td><td>Sw and</td></tr><tr><td><a href="#">9800_SWIM (172.100.1.54)</a></td><td>Wir Cor</td></tr></tbody></table>	Device Name	Dev	<a href="#">172.100.1.54</a>	Una	<a href="#">New-Cat9300-Stack-Switch (192.168.120.20)</a>	Dev Fan Una	<a href="#">9800_SWIM (172.100.1.54)</a>	Wir Cor	<a href="#">New-Cat9300-Stack-Switch (192.168.120.20)</a>	Sw and	<a href="#">9800_SWIM (172.100.1.54)</a>	Wir Cor	<span style="color: green;">✔</span> Unpack Images 2 minutes 30 seconds	
Device Name	Dev														
<a href="#">172.100.1.54</a>	Una														
<a href="#">New-Cat9300-Stack-Switch (192.168.120.20)</a>	Dev Fan Una														
<a href="#">9800_SWIM (172.100.1.54)</a>	Wir Cor														
<a href="#">New-Cat9300-Stack-Switch (192.168.120.20)</a>	Sw and														
<a href="#">9800_SWIM (172.100.1.54)</a>	Wir Cor														
		<span style="color: green;">✔</span> AP Pre-Image Download 8 minutes 6 seconds													
			<div style="border: 1px solid purple; padding: 5px;"><p>Task Name: AP Pre-Image Download</p><p>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.)</p></div>												
		<span style="color: green;">✔</span> Activation 13 minutes 15 seconds													

15 Records

# Habit #5 – Proactive insights with AI/ML



# Cisco AI Network Analytics Architecture



# AI Driven Baseline Issues

## Use case:

What are the expected KPI performance across AP's and SSID's? How can I effectively identify, isolate and mitigate deviations from the baseline performance.

## Key Benefits:



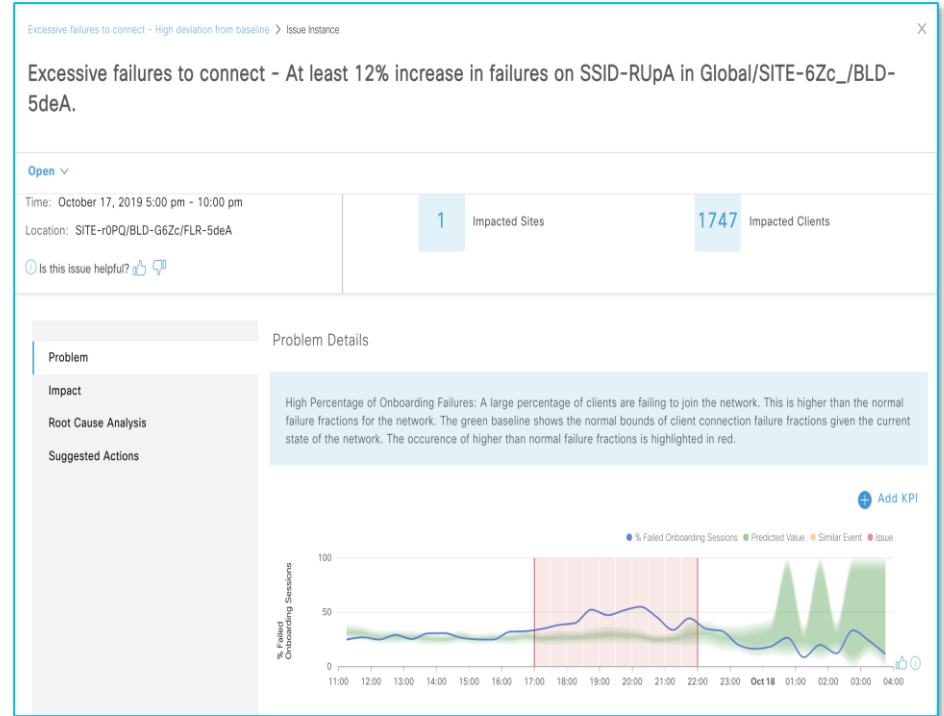
View Dynamic baselines and deviations for 12 (onboarding + throughput) KPI's



Accelerated troubleshooting with end-2-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.



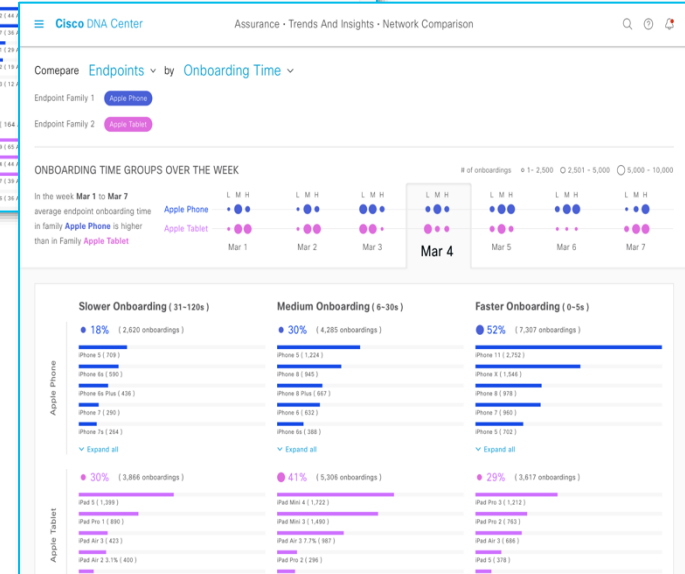
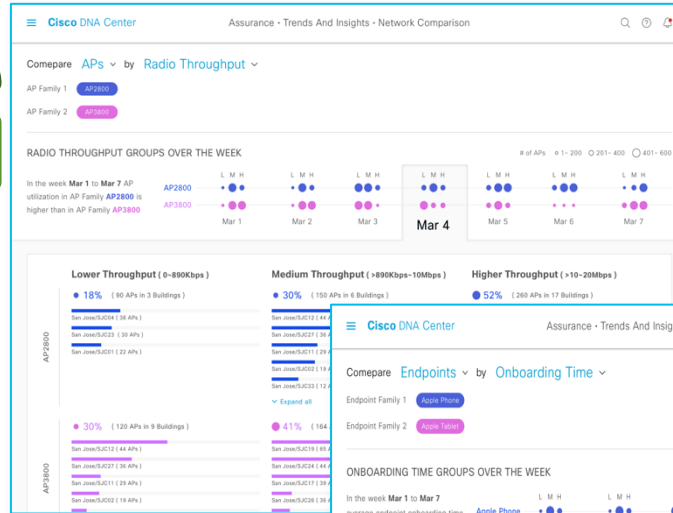
Flexibility to compare both on-boarding and throughput KPI's



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



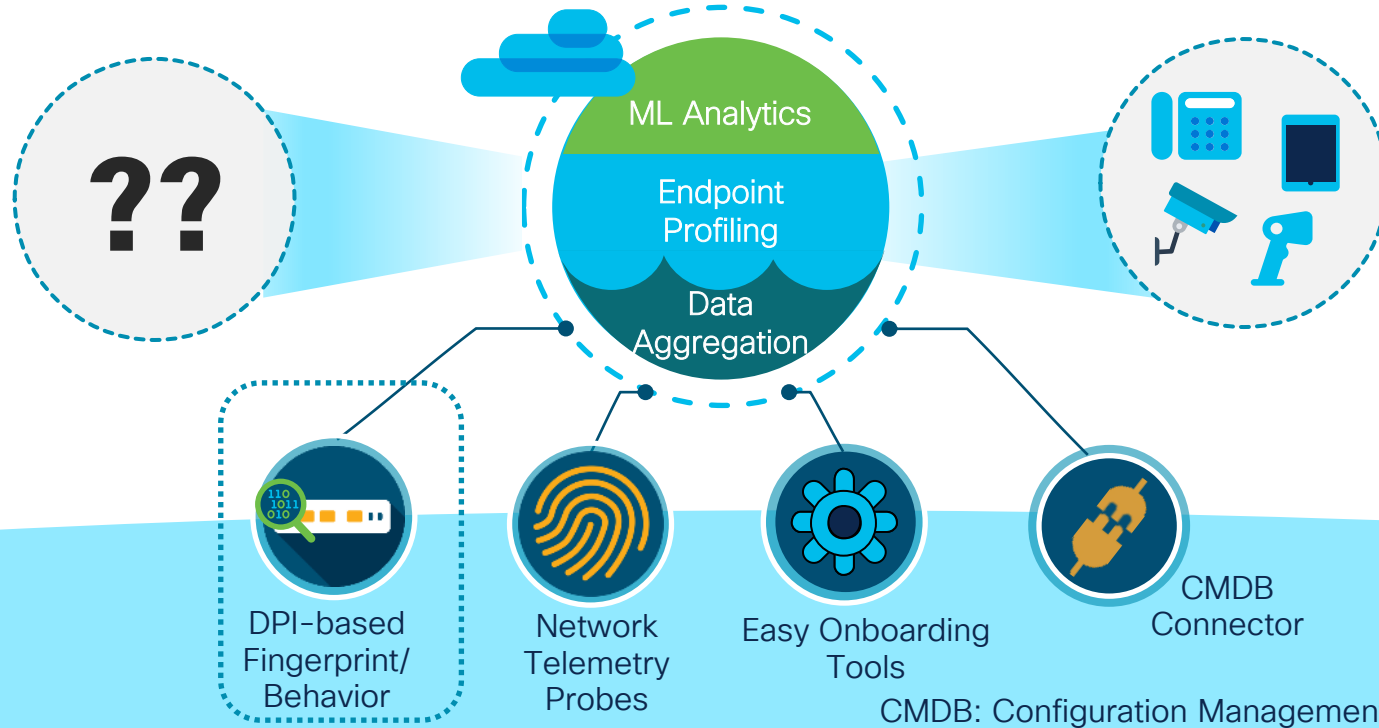
View and compare onboarding KPIs for specific device types for days of a week..



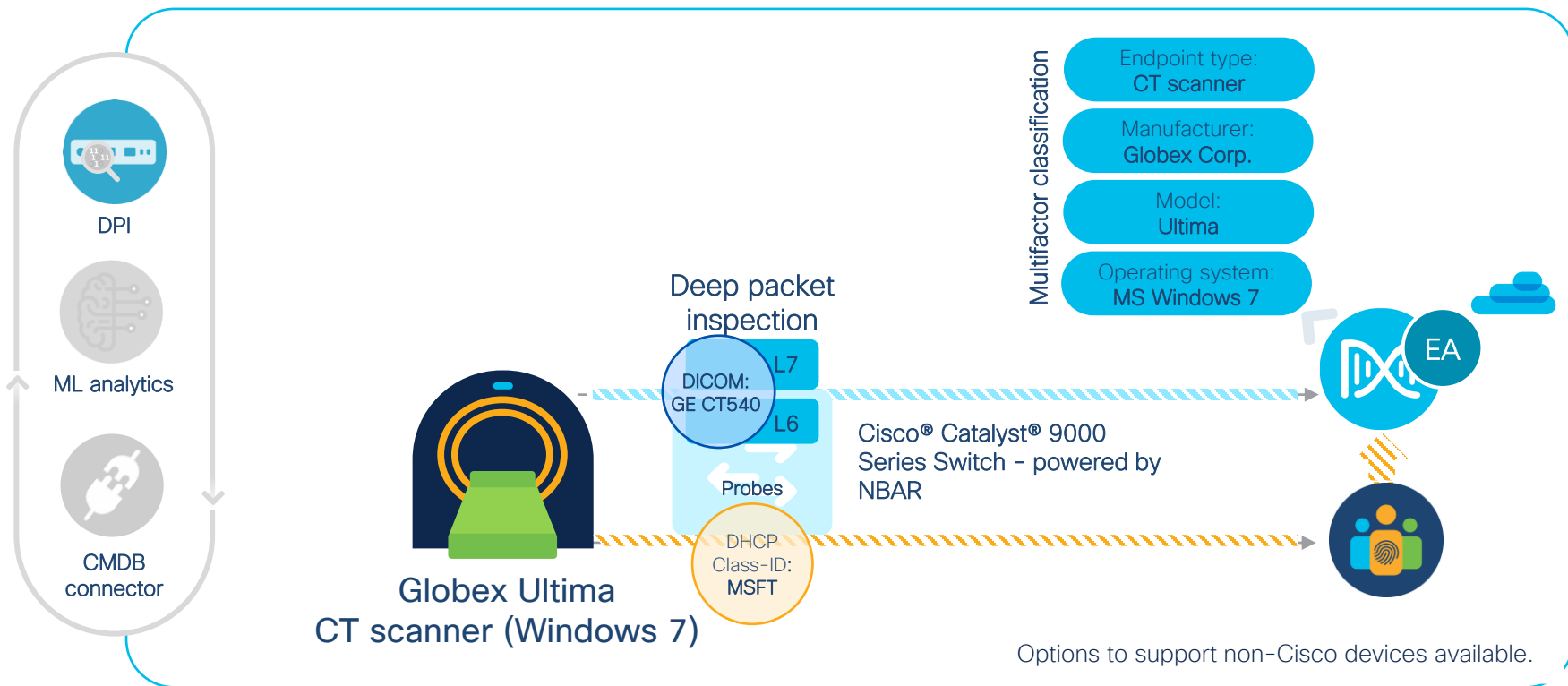


# AI Endpoint Analytics on Cisco DNA Center

Rapidly reducing the unknowns by aggregating data from different sources



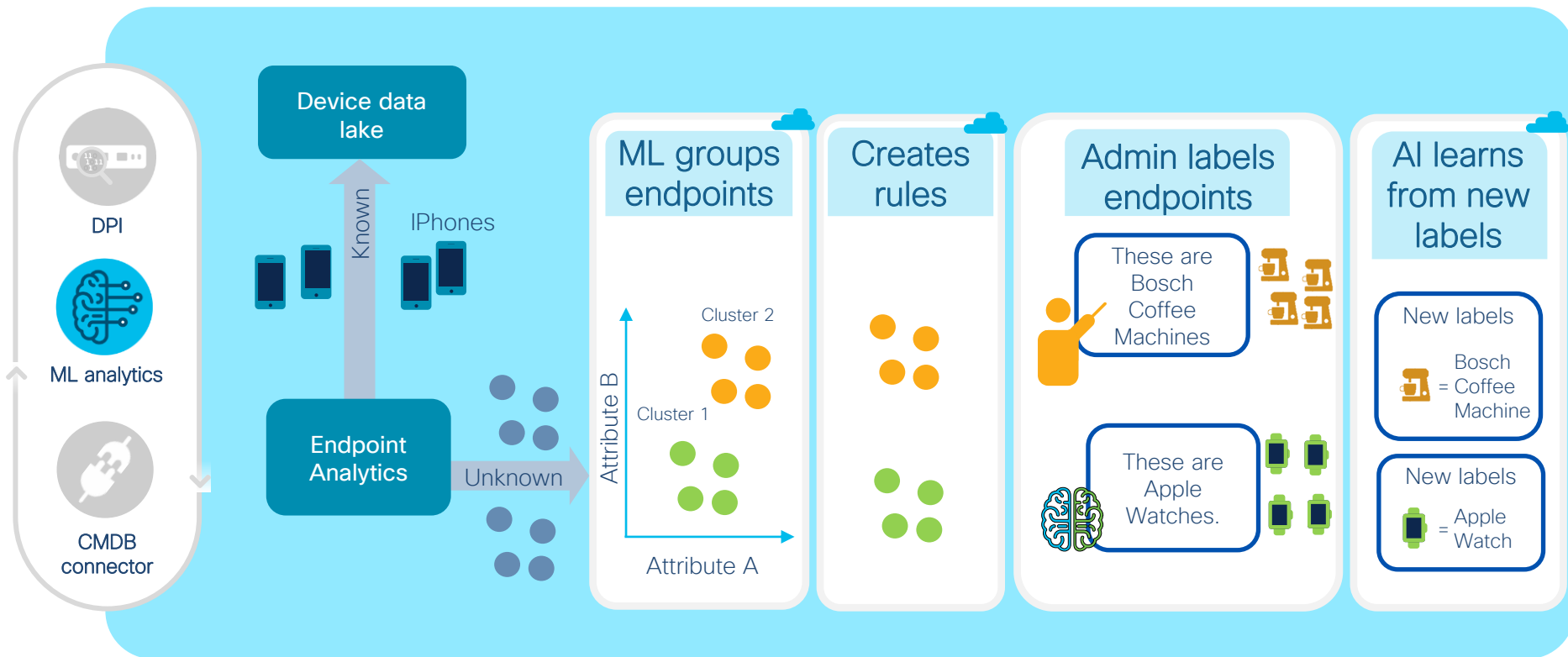
# Classification based on Deep Packet Inspection (DPI)



# Reducing Unknowns with Machine Learning

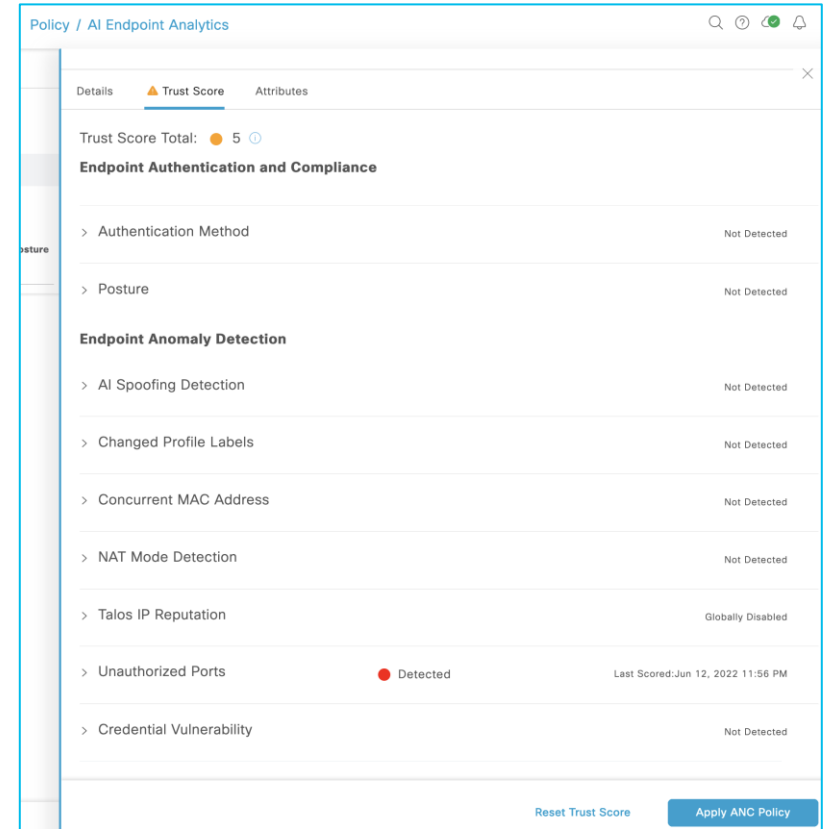
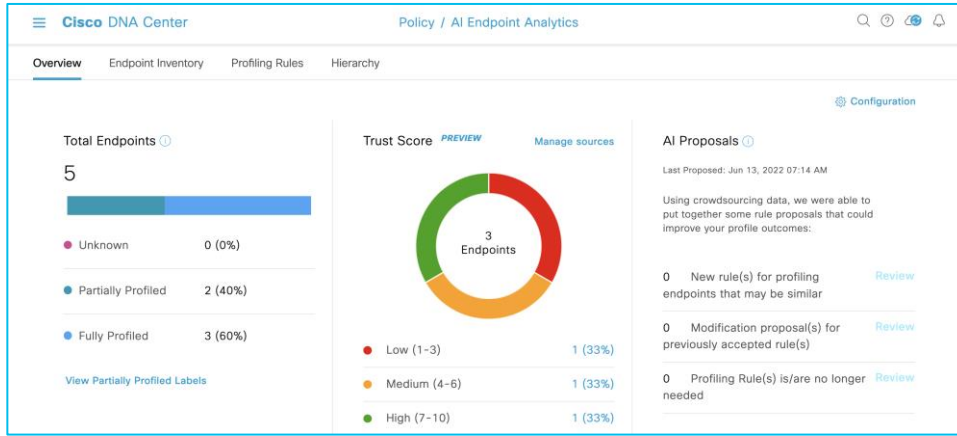


For your reference



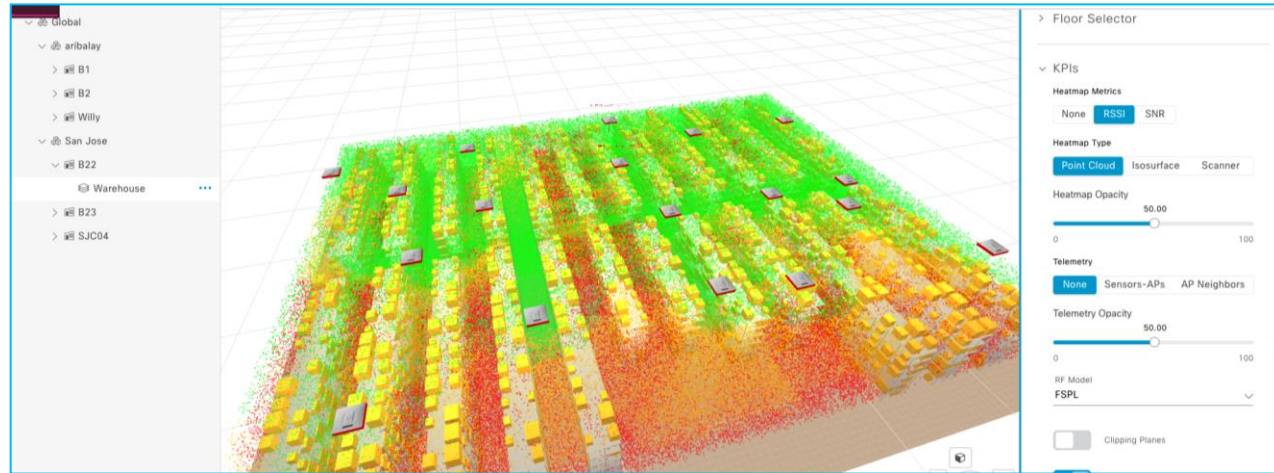
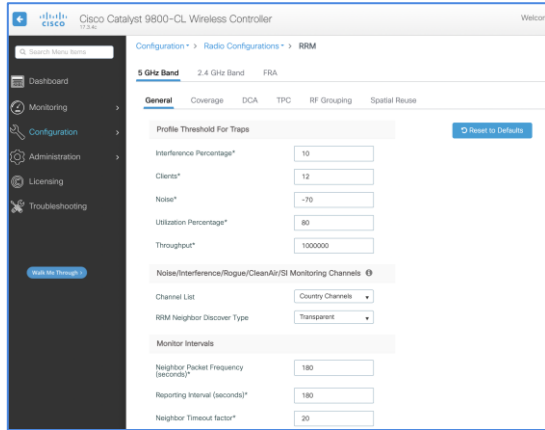
= done in cloud

# Trust Scores and Remediation



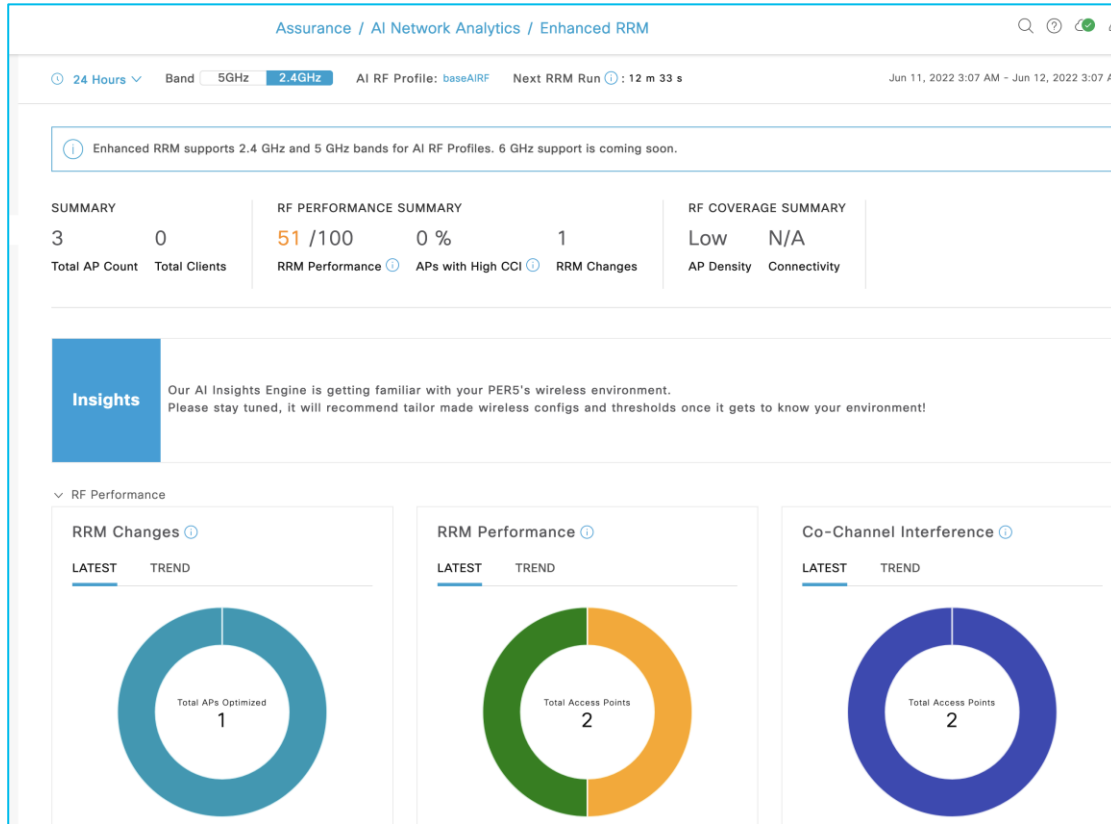
Adaptive Network Control - ANC  
Remediate the host via Identity Services  
Engine - ISE

# Why radio resource management



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

# Dashboard



# Habit #6 – APIs and other integrations



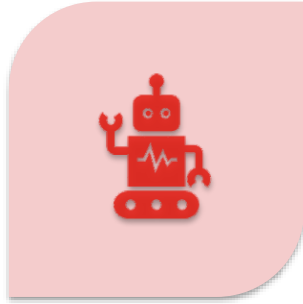
DRIVE FOR  
SHOW  
AND  
PUTT FOR  
DOUGH



GUI FOR  
SHOW  
AND  
API FOR  
DOUGH



# Why API?



AUTOMATION



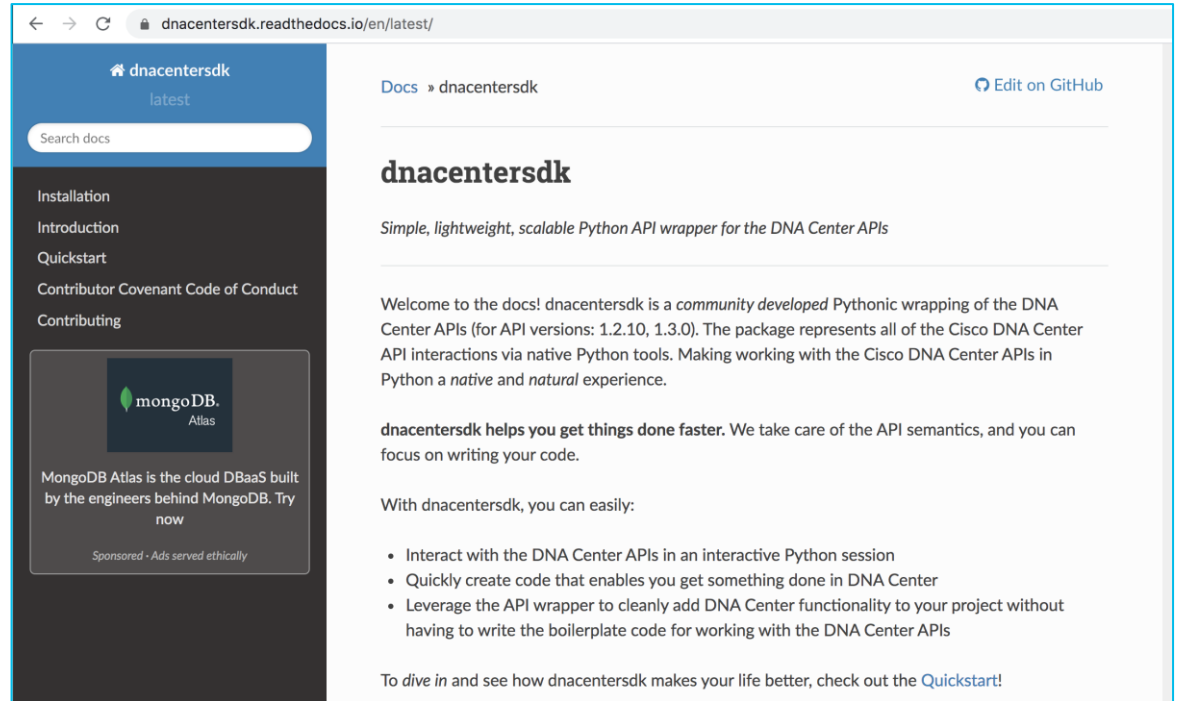
INTEGRATION



INNOVATION

# SDK

```
>>> from dnacentersdk import DNACenterAPI
>>> api = DNACenterAPI()
```



← → ↻ dnacentersdk.readthedocs.io/en/latest/

dnacentersdk  
latest

Search docs

Installation  
Introduction  
Quickstart  
Contributor Covenant Code of Conduct  
Contributing

mongoDB.  
Atlas

MongoDB Atlas is the cloud DBaaS built by the engineers behind MongoDB. Try now

Sponsored - Ads served ethically

Docs » 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). 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!](#)

# Go/Ansible/Terraform

The screenshot shows the GitHub repository page for 'cisco-en-programmability/dnacenter-go-sdk'. The repository is public and has 8 branches and 28 tags. A commit by 'fmuozmiranda' is highlighted, showing a file tree with folders like '.github', 'examples', 'scripts', and 'sdk'. A list of files is shown, including 'README.md', 'LICENSE', 'Makefile', 'go.mod', and 'go.sum', each with a brief description of its purpose.

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

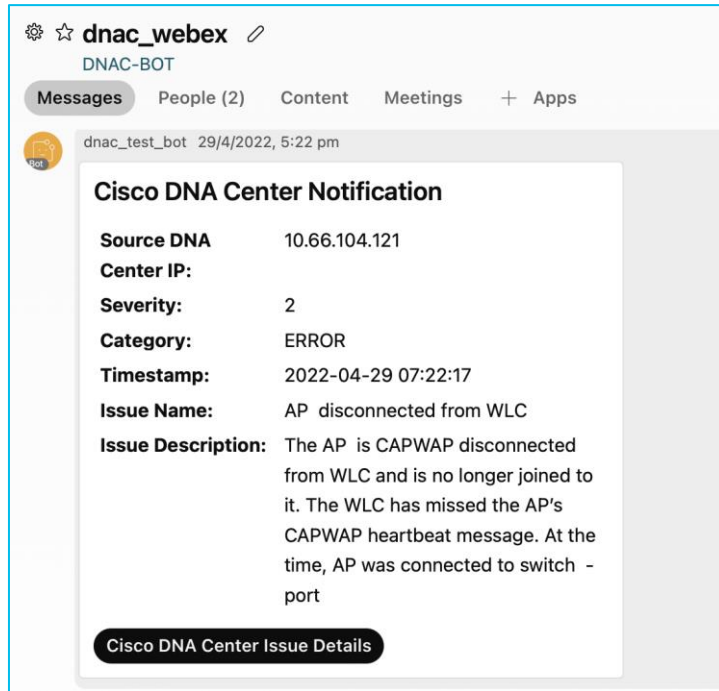
The screenshot shows the Ansible Galaxy page for the 'cisco.dnac' collection. The page is titled 'Community Authors > cisco > dnac'. It features the Cisco and dnac logos, and buttons for 'Details', 'Read Me', and 'Content'. The 'Info' section includes an installation command: '\$ ansible-galaxy collection install cisco.dnac'. A note states: 'NOTE: Installing collections with ansible-galaxy is only supported on Linux and macOS. Download tarball'. The 'Install Version' section shows '6.4.0 released 2 months ago (latest)'. The 'Tags' section includes 'cisco', 'dnac', 'cloud', 'collection', 'networking', and 'sdi'. The description states: 'Ansible Collection - cisco.dnac', 'Ansible Modules for DNA Center', and 'The dnacenter-ansible project provides an Ansible collection for managing and automating your DNA Center. This collection has been tested and supports Cisco DNA Center 2.2.3.3. Note: This collection is not compatible with versions of Ansible before v2.8. Other versions of this collection have support for previous Cisco DNA Center versions. The record the Compatibility matrix.'

<https://galaxy.ansible.com/cisco/dnac>

The screenshot shows the Terraform Registry page for the 'cisco-en-programmability/dnacenter' provider. The page is titled 'Providers / cisco-en-programmability / dnacenter / Version 0.3.0-beta'. It features the Terraform logo and a search bar. The 'dnacenter' provider is listed, with the logo for 'en' (Cisco Enabling Network Engineering) and the text 'by: cisco-en-programmability'. The 'Networking' category is highlighted. The 'VERSION' is '0.3.0-beta', 'PUBLISHED' is '2 months ago', and 'SOURCE CODE' is 'cisco-en-programmability/terraform-provider-dnacenter'.

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

# Native Webex Issue Integration



The screenshot shows a Webex chat window for a group named "dnac\_webex". The chat header includes a settings gear, a star, the group name "dnac\_webex", and a pencil icon for editing. Below the header, there are tabs for "Messages", "People (2)", "Content", "Meetings", and "+ Apps". The main chat area shows a message from "dnac\_test\_bot" dated "29/4/2022, 5:22 pm". The message content is a "Cisco DNA Center Notification" with the following details:

- Source DNA:** 10.66.104.121
- Center IP:**
- Severity:** 2
- Category:** ERROR
- Timestamp:** 2022-04-29 07:22:17
- Issue Name:** AP disconnected from WLC
- Issue Description:** The AP is CAPWAP disconnected from WLC and is no longer joined to it. The WLC has missed the AP's CAPWAP heartbeat message. At the time, AP was connected to switch - port

At the bottom of the notification card, there is a button labeled "Cisco DNA Center Issue Details".

# Habit #7 – Minimizing upgrade risk with AURA tool

# AURA

## Focus Areas for Automation

DNA Center Scale

SDA Control &  
Security Audit

DNA Center Infra  
Health

SDA Device CLI  
Capture

DNA Center  
Assurance

WLC/eWLC  
Assurance

Bugs Causing  
Upgrade Failures

Upgrade  
Readiness

PDF Generation  
(Open Source)

SDA Compatibility  
Check

DNAC-ISE  
Integration

## Cisco DNA Center AURA (Audit & Upgrade Readiness Analyzer)

- **AURA** is a tool that covers health, scale & upgrade readiness checks across the DNAC Use Cases
- Simple & Straight Forward:
  - Copy **one** executable file to the DNAC and execute it on the DNAC
  - Using existing pre-installed libraries/software ONLY
  - Only input required – DNA Center passwords
  - Automatically generated PDF report & Zipped Log file that can be automatically uploaded to Cisco SR
  - Not Intrusive – only DB reads, show commands and API calls
  - Works with 1.2.8/10/12, 1.3.x, 2.1.x, 2.2.x, 2.3.x
- Execution time: DNAC node <15mins. SDA=depends on scale (approx. 30min for 30 SDA Devices)

# Sample (32-page) report

## Cisco DNA Center AURA Results - v1.6.4

The Cisco DNA Center AURA (Audit & Upgrade Readiness) tool performs a variety of health, scale & upgrade readiness checks across the Cisco DNA Center and the rest of the Fabric network without affecting any of the devices. This report is auto generated by the script and documents all the checks and logs performed by the script. Thank you for running it, please reach out to dna\_center\_audit\_tool@cis.com for any feedback.

A total of 171 checks were executed on the setup, found 10 errors and 24 warnings. Please evaluate the Warnings & Errors, ensure the Errors are eliminated prior to proceeding with an upgrade.

### Summary of the Results

#### Cisco DNA Center Device Details:

Model	Serial Number	Software Version	Node IP Address
DN1-HW-APL	FCH2127V008	2.2.3.4	10.10.10.144

#### Script Execution Time:

Start Time	End Time
2022-04-27_22:39:56	2022-04-27_22:50:10

#### Cisco DNA Center Infra Health Results:

Checks Executed	Errors Found	Warnings Found
90	5	16

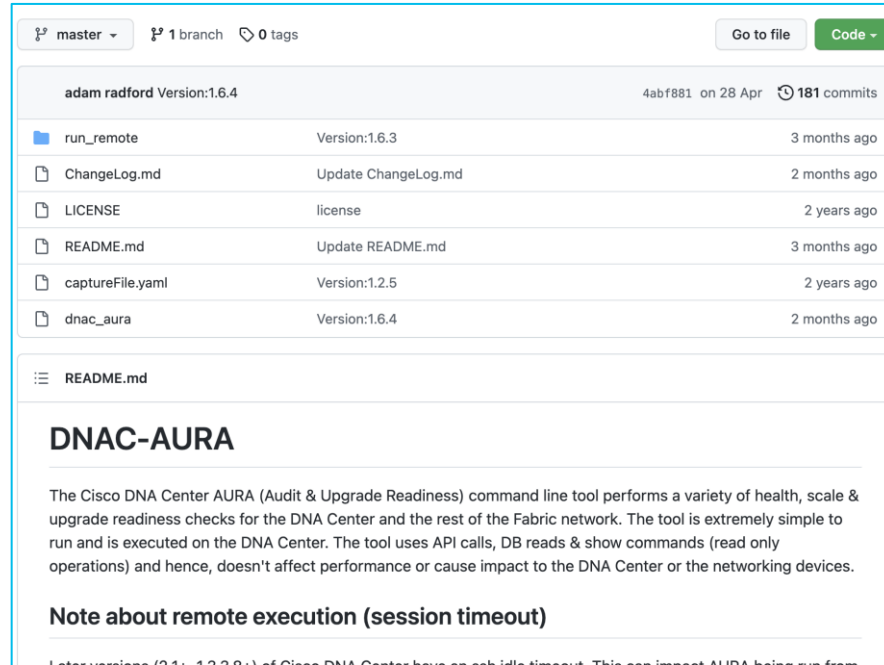
#### Cisco DNA Center & Device Assurance Results:

Checks Executed	Errors Found	Warnings Found
17	0	2

#### Cisco DNA Center & Device Upgrade Readiness Results:

Checks Executed	Errors Found	Warnings Found
37	5	5

# Download from git



The screenshot shows a GitHub repository page for 'adam radford Version:1.6.4'. The repository has 1 branch and 0 tags. The file list includes:

File	Commit Message	Time
run_remote	Version:1.6.3	3 months ago
ChangeLog.md	Update ChangeLog.md	2 months ago
LICENSE	license	2 years ago
README.md	Update README.md	3 months ago
captureFile.yaml	Version:1.2.5	2 years ago
dnac_aura	Version:1.6.4	2 months ago

The README.md file content is visible below the file list:

## DNAC-AURA

The Cisco DNA Center AURA (Audit & Upgrade Readiness) command line tool performs a variety of health, scale & upgrade readiness checks for the DNA Center and the rest of the Fabric network. The tool is extremely simple to run and is executed on the DNA Center. The tool uses API calls, DB reads & show commands (read only operations) and hence, doesn't affect performance or cause impact to the DNA Center or the networking devices.

### Note about remote execution (session timeout)

Later versions (2.1, 1.2.2.2) of Cisco DNA Center have an idle timeout. This can impact AURA being run from

<https://github.com/CiscoDevNet/DNAC-AURA>



# Restricted Shell

In Cisco DNA Center 2.3.3 there is a restricted shell by default

- Can be access unrestricted shell using the command `_shell`

In Cisco DNA Center 2.3.4 and above the restricted shell cannot be disabled

- Need to get a consent token from tac (4 days)

# Validation Tool

System Health / Validation Tool

Validation Runs (1) As of: Dec 8, 2022 9:03 AM

Search Table

Add Delete 0 Selected

Name	Description	Selected Set(s)	Status	Start Time	Duration	Actions
AURAIinternal		Appliance Infrastructure Status +4	Critical	Oct 11, 2022 3:32 PM	5 min	<a href="#">View Status</a>

1 Records Show Records: 10 1 - 1

New Validation Run

Triggering a Validation Run can be a combination of multiple validation sets or at least one validation set.

Name\*

validation

Description

Validation Set(s) Selection\*

- Appliance Infrastructure Status
- Appliance Scale
- Assurance Health
- Cisco ISE Health and Cisco DNA Center Role
- Upgrade Readiness Status

Upgrade Readiness Status








- System software update mode (online/offline)
- Catalog server settings
- Catalog server repository settings
- Catalog override default repository settings
- HTTP proxy configuration settings
- Catalog server connectivity status
- HTTP proxy reachability status
- Backup status (backup success < than 1 week)
- Service(s) - Operational status
- Service(s) - Restart counts for the past 24 hours
- Pods - Operational status
- Disk storage available - root directory
- Disk storage available - data directory
- Exited pod(s) count
- System certificate status
- Authentication and Policy servers configuration and status
- Workflow status
- Release status

Cancel Run

Built into DNA Center  
Number of checks will grow over time

# Take aways



-  Device Controllability to maximize value
-  Telemetry for network/application/user insights
-  Software Image management to keep up to date
-  Compliance and Configuration management
-  AI/ML for Alops
-  API for automation/integration/innovation
-  AURA – Automated Upgrade Readiness Assessment (and operational health)

# Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at <https://www.ciscolive.com/emea/learn/sessions/session-catalog.html>



# Continue Your Education



Visit the Cisco Showcase for related demos.



Book your one-on-one Meet the Engineer meeting.



Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.



Visit the On-Demand Library for more sessions at [ciscolive.com/on-demand](https://ciscolive.com/on-demand).



The bridge to possible

Thank you

CISCO *Live!*

CISCO *Live!*

ALL IN