

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



"Reconciliation" - Dustin Koa Art

CISCO *Live!*



7 Habits for success with Cisco Catalyst Center

Adam Radford, Distinguished Solutions Engineer
@adamradford123
BRKOPS-2416

CISCO *Live!*

#CiscoLiveAPJC

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

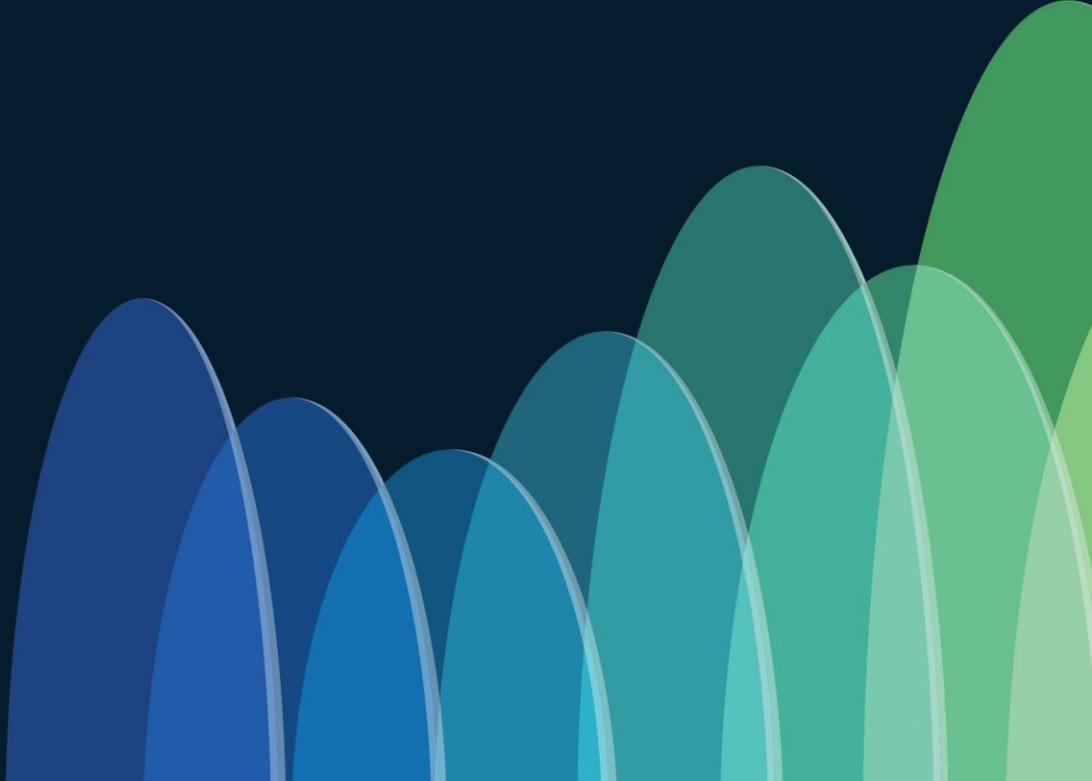
Webex spaces will be moderated by the speaker until November 15, 2024.

CISCO *Live!*

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



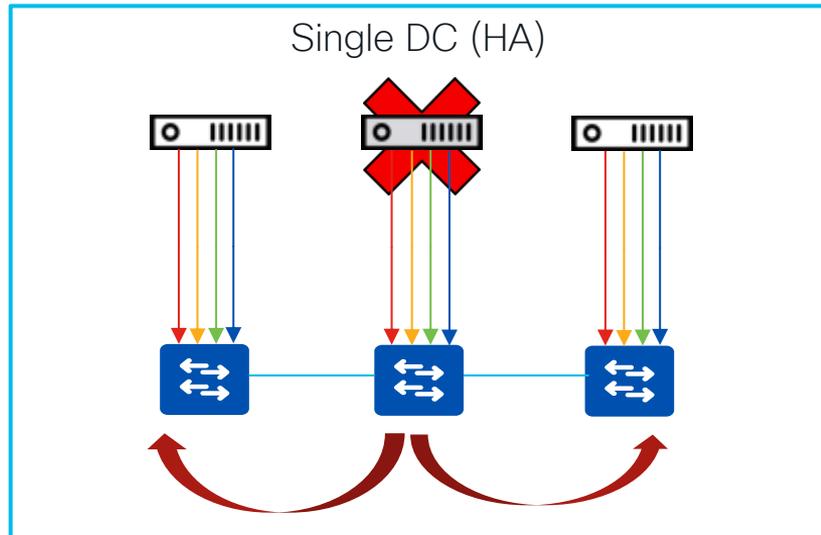
Habit #1 – Understand
Cisco Catalyst Center
Resiliency and design
what's best for your
environment



Physical Appliance High Availability with clustering



Physical Appliance



✓ Software or Hardware Failure

✓ Active/Active

✓ Near Real-Time Synchronization

Considerations

✓ Hardware Appliance needs to match

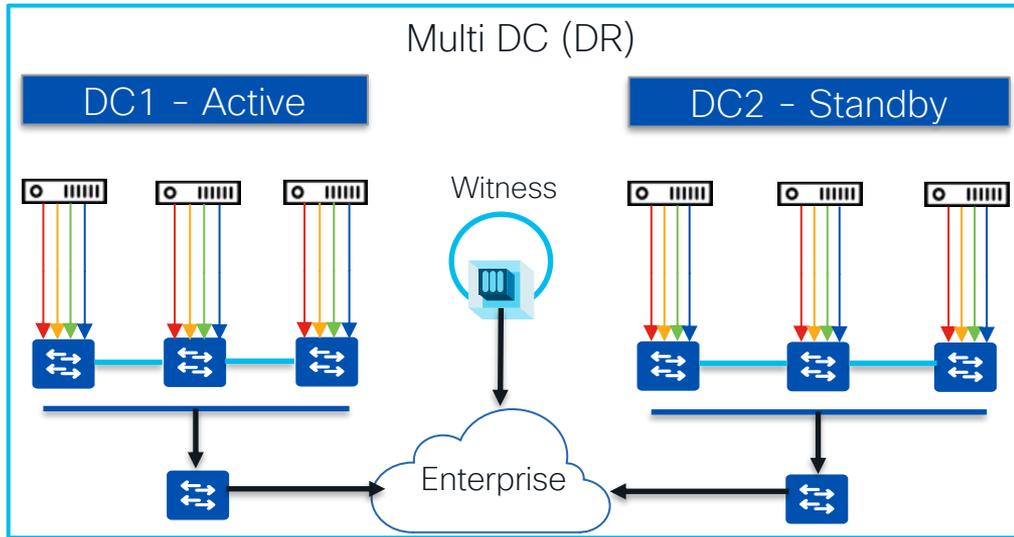
✓ 3-node cluster in single DC

✗ DN3 can't cluster with DN2 (temporary)

Physical Appliance Disaster Recovery



Physical Appliance



✓ Resiliency in Site failure

✓ Active/Standby

✓ 3+3+1 or 1+1+1 across DC's

✓ Not all data gets replicated

Considerations

✓ Identical third-party certificates on both DR clusters. Don't use self-signed certs

✓ Deploy witness in a third location

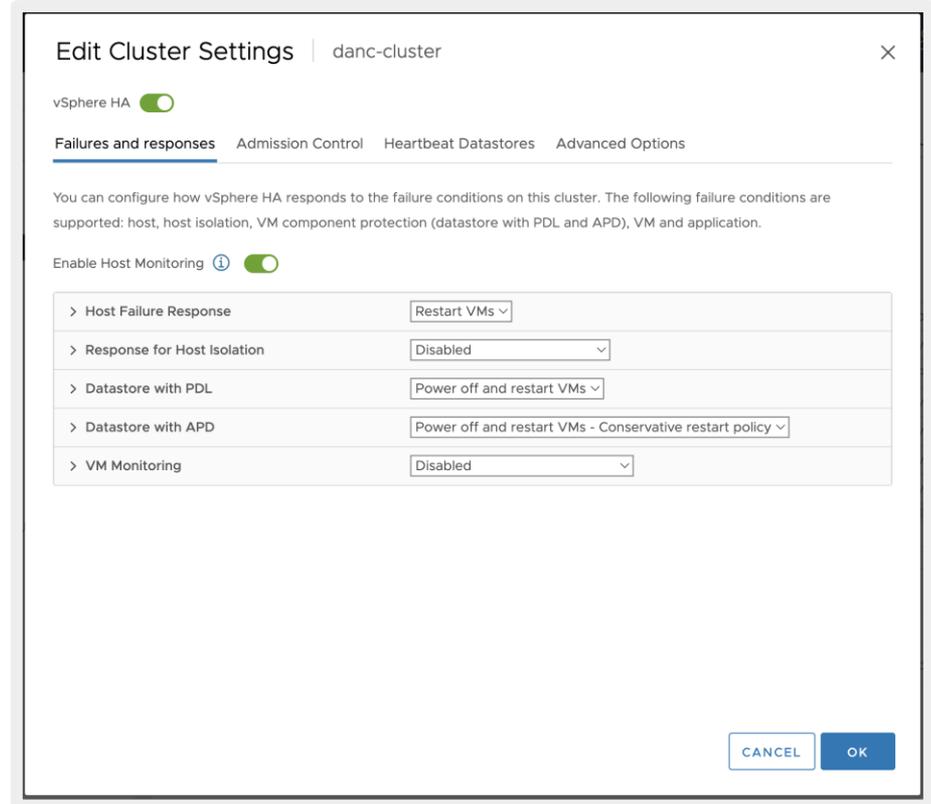
✓ DR VIP with BGP advertisement recommended for L3

High Availability in Virtual Appliances



Clustering is not supported with ESXi VM and AWS VA

High Availability is delivered using the hosting infrastructure HA features

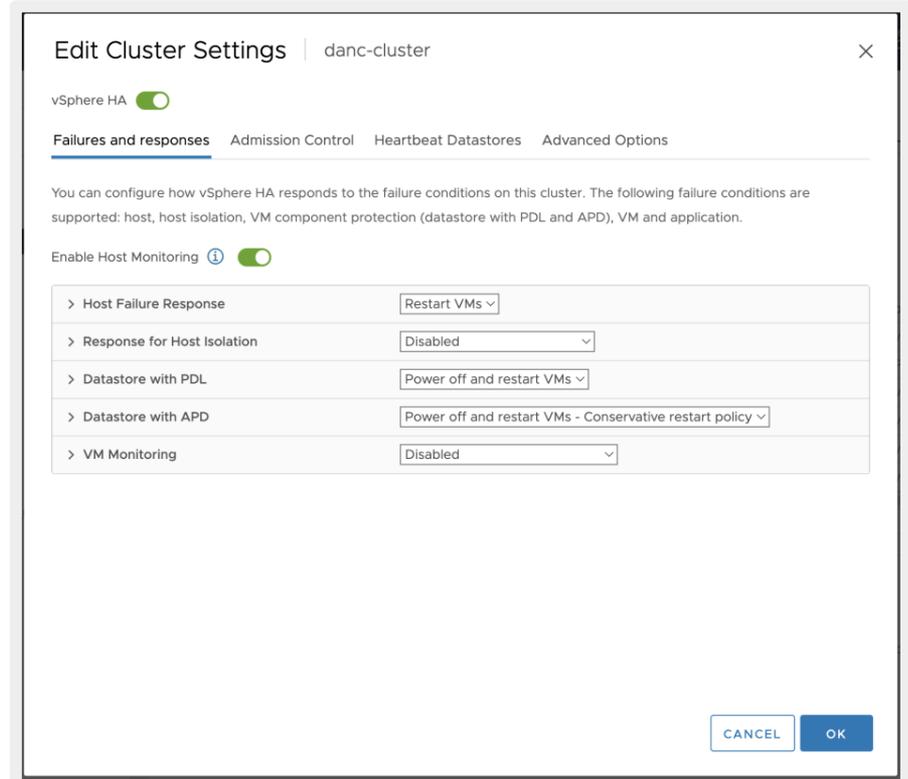


High Availability in ESXi VA

ESXi High Availability delivered via VMware vSphere's HA functionality

If a host failure occurs, the virtual machines restart on alternate hosts

At least two hosts must have the unreserved CPU/Memory resources required for ESXi VM



High Availability in AWS VA



If a Catalyst Center EC2 (*) instance crashes, AWS brings up another instance automatically

Single-node EC2 HA within an Availability Zone (AZ) is enabled by default.

aws

AWS Account ID * ⓘ

878813814009

Access Key ID * ⓘ

.....

Secret Access Key * ⓘ

.....

↻

(*) Amazon EC2: Amazon Elastic Compute Cloud

Backup and Restore - Appliance, AWS VA, ESXi VA



Physical Appliance

vmware®



↓ Types of backup



 System and network automation ★

 System, network automation and assurance

Backups can be On-Demand or Scheduled

Backup and Restore - Appliance, AWS VA, ESXi VM



Physical Appliance



↓ Types of backup

Create Backup

BASICS

Backup Name*
10oct2023

Create now Schedule daily Schedule weekly

Repeat weekly on:

S M T W T F S

At this time:
🔒 12 : 00 : AM

SCOPE

Cisco DNA Center (All data) [ⓘ]
 Cisco DNA Center (without Assurance data) [ⓘ]

Use this option to back up only automation data. With this option, Assurance data is not backed up.

Create Backup

BASICS

Backup Name*
10oct2023

Create now Schedule daily Schedule weekly

Repeat weekly on:

S M T

At this time:
🔒 12 : 00 : AM

SCOPE

Cisco DNA Center (All data) [ⓘ]
 Cisco DNA Center (without Assurance data) [ⓘ]

Use this option to back up automation and Assurance data. You must have two backup directories:
-One backup location is an external NFS server for Assurance data;
-One backup location is an external remote sync (rsync) target location for automation and system data;

Backup and Restore – Appliance, AWS VA



Physical Appliance



↓ Backup Destinations



 RSYNC for Automation Backup



 Linux-based NFS server for Assurance Backup

Backup and Restore – Appliance and AWS VA



Physical Appliance



System / Backup & Restore

Backup & Restore

Backups Schedule Activity Configure

Cisco DNA Center (Remote Host) *i* Cisco DNA Center (NFS) *i*

Configured

SSH IP Address*
10.85.54.179

SSH Port*
22 Hint

Server Path*
/home/netadmin/TRN6_DNAC_Backups/

Username*
netadmin

Password*

Encryption Passphrase* Hint

DNA Center

Backup & Restore

Backups Schedule Activity Configure

Cisco DNA Center (Remote Host) *i* Cisco DNA Center (NFS) *i*

Configured

Host*
10.85.54.179

Server Path*
/home/netadmin/TRN6_DNAC_Backups/

Backup and Restore – Appliance to AWS VA



Physical Appliance



- Backup and Restore – Hardware Appliance to AWS VA is supported
- Hardware appliance used for the backup has to be 44-core
- Supports migration from physical to cloud-hosted virtual appliance



44c Physical Appliance



Procedure: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/catalyst-center/catalyst-center-va/aws/admin-guide/1_7/b_cisco-catalyst-center-va-launchpad-administrator-guide_1-7/m_backup_and_restore.html

Backup and Restore - ESXi Virtual Appliance



Physical Appliance

vmware®



↓ Types of backup

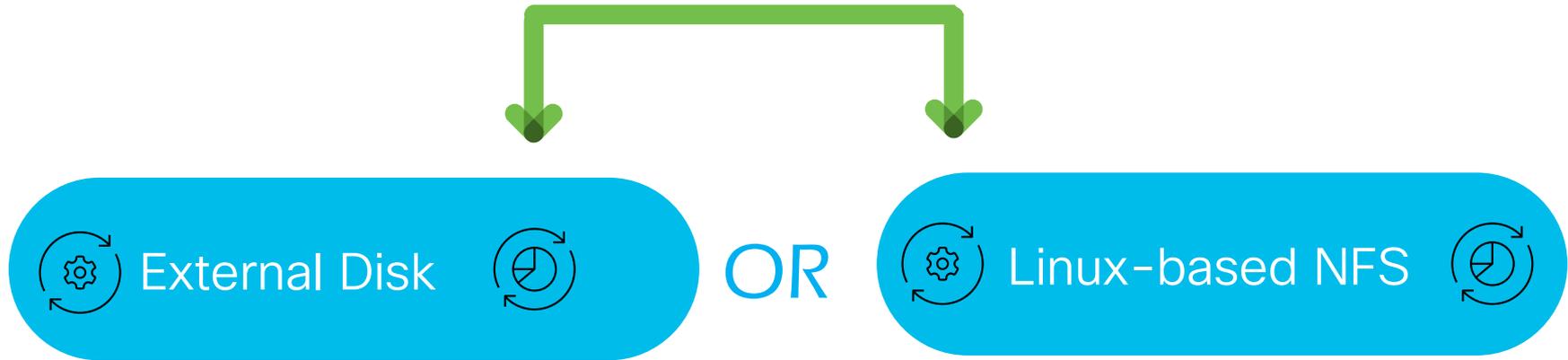


 System and network automation ★

 System, network automation and assurance

Backups can be On-Demand or Scheduled

Backup and Restore - ESXi Virtual Appliance



Single destination for System, Automation and Assurance & ability to schedule data retention

Backup and Restore – ESXi Virtual Appliance

The screenshot displays the Cisco DNA Center interface for configuring backup settings. The main page is titled "Backup Configuration" under "System Configuration". It offers two options: "Physical Disk" and "NFS" (which is selected). The NFS configuration includes a "Mount Path*" field with the value "nfs://nfs-e51b0f72-fb9b-5b09-b7a5-95c6d8b62419" and an "Encryption passphrase*" field. A "Backup Retention (in number of backups)*" field is set to "14". A modal dialog titled "Add NFS" is open, showing fields for "Server Host*" (10.106.172.227), "Source Path*" (/var/share/storage-1), "NFS Version*" (NFS 4), "Port" (2050), and "Port Mapper" (111). Buttons for "Reset", "Submit", "Cancel", and "Save" are visible.

Backup Storage Recommendations



Reference

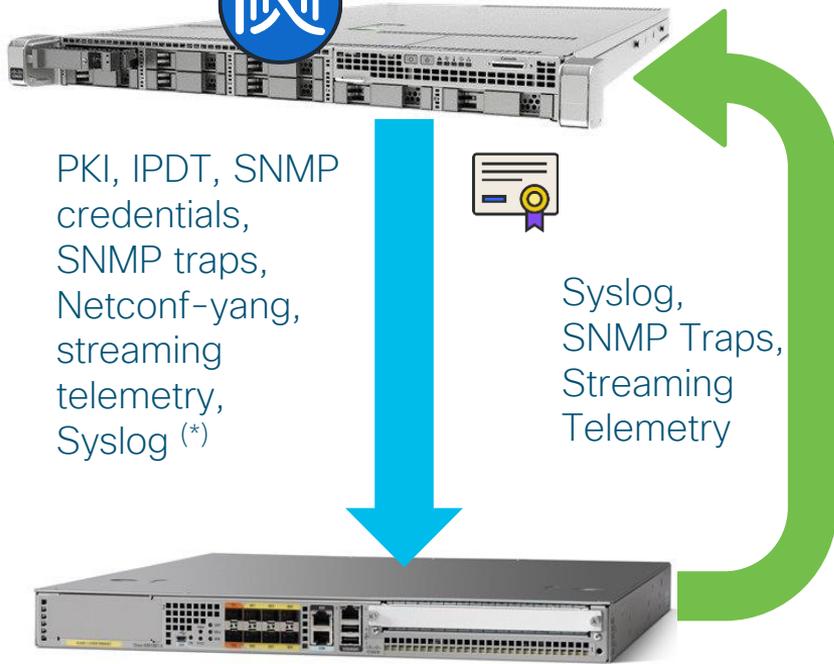
Appliance	NFS Storage (14 Days Incremental)	Rsync Storage (Daily Full)
DN2-HW-APL	1.7 TB	50 GB
DN2-HW-APL-L	3 TB	100 GB
DN2-HW-APL-XL	8.4 TB	300 GB

Recommendations for fully loaded appliance configurations with the maximum number of access points and network devices

Habit #2 – Find issues before your users with telemetry



Benefits of Telemetry data captured via Catalyst Center



- 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

Inventory Device View

TRN6-SDA-CAMPUS-E1.cirrus.cloud

Run Commands View 360

Reachable Managed IP Address: 10.85.62.106 Device Model: Cisco Catalyst 9300 Switch Device Role: ACCESS Uptime: 28 days 3 hrs 27 mins Site: Global/Canada/Ontario/Toronto/TRN6/TRN6-28-SELab

DETAILS

Interfaces

Hardware & Software

Configuration

Power

Fans

SFP Modules

User Defined Fields

Config Drift

REP Rings

SECURITY

Advisories

Color Code Status

All Devices / TRN6-SDA-CAMPUS-E1.cirrus.cloud

TRN6-SDA-CAMPUS-E1.cirrus.cloud

Run Commands View 360

Reachable Managed IP Address: 10.85.62.106 Device Model: Cisco Catalyst 9300 Switch Device Role: ACCESS Uptime: 28 days 3 hrs 27 mins Site: Global/Canada/Ontario/Toronto/TRN6/TRN6-28-SELab

DETAILS

Interfaces

Hardware & Software

Configuration

Power

Fans

SFP Modules

User Defined Fields

Config Drift

REP Rings

SECURITY

Advisories

COMPLIANCE

Summary

All Ports > TenGigabitEthernet1/0/16

Port action Access VLAN Update is not supported on the selected port. Reason: VLAN changes are not supported on devices that are part of the fabric

Type	Physical	Speed	5000 Mbps
Access VLAN	10_85_49_0-InfRA_VN (1021)	MTU	9100 Bytes
Voice VLAN	-	Last Input	Feb 28, 2023 10:34 AM
MAC Address	ec:1d:8b:55:72:90	Last Output	Feb 28, 2023 10:34 AM
Link	FullDuplex	Admin Status	Up
PoE	Enabled	Operational Status	Connected
Max Allocated Power	60.0 Watts	Allocated Power	32.2 Watts
Power Drawn	14 Watts		

Neighbor Details

Name	Campus_Fabric_AP1	Neighbor	GigabitEthernet0
Capabilities	ROUTER_TB_BRIDGE		

PORT DESCRIPTION: ** jinja ninja for 16** march 22

TRN6-SDA-CAMPUS-E1.cirrus.cloud

Run Commands View 360

Managed IP Address: 10.85.62.106 Device Model: Cisco Catalyst 9300 Switch Device Role: ACCESS Uptime: 28 days 3 hrs 27 mins Site: Global/Canada/Ontario/Toronto/TRN6/TRN6-28-SELab

Choose Access VLANs to be color coded in ports view

- default(1) x
- 10_85_49_0-InfRA_VN(1021) x
- 10_85_61_0-Comp_VN(1022) x
- 10_85_58_64-Guest_VN(1024) x

Color Code Access VLANs

User Defined Fields

Config Drift

REP Rings

SECURITY

Advisories

COMPLIANCE

Summary

Detailed port information: port status, PoE, VLAN's, Last Input/Output

Inventory Device - Port Configuration and Actions

The screenshot shows the Cisco DNA Center interface for a device named 'C9K-STACK'. The device is a Cisco Catalyst 9300 Switch with IP address 10.85.54.54. The 'Interfaces' section is expanded to show 'GigabitEthernet2/0/1'. A blue circle with the number '1' highlights the configuration for this port, which is currently set to 'Access VLAN default (1)' and has 'No port description added'. A green box highlights the 'GigabitEthernet2/0/1' configuration details in the left sidebar.

The screenshot shows the 'Edit Access VLAN' dialog box in Cisco DNA Center. A blue circle with the number '2' highlights the dialog box. The dialog shows a search for VLANs, with 'default (1)' selected. The dialog also shows a list of VLANs: 'default (1)', 'VLAN0419 (419)', and 'VLAN0420 (420)'. The 'Save' button is highlighted.

Change port **VLAN** and **description**
Shut down a port or **Clear Mac Table**

Inventory Device - Stack

1

Stack View - Active/Standby, Stack Number and Stack View

2

Platform: C9300-24P Address: 70:18:a7:6e:ff:00 Serial Number: FCW2245CH6P Role: ACTIVE Stack Member Number: 1

Platform: C9300-24P Address: 70:18:a7:33:82:00 Serial Number: FOC2245Z0C2 Role: STANDBY Stack Member Number: 2

Stack #	Role	MAC Address	State	Priority	Switch Port -> Neighbor Port
1	Active	70:18:a7:6e:ff:00	Ready	15	1/1 -> 2/1, 1/2 -> 2/1
2	Standby	70:18:a7:33:82:00	Ready	11	2/1 -> 1/1, 2/2 -> 1/1

Stack

Inventory Insights

Find configuration inconsistencies and misconfigurations

Cisco DNA Center

- Design >
- Policy >
- Provision >
- Assurance >
- Workflows
- Tools >

NETWORK DEVICES

- Inventory
- Plug and Play
- LAN Automation
- Inventory Insights**

SD-ACCESS

- Inventory Insights
- Zero-Trust Overview
- Virtual Networks

1

2

Cisco DNA Center Provision / Network Devices / Inventory Insights

Search Hierarchy Search Help

- Global
 - Unassigned Devices
 - APJC
 - Canada
 - LBC-Canada-Ontario
 - US

Insights Instances

Speed/Duplex settings mismatch	2
VLAN Mismatch	9
2 Records	

Speed/Duplex settings mismatch (2)

As of: Mar 7, 2023 3:40 PM

Devices		Interface		Speed		Duplex	
Device A	Device B	Interface A	Interface B	Speed A	Speed B	Duplex A	Duplex B
TRN6-TBRANCH-DIST.cisco.com (10.85.54.17)	TRN6_TBRANCH_WLC (10.85.54.20)	GigabitEthernet1/0/24	GigabitEthernet0/0/1	1 Gbps	1 Gbps	FullDuplex	AutoNegotiate
DNA-DC-3850-TCP (10.85.54.130)	TRN6-Campus_Fabric_WLC (10.85.54.168)	GigabitEthernet1/0/13	GigabitEthernet0/0/5	1 Gbps	1 Gbps	FullDuplex	AutoNegotiate

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



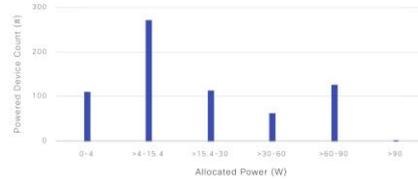
Off: Power Denied (48) Off: Error Disabled (42)

View Details

PoE Powered Device Distribution

LATEST TREND

Allocated Power

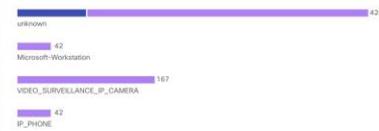


View Details

PoE Insights

Perpetual PoE

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



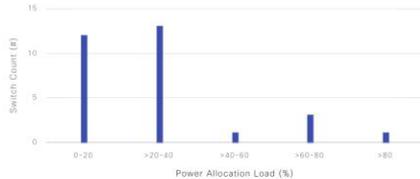
Enabled Not Enabled

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

Cisco DNA Center

PoE Operational State Distribution

LATEST TREND



On (44) Off (0) Off: Faulty (1)
Off: Power Denied (0) Off: Error Disabled (0)

View Details

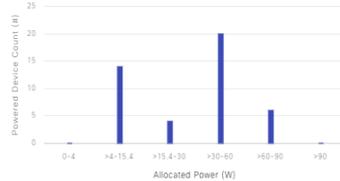
PoE Operational State

PoE endpoint distribution based on their power allocation

PoE Powered Device Allocation

LATEST TREND

Allocated Power



View Details

PoE Endpoint Classification

How many free 60W PoE ports do I have right now?

PoE Port Availability

LATEST TREND



View Details

PoE Port Availability

PoE AP Power Mode Distribution



LATEST TREND



Fully Powered (34) Partially Powered (0)

View Details

AP Power Mode

Power Allocation Load Distribution

LATEST TREND

0/3 (0%) of switches have >80% load.



PoE Budget Monitoring

Power Usage

LATEST TREND

NEW

Allocation



PoE Power Allocation (3.20k) System Power Allocation (0)
Available Power (13.5k)

Power Usage

PoE Insights

Perpetual PoE

42/44 (95%) of powered devices are not enabled for Perpetual PoE.



PoE Insights

Are my AP's fully or partially powered?

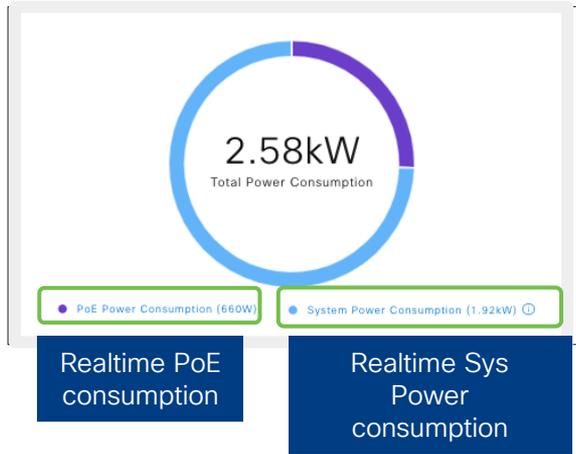
Are all my critical PoE endpoints protected when the switch reboots?

What is the real time power consumption of my access network

How are my PoE endpoints functioning?

Which switches have capacity to add 10 new IP Cameras?

Realtime Power Consumption Reporting

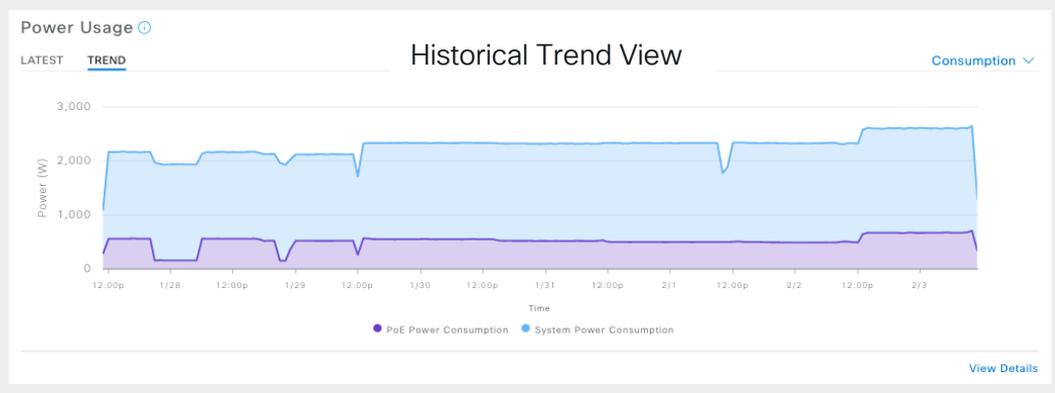


Realtime PoE consumption

Realtime Sys Power consumption

```
9300-2#sh power module
Automatic Module Shutdown : Enabled
Power Budget Mode = SP-PS
```

Mod	Model No	shutdown Priority	Power State	Budget	Instantaneous	Peak	Out of Reset	In Reset
1	C9300-24UX	4	accepted	505	139	139	505	50



Catalyst 9200, 9300 and 9400 starting IOS-XE 17.14.1

Select a data type below to filter the proceeding data

Top Location (Switch Count)

Global/SJC24-9410 (1)

Current data selected: **System Power Consumption**

Switch Table (1)

Search Table

Identifier	Switch Type	IP Address	Location	Total Power Allocation	Total Power Consumption	Power Load (%)
assur-sw-10.cisco.com	Cisco Catalyst 9300L Switch Stack	121.6.180.1	Global/SJC24-9410	715.0W	81.5W	11.4

Instantaneous System Power + PoE Consumption



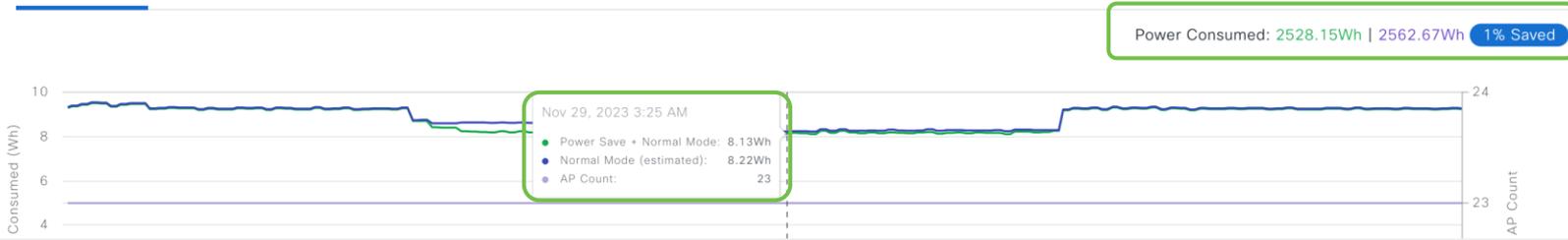
Power over Ethernet Analytics

AP Power Save Mode Distribution & AP Savings on Power Consumed

AP Power Savings

🕒 24 hours: Nov 28, 2023 3:03 PM - Nov 29, 2023 3:03 PM | 🌐 Global

Power Consumed



Identifier	Device Type	Switch Name	Switch Port	Total Power Consumed	Total Power Savings
Assurance_9130_3	Cisco Catalyst 9130AXI Unified Access Point	B18-live-C9200.wireless-tme.com	GigabitEthernet1/0/3	250.18Wh	--
SJC14-TME-AP11	Cisco Catalyst 9120AXI Unified Access Point	B18-live-C9200.wireless-tme.com	GigabitEthernet1/0/11	205.32Wh	10.47Wh
SJC14-TME-AP9	Cisco Catalyst 9120AXI Unified Access Point	B18-live-C9200.wireless-tme.com	GigabitEthernet1/0/12	209.32Wh	1.30Wh
Traffic_Assurance_01	Cisco Catalyst 9120AXI Unified Access Point	B18-live-C9200.wireless-tme.com	GigabitEthernet1/0/13	203.49Wh	8.92Wh

Stack PoE Insights in Device 360

Network > Device 360

Detail Information

Device Info Interfaces Fabric Site Virtual Network StackWise (4) **PoE** Power Supply

POWER SUMMARY
 Total Power Budget 6342.0W
 Allocated Power 1205.2W
 Remaining Power 5136.8W
 Power Allocation Load 19.0%

Overall Power Budget of 4 Switches in a Stack

Module Power Details (4)

Search Table

Power Budget of a Single Switch in a Stack

Chassis/Module ID	Total Power Budget	Allocated Power	Remaining Power	Power Allocation Load	Max Power Per Port	Total Ports	Used Ports	Free Ports	Last Seen
1/1	1800.0W	415.7W	1384.3W	23.1%	60.0W	48	24	24	Jul 22, 2021 11:40 AM
1/2	720.0W	138.6W	581.4W	19.3%	30.0W	24	8	16	Jul 22, 2021 11:40 AM
1/3	2382.0W	281.3W	2100.7W	11.8%	90.0W	48	26	22	Jul 22, 2021 11:40 AM
1/4	1440.0W	369.6W	1070.4W	25.7%	60.0W	24	8	16	Jul 22, 2021 11:40 AM

4 Records Show Records: 10

Overall Power Budget switches in a stack

Power Budget for each switch

PoE interfaces for each switch with detailed PoE info

POE CONFIG All Fast PoE UPOE+ Perpetual PoE Policing Four Pair ADMIN STATUS All Static Auto

POE OPER STATUS (SIGNAL PAIR) All On Off Off: PD Faulty Off: Power Denied Off: Error Disabled

Interface Name Admin Status **Operational Status** Time **IEEE PD Class (Signal/Spare)** **Powered Device Type** Powered Device Model Allocated

GigabitEthernet1/0/1	Static	On	Apr 26, 12:00 PM	IEEE4/NONE	IEEE PD	IEEE PD	16.0W
GigabitEthernet1/0/2	Auto	On	Apr 26, 12:00 PM	IEEE4/NONE	IEEE PD	IEEE PD	59.0W
GigabitEthernet1/0/3	Auto	On	Apr 26, 12:00 PM	IEEE4/NONE	IEEE PD	IEEE PD	59.0W

POE Oper Status

PD Class

Device Type

Device Info Interfaces **PoE** Power Supply

Power Stack (2)

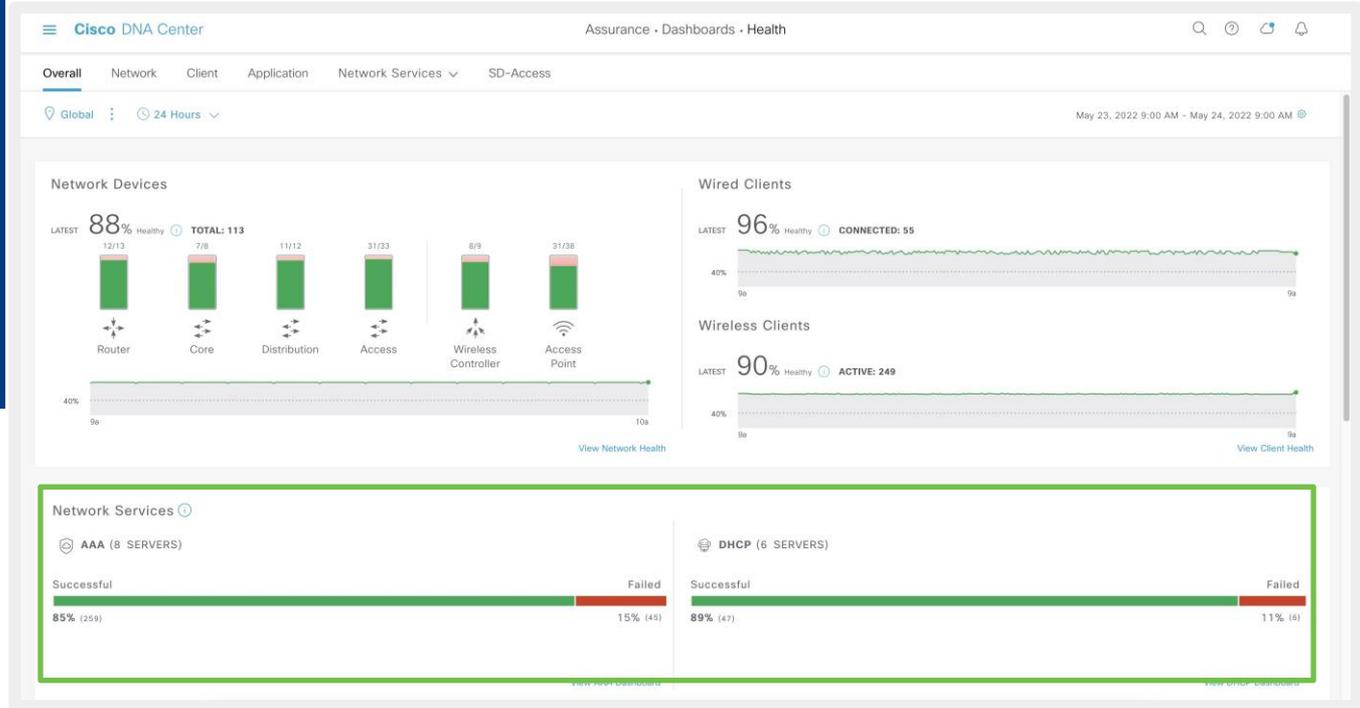
Search Table

Power Stack Name	Stack Mode	Stack Topology	Total Power	Reserved Power	Allocated Power	Switch Available Power	Power Consumed by System	Power Consumed by PoE
Powerstack-1	SP-PS	Standalone	1100W	0W	415W	685W	129W	12W
Powerstack-2	SP-PS	Standalone	1500W	0W	1284W	216W	139W	34W



Network Services Analytics - AAA/DHCP

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



Network Services Analytics – AAA/DHCP

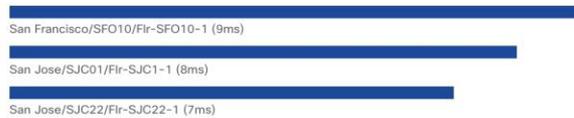
DHCP SUMMARY

6 Servers
210ms Average Latency -11.11%

DHCP TRANSACTIONS

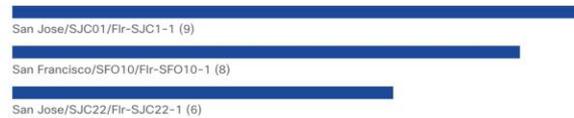
53 Total +54.55%
47 Successful +54.55%
6 Failed

Top Sites by Highest Latency



[View Details](#)

Top Sites by Transaction Failures



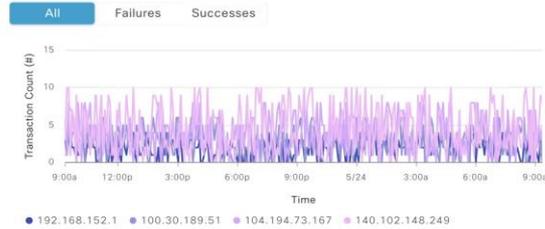
[View Details](#)

DHCP Server Latency



[View Details](#)

DHCP Server Transactions



- Dashlets' details for highest latency and highest number of transaction failures

Tracked by Network Services Analytics - AAA/DHCP



Reference

AAA

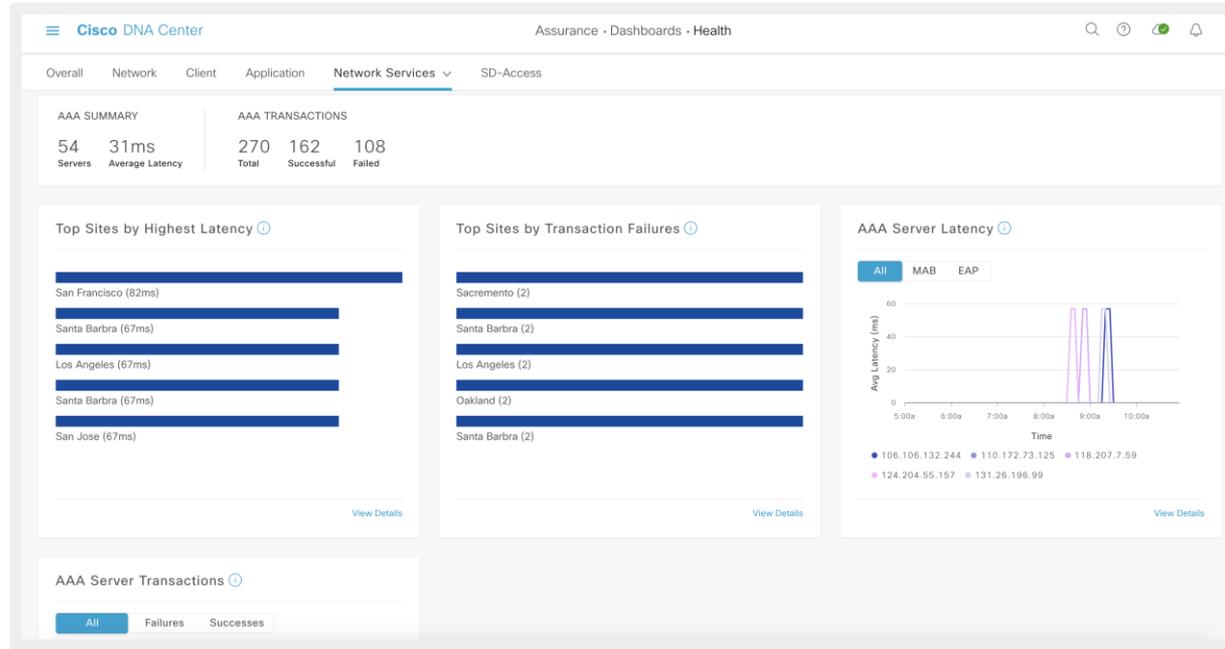
- AAA Servers
- AAA Server Latency
- AAA Server Transactions
- AAA Transaction Failures %
- Top Sites by Transaction Failures
- Top Sites by Highest Latency
- AAA Servers by WLC

DHCP

- DHCP Servers
- DHCP Server Latency
- DHCP Server Transactions
- DHCP Transaction Failures %
- Top Sites by Transaction Failures
- Top Sites by Highest Latency

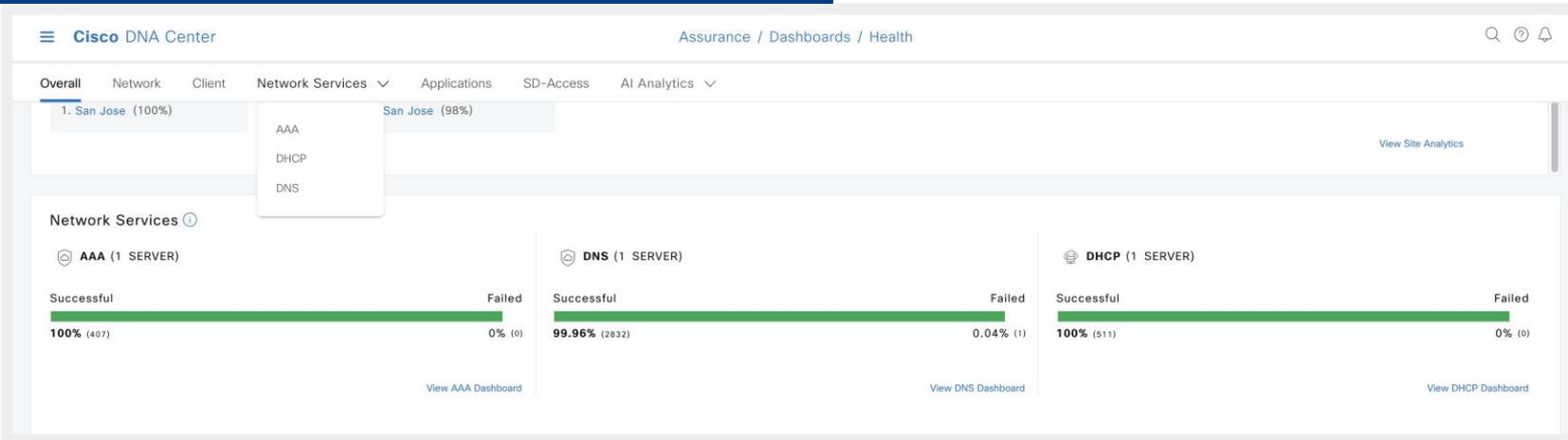
Network Services Analytics – AAA/DHCP

- 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



Network Services Analytics – DNS

- 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



Reference

DNS Summary information
of servers, average latency
, total transactions

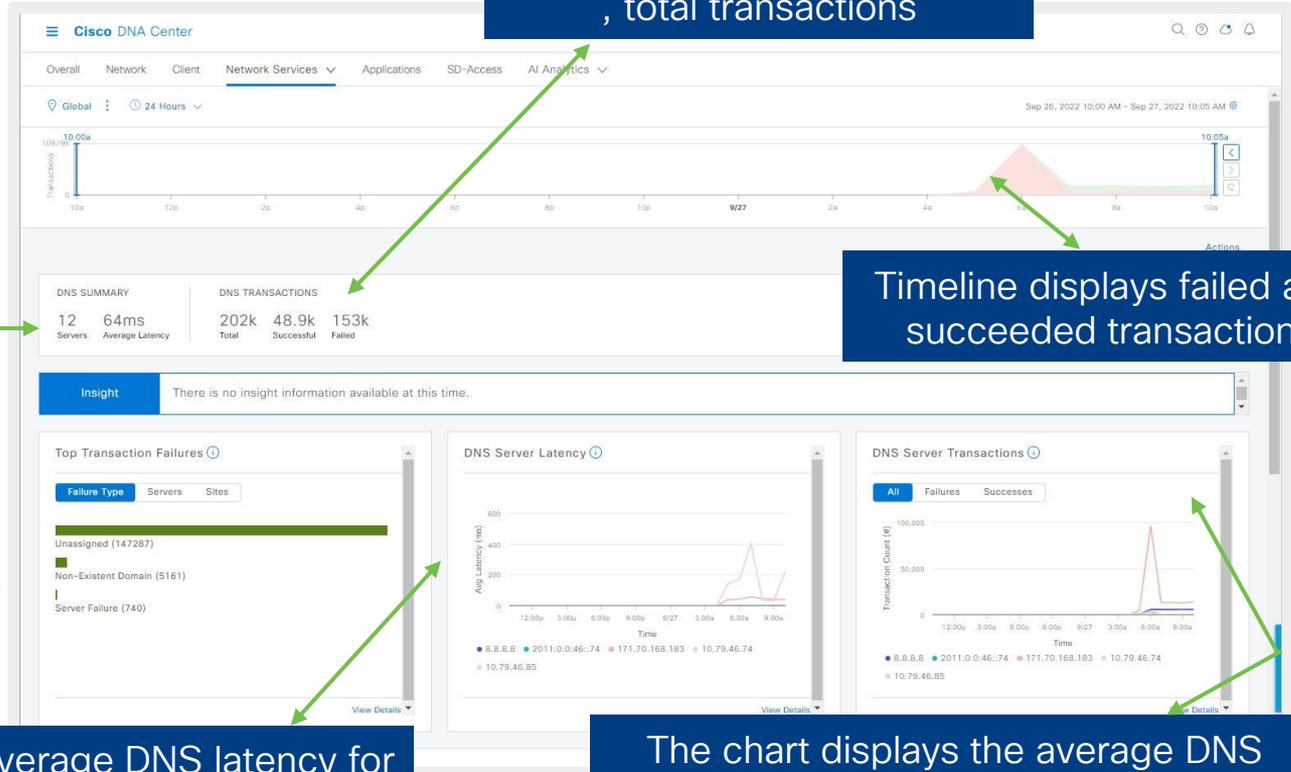
Count of DNS servers
and average latency
(in ms) of your
network.

Top DNS server
transaction failure types,
servers, and sites

Average DNS latency for
each DNS server.

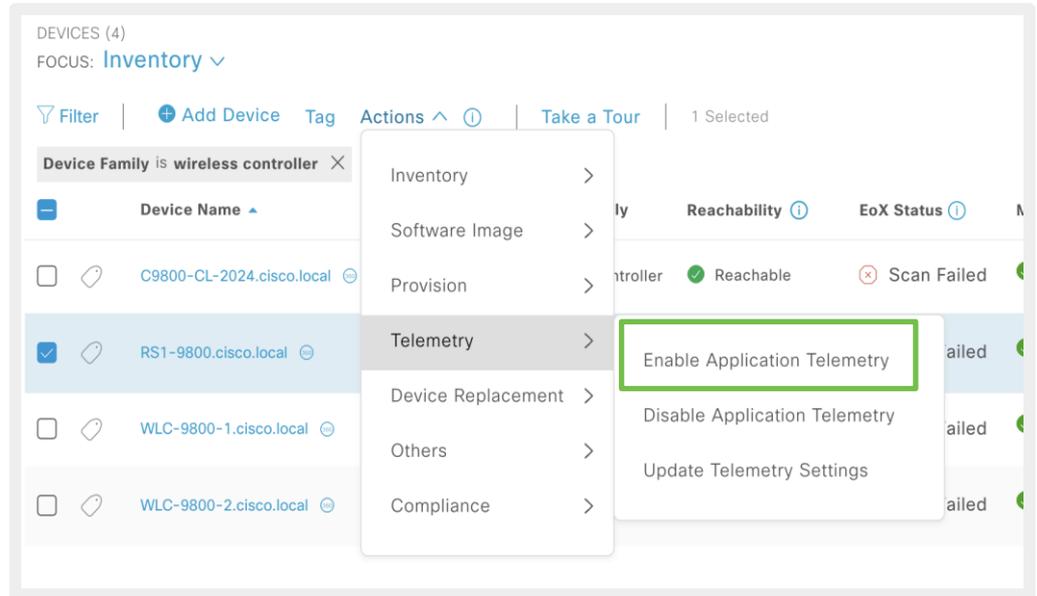
The chart displays the average DNS
server transactions status for each DNS
server reported by wireless controllers.

Timeline displays failed and
succeeded transactions



Network Services Analytics – DNS

- Supported in switches, routers and eWLC's.
- No support on AireOS WLC
- Minimum version IOS-XE 17.10
- Enabled via Application Telemetry



Network Services – DNS Dashboard



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
!
```

```
interface GigabitEthernet1/0/8
 description Description pushed by DNAC 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
```

C9300-24P

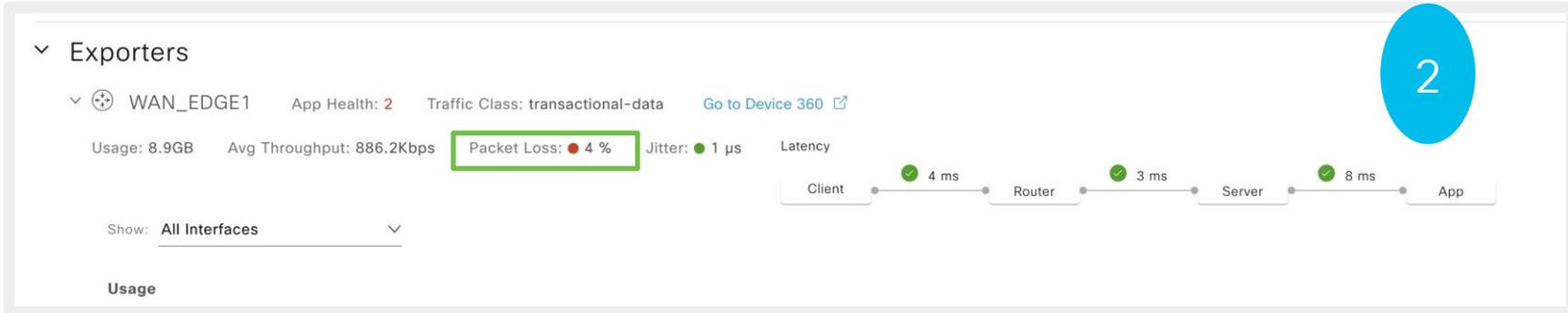
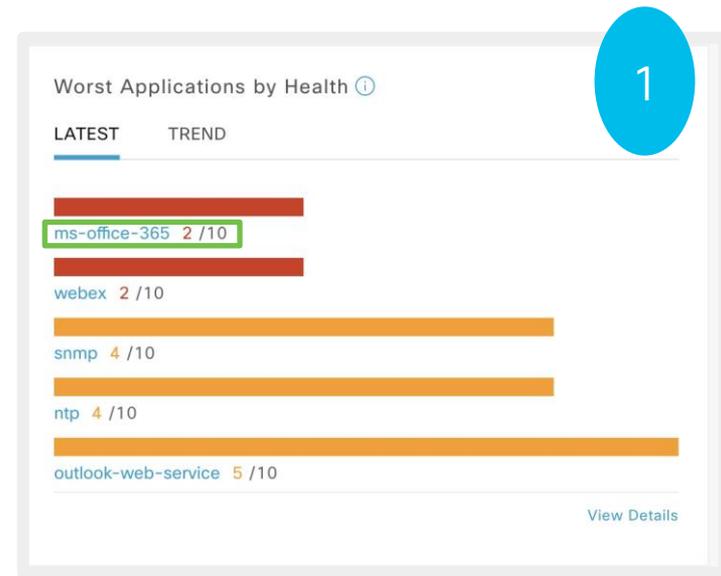
IOS-XE: 17.11.01

Cisco DNA Center

Version 2.3.5.3-70194

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

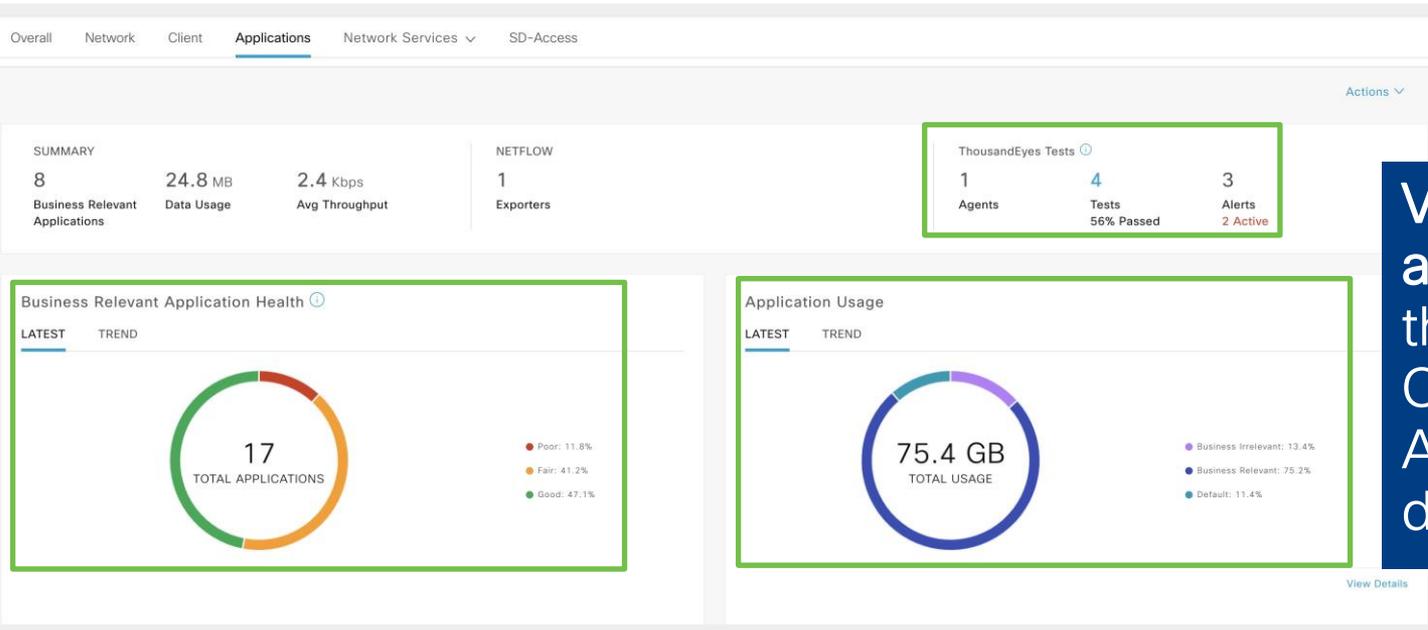
LATEST

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

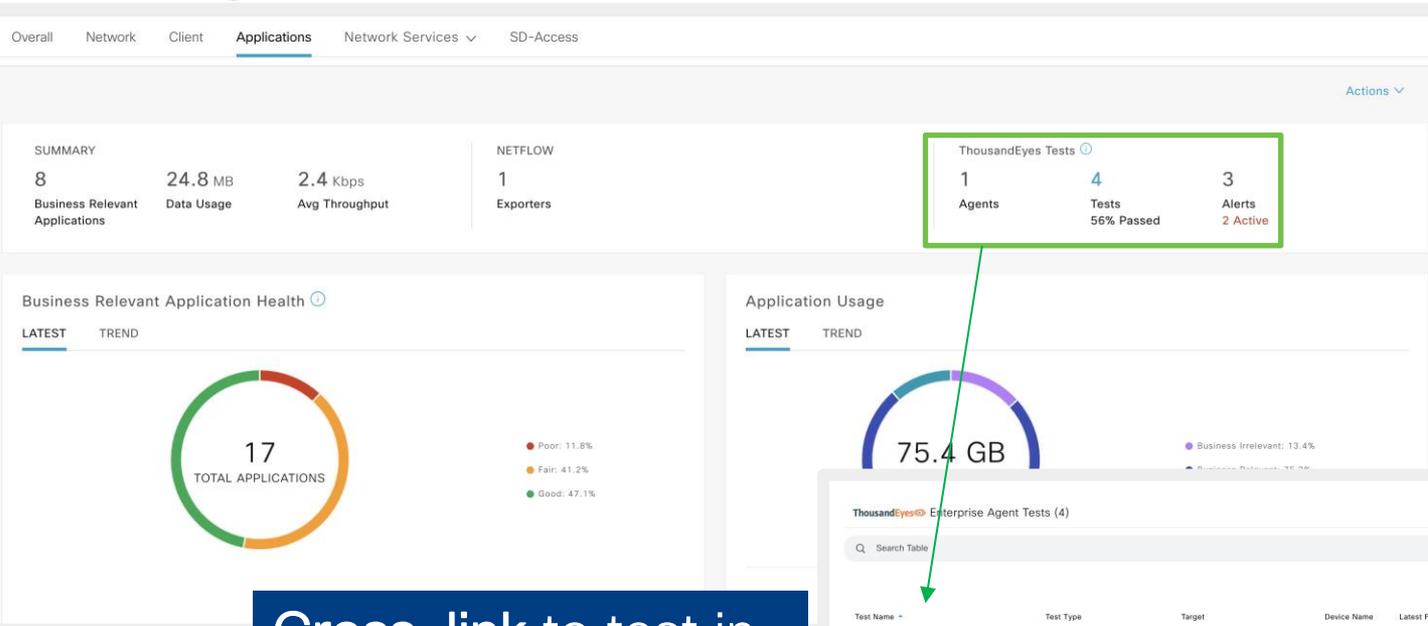
(*) New with Catalyst Center 2.3.5 and IOS-XE 17.10.1 or later with C91xx AP's

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 shows the Cisco DNA Center interface for a device named 'C9K-STACK'. The 'Compliance Summary' section displays several compliance checks:

- 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.

Callout boxes provide additional context:

- End of Sale & End of Life alerts:** Points to the EoX - End of Life check.
- Identify whether the startup and running configurations of a device are in sync:** Points to the Startup vs Running Configuration check.
- Violation of intent provisioned to a device through Catalyst Center:** Points to the Network Settings and Network Profiles checks.
- Difference in network settings compared to "Network Settings" in Design:** Points to the Network Settings check.
- Violation of application visibility intent provisioned to a device through CBAR and NBAR:** Points to the Application Visibility check.
- See if the tagged golden image is running on the device:** Points to the Software Image check.
- Check whether the devices are running without critical security vulnerabilities:** Points to the Critical Security Advisories check.

Compliance: Network Profiles - Switches

The screenshot displays the Cisco DNA Center interface for a switch named C9K-BRANCH-STACK. The breadcrumb path is 'All Devices / C9K-BRANCH-STACK'. The switch status is 'Reachable' and 'Managed'. Key details include 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 'Compliance Summary' section shows four items: 'Startup vs Running Configuration' (4 mins out of sync, 1 line removed), 'Network Profiles' (1 change, CLI Template: 1), 'Software Image' (17.08.01 Golden Image Version, Running Version: 17.8.1), and 'Critical Security Advisories' (0). The 'Network Profiles' item is highlighted with a green box.

Compliance Summary

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

- Startup vs Running Configuration** (4 mins since out of sync)
 - Compliance last run on: Sep 2nd, 2022, 03:01:30 PM
 - Lines added: 0
 - Lines removed: 1
 - Lines modified: 0
- Network Profiles** (1 Changes, CLI Template: 1)
 - Non-Compliant since Sep 2nd, 2022, 03:01:45 PM
 - Compliance last run on: Sep 2nd, 2022, 03:01:30 PM
- Software Image** (17.08.01 Golden Image Version, Running Version: 17.8.1)
 - Compliant since May 2nd, 2022, 03:53:28 PM
 - Compliance last run on: Sep 2nd, 2022, 03:01:30 PM
- Critical Security Advisories** (0)
 - Compliant since May 7th, 2022, 08:01:15 PM
 - Compliance last run on: Sep 2nd, 2022, 03:01:30 PM

Compliance: Network Profiles - Switches

Config pushed by Catalyst 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 Catalyst Center interface for a network profile named 'C9K-BRANCH-STACK'. The interface includes a navigation sidebar on the left with categories like 'Interfaces', 'Hardware & Software', and 'Configuration'. The main content area displays 'Compliance Summary / Network Profiles' for the selected device. It shows a 'CLI Template (1)' with a search bar and a table of 'CLI Deviations'. The table has columns for line numbers and CLI commands. A tooltip points to a red-highlighted row in the table, stating 'The highlighted text in red are the missing CLIs.' The table content is as follows:

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

Config Drift

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: **Sep 30, 2022** **Oct 15, 2022**

No. of Lines

Config Drift Days

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

Config Drift Version
CCA_C9K-TBRANCH-Std-Config Remove Label ✎

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
```

Config Drift Version
October 14, 2022 11:48 AM

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: lilia
Config Method: console
October 14, 2022 11:48 AM

Compliance: Network Profiles – Wireless

The screenshot displays the Cisco DNA Center interface for a device named **STL01-C9800-CL.dlab.local**. The breadcrumb navigation path is **All Devices / STL01-C9800-CL.dlab.local**. The device status is **Reachable** and **Managed**. Key details include IP Address: 172.16.255.35, Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud, Role: ACCESS, Uptime: 22 hrs 56 mins, and Site: Global/Canada/Quebec/Saint-Lambert/STL01.

The **COMPLIANCE** section is active, showing a **Summary** of compliance checks. The **Network Profiles** check is highlighted with a green box and shows a red status icon, indicating non-compliance. It reports: **Non-Compliant since Feb 9th, 2022, 02:38:20 AM**, **Compliance last run on: Apr 2nd, 2022, 11:16:36 AM**, and **3** total changes, consisting of **1 Model Config** and **1 Wireless** change.

Check Name	Status	Compliance Last Run	Details
Startup vs Running Configuration	Non-Compliant	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	Apr 2nd, 2022, 11:16:36 AM	3 total changes: 1 Model Config, 1 Wireless
Application Visibility	Compliant	Apr 2nd, 2022, 11:16:54 AM	0 Changes
Software Image	Compliant	Apr 2nd, 2022, 11:16:36 AM	Golden Image Version: 17.07.01; Running Version: 17.7.1
Critical Security Advisories	Compliant	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 main content area is titled "Compliance Summary / Network Profiles" and shows a "CLI Template (1)" tab selected. Below this, there is a "CLI Deviations" section with a search bar and a table of deviations. The table has two rows, both highlighted in red, indicating deviations from the template. The first row shows "ap dot11 24ghz SI" and the second row shows "ap dot11 5ghz SI". To the right of the table, there is a "Realize Template: Enabling SI" section with a refresh icon. The left sidebar contains navigation menus for "DETAILS", "SECURITY", and "COMPLIANCE", with "Summary" selected under "COMPLIANCE".

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

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 table lists network profiles, with 'Wireless (1)' highlighted by a green box. The table has columns for Model Name, Attribute, Status, Intended Value, and Actual Value. The row shows 'Wlan/BestCorpWl_Global_NF_e5f0c407' with Attribute 'FT Adaptive', Status 'Changed', Intended Value 'Adaptive', and Actual Value 'Disabled'. The status 'Changed' is highlighted in red. A search bar and a filter icon are visible above the table. The left sidebar shows navigation options under 'DETAILS', 'SECURITY', and 'COMPLIANCE'.

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/BestCorpWl_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 device is a Cisco Catalyst 9800-CL Wireless Controller for Cloud, with IP address 172.16.255.35. The interface shows a compliance summary for network profiles, specifically for wireless. A table lists one profile with a compliance issue: IPv4 DHCP Required is set to YES in the intended value but NO in the actual value.

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

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 C

Reachable Managed IP Adc

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	-	Acknowledge
<input type="checkbox"/>	DNS NR Settings	nameServers	Changed	173.37.137.85	-	Acknowledge

Showing 2 of 2

Fix Config Compliance Issues

The screenshot shows the Cisco DNA Center interface for a device named C9K-STACK. The device is a Cisco Catalyst 9300 Switch with IP address 10.85.54.54. The compliance summary shows the next check is scheduled for Jan 17, 2023, 02:50 PM. There are four violation cards:

- 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 Open Violations. General: 2.
- Network Profiles**: Non-Compliant since Oct 14th, 2022, 01:23:01 PM. Compliance last run on: Jan 17th, 2023, 02:55:24 PM. 1 Open Violation. CLI Template: 1.
- 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.

Fix Configuration Compliance Issues

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

Note: Routing, HA Remediation, Software Image, Security 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

Network Compliance Event Notification

- Config change generates a config drift in Catalyst Center
- Config drift will send an event through notification channels (version 2.3.7)
- Configurable per site
- Supported Channels: Email, REST, PAGERDUTY and Webex

Summary

Review your notification and make any changes. If you are satisfied, select "Finish" to complete this workflow

∨ Name and Description [Edit](#)

Name Config Drift Campus

Description Config Drift Campus

∨ Site and Events [Edit](#)

Sites (1) Global/Canada/Ontario/Toronto/TRN6

Events (1) Device config collection event

∨ Email Settings [Edit](#)

From DNAC-Toronto-lab@cisco.com

To (1) lroussea@cisco.com

Subject Config Drift Event

Network Compliance Event Notification



Reference

Sample email notification

Dear Cisco DNA Center Customer,
You are receiving this message due to the email notification preference(s) set by your Cisco DNA Center Administrator.
Here are the details about the event:

Event Name	NETWORK-DEVICES-CONFIG-COLLECT
Event ID	NETWORK-DEVICES-CONFIG-COLLECT
Event Type	NETWORK
Event Time	12-October-2022 12:30:51
IP Address	10.104.249.137
Category	OUT OF BAND
Client IP Address	10.61.42.13
DEVICEUUID	6d28e45-3d5-4d21-bb30-ec758012d3ea
Connection Mode	vty1
Triggered By	CONFIG_CHANGE_EVENT
Device User Name	admin

[View in Cisco DNA Center](#)

Sample Webhook notification

```
{
  "version": "1.0.0",
  "instanceId": "057a8e23-8e1a-467e-8285-d5a1ff43528f",
  "eventId": "NETWORK-DEVICES-CONFIG-COLLECT",
  "namespace": null,
  "name": "Device config collection event",
  "description": "Shows a config drift event across the selected list of devices.",
  "type": "NETWORK",
  "category": "INFO",
  "domain": "Know Your Network",
  "subDomain": "Devices",
  "severity": 5,
  "source": "EXTERNAL",
  "timestamp": 1677144361144,
  "details": {
    "IP Address": "10.106.190.100",
    "Category": "IN BAND",
    "Client IP Address": "Not Applicable",
    "DEVICEUUID": "107440ec-330f-4255-",
    "Connection Mode": "Not Applicable",
    "Triggered By": "Initial Archive",
    "Device User Name": "Not Applicable"
  },
  "ciscoDnaEventLink": "https://&lt;D;tails?deviceId=&deviceIds",
  "note": "To get more details, use AI",
  "context": null,
  "userId": null,
  "i18n": null,
  "eventHierarchy": null,
  "message": null,
  "messageParams": null,
  "parentInstanceId": null,
  "network": null,
  "dnacIP": "10.104.241.138"
}
```

D DNAC-Toronto-lab@cisco.com
To: Lila Rousseau (rousseau)

Dear Cisco DNA Center Customer,
You are receiving this message due to the email notification preference(s) set by your Cisco DNA Center Administrator.
Here are the details about the event:

Event Name	Device config collection event
Event ID	NETWORK-DEVICES-CONFIG-COLLECT
Event Type	NETWORK
Event Time	24-January-2024 16:01:04
IP Address	10.85.54.54
Category	IN BAND
Client IP Address	10.85.54.180
DEVICEUUID	82a8469c-a262-4c9c-af33-a7f3e524d97e
Connection Mode	vty1
Triggered By	Config Change Event
Device User Name	netadmin

[View in Cisco DNA Center](#)

General

for testing

Messages People (2) Content Meetings

Cisco DNA Center Notification

Source DNA	10.104.241.138
Center IP:	
Severity:	5
Category:	INFO
Timestamp:	2023-01-18 13:50:44
Issue Name:	Device config collection event
Issue Description:	Shows a config drift event across the selected list of devices.

[Cisco DNA Center Issue Details](#)

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



Reference

The screenshots illustrate the workflow for creating a configuration archive:

- Downloads:** Shows the file `Export_Configs-10_Feb_2022_18_04_00_353-oWF.zip` being prepared for archiving.
- Archive Utility:** A dialog box prompts for a password for the archive: "Please enter the password for 'Export_Configs-10_Feb_2022_18_04_00_353-oWF.zip'." The password field is masked with dots.
- Export_Configs-10...:** A file browser window showing the contents of the archive, which are organized into folders for each device IP address and their respective configurations.
- 10.85.54.54-C9K-...:** A file browser window showing the contents of a specific device's configuration folder, including files like `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`.

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

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

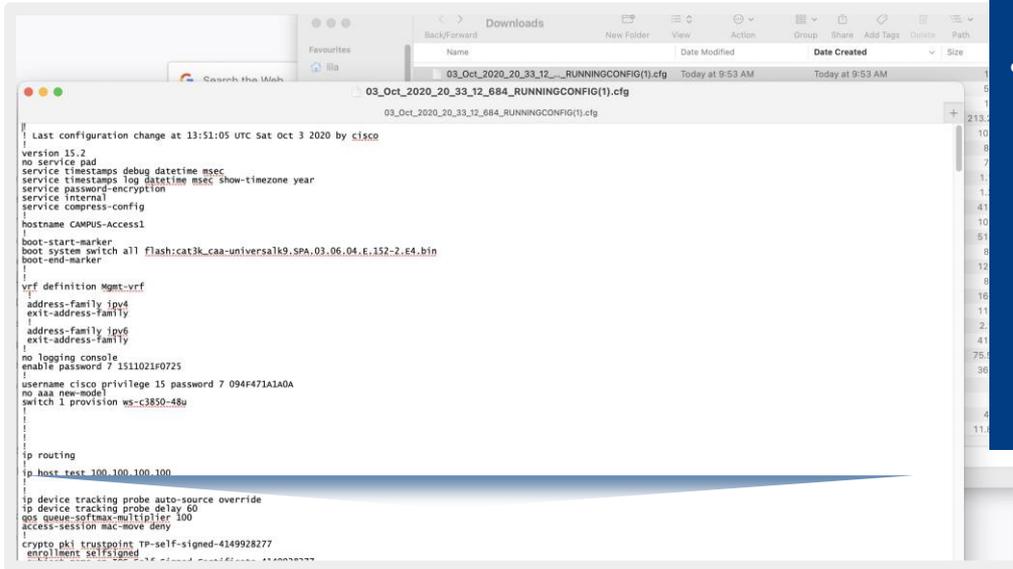
Device Configuration Management

API's to retrieve device configuration

- The API's available in Catalyst Center 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



The image shows a macOS file explorer window with a list of files in the Downloads folder. The selected file is '03_Oct_2020_20_33_12_684_RUNNINGCONFIG(1).cfg'. A preview window is open showing the contents of this file, which is a Cisco IOS configuration. The configuration includes details such as the last configuration change, version 15.2, hostname 'CAMPUS-Access1', and various network settings like VRF definitions, IP routing, and device tracking.

```
! 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
```

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

SWIM Demo

CISCO *Live!*



What you need to know about SWIM

Intent Based Network Upgrades



Golden-image driven to automate process and drive consistency

Trustworthiness Integration



Assures that device images are not compromised in any way.

Common Workflow



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

Upgrade Checks



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

Software Upgrade Recommendations

- To reduce the network downtime, it's recommended to perform [distribution and activation job separately](#)
- [Maintenance window](#) is typically required for activation
- Wireless
- Start with [ISSU, AP Pre-Image Download, Staggered Upgrade](#)
- Use [Rolling AP upgrades](#) were 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

Image Update

Devices (2) Focus: Software

imageNeedsUpdate: (outd...

1 Selected Add Device

Device Name

pnp-9800

WLC9800.adamlab.c...

1 Selected Update ISSU

Device To Image Comment

pnp-9800 (10.10.10.148) C9800-CL-universalk9.17.09.03.S PA.bin ISSU ISSU Validation Successful Update Readiness Report

Enable ISSU Update

Disable ISSU Update

Image Update

1 Analyze Selection 2 Distribute 3 Activate 4 Schedule and Clean Up 5 Summary

Analyze Selection

Before you proceed for the Update, analyze your selection.

Devices to Update: 1 Device Family: 1 Sites: 1

Search Table

1 Selected Update ISSU

Device From Image To Image Comment

pnp-9800 (10.10.10.148) C9800-CL-universalk9.17.09.02.S PA.bin C9800-CL-universalk9.17.09.03.S PA.bin ISSU ISSU Validation Successful Update Readiness Report

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 A.bin	C9800-CL-universalk9.17.09.03.SP A.bin ISSU	<input checked="" type="checkbox"/> 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 version 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

Device Name	Device Type
172.100.1.54	Wireless Controller
New-Cat9300-Stack-Switch (192.168.120.20)	Switch
9800_SWIM (172.100.1.54)	Wireless Controller
New-Cat9300-Stack-Switch (192.168.120.20)	Switch
9800_SWIM (172.100.1.54)	Wireless Controller

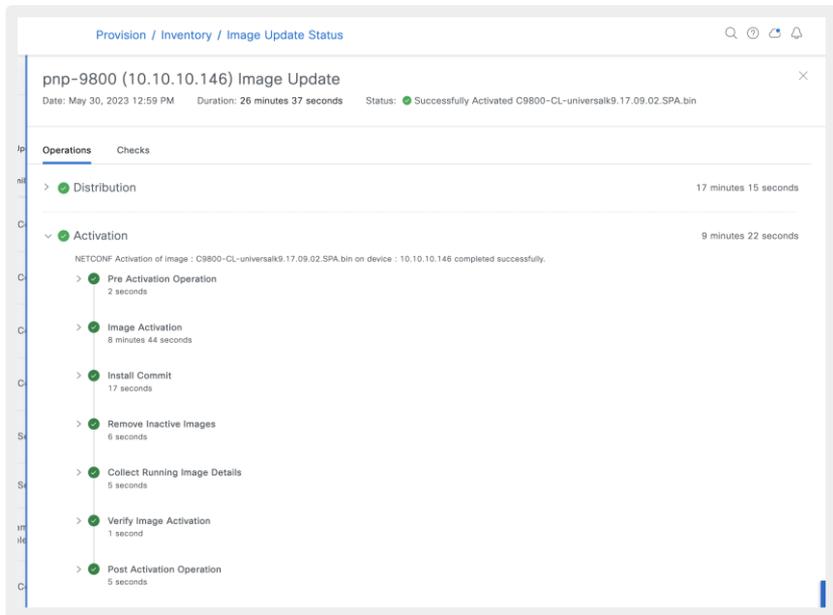
Operations

- > ● Image Checksum Verification On Device (40 seconds)
- > ● Unpack Images (2 minutes 30 seconds)
- > ● AP Pre-Image Download (8 minutes 6 seconds)
- > ● Activation (13 minutes 15 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 for normal wireless vs ISSU wireless



Provision / Inventory / Image Update Status

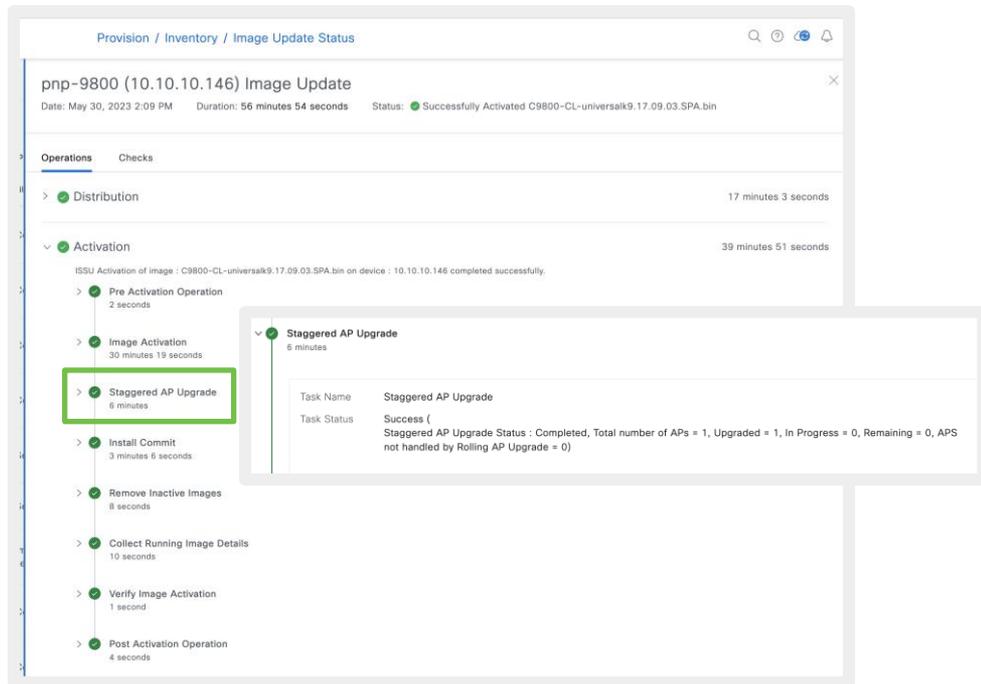
pnp-9800 (10.10.10.146) Image Update

Date: May 30, 2023 12:59 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 6 seconds
 - Remove Inactive Images 8 seconds
 - Collect Running image Details 10 seconds
 - Verify Image Activation 1 second
 - Post Activation Operation 4 seconds

Staggered AP Upgrade
6 minutes

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



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
-----
```

Software Maintenance Update (SMU) support

The screenshot shows the Cisco Catalyst 9300 Switch Image Repository interface. On the left, there is a sidebar with navigation options: SUMMARY, Roles & Tags, Major Versions, Golden Images, and Recommendation. The main area displays a list of images (35) with a search filter. A table lists image details, with a green box highlighting the 'Version' column for the image 'cat9k_iosxe.17.09.04.SPA.bin', showing '17.09.04.0.5180' and 'Add On (1)'. A green arrow points from this box to a detailed 'Add On List (1)' window. This window shows 'BASE IMAGE INFORMATION' (Family: Cisco Catalyst 9300 Switch, Image Name: cat9k_iosxe.17.09.04.SPA.bin) and a list of add-ons. The 'PSIRT SMU (1)' tab is selected, showing details for 'cat9k_iosxe.17.09.04.CSCwh87343.SPA.smu.bin'. A green box highlights the 'Golden Image' status, which is 'Not Available' with the message: 'This PSIRT SMU can't be golden tagged because base image is not tagged with role ALL.' Other add-on attributes include Description (Cisco IOS-XE Patch package), Defects, CVEID(S), Reboot Required (Yes), Category (bulk-patch), Supercedes (Not Available), Compliant Devices (Not Available), and Image Verification (Verified).

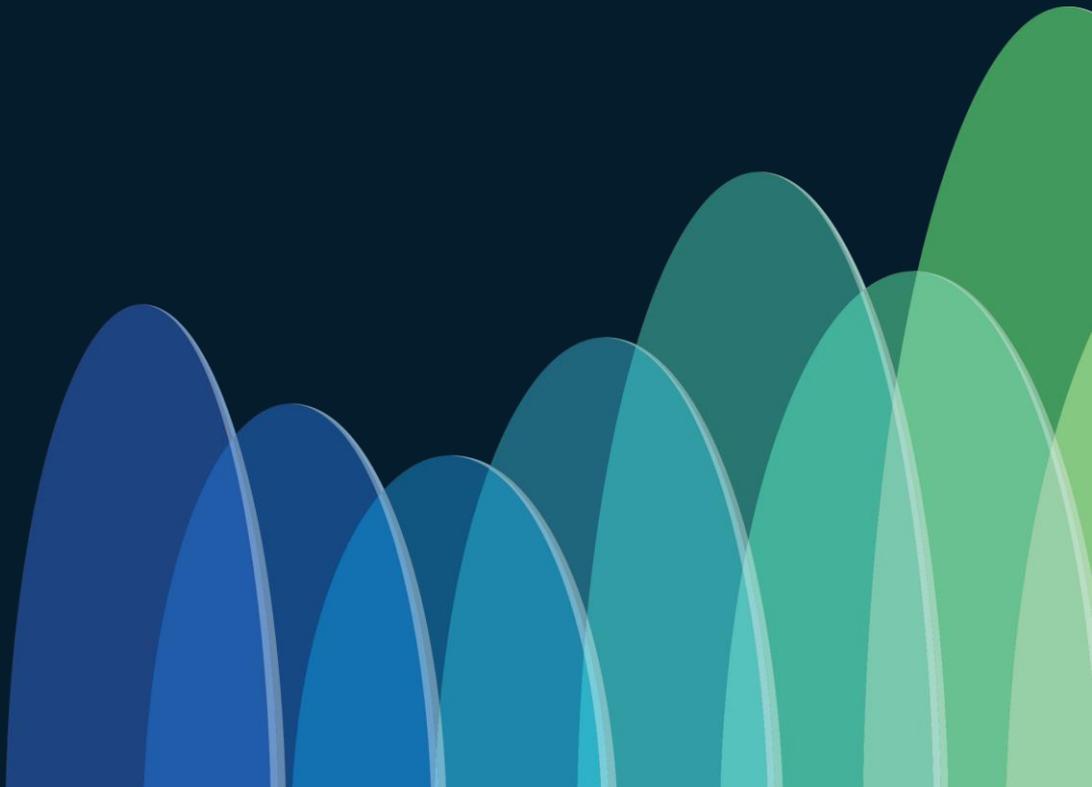
Need to mark as golden (along with main image)

Downloadable direct from CCO

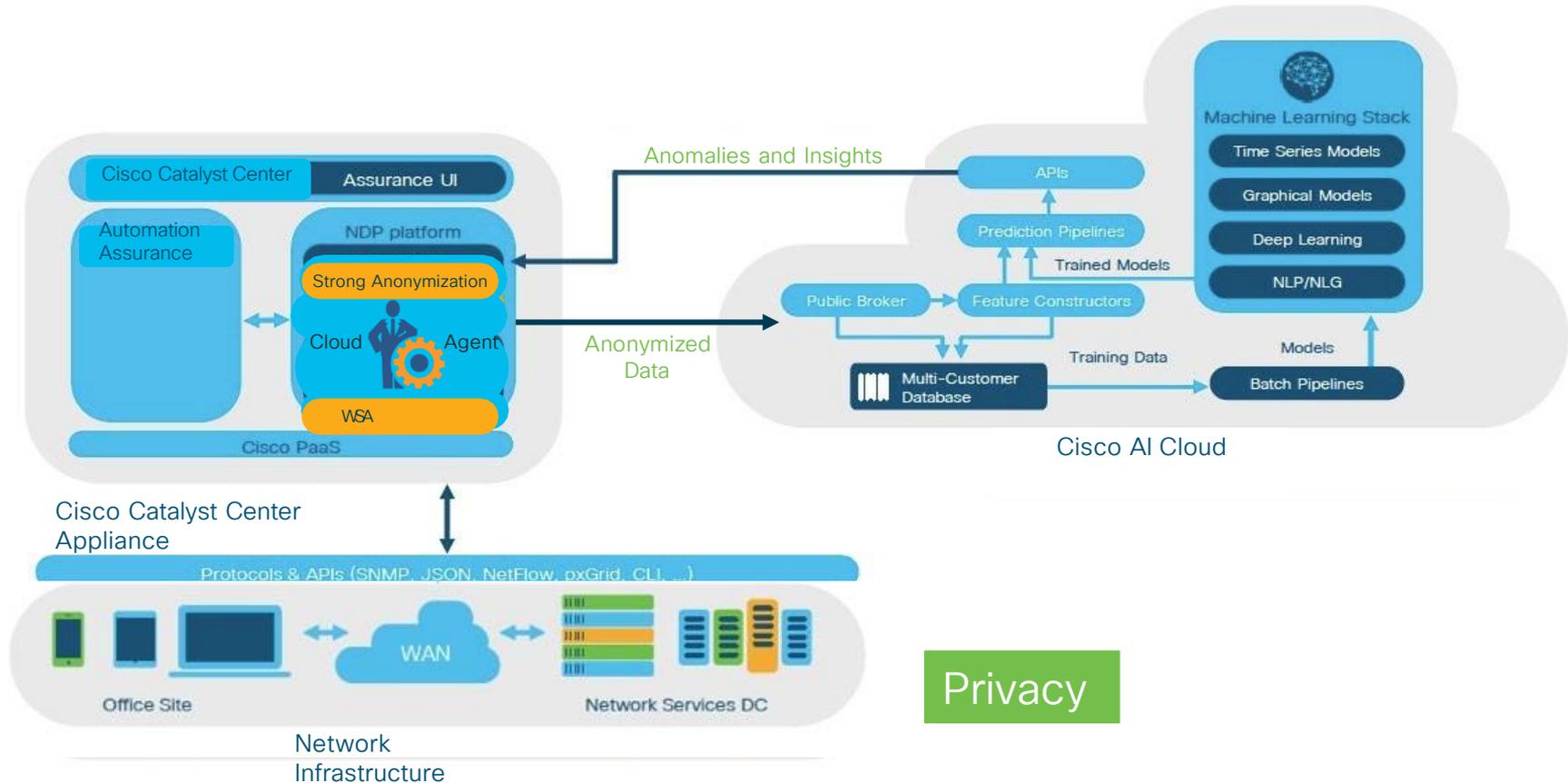
Wireless APSP and APDP are also supported (9300 EWC – SDA Mode)

AP service pack and device pack manual download from CCO/upload

Habit #5 - Explore 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:



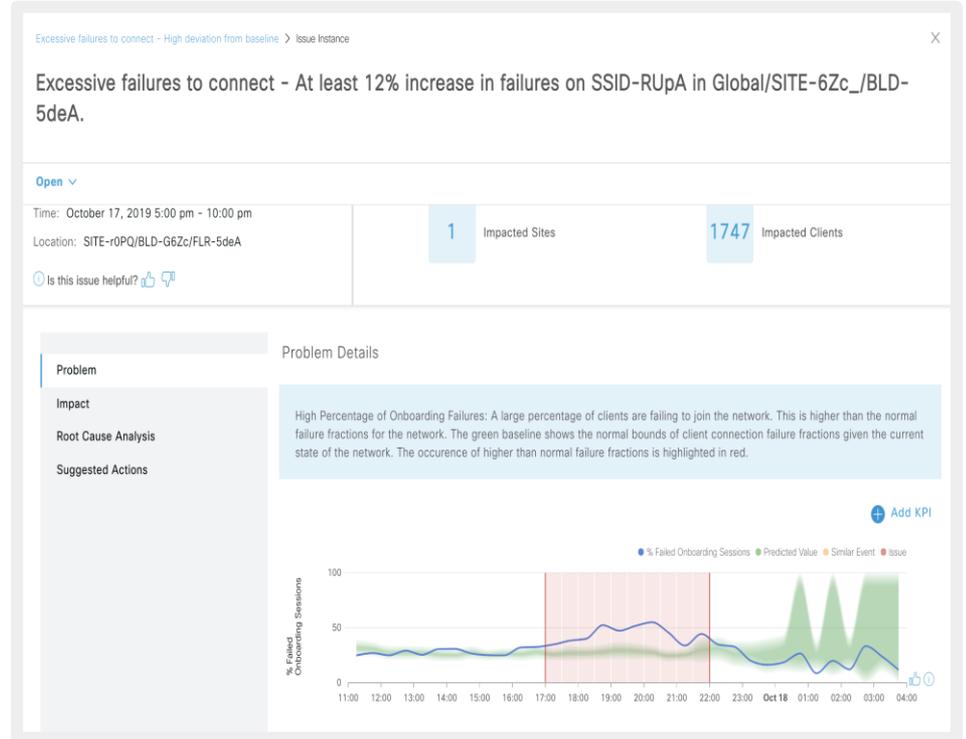
View Dynamic baselines and deviations for 12 (onboarding + throughput) KPI's



Accelerated troubleshooting with end-2-end workflow complete with impact and potential root cause details



Active feedback loop (thumbs 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.



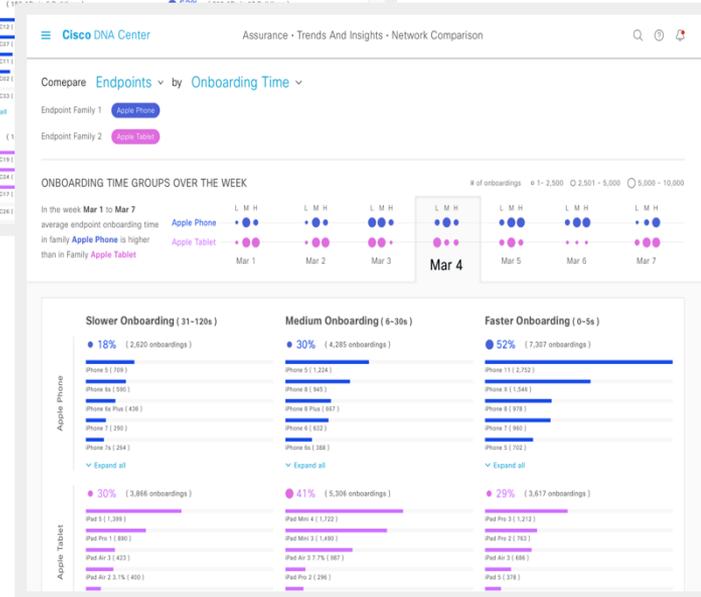
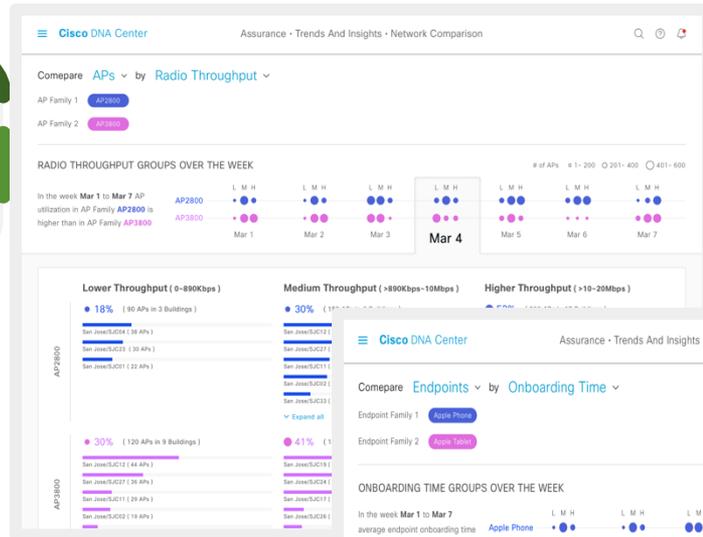
Flexibility to compare both on-boarding and throughput KPI's



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

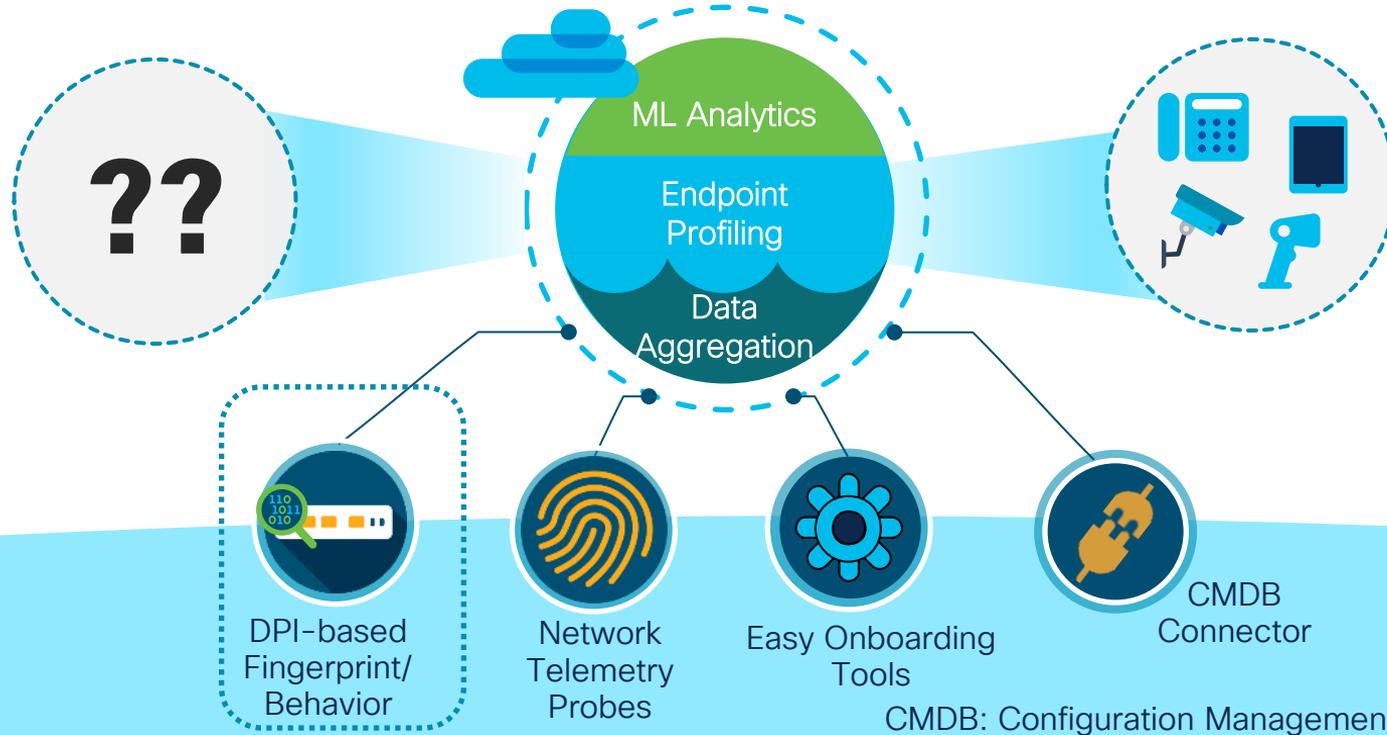


View and compare onboarding KPIs for specific device types for days of a week..

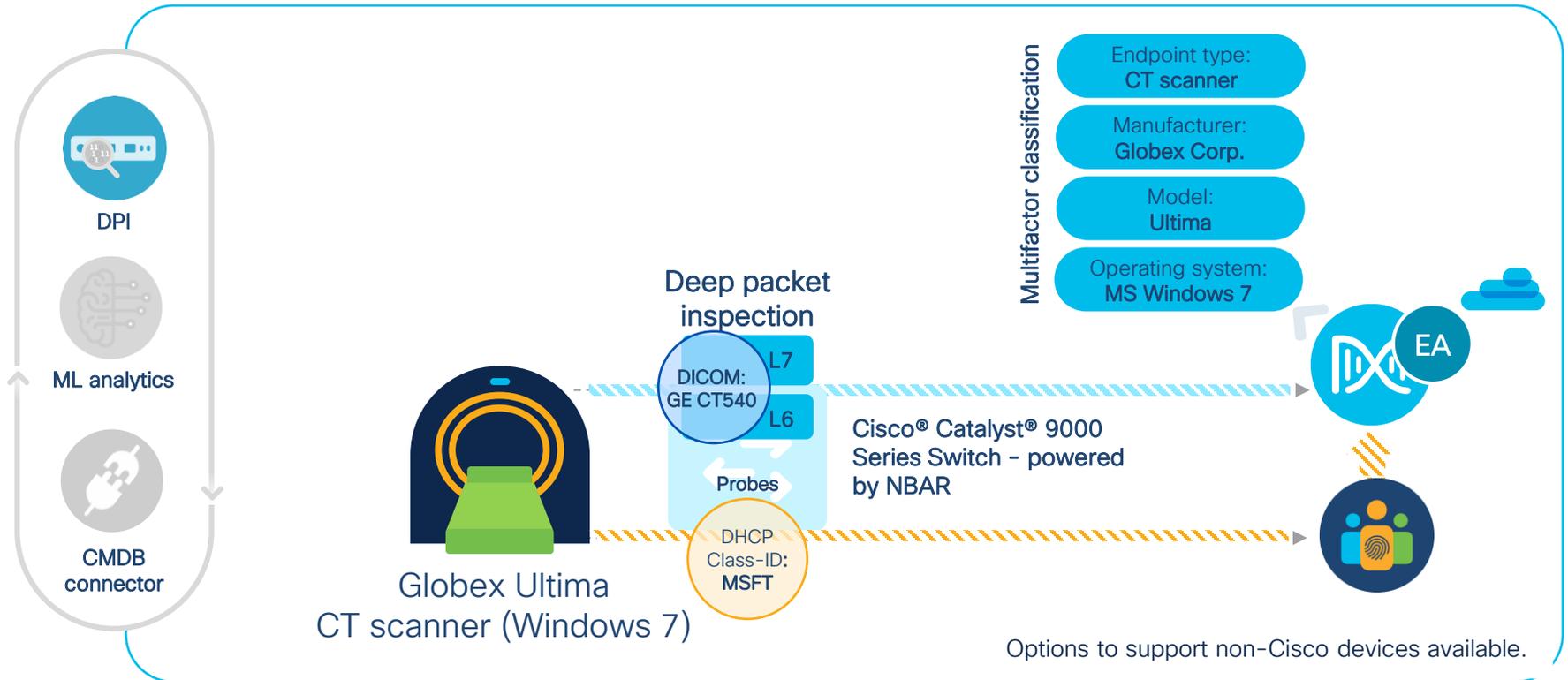


AI Endpoint Analytics on Cisco Catalyst Center

Rapidly reducing the unknowns by aggregating data from different sources



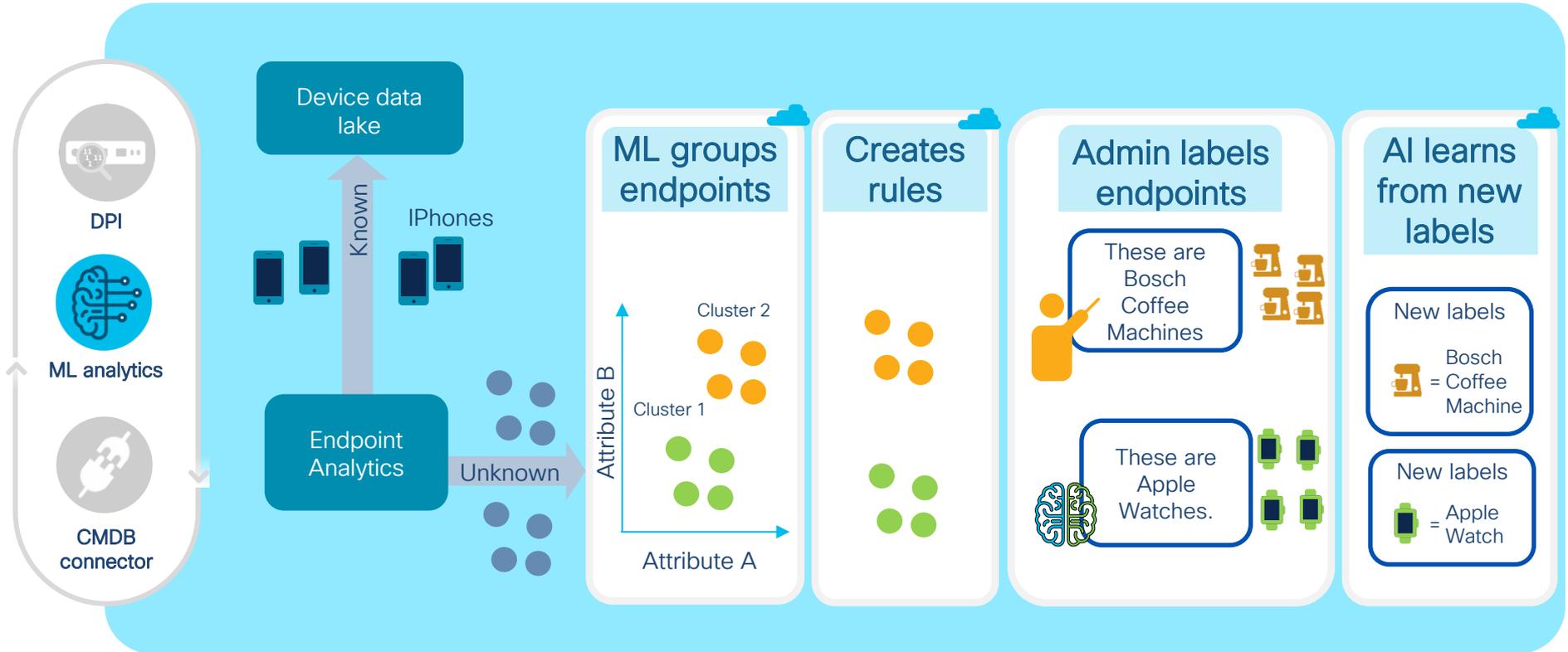
Classification based on Deep Packet Inspection (DPI)



Reducing Unknowns with Machine Learning

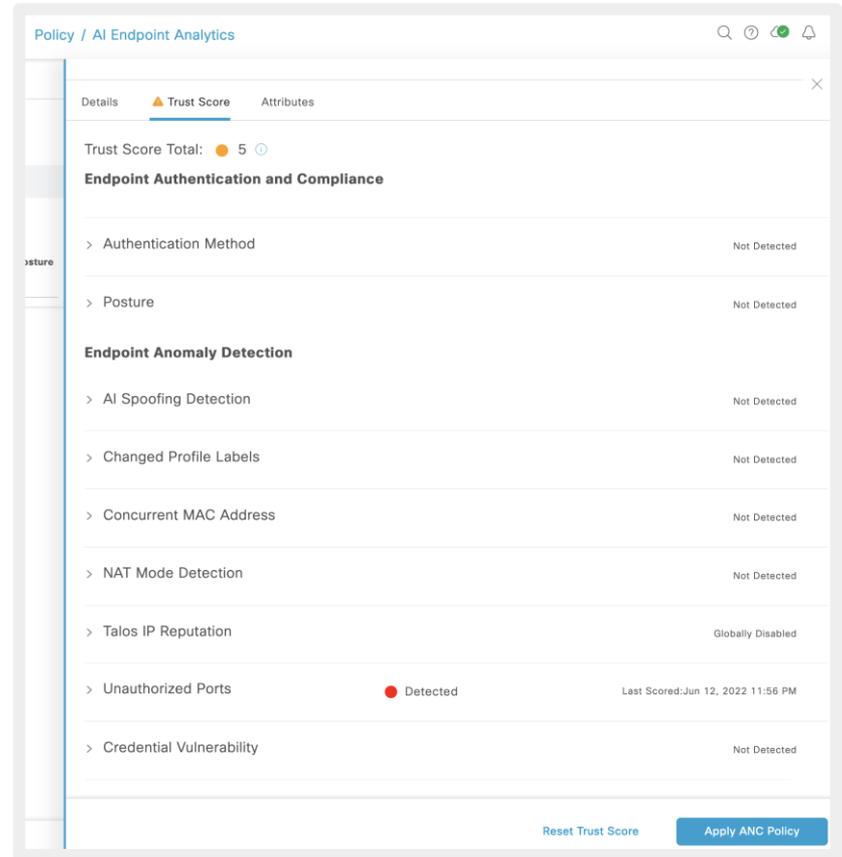
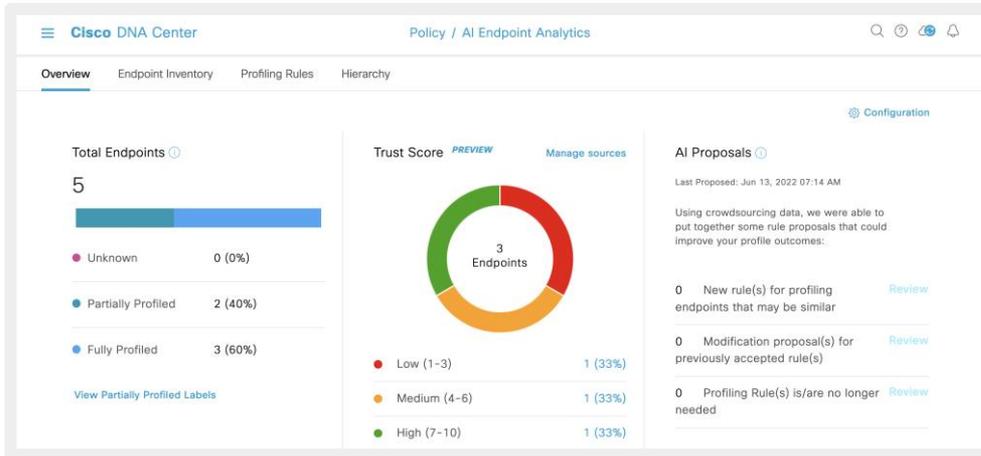


Reference



= done in cloud

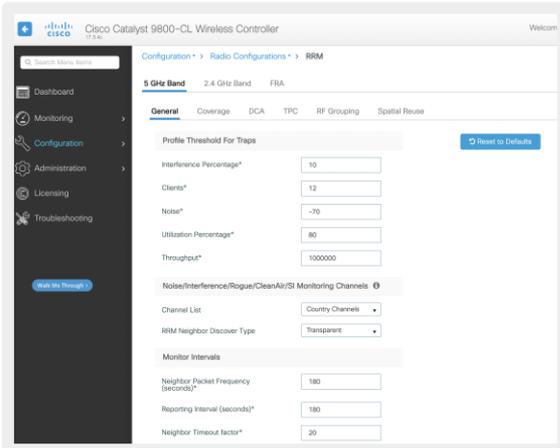
Trust Scores and Remediation



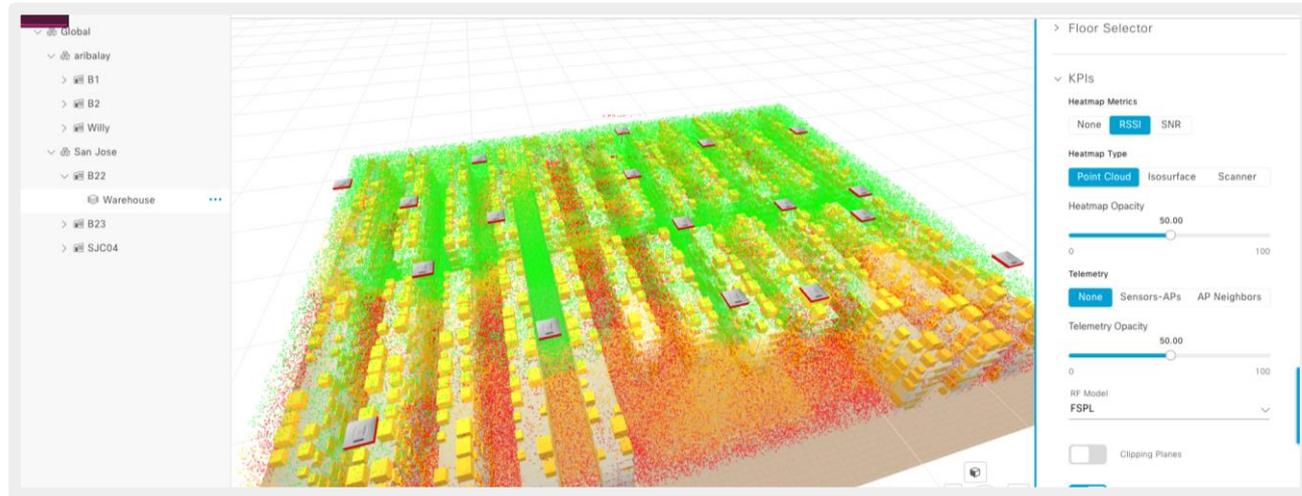
Adaptive Network Control - ANC

Remediate the host via Identity Services Engine - ISE

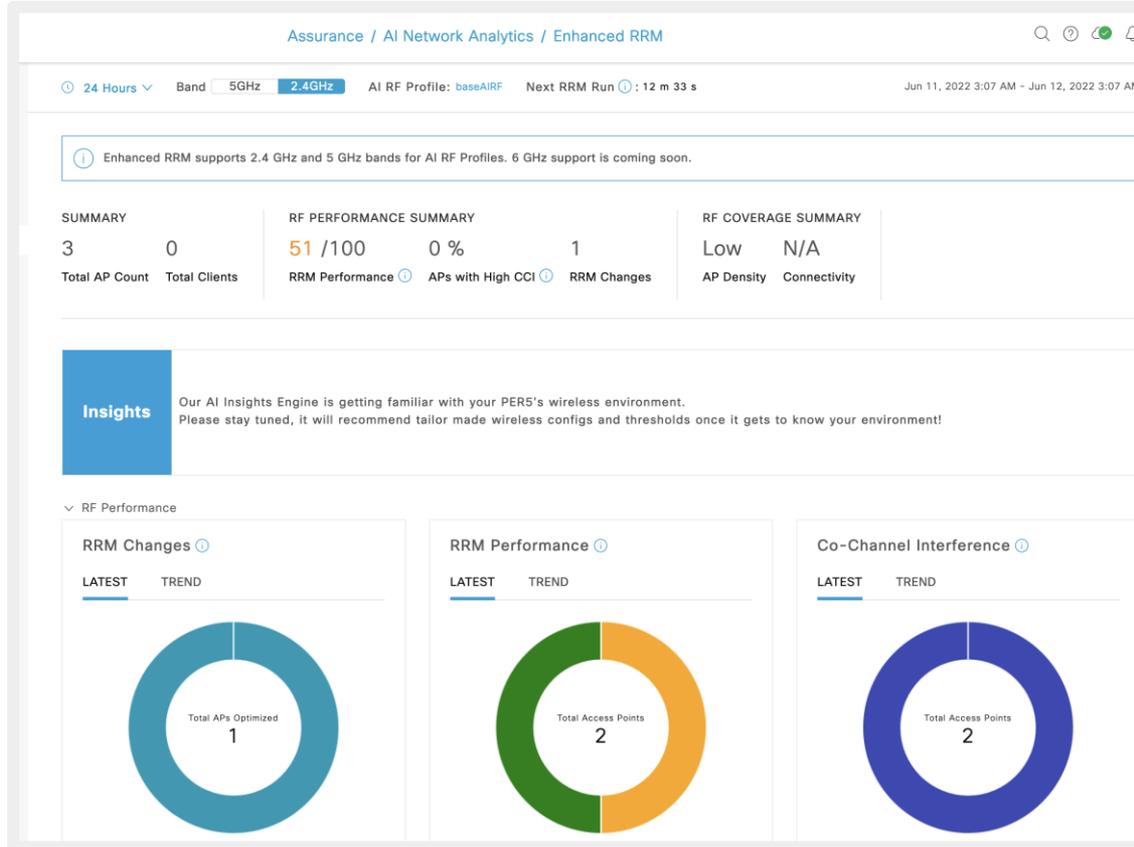
Why radio resource management



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



Dashboard



2.3.7.4 Supports "brownfield" 9800 Deployments

The screenshot shows the Catalyst Center web interface. At the top left is the Cisco logo and 'Catalyst Center' text. At the top right is the page title 'Configure AI-Enhanced RRM'. The main content area is titled 'Select Deployment Type' with a subtitle 'Select how you would like to deploy AI-Enhanced RRM'. There are two radio button options:

- Enable Without Device Provisioning** (selected): This flow enables AI-Enhanced RRM without provisioning your wireless controllers or access points from Catalyst Center. You may provision using your choice of tool or WLC WebUI or CLI. If you do not want Catalyst Center to manage the configuration of your devices, choose this option.
- Enable With Device Provisioning**: This flow enables AI-Enhanced RRM and requires your wireless controllers and access points to be provisioned by Catalyst Center. If you would like Catalyst Center to have full control over the manageability of your devices, choose this option.

Habit #6 – Secure Devices and Users (AAA & ISE)

Identity Services Engine

The screenshot shows the Cisco DNA Center interface. The top navigation bar includes the Cisco DNA Center logo and the path 'System / Settings'. A search bar is on the left. The main content area is titled 'Authentication and Policy Servers' and contains a table of configured servers. The table has columns for IP Address, Protocol, Type, Status, and Actions. One ISE server is highlighted in blue.

Settings / External Services

Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

[Add](#) [Export](#) As of: Apr 23, 2023 4:08 PM

IP Address	Protocol	Type	Status	Actions
10.10.10.130	RADIUS	AAA	ACTIVE	...
10.66.104.67	RADIUS	ISE	ACTIVE	...
10.10.10.120	RADIUS	AAA	ACTIVE	...

Only one ISE integration can be done per Catalyst Center.

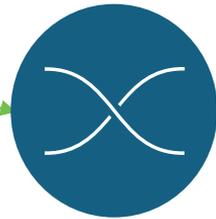
Other AAA servers can be added, but as an AAA server only (even if they are ISE servers)

Difference between ISE and AAA integration

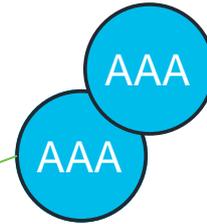


ISE

- Catalyst Center discovers the PSN nodes
- AAA config pushed to devices during site assignment
- PnP will add network device as a NAD to ISE
- PxGrid:
 - Provides Username for wired devices
 - Device attributes for AI endpoint analytics
 - Micro-segmentation for SDA



Cisco
Catalyst
Center



AAA config pushed to devices
during site assignment

Pre-requisites for ISE integration

ISE API needs to be enabled – ERS read write

No proxy server between ISE and Catalyst Center

PxGrid needs to be enabled on ISE

FQDN is required for the integration, not just an IP address (certificate)

If using Enterprise issued Certificate, need VIP + real IP for Catalyst Center Cluster

CLI credentials on ISE no longer used for integration. API only

IP reachability required

Site Settings for AAA

The screenshot shows the Cisco DNA Center interface for configuring AAA settings. The breadcrumb path is "Design / Network Settings". The "Network" tab is selected in the top navigation bar. On the left, a search bar "Find Hierarchy" is present, and a tree view shows the hierarchy: Global > AUS > brownfield > C > CLMEL > DC - syd > deak > EK > flex_area > HongKong > nirvana > NZ > PIM > spécial > stores > test > thirdwheel. The main content area contains a descriptive paragraph: "Configure AAA, NTP, and Image Distribution (SFTP) servers using the 'Add Servers' link. Once devices are discovered, Cisco DNA Center will deploy using these settings." Below this is the "AAA Server" configuration section, which is divided into "NETWORK" and "CLIENT/ENDPOINT" tabs. The "Client/Endpoint" tab is currently selected. Each section has radio buttons for "ISE" and "AAA", and "RADIUS" and "TACACS" protocols. The "RADIUS" protocol is selected in both sections. Each section also has a field for "IP Address (Primary)" with a dropdown menu showing "10.10.10.127" and a plus sign to add more addresses. A "Change Shared Secret" link is provided for each section.

Sample Config

```
authentication convert-to new-style
ip radius source-interface GigabitEthernet1/0/23
aaa new-model
aaa session-id common
aaa group server radius dnac-client-radius-group
  server name dnac-radius_10.10.10.127
  ip radius source-interface GigabitEthernet1/0/23
  exit
aaa group server radius dnac-network-radius-group
  server name dnac-radius_10.10.10.127
  ip radius source-interface GigabitEthernet1/0/23
  exit
aaa accounting identity default start-stop group dnac-client-radius-group
aaa accounting update newinfo periodic 2880
aaa accounting exec default start-stop group dnac-network-radius-group
aaa authorization exec default local
aaa authorization network default group dnac-client-radius-group
aaa authorization network dnac-cts-list group dnac-client-radius-group
aaa authorization exec VTY_author group dnac-network-radius-group local if-
authenticated
aaa authentication login default local
aaa authentication dotlx default group dnac-client-radius-group
aaa authentication login dnac-cts-list group dnac-client-radius-group local
aaa authentication login VTY_authen group dnac-network-radius-group local
dotlx system-auth-control
```

```
authentication radius server dnac-radius_10.10.10.127
  address ipv4 10.10.10.127 auth-port 1812 acct-port 1813
  pac key *****
  retransmit 3
  timeout 4
  automate-tester username dummy ignore-acct-port probe-on
  exit
radius-server vsa send authentication
radius-server vsa send accounting
radius-server dead-criteria time 5 tries 3
radius-server deadtime 3
radius-server attribute 31 send nas-port-detail mac-only
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 25 access-request include
radius-server attribute 8 include-in-access-req
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
cts authorization list dnac-cts-list
line vty 0 15
  login authentication VTY_authen
  authorization exec VTY_author
aaa server radius dynamic-author
client 10.10.10.127 server-key *****
client 10.66.104.67 server-key *****
exit
```

Device AAA and Site AAA interaction

Device has AAA configured	Site has AAA defined	Provisioning Workflow Success
		
		
		
		

Note: If just client/device AAA, then all will work.
Network AAA is the issue – due to lockout concerns (NAD entry in ISE)

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

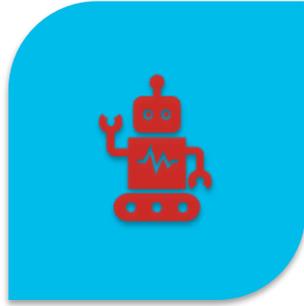


**DRIVE FOR
SHOW
AND
PUTT FOR
DOUGH**

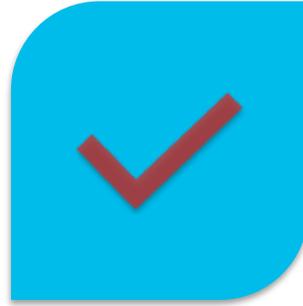


**GUI FOR
SHOW
AND
API FOR
DOUGH**

Why API?



AUTOMATI
ON



INTEGRATIO
N



INNOVATIO
N

API First 2.3.7.6 release notes

Table 6. New and Changed Features in Catalyst Center Platform, Release 2.3.7.7

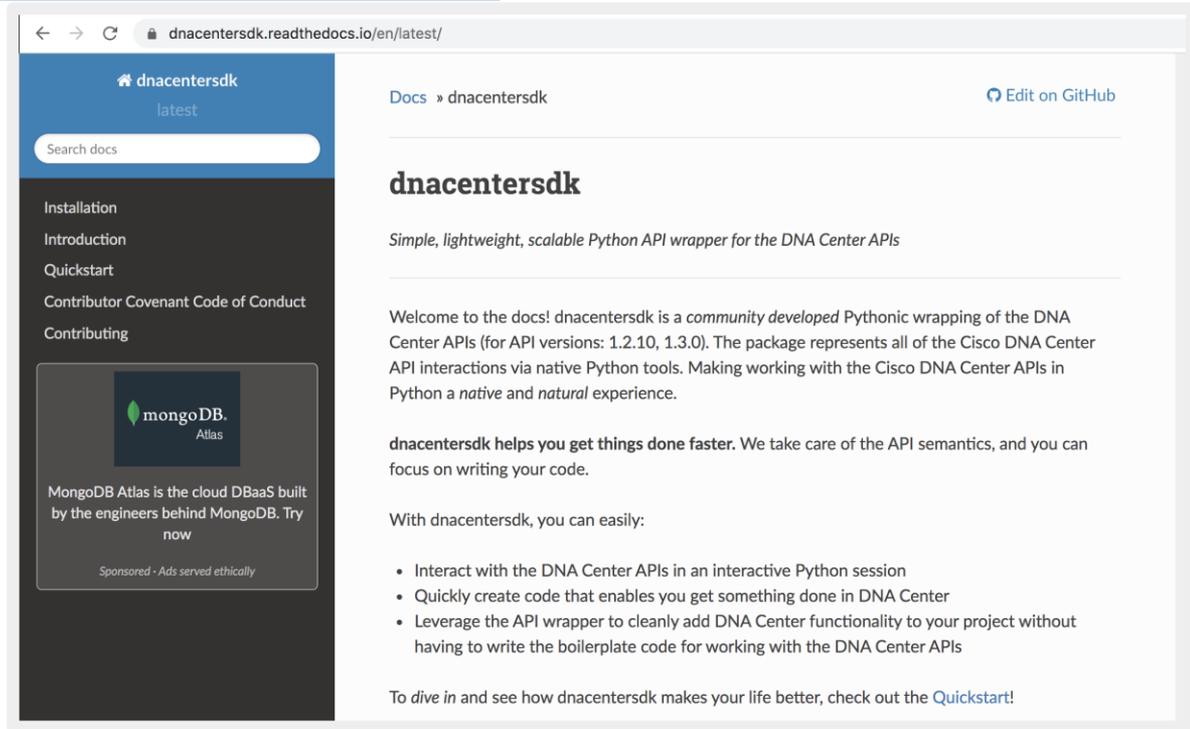
Feature	Description
New APIs	
Compliance API	<p>Catalyst Center platform supports the following Compliance API:</p> <ul style="list-style-type: none"> POST <cluster-ip>/dna/intent/api/v1/compliance/networkDevices/\${id}/issues/remediation/provision Compliance Remediation <p>To access the new Compliance API, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Know Your Network drop-down list and choose Compliance.</p>
Issues APIs	<p>Catalyst Center platform supports the following Issues APIs:</p> <ul style="list-style-type: none"> POST <cluster-ip>/dna/intent/api/v1/issues/resolve Resolve the given list of issues. POST <cluster-ip>/dna/intent/api/v1/issues/ignore Ignore the given list of issues. POST <cluster-ip>/dna/intent/api/v1/issues/\${id}/update Update the given issue by updating selected fields. <p>To access the new Compliance API, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Know Your Network drop-down list and choose Issues.</p>
Licenses APIs	<p>Catalyst Center platform supports the following Licenses APIs:</p> <ul style="list-style-type: none"> PUT <cluster-ip>/dna/intent/api/v1/licenseSetting Update license setting. GET <cluster-ip>/dna/intent/api/v1/licenseSetting Retrieve license setting. <p>To access the new Licenses APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Cisco DNA Center System drop-down list and choose Licenses.</p>
Network Settings APIs	<p>Catalyst Center platform supports the following Network Settings APIs:</p> <ul style="list-style-type: none"> PUT <cluster-ip>/dna/intent/api/v1/sites/{id}/timeZoneSettings Set time zone for a site. PUT <cluster-ip>/dna/intent/api/v1/sites/{id}/bannerSettings Set banner settings for a site. PUT <cluster-ip>/dna/intent/api/v1/sites/{id}/telemetrySettings Set telemetry settings for a site. <p>To access the new Network Settings APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Site Management drop-down list and choose Network Settings.</p>
SDA APIs	<p>Catalyst Center platform supports the following SDA APIs:</p> <p>Multicast APIs</p> <ul style="list-style-type: none"> GET <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks Get multicast virtual networks. GET <cluster-ip>/dna/intent/api/v1/sda/multicast Get multicast. PUT <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks Update multicast virtual networks. GET <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks/count Get multicast virtual network count. DELETE <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks/\${id} Delete multicast virtual network by ID. POST <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks Add multicast virtual networks.

Site Design APIs	<p>Catalyst Center platform supports the following Site Design APIs:</p> <ul style="list-style-type: none"> POST <cluster-ip>/dna/intent/api/v1/networkDevices/assignToSite/apply Assign network devices to a site. POST <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/\${profileid}/siteAssignments Assign a network profile for sites to the given site <p>To access the new Site Design APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Site Management drop-down list and choose Site Design.</p>
SWIM APIs	<p>Catalyst Center platform supports the following SWIM APIs:</p> <ul style="list-style-type: none"> GET <cluster-ip>/dna/intent/api/v1/images Get list of images available under the given site and product name. POST <cluster-ip>/dna/intent/api/v1/images/\${id}/download Download the software image from Cisco.com on the disk for the given 'id'. GET <cluster-ip>/dna/intent/api/v1/productNames Get the list of network device product names, their ordinal, and the support PIDs based on filter criteria. GET <cluster-ip>/dna/intent/api/v1/productNames/count Get count of product names based on filter criteria. GET <cluster-ip>/dna/intent/api/v1/images/\${imageld}/productNames/\${productNameOrdinal} Update the list of sites for the network device product name assigned to the software image. GET <cluster-ip>/dna/intent/api/v1/siteWiseProductNames Get network device product names for a site. POST <cluster-ip>/dna/intent/api/v1/images/\${imageld}/productNames Assign network device product name and sites for the given image identifier. GET <cluster-ip>/dna/intent/api/v1/siteWiseProductNames/count Get the count of network device product names for the given filters. DELETE <cluster-ip>/dna/intent/api/v1/images/\${imageld}/productNames/\${productNameOrdinal} Removes the network device product name from all the sites for the given software image. PUT <cluster-ip>/dna/intent/api/v1/images/\${imageld}/productNames/\${productNameOrdinal} Update the list of sites for the network device product name assigned to the software image. GET <cluster-ip>/dna/intent/api/v1/images/count Count of images available under the given site and product name. GET <cluster-ip>/dna/intent/api/v1/images/\${id}/addonImages Retrieves the list of applicable add-on images if available for the given software image. GET <cluster-ip>/dna/intent/api/v1/images/\${id}/addonImages/count Count of add-on images available for the given software image identifier. GET <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings Retrieve the list of remote image distribution servers. POST <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings Add image distribution server for distributing software images. GET <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings/\${id} Get image distribution server for specified server identifier. PUT <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings/\${id} Update remote image distribution server. DELETE <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings/\${id} Delete remote image distribution server.

SDK

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

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



The screenshot shows the documentation page for dnacentersdk. The browser address bar displays `dnacentersdk.readthedocs.io/en/latest/`. The page header includes the dnacentersdk logo and a search bar. A navigation menu on the left lists: Installation, Introduction, Quickstart, Contributor Covenant Code of Conduct, and Contributing. The main content area features the title **dnacentersdk** and a subtitle: *Simple, lightweight, scalable Python API wrapper for the DNA Center APIs*. The introductory text states: "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." Below this, it says: "dnacentersdk helps you get things done faster. We take care of the API semantics, and you can focus on writing your code." A section titled "With dnacentersdk, you can easily:" is followed by a bulleted list:

- 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

The page concludes with: "To *dive in* and see how dnacentersdk makes your life better, check out the [Quickstart!](#)"

Go/Ansible/Terraform



Reference

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 on the right, including .gitignore, CHANGELOG.md, LICENSE, Makefile, README.md, 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. It features the Cisco logo and the collection name 'dnac'. The page includes tabs for 'Details', 'Read Me', and 'Content'. The 'Info' section provides installation instructions, a note about installing with ansible-galaxy, and the latest version (6.4.0) released 2 months ago. It also lists tags for 'cisco', 'dnac', 'cloud', 'collection', 'networking', and 'sdi'. A description explains that the collection provides Ansible modules for managing and automating tasks related to DNA Center.

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

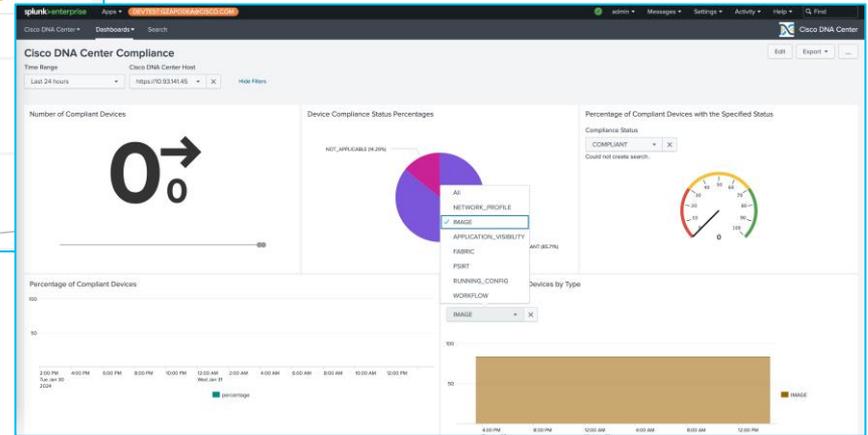
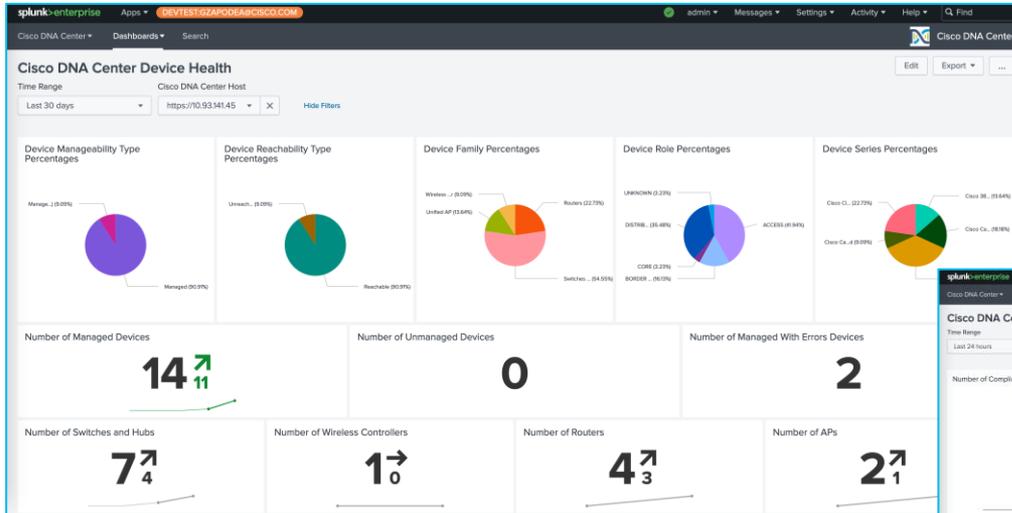
The screenshot shows the Terraform Registry page for the 'cisco-en-programmability/dnacenter' provider. The page has a search bar and navigation links for 'Providers', 'cisco-en-programmability', 'dnacenter', and 'Version 0.3.0-beta'. The provider name 'dnacenter' is prominently displayed, along with the logo for 'en' (Cisco Envision). It indicates the provider is for 'Networking' and was published 2 months ago. A link to the source code is provided: 'cisco-en-programmability/terraform-provider-dnacenter'.

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



Splunk Integration (existing)

<https://github.com/cisco-en-programmability/splunk-apps>



Native Webex Issue Integration



Reference

The screenshot shows a Webex chat interface for a group named 'dnac_webex'. The chat history shows a message from 'dnac_test_bot' at 29/4/2022, 5:22 pm. The message content is a structured notification from Cisco DNA Center. The notification details are as follows:

- 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'.

2.3.7.5 - L2 Advanced Port Configuration

All Devices / perth-9k-edge

perth-9k-edge Run Commands View 360

Reachable Managed IP Address: 10.10.9.128 Device Model: Cisco Catalyst 9300 Switch Device Role: ACCESS Uptime: 4

DETAILS

Summary

System >

Interfaces >

Layer 2 Configuration **BETA** >

Browse Configurations >

User Defined Fields

REP Rings

Wireless Info

SECURITY

Advisories

FIELD NOTICES

Field Notices

Potential Field Notices

COMPLIANCE

Summary



System	Value	Component	Count
Image (Version)	17.9.2	Fan Tray	3
IP Address	10.10.9.128	Power Supply	2
MAC Address	68:ca:e4:36:35:00	SFP Modules	0
Platform	C9300-48U	Serial Number	FCW2

View System Details

Layer 2 Configuration BETA	Value	Component	Count
CDP	Enabled	STP Mode	Rapid
LLDP	Enabled	VTP Mode	Transp
IGMP Snooping	Enabled	MLD Snooping	Disabl
VLANs	7	Port Channels	0
Ports	65		

View Layer2 Details

Port Configuration

1 Selected Edit

- AppGigabitEthernet1/0/1
- FortyGigabitEthernet1/0/2
- FortyGigabitEthernet1/0/3
- GigabitEthernet1/0/4
- GigabitEthernet1/0/5

Edit Port

Reset Set to Default

Port Name GigabitEthernet1/0/1

Configuration

Switchport Description

Switchport Mode **Dynamic Auto**

Switchport Access VLAN ID **1**

Switchport Voice VLAN ID

Switchport Admin Status **No Shutdown**

Authentication Mode **Open**

Cancel Save

Add extra attributes

The screenshot shows the 'Add Configurations' dialog box. On the left, there is a list of 25 unselected configuration options, including CTS SGT, DHCP Snooping Rate, and VTP Admin Status. On the right, one option, 'Switchport Allowed VLAN', is selected and highlighted with a red box. Above the selected item, there are buttons for 'Remove All' and 'Add'. At the bottom of the dialog, there are 'Cancel' and 'Add' buttons.

The screenshot shows the 'Edit Port' configuration page. It features several configuration fields: 'Switchport Mode' set to 'Dynamic Auto', 'Switchport Access VLAN ID' set to '1', 'Switchport Voice VLAN ID' (empty), 'Switchport Admin Status' set to 'No Shutdown', and 'Authentication Mode' with 'Open' selected. A red box highlights the 'Switchport Allowed VLAN' field, which is currently set to 'ALL'. At the bottom, there is a '+ Add Configurations' button.

One more thing (bonus)... Cloud support model

```
False
trad-4331-adamlab-cisco-com 10.10.5.2 IOS True False False None
False
wlc9800-adamlab-cisco-com 192.168.200.201 IOS True False False None
False
```

Untouched inventory from service co4z-4wr-d-w455.

```
>>> dnac=service.inventory["10-66-104-121"]
```

```
>>> dnac.interactive()
```

```
22:13:27.178Z INFO | internal | starting interactive session (will be closed when detached)
```

```
22:13:27.778Z INFO | internal | Session log initialized [filepath='/Users/aradford1/.radkit/session_logs/client/20230803-081327-10-66-104-121.log']
```

```
Attaching to 10-66-104-121 ...
```

```
Type: ~. to detach.
```

```
~? for other shortcuts.
```

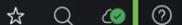
```
When using nested SSH sessions, add an extra ~ per level of nesting.
```

```
Last login: Wed Aug 2 08:11:05 UTC 2023 from 10.81.7.132 on pts/1
```

```
Welcome to the Maglev Appliance
```

```
System information as of Wed Aug 2 22:13:29 UTC 2023
```

Design / Image Repository / Image Family



iller for Cloud

About

Cisco DNA Sense

API Reference

Developer Resources

Contact Support

Remote Support Authorization

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

 ISE and AAA for network and device security

 API for automation/integration/innovation

Keynote Deep Dives

Wednesday

10:30am - 11:30am



Experiences Amplified:
How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106



Smart, Secure, Seamless:
Transforming Experiences with Next-Generation Networking

Level 2
Room 204



Harness a Bold New Era:
Transform Data Centre and Service Provider Connectivity

Level 2
Room 203



Securing User to Application and Everything in Between

Level 2
Melbourne Room 2



Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations



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



Complete your surveys in the **Cisco Live mobile app**.



Continue your education

- Visit the Cisco Stand 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



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC