



The bridge to possible

7 Habits for success with Cisco Catalyst Center

Adam Radford, Distinguished Solutions Engineer

@adamradford123

Lila Rousseaux, Principal Solutions Engineer

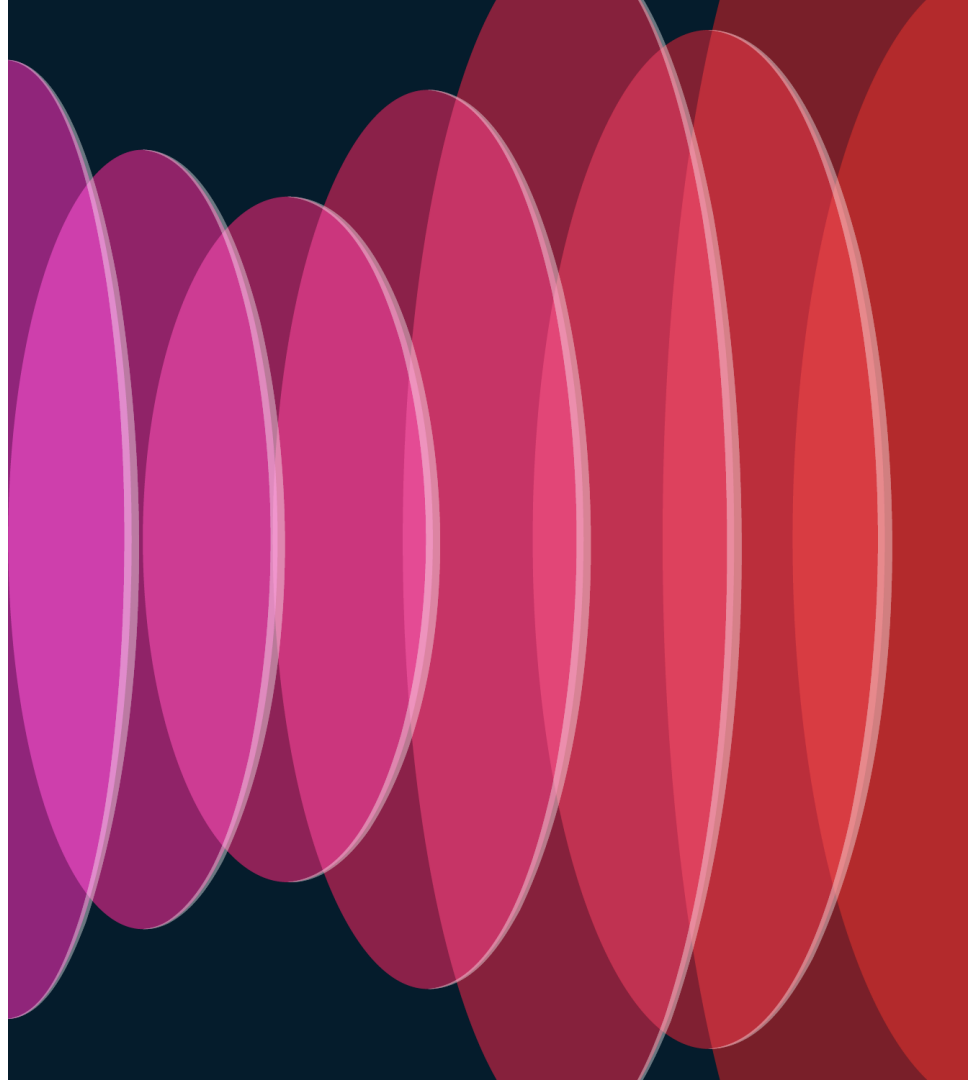
@lila_rousseau

BRKOPS-2416

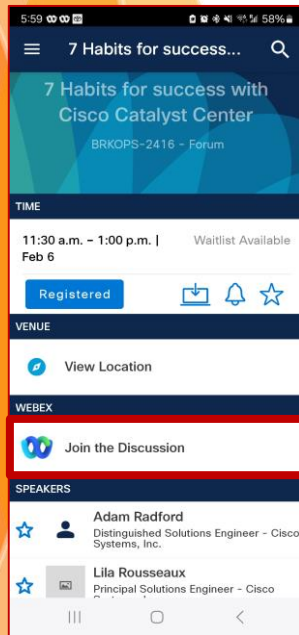
CISCO *Live!*

#CiscoLive

... any regularly repeated behaviour that requires little or no thought and is learned rather than innate.



Agenda



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

Habit #2 - Find issues before your users with telemetry

Habit #3 - Leverage Compliance and Configuration management

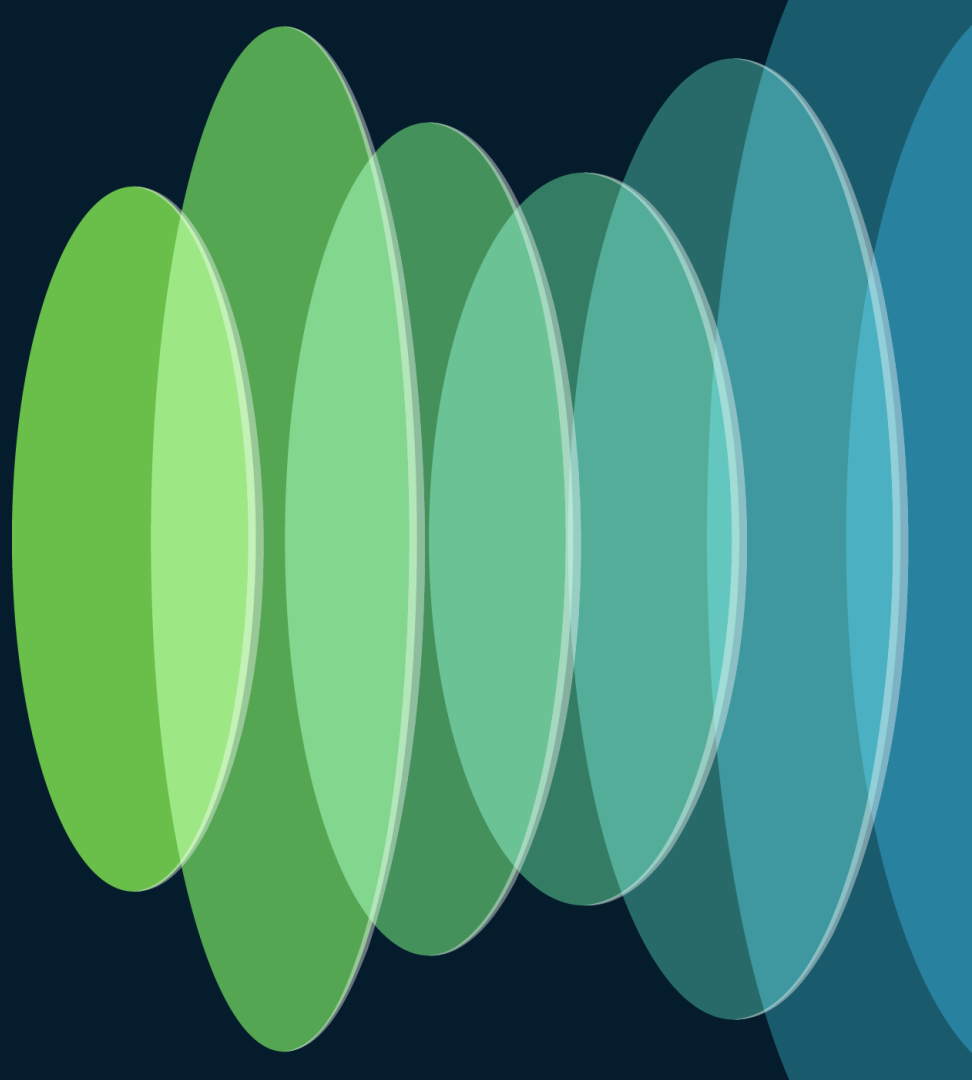
Habit #4 - Keep your infrastructure code up to date with software image management

Habit #5 - Explore Proactive insights with AI/ML

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

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

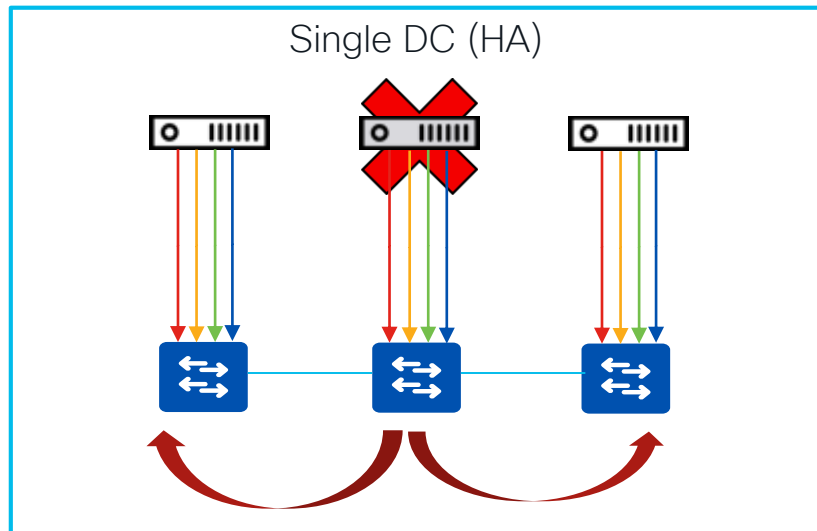
Habit #1 – Understand
Cisco Catalyst Center
Resiliency and design
what's best for your
environment



Physical Appliance High Availability with clustering



Physical Appliance



- ✓ Software or Hardware Failure
- ✓ Active/Active
- ✓ Near Real-Time Synchronization

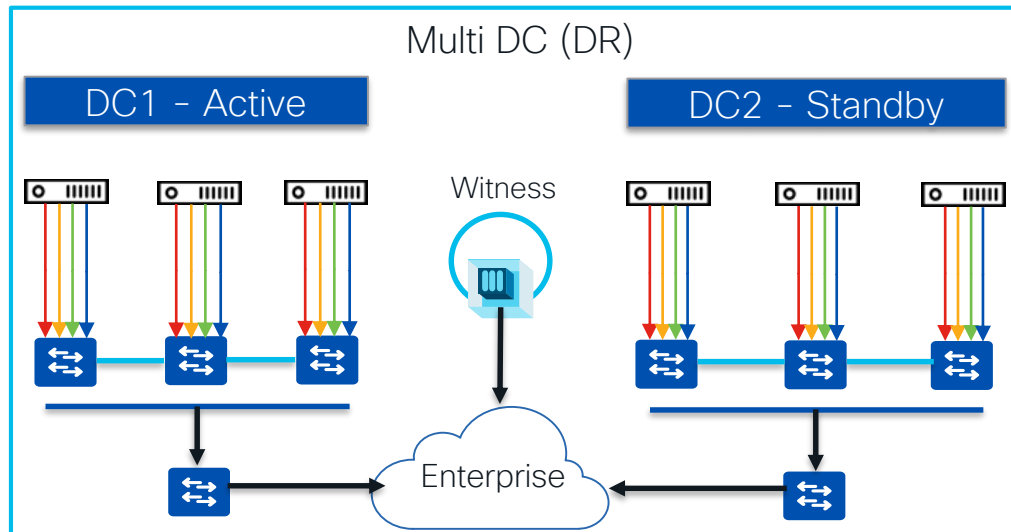
Considerations

- ✓ 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

The screenshot shows the 'Edit Cluster Settings' window for a cluster named 'danc-cluster'. The 'vSphere HA' toggle is turned on. The 'Failures and responses' tab is selected, showing configuration options for host failure response, host isolation, datastore protection (PDL and APD), and VM monitoring. The 'Host Failure Response' is set to 'Restart VMs', 'Response for Host Isolation' is 'Disabled', 'Datastore with PDL' is 'Power off and restart VMs', 'Datastore with APD' is 'Power off and restart VMs - Conservative restart policy', and 'VM Monitoring' is 'Disabled'. There are 'CANCEL' and 'OK' buttons at the bottom right.

Setting	Value
Host Failure Response	Restart VMs
Response for Host Isolation	Disabled
Datastore with PDL	Power off and restart VMs
Datastore with APD	Power off and restart VMs - Conservative restart policy
VM Monitoring	Disabled

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

The screenshot shows the 'Edit Cluster Settings' window for a cluster named 'danc-cluster'. The 'vSphere HA' feature is enabled, indicated by a green toggle switch. The 'Failures and responses' tab is selected, showing configuration options for various failure conditions. The 'Enable Host Monitoring' option is also enabled. The configuration table below lists the response actions for different failure scenarios.

Failure Condition	Response Action
Host Failure Response	Restart VMs
Response for Host Isolation	Disabled
Datastore with PDL	Power off and restart VMs
Datastore with APD	Power off and restart VMs - Conservative restart policy
VM Monitoring	Disabled

At the bottom right of the window are 'CANCEL' and 'OK' buttons.

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.

(*) Amazon EC2: Amazon Elastic Compute Cloud

Backup and Restore - Appliance, AWS VA, ESXi VA

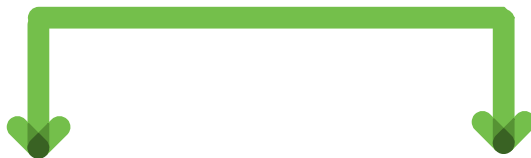


Physical Appliance

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

vmware®



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:

 : : **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:

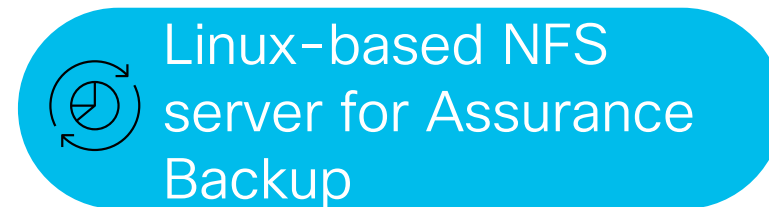
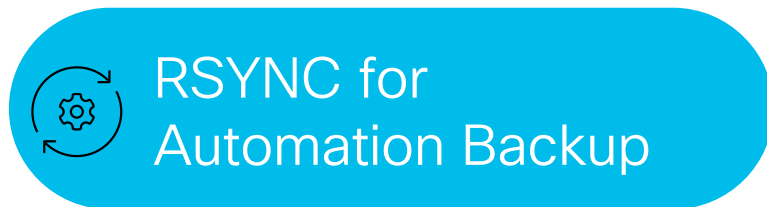
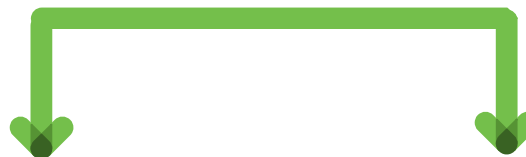
 : : **SCOPE**☒ Cisco DNA Center (All data)☐ Cisco DNA Center (without Assurance data)Use this option to back up automation and Assurance data. You must have two backup directories:
-One backup location is an external NFS server for Assurance data;
-One backup location is an external remote sync (rsync) target location for automation and system data;

cisco Live!

Backup and Restore – Appliance, AWS VA



Physical Appliance



Backup and Restore – Appliance and AWS VA



Physical Appliance



System / Backup & Restore

Backup & Restore

BackupsScheduleActivityConfigure

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

Configured

SSH IP Address*
10.85.54.179

SSH Port*
22

Server Path*
/home/netadmin/TRN6_DNAC_Backups/

Username*
netadmin

Password*

Encryption Passphrase*

DNA Center

Backup & Restore

BackupsScheduleActivityConfigure

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

Configured

Host*
10.85.54.179

Server Path*
/home/netadmin/TRN6_DNAC_Backups/

Backup and Restore – Appliance to AWS VA



- 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



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

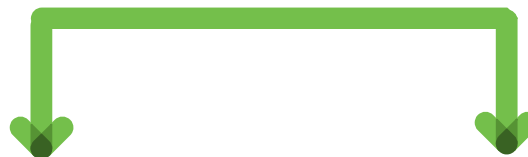


Physical Appliance

vmware®



Types of backup

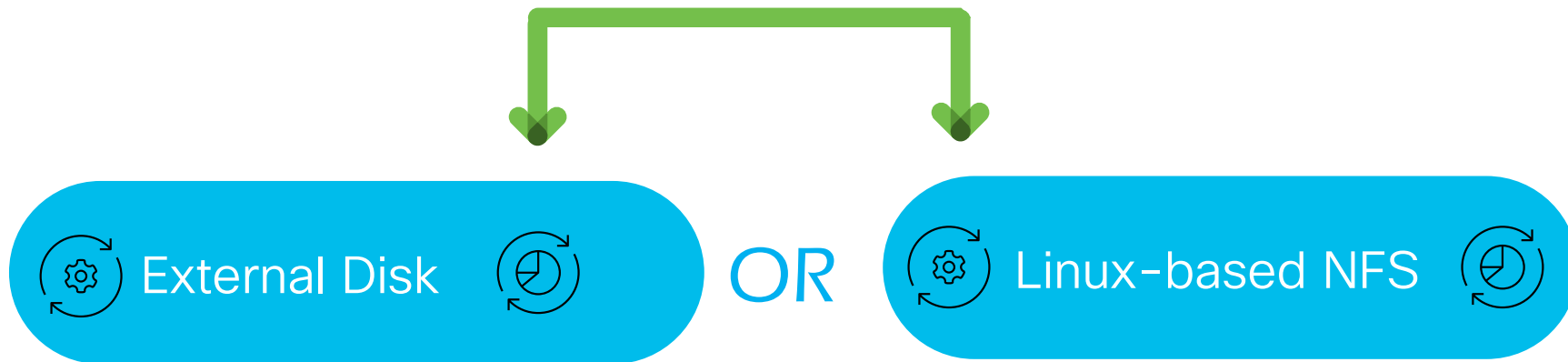


 System and network automation ★

 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. The top navigation bar shows 'DNA Center' and 'System / Settings'. The left sidebar lists 'System Configuration' with sub-items: Proxy, Debugging Logs, High Availability, Backup Configuration (selected), Login Message, Trust & Privacy, and System Certificates. The main content area is titled 'Backup Configuration' under 'Settings / System Configuration'. It describes two backup methods: Physical Disk and Network File System (NFS). The NFS option is selected. The 'Mount Path*' is set to 'nfs://nfs-e51b0f72-fb9b-5b09-b7a5-95c6d8b62419'. An 'Encryption passphrase*' field is present with a note 'Encryption passphrase available'. The 'Backup Retention (in number of backups)*' is set to '14'. At the bottom of this section are 'Reset' and 'Submit' buttons. A modal window titled 'Add NFS' is open on the right, containing fields for 'Server Host*' (10.106.172.227), 'Source Path*' (/var/share/storage-1), 'NFS Version*' (NFS 4), 'Port' (2050), and 'Port Mapper' (111). The modal has 'Cancel' and 'Save' buttons at the bottom.

Backup Configuration

Physical Disk Cisco DNA Center Virtual Appliance provides an option to mount an external disk to the Virtual Machine for Assurance and Automation backups. Note: Physical Disk option is only supported for single node Virtual Machines.

Network File System (NFS) Cisco DNA Center creates the backup files and posts them to a remote server. Each backup is uniquely stored using the UUID as the directory name. For information about the remote server requirements, see Backup Server Requirements listed in the Administrator Guide. [Backup Server Requirements](#)

☐ Physical Disk ☒ NFS [View NFS](#) | [Add NFS](#)

Mount Path*

nfs://nfs-e51b0f72-fb9b-5b09-b7a5-95c6d8b62419

Encryption passphrase*

Backup Retention (in number of backups)*

14

[Info](#)

[Reset](#) [Submit](#)

Add NFS

Server Host*

10.106.172.227

Source Path*

/var/share/storage-1

NFS Version*

NFS 4

Port

2050

Port Mapper

111

[Cancel](#) [Save](#)

Backup Storage Recommendations

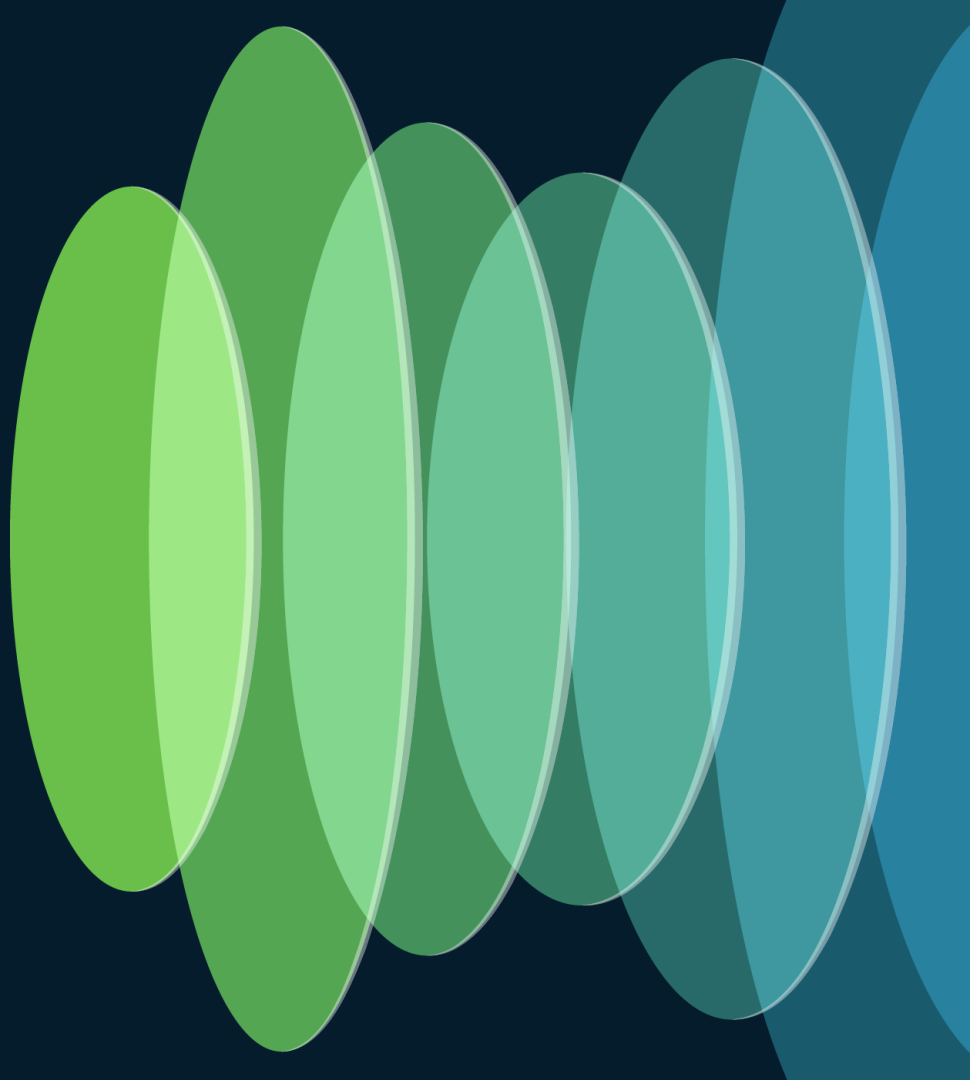


Reference

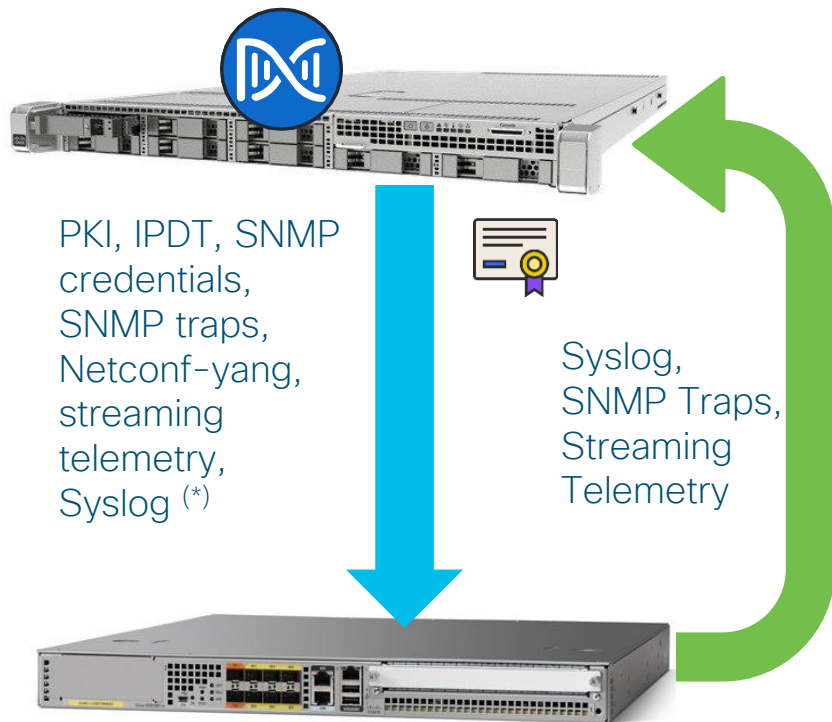
Appliance	NFS Storage (14 Days Incremental)	Rsync Storage (Daily Full)
DN2-HW-APL	1.7 TB	50 GB
DN2-HW-APL-L	3 TB	100 GB
DN2-HW-APL-XL	8.4 TB	300 GB

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 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

1

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

Connected Error Disabled Admin Disabled Not Connected PoE Enabled

2

3

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

Color Code Access VLANs

default(1) x

10_85_49_0-INFRA_VN(1021) x

10_85_61_0-Corp_VN(1022) x

10_85_58_54-Guest_VN(1024) x

Not Configured Default (1) 10_85_49_0-INFRA_VN(1021) 10_85_61_0-Corp_VN(1022) 10_85_58_54-Guest_VN(1024)

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

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

TenGigabitEthernet1/0/16 Tag Port Actions

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

Neighbor Details

Name	Campus_Fabric_AP1	Neighbor	GigabitEthernet0
Capabilities	ROUTER, TB_BRIDGE		

PORT DESCRIPTION

** jinja Jinja for 16** march 22

Inventory Device – Port Configuration and Actions

The screenshot displays the Cisco DNA Center interface. At the top, a green box highlights the 'C9K-STACK' header. Below it, a blue circle with the number '1' is positioned over the 'GigabitEthernet2/0/1' port configuration details. The interface shows a list of devices, including 'C9300-24P' and 'C9300-24P', with their respective IP addresses, device models, and roles. The 'GigabitEthernet2/0/1' port is highlighted in green, indicating it is active. The 'Access VLAN' is set to 'default (1)', and the 'Voice VLAN' is set to '-'. The 'PoE' status is 'Disabled'.

The screenshot shows the 'Edit Access VLAN' dialog box. A blue circle with the number '2' is positioned over the dialog. The dialog contains a search bar and a list of VLANs. The 'default (1)' VLAN is selected. The 'Save' button is highlighted in blue.

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

CISCO *Live!*

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

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

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

Insights

Insights	Instances
Speed/Duplex settings mismatch	2
VLAN Mismatch	9

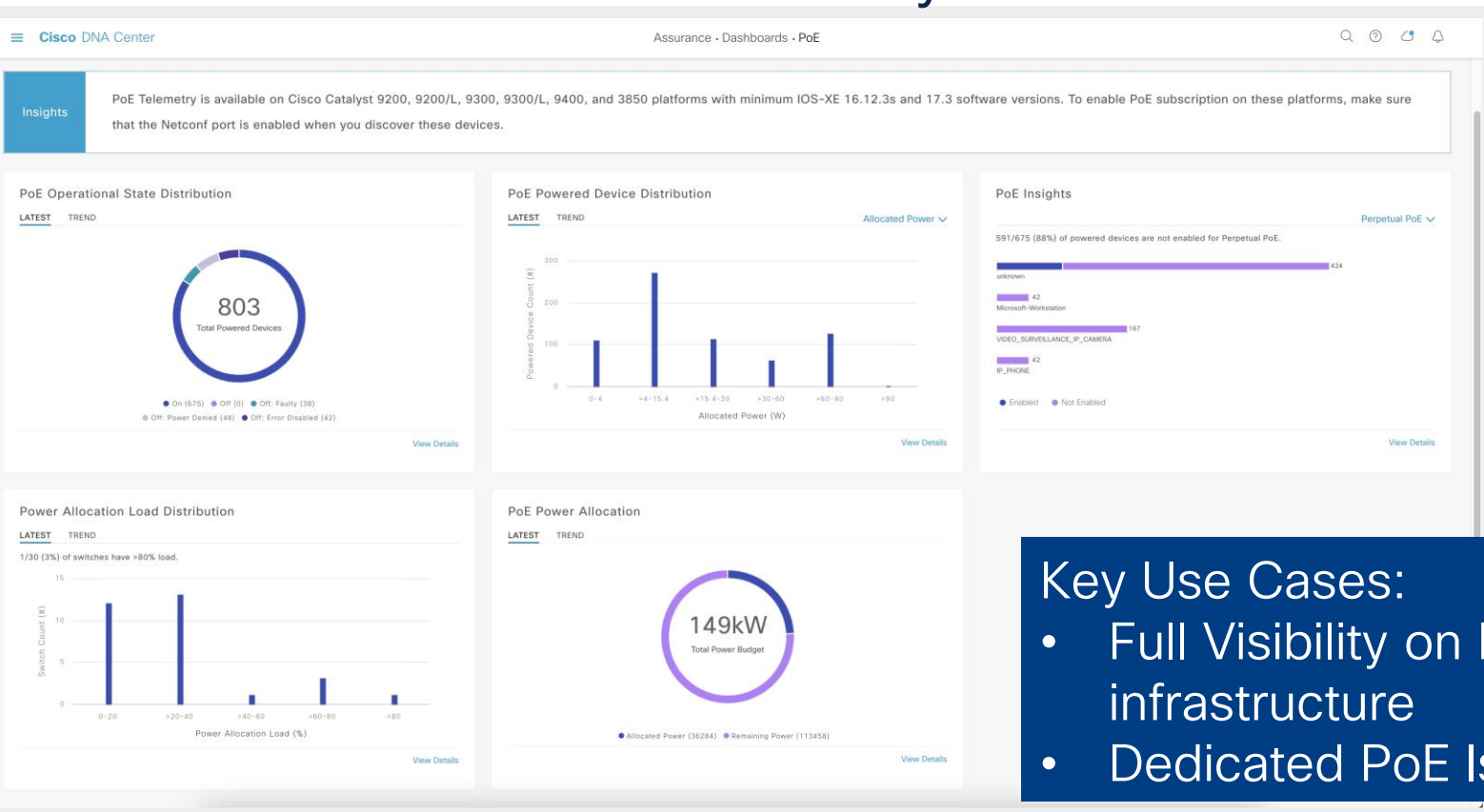
2 Records

Speed/Duplex settings mismatch (2)

As of: Mar 7, 2023 3:40 PM

Devices		Interface		Link	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	up	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	up	1 Gbps	1 Gbps	FullDuplex	AutoNegotiate

Power over Ethernet Analytics



Key Use Cases:

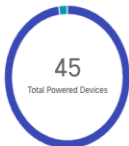
- Full Visibility on PoE infrastructure
- Dedicated PoE Issue Types

Power over Ethernet Analytics

Cisco DNA Center

PoE Operational State Distribution

LATEST TREND



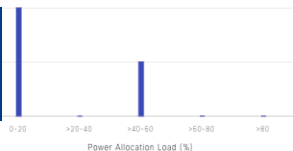
View Details

PoE Operational State

Power Allocation Load Distribution

LATEST TREND

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



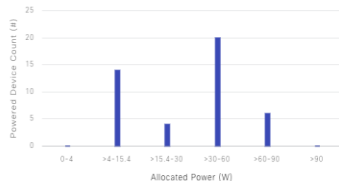
PoE Budget Monitoring

PoE endpoint distribution based on their power allocation

PoE Powered Device

LATEST TREND

Allocated Power



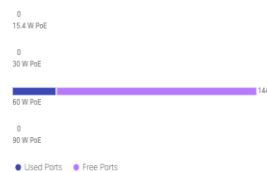
View Details

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



NEW

View Details

AP Power Mode

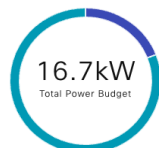
Are my AP's fully or partially powered?

NEW

Power Usage

LATEST TREND

Allocation



Power Usage

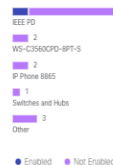
What is the real time power consumption of my access network

PoE Insights

LATEST TREND

Perpetual PoE

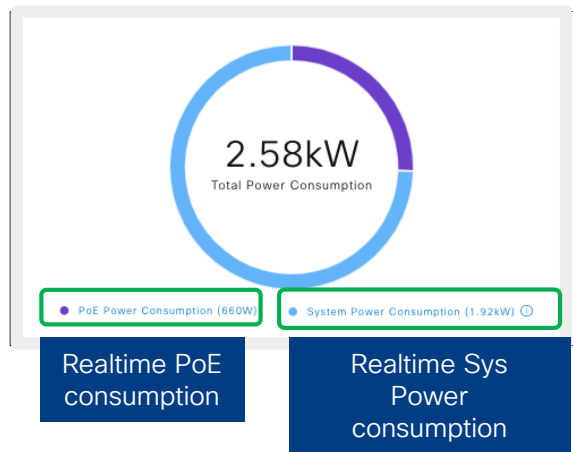
42/44 (95%) of powered devices are not enabled for Perpetual PoE.



PoE Insights

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

Realtime Power Consumption Reporting



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

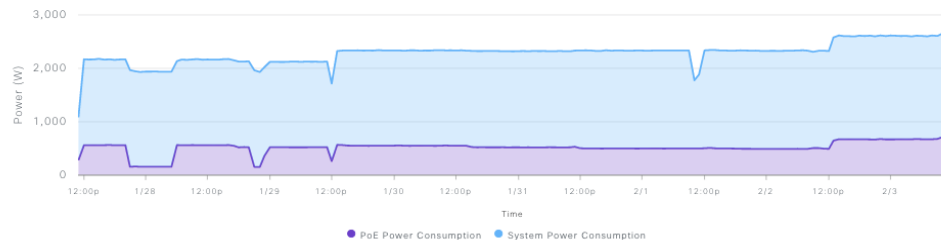
Power Usage

LATEST

TREND

Historical Trend View

Consumption



View Details

Catalyst 9200,
9300 and 9400
starting IOS-XE
17.14.1

Instantaneous System
Power + PoE Consumption

Select a data type below to filter the proceeding

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

Power over Ethernet Analytics

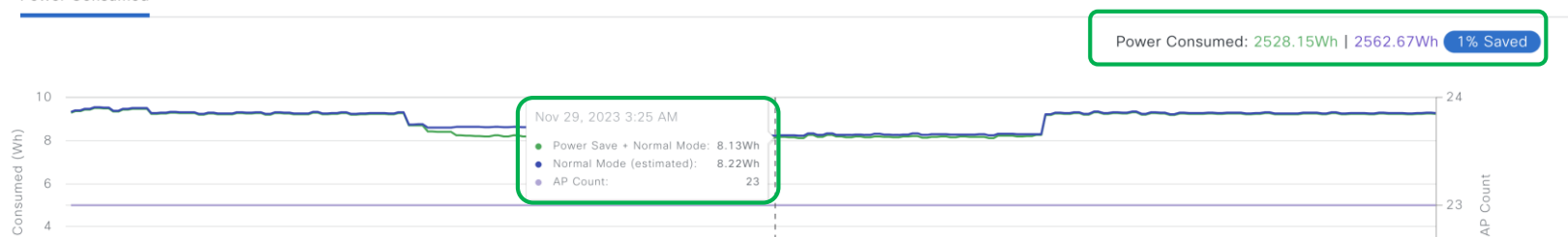
AP Power Save Mode Distribution & AP Savings on Power Consumed

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)

Q 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 < 1 >

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

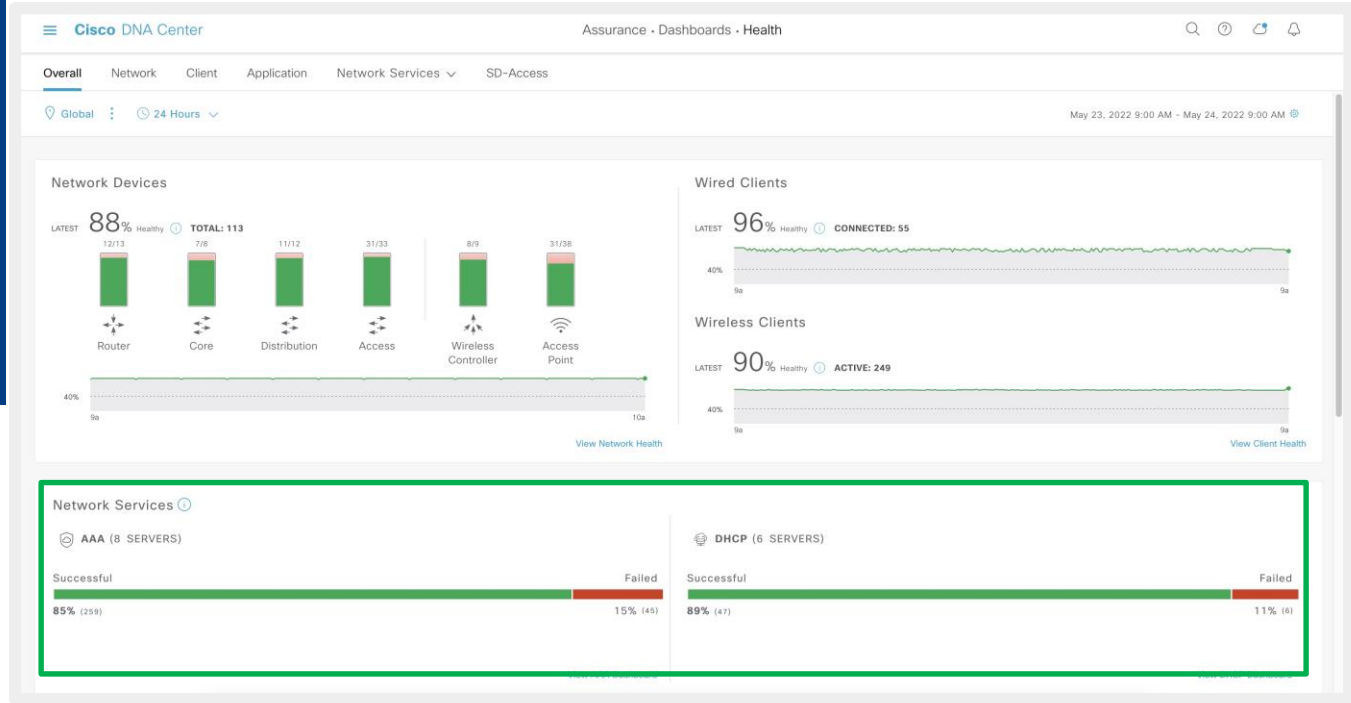
Power Stack (2)

Q 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 ⓘ

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

[View Details](#)

Top Sites by Transaction Failures ⓘ

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

[View Details](#)

DHCP Server Latency ⓘ



[View Details](#)

DHCP Server Transactions ⓘ



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

Tracked by Network Services Analytics - AAA/DHCP



Reference

AAA

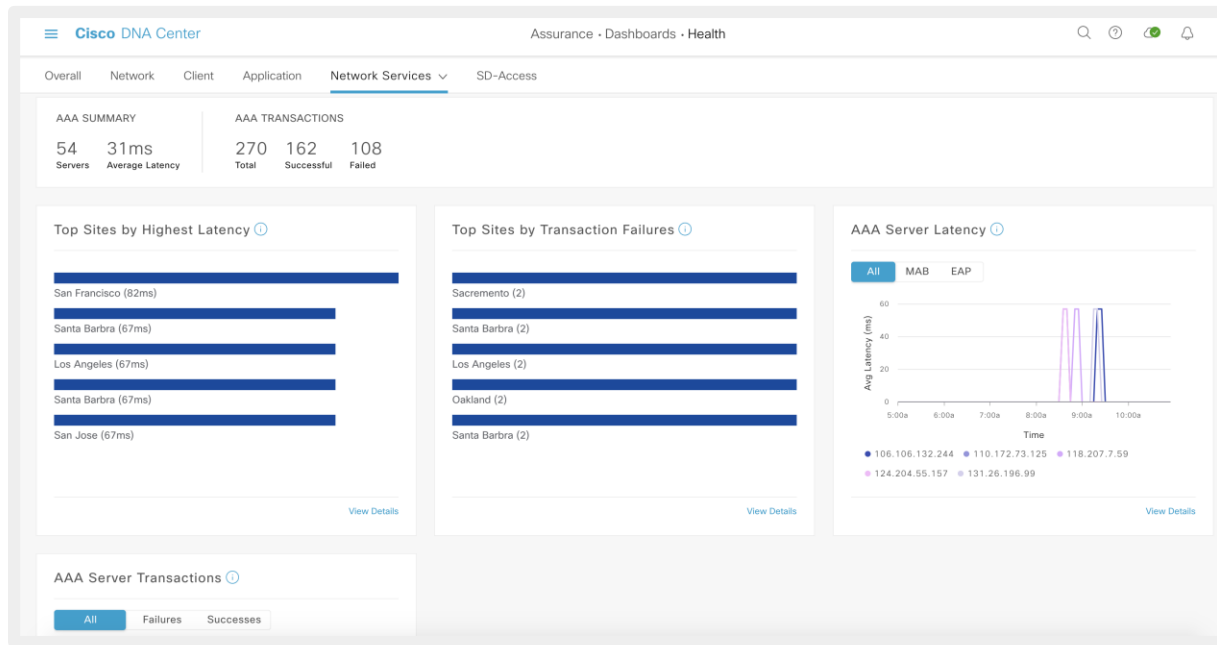
- AAA Servers
- AAA Server Latency
- AAA Server Transactions
- AAA Transaction Failures %
- Top Sites by Transaction Failures
- Top Sites by Highest Latency
- AAA Servers by WLC

DHCP

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

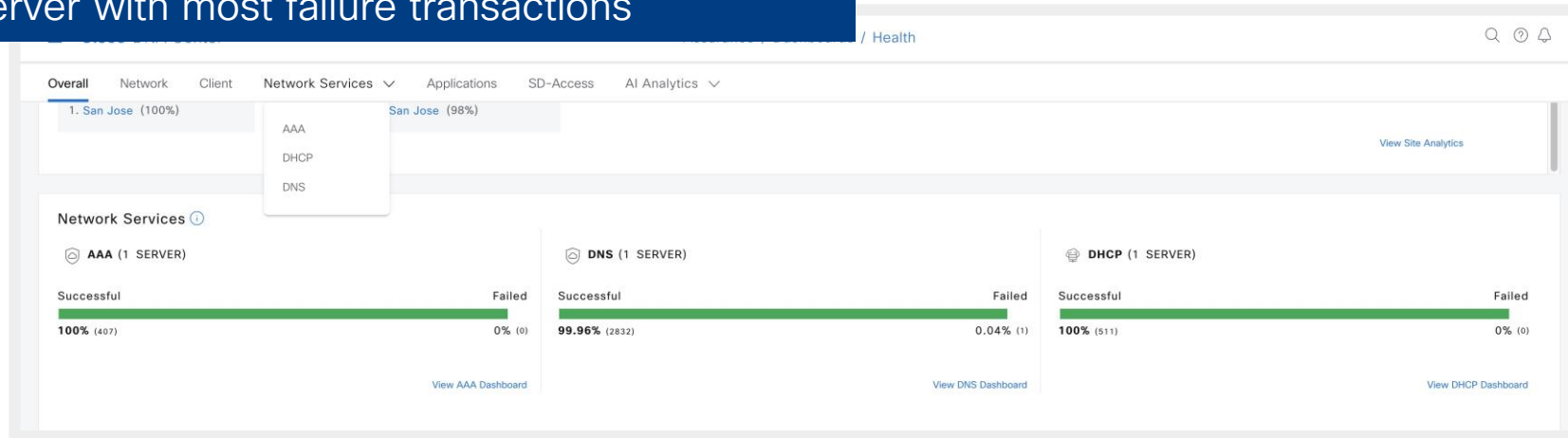
Network Services Analytics – AAA/DHCP

- 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

DNS Summary information
of servers, average latency
, total transactions



Reference

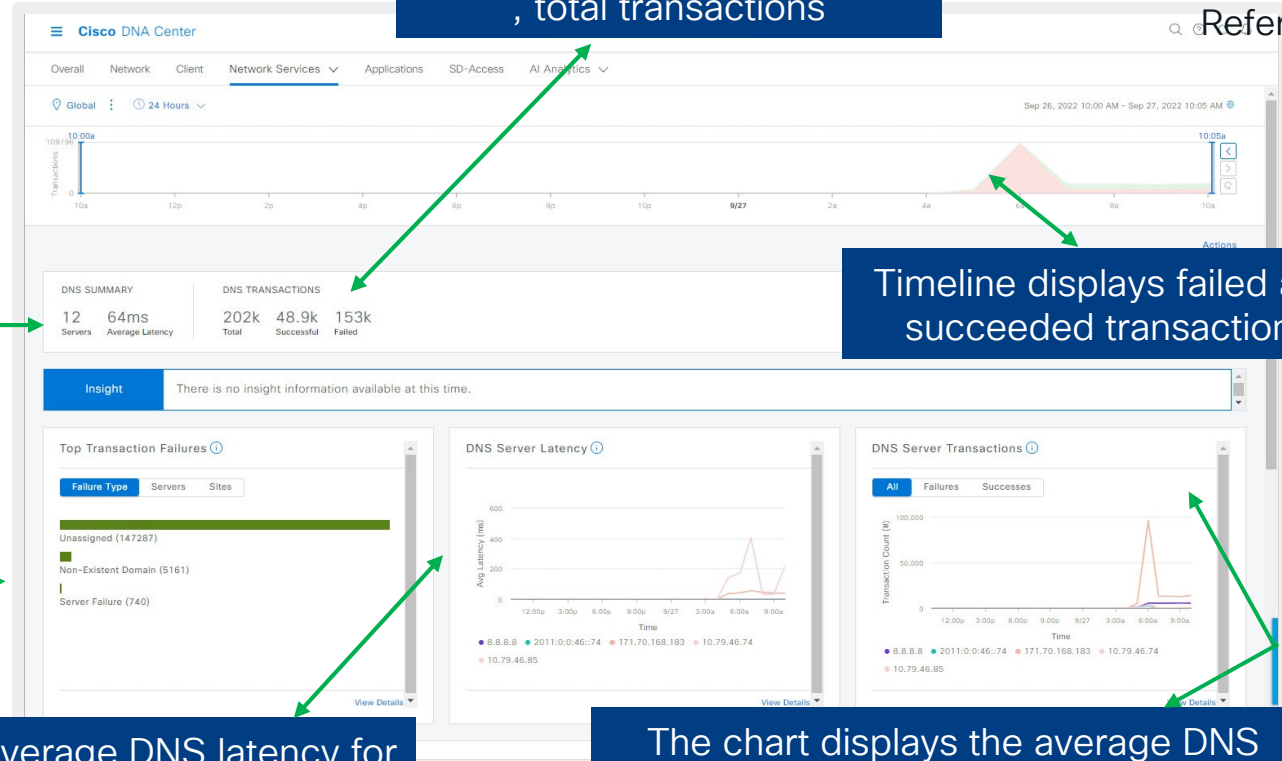
Count of DNS servers
and average latency
(in ms) of your
network.

Top DNS server
transaction failure types,
servers, and sites

Timeline displays failed and
succeeded transactions

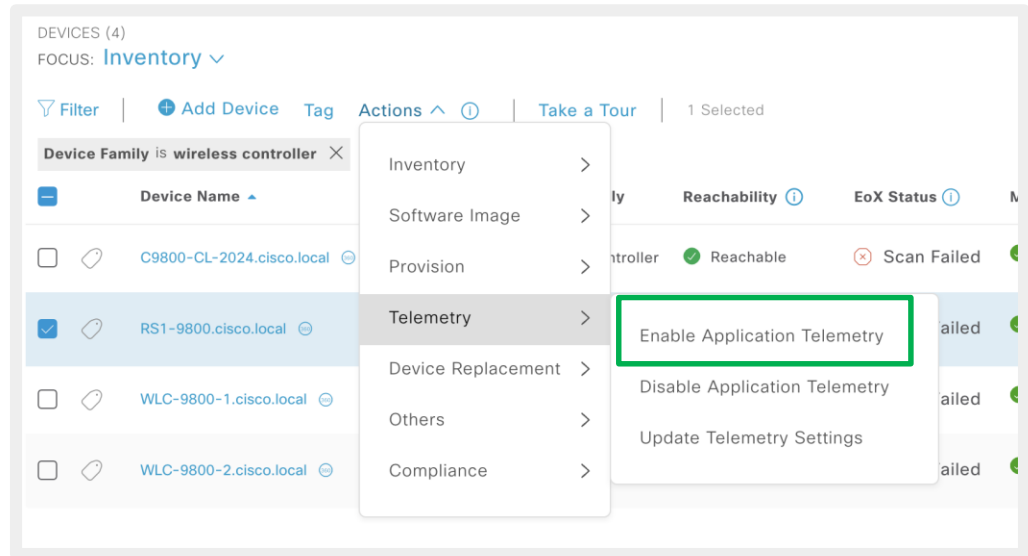
Average DNS latency for
each DNS server.

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



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 dnarecord_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 dnarecord_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

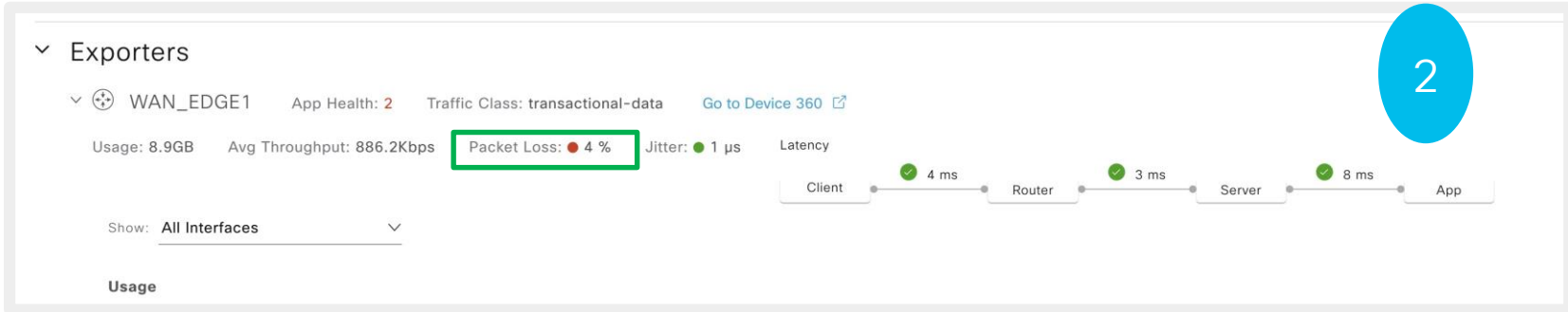
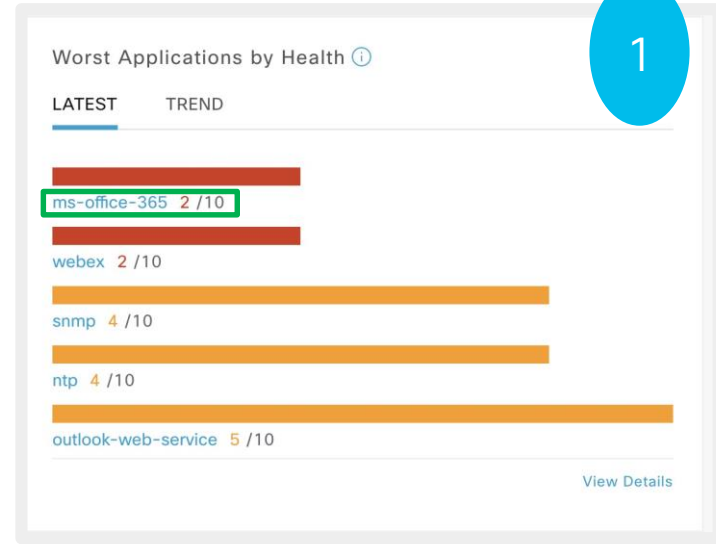
IOS-XE: 17.11.01

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

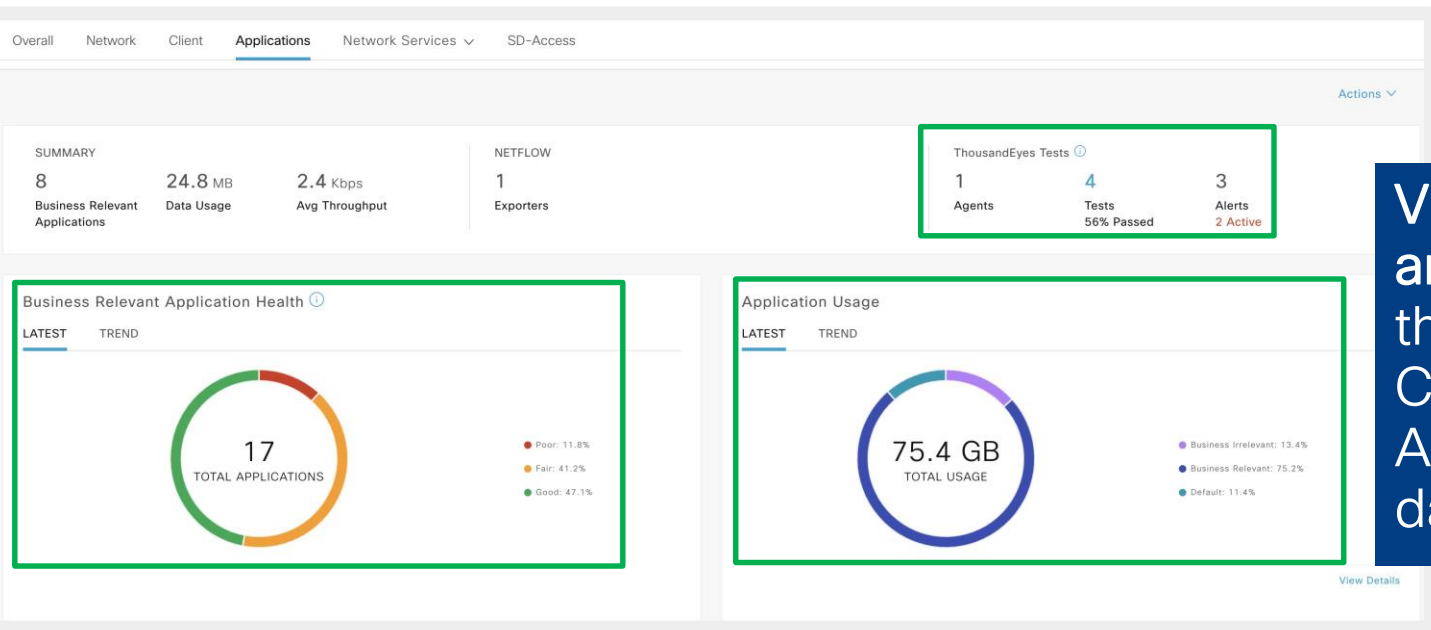
Gordon.Thomson 1.3Kbps

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

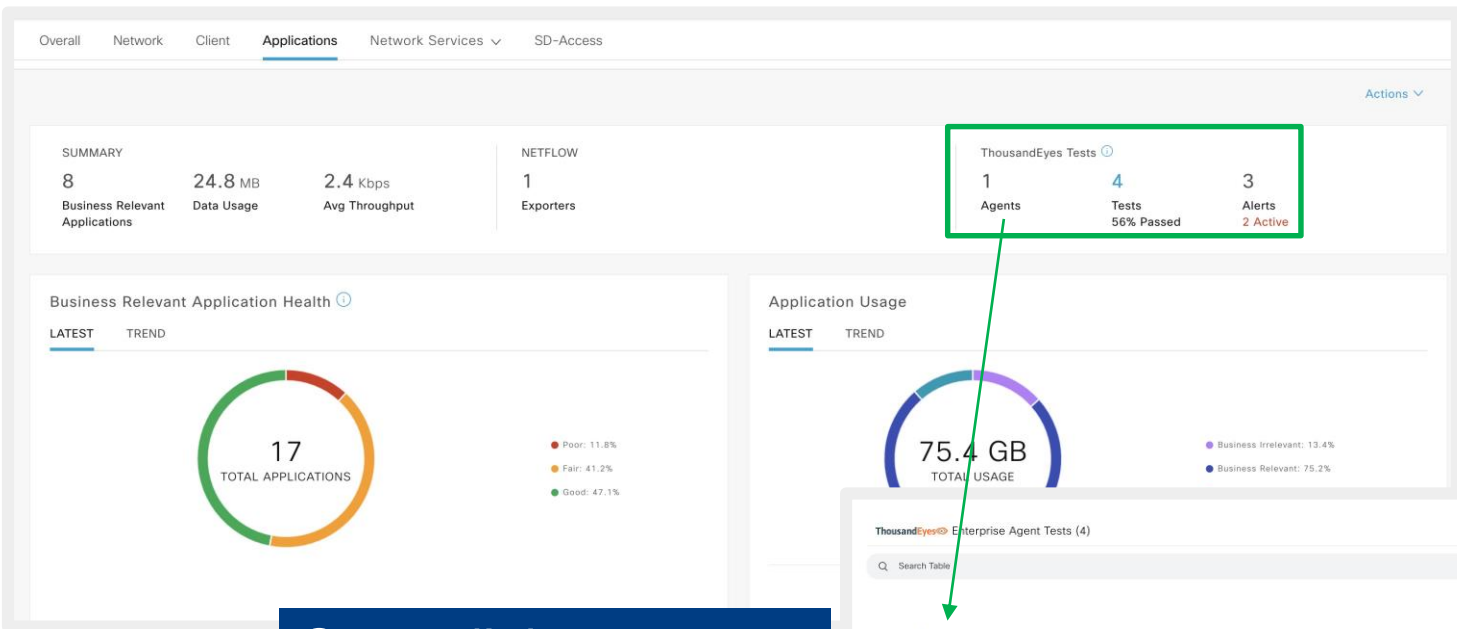
(*) New with Catalyst Center 2.3.5 and IOS-XE 17.10.1 or later with C91xx AP's

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.

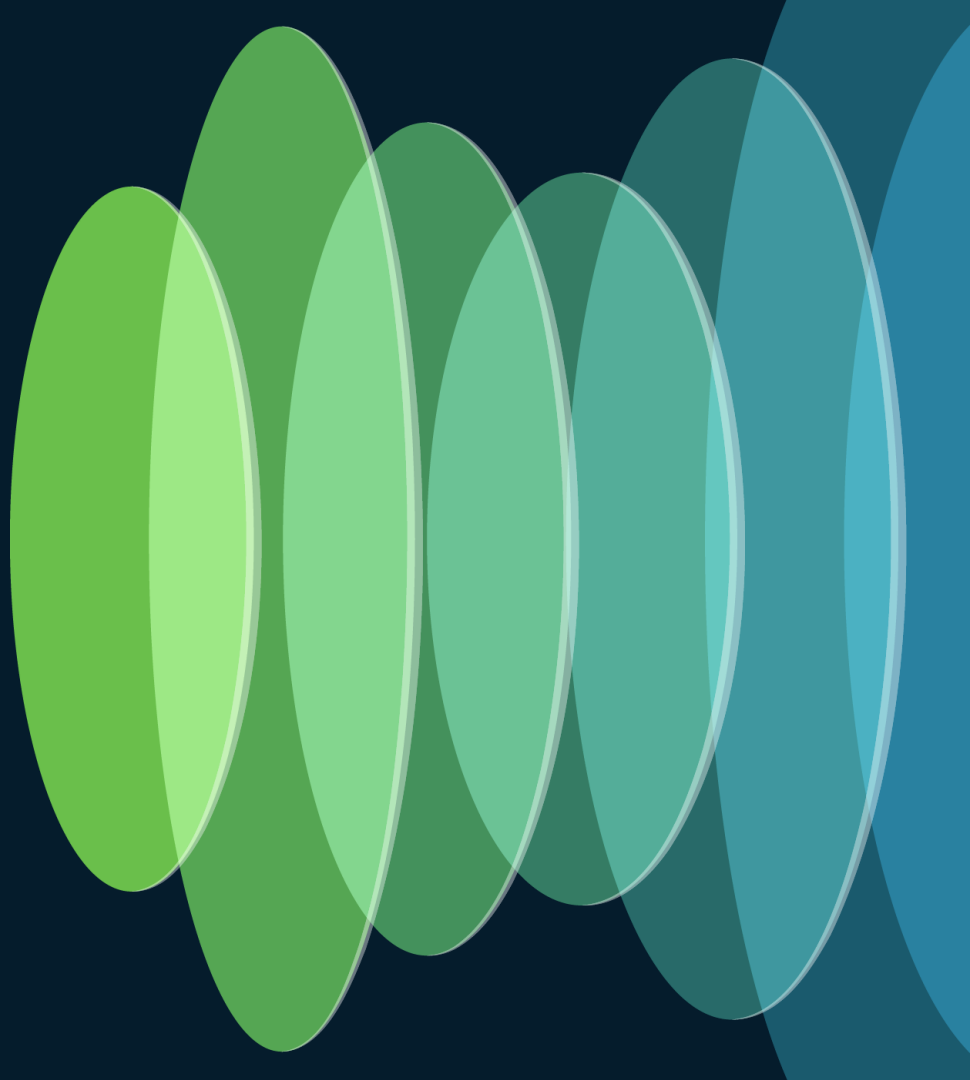
ThousandEyes Enterprise Agent Tests (4)

Search Table

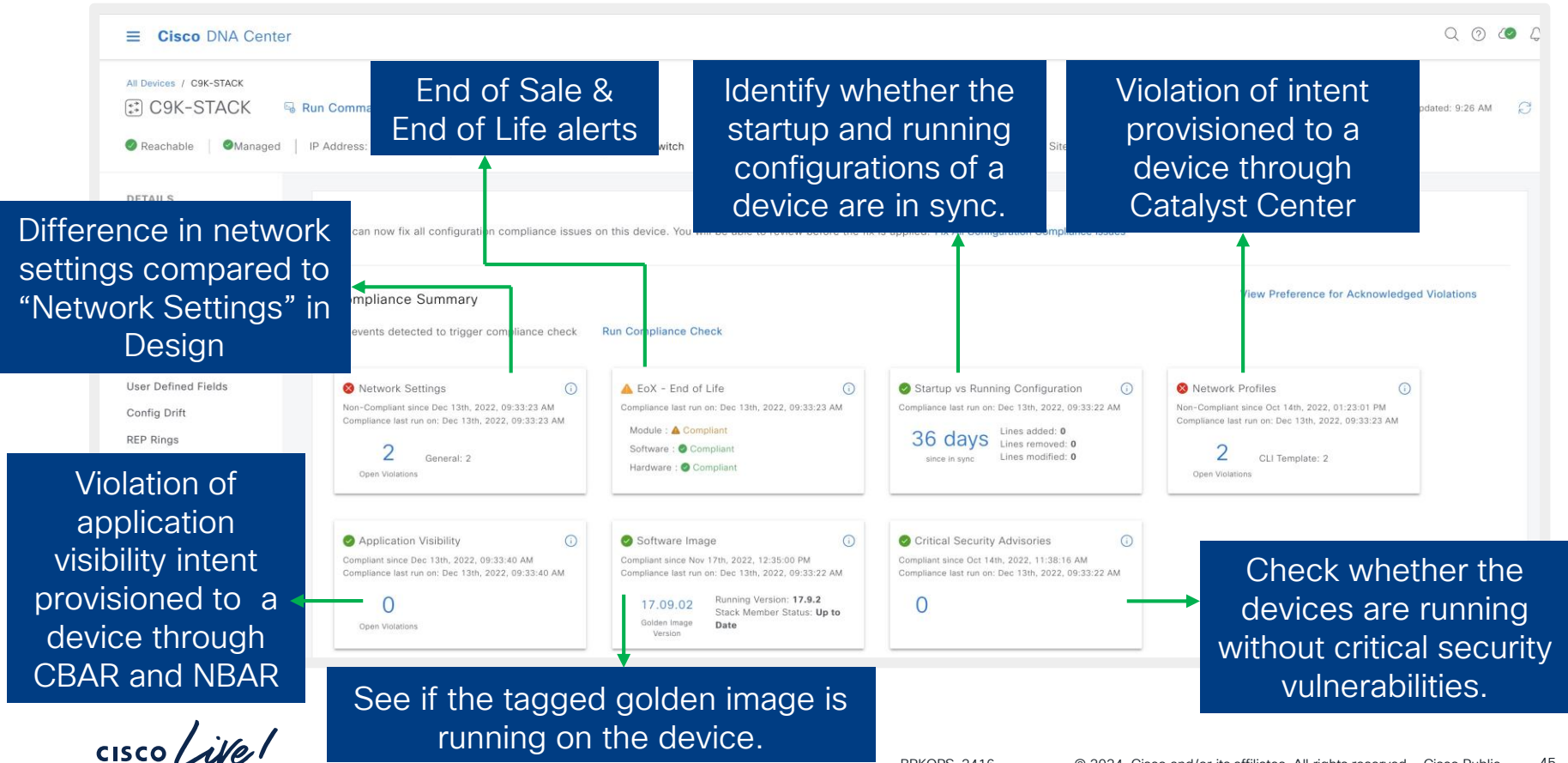
As of: Mar 6, 2023 12:13 PM

Test Name	Test Type	Target	Device Name	Latest Fetch Sampling Time	Packet Loss (%) Avg / Latest	Jitter (ms) Avg / Latest	Latency (ms) Avg / Latest	Resp.
NetSense - www.slack-redir.net	Web - HTTP Server	https://www.slack-redir.net	SJC01-C9300-01	5 months ago	0 / --	0 / --	0 / --	
Office 365 Login	Network - Agent to Server	52.112.14.70:80	SJC01-C9300-01	5 months ago	100 / --	0 / --	0 / --	
Salesforce	Web - HTTP Server	https://www.salesforce.com	SJC01-C9300-01	5 months ago	0 / --	0 / --	0 / --	
webex	Web - HTTP Server	https://www.webex.com	SJC01-C9300-01	5 months ago	0 / --	0 / --	0 / --	

Habit #3 – Leverage Compliance and Configuration management



Cisco Catalyst Center Compliance Landscape



Compliance: Network Profiles – Switches

The screenshot displays the Cisco DNA Center interface for a specific device, C9K-BRANCH-STACK. The top navigation bar shows the device name and a green box highlights the breadcrumb path 'All Devices / C9K-BRANCH-STACK'. Below this, the device's status is shown as 'Reachable' and 'Managed', along with its IP address (10.85.54.54), model (Cisco Catalyst 9300 Switch), role (ACCESS), uptime (122 days 23 hrs 9 mins), and site (Global/Canada/Ontario/Toronto/TBRANCH). The left sidebar lists various configuration categories, with 'Configuration' expanded. The main content area, titled 'Compliance Summary', shows a 'Run Compliance Check' button and a message: 'No events detected to trigger compliance check'. Below this, four compliance cards are displayed. The 'Network Profiles' card is highlighted with a green box and shows a red 'X' icon, indicating non-compliance. It states 'Non-Compliant since Sep 2nd, 2022, 03:01:45 PM' and 'Compliance last run on: Sep 2nd, 2022, 03:01:30 PM'. The card also shows '1 Changes' and 'CLI Template: 1'. Other cards include 'Startup vs Running Configuration' (4 mins since out of sync, 1 line removed), 'Software Image' (Compliant since May 2nd, 2022, 03:53:28 PM, 17.08.01 Golden Image Version, Running Version: 17.8.1), and 'Critical Security Advisories' (Compliant since May 7th, 2022, 08:01:15 PM, 0).

Compliance Summary

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

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

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
```

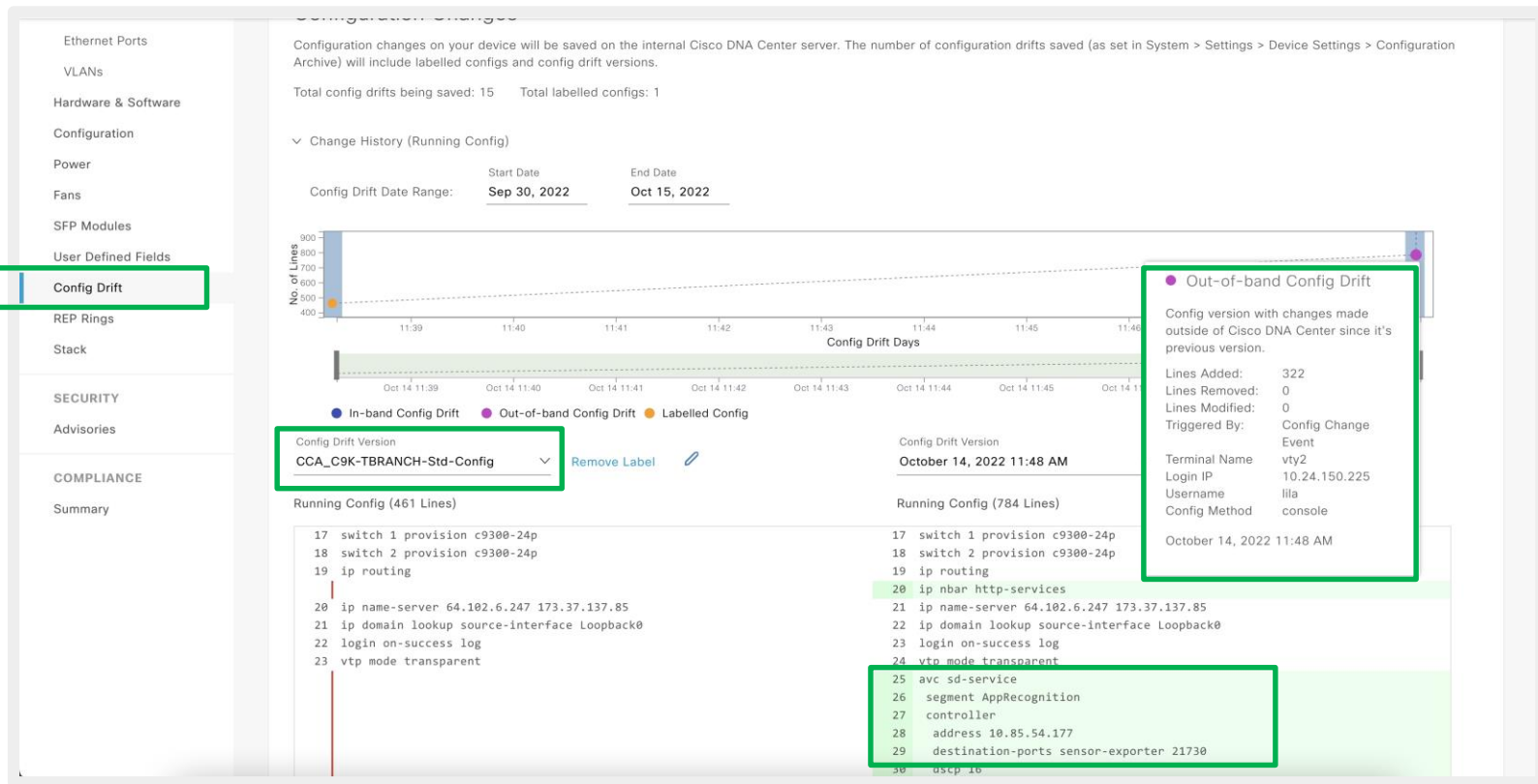
Out of band changes:

```
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 managing network profiles. The top navigation bar includes 'All Devices / C9K-BRANCH-STACK', 'Run Commands', and 'View 360'. The main content area is titled 'Compliance Summary / Network Profiles' and shows 'CLI Template (1)' and 'CLI Deviations' as of May 26, 2022 2:25 PM. A search bar is present. The 'Template' section shows 'PDESCRIPTION' selected. The 'Realize Template: PDESCRIPTION' section displays a table of CLI deviations. A callout box points to the highlighted text in red in the table, stating: 'The highlighted text in red are the missing CLIs.'

Line	CLI
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



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 ⓘ

Compliance last run on: Apr 2nd, 2022, 11:16:36 AM

1 hr since out of sync Lines added: 2 Lines removed: 2 Lines modified: 0

Network Profiles ⓘ

Non-Compliant since Feb 9th, 2022, 02:38:20 AM Compliance last run on: Apr 2nd, 2022, 11:16:36 AM

3 Changes Model Config: 1 Wireless: 1 +1 more

Application Visibility ⓘ

Compliant since Apr 2nd, 2022, 11:16:54 AM Compliance last run on: Apr 2nd, 2022, 11:16:54 AM

0 Changes

Software Image ⓘ

Compliant since Feb 3rd, 2022, 05:10:45 PM Compliance last run on: Apr 2nd, 2022, 11:16:36 AM

17.07.01 Running Version: 17.7.1 Golden Image Version

Critical Security Advisories ⓘ

Compliant since Feb 8th, 2022, 07:00:11 PM Compliance last run on: Apr 2nd, 2022, 11:16:36 AM

0

Compliance: Network Profiles – Wireless

Cisco DNA Center

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. At the top, the breadcrumb navigation shows 'All Devices / STL01-C9800-CL.dlab.local'. Below this, the device name 'STL01-C9800-CL.dlab.local' is shown with links for 'Run Commands' and 'View 360'. The device status is 'Reachable' and 'Managed', with an IP address of 172.16.255.35. The device model is 'Cisco Catalyst 9800-CL Wireless Controller for Cloud', and its role is 'ACCESS'. The uptime is '22 hrs 56 mins' and the site is 'Global/Canada/Quebec/Saint-Lambert/STL01'. The left sidebar contains a 'DETAILS' section with a dropdown menu showing 'Interfaces', 'Ethernet Ports', 'Virtual Ports', 'Hardware & Software', 'User Defined Fields', 'Config Drift', 'Wireless Info', and 'Mobility'. The 'COMPLIANCE' section is also visible with a 'Summary' link. The main content area shows the 'Compliance Summary / Network Profiles' page. Under the 'Model Config (1)' tab, the 'Wireless (1)' profile is selected and highlighted with a green box. Below this is a search bar and a table with the following data:

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

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

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

Reachable Managed IP Addr

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

☐	Model Name	Attribute	Status	Intended Value	Actual Value	Action
☐	DNS NR Settings	nameServers	Changed	64.102.6.247	-	Acknowledge
☐	DNS NR Settings	nameServers	Changed	173.37.137.85	-	Acknowledge

Showing 2 of 2

Fix Config Compliance Issues

Cisco DNA Center

All Devices / C9K-STACK

C9K-STACK
PORT_SECURITY

Reachable Managed IP Address: 10.85.54.54 Device Model: Cisco Catalyst 9300 Switch Device Role: ACCESS Uptime: 61

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.

Compliance Summary

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

Issue	Compliance last run on	Status
EoX - End of Life	Jan 17th, 2023, 02:55:23 PM	Compliant
Network Settings	Jan 17th, 2023, 02:55:23 PM	Non-Compliant
Network Profiles	Jan 17th, 2023, 02:55:23 PM	Non-Compliant
Application Visibility	Jan 17th, 2023, 02:56:06 PM	Compliant

Fix Configuration Compliance Issues

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

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

Summary of Issues to be Fixed ⓘ

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

Compliance Type	Issues Identified ⓘ
Network Profiles	1
Network Settings	2

Schedule the Fix

When would you like to apply the fix?

☒ Now

☐ Later

☐ Generate Preview

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

Task Name*

C9K-STACK - Compliance Fix

[Cancel](#) [Apply](#)

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
Event Time	12-October-2022 12:30:51
IP Address	10.104.249.137
Category	OUT OF BAND
Client IP Address	10.65.62.13
DEVICEUUID	6da28e45-3d5-4a21-8b30-e0758012d8ea
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-d5a1ff43520f",
  "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=$deviceId",
  "note": "To get more details, use A
",
  "context": null,
  "userId": null,
  "i18n": null,
  "eventHierarchy": null,
  "message": null,
  "messageParams": null,
  "parentInstanceId": null,
  "network": null,
  "dnacIP": "10.104.241.138"
}
```

DNAC-Toronto-lab@cisco.com

To: Lila Rousseau (lroussea)

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:

5

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

cisco Live!

#CiscoLive

BRKOPS-2416

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

56

Device Configuration Management

Configuration Archive

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 screenshot illustrates the process of exporting device configurations to a local archive. It shows three overlapping windows:

- Downloads Window:** Displays the file `Export_Configs-10_Feb_2022_18_04_00_353-oWF.zip`.
- Archive Utility Window:** A password prompt for the archive file. The text reads: "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... Window:** Shows the contents of the exported archive, which are configuration files for various network devices. The files listed are:
 - `10.85.51.69-TRN6-E2.cisco.com`
 - `10.85.54.17-TRN6-TBRANCH-DIST.cisco.com`
 - `10.85.54.20-TRN6-TBRANCH-WLC`
 - `10.85.54.23-TBRANCH-C9200-1.lila.com`
 - `10.85.54.24-TBRANCH-C9200L-2.cisco.com`
 - `10.85.54.25-TBRANCH-C9200L-3.cisco.com`
 - `10.85.54.51-TRN6-TBRANCH-FUSION`
 - `10.85.54.53-TRN6-TBRANCH-C3650-S1.cisco.com`
 - `10.85.54.54-C9K-BRANCH-STACK`
 - `10.85.54.99-wlc01`
 - `10.85.54.102-wlc02`
- 10.85.54.54-C9K-... Window:** Shows the contents of a specific configuration file, `10.85.54.54-C9K-...`. The files listed are:
 - `10_Feb_2022_18_04_00_353_RUNNINGCONFIG.cfg`
 - `10_Feb_2022_18_04_00_353_STARTUPCONFIG.cfg`
 - `10_Feb_2022_18_04_00_353_vlan.dat.bat`

Device Configuration Management



Reference

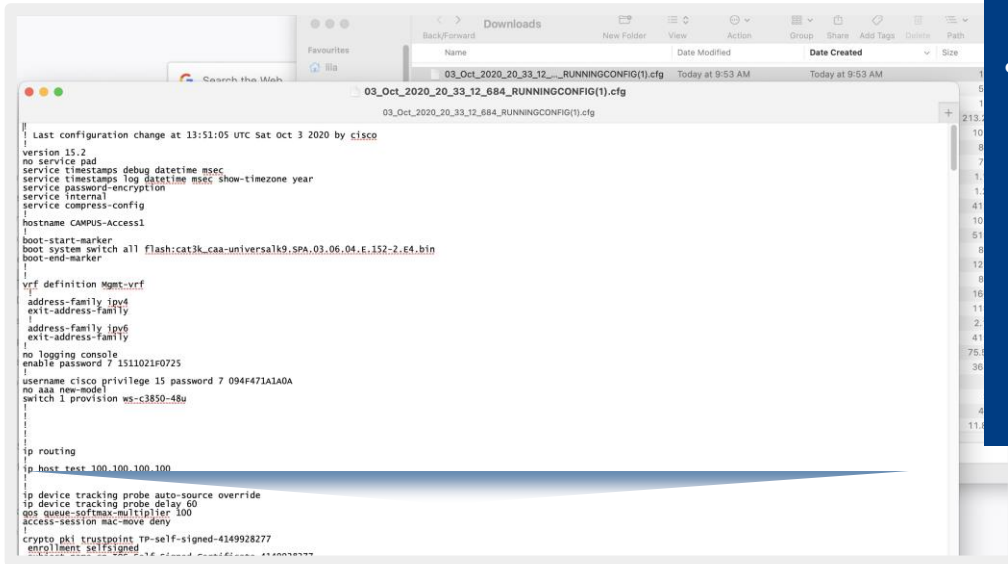
10_Feb_2022_18_04_00_353_RUNNINGCONFIG.cfg 10_Feb_2022_18_04_00_353_RUNNINGCONFIG.cfg

```
| 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/gvcAL9GF0$uk6/kumGDPS/ABbtHwK8xzqGeVEVvm3idf83ZIm4zH9Z  
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
```

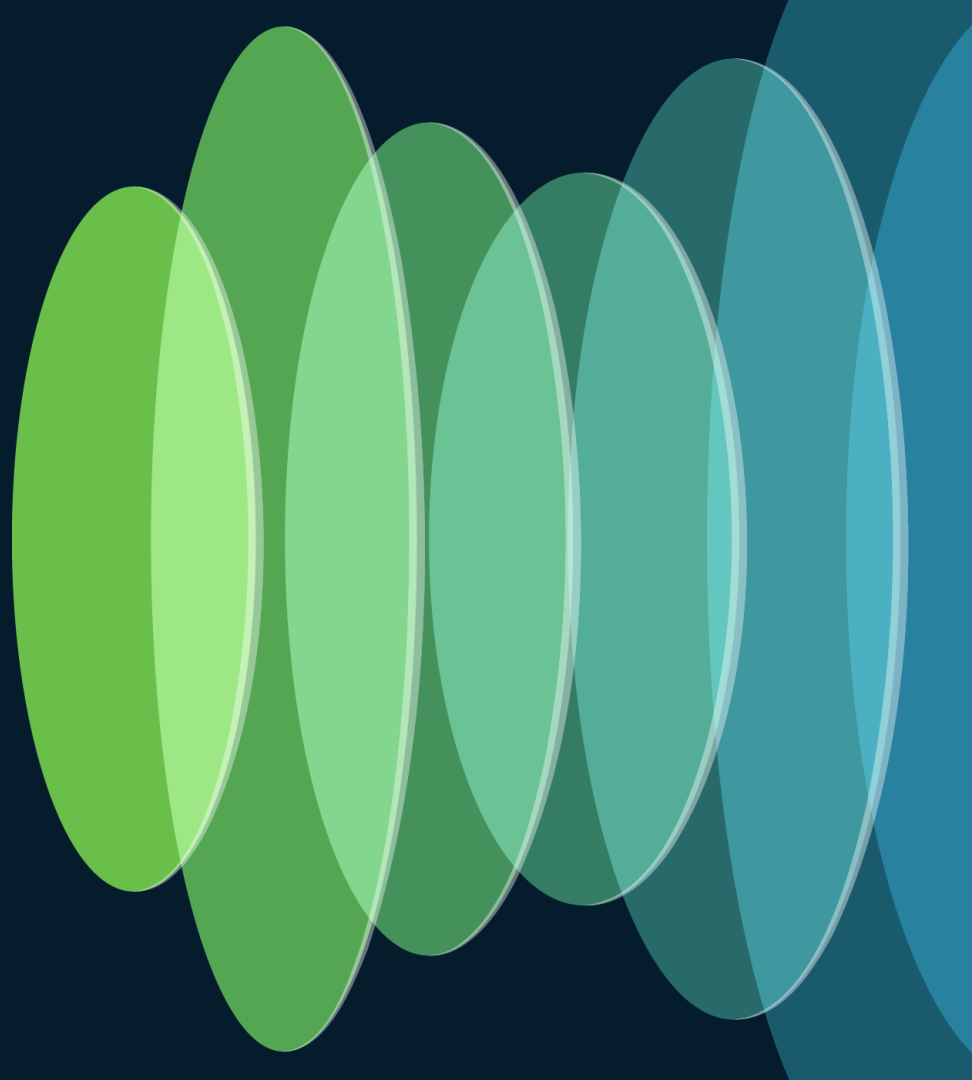
Device Configuration Management

API's to retrieve device configuration

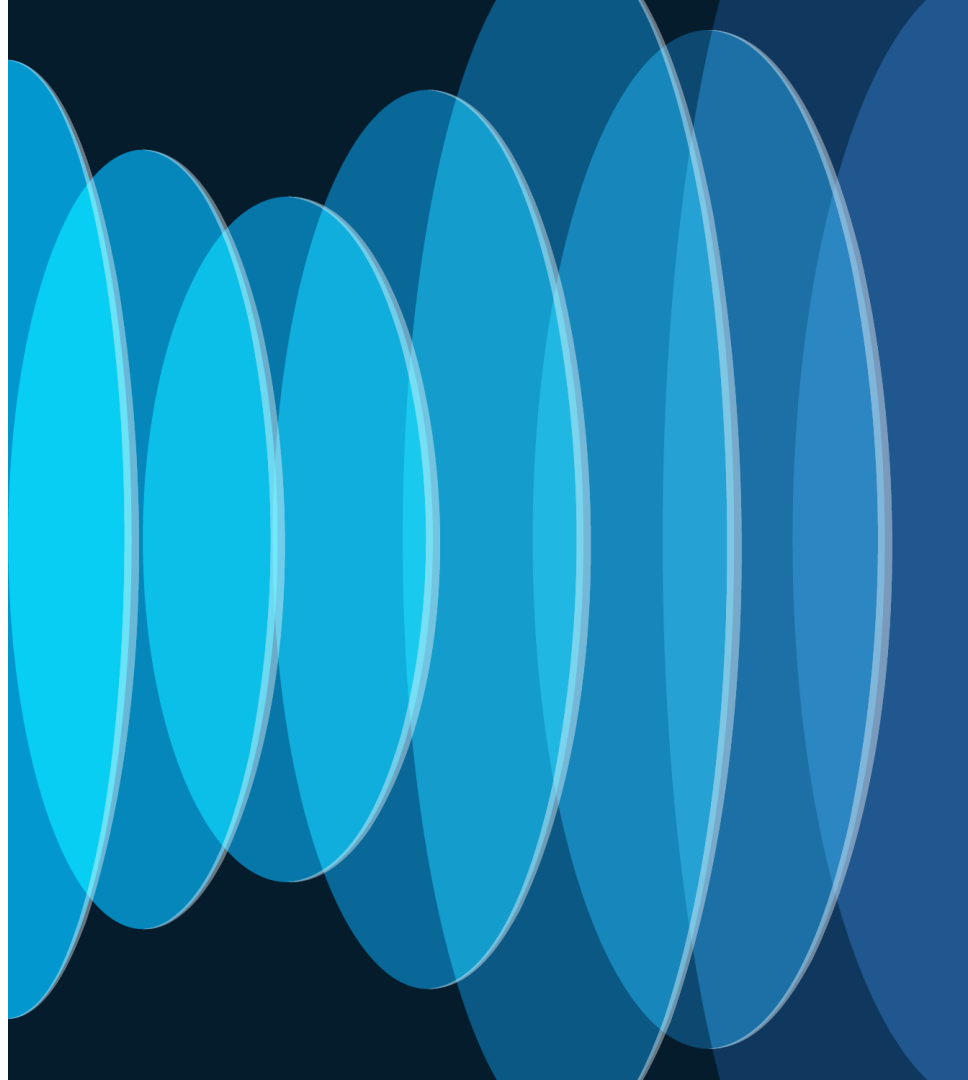
- The API's available in Catalyst Center allows you to retrieve raw startup, running configs and VLAN DB.
- API details:
 - POST /network-device-archive/cleartext
 - A zip file is generated which contains raw running-config, startup-config and VLAN DB



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



SWIM Demo



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](#) where ISSU not available
- Consider [external file servers](#) for remote sites
- [Install Mode](#) is recommended mode
 - “Bundle”/”Install” mode [conversion is not supported](#)

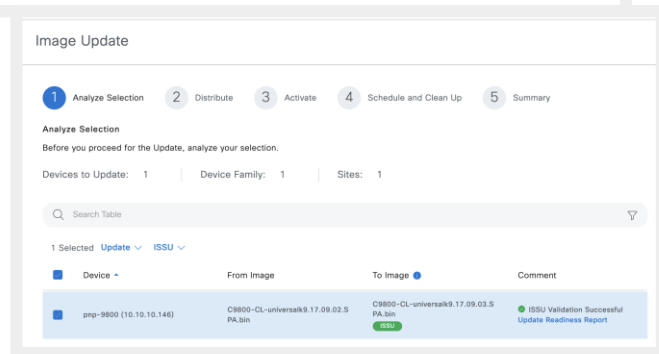
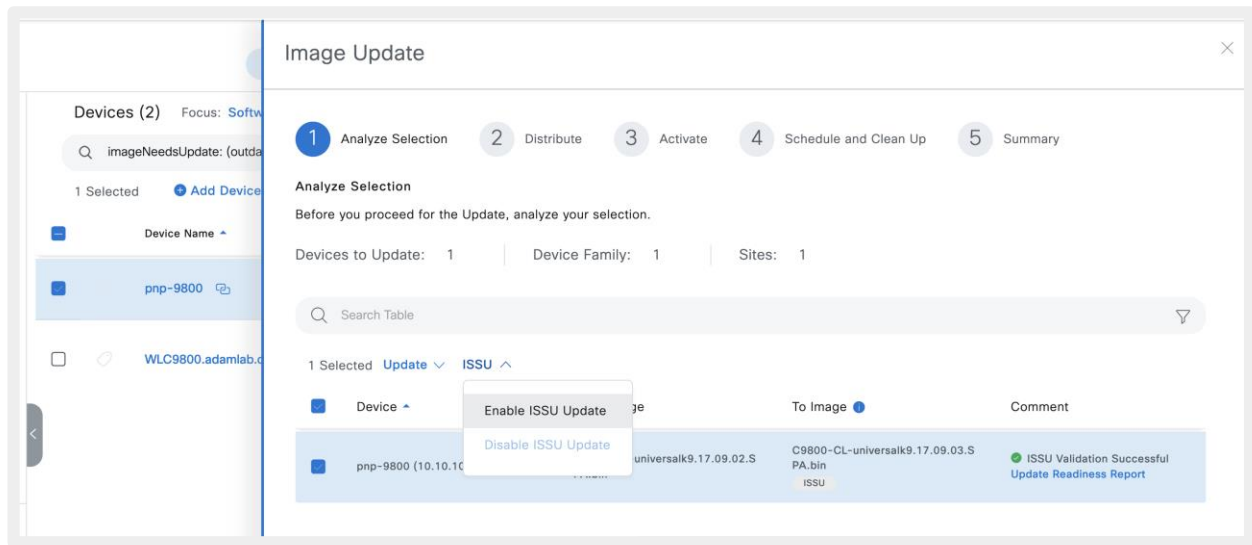
Control over SWIM- ISSU

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



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	✓ 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

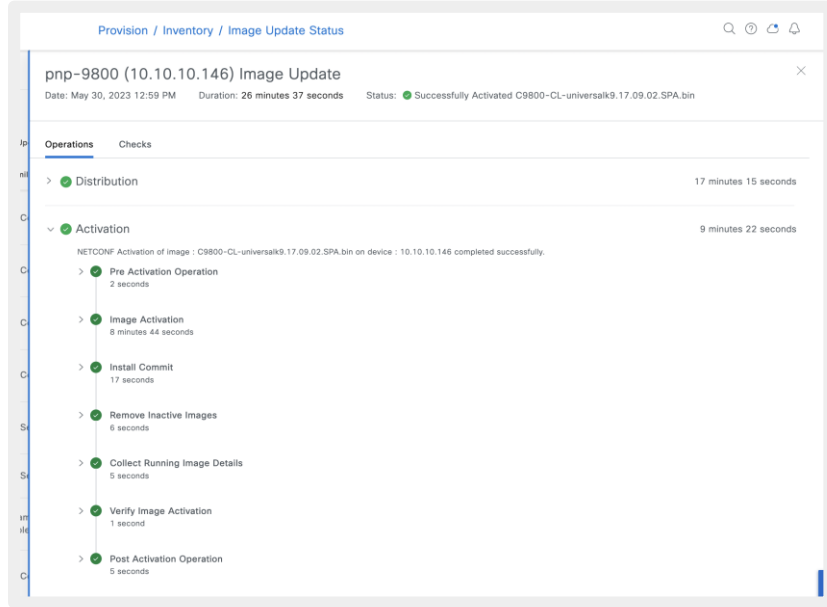
AP Pre-image download by default available starting version 2.3.3.x

The screenshot shows the Cisco DNA Center interface for managing network devices. The main heading is "9800_SWIM (172.100.1.54) Image Update". Below this, the date and duration are shown: "Date: Sep 27, 2022 4:20 PM" and "Duration: 27 minutes 7 seconds". The status is "Successfully Activated C9800-CL-universalk9.16.12.05.SPA.bin".

The interface is divided into several sections:

- SUMMARY**: Shows "Task Names (4)" and "Image Versions (7)".
- Devices Updates**: A table listing devices and their update status. The table has columns for "Device Name", "Image Version", and "Status". The devices listed are "New-Cat9300-St", "9800_SWIM (172.100.1.54)", and "New-Cat9300-St".
- Operations**: A section showing the progress of the update operation. It includes a "Task Name" of "AP Pre-Image Download" and a "Task Status" of "Success". The status details are: "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." The operation took "8 minutes 6 seconds".
- Checks**: A section showing the progress of the update operation. It includes a "Task Name" of "Activation" and a "Task Status" of "Success". The operation took "13 minutes 15 seconds".

Activation for normal wireless vs ISSU wireless



Provision / Inventory / Image Update Status

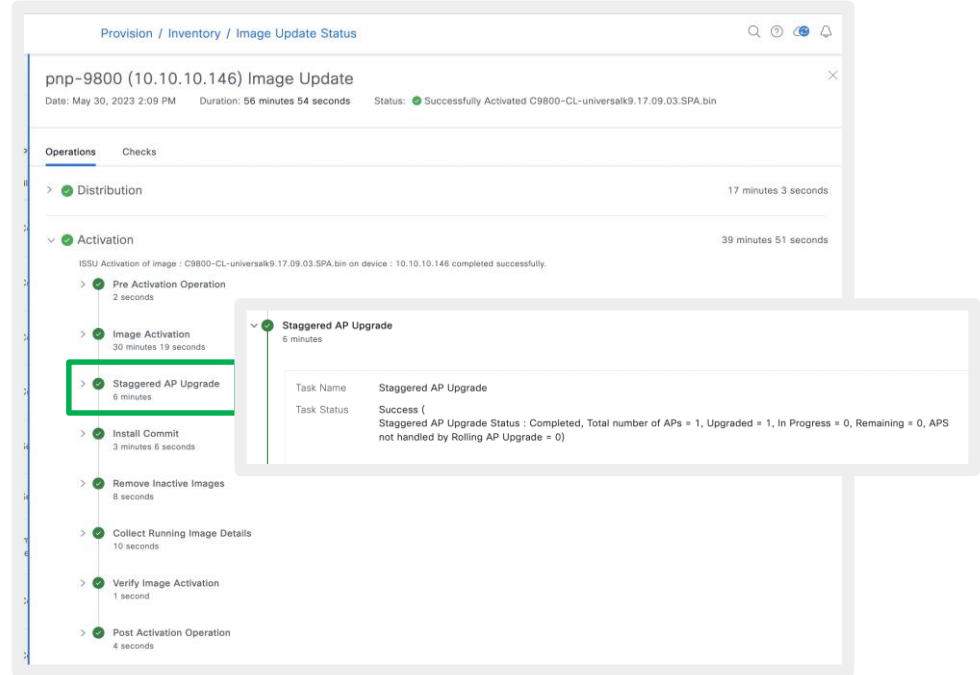
pnp-9800 (10.10.10.146) Image Update

Date: May 30, 2023 12:59 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

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 displays the Cisco Catalyst 9300 Switch Image Repository. On the left, a sidebar shows navigation options: Roles & Tags, Major Versions, Golden Images, and Recommendation. The main area shows a list of 35 images. A specific image, 'cat9k_iosxe.17.09.04.SPA.bin', is highlighted with a green box around its version '17.09.04.0.5180' and a link 'Add On (1)'. A green arrow points from this link to a detailed view of the 'Add On List (1)'. This view shows the 'Add On' image 'cat9k_iosxe.17.09.04.CSCwh87343.SPA.smu.bin' with various attributes. A green box highlights the 'Golden Image' status, which is 'Not Available' because the base image is not tagged with role ALL. Other attributes include Description (Cisco IOS-XE Patch package), Defects, CVEID(S), Reboot Required (Yes), Category (bulk-patch), Supersedes (Not Available), Compliant Devices (Not Available), and Image Verification (Verified).

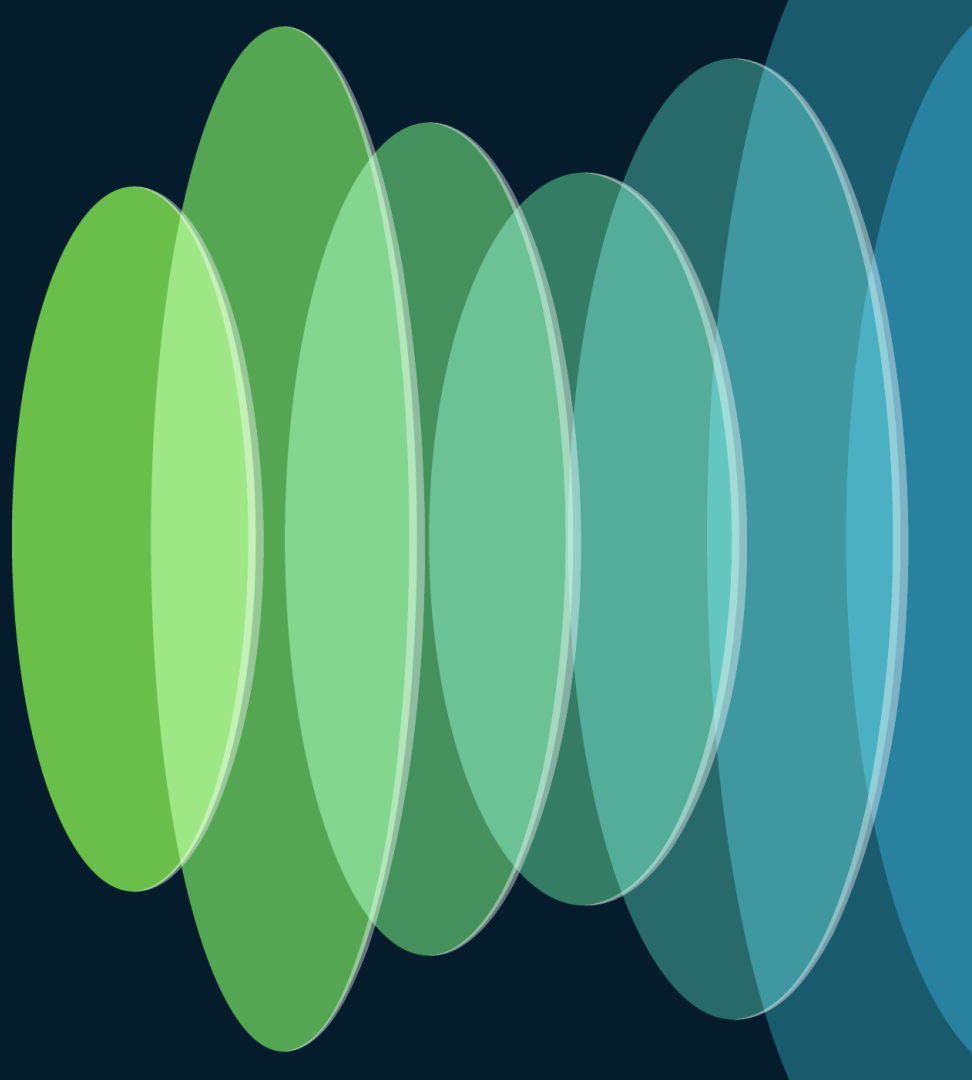
Need to mark as golden (along with main image)

Downloadable direct from CCO

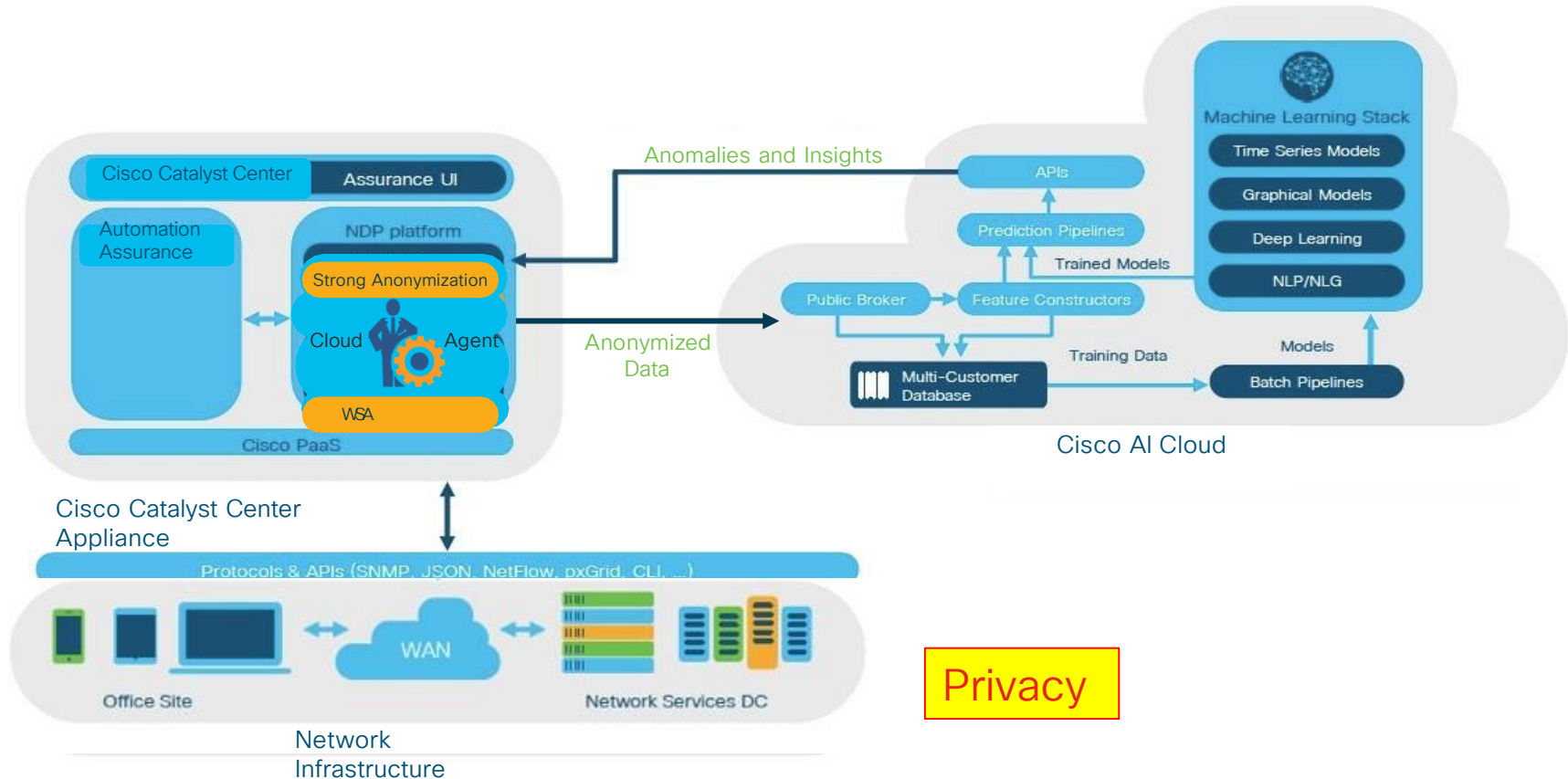
Wireless APSP and APDP are also supported (9300 EWC – SDA Mode)

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:



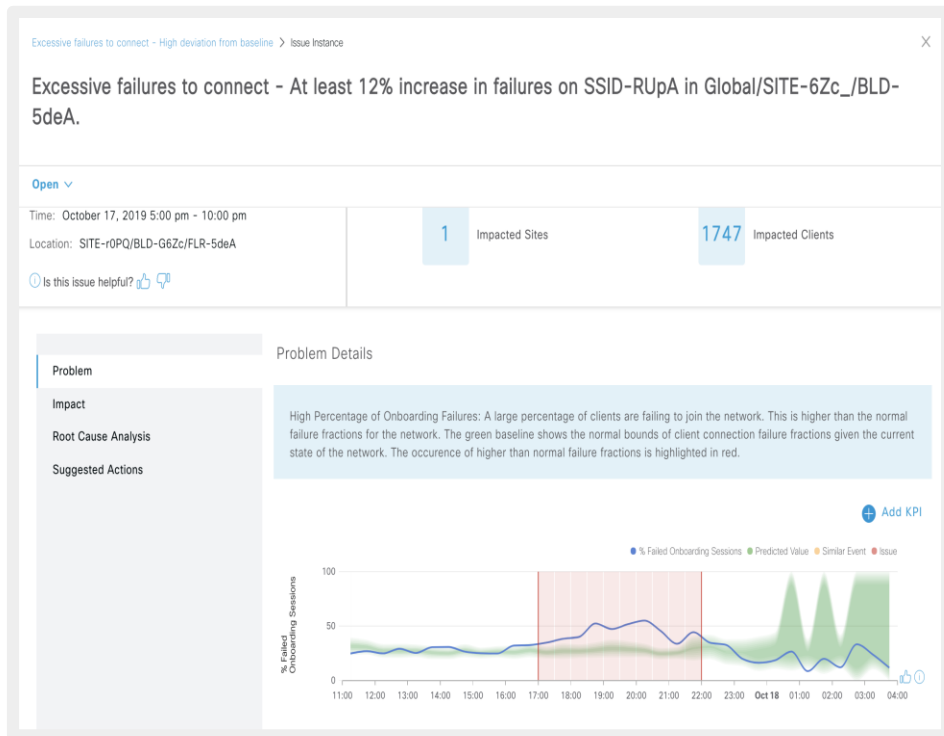
View Dynamic baselines and deviations for 12 (onboarding + throughput) KPI's



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



Active feedback loop (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.



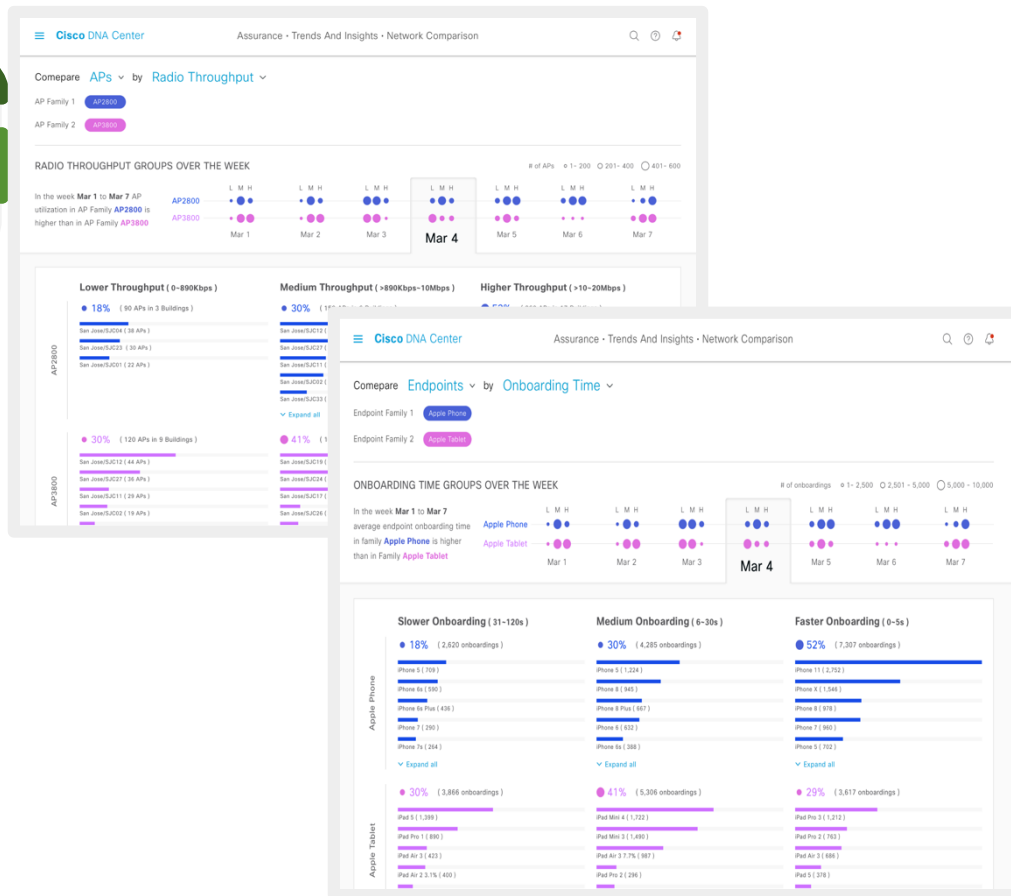
Flexibility to compare both on-boarding and throughput KPI's



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

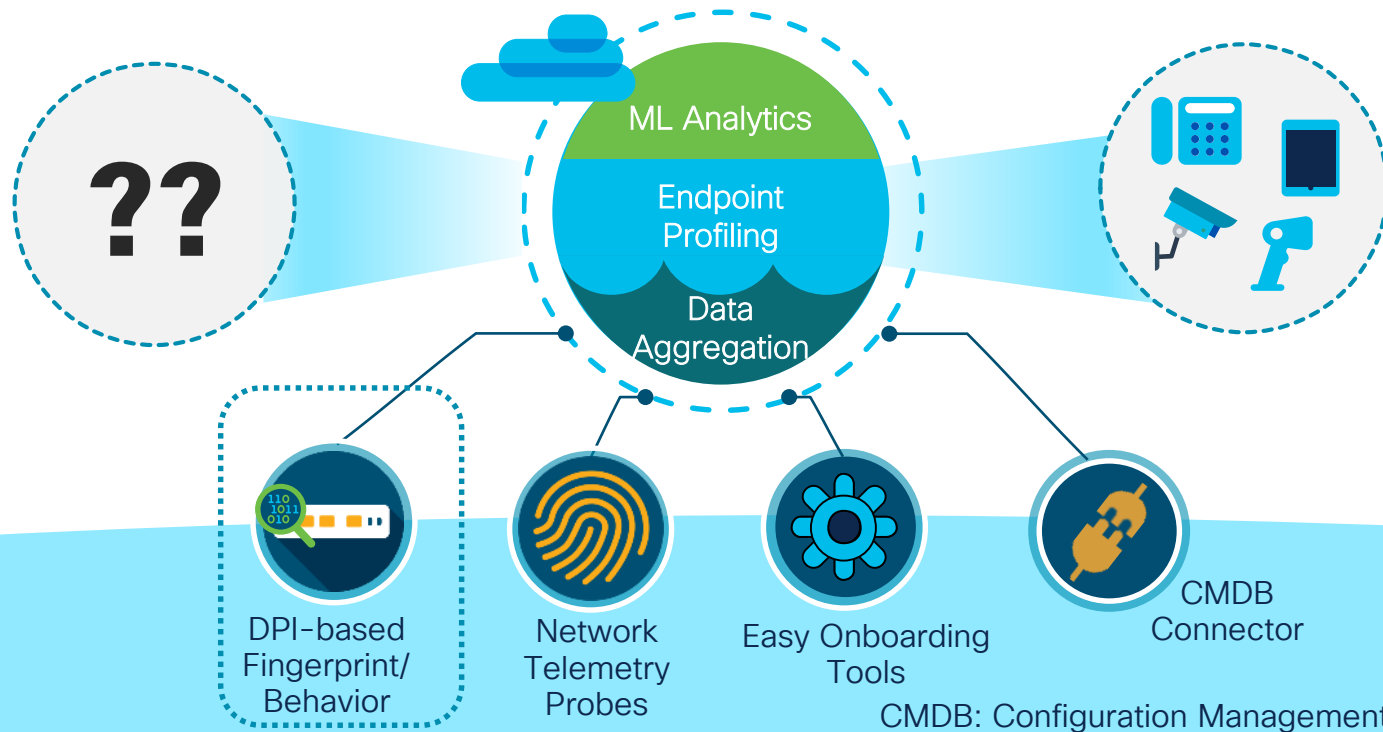


View and compare onboarding KPIs for specific device types for days of a week..

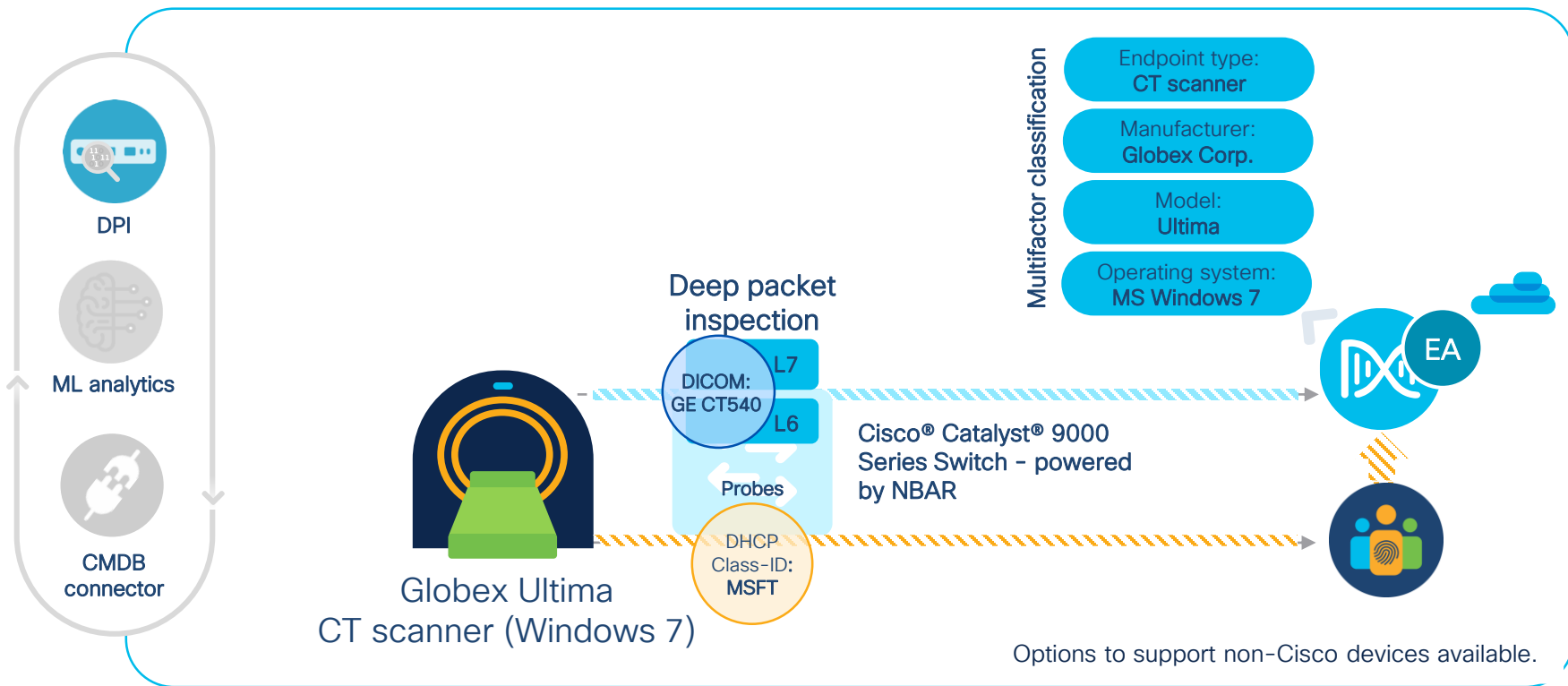


AI Endpoint Analytics on Cisco Catalyst Center

Rapidly reducing the unknowns by aggregating data from different sources



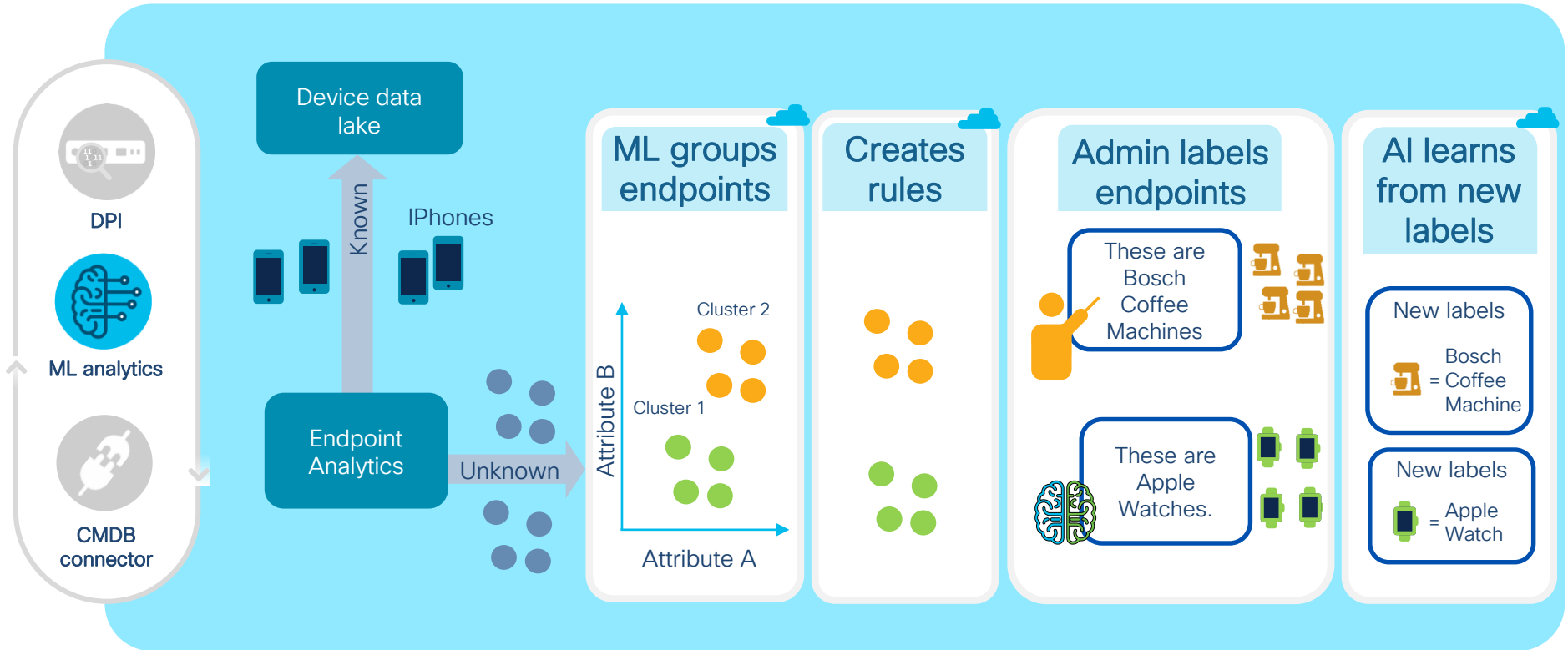
Classification based on Deep Packet Inspection (DPI)



Reducing Unknowns with Machine Learning

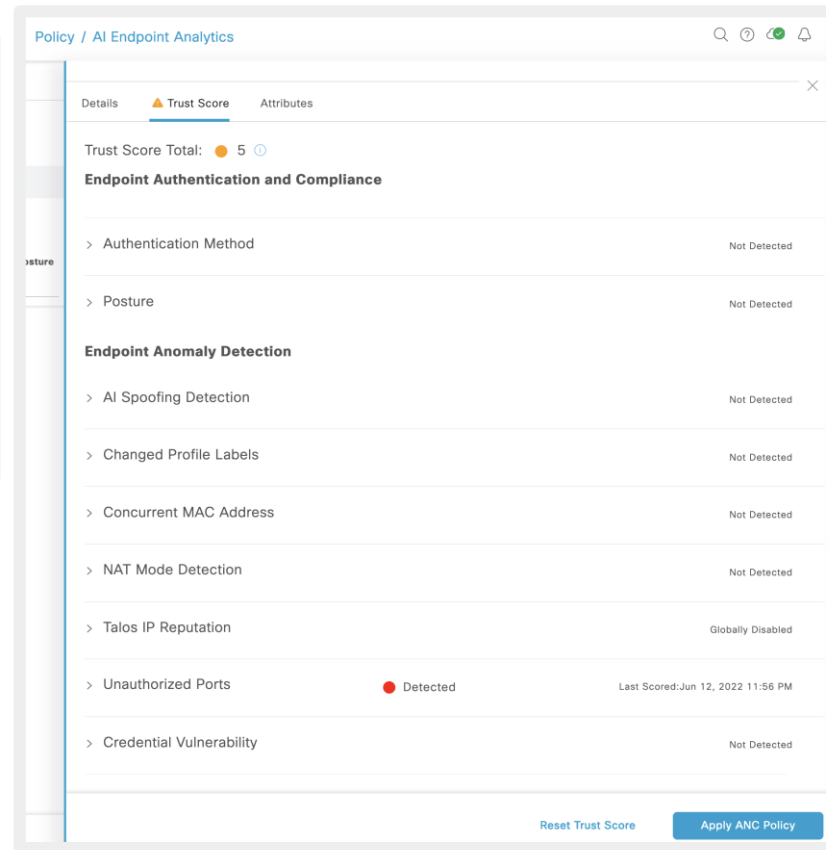
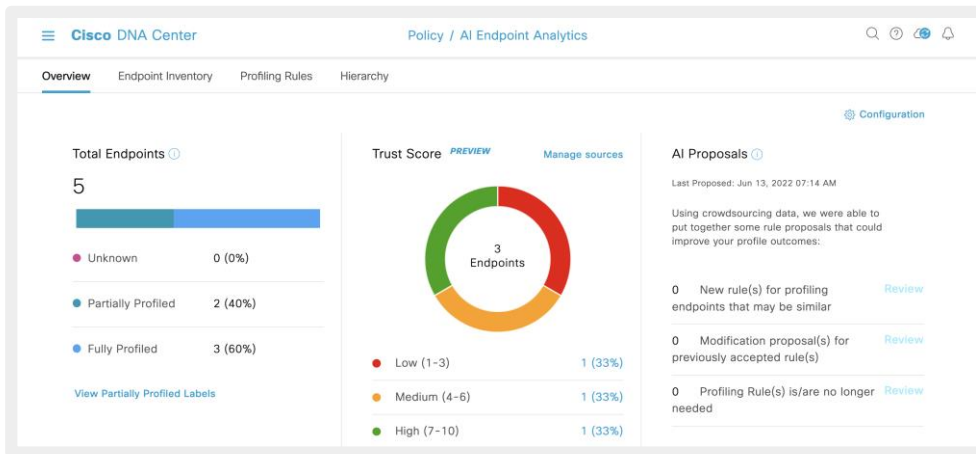


Reference



= done in cloud

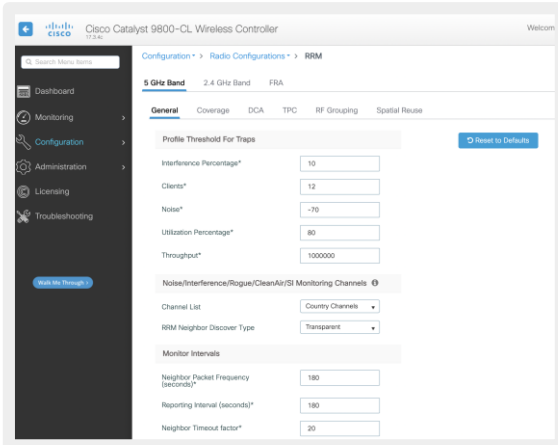
Trust Scores and Remediation



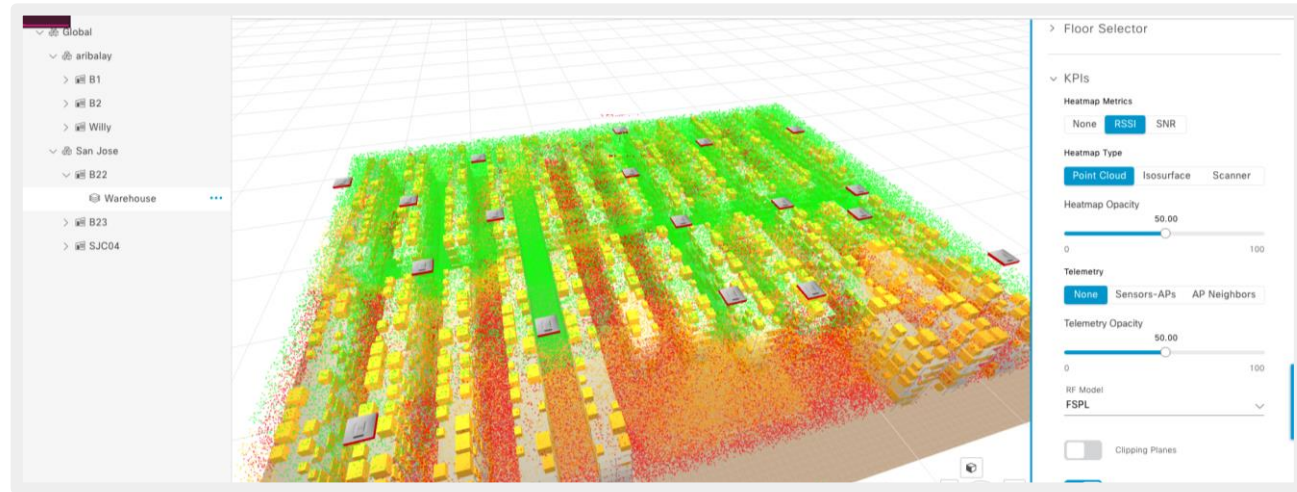
Adaptive Network Control - ANC

Remediate the host via Identity Services Engine - ISE

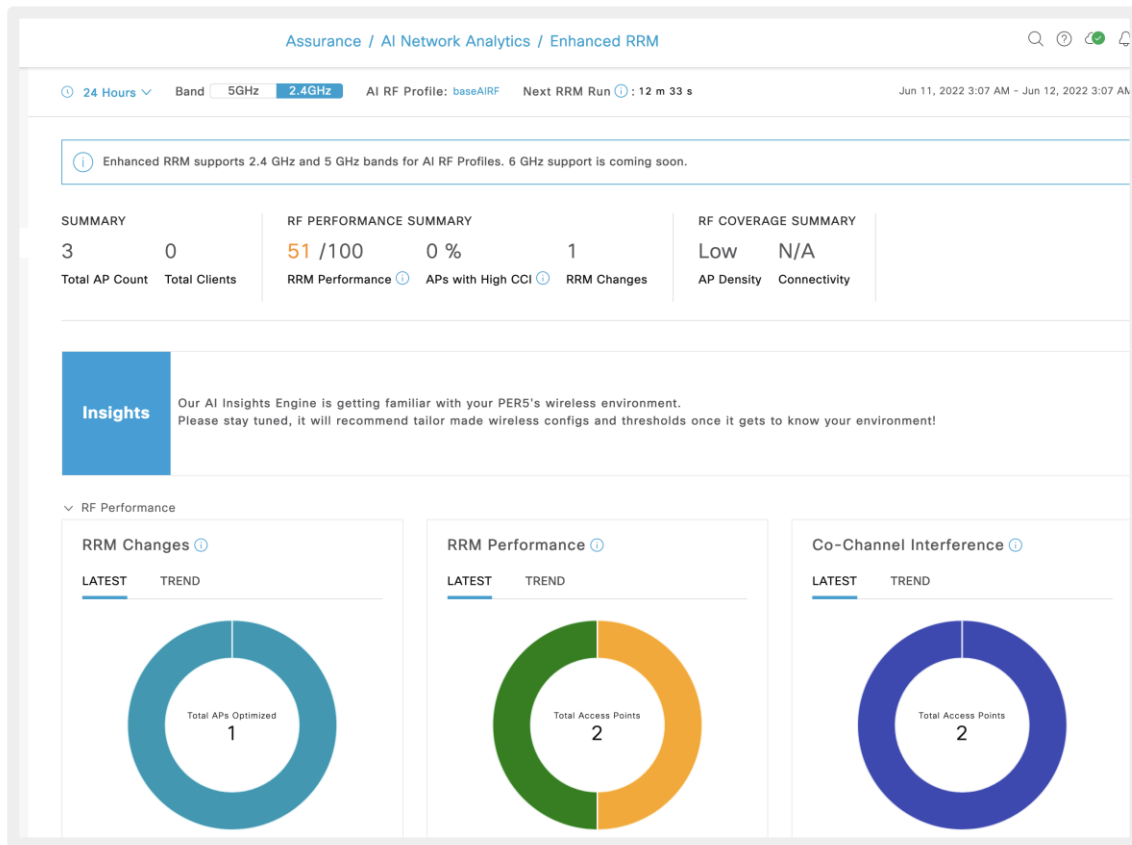
Why radio resource management



- 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

 Catalyst Center

Configure AI-Enhanced RRM

Select Deployment Type

Select how you would like to deploy AI-Enhanced RRM

Enable Without Device Provisioning

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.

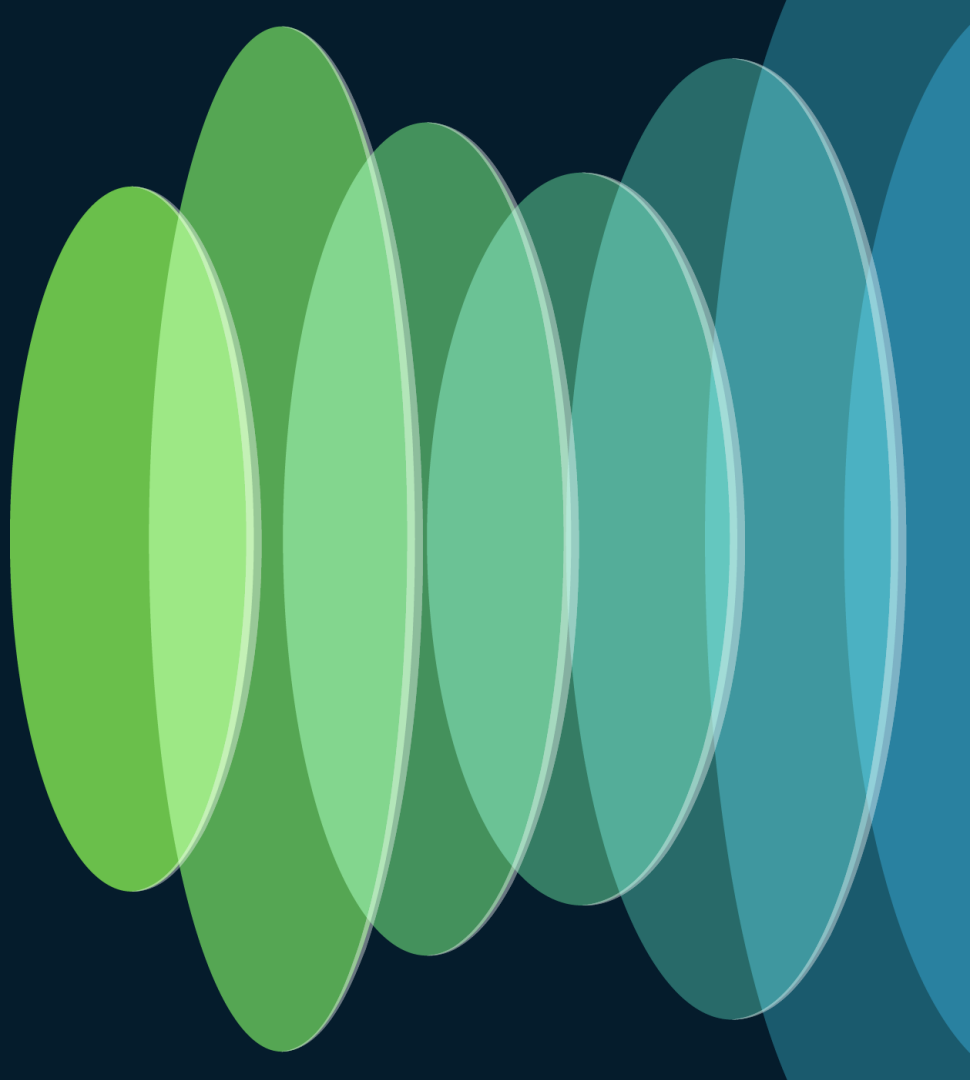
If you do not want Catalyst Center to manage the configuration of your devices, choose this option.

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 includes a description: '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.' Below this, there are 'Add' and 'Export' buttons. A table lists the configured servers with columns for IP Address, Protocol, Type, Status, and Actions. The table contains three entries: two RADIUS servers (AAA) and one ISE server (ACTIVE). The status of the ISE server is highlighted in blue.

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.

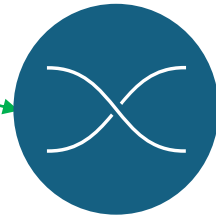
Other AAA servers can be added, but as an AAA server only (even if they are ISE servers)

Difference between ISE and AAA integration

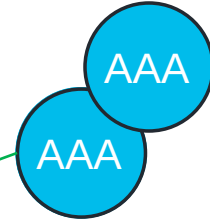


ISE

- 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

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 top navigation bar includes 'Cisco DNA Center' and 'Design / Network Settings'. Below this, a tabbed interface shows 'Network' as the active tab, with other tabs like 'Device Credentials', 'IP Address Pools', 'SP Profiles', 'Wireless', 'Telemetry', and 'Security and Trust'. On the left, a 'Find Hierarchy' search bar is present, and a tree view lists various sites under 'Global', including AUS, brownfield, C, CLMEL, DC - syd, deak, EK, flex_area, HongKong, nirvana, NZ, PIM, spécial, stores, test, and thirdwheel. The main content area is titled '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, the 'AAA Server' configuration is shown. It has two sections: 'NETWORK' and 'CLIENT/ENDPOINT'. Each section has a 'Servers' table with columns for 'Protocol' and 'IP Address (Primary)'. In the 'NETWORK' section, the 'ISE' protocol is selected, and the IP address is '10.66.104.67'. In the 'CLIENT/ENDPOINT' section, the 'RADIUS' protocol is selected, and the IP address is '10.10.10.127'. Both sections have a 'Change Shared Secret' link.

Cisco DNA Center Design / Network Settings

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

Find Hierarchy Search Help

Global

- AUS
- brownfield
- C
- CLMEL
 - DC - syd
 - deak
- EK
- flex_area
- HongKong
 - nirvana
- NZ
- PIM
 - spécial
- stores
 - test
- thirdwheel

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.

AAA Server

☒ Network ☒ Client/Endpoint

NETWORK

Servers	Protocol
☒ ISE ☐ AAA	☒ RADIUS ☐ TACACS
Network	IP Address (Primary)
10.66.104.67	10.10.10.127

[Change Shared Secret](#)

CLIENT/ENDPOINT

Servers	Protocol
☒ ISE ☐ AAA	☒ RADIUS ☐ TACACS
Client/Endpoint	IP Address (Primary)
10.66.104.67	10.10.10.127

[Change Shared Secret](#)

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 dot1x 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
dot1x system-auth-control
```

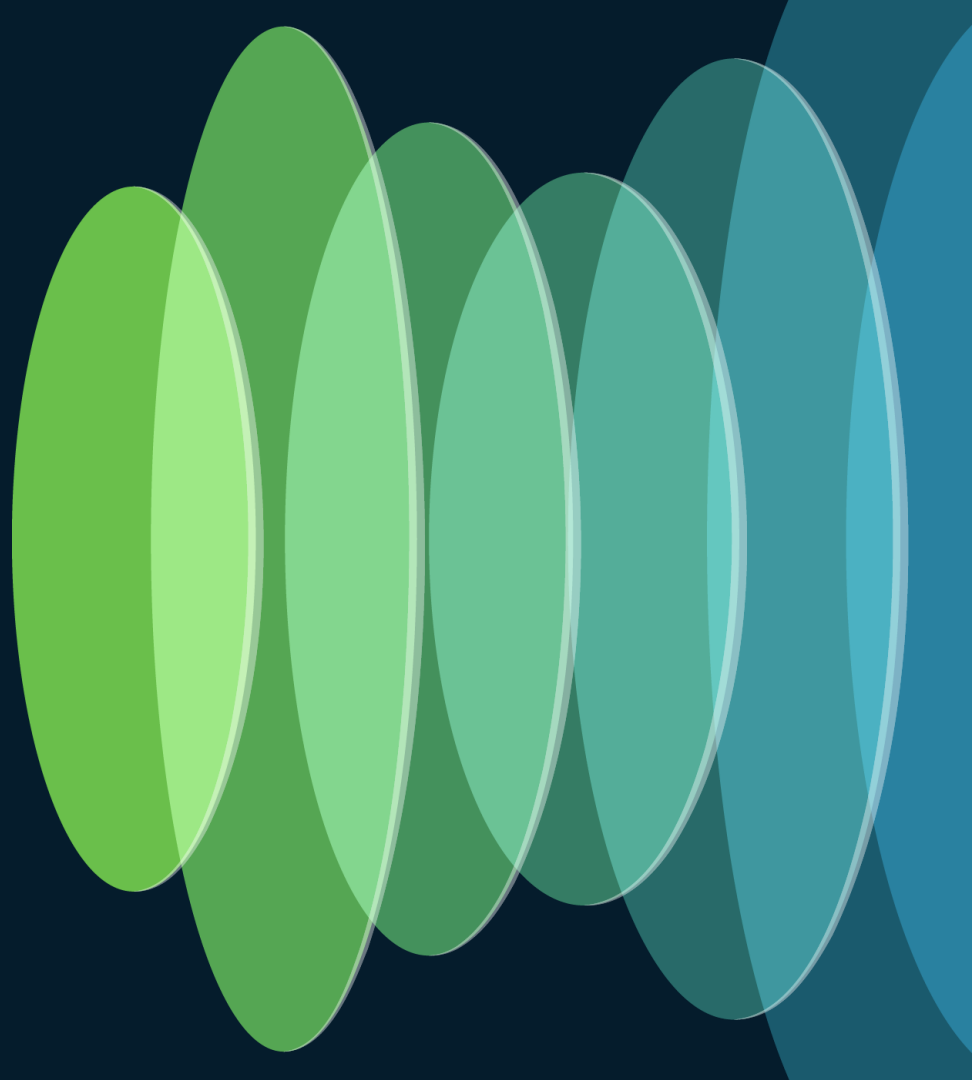
```
authentication radius server dnac-radius_10.10.10.127
  address ipv4 10.10.10.127 auth-port 1812 acct-port 1813
  pac key *****
  retransmit 3
  timeout 4
  automate-tester username dummy ignore-acct-port probe-on
  exit
radius-server vsa send authentication
radius-server vsa send accounting
radius-server 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



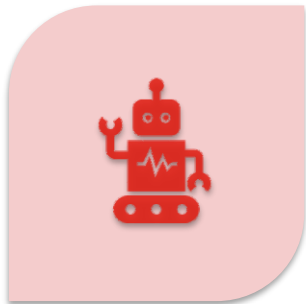


DRIVE FOR
SHOW
AND
PUTT FOR
DOUGH



GUI FOR
SHOW
AND
API FOR
DOUGH

Why API?



AUTOMATION



INTEGRATION



INNOVATION

API First 2.3.7.7 release notes

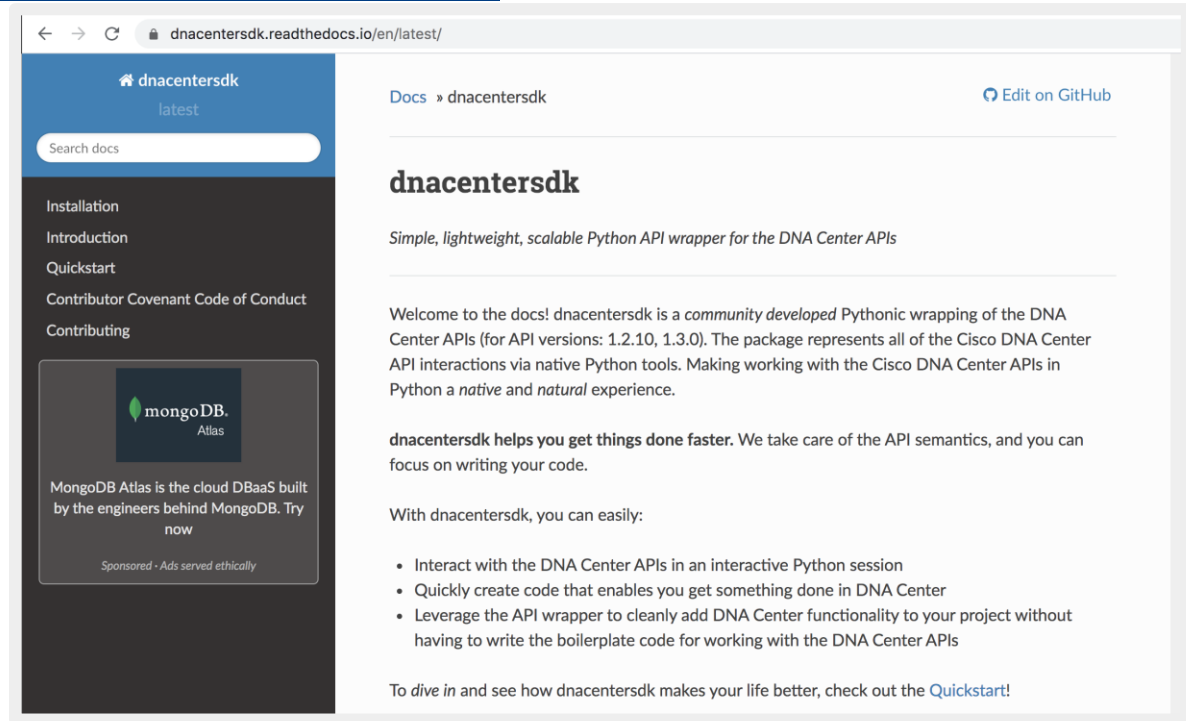
Table 6. New and Changed Features in Catalyst Center Platform, Release 2.3.7.7	
Feature	Description
New APIs	
Compliance API	Catalyst Center platform supports the following Compliance API: • POST <cluster-ip>/dna/intent/api/v1/compliance/networkDevices/\${id}/issues/remediation/provision Compliance Remediation 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.
Issues APIs	Catalyst Center platform supports the following Issues APIs: • 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. 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.
Licenses APIs	Catalyst Center platform supports the following Licenses APIs: • PUT <cluster-ip>/dna/intent/api/v1/licenseSetting Update license setting. • GET <cluster-ip>/dna/intent/api/v1/licenseSetting Retrieve license setting. 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.
Network Settings APIs	Catalyst Center platform supports the following Network Settings APIs: • 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. 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.
SDA APIs	Catalyst Center platform supports the following SDA APIs: Multicast APIs • 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	Catalyst Center platform supports the following Site Design APIs: • 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 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
SWIM APIs	Catalyst Center platform supports the following SWIM APIs: • 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>/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 dnacentersdk documentation website. The browser address bar displays `dnacentersdk.readthedocs.io/en/latest/`. The page has a blue header with the `dnacentersdk` logo and a search bar. A left sidebar lists navigation links: Installation, Introduction, Quickstart, Contributor Covenant Code of Conduct, and Contributing. Below these links is a MongoDB Atlas advertisement. The main content area shows the breadcrumb `Docs » dnacentersdk` and an `Edit on GitHub` link. The title `dnacentersdk` is followed by the tagline `Simple, lightweight, scalable Python API wrapper for the DNA Center APIs`. The introductory text describes the package as a community-developed Pythonic wrapper for DNA Center APIs (versions 1.2.10, 1.3.0). A bulleted list highlights key features: interacting with APIs in an interactive Python session, quickly creating code for DNA Center tasks, and leveraging the API wrapper to avoid boilerplate. The page concludes with a link to the `Quickstart!`.

Go/Ansible/Terraform



Reference

cisco-en-programmability / dnacenter-go-sdk

<> Code Issues Pull requests 1 Actions Projects Wiki Security Insights

main 8 branches 28 tags

Go to file Code

fmunozmiranda Update README.md

85a926c 17 days ago 179 commits

.github	Update issue templates
examples	Update module version
scripts	Add workflow and scripts
sdk	- Changed "RequestConfiguration"
.gitignore	Initial SDK commit
CHANGELOG.md	- Changed "RequestConfiguration"
LICENSE	Included LICENSE, more details t
Makefile	Add Makefile
README.md	Update README.md
go.mod	Update module version
go.sum	Update dependencies

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

ANSIBLE GALAXY

Home Search Community

Community Authors > cisco > dnac

dnac
Ansible Modules for Cisco DNA Center

Details Read Me Content

Info

Installation

```
$ ansible-galaxy collection install cisco.dnac
```

NOTE: Installing collections with ansible-galaxy is only supported for Ansible 2.10 and later.

Install Version

6.4.0 released 2 months ago (latest)

Tags

cisco dnac cloud collection networking sdn

Ansible Collection - cisco.dnac

Ansible Modules for DNA Center

The dnacenter-ansible project provides an Ansible collection for managing and automating tasks related to 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 release history is available in the [Compatibility matrix](#).

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

Terraform Registry

Search Providers and Modules

Providers / cisco-en-programmability / dnacenter / Version 0.3.0-beta / Latest Version

dnacenter

en

dnacenter

by cisco-en-programmability

Networking

VERSION
0.3.0-beta

PUBLISHED
2 months ago

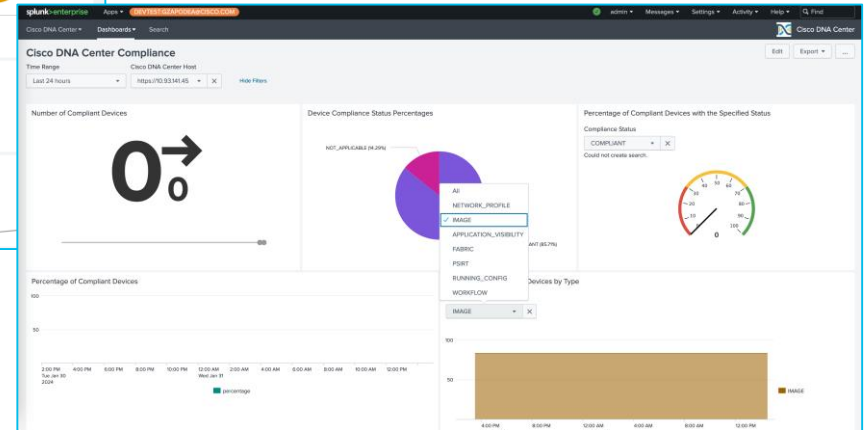
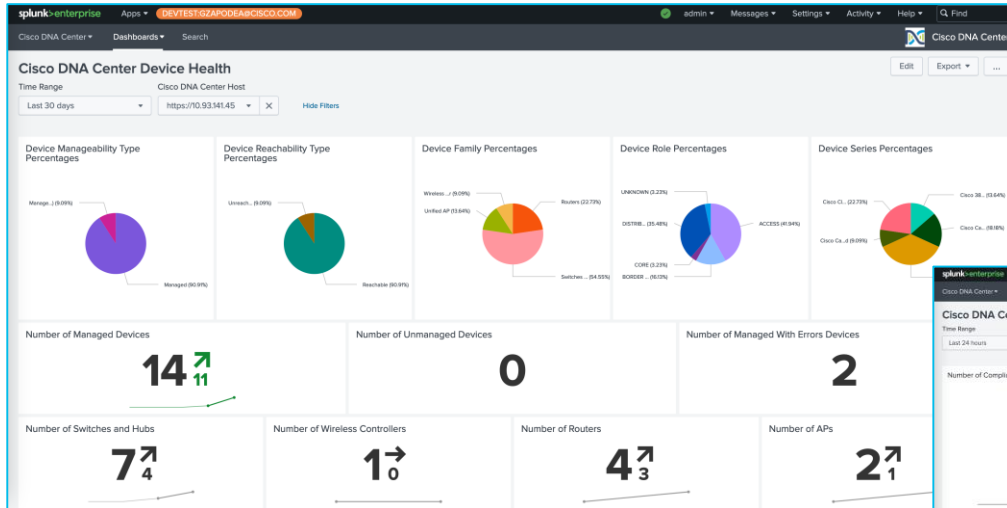
SOURCE CODE
[cisco-en-programmability/terraform-provider-dnacenter](https://github.com/cisco-en-programmability/terraform-provider-dnacenter)

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

CISCO Live!

Splunk Integration (existing)

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



Native Webex Issue Integration



Reference

The screenshot shows a Webex chat window for a contact named 'dnac_webex' (DNAC-BOT). The chat history shows a message from 'dnac_test_bot' at 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'.

2.3.7.5 - L2 advanced port configuration

All Devices / 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: 4m

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



● Connected ● Error Disabled ● Admin Disabled ● Not Connected ⚡ PoE Enabled

▼ System

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	FCW21A0000000000000000000000000000

[View System Details](#)

▼ Layer 2 Configuration BETA [Edit](#)

CDP	Enabled	STP Mode	Rapid- Spanning Tree
LLDP	Enabled	VTP Mode	Transparent
IGMP Snooping	Enabled	MLD Snooping	Disabled
VLANs	7	Port Channels	0
Ports	65		

[View Layer2 Details](#)

Port Name

Port Name (65)

Search Table

1 Selected Edit

Port Name

AppGigabitEthernet1/0/1

FortyGigabitEthernet1/0/24

FortyGigabitEthernet1/0/25

FortyGigabitEthernet1/0/26

GigabitEthernet1/0/27

GigabitEthernet1/0/28

GigabitEthernet1/0/29

ResetSet to Default

Port NameGigabitEthernet1/0/1

Configuration

Switchport Description

Switchport ModeDynamic Auto

Switchport Access VLAN ID1

Switchport Voice VLAN ID

Switchport Admin StatusNo Shutdown

Authentication ModeOpenClosed

No Shutdown

CancelSave

Add extra attributes

Edit Port / Add Configurations

Search

Add All 25 Unselected Remove All 1 Selected

- + CTS SGT
- + CTS SGT-Propagate
- + CTS SGT-Trusted
- + DHCP Snooping Rate
- + DHCP Snooping Trust
- + LLDP Receive/Transmit
- + Switchport DTP Negotiation
- + Switchport Native VLAN
- + Switchport Protected
- + Switchport Pruning VLAN
- + VTP Admin Status

✕ Switchport Allowed VLAN

Cancel Add

Edit Port

↶ Reset ↶ Set to Default

Switchport Mode ⓘ Dynamic Auto ⓘ

Switchport Access VLAN ID ⓘ 1 ⓘ

Switchport Voice VLAN ID ⓘ

Switchport Admin Status ⓘ No Shutdown ⓘ

Authentication Mode ⓘ ☒ Open ☐ Closed

Switchport Allowed VLAN ⓘ  ALL

+ Add Configurations

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

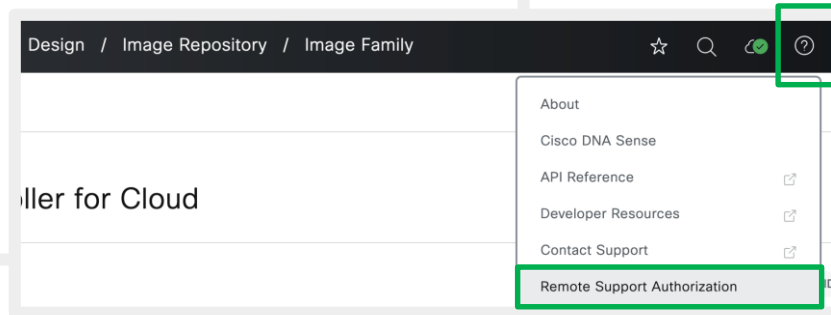
Untouched inventory from service co4z-4 wrd-w455.
>>> dnac=service.inventory["10-66-104-121"]
>>> dnac.interactive()
22:13:27.178Z INFO | internal | starting interactive session (will be closed when detached)
22:13:27.778Z INFO | internal | Session log initialized [filepath='/Users/aradford1/.radkit/session_logs/client/20230803-081327-10-66-104-121.log']

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
```



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

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.



Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn **exclusive prizes!**



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

Continue your education

CISCO *Live!*



cisco.com/go/catalyst-center



www.youtube.com/@CiscoCatalystCenter



cs.co/dnac-resources

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer 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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive