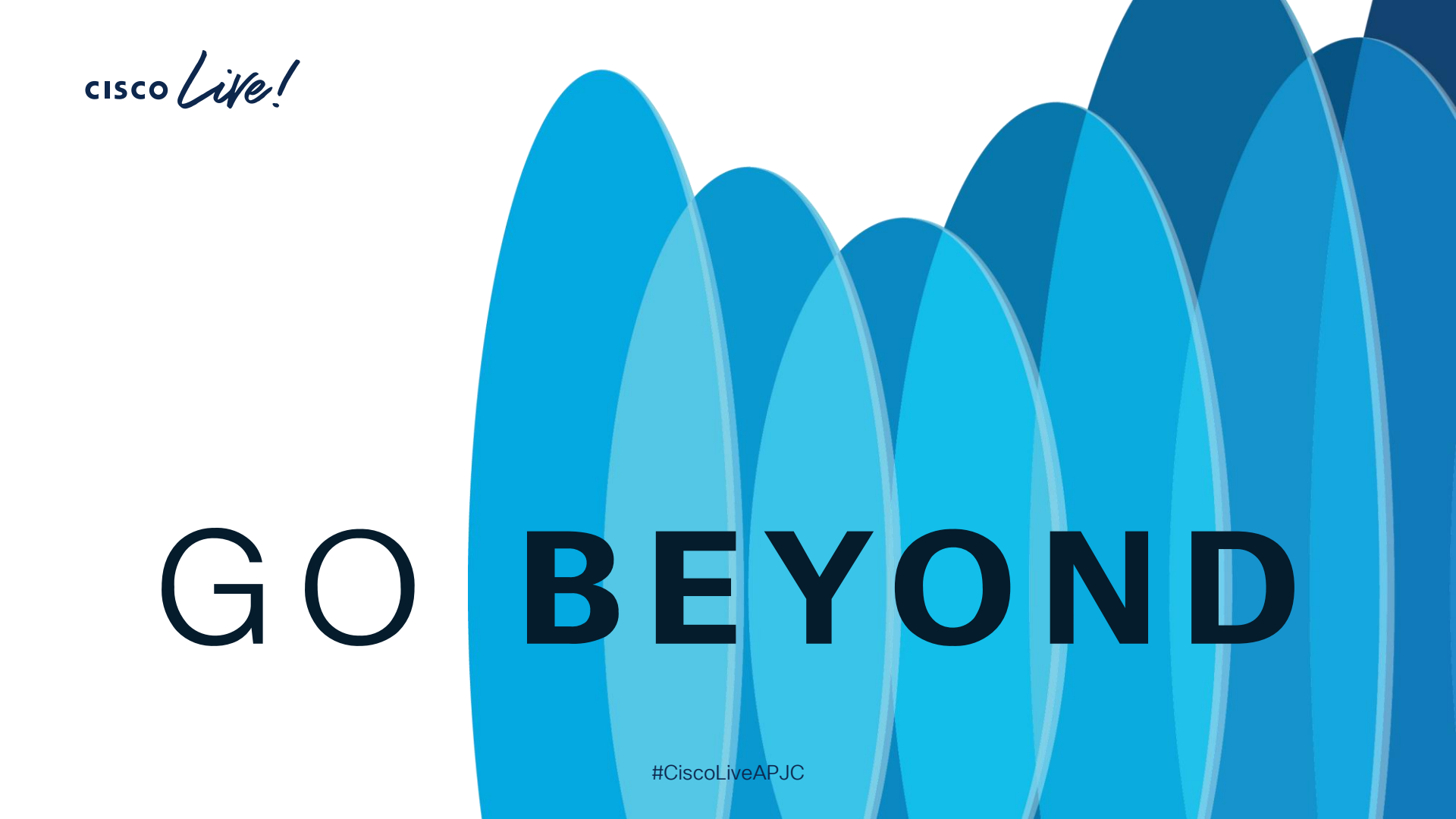

cisco Live!
GO BEYOND
#CiscoLiveAPJC

"Reconciliation"- Dustin Koa Art

7 Habits for success with Cisco Catalyst Center

Adam Radford, Distinguished Solutions Engineer
@adamradford123

BRKOPS-2416

Cisco Webex App

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

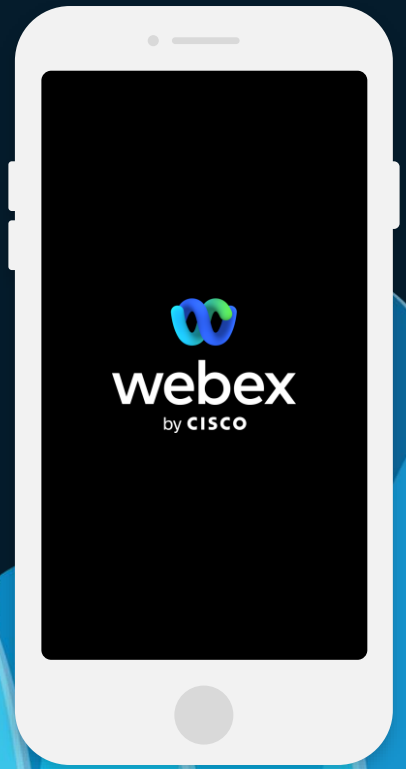
Questions?

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

How

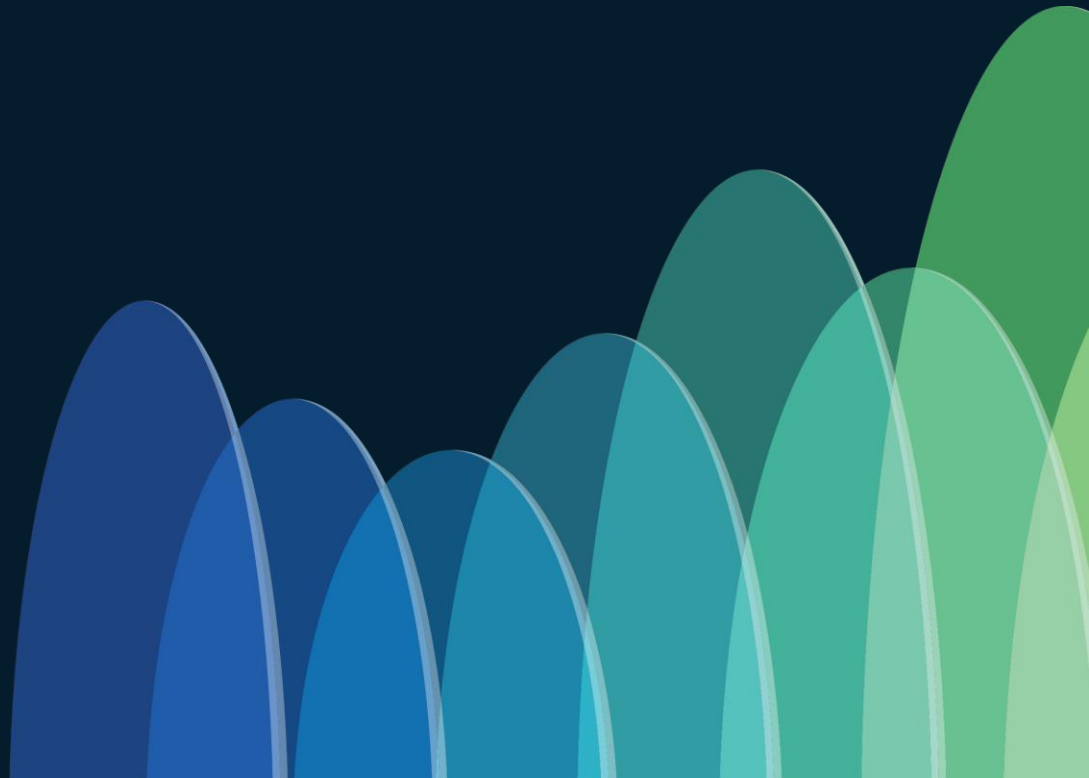
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

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



cisco Live!

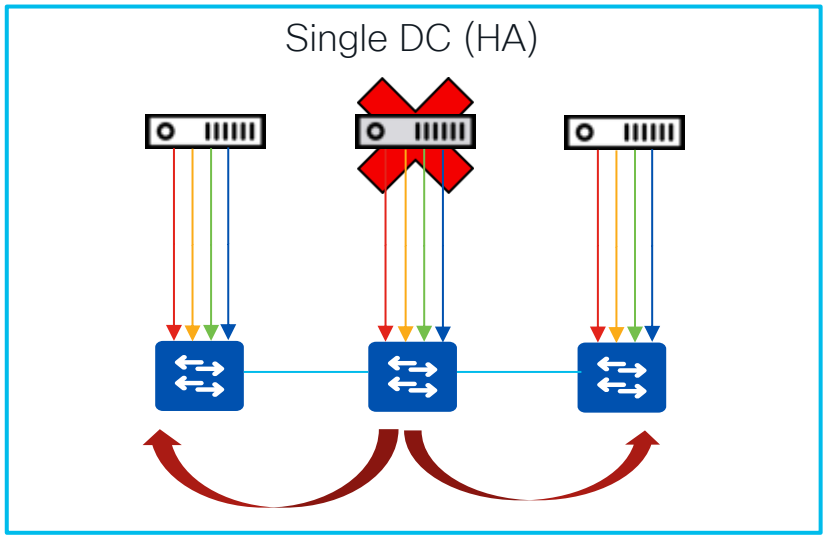
Habit #1 – Understand Cisco Catalyst Center Resiliency and design what's best for your environment



cisco Live!

Physical Appliance High Availability with clustering

Physical Appliance



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

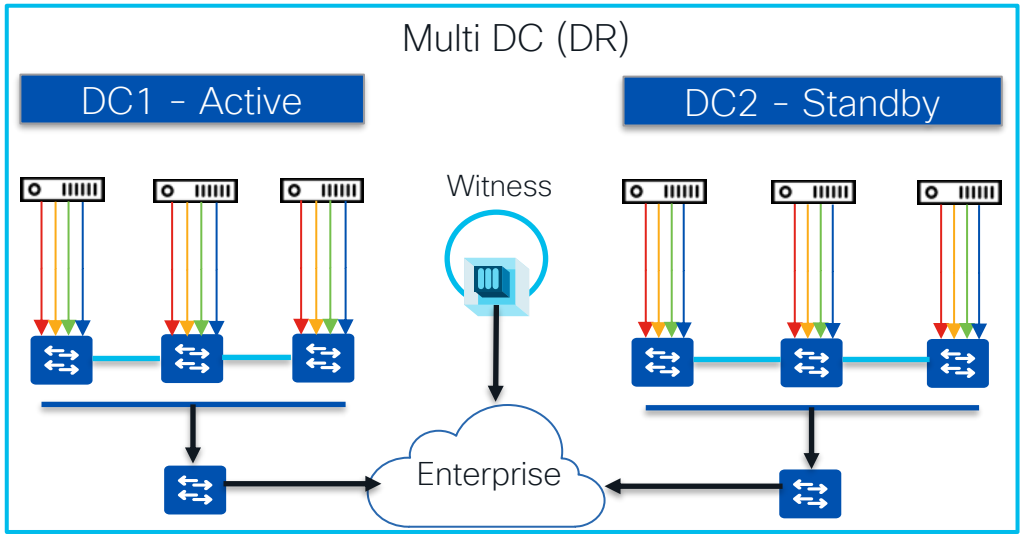
Considerations

- Hardware Appliance needs to match
- 3-node cluster in single DC
- DN3 can't cluster with DN2 (temporary)

Catalyst Center High Availability: *https://youtu.be/06sQYUsAdSo?si=a0RjbblJS5I1mVpM*

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

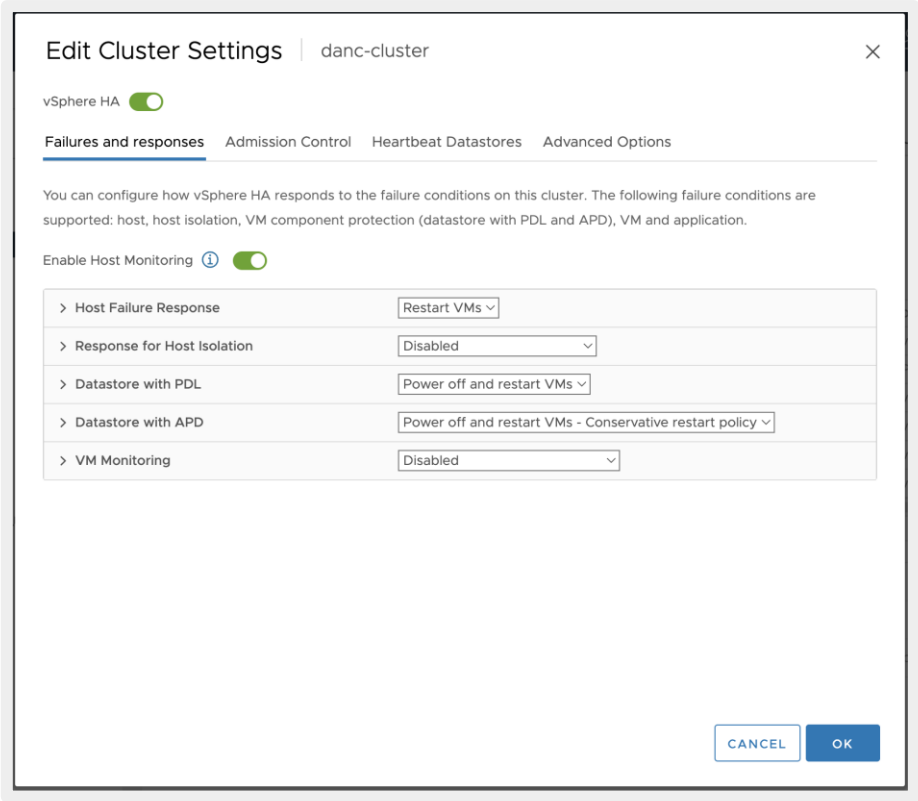
- Identical third-party certificates on both DR clusters. Don't use self-signed certs
- Deploy witness in a third location
- DR VIP with BGP advertisement recommended for L3

How to Configure Disaster Recovery: *https://youtu.be/PVQi_9h8iSg?si=g02hVIwJzDGBIZOT*

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

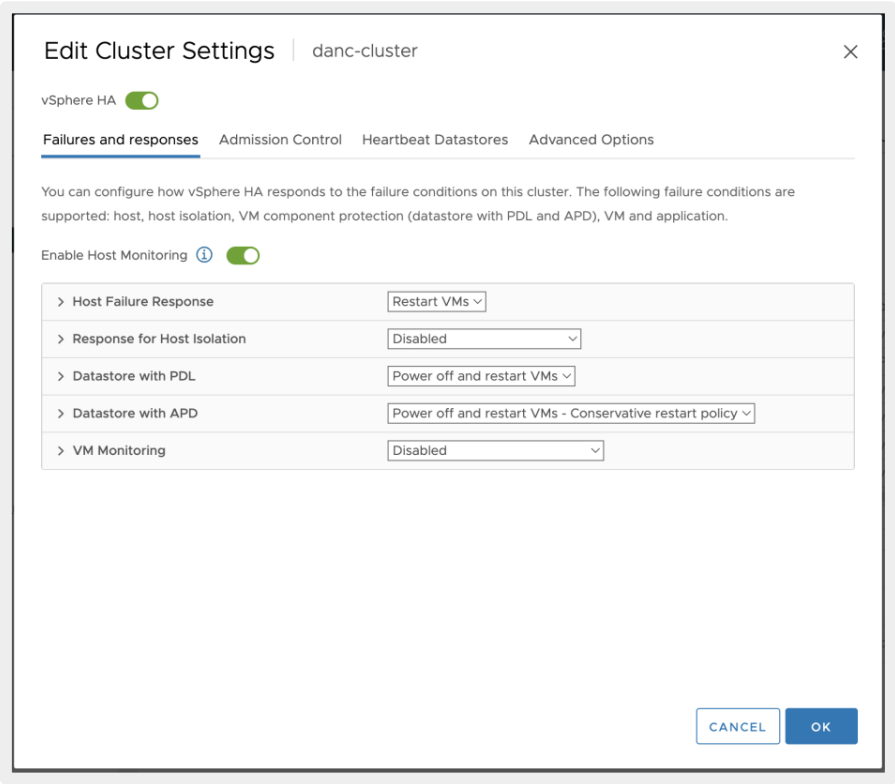


High Availability in ESXi VA

ESXi High Availability delivered via VMware vSphere's HA functionality

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

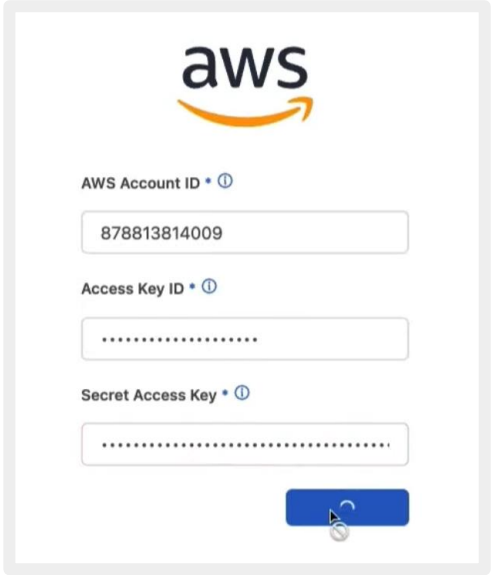
At least two hosts must have the unreserved CPU/Memory resources required for ESXi VM



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.



(*) Amazon EC2: Amazon Elastic Compute Cloud

Backup and Restore – Appliance, AWS VA, ESXi VA

Physical Appliance

vmware®

aws

Types of backup

- System and network automation ★
- System, network automation and assurance

Backups can be On-Demand or Scheduled

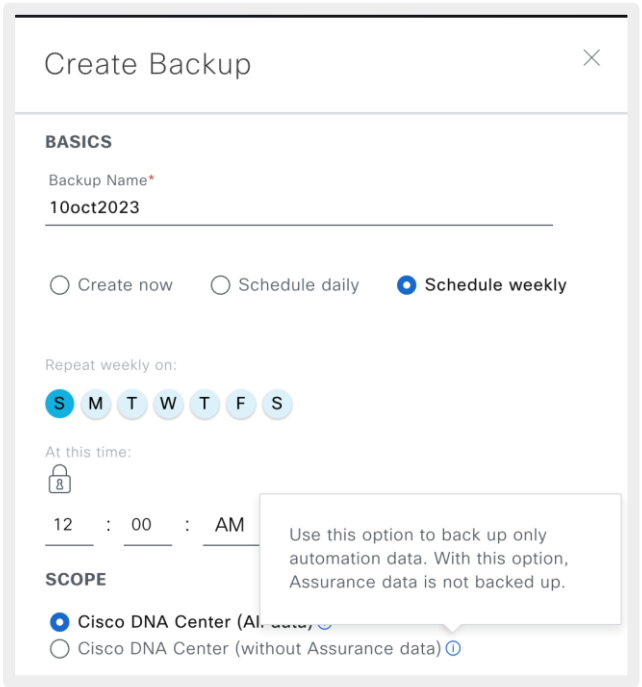
Backup and Restore – Appliance, AWS VA, ESXi VM

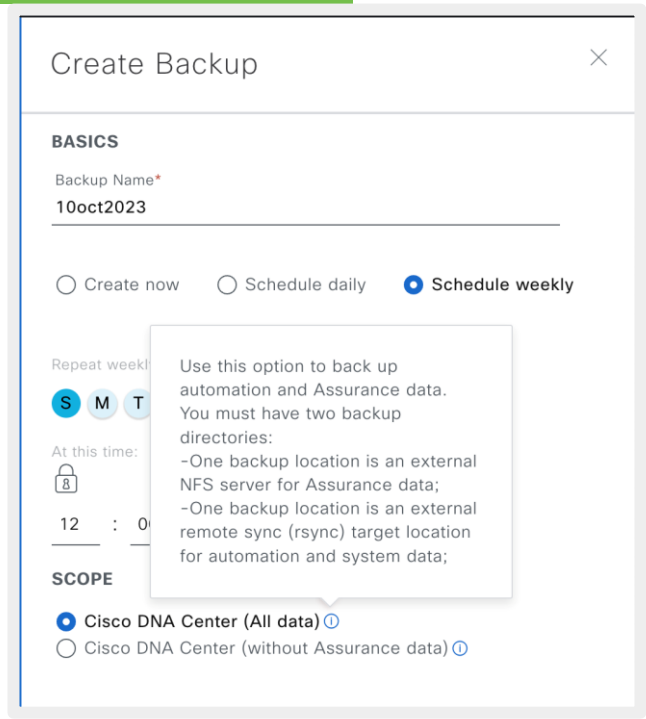
Physical Appliance

vmware®

aws

Types of backup





Backup and Restore – Appliance, AWS VA

Physical Appliance

aws

Backup Destinations

RSYNC for Automation Backup

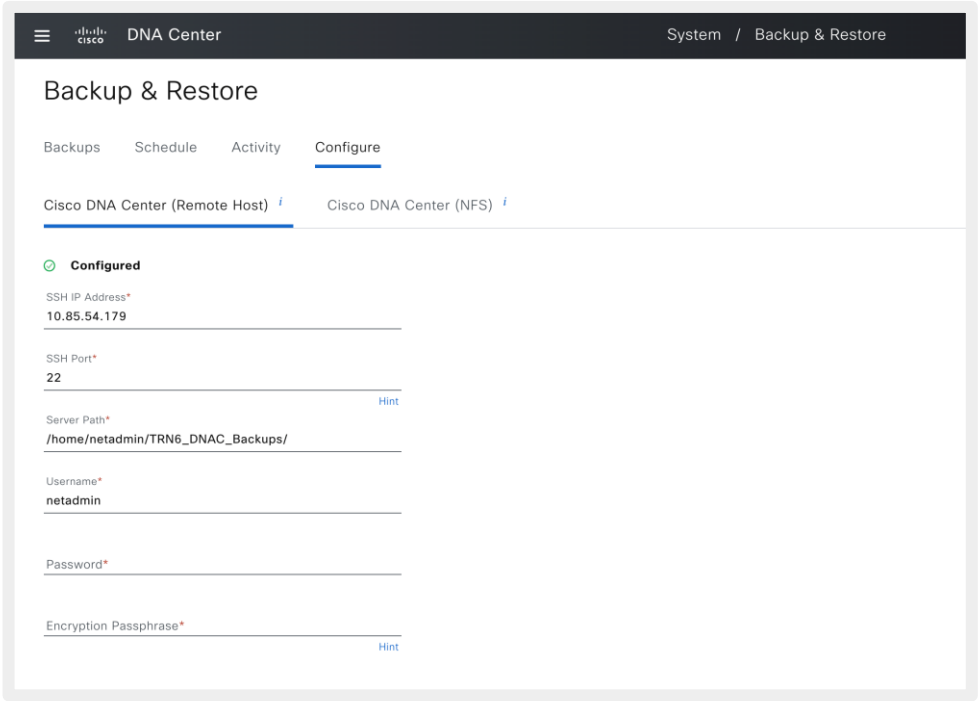
+

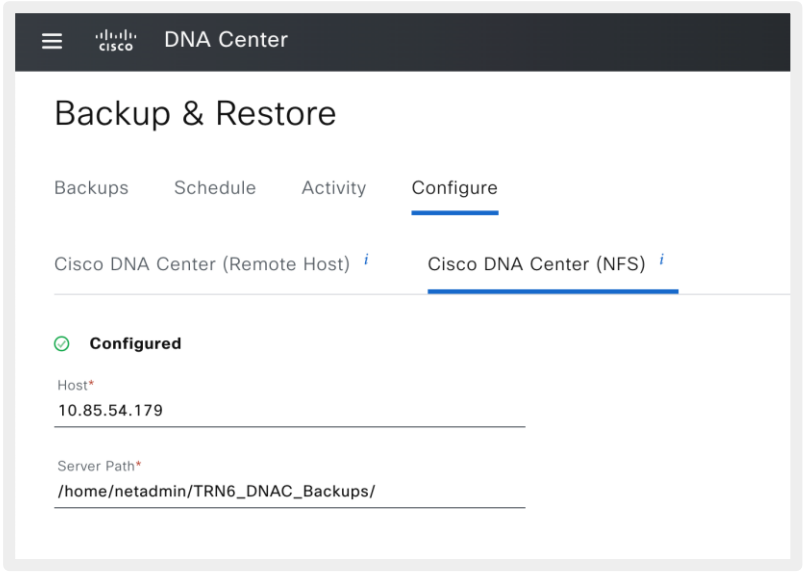
Linux-based NFS server for Assurance Backup

Backup and Restore – Appliance and AWS VA

Physical Appliance

aws





Backup and Restore - Appliance to AWS VA

Physical Appliance

aws

- 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

aws

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-launchapd-administrator-guide_1-7/m_backup_and_restore.html*

Backup and Restore – ESXi Virtual Appliance

Physical Appliance

vmware

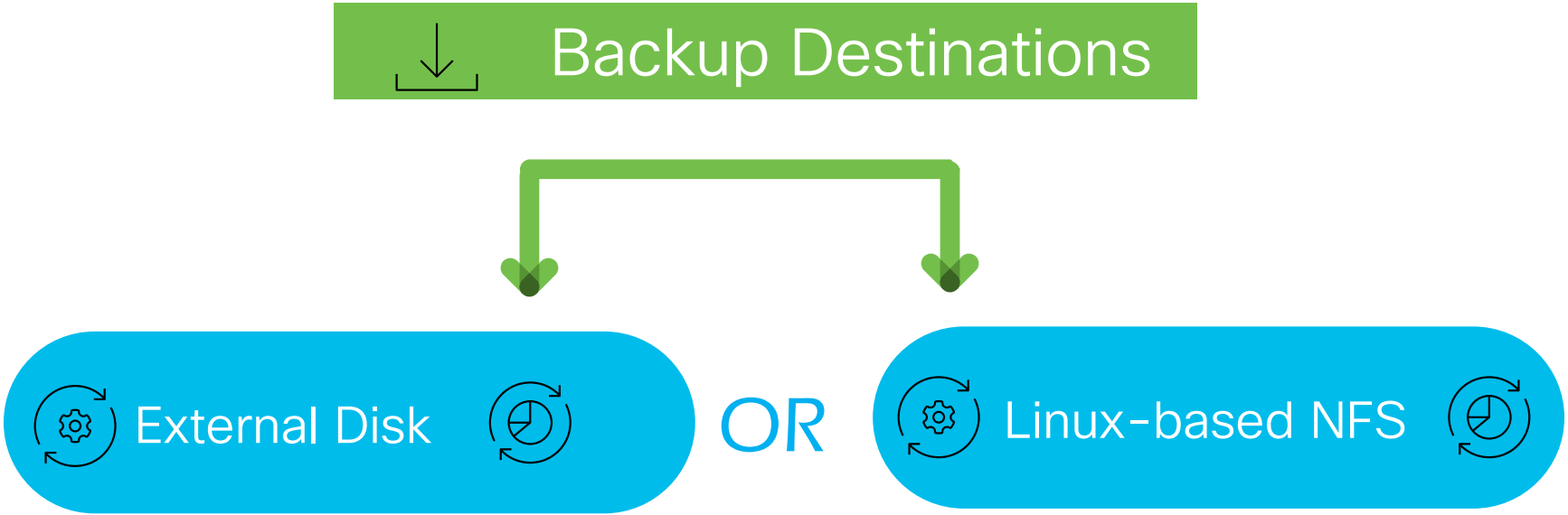
aws

Types of backup

- System and network automation ★
- System, network automation and assurance

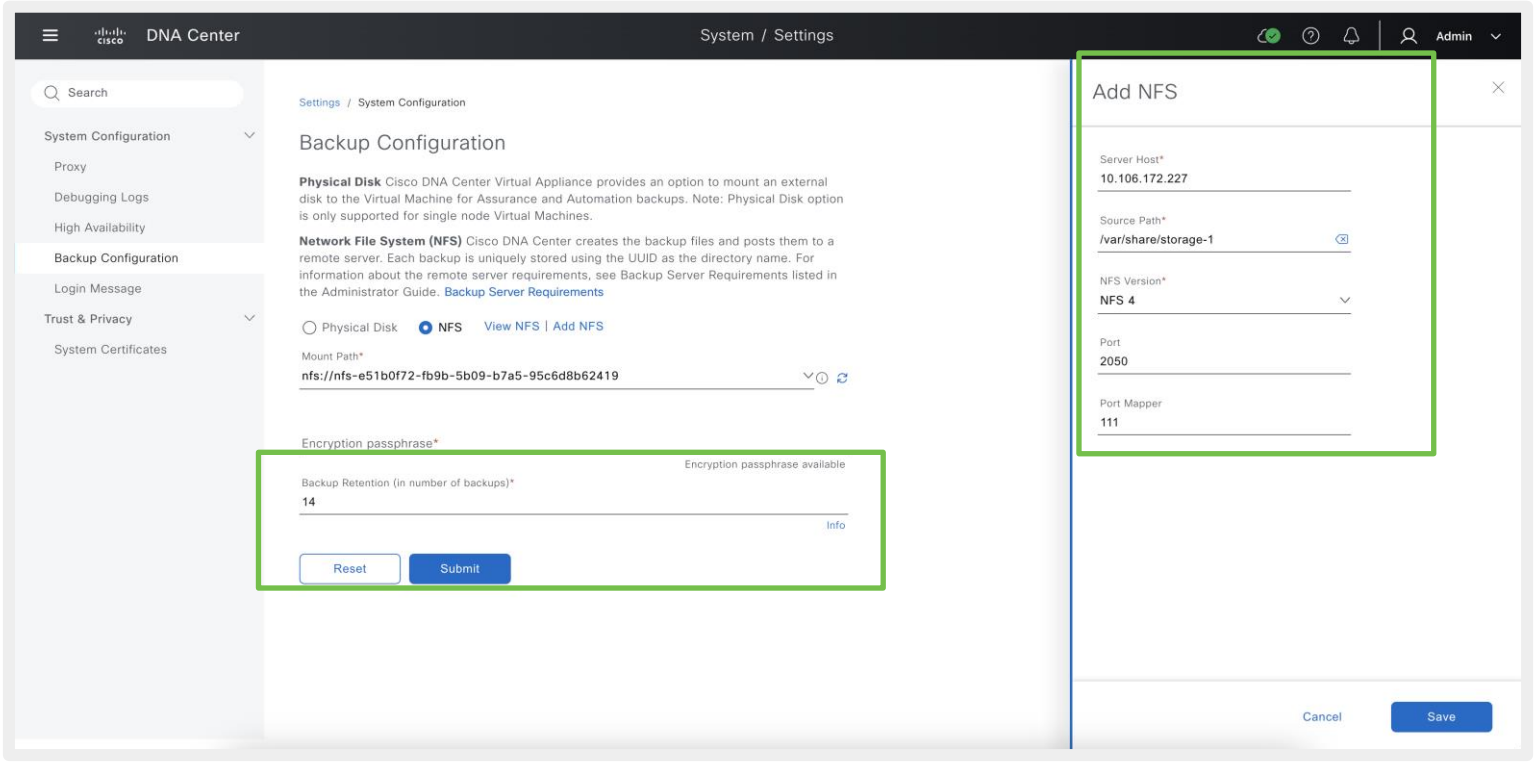
Backups can be On-Demand or Scheduled

Backup and Restore - ESXi Virtual Appliance



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

Backup and Restore – ESXi Virtual Appliance



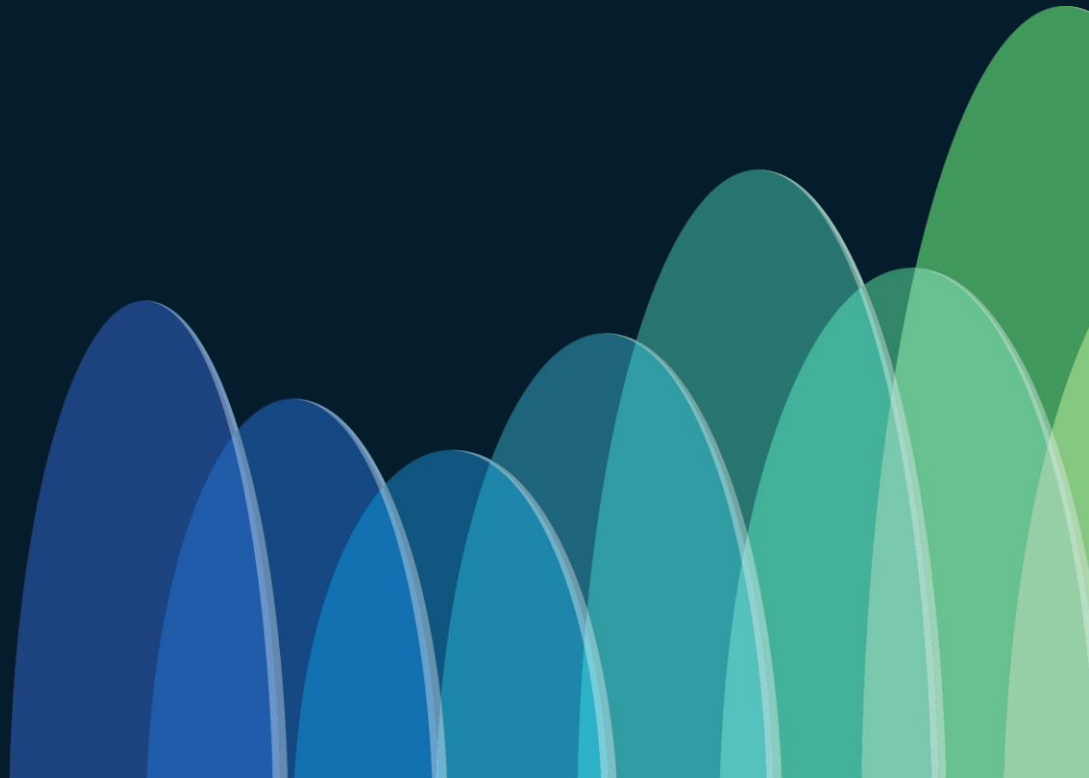
Backup Storage Recommendations

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

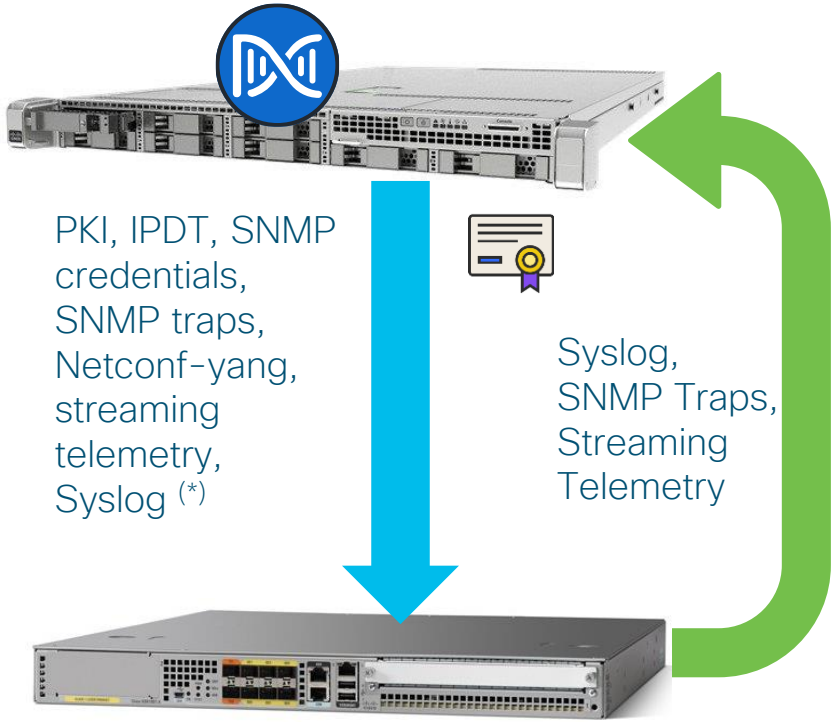
Recommendations for fully loaded appliance configurations with the maximum number of access points and network devices

Habit #2 – Find issues before your users with telemetry



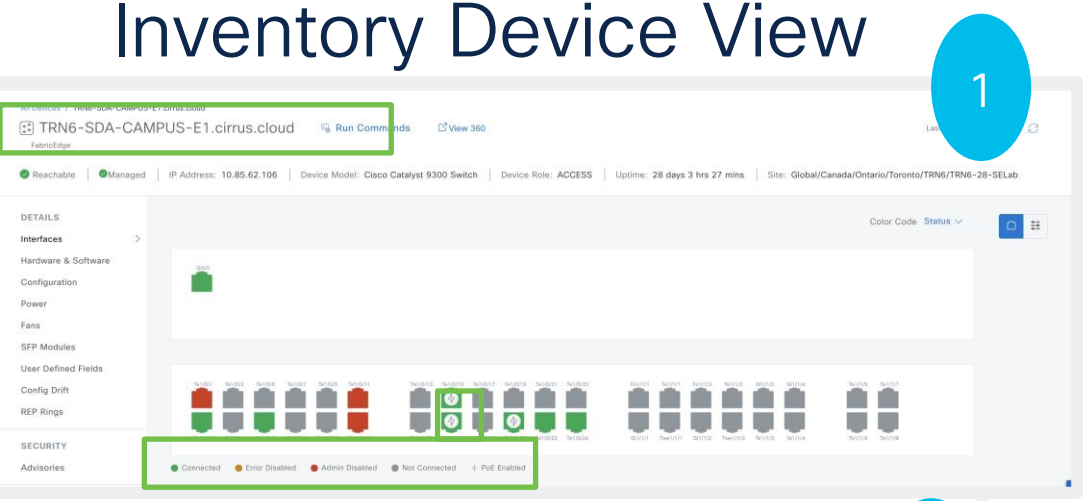
cisco Live!

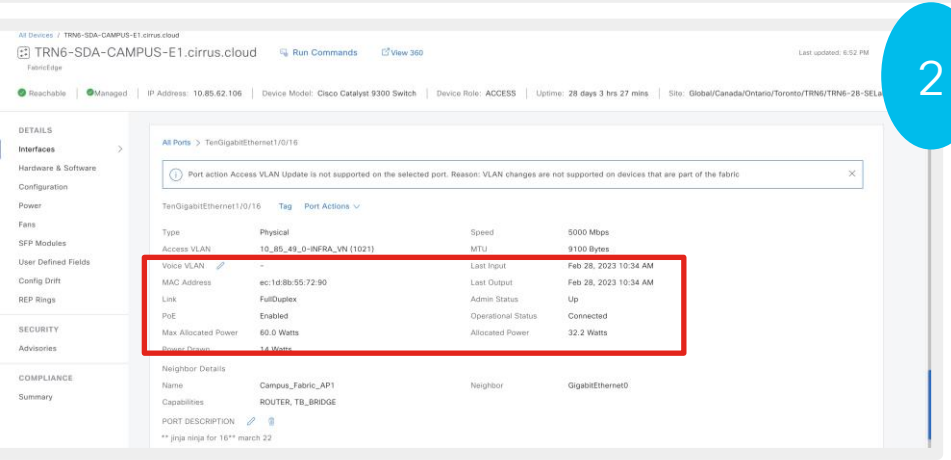
Benefits of Telemetry data captured via Catalyst Center

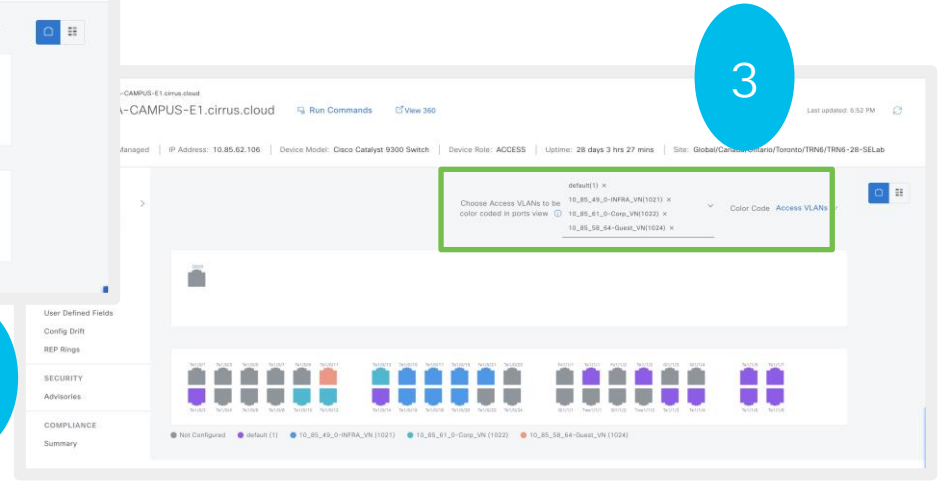


- Network and Client Health
- Application Health
- Network Services (AAA, DHCP, DNS)
- View and Manage Issues
- Visibility into Wi-Fi 6/6E Readiness
- Monitor Power over Ethernet
- EoX Insights
- Inventory Insights
- Network Trends and Insights

Inventory Device View

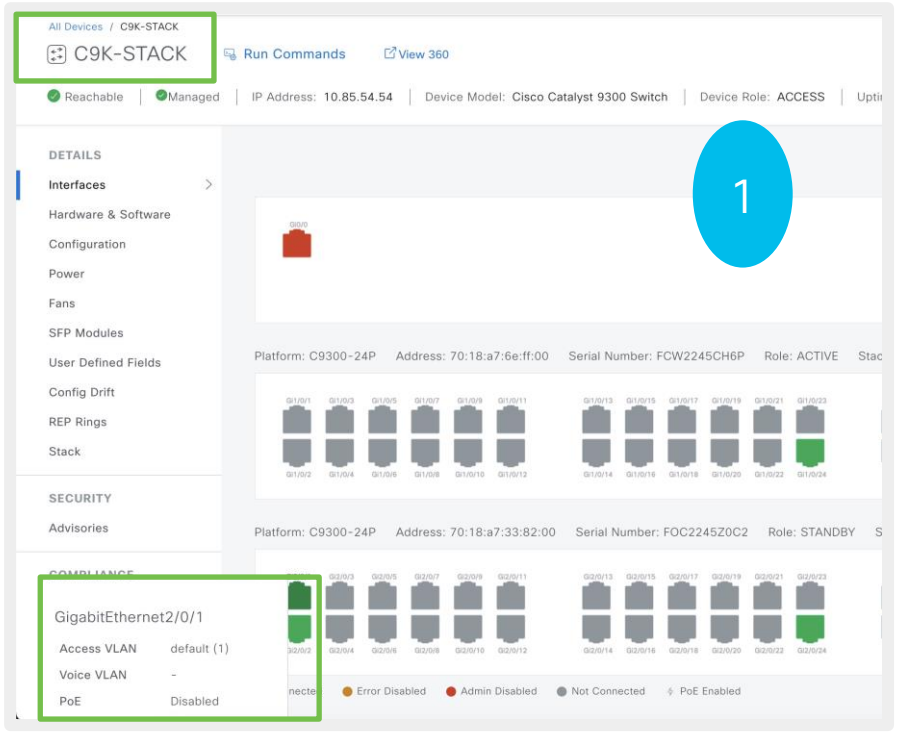


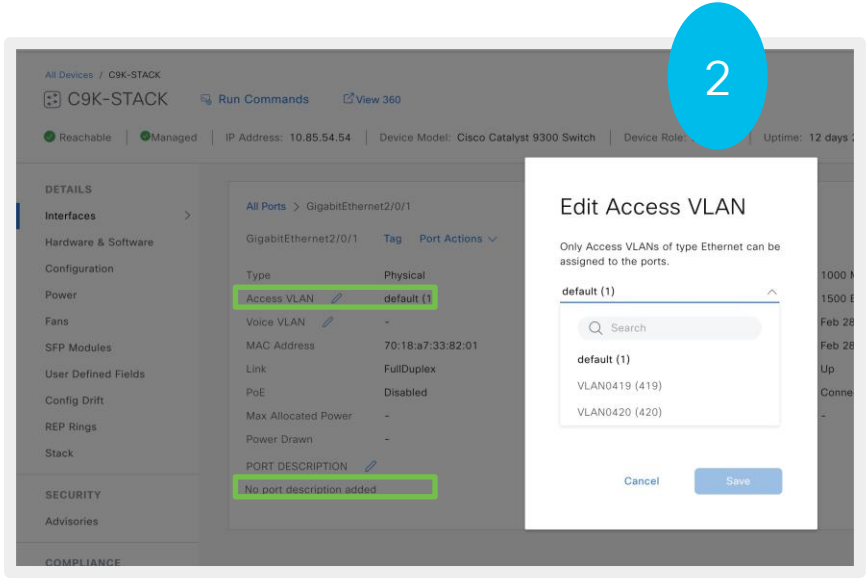




Detailed port information: port status, PoE, VLAN's, Last Input/Output

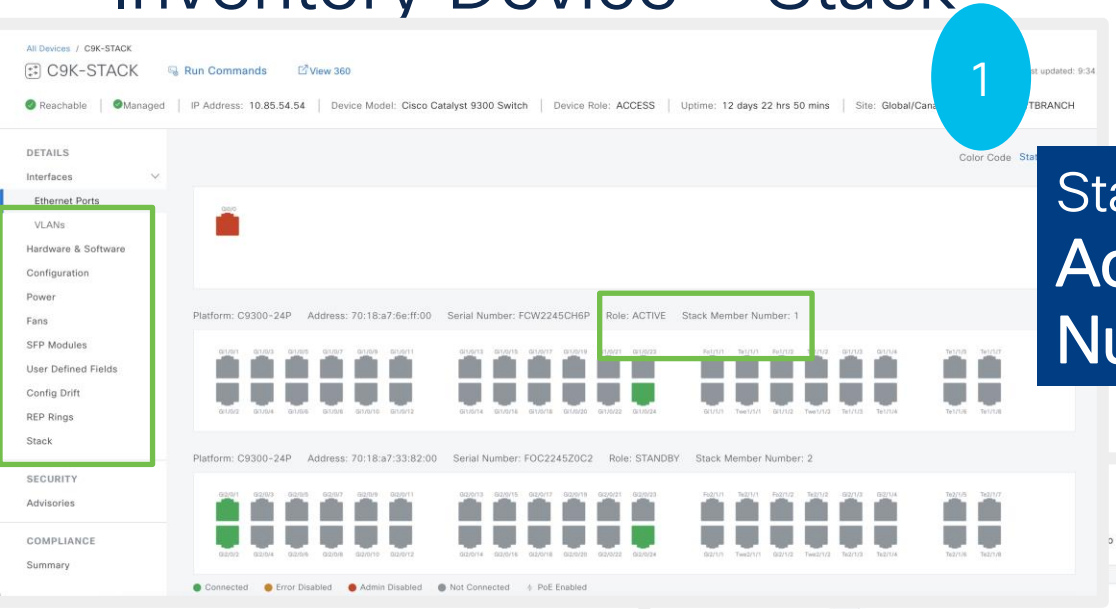
Inventory Device – Port Configuration and Actions





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

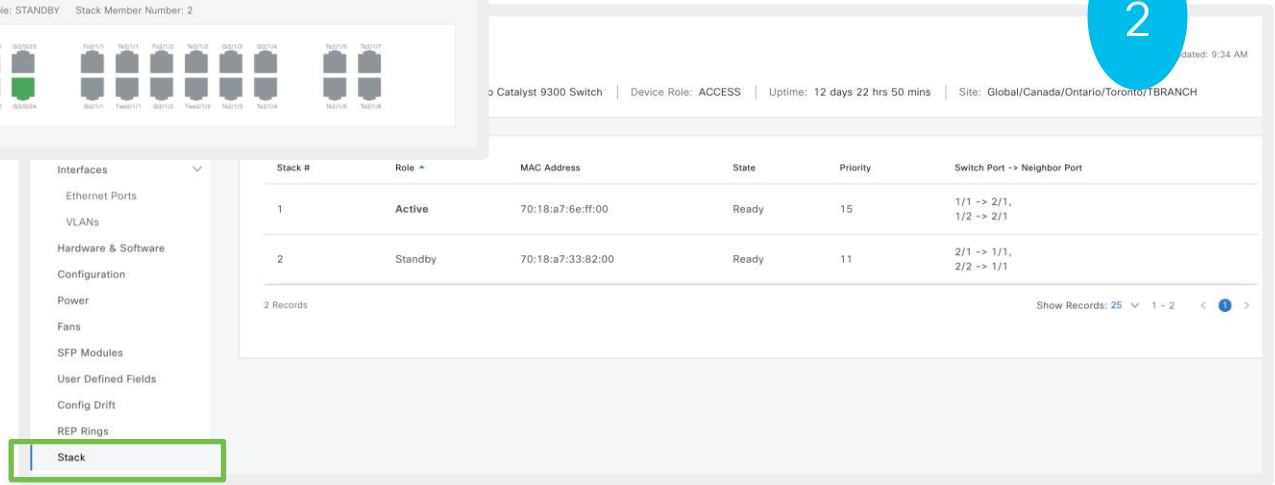
Inventory Device – Stack



1

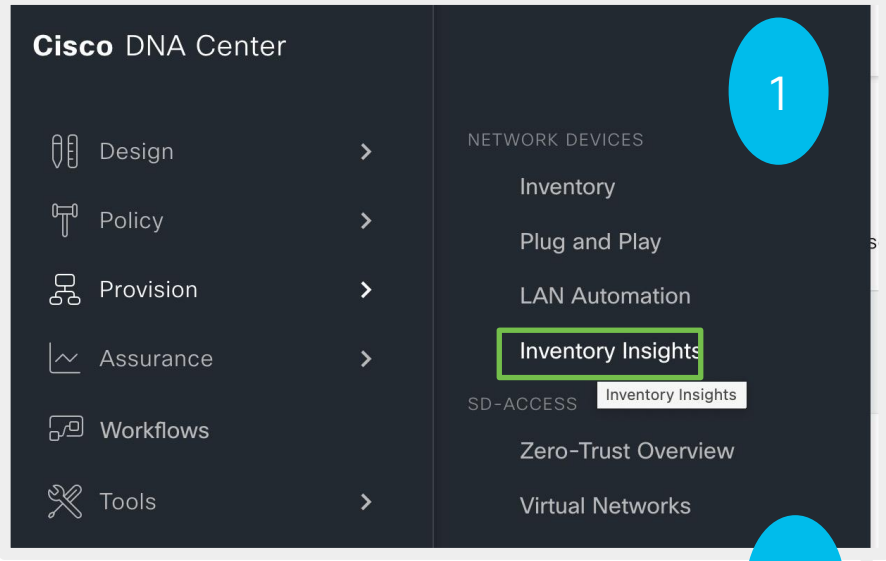
Stack View –
Active/Standby, Stack Number and **Stack View**

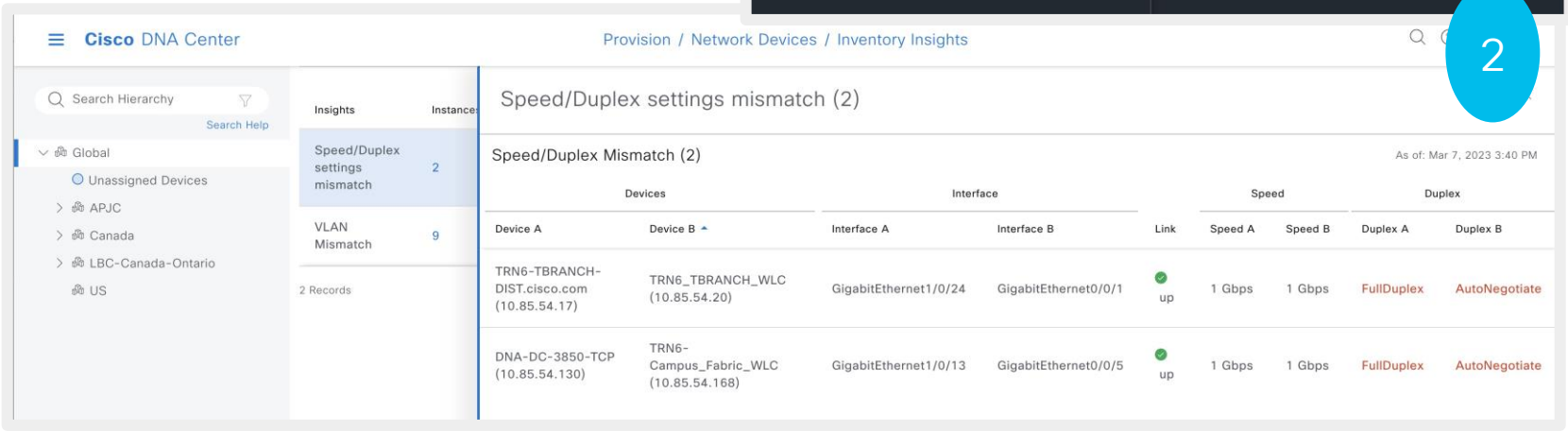
2



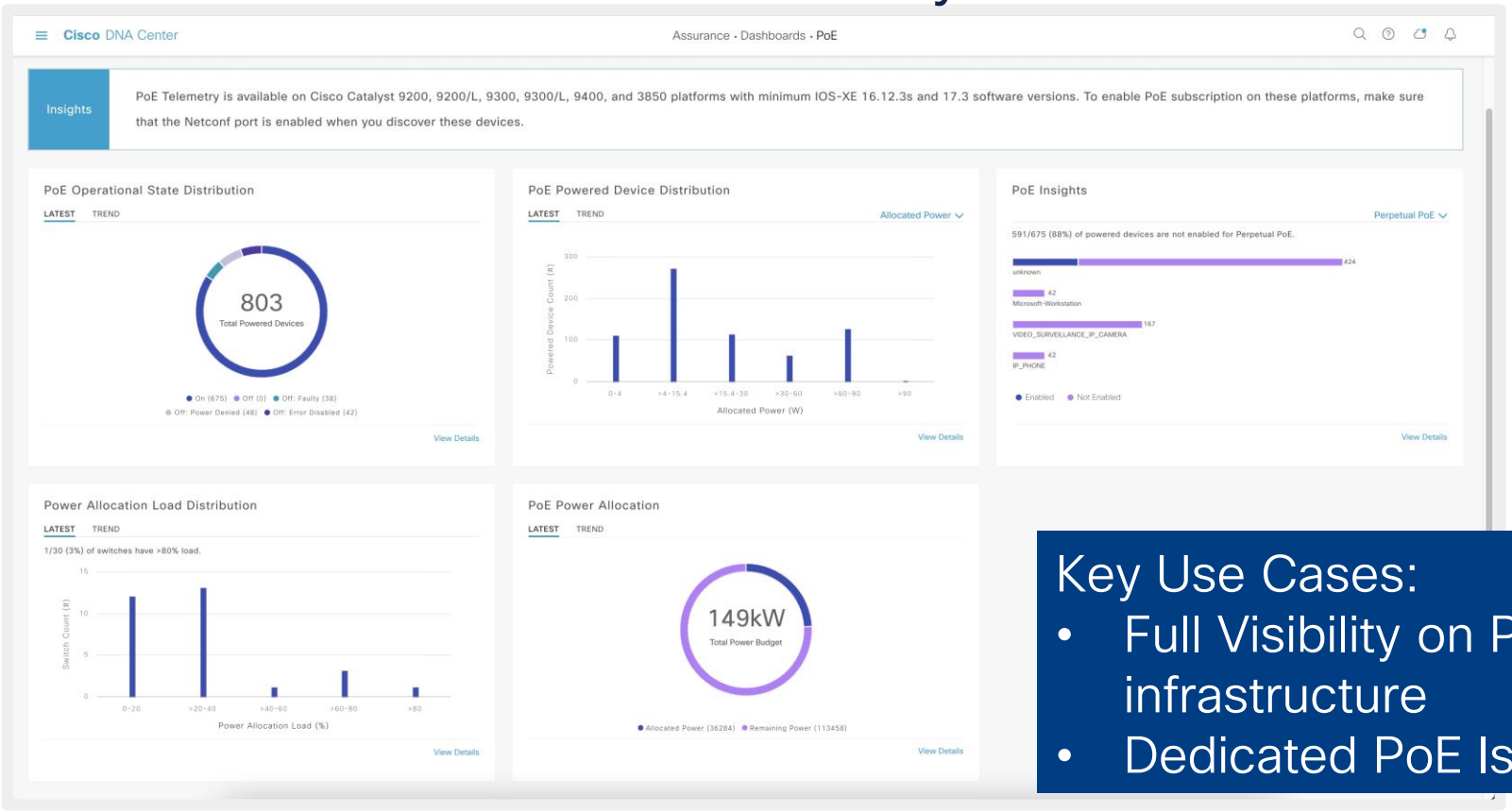
Inventory Insights

Find **configuration inconsistencies** and **misconfigurations**





Power over Ethernet Analytics

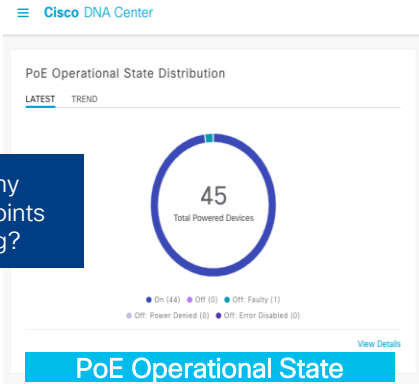


Key Use Cases:

- Full Visibility on PoE infrastructure
- Dedicated PoE Issue Types

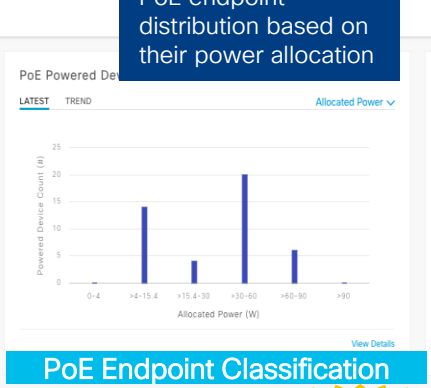
Power over Ethernet Analytics

How are my PoE endpoints functioning?



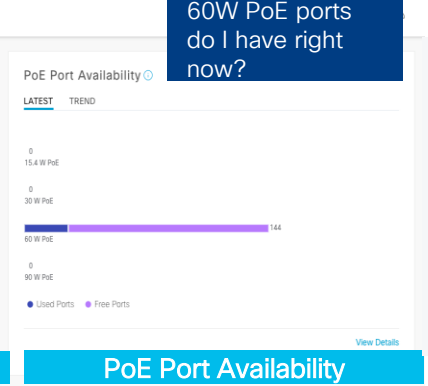
PoE Operational State

PoE endpoint distribution based on their power allocation

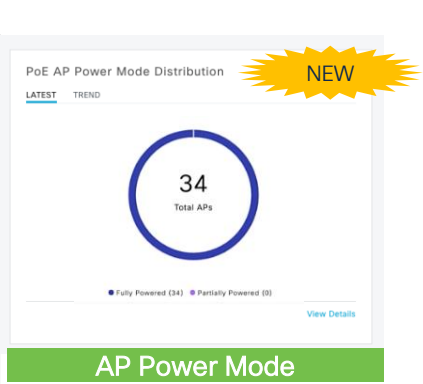


PoE Endpoint Classification

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



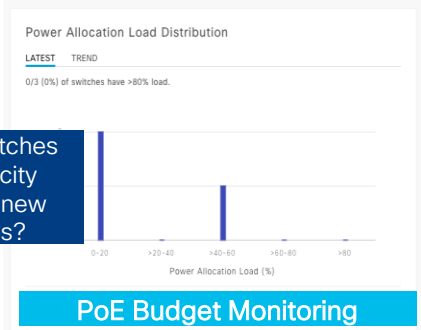
PoE Port Availability



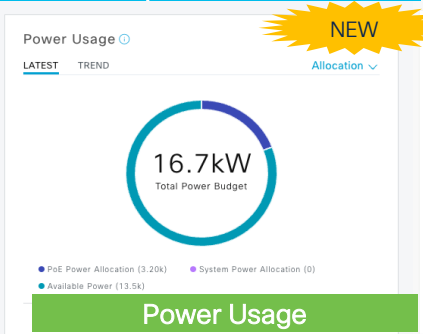
AP Power Mode

Are my AP's fully or partially powered?

Which switches have capacity to add 10 new IP Cameras?

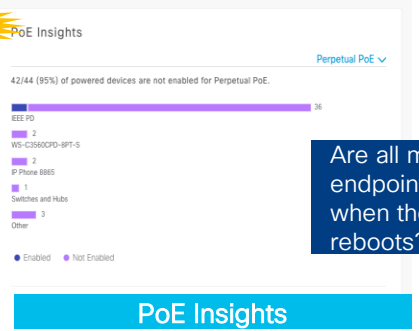


PoE Budget Monitoring



Power Usage

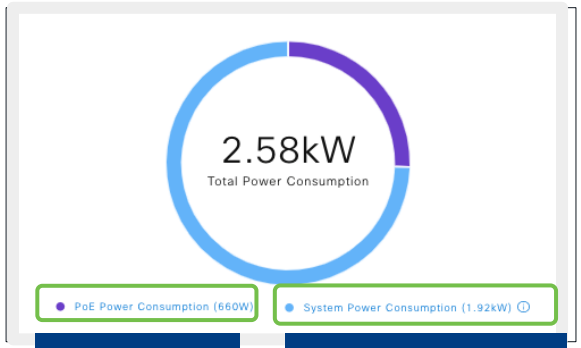
What is the real time power consumption of my access network



PoE Insights

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

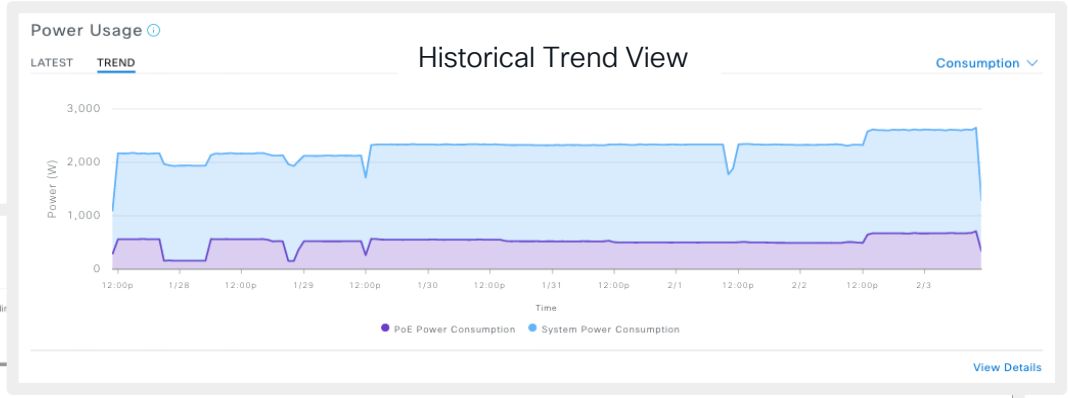
Realtime Power Consumption Reporting



Realtime PoE consumption

Realtime Sys Power consumption

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

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

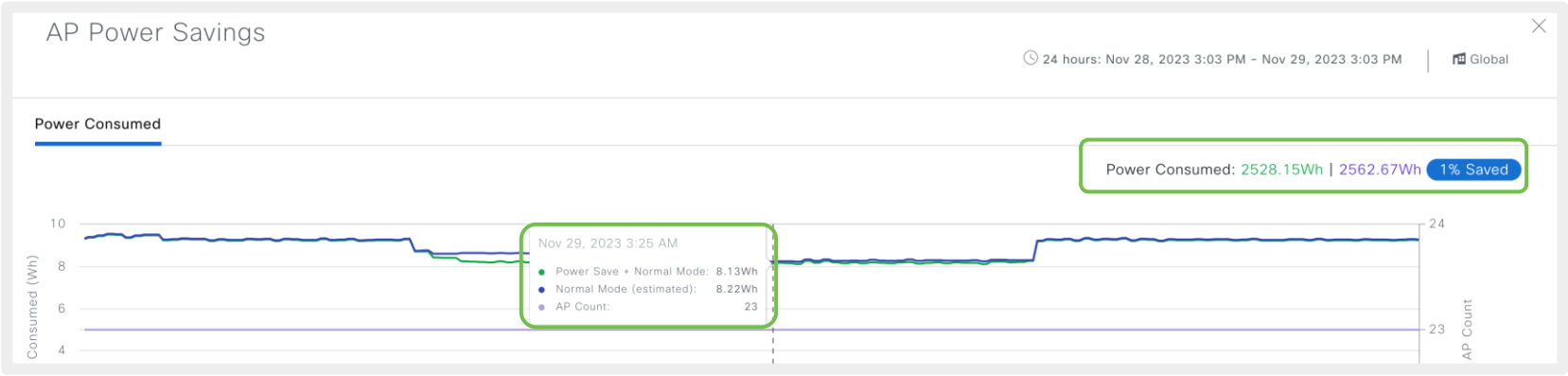


Instantaneous System Power + PoE Consumption

Catalyst 9200, 9300 and 9400 starting IOS-XE 17.14.1

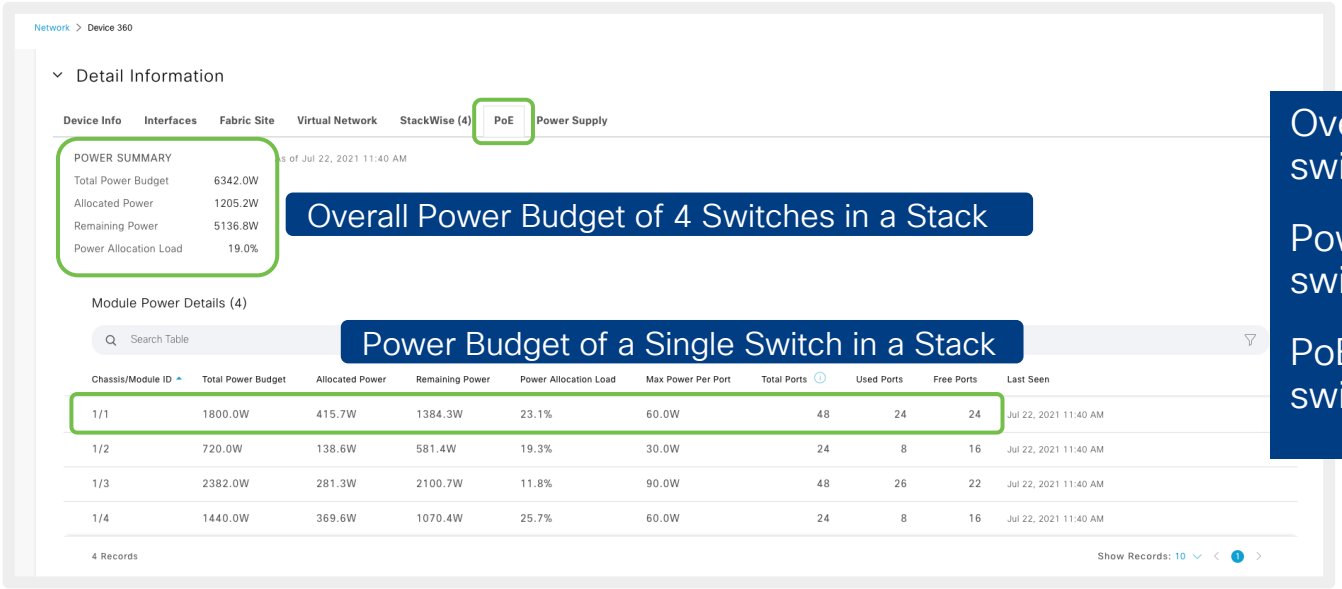
Power over Ethernet Analytics

AP Power Save Mode Distribution & AP Savings on 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

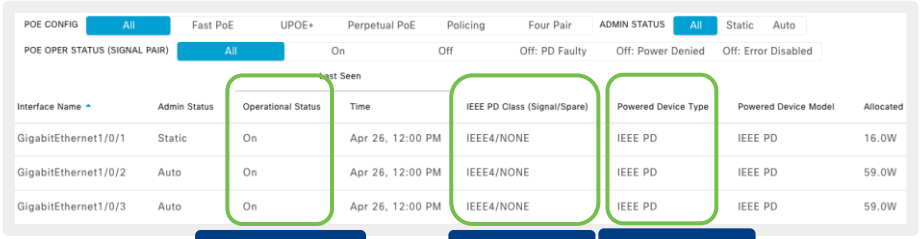
Stack PoE Insights in Device 360

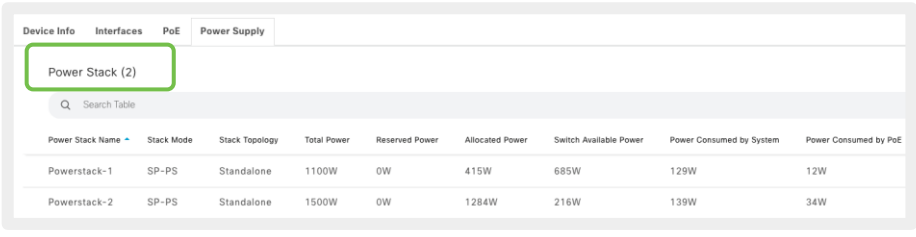


Overall Power Budget switches in a stack

Power Budget for each switch

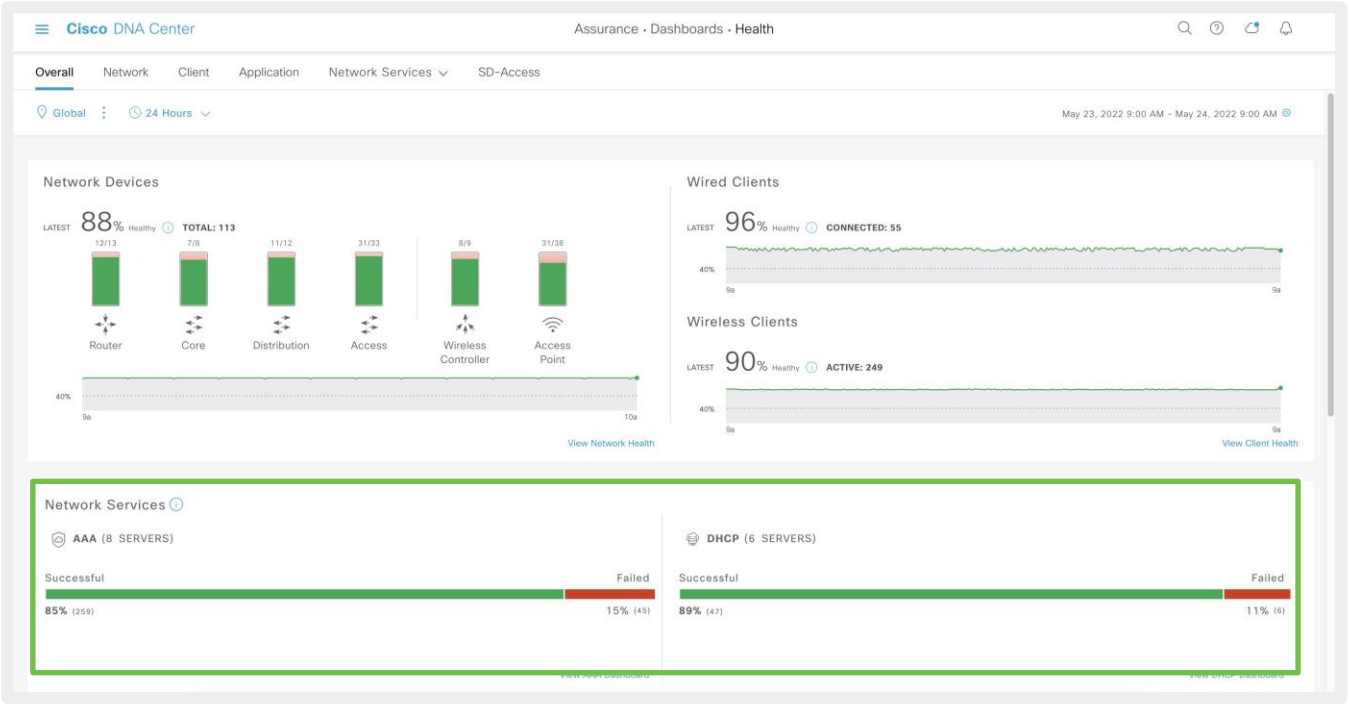
PoE interfaces for each switch with detailed PoE info



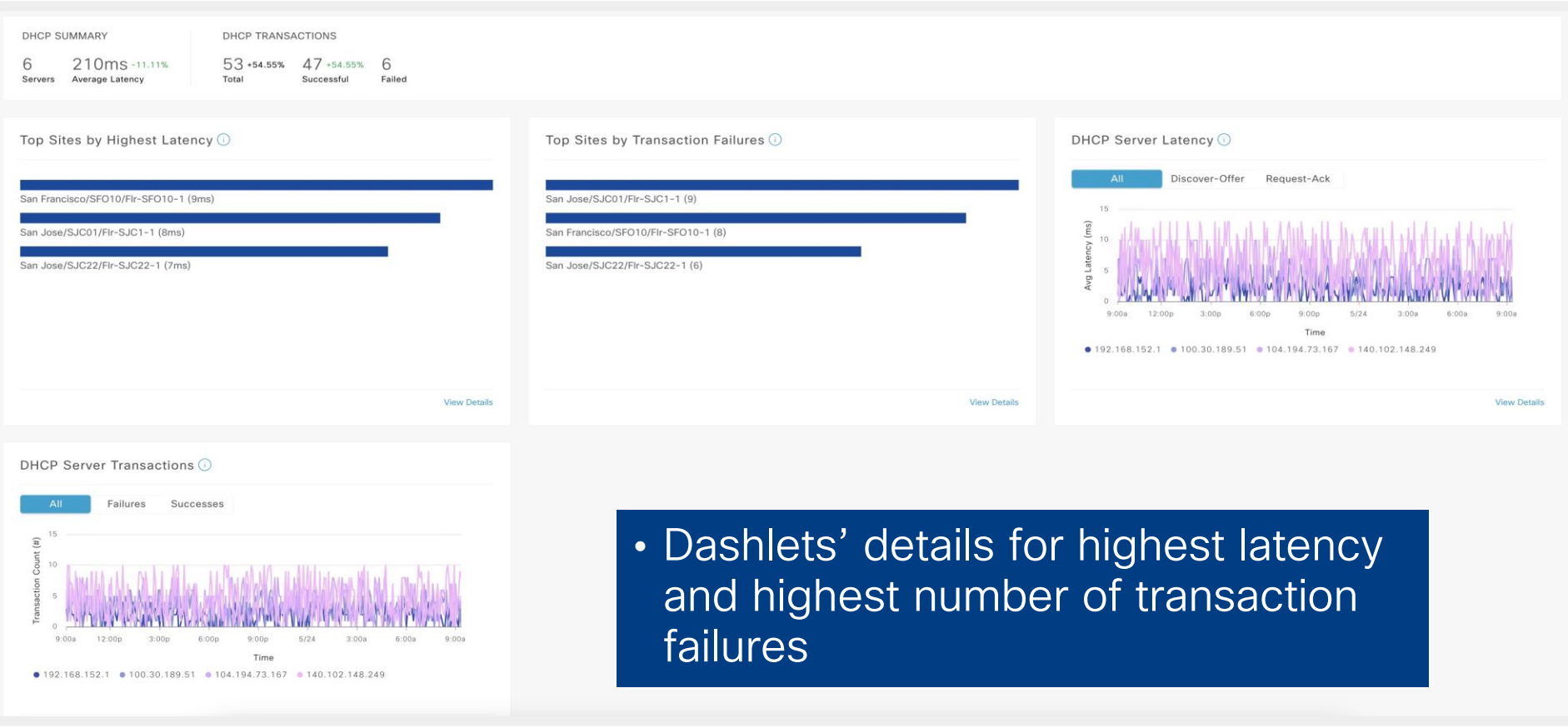


Network Services Analytics – AAA/DHCP

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



Network Services Analytics – AAA/DHCP



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

Tracked by Network Services Analytics – AAA/DHCP

Reference

AAA

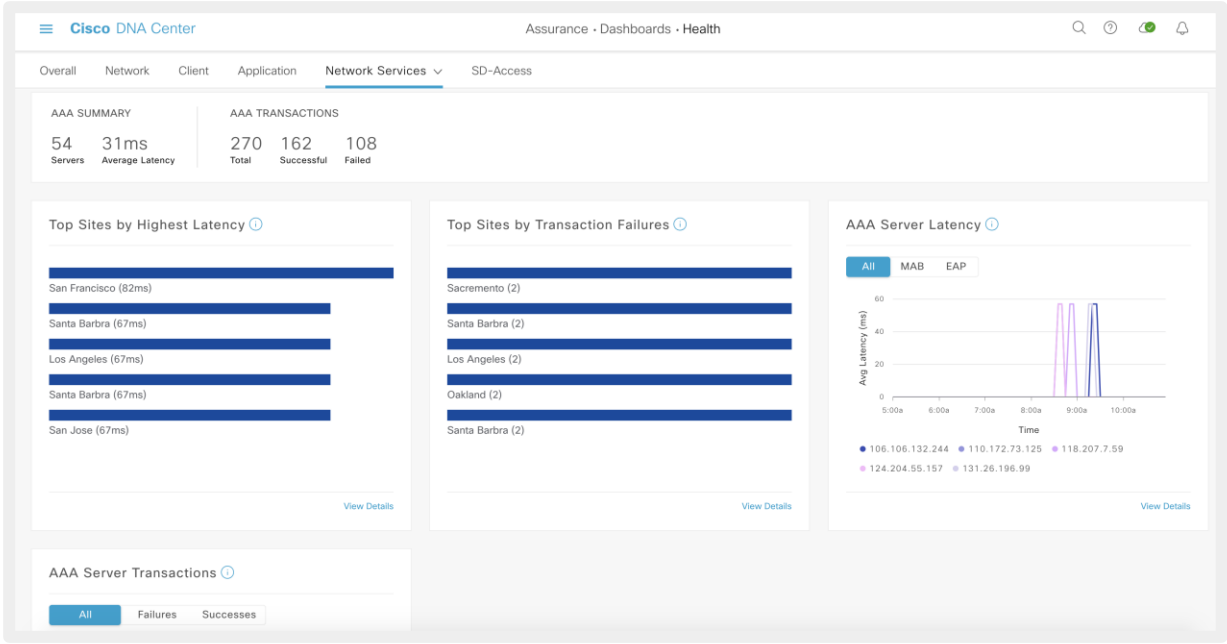
- AAA Servers
- AAA Server Latency
- AAA Server Transactions
- AAA Transaction Failures %
- Top Sites by Transaction Failures
- Top Sites by Highest Latency
- AAA Servers by WLC

DHCP

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

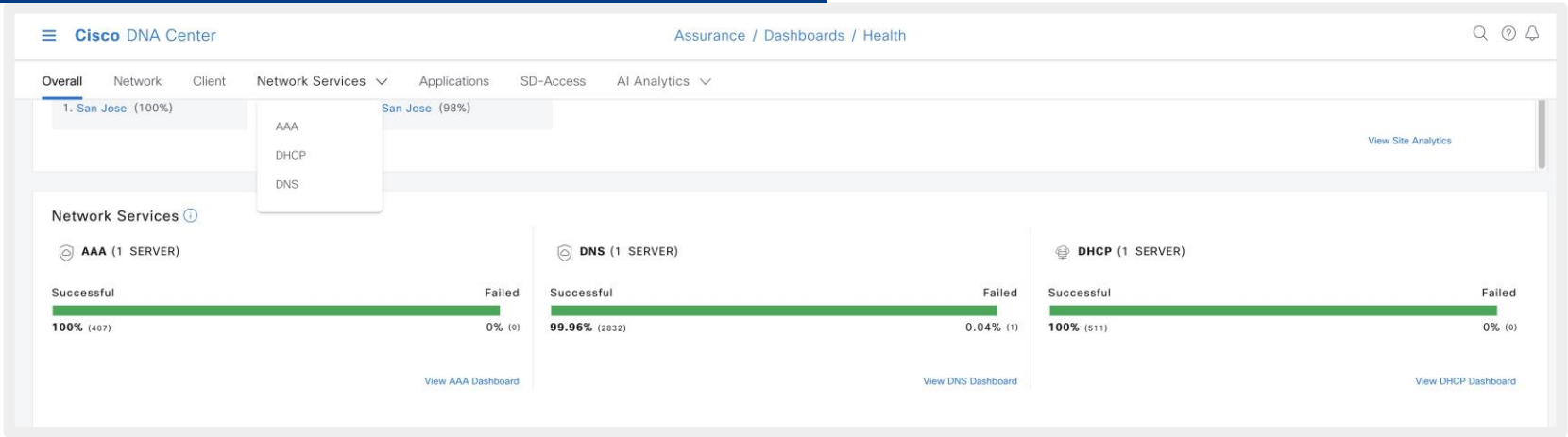
Network Services Analytics – AAA/DHCP

- 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



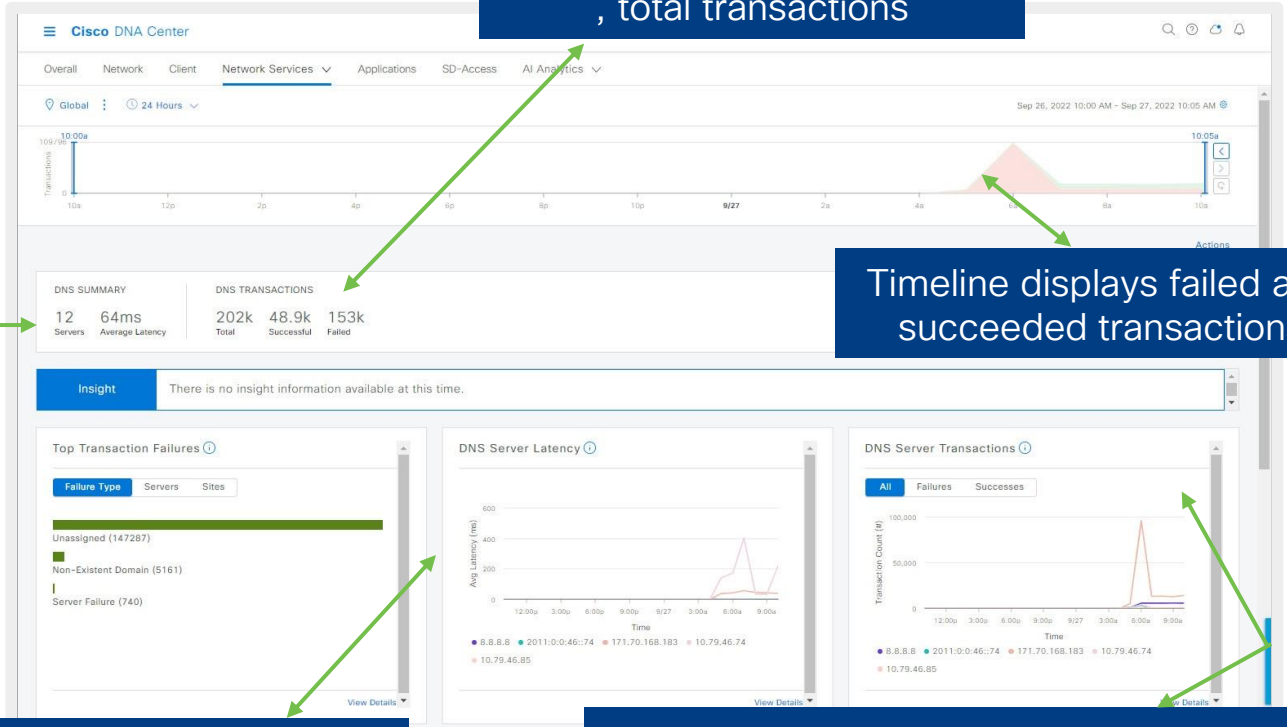
Network Services – DNS

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



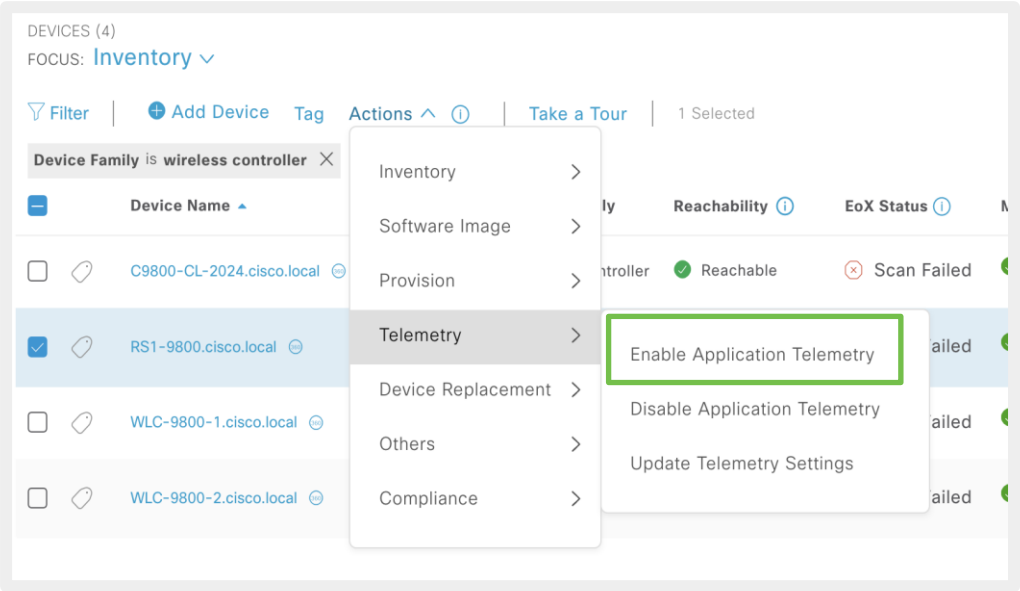
Timeline displays failed and succeeded transactions

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

C9300-24P
IOS-XE: 17.11.01

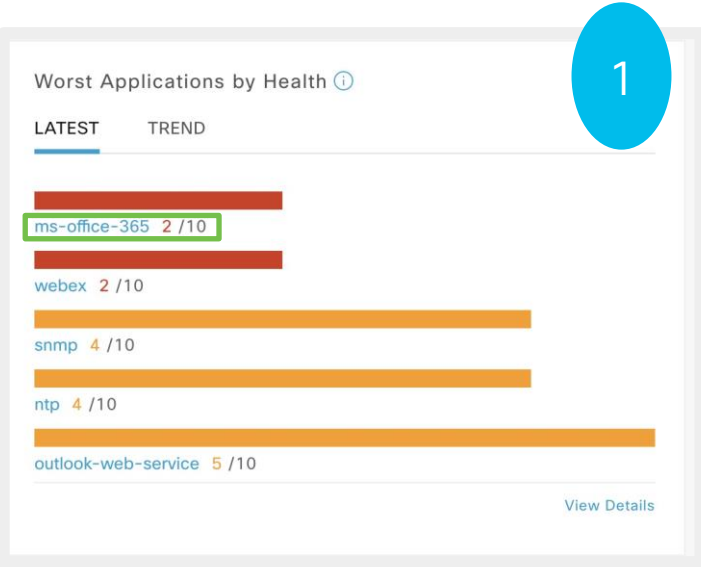
Cisco DNA Center
Version 2.3.5.3-70194

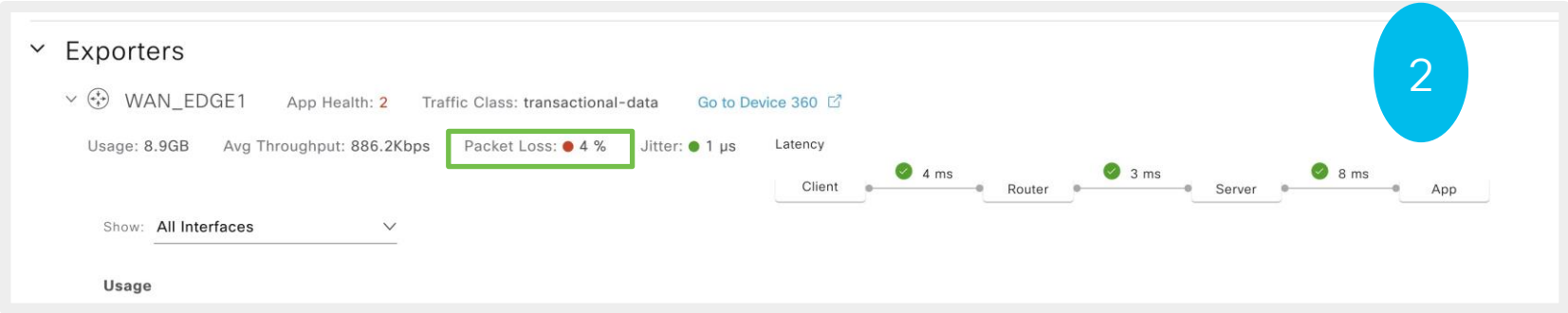
```
flow record dnacrecord_dns
 match ipv4 version
 match ipv4 protocol
 match connection client ipv4 address
 match connection server ipv4 address
 match flow observation point
 match application dns qtype
 match application dns rcode
 collect datalink mac source address input
 collect timestamp absolute 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 lor
 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
```

Application Visibility

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





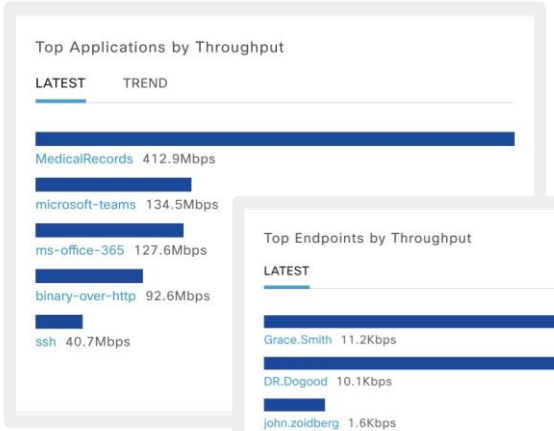
Application Visibility vs Application Experience

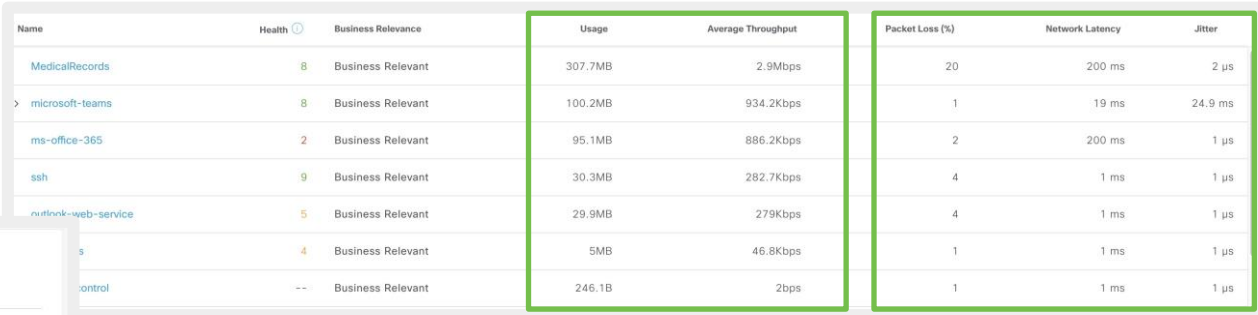
How Much = quantitative (usage)

- 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(*)

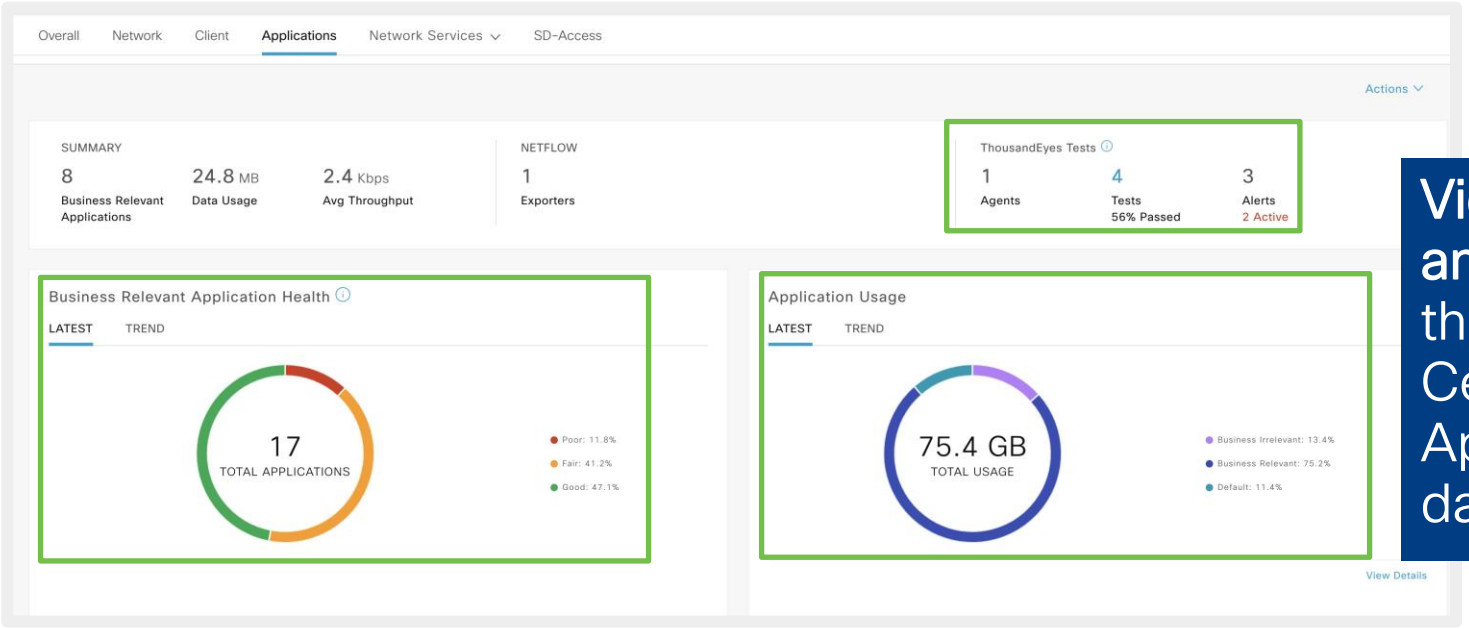




Name	Health	Business Relevance	Usage	Average Throughput	Packet Loss (%)	Network Latency	Jitter
MedicalRecords	8	Business Relevant	307.7MB	2.9Mbps	20	200 ms	2 µs
microsoft-teams	8	Business Relevant	100.2MB	934.2Kbps	1	19 ms	24.9 ms
ms-office-365	2	Business Relevant	95.1MB	886.2Kbps	2	200 ms	1 µs
ssh	9	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

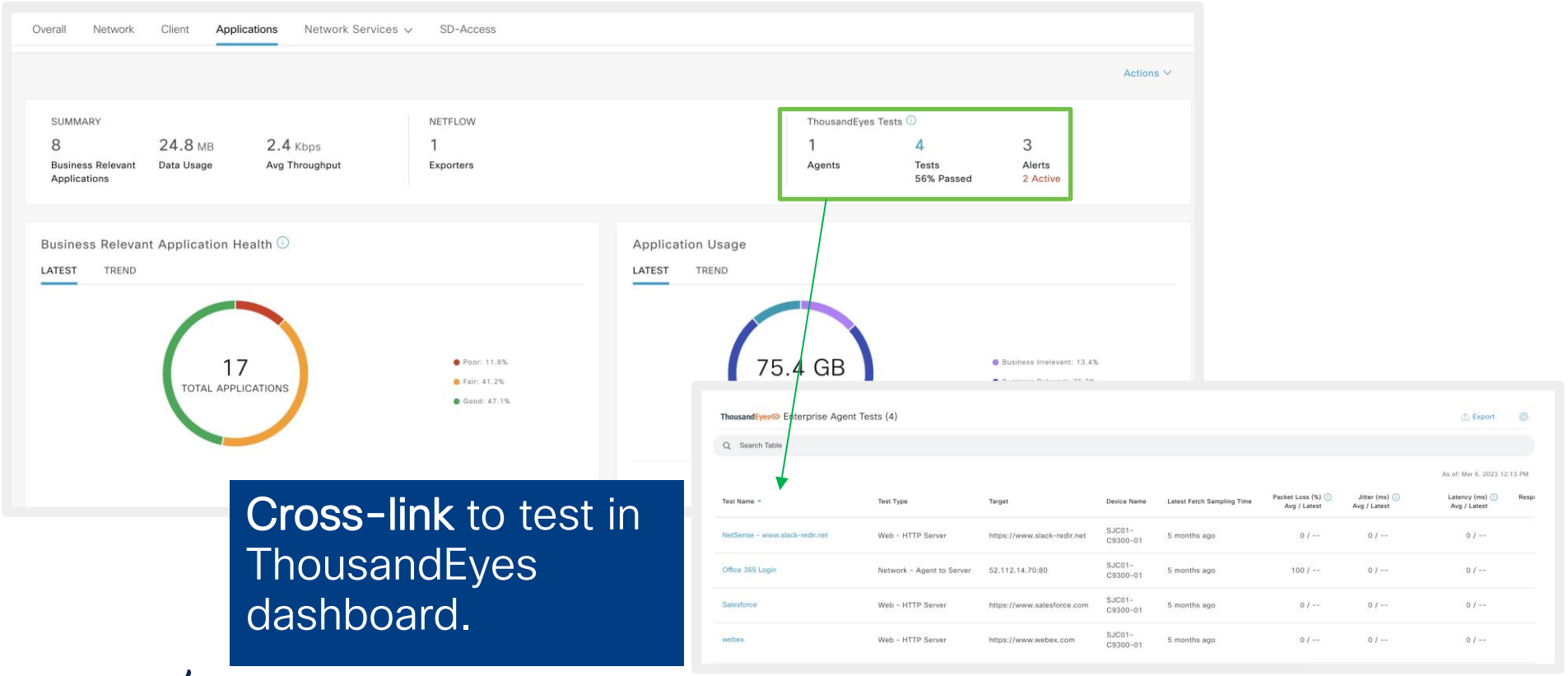
(*) New with Catalyst Center 2.3.5 and IOS-XE 17.10.1 or later with C91xx AP's

Application Health Dashboard: ThousandEyes Integration



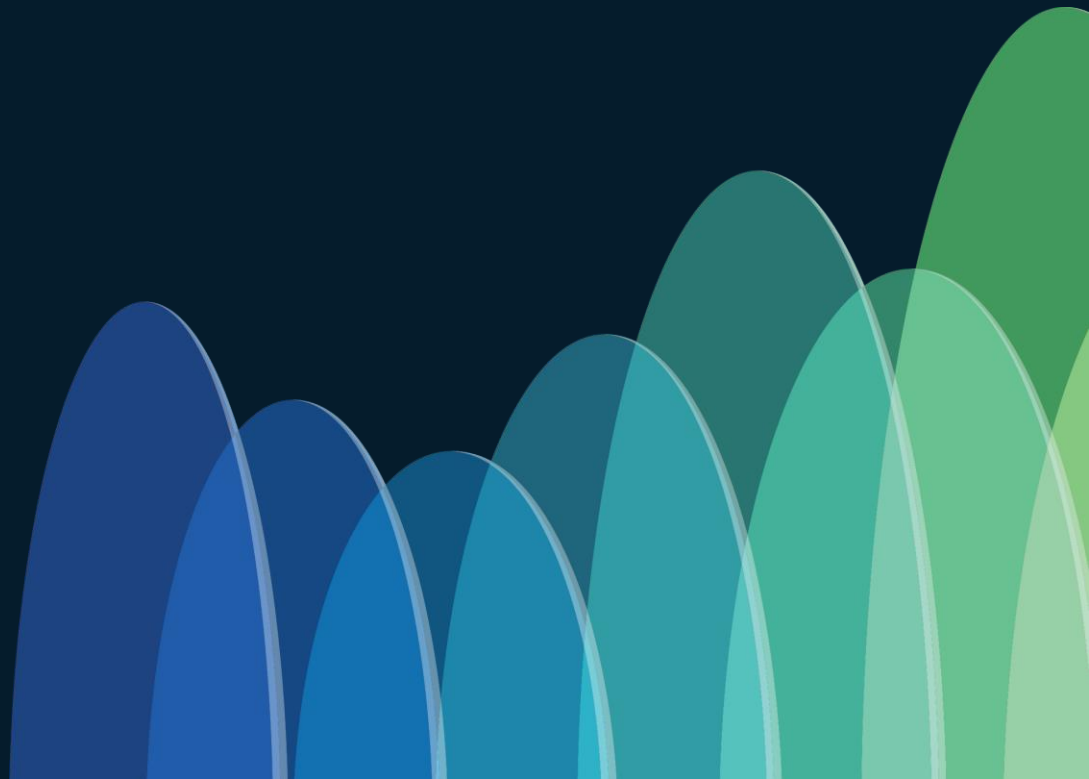
View agent, test, and alert data on the Catalyst Center Application dashboard

Application Health Dashboard: ThousandEyes Integration



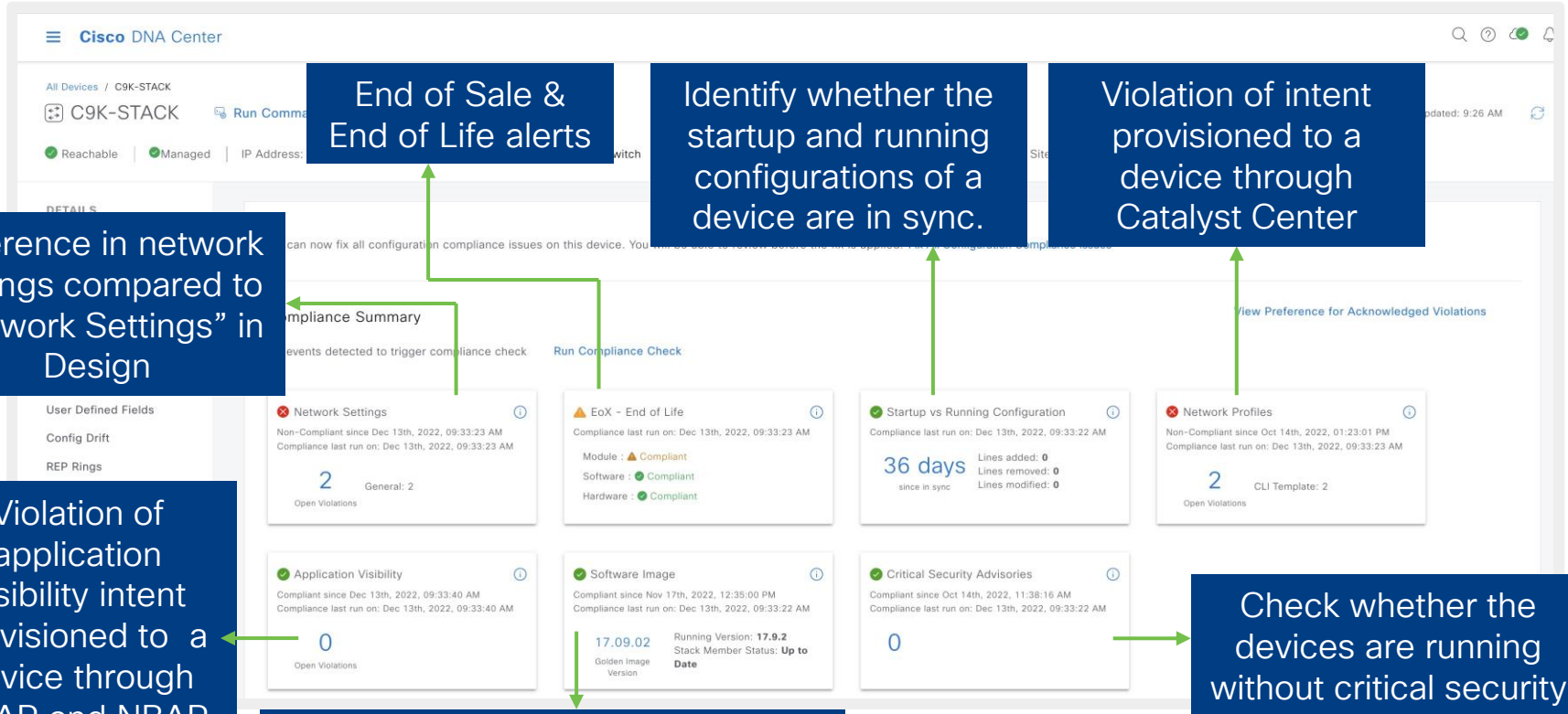
Cross-link to test in ThousandEyes dashboard.

Habit #3 - Leverage Compliance and Configuration management



cisco Live!

Cisco Catalyst Center Compliance Landscape



End of Sale & End of Life alerts

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

Violation of intent provisioned to a device through Catalyst Center

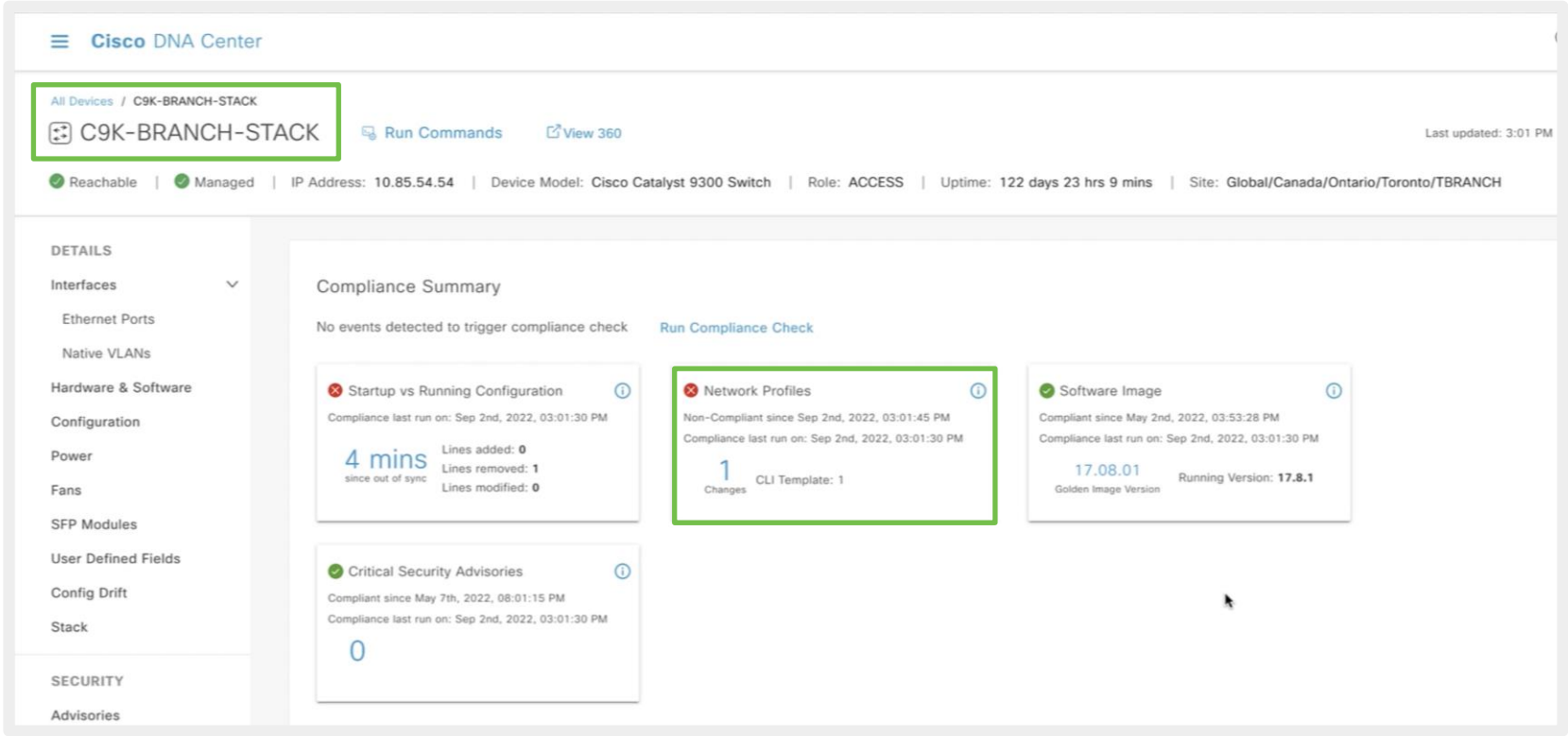
Difference in network settings compared to "Network Settings" in Design

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

Check whether the devices are running without critical security vulnerabilities.

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

Compliance: Network Profiles – Switches



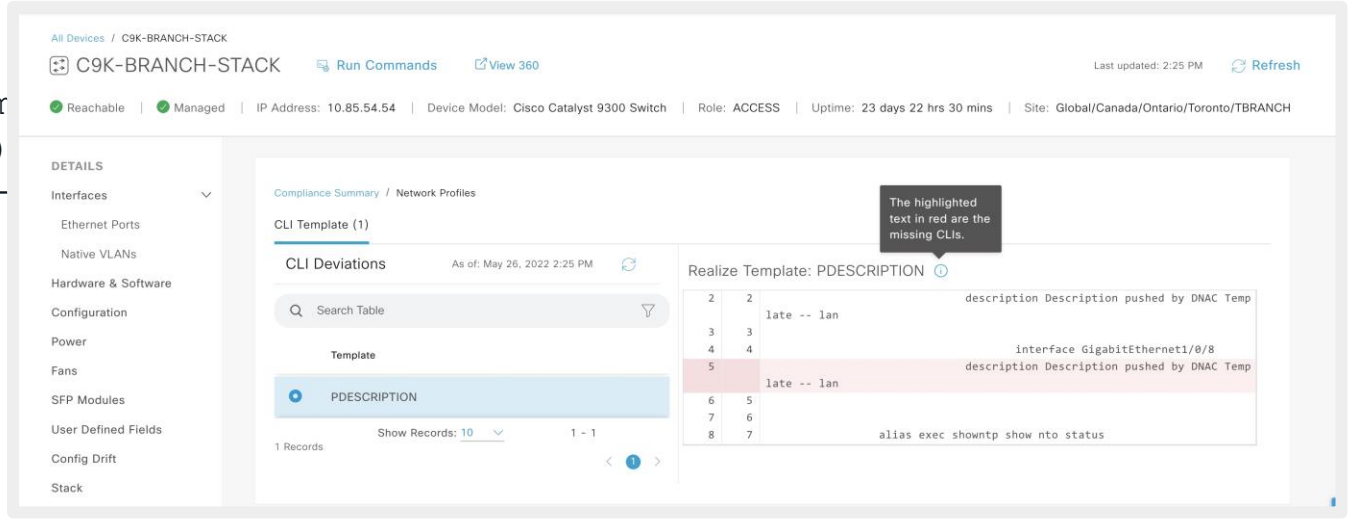
Compliance: Network Profiles – Switches

Config pushed by Catalyst Center via templates:

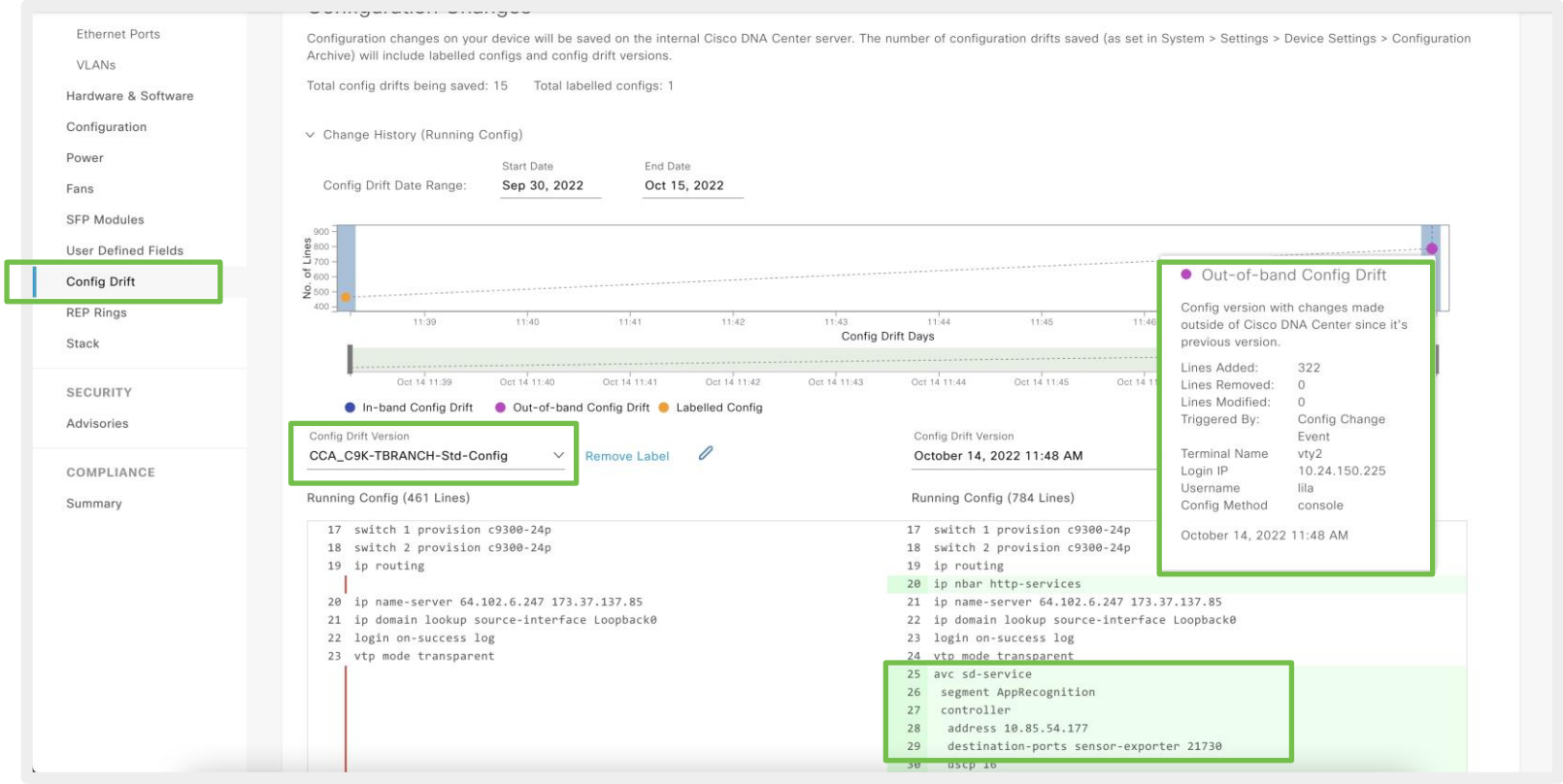
```
interface GigabitEthernet1/0/7
 description Description pushed by DNAC Template -- lan
!
interface GigabitEthernet1/0/8
 description Description pushed by DNAC Template -- lan
```

Out of band changes:

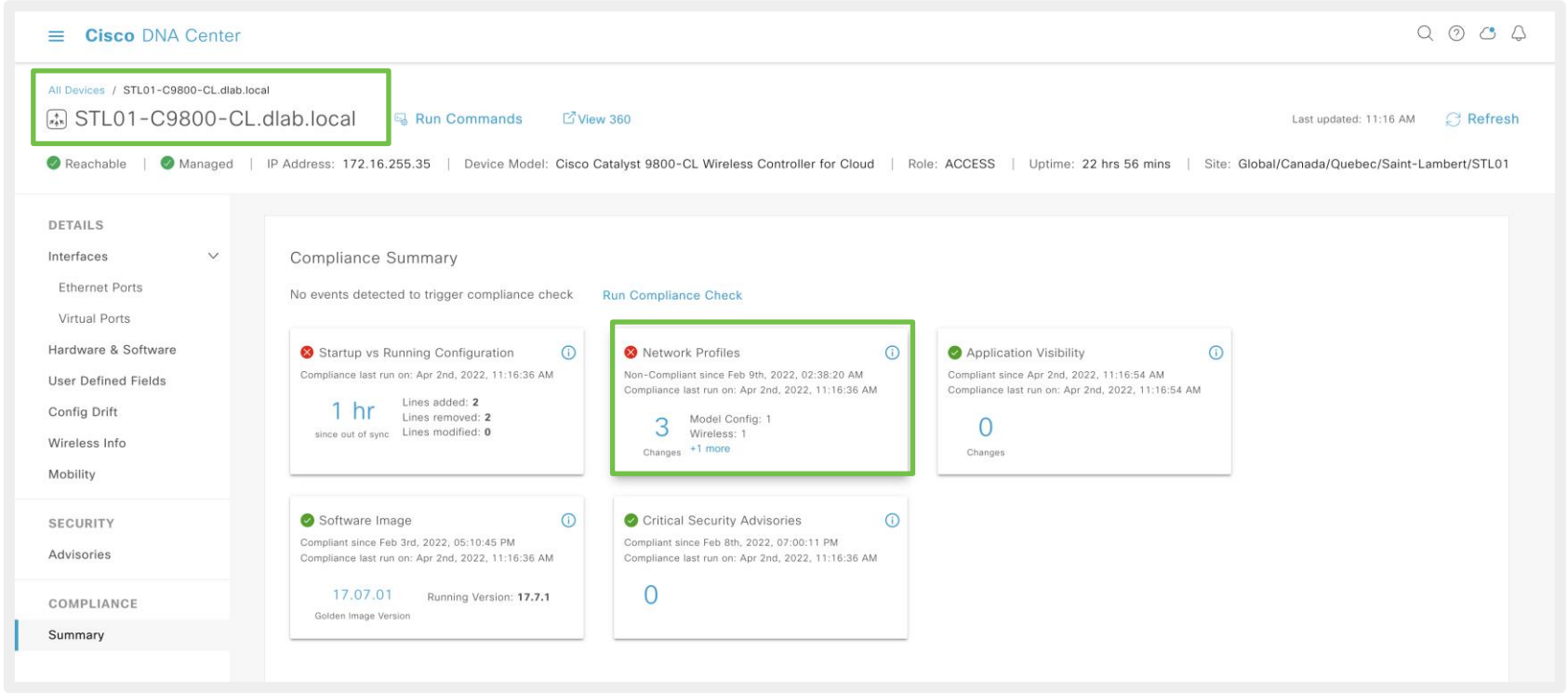
```
C9K-BRANCH-STACK#conf t
Enter configuration comm
C9K-BRANCH-STACK(config)
C9K-BRANCH-STACK(config-
```



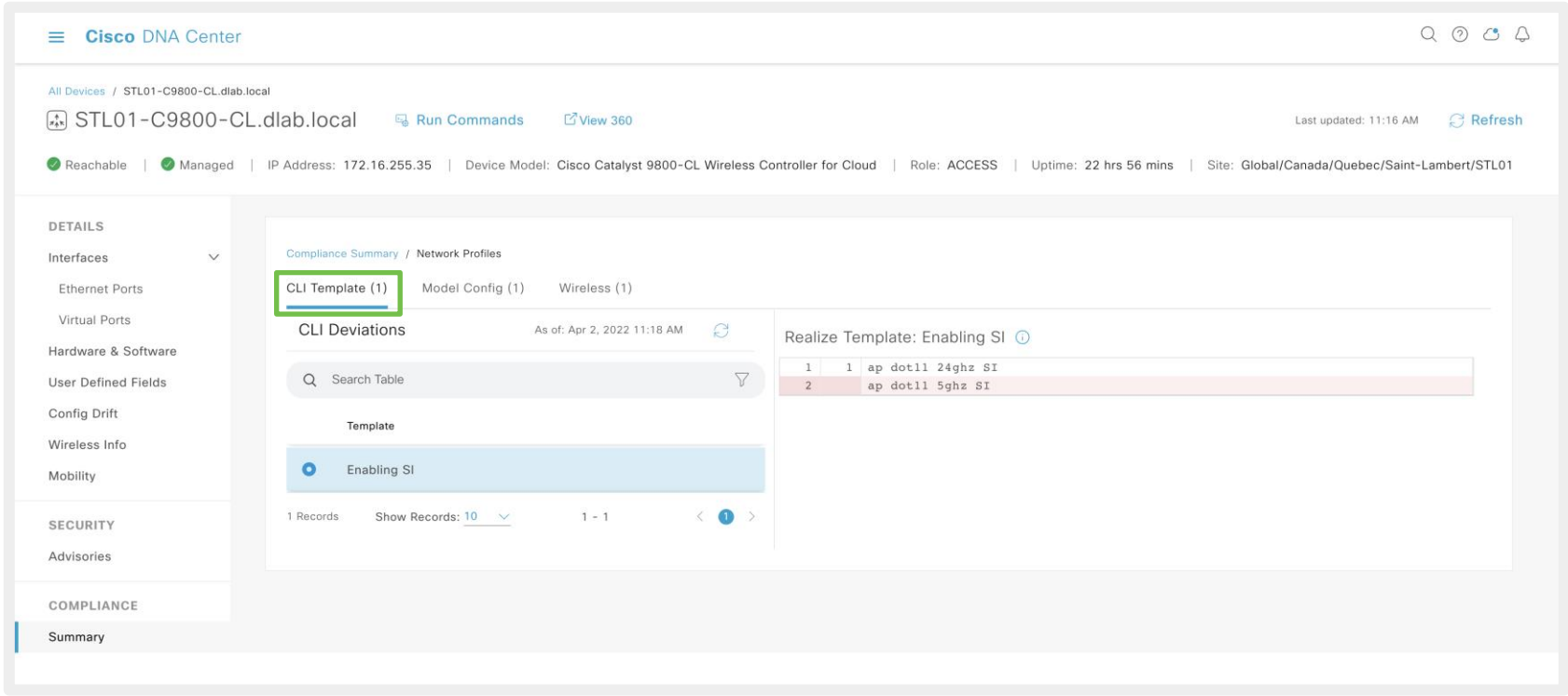
Config Drift



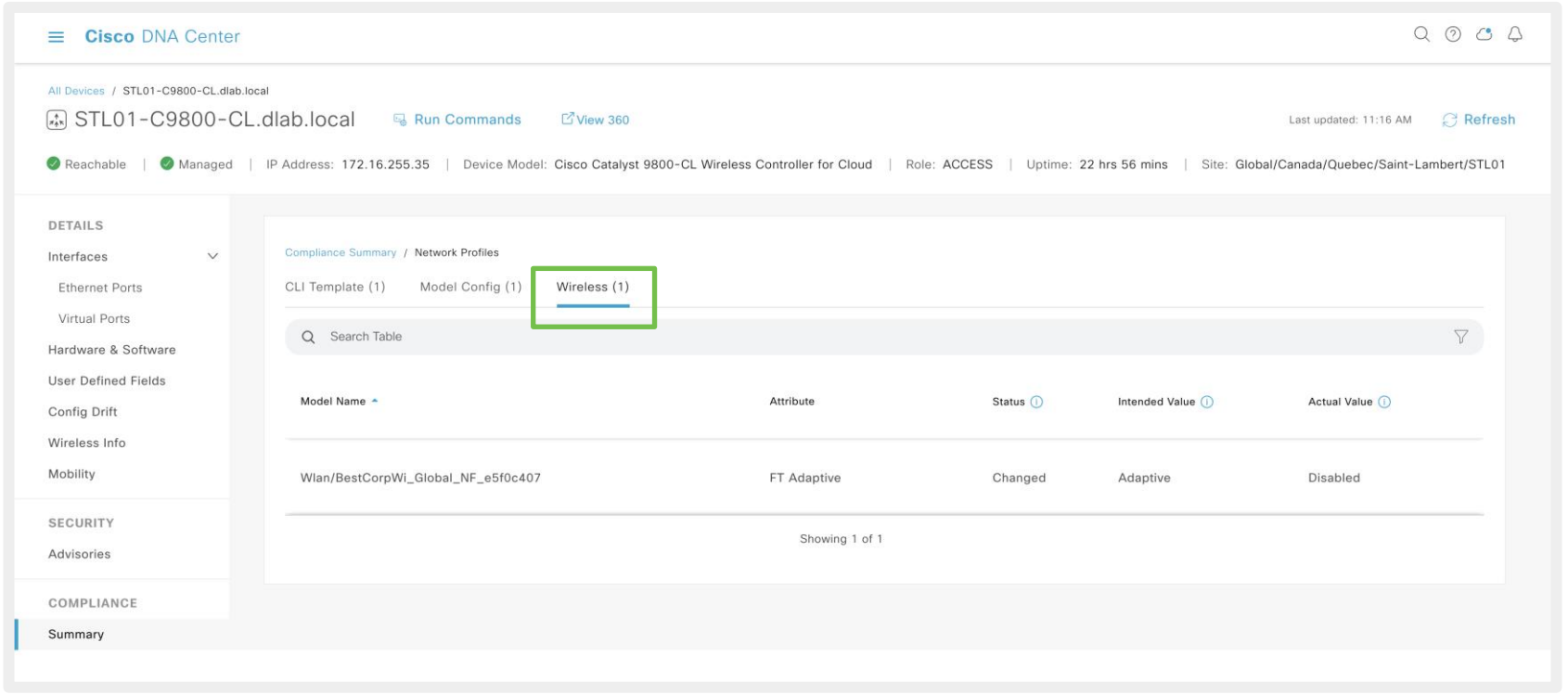
Compliance: Network Profiles – Wireless



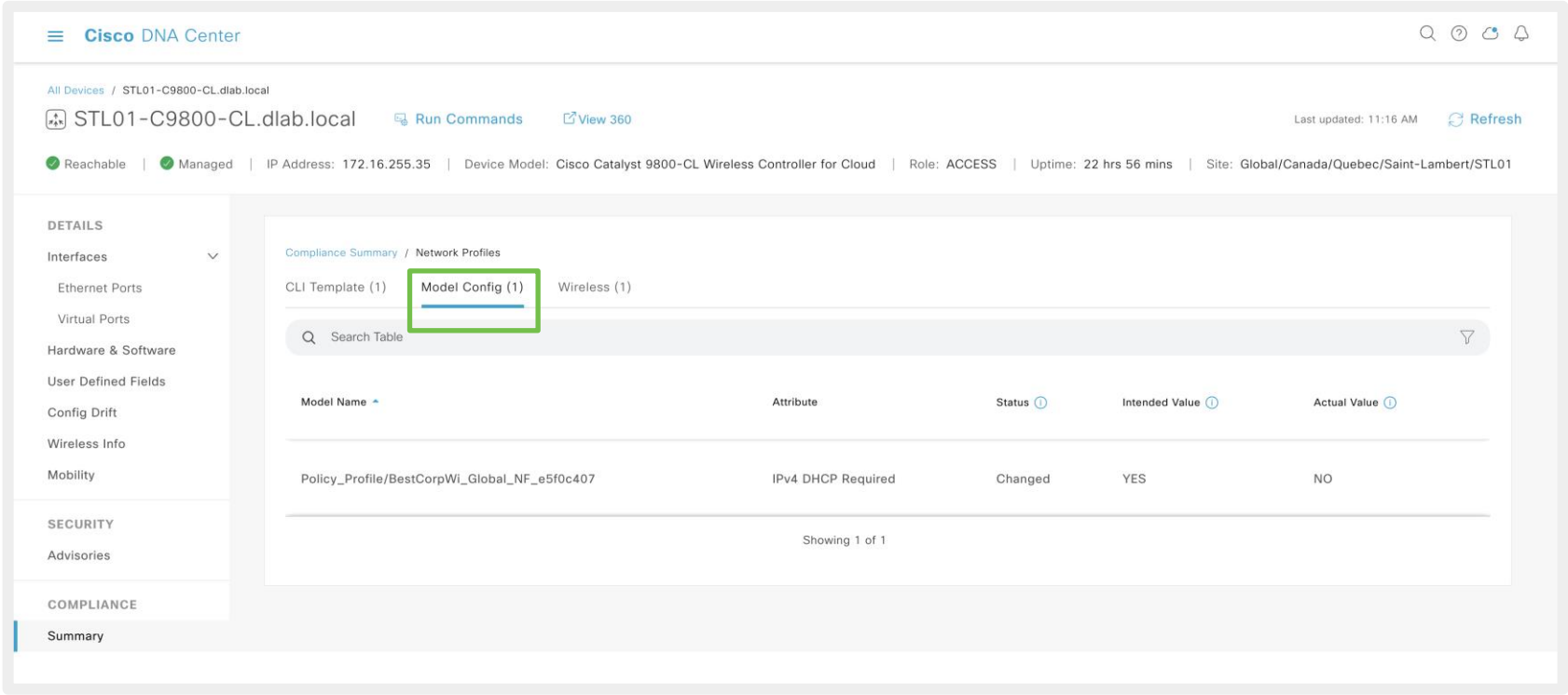
Compliance: Network Profiles – Wireless



Compliance: Network Profiles – Wireless

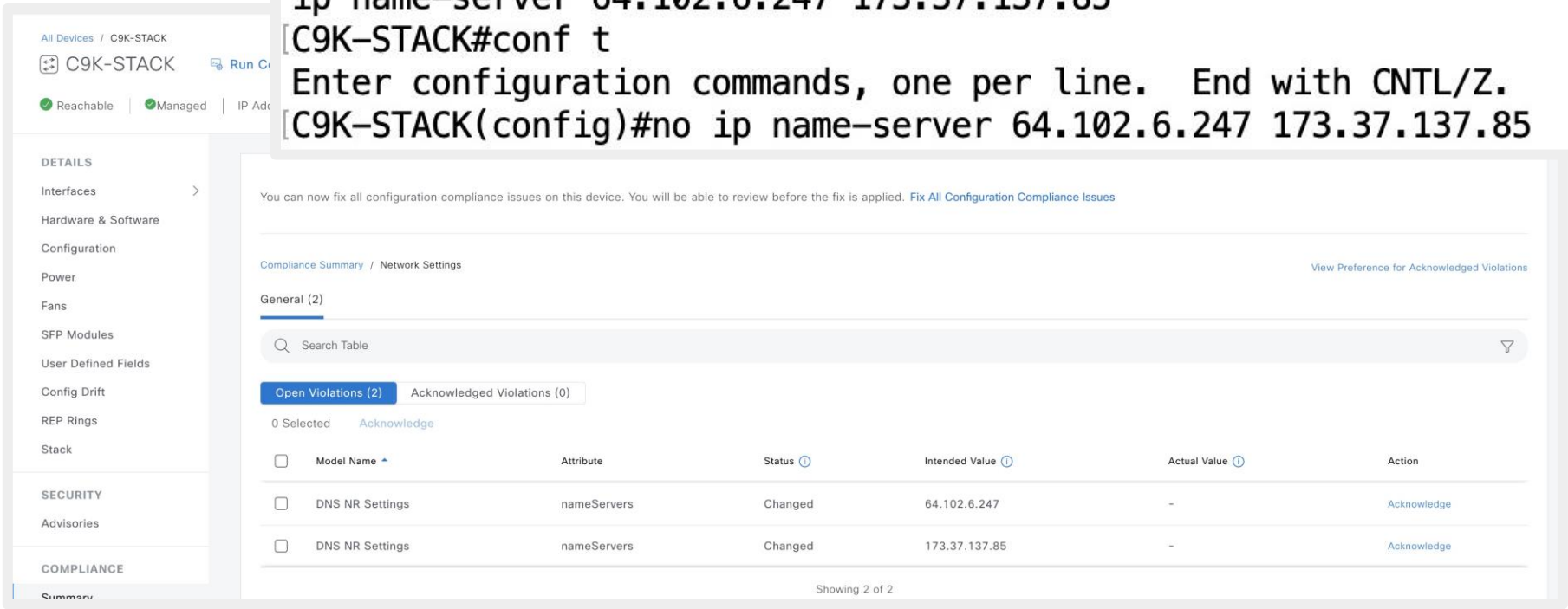


Compliance: Network Profiles – Wireless

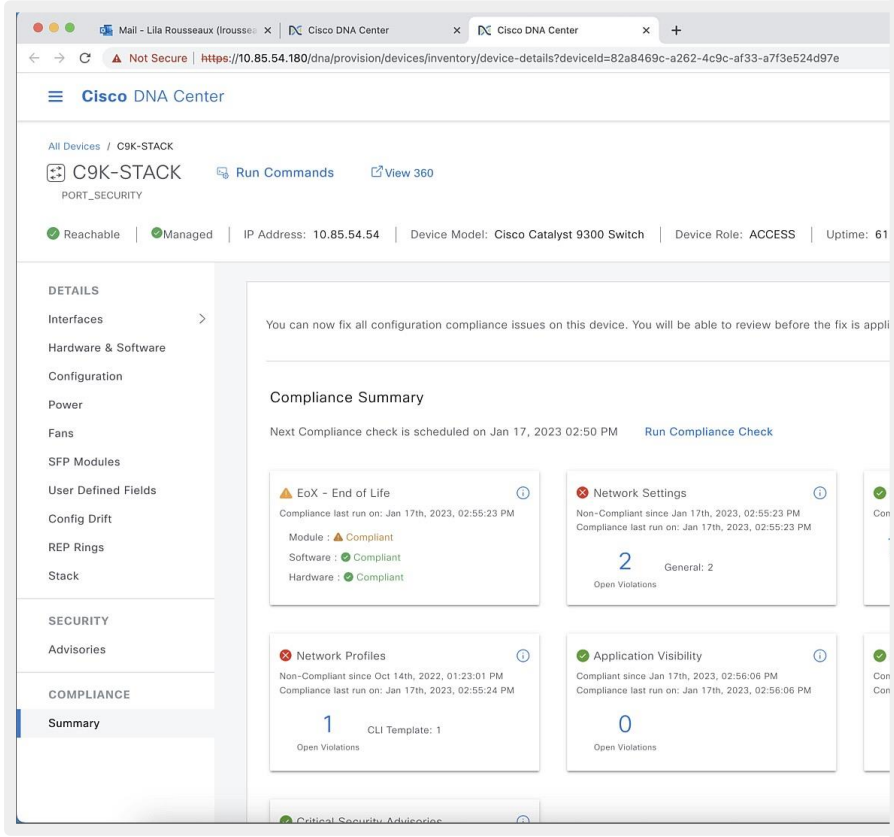


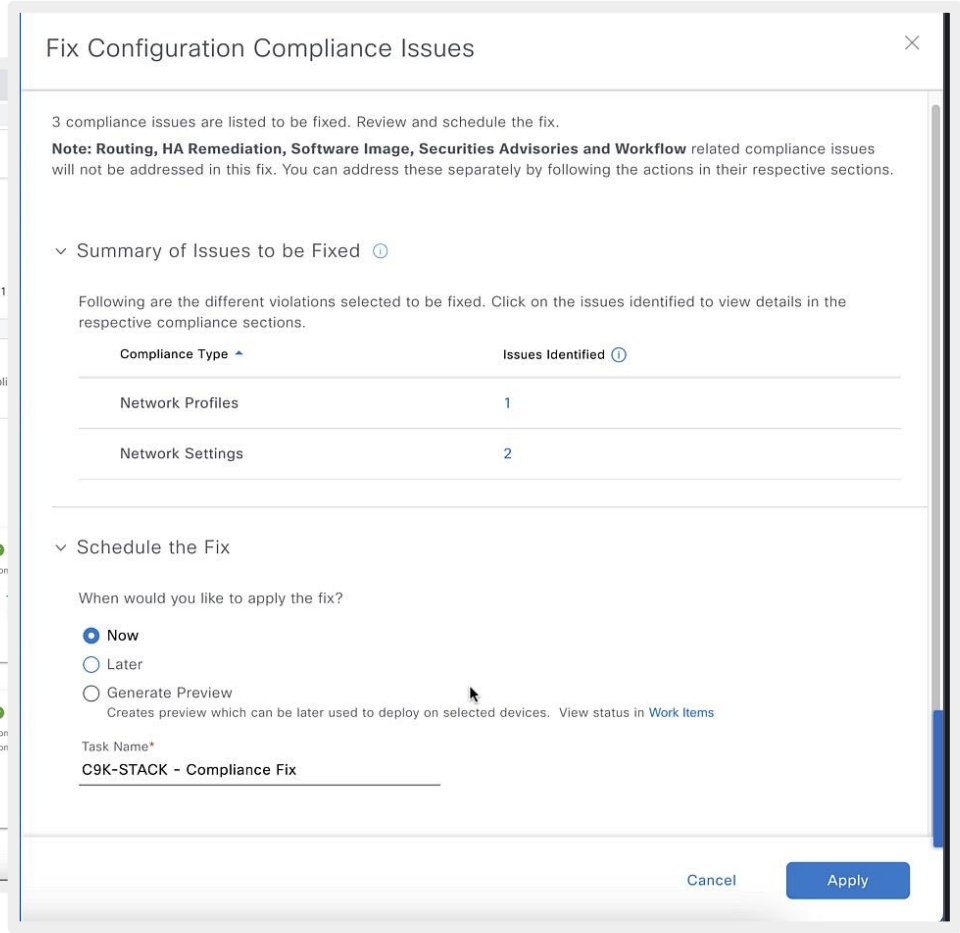
Network Setting Compliance

```
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
```



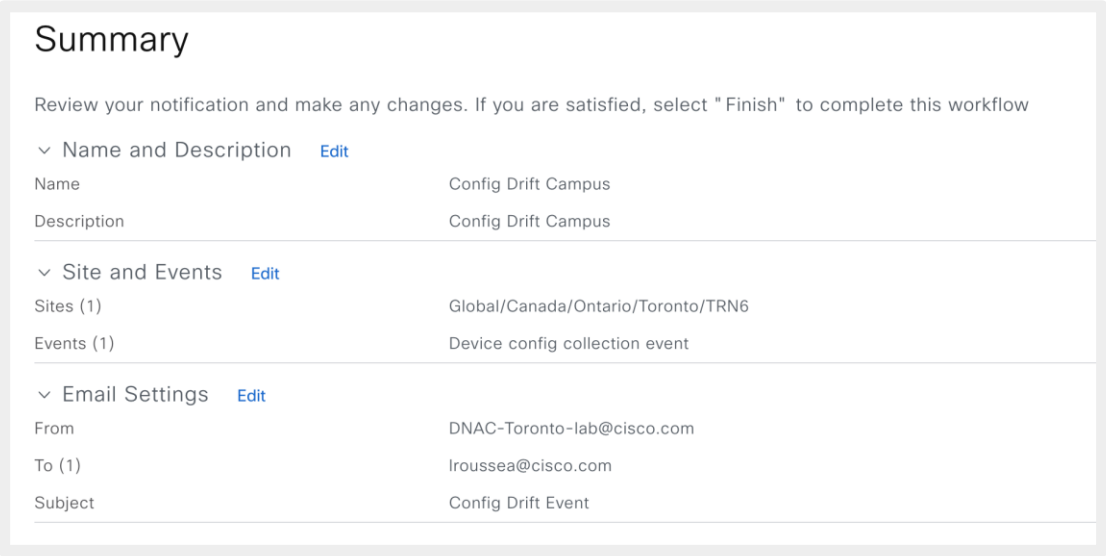
Fix Config Compliance Issues





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



Network Compliance Event Notification

Reference

Sample email notification

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 Applicabl
    "Triggered By": "Initial Archive",
    "Device User Name": "Not Applicab
  },
  "ciscoDnaEventLink": "https://&lt;DN
tails?deviceId=$deviceId$",
  "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"
}
```


DNAC-Toronto-lab@cisco.com

To: Lila Rousseaux (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

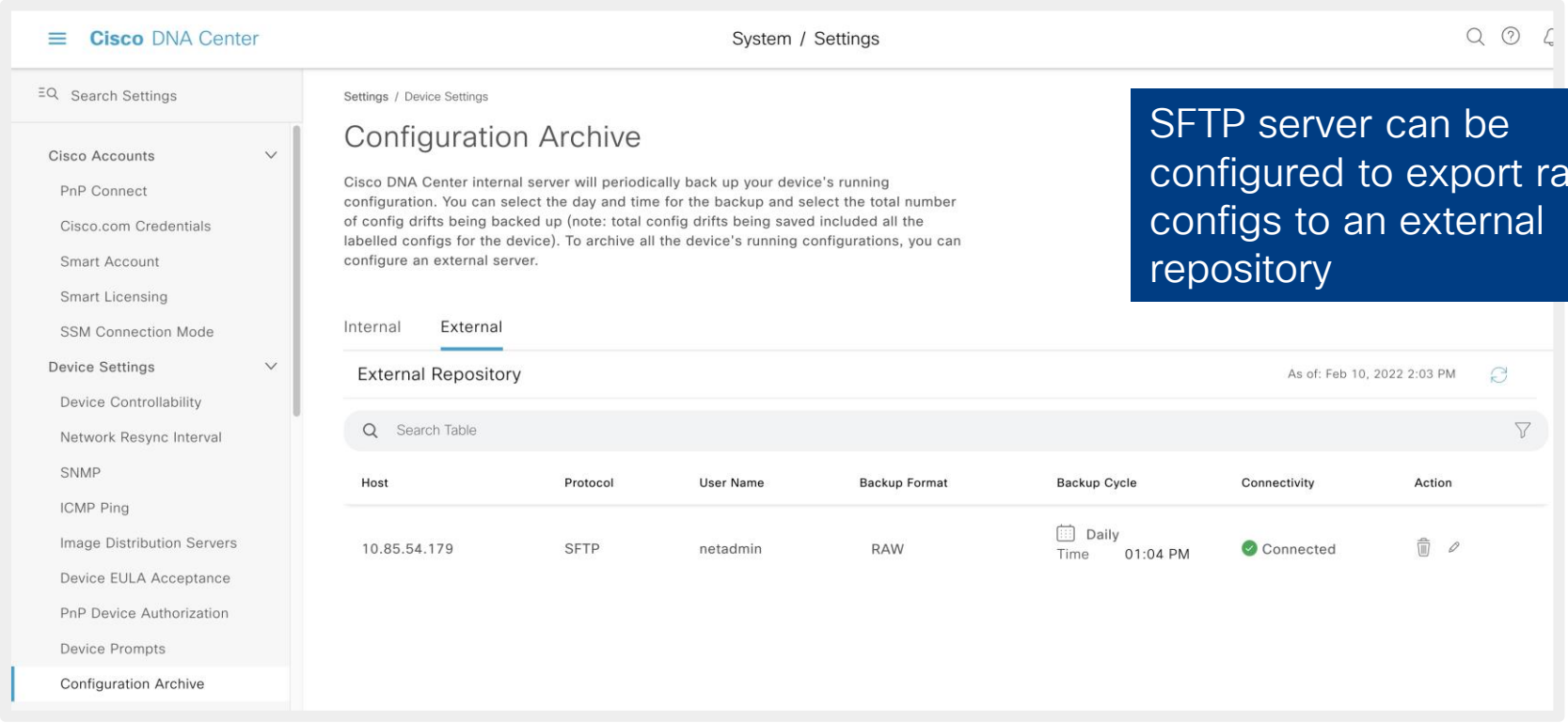
Messages | People (2) | Content | Meetings

Cisco DNA Center Notification

Source DNA Center IP:	10.104.241.138
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

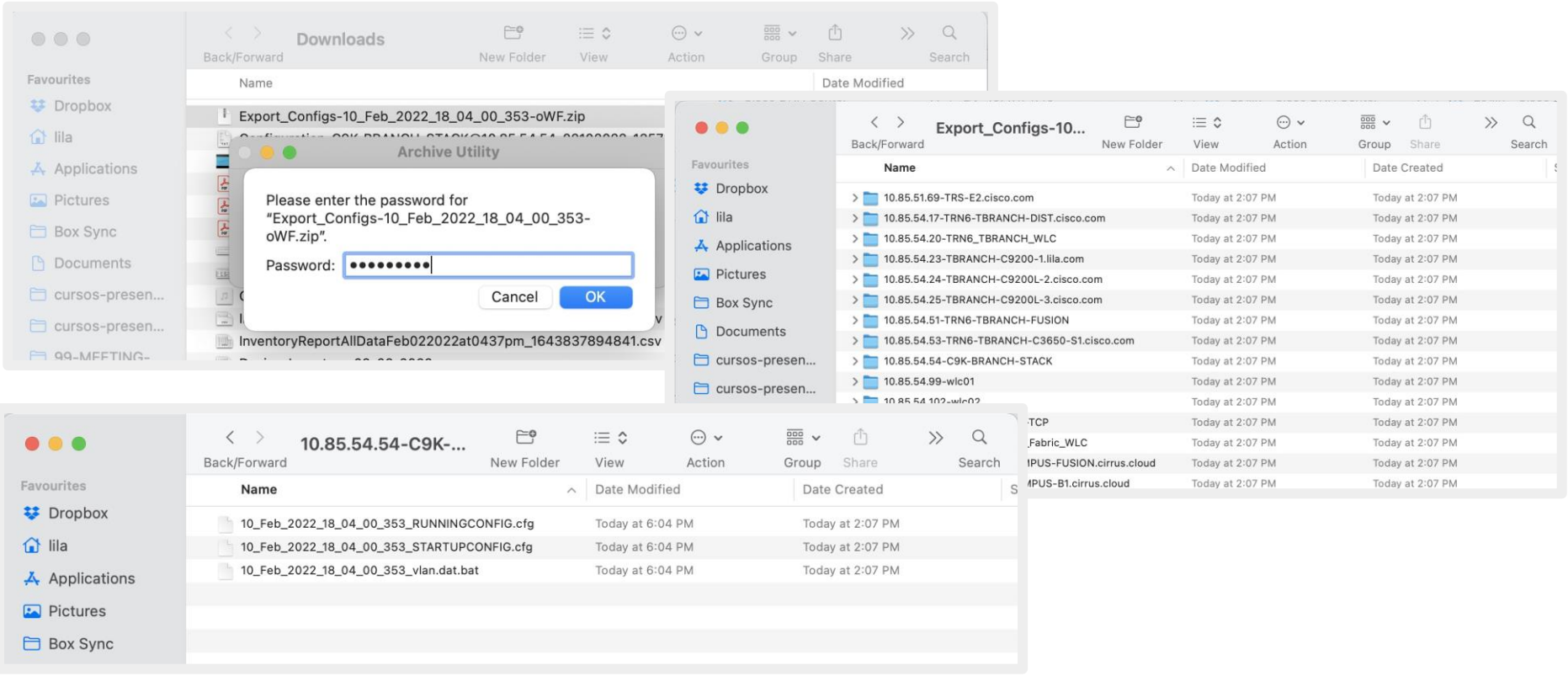


SFTP server can be configured to export raw configs to an external repository

Device Configuration Management

Configuration Archive

Reference



Device Configuration Management

Configuration Archive

Reference

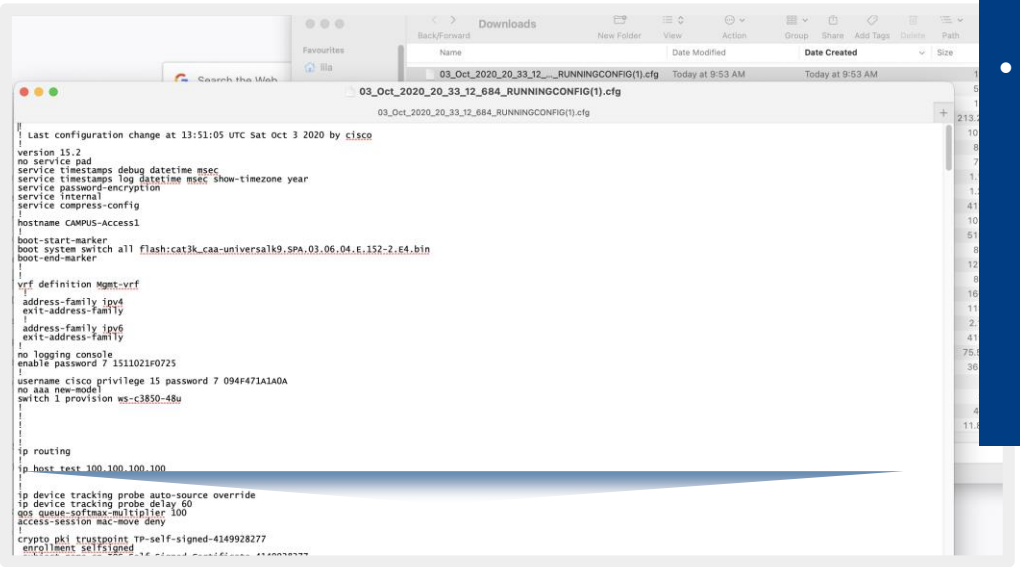
10_Feb_2022_18_04_00_353_RUNNINGCONFIG.cfg

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/gvcAL9GFOU$k6/kumGDPS/ABbtHwK8xZqGeVEVvM3idf83ZIm4zH92
!
no aaa new-model
boot system switch all flash:packages.conf
switch 1 provision c9300-24p
switch 2 provision c9300-24p
!
!
!
!
ip routing
!
!
ip nbar attribute-map BR2
 attribute business-relevance default
ip nbar attribute-map TC3
 attribute traffic-class multimedia-streaming
```

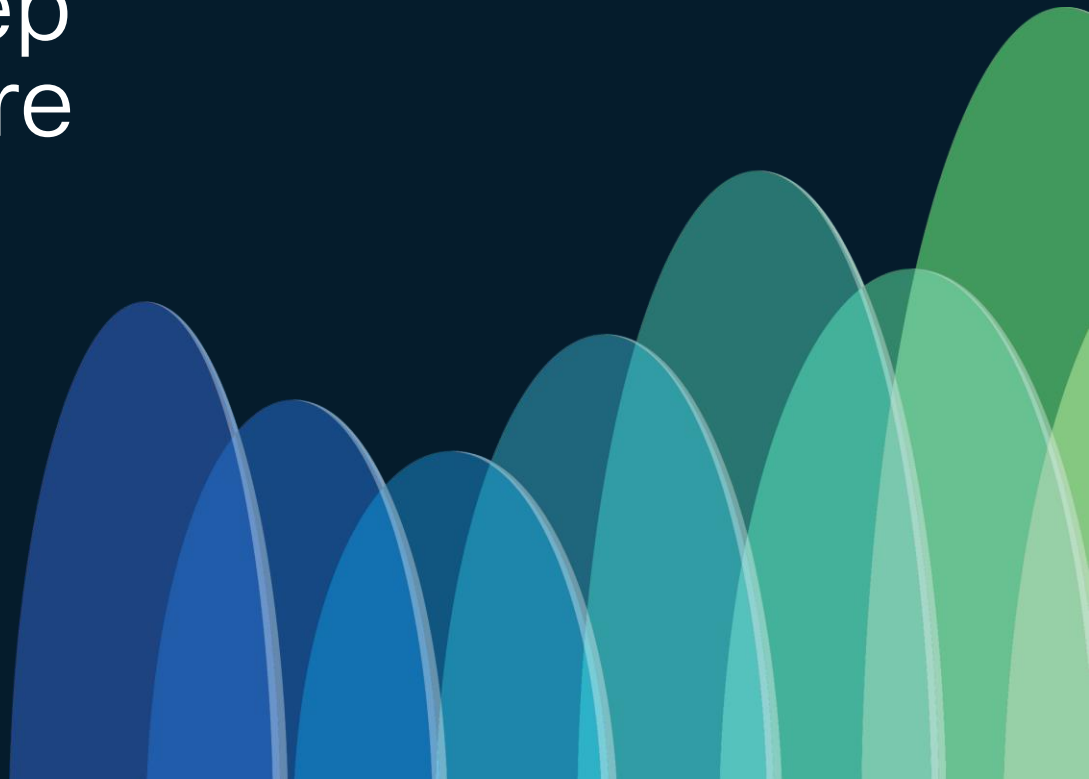
Device Configuration Management

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



cisco Live!

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 were ISSU not available
- Consider external file servers for remote sites
- Install Mode is recommended mode
- "Bundle"/"Install" mode conversion is not supported

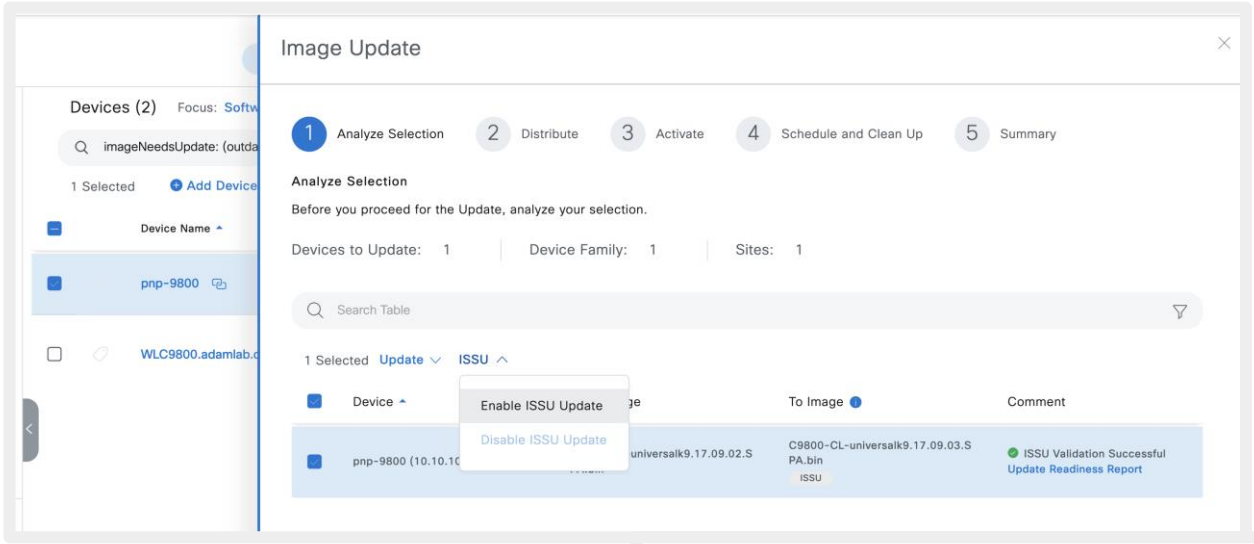
Control over SWIM- ISSU

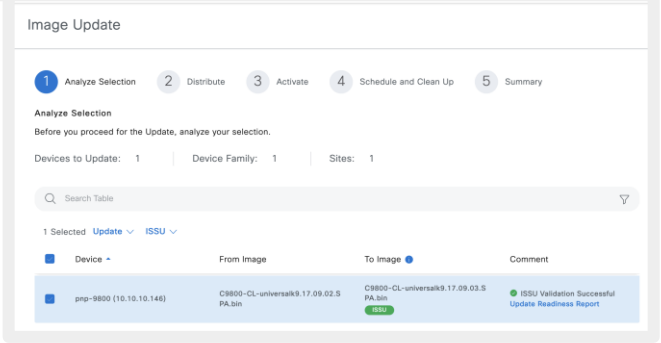
ISSU supports both Wired & Wireless devices

ISSU support for C9800 controller starting 17.3

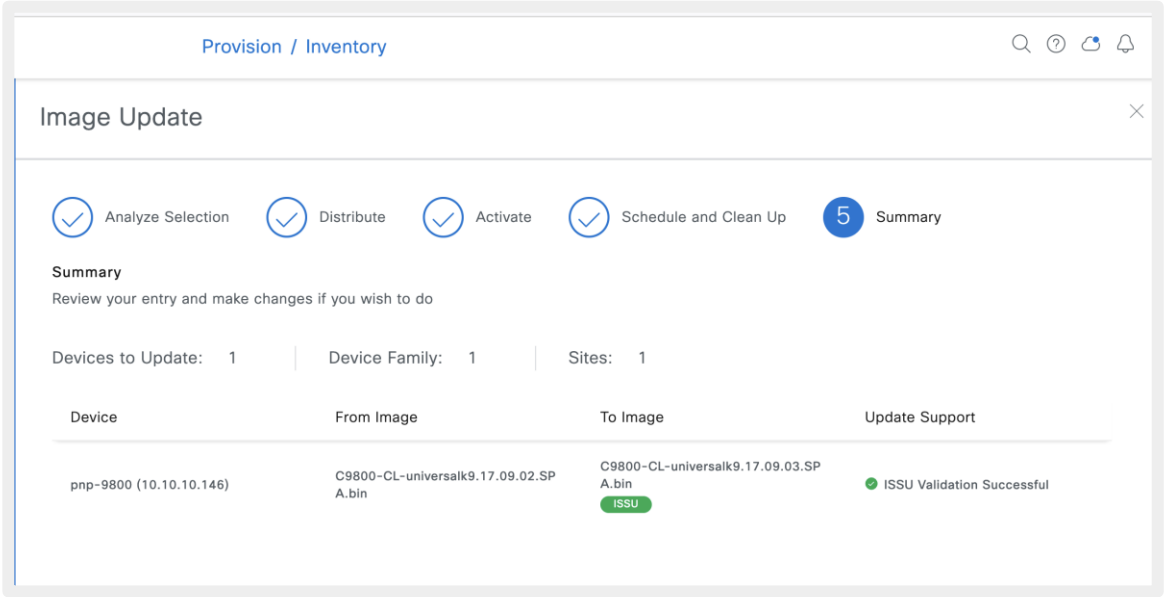
Helps reduce downtime for wireless Infrastructure

ISSU requires controllers in HA SSO or N+1





Ready to go ISSU

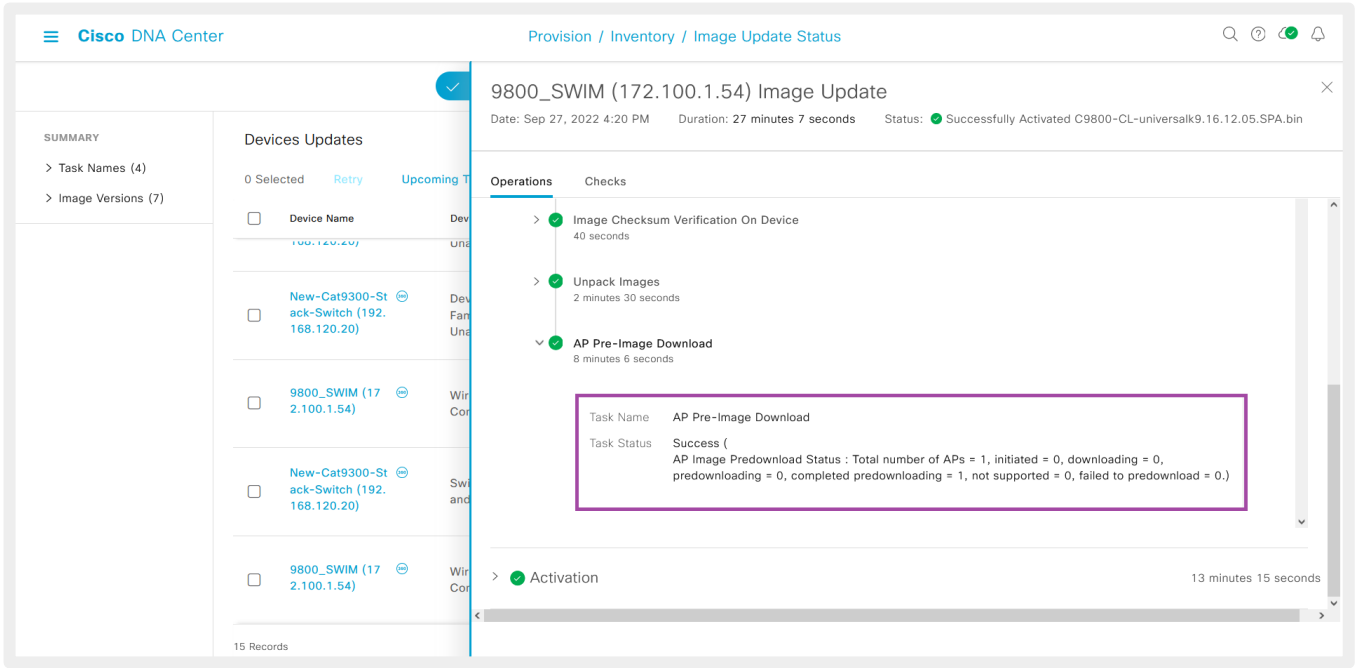


Control SWIM- AP Pre-Image Download/Rolling AP Upgrade

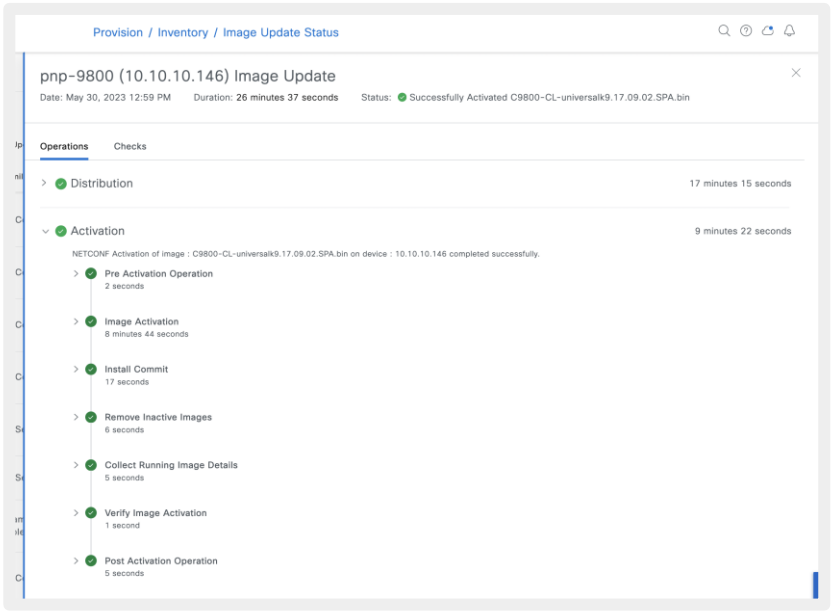
ISSU together with AP Pre-Image Download and Rolling AP Upgrade helps reduce network downtime

Controllers needs to be provisioned for Rolling AP Upgrade

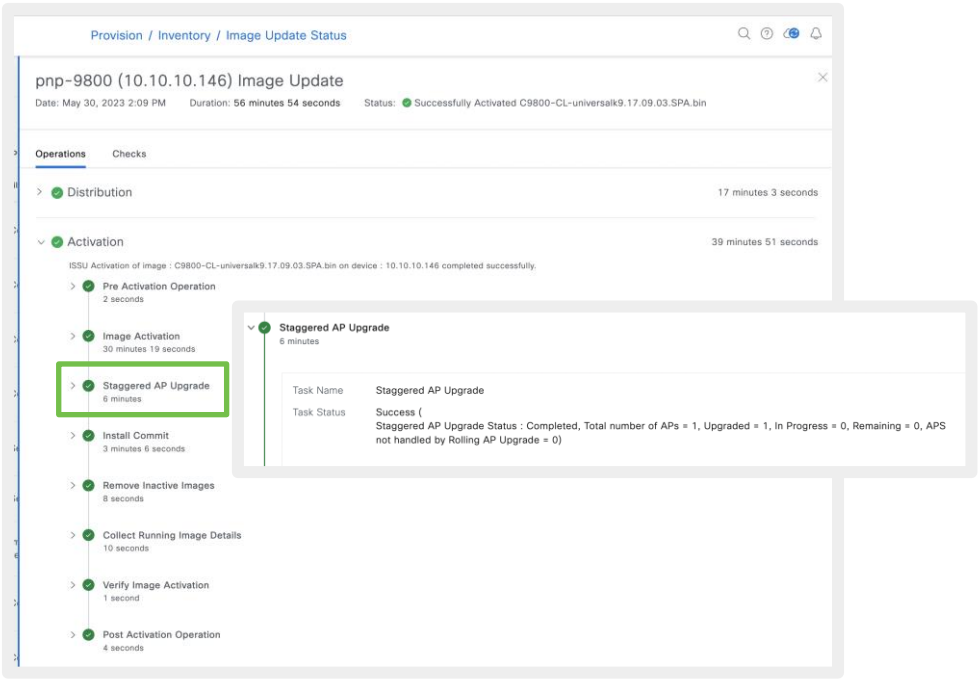
AP Pre-image download by default available starting version 2.3.3.x



Activation for normal wireless vs ISSU wireless



Normal Activation



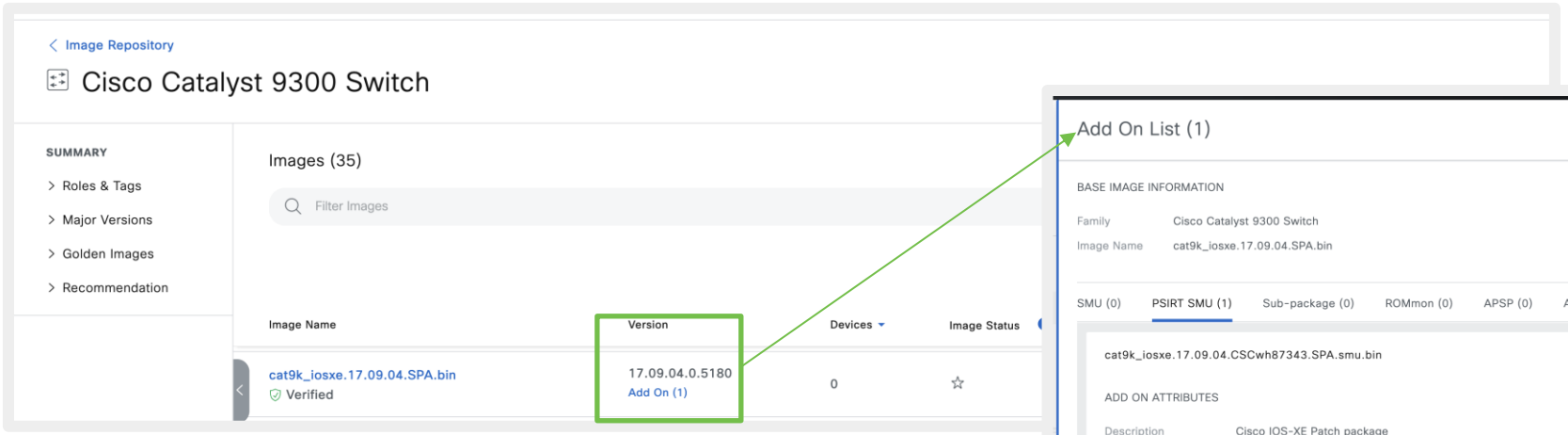
ISSU Activation

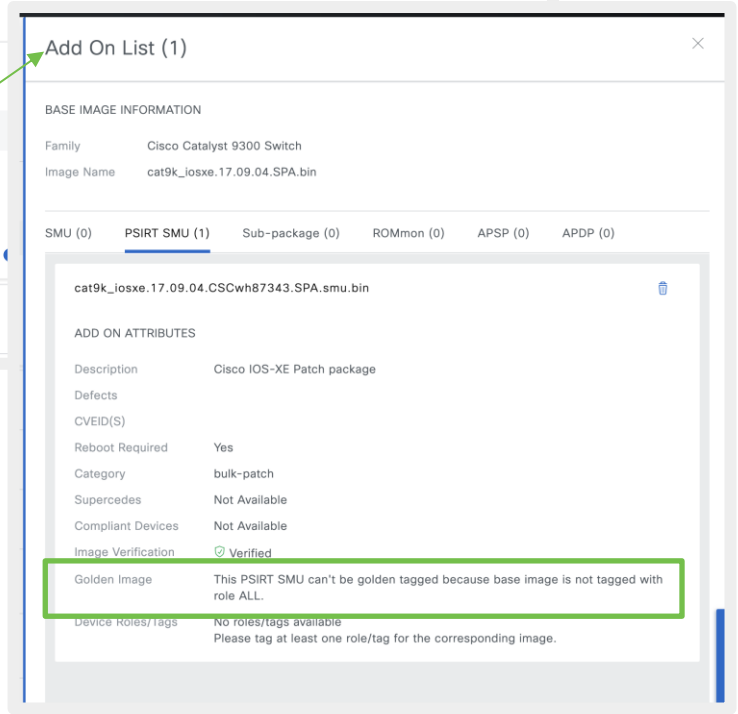
Staggered Upgrade

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





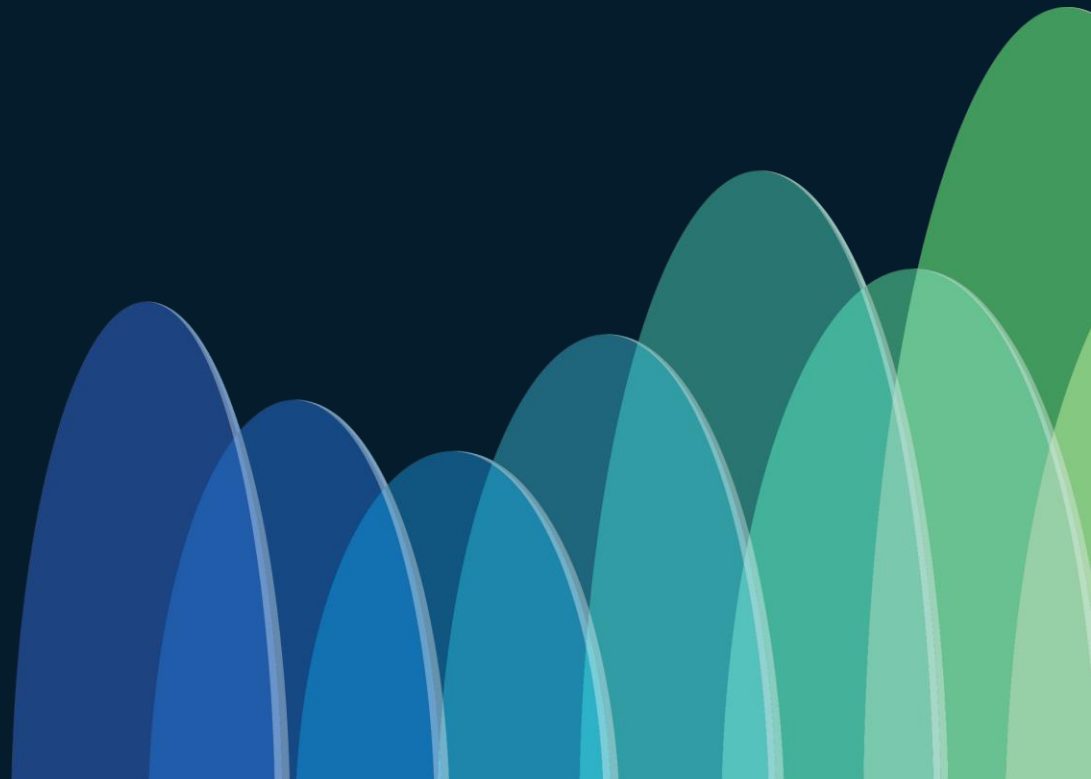
Need to mark as golden (along with main image)

Downloadable direct from CCO

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

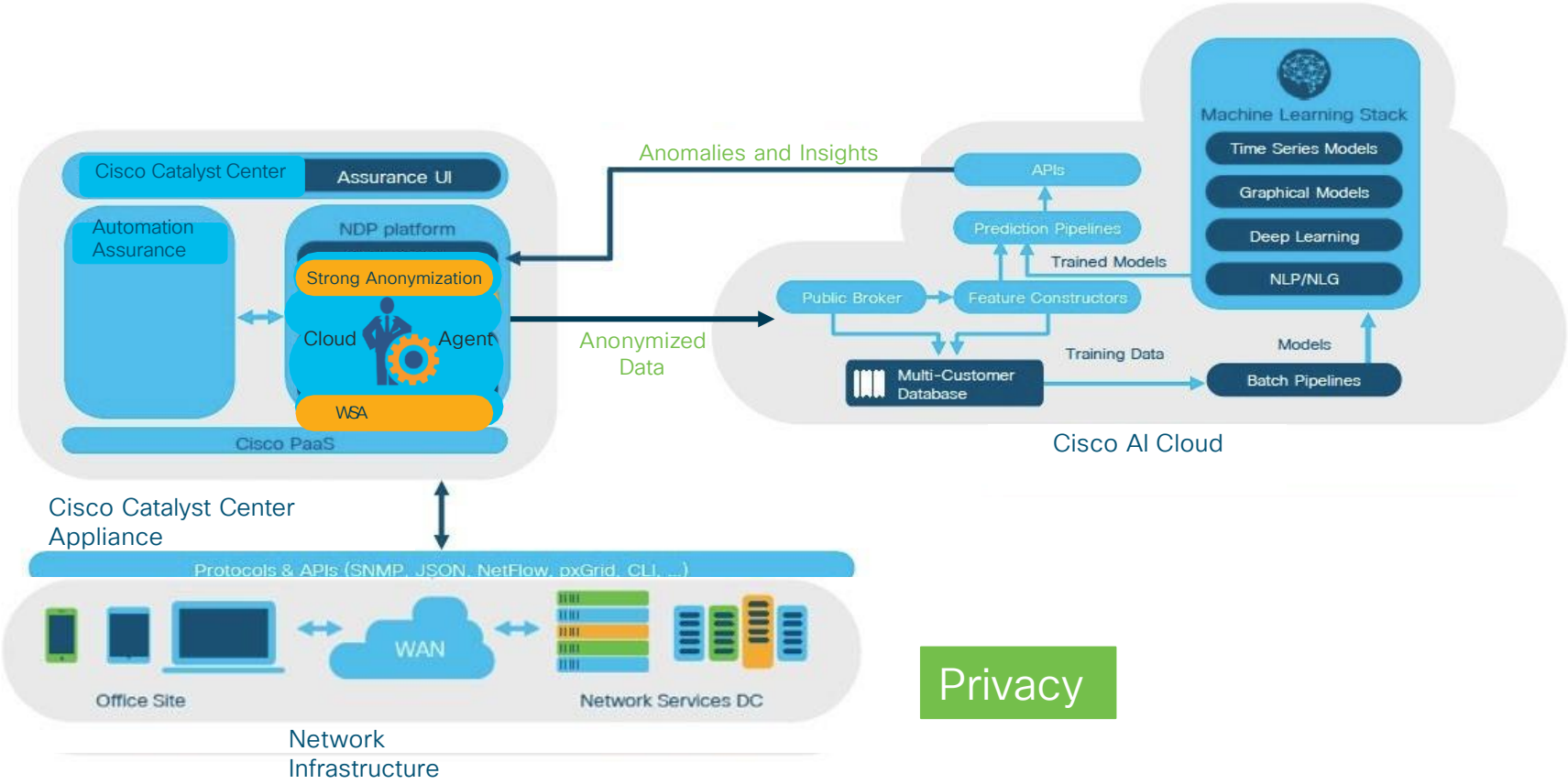
AP service pack and device pack manual download from CCO/upload

Habit #5 - Explore Proactive insights with AI/ML



cisco Live!

Cisco AI Network Analytics Architecture

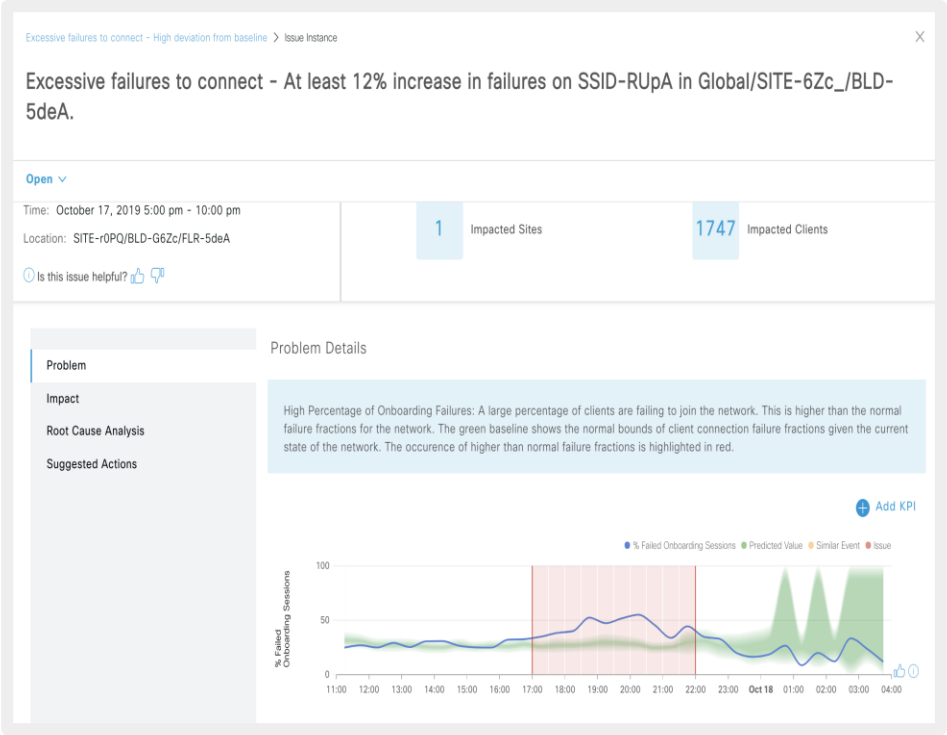


AI Driven Baseline Issues

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



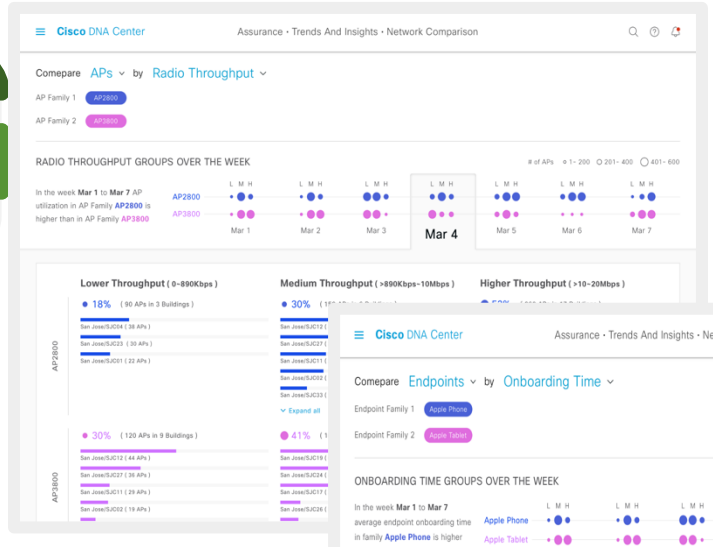
AI Analytics – AP Family & Endpoint Comparison

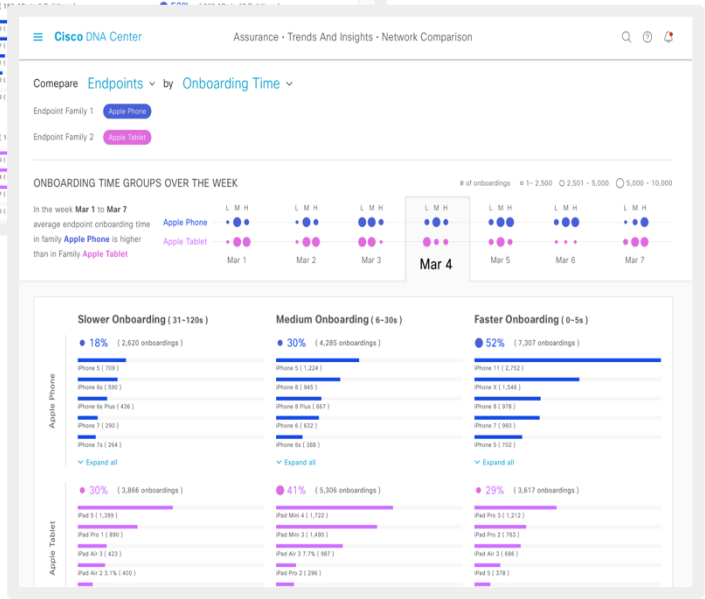
Use case:

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

Key Benefits:

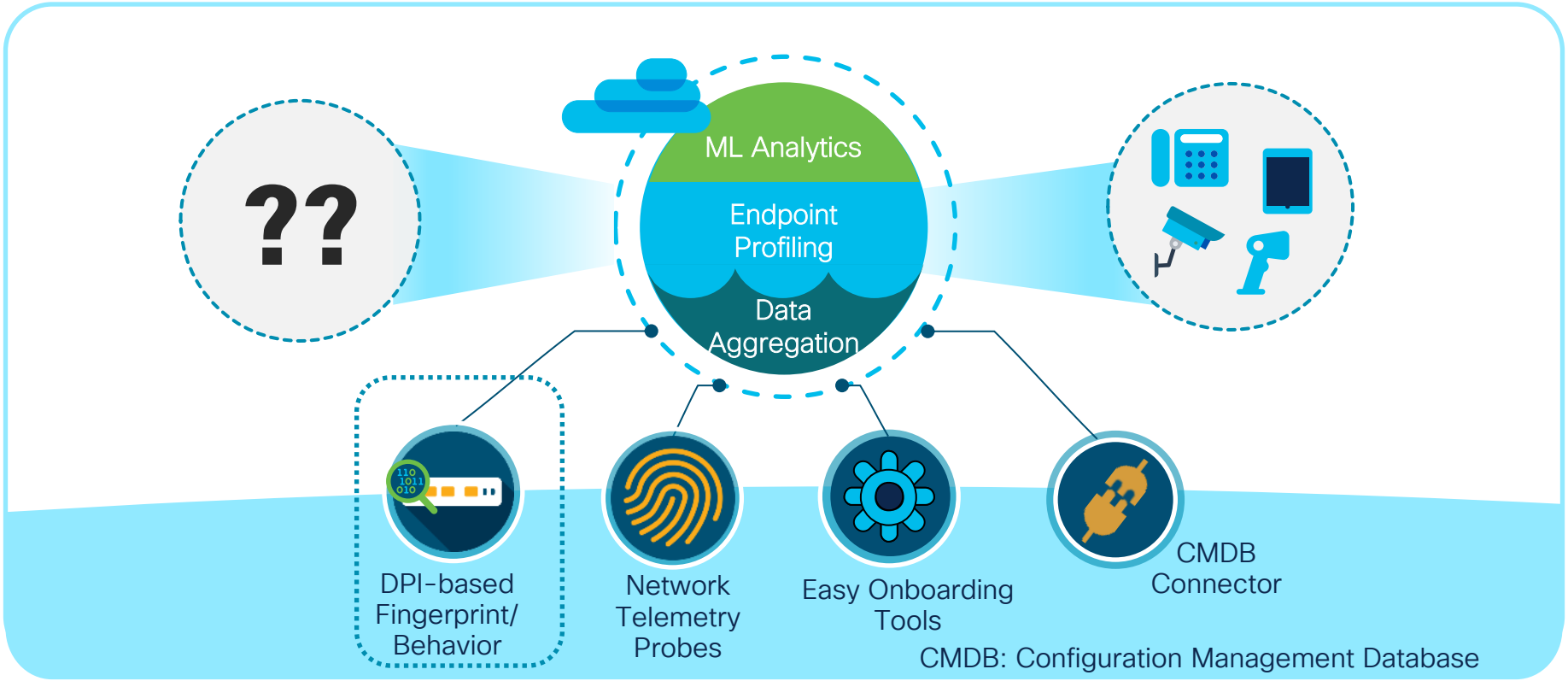
- Compare AP performance across traffic classes.
- Flexibility to compare both on-boarding and throughput KPI's
- View and compare dynamic performance clusters for a selected KPI and AP families.
- View and compare onboarding KPIs for specific device types for days of a week..



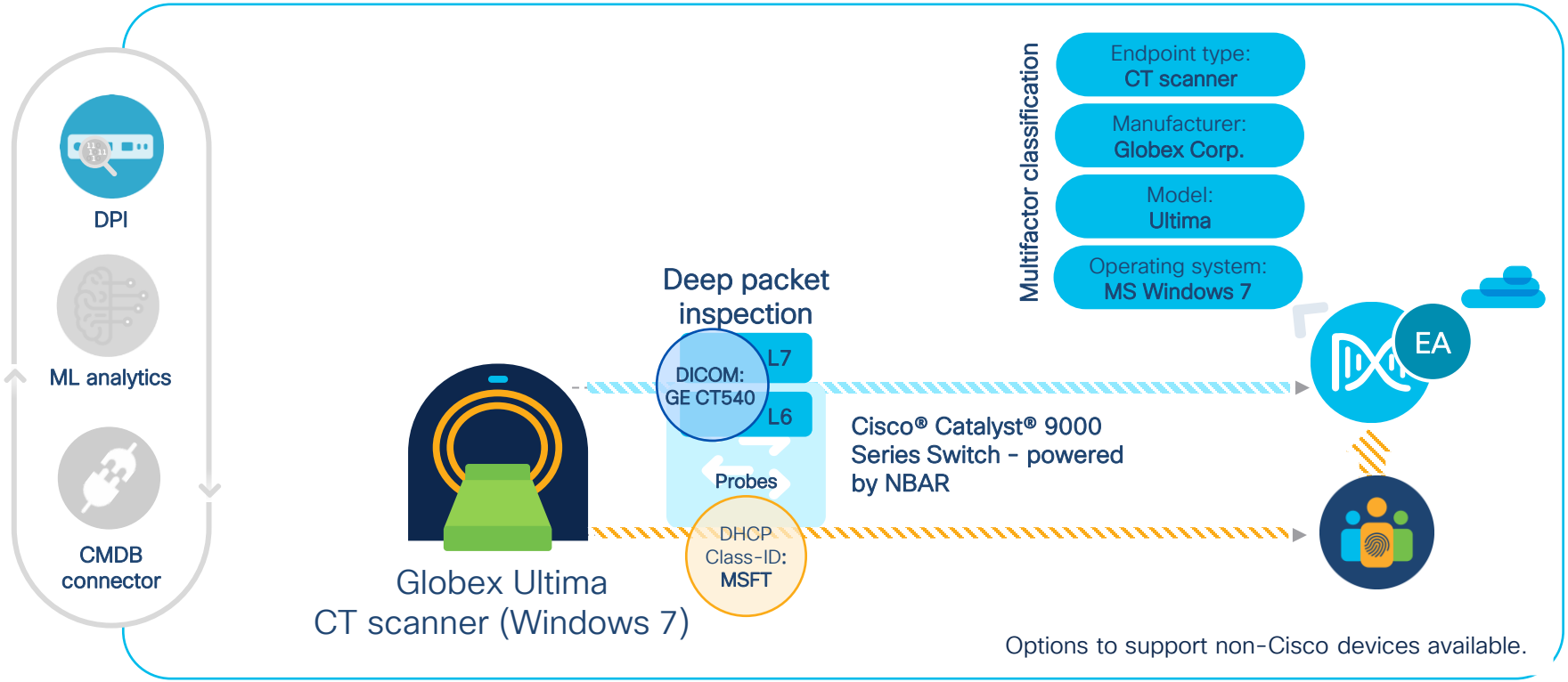


AI Endpoint Analytics on Cisco Catalyst Center

Rapidly reducing the unknowns by aggregating data from different sources

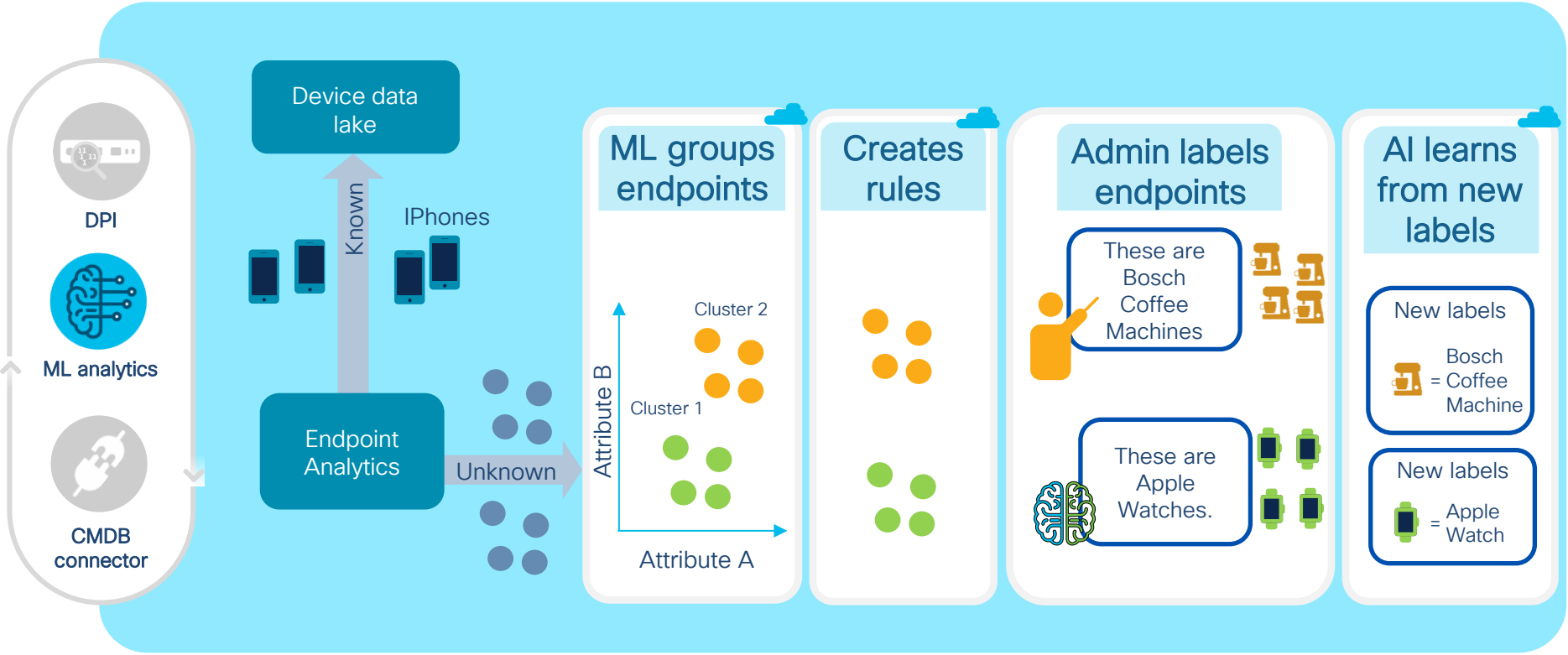


Classification based on Deep Packet Inspection (DPI)



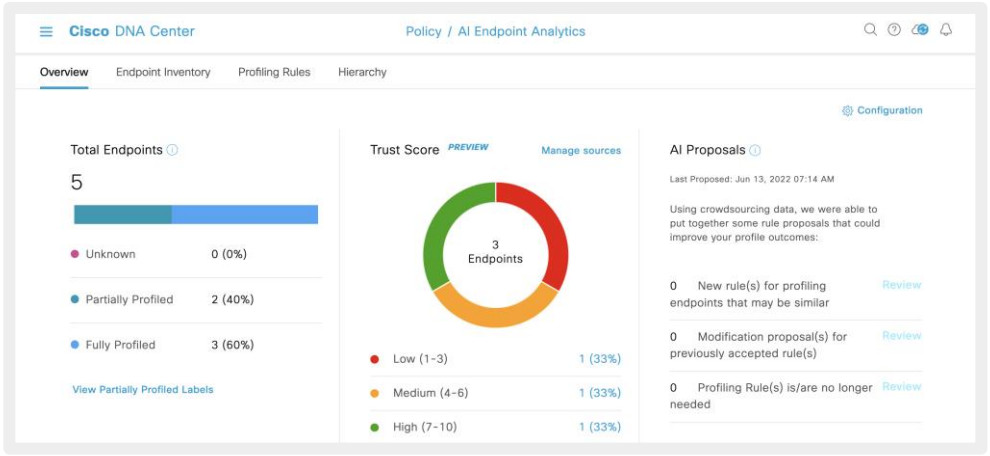
Reducing Unknowns with Machine Learning

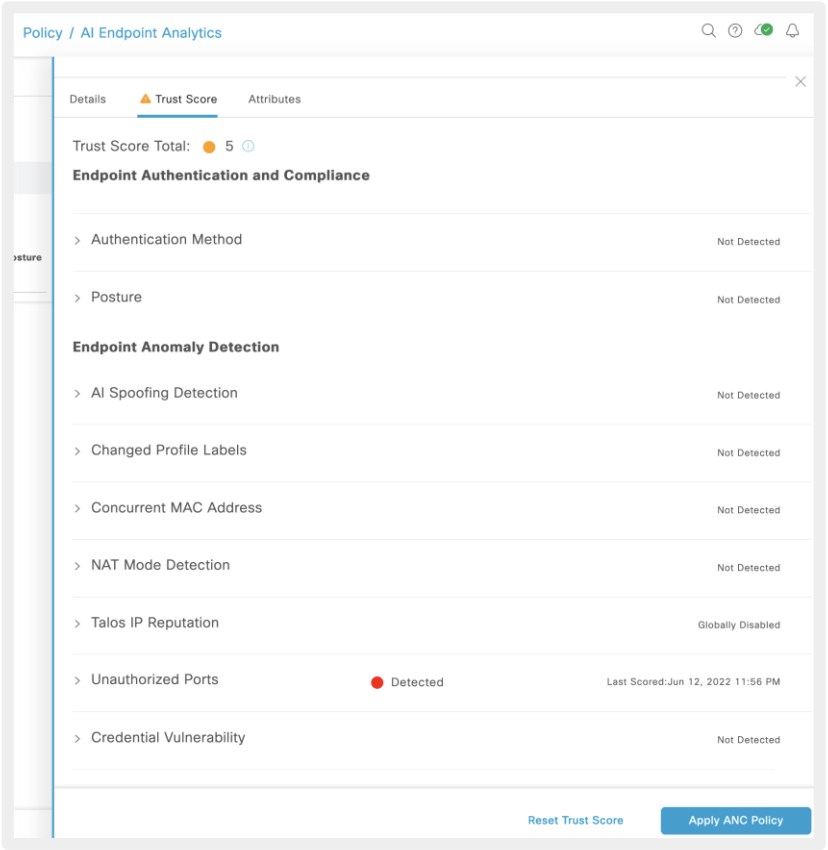
Reference



= done in cloud

Trust Scores and Remediation

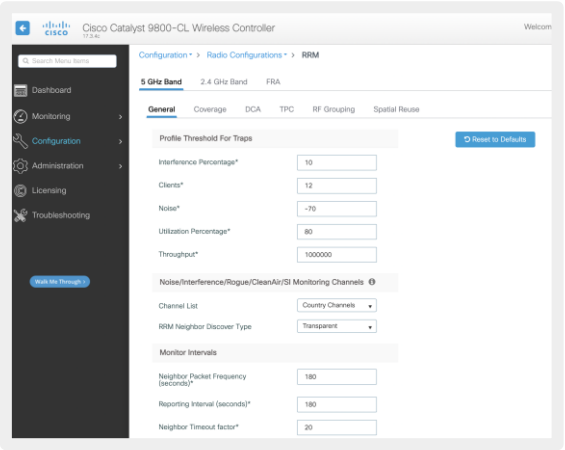




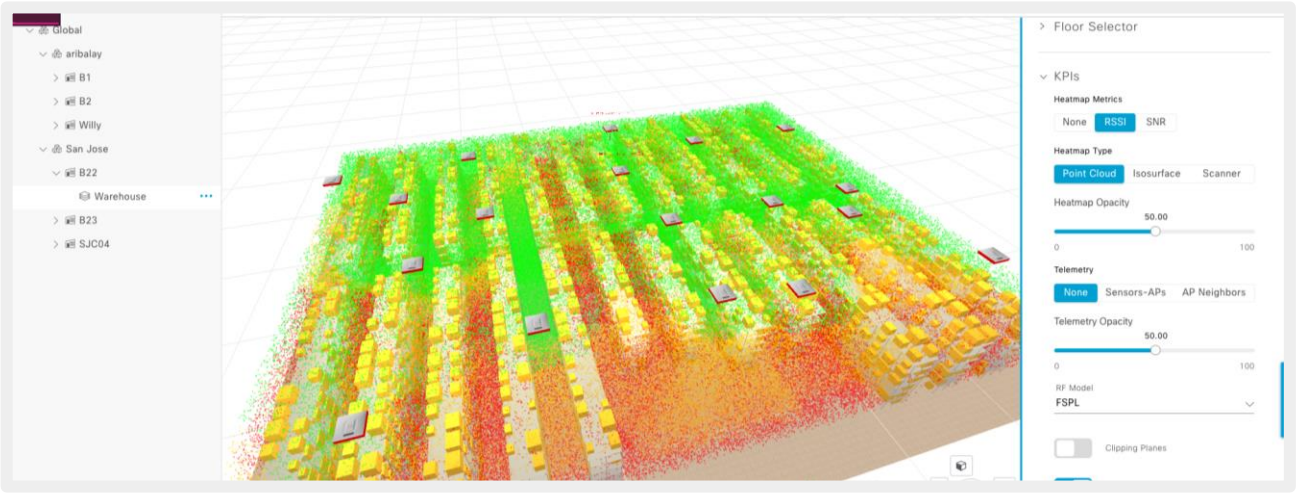
Adaptive Network Control - ANC

Remediate the host via Identity Services Engine - ISE

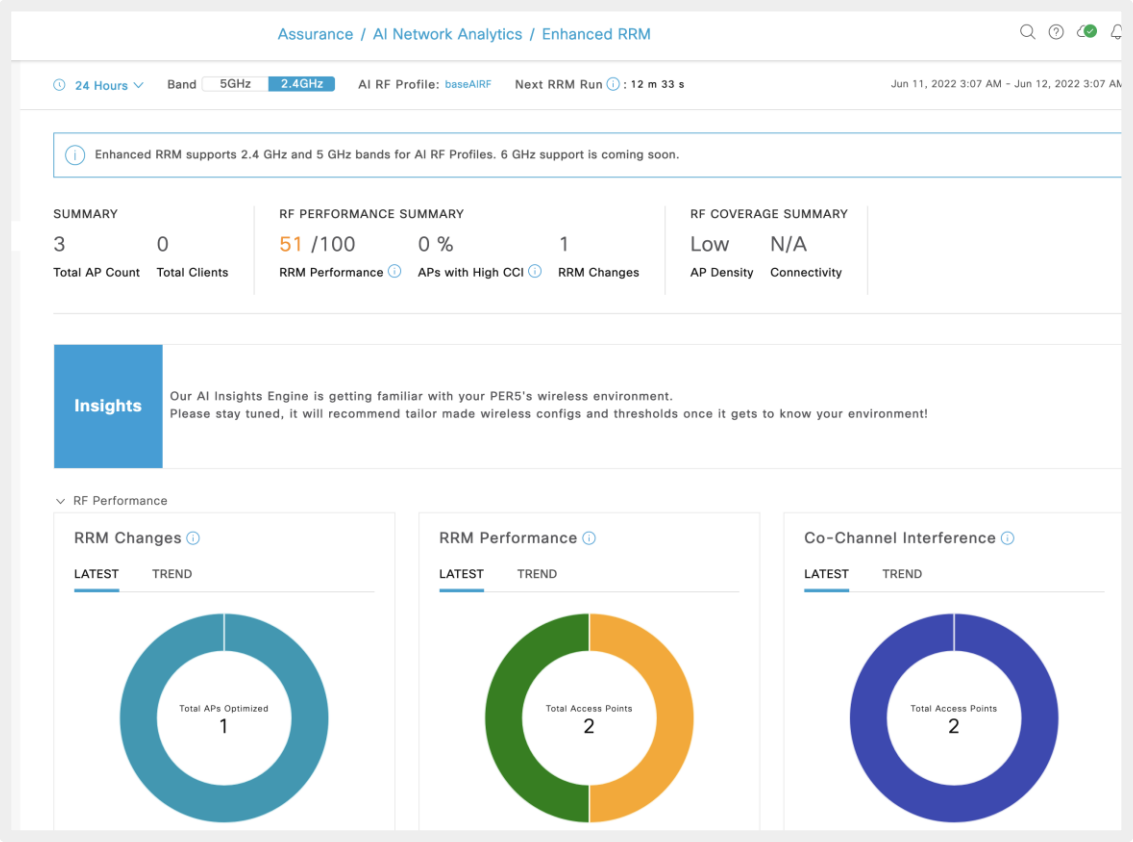
Why radio resource management



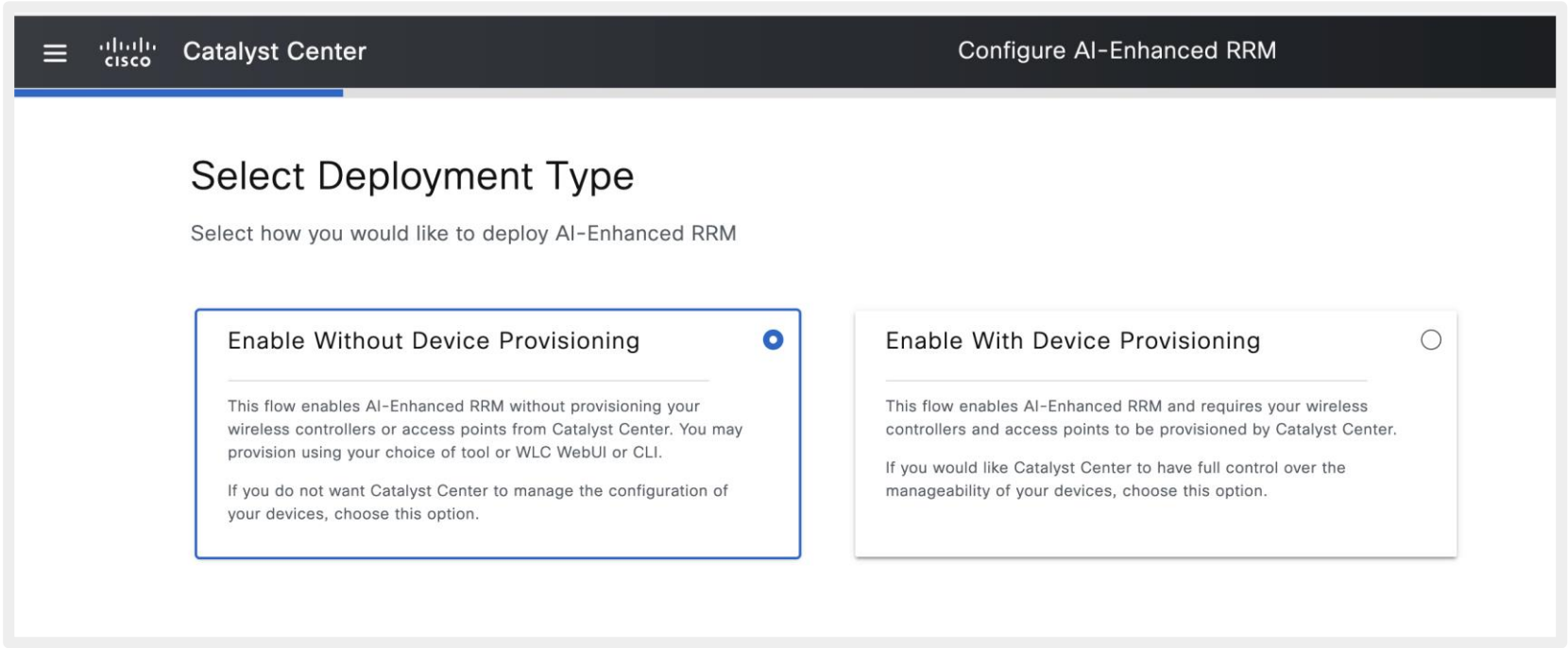
- 10min worth of data
- No "busy hour(s)"
- No building segmentation
- No visibility
- Lots of tuning knobs
- No simulation mode **



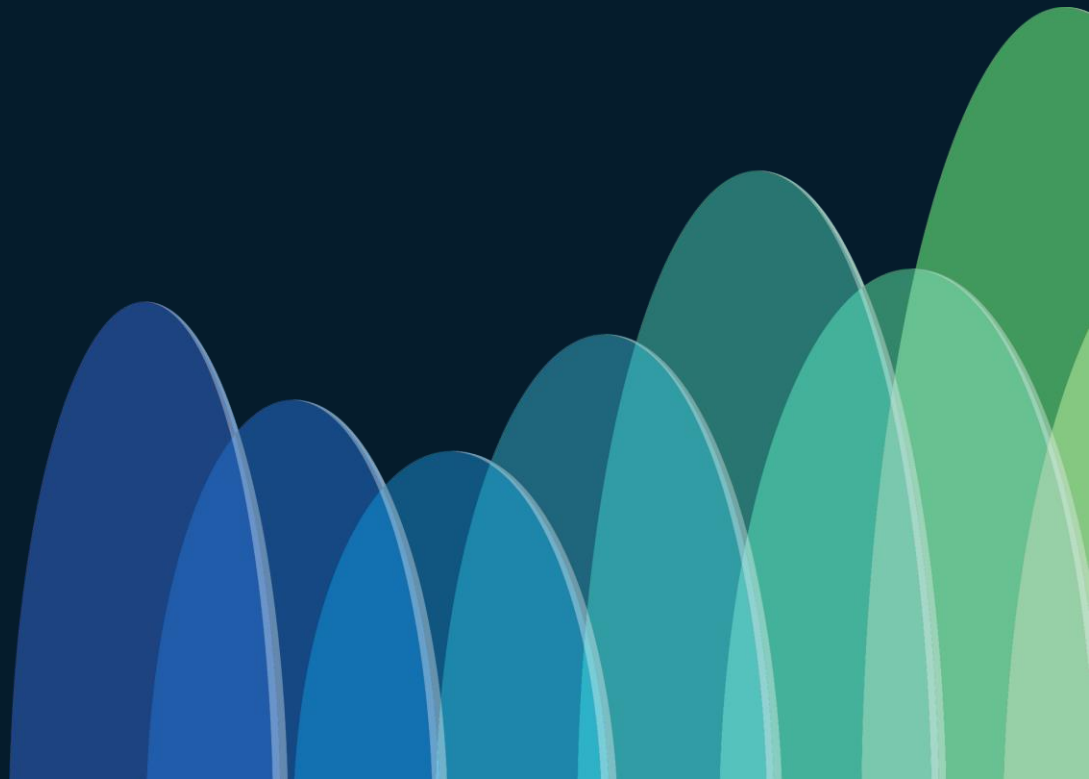
Dashboard



2.3.7.4 Supports "brownfield" 9800 Deployments

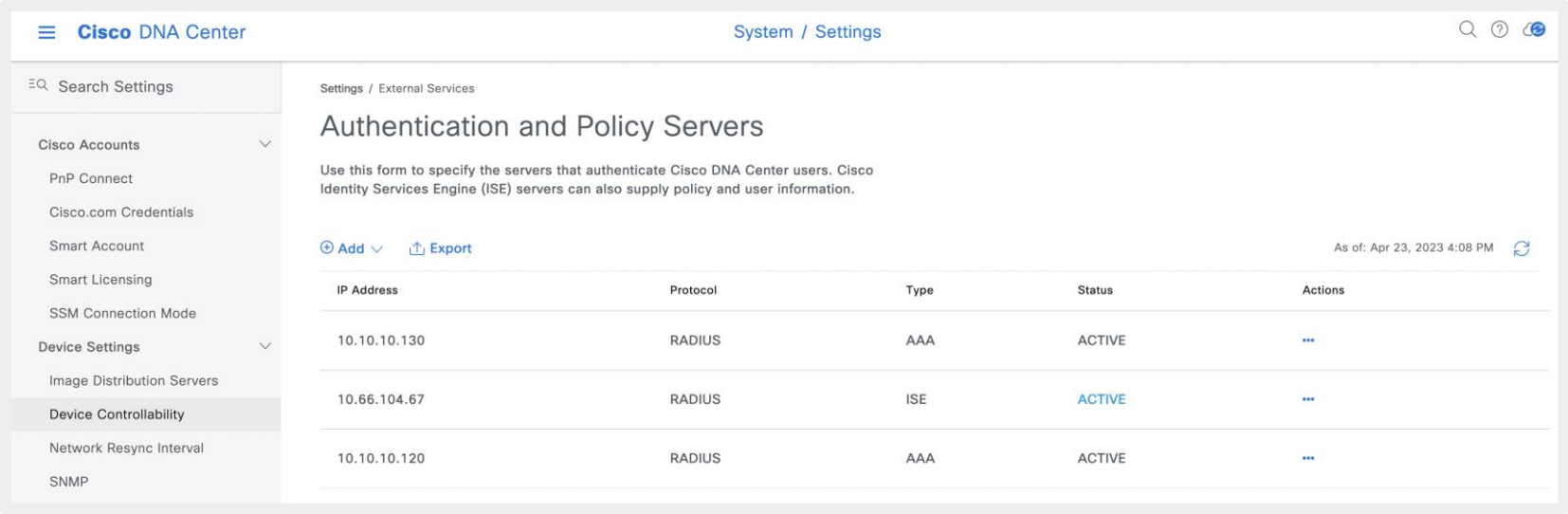


Habit #6 - Secure Devices and Users (AAA & ISE)



cisco Live!

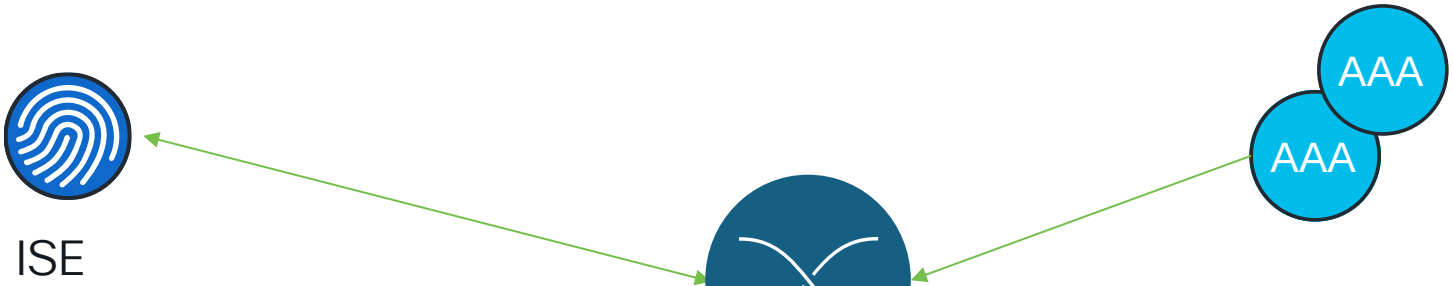
Identity Services Engine



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



- 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

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

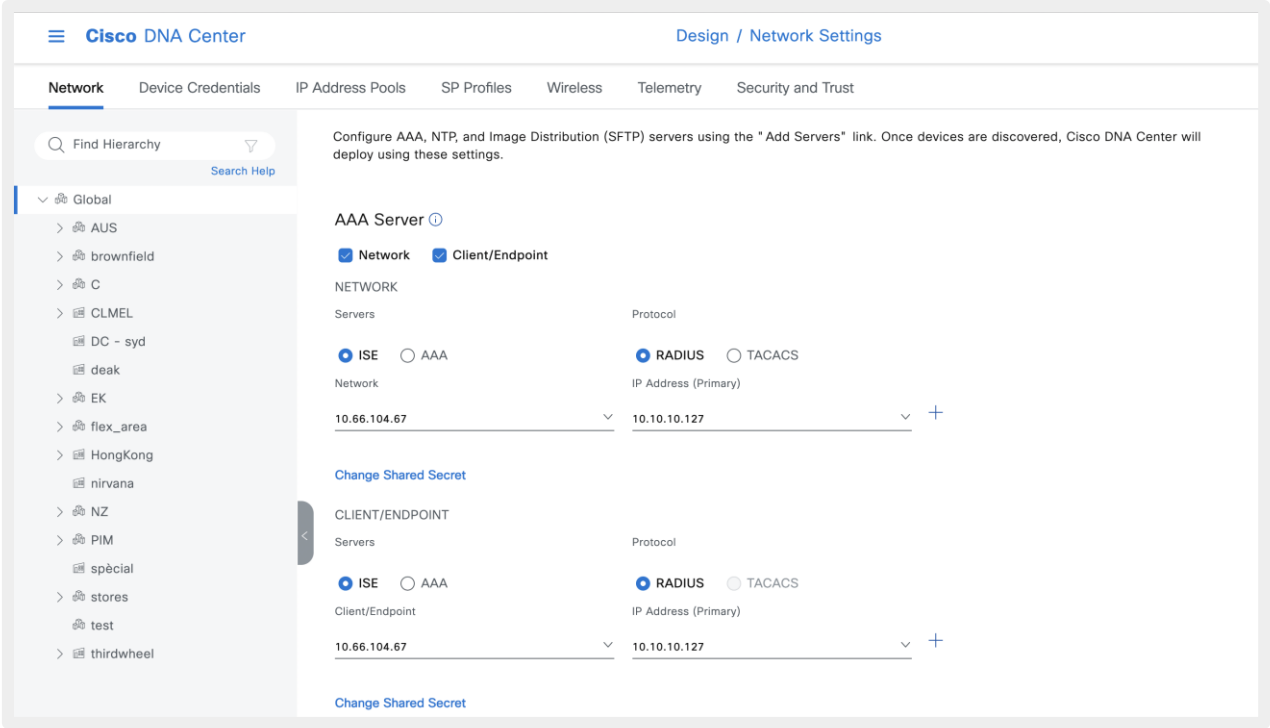
FQDN is required for the integration, not just an IP address (certificate)

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



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
```

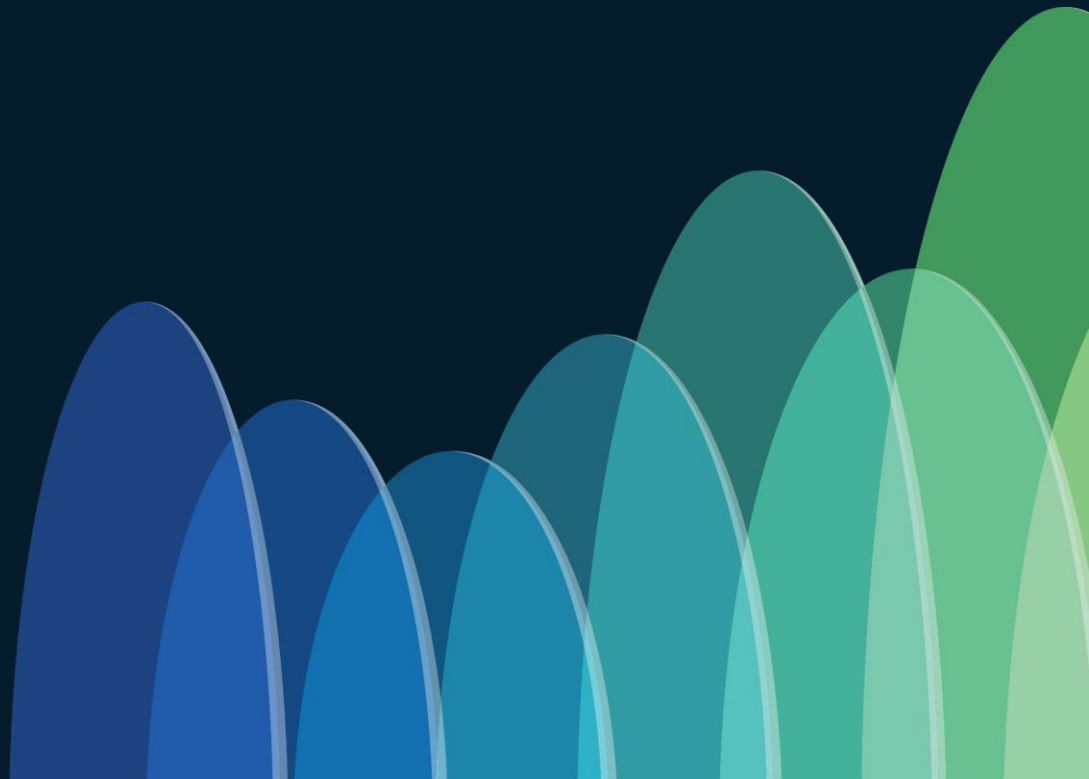
```
authentication radius server dnac-radius_10.10.10.127
 address ipv4 10.10.10.127 auth-port 1812 acct-port 1813
pac key ******
 retransmit 3
 timeout 4
 automate-tester username dummy ignore-acct-port probe-on
 exit
radius-server vsa send authentication
radius-server vsa send accounting
radius-server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

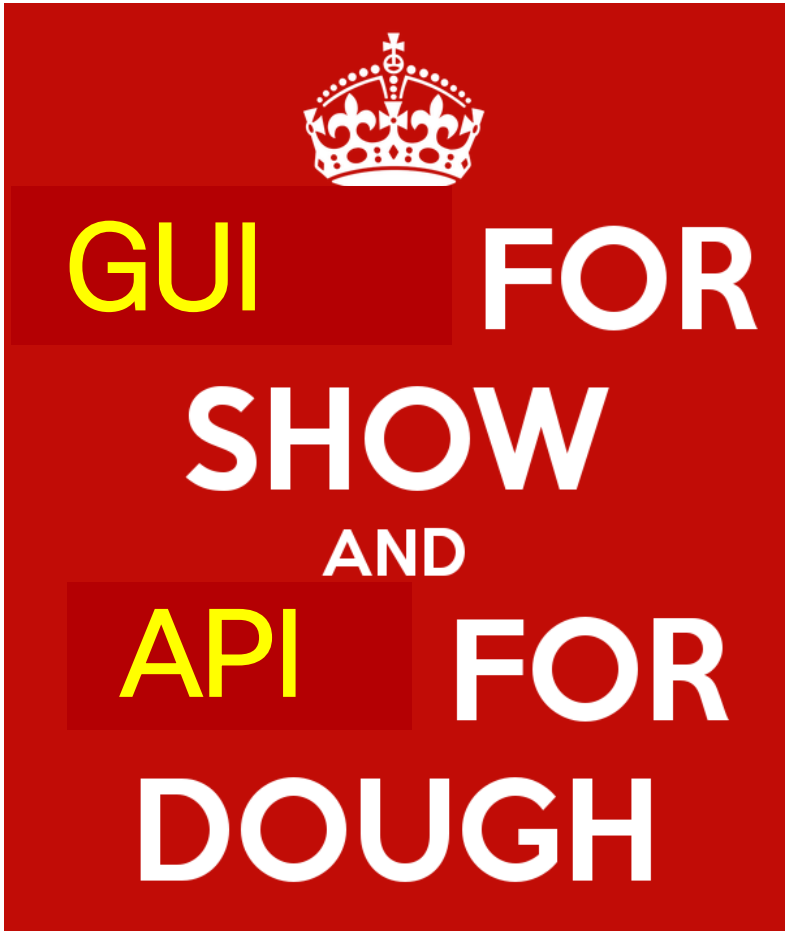
Device has AAA configured	Site has AAA defined	Provisioning Workflow Success
✓	✓	✗
✗	✓	✓
✓	✗	✓
✗	✗	✓

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

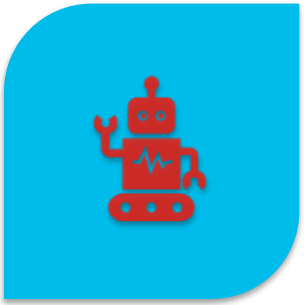
Habit #7 - Up your automation game with APIs and other integrations



cisco Live!



Why API?



AUTOMATION

INTEGRATION

INNOVATION

API First 2.3.7.6 release notes

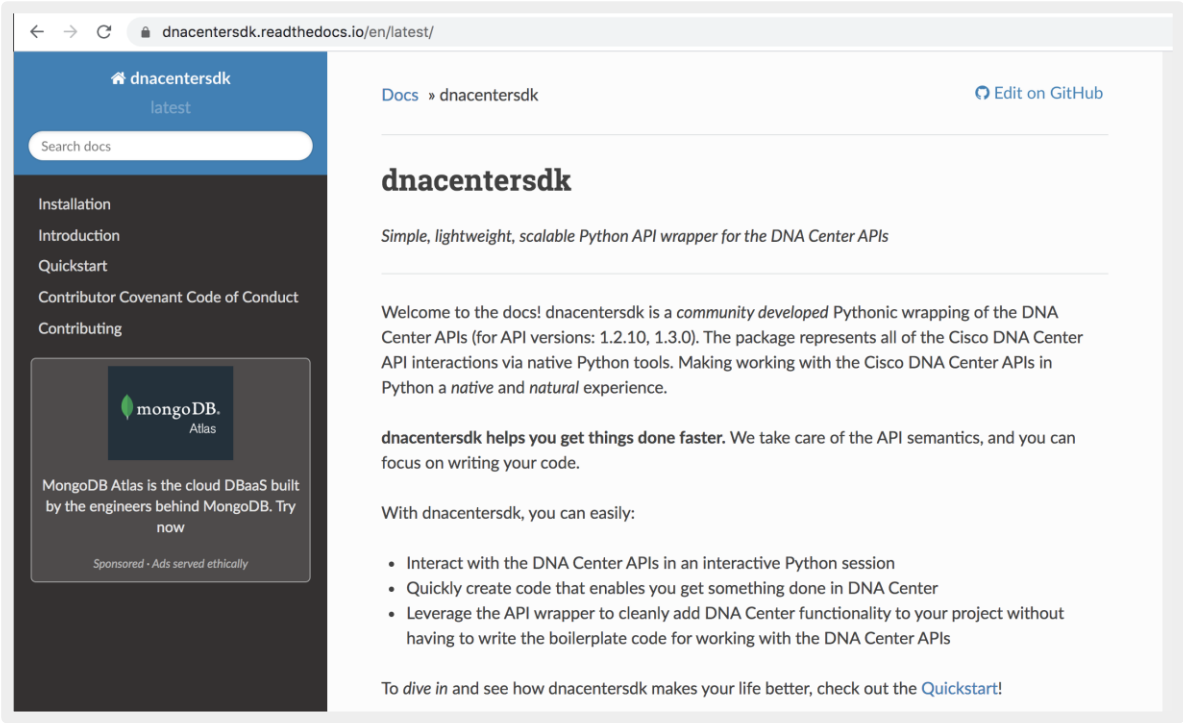
Table 6. New and Changed Features in Catalyst Center Platform, Release 2.3.7.7

Feature	Description
New APIs	
Compliance API	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/${imageId}/productNames/${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/${imageId}/productNames Assign network device product name and sites for the given image identifier. • GET <cluster-ip>/dna/intent/api/v1/siteWiseProductNames/count Get the count of network device product names for the given filters. • DELETE <cluster-ip>/dna/intent/api/v1/images/${imageId}/productNames/${productNameOrdinal} Removes the network device product name from all the sites for the given software image. • PUT <cluster-ip> /dna/intent/api/v1/images/${imageId}/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.

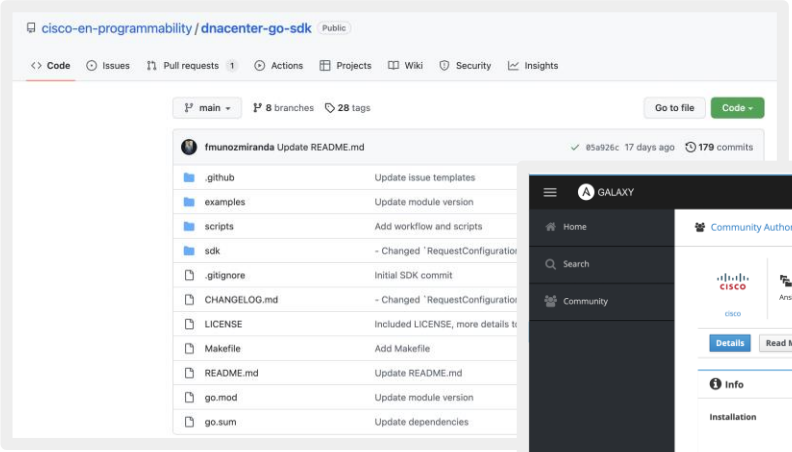
SDK

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

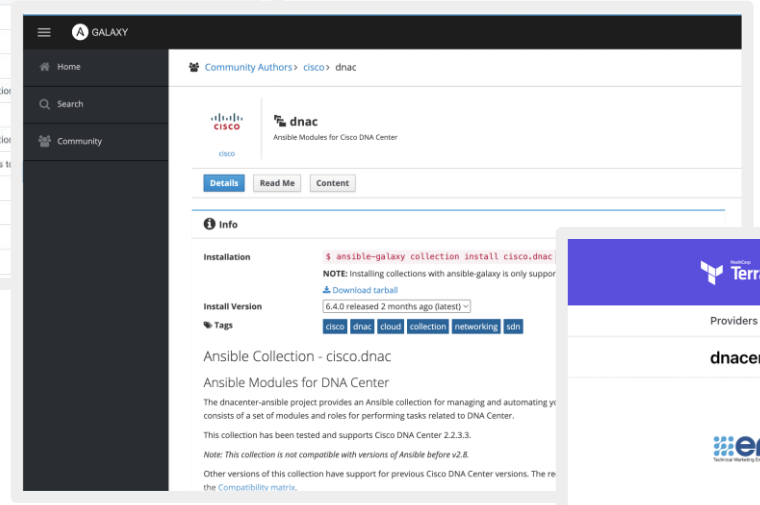


Go/Ansible/Terraform

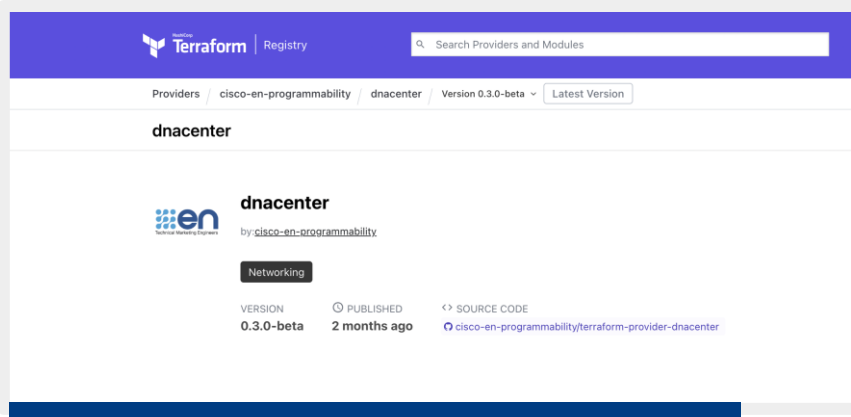
Reference



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



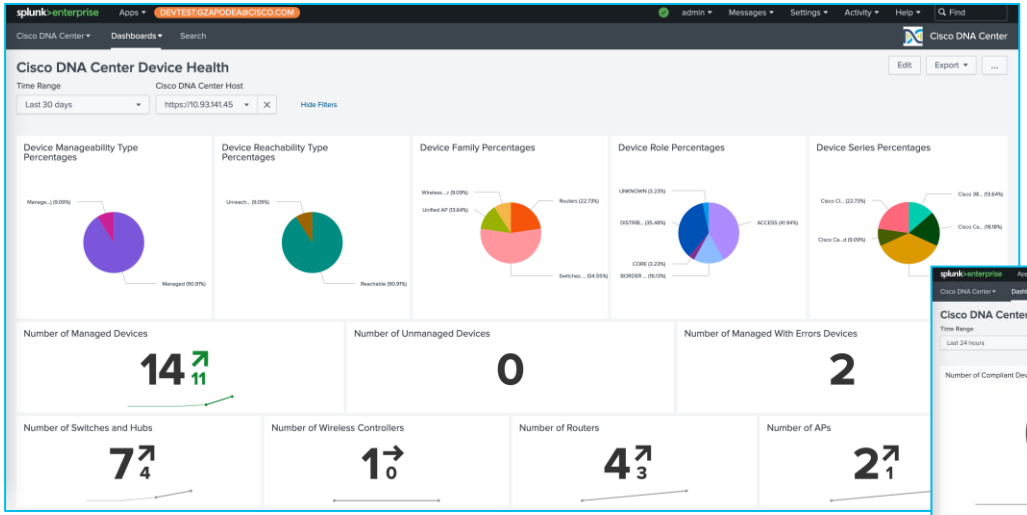
https://galaxy.ansible.com/cisco/dnac

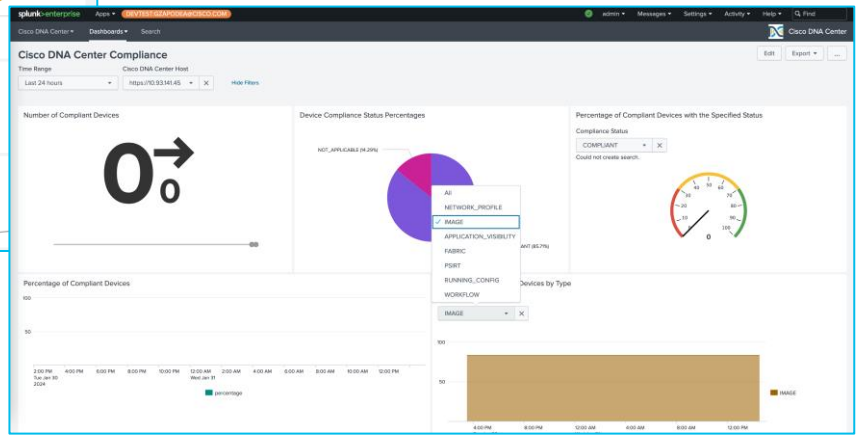


https://registry.terraform.io/providers/cisco-en-programmability/dnacenter/latest

Splunk Integration (existing)

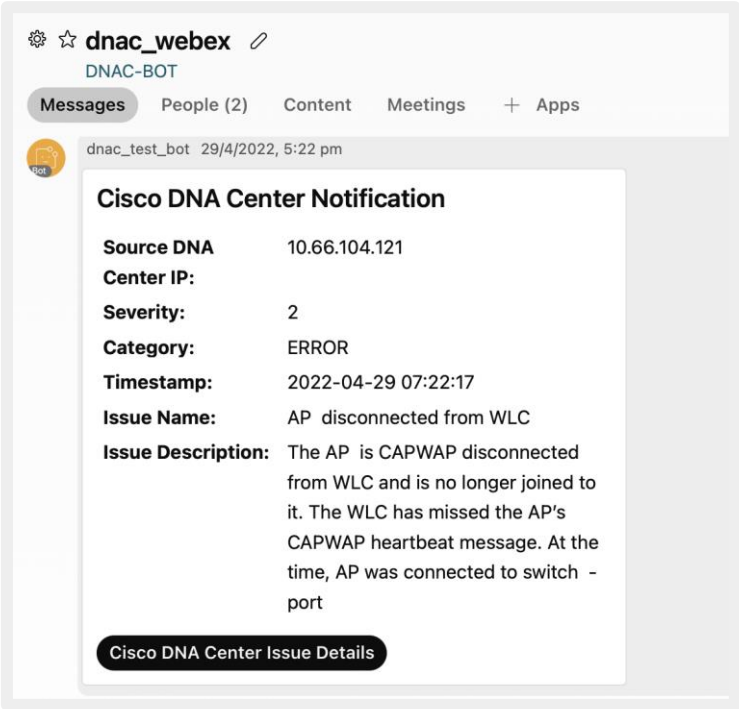
https://github.com/cisco-en-programmability/splunk-apps



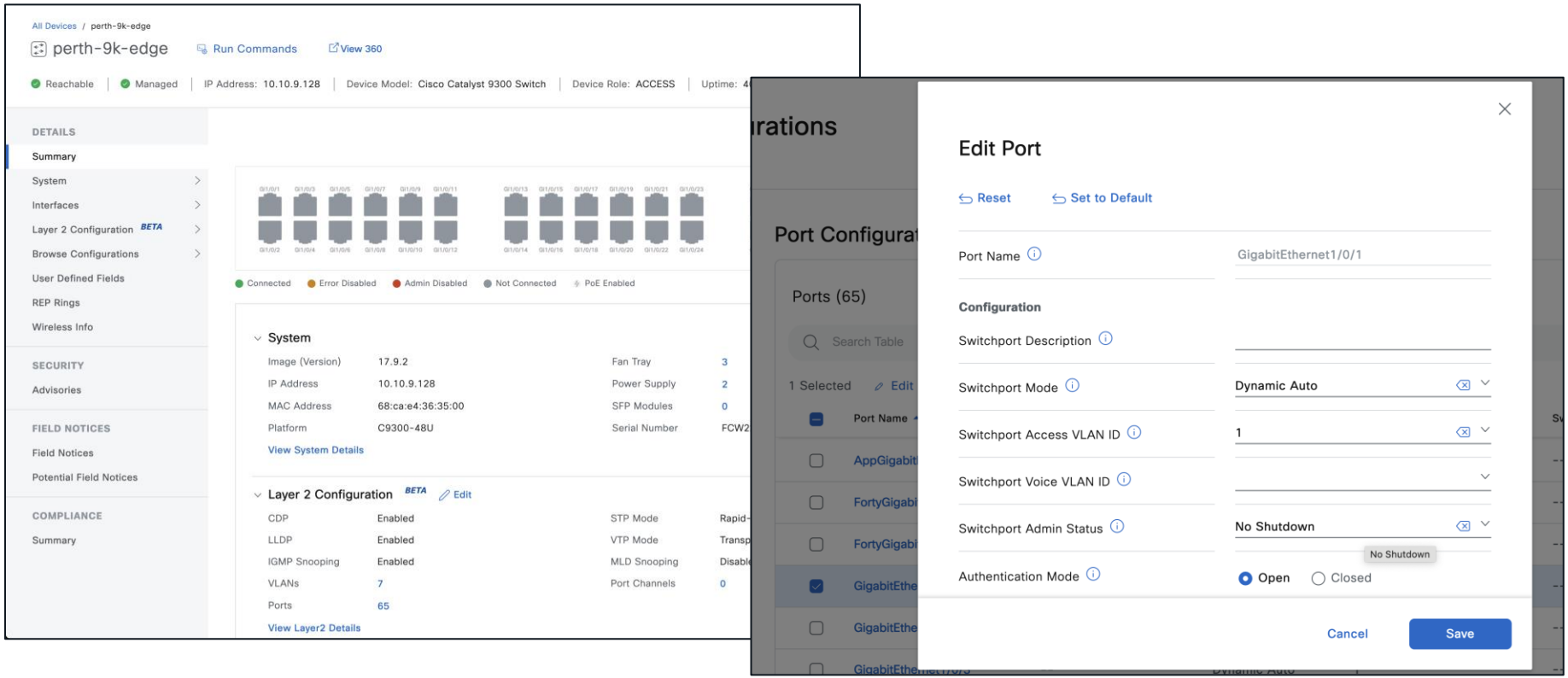


Native Webex Issue Integration

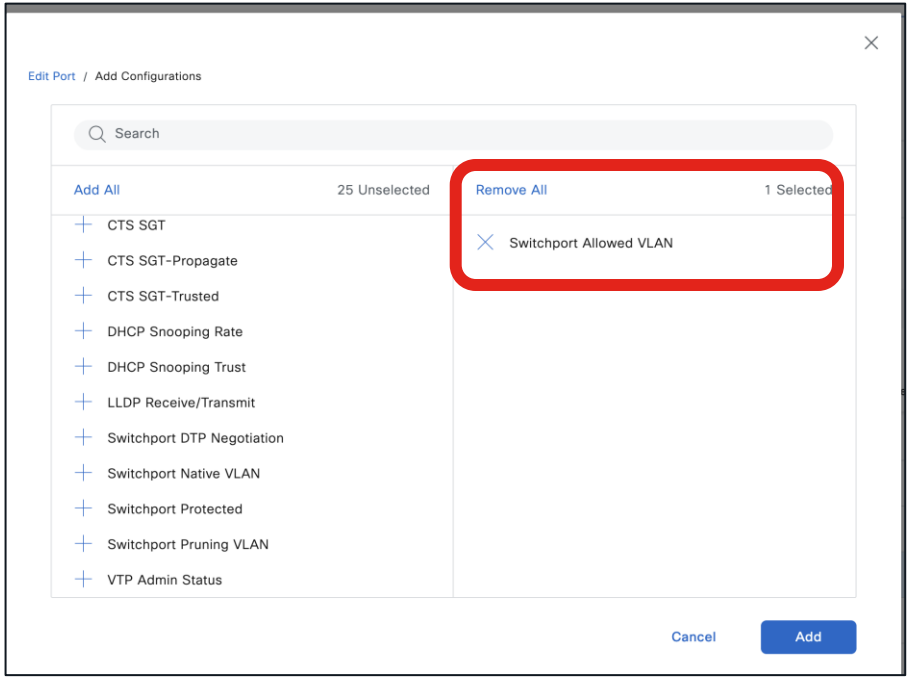
Reference

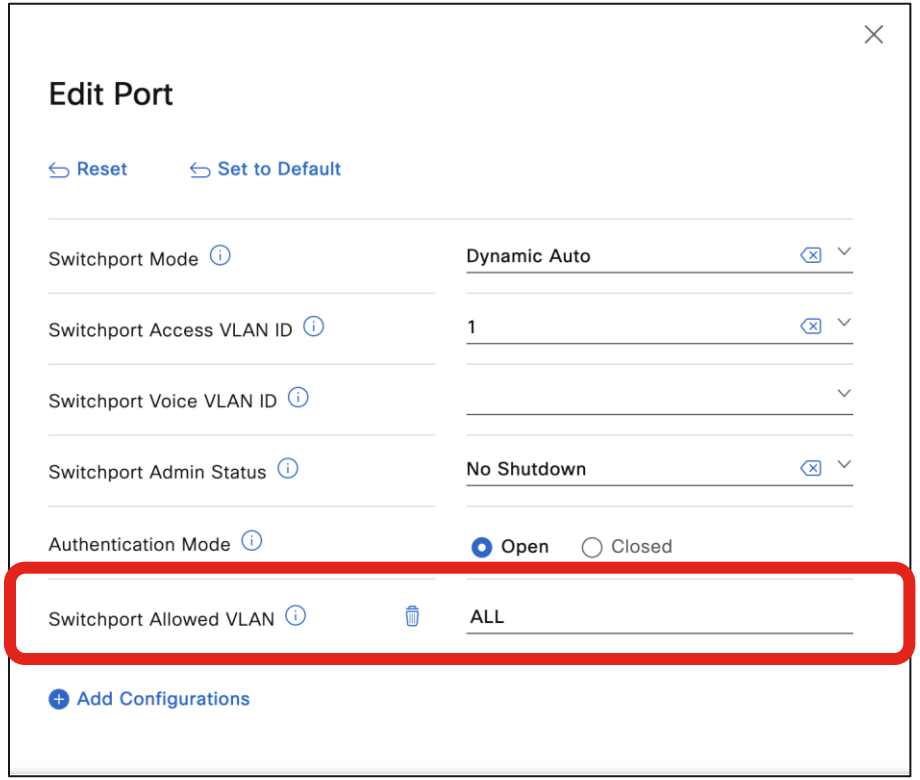


2.3.7.5 – L2 Advanced Port Configuration



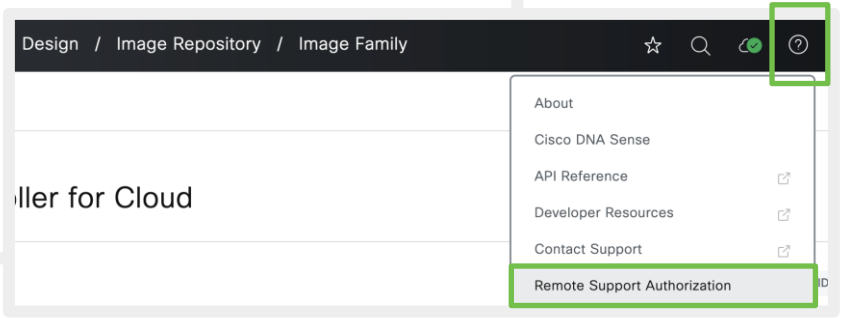
Add extra attributes





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-4wrd-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/2
0230803-081327-10-66-104-121.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

cisco Live!

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

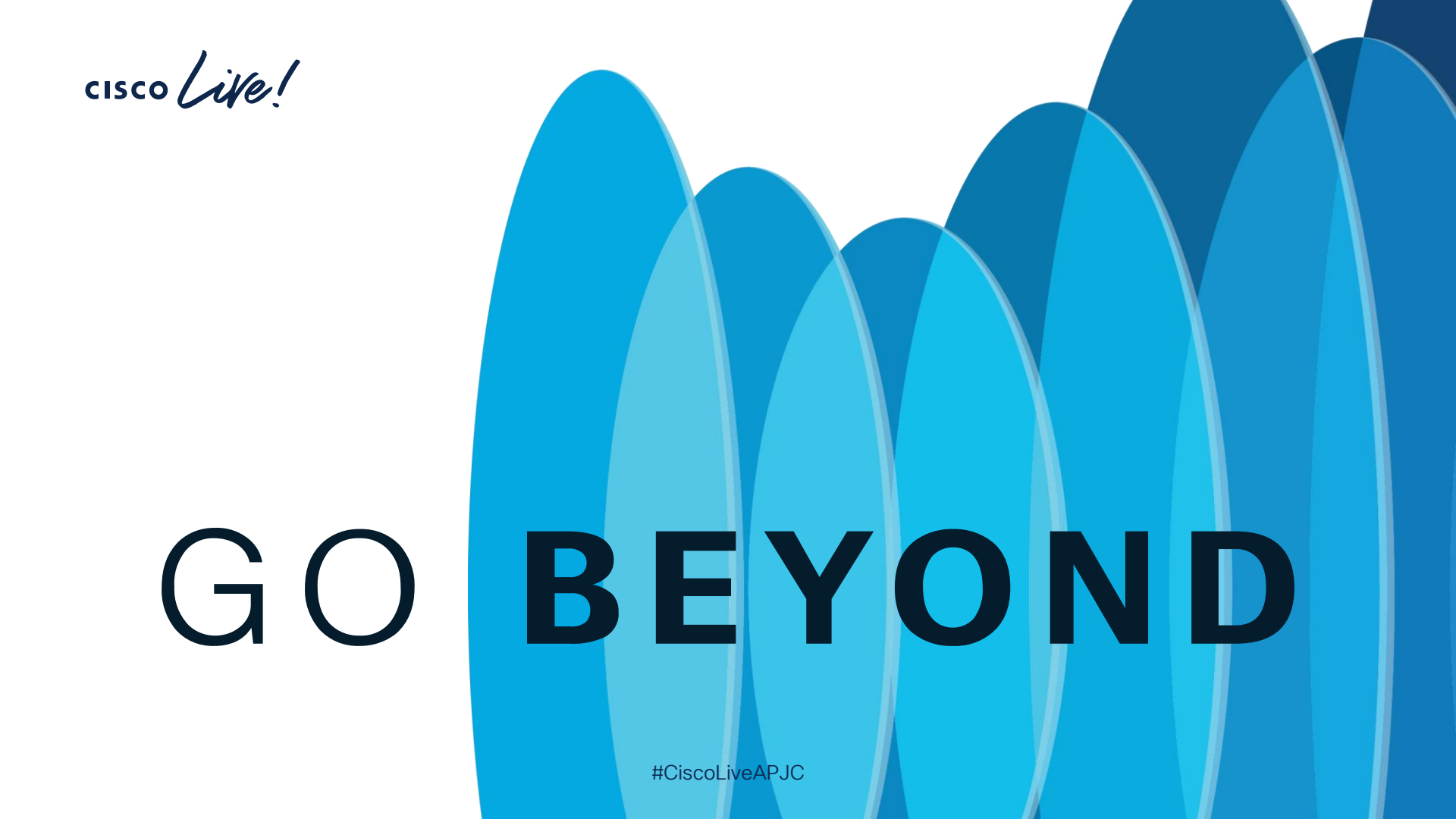
Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

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


cisco
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
GO BEYOND
#CiscoLiveAPJC