cisco Live!

Let’s go

The bridge to possible

7 Habits for success with Cisco Catalyst Center

Adam Radford, Distinguished Solutions Engineer @adamradford123

Lila Rousseaux, Principal Solutions Engineer @lila_rousseaux

Habit ...

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

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

Agenda

Habit #1 - Understanding and embracing Device Controllability

Habit #2 - Find issues before your users with telemetry

Habit #3 - Leverage Compliance and Configuration management

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

Habit #5 - Explore Proactive insights with AI/ML

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

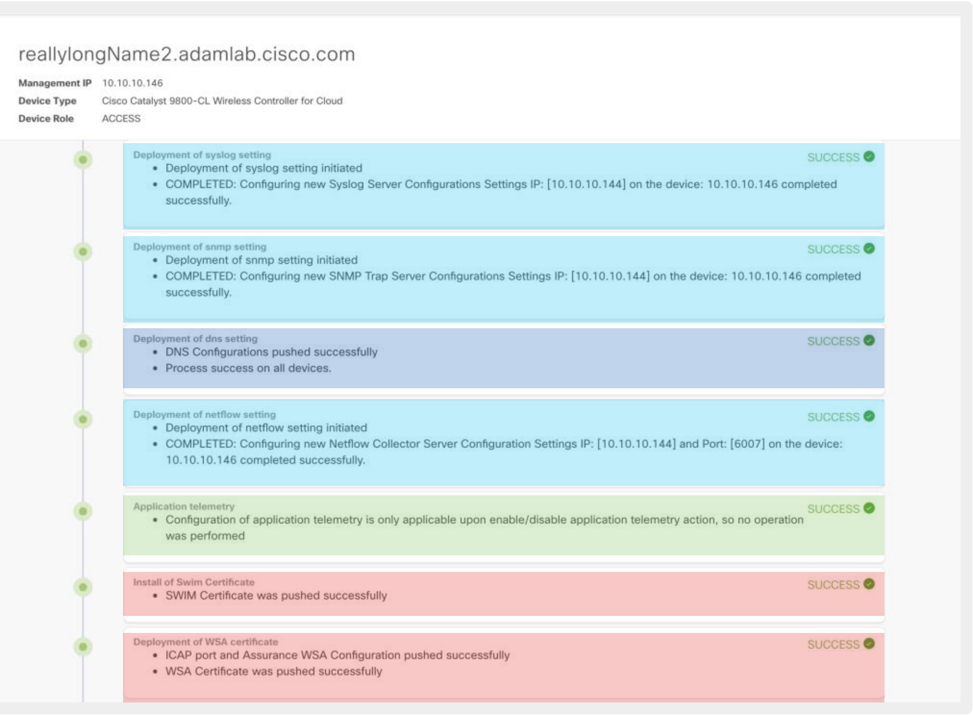
Habit #7 - Up your automation game with APIs and other integrations

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

Habit #1 – Understanding (and embracing) device controllability

Device Controllability

Monitoring | Settings | Telemetry | Trust



reallylongName2.adamlab.cisco.com

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

Deployment of syslog setting — SUCCESS
- Deployment of syslog setting initiated
- COMPLETED: Configuring new Syslog Server Configurations Settings IP: [10.10.10.144] on the device: 10.10.10.146 completed successfully.

Deployment of snmp setting — SUCCESS
- Deployment of snmp setting initiated
- COMPLETED: Configuring new SNMP Trap Server Configurations Settings IP: [10.10.10.144] on the device: 10.10.10.146 completed successfully.

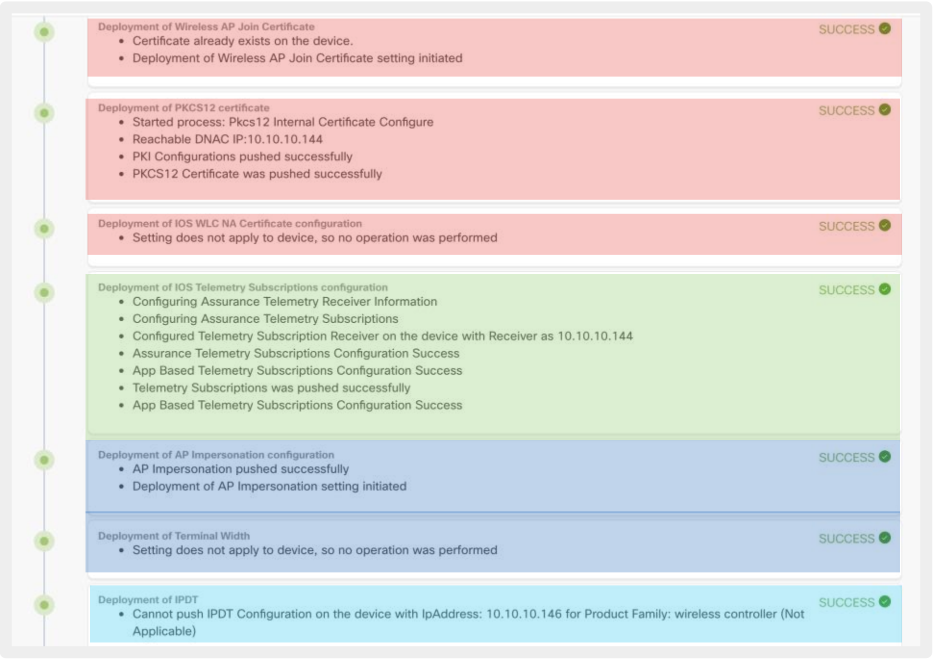
Deployment of dns setting — SUCCESS
- DNS Configurations pushed successfully
- Process success on all devices.

Deployment of netflow setting — SUCCESS
- Deployment of netflow setting initiated
- COMPLETED: Configuring new Netflow Collector Server Configuration Settings IP: [10.10.10.144] and Port: [6007] on the device: 10.10.10.146 completed successfully.

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

Install of Swim Certificate — SUCCESS
- SWIM Certificate was pushed successfully

Deployment of WSA certificate — SUCCESS
- ICAP port and Assurance WSA Configuration pushed successfully
- WSA Certificate was pushed successfully



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

Deployment of PKCS12 certificate — SUCCESS
- Started process: Pkcs12 Internal Certificate Configure
- Reachable DNAC IP:10.10.10.144
- PKI Configurations pushed successfully
- PKCS12 Certificate was pushed successfully

Deployment of IOS WLC NA Certificate configuration — SUCCESS
- Setting does not apply to device, so no operation was performed

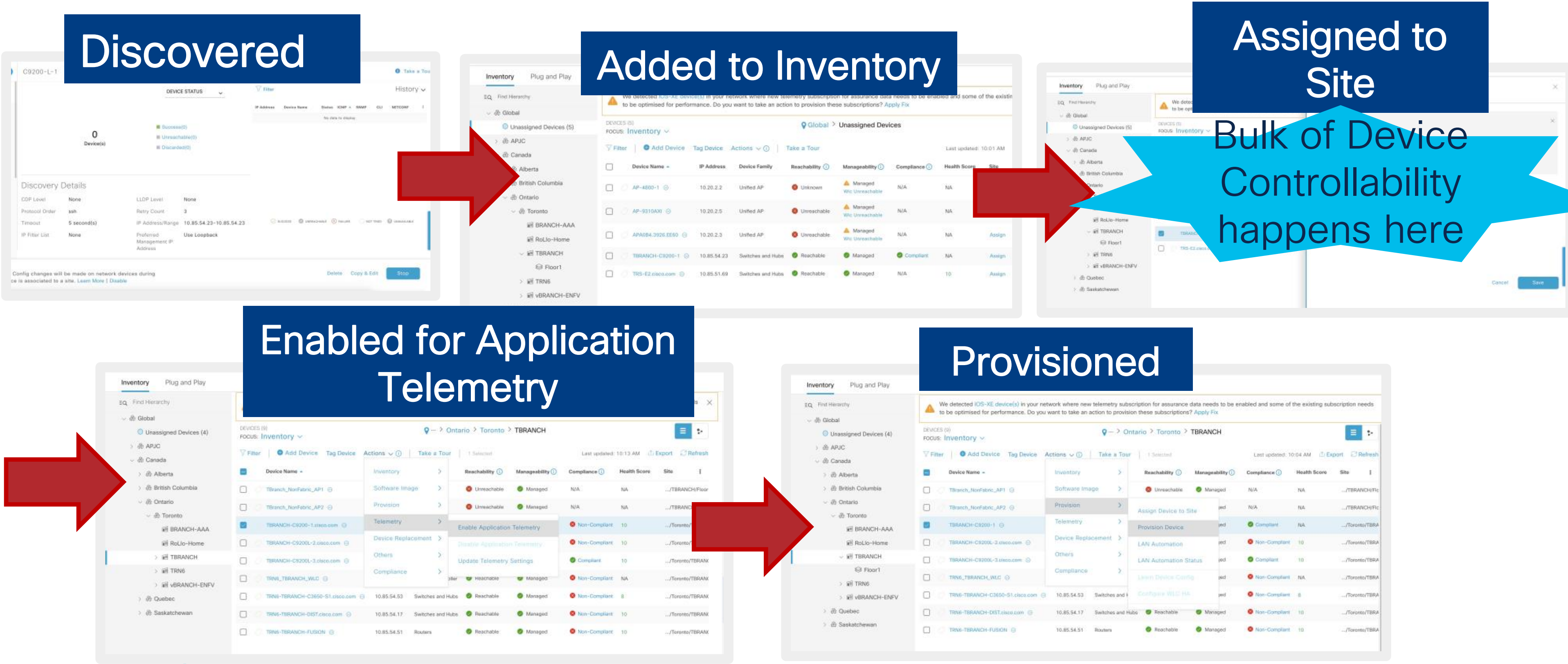
Deployment of IOS Telemetry Subscriptions configuration — SUCCESS
- Configuring Assurance Telemetry Receiver Information
- Configuring Assurance Telemetry Subscriptions
- Configured Telemetry Subscription Receiver on the device with Receiver as 10.10.10.144
- Assurance Telemetry Subscriptions Configuration Success
- App Based Telemetry Subscriptions Configuration Success
- Telemetry Subscriptions was pushed successfully
- App Based Telemetry Subscriptions Configuration Success

Deployment of AP Impersonation configuration — SUCCESS
- AP Impersonation pushed successfully
- Deployment of AP Impersonation setting initiated

Deployment of Terminal Width — SUCCESS
- Setting does not apply to device, so no operation was performed

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

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



Discovered

Added to Inventory

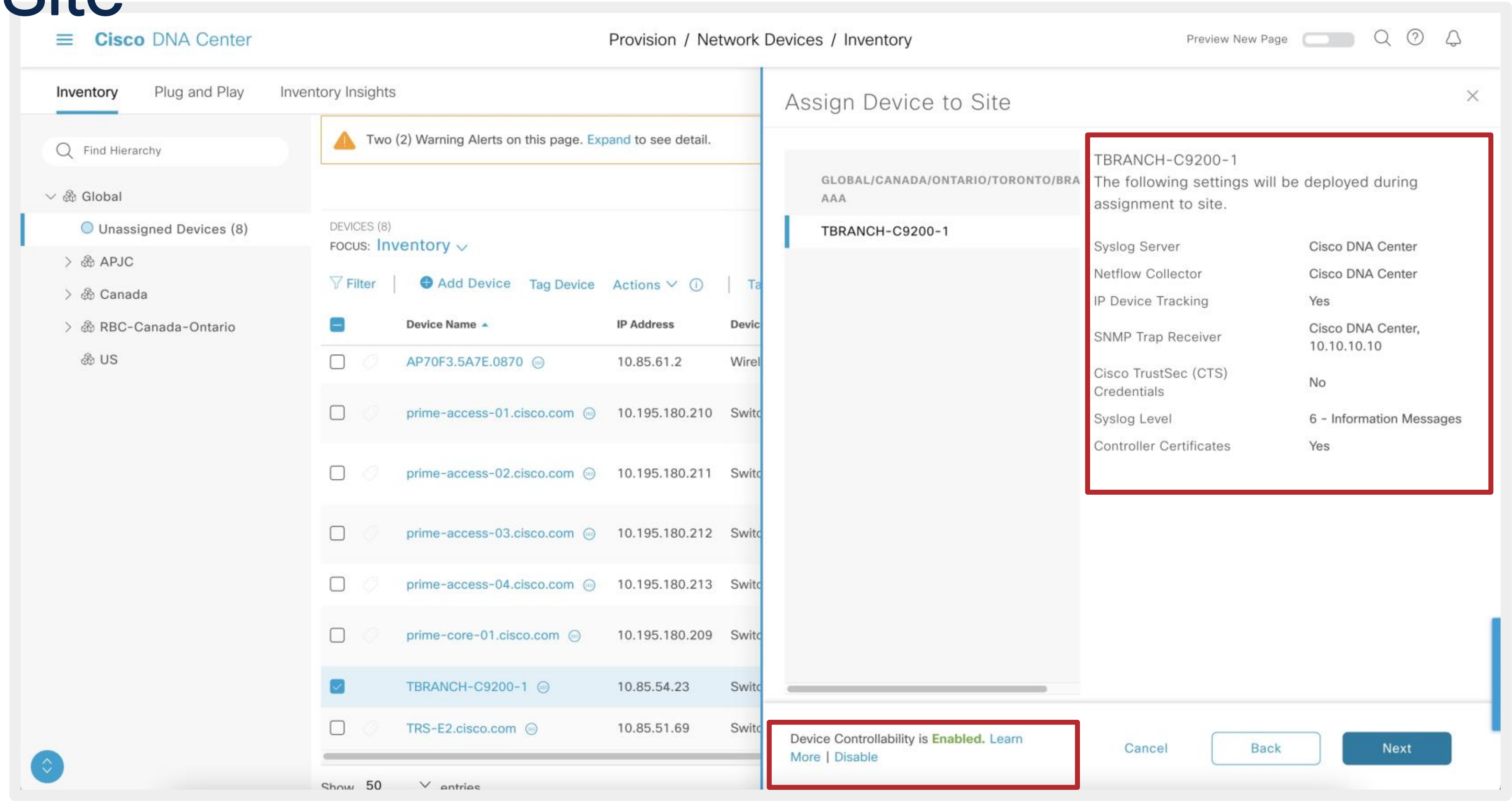
Assigned to Site

Bulk of Device Controllability happens here

Enabled for Application Telemetry

Provisioned

Adding a **switch** to Catalyst Center – **Assign to Site**



Two (2) Warning Alerts on this page. Expand to see detail.

DEVICES (8)
FOCUS: Inventory

☐	Device Name	IP Address	Devic
☐	AP70F3.5A7E.0870	10.85.61.2	Wirel
☐	prime-access-01.cisco.com	10.195.180.210	Switc
☐	prime-access-02.cisco.com	10.195.180.211	Switc
☐	prime-access-03.cisco.com	10.195.180.212	Switc
☐	prime-access-04.cisco.com	10.195.180.213	Switc
☐	prime-core-01.cisco.com	10.195.180.209	Switc
☑	TBRANCH-C9200-1	10.85.54.23	Switc
☐	TRS-E2.cisco.com	10.85.51.69	Switc

Assign Device to Site

GLOBAL/CANADA/ONTARIO/TORONTO/BRA AAA

TBRANCH-C9200-1

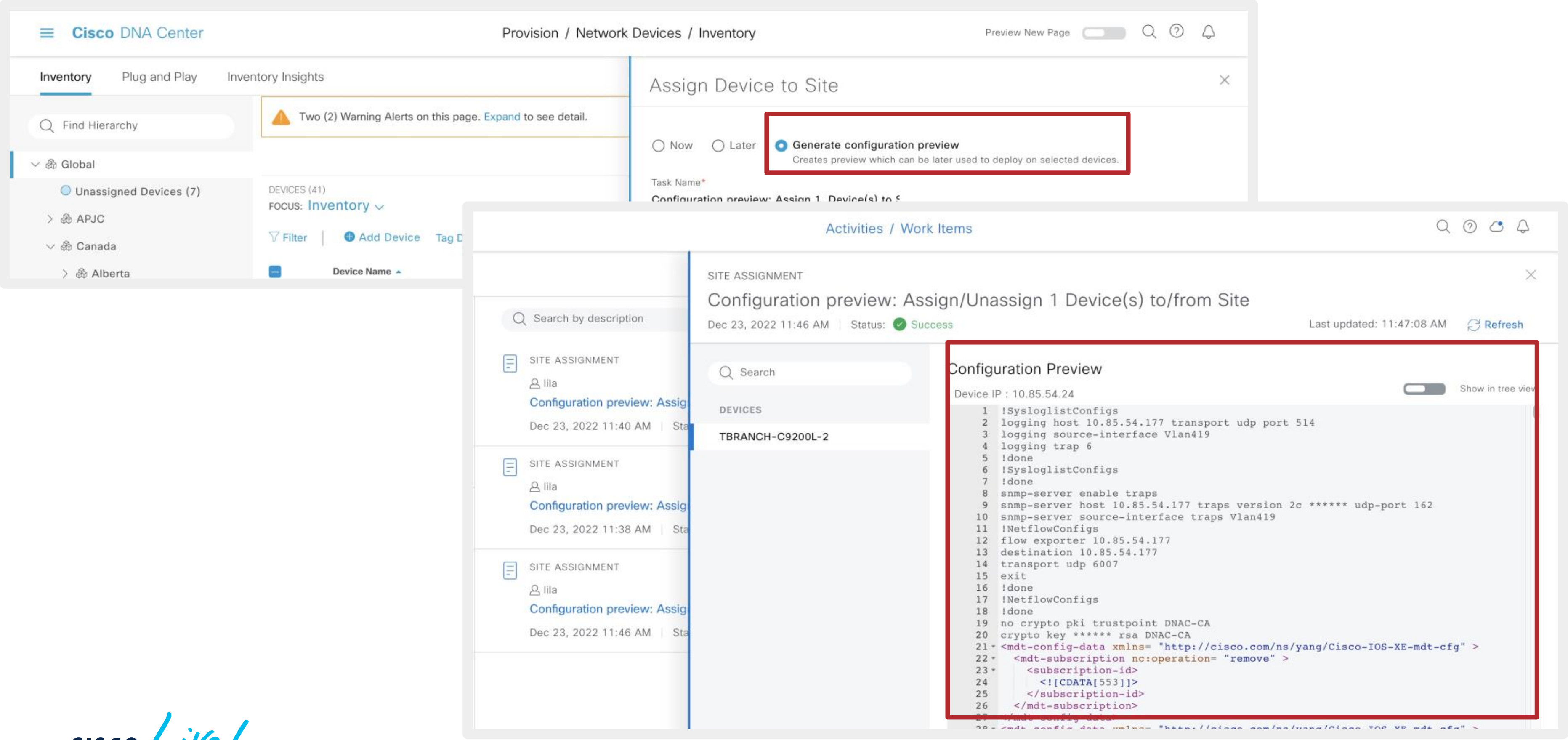
TBRANCH-C9200-1
The following settings will be deployed during assignment to site.

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

Device Controllability is Enabled. Learn More | Disable

Cancel | Back | Next

Adding a **switch** to Catalyst Center – **Assign to Site**



Two (2) Warning Alerts on this page. Expand to see detail.

Assign Device to Site

○ Now ○ Later ● Generate configuration preview
Creates preview which can be later used to deploy on selected devices.

Task Name*
Configuration preview: Assign 1 Device(s) to S

SITE ASSIGNMENT

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

Dec 23, 2022 11:46 AM | Status: ✓ Success

Last updated: 11:47:08 AM

TBRANCH-C9200L-2

Configuration Preview

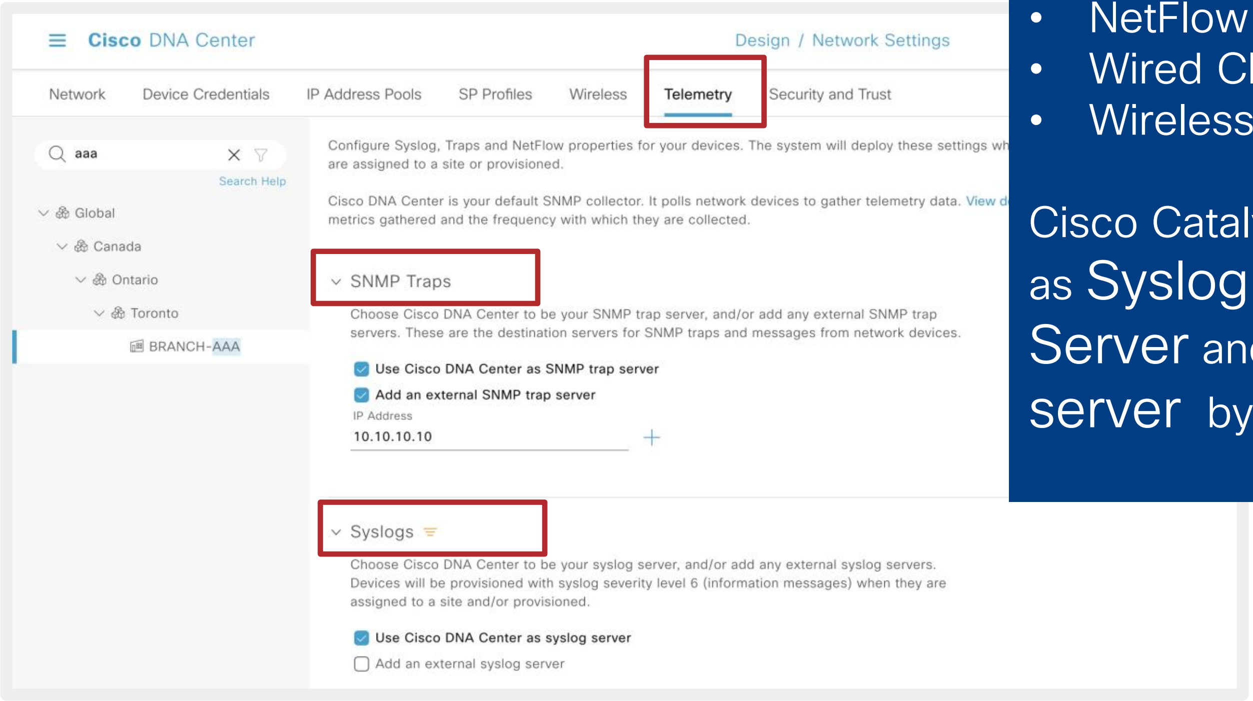
Device IP : 10.85.54.24

```
!SysloglistConfigs
logging host 10.85.54.177 transport udp port 514
logging source-interface Vlan419
logging trap 6
!done
!SysloglistConfigs
!done
snmp-server enable traps
snmp-server host 10.85.54.177 traps version 2c ****** udp-port 162
snmp-server source-interface traps Vlan419
!NetflowConfigs
flow exporter 10.85.54.177
destination 10.85.54.177
transport udp 6007
exit
!done
!NetflowConfigs
!done
no crypto pki trustpoint DNAC-CA
crypto key ****** rsa DNAC-CA
<mdt-config-data xmlns= "http://cisco.com/ns/yang/Cisco-IOS-XE-mdt-cfg" >
  <mdt-subscription nc:operation= "remove" >
    <subscription-id>
      <![CDATA[553]]>
    </subscription-id>
  </mdt-subscription>
</mdt-config-data>
<mdt-config-data xmlns= "http://cisco.com/ns/yang/Cisco-IOS-XE-mdt-cfg" >
```

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

Device Controllability

Site-level customization



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

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

SNMP Traps

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

☑ Use Cisco DNA Center as SNMP trap server

☑ Add an external SNMP trap server

IP Address

10.10.10.10

Syslogs

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

☑ Use Cisco DNA Center as syslog server

□ Add an external syslog server

Telemetry Configuration:

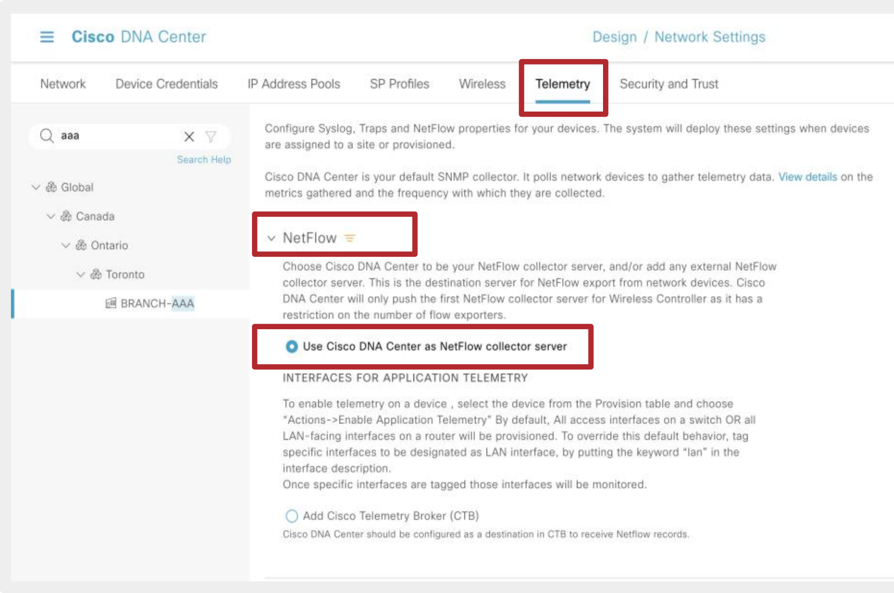
- SYSLOG Server
- SNMP Trap Server
- SNMP Polling
- NetFlow
- Wired Client Data Collection
- Wireless Telemetry

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

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

Device Controllability

Site-level customization



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

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

NetFlow

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

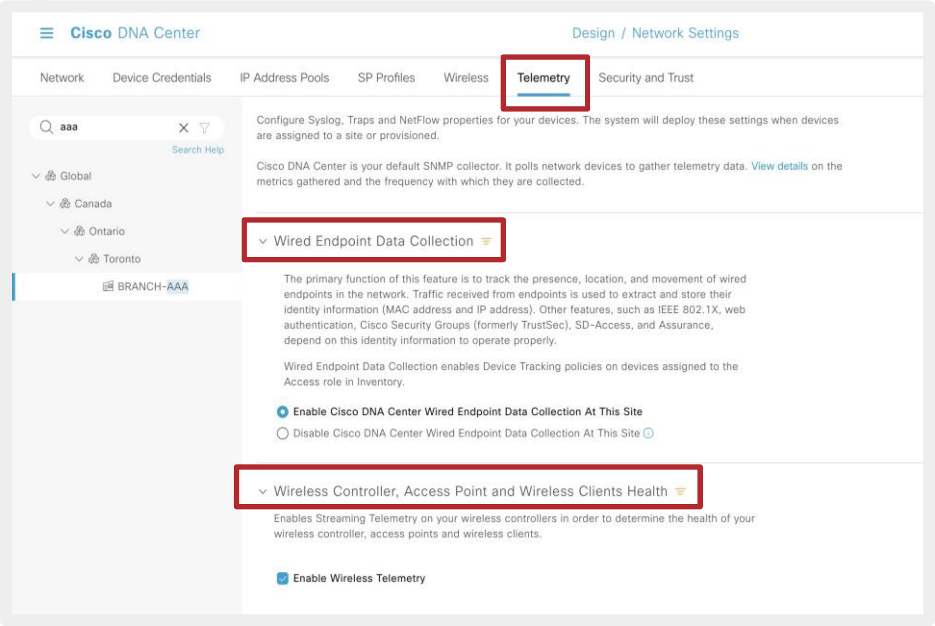
● Use Cisco DNA Center as NetFlow collector server

INTERFACES FOR APPLICATION TELEMETRY

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

○ Add Cisco Telemetry Broker (CTB)

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



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

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

Wired Endpoint Data Collection

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

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

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

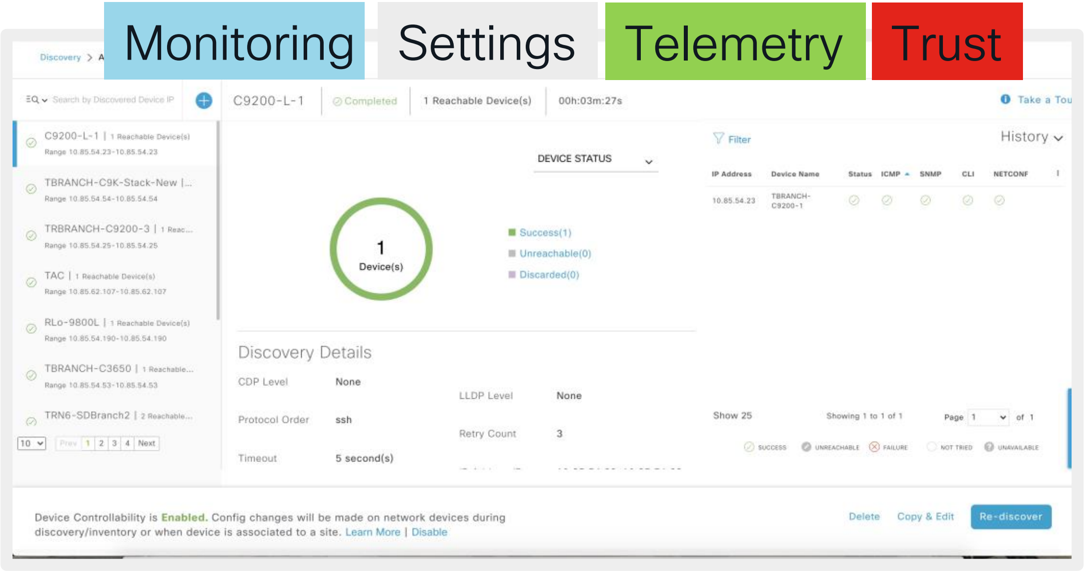
○ Disable Cisco DNA Center Wired Endpoint Data Collection At This Site

Wireless Controller, Access Point and Wireless Clients Health

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

☑ Enable Wireless Telemetry

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



Monitoring Settings Telemetry Trust

C9200-L-1 | Completed | 1 Reachable Device(s) | 00h:03m:27s

- C9200-L-1 | 1 Reachable Device(s)
  Range 10.85.54.23-10.85.54.23
- TBRANCH-C9K-Stack-New |...
  Range 10.85.54.54-10.85.54.54
- TRBRANCH-C9200-3 | 1 Reac...
  Range 10.85.54.25-10.85.54.25
- TAC | 1 Reachable Device(s)
  Range 10.85.62.107-10.85.62.107
- RLo-9800L | 1 Reachable Device(s)
  Range 10.85.54.190-10.85.54.190
- TBRANCH-C3650 | 1 Reachable...
  Range 10.85.54.53-10.85.54.53
- TRN6-SDBranch2 | 2 Reachable...

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

Show 25 Showing 1 to 1 of 1 Page 1 of 1

Discovery Details

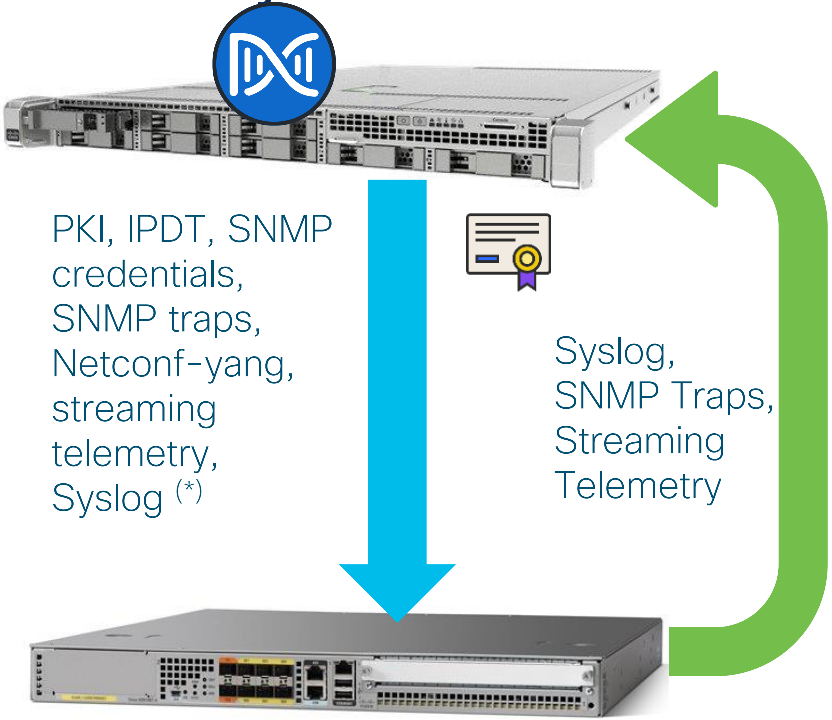
CDP Level: None
LLDP Level: None
Protocol Order: ssh
Retry Count: 3
Timeout: 5 second(s)

Device Controllability is **Enabled**. Config changes will be made on network devices during discovery/inventory or when device is associated to a site. Learn More | Disable

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

Habit #2 – Find issues before your users with telemetry

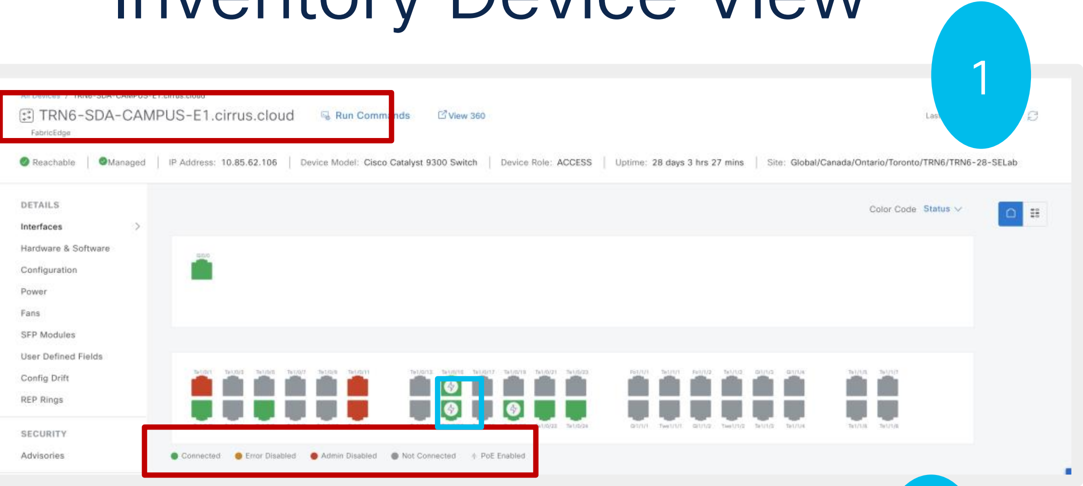
Benefits of Telemetry data captured via Catalyst Center


PKI, IPDT, SNMP credentials, SNMP traps, Netconf-yang, streaming telemetry, Syslog (*)
Syslog, SNMP Traps, Streaming Telemetry

- 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

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

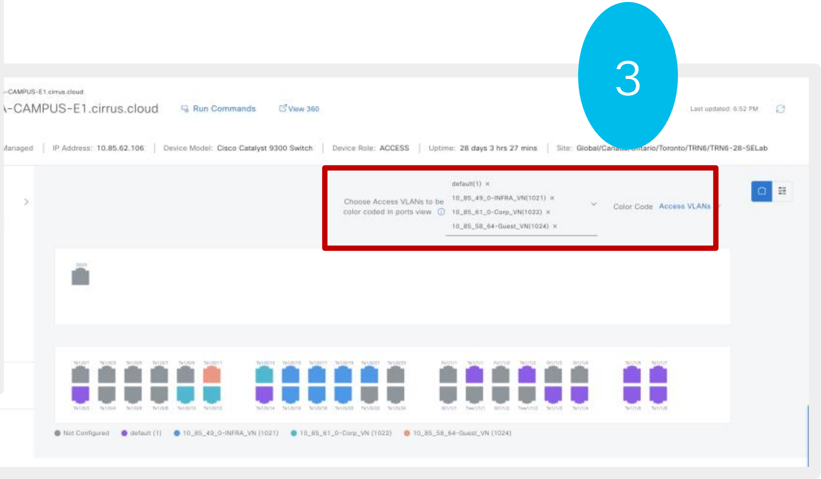
Inventory Device View



TRN6-SDA-CAMPUS-E1.cirrus.cloud

FabricEdge

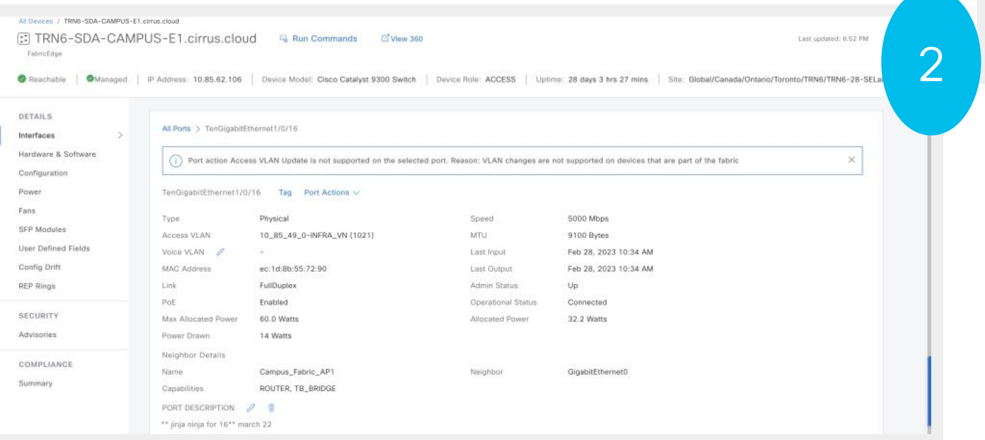
Reachable | Managed | IP Address: 10.85.62.106 | Device Model: Cisco Catalyst 9300 Switch | Device Role: ACCESS | Uptime: 28 days 3 hrs 27 mins | Site: Global/Canada/Ontario/Toronto/TRN6/TRN6-28-SELab



-CAMPUS-E1.cirrus.cloud

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

Choose Access VLANs to be color coded in ports view: default(1) ×, 10_85_49_0-INFRA_VN(1021) ×, 10_85_61_0-Corp_VN(1022) ×, 10_85_58_64-Guest_VN(1024) ×



TRN6-SDA-CAMPUS-E1.cirrus.cloud

FabricEdge

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-SELa

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

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

Neighbor Details

Name	Campus_Fabric_AP1	Neighbor	GigabitEthernet0
Capabilities	ROUTER, TB_BRIDGE		

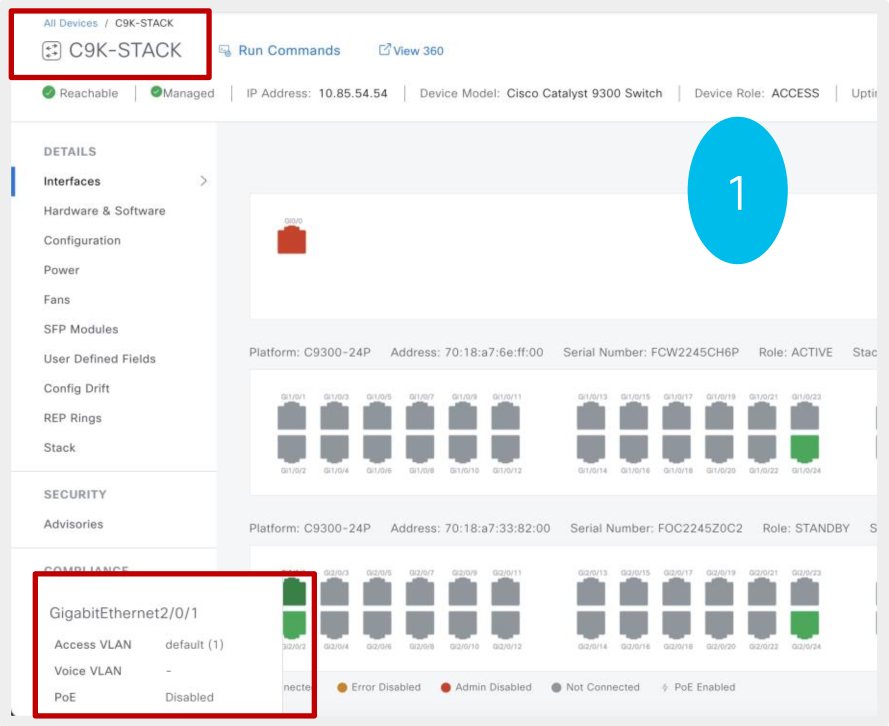
PORT DESCRIPTION

** jinja ninja for 16** march 22

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

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

Inventory Device - Port Configuration



All Devices / C9K-STACK

C9K-STACK   Run Commands   View 360

Reachable | Managed | IP Address: 10.85.54.54 | Device Model: Cisco Catalyst 9300 Switch | Device Role: ACCESS | Uptir

DETAILS
- Interfaces
- Hardware & Software
- Configuration
- Power
- Fans
- SFP Modules
- User Defined Fields
- Config Drift
- REP Rings
- Stack

SECURITY
- Advisories

COMPLIANCE

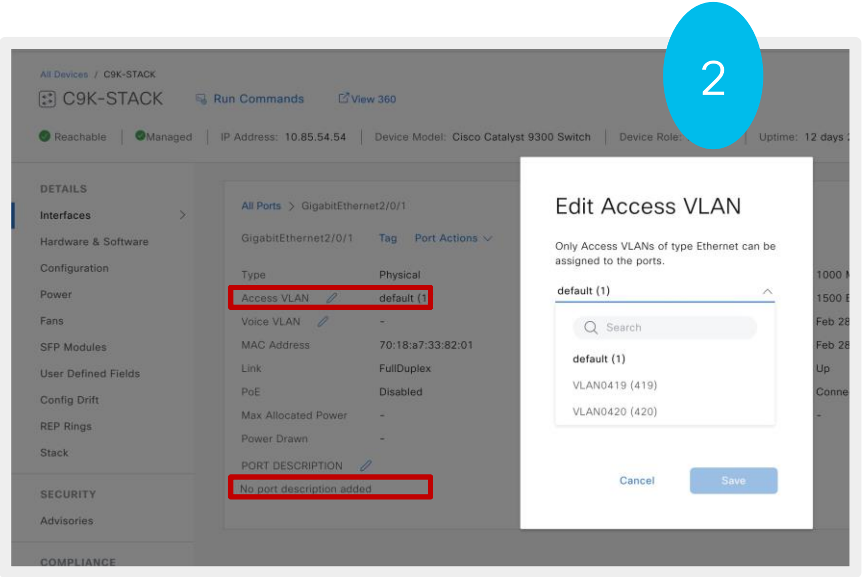
Platform: C9300-24P   Address: 70:18:a7:6e:ff:00   Serial Number: FCW2245CH6P   Role: ACTIVE   Stac

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

GigabitEthernet2/0/1

Access VLAN	default (1)
Voice VLAN	-
PoE	Disabled

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



All Devices / C9K-STACK

C9K-STACK   Run Commands   View 360

Reachable | Managed | IP Address: 10.85.54.54 | Device Model: Cisco Catalyst 9300 Switch | Device Role: | Uptime: 12 days

DETAILS
- Interfaces
- Hardware & Software
- Configuration
- Power
- Fans
- SFP Modules
- User Defined Fields
- Config Drift
- REP Rings
- Stack

SECURITY
- Advisories

COMPLIANCE

All Ports > GigabitEthernet2/0/1

GigabitEthernet2/0/1   Tag   Port Actions

Type	Physical
Access VLAN	default (1
Voice VLAN	-
MAC Address	70:18:a7:33:82:01
Link	FullDuplex
PoE	Disabled
Max Allocated Power	-
Power Drawn	-

PORT DESCRIPTION

No port description added

1000 M
1500 E
Feb 28
Feb 28
Up
Conne
-

Edit Access VLAN

Only Access VLANs of type Ethernet can be assigned to the ports.

default (1)

Search

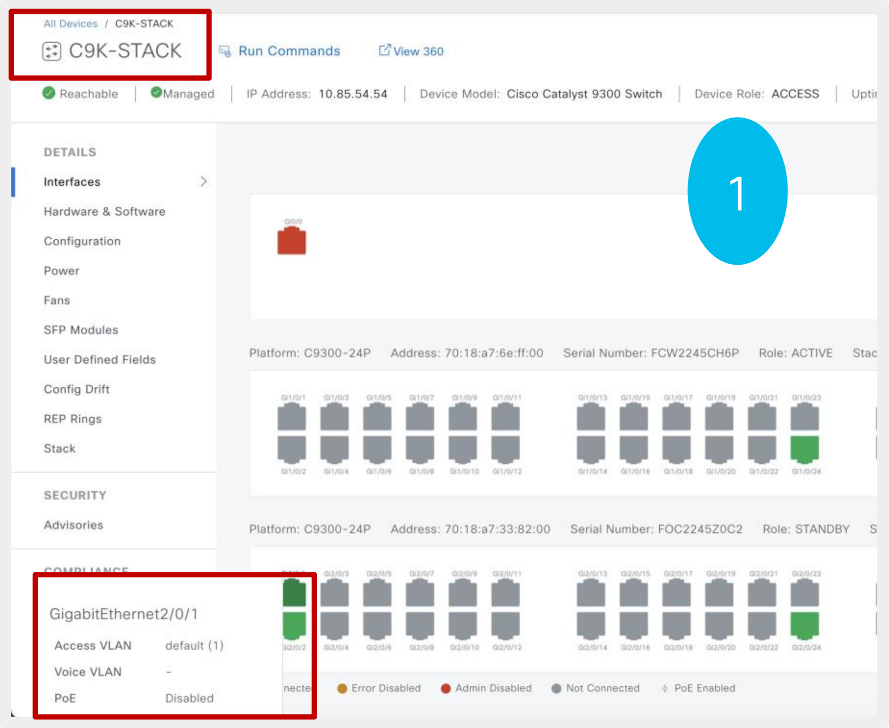
- default (1)
- VLAN0419 (419)
- VLAN0420 (420)

Cancel   Save

Change port **VLAN** and **description**

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

Inventory Device - Port Actions



All Devices / C9K-STACK

C9K-STACK   Run Commands   View 360

Reachable | Managed | IP Address: 10.85.54.54 | Device Model: Cisco Catalyst 9300 Switch | Device Role: ACCESS | Upti

DETAILS

- Interfaces
- Hardware & Software
- Configuration
- Power
- Fans
- SFP Modules
- User Defined Fields
- Config Drift
- REP Rings
- Stack

SECURITY

- Advisories

COMPLIANCE

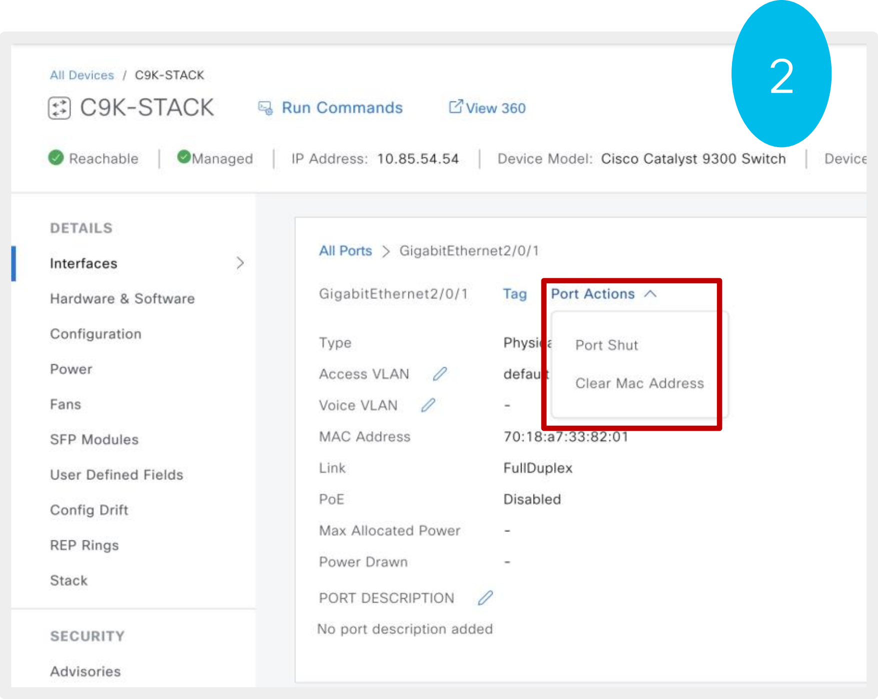
Platform: C9300-24P   Address: 70:18:a7:6e:ff:00   Serial Number: FCW2245CH6P   Role: ACTIVE   Stac

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

GigabitEthernet2/0/1

Access VLAN	default (1)
Voice VLAN	-
PoE	Disabled

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



All Devices / C9K-STACK

C9K-STACK   Run Commands   View 360

Reachable | Managed | IP Address: 10.85.54.54 | Device Model: Cisco Catalyst 9300 Switch | Device

DETAILS

- Interfaces
- Hardware & Software
- Configuration
- Power
- Fans
- SFP Modules
- User Defined Fields
- Config Drift
- REP Rings
- Stack

SECURITY

- Advisories

All Ports > GigabitEthernet2/0/1

GigabitEthernet2/0/1   Tag   Port Actions

- Port Shut
- Clear Mac Address

Type	Physica
Access VLAN	defau
Voice VLAN	-
MAC Address	70:18:a7:33:82:01
Link	FullDuplex
PoE	Disabled
Max Allocated Power	-
Power Drawn	-

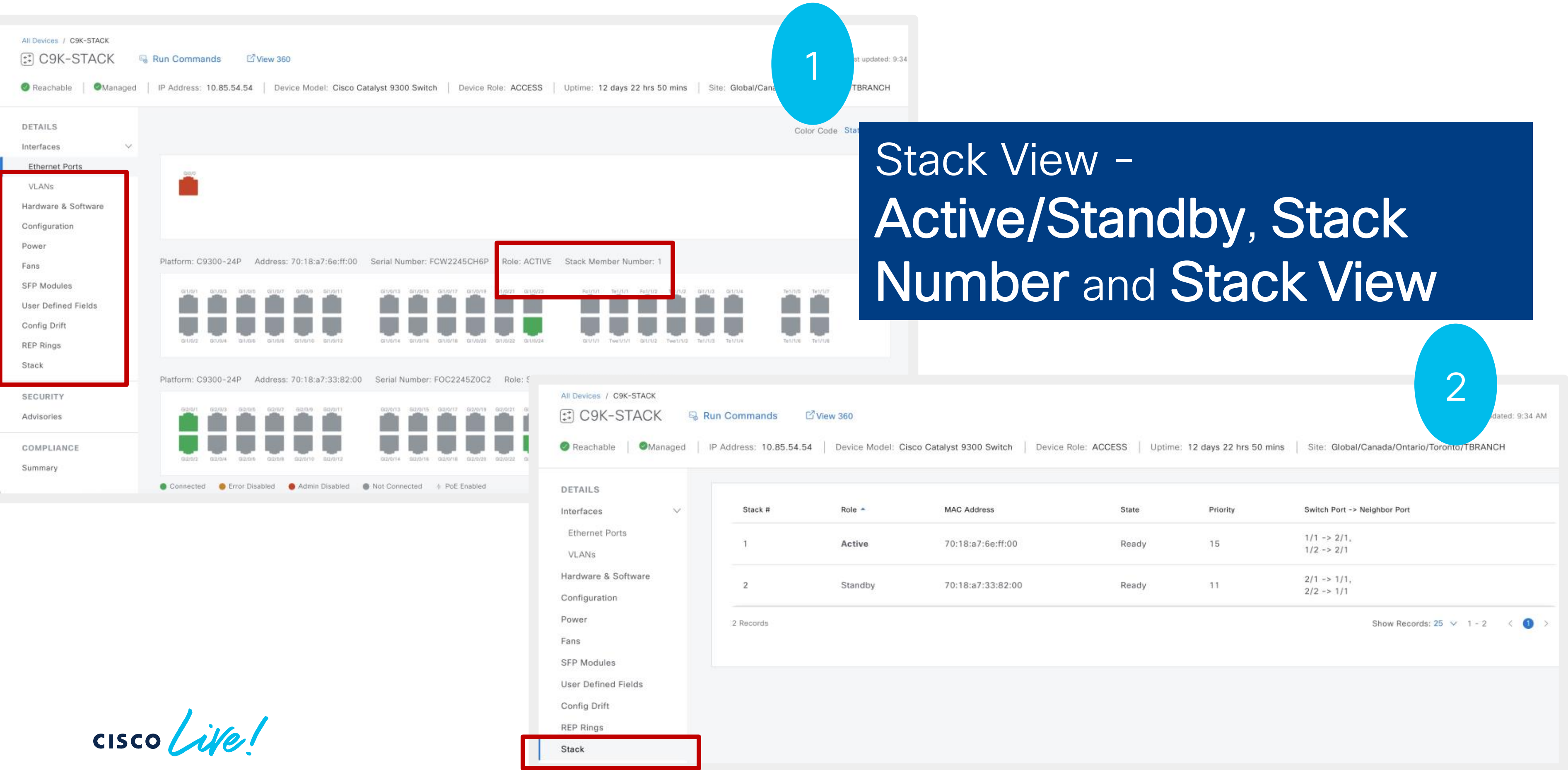
PORT DESCRIPTION

No port description added

Quickly and easily shut down a port or Clear Mac Table

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

Inventory Device - Stack



All Devices / C9K-STACK

C9K-STACK   Run Commands   View 360   ...st updated: 9:34

Reachable | Managed | IP Address: 10.85.54.54 | Device Model: Cisco Catalyst 9300 Switch | Device Role: ACCESS | Uptime: 12 days 22 hrs 50 mins | Site: Global/Cana... ...TBRANCH

Color Code   Stat...

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

Platform: C9300-24P   Address: 70:18:a7:33:82:00   Serial Number: FOC2245Z0C2   Role: S...

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

All Devices / C9K-STACK

C9K-STACK   Run Commands   View 360   ...dated: 9:34 AM

Reachable | Managed | IP Address: 10.85.54.54 | Device Model: Cisco Catalyst 9300 Switch | Device Role: ACCESS | Uptime: 12 days 22 hrs 50 mins | Site: Global/Canada/Ontario/Toronto/TBRANCH

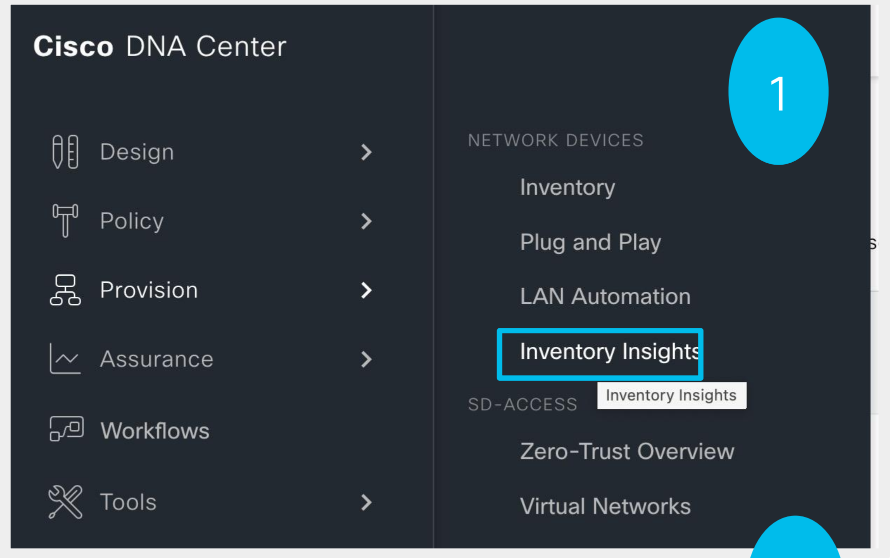
Stack #	Role ▲	MAC Address	State	Priority	Switch Port -> Neighbor Port
1	**Active**	70:18:a7:6e:ff:00	Ready	15	1/1 -> 2/1, 1/2 -> 2/1
2	Standby	70:18:a7:33:82:00	Ready	11	2/1 -> 1/1, 2/2 -> 1/1

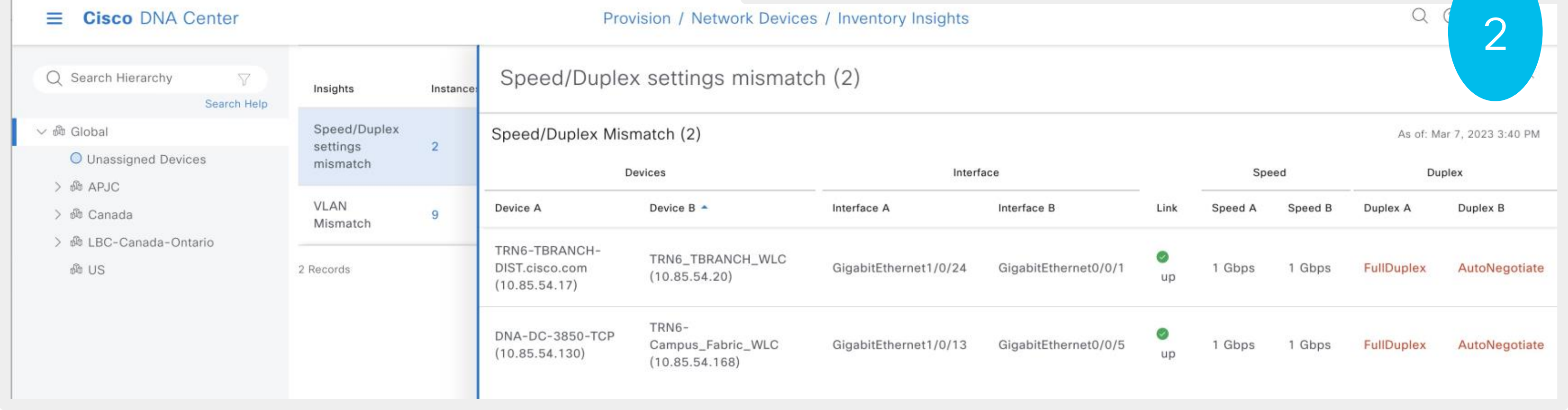
2 Records   Show Records: 25   1 - 2   ‹ 1 ›

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

Inventory Insights

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





Insights	Instances
Speed/Duplex settings mismatch	2
VLAN Mismatch	9

2 Records

Speed/Duplex settings mismatch (2)

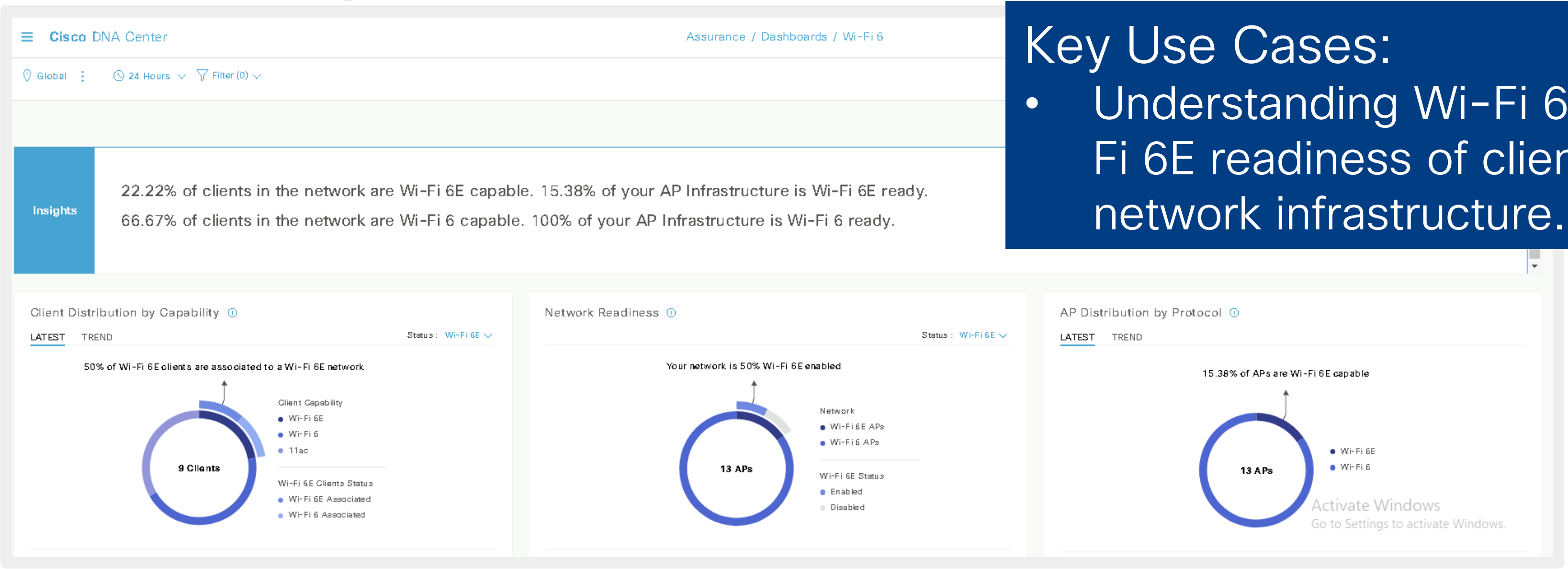
Speed/Duplex Mismatch (2)

As of: Mar 7, 2023 3:40 PM

Devices		Interface			Speed		Duplex	
Device A	Device B ▲	Interface A	Interface B	Link	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

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

Wi-Fi 6/6E Readiness Dashboard



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

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

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

Your network is 50% Wi-Fi 6E enabled

15.38% of APs are Wi-Fi 6E capable

Activate Windows
Go to Settings to activate Windows.

Key Use Cases:

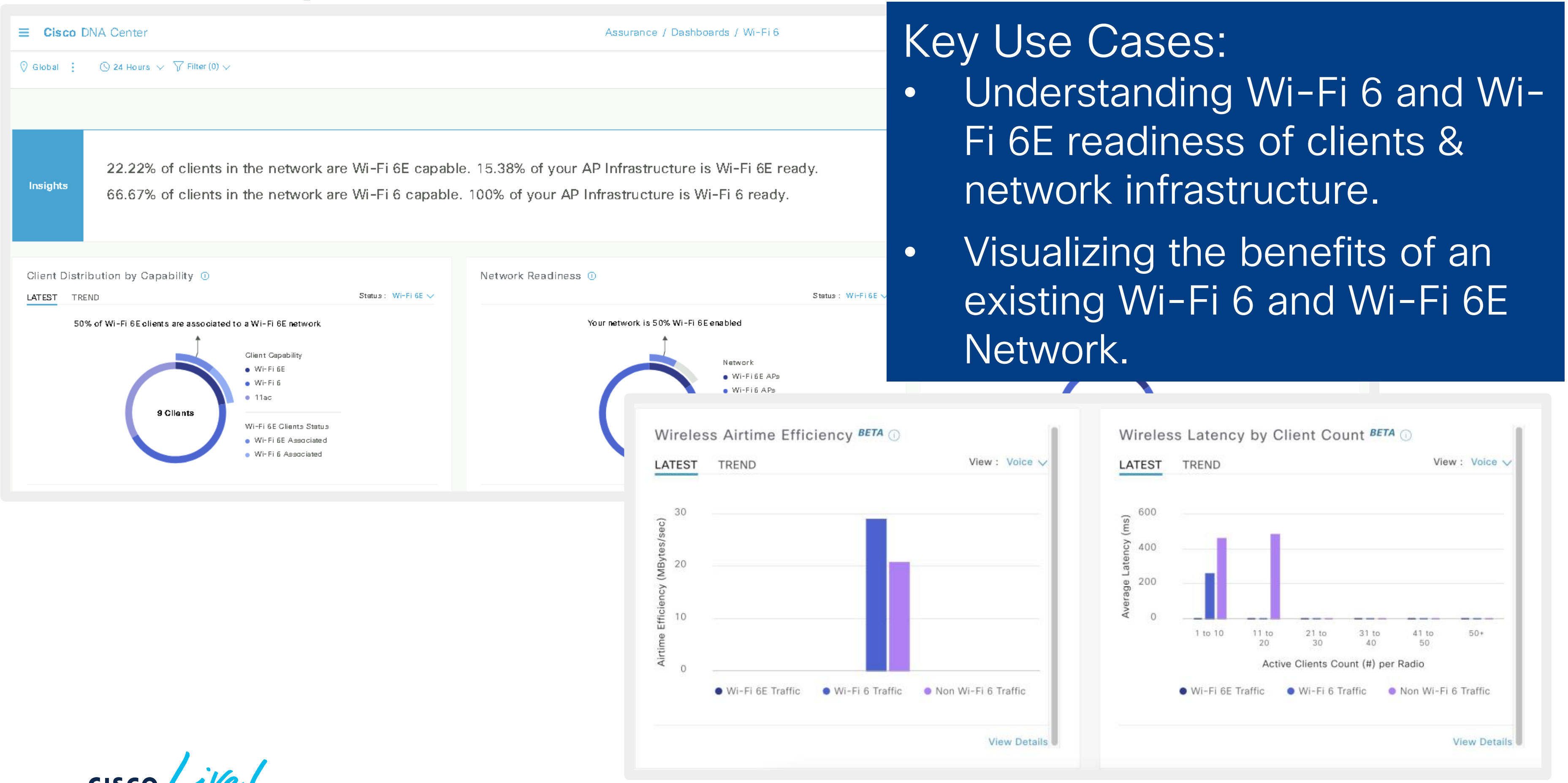
- Understanding Wi-Fi 6 and Wi-Fi 6E readiness of clients & network infrastructure.

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

Wi-Fi 6/6E Readiness Dashboard

Key Use Cases:

- Understanding Wi-Fi 6 and Wi-Fi 6E readiness of clients & network infrastructure.
- Visualizing the benefits of an existing Wi-Fi 6 and Wi-Fi 6E Network.



Cisco DNA Center

Assurance / Dashboards / Wi-Fi 6

Global

24 Hours

Filter (0)

Insights

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

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

Client Distribution by Capability

LATEST TREND Status : Wi-Fi 6E

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

Network Readiness

Status : Wi-Fi 6E

Your network is 50% Wi-Fi 6E enabled

Wireless Airtime Efficiency BETA

LATEST TREND View : Voice

View Details

Wireless Latency by Client Count BETA

LATEST TREND View : Voice

View Details

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

Wi-Fi 6/6E Readiness Dashboard

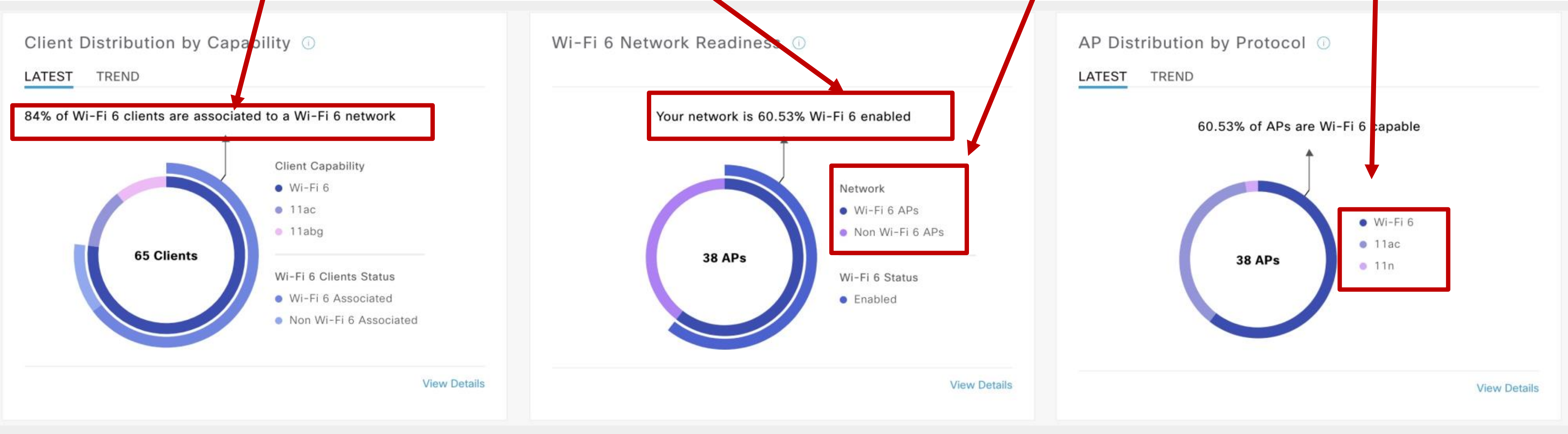
For your reference

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

Percentage of AP's Wi-Fi 6 enabled

Percentage of AP's Wi-Fi 6 capable

Wi-Fi version distribution



Client Distribution by Capability

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

Wi-Fi 6 Network Readiness

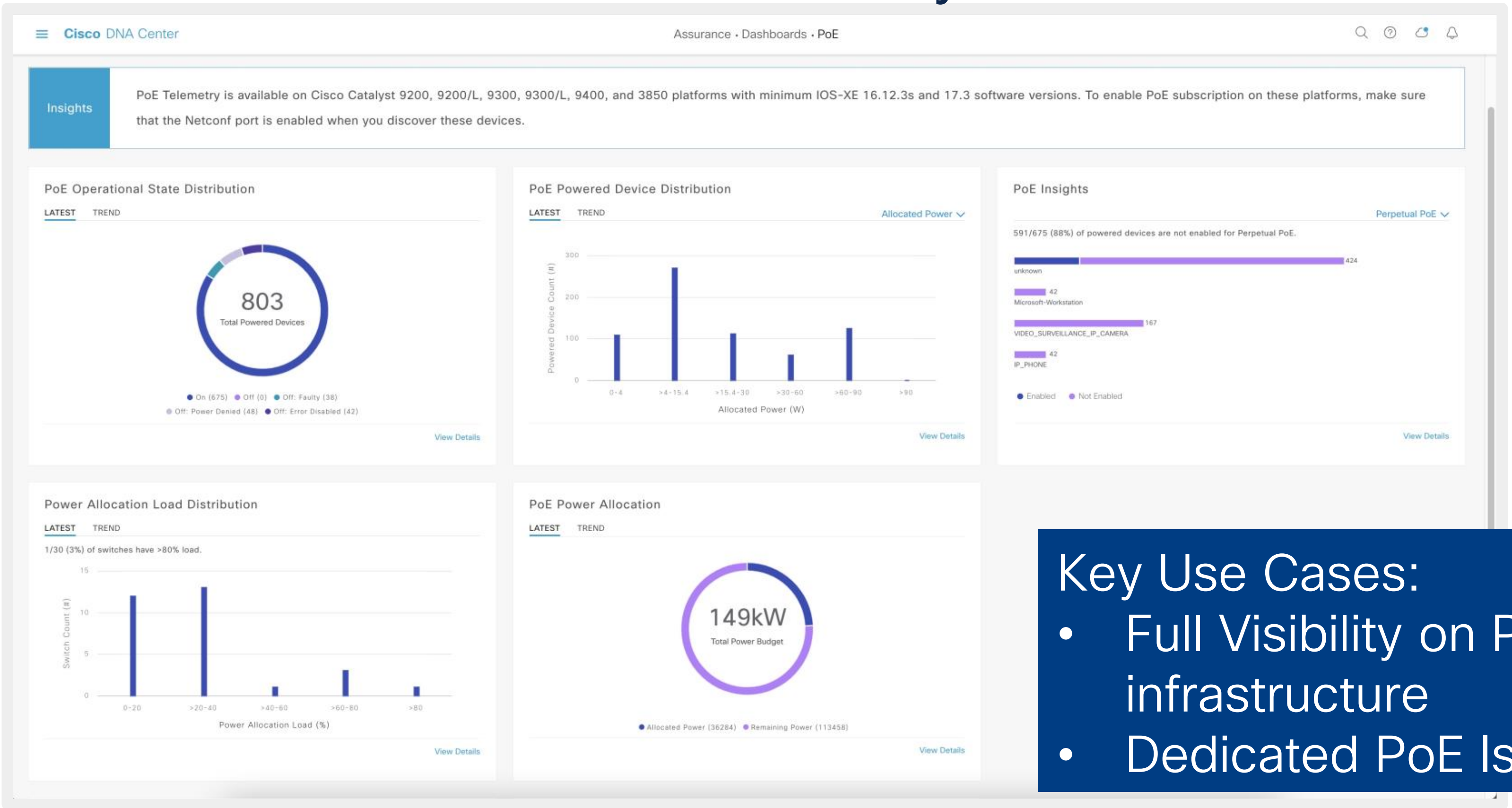
Your network is 60.53% Wi-Fi 6 enabled

AP Distribution by Protocol

60.53% of APs are Wi-Fi 6 capable

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

Power over Ethernet Analytics



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

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

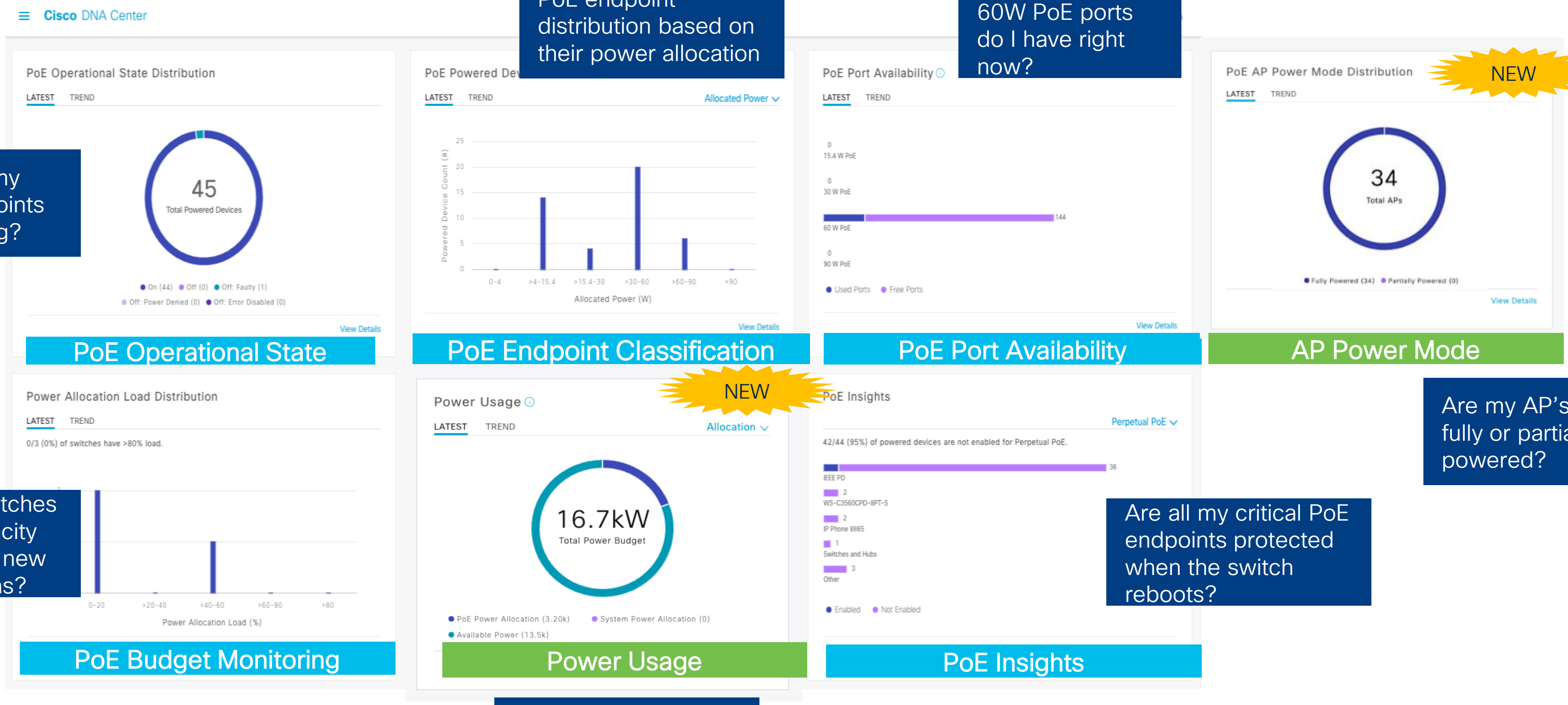
1/30 (3%) of switches have >80% load.

Key Use Cases:

- Full Visibility on PoE infrastructure
- Dedicated PoE Issue Types

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

Power over Ethernet Analytics



Cisco DNA Center

PoE Operational State Distribution

LATEST TREND

45
Total Powered Devices
● On (44) ● Off (0) ● Off: Faulty (1)
● Off: Power Denied (0) ● Off: Error Disabled (0)
View Details

PoE Powered De

LATEST TREND Allocated Power

Powered Device Count (#)
25
20
15
10
5
0
0-4
>4-15.4
>15.4-30
>30-60
>60-90
>90
Allocated Power (W)
View Details

PoE Port Availability

LATEST TREND

0
15.4 W PoE
0
30 W PoE
144
60 W PoE
0
90 W PoE
● Used Ports ● Free Ports
View Details

PoE AP Power Mode Distribution

LATEST TREND

34
Total APs
● Fully Powered (34) ● Partially Powered (0)
View Details

Power Allocation Load Distribution

LATEST TREND

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

0-20
>20-40
>40-60
>60-80
>80
Power Allocation Load (%)

Power Usage

LATEST TREND Allocation

16.7kW
Total Power Budget
● PoE Power Allocation (3.20k) ● System Power Allocation (0)
● Available Power (13.5k)

PoE Insights

Perpetual PoE

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

PoE endpoint distribution based on their power allocation

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

NEW

How are my PoE endpoints functioning?

PoE Operational State

PoE Endpoint Classification

PoE Port Availability

AP Power Mode

NEW

Are my AP’s fully or partially powered?

Which switches have capacity to add 10 new IP Cameras?

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

PoE Budget Monitoring

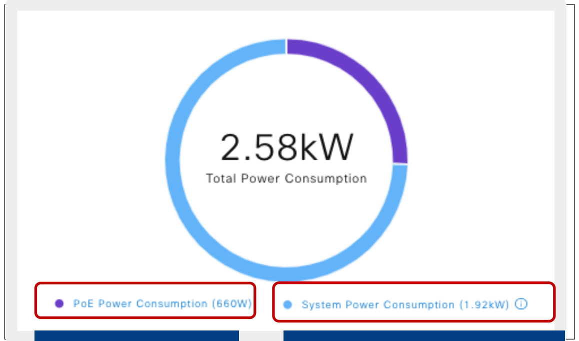
Power Usage

PoE Insights

What is the real time power consumption of my access network

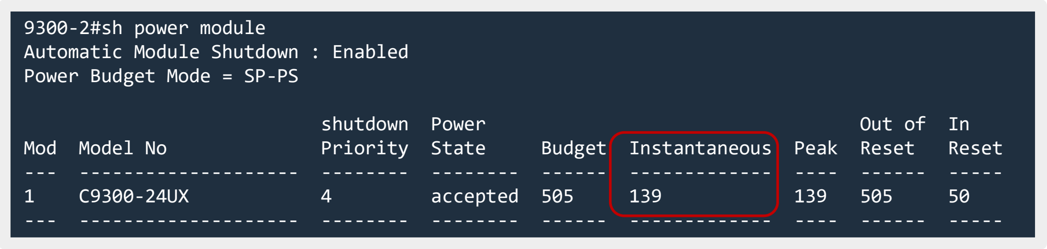
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Realtime Power Consumption Reporting

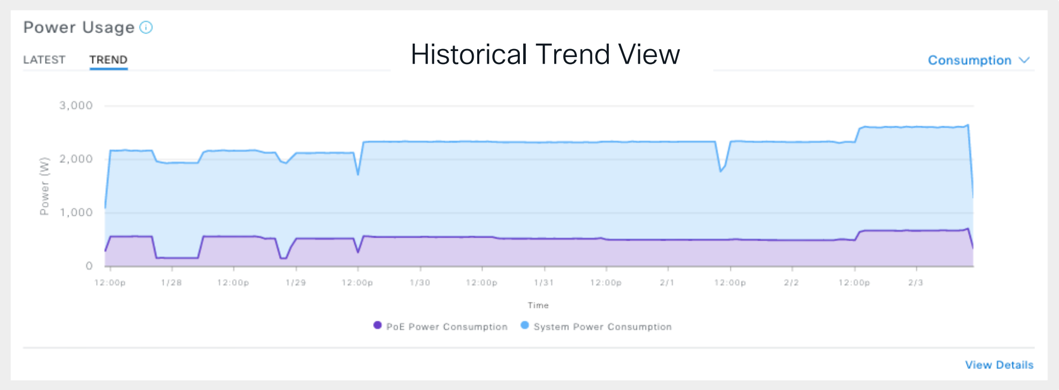


Realtime PoE consumption

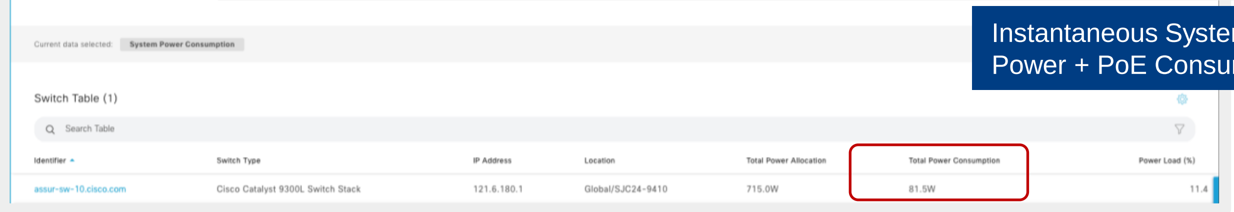
Realtime Sys Power consumption



```
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
---  --------------------          -------- -------- ------ ------------- ----  ------  -----
```



Historical Trend View



Select a data type below to filter the proceedir

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

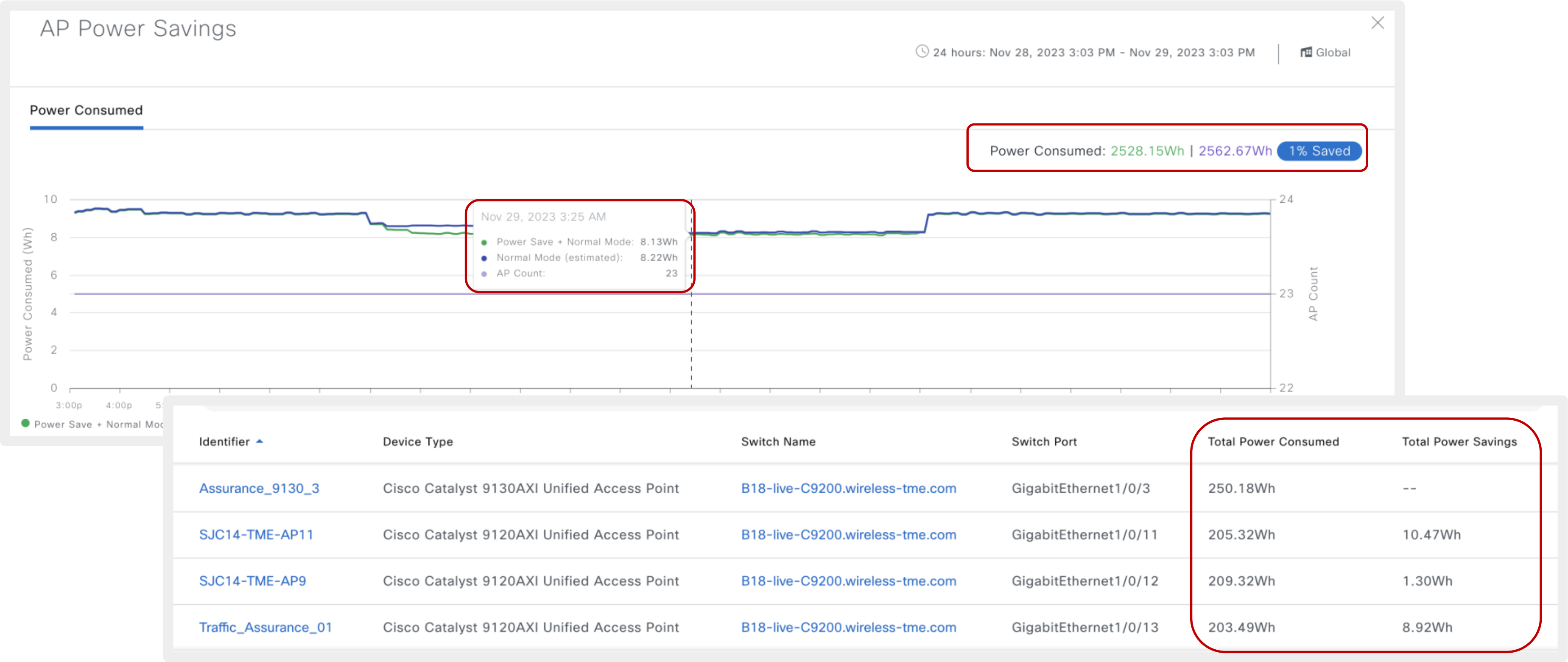
Supported for Catalyst 9300 and 9400 switches starting IOS XE 17.8

Instantaneous System Power + PoE Consumption

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

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

Power Consumed: 2528.15Wh | 2562.67Wh 1% Saved

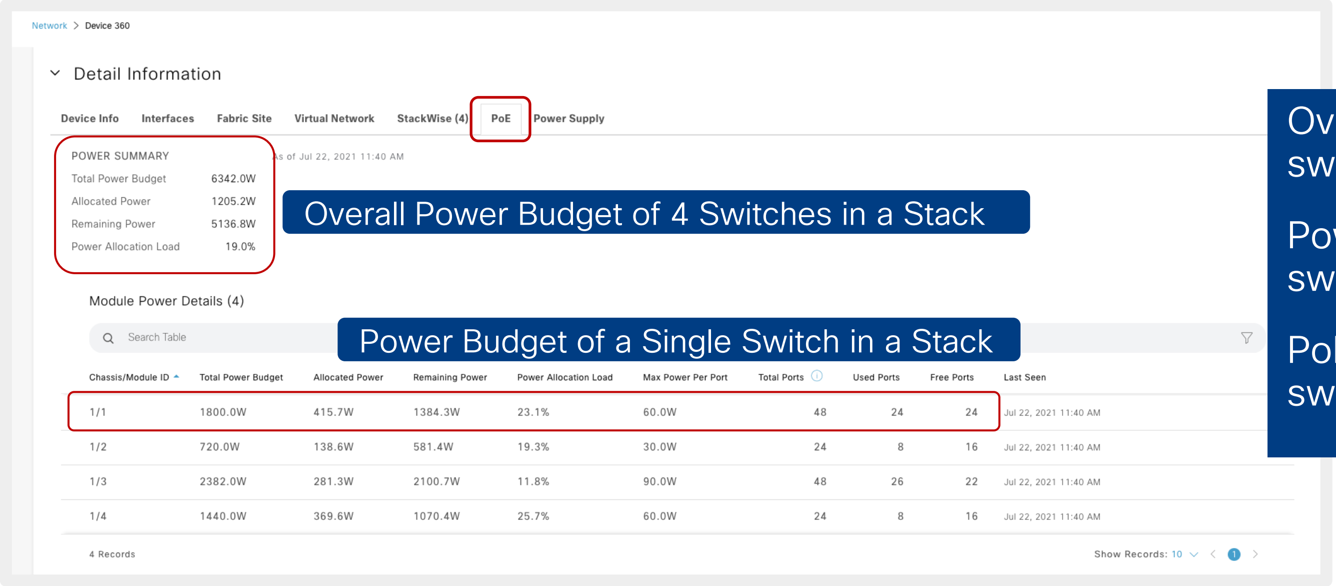
Nov 29, 2023 3:25 AM

- Power Save + Normal Mode: 8.13Wh
- Normal Mode (estimated): 8.22Wh
- AP Count: 23

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

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

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

As of Jul 22, 2021 11:40 AM

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

Overall Power Budget of 4 Switches in a Stack

Module Power Details (4)

Search Table

Power Budget of a Single Switch in a Stack

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

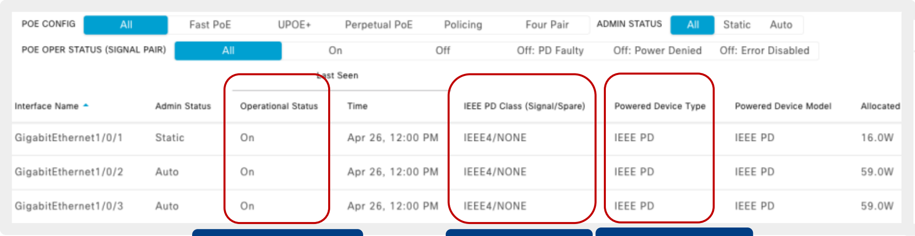
4 Records

Show Records: 10 < 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

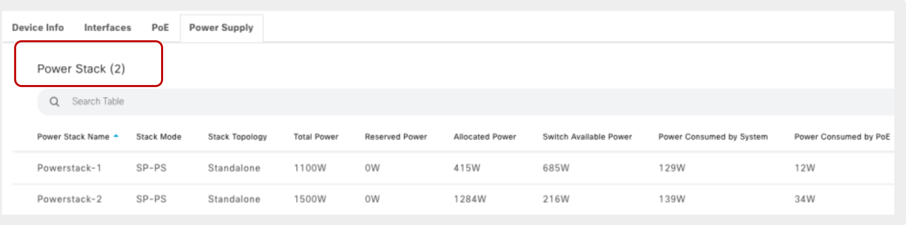
POE OPER STATUS (SIGNAL PAIR): All | On | Off | Off: PD Faulty | Off: Power Denied | Off: Error Disabled

			Last Seen				
Interface Name	Admin Status	Operational Status	Time	IEEE PD Class (Signal/Spare)	Powered Device Type	Powered Device Model	Allocated
GigabitEthernet1/0/1	Static	On	Apr 26, 12:00 PM	IEEE4/NONE	IEEE PD	IEEE PD	16.0W
GigabitEthernet1/0/2	Auto	On	Apr 26, 12:00 PM	IEEE4/NONE	IEEE PD	IEEE PD	59.0W
GigabitEthernet1/0/3	Auto	On	Apr 26, 12:00 PM	IEEE4/NONE	IEEE PD	IEEE PD	59.0W

POE Oper Status

PD Class

Device Type



Device Info | Interfaces | PoE | Power Supply

Power Stack (2)

Search Table

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

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

PoE Analytics

Under the Hood

For your reference

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

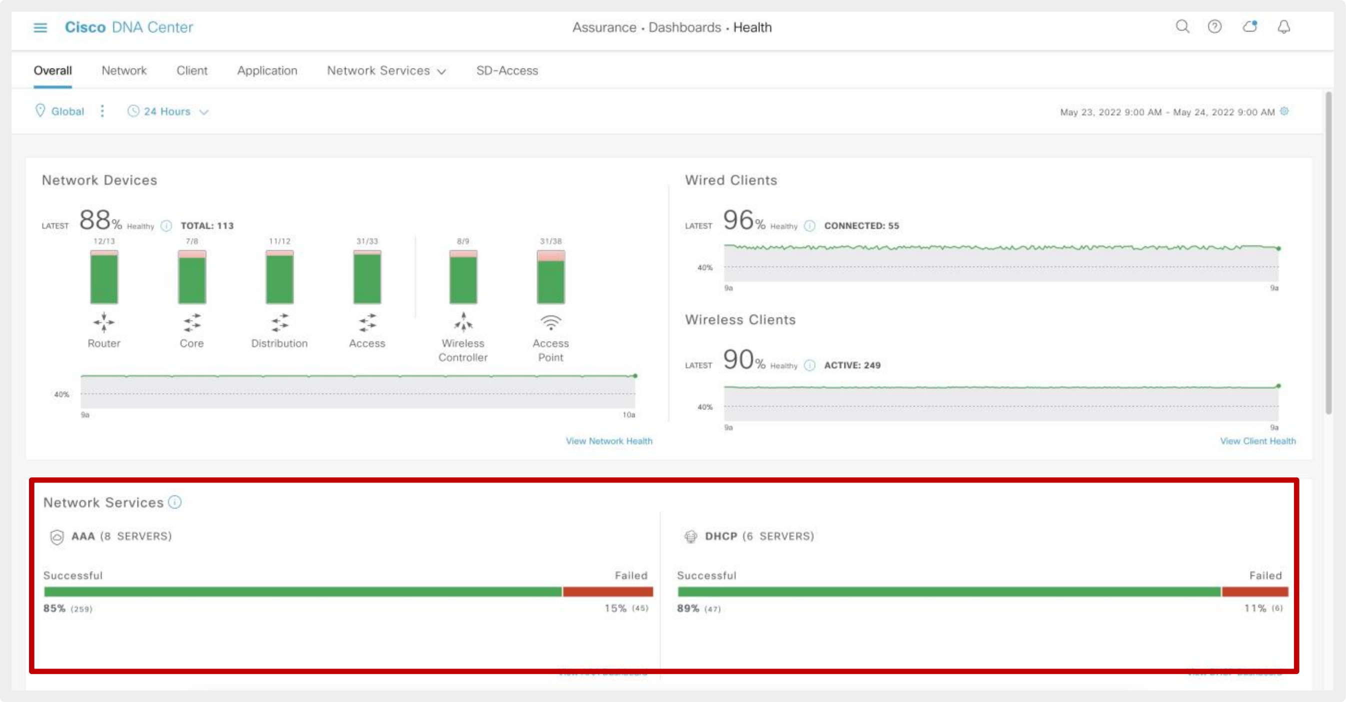
```
telemetry ietf subscription 502
 encoding encode-tdl
 filter tdl-uri
/services;serviceName=ios_oper/poe_stack
 receiver-type protocol
 source-address 10.85.54.24
 stream native
 update-policy periodic 60000
 receiver name DNAC_ASSURANCE_RECEIVER
telemetry ietf subscription 503
 encoding encode-tdl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

Subscriptions automatically configured as part of “Device Controllability”

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

Network Services Analytics

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



May 23, 2022 9:00 AM - May 24, 2022 9:00 AM

Network Devices: LATEST 88% Healthy TOTAL: 113

Wired Clients: LATEST 96% Healthy CONNECTED: 55

Wireless Clients: LATEST 90% Healthy ACTIVE: 249

Network Services

AAA (8 SERVERS)

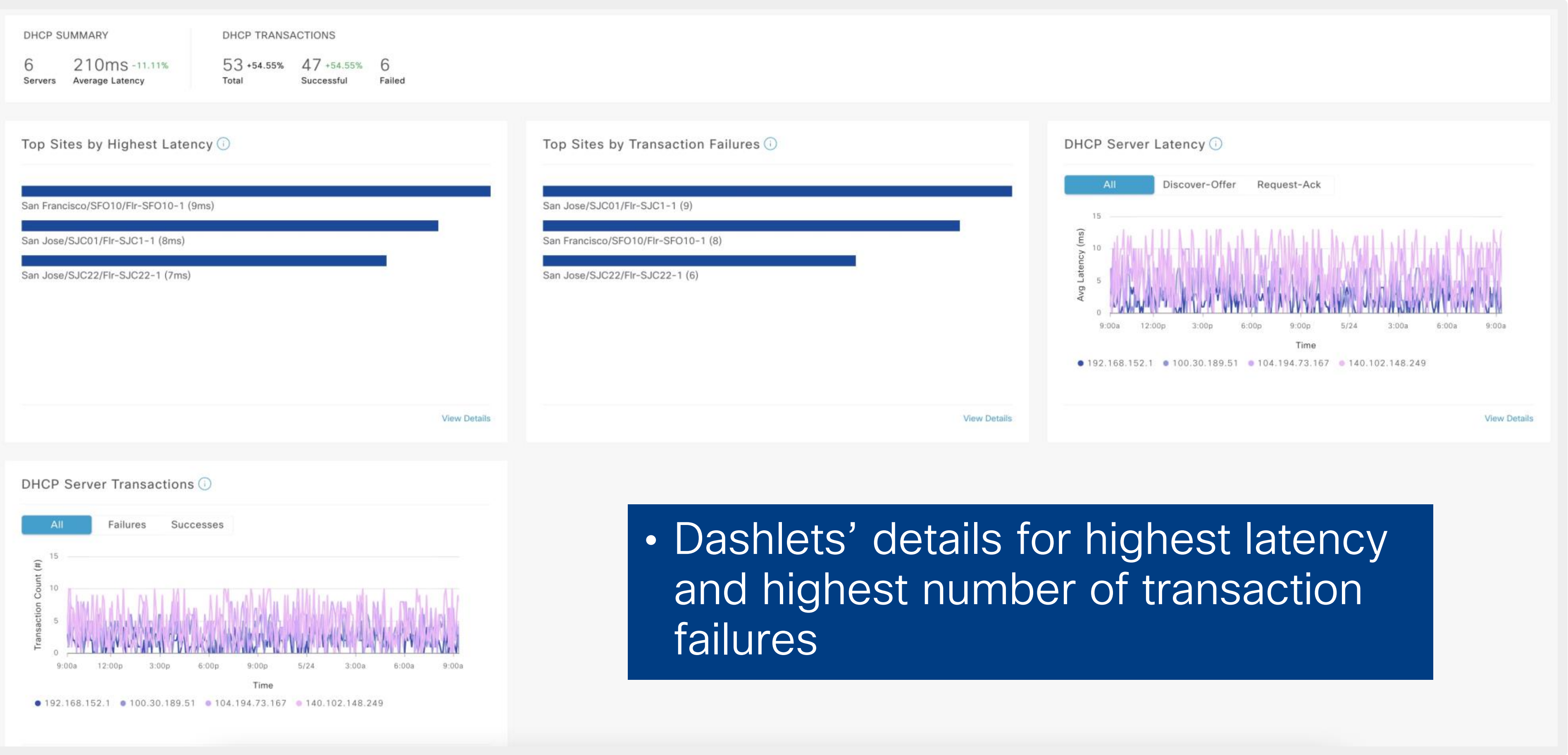
Successful 85% (259) Failed 15% (45)

DHCP (6 SERVERS)

Successful 89% (47) Failed 11% (6)

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

Network Services Analytics



DHCP SUMMARY

6 Servers

210ms -11.11% Average Latency

DHCP TRANSACTIONS

53 +54.55% Total

47 +54.55% Successful

6 Failed

Top Sites by Highest Latency ⓘ

San Francisco/SFO10/Flr-SFO10-1 (9ms)

San Jose/SJC01/Flr-SJC1-1 (8ms)

San Jose/SJC22/Flr-SJC22-1 (7ms)

View Details

Top Sites by Transaction Failures ⓘ

San Jose/SJC01/Flr-SJC1-1 (9)

San Francisco/SFO10/Flr-SFO10-1 (8)

San Jose/SJC22/Flr-SJC22-1 (6)

View Details

DHCP Server Latency ⓘ

View Details

DHCP Server Transactions ⓘ

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

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

Tracked by Network Services Analytics

For your 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

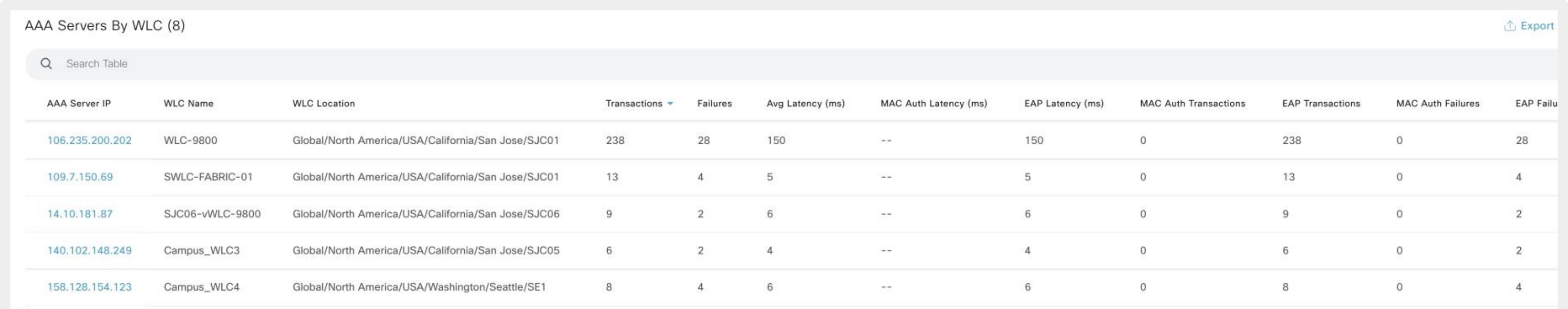
DHCP

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

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

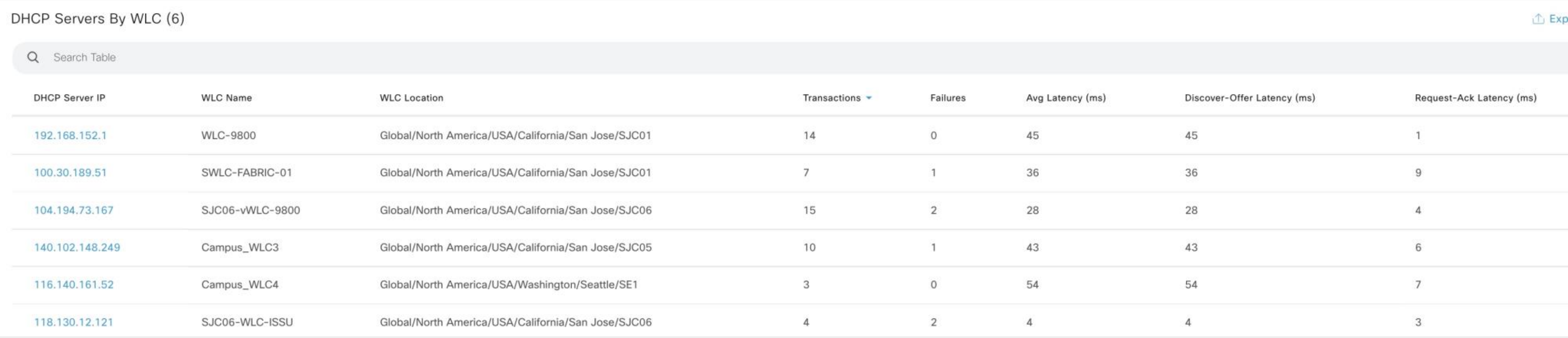
Network Services Analytics

- Mapping of WLCs to corresponding AAA/DHCP servers



AAA Servers By WLC (8)

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

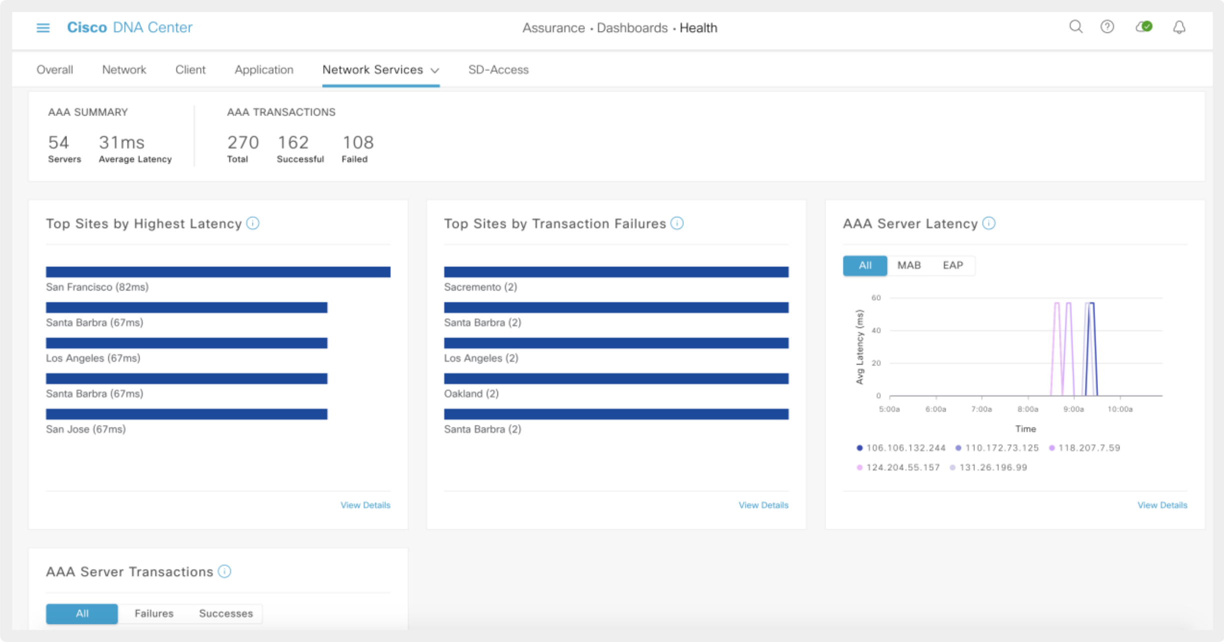


DHCP Servers By WLC (6)

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

Network Services Analytics

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



AAA SUMMARY

54 Servers
31ms Average Latency

AAA TRANSACTIONS

270 Total
162 Successful
108 Failed

Top Sites by Highest Latency

- San Francisco (82ms)
- Santa Barbra (67ms)
- Los Angeles (67ms)
- Santa Barbra (67ms)
- San Jose (67ms)

Top Sites by Transaction Failures

- Sacremento (2)
- Santa Barbra (2)
- Los Angeles (2)
- Oakland (2)
- Santa Barbra (2)

AAA Server Latency

All | MAB | EAP

● 106.106.132.244 ● 110.172.73.125 ● 118.207.7.59
● 124.204.55.157 ● 131.26.196.99

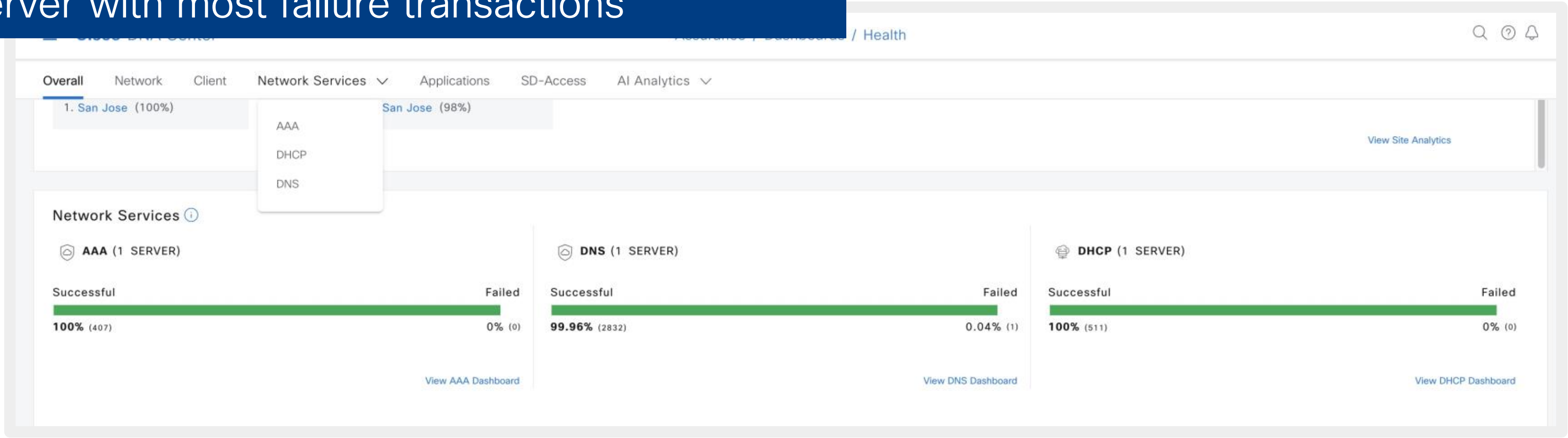
AAA Server Transactions

All | Failures | Successes

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

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



1. San Jose (100%)

San Jose (98%)

Network Services

AAA (1 SERVER)

Successful — 100% (407)
Failed — 0% (0)

DNS (1 SERVER)

Successful — 99.96% (2832)
Failed — 0.04% (1)

DHCP (1 SERVER)

Successful — 100% (511)
Failed — 0% (0)

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

Network Services DNS

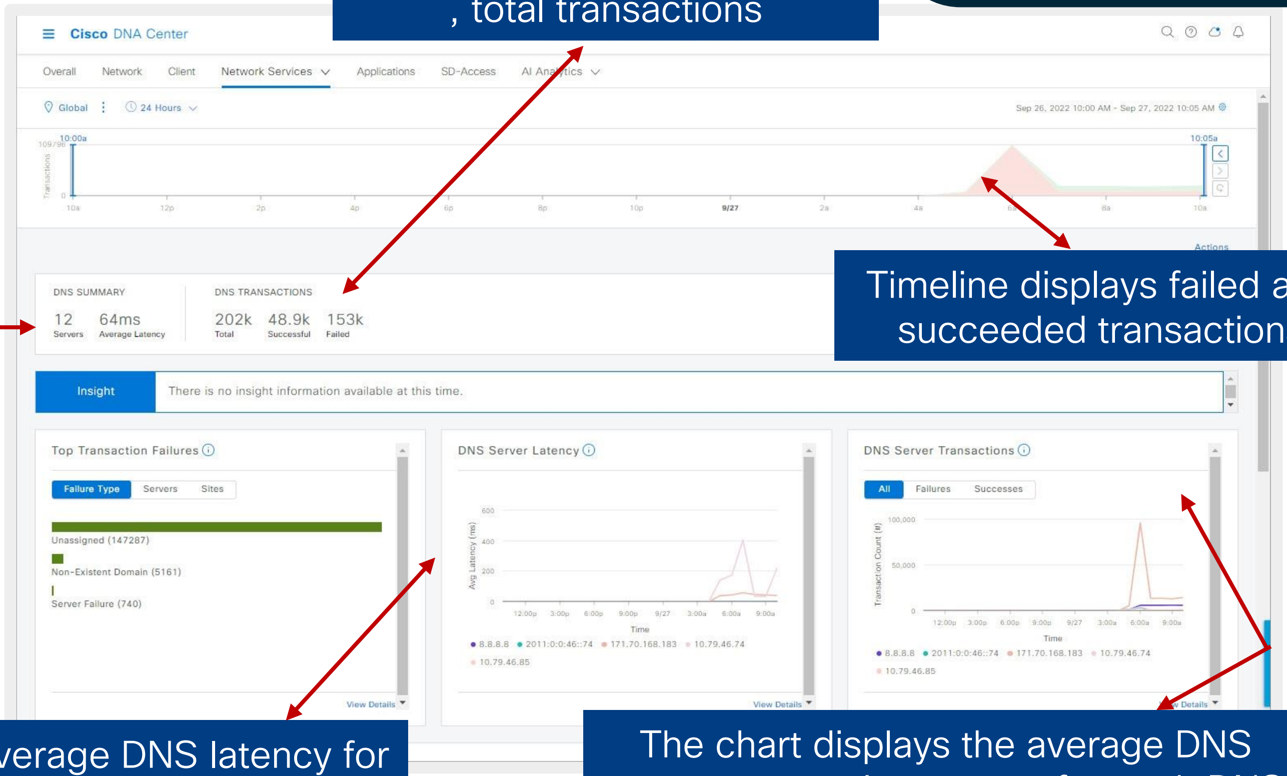
For your reference

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



Sep 26, 2022 10:00 AM - Sep 27, 2022 10:05 AM

DNS SUMMARY

12 Servers

64ms Average Latency

DNS TRANSACTIONS

202k Total

48.9k Successful

153k Failed

There is no insight information available at this time.

Unassigned (147287)

Non-Existent Domain (5161)

Server Failure (740)

Average DNS latency for each DNS server.

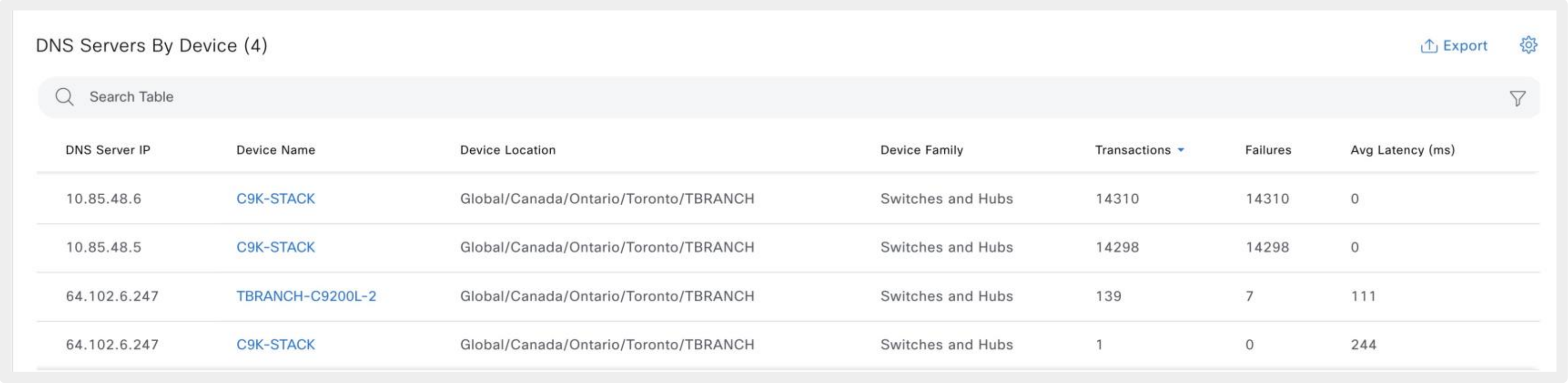
The chart displays the average DNS server transactions status for each DNS server reported by wireless controllers.

Network Services – DNS Dashboard

For your reference

Find DNS servers by device

Displays total transactions, failures and average latency per server



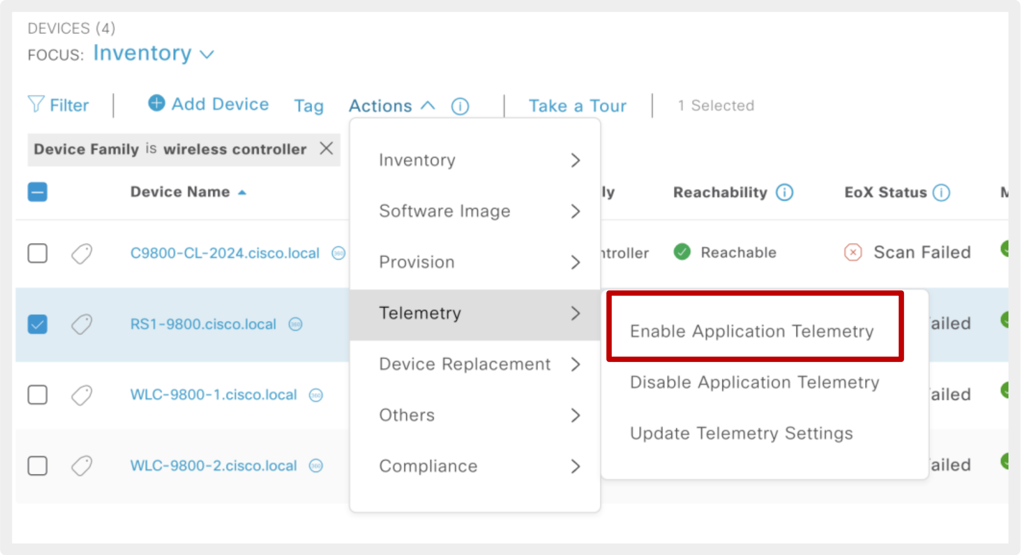
DNS Servers By Device (4)

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

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

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



DEVICES (4)

FOCUS: Inventory

Filter | Add Device Tag Actions | Take a Tour | 1 Selected

Device Family is wireless controller ×

		Device Name	ly	Reachability	EoX Status
☐		C9800-CL-2024.cisco.local	ntroller	Reachable	Scan Failed
☑		RS1-9800.cisco.local			ailed
☐		WLC-9800-1.cisco.local			ailed
☐		WLC-9800-2.cisco.local			ailed

Inventory
Software Image
Provision
Telemetry
Device Replacement
Others
Compliance
Enable Application Telemetry
Disable Application Telemetry
Update Telemetry Settings

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

Network Services – DNS Dashboard

For your reference

C9300-24P

IOS-XE: 17.11.01

Cisco DNA Center

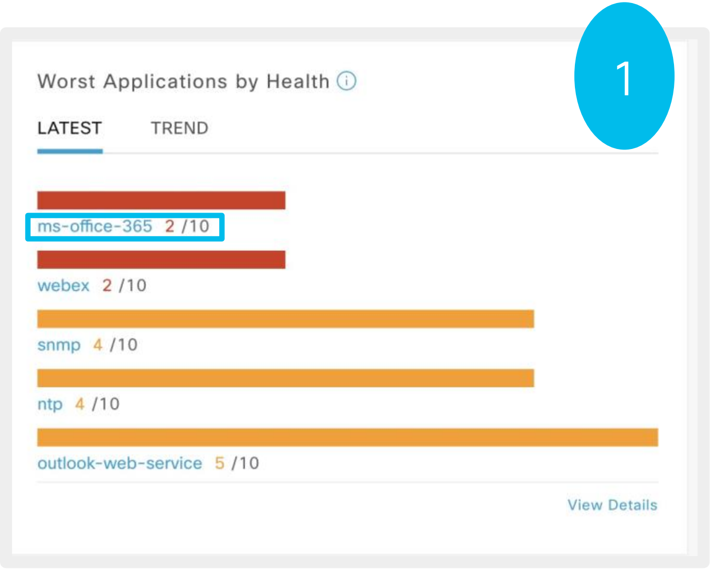
Version 2.3.5.3-70194

```
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


1

Worst Applications by Health ⓘ

LATEST TREND

ms-office-365 2 /10

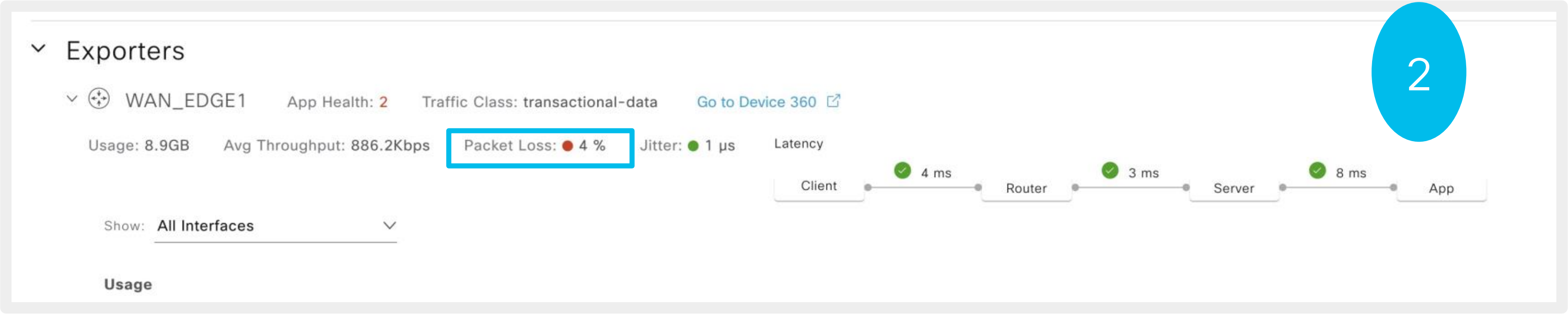
webex 2 /10

snmp 4 /10

ntp 4 /10

outlook-web-service 5 /10

View Details


2

Exporters

WAN_EDGE1 App Health: 2 Traffic Class: transactional-data Go to Device 360

Usage: 8.9GB Avg Throughput: 886.2Kbps Packet Loss: ● 4 % Jitter: ● 1 µs

Latency

Show: All Interfaces

Usage

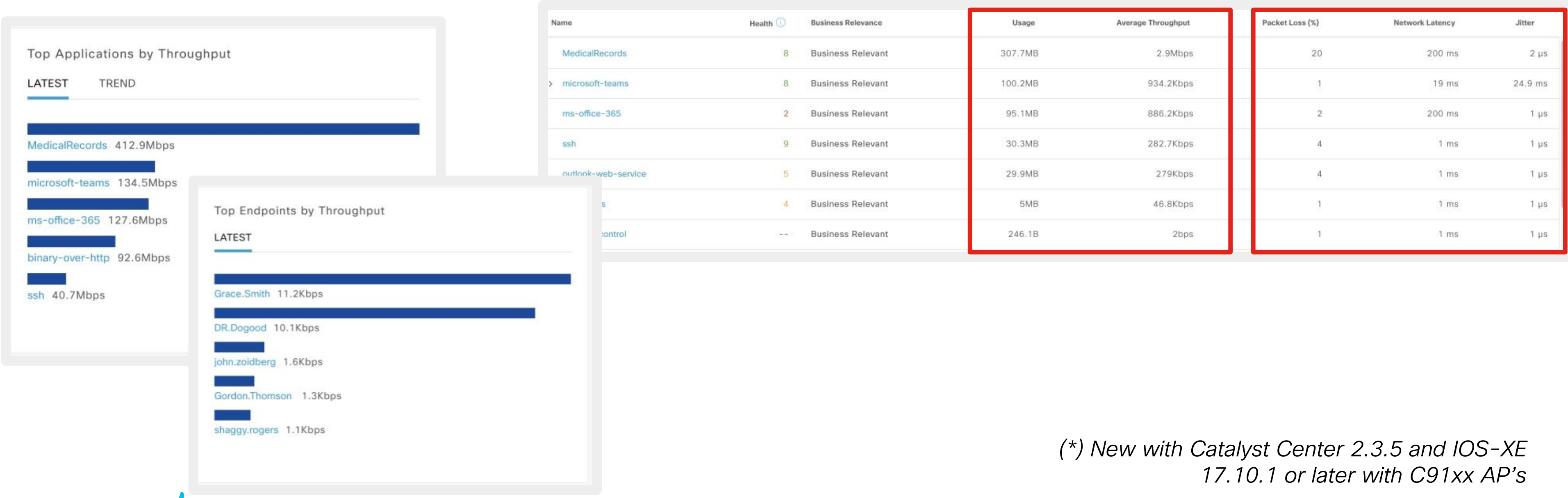
Application Visibility vs Application Experience

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

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

Top Endpoints by Throughput

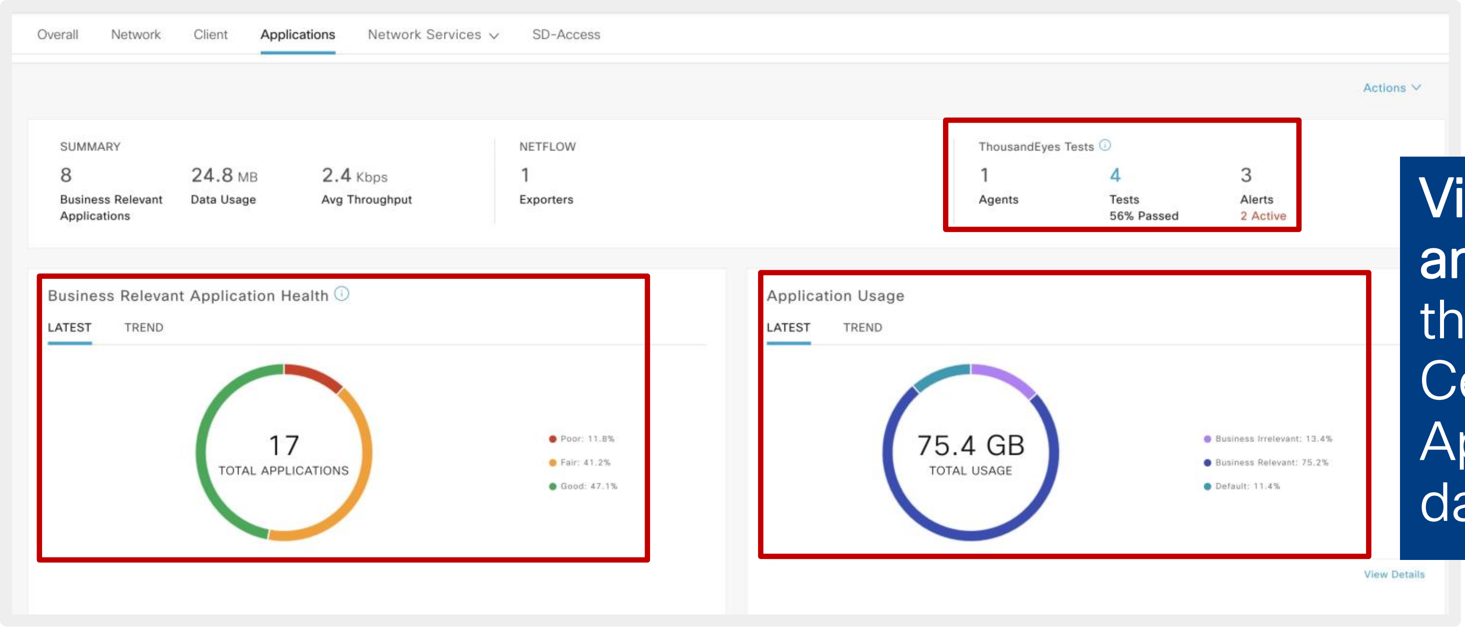
Grace.Smith	11.2Kbps
DR.Dogood	10.1Kbps
john.zoidberg	1.6Kbps
Gordon.Thomson	1.3Kbps
shaggy.rogers	1.1Kbps

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
ontrol	--	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

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

Application Health Dashboard: ThousandEyes Integration



Overall | Network | Client | Applications | Network Services ⌄ | SD-Access

Actions ⌄

SUMMARY

8 Business Relevant Applications

24.8 MB Data Usage

2.4 Kbps Avg Throughput

NETFLOW

1 Exporters

ThousandEyes Tests ⓘ

1 Agents

4 Tests 56% Passed

3 Alerts 2 Active

Business Relevant Application Health ⓘ

LATEST | TREND

17 TOTAL APPLICATIONS

● Poor: 11.8%
● Fair: 41.2%
● Good: 47.1%

Application Usage

LATEST | TREND

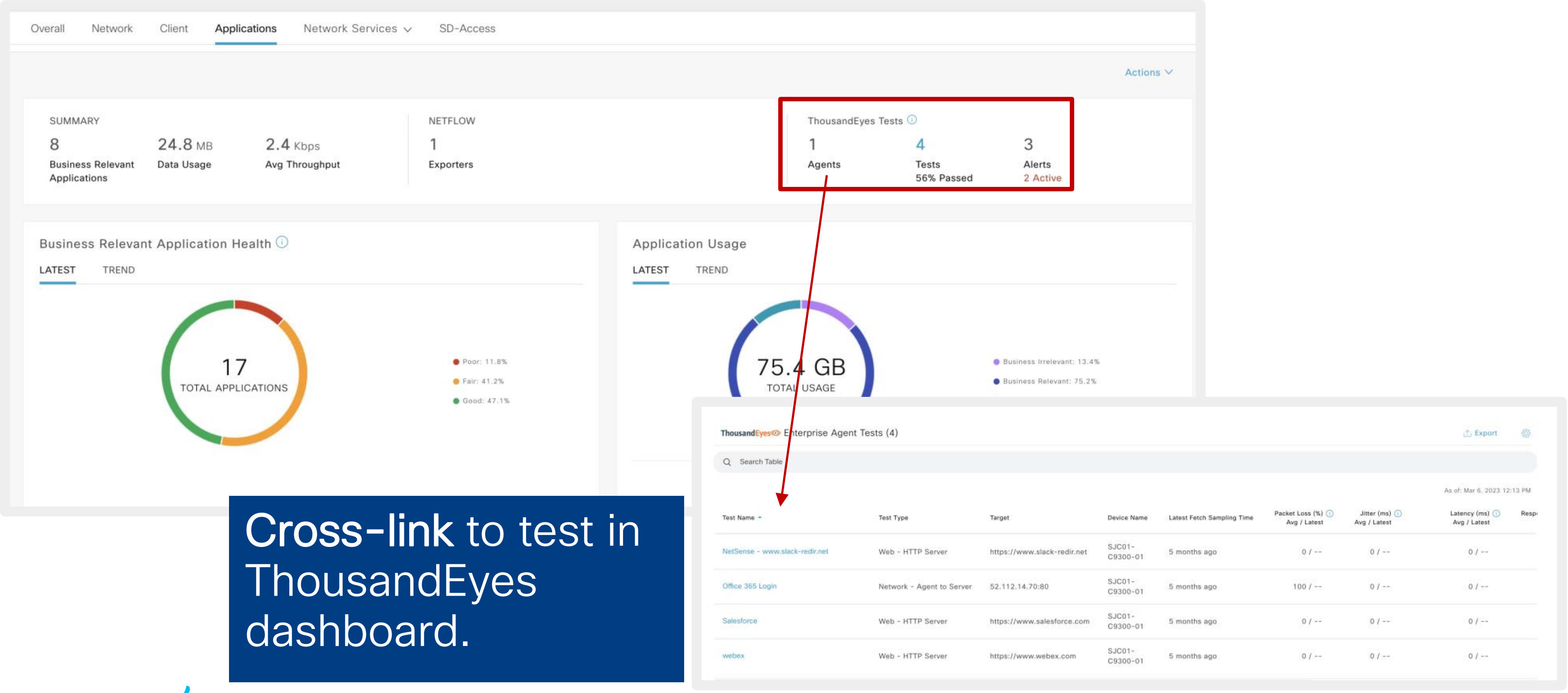
75.4 GB TOTAL USAGE

● Business Irrelevant: 13.4%
● Business Relevant: 75.2%
● Default: 11.4%

View Details

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

Application Health Dashboard: ThousandEyes Integration



SUMMARY

8 Business Relevant Applications

24.8 MB Data Usage

2.4 Kbps Avg Throughput

NETFLOW

1 Exporters

ThousandEyes Tests

1 Agents

4 Tests 56% Passed

3 Alerts 2 Active

Business Relevant Application Health

Application Usage

ThousandEyes Enterprise Agent Tests (4)

As of: Mar 6, 2023 12:13 PM

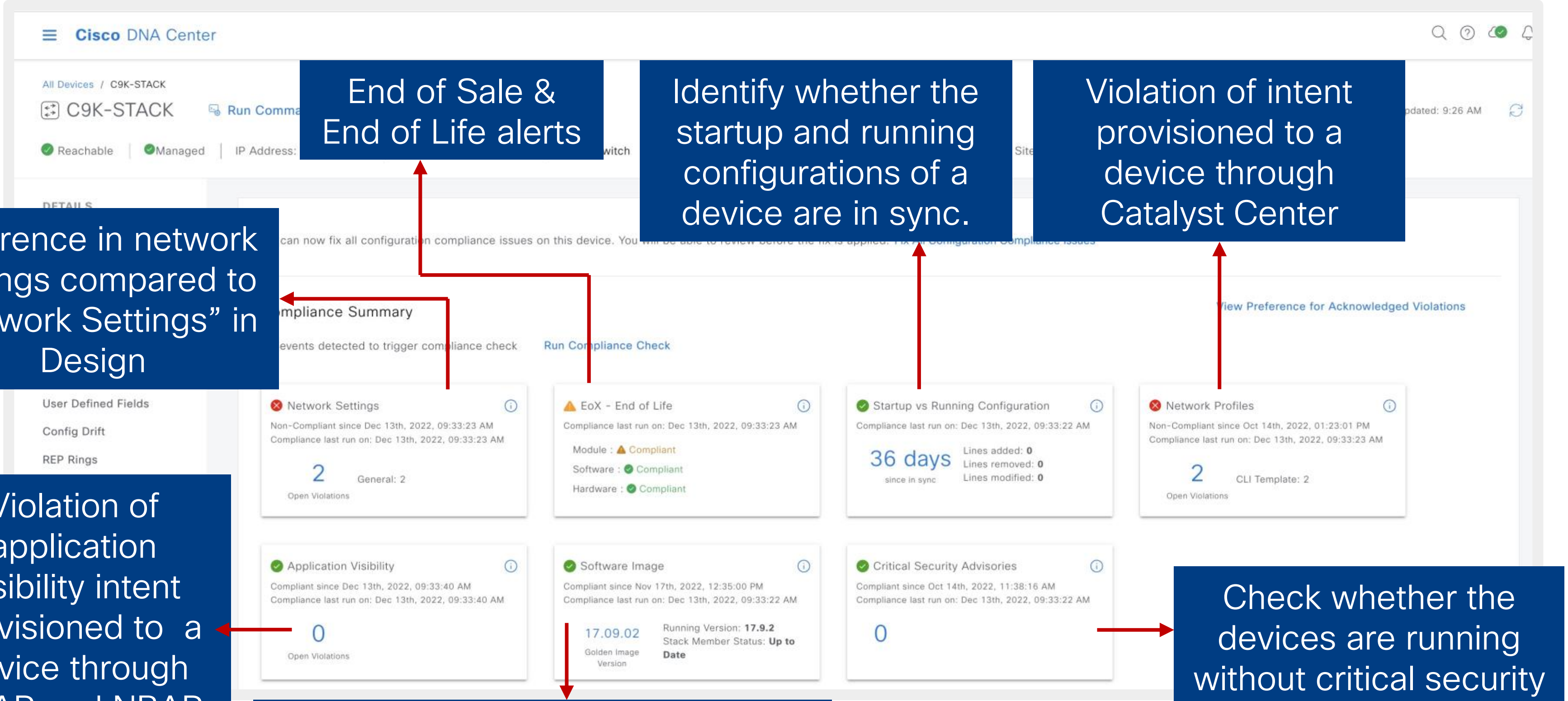
Test Name	Test Type	Target	Device Name	Latest Fetch Sampling Time	Packet Loss (%) Avg / Latest	Jitter (ms) Avg / Latest	Latency (ms) Avg / Latest	Resp
NetSense - www.slack-redir.net	Web - HTTP Server	https://www.slack-redir.net	SJC01-C9300-01	5 months ago	0 / --	0 / --	0 / --	
Office 365 Login	Network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

Cross-link to test in ThousandEyes dashboard.

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

Habit #3 - Leverage Compliance and Configuration management

Cisco Catalyst Center Compliance Landscape



Cisco DNA Center

All Devices / C9K-STACK

C9K-STACK   Run Comma

Reachable | Managed | IP Address: witch   Site   pdated: 9:26 AM

DETAILS

User Defined Fields

Config Drift

REP Rings

can now fix all configurati n compliance issues on this device. You

mpliance Summary

events detected to trigger com liance check   Run Co pliance Check

iew Preference for Acknowledged Violations

Network Settings
Non-Compliant since Dec 13th, 2022, 09:33:23 AM
Compliance last run on: Dec 13th, 2022, 09:33:23 AM
2 Open Violations   General: 2

EoX - End of Life
Compliance last run on: Dec 13th, 2022, 09:33:23 AM
Module : Compliant
Software : Compliant
Hardware : Compliant

Startup vs Running Configuration
Compliance last run on: Dec 13th, 2022, 09:33:22 AM
36 days since in sync
Lines added: **0**
Lines removed: **0**
Lines modified: **0**

Network Profiles
Non-Compliant since Oct 14th, 2022, 01:23:01 PM
Compliance last run on: Dec 13th, 2022, 09:33:23 AM
2 Open Violations   CLI Template: 2

Application Visibility
Compliant since Dec 13th, 2022, 09:33:40 AM
Compliance last run on: Dec 13th, 2022, 09:33:40 AM
0 Open Violations

Software Image
Compliant since Nov 17th, 2022, 12:35:00 PM
Compliance last run on: Dec 13th, 2022, 09:33:22 AM
17.09.02 Golden Image Version
Running Version: **17.9.2**
Stack Member Status: **Up to Date**

Critical Security Advisories
Compliant since Oct 14th, 2022, 11:38:16 AM
Compliance last run on: Dec 13th, 2022, 09:33:22 AM
0

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

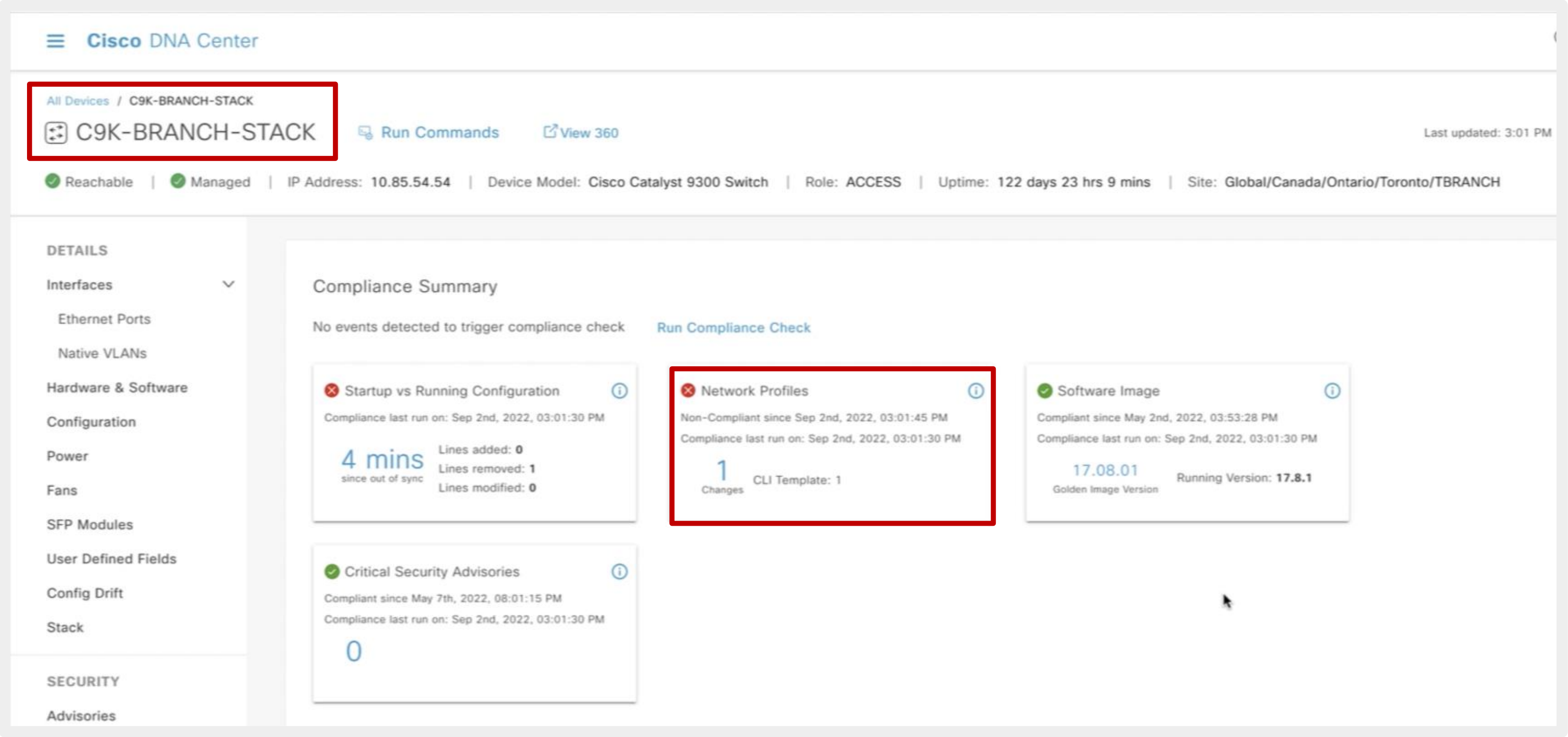
Difference in network settings compared to “Network Settings” in Design

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

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

Check whether the devices are running without critical security vulnerabilities.

Compliance: Network Profiles - Switches



All Devices / C9K-BRANCH-STACK

C9K-BRANCH-STACK

Last updated: 3:01 PM

✓ Reachable | ✓ Managed | IP Address: 10.85.54.54 | Device Model: Cisco Catalyst 9300 Switch | Role: ACCESS | Uptime: 122 days 23 hrs 9 mins | Site: Global/Canada/Ontario/Toronto/TBRANCH

Compliance Summary

No events detected to trigger compliance check

☒ Startup vs Running Configuration

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

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

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

Compliant since May 7th, 2022, 08:01:15 PM

Compliance last run on: Sep 2nd, 2022, 03:01:30 PM

0

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

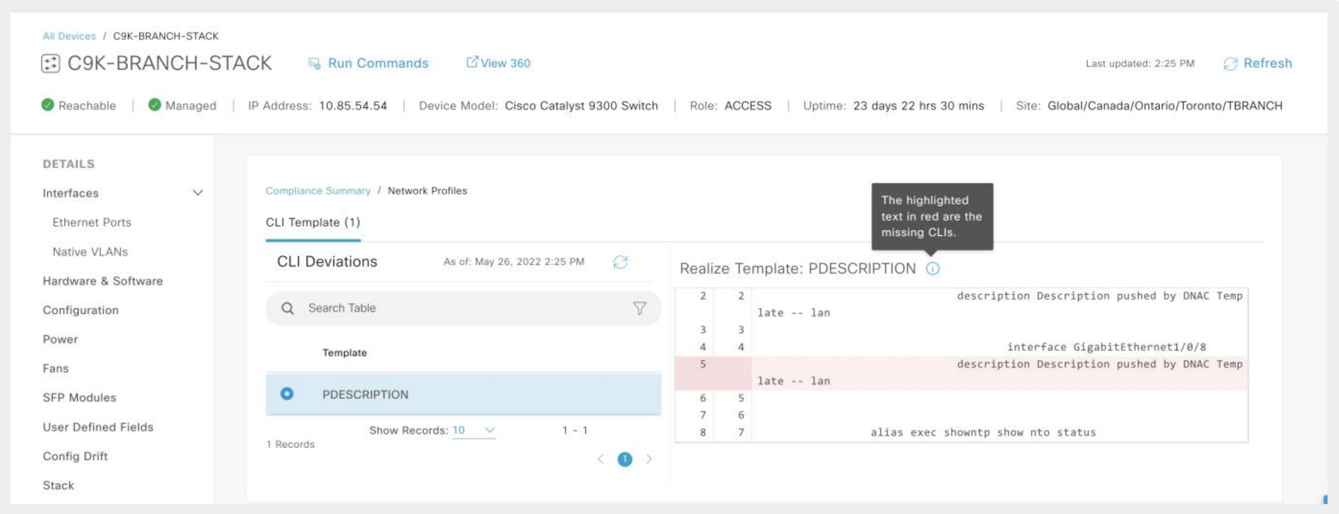
Compliance: Network Profiles - Switches

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-
```



All Devices / C9K-BRANCH-STACK

C9K-BRANCH-STACK Run Commands View 360 Last updated: 2:25 PM Refresh

Reachable | Managed | IP Address: 10.85.54.54 | Device Model: Cisco Catalyst 9300 Switch | Role: ACCESS | Uptime: 23 days 22 hrs 30 mins | Site: Global/Canada/Ontario/Toronto/TBRANCH

Compliance Summary / Network Profiles

CLI Template (1)

CLI Deviations As of: May 26, 2022 2:25 PM

Search Table

Template
● PDESCRIPTION

Show Records: 10 1 - 1

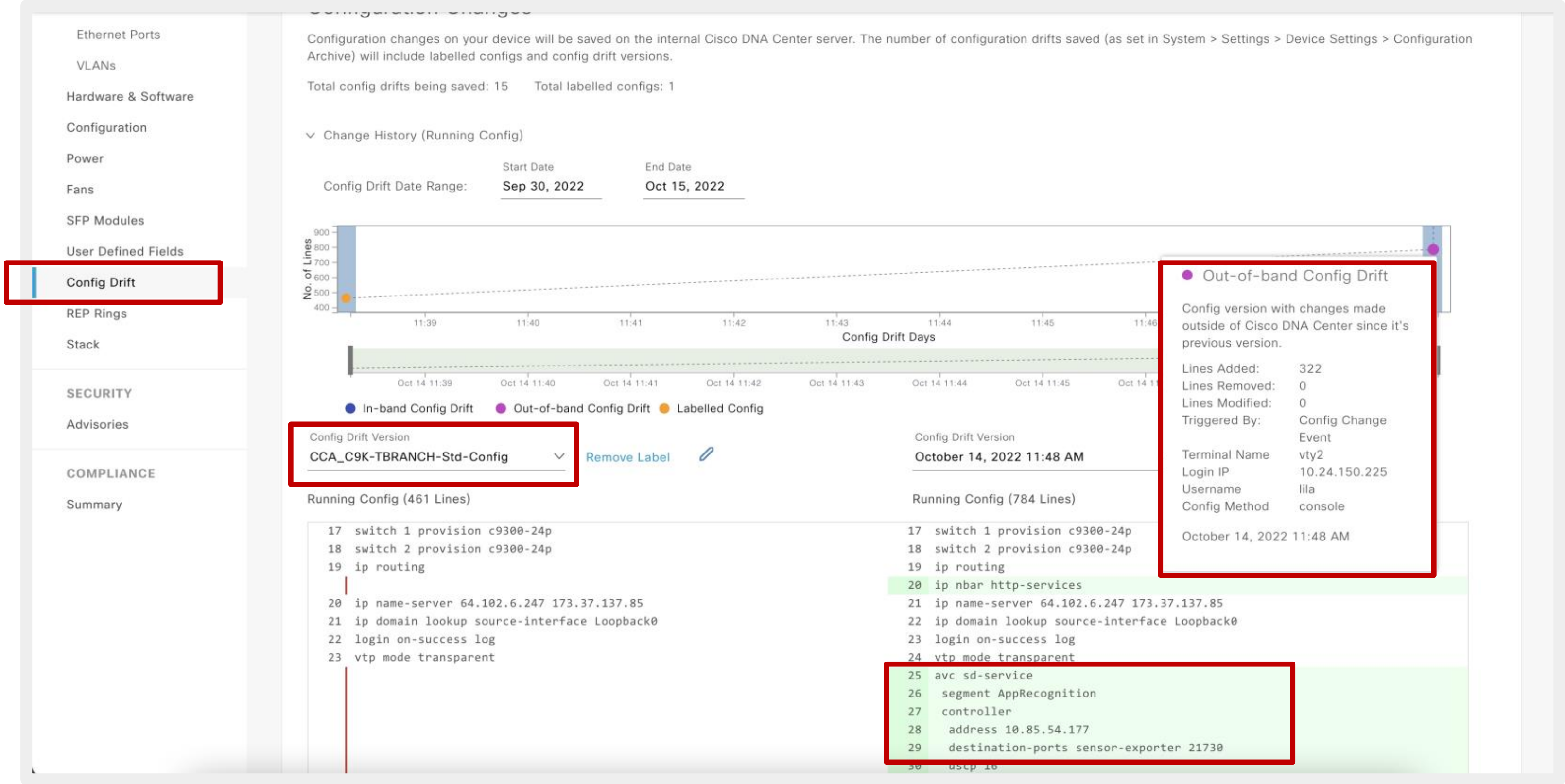
1 Records

The highlighted text in red are the missing CLIs.

Realize Template: PDESCRIPTION

```
 description Description pushed by DNAC Template -- lan

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


alias exec showntp show nto status
```

Config Drift



Configuration Changes

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

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

Change History (Running Config)

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

● Out-of-band Config Drift

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

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

October 14, 2022 11:48 AM

Config Drift Version: CCA_C9K-TBRANCH-Std-Config

Running Config (461 Lines)

```
switch 1 provision c9300-24p
switch 2 provision c9300-24p
ip routing

ip name-server 64.102.6.247 173.37.137.85
ip domain lookup source-interface Loopback0
login on-success log
vtp mode transparent
```

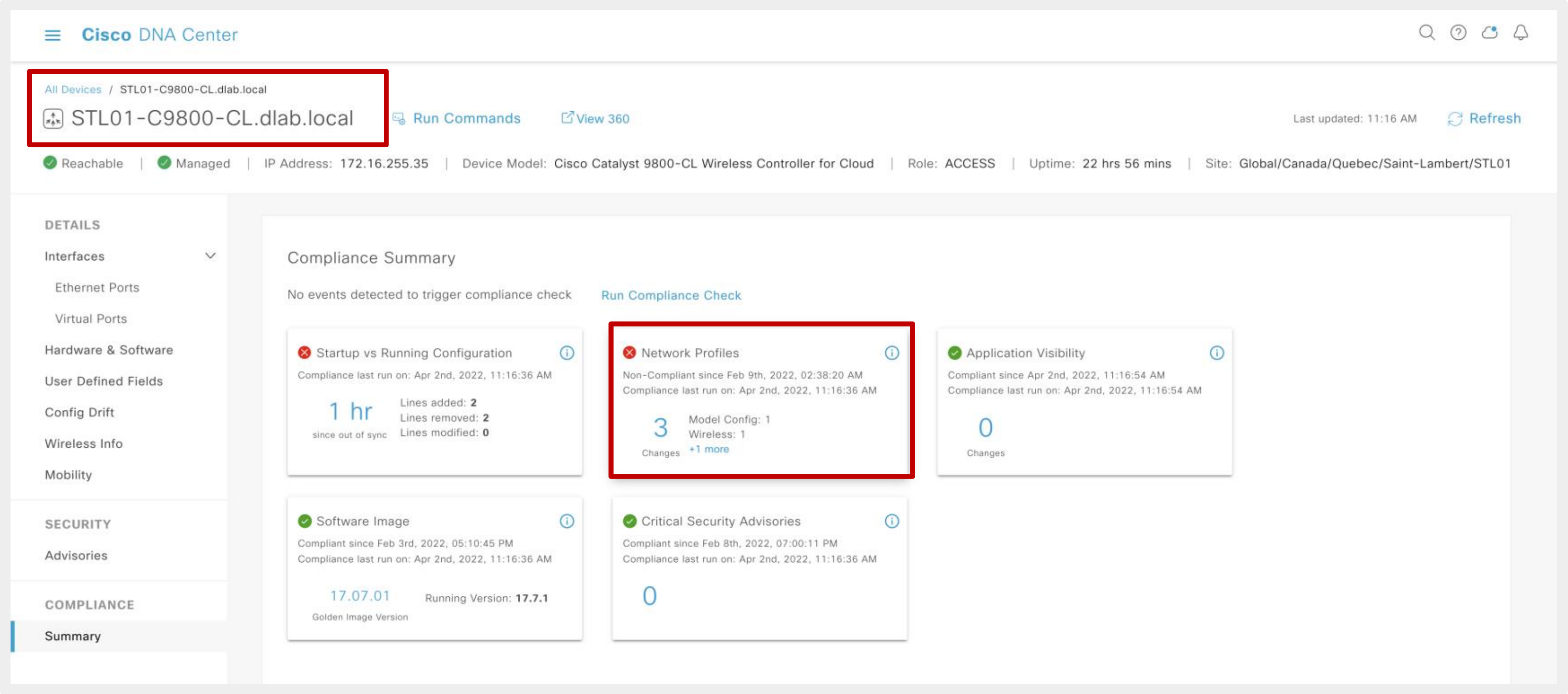
Config Drift Version: October 14, 2022 11:48 AM

Running Config (784 Lines)

```
switch 1 provision c9300-24p
switch 2 provision c9300-24p
ip routing
ip nbar http-services
ip name-server 64.102.6.247 173.37.137.85
ip domain lookup source-interface Loopback0
login on-success log
vtp mode transparent
avc sd-service
 segment AppRecognition
 controller
  address 10.85.54.177
  destination-ports sensor-exporter 21730
  dscp 16
```

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

Compliance: Network Profiles - Wireless



STL01-C9800-CL.dlab.local

Last updated: 11:16 AM

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

Compliance Summary

No events detected to trigger compliance check

☒ Startup vs Running Configuration
Compliance last run on: Apr 2nd, 2022, 11:16:36 AM
1 hr since out of sync
Lines added: **2**
Lines removed: **2**
Lines modified: **0**

☒ Network Profiles
Non-Compliant since Feb 9th, 2022, 02:38:20 AM
Compliance last run on: Apr 2nd, 2022, 11:16:36 AM
3 Changes
Model Config: 1
Wireless: 1
+1 more

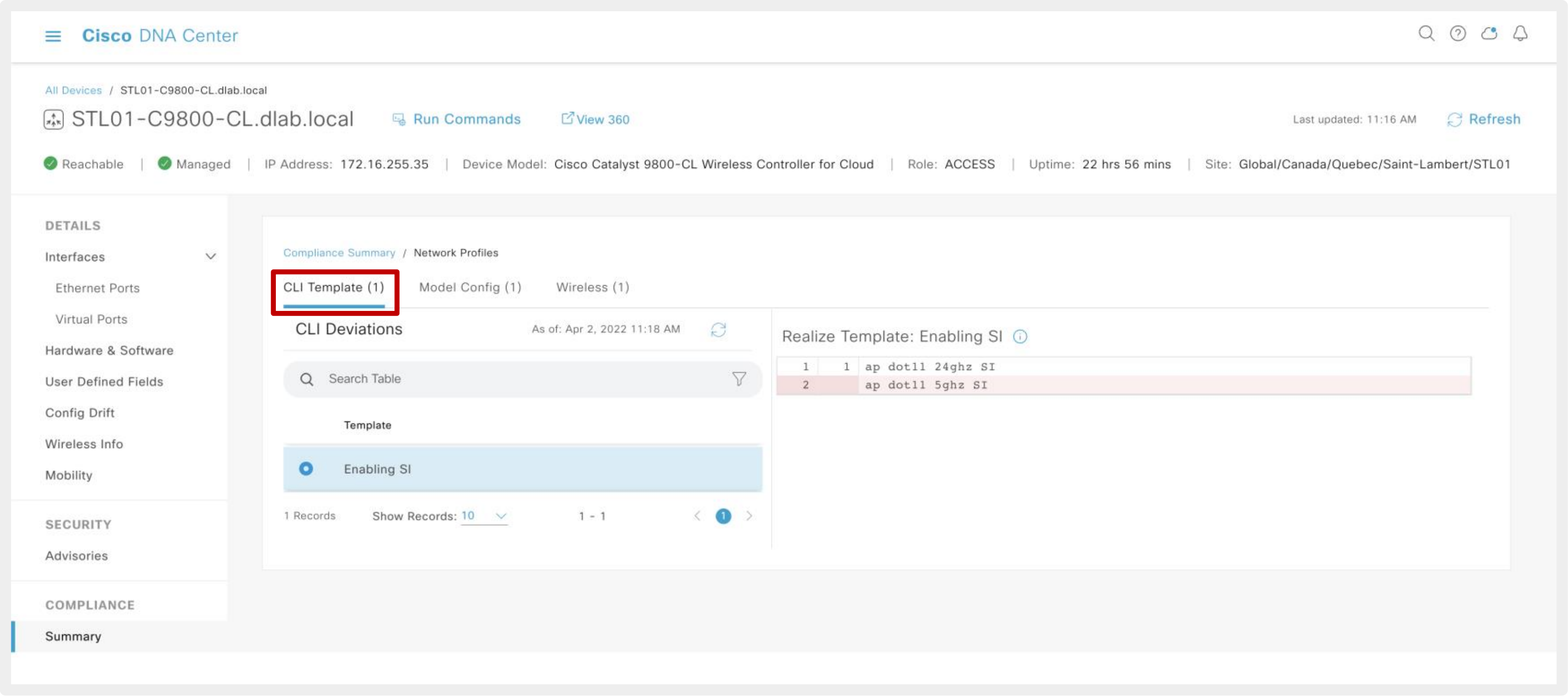
✓ Application Visibility
Compliant since Apr 2nd, 2022, 11:16:54 AM
Compliance last run on: Apr 2nd, 2022, 11:16:54 AM
0 Changes

✓ Software Image
Compliant since Feb 3rd, 2022, 05:10:45 PM
Compliance last run on: Apr 2nd, 2022, 11:16:36 AM
17.07.01 Golden Image Version
Running Version: **17.7.1**

✓ Critical Security Advisories
Compliant since Feb 8th, 2022, 07:00:11 PM
Compliance last run on: Apr 2nd, 2022, 11:16:36 AM
0

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

Compliance: Network Profiles - Wireless



STL01-C9800-CL.dlab.local

Last updated: 11:16 AM

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

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

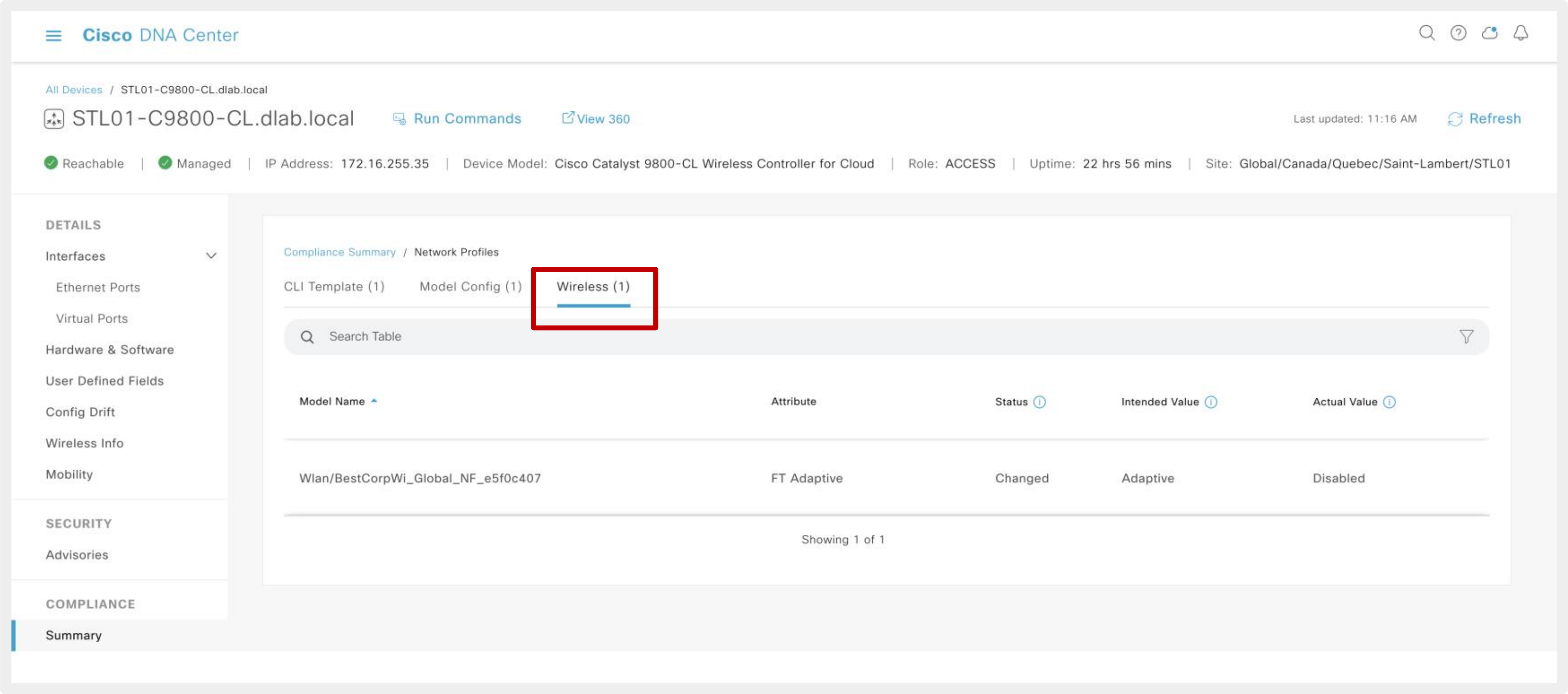
● Enabling SI

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



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

STL01-C9800-CL.dlab.local

Last updated: 11:16 AM

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

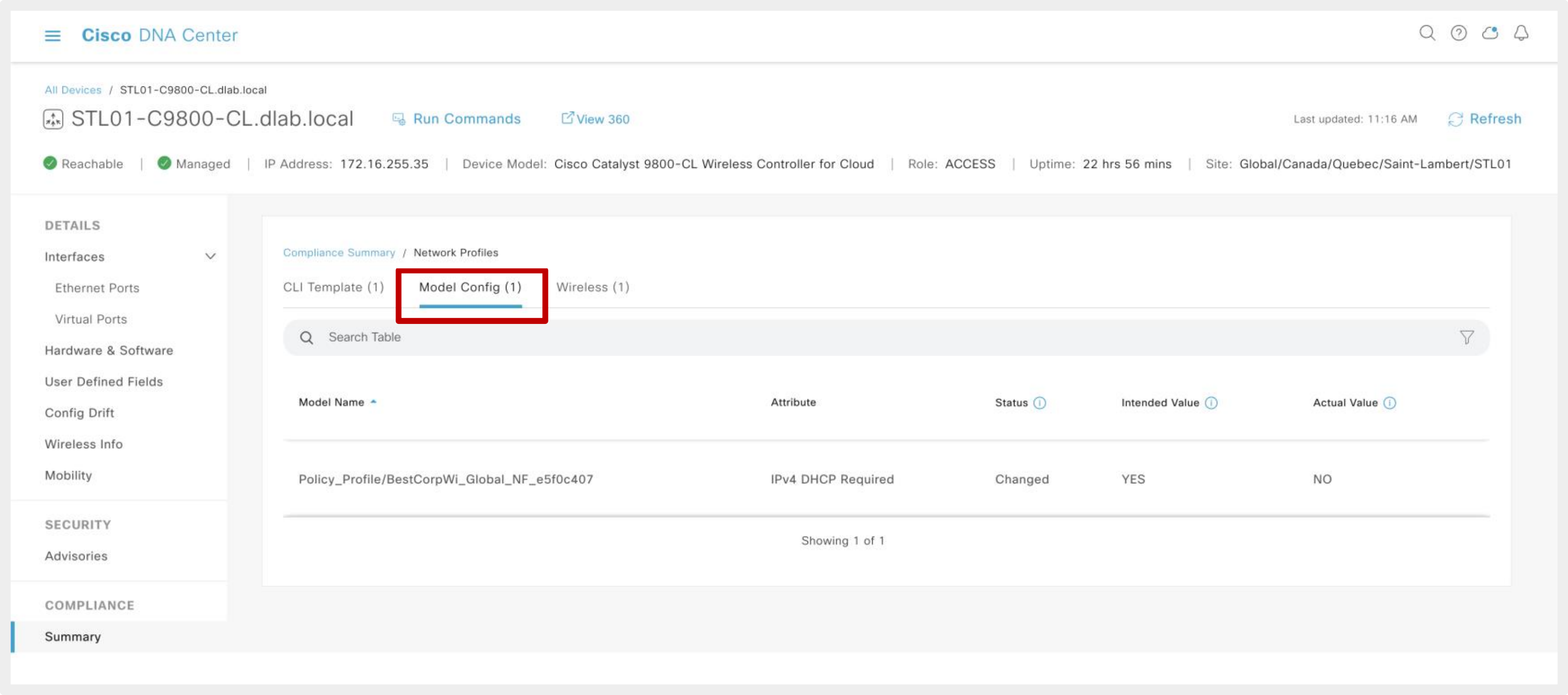
Compliance Summary / Network Profiles

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

Showing 1 of 1

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

Compliance: Network Profiles - Wireless



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

STL01-C9800-CL.dlab.local

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

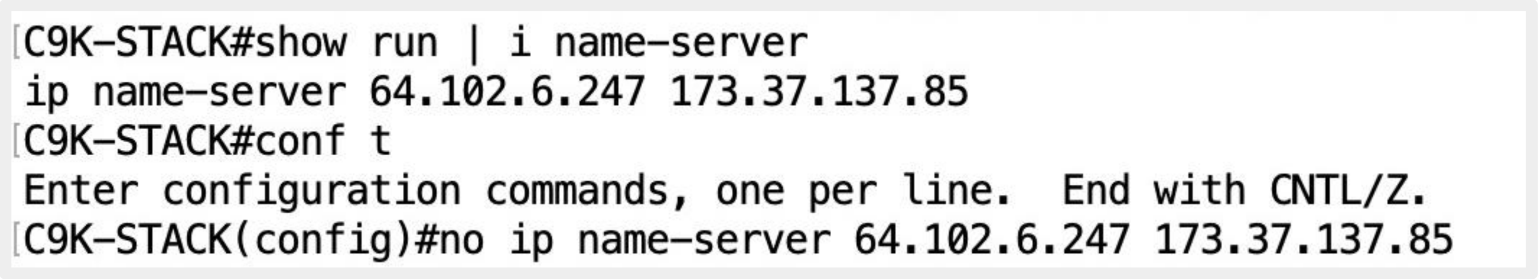
Compliance Summary / Network Profiles

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

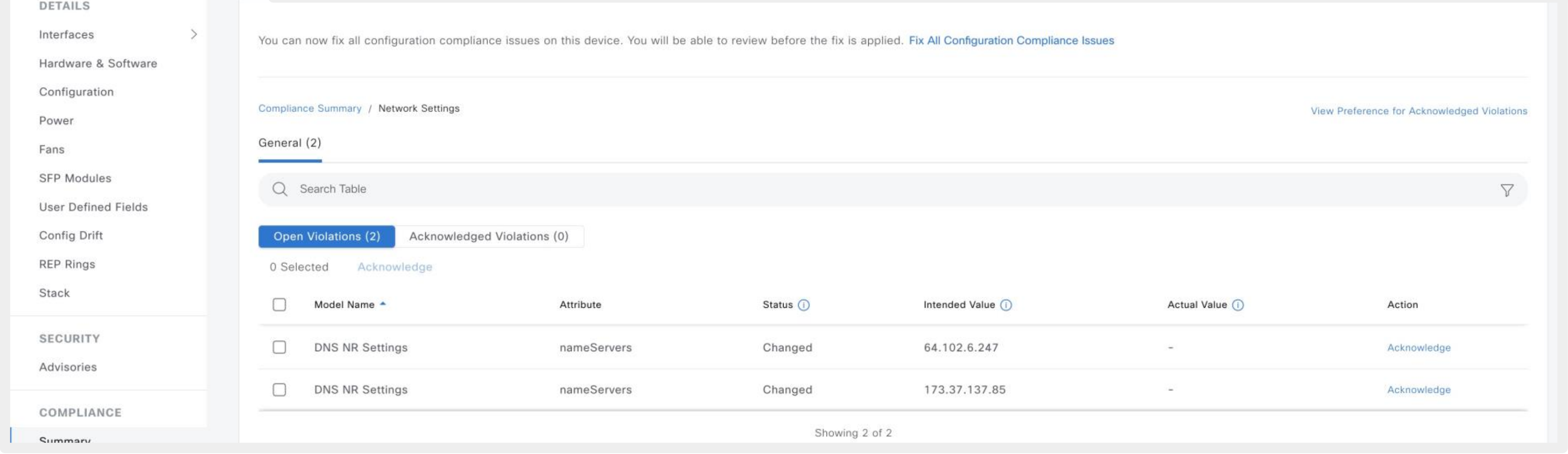
Showing 1 of 1

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

Network Setting Compliance



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



All Devices / C9K-STACK

C9K-STACK   Run C

● Reachable | ●Managed | IP Add

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

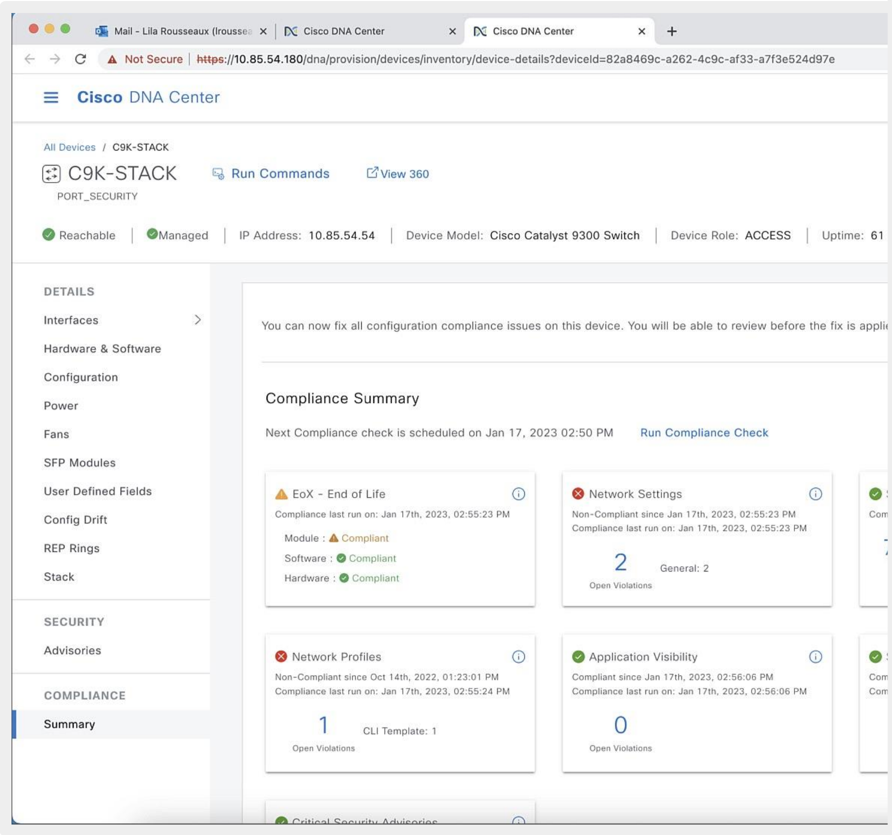
Open Violations (2)   Acknowledged Violations (0)

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



https://10.85.54.180/dna/provision/devices/inventory/device-details?deviceId=82a8469c-a262-4c9c-af33-a7f3e524d97e

All Devices / C9K-STACK

C9K-STACK Run Commands View 360

PORT_SECURITY

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

You can now fix all configuration compliance issues on this device. You will be able to review before the fix is appli

Compliance Summary

Next Compliance check is scheduled on Jan 17, 2023 02:50 PM Run Compliance Check

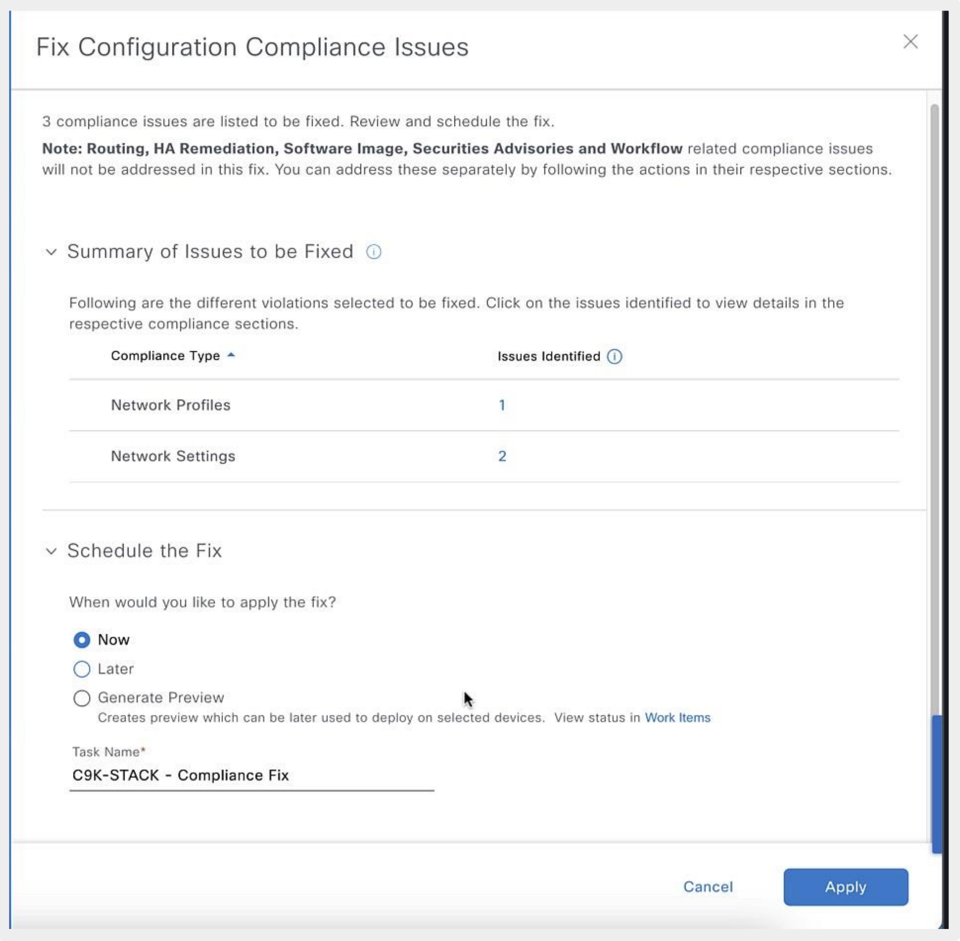
EoX - End of Life
Compliance last run on: Jan 17th, 2023, 02:55:23 PM
Module : Compliant
Software : Compliant
Hardware : Compliant

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

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

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

Critical Security Advisories



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?

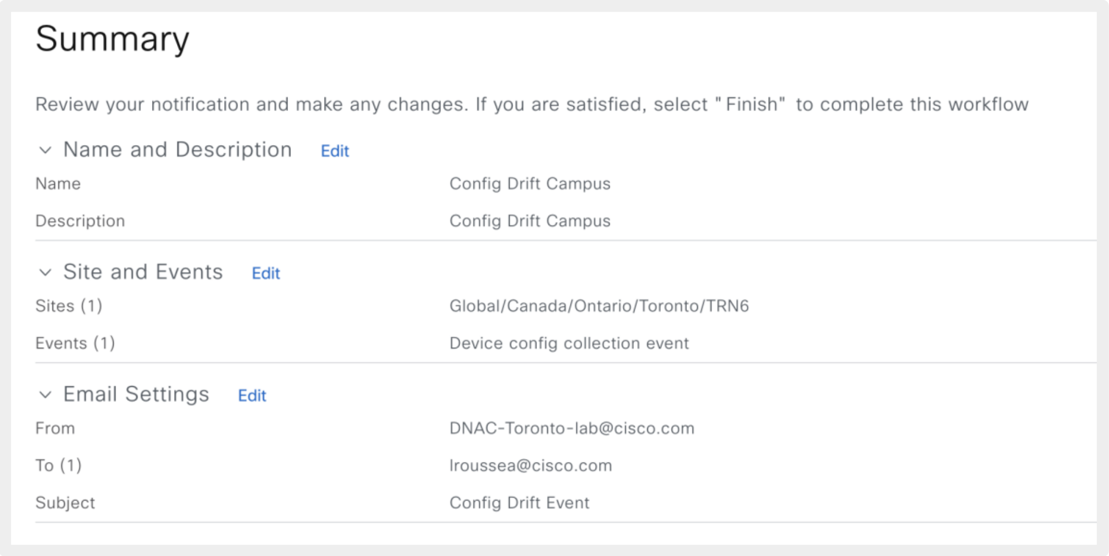
● Now
○ Later
○ Generate Preview
Creates preview which can be later used to deploy on selected devices. View status in Work Items

Task Name*: C9K-STACK - Compliance Fix

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

Network Compliance Event Notification

- When a config change happens to a device, there will be a respective config drift in Cisco Catalyst Center
- With Catalyst Center 2.3.7, config drift will send an event through notification channels
- 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	Config Drift Campus
Description	Config Drift Campus

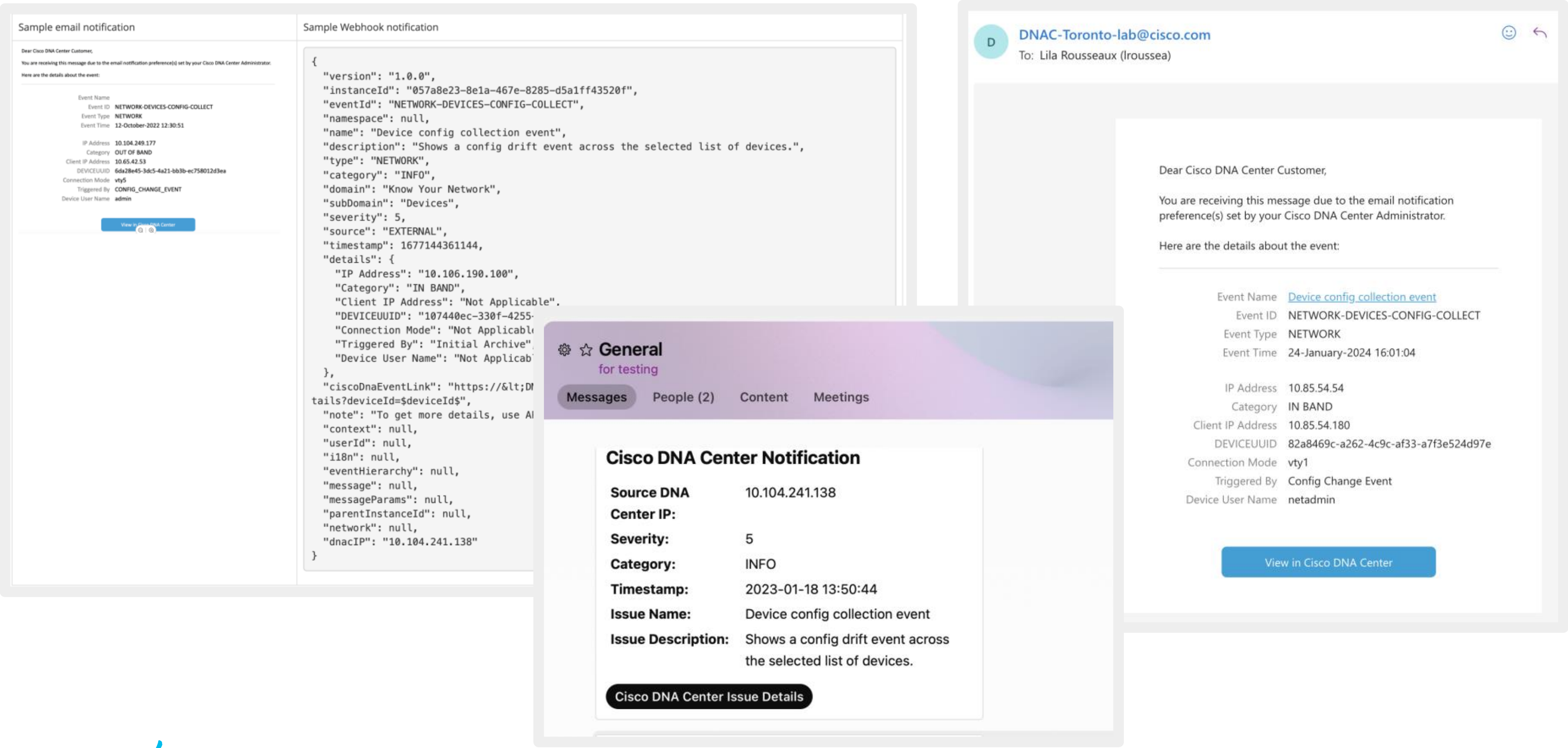
Sites (1)	Global/Canada/Ontario/Toronto/TRN6
Events (1)	Device config collection event

From	DNAC-Toronto-lab@cisco.com
To (1)	lroussea@cisco.com
Subject	Config Drift Event

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

Network Compliance Event Notification

For your 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	
Event ID	NETWORK-DEVICES-CONFIG-COLLECT
Event Type	NETWORK
Event Time	12-October-2022 12:30:51
IP Address	10.104.249.177
Category	OUT OF BAND
Client IP Address	10.65.42.53
DEVICEUUID	6da28e45-3dc5-4a21-bb3b-ec758012d3ea
Connection Mode	vty5
Triggered By	CONFIG_CHANGE_EVENT
Device User Name	admin

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"
}
```

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.

DNAC-Toronto-lab@cisco.com
To: Lila Rousseaux (lroussea)

Dear Cisco DNA Center Customer,

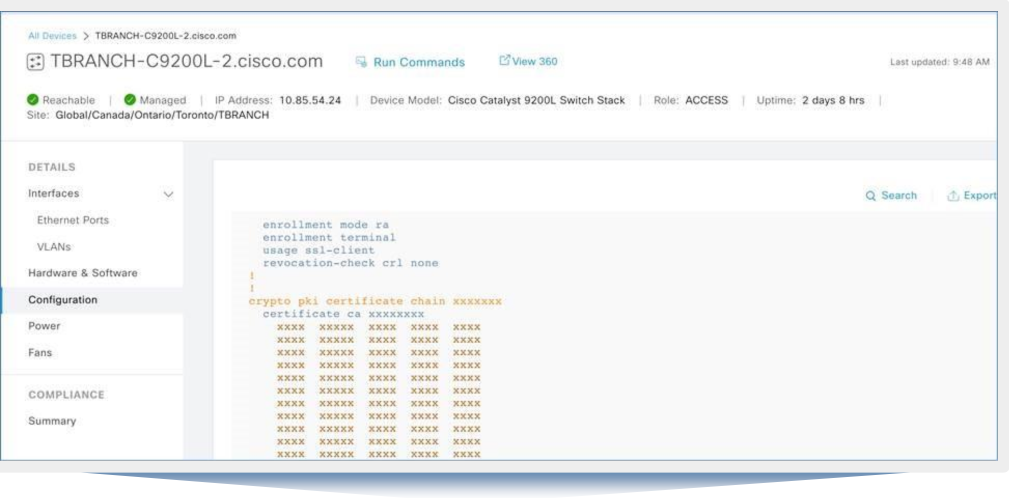
You are receiving this message due to the email notification preference(s) set by your Cisco DNA Center Administrator.

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

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

Device Configuration Management



Reachable | Managed | IP Address: 10.85.54.24 | Device Model: Cisco Catalyst 9200L Switch Stack | Role: ACCESS | Uptime: 2 days 8 hrs |
Site: Global/Canada/Ontario/Toronto/TBRANCH

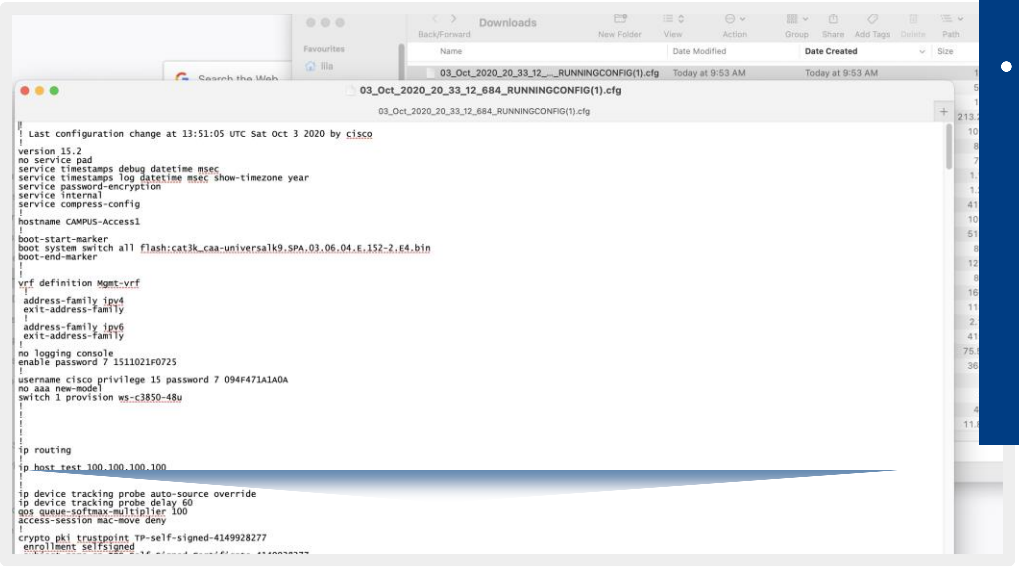
```
  enrollment mode ra
  enrollment terminal
  usage ssl-client
  revocation-check crl none
!
!
crypto pki certificate chain xxxxxxx
  certificate ca xxxxxxxx
    xxxx  xxxxx  xxxx  xxxx  xxxx
    xxxx  xxxxx  xxxx  xxxx  xxxx
    xxxx  xxxxx  xxxx  xxxx  xxxx
    xxxx  xxxxx  xxxx  xxxx  xxxx
    xxxx  xxxxx  xxxx  xxxx  xxxx
    xxxx  xxxxx  xxxx  xxxx  xxxx
    xxxx  xxxxx  xxxx  xxxx  xxxx
    xxxx  xxxxx  xxxx  xxxx  xxxx
    xxxx  xxxxx  xxxx  xxxx  xxxx
    xxxx  xxxxx  xxxx  xxxx  xxxx
    xxxx  xxxxx  xxxx  xxxx  xxxx
```

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

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

Device Configuration Management

API's to retrieve device configuration



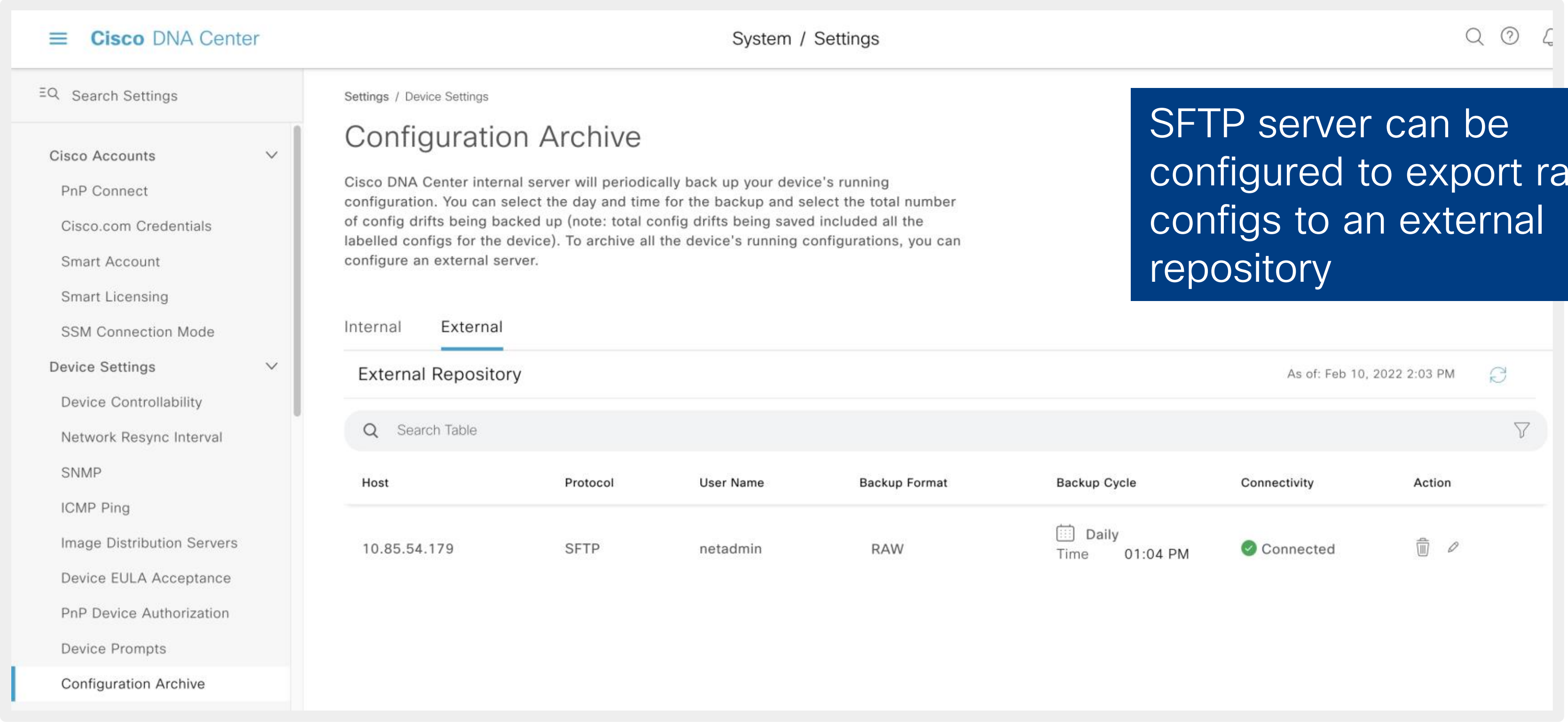
```
!
! Last configuration change at 13:51:05 UTC Sat Oct 3 2020 by cisco
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec show-timezone year
service password-encryption
service internal
service compress-config
!
hostname CAMPUS-Access1
!
boot-start-marker
boot system switch all flash:cat3k_caa-universalk9.SPA.03.06.04.E.152-2.E4.bin
boot-end-marker
!
!
vrf definition Mgmt-vrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
no logging console
enable password 7 1511021F0725
!
username cisco privilege 15 password 7 094F471A1A0A
no aaa new-model
switch 1 provision ws-c3850-48u
!
!
!
!
!
ip routing
!
ip host test 100.100.100.100
!
!
ip device tracking probe auto-source override
ip device tracking probe delay 60
qos queue-softmax-multiplier 100
access-session mac-move deny
!
crypto pki trustpoint TP-self-signed-4149928277
 enrollment selfsigned
```

- 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

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

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.

External Repository

As of: Feb 10, 2022 2:03 PM

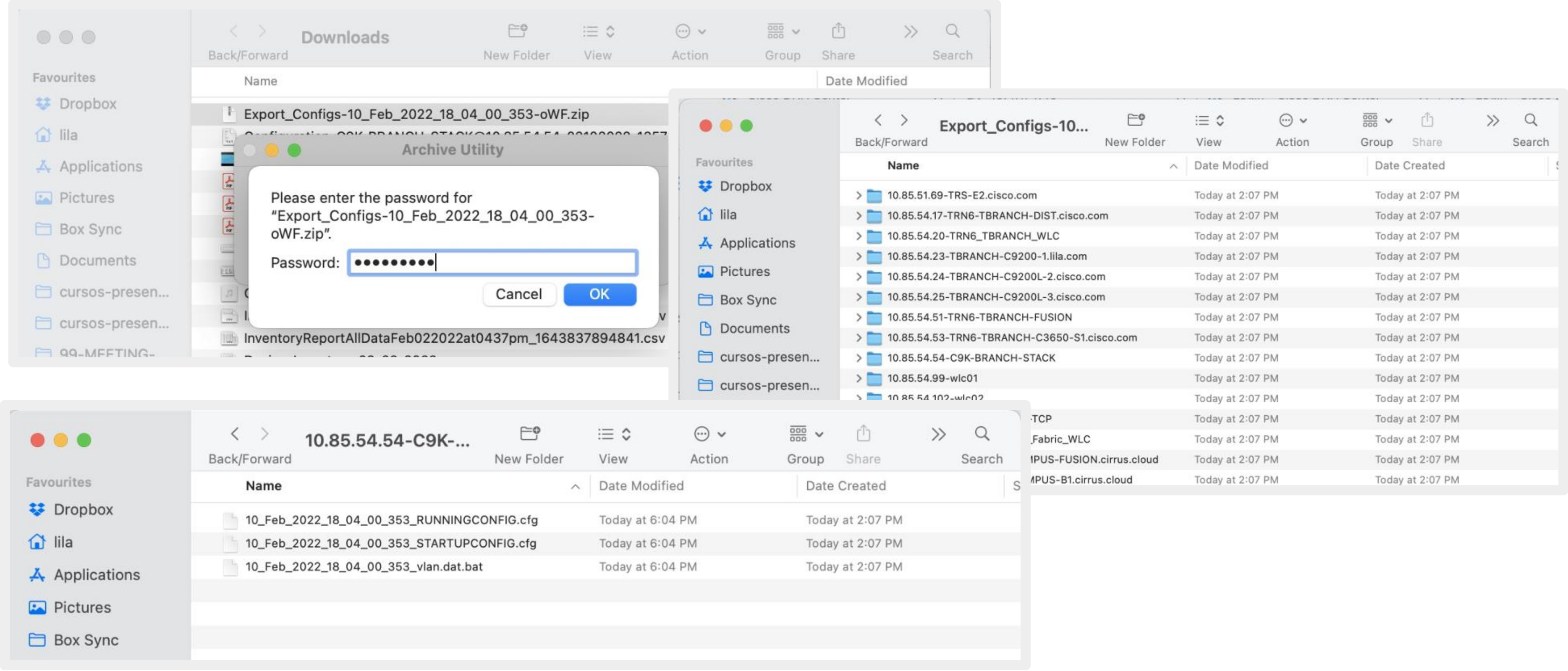
Host	Protocol	User Name	Backup Format	Backup Cycle	Connectivity	Action
10.85.54.179	SFTP	netadmin	RAW	Daily Time 01:04 PM	Connected	

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

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

Device Configuration Management

Configuration Archive



Name	Date Modified
Export_Configs-10_Feb_2022_18_04_00_353-oWF.zip	
InventoryReportAllDataFeb022022at0437pm_1643837894841.csv	

Archive Utility

Please enter the password for "Export_Configs-10_Feb_2022_18_04_00_353-oWF.zip".

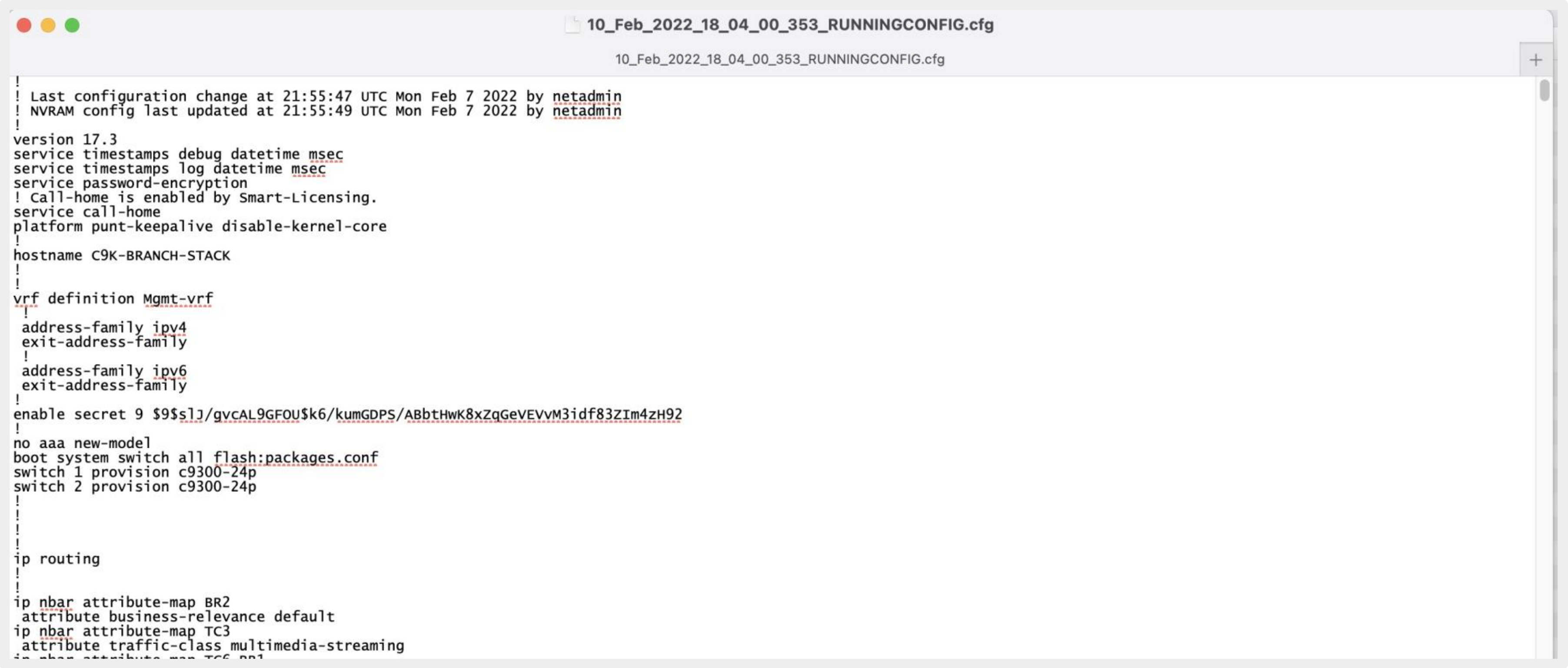
Password: ●●●●●●●●●●

Name	Date Modified	Date Created
10.85.51.69-TRS-E2.cisco.com	Today at 2:07 PM	Today at 2:07 PM
10.85.54.17-TRN6-TBRANCH-DIST.cisco.com	Today at 2:07 PM	Today at 2:07 PM
10.85.54.20-TRN6_TBRANCH_WLC	Today at 2:07 PM	Today at 2:07 PM
10.85.54.23-TBRANCH-C9200-1.lila.com	Today at 2:07 PM	Today at 2:07 PM
10.85.54.24-TBRANCH-C9200L-2.cisco.com	Today at 2:07 PM	Today at 2:07 PM
10.85.54.25-TBRANCH-C9200L-3.cisco.com	Today at 2:07 PM	Today at 2:07 PM
10.85.54.51-TRN6-TBRANCH-FUSION	Today at 2:07 PM	Today at 2:07 PM
10.85.54.53-TRN6-TBRANCH-C3650-S1.cisco.com	Today at 2:07 PM	Today at 2:07 PM
10.85.54.54-C9K-BRANCH-STACK	Today at 2:07 PM	Today at 2:07 PM
10.85.54.99-wlc01	Today at 2:07 PM	Today at 2:07 PM
10.85.54.102-wlc02	Today at 2:07 PM	Today at 2:07 PM
TCP	Today at 2:07 PM	Today at 2:07 PM
Fabric_WLC	Today at 2:07 PM	Today at 2:07 PM
MPUS-FUSION.cirrus.cloud	Today at 2:07 PM	Today at 2:07 PM
MPUS-B1.cirrus.cloud	Today at 2:07 PM	Today at 2:07 PM

Name	Date Modified	Date Created
10_Feb_2022_18_04_00_353_RUNNINGCONFIG.cfg	Today at 6:04 PM	Today at 2:07 PM
10_Feb_2022_18_04_00_353_STARTUPCONFIG.cfg	Today at 6:04 PM	Today at 2:07 PM
10_Feb_2022_18_04_00_353_vlan.dat.bat	Today at 6:04 PM	Today at 2:07 PM

Device Configuration Management

Configuration Archive



10_Feb_2022_18_04_00_353_RUNNINGCONFIG.cfg
10_Feb_2022_18_04_00_353_RUNNINGCONFIG.cfg
+

```
!
! Last configuration change at 21:55:47 UTC Mon Feb 7 2022 by netadmin
! NVRAM config last updated at 21:55:49 UTC Mon Feb 7 2022 by netadmin
!
version 17.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
! Call-home is enabled by Smart-Licensing.
service call-home
platform punt-keepalive disable-kernel-core
!
hostname C9K-BRANCH-STACK
!
!
vrf definition Mgmt-vrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable secret 9 $9$slJ/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
ip nbar attribute-map TC6 BR1
```

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

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

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

Software Upgrade Recommendations

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

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

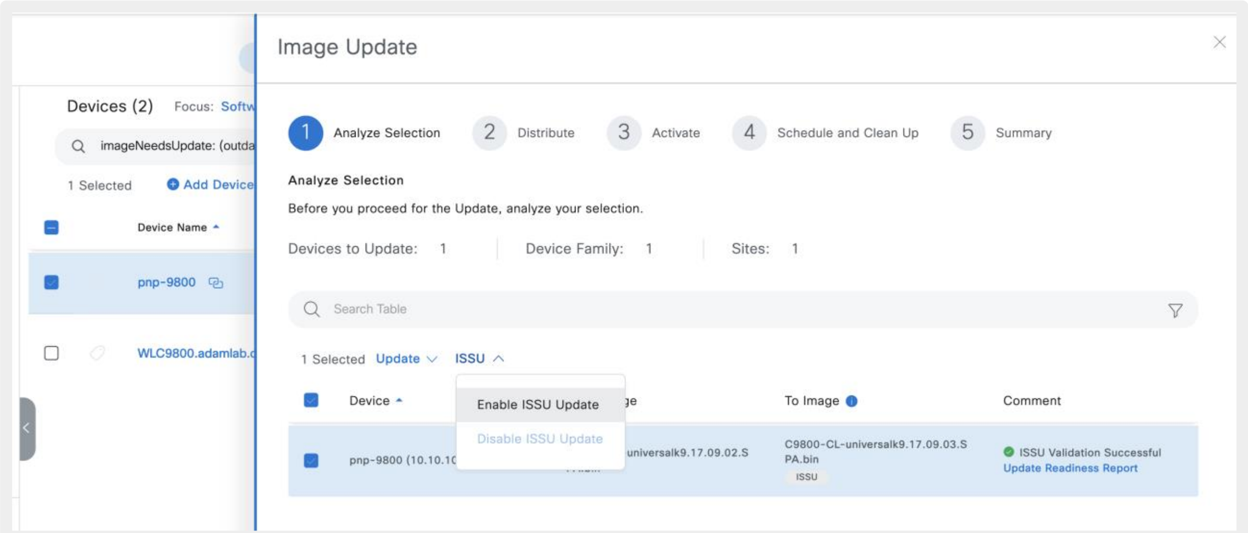
Control over SWIM- ISSU

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



Devices (2) Focus: Softw

imageNeedsUpdate: (outda

1 Selected ⊕ Add Device

☑	Device Name ▲
☑	pnp-9800
□	WLC9800.adamlab.c

Image Update

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

Analyze Selection

Before you proceed for the Update, analyze your selection.

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

Search Table

1 Selected Update ISSU

- Enable ISSU Update
- Disable ISSU Update

☑	Device ▲	…ge	To Image	Comment
☑	pnp-9800 (10.10.1…	…universalk9.17.09.02.S	C9800-CL-universalk9.17.09.03.S PA.bin ISSU	ISSU Validation Successful Update Readiness Report

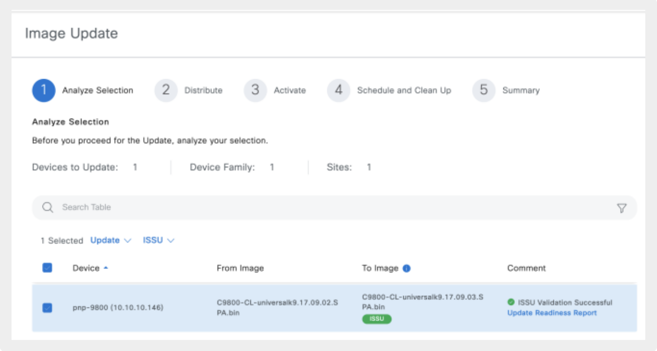


Image Update

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

Analyze Selection

Before you proceed for the Update, analyze your selection.

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

Search Table

1 Selected Update ISSU

☑	Device ▲	From Image	To Image	Comment
☑	pnp-9800 (10.10.10.146)	C9800-CL-universalk9.17.09.02.S PA.bin	C9800-CL-universalk9.17.09.03.S PA.bin ISSU	ISSU Validation Successful Update Readiness Report

Ready to go ISSU

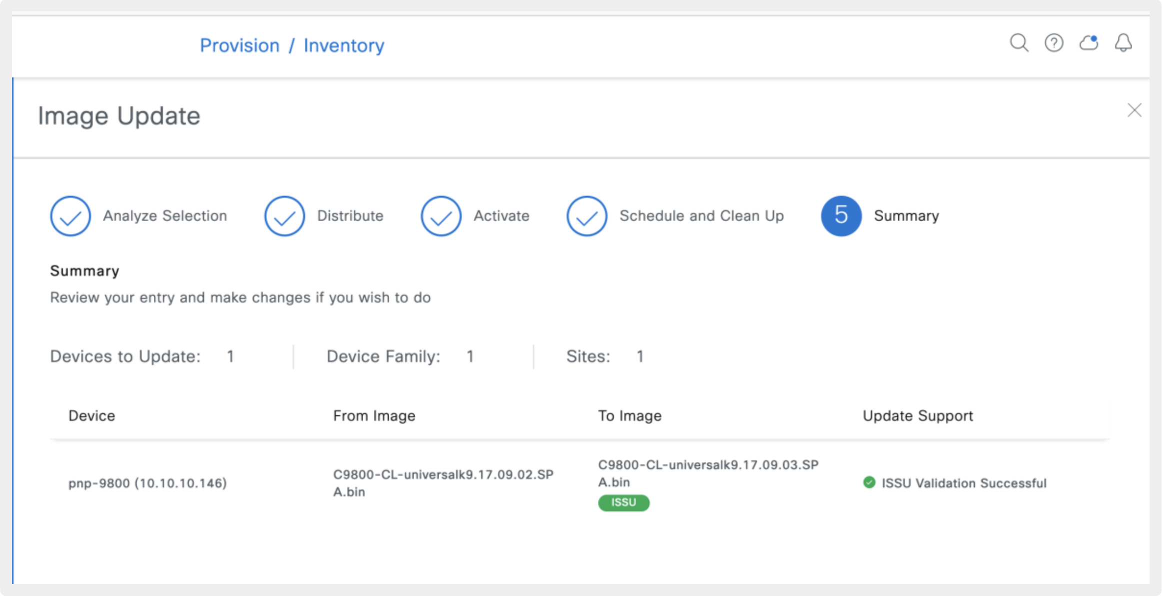


Image Update

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.SPA.bin	C9800-CL-universalk9.17.09.03.SPA.bin ISSU	● ISSU Validation Successful

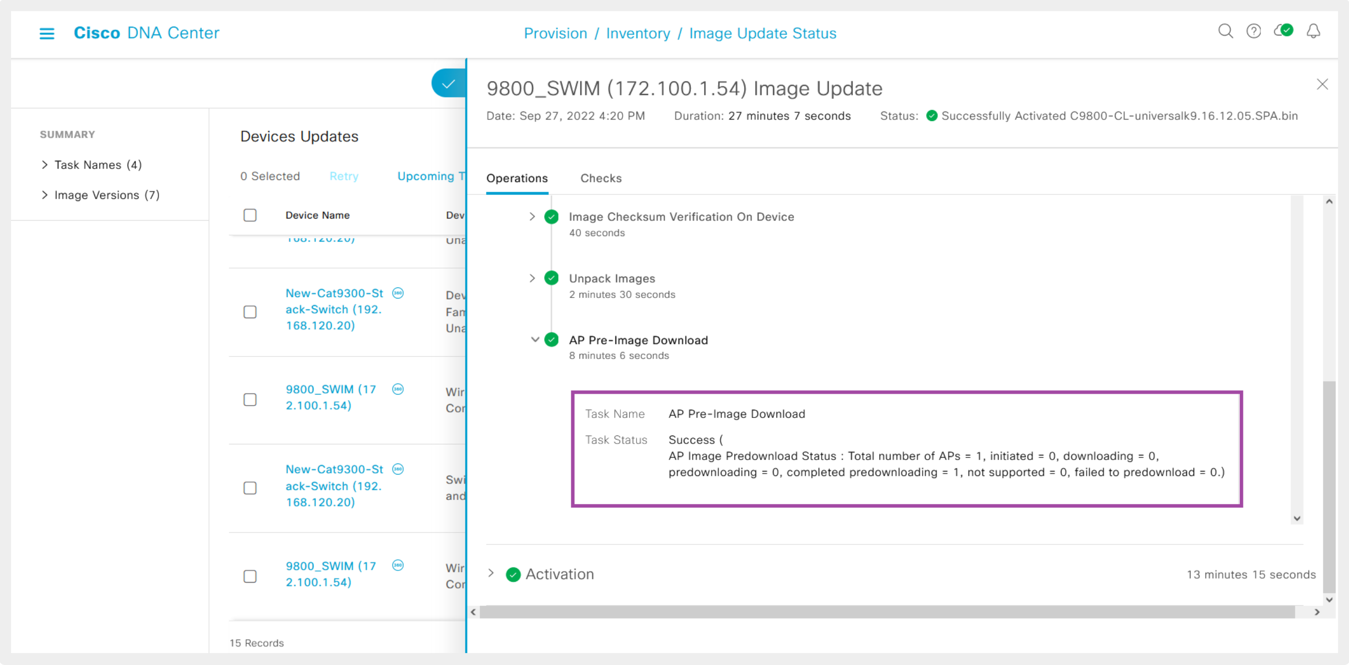
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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



New-Cat9300-Stack-Switch (192.168.120.20)

9800_SWIM (172.100.1.54)

New-Cat9300-Stack-Switch (192.168.120.20)

9800_SWIM (172.100.1.54)

15 Records

9800_SWIM (172.100.1.54) Image Update

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

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

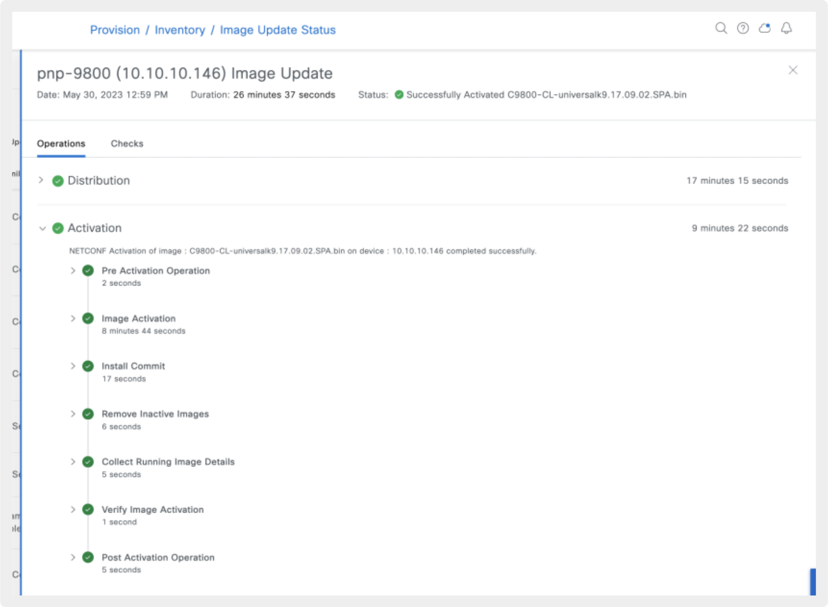
Task Name AP Pre-Image Download

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

- Activation 13 minutes 15 seconds

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

Activation for normal wireless vs ISSU wireless



Provision / Inventory / Image Update Status

pnp-9800 (10.10.10.146) Image Update

Date: May 30, 2023 12:59 PM Duration: 26 minutes 37 seconds Status: ✓ Successfully Activated C9800-CL-universalk9.17.09.02.SPA.bin

Operations Checks

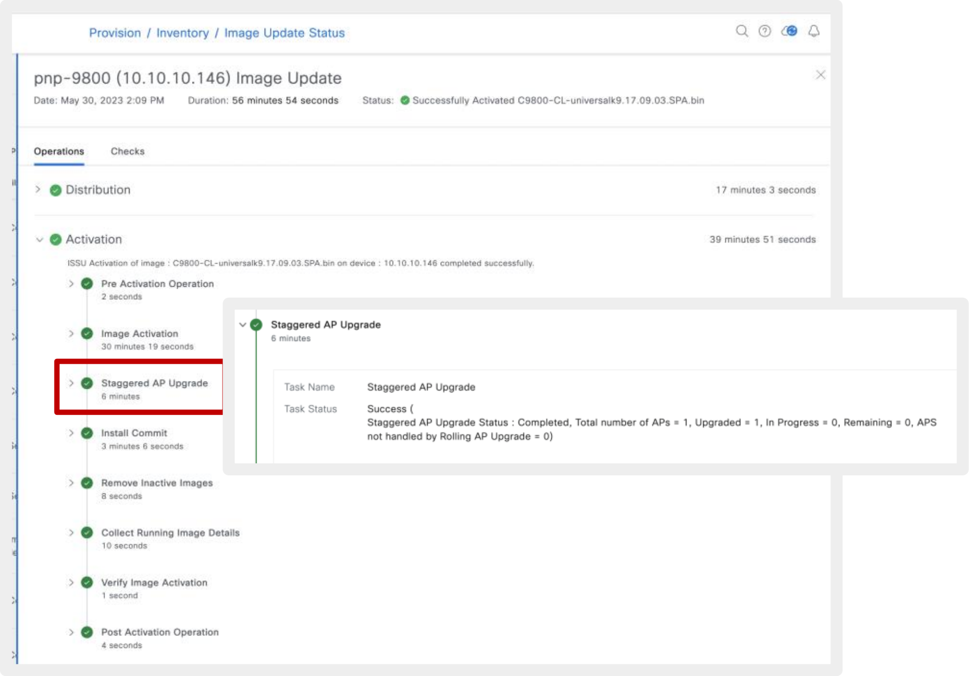
› ✓ Distribution 17 minutes 15 seconds

⌄ ✓ Activation 9 minutes 22 seconds

NETCONF Activation of image : C9800-CL-universalk9.17.09.02.SPA.bin on device : 10.10.10.146 completed successfully.

- › ✓ Pre Activation Operation
  2 seconds
- › ✓ Image Activation
  8 minutes 44 seconds
- › ✓ Install Commit
  17 seconds
- › ✓ Remove Inactive Images
  6 seconds
- › ✓ Collect Running Image Details
  5 seconds
- › ✓ Verify Image Activation
  1 second
- › ✓ Post Activation Operation
  5 seconds

Normal Activation



Provision / Inventory / Image Update Status

pnp-9800 (10.10.10.146) Image Update

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

Operations Checks

› ✓ Distribution 17 minutes 3 seconds

⌄ ✓ Activation 39 minutes 51 seconds

ISSU Activation of image : C9800-CL-universalk9.17.09.03.SPA.bin on device : 10.10.10.146 completed successfully.

- › ✓ Pre Activation Operation
  2 seconds
- › ✓ Image Activation
  30 minutes 19 seconds
- › ✓ Staggered AP Upgrade
  6 minutes
- › ✓ Install Commit
  3 minutes 6 seconds
- › ✓ Remove Inactive Images
  8 seconds
- › ✓ Collect Running Image Details
  10 seconds
- › ✓ Verify Image Activation
  1 second
- › ✓ Post Activation Operation
  4 seconds

⌄ ✓ Staggered AP Upgrade
6 minutes

Task Name Staggered AP Upgrade

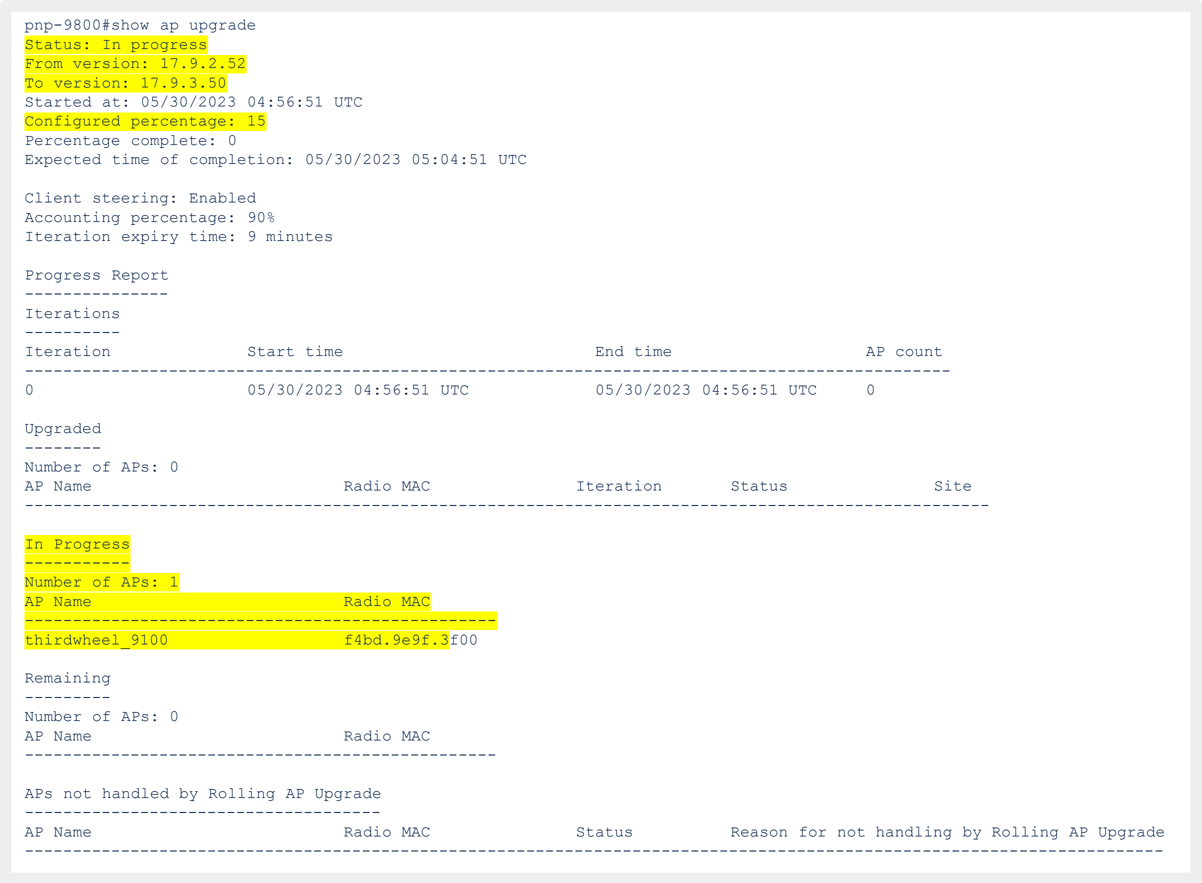
Task Status Success (
Staggered AP Upgrade Status : Completed, Total number of APs = 1, Upgraded = 1, In Progress = 0, Remaining = 0, APS not handled by Rolling AP Upgrade = 0)

ISSU Activation

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

Staggered Upgrade

For your reference

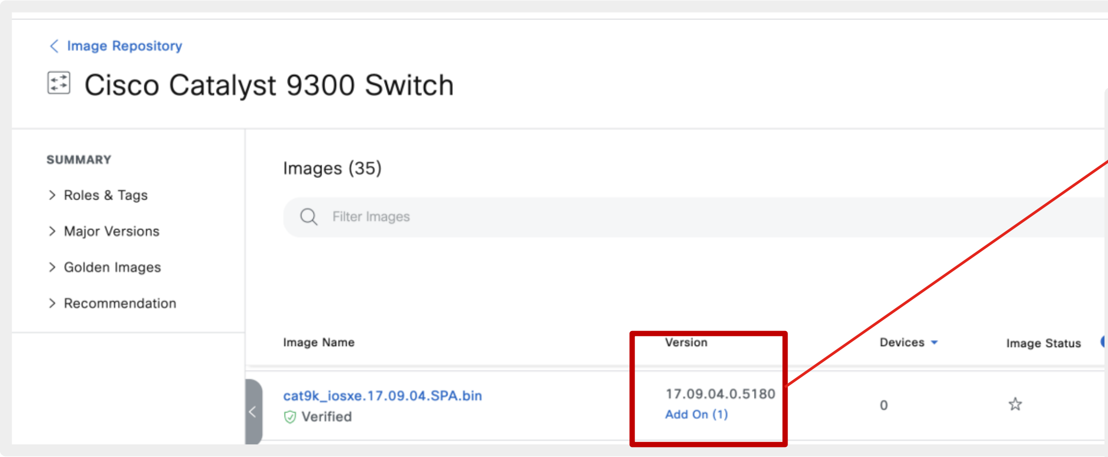


```
pnp-9800#show ap upgrade
Status: In progress
From version: 17.9.2.52
To version: 17.9.3.50
Started at: 05/30/2023 04:56:51 UTC
Configured percentage: 15
Percentage complete: 0
Expected time of completion: 05/30/2023 05:04:51 UTC

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

Progress Report
---------------
Iterations
----------
Iteration              Start time                           End time                    AP count
-------------------------------------------------------------------------------------------------
0                      05/30/2023 04:56:51 UTC              05/30/2023 04:56:51 UTC     0

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

In Progress
-----------
Number of APs: 1
AP Name                          Radio MAC
-------------------------------------------------
thirdwheel_9100                  f4bd.9e9f.3f00

Remaining
---------
Number of APs: 0
AP Name                          Radio MAC
-------------------------------------------------

APs not handled by Rolling AP Upgrade
-------------------------------------
AP Name                          Radio MAC                Status          Reason for not handling by Rolling AP Upgrade
-----------------------------------------------------------------------------------------------------------------------
```

cisco Live!

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

Software Maintenance Update (SMU) support



< Image Repository

Cisco Catalyst 9300 Switch

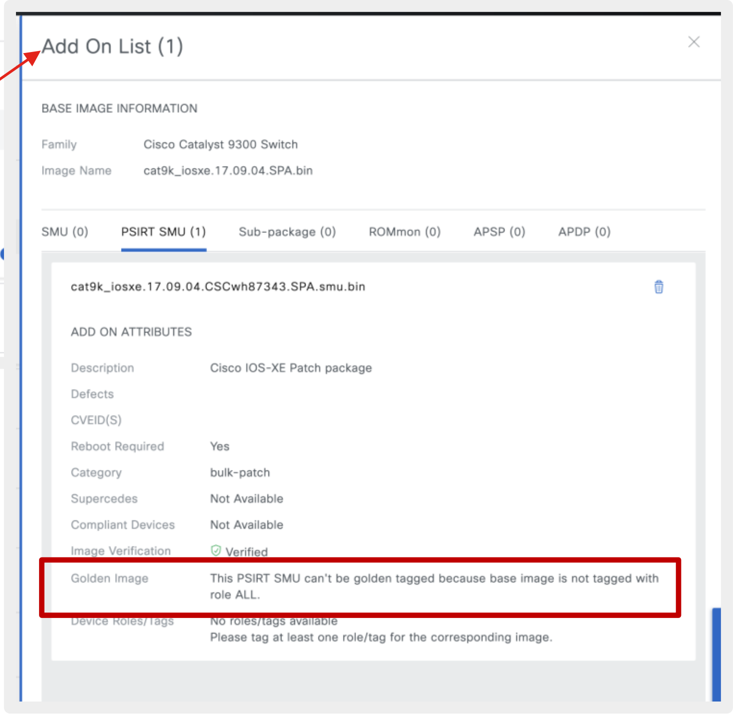
SUMMARY

- > Roles & Tags
- > Major Versions
- > Golden Images
- > Recommendation

Images (35)

Filter Images

Image Name	Version	Devices	Image Status
cat9k_iosxe.17.09.04.SPA.bin Verified	17.09.04.0.5180 Add On (1)	0	☆



Add On List (1)

BASE IMAGE INFORMATION

Family Cisco Catalyst 9300 Switch

Image Name cat9k_iosxe.17.09.04.SPA.bin

cat9k_iosxe.17.09.04.CSCwh87343.SPA.smu.bin

ADD ON ATTRIBUTES

Description	Cisco IOS-XE Patch package
Defects	
CVEID(S)	
Reboot Required	Yes
Category	bulk-patch
Supercedes	Not Available
Compliant Devices	Not Available
Image Verification	Verified
Golden Image	This PSIRT SMU can't be golden tagged because base image is not tagged with role ALL.
Device Roles/Tags	No roles/tags available Please tag at least one role/tag for the corresponding image.

Need to mark as golden (along with main image)

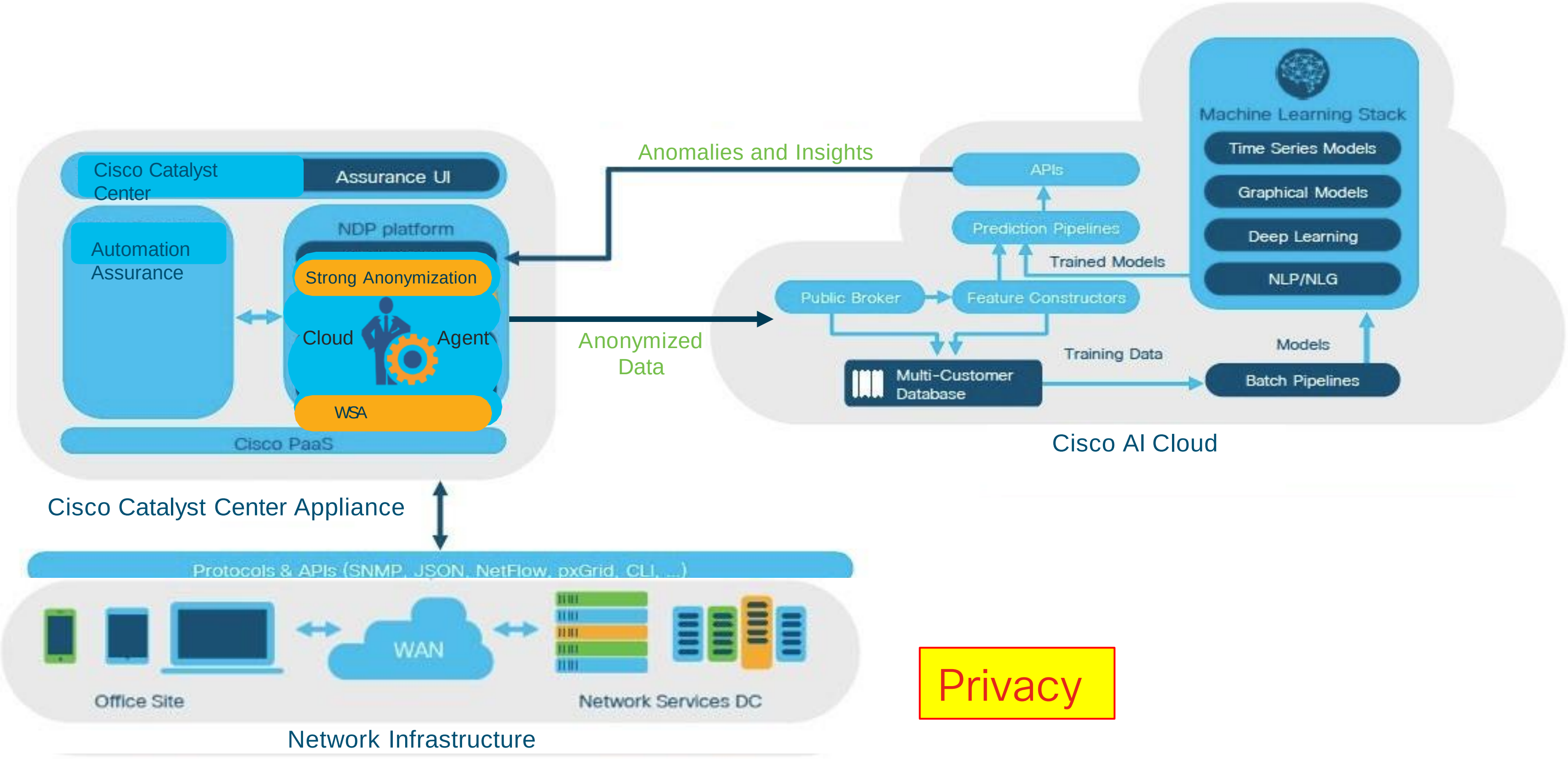
Downloadable direct from CCO

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

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

Habit #5 - Explore Proactive insights with AI/ML

Cisco AI Network Analytics Architecture



Privacy

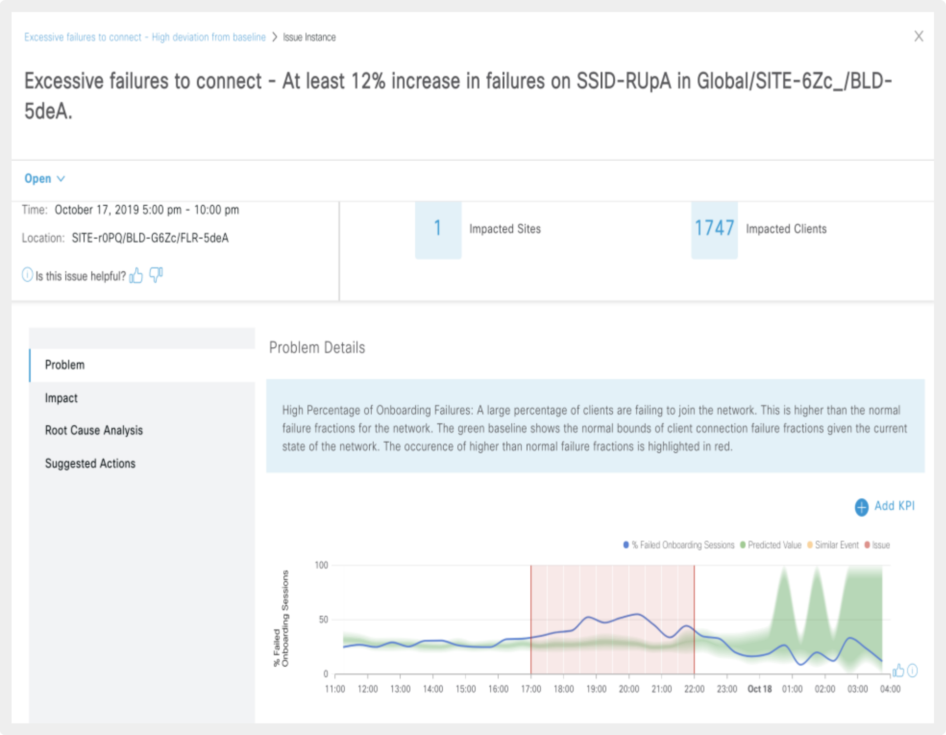
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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



Excessive failures to connect - High deviation from baseline > Issue Instance

Excessive failures to connect - At least 12% increase in failures on SSID-RUpA in Global/SITE-6Zc_/BLD-5deA.

Open

Time: October 17, 2019 5:00 pm - 10:00 pm

Location: SITE-r0PQ/BLD-G6Zc/FLR-5deA

Is this issue helpful?

1 Impacted Sites

1747 Impacted Clients

Problem Details

High Percentage of Onboarding Failures: A large percentage of clients are failing to join the network. This is higher than the normal failure fractions for the network. The green baseline shows the normal bounds of client connection failure fractions given the current state of the network. The occurence of higher than normal failure fractions is highlighted in red.

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

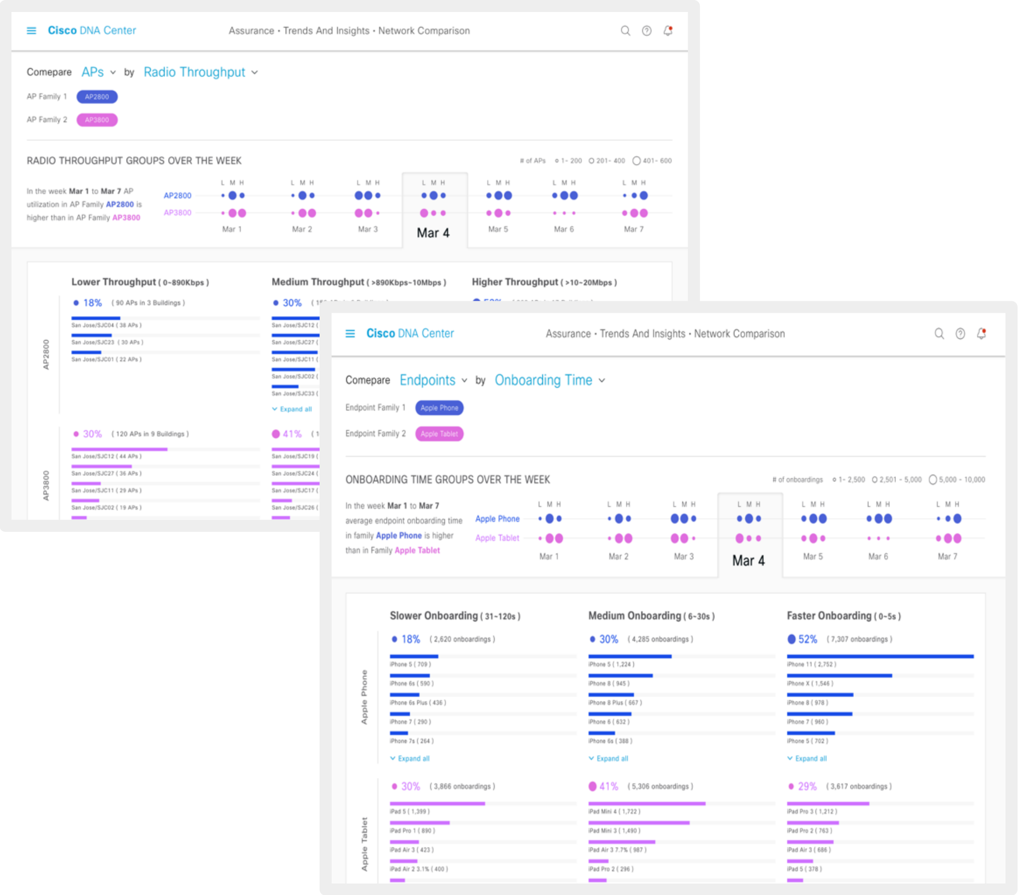
AI Analytics – AP Family & Endpoint Comparison

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..



Comepare APs by Radio Throughput

AP Family 1: AP2800
AP Family 2: AP3800

RADIO THROUGHPUT GROUPS OVER THE WEEK

In the week **Mar 1** to **Mar 7** AP utilization in AP Family **AP2800** is higher than in AP Family **AP3800**

Lower Throughput (0~890Kbps)

18% (90 APs in 3 Buildings)

San Jose/SJC04 (38 APs)
San Jose/SJC23 (30 APs)
San Jose/SJC01 (22 APs)

30% (120 APs in 9 Buildings)

San Jose/SJC12 (44 APs)
San Jose/SJC27 (36 APs)
San Jose/SJC11 (29 APs)
San Jose/SJC02 (19 APs)

Medium Throughput (>890Kbps~10Mbps)

30%

San Jose/SJC12 (
San Jose/SJC27 (
San Jose/SJC11 (
San Jose/SJC02 (
San Jose/SJC33 (

41%

San Jose/SJC19 (
San Jose/SJC24 (
San Jose/SJC17 (
San Jose/SJC26 (

Higher Throughput (>10~20Mbps)

Comepare Endpoints by Onboarding Time

Endpoint Family 1: Apple Phone
Endpoint Family 2: Apple Tablet

ONBOARDING TIME GROUPS OVER THE WEEK

In the week **Mar 1** to **Mar 7** average endpoint onboarding time in family **Apple Phone** is higher than in Family **Apple Tablet**

Slower Onboarding (31~120s)

18% (2,620 onboardings)

iPhone 5 (709)
iPhone 6s (590)
iPhone 6s Plus (436)
iPhone 7 (290)
iPhone 7s (264)

30% (3,866 onboardings)

iPad 5 (1,399)
iPad Pro 1 (890)
iPad Air 3 (423)
iPad Air 2 3.1% (400)

Medium Onboarding (6~30s)

30% (4,285 onboardings)

iPhone 5 (1,224)
iPhone 8 (945)
iPhone 8 Plus (667)
iPhone 6 (632)
iPhone 6s (388)

41% (5,306 onboardings)

iPad Mini 4 (1,722)
iPad Mini 3 (1,490)
iPad Air 3 7.7% (987)
iPad Pro 2 (296)

Faster Onboarding (0~5s)

52% (7,307 onboardings)

iPhone 11 (2,752)
iPhone X (1,546)
iPhone 8 (978)
iPhone 7 (960)
iPhone 5 (702)

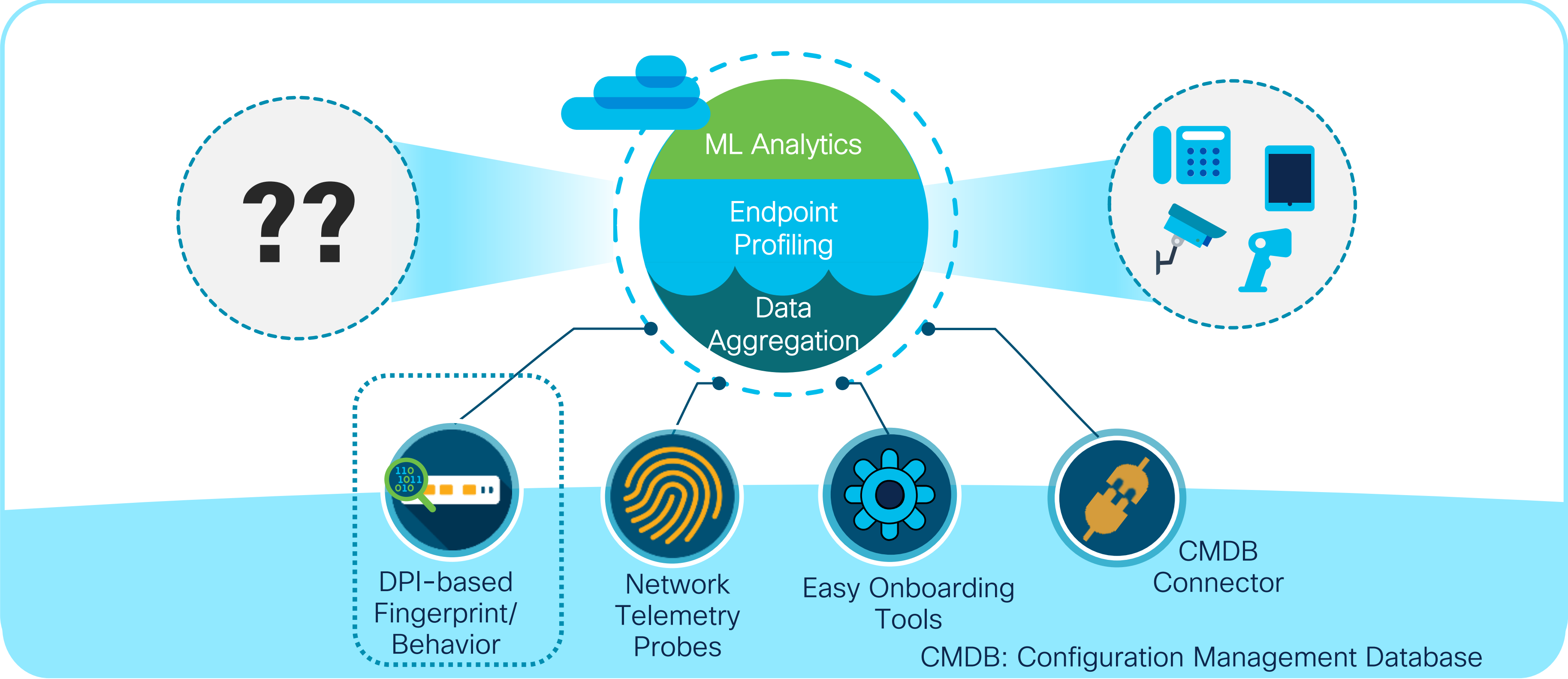
29% (3,617 onboardings)

iPad Pro 3 (1,212)
iPad Pro 2 (763)
iPad Air 3 (686)
iPad 5 (378)

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

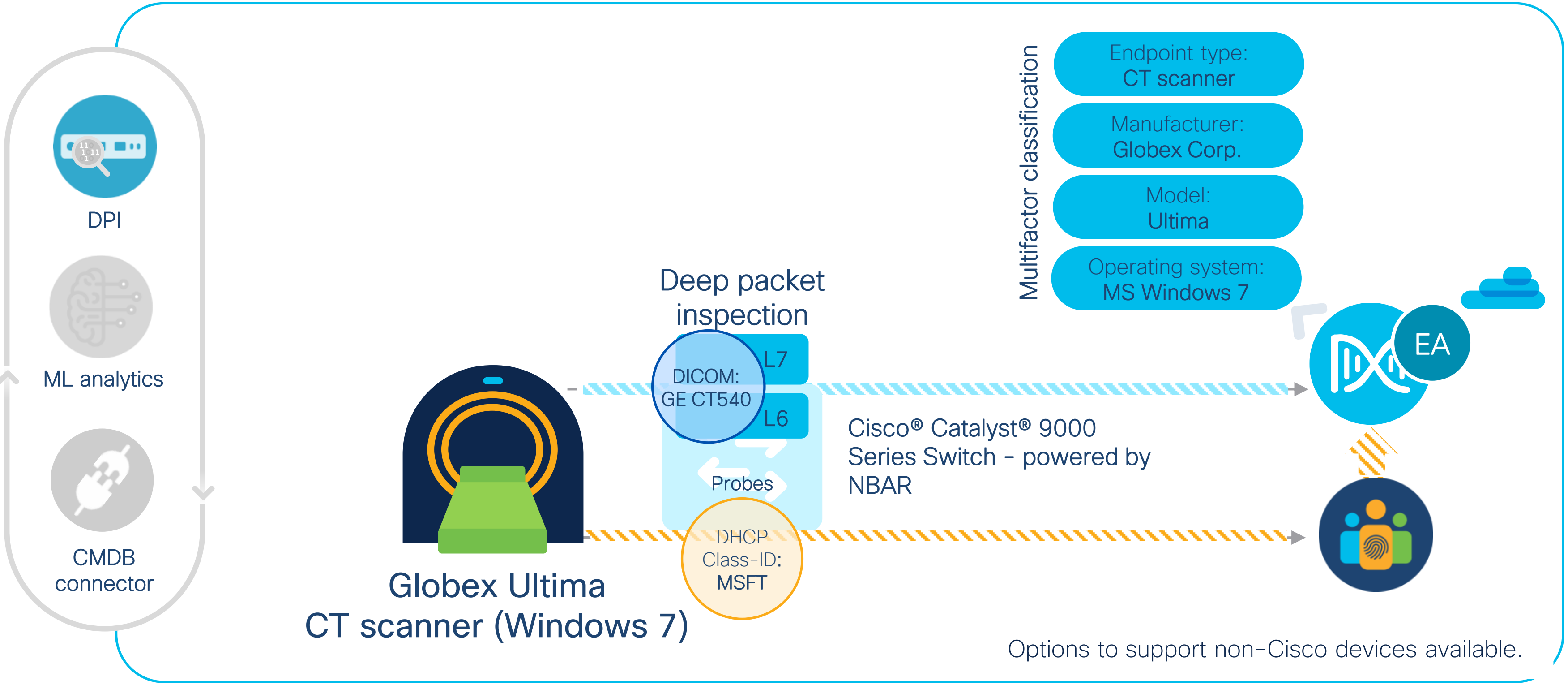
AI Endpoint Analytics on Cisco Catalyst Center

Rapidly reducing the unknowns by aggregating data from different sources



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

Classification based on Deep Packet Inspection (DPI)


DPI
ML analytics
CMDB connector
Multifactor classification
Endpoint type: CT scanner
Manufacturer: Globex Corp.
Model: Ultima
Operating system: MS Windows 7
Deep packet inspection
L7
DICOM: GE CT540
L6
Probes
DHCP Class-ID: MSFT
EA
Globex Ultima CT scanner (Windows 7)

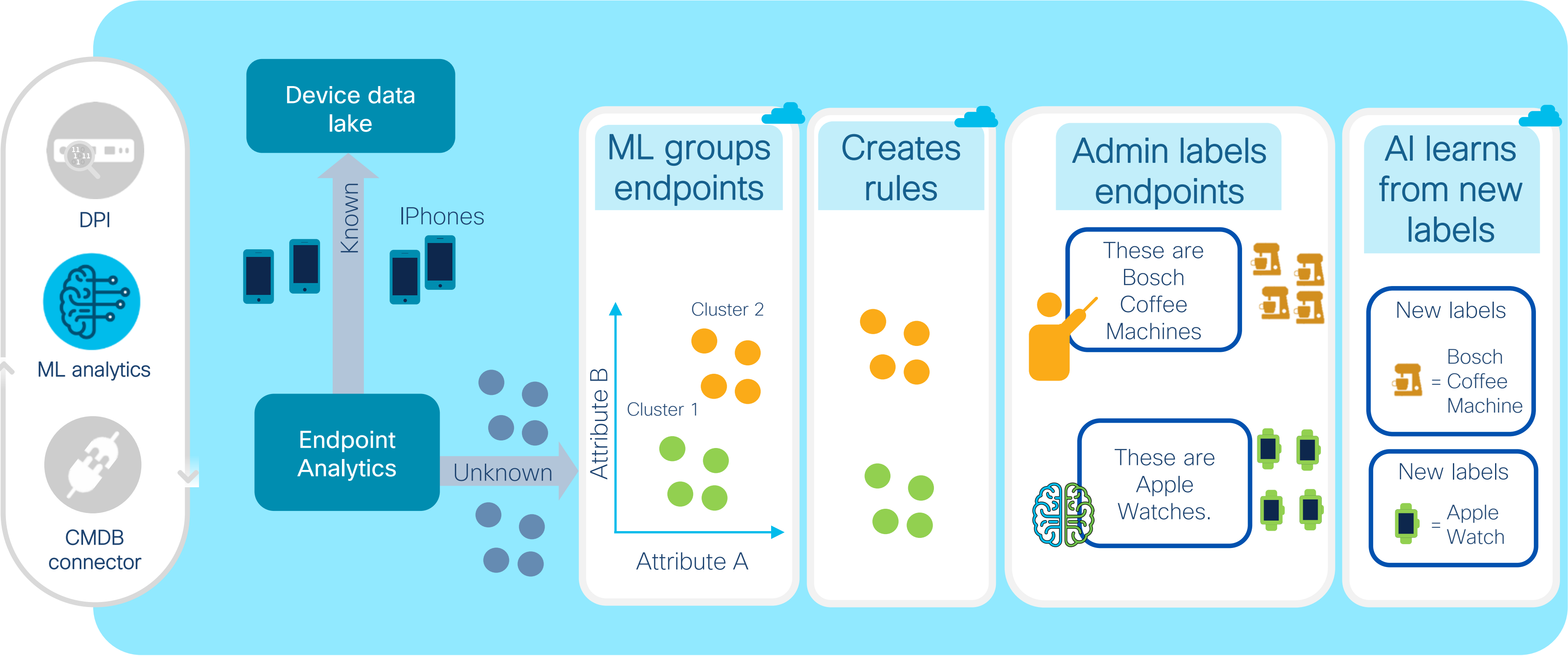
Cisco® Catalyst® 9000 Series Switch – powered by NBAR

Options to support non-Cisco devices available.

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

Reducing Unknowns with Machine Learning

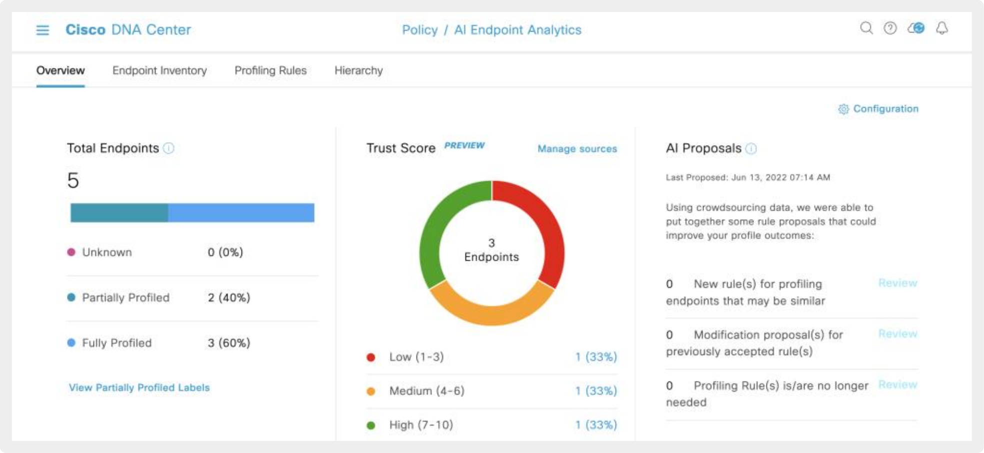
For your reference



= done in cloud

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

Trust Scores and Remediation



Cisco DNA Center — Policy / AI Endpoint Analytics

Overview | Endpoint Inventory | Profiling Rules | Hierarchy

Configuration

Total Endpoints

5

● Unknown	0 (0%)
● Partially Profiled	2 (40%)
● Fully Profiled	3 (60%)

View Partially Profiled Labels

Trust Score PREVIEW — Manage sources

3 Endpoints

● Low (1-3)	1 (33%)
● Medium (4-6)	1 (33%)
● High (7-10)	1 (33%)

AI Proposals

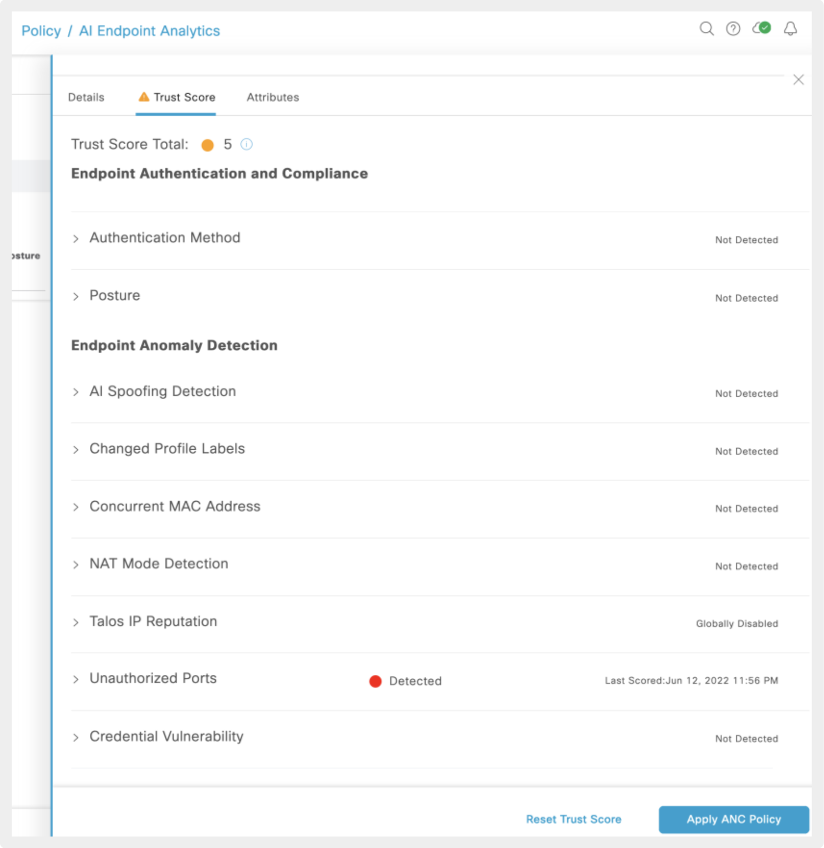
Last Proposed: Jun 13, 2022 07:14 AM

Using crowdsourcing data, we were able to put together some rule proposals that could improve your profile outcomes:

0	New rule(s) for profiling endpoints that may be similar	Review
0	Modification proposal(s) for previously accepted rule(s)	Review
0	Profiling Rule(s) is/are no longer needed	Review

Adaptive Network Control - ANC

Remediate the host via Identity Services Engine - ISE



Policy / AI Endpoint Analytics

Details | Trust Score | Attributes

Trust Score Total: ● 5

Endpoint Authentication and Compliance

Authentication Method		Not Detected
Posture		Not Detected

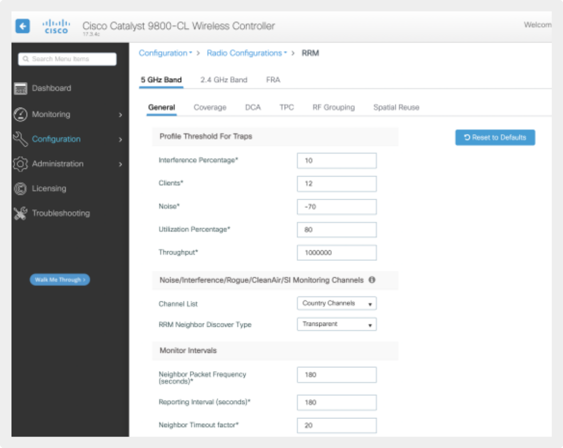
Endpoint Anomaly Detection

AI Spoofing Detection		Not Detected
Changed Profile Labels		Not Detected
Concurrent MAC Address		Not Detected
NAT Mode Detection		Not Detected
Talos IP Reputation		Globally Disabled
Unauthorized Ports	● Detected	Last Scored:Jun 12, 2022 11:56 PM
Credential Vulnerability		Not Detected

Reset Trust Score | Apply ANC Policy

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

Why radio resource management



Configuration › Radio Configurations › RRM

5 GHz Band | 2.4 GHz Band | FRA

General | Coverage | DCA | TPC | RF Grouping | Spatial Reuse

Reset to Defaults

Profile Threshold For Traps

Interference Percentage*	10
Clients*	12
Noise*	-70
Utilization Percentage*	80
Throughput*	1000000

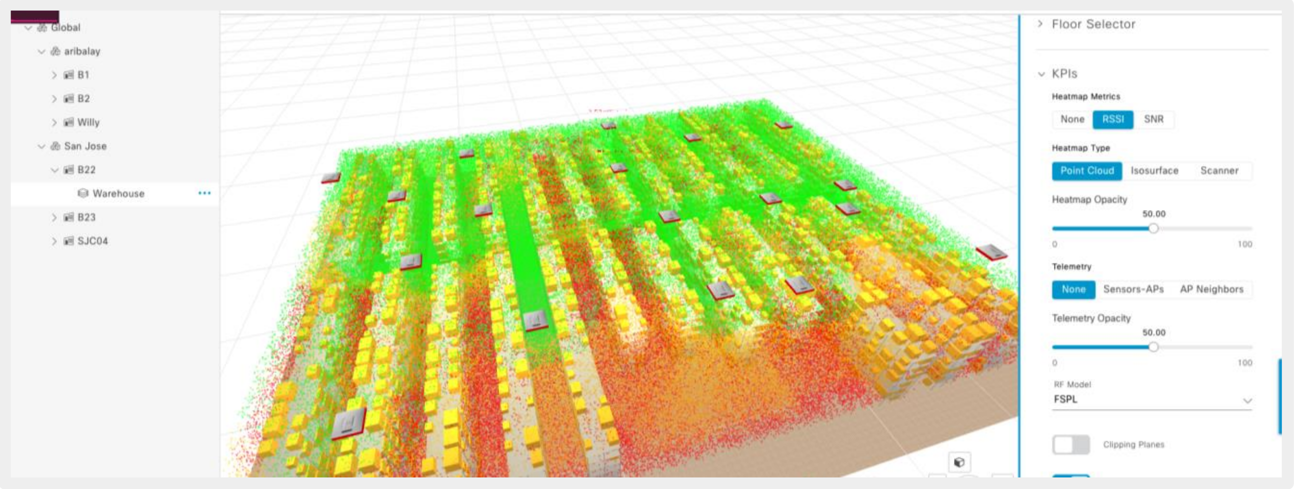
Noise/Interference/Rogue/CleanAir/SI Monitoring Channels

Channel List	Country Channels
RRM Neighbor Discover Type	Transparent

Monitor Intervals

Neighbor Packet Frequency (seconds)*	180
Reporting Interval (seconds)*	180
Neighbor Timeout factor*	20

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



Heatmap Metrics: None | RSSI | SNR

Heatmap Type: Point Cloud | Isosurface | Scanner

Heatmap Opacity: 50.00 (0 – 100)

Telemetry: None | Sensors-APs | AP Neighbors

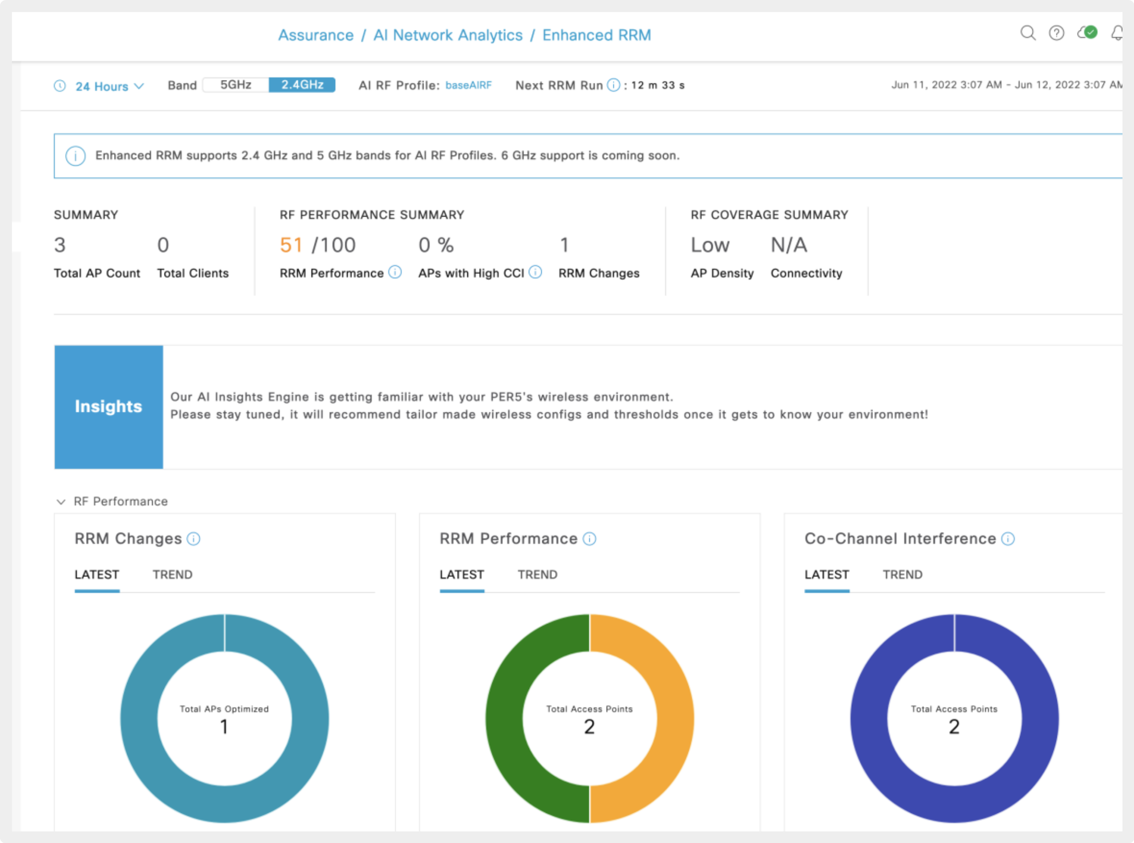
Telemetry Opacity: 50.00 (0 – 100)

RF Model: FSPL

Clipping Planes

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

Dashboard



Assurance / AI Network Analytics / Enhanced RRM

24 Hours | Band: 5GHz **2.4GHz** | AI RF Profile: baseAIRF | Next RRM Run: 12 m 33 s | Jun 11, 2022 3:07 AM - Jun 12, 2022 3:07 AM

Enhanced RRM supports 2.4 GHz and 5 GHz bands for AI RF Profiles. 6 GHz support is coming soon.

SUMMARY

3 Total AP Count

0 Total Clients

RF PERFORMANCE SUMMARY

51 /100 RRM Performance

0 % APs with High CCI

1 RRM Changes

RF COVERAGE SUMMARY

Low AP Density

N/A Connectivity

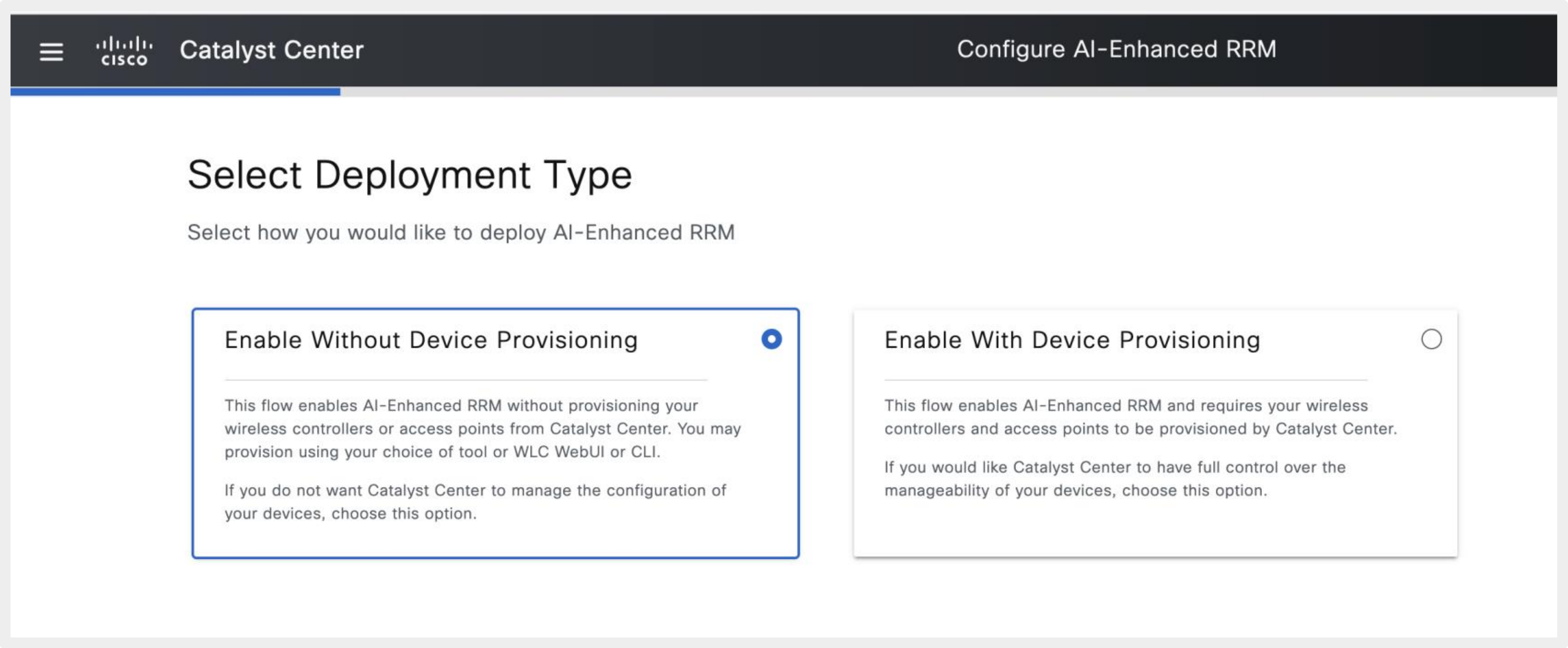
Insights

Our AI Insights Engine is getting familiar with your PER5's wireless environment.
Please stay tuned, it will recommend tailor made wireless configs and thresholds once it gets to know your environment!

RF Performance

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

2.3.7.4 supports "brownfield" 9800 deployments



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 ○

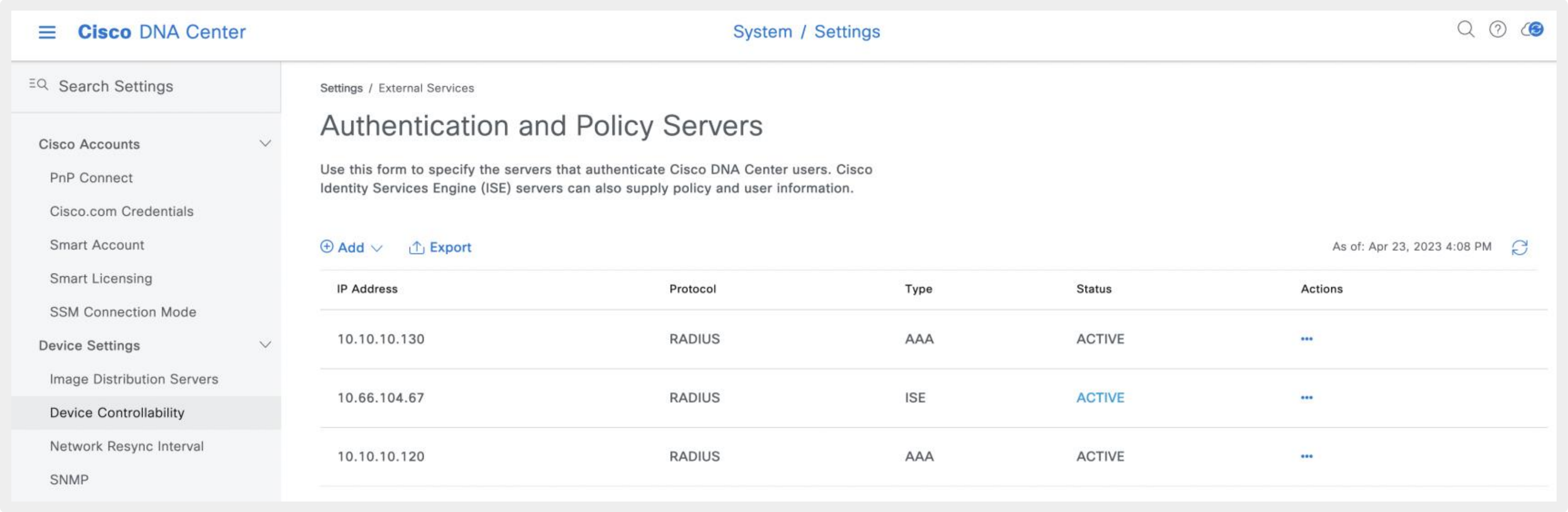
This flow enables AI-Enhanced RRM and requires your wireless controllers and access points to be provisioned by Catalyst Center.

If you would like Catalyst Center to have full control over the manageability of your devices, choose this option.

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

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

Identity Services Engine



Authentication and Policy Servers

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

As of: Apr 23, 2023 4:08 PM

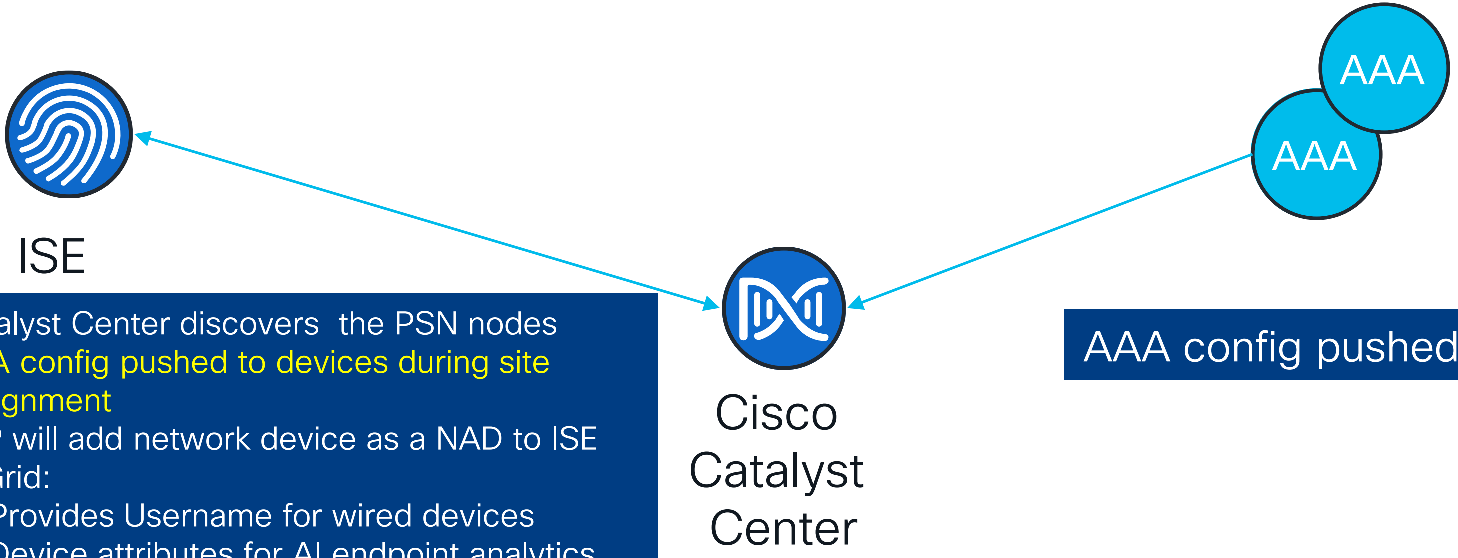
IP Address	Protocol	Type	Status	Actions
10.10.10.130	RADIUS	AAA	ACTIVE	•••
10.66.104.67	RADIUS	ISE	ACTIVE	•••
10.10.10.120	RADIUS	AAA	ACTIVE	•••

Only one ISE integration can be done per Catalyst Center.

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

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

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

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

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)

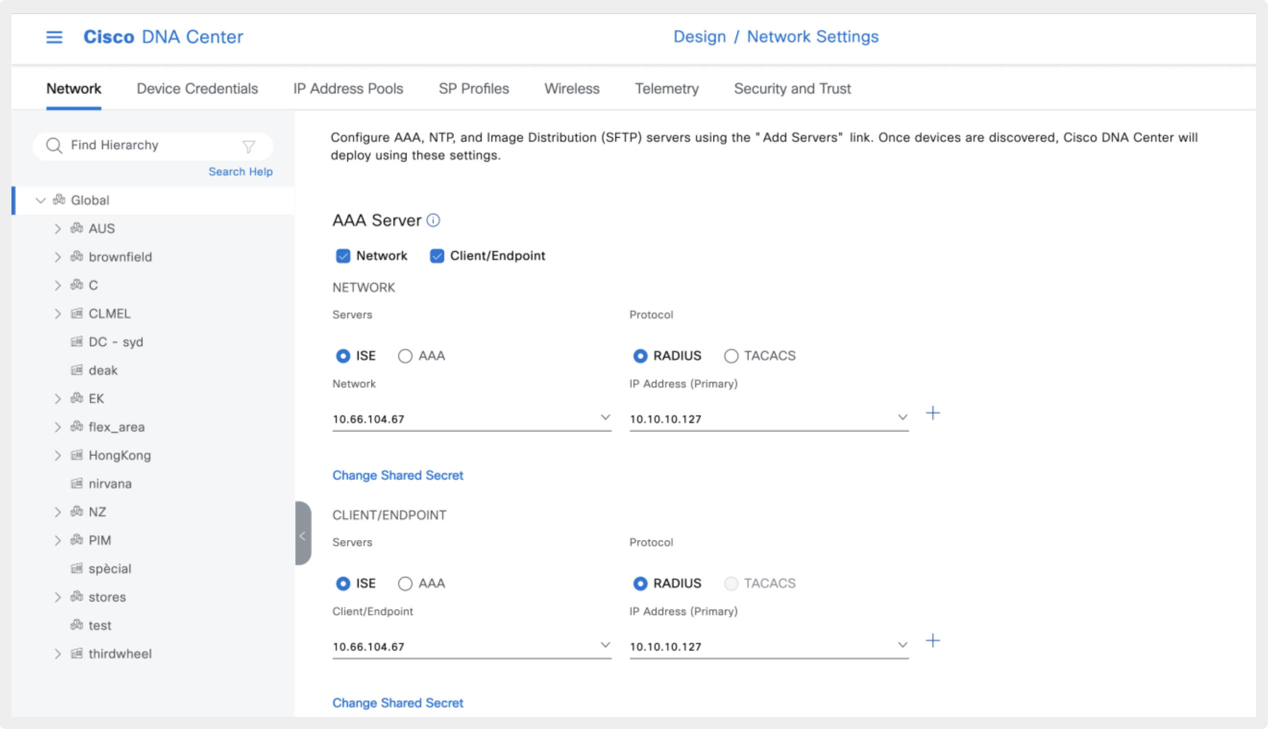
If using Enterprise issued Certificate, need VIP + real IP for Catalyst Center Cluster

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

IP reachability required

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

Site Settings for AAA



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: ● ISE ○ AAA

Protocol: ● RADIUS ○ TACACS

Network: 10.66.104.67

IP Address (Primary): 10.10.10.127

Change Shared Secret

CLIENT/ENDPOINT

Servers: ● ISE ○ AAA

Protocol: ● RADIUS ○ TACACS

Client/Endpoint: 10.66.104.67

IP Address (Primary): 10.10.10.127

Change Shared Secret

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

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

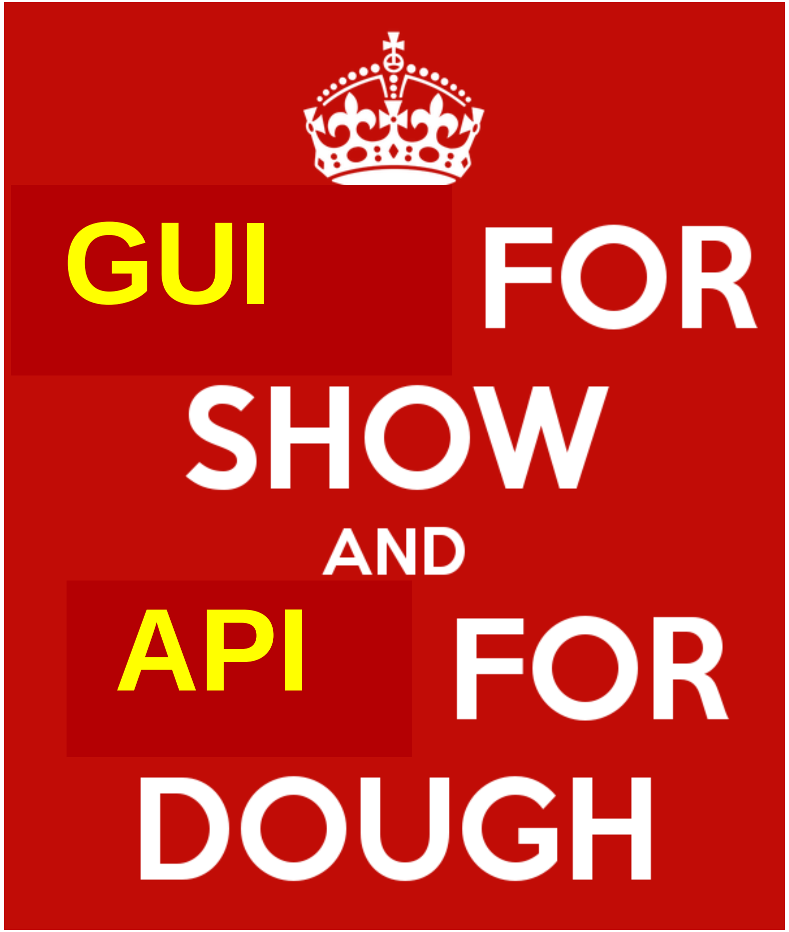
Device has AAA configured	Site has AAA defined	Provisioning Workflow Success
☑	☑	☒
☒	☑	☑
☑	☒	☑
☒	☒	☑

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

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

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

DRIVE FOR
SHOW
AND
PUTT FOR
DOUGH


GUI FOR
SHOW
AND
API FOR
DOUGH

Why API?

AUTOMATI
ON

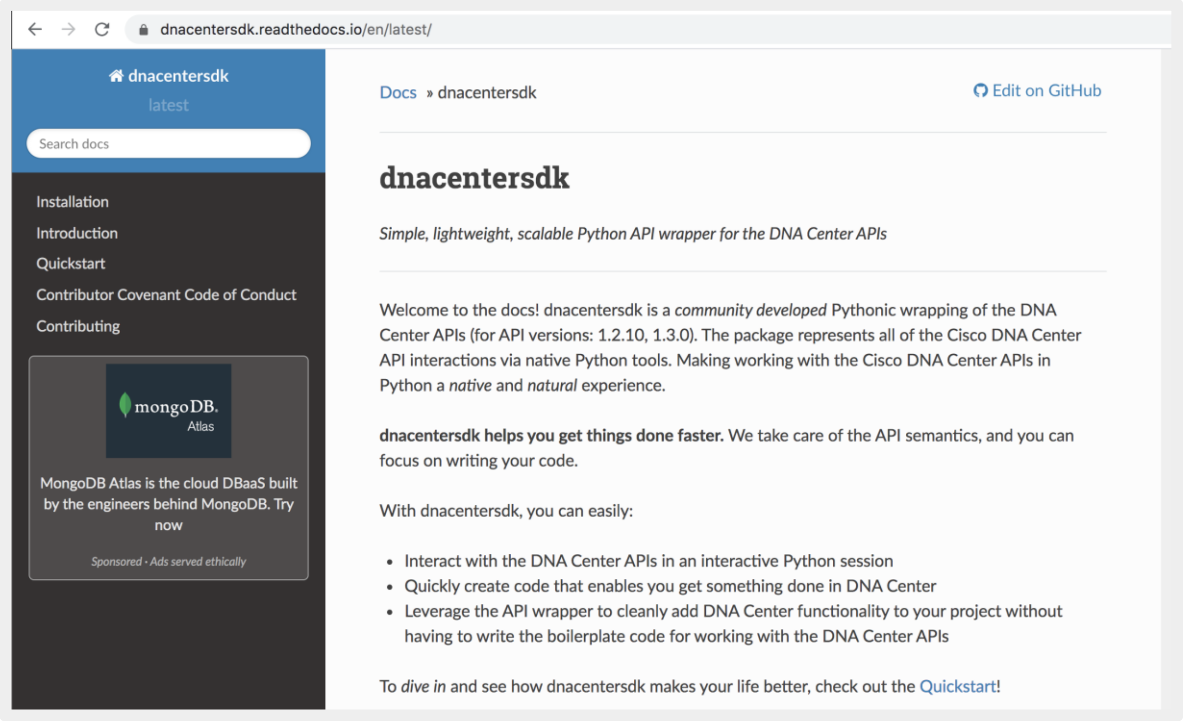
INTEGRATIO
N

INNOVATIO
N

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

SDK

```
>>> from dnacentersdk import DNACenterAPI

>>> api = DNACenterAPI()
```



mongoDB. Atlas

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

Sponsored · Ads served ethically

dnacentersdk

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

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

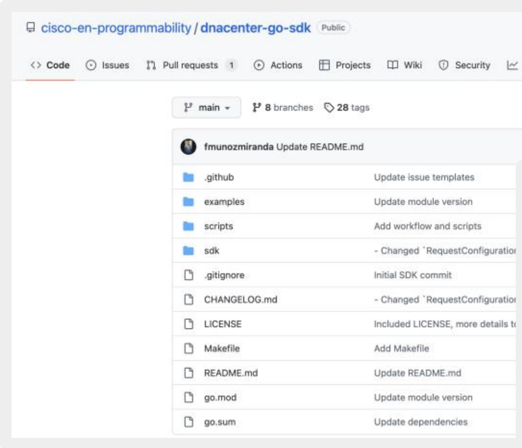
dnacentersdk helps you get things done faster. We take care of the API semantics, and you can focus on writing your code.

With dnacentersdk, you can easily:

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

To *dive in* and see how dnacentersdk makes your life better, check out the Quickstart!

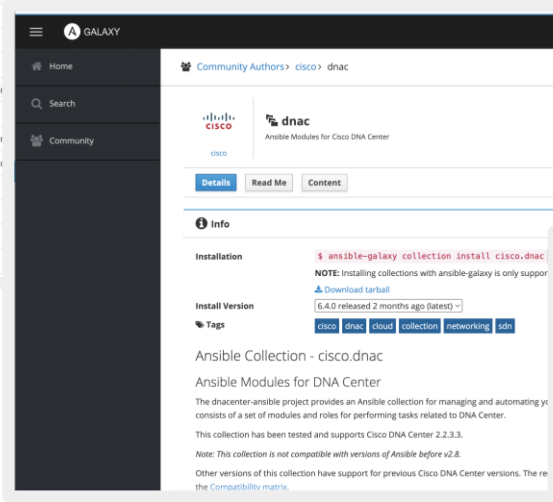
Go/Ansible/Terraform



fmunozmiranda Update README.md ✓ 05a926c 17 days ago 179 commits

.github	Update issue templates
examples	Update module version
scripts	Add workflow and scripts
sdk	- Changed `RequestConfiguratio
.gitignore	Initial SDK commit
CHANGELOG.md	- Changed `RequestConfiguratio
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



GALAXY
Home
Search
Community
Community Authors › cisco › dnac
cisco
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 suppor

Download tarball

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

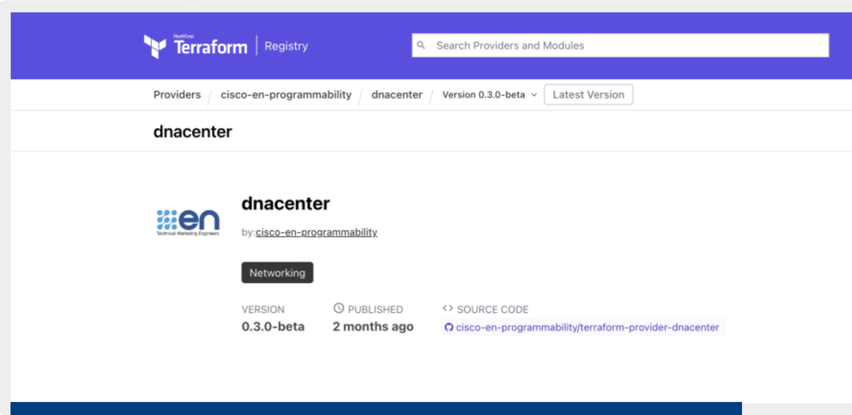
The dnacenter-ansible project provides an Ansible collection for managing and automating yo
consists of a set of modules and roles for performing tasks related to DNA Center.

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 re
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
dnacenter
by: cisco-en-programmability
Networking

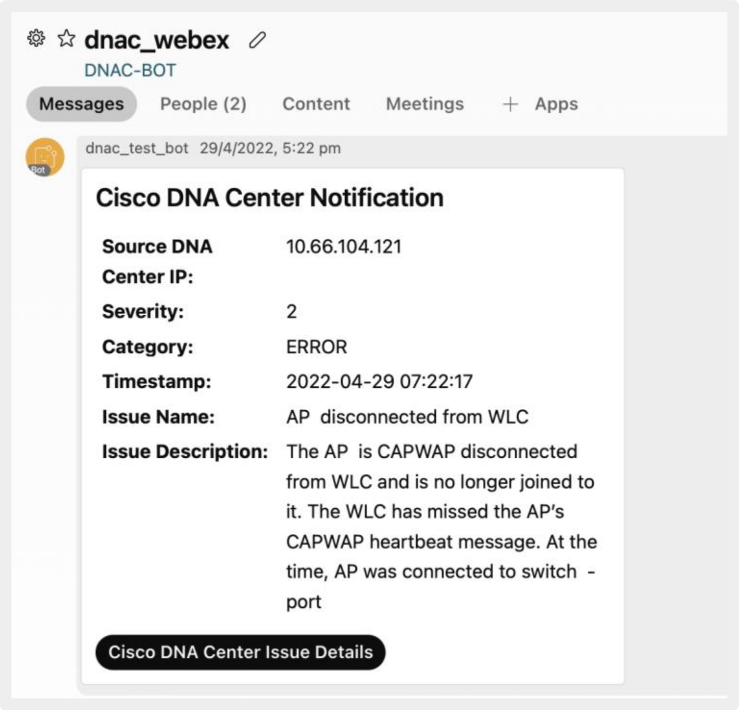
VERSION 0.3.0-beta

PUBLISHED 2 months ago

SOURCE CODE cisco-en-programmability/terraform-provider-dnacenter

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

Native Webex Issue Integration



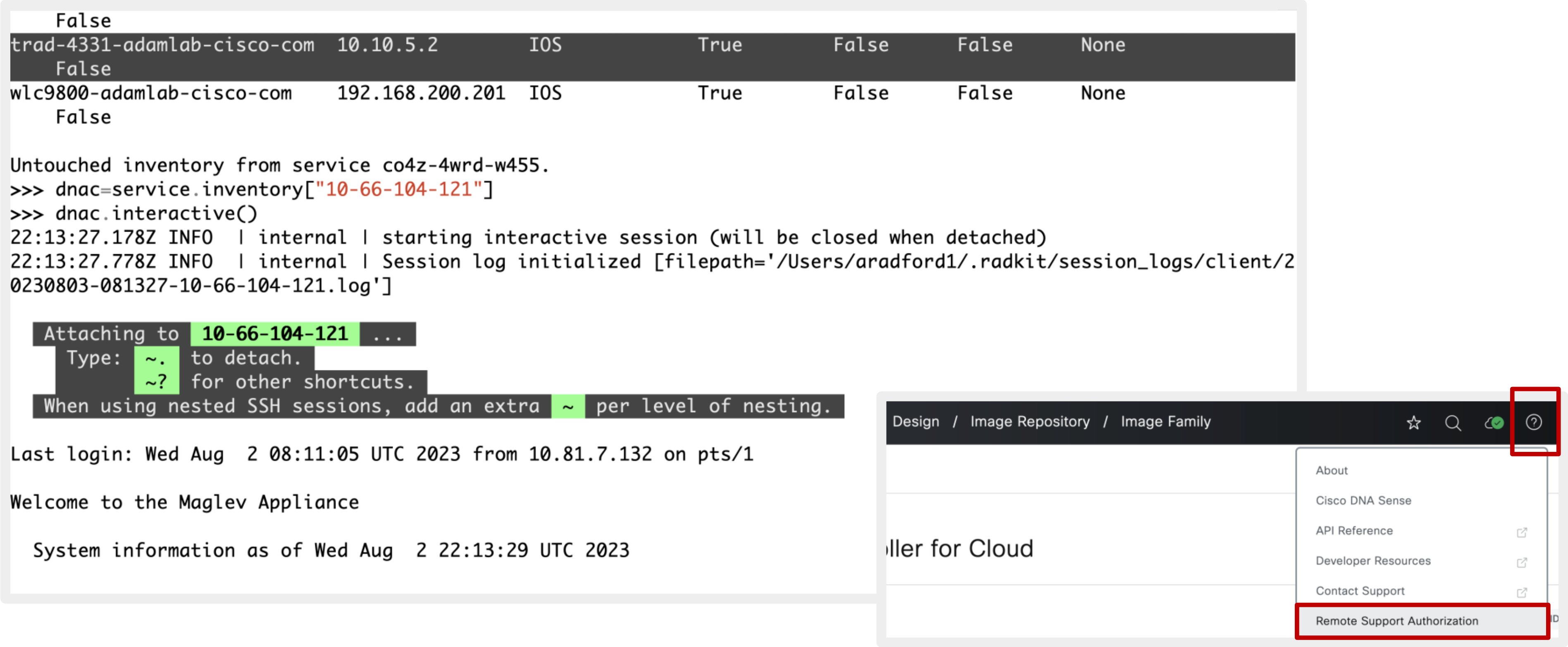
dnac_test_bot 29/4/2022, 5:22 pm

Cisco DNA Center Notification

Source DNA Center IP:	10.66.104.121
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

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

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

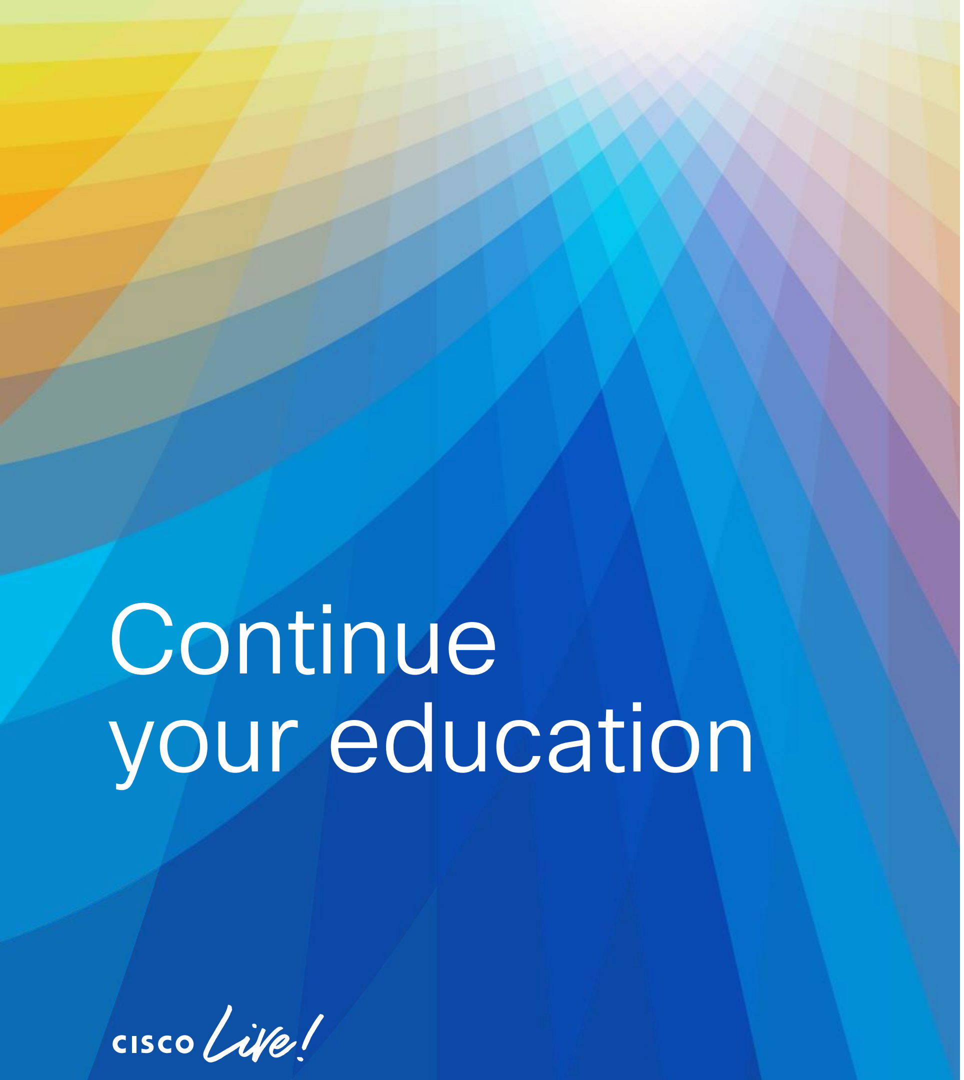


```
    False
trad-4331-adamlab-cisco-com  10.10.5.2        IOS            True          False         False         None
    False
wlc9800-adamlab-cisco-com    192.168.200.201  IOS            True          False         False         None
    False

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']

  Attacking 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

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



Continue your education

cisco.com/go/catalyst-center

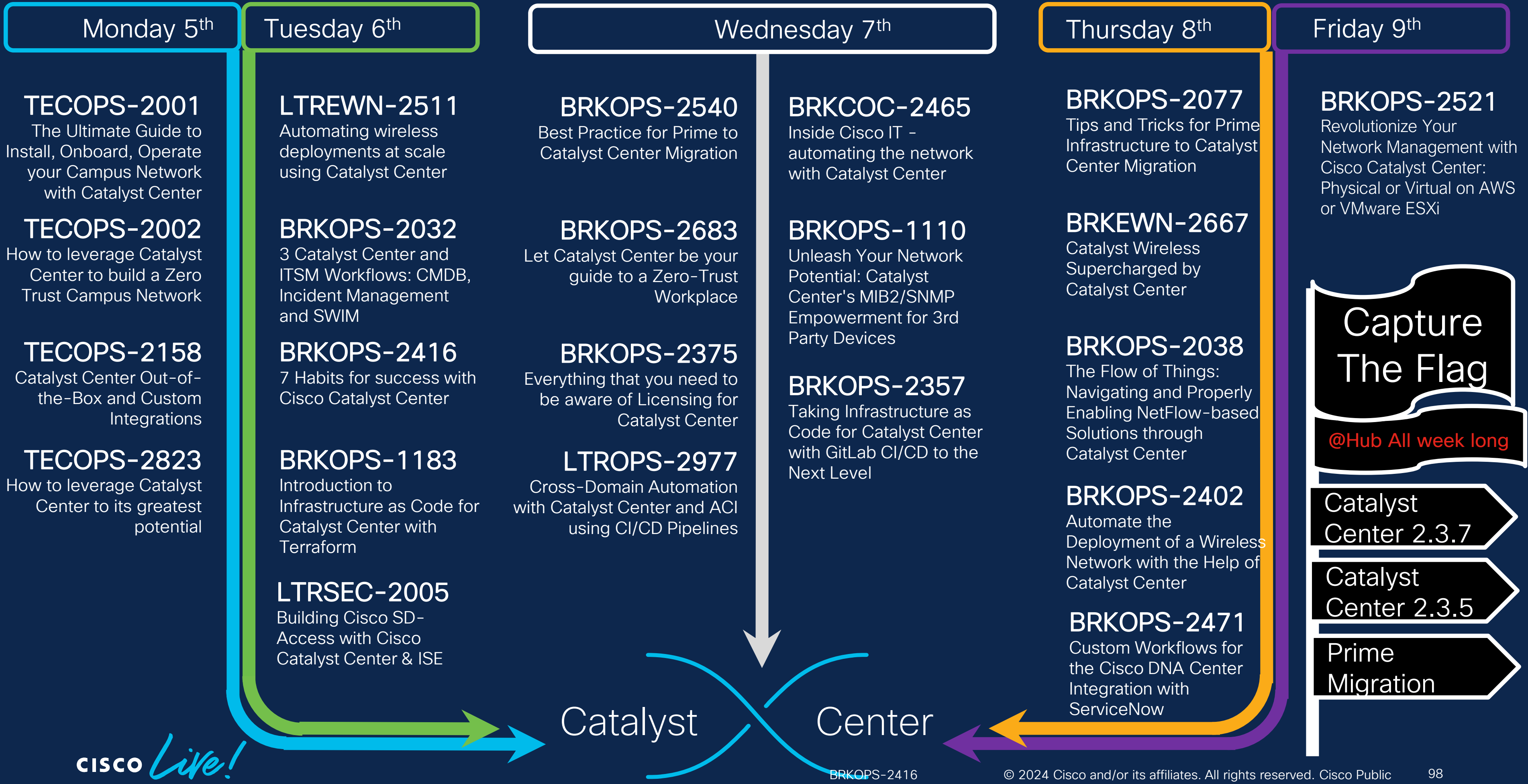
www.youtube.com/@CiscoCatalystCenter

Cisco Community

cs.co/dnac-resources

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

Cisco Live EMEA Catalyst Center Learning Map



Monday 5th

TECOPS-2001
The Ultimate Guide to Install, Onboard, Operate your Campus Network with Catalyst Center

TECOPS-2002
How to leverage Catalyst Center to build a Zero Trust Campus Network

TECOPS-2158
Catalyst Center Out-of-the-Box and Custom Integrations

TECOPS-2823
How to leverage Catalyst Center to its greatest potential

Tuesday 6th

LTREWN-2511
Automating wireless deployments at scale using Catalyst Center

BRKOPS-2032
3 Catalyst Center and ITSM Workflows: CMDB, Incident Management and SWIM

BRKOPS-2416
7 Habits for success with Cisco Catalyst Center

BRKOPS-1183
Introduction to Infrastructure as Code for Catalyst Center with Terraform

LTRSEC-2005
Building Cisco SD-Access with Cisco Catalyst Center & ISE

Wednesday 7th

BRKOPS-2540
Best Practice for Prime to Catalyst Center Migration

BRKOPS-2683
Let Catalyst Center be your guide to a Zero-Trust Workplace

BRKOPS-2375
Everything that you need to be aware of Licensing for Catalyst Center

LTROPS-2977
Cross-Domain Automation with Catalyst Center and ACI using CI/CD Pipelines

BRKCOC-2465
Inside Cisco IT - automating the network with Catalyst Center

BRKOPS-1110
Unleash Your Network Potential: Catalyst Center's MIB2/SNMP Empowerment for 3rd Party Devices

BRKOPS-2357
Taking Infrastructure as Code for Catalyst Center with GitLab CI/CD to the Next Level

Thursday 8th

BRKOPS-2077
Tips and Tricks for Prime Infrastructure to Catalyst Center Migration

BRKEWN-2667
Catalyst Wireless Supercharged by Catalyst Center

BRKOPS-2038
The Flow of Things: Navigating and Properly Enabling NetFlow-based Solutions through Catalyst Center

BRKOPS-2402
Automate the Deployment of a Wireless Network with the Help of Catalyst Center

BRKOPS-2471
Custom Workflows for the Cisco DNA Center Integration with ServiceNow

Friday 9th

BRKOPS-2521
Revolutionize Your Network Management with Cisco Catalyst Center: Physical or Virtual on AWS or VMware ESXi

Capture The Flag

@Hub All week long

Catalyst Center 2.3.7

Catalyst Center 2.3.5

Prime Migration

Catalyst Center

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

The bridge to possible

Thank you

Let’s go