

The background features a vibrant, abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, cyan, and yellow, creating a sunburst effect.

CISCO *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

# The Hidden Gems of Catalyst Center

Nathan Lee, Technical Solutions Architect  
@networkaugur  
BRKEMT-2397

CISCO *Live!*

#CiscoLiveAPJC

# Cisco Webex App

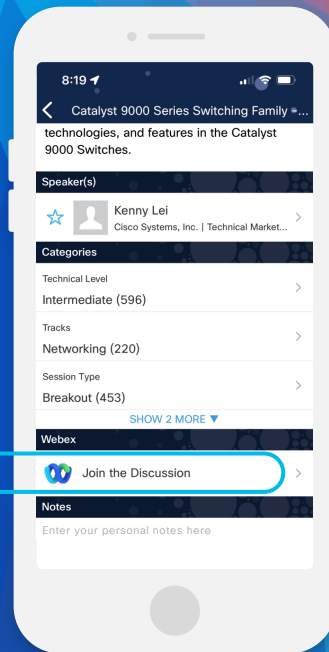
## Questions?

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

## How

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

Webex spaces will be moderated by the speaker until December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEMT-2397>

# Agenda

- Introduction
- Installation
- Settings
- Navigation
- Applications



# About the Speaker



Technical Solutions Architect  
Los Angeles, California, USA



**"World's Top University"**

-Times Higher Education, 2014

[www.theguardian.com/news/datablog/2014/oct/01/world-top-universities-2014-according-to-times-higher-education](http://www.theguardian.com/news/datablog/2014/oct/01/world-top-universities-2014-according-to-times-higher-education)

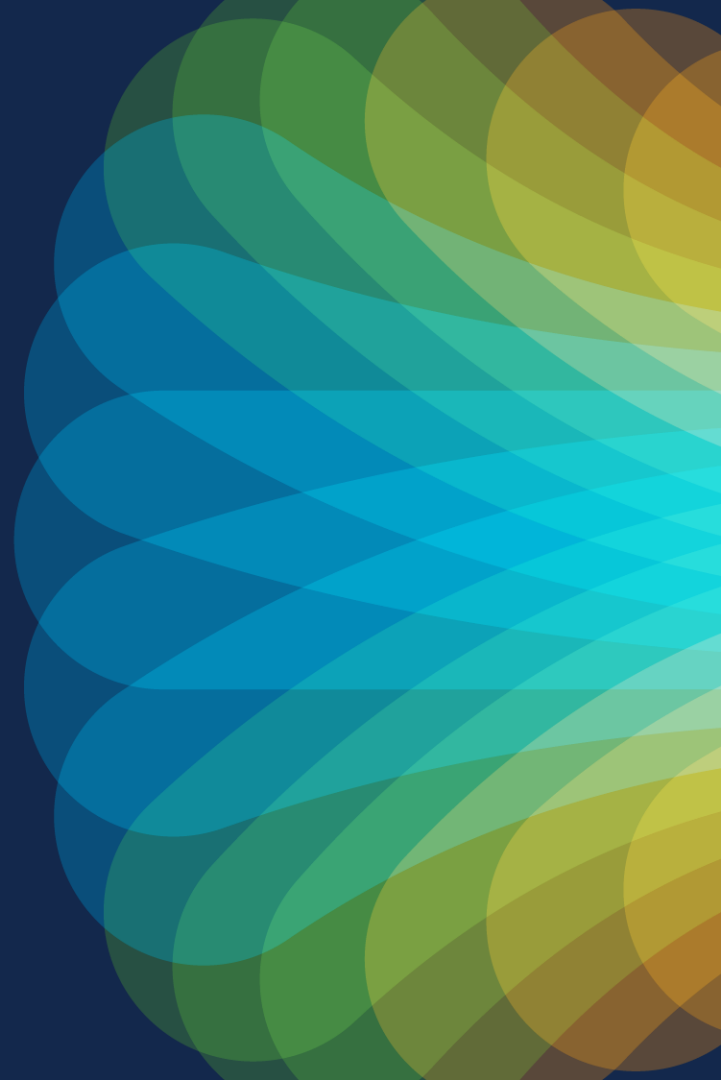
**Blackholes exist?**

[en.wikipedia.org/wiki/Thorne-Hawking-Preskill\\_bet](http://en.wikipedia.org/wiki/Thorne-Hawking-Preskill_bet)

# Session Assumptions and Objectives

- Catalyst Center 2.3.7.x, IOS-XE 17.12.x, and ISE 3.2 Patch 3 or greater
- High level overview of features
  - NOT deep dive
- Focus on proper deployment of features
  - Step-through deployment examples
  - Demos

# Installation



# Installation

- Cluster link
- DNS reachability
- SSL proxy

# Installation – Cluster Link

- Cluster link must be ACTIVE at all times, even if standalone
  - Non-active cluster link results in installation/upgrade failures
- Applies to all form factors of Cisco DNA Center or Catalyst Center versions
  - ESXi VA form factor (2.3.7+ has built-in, always active cluster link)
- Fix/workaround:
  - Always ensure cluster link is active and has IP address, even if connected to non-existent network

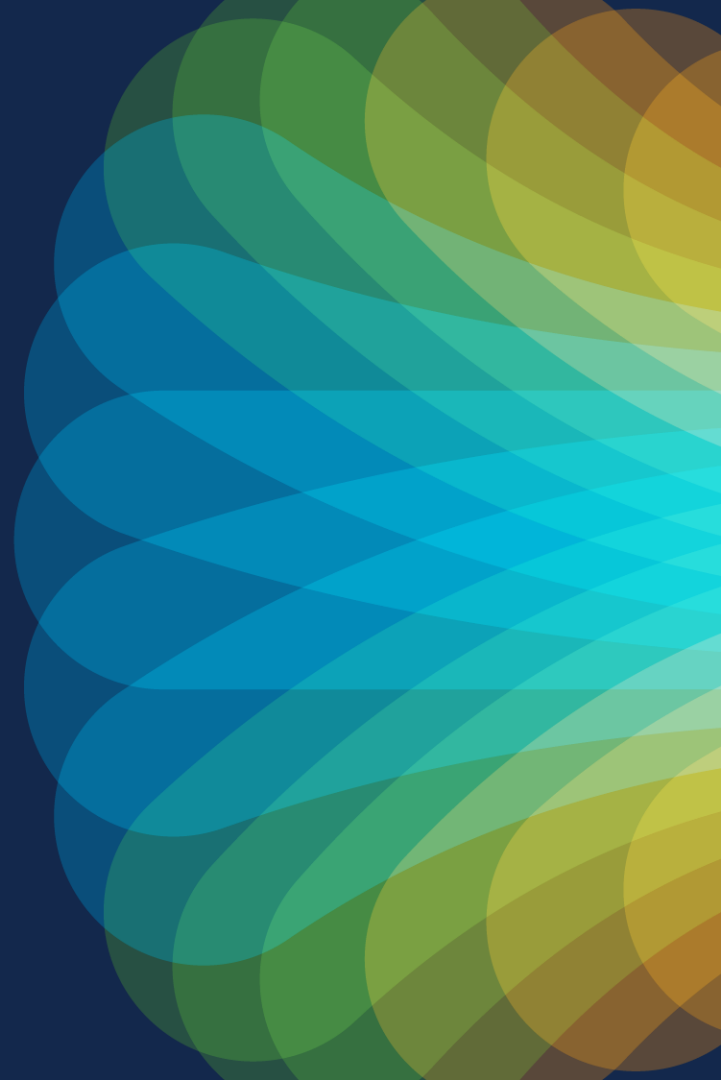
# Installation – DNS

- Non-airgap install requires DNS RESOLUTION of ciscoconnectdna.com domain
  - Resolution checked during initial system installation
  - Installation will fail if DNS resolution not successful
- Applies to all form factors of Cisco DNA Center or Catalyst Center versions
- Fix/workaround:
  - Create dummy DNS entry for ciscoconnectdna.com if necessary
  - If true Airgap environment, contact TAC for Airgap version of images

# Installation – SSL Proxy

- SSL proxy interferes with initial installation or during upgrades
  - SSL proxy injects own certificate to Catalyst Center, which is not trusted
  - Check /etc/maglev/maglev-config-wizard.log for error
    - `Get registry.ciscoconnectdna.com/v1/_ping: x509: certificate signed by unknown authority`
  - Result: installation or upgrade failures
  - CSCvi73428
- Applies to all form factors of Cisco DNA Center or Catalyst Center versions
- Fix/workaround:
  - Prevent network access to Catalyst Center during initial installation (keep in mind DNS resolution)
  - Install SSL proxy root CA onto Catalyst Center before upgrade (requires TAC due to Challenge Token)

# Settings





# Settings

- Visibility and Control of Configurations
- SNMP polling

# Settings – Visibility and Control of Configurations

- Initially known as VCR (Visibility, Control and Rollback)
- Enabled by default with Catalyst Center 2.3.7.0+
- When VCR is enabled, nearly all workflows **MUST** have configuration preview
  - Even workflows with no changes
- Suitable when ITSM and change management are company policy
- What if you don't want it...?

# Settings – Visibility and Control of Configurations

Transit

Schedule Operation:

- ☐ Now
- ☐ Later
- ☒ **Generate configuration preview** ⓘ  
Creates preview which can be later used to deploy on selected devices. View status in [Work Items](#)

Task Name\*

Creating IP-Based - IP-Transit

Cancel Apply

No devices found

No devices were found for deployment. You can still click on "Save Intent" to persist the intent to the database. This action will not affect configuration on any devices on the network.

As of: Nov 5, 2023 5:50:37 PM [Refresh](#)

Step 3 of 3: Preview Configuration

Review the device configuration provided below by clicking on each device. When you are done reviewing, click Deploy.

Status: ✔ Ready

Exit and Preview Later Discard Save Intent

No option to skip  
config preview if VCR is  
enabled, even if there  
is no actual config on  
devices

# Settings - Visibility and Control of Configurations

## Assign/Unassign 1 Device(s) to/from Site

### Step 3 of 3: Preview Configuration

Review the device configuration provided below by clicking on each device. When you are done reviewing, click Deploy.

As of: Oct 27, 2023 12:39:47 PM [Refresh](#)

Status: ● Ready

Q Search by device name

Border-C9300.cisco.local ●

Device IP: 100.124.0.1 Site: Unassigned ⓘ

Configurations - Side by side view

View by Configuration Source - All ▼

Configuration to be Deployed ⓘ  
161 Line(s)

Running Configuration ⓘ  
401 Line(s)

ⓘ Generation Status Legend

Exit and Preview Later

Discard

Deploy

```
1 sysloglistConfig
2 logging host 100.64.0.101 transport udp port 514
3 logging source-interface Loopback0
4 logging trap 6
5 done
6 sysloglistConfigs
7 idone
8 snmp-server enable traps
9 snmp-server host 100.64.0.101 traps version 2c ***** udp-port 162
10 snmp-server source-interface traps Loopback0
11 ip http client source-interface Loopback0
12 ip ssh source-interface Loopback0
13 ip ssh version 2
14 ip domain lookup
15 crypto pki trustpoint DNAC-CA
16 source interface Loopback0
17 enrollment mode ra
18 enrollment terminal
19 usage ssl-client
20 revocation-check crl none
21 exit
22 crypto pki authenticate DNAC-CA
23 -----BEGIN CERTIFICATE-----
24 MIIDpCCAs2AwIBAgIJUjEhZS8Pq4sL6m96KAa3owDQYJKoZIhvcNAQEL
25 BQAwYjEELMCsGA1UEAwwKjYyZ2UxMjM0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0
26 NzUyYHRyYVYyY2UxMjM0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0
27 QVYyYHRyYVYyY2UxMjM0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0
28 AwkYjY2Y2UxMjM0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0
29 DA1dARkKjYyY2UxMjM0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0
30 BgkqhkiG9w0BAQAAQCAQAMIBCBGCAQEAUF13YtDQPU76Gcx2ZMxrciaKse
31 BF/4KU6P9H1MOFB+1xse85ubBaksKHSuBzG1EKJqad1Tx+vx1AveOc33Poc+V+1
```

```
1 Building configuration...
2
3 Current configuration : 10780 bytes
4
5 Last configuration change at 18:53:58 UTC Fri Oct 27 2023 by netadmin
6
7 version 17.13
8 service timestamps debug datetime msec
9 service timestamps log datetime msec
10 platform punt-keepalive disable-kernel-core
11
12 hostname Border-C9300
13
14
15 vrf definition Mgmt-vrf
16
17 address-family ipv4
18 exit-address-family
19
20 address-family ipv6
21 exit-address-family
22
23 logging buffered 2000000
24 no logging console
25 no aaa new-model
26 switch 1 provision c9300-48u
27
28
29
30
31 ip routing
```

Diff view available  
with release 2.3.7.4+

Exit workflow  
(without deploying)  
and save preview to  
Activities Page

Discard workflow  
(2.3.7.3+: option to  
save preview config)

Deploy config now  
or at schedule

# Settings – Visibility and Control of Configurations

The screenshot shows the Cisco Catalyst Center interface. The top navigation bar includes the Cisco logo, 'Catalyst Center', and a breadcrumb trail 'System / Settings' which is highlighted with a green box. To the right of the breadcrumb are icons for favorites, search, cloud, help, notifications, and a user profile labeled 'admin'. On the left sidebar, a search bar is at the top, followed by a list of settings categories: 'Cisco Spaces/CMX Servers', 'Machine Reasoning Engine', 'Cloud Authentication', 'Cisco DNA - Cloud', 'Webex Integration', 'ThousandEyes Integration', 'System Configuration' (with a dropdown arrow), 'Debugging Logs', 'Visibility and Control of Configur...' (highlighted with a red box), 'Geo Map Settings', 'Proxy', and 'High Availability'. The main content area is titled 'Settings / System Configuration' and 'Visibility and Control of Configurations'. It contains a paragraph explaining the purpose of these settings: 'To further secure device configurations, you can review your device configurations and send them for approval by IT Service Management (ITSM). This means you can preview configurations before deploying them on devices (the Configuration Visibility Preview workflow) and send the planned network configuration changes to an ITSM administrator for approval (the Configuration Control workflow).' Below this, it states: 'If **Configuration Preview** is enabled, the device configurations must be reviewed before deploying them. If **ITSM Approval** is enabled, the planned configurations must be submitted for ITSM approval by an ITSM administrator.' A sub-header 'To enable ITSM, go to the [Enable ITSM](#) page.' is present. At the bottom, there are two toggle switches: 'Configuration Preview' (checked, highlighted with a red box) and 'ITSM Approval' (unchecked).

System / Settings

Search

Cisco Spaces/CMX Servers

Machine Reasoning Engine

Cloud Authentication

Cisco DNA - Cloud

Webex Integration

ThousandEyes Integration

System Configuration

Debugging Logs

Visibility and Control of Configur...

Geo Map Settings

Proxy

High Availability

Settings / System Configuration

## Visibility and Control of Configurations

To further secure device configurations, you can review your device configurations and send them for approval by IT Service Management (ITSM). This means you can preview configurations before deploying them on devices (the Configuration Visibility Preview workflow) and send the planned network configuration changes to an ITSM administrator for approval (the Configuration Control workflow).

If **Configuration Preview** is enabled, the device configurations must be reviewed before deploying them. If **ITSM Approval** is enabled, the planned configurations must be submitted for ITSM approval by an ITSM administrator.

To enable ITSM, go to the [Enable ITSM](#) page.

☒ Configuration Preview

☐ ITSM Approval

Enabled by default

# Settings – SNMP Polling

- Advanced features employ netconf-yang for telemetry (e.g. PoE stats, TrustSec data)
- Classic SNMP polling still dominant (e.g. system ID, interface MIB-II)
- By default, SNMP polling interval is 10min for most OIDs
- Modify default polling via new Collector-SNMP instance addition
- System Settings -> Data Platform -> Collectors

# Settings – SNMP Polling

[Collectors](#) / COLLECTOR-SNMP

## COLLECTOR-SNMP

NAMESPACE com.cisco.tesseract

INSTANCES 0

VERSION 0.7.0

Configurations Instances

Current Configurations (0)

 Export

 Add

 Update Configurations

≡ 🔍 Find

Name ▲

Template Name

Distribution Type

Summary

No data to display

# Settings – SNMP Polling

Template default

## SNMP Configuration

Configuration for SNMP collector

### Configuration

List of metrics to be enabled\*

- ☒ CPU
- ☒ Memory
- ☒ Interface
- ☒ Environment Temperature
- ☒ Device Availability
- ☐ QOS
- ☐ RTTMON
- ☐ LISP
- ☐ CLISP
- ☒ Ethernet Info

Polling Interval

10.00

5 100

### Collector Information

Satellite ID

satellite0

Site ID

site0

Configuration Name\*

SNMPPoll5min

Keep the name unique for this configuration

Save Configuration

Change from 10min

to 5min

Template default

## SNMP Configuration

Configuration for SNMP collector

### Configuration

List of metrics to be enabled\*

- ☒ CPU
- ☒ Memory
- ☒ Interface
- ☒ Environment Temperature
- ☒ Device Availability
- ☐ QOS
- ☐ RTTMON
- ☐ LISP
- ☐ CLISP
- ☒ Ethernet Info

Polling Interval

5.00

5 100

### Collector Information

Satellite ID

satellite0

Site ID

site0

Configuration Name\*

SNMPPoll5min

Keep the name unique for this configuration

Save Configuration



# Settings – SNMP Polling

Collectors / COLLECTOR-SNMP

## COLLECTOR-SNMP

NAMESPACE com.cisco.tesseract

INSTANCES 0

VERSION 0.7.0

Configurations


Instances

Current Configurations (1)

[Export](#)

[Update Configurations](#)

[Find](#)

	Name 	Template Name	Distribution Type	Summary		
<input type="radio"/>	SNMPPoll5min	default	one	1 Applied	0 Failed	0 Pending

1 Record(s)

Show Records: 25  1 - 1   

# Settings – SNMP Polling (Example)

Default Settings (output from “debug snmp packets”):

```
*Oct 30 21:05:57.000: SNMP: Response, reqid 1524744419, errstat 0, erridx 0  
  ciscoEnvMonTemperatureStatusEntry.3.1012 = 40  
  ciscoEnvMonTemperatureStatusEntry.2.1012 = Switch 1 - Inlet Temp Sensor
```

```
*Oct 30 21:15:56.992: SNMP: Response, reqid 1524744615, errstat 0, erridx 0  
  ciscoEnvMonTemperatureStatusEntry.3.1012 = 40  
  ciscoEnvMonTemperatureStatusEntry.2.1012 = Switch 1 - Inlet Temp Sensor
```

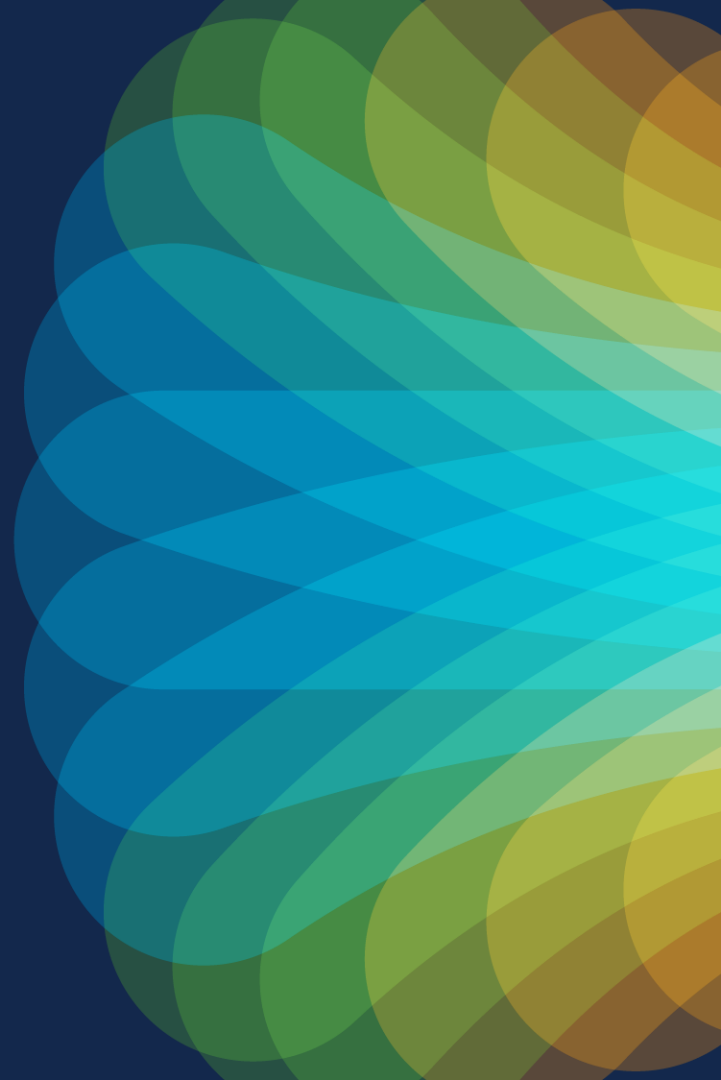
# Settings – SNMP Polling (Example)

New Collector-SNMP instance with 5min interval added:

```
*Oct 30 21:29:25.272: SNMP: Response, reqid 1524745201, errstat 0, erridx 0  
  ciscoEnvMonTemperatureStatusEntry.3.1012 = 40  
  ciscoEnvMonTemperatureStatusEntry.2.1012 = Switch 1 - Inlet Temp Sensor
```

```
*Oct 30 21:34:25.264: SNMP: Response, reqid 1524745397, errstat 0, erridx 0  
  ciscoEnvMonTemperatureStatusEntry.3.1012 = 39  
  ciscoEnvMonTemperatureStatusEntry.2.1012 = Switch 1 - Inlet Temp Sensor
```

# Navigation



# Navigation

- Dark mode
- Keyboard shortcuts
- Favorite Pages
- Inventory Focus customization
- SWIM
- PnP device onboarding

# Navigation – Dark Mode

- Dark mode supported with 2.3.7.0+
  - Appliance, AWS: 2.3.7.0+
  - ESXi VA: 2.3.7.3+
- Enabled through My Profile and Settings

The screenshot illustrates the steps to enable Dark Mode in the Cisco Catalyst Center interface. The top navigation bar shows the user is logged in as 'Demo'. A red box highlights the user profile dropdown menu, which contains the option 'My Profile and Settings'. A red arrow points from this menu item to the 'Display Settings' option in the left-hand navigation pane. The 'Display Settings' page is shown on the right, with a red box highlighting the 'Dark' mode toggle, which is currently selected.

Welcome to Catalyst Center!

Cisco DNA Center is becoming Catalyst Center

As part of our vision to converge our products around an integrated platform, we are changing the name of Cisco DNA Center to Catalyst Center in the next release. The capability and functionality of Catalyst Center remains the same as Cisco DNA Center.

LOGGED IN AS Demo Demo Log Out

My Profile and Settings

My Account

Display Settings

Communication Preferences

Notification Preferences

My Favorites

User Preference / Display Settings ☆

Display Settings

You can configure the display settings.

Set Appearance

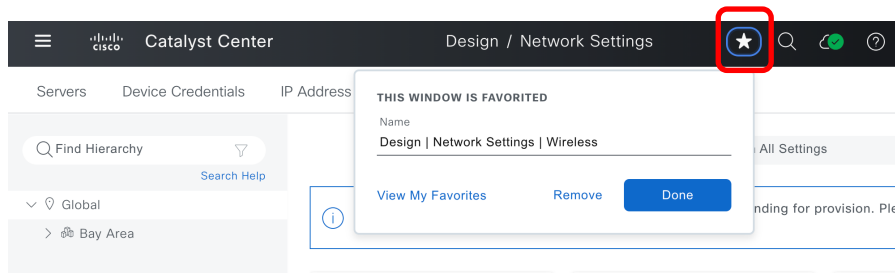
Light Dark

# Navigation – Keyboard Shortcuts

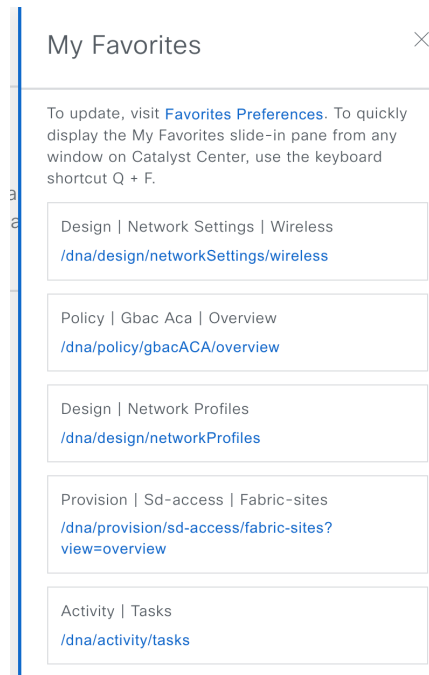
- Keyboard shortcuts available for both appliance and VA form factors
- [Alt/Option]+/ = Keyboard shortcut window
- Q+T = Command Runner "terminal" window for quick checks for a device
- Q+D = List of recently accessed devices that have been viewed through Device Details or Compliance (for current web browser session only)
- Q+A = Status of Activities Task list (does not dynamically refresh)
- Q+F = List of favorite pages
- [Alt/Option]+S = Global search window
- Shift+Q+M = Maximize Network Hierarchy geomap window (Esc to exit)

# Navigation – Favorite Pages

- Most commonly accessed pages can be added to Favorites list
- Quicker access for common/repetitive tasks
- Add/remove page from Favorites list by “starring” it (bulk remove through My Profile -> My Favorites)
- Q+F = List of favorite pages



Q+F







# Navigation – Inventory Focus Customization

- Each Focus on Inventory page parlay different device status
- Customize Focus to show common or critical status
- Focus customization persists through browser cookie only, not on any Catalyst Center system settings -> customized view lost if browser cookie deleted or if different browser used








The screenshot shows the Cisco Catalyst Center interface. The top navigation bar includes 'Provision / Inventory'. Below it, there are tabs for 'All', 'Routers', 'Switches', 'Wireless Controllers', 'Access Points', and 'Sensors'. The 'Devices (1)' section shows a dropdown menu with 'Focus: Default'. A red box highlights this dropdown. To the right of the 'Export' button is a gear icon, also highlighted with a red box. A red arrow points from this gear icon to the 'Table Settings' modal on the right. The 'Table Settings' modal has a 'Table Appearance' section with a 'Custom View Name\*' field set to 'CustomView'. Below this is a list of columns to display, including 'Device Family', 'MAC Address', 'Site', 'Reachability', 'Support Type', 'Platform', 'Serial Number', 'Uptime', 'Last Updated', 'Resync Interval', 'Manageability', and 'Device Role'. The 'Manageability' and 'Device Role' checkboxes are checked and highlighted with a red box. At the bottom of the modal are 'Cancel', 'Reset All Settings', and 'Apply' buttons, with 'Apply' highlighted by a red box.


Device Name	IP Address	Device Family	MAC Address
Border.cisco.local	100.124.0.1	Switches and Hubs (WLC Capable)	00:c1:b1:13:26:80

# Navigation – Inventory Focus Customization

  Catalyst Center

Provision / Inventory

     |  Demo 

 Global

✓ All





Routers


Switches



Wireless Controllers



Access Points




Sensors


   







Devices (1) Focus: CustomView 

Take a tour  Export 

 Click here to apply basic or advanced filters or view recently applied filters 

0 Selected Tag  Add Device Actions  

As of: Nov 6, 2023 2:17 PM 

<input type="checkbox"/>	Device Name	IP Address	Manageability 	Device Role	Compliance 
<input type="checkbox"/> 	Border.cisco.local	100.124.0.1	 Managed	ACCESS	  Compliant

# Navigation Demo

# Navigation – SWIM

- High scalability of device upgrade
  - Scheduled 100 devices for upgrades with GUI (1000 with API)
  - Distributions and activations of image occur in batches of 40 devices at a time
- Simultaneous parallel and sequential upgrades (2.3.7.0+)
- NETCONF enablement on device recommended for SWIM
  - Improved SWIM transactions with device
- Software Image Management (SWIM) defaults to Global hierarchy view
  - Be aware of hierarchy level when assigning image to device platform at lower hierarchy

# Navigation – SWIM










 Catalyst Center

Image Repository / Summary

     |  admin

 Global

 All

Routers

Switches

Wireless Controllers

Security and VPN

Sensors

Virtual Devices

SUMMARY

0

Device Families

0

Devices

0

Device Families Without Golden Image

TOTAL IMAGES

0

Running

1

Imported

0

Golden

ADVISORIES

Not Available


Image Families


[Take a Tour](#)

Cisco.com ID

nathanle (Not me?)


[Sync Updates](#)




 Filter Image Families

[Update Devices](#)

[Import Image](#)

 [Show Tasks](#)

As of: Oct 26, 2023 2:12 PM



Advisories

Family Name	Devices	Images	Critical	High	Images Marked Golden
Imported Images	N/A	1	N/A	N/A	N/A

# Navigation – SWIM

[← Image Repository](#)

## ↓ Imported Images

Images (1)

[Show Tasks](#)

Cisco.com ID

nathanle (Not me?)



[↓ Import Image](#)

As of: Oct 26, 2023 2:18 PM



Image Name ▲

Version

Device Series Assigned

Action

[cat9k\\_iosxe.17.13.01eft10.SPA.bin](#)

⚠ Unable to verify

17.13.01.0.932  
Add On (N/A)

0

[Assign](#)

[Delete](#)

# Navigation – SWIM

## Assign Device Family



Select the right device series for the image, wrong selection may cause issues during device upgrade.

Assign cat9k\_iosxe.17.13.01eft10.SPA.bin to one or more supporting device series from the list below.

Cisco Device Series

All Device Series

4 Selected

Select Site

Select a device type • Switches and Hubs

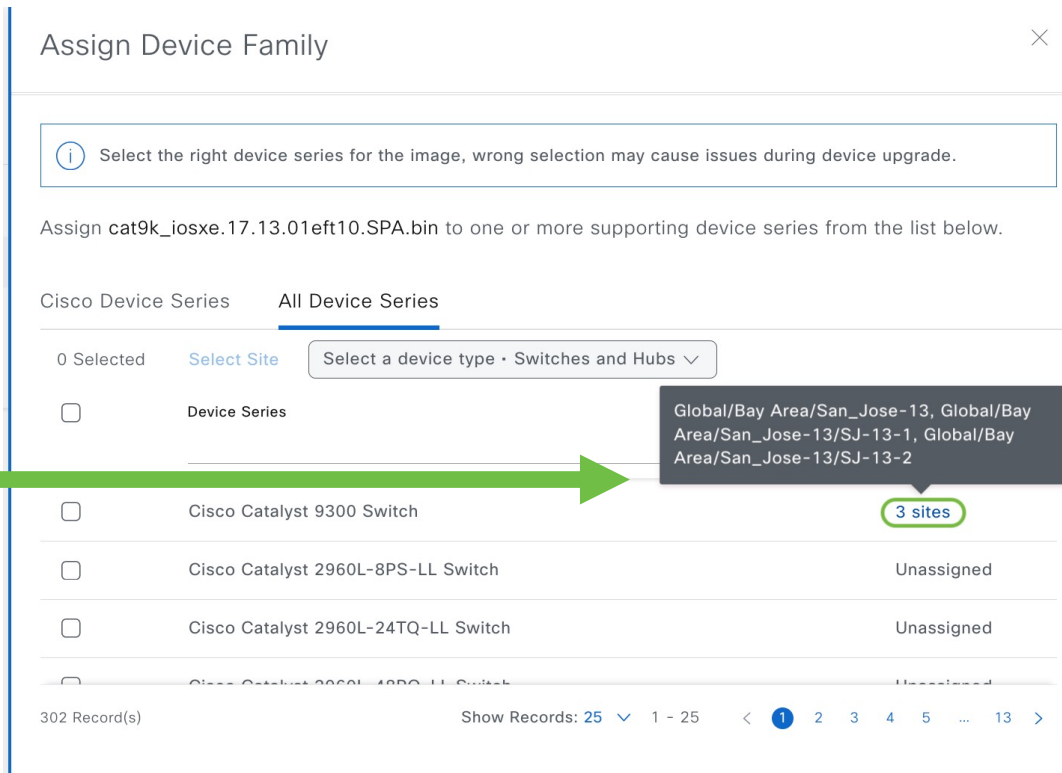
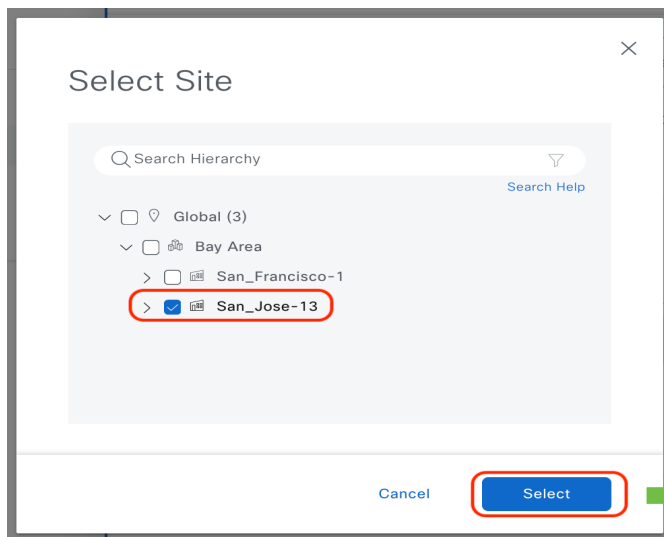


Device Series

Sites

Cisco Catalyst 9300 Switch

# Navigation – SWIM





# Navigation – SWIM

The screenshot displays the Cisco SWIM (Software Image Management) interface. A red box highlights the 'Image Repository' link in the left sidebar, with a red arrow pointing to the 'Imported Images' section. The main content area shows a summary of imported images, including a table of image families and a list of imported images.

**Image Repository**

Imported Images

Images (1)

Filter Imported Images

Import Image

Image Name ▲

cat9k\_iosxe.17.13.01eft10.SPA.bin

Unable to verify

**Global**

✓ All Routers Switches Wireless Controllers Security and VPN Sensors Virtual Devices

**SUMMARY**

Device Families	Devices	Device Families Without Golden Image
0	0	0

**TOTAL IMAGES**

Running	Imported	Golden
0	1	0

**ADVISORIES**

Not Available

**Image Families**

Take a Tour Cisco.com ID nathanle (Not me?) Sync Updates ⓘ

Filter Image Families

Update Devices Import Image Show Tasks As of: Oct 26, 2023 2:38 PM ↻

Family Name ▲	Devices	Images	Advisories ⓘ		Images Marked Golden
			Critical	High	
Imported Images ⓘ	N/A	1	N/A	N/A	N/A

No platform for which to specify Golden Image!

# Navigation – SWIM

Global

AllRoutersSwitchesWireless ControllersSecurity and VPNSENSORSVirtual Devices

SUMMARY

000

Device FamiliesDevicesDevice Families Without Golden Image

TOTAL IMAGES

010

RunningImportedGolden

ADVISORIES

Not Available

Image Families

Take a TourCisco.com IDnathanle (Not me?)Sync Updates

Filter Image Families

Update DevicesImport ImageShow TasksAs of: Oct 26, 2023 2:38 PM

Advisories

Family Name	Devices	Images	Advisories		Images Marked Golden
			Critical	High	
Imported Images	N/A	1	N/A	N/A	N/A

# Navigation – SWIM

 San\_Jose-13

✓ All

Routers

Switches

Wireless Controllers

Security and VPN

Sensors

Virtual Devices

## SUMMARY

0  
Device Families

0  
Devices

0  
Device Families  
Without Golden Image

## TOTAL IMAGES

1  
Running

1  
Imported

0  
Golden

## ADVISORIES

0  
Critical  
On Running Images

0  
High  
On Running Images

## Image Families

[Take a Tour](#)

Cisco.com ID

nathanle (Not me?)

[Sync Updates](#) ⓘ

🔍 Filter Image Families



[↻ Update Devices](#) [⬇ Import Image](#) [☰ Show Tasks](#) As of: Oct 26, 2023 2:39 PM [↺](#)

## Advisories ⓘ

Family Name ▲	Devices	Images	Critical	High	Images Marked Golden
Imported Images ⓘ	N/A	1	N/A	N/A	N/A
Cisco Catalyst 9300 Switch	0	1	0	0	0

# Navigation – SWIM

San\_Jose-13

< Image Repository

## Cisco Catalyst 9300 Switch

### SUMMARY

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

Images (1)

Show Tasks

Cisco.com ID

nathanle (Not me?)

Filter Images

As of: Oct 26, 2023 2:39 PM

### Advisories

Image Name	Version	Devices	Image Status	Critical	High	Device Roles & Tags
cat9k_iosxe.17.13.01eft10.SPA.bin Unable to verify	17.13.01.0.932 Add On (N/A)	0	★	0	0	Role: All

# Navigation – PnP Device Onboarding

- General recommendations for Network Plug and Play (PnP)
  - Just cable up and power up—little reasons to connect to console of device
  - PnP support Stackwise switches (no support for Stackwise Virtual – SWV)
  - SWIM with PnP for install mode only (not supported for bundle mode)
  - Leave PnP or LAN Auto running while resolving issues (e.g. network reachability, license level)
  - LAN Auto active + PnP of non-fabric devices = supported
  - LAN Auto active + SDA Extended Node onboarding = CONFLICT! NOT SUPPORTED!
  - “pnpa service reset no-prompt” = quick and easy reset of device for PnP, if absolutely needed
- But if problem is encountered, it's ok to connect to console of PnP device
  - It's ok to get into config mode
  - It's possible to restart PnP process without rebooting device

# Navigation – PnP Restart Without Rebooting

- A. Delete device in Error state on Catalyst Center PnP page
- B. Connect to console port of PnP device and stop PnP service
  - `Switch# pnp service discovery stop`
- C. Delete existing PnP profile on device
  - `Switch(config)# no pnp profile pnp-zero-touch`
- D. Create new PnP profile on device
  - `Switch(config)# pnp profile pnp-zero-touch`
  - `Switch(config)# transport http ipv4 {PnP-Server-IP} port 80`
- E. Restart PnP service on device (optional)
  - `Switch# pnp service discovery start`
- F. Claim device on Catalyst Center PnP page

# PnP Demo

# Applications



# Applications

- App-hosting
- Application Telemetry and CBAR
- AI Endpoint and Trust Analytics

# Applications – App-Hosting

- App-hosting uses RESTCONF from Catalyst Center
  - HTTPS server required to be enabled on switches
  - Should run versions of IOS-XE that address WebUI critical vulnerability
  - Use http access-class to limit web access to device (best practice)
- User credential for https must have level 15 privilege
  - Authentication can be local or through AAA
  - On Catalyst Center: HTTPS credential (and TCP port) added during discovery or under Inventory after onboarding
  - On IOS-XE switches: “ip http authentication {local|aaa}”

# Applications – App-Hosting (Example)

Catalyst Center

Enable Apps on Switches

Select Switches

Select switches where you want to enable **ThousandEyes Enterprise Agent**.

Switches (4)

Filter 0 Selected

Device Name	Site	IP Address	Serial Number	Image Version	Device Series
<input type="checkbox"/> Border.cisco.local	.../Bay Area/San_Jose-13	100.124.0.1	FCW2125L104	17.12.1	Cisco Catalyst 9300 Serie...
<input type="checkbox"/> Cat3650-Old.cisco.local	.../Bay Area/San_Jose-13	100.124.127.36	FDO1946X034	16.12.10a	Cisco Catalyst 3650 Serie...
<input type="checkbox"/> Edge-L.cisco.local	.../San_Jose-13/SJ-13-1	100.124.126.129	FCW2333G0QW	17.12.2	Cisco Catalyst 9300 Serie...
<input type="checkbox"/> Edge-R.cisco.local	.../San_Jose-13/SJ-13-1	100.124.126.134	FCW2125L10A	17.12.2	Cisco Catalyst 9300 Serie...

4 Record(s)

Show Records: 25 1 - 4

Why is “100.124.126.134” marked “Not Ready”?

Readiness Check	Result	Message
Are HTTPS Credentials Provided in the Inventory	Failed	HTTP(s) Username is missing in the Inventory. Provide HTTP(s) Username in the Inventory and try again. The HTTPS credentials are required to connect to App Hosting. Provide the HTTPS credentials in Device Inventory.
Are HTTPS Credentials Valid	Skipped	Test cannot be performed as HTTPS credentials for the device are not provided in the inventory. The HTTPS credentials are required to connect to App Hosting. Provide the HTTPS credentials in Device Inventory.

Not Ready

See Details

# Applications – App-Hosting (Example)

```
Edge-R#sh run | inc ip http
no ip http server
ip http authentication local
ip http secure-server
ip http max-connections 16
ip http client source-interface Loopback0
Edge-R#
```

Catalyst Center Provision / Inventc

Global

Devices (8) Focus: Inventory

Click here to apply basic or advanced filters or view records

1 Selected Tag Add Device Edit Device

Device Name	IP Address
Edge-L.cisco.local	100.124.126.129
Edge-R.cisco.local	100.124.126.134
Cat3650-Old.cisco.local	100.124.127.36
C9800-CL.cisco.local	100.124.125.104

Edit Device

Credentials Management IP Resync Interval Device

HTTP(S)

☐ Select global credential ☒ Add device specific credential

Username\* netadmin Password\*

Port\* 443

View Username Criteria View Password Criteria

The HTTP(S) credentials are required for connecting to Meraki, Firepower Management Center, Application Hosting, and NFV/Compute devices. The HTTP(S) credentials are not validated for Network Device.

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](#)

Cancel Update

## Select Switches

Select switches where you want to enable **ThousandEyes Enterprise Agent**.

Switches (4)

Import Export

Filter 0 Selected

<input type="checkbox"/>	Device Name	Site	IP Address	Serial Number	Image Version	Device Series	Readiness
<input type="checkbox"/>	Border.cisco.local	.../Bay Area/San_Jose-13	100.124.0.1	FCW2125L104	17.12.1	Cisco Catalyst 9300 Serie...	Not Ready <a href="#">See Details</a>
<input type="checkbox"/>	Cat3650-Old.cisco.local	.../Bay Area/San_Jose-13	100.124.127.36	FDO1946X034	16.12.10a	Cisco Catalyst 3650 Serie...	Not Ready <a href="#">See Details</a>
<input type="checkbox"/>	Edge-L.cisco.local	.../San_Jose-13/SJ-13-1	100.124.126.129	FCW2333G0QW	17.12.2	Cisco Catalyst 9300 Serie...	Not Ready <a href="#">See Details</a>
<input type="checkbox"/>	Edge-R.cisco.local	.../San_Jose-13/SJ-13-1	100.124.126.134	FCW2125L10A	17.12.2	Cisco Catalyst 9300 Serie...	Ready <a href="#">See Details</a>

4 Record(s)

Show Records: 25 1 - 4

# Application Telemetry?

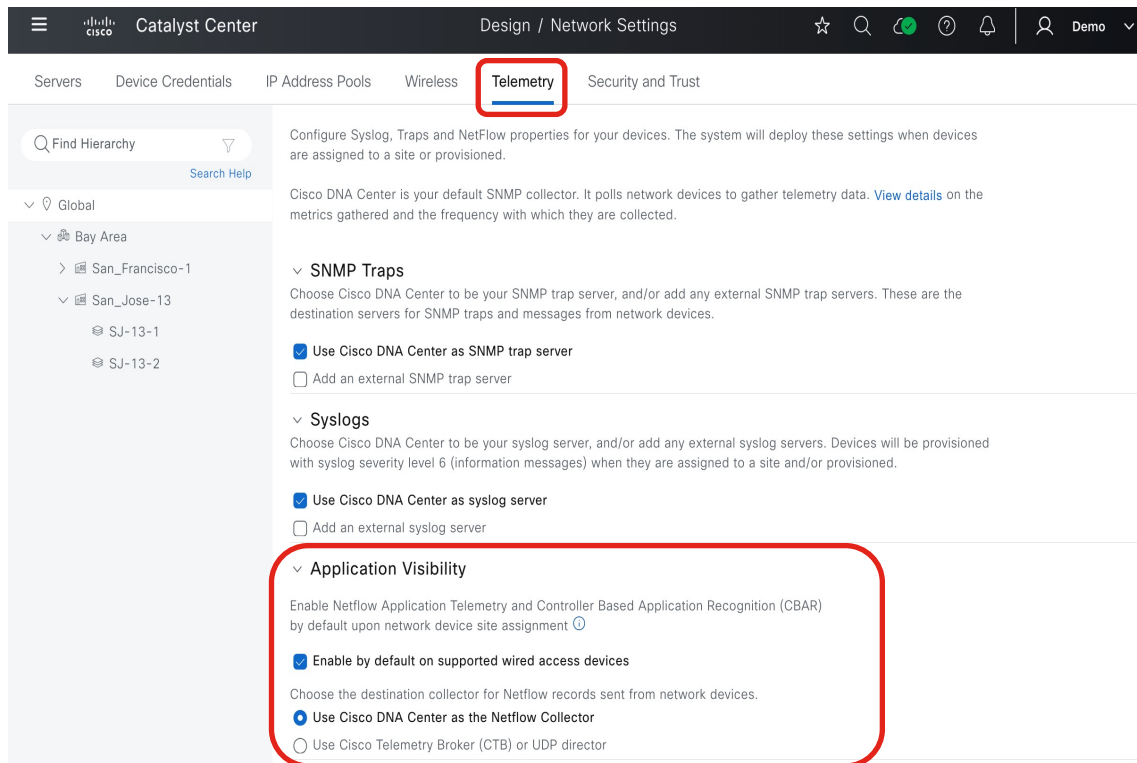
## Application Visibility?

## Application Experience?

# Application Experience

- Application Telemetry
  - Configuration on network devices orchestrated by Catalyst Center to send traffic telemetry to Catalyst Center or Cisco Telemetry Broker
  - NetFlow/IPFIX exports from devices
- Application Visibility
  - Classification of applications done locally on devices (NBAR) and/or on Catalyst Center (CBAR)
  - Classification export from devices on a separate stream from regular App Telemetry
- Application Experience
  - Term used to encompass Application Visibility and Control solution
  - Often used to describe qualitative Application Visibility (as opposed to quantitative AppViz)

# Application Telemetry Deployment



The screenshot displays the Cisco Catalyst Center web interface. The top navigation bar shows 'Design / Network Settings'. The left sidebar contains a hierarchy of locations: Global, Bay Area, San\_Francisco-1, and San\_Jose-13. The main content area is titled 'Telemetry' and contains configuration options for Syslog, Traps, and NetFlow. The 'Application Visibility' section is highlighted with a red box, showing the following configuration:

- Application Visibility**
  - Enable Netflow Application Telemetry and Controller Based Application Recognition (CBAR) by default upon network device site assignment ⓘ
  - ☒ Enable by default on supported wired access devices
  - Choose the destination collector for Netflow records sent from network devices.
    - ☒ Use Cisco DNA Center as the Netflow Collector
    - ☐ Use Cisco Telemetry Broker (CTB) or UDP director

- Catalyst Center as NetFlow Collector enabled under **Design** -> **Network Settings** -> **Telemetry**
- Alternative option to set Cisco Telemetry Broker (CTB) as NetFlow destination instead
- CTB as destination recommended when Secure Network Analytics (StealthWatch) is also deployed

# Application Telemetry Deployment

The screenshot shows the Cisco Catalyst Center interface. The top navigation bar includes 'Servers', 'Device Credentials', 'IP Address Pools', 'Wireless', 'Telemetry' (highlighted with a red box), and 'Security and Trust'. The left sidebar shows a hierarchy: 'Global' > 'Bay Area' > 'San\_Francisco-1' > 'San\_Jose-13' > 'SJ-13-1' > 'SJ-13-2'. The main content area is titled 'Design / Network Settings' and contains the following sections:

- 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.
- SNMP Traps**
- Syslogs**
- Application Visibility**
  - Enable Netflow Application Telemetry and Controller Based Application Recognition (CBAR) by default upon network device site assignment [?](#)
  - ☒ **Enable by default on supported wired access devices**
  - Choose the destination collector for Netflow records sent from network devices.
    - ☒ **Use Cisco DNA Center as the Netflow Collector**
    - ☐ Use Cisco Telemetry Broker (CTB) or UDP director
- 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 [?](#)

## Strongly Recommended to enable Wired Data Endpoint Collection

- Provides granular client information for Assurance, ISE accounting, and other features
- Required setting for Software-Defined Access (SDA) fabric deployment
- Default setting is Enable on virtual form factor of Catalyst Center but Disable on physical appliance image



# Application Telemetry Deployment

The screenshot shows the Cisco Catalyst Center interface. The top navigation bar includes 'Servers', 'Device Credentials', 'IP Address Pools', 'Wireless', 'Telemetry' (highlighted), and 'Security and Trust'. The 'Telemetry' section is titled 'Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned.' It includes a section for 'Cisco DNA Center as the NetFlow Collector' with two radio buttons: 'Use Cisco DNA Center as the NetFlow Collector' (selected) and 'Use Cisco Telemetry Broker (CTB) or UDP director'. Below this is the 'Wired Endpoint Data Collection' section, which is expanded to show 'Enable Cisco DNA Center Wired Endpoint Data Collection At This Site' (selected) and 'Disable Cisco DNA Center Wired Endpoint Data Collection At This Site'. The 'Wireless Controller, Access Point and Wireless Clients Health' section is also expanded, showing 'Enable Wireless Telemetry' (checked) and 'Disable Wireless Telemetry'. The 'Reset' and 'Save' buttons are at the bottom right.

- Ensure telemetry for wireless networks is enabled (set by default)

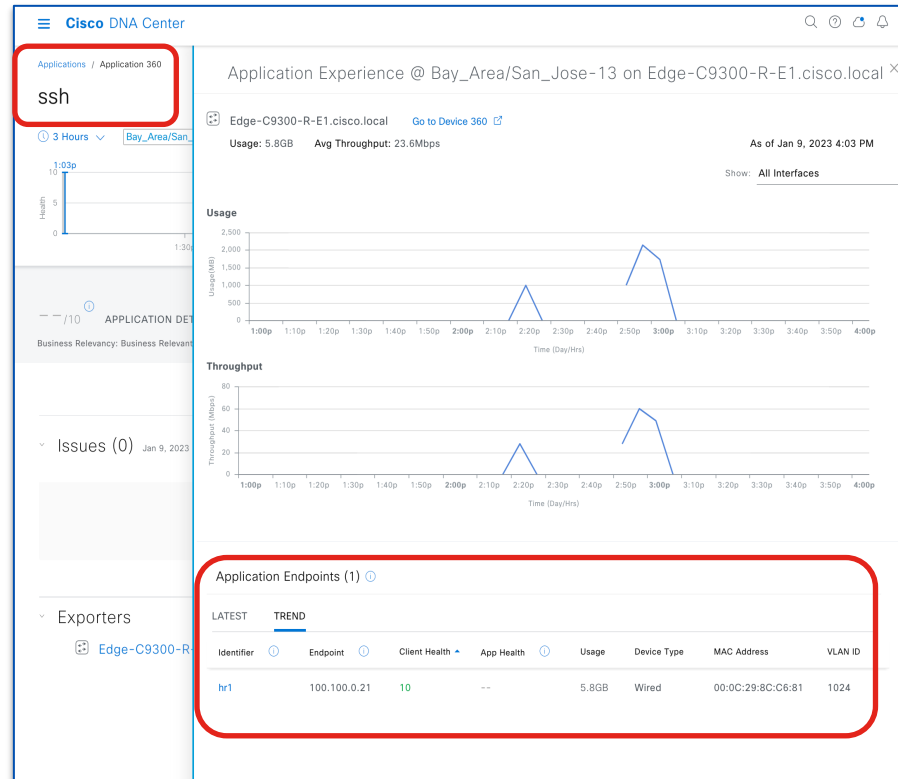
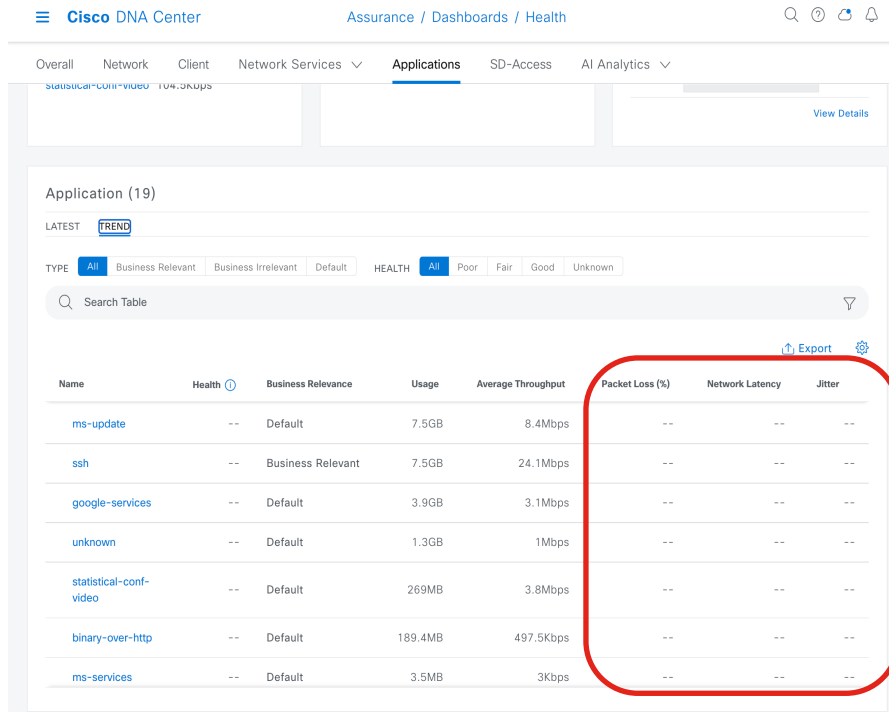
# Application Telemetry from Access Switches

## Overview

- Flexible NetFlow config to match applications orchestrated from Catalyst Center
- Supported for Software Defined Access (SDA) fabric or non-fabric
- Switches must be activated with DNA-Advantage licenses
- Quantitative visibility only – no performance metric (loss, jitter, latency)
- Application customization through CBAR

# Application Telemetry from Switches

- Switch-based Application Visibility does not include performance metrics

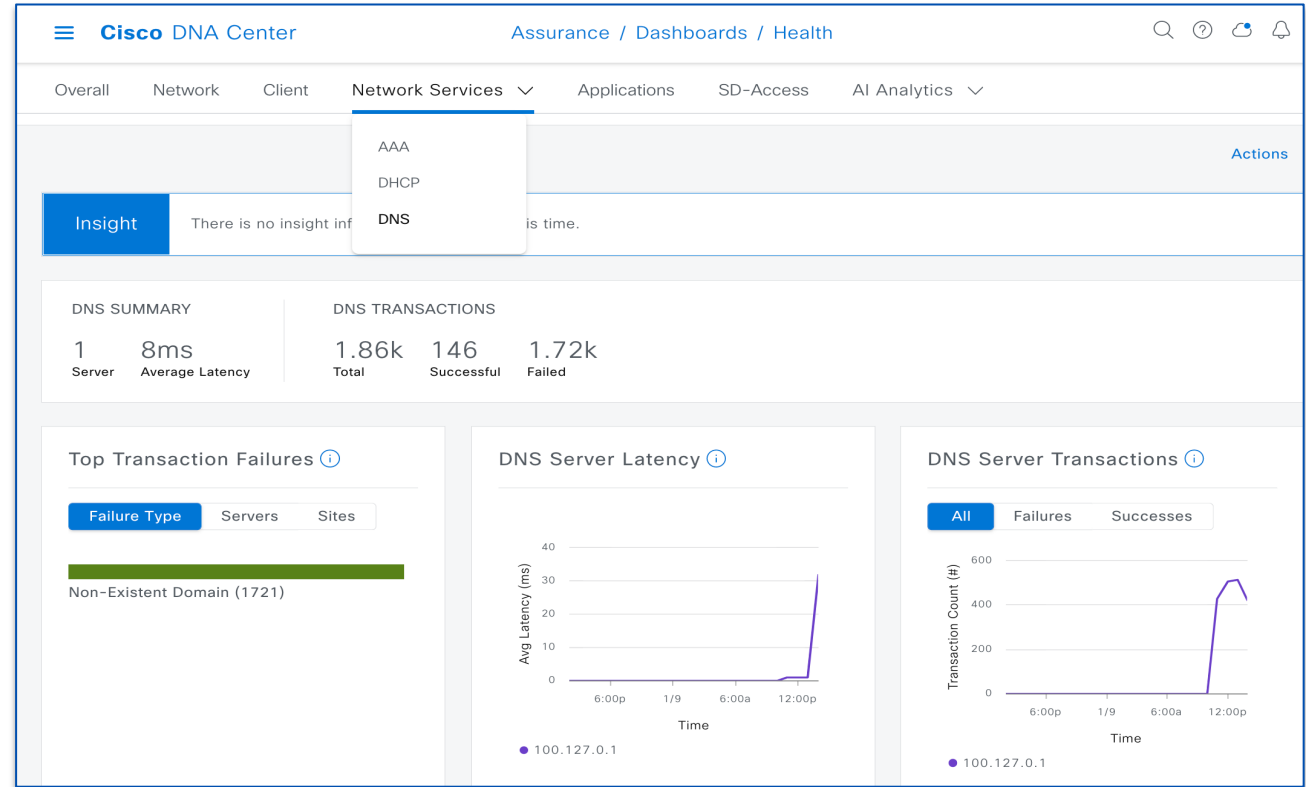


- Client level Application usage visibility

# Application Telemetry from Switches - DNS

## DNS Health Visibility

- Utilize time travel feature to view DNS metrics at specific points in time
- View summary of all DNS servers and average latency
- View all successful and failed transactions
- Obtain AI insights into DNS events



# Application Telemetry from Access Switches

## Deployment Considerations

- Netconf Enablement on Switches **Highly Recommended**
  - Enable through Catalyst Center (PnP/LAN Auto onboarding or via Discovery tool)
  - Allows for additional telemetry info for PoE status, AAA/SGT counters, LISP status
- Enabling Application Telemetry pushes NetFlow monitor to ACCESS mode ports
  - Manually add keyword “lan” to interface description of desired interfaces to forcibly apply NF monitor
- Cannot incrementally enable Application Telemetry on new interfaces
  - Disable, then re-enable Application Telemetry for entire device
  - Alternatively, use Template or manual CLI to apply required configuration to new interfaces

# Switch Application Telemetry Deployment

- Switches MUST be in Inventory
- Switches MUST in be Access Device Role

Click on Pencil icon to change role

The screenshot shows the Cisco Catalyst Center interface. The top navigation bar includes the Cisco logo, 'Catalyst Center', and 'Provision / Inventory'. Below this, there are tabs for 'Global', 'All', 'Routers', 'Switches', 'Wireless Controllers', 'Access Points', and 'Sensors'. The 'Switches' tab is selected. The main content area shows a table of devices with columns: Device Name, IP Address, Manageability, Device Role, Application Telemetry, and Compliance. The 'Device Role' column is highlighted with a red box, and a red arrow points to the pencil icon next to the 'ACCESS' role for the 'Border.cisco.local' device.

Device Name	IP Address	Manageability	Device Role	Application Telemetry	Compliance
Border.cisco.local	100.124.0.1	Managed	ACCESS	Enabled	Non-Compliant
Edge-R	100.124.126.129	Managed	ACCESS	Not Provisioned	Non-Compliant
Edge-L	100.124.126.134	Managed	ACCESS	Not Provisioned	Compliant

# Switch Application Telemetry Deployment

## Catalyst Center 2.3.5.x and below

- Initiate Application Telemetry via Provision -> Inventory

The screenshot shows the Cisco Catalyst Center web interface. At the top, the 'Provision / Inventory' tab is selected. A notification bar indicates that application telemetry actions will move to 'Application Visibility Setup'. Below this, the 'Devices (4)' section is active, with a focus on 'CustomView'. A search bar is present. The '3 Selected' devices are listed: 'Border.cisco.local', 'Edge-R', 'Edge-L', and 'C9800-CL'. The 'Edge-R', 'Edge-L', and 'C9800-CL' devices are selected, indicated by blue checkmarks in a column on the left. A red box highlights this selection column. An 'Actions' dropdown menu is open, with 'Telemetry' selected, also highlighted by a red box. This opens a sub-menu with three options: 'Enable Application Telemetry', 'Disable Application Telemetry', and 'Update Telemetry Settings'. The 'Enable Application Telemetry' option is highlighted by a red box. The main table displays the status of application telemetry for the selected devices. The 'Border.cisco.local' device has 'Application Telemetry' set to 'Disabled'. The 'Edge-R', 'Edge-L', and 'C9800-CL' devices have 'Application Telemetry' set to 'Not Provisioned'.

Device Name	Manageability	Device Role	Application Telemetry
Border.cisco.local	Managed	ACCESS	Disabled
Edge-R		ACCESS	Not Provisioned
Edge-L		ACCESS	Not Provisioned
C9800-CL		ACCESS	Not Provisioned

# Switch Application Telemetry Deployment

- NetFlow configuration pushed to Access Switches (IPv4) – Flow Record

## flow record dnarecord

```
match ipv4 version
match ipv4 protocol
match application name
match connection client ipv4 address
match connection server ipv4 address
match connection server transport port
match flow observation point
collect timestamp absolute first
collect timestamp absolute last
collect flow direction
collect connection initiator
collect connection client counter packets long
collect connection client counter bytes network long
collect connection server counter packets long
collect connection server counter bytes network long
collect connection new-connections
collect datalink mac source address input
```

## flow record dnarecord\_dns

```
match ipv4 version
match ipv4 protocol
match connection client ipv4 address
match connection server ipv4 address
match flow observation point
match application dns qtype
match application dns rcode
collect datalink mac source address input
collect timestamp absolute first
collect timestamp absolute last
collect connection client counter packets long
collect connection client counter bytes network long
collect connection server counter packets long
collect connection server counter bytes network long
collect application dns requests
collect application dns delay response sum
```



# Switch Application Telemetry Deployment

- NetFlow configuration pushed to Access Switches (IPv4) – Flow Exporter and Monitor

## **flow exporter dnacexporter**

```
destination <Catalyst Center IPv4 address>
source Loopback0
transport udp 6007
export-protocol ipfix
option interface-table timeout 300
option vrf-table timeout 300
option sampler-table
option application-table timeout 300
option application-attributes timeout 300
```

## **flow monitor dnacmonitor**

```
exporter dnacexporter
cache timeout inactive 10
cache timeout active 60
record dnacrecord
```

## **flow monitor dnacmonitor\_dns**

```
exporter dnacexporter
cache timeout inactive 10
cache timeout active 60
record dnacrecord_dns
```

# Switch Application Telemetry Deployment

- NetFlow configuration pushed to Access Switches (IPv4) – Flow Interface Monitoring

## **interface GigabitEthernet1/0/1**

```
ip flow monitor dnacmonitor input
ip flow monitor dnacmonitor_dns input
ip flow monitor dnacmonitor output
ip flow monitor dnacmonitor_dns output
```

## **interface GigabitEthernet1/1/2**

```
description lan
ip flow monitor dnacmonitor input
ip flow monitor dnacmonitor_dns input
ip flow monitor dnacmonitor output
ip flow monitor dnacmonitor_dns output
```

keyword “lan” can be manually added to the interface description to forcefully apply NetFlow monitor to an interface not configured with “switchport mode access”

# Switch Application Telemetry Deployment

- NetFlow configuration pushed to Access Switches (IPv6) – Flow Record

## flow record dnacrecord\_v6

```
match ipv6 version
match ipv6 protocol
match application name
match connection client ipv6 address
match connection server ipv6 address
match connection server transport port
match flow observation point
collect timestamp absolute first
collect timestamp absolute last
collect flow direction
collect connection initiator
collect connection client counter packets long
collect connection client counter bytes network long
collect connection server counter packets long
collect connection server counter bytes network long
collect connection new-connections
collect datalink mac source address input
```

## flow record dnacrecord\_dns\_v6

```
match ipv6 version
match ipv6 protocol
match connection client ipv6 address
match connection server ipv6 address
match flow observation point
match application dns qtype
match application dns rcode
collect datalink mac source address input
collect timestamp absolute first
collect timestamp absolute last
collect connection client counter packets long
collect connection client counter bytes network long
collect connection server counter packets long
collect connection server counter bytes network long
collect application dns requests
collect application dns delay response sum
```

# Switch Application Telemetry Deployment

- NetFlow configuration pushed to Access Switches (IPv6) – Flow Exporter and Monitor

## flow exporter dnacexporter


```
destination <Catalyst Center IPv4/IPv6 address>  
source Loopback0  
transport udp 6007  
export-protocol ipfix  
option interface-table timeout 300  
option vrf-table timeout 300  
option sampler-table  
option application-table timeout 300  
option application-attributes timeout 300
```

## flow monitor dnacmonitor\_v6

```
exporter dnacexporter  
cache timeout inactive 10  
cache timeout active 60  
record dnacrecord_v6
```

## flow monitor dnacmonitor\_dns\_v6

```
exporter dnacexporter  
cache timeout inactive 10  
cache timeout active 60  
record dnacrecord_dns_v6
```



If Catalyst Center is deployed in IPv6-only mode, then destination is IPv6 address

# Switch Application Telemetry Deployment

- NetFlow configuration pushed to Access Switches (IPv6) – Flow Interface Monitoring

## **interface GigabitEthernet1/0/1**

```
ipv6 flow monitor dnacmonitor_v6 input  
ipv6 flow monitor dnacmonitor_dns_v6 input  
ipv6 flow monitor dnacmonitor_v6 output  
ipv6 flow monitor dnacmonitor_dns_v6 output
```

## **interface GigabitEthernet1/1/2**

```
description lan  
ipv6 flow monitor dnacmonitor_v6 input  
ipv6 flow monitor dnacmonitor_dns_v6 input  
ipv6 flow monitor dnacmonitor_v6 output  
ipv6 flow monitor dnacmonitor_dns_v6 output
```

# Application **Visibility** from Access Switches

- NBAR (Network-Based Application Recognition)
  - Application classification capability local to each device
- CBAR (Controller-Based Application Recognition)
  - Catalyst Center capability to share and dynamically update NBAR application signatures between network devices
- NBAR classifies >1400 apps natively (including encrypted ones)
- Expand list of 1400+ classified apps through discovered apps or customized apps via CBAR
- Separate feature from Application Telemetry
  - Enablement order does not matter (i.e. can enable NBAR/CBAR prior to App Telemetry)
  - However, requires Application Telemetry to export flow info via NetFlow
- Supported for Software Defined Access (SDA) fabric or non-fabric
- Switches must be activated with DNA-Advantage licenses
- Works in conjunction with Application QoS Policy to push configs for proper queuing policies for specified apps to network infrastructure

# Switch Application Visibility Deployment

## Catalyst Center 2.3.5.x and below

- Enable through Provision > Application Visibility
- Switches must be in Access Role to be “Ready”

Service Catalog / Application Visibility

Setup 1479 Applications 28 Application Sets

1 Enable CBAR 2 Enable Services On devices 3 Connect External Sources

Select the devices on which you like to enable the CBAR or check below to enable all ready devices

☐ Enable CBAR on all ready devices

Device Family **All** Routers Switches Wireless Controllers Telemetry Appliance

CBAR Readiness **All** Ready Not ready Enabled

Site Devices (3)

<input type="checkbox"/>	Device name	Management IP	Site	Fabric	Device Type	Role	OS Image	Active recognition method	Readiness Status	WAN Interfaces
<input type="checkbox"/>	Border-C9300.cisco.local	100.124.0.1	...a/San_Jose-13	Global/Bay_Area...	Cisco Catalyst 9300 Switch	Border Router	17.10.1	Network-based (NBAR)	Not ready	N/A
<input type="checkbox"/>	Edge-C9300-L-E1.cisco.local	100.124.126.133	...se-13/SJ-13-2	Global/Bay_Area...	Cisco Catalyst 9300 Switch	Access switch	17.10.1	Network-based (NBAR)	Ready	N/A
<input type="checkbox"/>	Edge-C9300-R-E1.cisco.local	100.124.126.132	...se-13/SJ-13-1	Global/Bay_Area...	Cisco Catalyst 9300 Switch	Access switch	17.10.1	Network-based (NBAR)	Ready	N/A

3 Records

Showing 3 of 3 [Show more](#)

[Skip](#) [Next](#)

# Switch Application **Visibility** Deployment

## Catalyst Center 2.3.5.x and below



- Enhanced app classification and dynamic Protocol Pack updates through NBAR Cloud



# Switch Application **Visibility** Deployment

## Catalyst Center 2.3.5.x and below



- Obtain credential for NBAR Cloud at Cisco API console
  - <https://apiconsole.cisco.com/apps/myapps>
  - Create app service tying in Client Credentials and at least Hello API

The screenshot shows the Cisco API Console interface. The top navigation bar includes 'Cisco API Console', 'Documentation', 'Interactive APIs', and 'My Apps & Keys'. The 'My Apps & Keys' tab is selected and circled in red. Below this, the 'My Apps & Keys' section has two sub-tabs: 'Applications' and 'Keys'. The 'Applications' tab is active, and the 'Register a New App' button is circled in red. A red arrow points from this button to the 'Register an Application' form on the right.

**Register an Application**

Get a key and register your application using the form below to start working with our APIs.

**Application Details**

Name of your application: \*

AppViz for NBAR Cloud

Application description (optional):

NBAR Cloud enablement for Cisco DNA Center Application Visibility and AI Endpoint Analytics

**OAuth2.0 Credentials**

Choose at least one Grant Type:

☐ Resource Owner Credentials ☐ Authorization Code ☒ Client Credentials ☐ Implicit

☐ Refresh Token (the grant type you selected allows you to refresh the token)

**Rate Limits**

10 Calls per second  
100,000 Calls per day

☒ Hello API

☒ Hello API

**RATE LIMITS**

100 Calls per second  
500,000 Calls per day

☐ HelloCommerce API

☒ HelloCommerce API

**RATE LIMITS**

10 Calls per second  
100,000 Calls per day

**Terms of Service**

Please review the services you have selected above and agree to the [terms of service](#)

☒ I agree to the terms of service

**Register**

# Switch Application **Visibility** Deployment

## Catalyst Center 2.3.5.x and below



- Input obtained credential to enable NBAR Cloud

The image shows two side-by-side screenshots. The left screenshot is from the Cisco API Console, specifically the 'My Apps & Keys' section. It shows a table of registered applications. A red box highlights the first application, 'Hello API', and a red arrow points from this box to the right screenshot. The right screenshot is from the Cisco DNA Center, showing the 'Configure NBAR Cloud' dialog. A red box highlights the 'Enable' checkbox, which is checked. Another red box highlights the 'Save' button at the bottom right of the dialog.

**API Console Portal**

My Apps & Keys

Applications Keys Register a New App

AppViz for NBAR Cloud

NBAR Cloud enablement for Cisco DNA Center Application Visibility and AI Endpoint Analytics

Registered: 1/10/23 4:39 pm Grant Type: Client Credentials

API	KEY	CLIENT SECRET	STATUS
Hello API	jprpjtq976b4hjyx5vqxqrm	G4tvZNsCSmGMtrrdmdjFhvp6	active

Edit This App Delete This App Add APIs

**Configure NBAR Cloud**

☒ Enable

Enter Client ID and Client Secret retrieved from [Cisco API Console](#)

Client ID\*  
jprpjtq976b

Client Secret\*  
G4tvZNsCSmGMtrrdmdjFhvp6

Organization Name\*  
Cisco

☒ Enable Protocol Pack Auto Update

☒ Improve my network using NBAR Cloud telemetry

NBAR classification telemetry data is being sent to region  
USA

Cancel Save

API Console Portal

Cisco DNA Center

# Switch Application **Visibility** Deployment

- NBAR/CBAR configuration pushed to Switches

```
platform wdvavc serviceability
```

```
avc sd-service
```

```
segment AppRecognition  
controller
```

```
address <Catalyst Center IPv4 address>
```

```
destination-ports sensor-exporter 21730
```

```
dscp 16
```

```
source-interface Loopback0
```

```
transport application-updates https url-prefix sdavc
```

```
interface GigabitEthernet1/0/1
```

```
ip nbar protocol-discovery
```

App classification via NBAR done locally on switches and then exported to Catalyst Center in JSON format using separate UDP stream

Lo0 source interface if SDA fabric node; uplink interface otherwise

NBAR command applies to all ports by default; can selectively disable ports through “re-configure” link on Application Visibility dashboard

# Switch Application **Visibility** Deployment

- NBAR/CBAR verification on Switches

```
Edge-C9300-R-E1#show ip nbar protocol-pack loaded
```

```
Loaded Protocol Pack(s):
```

```
Name: Advanced Protocol Pack
Version: 63.0
Publisher: Cisco Systems Inc.
NBAR Engine Version: 47
State: Active
```

} IOS-XE native protocol pack

```
Name: Secondary Protocol Pack
Version: 00a884d9b76bce6bf667515b50b0c8
Publisher: SD-AVC
NBAR Engine Version: 1001
Creation time: Thu Jan 12 17:08:11 UTC 2023
NBAR PP level: 1
File: bootflash:/sdavc/PPDK_AppRecognition_00a884d9b76bce6bf667515b50b0c8.pack
State: Active
```

} CBAR installed protocol pack

# Switch Application **Visibility** Deployment

- NBAR/CBAR verification on Switches

```
Edge-C9300-R-E1#show avc sd-service info summary
Status: CONNECTED
```

```
Device ID: Edge-C9300-R-E1.cisco.local
Device segment name: AppRecognition
Device address: 100.124.126.132
Device OS version: 17.10.01
Device type: C9300-48U
```

Active controller:

```
Type   : Primary
IP     : 100.64.0.101
Status: Connected
Version      : 4.4.0
```

Last connection: 20:13:17.000 UTC Thu Jan 12 2023

Active SDAVC import files:

```
Protocol pack:      Not loaded
Secondary protocol pack:
```

PPDK AppRecognition 00a884d9b76bce6bf667515b50b0c8.pack

Rules pack: Not loaded

```
Edge-C9300-R-E1#sh avc sd-service info summary
Status: CONNECTED
```

```
Device ID: Edge-C9300-R-E1.cisco.local
Device segment name: AppRecognition
Device address: 100.124.126.132
Device OS version: 17.10.01
Device type: C9300-48U
```

Active controller:

```
Type   : Primary
Address : 100.64.0.101
Status  : Connected
Version      : 4.4.0
```

Last connection: 22:30:35.000 UTC Thu Jan 12 2023

Active SDAVC import files:

```
Protocol pack:      Not loaded
Secondary protocol pack:
```

PPDK AppRecognition 00a884d9b76bce6bf667515b50b0c8.pack

Rules pack: pp\_update\_AppRecognition\_a\_v2\_b31c143960a1.pack

Moments later

# Switch Application **Visibility** Deployment

- NBAR/CBAR classified Top-N applications (reflected on Catalyst Center)

```
Edge-C9300-R-E1#sh ip nbar protocol-discovery top-n
```

```
GigabitEthernet1/0/1
```

```
Last clearing of "show ip nbar protocol-discovery" counters 07:08:19
```

	Input	Output
	-----	-----
Protocol	Packet Count	Packet Count
	Byte Count	Byte Count
	5min Bit Rate (bps)	5min Bit Rate (bps)
	5min Max Bit Rate (bps)	5min Max Bit Rate (bps)
	-----	-----
ms-services	3915973	9324733
	261709271	11022843082
	3000	3000
	1649000	68846000
ssh	2030585	703017
	3068521966	53667192
	65800000	1175000
	65800000	1175000
google-services	1048736	2242508
	68295263	2290752005
	0	0
	486000	15529000
unknown	28192	79902
	1947180	103014893
	0	0

# Applications – Application Telemetry and CBAR

Catalyst Center 2.3.7.x and above

- Application Telemetry and CBAR AUTOMATICALLY enabled for devices in Access role, when assigned to network site (e.g. PnP onboarding, manual discovery with site assignment)
- To prevent Application Telemetry and CBAR from automatically enabled, do not assign device to site during Discovery or PnP onboarding
- To disable Application Telemetry and CBAR on devices, go to Provision -> Application Visibility Setup

# Applications – Application Telemetry and CBAR

Catalyst Center 2.3.7.x and above

- Disable (and Enable) Application Telemetry via Provision -> Application Visibility -> Network Devices Enablement

Services / Service Catalog / Application Visibility Setup

Service Catalog / Application Visibility Setup

Overview **Network Devices Enablement** 1479 Applications 28 Application Sets CBAR Extensions

Site Devices (4) Last Updated: 11:55 pm Refresh

Device Family: All Routers Switches Wireless Controllers Telemetry Appliance

CBAR Readiness: All Ready Not ready Enabled

Telemetry Readiness: All Ready Not ready Enabled

Filter: CBAR Application Telemetry Update Protocol Pack

Device name Enable Application Telemetry Disable Application Telemetry

Device name	IP Address	Device Type	Recognition method	CBAR Deployment Status	Application Telemetry Deployment Status
<input type="checkbox"/> Border.cisco.local			Network-based (NBAR)	Not deployed	Not deployed
<input checked="" type="checkbox"/> C9800-CL.cisco.local	100.126.0.6	Network-based (NBAR)	Not deployed	Not deployed	Not deployed
<input checked="" type="checkbox"/> Edge-L	100.124.126.134	Network-based (NBAR)	Not deployed	Not deployed	Not deployed
<input checked="" type="checkbox"/> Edge-R	100.124.126.129	Network-based (NBAR)	Not deployed	Not deployed	Not deployed

Showing 4 of 4 Show more



# Switch Application **Visibility** Deployment

Catalyst Center 2.3.7.x and above

- Option to selectively enable NBAR/CBAR on selected interfaces (default is to enable on all access ports)

The screenshot displays the Cisco Catalyst Center interface for configuring Application Visibility Setup. The left sidebar shows the navigation menu with 'Service Catalog' and 'Application Visibility Setup'. The main content area is divided into two panels.

The left panel, titled 'Network Devices Enablement', shows a table of site devices. The table has columns for 'Device name', 'Management IP', and 'Active recognition'. The devices listed are 'Border.cisco.local', 'C9800-CL.cisco.local', 'Edge-L', and 'Edge-R'. The 'Edge-L' and 'Edge-R' devices are selected, indicated by blue checkmarks in the 'Active recognition' column.

The right panel, titled 'Enable CBAR', shows a list of interfaces. The table has columns for 'Interfaces' and 'Status'. The interfaces listed are 'GigabitEthernet2/0/9', 'GigabitEthernet2/0/8', 'GigabitEthernet2/0/7', 'GigabitEthernet2/0/6', 'GigabitEthernet2/0/5', 'GigabitEthernet2/0/4', 'GigabitEthernet2/0/3', and 'GigabitEthernet2/0/2'. All interfaces have their status toggles set to 'On'.

# Applications – Application Telemetry and CBAR

Catalyst Center 2.3.7.x and above

- Enhanced app classification and dynamic Protocol Pack updates through CBAR Cloud

The screenshot shows the Catalyst Center interface for Application Visibility Setup. The breadcrumb trail is Services / Service Catalog / Application Visibility Setup. The left sidebar shows a search hierarchy with 'Global' and 'Bay Area' options. The main content area has tabs for Overview, Network Devices Enablement, 1479 Applications, 28 Application Sets, and CBAR Extensions (highlighted with a red box). Under CBAR Extensions, there is a 'CBAR Cloud' link (highlighted with a red box) and an 'Enable' button (highlighted with a red box). Below this, a checkbox labeled 'Improve network visibility by sharing telemetry' is checked. The section 'CBAR Dynamic Application Feeds' shows 'Enable Application Feeds Update' set to 'All'. A table lists various applications with their last update times and application counts.

Application	Last updated on Nov 6, 2023 18:04	Applications
Telegram	1 applications	
Google Meet	1 applications	
ServiceNow	1 applications	
Sugarcrm	1 applications	
SAP	1 applications	
HubSpot	1 applications	
RingCentral	1 applications	
Github	1 applications	
Crashplan	1 applications	
O365	15 applications	
Intuit	1 applications	
Box	1 applications	
Workday	1 applications	
Zscaler	1 applications	
Microsoft Intune	1 applications	
Atlassian	2 applications	
Code42	1 applications	
Amazon Chime	2 applications	

Buttons: Reset, Apply

# Applications – Application Telemetry and CBAR

Catalyst Center 2.3.7.x and above

- Enhanced app classification and dynamic Protocol Pack updates through CBAR Cloud

Service Catalog / Application Visibility Setup

Overview Network Devices Enablement 1479 Applications 28 Application Sets CBAR Extensions

CBAR Health Issues and Remedies

P1 0 Issues P2 0 Issues P3 1 Issues

Device Protocol Pack outdated [Show devices](#)

Site Devices (4)

Device Family: All Routers Switches Wireless Controllers Telemetry Appliance

CBAR Readiness: All Ready Not ready Enabled

Telemetry Readiness: All Ready Not ready Enabled

Filter: CBAR Application Telemetry Update Protocol Pack

Device name	Management IP	Deployment Status	Application Telemetry Deployment Status
Border.cisco.local	100.124.0.1	Deployed	Not deployed
C9800-CL.cisco.local	100.126.0.6	Deployed	Completed
Edge-L	100.124.126.134	Deleted and configure	Completed
Edge-R	100.124.126.129	Completed	Completed

Showing 4 of 4 [Show more](#)

**Warning**

Enabling Automatic Protocol Pack Update, automatically updates the NBAR protocol pack on your devices, once a new update appears in the cloud. These updates may actively impact your QoS marking policies as application classification rules may dynamically change.

Are you sure you want to enable automatic protocol pack updates?

No Yes

# Application Telemetry and Visibility for Wireless

- Application telemetry with performance metrics for wireless clients
- Supported for APs in local, Flex, and SDA Fabric deployment mode
  - Flex and SDA Fabric support requires minimum WiFi6 APs (C91xx) running IOS-XE 17.10.x and Cisco Catalyst Center 2.3.5.x
  - Support for Guest SSIDs, on top of previously supported Enterprise SSIDs, requires minimum Cisco Catalyst Center 2.3.5.x and IOS-XE 17.10.x
- All flavors of C9800 supported (virtual or physical appliance, embedded wireless controller on C9300/C9400 switches)
- Newly added SSIDs will not inherit Application Telemetry push
  - Forced Update of Telemetry in Inventory does not update App Telemetry
  - Need to disable Application Telemetry -> re-enable Application Telemetry
  - Disable/Enable App Telemetry causes existing wireless policy to bounce -> may affect wireless client connectivity momentarily
  - Can use Template or manual CLI to add NetFlow config to new wireless SSIDs

# Application Telemetry and Visibility Deployment for Wireless

Catalyst Center 2.3.7.x and above

- Enable through Provision > Application Visibility
- WLC must have WLAN and AP assigned to be “Ready” for CBAR

The screenshot shows the Cisco Catalyst Center interface for Application Visibility. The 'Network Devices Enablement' tab is active, showing 1479 Applications and 28 Application Sets. The 'Filter' dropdown is set to 'CBAR'. A context menu is open over the 'CBAR' filter button, showing options like 'Enable CBAR on selected devices' and 'Enable CBAR on all ready devices'. The table below lists devices with their status.

Device	IP	Active recognition method	CBAR Deployment Status	Application Telemetry Deployment Status
C9800-CL.cisco.local	100.126.0.6	Network-based (NBAR)	Not deployed	Not deployed
Cat3650-Old.cisco.local	100.124.127.36	IP/Port	Not deployed	Not deployed

# Application Telemetry and Visibility Deployment for Wireless

Catalyst Center 2.3.7.x and above

- SSID will flap when Application Telemetry is enabled/disabled

Enable Application Telemetry

By default, all access interfaces on a switch OR all LAN-facing interfaces on a router will be provisioned to send Netflow with Application telemetry.

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 only those interfaces will be monitored.

By default, all non-guest WLANs on Wireless Controllers will be provisioned to send Netflow with Application telemetry.

To override this default behavior, tag specific WLAN profile names with keyword "lan".

Once specific WLANs are tagged, only those WLANs will be monitored.

For each wireless controller, select the AP modes where you would like to enable application telemetry.

For Catalyst 9800 Series Wireless Controllers, the application telemetry source is always Netflow.

For AireOS wireless controllers, the application telemetry source may be either Netflow or WSA (Wireless Service Assurance).

Enabling or disabling application telemetry on the selected SSID types will cause a disruption in network services.

Note: In order to update application telemetry configuration on the WLC, disable application telemetry first and then re-enable it. To do so, please use the Disable/Enable Application Telemetry buttons in the Actions menu.

C9800-CL-cisco.local

☒ Local

☐ Flex/Fabric

☐ Include Guest SSIDs [0](#)

Telemetry Source: **NetFlow**

Note: Devices require DNA Advantage license for this feature to be enabled.

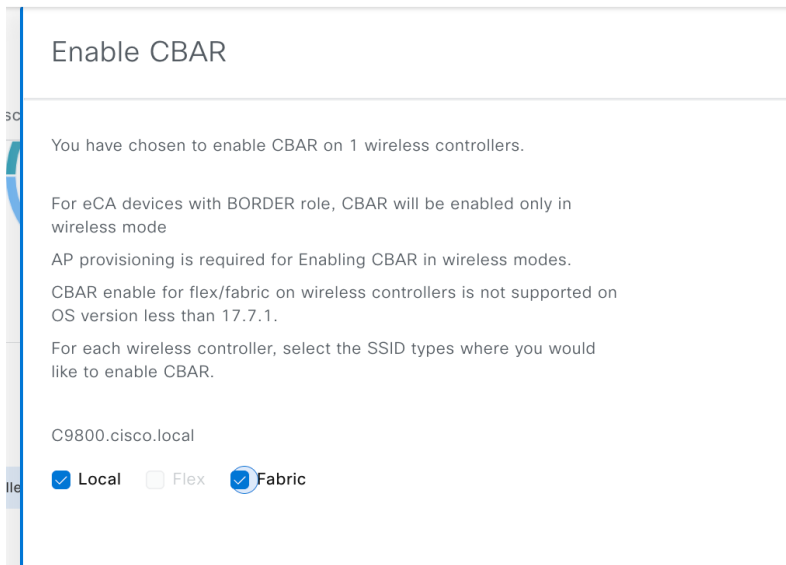
Cancel

Enable

# Application Telemetry and Visibility Deployment for Wireless

Catalyst Center 2.3.7.x and above

- Specify SSID type to enable CBAR



The screenshot shows the 'Enable CBAR' configuration page in Catalyst Center. The page has a title 'Enable CBAR' at the top. Below the title, there is a message: 'You have chosen to enable CBAR on 1 wireless controllers.' This is followed by two paragraphs of information: 'For eCA devices with BORDER role, CBAR will be enabled only in wireless mode' and 'AP provisioning is required for Enabling CBAR in wireless modes.' Below these paragraphs, there is a note: 'CBAR enable for flex/fabric on wireless controllers is not supported on OS version less than 17.7.1.' This is followed by another instruction: 'For each wireless controller, select the SSID types where you would like to enable CBAR.' At the bottom, there is a section for the controller 'C9800.cisco.local' with three radio button options: 'Local' (selected with a blue checkmark), 'Flex' (unselected), and 'Fabric' (selected with a blue checkmark).

Enable CBAR

You have chosen to enable CBAR on 1 wireless controllers.

For eCA devices with BORDER role, CBAR will be enabled only in wireless mode

AP provisioning is required for Enabling CBAR in wireless modes.

CBAR enable for flex/fabric on wireless controllers is not supported on OS version less than 17.7.1.

For each wireless controller, select the SSID types where you would like to enable CBAR.

C9800.cisco.local

☒ Local ☐ Flex ☒ Fabric

# Wireless Application Telemetry Deployment

- NetFlow configuration pushed to standalone C9800 Wireless controller – Flow Exporter (SDA, Flex, Non-Fabric)

## **flow exporter avc\_exporter**

```
destination <Catalyst Center IPv4 Address>  
source <Source-Interface>  
transport udp 6007
```

## **export-protocol ipfix**

```
option vrf-table timeout 300  
option ssid-table timeout 300  
option application-table timeout 300  
option application-attributes timeout 300
```

## **flow exporter avc\_local\_exporter**

```
destination local wlc
```

## **flow exporter avc\_exporter\_v9**

```
destination <Cisco DNA Center IPv4 Address>  
source <Source-Interface>  
transport udp 6007
```

```
option vrf-table timeout 300  
option ssid-table timeout 300  
option application-table timeout 300  
option application-attributes timeout 300
```



# Wireless Application Telemetry Deployment

- NetFlow configuration pushed to standalone C9800 Wireless controller – Flow Record and Monitor (SDA or Flex Wireless)

**flow monitor avc\_ipv4\_assurance**

```
exporter avc_exporter
exporter avc_local_exporter
cache timeout active 60
record wireless avc ipv4 assurance
```

**flow monitor avc\_ipv4\_assurance\_rtp**

```
exporter avc_exporter
cache timeout active 60
record wireless avc ipv4 assurance-rtp
```

**flow monitor avc\_ipv4\_assurance\_v9**

```
exporter avc_exporter_v9
cache timeout active 60
record wireless avc ipv4 assurance
```

**flow monitor avc\_ipv4\_assurance\_rtp\_v9**

```
exporter avc_exporter_v9
cache timeout active 60
record wireless avc ipv4 assurance-rtp
```

**flow monitor avc\_ipv4\_assurance\_dns**

```
exporter avc_exporter
cache timeout active 60
record wireless avc ipv4 assurance-dns
```

Built-in Flow Records

**flow monitor avc\_ipv6\_assurance**

```
exporter avc_exporter
exporter avc_local_exporter
cache timeout active 60
record wireless avc ipv6 assurance
```

**flow monitor avc\_ipv6\_assurance\_rtp**

```
exporter avc_exporter
cache timeout active 60
record wireless avc ipv6 assurance-rtp
```

**flow monitor avc\_ipv6\_assurance\_v9**

```
exporter avc_exporter_v9
cache timeout active 60
record wireless avc ipv6 assurance
```

**flow monitor avc\_ipv6\_assurance\_rtp\_v9**

```
exporter avc_exporter_v9
cache timeout active 60
record wireless avc ipv6 assurance-rtp
```

**flow monitor avc\_ipv6\_assurance\_dns**

```
exporter avc_exporter
cache timeout active 60
record wireless avc ipv6 assurance-dns
```

**wireless profile policy <POLICY-NAME>**

```
ipv4 flow monitor avc_ipv4_assurance_v9 input
ipv4 flow monitor avc_ipv4_assurance_rtp_v9 input
ipv4 flow monitor avc_ipv4_assurance_v9 output
ipv4 flow monitor avc_ipv4_assurance_rtp_v9 output
ipv6 flow monitor avc_ipv6_assurance_v9 input
ipv6 flow monitor avc_ipv6_assurance_rtp_v9 input
ipv6 flow monitor avc_ipv6_assurance_v9 output
ipv6 flow monitor avc_ipv6_assurance_rtp_v9 output
```

SDA/Flex export in  
FNFv9 format; no DNS  
Health Visibility

# Wireless Application Telemetry Deployment

- NetFlow configuration pushed to standalone C9800 Wireless controller – Flow Record and Monitor (Non-Fabric Wireless)

## flow monitor avc\_ipv4\_assurance

```
exporter avc_exporter
exporter avc_local_exporter
cache timeout active 60
record wireless avc_ipv4_assurance
```

## flow monitor avc\_ipv4\_assurance\_rtp

```
exporter avc_exporter
cache timeout active 60
record wireless avc_ipv4_assurance-rtp
```

## flow monitor avc\_ipv4\_assurance\_v9

```
exporter avc_exporter_v9
cache timeout active 60
record wireless avc_ipv4_assurance
```

## flow monitor avc\_ipv4\_assurance\_rtp\_v9

```
exporter avc_exporter_v9
cache timeout active 60
record wireless avc_ipv4_assurance-rtp
```

## flow monitor avc\_ipv4\_assurance\_dns

```
exporter avc_exporter
cache timeout active 60
record wireless avc_ipv4_assurance-dns
```

## flow monitor avc\_ipv6\_assurance

```
exporter avc_exporter
exporter avc_local_exporter
cache timeout active 60
record wireless avc_ipv6_assurance
```

## flow monitor avc\_ipv6\_assurance\_rtp

```
exporter avc_exporter
cache timeout active 60
record wireless avc_ipv6_assurance-rtp
```

## flow monitor avc\_ipv6\_assurance\_v9

```
exporter avc_exporter_v9
cache timeout active 60
record wireless avc_ipv6_assurance
```

## flow monitor avc\_ipv6\_assurance\_rtp\_v9

```
exporter avc_exporter_v9
cache timeout active 60
record wireless avc_ipv6_assurance-rtp
```

## flow monitor avc\_ipv6\_assurance\_dns

```
exporter avc_exporter
cache timeout active 60
record wireless avc_ipv6_assurance-dns
```

Non-fabric export in  
IPFIX format and  
includes DNS Health  
Visibility

## wireless profile policy <POLICY-NAME>

```
ipv4 flow monitor avc_ipv4_assurance input
ipv4 flow monitor avc_ipv4_assurance_dns input
ipv4 flow monitor avc_ipv4_assurance_rtp input
ipv4 flow monitor avc_ipv4_assurance output
ipv4 flow monitor avc_ipv4_assurance_dns output
ipv4 flow monitor avc_ipv4_assurance_rtp output
ipv6 flow monitor avc_ipv6_assurance input
ipv6 flow monitor avc_ipv6_assurance_dns input
ipv6 flow monitor avc_ipv6_assurance_rtp input
ipv6 flow monitor avc_ipv6_assurance output
ipv6 flow monitor avc_ipv6_assurance_dns output
ipv6 flow monitor avc_ipv6_assurance_rtp output
```

# Wireless Application Telemetry Deployment

- NetFlow configuration pushed to embedded C9800 Wireless controller on C9300/C9400 - Flow Exporter (SDA Wireless)

## **flow exporter avc\_exporter\_v9**

```
destination <Catalyst Center IPv4 Address>  
source Loopback0  
transport udp 6007  
option vrf-table timeout 300  
option ssid-table timeout 300  
option application-table timeout 300  
option application-attributes timeout 300
```

Source is Loopback0 for  
embedded wireless  
controller on C9300/C9400

# Wireless Application Telemetry Deployment



For Your  
Reference

- NetFlow configuration pushed to embedded C9800 Wireless controller on C9300/C9400 – Flow Record and Monitor (SDA Wireless)

## flow monitor avc\_ipv4\_assurance\_v9

```
exporter avc_exporter_v9
cache timeout active 60
record wireless avc ipv4 assurance
```

## flow monitor avc\_ipv4\_assurance\_rtp\_v9

```
exporter avc_exporter_v9
cache timeout active 60
record wireless avc ipv4 assurance-rtp
```

## flow monitor avc\_ipv6\_assurance\_v9

```
exporter avc_exporter_v9
cache timeout active 60
record wireless avc ipv6 assurance
```

## flow monitor avc\_ipv6\_assurance\_rtp\_v9

```
exporter avc_exporter_v9
cache timeout active 60
record wireless avc ipv6 assurance-rtp
```

## wireless profile policy <POLICY-NAME>

```
ipv4 flow monitor avc_ipv4_assurance_v9 input
ipv4 flow monitor avc_ipv4_assurance_rtp_v9 input
ipv4 flow monitor avc_ipv4_assurance_v9 output
ipv4 flow monitor avc_ipv4_assurance_rtp_v9 output
ipv6 flow monitor avc_ipv6_assurance_v9 input
ipv6 flow monitor avc_ipv6_assurance_rtp_v9 input
ipv6 flow monitor avc_ipv6_assurance_v9 output
ipv6 flow monitor avc_ipv6_assurance_rtp_v9 output
```

SDA export in FNFv9  
format; no DNS Health  
Visibility

# Wireless Application **Visibility** Deployment



- NBAR/CBAR configuration pushed to Wireless Controllers

## **avc sd-service**

```
segment AppRecognition
controller
address <Catalyst Center IPv4 address>
destination-ports sensor-exporter 21730
dscp 16
source-interface <Source-Interface>
transport application-updates https url-prefix sdavc
```

## **wireless profile policy <POLICY-NAME>**

```
ip nbar protocol-discovery
```

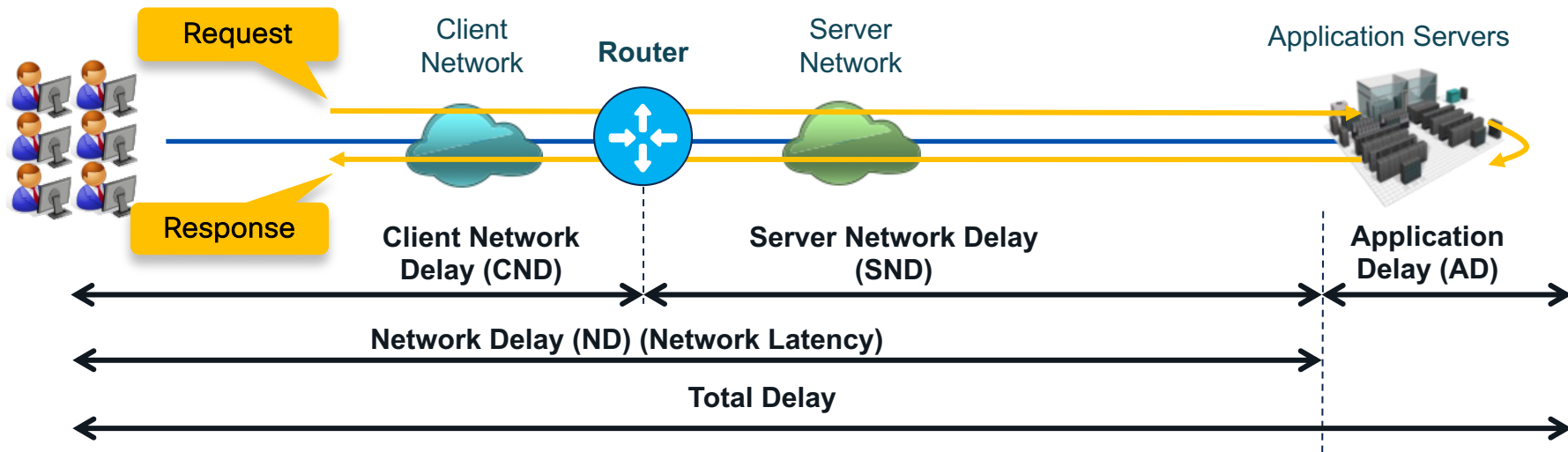
NBAR command applies to wireless profile policy for each SSID

# Application Telemetry and Visibility from Routers

- Routers provide enhanced application performance metrics, e.g. loss, latency, jitter
- Performance monitor configuration orchestrated onto routers
- NetFlow export for data analysis
- Performance metrics only for TCP and RTP media applications
  - Quantitative-only metrics for UDP traffic
- Application Health Scores calculated from performance metrics

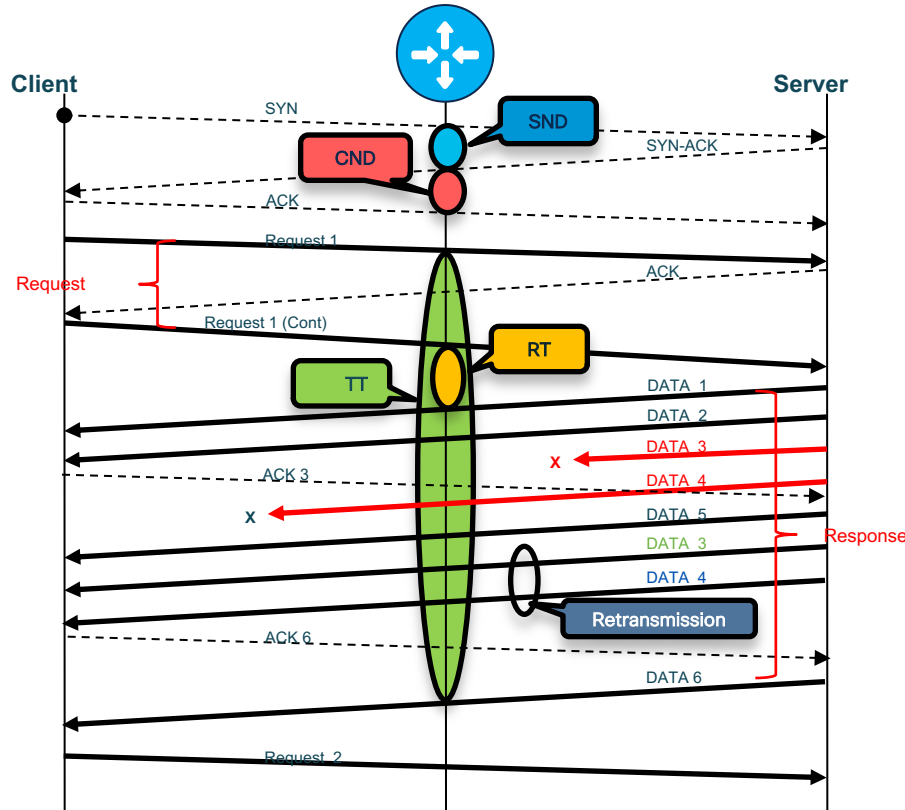
# Application Telemetry and Visibility from Routers

- Application Response Time (ART) calculation broken into components
- Calculated response times provides insight into location of performance bottlenecks
- Latency calculated per application



# Application Telemetry and Visibility from Routers

- Application Response Time calculation for TCP traffic



Network Delay  
(ND, Latency)

$$ND = CND + SND$$

Response  
Time (RT)

$$t(\text{First response pkt}) - t(\text{Last request pkt})$$

Transaction  
Time (TT)

$$t(\text{Last response pkt}) - t(\text{First request pkt})$$

Application  
Delay (AD)

$$AD = RT - SND$$

Retransmission

Loss



# Application Telemetry from Routers

- Flow Records (of type performance-monitor) for TCP, media apps and DNS queries

## Media Monitoring

- RTP SSRC
- RTP Jitter (min/max/mean)
- Transport Counter (expected/loss)
- Media Counter (bytes/packets/rate)
- Media Event
- Collection interval
- TCP MSS
- TCP round-trip time

## Application Response Time

- CND - Client Network Delay (min/max/sum)
- SND - Server Network Delay (min/max/sum)
- ND - Network Delay (min/max/sum)
- AD - Application Delay (min/max/sum)
- Total Response Time (min/max/sum)
- Total Transaction Time (min/max/sum)
- Number of New Connections
- Number of Late Responses
- Number of Responses by Response Time
  - (7-bucket histogram)
- Number of Retransmissions
- Number of Transactions
- Client/Server Bytes
- Client/Server Packets

## Other Metrics

- L3 counter (bytes/packets)
- Flow event
- Flow direction
- Client and server address
- Source and destination address
- Transport information
- Input and output interfaces
- L3 information (TTL, DSCP, TOS, etc.)
- Application information (from NBAR2)
- Monitoring class hierarchy
- DNS requests and responses

Latency, Application Delay, and Loss values shown on Cisco DNA Center Application Assurance

# Application Telemetry and Visibility Deployment for Wireless

## Catalyst Center 2.3.7.x and above

- Enable through Provision > Application Visibility
- For Telemetry, workflow enables all LAN facing ports on router for Telemetry -> Use 'lan' keyword if Telemetry not configured on desired interface

The screenshot shows the Cisco Catalyst Center interface for enabling Application Telemetry. The main panel displays the 'Network Devices Enablement' section with 1479 Applications. A red box highlights the 'Application Telemetry' dropdown menu, which is open, showing 'Enable Application Telemetry' and 'Disable Application Telemetry' options. Another red box highlights the 'Border-C8300' device in the list. The right sidebar shows the 'Enable Application Telemetry' dialog box with instructions on enabling Netflow with application telemetry on 1 Router.

**Enable Application Telemetry**

You have chosen to enable Netflow with application telemetry on 1 Router.

By default, all access interfaces on a switch OR all LAN-facing interfaces on a router will be provisioned to send Netflow with Application telemetry.  
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 only those interfaces will be monitored.

Note: Devices require DNA Advantage license for this feature to be enabled.

**Cancel** **Enable**

# Application Telemetry and Visibility Deployment for Wireless

Catalyst Center 2.3.7.x and above

- For CBAR, need to specify at least one “WAN” interface

The screenshot shows the Catalyst Center interface for Application Visibility. The left sidebar contains a search hierarchy with 'Global' and 'Bay Area' options. The main content area has tabs for 'Overview', 'Network Devices Enablement', '1479 Applications', '28 Application Sets', and 'CBAR Extensions'. Under 'Network Devices Enablement', there are buttons for 'Device Family' (All, Routers, Switches, Wireless Controllers, Telemetry Appliance) and 'Active Recognition Method' (All, CBAR, NBAR, IP/Port, Not Supported). A table lists devices, with 'Border-C8300' highlighted. The 'CBAR Readiness Status' for this device is 'Not ready WAN Interfaces', which is circled in red. A red arrow points from this status to the 'WAN Connectivity Settings' dialog box on the right.

Device name	Management IP	Active recognition method	CBAR Readiness Status	CBAR Deployment Status
Border-C8300	100.124.0.2	Network-based (NBAR)	Not ready WAN Interfaces	Not deployed

The dialog box titled 'WAN Connectivity Settings for Device Border-C8300' shows a table for configuring WAN interfaces. The 'Add Row' button is circled in red. The table has columns for 'Interface', 'Role', 'Service Provider Profile', and 'Sub-Line Rate (Mbps)'. The first row is highlighted, showing 'Select Interface' as 'GigabitEthernet0/0/0', 'Select Role' as 'WAN', and 'Enter value' for 'Sub-Line Rate'. The 'Save' button is at the bottom right.

Interface	Role	Service Provider Profile	Sub-Line Rate (Mbps)
Select Interface GigabitEthernet0/0/0	Select Role WAN	Select Profile	Enter value

# Router Application Telemetry Deployment

- Performance monitor configuration pushed on Router
- Flow records apply to both IPv4 and IPv6 traffic

## performance monitor context tesseract profile application-assurance

```
exporter destination <Catalyst Center IPv4 address> source Loopback0 transport udp port 6007
traffic-monitor assurance-monitor
traffic-monitor assurance-rtp-monitor
traffic-monitor assurance-dns-monitor
```

## interface GigabitEthernet0/0/1

```
description LAN Upstream to Enterprise
performance monitor context tesseract
```

## interface GigabitEthernet0/0/2

```
description Downstream to Access Network lan
performance monitor context tesseract
```

Keyword “lan” manually added to interface description to ensure performance monitor configuration pushed to appropriate interfaces

# Router Application Telemetry Deployment

- NetFlow verification – cache



```
C8300#show performance monitor context tesseract traffic-monitor assurance-dns-monitor cache
CONNECTION IPV4 INITIATOR ADDRESS:      100.100.0.21
CONNECTION IPV4 RESPONDER ADDRESS:      100.127.0.1
FLOW OBSPOINT ID:                       4294967300
APPLICATION DNS QTYPE:
APPLICATION DNS RCODE:
IP VERSION:                             4
IP PROTOCOL:                            17
ip vrf id input:                         0                (DEFAULT)
timestamp abs first:                     18:07:15.383
timestamp abs last:                     18:07:15.449
connection server packets counter:       4
connection client packets counter:       0
connection server network bytes counter: 640
connection client network bytes counter: 0
application dns requests:                4
application dns delay resp sum:          4
```

# Router Application Telemetry Deployment

- NetFlow verification – export (1)

```
C8300#show performance monitor context tesseract exporter
Flow Exporter tesseract-1:
  Description:          performance monitor context tesseract exporter
  Export protocol:      IPFIX (Version 10)
  Transport Configuration:
    Destination type:    IP
    Destination IP address: 100.64.0.101
    Source IP address:   100.124.0.2
    Source Interface:    Loopback0
    Transport Protocol:  UDP
    Destination Port:    6007
    Source Port:         49360
    DSCP:                0x0
    TTL:                255
    Output Features:     Used
[...]
Flow Exporter tesseract-1:
  Packet send statistics (last cleared 1d09h ago):
    Successfully sent:    157584                (210868698 bytes)
```

# Router Application Telemetry Deployment

- NetFlow verification – export (2)

Client send statistics:

Client: Option options interface-table

Records added:	5226
- sent:	5226
Bytes added:	553956
- sent:	553956

Client: Option options application-name

Records added:	603402
- sent:	603402
Bytes added:	50082366
- sent:	50082366

Client: Flow Monitor tesseract-app\_assurance\_ipv4

Records added:	191695
- sent:	191695
Bytes added:	20319670
- sent:	20319670

# Router Application **Visibility** Deployment

- NBAR/CBAR configuration pushed to Routers

## **avc sd-service**

```
segment AppRecognition  
controller  
address <Catalyst Center IPv4 address>  
destination-ports sensor-exporter 21730  
dscp 16  
source-interface Loopback0  
transport application-updates https url-prefix sdavc
```

Lo0 source interface if SDA fabric node;  
uplink interface otherwise

## **interface GigabitEthernet0/0/0**

```
ip nbar protocol-discovery
```

NBAR command pushed to specified "WAN" interface

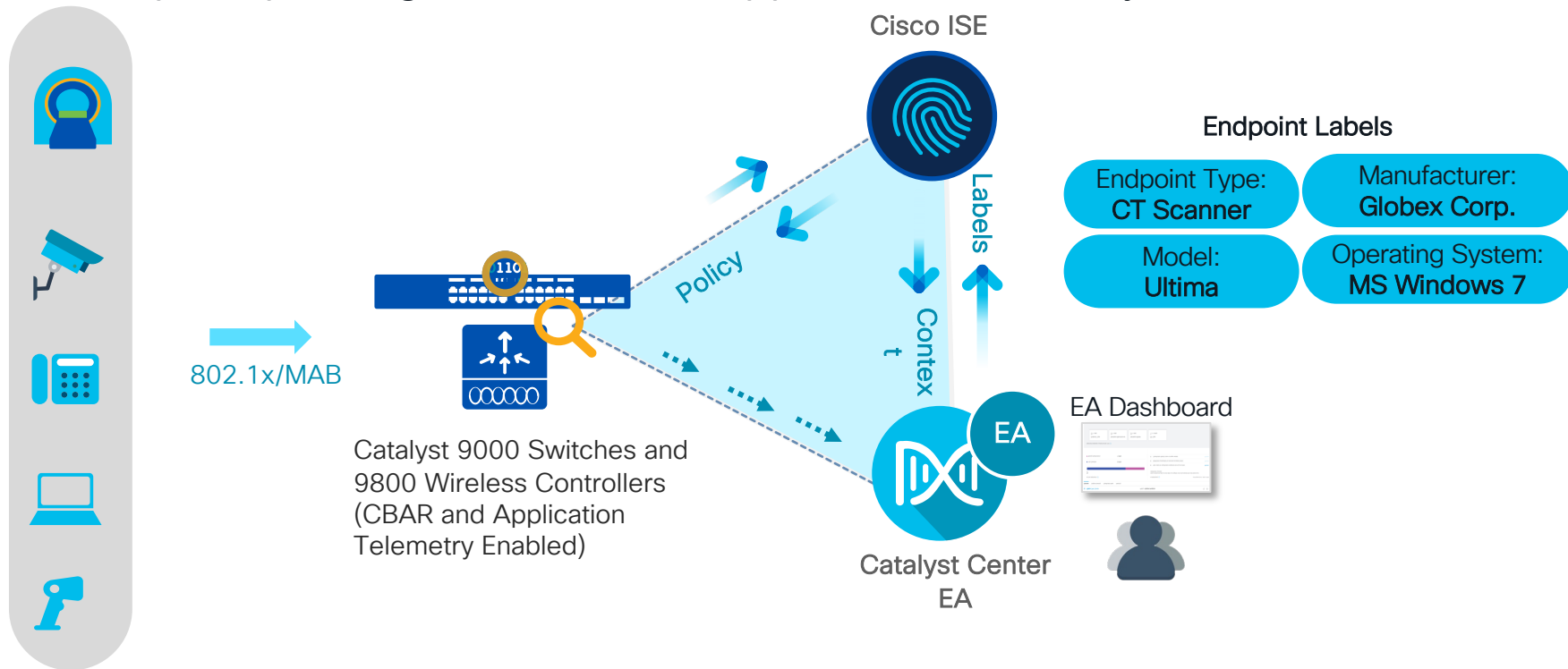


# AI Endpoint and Trust Analytics

- NBAR deep packet inspection allows for initial identification and classification of connected endpoints
- Correlate data from multiple sources to enhance classification
- AI/ML capability to group new/unknown devices
- Custom device labeling and crowdsourcing
- NetFlow export required for Talos and IP Spoof Detection
- Dynamic Trust Score with continuous monitoring of device behavior

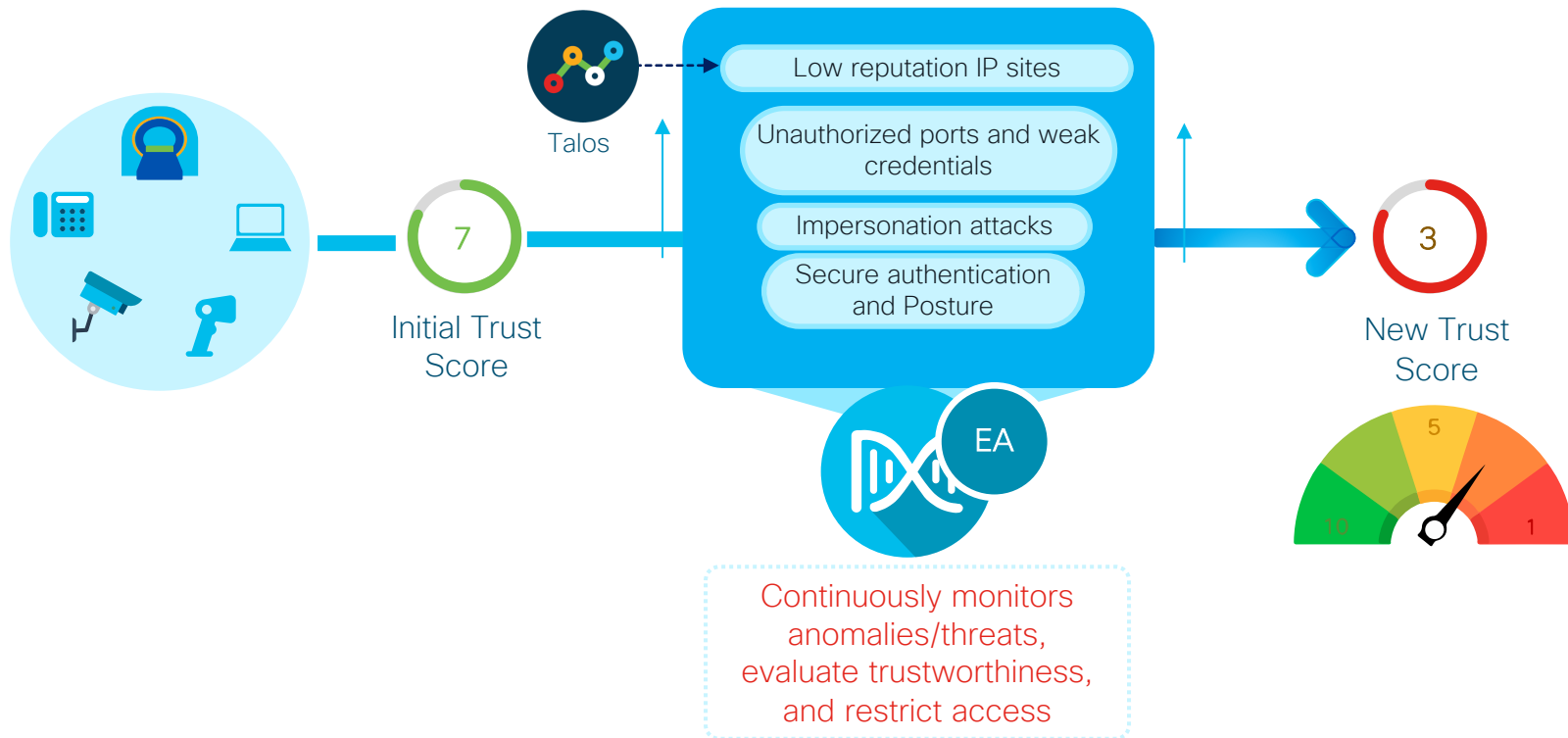
# AI Endpoint and Trust Analytics

- Endpoint profiling via CBAR and Application Telemetry



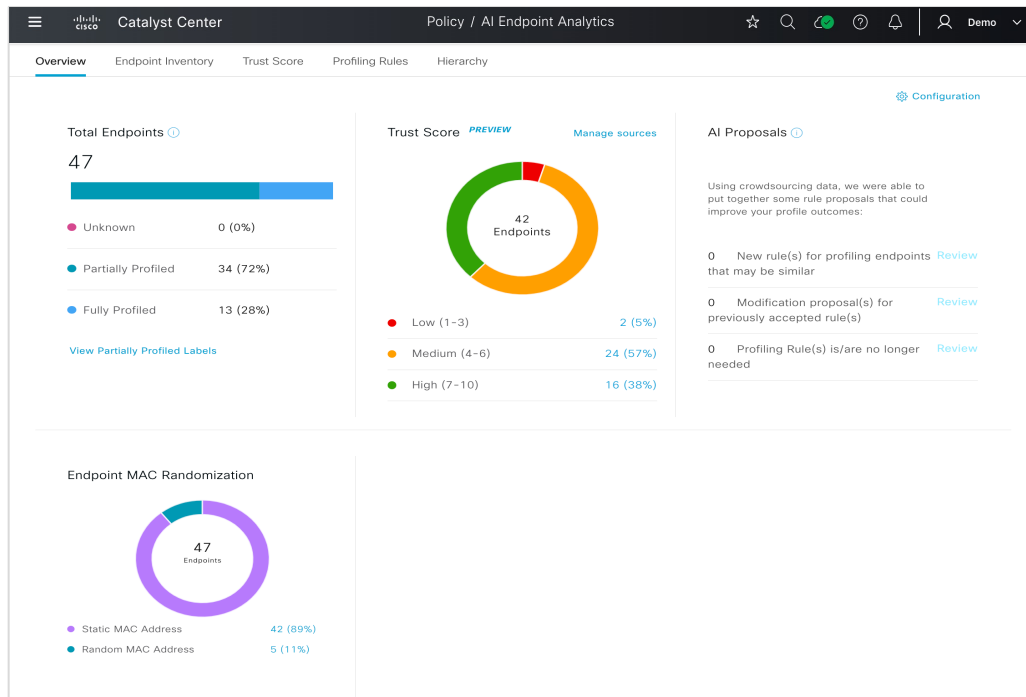
# AI Endpoint and Trust Analytics

- Continuous validation of endpoints for Trusted Access



# AI Endpoint and Trust Analytics

- EA Dashboard



# AI Endpoint and Trust Analytics

- Endpoint Inventory

Catalyst Center

Policy / AI Endpoint Analytics

Demo

Overview

Endpoint Inventory

Trust Score

Profiling Rules

Hierarchy

Endpoint Inventory (47)

Focus: All Endpoints - Default View

Take a Tour

Q

Search

0 Selected

Register Endpoints

More Actions

Export

	MAC Address	Is Random MAC	Trust Score	IP Address	Last Seen	Hostname	Endpoint Type	OS Type	Hardware Model	Hardware Manufactu
	00:50:56:AE:12:5F	No	10	172.16.1.201	Jan 11, 2023 07:04 AM	wx-emp2	Workstation	Windows	VMWare-Device	VMware, Inc.
	D4:3B:04:C7:86:A7	No	6	192.168.1.29	Jan 10, 2023 08:16 PM	-	Workstation	Windows	Intel-Device	Intel Corporation
	00:50:56:AE:73:9E	No	3	172.16.1.202	Jan 10, 2023 08:11 PM	wx-emp1	Workstation	Windows	VMWare-Device	VMware, Inc.
	00:50:56:11:11:11	No	8	172.16.1.200	Jan 13, 2023 06:01 PM	kali	Workstation	Kali Linux	VMWare-Device	VMware, Inc.
	44:61:32:EA:0D:71	No	6	172.16.1.124	Jan 10, 2023 08:14 PM	-	Thermostat	-	ecobee3 lite	ecobee Inc.
	94:6A:B0:54:35:6E	No	6	192.168.1.26	Jan 10, 2023 08:48 PM	-	Smart TV	webOS	43UK6300YVB	LG Corporation
	00:1A:E3:1B:9B:C0	No	6	10.56.97.218	Jan 10, 2023 08:14 PM	-	Printer	-	Lexmark-Printer T522	Lexmark Internation
	5A:00:20:99:77:2F	Yes	9	10.1.10.201	Jun 30, 2022 09:59 PM	-	Mobile Device	iOS 15.6	Apple-Device	Apple, Inc.

# AI Endpoint and Trust Analytics

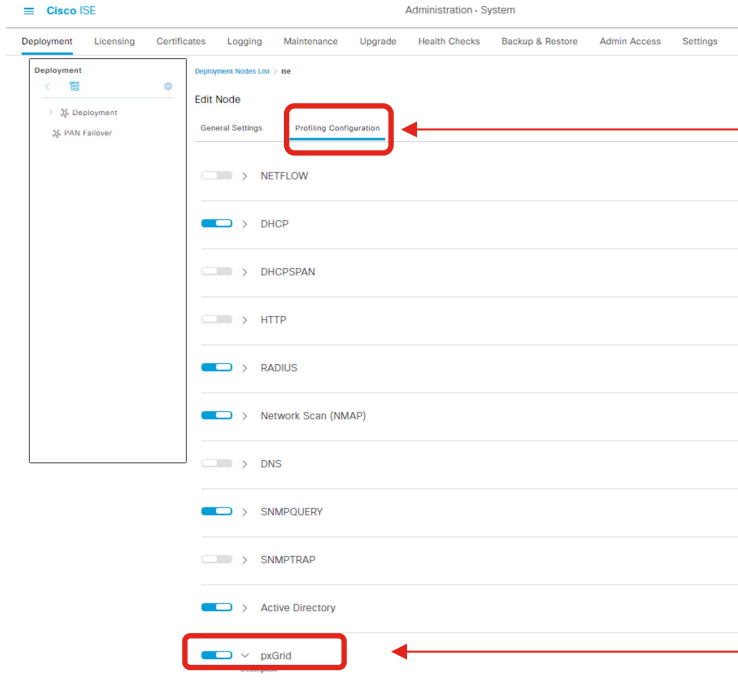
- Trust Scores and Remediation through Adaptive Network Control via ISE

The screenshot displays the 'Policy / AI Endpoint Analytics' interface. At the top, there are tabs for 'Details', 'Trust Score' (selected), and 'Attributes'. Below the tabs, the 'Trust Score Total' is shown as 5. The interface is divided into two main sections: 'Endpoint Authentication and Compliance' and 'Endpoint Anomaly Detection'. Under 'Endpoint Authentication and Compliance', there are two items: 'Authentication Method' and 'Posture', both marked as 'Not Detected'. Under 'Endpoint Anomaly Detection', there are seven items: '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, marked with a red dot), and 'Credential Vulnerability' (Not Detected). At the bottom of the interface, there are two buttons: 'Reset Trust Score' and 'Apply ANC Policy' (highlighted with a red box).

Category	Item	Status	Last Scored
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	Jun 12, 2022 11:56 PM
	Credential Vulnerability	Not Detected	

# AI Endpoint and Trust Analytics Deployment

- On Cisco ISE, ensure pxGrid is enabled for Profiling
  - Access via Administration -> System -> Deployment -> <Edit ISE node> -> Profiling



Profiling Configuration

Enable pxGrid, then Save

# AI Endpoint and Trust Analytics Deployment

- On Cisco ISE, enable attribute sharing and consumption for Endpoint Analytics
  - Access via Work Centers -> Profiler -> Settings

Cisco ISE Work Centers - Profiler

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans

Profiler Settings

Profiling

▼ Profiler Settings

CoA Type\* Reauth ▼

Current custom SNMP community strings \*\*\*\*\* Show

Change custom SNMP community strings ⓘ

Confirm changed custom SNMP community strings: ⓘ

☐ EndPoint Attribute Filter ⓘ

☐ Anomalous Behaviour Detection ⓘ

☐ Anomalous Behaviour Enforcement

☒ Custom Attribute for Profiling Enforcement

☐ Profiling for MUD

☒ Profiler Forwarder Persistence Queue

☐ XSS Security Scan Enforcement for EndPoint Probe Data ⓘ

AI Endpoint Analytics Settings

☒ Publish Endpoint Attributes to AI Endpoint Analytics ⓘ

☒ Consume Endpoint Profiles from AI Endpoint Analytics ⓘ

Enable Custom Attribute for Profiling Enforcement

Enable Publishing and Consumption of endpoint attributes, then Save



# AI Endpoint and Trust Analytics Deployment

- Ensure Cisco ISE has been successfully added to Catalyst Center (see next slide if adding ISE to Catalyst Center for the first time)

The screenshot displays the Cisco Catalyst Center web interface. The top navigation bar includes the Catalyst Center logo and the path 'System / Settings'. The left sidebar contains a search bar and a list of navigation items: 'PnP Device Authorization', 'Device Prompts', 'Configuration Archive', 'External Services' (highlighted with a green box), 'Umbrella', 'Authentication and Policy Servers' (highlighted with a red box), 'Integrity Verification', 'SD-Access Compatibility Matrix', and 'vManage'. The main content area is titled 'Authentication and Policy Servers' and includes a description: 'Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.' Below this, there are links for '+ Add' and 'Export'. A table lists the configured servers:

IP Address	Protocol	Type	Status
10.172.3.100	RADIUS_TACACS	ISE	ACTIVE

# AI Endpoint and Trust Analytics Deployment



- Adding Cisco ISE to Catalyst Center for the first time (1)

**Global RADIUS shared secret to be provisioned to new devices**

**ISE WebUI admin credential (need not match SSH password)**

**FQDN MUST match that on ISE admin settings page**

**Address for any load balancer used in front of ISE clusters**

**pxGrid required for SDA and EA**

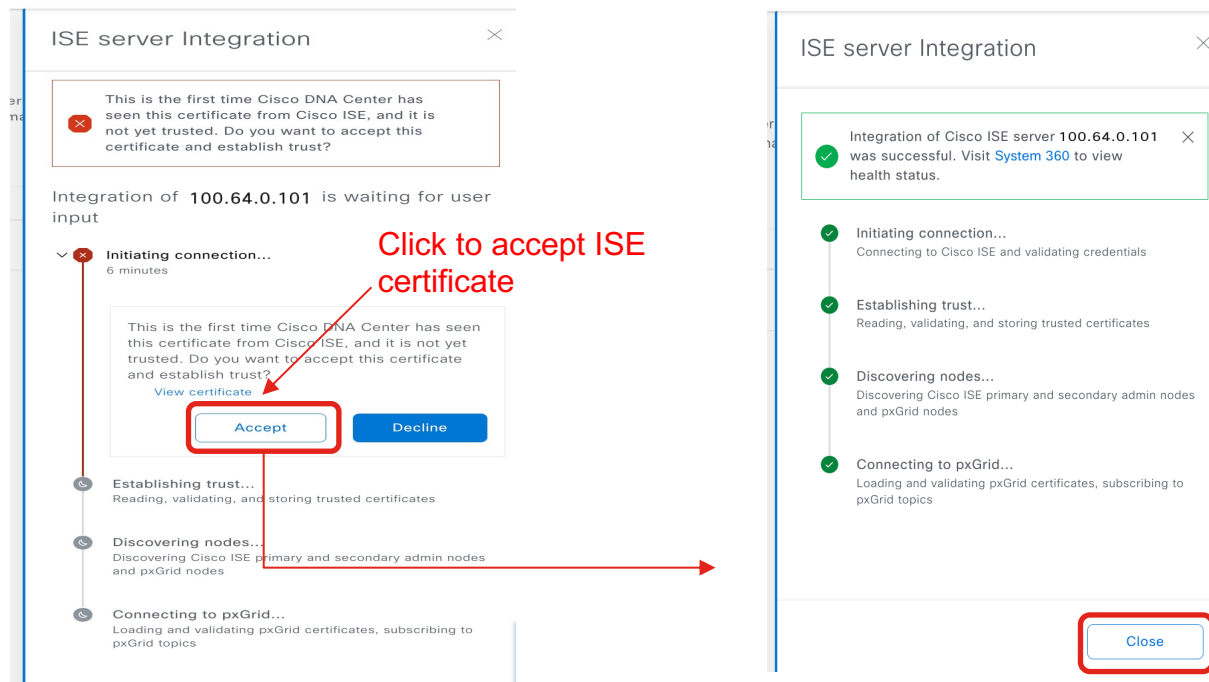
**TACACS not selected by default**

**Only one instance of ISE can be added**

**Add**

# AI Endpoint and Trust Analytics Deployment

- Adding Cisco ISE to Catalyst Center for the first time (2)



# AI Endpoint and Trust Analytics Deployment



- On Cisco ISE, verify that Catalyst Center is SUBSCRIBING to Endpoint Analytics topic
  - Access via Administration -> pxGrid Services -> Diagnostics

Cisco ISE Administration - pxGrid Services

Summary Client Management **Diagnostics** Settings

WebSocket

Clients Topics

Catalyst Center pxGrid connection to ISE

Mouse over to verify the pxGrid topics that Catalyst Center is subscribing to, including those for Endpoint Analytics

Refresh

Client Name	Session Id	Subscriptions	Publications	IP Address	Status
~ise-mnt-ise	ise:0	/topic/com.cisco.ise.sessio...	/topic/com.cisco.ise.sessio...	100.64.0.100	Connected
~ise-fanout-ise	ise:2	/topic/wildcard		127.0.0.1	Connected
~ise-fanout-ise	ise:3	/topic/distributed	/topic/distributed	100.64.0.100	Connected
~ise-admin-ise	ise:4	/topic/com.cisco.ise.pxgrid...	/topic/com.cisco.ise.teleme...	100.64.0.100	Connected
pxgrid_client_1673849553	ise:7	/topic/com.cisco.ise.config...		100.64.0.101	Connected

No Publication attachments from Catalyst Center, yet

# AI Endpoint and Trust Analytics Deployment

- On Catalyst Center, enable **Endpoint Smart Grouping** and **AI Spoofing Detection** under System -> Settings -> Cisco AI Analytics

The screenshot shows the Catalyst Center interface. In the left sidebar, 'External Services' is highlighted in green, and 'Cisco AI Analytics' is highlighted in red. The main content area is titled 'Cisco AI Analytics' and contains the following settings:

- Enable AI Network Analytics**: Checked (indicated by a red box and a red arrow pointing to the text 'Enable AI Network Analytics').
- AI-Enhanced RRM**: Disabled.
- Enable Endpoint Smart Grouping**: Checked (indicated by a red box and a red arrow pointing to the text 'Endpoint Smart Grouping and Tagging').
- AI SPOOFING DETECTION PREVIEW**: This section includes the setting **Enable AI Spoofing Detection**, which is checked (indicated by a red box and a red arrow pointing to the text 'Enable AI Spoofing Detection').

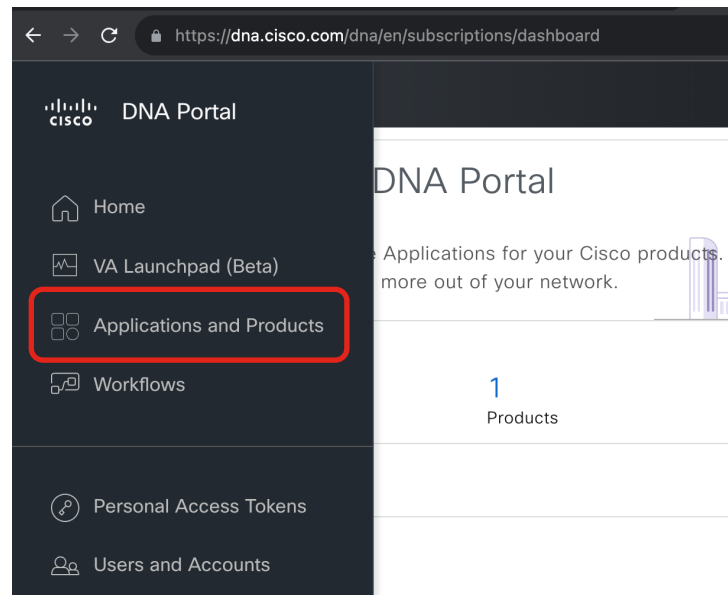
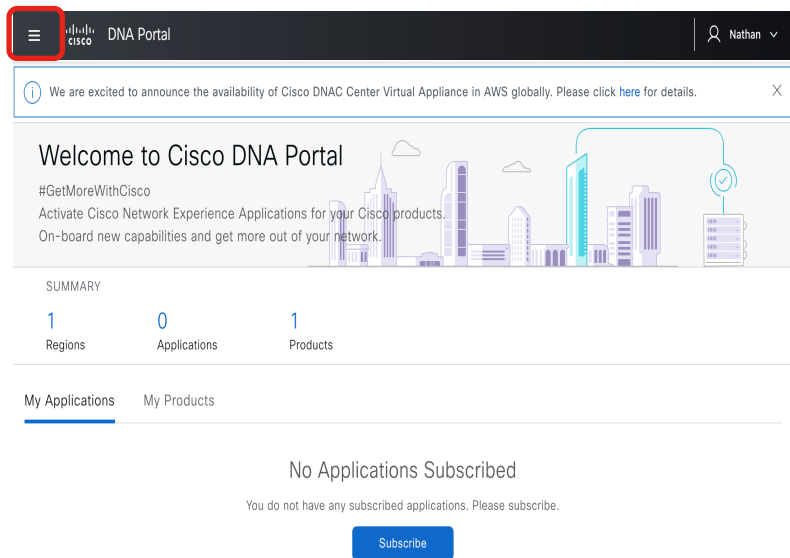
# AI Endpoint and Trust Analytics Deployment

- Talos IP Reputation requires integration with dna.cisco.com (Cisco Cloud Services)

The screenshot shows the Cisco Catalyst Center interface. The top navigation bar includes the Cisco logo, 'Catalyst Center', 'System / Settings', and user information 'Demo'. The left sidebar contains a search bar and a list of settings categories: Device EULA Acceptance, PnP AP Location, Device Prompts, Configuration Archive, External Services (highlighted with a green box), Cisco AI Analytics, Talos IP Reputation (highlighted with a red box), Destinations, and Cisco Spaces/CMX Servers. The main content area is titled 'Settings / External Services' and 'Talos IP Reputation'. It contains a descriptive paragraph about enabling Talos IP Reputation and a toggle switch currently set to 'Disabled' with a yellow warning triangle. A dark grey tooltip box points to the toggle, stating: 'Catalyst Center needs to be registered with Cisco Cloud Services, before Talos IP Reputation integration can be enabled.'

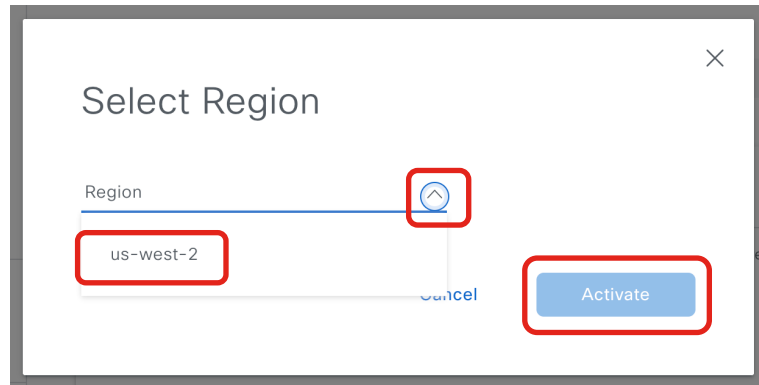
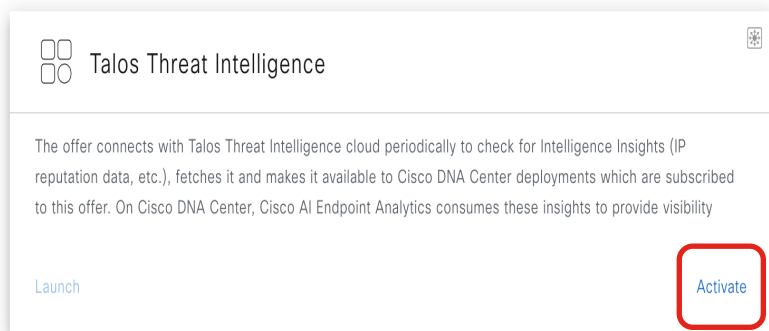
# AI Endpoint and Trust Analytics Deployment

- Log onto [dna.cisco.com](https://dna.cisco.com) with CCO ID to register with cloud apps. **Initial** interaction with [dna.cisco.com](https://dna.cisco.com) should be done from computer with direct access to Catalyst Center (for later steps)



# AI Endpoint and Trust Analytics Deployment

- Select Talos offering and activate in the US-West-2 region \*



\* Talos service with Catalyst Center currently available only in AWS US-West-2 region



# AI Endpoint and Trust Analytics Deployment

- Register your Catalyst Center cluster

Region • us-west-2 ▾

### Choose your Product

You are subscribed to this application. Select the product for which you would like to activate your application. Not seeing the product you want? Click [here](#) to register.

If you wish to manage products that are activated for this application click [here](#).

✓ All Cisco DNA Center

↻ Search by name

Clicking Register will launch browser, connecting to hostname/IP address of Catalyst Center as part of integration

Activate Talos Threat Intelligence application for your Product

Please enter details about your product.  
If you want to choose an existing product click [here](#).

If you are running Cisco DNA Center 2.3.4.x or older, Go to [Product](#) page to register and generate OTP.

Host Name/IP  
100.64.0.101

Product Name\*  
CiscoLive-Demo

Type\*  
Cisco DNA Center ▾

Region  
us-west-2 ▾

Description

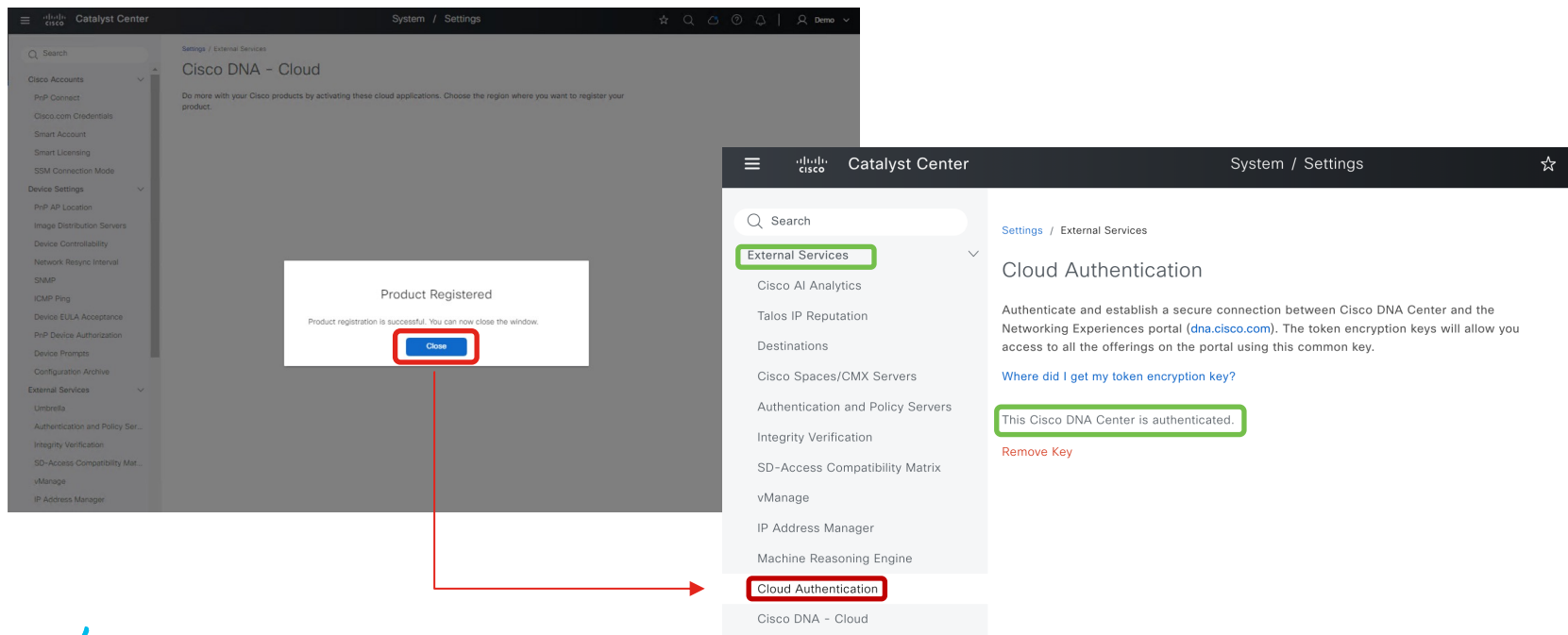
Previous Register

IP address reachable via web browser

Any preferred name

# AI Endpoint and Trust Analytics Deployment

- OTP Key automatically added to Catalyst Center after logging in on newly launched window



# AI Endpoint and Trust Analytics Deployment

- Continue Talos activation workflow on Cisco DNA Portal

Choose your Product


You are subscribed to this application. Select the product for which you would like to activate your application. Not seeing the product you want? Click [here](#) to register.

If you wish to manage products that are activated for this application click [here](#).

All

Cisco DNA Center

1 selected X

 CiscoLive-Demo

Previous

Configure Access Control

Choose the functional capabilities and API Access control to be allowed for application "Talos Threat Intelligence" on this products "CiscoLive-Demo".

CAPABILITIES

There are no messaging capabilities configured for this application.

API ACCESS

☒ Allow All API Group for DNAC

PreviousNext

Summary

Please review all settings that you have entered. Click corresponding Edit for the settings you like to change.

Selected Application [Edit](#)

Name Talos Threat Intelligence

Description The offer connects with Talos Threat Intelligence cloud periodically to check for intelligence insights (IP reputation data, etc.), fetches it and makes it available to Cisco DNA Center deployments which are subscribed to this offer. On Cisco DNA Center, Cisco AI Endpoint Analytics consumes these insights to provide visibility about the endpoints which are communicating to untrusted IP addresses for further user action.

Selected Product [Edit](#)

Region us-west-2

Name CiscoLive-Demo

Description

Selected Scopes [Edit](#)



☒ Allow All API Group for DNAC


PreviousActivate

## SUCCESS!

Done! Your Product is connected to Talos Threat Intelligence

It could take up to 5-10 minutes to activate this application on your products.

 Your Product is connected to Talos Threat Intelligence 



CISCO *Live!*

#CiscoLiveAPJC

BRKEMT-2397

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

121

# AI Endpoint and Trust Analytics Deployment

- If registration error due to “different environment” is encountered, then manually SSH into Catalyst Center to set proper cloud URL (case sensitive)

Register Product

Device CiscoLive-Demo registration failed. OTP was generated by a different environment than the environment configured on this system

Host Name/IP\*  
100.64.0.101

Product Name\*  
CiscoLive-Demo

Type\*  
Cisco DNA Center

Region  
us-west-2

Cancel Register

magctl service setenv registration CLOUD\_URL https://www.ciscoconnectdna.com

```
maglev@maglev-master-192-0-1-1:~$ magctl service setenv registration CLOUD_URL https://www.ciscoconnectdna.com
maglev@maglev-master-192-0-1-1:~$ magctl appstack status -f
```

NAME	NODE	NOMINATED NODE	READINESS GATES	READY	STATUS	RESTARTS	AGE	IP
maglev-system	192.0.1.1	license-service-cleanup-job-fjb72	<none>	0/1	Completed	0	27h	16
maglev-system	192.0.1.1	registration-7db55d6d59-8vdp2	<none>	0/1	Running	0	11s	16
maglev-system	192.0.1.1	release-job-8cc6798c-98e7-49e8-a4f5-079570c0aa2a-packages-j912n	<none>	0/1	Completed	0	26h	16

Wait at least 30s after changing registration URL in order for service to restart, then try registering Catalyst Center again

# AI Endpoint and Trust Analytics Deployment

- If “unexpected error” occurs on Activation Summary screen, verify that the Smart Account associated with CCO ID has active Cisco DNA licenses. Contact TAC for resolution.

The screenshot shows the Cisco DNA Portal interface. At the top, the header includes the Cisco logo, 'DNA Portal', and the text 'Activate application on your product'. A user profile 'Nathan' is visible in the top right. Below the header, there is a dropdown menu for 'Region' set to 'us-west-2'. A red-bordered error box displays the message: 'Unexpected error occurred while activating app for product. Please contact support for further assistance.' Below the error box, the 'Summary' section is visible, with a sub-header 'Selected Application' and an 'Edit' link. The application details include: Name: Talos Threat Intelligence; Description: The offer connects with Talos Threat Intelligence cloud periodically to check for Intelligence Insights (IP reputation data, etc.), fetches it and makes it available to Cisco DNA Center deployments which are subscribed to this offer. On Cisco DNA Center, Cisco AI Endpoint Analytics consumes these insights to provide visibility about the endpoints which are communicating to untrusted IP addresses for further user action. Below this, the 'Selected Product' section is shown with an 'Edit' link. The product details include: Region: us-west-2; Name: CiscoLive-Demo-N62; Description: 100.64.0.101 NAT to 136. At the bottom, the 'Selected Scopes' section is visible with an 'Edit' link and a checkbox labeled 'Allow All API Group for DNAC' which is checked. At the very bottom, there are 'Exit', 'Previous', and 'Activate' buttons.

Summary

Please review all settings that you have entered. Click corresponding Edit for the settings you like to change.

Selected Application [Edit](#)

Name: Talos Threat Intelligence

Description: The offer connects with Talos Threat Intelligence cloud periodically to check for Intelligence Insights (IP reputation data, etc.), fetches it and makes it available to Cisco DNA Center deployments which are subscribed to this offer. On Cisco DNA Center, Cisco AI Endpoint Analytics consumes these insights to provide visibility about the endpoints which are communicating to untrusted IP addresses for further user action.

Selected Product [Edit](#)

Region: us-west-2

Name: CiscoLive-Demo-N62

Description: 100.64.0.101 NAT to 136

Selected Scopes [Edit](#)

☒ Allow All API Group for DNAC

[Exit](#) [Previous](#) [Activate](#)

# AI Endpoint and Trust Analytics Deployment

- Successful registration confirmation to Cisco DNA Portal (**may take more than 5 minutes after registration to show activation**)

The screenshot shows the Cisco DNA Portal interface. The top navigation bar includes the Cisco logo, 'DNA Portal', and 'Applications and Products / App 360'. The user 'Nathan' is logged in. The main content area is titled 'Talos Threat Intelligence'. Below this, it shows 'Status: Connected' and 'Account: nathanle@cisco.com'. A 'SUMMARY' section indicates '1 Activated'. The 'Products' tab is selected, showing 'Activations (1)'. A table lists the activation:

Name	Type	Region	Status	Actions
Cisco DNA-Demo	Cisco DNA Center	us-west-2	Activated	

Cisco DNA Portal

The screenshot shows the Catalyst Center 'System / Settings' page. The left sidebar lists various services, with 'Cisco DNA - Cloud' selected. The main content area is titled 'Cisco DNA - Cloud' and shows 'Do more with your Cisco products by activating these cloud applications.' It indicates 'This Cisco DNA Center is registered with us-west-2 region.' and has a 'Select Region' dropdown set to 'us-west-2'. Below this, the 'Applications (4)' section displays a table of active and pending applications:

Name	Tenant Subscription Status	Category	Offers	Vendor	Actions
Talos Threat Intelligence	Connected	**	talos	Cisco	...
Cisco User Defined Network	To Be Connected	UPN	upn	Cisco	...
Plug and Play as a Service	To Be Connected	**	pnp	Cisco	...
AppX MS-Teams	To Be Connected	Data Analysis	avc	Cisco	...

Catalyst Center  
System Settings

# AI Endpoint and Trust Analytics Deployment

- Talos IP Reputation can now be enabled

The screenshot shows the Cisco Catalyst Center interface. The top navigation bar includes the Cisco logo, 'Catalyst Center', and 'System / Settings'. The left sidebar contains a search bar and a list of settings categories: Device Prompts, Configuration Archive, External Services (highlighted with a green box), Cisco AI Analytics, Talos IP Reputation (highlighted with a red box), Destinations, Cisco Spaces/CMX Servers, Authentication and Policy Servers, and Integrity Verification. The main content area is titled 'Settings / External Services' and 'Talos IP Reputation'. It contains a description of the feature and a toggle switch. The toggle switch is currently in the 'Disabled' position (greyed out). A red box highlights the toggle switch, and a red arrow points from a text box below to the toggle. The text box says: 'Enabling in-progress. Enabling can take upto 60 seconds.'

Settings / External Services

## Talos IP Reputation

Enabling Cisco Talos IP Reputation connects Catalyst Center to Talos, detecting when endpoints attempt to access IPs with an untrusted reputation. Talos Intelligence Group manages the world's most comprehensive real-time threat detection network. Enabling process for Cisco Talos IP Reputation can take up to 60 seconds.

☐ Disabled

Enabling in-progress. Enabling can take upto 60 seconds.

May take more than 60 seconds AFTER enabling Talos IP Reputation for block lists to be downloaded onto Catalyst Center

# AI Endpoint and Trust Analytics Deployment

- Talos IP Reputation ready for service

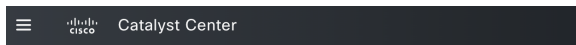
The screenshot shows the Cisco Catalyst Center interface. The top navigation bar includes the Cisco logo, the text 'Catalyst Center', and 'System / Settings'. A search bar is on the left. The left sidebar lists various settings categories: Device Prompts, Configuration Archive, External Services (expanded), Cisco AI Analytics, Talos IP Reputation (selected), Destinations, Cisco Spaces/CMX Servers, Authentication and Policy Servers, Integrity Verification, SD-Access Compatibility Matrix, vManage, IP Address Manager, Machine Reasoning Engine, Cloud Authentication, and Cisco DNA - Cloud. The main content area is titled 'Settings / External Services' and 'Talos IP Reputation'. It contains a description of the service and a toggle switch labeled 'Enabled'. Below this is a section titled 'Talos Intelligence Update' containing a table with the following data:

File Name	Last Received Version
IPv4 Block List	1699263129
IPv6 Block List	1699263168
Talos Threat Level	1626977550



# AI Endpoint and Trust Analytics Deployment

- Enable AI Endpoint Analytics through Policy -> AI Endpoints Analytics



## Set up prerequisites and configurations

Cisco AI Endpoint Analytics is an endpoint visibility solution that helps you identify and profile endpoints and Internet of Things (IoT) devices. It profiles the endpoints using the telemetry information received from the network from various sources, such as Deep Packet Inspection (DPI) data, Cisco ISE, self-registration portals and configuration management database (CMDB) software such as ServiceNow. It uses a Trust Score concept that allow you to identify and act upon potentially risky endpoints and identify the risk factor using single value, which can be used for deciding enforcement action using ISE. [Manage Configurations](#).

AI Endpoint Analytics works for endpoints coming to Catalyst Center from:

Cisco Catalyst 9000 series access devices.

Cisco Traffic Telemetry Appliance running IOS-XE 17.3.1 or later.

Additional endpoint information can optionally be retrieved from Catalyst Center integrated ISE, running one of:

Cisco ISE 2.4.0.357 Patch 11+ or

Cisco ISE 2.6.0.156 Patch 4+ or

Cisco ISE 2.7.0.356 Patch 1+ or

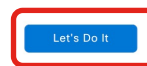
Cisco ISE 3.0 onwards



[Endpoint Analytics Deployment Guide](#)

## Set up prerequisites and configurations

Complete the following recommended prerequisites to get started with AI Endpoint Analytics. You can always review and manage your configurations anytime later from the Manage Configurations page.



☒ Don't show this to me again



# AI Endpoint and Trust Analytics Deployment

- Verify all prerequisites are met for EA to function properly



## Endpoint Analytics prerequisites (Day 0 configuration)

Complete the following recommended prerequisites to get started with AI Endpoint Analytics. You can always review and manage your configurations anytime later from the [Manage Configurations](#) page.

### ✓ DPI Enablement (CBAR) (3 of 3 items are completed)

Enable Deep Packet Inspection (DPI) on your Catalyst 9000 series access devices which provides deep insights into endpoint traffic and help profiling the endpoint accurately. DPI is enabled on Catalyst access devices using CBAR (Controller Based Application Recognition) enablement flow in the Catalyst Center. To improve endpoint profiling, it is recommended you enable CBAR at the Catalyst Center level and on all Catalyst 9000 series access devices.

Enable CBAR on the Catalyst Center

Status ✓ Enabled

Enable CBAR on Catalyst switches

Status ✓ Enabled

To add or modify cbar to switches, visit Network Devices Enablement under [Application Visibility Setup](#)

We have detected that from **4** devices in the Cisco DNA inventory, CBAR is enabled on **2** devices and CBAR is warning state in **0** devices error state in **1** devices

Enable System Rule Updates

Enable System Rule updates in AI Endpoint Analytics by configuring CBAR cloud. This will help keeping your profiling rules up-to-date to get better profiling results. You can use the Profile Rule Settings configuration to change your update schedule if needed.

Status ✓ Enabled

### > ✓ ISE Configuration (2 of 2 items are completed)

### > ✓ AI Analytics Integration (1 of 1 items are completed)

### ✓ ISE Configuration (2 of 2 items are completed)

We detected that you have Cisco ISE 3.2.0.542 integrated with this Catalyst Center. We recommend integrating it with AI Endpoint Analytics to enable endpoint probe data retrieval from ISE for increased visibility and publishing of AI Endpoint Analytics actionable insights to ISE for use in authorization policies to secure your network.

Endpoint attributes forwarding from Cisco ISE

Enable endpoint attribute forwarding from Cisco ISE to AI Endpoint Analytics for increased visibility using Cisco ISE probes.



Endpoint profile publishing to Cisco ISE

Allows publishing AI Endpoint Analytics actionable insights to Cisco ISE for authorizing endpoint access to network and for endpoint control.



### ✓ AI Analytics Integration (1 of 1 items are completed)

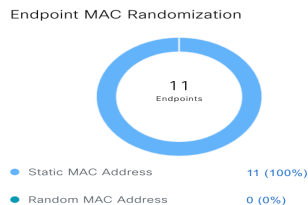
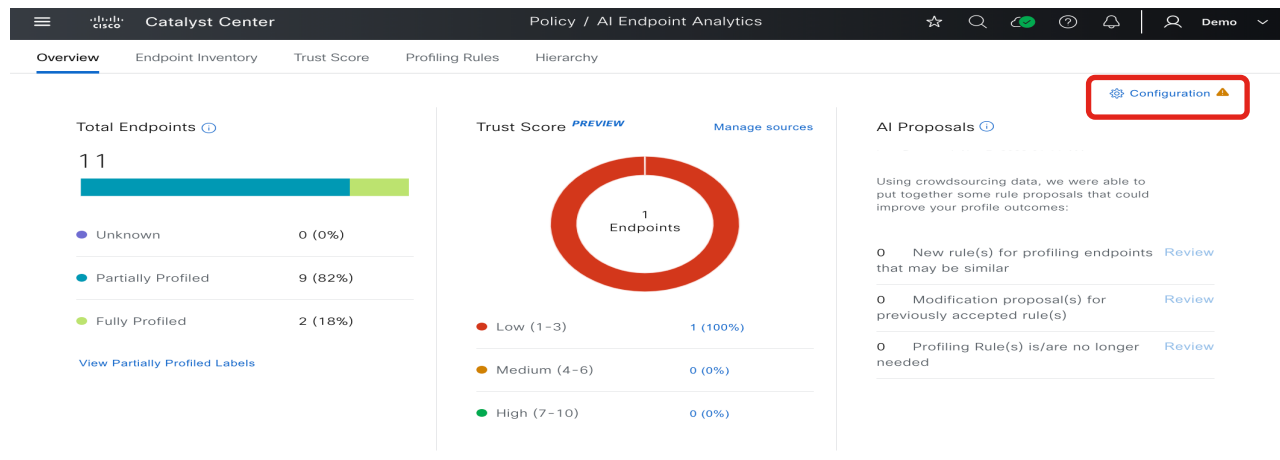
Endpoint smart grouping

Using AI and machine learning, Endpoint Smart Grouping reduces the number of unknown endpoints in the network by providing AI-based endpoint groupings, automated custom profiling rules, and crowdsourced endpoint labels.



# AI Endpoint and Trust Analytics Deployment

- AI Endpoint Analytics functional state



# AI Endpoint and Trust Analytics Deployment

- Endpoint Analytics functional state

**Manage Configurations**

Profile Rule Settings  
ISE Configuration  
Trust Analytics  
Endpoint Purge Policy  
Endpoint Subnet Inspection

## Manage Configurations

This page provides an overview and status of Catalyst Center level configurations to be done to get complete value out of AI Endpoint Analytics. For other AI Endpoint Analytics configurations, please use appropriate settings in left hand side menu. Click on each configuration name to know more and follow the steps for enablement.

[Refresh](#)

### Required Configurations (3)

This is list of recommended configurations to get started using AI Endpoint Analytics, providing increased visibility for endpoint profiling and enabling manual/automated policy enforcement with Cisco ISE.

Status: [All](#) [Enabled](#) [Disabled](#)

Configuration Name	Status	Details
<a href="#">DPI Enablement (CBAR)</a>	Enabled	3 of 3 items are completed
<a href="#">ISE Configuration</a>	Enabled	2 of 2 items are completed
<a href="#">AI Analytics Integration</a>	Enabled	1 of 1 items are completed

### Optional Configurations (4)

Following is the list of optional configurations for specific use-cases which can be enabled based on your requirements.

Status: [All](#) [Enabled](#) [Disabled](#)

Configuration Name	Status	Details
<a href="#">Security Sensor</a>	Disabled	0 of 3 items are completed
<a href="#">ServiceNow</a>	Disabled	0 of 1 items are completed
<a href="#">Talos IP Reputation</a>	Enabled	5 of 5 items are completed
<a href="#">AI Spoofing detection</a>	Enabled	3 of 3 items are completed

# AI Endpoint and Trust Analytics Deployment

- On Cisco ISE, verify that Catalyst Center is publishing to Endpoint Analytics topic
  - Access via Administration -> pxGrid Services -> Diagnostics

The screenshot shows the Cisco ISE Administration interface for pxGrid Services. The 'Diagnostics' tab is selected, and the 'WebSocket' section is active. Under 'Clients', a table lists various connections. A red arrow points to the 'ise-admin-ise' client, which is highlighted with a green box. Another red arrow points to the 'Publications' column for this client, which is also highlighted with a green box. A third red arrow points to the list of topics published by this client, which is highlighted with a green box. The topics include '/topic/com.cisco.endpoint.analytics.data' and '/topic/com.cisco.ea.data'.

Mouse over to verify Catalyst Center is publishing to com.cisco.ea.data topic

Catalyst Center pxGrid connection to ISE

Client Name	Session Id	Subscriptions	Publications	IP Address	Status
~ise-mnt-ise	ise:0	/topic/com.cisco.ise.sessio...	/topic/com.cisco.ise.sessio...	100.64.0.100	Connected
~ise-fanout-ise	ise:2	/topic/wildcard		127.0.0.1	Connected
~ise-fanout-ise	ise:3	/topic/distributed	/topic/distributed	100.64.0.100	Connected
~ise-admin-ise	ise:4	/topic/com.cisco.ise.pxgrid...	/topic/com.cisco.ise.teleme...	100.64.0.100	Connected
pxgrid_client_1673849553	ise:7	/topic/com.cisco.ise.config...	/topic/com.cisco.endpoint...	100.64.0.101	Connected

Topics published by pxgrid\_client\_1673849553:

- /topic/com.cisco.endpoint.analytics.data
- /topic/com.cisco.ea.data
- /topic/com.cisco.local
- /topic/com.cisco.endpoint.asset

# Take Aways

1. Efficient means of navigating and operating Catalyst Center
2. Leverage application gems to gain powerful utilization and insights of your network
3. Check Release Notes/User Guides
4. Search [ciscolive.com](https://ciscolive.com)
5. Join Cisco Community

CISCO *Live!*

# Did you know?

You can have a  
one-on-one session with  
a technical expert!

Visit Meet the Expert in The HUB  
to meet, greet, whiteboard & gain  
insights about your unique questions  
with the best of the best.



## Meet the Expert Opening Hours:

<b>Tuesday</b>	<b>3:00pm – 7:00pm</b>
<b>Wednesday</b>	<b>11:15am – 7:00pm</b>
<b>Thursday</b>	<b>9:30am – 4:00pm</b>
<b>Friday</b>	<b>10:30am – 1:30pm</b>

# Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt





# Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](https://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC