cisco Live!

Let's go

The bridge to possible

The Hidden Gems of Catalyst Center

Nathan Lee, Technical Solutions Architect
@networkaugur

BRKEMT-2397

Cisco Webex App

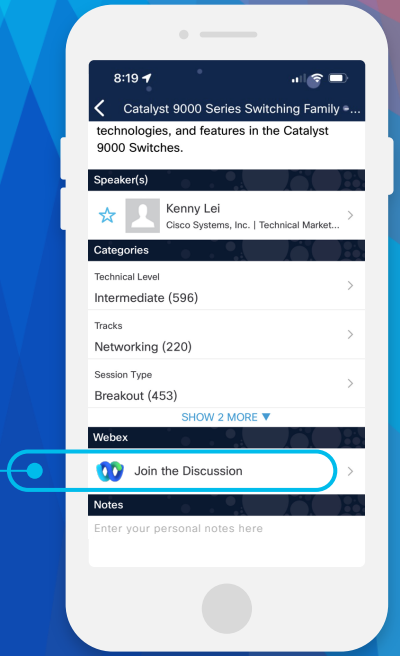
Questions?

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

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

Agenda

- Introduction
- Installation
- Settings
- Navigation
- Applications

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

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

Blackholes exist?
en.wikipedia.org/wiki/Thorne-Hawking-Preskill_bet

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

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

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

Installation

Installation

- Cluster link
- DNS reachability
- SSL proxy

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

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

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

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

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

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)

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

Settings

Settings

- Visibility and Control of Configurations
- SNMP polling

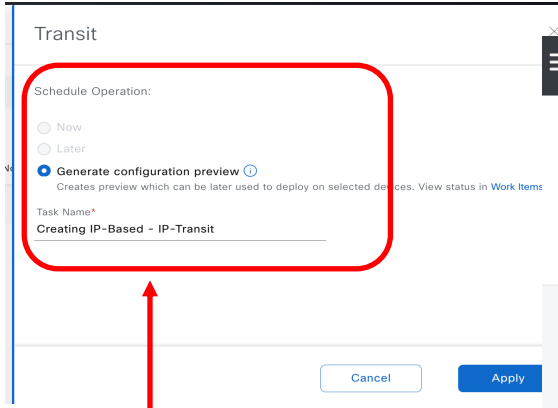
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Settings – Visibility and Control of Configurations

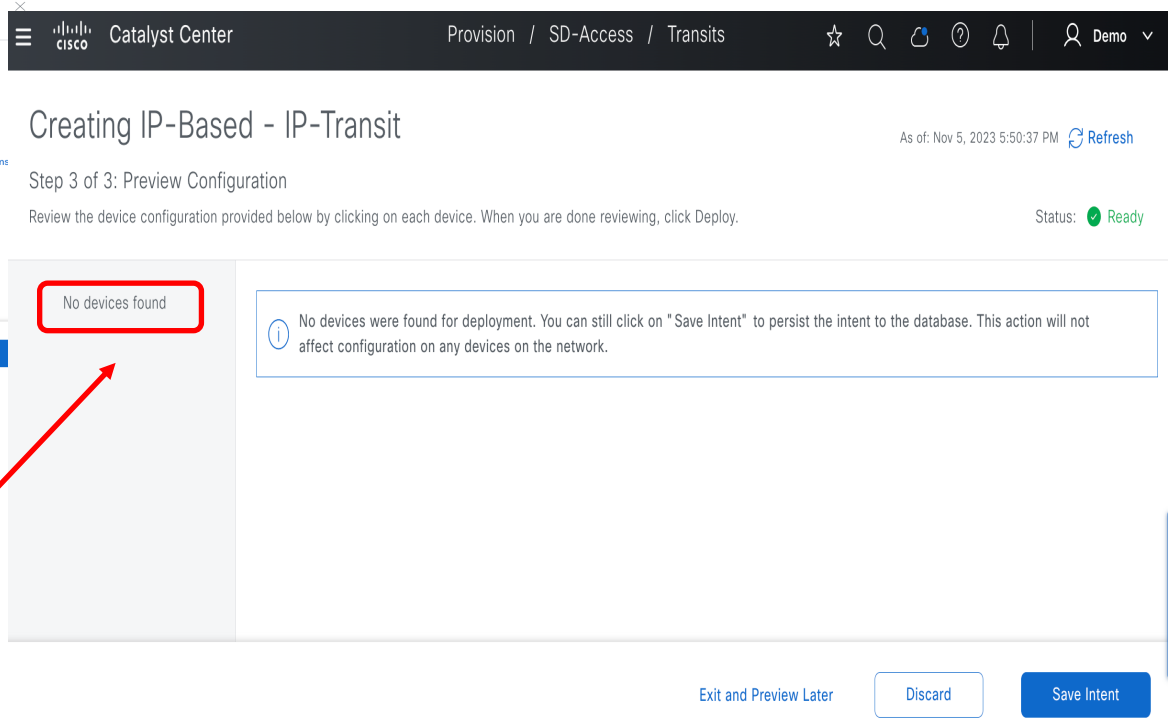
- Initially known as VCR (Visibility, Control and Rollback)
- Enabled by default with Catalyst Center 2.3.7.0+
- When VCR is enabled, nearly all workflows MUST have configuration preview
  - Even workflows with no changes
- Suitable when ITSM and change management are company policy
- What if you don't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

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

Settings - Visibility and Control of Configurations



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



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

Settings - Visibility and Control of Configurations

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

As of: Oct 27, 2023 12:39:47 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

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

Search all configurations

Configuration to be Deployed
161 Line(s)

```
!SysloglistConfigs
logging host 100.64.0.101 transport udp port 514
logging source-interface Loopback0
logging trap 6
!done
!SysloglistConfigs
!done
snmp-server enable traps
snmp-server host 100.64.0.101 traps version 2c ****** udp-port 162
snmp-server source-interface traps Loopback0
ip http client source-interface Loopback0
ip ssh source-interface Loopback0
ip ssh version 2
ip domain lookup
crypto pki trustpoint DNAC-CA
source interface Loopback0
enrollment mode ra
enrollment terminal
usage ssl-client
revocation-check crl none
exit
crypto pki authenticate DNAC-CA
-----BEGIN CERTIFICATE-----
MIIDpTCCAo2gAwIBAgIURSGhBo[illegible]B+eZBFg4zL6m96XAa3owDQYJKoZIhvcNAQEL
BQAwYjEtMCsGA1UEAwwkYjY2[illegible]2UxMjMtOTg4OSlmODI4LTZiZmYtNWNkMTI0YWE5
NzUyMRYwFAYDVQQKDAlDa[illegible]jbyBTeXNOZWlzMRkwFwYDVQQLDBBDaXNjbyBETkEg
Q2VudGVyMB4XDTIzMT[illegible]sIAlMDIwMVoXDTI2MDcyMzAlMDIwMVowYjEtMCsGA1UE
AwwkYjY2Y2UxMjMt[illegible]g4OSlmODI4LTZiZmYtNWNkMTI0YWE5NzUyMRYwFAYDVQQK
DAlDaXNjbyBT[illegible]NOZWlzMRkwFwYDVQQLDBBDaXNjbyBETkEgQ2VudGVyMIIBIjAN
BgkqhkiG9w[illegible]AQEFAAOCAQ8AMIIBCgKCAQEAuFL3YtDTQPUZ6Gcx2ZMxrrCiskXe
BF/4KU6[illegible]HoiMOFB+lxse85uBBaksKHSubZGlEKJqaD1Tx+vxlAveOc3PqC+v+l
```

Running Configuration
401 Line(s)

```
Building configuration...

Current configuration : 10780 bytes
!
! Last configuration change at 18:53:58 UTC Fri Oct 27 2023 by netadmin
!
version 17.13
service timestamps debug datetime msec
service timestamps log datetime msec
platform punt-keepalive disable-kernel-core
!
hostname Border-C9300
!
!
vrf definition Mgmt-vrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
logging buffered 20000000
no logging console
no aaa new-model
switch 1 provision c9300-48u
!
!
!
!
ip routing
```

Generation Status Legend

Exit and Preview Later | Discard | Deploy

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

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

Settings - Visibility and Control of Configurations

Catalyst Center | System / Settings | admin

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 configuratior 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 — Enabled by default

ITSM Approval

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

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

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

Settings - SNMP Polling

Catalyst Center | System / Data Platform / COLLECTOR-SNMP | admin

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			

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

Settings - SNMP Polling

Template default

SNMP Configuration

Configuration for SNMP collector

Configuration

List of metrics to be enabled*

- [x] CPU
- [x] Memory
- [x] Interface
- [x] Environment Temperature
- [x] Device Availability
- [ ] QOS
- [ ] RTTMON
- [ ] LISP
- [ ] CLISP
- [x] 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

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*

- [x] CPU
- [x] Memory
- [x] Interface
- [x] Environment Temperature
- [x] Device Availability
- [ ] QOS
- [ ] RTTMON
- [ ] LISP
- [ ] CLISP
- [x] Ethernet Info

Polling Interval

5.00

5 100

Collector Information

Satellite ID

satellite0

Site ID

site0

Configuration Name*

SNMPoll5min

Keep the name unique for this configuration

Keep the name unique for this configuration

Save Configuration

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

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		
SNMPoll5min	default	one	1 Applied	0 Failed	0 Pending

1 Record(s) Show Records: 25 1 - 1 1

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

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
```


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

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
```


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

Navigation

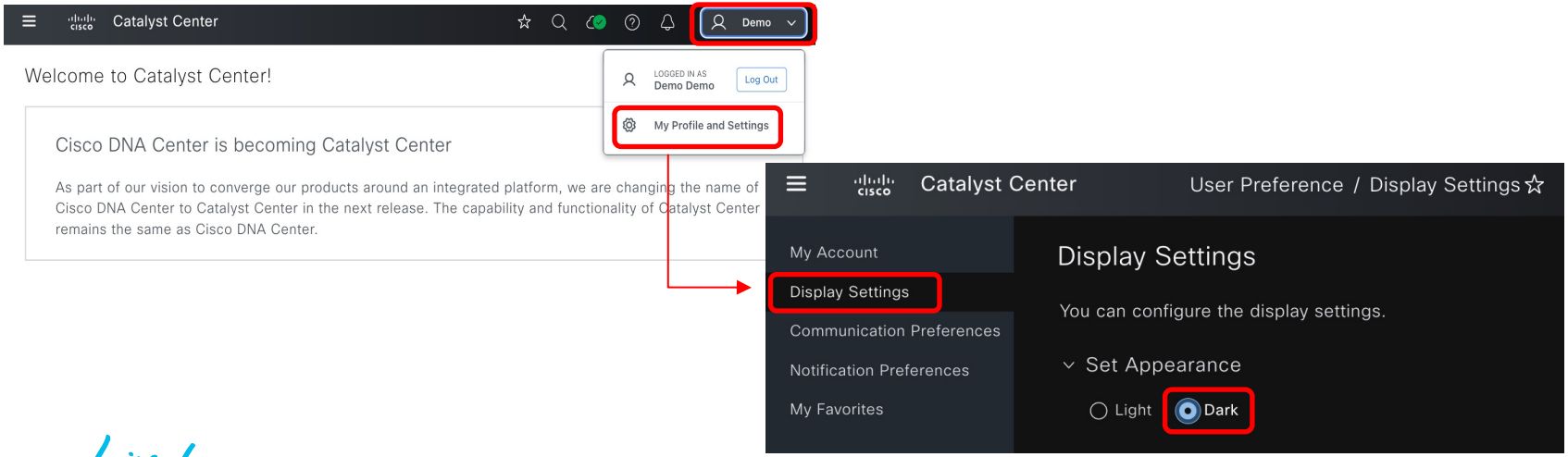
Navigation

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

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

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



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

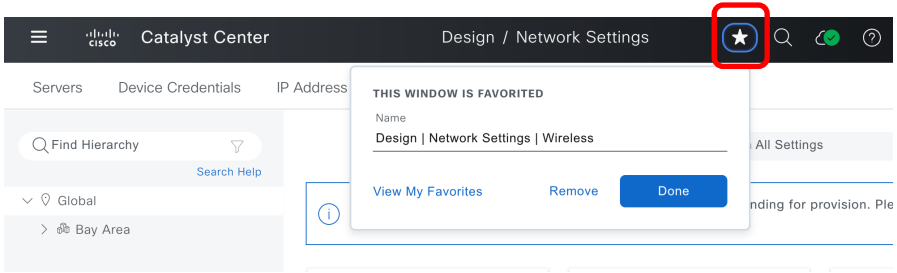
Navigation – Keyboard Shortcuts

- 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)

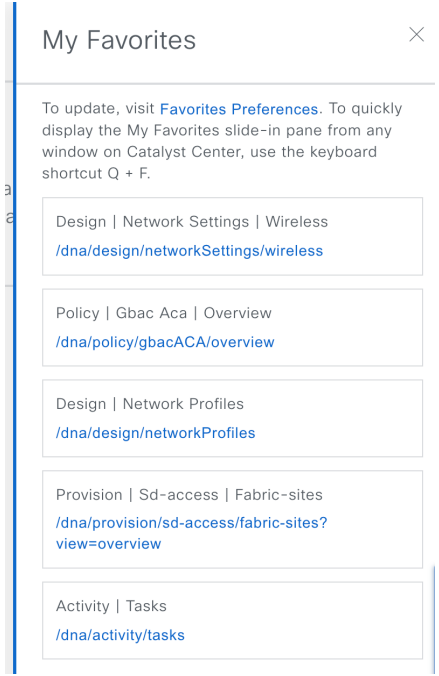
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

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



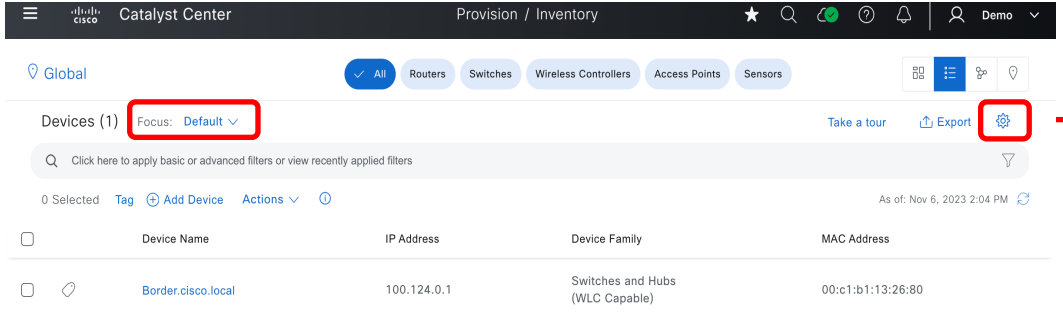
Q+F

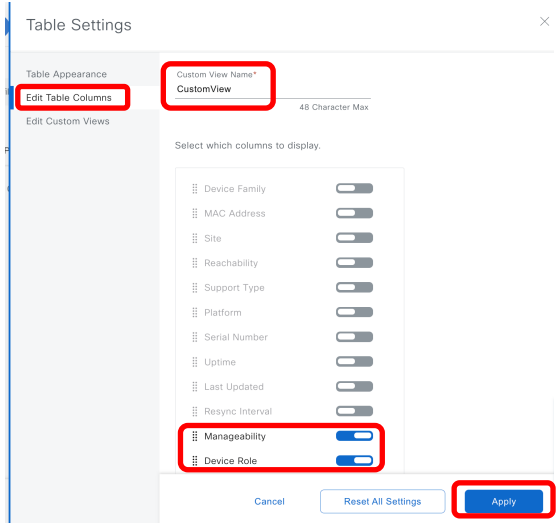


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Navigation – Inventory Focus Customization

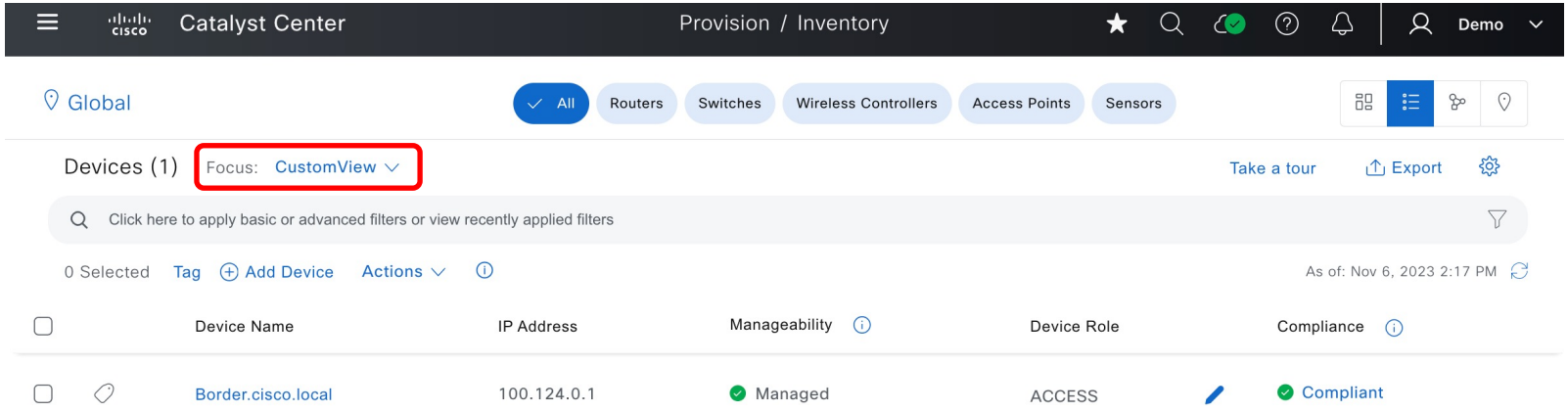
- Each Focus on Inventory page parlay different device status
- Customize Focus to show common or critical status
- Focus customization persists through browser cookie only, not on any Catalyst Center system settings -> customized view lost if browser cookie deleted or if different browser used





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

Navigation – Inventory Focus Customization



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

Navigation Demo

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

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

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

Navigation – SWIM

Catalyst Center | Image Repository / Summa | 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

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

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

Navigation – SWIM

Image Repository

Imported Images

Images (1)

Show Tasks | Cisco.com ID | nathanle (Not me?)

Filter Imported Images

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

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

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.

1

Cisco Device Series | All Device Series

4 Selected | 5 Select Site | Select a device type · Switches and Hubs 2

4

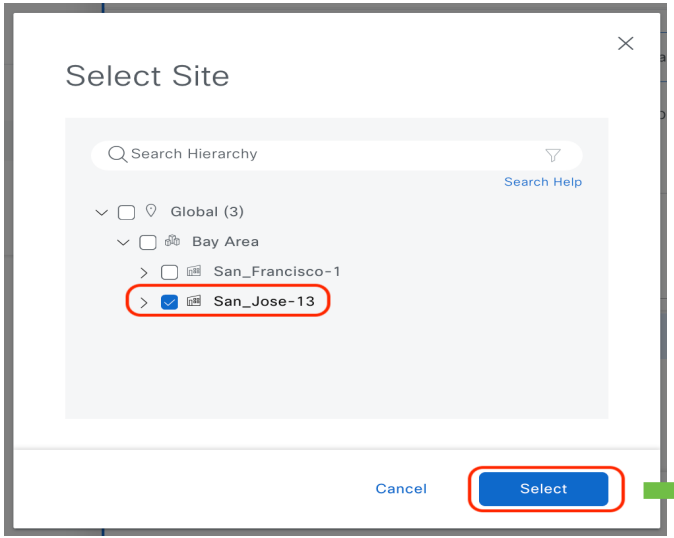
Device Series | Sites

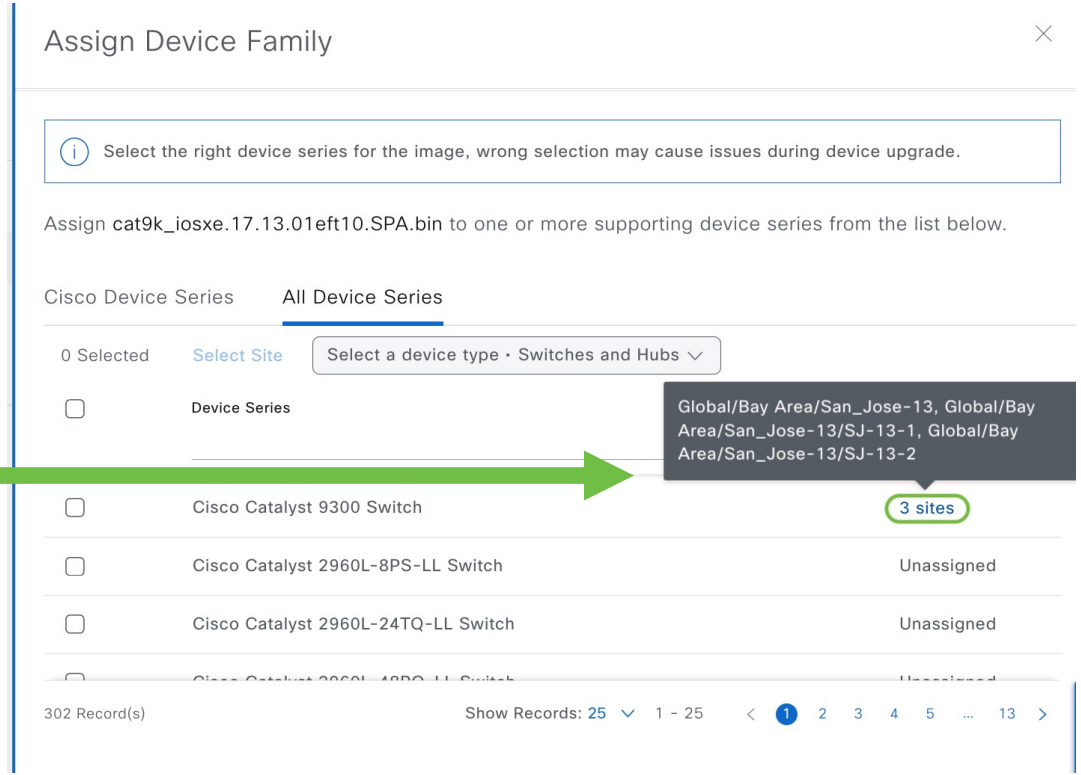
3

Cisco Catalyst 9300 Switch

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

Navigation – SWIM





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

Navigation – SWIM

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			TOTAL IMAGES			ADVISORIES
0	0	0	0	1	0	Not Available
Device Families	Devices	Device Families Without Golden Image	Running	Imported	Golden	

mage Families

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

r Image Families

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

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

No platform for which to specify Golden Image!

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

Navigation – SWIM

Global

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

SUMMARY

0	0	0
Device Families	Devices	Device Families Without Golden Image

TOTAL IMAGES

0	1	0
Running	Imported	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 2:38 PM

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

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

Navigation – SWIM

San_Jose-13

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

SUMMARY			TOTAL IMAGES			ADVISORIES	
0	0	0	1	1	0	0	0
Device Families	Devices	Device Families Without Golden Image	Running	Imported	Golden	Critical On Running Images	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

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

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

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

Image Name	Version	Devices	Image Status	Advisories: Critical	Advisories: 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

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

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

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

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

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

PnP Demo

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

Applications

Applications

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

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

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}”

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

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	
Border.cisco.local	.../Bay Area/San_Jose-13	100.124.0.1	FCW2125L104	17.12.1	Cisco Catalyst 9300 Serie...	Not Ready See Details
Cat3650-Old.cisco.local	.../Bay Area/San_Jose-13	100.124.127.36	FDO1946X034	16.12.10a	Cisco Catalyst 3650 Serie...	Not Ready See Details
Edge-L.cisco.local	.../San_Jose-13/SJ-13-1	100.124.126.129	FCW2333G0QW	17.12.2	Cisco Catalyst 9300 Serie...	Not Ready See Details
Edge-R.cisco.local	.../San_Jose-13/SJ-13-1	100.124.126.134	FCW2125L10A	17.12.2	Cisco Catalyst 9300 Serie...	Not Ready See Details

4 Record(s) Show Records: 25 1 - 4

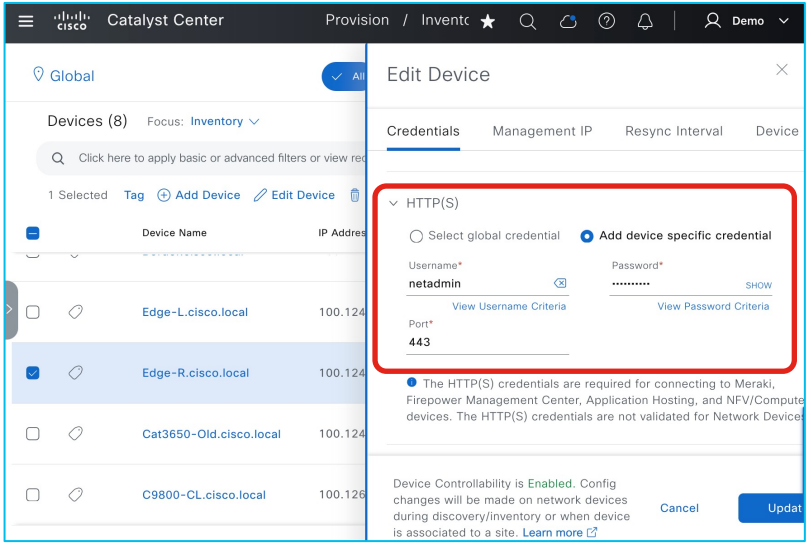
Why is "100.124.126.134" marked "Not Ready"?

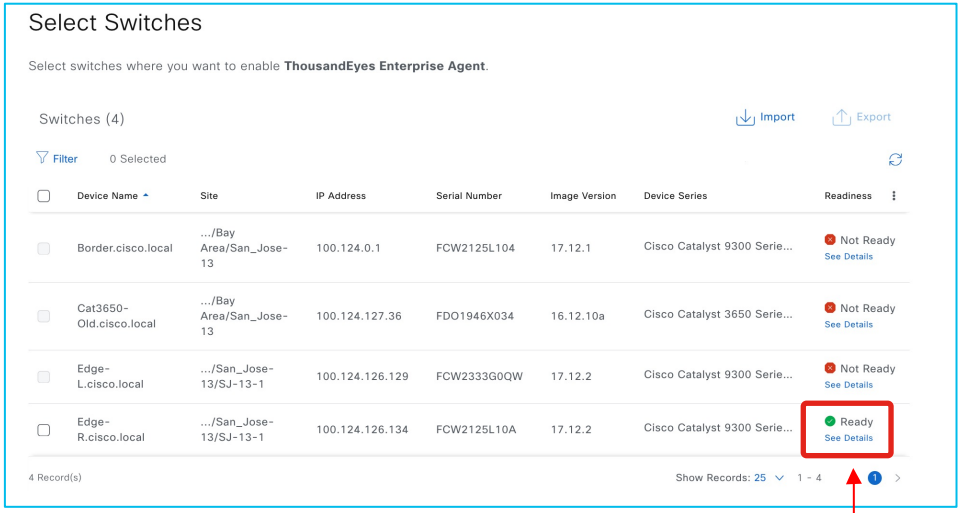
Readiness Check	Result	Message
Are HTTPS Credentials Provided in the Inventory	Failed	HTTP(s) Username is missing in the Inventory. Provide HTTP(s) Username in the Inventory and try again. The HTTPS credentials are required to connect to App Hosting. Provide the HTTPS credentials in Device Inventory.
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.

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

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#
```





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

Application Telemetry?

Application Visibility?

Application Experience?

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

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)

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

Application Telemetry Deployment

Catalyst Center | Design / Network Settings | Demo

Servers | Device Credentials | IP Address Pools | Wireless | Telemetry | Security and Trust

Find Hierarchy
Search Help
- Global
  - Bay Area
    - San_Francisco-1
    - San_Jose-13
      - SJ-13-1
      - SJ-13-2

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

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

- [x] Use Cisco DNA Center as SNMP trap server
- [ ] Add an external SNMP trap server

Syslogs

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

- [x] Use Cisco DNA Center as syslog server
- [ ] Add an external syslog server

Application Visibility

Enable Netflow Application Telemetry and Controller Based Application Recognition (CBAR) by default upon network device site assignment

- [x] 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

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

Application Telemetry Deployment

Catalyst Center | Design / Network Settings | Demo

Servers | Device Credentials | IP Address Pools | Wireless | Telemetry | Security and Trust

Find Hierarchy
Search Help
- Global
  - Bay Area
    - San_Francisco-1
    - San_Jose-13
      - SJ-13-1
      - SJ-13-2

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

v 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

v 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

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

Application Telemetry Deployment

Catalyst Center | Design / Network Settings | Demo

Servers | Device Credentials | IP Address Pools | Wireless | Telemetry | Security and Trust

Find Hierarchy
Search Help
Global
Bay Area

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.

- 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

Wireless Controller, Access Point and Wireless Clients Health

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

- [x] Enable Wireless Telemetry

Reset | Save

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

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

Application Telemetry from Access Switches

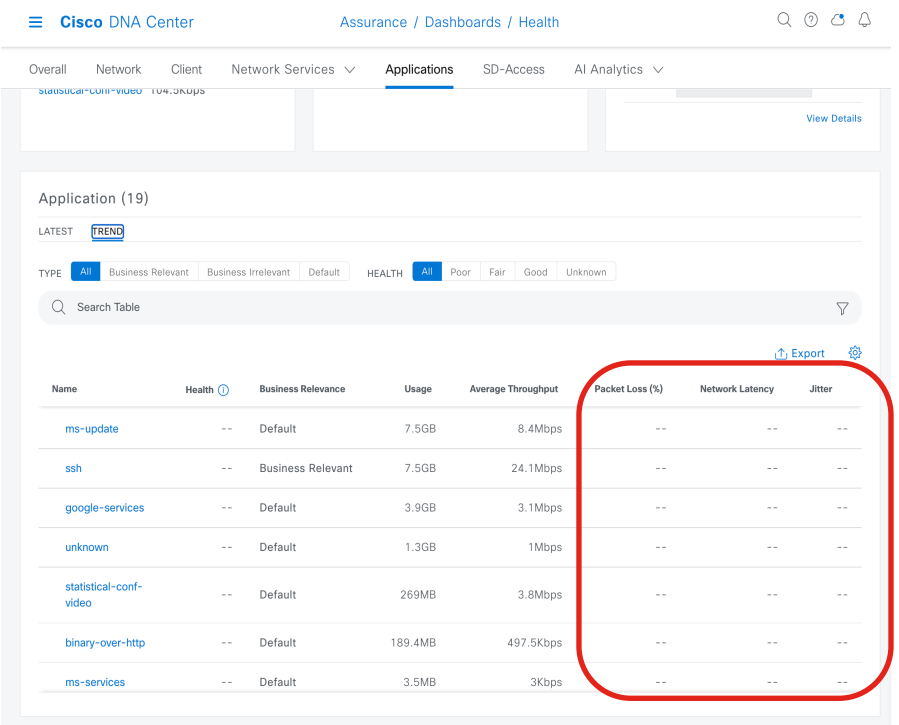
Overview

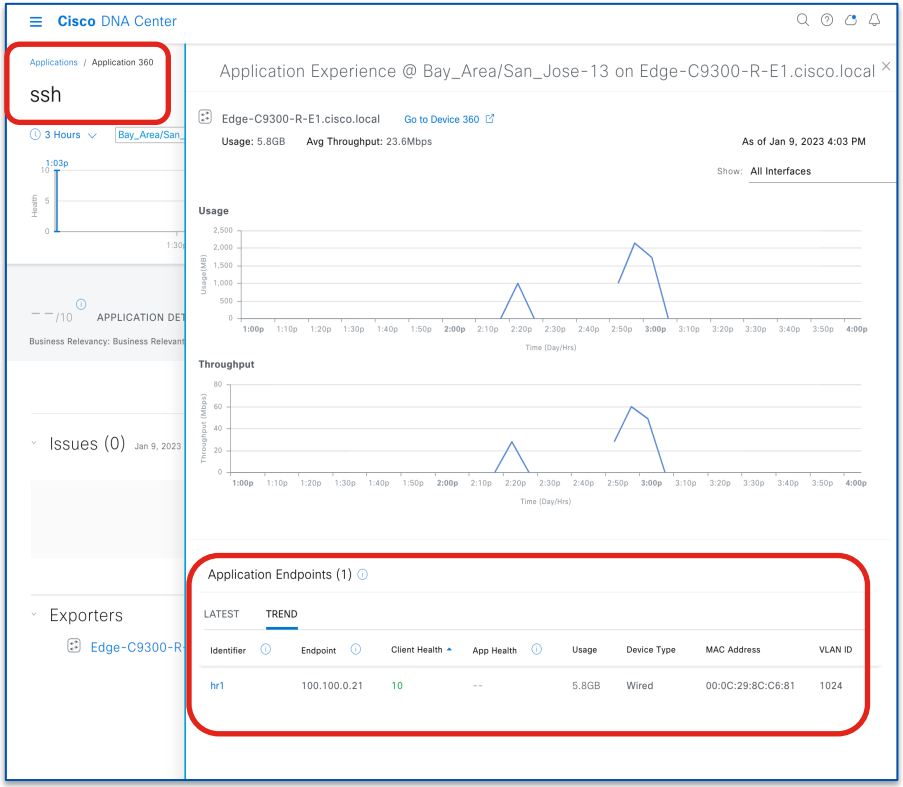
- Flexible NetFlow config to match applications orchestrated from Catalyst Center
- Supported for Software Defined Access (SDA) fabric or non-fabric
- Switches must be activated with DNA-Advantage licenses
- Quantitative visibility only – no performance metric (loss, jitter, latency)
- Application customization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

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

Application Telemetry from Switches

- Switch-based Application Visibility does not include performance metrics





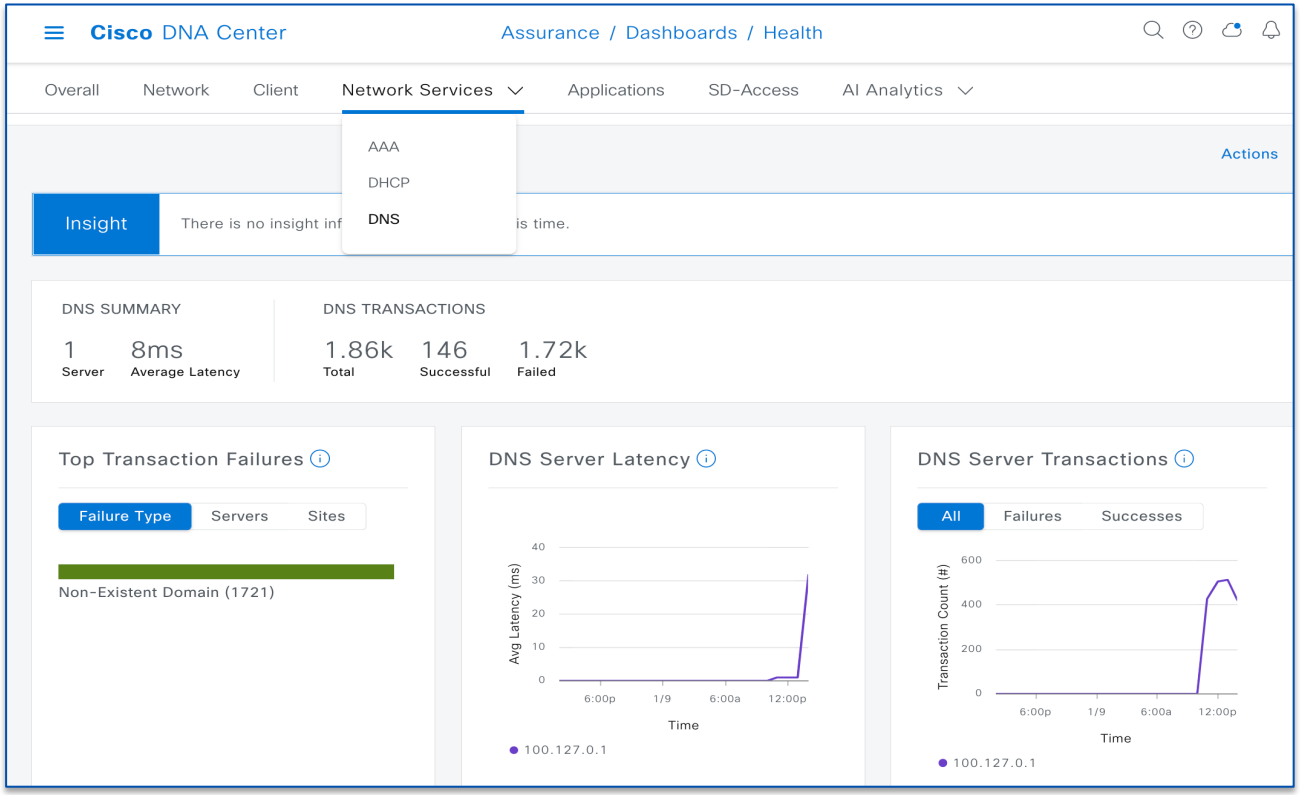
- Client level Application usage visibility

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

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



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

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

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

Switch Application Telemetry Deployment

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

Click on Pencil icon to change role

Catalyst Center | Provision / Inventory | Demo

Global | All | Routers | Switches | Wireless Controllers | Access Points | Sensors

Devices (3) 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

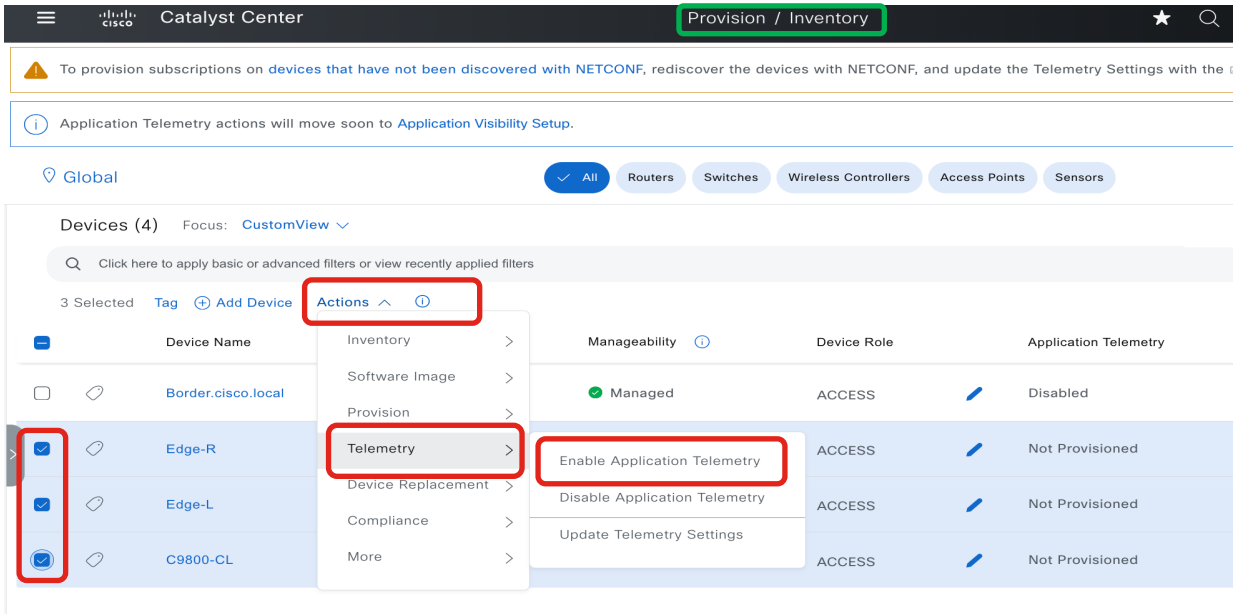
Device Name	IP Address	Manageability	Device Role	Application Telemetry	Compliance
Border.cisco.local	100.124.0.1	Managed	ACCESS	Enabled	Non-Compliant
Edge-R	100.124.126.129	Managed	ACCESS	Not Provisioned	Non-Compliant
Edge-L	100.124.126.134	Managed	ACCESS	Not Provisioned	Compliant

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

Switch Application Telemetry Deployment

Catalyst Center 2.3.5.x and below

- Initiate Application Telemetry via **Provision -> Inventory**



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

Switch Application Telemetry Deployment

For Your Reference

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

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


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

Switch Application Telemetry Deployment

For Your Reference

- 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
```


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

Switch Application Telemetry Deployment

For Your Reference

- 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”

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

Switch Application Telemetry Deployment

For Your Reference

- 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
```


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

Switch Application Telemetry Deployment

For Your Reference

- 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

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

Switch Application Telemetry Deployment

For Your Reference

- 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
```


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

Application Visibility from Access Switches

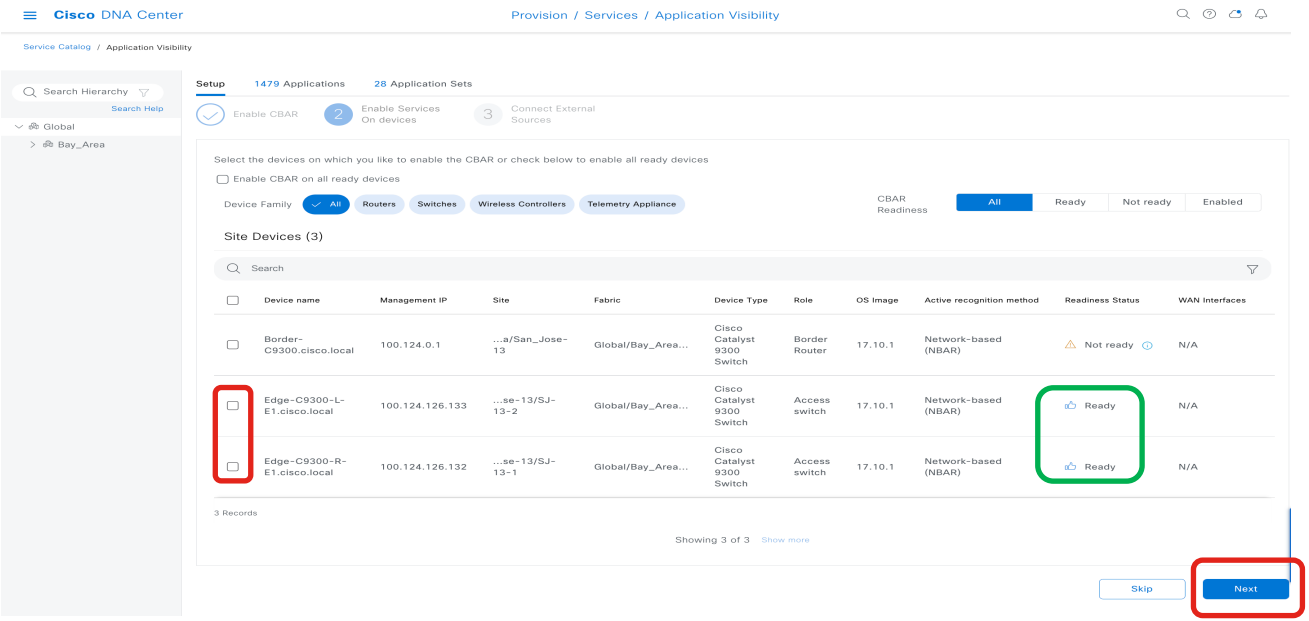
- NBAR (Network-Based Application Recognition)
  - Application classification capability local to each device
- CBAR (Controller-Based Application Recognition)
  - Catalyst Center capability to share and dynamically update NBAR application signatures between network devices
- NBAR classifies >1400 apps 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

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

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”



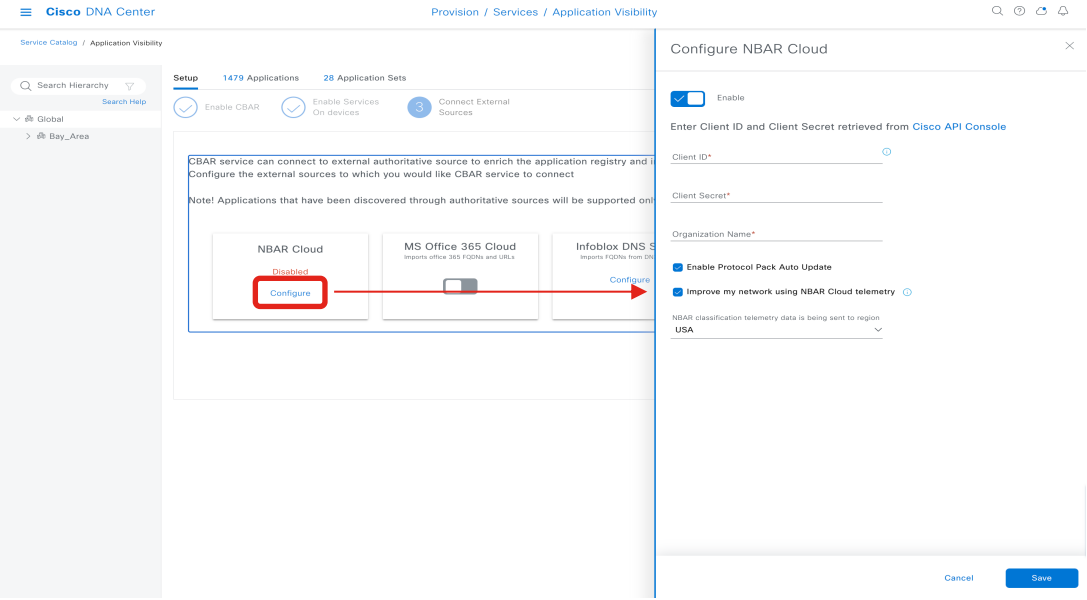
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Switch Application Visibility Deployment

Catalyst Center 2.3.5.x and below

For Your Reference

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



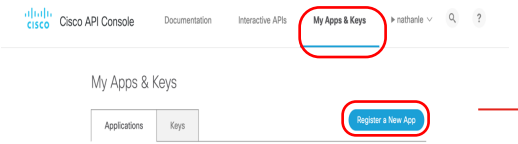
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

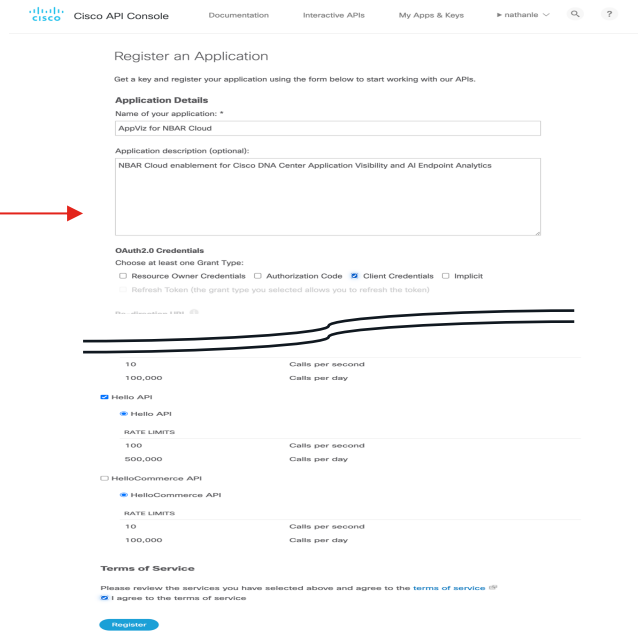
Switch Application Visibility Deployment

For Your Reference

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





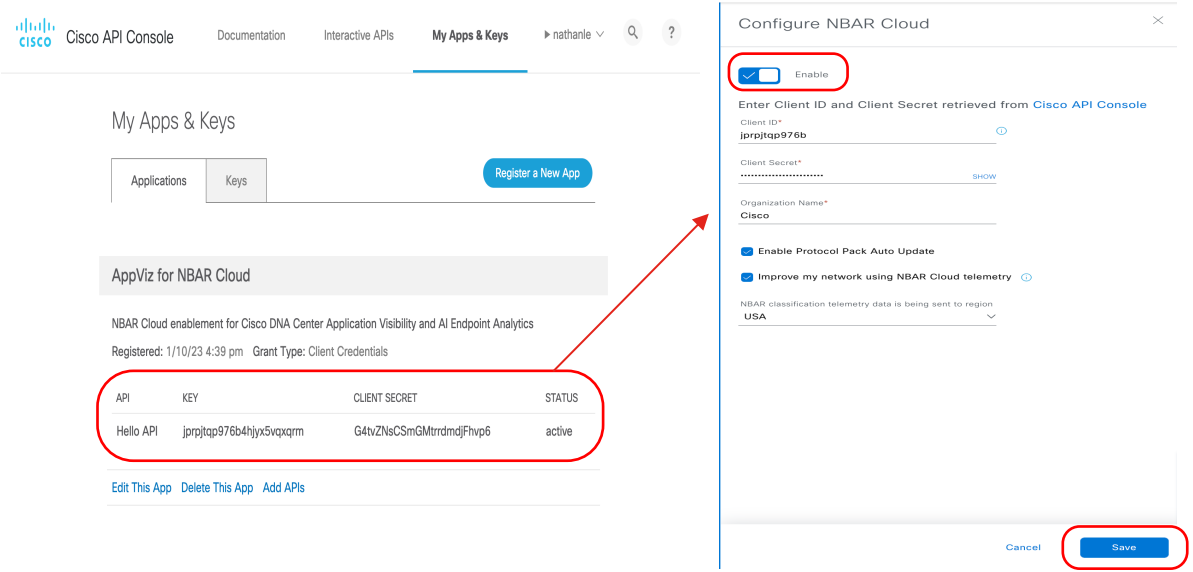
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Switch Application Visibility Deployment

For Your Reference

Catalyst Center 2.3.5.x and below

- Input obtained credential to enable NBAR Cloud



API Console Portal

Cisco DNA Center

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

Switch Application Visibility Deployment

- NBAR/CBAR configuration pushed to Switches

```
platform wdavc 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

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

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

  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
```

IOS-XE native protocol pack

CBAR installed protocol pack

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

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
```

Moments later

```
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
```


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

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
```


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

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

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

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**

Catalyst Center | Services / Service Catalog / Application Visibility Setup | Demo

Service Catalog / Application Visibility Setup

Search Hierarchy
Search Help
Global
Bay Area

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

Enable Application Telemetry
Disable Application Telemetry

Device name		cognition method	CBAR Deployment Status	Application Telemetry Deployment Status
Border.cisco.local		-based (NBAR)	Not deployed	Not deployed
C9800-CL.cisco.local	100.126.0.6	Network-based (NBAR)	Not deployed	Not deployed
Edge-L	100.124.126.134	Network-based (NBAR)	Not deployed	Not deployed
Edge-R	100.124.126.129	Network-based (NBAR)	Not deployed	Not deployed

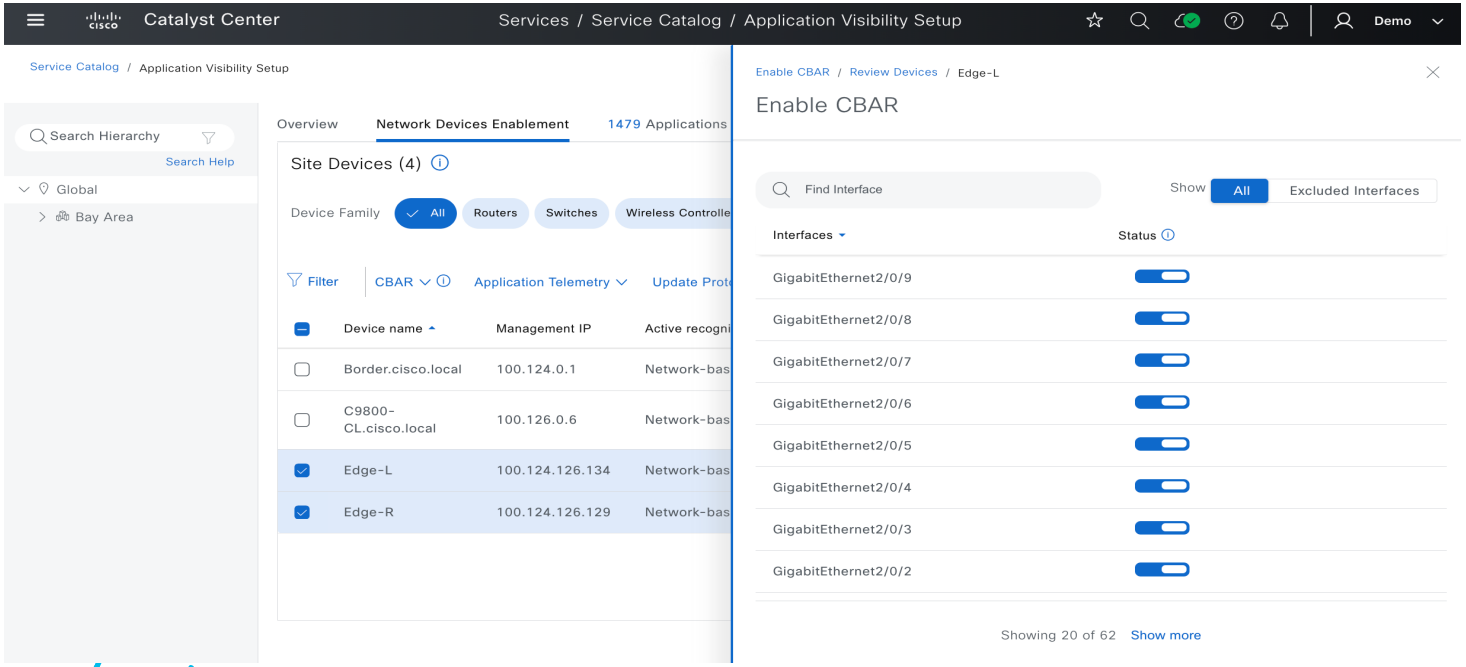
Showing 4 of 4 Show more

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

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)

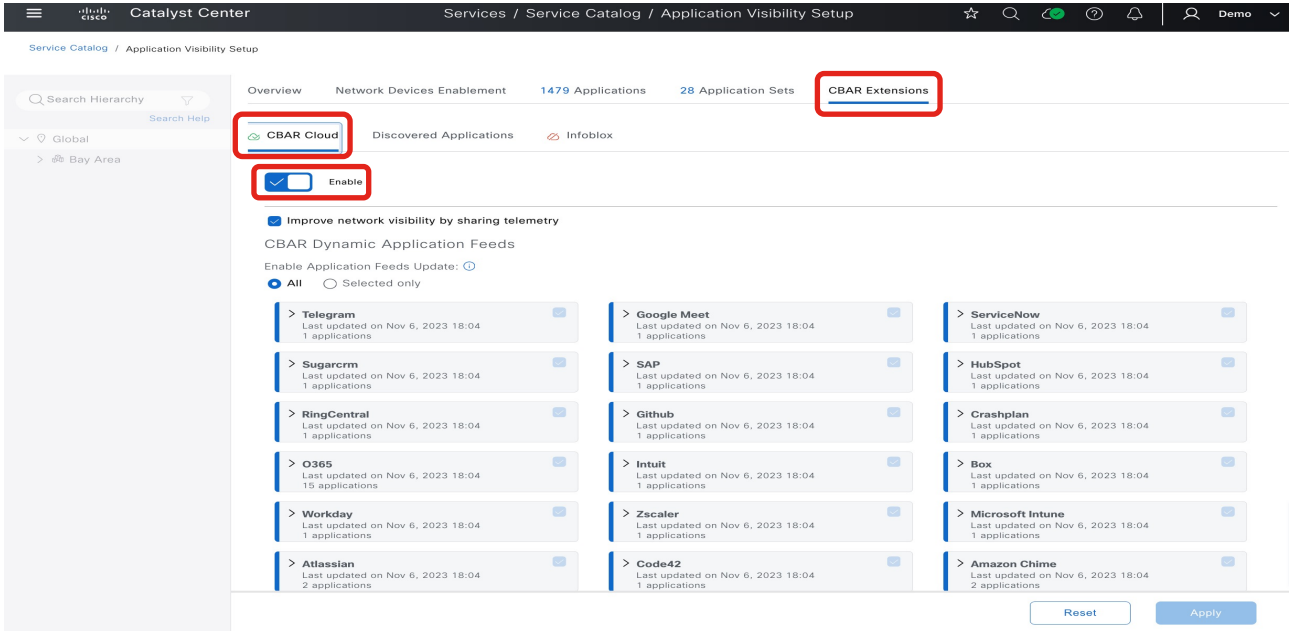


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Applications – Application Telemetry and CBAR

Catalyst Center 2.3.7.x and above

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



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

Applications – Application Telemetry and CBAR

Catalyst Center 2.3.7.x and above

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

Catalyst Center | Services / Service Catalog / Application Visibility Setup | Demo

Service Catalog / Application Visibility Setup

Search Hierarchy
Search Help
Global
Bay Area

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

CBAR Health Issues and Remedies — Last Updated: 12:34 am — Refresh

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

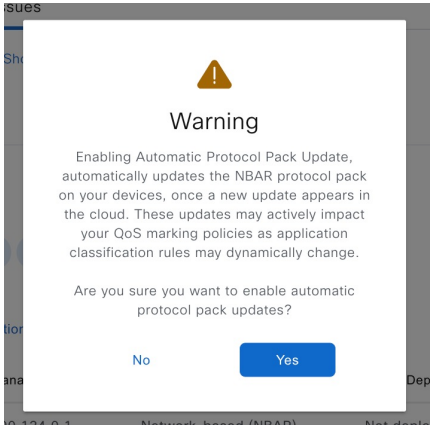
Telemetry Readiness: All | Ready | Not ready | Enabled

Filter | CBAR | Application Telemetry | Update Protocol Pack

Update All Devices
Update Selected Devices
Update Selected Devices From File
Auto Update
Include Selected Devices
Exclude Selected Devices

Device name	Management IP		Deployment Status	Application Telemetry Deployment Status
Border.cisco.local	100.124.0.1		eployed	Not deployed
C9800-CL.cisco.local	100.126.0.6		eployed	Completed
Edge-L	100.124.126.134		leted onfigure	Completed
Edge-R	100.124.126.129	CBAR	Completed Re-Configure	Completed

Showing 4 of 4 Show more



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

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

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

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

Catalyst Center | Provision / Services / Application Visibility | Demo

Service Catalog / Application Visibility

Search Hierarchy
Search Help
Global
Bay Area

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

Device Protocol Pack outdated Show devices

Site Devices (6)

Device Family: All | Routers | Switches | Wireless Controllers | Telemetry Appliance

CBAR Readiness: All | Ready | Not ready | Enabled

Active Recognition Method: All | CBAR | NBAR | IP/Port | Not Supported

Telemetry Readiness: All | Ready | Not ready | Enabled

Filter | CBAR | Application Telemetry | Update Protocol Pack

- Enable CBAR on selected devices
- Disable CBAR on selected devices
- Enable CBAR on all ready devices
- Disable CBAR on all devices

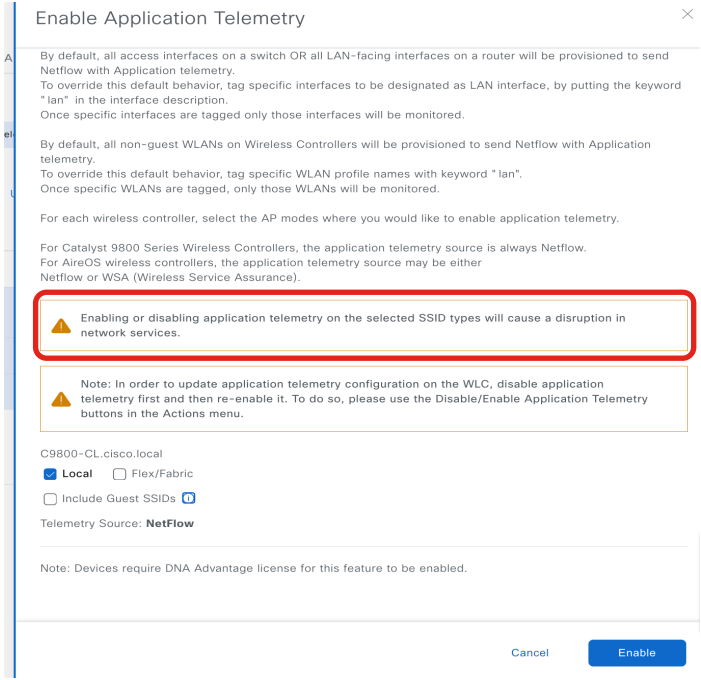
Dev	IP	Active recognition method	CBAR Deployment Status	Application Telemetry Deployment Status
Bor	2	Network-based (NBAR)	Not deployed	Not deployed
Bor	1	Network-based (NBAR)	Not deployed	Not deployed
C9800-CL.cisco.local	100.126.0.6	Network-based (NBAR)	Not deployed	Not deployed
Cat3650-Old.cisco.local	100.124.127.36	IP/Port	Not deployed	Not deployed

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

Application Telemetry and Visibility Deployment for Wireless

Catalyst Center 2.3.7.x and above

- **SSID will flap when Application Telemetry is enabled/disabled**

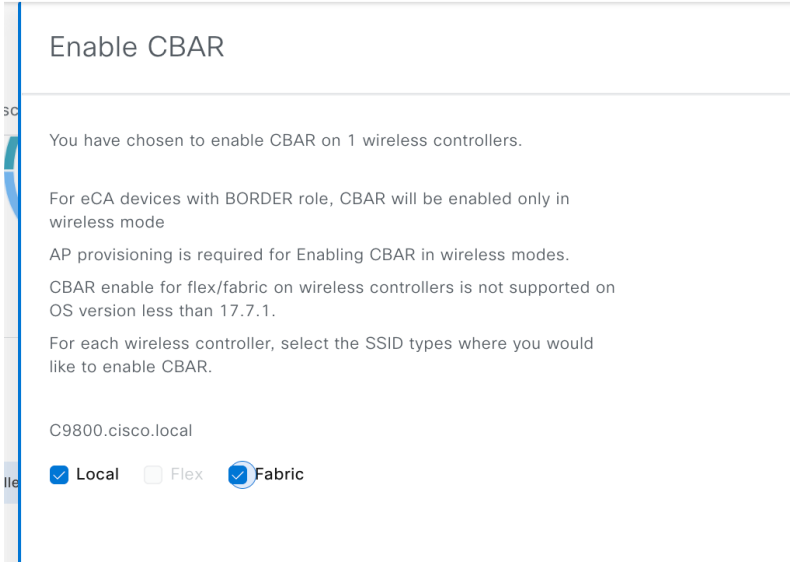


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Application Telemetry and Visibility Deployment for Wireless

Catalyst Center 2.3.7.x and above

- Specify SSID type to enable CBAR



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

Wireless Application Telemetry Deployment

For Your Reference

- 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
```


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

Wireless Application Telemetry Deployment

For Your Reference

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

Built-in Flow Records

```
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
```

```
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

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

Wireless Application Telemetry Deployment

For Your Reference

- 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
```


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

Wireless Application Telemetry Deployment

For Your Reference

- 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

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

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

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

Wireless Application Visibility Deployment

For Your Reference

- 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

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

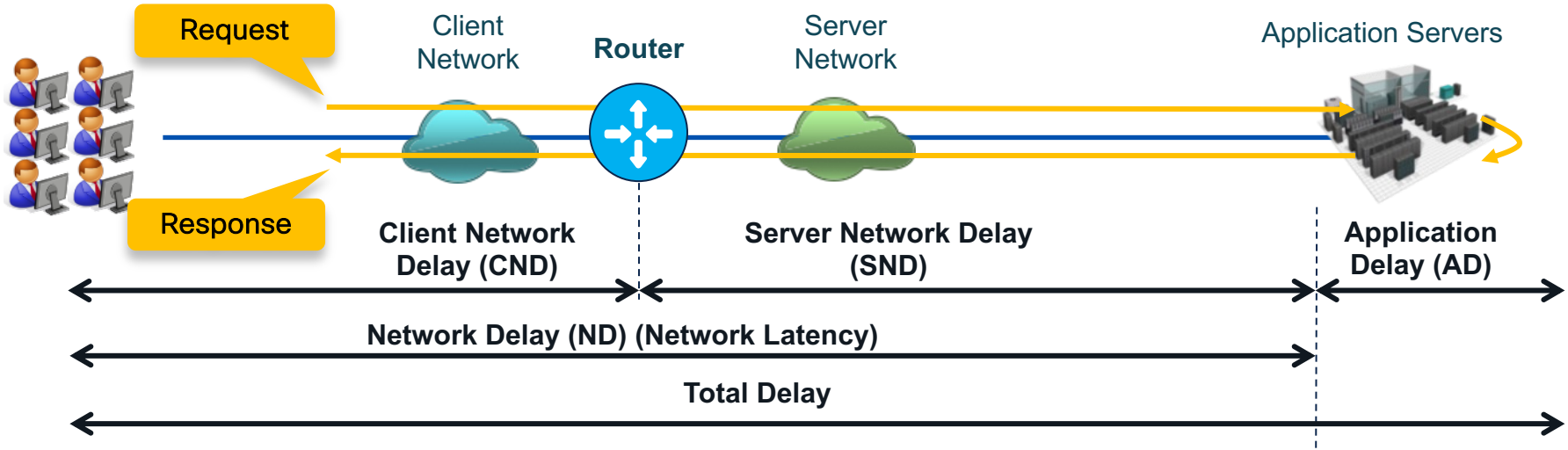
Application Telemetry and Visibility from Routers

- 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 Heath Scores calculated from performance metrics

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

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

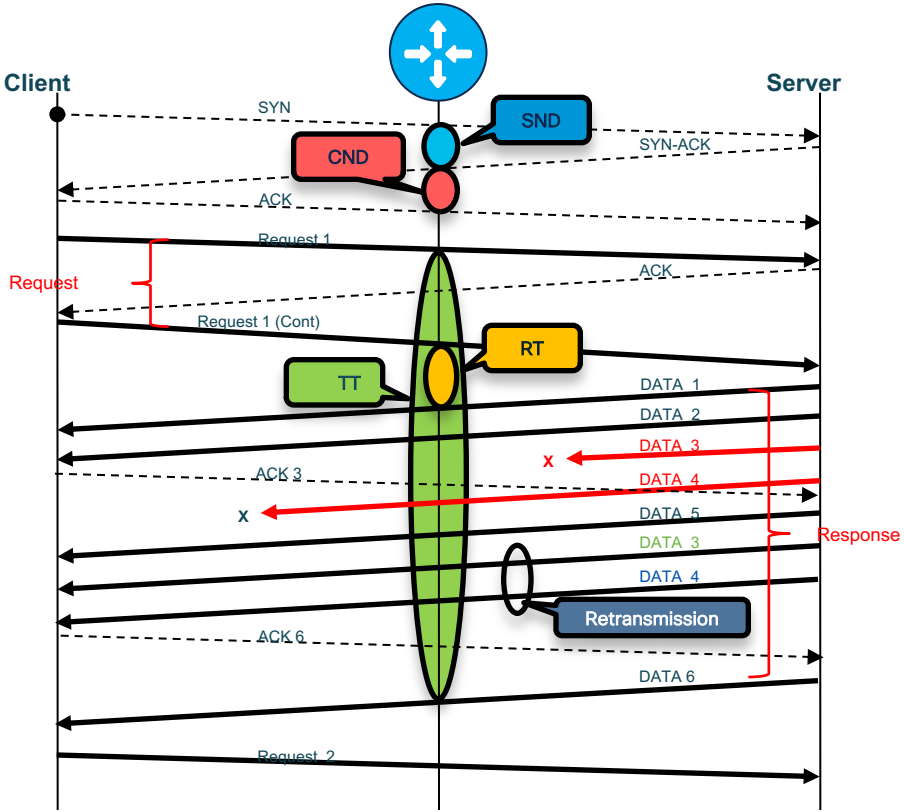


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Application Telemetry and Visibility from Routers

For Your Reference

- Application Response Time calculation for TCP traffic



Network Delay (ND, Latency)	ND = CND + SND
Response Time (RT)	t(First response pkt) – t(Last request pkt)
Transaction Time (TT)	t(Last response pkt) – t(First request pkt)
Application Delay (AD)	AD = RT – SND
Retransmission	Loss

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

Application Telemetry from Routers

For Your Reference

- 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

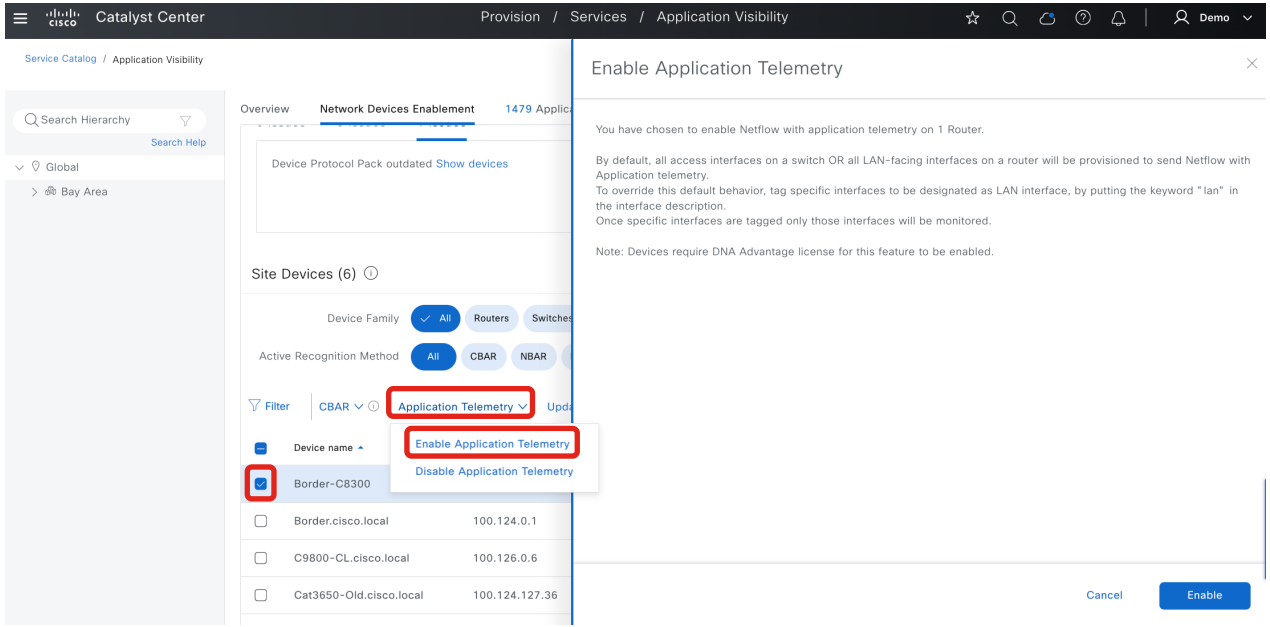
Latency, Application Delay, and Loss values shown on Cisco DNA Center Application Assurance

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

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

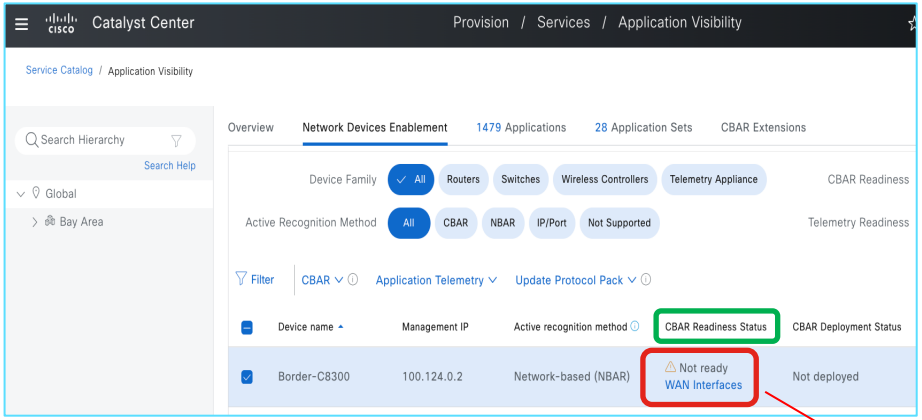


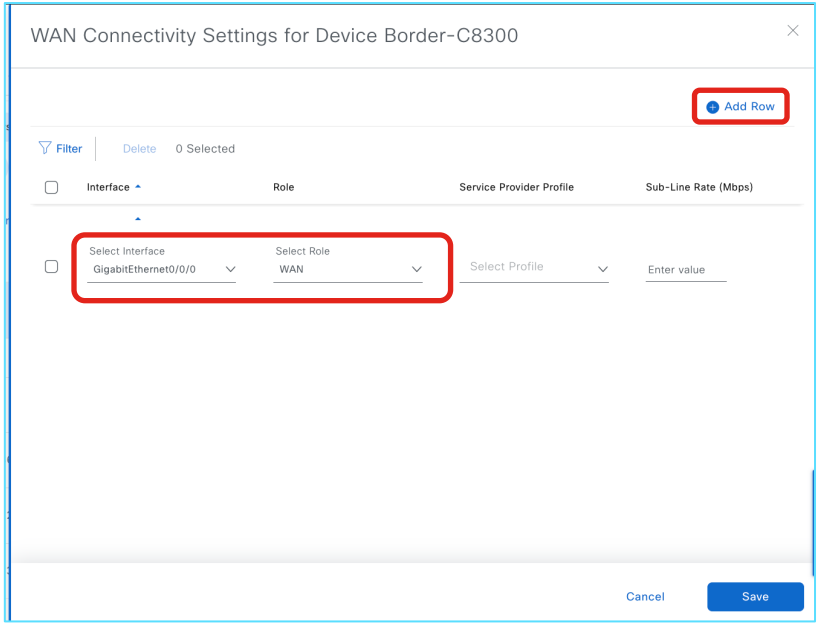
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

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





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

Router Application Telemetry Deployment

For Your Reference

- 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

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

Router Application Telemetry Deployment

- NetFlow verification – cache

For Your Reference

```
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
```


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

Router Application Telemetry Deployment

- NetFlow verification – export (1)

For Your Reference

```
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)
```


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

Router Application Telemetry Deployment

- NetFlow verification – export (2)

For Your Reference

```
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
```


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

Router Application Visibility Deployment

For Your Reference

- 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

interface GigabitEthernet0/0/0
 ip nbar protocol-discovery
```

Lo0 source interface if SDA fabric node; uplink interface otherwise

NBAR command pushed to specified "WAN" interface

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

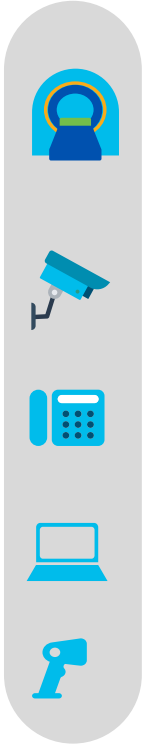
AI Endpoint and Trust Analytics

- 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

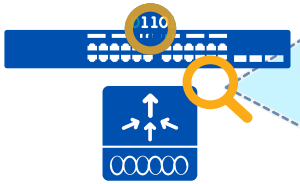
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

AI Endpoint and Trust Analytics

- Endpoint profiling via CBAR and Application Telemetry



802.1x/MAB



Catalyst 9000 Switches and 9800 Wireless Controllers (CBAR and Application Telemetry Enabled)

Cisco ISE

Policy

Labels

Context

EA

Catalyst Center EA

Endpoint Labels

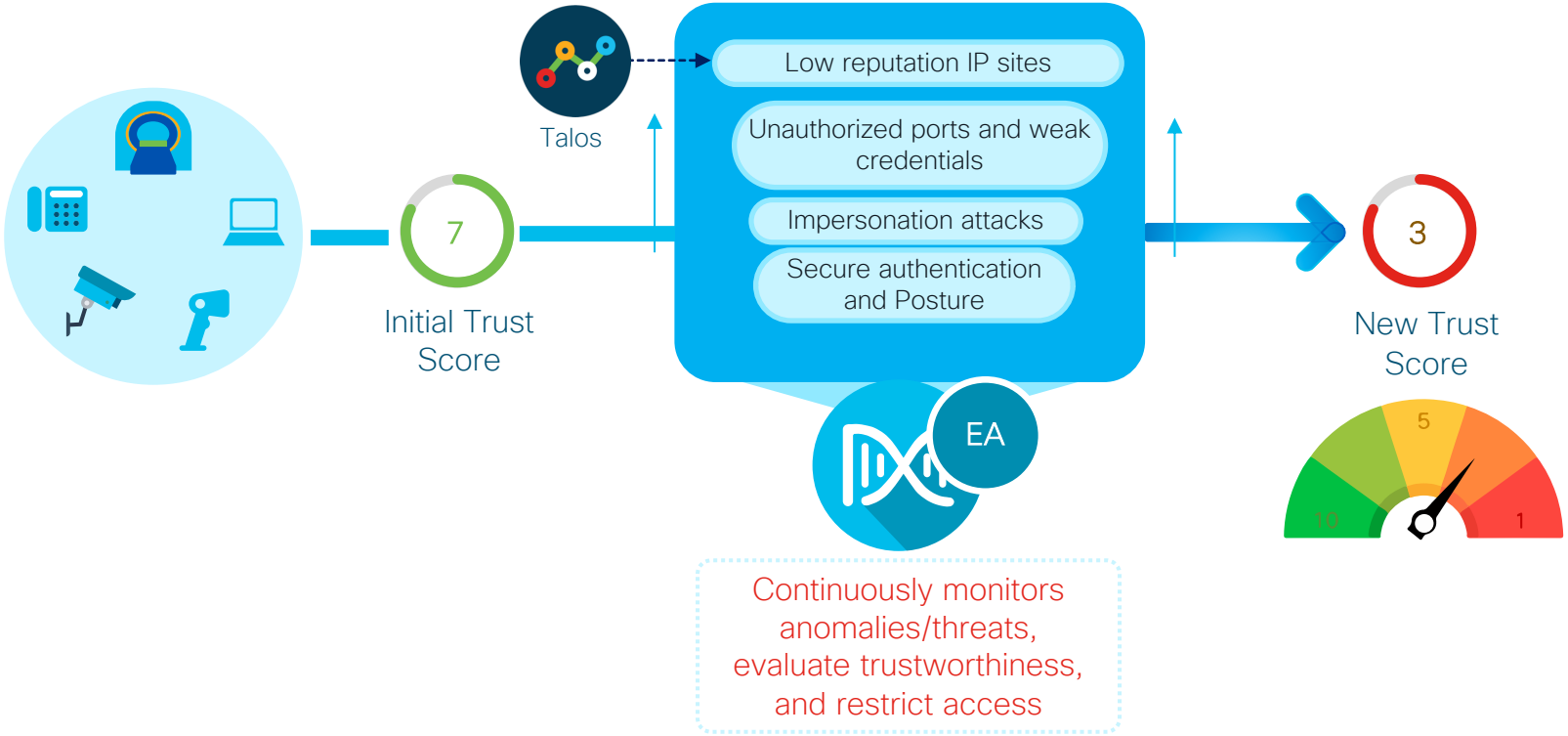
Endpoint Type: **CT Scanner**	Manufacturer: **Globex Corp.**
Model: **Ultima**	Operating System: **MS Windows 7**

EA Dashboard

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

AI Endpoint and Trust Analytics

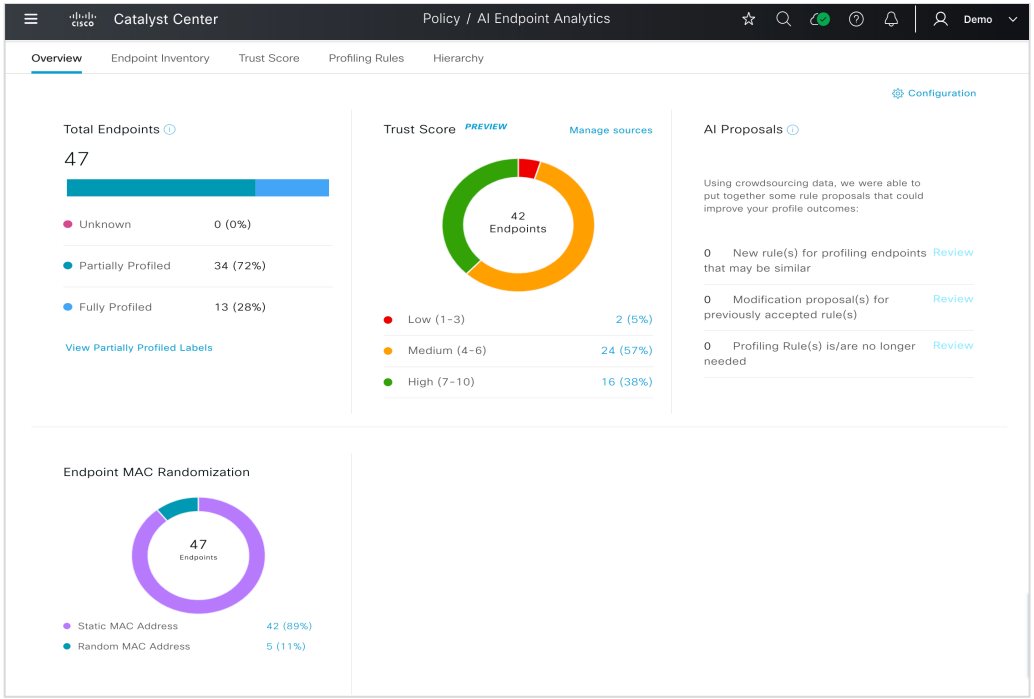
- Continuous validation of endpoints for Trusted Access



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

AI Endpoint and Trust Analytics

- EA Dashboard



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

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

Search

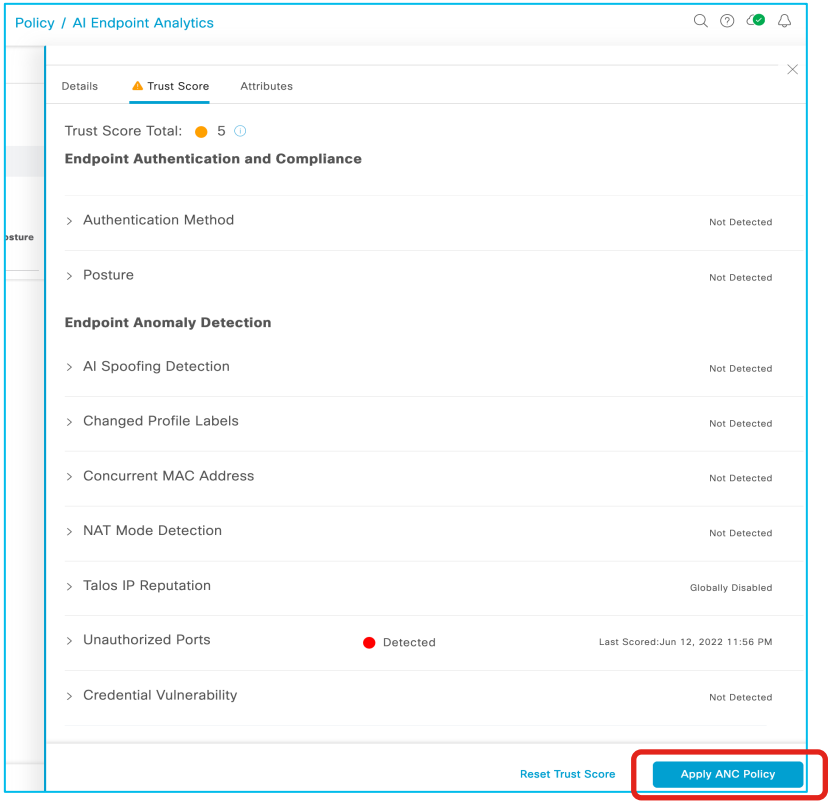
0 Selected | Register Endpoints | More Actions | Export

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 Internatio
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.

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

AI Endpoint and Trust Analytics

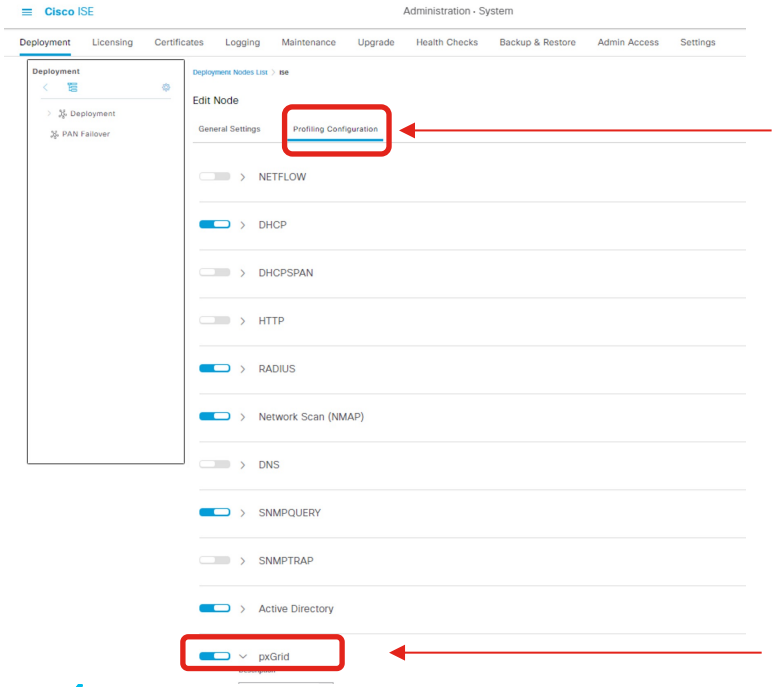
- Trust Scores and Remediation through Adaptive Network Control via ISE



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

AI Endpoint and Trust Analytics Deployment

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



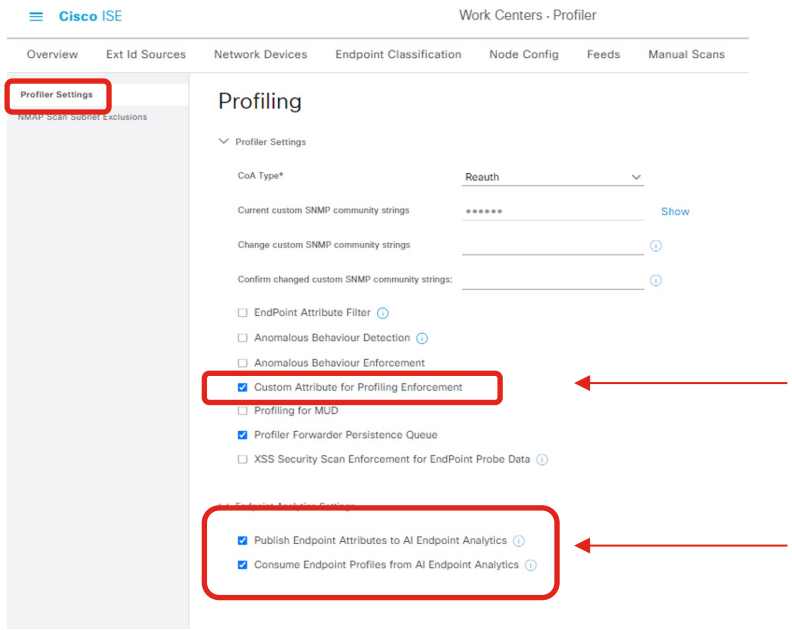
Profiling Configuration

Enable pxGrid, then Save

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

AI Endpoint and Trust Analytics Deployment

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



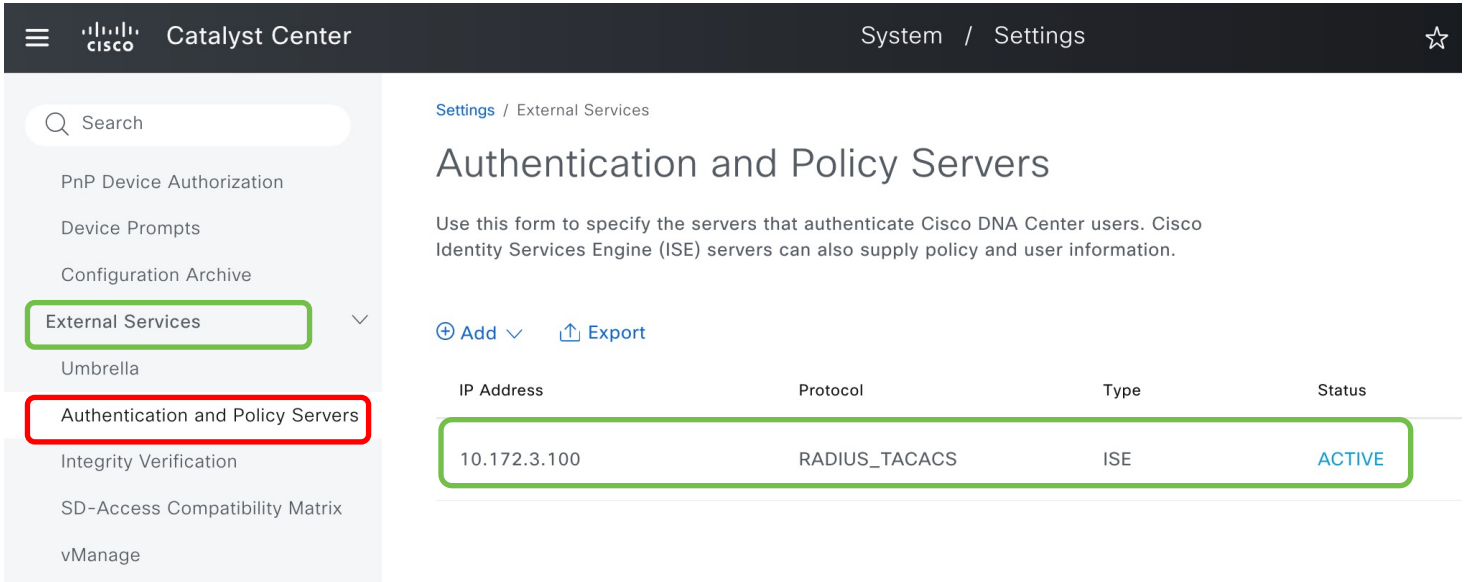
Enable Custom Attribute for Profiling Enforcement

Enable Publishing and Consumption of endpoint attributes, then Save

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

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)

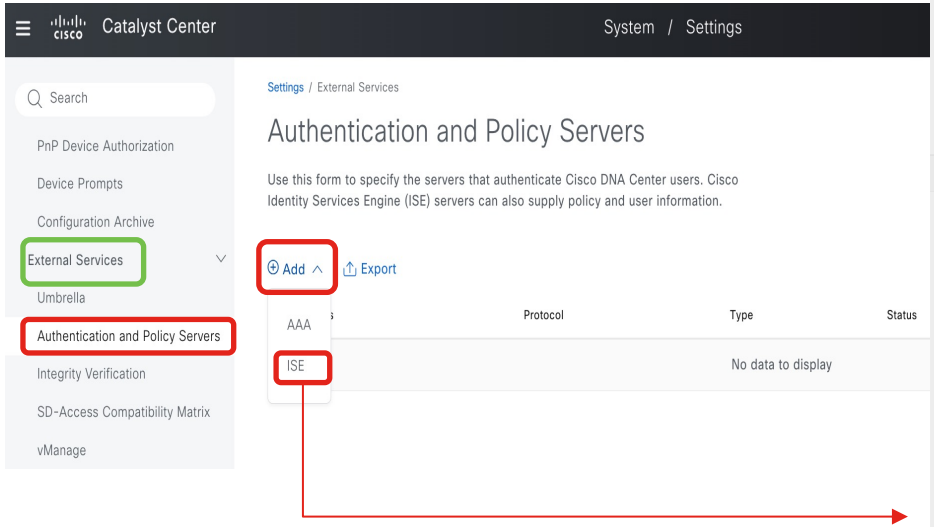


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

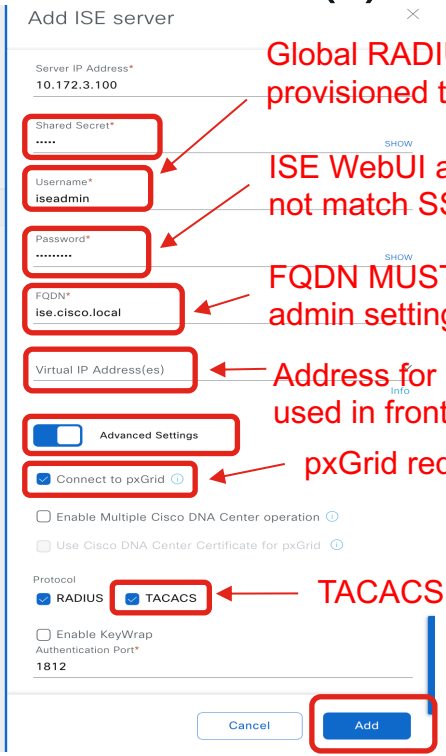
AI Endpoint and Trust Analytics Deployment

For Your Reference

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



Only one instance of ISE can be added



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

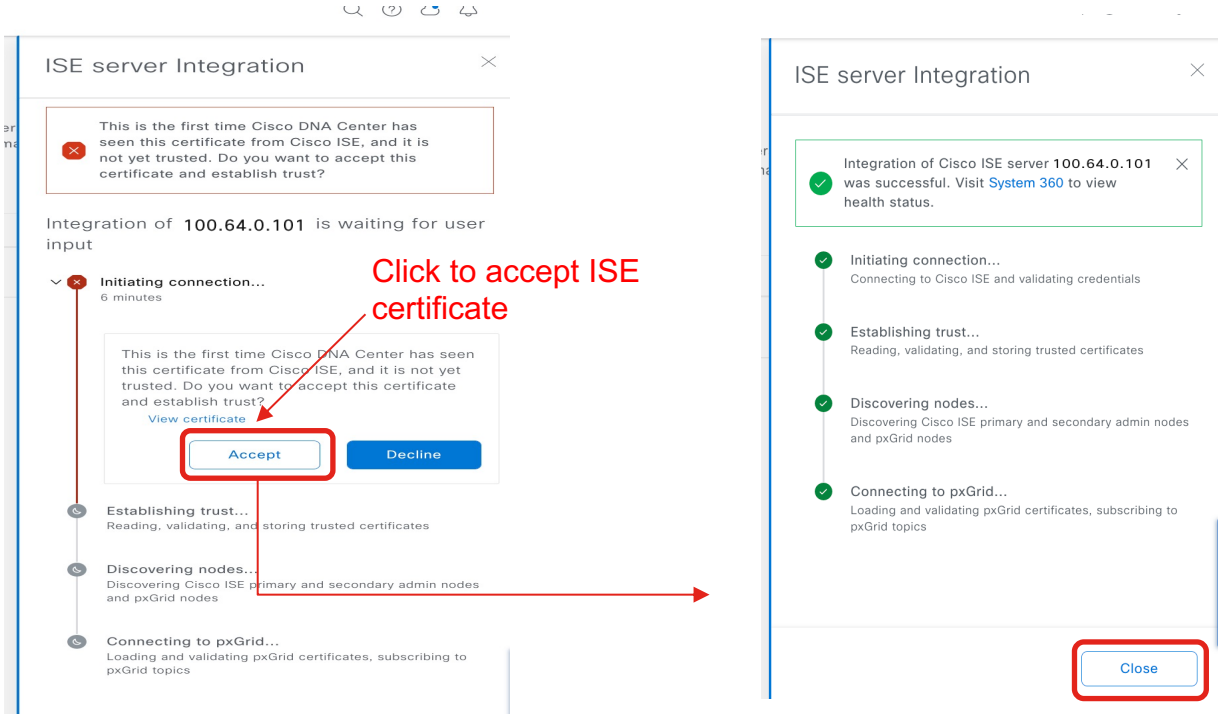
TACACS not selected by default

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

AI Endpoint and Trust Analytics Deployment

For Your Reference

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



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

AI Endpoint and Trust Analytics Deployment

For Your Reference

- 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
Log
Tests

WebSocket

Clients | Topics

Clients

Rows/Page 5 | 1 / 1

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

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

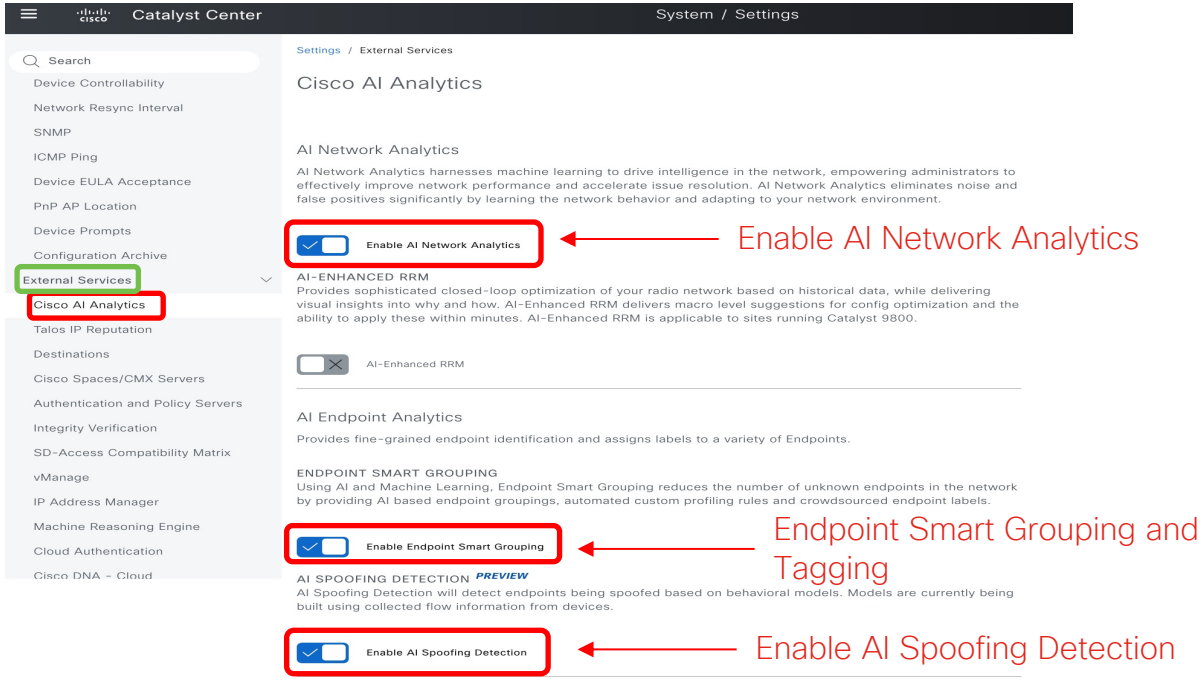
Catalyst Center pxGrid connection to ISE

No Publication attachments from Catalyst Center, yet

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

AI Endpoint and Trust Analytics Deployment

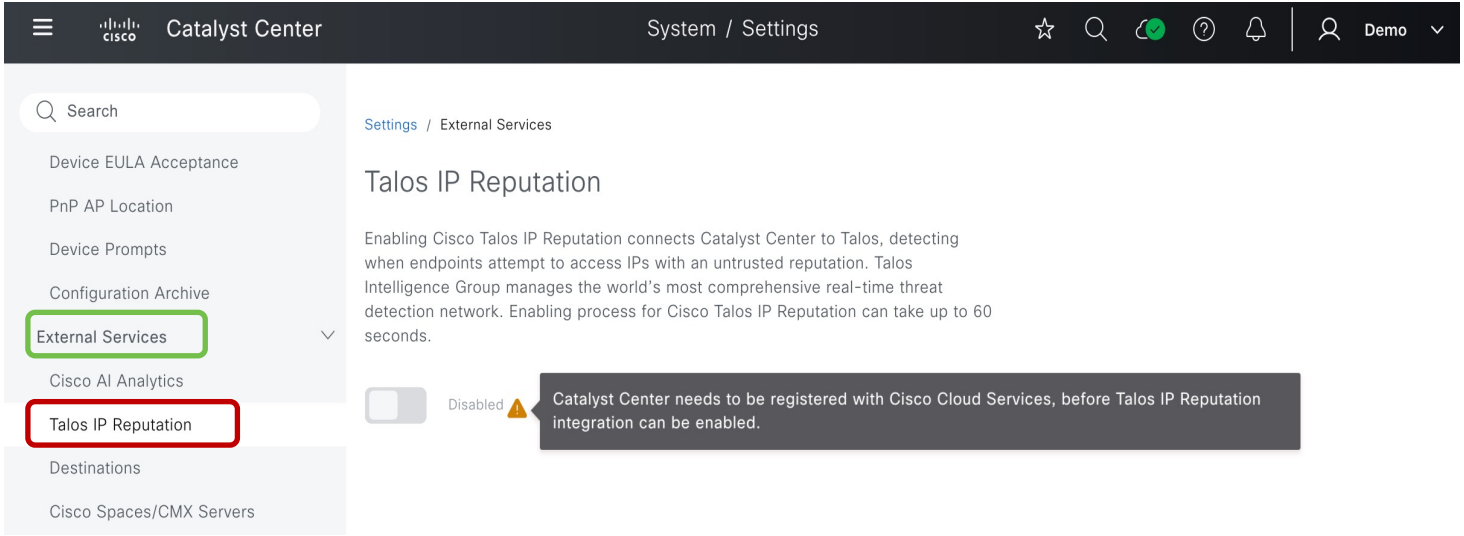
- On Catalyst Center, enable Endpoint Smart Grouping and AI Spoofing Detection under System -> Settings -> Cisco AI Analytics



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

AI Endpoint and Trust Analytics Deployment

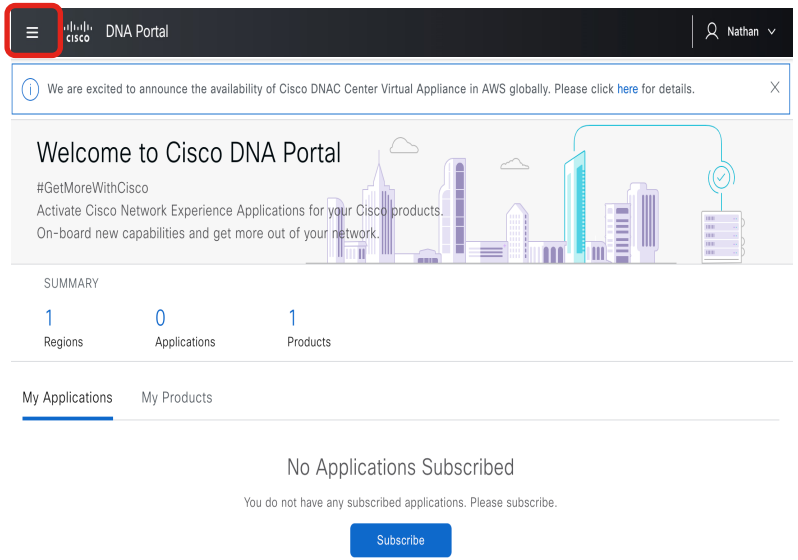
- Talos IP Reputation requires integration with dna.cisco.com (Cisco Cloud Services)

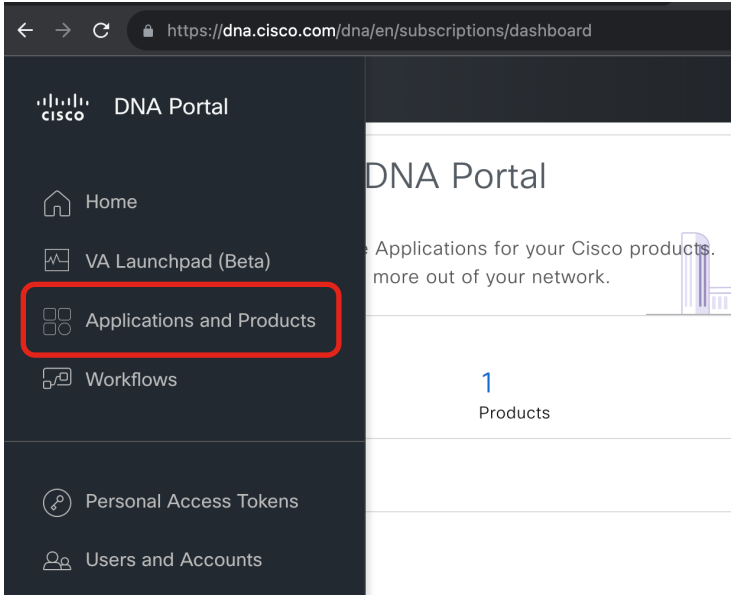


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

AI Endpoint and Trust Analytics Deployment

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

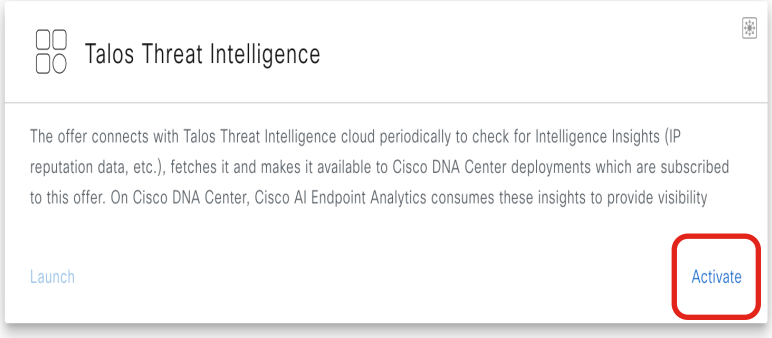


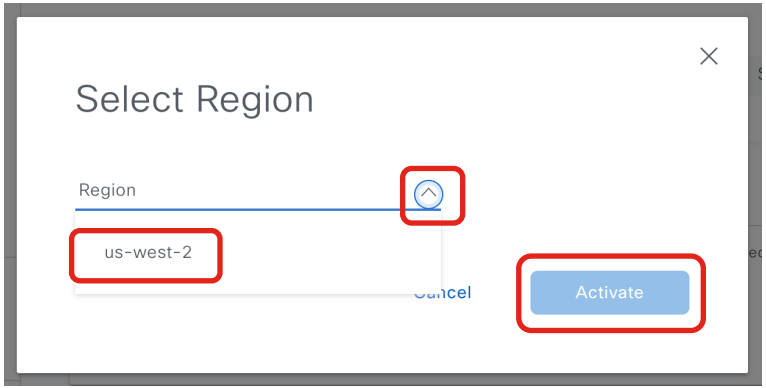


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

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

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

IP address reachable via web browser

Any preferred name

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

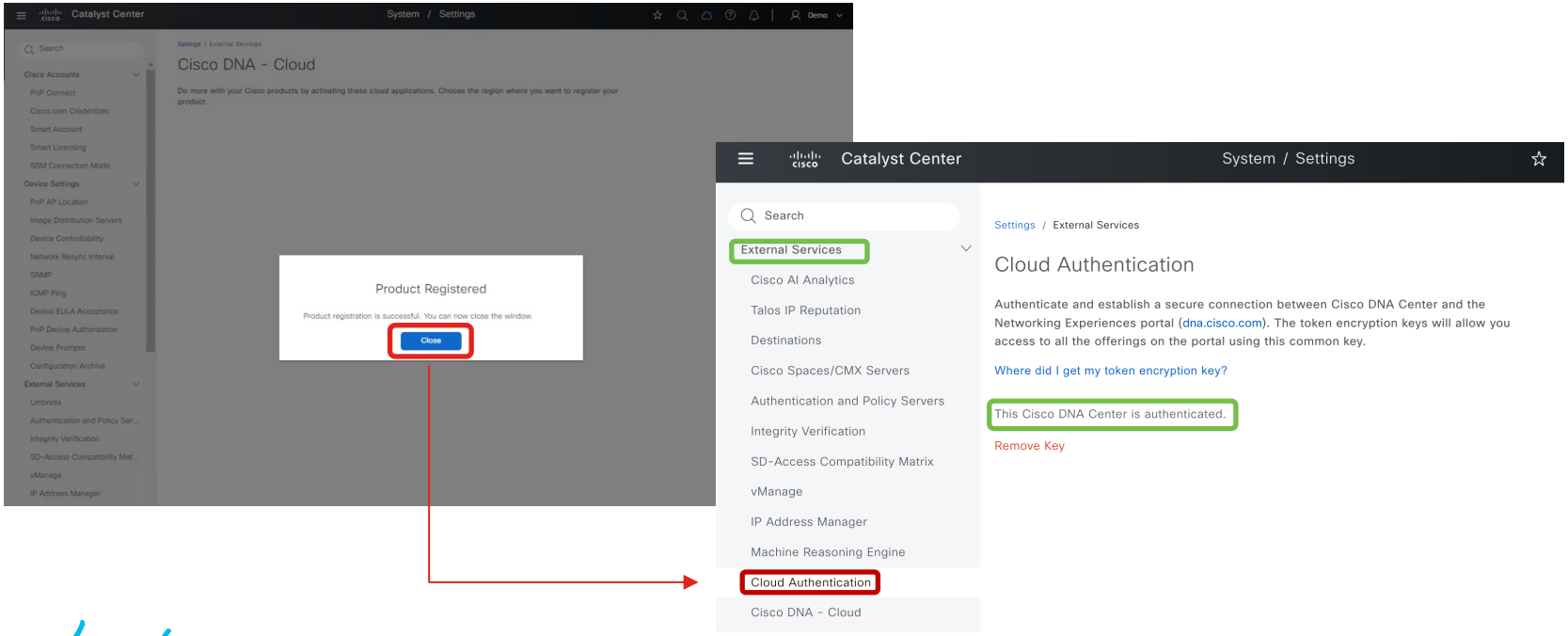
Previous | Register

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

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

AI Endpoint and Trust Analytics Deployment

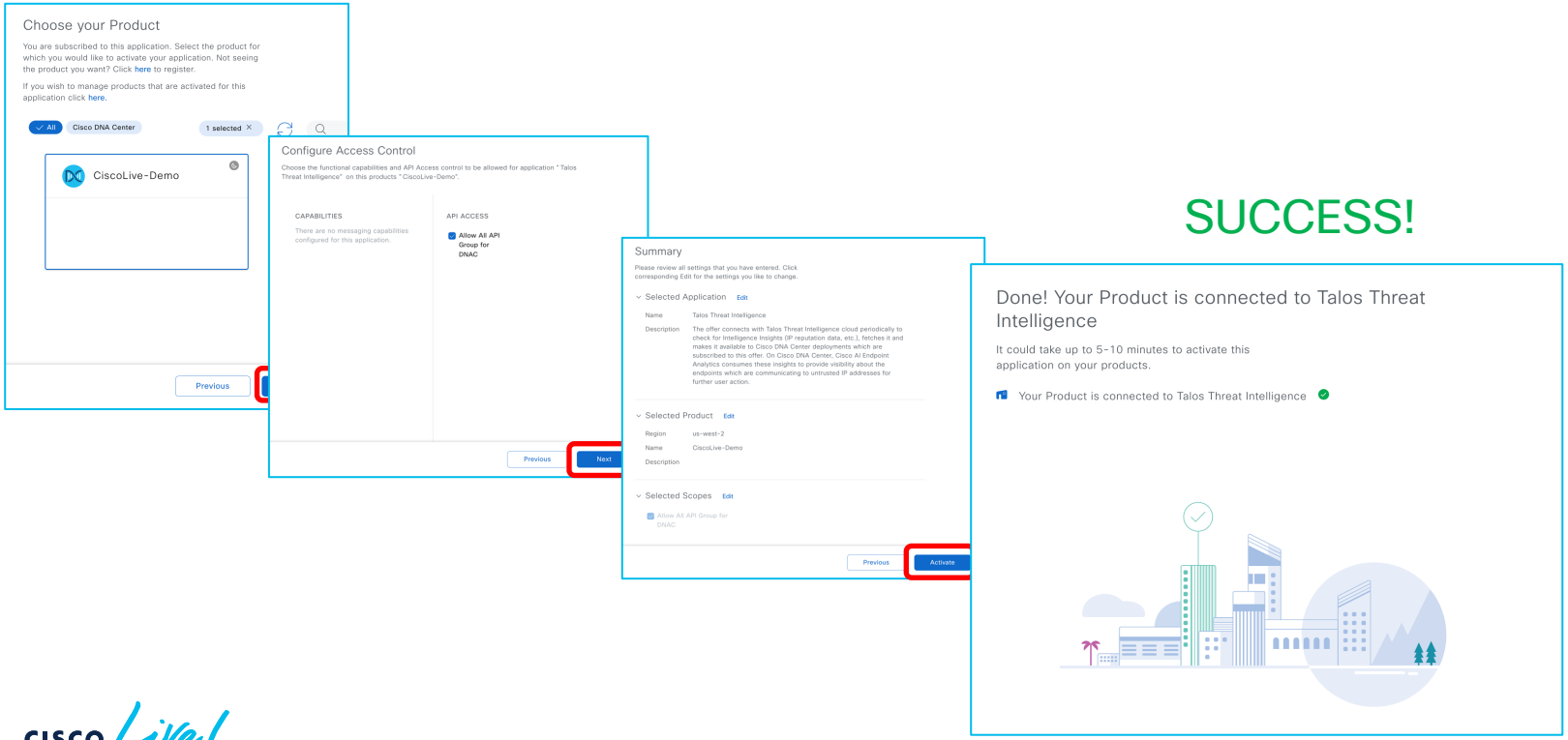
- OTP Key automatically added to Catalyst Center after logging in on newly launched window



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

AI Endpoint and Trust Analytics Deployment

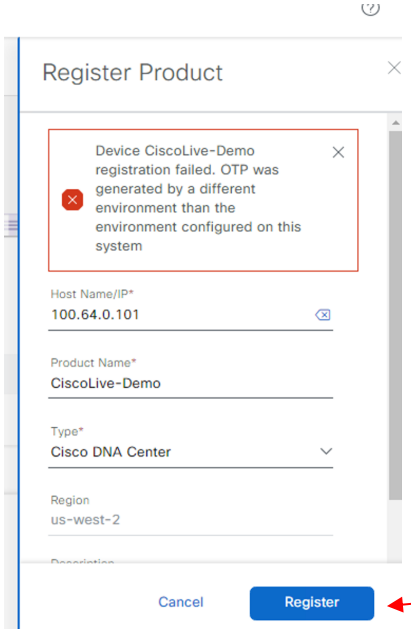
- Continue Talos activation workflow on Cisco DNA Portal



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

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)



magctl service setenv registration CLOUD_URL https://www.ciscoconnectdna.com

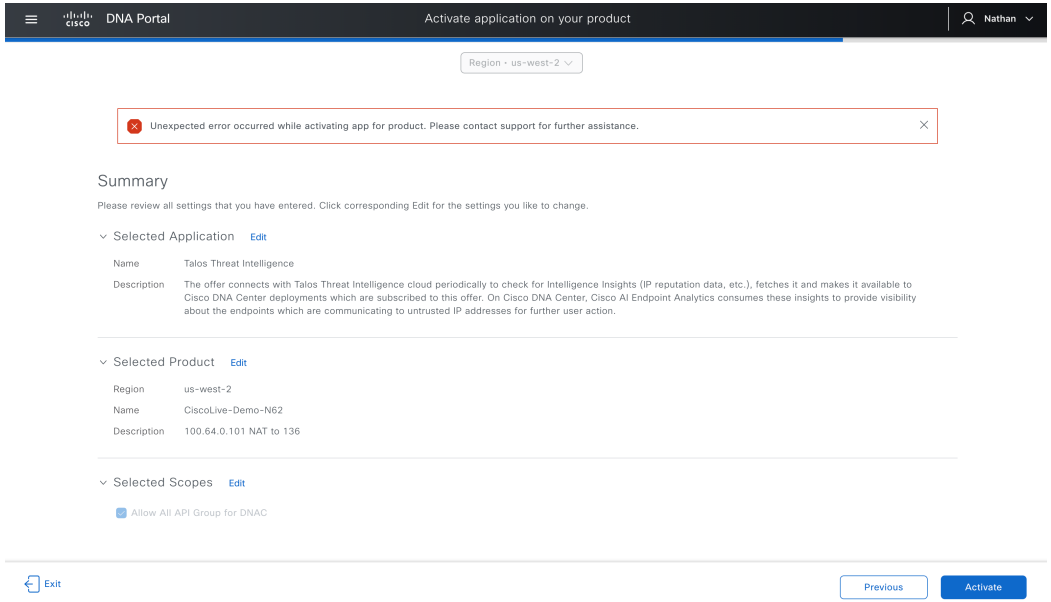
```
maglev@maglev-master-192-0-1-1:~$
maglev@maglev-master-192-0-1-1:~$
maglev@maglev-master-192-0-1-1:~$ magctl service setenv registration CLOUD_URL https://www.ciscoconnectdna.com
deployment.apps/registration patched
maglev@maglev-master-192-0-1-1:~$ magctl appstack status -f
NAMESPACE                NAME                                                    READY   STATUS      RESTARTS   AGE   IP
                NODE         NOMINATED NODE   READINESS GATES
maglev-system            license-service-cleanup-job-fjb72                       0/1     Completed   0          27h   16
9.254.40.92     192.0.1.1    <none>           <none>
maglev-system            registration-7db55d6d59-8vpd2                           0/1     Running     0          11s   16
9.254.40.159    192.0.1.1    <none>           <none>
maglev-system            release-job-8cc6798c-98e7-49e8-a4f5-079570c0aa2a-packages-j912n   0/1     Completed   0          26h   16
9.254.40.107    192.0.1.1    <none>           <none>
maglev@maglev-master-192-0-1-1:~$ magctl appstack status -f
NAMESPACE                NAME                                                    READY   STATUS      RESTARTS   AGE   IP
                NODE         NOMINATED NODE   READINESS GATES
maglev-system            license-service-cleanup-job-fjb72                       0/1     Completed   0          27h   16
9.254.40.92     192.0.1.1    <none>           <none>
maglev-system            release-job-8cc6798c-98e7-49e8-a4f5-079570c0aa2a-packages-j912n   0/1     Completed   0          26h   16
9.254.40.107    192.0.1.1    <none>           <none>
```

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

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

AI Endpoint and Trust Analytics Deployment

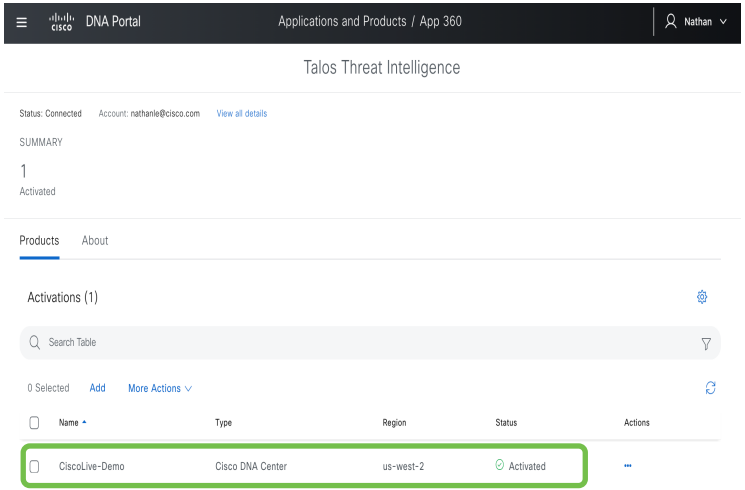
- If “unexpected error” occurs on Activation Summary screen, verify that the Smart Account associated with CCO ID has active Cisco DNA licenses. Contact TAC for resolution.



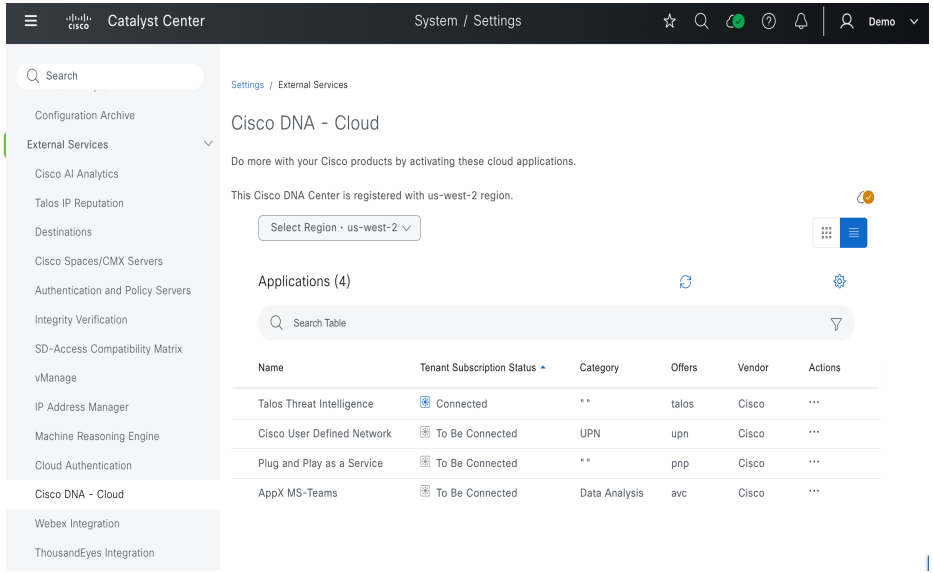
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

AI Endpoint and Trust Analytics Deployment

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



Cisco DNA Portal

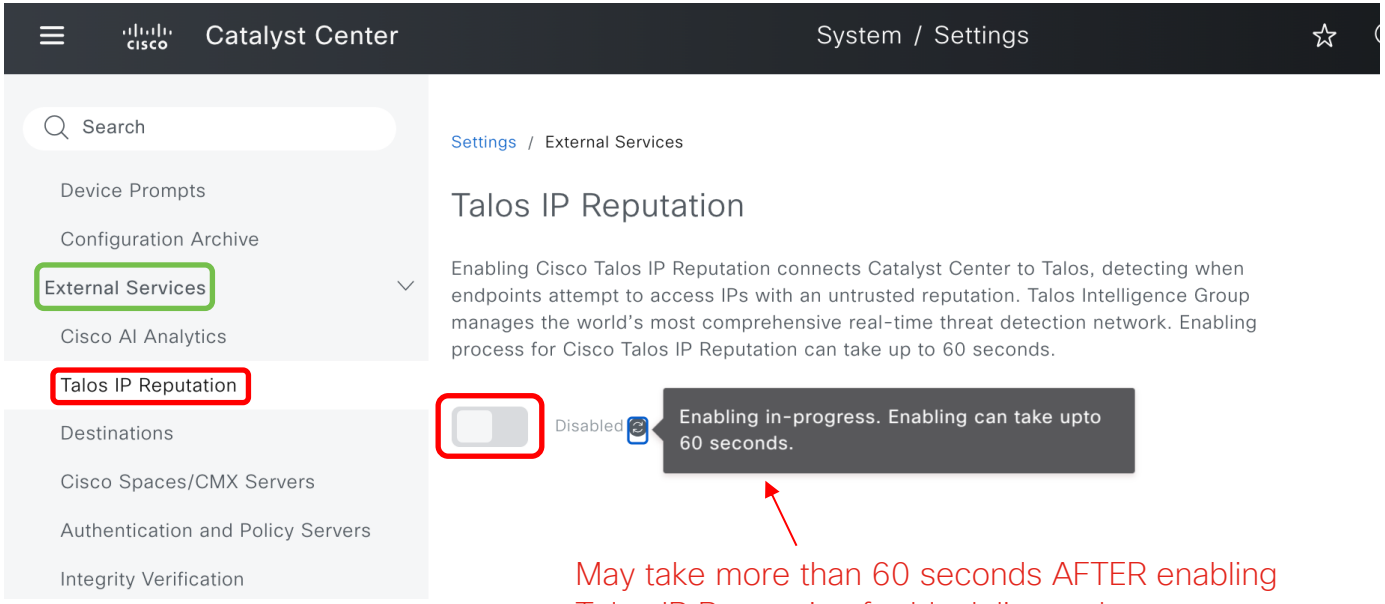


Catalyst Center
System Settings

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

AI Endpoint and Trust Analytics Deployment

- Talos IP Reputation can now be enabled

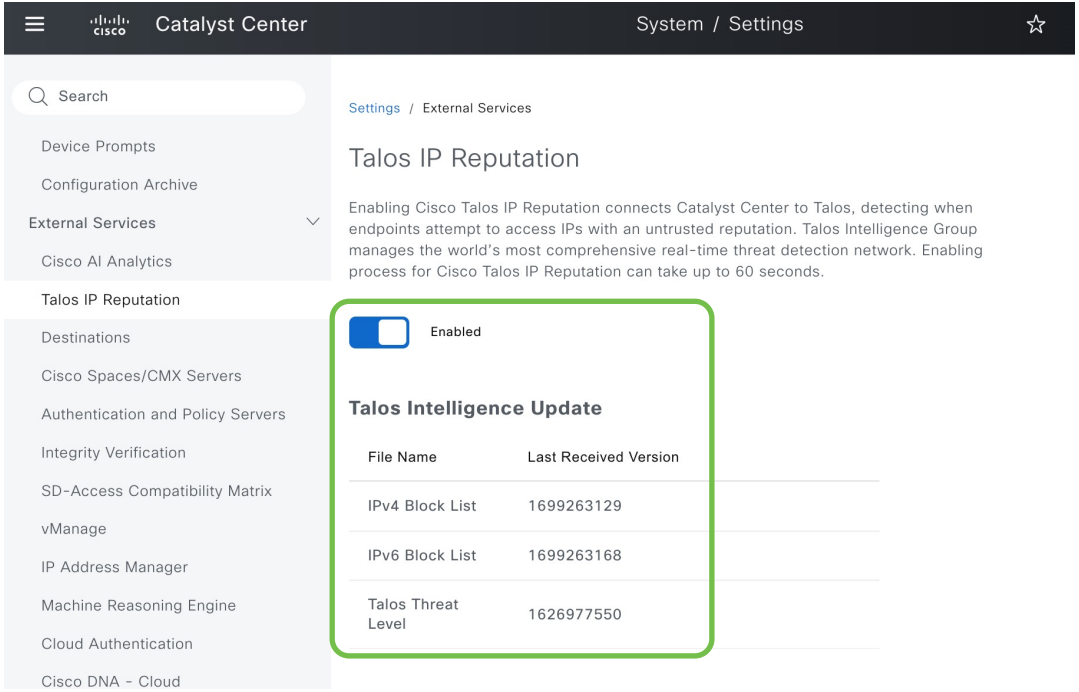


May take more than 60 seconds AFTER enabling Talos IP Reputation for block lists to be downloaded onto Catalyst Center

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

AI Endpoint and Trust Analytics Deployment

- Talos IP Reputation ready for service



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

AI Endpoint and Trust Analytics Deployment

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

Catalyst Center

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

Configure

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.

Let's Do It

Don't show this to me again

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

AI Endpoint and Trust Analytics Deployment

- Verify all prerequisites are met for EA to function properly

Catalyst Center — Set up prerequisites and configurations

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.

Enabled

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.

Enabled

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.

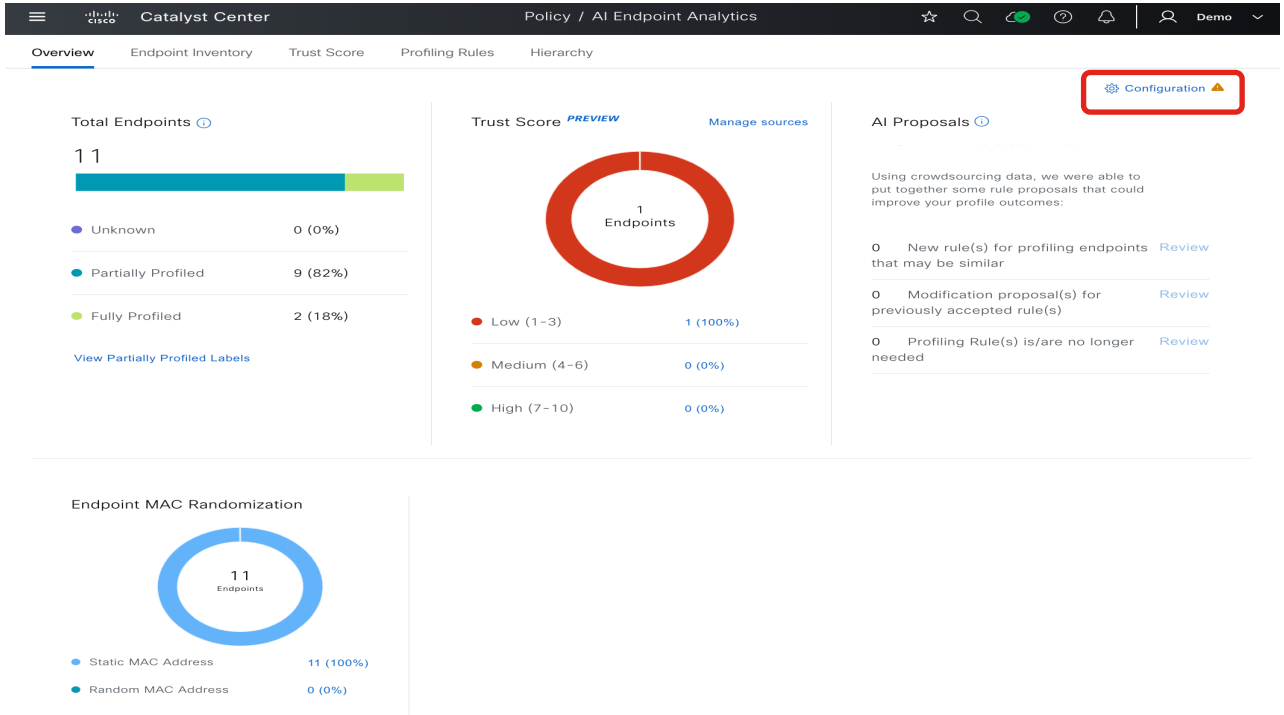
Enable Endpoint Smart Grouping

Finish

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

AI Endpoint and Trust Analytics Deployment

- AI Endpoint Analytics functional state



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

AI Endpoint and Trust Analytics Deployment

- Endpoint Analytics functional state

Catalyst Center

Demo

AI Endpoint Analytics / Configurations

- 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
DPI Enablement (CBAR)	Enabled	3 of 3 items are completed
ISE Configuration	Enabled	2 of 2 items are completed
AI Analytics Integration	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.

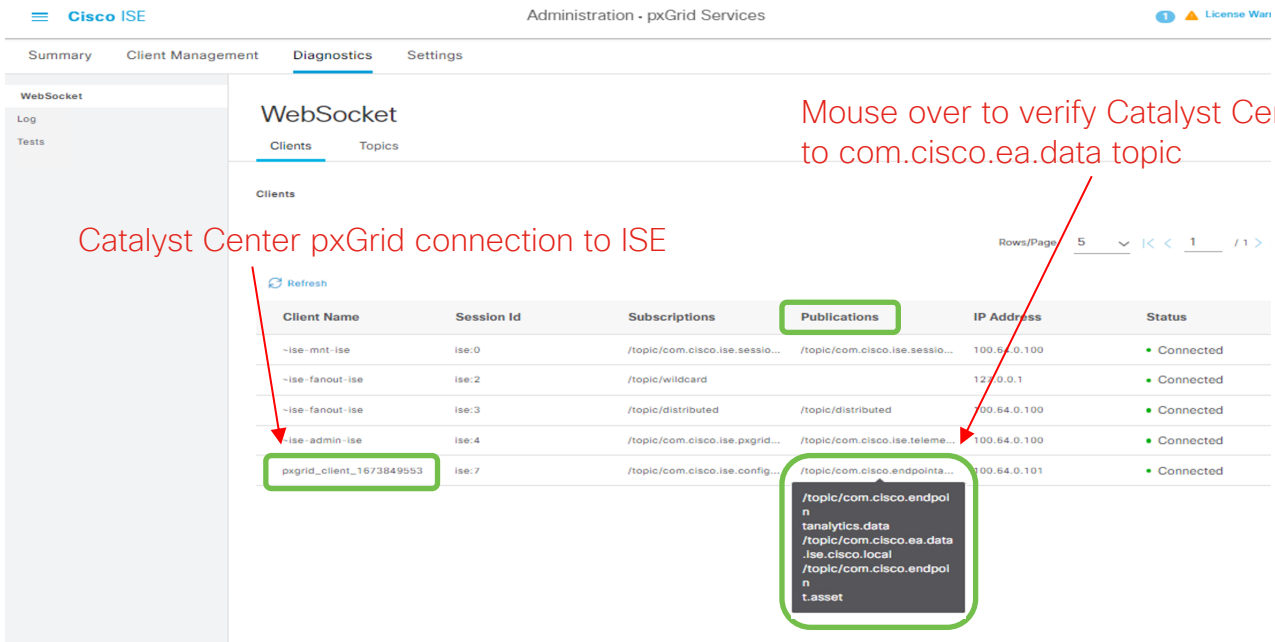
Status: All | Enabled | Disabled

Configuration Name	Status	Details
Security Sensor	Disabled	0 of 3 items are completed
ServiceNow	Disabled	0 of 1 items are completed
Talos IP Reputation	Enabled	5 of 5 items are completed
AI Spoofing detection	Enabled	3 of 3 items are completed

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

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



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

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
5. Join Cisco Community

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

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:

Tuesday	**3:00pm – 7:00pm**
Wednesday	**11:15am – 7:00pm**
Thursday	**9:30am - 4:00pm**
Friday	**10:30am - 1:30pm**

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

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

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

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

Thank you

cisco Live!

Let's go

#CiscoLiveAPJC