

CISCO *Live!*

Let's go



The bridge to possible

The Flow of Things

Navigating and Properly Enabling NetFlow-based
Solutions Through Catalyst Center

Nathan Lee, Technical Solutions Architect
@networkaugur

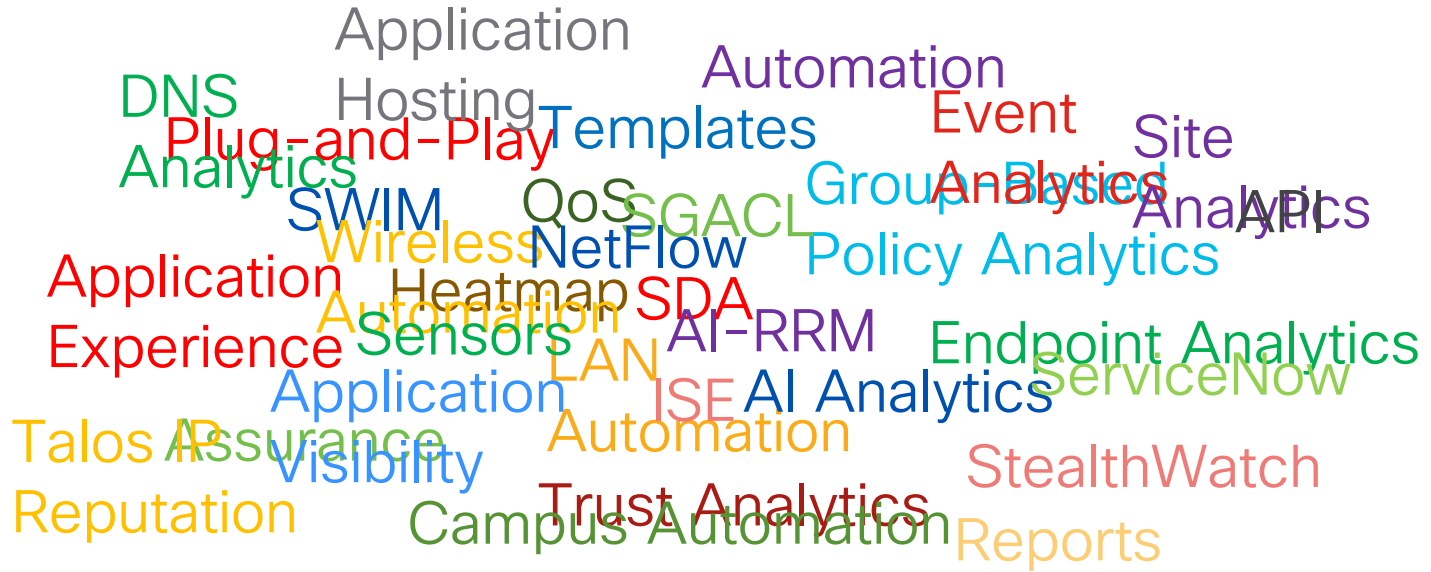
CISCO *Live!*

BRKOPS-2038

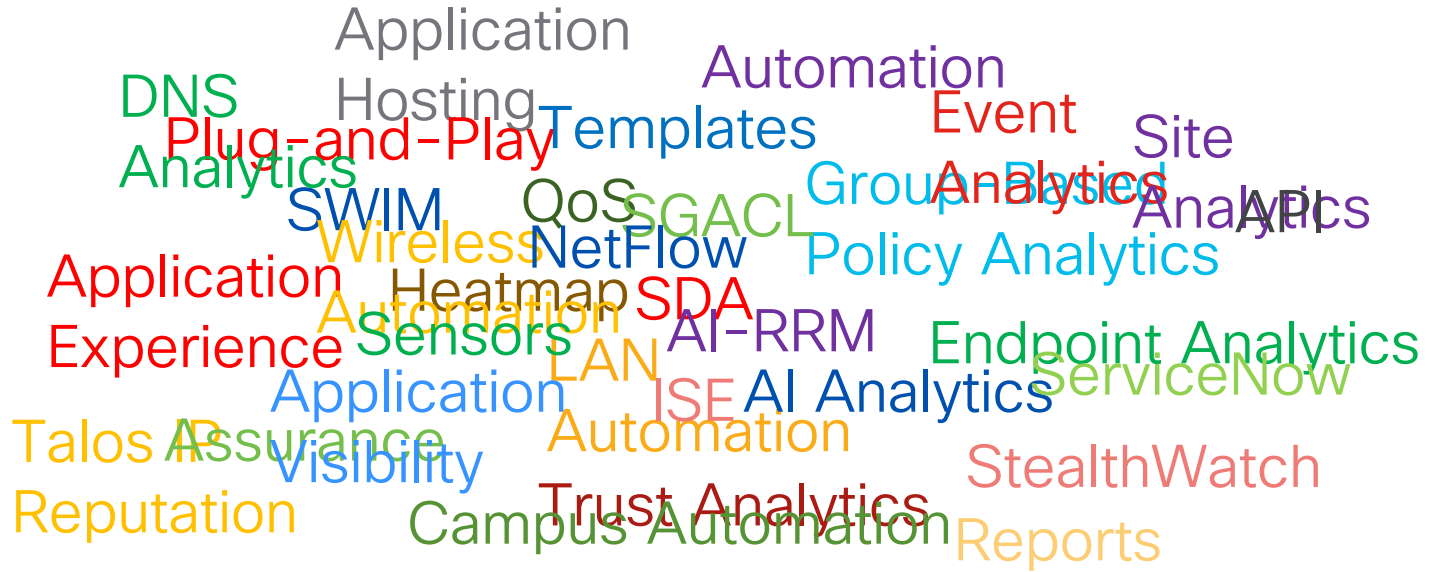
Agenda

- Introduction
- NetFlow Basics
- Application Experience
- Applications
- Summary

Cisco Catalyst Center Features



Cisco Catalyst Center Features

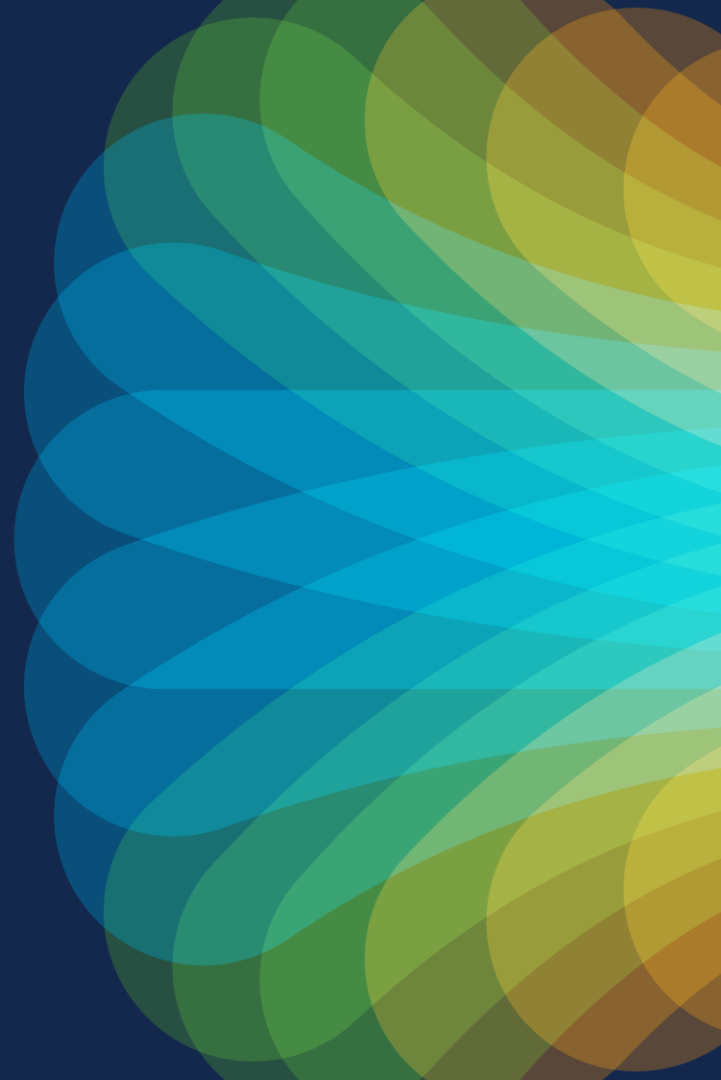


Session Assumptions and Objectives

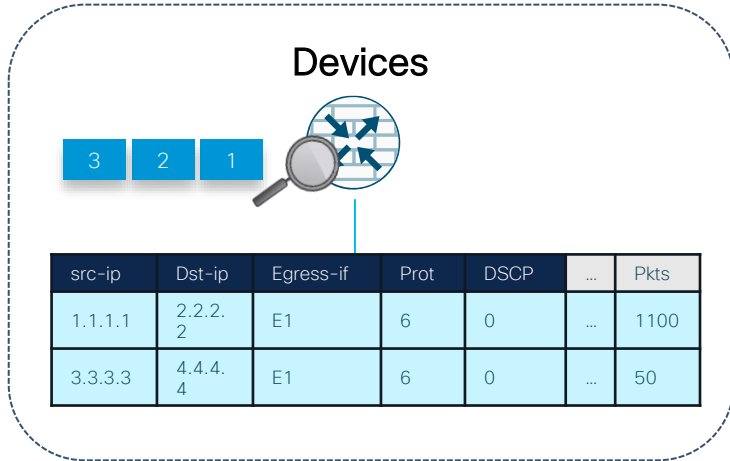
- Catalyst Center 2.3.7.x, IOS-XE 17.12.x or greater, and ISE 3.2 Patch 3 or greater
- High level overview of features
 - NOT deep dive
- Focus on proper deployment of features
 - Step-through deployment examples

Proper workflow leads to proper NetFlow!

NetFlow Basics

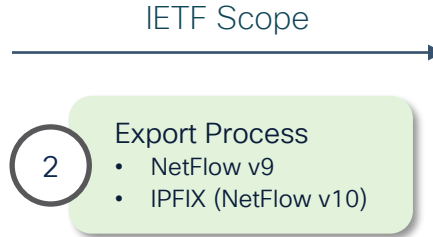


NetFlow Basics

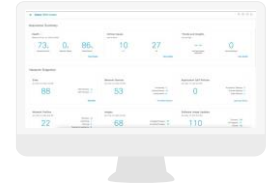


Implementation specific

- 1
- Metering Process
 - Flexible NetFlow
 - Performance Monitor



NetFlow Collector



- Capacity Planning
- Security
- Performance Analysis
- Visibility
- Troubleshooting

What are Flows?

- Fundamental units of network traffic monitoring and management, e.g. TCP/UDP sessions
- Each flow defined by a set of key fields
 - IPv4/IPv6 source and destination addresses, L4 protocol, L4 source and destination ports
 - Each flow is unidirectional TCP/UDP session
- Tracked in on-device cache with flow records containing key fields and some non-key fields, e.g. counters and timestamps
- Example:

IPv4 Packet	Key Fields		Non-key Fields		Flow Record
	Src Address	Dst Address	Protocol	Packet Counter	
P1	1.1.1.1	1.1.1.2	UDP	1	F1
P2	1.1.1.1	1.1.1.3	UDP	1	F2
P3	1.1.1.1	1.1.1.2	TCP	2	F3
P4	1.1.1.1	1.1.1.2	UDP	3	F1

Flexible NetFlow (FNF) Configuration

- Define **flow record**
 - Specify key and non-key fields of interest
- Define one or more **flow exporters**
 - Export destination
 - Transport protocols (NetFlow Version 9 or IPFIX)
- Define **flow monitor**
 - Specify cache parameters
 - Reference above flow record and exporter(s)
- Apply ingress/egress flow monitor to **interface**

Flexible NetFlow Configuration Example

- Identify flow by a unique combination of IPv4 source address, destination address and application protocol key fields
- Maintain a counter of bytes for each flow
- Send reports on aged out flows to server at 100.64.0.101 on udp port 2055
- Cache up to 1M flows, age out flows that go silent for 1 sec
- Monitor traffic on interface Gig1/0/1

With Cisco Catalyst Center, all relevant NetFlow configuration is automated and orchestrated on network devices!

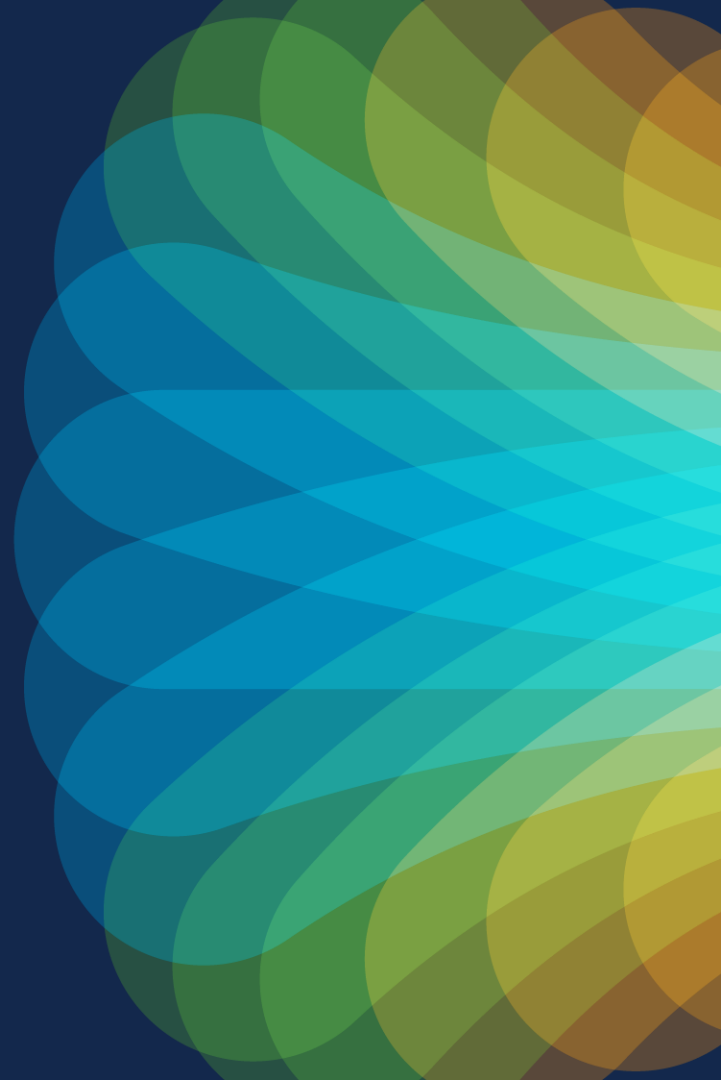
```
flow record FNF-Record
match ipv4 source address
match ipv4 destination address
match application name
collect counter bytes

flow exporter FNF-Exporter
destination 100.64.0.101
transport udp 2055

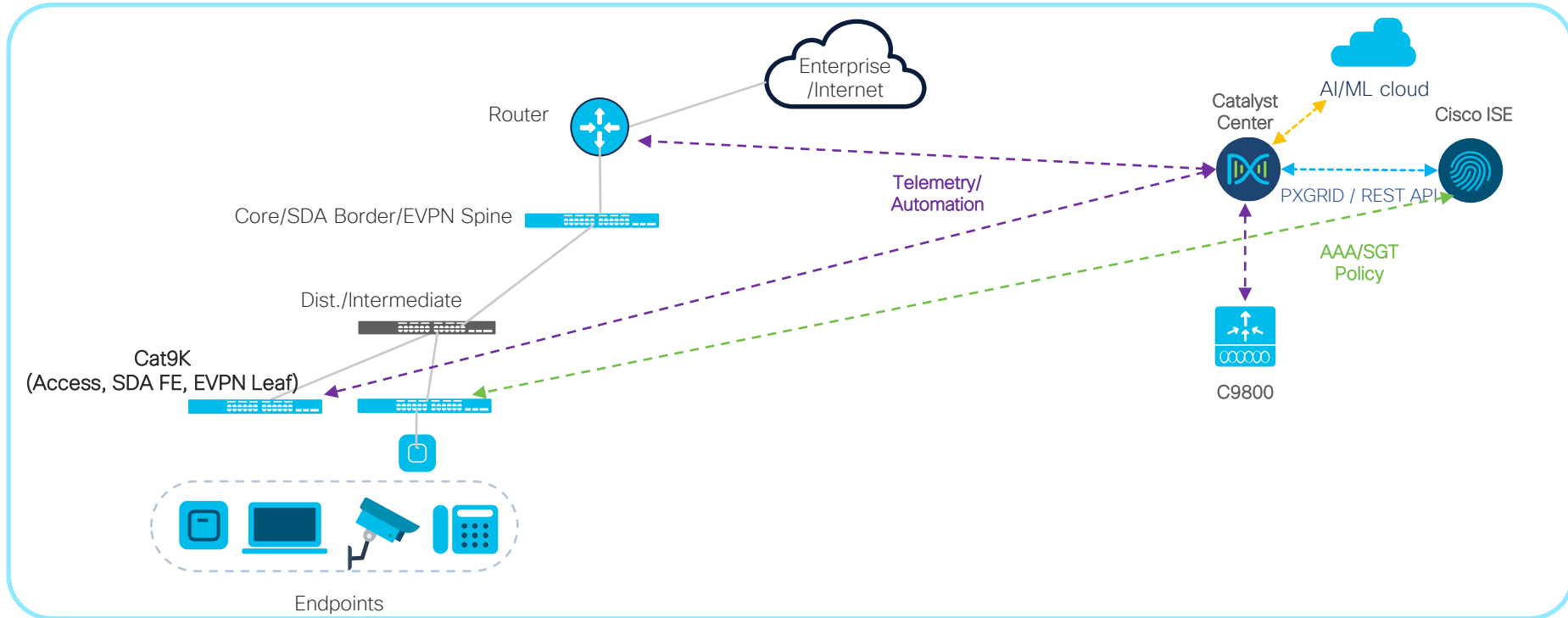
flow monitor FNF-Monitor
record FNF-Record
exporter FNF-Exporter
cache entries 1000000
cache timeout inactive 1

interface Gig1/0/1
ipv4 flow monitor FNF-Monitor input
```

Application Experience



Application Experience



Application Telemetry?

Application Visibility?

Application Experience?

Application Experience

- Application Telemetry
 - Configuration on network devices orchestrated by Catalyst Center to send traffic telemetry to Catalyst Center or Cisco Telemetry Broker
 - **NetFlow/IPFIX** exports from devices
- Application Visibility
 - Classification of applications
 - Locally on devices (**NBAR**) and/or on Catalyst Center (**CBAR**)
 - Classification export from devices on a separate stream from regular App Telemetry
- Application Experience
 - Umbrella term used to encompass Application Telemetry and Application Visibility
 - Also often used to describe **qualitative** Application Visibility (as opposed to **quantitative** AppViz)

Application Telemetry Deployment

The screenshot shows the Cisco Catalyst Center interface. The top navigation bar includes the Cisco logo, 'Catalyst Center', and 'Design / Network Settings'. Below this, there are tabs for 'Servers', 'Device Credentials', 'IP Address Pools', 'Wireless', 'Telemetry', and 'Security and Trust'. The 'Telemetry' tab is highlighted with a red box. The main content area is titled 'Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned.' It contains several sections: 'SNMP Traps' with a checked option 'Use Cisco DNA Center as SNMP trap server'; 'Syslogs' with a checked option 'Use Cisco DNA Center as syslog server'; and 'Application Visibility' which is highlighted with a red box. The 'Application Visibility' section includes the text 'Enable Netflow Application Telemetry and Controller Based Application Recognition (CBAR) by default upon network device site assignment' and a checked option 'Enable by default on supported wired access devices'. Below this, it says 'Choose the destination collector for Netflow records sent from network devices.' and has a checked option 'Use Cisco DNA Center as the Netflow Collector' and an unchecked option 'Use Cisco Telemetry Broker (CTB) or UDP director'.

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

Application Telemetry Deployment

The screenshot shows the Catalyst Center interface for configuring network settings. The 'Telemetry' tab is selected. The 'Wired Endpoint Data Collection' section is expanded, showing the following configuration options:

- Enable by default on supported wired access devices
- Use Cisco DNA Center as the Netflow Collector
- Use Cisco Telemetry Broker (CTB) or UDP director
- Enable Cisco DNA Center Wired Endpoint Data Collection At This Site
- Disable Cisco DNA Center Wired Endpoint Data Collection At This Site

Strongly Recommended to enable Wired Data Endpoint Collection

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

Application Telemetry Deployment

The screenshot shows the Cisco Catalyst Center interface for configuring Telemetry. The 'Telemetry' tab is selected and highlighted with a red box. The page content includes:

- Navigation tabs: Servers, Device Credentials, IP Address Pools, Wireless, **Telemetry**, Security and Trust.
- Left sidebar: Find Hierarchy (Global, Bay Area).
- Main content 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 (checked) or Use Cisco Telemetry Broker (CTB) or UDP director.
 - Wired Endpoint Data Collection:
 - Enable Cisco DNA Center Wired Endpoint Data Collection At This Site (checked) or Disable Cisco DNA Center Wired Endpoint Data Collection At This Site.
 - Wireless Controller, Access Point and Wireless Clients Health (highlighted with a red box):
 - Enable Wireless Telemetry (checked).
- Buttons: Reset, Save.

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

Application Telemetry from Access Switches

Overview

- Flexible NetFlow config orchestrated from Catalyst Center to match applications
- Supported for Software Defined Access (SDA) fabric or non-fabric
- Switches must be activated with DNA-Advantage licenses
 - IOS-XE requires DNA/Catalyst Essential for Flexible NetFlow
 - Application Assurance on Catalyst Center requires DNA/Catalyst Advantage → Switches must have Advantage licenses
- Quantitative visibility only – no performance metric (loss, jitter, latency)

Application Telemetry from Switches

- Switch-based Application Visibility does not include performance metrics

The screenshot shows the Catalyst Center Applications dashboard. A table lists various applications with their health, business relevance, usage, and throughput. The 'ssh' application is highlighted with a red box, and its performance metrics (Packet Loss, Network Latency, and Jitter) are also highlighted with a red box.

Name	Health	Business Relevance	Usage	Average Throughput	Packet Loss (%)	Network Latency	Jitter
rms-update	--	Default	7.5GB	8.4Mbps	--	--	--
ssh	--	Business Relevant	7.5GB	24.1Mbps	--	--	--
google-services	--	Default	3.9GB	3.1Mbps	--	--	--
unknown	--	Default	1.3GB	1Mbps	--	--	--
statistical-conf-video	--	Default	269MB	3.8Mbps	--	--	--
binary-over-http	--	Default	189.4MB	497.5Kbps	--	--	--
rms-services	--	Default	3.5MB	3Kbps	--	--	--

The screenshot shows the Catalyst Center Application Experience dashboard for the 'ssh' application. It displays usage and throughput graphs over time. The 'ssh' application is highlighted with a red box. Below the graphs, there is a table for Application Endpoints.

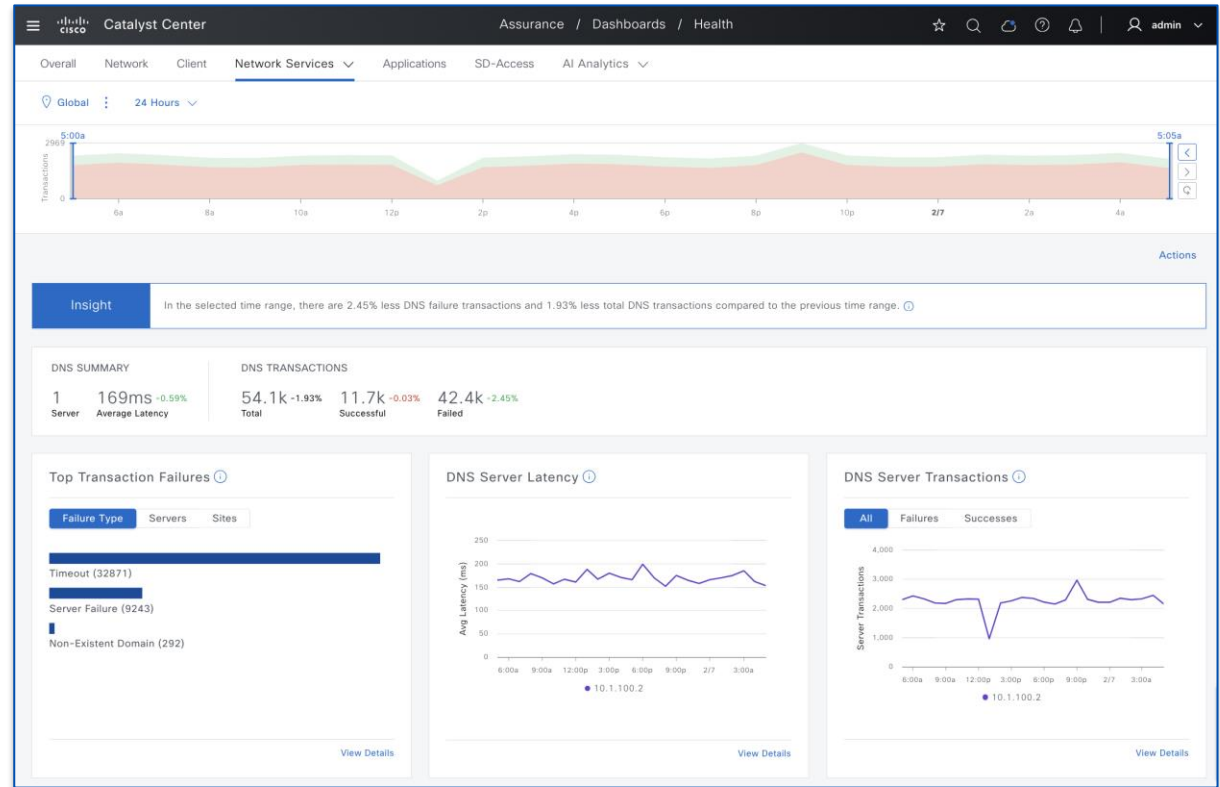
Identifier	Endpoint	Client Health	App Health	Usage	Device Type	MAC Address	VLAN ID
hr1	100.100.0.21	10	--	5.8GB	Wired	00:0C:29:8C:C6:81	1024

- Client level Application usage visibility

Application Telemetry from Switches - DNS

DNS Health Visibility

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



Application Telemetry from Access Switches

Deployment Considerations

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

Switch Application Telemetry Deployment

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

Click on Pencil icon to change role under Inventory

The screenshot shows the Cisco Catalyst Center interface for managing network devices. The page title is 'Provision / Inventory'. Below the navigation bar, there are filters for 'Global' and device types: 'All', 'Routers', 'Switches', 'Wireless Controllers', 'Access Points', and 'Sensors'. The main content area shows a list of 3 devices. The table columns are: Device Name, IP Address, Manageability, Device Role, Application Telemetry, and Compliance. The 'Device Role' column is highlighted with a red box, and a red arrow points from the text 'Click on Pencil icon to change role under Inventory' to a pencil icon in the 'ACCESS' role cell for the 'Edge-L' device.

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

Switch Application Telemetry Deployment

Catalyst Center 2.3.5.x and below

- Initiate Application Telemetry via Provision -> Inventory

The screenshot shows the Cisco Catalyst Center interface. At the top, the navigation bar includes the Cisco logo, the text 'Catalyst Center', and a highlighted 'Provision / Inventory' tab. Below the navigation bar, there is a warning message and an information message. The main content area shows a list of devices under the 'Provision / Inventory' view. The 'Devices (4)' section is active, and three devices are selected: 'Edge-R', 'Edge-L', and 'C9800-CL'. A red box highlights the 'Actions' menu for the selected devices, which is open, showing options like 'Inventory', 'Software Image', 'Provision', 'Telemetry', 'Device Replacement', 'Compliance', and 'More'. The 'Telemetry' option is highlighted with a red box, and a sub-menu is open, showing 'Enable Application Telemetry', 'Disable Application Telemetry', and 'Update Telemetry Settings'. The 'Enable Application Telemetry' option is also highlighted with a red box. The table below shows the details for the selected devices, including their names, manageability status, device roles, and application telemetry status.

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



Switch Application Telemetry Deployment

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

flow record 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
```



Switch Application Telemetry Deployment

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

flow exporter dnacexporter

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

IPFIX format required
for DNS flow export

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
```

Lo0 source interface if SDA fabric node;
uplink interface otherwise



Switch Application Telemetry Deployment

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

interface GigabitEthernet1/0/1

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

interface GigabitEthernet1/1/2

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

keyword “lan” can be manually added to the interface description to forcefully apply NetFlow monitor to an interface not configured with “switchport mode access”; CAUTION: interfaces w/o “lan” keyword will NOT get NetFlow monitor applied, that otherwise would automatically



Switch Application Telemetry Deployment

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

flow record dnarecord_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 dnarecord_dns_v6

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

Switch Application Telemetry Deployment

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

flow exporter dnacexporter

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

flow monitor dnacmonitor_v6

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

flow monitor dnacmonitor_dns_v6

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

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



Switch Application Telemetry Deployment

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

interface GigabitEthernet1/0/1

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

interface GigabitEthernet1/1/2

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

Application **Visibility** from Access Switches

- NBAR (Network-Based Application Recognition)
 - Application classification using deep packet inspection; 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)
 - Application classification info exported via **IPFIX**
- Supported for Software Defined Access (SDA) fabric or non-fabric
- Switches must be activated with DNA-Advantage licenses
- Works in conjunction with Application QoS Policy to push configs for proper queuing policies for specified apps to network infrastructure

Switch Application Visibility Deployment

Catalyst Center 2.3.5.x and below

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

The screenshot displays the Cisco DNA Center interface for configuring Application Visibility. The breadcrumb trail is "Provision / Services / Application Visibility". The page title is "Service Catalog / Application Visibility". The "Setup" section shows three steps: "Enable CBAR" (completed), "Enable Services On devices" (current step), and "Connect External Sources".

The main content area is titled "Select the devices on which you like to enable the CBAR or check below to enable all ready devices". It includes a "Device Family" filter set to "All" and "Switches" selected. The "CBAR Readiness" filter is set to "All".

The "Site Devices (3)" table is as follows:

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

At the bottom right, there are "Skip" and "Next" buttons. The "Next" button is highlighted with a red box.

Switch Application **Visibility** Deployment

Catalyst Center 2.3.5.x and below

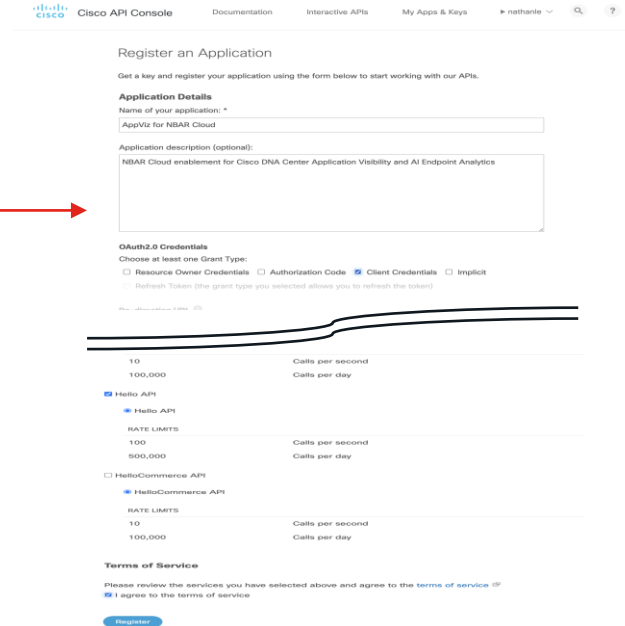
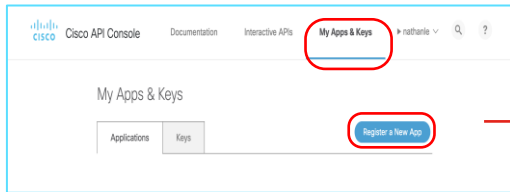
- Enhanced app classification and dynamic Protocol Pack updates through **NBAR Cloud**

The screenshot displays the Cisco DNA Center interface for configuring NBAR Cloud. The main window is titled "Configure NBAR Cloud" and is divided into two panes. The left pane shows the "Setup" section with three steps: "Enable CBAR", "Enable Services On devices", and "Connect External Sources". Below this, there is a section for "Configure the external sources" with a note: "Note! Applications that have been discovered through authoritative sources will be supported only". Three external sources are listed: "NBAR Cloud" (status: Disabled), "MS Office 365 Cloud" (status: Enabled), and "Infoblox DNS S" (status: Enabled). A red box highlights the "Configure" button for NBAR Cloud, with a red arrow pointing to the right pane. The right pane is the "Configure NBAR Cloud" dialog, which has a "Enable" checkbox checked. It includes fields for "Client ID*", "Client Secret*", and "Organization Name*". There are two checked options: "Enable Protocol Pack Auto Update" and "Improve my network using NBAR Cloud telemetry". A dropdown menu for "NBAR classification telemetry data is being sent to region" is set to "USA". At the bottom of the dialog are "Cancel" and "Save" buttons.

Switch Application **Visibility** Deployment

Catalyst Center 2.3.5.x and below

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



Switch Application **Visibility** Deployment Catalyst Center 2.3.5.x and below

- Input obtained credential to enable NBAR Cloud

My Apps & Keys

Applications Keys Register a New App

AppViz for NBAR Cloud

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

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

API	KEY	CLIENT SECRET	STATUS
Hello API	jprjtap976b4hjyx5vqxqrm	G4tvZNsCSmGMtrrdmdjFhvp6	active

Edit This App Delete This App Add APIs

API Console Portal

Configure NBAR Cloud

Enable

Enter Client ID and Client Secret retrieved from Cisco API Console

Client ID*
jprjtap976b

Client Secret*
G4tvZNsCSmGMtrrdmdjFhvp6

Organization Name*
Cisco

Enable Protocol Pack Auto Update

Improve my network using NBAR Cloud telemetry

NBAR classification telemetry data is being sent to region
USA

Cancel Save

Catalyst Center

Switch Application **Visibility** Deployment

- NBAR/CBAR **configuration** pushed to Switches

```
platform wdvavc serviceability
```

```
avc sd-service
```

```
segment AppRecognition
```

```
controller
```

```
address <Catalyst Center IPv4/IPv6 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

Lo0 source interface if SDA fabric node; uplink interface otherwise

Transport method (http vs https) to Catalyst Center for protocol pack updates

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

Switch Application **Visibility** Deployment

- NBAR/CBAR **verification** on Switches

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

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

```
Name:                Advanced Protocol Pack
Version:             66.0
Publisher:           Cisco Systems Inc.
NBAR Engine Version: 49
State:               Active
```

} IOS-XE native protocol pack

```
Name:                Secondary Protocol Pack
Version:             00a45f9ef24653692385f5bf72cb
Publisher:           SD-AVC
NBAR Engine Version: 1001
Creation time:       Tue Jan 30 20:44:55 UTC 2024
NBAR PP level:       1
File:                flash:/sdavc/PPDK_AppRecognition_00a45f9ef24653692385f5bf72cb.pack
State:               Active
```

} CBAR installed protocol pack

Switch Application **Visibility** Deployment

- NBAR/CBAR verification on Switches

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

```
Status: CONNECTED
```

```
Device ID: Edge-C9300-R-E1.cisco.local
```

```
Device segment name: AppRecognition
```

```
Device address: 100.124.126.132
```

```
Device OS version: 17.12.02
```

```
Device type: C9300-48U
```

```
Active controller:
```

```
Type : Primary
```

```
IP : 100.64.0.101
```

```
Status: Connected
```

```
Version : 4.5.0
```

```
Last connection: 00:35:17.000 UTC Fri Feb 2 2024
```

```
Active SDAVC import files:
```

```
Protocol pack: Not loaded
```

```
Secondary protocol pack:
```

```
PPDK AppRecognition 00a45fbe9ef24653692385f5bf72cb.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: 17.12.02
```

```
Device type: C9300-48U
```

```
Active controller:
```

```
Type : Primary
```

```
Address : 100.64.0.101
```

```
Status : Connected
```

```
Version : 4.5.0
```

```
Last connection: 00:38:13.000 UTC Fri Feb 2 2024
```

```
Active SDAVC import files:
```

```
Protocol pack: Not loaded
```

```
Secondary protocol pack:
```

```
PPDK AppRecognition 00a45fbe9ef24653692385f5bf72cb.pack
```

```
Rules pack:
```

```
pp_update_AppRecognition_a_v2_0f687ddbc41d.pack
```

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
```

Protocol	Input	Output
	-----	-----
	Packet Count	Packet Count
	Byte Count	Byte Count
	5min Bit Rate (bps)	5min Bit Rate (bps)
	5min Max Bit Rate (bps)	5min Max Bit Rate (bps)

ms-services	3915973	9324733
	261709271	11022843082
	3000	3000
	1649000	68846000
ssh	2030585	703017
	3068521966	53667192
	65800000	1175000
	65800000	1175000
google-services	1048736	2242508
	68295263	2290752005
	0	0
	486000	15529000
unknown	28192	79902
	1947180	103014893
	0	0

Applications – Application Telemetry and CBAR

Catalyst Center 2.3.7.x and above

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

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**

The screenshot shows the Cisco Catalyst Center interface for configuring Application Telemetry. The breadcrumb navigation is **Services / Service Catalog / Application Visibility**. The page title is **Network Devices Enablement**, showing 1479 Applications, 28 Application Sets, and CBAR Extensions. The page is updated at 11:55 pm.

The interface includes a search hierarchy on the left, a filter section with **Application Telemetry** selected, and a table of devices. The table has columns for Device name, IP address, Recognition method, CBAR Deployment Status, and Application Telemetry Deployment Status. The 'Edge-L' and 'Edge-R' rows are selected, and the 'Application Telemetry' dropdown menu is open, showing **Enable Application Telemetry** and **Disable Application Telemetry** options.

Device name	IP Address	Recognition method	CBAR Deployment Status	Application Telemetry Deployment Status
Border.cisco.local		Network-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

Switch Application Visibility Deployment

Catalyst Center 2.3.7.x and above

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

The screenshot displays the Cisco Catalyst Center interface for configuring Application Visibility Setup. The main view is titled 'Enable CBAR' and is focused on the 'Edge-L' device. The interface shows a list of interfaces with their corresponding status (enabled/disabled) via toggle switches.

Enable CBAR Configuration:

Interfaces	Status
GigabitEthernet2/0/9	Enabled
GigabitEthernet2/0/8	Enabled
GigabitEthernet2/0/7	Enabled
GigabitEthernet2/0/6	Enabled
GigabitEthernet2/0/5	Enabled
GigabitEthernet2/0/4	Enabled
GigabitEthernet2/0/3	Enabled
GigabitEthernet2/0/2	Enabled

Showing 20 of 62 [Show more](#)

Device List (Left Panel):

Device name	Management IP	Active recognition
<input type="checkbox"/> Border.cisco.local	100.124.0.1	Network-based
<input type="checkbox"/> C9800-CL.cisco.local	100.126.0.6	Network-based
<input checked="" type="checkbox"/> Edge-L	100.124.126.134	Network-based
<input checked="" type="checkbox"/> Edge-R	100.124.126.129	Network-based

Applications – Application Telemetry and CBAR

Catalyst Center 2.3.7.x and above

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

The screenshot displays the Catalyst Center interface for Application Visibility Setup. The breadcrumb trail is Services / Service Catalog / Application Visibility Setup. The page title is Service Catalog / Application Visibility Setup. The navigation tabs include Overview, Network Devices Enablement, 1479 Applications, 28 Application Sets, and CBAR Extensions (highlighted with a red box). The main content area shows the CBAR Cloud configuration. A red box highlights the 'CBAR Cloud' tab, and another red box highlights the 'Enable' toggle switch, which is currently turned on. Below the toggle, there is a section for 'CBAR Dynamic Application Feeds' with an 'Enable Application Feeds Update' option set to 'All'. A grid of application cards is displayed, each with a chevron icon, the application name, and the number of applications. The applications listed are: Telegram (1), Google Meet (1), ServiceNow (1), Sugarcrm (1), SAP (1), HubSpot (1), RingCentral (1), Github (1), Crashplan (1), O365 (15), Intuit (1), Box (1), Workday (1), Zscaler (1), Microsoft Intune (1), Atlassian (2), Code42 (1), and Amazon Chime (2). At the bottom right, there are 'Reset' and 'Apply' buttons.

Applications – Application Telemetry and CBAR

Catalyst Center 2.3.7.x and above

- New protocol pack classification differences may affect current QoS policies

Service Catalog / Application Visibility Setup

Overview Network Devices Enablement 1479 Applications 28 Application Sets CBAR Extensions

CBAR Health Issues and Remedies

P1 0 Issues P2 0 Issues P3 1 Issues

Device Protocol Pack outdated [Show devices](#)

Site Devices (4)

Device Family: All Routers Switches Wireless Controllers Telemetry Appliance

CBAR Readiness: All Ready Not ready Enabled

Telemetry Readiness: All Ready Not ready Enabled

Filter: CBAR Application Telemetry Update Protocol Pack

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

Showing 4 of 4 [Show more](#)

Warning

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

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

No Yes

Application Telemetry and Visibility for Wireless

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

Application Telemetry and Visibility Deployment for Wireless

Catalyst Center 2.3.7.x and above

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

Service Catalog / Application Visibility

Provision / Services / Application Visibility

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

Dev	IP	Active recognition method	CBAR Deployment Status	Application Telemetry Deployment Status
<input type="checkbox"/>	Bo	Network-based (NBAR)	Not deployed	Not deployed
<input type="checkbox"/>	Bo	Network-based (NBAR)	Not deployed	Not deployed
<input checked="" type="checkbox"/>	C9800-CL.cisco.local	100.126.0.6	Network-based (NBAR)	Not deployed
<input type="checkbox"/>	Cat3650-Old.cisco.local	100.124.127.36	IP/Port	Not deployed

Application Telemetry and Visibility Deployment for Wireless

Catalyst Center 2.3.7.x and above

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


Enable Application Telemetry


By default, all access interfaces on a switch OR all LAN-facing interfaces on a router will be provisioned to send Netflow with Application telemetry.
To override this default behavior, tag specific interfaces to be designated as LAN interface, by putting the keyword "lan" in the interface description.
Once specific interfaces are tagged only those interfaces will be monitored.

By default, all non-guest WLANs on Wireless Controllers will be provisioned to send Netflow with Application telemetry.
To override this default behavior, tag specific WLAN profile names with keyword "lan".
Once specific WLANs are tagged, only those WLANs will be monitored.

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


For Catalyst 9800 Series Wireless Controllers, the application telemetry source is always Netflow.
For AireOS wireless controllers, the application telemetry source may be either Netflow or WSA (Wireless Service Assurance).

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

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

C9800-CL.cisco.local

Local Flex/Fabric

Include Guest SSIDs 

Telemetry Source: **NetFlow**

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

Cancel Enable

Application Telemetry and Visibility Deployment for Wireless

Catalyst Center 2.3.7.x and above

- Specify **SSID type** to enable **CBAR**

Enable CBAR

You have chosen to enable CBAR on 1 wireless controllers.

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

AP provisioning is required for Enabling CBAR in wireless modes.

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

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

C9800.cisco.local

Local Flex Fabric

Wireless Application Telemetry Deployment

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

flow exporter avc_exporter

```
destination <Catalyst Center IPv4 Address>
source <Source-Interface>
transport udp 6007
export-protocol ipfix
option vrf-table timeout 300
option ssid-table timeout 300
option application-table timeout 300
option application-attributes timeout 300
```

flow exporter avc_local_exporter

```
destination local wlc
```

flow exporter avc_exporter_v9

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

Wireless Application Telemetry Deployment

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

```
flow monitor avc_ipv4_assurance
```

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

```
flow monitor avc_ipv4_assurance_rtp
```

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

```
flow monitor avc_ipv4_assurance_v9
```

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

```
flow monitor avc_ipv4_assurance_rtp_v9
```

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

```
flow monitor avc_ipv4_assurance_dns
```

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

Built-in Flow Records

```
flow monitor avc_ipv6_assurance
```

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

```
flow monitor avc_ipv6_assurance_rtp
```

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

```
flow monitor avc_ipv6_assurance_v9
```

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

```
flow monitor avc_ipv6_assurance_rtp_v9
```

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

```
flow monitor avc_ipv6_assurance_dns
```

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

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

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

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

Wireless Application Telemetry Deployment

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

flow monitor avc_ipv4_assurance

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

flow monitor avc_ipv4_assurance_rtp

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

flow monitor avc_ipv4_assurance_v9

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

flow monitor avc_ipv4_assurance_rtp_v9

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

flow monitor avc_ipv4_assurance_dns

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

flow monitor avc_ipv6_assurance

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

flow monitor avc_ipv6_assurance_rtp

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

flow monitor avc_ipv6_assurance_v9

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

flow monitor avc_ipv6_assurance_rtp_v9

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

flow monitor avc_ipv6_assurance_dns

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

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

wireless profile policy <POLICY-NAME>

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

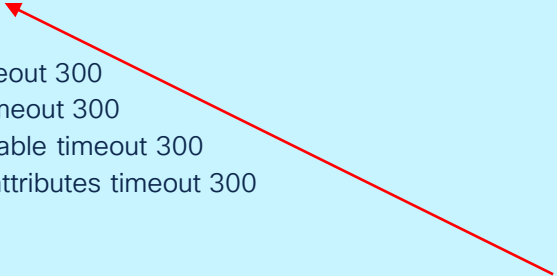
Wireless Application Telemetry Deployment

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

flow exporter avc_exporter_v9

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

Source is Loopback0 for
embedded wireless
controller on C9300/C9400



Wireless Application Telemetry Deployment

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

```
flow monitor avc_ipv4_assurance_v9
exporter avc_exporter_v9
cache timeout active 60
record wireless avc ipv4 assurance
```

```
flow monitor avc_ipv4_assurance_rtp_v9
exporter avc_exporter_v9
cache timeout active 60
record wireless avc ipv4 assurance-rtp
```

```
flow monitor avc_ipv6_assurance_v9
exporter avc_exporter_v9
cache timeout active 60
record wireless avc ipv6 assurance
```

```
flow monitor avc_ipv6_assurance_rtp_v9
exporter avc_exporter_v9
cache timeout active 60
record wireless avc ipv6 assurance-rtp
```

```
wireless profile policy <POLICY-NAME>
  ipv4 flow monitor avc_ipv4_assurance_v9 input
  ipv4 flow monitor avc_ipv4_assurance_rtp_v9 input
  ipv4 flow monitor avc_ipv4_assurance_v9 output
  ipv4 flow monitor avc_ipv4_assurance_rtp_v9 output
  ipv6 flow monitor avc_ipv6_assurance_v9 input
  ipv6 flow monitor avc_ipv6_assurance_rtp_v9 input
  ipv6 flow monitor avc_ipv6_assurance_v9 output
  ipv6 flow monitor avc_ipv6_assurance_rtp_v9 output
```



SDA export in FNFv9
format; no DNS Health
Visibility

Wireless Application **Visibility** Deployment

- **NBAR/CBAR** configuration pushed to Wireless Controllers

avc sd-service

```
segment AppRecognition
controller
address <Catalyst Center IPv4/IPv6 address>
destination-ports sensor-exporter 21730
dscp 16
source-interface <Source-Interface>
transport application-updates https url-prefix sdavc
```

wireless profile policy <POLICY-NAME>

```
ip nbar protocol-discovery
```

NBAR command applies to wireless profile policy for each SSID

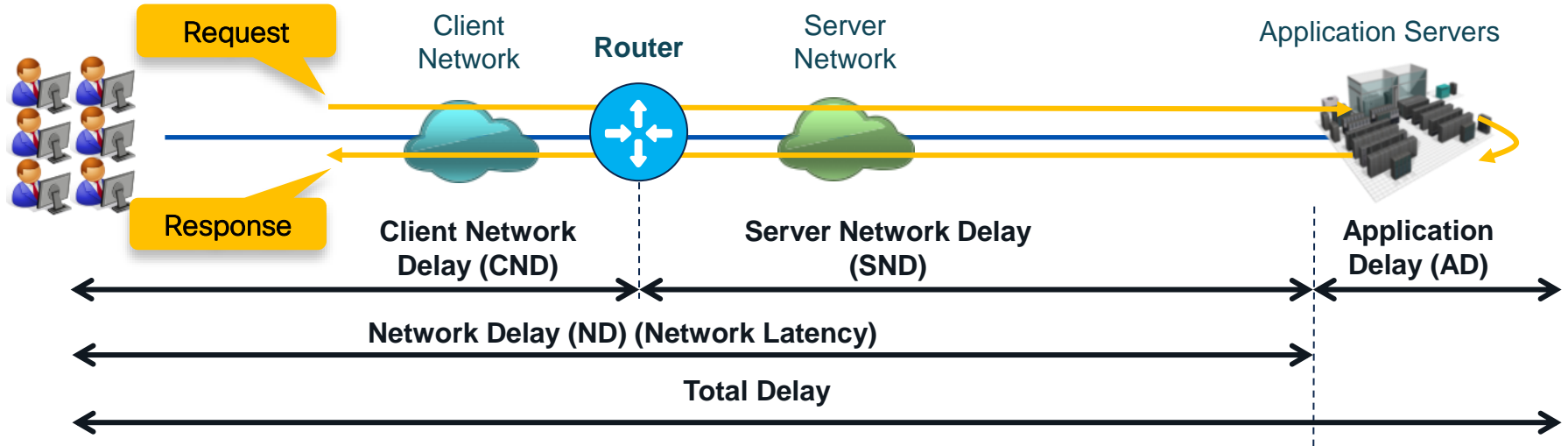


Application Telemetry and Visibility from Routers

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

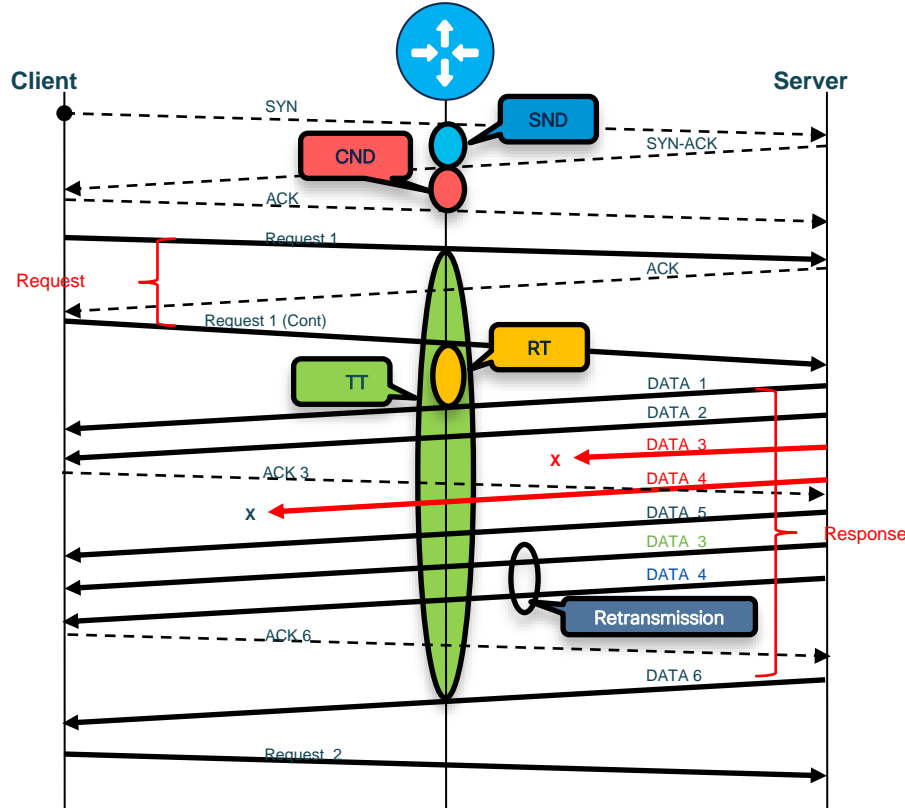
Application Telemetry and Visibility from Routers

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



Application Telemetry and Visibility from Routers

- Application Response Time calculation for TCP traffic



Network Delay
(ND, Latency)

$$ND = CND + SND$$

Response
Time (RT)

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

Transaction
Time (TT)

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

Application
Delay (AD)

$$AD = RT - SND$$

Retransmission

Loss

Application Telemetry from Routers

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

Media Monitoring

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

Application Response Time

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

Other Metrics

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

Latency, Application Delay, and Loss values shown on Catalyst Center Application Assurance

Application Telemetry and Visibility Deployment for Routers

Catalyst Center 2.3.7.x and above

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

The screenshot displays the Cisco Catalyst Center Provisioning interface. The main navigation bar shows 'Provision / Services / Application Visibility'. The left sidebar contains a search hierarchy for 'Global' and 'Bay Area'. The central pane is titled 'Network Devices Enablement' and shows a list of 'Site Devices (6)'. The 'Device Family' is set to 'Routers' and the 'Active Recognition Method' is 'CBAR'. A filter is applied to 'Application Telemetry'. The device list includes 'Border-C8300', 'Border.cisco.local', 'C9800-CL.cisco.local', and 'Cat3650-Old.cisco.local'. A modal window titled 'Enable Application Telemetry' is open, showing instructions for enabling NetFlow with application telemetry on 1 router. The modal includes a table of devices and an 'Enable' button.

Enable Application Telemetry

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

By default, all access interfaces on a switch OR all LAN-facing interfaces on a router will be provisioned to send Netflow with Application telemetry.
To override this default behavior, tag specific interfaces to be designated as LAN interface, by putting the keyword "lan" in the interface description.
Once specific interfaces are tagged only those interfaces will be monitored.

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

Device name	IP Address
<input type="checkbox"/> Border-C8300	
<input type="checkbox"/> Border.cisco.local	100.124.0.1
<input type="checkbox"/> C9800-CL.cisco.local	100.126.0.6
<input type="checkbox"/> Cat3650-Old.cisco.local	100.124.127.36

Cancel **Enable**

Application Telemetry and Visibility Deployment for Routers

Catalyst Center 2.3.7.x and above

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

The screenshot shows the Catalyst Center interface for Application Visibility. The 'Network Devices Enablement' tab is active, displaying a table of devices. The 'CBAR Readiness Status' column for the 'Border-C8300' device is highlighted with a green box and contains the text 'Not ready WAN Interfaces'. A red box highlights this text, with a red arrow pointing to the 'WAN Connectivity Settings' dialog box on the right.

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

The screenshot shows the 'WAN Connectivity Settings for Device Border-C8300' dialog box. The 'Add Row' button is highlighted with a red box. Below it, a table lists WAN interfaces. The first row is highlighted with a red box, showing 'GigabitEthernet0/0/0' selected for the interface and 'WAN' selected for the role.

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

Router Application Telemetry Deployment

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

performance monitor context tesseract profile application-assurance

```
exporter destination <Catalyst Center IPv4/IPv6 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
```

Lo0 source interface if SDA fabric node;
uplink interface otherwise

When keyword "LAN" is used, interfaces w/o keyword
would NOT get App Telemetry configuration (that otherwise
would have automatically been configured)

Router Application Telemetry Deployment

- NetFlow verification – cache

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

Router Application Telemetry Deployment

- NetFlow verification – export (1)

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

Router Application Telemetry Deployment

- NetFlow verification – export (2)

```
Client send statistics:
```

```
Client: Option options interface-table
```

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

```
Client: Option options application-name
```

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

```
Client: Flow Monitor tesseract-app_assurance_ipv4
```

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


Router Application **Visibility** Deployment

- NBAR/CBAR configuration pushed to Routers

avc sd-service

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

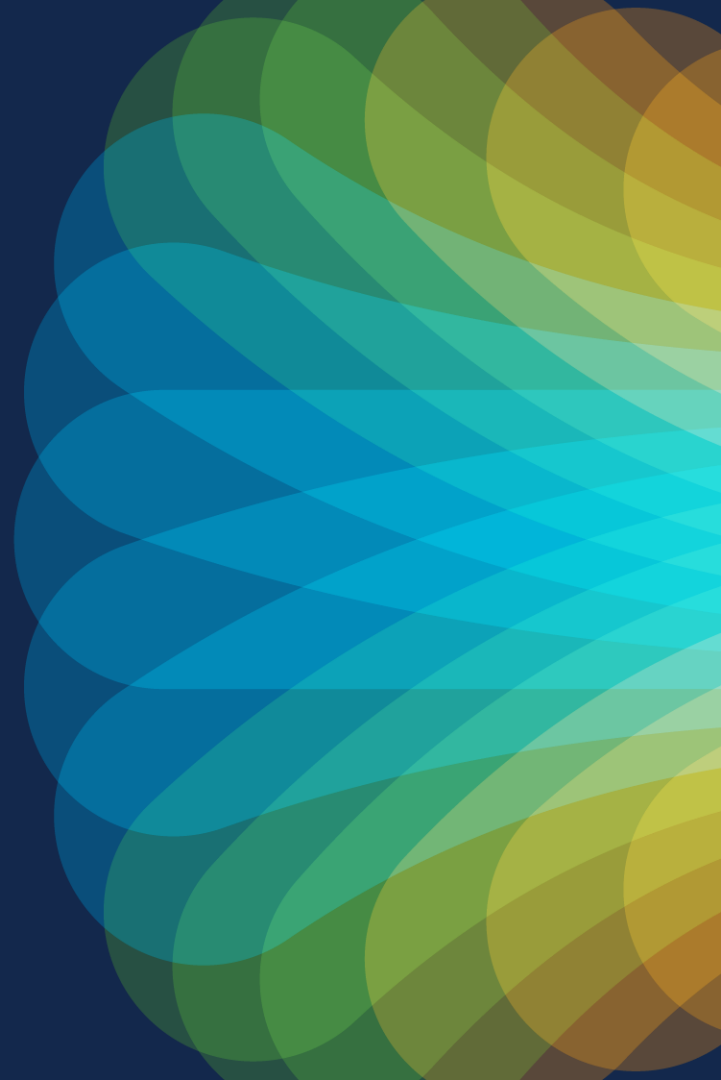
Lo0 source interface if SDA fabric node;
uplink interface otherwise

interface GigabitEthernet0/0/0

```
ip nbar protocol-discovery
```

NBAR command pushed to specified "WAN" interface

StealthWatch



StealthWatch with Catalyst Center

Deployment Considerations

- Secure Network Analytics (StealthWatch) focuses on security monitoring using NetFlow export
- Catalyst Center integration with SNA Management Console
 - Encrypted Traffic Analytics (ETA) and **wired NetFlow** config can coexist on same interface post IOS-XE 17.3
 - Cannot enable “FNF” mode on SSA (StealthWatch Security Analytics) application if **Application Telemetry** already enabled on device
- Catalyst Center integration with Cisco Telemetry Broker (CTB, formerly StealthWatch UDPD)
 - Integration with CTB is **independent** of integration with SNA
 - Identical NetFlow configuration for App Telemetry but with CTB as destination
 - Multiple forwarding rules configured through SNA Management Console
- **Flow exporter** source interface (IP address) needs to match between network device and SNA flow exporter configuration → Catalyst Center will add exporters to SNA
- Can use Template or manual CLI as alternative to StealthWatch integration

StealthWatch with Catalyst Center

Integration with **SNA Management Console** through **System → Settings**

The screenshot displays the Catalyst Center interface for configuring Stealthwatch. The breadcrumb trail is 'System / Settings'. The left-hand navigation menu includes 'External Services' (highlighted with a green box), 'Umbrella', 'Authentication and Policy Servers', 'Integrity Verification', 'SD-Access Compatibility Matrix', 'IP Address Manager', 'Cloud Access Login', 'Cisco AI Analytics', 'Stealthwatch' (highlighted with a red box), 'Talos IP Reputation', 'Destinations', 'Cisco Spaces/CMX Servers', 'Catalyst Dashboard', 'Machine Reasoning Engine', and 'Cloud Authentication'. The main content area is titled 'Stealthwatch' and contains the following text: 'Use this page to associate Stealthwatch with Cisco DNA Center. Register a Stealthwatch Management Console with Cisco DNA Center to integrate with Stealthwatch and utilize read-only APIs to retrieve the usable flow destinations for Stealthwatch Security Analytics.' Below this text is a form with the following fields: 'SMC IP Address or FQDN*' (containing '100.64.0.171', highlighted with a red box), 'Username*', and 'Password*'. A warning icon (a triangle with an exclamation mark) is located to the right of the IP address field. Below the IP address field, a message reads: 'Certificate is not trusted for this IP address or FQDN. Please click the warning to learn more.' A modal dialog box is open, displaying the message: 'The certificate associated with this IP address or FQDN is not trusted.' It includes a link for 'Certificate details', a checked radio button for 'Allow Cisco DNA Center to access this IP address or FQDN and add the untrusted certificate to the Trusted Certificates', and an 'Allow' button. Red arrows point from the text 'Click on warning to accept certificate' to the warning icon and the 'Allow' button. Another red arrow points from the text 'Ensure StealthWatch administrator accounts (those beside default “admin”) have logged in and changed password before using for integration (silent failure otherwise)' to the 'Username*' field.

StealthWatch with Catalyst Center

Select SNA **FlowCollector** Destination at **Design** → **Network Settings**

The screenshot shows the Catalyst Center interface for configuring network settings. The breadcrumb path is Design / Network Settings. The left sidebar shows a hierarchy with 'Global' selected. The main content area is titled 'Stealwatch Flow Destination' and includes a description: 'The flow destination set here is used to provision SSA on this site.' There are two radio button options: 'Stealwatch Cloud' and 'Select from flow destinations configured in the Stealwatch'. The second option is selected. Below it is a search dropdown menu with the entry '100.64.0.172:2055 (FLOW_COLLE...' visible. At the bottom right, there are 'Reset' and 'Save' buttons.

StealthWatch with Catalyst Center

Enable Encrypted Traffic Analytics through Provision → StealthWatch Security (1)

The screenshot shows the 'Schedule Deployment' window in the Catalyst Center Provision interface. The window title is 'Bay_Area' and it shows 'Ready (1)', 'Not Ready (0)', and 'Enabled (0)' devices. A table lists the device 'U-Edge-1.cisco.local' with IP '100.124.2.65' and type 'Cisco Catalyst 9300 Switch'. The 'ETA Telemetry' checkbox is checked. The 'Enable' button at the bottom right is highlighted with a red box.

Name	IP Address	Device Type	SSA Status	SWT Status
U-Edge-1.cisco.local	100.124.2.65	Cisco Catalyst 9300 Switch	Disabled	Not Supported

Destination is FlowCollector

```
et-analytics
ip flow-export destination 100.64.0.172 2055

interface GigabitEthernet1/0/1
et-analytics enable
```

ETA is selected by default
→ Compatible with App Telemetry if
IOS-XE is 17.3+

ETA enabled on all access ports
(Configured in addition to App Telemetry FNF)

StealthWatch with Catalyst Center

Enable Encrypted Traffic Analytics through Provision → StealthWatch Security (2)

Screenshot of the Catalyst Center Provision Services page for Stealthwatch Security. The page shows a 'Schedule Deployment' dialog with a table of devices. A red box highlights the 'ETA as default' checkbox, which is currently unchecked. Another red box highlights the 'ETA Telemetry' checkbox, which is checked. A third red box highlights the 'Enable' button at the bottom right. Red arrows point from the 'ETA as default' and 'ETA Telemetry' checkboxes to the 'Enable' button. On the left side of the page, a green circle highlights a '1 Capable Device' in the site hierarchy.

- If ETA is disabled, then StealthWatch “FNF” config mode is attempted
- If App Telemetry is not enabled, then “FNF” mode is success
- Switch added as Flow Exporter on SNA Management Console

flow record SSA-FNF-REC

```
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect timestamp absolute first
collect timestamp absolute last
collect counter bytes long
collect counter packets long
```

flow exporter SSA-FNF-EXP

```
destination 100.64.0.172
transport udp 2055
template data timeout 30
option interface-table
option application-table timeout 10
```

flow monitor SSA-FNF-MON

```
exporter SSA-FNF-EXP
record SSA-FNF-REC
cache timeout active 60
```

interface GigabitEthernet1/0/1

```
ip flow monitor SSA-FNF-MON input
ip flow monitor SSA-FNF-MON output
```

StealthWatch FNF monitor applied to all access ports

StealthWatch with Catalyst Center

Enable Encrypted Traffic Analytics through Provision → StealthWatch Security (3)

The screenshot shows the Catalyst Center Provision Services page for Stealthwatch Security. The 'Schedule Deployment' window is open, showing a table of devices. The 'ETA as default' toggle is disabled, and the 'ETA Telemetry' toggle is enabled. The 'Enable' button is highlighted. A '1 Capable Device' indicator is shown in the left sidebar. Red arrows point from the text box on the right to these elements.

Name	IP Address	Device Type	SSA Status	SWC Status
Edge-1.cisco.local	100.124.2.65	Cisco Catalyst 9300 Switch	Disabled	Not Supported

Switch console:

```
Flow Monitor: Failed to add monitor to interface: wdavc and non-wdavc monitors cannot exist on an interface for same traffic type and direction
```

“wdavc” = wired AVC

- If ETA is disabled, then StealthWatch “FNF” config mode is attempted
- If App Telemetry is enabled, then “FNF” mode is not compatible
- Silent error; need to check task logs on Catalyst Center for details

StealthWatch with Catalyst Center

Setting Cisco Telemetry Broker as NetFlow Collector Under Design → Telemetry

- CTB Setting can be set **with or without** StealthWatch Integration

The screenshot shows the Cisco Catalyst Center interface for configuring Telemetry. The 'Telemetry' tab is selected. The configuration page includes sections for SNMP Traps, Syslogs, and Application Visibility. Under Application Visibility, the 'Enable Netflow Application Telemetry and Controller Based Application Recognition (CBAR) by default upon network device site assignment' is checked. The 'Use Cisco Telemetry Broker (CTB) or UDP director' option is selected, with the IP address '100.64.0.173' and port '2055' specified. A red arrow points from the text 'Configure forwarding rule on UDPD to point to SNA FlowCollector and Catalyst Center' to the selected option. The 'Save' button at the bottom right is also highlighted with a red box.

- Resulting App Telemetry config same as if Catalyst Center was destination
- Configure forwarding rule on UDPD to point to SNA FlowCollector and Catalyst Center

StealthWatch with Catalyst Center

- Access to CTB Configuration under **Configure** → **UDP Director** on Management Console

The screenshot displays the Cisco Network Analytics Management Console interface. At the top, the navigation bar includes the 'Network Analytics' logo, the domain 'cisco.com', and a series of dropdown menus: 'Monitor', 'Investigate', 'Report', and 'Configure'. The 'Configure' menu is highlighted with a red box. Below the navigation bar, the main content area is titled 'Security Insight Dashboard | Inside Hosts'. On the left, there is a section for 'Alarming Hosts' with three metrics: 'Concern Index', 'Target Index', and 'Recon', each showing a value of 0. On the right, a navigation sidebar is visible, divided into two columns: 'DETECTION' and 'GLOBAL'. The 'DETECTION' column lists 'Host Group Management', 'Alarm Severity', 'Policy Management', 'Response Management', 'Network Scanners', 'Analytics', and 'Alerts'. The 'GLOBAL' column lists 'Central Management', 'User Management', 'Manager', 'Packet Analyzer', 'UDP Director', and 'External Lookup'. The 'UDP Director' option is highlighted with a red box.

StealthWatch with Catalyst Center

- Forwarding Rule on UDP Director (1)

The screenshot shows the Cisco Network Analytics interface. At the top, there is a navigation bar with the 'Network Analytics' logo and 'cisco.com' link. Below the navigation bar are tabs for 'Monitor', 'Investigate', 'Report', and 'Configure'. The main content area is titled 'UDP Director Configuration'. Underneath, there is a section for 'UDP Directors' with a table listing the configuration details for a device named 'udpd'. The table has columns for Name, Device IP, Device Model, and Management Channel Status. The 'Actions' column for the 'udpd' row is expanded, showing three options: 'Configure Forwarding Rules', 'Configure High Availability', and 'Export Forwarding Rules'. The 'Configure Forwarding Rules' option is highlighted with a red box, and the 'More' icon (three dots) in the Actions column is also highlighted with a red box.

Name	Device IP	Device Model	Management Channel Status	Actions
udpd	100.64.0.173 ...	UDVE	● ↻	<ul style="list-style-type: none">Configure Forwarding RulesConfigure High AvailabilityExport Forwarding Rules

StealthWatch with Catalyst Center

- Forwarding Rule on UDP Director (2)

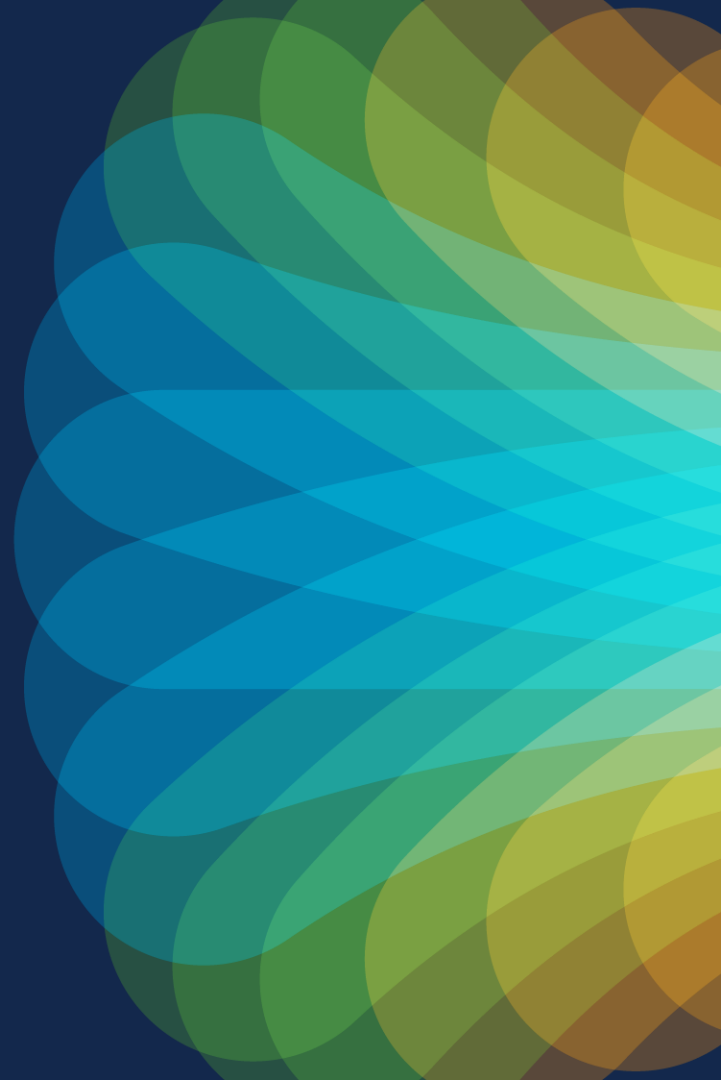
The screenshot shows the Network Analytics interface for Cisco.com. The top navigation bar includes 'Monitor', 'Investigate', 'Report', and 'Configure' menus. The main content area is titled 'Forwarding Rules | udpd - 100.64.0.173'. It features a 'Global Search' input field, a red-bordered 'Add New Rule' button, and an 'Import/Export' dropdown menu. Below these elements is a table with two rows of forwarding rules. The table columns are: Rule, Description, Source IP Address & Port List, Destination IP Address, Destination Port Number, and Actions.

Rule	Description	Source IP Address & Port List	Destination IP Address	Destination Port Number	Actions
1	Edge to Catalyst Center	All:5555	100.64.0.101	2055	...
2	Edge to FlowCollector	All:5555	100.64.0.172	2055	...

NetFlow-Dependent Applications

- AI Endpoint and Trust Analytics
- Group Policy Analytics

AI Endpoint and Trust Analytics



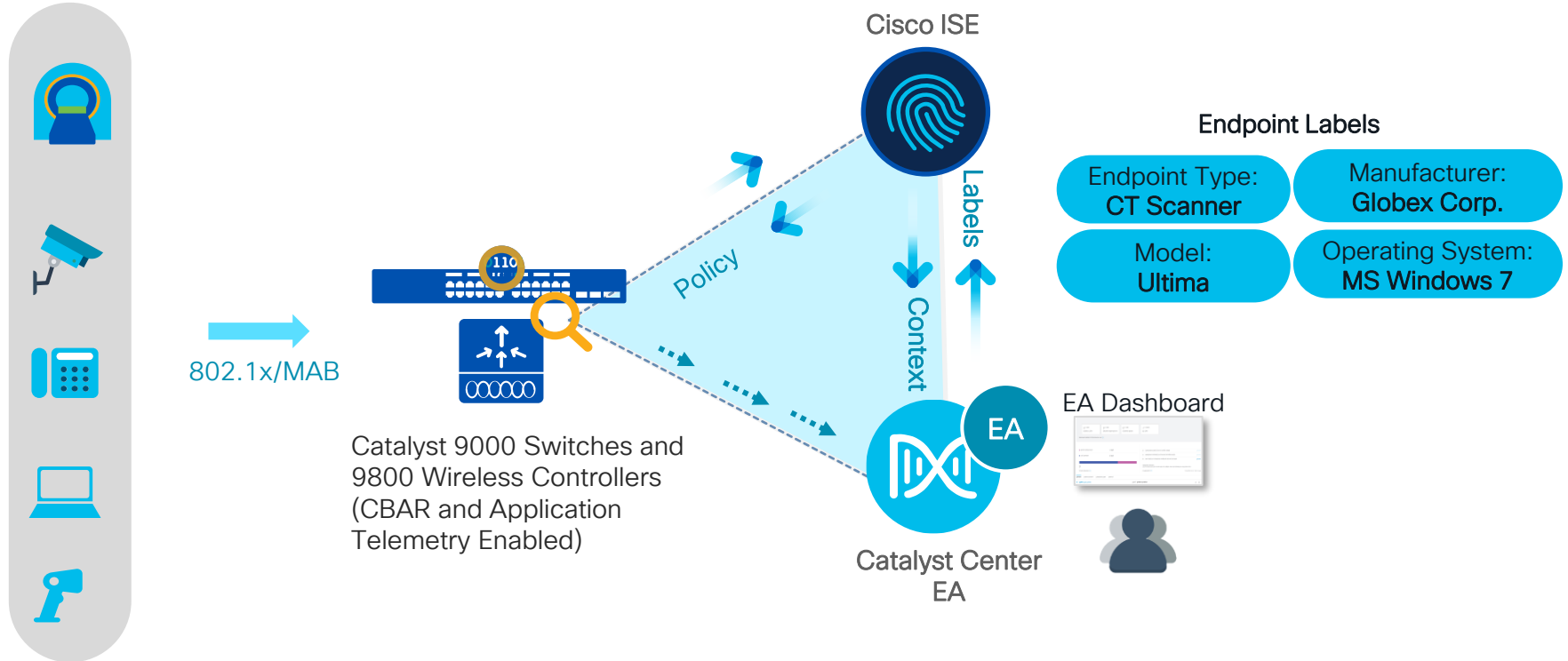
AI Endpoint and Trust Analytics

- 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
- Dynamic Trust Score with continuous monitoring of device behavior
- NetFlow export required for Talos and IP Spoof Detection

Proper workflow leads to proper NetFlow,
allowing for completeness of solution!

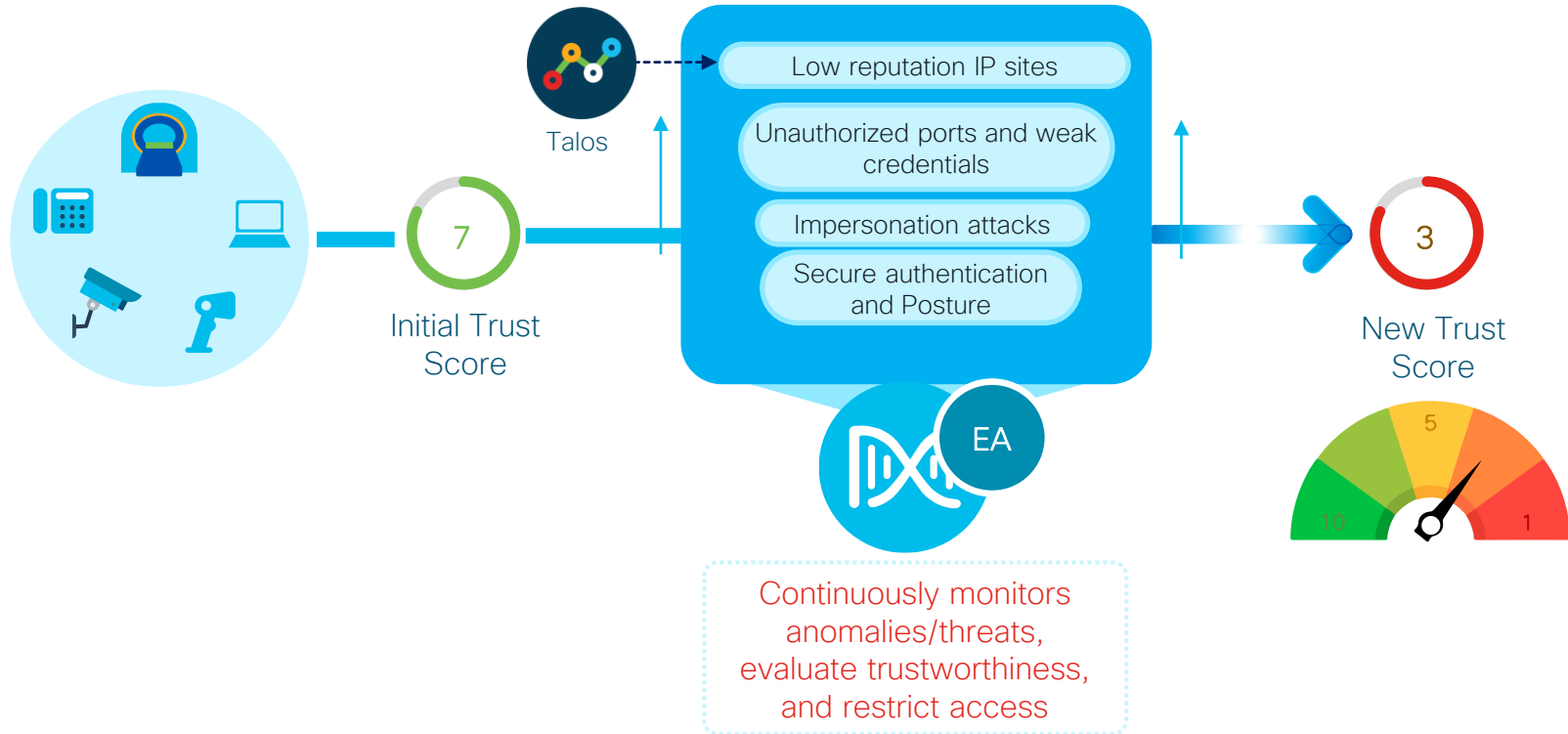
AI Endpoint and Trust Analytics

- Endpoint profiling via CBAR and Application Telemetry



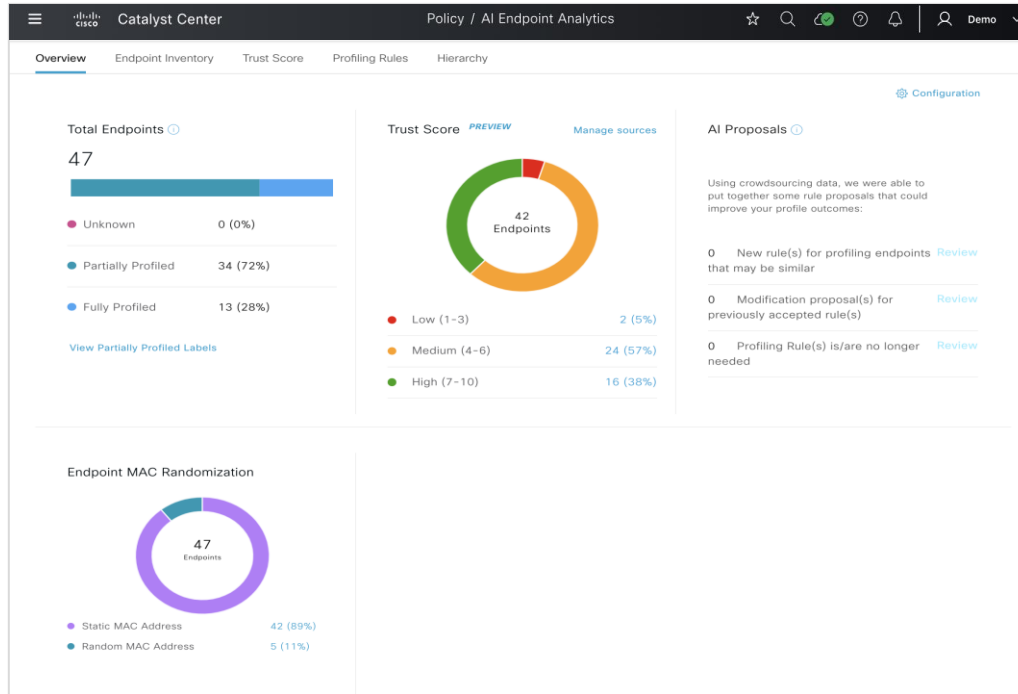
AI Endpoint and Trust Analytics

- Continuous validation of endpoints for Trusted Access



AI Endpoint and Trust Analytics

- EA Dashboard



AI Endpoint and Trust Analytics

- Endpoint Inventory

The screenshot displays the Cisco Catalyst Center interface for AI Endpoint Analytics. The main heading is "Endpoint Inventory (47)" with a focus on "All Endpoints - Default View". A search bar is present above the table. The table lists various endpoints with their respective trust scores and details.

MAC Address	Is Random MAC	Trust Score	IP Address	Last Seen	Hostname	Endpoint Type	OS Type	Hardware Model	Hardware Manufacturer
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 International
5A:00:20:99:77:2F	Yes	9	10.1.10.201	Jun 30, 2022 09:59 PM	-	Mobile Device	iOS 15.6	Apple-Device	Apple, Inc.

AI Endpoint and Trust Analytics

- Trust Scores and Remediation through Adaptive Network Control via ISE

The screenshot displays the 'Policy / AI Endpoint Analytics' interface. At the top, there are navigation icons for search, refresh, and notifications. Below the header, there are tabs for 'Details', 'Trust Score', and 'Attributes'. The 'Trust Score' tab is active, showing a total score of 5 with a yellow indicator. The interface is divided into two main sections: 'Endpoint Authentication and Compliance' and 'Endpoint Anomaly Detection'. Under 'Endpoint Authentication and Compliance', there are two items: 'Authentication Method' and 'Posture', both marked as 'Not Detected'. Under 'Endpoint Anomaly Detection', there are seven items: 'AI Spoofing Detection' (Not Detected), 'Changed Profile Labels' (Not Detected), 'Concurrent MAC Address' (Not Detected), 'NAT Mode Detection' (Not Detected), 'Talos IP Reputation' (Globally Disabled), 'Unauthorized Ports' (Detected with a red dot and 'Last Scored: Jun 12, 2022 11:56 PM'), and 'Credential Vulnerability' (Not Detected). At the bottom of the interface, there are two buttons: 'Reset Trust Score' and 'Apply ANC Policy', which is highlighted with a red box.

AI Endpoint and Trust Analytics Deployment

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

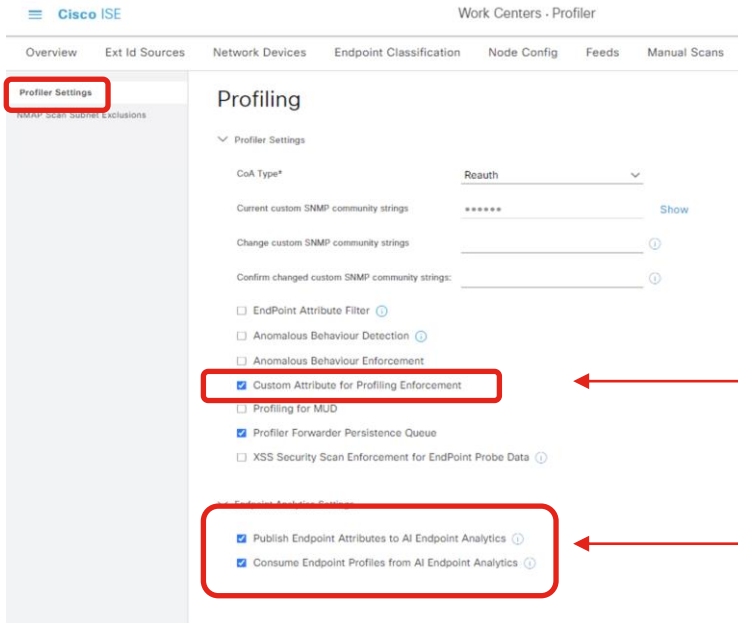
The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration - System'. Below this, a menu bar contains 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The 'Deployment' section is expanded, showing 'Deployment' and 'PAN Failover'. The 'Edit Node' page is displayed, with the 'Profiling Configuration' tab selected and highlighted by a red box. A red arrow points from the text 'Profiling Configuration' to this tab. Below the tab, various services are listed with toggle switches: NETFLOW (disabled), DHCP (enabled), DHCPSPAN (disabled), HTTP (disabled), RADIUS (enabled), Network Scan (NMAP) (enabled), DNS (disabled), SNMPQUERY (enabled), SNMPTRAP (disabled), and Active Directory (enabled). At the bottom, the 'pxGrid' toggle switch is also highlighted with a red box, and a red arrow points from the text 'Enable pxGrid, then Save' to it.

Profiling Configuration

Enable pxGrid, then Save

AI Endpoint and Trust Analytics Deployment

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



The screenshot shows the Cisco ISE interface for the 'Work Centers - Profiler' section. The 'Profiler Settings' tab is selected and highlighted with a red box. The 'Profiling' section is expanded, showing various settings. Two settings are highlighted with red boxes and arrows pointing to explanatory text:

- Custom Attribute for Profiling Enforcement
- Publish Endpoint Attributes to AI Endpoint Analytics
- Consume Endpoint Profiles from AI Endpoint Analytics

Enable Custom Attribute for Profiling Enforcement

Enable Publishing and Consumption of endpoint attributes, then Save

AI Endpoint and Trust Analytics Deployment

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

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

IP Address	Protocol	Type	Status
10.172.3.100	RADIUS_TACACS	ISE	ACTIVE

AI Endpoint and Trust Analytics Deployment



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

Catalyst Center System / Settings

Settings / External Services

Authentication and Policy Servers

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

Add **Export**

Protocol	Type	Status
AAA		
ISE		No data to display

Add ISE server

Server IP Address*
10.172.3.100

Shared Secret*
.....

Username*
iseadmin

Password*
.....

FQDN*
ise.cisco.local

Virtual IP Address(es)

Advanced Settings

Connect to pxGrid

Enable Multiple Cisco DNA Center operation

Use Cisco DNA Center Certificate for pxGrid

Protocol
 RADIUS TACACS

Enable KeyWrap
Authentication Port*
1812

Cancel **Add**

Global RADIUS shared secret to be provisioned to new devices

ISE WebUI admin credential (need not match SSH password)

FQDN MUST match that on ISE admin settings page

Address for any load balancer used in front of ISE clusters

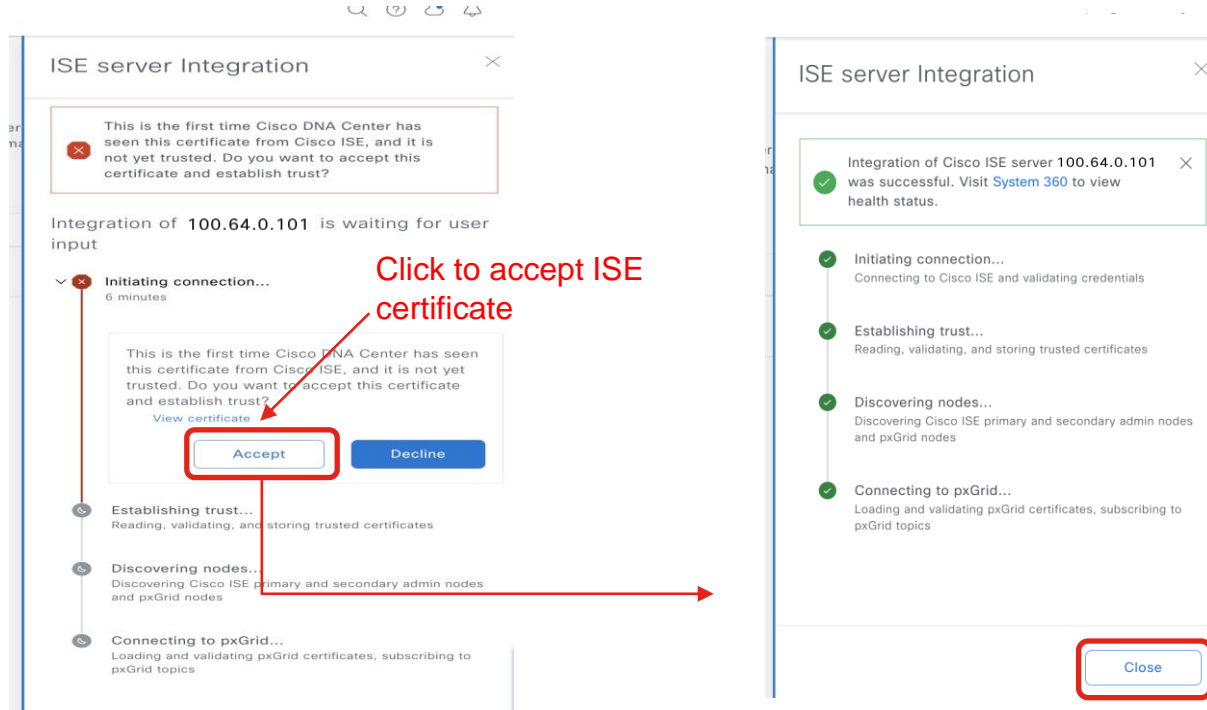
pxGrid required for SDA and EA

TACACS not selected by default

Only one instance of ISE can be added

AI Endpoint and Trust Analytics Deployment

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



The image displays two sequential screenshots of the 'ISE server Integration' dialog box in Cisco Catalyst Center.

Left Screenshot: The dialog box is titled 'ISE server Integration'. It contains a warning message: 'This is the first time Cisco DNA Center has seen this certificate from Cisco ISE, and it is not yet trusted. Do you want to accept this certificate and establish trust?'. Below this message, it states 'Integration of 100.64.0.101 is waiting for user input'. A progress indicator shows 'Initiating connection...' with a red 'x' icon and a 6-minute timer. Below the progress indicator, there is another identical warning message. A red box highlights the 'Accept' button, and a red arrow points to it with the text 'Click to accept ISE certificate'. Below the 'Accept' button, there is a 'Decline' button. At the bottom of the dialog, there is a 'Close' button.

Right Screenshot: The dialog box shows the successful completion of the integration process. A green checkmark icon is displayed next to the message: 'Integration of Cisco ISE server 100.64.0.101 was successful. Visit [System 360](#) to view health status.'. Below this message, a progress indicator shows four steps: 'Initiating connection...', 'Establishing trust...', 'Discovering nodes...', and 'Connecting to pxGrid...', all with green checkmark icons. At the bottom of the dialog, there is a 'Close' button.

AI Endpoint and Trust Analytics Deployment

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

The screenshot shows the Cisco ISE Administration interface for pxGrid Services. The 'Diagnostics' tab is active, and the 'WebSocket' section is expanded to show 'Clients'. A table lists several clients with their session IDs, subscriptions, publications, IP addresses, and status. The client 'pxgrid_client_1673849553' is highlighted with a green box. A red box highlights the 'Publications' column for this client, which is empty. Red arrows point from text annotations to these elements.

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

Catalyst Center pxGrid connection to ISE

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

No Publication attachments from Catalyst Center, yet

AI Endpoint and Trust Analytics Deployment

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

The screenshot displays the Catalyst Center interface for configuring AI Analytics. The left sidebar contains a search bar and a list of settings, with 'External Services' and 'Cisco AI Analytics' highlighted. The main content area is titled 'Cisco AI Analytics' and includes the following sections:

- AI Network Analytics**: A description of how machine learning is used to improve network performance. A checkbox labeled 'Enable AI Network Analytics' is checked and highlighted with a red box and arrow.
- AI-ENHANCED RRM**: A description of radio network optimization. A checkbox labeled 'AI-Enhanced RRM' is unchecked.
- AI Endpoint Analytics**: A description of fine-grained endpoint identification. Below this, the **ENDPOINT SMART GROUPING** section is shown with a description of AI-based endpoint profiling. A checkbox labeled 'Enable Endpoint Smart Grouping' is checked and highlighted with a red box and arrow.
- AI SPOOFING DETECTION *PREVIEW***: A description of detecting spoofed endpoints. A checkbox labeled 'Enable AI Spoofing Detection' is checked and highlighted with a red box and arrow.

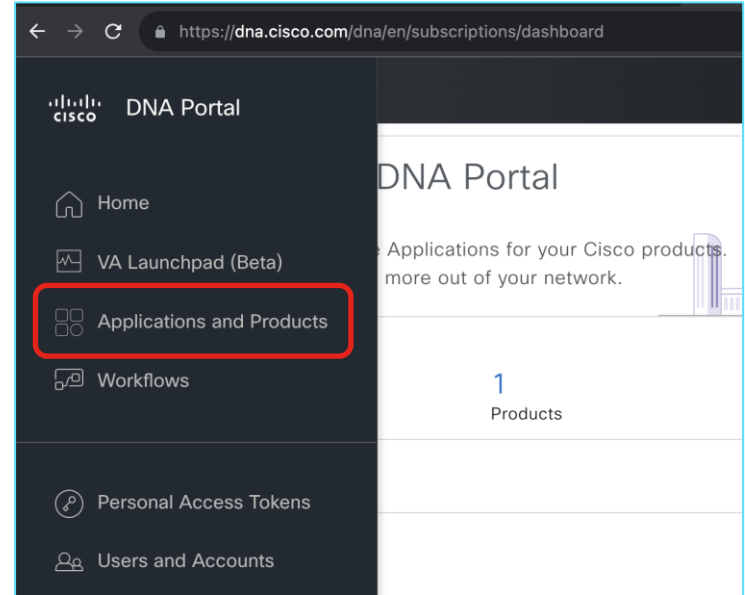
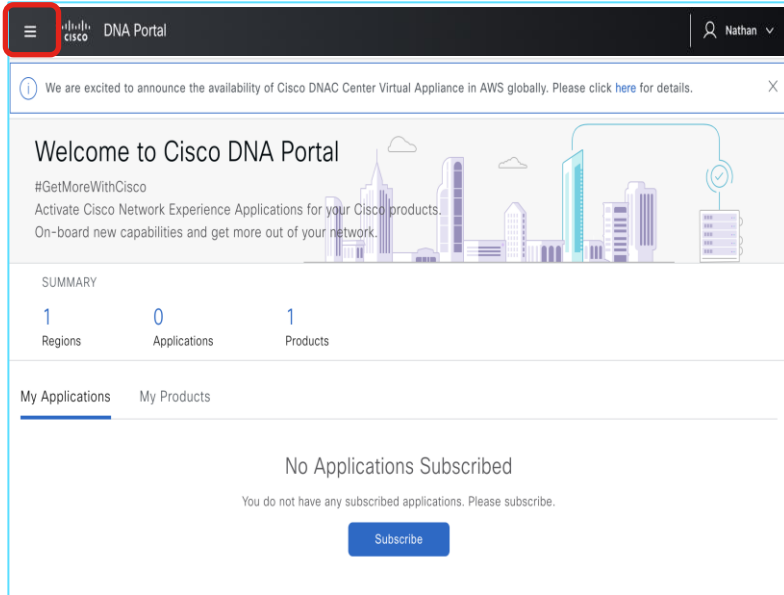
AI Endpoint and Trust Analytics Deployment

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

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

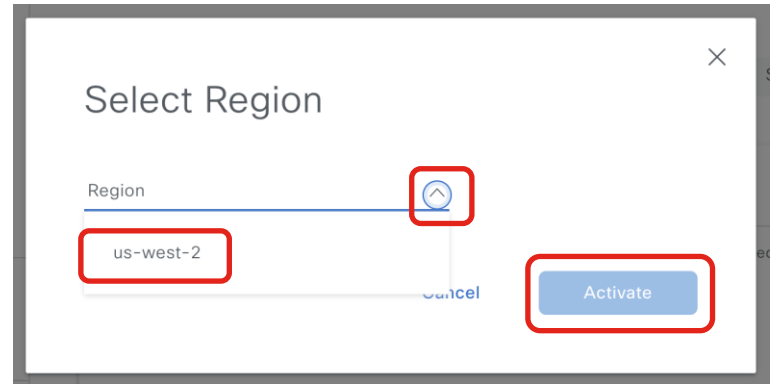
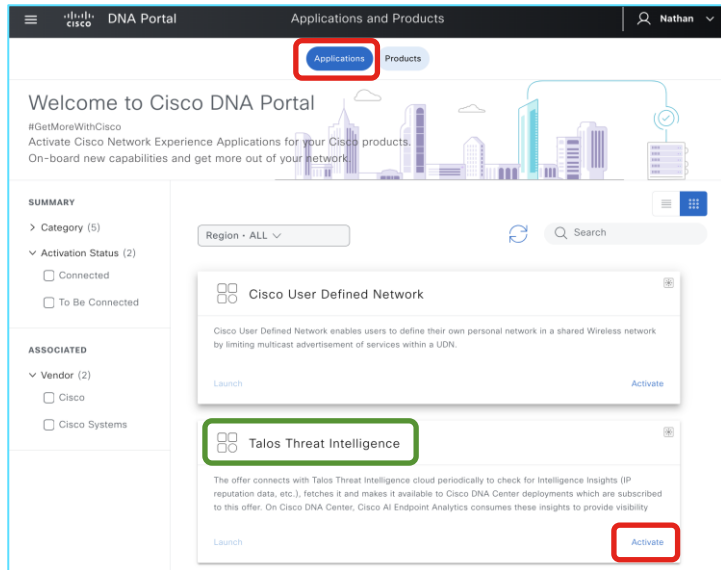
AI Endpoint and Trust Analytics Deployment

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



AI Endpoint and Trust Analytics Deployment

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



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

AI Endpoint and Trust Analytics Deployment

- Register your Catalyst Center cluster

Region · us-west-2

Choose your Product

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

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

All Cisco DNA Center

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

Register Product

Host Name/IP*
100.64.0.101

Product Name*
CiscoLive-Demo

Type*
Cisco DNA Center

Description

Select your Cisco DNA Center Version
 2.3.4.x or older 2.3.5.x or newer

Enable Cloud Access Login

Cancel

IP address reachable via web browser

Any preferred name

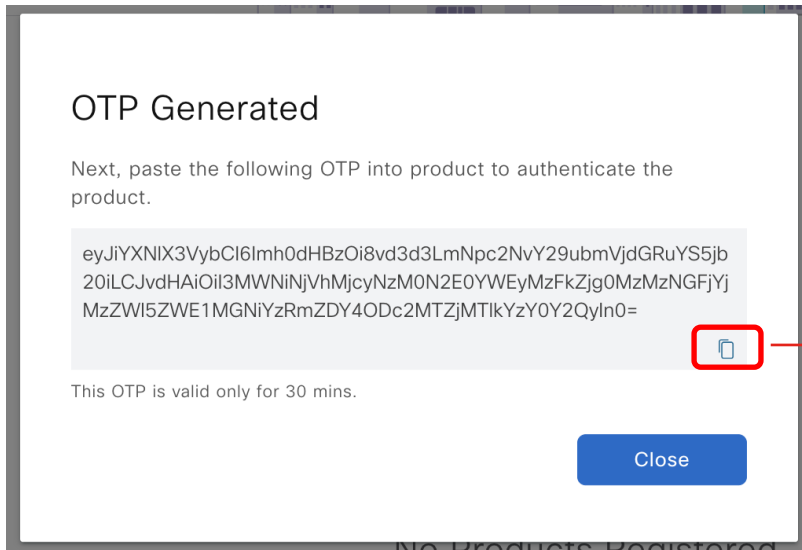
AI Endpoint and Trust Analytics Deployment

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

The image consists of two screenshots from the Cisco Catalyst Center interface. The left screenshot shows the 'Cisco DNA - Cloud' settings page with a 'Product Registered' dialog box overlaid. The dialog box contains the text 'Product registration is successful. You can now close the window.' and a blue 'Close' button, which is highlighted with a red rectangular box. A red arrow points from this button to the 'Cloud Authentication' option in the 'External Services' menu of the right screenshot. The right screenshot shows the 'Cloud Authentication' page, which includes the text 'This Cisco DNA Center is authenticated.' highlighted with a green rectangular box. The 'External Services' menu item is also highlighted with a green rectangular box. The 'Cloud Authentication' option in the menu is highlighted with a red rectangular box.

AI Endpoint and Trust Analytics Deployment

- If Catalyst Center is NOT reachable from operator's computer during integration (e.g. NAT), copy displayed OTP directly onto Catalyst Center



OTP Generated

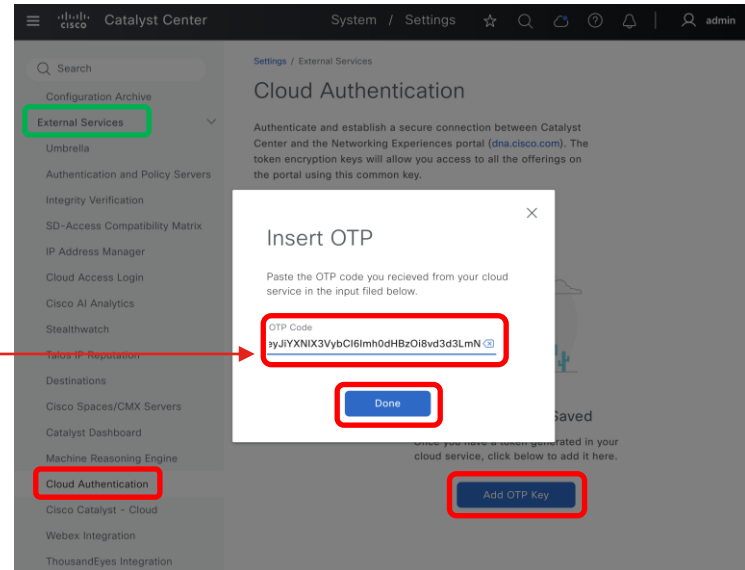
Next, paste the following OTP into product to authenticate the product.

```
eyJiYXNlX3VybCI6Imh0dHBzOi8vd3d3LmNpc2NvY29ubmVjdGRuYS5jb20iLCJvdHAiOiI3MWNiNjVhMjcyNm0N2E0YWEyMzFkZjg0MzMzNGFjYjMzZWl5ZWE1MGNiYzRmZDY0ODc2MTZjMjMTikYzY0Y2QyIn0=
```

This OTP is valid only for 30 mins.

Close

Cisco DNA Portal



Catalyst Center

System / Settings

Settings / External Services

Cloud Authentication

Authenticate and establish a secure connection between Catalyst Center and the Networking Experiences portal (dna.cisco.com). The token encryption keys will allow you access to all the offerings on the portal using this common key.

Insert OTP

Paste the OTP code you received from your cloud service in the input field below.

OTP Code
eyJiYXNlX3VybCI6Imh0dHBzOi8vd3d3LmNpc2NvY29ubmVjdGRuYS5jb20iLCJvdHAiOiI3MWNiNjVhMjcyNm0N2E0YWEyMzFkZjg0MzMzNGFjYjMzZWl5ZWE1MGNiYzRmZDY0ODc2MTZjMjMTikYzY0Y2QyIn0=

Done

Add OTP Key

Catalyst Center System Settings

AI Endpoint and Trust Analytics Deployment

- Continue Talos activation workflow on Cisco DNA Portal

Choose your Product

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

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

1 selected X

CiscoLive-Demo

Previous

Configure Access Control

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

CAPABILITIES

There are no messaging capabilities configured for this application.

API ACCESS

Allow All API Group for DNAC

Previous Next

Summary

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

Selected Application [Edit](#)

Name: Talos Threat Intelligence

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

Selected Product [Edit](#)

Region: us-west-2

Name: CiscoLive-Demo

Description:

Selected Scopes [Edit](#)

Allow All API Group for DNAC

Previous **Activate**

SUCCESS!

Done! Your Product is connected to Talos Threat Intelligence

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

Your Product is connected to Talos Threat Intelligence ✔

AI Endpoint and Trust Analytics Deployment

When Success is not in your cards!

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



Register Product

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

Host Name/IP*
100.64.0.101

Product Name*
CiscoLive-Demo

Type*
Cisco DNA Center

Region
us-west-2

Cancel Register

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

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

NAMESPACE	NAME	NOMINATED NODE	READINESS GATES	READY	STATUS	RESTARTS	AGE	IP
maglev-system	license-service-cleanup-job-fjb72	8.254.40.92	<none>	0/1	Completed	0	27h	16
maglev-system	registration-7db55d6d59-8vpd2	8.254.40.159	<none>	0/1	Running	0	11s	16
maglev-system	release-job-8cc6798c-98e7-49e8-a4f5-079570c0aa2a-packages-j912n	8.254.40.107	<none>	0/1	Completed	0	26h	16

```
maglev@maglev-master-192-0-1-1:~$ magctl appstack status -f
```

NAMESPACE	NAME	NOMINATED NODE	READINESS GATES	READY	STATUS	RESTARTS	AGE	IP
maglev-system	license-service-cleanup-job-fjb72	8.254.40.92	<none>	0/1	Completed	0	27h	16
maglev-system	release-job-8cc6798c-98e7-49e8-a4f5-079570c0aa2a-packages-j912n	8.254.40.107	<none>	0/1	Completed	0	26h	16

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

AI Endpoint and Trust Analytics Deployment

When Success is not in your cards!

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

The screenshot shows the Cisco DNA Portal interface. At the top, there is a navigation bar with the Cisco logo, "DNA Portal", and the text "Activate application on your product". A user profile for "Nathan" is visible in the top right. Below the navigation bar, there is a dropdown menu for "Region" set to "us-west-2". A red-bordered error message box is displayed, containing the text: "Unexpected error occurred while activating app for product. Please contact support for further assistance." Below the error message, the "Summary" section is visible, with instructions to "Please review all settings that you have entered. Click corresponding Edit for the settings you like to change." The summary is divided into three sections: "Selected Application" (Talos Threat Intelligence), "Selected Product" (CiscoLive-Demo-N62), and "Selected Scopes" (Allow All API Group for DNAC). At the bottom of the screen, there are "Exit", "Previous", and "Activate" buttons.

AI Endpoint and Trust Analytics Deployment

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

The screenshot shows the Cisco DNA Portal interface for Talos Threat Intelligence. The status is 'Connected' and 'Activated'. A table lists the activation details:

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

Cisco DNA Portal

The screenshot shows the Catalyst Center System Settings for Cisco DNA - Cloud. The configuration is set to 'Connected' for the 'us-west-2' region. A table lists the applications and their subscription status:

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

Catalyst Center System Settings

AI Endpoint and Trust Analytics Deployment

- Talos IP Reputation can now be enabled

The screenshot shows the Catalyst Center interface. The top navigation bar includes the Cisco logo, 'Catalyst Center', and 'System / Settings'. The left sidebar contains a search bar and a list of menu items: 'Device Prompts', 'Configuration Archive', 'External Services' (highlighted with a green box), 'Cisco AI Analytics', 'Talos IP Reputation' (highlighted with a red box), 'Destinations', 'Cisco Spaces/CMX Servers', 'Authentication and Policy Servers', and 'Integrity Verification'. The main content area is titled 'Talos IP Reputation' and includes a description: 'Enabling Cisco Talos IP Reputation connects Catalyst Center to Talos, detecting when endpoints attempt to access IPs with an untrusted reputation. Talos Intelligence Group manages the world's most comprehensive real-time threat detection network. Enabling process for Cisco Talos IP Reputation can take up to 60 seconds.' Below the text is a toggle switch labeled 'Disabled' with a refresh icon. The toggle is currently in the 'off' position and is highlighted with a red box. A dark grey tooltip box is overlaid on the toggle, containing the text 'Enabling in-progress. Enabling can take upto 60 seconds.' A red arrow points from this tooltip to the red text below.

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

AI Endpoint and Trust Analytics Deployment

- Talos IP Reputation ready for service

The screenshot shows the Catalyst Center interface. The top navigation bar includes the Cisco logo, the text 'Catalyst Center', and 'System / Settings'. A search bar is located on the left. The main content area is titled 'Settings / External Services' and 'Talos IP Reputation'. A descriptive paragraph explains that enabling this service connects Catalyst Center to Talos for real-time threat detection. A green box highlights the 'Enabled' toggle switch and a table titled 'Talos Intelligence Update'.

Settings / External Services

Talos IP Reputation

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

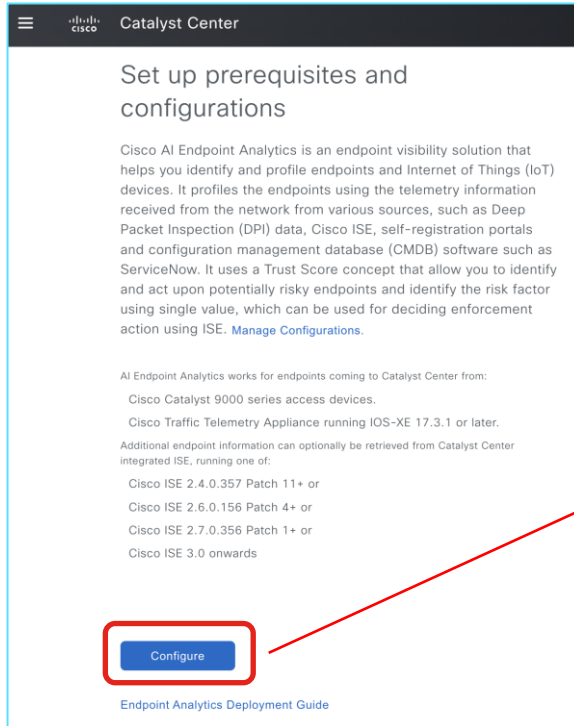
Enabled

Talos Intelligence Update

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

AI Endpoint and Trust Analytics Deployment

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



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:

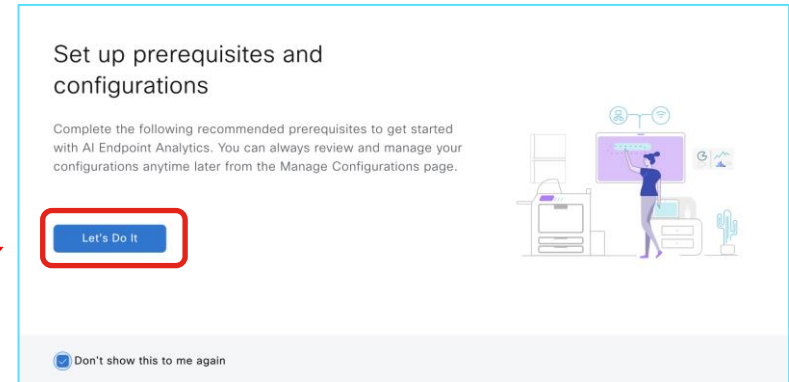
- Cisco Catalyst 9000 series access devices.
- Cisco Traffic Telemetry Appliance running IOS-XE 17.3.1 or later.

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

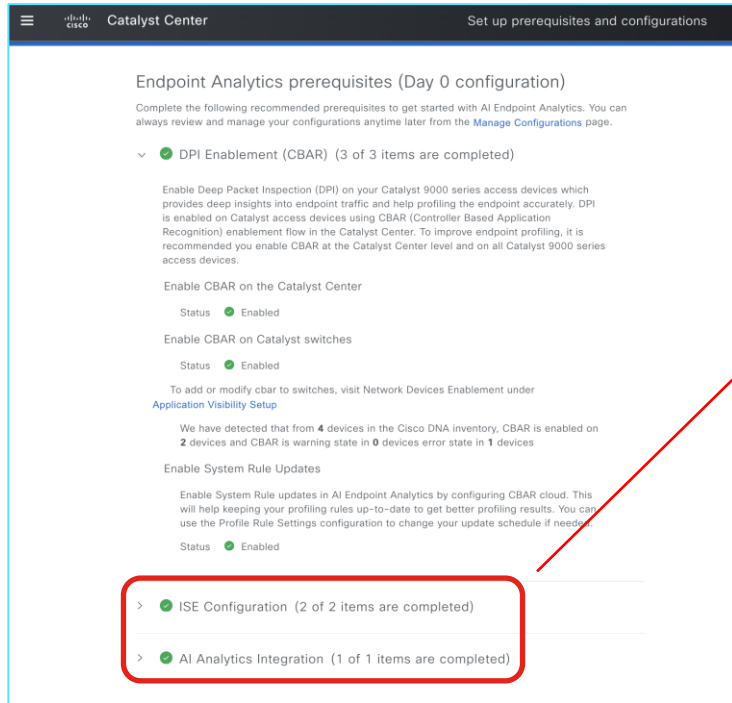
Complete the following recommended prerequisites to get started with AI Endpoint Analytics. You can always review and manage your configurations anytime later from the Manage Configurations page.

[Let's Do It](#)

Don't show this to me again

AI Endpoint and Trust Analytics Deployment

- Verify all prerequisites are met for EA to function properly

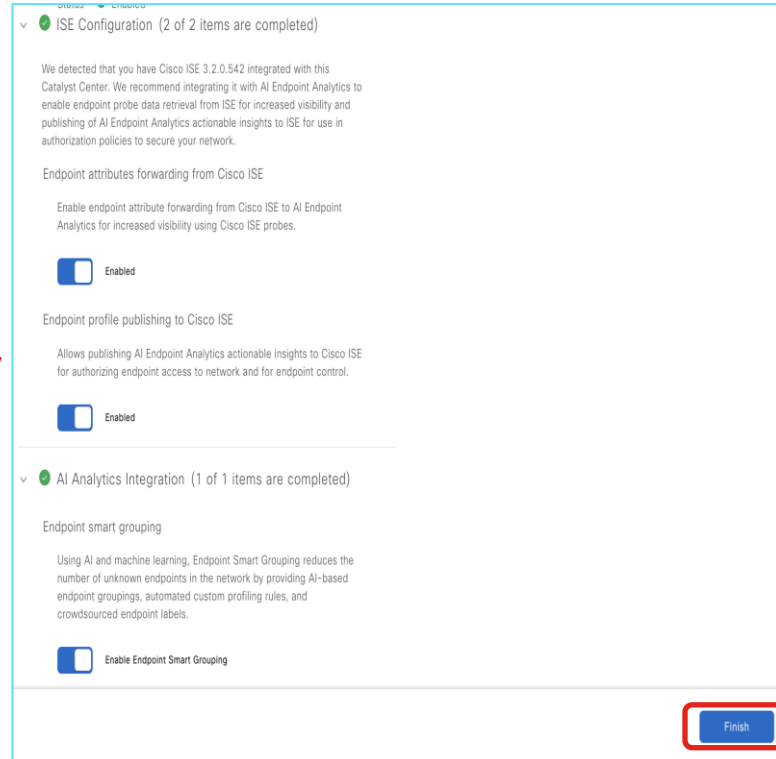


Catalyst Center Set up prerequisites and configurations

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

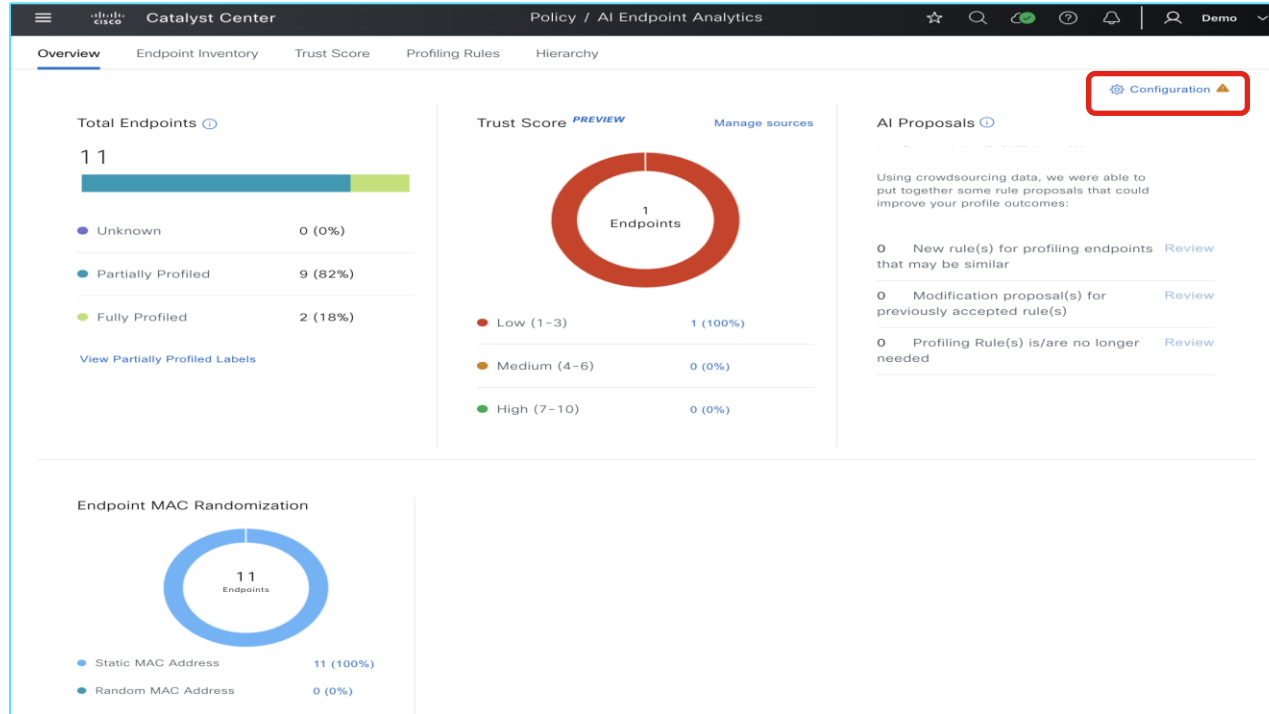
Using AI and machine learning, Endpoint Smart Grouping reduces the number of unknown endpoints in the network by providing AI-based endpoint groupings, automated custom profiling rules, and crowdsourced endpoint labels.

Enable Endpoint Smart Grouping

[Finish](#)

AI Endpoint and Trust Analytics Deployment

- AI Endpoint Analytics functional state



AI Endpoint and Trust Analytics Deployment

- Endpoint Analytics functional state

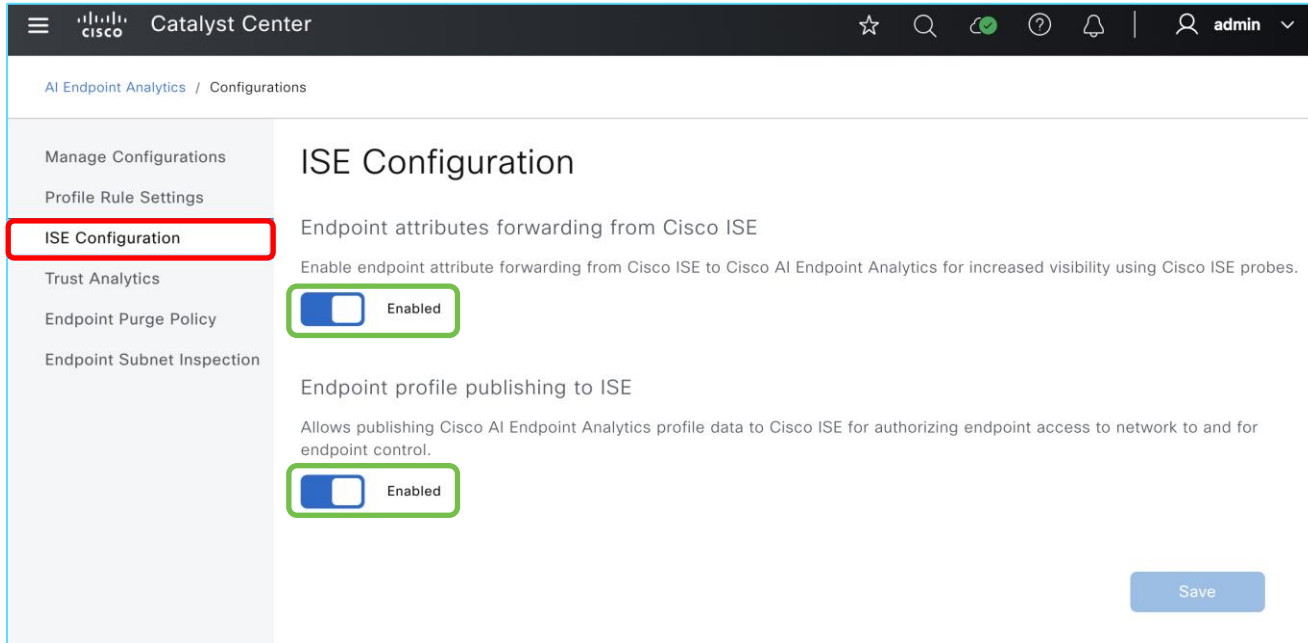
The screenshot displays the 'Manage Configurations' page in the Cisco Catalyst Center interface. The left-hand navigation menu has 'Manage Configurations' highlighted with a red box. The main content area is titled 'Manage Configurations' and includes a 'Refresh' button. It is divided into two sections: 'Required Configurations (3)' and 'Optional Configurations (4)'. Both sections feature a table with columns for 'Configuration Name', 'Status', and 'Details'. In the 'Required Configurations' table, three items are listed: 'DPI Enablement (CBAR)', 'ISE Configuration', and 'AI Analytics Integration', all with a green checkmark and 'Enabled' status. In the 'Optional Configurations' table, four items are listed: 'Security Sensor' (Disabled), 'ServiceNow' (Disabled), 'Talos IP Reputation' (Enabled), and 'AI Spoofing detection' (Enabled). The 'Talos IP Reputation' and 'AI Spoofing detection' rows are highlighted with a green box.

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

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

AI Endpoint and Trust Analytics Deployment

- Ensure Endpoint Profile Bidirectional Sharing with ISE



The screenshot shows the Catalyst Center interface for ISE Configuration. The left sidebar contains a menu with the following items: Manage Configurations, Profile Rule Settings, ISE Configuration (highlighted with a red box), Trust Analytics, Endpoint Purge Policy, and Endpoint Subnet Inspection. The main content area is titled "ISE Configuration" and contains two sections:

- Endpoint attributes forwarding from Cisco ISE**: "Enable endpoint attribute forwarding from Cisco ISE to Cisco AI Endpoint Analytics for increased visibility using Cisco ISE probes." This section has a toggle switch that is turned on and labeled "Enabled", which is highlighted with a green box.
- Endpoint profile publishing to ISE**: "Allows publishing Cisco AI Endpoint Analytics profile data to Cisco ISE for authorizing endpoint access to network to and for endpoint control." This section also has a toggle switch that is turned on and labeled "Enabled", which is highlighted with a green box.

A "Save" button is located at the bottom right of the configuration area.

AI Endpoint and Trust Analytics Deployment

- On Cisco ISE, verify profile bidirectional sharing to Endpoint Analytics
 - Access via **Work Centers** → **Profiler** → **Settings**

The screenshot displays the Cisco ISE interface for the Profiler Settings page. The top navigation bar includes 'Work Centers - Profiler' and 'Settings'. The left sidebar shows 'Profiler Settings' and 'Cisco AI Analytics'. The main content area is titled 'Profiling' and contains the following settings:

- Profiler Settings**
 - CoA Type*: Reauth
 - Current custom SNMP community strings: ***** Show
 - Change custom SNMP community strings: ⓘ
 - Confirm changed custom SNMP community strings: ⓘ
 - EndPoint Attribute Filter ⓘ
 - Anomalous Behaviour Detection ⓘ
 - Anomalous Behaviour Enforcement
 - Custom Attribute for Profiling Enforcement
 - Profiling for MUD
 - Profiler Forwarder Persistence Queue
 - XSS Security Scan Enforcement for EndPoint Probe Data ⓘ
- Endpoint Analytics Settings**
 - Publish Endpoint Attributes to AI Endpoint Analytics ⓘ
 - Consume Endpoint Profiles from AI Endpoint Analytics ⓘ

AI Endpoint and Trust Analytics Deployment

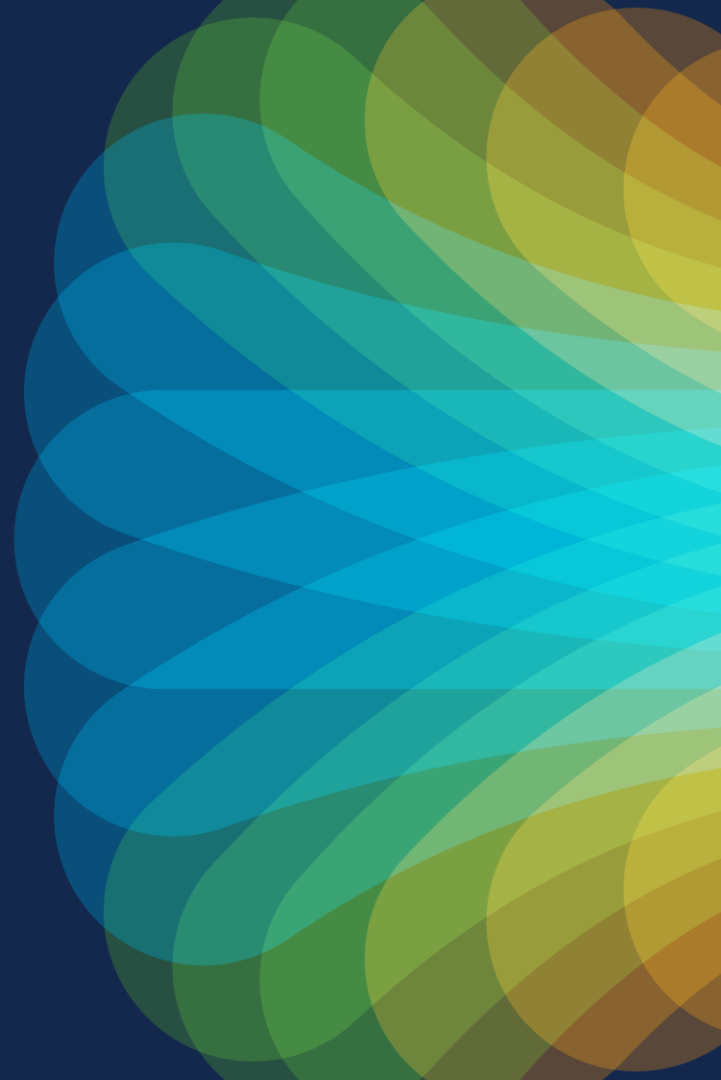
- On Cisco ISE, verify that Catalyst Center is publishing to Endpoint Analytics topic
 - Access via **Administration -> pxGrid Services -> Diagnostics**

The screenshot shows the Cisco ISE Administration interface for pxGrid Services. The 'Diagnostics' tab is active, and the 'WebSocket' section is expanded to show 'Clients'. A table lists several clients with columns for Client Name, Session Id, Subscriptions, Publications, IP Address, and Status. The 'pxgrid_client_1673849553' client is highlighted with a green box. A tooltip is visible over the 'Publications' column for this client, listing several topics including '/topic/com.cisco.ea.data'. Red arrows and text annotations provide context: one points to the client name with the text 'Catalyst Center pxGrid connection to ISE', and another points to the tooltip with the text 'Mouse over to verify Catalyst Center is publishing to com.cisco.ea.data topic'.

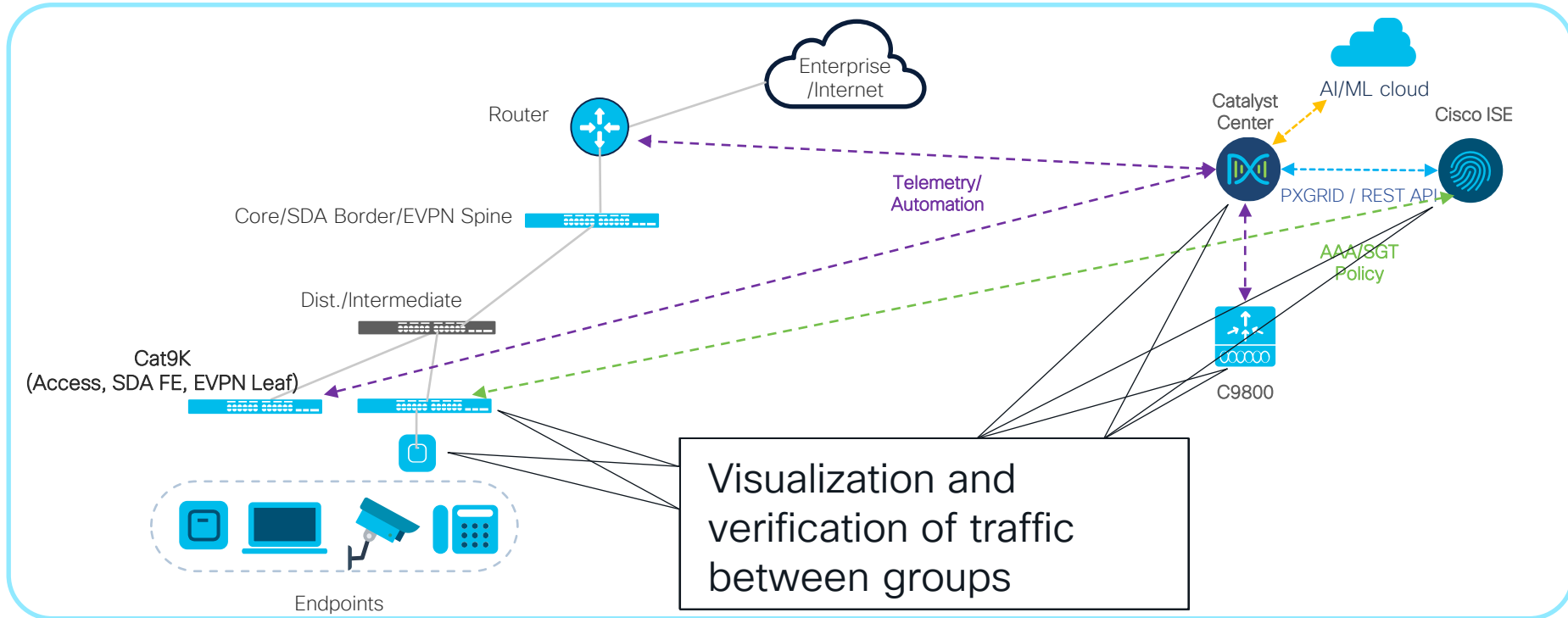
Client Name	Session Id	Subscriptions	Publications	IP Address	Status
-ise-mnt-ise	ise:0	/topic/com.cisco.ise.sessio...	/topic/com.cisco.ise.sessio...	100.64.0.100	Connected
-ise-fanout-ise	ise:2	/topic/wildcard		127.0.0.1	Connected
-ise-fanout-ise	ise:3	/topic/distributed	/topic/distributed	100.64.0.100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

```
/topic/com.cisco.endpoints...
n
tanalytics.data
/topic/com.cisco.ea.data
.ise.cisco.local
/topic/com.cisco.endpoi
n
t.asset
```

Group Policy Analytics



Group Policy Analytics



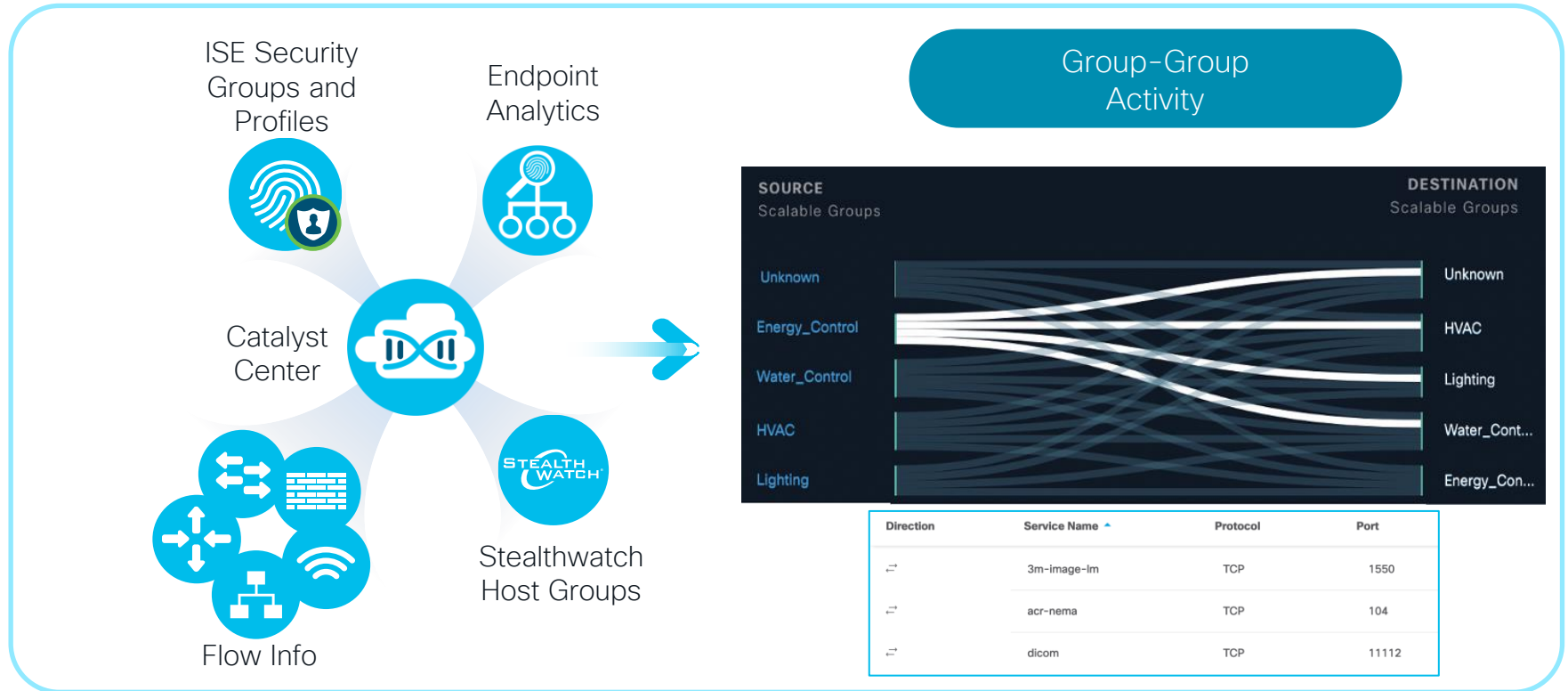
Group Policy Analytics

Overview

- **Visualization of Flow** data based on Security Group Tags
 - NetFlow export does not include SGT info*
 - Relies on **correlation** of NetFlow data with mappings from ISE, EA, StealthWatch
- Allows for verification of configured Group Policies
- Ability to add discovered flows to configured SG Contracts
- GBPA currently **NOT** supported with Catalyst Center OVA

*IOS-XE 17.13.1 can be configured to include SGT permit/deny action in flow export; however, currently only StealthWatch 7.4.2 can consume that info

Group Policy Analytics



Group Policy Analytics

Detecting Ports and Protocols Between Groups

The screenshot displays the Cisco Scalable Groups Traffic analytics interface. On the left, a dark sidebar shows the navigation path: Scalable Groups Traffic > Scanners ↔ Storage. Below this, the 'SOURCE' is identified as 'Scalable Groups' and the 'DESTINATION' is also 'Scalable Groups'. A progress bar at the bottom of the sidebar indicates the flow from 'Scanners' to 'Storage'.

The main content area is titled 'Scanners → Storage' and features a search bar labeled 'Search Table'. Below the search bar are three action buttons: 'Create Report', 'Download Report', and 'View Contract'. The 'View Contract' button is highlighted with a red box. A red arrow points from this button to a table of detected traffic.

Direction	Service Name	Protocol	Port
↔	3m-image-lm	TCP	1550
↔	acr-nema	TCP	104
↔	dicom	TCP	11112

The table is highlighted with a green border. A green arrow points from the bottom of the table back to the 'View Contract' button.

Use detected ports and protocols to verify or modify needed access control policies

Group Policy Analytics

Modifying Contract Between Groups

The screenshot displays the Cisco Catalyst Center interface for Group Policy Analytics. The breadcrumb trail is: Overview > Policy Analytics for Security Groups > Water_Control > Energy_Control > Contract Page. The current view is for the contract 'Water_Control → Energy_Control' with a 'Default' status. The interface is split into two main sections:

- CONFIGURED CONTRACT:** This section shows the contract configuration. It includes a search bar and a table with columns: #, Action, Application, Protocol, Source Port, Destination Port, Logging, and Action. The table currently displays 'No data to display'. A red box highlights the 'Create Access contract' button.
- DISCOVERED via Policy Analytics:** This section shows traffic flows. It includes a search bar and a table with columns: Direction, Service Name, Protocol, Port, and Flow Count. The table lists several flows, including ftp, telnet, tftp, and https, along with unassigned flows.

At the bottom of the interface, there are options for 'Default Action', 'Logging', and 'View traffic'. The bottom right corner shows '971 Record(s)' and 'Show Records: 10'.

Group Policy Analytics

Modifying Contract Between Groups

Catalyst Center Policy / Group-Based Access Control

Overview Policies Security Groups Access Contracts

Overview > Policy Analytics for Security Groups > Water_Control > Energy_Control > Contract Page

Water_Control → Energy_Control Default

> Policy Details

Inherited from Default Policy [Change contract](#) [Create Access contract](#)

CONTRACT CONTENT (2)

#	Action*	Application*	Transport Protocol	Source / Destination	Port	Logging	Action
1	Select Value*	Select Value*	Select Value	Destination		<input type="checkbox"/>	+ X
2	Select Value*	ftp	TCP	Destination	21	<input type="checkbox"/>	+ X

All Unique Traffic Flows

Search Table

Direction	Service Name	Protocol	Port	Flow Count	Action
→	ftp	TCP	21	26	Add to contract
→	telnet	TCP	23	25	Add to contract
→	fttp	UDP	69	25	Add to contract
→	https	TCP	443	25	Add to contract
→	Unassigned	TCP	49167	1	Add to contract

Group Policy Analytics

Deployment Consideration

- Successful integration with Cisco ISE is required
- Application Telemetry MUST be enabled on access switches and C9800
- CBAR MUST be enabled on access switches and C9800 in order to visualize traffic for ISE device profiles
- Initial sync will cause Cisco ISE to be in read-only mode from Group Policy perspective (normal and recommended operating mode)
 - Option to revert ISE back to read-write mode only available after initial sync
 - Reverting ISE to read-write mode will prevent Group Policy Analytics functionality on Catalyst Center from viewing granular traffic flows and adding/modifying contracts
- Catalyst Center does not support following scenarios on ISE:
 - Multiple contracts or SGACL per policy
 - Multiple policy matrices
- Supported for SDA Fabric or non-fabric networks

Group Policy Analytics Deployment

- Ensure Cisco ISE has been successfully added to Catalyst Center

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

IP Address	Protocol	Type	Status
10.172.3.100	RADIUS_TACACS	ISE	ACTIVE

Group Policy Analytics Deployment

- Sync Security Groups and Policies from Cisco ISE through **Policy -> Group-Based Access Control**

The screenshot displays the Catalyst Center interface for 'Policy / Group-Based Access Control'. The breadcrumb navigation shows 'Overview', 'Policies', 'Security Groups', and 'Access Contracts'. A central information box explains the migration process from Cisco ISE. Below this, a search bar and a dashboard with two cards are visible. The 'SECURITY GROUPS' card shows 0 items, and the 'ISE PROFILES' card shows 0 items. A dropdown menu is open, showing 'Start migration' and 'Schedule migration' options.

In order to begin using Catalyst Center as the administration point for Group-Based Access Control, Catalyst Center must migrate policy data from the Cisco Identity Services Engine (ISE):

- Any policy features in Cisco ISE that are currently not supported in Catalyst Center will not be migrated, you will have a chance to review the migration rule after click on "Start migration"
- Any policy information in Catalyst Center not already exist in Cisco ISE will be copied to Cisco ISE to ensure the 2 sources are in sync

Once the data migration is initiated, you cannot use Group-Based Access Control in Catalyst Center until the operation is complete. After policy data migration has completed, if you prefer to manage Group-Based Access Control in Cisco Identity Services Engine, you can click on "Group-Based Access Control Configuration".

Start migration ^

Start migration

Schedule migration

View traffic for ...

0 SECURITY GROUPS

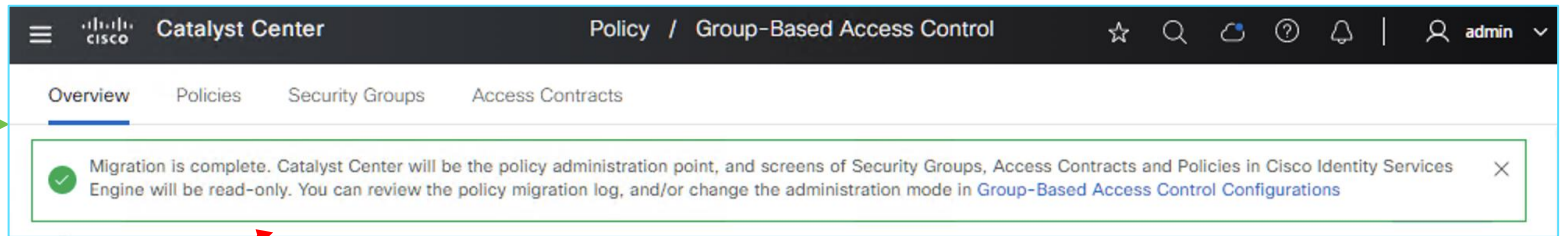
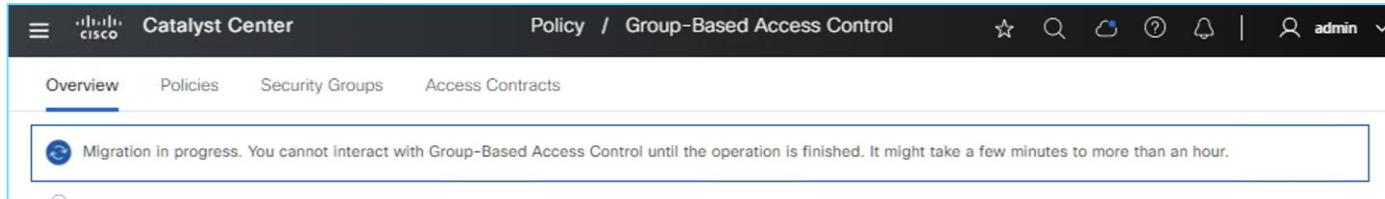
0 ISE PROFILES

Start migration: Immediate syncing between Catalyst Center and ISE

Schedule migration: Schedule future sync task between Catalyst Center and ISE

Group Policy Analytics Deployment

- Successful sync between Catalyst Center and ISE



”Catalyst Center will be the policy administration point, and screens of Security Groups, Access Contracts and Policies in Cisco Identity Services Engine will be read-only.”

Summary

- NetFlow offers powerful insight with minimal overhead
- Applications like Policy Analytics and AI Endpoint and Trust Analytics leverage NetFlow to provide enhanced security visibility
- Catalyst Center automates all necessary NetFlow configuration on relevant devices...
- ...when done through proper workflow

Cisco Live EMEA Catalyst Center Learning Map

Monday 5th

TECOPS-2001

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

TECOPS-2002

How to leverage Catalyst Center to build a Zero Trust Campus Network

TECOPS-2158

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

TECOPS-2823

How to leverage Catalyst Center to its greatest potential

Tuesday 6th

LTREWN-2511

Automating wireless deployments at scale using Catalyst Center

BRKOPS-2032 ★

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

BRKOPS-2416

7 Habits for success with Cisco Catalyst Center

BRKOPS-1183

Introduction to Infrastructure as Code for Catalyst Center with Terraform

LTRSEC-2005

Building Cisco SD-Access with Cisco Catalyst Center & ISE

Wednesday 7th

BRKOPS-2540

Best Practice for Prime to Catalyst Center Migration

BRKOPS-2683

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

★ BRKOPS-2375

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

LTROPS-2977

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

BRKCOC-2465

Inside Cisco IT - automating the network with Catalyst Center

BRKOPS-1110 ★

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

BRKOPS-2357

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

Thursday 8th

BRKOPS-2077

Tips and Tricks for Prime Infrastructure to Catalyst Center Migration

BRKEWN-2667

Catalyst Wireless Supercharged by Catalyst Center

BRKOPS-2038

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

BRKOPS-2402

Automate the Deployment of a Wireless Network with the Help of Catalyst Center

★ BRKOPS-2471

Custom Workflows for the Catalyst Center Integration with ServiceNow

Friday 9th

★ BRKOPS-2521

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

Capture The Flag

@Hub All week long

Catalyst Center 2.3.7

Catalyst Center 2.3.5

Prime Migration

Catalyst

Center

★ BU led sessions

CISCO Live!



The bridge to possible

Thank you

CISCO *Live!*

CISCO *Live!*

Let's go