

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Understanding Various Catalyst Center Integrations for Day-to-Day Network Operations

Ramkumar Chellappa, Technical Leader, TME
@ramkchel
BRKOPS-2118

Cisco Webex App

Questions?

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

How

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

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



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKOPS-2118>



Ramkumar Chellappa

Technical Lead-TME for Catalyst Center NetOps



Scan to add me on LinkedIn! →

www.linkedin.com/in/ramkumarchellappa



Fields of Expertise

14+ years of Experience. TME for Automation Use Cases in Catalyst Center



Personal Life

Indian, Chennai. Married with 2 Kids



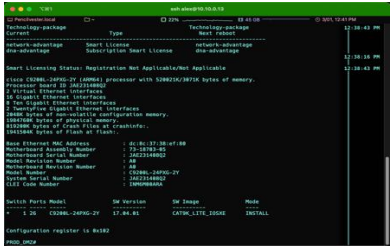
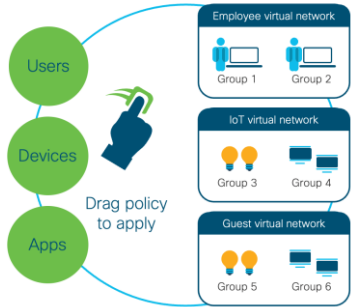
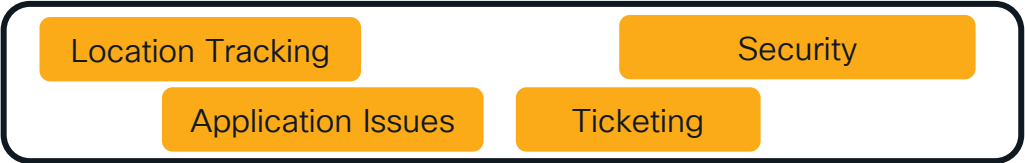
Hobbies

Playing Cricket, Long Drives

My Road Trip...



Your Road Trip...



User Experience

Point A

Point B

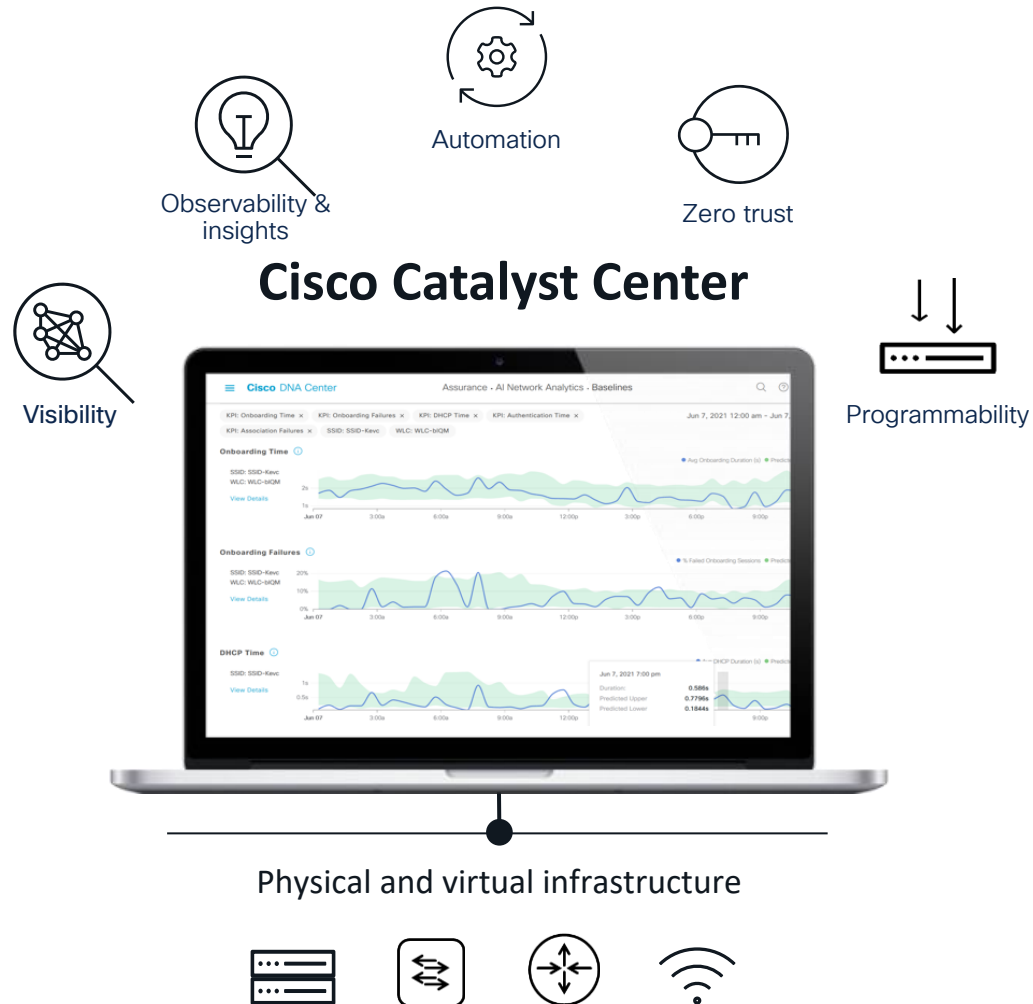
Goals:

- Security
- Visibility
- Accuracy

It's about Simplifying Networking Operations, with Less driving Effort.

Simplifying Network Operations

Facilitating the jobs your teams need to do



NetOps

Automation and workflows simplify building and maintaining large scale networks. AI/MR streamlines and simplifies complex tasks



AIOps

AI/ML and predictive insights for **proactive optimization** to ensure consistent performance and reliability and the **optimal user experience**



SecOps

AI/ML and DPI Identify and classify endpoints, enforce security policies and mitigate threats for a **complete workplace zero trust solution**



DevOps

Mature APIs, SDKs, and **closed-loop integrations**, untangle the complexities of interconnecting third party systems

cisco *Live!*

Agenda

Integrations for Network Management

- Ekahau
- Cisco Spaces
- Cisco ISE
- Secure Analytics - Group based policy analytics & AI Endpoint analytics

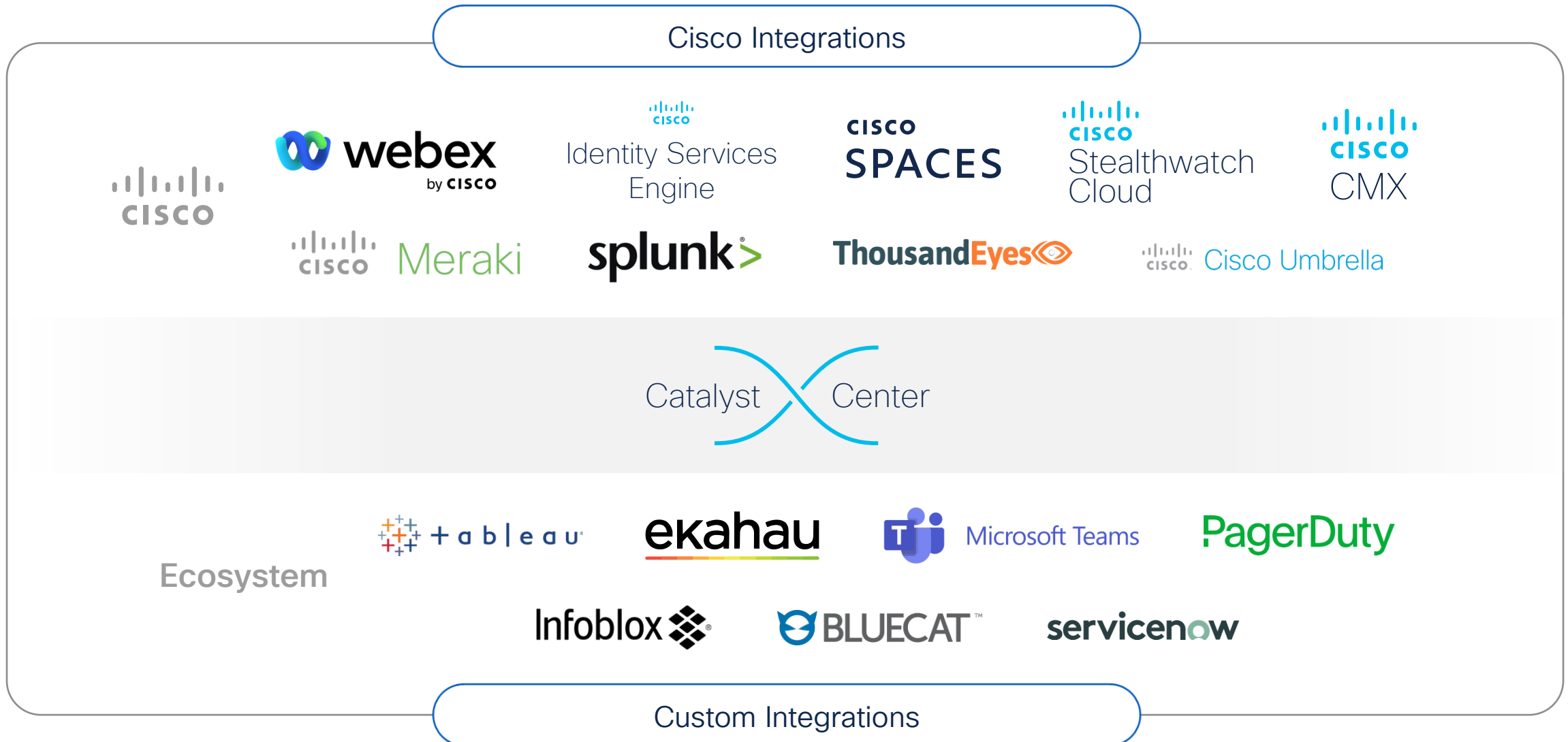
Integrations for (Network) Assurance/Monitoring

- MS Teams
- Thousand Eyes
- SD-AVC (Infoblox DNS A-Records, NBAR Cloud, MS Feeds)

Integrations to Simplify Network Operations

- ITSM (Change Management and Event Management)
- Event Notifications (SNMP/Syslog/SMTP/Webhooks)

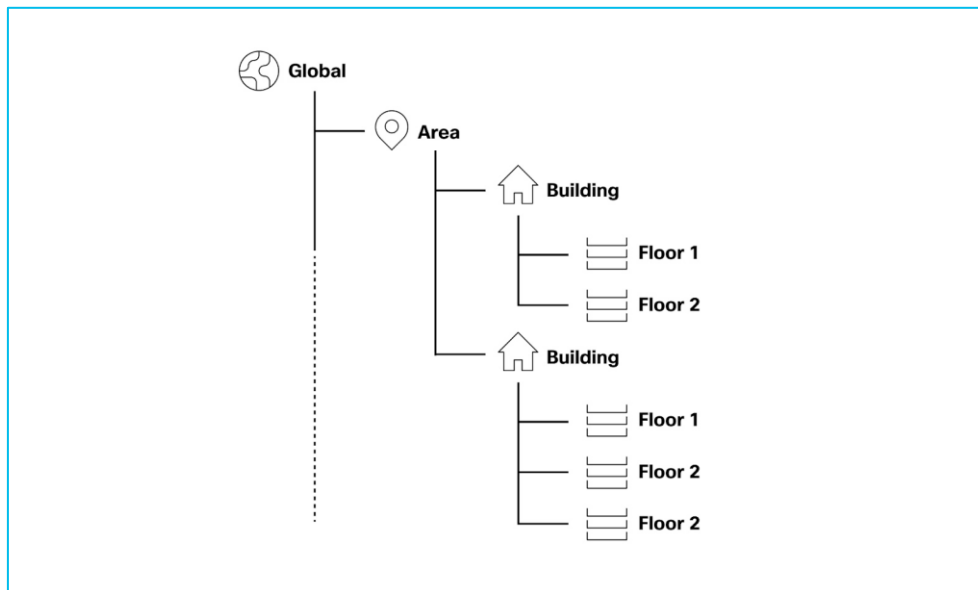
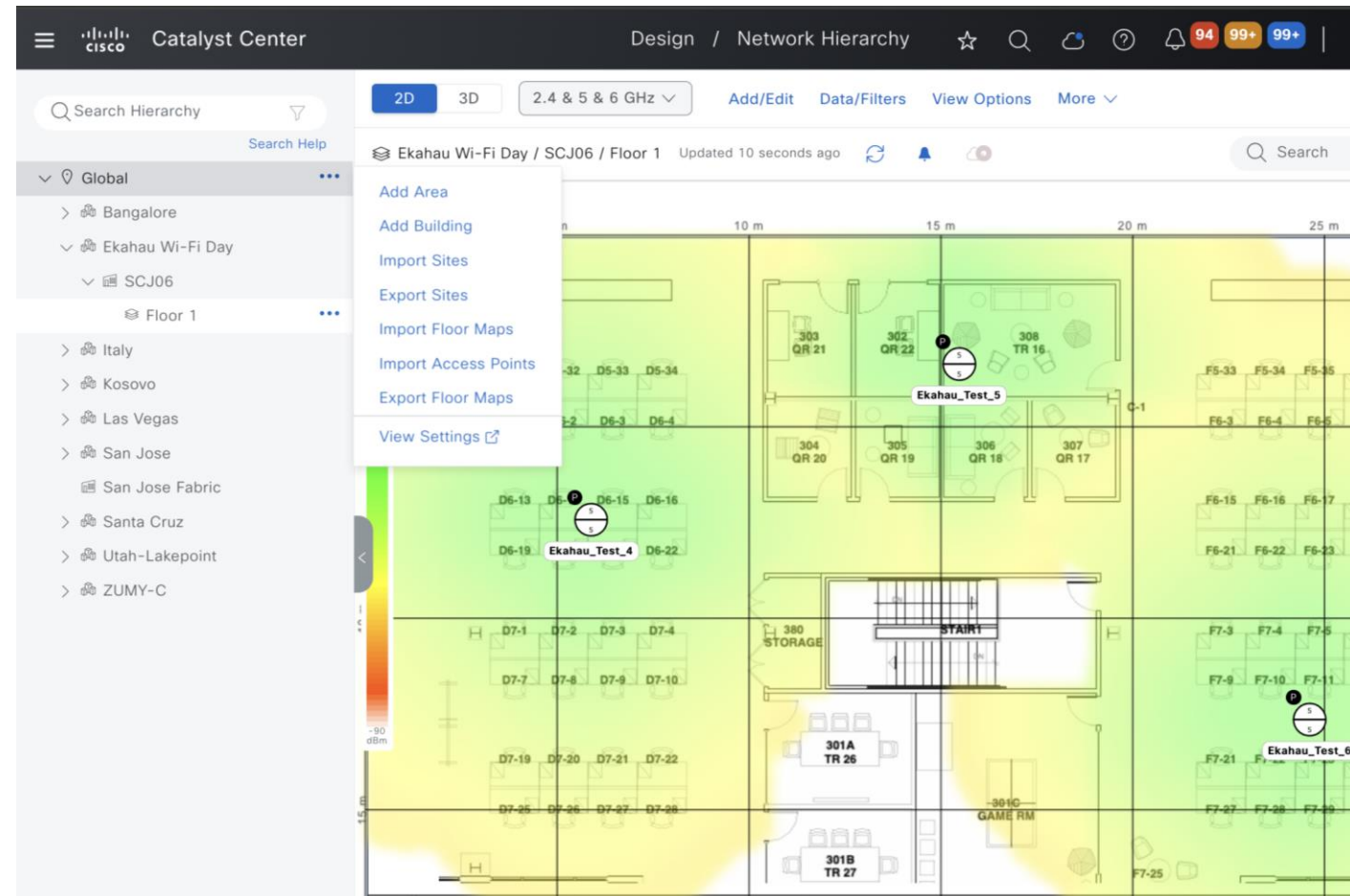
Catalyst Center out-of-the-box API integrations



Integrations for Network Management

Creating Site Hierarchy

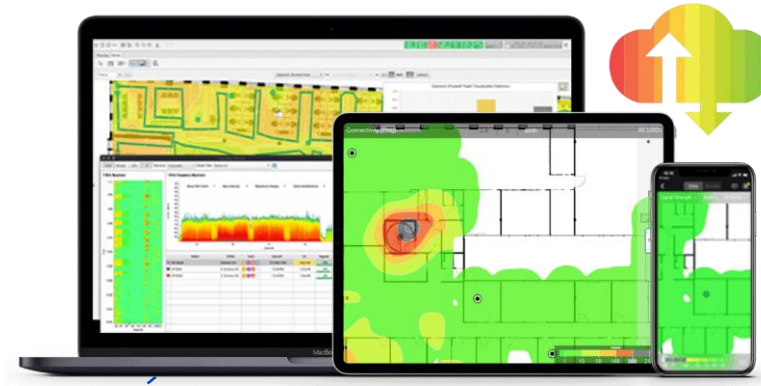
Create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network.



Importing Ekahau Projects to Catalyst Center



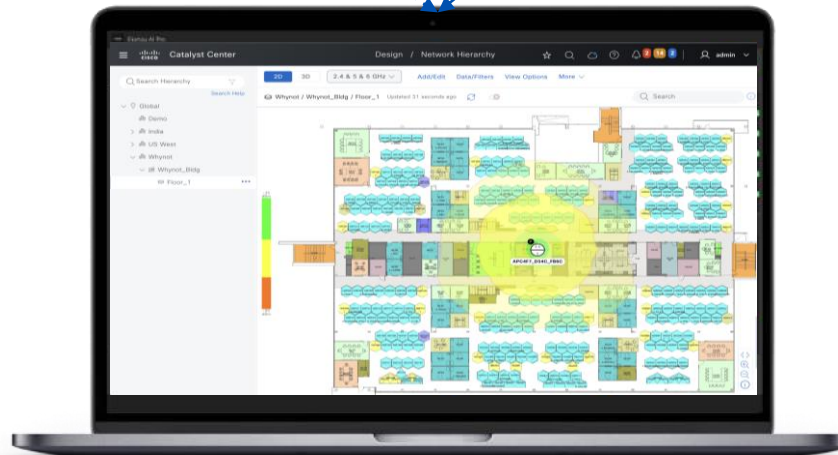
Ekahau Pro



Ekahau Cloud

Ekahau Pro version 11 –
Catalyst Center version 2.3.5.x

Ekahau cloud – Catalyst Center
version 2.3.7.x

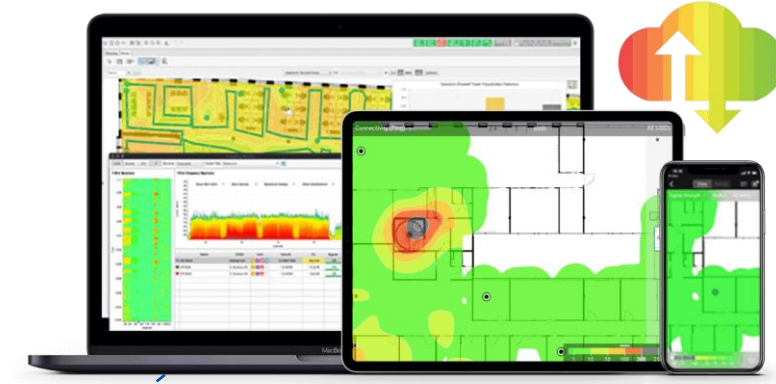


Catalyst Center

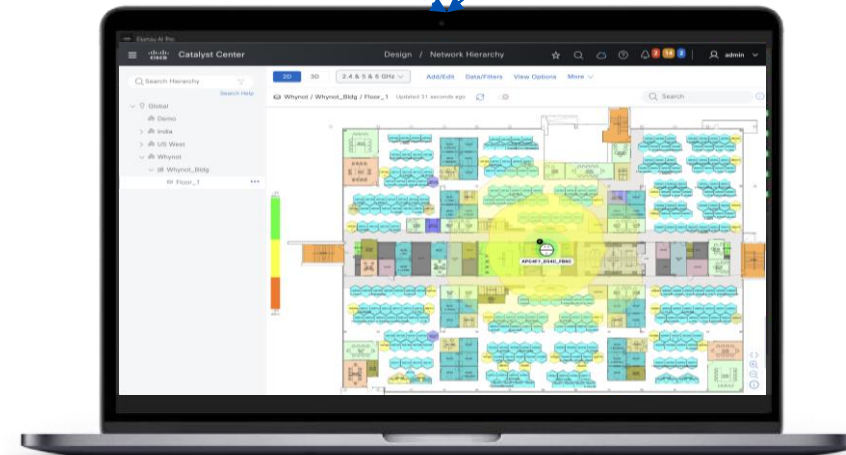
Importing Ekahau Projects to Catalyst Center



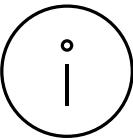
Ekahau Pro



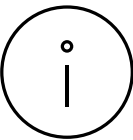
Ekahau Cloud



Catalyst Center



Ekahau Pro – **Area name and Building Name** created in Catalyst Center must be same as **Ekahau Project Name** or **Building Name** in Ekahau Project



Ekahau Cloud – Mention **Area/Sub-Area/Building** name before exporting the Ekahau Project

Importing Ekahau Projects to Catalyst Center

Drag and Drop Ekahau files (.esx) to import

To import Ekahau Projects, select an Area/Building and Import Ekahau Project

Import Preview

Import Preview Total Area(s): 1, Building(s): 2, Floor(s): 4, APs: 0, PAPs: 4

Site Hierarchy Preview

- AREA Whynot Total Area(s): 1, Building(s): 2, Floor(s): 4, ... 1/3 0/6 0/0
- BUILDING Building 1 Total Floor(s): 2, APs: 0, PAPs: 2 1/1 1/3 0/0
 - FLOOR 14th floor Total APs: 0, PAPs: 1 0/0 1/1 0/0
 - FLOOR 15th floor Total APs: 0, PAPs: 1 0/0 1/1 0/0
- BUILDING Building 2 Total Floor(s): 2, APs: 0, PAPs: 2 1/1 1/3 0/0
 - FLOOR 16th floor Total APs: 0, PAPs: 1 0/0 1/1 0/0
 - FLOOR 17th floor Total APs: 0, PAPs: 1 0/0 1/1 0/0

Import Summary - 14th floor

Information (0) Warning (1) Errors (0)

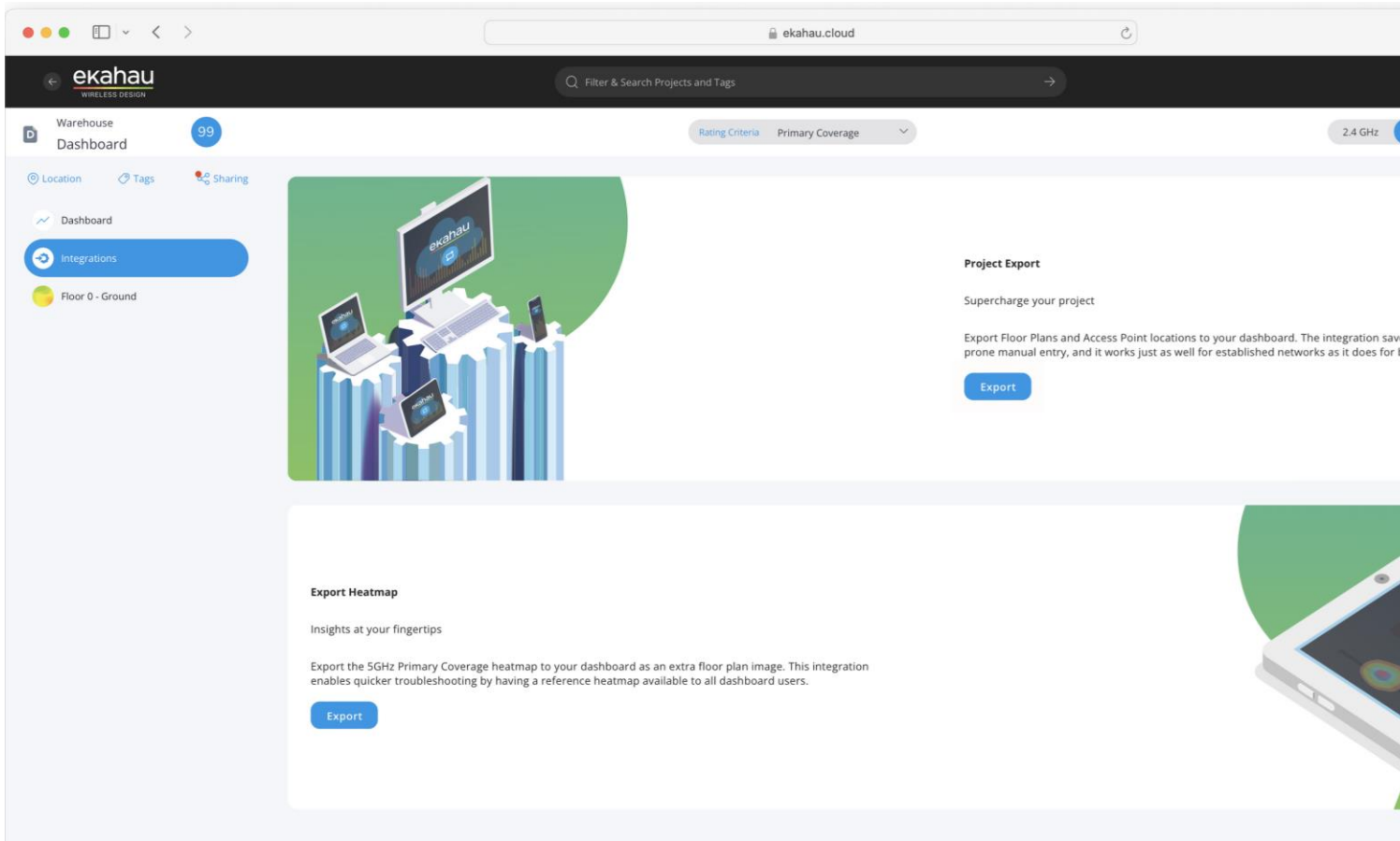
Message

Hierarchy element '14th floor' doesn't exist, it will be created

Showing 1 of 1

Importing Ekahau Projects to Catalyst Center

Using API method



Project export ?

< Back

CISCO

Username *

Password *

OnPremise Url *

Project export ?

< Back

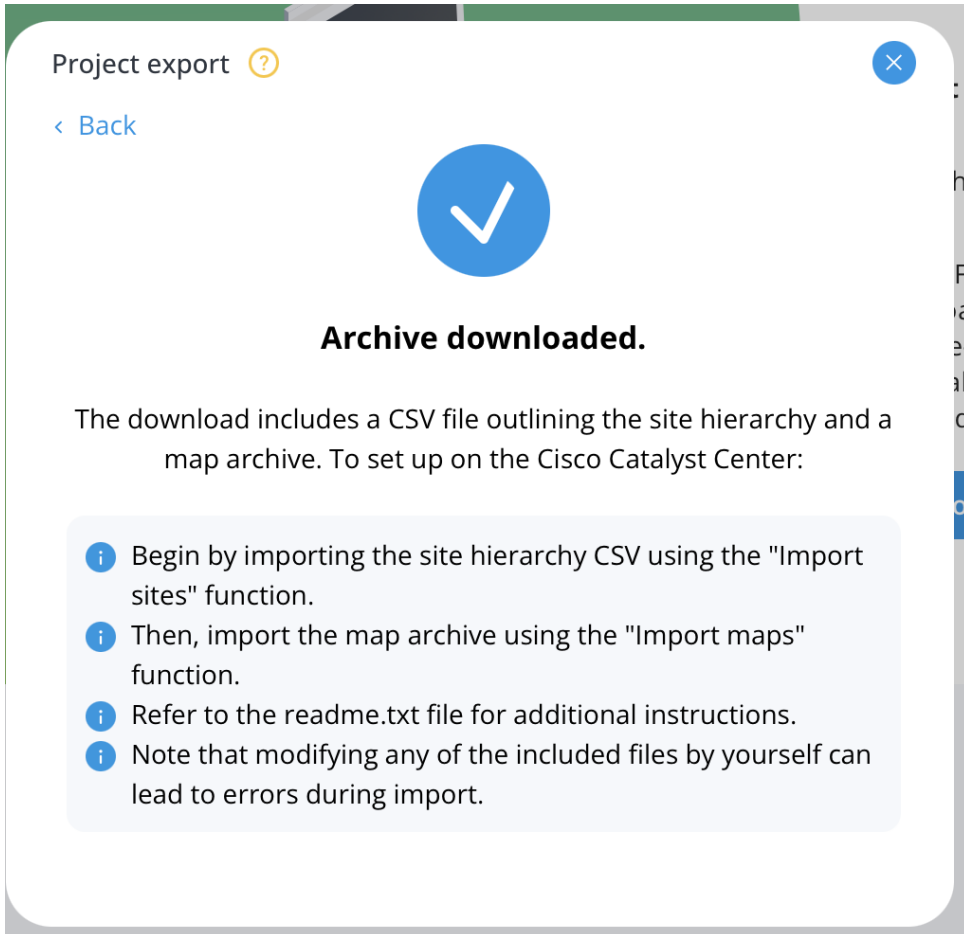
CISCO

Site path *

Buildings *

Importing Ekahau Projects to Catalyst Center

Without Login



Project export ?

< Back

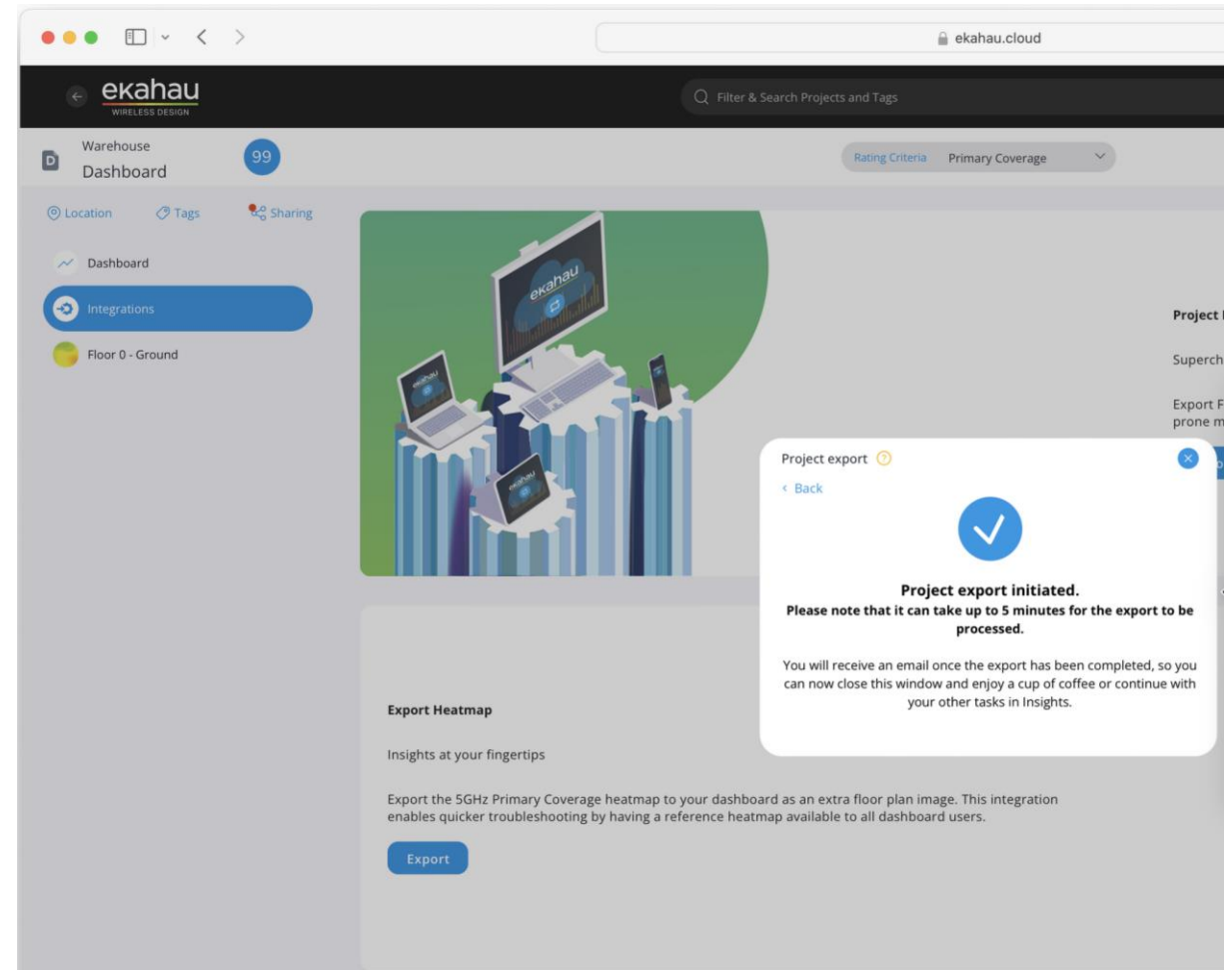


Archive downloaded.

The download includes a CSV file outlining the site hierarchy and a map archive. To set up on the Cisco Catalyst Center:

- Begin by importing the site hierarchy CSV using the "Import sites" function.
- Then, import the map archive using the "Import maps" function.
- Refer to the readme.txt file for additional instructions.
- Note that modifying any of the included files by yourself can lead to errors during import.

With Login



ekahau WIRELESS DESIGN

Filter & Search Projects and Tags

Warehouse Dashboard 99

Location Tags Sharing

Dashboard

Integrations

Floor 0 - Ground

Project export ?

< Back



Project export initiated.

Please note that it can take up to 5 minutes for the export to be processed.

You will receive an email once the export has been completed, so you can now close this window and enjoy a cup of coffee or continue with your other tasks in Insights.

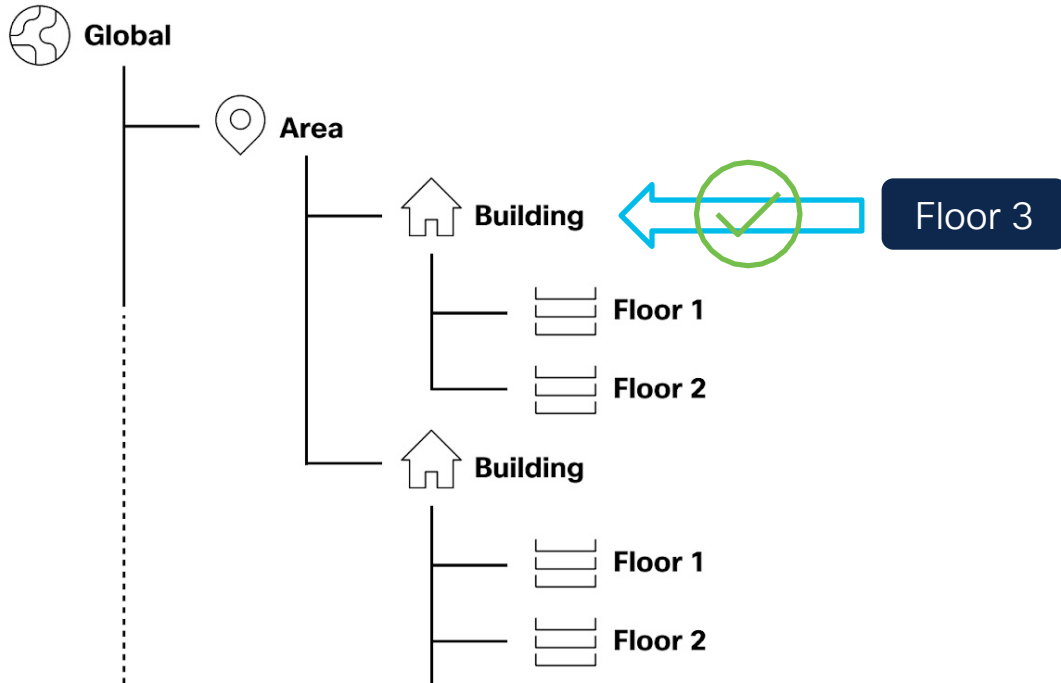
Export Heatmap

Insights at your fingertips

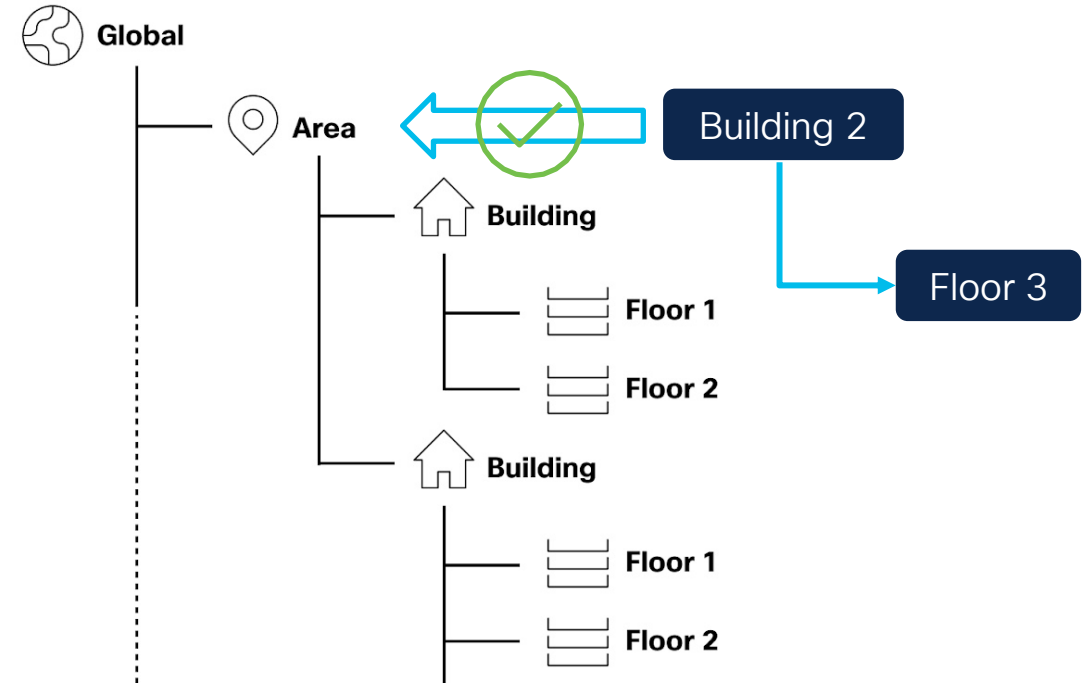
Export the 5GHz Primary Coverage heatmap to your dashboard as an extra floor plan image. This integration enables quicker troubleshooting by having a reference heatmap available to all dashboard users.

Export

Catalyst Center-Ekahau Anchor Points

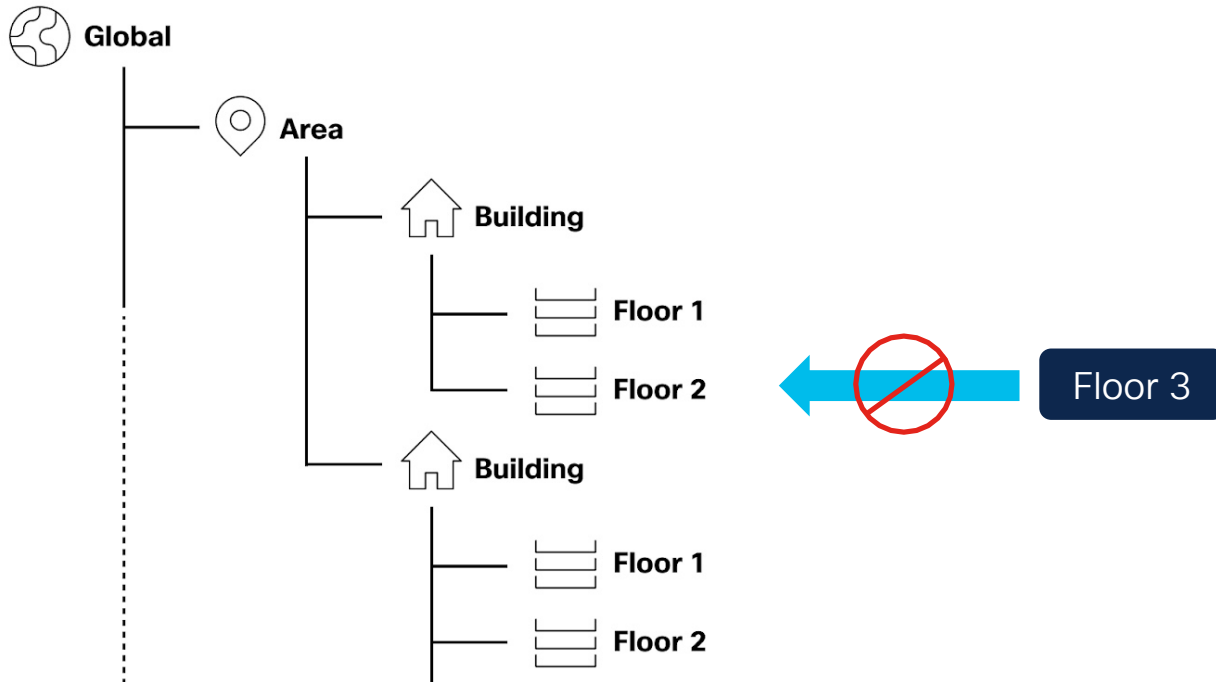


- ✓ If the floor already exist, then the floor is updated with changes
- ✓ If the floor does not exist, then a new floor is created.

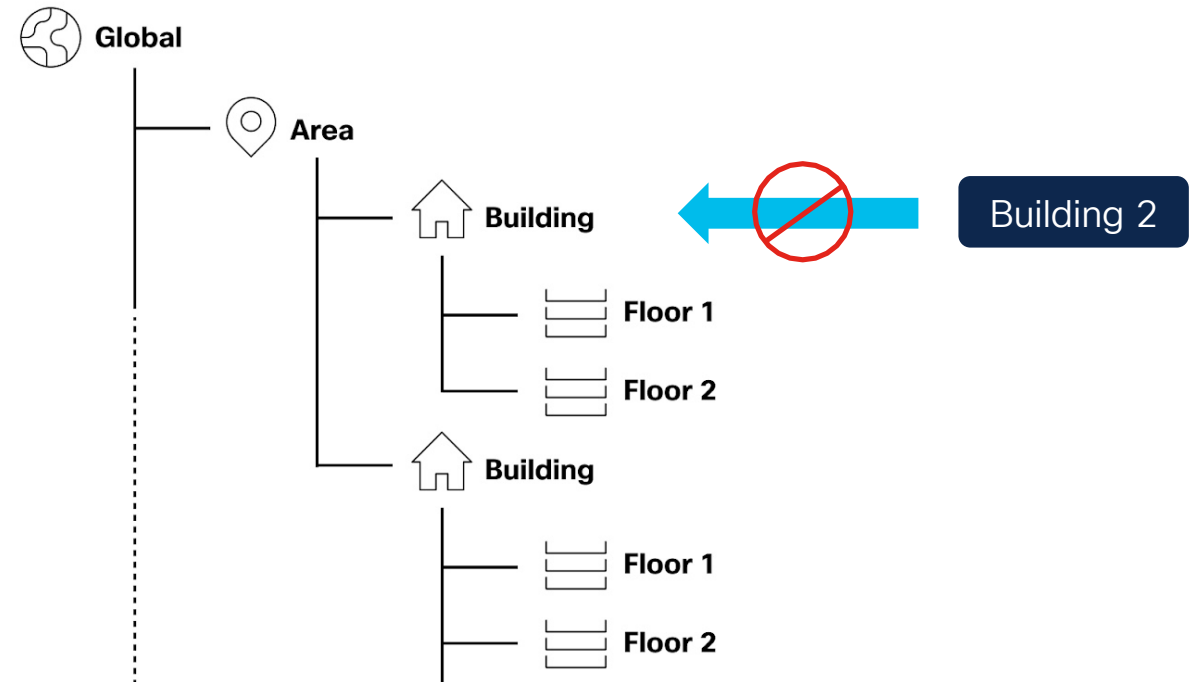


- ✓ If the building already exist, then the new floor is created
- ✓ If the building does not exist, then a new building is created with the floors

Catalyst Center-Ekahau Anchor Points



i Floor is not an anchor point to import a new floor



i Building is not an anchor point to import a new building

“Anchor Point” is the site or building in Catalyst Center Site Hierarchy where an Ekahau Project may be imported

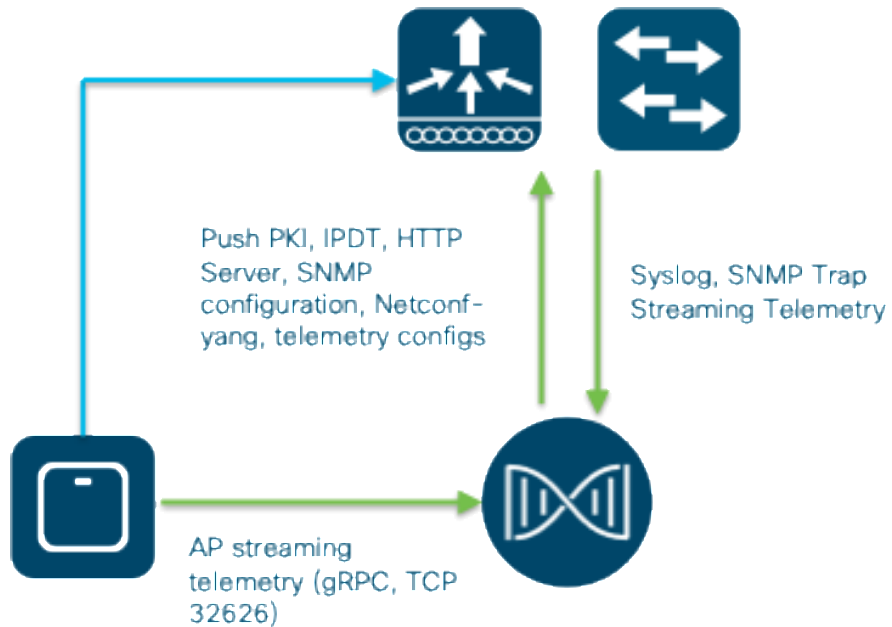
Catalyst Center- Network Heatmaps



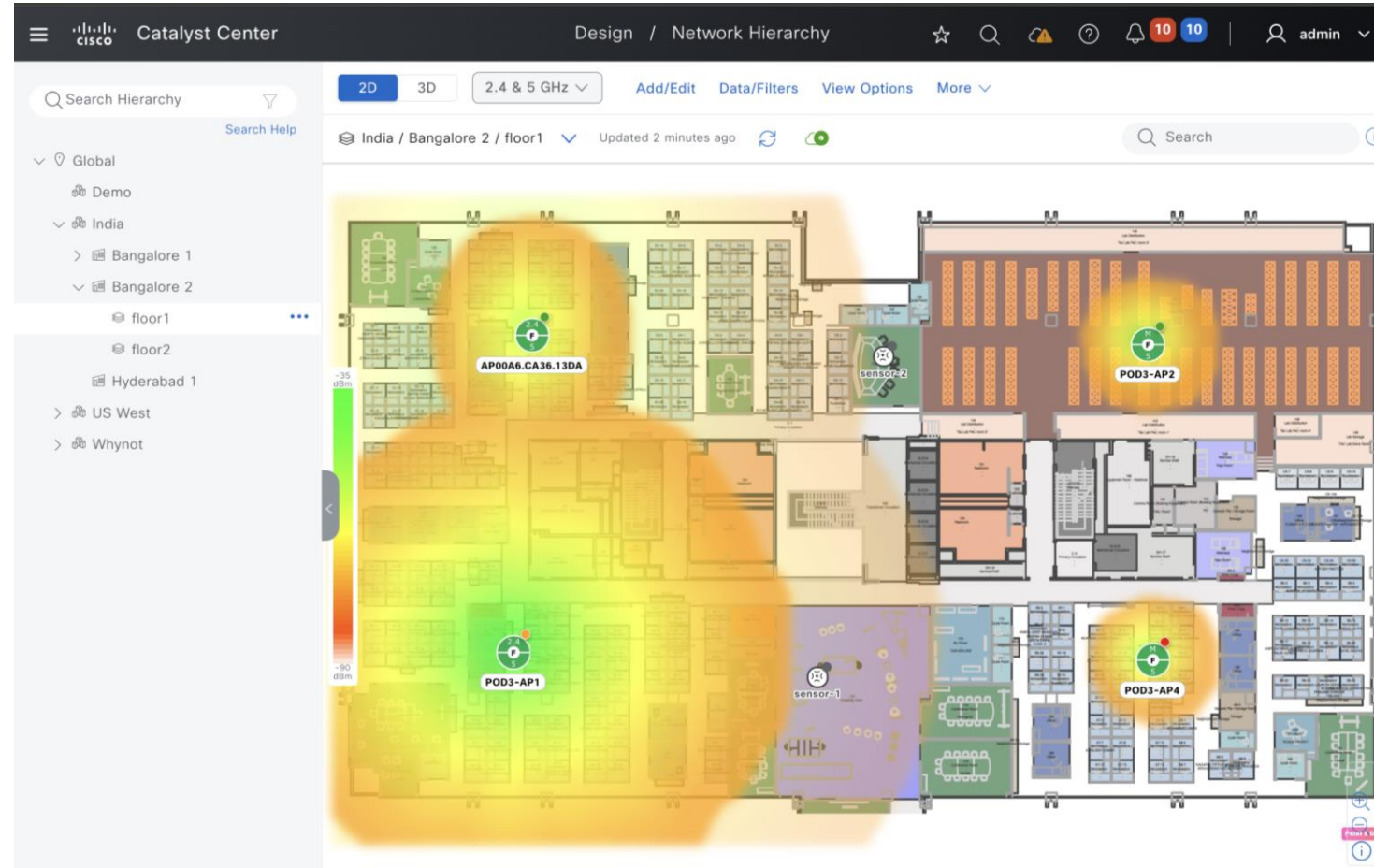
Onboarding devices to Catalyst Center



Assign devices to Sites Switches/WLC
to Buildings
AP to floor



cisco *Live!*



Integrating Cisco Spaces to Catalyst Center



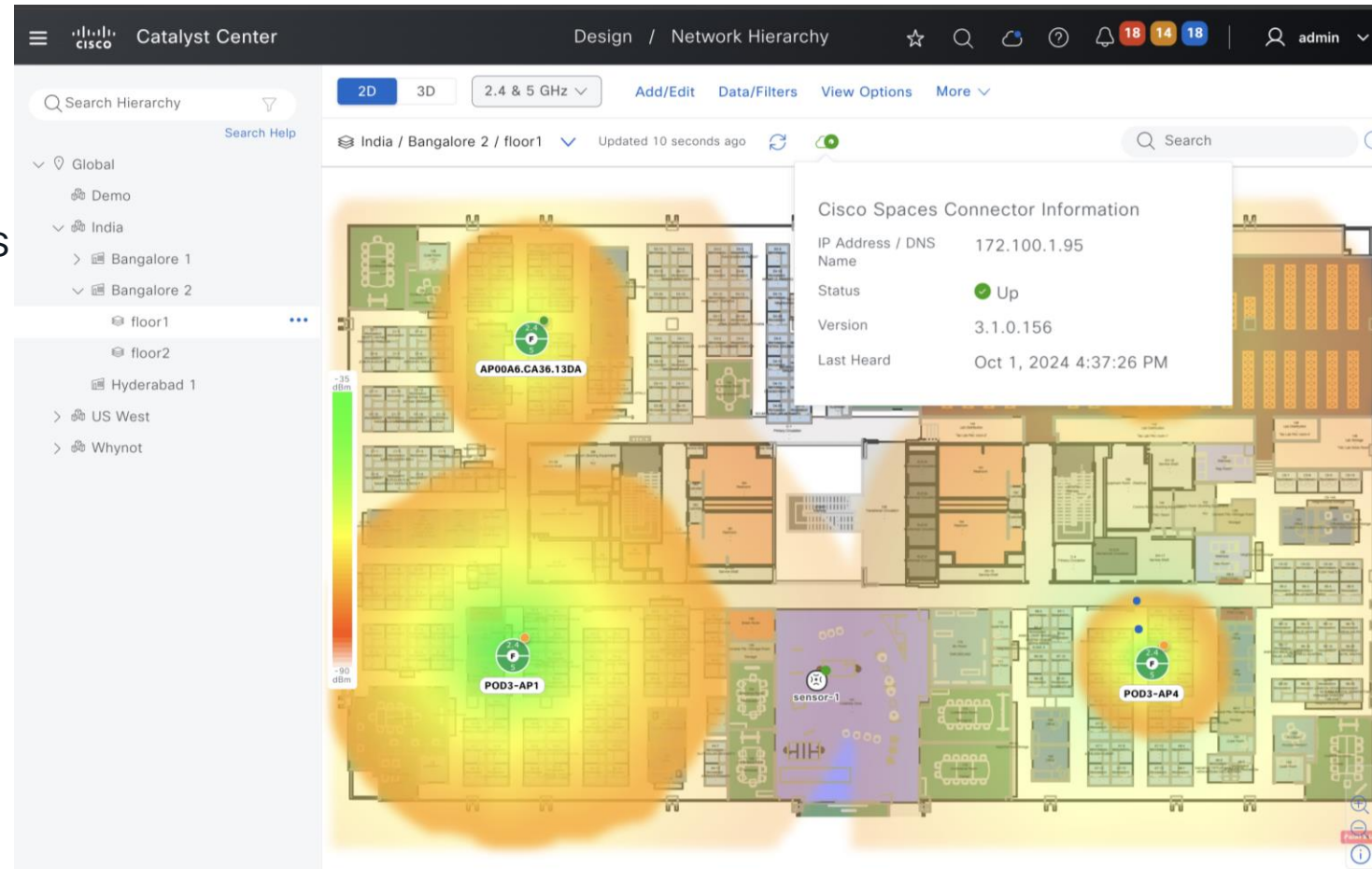
Maps uploaded from Catalyst Centre to Cisco spaces and visible in Cisco Spaces Map service.



Subsequent changes on the floor plan automatically pushed from Catalyst Centre to Map service.



Calculated locations of endpoints, rogues, interferers is continuously streamed from Cisco Spaces to Catalyst Centre



Integrating Cisco Spaces to Catalyst Center

The image displays two overlapping web interfaces. The background interface is the 'Cisco Spaces' dashboard, showing a list of instances. The foreground interface is the 'Catalyst Center' 'Settings / External Services' page, specifically the 'Cisco Spaces/CMX Servers' configuration screen. A modal window titled 'Activate Cisco Spaces' is open on the right, providing instructions and a token for activation.

Cisco Spaces Dashboard (Background):

- Header: Spaces
- Left Sidebar: Dashboard, Home, Location Hierarchy, Integrations (selected), Configure, Monitor, Admin Management, IoT Services, Setup.
- Instances List:
 - POD4-DNAC** (Active)
 - Member ID: DNAC-Id:dc87bee55d6ee29e1231
 - Activated date: Mar 22, 2022
 - Dnac-pod3** (Active)
 - Member ID: DNAC-Id:55c6e7ce7b5306d82ca7
 - Activated date: Jul 10, 2024
 - CC-TME-Instance** (Not Activated)
 - Configure below token in Cisco Catalyst Center
 - Display Token button
 - Expiring in 2 days

Catalyst Center Settings (Foreground):

- Header: Catalyst Center, System / Settings
- Left Sidebar: Search, PnP Device Authorization, Device Prompts, Configuration Archive, External Services (selected), Authentication and Policy Servers, Integrity Verification, SD-Access Compatibility Matrix, IP Address Manager, Cloud Access Login, Cisco AI Analytics, Stealthwatch, Talos IP Reputation, Destinations, Cisco Spaces/CMX Servers (highlighted), Global Manager Integration, Machine Reasoning Engine, Cisco Catalyst Cloud, Webex Integration, ThousandEyes Integration, System Configuration, Debugging Logs.
- Main Content: Settings / External Services, Cisco Spaces/CMX Servers.
 - Instructions: To integrate Catalyst Center with Cisco Spaces, please provide the Cisco Spaces tenant token. To integrate Catalyst Center with CMX Servers, please provide the CMX Server credentials.
 - Cisco Spaces Status: Activate button, Activation Status: Not Registered, Tenant: None, Connection Status: N/A.
 - CMX Servers: 0 Selected, Add, Edit, Delete buttons. A table with columns for IP Address / DNS Name and Username is shown with 'No data to display'.

Activate Cisco Spaces Modal (Right):

- Title: Activate Cisco Spaces
- Instructions: Please follow below steps:
 - Step 1: Configure the connector and token in Cisco Spaces. See Guidelines.
 - Step 2: Copy and paste the tenant token to below field.
- Tenant Token*: A long alphanumeric string is displayed in a text box.
- Buttons: Cancel, Activate.

Adding WLC to Cisco Spaces

Map Spaces instance under Network Settings > Wireless

The screenshot shows the Cisco Catalyst Center web interface. The top navigation bar includes the Cisco logo, 'Catalyst Center', and a breadcrumb trail: 'Design / Network Settings / Wireless'. On the right of the bar are icons for favorites, search, alerts, help, and notifications. A left sidebar contains a 'Search Hierarchy' box and a tree view with 'Global' expanded, showing 'Demo', 'India', 'US West', and 'Whynot'. The main content area is titled 'Cisco Spaces/CMX Servers' and includes a sub-header 'All / Cisco Spaces'. Below this, it states 'Cisco Spaces settings are inherited by all children sites. Overrides done at the child level do not affect the parent.' There is a 'Location Services' section with a dropdown menu currently set to 'Cisco Spaces - GES-CSS-ENT' and a 'Clear' button.

Add WLC and Spaces connector to Cisco Spaces

Configure Spaces Connector

You will need a token to configure Spaces Connector. You need to connect to `https://<your connector IP>/` from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS proxy.

3 / 3 connector(s) active

[Create Connector](#)
[View Connectors](#)

Add Controllers

Add and associate controllers to your Cisco Spaces Connector(s)

1 / 1 controller(s) active

[Add Controllers](#)
[View Controllers](#)

Sample WLC config for WLC to talk to Spaces connector

```
en
conf t
nmsp enable
aaa new-model
username 000C298E1E2D mac aaa attribute list cmx_000C298E1E2D
aaa attribute list cmx_000C298E1E2D
attribute type password 23ee446dbe498de8f0359728ccdb8bba529298663e0280a31d46dbb5a6c7dd81
aaa authorization credential-download wcm_loc_serv_cert local
```


Search Hierarchy

Search Help

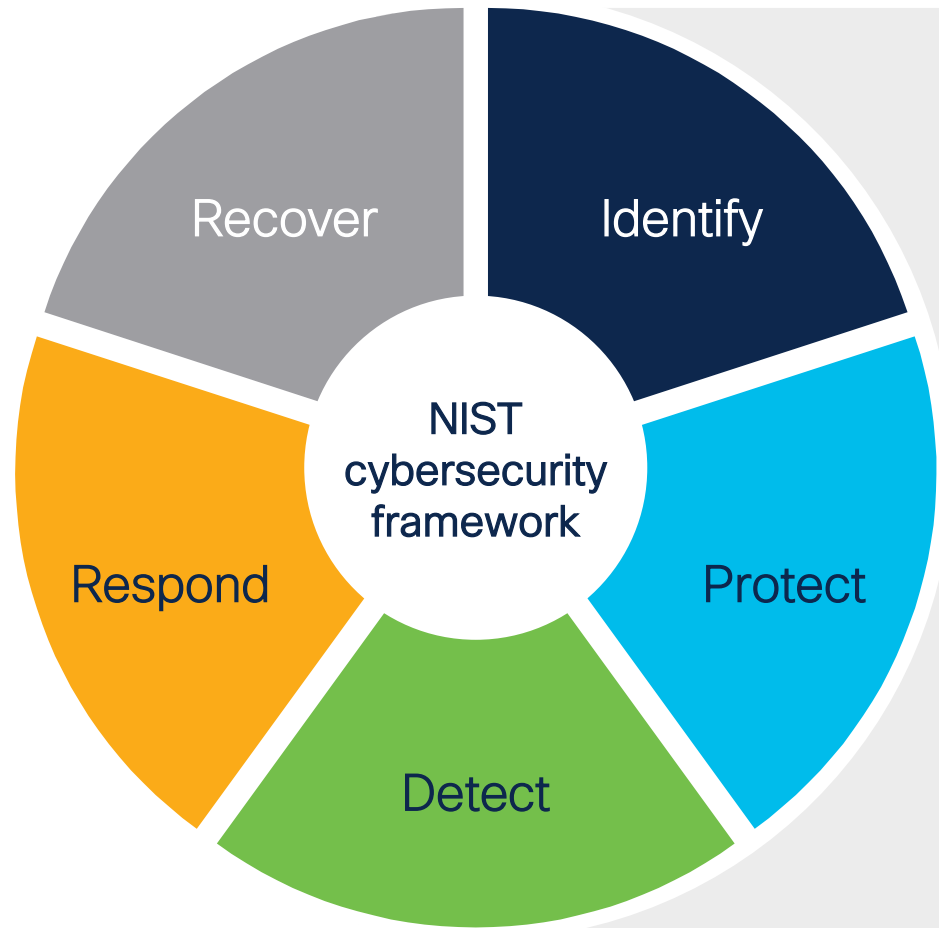
-  Global
 -  Demo
 -  India
 -  Bangalore 1
 -  Bangalore 2
 -  floor1
 -  floor2
 -  Hyderabad 1
 -  US West
 -  Whynot

 Add Site
  Import
  Export

 Search for a building



Device visibility and Network Segmentation are Critical



How do I know what's on my network?

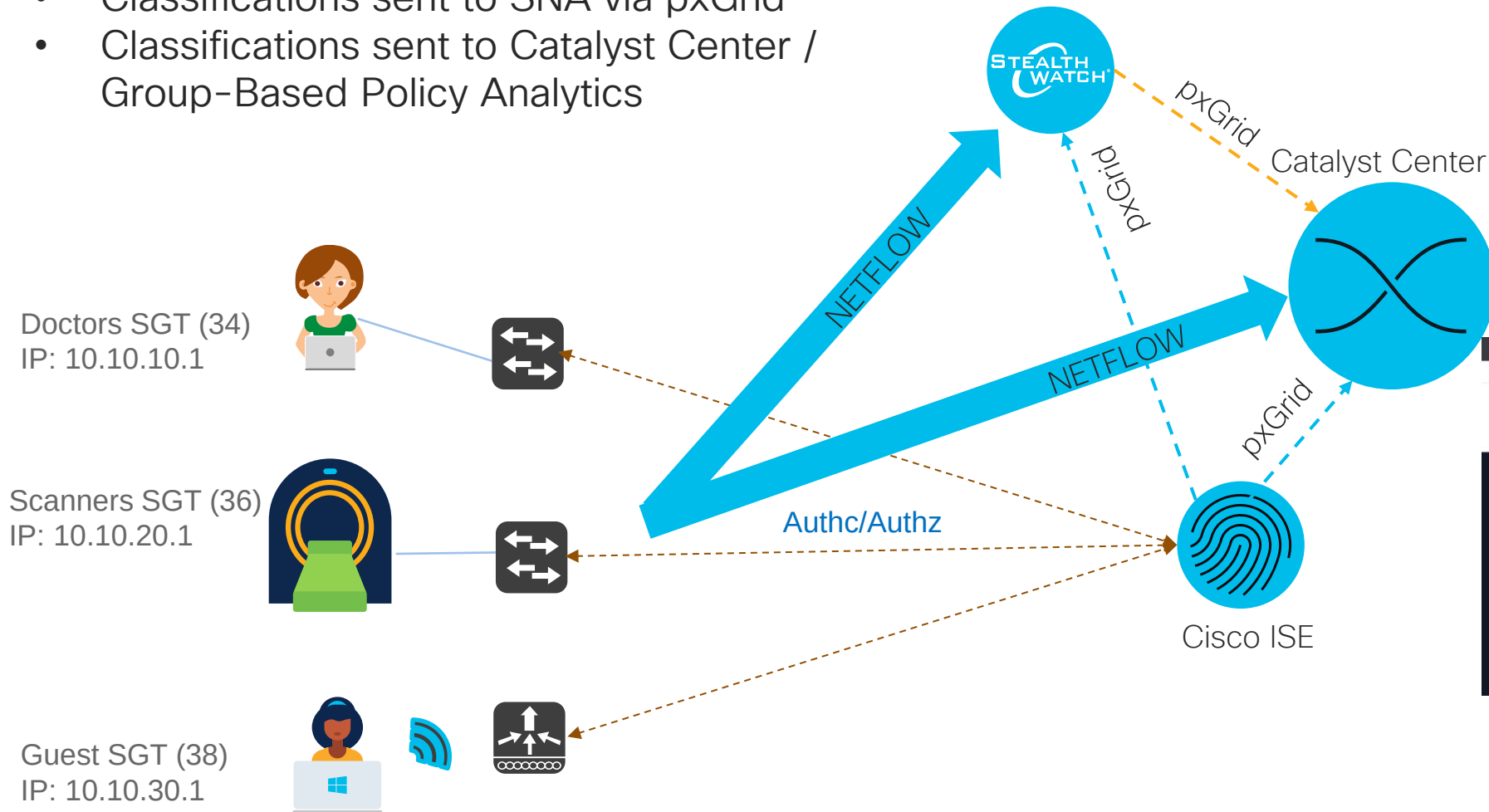
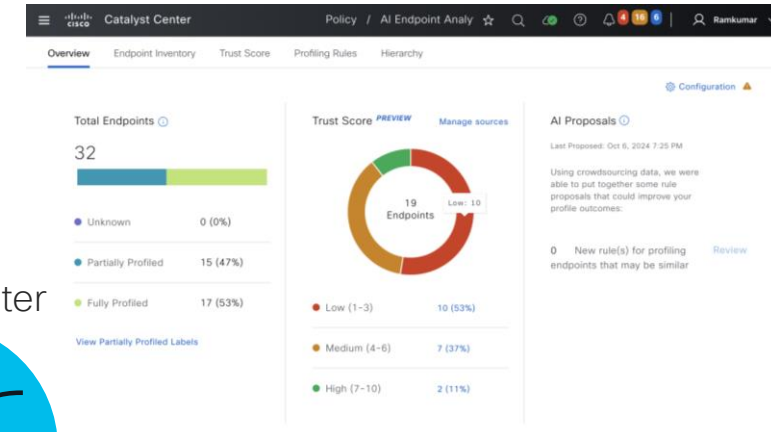
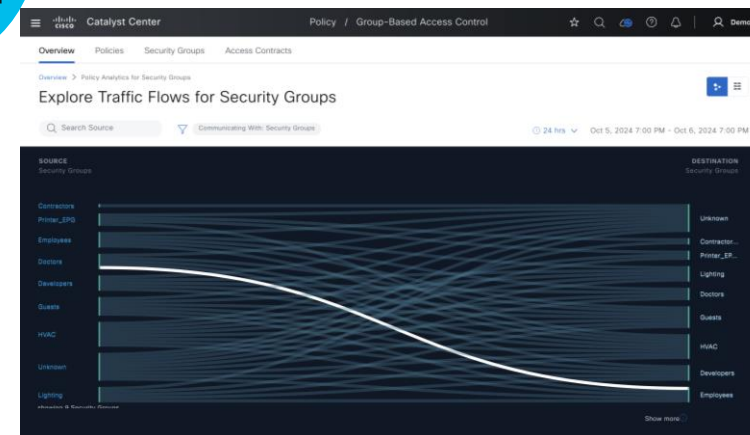
How do I make sure devices have right level of access?

How do I detect endpoint threats and vulnerability and contain it?



Classification, Leading to Visibility & Enforcement

- Classification: Dynamic/ISE
- Classifications sent to SNA via pxGrid
- Classifications sent to Catalyst Center / Group-Based Policy Analytics



Pre-Requisites

- ✓ ISE is Integrated in Catalyst Center
- ✓ AI Settings enabled on Catalyst Center for AI Endpoint Analytics and Talos settings
- ✓ Netflow is enabled on devices
- ✓ CBAR (SD-AVC) is enabled on devices
- ✓ Catalyst Center connected to Cisco Catalyst Cloud (Formerly Known as Cisco DNA Cloud).

Cisco ISE Integration – AI Endpoint Analytics

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

The screenshot displays the Cisco Catalyst Center web interface. The top navigation bar shows 'System / Settings' and the user 'admin'. The left sidebar contains a search bar and a list of settings categories. The 'External Services' category is highlighted, and the 'Authentication and Policy Servers' option is selected. The main content area shows the 'Authentication and Policy Servers' configuration page. It includes a description: 'Use this form to specify the servers that authenticate Catalyst Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.' Below this, there are 'Add' and 'Export' buttons. A table lists the configured servers:

IP Address	Protocol	Type	Status	Actions
172.100.1.99	RADIUS_TACACS	ISE	ACTIVE	...

Enabling AI Endpoint Analytics on CC

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

The screenshot shows the Cisco Catalyst Center web interface. The top navigation bar includes the Cisco logo, 'Catalyst Center', and a breadcrumb trail: 'System / Settings'. The left sidebar contains a search bar and a list of navigation items. 'External Services' is highlighted with an orange box, and its dropdown menu is open, showing 'Cisco AI Analytics' also highlighted with an orange box. The main content area is titled 'AI Endpoint Analytics' and describes its function: 'Provides fine-grained endpoint identification and assigns labels to a variety of Endpoints.' Below this, the 'ENDPOINT SMART GROUPING' section is shown, with a description: '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.' A toggle switch for 'Enable Endpoint Smart Grouping' is shown with a checkmark icon and is currently turned on. The 'AI SPOOFING DETECTION **PREVIEW**' section follows, with a description: 'AI Spoofing Detection will detect endpoints being spoofed based on behavioral models. Models are currently being built using collected flow information from devices.' A toggle switch for 'Enable AI Spoofing Detection' is also shown with a checkmark icon and is currently turned on. At the bottom of the main content area, there is an 'Update' button and a section for 'Cloud Data Storage' showing 'Europe (Germany)' and a 'Deployment ID' of 'vemc1jx2'. A link to 'Download configuration file' is provided.

Search

Device Prompts

Configuration Archive

External Services

Umbrella

Authentication and Policy Servers

Integrity Verification

SD-Access Compatibility Matrix

IP Address Manager

Cloud Access Login

Cisco AI Analytics

Stealthwatch

Talos IP Reputation

Destinations

Cisco Spaces/CMX Servers

Global Manager Integration

Machine Reasoning Engine

Cisco Catalyst Cloud

Webex Integration

ThousandEyes Integration

AI Endpoint Analytics

Provides fine-grained endpoint identification and assigns labels to a variety of Endpoints.

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

AI SPOOFING DETECTION **PREVIEW**

AI Spoofing Detection will detect endpoints being spoofed based on behavioral models. Models are currently being built using collected flow information from devices.

Enable AI Spoofing Detection

Update

Cloud Data Storage ⓘ

Europe (Germany)

Deployment ID ⓘ

vemc1jx2

[Download configuration file](#)

Network Settings Requirements for AI Endpoint Analytics



Ensure Catalyst Center as Netflow collector under **Design > Network Settings > Telemetry**



Alternative option is to use CTB as Netflow Destination



Strongly recommend to enable Wired Endpoint Data Collection

- Provides **granular** client information for Assurance, ISE accounting, and other features.
- Required setting for Software-Defined Access (**SDA**) fabric deployment

The screenshot shows the Cisco Catalyst Center interface. The top navigation bar includes 'Design / Network Settings'. The left sidebar shows a hierarchy: Global > Demo > India > US West > Whynot. The main content area is titled 'Telemetry' and contains the following sections:

- Application Visibility**: A section with a description and two radio button options. The first option, 'Use Catalyst Center as the Netflow Collector', is selected. The second option is 'Use Cisco Telemetry Broker (CTB) or UDP director'.
- Wired Endpoint Data Collection**: A section with a description and two radio button options. The first option, 'Enable Catalyst Center Wired Endpoint Data Collection At This Site', is selected. The second option is 'Disable Catalyst Center Wired Endpoint Data Collection At This Site'.

At the bottom right of the page, there are 'Reset' and 'Save' buttons.

Enabling Netflow on Devices- Switches



Enable Application Telemetry from
Provision > Actions > Telemetry >
Enable Application Telemetry

Catalyst Center Provision / Inventory

To provision subscriptions on devices that have not been discovered with NETCONF, rediscover the devices with NETCONF, and update the Telemetry Settings with the Force Configuration Push option.

Global

All Routers Switches Wireless Controllers Access Points Sensors

Devices (10) Focus: Inventory

deviceName: (*POD4*)

1 Selected Tag Add Device Edit Device Delete Device Actions

Tags Device Name IP Address Inventory Software Image Provision Telemetry Device Replacement Switch Refresh Compliance More

POD4

POD4-Anchor 192.168.4.16 NA

POD4-AP1 192.168.4.17 NA

POD4-AP2 192.168.4.18 NA

POD4-AP3 192.168.4.19 NA

POD4-AP4 192.168.4.20 NA

POD4-C9300-Access1.tmelab.com 192.168.4.4 Cisco

POD4-C9800-CL1.tmelab.com 192.168.4.7 Cisco

Reachability EoX Status Manageability Compliance Site

Managed Non-Compliant Assign

Managed NA .../Bang

Managed NA Assign

Reachable Not Scanned Managed NA Assign

Reachable Not Scanned Managed NA Assign

Reachable 1 alert Managed Non-Compliant .../Bang

Reachable 1 alert Managed Non-Compliant .../India

As of: Oct 6, 2024 3:45 PM

Enabling Netflow on Devices - WLC

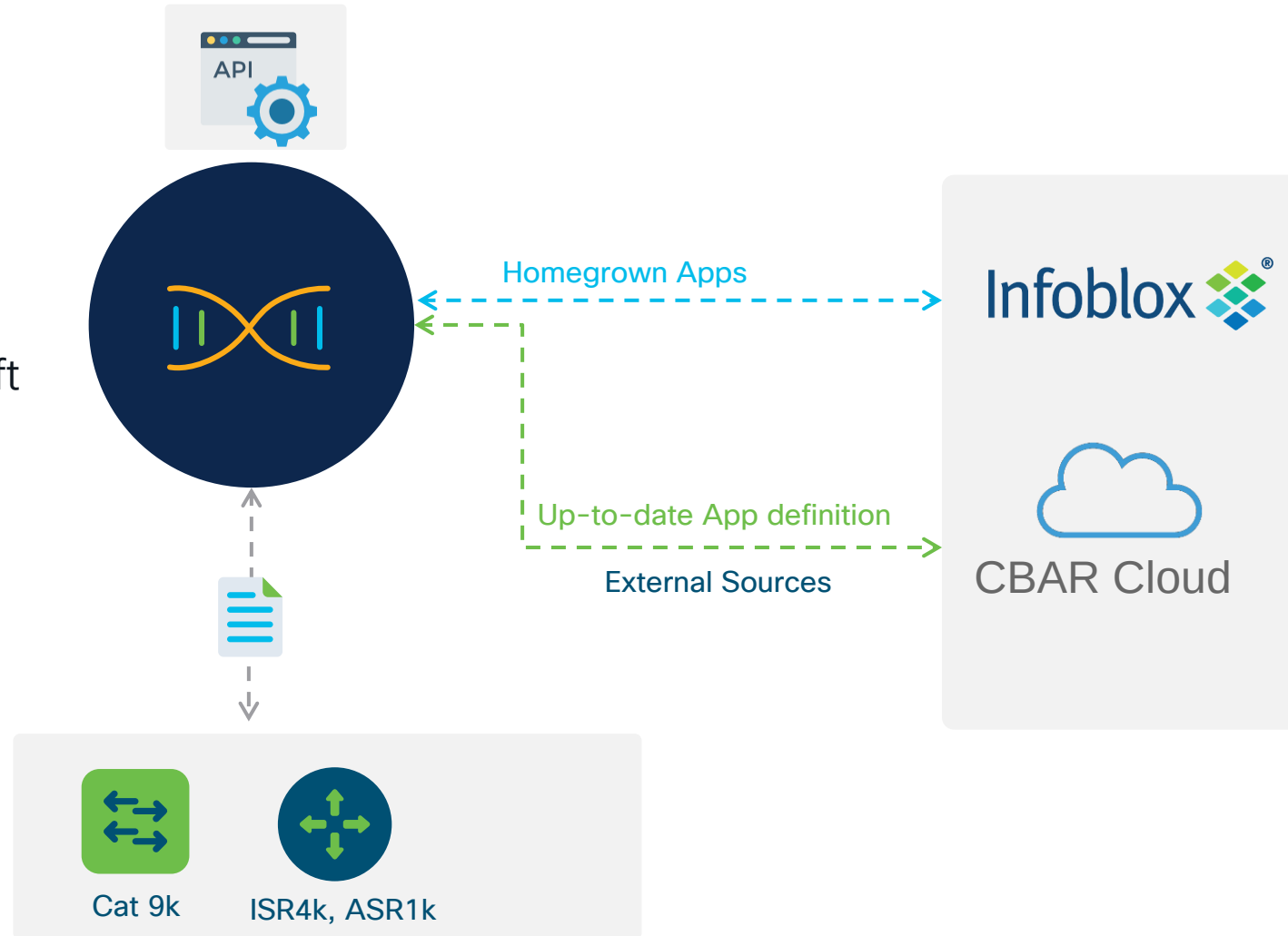
- ✓ Enable Application Telemetry from Provision > Actions > Telemetry > Enable Application Telemetry
- i WLC need not be provisioned for enabling Application telemetry
- i Supported for local, Flex/Fabric SSIDs

The screenshot displays the Cisco Catalyst Center web interface. The top navigation bar shows 'Catalyst Center' and 'Provision / Inventory'. The left sidebar indicates 'Global' and 'Devices (4)' with a focus on 'Provision'. A table lists devices: 'WLC', 'POD4-C9800-CL1', 'POD4-3504-1', and 'C9800-vWLC'. The 'POD4-C9800-CL1' device is selected, and the 'Telemetry' action is chosen from the dropdown menu. The main panel, titled 'Enable Application Telemetry', provides instructions on enabling Netflow with application telemetry on wireless controllers. It includes a warning about network disruption and a note about disabling and re-enabling telemetry for updates. For the selected device 'POD4-C9800-CL1', the 'Local' option is selected under 'Telemetry Source', and 'Include Guest SSIDs' is unchecked. The 'Telemetry Source' is set to 'NetFlow'. At the bottom right, there are 'Cancel' and 'Enable' buttons.

CBAR- Application Visibility Service

- Enrichment of Application Registry through exploration of un-classified applications
- Protocol Pack Updates for default NBAR application signatures and ports
- Connecting to external sources like Microsoft Endpoints to update Microsoft O365 Signatures

Identify voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based applications.



Enabling CBAR on Devices

- ✓ Enable CBAR from Provision > Application Visibility
- i Device Role needs to be Access for it be Ready

Catalyst Center

Provision / Services / Application Visibility

6146

admin

Service Catalog / Application Visibility

Search Hierarc

Search Help

Global

Demo

India

US West

Whynot

Overview

Network Devices Enablement

1479 Applications

28 Application Sets

CBAR Extensions

Site Devices (22)

Device Family: All, Routers, Switches, Wireless Controllers, More · 1

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

CBAR Readiness: All, Ready, More · 2

Telemetry Readiness: All, Ready, More · 2

Filter

CBAR

Application Telemetry

Update Protocol Pack

	Device	IP	Active recognition method	CBAR Deployment Status	Application Telemetry Readiness Status
☐	Dev				
☐	980	73	Network-based (NBAR)	Not deployed	Enabled
☐	C93	199	Network-based (NBAR)	Not deployed	Ready
☐	C9300-Edge	192.168.2.9	Network-based (NBAR)	Not deployed	Not ready
☐	C9300Access-1-Pod2.cisco.com	172.100.1.199	Network-based (NBAR)	Not deployed	Not ready
☐	C9300Access-1-POD3.tmelab.com	192.168.3.3	Network-based (NBAR)	Not deployed	Ready
☐	C9300Access-2-Pod2.tmelab.com	192.168.2.5	Network-based (NBAR)	Not deployed	Enabled
☐	CF-1	172.100.1.20	Network-based (NBAR)	Not deployed	Not ready



Enabling CBAR on Devices

- ✓ Enable CBAR from Provision > Application Visibility
- i Device Role needs to be Access for it be Ready
- ✓ Protocol Pack with latest signatures can be updated

The screenshot shows the Cisco Catalyst Center interface for Application Visibility. The 'Network Devices Enablement' tab is active, displaying a list of 22 site devices. The table includes columns for Device name, Management IP, Device Family, Active Recognition Method, and Application Telemetry Readiness Status. A context menu is open over the 'C9300-3-Pod2.tmelab.com' device, showing options like 'Update All Devices', 'Update Selected Devices', 'Update Selected Devices From File', 'Auto Update' (with a toggle switch), 'Include Selected Devices', and 'Exclude Selected Devices'.

Device name	Management IP	Device Family	Active Recognition Method	Application Telemetry Readiness Status
9800_Brownfield.tmelab.com	172.100.1.1	Access	CBAR	Not deployed, Enabled
C9300-3-Pod2.tmelab.com	192.168.2.5	Access	CBAR	Not deployed, Ready
C9300-Edge	192.168.2.5	Access	CBAR	Not deployed, Not ready
C9300Access-1-Pod2.cisco.com	172.100.1.199	Access	CBAR	Not deployed, Not ready
C9300Access-1-POD3.tmelab.com	192.168.3.3	Access	CBAR	Not deployed, Ready
C9300Access-2-Pod2.tmelab.com	192.168.2.5	Access	CBAR	Not deployed, Enabled
CE-1	172.100.1.20	Access	CBAR	Not deployed, Not ready

CBAR Application Classification

- ✓ Discovered Applications Classified and Unclassified are shown
- ✓ Discovered Applications automatically categorized under Traffic Class
- ✓ Use “Import” to add the discovered applications to application registry.

The screenshot displays the Cisco Catalyst Center interface for Application Visibility. The top navigation bar includes the Cisco logo, 'Catalyst Center', and links to 'Provision', 'Services', and 'Application Visibility'. The user is logged in as 'admin'. The main content area is titled 'Service Catalog / Application Visibility' and shows '1482 Applications' and '31 Application Sets'. The 'CBAR Cloud' tab is active, displaying 'Discovered Applications'. A donut chart shows '947.2M Observed Traffic' with a breakdown: (88.2%) Classified, (11.8%) Unclassified, and various protocols like ipfix, netflow, snmp, ms-services, ssh, and Other. Below the chart, a table lists discovered applications with columns for Server Name, BW, Application Name, Application Set, and Traffic Class. The 'Import' button is highlighted with a blue box. A message box prompts the user to use 'Import' to add discovered server names as applications to the application registry.

Search Hierarc Search Help

Global

- Demo
- India
 - Bangalore 1
 - Bangalore 2
 - Hyderabad 1
- US West
- Whynot

Overview Network Devices Enablement 1482 Applications 31 Application Sets CBAR Extensions

CBAR Cloud Discovered Applications Infoblox

947.2M Observed Traffic

- (88.2%)Classified
 - (35.8%)ipfix
 - (17.5%)netflow
 - (9.3%)snmp
 - (7.6%)ms-services
 - (6.7%)ssh
 - (11.3%)Other
- (11.8%)Unclassified

Nov 10, 2024 12:21 PM - Nov 11, 2024 12:21 PM

(12)Server Name (11)Server IP/Port

Use "Import" to add the following discovered server names as applications to application registry.

Hide Ignored Applications

Filter Import Ignore Unignore

Server Name	BW	Application Name	Application Set	Traffic Class
☐ dnaservices.cisco.com	13.09 MB (0.7%)	dnaservices	general-misc	Transactional Data
☐ tools.cisco.com	0 Bytes	tools.cisco.c	general-misc	Transactional Data

Integrating with CBAR Cloud

- ✓ Starting 2.3.7.6, CBAR Cloud can be enabled with a toggle button.
- i Ensure, Catalyst Center is registered to Cisco Catalyst Cloud (see next slides for steps)

The screenshot shows the Cisco Catalyst Center interface. The top navigation bar includes the Cisco logo, 'Catalyst Center', and links for 'Provision / Services / Application Visibility'. The left sidebar shows a search hierarchy with options like 'Global', 'Demo', 'India', 'US West', and 'Whynot'. The main content area is titled 'Application Visibility' and has tabs for 'Overview', 'Network Devices Enablement', '1479 Applications', '28 Application Sets', and 'CBAR Extensions'. The 'CBAR Extensions' tab is active, showing a toggle switch for 'CBAR Cloud' which is currently set to 'Enable'. Below this, there are checkboxes for 'Improve network visibility by sharing telemetry' and 'CBAR Dynamic Application Feeds'. A section for 'Enable Application Feeds Update' shows a radio button selection for 'All' (selected) and 'Selected only'. A grid of application cards is displayed, each with a name, last update time, and number of applications. The cards include ServiceNow, HubSpot, Microsoft Intune, Zoom, Sugarcrm, RingCentral, Code42, Dropbox, SAP, Zscaler, Amazon Chime, and Webex. At the bottom right, there are 'Reset' and 'Apply' buttons.

Application	Last updated on	Applications
ServiceNow	Sep 27, 2024 20:51	1 applications
HubSpot	Sep 27, 2024 20:51	1 applications
Microsoft Intune	Sep 27, 2024 20:51	1 applications
Zoom	Sep 27, 2024 20:51	2 applications
Sugarcrm	Sep 27, 2024 20:51	1 applications
RingCentral	Sep 27, 2024 20:51	1 applications
Code42	Sep 27, 2024 20:51	1 applications
Dropbox	Sep 27, 2024 20:51	1 applications
SAP	Sep 27, 2024 20:51	1 applications
Zscaler	Sep 27, 2024 20:51	1 applications
Amazon Chime	Sep 27, 2024 20:51	2 applications
Webex	Sep 27, 2024 20:51	1 applications

Integrating Cisco Catalyst Cloud with Catalyst Center (2.3.7.6)

Once successfully integrated, connection status will be available under System > Settings > External Services > Cisco Catalyst Cloud

All the Applications can be viewed and enabled from the same navigation path

The screenshot shows the Cisco Catalyst Center interface. The left sidebar contains a navigation menu with the following items: Configuration Archive, External Services (expanded), Authentication and Policy Servers, Integrity Verification, SD-Access Compatibility Matrix, IP Address Manager, Cloud Access Login, Cisco AI Analytics, Stealthwatch, Talos IP Reputation, Destinations, Cisco Spaces/CMX Servers, Global Manager Integration, Machine Reasoning Engine, Cisco Catalyst Cloud (highlighted), Webex Integration, ThousandEyes Integration, System Configuration (expanded), Debugging Logs, Visibility and Control of Configur..., and Geo Map Settings.

The main content area is titled "Cisco Catalyst Cloud" and includes the instruction: "Use this page to register this Catalyst Center with Cisco Catalyst Cloud." A warning message states: "To allow automatic login from the Cisco cloud, manage Cloud Access Login in System Settings." Below this, a box displays registration details: Registered to Cisco Catalyst Cloud Portal, Registered by pi@gmail.com, Account AssuranceBlr, and Registered on 6 October 2024. A "De-register" button is present, with a note: "Click 'De-register' to unregister this Catalyst Center with Cisco Catalyst Cloud."

The "Applications (4)" section shows a table of applications as of Oct 6, 2024 6:08 PM. The table has columns for Name, Tenant Subscription Status, Category, Offers, Vendor, and Actions. The first two rows are highlighted with a blue box:

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

Integration Catalyst Center with Infoblox

Enable Infoblox from System > Settings > External Services > IP Address Manager

The screenshot shows the Cisco Catalyst Center interface. The left sidebar contains a search bar and a list of navigation items: PnP Device Authorization, Device Prompts, Configuration Archive, External Services (highlighted with a red box), Authentication and Policy Servers, Integrity Verification, SD-Access Compatibility Matrix, IP Address Manager (highlighted with a red box), Cloud Access Login, Cisco AI Analytics, Stealthwatch, Talos IP Reputation, Destinations, Cisco Spaces/CMX Servers, Global Manager Integration, Machine Reasoning Engine, Cisco Catalyst Cloud, Webex Integration, ThousandEyes Integration, System Configuration, and Debugging Logs. The main content area is titled 'Settings / External Services' and 'IP Address Manager'. It includes a description: 'Use this form to integrate with the external IP Address Manager (IPAM) server. The configuration is used to communicate with the IPAM server for management of IP addresses. Visit [IP Address Pools](#) to manage IP addresses after successful integration.' The form fields are: Server Name* (Infoblox, with a tooltip 'The host name of the IPAM server'), Server URL* (https://172.100.1.96, with a tooltip 'The URL of the IPAM server (for example: https://www.cisco.com)'), Username* (admin, with a tooltip 'The IPAM server login user name'), Password* (empty, with a tooltip 'The password for the login user name'), Provider* (INFOBLOX, with a dropdown arrow), View* (default, with a tooltip 'Choose the view under which pools are created in IPAM server'), and a checkbox 'Sync global pools from IP Address Pools to the selected view from IPAM server.' at the bottom. At the bottom of the form are 'Delete' and 'Save' buttons. On the right side of the image, there are five blue arrows pointing to the form fields with corresponding labels: 'Server Name', 'URL/IP address of IPAM Server', 'Credentials of the IPAM Server', 'Provider Infoblox/Bluecat/Gener ic', and 'View to sync IP address pools created in CC to be synced in IPAM (For SDA Use Cases)'.

Search

PnP Device Authorization

Device Prompts

Configuration Archive

External Services

Authentication and Policy Servers

Integrity Verification

SD-Access Compatibility Matrix

IP Address Manager

Cloud Access Login

Cisco AI Analytics

Stealthwatch

Talos IP Reputation

Destinations

Cisco Spaces/CMX Servers

Global Manager Integration

Machine Reasoning Engine

Cisco Catalyst Cloud

Webex Integration

ThousandEyes Integration

System Configuration

Debugging Logs

Settings / External Services

IP Address Manager

Use this form to integrate with the external IP Address Manager (IPAM) server. The configuration is used to communicate with the IPAM server for management of IP addresses. Visit [IP Address Pools](#) to manage IP addresses after successful integration.

Server Name*

Infoblox

The host name of the IPAM server

Server URL*

https://172.100.1.96

The URL of the IPAM server (for example: https://www.cisco.com)

Username*

admin

The IPAM server login user name

Password*

The password for the login user name

Provider*

INFOBLOX

View*

default

Choose the view under which pools are created in IPAM server

☐ Sync global pools from IP Address Pools to the selected view from IPAM server.

Delete Save

Server Name

URL/IP address of IPAM Server

Credentials of the IPAM Server

Provider
Infoblox/Bluecat/Gener ic

View to sync IP address pools created in CC to be synced in IPAM (For SDA Use Cases)

Enhancing CBAR with Infoblox DNS TXT/ A-Records

- ✓ Provide details on specific DNS Zones to inspect
- ✓ Inside the Zone, the inspection should happen on TXT Records/A Records
- ✓ Automatically add the resolved applications to Traffic Class and relevant Application set
- i Once Classified the classified applications are pushed to devices for NBAR enrichment

Catalyst Center

Provision / Services / Application Visibility

Service Catalog / Application Visibility

Search Hierarc Search Help

Global

Demo

India

US West

Whynot

Overview Network Devices Enablement

CBAR Cloud Discovered Applications

In order to poll Infoblox applications please c

Use "Im

Filter Import 0 Selected

Application Name Server

Infoblox Connector Settings

Click [Here](#) to Edit IPAM/DNS Server Credentials in Catalyst Center Settings

IPAM Server Details:

Server Name: Infoblox Server URL: https://172.100.1.96

☐ All DNS Zones DNS Zones to inspect* This field is required

Inspect

TXT Record

☒ Read Application name from ~~Route Name~~

extensible attribute: app-name AVC RRTYPE format

Default Traffic Class

Transactional Data

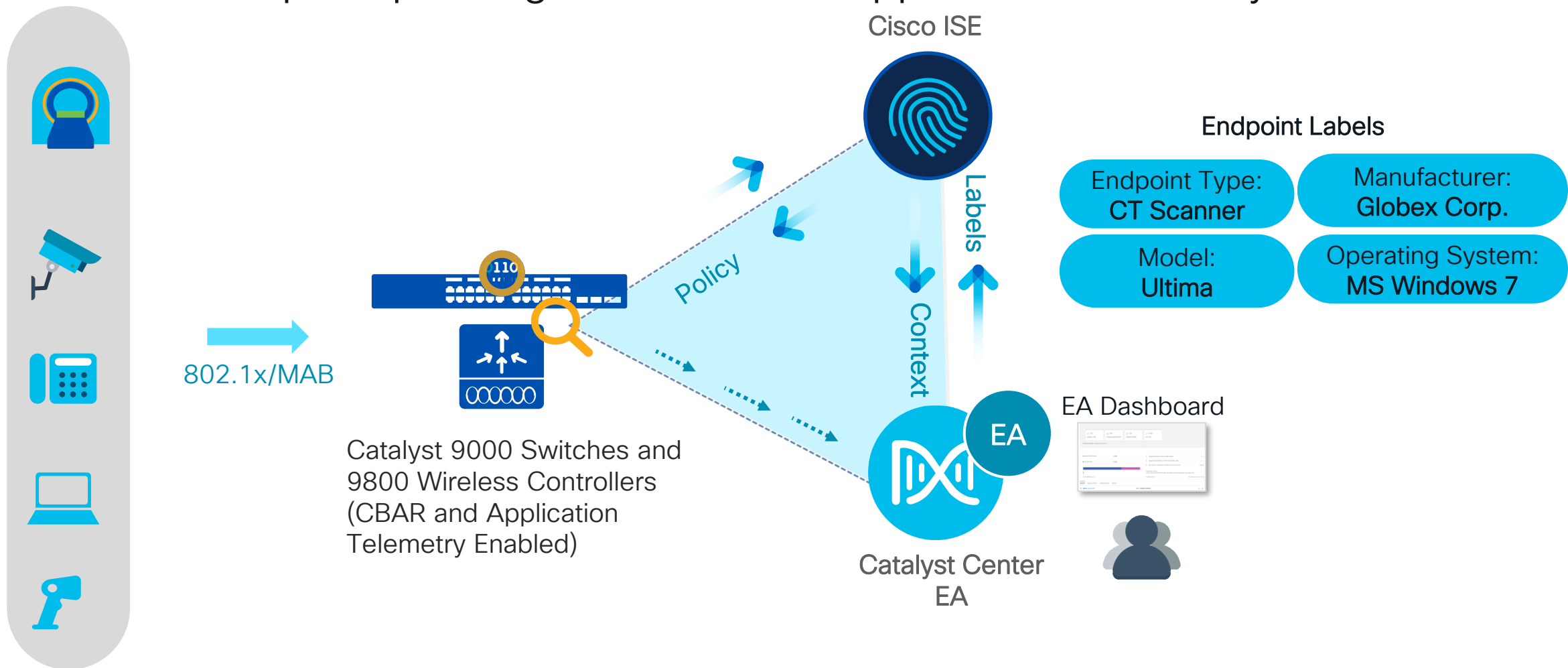
Default Application Set

local-services

Cancel Save

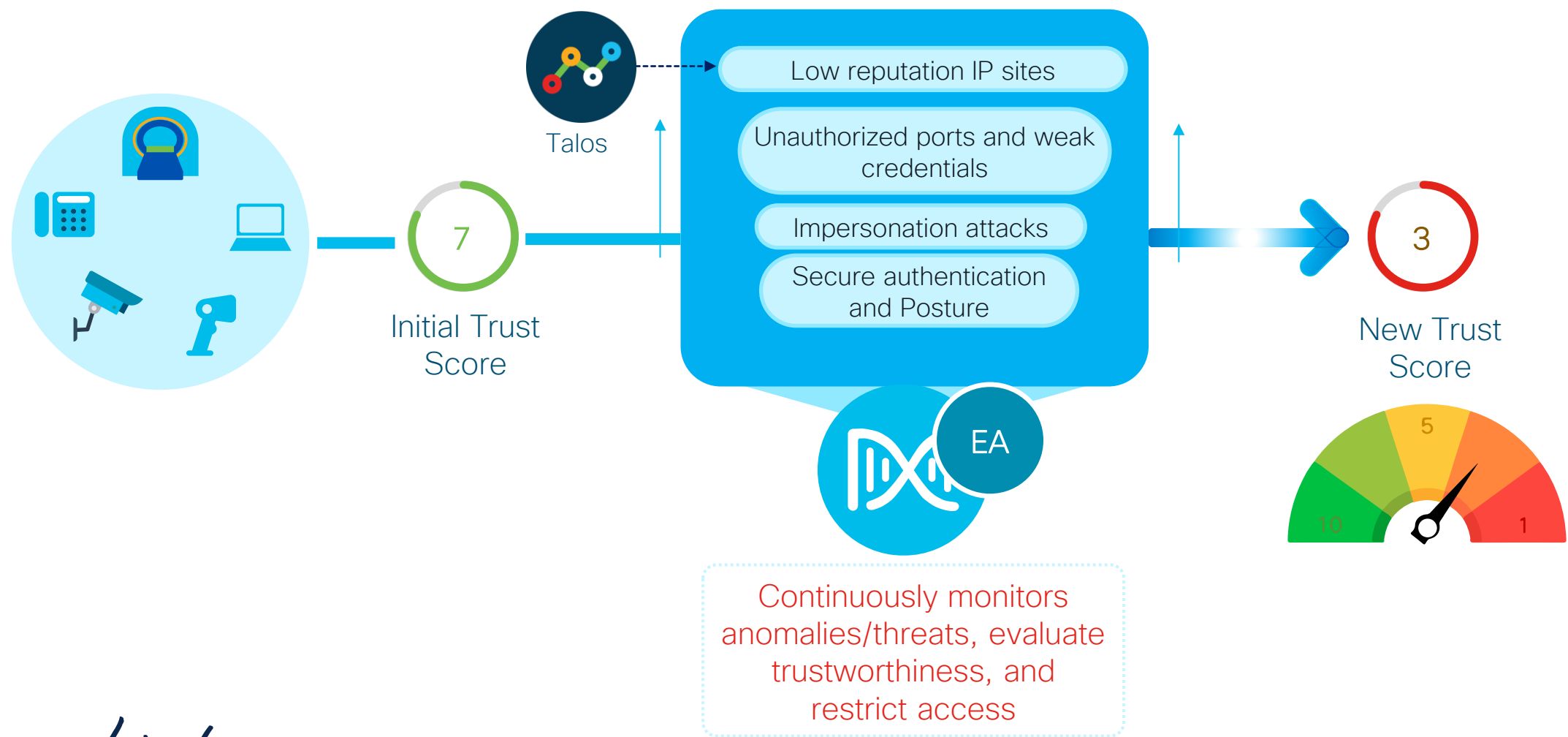
AI Endpoint Analytics

Endpoint profiling via CBAR and Application Telemetry



AI Endpoint Analytics

Continuous validation of endpoints for Trusted Access



AI Endpoint Analytics



Provides visibility on Endpoints which are Profiled and Unknown

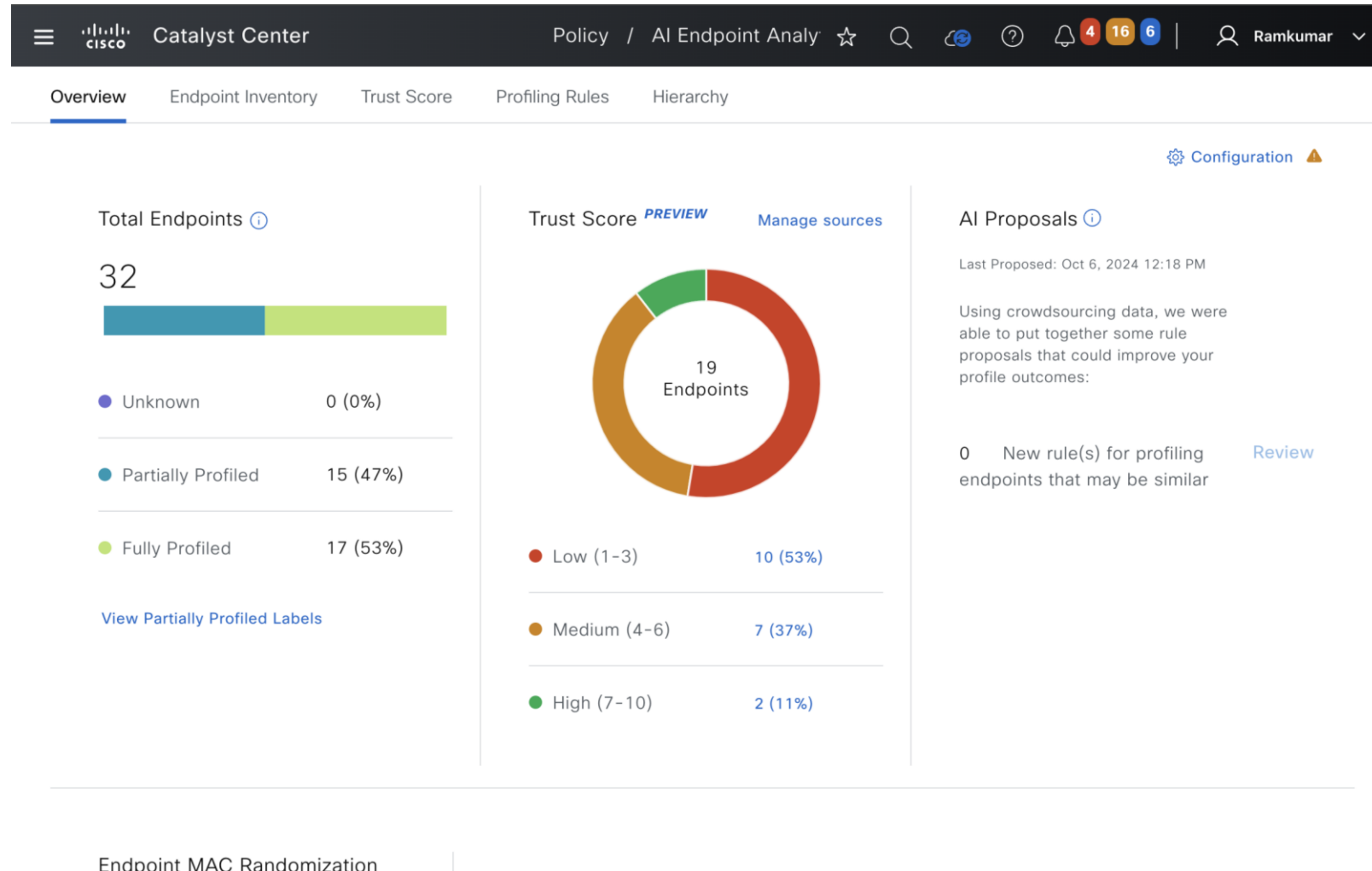


Provides Trust Score based on

- Authentication Method
- Posture
- Endpoint Attribute Conflict
- AI Spoofing Detection
- Open Port Scan
- Credential Vulnerabilities
- NAT Mode Detection
- Concurrent MAC Detection
- Talos IP Reputation



AI Proposals based on crowdsourced data for endpoint profiling



AI Endpoint Analytics

✓ Navigate to Endpoint Inventory to view the details on endpoints

✓ View the trust score of devices, endpoint type

Catalyst Center

Policy / AI Endpoint Analy ☆ 🔍 🔄 ⓘ 🔔 4 16 6 | 👤 Ramkumar ▾

Overview

Endpoint Inventory

Trust Score

Profiling Rules

Hierarchy

Endpoint Inventory (32) Focus: All Endpoints - Default View ▾ ⓘ Take a Tour ⚙️

🔍 Filter for endpoints by selecting values ▾

0 Selected

Register Endpoints

More Actions ▾

Export As of: Oct 6, 2024 12:21 PM 🔄

☐	MAC Address ⓘ	Is Random MAC	Trust Score ⓘ	IP Address	Last Seen	Hostname ⓘ	Endpoint Type
☐	00:50:56:A0:4F:78	No	● 3	10.5.1.135	Aug 28, 2024 2:05 PM	kernow-w7-1	Virtual-Machine
☐	00:50:56:A0:56:22	No	● 9	169.254.133.109	Sep 10, 2024 3:51 PM	kernow-w7-1	Virtual-Machine
☐	00:50:56:A0:6E:B2	No	● 3	10.4.1.129	Aug 28, 2024 2:05 PM	kernow-w7-1	Virtual-Machine
☐	00:50:56:A0:72:89	No	● 3	10.5.1.115	Aug 23, 2024 4:07 AM	kernow-w7-1	Test EP
☐	00:50:56:A0:A5:22	No	● 9	10.6.5.181	Sep 10, 2024 3:31 PM	kernow-w7-1	Virtual-Machine
☐	00:50:56:A0:B9:44	No	● 3	10.5.1.136	Aug 28, 2024 2:05 PM	kernow-w7-1	Virtual-Machine

32 Record(s) Show Records: 100 ▾ 1 - 32 < 1 >

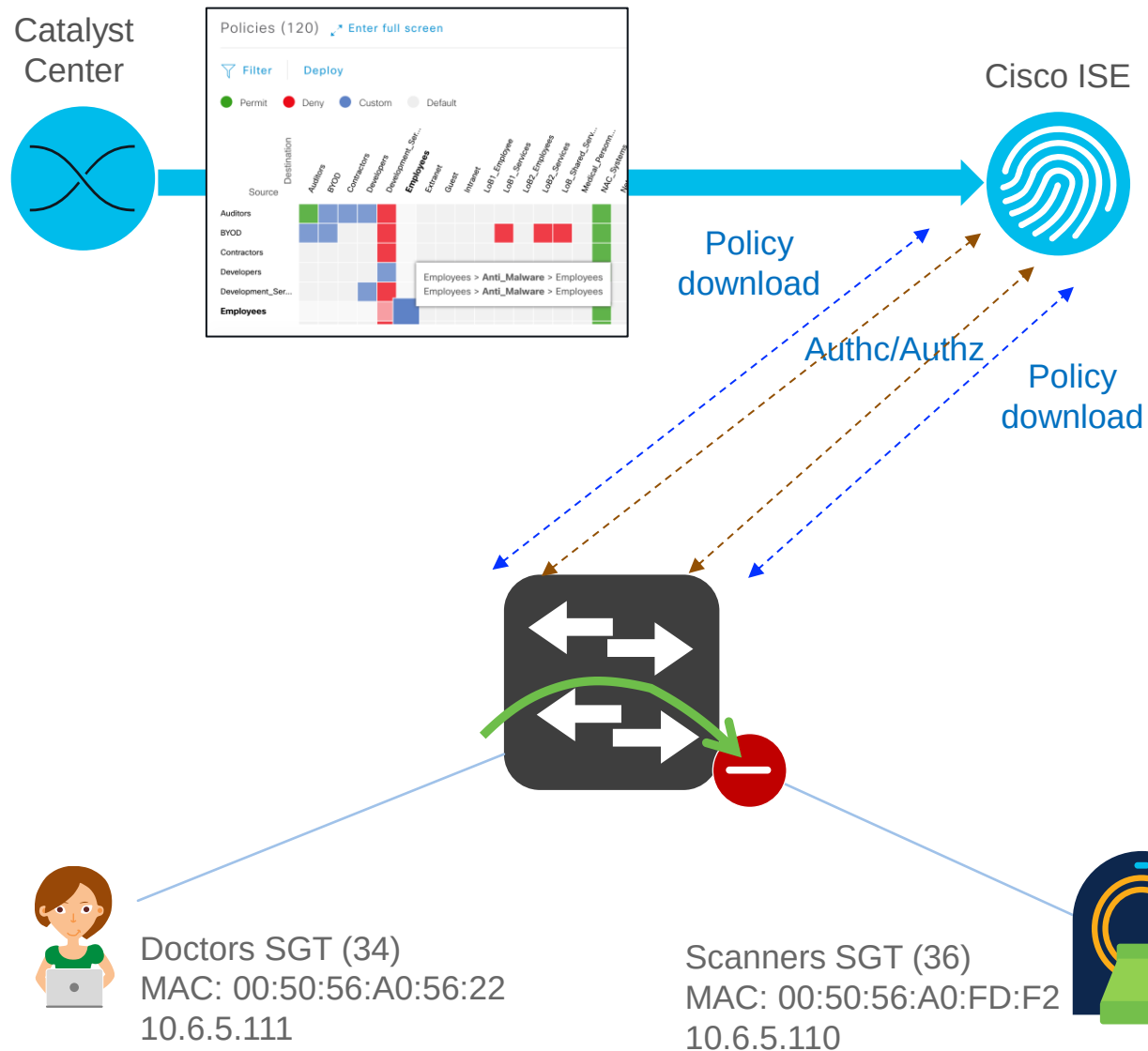
AI Endpoint Analytics

- ✓ Navigate to Endpoint Inventory to view the details on endpoints
- ✓ View the trust score of devices, endpoint type
- ✓ Select an endpoint to view Trust score context
- ✓ Use the ANC policy option to trigger a CoA for the endpoint and place in Quarantine policy

The screenshot displays the Cisco Catalyst Center AI Endpoint Analytics interface. The main table lists endpoints with their MAC addresses, whether they are random MACs, their trust scores, and IP addresses. The selected endpoint, 00:50:56:8F:4D:8C, has a trust score of 3, which is highlighted as low. A tooltip provides a warning about this low score. The right-hand pane shows the 'Trust Score' tab, which details the 'Endpoint Context' for the selected device. This context includes 'Talos IP Reputation' (Detected) and 'Talos Threat Level' (Untrusted). The interface also features a 'Reset Trust Score' button and an 'Apply ANC Policy' button.

MAC Address	Is Random MAC	Trust Score	IP
00:00:00:00:00:03	No	6	10
00:06:F6:EB:55:40	No	6	10
00:0C:29:4C:8B:F5	No	6	10
00:50:56:8F:4D:8C	No	3	10
00:50:56:A0:1A:50	No	3	10
00:50:56:A0:4F:78	No	3	10

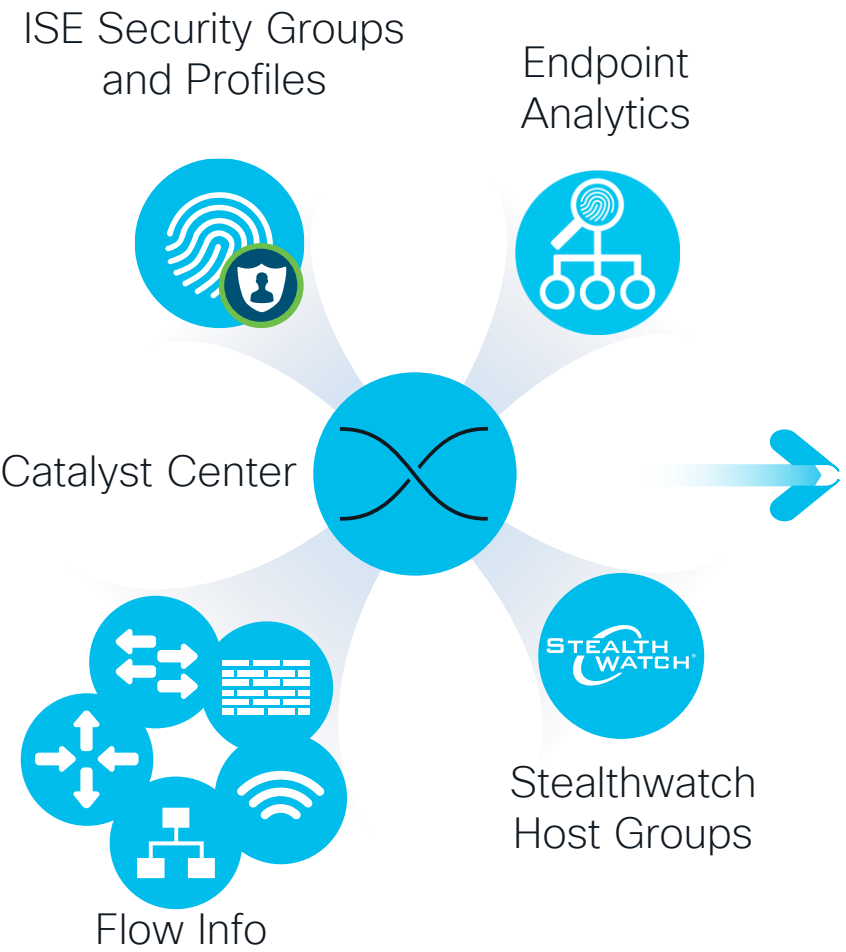
Classification, Leading to Visibility & Enforcement



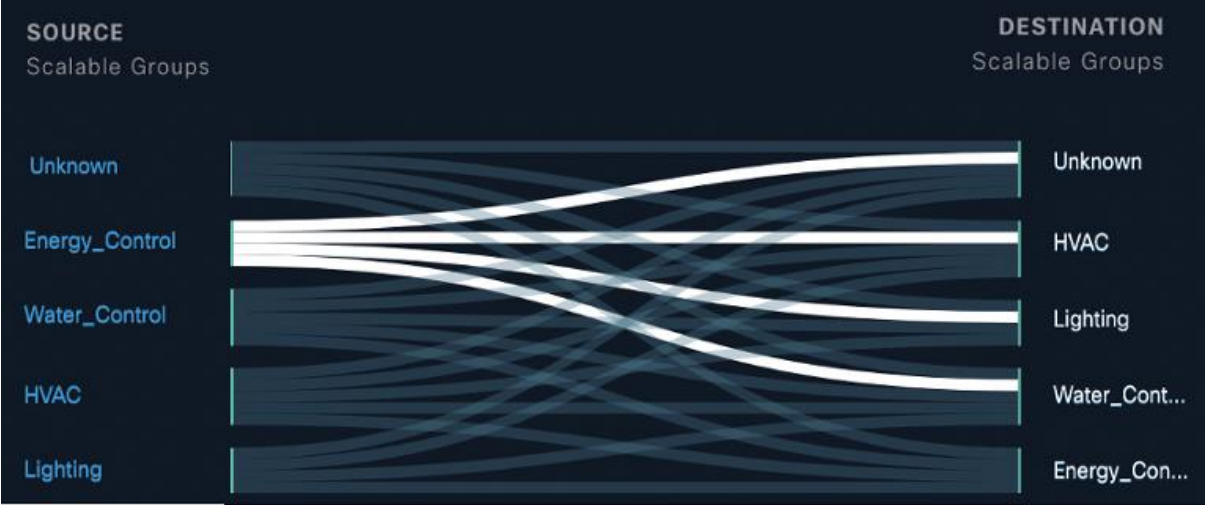
- Classification: Dynamic/ISE
- Src SGT found, Dst SGT found
- Enforcement: At Egress

		Destination	
Egress Policy		Doctors	Scanners
Source	Doctors	Permit All	Deny All
	PLC	Permit All	Deny All
	Scanners	Deny All	Permit All

Group-Based Policy Analytics



Group-Group Activity



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

Stealthwatch – Catalyst Center Integration

Integration with SNA Management Console through System → Settings

The screenshot shows the Cisco Catalyst Center web interface. The top navigation bar includes the Cisco logo, 'Catalyst Center', and a breadcrumb trail 'System / Settings'. The left sidebar contains a search bar and a list of settings categories: PnP AP Location, Image Distribution Servers, Device Controllability, Network Resync Interval, SNMP, ICMP Ping, Device EULA Acceptance, PnP Device Authorization, Device Prompts, Configuration Archive, External Services (highlighted with an orange box), Authentication and Policy Servers, Integrity Verification, SD-Access Compatibility Matrix, IP Address Manager, Cloud Access Login, Cisco AI Analytics, Stealthwatch (highlighted with an orange box), Talos IP Reputation, Destinations, Cisco Spaces/CMX Servers, and Global Manager Integration. The main content area is titled 'Settings / External Services' and 'Stealthwatch' (highlighted with an orange box). It contains instructions to use the page to associate Stealthwatch with Catalyst Center and to register a Stealthwatch Management Console. A form field for 'SMC IP Address or FQDN*' is populated with '172.100.1.98'. Below this, a warning message states: 'Certificate is not trusted for this IP address or FQDN. Please click the warning to learn more.' A blue arrow points from the text 'Click on warning to accept certificate' to the warning icon. The form also includes fields for 'Username*' (admin) and 'Password*'. At the bottom of the form are 'Delete' and 'Save' buttons. A modal dialog box is open, displaying the warning message and a checkbox labeled 'Allow Catalyst Center to access this IP address or FQDN and add the untrusted certificate to the Trusted Certificates', which is checked. A blue arrow points from the text 'Click on warning to accept certificate' to the 'Allow' button in the modal.

Settings / External Services

Stealthwatch

Use this page to associate Stealthwatch with Catalyst Center.

Register a Stealthwatch Management Console with Catalyst Center to integrate with Stealthwatch and utilize read-only APIs to retrieve the usable flow destinations for Stealthwatch Security Analytics.

SMC IP Address or FQDN*

172.100.1.98

Certificate is not trusted for this IP address or FQDN. Please click the warning to learn more.

Username*

admin

Password*

.....

Delete Save

The certificate associated with this IP address or FQDN is not trusted.

[Certificate details](#)

☒ Allow Catalyst Center to access this IP address or FQDN and add the untrusted certificate to the Trusted Certificates

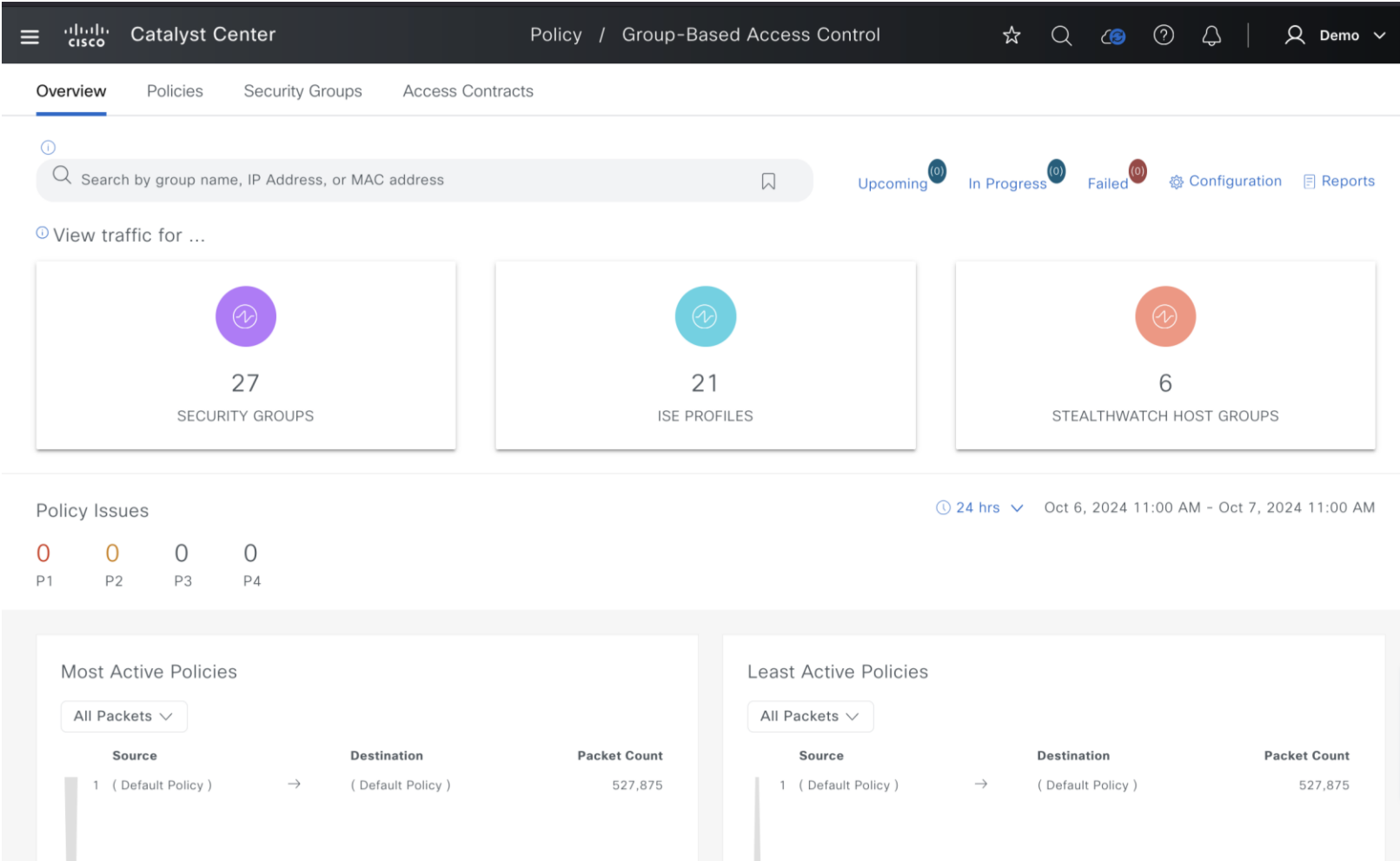
Allow

Ensure StealthWatch administrator accounts (those beside default “admin”) have logged in and changed password before using for integration (silent failure otherwise)

Group-Based Policy Analytics



Visualization of Flow data based on Security Groups, ISE Profiles, Stealthwatch Host Groups

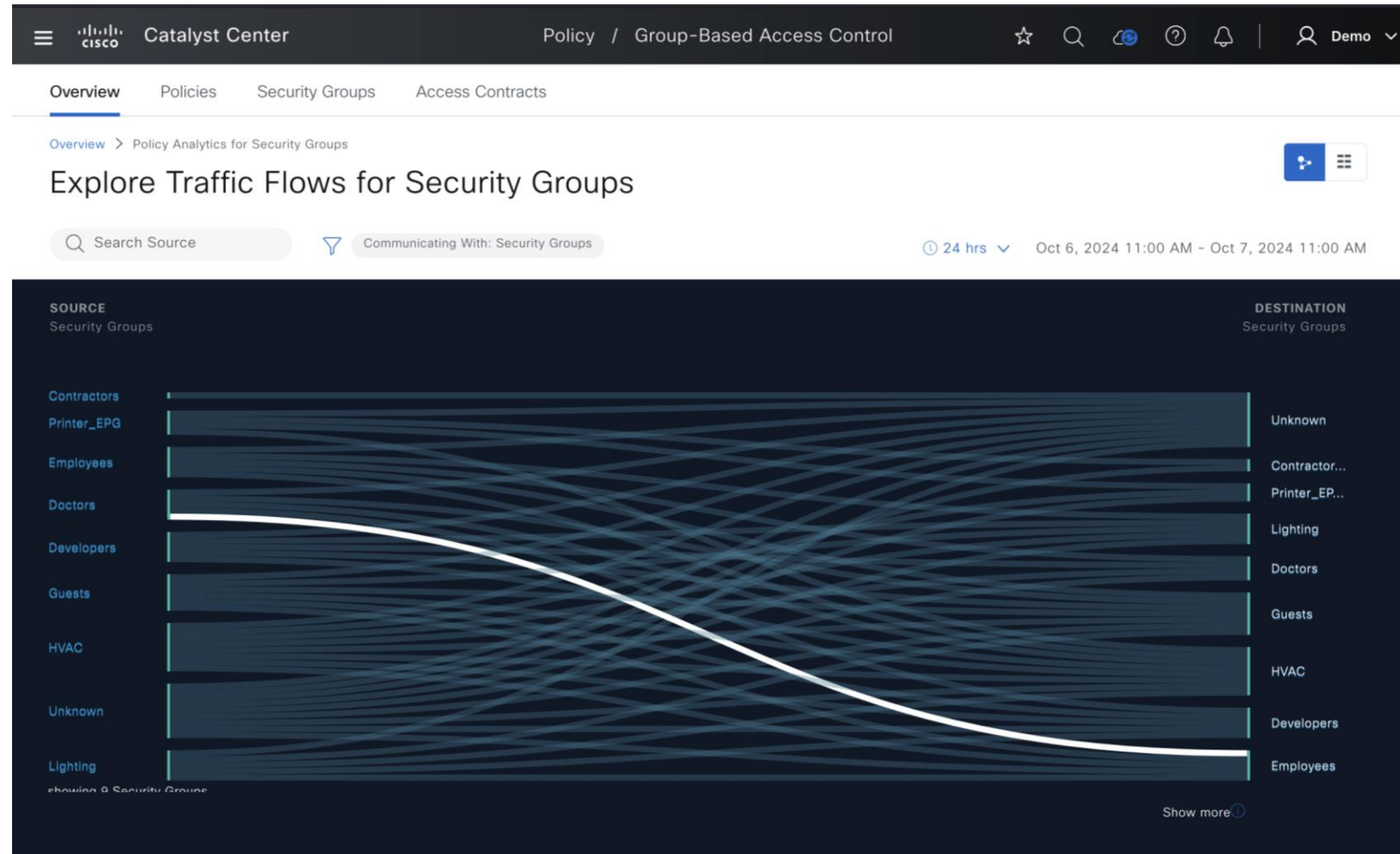


Group-Based Policy Analytics

✓ Visualization of Flow data based on Security Groups, ISE Profiles, Stealthwatch Host Groups

✓ Netflow export does not have SGT data.

✓ Relies on correlation of NetFlow data with mappings from ISE, EA, StealthWatch



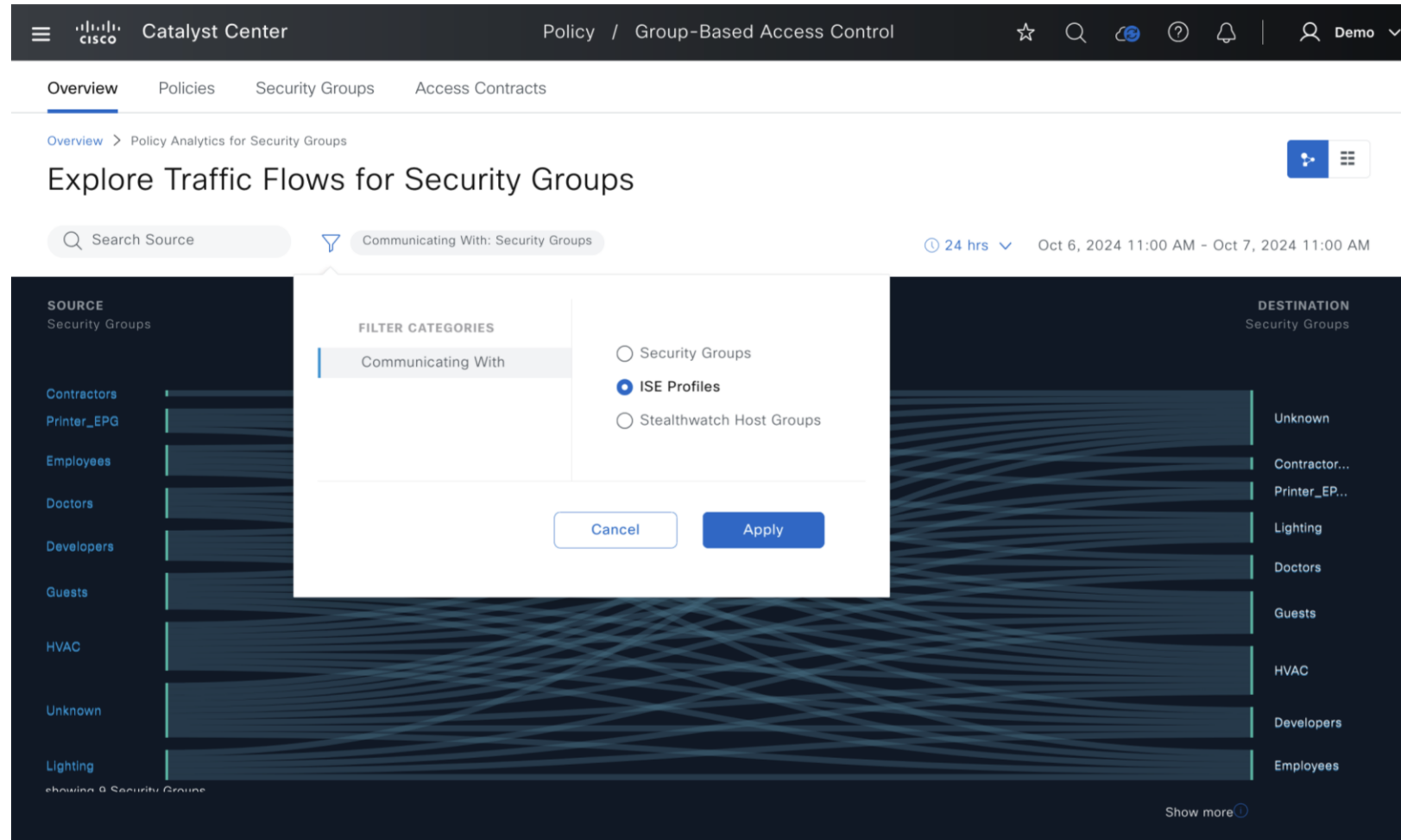
Group-Based Policy Analytics

✓ Visualization of Flow data based on Security Groups, ISE Profiles, Stealthwatch Host Groups

✓ Netflow export does not have SGT data.

✓ Relies on correlation of NetFlow data with mappings from ISE, EA, StealthWatch

✓ Visualization of Flows based on destination group types (Security Groups, ISE Profiles or Stealthwatch Host Groups)



Visualization of services and flow count based on group to group communication

Catalyst Center

Policy / Group-Based Access Control

Overview Policies Security Groups Access Contracts

Overview > Policy Analytics for Security Groups > Guests → HVAC > Contract Page

Guests → HVAC

> Policy Details

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

Search Table

#	Action	Application	Protocol	Source Port	Destination Port	Logging	Action
No data to display							

All Unique Traffic Flows 24 hrs Oct 1, 2024 12:00 PM - Oct 2, 2024 12:00 PM

Search Table

Direction	Service Name	Protocol	Port	Flow Count
↔	Unassigned	ICMP	0	32
↔	Unassigned	IGMP	0	30
↔	Unassigned	IPv6-ICMP	0	444
↔	ssh	TCP	22	24
↔	dns	TCP	53	13
↔	dns	UDP	53	263
↔	dhcp	UDP	67	207
↔	dhcp	UDP	68	58

Default Action Logging [View traffic](#)

95 Record(s) Show Records: 10 1 - 10

Group-Based Policy Analytics



Visualization of services and flow count based on group-to-group communication



Visualization of flows based on Netflow data

Catalyst Center

Policy / Group-Based Access Control

admin

Overview

Policies

Security Groups

Access Contracts

Overview

Policy Analytics for Security Groups

SGT Assignment Not Available

SGT Assignment Not Available

Contract Page

Endpoint List

SGT Assignment Not Available -> SGT Assignment Not Available

Port:0

Protocol: IPv6-ICMP

Service Name: Unassigned

Date Selected: Oct 1, 2024 12:00 PM - Oct 2, 2024 12:00 PM

Search Table

Source IP Address	Source MAC Address	Source Location	Destination IP Address	Destination MAC Address	Destination Location	Flow Count
ff02::2	70:F3:5A:79:FE:F1	UNRESOLVED	fe80::72f3:5aff:fe79:fef1	5C:E1:76:29:00:8C	UNRESOLVED	22
ff02::1:ff79:fef1	70:F3:5A:79:FE:F1	UNRESOLVED	::	5C:E1:76:29:00:8C	UNRESOLVED	21
ff02::2	70:F3:5A:7B:5B:51	UNRESOLVED	fe80::72f3:5aff:fe7b:5b51	5C:E1:76:29:00:8C	UNRESOLVED	21
ff02::1:ff7b:5b51	70:F3:5A:7B:5B:51	UNRESOLVED	::	5C:E1:76:29:00:8C	UNRESOLVED	20
ff02::1:ff7a:6a51	70:F3:5A:7A:6A:51	UNRESOLVED	::	5C:E1:76:29:00:8C	UNRESOLVED	17
ff02::2	70:F3:5A:7A:6A:51	UNRESOLVED	fe80::72f3:5aff:fe7a:6a51	5C:E1:76:29:00:8C	UNRESOLVED	15
::	70:F3:5A:7B:5B:51	UNRESOLVED	ff02::16	AC:4A:56:9B:9F:C0	UNRESOLVED	15
ff02::2	70:F3:5A:79:FE:F1	UNRESOLVED	fe80::72f3:5aff:fe79:fef1	5C:E1:76:28:F1:F4	UNRESOLVED	13
ff02::1:ff79:fef1	70:F3:5A:79:FE:F1	UNRESOLVED	::	5C:E1:76:28:F1:F4	UNRESOLVED	13

Show Records: 10

1 - 10

Group-Based Policy Analytics

✓ Visualization of services and flow count based on group to group communication

✓ Visualization of flows based on Netflow data

✓ Ability to add/modify contracts to be pushed to ISE for policy enforcement

Catalyst Center

Policy / Group-Based Access Control

Overview Policies Security Groups Access Contracts

Overview > Policy Analytics for Security Groups > SGT Assignment Not Available > SGT Assignment Not Available > Contract Page

SGT Assignment Not Available → SGT Assignment Not Available Default

> Policy Details

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

CONTRACT CONTENT (1)

#	Action *	Application *	Transport Protocol	Source / Destination	Port	Logging	Action
1	Select Value*	Select Value*	Select Value*	Destination		☐	+ ×

Default Action Permit Logging ☐

Cancel Next

All Unique Traffic Flows 24 hrs Oct 6, 2024 12:00 PM - Oct 7, 2024 12:00 PM

Search Table

Direction	Service Name	Protocol	Port	Flow Count	Action
→	Unassigned	ICMP	0	18	Add to contract
→	Unassigned	IGMP	0	9	Add to contract
↔	Unassigned	IPv6-ICMP	0	337	Add to contract
↔	ssh	TCP	22	25	Add to contract
↔	dns	TCP	53	4	Add to contract
↔	dns	UDP	53	141	Add to contract
↔	dhcp	UDP	67	186	Add to contract
→	dhcp	UDP	68	57	Add to contract

103 Record(s) Show Records: 10 1 - 10 < >

Integrations for (Network) Assurance/Monitoring



Scenario- Application Experience



Not able to connect to my application



Helpdesk

Authentication Problem?, RF Issue or app problem?

Network is stable. Must be the app.



Network Ops



IT Routing Loop

Code is fine. Don't care about anything else

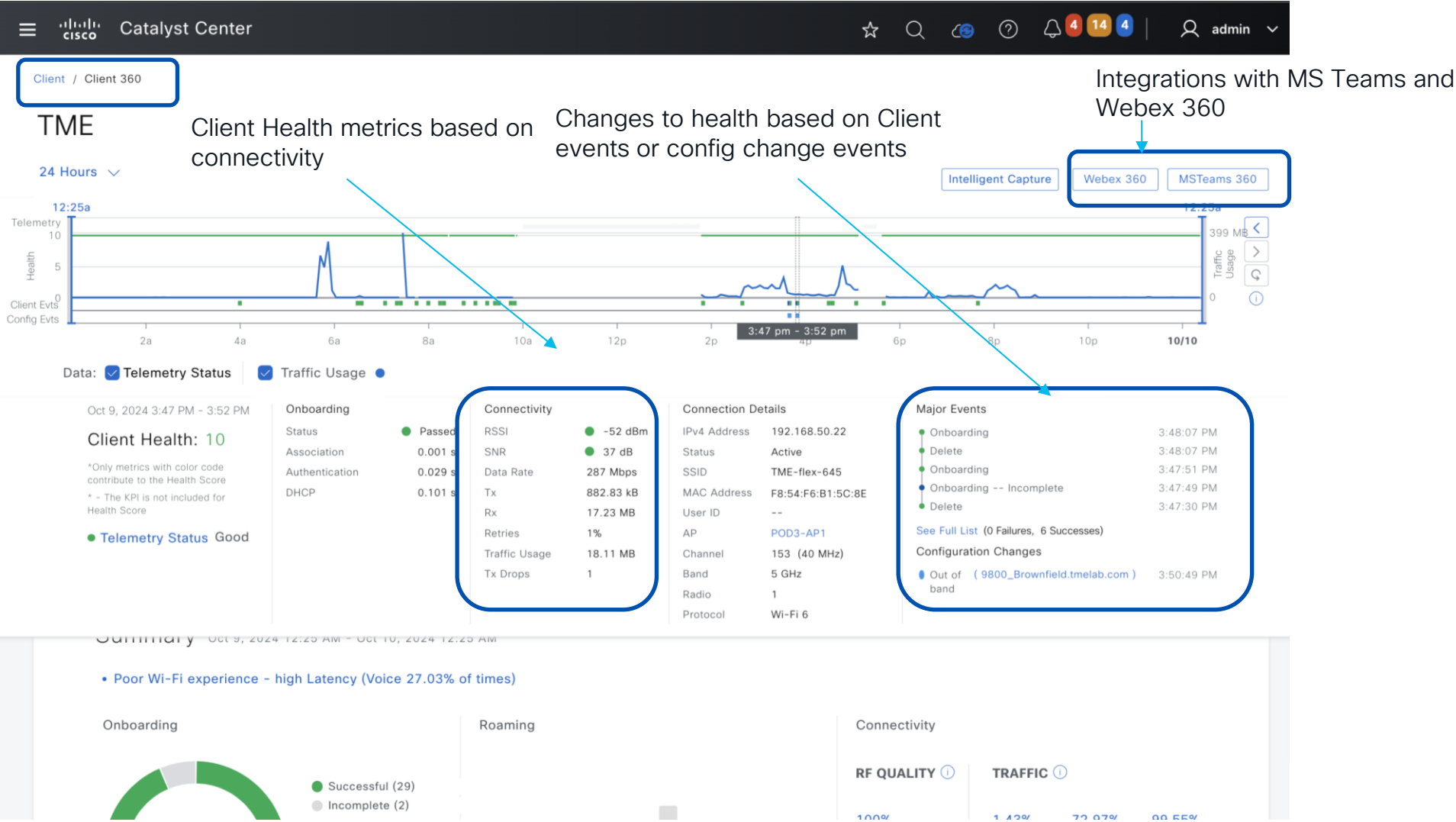


AppDev

Dear User: We do not have enough info/context to troubleshoot further and are thus wait/closing your case.

Client 360

Navigate to Client 360 to understand client connectivity and experience



Catalyst Center MS-Teams Integration

✓ In Client 360 View > Click on MS Teams to view MS Teams Call records

✓ Call details contains MS Teams call score and Network APM Score

✓ Health scores based on Audio/Video/Share Quality to precisely understand the problem

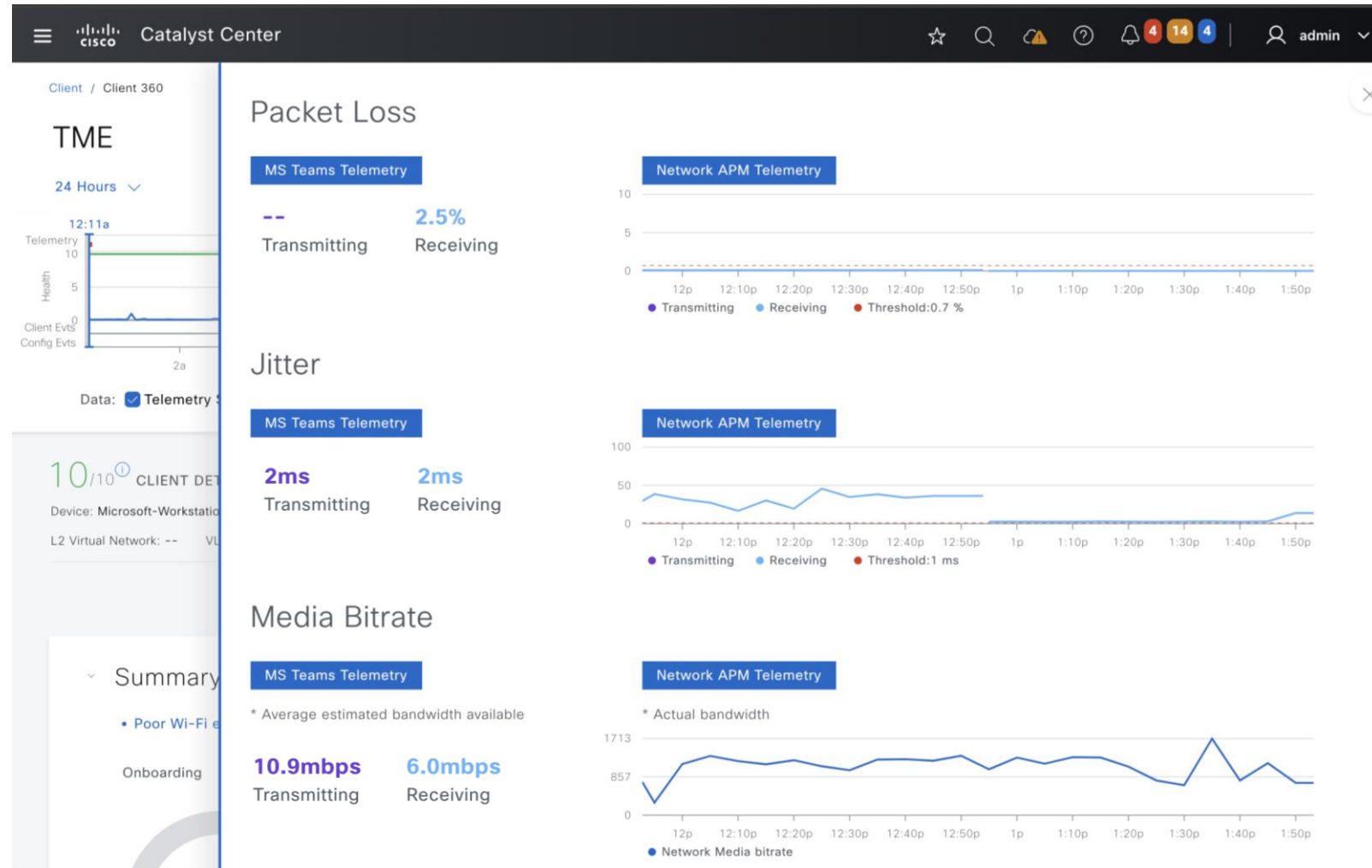
The screenshot displays the Cisco Catalyst Center interface. On the left, the 'Client 360 View' for 'Client 360' is visible, showing a 'TME' (Telemetry Monitoring Engine) section with a '24 Hours' filter. Below this, a 'Summary' section shows a 'Poor Wi-Fi' status and 'Onboarding' progress. The main panel, titled 'Application Experience for MS Teams: TME', shows a 'Meetings (2)' table. The table has columns for Meeting Name, MS Teams Score, Network APM Score, Duration, Start Time, End Time, Status, Meeting Type, and Participants. A single meeting is listed: 'test-user long last-name testing with hyphen participated in a peer-to-peer call' with an MS Teams Score of 10/10 and a Network APM Score of 7/10. Below the table, there are tabs for 'Audio Quality', 'Video Quality', and 'Share Quality'. The 'Video Quality' tab is active, showing a '10/10' MS Teams Score and a '7/10' Network APM Score. The 'Packet Loss' section is also visible at the bottom.

Meeting Name	MS Teams Score	Network APM Score	Duration	Start Time	End Time	Status	Meeting Type	Participants
test-user long last-name testing with hyphen participated in a peer-to-peer call	10/10	7/10	02:00 h	Oct 10, 2024 11:52 AM	Oct 10, 2024 1:53 PM	Ended	Peer To Peer	2

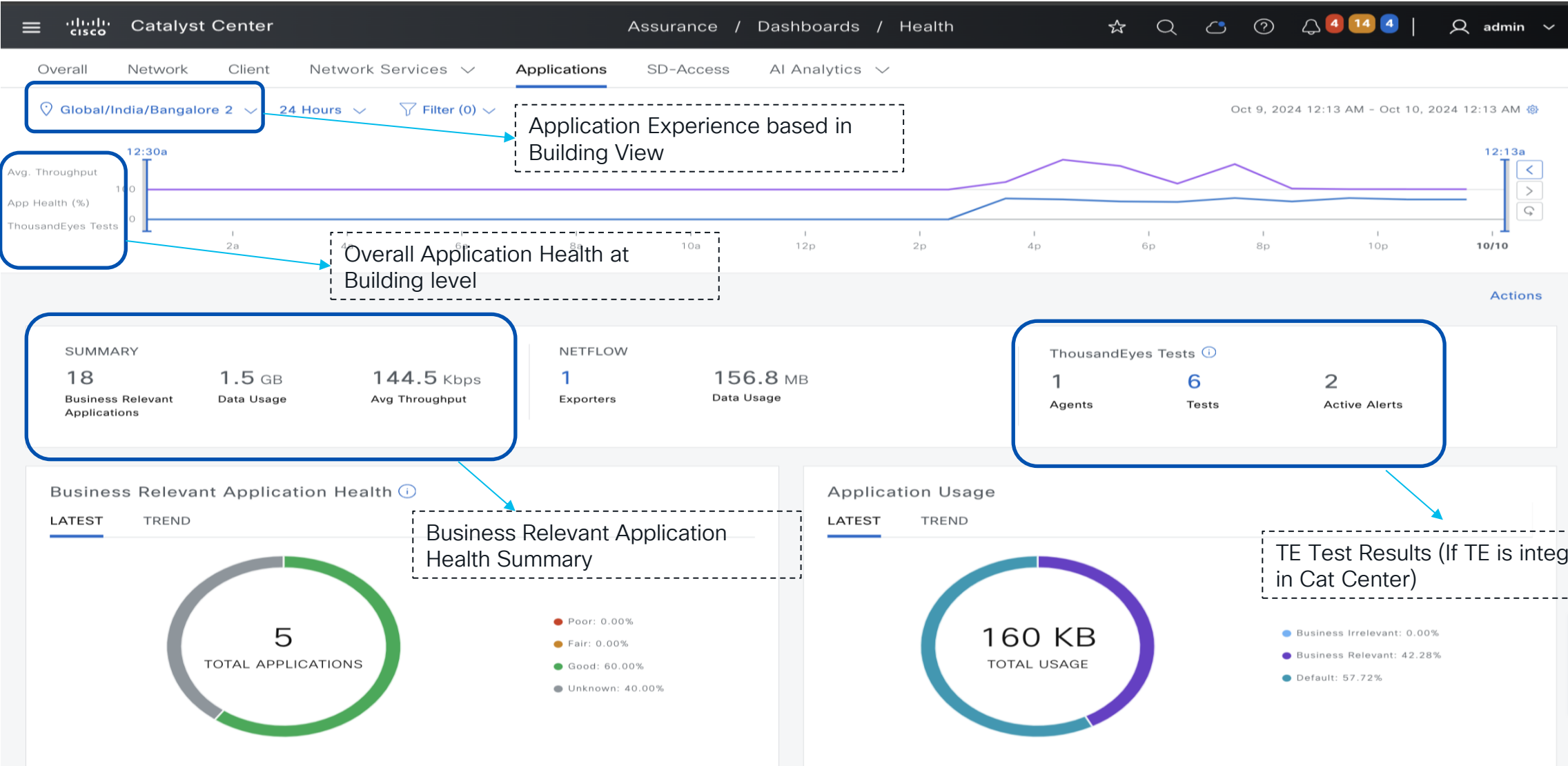
Catalyst Center MS-Teams Integration

✓ Packet Loss, latency, Jitter details collected from MS Teams and Network APM

✓ Once data is polled, Call records are stored in Catalyst Center for 14 days



Application Experience Dashboard



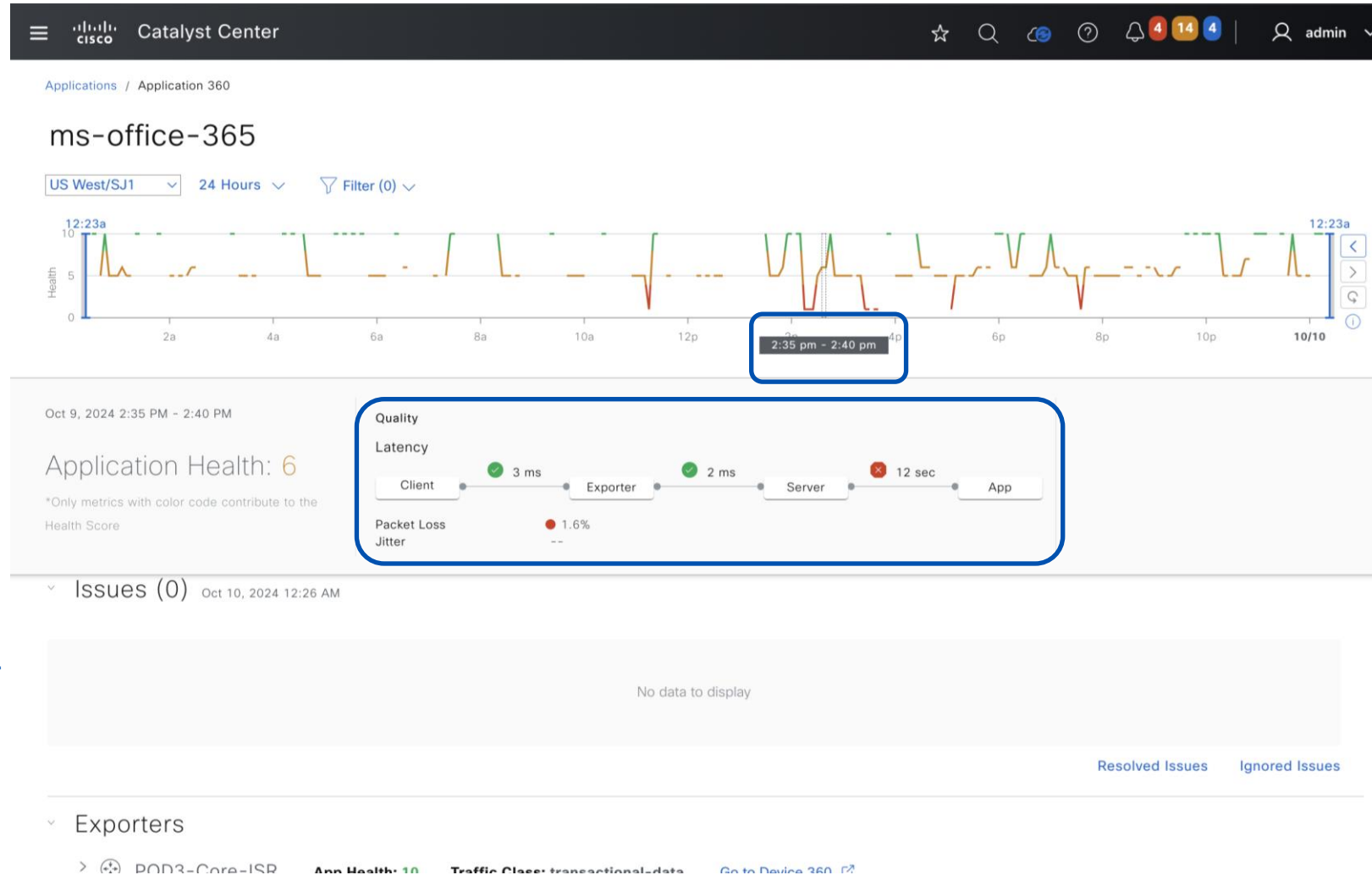
Application Experience- Application 360

✓ Application 360 provides details based on Packet Loss, Latency and Jitter (RTP)

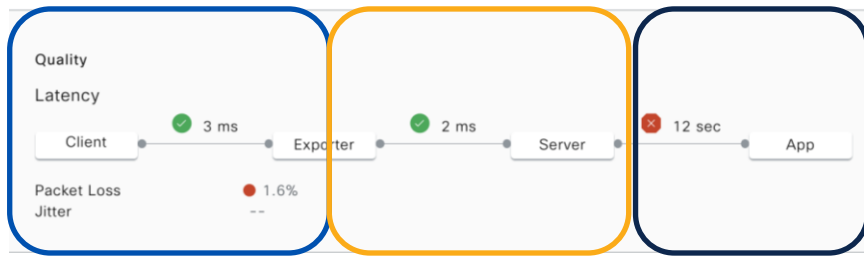
✓ Latency metrics based on

- Client to Exporter
- Exporter to Server
- Server to Application

Client Network Latency = Client to Exporter
Server Network Latency = Exporter to Server
Application Server Latency = Server to Application

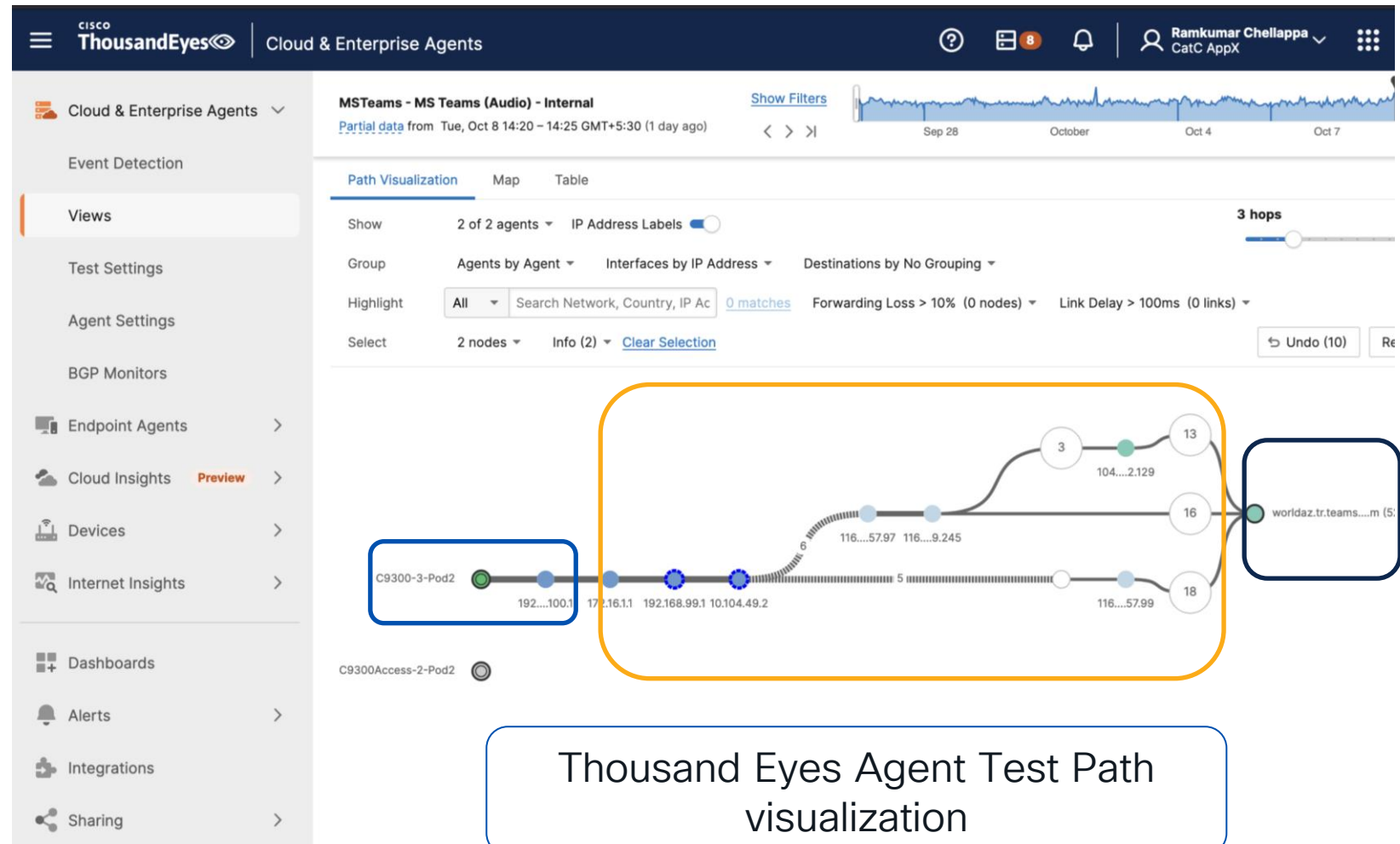


Catalyst Center- Thousand Eyes Integration



Catalyst Center App Ex 360 View

Agent Test Path visualization provide details on latency between routed hops



Catalyst Center- Thousand Eyes Integration

✓ Navigate to System > Settings > External Services > ThousandEyes Integration

✓ Use the link to cross launch to TE Dashboard to generate an Oauth Token

The screenshot shows the Cisco Catalyst Center web interface. The top navigation bar includes the Cisco logo, 'Catalyst Center', and 'System / Settings'. The left sidebar contains a search bar and a list of settings categories. 'External Services' is highlighted in the sidebar, and 'ThousandEyes Integration' is highlighted within it. The main content area is titled 'Settings / External Services' and 'ThousandEyes Integration'. It features an information box stating that the ThousandEyes token is associated with the user profile Login Account Group. Below this, a text field is labeled 'Insert new token here' with a 'Save' button. A blue button labeled 'Go to ThousandEyes page to get the OAuth Bearer Token' is also present.

Catalyst Center- Thousand Eyes Integration

✓ Navigate to System > Settings > External Services > ThousandEyes Integration

✓ Use the link to cross launch to TE Dashboard to generate an Oauth Token

✓ In TE Dashboard, Navigate to Account Settings > Users & Roles

The screenshot displays the Cisco ThousandEyes Account Settings interface. The left sidebar contains a navigation menu with options such as Cloud & Enterprise Agents, Endpoint Agents, Cloud Insights, Devices, Internet Insights, Dashboards, Alerts, Integrations, Sharing, Account Settings, Users and Roles, Activity Log, and Organization Settings. The 'Users & Roles' option is highlighted with a blue box. The main content area shows the 'Account Settings' for the user 'ramkchel@cisco.com'. It includes fields for Email, Password, and a 'Change Password' link. Below this, the 'YOUR ACCESS' section shows the user's roles: CatC AppX, Account Admin, and Regular User. The 'Login Account Group' is set to 'CatC AppX'. The 'TIME ZONE' section shows the 'Web Interface' set to 'Default (System time)'. At the bottom, the 'User API Tokens' section displays a 'Basic Authentication Token' field with a 'Regenerate' button. A 'Create' button for 'OAuth Bearer Token' is also visible and highlighted with a blue box.

Catalyst Center- Thousand Eyes Integration

✓ Navigate to System > Settings > External Services > ThousandEyes Integration

✓ Use the link to cross launch to TE Dashboard to generate an OAuth Token

✓ In TE Dashboard, Navigate to Account Settings > Users & Roles

✓ Copy the token in Cat Center to integrate with TE Dashboard

The screenshot shows the Cisco Catalyst Center web 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: Configuration Archive, External Services (expanded), Authentication and Policy Servers, Integrity Verification, SD-Access Compatibility Matrix, IP Address Manager, Cloud Access Login, Cisco AI Analytics, Stealthwatch, Talos IP Reputation, Destinations, Cisco Spaces/CMX Servers, Global Manager Integration, Machine Reasoning Engine, Cisco Catalyst Cloud, Webex Integration, ThousandEyes Integration, System Configuration (expanded), Debugging Logs, Visibility and Control of Configur..., and Geo Map Settings. The main content area is titled 'Settings / External Services' and 'ThousandEyes Integration'. It features an information box stating: 'ThousandEyes token is associated with the user profile Login Account Group. Cisco Catalyst Center collects the data that is returned from ThousandEyes API based on the saved token. Changing the user profile Login Account Group impacts the data returned from the API.' Below this, a text explains: 'Use this page to enable ThousandEyes integration. Once enabled, Cisco Catalyst Center can provide ThousandEyes tests information for Application Health dashboard.' A link 'Go to ThousandEyes page to get the OAuth Bearer Token' is provided. A form field labeled 'Insert new token here' contains the text '16d' and a copy icon. A blue 'Save' button is at the bottom of the form.

Catalyst Center – Thousand Eyes Test Results

Catalyst Center

Assurance / Dashboards / Health

☆

🔍

🔄

?

🔔

👤 Demo

Overall

Network

Client

Network Services

Applications

SD-Access

AI Analytics

SUMMARY

14

Business Relevant Applications

666 MB

Data Usage

64.7 Kbps

Avg Throughput

NETFLOW

2

Exporters

290.3 MB

Data Usage

ThousandEyes Tests

1

Agents

6

Tests

2

Active Alerts

ThousandEyes Enterprise Agent Tests (6)

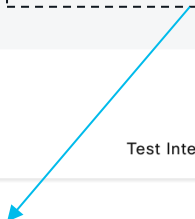
🔍 Search Table

🔗 Export

⚙️

Test Name	Test Type	Target	Test Interval	Device Name	Last Updated	# of Active Alerts	Test Failures	Packet Loss (%)		
								Latest	Average	Latency
Office 365 Login	Network - Agent to Server	52.112.14.70:80		LDN1-C9300-Edge1.PseudoCo.com	--	1	0%	--	100	--
Salesforce	Web - HTTP Server	https://www.salesforce.com		LDN1-C9300-Edge1.PseudoCo.com	--	0	1%	--	0	--
webex-meeting	Web - HTTP Server	https://www.webex.com		LDN1-C9300-Edge1.PseudoCo.com	--	0	0%	--	0	--

Test Results from TE Dashboard with Average and Latest details on Packet Loss, Latency, Jitter and Response Time



Catalyst Center MS-Teams Integration

MS-Teams can be integrated to Catalyst Center from the Cisco DNA-Cloud Portal

The screenshot shows the Cisco DNA Center interface. The top navigation bar includes the Cisco logo, 'DNA Center', and 'System / Settings'. The user is logged in as 'admin'. The left sidebar contains a search bar and a list of navigation items: Integrity Verification, vManage, IP Address Manager, Cloud Access Login, Cisco AI Analytics, Stealthwatch, Destinations, CMX Servers/Cisco Spaces, Machine Reasoning Engine, Cloud Authentication, Cisco DNA - Cloud (selected), Webex Integration, ThousandEyes Integration, System Configuration, Debugging Logs, Visibility and Control of Configur..., Proxy, and High Availability. The main content area is titled 'Settings / External Services' and 'Cisco DNA - Cloud'. It includes a 'Select Region' dropdown set to 'us-west-2' and a search bar. Below these are four integration cards: 'Cisco User Defined Network', 'Talos Threat Intelligence', 'Plug and Play as a Service', and 'AppX MS-Teams'. The 'AppX MS-Teams' card is highlighted with an orange border. Each card has an 'Activate' button.

Cisco DNA - Cloud

Do more with your Cisco products by activating these cloud applications. Choose the region where you want to register your product.

Select Region • us-west-2

Cisco User Defined Network

Cisco User Defined Network enables users to define their own personal network in a shared Wireless network by limiting multicast advertisement of services within a UDN.

Activate

Talos Threat Intelligence

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

Activate

Plug and Play as a Service

Plug and Play as a service enables users to securely day-0 onboard Catalyst 9K family of devices. During onboarding process you can upgrade image and deploy configuration to the device. After onboarding you can redirect the device to be

Activate

AppX MS-Teams

AppX MS-Teams application connects AppX cloud service with Microsoft Teams API, to collect call quality metrics and to enrich Cisco DNA Center application dashboards to get better visibility on the network.

Activate

Integrations to Simplify Network Operations



Catalyst Center Destinations

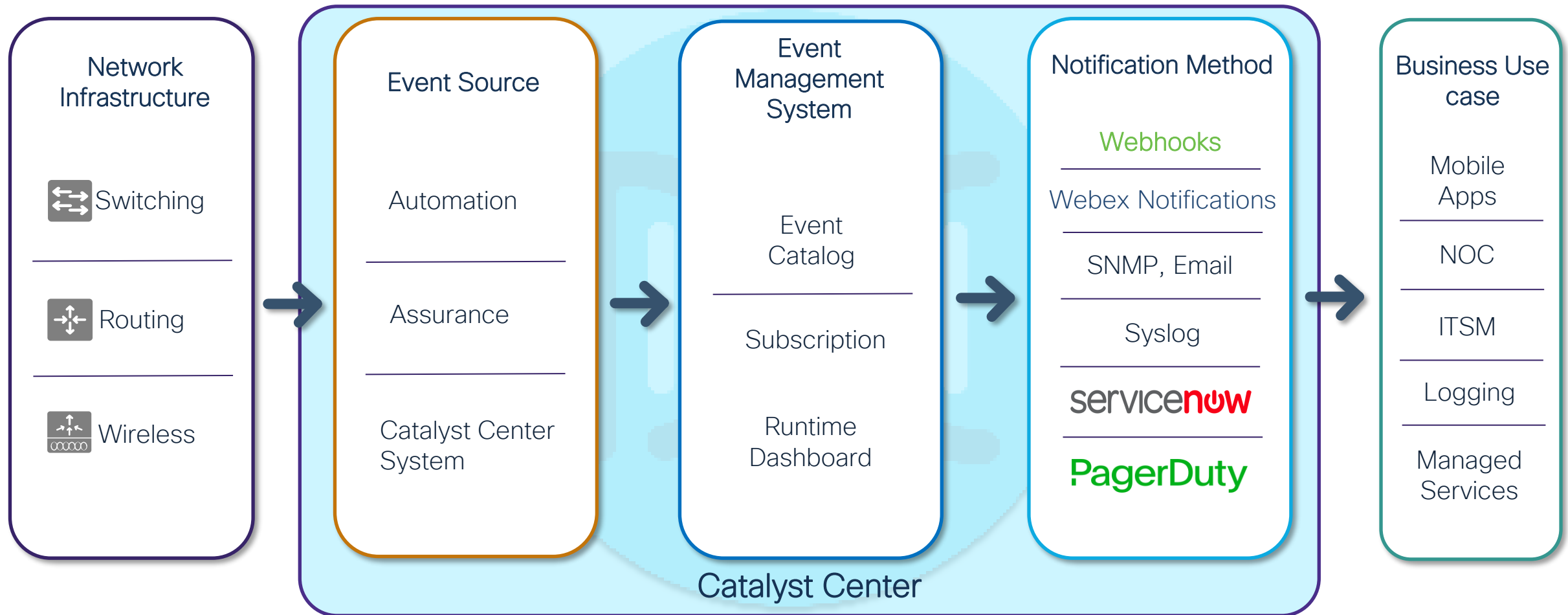
✓ Navigate to System > Settings > External Services > Destination to add various destination for event notifications

✓ Configure various external destinations

- Webhooks
- Email
- SNMP
- Syslog
- ITSM

The screenshot displays the Cisco Catalyst Center web interface. The top navigation bar shows 'System / Settings' and a user profile 'admin'. The left sidebar contains a search bar and a list of navigation items: SNMP, ICMP Ping, Device EULA Acceptance, PnP Device Authorization, Device Prompts, Configuration Archive, External Services (expanded), Authentication and Policy Servers, Integrity Verification, SD-Access Compatibility Matrix, IP Address Manager, Cloud Access Login, Cisco AI Analytics, Stealthwatch, Talos IP Reputation, Destinations (selected), Cisco Spaces/CMX Servers, Global Manager Integration, Machine Reasoning Engine, Cisco Catalyst Cloud, and Webex Integration. The main content area is titled 'Settings / External Services' and 'Destinations'. It includes a sub-header 'Configure various types of destinations to deliver event notifications from Catalyst Center Platform'. Below this are tabs for 'Webhook', 'Email' (selected), 'Syslog', 'SNMP', and 'ITSM'. The 'Email' tab has a sub-header 'Configure settings to send out emails from Catalyst Center Platform'. The configuration section is titled 'Primary SMTP Server' and includes fields for 'Hostname/IP*' (173.37.93.161), 'Type*' (DEFAULT), 'Port' (25), 'Username', and 'Password'. Each field has a descriptive tooltip: 'Primary SMTP Server Address. Supports both IPv4 and IPv6.', 'Primary SMTP Type', 'Username for Authenticating Primary SMTP Server', and 'Password for Authenticating Primary SMTP Server'. At the bottom, there is a section for 'Secondary SMTP Server (optional)'.

Catalyst Center Event Notification Framework

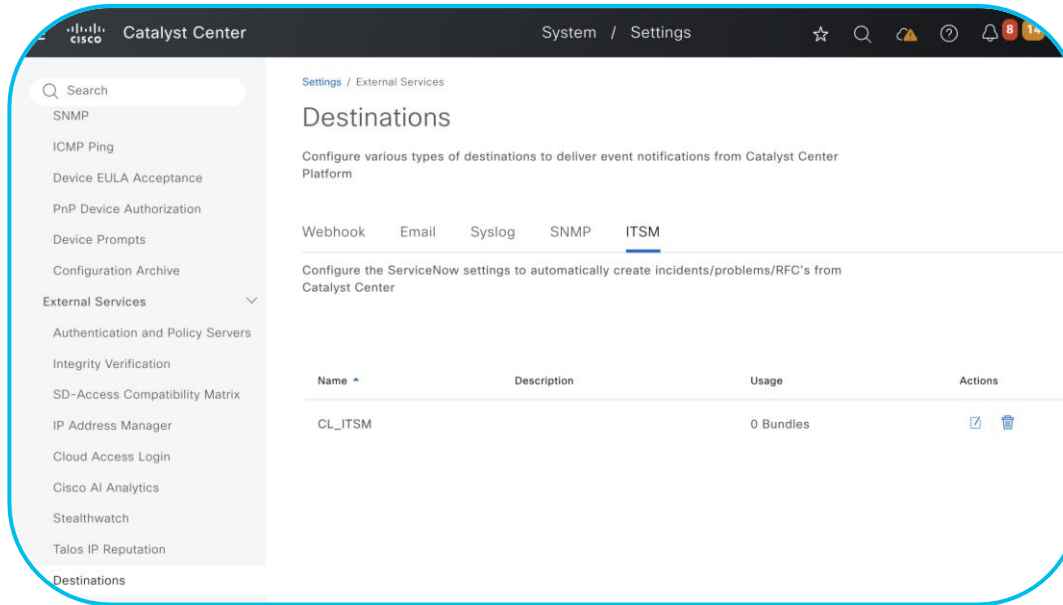


Catalyst Center ITSM Integration

Catalyst Center



+ servicenow

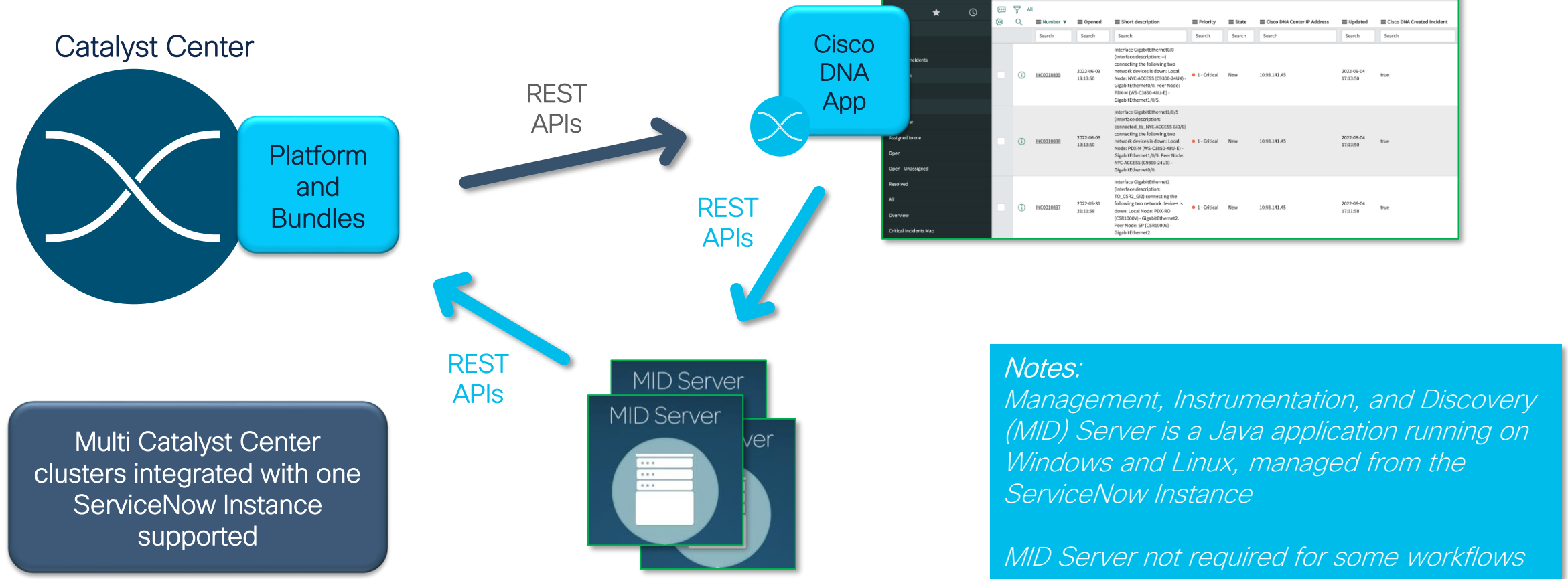


Catalyst Center ServiceNow Integration:

- Increased IT efficiency by streamlining and customizing processes
- Automated ServiceNow CMDB population with rich asset data
- Enhanced incident management with enriched issue data
- Simplified change management with closed loop functionality
- Endpoint attribute synchronization for client profiling

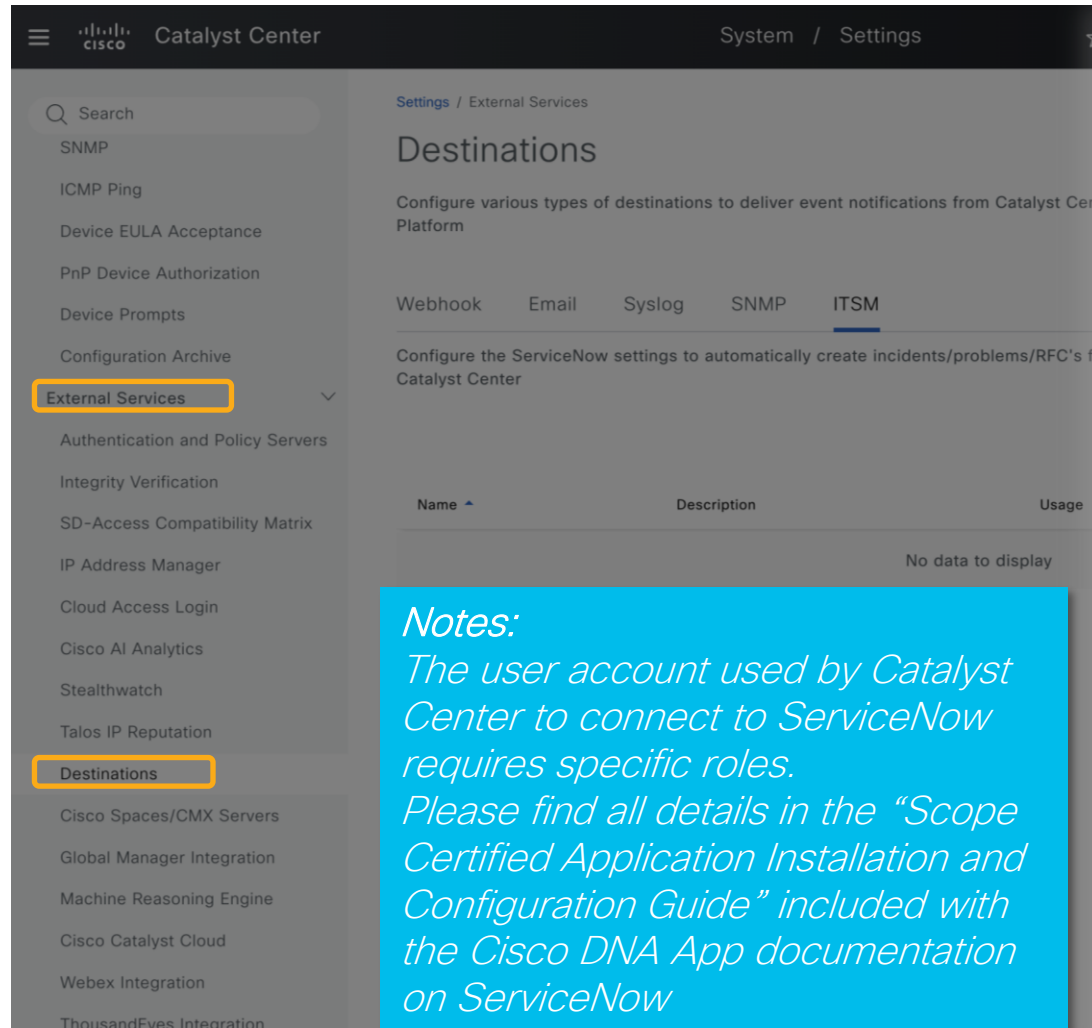
Catalyst Center ITSM Integration- Architecture

With the Cisco DNA App

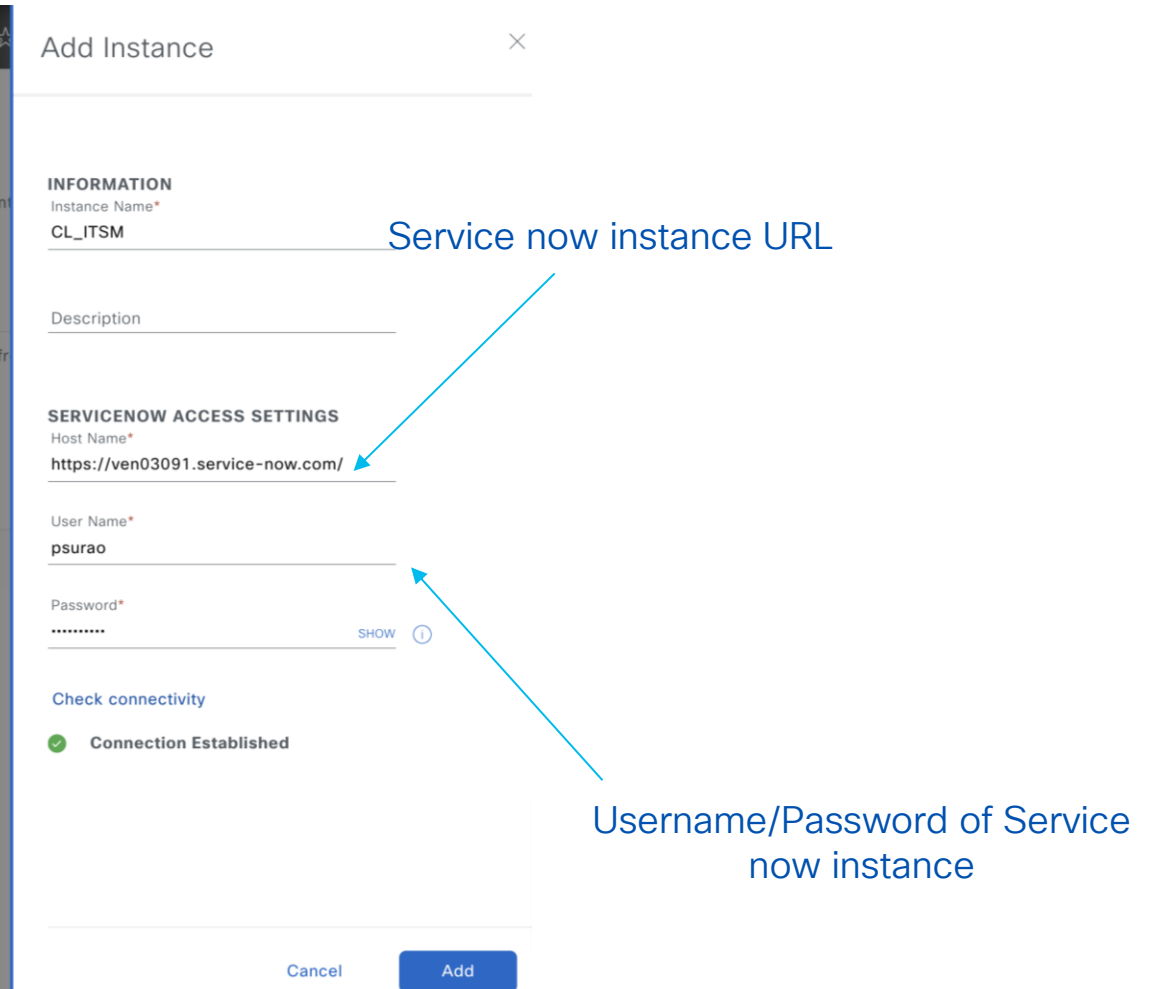


ITSM Integration Settings

Integration with ITSM through **System** → **Settings**



Notes:
The user account used by Catalyst Center to connect to ServiceNow requires specific roles.
Please find all details in the “Scope Certified Application Installation and Configuration Guide” included with the Cisco DNA App documentation on ServiceNow



Service now instance URL

Username/Password of Service now instance

Integration Settings

✓ Navigate to System > Settings > System Configuration > Integration Settings

✓ Configure the Callback URL Hostname/IP Address

✓ This Hostname/IP Address will be used to cross launch from external integrated systems to Catalyst Center

The screenshot displays the Cisco Catalyst Center web interface. The top navigation bar shows 'System / Settings' and a user profile 'admin'. The left sidebar contains a search bar and a list of configuration categories. 'System Configuration' is highlighted with an orange box, and 'Integration Settings' is also highlighted with an orange box. The main content area shows the 'Integration Settings' page with a sub-header 'Settings / System Configuration'. A text input field labeled 'Callback URL Host Name or IP Address' contains the value '10.104.49.195' and is highlighted with a blue box. Below the input field are 'Clear' and 'Apply' buttons. A tooltip message states: 'This Host Name or IP Address will be used in the Integration Callback URLs'.

Configuring Bundles in Catalyst Center

✓ Navigate to **Platform > Manage > Bundles** to enable and configure bundles

✓ Select the necessary bundles to enable and configure

Catalyst Center Platform / Manage

Bundles Configurations

Bundles

Filter Find

Bundle	Status	Description
A AI Endpoint Analytics Cisco Systems, Inc. v1.2.2 Catalyst Center 2.2.3.0+ Version Dated Nov 20, 2023	NEW	API bundle to access various services provided by AI Endpoint Analytics application. AI Endpoint Analytics package must be installed on Catalyst Center, before this bundle can be used.
B Basic ITSM (ServiceNow) CMDB synchronization Cisco Systems, Inc. v1.18.5 Catalyst Center 1.2.5 + Version Dated Apr 22, 2024	NEW	You can schedule a synchronization or trigger an update between Catalyst Center's device inventory and your ITSM(ServiceNow) configuration management database(CMDB). These activities integrate Catalyst Center's processes into the IT System Management processes of incident, change or problem management. Note: If your network...
C Catalyst Center Automation events for ITSM (ServiceNow) Cisco Systems, Inc. v1.13.1 Catalyst Center 1.2.5 + Version Dated Mar 26, 2024	NEW	This bundle can be used to: 1. Monitor and publish events that require software image updates for compliance, security or any other operational triggers, to an ITSM(ServiceNow) system. 2. Monitor and publish events that involve changes to the configuration of network devices for security or other operational triggers, to an...
E Endpoint Attribute Retrieval with ITSM (ServiceNow) Cisco Systems, Inc. v1.8.0 Catalyst Center 2.1.1 + Version Dated Mar 19, 2024	ENABLED	You can schedule a synchronization or trigger an update between the Endpoint Inventory and your ITSM (ServiceNow) configuration management database (CMDB). Endpoint attribute information from ServiceNow can be used to help profile endpoints on your network. ServiceNow appears in the endpoint profiling workspace as an...
N Network Issue Monitor and Enrichment for ITSM Cisco Systems, Inc. v1.13.2 Catalyst Center 1.2.5 + Version Dated May 17, 2024	ACTIVE	You can use this bundle to monitor your network for assurance and maintenance issues, and then publish the event details about these issues to an ITSM(ServiceNow) system. This bundle also contains APIs that extract rich network context data. This bundle also enables closed loop integration. Please note that, for the ServiceNow...

ITSM Integration- Scheduler

✓ Navigate to [Platform > Developer Toolkit > Integrations](#) to enable scheduler for ITSM CMDB sync

✓ CMDB/Asset Sync scheduler options include

- Run Now
- Run Later
- Recurring

The screenshot displays the Cisco Catalyst Center web interface. The top navigation bar shows 'Platform / Developer Toolkit'. The left sidebar has tabs for 'APIs', 'Integration Flows', and 'Event Notification'. Under 'Integration Flows', there is a section for 'Integrations' with a list including 'ITSM Integration'. The main content area is titled 'Schedule to Publish Inventory Details - ServiceNow Connector'. It shows a 'Description' of the scheduler's function, 'Tags' including 'ServiceNow', and a section 'How to use this flow' with three radio button options: 'Run Now', 'Run Later', and 'Recurring'. The 'Recurring' option is selected and highlighted with a blue box. Below this, there are fields for 'Repeats' (set to 'Daily'), 'Set Schedule Start' (checked), a date field set to 'Oct 8, 2024', and a time field set to '2:35 PM'.

Runtime Dashboard

✓ Navigate to [Platform > Runtime Dashboard](#)

✓ Total number of devices in inventory and synchronized, errors (if any)

✓ Summary of all scheduled synchronizations, success/fail counts and length of time

✓ Details of change request created in ServiceNow

The screenshot displays the Cisco Catalyst Center Runtime Dashboard. The top navigation bar includes the Cisco logo, 'Catalyst Center', and 'Platform / Runtime Dashboard'. The main content area is titled 'Provision Device (C9300-Edge-Pod2) (1)' and shows a 'Last 6 hours' filter. The dashboard is divided into several sections:

- API Summary:** Includes a 'Call Status' section showing 'Total API's' as 0, and a 'Completed Call Performance' table with columns for API Name and Version, currently showing 'No data'.
- Call Status:** Features a 'Search Table' bar, a 'Retry' button, and a 'Last In-Event Flow' table. The table has columns: Event Id, Source, Destination, ITSM Workflow, DNA Event Status, ITSM Status, ITSM Id, ITSM Link, and ITSM 1. A single record is visible with Event Id '33133d76-7ec7-4886-a23a-2963591c607c', Source 'ServiceNow', Destination 'Cisco DNA Center', ITSM Workflow 'RFC', DNA Event Status 'NA', ITSM Status 'New', ITSM Id 'CHG0030388', and ITSM Link 'https://ven03091.service-now.com/nav_to.do?uri=change_request.do?sys_id=57c33ecc47b91e1086c7bcff016d43da'.
- CMDB Synchronization Summary:** Includes a 'Search Table' bar and a table with columns 'Devices from Inventory' and 'Devices Synchronized'. Both columns show a value of 42.

A blue note box on the right states: *Note: Incident number and link will not be available if MID server not operational. Incident may still be created.*

Recap- Catalyst Center Integrations

Cisco Integrations



Ecosystem



Custom Integrations

Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106



Smart, Secure, Seamless:
Transforming Experiences with Next-Generation Networking

Level 2
Room 204



Harness a Bold New Era:
Transform Data Centre and Service Provider Connectivity

Level 2
Room 203



Securing User to Application and Everything in Between

Level 2
Melbourne Room 2



Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations



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



Complete your surveys in the **Cisco Live mobile app**.



Continue your education

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



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC