

Cisco Catalyst Center: Built-In Integrations for Streamlined Network Operations

CISCO Live !

Ramkumar Chellappa
Technical Leader, TME, @ramkchel

Surya Prakash Rao
TME, @psurao

Cisco Webex App

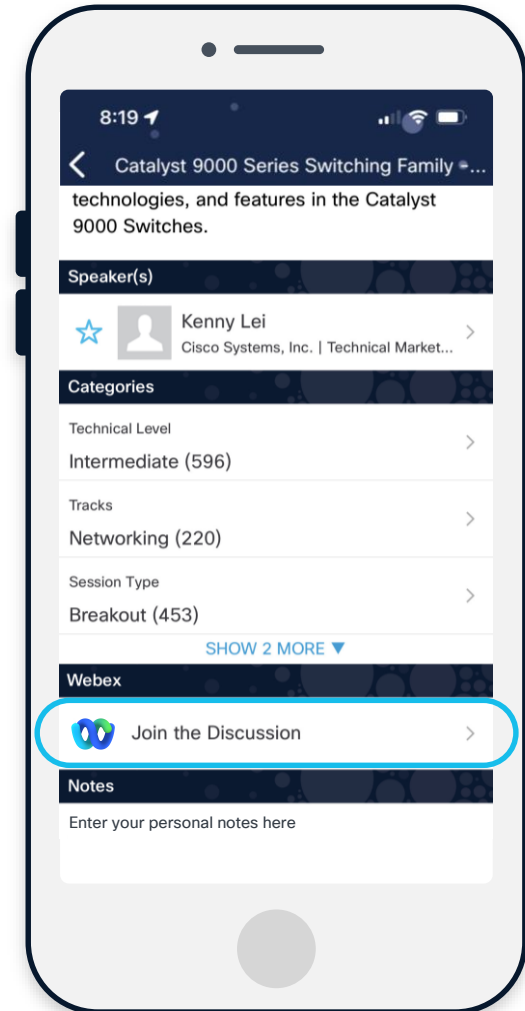
Questions?

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

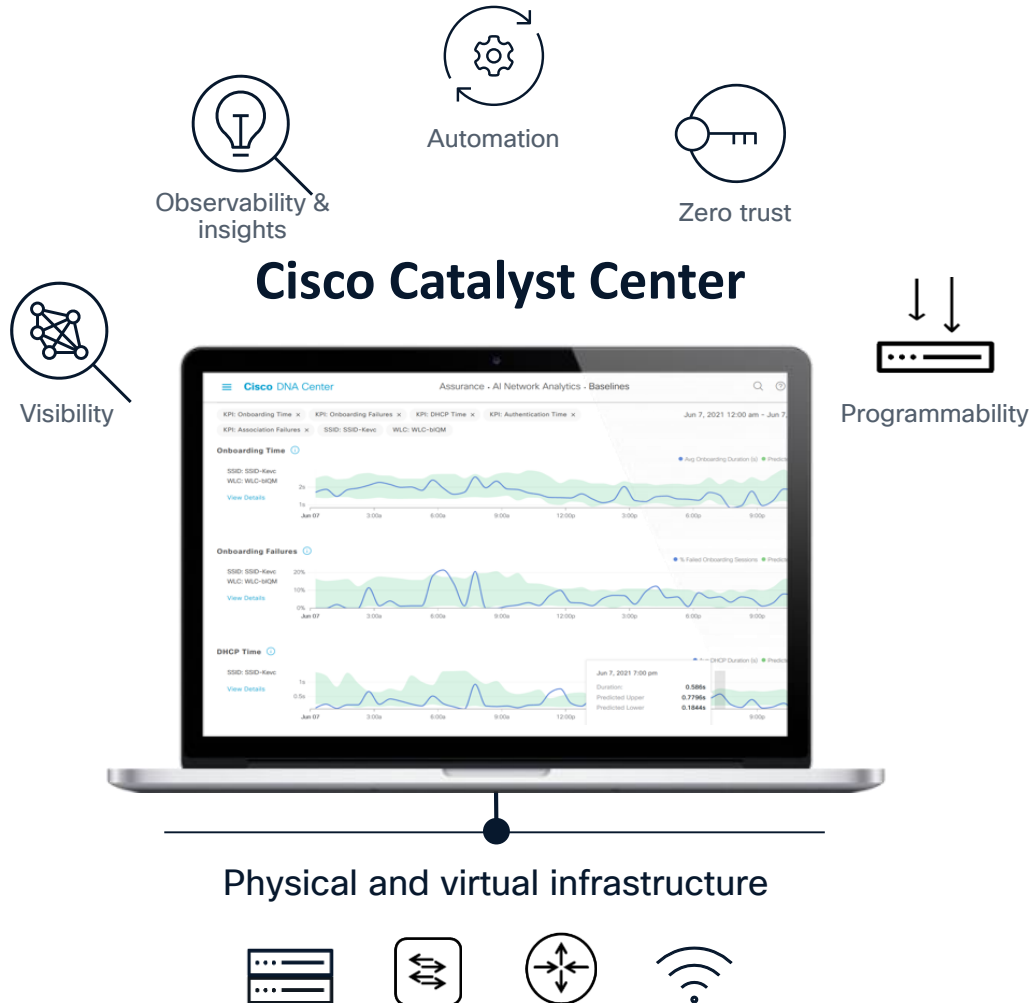
Webex spaces will be moderated by the speaker until June 13, 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKOPS-2609>

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

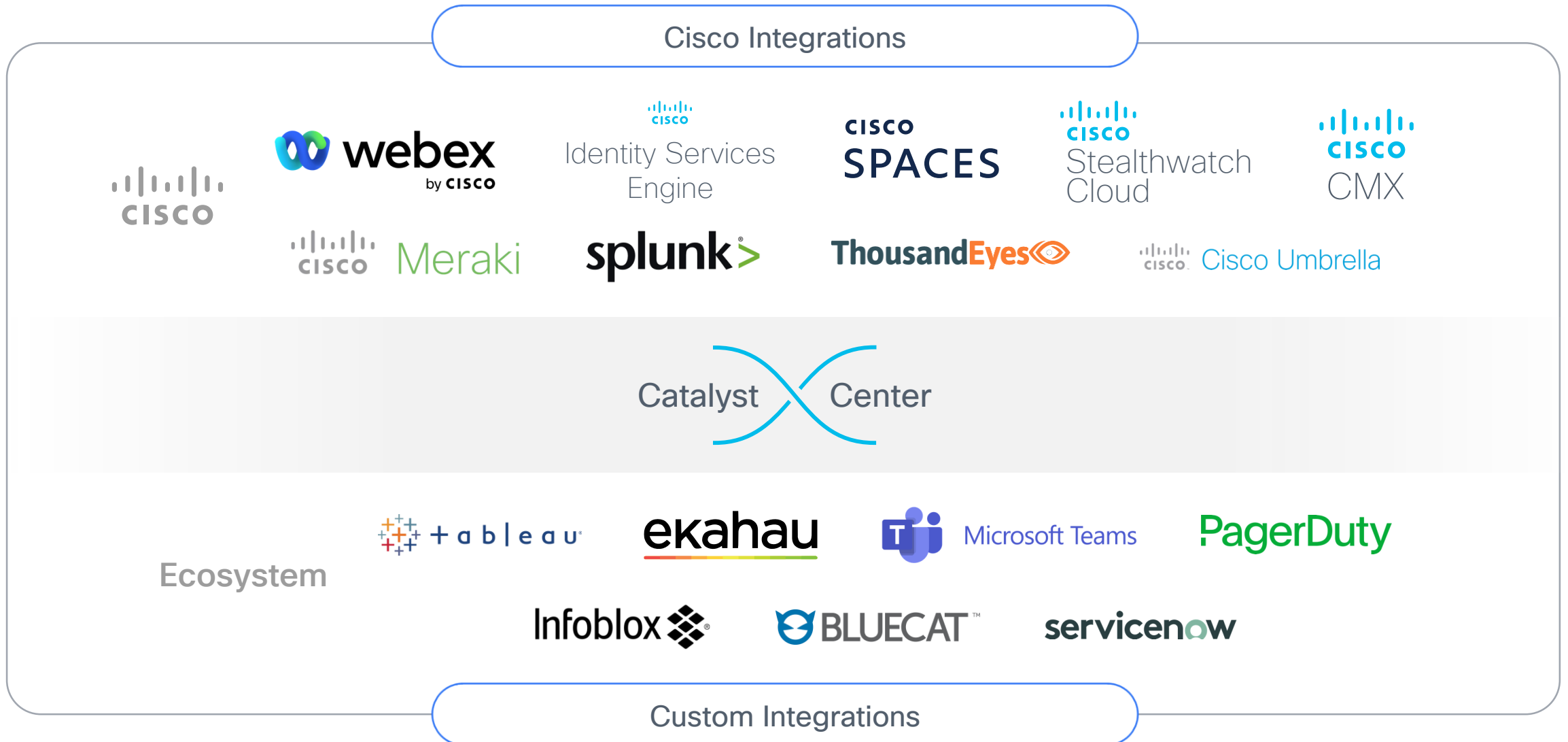
AI/ML and DPI Identify and classify endpoints, enforce security policies and mitigate threats for a **complete workplace zero trust solution**



DevOps

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

Catalyst Center out-of-the-box API Integrations



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)

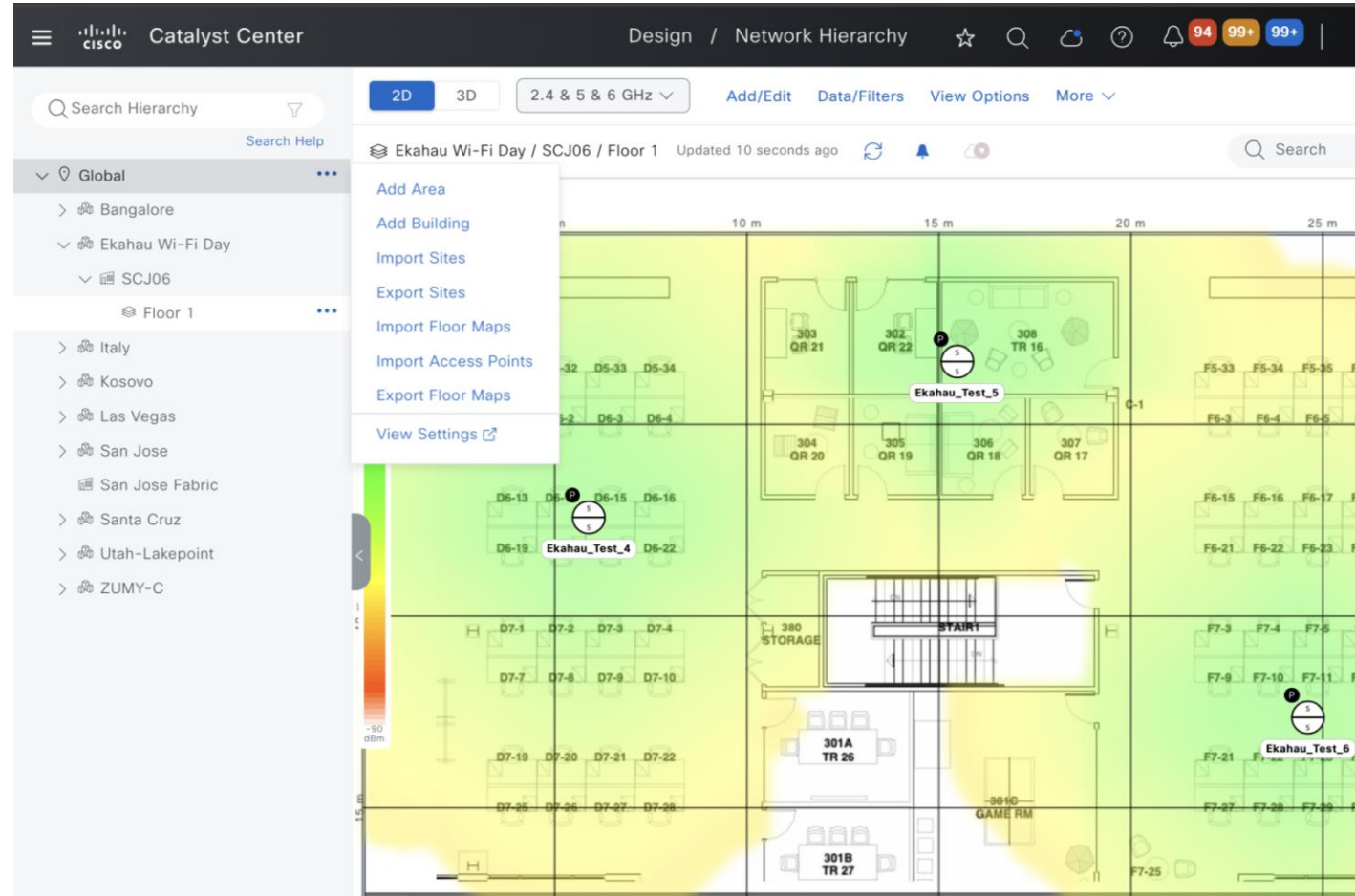
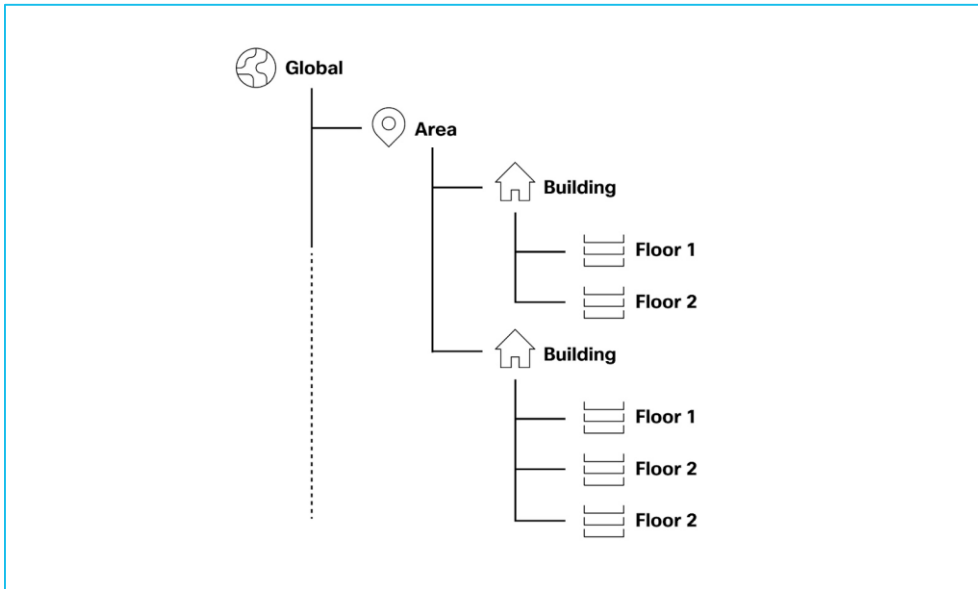
Integrations to Simplify Network Operations

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

Integrations for Network Management

Creating Site Hierarchy

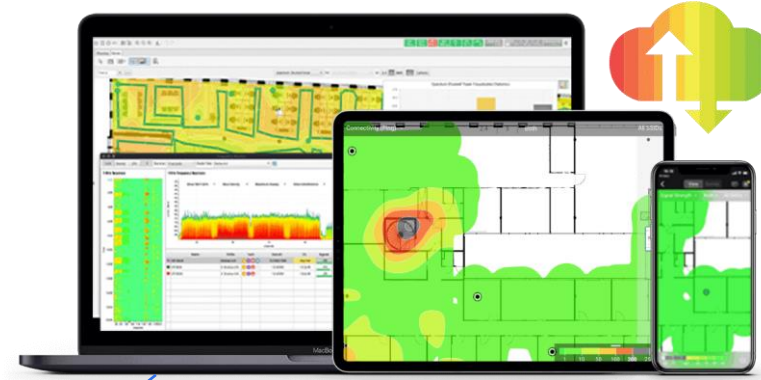
Create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network.



Importing Ekahau Projects to Catalyst Center



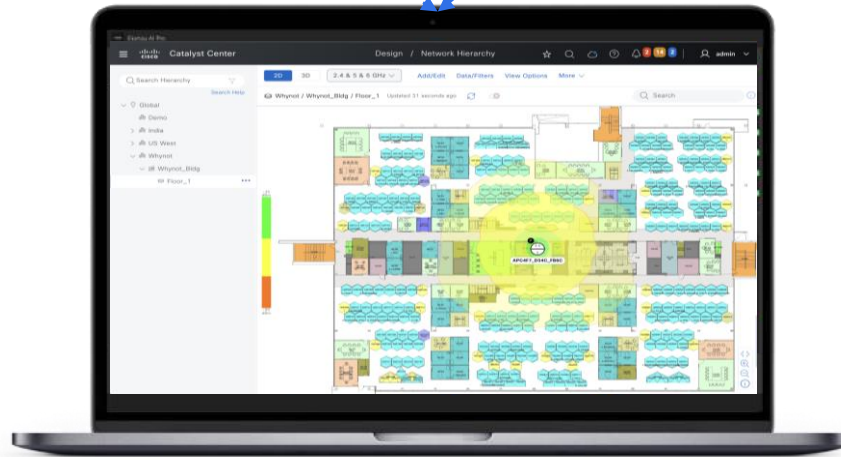
Ekahau Pro



Ekahau Cloud

Ekahau Pro version 11 –
Catalyst Center version 2.3.5.x

Ekahau cloud – Catalyst Center
version 2.3.7.x

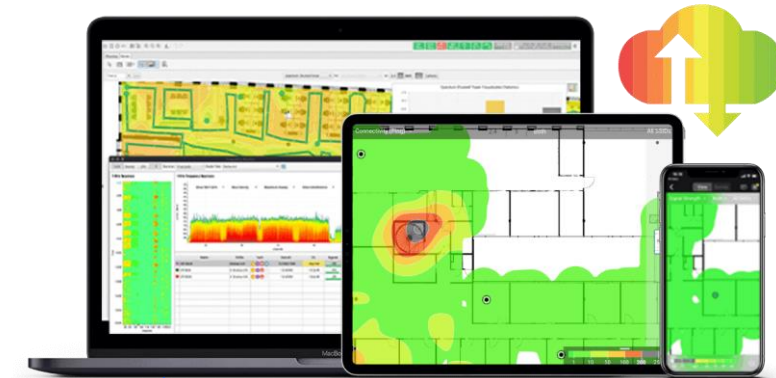


Catalyst Center

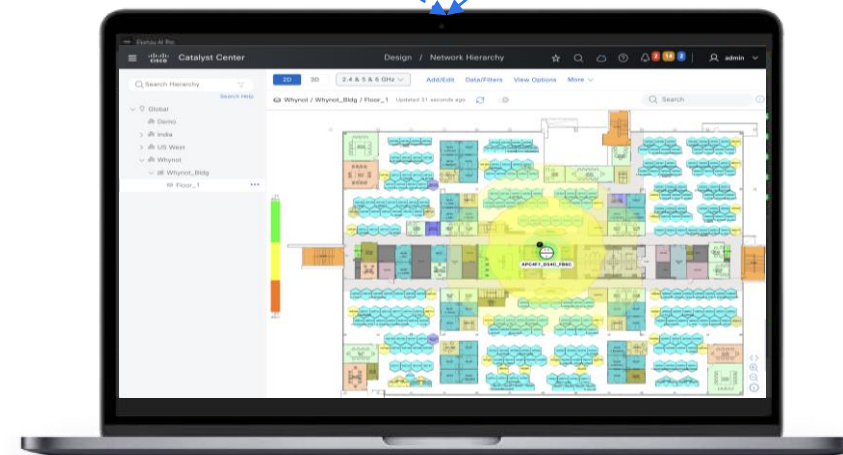
Importing Ekahau Projects to Catalyst Center



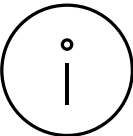
Ekahau Pro

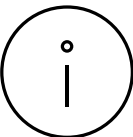


Ekahau Cloud



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)

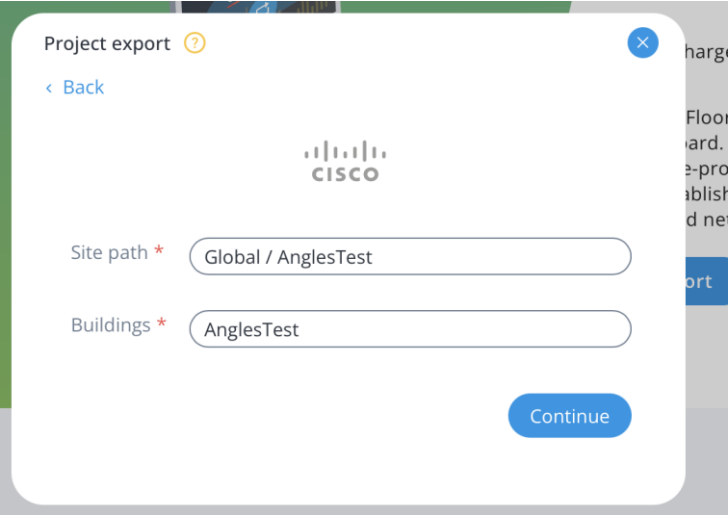
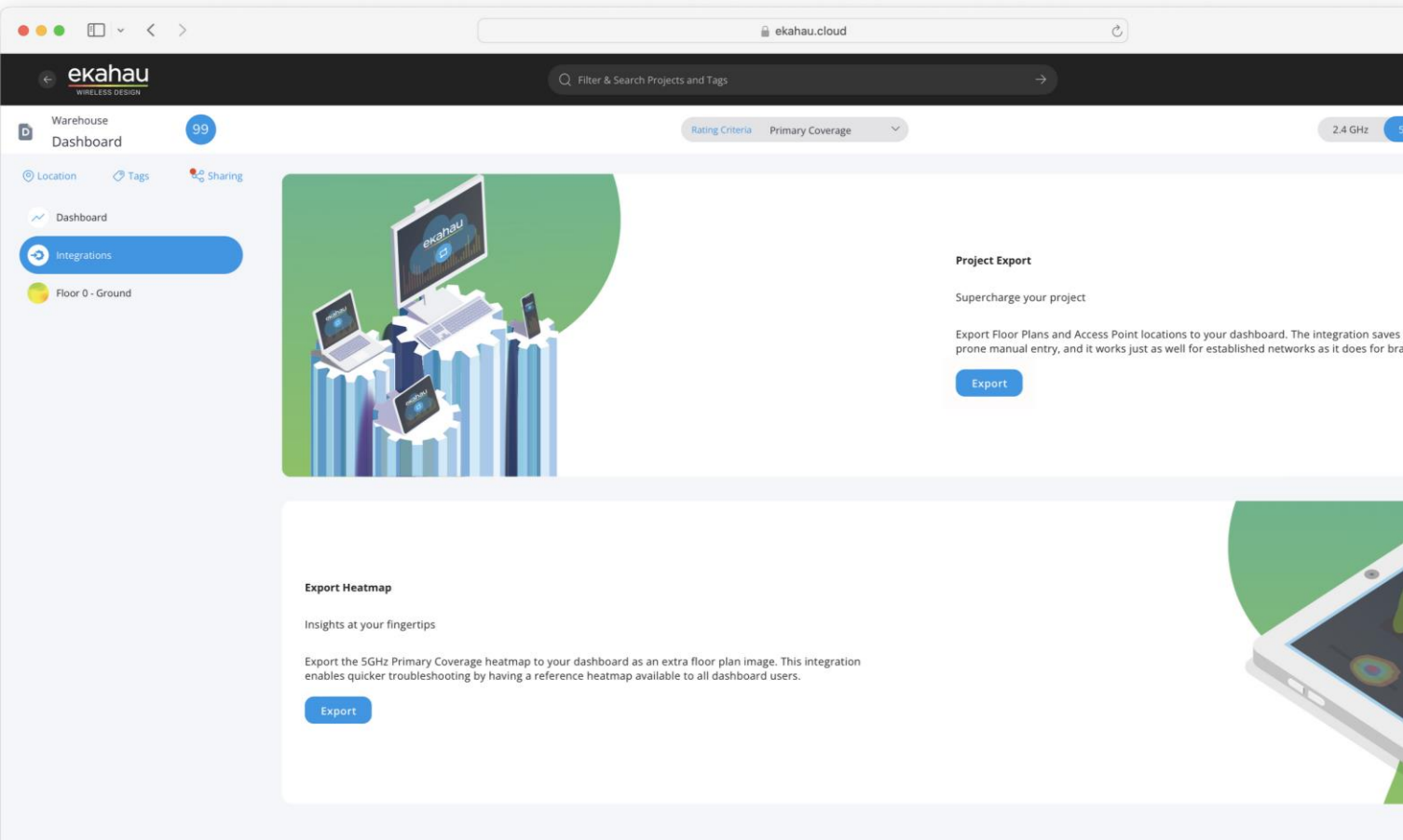
Message

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

Showing 1 of 1

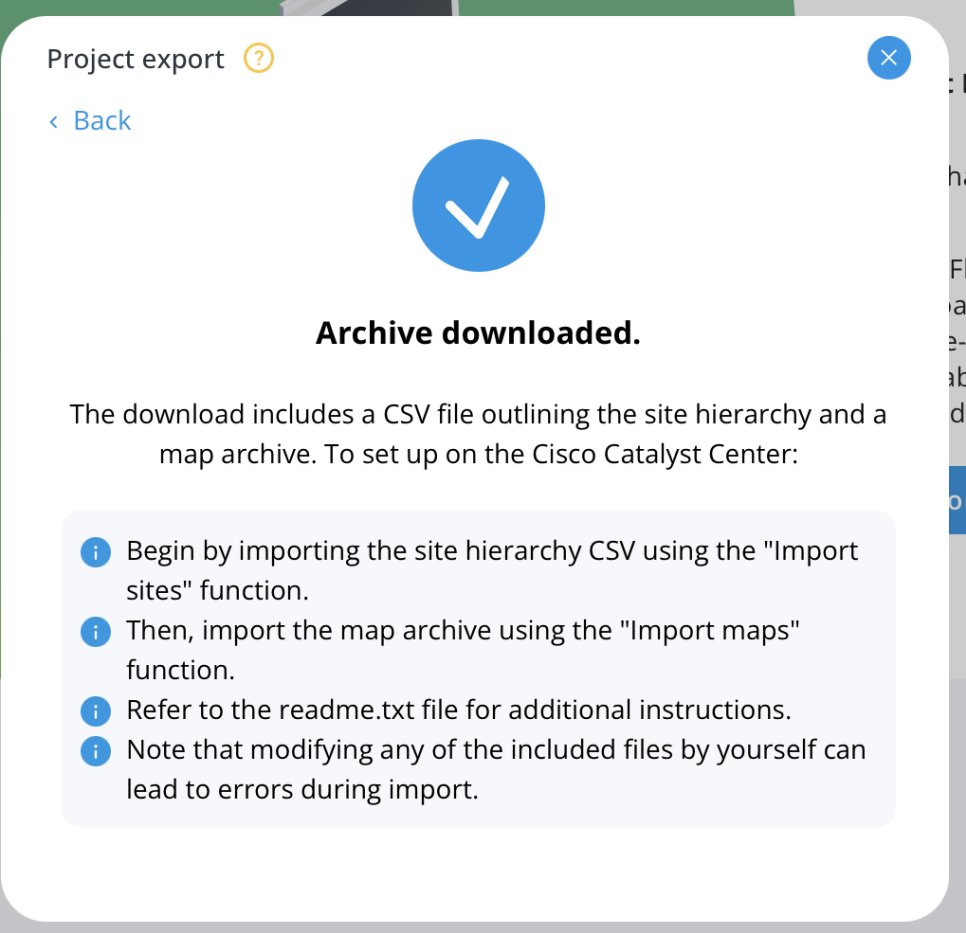
Importing Ekahau Projects to Catalyst Center

Using API method



Importing Ekahau Projects to Catalyst Center

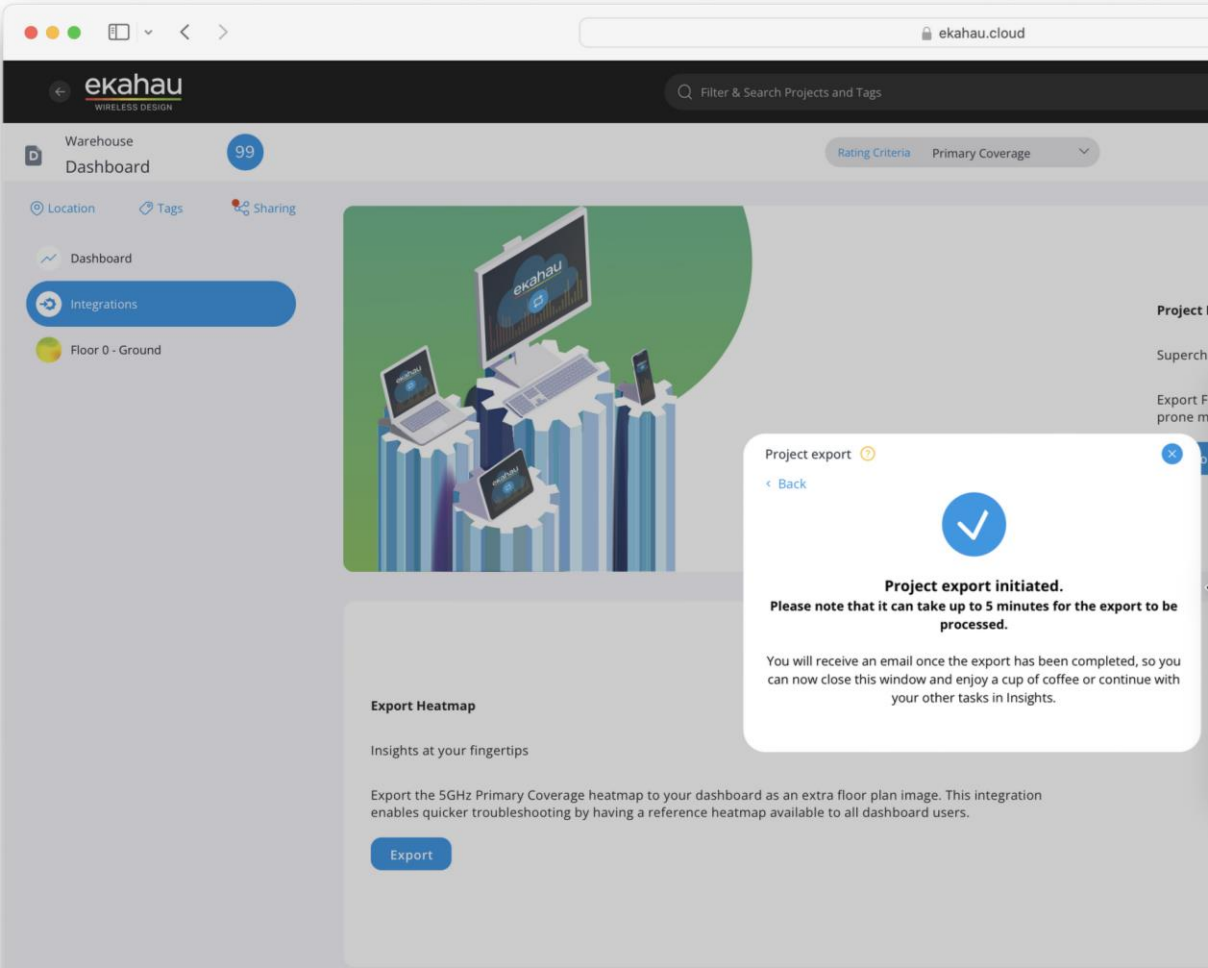
Without Login



The screenshot shows a modal window titled "Project export" with a question mark icon and a close button. It features a blue checkmark icon and the text "Archive downloaded." Below this, it states: "The download includes a CSV file outlining the site hierarchy and a map archive. To set up on the Cisco Catalyst Center:"

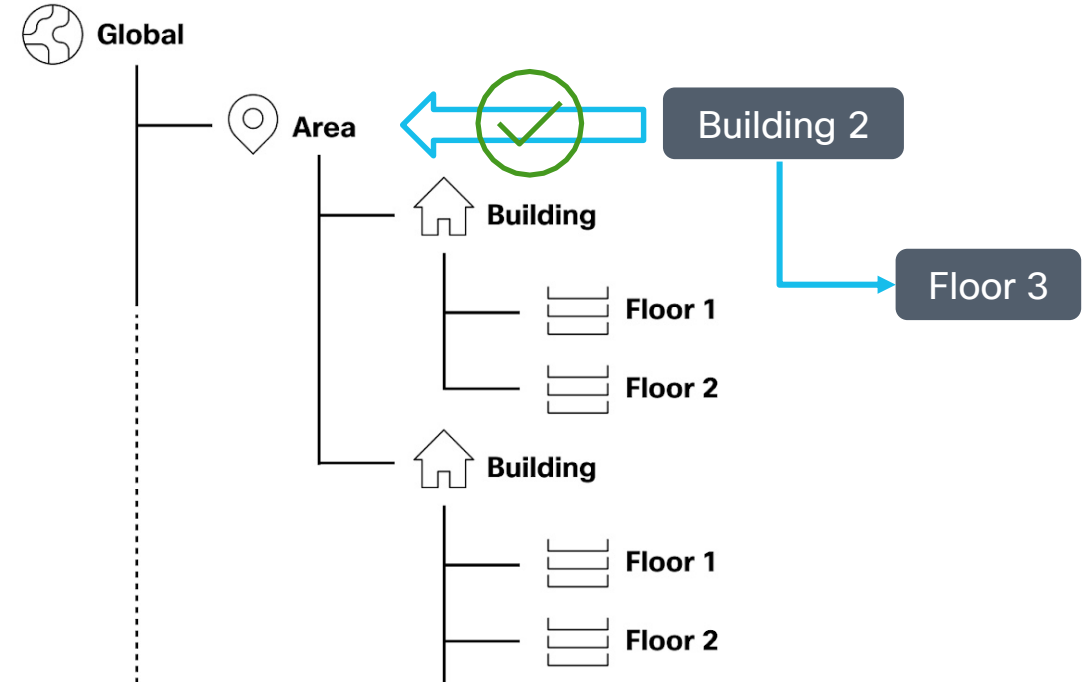
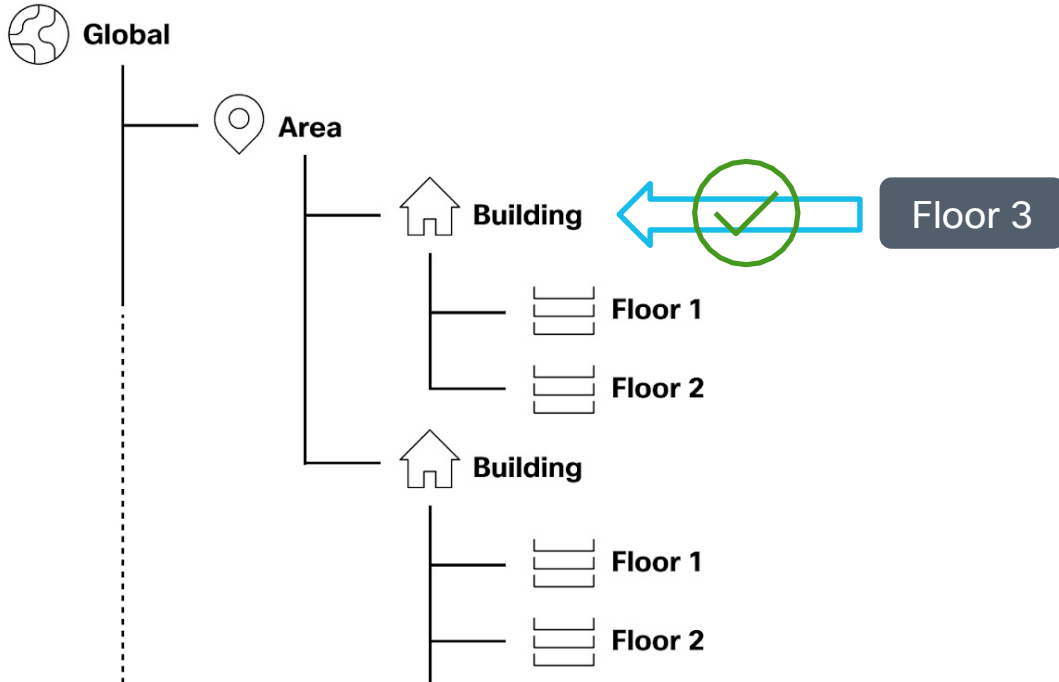
- Begin by importing the site hierarchy CSV using the "Import sites" function.
- Then, import the map archive using the "Import maps" function.
- Refer to the readme.txt file for additional instructions.
- Note that modifying any of the included files by yourself can lead to errors during import.

With Login



The screenshot shows the Ekahau dashboard interface. The top navigation bar includes the Ekahau logo, a search bar, and a "Warehouse Dashboard" section with a notification badge showing "99". A sidebar on the left contains navigation options like "Location", "Tags", "Sharing", "Dashboard", "Integrations", and "Floor 0 - Ground". The main content area features a large illustration of a laptop, a smartphone, and a tablet on a stack of books, with a gear icon. A modal window titled "Project export" is overlaid on the right side, displaying a blue checkmark icon and the text "Project export initiated. Please note that it can take up to 5 minutes for the export to be processed." Below this, it says: "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."

Catalyst Center-Ekahau Anchor Points



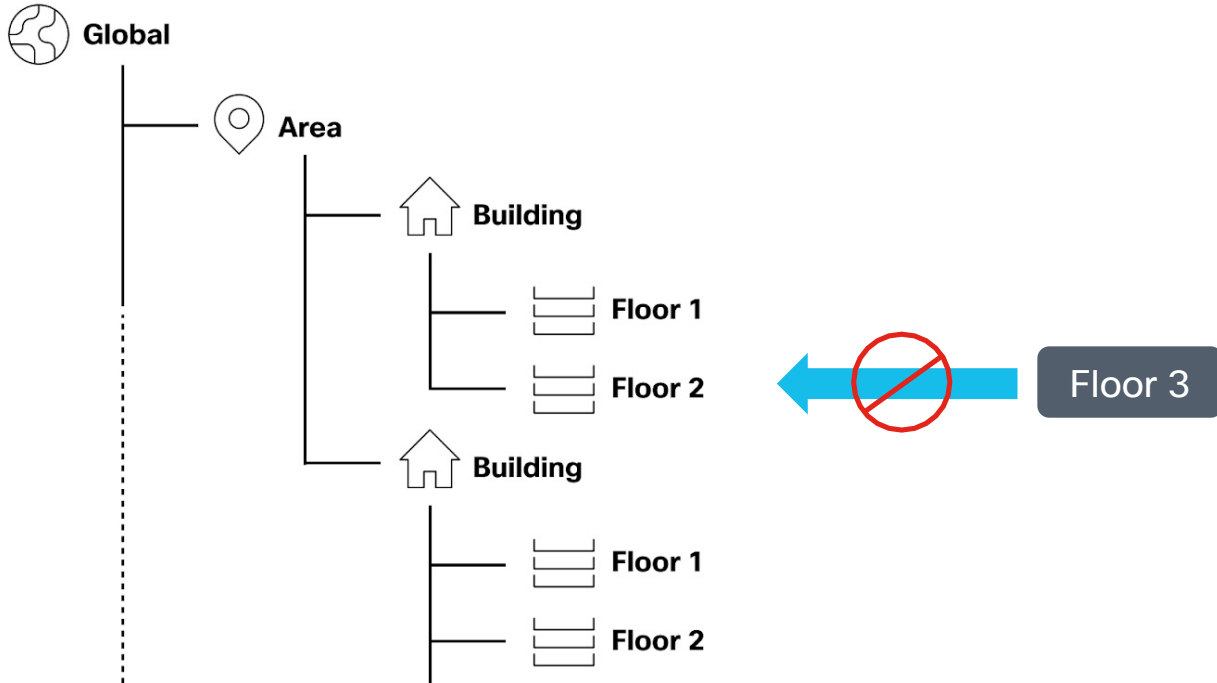
✓ If the floor already exist, then the floor is updated with changes

✓ If the floor does not exist, then a new floor is created.

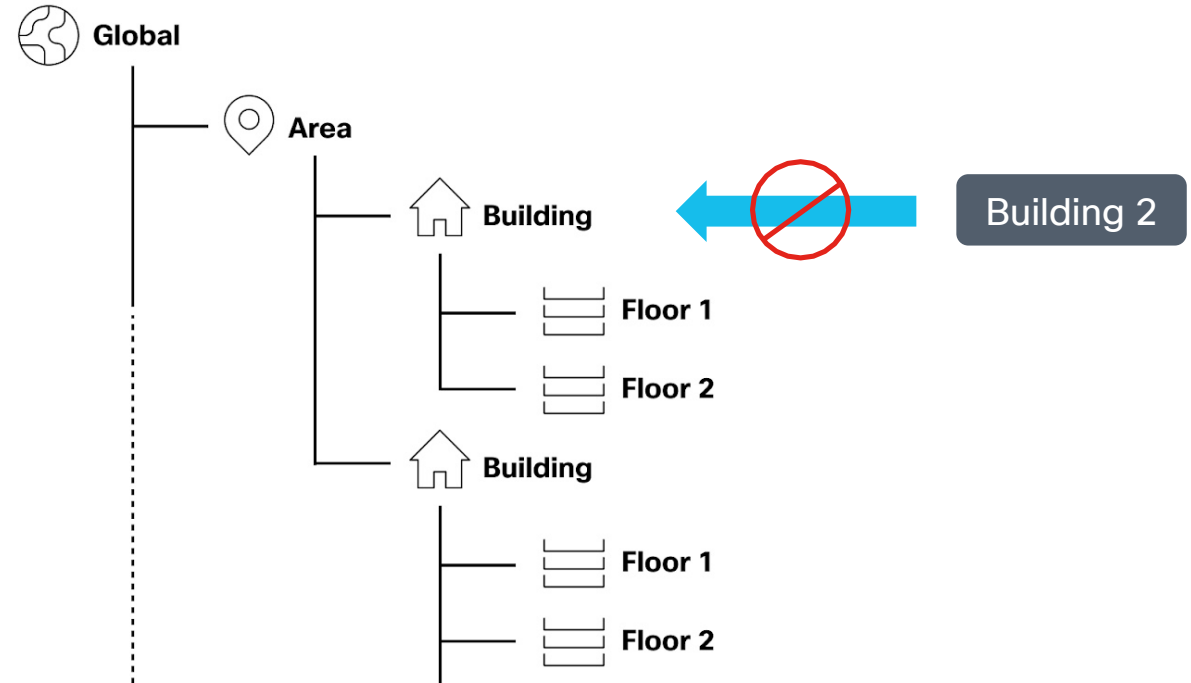
✓ If the building already exist, then the new floor is created

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

Catalyst Center-Ekahau Anchor Points



Floor is not an anchor point to import a new floor



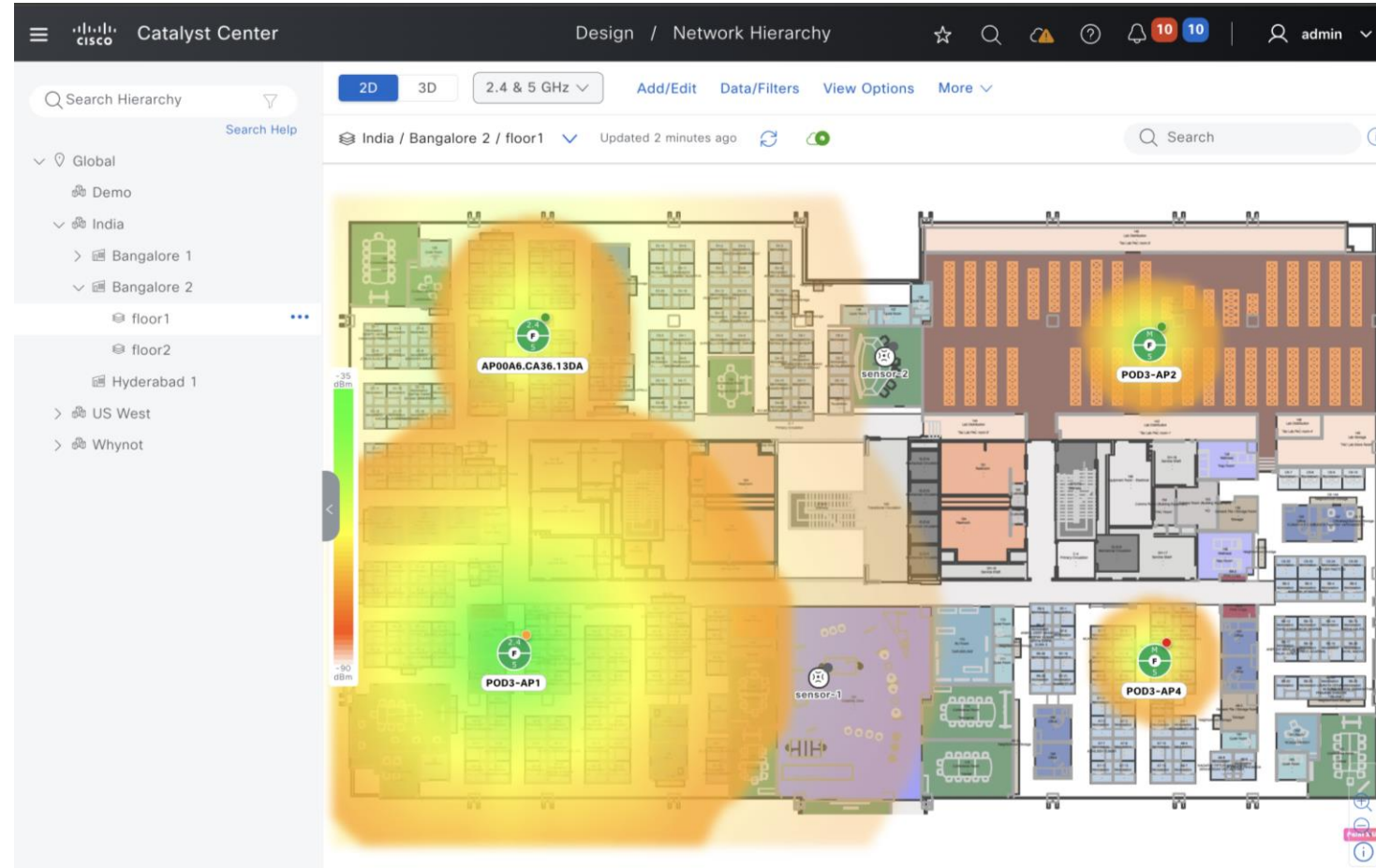
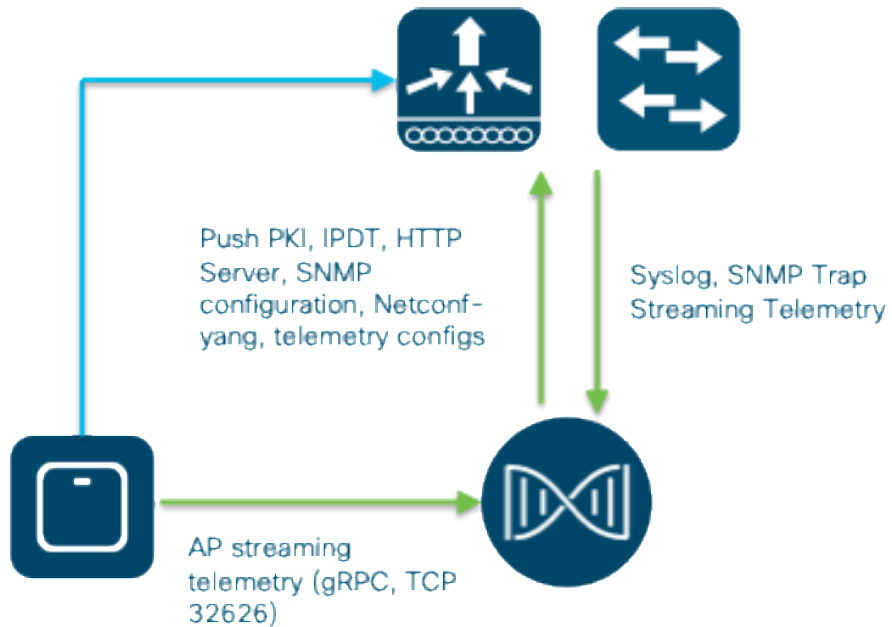
Building is not an anchor point to import a new building

“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



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

The screenshot displays the Cisco Catalyst Center interface. The top navigation bar shows 'Design / Network Hierarchy' and the user 'admin'. The left sidebar contains a 'Search Hierarchy' section with a tree view showing locations: Global, Demo, India (Bangalore 1, Bangalore 2), Hyderabad 1, US West, and Whynot. The main area shows a 2D floor plan map of 'India / Bangalore 2 / floor1' with a heatmap overlay. A detailed view of a 'Cisco Spaces Connector' is shown, providing the following information:

Cisco Spaces Connector Information	
IP Address / DNS Name	172.100.1.95
Status	Up
Version	3.1.0.156
Last Heard	Oct 1, 2024 4:37:26 PM

Adding WLC to Cisco Spaces

Map Spaces instance under Network Settings > Wireless

The screenshot shows the Catalyst Center interface. The breadcrumb navigation is Design / Network Settings / Wireless. The main heading is 'Cisco Spaces/CMX Servers'. Below the heading, 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. On the left, there is a 'Search Hierarchy' sidebar with a search bar and a list of locations: Global, Demo, India, US West, and Whynot.

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
```

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.

A status bar showing '3 / 3 connector(s) active'. To the right are two links: 'Create Connector' and 'View Connectors'.

Add Controllers

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

A status bar showing '1 / 1 controller(s) active'. To the right are two links: 'Add Controllers' and 'View Controllers'.

🔍 Search Hierarchy 🔽
[Search Help](#)

+ Add Site ↓ Import ↑ Export

🔍 Search for a building 🔊 ☰

- 📍 Global ⋮
- 🏢 Demo
- 📍 India
 - > 🏢 Bangalore 1
 - 📍 Bangalore 2
 - 🏠 floor1
 - 🏠 floor2
 - 🏢 Hyderabad 1
- > 🏢 US West
- > 🏢 Whynot



Device visibility and Network Segmentation are Critical



How do I know what's on my network?

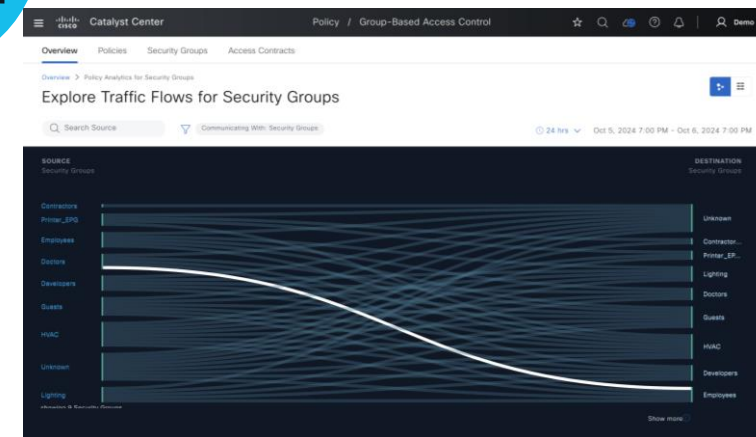
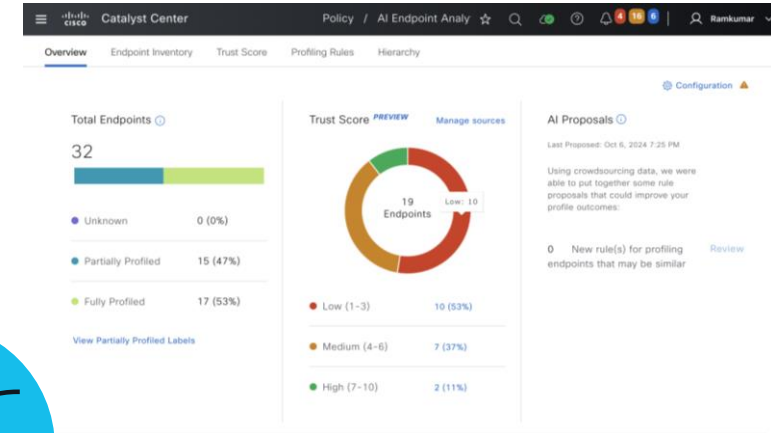
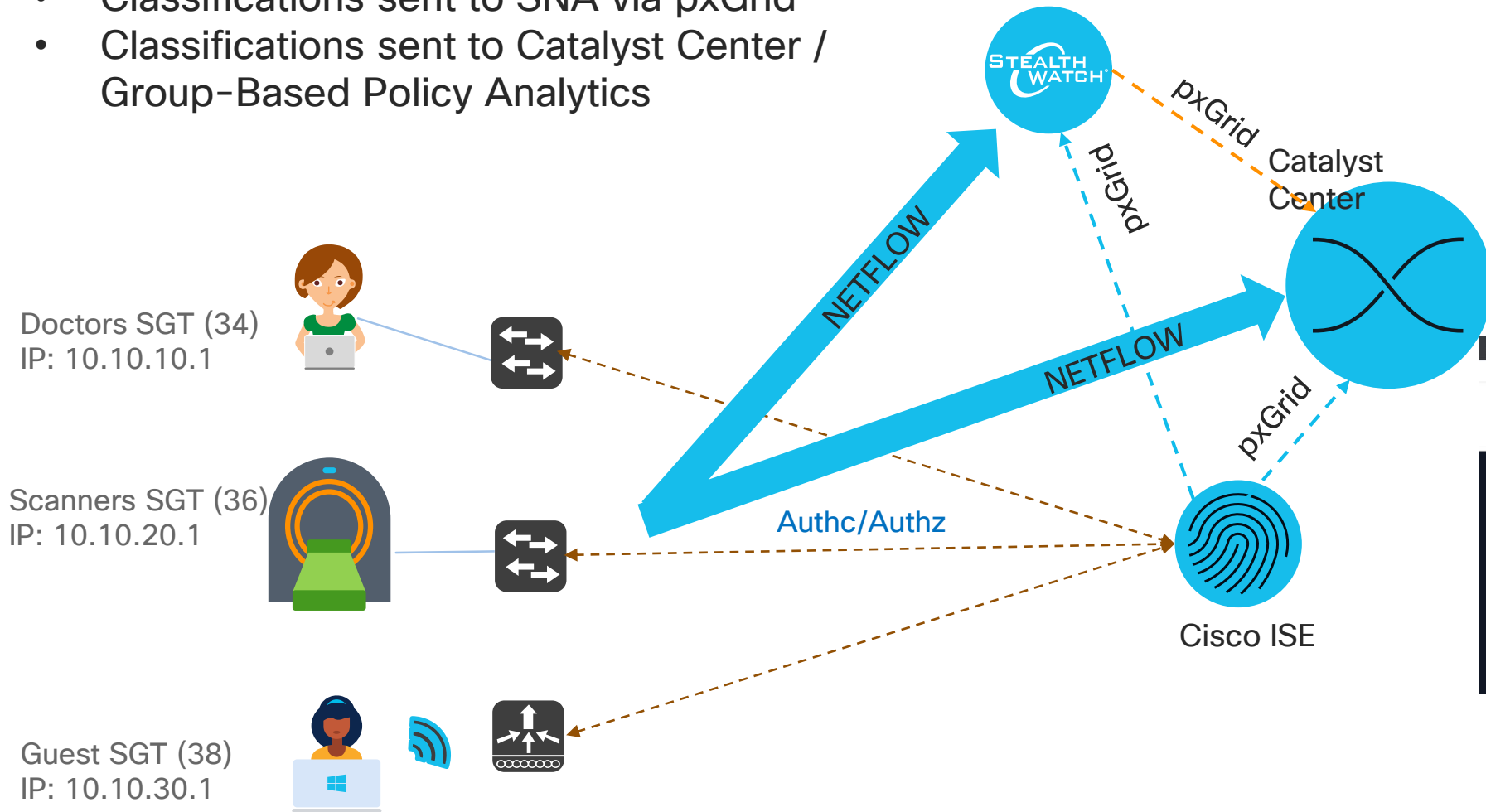
How do I make sure devices have right level of access?

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

The screenshot shows the Cisco ISE Administration / System interface. The top navigation bar includes 'Administration / System' and a menu. Below it, a secondary navigation bar lists various system functions: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, and Settings. The 'Deployment' section is active, showing a 'Deployment Nodes List' with one node 'ise34'. The 'Edit Node' page is open, displaying 'General Settings' and a 'Profiling Configuration' tab, which is highlighted with a red box. Below the tabs, a list of services is shown with toggle switches: NETFLOW (off), DHCP (on), DHCPSPAN (off), HTTP (off), RADIUS (on), Network Scan (NMAP) (on), DNS (off), SNMPQUERY (on), SNMPTRAP (off), and pxGrid (on). The 'pxGrid' toggle is also highlighted with a red box.



Ensure that pxGrid is enabled under Profiling configuration in ISE



Enable Custom Attribute for Profiling Enforcement



Enable Publishing and Consumption of endpoint attributes, then Save

The screenshot shows the Cisco ISE Work Centers / Profiler interface. The top navigation bar includes 'Work Centers / Profiler' and a menu. Below it, a secondary navigation bar lists various profiler functions: Overview, Ext Id Sources, Network Devices, Endpoint Classification, Node Config, and Feeds. The 'Overview' section is active, showing 'Profiler Settings' and 'Cisco AI Analytics'. The 'Custom Attribute for Profiling Enforcement' checkbox is checked and highlighted with a red box. Below it, the 'MFC Profiling and AI Rules' section is expanded, showing 'MFC (multi-factor classification) introduces four attributes for profiling endpoints. choose to disable MFC, AI rules will no longer be suggested. However, the MFC is' and 'Enable' checkbox checked. The 'Endpoint Analytics Settings' section is also expanded, showing 'Publish Endpoint Attributes to AI Endpoint Analytics' and 'Consume Endpoint Profiles from AI Endpoint Analytics' checkboxes, both checked and highlighted with a red box.

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 shows the Catalyst Center interface with the following details:

- Page Title: Authentication and Policy Servers
- Sub-page: Settings / External Services
- Instructions: 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.
- Buttons: Add (with dropdown), Export
- Refresh: As of: Sep 21, 2024 1:32 PM
- Table:

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

The left sidebar menu includes the following items:

- Device Settings
 - 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
 - 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 ISE Integration - AI Endpoint Analytics

System / Settings

Settings / External Services

Authentication and Policy Servers

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.

⊕ Add ^ ↗ Export

AAA	is	Protocol	Type
ISE			No data to display

Add ISE server

Server IP Address*
172.100.1.99

Shared Secret*
..... SHOW

Username*
admin

Password*
..... SHOW

FQDN*
ise34.tmelab.com

Virtual IP Address(es)
Info

Advanced Settings

Connect to pxGrid ⓘ

Enable Multiple Catalyst Center operation ⓘ

Cancel Save

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

Cisco ISE Integration - AI Endpoint Analytics

ISE server Integration

This is the first time Cisco Catalyst Center has seen this certificate from Cisco ISE, and it is not yet trusted. Do you want to accept this certificate and establish trust?

Integration of 172.100.1.99 is waiting for user input

Initiating connection...
less than a minute ago

This is the first time Cisco Catalyst Center has seen this certificate from Cisco ISE, and it is not yet trusted. Do you want to accept this certificate and establish trust?

View certificate

Accept Decline

Establishing trust...
Reading, validating, and storing trusted certificates

Discovering nodes...
Discovering Cisco ISE primary and secondary admin nodes and pxGrid nodes

Connecting to pxGrid...
Loading and validating pxGrid certificates, subscribing to pxGrid topics

Click to Accept ISE Certificate

System / Settings

Settings / External Services

Authentication and Policy Servers

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

Add Export

IP Address	Protocol	Type
172.100.1.99	RADIUS_TACACS	ISE

ISE server Integration

Integration of Cisco ISE server 172.100.1.99 was successful. Visit [System 360](#) to view health status.

Initiating connection...
Connecting to Cisco ISE and validating credentials

Establishing trust...
Reading, validating, and storing trusted certificates

Discovering nodes...
Discovering Cisco ISE primary and secondary admin nodes and pxGrid nodes

Connecting to pxGrid...
Loading and validating pxGrid certificates, subscribing to pxGrid topics

Close

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, the text 'Catalyst Center', and the path 'System / Settings'. The left sidebar contains a search bar and a list of menu items: 'External Services' (highlighted with a red box), 'Umbrella', 'Authentication and Policy Servers', 'Integrity Verification', 'SD-Access Compatibility Matrix', 'IP Address Manager', 'Cloud Access Login', 'Cisco AI Analytics' (highlighted with a red box), 'Stealthwatch', 'Talos IP Reputation', 'Destinations', 'Cisco Spaces/CMX Servers', 'Global Manager Integration', 'Machine Reasoning Engine', 'Cisco Catalyst Cloud', 'Webex Integration', and 'ThousandEyes Integration'. The main content area is titled 'AI Endpoint Analytics' and provides a description: 'Provides fine-grained endpoint identification and assigns labels to a variety of Endpoints.' Below this, the 'ENDPOINT SMART GROUPING' section is described: '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 and the switch turned on (highlighted with a red box). The 'AI SPOOFING DETECTION *PREVIEW*' section is described: '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 shown, with a checkmark and the switch turned on (highlighted with a red box). Below the toggles is an 'Update' button. At the bottom, there is a 'Cloud Data Storage' section with 'Europe (Germany)' selected, a 'Deployment ID' of 'vemc1jx2', and a link to '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 for configuring Telemetry settings. The breadcrumb path is Design / Network Settings. The left sidebar shows a hierarchy: Global > Demo > India > US West > Whynot. The main content area has a search bar and a description: "Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned." Below this, it states: "Catalyst 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." Two sections are highlighted with red boxes:

- Application Visibility:** "When assigning Catalyst 9000 or Traffic Telemetry Appliance devices to the site, enable NetFlow Application Telemetry and Controller-Based Application Recognition by default." There is an unchecked checkbox "Enable by default on supported wired access devices". Below, it says "Choose the destination collector for Netflow records sent from network devices." and has two radio buttons: "Use Catalyst Center as the Netflow Collector" (selected) and "Use Cisco Telemetry Broker (CTB) or UDP director".
- Wired Endpoint Data Collection:** "The primary function of this feature is to track the presence, location, and movement of wired endpoints in the network. Traffic received from endpoints is used to extract and store their identity information (MAC address and IP address). Other features, such as IEEE 802.1X, web authentication, Cisco Security Groups (formerly TrustSec), SD-Access, and Assurance, depend on this identity information to operate properly." Below, it says "Wired Endpoint Data Collection enables Device Tracking policies on devices assigned to the Access role in Inventory." and has two radio buttons: "Enable Catalyst Center Wired Endpoint Data Collection At This Site" (selected) and "Disable Catalyst Center Wired Endpoint Data Collection At This Site".

At the bottom right, there are "Reset" and "Save" buttons.

Enabling Netflow on Devices- Switches



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

The screenshot shows the Cisco Catalyst Center Provisioning console. The top navigation bar includes 'Catalyst Center', 'Provision / Inventory', and user information. A notification banner at the top states: '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.' Below this, there are filters for 'Global' and device types: 'All', 'Routers', 'Switches', 'Wireless Controllers', 'Access Points', and 'Sensors'. The main area displays a table of devices with columns for 'Tags', 'Device Name', 'IP Address', 'Inventory', 'Reachability', 'EoX Status', 'Manageability', 'Compliance', and 'Site'. A search filter 'deviceName: (*POD4*)' is applied. The 'Actions' menu is open for the selected device 'POD4-C9300-Access1.tmelab.com', showing options like 'Inventory', 'Software Image', 'Provision', 'Telemetry', 'Device Replacement', 'Switch Refresh', 'Compliance', and 'More'. The 'Telemetry' option is highlighted, and its sub-menu is open, showing 'Enable Application Telemetry', 'Disable Application Telemetry', and 'Update Telemetry Settings'. The 'Enable Application Telemetry' option is highlighted with a red box.

Tags	Device Name	IP Address	Inventory	Reachability	EoX Status	Manageability	Compliance	Site
	POD4							
	POD4-Anchor	192.1				Managed	Non-Compliant	Assign
	POD4-AP1	192.1				Managed	NA	.../Bang
	POD4-AP2	192.1				Managed	NA	Assign
	POD4-AP3	192.1		Reachable	Not Scanned	Managed	NA	Assign
	POD4-AP4	192.168.4.16	NA	Reachable	Not Scanned	Managed	NA	Assign
<input checked="" type="checkbox"/>	POD4-C9300-Access1.tmelab.com	192.168.4.4	Cisco	Reachable	1 alert	Managed	Non-Compliant	.../Bang
	POD4-C9800-CL1.tmelab.com	192.168.4.7	Cisco	Reachable	1 alert	Managed	Non-Compliant	.../India

Enabling Netflow on Devices - WLC



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



WLC need not be provisioned for enabling Application telemetry



Supported for local, Flex/Fabric SSIDs

The screenshot shows the Cisco Catalyst Center interface. On the left, a table lists devices under 'Global'. The 'POD4-C9800-CL1' device is selected, and the 'Telemetry' action is chosen from the dropdown menu. The right pane shows the 'Enable Application Telemetry' configuration for the selected device. It includes a warning about network disruption and a note about disabling and re-enabling the feature. The configuration for 'POD4-C9800-CL1' shows 'Local' selected for the application telemetry source, with 'Flex/Fabric' and 'Include Guest SSIDs' options unselected. The 'Telemetry Source' is set to 'NetFlow'. At the bottom, there are 'Cancel' and 'Enable' buttons.

Tags	Device Name	Inventory
<input type="checkbox"/>	WLC	Software Image
<input checked="" type="checkbox"/>	POD4-C9800-CL1	Provision
<input type="checkbox"/>	POD4-3504-1	Telemetry
<input type="checkbox"/>	C9800-vWLC	Device Replacement
		Compliance
		More

4 Record(s)

Enable Application Telemetry

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

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).

Warning: 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.

POD4-C9800-CL1

Local Flex/Fabric

Include Guest SSIDs

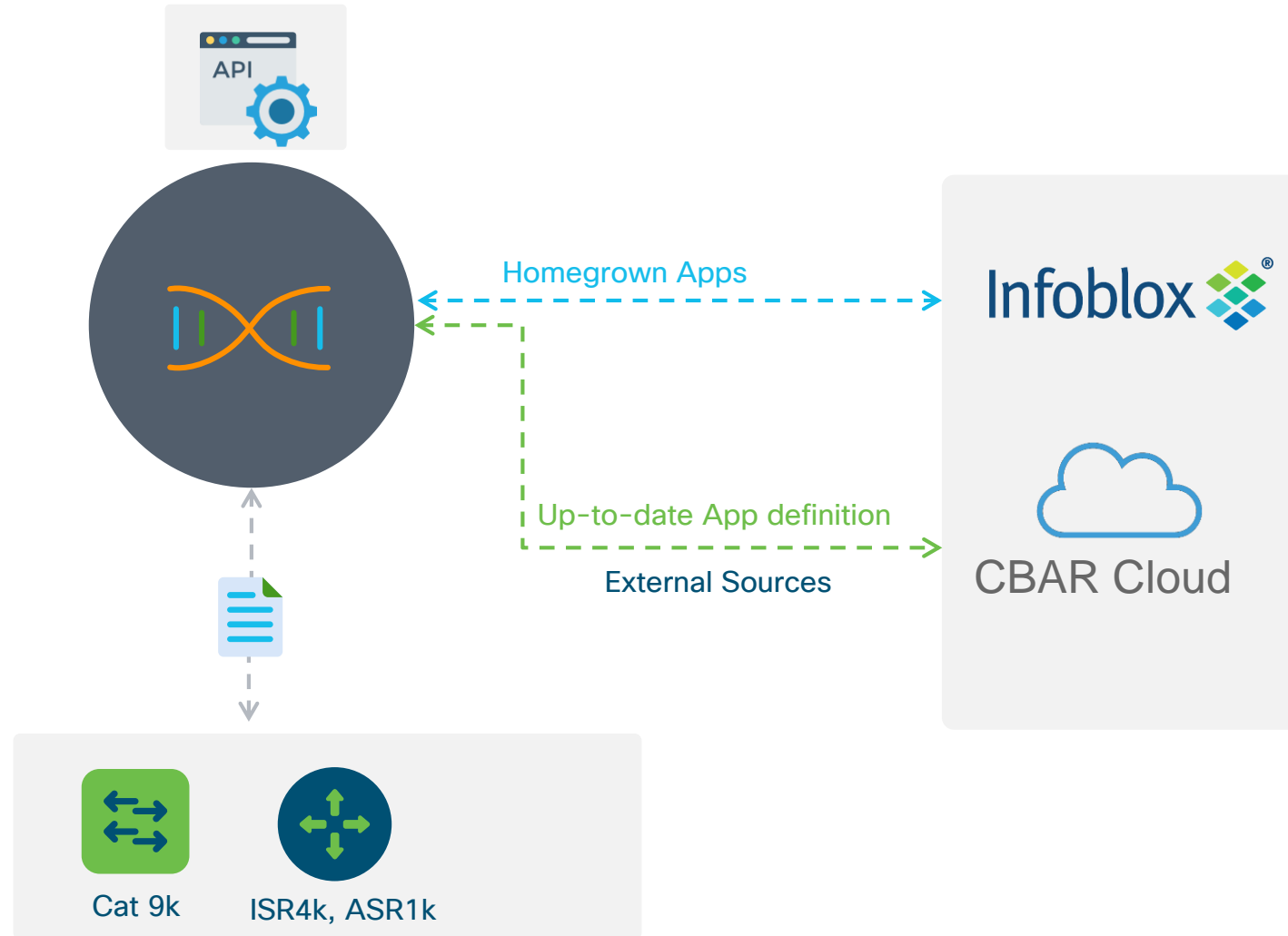
Telemetry Source: **NetFlow**

Cancel **Enable**

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



Device Role needs to be Access for it be Ready

The screenshot shows the Cisco Catalyst Center interface for Application Visibility. The page is titled "Network Devices Enablement" and shows 1479 Applications and 28 Application Sets. The "Site Devices (22)" section is active, with filters for Device Family (All, Routers, Switches, Wireless Controllers) and Active Recognition Method (All, CBAR, NBAR, IP/Port, Not Supported). The "CBAR Readiness" and "Telemetry Readiness" filters are set to "All".

A dropdown menu is open, showing options to "Enable CBAR on selected devices", "Enable CBAR on all ready devices", and "Disable CBAR on all devices". The table below shows the status of various devices:

Device	IP Address	Active recognition method	CBAR Deployment Status	Application Telemetry Readiness Status
9800-Edge	192.168.2.9	Network-based (NBAR)	Not deployed	Enabled
C9300-Edge	192.168.2.9	Network-based (NBAR)	Not deployed	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
- ⓘ 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 'Network Devices Enablement'. The page title is 'Network Devices Enablement' with 1479 Applications and 28 Application Sets. The 'Site Devices (22)' section shows filters for Device Family (All, Routers, Switches, Wireless Controllers) and Active Recognition Method (All, CBAR, NBAR, IP/Port, Not Supported). A table lists devices with columns for Device name, Management IP, Device Role, and Application Telemetry Readiness Status. A context menu is open over the table, showing options: 'Update All Devices', 'Update Selected Devices', 'Update Selected Devices From File', 'Auto Update' (toggle), 'Include Selected Devices', and 'Exclude Selected Devices'. The 'Auto Update' toggle is currently off.

Device name	Management IP	Device Role	Application Telemetry Readiness Status
9800_Brownfield.tmelab.com	172.100.1.1	Access	Not deployed
C9300-3-Pod2.tmelab.com	192.168.2.5	Access	Not deployed
C9300-Edge	192.168.2.5	Access	Not deployed
C9300Access-1-Pod2.cisco.com	172.100.1.199	Access	Not deployed
C9300Access-1-POD3.tmelab.com	192.168.3.3	Access	Not deployed
C9300Access-2-Pod2.tmelab.com	192.168.2.5	Access	Not deployed
CE-1	172.100.1.20	Access	Not deployed

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 navigation links for 'Provision / Services / Application Visibility'. The main content area is titled 'Service Catalog / Application Visibility' and features a search bar and a navigation tree on the left. The central dashboard shows '1482 Applications' and '31 Application Sets'. A donut chart displays '947.2M Observed Traffic' with a legend: (88.2%) Classified, (11.8%) Unclassified, and various sub-categories like ipfix, netflow, snmp, ms-services, and ssh. Below the chart, a table lists discovered applications with columns for Server Name, BW, Application Name, Application Set, and Traffic Class. The 'Import' button in the table's toolbar is highlighted with a red box.

Server Name	BW	Application Name	Application Set	Traffic Class
<input type="checkbox"/> dnaservices.cisco.com	13.09 MB (0.7%)	dnaservices	general-misc	Transactional Data
<input type="checkbox"/> 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.

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 navigation links for 'Provision / Services / Application Visibility'. The user is logged in as 'admin'. The main content area is titled 'Application Visibility' and has tabs for 'Overview', 'Network Devices Enablement', '1479 Applications', '28 Application Sets', and 'CBAR Extensions'. Under the 'CBAR Extensions' tab, there is a section for 'CBAR Cloud' with a toggle switch labeled 'Enable' that is currently turned on. Below this, there is a checkbox for 'Improve network visibility by sharing telemetry' which is also checked. The 'CBAR Dynamic Application Feeds' section shows a list of applications with their last update times and the number of applications. The applications listed are: 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.

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 'Cisco Catalyst Cloud' selected. The main content area is titled 'Cisco Catalyst Cloud' and includes a registration status box with the following details:

- Registered to: Cisco Catalyst Cloud Portal
- Registered by: pl [redacted]@gmail.com
- Account: AssuranceBlr
- Registered on: 6 October 2024

Below this is a 'De-register' button and a note: 'Click 'De-register' to unregister this Catalyst Center with Cisco Catalyst Cloud.'

The 'Applications (4)' section displays a table with the following data:

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 Catalyst Center interface for configuring the IP Address Manager. The left sidebar contains a search bar and a list of settings categories, with 'External Services' and 'IP Address Manager' highlighted with red boxes. The main content area is titled 'IP Address Manager' and 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 configuration form contains the following fields:

- 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** (Dropdown menu)
- 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.

At the bottom of the form are 'Delete' and 'Save' buttons. Red arrows on the right side of the image point to each of these fields with the following labels:

- Server Name
- URL/IP address of IPAM Server
- Credentials of the IPAM Server
- Provider Infoblox/Bluecat/Generic
- View to sync IP address pools created in CC to be synced in IPAM (For SDA Use Cases)

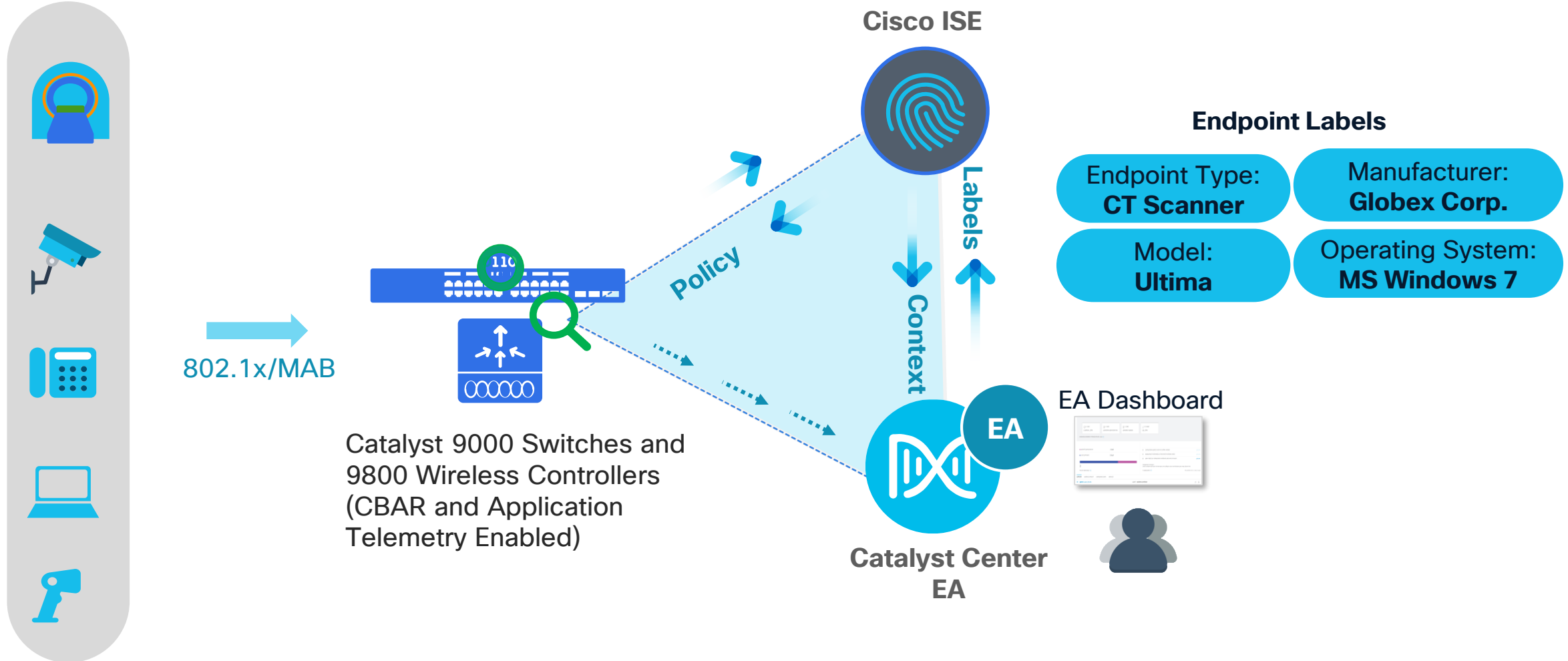
Enhancing CBAR with Infoblox DNS TXT/ A-Records

- ✓ 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

The screenshot displays the 'Infoblox Connector Settings' configuration page in the Cisco Catalyst Center. The page is titled 'Infoblox Connector Settings' and includes a navigation breadcrumb 'Provision / Services / Application Visibility'. The main content area is divided into sections: 'IPAM Server Details' with fields for 'Server Name: Infoblox' and 'Server URL: https://172.100.1.96'; 'DNS Zones to inspect*' with a dropdown menu; 'Inspect' with a dropdown menu set to 'TXT Record'; 'Read Application name from Route Name' with a checked checkbox; 'extensible attribute: app-name' with radio buttons for 'app-name' and 'AVC RRTYPE format'; 'Default Traffic Class' with a dropdown menu set to 'Transactional Data'; and 'Default Application Set' with a dropdown menu set to 'local-services'. A 'Save' button is visible at the bottom right.

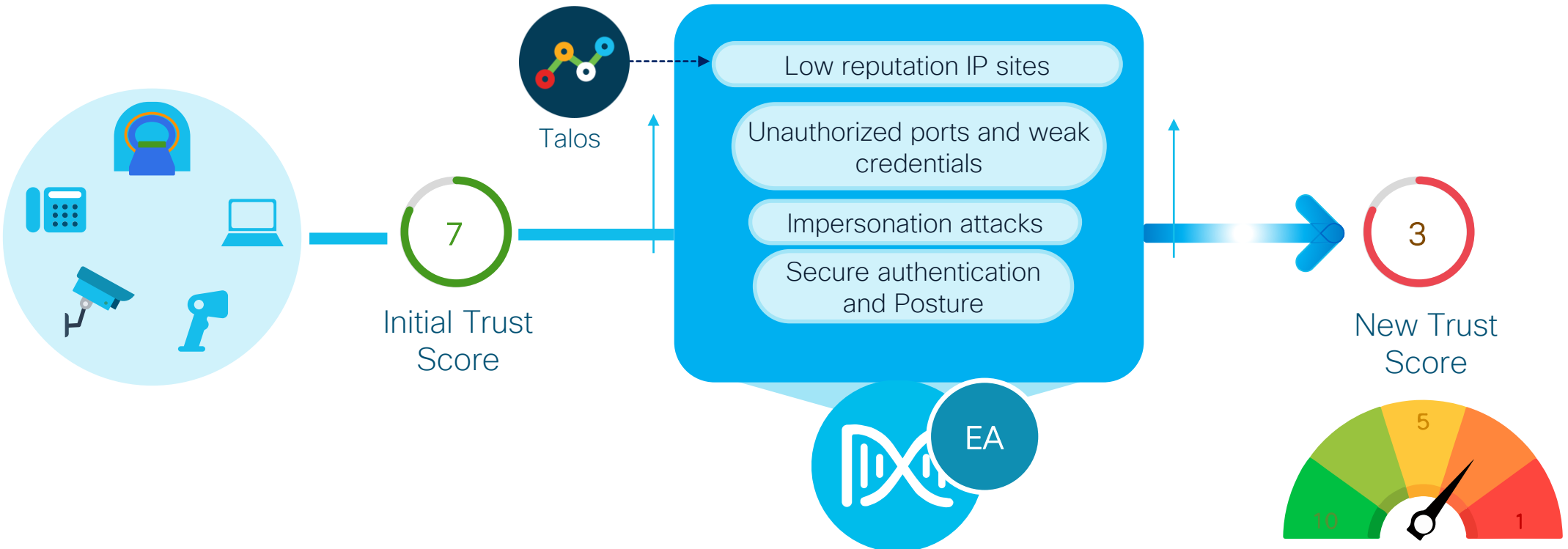
AI Endpoint Analytics

Endpoint profiling via CBAR and Application Telemetry



AI Endpoint Analytics

Continuous validation of endpoints for Trusted Access



Continuously monitors anomalies/threats, evaluate trustworthiness, and restrict access

AI Endpoint Analytics



Provides visibility on Endpoints which are Profiled and Unknown

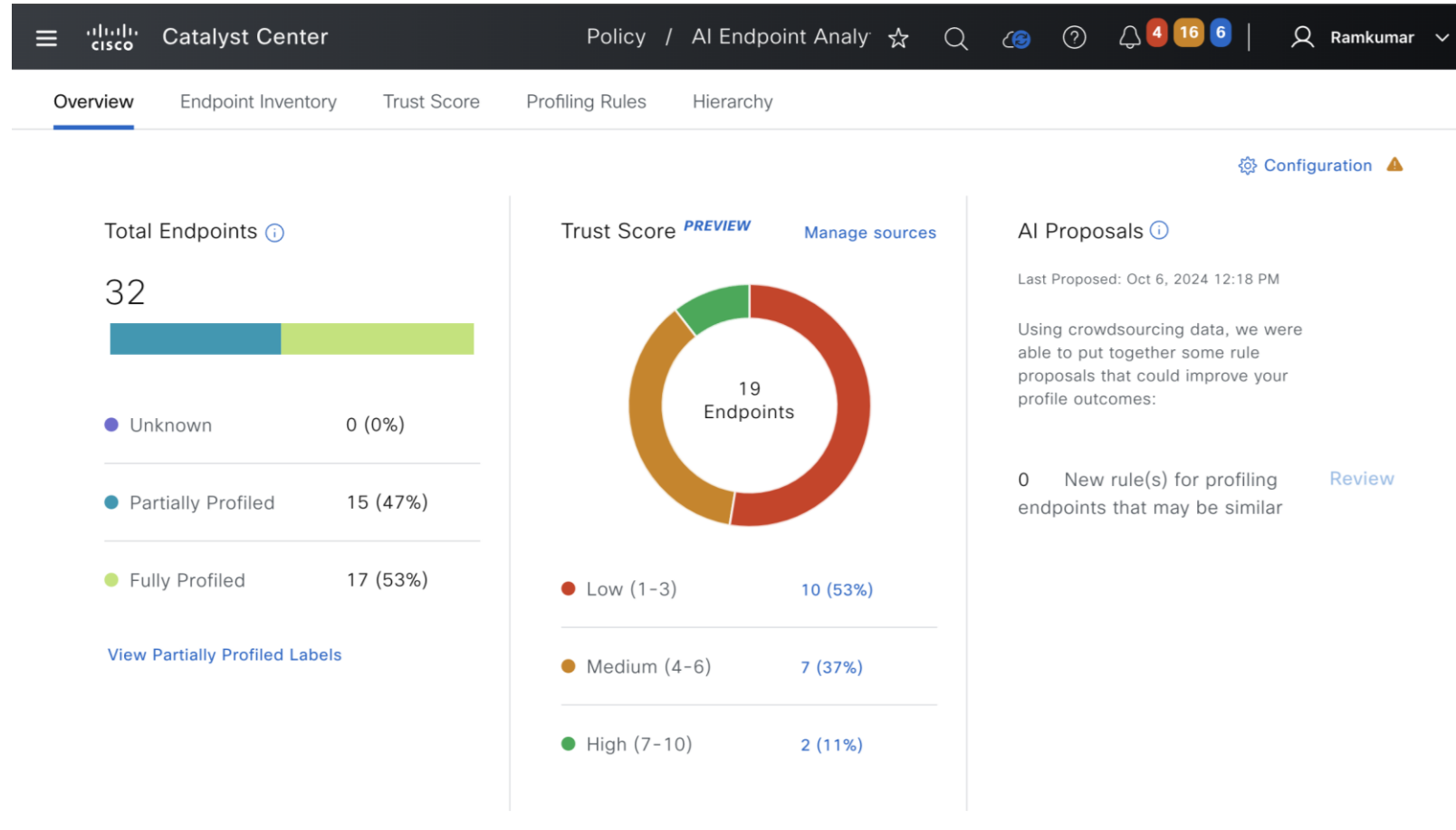


Provides Trust Score based on

- 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

The screenshot displays the Cisco Catalyst Center interface for AI Endpoint Analytics. The top navigation bar includes the Cisco logo, 'Catalyst Center', and a breadcrumb trail: 'Policy / AI Endpoint Analy'. The main navigation tabs are 'Overview', 'Endpoint Inventory' (selected), 'Trust Score', 'Profiling Rules', and 'Hierarchy'. The 'Endpoint Inventory' section shows 32 records with a focus on 'All Endpoints - Default View'. A search bar is present with the text 'Filter for endpoints by selecting values'. Below the search bar, there are options for '0 Selected', 'Register Endpoints', and 'More Actions'. An 'Export' button is also visible, dated 'As of: Oct 6, 2024 12:21 PM'. The table below lists several endpoints with their respective MAC addresses, random MAC status, trust scores (indicated by red or green dots), IP addresses, last seen timestamps, hostnames, and endpoint types.

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

AI Endpoint Analytics

✓ Navigate to Endpoint Inventory to view the details on endpoints

✓ View the trust score of devices, endpoint type

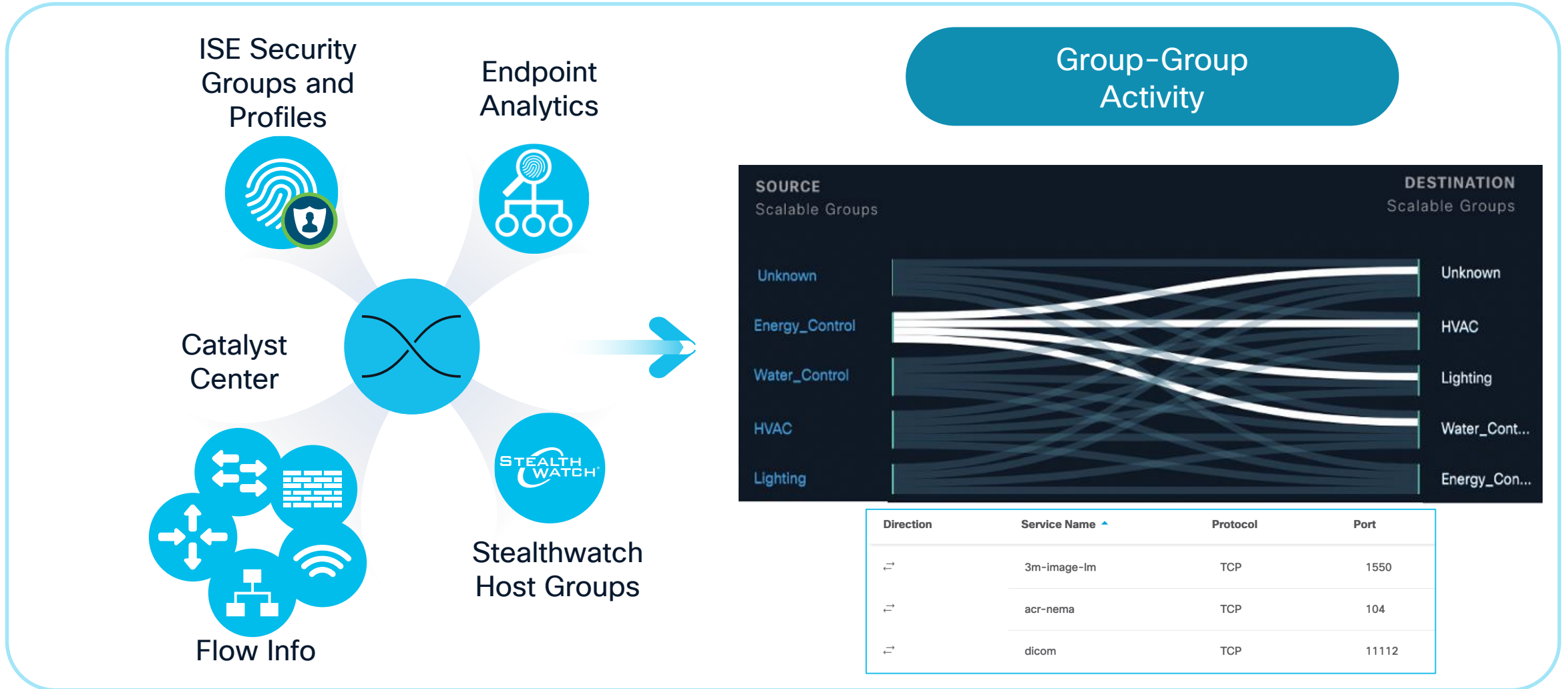
✓ Select an endpoint to view Trust score context

✓ Use the ANC policy option to trigger a CoA for the endpoint and place in Quarantine policy

The screenshot displays the Cisco Catalyst Center interface for AI Endpoint Analytics. The main view is the 'Endpoint Inventory' section, which lists 32 endpoints. A table shows columns for MAC Address, Is Random MAC, Trust Score, and IP. The endpoint with MAC address 00:50:56:8F:4D:8C is highlighted, showing a Trust Score of 3. The right-hand pane shows the details for this endpoint, including a 'Trust Score' of 3 and a 'Talos IP Reputation' status of 'Detected'. A red box highlights the 'Apply ANC Policy' button at the bottom right of the details pane.

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

Group-Based Policy Analytics



Stealthwatch - Catalyst Center Integration

Integration with SNA Management Console through System → Settings

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](#)

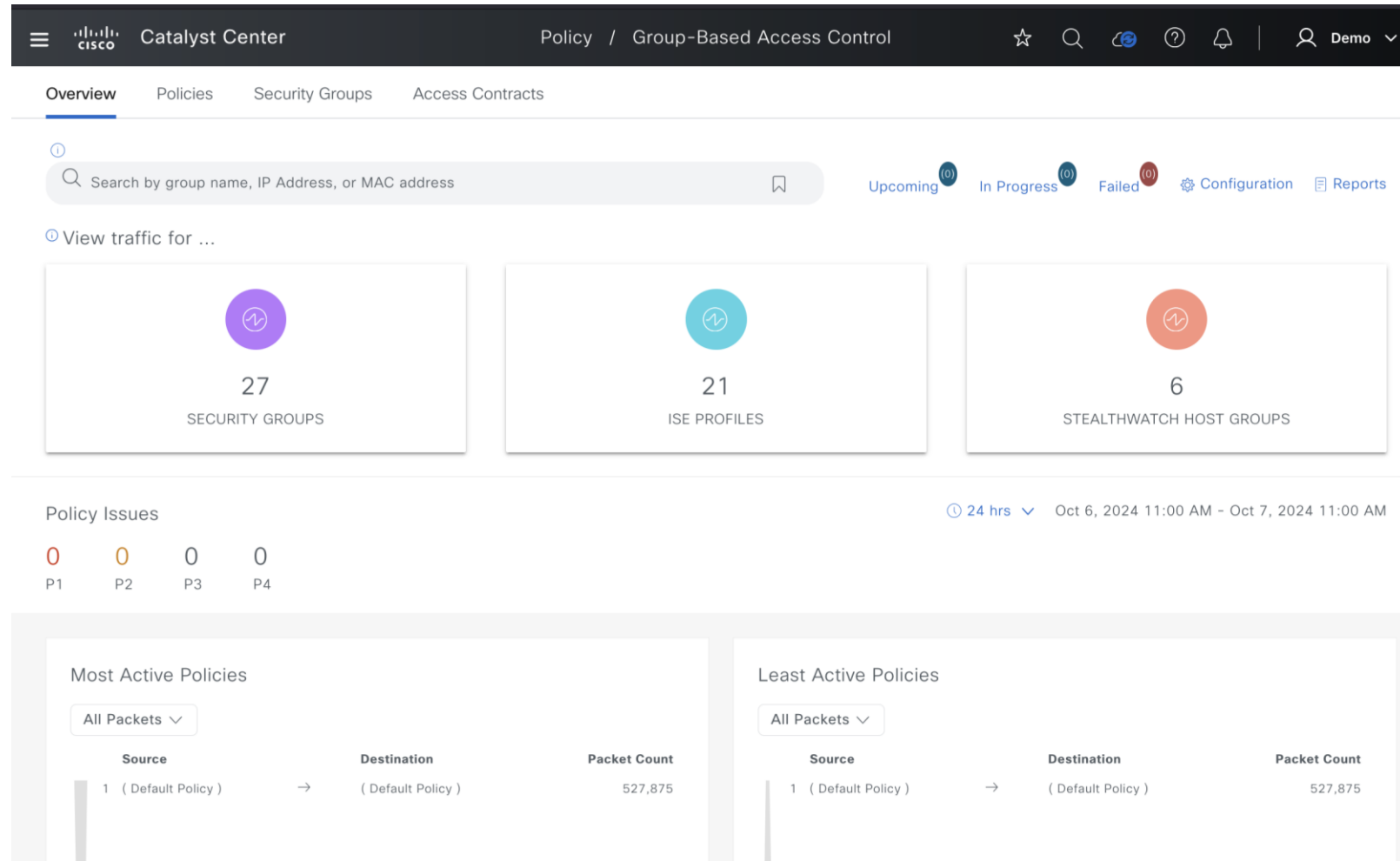
Click on warning to accept certificate

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

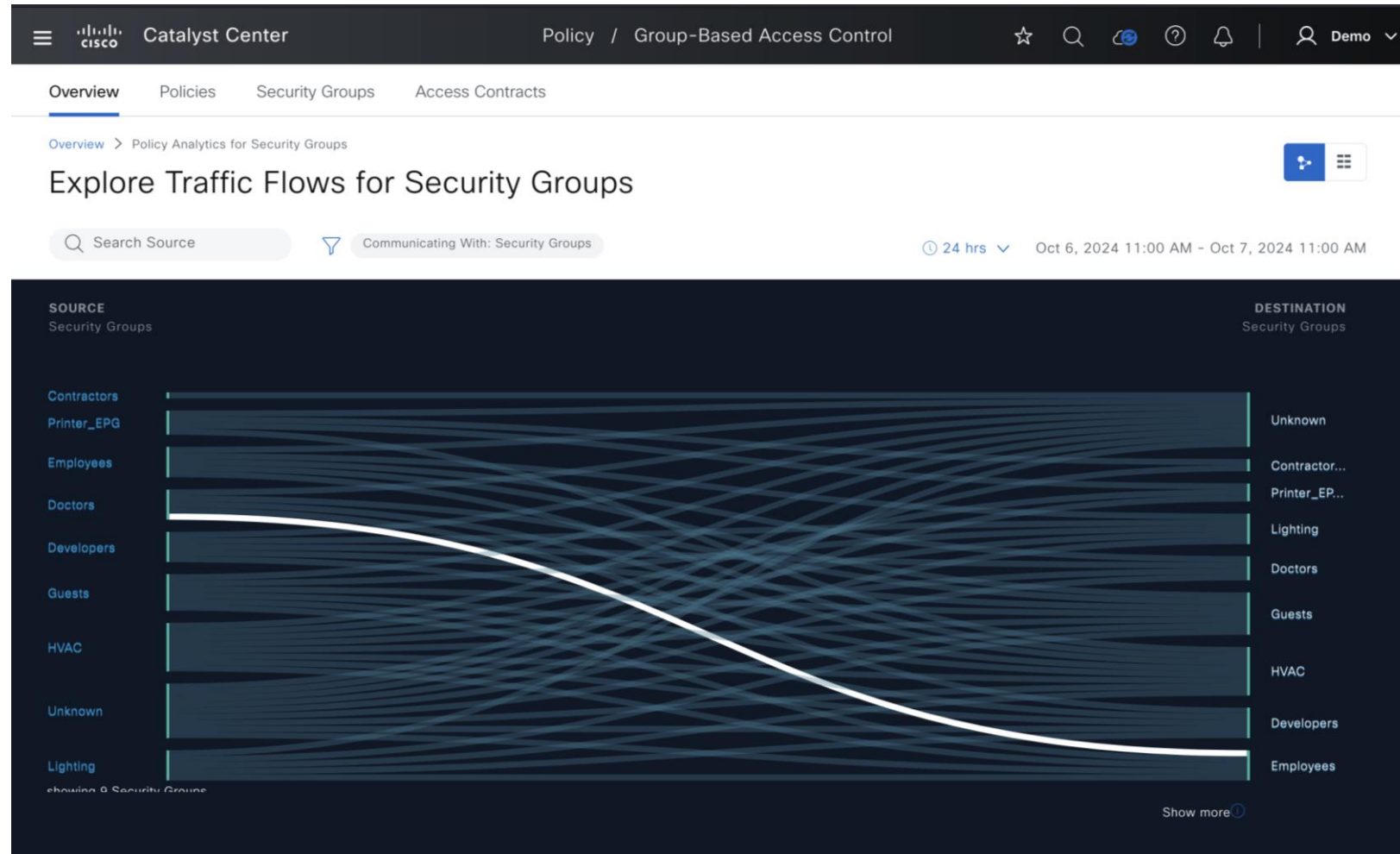


Group-Based Policy Analytics

✓ 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)

The screenshot displays the Cisco Catalyst Center interface for Group-Based Access Control. The main view is titled "Explore Traffic Flows for Security Groups" and shows a network flow visualization. A filter dialog is open, allowing users to select filter categories: "Security Groups", "ISE Profiles" (which is selected), and "Stealthwatch Host Groups". The background visualization shows traffic flows between source and destination security groups. The source groups listed include Contractors, Printer_EPG, Employees, Doctors, Developers, Guests, HVAC, Unknown, and Lighting. The destination groups listed include Unknown, Contractor..., Printer_EP..., Lighting, Doctors, Guests, HVAC, Developers, and Employees. The interface also shows a search bar for source groups and a time range filter set to "24 hrs" for the period "Oct 6, 2024 11:00 AM - Oct 7, 2024 11:00 AM".

Group-Based Policy Analytics



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 P

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

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

Default Action Logging [View traffic](#)

Group-Based Policy Analytics

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

Visualization of flows based on Netflow data

The screenshot shows the Cisco Catalyst Center interface for Policy Analytics. The breadcrumb trail is: Overview / Policy Analytics for Security Groups / SGT Assignment Not Available -> SGT Assignment Not Available / Contract Page / Endpoint List. The filters are: 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. A search bar is present above the table. The table has 7 columns: Source IP Address, Source MAC Address, Source Location, Destination IP Address, Destination MAC Address, Destination Location, and Flow Count. A red box highlights the row with Source IP Address ff02::2, Source MAC Address 70:F3:5A:7B:5B:51, Destination IP Address fe80::72f3:5aff:fe7b:5b51, and Flow Count 21.

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

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

The screenshot displays the Cisco Catalyst Center interface for Group-Based Access Control. The breadcrumb trail is: Overview > Policy Analytics for Security Groups > SGT Assignment Not Available > SGT Assignment Not Available > Contract Page. The current page is titled "SGT Assignment Not Available → SGT Assignment Not Available" with a "Default" filter. Under "Policy Details", it shows "Inherited from Default Policy" and two buttons: "Change contract" and "Create Access contract", both highlighted with a red box. Below this is the "CONTRACT CONTENT (1)" table:

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

At the bottom, the "Default Action" is set to "Permit" and "Logging" is toggled on. "Cancel" and "Next" buttons are visible.

On the right, the "All Unique Traffic Flows" section shows a table of traffic flows for the period Oct 6, 2024 12:00 PM - Oct 7, 2024 12:00 PM. The table has columns for Direction, Service Name, Protocol, Port, Flow Count, and Action. The "Add to contract" button for each row is highlighted with a red box.

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

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

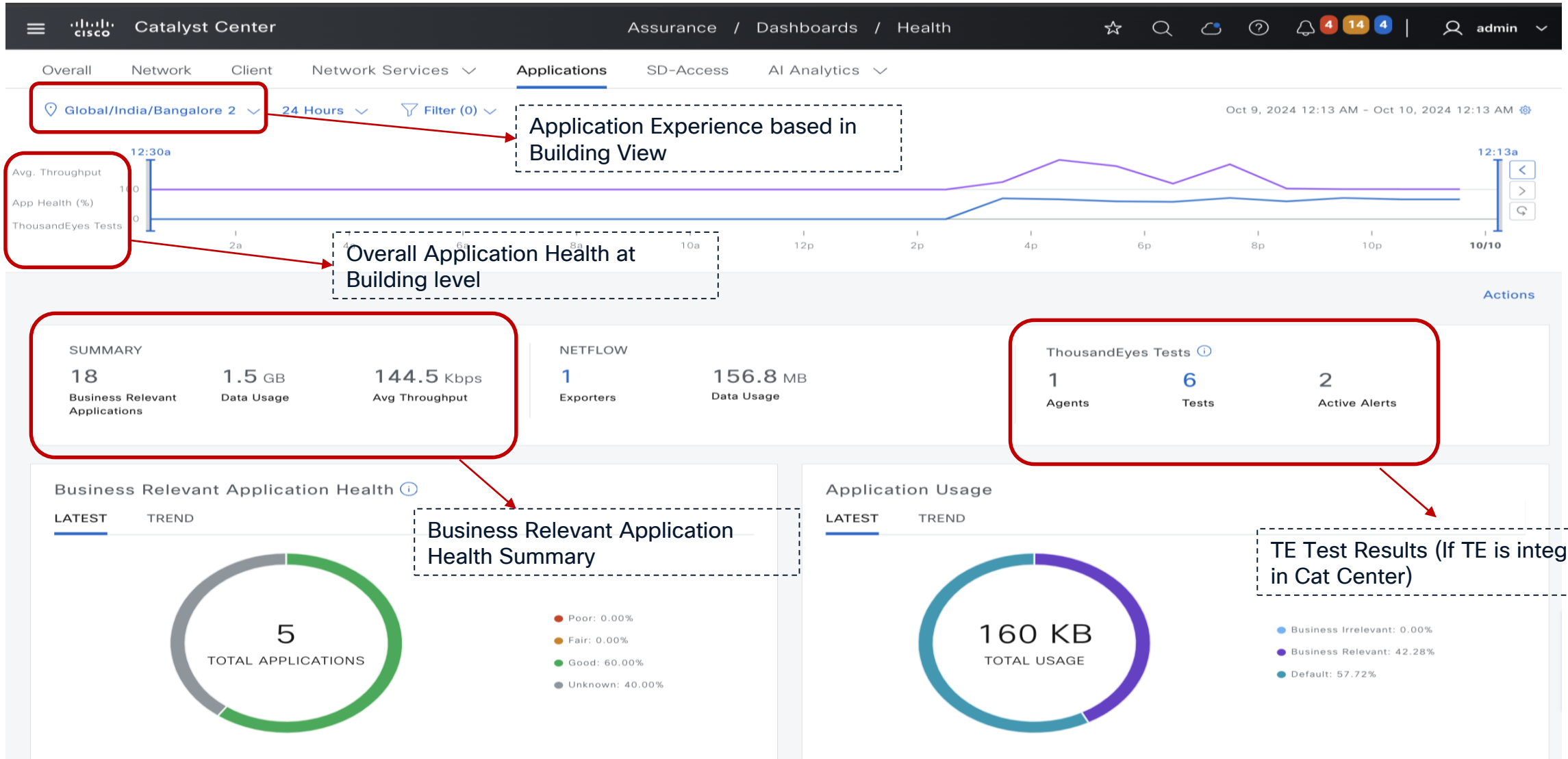
Code is fine. Don't care about anything else



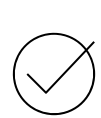
AppDev

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

Application Experience Dashboard



Application Experience- Application 360



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



Latency metrics based on

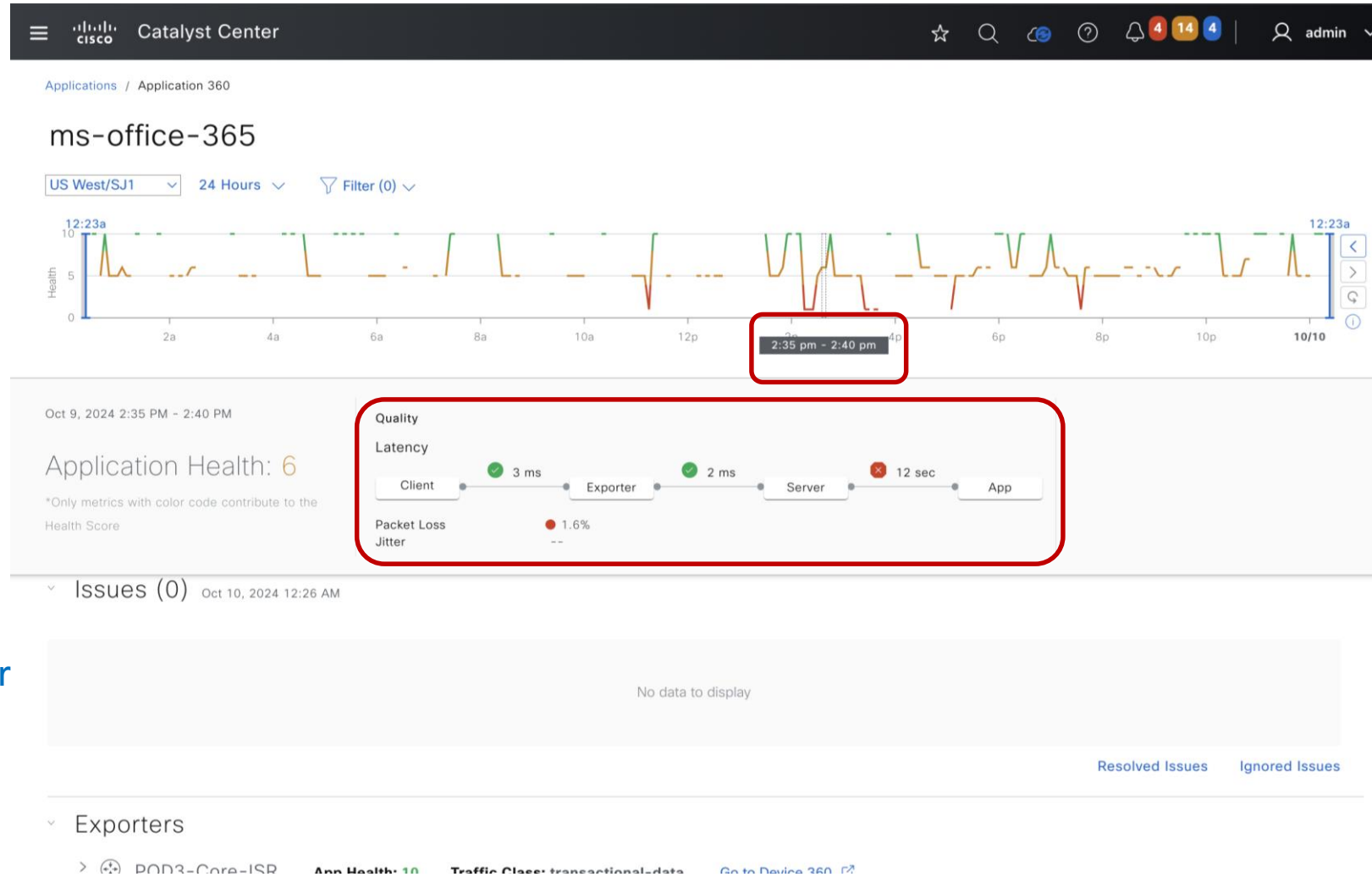
- Client to Exporter
- Exporter to Server
- Server to Application

Client Network Latency = Client to Exporter

Server Network Latency = Exporter to Server

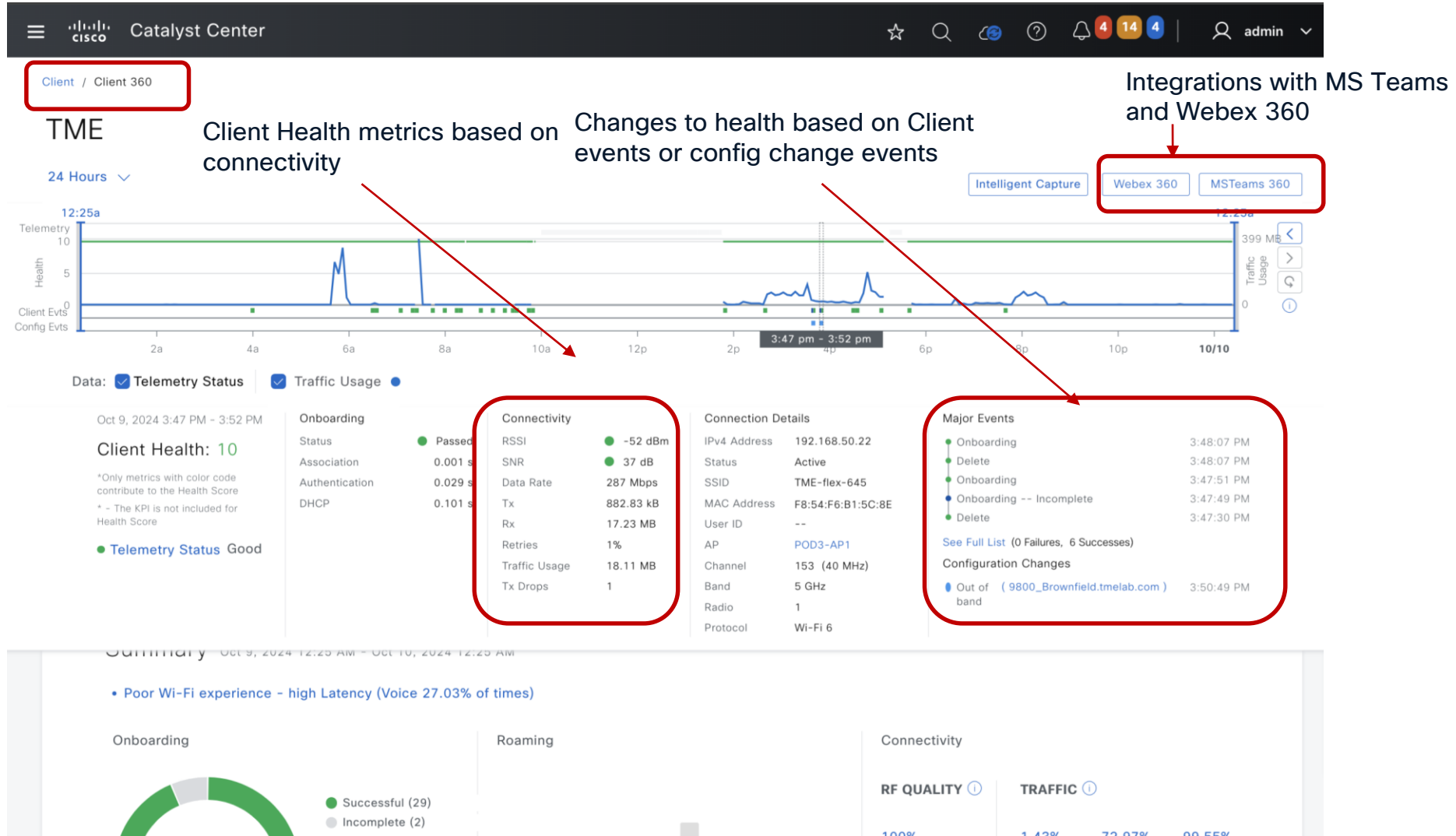
Application Server Latency = Server to

Application



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

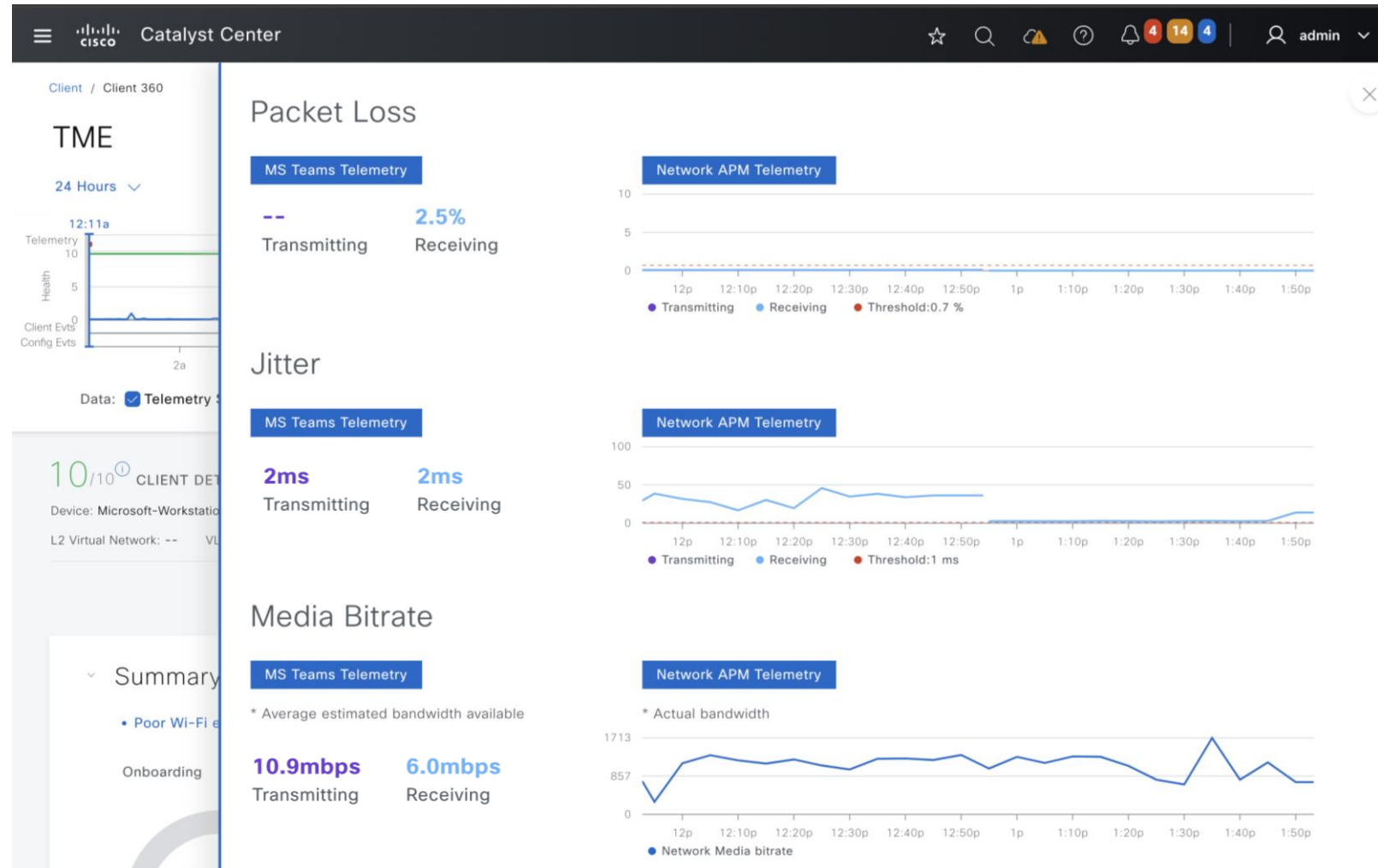
The screenshot displays the Cisco Catalyst Center interface for Client 360. The main view is titled "Application Experience for MS Teams: TME". It shows a table of meetings with the following columns: Meeting Name, MS Teams Score, Network APM Score, Duration, Start Time, End Time, Status, Meeting Type, and Participants. A single meeting is listed with a score of 10/10 and a duration of 02:00 h. Below the table, there are sections for "TEST-USER LONG LAST-NAME TESTING WITH HYPHEN PARTICIPATED IN A PEER-TO-PEER CALL" and "Packet Loss". The interface also includes a search bar, date filters, and a summary section with a "Summary" dropdown menu.

Meeting Name	MS Teams Score	Network APM Score	Duration	Start Time	End Time	Status	Meeting Type	Parti
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

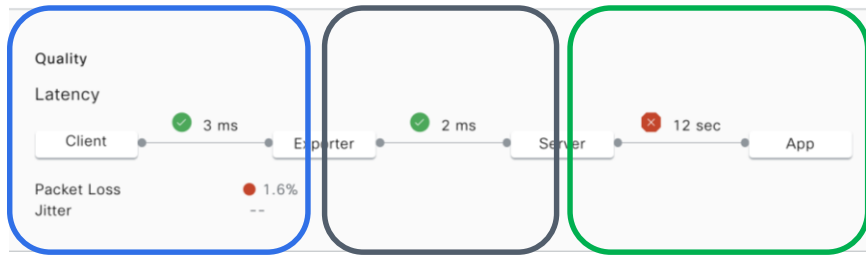


Catalyst Center MS-Teams Integration

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

The screenshot displays the Cisco DNA Center interface. The top navigation bar shows 'DNA Center' and 'System / Settings'. 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 (highlighted), 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 are four application cards, each with an 'Activate' button. The 'AppX MS-Teams' card is highlighted with a red border. The description for AppX MS-Teams reads: '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.'

Catalyst Center- Thousand Eyes Integration



Catalyst Center App Ex 360 View

Agent Test Path visualization provide details on latency between routed hops

The screenshot shows the Thousand Eyes Agent Test Path visualization interface. The path starts at C9300-3-Pod2 and ends at worldaz.tr.teams....m (S). The path consists of several hops, with IP addresses 192...100.1, 172.16.1.1, 192.168.99.1, 10.104.49.2, 116...57.97, 116...9.245, 104...2.129, and 116...57.99. The path is visualized as a line with nodes and links. The interface includes a sidebar with navigation options like Cloud & Enterprise Agents, Event Detection, Views, Test Settings, Agent Settings, BGP Monitors, Endpoint Agents, Cloud Insights, Devices, Internet Insights, Dashboards, Alerts, Integrations, and Sharing. The main area shows the path visualization with filters and controls.

Thousand Eyes Agent Test Path visualization

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: Configuration Archive, External Services (highlighted with a red box), 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 (highlighted with a red box), System Configuration, 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 block explains: 'Use this page to enable ThousandEyes integration. Once enabled, Cisco Catalyst Center can provide ThousandEyes tests information for Application Health dashboard.' A red box highlights a blue link: 'Go to ThousandEyes page to get the OAuth Bearer Token'. Below the link is a text input field labeled 'Insert new token here' and a 'Save' button.

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 navigation pane includes sections for Agents, Dashboards, Alerts, Integrations, Sharing, Account Settings, Activity Log, and Organization Settings. The 'Account Settings' section is expanded, with 'Users and Roles' selected. The main content area shows the user profile for 'Ramkumar Chellappa' (ramkchel@cisco.com) with roles 'Account Admin' and 'Regular User'. The 'User API Tokens' section shows a 'Basic Authentication Token' field and a red box around the 'OAuth Bearer Token Create' button.

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

Catalyst Center System / Settings

Settings / External Services

ThousandEyes Integration

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.

Use this page to enable ThousandEyes integration. Once enabled, Cisco Catalyst Center can provide ThousandEyes tests information for Application Health dashboard.

[Go to ThousandEyes page to get the OAuth Bearer Token](#)

Insert new token here

16d

Save

Catalyst Center – Thousand Eyes Test Results

Assurance / Dashboards / Health

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

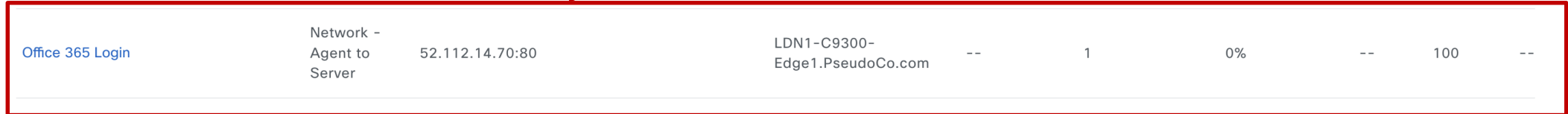
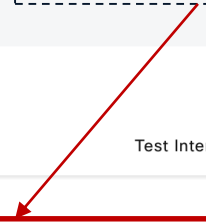
ThousandEyes Enterprise Agent Tests (6)

Search Table

Export

Test Name	Test Type	Target	Test Interval	Device Name	Last Updated	# of Active Alerts	Test Failures	Packet Loss (%)		
								Latest	Average	Lat
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



Integrations to Simplify Network Operations

Catalyst Center Destinations

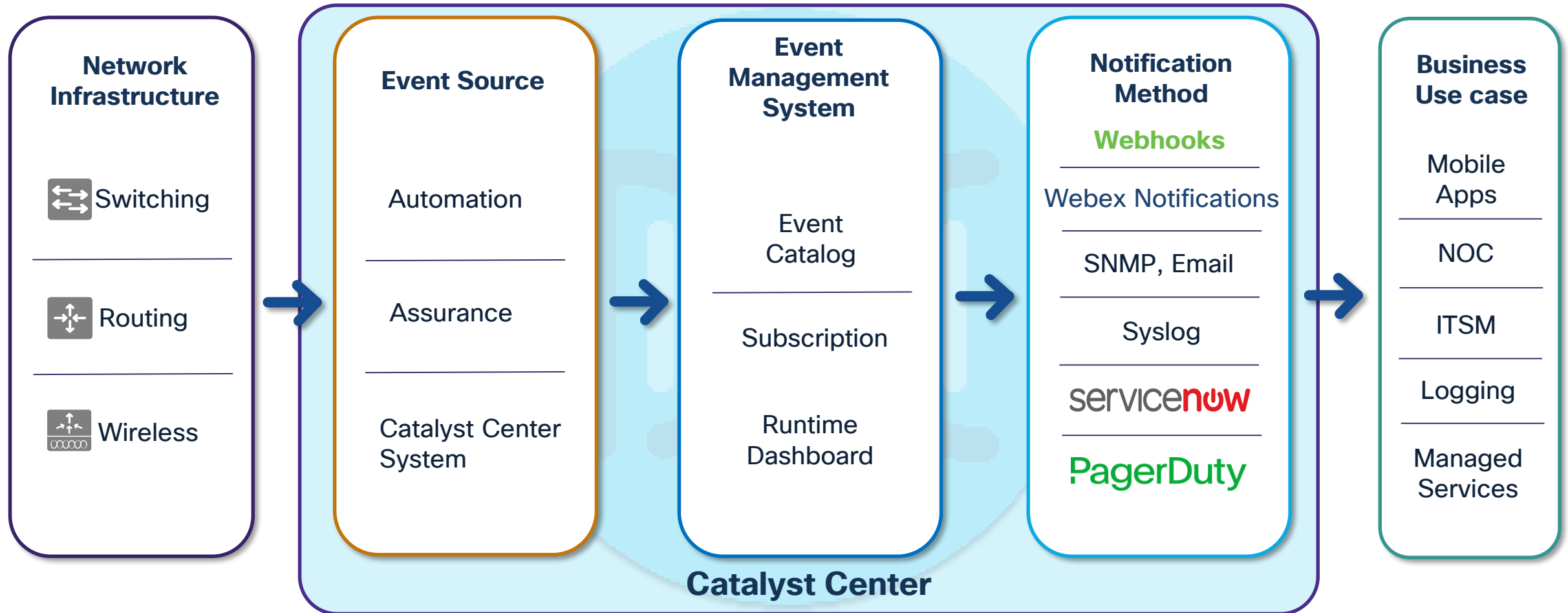
✓ Navigate to System > Settings > External Services > Destination to add various destination for event notifications

✓ Configure various external destinations

- Webhooks
- Email
- SNMP
- Syslog
- ITSM

The screenshot displays the 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 menu items, with 'Destinations' highlighted under the 'External Services' section. The main content area is titled 'Destinations' and shows the configuration for 'Email' notifications. The 'Primary SMTP Server' section is expanded, showing fields for 'Hostname/IP*' (173.37.93.161), 'Type*' (DEFAULT), 'Port' (25), 'Username', and 'Password'. The 'Secondary SMTP Server (optional)' section is also visible but empty.

Catalyst Center Event Notification Framework

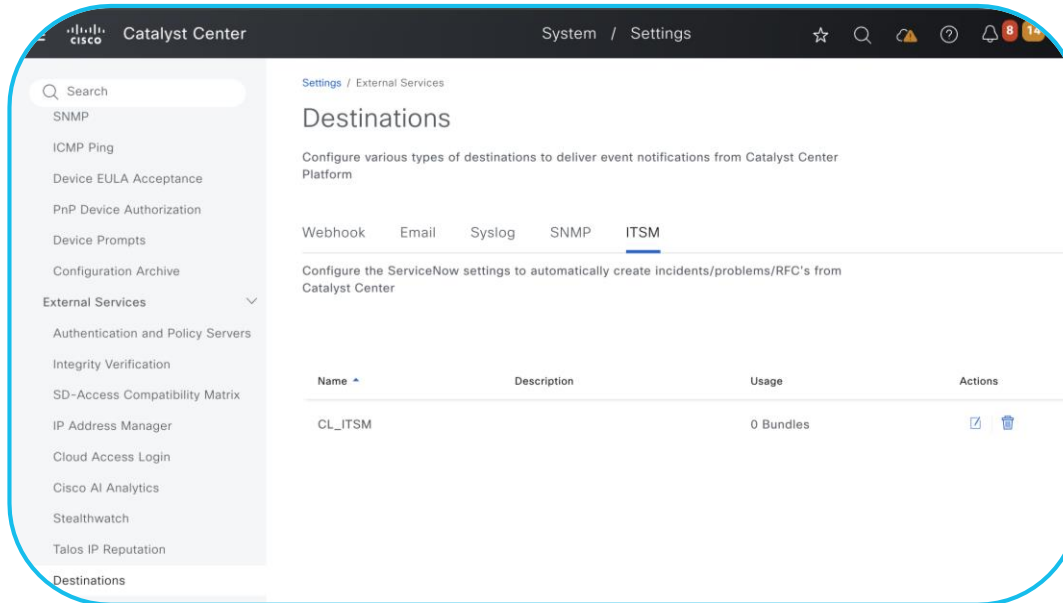


Catalyst Center ITSM Integration

Catalyst Center



+ servicenow

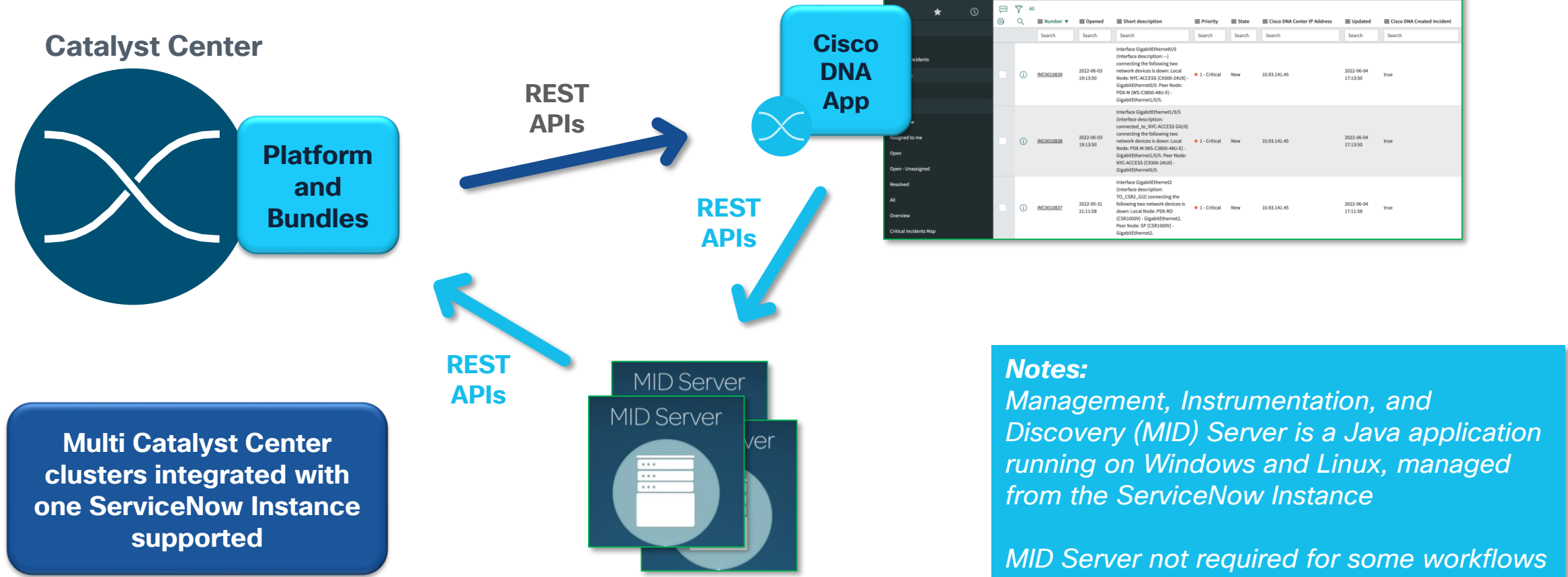


Catalyst Center ServiceNow Integration:

- 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

Cancel Add

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 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 settings categories: Global Manager Integration, Machine Reasoning Engine, Cisco Catalyst Cloud, Webex Integration, ThousandEyes Integration, System Configuration (highlighted with a red box), Debugging Logs, Visibility and Control of Configur..., Geo Map Settings, Proxy, High Availability, Multiple Cisco Catalyst Center S..., Integration Settings (highlighted with a red box), System Health, Login Message, Authentication API Encryption, Terms and Conditions, Product Telemetry, Trust & Privacy, Account Lockout, and Anonymize Data. The main content area is titled 'Settings / System Configuration' and 'Integration Settings'. It features a text input field for 'Callback URL Host Name or IP Address' with the value '10.104.49.195' entered. A red box highlights this field. Below the field are 'Clear' and 'Apply' buttons. A note below the field 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

The screenshot shows the Catalyst Center interface for managing bundles. The top navigation bar includes the Cisco logo, 'Catalyst Center', and 'Platform / Manage'. The main content area is titled 'Bundles' and features a 'Filter' button and a search bar. A table lists the following bundles:

Bundle	Status	Description	Action
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.	Enable
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...	Enable
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...	Enable
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...	Configure
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...	Configure

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 shows the Catalyst Center interface with the 'Integration Flows' tab selected. The 'Integrations' section is expanded, showing 'ITSM Integration'. The 'Schedule to Publish Inventory Details - ServiceNow Connector' integration flow is selected, and the scheduler configuration modal is open. The modal title is 'Schedule to Publish Inventory Details - ServiceNow Connector' and it is currently 'Not Scheduled'. The 'Description' field states: 'This scheduler discovers the devices in the network in a scheduled frequency and extracts the required device information to be able to sync the Inventory with an ITSM system.' The 'Tags' field contains 'ServiceNow'. The 'How to use this flow' section explains that integration flows can be scheduled to run periodically at a specified date/time. A note states: '* Schedule window cannot be lower than 24 hours'. The 'Repeats' dropdown is set to 'Daily'. The 'Set Schedule Start' checkbox is checked, and the start date is 'Oct 8, 2024' and the start time is '2:35 PM'. The 'Run Now', 'Run Later', and 'Recurring' radio buttons are visible, with 'Recurring' selected and highlighted by a red box.

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

Provision Device (C9300-Edge-Pod2) (1)

Last 6 hours ▾

As of: Nov 6, 2024 7:05 PM Refresh

API Summary ⓘ

Call Status

Total API's
0

Retry 0 Selected

Last In-Event Flow

Event Id	Source	Destination	ITSM Workflow	DNA Event Status	ITSM Status	ITSM Id	ITSM Link	ITSM T
33133d76-7ec7-4886-a23a-2963591c607c	ServiceNow	Cisco DNA Center	RFC	NA	New	CHG0030388	https://ven03091.servicenow.com/nav_to.do?uri=change_request.do?sys_id=57c33ecc47b91e1086c7bcff016d43da	Unas

Completed Call Performance

API Name ▲	Version
No da	

CMDB Synchronization Su

Search Table

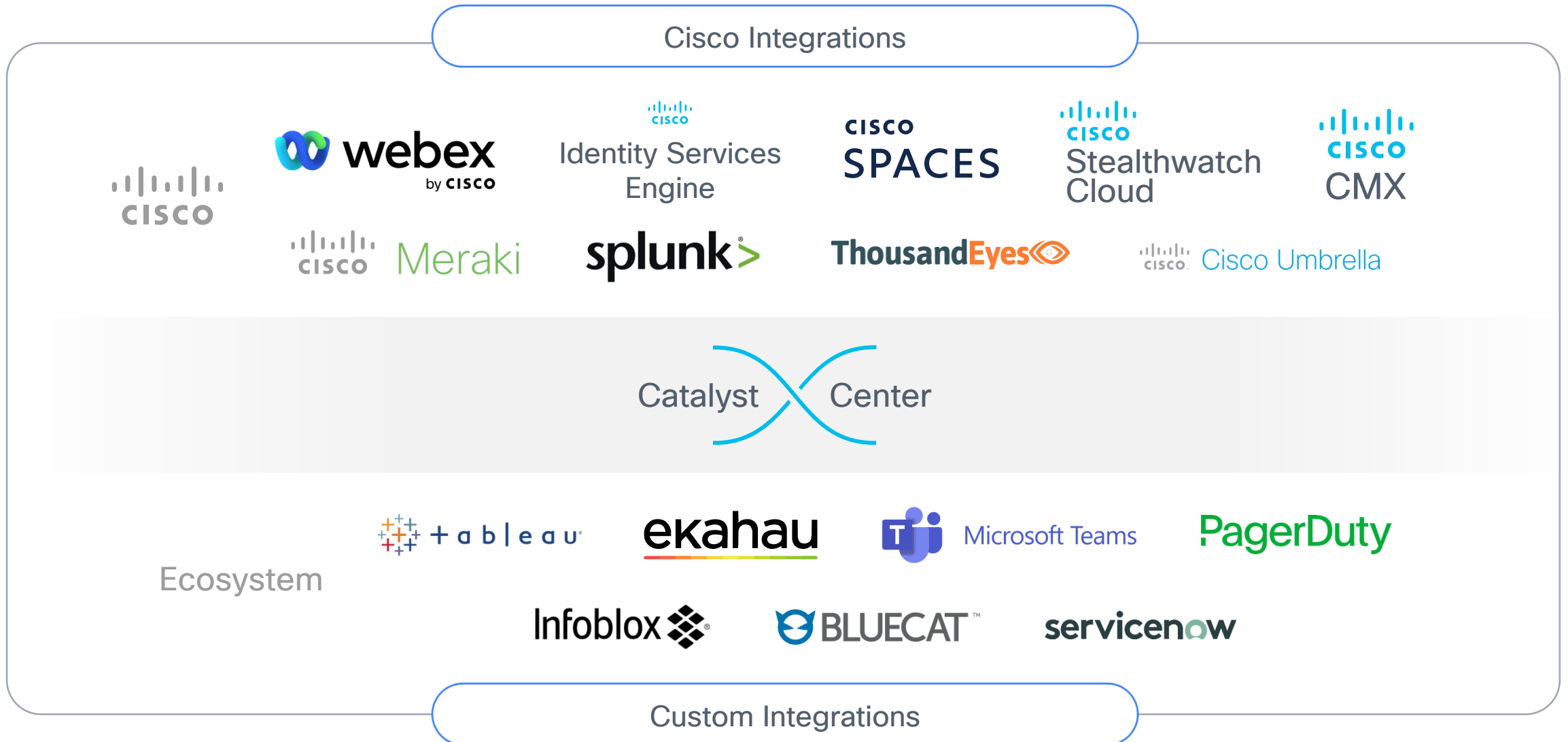
1 Record(s)

Show Records: 10 ▾ 1 - 1 < 1 >

Devices from Inventory ▲	De
42	42

Note: Incident number and link will not be available if MID server not operational. Incident may still be created.

Recap- Catalyst Center Integrations



Cisco Live US Catalyst Center Learning Map

Sunday—8th

TECOPS-2001 9:00AM

The Ultimate Guide to Install, Onboard, and Operate Your Campus Network with Cisco Catalyst Center

LTRSEC-2005 9:00AM

Building Cisco SD-Access with Cisco Catalyst Center & ISE

TECENS-2680 2:00PM

BGP EPVN in Enterprise Campus with Catalyst 9000 Switching Platforms

Monday—9th

BRKOPS-2698 8:00AM

Choosing the Right Cisco Catalyst Center Deployment Model for Your Network

CIUG-1100 10:00AM

Cisco Catalyst Center: AI-Driven Switching: Revolutionizing Automation and Assurance

LTRXAR-3783 1:00PM

Cross-Architecture Integration Experience Lab

BRKENS-1601 1:30PM

Catalyst Center and Meraki Cloud: The Right Choice for your Catalyst 9000 Switch Management!

BRKOPS-2609 1:30PM

Cisco Catalyst Center: Built-In Integrations for Streamlined Network Operations

LTROPS-2341 2:00PM

Build a Flexible Network Automation Workflow with GitLab CI/CD, Catalyst Center, NetBox, and Ansible

IBOENS-1100 2:30PM

Cisco Catalyst Center and SD-Access Design Fundamentals

BRKEWN-2029 4:00PM

Separating hype from reality, real world use cases of AIOps and Assurance for wireless within Catalyst Center

BRKCOC-2483 4:00PM

Cisco IT: Streamlining Network Management and Decisions with Catalyst Center Automation and Splunk

CISCOU-3004 5:00PM

Configuring and Troubleshooting Catalyst Center Templates

Tuesday—10th

BRKEWN-2306 1:30PM

Wireless Network Automation and Assurance with Cisco Catalyst Center

IBOOPS-2391 1:30PM

AI/ML in Cisco Catalyst Center: Transforming Network Operations!

BRKOPS-2697 2:00PM

Unlocking the Automation Power in Catalyst Center for Wired and Wireless Networks

DEVWKS-1004 2:30PM

Deploy Cisco Catalyst Center with Rest-API's

Wednesday—11th

DEVNET-2660 10:00AM

Catalyst Center Network Operations Essentials using UI and APIs

DEVNET-2176 10:30AM

Deploying Cisco Catalyst Center with CICD

BRKTRS-2821 2:30PM

Troubleshooting Strategies for Cisco Catalyst Center & SD-Access

BRKXAR-1013 2:30PM

4 Ways to Streamline Your Licensing with Cisco's Networking Subscription Across Your Portfolio

BRKOPS-2379 3:30PM

Automate Catalyst Center with Cisco Workflows

BRKOPS-2835 4:00PM

5 new things you need to know about Catalyst Center licensing

Thursday—12th

BRKIOT-2016 8:30AM

Streamline Your Success: Automating OT Services with Cisco Catalyst Center Best Practices

BRKOPS-2442 8:30AM

Leveraging Digital Twin for Advanced Network Management with Cisco Catalyst Center

DEVNET-3000 9:30AM

Open-Source GenAI Bot for Catalyst Center

BRKOPS-2570 10:30AM

AI-Powered Automation: Building Smarter Apps for Cisco Catalyst Center Operations

BRKOPS-2492 10:30AM

Let's Deploy Catalyst Center Global Manager (CCGM): Single Pane of Glass for Multiple Catalyst Centers

BRKOPS-2343 10:30AM

Decoding Site Reliability Engineering Through Catalyst Center

○ BU-led sessions

Catalyst Center

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.



Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live mobile app.

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer 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 !

