

7 Habits for Optimizing Your Cisco Catalyst Center Environments in 2026

CISCO Live !

Adam Radford
Distinguished Solutions Engineer
@adamradford123

Lila Rousseaux
Principal Solutions Engineer
@lila_rousseau

Webex App

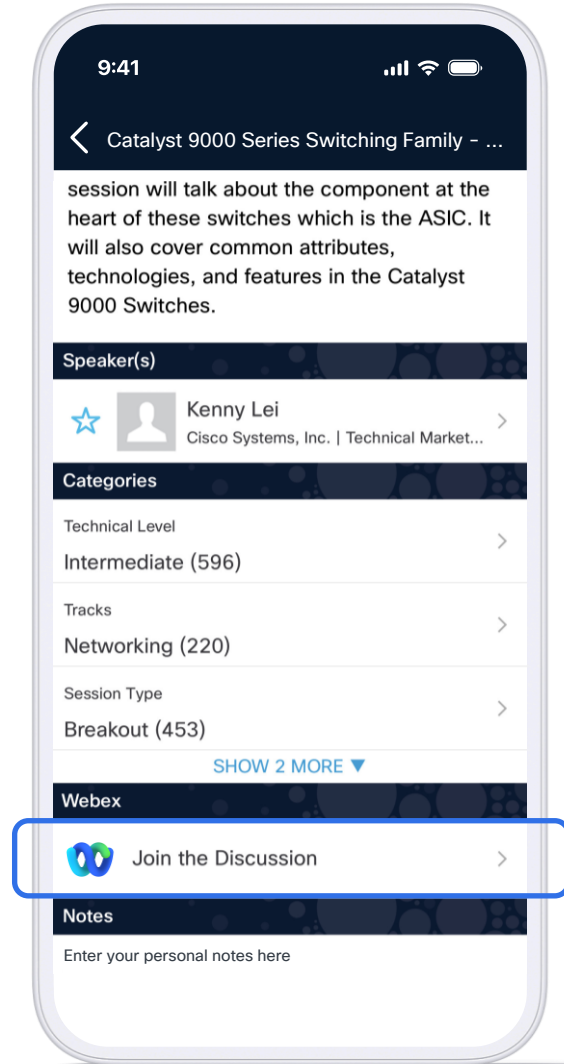
Questions?

Use Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Events 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 February 27, 2026.



Habit



... any regularly repeated behaviour that requires little or no thought and is learned rather than innate.

Agenda

Habit #1

Deploy at scale with Campus Automation

Habit #2

Stay Compliant by Design

Habit #3

Keep Software Current

Habit #4

Assure with Insight

Habit #5

Transform with AIOps

Habit #6

Integrate to Innovate

Habit #7

Maintain Platform Currency for Maximum Resiliency

Habit #1

Deploy at scale with Campus Automation

Evolution of Automation

Intent

Wireless primary
Switching templates

Per Device

Day-N
Wired + Wireless

Config At Scale

Coverage/scale

Campus Automation

Simplified View and Edit of Switch Configuration

Summary View of Configurations

Actionable Switch Ports

Instant Edit and Provisioning

View/Edit of Detailed Configurations

The screenshot displays the configuration page for a Cisco Catalyst 9300 Switch. The breadcrumb trail is 'All Devices / C9K-STANDALONE-2.cirrus.cloud'. The device name is 'C9K-STANDALONE-2.cirrus.cloud', with options to 'Run Commands' and 'View 360'. Status indicators show 'Reachable' and 'Managed'. The IP address is '10.85.54.26', and the device model is 'Cisco Catalyst 9300 Switch'. The site is 'Global/Canada/Ontario/Toronto/TBRANCH-SCARBOROUGH'. The left sidebar shows a 'CONFIGURATION' menu with 'Discovery Protocols' selected. The main content area shows 'Discovery Protocols' configuration with an 'Edit' link. Under 'CDP', 'Admin Status' is 'Enabled (default)', 'Hold Time' is '180 (default)', and 'Timer' is '60 (default)'. Under 'LLDP', 'Admin Status' is 'Disabled (default)', 'Hold Time' is '120 (default)', and 'Timer' is '30 (default)'. Both sections have a 'Default Configurations' link.

Catalyst Center- Per-Device Configuration - Switches

Phase 1: Layer 2 configurations

CONFIGURATION

- Layer 2
- VLAN
- Discovery Protocols
- STP
- VTP
- DHCP Snooping
- IGMP Snooping
- MLD Snooping
- Authentication
- Cisco TrustSec
- Logical Ports
- Port Configuration

Port Configuration [Edit](#) Only Layer 2 ports are

Ports (41) Focus: **Default View**

Search Table

Port Name	Switchport Description
TenGigabitEthernet1/0/22	--
TenGigabitEthernet1/0/23	***** Uplink #1 to C3650 DISTRI **
TenGigabitEthernet1/0/24	***** Uplink #2 to C3650 DISTRI **
TenGigabitEthernet1/1/1	--

Simplified visualization

View Port [Edit](#)

Port Name [i](#) TenGigabitEthernet1/0/23

Switchport

Description [i](#) ***** Uplink #1 to C3650 DISTRI *****

Mode [i](#) Trunk

Access VLAN ID [i](#) 1 (default)

Voice VLAN ID [i](#) --

Admin Status [i](#) Enabled (default)

Allowed VLANs [i](#) 419,420

[> Default Configurations](#)

VLAN Trunking

Dot1x

Authentication Mode [i](#) Closed (default)

[Close](#)

Catalyst Center- Per-Device Configuration - Switches

Phase 1: Layer 2 configurations

Edit 2 Port

2 Selected Ports >

Switchport

Switchport Description ⓘ

Campus Automation Description

Switchport Mode ⓘ

Access ⓘ

Switchport Access VLAN ID ⓘ

420 (VLAN0420) ⓘ

Switchport Admin Status ⓘ

Enabled ⓘ

+ Add Configurations

Configuration to be Deployed ⓘ

10 Line(s)

```
1 interface GigabitEthernet1/1/2
2   description Campus Automation Description
3   switchport access vlan 420
4   switchport mode access
5   exit
6 interface GigabitEthernet1/1/3
7   description Campus Automation Description
8   switchport access vlan 420
9   switchport mode access
10  exit
```

Simplified Configuration

Catalyst Center- Per-Device Configuration - Switches



Reference

Pre-Requisites

- Catalyst 9000 Series Switches running Cisco IOS-XE 17.3 or later
- Cisco Catalyst Center version 2.3.7.9 or later
 - L2 Configurations available
- For devices provisioned using SDA, only Config Visibility is supported

9800 WLC - Per device configuration

All Devices / ar9800.adamlab.cisco.com

ar9800.adamlab.cisco.com Manage 1 APs Run Commands View 360 Last Updated: 3 hours 12 minutes ago

Reachable Managed IP Address: 10.10.21.200 Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud Device Role: ACCESS Uptime: 185 days 11 hrs 18 mins Site: Global/SYD/north sydney

SECURITY

Advisories

FIELD NOTICES

Field Notices

Potential Field Notices

CONFIGURATION BETA

- WLAN >
- RF >
- AP Join >
- Flex Profiles
- Tags >
- Security >
- Global Radio Configurations >
- Global Wireless Configurations >
- MDNS
- EoGRE
- Layer 2 >
- Network Settings >

Hardware

Device Type	Wireless Controller	Series	Cisco Catalyst 9800 Wireless Controllers for Cloud
Platform	C9800-CL-K9	Serial Number	9MZF69DI31J
MAC Address	00:50:56:a0:66:8f	Vendor	Cisco

Software

Image	C9800-CL-universalk9.17.14.01.SPA.bin	Version	17.14.1
-------	---------------------------------------	---------	---------

Operational Summary

Uptime	185 days 11 hrs 18 mins	Provision Status	Success
Last Provisioned	Jul 16, 2024 8:38 PM	Resync Interval	24 hours
Last Synced	3 hours ago	Cisco ISE Integration Status	Not Applicable

Private Beta: 2.3.7.6
2.3.7.9

IOS-XE 17.12+

Management choice: Site-Based or Per-device

All Devices / ar9800.adamlab.cisco.com

ar9800.adamlab.cisco.com Manage 1 APs Run Commands View 360 Last Updated: 3 hours 12 minutes ago

Reachable Managed IP Address: 10.10.21.200 Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud Device Role: ACCESS Uptime: 185 days 11 hrs 18 mins Site: Global/SYD/north sydney

WLAN Profiles ⓘ

Managed via Site-Based Network Profiles ⓘ

This device is managed using site-based Network Profiles. All configurations are in **read-only** mode. Changes can only be made via the Network Profile.

WLAN Profiles (2)

Search for WLAN Profile Name or SSID Name

0 Selected

<input type="checkbox"/>	WLAN Profile Name	Status	WLAN ID	SSID Name	Policy Tags	AP Configuration Sets
<input type="checkbox"/>	new_profile	✓	18	new	6	0
<input type="checkbox"/>	test_profile	✓	17	test	3	1

2 Record(s) Show Records: 25 1 - 2 < 1 >

2.3.7.9 – Convert to per-device mode

The screenshot shows the Catalyst Center interface for device **pnp-9800**. A red box highlights the **Enable Per-Device Configuration** button. The interface is divided into sections: **DETAILS** (Interfaces, System, Browse Configurations, User Defined Fields, Wireless Info), **SECURITY** (Advisories), and **FIELD NOTICES** (Field Notices, Potential Field Notices). The main content area shows hardware details (Device Type: Wireless Controller, Platform: C9800-CL-K9, MAC Address: 00:1e:e5:a7:bf:ff), software details (Image: C9800-CL-universalk9.17.12.03.SPA.bin, Version: 17.12.3), and an operational summary (Uptime: 63 days 5 hrs 30 mins, Provision Status: Success with a warning icon, Resync Interval: 24 hours, Cisco ISE Integration Status: Success with a checkmark icon).

Device Mode	Per Device Config Support
Intent Mode config	read only
Greenfield	read-write
Assurance only	read-write

Per-Device configuration mode

All Devices / ar9800.adamlab.cisco.com

ar9800.adamlab.cisco.com Manage 1 APs Run commands View 360 Last Updated: 3 hours 11 minutes ago

Reachable | Managed | IP Address: 10.10.21.200 | Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud | Device Role: ACCESS | Uptime: 27 days 27 mins | Site: Global/Sydney/RoseBay

DETAILS

- Interfaces >
- System >
- Browse Configurations >
- User Defined Fields
- Wireless Info

CONFIGURATION

- WLAN ▼
 - WLAN Profiles
 - Policy Profiles
 - Remote LAN Profiles
 - Remote LAN Policies
 - 802.11be Profiles

WLAN Profiles ⓘ

Per-device configuration ⓘ ⚠

WLAN Profiles (3)

Search for WLAN Profile Name or SSID Name

0 Selected Actions ▼

<input type="checkbox"/>	WLAN Profile Name	Status	WLAN ID	SSID Name	Policy Tags	AP Configuration Sets
<input type="checkbox"/>	new_profile	✓	18	new	6	0
<input type="checkbox"/>	test_profile	✓	17	test	3	1
<input type="checkbox"/>	sss_profile	✗	1	sss	0	0

3 Record(s) Show Records: 25 ▼ 1 - 3 < 1 >

Any configurations made outside Catalyst Center (e.g., via CLI or WebUI) will be detected and imported at the next inventory sync, which may cause conflicts. To ensure consistency and predictable outcomes, it's recommended always use Catalyst Center for all supported configurations.

Features supported



Reference

WLAN

- WLAN Profiles
- Policy Profiles
- Remote LAN Profiles
- Remote LAN Policies
- 802.11be Profiles

RF

- RF Profiles
- Radio Antenna Profiles
- Multi BSSID Profiles

AP Join

- AP Join Profiles
- AP Priming
- Mesh
- Power Profiles
- Calendar Profile

Flex Profiles

Tags

- Site Tags
- Policy Tags
- RF Tags
- Tag Mapping

Security

- AAA
- AAA Policy
- ACL
- EAP
- URL Filters
- Guest User
- Web Auth
- Trustsec
- Local Policy
- Wireless Protection Policies

Global Radio Configurations

- CleanAir
- High Throughput
- Media Parameters
- Network Parameters
- Global Parameters
- RRM

Global Wireless Configurations

- Airtime Fairness
 - Guest LAN
 - Media Stream
 - Advanced
 - Multicast
 - Location
 - Excluded Clients
 - QoS
 - Application Visibility
 - ~~Mobility**~~
 - Country
- mDNS
- EoGRE
- ### Layer 2
- VLAN
 - Interfaces
 - Discovery Protocols

Network Settings

- DHCP Pools
- HTTP/HTTPS
- SNMP
- NTP

Layer 3

- Routing

Administration

- Device
- User Administration
- DNS

~~Mobility**~~

in 2.3.7.9

New in 3.1.3

** removed in 3.1.5

Mobility is now part of inventory configuration (not per-device)

The screenshot shows the Cisco Inventory Management interface. At the top, there are tabs for 'All', 'Routers', 'Switches', 'Wireless Controllers', 'Access Points', and 'Sensors'. Below this, the 'Devices (4)' section is active, with a focus on 'Software Images'. A search bar is present with the text 'Click here to apply basic or advanced filters or view recently applied filters'. The main table displays a list of devices with columns for 'Tags', 'Device Name', 'IP Address', 'Reachability', and 'Image Version'. The device 'ar9800.adamlab.cisco.com' is selected, and the 'Actions' menu is open over it. The 'Provision' option is highlighted, and a sub-menu is visible with 'Configure WLC Mobility' selected. Other options in the sub-menu include 'Assign Device to Site', 'Provision Device', 'Configure WLC HA', 'Manage LED Flash Status', and 'Factory Reset'.

Tags	Device Name	IP Address	Reachability	Image Version
<input type="checkbox"/>	9k-tor-app-temp.adamlab.cisco.com	10.10.10.10		17.18.1
<input type="checkbox"/>	APF4BD.9E9A.F1EC	10.10.10.10		17.15.3.28
<input checked="" type="checkbox"/>	ar9800.adamlab.cisco.com	10.10.10.10		17.15.3
<input type="checkbox"/>	perth-9k-edge	10.10.10.10		17.15.3

A Policy Profile contains a lot of attributes

Edit Policy Profile: adam

Search

General

Access Policies

QoS and AVC

Mobility

Advanced

WLAN Timeout

WLAN Flex Policy

AAA Policy

DHCP

DNS Layer Security

Miscellaneous

General

Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Configure WLAN switching policy , status and related configs

Policy Profile Name
adam

Description
Length: 0 to 64

Status *i*

IP MAC Binding *i*

Passive Client *i*

Encrypted Traffic Analytics *i*

WLAN Switching Policy

Central Switching *i*

Central DHCP *i*

Central Authentication *i*

Flex NAT/PAT *i*

Example: Turn off 2.4GHz

The image displays three overlapping screenshots of the Cisco WLAN configuration interface, illustrating the process of turning off the 2.4 GHz radio policy.

Top-Left Screenshot (General Tab): Shows the 'Edit WLAN Profile: test_profile' configuration page. The 'General' tab is selected. The 'Radio Policy' section shows the 2.4 GHz radio policy is currently turned **ON**. Other radio policies for 6 GHz and 5 GHz are also visible.

Middle Screenshot (Radio Policy Section): Shows the 'Radio Policy' section of the configuration page. The 2.4 GHz radio policy is now turned **OFF**, while the 6 GHz and 5 GHz policies remain turned on.

Right Screenshot (Provision Workflow): Shows the 'Provision' workflow for the configuration. The 'Preview and Deploy (Recommended)' option is selected, indicating the configuration is ready to be deployed to the network.

Now in VCR mode

Edit WLAN Profile: test_profile / Provision

Provision

Learn how the Visibility and Control of Configurations feature helps optimize your workflow.

This workflow supports enforcing network administrators and other users to preview configurations before deploying them on the network devices. To configure this setting, go to System → Settings → Visibility and Control of Configurations.

Warning

You are provisioning changes using the Per-Device Configuration. This feature is currently in **Beta** with no official Cisco technical support. Contact [Cisco](#) for more details.

Cancel **Ok**

Cancel **Apply**

Edit WLAN Profile: test_profile-04_Dec_2024_12_48_AM As of: 12:51:58 AM

Step 1 of 3: Performing Initial Checks

Cisco Catalyst Center is now performing early validations to ensure a seamless provisioning operation.

- ✓ Pending Operations ⓘ
Success. No pending operations conflicting with the current operation found.
- ✓ Device Level Validations ⓘ
Success. No issues were found on a preliminary check of the devices involved in this operation. More checks will be performed as the workflow progresses. Currently, these preliminary checks are performed only on Switches and Routers. Wireless controllers, Access Points and other devices are not included.

Exit Recheck Back **Next**

Visibility

Edit WLAN Profile: test_profile-04_Dec_2024_12_48_AM

As of: 12:52:58 AM [Refresh](#)

Step 3 of 3: Preview Configuration

Review the device configuration provided below by clicking on each device. When you are done reviewing, click Deploy. Click [Exit and Preview Later](#) to defer the review. The deferred review can be found in the [Tasks](#) menu.

Status: ✔ Ready

Search by device name

Device IP: 10.10.21.200 Site: Global/Syd [ⓘ](#)

ar9800.adamlab.cisco.com ✔

Configuration to be Deployed

View by Configuration Source · All ⌵

YANG - All

17 Line(s)

```
1 <wlan-cfg-data xmlns= "http://cisco.com/ns/yang/Cisco-IOS-XE-w
2 <wlan-cfg-entries >
3 <wlan-cfg-entry >
4 <profile-name>
5 <![CDATA[test_profile]]>
6 </profile-name>
7 <wlan-radio-policies >
8 <wlan-radio-policy >
9 <band>dot11-5-ghz-band</band>
10 <slot0>true</slot0>
11 <slot1>true</slot1>
12 <slot2>true</slot2>
13 </wlan-radio-policy>
14 </wlan-radio-policies>
15 </wlan-cfg-entry>
16 </wlan-cfg-entries>
17 </wlan-cfg-data>
```

[ⓘ](#) Generation Status Legend

Device IP: 10.10.21.200 Site: Global/Sydney/RoseBay [ⓘ](#)

Configuration to be Deployed

View by Source · All ⌵

Search configuration

GENERATED CLI - ALL

1 Line(s)

Below is the "CLI preview" of the effective configuration change on the device after applying the YANG configuration payload. This CLI configuration should not be applied directly by logging onto the device.

```
1 no radio policy dot11 24ghz
```

[Exit and Preview Later](#)

[Discard](#)

[Deploy](#)

Convert yang to CLI – human readable

Provisioning Task

Edit WLAN Profile: test_profile-04_Dec_2024_12_48_AM

Task · PROVISION

Active · In Progress

Start: Dec 4, 2024 12:53 AM

As of: 12:53:49 AM [Refresh](#)

TASK PROGRESS



i This task was created to deploy configuration that was previously previewed as a work item. [View Work Item Details](#)

Hostname ar9800.adamlab.cisco.com

IP Address 10.10.21.200

Status **Success**

▼ Payload

```
{ "featureName": "WlanConfigProfileGen_Configuration", "featureInstances": [{"@operator": "UPDATE", "connectedModelGraph": {"wlanDot11BeProfileName": "", "wlanRadioPolicyGen": [{"java.util.HashSet", [{"@class": "com.cisco.dnac.wireless.model.WlanCfg.WlanRadioPolicyGen", "wlanRadioPolicySlot0": true, "wlanRadioPolicyBand": "DOT11_5_GHZ_BAND", "cd7c-42ca-961c-6be2f358a5f2", "wlanProfileName": "test_profile", "wlanRadioPolicySlot2": true, "wlanRadioPolicySlot1": true}]]}, {"wlanWpa2Aes": true, "@class": "com.cisco.8d33-4009-9df3-5030d5c33530", "wlanProfileName": "test_profile"}]}}
```

Success

Edit WLAN Profile: test_profile-04_Dec_2024_12_48_AM



Task · PROVISION

Completed · Success

Start: Dec 4, 2024 12:53 AM End: Dec 4, 2024 12:53 AM

As of: 12:54:30 AM Refresh

TASK PROGRESS



1	1	0	0	0	0
Total	Success	Failed	Stopped	In Progress	Not Started

This task was created to deploy configuration that was previously previewed as a work item. [View Work Item Details](#)

Hostname ar9800.adamlab.cisco.com

IP Address 10.10.21.200

Status Success

> Payload

Updating/Adding Telemetry

Update Telemetry Settings Task

As of: 3:48:56 PM [Refresh](#)

Step 3 of 3: Preview Configuration

Review the device configuration provided below by clicking on each device. When you are done reviewing, click Deploy. Click [Exit and Preview Later](#) to defer the review. The deferred review can be found in the [Tasks](#) menu.

Status: ● Ready

Search by device name

ar9800.adamlab.cisco.com ●

```
3 snmp-server source-interface traps GigabitEthernet1
4 no crypto pki trustpoint DNAC-CA
5 crypto key ***** rsa DNAC-CA
6 ip http client source-interface GigabitEthernet1
7 ip ssh source-interface GigabitEthernet1
8 ip ssh version 2
9 ip domain lookup
10 crypto pki trustpoint DNAC-CA
11 source interface GigabitEthernet1
12 enrollment mode ra
13 enrollment terminal
14 usage ssl-client
15 revocation-check crl none
16 exit
17 crypto pki authenticate DNAC-CA
18 -----BEGIN CERTIFICATE-----
19 -----END CERTIFICATE-----
```

Generated CLI - All

8 Line(s)

Below is the "CLI preview" of the effective configuration change on the device after applying the YANG configuration payload. This CLI configuration should not be applied directly by logging onto the device.

```
1 crypto pki trustpoint sdn-network-infra-iwan
2 enrollment url http://10.10.21.124:80/ejbca/publicweb/apply/scep/sdnccep-PREVIEW
3 fqdn PREVIEW_FQDN.com
4 no revocation-check crl
5 no rsakeypair sdn-network-infra-iwan
6 subject-name CN=PREVIEW_sdn-network-infra-iwan
7 no subject-alt-name ar9800.adamlab.cisco.com
8 !
```

Is this feature helpful?

[Exit and Preview Later](#)

[Discard](#)

[Deploy](#)

This does not change from intent or assurance only.

Not part of the per device configuration

2.3.7.10 / 3.1.3 – clone profile from another device

All Devices / ar9800.adamlab.cisco.com

ar9800.adamlab.cisco.com Manage 1 APs Run commands View 360 Last Updated: 31 minutes ago

Reachable Managed IP Address: 10.10.21.200 Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud Device Role: ACCESS
Uptime: 153 days 2 hrs 54 mins Site: Global/Sydney/RoseBay

Search Features

DETAILS

- Interfaces >
- System >
- Browse Configurations >

User Defined Fields

Wireless Info

CONFIGURATION

- WLAN >
- WLAN Profiles
- Policy Profiles
- Remote LAN Profiles
- Remote LAN Policies

WLAN Profiles [?]

Per-device configuration [?]

✔ Create WLAN Profile-30_Sep_2025_02_38_PM is completed successfully. [View Task Details](#)

WLAN Profiles (3) [Add](#) [Clone from another WLC](#)

Search for WLAN Profile Name or SSID Name

0 Selected [Actions](#) ▾

<input type="checkbox"/>	WLAN Profile Name	Status	WLAN ID	SSID Name	Policy Tags	AP Configuration Sets
<input type="checkbox"/>	new_profile	✔	18	new	6	0
<input type="checkbox"/>	test_profile	✔	17	test	3	1

What about the AP?

The screenshot displays the Cisco Meraki dashboard for a specific device (ar9800.adamlab.cisco.com). The top navigation bar includes 'Manage 1 APs', 'Run commands', and 'View 360'. A status bar shows 'Reachable', 'Managed', IP Address: 10.10.21.200, Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud, Device Role: ACCESS, and Uptime: 34 days 19 hrs 52 mins. The left sidebar contains navigation options like 'Hardware', 'Device Type', 'Platform', 'MAC Address', 'Software', and 'Image'. The main content area is titled 'Access Points' and features an informational message: 'This Operational Access Points tab displays the state of the network only after the controller has been resynced. To configure other AP and Radio Parameters, launch the **Configure Access Points workflow**'. Below this is a table of 'Operational Access Points (1)' with columns for AP Name, IP Address, AP Ethernet MAC Address, Connection Status, Policy Tag, and Site Tag. A single AP is listed with MAC address f4:bd:9e:9a:f1:ec and status 'Reachable'. A modal window titled 'Edit AP Configuration Set' is open on the right, showing fields for AP Ethernet MAC Address, Policy Tag (PT_SYD_north_F1_407e5), Site Tag (ST_SYD_northsyd_576e4_0), and RF Tag (test).

AP Name	IP Address	AP Ethernet MAC Address	Connection Status	Policy Tag	Site Tag
APF4BD.9E9A.F1EC	10.10.33.2	f4:bd:9e:9a:f1:ec	Reachable	PT_SYD_north_F1_407e5	ST_SYD_northsyd_576e4_0

Operational Access Points (1)

0 Selected [Edit AP Configuration Set](#) [Assign AP to Site](#) As of: Nov 11, 2025

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

Edit AP Configuration Set

AP Ethernet MAC Address: f4:bd:9e:9a:f1:ec

Policy Tag*: PT_SYD_north_F1_407e5

Site Tag*: ST_SYD_northsyd_576e4_0

RF Tag*: test

- Manage AP tags @ scale
- Bulk edit tags
- Use AP existing config workflows for other configuration
- Remember resync is important after any config push (it happens automatically – not instant)

Summary

Introduced in
CatC 2.3.7.9

Why Catalyst Center?

- ✓ Supports both **Brownfield** & **Greenfield** deployments
- ✓ C9800-like **intuitive UI** experience
- ✓ **Smart search**: find favorite “config” by name, description, or common terms – even with typo
- ✓ **95% config parity** with Cisco Prime (for C9800 WLC)
- ✓ Config Cloning introduced in 2.3.7.10

CatC Platform offered capabilities

- ✓ **Visibility & Control**: change management with CLI preview
- ✓ **Config drift** detection: track what changed and when
- ✓ **Audit trail**: see who made changes and when
- ✓ **Assurance**: Visibility, Observability and Insights

© 2026 Cisco and/or its affiliates. All rights reserved.

* In ideal conditions, subject to change.

How?

When 'Per-Device Configuration' is enabled, no configuration is pushed.

Catalyst Center only learns the device's existing configuration.

The image shows three screenshots of the Catalyst Center interface illustrating the steps to enable per-device configuration:

- Step 1: Inventory > View Device Details**: A screenshot of the 'Devices (4)' list in the 'Inventory' view. A device named 'C9800-IDT-13' is selected, and the 'View Device Details' option is highlighted in the context menu.
- Step 2: "Enable Per-Device Configuration"**: A screenshot of the 'View Device Details' page for 'C9800-IDT-13'. The 'Enable Per-Device Configuration' toggle is shown in the 'Operational Summary' section.
- Step 3: Resync WLC**: A screenshot of the 'WLAN Profiles' page. A warning message is displayed: "After enabling per-device configuration, ensure that the device is resynchronized before performing any operations. You can manually resync the device from the inventory." Below the message, the 'WLAN Profiles (0)' table is shown with a 'No data to display' message.

* Capabilities mentioned are supported for Wired Infrastructure as well

BRKOPS-2416



What is next?

Per Device

Day-N

Wired + Wireless



**Config At
Scale**

Coverage/scale

3.1.5 Networks, and Device Groups - Beta

NOTE: Today this is switching only

Networks [Learn more](#)

Overview Unassigned devices 0

Q Search 1 results [Export](#) [+ Create Network](#)

Network name	Device groups	Devices
Network 1	2	3

← All networks **Network 1** [Learn more](#) [Action](#)

Device groups 2 **Devices** 3

Q Search 2 results [Export](#) [+ Create Device group](#)

Device group name	Type	Devices
Device group 1	wired	2
Device group 2	wireless	1

All networks > Network 1 **Device group 1** [Learn more](#) Wired device group

Devices

Q Search 2 results [Export](#) [Compare configuration](#) [+ Assign devices](#)

Device name	IP address	Manageability	Platform	Uptime	Site
<input type="checkbox"/> 9k-tor-app-temp.adamlab.cisco.com	10.10.15.102	Managed	C9300-48U	7 days, 23:19:40.29	Global/S
<input type="checkbox"/> perth-9k-edge	10.10.9.4	Managed	C9300-48U	111 days, 20:26:16.00	Global/S

- Networks are a logical grouping containing device groups
- Device groups are group of devices that have similar configuration
- Group profiles are configurations required in device groups
- Report on devices that don't have the configurations within the profile (config push in the future)

3.1.5 Compare to profile – no provisioning (yet)

The screenshot displays the Cisco DNA Center interface. A 'Compare configuration' dialog box is open, showing the following details:

- Compare configuration**
- All devices selected.
- Compare the configurations of devices in a device group against a group profile.
- Select profile type: Layer 2
- Select profile: adam
- Buttons: Cancel, Compare

The background shows a table of devices with columns for IP address, Platform, Device Role, Uptime, Site, and Network. A detailed view of a device is also shown:

9k-tor-app-temp.adamlab.cisco.com Managed
Compared with adam on Sep 30, 2025 03:47 PM

IP address	Platform	Device Role	Uptime	Site	Network
10.10.15.102	Cisco Catalyst 9300 Switch	ACCESS	7 days, 23 hrs	Global/Sydney/RoseBay	Network 1

Layer 2

- VLAN ✖
- Discovery Protocols
- STP ✖
- VTP
- DHCP Snooping
- IGMP Snooping
- MLD Snooping
- UDLD
- Authentication

VLAN

VLANs (10) Focus: Default View Export

VLAN ID	VLAN Name	Admin Status
15 Missing in profile	VLAN0015	Enabled
20 Missing in profile	VLAN0020	Enabled
80 Missing in profile	VLAN0080	Enabled
99 Missing in device	--	--



Habit #2

Stay Compliant by Design

Cisco Catalyst Center Compliance Landscape

Configuration Compliance



Identify whether the startup and running configurations of a device are in sync.

Violation of intent provisioned to a device through Catalyst Center

Difference in network settings compared to "Network Settings" in Design

Violation of application visibility intent provisioned to a device through CBAR and NBAR

Compliance Summary

Run Compliance Check

Check Name	Status	Open Violations	Additional Info
Network Settings	Non-Compliant	2	General: 2
EoX - End of Life	Compliant	0	Module: Compliant, Software: Compliant, Hardware: Compliant
Startup vs Running Configuration	Compliant	0	36 days since in sync, Lines added: 0, Lines removed: 0, Lines modified: 0
Network Profiles	Non-Compliant	2	CLI Template: 2
Application Visibility	Compliant	0	
Software Image	Compliant	0	Golden Image Version: 17.09.02, Running Version: 17.9.2, Stack Member Status: Up to Date
Critical Security Advisories	Compliant	0	

Cisco Catalyst Center Compliance Landscape

Configuration Compliance

Violation of intent provisioned to a device through Catalyst Center

Note: Currently available for Intent Based Automation only

Compliance Summary

No events detected to trigger compliance check [Run Compliance Check](#)

Category	Item	Status	Open Violations
Network Settings	Network Settings	Non-Compliant since Dec 13th, 2022, 09:33:23 AM	2
	General	Compliance last run on: Dec 13th, 2022, 09:33:23 AM	2
EoX - End of Life	EoX - End of Life	Compliance last run on: Dec 13th, 2022, 09:33:23 AM	0
	Module	Compliant	0
	Software	Compliant	0
Startup vs Running Configuration	Startup vs Running Configuration	Compliance last run on: Dec 13th, 2022, 09:33:22 AM	0
	36 days since in sync	Lines added: 0	0
		Lines removed: 0	0
Network Profiles	Network Profiles	Non-Compliant since Oct 14th, 2022, 01:23:01 PM	2
	CLI Template	Compliance last run on: Dec 13th, 2022, 09:33:23 AM	2
Application Visibility	Application Visibility	Compliant since Dec 13th, 2022, 09:33:40 AM	0
		Compliance last run on: Dec 13th, 2022, 09:33:40 AM	0
Software Image	Software Image	Compliant since Nov 17th, 2022, 12:35:00 PM	0
	17.09.02	Running Version: 17.9.2	0
Critical Security Advisories	Critical Security Advisories	Compliant since Oct 14th, 2022, 11:38:16 AM	0
		Compliance last run on: Dec 13th, 2022, 09:33:22 AM	0

Cisco Catalyst Center Compliance Landscape

Non-Configuration Compliance



End of Sale & End of Life alerts

Check whether the devices are running without critical security vulnerabilities.

See if the tagged golden / standard image is running on the device.

Compliance Summary

No events detected to trigger compliance check [Run Compliance Check](#)

Category	Item	Status	Details
Network Settings	Network Settings	Non-Compliant	2 Open Violations (General: 2)
	EoX - End of Life	Compliant	Module: Compliant, Software: Compliant, Hardware: Compliant
	Startup vs Running Configuration	Compliant	36 days since in sync, Lines added: 0, Lines removed: 0, Lines modified: 0
	Network Profiles	Non-Compliant	2 Open Violations (CLI Template: 2)
Application Visibility	Application Visibility	Compliant	0 Open Violations
	Software Image	Compliant	17.09.02 Golden Image Version, Running Version: 17.9.2, Stack Member Status: Up to Date
	Critical Security Advisories	Compliant	0 Open Violations

Config Drift



Ethernet Ports

VLANs

Hardware & Software

Configuration

Power

Fans

SFP Modules

User Defined Fields

Config Drift

REP Rings

Stack

SECURITY

Advisories

COMPLIANCE

Summary

Configuration Changes

Configuration changes on your device will be saved on the internal Cisco DNA Center server. The number of configuration drifts saved (as set in System > Settings > Device Settings > Configuration Archive) will include labelled configs and config drift versions.

Total config drifts being saved: 15 Total labelled configs: 1

Change History (Running Config)

Config Drift Date Range: Start Date: Sep 30, 2022 End Date: Oct 15, 2022

● In-band Config Drift ● Out-of-band Config Drift ● Labelled Config

Config Drift Version: CCA_C9K-TBRANCH-Std-Config Remove Label

Config Drift Version: October 14, 2022 11:48 AM

Running Config (461 Lines)

```
17 switch 1 provision c9300-24p
18 switch 2 provision c9300-24p
19 ip routing
20 ip name-server 64.102.6.247 173.37.137.85
21 ip domain lookup source-interface Loopback0
22 login on-success log
23 vtp mode transparent
```

Running Config (784 Lines)

```
17 switch 1 provision c9300-24p
18 switch 2 provision c9300-24p
19 ip routing
20 ip nbar http-services
21 ip name-server 64.102.6.247 173.37.137.85
22 ip domain lookup source-interface Loopback0
23 login on-success log
24 vtp mode transparent
25 avc sd-service
26 segment AppRecognition
27 controller
28 address 10.85.54.177
29 destination-ports sensor-exporter 21730
30 dscp 16
```

Out-of-band Config Drift

Config version with changes made outside of Cisco DNA Center since it's previous version.

Lines Added: 322
Lines Removed: 0
Lines Modified: 0
Triggered By: Config Change Event

Terminal Name: vty2
Login IP: 10.24.150.225
Username: lila
Config Method: console

October 14, 2022 11:48 AM

New in 3.1 Rule Based Compliance

- Custom rules and policies to detect any violations
- Can use string comparisons, regular expressions, and expression evaluations
- Applied to configs, show commands, and device properties
- Each rule can have variables, multiple conditions, and configurable violation messages and severity level

The screenshot displays the configuration interface for a rule. It is divided into two main sections: 'Condition' and 'Action'.

Condition Section:

- Scope:** Device command outputs
- Show command * (i):** show install summary
- Parse as blocks (i)
- Operator (i):** Contains the string
- Value * (i):** CSCwn27950

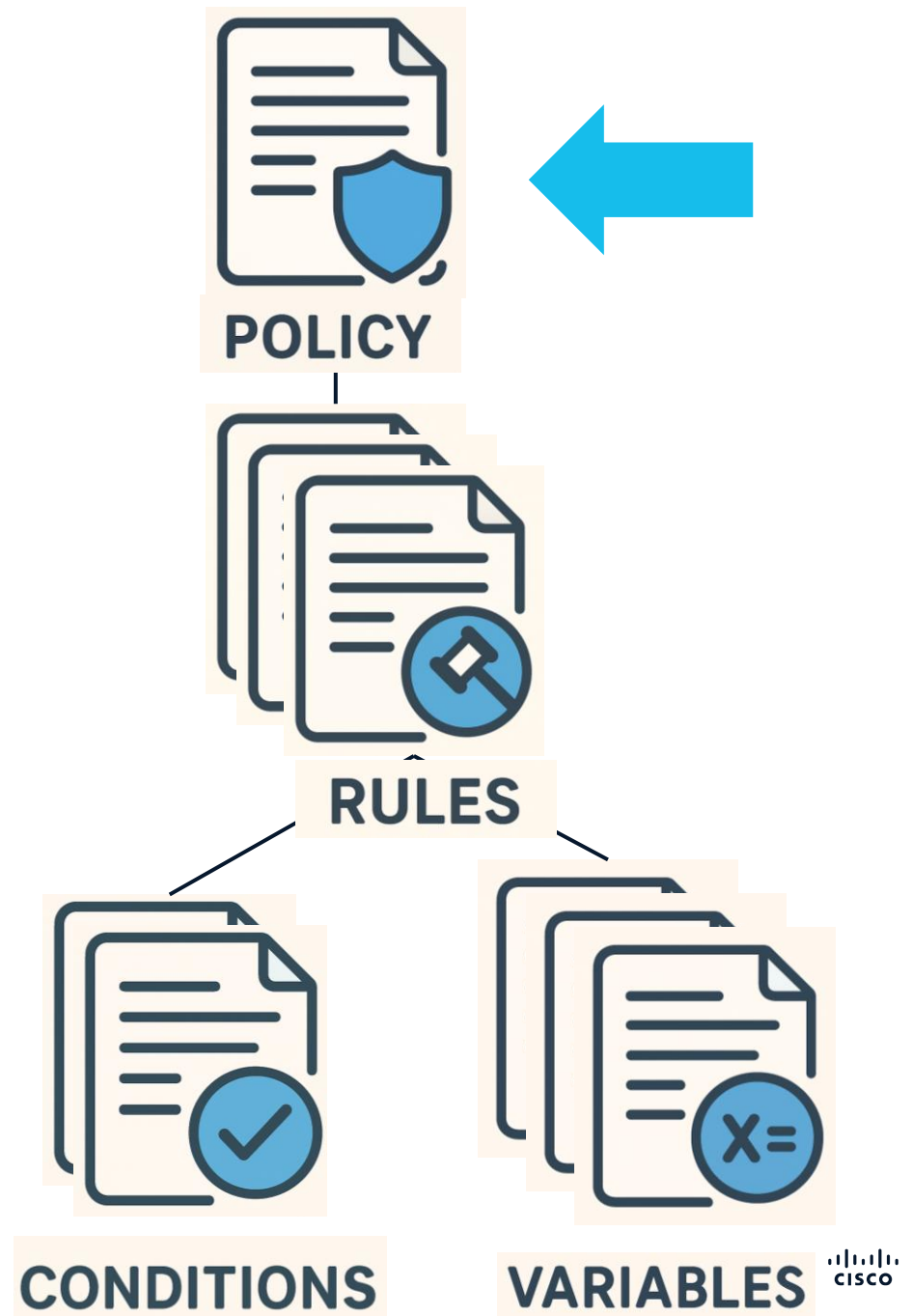
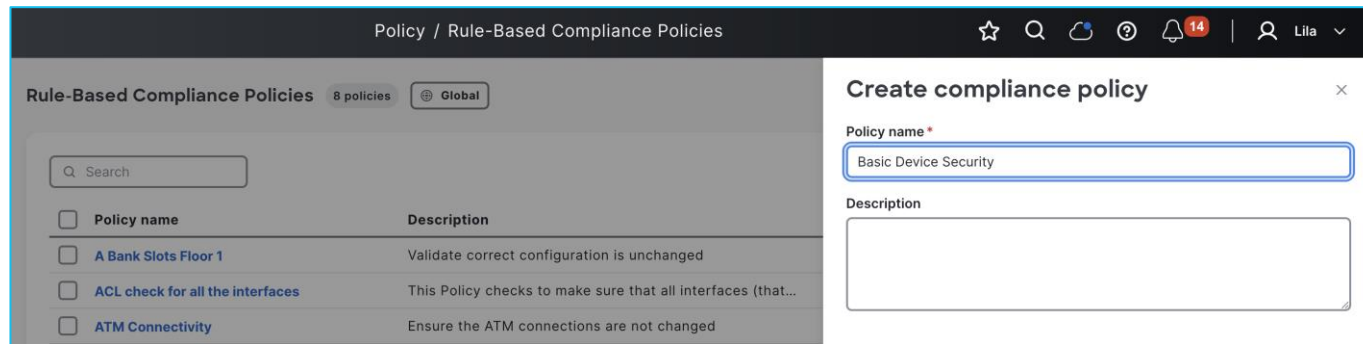
Action Section:

- Match:** Selected radio button.
- Action:** Do not raise a violation
- Does not match:** Unselected radio button.
- Action:** Raise a violation
- Violation severity:** Minor (with warning icon)
- Custom violation message (optional) (i):** The device may reload unexpectedly because the required fixed SMU is not activated.

New in 3.1 - Rule Based Compliance Policy

A policy is a logical grouping of rules

A policy is applied by assigning it to one or more sites, including Global.



New in 3.1 - Rule Based Compliance Policy

The policy is inherited by all the children of the policy root sites.

There is no overriding of policies at a child site

More than one policy can be assigned

- Global
 - APAC
 - APJC
 - Canada
 - Alberta
 - British Columbia
 - Ontario
 - Baden
 - Toronto
 - BRANCH-AAA
 - RoLlo-Home
 - TBRANCH
 - TBRANCH-NORTH-YC
 - TBRANCH-SCARBORC
 - TRN6
 - vBRANCH-ENFV
 - Quebec
 - Saskatchewan

Policy 1

Policy 2

New in 3.1 - Rule Based Compliance Rule

Rules contain platform-specific sequence of checks that constitutes configuration violations.

Create rule

Rule name *
Posture Check for SNMP

Description

▼ Add impact and suggested fix

Impact ⓘ

Suggested fix ⓘ

Software type *
IOS-XE

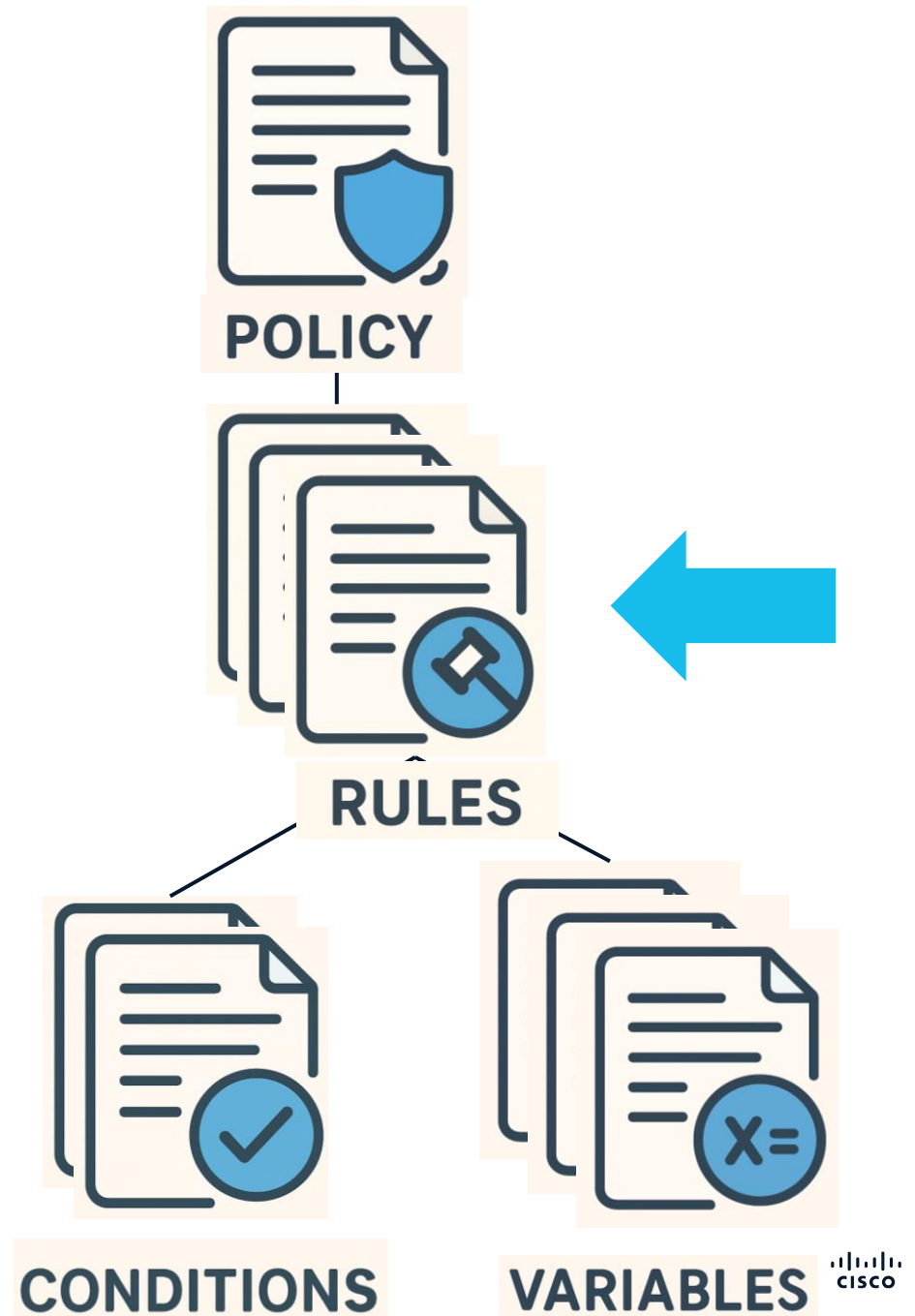
Device family *
3 Selected

Search

Device series

Rockwell Stratix 5800 Series Switches

- Routers ✓
- Switches and Hubs ✓
- Wireless Controller ✓



New in 3.1 - Rule Based Compliance Conditions

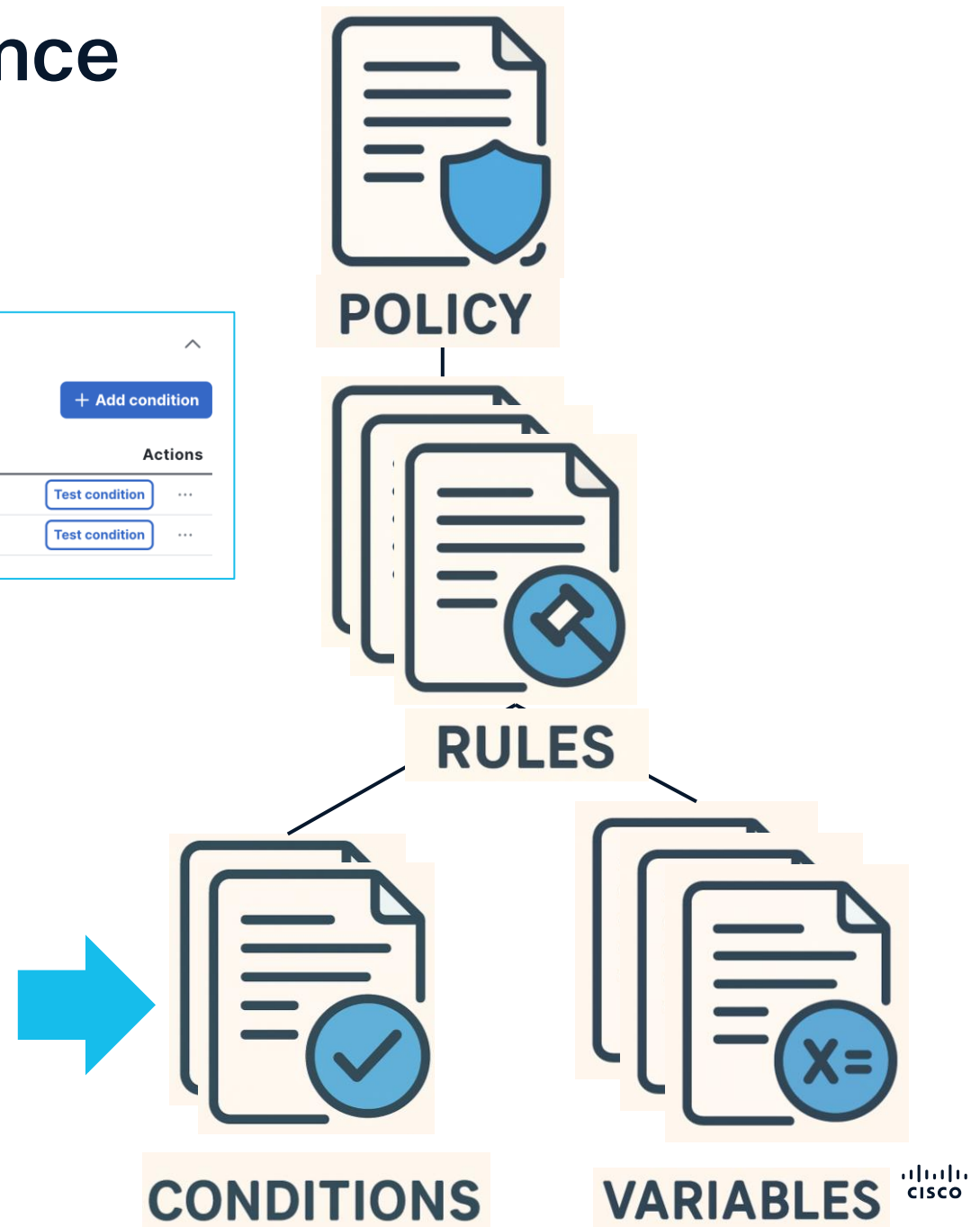
Conditions 2

Search

+ Add condition

#	Condition scope	MATCH action	DOES NOT MATCH action	Actions
1	Configuration must match the expression 'snmp-server community (publi...	Raise a violation	Continue	Test condition ...
2	Configuration must match the expression "snmp-server enable traps.*"	Do not raise a violation	Raise a violation and continue	Test condition ...

- Define the specific checks
- Executed sequentially as defined by the user. There is no priority for conditions.
- Conditions can be chained together for complex use-cases.
- Contain three major sections: Scope (Source for the check), Operator (Validation to be performed), and Actions.

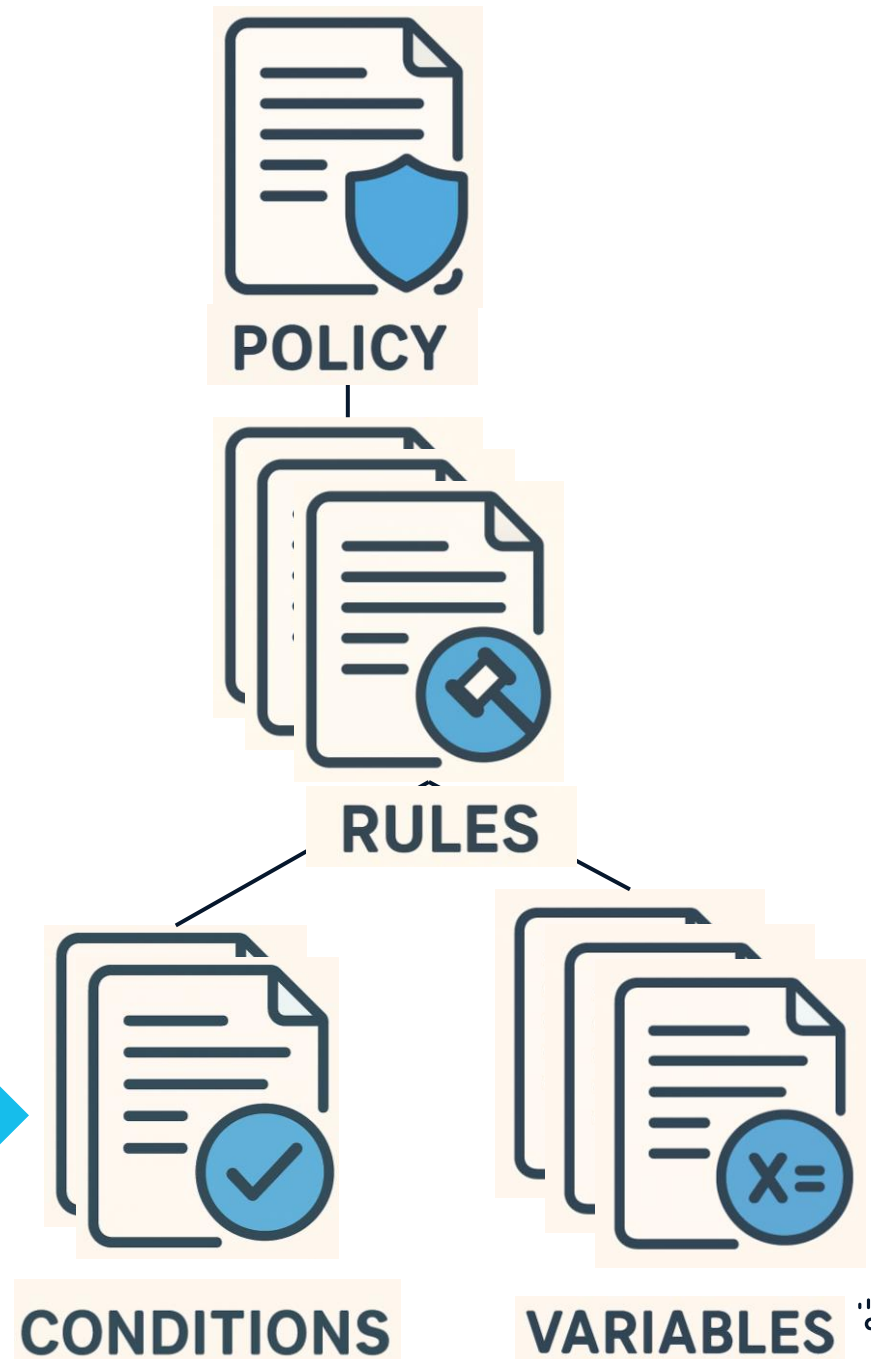
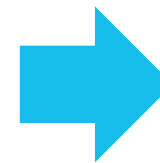


New in 3.1 - Rule Based Compliance

Conditions: Scope, Operators and Actions

The image shows a configuration dialog titled "Add condition" with a close button (X) in the top right. It features a search bar for "Sample conditions (optional)" and a toggle for "Advanced settings". The dialog is divided into sections for "Condition", "Scope", "Operator", and "Action".

- Condition:** A dropdown menu with "Sample conditions (optional)" selected.
- Scope:** A dropdown menu with "Configuration" selected. Below it, a list of options includes "Configuration" and "Device command outputs".
- Operator:** A dropdown menu with "Contains the string" selected. Below it, a list of operators includes "Contains the string", "Does not contain the string", "Matches the expression", "Does not match the expression", and "Evaluate expression".
- Action:** A dropdown menu with "A" selected.



New in 3.1 - Rule Based Compliance

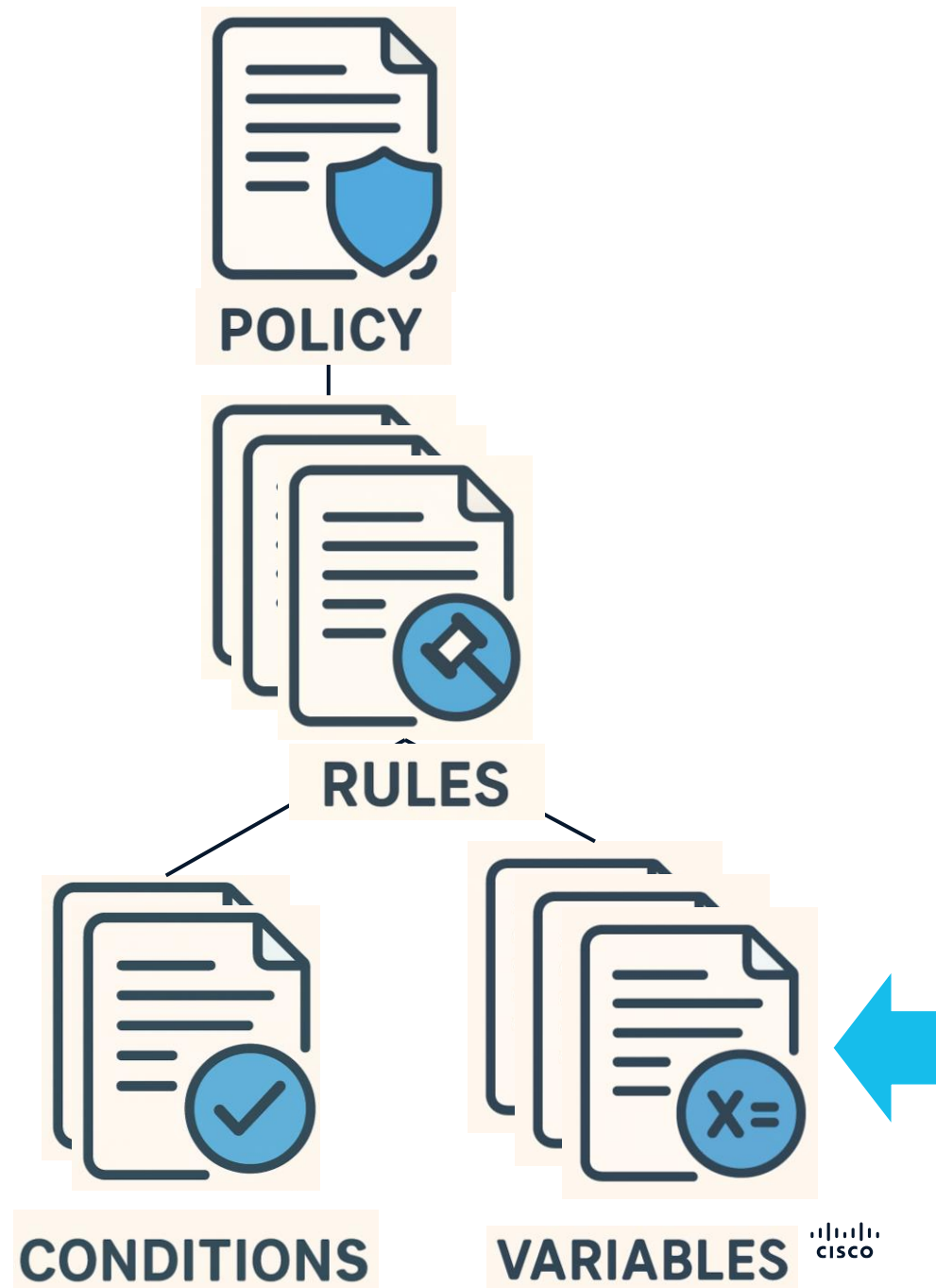
Variables

- Variables allow the customization of policies and rules across multiple sites.
- Variables are instantiated when assigning the policy to a site
- Variables values are inherited by the child sites but can be overridden

The screenshot displays the configuration for a rule-based compliance policy named 'SMU_EXISTANCE'. The policy description is: 'Raise a compliance if the device running with 117.10.01 doesn't have a CSCww23355 related SMU'. The 'Device type' is set to 'SMU_EXISTANCE'. Under the 'Variables' section, there is one variable defined:

Variable name	Identifier	Data type
smuDefectId	_smuDefectId	String

The 'Edit variable' dialog is open, showing the configuration for the variable 'smuDefectId'. The 'Name' field contains 'smuDefectId', the 'Identifier' field contains '_smuDefectId', and the 'Data type' is set to 'String'. The 'Input required' checkbox is checked.



Rule-Based Compliance Scale Considerations



Reference

Category	System Limit	Individual Limits
Policies	500	
Rules	5000	One policy: Up to 20 rules
Variables	12,500 (50% of rules use variables, avg. 5 per rule)	One rule: Up to 10 variables
Conditions	25,000 (avg., 5 conditions per rule)	One rule: Up to 10 conditions

Demo:

- 1) Create a policy**
- 2) Create a rule**
- 3) Create a Basic Condition**
- 4) Testing Conditions**
- 5) Assign Policy**
- 6) Run Compliance Check**

- Design
- Policy
- Provision
- Assurance
- Workflows
- Energy Management
- Tools
- Platform
- Activities
- Reports
- System
- Explore

Welcome to Catalyst Center!

[Explore](#) [Try the new home page! ^{BETA}](#)

Info **Cisco Catalyst Center UI is changing**
As part of our vision to unify our products and deliver a consistent experience, we will be updating the UI theme of Catalyst Center. Please rest assured that the capabilities and functionalities of Catalyst Center will remain unchanged. These updates will be rolled out over the next few releases, and during this period, you may notice some minor inconsistencies in the UI. Thank you for your understanding and patience as we work to enhance your experience.

Warning Some of your license compliance requirements have not been met. [Learn more.](#)

Assurance Summary

Health ⓘ

Healthy as of Oct 3, 2025 5:23 PM

59%	--%	100%
Network Devices	Wireless Clients	Wired Clients

[View Details](#)

Critical Issues

Last 24 Hours

9	1
P1	P2

[View Details](#)

Trends and Insights

Last 30 Days

0	0
AP Performance Advisories	Trend Deviations

[View Details](#)

Network Snapshot

Sites

As of Oct 3, 2025 5:23 PM

65	DNS Servers : 2
	NTP Servers : 4

Network Devices

As of Oct 3, 2025 5:23 PM

BRKOPS-2416	Unclaimed: 1
37	Unprovisioned: 3

Application QoS Policies

As of Oct 3, 2025 5:25 PM

0	Successful Deploys: 0
	Errored Deploys: 0

Demo:

**Import of Policy
Use of Variables**

- Design >
- Policy >**
- Provision >
- Assurance >
- Workflows
- Energy Management
- Tools >
- Platform >
- Activities >
- Reports
- System >
- Explore

Rule-Based Compliance Policies 8 policies Global

Search Import policy Create policy

<input type="checkbox"/> Policy name	Description	Rules	Sites	Status	Actions
<input type="checkbox"/> A Bank Slots Floor 1	Validate correct configuration is unchanged	1	Assign	No sites assigned	...
<input type="checkbox"/> ACL check for all the interfaces	This Policy checks to make sure that all interfaces (that...	1	3	Active	...
<input type="checkbox"/> ATM Connectivity	Ensure the ATM connections are not changed	1	Assign	No sites assigned	...
<input type="checkbox"/> Basic Device Security	Devices should be configured with secure protocols	3	Assign	No sites assigned	...
<input type="checkbox"/> Basic Device Security Updated	Devices should be configured with secure protocols	3	5	Active	...
<input type="checkbox"/> Devices should be FIPS 140-2 compliant	Devices should be using secure protocols and FIPS 140...	4	Assign	No sites assigned	...
<input type="checkbox"/> Infrastructure Resilience readiness	Check for insure commands for Secure by Default	3	3	Active	...
<input type="checkbox"/> Prohibit well known SNMP community strings	Prohibit well known SNMP community strings	1	3	Active	...

Understanding a rule starts with what it can validate

The screenshot displays the Cisco Catalyst Center interface for a device named C9K-STACK-1. The top navigation bar shows 'All Devices / C9K-STACK-1' and a 'Run commands' button. The device status is 'Reachable' and 'Managed' with an IP address of 10.85.54.54. The device model is 'Cisco Catalyst 9300 Switch' and its role is 'DISTRIBUTION'. The uptime is '37 days 6 hrs 22 mins'. The site is 'Global/Canada/Ontario/Toronto/TBRANCH'. The main content area shows a 'Switch Number 1' dropdown and a grid of ports (Tw1/0/1 to Tw1/0/29). A 'Command Runner' window is open, displaying the output of the 'show install summary' command. The output shows the installed package information for the system image.

Platform: C9300-48UXM Address: 6c:dd:30:ef:26:00 Serial Number: FCW2146L0C0 Role: STANDBY Switch Number: 1

Color Code Status

Tw1/0/1 Tw1/0/3 Tw1/0/5 Tw1/0/7 Tw1/0/9 Tw1/0/11 Tw1/0/13 Tw1/0/15 Tw1/0/17 Tw1/0/19 Tw1/0/21 Tw1/0/23 Tw1/0/25 Tw1/0/27 Tw1/0/29

Tw1/0/2 Tw1/0/4 Tw1/0/6 Tw1/0/8 Tw1/0/10

Connected Error Disabled Admin Dis

```
C9K-STACK-1> show install summary
[ Switch 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
             C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St  Filename/Version
-----
IMG   C   17.15.03.0.5635
-----
Auto abort timer: inactive
-----
C9K-STACK-1>
```

© 2

CISCO

Run compliance for assigned policies in bulk

Devices (9) Focus: **Inventory** Take a tour Export

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

2 Selected Tag + Add device Edit Device Delete Device **Actions** As of: Nov 8, 2025 7:49 AM

Tags	Device Name	IP Addr	Reachability	EoX Status	Manag
<input type="checkbox"/>	C3650-ACCESS.cisco.com	10.85.	Reachable	3 alerts	<input checked="" type="checkbox"/> M
<input checked="" type="checkbox"/>	C9K-STACK-1	10.85.	Reachable	2 alerts	<input checked="" type="checkbox"/> M
<input checked="" type="checkbox"/>	C9K-STANDALONE-1.cisco.com	10.85.			<input checked="" type="checkbox"/> M
<input type="checkbox"/>	TBranch_NonFabric_AP1	10.85.54.30	NA		<input checked="" type="checkbox"/> M

- Inventory >
- Software Image >
- Provision >
- Telemetry >
- Device Replacement >
- Switch Refresh >
- Compliance >**
 - Run Compliance Check
 - Write Running Config to Startup Config
 - Check Startup Config Write Status
- More >



Habit #3

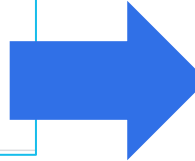
Keep Software Current

Intent Based Network Upgrades

Golden/Standard-image driven to automate process and drive consistency

cat9k_lite_iosxe.17.01.01.SPA.bin	17.01.01.0.203	0	★
Verified	Add On (N/A)		

Select Golden Image
(3.x change to standard image)



Tags	Device Name	Inventory	Reachability	EoX Status	Manage
	NA				
<input checked="" type="checkbox"/>	TBRANCH-C9300-2				Unr Device U
<input checked="" type="checkbox"/>	TBRANCH-C9200L-2.mtllab.cisco.com				
<input type="checkbox"/>	Sensor-Pod-0				
<input checked="" type="checkbox"/>	QUE02-C9300-EiaB.mtllab.cisco.com	10.3.1.1	Unreachable	Not Scanned	Mar

Common Upgrade Workflow

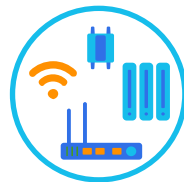
Distribution



Copy of Images to flash via HTTPS/SCP

Install add file <Image Name>

ap image pre-download (C9800)



Activation

Install activate <image name>

Install Commit

Image Update- Parallel or sequential order



Reference

Device Activation Order

You can use filters to sort devices and order their activation in parallel or sequentially. After devices are sorted, you can reorder them sequentially.

Select between Parallel and Sequential Order

Devices in Sequential(2) and Devices in Parallel(4) [Edit Order](#) Terminate on Update Failure:

Parallel **Sequential**

Filter Devices

0 Selected [Move to Parallel Update Order](#) [Reorder List](#) [ISSU](#)

<input type="checkbox"/>	Device Name	IP Address	Site	Device Series	Device Role	Current Image	Update Image i
<input type="checkbox"/>	TRN6-TBRANCH-DIST.cisco.com	10.85.54.17	Global/Canada/Ontario...	Cisco Catalyst 3650 Se...	Distribution	cat3k_caa-universalk9.16...	cat3k_caa-universalk9.16...
<input type="checkbox"/>	TRN6-TBRANCH-C3650-S1.cisco.com	10.85.54.53	Global/Canada/Ontario...	Cisco Catalyst 3650 Se...	Access	cat3k_caa-universalk9.16...	cat3k_caa-universalk9.16...

Image Update- Parallel or sequential order



Reference

Device Activation Order

You can use filters to sort devices and order their activation in parallel or sequentially. After devices are sorted, you can reorder them sequentially.

Devices in Sequential(2) and Devices in Parallel(4) [Edit Order](#) Terminate on Update Failure:

Parallel Sequential

Devices in Sequential(2) and Devices in Parallel(4) [Edit Order](#) Termin

Parallel Sequential

Filter Devices

0 Selected [Move to Parallel Update Order](#) [Reorder List](#) ISSU

<input type="checkbox"/>	Device Name	IP Address	Site
<input type="checkbox"/>	TRN6-TBRANCH-DIST.cisco.com	10.85.54.17	Global/C
<input type="checkbox"/>	TRN6-TBRANCH-C3650-S1.cisco.com	10.85.54.53	Global/C

Edit Order

4 devices will be updated together and then, 2 devices will be updated one after the other. Change activation order by reordering list below.

UPDATE ORDER:

- ☰ Devices in Parallel(4)
- ☰ Devices in Sequential(2)

Cancel Save

Update Image ⓘ

rsalk9.16...	cat3k_caa-universalk9.16...
rsalk9.16...	cat3k_caa-universalk9.16...

Select between Parallel and Sequential Order

Ability to select the specific order for Sequential category

Image Update- Parallel or sequential order



Reference

Device Activation Order

You can use filters to sort devices and order their activation in parallel or sequentially. After devices are sorted, you can reorder them sequentially.

Devices in Sequential(2) and Devices in Parallel(4) [Edit Order](#) Terminate on Update Failure:

Parallel Sequential

Filter Devices

0 Selected [Move to Parallel Update Order](#) [Reorder List](#) [ISSU](#)

Device Name	IP Address	Site	Device Series	Device Role	Current Image
<input type="checkbox"/> TRN6-TBRANCH-DIST.cisco.com	10.85.54.17	Global/Canada/Ontario...	Cisco Catalyst 3650 Se...	Distribution	cat3k_caa-universalk...
<input type="checkbox"/> TRN6-TBR...					...caa-universalk9.16...

Terminate on Update Failure: [?](#)

If update fails for any device in sequential order, subsequent devices in sequential or in parallel order won't be considered for update.

Select between Parallel and Sequential Order

Ability to select the specific order for Sequential category

Ability to act upon failed upgrades

New in 3.1.x - SWIM Page Redesign - More insights

The screenshot displays the Cisco Catalyst Center Software Image Management (SWIM) page. The page is titled "Software Image Management" and includes a navigation bar with "Overview", "Images", "Devices", and "Updates". The "Overview" tab is selected. The page shows several key metrics and insights:

- Images:**
 - Cisco recommends assigning standard images to product families.
 - Device families without standard: 76 ⚠️
 - Critical advisories: 194 ❌
 - High advisories: 3225 ⚠️
- Updates:**
 - Failed Updates: 65 ❌
 - In Progress Updates: 0 ⓘ
 - Successful Updates: 10 ⓘ
- Devices:**
 - Total eligible devices: 351 ⓘ
 - No standard image tagged: 318 ⚠️
 - Ready for update: 7 ⚠️
 - Update readiness failed: 15 ❌
 - Failed image updates: 3 ❌
 - Running standard image: 6 ✅

Two blue callout boxes highlight specific data points:

- Devices with no standard image tagged** (pointing to the 318 ⚠️ metric)
- New Data points: Devices that failed readiness checks** (pointing to the 15 ❌ metric)

New in 3.1.x - SWIM Page Redesign - More insights

Catalyst Center Provision / Network Devices / Software Image Management

Software Image Management Global Switches Wireless controllers Cisco.com ID (Change) Sync Updates

Overview **Images** Devices Updates Updated 10 minutes ago Refresh

Images Images running Show images summary

Show imported images Show task Import images

Product Family Name	Devices	Images	Images Marked Standard	Critical Advisories	High Advisories
Cisco Catalyst 9300 Switch	33	9	✔ 1	23	363
Cisco Catalyst 3650-24PD-E Switch	84	4	⚠	13	150
Cisco Catalyst 9800-CL Wireless Controller for Cloud	22	9	⚠	18	373
Cisco Catalyst 38xx stack-able ethernet switch	13	5	⚠	22	289

Software Insights
Ex. Of 33 x 9300 switches, they have 9 images and only one of those images is standard

Extended Fast Software Upgrade (xFSU)

- xFSU minimizes downtime during software reloads and upgrades
- For Catalyst 9300 Series Switches in both standalone and stack

Control Plane upgraded to IOS XE V2

Control plane notifies neighbors of Graceful Restart

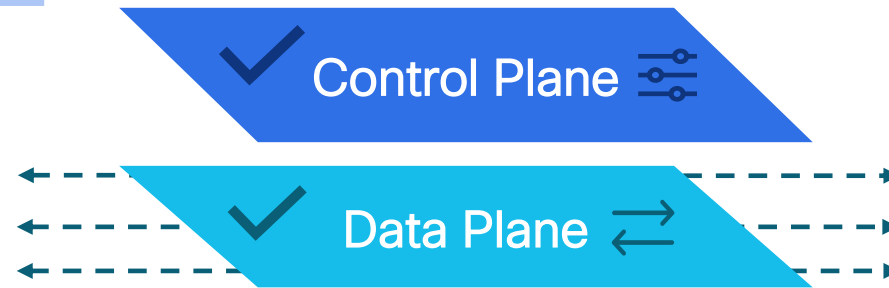
Switch and certain feature configurations are **cached** in the bootflash

Data Plane goes for an upgrade V1 → V2

Data Plane lets traffic flow based on V1 FIB entries

The ASIC is reset by **Flushing** all the TCAM entries

Control Plane goes for an upgrade IOS XE V1 → V2



Data Plane upgraded to V2

```
>_ Command to trigger xFSU  
C9300# install add file <image>  
activate xfsu commit
```



Catalyst 9300/X/L/LM

Total Downtime
< 5 sec

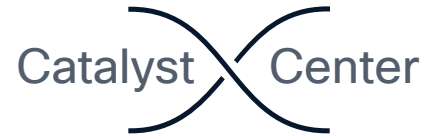
xFSU uses Control and Data plane separation with NSF and Graceful Restart architecture



Habit #4

Assure with Insight

Catalyst Center and ThousandEyes Agents



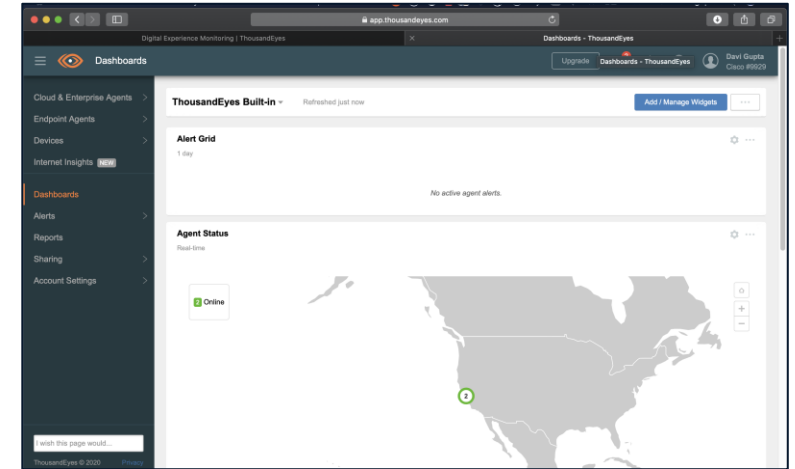
ThousandEyes portal

ThousandEyes Enterprise Agent Tests (4)

Search Table

As of: Mar 6, 2023 12:13 PM

Test Name	Test Type	Target	Device Name	Latest Fetch Sampling Time	Packet Loss (%) Avg / Latest	Jitter (ms) Avg / Latest	Latency (ms) Avg / Latest	Resp.
NetSense - www.slack-redir.net	Web - HTTP Server	https://www.slack-redir.net	SJC01-C9300-01	5 months ago	0 / --	0 / --	0 / --	
Office 365 Login	Network - Agent to Server	52.112.14.70:80	SJC01-C9300-01	5 months ago	100 / --	0 / --	0 / --	
Salesforce	Web - HTTP Server	https://www.salesforce.com	SJC01-C9300-01	5 months ago	0 / --	0 / --	0 / --	
webex	Web - HTTP Server	https://www.webex.com	SJC01-C9300-01	5 months ago	0 / --	0 / --	0 / --	



Agent Deployment at Scale
Visualize Test results in
Application Health
Dashboard

ThousandEyes
Enterprise Agent



C9300/C9400

BRKOPS-2416

ThousandEyes Integration

Before 3.x - Manually paste OAuth Bearer token from ThousandEyes portal

The screenshot shows the Catalyst Center interface. The top navigation bar includes the Cisco logo and 'Catalyst Center' on the left, and 'System / Settings' on the right. A search bar is located in the top left. The left sidebar contains a search bar and a list of settings categories: Cisco Spaces/CMX Servers, Global Manager Integration, Machine Reasoning Engine, Cisco Catalyst Cloud, Webex Integration, ThousandEyes Integration, System Configuration, Debugging Logs, Visibility and Control of Configur..., Geo Map Settings, and Proxy. The main content area is titled 'Settings / External Services' and 'ThousandEyes Integration'. It features an information icon and a text box stating: 'ThousandEyes token is associated with the user profile Login Account. Cisco Catalyst Center collects the data that is returned from ThousandEyes based on the saved token. Changing the user profile Login Account will change the data returned from the API.' Below this, there is a paragraph: 'Use this page to enable ThousandEyes integration. Once enabled, Cisco Catalyst Center will provide ThousandEyes tests information for Application Health dashboard.' A link reads 'Go to ThousandEyes page to get the OAuth Bearer Token'. There is a text input field labeled 'Insert new token here' and a 'Save' button.

After 3.x: Single Sign-On. Account Admin or Org Admin user

The screenshot shows the 'ThousandEyes Enterprise Agent' configuration page. The left sidebar has a progress indicator with steps: 1. Connect ThousandEyes (checked), 2. Select Applications, 3. Configure Application, 4. Select Locations, 5. Select Switches, and 6. Summary. The main content area is titled 'Connect ThousandEyes' and features the Cisco ThousandEyes logo. It includes the text: 'Authorize ThousandEyes access to Catalyst Center' and 'By connecting your ThousandEyes account to Catalyst Center, you agree to Cisco's Terms and Conditions to authorize ThousandEyes access to System Information.' Below this, it says: 'Device authentication code for existing accounts: Verify that the popup window shows the same code after you click Log in.' A modal window titled 'Log In - ThousandEyes' is overlaid, showing a login form with fields for Email, Password, and Region (set to Default). There is a 'Keep me logged in' checkbox and a 'Log In' button. The modal also shows a 'Cancel' button and 'All changes are discarded' text.

New in 3.1 - ThousandEyes Enterprise Agent Enhancements

Out-of-the-box Test creation from Catalyst Center at the time of Agent installation without going to ThousandEyes portal later

The screenshot displays the ThousandEyes Enterprise Agent installation wizard, divided into two main sections: 'Select Applications' and 'Configure Application'.

Select Applications: This section allows users to choose applications to monitor. The available options are Microsoft 365, Webex, Salesforce, and Custom application. A 'Continue without an application' button is also present.

Configure Application: This section shows the configuration for three selected applications:

- Microsoft 365:** Subdomain name (ex: your_company.sharepoint.com), Test interval (5 minutes), and 5 tests included: M365 - OneDrive - Web, M365 - Login - Web, M365 - App Portal - Web, M365 - SharePoint - Web, and M365 - Outlook - Web.
- Slack:** Subdomain name (ex: your_company.slack.com), Test interval (5 minutes), and 2 tests included: Slack - Web and Slack - api.slack.com.
- Webex:** Webex site ID and 1 test included.

The wizard includes a progress indicator on the left with steps: Connect ThousandEyes, Select Applications, Configure Application, Select Locations, Select Switches, and Summary. The 'Configure Application' step is currently active. At the bottom, there are 'Cancel', 'Back', and 'Next' buttons.

You do need HTTPS credentials on the switch

← All discoveries

C9K-STANDALONE-1 Feb 25, 2025 02:47 PM Last updated: this minute

Completed Type: Range Retry count: 3 Protocol order: SSH Total time: 2 minutes 14 seconds [View all details](#) [Re-discover](#)

1 Discovered 1 Reachable 0 Unreachable 0 Discarded

Devices 1

Search

IP address	Device name
10.85.54.77	C9K-STANDALONE-1

To enable application hosting on C9K switch:

- Configure a secure HTTP server
- Configure local or AAA authentication for the HTTPS user. Privilege level 15 required
- Configure NETCONF port on the device before discovery

Command Runner

C9K-STANDALONE-1.cisco.com@10.85.54...

```
C9K-STANDALONE-1.cisco.com> show run | i httpuser  
username httpuser privilege 15 password 7 xxxxxxxx
```

```
C9K-STANDALONE-1.cisco.com> show run | i secure-server  
ip http secure-server
```

```
C9K-STANDALONE-1.cisco.com> show run | i netconf  
netconf-yang
```

```
C9K-STANDALONE-1.cisco.com> █
```

You do need HTTPS credentials on the switch

1 Selected Tag + Add device Software Image Management Actions ^ ⓘ As of: Jan

Tags	Device Name	IP Address
<input type="checkbox"/>	TBRANCH-C3650-STACK	10.85.54
<input type="checkbox"/>	TRN6-TBRANCH-DIST.cisco.com	10.85.54
<input type="checkbox"/>	C3650-ACCESS.cisco.com	10.85.54
<input checked="" type="checkbox"/>	C9K-STANDALONE-1.cisco.com	10.85.54
<input type="checkbox"/>	TRN6-TBRANCH-FUSION	10.85.54

Inventory > Edit Device
Software Image > Resync Device
Provision > Reboot Device
Telemetry > Delete Device
Device Replacement > Export Inventory
Switch Refresh > Schedule Maintenance

To enable application hosting on C9K switch:

- Configure a secure HTTP server
- Configure local or AAA authentication for the HTTPS user. Privilege level 15 required
- Configure NETCONF port on the device before discovery

Devices (8) F

1 Selected Tag +

SNMP Retries and Timeout*

HTTP(S)

Select global credential Add device specific credential

Username* Password*
htpuser Show

Port*
443

View Username Criteria View Password Criteria

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

You do need HTTPS credentials on the switch

Why is "10.10.15.102" marked "Not Ready"?

Readiness Check	Result	Message
Are HTTPS Credentials Provided in the Inventory	✖ Failed	HTTP(s) Username is missing in the Inventory. Provide HTTP(s) Username in the Inventory and try again. The HTTPS credentials are required to connect to App Hosting. Provide the HTTPS credentials in Device Inventory.
Are HTTPS Credentials Valid	✔ Skipped	Test cannot be performed as HTTPS credentials for the device are not provided in the inventory. The HTTPS credentials are required to connect to App Hosting. Provide the HTTPS credentials in Device Inventory.
Does IOS-XE Version support App Hosting	✔ Passed	
Is App Hosting in Sync with the Device	✖ Failed	Failed to authenticate with the device. Verify HTTPS credentials specified in Inventory. Go to Inventory page and edit the device. Confirm that you have provided the correct HTTPS credentials. Also, ensure that the HTTPS username that you have provided in Catalyst Center is also configured on the device with privilege level 15.
Is App Hosting in Sync with the Inventory	✔ Passed	
Is Device Series Supported by Catalyst Center for App Hosting	✔ Passed	
Is Device compatible for App	✖ Failed	The device capability is not discovered successfully. Refresh this device again and install the app. Resync the device from Inventory and then retry.
Is Device in Managed state in the Inventory	✔ Passed	
Is HTTPS Username Configured on the Device	✔ Skipped	
Is Secure HTTP Server Configured on the Device	✔ Passed	

To enable application hosting on C9K switch:
Configure a secure HTTP server

Configure local or AAA authentication for the HTTPS user. Privilege level 15 required

Configure NETCONF port on the device before discovery

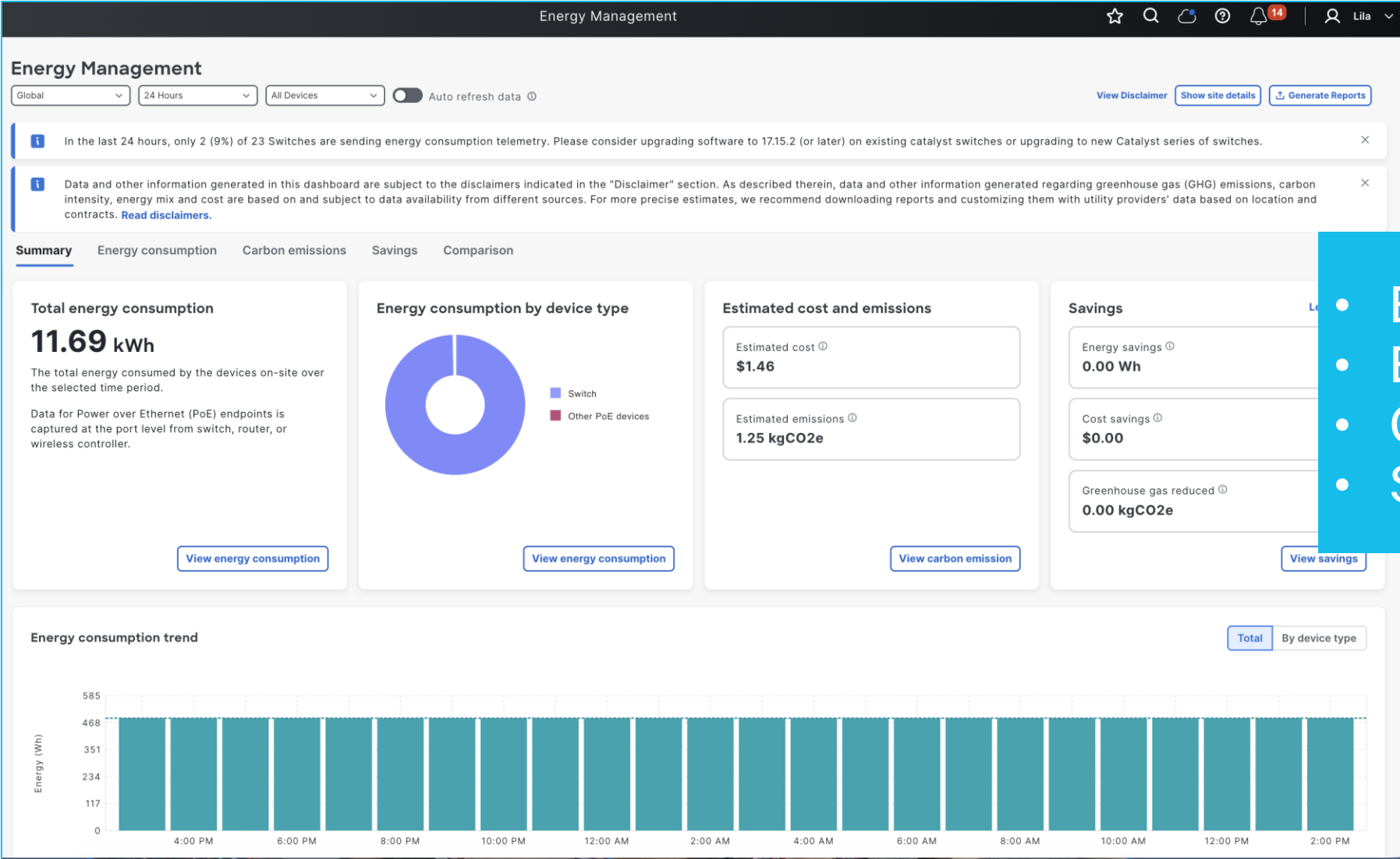
WHY?

There is a REST API that is used to deploy and manage the container in IOS-XE.

The valid characters for the HTTP credential is different to IOS-XE ssh passwords

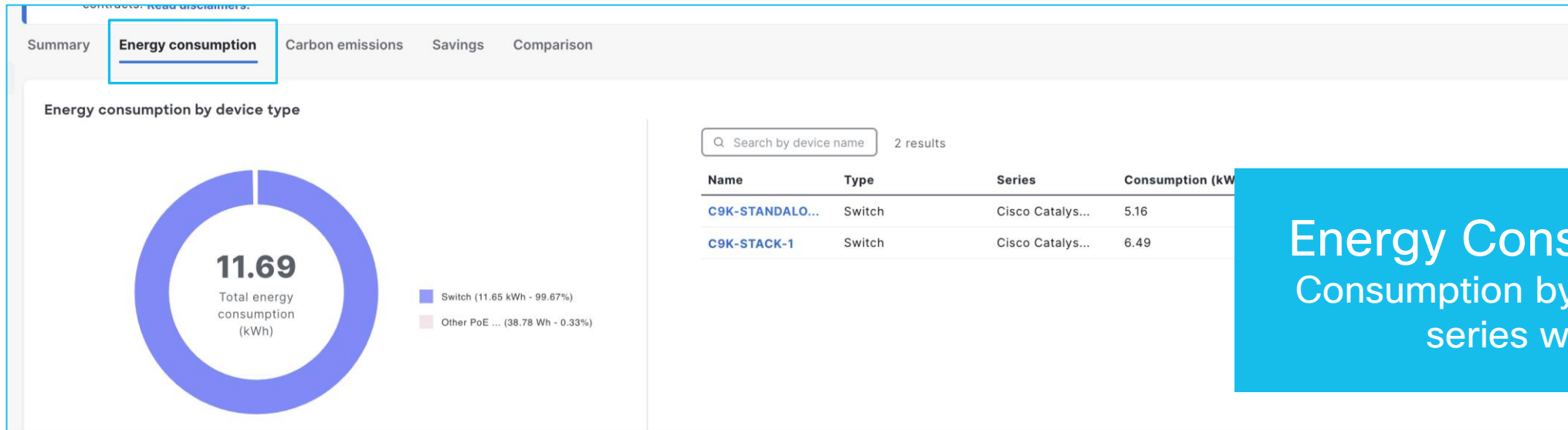
This has always been the case

New in 3.1.6 - Energy Management Dashboard

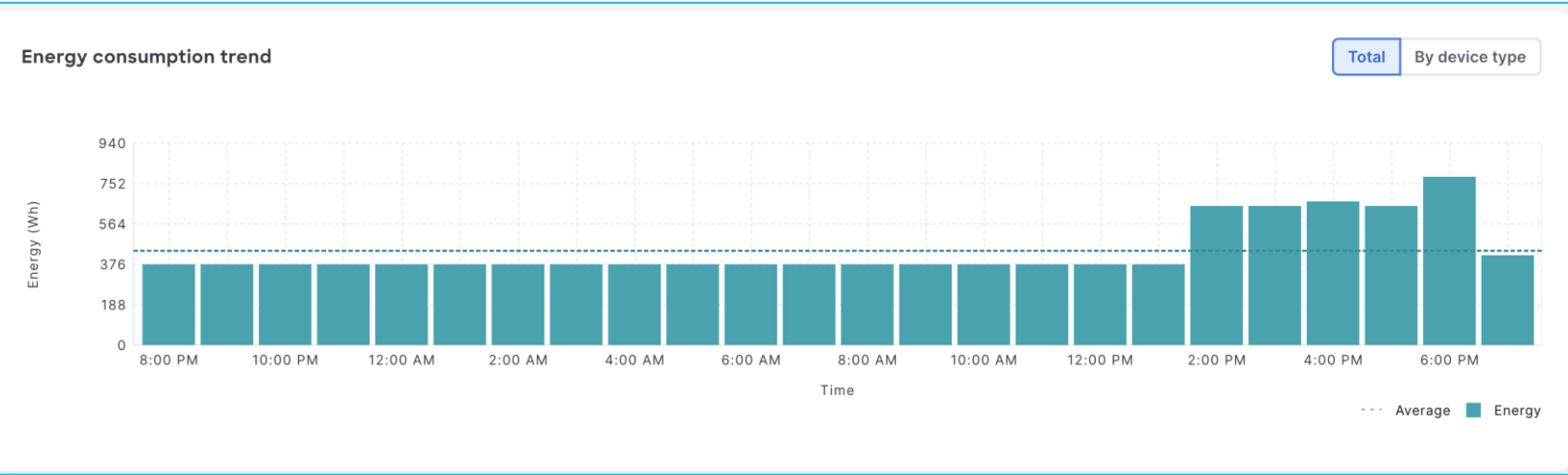


- Energy consumption
- Emissions
- Cost
- Savings

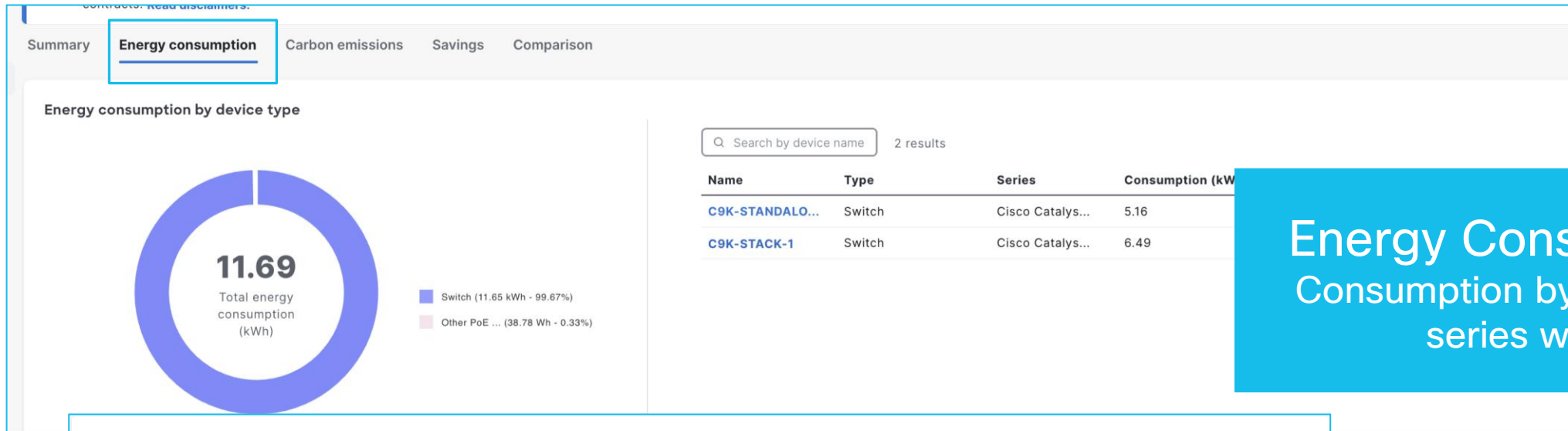
New in 3.1.6 - Energy Management Dashboard



Energy Consumption tab:
Consumption by device type and series with trends



New in 3.1.6 - Energy Management Dashboard



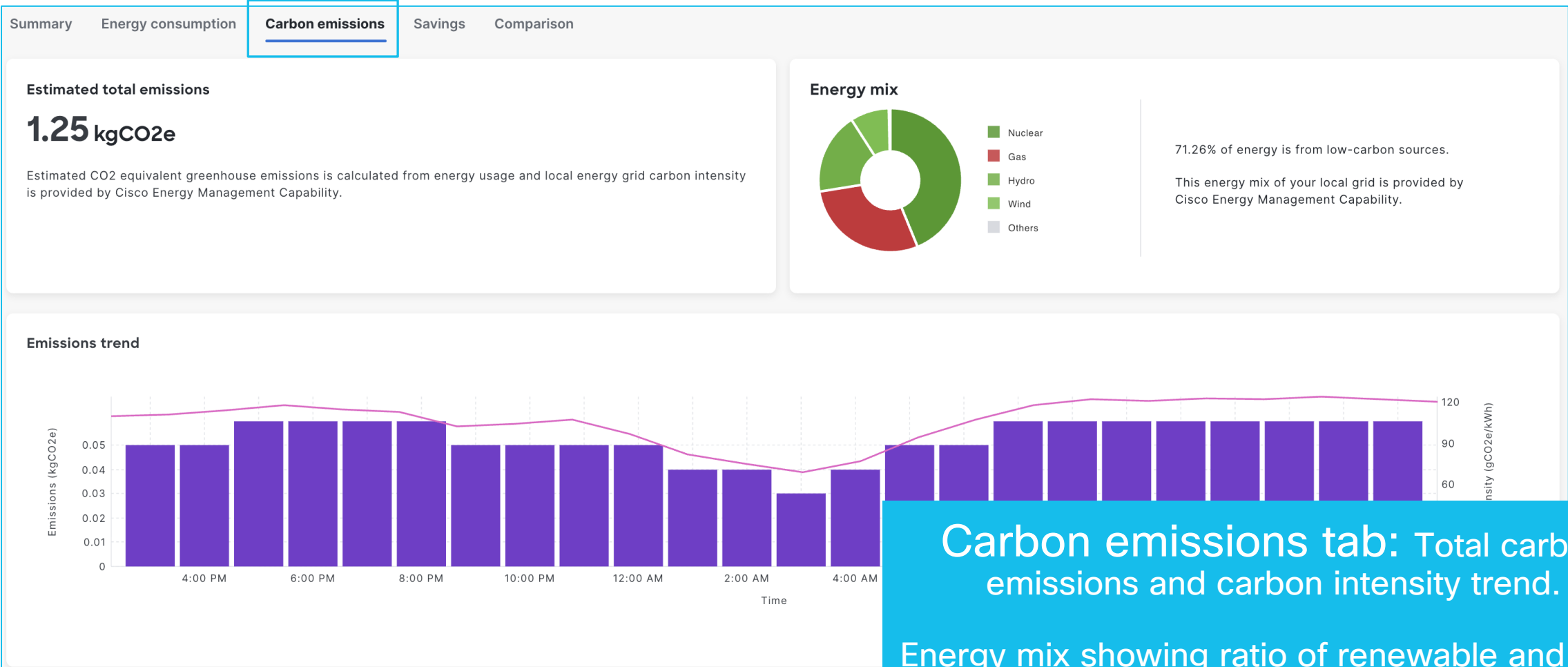
Energy Consumption tab:
Consumption by device type and series with trends



Savings tab:
Cost and energy savings realized for wireless APs when in energy savings mode

DISCLAIMER: Data and outcomes shown are for illustrative purposes and do not represent actual values
BRKOPS-2416

New in 3.1.6 - Energy Management Dashboard

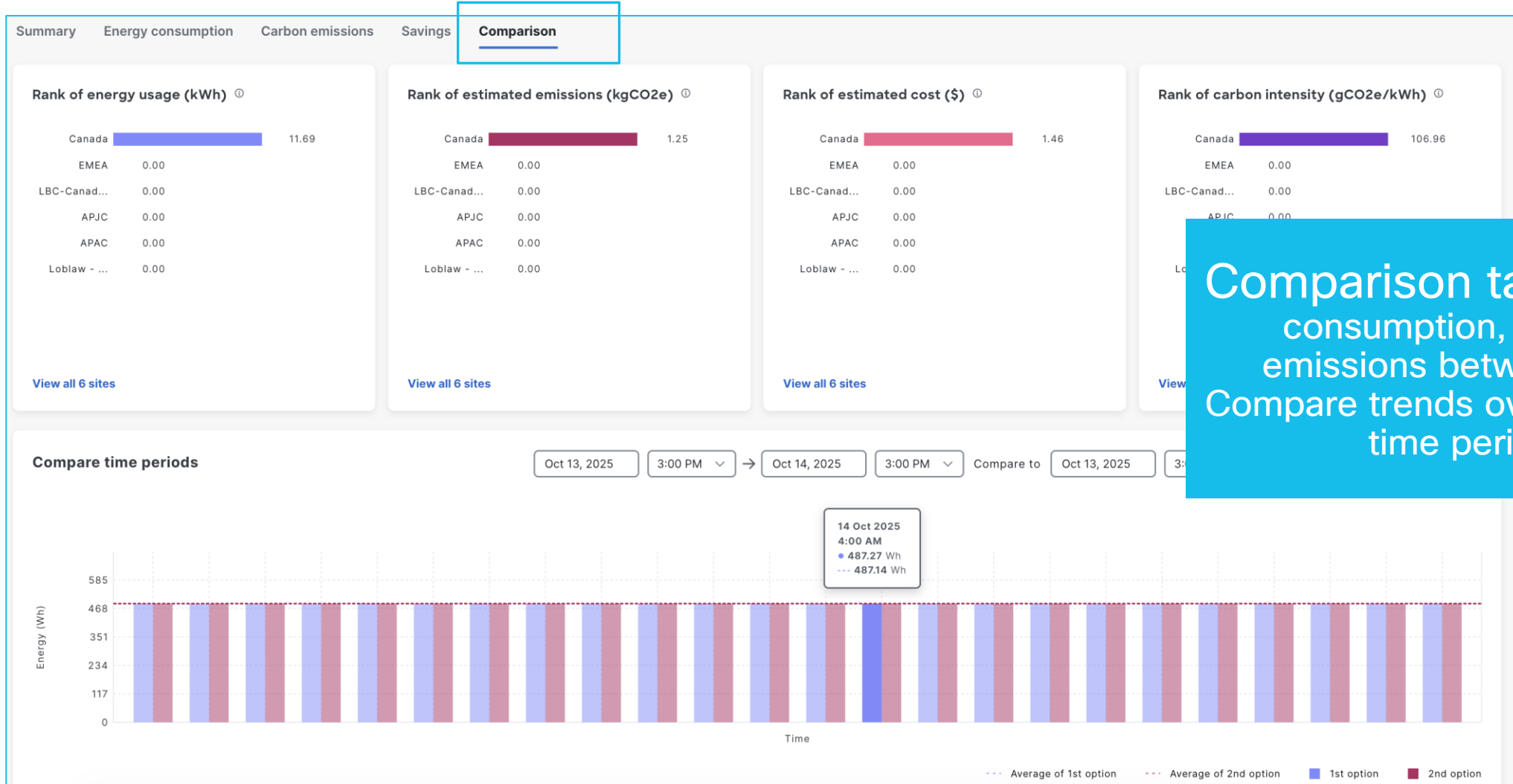


Carbon emissions tab: Total carbon emissions and carbon intensity trend.

Energy mix showing ratio of renewable and low-carbon sources versus fossil fuel-based sources of electricity

DISCLAIMER: Data and outcomes shown are for illustrative purposes and do not represent actual values

New in 3.1.6 - Energy Management Dashboard



Comparison tab: Compare consumption, cost and emissions between sites. Compare trends over 2 different time periods

DISCLAIMER: Data and outcomes shown are for illustrative purposes and do not represent actual values

Where does the data come from?

Electricity Maps provides global access to electricity mix, prices, load, and carbon intensity. Available in real-time, historically and forecasted.

System / Settings

Settings > External Services

Cisco Catalyst Cloud

Use this page to register this Catalyst Center with Cisco Catalyst Cloud.

Registered to **Cisco Catalyst Cloud Portal**

Registered by ar [redacted]

Account auto-cisco-com

Registered on 1 September 2025

De-register

Click 'De-register' to unregister this Catalyst Center with Cisco Catalyst Cloud.

Applications

- 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.
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.
Activate
- Meraki Dashboard**
Integrate Catalyst Center to Meraki to monitor your network deployments in one place. See <http://cs.co/9001AAmZl> for details.
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 Catalyst Center application.
Activate

- Data from 9200/9300/9400 + AP
- 17.15.2 IOS-XE
- Need streaming telemetry connection from switches/WLC (60min updates)
- Cisco Energy Management Capability (EMC) uses electricitymaps.com for costs, etc
- Need Catalyst Center to be registered with cloud to access EMC
- Data kept for 30 days on Catalyst Center
- API and reports to get it off

Subscriptions on switch – Pre 3.1.6

```
telemetry ietf subscription 500
encoding encode-tdl
filter tdl-uri /services;serviceName=ios_oper/poe_port_detail
receiver-type protocol
source-address 10.10.3.122
stream native
update-policy periodic 60000
receiver name DNAC_ASSURANCE_RECEIVER

telemetry ietf subscription 501
encoding encode-tdl
filter tdl-uri /services;serviceName=ios_oper/poe_module
receiver-type protocol
source-address 10.10.3.122
stream native
update-policy periodic 60000
receiver name DNAC_ASSURANCE_RECEIVER

telemetry ietf subscription 504
encoding encode-tdl
filter nested-uri
/services;serviceName=ios_oper/platform_component;cname=0?platform_properties
receiver-type protocol
source-address 10.10.9.4
stream native
update-policy periodic 30000
receiver name DNAC_ASSURANCE_RECEIVER
```

- These are the 3 subscriptions required
- Periodic time is in cento-seconds
- 600 seconds = 10mins

Subscriptions on switch – 3.1.6

```
telemetry ietf subscription 500
encoding encode-tdl
filter tdl-uri /services;serviceName=ios_oper/poe_port_detail
receiver-type protocol
source-address 10.10.9.4
stream native
update-policy periodic 360000
receiver name DNAC_ASSURANCE_RECEIVER

telemetry ietf subscription 501
encoding encode-tdl
filter tdl-uri /services;serviceName=ios_oper/poe_module
receiver-type protocol
source-address 10.10.9.4
stream native
update-policy periodic 360000
receiver name DNAC_ASSURANCE_RECEIVER

telemetry ietf subscription 504
encoding encode-tdl
filter nested-uri
/services;serviceName=ios_oper/platform_component;cname=0?platform_properties
receiver-type protocol
source-address 10.85.54.54
stream native
update-policy periodic 30000
receiver name DNAC_ASSURANCE_RECEIVER
```

- Periodic time is in cento-seconds
- 3600 seconds = 1 hour

On the POE dashboard, notified of change

The screenshot shows the Assurance / Dashboards / PoE interface. At the top, there is a navigation bar with the breadcrumb "Assurance / Dashboards / PoE" and user information "adam". Below the navigation bar, the main content area shows a notification box with the following text:

Update: PoE Data Collection Frequency Change. [Collapse to hide.](#)

Data Collection Frequency for PoEs reduced to once per hour.

PoE Data Collection Frequency is now once per hour in order to improve system response time and accommodate additional energy consumption data.

Seven (7) Impacted Dashlets:

- PoE Operational State Distribution
- PoE Powered Device Distribution
- PoE Insights
- Power Allocation Load Distribution
- Power Usage
- PoE Port Availability
- PoE AP Power Mode Distribution

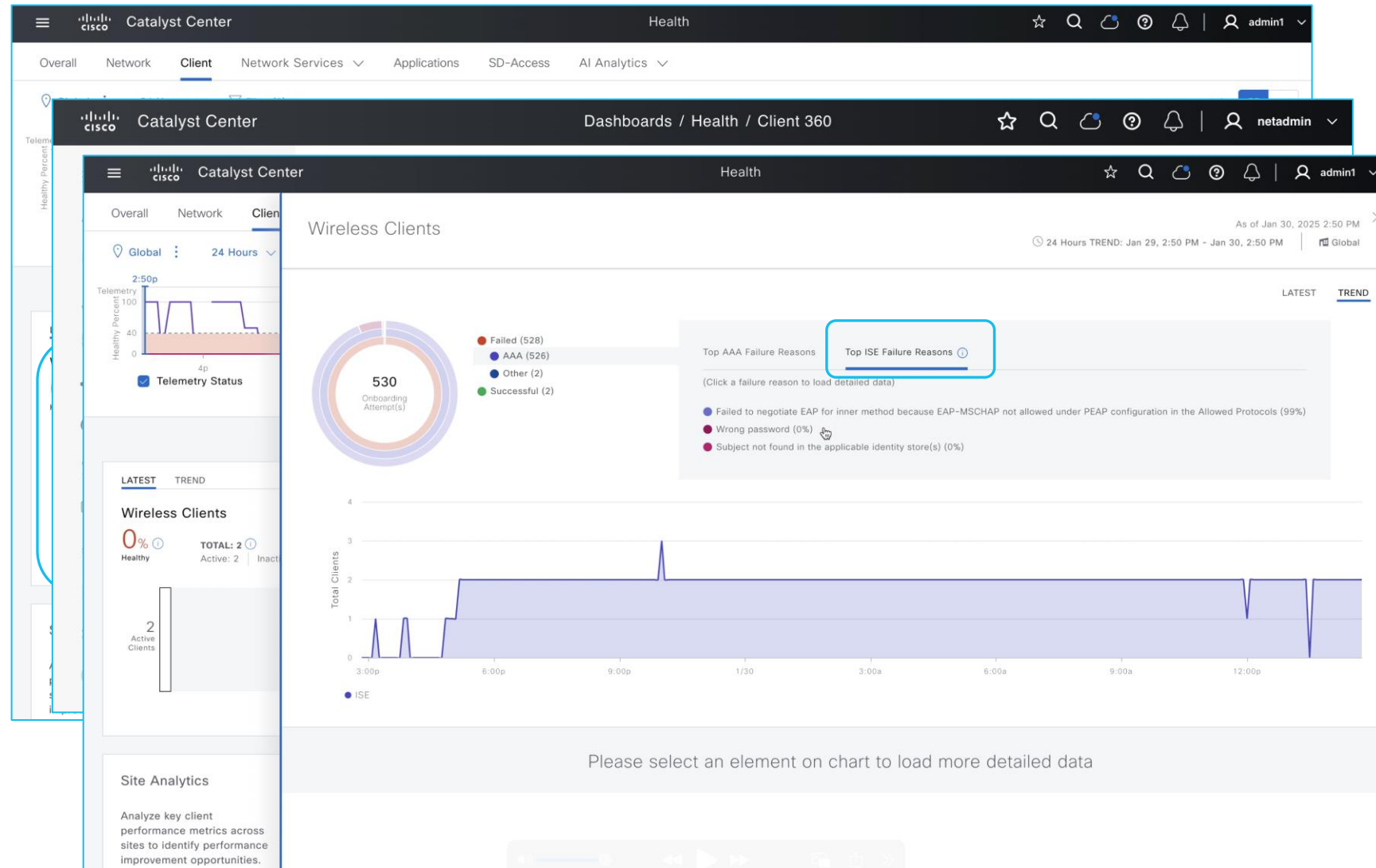
Energy Management Dashboard provides "Energy" view of environment vs PoE view
POE dashboard great for drilling into client devices

New in 3.1 - ISE Authentication Failures

Previously check the ISE live logs to understand the Client's onboarding failure reason

With ISE integration, see the the failure reason of client onboarding, in Catalyst Center

NOTE: AAA Failure reasons count might be different to ISE due to retries and failure throttling on ISE

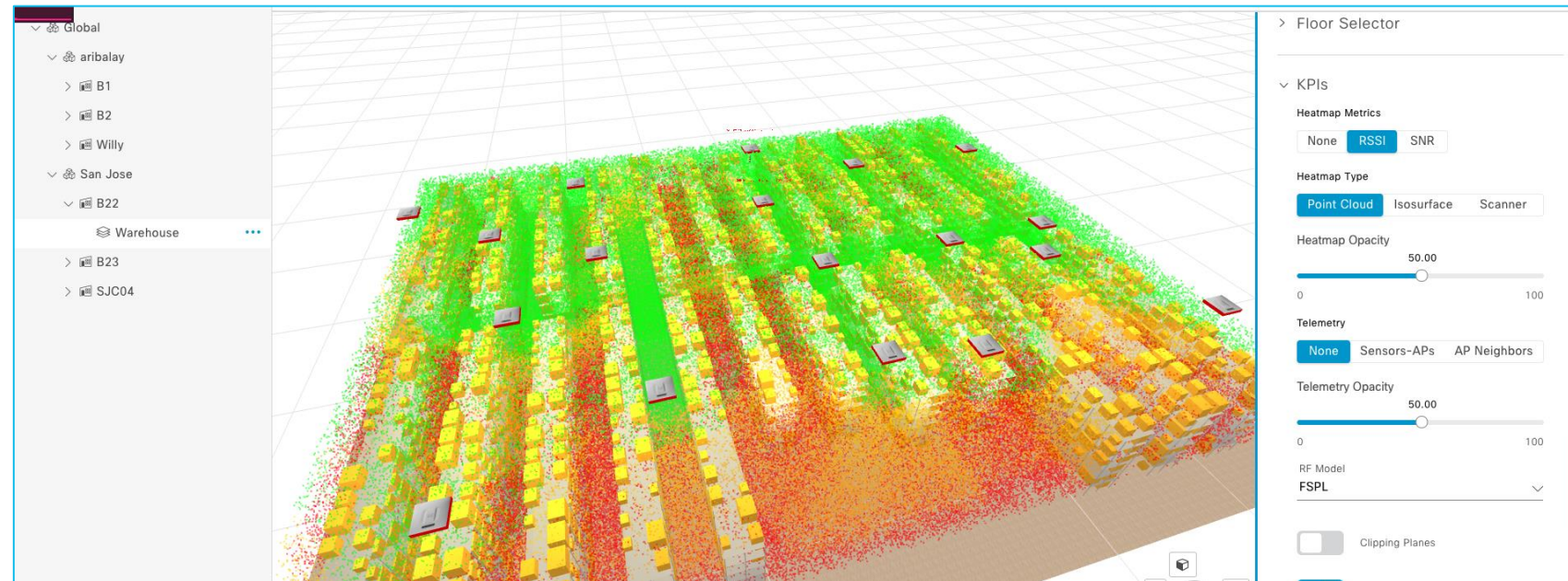
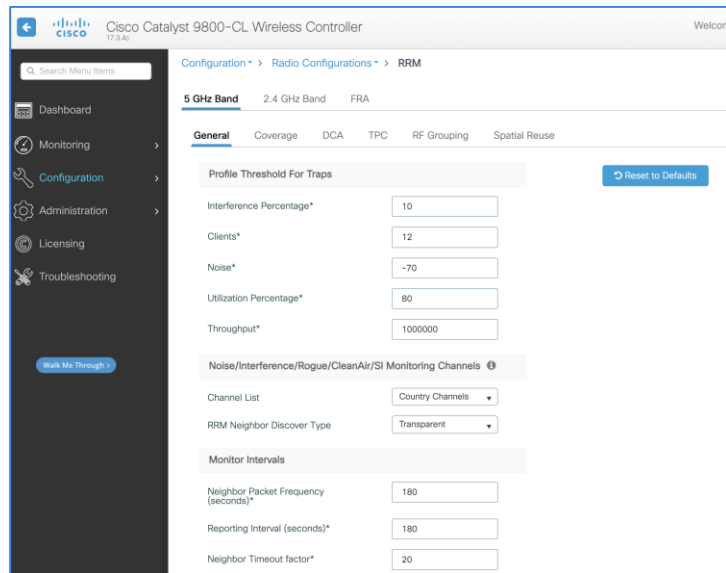




Habit #5

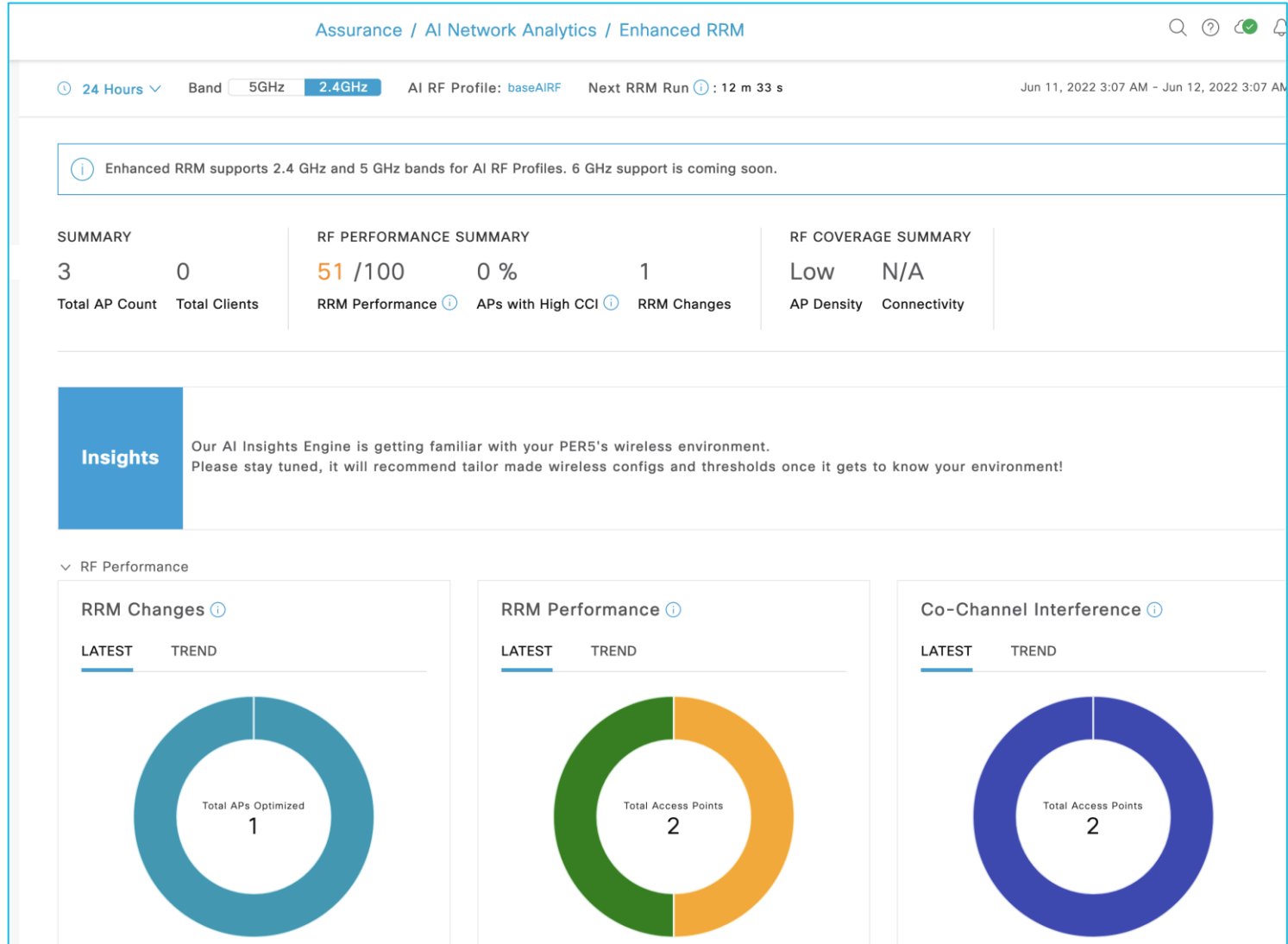
Transform with AIOps

Why radio resource management



- 10min worth of data
- No "busy hour(s)"
- No building segmentation
- No visibility
- Lots of tuning knobs
- No simulation mode **

Dashboard



Scale Limits

Enabled per WLC

"Brownfield" now supported 2.3.7.4

All AP can be enabled:

Limit per building

- 1500 (5 & 2.4 GHz radios)
- 600 (6GHz radio)

Release 3.1.3

Significant provisioning scale improvements

Extreme case: 24h+ -> 4 hour

AI Assistant

Wireless Clients
Healthy: 100%
TOTAL: 6
Active: 6 | Inactive: 0 | New: 0
6 Active Clients, 6 Onboarded, Good Connectivity 100%

AI Assistant
You: Show me all switch ports connected to access points. Tell me how many are APs, Cisco APs, and how many are third-party APs?
AI Assistant (05:30 pm): Here are the results for switch ports connected to access points (APs):

AP connectivity summary		
Total APs connected	Cisco APs connected	Third-party APs connected
6	0	0

This means all 6 APs currently connected to your switch ports are not identified as Cisco or third-party APs by name. If you need a detailed list of the specific ports or more information about the APs, please let me know.

Ask the AI Assistant a question

Assistant can make mistakes. Verify responses. Learn how the AI Assistant handles your data at [AI Assistant](#)

EFT: December 2025
Beta: 2.3.7.11 / 3.2.x

Dashboard + Catalyst Center Global Overview

The screenshot shows the Meraki Catalyst Center Global Overview dashboard. At the top, it displays 'Global Overview' with a search bar and a refresh button. Below this, there's a 'Network/site health' section with a circular gauge showing '1.1k' total networks/sites. The gauge is divided into three segments: Good (827), Fair (145), and Poor (138). To the right, there are several summary cards for 'Offline/Poor devices' categorized by type: Routers & WAN Appliances (306 total), Core Switches (456 total), Distribution Switches (488 total), Access Switches (896 total), WLCs & CGs (12 total), and Access Points (3214 total). Below these is a table for 'Organizations' with columns for Organization, Controller Type, Networks & Sites, Critical Alerts, Routers & WAN Appliances, Switches, WLCs & CGs, and Access Points. The table lists various organizations like Central Europe, Singapore, US, China, Japan, etc.

EFT: Mid November
 Requires: 2.3.7.x or 3.x build
 Limited access

Organizations Poor networks & sites

Search: Network/site health Device status 115 results

Organization	Controller type	Networks & sites	Critical alerts	Routers & WAN appliances	Cellular gateways	Switches	WLCs & CGs
Central Europe	Catalyst Center	16 / 231	21	2 / 60		9 / 567	1 / 8
Singapore	Dashboard	13 / 35	20	1 / 23	3 / 3	8 / 64	3 / 512
US	Catalyst Center	5 / 201	18	1 / 17		3 / 80	2 / 1456
China	Catalyst Center	5 / 31	18	1 / 9		2 / 31	4 / 215
Japan	Catalyst Center	4 / 483	15	5 / 16		2 / 45	6 / 3118

Access Switches Offline / Poor devices

Search: 9 results

Status	Device name	Network / Site	Organization	Total alerts
Offline	98:18:88-01:55:80	Bluejay-CoreNet	Singapore	3
Offline	Switch C9200L-PEN	IronPeak-FG05	Central Europe	3
Offline	Dallas-Access101	DeltaPoint-Branch01	UK Manchester	2
Offline	Branch1-MS150-566	Ced		
Offline	Marketing-C9300-667	Falc		
Offline	SEA-F1-9164-6	Mag		
Offline	HQ-access57-MS130	Nim		
Offline	HUB-East-MS150-45	Crin		
Offline	HQ-RTR1-675	Ech		

Switch C9200L-PEN.enprglab.local

Model: C9200L-24P-4X Management IP: 192.168.138.130 Location: Global / Prague / PRG07 Software: 17.9.3 Risk: ACCESS Fabric Role: EX Fabric Size: Global/Prague/PRG07 Virtual Networks: VN-ISP-Profiled_Devices (15 more)

Issues Physical Neighbor Topology Event Viewer Path Trace Application Experience Device Info Interfaces Fabric Site PoE



Habit #6

Integrate to Innovate

Why API?



AUTOMATION



INTEGRATION



INNOVATION

API First 2.3.7.6 release notes

Table 6. New and Changed Features in Catalyst Center Platform, Release 2.3.7.7

Feature	Description
New APIs	
Compliance API	<p>Catalyst Center platform supports the following Compliance API:</p> <ul style="list-style-type: none"> POST <cluster-ip>/dna/intent/api/v1/compliance/networkDevices/{id}/issues/remediation/provision Compliance Remediation. <p>To access the new Compliance API, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Know Your Network drop-down list and choose Compliance.</p>
Issues APIs	<p>Catalyst Center platform supports the following Issues APIs:</p> <ul style="list-style-type: none"> POST <cluster-ip>/dna/intent/api/v1/issues/resolve Resolve the given list of issues. POST <cluster-ip>/dna/intent/api/v1/issues/ignore Ignore the given list of issues. POST <cluster-ip>/dna/intent/api/v1/issues/{id}/update Update the given issue by updating selected fields. <p>To access the new Compliance API, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Know Your Network drop-down list and choose Issues.</p>
Licenses APIs	<p>Catalyst Center platform supports the following Licenses APIs:</p> <ul style="list-style-type: none"> PUT <cluster-ip>/dna/intent/api/v1/licenseSetting Update license setting. GET <cluster-ip>/dna/intent/api/v1/licenseSetting Retrieve license setting. <p>To access the new Licenses APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Cisco DNA Center System drop-down list and choose Licenses.</p>
Network Settings APIs	<p>Catalyst Center platform supports the following Network Settings APIs:</p> <ul style="list-style-type: none"> PUT <cluster-ip>/dna/intent/api/v1/sites/{id}/timeZoneSettings Set time zone for a site. PUT <cluster-ip>/dna/intent/api/v1/sites/{id}/bannerSettings Set banner settings for a site. PUT <cluster-ip>/dna/intent/api/v1/sites/{id}/telemetrySettings Set telemetry settings for a site. <p>To access the new Network Settings APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Site Management drop-down list and choose Network Settings.</p>
SDA APIs	<p>Catalyst Center platform supports the following SDA APIs:</p> <p>Multicast APIs</p> <ul style="list-style-type: none"> GET <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks Get multicast virtual networks. GET <cluster-ip>/dna/intent/api/v1/sda/multicast Get multicast. PUT <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks Update multicast virtual networks. GET <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks/count Get multicast virtual network count. DELETE <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks/{id} Delete multicast virtual network by ID. POST <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks Add multicast virtual networks.

Site Design APIs	<p>Catalyst Center platform supports the following Site Design APIs:</p> <ul style="list-style-type: none"> POST <cluster-ip>/dna/intent/api/v1/networkDevices/assignToSite/apply Assign network devices to a site. POST <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/{profileid}/siteAssignments Assign a network profile for sites to the given site <p>To access the new Site Design APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Site Management drop-down list and choose Site Design.</p>
SWIM APIs	<p>Catalyst Center platform supports the following SWIM APIs:</p> <ul style="list-style-type: none"> GET <cluster-ip>/dna/intent/api/v1/images Get list of images available under the given site and product name. POST <cluster-ip>/dna/intent/api/v1/images/{id}/download Download the software image from Cisco.com on the disk for the given 'id'. GET <cluster-ip>/dna/intent/api/v1/productNames Get the list of network device product names, their ordinal, and the support PIDs based on filter criteria. GET <cluster-ip>/dna/intent/api/v1/productNames/count Get count of product names based on filter criteria. GET <cluster-ip>/dna/intent/api/v1/images/{imageid}/productNames/{productNameOrdinal} Update the list of sites for the network device product name assigned to the software image. GET <cluster-ip>/dna/intent/api/v1/siteWiseProductNames Get network device product names for a site. POST <cluster-ip>/dna/intent/api/v1/images/{imageid}/productNames Assign network device product name and sites for the given image identifier. GET <cluster-ip>/dna/intent/api/v1/siteWiseProductNames/count Get the count of network device product names for the given filters. DELETE <cluster-ip>/dna/intent/api/v1/images/{imageid}/productNames/{productNameOrdinal} Removes the network device product name from all the sites for the given software image. PUT <cluster-ip>/dna/intent/api/v1/images/{imageid}/productNames/{productNameOrdinal} Update the list of sites for the network device product name assigned to the software image. GET <cluster-ip>/dna/intent/api/v1/images/count Count of images available under the given site and product name. GET <cluster-ip>/dna/intent/api/v1/images/{id}/addonImages Retrieves the list of applicable add-on images if available for the given software image. GET <cluster-ip>/dna/intent/api/v1/images/{id}/addonImages/count Count of add-on images available for the given software image identifier. GET <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings Retrieve the list of remote image distribution servers. POST <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings Add image distribution server for distributing software images. GET <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings/{id} Get image distribution server for specified server identifier. PUT <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings/{id} Update remote image distribution server. DELETE <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings/{id} Delete remote image distribution server.

2.3.7.9 release notes

For detailed information about the APIs, see the [Cisco Catalyst Center APIs on Cisco DevNet](#).

Table 9. New and changed features in Catalyst Center platform 2.3.7.9

Feature	Description
New APIs	
Applications APIs	<p>Catalyst Center platform supports the following Applications APIs:</p> <ul style="list-style-type: none"> GET <cluster-ip>/dna/data/api/v1/networkApplications Retrieves the list of network applications along with experience and health metrics. GET <cluster-ip>/dna/data/api/v1/networkApplications/count Retrieves the total count of network applications by applying basic filtering. POST <cluster-ip>/dna/data/api/v1/networkApplications/trendAnalytics Retrieves the Trend analytics data related to network applications. <p>To access the new Applications APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Know Your Network drop-down list and choose Applications.</p>
Application Policy APIs	<p>Catalyst Center platform supports the following Application Policy APIs:</p> <ul style="list-style-type: none"> GET <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices Retrieve the list of network devices with their application visibility status. GET <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/count Retrieve the count of network devices for the given application visibility status filters. POST <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/enableAppTelemetry Enable application telemetry feature on multiple network devices. POST <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/disableAppTelemetry Disable application telemetry feature on multiple network devices. POST <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/enableCbar Enable CBAR feature on multiple network devices. POST <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/disableCbar Disable CBAR feature on multiple network devices. GET <cluster-ip>/dna/intent/api/v1/qosPolicySetting Retrieves the application QoS policy setting. PUT <cluster-ip>/dna/intent/api/v1/qosPolicySetting Updates the application QoS policy setting. <p>To access the new Application Policy APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Policy drop-down list and choose Application Policy.</p>
Cisco Integrated Management Controller (IMC) APIs	<p>Catalyst Center platform supports the following Cisco IMC APIs:</p> <ul style="list-style-type: none"> GET <cluster-ip>/dna/system/api/v1/ciscolmcs Retrieves Cisco IMC configurations for Catalyst Center nodes. POST <cluster-ip>/dna/system/api/v1/ciscolmcs Adds Cisco IMC configuration to a Catalyst Center node. GET <cluster-ip>/dna/system/api/v1/ciscolmcs/{id} Retrieves the Cisco IMC configuration for a Catalyst Center node. PUT <cluster-ip>/dna/system/api/v1/ciscolmcs/{id} Updates the Cisco IMC configuration for a Catalyst Center node. DELETE <cluster-ip>/dna/system/api/v1/ciscolmcs/{id} Deletes the Cisco IMC configurations for a Catalyst Center node. <p>To access the new Cisco IMC APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Appliance drop-down list and choose Cisco IMC.</p>
Compliance APIs	<p>Catalyst Center platform supports the following Compliance APIs:</p> <ul style="list-style-type: none"> POST <cluster-ip>/dna/intent/api/v1/networkBugs/trials Creates a trial for bugs detection on network devices. GET <cluster-ip>/dna/intent/api/v1/networkBugs/trials Get trial details for bugs detection on network devices. POST <cluster-ip>/dna/intent/api/v1/networkBugs/triggerScan

Configuration Archive APIs	<p>Catalyst Center platform supports the following Configuration Archive APIs:</p> <ul style="list-style-type: none"> GET <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles Get Network Device Configuration File Details. GET <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles/count Count of Network Device Configuration Files. GET <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles/{id} Get Configuration File Details by ID. POST <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles/{id}/downloadMasked Download masked device configuration. POST <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles/{id}/downloadUnmasked Download Unmasked (raw) Device Configuration as ZIP. <p>To access the new Configuration Templates APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Site Management drop-down list and choose Configuration Archive APIs.</p>
Configuration Templates APIs	<p>Catalyst Center platform supports the following Configuration Templates APIs:</p> <ul style="list-style-type: none"> GET <cluster-ip>/dna/intent/api/v1/templates/{templateId}/networkProfilesForSites Retrieve the network profiles attached to a CLI template. GET <cluster-ip>/dna/intent/api/v1/templates/{templateId}/networkProfilesForSites/count Retrieve count of network profiles attached to a CLI template. POST <cluster-ip>/dna/intent/api/v1/templates/{templateId}/networkProfilesForSites Attach network profile to a Day-N CLI template. POST <cluster-ip>/dna/intent/api/v1/templates/{templateId}/networkProfilesForSites/bulk Attach a list of network profiles to a Day-N CLI template. DELETE <cluster-ip>/dna/intent/api/v1/templates/{templateId}/networkProfilesForSites/bulk Detach a list of network profiles from a Day-N CLI template. DELETE <cluster-ip>/dna/intent/api/v1/templates/{templateId}/networkProfilesForSites/{profileId} Detach a network profiles from a Day-N CLI template. GET <cluster-ip>/templates/{templateId}/versions Get Template Versions. GET <cluster-ip>/dna/intent/api/v1/templates/{templateId}/versions/{versionId} Get Template Version. GET <cluster-ip>/dna/intent/api/v1/templates/{templateId}/versions/count Get Template Versions Count. POST <cluster-ip>/dna/intent/api/v1/templates/{templateId}/versions/commit Commit Template For a New Version. GET <cluster-ip>/dna/intent/api/v1/projects Get Template Projects. POST <cluster-ip>/dna/intent/api/v1/projects Create Template Project. PUT <cluster-ip>/dna/intent/api/v1/projects/{projectId} Update Template Project. GET <cluster-ip>/dna/intent/api/v1/projects/{projectId} Get Template Project. DELETE <cluster-ip>/dna/intent/api/v1/projects/{projectId} Delete Template Project. GET <cluster-ip>/dna/intent/api/v1/projects/count Get Template Project Count. <p>To access the new Configuration Templates APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Site Management drop-down list and choose Configuration Templates APIs.</p>
Devices APIs	<p>Catalyst Center platform supports the following Devices APIs:</p> <ul style="list-style-type: none"> POST <cluster-ip>/dna/intent/api/v1/networkDevices/deleteWithoutCleanup Delete a network device without configuration cleanup. POST <cluster-ip>/dna/intent/api/v1/networkDevices/deleteWithCleanup

3.1.5 release notes

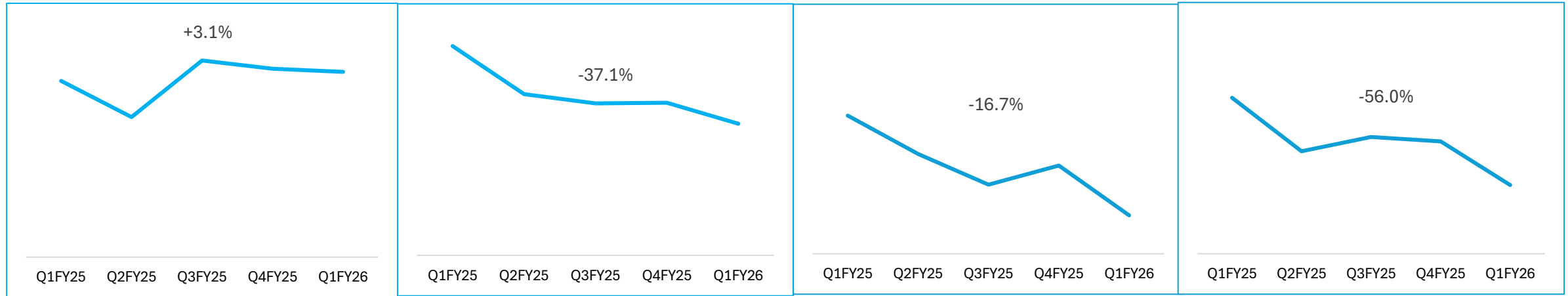
<p>Compliance API Operations</p>	<p>Catalyst Center platform supports the following Compliance API operations:</p> <ul style="list-style-type: none"> • POST <cluster-ip>/dna/intent/api/v1/compliancePolicies Create a new policy. • GET <cluster-ip>/dna/intent/api/v1/compliancePolicies Retrieve the policies. • GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/count Retrieve the count of policies. • GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${id} Retrieve a specific policy. • PUT <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${id} Update an existing policy. • DELETE <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${id} Delete a specific policy. • POST <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules Create a new rule. • GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules Retrieve the rules. • GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/count Retrieve the count of rules. • GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${id} Retrieve a specific rule. • PUT <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${id} Update an existing rule. • DELETE <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${id} Delete a specific rule. • POST <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/conditions Create a new condition • GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/conditions Retrieve the conditions. • GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/conditions/count Retrieve the count of conditions. • GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/conditions/\${id} Retrieve a specific condition. • PUT <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/conditions/\${id} Update an existing condition. • DELETE <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/conditions/\${id} Delete a specific condition. • POST <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/variables Create a new variable. • GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/variables Retrieve the variables. • GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/variables/count Retrieve the count of variables. • GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/variables/\${id} Retrieve a specific variable. • PUT <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/variables/\${id} Update an existing variable. • DELETE <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/variables/\${id} Delete a specific variable. • PUT <cluster-id>/dna/intent/api/v1/compliancePolicies/\${policyId}/siteAssignments Set site assignments for policy. • GET <cluster-id>/dna/intent/api/v1/compliancePolicies/\${policyId}/siteAssignments
----------------------------------	--

<p>Devices API Operations</p>	<p>Catalyst Center platform supports the following Devices API operations:</p> <ul style="list-style-type: none"> • GET <cluster-ip>/dna/intent/api/v1/filterGroups Get the filter groups for given search criteria. • POST <cluster-ip>/dna/intent/api/v1/filterGroups Create filter group. • GET <cluster-ip>/dna/intent/api/v1/filterGroups/\${id} Get the filter group details for the given ID. • PUT <cluster-ip>/dna/intent/api/v1/filterGroups/\${id} Update filter group. • DELETE <cluster-ip>/dna/intent/api/v1/filterGroups/\${id} Delete a filter group. • GET <cluster-ip>/dna/intent/api/v1/filterGroupAssociations Get the filter group associations. • DELETE <cluster-ip>/dna/intent/api/v1/filterGroupAssociations/\${id} Delete filter group association. • POST <cluster-ip>/dna/intent/api/v1/filterGroupAssociations Create filter group association. <p>To access the new Filter Groups API operations, click the menu icon and choose Platform. Expand the Know Your Network drop-down list and choose Devices.</p>
<p>User and Roles API Operations</p>	<p>Catalyst Center platform supports the following User and Roles API operations:</p> <ul style="list-style-type: none"> • POST <cluster-ip>/dna/system/api/v2/roles Add role v2. • POST <cluster-ip>/dna/system/api/v1/accessGroups Add access group. • GET <cluster-ip>/dna/system/api/v1/accessGroups/\${id} Get access group. • DELETE <cluster-ip>/dna/system/api/v1/accessGroups/\${id} Delete access group. • PUT <cluster-ip>/dna/system/api/v1/accessGroups/\${id} Update access group. • GET <cluster-ip>/dna/system/api/v1/accessGroups Get access groups. • GET <cluster-ip>/dna/system/api/v1/accessGroups/count Get access group count. • DELETE <cluster-ip>/dna/system/api/v2/roles/\${id} Delete role v2. • GET <cluster-ip>/dna/system/api/v2/roles/Permissions Get permissions v2. • GET <cluster-ip>/dna/system/api/v2/roles/\${id} Get role v2. • PUT <cluster-ip>/dna/system/api/v2/roles/\${id} Update role v2. • GET <cluster-ip>/dna/system/api/v2/roles Get roles v2. <p>To access the new User and Roles API operations, click the menu icon and choose Platform. Expand the System drop-down list and choose User and Roles.</p>

Habit #7

**Maintain Platform Currency for
Maximum Resiliency**

Catalyst Center - Improving Quality Trends



SR Trends	Escalation Trends	Defect Trends	Defect Density*
-----------	-------------------	---------------	-----------------

-1.0% Q/Q
+3.1% Y/Y

-14.0% Q/Q
-37.1% Y/Y

-9.1% Q/Q
-16.7% Y/Y

-38.8% Q/Q
-56.0% Y/Y

- Marginal 3.1% increase in YoY SR cases despite a huge 15.2% increase in CatC deployments and 27.2% increase in managed devices count during the same period
- Huge decrease in Q/Q and Y/Y escalated case volumes
- Healthy reduction in field defects
- Systematic and large reduction in Q/Q and Y/Y defect density*

* No of defects per Million managed devices

Why is upgrade to 3.x different than previous upgrades?

Catalyst Center 3.x introduces an architectural evolution for efficiency and innovation:

- improved network automation and monitoring
- optimized resource utilization, and
- increased security

Data migration will be used as the bridge to the new platform

- As part of the upgrade workflow, both RSYNC and NFS will be required

Faster upgrades

Single backup destination

Automation Enhancements

SB-RBAC

Consistent look and feel across Cisco platforms

Rule-based compliance

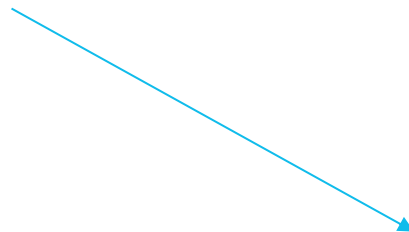
Backup Retention

Catalyst Center - Current RBAC

Users

Role

Permissions



Assurance Deny Read Write

Monitoring and Troubleshooting Deny Read Write



Network Design Deny Read Write

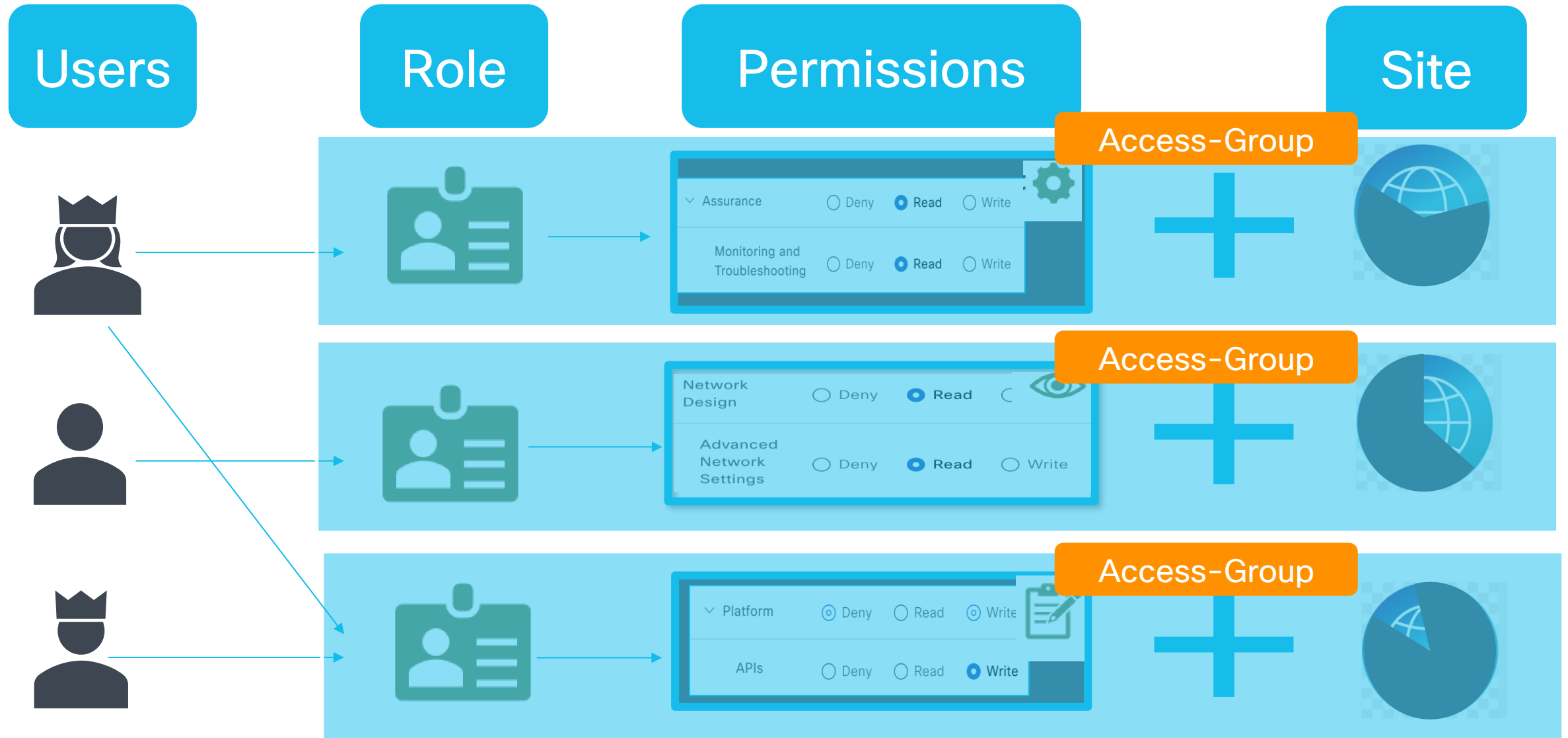
Advanced Network Settings Deny Read Write



Platform Deny Read Write

APIs Deny Read Write

New in Catalyst Center 3.1.x- Site based RBAC



New in Catalyst Center 3.1.x- Site based RBAC

Create an RBAC Role



Define the Access

i These permissions enable different capabilities in Catalyst Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these permissions allow. Click here to [Learn More](#). ×

Define the **Cisco-Live-Operator(v2)** role. Custom roles permit or restrict user access to certain Catalyst Center functions. By default, roles are configured with Read permission, which is an Observer role. If a role is configured with Deny permission, all related content for that capability is removed from the GUI.

Extensions	<input type="radio"/> Deny	<input checked="" type="radio"/> Read	<input type="radio"/> Write	and third-p
Network Design	<input type="radio"/> Deny	<input checked="" type="radio"/> Read	<input type="radio"/> Write	Configure n repository.
Network Management	<input checked="" type="radio"/> Deny	<input checked="" type="radio"/> Read	<input type="radio"/> Write	Discover an
Discovery	<input type="radio"/> Deny	<input checked="" type="radio"/> Read	<input type="radio"/> Write	Discover ne
Hierarchy	<input type="radio"/> Deny	<input checked="" type="radio"/> Read	<input type="radio"/> Write	Create a ne location. Th
Inventory	<input type="radio"/> Deny	<input checked="" type="radio"/> Read	<input type="radio"/> Write	Add, update manage net
License	<input checked="" type="radio"/> Deny	<input type="radio"/> Read	<input type="radio"/> Write	Manage sof This permis Group if se

Role Created Successfully.

Any changes made should take effect immediately.

Cisco-Live-Operator has been created.

What's Next?

[Add Access Group](#)

[Back to Roles Page](#)

[Workflows Home](#)

New in Catalyst Center 3.1.x- Site based RBAC

Create an
Access
Group
(Associated to
Role)



Create Your Access Group

Let's start by naming the access group and we recommend to give a brief description of the group which could be helpful to other administrators. From there you can select the level of access and which site to apply it to.

Name*
TBRANCH-CL-Operator

Description

Role*
Assurance-Only
Cisco-Live-Operator

Scope *

Search Hierarchy

Search Help

- Global
- APAC
- APJC
- Canada
- EMEA
- LBC-Canada-Ontario
- Loblaw - George Weston

- Access Group = Role + Scope

New in Catalyst Center 3.1.x- Site based RBAC

Create an
Access
Group
(Associated to
Role)



Create Your Access Group

Let's start by naming the access group and we recommend to give a brief description of the group which could be helpful to other administrators. From there you can select the level of access and which site to apply it to.

Create Your Access Group

Let's start by naming the access group and we recommend to give a brief description of the group which could be helpful to other administrators. From there you can select the level of access and which site to apply it to.

Name*
TBRANCH-CL-Operator

Description

Role*
Cisco-Live-Operator

Scope *

Search: tbr | X Filter Search Help

- Global
- Canada
 - Ontario
 - Toronto
 - TBRANCH
 - TBRANCH-NORTH-YORK**
 - TBRANCH-SCARBOROUGH

- Access Group = Role + Scope
- A scope is a SINGLE site, but includes children

New in Catalyst Center 3.1.x- Site based RBAC

Create an
Access
Group
(Associated to
Role)



Create Your Access Group

Let's start by naming the access group and we recommend to give a brief description of the group which could be helpful to other administrators. From there you can select the level of access and which site to

Create Your Access Group

Let's start by naming the access group and we recommend to give a brief description of the group which could be helpful to other administrators. From there you can select the level of access and which site to apply it to.

Name*
TBRANCH-CL-Operator

Description

Scope *

Search tbrl X Filter Search Help

- Global
- Canada
 - Ontario
 - Toronto
 - TBRANCH
 - TBRANCH-NORTH-YORK**
 - TBRANCH-SCARBOROUGH

Done! Access Group created Successfully.

Any changes made should take effect immediately.

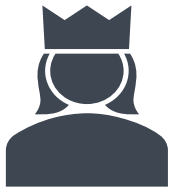
What's Next?

Add Users

[Back to Access Group](#)

New in Catalyst Center 3.1.x- Site based RBAC

Add user &
assign
Access
Group



User Management

Catalyst Center uses Users, Roles and Access Groups

Search Table

Filter Edit

Username	First Name
ciscotac	Cisco
crwickha	Craig
demouser	
donnyo	Don

Update Internal User

First Name
Lila

Last Name
Rousseaux

Email
lroussea@cisco.com

Username
lila

Access Group*

- SUPER-ADMIN_GLOBAL x
- Tbranch-Assurance x
- TBRANCH-CL-Operator x

A user can have multiple Access Groups: user selects the access-group, No logout/login required. Context change

Internal and external users are supported. For SBRBAC the access-group needs to be configured in your AAA server

Example: Cisco-avpair=ags=TBRANCH-Operator

- Design >
- Policy >
- Provision >**
- Assurance >
- Workflows
- Energy Management
- Tools >
- Platform >
- Activities >
- Reports
- System >
- Explore

Software Image Management

TBRANCH

All Devices

Cisco.com ID lroussea@cisco.com (Change) Sync Updates

- Overview**
- Images
- Devices
- Updates

Updated 5 minutes ago Refresh

Images

Cisco recommends assigning standard images to product families.

Device families without standard 2 ⚠️	Critical advisories 13 ❌
High advisories 160 ⚠️	

Updates

Failed Updates 2 ❌	In Progress Updates 0 ℹ️
Successful Updates 22 ℹ️	

Devices

No standard image tagged 2 ⚠️	Ready for update 2 ⚠️
Update readiness failed 0 ❌	Failed image updates 1 ❌

Image Update Tools

- Schedule Image Update
- Check Image Update Status
- Download Update Readiness Report

What habit will you be embracing?



Deploy at Scale



Stay Compliant



Keep your software current



Assure with insight



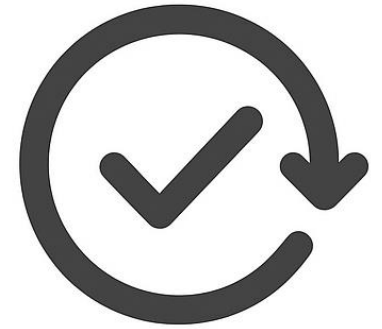
Transform with AIOps



Integrate to Innovate



Maintain Platform Current



Complete your session surveys



Complete your surveys in the Cisco Events App.



Complete a minimum of 4 session surveys and the overall event survey to receive a unique Cisco Live t-shirt.
(from 11:30 on Thursday, while supplies last)

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer meeting

Visit the Technical Solutions Clinics to discuss your technical questions



Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at CiscoLive.com/On-Demand

Contact me at: BRKOPS-2416 Webex Space

Thank you

CISCO Live !

