



Cisco Catalyst Center 2.3.7 Release Overview

September 2024

Contents

AIOps: AI-driven insights	2
Event analytics.....	2
Over the Air Sniffer.....	3
AP power savings insights	4
Per-SSID filtering.....	5
Wireless client latency insights.....	5
Day 0 automation enhancements	6
NetOps with Catalyst Center Automation	6
Configuration visibility and control	7
Campus automation	8
Third-party device support	9
New devices.....	9
LAN automation enhancements	10
Cisco Identity Services Engine (ISE) Visibility.....	10
Enhanced endpoint visibility	10
SecOps: Zero-trust workplace	10
New APIs.....	11
DevOps: Innovation and integrations	11

AIOps: AI-driven insights

Event analytics

Network devices can generate a huge number of events related to the network infrastructure and the users on the network. Because of the amount of data, it can be challenging for network administrators to correlate all the events to understand which ones are relevant.

Cisco® Catalyst® Center’s Event Analytics uses AI to provide network administrators insights into the events that are the most relevant for them. For both wired and wireless devices, it shows:

- When are events happening the most
- What are the highest priority events
- Which event types are most and least common

Catalyst Center uses event correlation to show the network administrator which sites, devices, and users are impacted by an event so that administrators can triage them quickly and resolve issues faster.

With Event Analytics, event data retention for events is increased to 60 days, giving the users greater visibility. Cloud connectivity is required for Event Analytics.

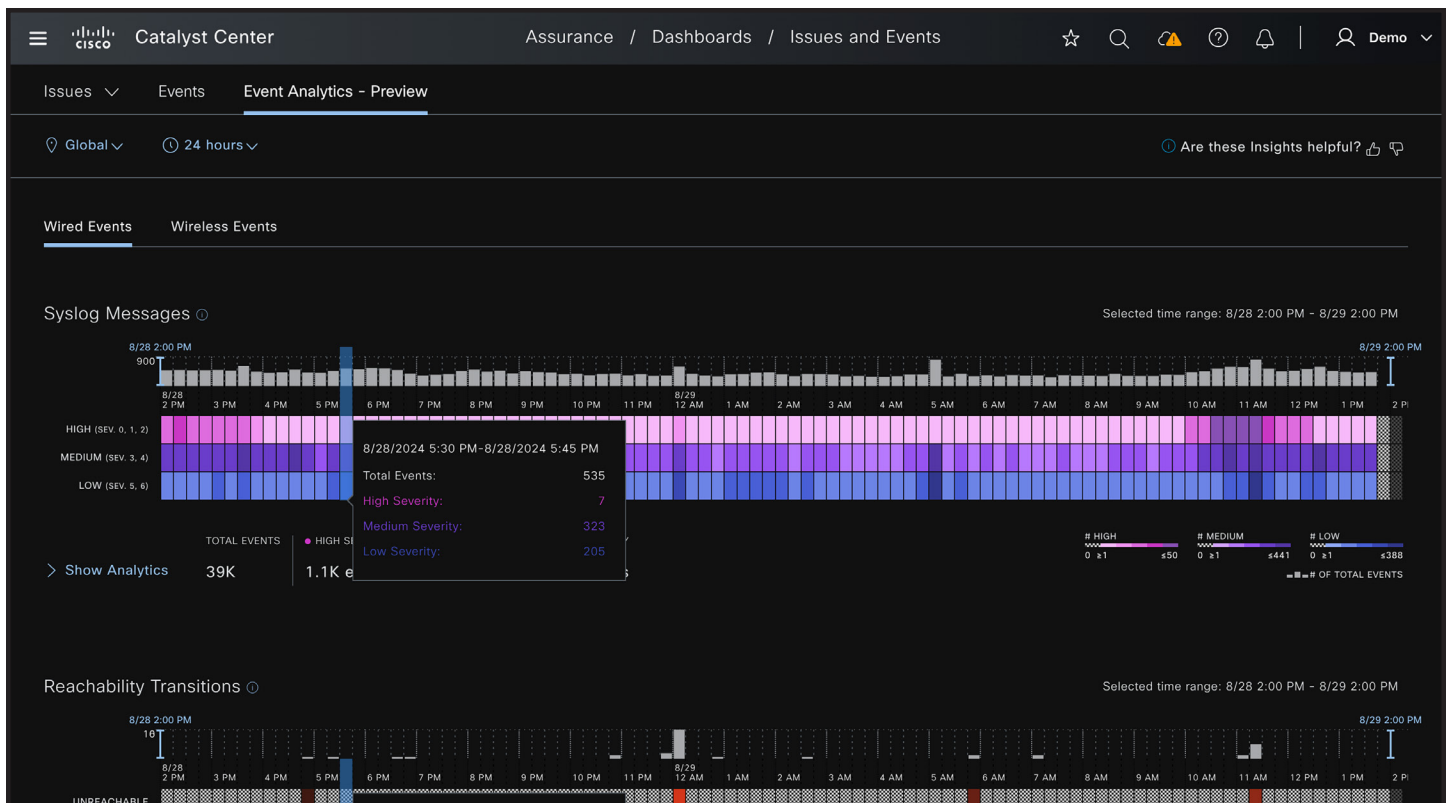


Figure 1. Event analytics

Over the Air Sniffer

Troubleshooting wireless problems can be challenging and time-consuming. Catalyst Center’s Over the Air Sniffer makes troubleshooting wireless issues easier and removes the complexity of data collection.

The Over the Air Sniffer expands on Catalyst Center’s Intelligent Capture by listening to more than just the packets between a single client and access point. It can listen to all the packets for a radio on up to two access points at a time, on any band.

Using a floor map view, the network administrator can easily select which neighboring radios to use based on

the radio, Received Signal Strength Indicator (RSSI), and client count.

Use cases include:

- Troubleshoot channel-wide wireless client problems such as poor performance and connectivity issues
- Analyze wireless traffic to improve the network’s performance and security
- Identify threats from rogue access points

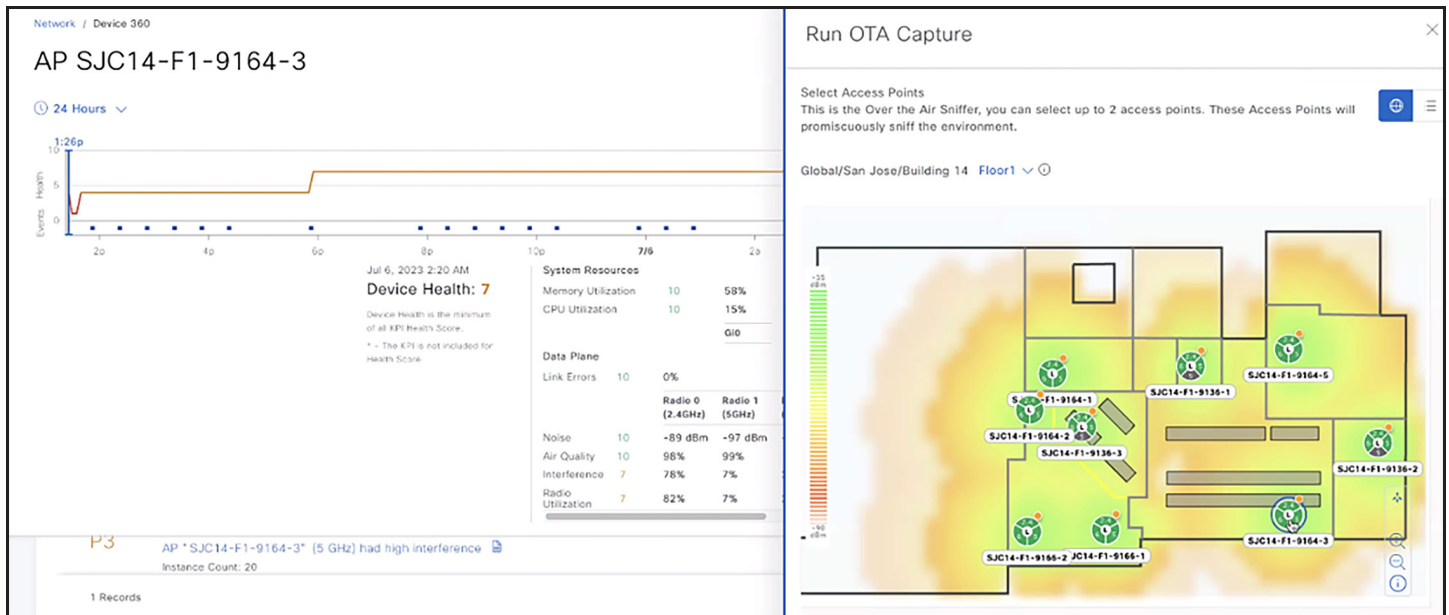


Figure 2. Over the Air Sniffer

AP power savings insights

For IT organizations to reach sustainability goals, they need to find ways to reduce power consumption and report on the impact of their initiatives.

Catalyst Center enables customers to configure AP power profiles on their Wireless LAN Controllers (WLCs). With AP Power Save Mode, the access points can use 20 percent less power during off-peak times by shutting off radios, lowering spatial streams and port speeds, and disabling USB ports when there

are no users. The network administrator can set up calendar profiles, which define off-peak times.

Now, Catalyst Center is giving insights into the power saved by AP power profiles. The network administrator can now see power saved when the mode is enabled and get insights into what devices haven't yet configured. This makes it easy to identify devices using more power than they need and take action.

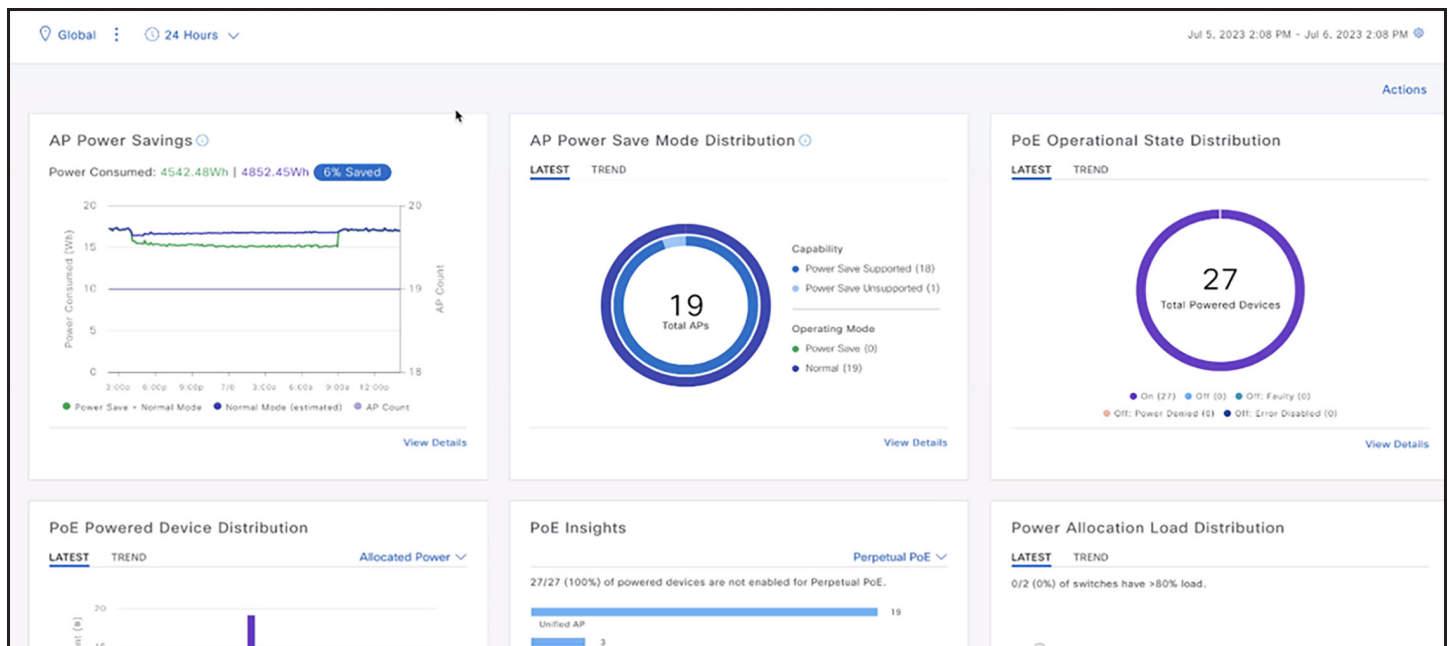


Figure 3. AP power savings insights

Per-SSID filtering

Commonly, IT organizations deploy multiple SSIDs, to support different operational needs. With large wireless networks, being able to filter out the noise and focus on business-critical networks when monitoring and troubleshooting is paramount.

Catalyst Center enables customers to filter out data for the SSIDs they want to exclude, enabling them to focus on the wireless networks that are most critical, and reduce problem resolution times.

Wireless client latency insights

Optimizing today's wireless network with different device types running critical applications across different access points can be tricky. But it's important for wireless network administrators to identify what can cause client latency.

Catalyst Center's Wi-Fi 6 Dashboard now includes client latency breakdowns by location, access point, and band. This makes it easy to know where there are problems, what's the impact, and how to address them.

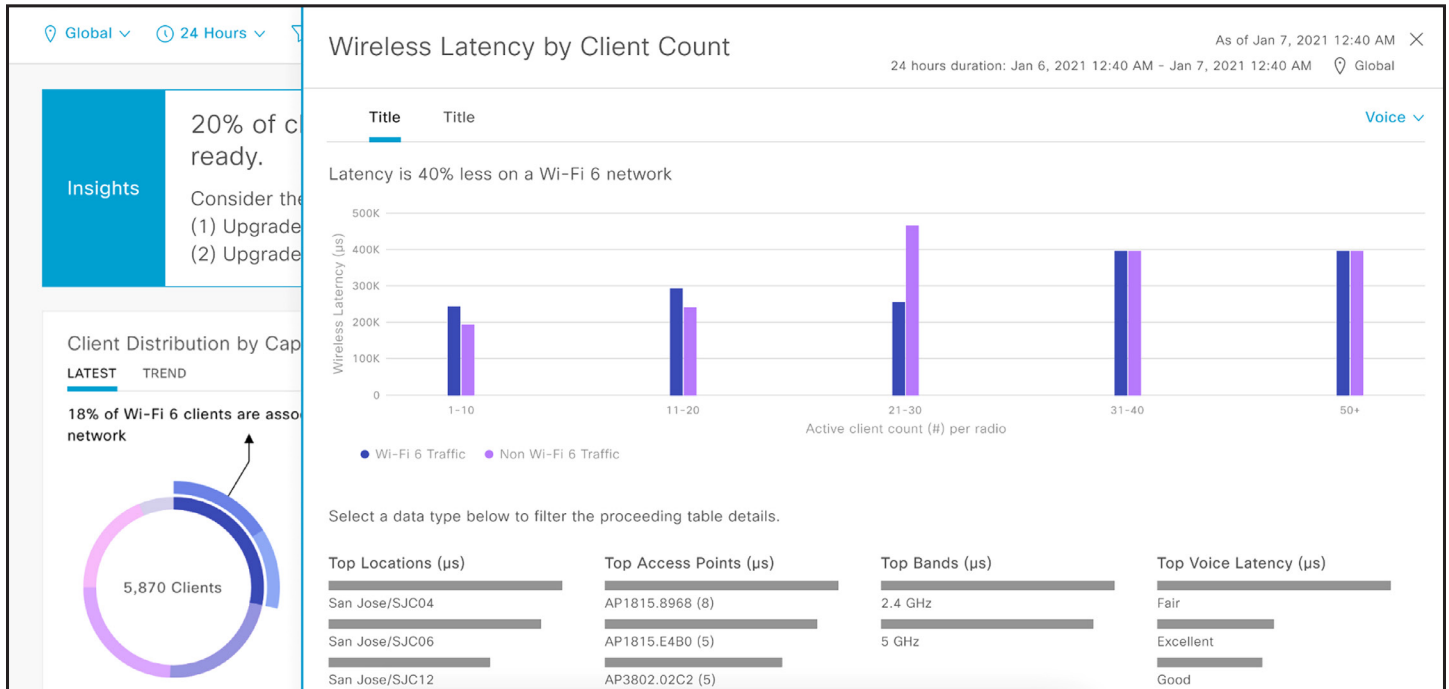


Figure 4. Wireless client latency insights

NetOps with Catalyst Center Automation

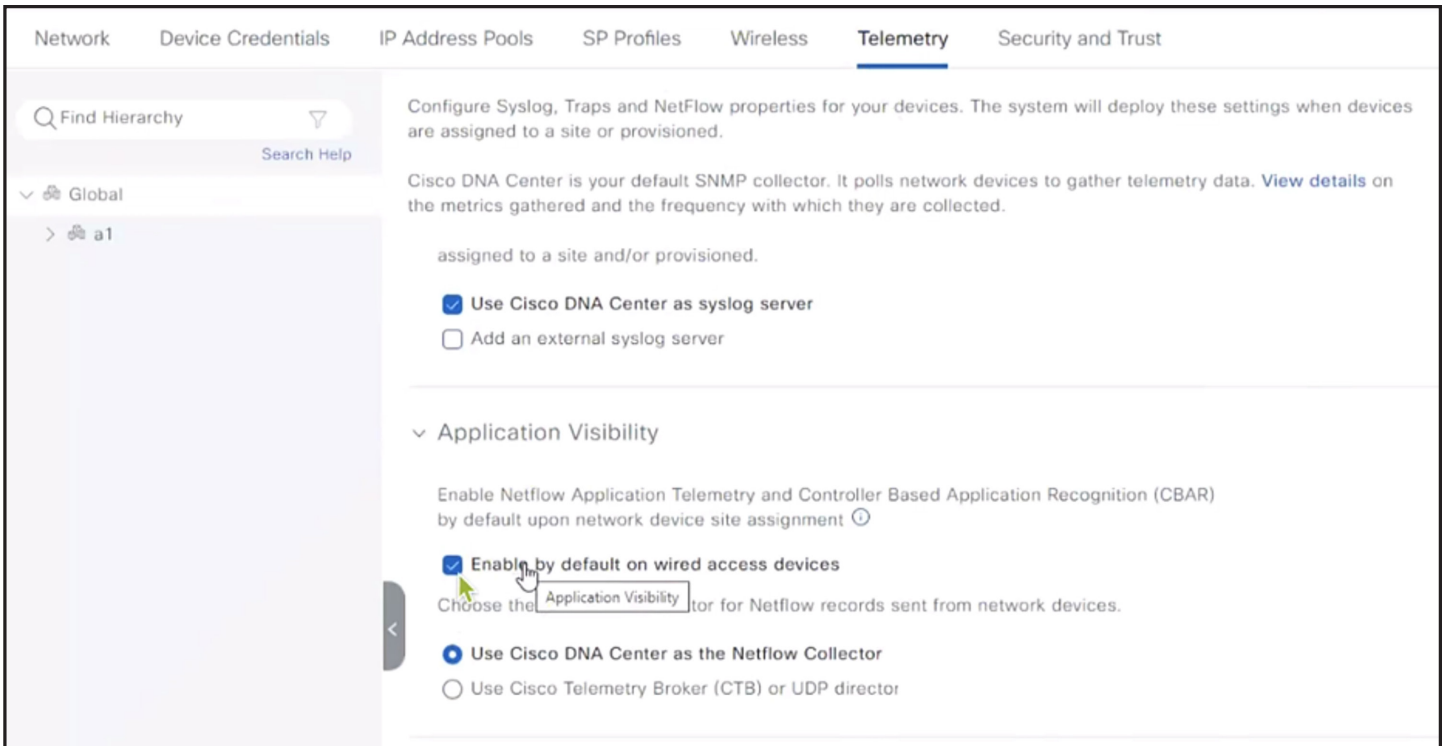
Day 0 automation enhancements

Using automation at deployment time can increase efficiency and help to ensure that new devices are configured correctly. Catalyst Center 2.3.7 introduces several new capabilities that make it easier to automate Day 0 device configuration. New settings include:

- Application Visibility and Control (AVC) - Automatically configure AVC on wired devices, and easily get application health and visibility in Catalyst Center.

- NETCONF - Automatically configure NETCONF on the devices. The configuration settings can be added to the Day 0 template and are applied when new devices are added to a site.
- QoS - Automatically deploy QoS policies on new devices to ensure optimal network performance.

Additionally, Catalyst Center now supports Plug and Play with Cisco Catalyst 9800 Series Wireless LAN Controllers.



The screenshot displays the Catalyst Center configuration interface for Telemetry. The top navigation bar includes tabs for Network, Device Credentials, IP Address Pools, SP Profiles, Wireless, Telemetry (selected), and Security and Trust. A search bar labeled 'Find Hierarchy' is present on the left. The main content area is titled 'Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned.' Below this, it states 'Cisco DNA Center is your default SNMP collector. It polls network devices to gather telemetry data. View details on the metrics gathered and the frequency with which they are collected.' There are two radio button options: 'Use Cisco DNA Center as syslog server' (checked) and 'Add an external syslog server'. A section titled 'Application Visibility' is expanded, showing the text 'Enable Netflow Application Telemetry and Controller Based Application Recognition (CBAR) by default upon network device site assignment'. It includes a checked checkbox for 'Enable by default on wired access devices' with a tooltip 'Application Visibility' pointing to it. Below this, it says 'Choose the Application Visibility collector for Netflow records sent from network devices.' and offers two radio button options: 'Use Cisco DNA Center as the Netflow Collector' (selected) and 'Use Cisco Telemetry Broker (CTB) or UDP director'.

Figure 5. Day 0 automation

Configuration visibility and control

It has been shown that 80% of network outages are result of a change. Ensuring that changes are successful is key to any IT network operations. Catalyst Center is reducing the risk in configuration changes by offering enhanced visibility. The network administrator can see exactly what lines of the configuration will be changed on all the devices that are being updated.

And there's improved control over the configuration process. For customers using ServiceNow IT Service Management (ITSM) integration, configuration tasks can be a part of the ServiceNow change management workflows, ensuring that standardized methods are used to handle changes, thus improving compliance, and reducing mistakes.

Preview Configuration

Select a device to start generating the configuration for preview. You can choose to stay on this screen, or preview and approve the activity later in the Activities page. Clicking "Submit for Approval" will submit the configurations for all devices.

Group By: Platforms ⌵ ⓘ

Search by name or IP

TARGET DEVICES

- ⌵ C9200L-24P-4G
 - device1.cisco.com ✔
 - device2.cisco.com ✘
- ⌵ C9300-24P
 - device3.cisco.com
- ⌵ WS-C3650-24PD
 - device4.cisco.com

IP Address: 10.62.8.71 Site: Global/Bangalore/Cessna/BGL12/Floor1

⚠ Some insights that app wants to highlight ✕

Config Sourced From: All ⌵ ⚙️ Hide line numbers | 🔍 Search

```

cts role-based enforcement
banner motd ^CWelcome to DNA-C TME Lab!!^C
!
line con 0
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  authorization exec VTY_author
  login xxxxxx
  transport input all
line vty 5 97
  authorization exec VTY_author
  login xxxxxx
  transport input all
!
ntp server 72.163.32.44
!
wsma agent exec
  profile httplistener
  profile httpslistener
!
wsma agent config
  profile httplistener
  profile httpslistener

wsma agent filesys
  profile httplistener
  profile httpslistener
                    
```

Preview Configuration Later
Discard
Submit for Approval

Figure 6. Configuration visibility

Campus automation

Catalyst Center is simplifying brownfield management, giving customers better visibility into their networks and improved operational simplicity. Campus Automation can:

- Discover brownfield wired and wireless network devices and add them to the inventory.
- Automatically learn device configurations. Network administrators can see the configurations without any changes being made to the network.
- Simplify network automation tasks such as updating multiple port configurations, updating Layer 2 configurations like VLANs, or Spanning Tree Protocol (STP).

Campus Automation is a beta feature in 2.3.7.

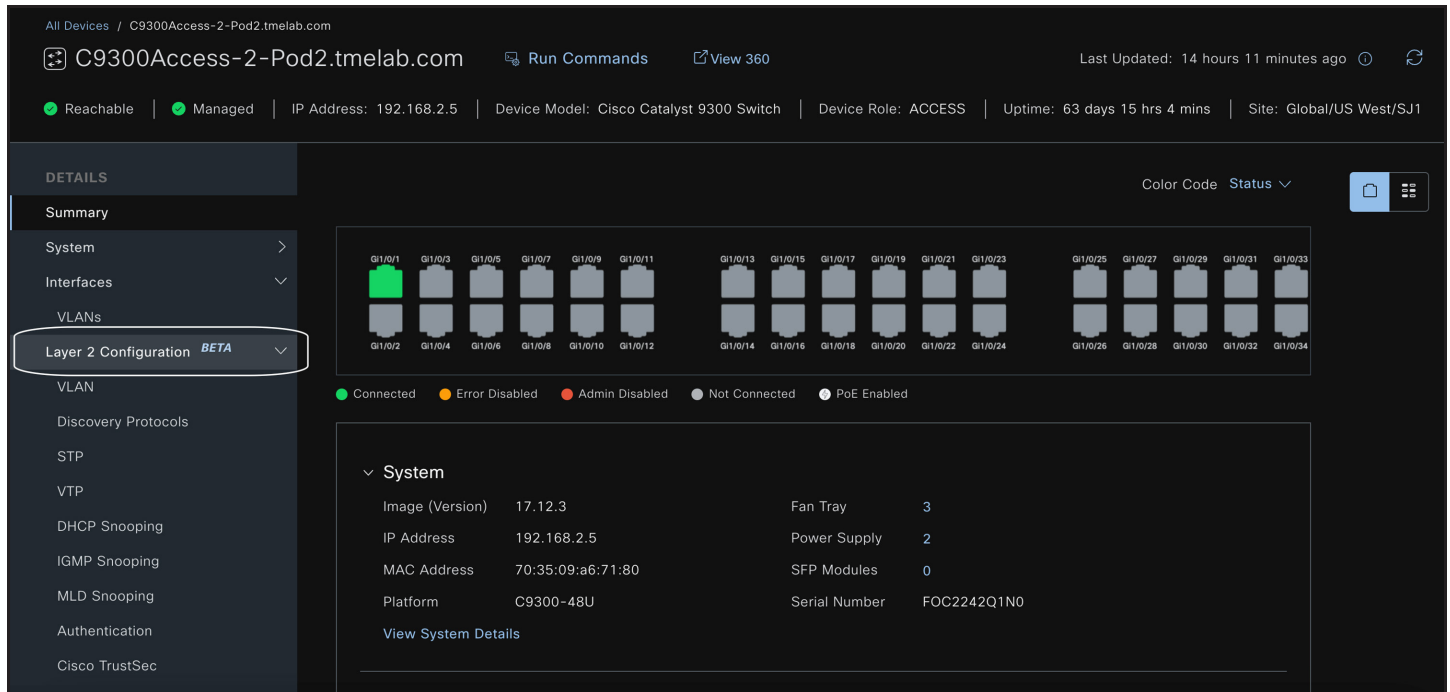


Figure 7. Campus automation

Third-party device support

It's common for IT organizations to deploy devices and systems from multiple vendors. But doing so can add complexity and make management difficult.

Catalyst Center customers often have third-party devices and firewalls and would like visibility of those along with their Cisco gear. Now, administrators can add any devices that support the SNMP MIB-II standard into Catalyst Center. This gives them visibility into the devices' reachability and inventory information, as well as topology.

Third-party device support helps customers reduce complexity and get improved visibility over their entire network.

New devices

This version adds support for additional models in these families:

- Cisco Catalyst IE3100 Rugged Series Switches
- Cisco ESR6300 Embedded Series Router
- Cisco Catalyst IE9300 Rugged Series Switch
- Cisco Catalyst ESS 9300 Embedded Switch
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9500 Series Switches
- Cisco Catalyst 9166 Series Access Points
- Rockwell Stratix 5400 Industrial Ethernet Switches



SecOps: Zero-trust workplace

LAN automation enhancements

Catalyst Center is adding the following improvements to LAN Automation:

- LAN Automation can accommodate IP address pools as small as /28, to avoid wasting IP addresses in networks with fewer endpoints.
- When the network administrator maps device serial numbers to hostnames, they can now also manually configure the loopback addresses, giving them additional control over the network design.

Cisco Identity Services Engine (ISE) Visibility

Network administrators can add ISE instances to Catalyst Center, giving them visibility into reachability of those systems and quickly identify if there are outages.

Enhanced endpoint visibility

Cisco Endpoint Analytics (EA) helps organizations to gain visibility into their endpoints and identify potential security threats. Catalyst Center is making it easier for network administrators to get insights into their endpoints and their threat levels. The new capabilities include:

- Dashlet on the Catalyst Center home page that includes EA data and workflows to the EA dashboard.
- EA insights on the Client 360 page, so that network administrators can easily see the Trust Score and get improved profiling insights.



DevOps: Innovation and integrations

New APIs

Catalyst Center 2.3.7 makes integrations easier than ever, adding more than 200 new APIs, including new ones in these areas:

- Compliance
- Configuration Archive
- Device Onboarding (PnP)
- Devices
- Event Management
- LAN Automation
- New Assurance Events
- Sites
- System Settings
- User and Roles