

Cisco DNA Center Release 2.3.5 Overview

May 2023



AIOps: AI-driven insights

DNS service dashboard

Today, users expect a consistently seamless experience whether they're plugged in or connected wirelessly. When they experience problems, it's common for them to blame the network connection.

But it's not always a connectivity problem – a lot of network components, including DNS, need to work well for users to get the results they expect.

Cisco DNA Center's DNS dashboard helps network administrators quickly isolate and identify the root causes when there are DNS problems. Just like the existing dashboards for DHCP and AAA, the DNS

dashboard gives the network administrator deep insights into DNS health, including:

- Performance
- Latency
- Failures
- Causes of failures

This gives network administrators the ability to easily identify and resolve problems that in the past were extremely difficult to troubleshoot.

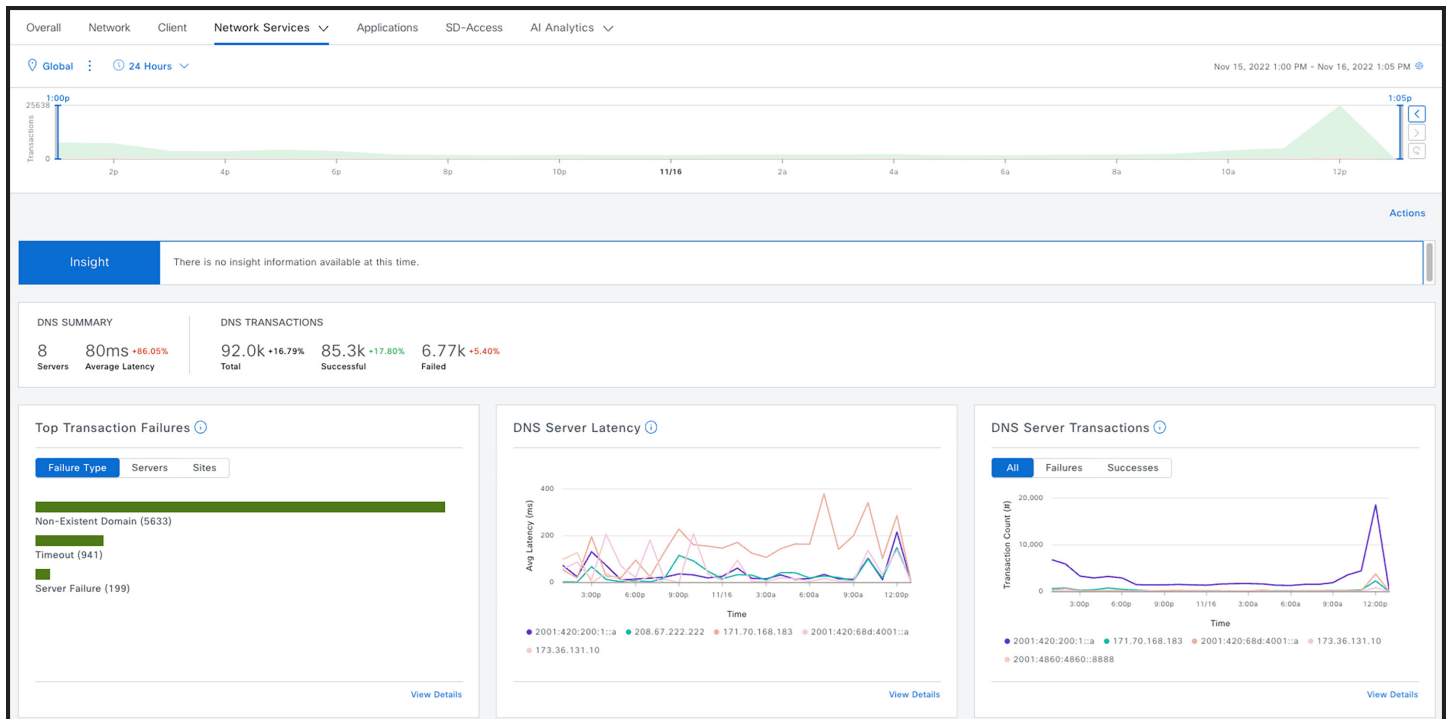


Figure 1. DNS service health

Wireless client 360 enhancements

Cisco DNA Center continues to simplify the process to identify and troubleshoot individual client issues. The network administrator can now easily identify what the problem is, when it occurred, why it occurred and how widespread the impact is.

What: The network administrator can quickly get insights into what the problem is that a client experienced. The summary includes onboarding, roaming, and connectivity experience.

When: Using the health trendline, the network administrator can identify when the problem occurred and correlate it with configuration changes.

Why: The client 360 page now gives visibility into why; that is, what events and KPIs contributed to the problem.

How impactful: The network administrator can easily see whether a problem is isolated to a single user or is affecting more users.

All of this makes IT more efficient in operating the network, and it helps users have a better experience.

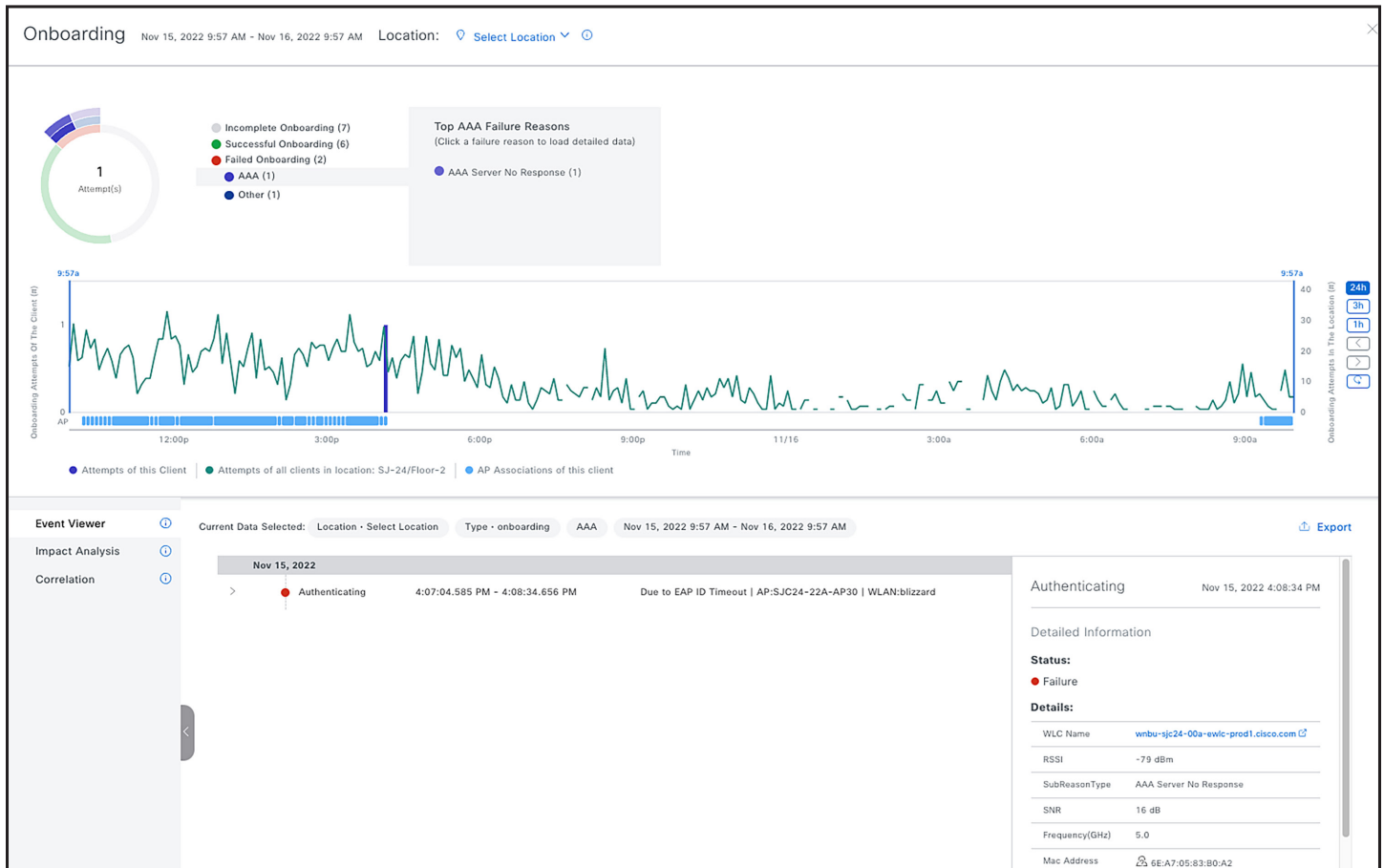


Figure 2. Client 360 onboarding

Wireless troubleshooting

Cisco DNA Center’s Machine Reasoning Engine (MRE) can step through complex troubleshooting processes that traditionally have required domain expertise typically found in senior network engineers. This version is making it easier for a network administrator of any experience level to use the MRE for access point and client log collection.

When the network administrator uses the network reasoner workflow to troubleshoot a wireless client issue, they can select multiple Wireless LAN Controllers (WLCs) to run troubleshooting algorithms on. After the MRE creates its conclusions, the network administrator can easily download logs and packet captures to accelerate their troubleshooting and shorten resolution times.

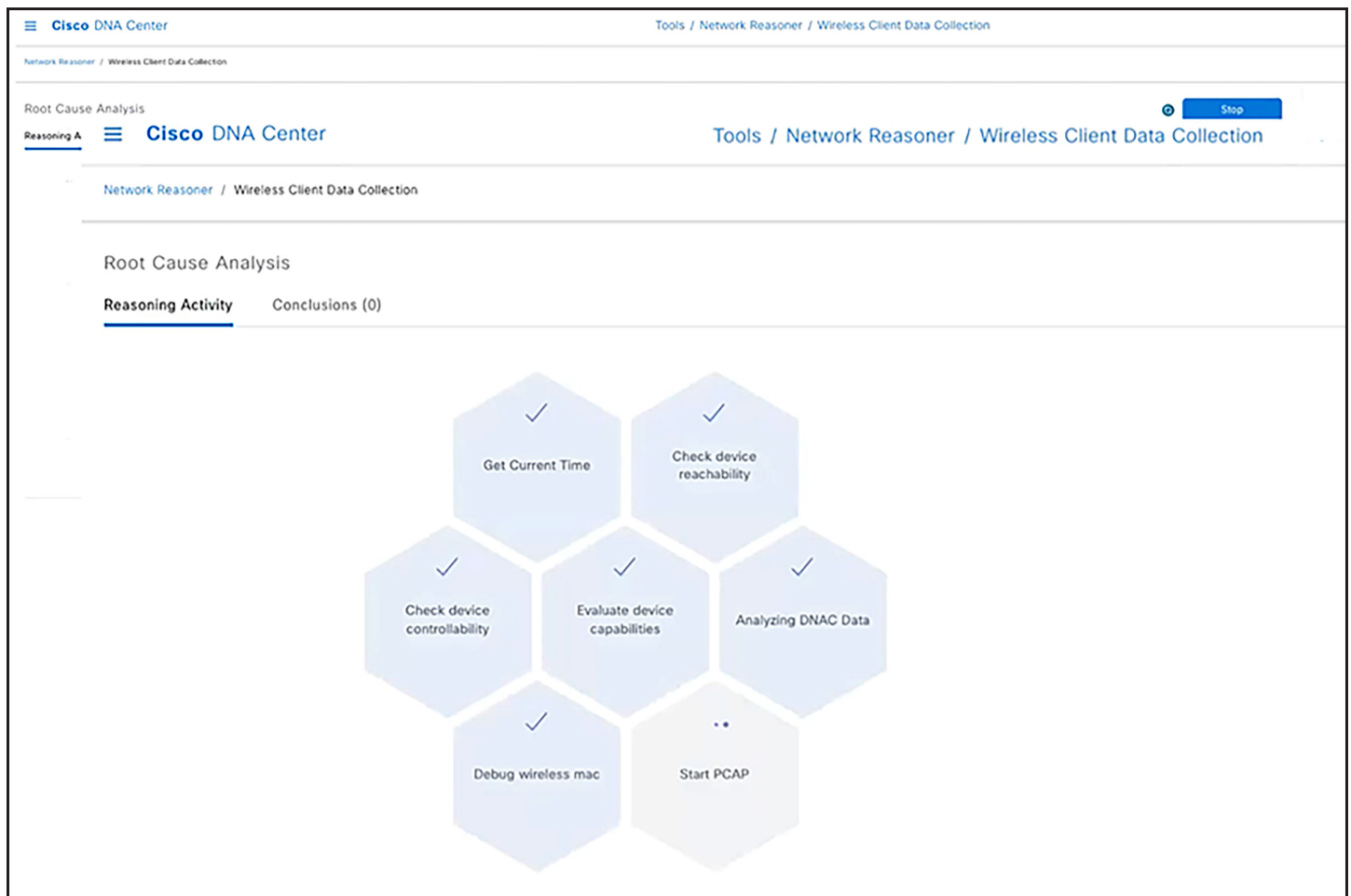


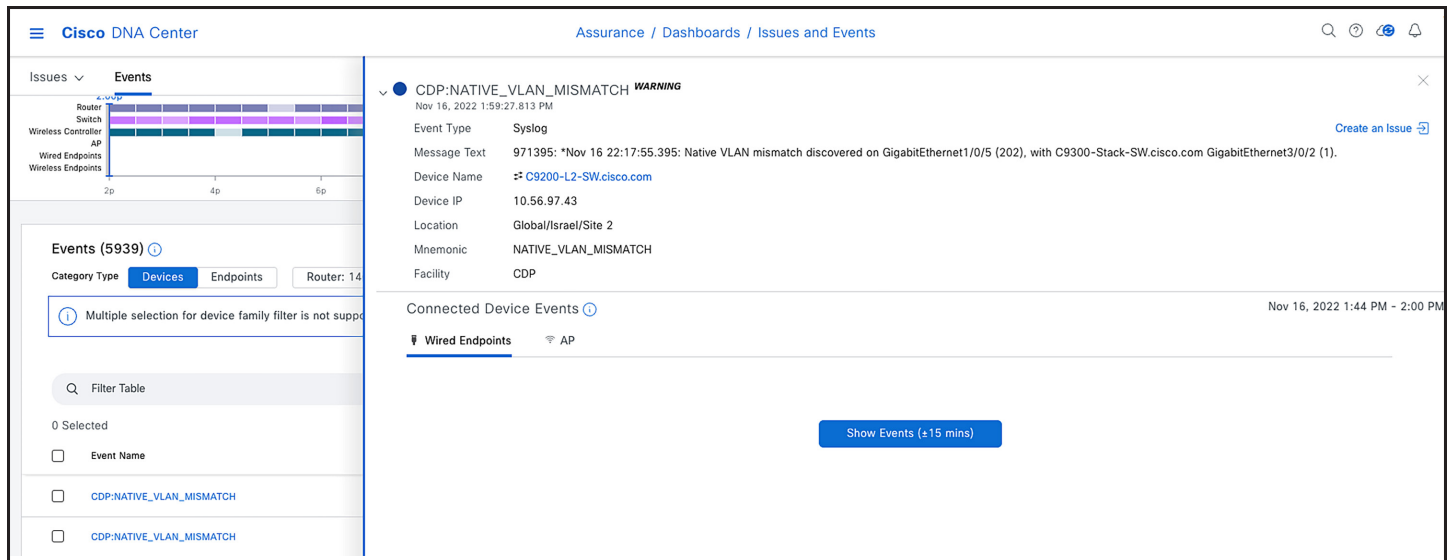
Figure 3. Wireless troubleshooting

User-defined issues

One of the most important capabilities for a network controller is to automatically identify critical problems and proactively notify the appropriate members of the IT team. Cisco DNA Center already offers more than 200 pre-defined issue types that can notify network administrators about problems with network devices, clients, and application health.

Cisco DNA Center is offering more flexibility, allowing network administrators to define their own custom issues for syslog messages.

The network administrator can simply create an issue type that searches for user-defined text in incoming syslog messages from the network devices. When matching messages arrive, Cisco DNA Center will raise issues of the right priority and optionally send out notifications. This makes it easier than ever for IT teams to proactively address problems before user experience is negatively impacted.



The screenshot displays the Cisco DNA Center interface for managing issues and events. The main view shows a list of events, with one event selected: **CDP:NATIVE_VLAN_MISMATCH** (WARNING). The event details include:

- Event Type: Syslog
- Message Text: 971395: *Nov 16 22:17:55.395: Native VLAN mismatch discovered on GigabitEthernet1/0/5 (202), with C9300-Stack-SW.cisco.com GigabitEthernet3/0/2 (1).
- Device Name: C9200-L2-SW.cisco.com
- Device IP: 10.56.97.43
- Location: Global/Israel/Site 2
- Mnemonic: NATIVE_VLAN_MISMATCH
- Facility: CDP

The interface also shows a filter table for the event name, with two entries for **CDP:NATIVE_VLAN_MISMATCH**. A button labeled **Show Events (±15 mins)** is visible at the bottom right of the event details panel.

Figure 4. User-defined issues

Site analytics

Users expect the network and critical applications to work well wherever they are. As networks and applications scale, this poses challenges for IT organizations that need to deliver consistent and reliable performance across multiple sites and domains.

Cisco DNA Center Site Analytics helps IT teams proactively identify underlying issues that can have a site-wide impact on user experience.

Site Analytics gives the network administrator a single view of customizable KPIs to help them understand the health of devices, users, and applications. They can use the trendline view to narrow down when a KPI violation occurred. The heatmap view gives insights into how many KPIs have been violated. The network administrator can easily drill down to the site level to get a deeper understanding of the impact and do root cause analysis, reducing mean time to resolution.

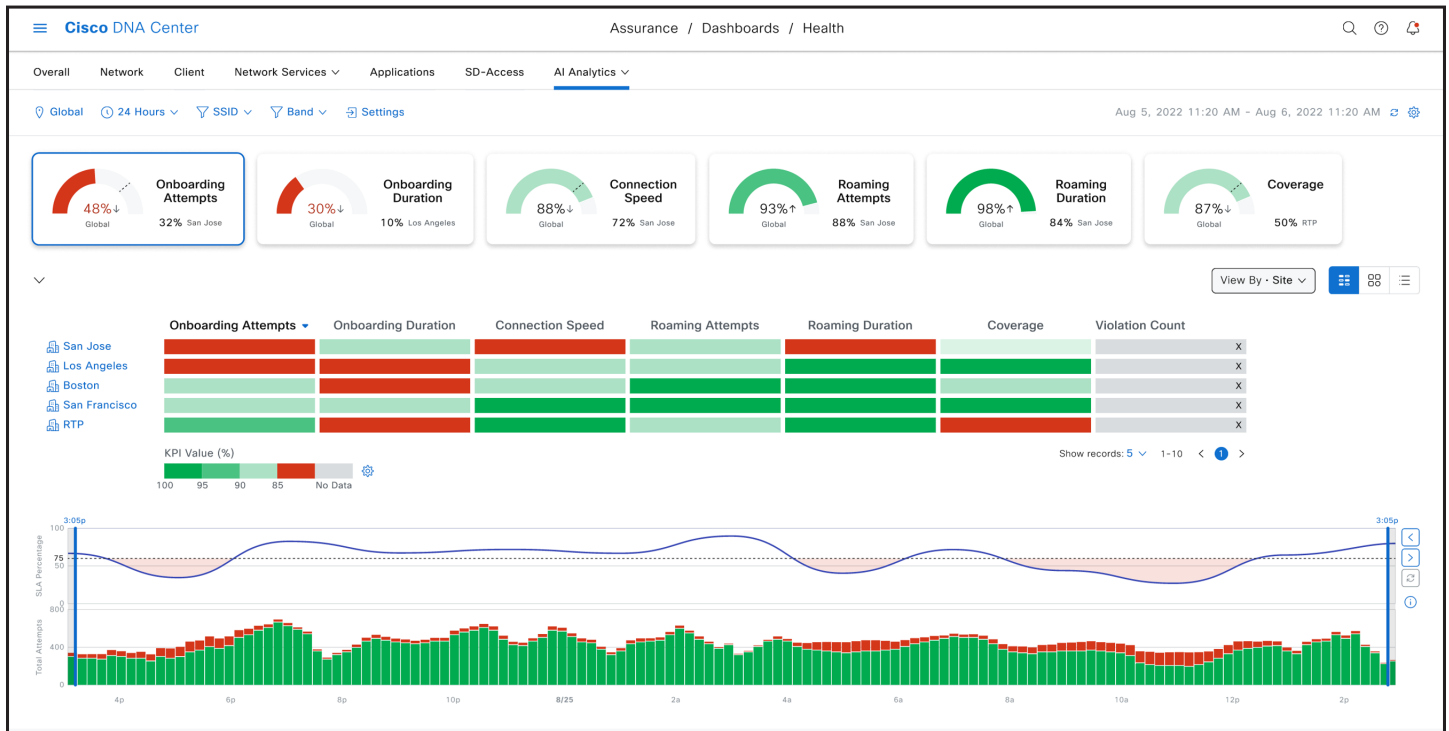


Figure 5. Site analytics

Microsoft Teams 360

The shift to remote work has made team collaboration tools more critical than ever. For IT teams, this means that troubleshooting user issues with these tools is extremely important.

Customers who support Microsoft Teams will have access to a comprehensive view of Microsoft Teams

performance insights, including aggregated data and details on a per-user and per-call basis. This data, coupled with Cisco DNA Center’s client data, helps customers quickly identify and resolve issues, and enables them to deliver a better quality of service to their users.

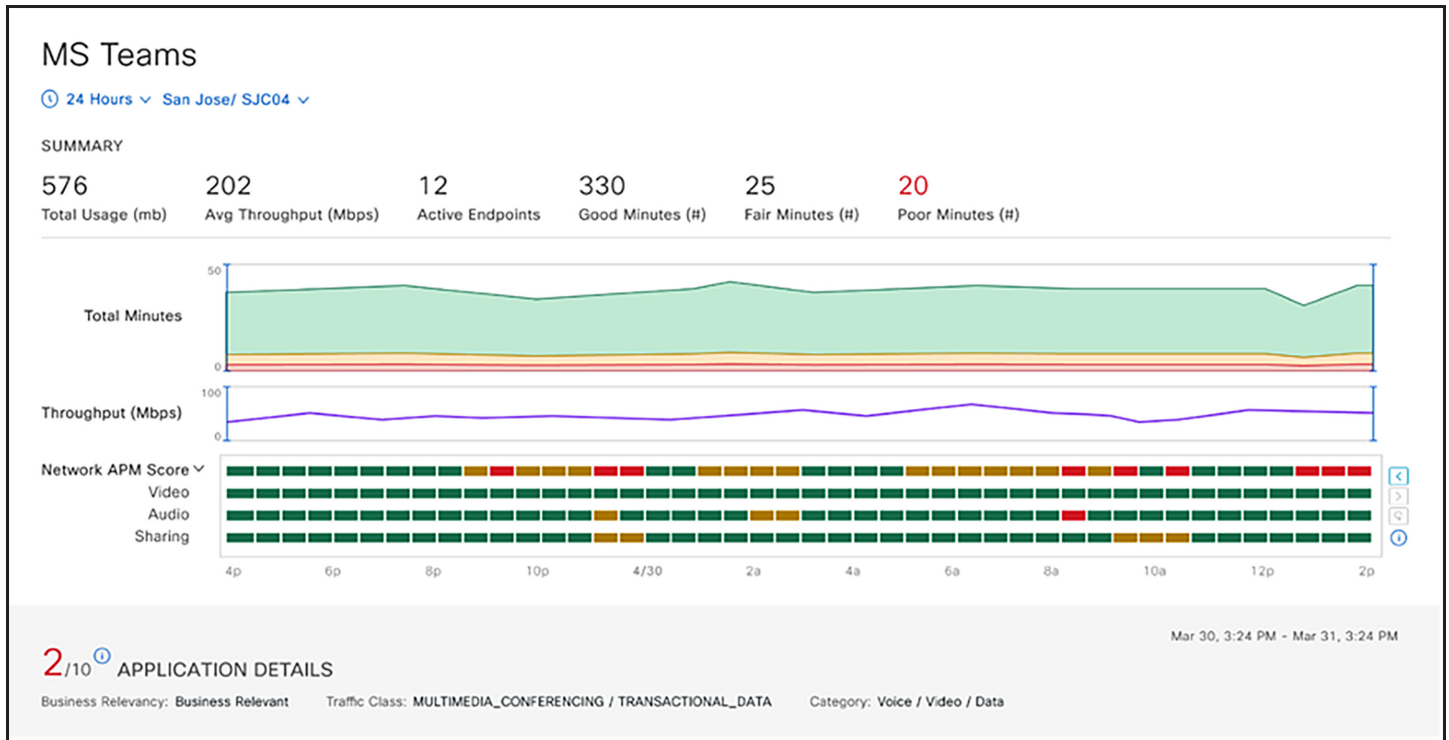


Figure 6. Microsoft Teams 360

Flexible reports

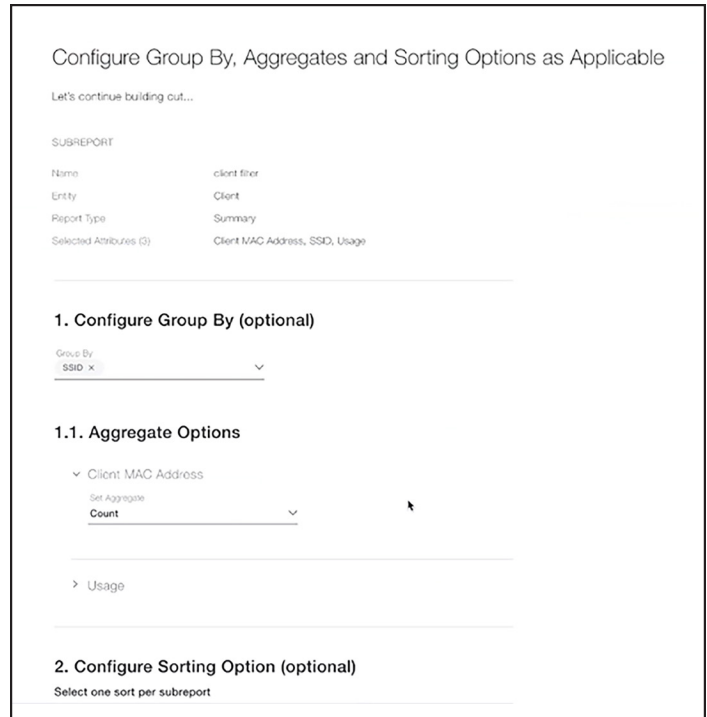
To make informed decisions, IT executives need to be able to extract data from different areas and correlate different data sets. Additionally, they need the agility to generate new types of reports on the fly. Users of Cisco DNA Center have the flexibility to define their own custom report types.

With this flexible reporting capability, a user can create custom reports based on their needs. A flexible report can include subreports about different entities like clients, network devices, and access points. The network administrator can choose which attributes (for example, IP address and OS version) to include in the report. In addition, they can group, aggregate, filter, and sort the report data.

For example, if a wireless network administrator wants to quantify clients with poor, fair, or good health, they can easily create and run a report on client count, grouped by health score.

Or perhaps a team may want to understand how many 2.4 GHz clients have been connecting to each of their SSIDs. They can do that too, and the report can also give insights into KPIs such as onboarding times and client usage.

Custom reports can be exported in .csv format.



Configure Group By, Aggregates and Sorting Options as Applicable

Let's continue building out...

SUBREPORT

Name	client filter
Entity	Client
Report Type	Summary
Selected Attributes (3)	Client MAC Address, SSID, Usage

1. Configure Group By (optional)

Group By
SSID x

1.1. Aggregate Options

Client MAC Address

Set Aggregate
Count

Usage

2. Configure Sorting Option (optional)

Select one sort per subreport

Figure 7. Flexible reports

AI-enhanced radio resource management for Wi-Fi 6e

Customers with Wi-Fi 6e access points can ensure optimum performance of Wi-Fi 6e deployments with AI-enhanced Radio Resource Management (RRM). Cisco DNA Center's AI-enhanced RRM delivers deep visibility into the RF landscape and provides actionable insights. Customers can view KPIs including RRM changes, interference, and health.

Power consumption dashlets

As IoT-device deployments grow exponentially, IT organizations are facing greater challenges in managing PoE (power over Ethernet) resources. Cisco DNA Center is making it easier for customers to stay on top of overall power consumption.

Increased duration for wireless client reports

As network operators do network capacity planning, access to more data can help them make better decisions. When the network administrator generates a client session report or client detail report, they can choose to report on a period of up to 180 days.

In addition to insights about power sent to PoE devices, there are now insights into a switch's system power consumption and overall power consumption, so network administrators know whether the switch is nearing its capacity. Aggregate views at the site and global levels help the network administrator stay on top of PoE status across their deployment.

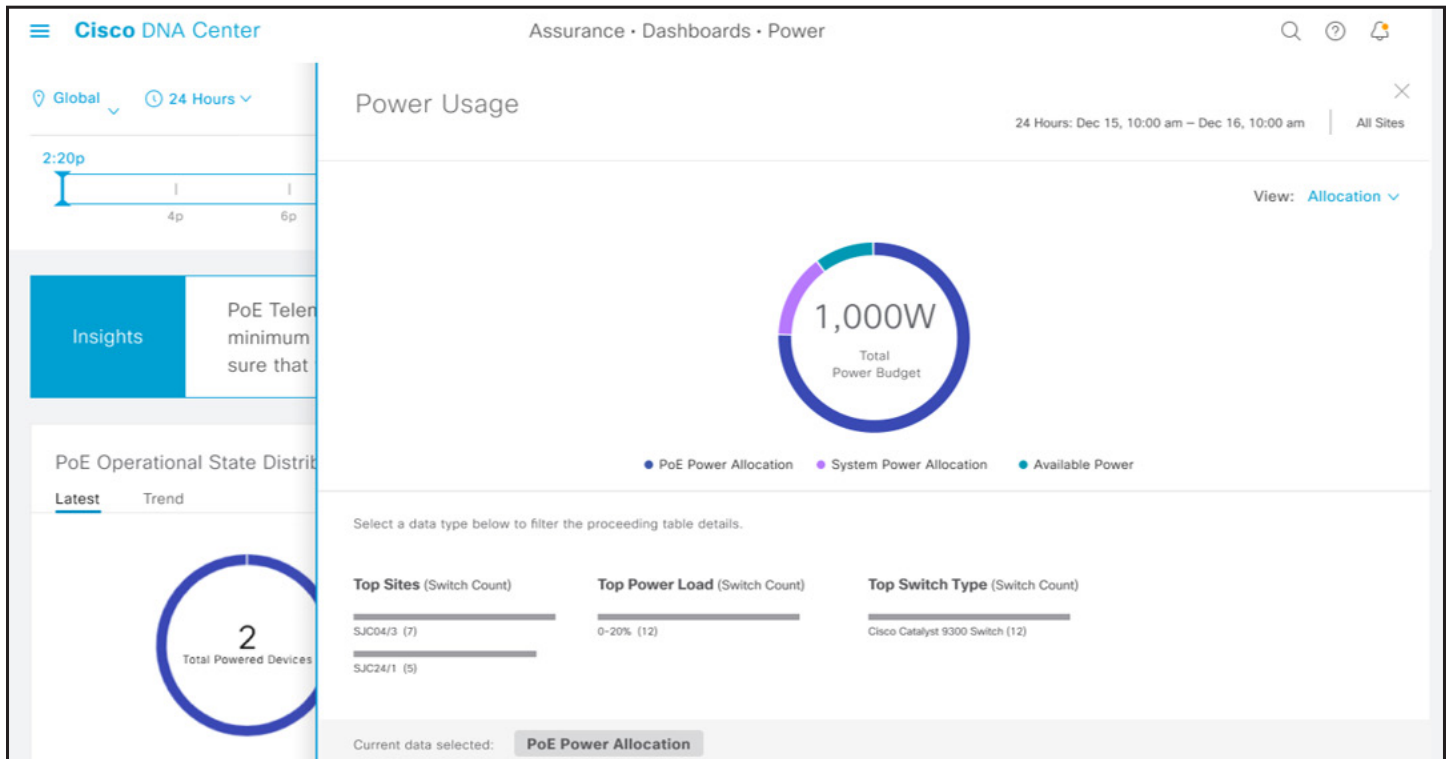


Figure 8. Power consumption dashlets

AP to switch issue correlation

When disruptions occur on the network, IT teams need to focus on the tasks that will have the biggest impact. And when multiple access points are having issues caused by a switch, the biggest impact will come from addressing the switch problem.

When multiple access points are down because their upstream switch is down, Cisco DNA Center will automatically correlate these events into a single issue so the network engineers can easily understand the root cause and the impact, and they can focus on addressing the root issue.

Software image management enhancements

Cisco DNA Center 2.3.5 introduces NETCONF notification support for Software Image Management (SWIM) operations. This provides live updates on the image upgrade process. Network administrators are now able to get status updates about a SWIM operation within seconds and take necessary steps sooner in case of failure.

Automatic issue resolution

For IT teams, management of lots of issues in a fast-changing environment can be particularly challenging. Now when a switch has a power supply failure or a fan failure, and the problem is remediated, the issue in Cisco DNA Center will be automatically resolved, eliminating the need for a network engineer to manually resolve the issue in Cisco DNA Center.

Additionally, as part of SWIM operation Cisco DNA Center can automatically adapt to detect and handle network delays and timeout cases. The system can adjust the timeout window with each retry without any user intervention, driving the image distribution toward probable success.



NetOps with Cisco DNA Center automation

Network settings configuration compliance

Customers have come to rely on Cisco DNA Center to identify devices that are out of compliance for software version, end-of-life, and security advisories. Now, Cisco DNA Center is adding configuration compliance to its array of compliance checks, checking settings such as certificates, IPDT, telemetry, SNMP, AAA, DHCP, and NTP.

Network administrators don't have to wonder whether their network settings are compliant. Cisco DNA Center will identify compliance violations and make it easy for them to act and restore the network devices to a compliant state.

Compliance violation remediation

When devices are out of compliance, the actions that network administrators take depend on the reason for noncompliance. Maybe the startup-config is different from the running-config, or a device has a security advisory or any other type of violation.

With this new release, when a violation happens, it's easier than ever to rectify the situation. Cisco DNA Center identifies what is noncompliant, such as network settings, network profiles, or templates. Then workflows guide the network administrator through the remediation options.

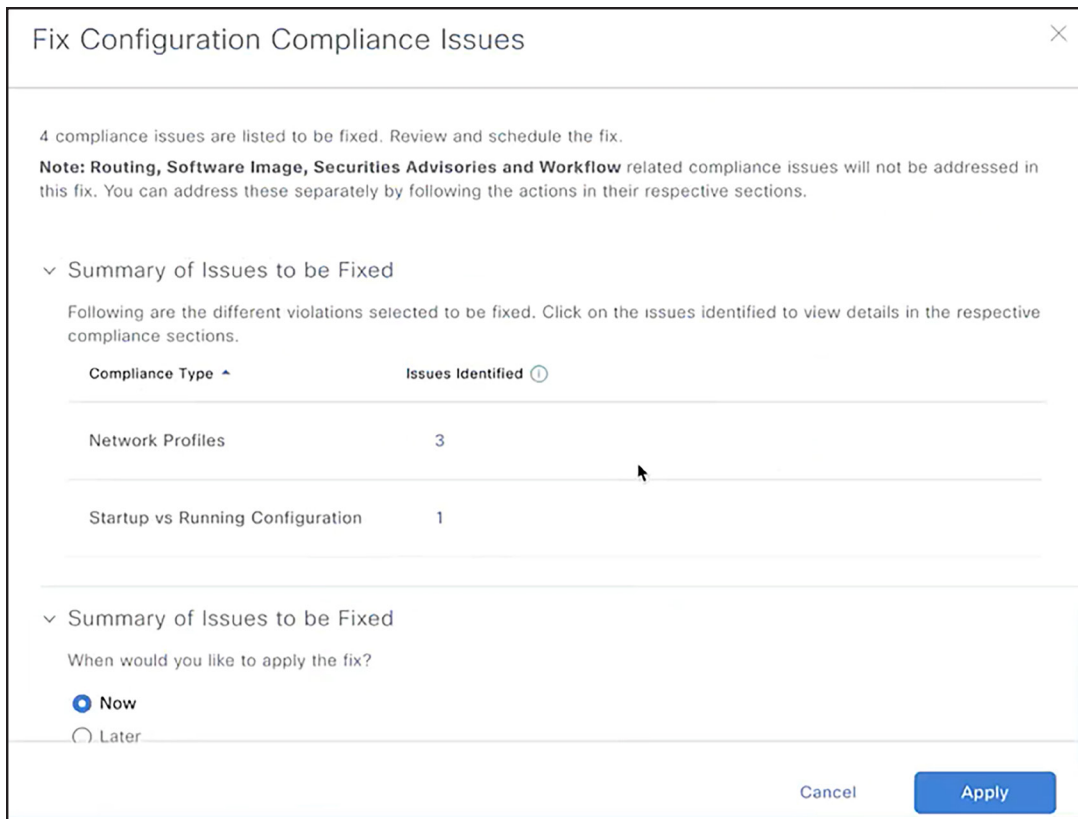


Figure 9. Fix compliance violations

End-of-life compliance

For a network administrator, it is important to identify devices that have either passed or are fast approaching their end-of-life milestones, to plan their refresh. Cisco DNA Center provides end-of-life compliance information for each device, including hardware,

software, and modules, as part of the compliance summary. For each device, the network administrator can see end-of-life compliance status, as well as details about end-of-life milestones.

Compliance acknowledgement

Throughout the device lifecycle, network administrators need to be able to focus on the compliance anomalies that matter most. With this new release they can simply acknowledge the less significant violations, enabling them to tackle the most critical issues.

When compliance checks are performed, those acknowledged attributes are excluded from the overall compliance status calculation. A separate list is maintained for the acknowledged violations for future reviews.

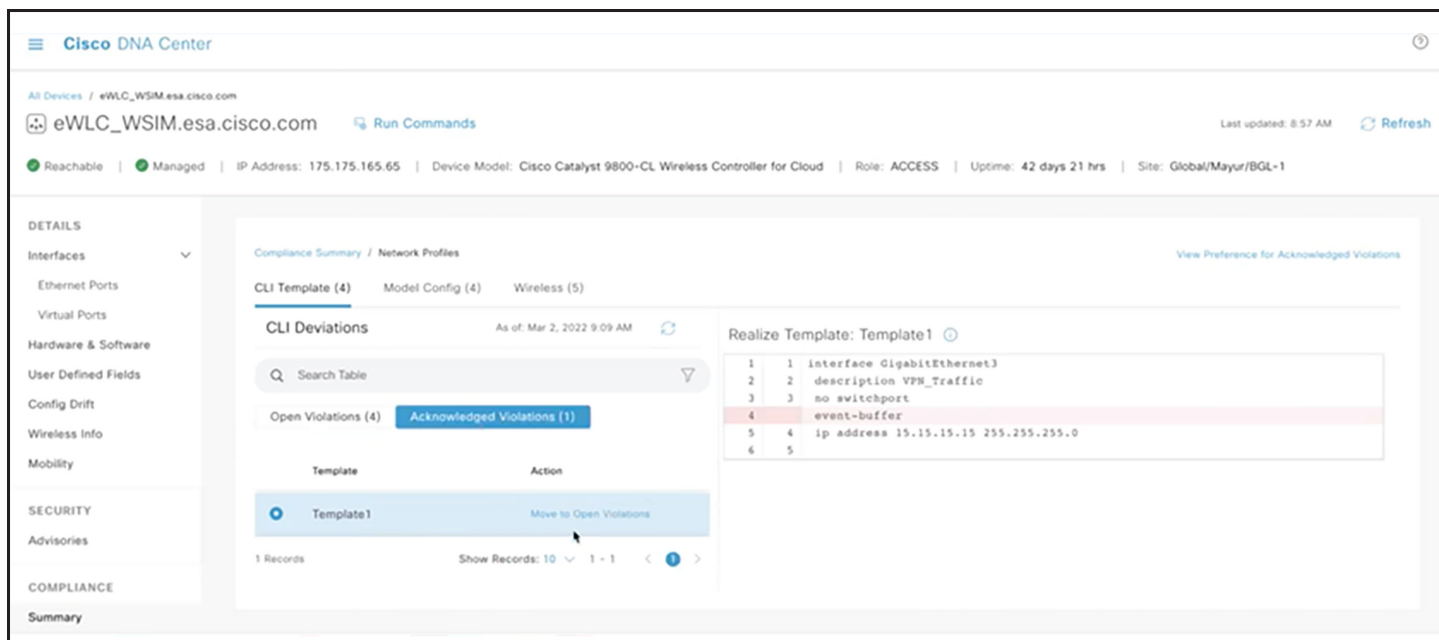


Figure 10. Compliance

AP power profiles

Cisco is committed to sustainability, with a goal of reaching net zero emissions by 2040. And we can only reach our goals by helping our customers reach their sustainability goals.

Cisco DNA Center enables customers to configure AP power profiles on their WLCs. With AP power profiles, the access points can use 20 percent less power during off-peak times by shutting off radios when there are no users.

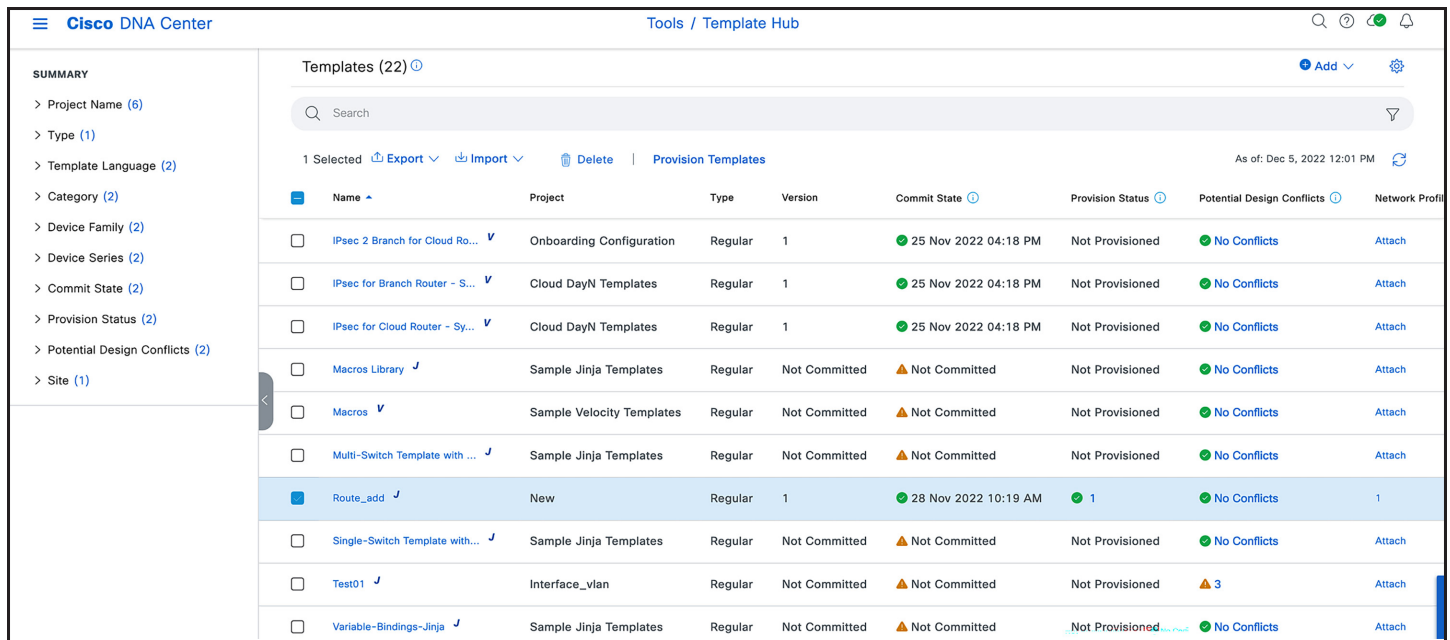
The network administrator has the option to set up calendar profiles, which define off-peak times.

The use of AP power profiles makes it easy for customers to improve energy efficiency, reduce costs, and meet sustainability goals.

Template hub

The new Template Hub simplifies management of configuration templates. The Template Hub enables network administrators to:

- Detect conflicts with templates
- Create, import, and export templates
- Provision and deploy templates
- Run simulations of variable data



Name	Project	Type	Version	Commit State	Provision Status	Potential Design Conflicts	Network Profile
IPsec 2 Branch for Cloud Ro...	Onboarding Configuration	Regular	1	25 Nov 2022 04:18 PM	Not Provisioned	No Conflicts	Attach
IPsec for Branch Router - S...	Cloud DayN Templates	Regular	1	25 Nov 2022 04:18 PM	Not Provisioned	No Conflicts	Attach
IPsec for Cloud Router - Sy...	Cloud DayN Templates	Regular	1	25 Nov 2022 04:18 PM	Not Provisioned	No Conflicts	Attach
Macros Library	Sample Jinja Templates	Regular	Not Committed	Not Committed	Not Provisioned	No Conflicts	Attach
Macros	Sample Velocity Templates	Regular	Not Committed	Not Committed	Not Provisioned	No Conflicts	Attach
Multi-Switch Template with ...	Sample Jinja Templates	Regular	Not Committed	Not Committed	Not Provisioned	No Conflicts	Attach
Route_add	New	Regular	1	28 Nov 2022 10:19 AM	1	No Conflicts	1
Single-Switch Template with...	Sample Jinja Templates	Regular	Not Committed	Not Committed	Not Provisioned	No Conflicts	Attach
Test01	Interface_vlan	Regular	Not Committed	Not Committed	Not Provisioned	3	Attach
Variable-Bindings-Jinja	Sample Jinja Templates	Regular	Not Committed	Not Committed	Not Provisioned	No Conflicts	Attach

Figure 11. Template hub

SecOps: Zero-trust workplace

Concurrent LAN automation sessions

LAN automation helps SDA customers simplify network operations, automate configuration tasks, and build a standard, error-free underlay network. Now, network administrators can run multiple concurrent LAN

automation sessions. This allows customers to reduce their change window times and build deployments at much greater scale.

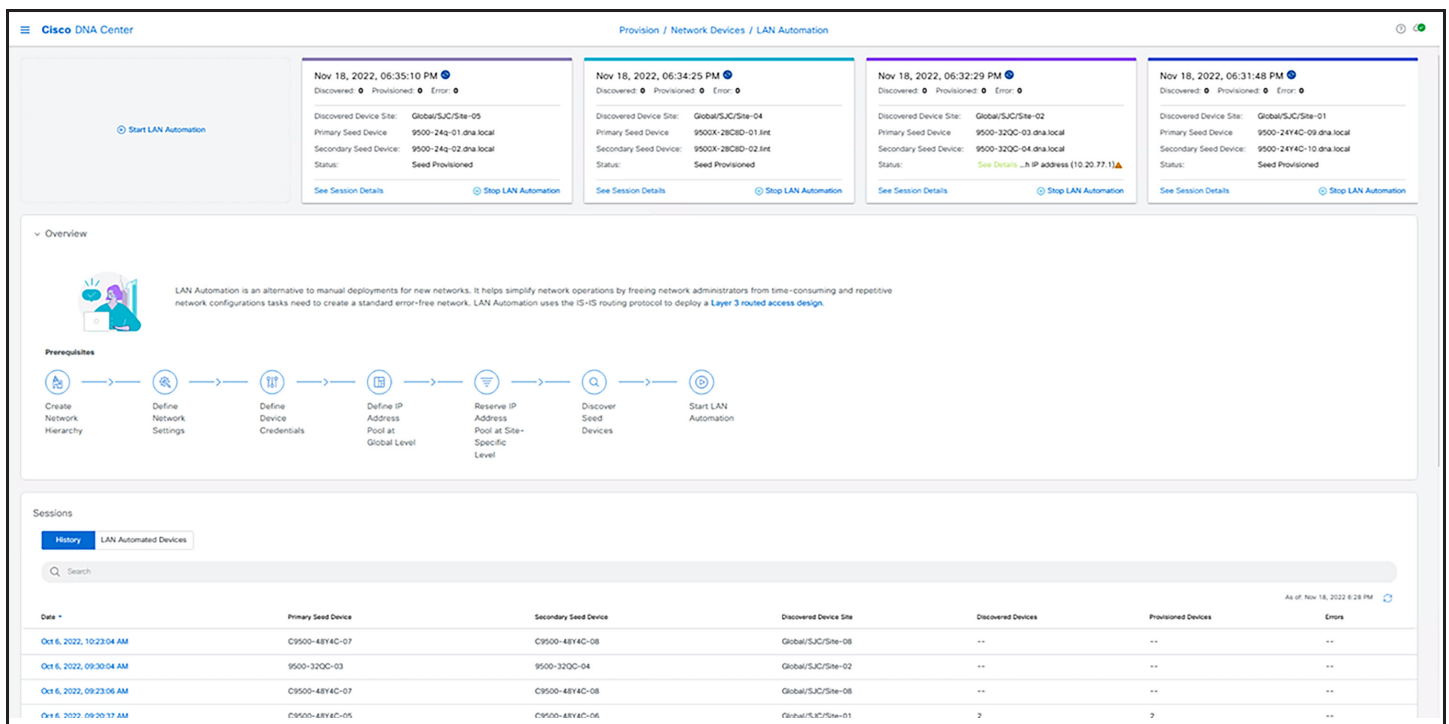


Figure 12. LAN automation

Trust score customization

Users can now customize the impact that each threat and/or vulnerability has on a given endpoint's trust score to prioritize those threats/vulnerabilities that are most sensitive for their organization and environment.

Once the required changes have been decided, it provides a comparison preview to show how the number of endpoints classified as High, Medium, or Low trust would change before applying.

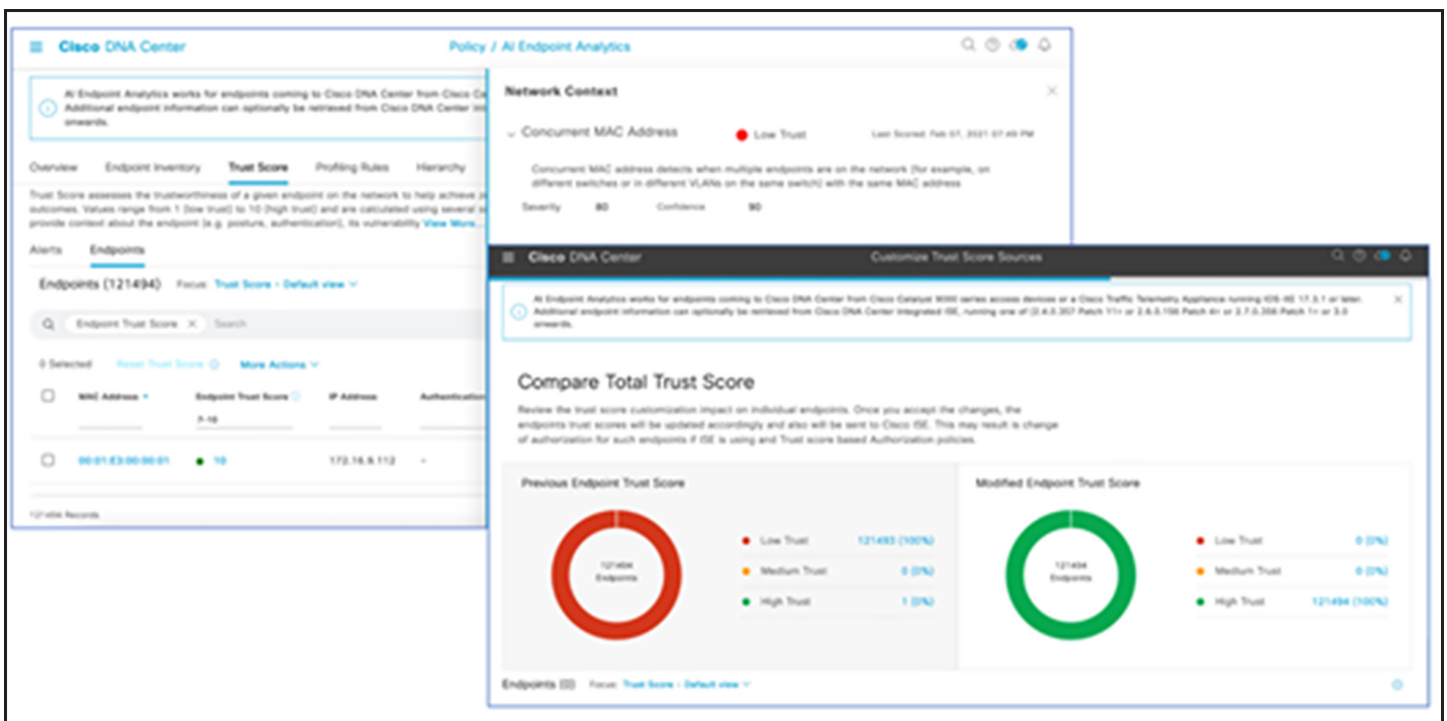


Figure 13. Trust score customization

Rogue access point remediation

When a rogue access point is discovered, security teams require that it is disabled as quickly as possible. With this new release, a network administrator can configure rogue rules that automatically perform

wireless containment of a rogue AP when it is discovered, so network administrators don't need to manually perform the action. Automatic containment can be configured for honeypot and custom rogue rules.

SD-Access extranet

Cisco DNA Center 2.3.5 makes it easier for fabric customers who want to provide internet and shared services to other virtual networks. Now there is no need for a dedicated peer node, and no requirement for complex route leak configuration.

SD-Access Extranet will provide administrators with an automated policy-based capability allowing communication from virtual networks to the internet and shared services in the fabric.

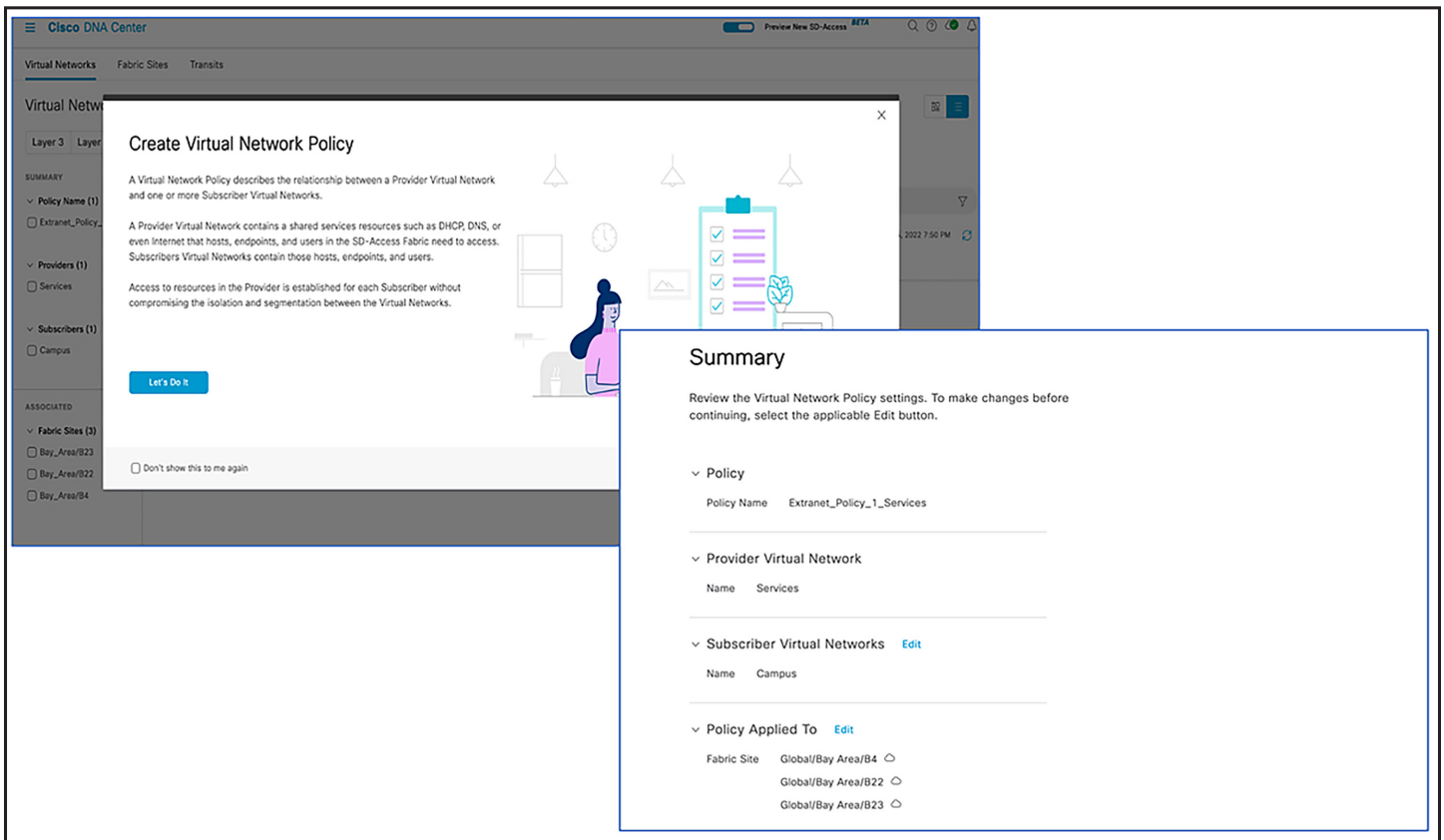


Figure 14. SD-Access extranet



DevOps: Innovation and integrations

New APIs

This new release includes these new integration points:

APIs

- EOX APIs: summary, status, and details
- Platform API to provide a list of installed packages
- User-defined fields APIs CRUD
- Rogue/aWIPS API for details and count
- API to get authentication and policy server
- Network Design Services (v2)
- LAN automation (get an LAN automation session)
- SDA APIs: fabric zone, HTTP return code

Events

- AI analytics roaming failure event
- BGP session status enhancements
- Assurance: user-defined issues
- Get webhook destination
- Get syslog, email, SNMP destinations
- Get email destination
- Get SNMP destination

Integration

- Incremental sync for endpoint analytics

Cisco DNA Center App for Splunk Enterprise

The Cisco DNA Center App for Splunk Enterprise integrates with Cisco DNA Center to offer a single view of network status, client health, application visibility and more.

This offers customers an easy way to get started integrating Cisco DNA Center and Splunk. It also gives users a way to view long-term network trends.

The Cisco DNA Center dashboard application has been published on Splunkbase.

The screenshot shows the Splunkbase interface for the Cisco DNA Center App. At the top, there is a search bar and navigation links for 'My Account', 'My Splunk', and 'Support & Services'. The app title 'Cisco DNA Center App' is prominently displayed next to a green 'DOWNLOAD' button. A red banner below the title states: 'This app is currently hidden and is scheduled to release on Fri Dec 30 2022 7:00:00 PM Australian Eastern Daylight Time'. Below this is a blue bar with 'ADMINISTRATOR TOOLS' and links for 'Manage App', 'View App in New Splunkbase', 'View App in Splunkbase Classic', and 'View Analytics'. The main content area is divided into two sections. On the left, under 'STATUS: APPROVED', there is a sidebar menu with options: 'Hosting', 'Description', 'Media', 'Details', 'Settings', 'Leads', and 'Editors'. On the right, the 'VERSIONS' section features a table with columns: VERSION, DEFAULT, VISIBILITY, COMPATIBILITY, UPLOAD DATE, COMPATIBILITY REPORT, VICTORIA, and CLASSIC. The table lists version 1.0.0 as the default, with a visibility icon, compatibility for 9.0, 8.2, 8.1, and 8.0, an upload date of Nov 11, 2022, and 'Passed' status in both Victoria and Classic environments. Below the table, there is a 'Scheduled Release Date: 12/30/2022 7:00:00 PM' with a timezone note '(GMT +11)'. A link 'Learn more about Compatibility Reports' is provided. At the bottom, there is a red button 'REQUEST APP ARCHIVING' and a link 'Learn more about app archiving.'.

VERSION	DEFAULT	VISIBILITY	COMPATIBILITY	UPLOAD DATE	COMPATIBILITY REPORT	VICTORIA	CLASSIC
1.0.0	🟢	👁️	9.0, 8.2, 8.1, 8.0	Nov 11, 2022	Details	Passed	Passed

Figure 15. Cisco DNA Center App on Splunkbase



Cisco DNA Center Platform

Cisco DNA Center Virtual Appliance

For years, Cisco customers have improved agility, gained insights, and automated tasks using Cisco DNA Center running on hardware appliances. Now, Cisco DNA Center is available as a virtual appliance on AWS.

Customers who have embraced virtualization have realized increases in IT efficiency, improved application resiliency, and reduced costs. Additionally, virtualization helps customers meet their sustainability goals.

Now, Cisco DNA Center customers will have the flexibility to deploy in AWS.

The Cisco DNA Center Virtual Appliance provides a quicker and more streamlined installation process. It includes the same capabilities as Cisco DNA Center when running on appliances, and the virtual appliance benefits from the inherent high availability capabilities of AWS.

Restricted shell

The new restricted shell enhances security by preventing users from getting to the shell of the underlying OS. This command line interface provides an easy-to-use set of validated commands that is consistent with other Cisco® solutions.

Scalability improvements

On a 3-node XL cluster, Cisco DNA Center now supports up to:

- 35,000 total combined devices
 - 25,000 APs plus 10,000 network devices (max)
- 300,000 concurrent clients
- 10,000 site elements

Note: Other combinations of devices and APs, exceeding the above thresholds, are not tested for scale and performance.

New devices

This version adds support for additional models in these families

- Cisco Catalyst® 9100 Series Access Points
- Cisco Catalyst 9200 Series Switches
- Cisco Catalyst 9500 Series Switches
- Cisco Catalyst 9600 Series Switches
- Cisco 1000 Integrated Services Routers
- Cisco Catalyst 8500 Series Routers
- Rockwell Stratix 5410 Industrial Distribution Switches