Cisco DNA Center – AIOps

An AI-Driven Approach to Digital Transformation

Cisco DNA Center - AIOps

An AI-driven Approach
to Digital Transformation

Preface

Authors

This book represents an intense collaboration between Technical Marketing, Engineering, and Product Management during a week-long intensive session at Cisco Headquarters in San Jose, CA.

- Prem Chandran – Technical Marketing
- Sean Sivak – Technical Marketing
- Harsharan Dhaliwal – Technical Marketing
- Suresh Subramanian – Engineering
- Federico Lovison – Engineering
- Shai Silberman – Product Management

Acknowledgments

A tremendous thank you to Cisco’s Enterprise Networking Technical Marketing, Product Management, Engineering, Sales, and Customer Experience teams who recognized the need for this book and supported its development. A special thanks to Jeff Scheaffer, Jeff McLaughlin, Todd Untrecht, and Bipin Kapoor for supporting the efforts of the authoring team. We would also like to thank Shannon Chavez for her incredible resource organization throughout this process, Sum Nguyen and Satpal Ranu who helped with the demo servers for the screenshots, and the many amazing Cisco resources who provided information and clarifications throughout the process.

We would also like to extend our sincerest appreciation to our Book Sprints team (*www.booksprints.net*):

- Karina Piersig – Book Sprint facilitator
- Christine Davis – Copy editor
- Raewyn Whyte – Copy editor
- Henrik van Leeuwen – Illustrator
- Lennart Wolfert – Illustrator
- Agathe Baëz – Book designer
- Barbara Rühling – Project manager

Karina and the team were outstanding in creating an environment that allowed our thoughts and ideas to collaboratively flourish to produce this publication.

Organization of this Book

This book is structured as an informative publication for a wide variety of personas involved in networking and enterprise IT infrastructure. Cisco DNA Center supports NetOps, AIOps, SecOps and DevOps use cases. NetOps covers key features like software image management, plug and play, configuration management and configuration compliance. SecOps covers key features like rapid threat containment, Endpoint classification and Trust Analytics. DevOps covers integrations, APIs and notifications to WebHooks. This book primarily focuses on AIOps. The opening chapters of the book provide a high-level overview of Cisco's vision for transforming digital networks and the benefits of AIOps within the context of Cisco DNA Center. The next several chapters provide technical deep dives into Cisco DNA Center's capabilities for AIOps, with product examples and real-world use cases. The closing chapters provide some additional resources for troubleshooting, deployment, and references to the features as well as terminology discussed in this book.

Intended Audience

This book is intended to cater to a wide variety of audiences from executives to technical practitioners of all levels. The technical nature of this book, however, is best suited for technical decision-makers, network managers, and network engineers. The content of this book is equally beneficial to users who are already familiar with Cisco DNA Center as well as to those who are needing to understand the role of Cisco DNA Center AIOps in increasing IT efficiency and business value.

Purpose of the Book

As we continue to introduce and promote the concept of AIOps, particularly within Cisco DNA Center, we set ourselves on a mission to write this book with the idea that it would serve both highly technical individuals and business decision-makers. We wanted them to be able to gain a solid understanding of what AIOps means in the era of digital transformation, as well as how Cisco DNA Center can help an organization to make that process as seamless, efficient, and valuable as possible.

Book Writing Methodology

The Book Sprints (*www.booksprints.net*) methodology was extraordinarily helpful in allowing us to craft this message. The Book Sprints team helped to foster a collaborative environment that let each individual utilize their strengths and rapidly complete this book.

We spent numerous hours writing, reviewing, and editing the content in this book. We are enormously proud and happy to present the key benefits and features of Cisco DNA Center AIOps to help organizations evolve the way they monitor, troubleshoot, and gain insights into their network.

1. Introduction

Cisco's strategy is to help customers connect, secure, and automate agile networks to accelerate the digital transformation of their environment. Our Integrated Cisco DNA Platform Suite securely connects people to people, people to applications, and devices to applications.

This is accomplished with AI-driven **visibility**, **observability**, and **insights** to ensure the health of users, applications, and infrastructure. AIOps with the Cisco DNA Center utilizes industry-leading Cisco AI Network Analytics with Machine Learning, Machine Reasoning, and Visual Analytics to eliminate excess noise, quickly identify issues, and remediate problems faster. This new agile approach of integrating AIOps, NetOps, SecOps, and DevOps personas evolves IT into a competitive advantage.

Cisco DNA Center AIOps enables **visibility** of the entire network through multiple lenses, such as geography, hierarchy, and topology, as well as at the site, building, and floor levels.

Cisco DNA Center AIOps provides **observability** of device health, client health, and application health utilizing key performance indicators (KPIs), which enables AI-driven issue identification and AI-driven root cause analysis. Cisco DNA Center combined with Machine Reasoning Engine (MRE) is like having 30-years of Cisco experience at hand.

Cisco DNA Center AIOps delivers **insights** on trends and changes in the environment over time and creates system-generated issues to proactively identify abnormal behavior.

Learn how Cisco DNA Center can digitally transform any network environment!

2. Digital Transformation Acceleration

The journey to Digital Transformation starts with Cisco DNA Center. Cisco's DNA Center is designed to embrace Cisco's core mission to help customers connect, secure, and automate in a cloud-first world.

Cisco DNA Center is part of the Integrated Platform Suite bringing together a collection of products and software leveraging Cisco's Unified Analytics Framework. With this Unified Analytics Framework, Cisco can deliver agile networks with insights, automation, and security. All this combines to accelerate our customers' digital transformation journey. No matter whether users or applications are on the campus, in the cloud, or the hybrid work environment, this acceleration creates a faster time to value with our product suites. At the center of this multi-domain network is Cisco DNA Center and the Integrated Platform Suite.

Cisco DNA Center accelerates Digital Transformation through the use of four key IT personas. Those personas include:

AIOps – AI-driven visibility, observability, insights, and troubleshooting to ensure the health of users, applications, and infrastructure.

NetOps – Automation to simplify the creation and maintenance of networks with the flexibility to move from manual network management to selectively autonomous network management.

SecOps – AI-driven security to classify endpoints and enforce security policies for a complete zero trust workplace solution.

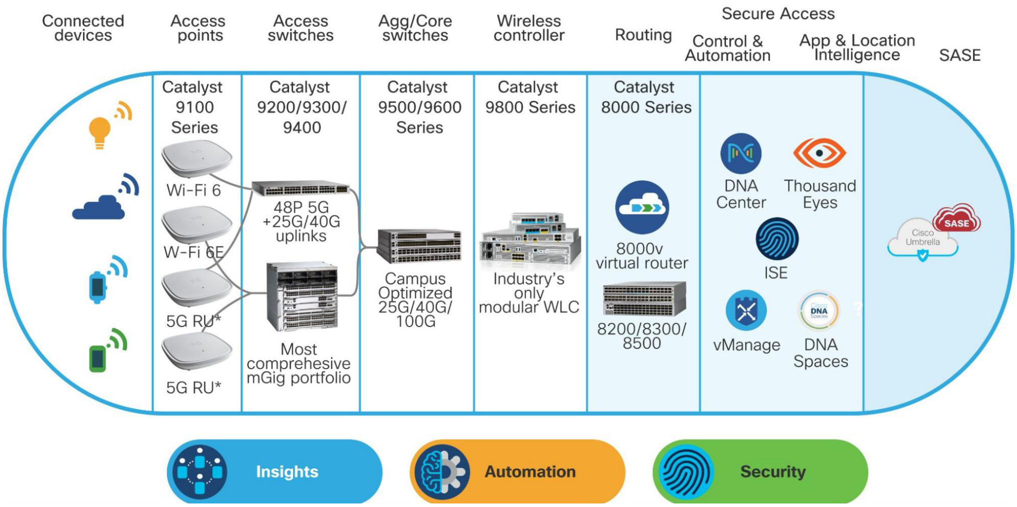
DevOps – Mature APIs, SDKs, and closed-loop integrations to simplify and streamline ecosystem integration.

Figure 2.1: The four Key IT Personas

Secure Agile Networks depend on beautifully coupled digital-ready infrastructure and software.

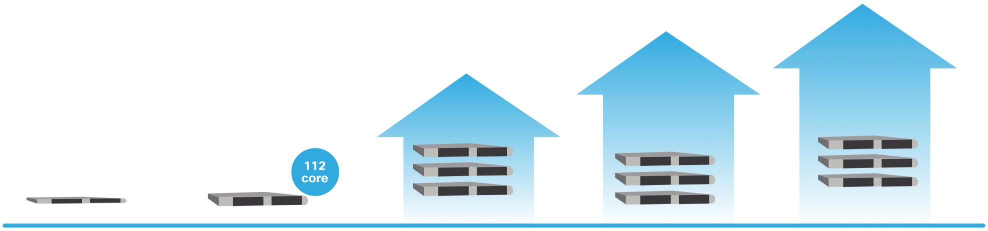
The infrastructure works in conjunction with the control software, and telemetry is designed into the products to drive agility, insights, automation, and security.

Figure 2.2: Product Suite



Cisco DNA Center is well suited for small and medium-sized enterprises up to the largest corporations on the planet. Designed to handle thousands of devices and hundreds of thousands of concurrent endpoints, Cisco DNA Center can handle just about any size organization, providing scale, insights, agility, automation, and security.

Figure 2.3: Cisco DNA Center Scaling



✓ NPI	✓ Vertical Scale	✓ HA/2x Scale	✓ 3x Scale	✓ 4x scale
1K NW Devices 4K APs 25K Endpoints	5K NW Devices 13K APs 100K Endpoints	5K NW Devices 13K APs 100K Endpoints 250K Transient 100K/s flows 2000 sites	8K NW Devices 16K APs 300K Endpoints 750K Transient 250K/s flows 4000 sites	Sum(10k NW devices, 18k Aps) = 24k Total 300k Endpoints 750k Transient 250K/s flows 6000 sites

Please see the **Cisco DNA Center Data Sheet** for more information on scaling.

3. How to get started with AIOps

The term AIOps stands for Artificial Intelligence for IT Operations. This term, originally coined by Gartner in 2017, refers to the way data and information from an environment or system are enhanced by an IT operations team. This chapter will cover AIOps basic concepts, benefits, and first steps to get started with Cisco DNA Center's AIOps.

AIOps Benefits

AIOps platforms utilize big data, modern machine learning, and industry-leading analytics to enhance IT operations with a focus on monitoring, automation, and troubleshooting with proactive AI-driven insights.

There are numerous benefits to using and employing Artificial Intelligence. When combining AIOps and NetOps IT personas, organizations have yielded the following benefits:

Increased observability has yielded quantifiable results in decreasing Mean Time To Resolution (MTTR) for system issues and troubleshooting workflows. Empowered by the generation of dynamic baselines, using AI has significantly reduced the alerting fatigue with more impactful and contextual AI-driven issues contributing to reduced MTTR.

Multitudes of system-generated automated insights, tracking systems, and user behaviors help customers understand how the network is being utilized and provide the ability to understand changing demands and usage patterns in the network. **Cisco DNA Center AI Insights** can assist customers with proactive capacity planning and network enhancements based on trends to keep up with ever-increasing demands.

Justification of hardware refresh is commonly accompanied by data to demonstrate the need. Cisco DNA Center AI-driven comparative analytics can demonstrate and compare and contrast service-level KPIs between sites, access points, and endpoints. Comparative analytics can also help compare the KPIs of peers in similar industries.

AI-driven predictive monitoring and insights can help prevent failures and drive proactive workflows and recommendations. With proactive actions, AIOps enable the organization to be more agile and to use IT as a competitive advantage, increasing business value to the organization.

User experience is king. Monitoring user experience using Cisco DNA Center AI provides insights, allowing engineers to proactively resolve issues before users are impacted.

With AIOps visibility, observability, and insights, organizations can commit fewer senior-level resources to work and troubleshoot issues.

AIOps is an accelerator to improve the Time To Value (TTV) and Return on Investment (ROI) propositions. A common challenge with traditional network management systems is the long time it takes to fully implement all the features to yield high-value benefits. With Cisco DNA Center and AIOps, once AI is enabled, the organization can begin to yield the benefits almost immediately.

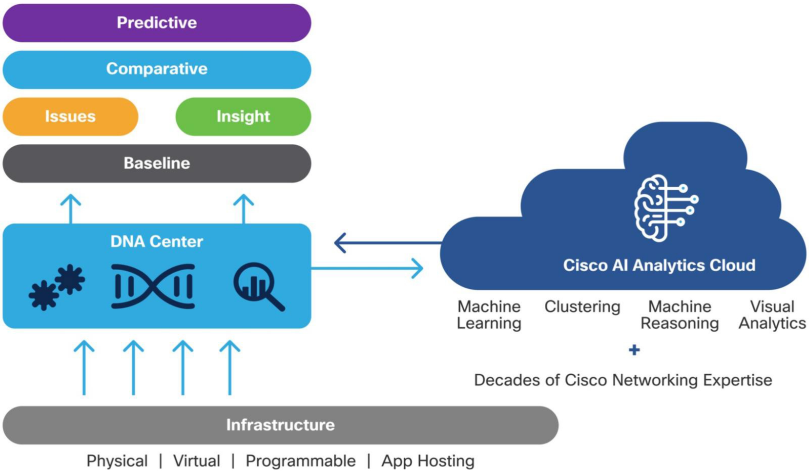
AIOps Key Customer Benefits with Cisco DNA Center:

- **Dynamic Baselining** offers the ability to determine what is normal in a specific environment.
- **Anomaly Detection** offers the ability to separate normal from abnormal behavior.
- **Trends and Insights** can show patterns over time, enabling predictive analysis to estimate future outcomes.
- **Comparative Analytics** compare KPIs internally as well as against peers to determine not only an organization's performance but also how it performs compared to other organizations of similar sizes.
- **Predictive Analytics** allows for a more proactive approach to troubleshooting by solving minor problems before they become major issues. This is based upon system-generated insights gathered from dynamic baselines, anomaly detection, and KPI comparison.

Cisco DNA AI Analytics Architecture

Cisco DNA Center gathers and aggregates data from network devices, clients, and applications. It then obfuscates, encrypts, and sends that data to the Cisco AI Network Analytics engine in the Cisco AI Analytics Cloud. Once on Cisco's servers, Machine Reasoning, Clustering, Machine Learning, and Visual Analytics are utilized to provide industry-leading AI Analytics.

Figure 3.1: Cisco's AI Analytics Architecture



After the AI Network Analytics Engine completes the processing of data through the pipeline above, the cloud engine pushes the AI-driven issues and insights back to Cisco DNA Center. These AI-driven issues are then able to provide actionable items such as:

- Customized network baselines
- Customized network issues
- Customized insights
- Comparative analytics
- Predictive analytics

These use cases are reviewed in detail in later chapters in this book.

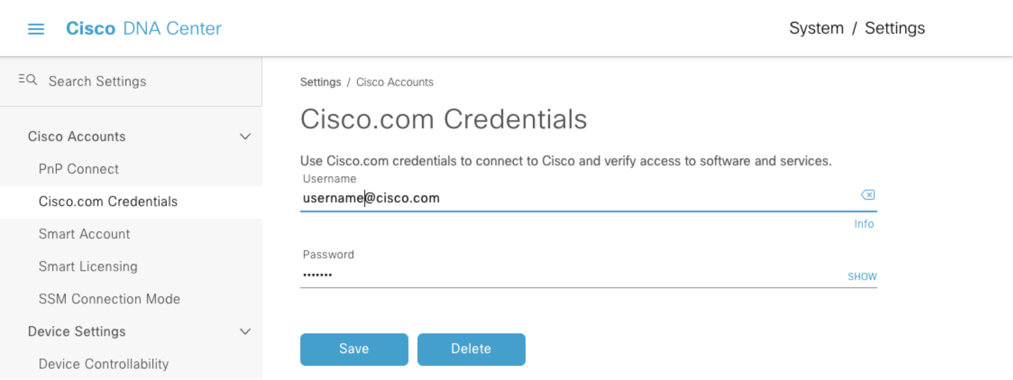
Getting started with Cisco AI Network Analytics

There are a few requirements before Cisco AI Network Analytics can be enabled on the Cisco DNA Center appliance:

- Cisco DNA Center version must be 1.3.1 or higher (This book refers to many features available only in 2.2.3 or later).
- All Assurance and AI Analytics Application packages must be downloaded and installed from the Cisco DNA Center web GUI.
- The Cisco DNA Center appliance **MUST** have access to the internet.

After ensuring that the above requirements have been met, the next step is to configure a Cisco.com CCO ID in the `System Settings` for Cisco DNA Center. Click `Save` to apply the credentials to ensure access to Cisco DNA Center software and services.

Figure 3.2: Cisco.com Credentials



Cisco.com Credentials

Use Cisco.com credentials to connect to Cisco and verify access to software and services.

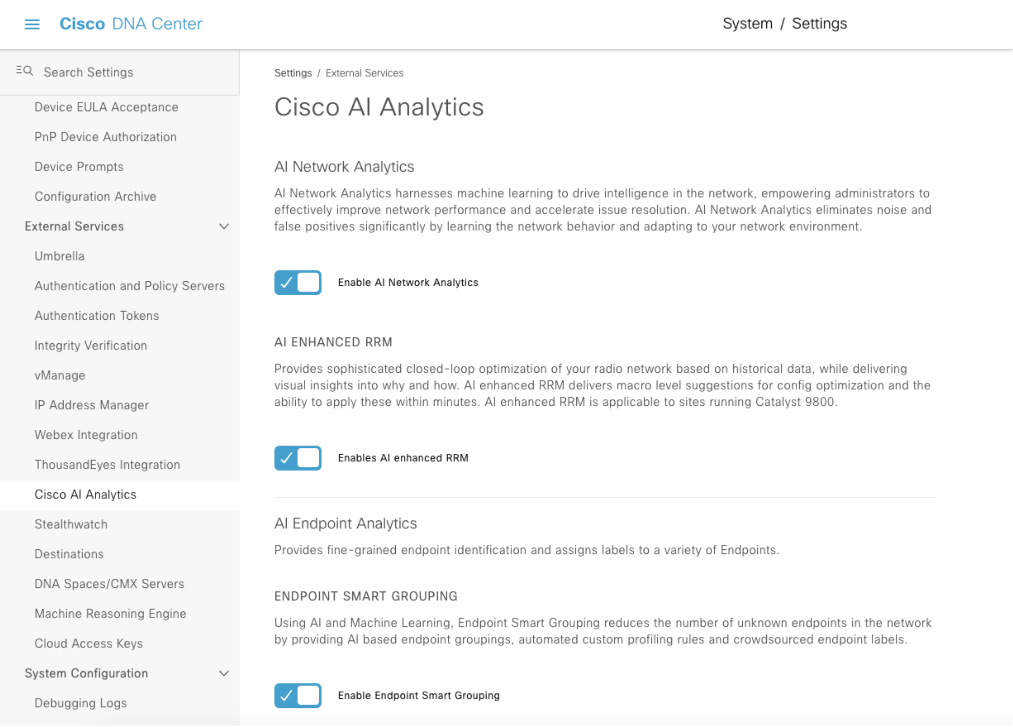
Username: username@cisco.com

Password: •••••••

Enabling Cisco AI Analytics

Cisco AI Analytics can be enabled by navigating to the `System Settings` and selecting `Cisco AI Analytics` from the `External Services` menu.

Figure 3.3: Enabling Cisco AI Analytics from the Cisco DNA Center System Settings



Cisco AI Analytics

AI Network Analytics

AI Network Analytics harnesses machine learning to drive intelligence in the network, empowering administrators to effectively improve network performance and accelerate issue resolution. AI Network Analytics eliminates noise and false positives significantly by learning the network behavior and adapting to your network environment.

☑ Enable AI Network Analytics

AI ENHANCED RRM

Provides sophisticated closed-loop optimization of your radio network based on historical data, while delivering visual insights into why and how. AI enhanced RRM delivers macro level suggestions for config optimization and the ability to apply these within minutes. AI enhanced RRM is applicable to sites running Catalyst 9800.

☑ Enables AI enhanced RRM

AI Endpoint Analytics

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

ENDPOINT SMART GROUPING

Using AI and Machine Learning, Endpoint Smart Grouping reduces the number of unknown endpoints in the network by providing AI based endpoint groupings, automated custom profiling rules and crowdsourced endpoint labels.

☑ Enable Endpoint Smart Grouping

Cisco AI Network Analytics has to be enabled to use all of the available AIOps features.

The following AIOps features: AI Enhanced RRM, AI Endpoint Analytics, and AI spoofing detection can also optionally be configured here.

After enabling Cisco AI Network Analytics, select the desired cloud region and click on `Configure`; at this point, once the user accepts the Cisco Universal Cloud Agreement, the local agent will contact the cloud service to register a new tenant.

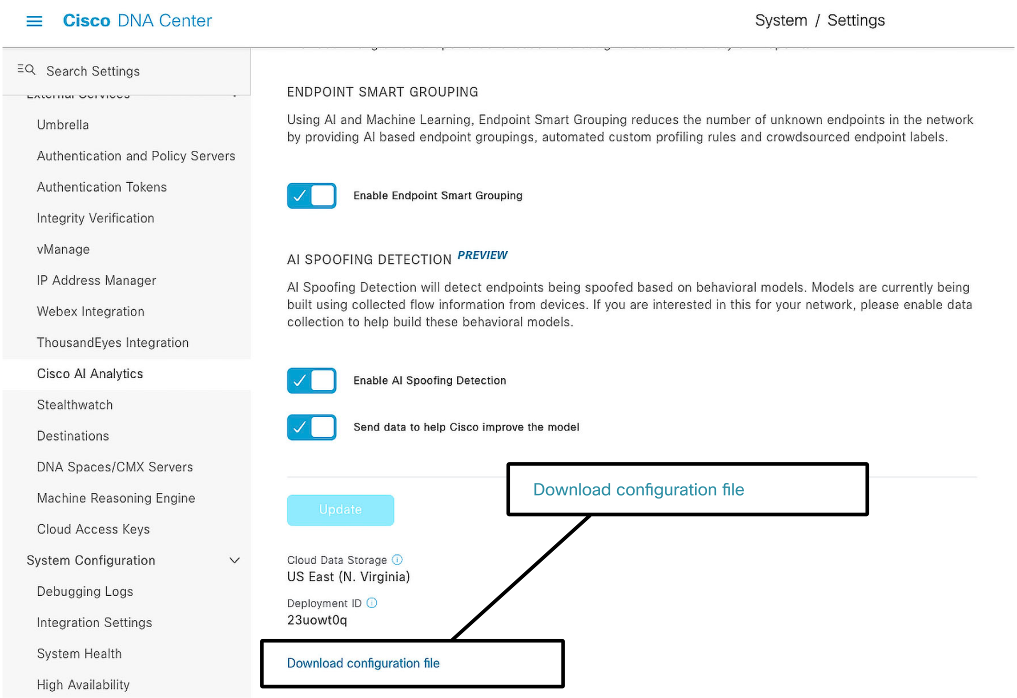
The registration usually takes a few seconds. Once it completes, the User Interface (UI) will automatically download the configuration file to the local machine. This file contains critical information to access the cloud service, including the tenant ID (also called Deployment ID or Customer ID), the anonymization key used to encrypt sensitive data, and the certificate used to authenticate the agent against the cloud endpoint, therefore the file should be stored in a secure location.

The AI Network Analytics configuration file can be backed up at any time by going back to the settings page. The configuration is also part of the global Cisco DNA Center Appliance Backup, however, it is highly recommended to keep a copy of the configuration file as well, as this would allow restoring the Cisco AI cloud connectivity using the same tenant ID, even in scenarios where a full appliance restore is not desirable.

Note Without the configuration file, all historical AIOps data will be lost in the event of a fresh install of the Cisco DNA Center.

Moreover, AI Network Analytics requires having only a single Cisco DNA Center appliance using the configuration for a given tenant ID at any given point in time. If the same configuration is restored and concurrently used on multiple appliances, the UI will show an error message.

Figure 3.4: Downloading AI Network Analytics Configuration File



ENDPOINT SMART GROUPING

Using AI and Machine Learning, Endpoint Smart Grouping reduces the number of unknown endpoints in the network by providing AI based endpoint groupings, automated custom profiling rules and crowdsourced endpoint labels.

☑ Enable Endpoint Smart Grouping

AI SPOOFING DETECTION *PREVIEW*

AI Spoofing Detection will detect endpoints being spoofed based on behavioral models. Models are currently being built using collected flow information from devices. If you are interested in this for your network, please enable data collection to help build these behavioral models.

☑ Enable AI Spoofing Detection

☑ Send data to help Cisco improve the model

Cloud Data Storage: US East (N. Virginia)

Deployment ID: 23uowt0q

Ensuring Data Privacy with Cisco AI Network Analytics

Cisco DNA Center encrypts all the data that is uploaded to the Cisco AI cloud with a unique customer ID and encryption key. All data stored in the Cisco AI cloud is anonymized and encrypted. No hostname, MAC addresses, IP addresses, device names, access points, or client-identifying information is distinguishable on the Cisco AI cloud. This data only becomes readable once it is decrypted. Where noted, personal data is de-identified before transfer to the AI Network Analytics Cloud.

For more information regarding data privacy with Cisco AI Network Analytics, please refer to the Cisco DNA Center Privacy Data Sheet in the **References** section of the book.

Geographic Data Locality

Due to data privacy and requirements in some regions, Cisco has created two AI Network Analytics cloud regions. One is located in the United States and one in the European Union (EU). **Please check with local data governance compliance to see which region is applicable.**

4. AIOps Basics

As an advanced intent-based network controller and user experience platform, Cisco DNA Center provides many features from basic to advanced visibility dashboards and user experience measurements. This chapter will cover Cisco DNA Center's Overall dashboard.

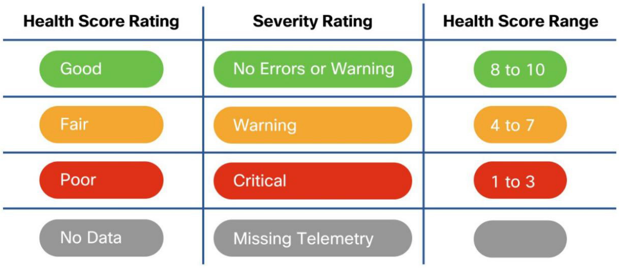
Health Scores

Cisco DNA Center acquires contextual information from network devices, clients, and applications. The key KPIs collected are used to calculate a health score for the network devices, clients, and applications. Based on the type of network device, the KPIs utilized will be different. A health score is then assigned to each particular network device, client, or application matching the lowest score from all included KPIs. Health score KPIs include items such as:

- Link utilization
- CPU utilization
- Memory utilization
- RSSI and SNR on wireless clients
- Air Quality
- Interference

The figure below illustrates the Cisco DNA Center health score ratings, severity ratings, and score ranges:

Figure 4.1: Health Score Range

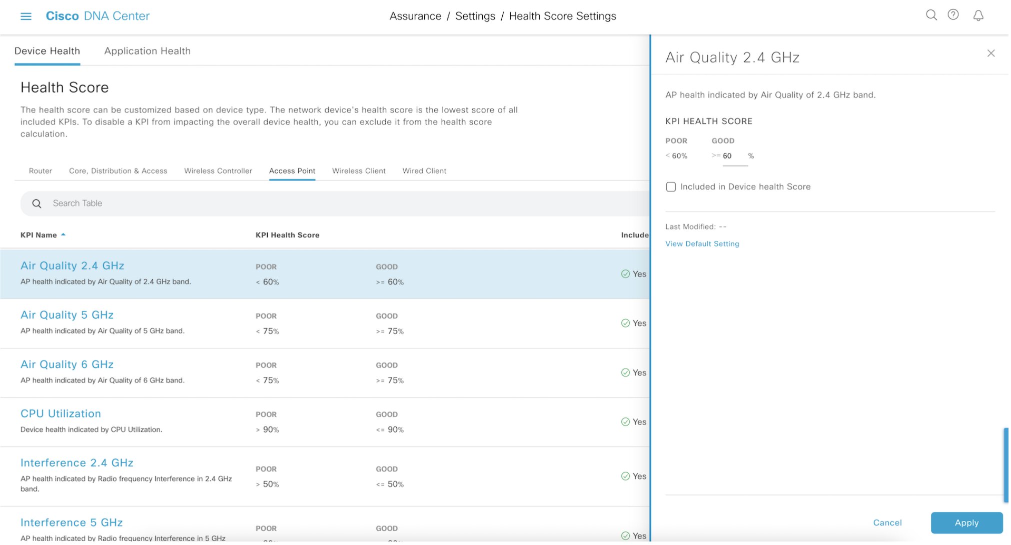


Health Score Rating	Severity Rating	Health Score Range
Good	No Errors or Warning	8 to 10
Fair	Warning	4 to 7
Poor	Critical	1 to 3
No Data	Missing Telemetry	

Note Not all KPIs have to be included in the health score calculation. Any KPI can be manually excluded from health score calculations.

For instance, if a wireless engineer did not want the Air Quality on 2.4GHz KPI to affect AP Health Scores, that KPI could be excluded from the health score calculation. This customization can be done from the `Assurance > Health Score Settings` page.

Figure 4.2: Health Score Settings



Cisco DNA Center

Assurance / Settings / Health Score Settings

Device Health | Application Health

Health Score

The health score can be customized based on device type. The network device's health score is the lowest score of all included KPIs. To disable a KPI from impacting the overall device health, you can exclude it from the health score calculation.

Router | Core, Distribution & Access | Wireless Controller | Access Point | Wireless Client | Wired Client

Search Table

KPI Name ▲	KPI Health Score		Include
Air Quality 2.4 GHz AP health indicated by Air Quality of 2.4 GHz band.	POOR < 60%	GOOD >= 60%	✓ Yes
Air Quality 5 GHz AP health indicated by Air Quality of 5 GHz band.	POOR < 75%	GOOD >= 75%	✓ Yes
Air Quality 6 GHz AP health indicated by Air Quality of 6 GHz band.	POOR < 75%	GOOD >= 75%	✓ Yes
CPU Utilization Device health indicated by CPU Utilization.	POOR > 90%	GOOD <= 90%	✓ Yes
Interference 2.4 GHz AP health indicated by Radio frequency Interference in 2.4 GHz band.	POOR > 50%	GOOD <= 50%	✓ Yes
Interference 5 GHz AP health indicated by Radio frequency Interference in 5 GHz	POOR	GOOD	✓ Yes

Air Quality 2.4 GHz

AP health indicated by Air Quality of 2.4 GHz band.

KPI HEALTH SCORE

POOR	GOOD
< 60%	>= 60 %

□ Included in Device health Score

Last Modified: --

View Default Setting

Health scores provide the network engineer with a quick and easy way to determine the health status of every network device, client, and application in the environment. If there is an issue, the network engineer would know exactly where to look to troubleshoot and provide a resolution. Keep in mind that Cisco DNA Center provides a sequence of steps to troubleshoot and fix the issue, based on Cisco's many years of experience designing, implementing, and maintaining networks of all shapes and sizes worldwide.

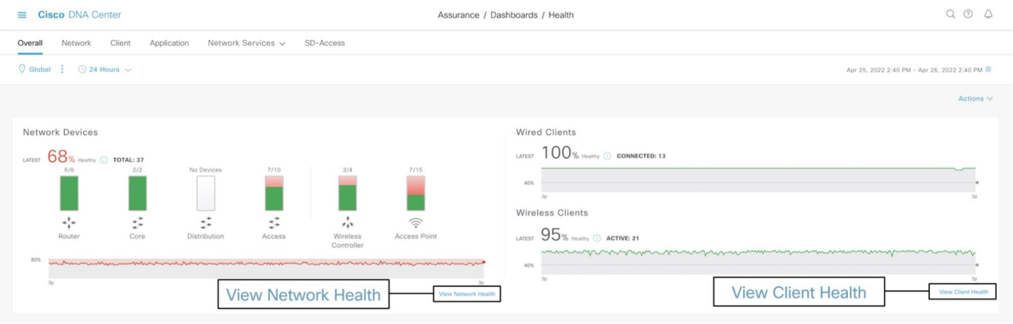
Overall Health Dashboard

The network engineer can view the Overall Dashboard by selecting `Assurance > Health` from the main menu. The Overall Health page shows the health scores of network devices and clients. This enables the network engineer to easily prioritize issues requiring attention and improve the MTTR. In the dashboard, network devices are categorized into:

- Routers
- Switches (categorized into Core, Distribution, and Access layer roles)
- Wireless LAN Controllers
- Wireless Access Points

Clients are separated into wired and wireless client categories. Additional information related to health scores and KPIs is available by drilling down into the desired `View Network Health` and `View Client Health` links, followed by selecting the device or client of interest.

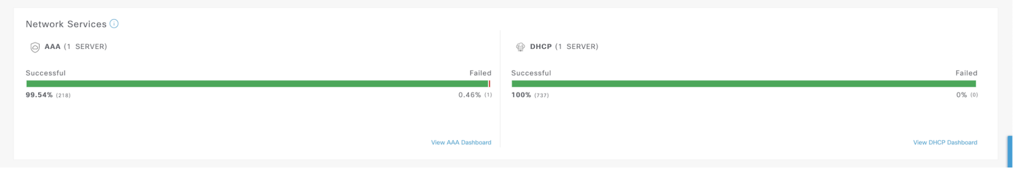
Figure 4.3: Overall Health



Cisco DNA Center provides performance analytics for Authentication/Authorization and Accounting (AAA) and Dynamic Host Configuration Protocol (DHCP) Network Services. The figure below displays both Successful and Failed transactions as well as server latency measurements. More detailed information is available by drilling down into the respective network service dashboard which is covered in Chapter 6.

The information presented by these dashboards comes directly from the Wireless LAN Controller (WLC), there is no need to separately configure AAA or DHCP within Cisco DNA Center to enable this telemetry.

Figure 4.4: Network Services (AAA and DHCP Servers)



99.54% (218)

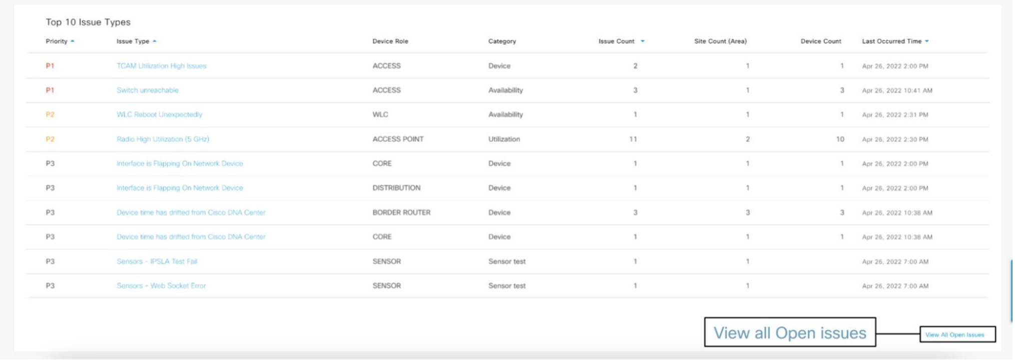
0.46% (1)

100% (737)

0% (0)

The **Top 10 Issue Types** dashlet on the figure below displays the 10 highest priority global issues for this Cisco DNA Center deployment. Clicking on the `View All Open Issues` links to the **Issues** dashboard.

Figure 4.5: Top 10 Issues



Top 10 Issue Types

Priority	Issue Type	Device Role	Category	Issue Count	Site Count (Area)	Device Count	Last Occurred Time
P1	TCAM Utilization High Issues	ACCESS	Device	2	1	1	Apr 26, 2022 2:00 PM
P1	Switch unreachable	ACCESS	Availability	3	1	3	Apr 26, 2022 10:41 AM
P2	WLC Reboot Unexpectedly	WLC	Availability	1	1	1	Apr 26, 2022 2:31 PM
P2	Radio High Utilization (5 GHz)	ACCESS POINT	Utilization	11	2	10	Apr 26, 2022 2:30 PM
P3	Interface is Flapping On Network Device	CORE	Device	1	1	1	Apr 26, 2022 2:00 PM
P3	Interface is Flapping On Network Device	DISTRIBUTION	Device	1	1	1	Apr 26, 2022 2:00 PM
P3	Device time has drifted from Cisco DNA Center	BORDER ROUTER	Device	3	3	3	Apr 26, 2022 10:38 AM
P3	Device time has drifted from Cisco DNA Center	CORE	Device	1	1	1	Apr 26, 2022 10:38 AM
P3	Sensors - IPSLA Test Fail	SENSOR	Sensor test	1	1		Apr 26, 2022 7:00 AM
P3	Sensors - Web Socket Error	SENSOR	Sensor test	1	1		Apr 26, 2022 7:00 AM

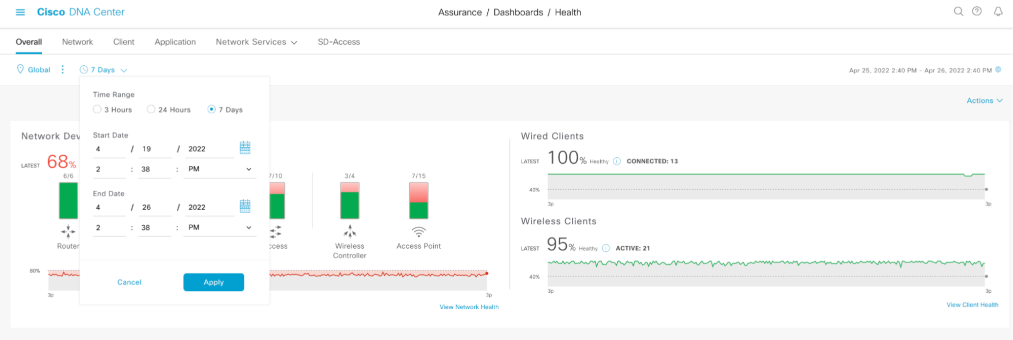
Real-World Scenario

Kyler works as a Network Engineer at a bank. He starts every morning by logging into Cisco DNA Center and checking the Top 10 Issues to see if any high-priority issues require immediate attention. If an issue is found, he drills down into the issue to get the description of the problem, follows the suggested actions, and resolves the issue. Once the issue is resolved, he highlights the issue and selects Action > Resolve.

Dashboard Filters

The **Overall Health** page can be filtered at the Global, Site, and Building levels in the hierarchy. A Filter, based on time schedules, can also be applied. Preset times are available, such as 3 hours, 24 hours, 7 days, or custom periods as far back as 30 days. Filtering helps eliminate excessive noise and allows for a more time-period focused approach to viewing issues and information.

Figure 4.6: Time Range Filters



Time Range
○ 3 Hours ○ 24 Hours ● 7 Days

Start Date
4 / 19 / 2022
2 : 38 : PM

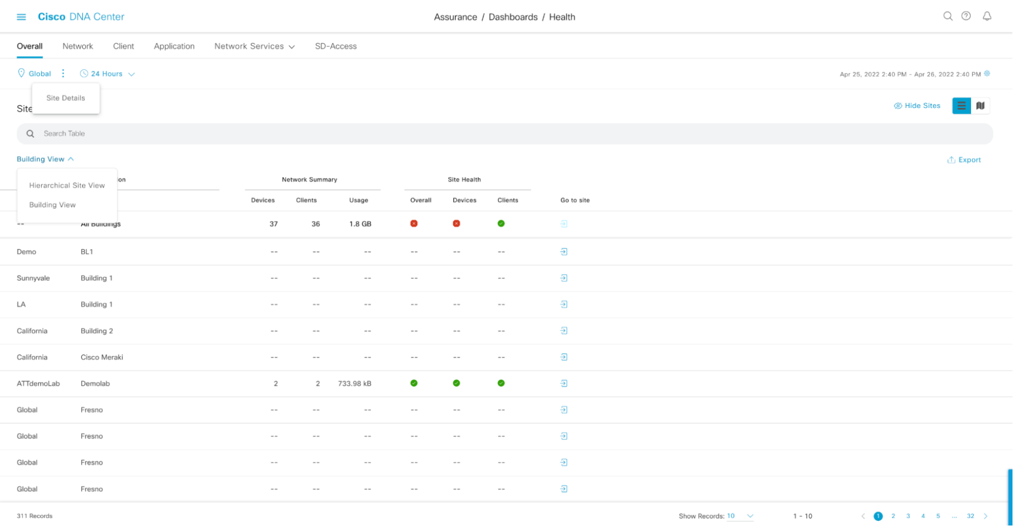
End Date
4 / 26 / 2022
2 : 38 : PM

Cancel Apply

Apr 25, 2022 2:40 PM - Apr 26, 2022 2:40 PM

Hierarchical and Building views are also available by clicking the `Site Details` link, allowing switching between the Flat view and Geo-Map view to visualize a Network Summary and Site Health. The figure below shows the Flat View.

Figure 4.7: Site Health Hierarchical Site – Building View



Apr 25, 2022 2:40 PM - Apr 26, 2022 2:40 PM

	on	Network Summary			Site Health			
		Devices	Clients	Usage	Overall	Devices	Clients	Go to site
--	All Buildings	37	36	1.8 GB	✖	✖	✓	⇥
Demo	BL1	--	--	--	--	--	--	⇥
Sunnyvale	Building 1	--	--	--	--	--	--	⇥
LA	Building 1	--	--	--	--	--	--	⇥
California	Building 2	--	--	--	--	--	--	⇥
California	Cisco Meraki	--	--	--	--	--	--	⇥
ATTdemoLab	Demolab	2	2	733.98 kB	✓	✓	✓	⇥
Global	Fresno	--	--	--	--	--	--	⇥
Global	Fresno	--	--	--	--	--	--	⇥
Global	Fresno	--	--	--	--	--	--	⇥
Global	Fresno	--	--	--	--	--	--	⇥

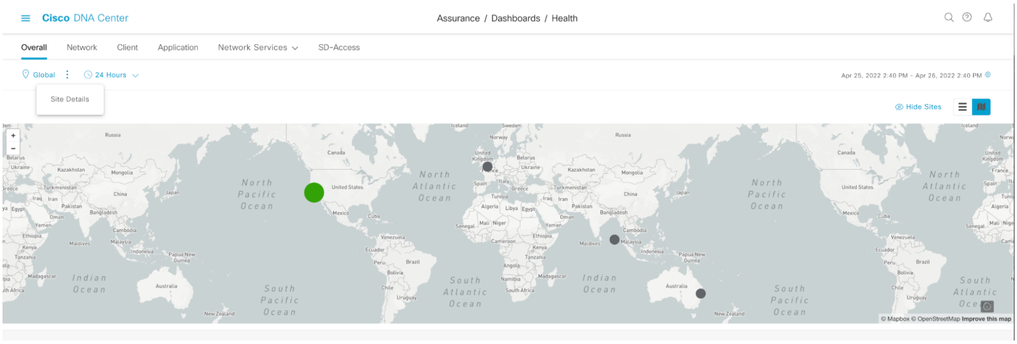
311 Records

Show Records: 10 1 - 10

1 2 3 4 5 ... 32

The figure below shows the Geo-Map View. This view can be useful for organizations with multiple geographical locations. This view can be zoomed in on specific geographic regions.

Figure 4.8: Site Health Geo Map View



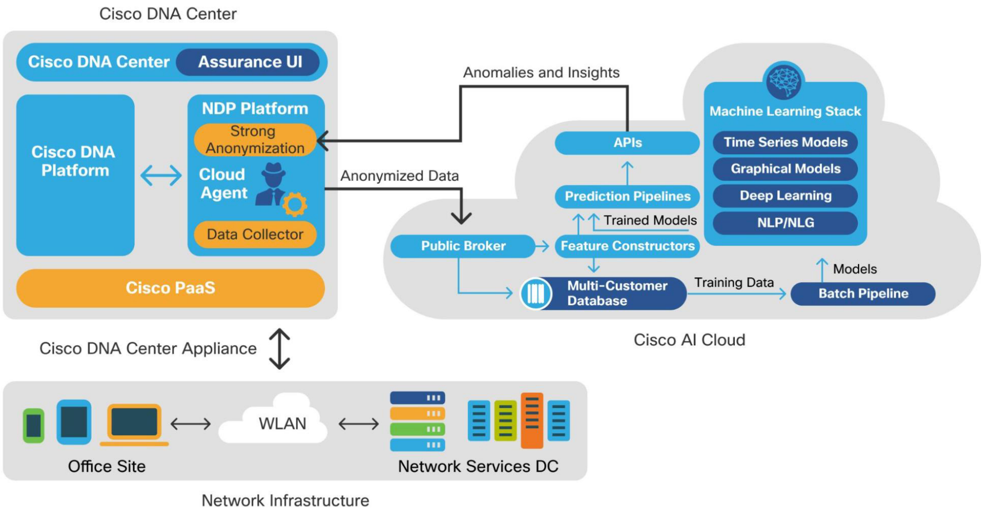
AIOps within Cisco DNA Center provides a wide variety of dashboards and insights into the network infrastructure and clients.

5. AI Network Analytics

This chapter dives into Cisco DNA Center's AI Network Analytics architecture and features, explaining the outcomes of the AI Network Analytics engine and demonstrating how and where to find AI-generated issues. The chapter further demonstrates, in detail, the immense value derived from dynamic baselining, network heatmaps, AI Enhanced RRM, comparative analytics, trends and insights. These features not only bring immediate valuable insights, but also enable the network engineers to rapidly assess issues and reduce MTTR.

Cisco AI Network Analytics Architecture

Figure 5.1: Cisco AI Network Analytics Architecture



Data collection from network devices takes place on the Cisco DNA Center appliance. A lightweight agent establishes a secure connection to the Cisco AI Analytics Cloud and exports network telemetry data, de-identifying sensitive details such as MAC/IP addresses and Host/User names before the data is uploaded to the customer's AI Cloud Analytics instance.

The data processing takes place on the Cisco AI cloud platform, with AI/ML model training as well as prediction pipelines producing results that are then made available to the users on the Cisco DNA Center GUI via an Application Programmable Interface (API) call to the Cisco AI cloud.

Sensitive data that was de-identified upon export is then restored to the original clear-text values only by the local Cisco DNA Center appliance before that data is displayed to the user.

Dynamic Baselining

Cisco AI Network Analytics learns and models the network and user behavior. After sufficient data collection and learning of typically one to four weeks, Cisco AI Network Analytics builds a model of the expected network behavior. It builds baselines for the following KPIs:

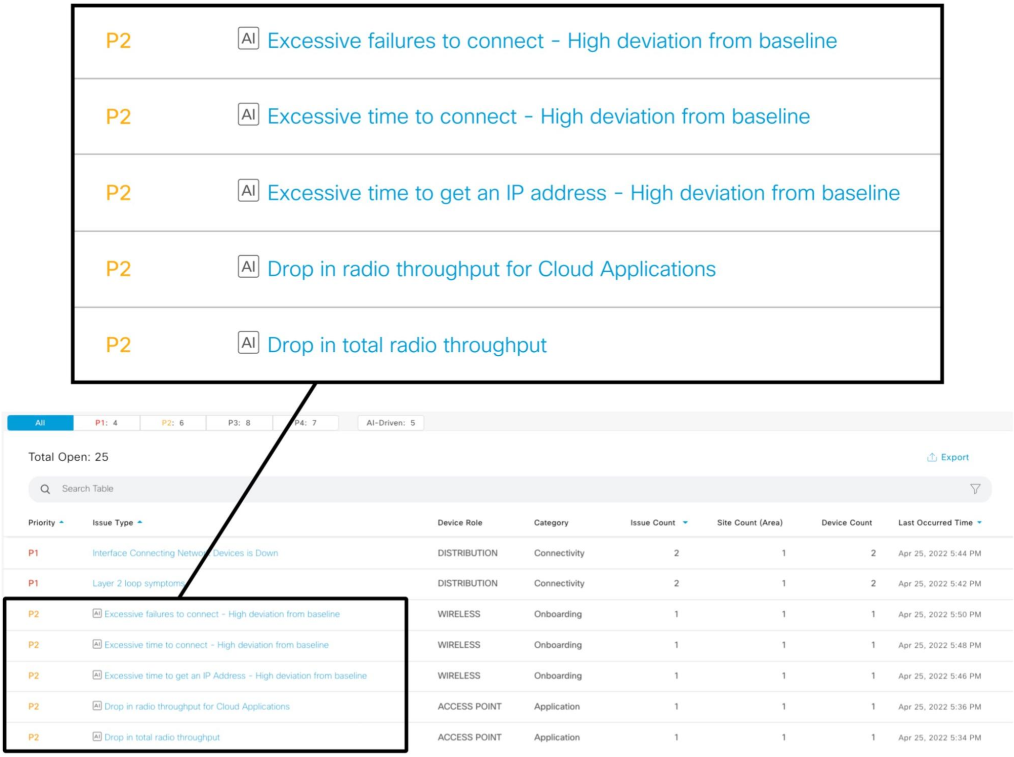
- Average onboarding time
- Average onboarding failures
- Average DHCP transaction times
- Average authentication time
- Wireless association failures
- Global application throughput
- Media/cloud/social/collaboration application throughput

AI-driven Issues

The dynamic baselines for the above-mentioned KPIs are also used to generate AI-driven issues that are accessible via the issues dashboard. Dynamic baselines are generated using machine learning models, trained using the customer's own network telemetry, considering multiple KPIs to include the complete network context. Using such baselines instead of static thresholds gives the Cisco DNA Center the ability to significantly reduce alert noise, making the network engineer's job significantly easier. The algorithms used to generate AI-driven issues help the network engineer to identify the probable root cause by displaying network KPIs that are likely to explain the reported issue. At the same time, the network engineer can add more KPIs to get a full networking context, therefore reducing the MTTR.

In the example below, there are several AI-driven issues, indicated by the special **AI** icon to the left of the issue type.

Figure 5.2: AI Issues



P2	AI Excessive failures to connect - High deviation from baseline
P2	AI Excessive time to connect - High deviation from baseline
P2	AI Excessive time to get an IP address - High deviation from baseline
P2	AI Drop in radio throughput for Cloud Applications
P2	AI Drop in total radio throughput

Total Open: 25

Priority	Issue Type	Device Role	Category	Issue Count	Site Count (Area)	Device Count	Last Occurred Time
P1	Interface Connecting Network Devices is Down	DISTRIBUTION	Connectivity	2	1	2	Apr 25, 2022 5:44 PM
P1	Layer 2 loop symptoms	DISTRIBUTION	Connectivity	2	1	2	Apr 25, 2022 5:42 PM
P2	AI Excessive failures to connect - High deviation from baseline	WIRELESS	Onboarding	1	1	1	Apr 25, 2022 5:50 PM
P2	AI Excessive time to connect - High deviation from baseline	WIRELESS	Onboarding	1	1	1	Apr 25, 2022 5:48 PM
P2	AI Excessive time to get an IP Address - High deviation from baseline	WIRELESS	Onboarding	1	1	1	Apr 25, 2022 5:46 PM
P2	AI Drop in radio throughput for Cloud Applications	ACCESS POINT	Application	1	1	1	Apr 25, 2022 5:36 PM
P2	AI Drop in total radio throughput	ACCESS POINT	Application	1	1	1	Apr 25, 2022 5:34 PM

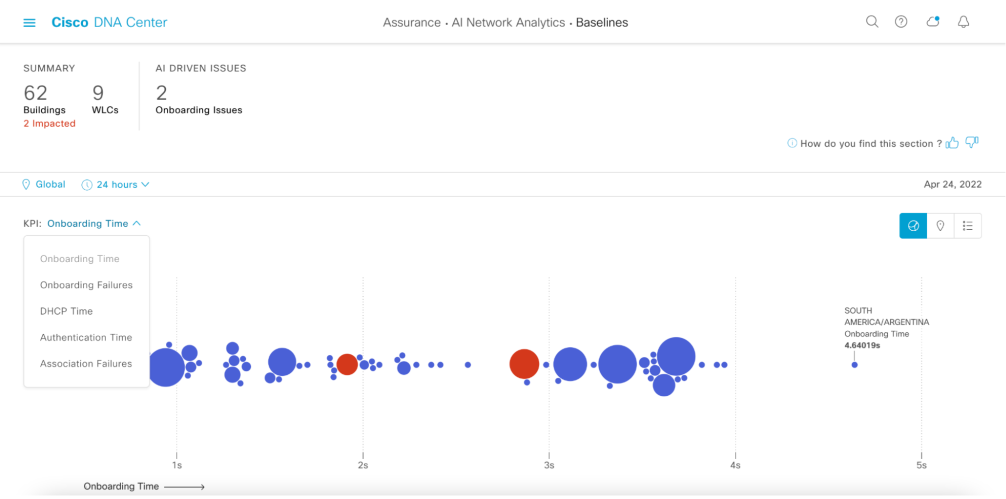
Baseline Dashboard

Dynamic baselines are also used as part of the baseline dashboard. This allows network engineers to visualize network performance compared to the predicted baseline.

The figure below illustrates the AI Network Analytics baseline dashboard showing onboarding times. The dashboard shows a holistic view of performance for various KPIs, based on the baselines driven by each individual network location. Each bubble represents a building, while the size of the bubble represents the number of clients in that building.

This view allows the network engineer to quickly identify buildings worthy of investigation, either because AI-driven issues were reported for the selected period (in red), or by identifying outlier buildings where no AI-driven issues were raised, therefore indicating locations that are likely to be persistently experiencing poor performance for a given KPI.

Figure 5.3: AI Network Analytics Onboarding Time Baseline



Cisco DNA Center

Assurance • AI Network Analytics • Baselines

SUMMARY

62 Buildings, 2 Impacted

9 WLCs

AI DRIVEN ISSUES

2 Onboarding Issues

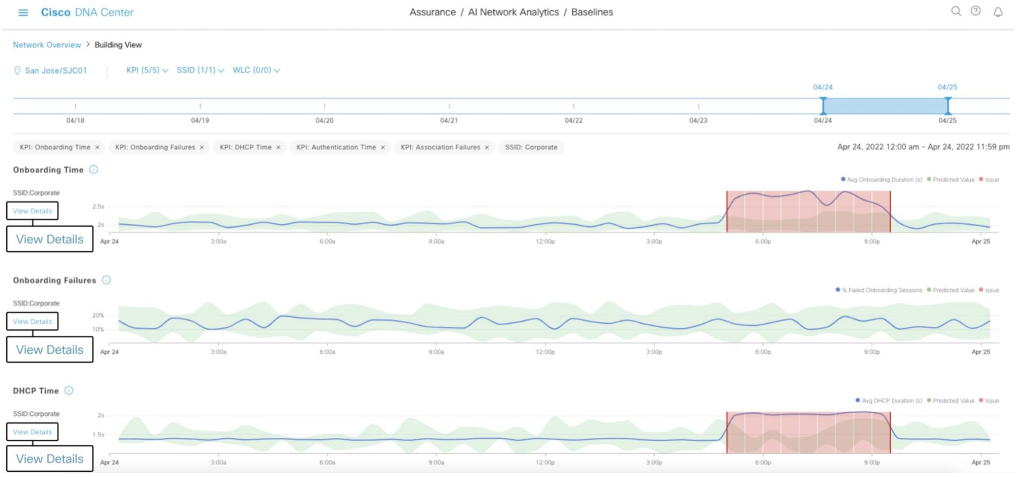
How do you find this section ?

Global | 24 hours | Apr 24, 2022

KPI: Onboarding Time

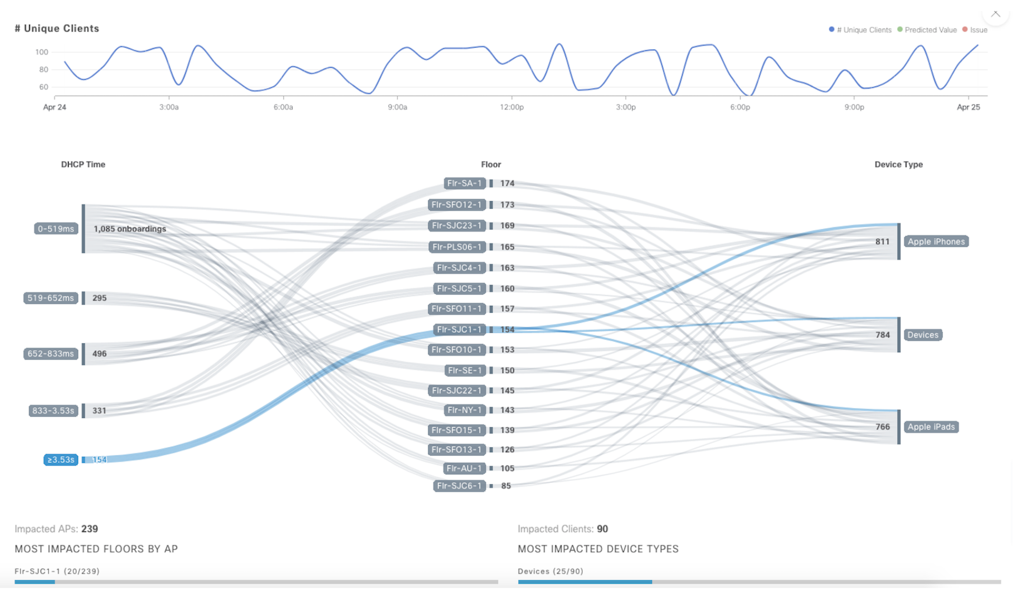
Selecting one of the `red bubbles` displays the details related to the selected building. This example in the figure below shows that the onboarding time was outside of the baseline from about 5pm to 9:15pm at this particular location. During that same period, DHCP Time was also outside of the baseline. This indicates that DHCP Time caused the onboarding time issue.

Figure 5.4: Baselines



Select the `View Details` under DHCP Time in the figure above to get more information to narrow down the DHCP issue. In the drill-down view, the network engineer can view the DHCP Time on the left side of the diagram. Hovering over the `highest DHCP Time` highlights the floors and clients that are affected. In the figure below, only clients on one floor are affected by the issue. The ability of Cisco DNA Center AI to correlate KPIs enables the network engineer to quickly troubleshoot onboarding issues.

Figure 5.5: DHCP Time Flow



Impacted APs: **239**

MOST IMPACTED FLOORS BY AP

Flr-SJC1-1 (20/239)

Impacted Clients: **90**

MOST IMPACTED DEVICE TYPES

Devices (25/90)

AP Performance Advisories

The Access Point (AP) Performance Advisories use machine learning to continually analyze APs with suboptimal client experience. The generated insights present extensive information about the potential root causes and provide suggestions for improvements by comparing the problematic radios with reference radios delivering good performance within the customer's network.

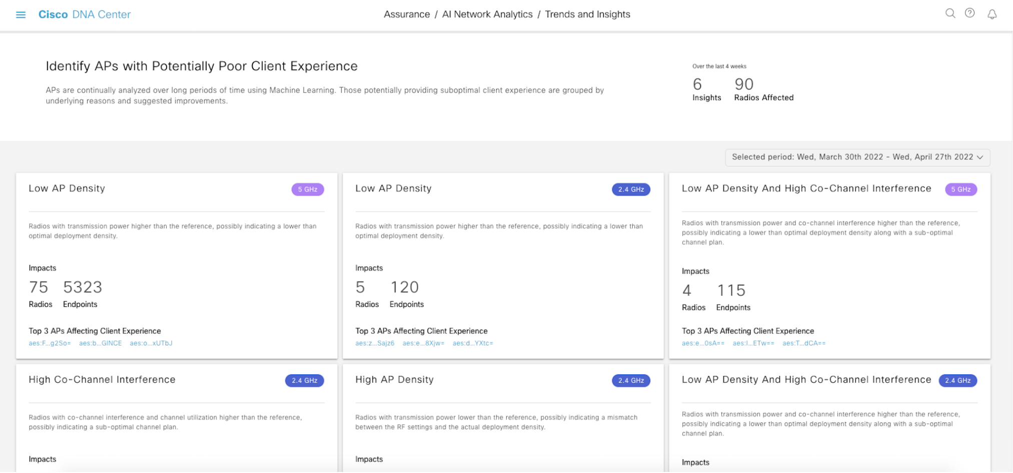
Upon opening the main page, the user is presented with a set of cards, each representing the suspected root cause for poor client experience, describing the identified problem along with the impact, in terms of the number of affected radios and clients.

The problems detected include RF-related issues such as channel utilization and Co-Channel Interference, as well as deployment-specific issues, such as low coverage due to AP density, or capacity issues, for example when APs are overloaded.

The radios included in these insights are among the most active on the network. To reduce noise, there is a filtering step as part of the data-processing pipeline removing APs with low activity.

The network operator can view details about the radios affected by issues such as Low AP Density and High Co-Channel Interference to proactively remedy problems before more users are impacted.

Figure 5.6: AP Performance Advisories



Identify APs with Potentially Poor Client Experience

APs are continually analyzed over long periods of time using Machine Learning. Those potentially providing suboptimal client experience are grouped by underlying reasons and suggested improvements.

Over the last 4 weeks

6 Insights 90 Radios Affected

Selected period: Wed, March 30th 2022 - Wed, April 27th 2022

Low AP Density — 5 GHz

Radios with transmission power higher than the reference, possibly indicating a lower than optimal deployment density.

Impacts

75 Radios 5323 Endpoints

Top 3 APs Affecting Client Experience

aes:F...g2So= aes:b...GINCE aes:o...xUTbJ

Low AP Density — 2.4 GHz

Radios with transmission power higher than the reference, possibly indicating a lower than optimal deployment density.

Impacts

5 Radios 120 Endpoints

Top 3 APs Affecting Client Experience

aes:z...Sajz6 aes:e...8Xjw= aes:d...YXtc=

Low AP Density And High Co-Channel Interference — 5 GHz

Radios with transmission power and co-channel interference higher than the reference, possibly indicating a lower than optimal deployment density along with a sub-optimal channel plan.

Impacts

4 Radios 115 Endpoints

Top 3 APs Affecting Client Experience

aes:e...0sA== aes:l...ETw== aes:T...dCA==

High Co-Channel Interference — 2.4 GHz

Radios with co-channel interference and channel utilization higher than the reference, possibly indicating a sub-optimal channel plan.

Impacts

High AP Density — 2.4 GHz

Radios with transmission power lower than the reference, possibly indicating a mismatch between the RF settings and the actual deployment density.

Impacts

Low AP Density And High Co-Channel Interference — 2.4 GHz

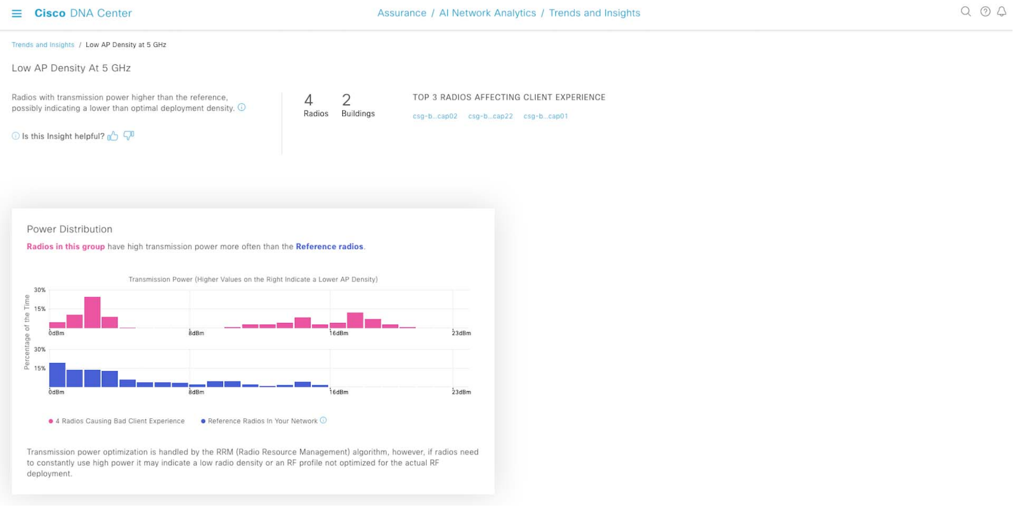
Radios with transmission power and co-channel interference higher than the reference, possibly indicating a lower than optimal deployment density along with a sub-optimal channel plan.

Impacts

Drilling down into the `Low AP Density` insight, this view shows there are a large number of APs with a higher transmission power than the reference radios. This also shows the number of radios showing bad client experience which could be caused by Low AP density.

The root cause presented in this view is automatically generated, based on the output of a machine learning pipeline, providing a weighted list of KPIs contributing to poor client experience. This allows network engineers to understand the problem by providing human-readable descriptions and take action to resolve the issue.

Figure 5.7: Low AP Density


Cisco DNA Center
Assurance / AI Network Analytics / Trends and Insights
Trends and Insights / Low AP Density at 5 GHz

Low AP Density At 5 GHz

Radios with transmission power higher than the reference, possibly indicating a lower than optimal deployment density.

Is this Insight helpful?

4 Radios 2 Buildings

TOP 3 RADIOS AFFECTING CLIENT EXPERIENCE

csg-b...cap02 csg-b...cap22 csg-b...cap01

Power Distribution

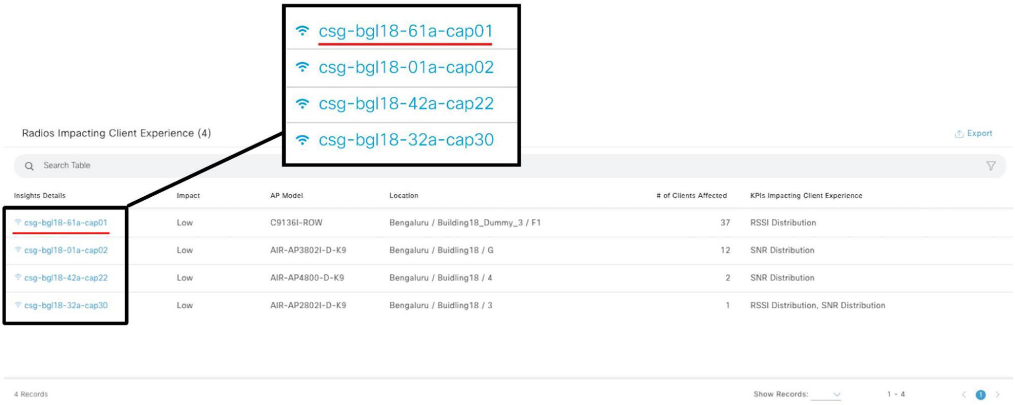
Radios in this group have high transmission power more often than the Reference radios.

Transmission Power (Higher Values on the Right Indicate a Lower AP Density)
Percentage of the Time
30%
15%
0dBm
8dBm
16dBm
23dBm
30%
15%
0dBm
8dBm
16dBm
23dBm
● 4 Radios Causing Bad Client Experience
● Reference Radios In Your Network

Transmission power optimization is handled by the RRM (Radio Resource Management) algorithm, however, if radios need to constantly use high power it may indicate a low radio density or an RF profile not optimized for the actual RF deployment.

At the bottom of the page, the user is presented with the full list of problematic radios. The list is by default sorted by impact, which is a function of the client experience KPIs and the affected clients. Once the user identifies a problematic radio to look at, they can click on the `AP name` and reach the radio-specific detailed view.

Figure 5.8: Radios Impacting Client Experience



Radios Impacting Client Experience (4)

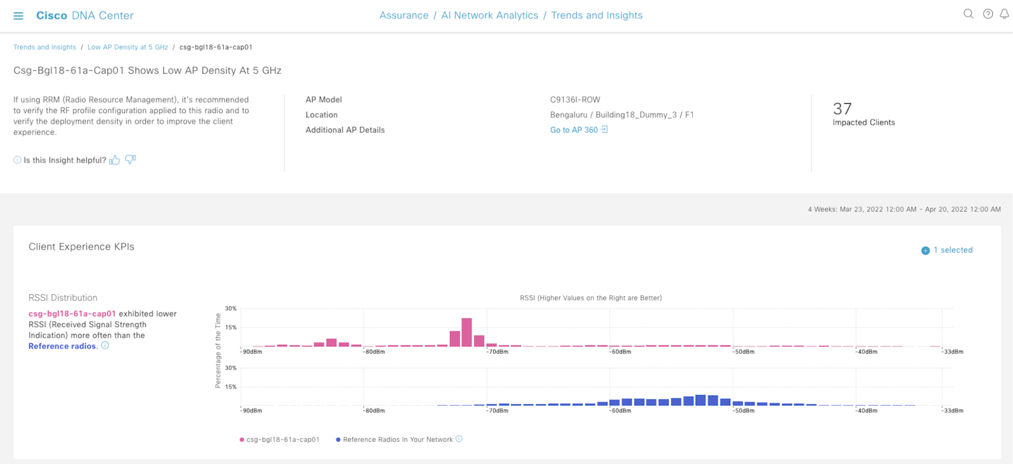
Insights Details	Impact	AP Model	Location	# of Clients Affected	KPIs Impacting Client Experience
csg-bgl18-61a-cap01	Low	C9136I-ROW	Bengaluru / Building18_Dummy_3 / F1	37	RSSI Distribution
csg-bgl18-01a-cap02	Low	AIR-AP3802I-D-K9	Bengaluru / Buidling18 / G	12	SNR Distribution
csg-bgl18-42a-cap22	Low	AIR-AP4800-D-K9	Bengaluru / Buidling18 / 4	2	SNR Distribution
csg-bgl18-32a-cap30	Low	AIR-AP2802I-D-K9	Bengaluru / Buidling18 / 3	1	RSSI Distribution, SNR Distribution

4 Records

Show Records: 1 - 4

Drilling down into one of the `radios` displays radio-specific trends and insights related to client experience KPIs, such as Received Signal Strength Indicator (RSSI) and Signal-to-Noise Ratio (SNR). These KPIs are shown between this radio and the reference radios for comparison. This radio has lower RSSI and SNR than the reference radios. This could be caused by low AP density in that location.

Figure 5.9: Client Experience KPIs



Cisco DNA Center

Assurance / AI Network Analytics / Trends and Insights

Trends and Insights / Low AP Density at 5 GHz / csg-bgl18-61a-cap01

Csg-Bgl18-61a-Cap01 Shows Low AP Density At 5 GHz

If using RRM (Radio Resource Management), it's recommended to verify the RF profile configuration applied to this radio and to verify the deployment density in order to improve the client experience.

Is this Insight helpful?

AP Model	C9136I-ROW
Location	Bengaluru / Building18_Dummy_3 / F1
Additional AP Details	Go to AP 360

37
Impacted Clients

4 Weeks: Mar 23, 2022 12:00 AM - Apr 20, 2022 12:00 AM

Client Experience KPIs

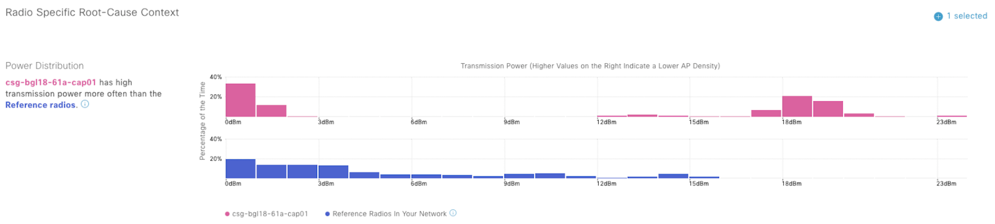
1 selected

RSSI Distribution

csg-bgl18-61a-cap01 exhibited lower RSSI (Received Signal Strength Indication) more often than the Reference radios.

Additionally, there is a Radio Specific Root-Cause Context page that shows this radio’s transmit power compared to the transmit power settings of the reference radios. If this radio’s power is higher than the reference radios, it can indicate there is low AP density as well.

Figure 5.10: Radio Specific Root Cause Context



Radio Specific Root-Cause Context

Power Distribution

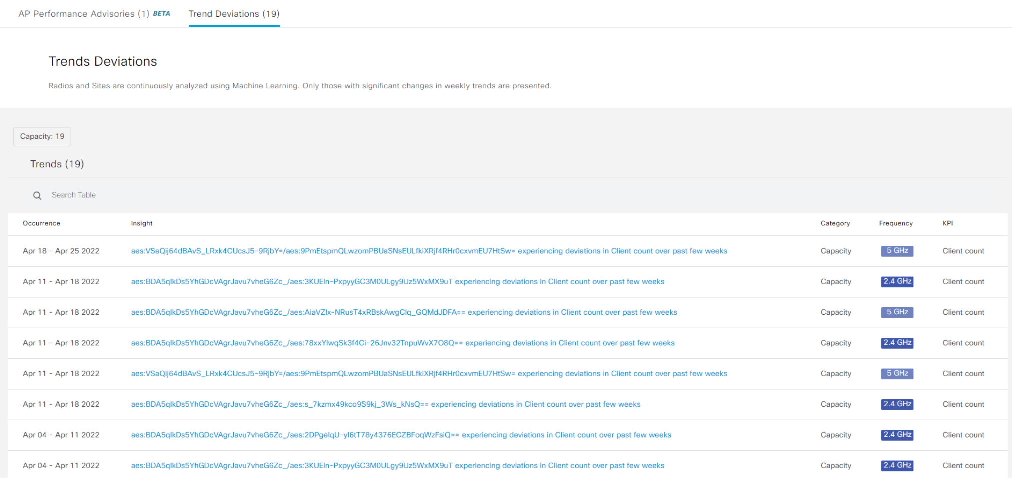
csg-bgl18-61a-cap01 has high transmission power more often than the **Reference radios.**

The network engineer can also dig into the other insights shown on the AP Advisories page and detect lower-performing APs quickly. This feature allows the network engineer to do something that is humanly not possible, but with the help of machine learning and big data, Cisco DNA Center AIOps brings these insights to the network engineer.

Trend Deviations

The Trend Deviations feature tracks a variety of metrics such as client count and radio throughput over several weeks. It uses machine learning to detect deviations in these trends during a 4-week period. A graph illustrates the deviation for the period selected for further analysis by a network engineer. The network engineer can select the system-generated insight to view it in a graphical format.

Figure 5.11: Trend Deviations



AP Performance Advisories (1) BETA | Trend Deviations (19)

Trends Deviations

Radios and Sites are continuously analyzed using Machine Learning. Only those with significant changes in weekly trends are presented.

Capacity: 19

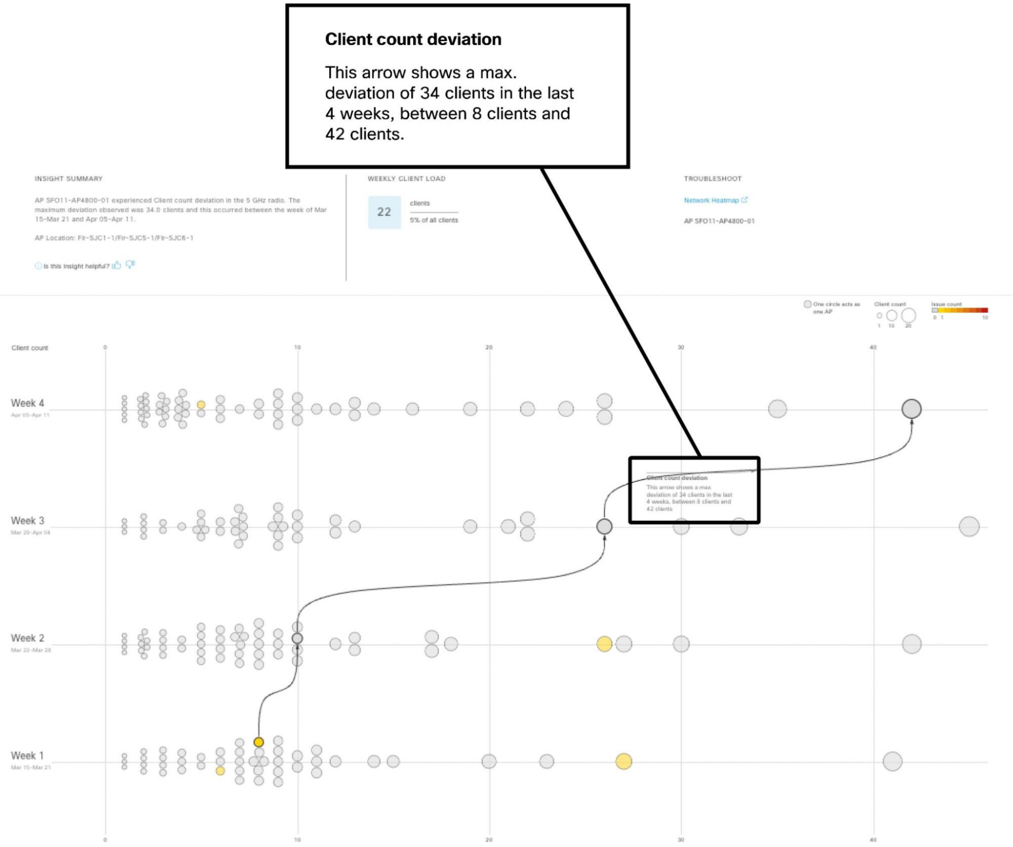
Trends (19)

Search Table

Occurrence	Insight	Category	Frequency	KPI
Apr 18 - Apr 25 2022	aes:VSaQij64dBAvS_LRxk4CUcsJ5-9RjbY=/aes:9PmEtspmQLwzomPBUaSNsEULfkiXRjf4RHr0cxvmEU7HtSw= experiencing deviations in Client count over past few weeks	Capacity	5 GHz	Client count
Apr 11 - Apr 18 2022	aes:BDA5qlkDs5YhGDcVAgrJavu7vheG6Zc_/aes:3KUEln-PxpyyGC3M0ULgy9Uz5WxMX9uT experiencing deviations in Client count over past few weeks	Capacity	2.4 GHz	Client count
Apr 11 - Apr 18 2022	aes:BDA5qlkDs5YhGDcVAgrJavu7vheG6Zc_/aes:AiaVZlx-NRusT4xRBskAwgClq_GQMdJDFA== experiencing deviations in Client count over past few weeks	Capacity	5 GHz	Client count
Apr 11 - Apr 18 2022	aes:BDA5qlkDs5YhGDcVAgrJavu7vheG6Zc_/aes:78xxYlwqSk3f4Ci-26Jnv32TnpuWvX7O8Q== experiencing deviations in Client count over past few weeks	Capacity	2.4 GHz	Client count
Apr 11 - Apr 18 2022	aes:VSaQij64dBAvS_LRxk4CUcsJ5-9RjbY=/aes:9PmEtspmQLwzomPBUaSNsEULfkiXRjf4RHr0cxvmEU7HtSw= experiencing deviations in Client count over past few weeks	Capacity	5 GHz	Client count
Apr 11 - Apr 18 2022	aes:BDA5qlkDs5YhGDcVAgrJavu7vheG6Zc_/aes:s_7kzmx49kco9S9kj_3Ws_kNsQ== experiencing deviations in Client count over past few weeks	Capacity	2.4 GHz	Client count
Apr 04 - Apr 11 2022	aes:BDA5qlkDs5YhGDcVAgrJavu7vheG6Zc_/aes:2DPgelqU-yl6tT78y4376ECZBFoqWzFsiQ== experiencing deviations in Client count over past few weeks	Capacity	2.4 GHz	Client count
Apr 04 - Apr 11 2022	aes:BDA5qlkDs5YhGDcVAgrJavu7vheG6Zc_/aes:3KUEln-PxpyyGC3M0ULgy9Uz5WxMX9uT experiencing deviations in Client count over past few weeks	Capacity	2.4 GHz	Client count

This figure demonstrates Cisco DNA Center's ability to detect a change in behavior where a given AP significantly increases its client count over a 4-week period. These types of insights are almost impossible without the use of AI. The figure below displays trends over a 4-week period for a particular AP for client count.

Figure 5.12: Trend Deviation – Client Count



Client count deviation

This arrow shows a max. deviation of 34 clients in the last 4 weeks, between 8 clients and 42 clients.

INSIGHT SUMMARY

AP SFO11-AP4800-01 experienced Client count deviation in the 5 GHz radio. The maximum deviation observed was 34.0 clients and this occurred between the week of Mar 15-Mar 21 and Apr 05-Apr 11.

AP Location: Flr-SJC1-1/Flr-SJC5-1/Flr-SJC6-1

Is this insight helpful?

WEEKLY CLIENT LOAD

22 clients

5% of all clients

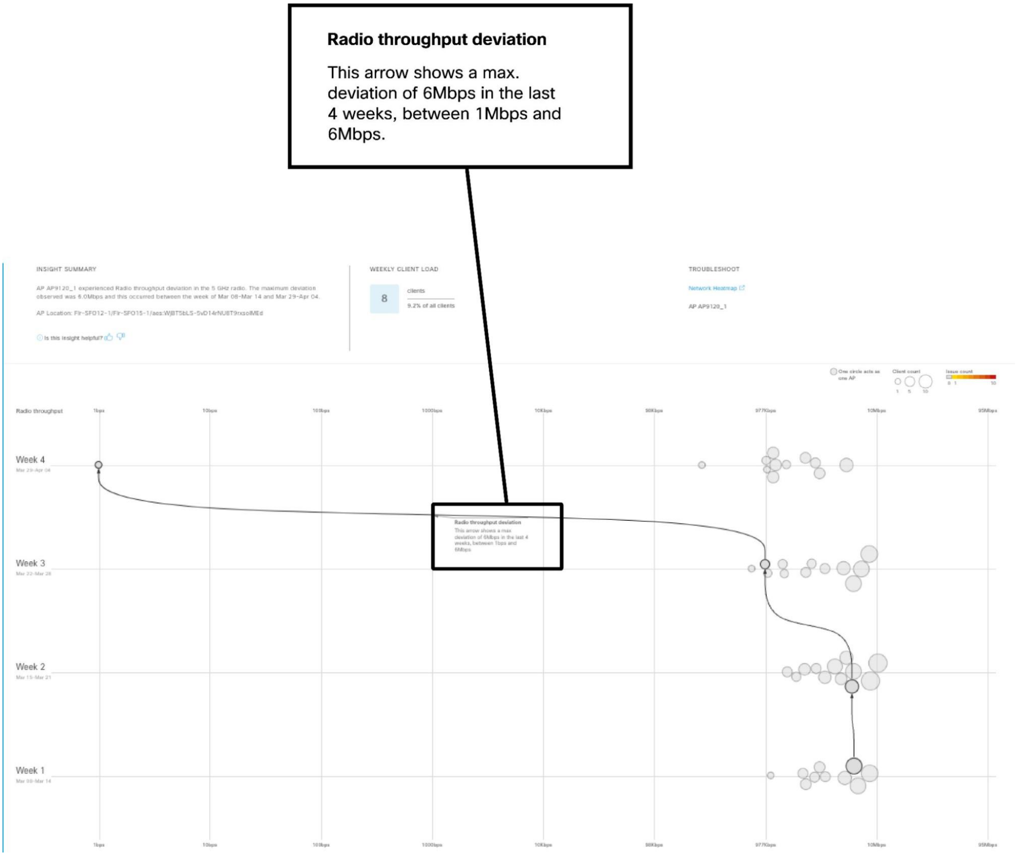
TROUBLESHOOT

Network Heatmap

AP SFO11-AP4800-01

The figure below shows another system-generated insight, AP throughput deviation. The view demonstrates Cisco DNA Center's ability to detect and point out a change in system behavior where a given AP significantly decreases its throughput over four weeks. This could be indicative of a configuration issue or hardware issue which would normally not be visible in a traditional network management system without the insights that AI provides. These insights enable the network engineer to quickly investigate an area or an AP based on a throughput decrease.

Figure 5.13: Trend Deviation – Radio Throughput



Radio throughput deviation

This arrow shows a max. deviation of 6Mbps in the last 4 weeks, between 1Mbps and 6Mbps.

INSIGHT SUMMARY

AP AP9120_1 experienced Radio throughput deviation in the 5 GHz radio. The maximum deviation observed was 6.0Mbps and this occurred between the week of Mar 08-Mar 14 and Mar 29-Apr 04.

AP Location: Flr-SFO12-1/Flr-SFO15-1/aes:WJBT5bLS-5vD14rNU8T9rxsolMEd

Is this insight helpful?

WEEKLY CLIENT LOAD

8 clients

9.2% of all clients

TROUBLESHOOT

Network Heatmap

AP AP9120_1

Radio throughput deviation

This arrow shows a max deviation of 6Mbps in the last 4 weeks, between 1bps and 6Mbps

AI Enhanced RRM

AI Enhanced RRM (Radio Resource Management) is the next evolution of Cisco's award-winning RRM. RRM was originally introduced with Cisco AireOS and Aironet in 2005 and manages the complexities of RF from Wi-Fi 1 to Wi-Fi 6 and now Wi-Fi 6E. RRM has fluidly grown to include innovative algorithms such as Flexible Radio Architecture (FRA) and Dynamic Bandwidth Selection (DBS) in addition to the traditional algorithms of Dynamic Channel Assignment (DCA) and Transmit Power Control (TPC).

On a Cisco Catalyst 9800 WLC, RRM runs as a service. Cisco RRM manages the RF Group (the components making up the RF Network) based on dynamic measurements between every AP and its neighbors, stored in a local database for the entire RF Group. At runtime, RRM draws on the last 10 minutes of collected data, and optimizes based on the current network conditions. Cisco RRM has proven to be extremely effective and trustworthy over the years, when configured correctly for the type of RF network coverage desired (Capacity vs Coverage) it can adapt to almost any size or deployment density. In Wi-Fi, RF Conditions can and do dynamically change with different network loads and numbers of devices and users in the environment, and RRM has measured up well to this task.

AI Enhanced RRM integrates the power of AI and ML with the reliable and trusted Cisco RRM product family of algorithms in the cloud. AI Enhanced RRM is coordinated through Cisco's DNA Center as a service. Existing Cisco Catalyst 9800 WLC RRM sites can be seamlessly transitioned to an intelligent centralized service. As with other Cisco DNA Center services, AI Enhanced RRM brings a host of new features. The Cisco DNA Center RRM Control Center allows administrators to quickly assess the health and performance of the RF coverage from the enterprise level down to a single site or building level.

Cisco AI Enhanced RRM is different as it brings the ability to analyze historical dynamic RF data over time. The ability to evaluate complex RF data often comes down to being able to factor in what's normal against the current data. **Normal** can and does vary from site to site based on the numbers and types of users, technology, equipment choices, and the architectural design density. Keep in mind that often normal is in the mind of the beholder.

After an initial learning period of a few days, the Cisco AI Analytics Cloud will begin to provide insights into the performance and tuning of the RF network. Insights provide granular guidance on:

- Performance against SLAs
- The effectiveness of present settings/configurations
- The quality of the coverage

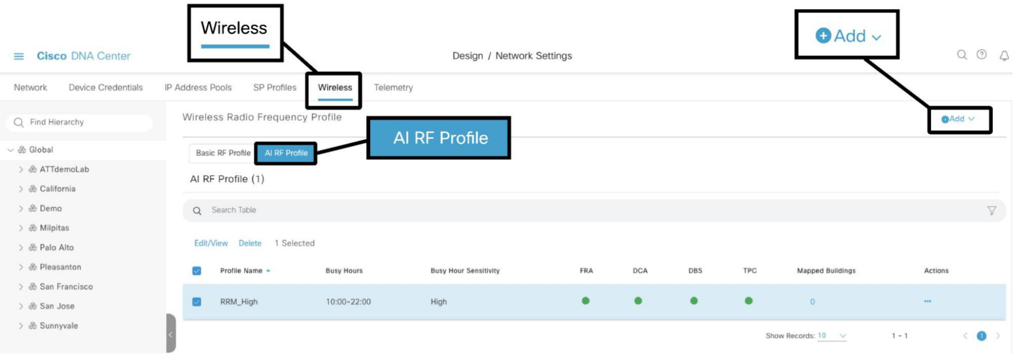
Together, the AI Enhanced RRM algorithms with the power of the Cisco AI Analytics Cloud and Cisco's DNA Center take Wi-Fi RF management to an unprecedented level. AI Enhanced RRM correlates 24x7 observations from the network and the client devices and applies 20+ years of Cisco RF excellence to drive exceptional user experiences into the future.

To get started with AI Enhanced RRM in Cisco DNA Center, there are some prerequisites:

- Cisco DNA Center running version 2.3.2 or higher.
- A Cisco Catalyst 9800 WLC (**MUST** be provisioned by Cisco DNA Center), running IOS XE 17.7 or higher.
- A large number (10+ at a minimum, the more the better) of APs connected to the Catalyst 9800 WLC.
- Cisco AI Analytics and AI Enhanced RRM are enabled under **Cisco AI Analytics** in the Cisco DNA Center System Settings.

After these requirements have been met, an AI RF profile can be created on Cisco DNA Center by navigating to `Design > Network Settings > Wireless` (with **global** location scope selected) then scrolling down to **RF Profile** and selecting `Add` then selecting the `AI RF Profile` tab as shown in the figure below.

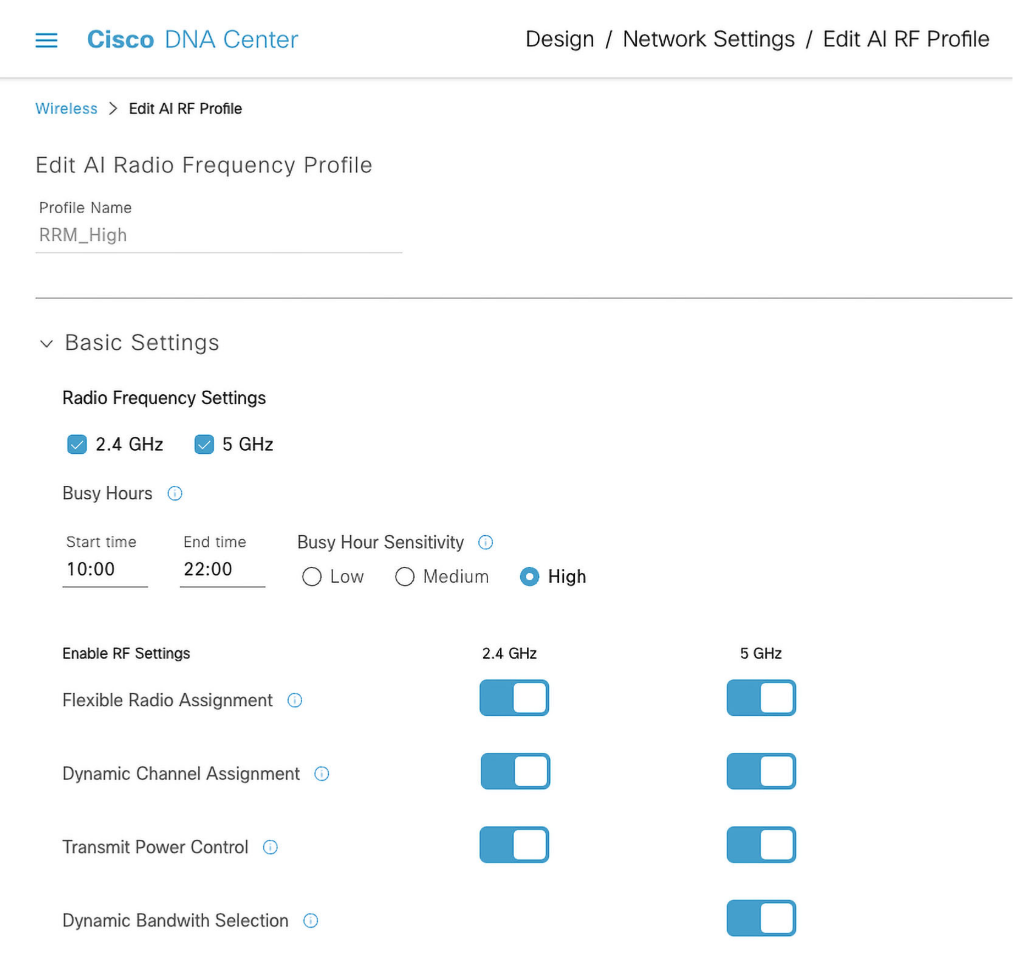
Figure 5.14: New AI RF Profile



☑	Profile Name	Busy Hours	Busy Hour Sensitivity	FRA	DCA	DBS	TPC	Mapped Buildings	Actions
☑	RRM_High	10:00-22:00	High	●	●	●	●	0	...

Configure a name for the profile as well as enable/disable any default RF settings. Set the Busy Hours and Busy Hours Sensitivity based on the organization's needs. Busy Hours refer to the set period during each day that RRM changes should not be implemented.

Figure 5.14: Set RRM Busy Hours



☰ Cisco DNA Center
Design / Network Settings / Edit AI RF Profile
Wireless > Edit AI RF Profile

Edit AI Radio Frequency Profile

Profile Name
RRM_High

Basic Settings

Radio Frequency Settings

☑ 2.4 GHz ☑ 5 GHz

Busy Hours

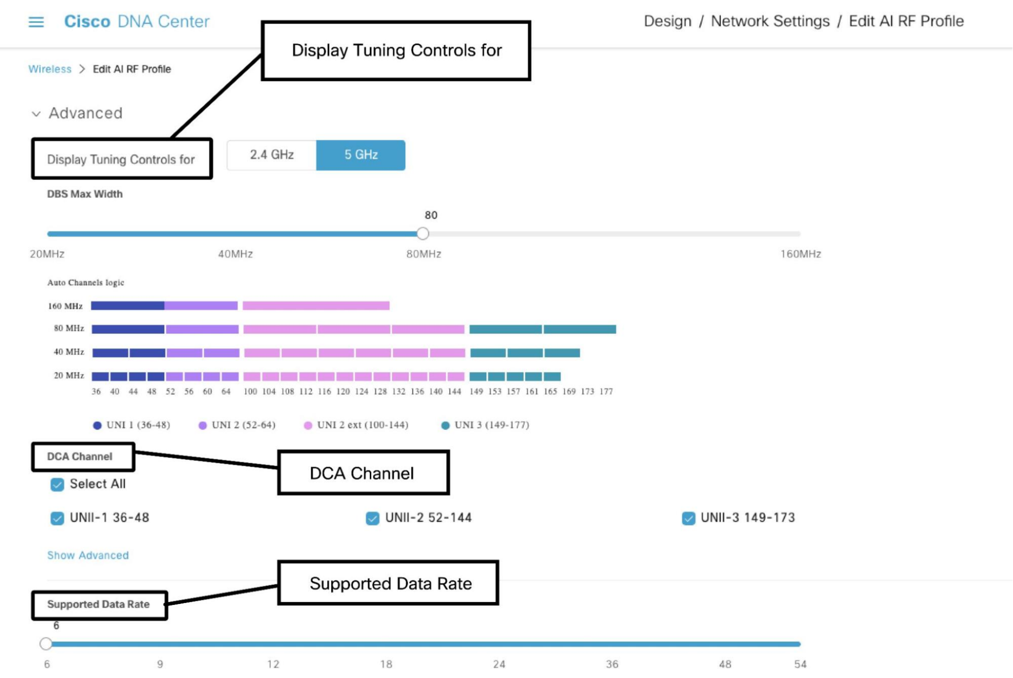
Start time 10:00
End time 22:00

Busy Hour Sensitivity
○ Low ○ Medium ● High

Enable RF Settings	2.4 GHz	5 GHz
Flexible Radio Assignment	●	●
Dynamic Channel Assignment	●	●
Transmit Power Control	●	●
Dynamic Bandwith Selection		●

Next, configure any advanced settings, such as which channels to utilize or Tx power, then save the new AI RF Profile.

Figure 5.15: RRM Advanced Profile Settings



Cisco DNA Center

Design / Network Settings / Edit AI RF Profile

Wireless > Edit AI RF Profile

Advanced

Display Tuning Controls for: 2.4 GHz | **5 GHz**

DBS Max Width: 80

DCA Channel

☑ Select All

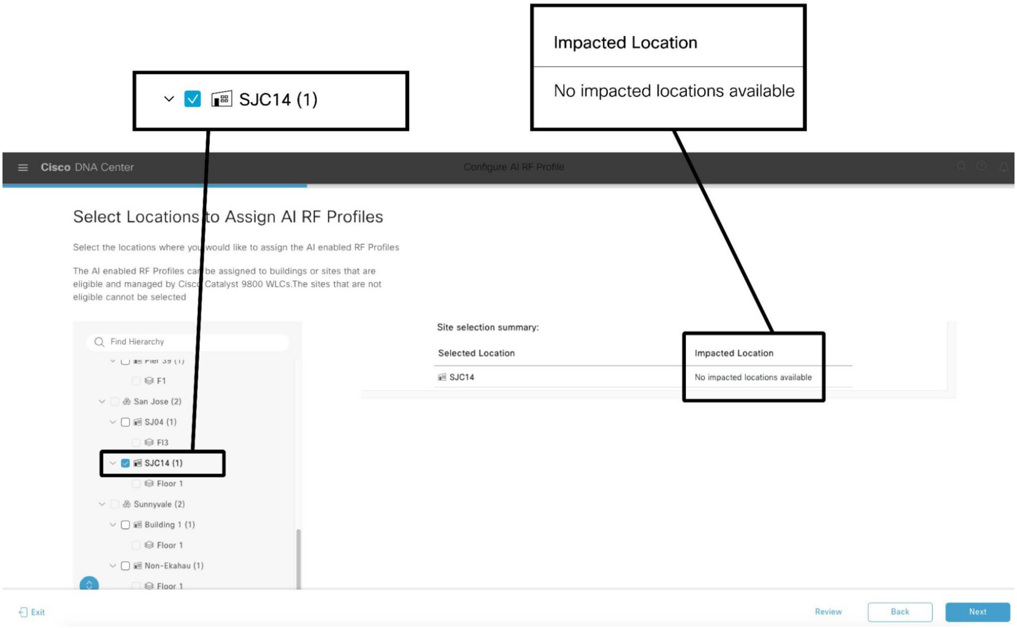
☑ UNII-1 36-48 ☑ UNII-2 52-144 ☑ UNII-3 149-173

Show Advanced

Supported Data Rate: 6

Now that the AI RF Profile has been created, it can be deployed to a site. To do this, navigate to the `Workflows` tab in the Cisco DNA Center main menu, and select the `Configure AI RF Profile` ;workflow. Give the workflow a name then select the site(s) to where the AI RF Profile will be deployed.

Figure 5.16: Assign AI RF Profile to Site



Select Locations to Assign AI RF Profiles

Select the locations where you would like to assign the AI enabled RF Profiles

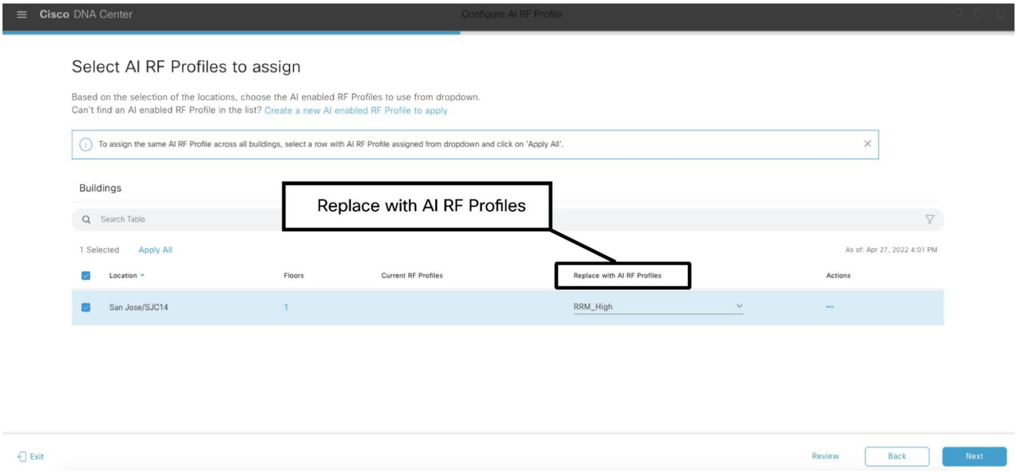
The AI enabled RF Profiles can be assigned to buildings or sites that are eligible and managed by Cisco Catalyst 9800 WLCs.The sites that are not eligible cannot be selected

Site selection summary:

Selected Location	Impacted Location
SJC14	No impacted locations available

On this page, different AI RF Profiles can be assigned to multiple sites in one workflow.

Figure 5.17: Select AI RF Profile



Select AI RF Profiles to assign

Based on the selection of the locations, choose the AI enabled RF Profiles to use from dropdown.
Can't find an AI enabled RF Profile in the list? Create a new AI enabled RF Profile to apply

To assign the same AI RF Profile across all buildings, select a row with AI RF Profile assigned from dropdown and click on 'Apply All'.

Buildings

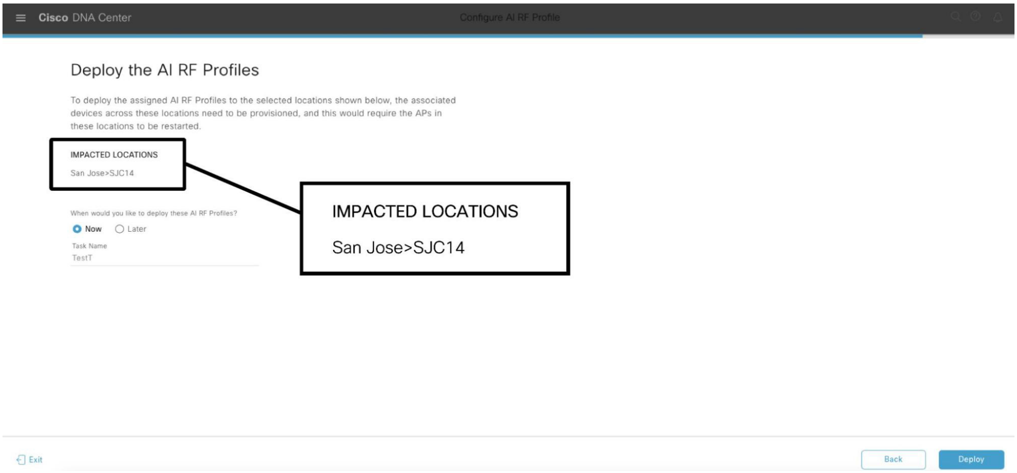
1 Selected Apply All

As of: Apr 27, 2022 4:01 PM

☑	Location	Floors	Current RF Profiles	Replace with AI RF Profiles	Actions
☑	San Jose/SJC14	1		RRM_High	···

The RF profile can either be deployed immediately or scheduled for a later time. Choose an option then click `Deploy`. A success message will indicate that the AI RF profile was deployed.

Figure 5.18: Schedule AI RF Profile Deployment



Deploy the AI RF Profiles

To deploy the assigned AI RF Profiles to the selected locations shown below, the associated devices across these locations need to be provisioned, and this would require the APs in these locations to be restarted.

IMPACTED LOCATIONS

San Jose>SJC14

When would you like to deploy these AI RF Profiles?

● Now ○ Later

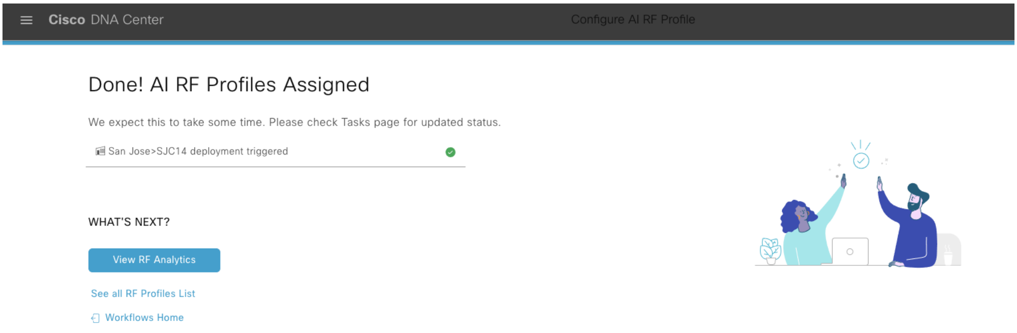
Task Name

TestT

IMPACTED LOCATIONS

San Jose>SJC14

Figure 5.19: AI RF Profile Assigned



Done! AI RF Profiles Assigned

We expect this to take some time. Please check Tasks page for updated status.

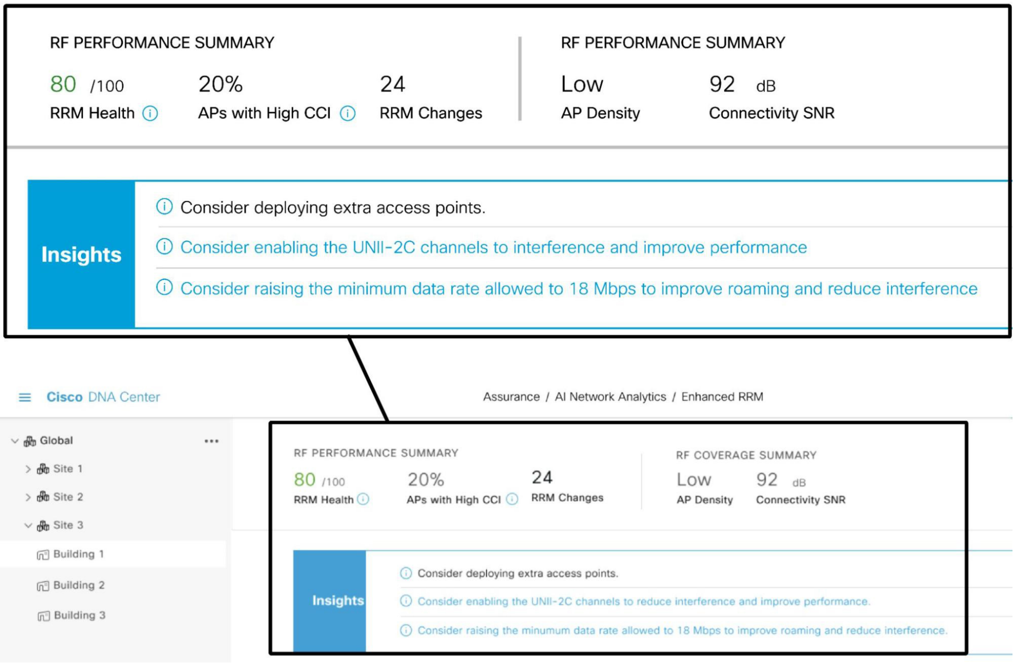
San Jose>SJC14 deployment triggered ✓

WHAT'S NEXT?

Once the profile has been deployed, it will take a few hours before data starts to populate on the **Enhanced RRM** page. The Enhanced RRM page can be found in `Assurance > Enhanced RRM` under the Cisco DNA Center main menu. Select a site from the menu on the left. At the top of the page is the RF Performance Summary which displays the overall RRM health percentage and number of RRM changes for the period selected. There is also an RF Coverage Summary which provides the current AP Density and connectivity Signal-To-Noise Ratio (SNR).

Below the summaries, AI Enhanced RRM truly distinguishes itself from Cisco's already powerful industry-leading RRM by harnessing Cisco DNA Center's AI and ML components along with the ability to store and use historical telemetry data and establish what is *normal* for a given observation over time. RRM on the controller has always been limited to viewing the current conditions as the data storage requirements are quite high.

Figure 5.20: Enhanced RRM Insights



RF PERFORMANCE SUMMARY

80 /100 RRM Health

20% APs with High CCI

24 RRM Changes

RF PERFORMANCE SUMMARY

Low AP Density

92 dB Connectivity SNR

Insights

- Consider deploying extra access points.
- Consider enabling the UNII-2C channels to interference and improve performance
- Consider raising the minimum data rate allowed to 18 Mbps to improve roaming and reduce interference

RF PERFORMANCE SUMMARY

80 /100 RRM Health

20% APs with High CCI

24 RRM Changes

RF COVERAGE SUMMARY

Low AP Density

92 dB Connectivity SNR

Insights

- Consider deploying extra access points.
- Consider enabling the UNII-2C channels to reduce interference and improve performance.
- Consider raising the minumum data rate allowed to 18 Mbps to improve roaming and reduce interference.

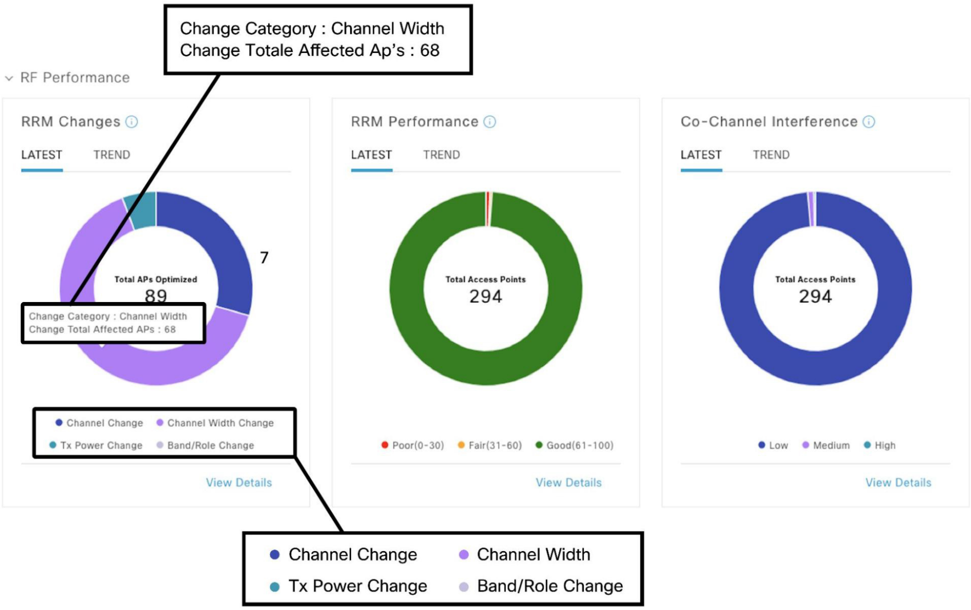
In addition to these insights, the Enhanced RRM page provides a series of dashlets that can help a network engineer easily visualize RF performance and coverage:

- **RRM Changes**: The total number of RRM changes performed during the selected time interval, broken down by type of change completed (Tx Power, Channel Change).
- **RRM Performance**: Measures how the RRM performance channel changes over time by observing metrics from co-channel interference, near-channel interference, and duty cycle.

- **Co-Channel Interference**: A breakdown of co-channel interference levels (low/medium/high) for all wireless access points at this site.

The network engineer can select View Details to view more detailed information on actionable insights for each category powered by AIOps.

Figure 5.21: AI Enhanced RRM Changes



Change Category : Channel Width
Change Totale Affected Ap's : 68

● Channel Change ● Channel Width
● Tx Power Change ● Band/Role Change

The Enhanced RRM page also provides more detailed dashlets that show more detailed statistics regarding the metrics measured to determine RRM changes:

- **Utilization per Channel**: Shows per-channel utilization. Trend allows visualization of history for up to two weeks. Selecting a time on the trend line opens the detail for that point in time, listing the contributing access points.
- **AP and Radar per Channel**: Breaks out the channel assignment spread by access point count. Radar detected is displayed on impacted channels for context.
- **AP Spatial Density**: Visualizes Neighboring AP/radio density in the RF neighborhood as the number of neighbors that can be seen at or above -70 dBm.
- **Power Distribution**: Visualizes power distribution across the networks and provides a corresponding neighbor count to correlate AP density with power assignments. Trend allows visualization of history for up to two weeks. Selecting a time on the trend line opens the detail for that point in time, listing the contributing APs.

Figure 5.22: Per Channel Metrics

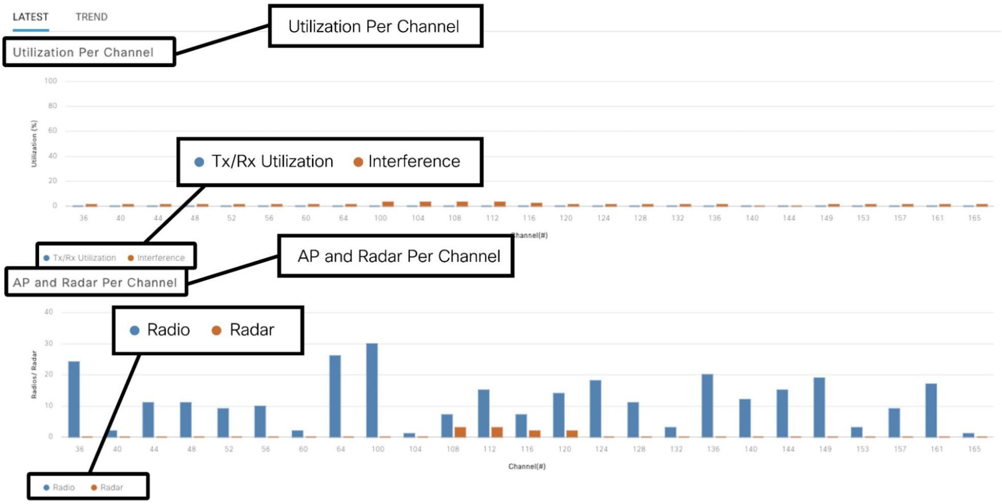
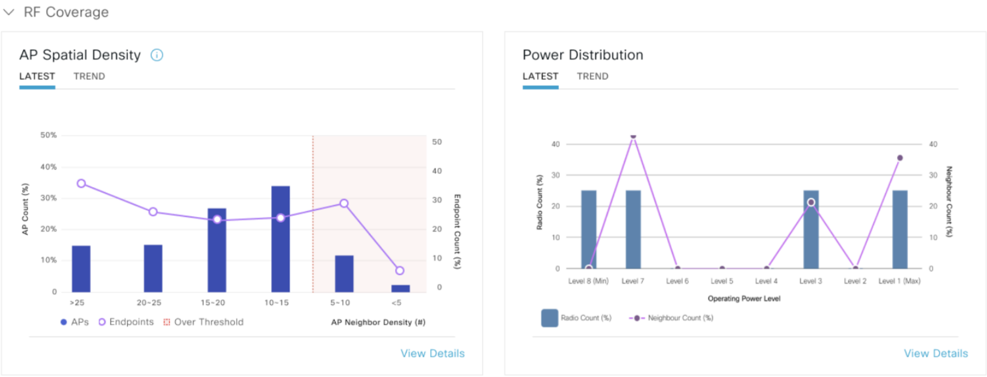


Figure 5.23: AP Spatial Density and Power Distribution Comparative Analytics



AI Network Comparative Analytics

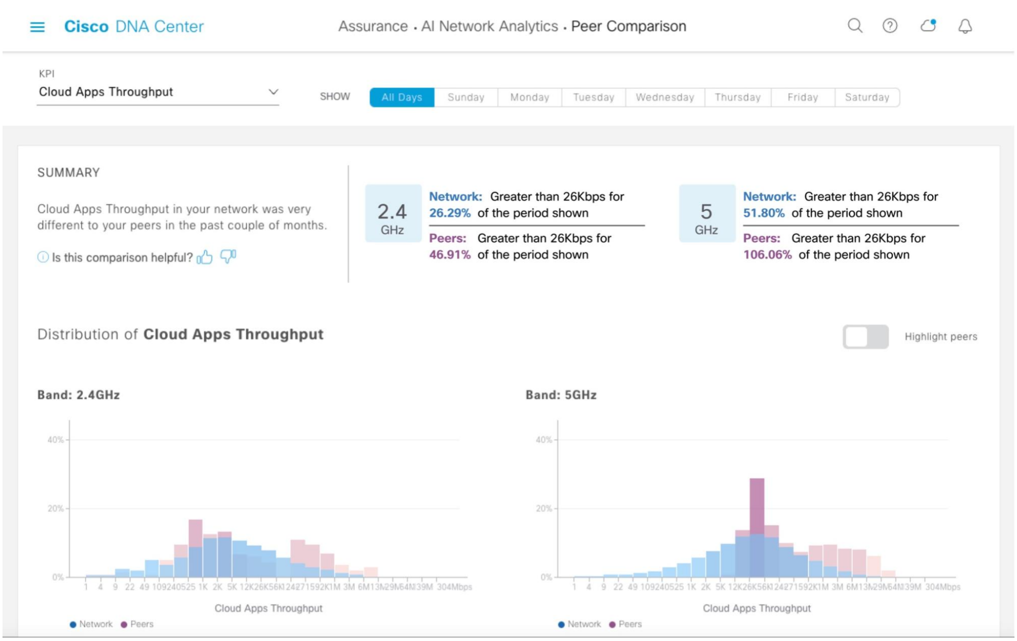
Peer Comparison

Peer comparison provides the ability to compare KPIs such as Cloud Apps Throughput and various RF KPIs, such as co-channel interference, between peers in similar vertical market segments. This can provide insightful information regarding how the network performs against an industry baseline.

Peer comparison baselines include:

- Radio throughput
- Cloud apps throughput
- Radio reset
- Packet failure rate
- Radio interference
- RSSI (Received Signal Strength Indicator)

Figure 5.24: Peer Comparison



Cisco DNA Center

Assurance • AI Network Analytics • Peer Comparison

KPI
Cloud Apps Throughput

SHOW: All Days | Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday

SUMMARY

Cloud Apps Throughput in your network was very different to your peers in the past couple of months.

Is this comparison helpful?

2.4 GHz
Network: Greater than 26Kbps for 26.29% of the period shown
Peers: Greater than 26Kbps for 46.91% of the period shown

5 GHz
Network: Greater than 26Kbps for 51.80% of the period shown
Peers: Greater than 26Kbps for 106.06% of the period shown

Distribution of **Cloud Apps Throughput**

Highlight peers

Band: 2.4GHz
40%
20%
0%
1 4 9 22 49 109240525 1K 2K 5K 12K26K56K124271592K1M 3M 6M13M29M64M139M 304Mbps
Cloud Apps Throughput
● Network ● Peers
Band: 5GHz
40%
20%
0%
1 4 9 22 49 109240525 1K 2K 5K 12K26K56K124271592K1M 3M 6M13M29M64M139M 304Mbps
Cloud Apps Throughput
● Network ● Peers

Network Comparison

Compare buildings, endpoints, and AP models across a variety of key wireless metrics such as radio throughput, average onboarding time, and channel utilization across a period of one week.

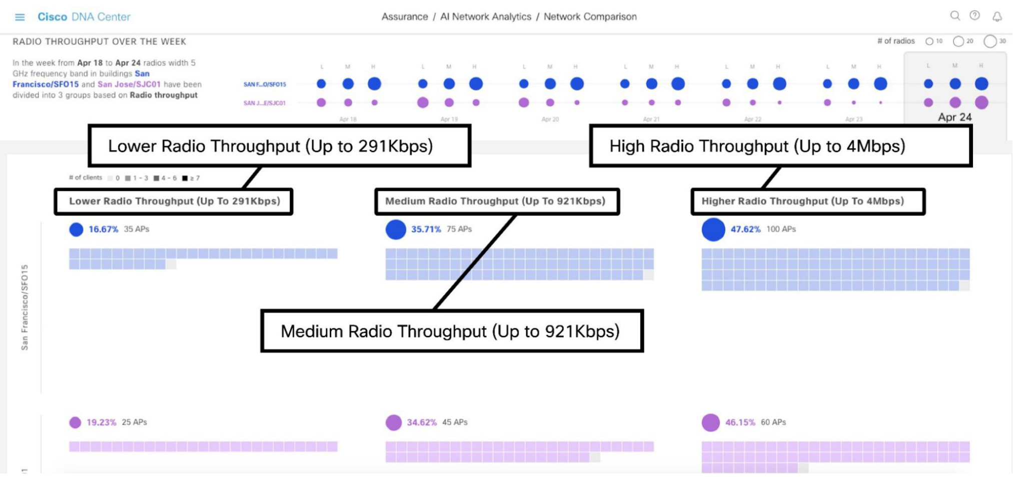
The Network Comparison view can be used to compare:

- Buildings
- AP models
- Endpoint/Client types

The devices are grouped into three categories making use of clustering techniques to automatically determine lower, medium, and high thresholds for the relevant KPIs.

This approach provides a full breakdown of the performance in each category. The categories are across a period of one week as well as in comparison with another building, endpoint, or AP model. This is particularly useful in planning new AP deployments and upgrades, as the page can show the progress of the deployment during the week, in addition to viewing how these wireless metrics are improved by the upgrades.

Figure 5.25: Network Comparison



RADIO THROUGHPUT OVER THE WEEK

In the week from **Apr 18** to **Apr 24** radios width 5 GHz frequency band in buildings **San Francisco/SFO15** and **San Jose/SJC01** have been divided into 3 groups based on **Radio throughput**

Lower Radio Throughput (Up to 291Kbps)

High Radio Throughput (Up to 4Mbps)

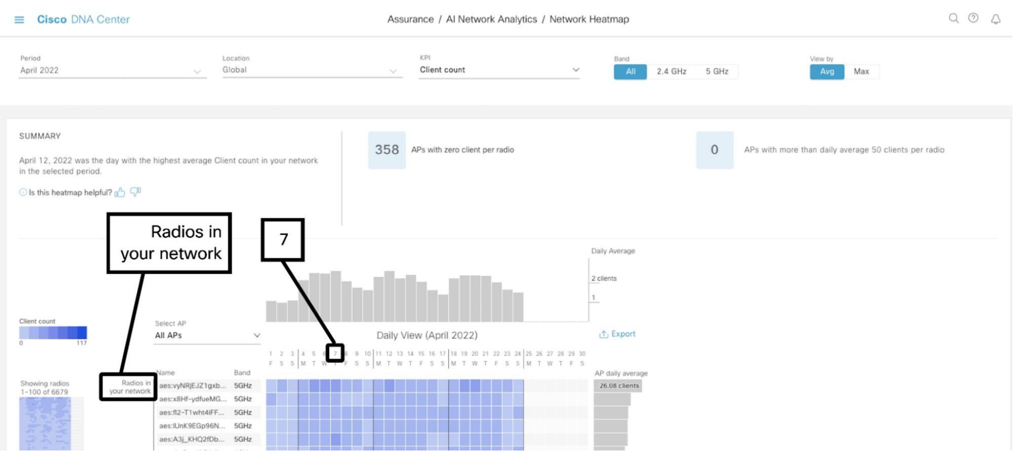
Medium Radio Throughput (Up to 921Kbps)

Cisco DNA Center
Assurance / AI Network Analytics / Network Comparison
# of radios ○ 10 ○ 20 ○ 30
L M H
SAN F...O/SFO15
SAN J...E/SJC01
Apr 18
Apr 19
Apr 20
Apr 21
Apr 22
Apr 23
Apr 24
# of clients 0 1 - 3 4 - 6 ≥ 7
Lower Radio Throughput (Up To 291Kbps)
Medium Radio Throughput (Up To 921Kbps)
Higher Radio Throughput (Up To 4Mbps)
16.67% 35 APs
35.71% 75 APs
47.62% 100 APs
San Francisco/SFO15
19.23% 25 APs
34.62% 45 APs
46.15% 60 APs

Network Heatmap

The network heatmap provides a list of all wireless APs in the network. They are ordered by the KPI selected, such as Client Count, Throughput, or Interference. This allows quick identification of top and bottom performing APs as well as spotting trends concerning those specific KPIs. The list shows the daily average (as well as the min/max) for all APs under the selected KPI, in decreasing order. Hovering over one of the `APs` for any given day provides the average value for that day, allowing the network engineer to see changes in the wireless network over time. The network heatmap allows the network engineer to visualize data from the current month as well as all previous months in which data was collected and processed, with available filters by site or band, to go from a global to a more specific view in the hierarchy. The network heatmap can also be exported for use offline and outside of Cisco DNA Center. Clicking on any of the dates will take the network engineer to an hourly view for that day for this KPI, giving an even more granular view for more detailed analysis.

Figure 5.26: Network Heatmap



Cisco DNA Center

Assurance / AI Network Analytics / Network Heatmap

Period: April 2022

Location: Global

KPI: Client count

Band: All | 2.4 GHz | 5 GHz

View by: Avg | Max

SUMMARY

April 12, 2022 was the day with the highest average Client count in your network in the selected period.

Is this heatmap helpful?

358 APs with zero client per radio

0 APs with more than daily average 50 clients per radio

Select AP: All APs

Showing radios 1-100 of 6679

Name	Band
aes:vyNRjEJZ1gxb...	5GHz
aes:x8Hf-ydfueMG...	5GHz
aes:fl2-T1wht4iFF...	5GHz
aes:lUnK9EGp96N...	5GHz
aes:A3j_KHQ2fDb...	5GHz

This chapter reviewed all the AI Network Analytics features, demonstrating the value of the insights it brings to the network engineer. This enables quick troubleshooting and the ability to identify issues and KPIs not possible to generate without Cisco's industry-leading AI Network Analytics engine.

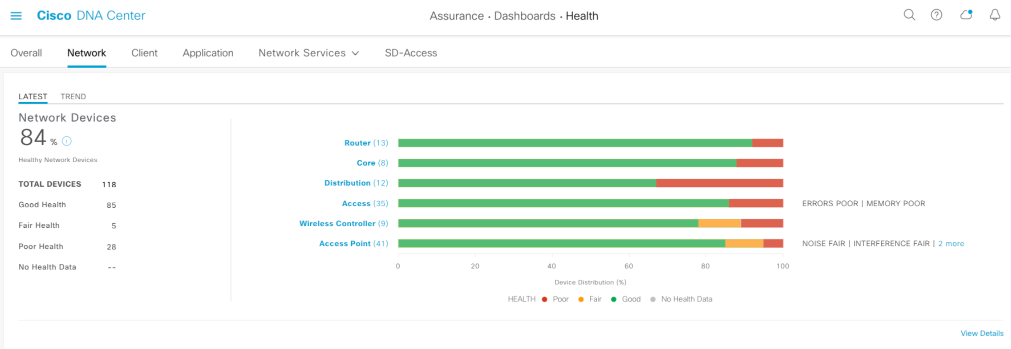
6. Wireless Monitoring

This chapter covers how to monitor the most visible aspect of the enterprise network. As the wireless network is where all the users live, it is important to learn how Cisco DNA Center can help network engineers monitor the wireless network to quickly and easily resolve issues reducing the MTTR for wireless issues and ensuring a superior user experience.

Network Health

The Network Health page provides visibility for all network devices managed by Cisco DNA Center. With this tool, a network engineer can easily identify any potential problems that may occur with the network devices across the entire infrastructure.

Figure 6.1: Network Health



Network Devices

84 %

Healthy Network Devices

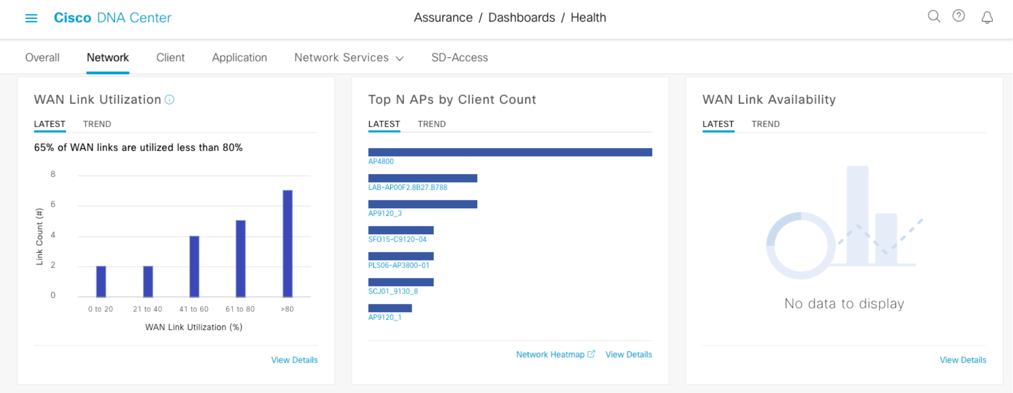
TOTAL DEVICES	118
Good Health	85
Fair Health	5
Poor Health	28
No Health Data	--

The Network Health page can be filtered by site or building, similar to the Overall Health page as demonstrated in **Chapter 4**. The Healthy Network Devices percentage is the number of devices in Good Health compared to the number of Total Devices. The Total Devices are further broken down into Good Health, Fair Health, Poor Health, and No Health data. This page also provides a chart separating Routers, Core switches, Distribution switches, Access switches, WLCs, and APs. Each device type's health percentage is also shown broken down by color.

Scrolling down the Network Health page will show a collection of dashlets, as shown below. While the dashlets are customizable, it is important to note that each dashlet provides two perspectives: **LATEST** and **TREND**. The

LATEST perspective displays the information for the previous 5 minutes. The TREND perspective displays information for the time period selected in the dashboard. For example, if the time period selected is 7 days, the TREND will show 7 days of data. This allows the network engineer to visualize the changes in the network to look for problems quickly and easily.

Figure 6.2: Network Health Dashlets



65% of WAN links are utilized less than 80%

No data to display

Figure 6.3: List of APs by Highest Client Count (in latest 5 mins)

This figure shows a dashlet with a list of APs with the highest Client Count for the last 5 minutes.

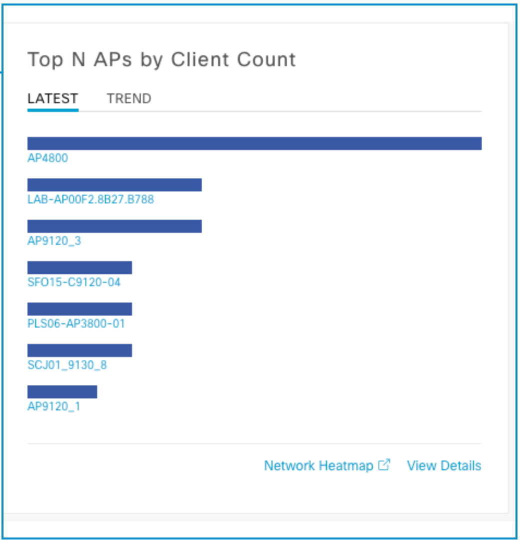
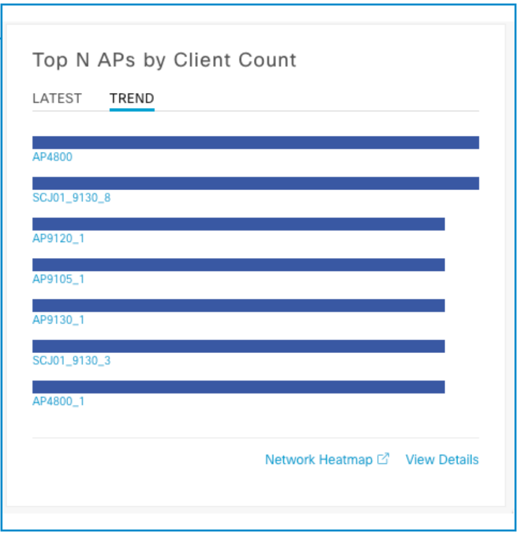


Figure 6.4: Trend Dashlet Network Health

This figure shows a list of APs from the `TREND` perspective with the highest client count for the last 24 hours.



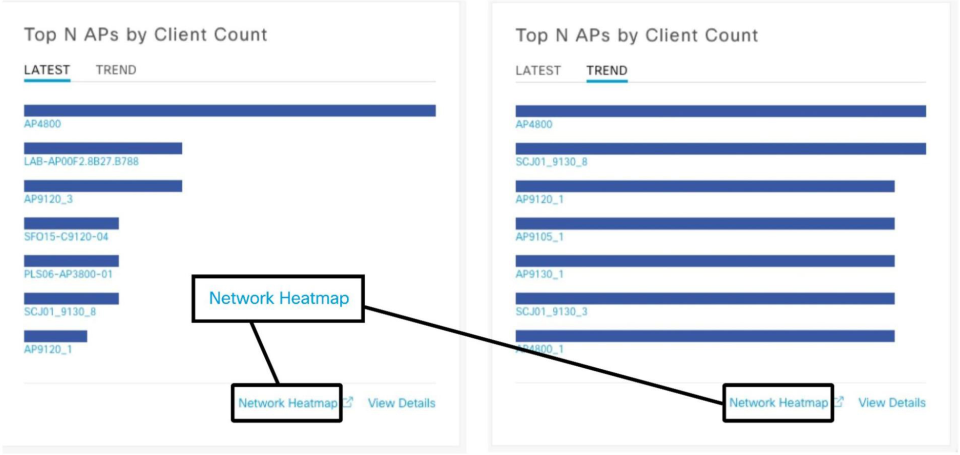
Top N APs by Client Count

Real-World Scenario

Saran is a wireless engineer at a large university. Saran likes to monitor the wireless network very carefully as it is the heart and soul of the students' access. As the university operates more than 5,000 wireless APs, Saran goes to the Network Health page where he can see 3 critical dashlets showing Total APs Up/Down, Top N APs by High Interference, and Top N APs by Client Count. Saran can see that all the wireless access points are up, have no significant issues with interference, and the client counts are in an acceptable range.

The below figure shows both the LATEST and TREND views for Top N APs by Client Count.

Figure 6.5: Top APs by Client Count



The figure below shows a dashlet with a list of Access Points with the highest Client Count for the last 5 minutes.

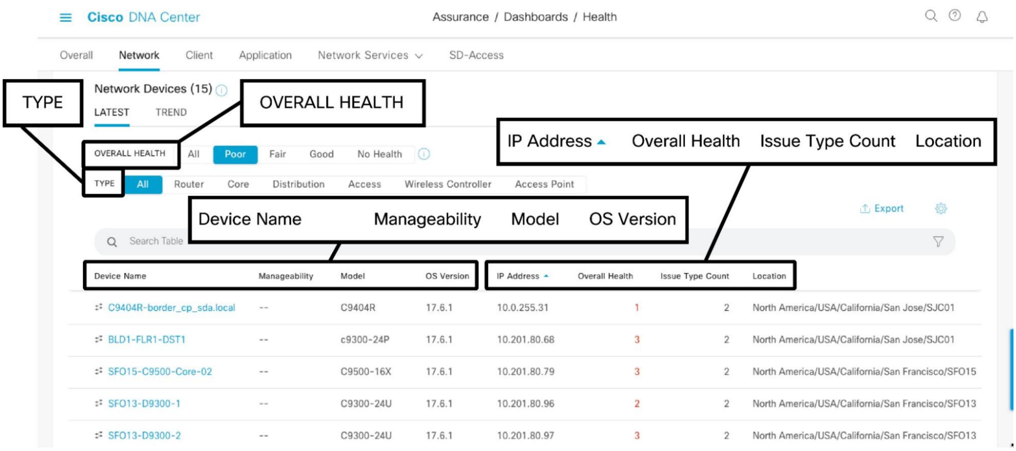
The figure below shows a list of Access Points from the TREND perspective with the highest client count for the last 24 hours.

On top of the LATEST and TREND tabs in this example, the user can reach the `Network Heatmap` (discussed in the previous chapter) directly from the above dashlet, highlighting the Top N APs and allowing a comparison of such APs with the rest of the network, as well as extending the visualization over a longer period. This feature can save time in understanding and planning for demand, and justification for a hardware refresh.

There are more dashlets available, in addition to the defaults. The dashboard can be customized by clicking the `Actions > Edit Dashboard` link. This provides a customizable set of metrics the network engineer is interested in viewing at a glance. Refer to the Cisco DNA Center user guide for the complete list of other dashlets available on this dashboard.

Scrolling further down the Network Health windows will display the **Network Devices** section of this dashboard which shows the device level details and additional information. This list can also be filtered based on Overall Health and Device Type.

Figure 6.6: Network Devices



Device Name	Manageability	Model	OS Version	IP Address ▲	Overall Health	Issue Type Count	Location
C9404R-border_cp_sda.local	--	C9404R	17.6.1	10.0.255.31	1	2	North America/USA/California/San Jose/SJC01
BLD1-FLR1-DST1	--	c9300-24P	17.6.1	10.201.80.68	3	2	North America/USA/California/San Jose/SJC01
SFO15-C9500-Core-02	--	C9500-16X	17.6.1	10.201.80.79	3	2	North America/USA/California/San Francisco/SFO15
SFO13-D9300-1	--	C9300-24U	17.6.1	10.201.80.96	2	2	North America/USA/California/San Francisco/SFO13
SFO13-D9300-2	--	C9300-24U	17.6.1	10.201.80.97	3	2	North America/USA/California/San Francisco/SFO13

The table above displays a wealth of information regarding the device. The columns shown can be edited by selecting the gear icon on the top right of the table. There are more than 20 different columns to choose from based on preference, making the dashlet highly customizable. The data in the dashlet can be exported as a CSV file to generate a report on the network devices with all the details. Some of the columns are listed below. Please refer to the Cisco DNA Center user guide for a list of all the columns available.

- Device name
- Manageability status
- Device model
- Device OS version
- Device IP address
- Overall health rating
- Issue type count
- Location of the device in the hierarchy

Click on the `Device Name` link to navigate to the **Device 360** page. The Device 360 is covered in detail in **Chapter 7**.

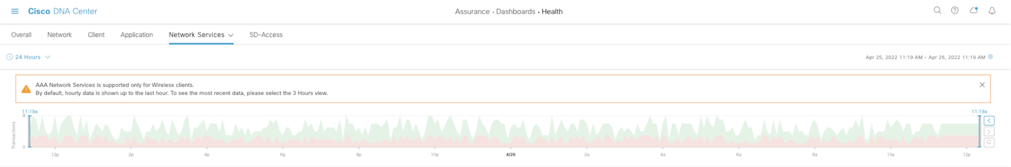
Network Services

Use of the Network Services dashboard can help the network engineer determine if a wireless issue is being caused by authentication issues or issues obtaining an IP Address. The Network Services menu has two dashboards, the AAA dashboard, and the DHCP dashboard. The information presented by these dashboards comes directly from the WLC via streaming telemetry. There is no need to separately configure AAA or DHCP within Cisco DNA Center to enable this telemetry.

AAA Dashboard

The AAA dashboard breaks down the performance of the network's AAA servers by latency and transactions. The timeline on the dashboard displays the number of AAA transaction failures and successes over the period selected. This timeline can be used to go back in time up to 30 days to view the historical data.

Figure 6.7: AAA Dashboard



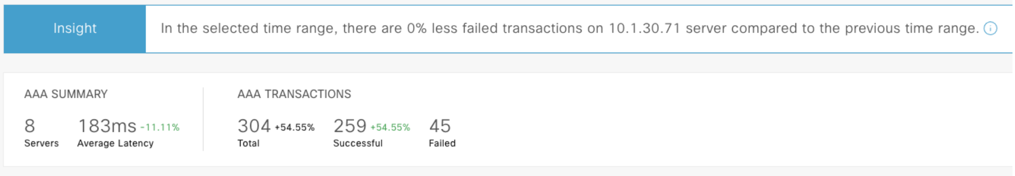
AAA Network Services is supported only for Wireless clients.
By default, hourly data is shown up to the last hour. To see the most recent data, please select the 3 Hours view.

The Insights section below the timeline displays the change in AAA server transactions compared to the same previous time range. For example, if the time range is 24 hours, then it displays the change in AAA transactions from the previous 24-hour period.

The next dashlet displays the AAA summary and the AAA transactions at a high level. The AAA summary shows the number of AAA servers and the average latency for authentication transactions across all AAA servers. The dashlet also displays the change in average latency from the previous 24-hour period. The AAA transactions section shows the Total number of transactions, number of Successful transactions, and number of Failed transactions across all AAA servers. The dashlet also displays the change in the number of successful and failed transactions from the previous 24-hour period.

If there is a high percentage increase in the number of failed transactions over the previous 24-hour period, it may indicate an issue that needs to be diagnosed.

Figure 6.8: AAA Insights



Insight In the selected time range, there are 0% less failed transactions on 10.1.30.71 server compared to the previous time range.

AAA SUMMARY

8 Servers

183ms -11.11% Average Latency

AAA TRANSACTIONS

304 +54.55% Total

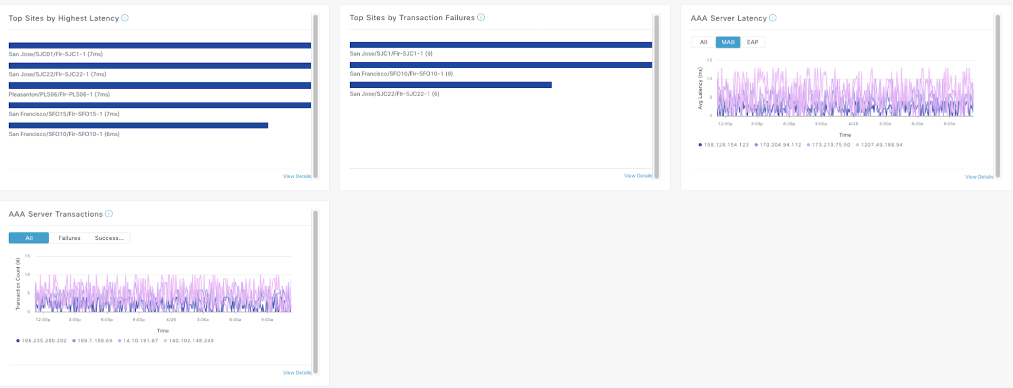
259 +54.55% Successful

45 Failed

The next section in the AAA dashboard displays four different dashlets:

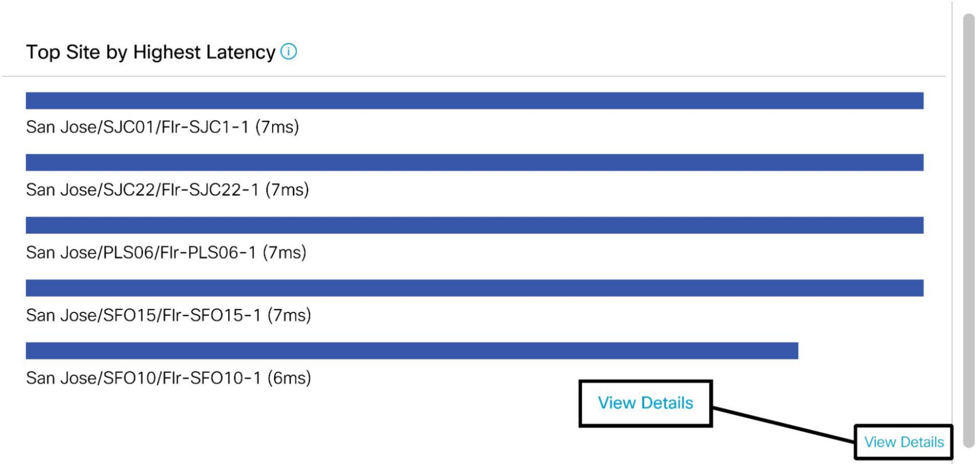
- Top N Sites by Highest Latency
- Top N Sites by Failed Transactions
- AAA Server Latency
- AAA Server Transactions

Figure 6.9: AAA Dashlets



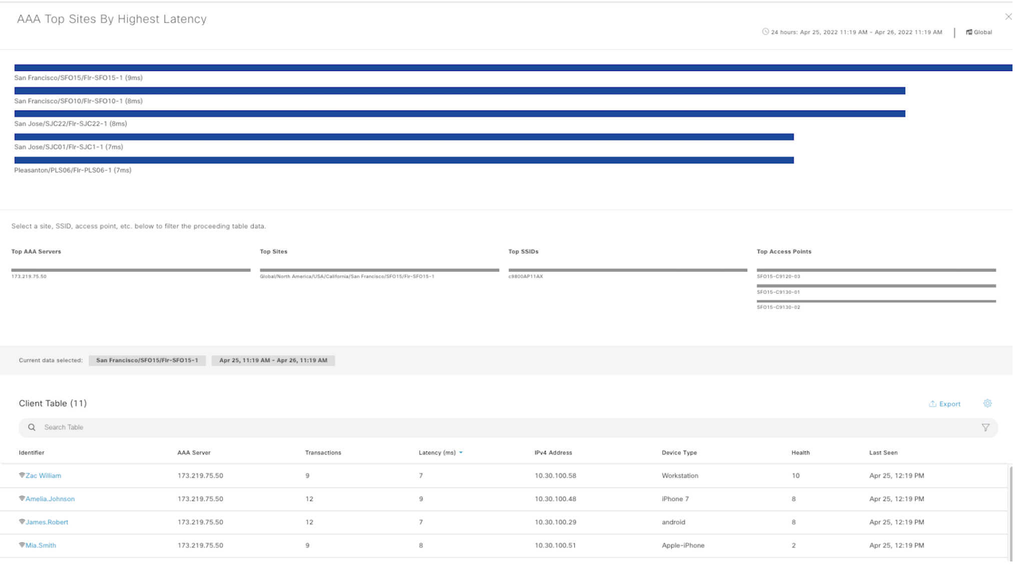
The AAA Latency is calculated as the average AAA round trip time from the WLC to the AAA server. The **Top N sites by Highest Latency** can be used to detect the most problematic sites for AAA issues. Selecting `View Details` on this dashlet can be used to drill down into the AAA data in more detail.

Figure 6.10: Top N Sites by Highest Latency


Top Site by Highest Latency
San Jose/SJC01/Flr-SJC1-1 (7ms)
San Jose/SJC22/Flr-SJC22-1 (7ms)
San Jose/PLS06/Flr-PLS06-1 (7ms)
San Jose/SFO15/Flr-SFO15-1 (7ms)
San Jose/SFO10/Flr-SFO10-1 (6ms)
View Details
View Details

When selecting one of the sites, the data can be filtered by **Top AAA Servers**, **Top SSIDs**, and **Top Access Points** contributing to the highest latency at the site. The dashlet displays the number of clients being affected by the filters selected. The information helps pinpoint the most problematic areas to help troubleshoot AAA issues affecting clients, quickly reducing MTTR.

Figure 6.11: View Details for Top N Sites by Highest Latency



AAA Top Sites By Highest Latency

24 hours: Apr 25, 2022 11:19 AM - Apr 26, 2022 11:19 AM | Global

San Francisco/SFO15/Flr-SFO15-1 (9ms)
San Francisco/SFO10/Flr-SFO10-1 (8ms)
San Jose/SJC22/Flr-SJC22-1 (8ms)
San Jose/SJC01/Flr-SJC1-1 (7ms)
Pleasanton/PLS06/Flr-PLS06-1 (7ms)

Select a site, SSID, access point, etc. below to filter the proceeding table data.

Top AAA Servers: 173.219.75.50

Top Sites: Global/North America/USA/California/San Francisco/SFO15/Flr-SFO15-1

Top SSIDs: c9800AP11AX

Top Access Points: SFO15-C9120-03, SFO15-C9130-01, SFO15-C9130-02

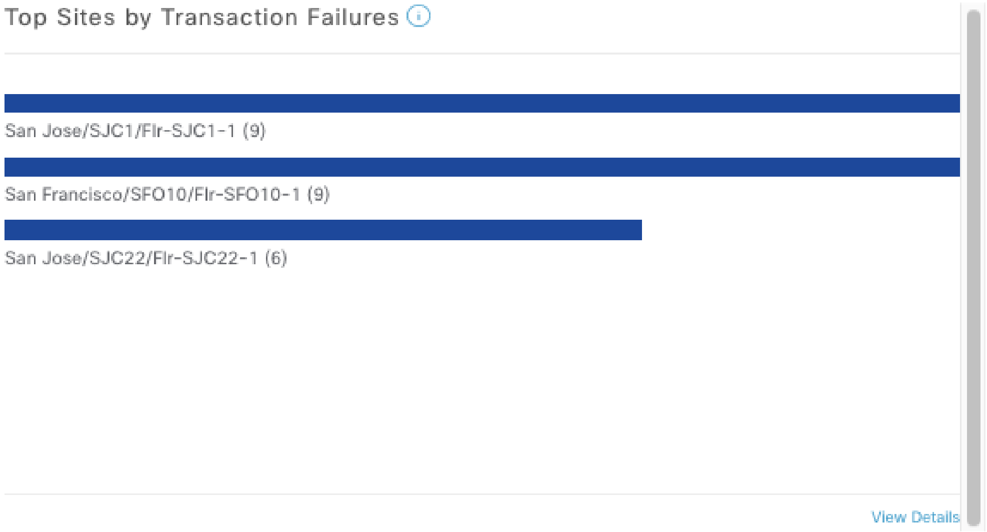
Current data selected: San Francisco/SFO15/Flr-SFO15-1 | Apr 25, 11:19 AM - Apr 26, 11:19 AM

Client Table (11)

Identifier	AAA Server	Transactions	Latency (ms)	IPv4 Address	Device Type	Health	Last Seen
Zac William	173.219.75.50	9	7	10.30.100.58	Workstation	10	Apr 25, 12:19 PM
Amelia.Johnson	173.219.75.50	12	9	10.30.100.48	iPhone 7	8	Apr 25, 12:19 PM
James.Robert	173.219.75.50	12	7	10.30.100.29	android	8	Apr 25, 12:19 PM
Mia.Smith	173.219.75.50	9	8	10.30.100.51	Apple-iPhone	2	Apr 25, 12:19 PM

The **Top N Sites by Transaction Failures** dashlet can similarly be used to pinpoint the most problematic areas to focus on troubleshooting for AAA issues. The dashlet allows a network engineer to instantly see if AAA issues are isolated to just one site or multiple sites.

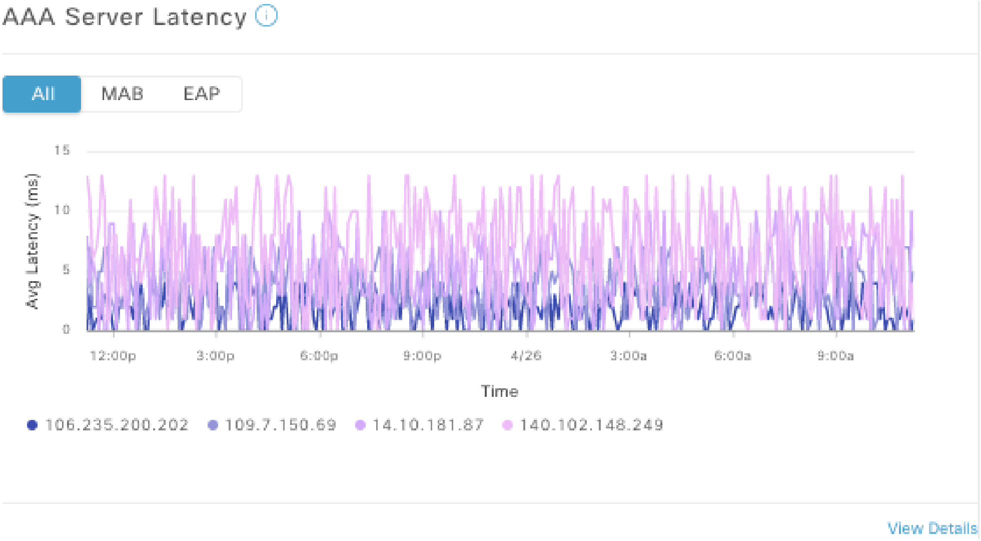
Figure 6.12: Top N Sites by Transaction Failures



Top Sites by Transaction Failures ⓘ
San Jose/SJC1/Flr-SJC1-1 (9)
San Francisco/SFO10/Flr-SFO10-1 (9)
San Jose/SJC22/Flr-SJC22-1 (6)
View Details

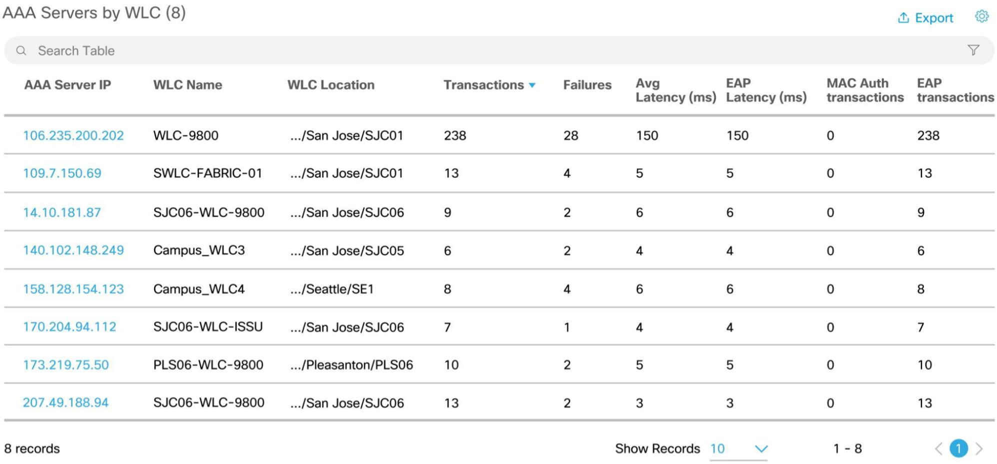
The dashlet figure below shows the average AAA server latency for each AAA server. The dashlet also breaks down the latency for the EAP and MAC Authentication Bypass (MAB) messages by each AAA server.

Figure 6.13: AAA Server Latency



The AAA dashboard also displays the list of AAA servers by WLC. The table shows a wealth of data such as the AAA server IP address, WLC Name, WLC Location, and the AAA transaction statistics such as the number of failures, successes, and latency for each AAA server. The AAA dashboard helps to isolate the top-used AAA servers and WLCs to monitor authentication performance.

Figure 6.14: AAA Servers by WLC



AAA Servers by WLC (8)

AAA Server IP	WLC Name	WLC Location	Transactions ▾	Failures	Avg Latency (ms)	EAP Latency (ms)	MAC Auth transactions	EAP transactions
106.235.200.202	WLC-9800	.../San Jose/SJC01	238	28	150	150	0	238
109.7.150.69	SWLC-FABRIC-01	.../San Jose/SJC01	13	4	5	5	0	13
14.10.181.87	SJC06-WLC-9800	.../San Jose/SJC06	9	2	6	6	0	9
140.102.148.249	Campus_WLC3	.../San Jose/SJC05	6	2	4	4	0	6
158.128.154.123	Campus_WLC4	.../Seattle/SE1	8	4	6	6	0	8
170.204.94.112	SJC06-WLC-ISSU	.../San Jose/SJC06	7	1	4	4	0	7
173.219.75.50	PLS06-WLC-9800	.../Pleasanton/PLS06	10	2	5	5	0	10
207.49.188.94	SJC06-WLC-9800	.../San Jose/SJC06	13	2	3	3	0	13

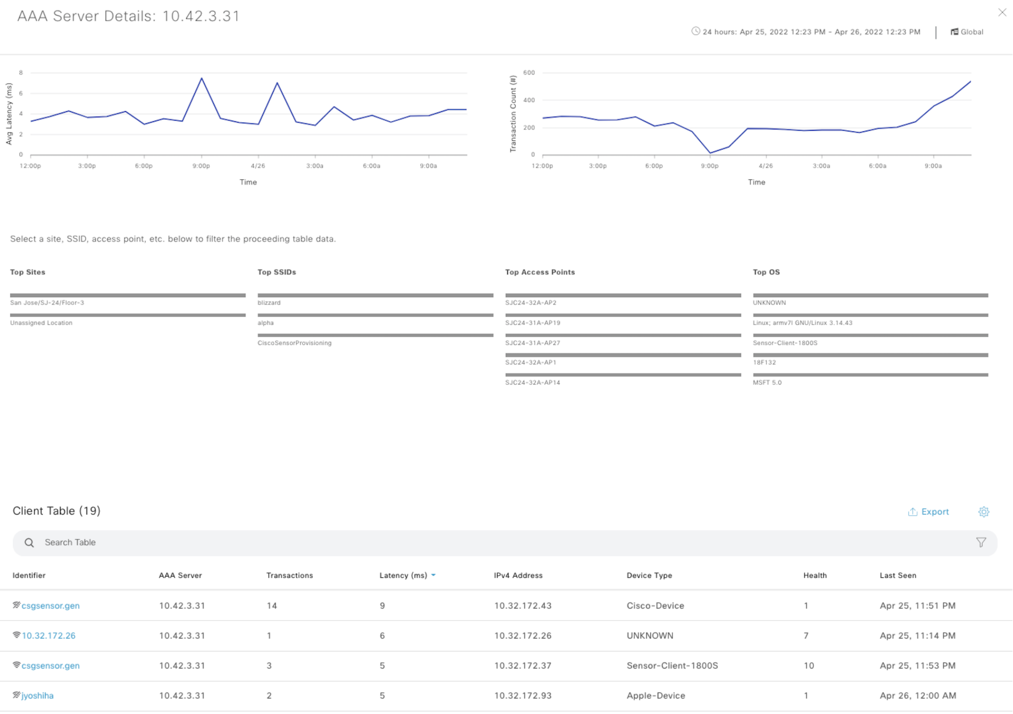
8 records

Show Records 10

1 - 8

Select any of the AAA servers to view the latency and transaction details as shown in the figure below. Select the graph to view the clients and their transaction details. The data can be filtered by SSID, Site, and Access Points. This can be used to find the clients with the highest latency to help troubleshoot client AAA issues. This AAA detail dashboard can also help visualize areas with high AAA latency which can help the engineer to quickly focus on contextual information and high priority areas with authentication issues.

Figure 6.15: AAA Server Details



AAA Server Details: 10.42.3.31

24 hours: Apr 25, 2022 12:23 PM - Apr 26, 2022 12:23 PM | Global

Select a site, SSID, access point, etc. below to filter the proceeding table data.

Top Sites	Top SSIDs	Top Access Points	Top OS
San Jose/SJ-24/Floor-3	blizzard	SJC24-32A-AP2	UNKNOWN
Unassigned Location	alpha	SJC24-31A-AP19	Linux; armv7l GNU/Linux 3.14.43
	CiscoSensorProvisioning	SJC24-31A-AP27	Sensor-Client-1800S
		SJC24-32A-AP1	18F132
		SJC24-32A-AP14	MSFT 5.0

Client Table (19)

Identifier	AAA Server	Transactions	Latency (ms)	IPv4 Address	Device Type	Health	Last Seen
csgsensor.gen	10.42.3.31	14	9	10.32.172.43	Cisco-Device	1	Apr 25, 11:51 PM
10.32.172.26	10.42.3.31	1	6	10.32.172.26	UNKNOWN	7	Apr 25, 11:14 PM
csgsensor.gen	10.42.3.31	3	5	10.32.172.37	Sensor-Client-1800S	10	Apr 25, 11:53 PM
jyoshiha	10.42.3.31	2	5	10.32.172.93	Apple-Device	1	Apr 26, 12:00 AM

Cisco AI Network Analytics generates baselines for AAA failures for each AAA server used to authenticate wireless clients. AI-driven issues are raised when the AAA failure rate exceeds the predicted baseline for a given AAA server. Please refer to Chapter 5 for more details.

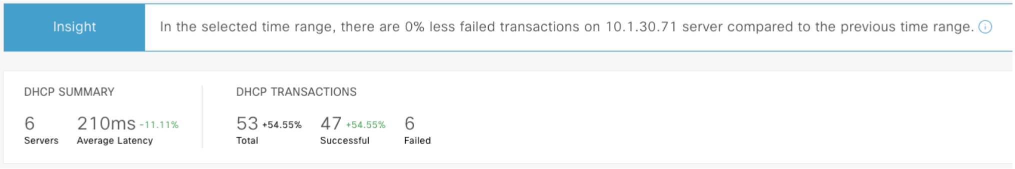
DHCP Dashboard

The DHCP dashboard breaks down the performance of the DHCP servers by latency and transactions. The timeline on the dashboard displays the number of DHCP transaction failures and successes over the time period selected. The timeline can be used to go back in time up to 30 days to view the historic data.

The Insights section below the timeline displays the change in DHCP server transactions compared to the previous time range. For example, if the time range is a 24-hour period, then it displays the change in DHCP transactions from the previous 24-hour period.

The next DHCP dashlet displays the DHCP summary and the DHCP transactions at a high level. The DHCP summary shows the number of DHCP servers and the average latency for transactions across all the DHCP servers. It also displays the change in average latency from the previous time period. The DHCP transactions section shows the total number of transactions, number of successful, and number of failed transactions across all the DHCP servers. The dashlet additionally displays the change in the number of successful and failed transactions from the previous time period. If there is a high percentage increase in the number of failed transactions over the previous time period, it may indicate a client-impacting DHCP issue that needs further investigation.

Figure 6.16: DHCP Summary



In the selected time range, there are 0% less failed transactions on 10.1.30.71 server compared to the previous time range.

DHCP SUMMARY

6 Servers

210ms -11.11% Average Latency

DHCP TRANSACTIONS

53 +54.55% Total

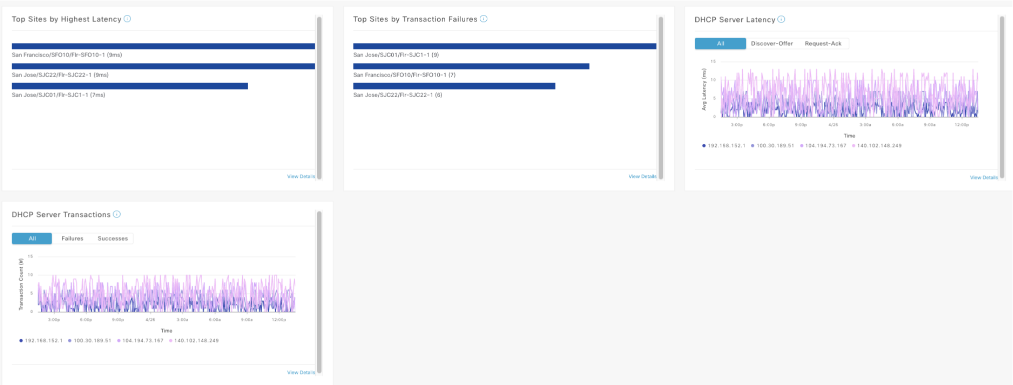
47 +54.55% Successful

6 Failed

The next section in the DHCP dashboard displays 4 different dashlets:

- Top N Sites by Highest Latency
- Top N Sites by Failed Transactions
- DHCP Server Latency
- DHCP Server Transactions

Figure 6.17: DHCP Dashlets



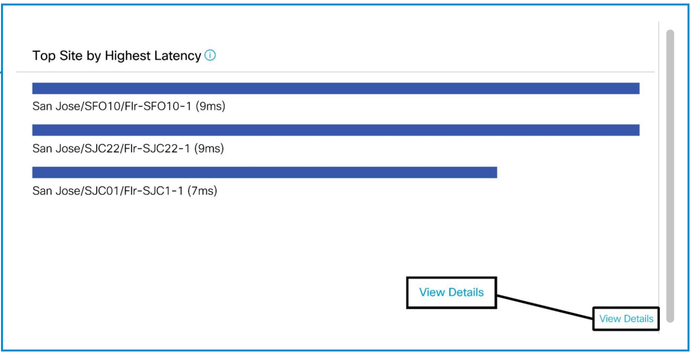
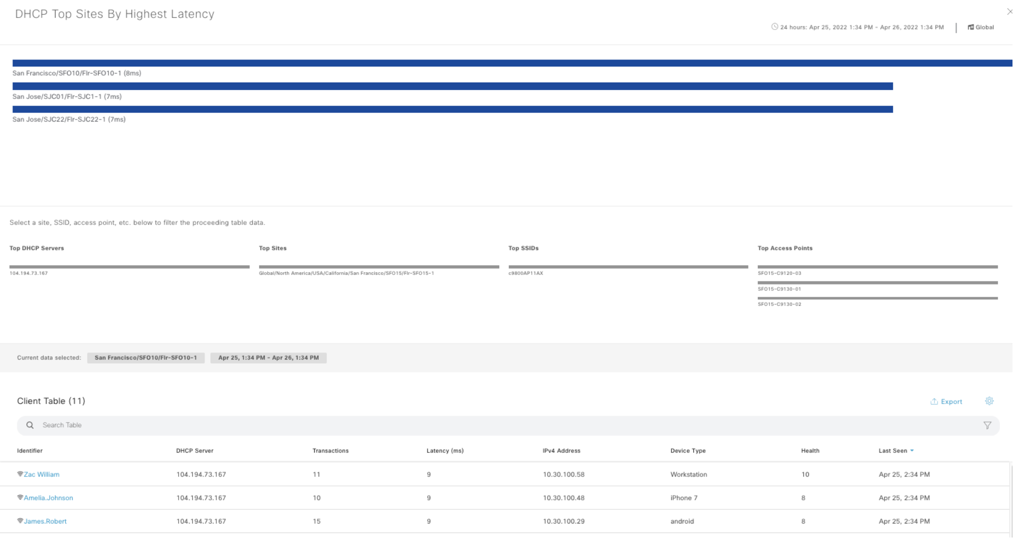

Top Site by Highest Latency ⓘ
San Jose/SFO10/Flr-SFO10-1 (9ms)
San Jose/SJC22/Flr-SJC22-1 (9ms)
San Jose/SJC01/Flr-SJC1-1 (7ms)
View Details
View Details

Figure 6.18: DHCP Top Sites by Highest Latency

The DHCP latency is calculated as the average DHCP packet round trip time from the WLC to the DHCP server. **The Top N Sites by Highest Latency** graph can be used to detect the most problematic sites for DHCP issues. Selecting `View Details` on this dashlet can be used to drill down into the site DHCP data in more detail.

Once a site is selected, the data can be filtered by `Top DHCP Servers`, `Top SSIDs`, or `Top APs` contributing to the highest DHCP latency on the site. The dashlet additionally displays the number of clients being affected by the filters selected. The data helps in pinpointing the most problematic DHCP areas to help quickly and easily troubleshoot DHCP issues affecting clients.

Figure 6.19: DHCP Top Sites by Highest Latency



DHCP Top Sites By Highest Latency

24 hours: Apr 25, 2022 1:34 PM - Apr 26, 2022 1:34 PM | Global

San Francisco/SFO10/Flr-SFO10-1 (8ms)

San Jose/SJC01/Flr-SJC1-1 (7ms)

San Jose/SJC22/Flr-SJC22-1 (7ms)

Select a site, SSID, access point, etc. below to filter the proceeding table data.

Top DHCP Servers	Top Sites	Top SSIDs	Top Access Points
104.194.73.167	Global/North America/USA/California/San Francisco/SFO15/Flr-SFO15-1	c9800AP11AX	SFO15-C9120-03 SFO15-C9130-01 SFO15-C9130-02

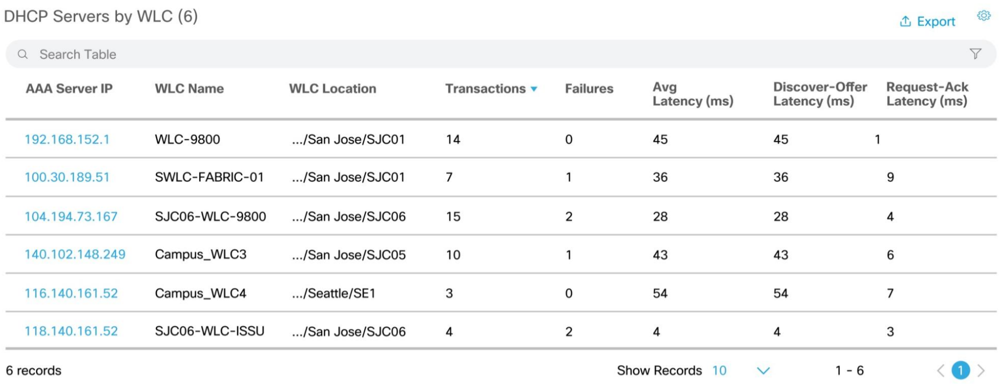
Current data selected: San Francisco/SFO10/Flr-SFO10-1 Apr 25, 1:34 PM - Apr 26, 1:34 PM

Client Table (11)

Identifier	DHCP Server	Transactions	Latency (ms)	IPv4 Address	Device Type	Health	Last Seen
Zac William	104.194.73.167	11	9	10.30.100.58	Workstation	10	Apr 25, 2:34 PM
Amelia.Johnson	104.194.73.167	10	9	10.30.100.48	iPhone 7	8	Apr 25, 2:34 PM
James.Robert	104.194.73.167	15	9	10.30.100.29	android	8	Apr 25, 2:34 PM

The DHCP dashboard also displays the list of DHCP servers with their respective WLCs. The table shows a wealth of data such as the DHCP server IP address, WLC, WLC Location, and the DHCP transaction details such as the number of failures, and latency for each DHCP server. This helps the network engineer to quickly identify the top-used DHCP servers and how the servers are performing.

Figure 6.20: DHCP Servers by WLC



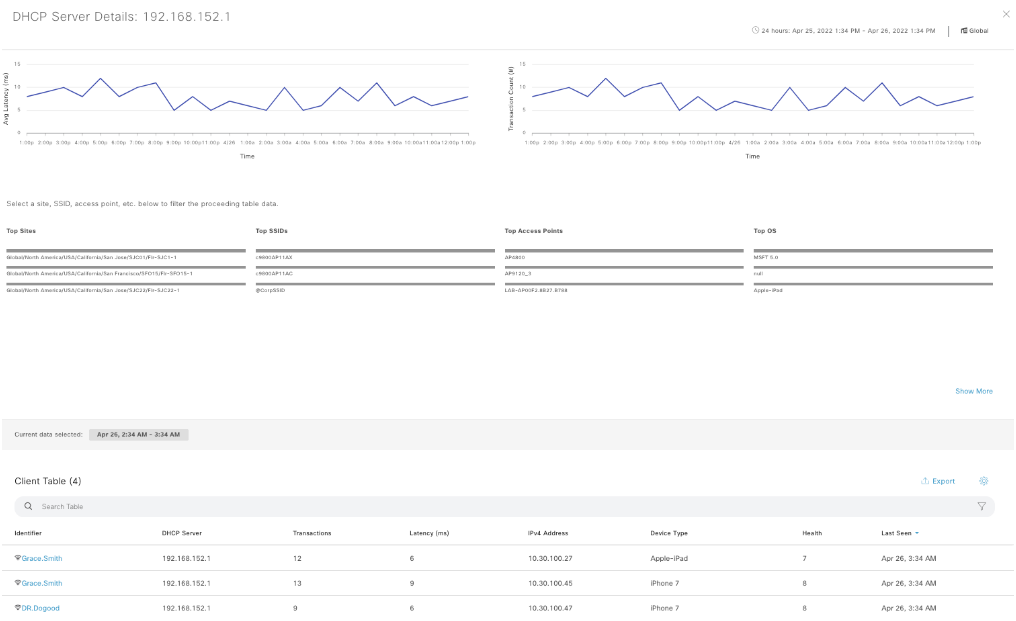
DHCP Servers by WLC (6)

AAA Server IP	WLC Name	WLC Location	Transactions ▾	Failures	Avg Latency (ms)	Discover-Offer Latency (ms)	Request-Ack Latency (ms)
192.168.152.1	WLC-9800	.../San Jose/SJC01	14	0	45	45	1
100.30.189.51	SWLC-FABRIC-01	.../San Jose/SJC01	7	1	36	36	9
104.194.73.167	SJC06-WLC-9800	.../San Jose/SJC06	15	2	28	28	4
140.102.148.249	Campus_WLC3	.../San Jose/SJC05	10	1	43	43	6
116.140.161.52	Campus_WLC4	.../Seattle/SE1	3	0	54	54	7
118.140.161.52	SJC06-WLC-ISSU	.../San Jose/SJC06	4	2	4	4	3

6 records

Select a `DHCP server` from the list to view the latency and transaction details. Select the graph to view the clients and their transaction details. This data can be filtered by SSID, Site, and APs. The network engineer can use this to find the clients with the highest latency or transactions to help quickly troubleshoot client DHCP issues.

Figure 6.21: DHCP Server Details


Avg Latency (ms)
15
10
5
0
1:00p 2:00p 3:00p 4:00p 5:00p 6:00p 7:00p 8:00p 9:00p 10:00p 11:00p 4/26 1:00a 2:00a 3:00a 4:00a 5:00a 6:00a 7:00a 8:00a 9:00a 10:00a 11:00a 12:00p 1:00p
Time
Transaction Count (#)
15
10
5
0
1:00p 2:00p 3:00p 4:00p 5:00p 6:00p 7:00p 8:00p 9:00p 10:00p 11:00p 4/26 1:00a 2:00a 3:00a 4:00a 5:00a 6:00a 7:00a 8:00a 9:00a 10:00a 11:00a 12:00p 1:00p
Time
Show More
Export
Search Table

DHCP Server Details: 192.168.152.1

24 hours: Apr 25, 2022 1:34 PM - Apr 26, 2022 1:34 PM | Global

Select a site, SSID, access point, etc. below to filter the proceeding table data.

Top Sites	Top SSIDs	Top Access Points	Top OS
Global/North America/USA/California/San Jose/SJC01/Flr-SJC1-1	c9800AP11AX	AP4800	MSFT 5.0
Global/North America/USA/California/San Francisco/SFO15/Flr-SFO15-1	c9800AP11AC	AP9120_3	null
Global/North America/USA/California/San Jose/SJC22/Flr-SJC22-1	@CorpSSID	LAB-AP00F2.8B27.B788	Apple-iPad

Current data selected: Apr 26, 2:34 AM - 3:34 AM

Client Table (4)

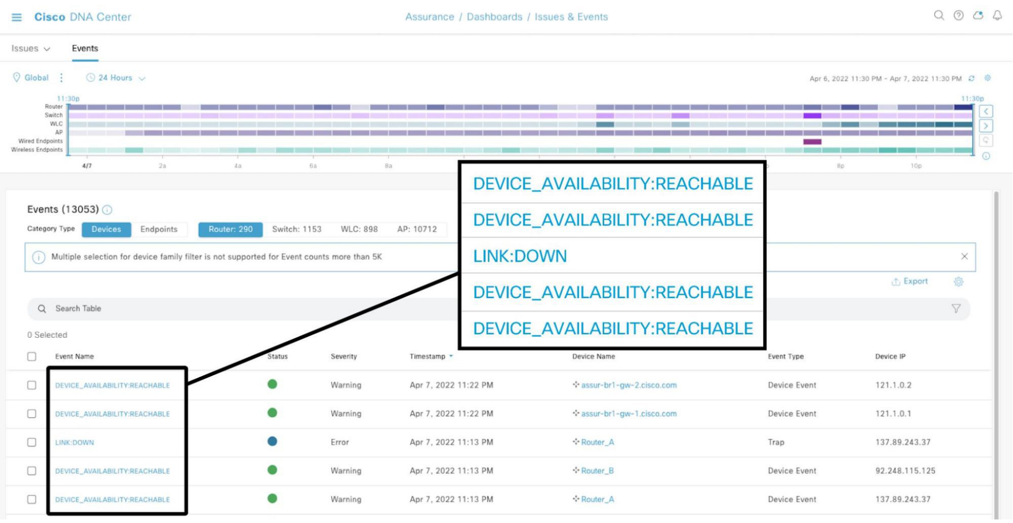
Identifier	DHCP Server	Transactions	Latency (ms)	IPv4 Address	Device Type	Health	Last Seen
Grace.Smith	192.168.152.1	12	6	10.30.100.27	Apple-iPad	7	Apr 26, 3:34 AM
Grace.Smith	192.168.152.1	13	9	10.30.100.45	iPhone 7	8	Apr 26, 3:34 AM
DR.Dogood	192.168.152.1	9	6	10.30.100.47	iPhone 7	8	Apr 26, 3:34 AM

Cisco AI Network Analytics generates baselines for DHCP failures, for each DHCP server used to serve wireless clients. AI-driven issues are raised when the DHCP failure rate exceeds the predicted baseline for a given server.

Events Viewer

The new Event Viewer provides the network engineer the ability to view all syslogs, traps, and telemetry events from all network devices on one centralized page. The new Event Viewer can be accessed from the `Assurance > Issues and Events` menu. The search function on this page helps to instantly search for an event among the thousands of events that may exist in the network. The events can be filtered and sorted for events related to routers, switches, and/or wireless devices.

Figure 6.22: Event Viewer



Events (13053)

Category Type: Devices | Endpoints — Router: 290 | Switch: 1153 | WLC: 898 | AP: 10712

Multiple selection for device family filter is not supported for Event counts more than 5K

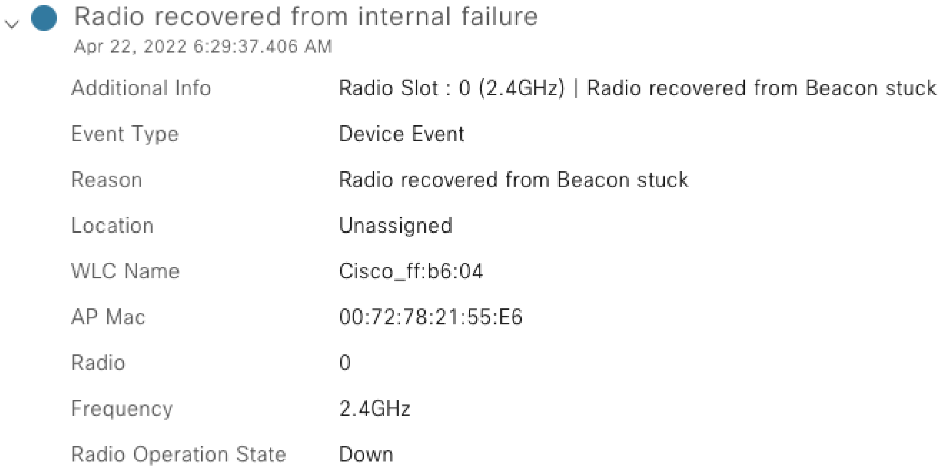
0 Selected

□	Event Name	Status	Severity	Timestamp	Device Name	Event Type	Device IP
□	DEVICE_AVAILABILITY:REACHABLE	●	Warning	Apr 7, 2022 11:22 PM	assur-br1-gw-2.cisco.com	Device Event	121.1.0.2
□	DEVICE_AVAILABILITY:REACHABLE	●	Warning	Apr 7, 2022 11:22 PM	assur-br1-gw-1.cisco.com	Device Event	121.1.0.1
□	LINK:DOWN	●	Error	Apr 7, 2022 11:13 PM	Router_A	Trap	137.89.243.37
□	DEVICE_AVAILABILITY:REACHABLE	●	Warning	Apr 7, 2022 11:13 PM	Router_B	Device Event	92.248.115.125
□	DEVICE_AVAILABILITY:REACHABLE	●	Warning	Apr 7, 2022 11:13 PM	Router_A	Device Event	137.89.243.37

DEVICE_AVAILABILITY:REACHABLE
DEVICE_AVAILABILITY:REACHABLE
LINK:DOWN
DEVICE_AVAILABILITY:REACHABLE
DEVICE_AVAILABILITY:REACHABLE

Selecting an `Event` displays the event details as shown below. The **Event Type** field indicates if the event is a syslog, trap, or device event. If it is a trap or syslog the severity of the event can also be viewed.

Figure 6.23: Event Viewer Details



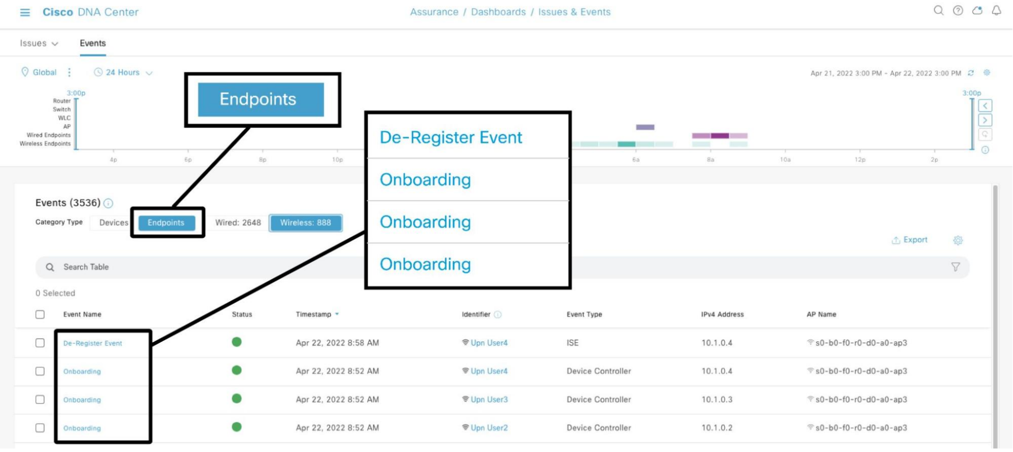
Radio recovered from internal failure

Apr 22, 2022 6:29:37.406 AM

Additional Info	Radio Slot : 0 (2.4GHz) | Radio recovered from Beacon stuck
Event Type	Device Event
Reason	Radio recovered from Beacon stuck
Location	Unassigned
WLC Name	Cisco_ff:b6:04
AP Mac	00:72:78:21:55:E6
Radio	0
Frequency	2.4GHz
Radio Operation State	Down

The endpoints events are available in the Event Viewer. Filters to view wired or wireless endpoints events are available as well. All events via streaming telemetry for wireless endpoints can also be viewed from this centralized page.

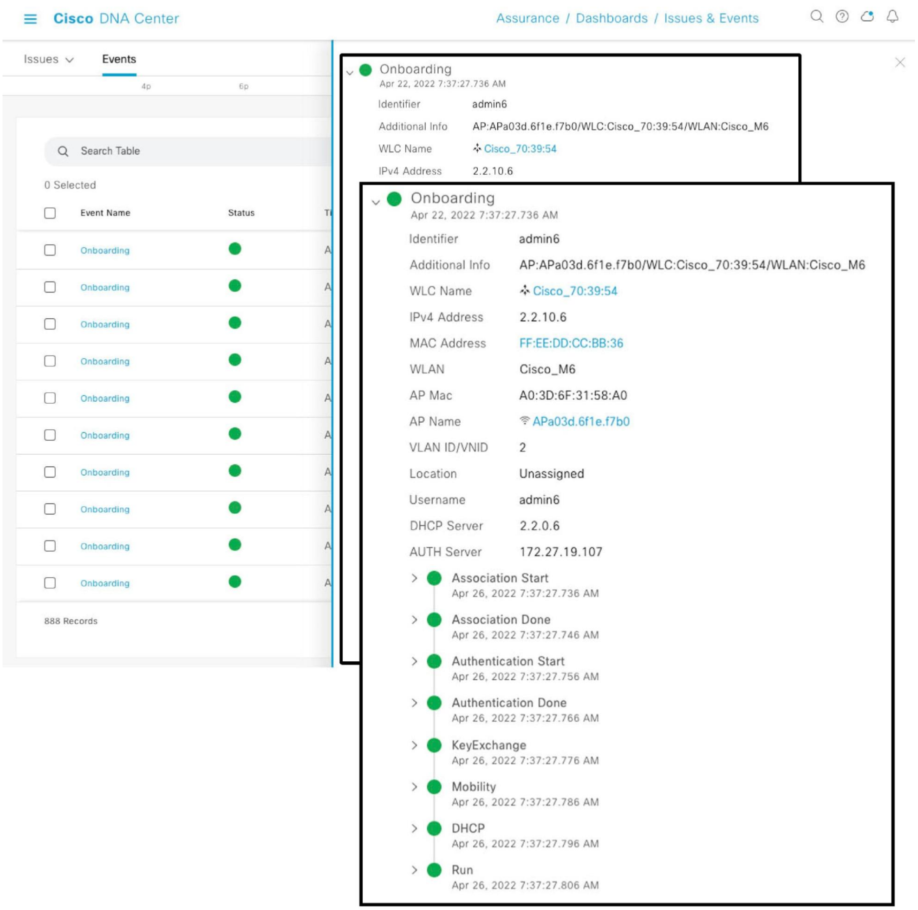
Figure 6.24: Endpoint Events on Event Viewer



	Event Name	Status	Timestamp	Identifier	Event Type	IPv4 Address	AP Name
□	De-Register Event	●	Apr 22, 2022 8:58 AM	Upn User4	ISE	10.1.0.4	s0-b0-f0-r0-d0-a0-ap3
□	Onboarding	●	Apr 22, 2022 8:52 AM	Upn User4	Device Controller	10.1.0.4	s0-b0-f0-r0-d0-a0-ap3
□	Onboarding	●	Apr 22, 2022 8:52 AM	Upn User3	Device Controller	10.1.0.3	s0-b0-f0-r0-d0-a0-ap3
□	Onboarding	●	Apr 22, 2022 8:52 AM	Upn User2	Device Controller	10.1.0.2	s0-b0-f0-r0-d0-a0-ap3

Drilling down into an event displays the event details. A wealth of information is provided in the event details as shown below. This helps the network engineer to troubleshoot endpoint issues as it allows quick viewing of connectivity details and any reasons for the failure, decreasing the MTTR.

Figure 6.25: Endpoint Event Details



0 Selected

□	Event Name	Status	Ti
□	Onboarding	●	A
□	Onboarding	●	A
□	Onboarding	●	A
□	Onboarding	●	A
□	Onboarding	●	A
□	Onboarding	●	A
□	Onboarding	●	A
□	Onboarding	●	A
□	Onboarding	●	A
□	Onboarding	●	A

888 Records

● Onboarding
Apr 22, 2022 7:37:27.736 AM

Identifier	admin6
Additional Info	AP:APa03d.6f1e.f7b0/WLC:Cisco_70:39:54/WLAN:Cisco_M6
WLC Name	Cisco_70:39:54
IPv4 Address	2.2.10.6

● Onboarding
Apr 22, 2022 7:37:27.736 AM

Identifier	admin6
Additional Info	AP:APa03d.6f1e.f7b0/WLC:Cisco_70:39:54/WLAN:Cisco_M6
WLC Name	Cisco_70:39:54
IPv4 Address	2.2.10.6
MAC Address	FF:EE:DD:CC:BB:36
WLAN	Cisco_M6
AP Mac	A0:3D:6F:31:58:A0
AP Name	APa03d.6f1e.f7b0
VLAN ID/VNID	2
Location	Unassigned
Username	admin6
DHCP Server	2.2.0.6
AUTH Server	172.27.19.107

● Association Start
Apr 26, 2022 7:37:27.736 AM

● Association Done
Apr 26, 2022 7:37:27.746 AM

● Authentication Start
Apr 26, 2022 7:37:27.756 AM

● Authentication Done
Apr 26, 2022 7:37:27.766 AM

● KeyExchange
Apr 26, 2022 7:37:27.776 AM

● Mobility
Apr 26, 2022 7:37:27.786 AM

● DHCP
Apr 26, 2022 7:37:27.796 AM

● Run
Apr 26, 2022 7:37:27.806 AM

3D Maps

An exciting addition to the existing 2D Maps feature within Cisco DNA Center is the new capability to use 3D Maps for visualizing AP coverage in a defined 3D space such as an office building. Both operational as well as planned APs can be visualized in 3D Maps, making the 3D maps feature incredibly powerful and accurate for planning new AP deployments.

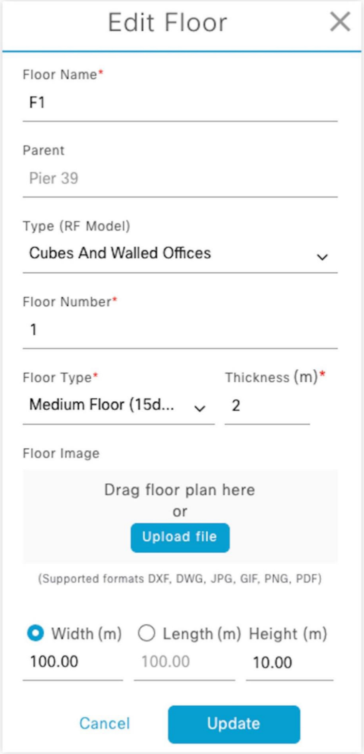
To view a 3D wireless map, a floor plan has to be created for the 3D wireless map. There are three ways to create the floor plan for the 3D wireless map:

- **Import a CAD file**: Use a CAD file (DXF or DWG file type) to import the floor plan, Cisco DNA Center imports the CAD layers and allows specification of which layers will appear as floor elements in the 3D wireless map.
- **Import a 2D image file**: Use the file types JPG, GIF, PNG, or PDF to import the floor plan. However, the user will need to manually create the floor elements, such as the walls and doors, for them to be represented in the 3D wireless map.
- **Import an Ekahau Pro Project plan**: The data from the Ekahau project, such as the obstacles, APs, and more, are imported into the 3D wireless map.

Note If you are using Cisco Prime Infrastructure, you can import floor maps and AP placement from Cisco Prime Infrastructure into Cisco DNA Center, however, the Cisco Prime Infrastructure maps will be 2D maps. The network engineer then can add the walls and other objects to create the 3D map.

Figure 6.26: Edit Floor

Click `Update` to upload the floor plan and update the floor settings. The 2D map will be displayed.



Edit Floor

Floor Name*
F1

Parent
Pier 39

Type (RF Model)
Cubes And Walled Offices

Floor Number*
1

Floor Type*
Medium Floor (15d...

Thickness (m)*
2

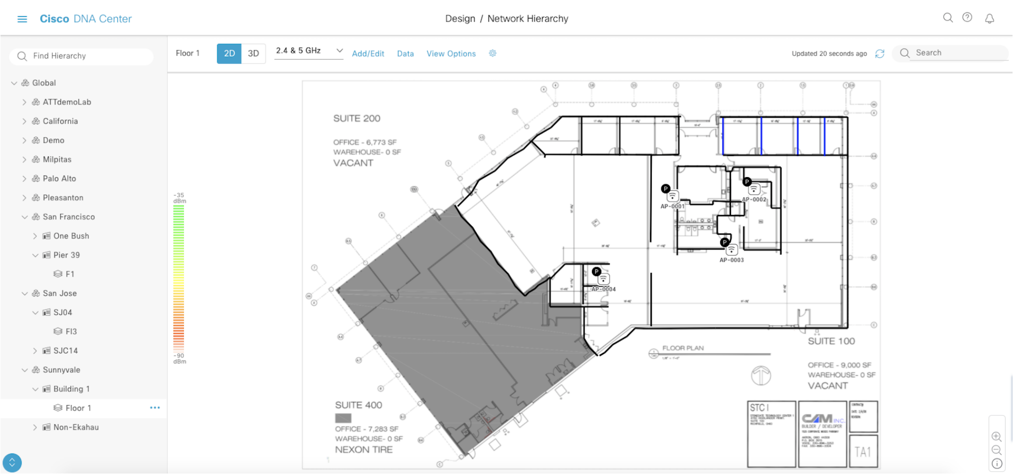
Floor Image

Drag floor plan here
or

(Supported formats DXF, DWG, JPG, GIF, PNG, PDF)

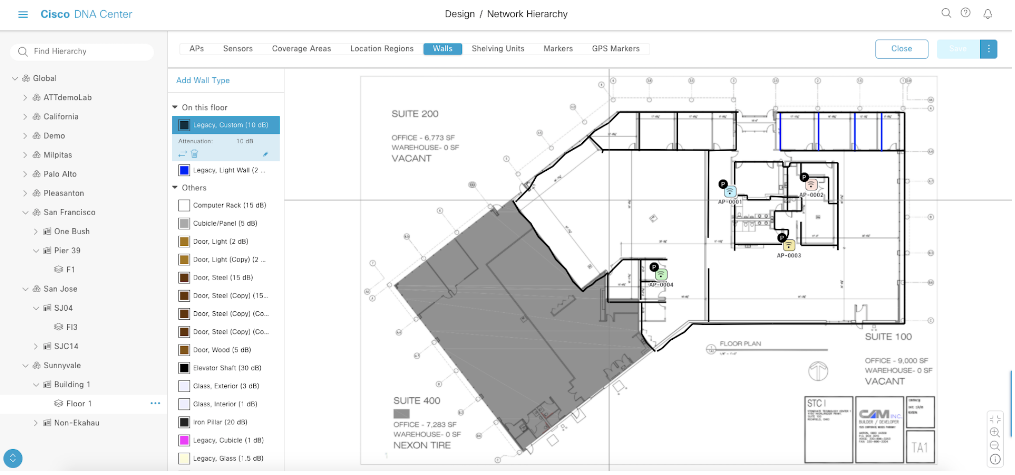
● Width (m) ○ Length (m) Height (m)
100.00 100.00 10.00

Figure 6.27: Floor 1 2D Map



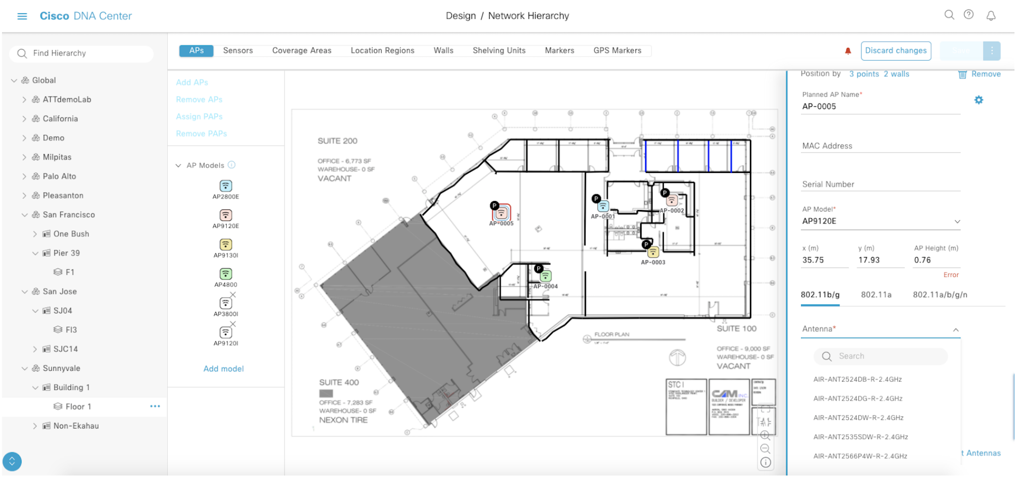
If the map imported was a 2D image, it can automatically be viewed as a 3D map. However, to get the most benefit, obstacles such as walls and doors that affect attenuation should be added to the floor map. By selecting `Add/Edit` above the map, these obstacles can be manually drawn in their respective locations, using one of the various wall types provided in the map editor, or using a custom wall type that can be manually defined. Additional items can be added and placed on the map such as shelving units and GPS markers and custom coverage areas and location regions can be defined as well.

Figure 6.28: Add walls to the floor map



After drawing the walls for the selected floor, APs will need to be placed on the map to show RF coverage within the physical space. This can be done by selecting the APs tab while editing the floor, selecting one or more AP models, and placing each AP in the respective physical location on the floor where the AP is located (or will be located). The proper antenna type for the new AP will need to be selected to provide an accurate RF model. Click `Save` to update the floor map.

Figure 6.29: Add an Access Point to the floor map



Planned AP Name*: AP-0005

MAC Address

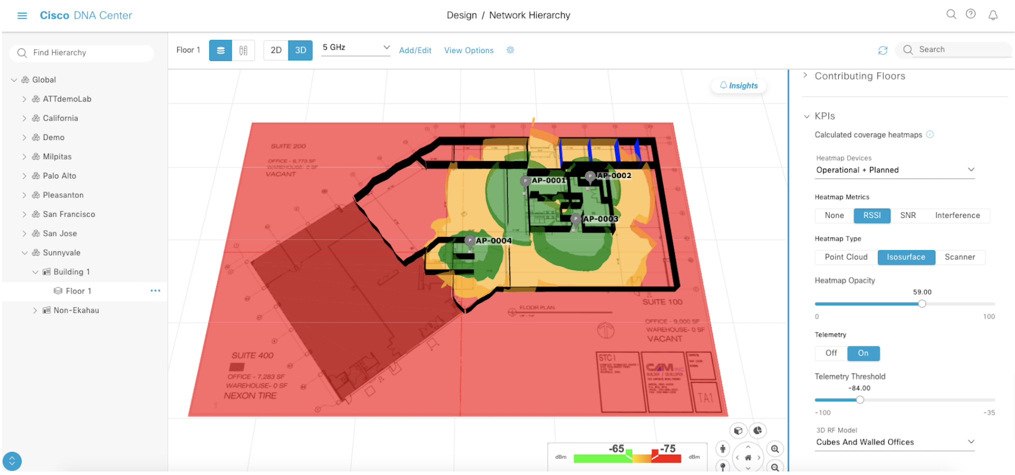
Serial Number

AP Model*: AP9120E

x (m)	y (m)	AP Height (m)
35.75	17.93	0.76

Now that the floor map is prepared, click the `3D` toggle to switch from 2D maps to 3D. The 3D map shows the RF coverage of the placed access points with the RSSI, Interference, and SNR ratio wireless KPIs. Above the map, there are toggles to switch between 2.4Ghz to 5Ghz bands. Click `View Options` to expand/collapse the side menu. By expanding the KPIs menu on the side menu the previously configured 3D RF Model and Floor Geometry can also be modified if needed.

Figure 6.30: Floor 1 3D Map



Calculated coverage heatmaps

Heatmap Devices: Operational + Planned

Heatmap Metrics: None [✓ RSSI] SNR Interference

Heatmap Type: Point Cloud [✓ Isosurface] Scanner

Heatmap Opacity: 59.00 (0–100)

Telemetry: Off [✓ On]

Telemetry Threshold: -84.00 (-100 – -35)

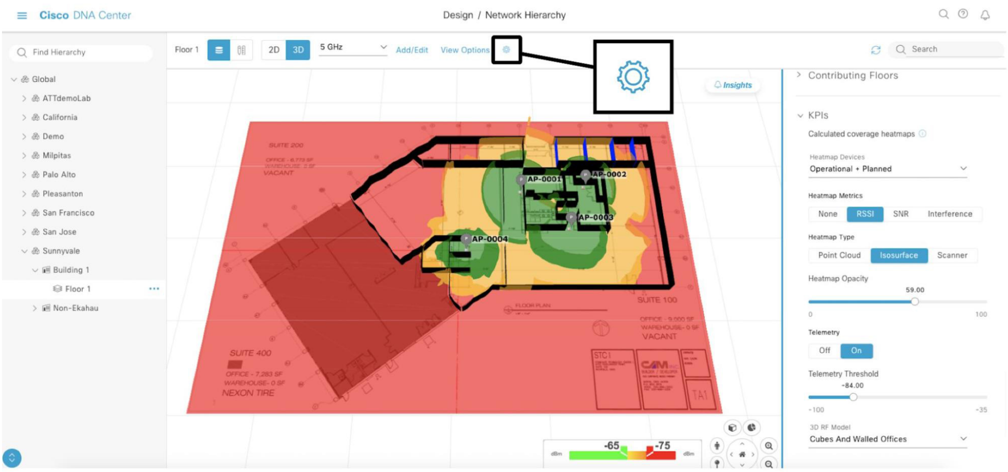
3D RF Model: Cubes And Walled Offices

The controls at the bottom of the page can be used to move and pan around the map and provide additional tools for visualizing the 3D map, such as cutting a slice from the floor to analyze only that segment or viewing the 3D map from the point of view of someone on the floor. The available heatmap types are:

- **Point Cloud**: A collection of individual points captured in the physical 3D space to show coverage quality across the floor.
- **Isosurface (RSSI only)**: A smoothed, 3D shaping of the RF coverage for each access point that shows how coverage is affected by walls and distance.
- **Scanner**: A 2D visualization of the RF coverage for all KPIs across the floor.

Lastly, insights can be custom configured by clicking the `gear icon` above the map and clicking `Insight Configurations`.

Figure 6.31: Point Cloud with SNR



Heatmap Devices: Operational + Planned

Heatmap Metrics: None | **RSSI** | SNR | Interference

Heatmap Type: Point Cloud | **Isosurface** | Scanner

Heatmap Opacity: 59.00 (0–100)

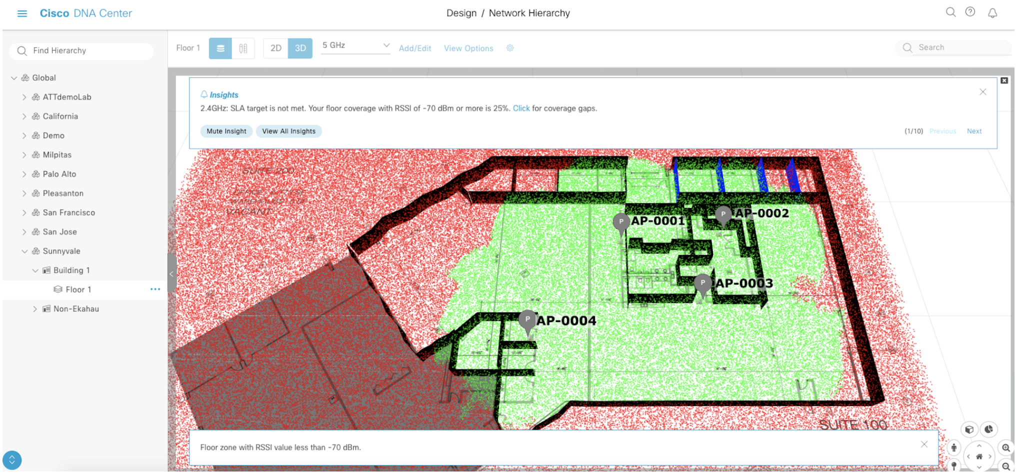
Telemetry: Off | **On**

Telemetry Threshold: -84.00 (-100 – -35)

3D RF Model: Cubes And Walled Offices

Based on what is configured in the Insight Configurations, clicking the `Insights` button on the map will provide a series of insights into the AP coverage for each of the KPIs. Each insight provides detailed information about which metrics are not meeting the service level agreements (SLAs) configured on the map and can show the coverage gaps directly on the map.

Figure 6.32: Insights for 3D Maps



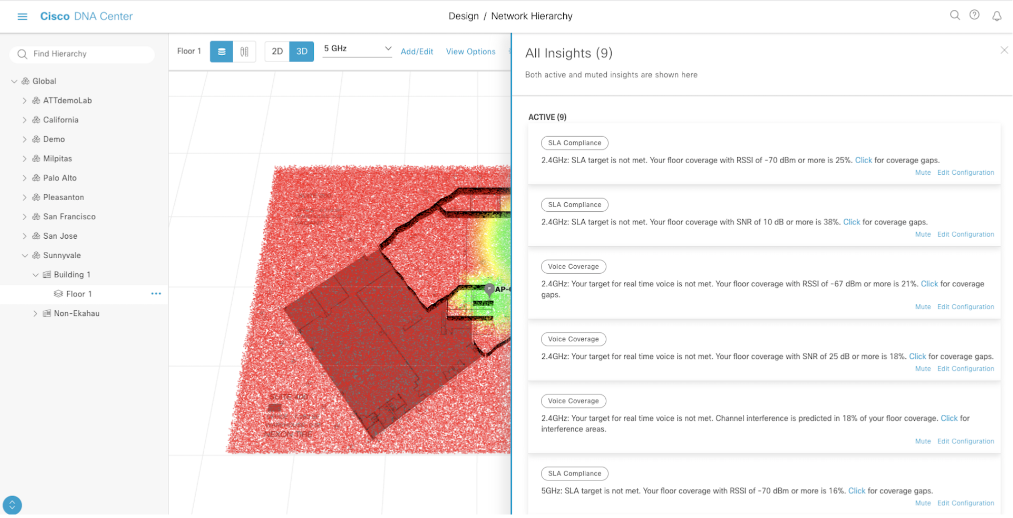
Insights

2.4GHz: SLA target is not met. Your floor coverage with RSSI of -70 dBm or more is 25%. Click for coverage gaps.

Floor zone with RSSI value less than -70 dBm.

Selecting `View All Insights` will display all the insights as shown below.

Figure 6.33: All Insights View in 3D Maps



All Insights (9)

Both active and muted insights are shown here

ACTIVE (9)

SLA Compliance

2.4GHz: SLA target is not met. Your floor coverage with RSSI of -70 dBm or more is 25%. Click for coverage gaps.

Mute Edit Configuration

SLA Compliance

2.4GHz: SLA target is not met. Your floor coverage with SNR of 10 dB or more is 38%. Click for coverage gaps.

Mute Edit Configuration

Voice Coverage

2.4GHz: Your target for real time voice is not met. Your floor coverage with RSSI of -67 dBm or more is 21%. Click for coverage gaps.

Mute Edit Configuration

Voice Coverage

2.4GHz: Your target for real time voice is not met. Your floor coverage with SNR of 25 dB or more is 18%. Click for coverage gaps.

Mute Edit Configuration

Voice Coverage

2.4GHz: Your target for real time voice is not met. Channel interference is predicted in 18% of your floor coverage. Click for interference areas.

Mute Edit Configuration

SLA Compliance

5GHz: SLA target is not met. Your floor coverage with RSSI of -70 dBm or more is 16%. Click for coverage gaps.

Mute Edit Configuration

The Cisco DNA Center 3D maps provide the wireless network engineer teleportation powers to be able to visualize the space in 3D and be able to see RF coverage, RSSI, and interference, giving a never before possible perspective of the RF landscape. This feature is a huge time saver and also enables the wireless engineer to perform many planning and troubleshooting tasks from their desks. This feature is a great example of how Cisco DNA Center can help accelerate the time to value.

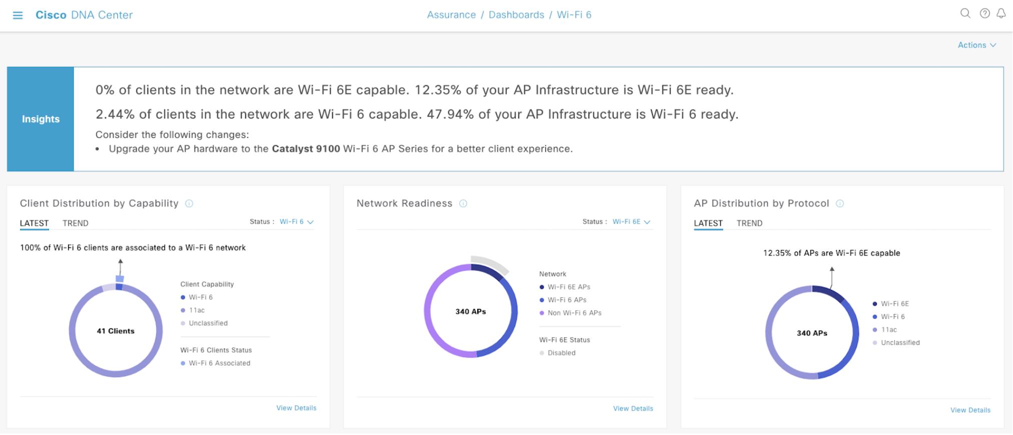
Wi-Fi 6 Dashboard

Cisco DNA Center provides a centralized dashboard that allows network engineers to visualize and quickly understand the network's Wi-Fi 6 readiness as well as the Wi-Fi 6 performance for existing deployments. To navigate to the Wi-Fi 6 dashboard from the Cisco DNA Center main menu, select `Assurance > Wi-Fi 6.` The Wi-Fi 6 dashboard provides an overview of the general readiness for Wi-Fi 6 in the network by providing a percentage of network devices and clients that are capable of and utilizing Wi-Fi 6. It also provides insights into the status of the network's Wi-Fi 6 deployment, such as suggestions to upgrade wireless controllers to the correct version to utilize Wi-Fi 6 analytics and the right APs required for Wi-Fi 6 deployment.

The Wi-Fi 6 dashboard also provides a series of dashlets that can give even further insight into the state of Wi-Fi 6 readiness, including:

- Client Distribution by Capability (802.11abg/802.11ac/Wi-Fi 6, Wi-FI 6E)
- Network Readiness (Wi-Fi 6/Wi-Fi 6E, Non-Wi-Fi 6 Access Points)
- AP Distribution by Protocol

Figure 6.34: Wi-Fi 6 Dashboard



Insights

0% of clients in the network are Wi-Fi 6E capable. 12.35% of your AP Infrastructure is Wi-Fi 6E ready.

2.44% of clients in the network are Wi-Fi 6 capable. 47.94% of your AP Infrastructure is Wi-Fi 6 ready.

Consider the following changes:

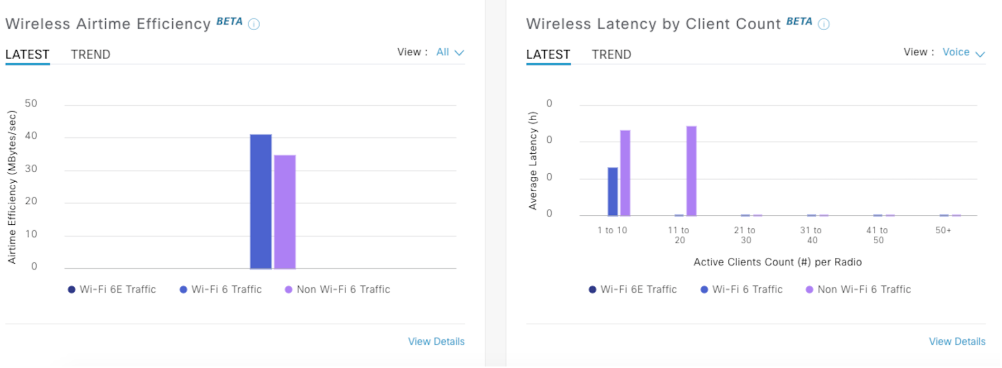
- Upgrade your AP hardware to the **Catalyst 9100** Wi-Fi 6 AP Series for a better client experience.

100% of Wi-Fi 6 clients are associated to a Wi-Fi 6 network

12.35% of APs are Wi-Fi 6E capable

In addition to these dashlets, there are an additional two new dashlets that provide insight into Wi-Fi 6/Wi-Fi 6E performance for existing deployments: **Wireless Airtime Efficiency** and **Wireless Latency by Client Count**. Wireless Airtime Efficiency is measured by calculating the percentage of peak usage minutes achieved at various speeds. The default tab for each dashlet, `LATEST`, shows the latest data from the past 5 minutes, and selecting `TREND` displays the data from the previous 24-hour period.

Figure 6.35: Airtime Efficiency and Client Count



Wireless Airtime Efficiency BETA

LATEST TREND

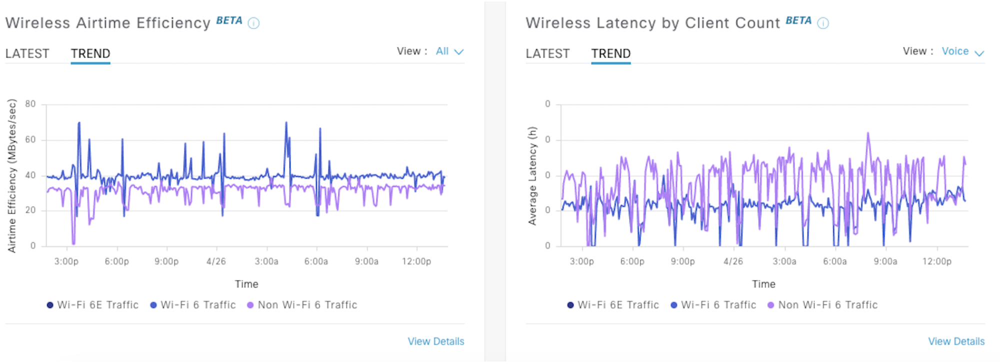
View : All

Wireless Latency by Client Count BETA

LATEST TREND

View : Voice

Figure 6.36: Wireless Trends



Wireless Airtime Efficiency BETA

LATEST TREND

View : All

Wireless Latency by Client Count BETA

LATEST TREND

View : Voice

All dashboards and dashlets items on the Wi-Fi 6 Dashboard now support the new Wi-Fi 6E protocol.

The Wi-FI 6 dashboard gives unparalleled visibility into the Wi-Fi 6/Wi-Fi 6E deployment in the network. This helps to plan how well the modernizing of wireless network is progressing and make the case for adding more Wi-Fi 6/Wi-Fi 6E APs to enhance the user experience.

7. Wireless Device Troubleshooting

Wireless troubleshooting is arguably one of the toughest jobs for network engineers. Wireless issues can be related to the WLC, the AP, the client, the network, and/or various other reasons. This chapter presents a suite of new and innovative wireless device troubleshooting tools and features within Cisco DNA Center.

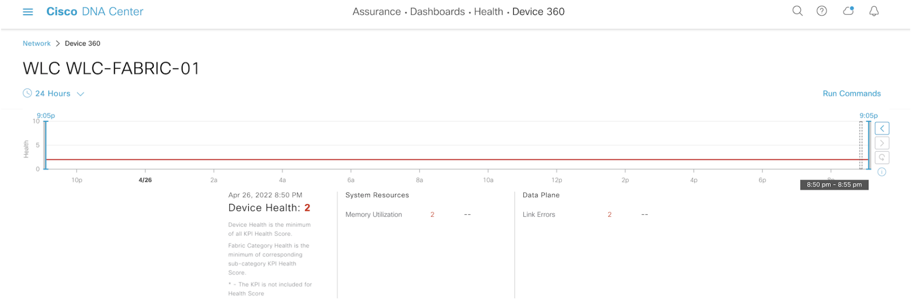
In the past, engineers have typically needed specialized tools to effectively troubleshoot wireless issues, such as spectrum analyzers and protocol analyzers. Spectrum analyzers allow the engineer to view the raw RF energy in the environment. Protocol analyzers allow the engineer to capture frames over the air for later analysis. Even with these specialized tools, it can be difficult or sometimes not even cost-effective to physically bring those specialized tools out to the end users' location to capture the issue while the user attempts to recreate the problem. If the wireless engineer was lucky enough to have captured the data while the user recreated the problem, it can still be incredibly difficult to ascertain the actual issue based upon radio frequency (RF) signatures viewed from a spectrum analyzer or pouring through possibly tens of thousands of frames that can be captured in just a few seconds with a protocol analyzer. Even then, the issue may not even be in the PCAP file, but what is not in the PCAP file. Advanced protocol knowledge is needed to not only see what is there but recognize what is not there. Then, after all that, the issue may not even be a wireless issue at all. For instance, there could be a wired issue or an issue with AAA, DHCP, and/or DNS that is preventing a user from successfully joining the wireless network or causing poor performance.

No matter what the reason, if a user is unable to use the wireless network, it is a wireless problem. This is where Cisco DNA Center really shines. Cisco DNA Center gives the network engineer the troubleshooting tools, contextual information, and insights needed to identify and eliminate problems that are negatively impacting wireless client network performance.

Wireless LAN Controller – Device 360

The Wireless LAN Controller Device 360 page allows the engineer to view the current Health Score of the WLC. It also allows the engineer to travel back in time to not only see what the Health Score was at a particular point in time, but also what KPIs were affecting the health score at that point in time. This can help reduce troubleshooting WLC issues from hours to just minutes.

Figure 7.1: Device 360



WLC WLC-FABRIC-01

Apr 26, 2022 8:50 PM

Device Health: 2

Device Health is the minimum of all KPI Health Score.

Fabric Category Health is the minimum of corresponding sub-category KPI Health Score.

* - The KPI is not included for Health Score

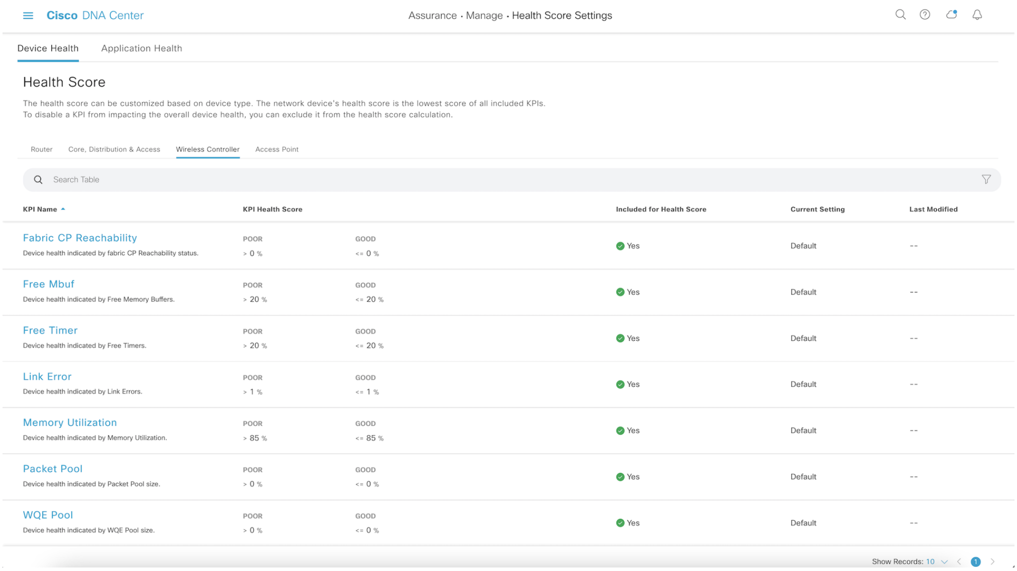
System Resources

Memory Utilization 2 --

Data Plane

Link Errors 2 --

Figure 7.2: Wireless LAN Controller KPIs



Health Score

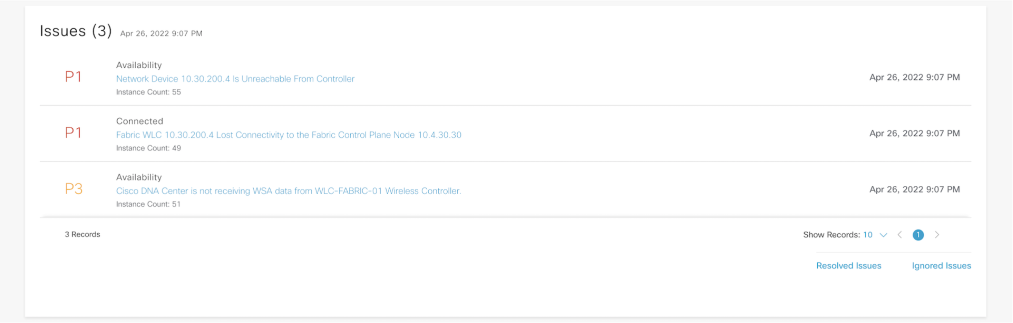
The health score can be customized based on device type. The network device's health score is the lowest score of all included KPIs.
To disable a KPI from impacting the overall device health, you can exclude it from the health score calculation.

KPI Name	KPI Health Score		Included for Health Score	Current Setting	Last Modified
Fabric CP Reachability Device health indicated by fabric CP Reachability status.	POOR > 0 %	GOOD <= 0 %	✓ Yes	Default	--
Free Mbuf Device health indicated by Free Memory Buffers.	POOR > 20 %	GOOD <= 20 %	✓ Yes	Default	--
Free Timer Device health indicated by Free Timers.	POOR > 20 %	GOOD <= 20 %	✓ Yes	Default	--
Link Error Device health indicated by Link Errors.	POOR > 1 %	GOOD <= 1 %	✓ Yes	Default	--
Memory Utilization Device health indicated by Memory Utilization.	POOR > 85 %	GOOD <= 85 %	✓ Yes	Default	--
Packet Pool Device health indicated by Packet Pool size.	POOR > 0 %	GOOD <= 0 %	✓ Yes	Default	--
WQE Pool Device health indicated by WQE Pool size.	POOR > 0 %	GOOD <= 0 %	✓ Yes	Default	--

Issues

The Issues dashlet displays the issues that have affected the wireless controller within the specified time frame. These issues are sorted by priority.

Figure 7.3: WLC 360 Issues



Issues (3) Apr 26, 2022 9:07 PM

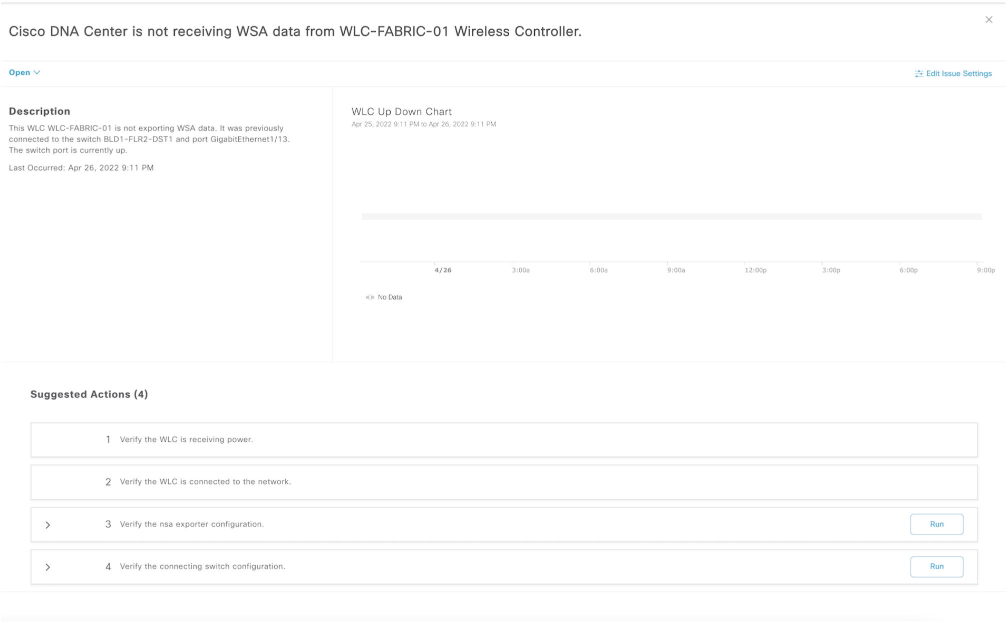
P1	Availability Network Device 10.30.200.4 Is Unreachable From Controller Instance Count: 55	Apr 26, 2022 9:07 PM
P1	Connected Fabric WLC 10.30.200.4 Lost Connectivity to the Fabric Control Plane Node 10.4.30.30 Instance Count: 49	Apr 26, 2022 9:07 PM
P3	Availability Cisco DNA Center is not receiving WSA data from WLC-FABRIC-01 Wireless Controller. Instance Count: 51	Apr 26, 2022 9:07 PM

3 Records

Show Records: 10

Clicking on an issue provides the network engineer with a description of the problem as well as a list of **Suggested Actions** that should be taken to solve that problem. The network engineer will also have the option to run commands specified in the Suggested Actions, directly from Cisco DNA Center. This saves the network engineer time because it eliminates the need to log into the device and type in the commands manually. The engineer also has the option to Resolve or Ignore the Issue. When ignoring the issue, it can be ignored for 1 hour up to 30 days.

Figure 7.4: WLC Issue Details



Cisco DNA Center is not receiving WSA data from WLC-FABRIC-01 Wireless Controller.

Description

This WLC WLC-FABRIC-01 is not exporting WSA data. It was previously connected to the switch BLD1-FLR2-DST1 and port GigabitEthernet1/13. The switch port is currently up.

Last Occurred: Apr 26, 2022 9:11 PM

Suggested Actions (4)

1 Verify the WLC is receiving power.

2 Verify the WLC is connected to the network.

3 Verify the nsa exporter configuration.

4 Verify the connecting switch configuration.

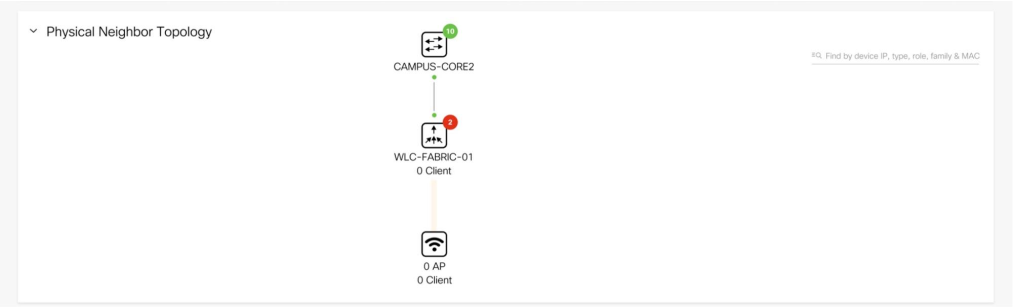
Real-World Scenario

Joshitha is a Help Desk Technician at a software development company. She receives a ticket that says, “Wi-Fi is broken”, but the ticket does not include any additional information other than the user’s username and phone number. She searches Cisco DNA Center for that username and pulls up the User 360 page. From that page, Joshitha can see that the user’s laptop is disconnected from the network. She scrolls down to the Issues dashlet and notices an issue with failed authentication due to a bad password. She calls the user to explain that they are unable to connect due to a bad password. The user then realizes they had Caps Lock on, disables it, and can log in successfully.

Physical Neighbor Topology

The Physical Neighbor Topology shows the number of APs connected to the WLC, the number of connected clients, the uplink switch and link status information, and the health scores of all connected devices. This allows the engineer to quickly visualize not only the Health Score of the WLC, but also the health scores of devices connected to that WLC.

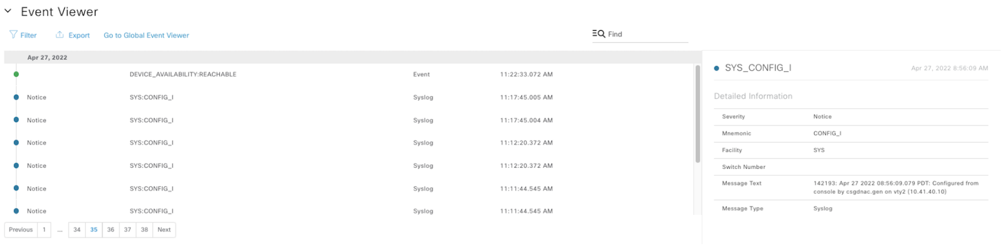
Figure 7.5: Physical Neighbor Topology


Physical Neighbor Topology
Find by device IP, type, role, family & MAC
10
CAMPUS-CORE2
2
WLC-FABRIC-01
0 Client
0 AP
0 Client

Event Viewer

The event viewer displays telemetry events, syslogs, and traps from the WLC. This helps a network engineer quickly troubleshoot any WLC issues by checking for any problem events and viewing the details directly in Cisco DNA Center. This feature also has a search that can be used to quickly find events that are of interest among the hundreds or thousands of events. There is also a link to launch the Global Event Viewer to view the events from all devices in one single location.

Figure 7.6: WLC Event Viewer



Apr 27, 2022

	DEVICE_AVAILABILITY:REACHABLE	Event	11:22:33.072 AM
Notice	SYS:CONFIG_I	Syslog	11:17:45.005 AM
Notice	SYS:CONFIG_I	Syslog	11:17:45.004 AM
Notice	SYS:CONFIG_I	Syslog	11:12:20.372 AM
Notice	SYS:CONFIG_I	Syslog	11:12:20.372 AM
Notice	SYS:CONFIG_I	Syslog	11:11:44.545 AM
Notice	SYS:CONFIG_I	Syslog	11:11:44.545 AM

SYS_CONFIG_I Apr 27, 2022 8:56:09 AM

Detailed Information

Severity	Notice
Mnemonic	CONFIG_I
Facility	SYS
Switch Number	
Message Text	142193: Apr 27 2022 08:56:09.079 PDT: Configured from console by csgdnac.gen on vty2 (10.41.40.10)
Message Type	Syslog

Path Trace

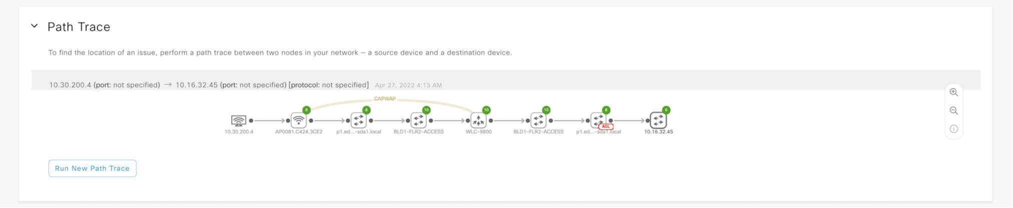
Path Trace allows the network engineer to pinpoint issues in the network. When running a Path Trace, the network engineer will specify the Source and Destination nodes, optionally a source and destination port, optionally TCP or UDP protocol.

When executing the Path Trace, Cisco DNA Center will display all the network devices between the Source and Destination as well as the Health Scores, link status, and ACLs along the path. This allows the network engineer to visualize where the problem is in the entire network path for the traffic flow. This helps resolve application experience issues quickly and easily.

After executing the Path Trace between the wireless controller and destination, Path Trace identifies any ACLs within the path, as well as receiving device, device interface, and QoS statistics.

In addition to Path Trace, there is also the option to perform a live packet capture with real data which is known as True Trace. To execute a True Trace with live packet capture, all intermediary devices in the path will need to be managed by Cisco DNA Center and running IOS XE 17.x or higher.

Figure 7.7: WLC 360 Path Trace



Path Trace

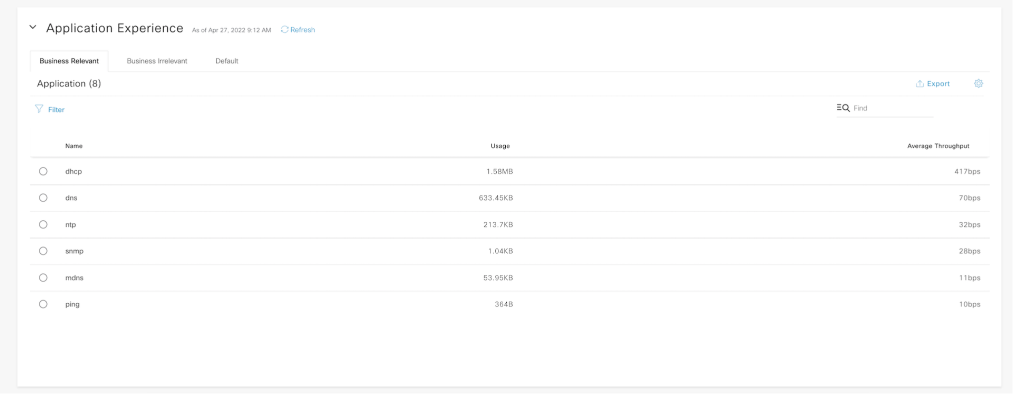
To find the location of an issue, perform a path trace between two nodes in your network – a source device and a destination device.

10.30.200.4 (port: not specified) → 10.16.32.45 (port: not specified) [protocol: not specified] Apr 27, 2022 4:13 AM

Application Experience

Visualize application visibility data such as Usage and Average Throughput. This allows the network engineer to see which applications are taking the most bandwidth and also which clients are using those applications. The application data comes directly from the WLC via NetFlow. Please refer to the **Application Health** section for more details on the application experience.

Figure 7.8: WLC 360 Application Experience



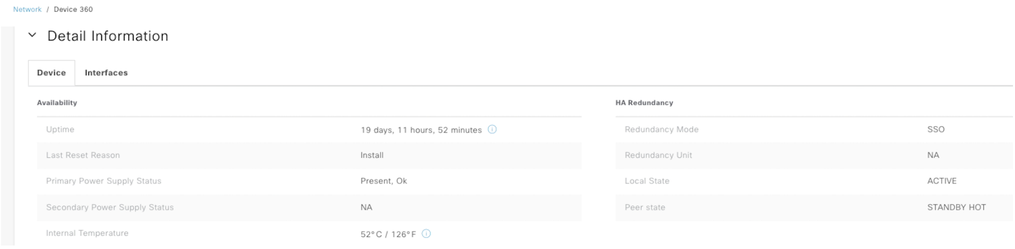
Application (8)

	Name	Usage	Average Throughput
○	dhcp	1.58MB	417bps
○	dns	633.45KB	70bps
○	ntp	213.7KB	32bps
○	snmp	1.04KB	28bps
○	mdns	53.95KB	11bps
○	ping	364B	10bps

Detail Information

This section has 2 tabs. One for the device and the other for the interfaces. The `Device` tab section shows helpful information related to the device such as Uptime, HA Redundancy Status, CPU and Memory Utilization, power supply and temperature status, AP and client counts, as well as licenses used. The CPU and temperature graphs can be customized to view particular CPU or temperature sensor information.

Figure 7.9: WLC 360 Detail Information



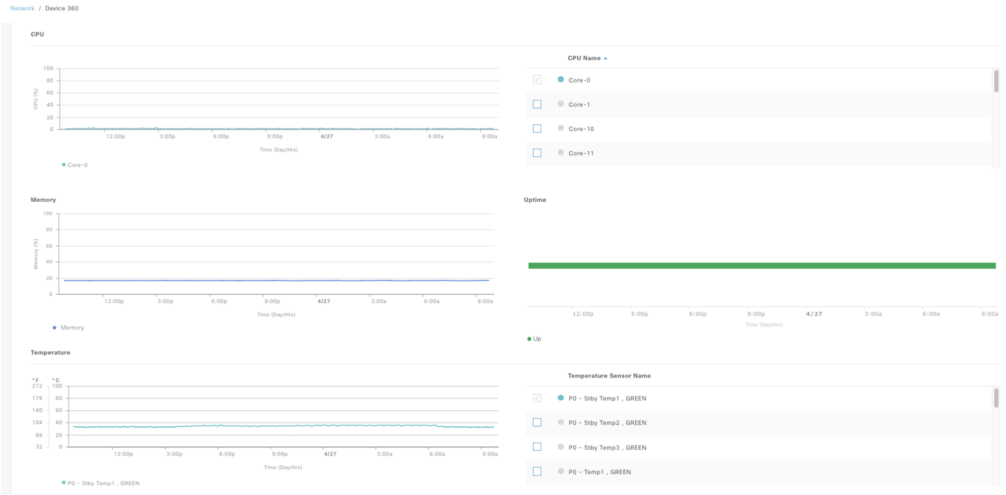
Network / Device 360

Detail Information

Device | Interfaces

Availability	
Uptime	19 days, 11 hours, 52 minutes ⓘ
Last Reset Reason	Install
Primary Power Supply Status	Present, Ok
Secondary Power Supply Status	NA
Internal Temperature	52°C / 126°F ⓘ

HA Redundancy	
Redundancy Mode	SSO
Redundancy Unit	NA
Local State	ACTIVE
Peer state	STANDBY HOT

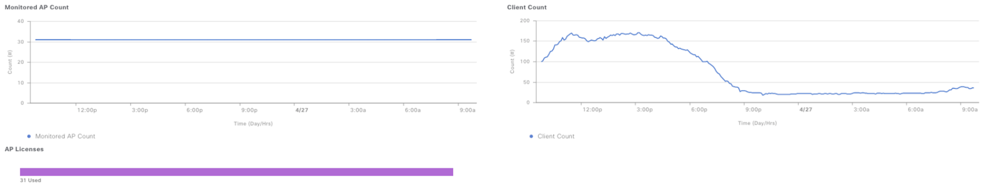


Network / Device 360

	CPU Name ▲
☑	● Core-0
□	● Core-1
□	● Core-10
□	● Core-11

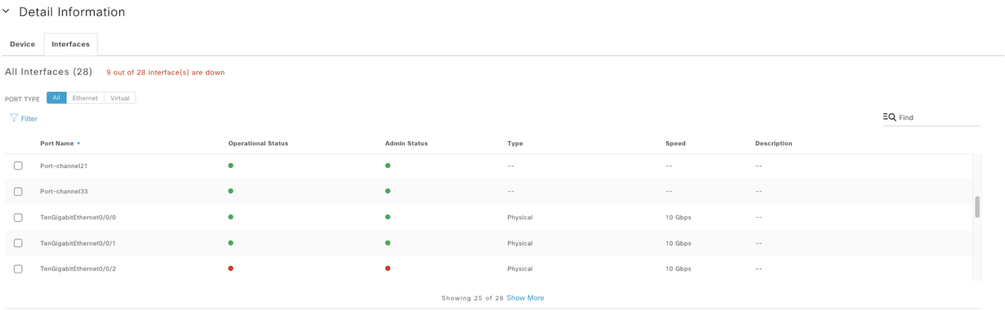
	Temperature Sensor Name
☑	● P0 - Stby Temp1 , GREEN
□	● P0 - Stby Temp2 , GREEN
□	● P0 - Stby Temp3 , GREEN
□	● P0 - Temp1 , GREEN

Figure 7.10: Detail Information Wireless Lan Controller



The `Interface` tab section displays detailed information on the ethernet and virtual interfaces on the Wireless LAN Controller. It shows the admin and operational status, speed, type, and description of each interface.

Figure 7.11: Interfaces Tab in Detail Information



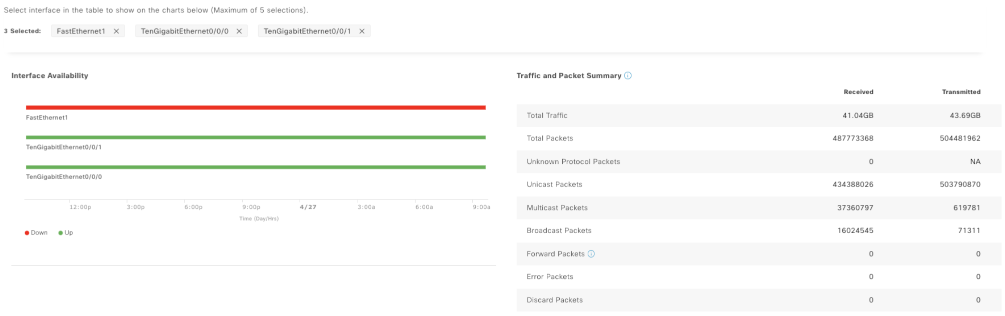
All Interfaces (28) 9 out of 28 interface(s) are down

	Port Name ▾	Operational Status	Admin Status	Type	Speed	Description
☐	Port-channel21	●	●	--	--	--
☐	Port-channel33	●	●	--	--	--
☐	TenGigabitEthernet0/0/0	●	●	Physical	10 Gbps	--
☐	TenGigabitEthernet0/0/1	●	●	Physical	10 Gbps	--
☐	TenGigabitEthernet0/0/2	●	●	Physical	10 Gbps	--

Showing 25 of 28 Show More

The network engineer can select the interfaces from the table to visualize the availability, traffic, and packet summary for those interfaces.

Figure 7.12: Interface Availability and Traffic Summary



Select interface in the table to show on the charts below (Maximum of 5 selections).

3 Selected: FastEthernet1 × TenGigabitEthernet0/0/0 × TenGigabitEthernet0/0/1 ×

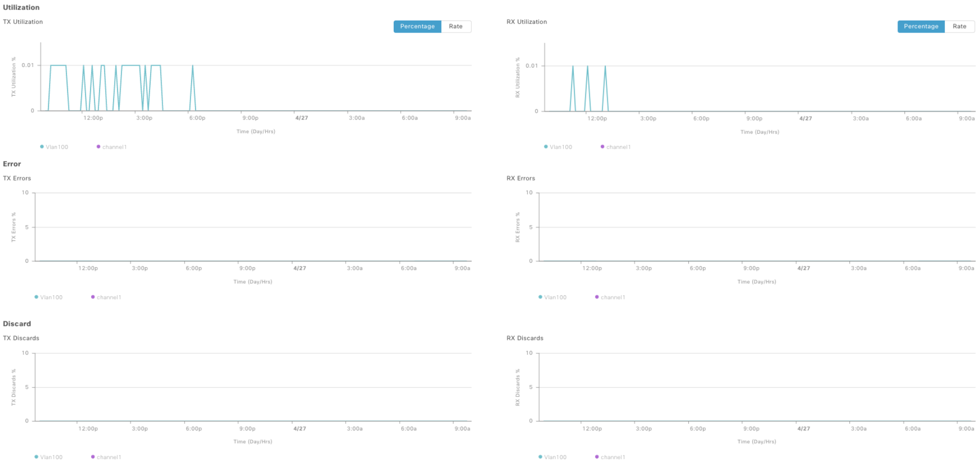
Interface Availability

Traffic and Packet Summary ⓘ

	Received	Transmitted
Total Traffic	41.04GB	43.69GB
Total Packets	487773368	504481962
Unknown Protocol Packets	0	NA
Unicast Packets	434388026	503790870
Multicast Packets	37360797	619781
Broadcast Packets	16024545	71311
Forward Packets ⓘ	0	0
Error Packets	0	0
Discard Packets	0	0

The Interfaces tab has filters to select all interfaces, ethernet, or virtual interfaces. This allows the network engineer to focus on the interfaces they wish to monitor. Selecting the interfaces shows the Tx, Rx, Errors, and Discards graphs for those interfaces over time.

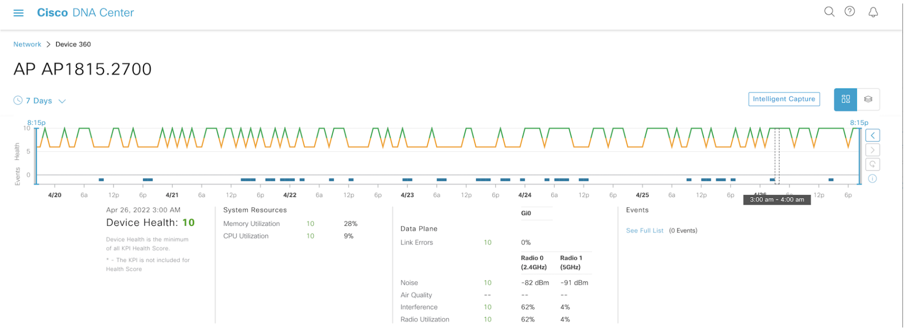
Figure 7.13: Interface Tx, Rx, Errors, and Discards



Access Point - Device 360

The Access Point Device 360 page allows the network engineer to view the current Health Score of access points. When hovering over a point in time, it also shows System Resources such as CPU and memory utilization, link errors, noise, air quality, interference, and radio utilization for both the 2.4Ghz, 5Ghz and 6Ghz bands, as well as any events such as channel changes that have occurred in the period selected. Similar to the WLC Device 360 page, it also allows the network engineer to travel back in time to not only see what the Health Score was at a particular point in time but also why it was assigned a particular health score based on the lowest KPI which was not being met. In addition, the network engineer can also visualize the events that have occurred at that point in time. This helps reduce the time to troubleshoot intermittent issues which can take hours to just a few minutes, as all the hard work is already done by Cisco DNA Center.

Figure 7.14: AP 360



AP AP1815.2700

Apr 26, 2022 3:00 AM

Device Health: 10

Device Health is the minimum of all KPI Health Score.

* - The KPI is not included for Health Score

System Resources

Memory Utilization	10	28%
CPU Utilization	10	9%

Data Plane

		Gi0	
Link Errors	10	0%	
		Radio 0 (2.4GHz)	Radio 1 (5GHz)
Noise	10	-82 dBm	-91 dBm
Air Quality	--	--	--
Interference	10	62%	4%
Radio Utilization	10	62%	4%

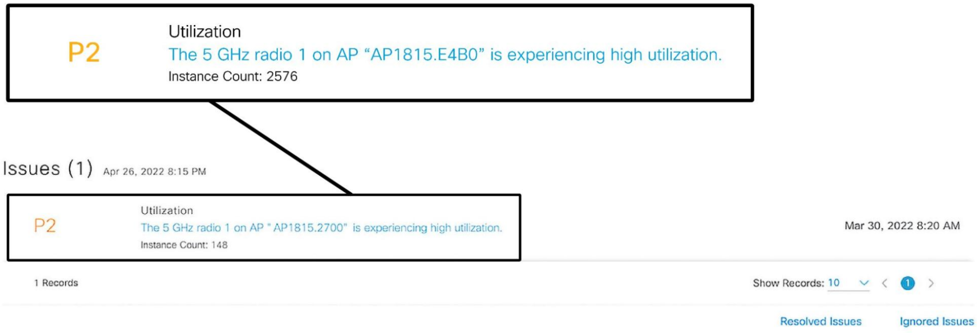
Events

See Full List (0 Events)

Issues

The Issues dashlet displays the issues that have affected the AP within the specified time frame. These issues are sorted by priority.

Figure 7.15: AP 360 Issues



P2
Utilization
The 5 GHz radio 1 on AP “AP1815.E4B0” is experiencing high utilization.
Instance Count: 2576

Issues (1) Apr 26, 2022 8:15 PM

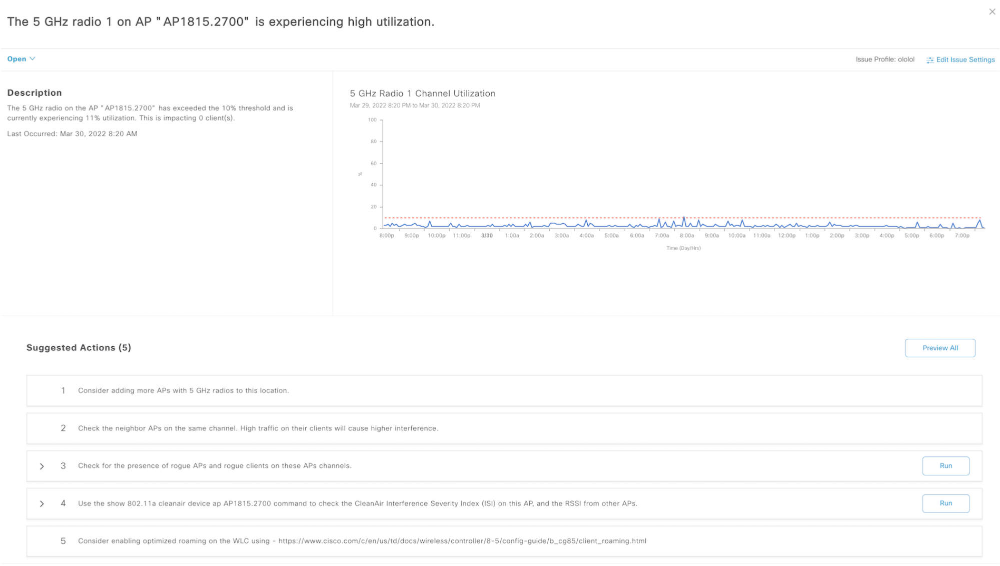
P2
Utilization
The 5 GHz radio 1 on AP " AP1815.2700" is experiencing high utilization.
Instance Count: 148
Mar 30, 2022 8:20 AM

1 Records

Show Records: 10

Clicking on an issue provides the engineer with a description of the problem as well as a list of suggested actions that should be taken to solve that problem. The engineer will also have the option to run commands specified in the Suggested Actions, directly from Cisco DNA Center. This saves the engineer time because it eliminates the need to log into the device and type in the commands manually. The engineer also has the option to Resolve or Ignore the Issue. When ignoring the issue, it can be ignored for 1 hour up to 30 days.

Figure 7.16: AP 360 Issue Details



The 5 GHz radio 1 on AP "AP1815.2700" is experiencing high utilization.

Description

The 5 GHz radio on the AP "AP1815.2700" has exceeded the 10% threshold and is currently experiencing 11% utilization. This is impacting 0 client(s).

Last Occurred: Mar 30, 2022 8:20 AM

Suggested Actions (5)

1 Consider adding more APs with 5 GHz radios to this location.

2 Check the neighbor APs on the same channel. High traffic on their clients will cause higher interference.

3 Check for the presence of rogue APs and rogue clients on these APs channels.

4 Use the show 802.11a cleanair device ap AP1815.2700 command to check the CleanAir Interference Severity Index (ISI) on this AP, and the RSSI from other APs.

5 Consider enabling optimized roaming on the WLC using - https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/client_roaming.html

AI-driven Issues: Radio Throughput

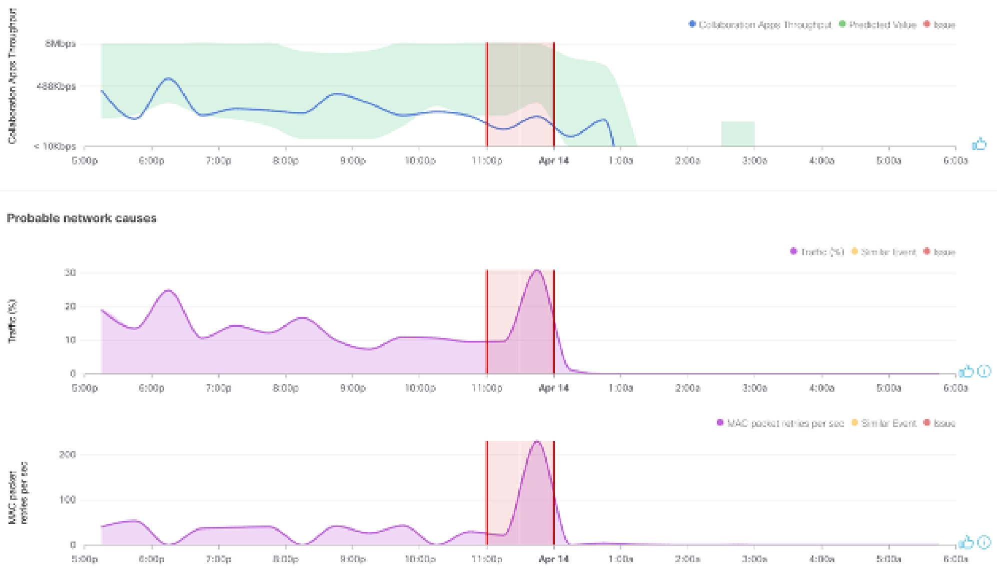
Cisco AI Network Analytics enables monitoring of client experience by generating application throughput baselines for each AP and radio on the network. The available baselines include total radio throughput as well as throughput by similar applications, such as Cloud, Media, Social, and Collaboration applications. Such baselines are generated using Machine Learning models taking multiple network KPIs as inputs, predicting the expected throughput range considering the full network context.

This is a good example of a use case where the traditional, static threshold-based, approach to alerting doesn’t work, as throughput can vary a lot depending on the network conditions.

The issue details include a view of the normal throughput, represented as a green band, along with the actual throughput, displayed as a blue line. The issue is raised when the throughput drops below the baseline and is highlighted in red.

From the issue details, the user can understand what clients were likely to be affected by this issue, and continue the investigation via the Client 360 view, as well as identify the specific applications observed at the time the issue was raised.

Figure 7.17: AI-driven Application Throughput Issue Details



Under the Root Cause Analysis tab, the user is presented with a list of KPIs automatically selected using ML techniques, representing the probable network cause.

The KPIs used to explain issues range from link quality and coverage metrics such as client RSSI/SNR and data rates, RF-related KPIs such as channel utilization and co-channel interference, and load-related KPIs including client count and traffic, up to radio interface metrics such as retransmissions and packet drops. The combination of the root cause KPIs can therefore describe a wide range of issues.

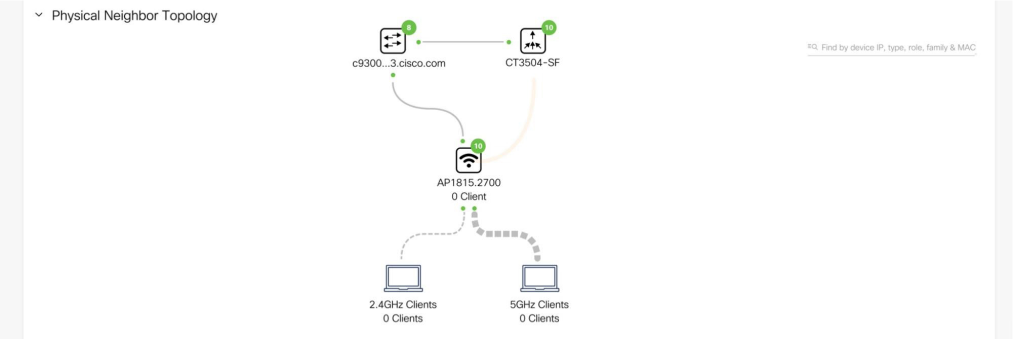
On top of the automatically selected KPIs for root cause analysis, the network engineer can also add more KPIs to the detailed issue view to get full network context, better understand the problem, and reduce the time to resolution.

Note Application Telemetry has to be provisioned to the WLCs for the throughput KPIs and baselines to be generated.

Physical Neighbor Topology

The Physical Neighbor Topology shows the AP's connection to the uplink switch, the WLC to which it is joined, link status, the number of clients on both the 2.4GHz and 5GHz bands, as well as health scores of those neighboring devices. The health scores are also overlaid on top of the devices. This helps the network engineer to quickly visualize if an AP has an issue and the clients which may be affected by it. It also helps the network engineer troubleshoot faster, as all the connectivity information is right at their fingertips.

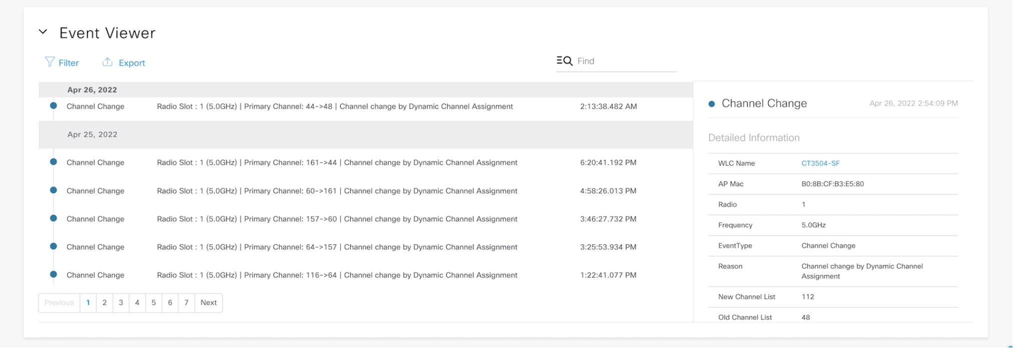
Figure 7.18: AP 360 Physical Neighbor Topology



Event Viewer

The Event Viewer shows a list of all the events that have occurred during the specified time. Clicking on an event displays more information about the event. For instance, Channel Change Events show the Radio Number, the Frequency, the old channel, the new channel, the reason for the change, as well as Interference, Noise, and Channel Utilization.

Figure 7.19: AP 360 Event Viewer



Apr 26, 2022

Channel Change	Radio Slot : 1 (5.0GHz) | Primary Channel: 44->48 | Channel change by Dynamic Channel Assignment	2:13:38.482 AM

Apr 25, 2022

Channel Change	Radio Slot : 1 (5.0GHz) | Primary Channel: 161->44 | Channel change by Dynamic Channel Assignment	6:20:41.192 PM
Channel Change	Radio Slot : 1 (5.0GHz) | Primary Channel: 60->161 | Channel change by Dynamic Channel Assignment	4:58:26.013 PM
Channel Change	Radio Slot : 1 (5.0GHz) | Primary Channel: 157->60 | Channel change by Dynamic Channel Assignment	3:46:27.732 PM
Channel Change	Radio Slot : 1 (5.0GHz) | Primary Channel: 64->157 | Channel change by Dynamic Channel Assignment	3:25:53.934 PM
Channel Change	Radio Slot : 1 (5.0GHz) | Primary Channel: 116->64 | Channel change by Dynamic Channel Assignment	1:22:41.077 PM

● Channel Change Apr 26, 2022 2:54:09 PM

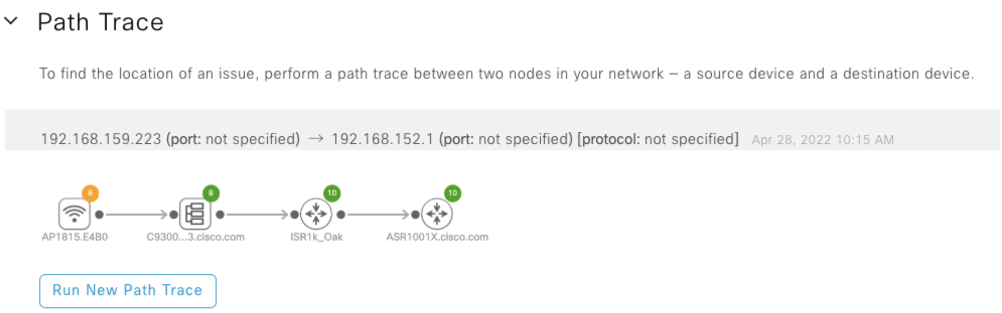
Detailed Information

WLC Name	CT3504-SF
AP Mac	B0:8B:CF:B3:E5:80
Radio	1
Frequency	5.0GHz
EventType	Channel Change
Reason	Channel change by Dynamic Channel Assignment
New Channel List	112
Old Channel List	48

Path Trace

As mentioned earlier in the chapter when discussing Wireless LAN Controllers, Path Trace is also available within the AP 360 page for running a trace from an access point to a destination. The steps and requirements for executing a Path Trace remain the same as mentioned previously.

Figure 7.20: Path Trace



Path Trace

To find the location of an issue, perform a path trace between two nodes in your network – a source device and a destination device.

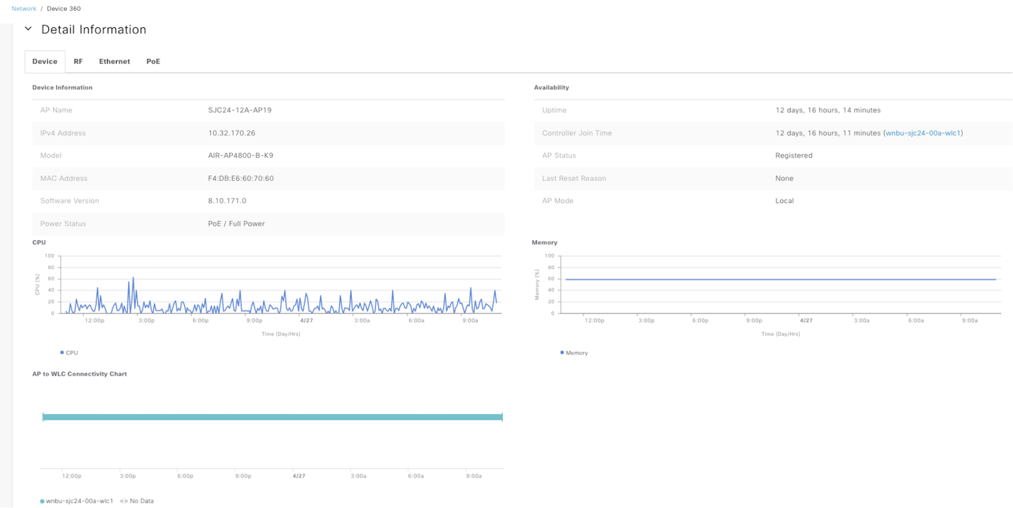
192.168.159.223 (port: not specified) → 192.168.152.1 (port: not specified) [protocol: not specified] Apr 28, 2022 10:15 AM

Detail Information

This section has 4 tabs that display a wealth of information about the access point and its performance. The 4 tabs are: `Device`, `RF`, `Ethernet`, and `PoE`.

The `Device` tab shows helpful information related to the access point such as AP Name, IP Address, Software Version, Power Status, Uptime, Join Status, Last Reset Reason, and AP Mode. It also shows CPU and Memory Utilization and a WLC Connectivity Chart.

Figure 7.21: AP 360 Detail Information Device Tab



Device Information

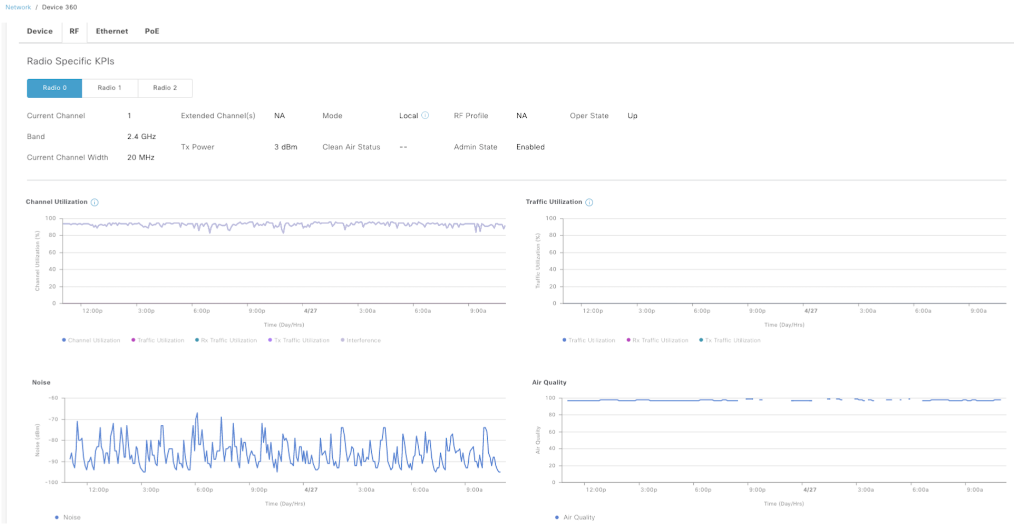
AP Name	SJC24-12A-AP19
IPv4 Address	10.32.170.26
Model	AIR-AP4800-B-K9
MAC Address	F4:DB:E6:60:70:60
Software Version	8.10.171.0
Power Status	PoE / Full Power

Availability

Uptime	12 days, 16 hours, 14 minutes
Controller Join Time	12 days, 16 hours, 11 minutes (wnbu-sjc24-00a-wlc1)
AP Status	Registered
Last Reset Reason	None
AP Mode	Local

The `RF` tab shows radio-specific KPIs for both the 2.4GHz and 5GHz bands. There are tabs for each radio. It also displays crucial troubleshooting information such as Channel Utilization, Traffic Utilization, Noise, Air Quality, Tx Power, Interference, Client Count, Throughput, Retries, Channel Change information over time, Wireless latency, Wireless Airtime Efficiency, and AP Radio Operational State. All this data is shown for the period selected in the AP 360 dashboard filter. For example, if 24 hours was the time selected, then the above data is shown for that period. This helps network engineers know exactly what is happening on each radio of the AP to troubleshoot client issues rapidly.

Figure 7.22: AP 360 Device Details RF Tab



Network / Device 360

Device | RF | Ethernet | PoE

Radio Specific KPIs

Radio 0 | Radio 1 | Radio 2

Current Channel 1

Band 2.4 GHz

Current Channel Width 20 MHz

Extended Channel(s) NA

Tx Power 3 dBm

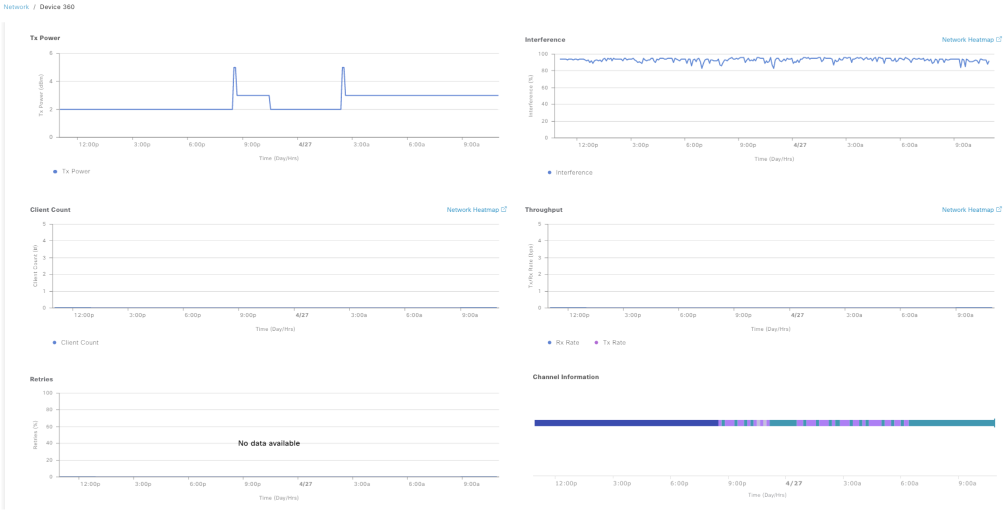
Mode Local

Clean Air Status --

RF Profile NA

Admin State Enabled

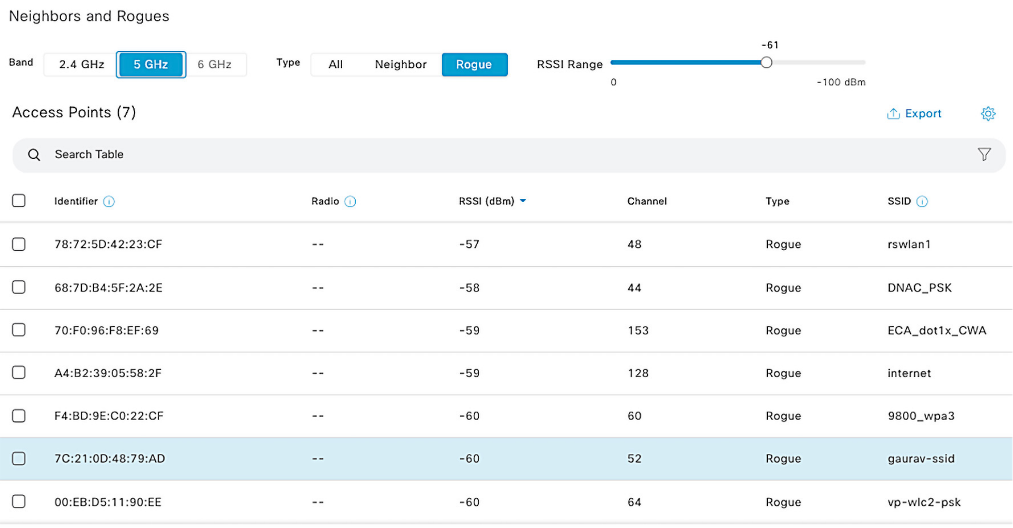
Oper State Up



Network / Device 360

For each radio, the Neighbors and Rogues are also shown in great detail, with the Rogue identifier, RSSI, Channel, Client Count, and Tx Power for each Rogue. Neighbor Rogue APs are also shown with the specific channel they are broadcasting on as well as the RSSI. This helps visualize any security threats quickly and easily for a particular access point.

Figure 7.23: Neighbors and Rogues



Neighbors and Rogues

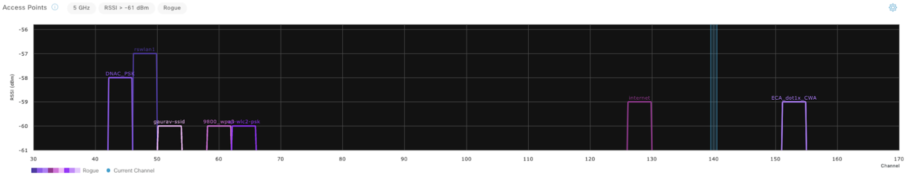
Band: 2.4 GHz | 5 GHz | 6 GHz — Type: All | Neighbor | Rogue — RSSI Range: 0 … -61 … -100 dBm

Access Points (7) — Export

Search Table

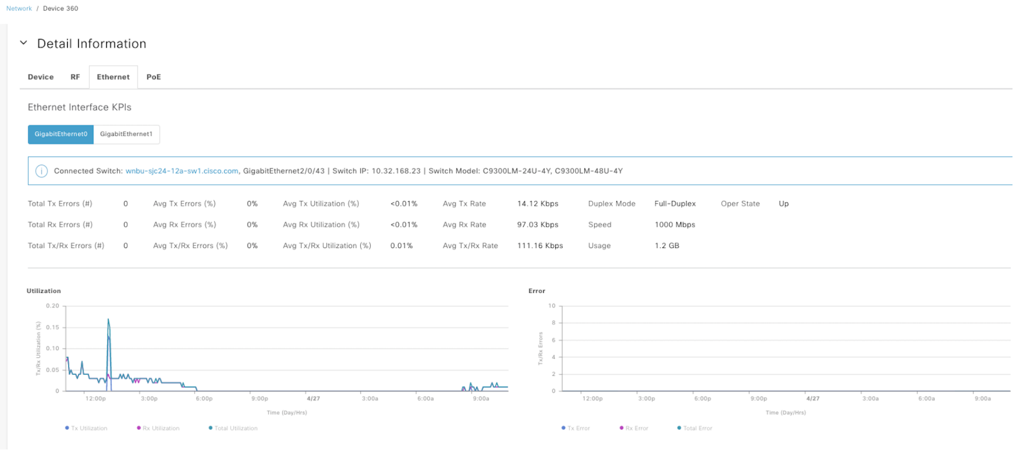
□	Identifier ⓘ	Radio ⓘ	RSSI (dBm)	Channel	Type	SSID ⓘ
□	78:72:5D:42:23:CF	--	-57	48	Rogue	rswlan1
□	68:7D:B4:5F:2A:2E	--	-58	44	Rogue	DNAC_PSK
□	70:F0:96:F8:EF:69	--	-59	153	Rogue	ECA_dot1x_CWA
□	A4:B2:39:05:58:2F	--	-59	128	Rogue	internet
□	F4:BD:9E:C0:22:CF	--	-60	60	Rogue	9800_wpa3
□	7C:21:0D:48:79:AD	--	-60	52	Rogue	gaurav-ssid
□	00:EB:D5:11:90:EE	--	-60	64	Rogue	vp-wlc2-psk

Figure 7.24: Tx Power



The Ethernet Tab displays the detailed information for each ethernet interface on the access point. It shows the connected switch name, IP address, and port number, which makes it easy to locate access points when a network engineer needs to troubleshoot the physical connection. It also has comprehensive information on Tx and Rx utilization and errors in addition to the duplex mode, speed, usage, and operational status.

Figure 7.25: AP 360 Detail Information



Network / Device 360

Detail Information

Device RF Ethernet PoE

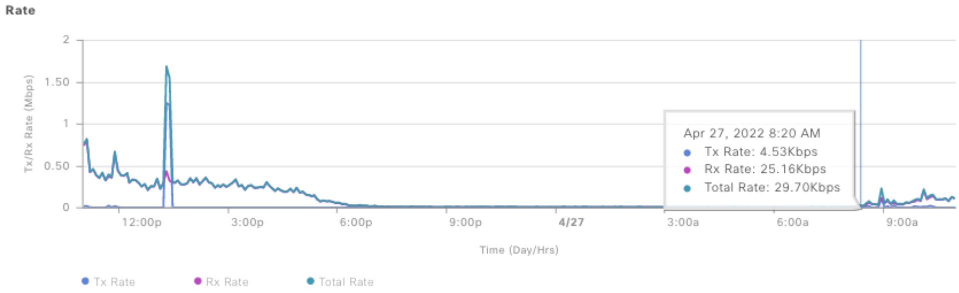
Ethernet Interface KPIs

GigabitEthernet0 GigabitEthernet1

Connected Switch: wnbu-sjc24-12a-sw1.cisco.com, GigabitEthernet2/0/43 | Switch IP: 10.32.168.23 | Switch Model: C9300LM-24U-4Y, C9300LM-48U-4Y

Total Tx Errors (#)	0	Avg Tx Errors (%)	0%	Avg Tx Utilization (%)	<0.01%	Avg Tx Rate	14.12 Kbps	Duplex Mode	Full-Duplex	Oper State	Up
Total Rx Errors (#)	0	Avg Rx Errors (%)	0%	Avg Rx Utilization (%)	<0.01%	Avg Rx Rate	97.03 Kbps	Speed	1000 Mbps		
Total Tx/Rx Errors (#)	0	Avg Tx/Rx Errors (%)	0%	Avg Tx/Rx Utilization (%)	0.01%	Avg Tx/Rx Rate	111.16 Kbps	Usage	1.2 GB		

Figure 7.26: AP 360 Device Detail Ethernet Tab



The `PoE` tab displays detailed information on the PoE port to which the access point is connected. The network engineer can view the switch name, interface name, admin and operational status, power consumption details, and the type of power used by the access point. This helps network engineers troubleshoot any PoE issues concerning the access point which can affect all the clients connected to it. The information here helps the network engineer to instantly view any PoE issues and fix them to minimize the downtime for the clients.

Intelligent Capture

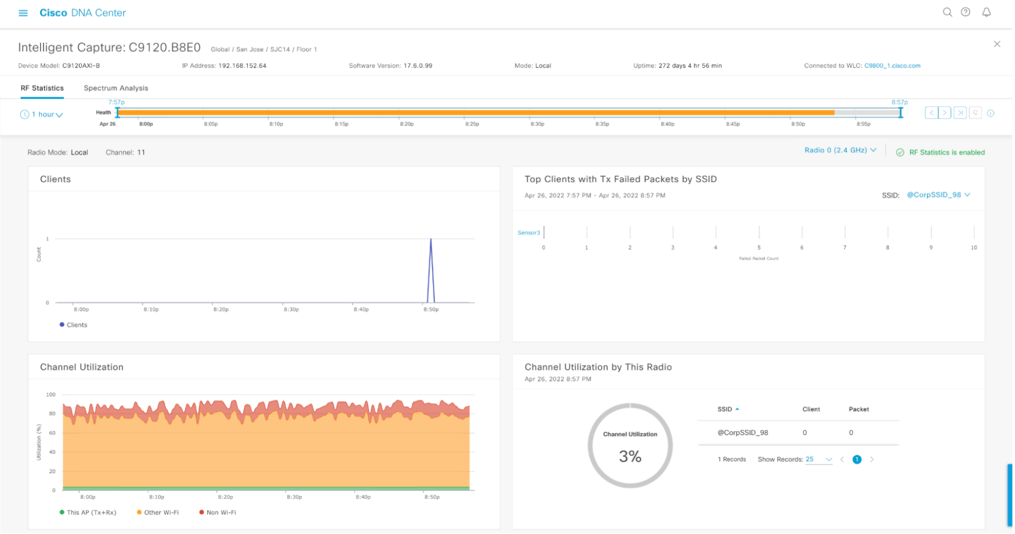
Clicking on the Intelligent Capture button in the upper right corner of the Access Point Device 360 Page brings you to the RF Statistics Page. This page displays even more troubleshooting information related to Clients:

- Clients with Transmit Failed Packets per SSID
- Channel Utilization
- Channel Utilization by This Radio
- Management and Data Frame Type Counts
- Transmit and Receive Frame Errors
- Transmit Power and Noise Floor
- Broadcast/Multicast Counters

This data is almost real time as it updates every 60 to 90 seconds. It gives the network engineer a real-world view of the RF environment which helps troubleshoot RF issues.

Intelligent Capture provides support for a direct communication link between Cisco DNA Center and access points (APs), so each of the APs can communicate with Cisco DNA Center directly. Using this channel, Cisco DNA Center can receive packet capture (PCAP) data, AP and client statistics, and spectrum data. With the direct link from the AP to Cisco DNA Center via gRPC, Intelligent Capture allows access to data from APs that is not available from wireless controllers, allowing network engineers to resolve even the most difficult wireless issues.

Figure 7.27: AP Intelligent Capture



Cisco DNA Center

Intelligent Capture: C9120.B8E0 Global / San Jose / SJC14 / Floor 1

Device Model: C9120AXI-B IP Address: 192.168.152.64 Software Version: 17.6.0.99 Mode: Local Uptime: 272 days 4 hr 56 min Connected to WLC: C9800_1.cisco.com

Radio Mode: Local Channel: 11 Radio 0 (2.4 GHz) RF Statistics is enabled

Top Clients with Tx Failed Packets by SSID

Apr 26, 2022 7:57 PM - Apr 26, 2022 8:57 PM SSID: @CorpSSID_98

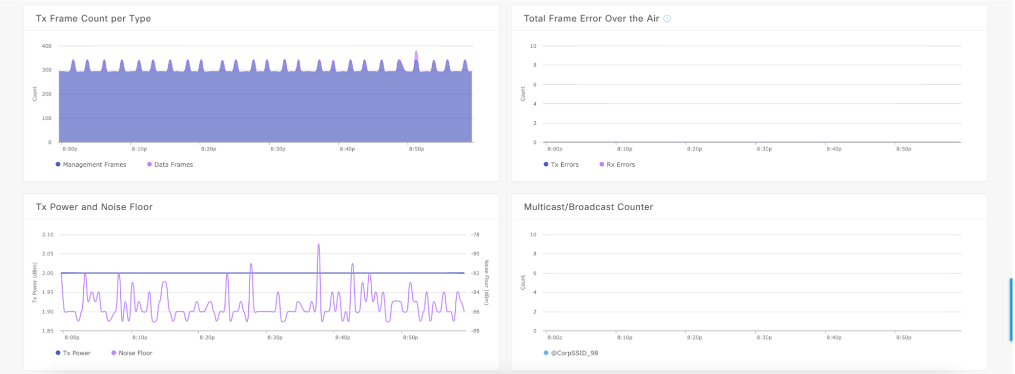
Channel Utilization by This Radio

Apr 26, 2022 8:57 PM

Channel Utilization 3%

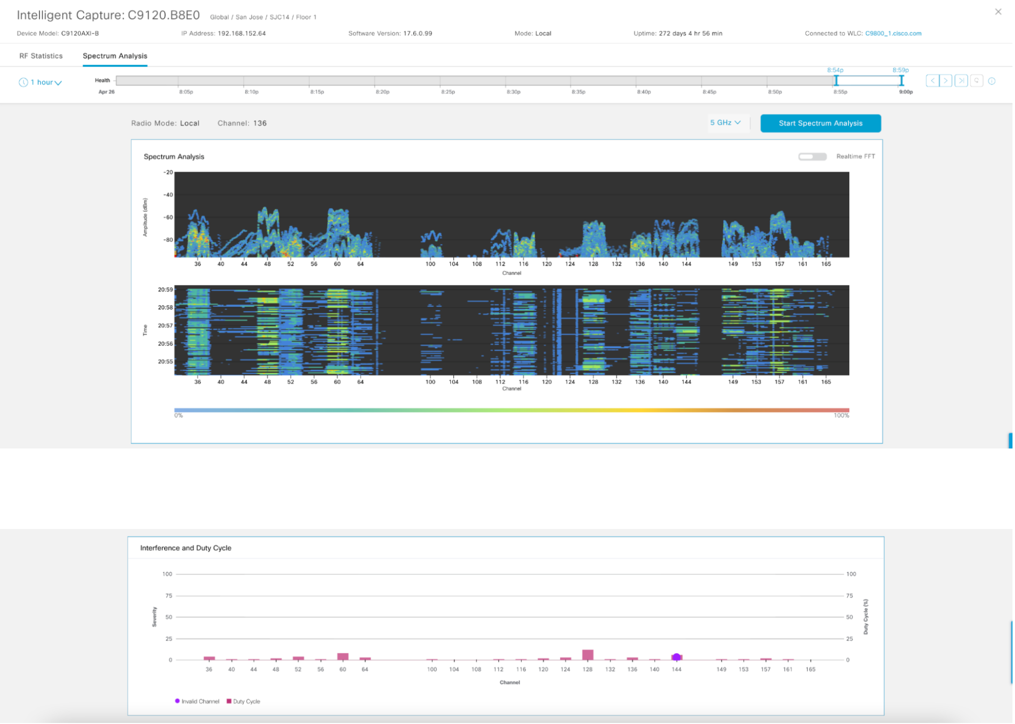
SSID	Client	Packet
@CorpSSID_98	0	0

1 Records Show Records: 25



A Spectrum Analyzer view is also available to show the raw RF energy as received by this AP. This allows the engineer to visualize Co-Channel Interference, Adjacent-Channel Interference, Narrowband Interference, and other sources of interference in the RF environment. This is available in both the 2.4GHz and 5GHz bands. Various views are available consisting of the Fast-Fourier Transform (FFT) view of the RF energy at a single point in time or continuously in real time. There is also a waterfall view that displays the RF energy over time, as well as interference and duty-cycle view, which shows the percentage of the amount of time an Interferer is broadcasting. This provides insight into what's going on in the RF environment surrounding an AP to better understand why wireless issues may be occurring for clients.

Figure 7.28: AP Intelligent Packet Capture Spectrum Analyzer



Intelligent Capture: C9120.B8E0 Global / San Jose / SJC14 / Floor 1

Device Model: C9120AXI-B IP Address: 192.168.152.64 Software Version: 17.6.0.99 Mode: Local Uptime: 272 days 4 hr 56 min Connected to WLC: C9800_1.cisco.com

Radio Mode: Local Channel: 136

Real-World Scenario

Adam is a wireless engineer at a law firm. All users in one corner of the building have been complaining about poor performance on wireless. He logs into Cisco DNA Center and sees that one AP located near that corner had a poor Health Score due to interference. He navigates to the Intelligent Capture on the Access Point 360 page. He then navigates to the Spectrum Analysis tab and notices from both the Waterfall and Interference and Duty Cycle views that something is interfering with the entire UNII-3 band with over a 90% Duty Cycle. He can either find and remove the device or devices causing the interference or move the APs off of the channels affected by the interference.

8. Wired Monitoring and Troubleshooting

Cisco DNA Center offers a variety of tools that are useful for monitoring and troubleshooting wired devices in the network. This chapter covers innovations in PoE, Machine Reasoning, and path tracing providing insights for wired devices managed by Cisco DNA Center.

Wired Monitoring

Power Over Ethernet (PoE)

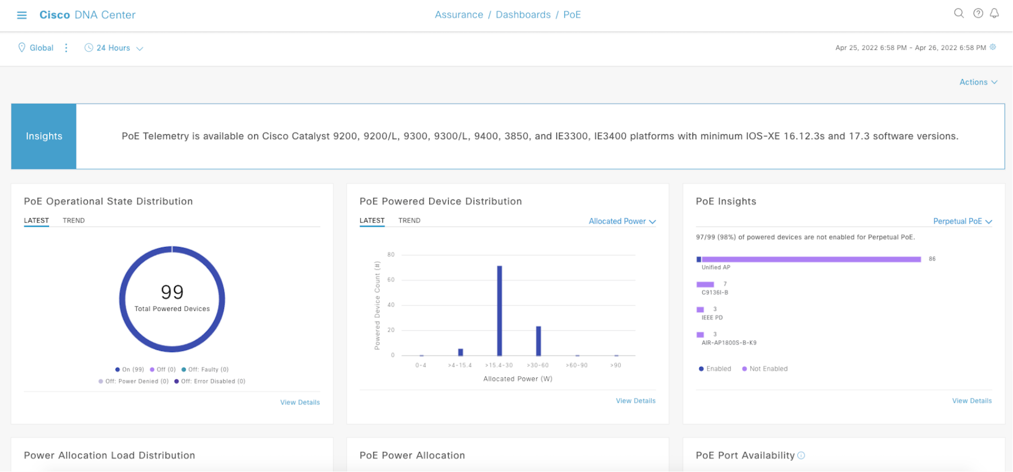
With the recent, rapid innovations in Power over Ethernet, many prominent industries including networking, heavy industry, healthcare, and education are continuing to increase their adoption of PoE-capable and IoT devices. The new features presented in Cisco DNA Center surrounding PoE provide insight into individual devices as well as a holistic view of PoE performance across the entire network.

PoE Dashboard

The PoE Dashboard provides a full view of PoE availability and distribution across the network. A series of insights and dashlets provides a variety of PoE Information including:

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

Figure 8.1: PoE Dashboard



PoE Telemetry is available on Cisco Catalyst 9200, 9200/L, 9300, 9300/L, 9400, 3850, and IE3300, IE3400 platforms with minimum IOS-XE 16.12.3s and 17.3 software versions.

97/99 (98%) of powered devices are not enabled for Perpetual PoE.

These dashlets are especially valuable in planning PoE and IoT deployments, as well as monitoring the overall power budget and consumption across the network.

Figure 8.2: PoE Operational State Distribution

The PoE Operational State Distribution dashlet provides information about how many powered devices are currently in the network, as well as their current operational state. Expanding the details for the dashlet provides a complete list of powered devices and their respective PoE information.

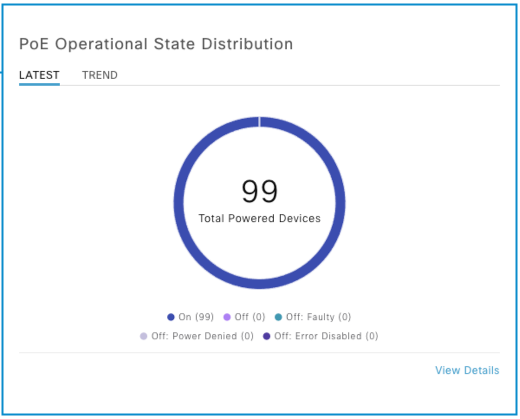
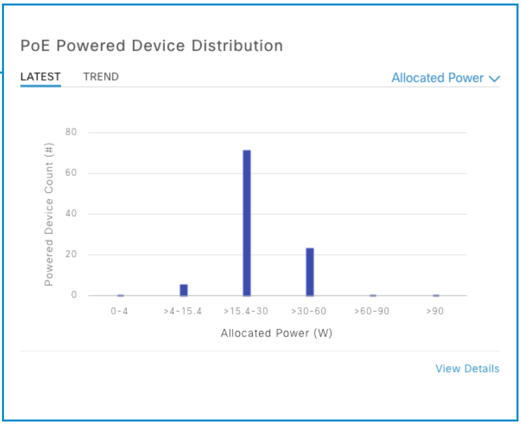
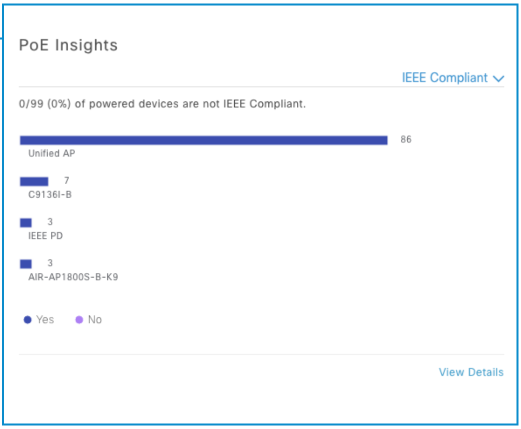


Figure 8.3: PoE Powered Device Distribution



The PoE Powered Device Distribution dashlet shows the power allocation as it is distributed amongst the entire network. This allows a network engineer to quickly identify how much of the network consists of high-powered vs low-powered devices. This is useful for PoE budget planning and power distribution management across devices. The dashlet also shows respective locations for both types of devices by expanding `View Details`. In addition to distribution by allocated power, the distributions by Powered Device Class and Powered Device Type can also be selected.

Figure 8.4: PoE Insights

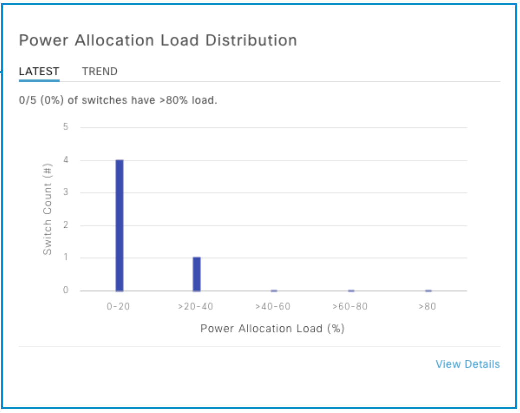


0/99 (0%) of powered devices are not IEEE Compliant.

The PoE Insights dashlet provides a breakdown of devices by device type, sorted in order from the greatest number of devices to the fewest. The dashlet is useful for indicating how many of each device type are enabled for:

- IEEE Compliance
- Perpetual PoE
- Fast PoE
- UPoE+

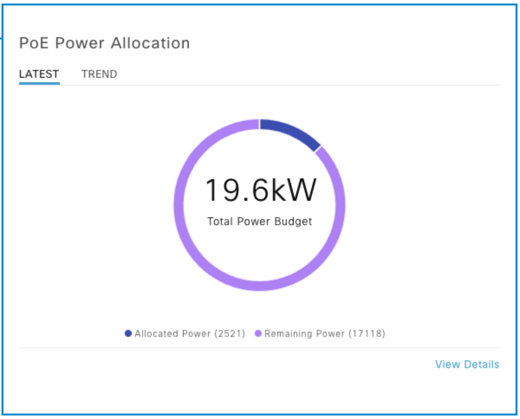
Figure 8.5: Power Allocation Load Distribution



0/5 (0%) of switches have >80% load.

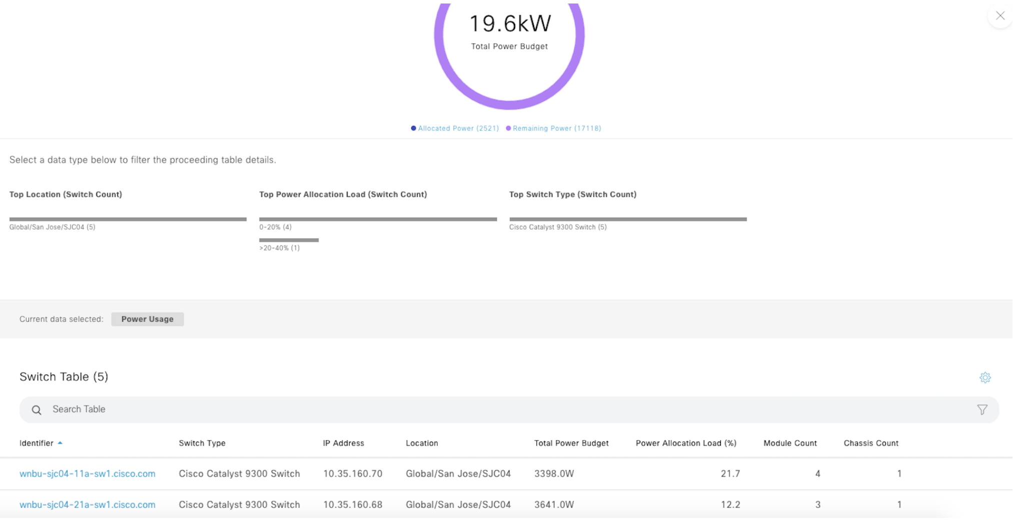
The Power Allocation Load Distribution dashlets provide an aggregated overview of all PoE-enabled switches in the network and the breakdown of their current power loads as a percentage. More information about each of the individual switches and their total power load can be seen under `View Details`. This dashlet is a critical part of PoE budget management and ensures that adding devices does not lead to **power denied** errors, especially in environments where PoE-based devices are not in a fixed location.

Figure 8.6: PoE Power Allocation



The dashlet for PoE Power Allocation displays the entire overall power budget across all PoE-capable switches in the network and divides it into the percentage of the power budget used and the percentage of the power budget still available. Click `View Details` and select `Allocated Power` from the graph to see the list of PoE-capable switches with their power load percentage.

Figure 8.7: Power Allocation View Details



Select a data type below to filter the proceeding table details.

Top Location (Switch Count)

Global/San Jose/SJC04 (5)

Top Power Allocation Load (Switch Count)

0-20% (4)

>20-40% (1)

Top Switch Type (Switch Count)

Cisco Catalyst 9300 Switch (5)

Current data selected: **Power Usage**

Switch Table (5)

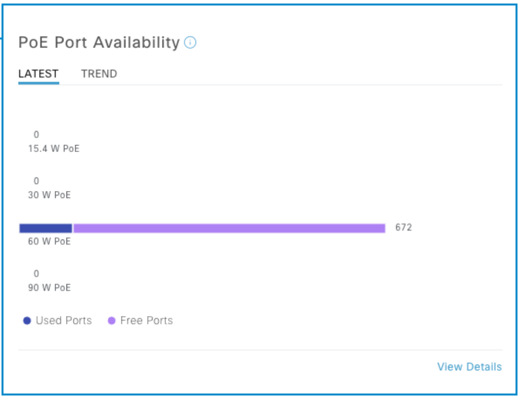
Search Table

Identifier ▲	Switch Type	IP Address	Location	Total Power Budget	Power Allocation Load (%)	Module Count	Chassis Count
wnbu-sjc04-11a-sw1.cisco.com	Cisco Catalyst 9300 Switch	10.35.160.70	Global/San Jose/SJC04	3398.0W	21.7	4	1
wnbu-sjc04-21a-sw1.cisco.com	Cisco Catalyst 9300 Switch	10.35.160.68	Global/San Jose/SJC04	3641.0W	12.2	3	1

Real-World Scenario

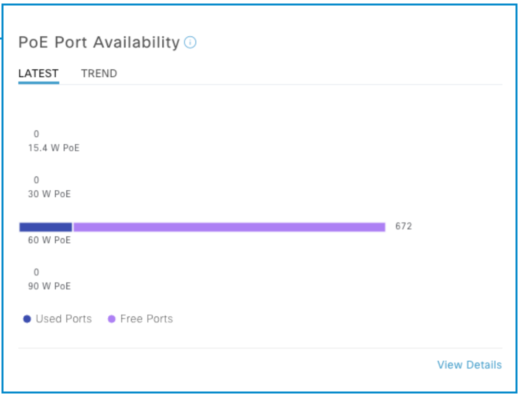
Royee works for a publisher as a Wireless Engineer. He is working on a project to refresh the wireless network with new Catalyst 9130 access points. He notices that in Building 24 on the 3rd floor, a handful of access points are not powering up. He logs into Cisco DNA Center and drills down to the 3rd floor in Building 24 and selects the switch stack where the APs were refreshed. By clicking on the PoE tab, he can see that one of the switches in the stack has no remaining power available. He then distributes the APs to other switches in the stack to provide the necessary power to run all of the new APs.

Figure 8.8: PoE Port Availability



PoE Port Availability provides the distribution of PoE ports, sorted by the amount of power allocated to the ports, and provides the breakdown of free vs allocated ports for each power level.

Figure 8.9: PoE Port Availability



Lastly, the PoE AP Power Mode Distribution dashlet shows how many PoE-capable access points in the network are fully powered versus partially powered. This perspective is important when it comes to running devices such as wireless access points where the inability to get full power results in possibly disabling some radios or reducing radio power capabilities. As increasingly, smart building functions rely on PoE power, this dashlet can be a critical troubleshooting dashboard.

PoE StackWise on Device 360

In addition to providing a high-level overview of PoE capability across the entire network, as seen in the previous section, Cisco DNA Center also provides an individual switch view of that particular switch's PoE capability and capacity. From the Device 360 page, all of the respective power budget and allocation details are provided, with information about PoE devices that are connected and receiving power from the switch. In addition, this feature supports PoE StackWise Switching and provides the respective power module information for the entire switch stack.

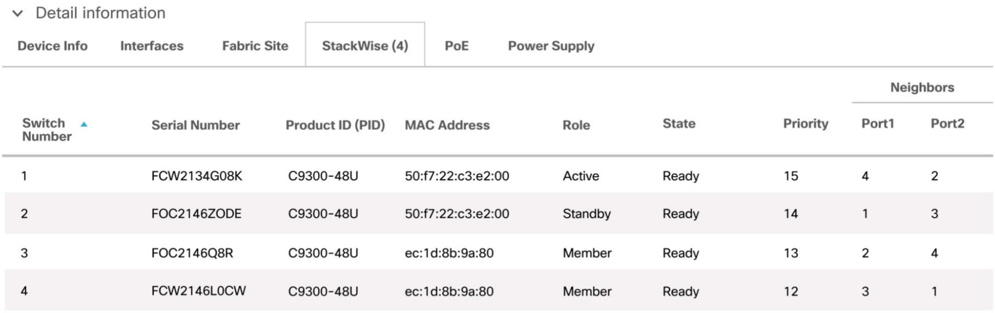
To navigate to Device 360, start by heading to `Assurance > Overall` from the Cisco DNA Center main menu, as demonstrated in **Chapter 4**, then select the `Network` menu from the top. At the bottom of the Network Dashboard page, select a PoE-capable switch from the list of all networking devices by clicking its hostname. If a switch's hostname is already known, the search bar may also be used to access its Device 360 page directly.

At the top of the page, select one of the three new menu options to go to its section in the Device 360 view:

- StackWise (for StackWise configured switches)
- PoE
- Power Supply

The StackWise section shows detailed information about the StackWise configuration for this switch, including device information, switch stack number, and stack member's role/state information.

Figure 8.10: StackWise Switch

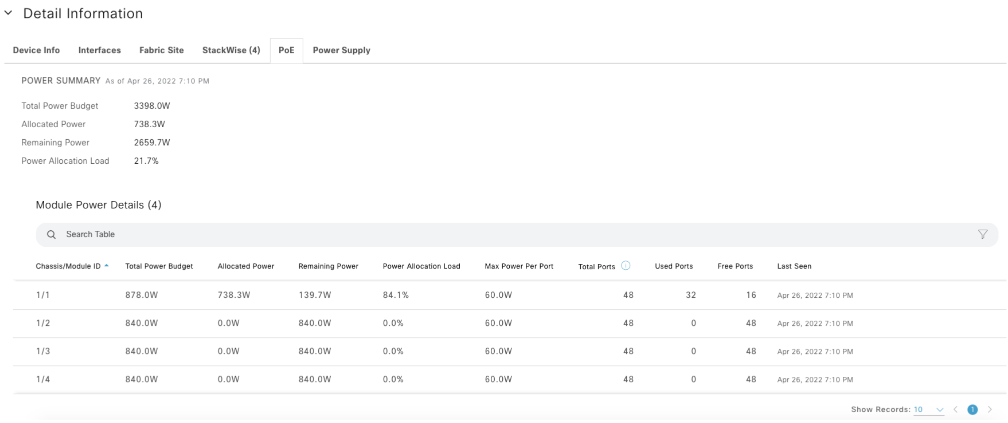


Detail information

							Neighbors	
Switch Number ▲	Serial Number	Product ID (PID)	MAC Address	Role	State	Priority	Port1	Port2
1	FCW2134G08K	C9300-48U	50:f7:22:c3:e2:00	Active	Ready	15	4	2
2	FOC2146ZODE	C9300-48U	50:f7:22:c3:e2:00	Standby	Ready	14	1	3
3	FOC2146Q8R	C9300-48U	ec:1d:8b:9a:80	Member	Ready	13	2	4
4	FCW2146L0CW	C9300-48U	ec:1d:8b:9a:80	Member	Ready	12	3	1

The PoE section provides details about the overall power budget, how much power is allocated, and what the current load distribution is. The power module details are also shown here, and all power modules for StackWise switches will be listed with details.

Figure 8.11: PoE Power Details



Detail Information

POWER SUMMARY As of Apr 26, 2022 7:10 PM

Total Power Budget	3398.0W
Allocated Power	738.3W
Remaining Power	2659.7W
Power Allocation Load	21.7%

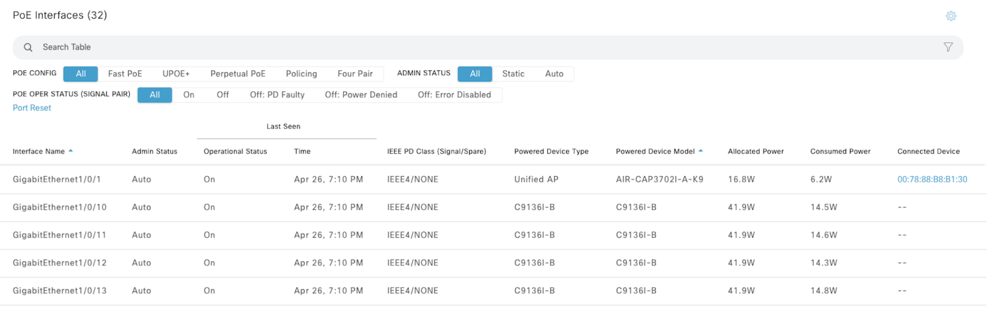
Module Power Details (4)

Chassis/Module ID	Total Power Budget	Allocated Power	Remaining Power	Power Allocation Load	Max Power Per Port	Total Ports	Used Ports	Free Ports	Last Seen
1/1	878.0W	738.3W	139.7W	84.1%	60.0W	48	32	16	Apr 26, 2022 7:10 PM
1/2	840.0W	0.0W	840.0W	0.0%	60.0W	48	0	48	Apr 26, 2022 7:10 PM
1/3	840.0W	0.0W	840.0W	0.0%	60.0W	48	0	48	Apr 26, 2022 7:10 PM
1/4	840.0W	0.0W	840.0W	0.0%	60.0W	48	0	48	Apr 26, 2022 7:10 PM

Show Records: 10

Below the Power Module Details, the PoE interfaces for the switch are displayed, showing all powered devices that are connected to each switchport. For each device, the respective PoE information includes device type, IEEE compliance, allocated power, and consumed power. The PoE interface provides various filters to allow quick pre-defined filter selections for PoE config modes, admin status, and PoE operational status of ports.

Figure 8.12: PoE Interfaces



PoE Interfaces (32)

		Last Seen							
Interface Name	Admin Status	Operational Status	Time	IEEE PD Class (Signal/Spare)	Powered Device Type	Powered Device Model	Allocated Power	Consumed Power	Connected Device
GigabitEthernet1/0/1	Auto	On	Apr 26, 7:10 PM	IEEE4/NONE	Unified AP	AIR-CAP3702I-A-K9	16.8W	6.2W	00:78:88:B8:B1:30
GigabitEthernet1/0/10	Auto	On	Apr 26, 7:10 PM	IEEE4/NONE	C9136I-B	C9136I-B	41.9W	14.5W	--
GigabitEthernet1/0/11	Auto	On	Apr 26, 7:10 PM	IEEE4/NONE	C9136I-B	C9136I-B	41.9W	14.6W	--
GigabitEthernet1/0/12	Auto	On	Apr 26, 7:10 PM	IEEE4/NONE	C9136I-B	C9136I-B	41.9W	14.3W	--
GigabitEthernet1/0/13	Auto	On	Apr 26, 7:10 PM	IEEE4/NONE	C9136I-B	C9136I-B	41.9W	14.8W	--

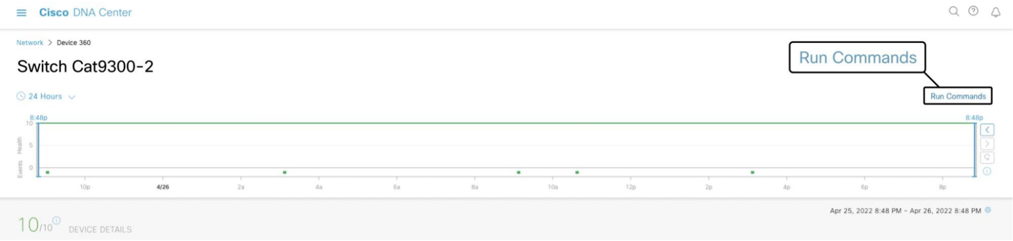
Command Runner

Although Cisco DNA Center restricts direct command-line interface (CLI) access to a device that is managed by Cisco DNA Center, the capability to run show commands on a network device from within Cisco DNA Center itself is incredibly useful for ensuring that configurations have been appropriately applied to the device and performing troubleshooting.

The Command Runner feature is used to run these show commands on various network devices. The Command Runner is accessible from a network device's Device 360 page.

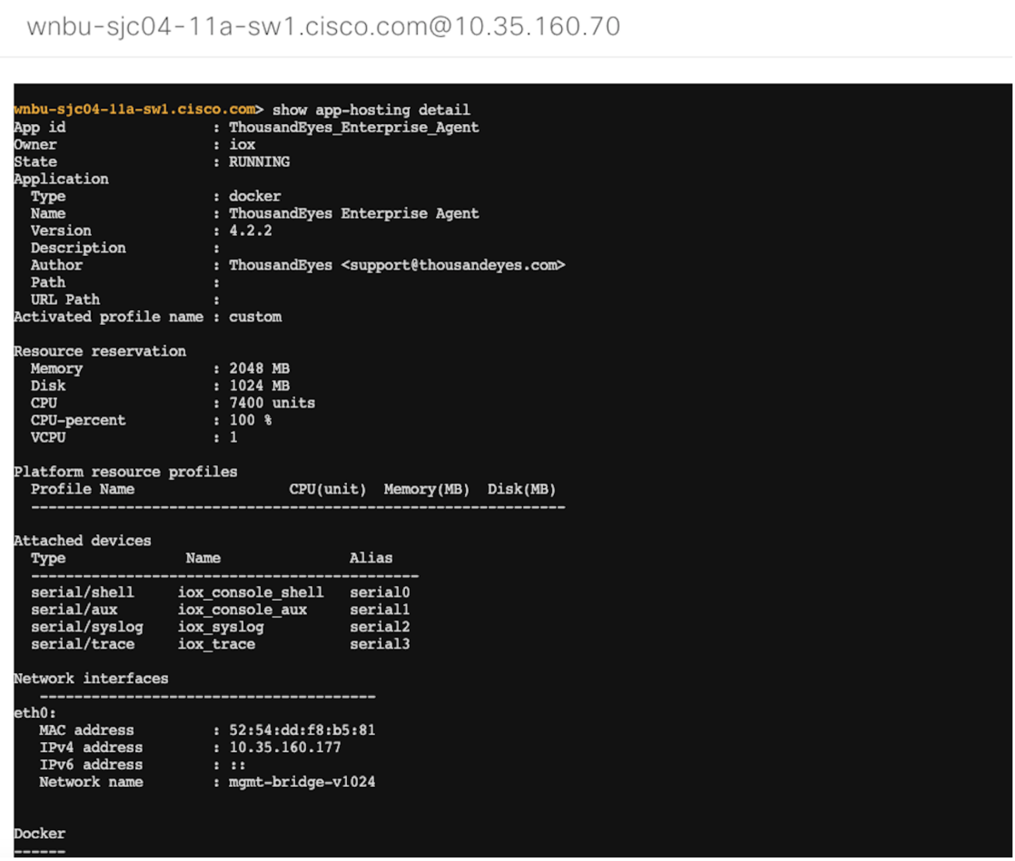
From the Device 360 page, click `Run Commands` on the right side of the page, above the timeline.

Figure 8.13: Device 360 Run Commands



In the following example, the switch that has been selected has a hosted application whose container needs to be verified if it is currently running or not. By entering the command: *show app-hosting detail,* the command is run on the device and the results are returned and presented. This ensures that a network engineer can easily monitor networking devices and verify configurations, even via CLI, directly through Cisco DNA Center.

Figure 8.14: Command Runner



wnbu-sjc04-11a-sw1.cisco.com@10.35.160.70

```
wnbu-sjc04-11a-sw1.cisco.com> show app-hosting detail
App id                 : ThousandEyes_Enterprise_Agent
Owner                  : iox
State                  : RUNNING
Application
  Type                 : docker
  Name                 : ThousandEyes Enterprise Agent
  Version              : 4.2.2
  Description          :
  Author               : ThousandEyes <support@thousandeyes.com>
  Path                 :
  URL Path             :
Activated profile name : custom

Resource reservation
  Memory               : 2048 MB
  Disk                 : 1024 MB
  CPU                  : 7400 units
  CPU-percent          : 100 %
  VCPU                 : 1

Platform resource profiles
  Profile Name                  CPU(unit)  Memory(MB)  Disk(MB)
  --------------------------------------------------------------

Attached devices
  Type              Name               Alias
  ---------------------------------------------
  serial/shell     iox_console_shell   serial0
  serial/aux       iox_console_aux     serial1
  serial/syslog    iox_syslog          serial2
  serial/trace     iox_trace           serial3

Network interfaces
   ---------------------------------------
eth0:
   MAC address         : 52:54:dd:f8:b5:81
   IPv4 address        : 10.35.160.177
   IPv6 address        : ::
   Network name        : mgmt-bridge-v1024


Docker
------
```

Wired Troubleshooting

In addition to the wide host of monitoring tools available for wired devices in the Cisco DNA Center, there are many features available that can assist a network engineer to quickly identify the root cause of a problem and also help to remedy it and reduce the MTTR for issues.

Device 360

The Device 360 view is one of the many lenses that Cisco DNA Center offers to provide rich and meaningful insights into the details of network devices, including their event history, historical health information, and connected interface information.

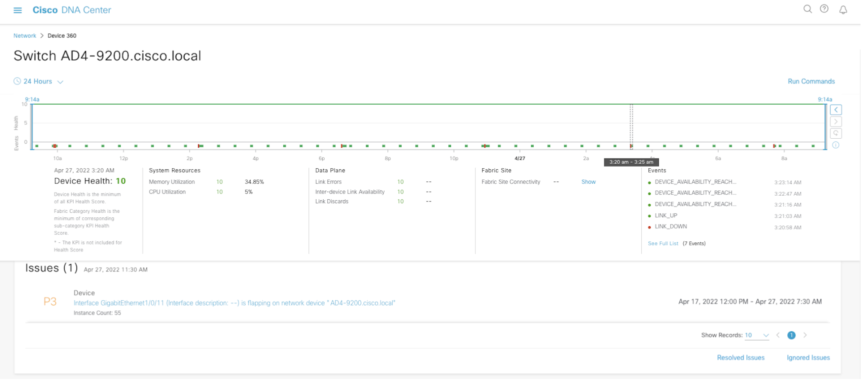
At first glance, the Device 360 page provides details about the selected device including:

- Model
- Management IP
- Location
- Software version
- Role
- High Availability status
- Uptime
- Reachability

The Device 360 view shows the same timeline that is displayed on many Cisco DNA Center pages shown previously. This allows a network engineer to hover over a specific point on the timeline and view the respective health score metric for the device at that point in time, as well as any events that occurred. Additionally, the time interval selector that was shown in previous sections can be utilized here to go back in time up to 30 days and see historical health score metrics and event information for the device.

An Issues table is also presented below, showing issues that affected this device within the period selected. Clicking on a particular issue directly provides detailed issue information as well as suggested steps for remediation, without having to leave the Device 360 page. All of these features combine to allow for much faster and more streamlined device troubleshooting and issue resolution.

Figure 8.15: Device 360 Overview



Switch AD4-9200.cisco.local

Apr 27, 2022 3:20 AM

Device Health: 10

Device Health is the minimum of all KPI Health Score.

Fabric Category Health is the minimum of corresponding sub-category KPI Health Score.

* - The KPI is not included for Health Score

System Resources

Memory Utilization	10	34.85%
CPU Utilization	10	5%

Data Plane

Link Errors	10	--
Inter-device Link Availability	10	--
Link Discards	10	--

Fabric Site

Fabric Site Connectivity	--	Show

Events

● DEVICE_AVAILABILITY_REACH...	3:23:14 AM
● DEVICE_AVAILABILITY_REACH...	3:22:47 AM
● DEVICE_AVAILABILITY_REACH...	3:21:16 AM
● LINK_UP	3:21:03 AM
● LINK_DOWN	3:20:58 AM

See Full List (7 Events)

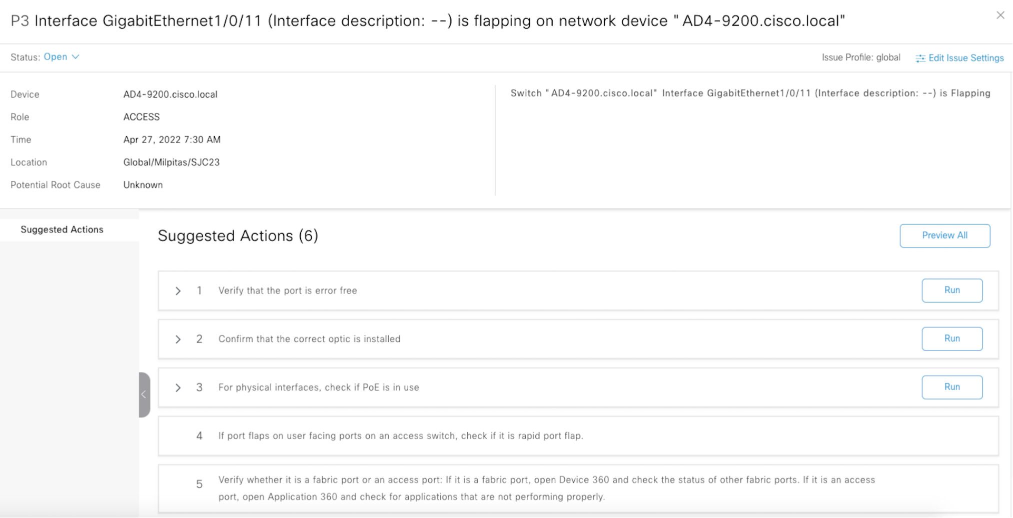
Issues (1) Apr 27, 2022 11:30 AM

P3 Device
Interface GigabitEthernet1/0/11 (Interface description: --) is flapping on network device " AD4-9200.cisco.local"
Instance Count: 55
Apr 17, 2022 12:00 PM - Apr 27, 2022 7:30 AM

Show Records: 10

Resolved Issues Ignored Issues

Figure 8.16: Device 360 Issue



P3 Interface GigabitEthernet1/0/11 (Interface description: --) is flapping on network device " AD4-9200.cisco.local"

Status: Open

Issue Profile: global

Device	AD4-9200.cisco.local
Role	ACCESS
Time	Apr 27, 2022 7:30 AM
Location	Global/Milpitas/SJC23
Potential Root Cause	Unknown

Switch " AD4-9200.cisco.local" Interface GigabitEthernet1/0/11 (Interface description: --) is Flapping

Suggested Actions (6)

1 Verify that the port is error free

2 Confirm that the correct optic is installed

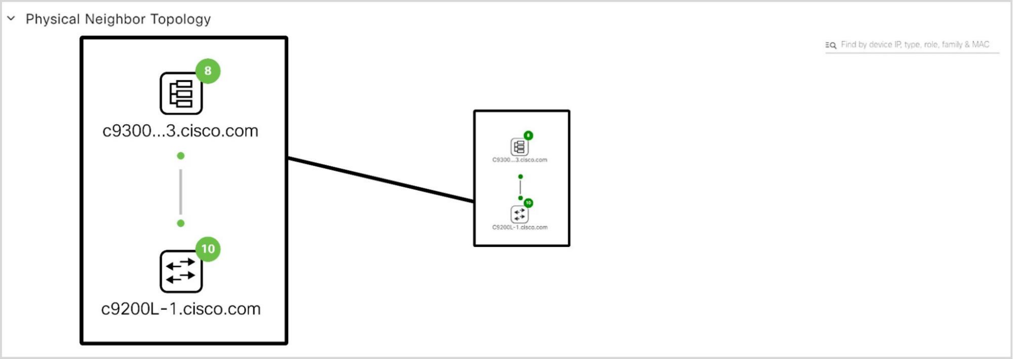
3 For physical interfaces, check if PoE is in use

4 If port flaps on user facing ports on an access switch, check if it is rapid port flap.

5 Verify whether it is a fabric port or an access port: If it is a fabric port, open Device 360 and check the status of other fabric ports. If it is an access port, open Application 360 and check for applications that are not performing properly.

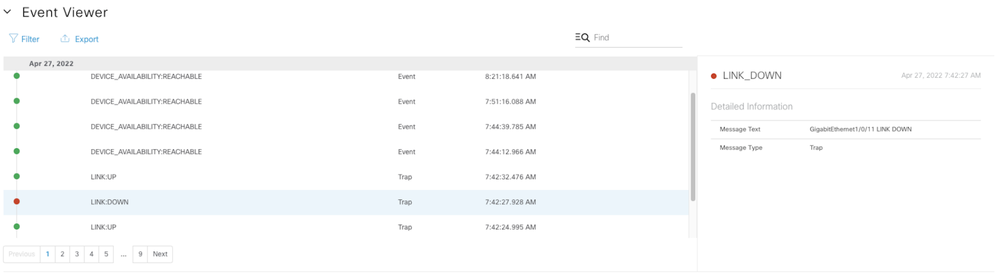
The Physical Neighbor Topology shows the device’s connection to other devices, as well as any connected clients. The topology also provides device-specific health scores and link status for each device. This is particularly useful in identifying link issues between devices, clients, and upstream devices.

Figure 8.17: Device 360 Physical Neighbor Topology



The Event Viewer displays any events from the switch that occurred in the time interval selected. When an event generates an error, there is detailed information provided about the root cause of the error.

Figure 8.18: Device 360 Event Viewer



Apr 27, 2022

●	DEVICE_AVAILABILITY:REACHABLE	Event	8:21:18.641 AM
●	DEVICE_AVAILABILITY:REACHABLE	Event	7:51:16.088 AM
●	DEVICE_AVAILABILITY:REACHABLE	Event	7:44:39.785 AM
●	DEVICE_AVAILABILITY:REACHABLE	Event	7:44:12.966 AM
●	LINK:UP	Trap	7:42:32.476 AM
●	LINK:DOWN	Trap	7:42:27.928 AM
●	LINK:UP	Trap	7:42:24.995 AM

● LINK_DOWN Apr 27, 2022 7:42:27 AM

Detailed Information

Message Text	GigabitEthernet1/0/11 LINK DOWN
Message Type	Trap

Path Trace

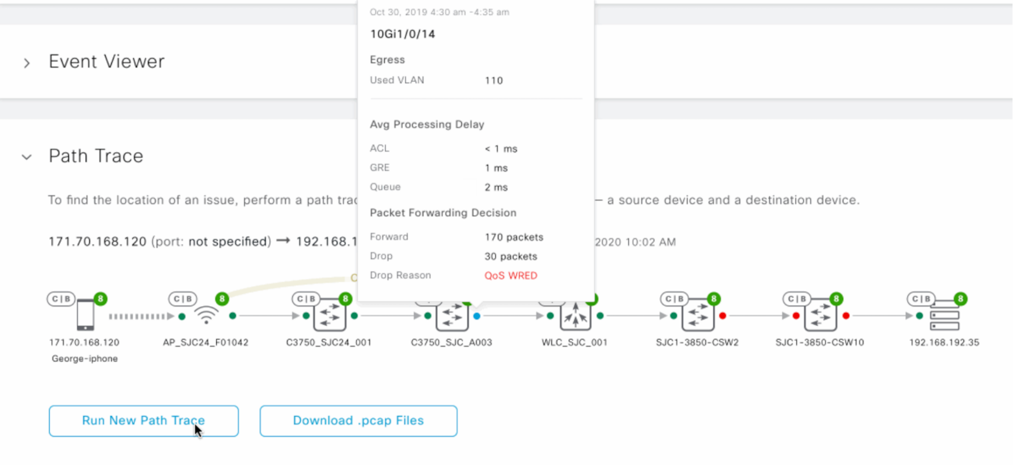
As mentioned in Chapter 7 regarding wireless troubleshooting, Path Trace is also available within the Device 360 view for switches. Path Trace allows the network engineer to pinpoint issues in the network. When running a Path Trace, the network engineer will specify the Source and Destination nodes, optionally a source and destination port, optionally TCP or UDP protocol.

When executing the Path Trace, Cisco DNA Center will display all the network devices between the Source and Destination as well as the Health Scores, link status, and ACLs along the path. This allows the network engineer to visualize where the problem is in the entire network path for the traffic flow. This helps resolve application experience issues quickly and easily.

After executing the Path Trace between the switch and destination, Path Trace identifies any ACLs within the path, as well as receiving device, device interface, and QoS statistics.

In addition to Path Trace, there is also the option to perform a live packet capture with real data which is known as True Trace. To execute a True Trace with live packet capture, all intermediary devices in the path will need to be managed by Cisco DNA Center and running IOS XE 17.x or higher.

Figure 8.19: Path Trace



Oct 30, 2019 4:30 am -4:35 am

10Gi1/0/14

Egress

Used VLAN 110

Avg Processing Delay

ACL < 1 ms

GRE 1 ms

Queue 2 ms

Packet Forwarding Decision

Forward 170 packets

Drop 30 packets

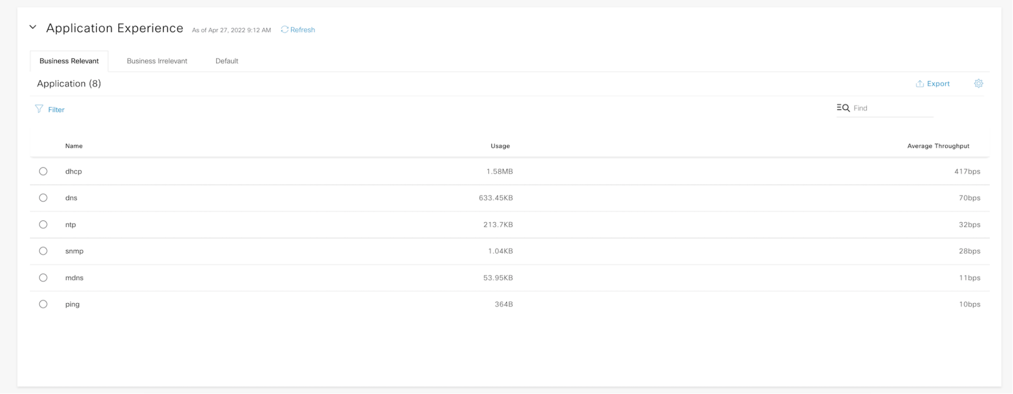
Drop Reason QoS WRED

To find the location of an issue, perform a path trac — a source device and a destination device.

171.70.168.120 (port: not specified) → 192.168.1 2020 10:02 AM

Visualize application visibility data such as Usage and Average Throughput. This allows the network engineer to see which applications are taking the most bandwidth and also which clients are using those applications. The application data comes directly from the device via NetFlow. Please refer to the **Application Health** section for more details about the application experience.

Figure 8.20: Device 360 Application Experience



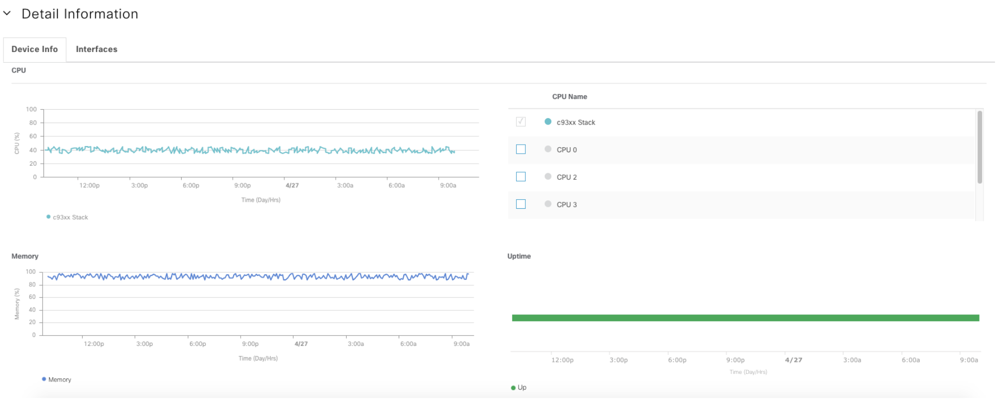
Application Experience As of Apr 27, 2022 9:12 AM

Application (8)

	Name	Usage	Average Throughput
○	dhcp	1.58MB	417bps
○	dns	633.45KB	70bps
○	ntp	213.7KB	32bps
○	snmp	1.04KB	28bps
○	mdns	53.95KB	11bps
○	ping	364B	10bps

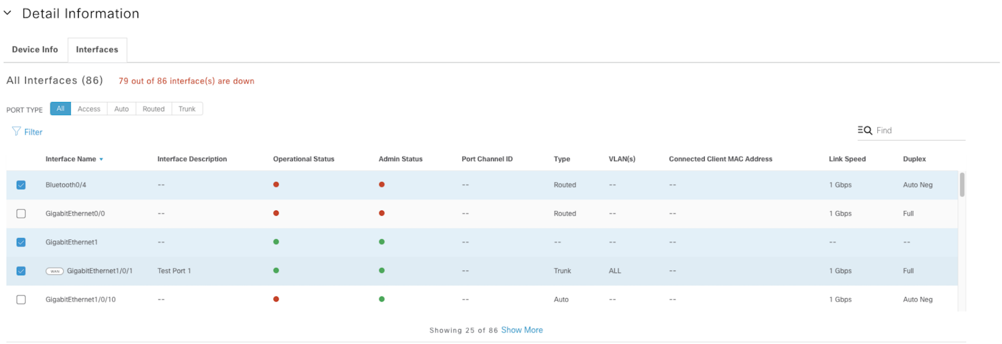
The Detail Information section provides information about the device hardware, as well as interface and utilization information. CPU and Memory usage statistics, as well as device temperature statistics are displayed, which makes the process of diagnosing hardware issues quicker and easier. All this information can be displayed without the need to go to the CLI to gather these statistics, diagnose hardware problems, and provide a quick hardware situational analysis.

Figure 8.21: Detail Information



This section also shows interface statistics, making it easy to view the status of all device interfaces, as well as interface-specific information such as link speed, duplex, and VLAN IDs. Similar to the hardware statistics, this gives the network engineer a singular view of the status of all interfaces for quick diagnosis and troubleshooting.

Figure 8.22: Device 360 Interfaces



All Interfaces (86) 79 out of 86 interface(s) are down

	Interface Name	Interface Description	Operational Status	Admin Status	Port Channel ID	Type	VLAN(s)	Connected Client MAC Address	Link Speed	Duplex
☑	Bluetooth0/4	--	🟥	🟥	--	Routed	--	--	1 Gbps	Auto Neg
□	GigabitEthernet0/0	--	🟥	🟥	--	Routed	--	--	1 Gbps	Full
☑	GigabitEthernet1	--	🟩	🟩	--	--	--	--	--	--
☑	WAN GigabitEthernet1/0/1	Test Port 1	🟩	🟩	--	Trunk	ALL	--	1 Gbps	Full
□	GigabitEthernet1/0/10	--	🟥	🟩	--	Auto	--	--	1 Gbps	Auto Neg

Showing 25 of 86 Show More

Machine Reasoning

Machine reasoning can automate complex networking management tasks and create workflows. This groundbreaking technology in Cisco DNA Center empowers less experienced engineers and saves time for seasoned IT professionals.

Machine reasoning is a new category of AI/ML technologies that can enable a computer to work through complex processes that would normally require a human. Common applications for machine reasoning are detail-driven workflows that are extremely time-consuming and tedious, similar to optimizing your tax returns by selecting the best deductions based on the many available options. Another example is the execution of workflows that require immediate attention and precise detail, such as the shut-off protocols in a refinery following a fire alarm. What both examples have in common is that executing each process requires a clear understanding of the relationship between the variables, including order, location, timing, and rules; in a workflow, each decision can alter subsequent steps.

Machine Reasoning Engine

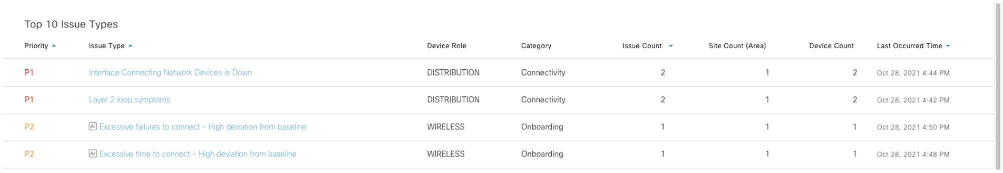
Cisco DNA Center's Machine Reasoning Engine (MRE) is comprised of several key components:

- AI/ML Engine identifies the issue and builds a recommended solution path with applicable knowledge packs.
- Knowledge packs are groups of troubleshooting workflows based on commonly experienced issues and Cisco TAC troubleshooting and solution steps combined with Cisco's deep network expertise.
- Existing troubleshooting tools native to Cisco DNA Center can automatically provide corresponding commands out to the AI engine.

Cisco DNA Center delivers some unique machine reasoning workflows with the addition of a powerful cloud-connected Machine Reasoning Engine (MRE). Experience the usefulness of MRE via proactive insights. When Cisco DNA Center flags an issue, it may determine to send this issue to the MRE for automated troubleshooting. If there is an MRE workflow to resolve this issue, a run button will be presented to execute that workflow and resolve the issue.

The list of Issues in Cisco DNA Center can be found in `Assurance > Issues` under the Cisco DNA Center main menu, or from the **Top 10 Issues** table in `Assurance > Overall.` In the following example, there is a P1 issue that was automatically raised regarding a Layer 2 Loop issue.

Figure 8.23: Layer 2 Loop Issue

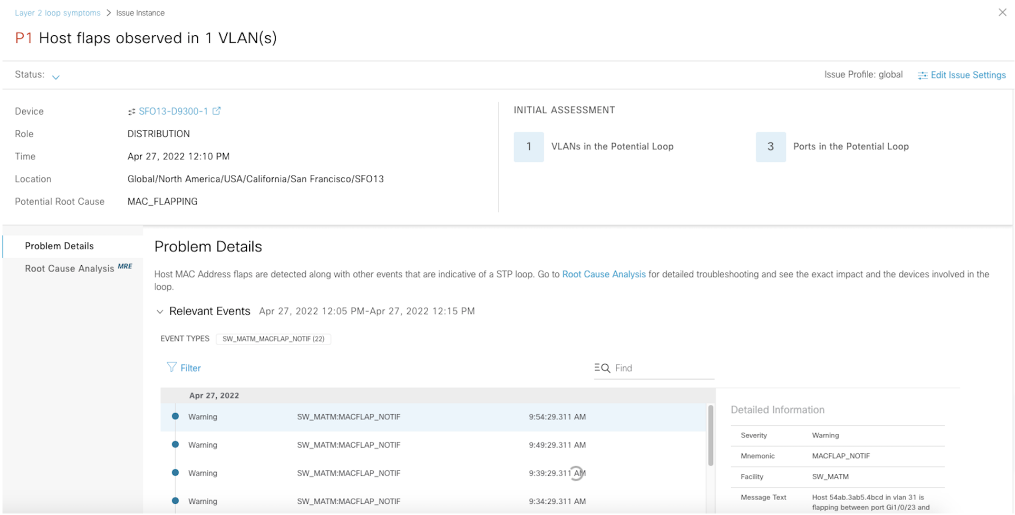


Top 10 Issue Types

Priority ▲	Issue Type ▲	Device Role	Category	Issue Count ▼	Site Count (Area)	Device Count	Last Occurred Time ▼
P1	Interface Connecting Network Devices is Down	DISTRIBUTION	Connectivity	2	1	2	Oct 28, 2021 4:44 PM
P1	Layer 2 loop symptoms	DISTRIBUTION	Connectivity	2	1	2	Oct 28, 2021 4:42 PM
P2	AI Excessive failures to connect - High deviation from baseline	WIRELESS	Onboarding	1	1	1	Oct 28, 2021 4:50 PM
P2	AI Excessive time to connect - High deviation from baseline	WIRELESS	Onboarding	1	1	1	Oct 28, 2021 4:48 PM

By selecting the issue, more details are presented about the devices and sites affected by the problem. In this case, host MAC Address flaps were observed in one VLAN, along with a couple of other events, which is typically indicative of a spanning tree protocol (STP) issue.

Figure 8.24: Host Flaps



Layer 2 loop symptoms > Issue Instance

P1 Host flaps observed in 1 VLAN(s)

Status:

Issue Profile: global | Edit Issue Settings

Device	SFO13-D9300-1
Role	DISTRIBUTION
Time	Apr 27, 2022 12:10 PM
Location	Global/North America/USA/California/San Francisco/SFO13
Potential Root Cause	MAC_FLAPPING

INITIAL ASSESSMENT

1 VLANs in the Potential Loop

3 Ports in the Potential Loop

Problem Details

Host MAC Address flaps are detected along with other events that are indicative of a STP loop. Go to Root Cause Analysis for detailed troubleshooting and see the exact impact and the devices involved in the loop.

Relevant Events Apr 27, 2022 12:05 PM-Apr 27, 2022 12:15 PM

EVENT TYPES SW_MATM_MACFLAP_NOTIF (22)

Apr 27, 2022

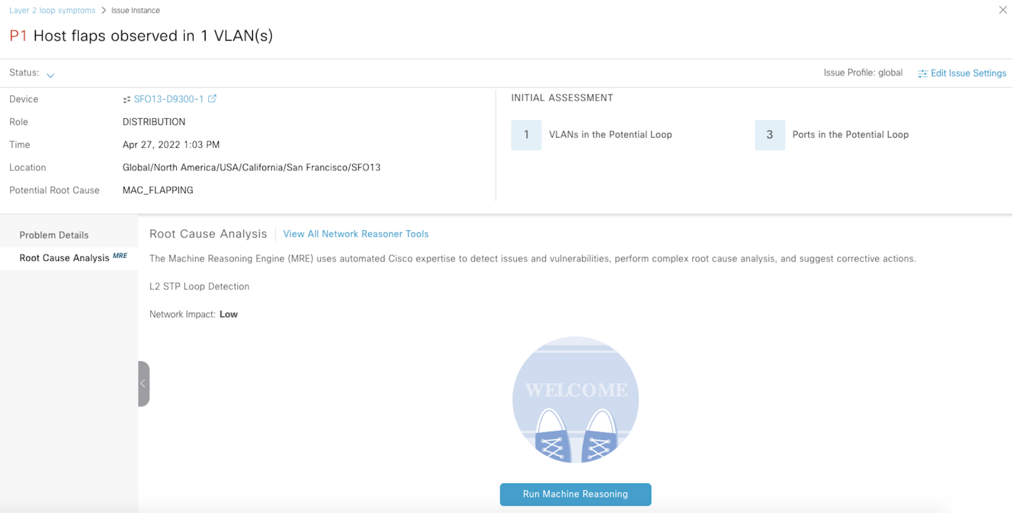
Warning	SW_MATM:MACFLAP_NOTIF	9:54:29.311 AM
Warning	SW_MATM:MACFLAP_NOTIF	9:49:29.311 AM
Warning	SW_MATM:MACFLAP_NOTIF	9:39:29.311 AM
Warning	SW_MATM:MACFLAP_NOTIF	9:34:29.311 AM

Detailed Information

Severity	Warning
Mnemonic	MACFLAP_NOTIF
Facility	SW_MATM
Message Text	Host 54ab.3ab5.4bcd in vlan 31 is flapping between port Gi1/0/23 and

After viewing the problem details, Root Cause Analysis using the Machine Reasoning Engine in Cisco DNA Center can provide further insight into the issue. The Machine Reasoning Engine uses existing knowledge of the initial issue, as well as runs commands on the affected network device(s). Then, it combines that with expert knowledge and machine learning from observing similar issues across multiple networks that are utilizing Cisco DNA Center. Finally, it analyzes the root cause of the issue and provides a solution to resolve it. This is incredibly powerful as it removes all of the manual work that would typically be involved in diagnosing and resolving such a complicated issue. MRE provides in-depth analysis and a simplified solution.

Figure 8.25: Run Machine Reasoning


Layer 2 loop symptoms > Issue Instance

P1 Host flaps observed in 1 VLAN(s)

Status:

Issue Profile: global

Device	SFO13-D9300-1
Role	DISTRIBUTION
Time	Apr 27, 2022 1:03 PM
Location	Global/North America/USA/California/San Francisco/SFO13
Potential Root Cause	MAC_FLAPPING

INITIAL ASSESSMENT

1 VLANs in the Potential Loop

3 Ports in the Potential Loop

Problem Details
Root Cause Analysis MRE

Root Cause Analysis

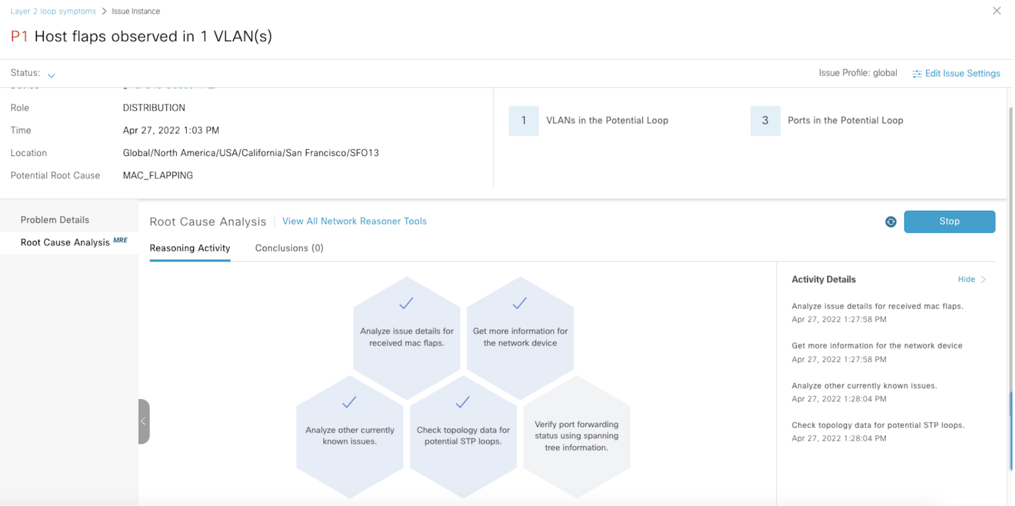
View All Network Reasoner Tools

The Machine Reasoning Engine (MRE) uses automated Cisco expertise to detect issues and vulnerabilities, perform complex root cause analysis, and suggest corrective actions.

L2 STP Loop Detection

Network Impact: **Low**

Figure 8.26: Machine Reasoning Engine



P1 Host flaps observed in 1 VLAN(s)

Role	DISTRIBUTION
Time	Apr 27, 2022 1:03 PM
Location	Global/North America/USA/California/San Francisco/SFO13
Potential Root Cause	MAC_FLAPPING

1 VLANs in the Potential Loop

3 Ports in the Potential Loop

Root Cause Analysis

✓ Analyze issue details for received mac flaps.

✓ Get more information for the network device

✓ Analyze other currently known issues.

✓ Check topology data for potential STP loops.

Verify port forwarding status using spanning tree information.

Activity Details

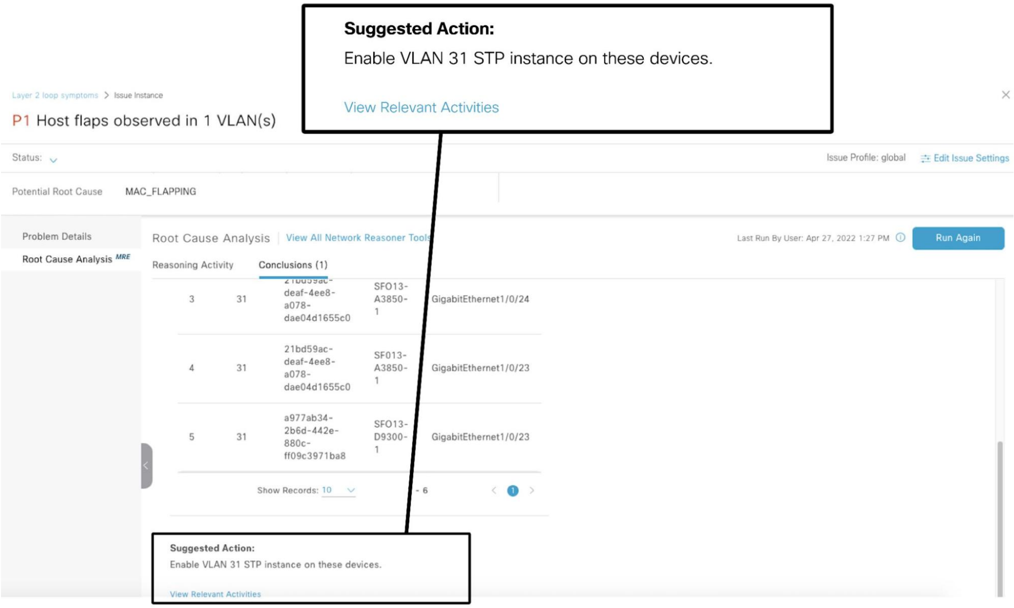
Analyze issue details for received mac flaps.
Apr 27, 2022 1:27:58 PM

Get more information for the network device
Apr 27, 2022 1:27:58 PM

Analyze other currently known issues.
Apr 27, 2022 1:28:04 PM

Check topology data for potential STP loops.
Apr 27, 2022 1:28:04 PM

Figure 8.27: Root Cause Analysis Conclusion



Suggested Action:

Enable VLAN 31 STP instance on these devices.

View Relevant Activities

Layer 2 loop symptoms > Issue Instance

P1 Host flaps observed in 1 VLAN(s)

Status:

Issue Profile: global

Edit Issue Settings

Potential Root Cause MAC_FLAPPING

Problem Details

Root Cause Analysis MRE

Root Cause Analysis | View All Network Reasoner Tools

Last Run By User: Apr 27, 2022 1:27 PM

Run Again

Reasoning Activity

Conclusions (1)

3	31	21bd59ac- deaf-4ee8- a078- dae04d1655c0	SFO13- A3850- 1	GigabitEthernet1/0/24
4	31	21bd59ac- deaf-4ee8- a078- dae04d1655c0	SF013- A3850- 1	GigabitEthernet1/0/23
5	31	a977ab34- 2b6d-442e- 880c- ff09c3971ba8	SFO13- D9300- 1	GigabitEthernet1/0/23

Show Records: 10 - 6 1

Suggested Action:

Enable VLAN 31 STP instance on these devices.

View Relevant Activities

9. Client Monitoring and Troubleshooting

The main goal of professionally designing, implementing, and maintaining networks is to provide the best possible client experience. Cisco DNA Center gives the network engineer the tools needed to ensure and validate that this objective has been achieved. This chapter will go over some of these tools that are available within the product today.

Client Health

The Client Health page displays the percentage of healthy clients in the environment at a global level during the past 24 hours. This view can also be filtered based on Site Level and SSID. The period can also be adjusted to 3 hours, 24 hours, or 7 days as well as be configured to go back in time up to 30 days.

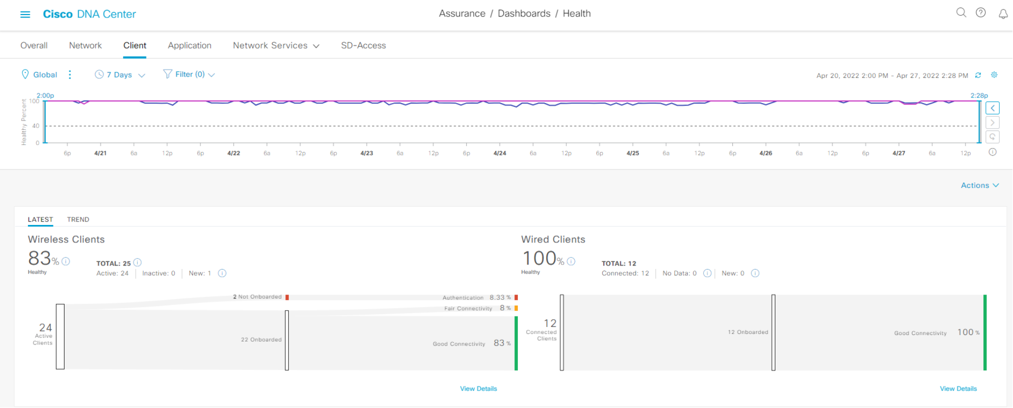
Clients are broken down into the Wireless and Wired Client categories. There are two views for each category: **LATEST** perspective and **TREND** perspective.

When viewed through the LATEST perspective, the Wireless Clients category displays the total number of clients, the number of active/inactive clients, new clients who have not yet been added to the Health Score calculations, the number of Onboarded Clients, the percentage of clients with Good Health, as well as the number of clients that have not been onboarded and percentages of the reasons why they have failed to onboard during the past 5 minutes.

When viewed through the TREND perspective, the Wireless Clients category displays the Client Count with their respective health category over a period specified by the filtered time.

This gives the engineer a quick view into the overall health of wired and wireless clients in the environment.

Figure 9.1: Client Health

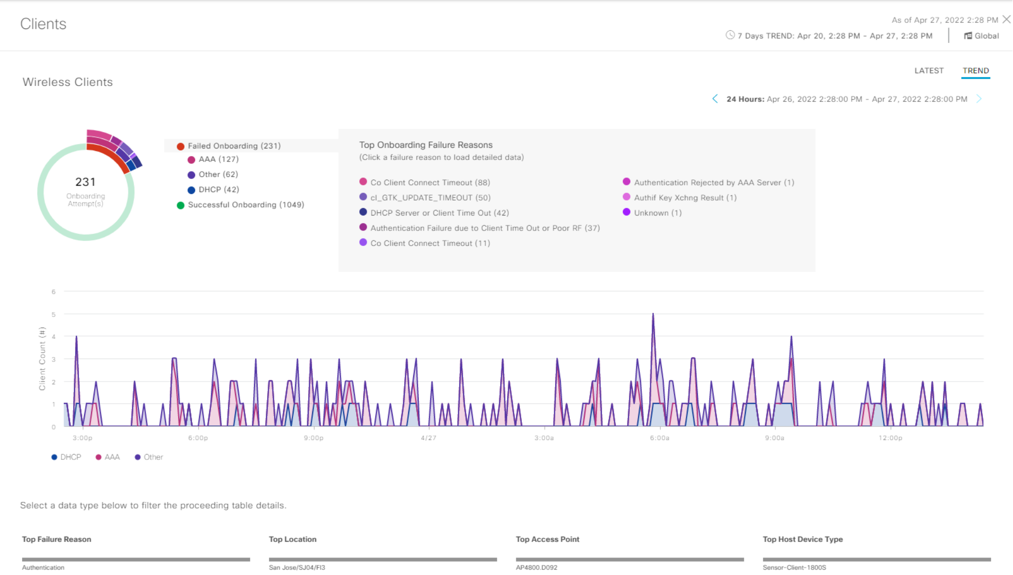


Clicking on `View Details` provides the engineer with additional metrics to determine the cause of failed onboarding attempts.

For instance, when clicking `View Details` under the **Wireless Clients** category, the engineer can view the number of Failed Onboarding attempts, the top reason for the failed attempt, the top location where the client failed to onboard, the top access point where it failed, as well as the top host device types that failed to onboard. This gives the engineer valuable insights as to why problems are occurring in the network.

What is the reason that most devices are failing to onboard? Is the problem related to AAA or DHCP? Is the issue only occurring at one site or multiple sites? Is it related to one AP or many APs? Is the problem only affecting certain device types? All of these questions can be answered from this one page.

Figure 9.2: Wireless Clients



Clients

As of Apr 27, 2022 2:28 PM ✕

7 Days TREND: Apr 20, 2:28 PM - Apr 27, 2:28 PM | Global

Wireless Clients

LATEST TREND

‹ **24 Hours:** Apr 26, 2022 2:28:00 PM - Apr 27, 2022 2:28:00 PM ›

231 Onboarding Attempt(s)

- ● Failed Onboarding (231)
  - ● AAA (127)
  - ● Other (62)
  - ● DHCP (42)
- ● Successful Onboarding (1049)

Top Onboarding Failure Reasons
(Click a failure reason to load detailed data)

- ● Co Client Connect Timeout (88)
- ● cl_GTK_UPDATE_TIMEOUT (50)
- ● DHCP Server or Client Time Out (42)
- ● Authentication Failure due to Client Time Out or Poor RF (37)
- ● Co Client Connect Timeout (11)
- ● Authentication Rejected by AAA Server (1)
- ● Authif Key Xchng Result (1)
- ● Unknown (1)

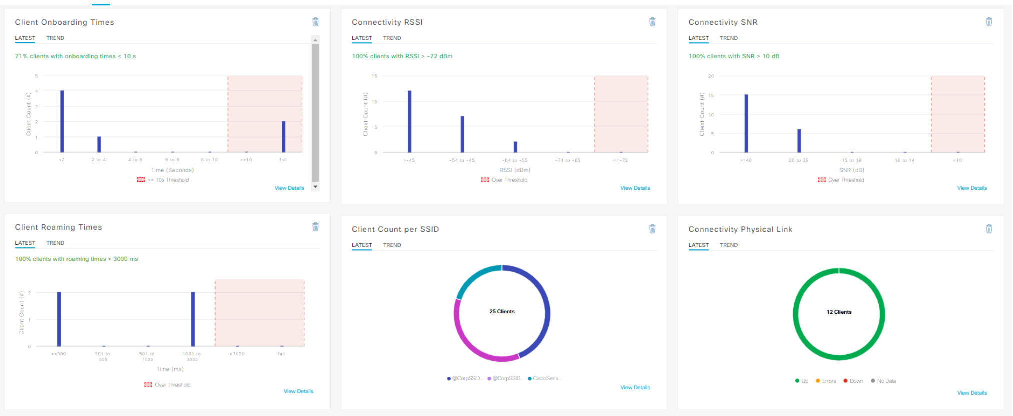
Select a data type below to filter the proceeding table details.

Top Failure Reason	Top Location	Top Access Point	Top Host Device Type
Authentication	San Jose/SJ04/FI3	AP4800.D092	Sensor-Client-1800S

Similar metrics are available when clicking `View Details` for Wired Clients instead of Wireless Clients, except Switches are shown instead of Access Points.

The dashboard is also highly customizable with various dashlets. This allows the engineer to configure the system to display the information that is the most beneficial to their troubleshooting style. For instance, dashlets are available for Client Roaming Times, RSSI, SNR, Onboarding Time, Data Rates, DNS, and Physical Links, just to name a few.

Figure 9.3: Client KPIs



71% clients with onboarding times < 10 s

100% clients with RSSI > -72 dBm

100% clients with SNR > 10 dB

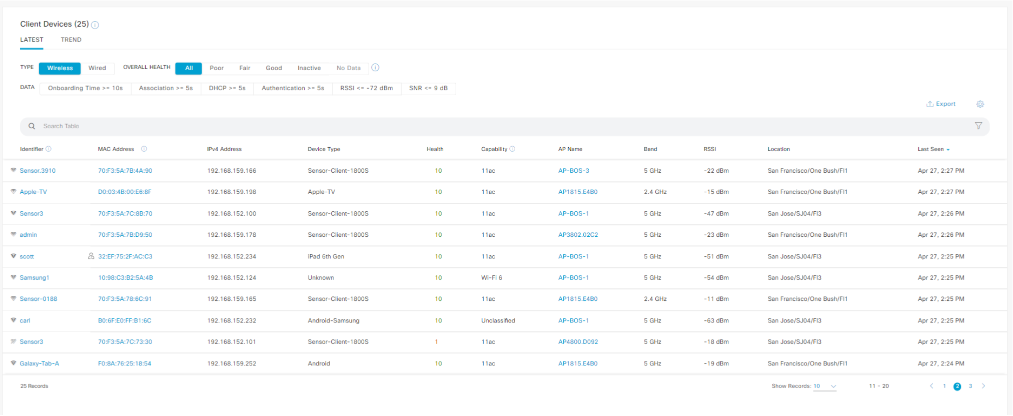
100% clients with roaming times < 3000 ms

A list of Client Devices is also available. This list can be filtered based on the `LATEST` and `TREND` perspectives as explained previously. It can also be filtered based on Wireless and Wired types, Overall Health status of Good, Fair, Poor, etc., as well as being filtered based on various data metrics against a threshold such as:

- Onboarding Times >= 10s
- Associations >= 5s
- DHCP >= 5s
- Authentication >= 5s
- RSSI <= -72dBm
- SNR <= 9dB

The filtering of the data metrics can be combined. An example would be filtering on wireless clients that have an RSSI <=-72dBm AND SNR <=9dB. This is extremely helpful if the engineer wanted to see a subset of client devices that match an extremely specific set of criteria. Numerous columns can be added to provide additional information to this page. An example would be adding the MAC Address column as shown in the screenshot below. Not only does it show the MAC Address of the client, but it also indicates if that client is using a Randomized MAC Address. Clicking on any particular client will then open the respective Client 360 page.

Figure 9.4: Client Devices



Identifier	MAC Address	IPv4 Address	Device Type	Health	Capability	AP Name	Band	RSSI	Location	Last Seen
Sensor.3910	70:F3:5A:7B:4A:90	192.168.159.166	Sensor-Client-1800S	10	11ac	AP-BOS-3	5 GHz	-22 dBm	San Francisco/One Bush/Fl1	Apr 27, 2:27 PM
Apple-TV	D0:03:4B:00:E6:8F	192.168.159.198	Apple-TV	10	11ac	AP1815.E4B0	2.4 GHz	-15 dBm	San Francisco/One Bush/Fl1	Apr 27, 2:27 PM
Sensor3	70:F3:5A:7C:8B:70	192.168.152.100	Sensor-Client-1800S	10	11ac	AP-BOS-1	5 GHz	-47 dBm	San Jose/SJ04/Fl3	Apr 27, 2:26 PM
admin	70:F3:5A:7B:D9:50	192.168.159.178	Sensor-Client-1800S	10	11ac	AP3802.02C2	5 GHz	-23 dBm	San Francisco/One Bush/Fl1	Apr 27, 2:26 PM
scott	32:EF:75:2F:AC:C3	192.168.152.234	iPad 6th Gen	10	11ac	AP-BOS-1	5 GHz	-51 dBm	San Jose/SJ04/Fl3	Apr 27, 2:25 PM
Samsung1	10:98:C3:B2:5A:4B	192.168.152.124	Unknown	10	Wi-Fi 6	AP-BOS-1	5 GHz	-54 dBm	San Jose/SJ04/Fl3	Apr 27, 2:25 PM
Sensor-0188	70:F3:5A:78:6C:91	192.168.159.165	Sensor-Client-1800S	10	11ac	AP1815.E4B0	2.4 GHz	-11 dBm	San Francisco/One Bush/Fl1	Apr 27, 2:25 PM
carl	B0:6F:E0:FF:B1:6C	192.168.152.232	Android-Samsung	10	Unclassified	AP-BOS-1	5 GHz	-63 dBm	San Jose/SJ04/Fl3	Apr 27, 2:25 PM
Sensor3	70:F3:5A:7C:73:30	192.168.152.101	Sensor-Client-1800S	1	11ac	AP4800.D092	5 GHz	-18 dBm	San Jose/SJ04/Fl3	Apr 27, 2:25 PM
Galaxy-Tab-A	F0:8A:76:25:18:54	192.168.159.252	Android	10	11ac	AP1815.E4B0	5 GHz	-19 dBm	San Francisco/One Bush/Fl1	Apr 27, 2:24 PM

25 Records

Show Records: 10 11 - 20

Client Troubleshooting

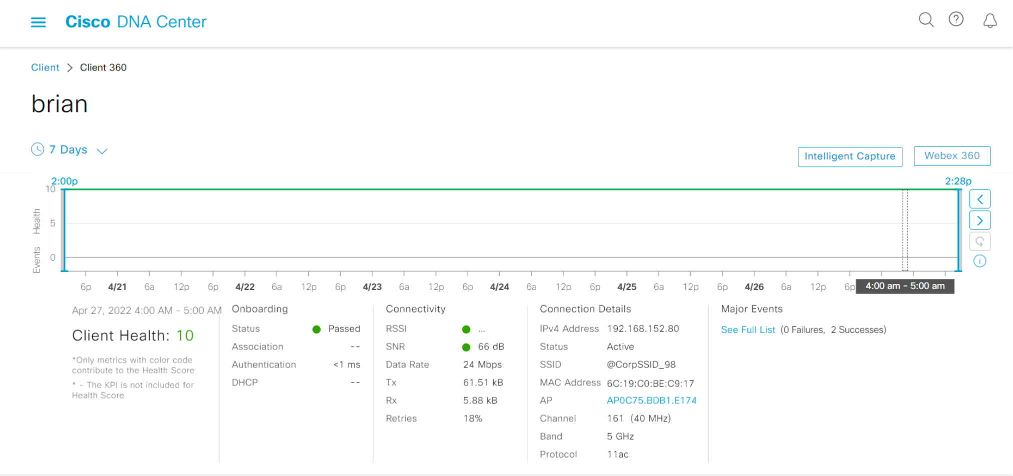
Client 360

There are multiple ways to access the Client 360 page. The engineer could select the client from the list of clients on the Client Health page, from a Device 360 page where the client is located, or even perform a Search from the Magnifying Glass icon in the upper right corner. The engineer could perform the search based on IP Address, MAC Address, and even the username of the user logged into the client.

Note When searching by username, the User 360 page will be displayed with a list of all the client devices the user has used to gain access to the network.

Similar to other Device 360 pages, the Client 360 page allows the network engineer to view the current Health Score of the client. When hovering over a point in time of a wireless client, it also shows Onboarding Status, Connectivity such as RSSI, SNR, Data Rate, Transmit and Receive bandwidth, and percentage of Retries, Connection Details such as IP Address, Status, SSID, MAC Address (with an icon indicating if it is a Randomized MAC), AP, Channel, Band, and Protocol, and a list of Major Events. It also offers the time travel feature allowing the network engineer to travel back in time to see Health Score and related metrics at a particular point in time. Replicating network issues is not an easy job but Cisco DNA Center makes the impossible possible. The ability of Cisco DNA Center to provide this information tremendously reduces the amount of time needed to troubleshoot client issues.

Figure 9.5: Client 360



brian

Apr 27, 2022 4:00 AM - 5:00 AM

Client Health: 10

*Only metrics with color code contribute to the Health Score

* - The KPI is not included for Health Score

Onboarding

Status	● Passed
Association	--
Authentication	<1 ms
DHCP	--

Connectivity

RSSI	● ...
SNR	● 66 dB
Data Rate	24 Mbps
Tx	61.51 kB
Rx	5.88 kB
Retries	18%

Connection Details

IPv4 Address	192.168.152.80
Status	Active
SSID	@CorpSSID_98
MAC Address	6C:19:C0:BE:C9:17
AP	AP0C75.BDB1.E174
Channel	161 (40 MHz)
Band	5 GHz
Protocol	11ac

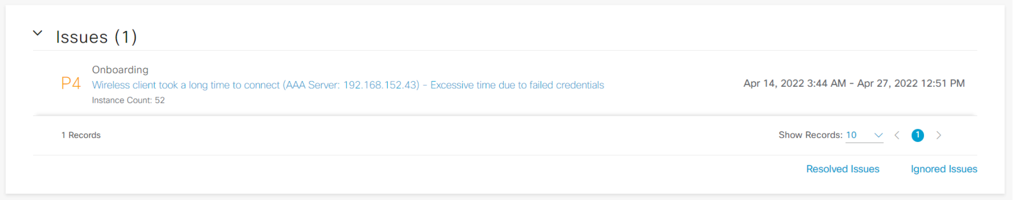
Major Events

See Full List (0 Failures, 2 Successes)

Issues

The Issues dashlet displays the issues that the client has experienced during the selected period. These issues are sorted by priority.

Figure 9.6: Issues



Issues (1)

P4 Onboarding
Wireless client took a long time to connect (AAA Server: 192.168.152.43) - Excessive time due to failed credentials
Instance Count: 52
Apr 14, 2022 3:44 AM - Apr 27, 2022 12:51 PM

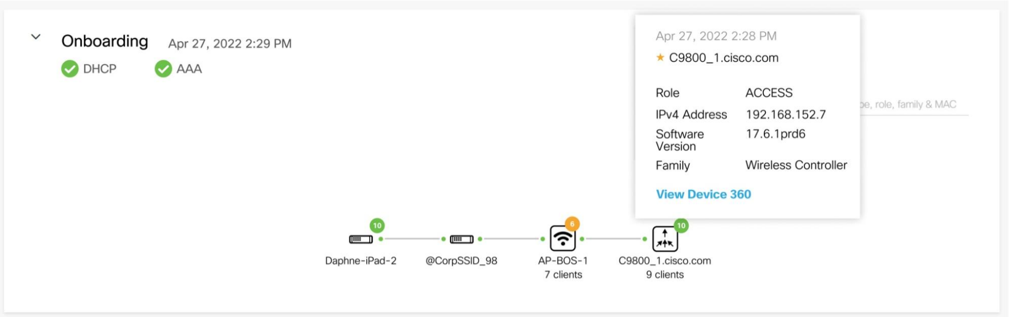
1 Records

Clicking on an issue provides the engineer with a Description of the problem as well as a list of Suggested Actions that should be taken to solve that problem, without having to leave the Client 360 page.

Onboarding

The Onboarding Dashlet displays the Client Device, SSID, AP, and WLC used by the client to connect to the network along with the Health Score of each object. Hovering over an object displays additional information as well. This provides the engineer with information not only on how and where the client is connected but also on the health of the wireless infrastructure used to connect. This helps the network engineer to quickly visualize whether the network devices are causing any client issues.

Figure 9.7: Onboarding Dashlet



Onboarding Apr 27, 2022 2:29 PM

✓ DHCP ✓ AAA

Apr 27, 2022 2:28 PM

★ C9800_1.cisco.com

Role	ACCESS
IPv4 Address	192.168.152.7
Software Version	17.6.1prd6
Family	Wireless Controller

View Device 360

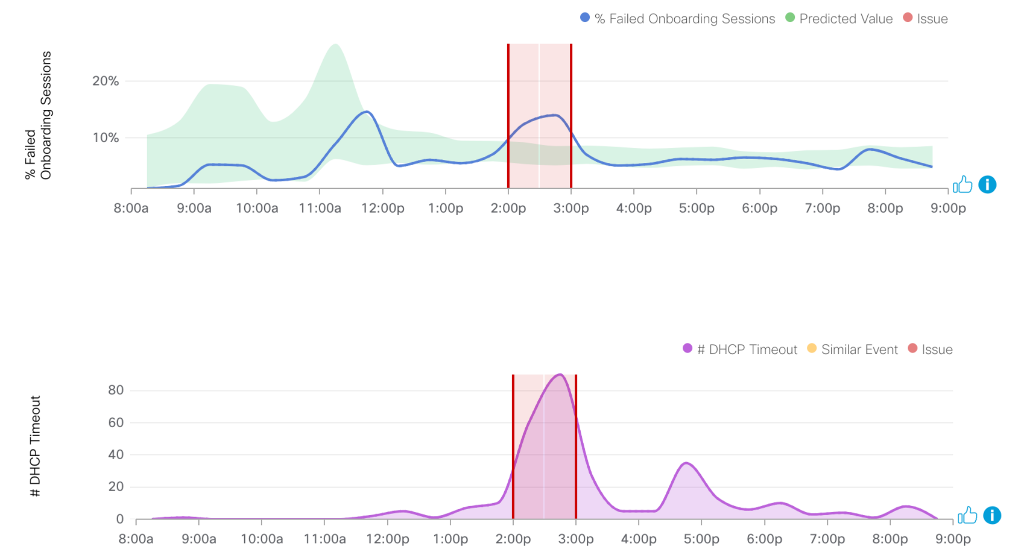
AI-driven Onboarding Baselines

On top of the client-specific view provided by Client 360, AI Network Analytics generates baselines for the time to connect and the connection failure rate, for each combination of Building and SSID in the network.

Such baselines are accessible directly through the Baseline dashboard and are used to generate AI-driven issues when these KPIs exceed the baseline. To access the baselines dashboard go to the main menu and then `Assurance > Baselines`. The AI-driven issues provide details about the time, location, and SSID a given anomaly was detected, along with the number of affected clients. The anomaly is visualized by displaying the KPI values, overlayed on the predicted normal range, represented as a green band.

The root cause analysis also presents other network KPIs that are likely to explain the reason for the reported failure, for instance in the example below, the spike in connection failures happening between 2 PM and 3 PM is likely to be explained as a problem with DHCP.

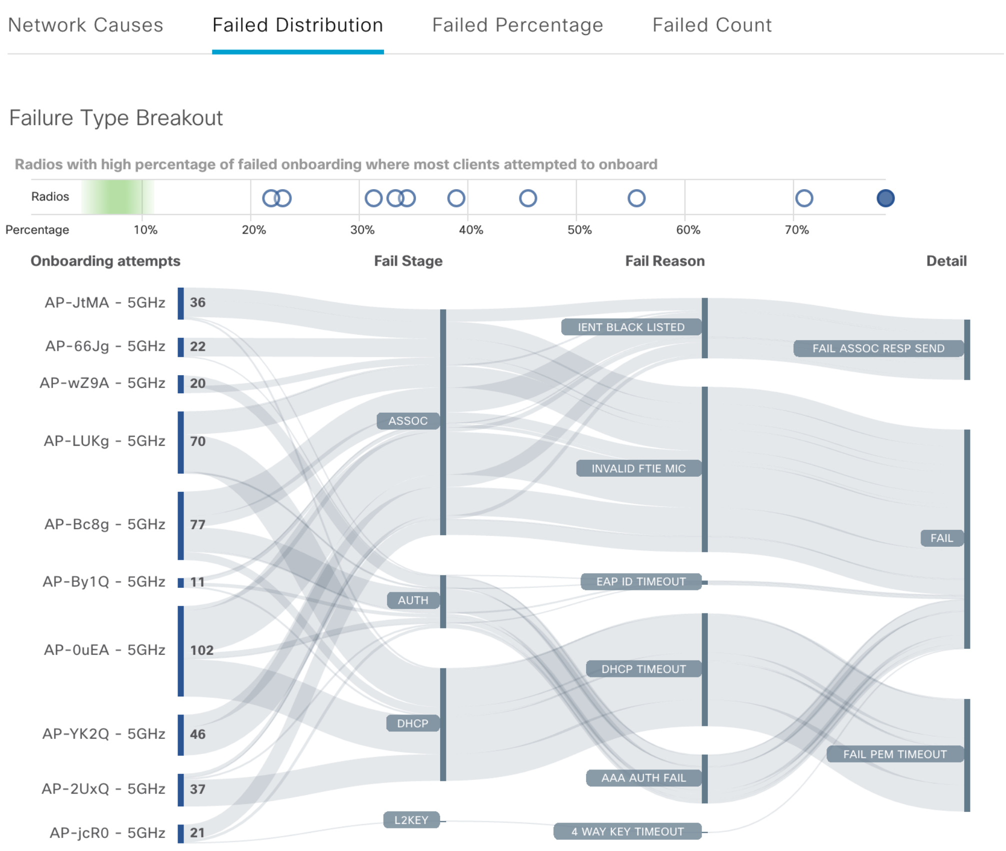
Figure 9.8: Example of AI-driven Issue for Excessive Connection Failures



The KPIs used for baselines and root cause analysis are aggregated at the Building and SSID levels. Different SSIDs typically have specific configuration and security policies that need to be considered to build the baseline, but at the same time, even the same SSID can have different normal behaviors depending on the location (e.g., headquarters vs. remote site).

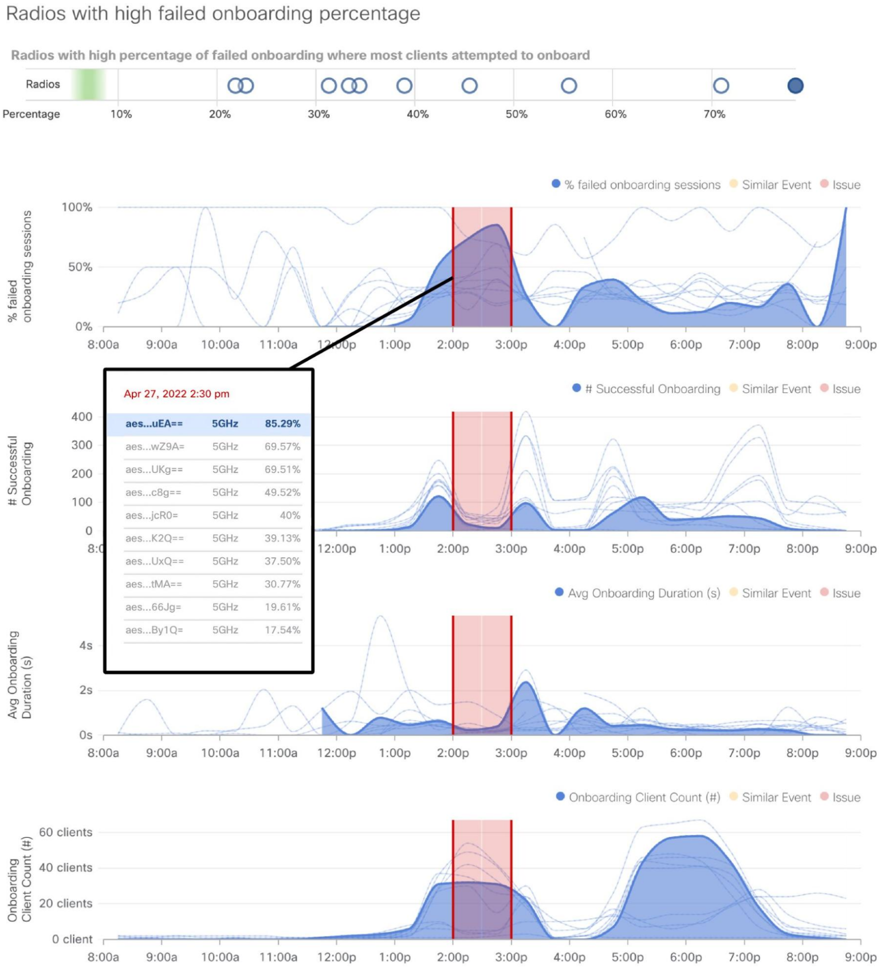
Once an anomaly is detected at the Building and SSID aggregation level, the issue details allow the user to drill down the impacted clients (allowing to cross-launch the Client 360 view for each of them) and the most impacted radios (with cross-launch links to AP 360), with a detail of the distribution of failures, including the specific error codes.

Figure 9.9: Failure Code Details by AP for AI-Driven Issues Root Cause Analysis



The `Failed Percentage` and `Failed Count` views allow investigation of the onboarding-related KPIs for the most affected radios, thereby further reducing the scope of the investigation to specific areas in the building.

Figure 9.10: Radio-level Details for AI-Driven Onboarding Failure Issues



Radios with high failed onboarding percentage

Radios with high percentage of failed onboarding where most clients attempted to onboard

Apr 27, 2022 2:30 pm

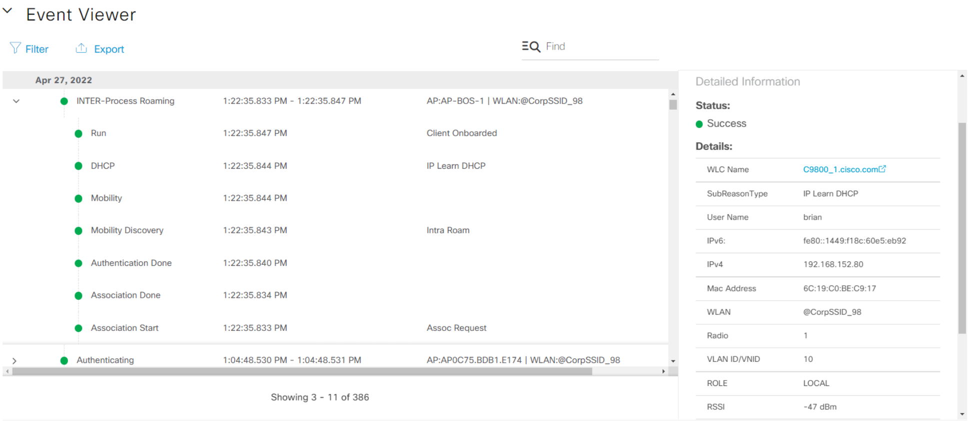
aes...uEA==	**5GHz**	**85.29%**
aes...wZ9A=	5GHz	69.57%
aes...UKg==	5GHz	69.51%
aes...c8g==	5GHz	49.52%
aes...jcR0=	5GHz	40%
aes...K2Q==	5GHz	39.13%
aes...UxQ==	5GHz	37.50%
aes...tMA==	5GHz	30.77%
aes...66Jg=	5GHz	19.61%
aes...By1Q=	5GHz	17.54%

Radios
Percentage
10%
20%
30%
40%
50%
60%
70%
● % failed onboarding sessions ● Similar Event ● Issue
% failed onboarding sessions
100%
50%
0%
8:00a
9:00a
10:00a
11:00a
12:00p
1:00p
2:00p
3:00p
4:00p
5:00p
6:00p
7:00p
8:00p
9:00p
● # Successful Onboarding ● Similar Event ● Issue
# Successful Onboarding
400
300
200
100
0
● Avg Onboarding Duration (s) ● Similar Event ● Issue
Avg Onboarding Duration (s)
4s
2s
0s
● Onboarding Client Count (#) ● Similar Event ● Issue
Onboarding Client Count (#)
60 clients
40 clients
20 clients
0 client

Event Viewer

The Event Viewer shows a list of all the Events that have occurred during the specified time. Clicking on an Event displays more information about the event, for instance, Intra or Inter-Controller Roaming with times and metrics, Associations, Authentications, DHCP, etc. This information can be extremely useful in troubleshooting performance problems. All these events come via streaming telemetry from the WLC which allows Cisco DNA Center to show critical troubleshooting information not possible using traditional methods.

Figure 9.11: Event Viewer



Apr 27, 2022

● INTER-Process Roaming	1:22:35.833 PM - 1:22:35.847 PM	AP:AP-BOS-1 | WLAN:@CorpSSID_98
● Run	1:22:35.847 PM	Client Onboarded
● DHCP	1:22:35.844 PM	IP Learn DHCP
● Mobility	1:22:35.844 PM	
● Mobility Discovery	1:22:35.843 PM	Intra Roam
● Authentication Done	1:22:35.840 PM	
● Association Done	1:22:35.834 PM	
● Association Start	1:22:35.833 PM	Assoc Request
● Authenticating	1:04:48.530 PM - 1:04:48.531 PM	AP:AP0C75.BDB1.E174 | WLAN:@CorpSSID_98

Showing 3 - 11 of 386

Detailed Information

Status:

● Success

Details:

WLC Name	C9800_1.cisco.com
SubReasonType	IP Learn DHCP
User Name	brian
IPv6:	fe80::1449:f18c:60e5:eb92
IPv4	192.168.152.80
Mac Address	6C:19:C0:BE:C9:17
WLAN	@CorpSSID_98
Radio	1
VLAN ID/VNID	10
ROLE	LOCAL
RSSI	-47 dBm

Path Trace

As mentioned in Chapters 7 and 8, the Path Trace/True Trace feature is also available from the client's perspective here on the Client 360 page. Please refer back to the previous two chapters for more information on Path Trace/True Trace.

Application Experience

Application Experience is available on the Client 360 page. This data comes directly from the WLC via NetFlow once it is configured. This allows the network engineer to see what business-critical applications the client is accessing and how much bandwidth the client is consuming in the network. This can help network engineers determine which applications to prioritize in times of congestion.

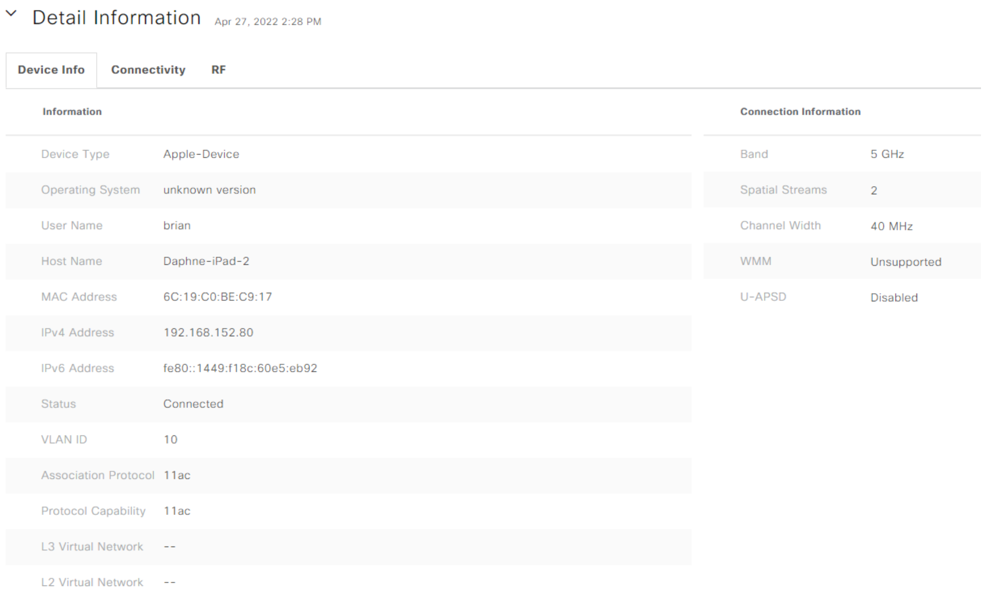
Please refer to **Chapter 10** for more details.

Detail Information

This section has 3 tabs that display a wealth of information about the Client and its performance. The 3 tabs are Device, Connectivity, and RF.

The `Device` tab shows helpful information related to the client such as Device Type, Username, IP Address, MAC Address, and VLAN ID. Wireless clients also show additional information such as Band, Spatial Streams, Channel Width, WMM, and U-APSD.

Figure 9.12: Device Information



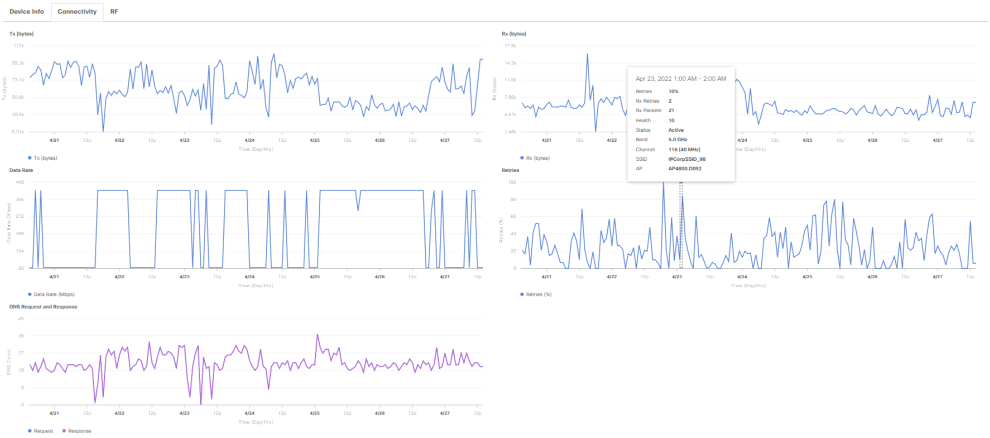
Detail Information Apr 27, 2022 2:28 PM

Information	
Device Type	Apple-Device
Operating System	unknown version
User Name	brian
Host Name	Daphne-iPad-2
MAC Address	6C:19:C0:BE:C9:17
IPv4 Address	192.168.152.80
IPv6 Address	fe80::1449:f18c:60e5:eb92
Status	Connected
VLAN ID	10
Association Protocol	11ac
Protocol Capability	11ac
L3 Virtual Network	--
L2 Virtual Network	--

Connection Information	
Band	5 GHz
Spatial Streams	2
Channel Width	40 MHz
WMM	Unsupported
U-APSD	Disabled

The `Connectivity` tab gives detailed information such as Tx and Rx (Bytes), Data Rate, Retries, and DNS Requests and Responses.

Figure 9.13: Connectivity



Apr 23, 2022 1:00 AM - 2:00 AM

Retries 10%

Rx Retries 2

Rx Packets 21

Health 10

Status Active

Band 5.0 GHz

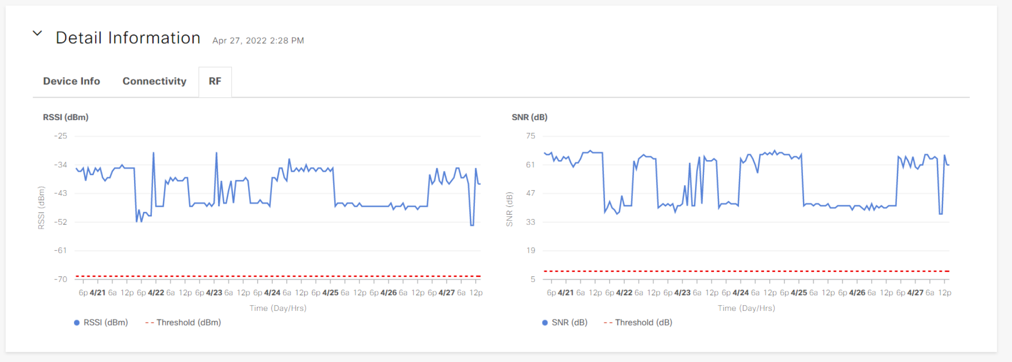
Channel 116 (40 MHz)

SSID @CorpSSID_98

AP AP4800.D092

The `RF` tab shows RSSI and SNR.

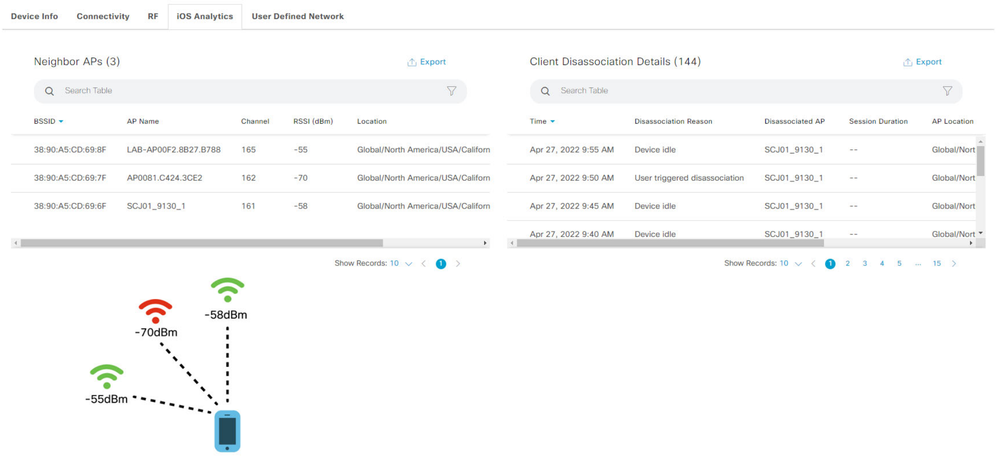
Figure 9.14: RF


Detail Information
Apr 27, 2022 2:28 PM
Device Info
Connectivity
RF
RSSI (dBm)
-25
-34
-43
-52
-61
-70
RSSI (dBm)
6p 4/21 6a 12p 6p 4/22 6a 12p 6p 4/23 6a 12p 6p 4/24 6a 12p 6p 4/25 6a 12p 6p 4/26 6a 12p 6p 4/27 6a 12p
Time (Day/Hrs)
RSSI (dBm)
Threshold (dBm)
SNR (dB)
75
61
47
33
19
5
SNR (dB)
6p 4/21 6a 12p 6p 4/22 6a 12p 6p 4/23 6a 12p 6p 4/24 6a 12p 6p 4/25 6a 12p 6p 4/26 6a 12p 6p 4/27 6a 12p
Time (Day/Hrs)
SNR (dB)
Threshold (dB)

iOS Analytics

If the device supports iOS Analytics, the iOS Analytics tab will also be displayed. Cisco has partnered with Apple, Samsung, and Intel in a collaborative effort to bring additional functionality to help troubleshoot devices. Those devices can send information to the wireless infrastructure, which can then be displayed within Cisco DNA Center. This allows the engineer to see how those devices view the wireless network from their perspective. For instance, it can show how many APs the device sees and at what RSSI. Has Hotspot been enabled on the device? Did it disconnect due to low signal strength? Cisco DNA Center with iOS, Samsung, and Intel Analytics answers these questions.

Figure 9.15: iOS Analytics



Neighbor APs (3)

BSSID	AP Name	Channel	RSSI (dBm)	Location
38:90:A5:CD:69:8F	LAB-AP00F2.8B27.B788	165	-55	Global/North America/USA/Californ
38:90:A5:CD:69:7F	AP0081.C424.3CE2	162	-70	Global/North America/USA/Californ
38:90:A5:CD:69:6F	SCJ01_9130_1	161	-58	Global/North America/USA/Californ

Client Disassociation Details (144)

Time	Disassociation Reason	Disassociated AP	Session Duration	AP Location
Apr 27, 2022 9:55 AM	Device idle	SCJ01_9130_1	--	Global/Nort
Apr 27, 2022 9:50 AM	User triggered disassociation	SCJ01_9130_1	--	Global/Nort
Apr 27, 2022 9:45 AM	Device idle	SCJ01_9130_1	--	Global/Nort
Apr 27, 2022 9:40 AM	Device idle	SCJ01_9130_1	--	Global/Nort

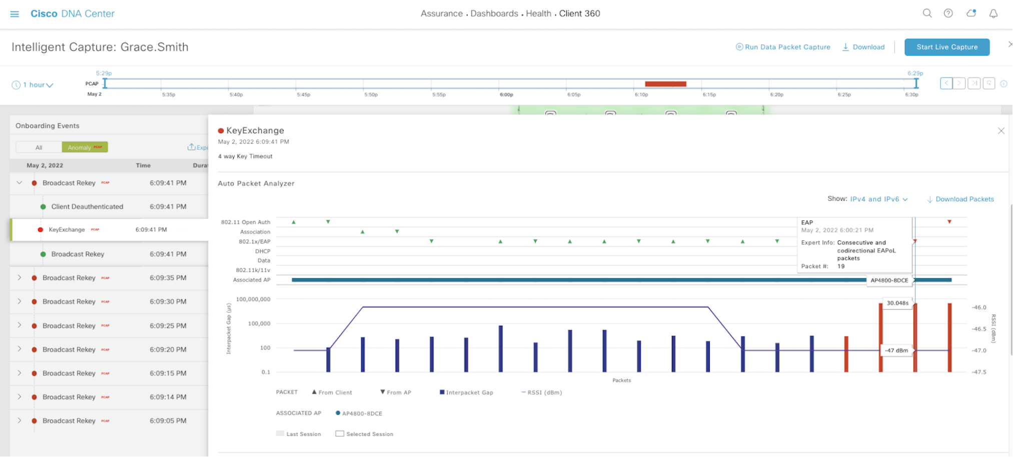
Intelligent Capture

Intelligent Capture allows the engineer to view, manage, and troubleshoot captured onboarding and data packets to identify client issues. The timeline is similar to other timelines in Cisco DNA Center but is limited to 1 hour, 3 hours, or 5 hours. Onboarding Events are shown in green, whereas Anomaly Events are shown in red. Anomaly Events are captured automatically when onboarding events occur. This allows the engineer to go back in time to see the packets while the client was failing to onboard. This negates the necessity for the engineer to start a Live Packet Capture first and then have the user recreate the problem.

Note Anomaly Capture has to be set up first from the `Assurance > Intelligent Capture Settings` page.

Start a Live Capture by clicking the `Start Live Capture` button. This will capture onboarding packets for Onboarding Events and RF Statistics. Live capture sessions will run for 3 hours by default but can be stopped before 3 hours or extended if necessary. This can be used to instantly troubleshoot a client if required in place of the scheduled capture. The engineer can view Live Packet Captures from the `Assurance > Intelligent Capture Settings` page. Captured packets can be viewed from the Onboarding Events page with events with a packet capture icon. These packets can be downloaded, exported, and/or viewed in the Auto Packet Analyzer section.

Figure 9.16: Intelligent Capture



Intelligent Capture: Grace.Smith

Onboarding Events

May 2, 2022	Time	Duration
Broadcast Rekey PCAP	6:09:41 PM	
Client Deauthenticated	6:09:41 PM	
KeyExchange PCAP	6:09:41 PM	
Broadcast Rekey	6:09:41 PM	
Broadcast Rekey PCAP	6:09:35 PM	
Broadcast Rekey PCAP	6:09:30 PM	
Broadcast Rekey PCAP	6:09:25 PM	
Broadcast Rekey PCAP	6:09:20 PM	
Broadcast Rekey PCAP	6:09:15 PM	
Broadcast Rekey PCAP	6:09:14 PM	
Broadcast Rekey PCAP	6:09:05 PM	

KeyExchange
May 2, 2022 6:09:41 PM
4 way Key Timeout

EAP
May 2, 2022 6:00:21 PM
Expert Info: Consecutive and codirectional EAPoL packets
Packet #: 19

The Client Location dashlet allows the engineer to view the location of the client and APs on a Floor Map. It also displays the Heat Map representing signal strength. Client Location requires the integration of Cisco CMX or Cisco DNA Spaces with Cisco DNA Center. Please see **Chapter 12** for more information about such integrations.

The RF Statistics dashlet shows RSSI, SNR, Rx Data Rates, Tx and Rx Packets, as well as Tx Retries. These are refreshed every 30 seconds to give a real-time view of the client RF environment to help troubleshoot client connectivity issues.

In addition to the Live Packet Capture, the engineer also has the ability to Schedule a Client Packet Capture, which can be done from the `Assurance > Intelligent Capture Settings` page.

While the Live Capture only captures packets related to Onboarding Events, clicking `Run Data Capture` will capture all packets transmitted between the client and AP.

10. Network Reasoner

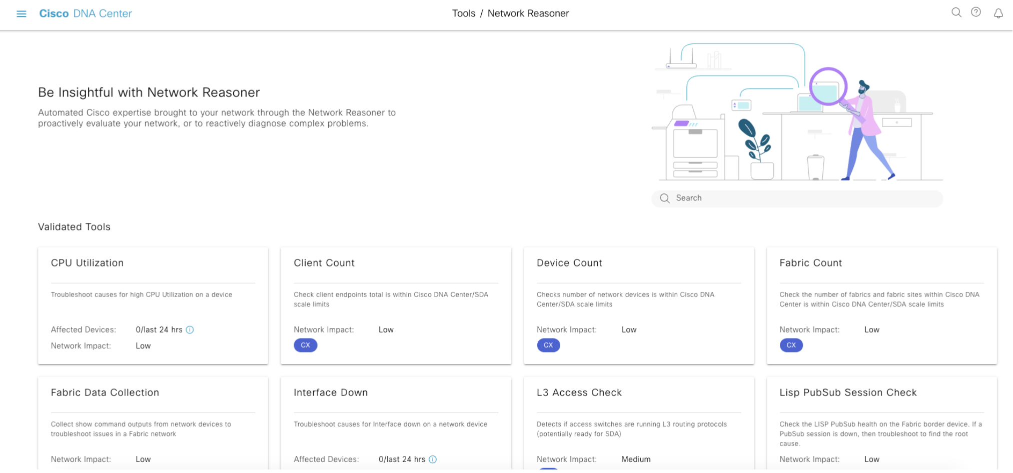
Cisco DNA Center's Network Reasoner tool provides a host of insights that can aid in proactively evaluating a network's health, or reactively diagnosing complex issues to get to the root cause quickly and seamlessly. Just as the Machine Reasoning Engine (MRE) mentioned in Chapter 8 provides the ability to run machine reasoning on issues that have been flagged, the Network Reasoner tool allows a network engineer to run machine reasoning to assist in troubleshooting a variety of issues. This chapter will cover all of the workflows that the Network Reasoner currently supports.

The Network Reasoner currently offers the following workflows:

- Redundant Link Check
- Power Supply Validation
- Ping Device Check
- CPU Utilization Check
- Interface Down
- System Bug Identifier

The Network Reasoner can be accessed via the Cisco DNA Center main menu, selecting `Tools > Network Reasoner`.

Figure 10.1: Network Reasoner



Be Insightful with Network Reasoner

Automated Cisco expertise brought to your network through the Network Reasoner to proactively evaluate your network, or to reactively diagnose complex problems.

Validated Tools

CPU Utilization

Troubleshoot causes for high CPU Utilization on a device

Affected Devices: 0/last 24 hrs

Network Impact: Low

Client Count

Check client endpoints total is within Cisco DNA Center/SDA scale limits

Network Impact: Low

CX

Device Count

Checks number of network devices is within Cisco DNA Center/SDA scale limits

Network Impact: Low

CX

Fabric Count

Check the number of fabrics and fabric sites within Cisco DNA Center is within Cisco DNA Center/SDA scale limits

Network Impact: Low

CX

Fabric Data Collection

Collect show command outputs from network devices to troubleshoot issues in a Fabric network

Network Impact: Low

Interface Down

Troubleshoot causes for Interface down on a network device

Affected Devices: 0/last 24 hrs

L3 Access Check

Detects if access switches are running L3 routing protocols (potentially ready for SDA)

Network Impact: Medium

Lisp PubSub Session Check

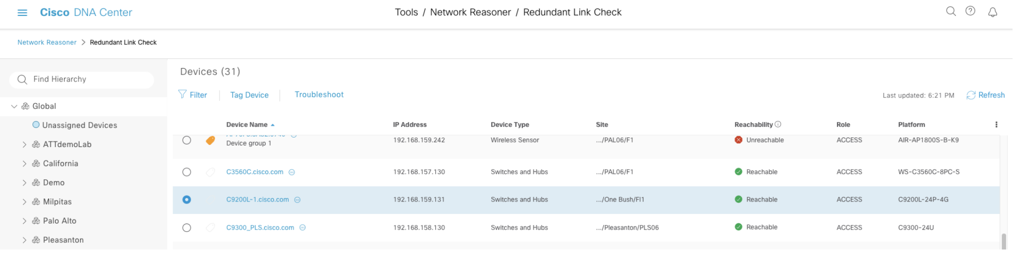
Check the LISP PubSub health on the Fabric border device. If a PubSub session is down, then troubleshoot to find the root cause.

Network Impact: Low

Redundant Link Check

The redundant link check workflow validates whether there are two uplinks associated with an **ACCESS** role device. After selecting this workflow, a list of devices with that role is displayed. Select a device, then click `Troubleshoot`.

Figure 10.2: Redundant Link Check



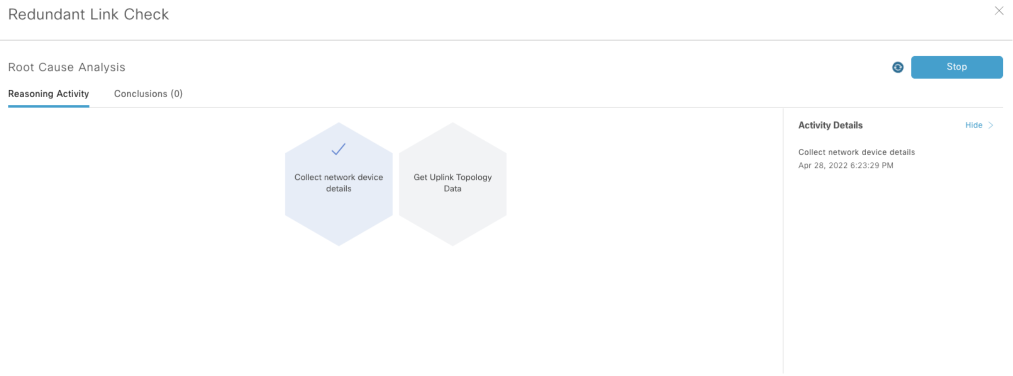
Devices (31)

Last updated: 6:21 PM

	Device Name	IP Address	Device Type	Site	Reachability	Role	Platform
○	Device group 1	192.168.159.242	Wireless Sensor	.../PAL06/F1	Unreachable	ACCESS	AIR-AP1800S-B-K9
○	C3560C.cisco.com	192.168.157.130	Switches and Hubs	.../PAL06/F1	Reachable	ACCESS	WS-C3560C-8PC-S
●	C9200L-1.cisco.com	192.168.159.131	Switches and Hubs	.../One Bush/Fl1	Reachable	ACCESS	C9200L-24P-4G
○	C9300_PLS.cisco.com	192.168.158.130	Switches and Hubs	.../Pleasanton/PLS06	Reachable	ACCESS	C9300-24U

The Network Reasoner runs a root cause analysis for checking redundant links on the selected network device.

Figure 10.3: Redundant Link Check Root Cause Analysis



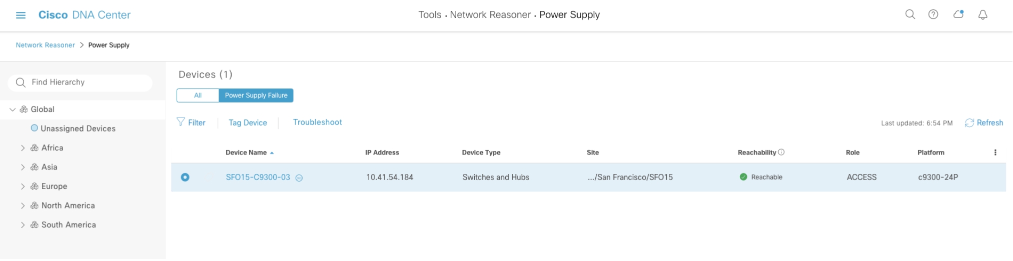
Collect network device details
Apr 28, 2022 6:23:29 PM

After the analysis is complete, the machine reasoner conclusions and suggested actions are presented. In this example, the switch selected does not have any redundant uplinks configuration and the reasoner recommends adding one while providing reasons why. This is particularly useful to a network engineer as it is a very streamlined process compared to manually checking for redundant links in a network which would involve having to manually log into each access switch and execute multiple commands. This workflow is an example of the tremendous time savings that can be yielded by Cisco DNA Center.

Power Supply Validation

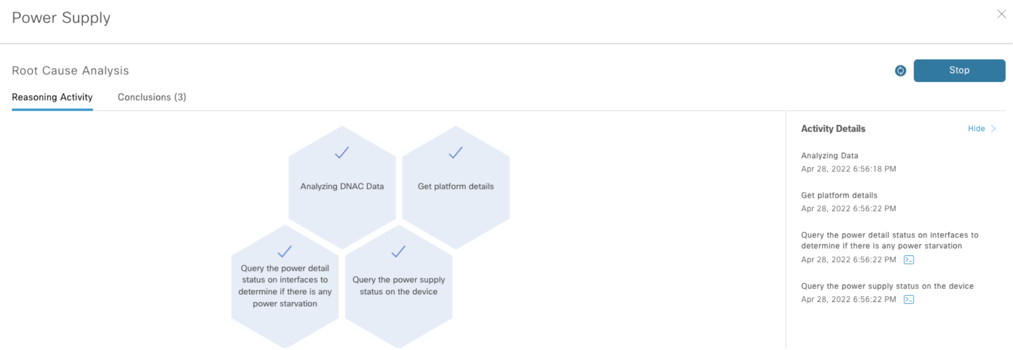
The Power Supply workflow determines the root cause for power supply issues on a network device. After entering this workflow and selecting a networking device with power supply issues, root cause analysis is programmatically performed for the issue.

Figure 10.4: Power Supply Troubleshooting



	Device Name	IP Address	Device Type	Site	Reachability	Role	Platform
●	SFO15-C9300-03	10.41.54.184	Switches and Hubs	.../San Francisco/SFO15	Reachable	ACCESS	c9300-24P

Figure 10.5: Power Supply Root Cause Analysis


Power Supply
Root Cause Analysis
Stop
Reasoning Activity
Conclusions (3)
✓ Analyzing DNAC Data
✓ Get platform details
✓ Query the power detail status on interfaces to determine if there is any power starvation
✓ Query the power supply status on the device
Activity Details
Hide

Analyzing Data
Apr 28, 2022 6:56:18 PM

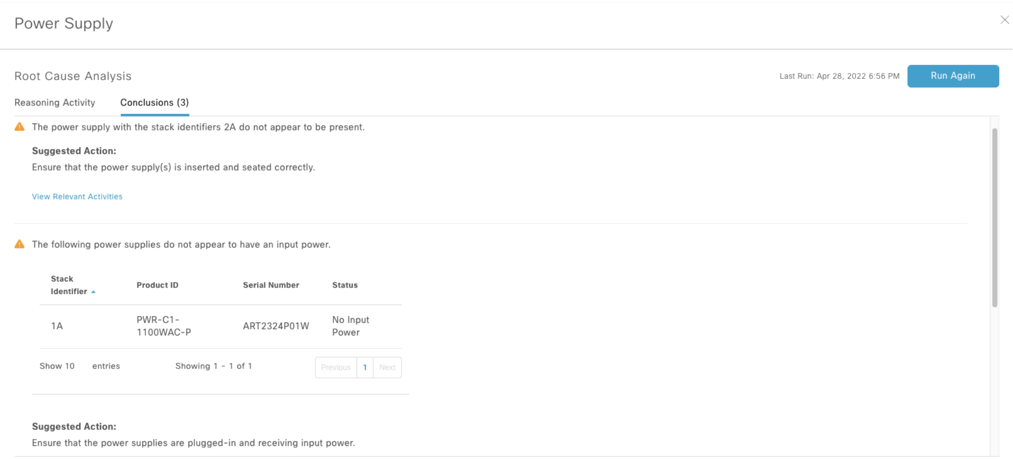
Get platform details
Apr 28, 2022 6:56:22 PM

Query the power detail status on interfaces to determine if there is any power starvation
Apr 28, 2022 6:56:22 PM

Query the power supply status on the device
Apr 28, 2022 6:56:22 PM

After the power supply analysis has been completed, the machine reasoner conclusions and suggested actions are presented. In this case, the switch experiencing power problems has a power supply that is not present.

Figure 10.6: Power Supply Conclusion



The power supply with the stack identifiers 2A do not appear to be present.

Suggested Action:
Ensure that the power supply(s) is inserted and seated correctly.

The following power supplies do not appear to have an input power.

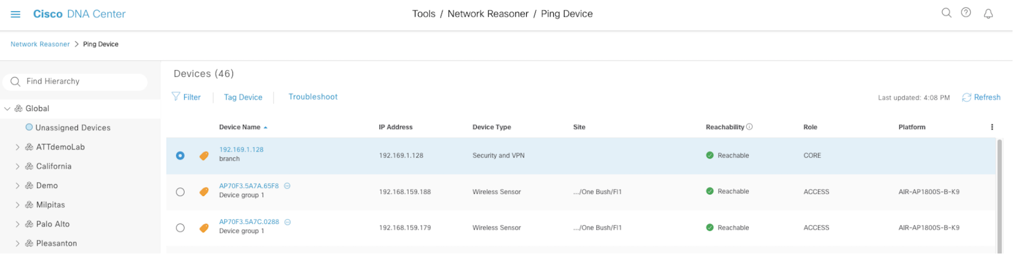
Stack Identifier	Product ID	Serial Number	Status
1A	PWR-C1-1100WAC-P	ART2324P01W	No Input Power

Suggested Action:
Ensure that the power supplies are plugged-in and receiving input power.

Ping Device Check

The Ping Device workflow provides a simple functionality that can ping a target IP address from a selected source device. After initiating the Ping Device workflow and selecting a network device to initiate the ping from, enter a target IP address, then click `Run Machine Reasoning`.

Figure 10.7 Select Network Device

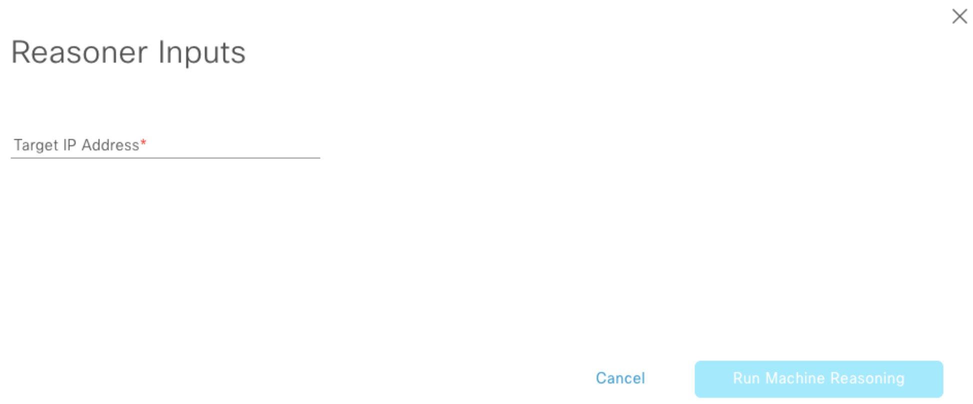


Devices (46)

Last updated: 4:08 PM

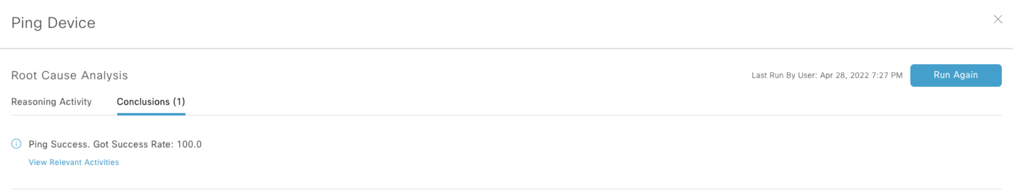
	Device Name	IP Address	Device Type	Site	Reachability	Role	Platform
●	192.169.1.128 branch	192.169.1.128	Security and VPN		Reachable	CORE	
○	AP70F3.5A7A.65F8 Device group 1	192.168.159.188	Wireless Sensor	.../One Bush/Fl1	Reachable	ACCESS	AIR-AP1800S-B-K9
○	AP70F3.5A7C.0288 Device group 1	192.168.159.179	Wireless Sensor	.../One Bush/Fl1	Reachable	ACCESS	AIR-AP1800S-B-K9

Figure 10.8: Ping Input Target IP



The ping is initiated and the results are displayed. This switch was able to ping its target IP with 100% success.

Figure 10.9: Ping Results



Ping Device

Root Cause Analysis

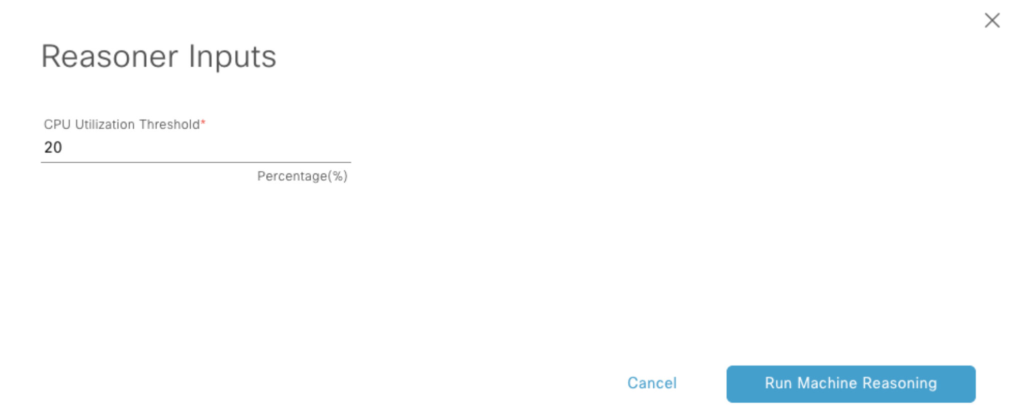
Last Run By User: Apr 28, 2022 7:27 PM

Ping Success. Got Success Rate: 100.0

CPU Utilization Check

The CPU Utilization workflow troubleshoots the causes of high CPU utilization on network devices. Select the CPU Utilization workflow then select a network device that has been experiencing high CPU utilization from the list displayed. Click `Troubleshoot` to begin root cause analysis. Provide a maximum CPU utilization threshold then click `Run Machine Reasoning` to initiate the root cause analysis.

Figure 10.10: CPU Utilization Threshold

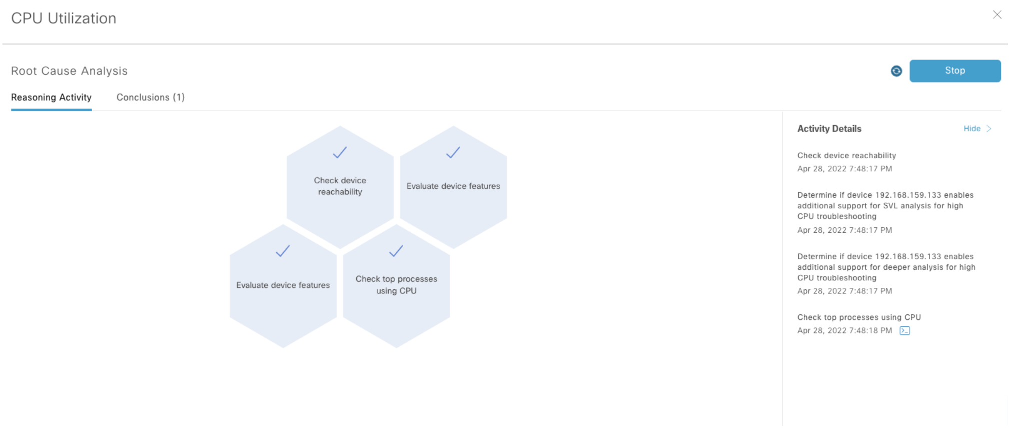


Reasoner Inputs

CPU Utilization Threshold*
20
Percentage(%)

Root Cause Analysis is initiated and checks the network device for CPU utilization above the threshold specified.

Figure 10.11: CPU Utilization Root Cause Analysis


CPU Utilization
Root Cause Analysis
Stop
Reasoning Activity
Conclusions (1)
✓ Check device reachability
✓ Evaluate device features
✓ Evaluate device features
✓ Check top processes using CPU
Activity Details
Hide

Check device reachability
Apr 28, 2022 7:48:17 PM

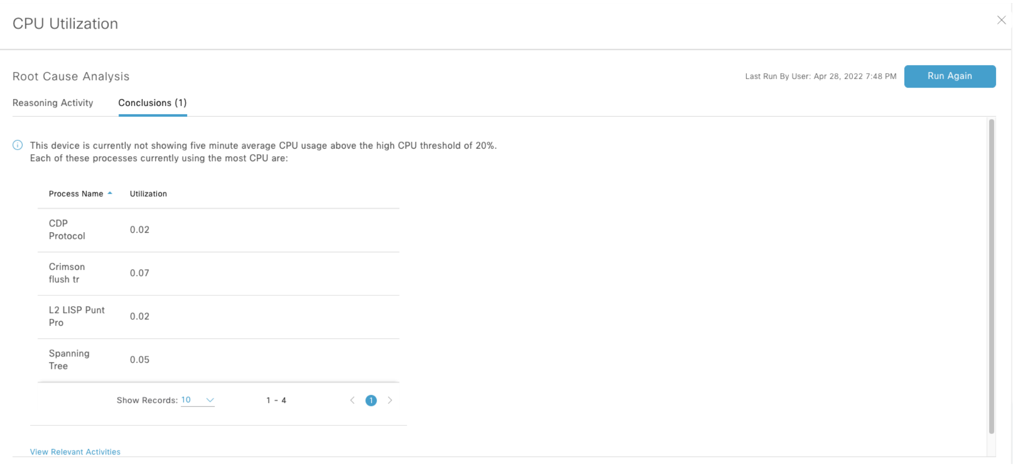
Determine if device 192.168.159.133 enables additional support for SVL analysis for high CPU troubleshooting
Apr 28, 2022 7:48:17 PM

Determine if device 192.168.159.133 enables additional support for deeper analysis for high CPU troubleshooting
Apr 28, 2022 7:48:17 PM

Check top processes using CPU
Apr 28, 2022 7:48:18 PM

Once the root cause analysis is complete, the results are displayed. In this example, the selected switch is not experiencing a high CPU utilization.

Figure 10.12: CPU Utilization Conclusion



CPU Utilization

Root Cause Analysis

Last Run By User: Apr 28, 2022 7:48 PM

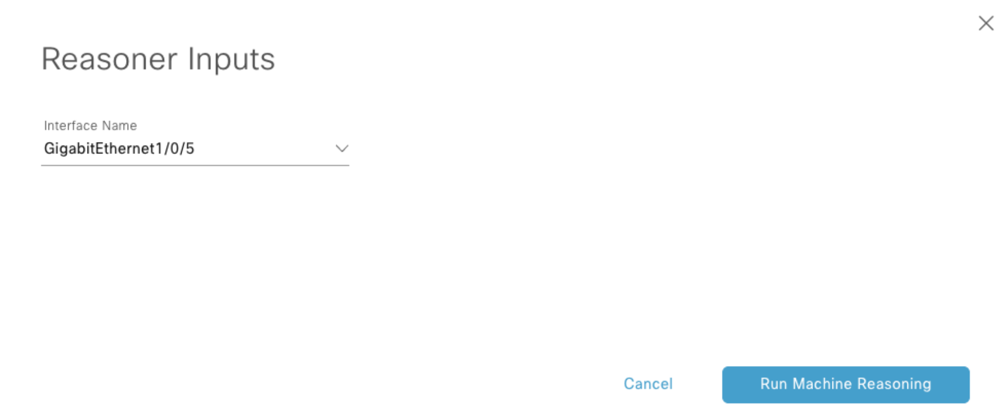
This device is currently not showing five minute average CPU usage above the high CPU threshold of 20%.
Each of these processes currently using the most CPU are:

Process Name	Utilization
CDP Protocol	0.02
Crimson flush tr	0.07
L2 LISP Punt Pro	0.02
Spanning Tree	0.05

Interface Down

The Interface Down workflow troubleshoots potential causes for an interface on a network device to be in a down state. After selecting the Interface Down workflow, select a switch that has experienced an interface down issue recently, then click `Troubleshoot`. Provide the interface that needs to be evaluated, then click `Run Machine Reasoning Engine`.

Figure 10.13: Select Device Interface

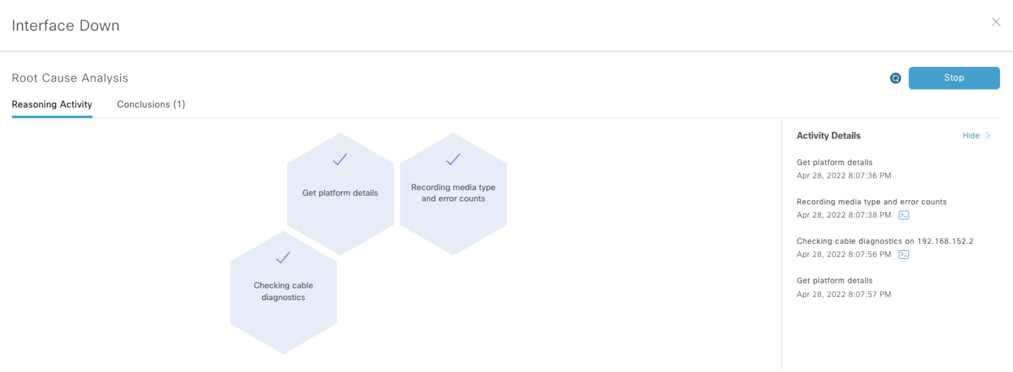


Reasoner Inputs

Interface Name
GigabitEthernet1/0/5

Root Cause Analysis begins to check the interface for issues.

Figure 10.14 Interface Down Root Cause Analysis



Get platform details
Apr 28, 2022 8:07:36 PM

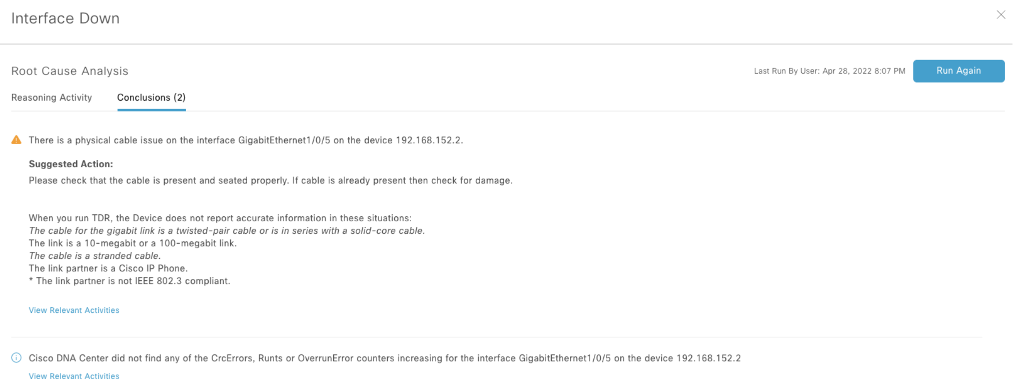
Recording media type and error counts
Apr 28, 2022 8:07:38 PM

Checking cable diagnostics on 192.168.152.2
Apr 28, 2022 8:07:56 PM

Get platform details
Apr 28, 2022 8:07:57 PM

Once the analysis is complete, the results are displayed, which indicates the cause of this device’s interface outage as being a physical cable issue.

Figure 10.15: Interface Down Conclusion



⚠ There is a physical cable issue on the interface GigabitEthernet1/0/5 on the device 192.168.152.2.

Suggested Action:
Please check that the cable is present and seated properly. If cable is already present then check for damage.

When you run TDR, the Device does not report accurate information in these situations:
The cable for the gigabit link is a twisted-pair cable or is in series with a solid-core cable.
The link is a 10-megabit or a 100-megabit link.
The cable is a stranded cable.
The link partner is a Cisco IP Phone.
* The link partner is not IEEE 802.3 compliant.

View Relevant Activities

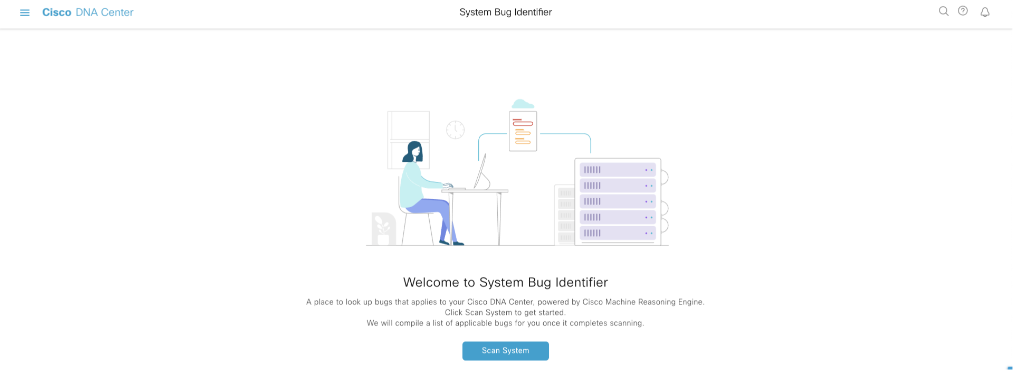
ⓘ Cisco DNA Center did not find any of the CrcErrors, Runts or OverrunError counters increasing for the interface GigabitEthernet1/0/5 on the device 192.168.152.2

View Relevant Activities

System Bug Identifier

The System Bug Identifier workflow can scan the Cisco DNA Center system for known bugs that it may be affected by. This is very helpful in preventing issues regarding bugs that have already been fixed, but not yet patched on a particular Cisco DNA Center appliance. After selecting this workflow, click `Scan System` to begin the scan for bugs.

Figure 10.16: Bug Identifier Scan System



Welcome to System Bug Identifier

A place to look up bugs that applies to your Cisco DNA Center, powered by Cisco Machine Reasoning Engine.
Click Scan System to get started.
We will compile a list of applicable bugs for you once it completes scanning.

Choose to begin the scan immediately or schedule it for a later time. Once the scan is initiated, the page indicates that the scan is in progress. After the scan is complete, a list of bugs that are affecting the Cisco DNA Center system are presented, with:

- Link to the bug ID
- Description of the issue
- Severity level
- The first time the issue was identified
- If there is a workaround for the issue
- Which Cisco DNA Center versions are affected by the bug

This allows a network engineer to quickly identify bugs with their Cisco DNA Center system and quickly perform any applicable workarounds, patching, or upgrades.

The Network Reasoner powered by Cisco's industry-leading Machine Reasoning Engine packs powerfully-automated workflows designed to bring process consistency, best practices, and help reduce the time tasks take to complete by staff. With the power of the Network Reasoner, more tasks can be assigned to less-experienced technical staff to complete with confidence. A task that would take hours in some cases is now completed with the click of a button in mere minutes.

11. Application Health

This chapter covers application visibility and application experience, which is critical to validating and troubleshooting user experience.

Cisco DNA Center processes complex application data and telemetry from network devices. The application data in Cisco DNA Center is displayed in the Application Health dashboard, Client 360, and Device 360 pages. The dashboard provides insights into the performance of the applications running in a network, which is highly valuable information for network engineers and saves a significant amount of time when troubleshooting application issues, reducing the MTTR.

Based on the network device from which the application data is collected, the network engineer can view some or all of the KPIs below:

- Application name
- Throughput
- DSCP markings
- Performance metrics (packet loss, latency, and jitter)

Application Name and Throughput are referred to as quantitative metrics and fall under Application Visibility, while DSCP markings, packet loss, jitter, and latency are referred to as qualitative metrics and fall under Application Experience.

Application Visibility data is available from routers and switches running IOS XE and for WLCs running both AireOS and IOS XE.

More detailed Application Experience data is available from routers running IOS XE running the Cisco Performance Monitor (PerfMon) feature and Cisco Application Response Time metrics, and from the Cisco Catalyst 9800 WLCs.

Optimized Application Performance Monitoring (APM) is a feature that reduces the overhead in collecting NetFlow data. This feature is supported on routers running IOS XE and Cisco Catalyst 9800 WLCs.

Please refer to the **Cisco DNA Center Assurance User Guide** for a complete list of devices and minimum OS versions necessary to benefit from this feature.

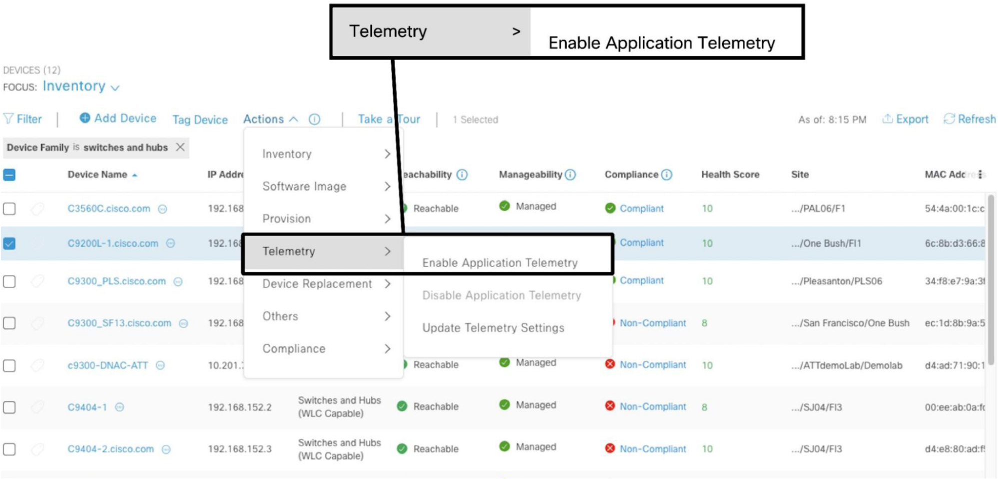
Configuring Application Visibility and Application Experience

The configuration for Application Visibility and Experience on network devices can be completely automated via the Cisco DNA Center inventory page by selecting the device and applying **application telemetry** ;as shown below. All the necessary commands required to enable Application Visibility and Experience, which can be quite a few lines to enter manually, are configured automatically in a few seconds using Cisco DNA Center Automation. This is invaluable to network engineers as it enables a key feature quickly and easily, increasing their productivity. The interfaces and WLANs on which the configurations are pushed are based on certain criteria. Please refer to the Cisco **DNA Center User Guide** for more details.

There are some key prerequisites before the application telemetry can be automatically applied to the network devices from Cisco DNA Center. This feature is not supported for Guest SSIDs. For the WLCs, the SSIDs need to be provisioned via the Cisco DNA Center automation features. If the SSIDs were already configured on the WLCs from the WLC GUI, then the required configuration can be manually applied on a per-SSID basis via the CLI of the WLC. Please refer to the section below on **Configuring Application Telemetry** on the Catalyst 9800 for the CLI commands required.

For network switches and routers, there are some prerequisites, but provisioning from Cisco DNA Center is not required for application telemetry to be pushed.

Figure 11.1: Enable Application Telemetry



	Device Name	IP Addr		eachability	Manageability	Compliance	Health Score	Site	MAC Adc
☐	C3560C.cisco.com	192.168		Reachable	Managed	Compliant	10	.../PAL06/F1	54:4a:00:1c:c
☑	C9200L-1.cisco.com	192.16				Compliant	10	.../One Bush/Fl1	6c:8b:d3:66:8
☐	C9300_PLS.cisco.com	192.168				Compliant	10	.../Pleasanton/PLS06	34:f8:e7:9a:3
☐	C9300_SF13.cisco.com	192.168				Non-Compliant	8	.../San Francisco/One Bush	ec:1d:8b:9a:5
☐	c9300-DNAC-ATT	10.201.		Reachable	Managed	Non-Compliant	10	.../ATTdemoLab/Demolab	d4:ad:71:90:1
☐	C9404-1	192.168.152.2	Switches and Hubs (WLC Capable)	Reachable	Managed	Non-Compliant	8	.../SJ04/Fl3	00:ee:ab:0a:f
☐	C9404-2.cisco.com	192.168.152.3	Switches and Hubs (WLC Capable)	Reachable	Managed	Non-Compliant	10	.../SJ04/Fl3	d4:e8:80:ad:f

Real-World Scenario

Aditya is a Network Architect working at a chain of retail stores. He handles the escalations of all the tickets that the other Network Engineers are unable to resolve. A ticket was escalated that said that users are not able to access Office 365. Aditya has recently deployed the ThousandEyes agents on their Catalyst 9000 switches using Cisco DNA Center. He brought up the Application Health page for Office 365. He then clicked on the ThousandEyes link and cross-launched the ThousandEyes interface. Once in the interface, it showed an issue with a load balancer at the SaaS provider. Aditya was able to notify the helpdesk that Office 365 is having an issue and was able to provide this information to Microsoft for quicker issue resolution.

Configuring Application Telemetry on the Catalyst 9800

If the SSIDs are not provisioned from Cisco DNA Center, then the application telemetry cannot be applied from Cisco DNA Center. In those cases where the SSIDs are already configured from the WLC GUI, the required commands to enable application visibility and experience can be configured on a per-SSID basis from the CLI. For the Catalyst 9800 WLC, the configuration can be applied for SSIDs in local, flex, or fabric mode.

Below are the commands to be applied to the Catalyst 9800 WLC CLI to enable application visibility and experience.

SSID in Local Mode:

```
flow exporter avc_exporter
    destination <Cisco DNA Center enterprise Virtual IP Addr>
    source <Source Interface>
    transport udp 6007
    export-protocol ipfix
    option vrf-table timeout 300
    option ssid-table timeout 300
    option application-table timeout 300
    option application-attributes timeout 300

flow exporter avc_local_exporter
    destination local wlc

flow monitor avc_ipv4_assurance
    exporter avc_exporter
    exporter avc_local_exporter
    cache timeout active 60
    default cache entries
    record wireless avc ipv4 assurance

flow monitor avc_ipv4_assurance_rtp
    exporter avc_exporter
    cache timeout active 60
    default cache entries
    record wireless avc ipv4 assurance-rtp

wireless profile policy WORK_FLOOR_Global_NF_8258fbfb
    shutdown
    ipv4 flow monitor avc_ipv4_assurance input
    ipv4 flow monitor avc_ipv4_assurance output
    ipv4 flow monitor avc_ipv4_assurance_rtp input
    ipv4 flow monitor avc_ipv4_assurance_rtp output
    no shutdown
```

SSID in Flex/Fabric mode:

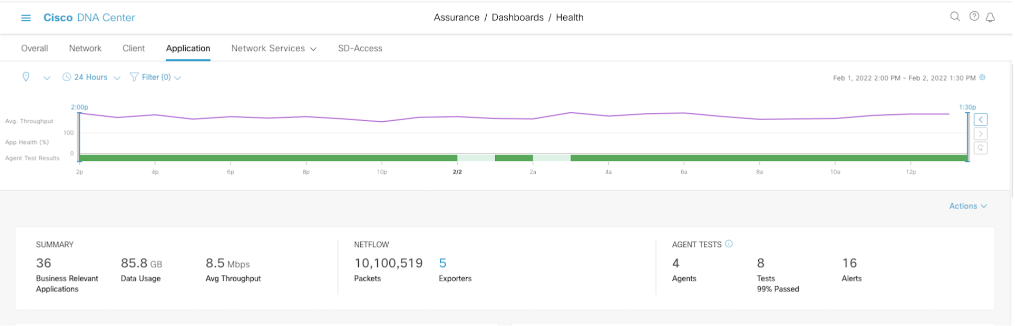
```
flow exporter avc_exporter
    destination <Cisco DNA Center enterprise Virtual IP Addr>
    source <Source Interface>
    transport udp 6007
    export-protocol ipfix
    option vrf-table timeout 300
    option ssid-table timeout 300
    option application-table timeout 300
    option application-attributes timeout 300
flow exporter avc_local_exporter
     destination local wlc
flow monitor avc_ipv4_assurance
    exporter avc_exporter
    exporter avc_local_exporter
    cache timeout active 60
    default cache entries
    record wireless avc ipv4 assurance
flow monitor avc_ipv4_assurance_rtp
     exporter avc_exporter
     cache timeout active 60
     default cache entries
     record wireless avc ipv4 assurance-rtp
flow monitor avc_basic_monitor
     exporter avc_exporter
     exporter avc_local_exporter
     cache timeout active 60
     default cache entries
     record wireless avc basic
wireless profile policy Flex_SSID_Global_NF_0cd02814
    shutdown
    ipv4 flow monitor avc_basic_monitor input
    ipv4 flow monitor avc_basic_monitor output
    no shutdown
wireless profile policy Fabric_SSID_Global_NF_0cd02814
    shutdown
    ipv4 flow monitor avc_basic_monitor input
    ipv4 flow monitor avc_basic_monitor output
    no shutdown
```

Visualizing Application Experience in Cisco DNA Center

The network engineer can navigate from the main menu of Cisco DNA Center to the `Assurance > Health` menu to access the different dashboards. From there, network engineers can select the `Application` tab to view the **Application Health Dashboard**. The network engineer can then use the site filters to select the desired site for which to visualize the application health.

On top of the dashboard is the timeline which displays the average throughput of the total traffic on the site, the percentage of healthy business-relevant applications, and the ThousandEyes agent test results if ThousandEyes is integrated with Cisco DNA Center. This integration is covered in **Chapter 12**.

Figure 11.2: Application Health Dashboard Timeline



SUMMARY

36 Business Relevant Applications

85.8 GB Data Usage

8.5 Mbps Avg Throughput

NETFLOW

10,100,519 Packets

5 Exporters

AGENT TESTS

4 Agents

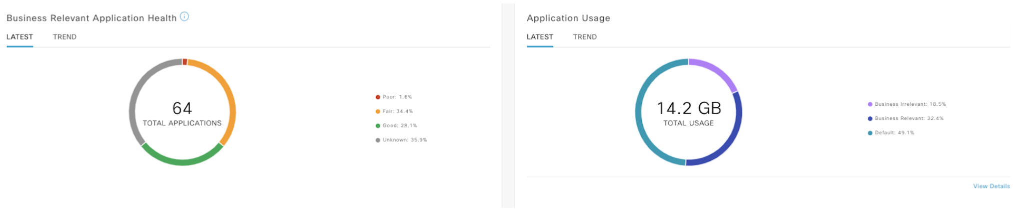
8 Tests 99% Passed

16 Alerts

Below the timeline, the network engineer can view the Summary data split into 3 sections. The first section shows the total business-relevant applications, data usage, and average throughput. The next section displays the number of NetFlow exporters sending NetFlow data to the Cisco DNA Center. These could be routers, switches, or WLC that the network engineer has set up with application telemetry. The last section in the Summary shows the number of ThousandEyes Agent setup and test results.

Below the Summary section, the Business Relevant Application Health and Application usage dashlets are shown. The network engineer can access the data needed to get an idea of the amount of traffic flowing through this site which could be used for capacity planning. The `TREND` tab in each dashlet shows the data for the period selected in the dashboard filter. So, if 24 hours were selected, the Trend would show 24-hours worth of data. This enables the network engineers to visualize the load on the network at this site. It is important to be able to visualize trends over time to look for patterns of increasing or decreasing loads. This data is key to making data-driven intelligent decisions on throttling or QoS.

Figure 11.3: Application Health Dashboard Dashlets

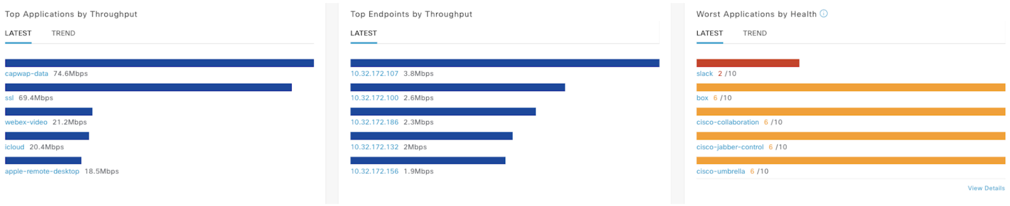


The section after the Summary displays 3 dashlets:

- Top Applications by Throughput
- Top Endpoints by Throughput
- Worst Applications by Health

These dashlets can be used by the network engineer to identify if any non-business applications are consuming too much bandwidth, to help decide if they need to throttle those applications. It can also be used to find endpoints consuming too much bandwidth. The last dashlet helps to find which applications are performing poorly in the network to help make decisions on debugging QoS or other network configurations related to traffic flow in the network.

Figure 11.4: Application Health Dashboard Dashlets

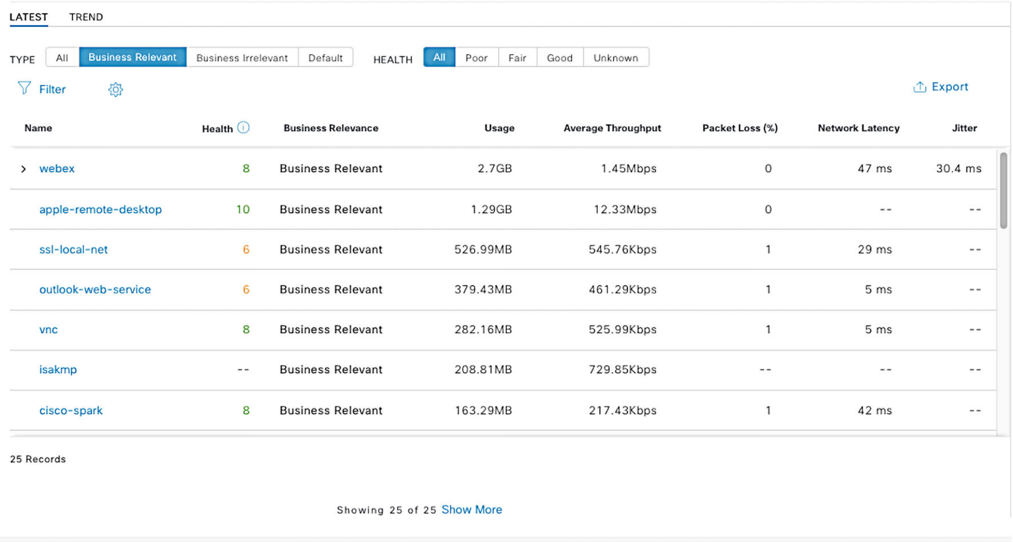


Below the dashlets, the network engineer can see the full list of applications running on the selected site. Filters can be chosen by All, Business Relevant, Business Irrelevant, or Default applications. Network engineers can also filter by the health of the applications. Application Health is only calculated for TCP-based applications.

Depending on the network device, the application experience data might or might not show. For example, if NetFlow data is sent only from switches to Cisco DNA Center, the network engineer will not see any Application Experience data. If NetFlow data is sent from routers or WLCs, then the data will appear. Application Visibility data will always show regardless of the device sending NetFlow to the Cisco DNA Center appliance.

The network engineer can view the usage and application throughput for application visibility and packet loss, jitter, and latency for application experience for each application in the below table. This table can be exported as a CSV report as well. The table can be sorted to view the Top Applications by throughput or usage, highly useful data for network engineers to make decisions on managing network bandwidth.

Figure 11.5: Application Health Dashboard Application Table



TYPE: All | **Business Relevant** | Business Irrelevant | Default

HEALTH: **All** | Poor | Fair | Good | Unknown

Name	Health	Business Relevance	Usage	Average Throughput	Packet Loss (%)	Network Latency	Jitter
› webex	8	Business Relevant	2.7GB	1.45Mbps	0	47 ms	30.4 ms
apple-remote-desktop	10	Business Relevant	1.29GB	12.33Mbps	0	--	--
ssl-local-net	6	Business Relevant	526.99MB	545.76Kbps	1	29 ms	--
outlook-web-service	6	Business Relevant	379.43MB	461.29Kbps	1	5 ms	--
vnc	8	Business Relevant	282.16MB	525.99Kbps	1	5 ms	--
isakmp	--	Business Relevant	208.81MB	729.85Kbps	--	--	--
cisco-spark	8	Business Relevant	163.29MB	217.43Kbps	1	42 ms	--

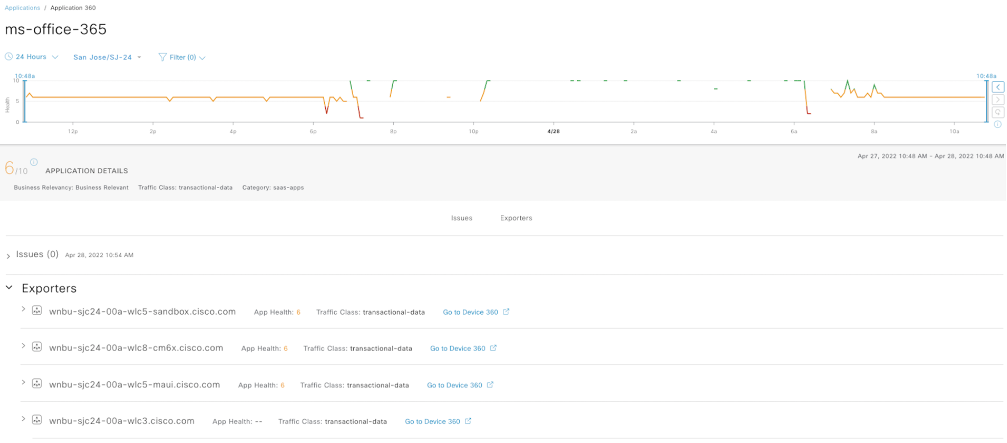
25 Records

Showing 25 of 25 Show More

Selecting an `application name` will take the network engineer to the Application 360 page.

In this example of the ms-office-365 application, the network engineer can see the timeline showing the health score of the application which is calculated using the application experience KPIs. For applications that do not have application experience, the application 360 timeline will be empty. Below the timeline, the network engineer can view the exporters (network devices such as switches, WLCs, and routers) sending application data via NetFlow to the Cisco DNA Center. This enables the network engineer to quickly visualize from which part of the network the application data is coming.

Figure 11.6: Application 360



Applications / Application 360

ms-office-365

24 Hours | San Jose/SJ-24 | Filter (0)

6/10 APPLICATION DETAILS

Apr 27, 2022 10:48 AM - Apr 28, 2022 10:48 AM

Business Relevancy: Business Relevant | Traffic Class: transactional-data | Category: saas-apps

Issues | Exporters

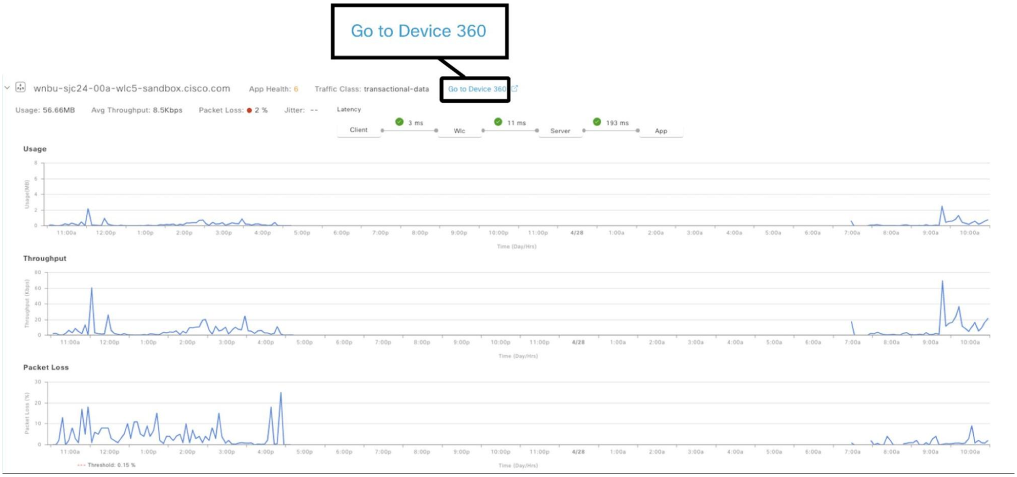
Issues (0) Apr 28, 2022 10:54 AM

Exporters

wnbu-sjc24-00a-wlc5-sandbox.cisco.com	App Health: 6	Traffic Class: transactional-data	Go to Device 360
wnbu-sjc24-00a-wlc8-cm6x.cisco.com	App Health: 6	Traffic Class: transactional-data	Go to Device 360
wnbu-sjc24-00a-wlc5-maui.cisco.com	App Health: 6	Traffic Class: transactional-data	Go to Device 360
wnbu-sjc24-00a-wlc3.cisco.com	App Health: --	Traffic Class: transactional-data	Go to Device 360

Expanding one of the exporters, as shown below, displays the usage, throughput, packet loss, and other metrics over time for the ms-office-365 application. This provides the network engineers with visibility to quickly identify whether there are any issues with this application and the usage of this application in the network. Network Engineers can also view the clients using this application, their usage, and the identifier of the client; which could be the username or the IP Address of the client.

Figure 11.7: Application 360 Exporter Section

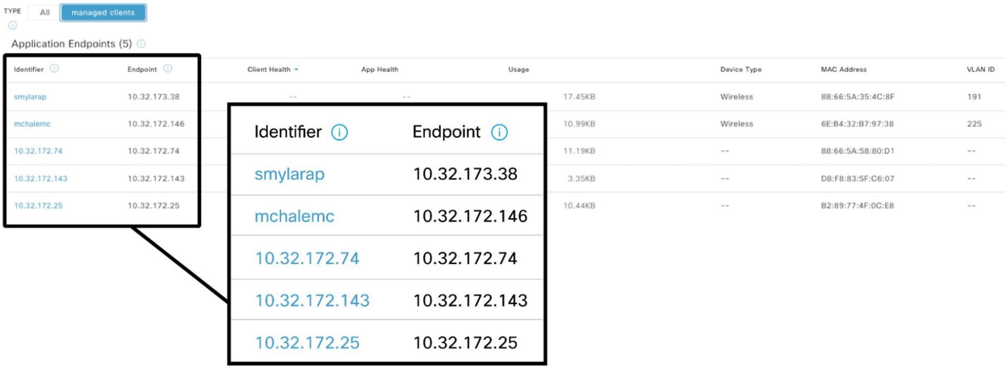


Go to Device 360

wnbu-sjc24-00a-wlc5-sandbox.cisco.com App Health: 6 Traffic Class: transactional-data Go to Device 360

Usage: 56.66MB Avg Throughput: 8.5Kbps Packet Loss: ● 2 % Jitter: --

Latency: Client — 3 ms — Wlc — 11 ms — Server — 193 ms — App



TYPE All managed clients

Application Endpoints (5)

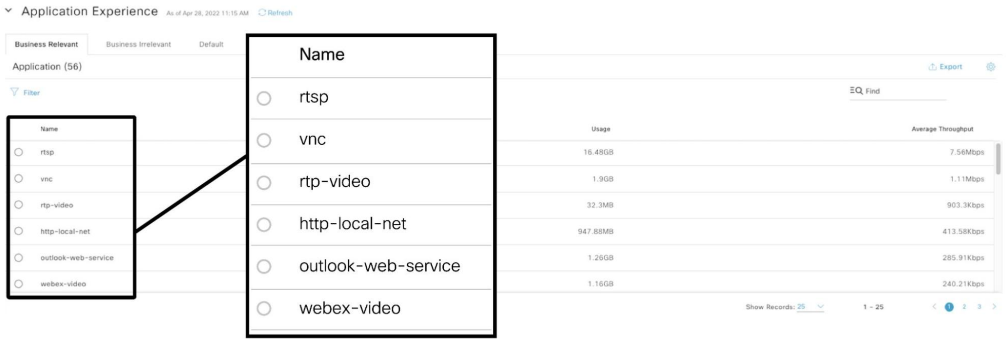
Identifier	Endpoint	Client Health	App Health	Usage	Device Type	MAC Address	VLAN ID
smylarap	10.32.173.38	--	--	17.45KB	Wireless	88:66:5A:35:4C:8F	191
mchalemc	10.32.172.146			10.99KB	Wireless	6E:B4:32:B7:97:38	225
10.32.172.74	10.32.172.74			11.19KB	--	88:66:5A:58:80:D1	--
10.32.172.143	10.32.172.143			3.35KB	--	D8:F8:83:5F:C6:07	--
10.32.172.25	10.32.172.25			10.44KB	--	B2:89:77:4F:0C:E8	--

Identifier	Endpoint
smylarap	10.32.173.38
mchalemc	10.32.172.146
10.32.172.74	10.32.172.74
10.32.172.143	10.32.172.143
10.32.172.25	10.32.172.25

Selecting the `Go to Device 360` page link, as shown in the screenshot above, will take the network engineer to the Device 360 page of this particular exporter which in this case is a WLC.

On the Device 360 page under the Application Experience section, the network engineer can view all the applications being sent via NetFlow from a particular device.

Figure 11.8: Device 360 Application Experience



Application Experience As of Apr 28, 2022 11:15 AM Refresh

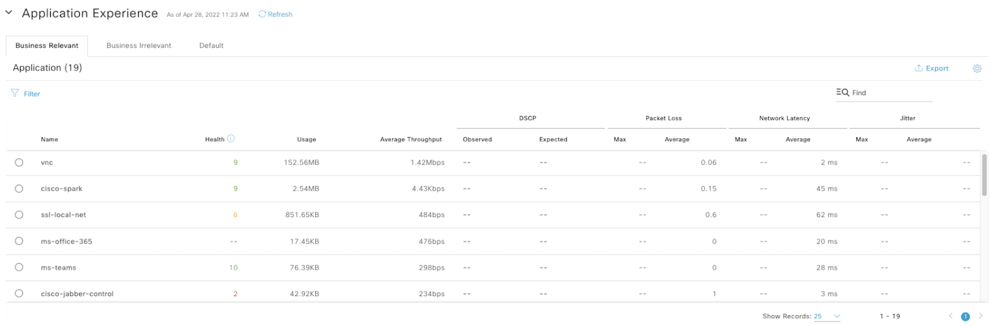
Application (56)

	Name	Usage	Average Throughput
○	rtsp	16.48GB	7.56Mbps
○	vnc	1.9GB	1.11Mbps
○	rtp-video	32.3MB	903.3Kbps
○	http-local-net	947.88MB	413.58Kbps
○	outlook-web-service	1.26GB	285.91Kbps
○	webex-video	1.16GB	240.21Kbps

Show Records: 25 1 - 25

The network engineer can also view the Application data for a particular client on the Client 360 page. This allows the engineer to view all the applications a client is using and troubleshoot client-specific application issues quickly and easily.

Figure 11.9: Client 360 Application Experience



Application Experience As of Apr 28, 2022 11:23 AM Refresh

Application (19)

				DSCP		Packet Loss		Network Latency		Jitter	
Name	Health	Usage	Average Throughput	Observed	Expected	Max	Average	Max	Average	Max	Average
○ vnc	9	152.56MB	1.42Mbps	--	--	--	0.06	--	2 ms	--	--
○ cisco-spark	9	2.54MB	4.43Kbps	--	--	--	0.15	--	45 ms	--	--
○ ssl-local-net	6	851.65KB	484bps	--	--	--	0.6	--	62 ms	--	--
○ ms-office-365	--	17.45KB	476bps	--	--	--	0	--	20 ms	--	--
○ ms-teams	10	76.39KB	298bps	--	--	--	0	--	28 ms	--	--
○ cisco-jabber-control	2	42.92KB	234bps	--	--	--	1	--	3 ms	--	--

Show Records: 25 1 - 19 1

Application Visibility and Application Experience give insights into the user experience in the network. This is critical for network engineers to have the insight, visibility, and tools to troubleshoot user experience issues. User experience issues can cause loss of productivity and loss of IT credibility. The wealth of information provided in Cisco DNA Center for Application Health from different perspectives enables the network engineer to quickly troubleshoot and remediate user experience issues increasing the business productivity of the organization.

12. Cisco DNA Center Integrations

This chapter will cover some of the key integrations Cisco DNA Center has with other applications to help organizations leverage the strength of all the applications. This helps the network engineer to troubleshoot difficult network issues quickly by leveraging the strength of each application from one single location. This chapter covers integrations with Webex Control Hub, ThousandEyes, and DNA Spaces.

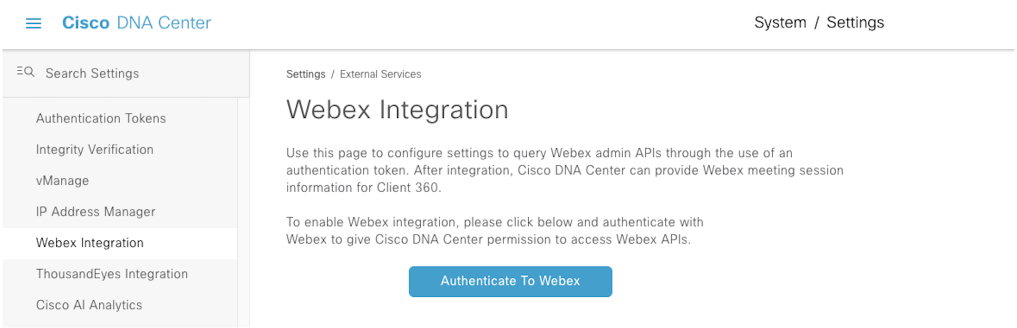
Cisco DNA Center Integration with Webex

Cisco DNA Center integrates with the Webex Control Hub to pull the meeting quality details from the control hub and display it for each client. This enables network engineers to view the Cisco Webex meeting details for a client in a single location and to troubleshoot Cisco Webex meeting issues. The network engineer can see whether the meeting had problems with the voice, video, or the share feature for each meeting. Cisco DNA Center also overlays the information coming from NetFlow, if available, on the same screen so the network engineer can visualize whether the meeting issue was caused by any network anomalies. For Cisco DNA Center to receive NetFlow data on the Webex meetings, the application telemetry needs to be configured on a router or WLC in the path of the Webex traffic. Netflow information and configuration was covered in detail in Chapter 11.

Setting Up Webex Integration

From the main menu of Cisco DNA Center, navigate to the `System > Settings` menu. From there the network engineer can find the `Webex Integration` settings on the left-hand side. Once there, authenticate to Webex Control Hub using the admin account for the Control Hub. Completing this step will set up the integration between Cisco DNA Center and the Webex Control Hub. The integration is a one-time process unless the admin password is changed.

Figure 12.1: Webex 360 Integration

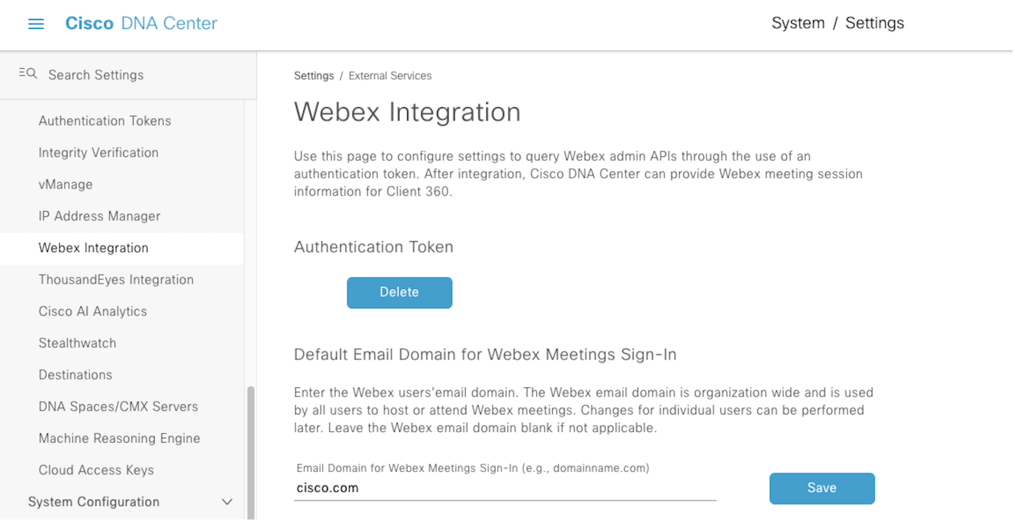


Webex Integration

Use this page to configure settings to query Webex admin APIs through the use of an authentication token. After integration, Cisco DNA Center can provide Webex meeting session information for Client 360.

To enable Webex integration, please click below and authenticate with Webex to give Cisco DNA Center permission to access Webex APIs.

Figure 12.2: Webex 360 Integration



Webex Integration

Use this page to configure settings to query Webex admin APIs through the use of an authentication token. After integration, Cisco DNA Center can provide Webex meeting session information for Client 360.

Authentication Token

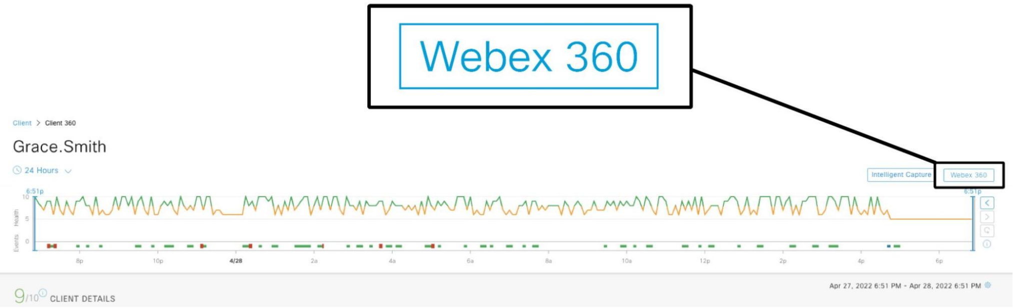
Default Email Domain for Webex Meetings Sign-In

Enter the Webex users'email domain. The Webex email domain is organization wide and is used by all users to host or attend Webex meetings. Changes for individual users can be performed later. Leave the Webex email domain blank if not applicable.

Email Domain for Webex Meetings Sign-In (e.g., domainname.com)
cisco.com

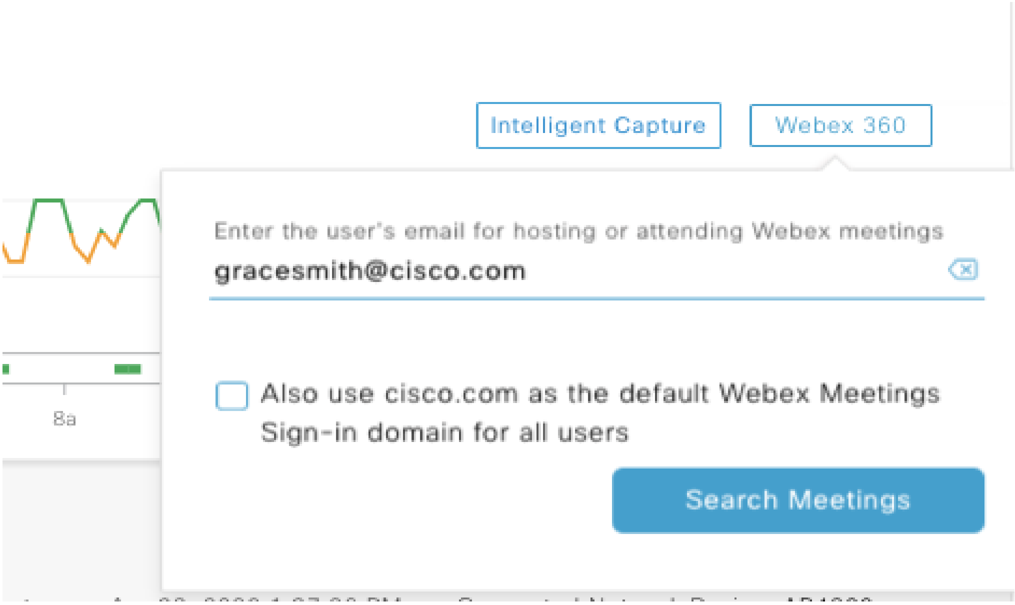
Once the Webex integration is complete, a network engineer can view the meeting quality details for a user, by searching for the user's client device in Cisco DNA Center used to join the Webex meeting. This can be done by searching for the client using the IP Address or username in the Global search box found in the top right corner of every page in Cisco DNA Center. This will pull up the Client 360 page. Now, on the top right corner, the network engineer will see a `Webex 360` button. Selecting that will open up the **Webex 360** page for this client.

Figure 12.3: Client 360 Webex 360 Link



The network engineer has to enter the `user's email address` used to attend the Webex meetings to view the meeting quality details for this user and click `Search Meetings`.

Figure 12.4: Webex 360 Configuration – User Email



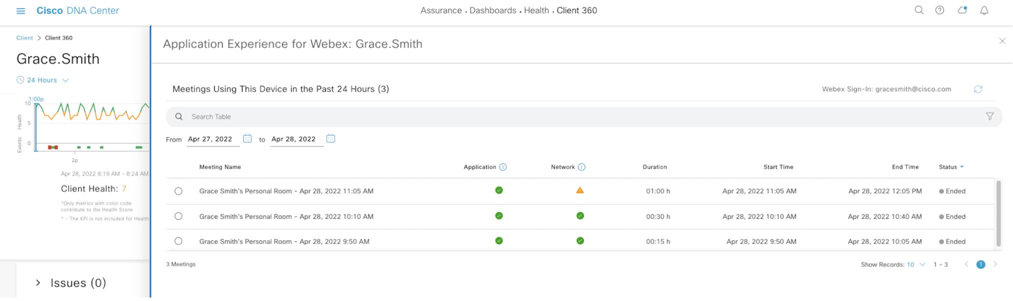
Enter the user's email for hosting or attending Webex meetings

gracesmith@cisco.com

□ Also use cisco.com as the default Webex Meetings Sign-in domain for all users

Once that is done, the Webex 360 page opens up displaying all the user's Webex meetings, as shown below. This information presented comes from the Webex Control Hub via the integration.

Figure 12.5: Webex 360 Application Experience



Cisco DNA Center

Assurance . Dashboards . Health . Client 360

Client > Client 360

Grace.Smith

24 Hours

Apr 28, 2022 8:19 AM - 8:24 AM

Client Health: 7

*Only metrics with color code contribute to the Health Score

* - The KPI is not included for Health

Issues (0)

Application Experience for Webex: Grace.Smith

Meetings Using This Device in the Past 24 Hours (3)

Webex Sign-In: gracesmith@cisco.com

Search Table

From Apr 27, 2022 to Apr 28, 2022

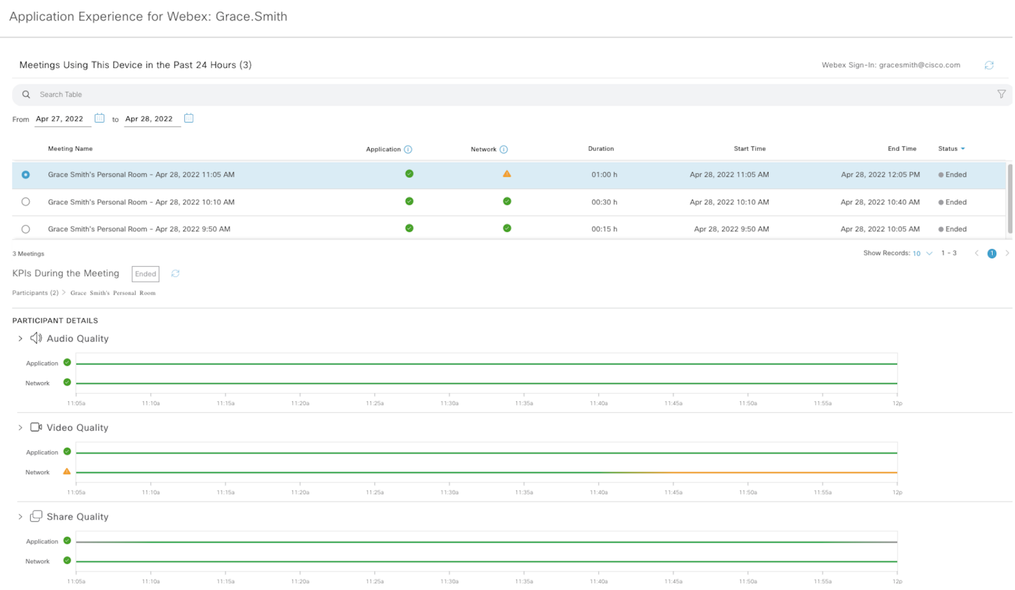
	Meeting Name	Application	Network	Duration	Start Time	End Time	Status
○	Grace Smith's Personal Room - Apr 28, 2022 11:05 AM	✓	⚠	01:00 h	Apr 28, 2022 11:05 AM	Apr 28, 2022 12:05 PM	● Ended
○	Grace Smith's Personal Room - Apr 28, 2022 10:10 AM	✓	✓	00:30 h	Apr 28, 2022 10:10 AM	Apr 28, 2022 10:40 AM	● Ended
○	Grace Smith's Personal Room - Apr 28, 2022 9:50 AM	✓	✓	00:15 h	Apr 28, 2022 9:50 AM	Apr 28, 2022 10:05 AM	● Ended

3 Meetings

Show Records: 10 1 - 3 1

Selecting a `meeting` displays the meeting quality details for voice, video, and the share feature. The network engineer can visualize if there are any issues with any of the components of the meeting.

Figure 12.6 Webex 360 Application Experience



Application Experience for Webex: Grace.Smith

Meetings Using This Device in the Past 24 Hours (3)

Webex Sign-In: gracesmith@cisco.com

Search Table

From Apr 27, 2022 to Apr 28, 2022

	Meeting Name	Application	Network	Duration	Start Time	End Time	Status
●	Grace Smith's Personal Room - Apr 28, 2022 11:05 AM	✓	⚠	01:00 h	Apr 28, 2022 11:05 AM	Apr 28, 2022 12:05 PM	● Ended
○	Grace Smith's Personal Room - Apr 28, 2022 10:10 AM	✓	✓	00:30 h	Apr 28, 2022 10:10 AM	Apr 28, 2022 10:40 AM	● Ended
○	Grace Smith's Personal Room - Apr 28, 2022 9:50 AM	✓	✓	00:15 h	Apr 28, 2022 9:50 AM	Apr 28, 2022 10:05 AM	● Ended

3 Meetings

Show Records: 10 1 - 3

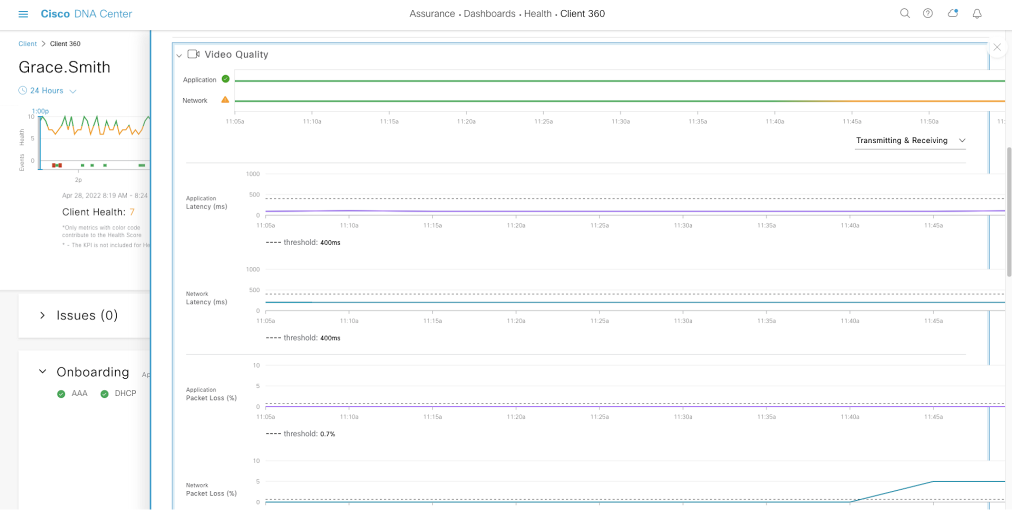
KPIs During the Meeting Ended

Participants (2) > Grace Smith's Personal Room

PARTICIPANT DETAILS

Expanding the `video quality`, for example, breaks down the video quality by latency, packet loss, and jitter. The application part of the graph is the data coming from the Webex Control Hub. The network data is coming via NetFlow and will only show if NetFlow is configured as mentioned earlier in this section.

Figure 12.7: Webex 360 Detailed View



Cisco DNA Center Integration with ThousandEyes

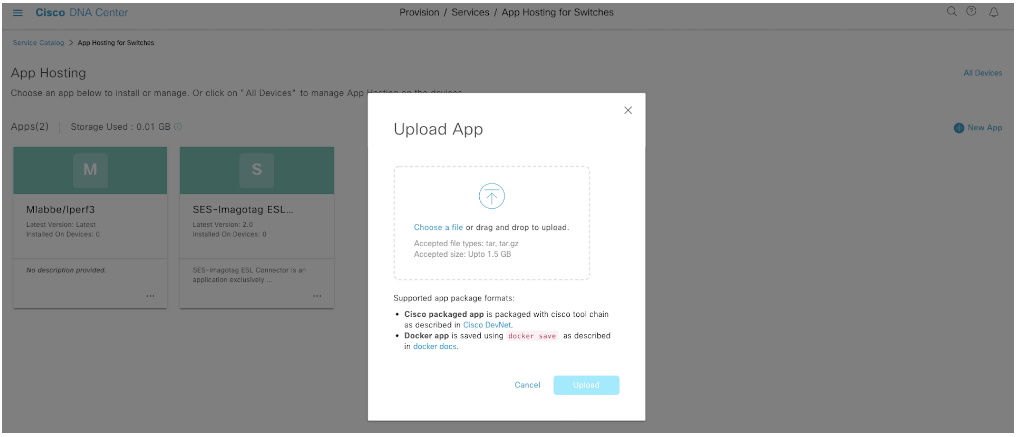
This section will cover the exciting new integration of Cisco DNA Center with ThousandEyes. This provides unparalleled visibility into the application flow through the internet for modern SaaS applications. This allows the network engineer to get to mean time to innocence and identify issue domains for SaaS applications quickly and easily reducing MTTR.

App Hosting on Catalyst 9300 and 9400

Cisco DNA Center makes it easy to deploy the ThousandEyes agent on a Cisco Catalyst 9300 or Cisco Catalyst 9400 switch. The switch-based agents register with the ThousandEyes dashboard, after which the network engineer can configure agent tests from the ThousandEyes dashboard to test various SaaS applications such as Microsoft 365, Salesforce, and any enterprise-specific applications running in the cloud or data center. Without Cisco DNA Center automation, a highly experienced network engineer would be required to apply CLI commands on the switch to deploy the agent. All the work now is automated via Cisco DNA Center, saving time for the network engineer and increasing their efficiency. The network engineer can navigate from the main menu to `Provision > App Hosting for Switches` to start the deployment of the ThousandEyes agent onto a qualified Catalyst switch. The **switch MUST be managed** in Cisco DNA Center before this process can begin.

The network engineer first needs to upload the ThousandEyes agent downloaded from the ThousandEyes site. Selecting the `New App` will open up the upload window where the engineer can upload the agent.

Figure 12.8: ThousandEyes Agent App Hosting



Choose an app below to install or manage. Or click on " All Devices" to manage App Hosting on the devices.

No description provided.

SES-Imagotag ESL Connector is an application exclusively ...

Choose a file or drag and drop to upload.

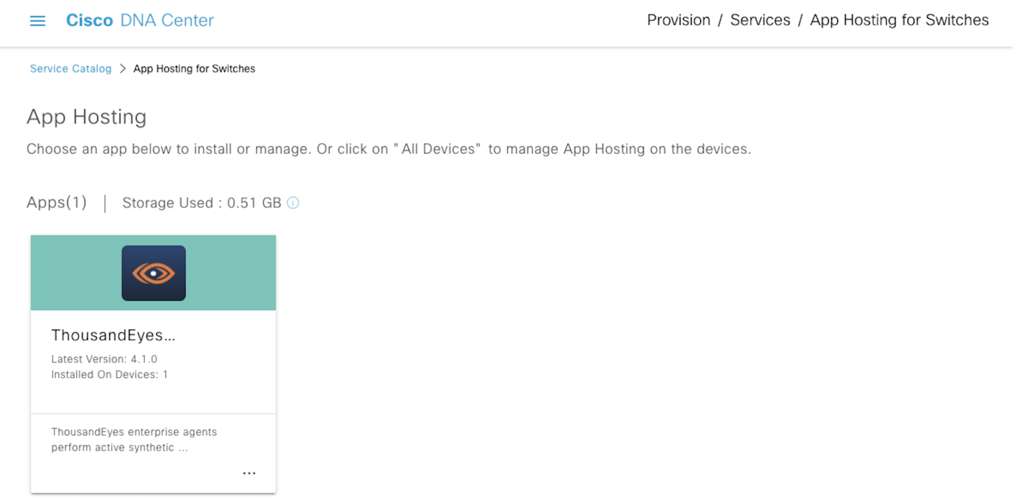
Accepted file types: tar, tar.gz
Accepted size: Upto 1.5 GB

Supported app package formats:

- **Cisco packaged app** is packaged with cisco tool chain as described in Cisco DevNet.
- **Docker app** is saved using `docker save` as described in docker docs.

The network engineer can now select the ThousandEyes card, shown below, to start the agent installation process on a compatible switch.

Figure 12.9: ThousandEyes Agent App Hosting



≡ Cisco DNA Center
Provision / Services / App Hosting for Switches
Service Catalog > App Hosting for Switches

App Hosting

Choose an app below to install or manage. Or click on " All Devices" to manage App Hosting on the devices.

Apps(1) | Storage Used : 0.51 GB ⓘ

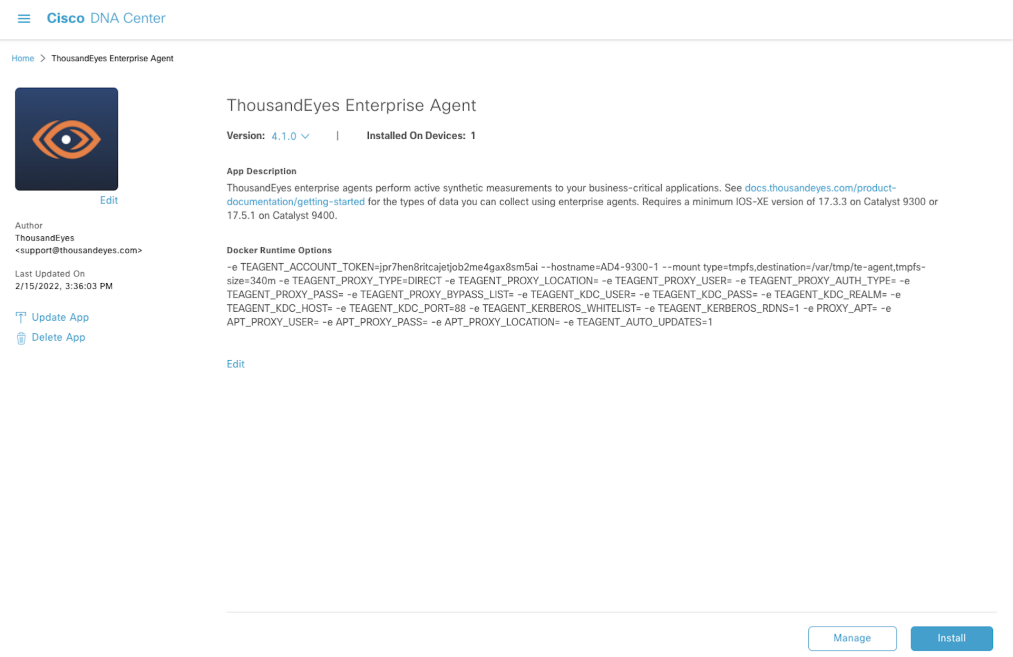
ThousandEyes...

Latest Version: 4.1.0

Installed On Devices: 1

ThousandEyes enterprise agents perform active synthetic ...

Figure 12.10: ThousandEyes Agent App Hosting



ThousandEyes Enterprise Agent

Version: 4.1.0 | **Installed On Devices:** 1

App Description

ThousandEyes enterprise agents perform active synthetic measurements to your business-critical applications. See docs.thousandeyes.com/product-documentation/getting-started for the types of data you can collect using enterprise agents. Requires a minimum IOS-XE version of 17.3.3 on Catalyst 9300 or 17.5.1 on Catalyst 9400.

Docker Runtime Options

```
-e TEAGENT_ACCOUNT_TOKEN=jpr7hen8ritcajetjob2me4gax8sm5ai --hostname=AD4-9300-1 --mount type=tmpfs,destination=/var/tmp/te-agent,tmpfs-size=340m -e TEAGENT_PROXY_TYPE=DIRECT -e TEAGENT_PROXY_LOCATION= -e TEAGENT_PROXY_USER= -e TEAGENT_PROXY_AUTH_TYPE= -e TEAGENT_PROXY_PASS= -e TEAGENT_PROXY_BYPASS_LIST= -e TEAGENT_KDC_USER= -e TEAGENT_KDC_PASS= -e TEAGENT_KDC_REALM= -e TEAGENT_KDC_HOST= -e TEAGENT_KDC_PORT=88 -e TEAGENT_KERBEROS_WHITELIST= -e TEAGENT_KERBEROS_RDNS=1 -e PROXY_APT= -e APT_PROXY_USER= -e APT_PROXY_PASS= -e APT_PROXY_LOCATION= -e TEAGENT_AUTO_UPDATES=1
```

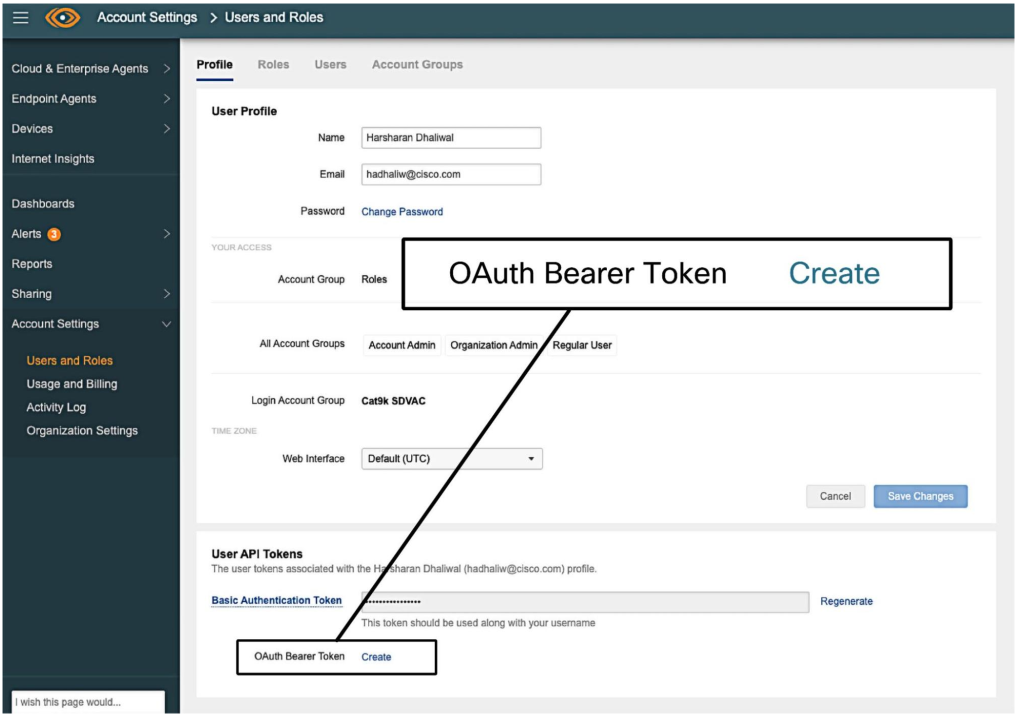
Author
ThousandEyes
<support@thousandeyes.com>

Last Updated On
2/15/2022, 3:36:03 PM

Integrating ThousandEyes with Cisco DNA Center

Once the ThousandEyes Enterprise Agent has been deployed on a Cisco Catalyst 9300 or Cisco Catalyst 9400 switch, an OAuth token must be generated from an active ThousandEyes account. To obtain the OAuth token, log in to an active ThousandEyes account. Use the menu on the left side to navigate to `Account Settings > Users and Roles`. At the bottom of the page click the option to `Create` an OAuth Bearer Token and copy the resulting key.

Figure 12.11: ThousandEyes OAuth Bearer Token



User Profile

Name: Harsharan Dhaliwal

Email: hadhaliw@cisco.com

Password: Change Password

YOUR ACCESS

Account Group	Roles
All Account Groups	Account Admin Organization Admin Regular User

Login Account Group: Cat9k SDVAC

TIME ZONE

Web Interface: Default (UTC)

User API Tokens

The user tokens associated with the Harsharan Dhaliwal (hadhaliw@cisco.com) profile.

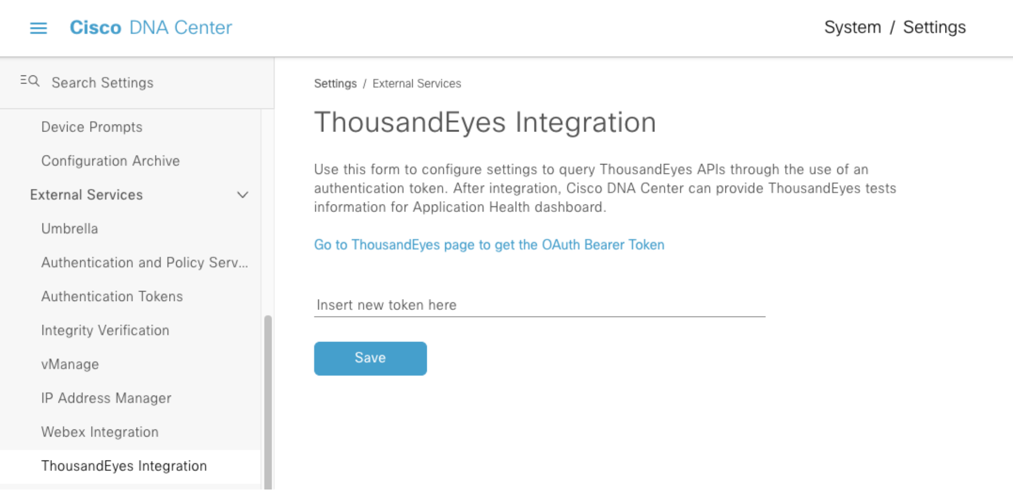
Basic Authentication Token: ....

This token should be used along with your username

OAuth Bearer Token: Create

After copying the token, go to Cisco DNA Center, then navigate to `System > Settings > External Services > ThousandEyes Integration`.

Figure 12.12: Cisco DNA Center ThousandEyes Token



ThousandEyes Integration

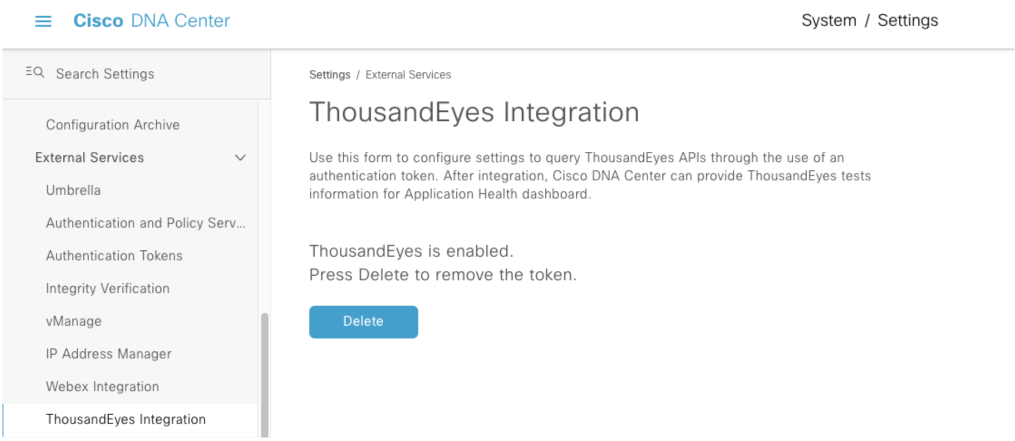
Use this form to configure settings to query ThousandEyes APIs through the use of an authentication token. After integration, Cisco DNA Center can provide ThousandEyes tests information for Application Health dashboard.

Go to ThousandEyes page to get the OAuth Bearer Token

Insert new token here

Paste here the token copied previously, then click `Save`. The page will indicate that ThousandEyes integration is now enabled.

Figure 12.13: ThousandEyes Enabled



ThousandEyes Integration

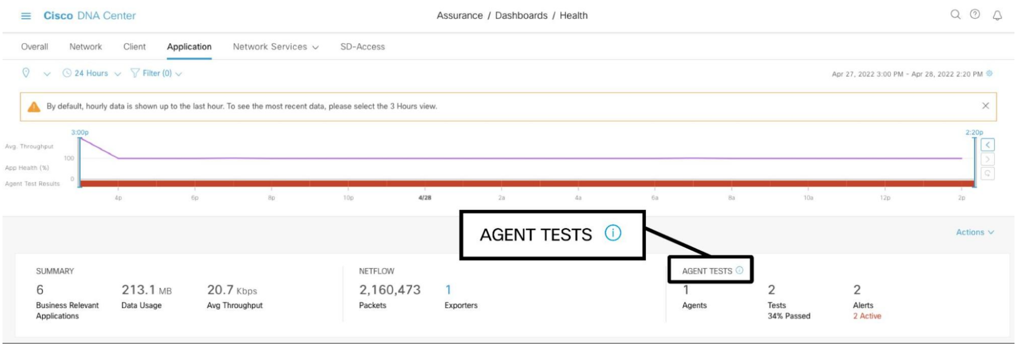
Use this form to configure settings to query ThousandEyes APIs through the use of an authentication token. After integration, Cisco DNA Center can provide ThousandEyes tests information for Application Health dashboard.

ThousandEyes is enabled.
Press Delete to remove the token.

Application Visibility With ThousandEyes

Now that the ThousandEyes integration is enabled, any Agent to Server or HTTP-Server tests created within the ThousandEyes dashboard can be run on the ThousandEyes enterprise agent and/or scheduled to run at regular intervals. All test settings are configured on the **ThousandEyes dashboard**. To view test results within Cisco DNA Center, navigate to `Assurance > Dashboards > Health` from the Cisco DNA Center main menu and then the Application tab. There is a dashlet for ThousandEyes on the right side of the page, indicating the number of active Catalyst 9000 servers ThousandEyes enterprise agents are running, as well as how many tests are being run (along with the percentage of passed tests), and the number of active alerts.

Figure 12.14: ThousandEyes Dashlet

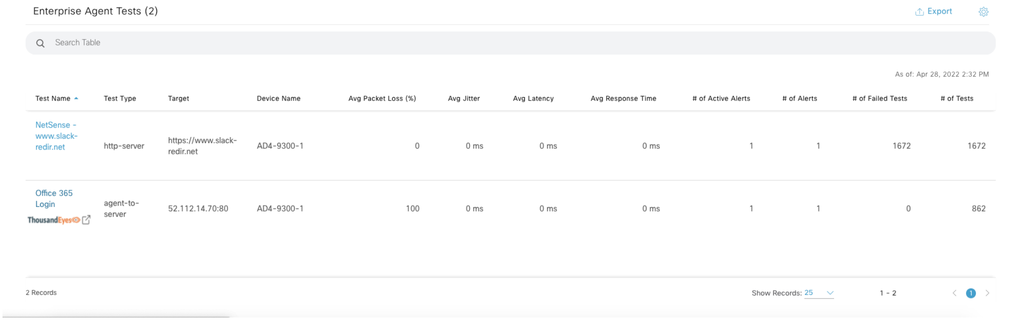


By default, hourly data is shown up to the last hour. To see the most recent data, please select the 3 Hours view.

SUMMARY			NETFLOW		AGENT TESTS		
6 Business Relevant Applications	213.1 MB Data Usage	20.7 Kbps Avg Throughput	2,160,473 Packets	1 Exporters	1 Agents	2 Tests 34% Passed	2 Alerts 2 Active

Scrolling down, there is also a table that shows all of the tests being run, with their respective test statistics, including: jitter, latency, packet loss, and the number of total tests/failed tests.

Figure 12.15: ThousandEyes Enterprise Agent Tests



Enterprise Agent Tests (2)

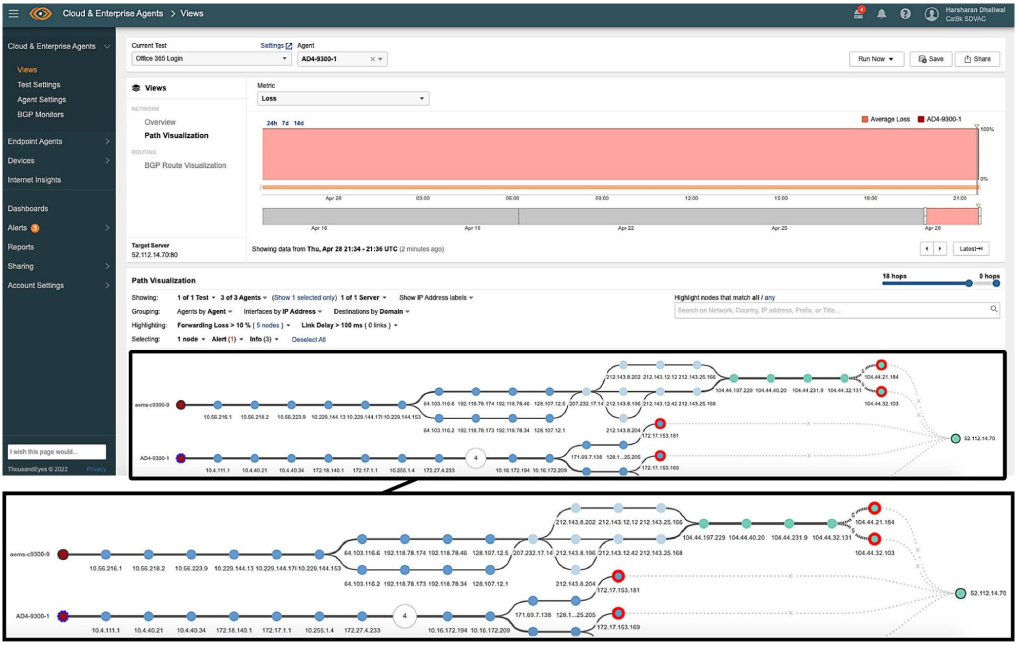
As of: Apr 28, 2022 2:32 PM

Test Name	Test Type	Target	Device Name	Avg Packet Loss (%)	Avg Jitter	Avg Latency	Avg Response Time	# of Active Alerts	# of Alerts	# of Failed Tests	# of Tests
NetSense - www.slack-redir.net	http-server	https://www.slack-redir.net	AD4-9300-1	0	0 ms	0 ms	0 ms	1	1	1672	1672
Office 365 Login ThousandEyes	agent-to-server	52.112.14.70:80	AD4-9300-1	100	0 ms	0 ms	0 ms	1	1	0	862

2 Records   Show Records: 25   1 - 2   1

By clicking the `name` of one of the tests in the table, Cisco DNA Center will cross-launch to the corresponding test within the ThousandEyes dashboard itself. In the ThousandEyes dashboard, all of the test information is available in greater detail and provides more historical testing data. The path from the agent to the target can be visualized to make it quick and efficient to diagnose the issue domain. The network engineer can now identify whether a user's application experience issues are on the client-side, in the enterprise network, or outside of the enterprise network (such as an ISP or in the SaaS provider network).

Figure 12.16: ThousandEyes Dashboard



Current Test: Office 365 Login

Agent: AD4-9300-1

Metric: Loss

Target Server
52.112.14.70:80

Showing data from **Thu, Apr 28 21:34 - 21:36 UTC** (2 minutes ago)

Path Visualization

Showing: 1 of 1 Test ▾ 3 of 3 Agents ▾ (Show 1 selected only) 1 of 1 Server ▾ Show IP Address labels ▾

Grouping: Agents by Agent ▾ Interfaces by IP Address ▾ Destinations by Domain ▾

Highlighting: Forwarding Loss > 10 % (5 nodes) ▾ Link Delay > 100 ms (0 links) ▾

Selecting: 1 node ▾ Alert (1) ▾ Info (3) ▾ Deselect All

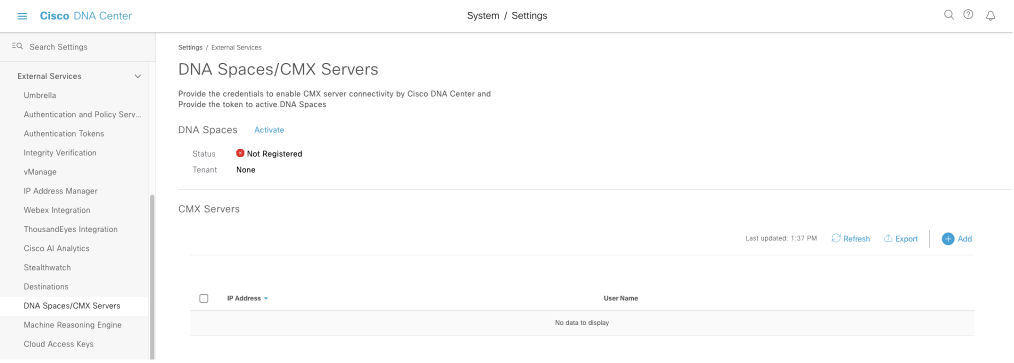
Integration with Cisco DNA Spaces

Cisco DNA Spaces is a location platform that provides highly scalable, reliable, and centralized services for user and device tracking. One significant advantage of Cisco DNA Spaces is its ability to track the location of clients in real time and display their locations in a centralized map view. Previously, a network engineer would need to utilize the dashboards on both Cisco DNA Spaces and Cisco DNA Center to take advantage of the real-time location data as well as the powerful network management capabilities of Cisco DNA Center.

The integration between Cisco DNA Spaces and Cisco DNA Center allows the network engineer to view real-time user locations directly on the floor map shown on Cisco DNA Center. This provides a single, centralized location to view floor maps, assigned networking devices, user locations, as well as RF coverage for wireless access points.

To enable this integration, an active Cisco DNA Spaces instance with a valid license is required. Within Cisco DNA Center, the **DNA Spaces Enabler** package must be installed, which can be downloaded and installed from `System > Software Management` in the Cisco DNA Center main menu. To confirm that the package has been installed, navigate to `System > Settings > External Services > Cisco DNA Spaces/CMX servers.` If the package has been successfully installed, an **Activate** button will be displayed.

Figure 12.17: DNA Spaces Activate



DNA Spaces/CMX Servers

Provide the credentials to enable CMX server connectivity by Cisco DNA Center and Provide the token to active DNA Spaces

DNA Spaces

Status ✖ Not Registered
Tenant None

CMX Servers

□	IP Address	User Name
	No data to display	

To activate the integration, a Cisco DNA Spaces Smart Connector will need to be configured, and an integration token must be generated within Cisco DNA Spaces. For more information on how to configure the Cisco DNA Spaces Smart Connector and generate the integration token, as well as how to add Cisco DNA Spaces sites to Cisco DNA Center, please refer to the **Cisco DNA Spaces Configuration Guide**.

Once the integration token has been generated, click `Activate` in the settings menu above. Paste in the token copied from Cisco DNA Spaces, then click `Connect`. The status of the integration will now show as **Activated** and will display the customer's name.

To utilize this feature, navigate to `Design > Network Hierarchy` from the Cisco DNA Center main menu. Select an individual floor at one of the network sites that was configured for the integration on Cisco DNA Spaces. In addition to the network device and floor map information already provided by Cisco DNA Center, the user locations are also now displayed on the map.

Figure 12.18: Cisco DNA Spaces Integration

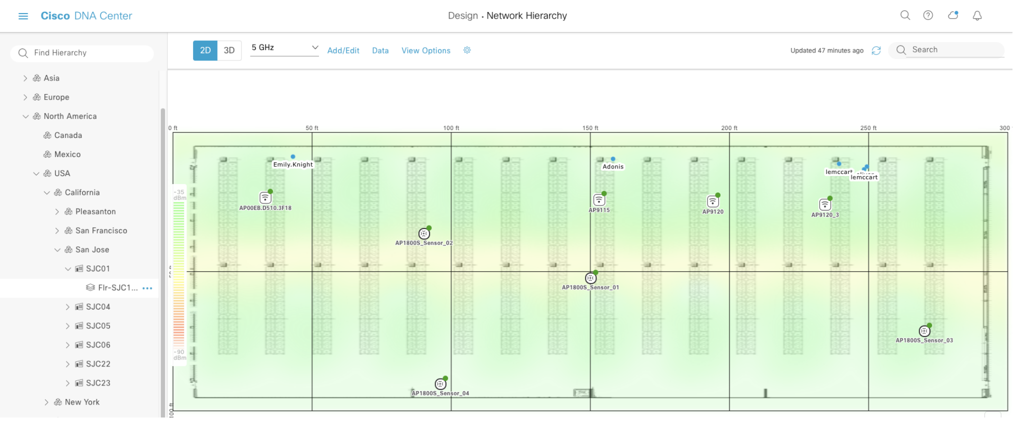
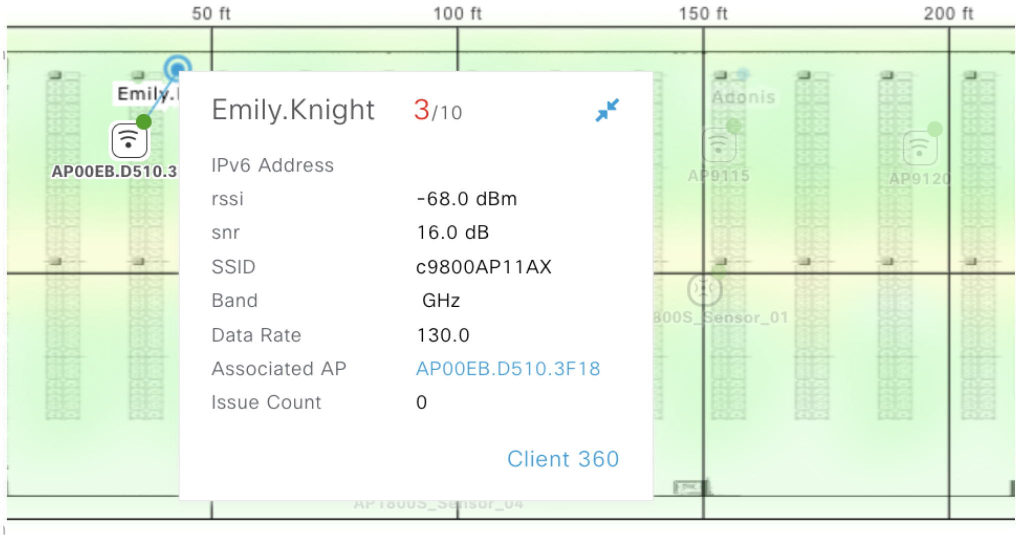


Figure 12.19: Cisco DNA Spaces User Information



Emily.Knight 3/10

IPv6 Address	
rssi	-68.0 dBm
snr	16.0 dB
SSID	c9800AP11AX
Band	GHz
Data Rate	130.0
Associated AP	AP00EB.D510.3F18
Issue Count	0

Client 360

The Cisco DNA Center integrations shown in this chapter demonstrate the flexibility and extendibility of Cisco DNA Center and show how the Integrations are designed to reduce the time to value with Cisco DNA Center. Key integrations empower the network engineer with state-of-the-art tools providing new capabilities and insights into applications and location services. Issues with SaaS applications often took hours to troubleshoot and get to the root cause. With Webex and ThousandEyes, network engineers can significantly reduce the MTTR.

13. Reports

Dashboard

Reports can be used to generate insights into network operations, asset management, uptime reporting, and provide executive summary statements for upper management. Operational reports have historically been used for multitudes of company-required purposes.

Generating Reports

To get to the Reports dashboard from the Cisco DNA Center main menu, select `Reports`.

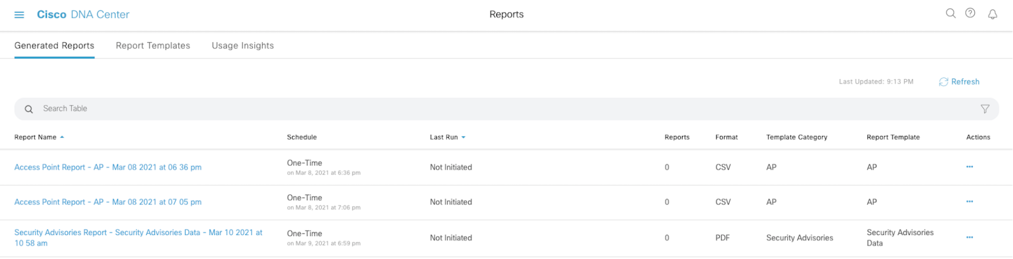
Reports can be run for specified periods and provide views of how the network is evolving. The scheduling feature of the reports allows the network engineer to automate the generation of key reports.

The Reports dashboard is comprised of three tabs:

- Generated Reports
- Report Templates
- Usage Insights

The **Generated Reports** tab displays the basic details of the reports generated previously such as the type of report, schedule, Last Run, and report format. From this tab, it is easy to get reports that have already been generated.

Figure 13.1: Generated Reports

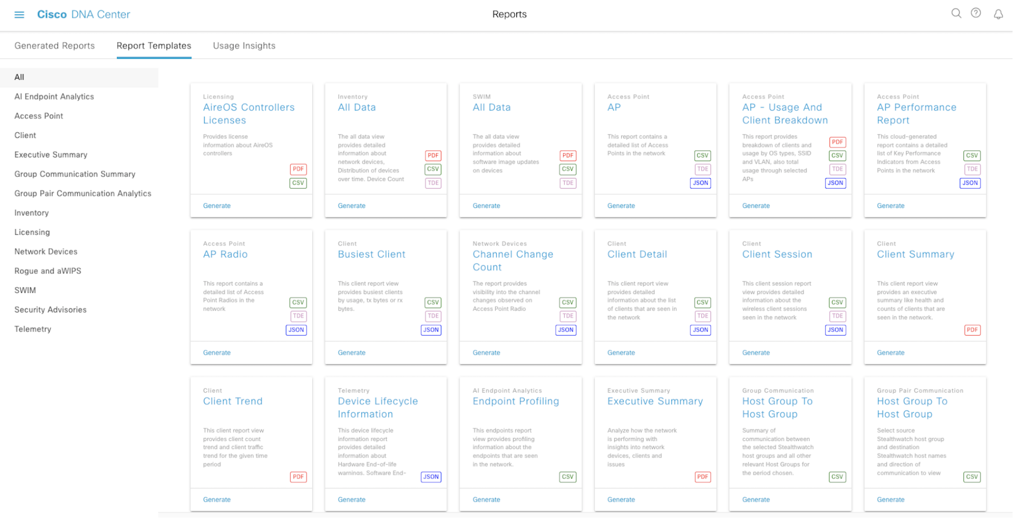


Report Name	Schedule	Last Run	Reports	Format	Template Category	Report Template	Actions
Access Point Report - AP - Mar 08 2021 at 06 36 pm	One-Time on Mar 8, 2021 at 6:36 pm	Not Initiated	0	CSV	AP	AP	•••
Access Point Report - AP - Mar 08 2021 at 07 05 pm	One-Time on Mar 8, 2021 at 7:06 pm	Not Initiated	0	CSV	AP	AP	•••
Security Advisories Report - Security Advisories Data - Mar 10 2021 at 10 58 am	One-Time on Mar 9, 2021 at 6:59 pm	Not Initiated	0	PDF	Security Advisories	Security Advisories Data	•••

The **Report Templates** tab displays all the pre-defined reports that can be generated in Cisco DNA Center. There are more than 36 reports that can be generated across different categories and domains. These report templates make it easy to generate reports as they walk the network engineer through a workflow to build the report parameters.

To get started, select `Generate` at the bottom of the desired report dashlet to start creating a report. The reports can be generated in CSV, PDF, JSON, or Tableau formats. Some reports are available in all formats, but some reports are only provided in limited formats. The formats available for each report template are marked in the **Report Templates** tab as shown in the figure below.

Figure 13.2: Report Templates



Licensing
AireOS Controllers Licenses
Provides license information about AireOS controllers
PDF CSV
Generate

Inventory
All Data
The all data view provides detailed information about network devices, Distribution of devices over time. Device Count
PDF CSV TDE
Generate

SWIM
All Data
The all data view provides detailed information about software image updates on devices
PDF CSV TDE
Generate

Access Point
AP
This report contains a detailed list of Access Points in the network
CSV TDE JSON
Generate

Access Point
AP - Usage And Client Breakdown
This report provides breakdown of clients and usage by OS types, SSID and VLAN, also total usage through selected APs
PDF CSV TDE JSON
Generate

Access Point
AP Performance Report
This cloud-generated report contains a detailed list of Key Performance Indicators from Access Points in the network
CSV TDE JSON
Generate

Access Point
AP Radio
This report contains a detailed list of Access Point Radios in the network
CSV TDE JSON
Generate

Client
Busiest Client
This client report view provides busiest clients by usage, tx bytes or rx bytes.
CSV TDE JSON
Generate

Network Devices
Channel Change Count
The report provides visibility into the channel changes observed on Access Point Radio
CSV TDE JSON
Generate

Client
Client Detail
This client report view provides detailed information about the list of clients that are seen in the network
CSV TDE JSON
Generate

Client
Client Session
This client session report view provides detailed information about the wireless client sessions seen in the network
CSV TDE JSON
Generate

Client
Client Summary
This client report view provides an executive summary like health and counts of clients that are seen in the network.
PDF
Generate

Client
Client Trend
This client report view provides client count trend and client traffic trend for the given time period
PDF
Generate

Telemetry
Device Lifecycle Information
This device lifecycle information report provides detailed information about Hardware End-of-life warnings. Software End-
JSON
Generate

AI Endpoint Analytics
Endpoint Profiling
This endpoints report view provides profiling information about the endpoints that are seen in the network.
CSV
Generate

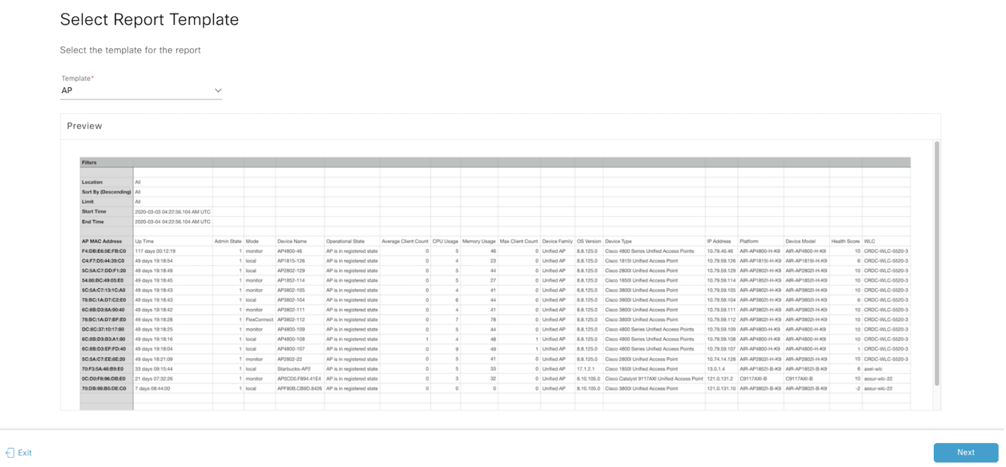
Executive Summary
Executive Summary
Analyze how the network is performing with insights into network devices, clients and issues
PDF
Generate

Group Communication
Host Group To Host Group
Summary of communication between the selected Stealthwatch host groups and all other relevant Host Groups for the period chosen.
CSV
Generate

Group Pair Communication
Host Group To Host Group
Select source Stealthwatch host group and destination Stealthwatch host names and direction of communication to view
CSV
Generate

When the `Generate` report option is selected, the network engineer is presented with a reporting workflow. The first part of the workflow as shown below displays the template being used for the report and a preview of a report sample. The `Next` button takes the network engineer to the next part of the workflow.

Figure 13.3: Report Template Selection



Select Report Template

Select the template for the report

Template*
AP

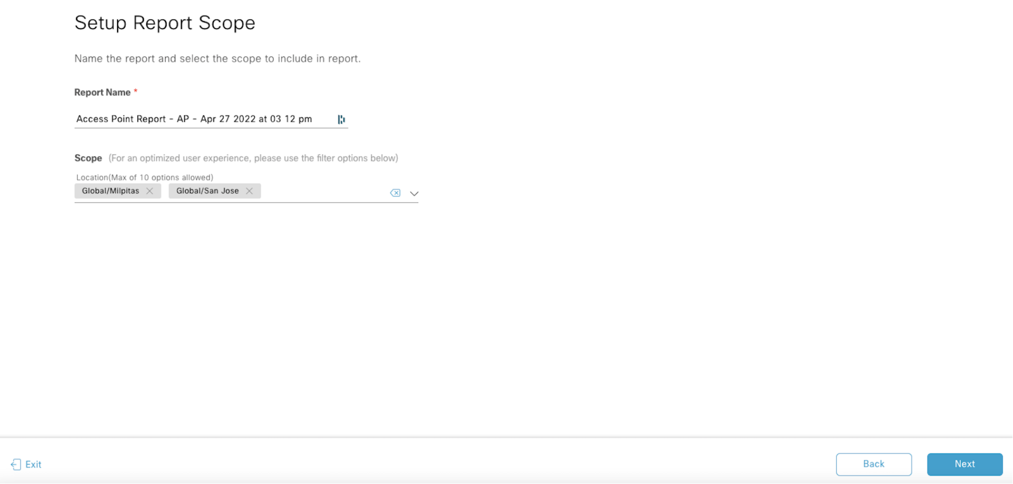
Preview

Filters	
Location	All
Sort By (Descending)	All
Limit	All
Start Time	2020-03-03 04:22:56.104 AM UTC
End Time	2020-03-04 04:22:56.104 AM UTC

AP MAC Address	Up Time	Admin State	Mode	Device Name	Operational State	Average Client Count	CPU Usage	Memory Usage	Max Client Count	Device Family	OS Version	Device Type	IP Address	Platform	Device Model	Health Score	WLC
F4:DB:E6:5E:FB:C0	117 days 00:12:19	1	monitor	AP4800-46	AP is in registered state	0	5	46	0	Unified AP	8.8.125.0	Cisco 4800 Series Unified Access Points	10.79.46.46	AIR-AP4800-H-K9	AIR-AP4800-H-K9	10	CRDC-WLC-5520-3
C4:F7:D5:44:39:C0	49 days 19:18:54	1	local	AP1815-126	AP is in registered state	0	4	23	0	Unified AP	8.8.125.0	Cisco 1815I Unified Access Point	10.79.59.126	AIR-AP1815I-H-K9	AIR-AP1815I-H-K9	6	CRDC-WLC-5520-3
5C:5A:C7:DD:F1:20	49 days 19:18:49	1	local	AP2802-129	AP is in registered state	0	5	44	0	Unified AP	8.8.125.0	Cisco 2800I Unified Access Point	10.79.59.129	AIR-AP2802I-H-K9	AIR-AP2802I-H-K9	10	CRDC-WLC-5520-3
54:86:BC:49:05:E0	49 days 19:18:45	1	monitor	AP1852-114	AP is in registered state	0	5	27	0	Unified AP	8.8.125.0	Cisco 1850I Unified Access Point	10.79.59.114	AIR-AP1852I-H-K9	AIR-AP1852I-H-K9	10	CRDC-WLC-5520-3
5C:5A:C7:13:1C:A0	49 days 19:18:43	1	monitor	AP3802-105	AP is in registered state	0	4	41	0	Unified AP	8.8.125.0	Cisco 3800I Unified Access Point	10.79.59.105	AIR-AP3802I-H-K9	AIR-AP3802I-H-K9	10	CRDC-WLC-5520-3
78:BC:1A:D7:C2:E0	49 days 19:18:43	1	local	AP3802-104	AP is in registered state	0	6	44	0	Unified AP	8.8.125.0	Cisco 3800I Unified Access Point	10.79.59.104	AIR-AP3802I-H-K9	AIR-AP3802I-H-K9	6	CRDC-WLC-5520-3
6C:8B:D3:8A:90:40	49 days 19:18:42	1	monitor	AP3802-111	AP is in registered state	0	4	41	0	Unified AP	8.8.125.0	Cisco 3800I Unified Access Point	10.79.59.111	AIR-AP3802I-H-K9	AIR-AP3802I-H-K9	10	CRDC-WLC-5520-3
78:BC:1A:D7:BF:E0	49 days 19:18:28	1	FlexConnect	AP3802-112	AP is in registered state	0	7	78	0	Unified AP	8.8.125.0	Cisco 3800I Unified Access Point	10.79.59.112	AIR-AP3802I-H-K9	AIR-AP3802I-H-K9	10	CRDC-WLC-5520-3
DC:8C:37:10:17:80	49 days 19:18:25	1	monitor	AP4800-109	AP is in registered state	0	5	44	0	Unified AP	8.8.125.0	Cisco 4800 Series Unified Access Points	10.79.59.109	AIR-AP4800-H-K9	AIR-AP4800-H-K9	10	CRDC-WLC-5520-3
6C:8B:D3:B3:A1:80	49 days 19:18:16	1	local	AP4800-108	AP is in registered state	1	4	48	1	Unified AP	8.8.125.0	Cisco 4800 Series Unified Access Points	10.79.59.108	AIR-AP4800-H-K9	AIR-AP4800-H-K9	10	CRDC-WLC-5520-3
6C:8B:D3:EF:FD:40	49 days 19:18:04	1	local	AP4800-107	AP is in registered state	0	9	49	1	Unified AP	8.8.125.0	Cisco 4800 Series Unified Access Points	10.79.59.107	AIR-AP4800-H-K9	AIR-AP4800-H-K9	1	CRDC-WLC-5520-3
5C:5A:C7:EE:8E:20	49 days 18:21:09	1	monitor	AP2802-22	AP is in registered state	0	5	41	0	Unified AP	8.8.125.0	Cisco 2800I Unified Access Point	10.74.14.128	AIR-AP2802I-H-K9	AIR-AP2802I-H-K9	10	CRDC-WLC-5520-3
70:F3:5A:46:B9:E0	33 days 09:15:44	1	local	Starbucks-AP2	AP is in registered state	0	5	33	0	Unified AP	17.1.2.1	Cisco 1850I Unified Access Point	13.0.1.4	AIR-AP1852I-B-K9	AIR-AP1852I-B-K9	6	axel-wlc
0C:D0:F8:96:DB:E0	21 days 07:32:26	1	monitor	AP0CD0.F894.41E4	AP is in registered state	0	3	32	0	Unified AP	8.10.105.0	Cisco Catalyst 9117AXI Unified Access Point	121.0.131.2	C9117AXI-B	C9117AXI-B	10	assur-wlc-22
70:DB:98:B5:DE:C0	7 days 08:44:00	1	local	APF80B.CB9D.8426	AP is in registered state	0	0	0	0	Unified AP	8.10.105.0	Cisco 3800I Unified Access Point	121.0.131.10	AIR-AP3802I-B-K9	AIR-AP3802I-B-K9	-2	assur-wlc-22

The next step of the workflow is where the network engineer can change the report name and set up the scope of the report. The report name field is filled in with a default name which includes the report type, date, and time. The network engineer can change this to a more meaningful name. For example, in this **AP report, the Location** needs to be selected in the scope. Depending on the report type, the scope options will vary.

Figure 13.4: Report Scope Selection



Setup Report Scope

Name the report and select the scope to include in report.

Report Name *

Access Point Report - AP - Apr 27 2022 at 03 12 pm

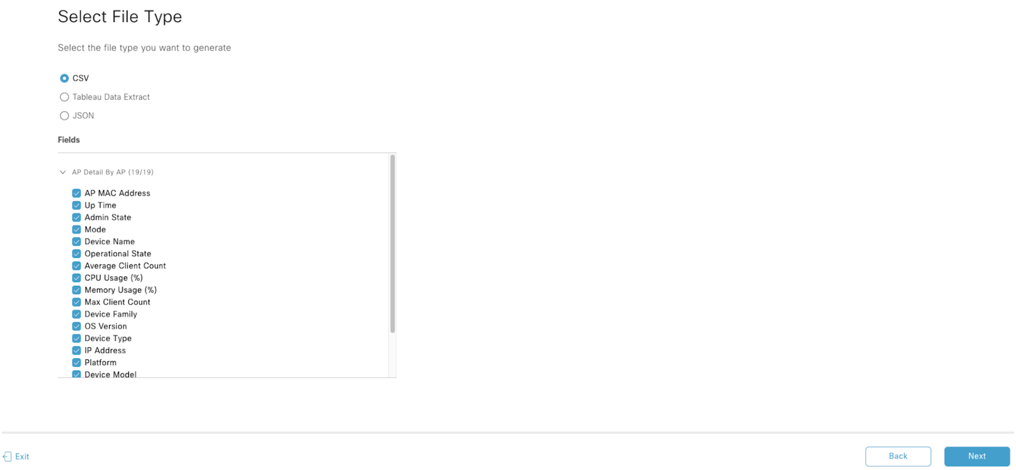
Scope (For an optimized user experience, please use the filter options below)

Location(Max of 10 options allowed)

Global/Milpitas ×   Global/San Jose ×

The next step is where the network engineer can select the File Type for the report such as CSV, PDF, or Tableau and also customize the fields needed to go into the report. By default, all fields are selected.

Figure 13.5: File Type Selection



Select File Type

Select the file type you want to generate

● CSV
○ Tableau Data Extract
○ JSON

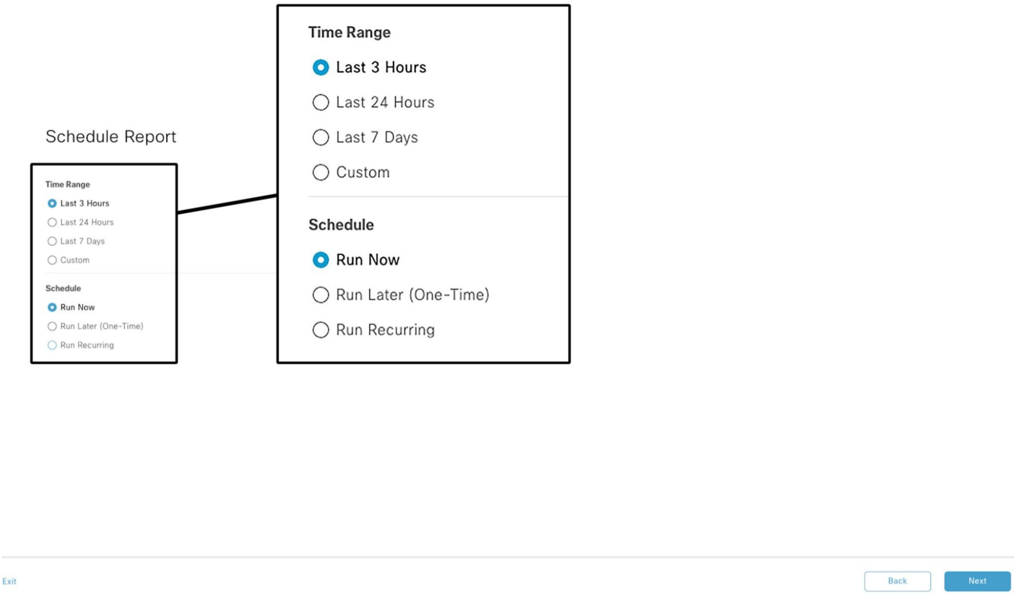
Fields

AP Detail By AP (19/19)

- ☑ AP MAC Address
- ☑ Up Time
- ☑ Admin State
- ☑ Mode
- ☑ Device Name
- ☑ Operational State
- ☑ Average Client Count
- ☑ CPU Usage (%)
- ☑ Memory Usage (%)
- ☑ Max Client Count
- ☑ Device Family
- ☑ OS Version
- ☑ Device Type
- ☑ IP Address
- ☑ Platform
- ☑ Device Model

In the next step, the network engineer can select the Time Range and Schedule for the report which provides multiple options. The Time Range provides predefined time intervals such as 3 hours, 24 hours, and 7 days. The custom Time Range option can be used to select a time range up to 6 months back. The schedule options are Run Now, Run Later, or Run Recurring.

Figure 13.6: Report Schedule Time Selection



Schedule Report

Time Range

● Last 3 Hours

○ Last 24 Hours

○ Last 7 Days

○ Custom

Schedule

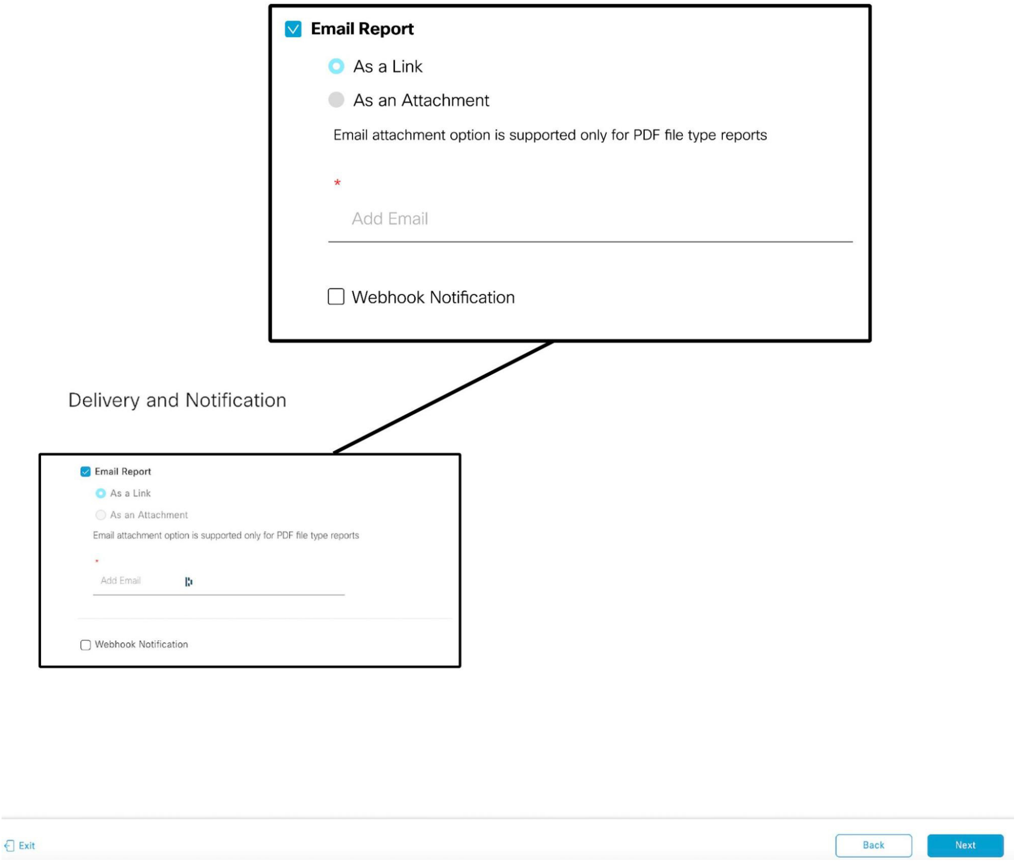
● Run Now

○ Run Later (One-Time)

○ Run Recurring

Next, the network engineer can select the delivery options for the report such as email and webhook. The reports are also available on the Cisco DNA Center Generated Reports page so the **Delivery and Notification** step can be skipped.

Figure 13.7: Report Delivery and Notification



Delivery and Notification

☑ Email Report

● As a Link

○ As an Attachment

Email attachment option is supported only for PDF file type reports

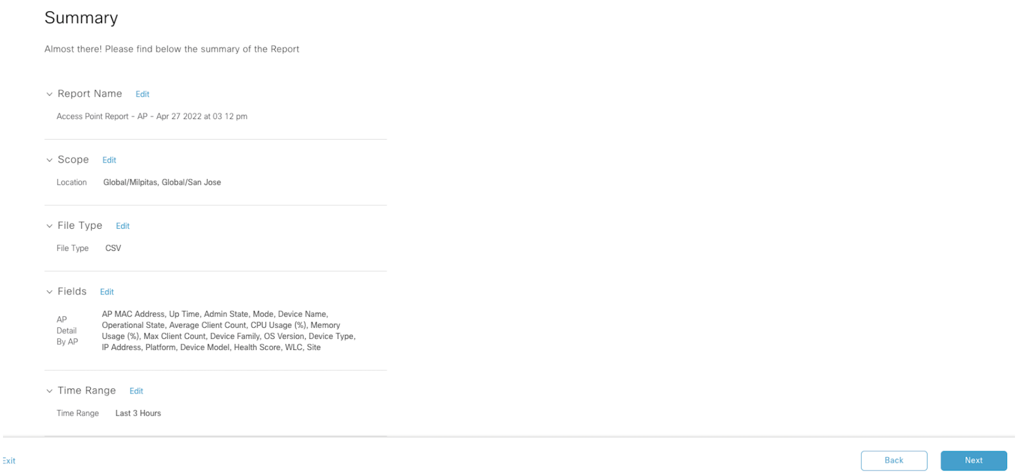
*

Add Email

□ Webhook Notification

Lastly, the network engineer is presented with the summary of the report options selected. The network engineer can select `Next` to generate the report or go `Back` and change any options if required.

Figure 13.8: Report Summary



Summary

Almost there! Please find below the summary of the Report

Report Name

Access Point Report - AP - Apr 27 2022 at 03 12 pm

Scope

Location: Global/Milpitas, Global/San Jose

File Type

File Type: CSV

Fields

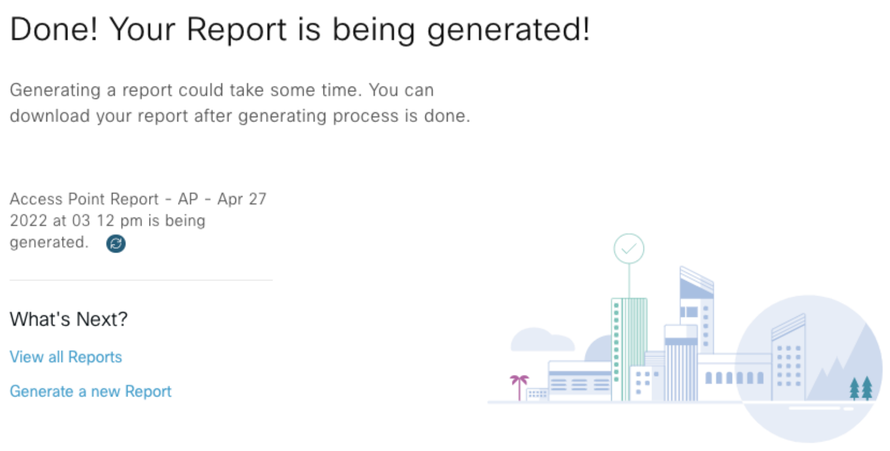
AP Detail By AP: AP MAC Address, Up Time, Admin State, Mode, Device Name, Operational State, Average Client Count, CPU Usage (%), Memory Usage (%), Max Client Count, Device Family, OS Version, Device Type, IP Address, Platform, Device Model, Health Score, WLC, Site

Time Range

Time Range: Last 3 Hours

Selecting `View All Reports` will take the network engineer to the **Generated Reports** tab. Depending on the type of report and the amount of data in the report, the time taken to generate the report will vary. As some reports will take a longer time to generate, it is safe to keep using Cisco DNA Center while the report generates in the background.

Figure 13.9: Completed Report Generation



Done! Your Report is being generated!

Generating a report could take some time. You can download your report after generating process is done.

Access Point Report - AP - Apr 27 2022 at 03 12 pm is being generated.

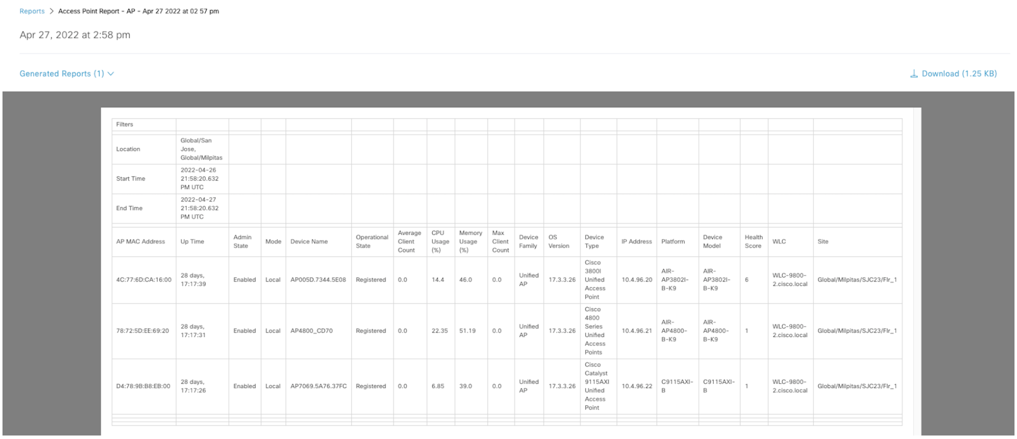
What's Next?

View all Reports

Generate a new Report

The network engineer can select the `Report Title` to view the report directly in Cisco DNA Center. They can also download the report using the download link. If they had chosen a delivery option such as email or webhook, the report will be delivered to those destinations as well.

Figure 13.10: View Generated Reports



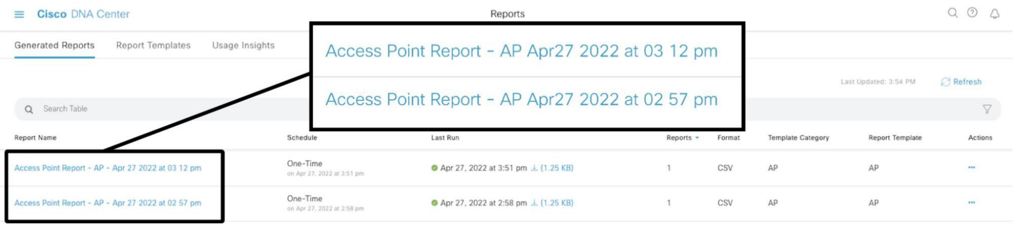
Reports > Access Point Report - AP - Apr 27 2022 at 02 57 pm

Apr 27, 2022 at 2:58 pm

Generated Reports (1)
Download (1.25 KB)

Filters	
Location	Global/San Jose, Global/Milpitas
Start Time	2022-04-26 21:58:20.632 PM UTC
End Time	2022-04-27 21:58:20.632 PM UTC

AP MAC Address	Up Time	Admin State	Mode	Device Name	Operational State	Average Client Count	CPU Usage (%)	Memory Usage (%)	Max Client Count	Device Family	OS Version	Device Type	IP Address	Platform	Device Model	Health Score	WLC	Site
4C:77:6D:CA:16:00	28 days, 17:17:39	Enabled	Local	AP005D.7344.5E08	Registered	0.0	14.4	46.0	0.0	Unified AP	17.3.3.26	Cisco 3800I Unified Access Point	10.4.96.20	AIR-AP3802I-B-K9	AIR-AP3802I-B-K9	6	WLC-9800-2.cisco.local	Global/Milpitas/SJC23/Flr_1
78:72:5D:EE:69:20	28 days, 17:17:31	Enabled	Local	AP4800_CD70	Registered	0.0	22.35	51.19	0.0	Unified AP	17.3.3.26	Cisco 4800 Series Unified Access Points	10.4.96.21	AIR-AP4800-B-K9	AIR-AP4800-B-K9	1	WLC-9800-2.cisco.local	Global/Milpitas/SJC23/Flr_1
D4:78:9B:B8:EB:00	28 days, 17:17:26	Enabled	Local	AP7069.5A76.37FC	Registered	0.0	6.85	39.0	0.0	Unified AP	17.3.3.26	Cisco Catalyst 9115AXI Unified Access Point	10.4.96.22	C9115AXI-B	C9115AXI-B	1	WLC-9800-2.cisco.local	Global/Milpitas/SJC23/Flr_1



Access Point Report - AP Apr27 2022 at 03 12 pm

Access Point Report - AP Apr27 2022 at 02 57 pm

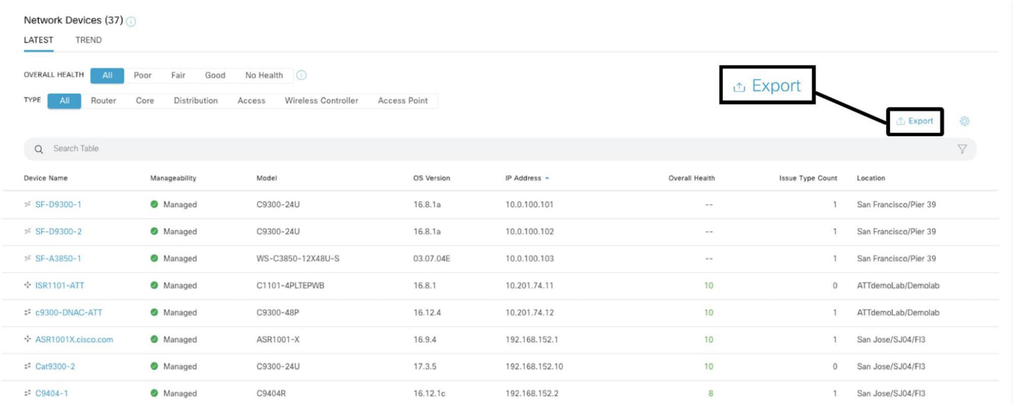
Report Name	Schedule	Last Run	Reports	Format	Template Category	Report Template	Actions
Access Point Report - AP - Apr 27 2022 at 03 12 pm	One-Time on Apr 27, 2022 at 3:51 pm	● Apr 27, 2022 at 3:51 pm (1.25 KB)	1	CSV	AP	AP	···
Access Point Report - AP - Apr 27 2022 at 02 57 pm	One-Time on Apr 27, 2022 at 2:58 pm	● Apr 27, 2022 at 2:58 pm (1.25 KB)	1	CSV	AP	AP	···

Ad-Hoc CSV Reports

CSV Reports can be generated from the Cisco DNA Center GUI. CSV format is not available in all dashlets. However, this option can be used to create reports quickly from GUI list views. The network engineer can customize the list views. For example, in the network devices table in the Network Health Dashboard, the table can be customized by adding columns that are relevant to the network engineer. Columns can be removed as well.

As can be seen in the image below, in the Network Devices table in the **Network Health** dashboard there is an `export` button on the top right corner which can be used to generate a CSV report on all the network devices. Anywhere a network engineer sees a similar export button they can generate the reports for that section.

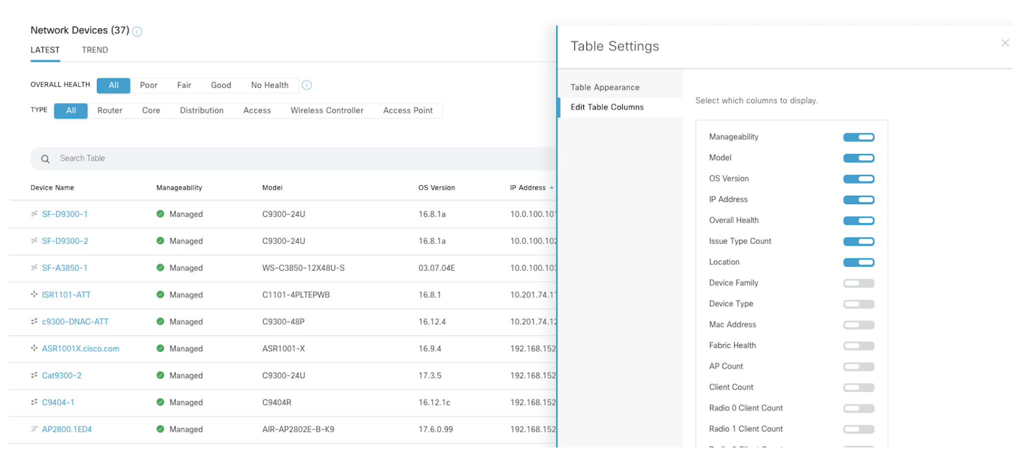
Figure 13.11: Export Based Reports



Device Name	Manageability	Model	OS Version	IP Address	Overall Health	Issue Type Count	Location
SF-D9300-1	Managed	C9300-24U	16.8.1a	10.0.100.101	--	1	San Francisco/Pier 39
SF-D9300-2	Managed	C9300-24U	16.8.1a	10.0.100.102	--	1	San Francisco/Pier 39
SF-A3850-1	Managed	WS-C3850-12X48U-S	03.07.04E	10.0.100.103	--	1	San Francisco/Pier 39
ISR1101-ATT	Managed	C1101-4PLTEPWB	16.8.1	10.201.74.11	10	0	ATTdemoLab/Demolab
c9300-DNAC-ATT	Managed	C9300-48P	16.12.4	10.201.74.12	10	1	ATTdemoLab/Demolab
ASR1001X.cisco.com	Managed	ASR1001-X	16.9.4	192.168.152.1	10	1	San Jose/SJ04/FI3
Cat9300-2	Managed	C9300-24U	17.3.5	192.168.152.10	10	0	San Jose/SJ04/FI3
C9404-1	Managed	C9404R	16.12.1c	192.168.152.2	8	1	San Jose/SJ04/FI3

The network engineer can customize the dynamic reports and add or remove columns that will be included in the report as seen in the figure below.

Figure 13.12: Add Remove Column To Export-Based Reports



Network Devices (37)

LATEST TREND

OVERALL HEALTH: All | Poor | Fair | Good | No Health

TYPE: All | Router | Core | Distribution | Access | Wireless Controller | Access Point

Search Table

Device Name	Manageability	Model	OS Version	IP Address
SF-D9300-1	● Managed	C9300-24U	16.8.1a	10.0.100.101
SF-D9300-2	● Managed	C9300-24U	16.8.1a	10.0.100.102
SF-A3850-1	● Managed	WS-C3850-12X48U-S	03.07.04E	10.0.100.103
ISR1101-ATT	● Managed	C1101-4PLTEPWB	16.8.1	10.201.74.11
c9300-DNAC-ATT	● Managed	C9300-48P	16.12.4	10.201.74.12
ASR1001X.cisco.com	● Managed	ASR1001-X	16.9.4	192.168.152
Cat9300-2	● Managed	C9300-24U	17.3.5	192.168.152
C9404-1	● Managed	C9404R	16.12.1c	192.168.152
AP2800.1ED4	● Managed	AIR-AP2802E-B-K9	17.6.0.99	192.168.152

Table Settings

Table Appearance

Edit Table Columns

Select which columns to display.

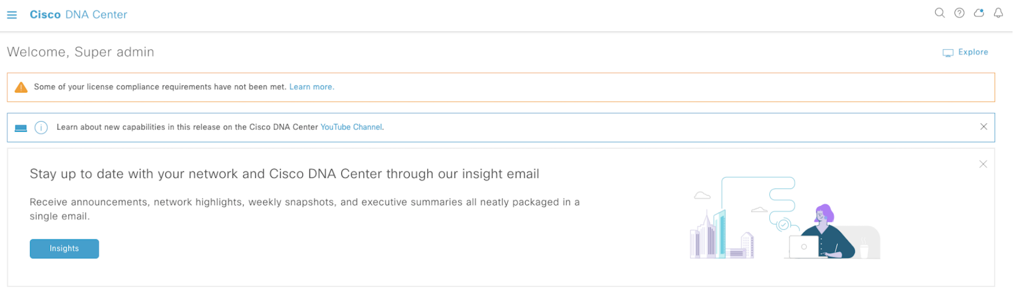
Manageability	●
Model	●
OS Version	●
IP Address	●
Overall Health	●
Issue Type Count	●
Location	●
Device Family	○
Device Type	○
Mac Address	○
Fabric Health	○
AP Count	○
Client Count	○
Radio 0 Client Count	○
Radio 1 Client Count	○

Weekly Insights Report

Network engineers or managers can now get weekly insight reporting from Cisco DNA Center. The main page of Cisco DNA Center has the Insights email feature. This allows network engineers or network managers to set up a weekly email that they will receive containing key insights on the network from Cisco DNA Center. The email will have new product announcements, network insights, and an executive summary. The executive summary part of the email will contain information about measurable time and cost savings realized from using Cisco DNA Center to manage the network infrastructure.

Selecting the `Insights` button will take the network engineer to a setup page to customize the insights email.

Figure 13.13: Weekly Insights Report



Welcome, Super admin

Some of your license compliance requirements have not been met. Learn more.

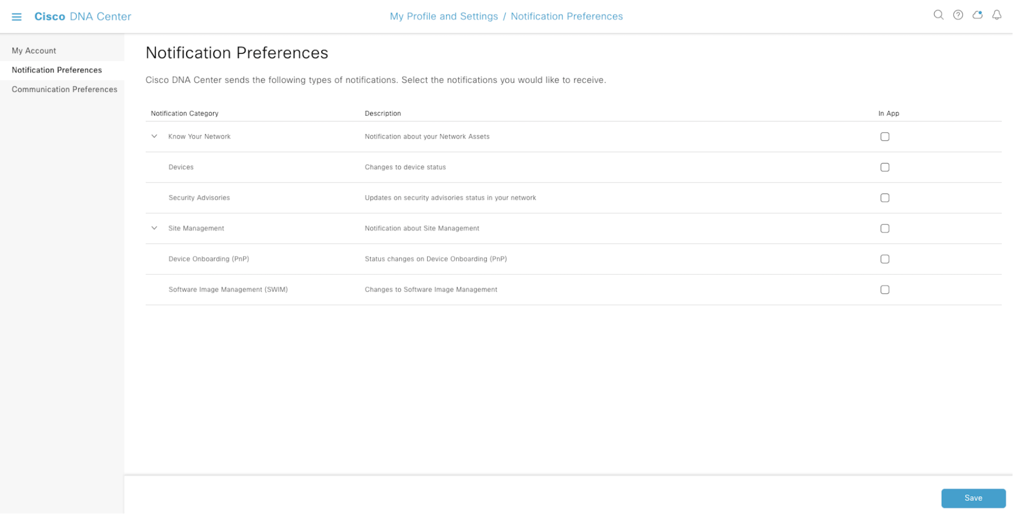
Learn about new capabilities in this release on the Cisco DNA Center YouTube Channel.

Stay up to date with your network and Cisco DNA Center through our insight email

Receive announcements, network highlights, weekly snapshots, and executive summaries all neatly packaged in a single email.

The Notification preferences can be used to select the information the network engineer wants to see in the weekly insights email.

Figure 13.14: Weekly Insights Report Notification Preferences



Cisco DNA Center
My Profile and Settings / Notification Preferences
My Account
Notification Preferences
Communication Preferences

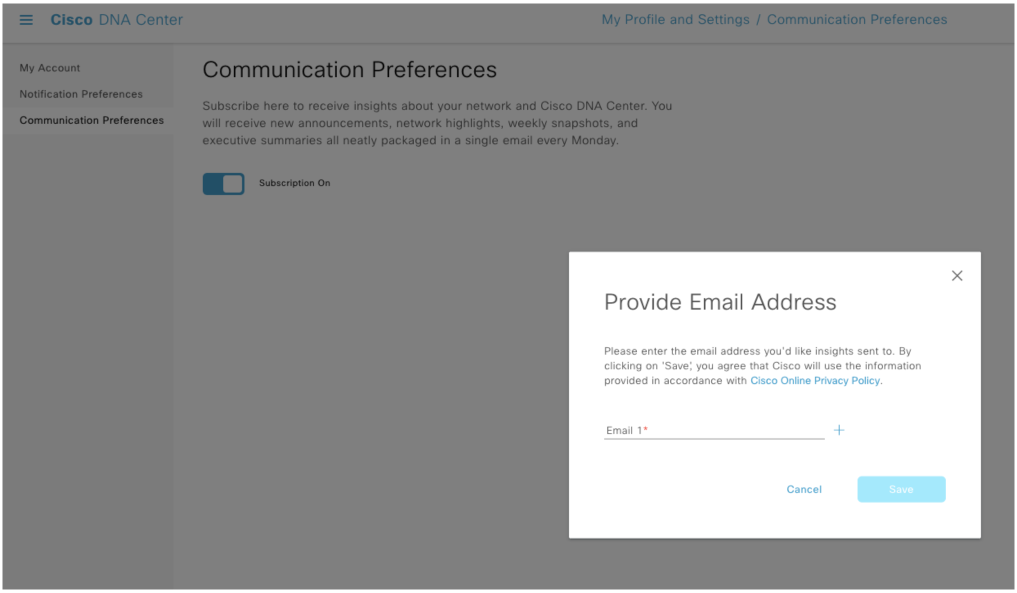
Notification Preferences

Cisco DNA Center sends the following types of notifications. Select the notifications you would like to receive.

Notification Category	Description	In App
Know Your Network	Notification about your Network Assets	□
Devices	Changes to device status	□
Security Advisories	Updates on security advisories status in your network	□
Site Management	Notification about Site Management	□
Device Onboarding (PnP)	Status changes on Device Onboarding (PnP)	□
Software Image Management (SWIM)	Changes to Software Image Management	□

The communication preferences page allows the network engineer or administrator to configure and distribute weekly insight reports. The SMTP server information needs to be configured in the `System > Settings` page of Cisco DNA Center for the system to be able to send emails.

Figure 13.15: Weekly Insights Report Communication Preferences


≡ Cisco DNA Center
My Profile and Settings / Communication Preferences
My Account
Notification Preferences
Communication Preferences

Communication Preferences

Subscribe here to receive insights about your network and Cisco DNA Center. You will receive new announcements, network highlights, weekly snapshots, and executive summaries all neatly packaged in a single email every Monday.

Subscription On

Provide Email Address

Please enter the email address you'd like insights sent to. By clicking on 'Save', you agree that Cisco will use the information provided in accordance with Cisco Online Privacy Policy.

Email 1*

Reporting is a key part of any administrative system. Cisco DNA Center reporting was designed to be intuitive and flexible. Using the templated reports organizations should be able to track assets, review network compliance, assess the state of the network, and perform capacity planning activities. New reports and reporting capabilities are added with every new Cisco DNA Center release.

14. Cisco DNA Center Server Troubleshooting

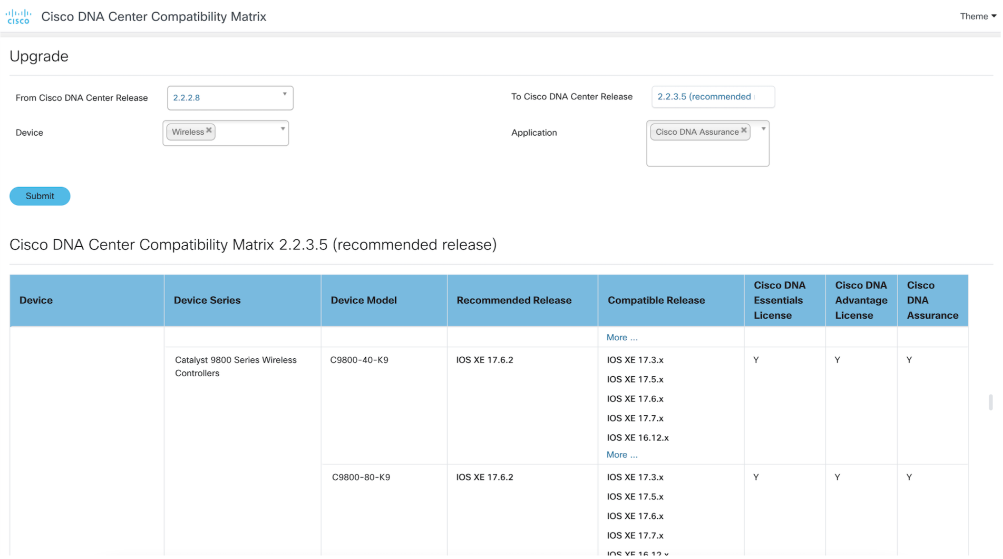
This chapter covers troubleshooting certain aspects of Cisco DNA Center.

Before debugging various modules, we need to check whether the devices are supported in the release and if Cisco DNA software modules are installed properly.

Supported Device and Version

For the supported IOS XE WLCs, AireOS WLCs, APs, and Switches in the Cisco DNA Center release, please refer to the compatibility matrix document mentioned in the References section.

Figure 14.1: Sample Cisco DNA Center Supported Device and Recommended Release



Upgrade

From Cisco DNA Center Release: 2.2.2.8

To Cisco DNA Center Release: 2.2.3.5 (recommended

Device: Wireless

Application: Cisco DNA Assurance

Cisco DNA Center Compatibility Matrix 2.2.3.5 (recommended release)

Device	Device Series	Device Model	Recommended Release	Compatible Release	Cisco DNA Essentials License	Cisco DNA Advantage License	Cisco DNA Assurance
				More ...			
	Catalyst 9800 Series Wireless Controllers	C9800-40-K9	IOS XE 17.6.2	IOS XE 17.3.x IOS XE 17.5.x IOS XE 17.6.x IOS XE 17.7.x IOS XE 16.12.x More ...	Y	Y	Y
		C9800-80-K9	IOS XE 17.6.2	IOS XE 17.3.x IOS XE 17.5.x IOS XE 17.6.x IOS XE 17.7.x IOS XE 16.12.x	Y	Y	Y

It is suggested to use the Recommended Release for the routers, switches and WLCs, though the compatible release is accepted as well.

Verify NETCONF on Catalyst 9000 Series Switches and WLCs

Before adding the Catalyst 9000 switches and WLCs to Cisco DNA Center verify whether the NETCONF is enabled on the device.

In the command line of Cisco DNA Center, please check if the Cisco DNA Center is able to receive data using the following command.

```
$ ssh -p 830 username@<deviceIP> -s netconf
The authenticity of host '[<Device IP>]:830 ([<Device
  IP>]:830)' can't be established.
RSA key fingerprint is
  SHA256:lCg9/hfonDlnzsCnM7uSLJt6QD9jNJSUbDOhxFf08DU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[<Device IP>]:830' (RSA) to
  the list of known hosts.
username@<Device IP>'s password:
<?xml version="1.0" encoding="UTF-8"?>
<hello
  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<capabilities>
<capability>urn:ietf:params:netconf:base:1.0</capability>
<capability>urn:ietf:params:netconf:base:1.1</capability>
<capability>urn:ietf:params:netconf:capability:writable-running:
  1.0</capability>
<capability>urn:ietf:params:netconf:capability:rollback-on-error:
  1.0</capability>
<capability>urn:ietf:params:netconf:capability:validate:1.0
  </capability>
<capability>urn:ietf:params:netconf:capability:validate:1.1
  </capability>
<capability>urn:ietf:params:netconf:capability:xpath:1.0
  </capability>
<capability>urn:ietf:params:netconf:capability:notification:1.0
  </capability>
<capability>urn:ietf:params:netconf:capability:interleave:1.0
  </capability>
<capability>urn:ietf:params:netconf:capability:with-defaults:1.0?
  basic-mode=explicit&amp;also-supported=report-all-tagged,report-
    all</capability>
<capability>urn:ietf:params:netconf:capability:yang-library:1.0?
  revision=2016-06-21&amp;module-set-id=116d099c87b0de473b7b1ec
    5528bfc53</capability>
<capability>http://tail-f.com/ns/netconf/actions/1.0</capability>
```

If the data is not seen, it needs to be enabled using the following configuration on the device.

NETCONF/YANG is supported as of IOS XE 16.3.1 software. For enabling NETCONF in the device, use the following commands.

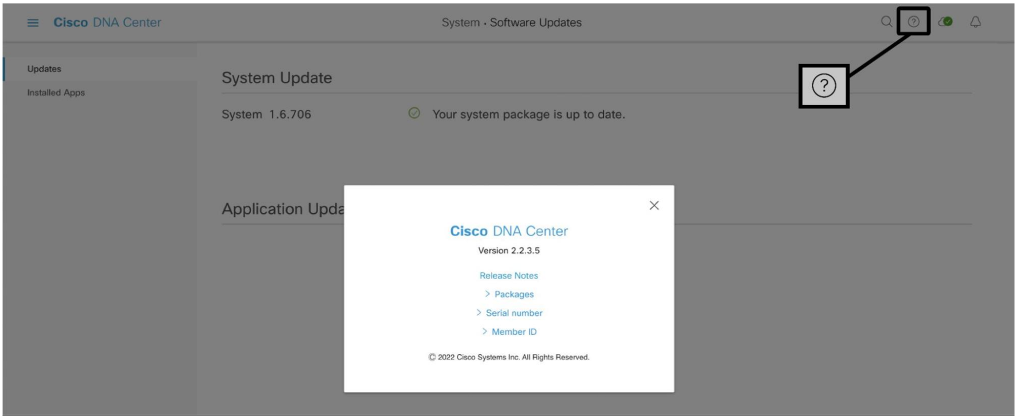
```
Cat9300-2#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Cat9300-2(config)#netconf-yang
Cat9300-2(config)#username <username> privilege 15 password
  0 <password> ---> Username/password used
  for NETCONF-SSH access

Cat9300-2(config)#aaa new-model
Cat9300-2(config)#aaa authorization exec default local
------------->
Required for NETCONF-SSH connectivity and edit-config operations

Please change aaa authorization exec default local
- command appropriately if you are using TACACS
```

Cisco DNA Center Software Packages Versions

Validate that the Cisco DNA Center deployment has the correct packages for the release installed. Please refer to the release notes for the version to verify the package versions.

From the Cisco DNA Center UI, click on the `question mark` (?) icon on the top right side of the screen to see the release notes link as shown in the figure below:

Figure 14.2: Release Notes URL



System 1.6.706 Your system package is up to date.

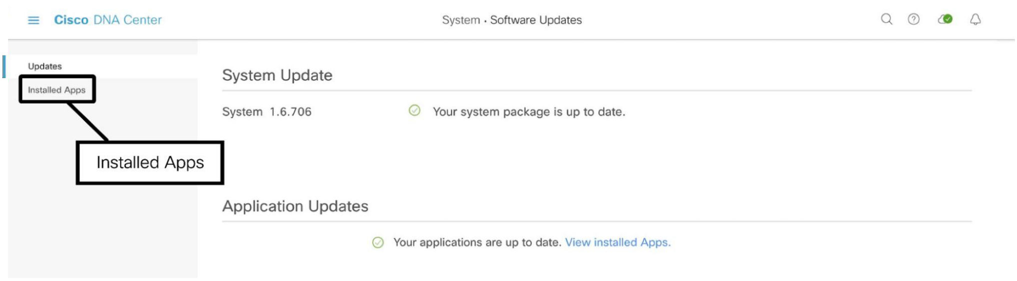
Cisco DNA Center
Version 2.2.3.5

© 2022 Cisco Systems Inc. All Rights Reserved.

Package versions should be under the section ***Package Versions in Cisco DNA Center, Release <release # (x.x.x.)***

Then go to `System > Software Updates` and obtain any necessary updates. Make sure the System package matches with the System package of the release note. Similarly for the Application packages, check in the Installed Apps section specifically for AI Network Analytics.

Figure 14.3: Application Packages Version



System 1.6.706

Your system package is up to date.

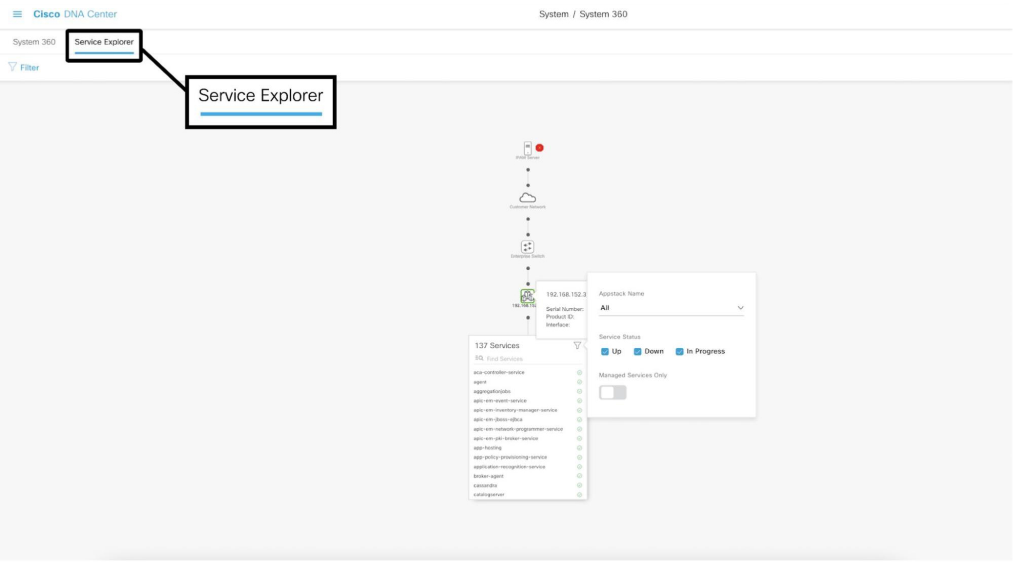
Your applications are up to date. View installed Apps.

If there is a version mismatch, there will be a `download/Install` button available. Please click and `install` the correct version of the packages.

Cisco DNA Center Services Status

In the Cisco DNA Center Service Explorer tab of `System > System 360` page, make sure all the services are in **RUNNING** status, particularly, NDP and assurance-backend Appstack Services.

Figure 14.4: Cisco DNA Center Services Status



192.168.152.3

Serial Number:
Product ID:
Interface:

Appstack Name: All

Service Status: ☑ Up ☑ Down ☑ In Progress

Managed Services Only: ○

137 Services

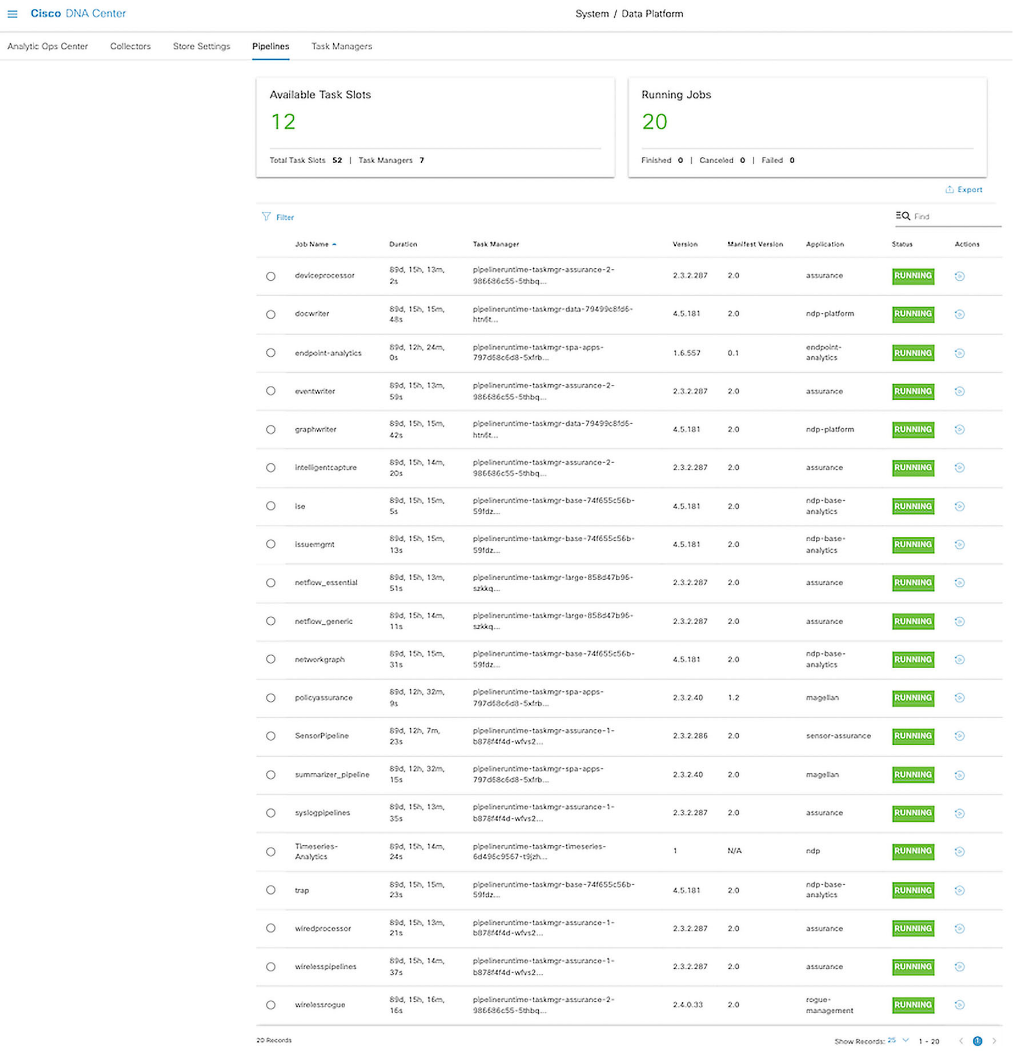
Find Services

- aca-controller-service ✓
- agent ✓
- aggregationjobs ✓
- apic-em-event-service ✓
- apic-em-inventory-manager-service ✓
- apic-em-jboss-ejbca ✓
- apic-em-network-programmer-service ✓
- apic-em-pki-broker-service ✓
- app-hosting ✓
- app-policy-provisioning-service ✓
- application-recognition-service ✓
- broker-agent ✓
- cassandra ✓
- catalogserver ✓

Cisco DNA Center Assurance Pipelines Status

Check all the pipelines are in **RUNNING** status in the pipelines tab of `System > Data Platform` page.

Figure 14.5: Pipelines Status



Available Task Slots
12
Total Task Slots 52 | Task Managers 7

Running Jobs
20
Finished 0 | Canceled 0 | Failed 0

	Job Name	Duration	Task Manager	Version	Manifest Version	Application	Status	Actions
○	deviceprocessor	89d, 15h, 13m, 2s	pipelineruntime-taskmgr-assurance-2-986686c55-5thbq...	2.3.2.287	2.0	assurance	RUNNING	
○	docwriter	89d, 15h, 15m, 48s	pipelineruntime-taskmgr-data-79499c8fd6-htn6t...	4.5.181	2.0	ndp-platform	RUNNING	
○	endpoint-analytics	89d, 12h, 24m, 0s	pipelineruntime-taskmgr-spa-apps-797d58c6d8-5xfrb...	1.6.557	0.1	endpoint-analytics	RUNNING	
○	eventwriter	89d, 15h, 13m, 59s	pipelineruntime-taskmgr-assurance-2-986686c55-5thbq...	2.3.2.287	2.0	assurance	RUNNING	
○	graphwriter	89d, 15h, 15m, 42s	pipelineruntime-taskmgr-data-79499c8fd6-htn6t...	4.5.181	2.0	ndp-platform	RUNNING	
○	intelligentcapture	89d, 15h, 14m, 20s	pipelineruntime-taskmgr-assurance-2-986686c55-5thbq...	2.3.2.287	2.0	assurance	RUNNING	
○	ise	89d, 15h, 15m, 5s	pipelineruntime-taskmgr-base-74f655c56b-59fdz...	4.5.181	2.0	ndp-base-analytics	RUNNING	
○	issuemgmt	89d, 15h, 15m, 13s	pipelineruntime-taskmgr-base-74f655c56b-59fdz...	4.5.181	2.0	ndp-base-analytics	RUNNING	
○	netflow_essential	89d, 15h, 13m, 51s	pipelineruntime-taskmgr-large-858d47b96-szkkq...	2.3.2.287	2.0	assurance	RUNNING	
○	netflow_generic	89d, 15h, 14m, 11s	pipelineruntime-taskmgr-large-858d47b96-szkkq...	2.3.2.287	2.0	assurance	RUNNING	
○	networkgraph	89d, 15h, 15m, 31s	pipelineruntime-taskmgr-base-74f655c56b-59fdz...	4.5.181	2.0	ndp-base-analytics	RUNNING	
○	policyassurance	89d, 12h, 32m, 9s	pipelineruntime-taskmgr-spa-apps-797d58c6d8-5xfrb...	2.3.2.40	1.2	magellan	RUNNING	
○	SensorPipeline	89d, 12h, 7m, 23s	pipelineruntime-taskmgr-assurance-1-b878f4f4d-wfvs2...	2.3.2.286	2.0	sensor-assurance	RUNNING	
○	summarizer_pipeline	89d, 12h, 32m, 15s	pipelineruntime-taskmgr-spa-apps-797d58c6d8-5xfrb...	2.3.2.40	2.0	magellan	RUNNING	
○	syslogpipelines	89d, 15h, 13m, 35s	pipelineruntime-taskmgr-assurance-1-b878f4f4d-wfvs2...	2.3.2.287	2.0	assurance	RUNNING	
○	Timeseries-Analytics	89d, 15h, 14m, 24s	pipelineruntime-taskmgr-timeseries-6d496c9567-t9jzh...	1	N/A	ndp	RUNNING	
○	trap	89d, 15h, 15m, 23s	pipelineruntime-taskmgr-base-74f655c56b-59fdz...	4.5.181	2.0	ndp-base-analytics	RUNNING	
○	wiredprocessor	89d, 15h, 13m, 21s	pipelineruntime-taskmgr-assurance-1-b878f4f4d-wfvs2...	2.3.2.287	2.0	assurance	RUNNING	
○	wirelesspipelines	89d, 15h, 14m, 37s	pipelineruntime-taskmgr-assurance-1-b878f4f4d-wfvs2...	2.3.2.287	2.0	assurance	RUNNING	
○	wirelessrogue	89d, 15h, 16m, 16s	pipelineruntime-taskmgr-assurance-2-986686c55-5thbq...	2.4.0.33	2.0	rogue-management	RUNNING	

20 Records

Show Records: 25 1 - 20 1

Troubleshooting AI Network Analytics

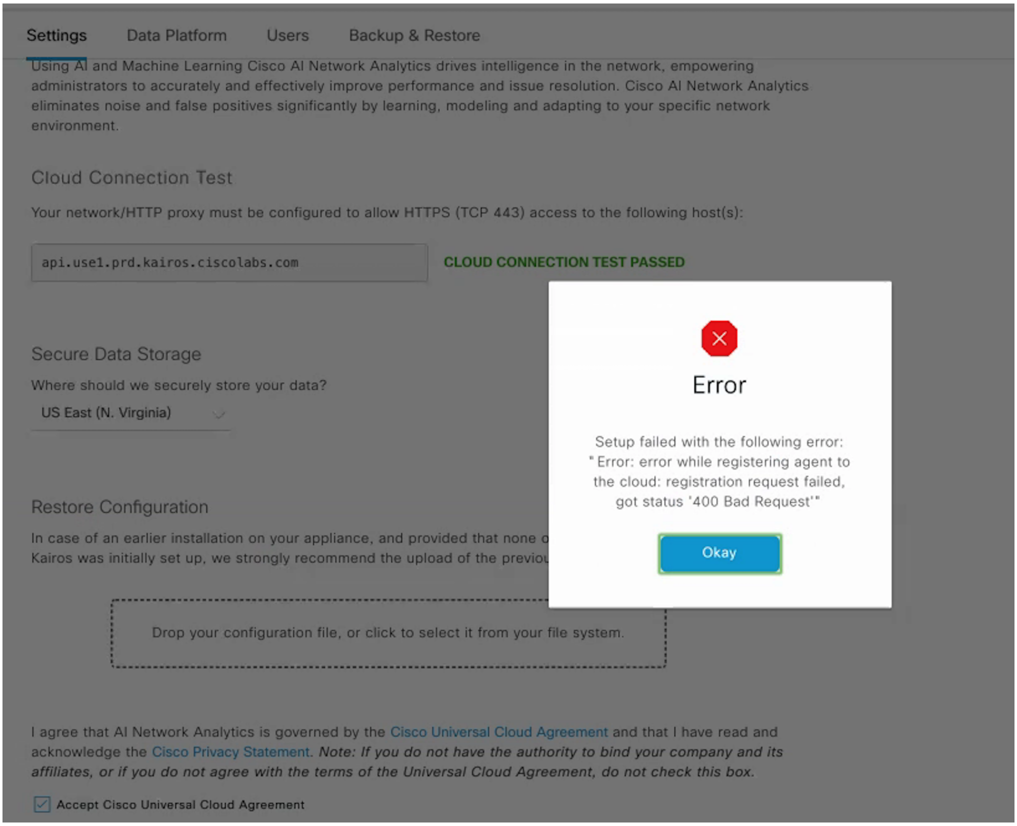
Troubleshooting Cloud registration

To enable the features offered via the Cisco AI Analytics cloud, the Cisco DNA Center appliance **MUST** have internet access, allowing outbound HTTPS connections on TCP port 443 to the following API endpoints:

- `api.use1.prd.kairos.ciscolabs.com` – US region
- `api.euc1.prd.kairos.ciscolabs.com` – EMER/APJC region

The cloud registration will fail if the Cisco DNA Center appliance cannot reach the cloud servers, or if the connection goes through SSL Inspection, as this will break the mutual authentication between the local agent and the cloud server.

Figure 14.6: Example of Failure Upon Cloud Tenant Registration on Cisco AI Analytics



Using AI and Machine Learning Cisco AI Network Analytics drives intelligence in the network, empowering administrators to accurately and effectively improve performance and issue resolution. Cisco AI Network Analytics eliminates noise and false positives significantly by learning, modeling and adapting to your specific network environment.

Cloud Connection Test

Your network/HTTP proxy must be configured to allow HTTPS (TCP 443) access to the following host(s):

api.use1.prd.kairos.ciscolabs.com

CLOUD CONNECTION TEST PASSED

Secure Data Storage

Where should we securely store your data?

US East (N. Virginia)

Restore Configuration

In case of an earlier installation on your appliance, and provided that none o
Kairos was initially set up, we strongly recommend the upload of the previou

Drop your configuration file, or click to select it from your file system.

I agree that AI Network Analytics is governed by the Cisco Universal Cloud Agreement and that I have read and acknowledge the Cisco Privacy Statement. *Note: If you do not have the authority to bind your company and its affiliates, or if you do not agree with the terms of the Universal Cloud Agreement, do not check this box.*

☑ Accept Cisco Universal Cloud Agreement

Error

Setup failed with the following error: "Error: error while registering agent to the cloud: registration request failed, got status '400 Bad Request'"

Okay

In case of errors upon cloud registration, make sure that the Cisco AI Analytics cloud API endpoints are reachable:

- If the connection requires an **HTTP proxy**, make sure that it is correctly configured on the Cisco DNA Center Appliance, by checking the Cisco DNA Appliance UI: `System > Settings > System Configuration > Proxy`.

- If the connection goes through **SSL Inspection**, verify that a bypass rule is configured to ensure SSL Inspection does not break traffic to the Cisco AI Analytics cloud API endpoints.

If the cloud registration still fails after verifying connectivity to the cloud, please make sure that the clock on the Cisco DNA Center appliance is properly synchronized with an NTP server, as time drift can cause issues with the validation steps happening as part of the registration process.

Product Activation

Each feature offered via the Cisco AI Network Analytics cloud has local requirements to be met before it can be enabled.

For instance, Cisco AI Network Analytics and AI Enhanced RRM require wireless devices to be managed by the Cisco DNA Center appliance. Therefore, they will not work if only wired devices are managed in Cisco DNA Center.

When enabling Cisco AI Network Analytics on a new Cisco DNA Center deployment managing wireless devices, ensure that the network devices are discovered and managed on the device inventory. If not, the network engineer will see no data for the Network Analytics features.

Missing Data

Following a successful cloud registration, the Cisco AI Analytics agent installed on the Cisco DNA Center appliance immediately starts exporting telemetry data to the cloud; it then takes approximately one hour for the cloud data processing pipelines to be activated.

Seeing results on the UI, however, will take more time, depending on the requirements of each use case. For instance, while Network Heatmaps usually take one day to start showing data, AI-driven issues require at least one week of data, and long-term analytics use cases such as

AP Performance Advisories will take approximately four weeks to produce insights.

When there's no data displayed on the AI Analytics pages, checking the output of Network Heatmaps is the easiest way to verify that the data ingestion and cloud pipelines are working correctly, as the heatmap views are expected to be always available.

Other use cases, such as AI-driven issues, Trends, and AP Performance Advisories only show results when the AI/ML algorithms running in the cloud identify interesting information to be displayed; for this reason, it may take additional time to start seeing results for such use cases, depending on the network size and specific activity.

If Network Heatmaps show no data, it is recommended to verify the network connectivity to the cloud (as described in the cloud registration troubleshooting section) as well as the Cisco DNA Assurance Health dashboards, to confirm whether data for the managed WLCs, Access Points, and clients show up correctly.

Some use cases, such as the Baseline Dashboard and AI-driven issues for Excessive Onboarding time and failures, perform data aggregation at the building level, therefore these features only work if the APs are assigned to a building in the Network Hierarchy.

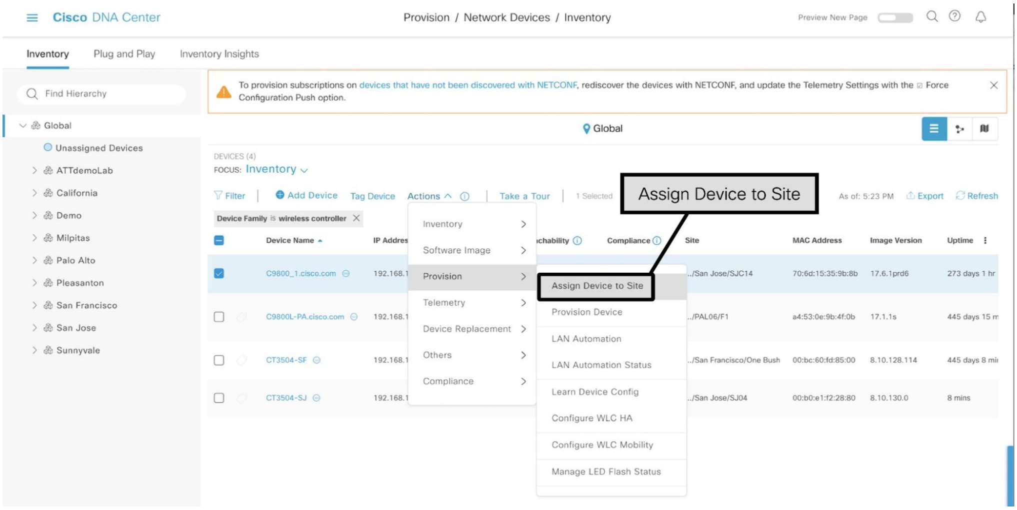
The computation of throughput-related KPIs (for all applicable use cases, including AI-driven issues, Network Heatmaps, Network Comparisons, Trends) makes use of AVC (Application Visibility and Control) data, exported via telemetry for AireOS WLCs or via NetFlow for IOS XE WLCs; if no throughput data or issues are seen in the UI, make sure that Application Telemetry is enabled on the managed WLCs.

If the cloud connectivity is confirmed to be working fine, all the previous checks have been completed, but data is still missing from the AI Analytics pages, please verify if data shows up on the Cisco DNA Assurance Health Dashboard.

Troubleshooting Wireless and Wired Assurance

When a device is added to the Cisco DNA Center using Discovery Tool, make sure it is assigned to a Site in `Provision > Network Devices > Inventory` page.

Figure 14.7: Assign Device to a Site



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

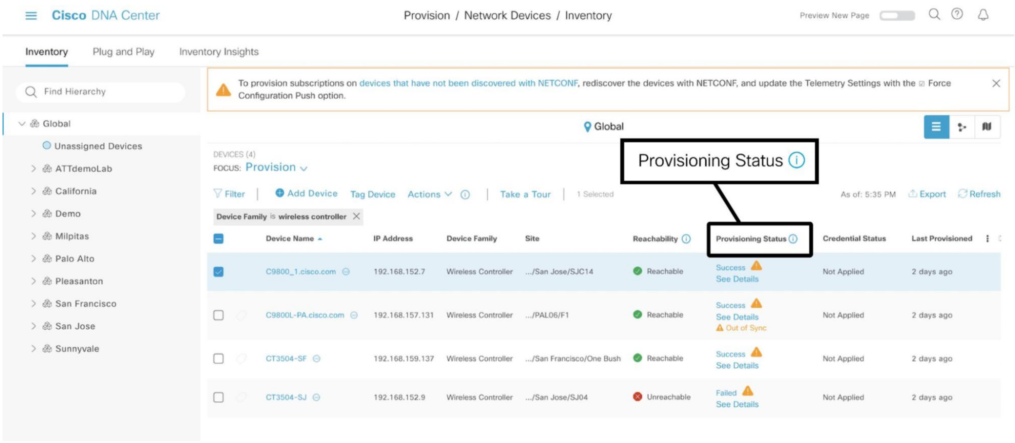
	Device Name	IP Addres	chability	Compliance	Site	MAC Address	Image Version	Uptime
☑	C9800_1.cisco.com	192.168.1			../San Jose/SJC14	70:6d:15:35:9b:8b	17.6.1prd6	273 days 1 hr
☐	C9800L-PA.cisco.com	192.168.1			../PAL06/F1	a4:53:0e:9b:4f:0b	17.1.1s	445 days 15 m
☐	CT3504-SF	192.168.1			../San Francisco/One Bush	00:bc:60:fd:85:00	8.10.128.114	445 days 8 mi
☐	CT3504-SJ	192.168.1			../San Jose/SJ04	00:b0:e1:f2:28:80	8.10.130.0	8 mins

Assign Device to Site

When the device is added to the site, Cisco DNA Center provisions the WLC with telemetry settings. It also adds commands to the device for downloading the certificates from the Cisco DNA Center. The file download and HTTP access can’t be blocked between the device and Cisco DNA Center.

Verify the telemetry provisioning status by changing the **FOCUS** to `Provision`. The figure below shows the detailed telemetry provisioning status.

Figure 14.18: Telemetry Provisioning Status



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

DEVICES (4)
FOCUS: Provision

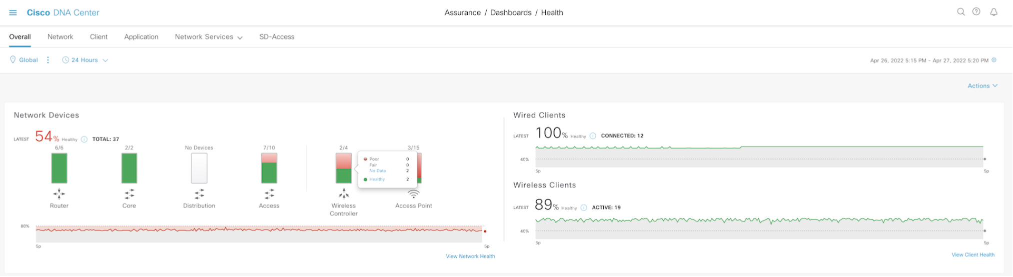
As of: 5:35 PM

Device Family is wireless controller

	Device Name	IP Address	Device Family	Site	Reachability	Provisioning Status	Credential Status	Last Provisioned
☑	C9800_1.cisco.com	192.168.152.7	Wireless Controller	.../San Jose/SJC14	Reachable	Success ⚠ See Details	Not Applied	2 days ago
□	C9800L-PA.cisco.com	192.168.157.131	Wireless Controller	.../PAL06/F1	Reachable	Success ⚠ See Details ⚠ Out of Sync	Not Applied	2 days ago
□	CT3504-SF	192.168.159.137	Wireless Controller	.../San Francisco/One Bush	Reachable	Success ⚠ See Details	Not Applied	2 days ago
□	CT3504-SJ	192.168.152.9	Wireless Controller	.../San Jose/SJ04	Unreachable	Failed ⚠ See Details	Not Applied	2 days ago

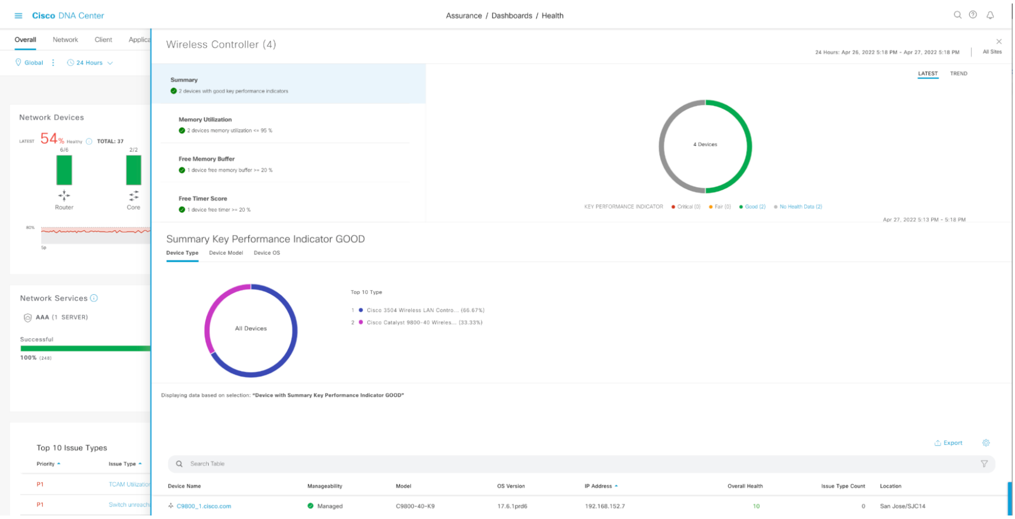
If the Provisioning Status is Success, Check the Overall tab on the `Assurance > Dashboards > Health` page.

Figure 14.9: Assurance Device Types Status



Click on the `green part` of the device type added to see the device with Assurance data such as that below for WLC.

Figure 14.10: Device Monitoring Status



Wireless Controller (4)

Summary
✓ 2 devices with good key performance indicators

Memory Utilization
✓ 2 devices memory utilization <= 95 %

Free Memory Buffer
✓ 1 device free memory buffer >= 20 %

Free Timer Score
✓ 1 device free timer >= 20 %

Summary Key Performance Indicator GOOD

Displaying data based on selection: **"Device with Summary Key Performance Indicator GOOD"**

Device Name	Manageability	Model	OS Version	IP Address	Overall Health	Issue Type Count	Location
C9800_1.cisco.com	● Managed	C9800-40-K9	17.6.1prd6	192.168.152.7	10	0	San Jose/SJC14

If the device is not in the table, contact Cisco Technical Support as this suggests that telemetry is still not coming into Cisco DNA Center.

Troubleshooting Application Assurance

Verify the network device has the Network Advantage license.

Verify the source interface in the flow exporter configuration of the network device has the applications configured.

Verify the destination IP in the flow exporter configuration is the Cisco DNA Center enterprise Virtual IP Address (VIP).

Verify all the WLAN configuration has application visibility/experience configurations as below

```
wireless profile policy Flex_SSID_Global_NF_0cd02814
    shutdown
    ipv4 flow monitor avc_basic_monitor input
    ipv4 flow monitor avc_basic_monitor output
    no shutdown
```

Verify whether Cisco DNA Center is receiving application data, using the following command from the Cisco DNA Center command line:

```
sudo tcpdump -i any -n udp port 6007
```

If you still don't see the application data, please contact **Cisco Technical Support**

Keep in mind that no matter what issue is encountered with Cisco DNA Center and related features, Cisco Technical Support is always there to provide assistance 24/7.

Appendix

References

Cisco DNA Center End-User Guides
https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html

Cisco DNA Center Compatibility Matrix
https://www.cisco.com/c/dam/en/us/td/docs/Website/enterprise/dnac_compatibility_matrix/index.html

Cisco DNA Center Release Notes
https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-release-notes-list.html

Application Hosting on Catalyst 9300 and 9400
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/178/b_178_programmability_cg/m_178_prog_app_hosting.html

Cisco DNA Spaces Configuration Guide
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/DNA-Spaces/cisco-dna-spaces-config/dnaspaces-configuration-guide/m_dnac.html

Additional Resources for Cisco DNA Center

Cisco DNA Center Demos
https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/demos.html

Cisco DNA Center Automation and Assurance v2.2.3.4 – Instant Demo
https://dcloud2-sjc.cisco.com/content/instantdemo/cisco-dna-center-automation-and-assurance-v2-2-3-4-instant-demo-sandbox?returnPathTitleKey=content-view

YouTube Channel – Cisco
https://www.youtube.com/channel/UCEWiIE6Htd8mvlOR6YQez1g

Acronyms

AAA – Authentication/Authorization and Accounting

AI – Artificial Intelligence

AI/ML – Artificial Intelligence/Machine Learning

AIOps – Artificial Intelligence for IT Operations

AP – Access Point

API – Application Programmable Interface

APM – Application Performance Monitoring

AVC – Application Visibility and Control

CLI – Command-Line Interface

CPU – Central Processing Unit

CSV – Comma Separated Values

DHCP – Dynamic Host Configuration Protocol

DBS – Dynamic Bandwidth Selection

DCA – Dynamic Channel Assignment

DevOps – Developer Operations

DNA – Digital Network Architecture

DNS – Domain Name System

DSCP – Differentiated Services Code Point

EAP – Extensible Authentication Protocol

EU – European Union

FFT – Fast-Fourier Transform

FRA – Flexible Radio Architecture

FTV – Faster Time To Value

gRPC – Google Remote Procedure Call

GUI – graphical user interface

HTTPS – Hypertext Transfer Protocol Secure

ICMP – Internet Control Message Protocol

IoT – Internet of Things

IP – Internet Protocol

IT – Information Technology

JSON – JavaScript Object Notation

KPI – Key Performance Indicator

MAB – MAC Authentication Bypass

MAC – Media Access Control

ML – Machine Learning

MRE – Machine Reasoning Engine

MTTR – Mean Time To Resolution

NETCONF – Network Configuration

NetOps – Network Operations

OPEX – Operational Expense

OAuth – Open Authentication

PCAP – Packet Capture

PDF – Portable Document Format

PerfMon – Performance Monitor

PoE – Power over Ethernet

RCA – Root Cause Analysis

RF – Radio Frequency

ROI – Return on Investment

RRM – Radio Resource Management

RSSI – Received Signal Strength Indicator

SaaS – Software as a Service

SDK – Software Development Kit

SecOps – Security Operations

SLAs – service level agreements

SNMP – Simple Network Management Protocol

SNR – Signal-To-Noise Ratio

STP – Spanning Tree Protocol

SSID – Service Set Identifier

TCP – Transmission Control Protocol

TPC – Transmit Power Control

TTV – Time to Value

UDP – User Datagram Protocol

UI – User Interface

UPoE – Universal Power Over Ethernet

WLC – Wireless LAN Controller

Prem Chandran
Sean Sivak
Harsharan Dhaliwal
Suresh Subramanian
Federico Lovison
Shai Silberman