

Cisco Catalyst Assurance User Guide, Release 3.2.x

First Published: 2026-05-05

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **New and Changed Information** 1

New and changed features in Cisco Catalyst Assurance 1

CHAPTER 2 **Cisco Catalyst Assurance Overview** 3

Assurance overview 3

Assurance architecture 3

IPv6 address support 4

User profile roles and permissions 5

Start with Assurance 5

CHAPTER 3 **Cisco AI Network Analytics Overview** 7

About Cisco AI Network Analytics 7

Cisco AI Network Analytics benefits 9

Cisco AI Network Analytics licensing and deployment 9

CHAPTER 4 **Set Up Catalyst Center to Use Assurance** 11

Limitations and restrictions of Assurance 11

Basic setup workflow 11

Discover devices 14

Discovery overview 14

Discovery prerequisites 15

Preferred management IP address 16

Discovery configuration guidelines and limitations 16

Discovery credentials 17

Discover your network using CDP 21

Discover your network using an IP address range or CIDR 24

Discover your network using LLDP 26
Manage Discovery jobs 29
Stop and start a Discovery job 29
Clone a Discovery job 29
Delete a Discovery job 29
View Discovery job information 30
Network hierarchy 30
Create the network hierarchy 32
Create, edit, and delete a site 32
Add, edit, and delete a building 34
Add, edit, and delete a floor 34
Existing Cisco network hierarchies 36
Export your site hierarchy from Cisco Prime Infrastructure 36
Export your map archive from Cisco Prime Infrastructure 37
Import your site hierarchy to Catalyst Center 38
Import your map archive to Catalyst Center 38
Use an existing Ekahau network hierarchy 39
Export the Ekahau project from Catalyst Center 39
Import an Ekahau project to Catalyst Center 40
Import an Ekahau site survey to Catalyst Center 41
Configure 2D floor map devices and overlay objects 42
Add, position, edit, and remove APs 44
Add, position, and remove sensors 45
Add, edit, and remove coverage areas 46
Add, edit, copy, and remove openings 47
Add, edit, and remove location regions 48
Add, edit, and remove walls 49
Add, copy, edit, and remove shelving units 50
Add, edit, and remove markers 51
Add, edit, and remove GPS markers 51
Add, edit, and remove align points 52
Manage Inventory 53
About Inventory 53
Update the device polling interval 54

Display information about your inventory 55
Deal with SSH key verification errors 61
Configure the automatic acceptance of SSH key changes 62
Delete a network device 62
Deploy your device configurations now or later 64
Preview and deploy your device configurations 64
Assign an unprovisioned device to a site 65
Add APs to a map 67
Position an AP on a map 68
About Cisco ISE configuration for Catalyst Center 72
Configure authentication and policy servers 72
Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry 76
Configure Cisco AI Network Analytics 77
Disable Cisco AI Network Analytics 79
Update the Machine Reasoning Knowledge Base 80
Enable localization 81

CHAPTER 5 **Monitor and Troubleshoot Overall Enterprise Health** 83
Enterprises 83
Monitor and troubleshoot the overall health of your enterprise 83

CHAPTER 6 **Monitor and Troubleshoot Network Health** 87
Monitor and troubleshoot the health of your network 87
Monitor and troubleshoot the health of a device 95
About Cisco StackWise Virtual and its limitations 108
About Cisco StackWise and its limitations 109
Configure health score settings for network devices 109
Enable SNMP Collector metrics for fabric devices 111
Understand network health score and KPI metrics 113
Network Health score 113
Device Category Health score 113
Individual Device Health score 113
Switch Health score 114

Router Health score 115
AP Health score 116
Wireless Controller Health score 118
Effects of maintenance mode on network health scores and KPI metrics 119
Understand RF calculations 120

CHAPTER 7 Monitor and Troubleshoot Client Health 123
Remote LAN support 123
Workgroup bridge client support 123
Monitor and troubleshoot the health of all client devices 123
Monitor and troubleshoot the health of a client device 137
Client tracking 147
Track known clients 148
Track new clients 150
Stop tracking clients 151
Configure excluded clients 152
Understand Client Health score and KPI metrics 153
Client Health score 153
Client Onboarding score 154
Client Connectivity score 154
Individual Client Health score 155

CHAPTER 8 Monitor Application Health 157
About Application Experience and Application Visibility 157
Supported platforms 158
Criteria for enabling application telemetry on devices 159
Application health prerequisites 161
Provision application telemetry settings 163
View Application Experience of a host 164
View Application Experience of a network device 165
Monitor the health of all applications 166
Install ThousandEyes Enterprise Agents 174
Manage enterprise agents and tests 176
Monitor the health of an application 178

Monitor and troubleshoot health of a Webex application 182
Monitor and troubleshoot the health of a Microsoft Teams application 185
Configure health score settings for applications 189
Understand application health score and KPI metrics 189
Overall application health score 189
Individual application health score 190

CHAPTER 9 Monitor Network Services 191
Monitor the AAA network service 191
Monitor the DHCP network service 195
Monitor the DNS network service 198

CHAPTER 10 Monitor and Troubleshoot SD-Access Health 203
SD-Access fabric 203
Add a fabric site 203
Add a device to a fabric 206
Monitor and troubleshoot the health of your SD-Access fabric 209
Monitor the health of a fabric site 214
Monitor the health of a transit and peer network 218
Monitor the health of a virtual network 223

CHAPTER 11 Monitor and Troubleshoot Your Network Using Site Analytics 229
About Site Analytics 229
Site Analytics dashboard insights 231
View Site Analytics 234
Configure Site Analytics settings 238

CHAPTER 12 View and Manage Issues 239
About issues 239
About the Machine Reasoning Engine 240
About the Layer 2 Loop issue involving VLANs 240
View open issues 241
Issue Instance Details for AI-driven issues 245
Issue Instance Details for AP-Disconnect Issues 248

Issue Instance Details for Layer 2 Loop issue 249
Issue Instance Details for a PoE issue 251
Issue Instance Details for Application health degradation issue 253
Troubleshoot wired client issues using MRE 254
View resolved issues 257
View ignored issues 259
Resolve or ignore issues 261
No Activity on Radio issue triggers 262
Automatic issue resolution 263
Manage global issue settings 266
Manage user-defined issue settings 267
Manage Custom Issue Settings 269
Enable issue notifications 270
Assurance, Cisco AI Network Analytics, and MRE issues 273
Router issues 273
Core, distribution, and access issues 275
Third-party device issues 278
Controller issues 279
Access point issues 280
Wired client issues 281
Wireless client issues 282
Enable AAA Failure Root Cause Analysis issues 285
Application issues 286
Sensor issues 286
AI-driven issues 288
MRE issues 289

CHAPTER 13 View and Manage Events 291
Events dashboard overview 291
View device events 291
View endpoint events 295
View event analytics dashboard 299

CHAPTER 14 Manage Sensors and Sensor-Driven Tests 305

About sensors and sensor-driven tests 305
Provision sensors 305
Provision the wireless Cisco Aironet 1800s Active Sensor 305
Enable Provisioning SSID on the wireless controller 306
Enable Provisioning SSID on the Cisco Catalyst Wireless Controller 307
Provision an AP or sensor device 308
Monitor and troubleshoot network health with sensors 310
Monitor and troubleshoot network health with all wireless sensors 310
Monitor and troubleshoot network health with a wireless sensor 315
Manage sensors and backhaul settings 317
Manage sensors in your network 317
Manage backhaul settings 319
Persistent wireless backhaul connections on sensor devices 321
Manage SCEP profiles 321
Sensor-driven tests 322
Create and run sensor-driven tests using templates 322
Manage sensor-driven test templates 326

CHAPTER 15 **Monitor Wi-Fi Readiness** 329
Wi-Fi Readiness assessments 329
Assure the Wi-Fi readiness of your network 329

CHAPTER 16 **Monitor Power over Ethernet** 335
About Power over Ethernet 335
Setup workflow for PoE telemetry 335
Configure NETCONF on your devices for PoE telemetry 337
Update telemetry settings for PoE telemetry 339
Monitor PoE-capable devices in your network 340

CHAPTER 17 **Manage Dashboards** 347
About dashboards 347
Create a custom dashboard 347
View a dashboard 348
Edit or delete a dashboard 348

Duplicate a dashboard 349
Mark a dashboard as a favorite 349
Change the position of a dashlet 349
Configure filter group settings 350

CHAPTER 18 **Observe Network Trends and Gain Insights** 353
About network trends and insights 353
View wireless AP performance advisories 353
View network trends and obtain insights 357
Compare APs and switches in network heatmaps 362
Compare KPI values with peers in your network 366
Compare buildings, AP model families, and wireless endpoint types 367
View and monitor network performance using baselines 370
View the RF network using the AI-enhanced RRM dashboard 373

CHAPTER 19 **Manage Intelligent Capture** 389
About Intelligent Capture 389
Supported devices for Intelligent Capture 389
Intelligent Capture best practices 390
How to configure and use Intelligent Capture 390
Onboarding Packet Capture for a client device 390
About Onboarding Packet Capture for a client device 390
About client statistics 391
Run an Onboarding Packet Capture live session for a client device 391
Schedule an Onboarding Packet Capture session for a client device 395
Stop in-progress Onboarding Packet Capture sessions on a client device 396
Full Packet Capture for a client device 397
About Full Packet Capture for a client device 397
Run a Full Packet Capture session on a client device 397
View Full Packet Capture history 399
OTA Sniffer Capture for a Wi-Fi band and channel 400
About OTA Sniffer Capture for a Wi-Fi band and channel 400
Run an OTA Sniffer Capture session on a Wi-Fi band and channel 400
Download PCAP files from a completed OTA Sniffer Capture session 403

AP Statistics Capture for APs and wireless controllers 403
About AP Statistics Capture for APs and wireless controllers 403
Enable or disable AP Statistics Capture on a specific AP 404
Enable or disable AP Statistics Capture on a wireless controller 405
View incompatible APs for AP Statistics Capture 406
View RF Statistics of an AP 406
Anomaly Capture for APs and wireless controllers 408
About Anomaly Capture for APs and wireless controllers 408
Enable or disable Anomaly Capture on a specific AP 409
Enable or disable Anomaly Capture on a wireless controller 410
View incompatible and supported APs for Anomaly Capture 411
Spectrum Analysis for APs 412
About Cisco AP functionality during spectrum analysis 412
Start a spectrum analysis session on an AP 412
View spectrum analysis data of an AP 413
Packet capture for wired client devices 416
Run a packet capture on a wired client device 416
Stop a running capture 418
Download a completed packet capture 418
Troubleshoot Intelligent Capture 418
Client or AP unable to send Intelligent Capture data to Catalyst Center 418
Troubleshoot wired packet capture issues 419

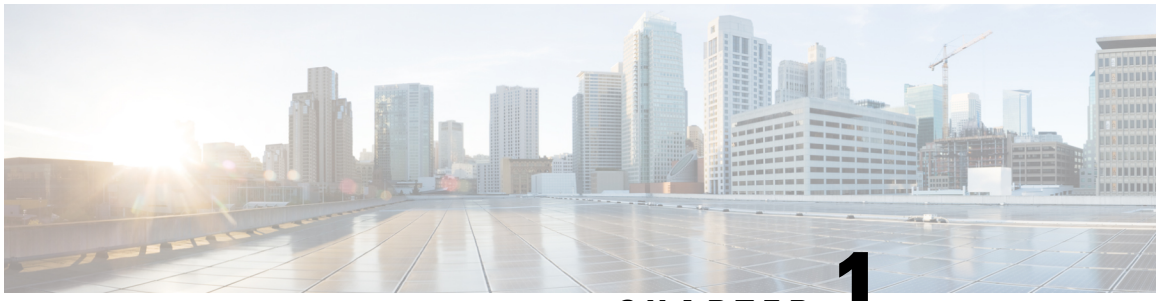
CHAPTER 20 **Manage SSID Monitoring Settings** 421
About SSID monitoring 421
Configure SSID monitoring settings 422
View the provisioning status for SSID monitoring 422

CHAPTER 21 **Trace the Path of a Device** 425
About path trace 425
Path trace limitations 425
Do a path trace 428

CHAPTER 22 **Integrate Cisco CMX for Wireless Maps** 431

About Cisco Connected Mobile Experiences integration 431
Add a user for the Cisco CMX API server 431
Create Cisco CMX settings 432
Troubleshoot Cisco CMX 434

CHAPTER 23 View Assurance Audit Logs 435
View audit logs for Assurance 435



CHAPTER 1

New and Changed Information

• New and changed features in Cisco Catalyst Assurance, on page 1

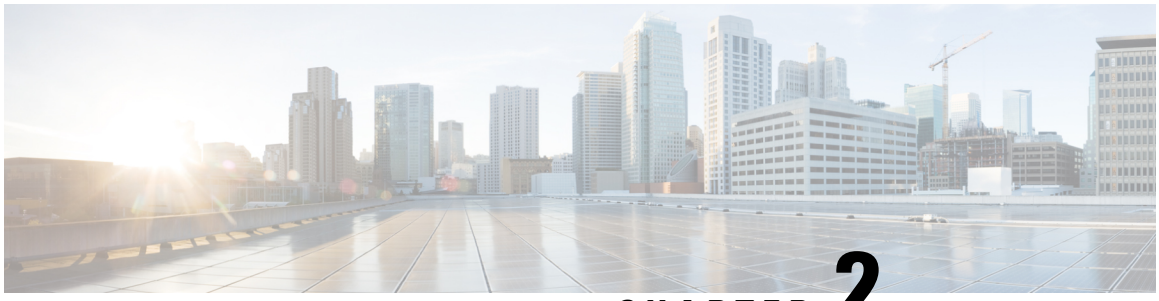
New and changed features in Cisco Catalyst Assurance

This table summarizes the new and changed features in Cisco Catalyst Assurance and tells you where they are documented.

Table 1: New and changed features in Cisco Catalyst Assurance 3.2.2

Feature	Description
Track when clients disconnect from the network	You can now track clients when they disconnect from the network and receive disconnect notifications. See Client tracking, on page 147.
Wi-Fi 7 Capability support	Wi-Fi 7 capability support is added to Client 360. Multiple Link Operational (MLO) capable clients can simultaneously connect to different combinations of 2.4-GHz, 5-GHz, or 6-GHz bands. See Wi-Fi Readiness assessments, and Assure the Wi-Fi readiness of your network.
Device and Client Health enhancements	Enhanced health score and issue detection for Wireless LAN Controllers and clients by incorporating critical KPIs such as retries, monitoring WLC HA pair failures and mobility tunnel status, and improving issue triggering to reflect accurate user health scores, including customer-specific escalated use cases.
ThousandEyes Agent enhancements	Added support for Direct, Static, and PAC proxy configurations, customizable Docker runtime options, and an Agent Details view for monitoring resources and network settings. See Manage enterprise agents and tests, on page 176.
Industrial Ethernet (IE) Switch support	Catalyst Center now supports ThousandEyes agent management for the Cisco Catalyst Industrial Ethernet (IE) 3500 Series and Cisco Catalyst Industrial Ethernet (IE) 9300 Series Switches. See Install ThousandEyes enterprise agents.

Feature	Description
Outdoor Area support	Catalyst Center now supports **Outdoor Areas** as a distinct site type in the Assurance dashboard. You can monitor outdoor access points and view their health status within the site map and hierarchy. See Monitor and troubleshoot the health of your network, Monitor and troubleshoot the health of all client devices, Monitor PoE-capable devices in your network, and Assure the Wi-Fi readiness of your network.
AAA Network Services enhancements	You can now view AAA server transaction statistics, latency trends, and client events aggregated from both wireless controllers and switches. See Monitor the AAA network service, on page 191.
Enhancements to OTA Sniffer capture	Enhancements to the OTA packet capture providing greater flexibility for troubleshooting complex Wi-Fi 7 and Multi-Link Operation (MLO) environments. These enhancements allow for simultaneous traffic capture across multiple radios and Access Points (APs).
AI Syslog Summarization and Explanation	AI-driven summarization of syslog messages and AI insight in the Event Analytics dashboard transforms raw syslog data into actionable insights, enabling quick identification of trends and facilitating efficient event analysis and management. See View event analytics dashboard, on page 299
Health Score-Based Issues	Catalyst Center now automatically generates an **Application Health Degradation** issue when an application's health score falls below a configurable threshold, which is set to 7 by default. Issues are categorized by both application and site, with separate issues created for each site if the degradation spans multiple locations.
Packet capture for wired client devices	You can now initiate a packet capture from Assurance to help troubleshoot a wired client device's connectivity or traffic issues. See Packet capture for wired client devices, on page 416.



CHAPTER 2

Cisco Catalyst Assurance Overview

- Assurance overview, on page 3
- Assurance architecture, on page 3
- IPv6 address support, on page 4
- User profile roles and permissions, on page 5
- Start with Assurance, on page 5

Assurance overview

Assurance provides a comprehensive solution to assure better and consistent service levels to meet growing business demands. It addresses not just reactive network monitoring and troubleshooting, but also proactive and predictive aspects of running a network and ensuring optimal client, application, and service performance.

Assurance provides these benefits:

- Provides actionable insights into network, client, and application-related issues. These issues consist of basic and advanced correlation of multiple pieces of information, thus eliminating white noise and false positives.
- Provides both system-guided as well as self-guided troubleshooting. For a large number of issues, Assurance provides a system-guided approach, where multiple Key Performance Indicators (KPIs) are correlated, and the results from tests and sensors are used to determine the root cause of a problem, after which possible actions are provided to resolve the problem. The focus is on highlighting the issue rather than monitoring data. Quite frequently, Assurance does the work of a Level 3 support engineer.
- Provides in-depth health scores for a network and its devices, clients, applications, and services. Client experience is assured both for access (onboarding) and connectivity.

Assurance architecture

Companies deal with an abundance of network data. Tackling the volume, variety, speed, and accuracy of network data is crucial for IT organizations. Assurance is designed to handle network data issues, if any.

Assurance is a multipurpose, real-time, network data collection and analytics engine that can significantly increase the business potential of network data.

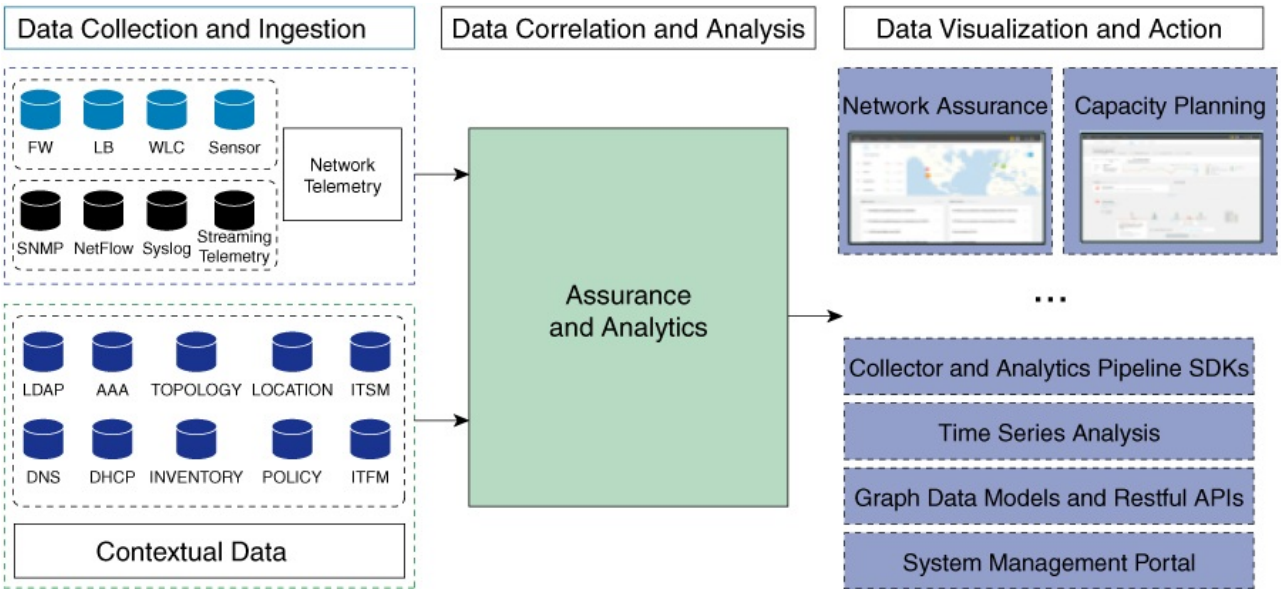
Assurance simplifies and abstracts the collection and analysis layers and offers a rich set of APIs along with a web interface. By using a single set of network data, Assurance powers a broad set of use cases. These

advantages streamline the operational and network management overhead of collecting and analyzing network data, thereby allowing companies to effectively focus on their business goals.

Given its flexible architecture, Assurance addresses many common use cases, including monitoring and troubleshooting, cost management, and policy discovery, while supporting the broader Catalyst Center strategy.

This figure and the information that follows describe the Assurance architecture:

Figure 1: Assurance architecture



- **Data Collection and Ingestion**: Assurance leverages streaming technologies to collect a variety of network telemetry and contextual data in real time.
- **Data Correlation and Analysis**: As and when data is ingested, Assurance correlates and analyzes the data.
- **Data Visualization and Action**: Data is stored in databases and exposed through APIs to Assurance as well as other applications for capacity planning. Assurance is an open system that provides:
  - Collector and analytics pipeline SDKs
  - Time-series analysis
  - Graph data models and restful APIs
  - System management portal

IPv6 address support

Catalyst Center, and therefore Cisco Catalyst Assurance, supports IPv6 addresses. A single IPv6 address can be represented in many text formats, but Catalyst Center supports IPv6 addresses in canonical format only. This canonical format is also called the normalized compressed format:

```
2001:db8::1:0:0:1
```

User profile roles and permissions

Catalyst Center supports role-based access control (RBAC). Your user role determines your permissions. Catalyst Center has these three main default user roles:

- SUPER-ADMIN-ROLE
- NETWORK-ADMIN-ROLE, and
- OBSERVER-ROLE.

The SUPER-ADMIN-ROLE allows comprehensive access and supports creating and assigning custom roles in the Catalyst Center GUI. The user roles for NETWORK-ADMIN-ROLE and OBSERVER-ROLE provide limited access.

You can create access groups that limit access to certain network sites. An access group combines a role and a site. You can log in to a specific access group at any time.

Catalyst Center supports these default access groups:

- **NW-ADMIN_Global** - For global access to the role NW-ADMIN
- **OBSERVER_Global** - For global access to the role OBSERVER, and
- **SUPER-ADMIN_Global** - For global access to the role SUPER-ADMIN.

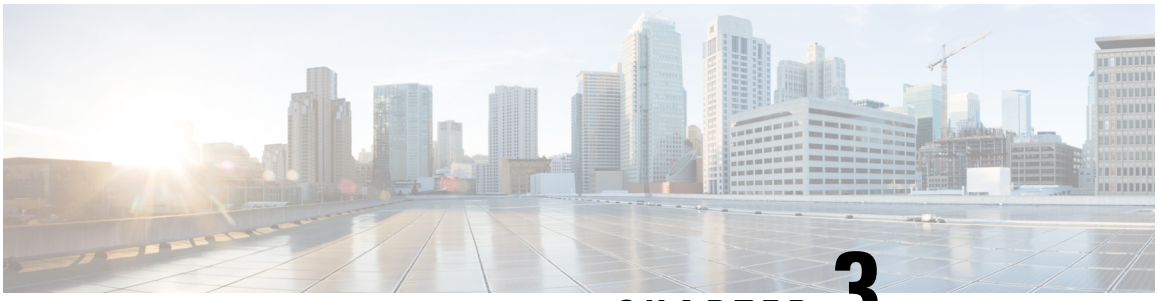
The behavior of Catalyst Center features depends on the user role and site specified in the access group. For more information, see *Configure site-based, role-based access control* in the *Cisco Catalyst Center Administrator Guide*.

Start with Assurance

To start using Assurance, you must first configure the Catalyst Center settings so that the server can communicate outside the network.

After you configure the Catalyst Center settings, your current environment determines how you start using Assurance:

- Existing infrastructure: If you have an existing infrastructure (existing deployment), start by running Discovery. After you run Discovery, all your devices are displayed on the **Inventory** window. For more information, see Basic setup workflow, on page 11.
- New or nonexisting infrastructure: If you do not have an existing infrastructure and are starting from scratch (new deployment), design a network hierarchy. For information about designing a network hierarchy, see the *Cisco Catalyst Center User Guide*.



CHAPTER 3

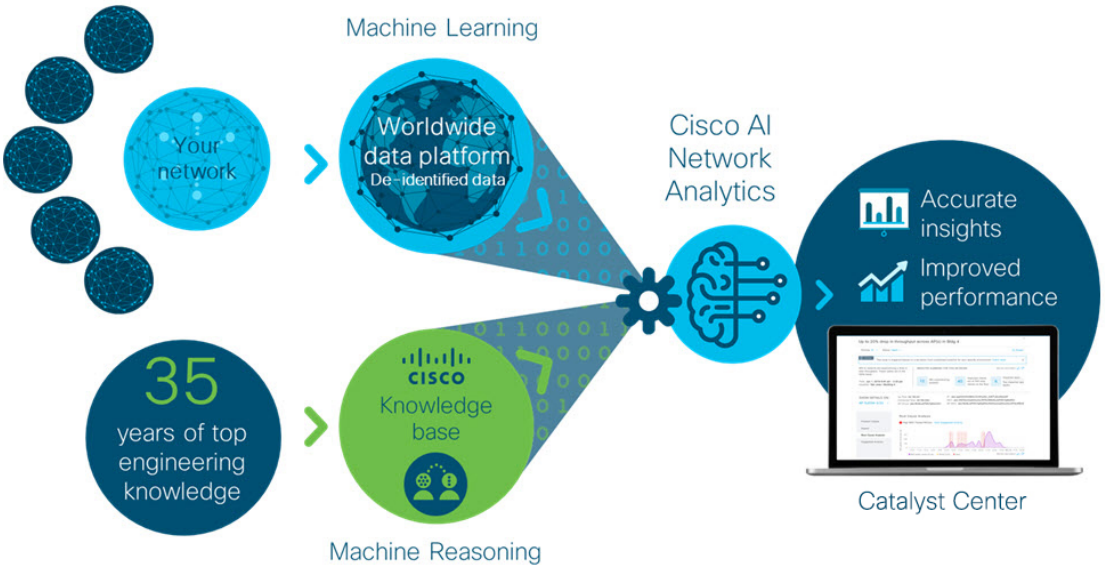
Cisco AI Network Analytics Overview

- About Cisco AI Network Analytics, on page 7
- Cisco AI Network Analytics benefits, on page 9
- Cisco AI Network Analytics licensing and deployment, on page 9

About Cisco AI Network Analytics

Cisco AI Network Analytics is an application within Catalyst Center that leverages the power of machine learning and machine reasoning to provide accurate insights that are specific to your network deployment, which allows you to quickly troubleshoot issues. This figure and the information that follows describes the Cisco AI Network Analytics architecture:

Figure 2: Cisco AI Network Analytics architecture



Cisco AI Network Analytics consists of:

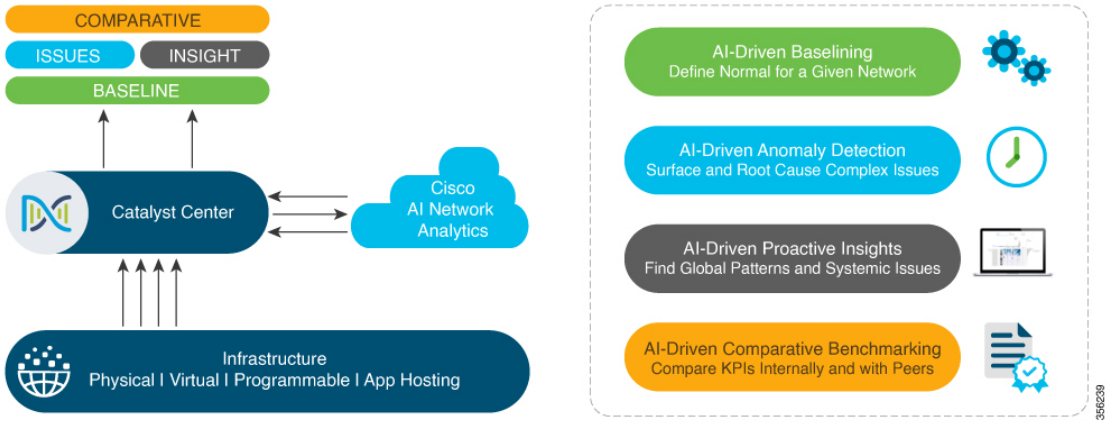
- A worldwide cloud-based data platform where machine learning models are built and analyzed for your specific network environment.

- A machine reasoning inference engine that automates human expertise and captures the workflows in a knowledge base repository.

Machine learning

Cisco AI Network Analytics leverages advanced machine learning techniques and an advanced cloud learning platform with deidentified network event data to identify critical issues in your network. Cisco AI Network Analytics provides a rich set of information so that you can quickly troubleshoot issues, know their root causes, identify trends and insights, and obtain relevant comparative perspectives. Cisco AI Network Analytics provides this value using a simple, intuitive, and powerful user interface within Catalyst Center that is fully integrated with Cisco Catalyst Assurance.

Figure 3: Cisco AI Network Analytics features



Cisco AI Network Analytics provides:

- **Cloud-Based Infrastructure**: Network events information is deidentified in Catalyst Center and sent through a secure encrypted channel to the Cisco AI Network Analytics cloud-based infrastructure. The Cisco AI Network Analytics cloud runs the machine learning model with such deidentified network event data and brings the issues and overall insights back to Catalyst Center.
- **Intelligent Issue Detection and Analysis**, which includes:
  - **AI-Driven Baselining**: Baselining is a method used to analyze network dynamics to extract behavioral patterns that help define what is the *normal* (baseline) behavior for that specific network. The actual network performance is then compared with that baseline.

    Cisco AI Network Analytics uses the most advanced machine learning techniques to define the baseline that is relevant to your specific network and sites with the current conditions. With this information, Cisco AI Network Analytics is able to define what is normal for each network and site at a specific moment, and identify the most important issues.
  - **AI-Driven Anomaly Detection**: Detect anomalies to determine their root causes and ease troubleshooting.

    Cisco AI Network Analytics can detect these types of AI-driven issues:
    - **Connection Issues** (onboarding issues): Excessive Time, Excessive Failures, Excessive DHCP Time, Excessive DHCP Failures, Excessive AAA Time, Excessive AAA Failures, Excessive Association Time, and Excessive Association Failures.

    - **Application Experience Issues**: Total Radio Throughput, Media Application Throughput, Cloud Application Throughput, Collab Application Throughput, and Social Application Throughput.

- **Trends and Insights**, which includes:
    - **Trend Deviations**: Determine global patterns (trends) and deviations to provide system-generated insights.
    - **AP Performance Advisories**: Detect APs that have a consistently poor client experience, and provide a root cause and suggested actions.
- **Comparative Benchmarking**, which includes:
    - **AI-Driven AP Comparisons in Network Heatmaps**: Compare all of the APs in your network for a given month in a heatmap to spot trends and gain insights.
    - **AI-Driven Peer Comparisons**: Determine how your network is doing in comparison to your peer networks for a selected Key Performance Indicator (KPI).
    - **AI-Driven Network Comparisons**: Determine how a network (such as sites, buildings, AP models, client types) is doing compared to another network for a selected KPI.

Cisco AI Network Analytics benefits

Cisco AI Network Analytics provides these benefits:

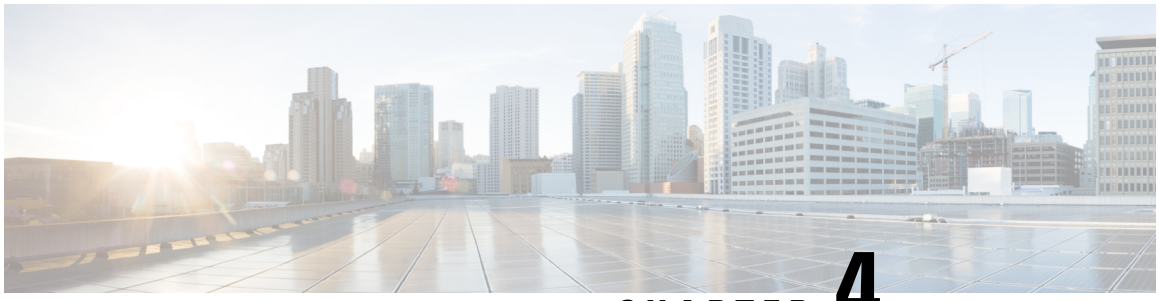
- **More Visibility**: Each network is unique, with the network environment always changing. Cisco AI Network Analytics continuously collects the relevant data from the local networks, correlates the data against the aggregate de-identified data set, and then leverages sophisticated machine learning models to create baselines that are relevant to specific networks and sites. These baselines learn and adapt as the network environments change and as the devices, users, and applications evolve.
- **Greater Insight**: Cisco AI Network Analytics uses machine learning to correlate the immense amount of data that is coming from the network against the individualized network baselines, to uncover the issues that can have the greatest impact on the network. This improves issue relevancy. Cisco AI Network Analytics discovers trends and patterns in the network behavior, so that IT can identify issues before they become a problem.
- **Guided Action**: Cisco AI Network Analytics uses machine learning algorithms and automated workflows to perform logical troubleshooting steps, which enable an engineer to execute and resolve an issue. This helps IT detect issues and vulnerabilities, analyze the root causes, and quickly execute corrective actions.

Cisco AI Network Analytics licensing and deployment

Cisco AI Network Analytics is part of the Advantage software license and is provided as an additional component that seamlessly blends in the Assurance user interface. Cisco AI Network Analytics provides advanced machine learning-generated insights to issues, along with the visualization tools required for analyzing, troubleshooting, and reacting to the issues raised by the machine learning engines.

Deploying Cisco AI Network Analytics requires a working instance of Catalyst Center (which runs in an appliance form factor) as well as HTTPS connectivity to the Cisco AI Network Analytics cloud. HTTPS connectivity is also supported through a proxy server. If you use the proxy server for HTTPS connectivity, the settings are inherited from the Catalyst Center global settings. Network event data is deidentified before it is sent to the cloud. Results and insights are returned by the Cisco AI Network Analytics cloud services, and are displayed after decryption, directly into the Assurance user interface. For more information, see Cisco Catalyst Center Offer Disclosure.

Cisco AI Network Analytics requires connectivity to the cloud infrastructure for storage and analysis. If you have less than 500 wireless APs, you can expect data usage of only 150-200 MB per day due to efficient encoding and optimization schemes. Data usage is proportional to network deployment size in terms of APs and wireless clients; therefore, larger deployments with 1800 APs have a data usage of 500-700 MB per day.



CHAPTER 4

Set Up Catalyst Center to Use Assurance

- Limitations and restrictions of Assurance, on page 11
- Basic setup workflow, on page 11
- Discover devices, on page 14
- Network hierarchy, on page 30
- Manage Inventory, on page 53
- Assign an unprovisioned device to a site, on page 65
- Add APs to a map, on page 67
- Position an AP on a map, on page 68
- About Cisco ISE configuration for Catalyst Center, on page 72
- Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry, on page 76
- Configure Cisco AI Network Analytics, on page 77
- Update the Machine Reasoning Knowledge Base, on page 80
- Enable localization, on page 81

Limitations and restrictions of Assurance

Assurance does not support devices that are connected through Network Address Translation (NAT).

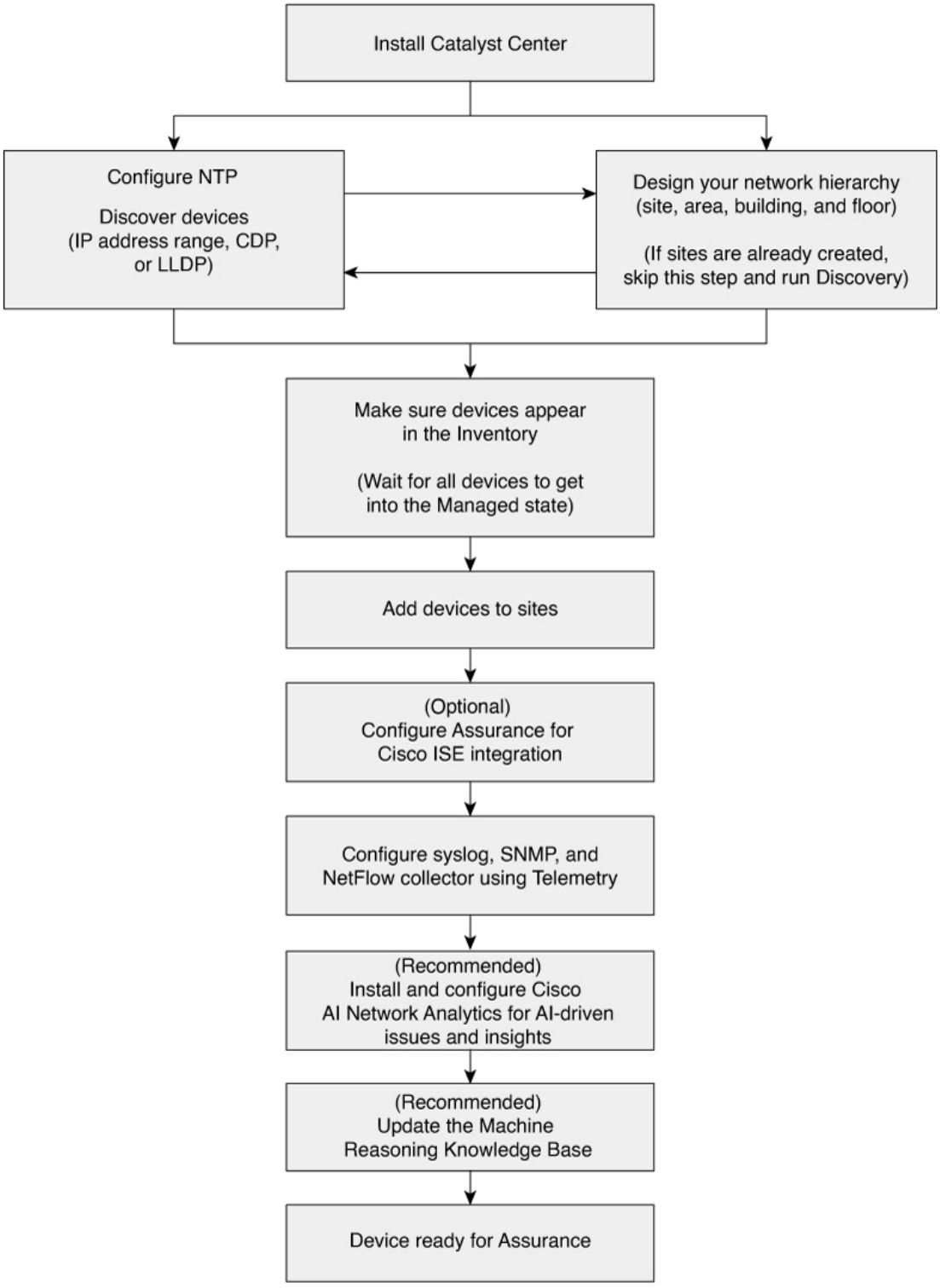
Basic setup workflow

Before you begin using the Assurance application, you must set up Catalyst Center to use Assurance.

This chapter provides the basic tasks you must do to set up Assurance. Use this chapter in conjunction with the *Cisco Catalyst Center User Guide*.

See this illustration and the procedure that follows to understand the basic workflow.

Figure 4: Basic workflow for setting up Catalyst Center to use Assurance



Before you begin

See Limitations and restrictions of Assurance, on page 11.

Procedure

Step 1 Install Catalyst Center.

See the *Cisco Catalyst Center Installation Guide*.

Step 2 Do these tasks in any order:

- Confirm that Catalyst Center and the devices it manages are synchronized with Network Time Protocol (NTP).
- Discover devices (routers, switches, wireless controllers, and access points).

  See Discover your network using an IP address range or CIDR, on page 24, Discover your network using CDP, on page 21 and Discover your network using LLDP, on page 26.

  Note
  Cisco Wireless Controllers must be discovered using the management IP address instead of the service port IP address. If not, the related wireless controller 360 and AP 360 windows will not display any data.

- Design a new network hierarchy or use an existing one.

  See Create the network hierarchy, on page 32 or Existing Cisco network hierarchies, on page 36.

  Note
  If sites are already created, you can skip this step and run Discovery.

Step 3 Make sure that the devices appear in the device Inventory.

See Display information about your inventory, on page 55.

Note
Before you add devices to sites, you must wait for all the devices to get into a Managed state.

Step 4 Add devices to sites.

See Assign an unprovisioned device to a site, on page 65.

Step 5 If you have APs, we recommend that you add them to a floor map.

See Add APs to a map, on page 67.

Step 6 If your network uses Cisco Identity Services Engine (ISE) for user authentication, you can configure Assurance for Cisco ISE integration. This enables you to see more information about wired clients, such as the username and operating system, in Assurance.

See About Cisco ISE configuration for Catalyst Center, on page 72.

Step 7 Configure the syslog, SNMP traps, and NetFlow Collector servers using Telemetry.

See Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry, on page 76.

Step 8 (Recommended) To view AI-driven issues and gain network insights, configure Cisco AI Network Analytics data collection.

See Configure Cisco AI Network Analytics, on page 77.

Step 9 (Recommended) To have access to the latest Machine Reasoning workflows, update the Machine Reasoning Knowledge Base.

See Update the Machine Reasoning Knowledge Base, on page 80.

Step 10 Start using the Assurance application.

Discover devices

Use the Catalyst Center Discovery feature to scan the devices in your network.

Discovery overview

Discovery scans the devices in your network and sends the list of discovered devices to inventory.

Discovery also works with Device Controllability to configure the required network settings on devices when these settings are missing from devices.

There are four ways to discover devices:

- Use Cisco Discovery Protocol (CDP) and provide a seed IP address.
- Specify a range of IP addresses. You can include up to 4096 devices in the range.
- Use Link Layer Discovery Protocol (LLDP) and provide a seed IP address.
- Use Classless Inter-Domain Routing (CIDR) and provide a seed IP address.

When you configure the Discovery criteria, you can use settings to reduce the time needed to discover devices:

- **CDP Level** and **LLDP Level**: If you use CDP or LLDP as the Discovery method, you can set the CDP or LLDP level to indicate the number of hops from the seed device that you want to scan. The default, level 16, might take a long time on a large network. If you need to discover fewer devices, set the level to a lower value.
- **Prefix Length**: If you use **CIDR** as a discovery method, you can set the prefix length value, which ranges from 20 to 30. The default value is 30.
- **Subnet Filters**: If you use an IP address range, you can specify devices in specific IP subnets for Discovery to ignore.
- **Preferred Management IP**: Whether you use CDP, LLDP, CIDR, or an IP address range, you can specify whether you want Catalyst Center to add any of the device's IP addresses or only the device loopback address.

Note For Cisco SD-Access Fabric and Cisco Catalyst Assurance, specify the device loopback address.

Regardless of the method you use, you must be able to reach the device from Catalyst Center and configure specific credentials and protocols in Catalyst Center to discover your devices. These credentials can be configured and saved in the **Design** > **Network Settings** > **Device Credentials** window or on a per job basis in the **Discovery** window.

Note If a device uses a first hop resolution protocol, such as Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP), the device can be discovered and added to the inventory along with its floating IP address. Later, if HSRP or VRRP fails, the IP address might be reassigned to a different device. This situation can cause issues with the data that Catalyst Center retrieves for analysis.

Discovery prerequisites

Before you run Discovery, complete these minimum prerequisites:

- View the *Cisco Catalyst Center Compatibility Matrix* to understand which devices will be discovered by Catalyst Center.
- Understand that the preferred network latency between Catalyst Center and devices is 100 ms round-trip time (RTT). (The maximum latency is 200 ms RTT.)
- Ensure that at least one SNMP credential is configured on your devices for use by Catalyst Center. At a minimum, this configuration can be an SNMPv2C read credential.
- To allow Catalyst Center to discover and manage devices, configure SSH credentials on them. Catalyst Center discovers and adds a device to its inventory if at least one of these criteria is met:
  - The account that is being used by Catalyst Center to SSH into your devices has privileged EXEC mode (level 15).
  - You configure the device's enable password as part of the CLI credentials configured in the Discovery job. For more information, see Discovery configuration guidelines and limitations, on page 16.
- In a dual-stack IPv4/IPv6 environment, note these points:
  - During a single discovery session, if a device is reachable via both IPv4 and IPv6, Catalyst Center retains only the first address family detected. To prevent duplicate device entries, Catalyst Center ignores the secondary address family.
  - For site-based, role-based access control (SRBAC), discovery is restricted by site access groups. A device already discovered under one site access group cannot be rediscovered or managed under a different site access group.
  - When the loopback option is enabled, the system defaults to IPv6. If an IPv6 loopback is unavailable, the system automatically falls back to IPv4.
  - Catalyst Center supports cross-family neighbor discovery. Discovery sessions seeded with IPv4 can identify IPv6 neighbors, and sessions seeded with IPv6 can identify IPv4 neighbors via CDP or LLDP.

Preferred management IP address

When Catalyst Center discovers a device, it uses one of the device IP addresses as the preferred management IP address. The IP address can be that of a built-in management interface of the device, another physical interface, or a logical interface such as Loopback0. You can configure Catalyst Center to use the device loopback IP address as the preferred management IP address, provided the IP address is reachable from Catalyst Center.

When you select **Use Loopback IP** as the preferred management IP address, Catalyst Center determines the preferred management IP address as detailed in this table:

Table 2: Preferred management IP address determination criteria

If	Then
If the device has one loopback interface	Catalyst Center uses that loopback interface IP address.
If the device has multiple loopback interfaces	Catalyst Center uses the loopback interface with the highest IP address.
If there is no loopback interface	Catalyst Center uses the Ethernet interface with the highest IP address. (Subinterface IP addresses are not considered.) The system also uses the loopback interface with the highest IP address.
If there are no Ethernet interfaces	Catalyst Center uses the serial interface with the highest IP address.

After a device is discovered, you can update the management IP address from the **Inventory** window.

Discovery configuration guidelines and limitations

This section describes the limitations and guidelines of device discovery.

- These are the guidelines and limitations for Catalyst Center to discover your Cisco Catalyst 3000 Series Switches and Catalyst 6000 Series Switches:
    - Configure the CLI username and password with privileged EXEC mode (level 15). These credentials are the same CLI username and password that you configure in Catalyst Center for the Discovery function. Catalyst Center requires the highest access level to the device.
    - Explicitly specify the transport protocols allowed on individual interfaces for both incoming and outgoing connections. Use the **transport input** and **transport output** commands for this configuration. For information about these commands, see the command reference document for the specific device type.
    - Don’t change the default login method for a device's console port and the VTY lines. If a device is already configured with a AAA (TACACS) login, make sure that the CLI credential defined in the Catalyst Center is the same as the TACACS credential defined in the TACACS server.
- These are the guidelines and limitations for Catalyst Center to discover your wireless controllers and APs:

- Cisco Wireless Controllers must be discovered using the management IP address instead of the service port IP address. If not, the related wireless controller 360 and AP 360 windows won't display any data.
- After the wireless controllers are discovered, Catalyst Center displays the list of associated APs in the inventory. The listed APs are connected to the wireless controller either during the discovery or through inventory sync.

Note For any new APs that join the wireless controller after the inventory sync:

- If the wireless controller isn't assigned to a site or provisioned in Catalyst Center, you must do a manual resync.
- If the wireless controller is assigned to a site, when a new AP joins the wireless controller, an SNMP trap is triggered. Using this SNMP trap, Catalyst Center discovers the newly joined AP. A manual resync isn't necessary.
- If the wireless controller is assigned to a site, Device Controllability must be enabled. If Device Controllability is disabled during the site assignment and later enabled, you must manually sync new APs.

- Third-party devices can't be discovered with the Catalyst Center discovery feature. You must add the third-party devices manually to your network. For more information, see "Add a Third-Party Device" in the *Cisco Catalyst Center User Guide*.

Discovery credentials

Discovery credentials are the CLI, SNMPv2c, SNMPv3, HTTP, HTTPS, and NETCONF configuration values for the devices that you want to discover. You must specify the credentials based on the types of devices you are trying to discover:

- Network devices: CLI and SNMP credentials.

Note For NETCONF-enabled devices such as embedded wireless controllers, you must specify SSH credentials with admin privilege and select the NETCONF port.

- Compute devices (NFVIS): CLI, SNMP, HTTP, and HTTPS credentials.

Because the various devices in a network can have different sets of credentials, you can configure multiple sets of credentials in Catalyst Center. The discovery process iterates through all sets of credentials that are configured for the Discovery job until it finds a set that works for the device.

If you use the same credential values for the majority of devices in your network, you can configure and save them to reuse in multiple Discovery jobs. To discover devices with unique credentials, you can add job-specific Discovery credentials when you run Discovery jobs. You can configure up to 10 global credentials for each credential type and define any five of them. If you need to define a job-specific credential, you can define five global credentials and one job-specific credential for each credential type.

To define credentials for a Discovery, click the menu icon and choose **Tools** > **Discovery** > **Add Discovery**. To continue, use these procedures and discovery credential information:

- Discover your network using CDP, on page 21
- Discover your network using an IP address range or CIDR, on page 24
- Discover your network using LLDP, on page 26

Table 3: CLI credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials. If authentication fails for CLI, Catalyst Center retries the authentication process for 300 seconds (5 minutes).
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it. For security reasons, re-enter the enable password. **Note** Passwords are encrypted for security reasons and are hidden in the configuration.

Table 4: SNMPv2c credentials

Field	Description
Read	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Read Community**: Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are hidden in the configuration.
Write	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Write Community**: Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are hidden in the configuration.

Table 5: SNMPv3 credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Select one of these modes: • **Authentication and Privacy**: Provides both authentication and encryption. • **Authentication, No Privacy**: Provides authentication, but does not provide encryption. • **No Authentication, No Privacy**: Does not provide authentication or encryption.
Auth. Type	Authentication type to be used. (Enabled if you select **Authentication and Privacy** or **Authentication, No Privacy** as **Mode**.) Select one of these authentication types: • **SHA**: Authentication based on HMAC-SHA. • **SHA256**: Authentication based on HMAC-SHA256. • **MD5 (not recommended)**: Authentication based on HMAC-MD5.
Auth. Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are hidden in the configuration.
Privacy Type	Privacy type. (Enabled if you select **Authentication and Privacy** as **Mode**.) Select one of these privacy types: • **AES128**: 128-bit CBC mode AES for encryption. • **CISCOAES192**: 192-bit CBC mode AES for encryption on Cisco devices. • **CISCOAES256**: 256-bit CBC mode AES for encryption on Cisco devices.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are hidden in the configuration.

Table 6: SNMP properties

Field	Description
Retries	Number of times Catalyst Center tries to communicate with network devices using SNMP.
Timeout (in Seconds)	Amount of time, in seconds, between retries.

Table 7: HTTP and HTTPS credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are **Read** or **Write**.
Read	You can configure up to 10 HTTPS read credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain between 7 and 128 characters, including at least one of these characters: • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? – **Note** The password cannot contain spaces or angle brackets (< >). Some Cisco IOS XE devices do not allow a question mark (?).

Field	Description
Write	You can configure up to 10 HTTPS write credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain between 7 and 128 characters, including at least one of these characters: • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? – **Note** The password cannot contain spaces or angle brackets (< >). Some Cisco IOS XE devices do not allow a question mark (?).

Table 8: NETCONF setting

Field	Description
Port	Port on the device. You can use one of these ports: • Port 830 (default). • Any other port that is available on the device. • A custom port that Catalyst Center configures. (You can use a custom port only if Device Controllability is enabled. For more information, see the Device Controllability section in the *Cisco Catalyst Center Administrator Guide*.) If authentication fails for NETCONF, Catalyst Center retries the authentication process for 300 seconds (5 minutes).

Discover your network using CDP

You can discover devices using Cisco Discovery Protocol (CDP), an IP address range, CIDR, or LLDP. This procedure shows you how to discover devices and hosts using CDP. For more information about the other discovery methods, see Discover your network using an IP address range or CIDR, on page 24 and Discover your network using LLDP, on page 26.

Note

- The Discovery function requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a *best effort*, the Discovery function uses the default SNMP RO community string, public.
- CLI credentials are not required to discover hosts; hosts are discovered through the network devices to which they are connected.

Before you begin

- Enable CDP on your network devices.
- Configure your network devices, as described in Discovery prerequisites, on page 15.
- Configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)

Procedure

Step 1 From the main menu, choose **Tools** > **Discovery**.

Step 2 In the **Discovery** window, click **Add Discovery**.

Step 3 In the **Discover Devices** window, complete these fields:

a) Enter a name for the discovery job.

b) Under **Discovery Type**, select **CDP**.

c) In the **IP Address** field, enter a seed IP address for Catalyst Center to start the Discovery scan.

d) (Optional) In the **Subnet Filter** field, enter an IP address or subnet to exclude from the Discovery scan.

You can enter addresses either as an individual IP address (*x.x.x.x*) or as a classless inter-domain routing (CIDR) address (*x.x.x.x/y*), where *x.x.x.x* refers to the IP address and *y* refers to the subnet mask. The subnet mask can be a value from 20 to 32.

e) Click .

Repeat Step d and Step e to exclude multiple subnets from the Discovery job.

f) (Optional) In the **CDP Level** field, enter the number of hops from the seed device that you want to scan.

Valid values are from 1 to 16. The default value is 16. For example, CDP level 3 means that CDP will scan up to three hops from the seed device.

g) For **Preferred Management IP**, select one of these options:

Option	Description
None	Allows the device to use any of its IP addresses.

Option	Description
Use Loopback IP	Specify the device's loopback interface IP address. **Note** If you select **Use Loopback IP** and the device does not have a loopback interface, Catalyst Center selects a management IP address using the logic described in Preferred management IP address, on page 16. **Note** To use the loopback interface IP address as the preferred management IP address, make sure that the CDP neighbor's IP address is reachable from Catalyst Center.

Step 4 In the **Provide Credentials** window, configure the discovery credentials and other settings as required.

Enter at least one CLI credential and one SNMP credential for Catalyst Center to configure for the devices it discovers. You can have a maximum of five global credentials and one task-specific credential for each type. For more details, see Discovery credentials, on page 17.

a) In the left pane, click **CLI** to add CLI credentials.
b) Expand **SNMP** to add SNMP credentials.
c) Expand **Advanced Settings** and configure these settings:

Setting	Task
Protocol Order	Select **SSH** or **Telnet**. If you select both, you can specify the order in which they are used by dragging the protocols up or down.
SNMP Polling Properties	Use the global SNMP polling properties defined in the **Network Settings** > **Device Credentials** window or modify for this discovery instance.

Note
You can configure other credentials such as, NETCONF, HTTP, and HTTPS, if required.

Step 5 In the **Schedule Job** window, do these steps:

a) Click **Now** to start device discovery immediately or click **Later** to schedule device discovery at a specific time.

If you select the **Daily** or **Weekly** recurrence option, the **Discover new devices only** option is disabled.

b) Click the toggle button to enable or disable the **Discover new devices only** option.
c) Click the **Assign devices to an existing site** link.

The **Visibility and Control of Configurations** dialog box appears with information about the settings that enable on the devices during site assignment. If Visibility of Configurations is enabled and a site is assigned during discovery, a configuration preview is not generated.

During the discovery workflow, devices can be assigned to existing sites only, new site creation is not supported.

In the dialog box, select any one of these options:

Option	Task
Assign to site without Configuration Preview	Use the **Search Hierarchy** search field or the filter icon to find a site, building, or area. For more details, see Search the network hierarchy.
Skip site assignment for now	Use this option if you want the devices to be assigned to sites later from inventory.

Step 6 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 7 Click **Start Discovery**.

You can view the status of the task in the **Activities** > **Tasks** window.

What to do next

The **Device Discovery** window displays an option to view the discovered devices based on the site assignment. Use this option to view devices assigned to a site or a network or the unassigned devices in the inventory.

Discover your network using an IP address range or CIDR

You can discover devices and hosts using an IP address range, CIDR, CDP, or LLDP. This procedure explains how to perform discovery using an IP address range or CIDR. For more information about the other Discovery methods, see Discover your network using CDP, on page 21, and Discover your network using LLDP, on page 26.

Before you begin

Your devices must have the required device configurations, as described in Discovery prerequisites, on page 15.

Procedure

Step 1 From the main menu, choose **Tools** > **Discovery**.

Step 2 In the **Discovery** window, click **Add Discovery**.

Step 3 In the **Discover Devices** window, complete these fields:

a) Enter a name for the discovery job.

b) Under **Discovery Type**, choose **IP Address/Range**, or **CIDR**.

c) If you choose **IP Address/Range** discovery type, do these steps:

1. In the **From** and **To** fields, enter the beginning and ending IP addresses (IP address range) for Catalyst Center to scan, and click .

   You can enter a single IP address range or multiple IP addresses for the discovery scan.

   Note

Cisco Wireless Controllers must be discovered using the Management IP address instead of the Service Port IP address. If not, the related wireless controller 360 and AP 360 pages will not display any data.

2. (Optional) To enter additional IP address ranges, repeat the previous step.

d) If you choose **CIDR** discovery type, do these steps:

1. In the **IP Address** field, enter a seed IP address for Catalyst Center to start the Discovery scan.
2. In the **Subnet Filter** field, enter an IP address or subnet to exclude from the Discovery scan.

   You can enter addresses either as an individual IP address (*x.x.x.x*) or as a classless inter-domain routing (CIDR) address (*x.x.x.x/y*), where *x.x.x.x* refers to the IP address and *y* refers to the subnet mask. The subnet mask can be a value from 20 to 32.

3. Click .

   (Optional) To exclude additional subnets from the Discovery job, repeat the previous steps.

4. In the **Prefix Length** field, enter a value between 20 and 30.

e) For **Preferred Management IP Address**, select one of these options:

- **None**: Allows the device to use any of its IP addresses.
- **Use Loopback IP**: Specify the device's loopback interface IP address.

Note
If you choose **Use Loopback IP** and the device does not have a loopback interface, Catalyst Center chooses a management IP address using the logic described in Preferred management IP address, on page 16.

Step 4 In the **Provide Credentials** window, configure the discovery credentials and other settings as required.

Enter at least one CLI credential and one SNMP credential for Catalyst Center to configure for the devices it discovers. You can have a maximum of five global credentials and one task-specific credential for each type. For more details, see Discovery credentials, on page 17.

a) In the left pane, click **CLI** to add CLI credentials.
b) Expand **SNMP** to add SNMP credentials.
c) Expand **Advanced Settings** and configure these settings:

Setting	Task
Protocol Order	Select **SSH** or **Telnet**. If you select both, you can specify the order in which they are used by dragging the protocols up or down.
SNMP Polling Properties	Use the global SNMP polling properties defined in the **Network Settings** > **Device Credentials** window or modify for this discovery instance.

Note
You can configure other credentials such as, NETCONF, HTTP, and HTTPS, if required.

Step 5 In the **Schedule Job** window, do these steps:

a) Click **Now** to start device discovery immediately or click **Later** to schedule device discovery at a specific time.

If you select the **Daily** or **Weekly** recurrence option, the **Discover new devices only** option is disabled.

b) Click the toggle button to enable or disable the **Discover new devices only** option.

c) Click the **Assign devices to an existing site** link.

The **Visibility and Control of Configurations** dialog box appears with information about the settings that enable on the devices during site assignment. If Visibility of Configurations is enabled and a site is assigned during discovery, a configuration preview is not generated.

During the discovery workflow, devices can be assigned to existing sites only, new site creation is not supported.

In the dialog box, select any one of these options:

Option	Task
Assign to site without Configuration Preview	Use the **Search Hierarchy** search field or the filter icon to find a site, building, or area. For more details, see Search the network hierarchy.
Skip site assignment for now	Use this option if you want the devices to be assigned to sites later from inventory.

Step 6 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 7 Click **Start Discovery**.

The status of the task displays in the **Activities** > **Tasks** window.

What to do next

The **Device Discovery** window displays an option to view the discovered devices based on the site assignment. Use this option to view devices assigned to a site or a network or the unassigned devices in the inventory.

Discover your network using LLDP

You can discover devices using Link Layer Discovery Protocol (LLDP), CDP, CIDR, or an IP address range. This procedure describes how to discover devices and hosts using LLDP. For more information about the other discovery methods, see Discover your network using CDP, on page 21 and Discover your network using an IP address range or CIDR, on page 24.

Note

- The Discovery function requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a *best effort*, the Discovery function uses the default SNMP RO community string, public.
- CLI credentials are unnecessary for host discovery. The system discovers hosts by using the network devices they are connected to.

Before you begin

- Enable the LLDP protocol on your network devices.
- Configure your network devices according to Discovery prerequisites, on page 15.
- Configure your network device host IP address as the client IP address. A host is an end-user device, such as a laptop computer or mobile device.

Procedure

Step 1 From the main menu, choose **Tools** > **Discovery**.

Step 2 In the **Discovery** window, click **Add Discovery**.

Step 3 In the **Discover Devices** window, complete these fields:

a) Enter a name for the discovery job.

b) Under **Discovery Type**, select **LLDP**.

c) In the **IP Address** field, enter a seed IP address for Catalyst Center to start the Discovery scan.

d) (Optional) In the **Subnet Filter** field, enter an IP address or subnet to exclude from the Discovery scan.

Enter addresses as individual IP addresses (*x.x.x.x*) or as a classless inter-domain routing (CIDR) address (*x.x.x.x/y*). In a CIDR address, *x.x.x.x* refers to the IP address, and *y* refers to the subnet mask. The subnet mask can be a value from 20 to 32 bits.

e) Click .

Repeat both Step c and Step d to exclude multiple subnets from the Discovery job.

f) (Optional) In the **LLDP Level** field, enter the number of hops from the seed device to scan.

Valid values are from 1 to 16. The default value is 16. For example, LLDP level 3 means that LLDP scans up to three hops from the seed device.

g) For **Preferred Management IP**, select one of these options:

- **None**: Allows the device use any of its IP addresses.
- **Use Loopback IP**: Specify the loopback interface IP address for the device.

Note
If you select this option and the device does not have a loopback interface, Catalyst Center selects a management IP address using the logic described in Preferred management IP address, on page 16.

Note
To use the loopback interface IP address as the preferred management IP address, make sure that the IP address of the LLDP neighbor is reachable from Catalyst Center.

Step 4 In the **Provide Credentials** window, configure the discovery credentials and other settings as required.

Enter at least one CLI credential and one SNMP credential for Catalyst Center to configure for the devices it discovers. You can have a maximum of five global credentials and one task-specific credential for each type. For more details, see Discovery credentials, on page 17.

a) In the left pane, click **CLI** to add CLI credentials.

b) Expand **SNMP** to add SNMP credentials.
c) Expand **Advanced Settings** and configure these settings:

Setting	Task
Protocol Order	Select **SSH** or **Telnet**. If you select both, you can specify the order in which they are used by dragging the protocols up or down.
SNMP Polling Properties	Use the global SNMP polling properties defined in the **Network Settings** > **Device Credentials** window or modify for this discovery instance.

Note
You can configure other credentials such as, NETCONF, HTTP, and HTTPS, if required.

Step 5 In the **Schedule Job** window, do these steps:

a) Click **Now** to start device discovery immediately or click **Later** to schedule device discovery at a specific time.

If you select the **Daily** or **Weekly** recurrence option, the **Discover new devices only** option is disabled.

b) Click the toggle button to enable or disable the **Discover new devices only** option.
c) Click the **Assign devices to an existing site** link.

The **Visibility and Control of Configurations** dialog box appears with information about the settings that enable on the devices during site assignment. If Visibility of Configurations is enabled and a site is assigned during discovery, a configuration preview is not generated.

During the discovery workflow, devices can be assigned to existing sites only, new site creation is not supported.

In the dialog box, select any one of these options:

Option	Task
Assign to site without Configuration Preview	Use the **Search Hierarchy** search field or the filter icon to find a site, building, or area. For more details, see Search the network hierarchy.
Skip site assignment for now	Use this option if you want the devices to be assigned to sites later from inventory.

Step 6 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 7 Click **Start Discovery**.

You can view the status of the task in the **Activities** > **Tasks** window.

What to do next

The **Device Discovery** window displays an option to view the discovered devices based on the site assignment. Use this option to view devices assigned to a site or a network or the unassigned devices in the inventory.

Manage Discovery jobs

These sections provide information about how to manage the Discovery jobs.

Stop and start a Discovery job

Procedure

Step 1 From the main menu, choose **Tools** > **Discovery**.

Step 2 To stop an active Discovery job, hover your cursor over the ellipsis icon (•••) in the **Actions** column and select **Stop Discovery**.

Step 3 To restart an inactive Discovery job, hover your cursor over the ellipsis icon in the **Actions** column and select **Re-discover**.

Clone a Discovery job

You can clone a Discovery job to retain all the information defined for that job.

Before you begin

Run at least one Discovery job.

Procedure

Step 1 From the main menu, choose **Tools** > **Discovery**.

Step 2 To copy a Discovery job, hover your cursor over the ellipsis icon (•••) in the **Actions** column and select **Copy & Edit**.

Catalyst Center creates a copy of the Discovery job named "Clone of *Discovery_Job*."

Step 3 (Optional) To change the name of the Discovery job, replace the default name in the **Discovery Name** field with a new name.

Step 4 Define or update the parameters for the new Discovery job.

Delete a Discovery job

You can delete a Discovery job regardless of whether it is active or inactive.

Procedure

Step 1 From the main menu, choose **Tools** > **Discovery**.

Step 2 To delete a Discovery job, hover your cursor over the ellipsis icon (•••) in the **Actions** column and select **Delete**.

Step 3 Click **OK** to confirm.

View Discovery job information

You can view information about a Discovery job, such as the settings and credentials that were used. You also can view the historical information about each Discovery job that was run, including information about the specific devices that were discovered or that failed to be discovered.

Before you begin

Run at least one Discovery job.

Procedure

Step 1 From the main menu, choose **Tools** > **Discovery**.

Step 2 In the **Discovery** window, click **All discoveries page from previous release**.

Step 3 In the left **Discoveries** pane, select the Discovery job. Alternatively, use the **Search** function to find a Discovery job by device IP address or name.

Step 4 Click the down arrow next to one of these areas for more information:

- **Discovery Details**: Displays the parameters that were used to run the Discovery job. Parameters include attributes such as the CDP or LLDP level, IP address range, and protocol order.
- **Credentials**: Provides the names of the credentials that were used.
- **History**: Lists each Discovery job that was run, including the time the job started, and whether any devices were discovered.

  To successfully discover embedded wireless controllers, the NETCONF port must be configured. If the NETCONF port is not configured, wireless data is not collected.

  Use the **Filter** function to display devices by any combination of IP addresses or ICMP, CLI, HTTPS, or NETCONF values.

Network hierarchy

You can create a network hierarchy that represents the geographical locations of your network.

Structure of a network hierarchy

The network hierarchy consists of sites. A site may refer to an area, building, floor, or an outdoor area. The placement of each site depends on network hierarchy rules. Refer to the figure and table to learn how to structure sites in your network hierarchy.

Figure 5: Network hierarchy

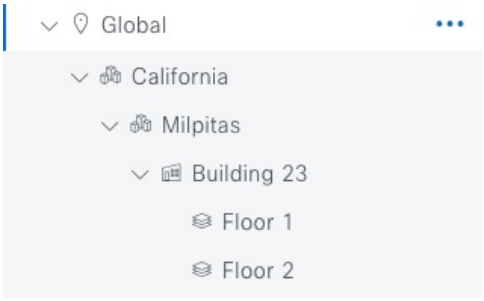


Table 9: Network hierarchy elements

Site types	Description	Rule
Global ( )	The default site element under which all other site elements reside.	Only areas and buildings can reside directly under **Global**.
Areas ( )	Areas identify a geographic region. They group other areas, buildings, or both. Therefore, they do not have a physical address.	Areas can reside directly under **Global** or other areas.
Buildings ( )	Buildings can have physical addresses or latitude and longitude coordinates.	Buildings can reside directly under **Global** or areas. They cannot contain areas, but they can contain floors or outdoor areas.
Outdoor Areas ( )	Outdoor areas can be added with physical address or latitude and longitude coordinates and with or without an image map.	Outdoor areas can reside under **Global** or under areas or buildings. You can add them with or without maps. If you decide to use maps, you can manually create them or import them from files, such as DXF, DWG, JPG, GIF, PNG, or PDF file formats. Then you can position your wireless devices on the maps to visualize your wireless network coverage. You cannot add site elements under outdoor areas and cannot move an existing outdoor area from one site to another.

Site types	Description	Rule
Floors ( )	Floors can be added to buildings with or without a background image that contains various building components, like walls and windows. Floor maps let you visualize wireless network coverage based on the position of your wireless devices on the floor map. You can manually create floor maps or add them from a background image, such as DXF, DWG, JPG, GIF, PNG, or PDF file formats.	Only floors reside under buildings. **Note** • You cannot move an existing floor to a different building. • You can change the site hierarchy for unprovisioned devices while preserving AP locations on floor maps.

Apply design settings to a site

The network hierarchy lets you apply design settings to a specific site. For example, you can apply design settings to an entire area or to a single floor.

Tip Naming hierarchical sites can help you identify where to apply design settings later.

Build your network hierarchy

To get started, build your network hierarchy using one of these methods:

- Create the network hierarchy. For more information, refer to Create the network hierarchy, on page 32.
- Import an existing network hierarchy from Cisco Prime Infrastructure or Ekahau Pro. For more information, refer to Existing Cisco network hierarchies, on page 36 or Use an existing Ekahau network hierarchy, on page 39.

Create the network hierarchy

Create the network hierarchy by creating new areas, buildings, and floors.

Create, edit, and delete a site

Catalyst Center allows you to easily define physical sites and then specify common resources for those sites. The **Design** area uses a hierarchical format for intuitive use, while eliminating the need to redefine the same resource in multiple places when provisioning devices. By default, there is one site called **Global**. You can add more sites, buildings, and areas to your network hierarchy. You must create at least one site before you can use the provision features.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

A world map appears in the right pane.

Step 2 From this window, you can add, edit, and delete sites. See this table for details.

Action	Steps
Add a site.	**a.** From the map toolbar, click **+ Add Site** > **Add Area**. Alternatively, you can hover your cursor over the ellipsis ••• next to the parent site in the left pane, and select **Add Area**. **b.** In the **Area Name** field, enter the site name. The **Area Name** field has restrictions, including: • The area name cannot exceed 40 characters. • Special characters & > < ? ' " / [ ] aren't allowed. **c.** From the **Parent** drop-down list, select a parent node. **Global** is the default parent node. **d.** Click **Add**.
Edit a site.	**a.** In the left pane, hover your cursor over the ellipsis ••• next to the site and select **Edit Area**. **b.** In the **Edit Area** dialog box, make the necessary edits. **c.** Click **Update**.
Delete a site.	**a.** In the left pane, hover your cursor over the ellipsis ••• next to the site and select **Delete Area**. **b.** Click **OK**.

Note

After you create the network hierarchy, you can move the sites between different parent sites only when:

- The new parent site has the same network settings as the current parent site.
- The new parent site has the same network profiles assigned as the site being moved.

Add, edit, and delete a building

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From this window, you can add, edit, and delete a building. See this table for details.

Action	Steps
Add a building.	**a.** In the **Network Hierarchy** window, click **+Add Site** > **Add Building**. Alternatively, you can hover your cursor over the ellipsis ••• next to the parent site in the left pane, and select **Add Building**. **b.** In the **Add Building** dialog box, add the building details. The **Building Name** field has restrictions, including: • The building name cannot exceed 40 characters. • Special characters & > < ? ' " / [ ] aren't allowed. You can enter the address in the field or click the map. Adding an address causes the **Longitude** and **Latitude** coordinate fields to be automatically populated. These coordinates correspond to the northwest corner of the building and are used by location services, such as Cisco Spaces or Cisco Connected Mobile Experiences (CMX), if they are integrated with Catalyst Center. **c.** Click **Add**.
Edit a building.	**a.** In the left pane, hover your cursor over the ellipsis ••• next to the site and select **Edit Building**. **b.** In the **Edit Building** dialog box, make the necessary edits. **c.** Click **Update**.
Delete a building.	**a.** In the left pane, hover your cursor over the ellipsis ••• next to the building and select **Delete Building**. **b.** Click **OK**.

Add, edit, and delete a floor

After you add a building, you can add floors to it. You can add a basic floor that doesn't have a floor map and add the floor map later, or you can add a floor and include a floor map at the same time.

To add a basic floor to a building, use this procedure.

To add a floor and a floor map at the same time, see the *Cisco Catalyst Center User Guide*.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From this window, you can add, edit, and delete a floor. See this table for details.

Action	Steps
Add a basic floor	**a.** In the left pane, hover your cursor over the ellipsis ••• next to the desired building and select **Add Floor**. **b.** In the **Floor Name** field, enter a name for the floor. The **Floor Name** field has restrictions, including: • The floor name cannot exceed 40 characters. • Special characters & > < ? ' " / [ ] aren't allowed. **c.** In the **Global Unit System** area, select **Feet** or **Meters**. When the floor is added, all the floors across all the sites sync to display all measurements in your chosen unit system. To update the global unit system, see "2D Map View Options" in the *Cisco Catalyst Center User Guide*. **d.** If you have wireless devices, for the **Type (RF Model)** drop-down list, select the RF model to apply to the floor. The RF model determines how the RF is calculated when computing 2D and 3D heatmaps that show the relative intensity of the RF signals in the coverage area. **e.** Configure the **Floor Number**, **Floor Type** and **Thickness** fields. The floor type and thickness are used when calculating a heatmap for wireless devices. **f.** Skip uploading a floor map image in **Floor Image** area. **g.** Configure map dimensions in the **Width**, **Length**, and **Height** fields. **h.** Click **Add**.
Edit a floor	**a.** In the left pane, hover your cursor over the ellipsis ••• next to the floor and select **Edit Floor**. **b.** In the **Edit Floor** dialog box, make the necessary changes. **c.** Click **Update** to save the changes.
Delete a floor	**a.** In the left pane, hover your cursor over the ellipsis ••• next to the floor and select **Delete Floor**. **b.** Click **OK**.

Existing Cisco network hierarchies

An existing Cisco network hierarchy is a site structure that you can export from Cisco Prime Infrastructure, import into Catalyst Center, and use to preserve site hierarchy and map data.

If you have an existing network hierarchy in Cisco Prime Infrastructure, you can export it and then import it into Catalyst Center, saving time and effort when creating a new network hierarchy.

You can use this information to recreate your network hierarchy:

- **Site Hierarchy**: Your existing site hierarchy is downloaded as a CSV file. The CSV file contains details such as site names, parent hierarchy, number of floors, location, and site address.
- **Map Archive**: Map information is downloaded as a map archive TAR file. The map archive file contains data such as the date and time, number of floors, and APs. Depending on what you download, the map archive can also include map information, such as floor dimensions (length, width, and height) and details about the APs and overlay objects that have been placed on the floor maps. You can also download calibration information, such as the RF attenuation model that has been applied to each floor.

  You can base the map archive on the global hierarchy or on a single site, building, or floor:

  - **Site**: The chosen site and all of its subsites, buildings, and floors are exported.
  - **Building**: The chosen building and all of its floors are exported.
  - **Floor**: The chosen floor is exported.



Note Catalyst Center supports the United States' Federal Information Processing Standards (FIPS). FIPS is an optional mode that can be enabled when installing the Catalyst Center image. By default, FIPS mode is disabled.

FIPS mode affects the export and import of map archives.

If FIPS mode is *enabled*:

- Exported map archives are unencrypted.
- Only unencrypted map archives can be imported.

If FIPS mode is *disabled*:

- Exported map archives are encrypted.
- Both encrypted and unencrypted map archives can be imported.

For details, refer to the *Cisco Catalyst Center User Guide*.

Export your site hierarchy from Cisco Prime Infrastructure

Use this task to export your site hierarchy from Cisco Prime Infrastructure as a CSV file. The CSV file contains details such as site names, parent hierarchy, number of floors, location, and site address.

Site hierarchy export is supported in Cisco Prime Infrastructure, Release 3.2 and later.

Procedure

Step 1 In Cisco Prime Infrastructure, choose **Inventory** > **Group Management** > **Network Device Groups**.

Step 2 In the **Device Groups** window, click **Export Groups**.

Step 3 In the **Export Groups** dialog box, select **APIC-EM**.

Step 4 To download the CSV file, click **OK**.

Export your map archive from Cisco Prime Infrastructure

Use this procedure to export map archive files from Cisco Prime Infrastructure and import them into Catalyst Center. Map archives contain map information, such as floor dimensions, and calibration information, such as the Radio Frequency (RF) attenuation model that has been applied to each floor in Cisco Prime Infrastructure.

Procedure

Step 1 From the Cisco Prime Infrastructure GUI, choose **Maps** > **Wireless Maps** > **Site Maps (New)**.

Step 2 From the **Export** drop-down list, select **Map Archive**.

The **Export Map Archive** window opens, and the **Select Sites** window opens by default.

Step 3 Check the check box next to a specific site, campus, building, or floor that you want to export.

Alternatively, check the **Select All** check box to export all the maps.

Step 4 Select at least one of these options:

- **Map Information**: Click **On** to export floor dimensions (length, width, and height) and details about the APs and overlay objects that have been placed on the floor maps.
- **Calibration Information**: Click **On** to export the RF attenuation model that has been applied to each floor. It is a good practice to export the existing calibration data from Cisco Prime Infrastructure. Otherwise, you must re-enter the calibration details manually.

  If you include calibration information, you also need to specify whether to include information for the selected maps or all the information.

  - **Calibration Information for selected maps**: Calibration information for the selected site maps is exported.
  - **All Calibration Information**: Calibration information for the selected map and any additional calibration information that is available in the system is exported.

Step 5 Click **Generate Map Archive**.

This message shows the progress of the operation:

```
Exporting data is in progress
```

A TAR file is created and saved to your local machine.

Step 6 Click **Done**.

Import your site hierarchy to Catalyst Center

Use this procedure to import a site hierarchy that you exported from Cisco Prime Infrastructure as a CSV file. For information about exporting the site hierarchy, refer to the *Cisco Catalyst Center User Guide*.

Before you begin

- Make sure that you have Cisco Wireless Controllers and APs in your Catalyst Center inventory. If not, discover them using the **Discovery** feature.
- Add and position APs on a floor map.
- If you manually created sites in Catalyst Center that are present in Cisco Prime Infrastructure, you must remove them from Catalyst Center before you can import them.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the map toolbar, click **Import** and select **Import Sites**.

Step 3 In the dialog box, select one of these options:

- **Merge with Existing Sites**: The imported site information is combined with the existing site information.
- **Overwrite Existing Sites**: If the same site already exists in Catalyst Center, the existing site information is overwritten with the imported site information.

Step 4 In the dialog box, drag and drop your CSV file into the download area.

To use the file picker instead, you can click **Choose a file**, navigate to where your CSV file is located, and then click **Import**.

Note
If you do not have a CSV file, click **CSV template** to download a CSV file that you can edit and upload.

Import your map archive to Catalyst Center

Use this task to import a map archive TAR file that you exported earlier into Catalyst Center. For example, you can upload the TAR file that you exported from Cisco Prime Infrastructure.



Note Catalyst Center supports the United States' Federal Information Processing Standards (FIPS). FIPS is an optional mode that can be enabled when installing the Catalyst Center image. By default, FIPS mode is disabled.

For information about exporting a map archive, refer to Export your map archive from Cisco Prime Infrastructure, on page 37.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the map toolbar, click **Import** and select **Import Floor Maps**.

Step 3 In the **Import Floor Maps** dialog box, drag and drop the map archive file.

Step 4 Click **Import**.

The map archive file is imported.

Use an existing Ekahau network hierarchy

The Ekahau Pro tool lets you create a complete network plan for your enterprise, including floor layout, AP locations, and obstacles. After creating the floor layout, you can export the simulated network plan as an Ekahau project file. You can also export the real-world site survey data into a format that Catalyst Center can use.

Export the Ekahau project from Catalyst Center

To augment the preconfigured working floors, the Catalyst Center allows you to export the working floors from Catalyst Center as an Ekahau project and import the project into the Ekahau Pro Tool.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

A world map displays in the right pane.

Step 2 In the left pane, select the site, building, or floor.

Step 3 To export a complete network map as an Ekahau project, from the **Export** drop-down list, select **Export Floor Maps**.

To export an Ekahau project of a site, building, or floor map, from the left pane, hover over the ellipsis ••• next to the site, building, or floor and select **Export Floor Maps**.

The **Export Floor Maps** dialog box is displayed.

Step 4 In the **Export Floor Maps** dialog box, select the **Ekahau Project** export format.

Step 5 Click **Export**.

An ESX file is created and saved to your computer.

Step 6 Import the ESX file into the Ekahau Pro tool, augment the floor, and save the file.

Step 7 Import the Ekahau project into the Catalyst Center under the site. For more information, see Import an Ekahau project to Catalyst Center, on page 40.

Import an Ekahau project to Catalyst Center

Before you begin

Importing an Ekahau Cloud project can fail if the project has local changes (such as removing an AP or wall), that are out-of-sync with the Ekahau Cloud project. To avoid this situation, make sure to synchronize any local changes to the Ekahau Cloud before importing the Ekahau Cloud project to Catalyst Center.

For the Ekahau versions that Catalyst Center supports, see the Compatibility Matrix. Ekahau releases new versions periodically. For information about importing a later version than Ekahau 11.0.2, see the Ekahau support article titled How to import Ekahau data into the Cisco Catalyst Center.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 Add the sites, buildings, and floors that you need in the network hierarchy.

Note
For more information, see Create, edit, and delete a site, on page 32, Add, edit, and delete a building, on page 34, and Add, edit, and delete a floor, on page 34.

While adding floors, make sure that you create floors with the same name given in the Ekahau project.

Step 3 In the left pane, hover your cursor over the ellipsis icon next to the site where you want to import the Ekahau project and select **Import Ekahau Project**.

The **Import Ekahau Project** dialog box appears.

Step 4 Drag and drop the ESX file into the boxed area in the **Import Ekahau Project** dialog box, or click the **click to select** link and browse to the ESX file.

Note
To import buildings, add coordinates to them in the Ekahau project. You can add coordinates in Ekahau Pro. After successfully importing an Ekahau Project, each planned AP is mapped to an existing real AP in the inventory using the AP name. The planned AP is displayed with an icon **P** on the floor map. For example, if the name of the planned AP is SJC01-02-AP-B-1, the import process searches for the real AP with the same name.

Step 5 If an AP is not found in the inventory and remains unmapped, the planned AP is retained on the floor.

To see the reason for the mismatch, hover your cursor over the planned AP icon on the floor map, and click **Import History**.

These attempts are made to map the planned APs to real APs:

- If the newly discovered APs match the planned AP, the planned AP is replaced with the discovered real AP.
- If a planned AP remains unmapped, you can manually replace the planned AP with the real AP, providing reasons for the failure.

Step 6 To manually assign the planned AP to a real AP, hover your cursor over the planned AP icon on the floor map, and click **Assign** > **Assign**.

The **Assign Planned APs** panel appears.

Step 7 In the **Assign Planned APs** panel, map the planned AP to a real AP by AP name, AP type, or All APs.

Step 8 Click the radio button next to the **AP Name**, and click **Assign** to manually assign the planned AP.

Step 9 Click **Save**.

Import an Ekahau site survey to Catalyst Center

To create your network hierarchy, you can upload an Ekahau site survey file and an AP mapping file (in CSV format).

The Ekahau site survey only contains the floor map with the APs known by name and position on the map. By default the AP model might not be set in the Ekahau site survey. A prerequisite of importing to Catalyst Center is to open the project in Ekahau and configure the AP models using Ekahau-allowed model names, for example, *Cisco C9130i* for the Catalyst Center 9130 AP.

Because the Ekahau site survey does not provide Catalyst Center with any information about the radios of each AP, the AP mapping file augments the Ekahau site survey with this information. The AP mapping file is limited in that you can only provide the desired AP mapping by AP model, not by AP name. So, if you have multiple APs of the same type but different antenna configurations, only one antenna configuration can be applied to all APs of that type within the project.

For each AP in the AP mapping file, you define the model number followed by the configuration of each antenna:

```
model,antennaName0,antennaAzimuth0,antennaElevation0,antennaName1,antennaAzimuth1,antennaElevation1
```

For example, this AP mapping file defines the configuration of a Catalyst 9130I with two antennas:

```
AP9130I,Internal-9130-2.4GHz,90d,0d,Internal-9130-5GHz,90d,0d
```

The model attribute must be the same as the equivalent planned AP model in the Catalyst Center GUI, for example, AP9130I for the Catalyst Center 9130 AP. Similarly, the *antennaName* attributes must also be the same names found and supported in the Catalyst Center GUI. If the AP has three or more radios, you can continue the *n*-based numbering pattern of the *antennaName*, *antennaAzimuth*, and *antennaElevation* parameters to define the antenna information for each radio by slot number supported by that AP model.

Catalyst Center includes a CSV template file that you can download and edit to define the required AP antenna information.

Figure 6: Fields and defaults contained in the CSV template file

	A	B	C	D	E	F	G	H	I	J
1	model	antennaName0	antennaAzimuth0	antennaElevation0	antennaName1	antennaAzimuth1	antennaElevation1	antennaName2	antennaAzimuth2	antennaElevation2
2	AP2700I	Internal-2700-5GHz	90d	0d	Internal-2700-2.4GHz	90d	0d			
3	AP1850I	Internal-1850-5GHz	90d	0d	Internal-1850-2.4GHz	90d	0d			
4	AP3800E	AIR-ANT2524DB-R-5GHz	179.9543762d	0d	AIR-ANT2524DB-R-2.4GHz	179.9543762d	0d			
5										

If an AP isn't in the Catalyst Center device inventory, it's imported as a planned AP. However, you can use a naming convention so that when you add an AP to the device inventory, Catalyst Center can automatically convert it to an actual AP.

The naming convention is AP, followed by the last four digits of the AP's MAC address, for example, AP-c4:e0. Using this information, Catalyst Center attempts to match the provided digits with the last four digits of an

AP's Ethernet MAC or radio MAC address. If this information isn't available or a match is unsuccessful, Catalyst Center attempts to match AP names.

Before you begin

- Open the project in Ekahau and configure the AP models using Ekahau-allowed model names, for example, *Cisco C9130i* for the Catalyst Center 9130 AP.
- Create an AP mapping file (CSV format) to provide Catalyst Center with information about the radios of each AP model that is being used.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 Click **Add Site** > **Add Area**.

Alternatively, you can hover over the ellipsis ••• next to the parent site or **Global** in the left pane, and select **Add Area**. For more information, see Create, edit, and delete a site, on page 32.

Step 3 In the left pane, hover your cursor over the ellipsis ••• icon next to the site you just created and select **Import Ekahau Survey**.

Step 4 In the **Import Ekahau Survey** dialog box, drag and drop the Ekahau Survey file into the **Ekahau Survey** box, or click the **Choose a file** link and browse to the ESX file.

Step 5 Drag and drop the CSV file into the **AP Mapping CSV** box, or click the **Choose a file** link and browse to the CSV file.

Note
If you do not have a CSV file, click **Download AP Mapping Template** to download a CSV file that you can edit and upload.

Step 6 Click **Import**.

After the files are successfully uploaded, a success message appears.

Step 7 Click **View Hierarchy** and navigate to the floors to verify that the devices have been imported and positioned properly.

Hover the cursor over a device to view its details.

Configure 2D floor map devices and overlay objects

In 2D maps, you can configure devices and overlay objects on your floor maps. The Cisco Catalyst Assurance User Guide provides basic guidance on working with 2D maps. In addition to 2D maps, Catalyst Center supports 3D maps with more capabilities. For a full description of both 2D and 3D map features, see the *Cisco Catalyst Center User Guide*.

Devices

- **APs**: An access point (AP) serves as the connection point between wireless and wired networks or as the center point of a standalone wireless network. In 2D maps, an AP represents an actual, installed

device. For a list of APs that Catalyst Center supports, see the *Cisco Catalyst Center Compatibility Matrix*.

- **Planned APs**: Planned APs are representations of APs that haven't been installed yet. By placing planned APs on a map, you can envision your wireless network RF coverage and make changes before you actually install the APs.
- **Sensors**: A sensor is a dedicated Cisco Aironet 1800S Active Sensor that gets bootstrapped using Cisco PnP. After it obtains the Assurance server reachability details, it communicates directly with the Assurance server. For more details, including information about sensor tests, see the Manage Sensors and Sensor-Driven Tests, on page 305.

Overlay objects

- **Coverage Areas**: By default, any area defined as part of a floor map is considered as a wireless coverage area. However, if you have a building that is nonrectangular or you want to mark a nonrectangular or polygon-shaped area on a floor, you can use the **Coverage Areas** drawing tool to create a coverage area.
- **Openings**: An opening, also called an atrium, is an open-air or skylight-covered area within a building. An opening can extend through multiple floors and can affect wireless signal coverage areas.
- **Location Regions**: Location regions are used by location services (Cisco CMX or Cisco Spaces). Location regions define areas that are included in or excluded while positioning clients. Inclusion areas are included in the calculations and exclusion areas aren't included. When you create a floor, by default, the whole region on the floor is defined as the inclusion region. You can manually edit the default inclusion region and set exclusion regions on the floor. For example, you can exclude areas such as openings or atriums, and large racks within a building, where positioning of real clients isn't possible.
- **Walls**: Walls define any exterior or interior vertical structures in a building, such as windows, cubicles, and doors. Because they can be made of different materials and have different densities, they can significantly impact RF signal attenuation and heatmap calculation. For example, the more walls you include in a floor map, the longer it can take to compute a heatmap. Although, even if you have a high number of walls on your floormap, you can adjust the number used to compute the heatmap. For information, see "2D Map View Options" and "3D Map View Options" in the *Cisco Catalyst Center User Guide*.
- **Shelving Units**: Shelving units are obstacles that can significantly impact RF signal attenuation and heatmap calculation. A high-ceiling warehouse is an example of a location with shelving units.
- **Markers**: A marker identifies a location on a map. When you create a marker, you can name it and position it to help you identify it later.
- **GPS Markers**: When integrated with Catalyst Center, location services, such as Cisco Spaces or Cisco Connected Mobile Experiences (CMX), use GPS markers to calculate the approximate geographical location of clients.
- **Align Points**: Align points are markers that are used to position multiple floors that have different physical shapes. In 3D maps, floors are aligned at the top-left corner of the map (point 0,0). If you manage each floor independently, the misalignment isn't a problem. However, to use some of the features of 3D maps, the floors need to be aligned as they are in reality. To compensate for this misalignment, you can insert one or more align points on two or more floors, so that the floors align properly one on top of the other in a 3D map.

Add, position, edit, and remove APs

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 In the left hierarchy tree, select a floor.

Step 3 From the map toolbar, click **2D** > **Add/Edit**.

By default, the **Devices** and **Access Points** toggle buttons are chosen.

Step 4 From this window, you can add, position, edit, and remove APs. See this table for details.

Action	Steps
Add APs.	**a.** In the left pane of the map, click **Add Access Points**. **b.** In the **Add Access Points** slide-in pane, do one of these tasks in the table: • **To add a single AP**: Locate the AP that you want to add, and scroll to the right and click **Add**. • **To add multiple APs**: Check the check boxes next to the APs you want to add and click **Add Selected**. Newly added APs appear in the **Unpositioned** category in the left pane of the map. **c.** From the **Unpositioned** category, click an AP. **d.** Click the location on the map where you want to position the AP. **e.** In the map toolbar, click **Save**.
Add planned APs.	**a.** From the left pane of the map, in the **Planned AP Models** area, click the AP model of the planned AP that you want to add. If the AP model isn't listed, click **Add Model** and select the AP model to add to the list. **b.** On the floor map, click the location where you want to place the planned AP. **c.** In the **Edit Planned AP** slide-in pane, click the gear icon and add a unique name pattern. **d.** Define the antenna type and the azimuth and elevation, if necessary. **e.** To continue adding planned APs with the same properties, click locations on the map. **f.** To stop adding planned APs, press **Esc** or right-click the floor map. **g.** In the map toolbar, click **Save**.

Action	Steps
Edit an AP.	**a.** In the map, right-click the AP and select **Edit**. **b.** Change any of the editable AP settings. Understand the information about these fields: • **Antenna**: For external APs, you must select an antenna. If an antenna isn't chosen, the AP will not be present in the map. • **Azimuth**: The azimuth is the angle of the antenna, measured relative to the x axis, clockwise. The azimuth range is 0 to 360. In Catalyst Center, pointing right is 0 or 360 degrees; pointing down is 90 degrees. You can manually enter the value or use the blue arrow under the field to change the value. For omnidirectional antennas, the azimuth is not relevant if the elevation is 0. • **Elevation**: You can manually enter the elevation in degrees or use the blue arrow under the field to change the value. For APs and antenna models that are designed to be placed on a ceiling, 0 elevation means pointing down. For APs and antenna models that are designed to be placed on a wall, 0 elevation means pointing horizontally and negative values mean pointing down. **c.** In the map toolbar, click **Save**.
Remove an AP.	**a.** Click the AP, or to select multiple APs, click the first AP and while pressing the **Shift** key, click the rest of the APs. **b.** In the **Edit** pane, click **Remove**. **c.** In the map toolbar, click **Save**.

Add, position, and remove sensors

Before you begin

Make sure you have the Cisco AP 1800S sensor in your inventory. The Cisco Aironet 1800s Active Sensor must be provisioned using Plug and Play for it to show up in the Inventory.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 From the map toolbar, click **2D** > **Add/Edit** > **Sensors**.

Step 4 From this window, you can add, position, edit, and remove sensors. See this table for details.

Action	Steps
Add sensors.	**a.** From the **Add Sensors** slide-in pane, click **Add** next to the sensor that you want to add, or to add multiple sensors, check the check boxes next to sensors you want to add and click **Add Selected**. Newly added sensors appear in the **Unpositioned** category in the map left pane. **b.** From the **Unpositioned** category in the map left pane, click a sensor. **c.** Click the location on the map where you want to position the sensor. **d.** Click **Save**.
Remove sensors.	**a.** Click the sensor, or to select multiple sensors, click the first sensor and while pressing the **Shift** key, click the rest of the sensors. **b.** In the **Edit** pane, click **Remove**. **c.** From the map toolbar, click **Save**.

Add, edit, and remove coverage areas

This procedure shows you how to mark a nonrectangular or polygon-shaped area as a coverage area on a floor map.

For more information about coverage areas, see Configure 2D floor map devices and overlay objects, on page 42.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Coverage Areas**.

Step 4 To add a coverage area, do these tasks:

a) In the **Coverage Area** dialog box, enter a name for the coverage area in the field.
b) Click **Add Coverage**.
c) Click on the map to create a point and initiate the drawing tool.
d) Continue creating points to define the coverage area shape.

Note
The coverage area shape must have at least three points. Click and drag a point to redefine the coverage area shape.

e) Double-click to exit the drawing tool and finalize the coverage area shape.

Step 5 To edit a coverage area, do these tasks:

a) In the map toolbar, click **Add/Edit** > **Coverage Areas**.

b) To redefine the shape of a coverage area, click and drag a point.
c) To edit a coverage area name, right-click the coverage area and select **Edit**.

Step 6 To delete a coverage area, do these tasks:

a) In the map toolbar, click **Add/Edit** > **Coverage Areas**.
b) Right-click the coverage area and select **Remove**.

Step 7 In the map toolbar, click **Save**.

Add, edit, copy, and remove openings

Creating an opening is similar to creating an open space or atrium on a floor. On multifloor buildings, typically the opening extends vertically through multiple floors. This procedure shows you how to add, edit, and remove openings on a floor map. It also shows you how to copy openings to other floors.

For more information about openings, see Configure 2D floor map devices and overlay objects, on page 42.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Openings**.

Step 4 To add an opening:

a) From the left pane of the map, click **Opening**.
b) Click on the map to create a point and initiate the drawing tool.
c) Continue creating points to define the opening shape.

Note
The opening shape must have at least three points. Click and drag a point to redefine the opening shape.

d) Double-click to exit the drawing tool and finalize the shape.

Step 5 To edit an opening:

a) In the map toolbar, click **Add/Edit** > **Openings**.
b) To redefine the shape of an opening, click and drag a point.
c) To move an opening, click inside the shaded area. Then, drag and drop the opening where you want to place it.

Step 6 To copy an opening from one floor to another:

a) In the map toolbar, click **Add/Edit** > **Openings**.
b) Right-click the opening and select **Copy to other floors**.
c) In the dialog box, check the check boxes next to the relevant floors.
d) Click **Copy**.
e) Click **Close**.

Step 7 To remove an opening:

a) In the map toolbar, click **Add/Edit** > **Openings**.
b) Right-click the opening and select **Remove**.

Step 8 In the map toolbar, click **Save**.

Add, edit, and remove location regions

Location regions are areas on the map that are either included in or excluded from the heatmap calculation. These topics show you how to add, edit, and remove location regions.

Add, edit, and remove an inclusion region

This procedure shows you how to add, edit, and remove an inclusion region. Use these guidelines to define an inclusion region on a floor map:

- Inclusion regions can be any polygon-shaped area and must have at least three points.
- You can only define one inclusion region on a floor. By default, an inclusion region is defined for each floor area when it is created. The inclusion region is indicated by a solid aqua line, and generally outlines the entire floor area.

For more information about inclusion regions, see Configure 2D floor map devices and overlay objects, on page 42.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Location Regions**.

Step 4 In the left pane of the map, click the **Inclusion** icon.

Step 5 To create an inclusion region, use the drawing tool:

a) Click the map to create a point where you want the inclusion region to begin.
b) Move the cursor to the next point and click again.
c) Continue creating points to define the inclusion region shape.
d) To finalize the shape, double-click the map.

Alternatively, from the left pane of the map, click the **Inclusion** icon.

e) To exit the drawing tool, double-click the map again.

Step 6 To edit the location of an inclusion region, drag and drop the shape to the new location.

Step 7 To remove an inclusion region, right-click the shape and select **Remove**.

Step 8 In the map toolbar, click **Save**.

Add, edit, and remove an exclusion region

This procedure shows you how to add, edit, and remove an exclusion region. Use these guidelines to define exclusion regions on a floor map:

- Exclusion regions can be any polygon-shaped area and must have at least three points.
- Exclusion regions are defined within the borders of an inclusion region.

- You can define multiple exclusion regions on a floor map.

For more information about exclusion regions, see Configure 2D floor map devices and overlay objects, on page 42.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Location Regions**.

Step 4 From the left pane of the map, click the **Exclusion** icon.

Step 5 To create an exclusion region, use the drawing tool:

a) Click the map to create a point where you want the exclusion region to begin.

b) Move the cursor to the next point and click again.

c) Continue creating points to define the exclusion region shape.

d) To finalize the shape, double-click the map.

Alternatively, from the map left pane, click the **Exclusion** icon.

e) To exit the drawing tool, double-click the map again.

Step 6 To edit the location of an exclusion region, drag and drop the shape to the new location.

Step 7 To remove an exclusion region, right-click the shape and select **Remove**.

Step 8 In the map toolbar, click **Save**.

Add, edit, and remove walls

This procedure shows you how to add, edit, move, and remove walls on a floor map.

For information about how walls impact RF signal attenuation and heatmap calculation, see Configure 2D floor map devices and overlay objects, on page 42.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Walls**.

Step 4 To add walls:

a) In the left pane of the map, click a wall type from the **Others** or **On this floor** category.

Note
If a wall type isn't listed, click **Add Wall Type** to create a custom wall type.

b) Click the map to create a point where you want the wall to begin.

c) Move the cursor to the next point, where you want to end the wall or where you want to create a corner and click again.
d) Continue creating points to define the wall shape.
e) To end a wall, double-click the map.

   Alternatively, from the left pane, click the wall type.

f) To exit the drawing tool, double-click the map again.

Step 5 To change a wall type, and depending on the wall type also configure its parameters:

a) Click the wall that you want to change.

   The **Wall Type** dialog box opens.

b) From the **Wall Type** drop-down list, select the type of wall.
c) Configure any other parameters that are appropriate for the new wall type.
d) Click **Update**.

Step 6 To move a wall:

a) Hover your cursor over the wall that you want to move.

   The wall turns black, which means it's selected.

b) Click the wall and drag and drop it to the new location.

Step 7 To remove a wall, right-click the wall and select **Remove**.

Step 8 In the map toolbar, click **Save**.

Add, copy, edit, and remove shelving units

This procedure shows you how to add, copy, edit, and remove shelving units on a floor map.

For information about shelving units, see Configure 2D floor map devices and overlay objects, on page 42.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Shelving Units**.

Step 4 To add shelving units:

a) In the left pane of the map, click the shelving type you want to add.
b) In the shelving dialog box, configure the name, dimensions, orientation, and whether the unit is double-sided, or leave the default values. Orientation means the angle of the shelving unit. A shelving unit with an orientation of zero means that the shelving unit is vertical and parallel to the y-axis.

   If a shelving type is not in the list, click **Add Shelving Type** to create a shelving type.

c) Click **Add Shelving**.

   The shelving unit appears on the map.

d) Drag and drop the shelving unit to its location on the map.

Step 5 To create a copy or an array of a shelving unit:

- To create a copy, right-click the shelving unit and select **Clone**.
- To create an array, right-click the shelving unit and select **Array**. Then specify the number of units and the distance between them.

Step 6 To edit the name, dimensions, orientation, and whether it is two-sided, right-click the shelving unit and select **Edit**.

Step 7 To remove a shelving unit, right-click the shelving unit and select **Remove**.

Step 8 In the map toolbar, click **Save**.

Add, edit, and remove markers

This procedure shows you how to add, edit, and remove markers.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Markers**.

Step 4 In the left pane of the map, click the **Markers** icon.

Step 5 In the **Place Markers** dialog box, enter the name for the marker, and click **Add**.

Step 6 To place the marker, click the map where you want to place the marker.

Step 7 To move a marker, hover your cursor over the marker until it turns blue. Then drag and drop it in the new location.

Step 8 To edit a marker, right-click the marker and select **Edit**.

Step 9 To remove a marker, right-click the marker and select **Remove**.

Step 10 In the map toolbar, click **Save**.

Add, edit, and remove GPS markers

This procedure shows you how to add, edit, and remove GPS markers. For more information about GPS markers, see Configure 2D floor map devices and overlay objects, on page 42.

Note The GPS marker is an attribute of the building. You can apply it to all the floors of the building.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **GPS Markers**.

Step 4 To add a GPS marker:

a) In the left pane of the map, click the **GPS Markers** icon.

b) On the map, click the location where you want to place the GPS marker.

GPS markers must be positioned inside the outer-perimeter walls, typically at the building corners.

c) In the **Place Markers** dialog box, enter the name, latitude, longitude, and the x and y coordinates in the appropriate fields.

The latitude and longitude coordinates of the GPS marker located in the northwest corner of a floor must match the building coordinates.

d) Click **Add**.

To include GPS markers in calculations, you must add at least three GPS markers.

Step 5 To edit a GPS marker, right-click the GPS marker and select **Edit**.

Step 6 To move a GPS marker, hover the cursor over the marker until it turns orange. Then drag and drop it in the new location.

Step 7 To remove a GPS marker, right-click the GPS marker and select **Remove**.

Step 8 In the map toolbar, click **Save**.

Add, edit, and remove align points

This procedure shows you how to add, edit, and remove align points. For more information about align points, see Configure 2D floor map devices and overlay objects, on page 42.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Align Points**.

Step 4 To add an align point:

a) In the left pane of the map, click the **Align Points** icon.

b) On the map, click the location where you want to place the align point.

Step 5 To edit the name of an align point:

a) Right-click the align point and select **Edit**.

b) Change the name and click **Update**.

Step 6 To change the location of an align point:

- Hover your cursor over the align point until it turns blue. Then drag and drop it in the new location.
- Right-click the align point and select **Edit**. Update its **x** and **y** coordinates and click **Update**.

Step 7 To remove an align point, right-click the align point and select **Remove**.

Step 8 In the map toolbar, click **Save**.

Manage Inventory

The Inventory function retrieves and saves details, such as host IP addresses, MAC addresses, and network attachment points about devices in its database.

About Inventory

The Inventory function retrieves and saves details, such as host IP addresses, MAC addresses, and network attachment points about devices in its database.

The Inventory feature can also work with the Device Controllability feature to configure the required network settings on devices, if these settings are not already present on the device.

Inventory uses these protocols, as required:

- Link Layer Discovery Protocol (LLDP).
- IP Device Tracking (IPDT) or Switch Integrated Security Features (SISF). (IPDT or SISF must be enabled on the device.)
- LLDP Media Endpoint Discovery. (This protocol is used to discover IP phones and some servers.)
- Network Configuration Protocol (NETCONF). For a list of devices, see Discovery prerequisites, on page 15.

After the initial discovery, Catalyst Center maintains the inventory by polling the devices at regular intervals. The default interval is every 24 hours. However, you can change this interval as required for your network environment. For more information, see Update the device polling interval, on page 54. Polling occurs for each device, link, host, and interface. Only the devices that have been active for less than one day are displayed. This prevents stale device data, if any, from being displayed. On average, polling 500 devices takes approximately 20 minutes. A configuration change in the device triggers an SNMP trap, which in turn triggers device resynchronization. Device resynchronization is also triggered after the inventory service restart under these circumstances:

- If there is an upgrade (Catalyst Center upgrade) after the inventory service restart.
- If the device synchronization is in terminated or delayed state after the service restart.
- If the **Last Sync** time for the device is more than 75 percent of the periodic resync interval configured on the device. For example, after the inventory service restart, if the **Last Sync** time for a device has crossed 18 hours and the configured periodic resync interval is 24 hours, the device will be resynchronized before the periodic resync interval. The percentage for the resync interval cutoff time may vary based on the value configured on the device.

Note Points regarding device resynchronization include:

- Port up/down events are grouped together every 80 seconds. As a result, only one event is reported per 80-second window for each device. This process updates the device's port-related inventory data.
- Configuration change events are grouped every 10 minutes, triggering a resync request for the device.
- If three consecutive syncs occur due to port up/down traps or configuration change traps, the next event-based sync for that device is delayed by 5 minutes.
- If the rate of event bursts exceeds 60% within a consolidation window, the resync for that device is delayed by 45 minutes.

Update the device polling interval

You can update the polling interval globally for all devices by choosing **System** > **Settings** > **Network Resync Interval**. To update the polling interval for a specific device, select **Device Inventory**. The value set using **Network Resync Interval** replaces any value configured in **Device Inventory**.

If you do not want a device to be polled, you can disable polling.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Select the devices to update.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Edit Device**.

Step 4 In the **Edit Device** slide-in pane, click **Resync Interval**.

Step 5 Select the resync type.

Note

- To set the resync type as global, go to **System** > **Settings**.
- The device-specific polling time supersedes the global polling time. If you set the device-specific polling time and then change the global polling time, Catalyst Center continues to use the device-specific polling time.

Step 6 In the **Resync Interval (in Mins)** field, enter the time interval (in minutes) between successive polling cycles.

Step 7 Click **Update**.

Display information about your inventory

You can display and filter for information about discovered devices in your inventory. You can also customize or change the information displayed in the **Devices** table.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information from the discovery process.

Note
For the devices that are added as Fully Qualified Domain Name (FQDN), hover your cursor over the **i** icon next to the device name in the **IP address** column to view the **Resolved IP Address**.

If the **Inventory** window contains APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In this dialog box, you have the option to:

Option	Task
Skip this dialog box in the future.	Check the **Don't show this again** check box.
Open the **License Manager** window and enable the licenses.	Click **License Manager** (for more information, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*)
Enable the licenses later.	Click **Do this later**.

Step 2 (Optional) To change the site, click **Global** and use either the search bar or network hierarchy to find a site.

The **Inventory** window displays the devices available in the chosen site.

Step 3 (Optional) To change the Inventory view, use the toggle button () in the top-right corner.

You can change your default view (the list layout) to other layouts, such as the topology, or map layout.

Step 4 (Optional) To change the **Devices** table focus views, from the **Focus** drop-down list, select a view, such as **Default**, **Inventory**, or **Software Images**.

Note
- The displayed columns change depending on the chosen focus view.
- The selected devices persist in each new focus view.

Step 5 (Optional) To filter for specific device details in the **Devices** table, use these filter options.

Option	Task
To filter for a device family	Select one or more of the device family buttons at the top of the **Inventory** window. For example, you can click **Routers** to display only routers in the table.
To filter for device work items, in the left pane	Check the check box of one or more work items. The table is immediately filtered for the work item. For example, you can check the **Unreachable** check box to display only unreachable devices in the table.
To filter for specific device details	Click **Filter devices** and select from these options: **Quick Filters**, **Advanced Filters**, or **Recent Filters**. Then click **Apply**.

Step 6 (Optional) To take a guided tour of the **Inventory** window, click **Take a tour** in the top-right corner.

Step 7 (Optional) To export all the data in the **Devices** table, click **Export** in the top-right corner.

Step 8 (Optional) To customize the **Devices** table, click the settings icon ( ) in the top-right corner, select your preferred options in the **Table Settings** slide-in pane, and then click **Apply**.

Option	Description
Table Appearance	Select to use the default or compact table view and table striping.
Edit Table Columns	Select to create a custom view and to hide or display columns.

Note
The column selection doesn't persist across sessions.

This table provides key information about specific table columns.

Column	Description
Device Name	Name of the device. Click the device name to view more information about that device. **Note** If a device name appears in red, the inventory has not polled the device or updated its information for over 30 minutes.

Column	Description

Support Type	Shows the device support level:
	• **Supported**: The device profile is tested for all applications on Catalyst Center. You can open a service request if any of the Catalyst Center functionalities for these devices don't work.
	• **Limited**: The device profile for legacy devices is tested only for these features and tested only on a best-effort basis on Catalyst Center.
	  • Discovery
	  • Topology
	  • Device Reachability
	  • Config Change Audit
	  • Inventory
	  • Software Image Management (Software images may not be available for EOL devices on cisco.com. Not recommended for EOL devices.)
	  • Template Provisioning (Applicable only for switches.)
	For more information, see the *Legacy Device Compatibility Matrix*.
	• **Third Party**: The device profile has been tested on Catalyst Center for third-party devices that are capable of populating SNMP MIB 2 values. Catalyst Center supports limited base automation (Inventory and Topology) and limited assurance capabilities, such as third-party device 360, device health calculation based on reachability status, and device interface and reachability issues.
	For more information, see the *Cisco Catalyst Center Compatibility Matrix*.
	• **Unsupported**: All remaining Cisco and third-party devices that aren't tested and certified on Catalyst Center. You can try out various functionalities on Catalyst Center for these devices, as a best effort. However, you can't raise a service request or a bug if Catalyst Center features don't work as expected.

Reachability	Shows various statuses: • **Reachable**: The device is reachable by Catalyst Center using SNMP, HTTP(S), and NETCONF polling. • **Ping Reachable**: The device is reachable by Catalyst Center using ICMP polling and not reachable using SNMP, HTTP, HTTPS, and NETCONF polling. • **Unreachable**: The device isn't reachable using SNMP, HTTP, HTTPS, NETCONF, or ICMP polling.

Column	Description
EoX Status	Shows the EoX scan status: • **Success**: The device is scanned for EoX alerts successfully. • **Not Scanned**: The device isn't scanned for EoX alerts. • **Scan Failed**: Catalyst Center isn't able to scan the device for EoX alerts. • **Scanning**: Catalyst Center is scanning the device for EoX alerts. Hover your cursor over the **i** icon next to **EoX Status**, and click **Consent to Connect** hyperlink. To initiate an EoX scan, you must accept and submit the authorization in the **Consent to Connect** dialog box. For the devices that are scanned successfully, the **EoX Status** column shows the number of alerts, if any. Click the number of alerts to view the alerts in detail. In the slide-in pane, click the **Hardware**, **Software**, and **Module** tabs to view the hardware, software, and module EoX alerts. **Note** The EoX feature doesn't support scanning APs for EoX alerts.
Manageability	Shows the device status: • **Managed with green tick icon**: Device is reachable and is fully managed. • **Managed with orange error icon**: Device is managed with some error, such as unreachable, authentication failure, missing NETCONF ports, internal error, and so on. Hover your cursor over the error message to view more details about the error and the impacted applications. **Note** If the verification of a device's SSH key failed, see Deal with SSH key verification errors, on page 61 for a description of how to deal with this issue. • **Unmanaged**: Device can't be reached and no inventory information was collected because of device connectivity issues. **Note** For an ongoing device resynchronization, the **Syncing** status is displayed. Click the status to view: • Ongoing sync details, • Previous sync details, • Reasons for the synchronization, and • The application that requested the synchronization. A message is displayed for pending resync requests that are in the queue. If multiple requests are pending, they are merged based on the features to be synced and the priority. The sync details can display multiple reasons for a sync event.
Platform	Cisco product part number

Column	Description
Device Role	Role assigned to each discovered device during the scan process. The device role is used to identify and group devices according to their responsibilities and placement within the network. If Catalyst Center is unable to determine a device role, it sets the device role to Unknown. **Note** If you manually change the device role, the assignment remains static. Catalyst Center doesn't update the device role even if it detects a change during a subsequent device resynchronization. If required, you can use the drop-down list in this column to change the assigned device role.
Site	The site to which the device is assigned. If the device isn't assigned to any site, do these steps: **a.** Click **Assign**. **b.** Click **Choose a Site**. **c.** Select a site from the hierarchy. **d.** Click **Save**. For more information, see Network hierarchy, on page 30.
Last Updated	Most recent date and time on which Catalyst Center scanned the device and updated the database with new information about the device. **Note** Click **Sync Details** to view the **Last Sync Start Time** and **Reason(s) for Last Sync**. For an ongoing device resynchronization, **Sync Details** displays: • Ongoing sync details, • Previous sync details, • Reasons for the synchronization, and • The application that requested the synchronization. A message is displayed for pending resync requests that are in the queue. If multiple requests are pending, they are merged based on the features to be synced and the priority. The sync details can display multiple reasons for a sync event.
Resync Interval	The polling interval for the device. Set the resync interval from the **Inventory** window by choosing **Actions** > **Edit Device** > **Resync Interval**. To set the resync type as **Global**, from the main menu, choose **System** > **Settings**. For more information, see the *Cisco Catalyst Center Administrator Guide*.

Column	Description
Provisioning Status	Shows the status of the last provisioning operation attempted on a device. Click **See Details** to view the status of past provisioning operations. • **Success**: The latest operation on the device was successful. • **Success with a warning icon**: The latest operation on the device was successful, but there are failures from past provisioning operations that may need user attention. • **Failed**: The latest operation on the device has failed. • **Failed with a warning icon**: The latest operation on the device has failed, and there are failures from past provisioning operations that may need user attention. • **Configuring**: The device is currently being configured. • **Pending**: The system is trying to determine if the device will be impacted by an ongoing provisioning operation. • **Not Provisioned**: The device has never been provisioned. • **Out of Sync**: The network settings or network profiles for a device have been modified after the last provisioning operation. IPv6 devices can be marked as Out of Sync.
Credential Status	Shows the device credential status: • **Not Applied**: The device credential isn't applied on the device. • **Success**: The device credential is applied on the device successfully. • **Failed**: The device credential failed on the device. Click **See Details** to view the details about the credentials. The **Credential Status** slide-in pane shows the **Type**, **Name/Description**, **Status**, and **Details** of the credential. For a device whose status is **Failed**, hover your cursor over the ellipsis icon (***) in the **Actions** column and select **Retry** or **Clear**. • **Retry**: Applies the credential on the device. • **Clear**: Clears the device credential.
AP CDP Neighbors	Displays details about the switch and port connected to an AP in the **Inventory** window. This window displays information about AP CDP neighbors even if the connected access switch is managed by Catalyst Center.

- **Edit Custom Views**: First you must create a custom view in the **Edit Table Columns** tab, and then you can edit the custom view.
- **Reset All Settings**: Reset the table settings to the default settings.

Step 9 (Optional) To manage your devices from the **Devices** table, you can tag devices, add devices, or use the **Actions** drop-down list.

Name	Description
Tag	Click **Tag** to tag devices, edit tags, delete tags, or create port group.
Add Device	Click **Add Device** to add a network device, add a compute device, or integrate a Meraki dashboard or Firepower Management Center (FMC) with Catalyst Center.
Actions drop-down list	Use the **Actions** drop-down list to manage your devices, software images, telemetry, and more. To view more details about each action option, click the right-adjacent information icon (ⓘ).

Step 10 (Optional) In the **Devices** table, you can do a variety of actions.

- To sort the columns in either ascending or descending order, click the column header.
- To view more details about a device, click the device name and then click **View Device Details**.
- To view a device's compliance details, click either **Non-Compliant** or **Compliant** under the **Compliance** column.
- To assign a site to a device, click **Assign** under the **Site** column.
- To change a device role, click the edit icon under the **Device Role** column and then select from the options, such as **ACCESS** or **CORE**.
- To change the number of entries, scroll down to the bottom of the window, and from the **Show Records** drop-down list, select the number of entries that you want to appear.

  Note
  If there are more than 25 entries in the table and you select a different focus view, the same number of entries appears in each new view.

Note
Each focus view displays different columns, and you can customize a table view to include columns, such as **Compliance**, **Site**, **Device Role**, and **Software Image**.

Deal with SSH key verification errors

In the **Inventory** window, Catalyst Center indicates the devices for which SSH key verification failed. To deal with this error, complete these steps.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 In the **Manageability** column, click the **SSH key verification failed** link for the device.

Step 3 In the dialog box that opens, follow one of these procedures:

If...	Then...
you want to enable or disable the automatic and global acceptance of SSH key changes,	click **SSH key configuration**. For more information, refer to Configure the automatic acceptance of SSH key changes, on page 62.
you want to open a slide-in pane that lists all devices with SSH key verification errors,	**a.** Click **All errors**. **b.** Check the check box for the devices with SSH key changes you approve. **c.** Click **Confirm**. This triggers a resync of the selected devices.
you know that the SSH key for a device was changed intentionally,	click **Confirm**. This triggers a resync of the device.

Configure the automatic acceptance of SSH key changes

In the **SSH key configuration** window, you can configure whether Catalyst Center automatically accepts SSH key changes.

Important When this option is enabled, you must manually resync every device on which SSH key verification failed.

Procedure

Step 1 From the main menu, choose **System** > **Device Settings** > **SSH key trust**.

Step 2 Click the **Accept all changes** toggle button to enable or disable the automatic acceptance of any SSH key changes that are made.

Delete a network device

Use this procedure to delete a network device from Catalyst Center.

You can delete devices that aren't a part of the fabric network from the Catalyst Center database.

Note

- If the device is a part of the fabric network, you can't delete it. Remove the device from the fabric network, and then delete it from the inventory. For more information, see "Remove a device from a fabric" in the *Cisco Catalyst Center User Guide*.
- When you remove a wireless sensor from the inventory, the sensor resets to factory defaults. When the sensor rejoins, it gets the current configuration.

Before you begin

You must have administrator (ROLE_ADMIN) permissions and access to all devices (RBAC Scope set to ALL) to perform this procedure.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.
The **Inventory** window displays the device information gathered during the discovery process.

Step 2 Check the check box next to the device or devices that you want to delete.

Note
You can select multiple devices by checking additional check boxes, or select all the devices by checking the check box at the top of the list.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Delete Device**.

Note
When you delete devices integrated with Cisco ISE, the deleted devices are moved to new Network Device Group (NDG) group in Cisco ISE.

Step 4 (Optional) In the **Warning** window, check the **Config Clean-Up** check box.

The Device Controllability workflow is triggered. The network settings and telemetry configuration are removed from the selected device. For more information, see "Device Controllability" in the Cisco Catalyst Center Administrator Guide.

Note
When you check this check box for a wireless controller that is provisioned through Catalyst Center, all AAA-related commands are deleted, including the commands that were manually configured on the wireless controller before it was discovered in Catalyst Center.

- To keep the AAA configurations during device deletion, do not check this check box.
- To view which AAA commands are deleted, manage AAA configurations in Catalyst Center.

Step 5 Click **OK** to confirm the action.

Deploy your device configurations now or later

At the scheduling step of a workflow that supports Visibility and Control of Configurations, complete this procedure to deploy your device configurations immediately or at a later time.

Before you begin

Ensure that you have disabled Visibility and Control of Configurations in the settings.

Procedure

Step 1 Click **Now** or **Later**. Update the task name if needed.

Note
If only visibility is enabled, or if both visibility and control are enabled, **Preview and Deploy (Recommended)** is selected by default. The options **Now** and **Later** are dimmed.

Step 2 On the **Performing Initial Checks** window, prepare and submit the task for deployment.

a) Address all the issues to deploy the device configurations.

Ensure all validations are successful by clicking **Recheck**.

b) Click **Submit**.

The device configurations deploy at the scheduled time. View the task in the **Tasks** window.

Preview and deploy your device configurations

When you reach the scheduling step in a workflow that supports Visibility and Control of Configurations, complete this procedure to preview and deploy your device configurations.

Before you begin

Ensure that Visibility and Control of Configurations is enabled in the settings.

Procedure

Step 1 Click **Preview and Deploy (Recommended)** and, if necessary, update the task name.

Note
By default, if only visibility is enabled or both visibility and control are enabled, **Preview and Deploy (Recommended)** is selected. The **Now** and **Later** options are dimmed.

Step 2 On the **Performing Initial Checks** window, address all the issues and then click **Next** to continue with your current deployment.

Ensure all validations are successful by clicking **Recheck** in the lower right corner of the window.

Step 3 On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations.

Tip
This preparation can take some time. You can click **Exit and Preview Later** and view the work item in the **Tasks** window.

Step 4 In the **Preview Configuration** window, complete these steps:

a) Review the device configurations.

b) Choose a deployment option.

Click...	To...
Deploy or **Submit for Approval**	deploy the device configurations.
Exit and Preview Later	review and deploy the device configurations later. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

Note
You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

Step 5 Schedule the deployment.

a) Indicate when and, if applicable, where you want to deploy the configuration.

If you are submitting the configurations for review, add notes for the IT administrator.

b) Click **Submit**.

You can check the work item approval status or the task deployment status on the **Tasks** window. If it is not approved, resubmit the work item for ITSM approval. When it is approved, the item is deployed at the scheduled time.

Note
After submitting the task, view the progress of the provisioning task with the **Task Progress** bar in the **Activities** > **Tasks** window by clicking the task name.

Assign an unprovisioned device to a site

Use this procedure to assign a device that hasn't been provisioned yet to a site.

Note

- Assigning devices to a site configures Catalyst Center as the syslog and SNMP trap server, which enables Syslog Level 2 and configures global telemetry settings.
- A wireless AP that hasn't been provisioned yet can be assigned to only a floor. Later, if it's still unprovisioned, it can be unassigned from the floor by removing it from its assigned floor map. For more information, see "Remove APs from a map" in the *Cisco Catalyst Center User Guide*.
- Third-party devices can be assigned to a site, but the devices are not managed by Catalyst Center. It's only for visibility.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.
The **Inventory** window displays the device information gathered during the discovery process.

Step 2 Check the check box for the devices that you want to assign to a site.

Note
You cannot assign Firepower Threat Defense (FTD) high availability (HA) paired devices to different sites. Assign both devices in the pair to the same site.

Step 3 From the **Actions** menu, choose **Provision** > **Assign Device to Site**.

Step 4 In the **Assign Device to Site** slide-in pane, click the link next to the Site icon ( ) for the device.

Step 5 In the **Choose a floor** slide-in pane, select the floor to assign to the device and click **Save**.

Step 6 (Optional) If you select multiple devices to add to the same location, check the **Apply to All** check box for the first device to assign its location to the rest of the devices and click **Next**.

Step 7 Review summary settings and click **Next**.

Note
Application Telemetry and Controller-Based Application Recognition (CBAR) is enabled on the applicable network devices by default, if you enable **Application Telemetry** and **CBAR** in the **Design** > **Network Settings** > **Telemetry** window. For more information, see Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry, on page 76.

Application and Endpoint Visibility enablement is skipped by default for the devices that does not support Controller-Based Application Recognition (CBAR) enablement or undeployed Application Visibility Service (AVS).

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 64.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 64.

Note

If only MD5 authentication type is configured on the device, the site assignment will be blocked for devices with software image version or golden tagged image version 17.14.1 and later.

To continue the site assignment, you must configure SHA authentication as well. For information on how to configure SHA as the authentication type for SNMP credentials, see "Edit Global Device Credentials" in the *Catalyst Center User Guide*.

Step 9 On the **Tasks** window, monitor the task deployment.

Step 10 When assigning devices to a site, if **Device Controllability** is enabled, a workflow automatically triggers to push the device configuration from the site to the devices.

For more information, see the Device Controllability section in the *Cisco Catalyst Center Administrator Guide*.

From the **Focus** drop-down list, choose **Provision** and click **See Details** in the **Provision Status** column. The configuration that is pushed to the device is shown in a separate window if you enabled **Device Controllability**.

Add APs to a map

This procedure describes how to add APs to a floor map. You can add a maximum of 200 APs to a floor.

Before you begin

Make sure that you have Cisco APs in your inventory. If not, discover them using the Discovery feature. See Discovery overview, on page 14.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 From the map toolbar, click **2D** > **Add/Edit**.

By default, the **Devices** and **Access Points** toggle buttons are chosen.

Step 4 In the left pane of the map, click **Add Access Points**.

Step 5 In the **Add Access Points** slide-in pane, do one of these tasks in the table:

Task	Action
To add a single AP	Locate the AP that you want to add, and scroll to the right and click **Add**
To add multiple APs	Check the check boxes next to the APs you want to add, and click **Add Selected**.
To add all APs	Click **All APs**, and click **Add Selected**.
To add autolocate capable APs	Click **Auto Locate Capable APs**, and click **Add Selected**.

Note
You can search for APs using the search option available. Use the **Filter** field to search for APs using the AP name, MAC address, model, or Cisco Wireless Controller. The search is case-insensitive. The search results appear in a table. Click **Add** to add one or more of these APs to the floor area.

In edit mode, newly added APs are displayed in the **Unpositioned** category in the map left pane. For more information, see Position an AP on a map, on page 68.

Step 6 After adding the APs to a floor, close the **Add Access Points** slide-in pane.

What to do next

When you add an AP to a map, the wireless map automatically stores this data even after the AP is deleted from the inventory:

- AP name
- AP MAC address
- Current site of the AP
- Current position of the AP on the map

Note If you delete the corresponding site from the network hierarchy, the stored AP data is also removed.

When you delete the wireless controller with all its managed APs from the inventory, Catalyst Center displays a planned AP icon for the corresponding APs on the map. For more information, see "About the AP Icon and Planned AP Icon" in the *Cisco Catalyst Center User Guide*.

If the same AP is rediscovered in the inventory later, Catalyst Center automatically places it back on the map at the same site and position even if a different wireless controller manages it.

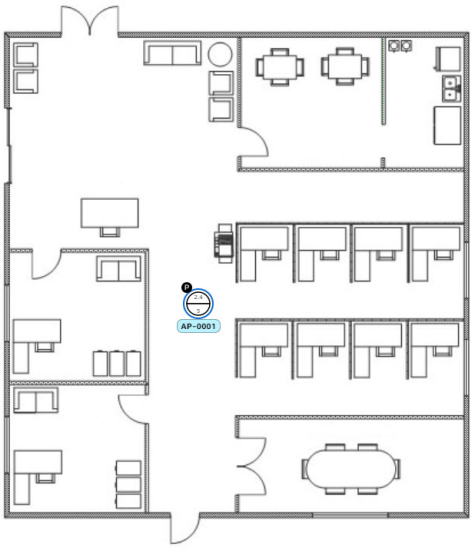
To remove the AP data from the map when the AP is deleted from the inventory, do one of these tasks:

- Before deleting the wireless controller from the inventory, assign the corresponding APs to the **Global** site. For more information, see Assign an unprovisioned device to a site, on page 65.
- After deleting the wireless controller from the inventory, remove the corresponding planned APs from the map. For more information, see "Remove APs from a Map" in the *Cisco Catalyst Center User Guide*.

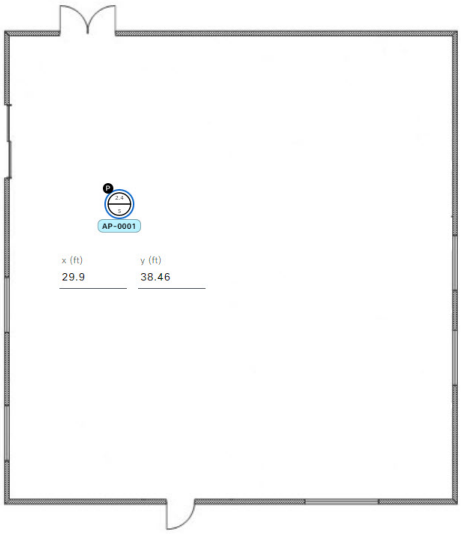
Position an AP on a map

After adding an AP to a floor, you must position it on the map using one of these methods:

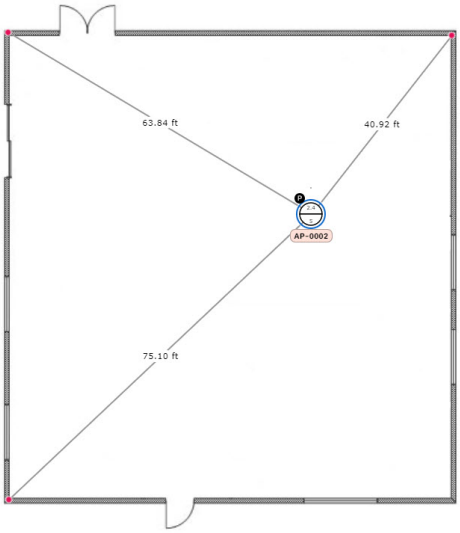
- Manually position it on the map. Use this method if you can approximate the location of the AP using reference points in the building that you can correlate to the detail on the floor map.



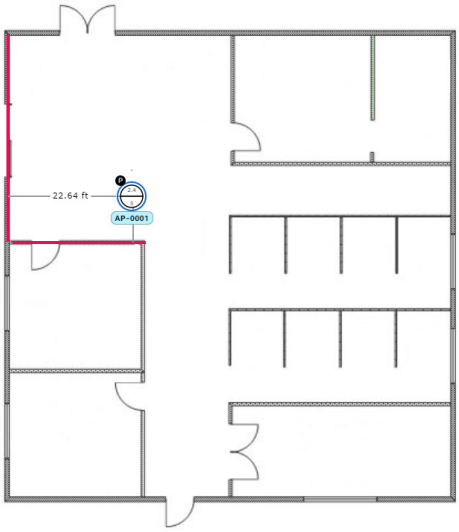
- Define its **x** and **y** coordinates. Use this method if you have the exact coordinates of the AP and you want its position on the map to be as accurate as possible.



- Triangulate it using 3 points. Use this method if you have large open space with only a few points from which to measure the distance to the AP. For example, you might measure from the AP to each corner of the room.



- Intersect it based on its distance from two walls. Use this method if the AP is located in a space where you have two walls that intersect, even if they aren't perpendicular to one another.



For all but the first method (manual positioning), you must have your measurements on hand, and make sure the unit of measure is specified correctly in the **Global Map Properties** settings. For information, see 2D map view options.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

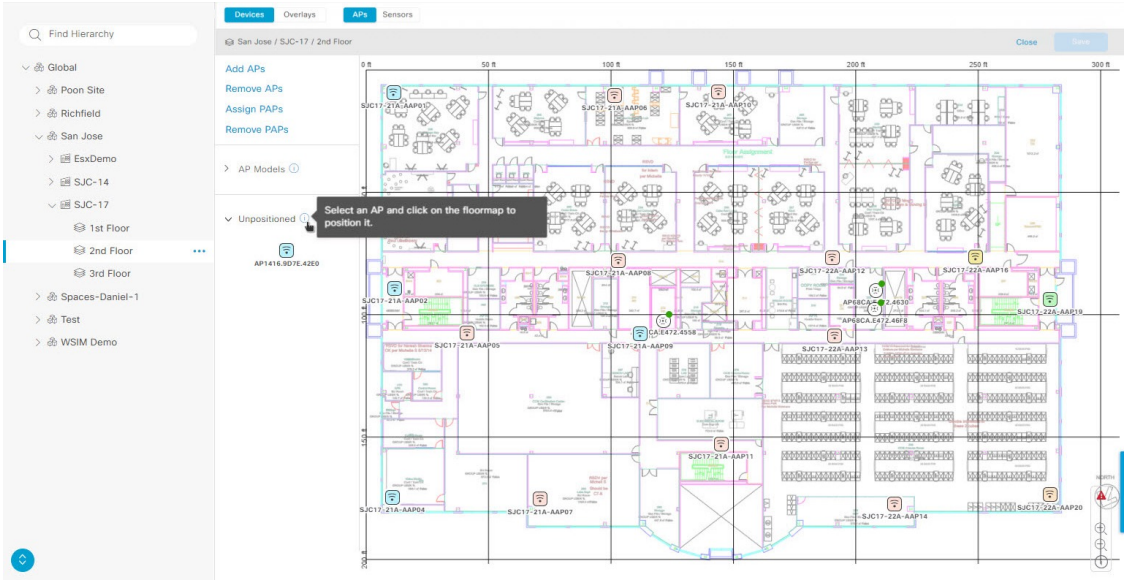
Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit**.

By default, the **Devices** and **Access Points** toggle buttons are chosen.

Step 4 From the left pane of the map, in the **Unpositioned** area, click an AP.

Figure 7: Unpositioned APs



Step 5 To position the AP, use one of these methods:

- Click the location on the floor map where you want to position the AP.
- Define its **x** and **y** coordinates in the **Edit AP** slide-in pane.
- Triangulate its location:

  a. In the **Edit AP** slide-in pane, click **3 points**.

  b. Click on floor map to draw the first point.

  c. In the dialog box, set the distance from the AP to the first point and click **Set Distance**.

  d. Define the second and third points similarly, and click **Save**.

- Define two walls on the floor map and position the APs between the defined walls:

  a. In the **Edit AP** slide-in pane, click **2 walls**.

  b. To define the first wall, click the floor map to start drawing the line. Click again to finish drawing the line.

  A dialog box is displayed to set the distance from the AP to the first wall.

  c. Enter the distance in meters, and click **Set Distance**.

  d. Define the second wall similarly, making sure that the distance to the AP from the first and second walls create an intersecting point.

  e. Click **Save**.

  The AP is placed based on the defined distance between the walls.

Step 6 In the map toolbar, click **Save**.

Note
If Cisco Connected Mobile Experiences (CMX) is synchronized with Catalyst Center, you can view the location of clients on the heatmap. See Create Cisco CMX settings, on page 432.

About Cisco ISE configuration for Catalyst Center

If your network uses Cisco ISE for user authentication, you can configure Catalyst Center for Cisco ISE integration. This enables you to see more information about wired clients, such as the username and operating system.

Cisco ISE configuration is centralized within NCP (Network Control Platform), which enables you to configure Cisco ISE at one GUI location. Here's the workflow for configuring Cisco ISE:

1. From the main menu, choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers**, and enter the Cisco ISE server details.
2. After the Cisco ISE server is successfully added, NCP establishes a connection with NDP (Network Data Platform) and sends the details of the pxGrid nodes, keystore, and truststore files.
3. NDP uses the configuration received from NCP to establish a pxGrid session.
4. NCP automatically detects pxGrid node failovers, persona moves, and communicates it to NDP.
5. If there are ISE deployment changes, NDP starts a new pxGrid session with a new pxGrid ACTIVE node.

Configure authentication and policy servers

Catalyst Center uses AAA servers for user authentication and Cisco ISE for both user authentication and access control. Use this procedure to configure AAA servers, including Cisco ISE.

Before you begin

If you are using Cisco ISE to perform both policy and AAA functions, make sure that Catalyst Center and Cisco ISE are integrated.

If you are using another product (not Cisco ISE) to perform AAA functions, do these tasks:

- Register Catalyst Center with the AAA server, including defining the shared secret on both the AAA server and Catalyst Center.
- Define an attribute name for Catalyst Center on the AAA server.
- For a Catalyst Center multihost cluster configuration, define all individual host IP addresses and the virtual IP address for the multihost cluster on the AAA server.

Before you configure Cisco ISE, confirm that:

- You have deployed Cisco ISE on your network. For information on supported Cisco ISE versions, see the Cisco Catalyst Center Compatibility Matrix. For information on installing Cisco ISE, see the Cisco Identity Services Engine Install and Upgrade guides.

- If you have a standalone Cisco ISE deployment, you must integrate Catalyst Center with the Cisco ISE node and enable the pxGrid service and External RESTful Services (ERS) on that node.
- If you have a distributed Cisco ISE deployment:

  You must integrate Catalyst Center with the primary policy administration node (PAN), and enable ERS on the PAN.



Note We recommend that you use ERS through the PAN. However, for backup, you can enable ERS on the Policy Service Nodes (PSNs).

  You must enable the pxGrid service on one of the Cisco ISE nodes within the distributed deployment. Although you can decide to do so, you do not have to enable pxGrid on the PAN. You can enable pxGrid on any Cisco ISE node in your distributed deployment.

  The PSNs that you configure in Cisco ISE to handle TrustSec or SD Access content and Protected Access Credentials (PACs) must also be defined in **Work Centers** > **Trustsec** > **Trustsec Servers** > **Trustsec AAA Servers**. For more information, see the *Cisco Identity Services Engine Administrator Guide*.

- You must enable communication between Catalyst Center and Cisco ISE on these ports: 443, 5222, 8910, and 9060.
- The Cisco ISE host on which pxGrid is enabled must be reachable from Catalyst Center on the IP address of the Cisco ISE eth0 interface.
- The Cisco ISE node can reach the fabric underlay network via the appliance's NIC.
- The Cisco ISE admin node certificate must contain the Cisco ISE IP address or the fully qualified domain name (FQDN) in either the certificate subject name or the Subject Alternative Name (SAN).
- The Catalyst Center system certificate must list both the Catalyst Center appliance IP address and FQDN in the SAN field.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers**.

Step 2 From the **Add** drop-down list, select **AAA** or **ISE**.

Step 3 To configure the primary AAA server, enter this information:

- **Server IP Address**: IP address of the AAA server.
- **Shared Secret**: Key for device authentications. The shared secret must contain from 4 to 100 characters. It cannot contain a space, question mark (?), or less-than angle bracket (<).

Note
Make sure that you do not configure a PSN that is part of an existing Cisco ISE cluster as a primary AAA server.

Step 4 To configure a Cisco ISE server, enter these details:

- **Server IP Address**: IP address of the Cisco ISE server.

- **Shared Secret**: Key for device authentications. The shared secret must contain from 4 to 100 characters. It cannot contain a space, question mark (?), or less-than angle bracket (<).
- **Username**: Username that is used to log in to Cisco ISE via HTTPS.
- **Password**: Password for the Cisco ISE HTTPS username.

  Note
  The username and password must be an ISE admin account that belongs to the Super Admin.

- **FQDN**: Fully qualified domain name (FQDN) of the Cisco ISE server.

  Note
  - We recommend that you copy the FQDN that is defined in Cisco ISE (**Administration** > **Deployment** > **Deployment Nodes** > **List**) and paste it directly into this field.
  - The FQDN that you enter must match the FQDN, Common Name (CN), or Subject Alternative Name (SAN) defined in the Cisco ISE certificate.

  The FQDN consists of two parts, a hostname and the domain name, in this format:

  hostname.domainname.com

  For example, the FQDN for a Cisco ISE server can be ise.cisco.com.

- **Virtual IP Address(es)**: Virtual IP address of the load balancer behind which the Cisco ISE policy service nodes (PSNs) are located. If you have multiple PSN farms behind different load balancers, you can enter a maximum of six virtual IP addresses.

Step 5 Click **Advanced Settings** and configure the settings:

- **Connect to pxGrid**: Check this check box to enable a pxGrid connection.

  If you want to use the Catalyst Center system certificate as the pxGrid client certificate (sent to Cisco ISE to authenticate the Catalyst Center system as a pxGrid client), check the **Use Catalyst Center Certificate for pxGrid** check box. You can use this option if all the certificates that are used in your operating environments must be generated by the same Certificate Authority (CA). If this option is disabled, Catalyst Center will send a request to Cisco ISE to generate a pxGrid client certificate for the system to use.

  When you enable this option, ensure that:

  - The Catalyst Center certificate is generated by the same CA as is in use by Cisco ISE (otherwise, the pxGrid authentication fails).
  - The Certificate Extended Key Use (EKU) field includes "Client Authentication."

- **Enable Multiple Catalyst Center operation**: Check this check box to integrate more than one Catalyst Center cluster with a single Cisco ISE system.
- **Protocol**: **RADIUS** (the default) and **TACACS**. You can select both protocols.

  Attention
  If you do not enable TACACS for a Cisco ISE server here, you cannot configure the Cisco ISE server as a TACACS server under **Design** > **Network Settings** > **Servers** when configuring a AAA server for network device authentication.

- **Authentication Port**: UDP port used to relay authentication messages to the AAA server. The default UDP port used for authentication is 1812.

- **Accounting Port**: UDP port used to relay important events to the AAA server. The default is UDP port 1812.
- **Port**: TCP port used to communicate with the TACACS server. The default TCP port used for TACACS is 49.
- **Retries**: Number of times that Catalyst Center attempts to connect with the AAA server before abandoning the attempt to connect. The default number of attempts is 3.
- **Timeout**: The time period for which the device waits for the AAA server to respond before abandoning the attempt to connect. The default timeout is 4 seconds.

Note
After the required information is provided, Cisco ISE is integrated with Catalyst Center in two phases. It takes several minutes for the integration to complete. The phase-wise integration status is shown in the **Authentication and Policy Servers** window and **System 360** window.

Cisco ISE server registration phase:

- **Authentication and Policy Servers** window: "In Progress"
- **System 360** window: "Primary Available"

pxGrid subscriptions registration phase:

- **Authentication and Policy Servers** window: "Active"
- **System 360** window: "Primary Available" and "pxGrid Available"

If the status of the configured Cisco ISE server is shown as "FAILED" due to a password change, click **Retry**, and update the password to resynchronize the Cisco ISE connectivity.

Step 6 Click **Add**.

Step 7 To add a secondary server, repeat the preceding steps.

Step 8 To view the Cisco ISE integration status of a device:

a. From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information.

b. From the **Focus** drop-down menu, select **Provision**.

c. In the **Devices** table, the **Provisioning Status** column displays information about the provisioning status of your device (**Success**, **Failed**, or **Not Provisioned**).

Click **See Details** to open a slide-in pane with additional information.

d. In the slide-in pane that appears, click **See Details**.

e. Scroll down to the **ISE Device Integration** tile to view detailed information about the integration status of the device.

Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry

With Catalyst Center, you can configure global network settings when devices are assigned to a specific site. Telemetry polls network devices and collects telemetry data according to the settings in the SNMP server, syslog server, NetFlow Collector, or wired client.

Before you begin

Create a site and assign a device to the site. See Create, edit, and delete a site, on page 32.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings** > **Telemetry**.

Step 2 In the **SNMP Traps** area, do one of these tasks:

- Check the **Use Catalyst Center as SNMP trap server** check box.
- Check the **Add an external SNMP trap server** check box and enter the IP address of the external SNMP trap server. The selected server collects SNMP traps and messages from the network devices.

Step 3 In the **Syslogs** area, do one of these tasks:

- Check the **Use Catalyst Center as syslog server** check box.
- Check the **Add an external syslog server** check box and enter the IP address of the external syslog server.

Step 4 In the **Application Visibility** area, check the **Enable by default on wired access devices** check box to enable Application Telemetry and Controller-Based Application Recognition (CBAR) by default upon the network device site assignment.

Do one of these tasks:

- Click the **Use Catalyst Center as NetFlow collector** radio button. The NetFlow configuration on the device interfaces is completed only when you enable application telemetry on the device. Select the NetFlow collector at the site level to configure the NetFlow destination server to the device.
- Click the **Add Cisco Telemetry Broker (CTB)** radio button and add the IP address and port number of the Cisco Telemetry Broker. The Cisco Telemetry Broker collects NetFlow records from the device and sends the information to the destination.

  Note
  Catalyst Center must be configured as a destination in Cisco Telemetry Broker to receive NetFlow records. If Catalyst Center is not configured as a destination, the Application Experience does not work.

Step 5 In the **Wired Endpoint Data Collection** area, click the **Enable Catalyst Center Wired Endpoint Data Collection At This Site** radio button to turn on IP Device Tracking (IPDT) on the access devices of the site.

If you don't want to enable IPDT for the site, click the **Disable Catalyst Center Wired Endpoint Data Collection At This Site** radio button (the default).

After enabling IPDT, clients connected to access ports are visible in Catalyst Center. Clients connected to trunk ports and port channels aren’t visible in Catalyst Center.

Note
You must enable IPDT to preview the CLI configuration. When provisioning a device, you can preview the CLI configuration before deploying it on the device.

Step 6 In the **Wireless Controller, Access Point and Wireless Clients Health** area, check the **Enable Wireless Telemetry** check box to monitor the health of the wireless controllers, APs, and wireless clients in your network.

During the Device Controllability workflow, enabling Wireless Telemetry activates telemetry data collection and provisions telemetry commands to wireless configurations. When you disable this feature, telemetry setup stops, and monitoring capabilities are lost. For more information, see Device controllability in *Cisco Catalyst Center Administrator Guide*.

Step 7 Click **Save**.

Configure Cisco AI Network Analytics

Use this procedure to enable the Cisco AI Analytics features to export network event data from network devices and inventory, site hierarchy, and topology data to the Cisco AI Cloud.

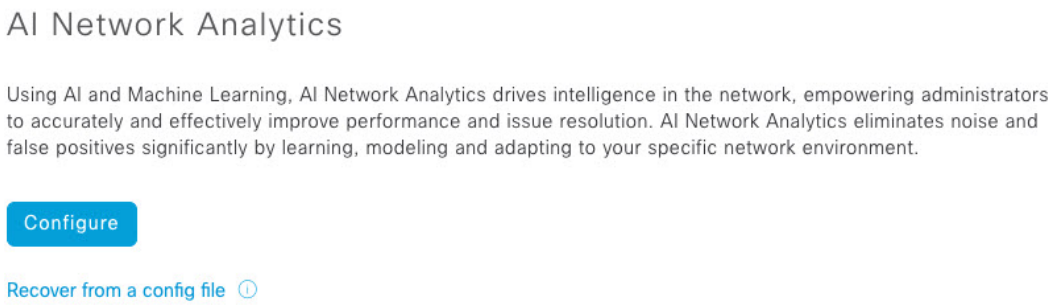
Before you begin

- Make sure that you have the Advantage software license for Catalyst Center. The **AI Network Analytics** application is part of the Advantage software license.
- Make sure that the latest version of the AI Network Analytics application is installed. See the "Download and Install Packages and Updates" topic in the *Cisco Catalyst Center Administrator Guide*.
- Make sure that your network or HTTP proxy is configured to allow outbound HTTPS (TCP 443) access to these cloud hosts:
  - **api.use1.prd.kairos.ciscolabs.com** (US East Region)
  - **api.euc1.prd.kairos.ciscolabs.com** (EU Central Region)

Procedure

Step 1 From the main menu, choose **System** > **Settings**.

Step 2 Scroll down to **External Services** and select **Cisco AI Analytics**.
The **AI Network Analytics** window opens.



Step 3 Do one of these tasks:

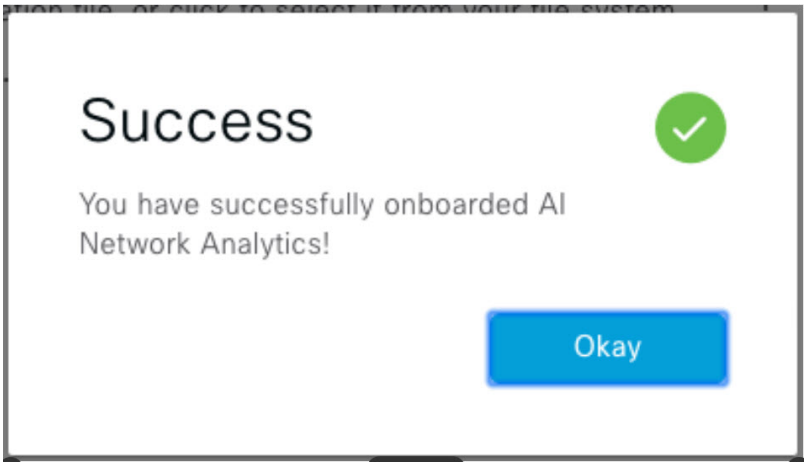
- If you have an earlier version of Cisco AI Network Analytics installed in your appliance, do these steps:
  a. Click **Recover from a config file**.

     The Restore AI Network Analytics window opens.

  b. Drag-and-drop the configuration files in the area provided or select the files from your file system.

  c. Click **Restore**.

     Cisco AI Network Analytics might take a few minutes to restore, and then the **Success** dialog box opens.



- For the first-time configuration of Cisco AI Network Analytics, do these steps:
  a. Click **Configure**.

  b. In the **Where should we securely store your data?** area, select the location to store your data. Options are: **Europe (Germany)** or **US East (North Virginia)**.

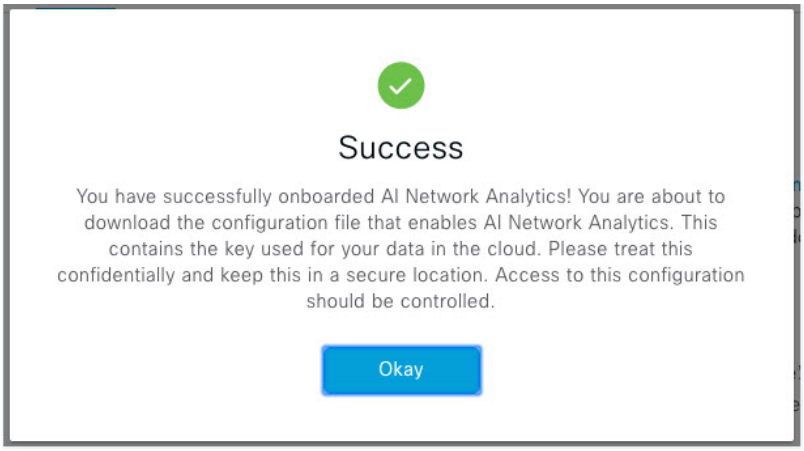
     The system starts testing cloud connectivity as indicated by the **Testing cloud connectivity...** tab. After cloud connectivity testing completes, the **Testing cloud connectivity...** tab changes to **Cloud connection verified**.

  c. Click **Next**.

     The terms and conditions window opens.

d. Click the **Accept Cisco Universal Cloud Agreement** check box to agree to the terms and conditions, and then click **Enable**.

Cisco AI Network Analytics might take a few minutes to enable, and then the **Success** dialog box opens.



Step 4 In the **Success** dialog box, click **Okay**.
The **AI Network Analytics** window opens, and the **Enable AI Network Analytics** toggle button displays .

Step 5 (Recommended) In the **AI Network Analytics** window, click **Download Configuration file**.

Disable Cisco AI Network Analytics

To disable Cisco AI Network Analytics data collection, you must disable the AI Network Analytics feature:

Procedure

Step 1 From the main menu, choose **System** > **Settings**.

Step 2 Scroll down to **External Services** and choose **Cisco AI Analytics**.

For each feature, a check mark ( ) indicates that the feature is enabled. If the check box is unchecked ( ), the feature is disabled.

Step 3 In the **AI Network Analytics** area, click the **Enable AI Network Analytics** toggle button so that it's unchecked ( ).

Step 4 Click **Update**.

Step 5 To delete your network data from the Cisco AI Network Analytics cloud, contact the Cisco Technical Response Center (TAC) and open a support request.

Step 6 If you have misplaced your previous configuration, click **Download configuration file**.

Update the Machine Reasoning Knowledge Base

Machine Reasoning knowledge packs are step-by-step workflows that are used by the Machine Reasoning Engine (MRE) to identify security issues and improve automated root cause analysis. These knowledge packs are continuously updated as more information is received. The Machine Reasoning Knowledge Base is a repository of these knowledge packs (workflows). To have access to the latest knowledge packs, you can either configure Catalyst Center to automatically update the Machine Reasoning Knowledge Base daily, or you can do a manual update.

Procedure

Step 1 From the main menu, choose **System** > **Settings**.

Step 2 Scroll down to **External Services** and select **Machine Reasoning Knowledge Base**.
The **Machine Reasoning Knowledge Base** window shows this information:

- **INSTALLED**: Shows the installed version and installation date of the Machine Reasoning Knowledge Base package.

When there's a new update to the Machine Reasoning Knowledge Base, the **AVAILABLE UPDATE** area is displayed in the **Machine Reasoning Knowledge Base** window, which provides the **Version** and **Details** about the update.

- **AUTO UPDATE**: Automatically updates the Machine Reasoning Knowledge Base in Catalyst Center daily.
- **CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER, SECURITY ADVISORY, FIELD NOTICES AND EOX**: Integrates Catalyst Center with CX Cloud that allows you to perform an automated config. This integration provides enhanced vulnerability detection on devices directly from the security advisories tool on Catalyst Center.

Step 3 (Recommended) Check the **AUTO UPDATE** check box to automatically update the Machine Reasoning Knowledge Base.
The **Next Attempt** area shows the date and time of the next update.

You can perform an automatic update only if Catalyst Center is successfully connected to the Machine Reasoning Engine in the cloud.

Step 4 To manually update the Machine Reasoning Knowledge Base in Catalyst Center, do one of these tasks:

- Under **AVAILABLE UPDATES**, click **Update**. A **Success** pop-up window appears with the status of the update.
- Manually download the Machine Reason Knowledge Base to your local machine and import it to Catalyst Center. Do these steps:

  a. Click **Download**.

  The **Opening mre_workflow_signed** dialog box appears.

  b. Open or save the downloaded file to the desired location in your local machine, and then click **OK**.

  c. Click **Import** to import the downloaded Machine Reasoning Knowledge Base from your local machine to Catalyst Center.

Step 5 Check the **CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER AND SECURITY ADVISORY** check box to enable Cisco CX Cloud connection with network bug identifier and security advisory.

Step 6 In the **Security Advisories Settings** area click the **RECURRING SCAN** toggle button to enable or disable the weekly recurring scan.

Step 7 Click the **CISCO CX CLOUD** toggle button to enable or disable the Cisco CX cloud.

Enable localization

You can view the Catalyst Center GUI windows in English (the default), Chinese, Japanese, or Korean.

To change the default language:

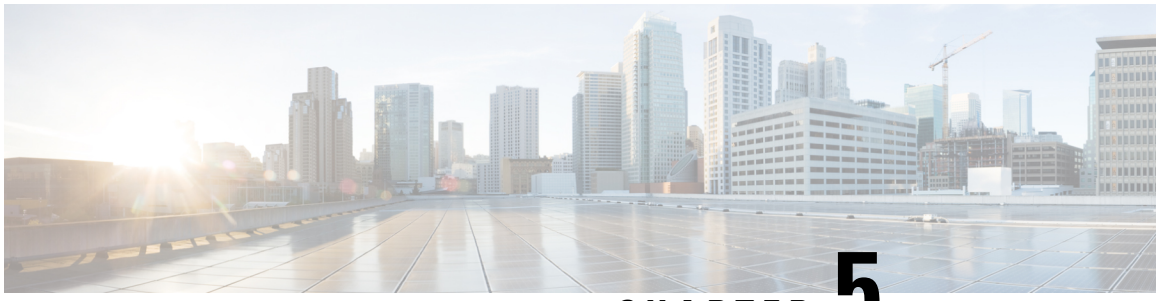
Procedure

Step 1 In your browser, change the locale to one of the supported languages: Chinese, Japanese, or Korean.

- From Google Chrome:
  1. **a.** Click the icon in the top-right corner, and then select **Settings**.
  2. **b.** Click **Languages**.
  3. **c.** Click **Add languages**.
  4. **d.** In the **Add languages** dialog box, select **Chinese**, **Japanese**, or **Korean**, and then click **Add**.
- From Mozilla Firefox:
  1. **a.** Click the icon in the top-right corner, and then select **Settings**.
  2. **b.** From the **Language and Appearance** > **Language** area, click **Choose**.
  3. **c.** From the **Select a language to add** drop-down list, select **Chinese**, **Japanese**, or **Korean**.
  4. **d.** Click **OK**.

Step 2 Log in to Catalyst Center.

The GUI shows in the selected language.



CHAPTER 5

Monitor and Troubleshoot Overall Enterprise Health

- Enterprises, on page 83
- Monitor and troubleshoot the overall health of your enterprise, on page 83

Enterprises

An enterprise is a network context that

- includes network devices, routers, switches, wireless controllers, and access points,
- enables monitoring and troubleshooting of overall health of your enterprise health in Assurance.
- supports analysis and visibility for proactive management.

You can use Assurance to monitor and troubleshoot the overall health of your enterprise. Your enterprise consists of network devices and clients.

A network consists of one or more devices, including routers, switches, wireless controllers, and access points. Note that clients and devices in maintenance mode are not part of the network health score.

A client is an end device (computer, phone, and so on) that is connected to a network device (access point or switch). Catalyst Center supports both wired and wireless clients.

Monitor and troubleshoot the overall health of your enterprise

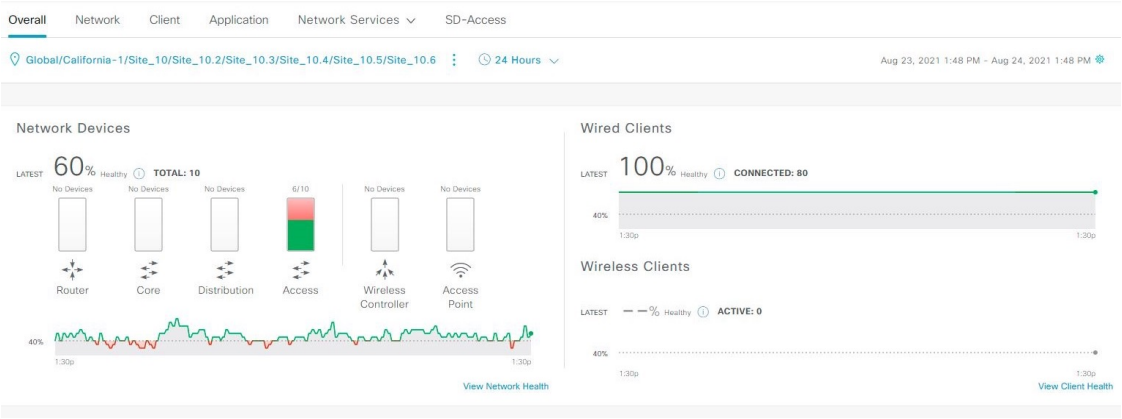
Use this procedure to get a global view of the health of your enterprise, which includes network devices and clients, and to determine if there are potential issues that must be addressed. Assurance supports site-based, role-based access control (SRBAC), which limits a user's scope of access to certain network sites. You must ensure you have access to the sites and devices while using the overall health dashboard. For more information on user roles and permissions, see Cisco Catalyst Center Administrator Guide.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Figure 8: Overall health dashboard



Step 2 Use the **Overall** health dashboard top menu bar for this functionality:

Overall health dashboard top menu bar	
Item	**Description**
Global **Location** pane	• Click Global to select the site, building, or floor from the Site hierarchy. • Click next to the location icon and select **Site Details** to view the Sites table. From the **Sites Details** table, you can do this functionality: • Click Hide Sites to hide the Sites table. • : Click this toggle button and use the drop-down list to select **Hierarchical Site View** or **Building View**. Based on what you select, the table displays the percentage of healthy clients and network devices for a specific location. • : Click this toggle button to display the health of all the sites in your enterprise on a geographic location-oriented health map. By default, the sites that are represented are color coded according to the severity of the problem. The color of the health score represents its severity. The health is measured on a scale of 1 to 10, where 10 is the best score. A score of 0 indicates that data could not be obtained. • From the **Go to sites** column, click for a site or building to display data only for that location on the **Overall** dashboard.
Time range	Enables you to display data for the last 3 hours, 24 hours, or 7 days.

Overall health dashboard top menu bar	
Item	**Description**
Actions drop-down list	Enables you to export the overall dashboard to PDF format. Click **Export Dashboard** to view the preview page and click **Save**. Enables you to customize the dashboard display when you select **Edit Dashboards** from the drop-down list. See Change the position of a dashlet, on page 349 and Create a custom dashboard, on page 347.

Step 3 Use the **Overall Health Summary** dashlet for this functionality:

Overall Health Summary dashlet	
Item	**Description**
Network Devices	**Network Score**: Percentage of healthy (good) devices (routers, switches, wireless controllers, and access points) in your overall enterprise. See Network Health score, on page 113. **Device Category Health Score**: Percentage of healthy (good) network devices for these device categories: **Router**, **Core** (including third-party devices), **Distribution**, **Access**, **Controller** and **Access Point**. **Note** When an SD-Access fabric is selected, this area provides the percentage of healthy network devices for these categories: **Fabric Edge**, **Fabric Border**, and **Fabric Control Plane**. Click **View Network Health** to open the **Network Health** dashboard. See Monitor and troubleshoot the health of your network, on page 87.
Wired Clients and **Wireless Clients**	Provides the score distribution between wired and wireless clients. The **Wired Client** score or the **Wireless Client** score is the percentage of healthy (good) wired or wireless client devices in your overall enterprise. See Client Health score, on page 153. Click **View Client Health** to open the **Client Health** dashboard. See Monitor and troubleshoot the health of all client devices, on page 123.

Step 4 Use the **Network Services** dashlet for this functionality:

Network Services dashlet	
Item	**Description**
AAA	Provides the total percentage of successful and failure transactions for all the AAA servers in your overall enterprise. Click **View AAA Dashboard** to open the **Network Services AAA** dashboard. See Monitor the AAA network service, on page 191.
DNS	Provides the total percentage of successful and failure transactions for all the DNS servers in your overall enterprise. Click **View DNS Dashboard** to open the **Network Services DNS** dashboard. See Monitor the DNS network service, on page 198.

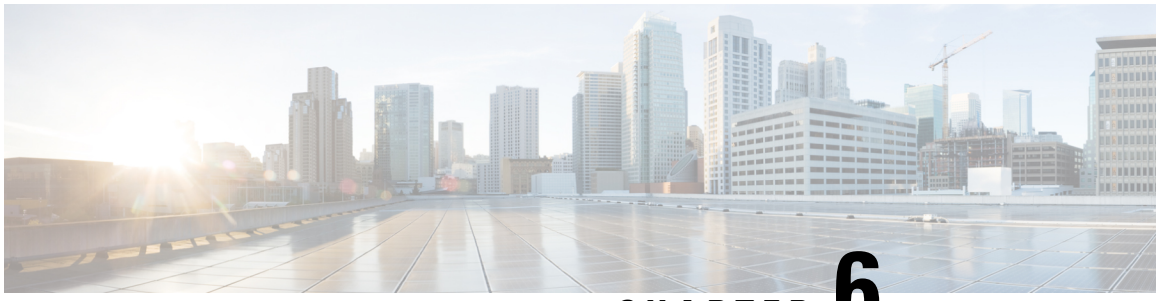
Network Services dashlet	
Item	**Description**
DHCP	Provides the total percentage of successful and failure transactions for all the DHCP servers in your overall enterprise. Click **View DHCP Dashboard** to open the **Network Services DHCP** dashboard. See Monitor the DHCP network service, on page 195.

Step 5 Use the **Site Analytics** dashlet for this functionality:

Site Analytics dashlet
The **Site Analytics** dashlet displays the sites with the worst wireless networking performance in terms of aggregated coverage, onboarding, roaming, and connection speed. The performance is based on the default performance thresholds or ones that you set in the **Site Analytics Settings** window. For information, see Configure Site Analytics settings, on page 238. AI Network Analytics must be enabled for site analytics data to be collected. Click the **Enable AI Network Analytics** link to go directly to the **Cisco AI Analytics** window where you can configure this system setting. For information, see Configure Cisco AI Network Analytics, on page 77. Under each KPI category, click a site name to display more information about the site or click **View Site Analytics** to go directly to the **Site Analytics** window. For information, see Monitor and Troubleshoot Your Network Using Site Analytics, on page 229. **Note** If AI Network Analytics isn't enabled, Assurance displays an example dashlet with sample data.

Step 6 Use the **Top 10 Issue Type** dashlet for this functionality:

Top 10 Issue Type Dashlet
Displays the top 10 issues, if any, that must be addressed. The issues are color coded and sorted by their preassigned priority level, starting with P1. Click an issue to open a slide-in pane with additional details about the issue type. From the slide-in pane, click an issue instance where you can do these tasks, as required: • To resolve the issue instance, from the **Status** drop-down list, select **Resolve**. • To ignore the issue instance: **a.** From the **Status** drop-down list, select **Ignore**. **b.** Set the number of hours to ignore the issue on the slider. **c.** Click **Confirm**. Click **View All Open Issues** to open the **Open Issues** window. For information about issues, see View open issues, on page 241.



CHAPTER 6

Monitor and Troubleshoot Network Health

- Monitor and troubleshoot the health of your network, on page 87
- Monitor and troubleshoot the health of a device, on page 95
- Configure health score settings for network devices, on page 109
- Enable SNMP Collector metrics for fabric devices, on page 111
- Understand network health score and KPI metrics, on page 113
- Understand RF calculations, on page 120

Monitor and troubleshoot the health of your network

Use this procedure to get a global view of your network and to determine if there are potential issues that must be addressed.

A network consists of one or more devices, including routers, switches, wireless controllers, and access points. Be aware that clients and devices in maintenance mode are not part of the network health score.

Assurance supports site-based, role-based access control (SRBAC), which limits a user's scope of access to certain network sites. You must ensure you have access to the sites and devices while using the network health dashboard. For more information on user roles and permissions, see Cisco Catalyst Center Administrator Guide

Note The network health score exists only in the context of a location. If the location of a device is not available, it is not counted in the network health score.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Network** tab.

The **Network** health dashboard appears.

Figure 9: Network health dashboard



Step 3 Click the location option (Global) in the top menu bar to select the site, building, or floor from the Site hierarchy.

Step 4 Click ⋮ next to the location icon and to switch between:

- **Site Map**: Provides a geographical view of your network hierarchy.
- **Site Table**: Provides a list-based view of all sites, including their health scores and device counts.

The location pane has this functionality:

Location option	
Item	**Description**
toggle button **List View**	Click this toggle button to display the sites and buildings from your network in a list format. Click the drop-down list for these options: • **Hierarchical Site View**: Sorts the list at a site level. From the **Go to sites** column, click for a site or building to display data only for that location on the **Network** dashboard. • **Building/Outdoor Area view** : Sorts the list at a building level. From the **Go to sites** column, click for a site or building to display data only for that location on the **Network** dashboard.
Export	Click **Export** to export the device information to a CSV file.

Location option	
Item	**Description**
 toggle button **Map View**	Click this toggle button to display the health of all the network sites on a geographic location-oriented network health map. By default, the network sites are color coded according to the severity of the problem.
	Click this close icon to hide the map or table view.

Step 5 Click the time range setting () in the top menu bar to specify the time range of data that appears on the dashboard.

a) From the drop-down menu, select the time range: **3 Hours**, **24 Hours**, or **7 Days**.
b) Specify the **Start Date** and time, and the **End Date** and time.
c) Click **Apply**.

Step 6 Click the **Actions** drop-down list in the top menu bar for this functionality:

- **Export Dashboard**: Enables you to export the network dashboard to PDF format. Click **Export Dashboard** to view the preview page and click **Save**.
- **Edit Dashboard**: Enables you to customize the dashboard display. See Change the position of a dashlet, on page 349 and Create a custom dashboard, on page 347.

Step 7 Use the **Network Health** timeline for this functionality.

You can specify a more granular time range. You can click and drag the timeline boundary lines to specify the time range. This sets the context for the custom charts on the dashboard.

You can use the arrow buttons on the right of the timeline to view data for up to 30 days.

Hover your cursor within the timeline chart to view the network device health score percentage at a specific time.

The dotted horizontal line represents the threshold for a healthy network, which by default is set to 40%.

To change the threshold value:

a. Hover your cursor over the information () icon.

b. In the tooltip, click the edit () icon.

c. In the **Network Health Threshold** slide-in pane, click and drag the blue line to set the threshold percentage value.

d. Click **Save**.

- Check the **Telemetry Status** check box below the timeline to view the horizontal bar in the timeline. To view the telemetry status:
  - Hover your cursor over the horizontal bar to view the network device telemetry status such as Good, Fair, or Poor in the tool tip
  - Click the **Telemetry Status** in the tool tip to open a slide-in pane to view the summary of the telemetry status.

Note
Changing the custom threshold affects when the Network Device Summary Health Score is displayed as red. The custom threshold does not change the number of healthy or unhealthy devices.

Note
Gaps in the timeline indicate that no health data was retrieved from the device. This situation can occur when a device is in maintenance mode.

Step 8 Use the **Network Devices Health Summary** dashlet for this functionality:

Network Devices health summary dashlet	
Item	**Description**

Network Devices Health Summary area	Includes these tabs:
	• **Latest**: Displayed by default. The left pane provides the network health summary score and the total number of devices. The right pane displays charts.
	  • **Network Health Summary Score**: The Network Health Summary score is the percentage of healthy (good) devices in your overall network or selected site. See Network Health score, on page 113.
	  • **Total Devices**: Provides the total number of network devices and the count of devices that have Good Health, Fair Health, Poor Health, and No Health Data.
	  • **Charts**: This color-coded snapshot-view chart shows the performance of each device category (Access, Core, Distribution, Router, Wireless Controller, and Access Points) over the last 5 minutes.
	  Hover your cursor over a color to display the health score and the number of devices associated with that color.
	  If the chart shows a low health score (red or orange), the KPIs that contributed to the low health score are shown next to the bar. Examples include link errors, high CPU, high memory, high noise, and low air quality.
	  You can also click a hyperlinked device category (**Access**, **Core** (including third party devices), **Distribution**, **Router**, **Wireless Controller**, and **Access Point**) to open a slide-in pane with additional details.
	• **Trend**: Click the **Trend** tab to display a trend chart. This color-coded trend chart shows the performance of devices over a time range. Hover your cursor over the chart to display the total number of devices and their health over time.
	The color in the charts represent the health of the network devices:
	●: Poor network devices. Health score range is 1 to 3.
	●: Fair network devices. Health score range is 4 to 7.
	●: Good network devices. Health score range is 8 to 10.
	●: No Health data (includes third party devices and devices in maintenance mode). Health score is 0.

View Details	Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to refresh the data in the table that is displayed below the chart.

Step 9 Use the **AP** dashlets to view this information:

Total APs up/down dashlet
Color-coded chart that provides this AP status information: number of APs that are connected to the network and the number of APs that are not connected to the network. The **Latest** tab provides a 5-minute snapshot view. The **Trend** tab provides a trend view for the time range that you selected in the time range settings. For example, if the time range is set to the last three hours, the trend tab displays three hours of data. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to refresh the data in the table that is displayed below the chart.

Top N APs by Client Count Dashlet
Chart that provides information about the APs that have the highest number of clients. The **Latest** tab provides a 5-minute snapshot view. The **Trend** tab provides a trend view for the time range that you selected in the time range settings. For example, if the time range is set to the last three hours, the trend tab displays three hours of data. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to refresh the data in the table that is displayed below the chart.

Top N APs by High Interference Dashlet
Information about the APs that have high interference. You can select 2.4 GHz, 5 GHz, or 6 GHz. The **Latest** tab provides a 5-minute snapshot view. The **Trend** tab provides a trend view for the time range that you selected in the time range settings. For example, if the time range is set to the last three hours, the trend tab displays three hours of data. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to refresh the data in the table that is displayed below the chart.

Step 10 Use the **Network Devices** dashlet for this functionality:

Network Devices dashlet	
Item	**Description**
Type	Filter the table based on the device type with these options: **All**, **Access**, **Core**, **Distribution**, **Router**, **WLC**, and **AP**. **Note** When you filter the devices based on device type "Router", it displays the device(s) with device role “Border Routers".

Network Devices dashlet	
Item	**Description**
Overall Health	Filter the table based on the overall health score of the device with these options: • **All** • **Poor**: Devices with a health score range from 1 to 3. • **Fair**: Devices with a health score range from 4 to 7. • **Good**: Devices with a health score range from 8 to 10. • **No Health**: Devices with no health data.
Network Devices table	View device information for all the devices in the network or for a selected site in a table format. **Note** The Overall Health Score is the minimum subscore of these KPI metric health scores: System Health, Data Plane Connectivity, and Control Plane Connectivity. In the **Overall Health Score** column, hover your cursor over a health score. The **Device Health** score is displayed along with the health and percentage value of all of the KPI metrics. The **Device Health** score is the minimum subscore of the KPI metrics, depending on the type of device. For routers and switches, these are the KPI metrics: System Resources (memory utilization and CPU utilization), Data Plane (uplink availability and link errors), and Fabric (Control Plane Reachability). The **Fabric Domain Name**, **Fabric Name** and **Fabric Role** columns display the fabric domain name, fabric name, and fabric role (Edge, Border, Map Server, and so on). Hover over your cursor on device icon against each device to view the reachability status (Reachable, Up, Unreachable, Rebooting, and so on). **Note** For third party devices, the device reachability status is either Reachable or Unreachable.
Device 360	Display a 360° view of a device by clicking the device name in the **Device** column. **Device 360** provides detailed information for troubleshooting device issues. **Note** When a site admin discovers a device that's not assigned to a site, the Device 360 window doesn't show data for the unassigned device. However, a global admin can see data for unassigned devices in the Device 360 window.
Export	Click **Export** to export the device information to a CSV file.

Network Devices dashlet	
Item	**Description**
⚙	Customize the table display: **a.** From the **Table Appearance** tab, set the table density and striping. **b.** From the **Edit Table Columns** tab, select the data you want displayed in the table. **c.** Click **Apply**.

Step 11 Use the **Network Devices Reachability** dashlet to view this information:

Network Devices Reachability Dashlet
Color-coded chart shows the reachability status of routers, switches, and wireless controllers. • **Reachable** • **Unreachable** The **Latest** tab provides a 5-minute snapshot view. The **Trend** tab provides a trend view for the time range that you selected in the time range settings. For example, if the time range is set to the last three hours, the trend tab displays three hours of data. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can hover your cursor over the timeline slider to view the reachability status of over a time period. The Reachability status count of top devices based on role and location is displayed below the timeline slider as horizontal bar graphs. You can select the data displayed as horizontal bars to filter the table based on the reachability status, device types, and location with these options: All, Access, Core, Distribution, Router, and WLC.

Step 12 Use the **WAN Link Utilization** dashlet to view this information:

WAN link use dashlet
The bar chart shows the status of the WAN link use percentage only for the available WAN links. **Note** For a link to be considered a WAN link, you must manually assign the system-generated WAN tag to the required port. See "Assign Tags to Ports" in the Manage Your Inventory chapter of the Catalyst Center User Guide. The **Latest** tab provides a 10-minute snapshot view of **Available** and **Not Available** WAN links. The **Trend** tab provides a trend view for the time range that you selected in the time range settings. For example, if the time range is set to the last three hours, the trend tab displays three hours of data. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can select an element on the chart to view more detailed data. You can select the data displayed as horizontal bars below the timeline slider to filter the table based on top locations, device types, and location.

Step 13 Use the **WAN Link Availability** dashlet to view this information:

WAN link availability dashlet
Color-coded chart displays the information on the available WAN links in your network. The **Latest** tab provides the percentage of WAN links available. The **Trend** tab provides a trend view for the time range that you selected in the time range settings. For example, if the time range is set to the last three hours, the trend tab displays three hours of data. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can select an element on the chart to view more detailed data. You can select the data displayed as horizontal bars below the timeline slider to filter the table based on top locations (link count) and device types (link count).

Monitor and troubleshoot the health of a device

Use this procedure to view details about a specific device and determine if there are potential issues that must be addressed.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Network** tab.

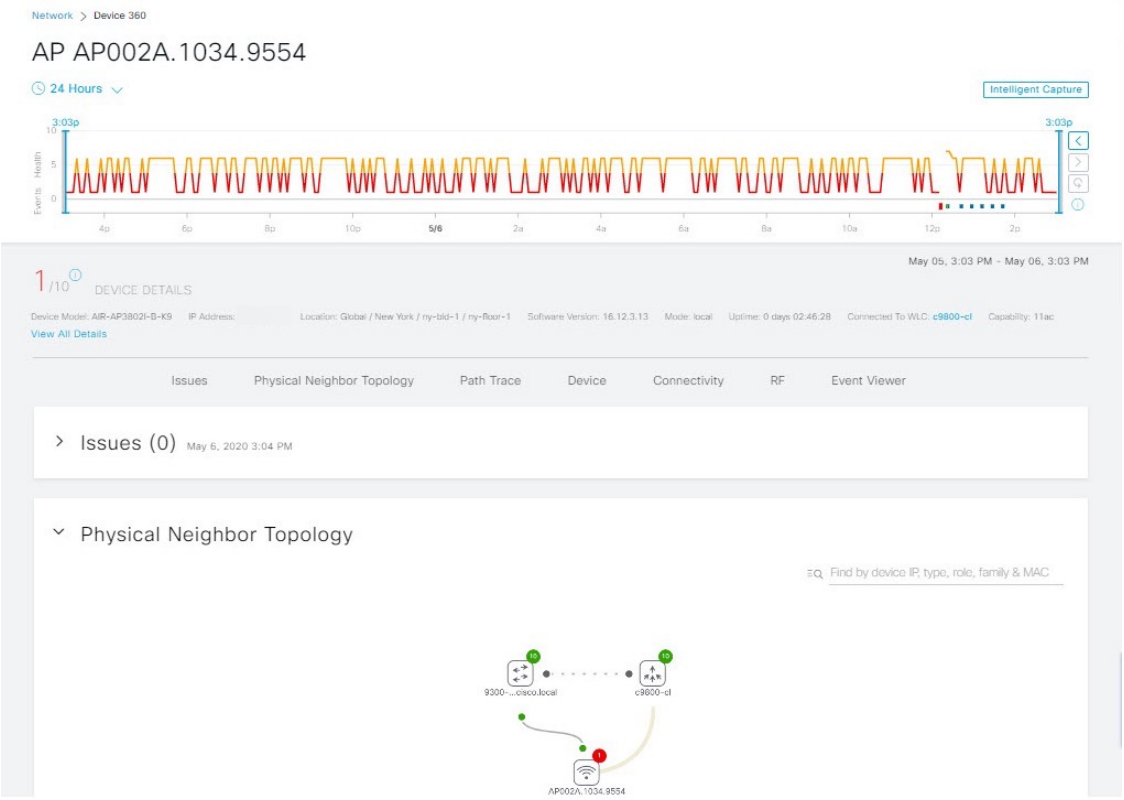
Step 3 In the **Network** health dashboard, do one of these tasks:

- In the **Network Devices** dashlet, click a device name in the **Device Name** column.
- In the **Search** field, enter the device name, IP address, or MAC address.

The **Device 360** window displays a 360° view of the network device.

Note
The **Map View** appears by default.

Figure 10: Device 360 window



Note
You can click the **View Device Details** hyperlink next to the device name to cross-launch the device inventory window.

Step 4 Click the time range setting (24 Hours) to specify the time range of data that is displayed on the window:

a) From the drop-down menu, select a time range: **3 hours**, **24 hours**, or **7 days**.
b) Specify the Start date and time and the End date and time.
c) Click **Apply**.

Step 5 Click **Intelligent Capture** to view, monitor, and troubleshoot captured onboarding and data packets for a specific network device and to determine if there are potential issues that must be addressed. See View RF Statistics of an AP, on page 406.

Note
Intelligent Capture is not supported for all the AP models. If **Intelligent Capture** is not displayed, verify that the AP is a supported model, and that the AP is assigned to a location on the **Network Health** dashboard.

Step 6 Use the timeline slider to view the health and events information about the network device over a period of time.

Note
Gaps in the timeline indicate that no health data was retrieved from the device. This situation can occur when a device is in maintenance mode.

Under Maintenance banner is displayed for the access points that are under maintenance mode when you hover your cursor during a specific time period.

The timeline slider displays this information:

- **Health**: You can hover your cursor over the timeline slider to view the device health score and KPIs for a 5-minute window. The device's health score is the minimum of all KPI health scores.

  When you double-click the graph, it displays the timeline slider for 1 hour.

  Note
  To display information for longer than 1 hour, manually move the timeline slider to the desired time range.

  When you double-click the timeline, it displays the timeline slider for a 1-hour time period. The entire window is refreshed, providing updates for that hour. Note that the timestamps next to each category (**Issues**, **Connectivity**, and so on) are also refreshed.

- Check the **Telemetry Status** check box below the timeline to view the horizontal bar in the timeline. To view the telemetry status:
  - Hover your cursor over the horizontal bar to view the network device telemetry status such as Good, Fair, or Poor in the tool tip.
  - If telemetry shows in red color, it indicates full data loss.
  - If telemetry shows in yellow color, it indicates partial data loss.
  - Click the **Telemetry Status** in the tool tip to open a slide-in pane to view the summary of the telemetry status.

Step 7 You can view the device's health score in the **Device Details** area, below the timeline.

Note
Devices in maintenance mode are not included in the calculation of a device's health score.

The details for the device's health score are as follows:

- **Switch**: The health score for switches is the minimum subscore of these parameters — memory utilization, CPU utilization, link errors, link discards, uplink availability, and reachability to the control plane. In addition, for fabric devices, fabric health is also included. For more information, see Switch Health score, on page 114.

  Note
  Switches: Uplink availability is based on infrastructure links.

  Cisco StackWise Virtual: Uplink availability is based on infrastructure links, Cisco StackWise Virtual links (SVL), and Dual Active Detection (DAD) links. See About Cisco StackWise Virtual and its limitations, on page 108.

  Cisco StackWise: Uplink availability is based on infrastructure links and Cisco StackWise links. See About Cisco StackWise and its limitations, on page 109.

- **Router**: The health score for routers is the minimum subscore of these parameters — memory utilization, CPU utilization, link errors, link discards, uplink availability, and reachability to the control plane. For more information, see Router Health score, on page 115.

  Note
  Uplink availability is based on infrastructure links.

- **AP**: The health score for APs is the minimum subscore of these parameters — memory utilization, CPU utilization, link errors, radio utilization, interference, noise, and air quality. For more information, see AP Health score, on page 116.

- **Wireless Controller**: The health score for wireless controllers is the minimum subscore of these parameters — memory utilization, free timers, free memory buffers (MBufs), work queue element (WQE) pools, packet pools, and link errors. For fabric wireless controllers, it includes fabric health. For more information, see Wireless Controller Health score, on page 118.

The color of the health score represents its severity. The health is measured on a scale of 1 to 10, where 10 is the best score. A score of 0 indicates that data could not be obtained, or that the device is in maintenance mode.

- : Critical issues. Health score range is 1 to 3.
- : Warnings. Health score range is 4 to 7.
- : No errors or warning. Health score range is 8 to 10.
- : No data available (includes devices in maintenance mode). Health score is 0.

Step 8 Use the **Device Details** area, below the timeline, to view the most current information about the device, such as the building and floor where the device is located, the device model, IP address, software version installed on the device, device role, HA status, the IP address or MAC address, and the uptime.

Note
For **Fabric Site**, elements are displayed in the device details area—**Fabric Role**, **Fabric Domain**, **System Resources**, **Data Plane**, **Virtual Network**, Transits and **Events**.

For **Cisco StackWise Virtual**, two additional elements are displayed—**Stack Status: StackWise Virtual** and **StackWise Virtual Domain**.

For **Cisco StackWise**, an additional **StackWise** element is displayed, along with the number of switches in the stack, such as **StackWise (2)**. A stack can contain a maximum of eight switches.

For **Mesh APs**, these details are displayed in the device details area—**Mode**, **Mesh Role** and **RAP**.

For PoE-capable devices, these elements are also displayed in the device details area—**IEEE Class**, **Negotiated Power Level**, and **PoE Status**.

Step 9 Click **View All Details** in the **Device Details** area to open a slide-in pane that displays additional attributes of a device, such as general information, network information, and rack location. Depending on the device type, additional device-specific details may be included.

Step 10 Use the **Issues** category to view issues that must be addressed.

Note
When a device is in maintenance mode, it does not trigger any issues.

Issues are listed based on the timestamp. The most recent issue is listed first. Next to the issue name is a Note icon ( ). If you're an admin user, you can add, edit, and delete notes. Click the Note icon ( ) and then click **Add**. If you're any other type of user, you can only view note information.

Click an issue to open a slide-in pane to view the corresponding details, such as the description of the issue, impact, and suggested actions.

From the slide-in pane, you can do these tasks:

- To resolve an issue:
  a. From the drop-down list, select **Resolve**.
  b. Click **Resolved Issues** to view the issues that are resolved.
- To ignore an issue:

a. From the drop-down list, select **Ignore**.

b. On the slider, set the number of hours to ignore the issue.

c. Click **Confirm**.

d. Click **Ignored Issues** to view the issues that have been ignored.

Step 11 Use the **Physical Neighbor Topology** category to view the topology of the device and how that device is connected to neighboring devices.

You can do these tasks:

- Click a node to display a slide-in pane that displays information about the node.
- Click a link between two devices to see the details about that specific link, such as the port/interface corresponding to the link, admin status, port mode, and so on.
- Hover your cursor over the link ends (dots) to see the status of the link.
- Hover your cursor over a group of devices and click **View Devices List** to view the list of devices and their details.
- In the Search field in the **Onboarding** area, you can search for a specific device. The specific node is selected, and the corresponding information about the device is displayed.

Note

- For AP 360, the 2-GHz and 5-GHz clients are displayed, and the dotted link lines going from these two clients are not clickable. Also, the link line between AP to wireless controller and wireless controller to AP is not clickable.
- For an SD-Access Fabric, the fabric groups are displayed with a fabric badge icon.
- The Cisco StackWise Virtual and Cisco StackWise are displayed with a stack icon ().
- Path Trace displays a switch icon if a Cisco StackWise Virtual or a Cisco StackWise is involved in that path.

Step 12 Use the **Event Viewer** category to view an audit trail of events for the device. The Event Viewer table provides information about the issue such as the reason code and the time stamp when the event occurred. Click an event to view details about that event in the right pane.

- **APs**: Lists scenarios and the sequence of subevents that led to each scenario. This allows you to pinpoint during which sub event an issue occurred. Radio resource management (RRM) events, such as Transmit Power Change, RF Channel Change, and Radio Reset, are displayed.
- **Switches and Routers**: Displays all syslogs that have a severity of Critical and above (Emergency and Alert), events for any links that are up or down, and events for devices that are reachable or unreachable. Syslogs that are less severe than Critical level (Error, Warning, Notice, and Info) are also displayed.
- **Wireless Controllers**: Lists wireless controller events. For Cisco AireOS devices, selected traps and syslogs are displayed. For Cisco IOS controllers, selected syslogs and events are displayed.

Step 13 Use the **Path Trace** category to run a path trace.

Click **Run New Path Trace** to display a network topology between a specified source device and a destination device. The topology includes the path's direction and the devices along the path, including their IP addresses. The display also shows the protocol of the devices along the path (**Switched**, **STP**, **ECMP**, **Routed**, **Trace Route**) or other source type.

See Do a path trace, on page 428.

Step 14 Click the **Application Experience** category to view the running applications in your network.

To view the metrics in a chart format, click the radio button next to an application. A slide-in pane opens with the relevant information.

See About Application Experience and Application Visibility, on page 157 and View Application Experience of a host, on page 164.

Note
This category is displayed only for routers.

Step 15 Use the **Detail Information** category to view the device's historical KPIs performing over a period of time.

Click these tabs to view the respective details:

Device info tab
Availability section displays information about the device CPU, memory, uptime, temperature, and so on. **HA Redundancy** section displays information about the Redundancy Mode, Redundancy Unit, Local State, and Peer State for the Cisco Embedded Wireless Controllers. For WLC 360, **STANDARD POWER SERVICE** section displays information about device Connection Status, Last Successful Connection and so on. **Note** For third party devices, only the Uptime chart appears. • If there are multiple sensors for a wireless controller, the data reflects the latest maximum temperature of all sensors. • For network devices that are configured out of band, the uptime chart does not correlate correctly with the heath score and other data. For example, the uptime chart for a 24-hour window shows that the device was down at 11:39 am and at 2:40 pm. Then, if you select a 3-hour window, 11:00 am – 2:00 pm (in the timeline slider), the downtime is not displayed. This issue occurs because Catalyst Center is not able to receive the sys uptime information from the device. To work around this issue, synchronize the configuration between the device and Catalyst Center.

Connectivity tab

Displays information about the health of a device's connection with the network. This tab is available for APs.

The Connectivity tab contains radio-specific KPIs, such as Radio 0, Radio 1, and Radio 2. Click the appropriate radio to view information such as Current Channel, Extended Channel(s), RF Profile, Band, Mode, and Current Channel Width. You can also view charts for Traffic, Client Count, and so on.

- **Traffic**: The traffic (in Mbps) for radios is displayed. The Rx (receiver) data packets and Tx (transmitter) data packets (in bytes) are shown as color-coded lines on the chart.

  Hover your cursor over a time instance on the graph to view the amount of traffic (Rx or Tx) sent or received for a particular day and time.

- **Client Count**: The number of clients for radios is displayed. The client count is shown as color-coded lines on the chart.

  Hover your cursor over a time instance on the graph to view the number of clients connected to an AP for a particular day and time.

- **Link Error**: To display information about interfaces, check the check boxes next to the interfaces on the right of the chart. Based on the interfaces you select, the error percentage for each interface is displayed as color-coded lines on the chart.

  Hover your cursor over a time instance on the graph to view the error percentage for a particular day and time. You can select a maximum of five interfaces.

- **Ethernet Interface KPI**: The Ethernet interface KPIs contain interfaces such as GigabitEthernet0 and GigabitEthernet1. Click the appropriate interface to display the charts for Utilization, Error, and Rate. You can also view the total and average values for the KPIs aggregated for a time range selected on the top of AP 360.

  Note
  A Connected Switch banner is displayed for interfaces connected with switches.

- **Top Clients with Tx Drops per SSID**: Displays the top 5 clients with packet drop count per selected SSID. This chart is available only for clients connected to Cisco 9800 wireless controllers starting from 17.12 version.

- **Retries**: The connection retries for radios are displayed in the retries chart.

  Note
  Only infrastructure links are considered for link errors. Infrastructure links are topological links connecting Catalyst Center-managed network devices, such as switches, routers, wireless controllers, and APs.

Fabric Site Tab

This tab is available for SD-Access fabric.

Fabric KPIs are grouped under different categories: **Fabric Site Connectivity**, **Fabric Infrastructure**, and **Fabric Control Plane**. You can filter the categories to view the respective KPIs. Based on the KPI selection, you can view the table displayed with reachability information, such as the destination, IP address, and type. Check the check box next to destination to view the control plane reachability status, LISP, and Pub/Sub session status charts.

Note
The uplink status chart shows data only if the Fabric Underlay Automation is used to provision the fabric.

Interfaces tab
Contains information about the selected interface, such as the name, description, operational status, and link speed. Use the PORT TYPE tabs to display information about a specific port type. The tabs that are displayed depend on the type of device selected: • **Switches and Routers**: Displays **All**, **Access**, **Auto**, **Routed**, and **Trunk** port types. • **Cisco StackWise Virtual**: Displays **All**, **Access**, **Auto**, **Routed**, **TrunkSVL**, and **DAD** port types. • **Cisco StackWise**: Displays **All**, **Access**, **Auto**, **Routed**, **Trunk**, and **StackWisePort** port types. • **Wireless Controller**: Displays **All**, **Ethernet**, and **Virtual** port types. The table contains sortable columns. However, if you try to sort a column with a new parameter, the expanded interface list collapses. **Note** For the **Link Speed** data column, the speed capacity of the interface or physical port is displayed. If the port has negotiated to a certain speed, that negotiated speed is displayed. To display the operational status of the interfaces for a particular day and time in a chart format, check the check boxes next to the interfaces. You can select a maximum of five interfaces. The first interface in the table is selected by default. The **Interface Availability**, **Utilization**, **Error**, and **Link Discard** charts are displayed below the table. The **Tx Utilization** and **Rx Utilization** chart values are populated in **Percentage** and **Rate (bps)**. You can toggle between the Percentage and Rate to view the utilization values. **Note** For wireless controllers, link discard information is not provided in a separate chart. It is provided, along with other data, in a **Traffic Summary** table. Data in the **Traffic Summary** table is shown only for the physical and Ethernet interfaces of a wireless controller. If you select an interface that supports digital optical monitoring (DOM), the **Digital Optical Monitoring** area displays the following metrics: • **Transmit Power**: Insufficient power can lead to signal degradation and increased bit error rates. Excessive power can cause receiver saturation and non-linear effects in the fiber. • **Receive Power**: Low RxPower can indicate issues such as fiber attenuation, dirty connectors, or misalignment, which can degrade network performance. • **Temperature Monitoring**: Monitoring temperature data helps network administrators take corrective actions to prevent overheating, which can cause permanent damage to optical components and lead to network failure. It can also identify cooling system failures in data center environments. • **Current Monitoring**: Excessive current can indicate potential problems like component failure or short circuits. Consistently high current levels can lead to overheating and the premature failure of a device. • **Voltage Monitoring**: Voltage that is too low might lead to insufficient power for the device, resulting in poor performance or a failure to operate. Conversely, excessive voltage can cause damage to a transceiver's electronic components.

PoE tab
This tab is available for PoE-capable switches and APs. Displays the device's Power over Ethernet (PoE) telemetry. **Switches** The **POWER SUMMARY** section displays the switch's overall PoE telemetry: • **Power Budget**: The overall power that the switch allocates for use with PoE-capable devices. • **Used Power**: The power being supplied by the switch to PoE-capable devices. • **Remaining Power:** The unused power available for use by PoE-capable devices. • **Power Usage**: The percentage of power being supplied by the switch to PoE-capable devices. This value is equal to the value of the **Used Power** divided by the value of the **Power Budget**. The **Power Stack** section lists the power stack devices connected to PoE, such as Power Stack Name, Stack Mode, Stack Topology, Allocated Power, Consumed Power, Remaining Power, and so on. The **Module Power Details** section lists the components in the switch that supply power for PoE. The **PoE Interfaces** section lists the PoE-capable devices connected to the switch's interfaces. At the top of the section is a count of interfaces that are currently off. You can customize the table by doing these tasks: • Use the **POE CONFIG**, **ADMIN STATUS**, and **POE OPER STATUS (SIGNAL PAIR)** filters above the table to filter the interfaces. • Use the search bar to perform searches for specific interfaces, PoE-capable devices, or any other values. • Click ⋮ to open a menu where you can add and remove columns for specific data types. **APs** The **Detail Information** section displays the AP's PoE telemetry: IEEE PD Class, Power Level, PoE Admin Status, PoE Oper Status, PoE Policing Status, Switch Name, Interface Name, Allocated Power, Consumed Power, Max Power Drawn, PoE Priority, PoE Configuration, and Perpetual PoE. The **Power Distribution** section displays a trend chart of the power distribution (allocated and consumed power) for the selected time range.

StackWise Tab
This tab is available for Cisco StackWise. Displays information about the Cisco StackWise, such as the serial number, product ID, MAC address, role, state, priority, and the neighboring switch number.

StackWise Virtual Tab
This tab is available for Cisco StackWise Virtual. Displays information about the Cisco StackWise Virtual, such as the serial number, product ID, MAC address, role, state, priority, uptime, and port numbers.

RF Tab

This tab is available for APs and wireless clients.

- The RF tab contains radio-specific KPIs, such as Radio 0, Radio 1, and Radio 2. Click the appropriate radio tab to display charts for radio channel utilization, traffic utilization, interference, noise, air quality, air-time efficiency, wireless latency by client distribution, Tx power, Top Clients with Tx drops per SSID, channel information, and so on.
- **RF Tab Limitation**

  When an AP with three radios (for example, a Cisco Catalyst 9130 AP) connects to a wireless controller running 17.2 or later, the device supports all three radios, and three radios (Radio 0, Radio 1, and Radio 2) are displayed under the RF tab.

  When that same AP connects to a wireless controller running version 17.1 older, the device supports two radios, and two radios (Radio 0 and Radio 1) are displayed under the RF tab.

  However, if an AP moves from a wireless controller running a newer version to one running an older version (17.2+ > 17.1), the RF tab continues to display the three radios (Radio 0, Radio 1, and Radio 2) that were initially detected.
- For AP 5-GHz radios, a DFS tab provides information about Dynamic Frequency Selection (DFS) radar events.
- For **AP 360**, under **RF** tab:

  Radio 2 (6GHz band), **STANDARD POWER MODE** section provides information about **Automated Frequency Coordination (AFC)** integration that includes AFC status, Last Response Time, Expiration, and AFC defined location details such as location type, lat/long, and so on.

  Neighbors and Rogues section contains **Band** (2-GHz and 5-GHz radio frequencies), **Type** (All, Neighbor, Rogue), and **RSSI Range** (0 to -100 dBm) filters. Depending on the filter selection, the AP table is refreshed.

  AP table includes the details, such as the Identifier, Radio, RSSI (dBm), Channel, Type, and SSID of the AP. Use the search bar to find AP devices, radios, or any other values.

  Note
  Catalyst Center stores only 10 neighbors with the highest RSSI for each 5-minute interval.

  Click  to open a menu where you can use **Edit Table Column** to enable or disable specific columns. Click **Export** to export the table data to a CSV file.
- Click the **KPI** drop-down list and check the check boxes next to the charts that you want to display. The charts provide various information, such as Throughput, Client Count, Channel Utilization, Top SSIDs by Client/Packet Count, and so on. Selected charts are displayed in the **RF** tab.
- Depending on the filter selection, the Wi-Fi analyzer graph is displayed below the table. The Wi-Fi graph summarizes the total and average values for the KPIs aggregated for a time range selected on the top of the AP 360 timeline slider.

  Check the check boxes next to the APs to view the Wi-Fi analyzer graph for the specific AP. Hover your cursor over the chart to view details.

  Click the **Chart Setting** icon to enable or disable the **Access Point Label**, which is shown in the graph for each AP.

Virtual Network Tab
This tab is available for SD-Access fabric. The KPIs are grouped under the **VN Services** and **Fabric Control plane** categories. You can select the category to view the **Dynamic Default Border**, **Remote Internet Availability**, **Multicast (external RP)**, and **Pub-Sub Session Status** KPIs. You can filter the categories to display the table with reachability information, such as the destination, IP address, and type. Check the check box next to destination to view the status, such as control plane reachability status, LISP, and Pub/Sub session status charts.

Transits and Peers Network Tab
This tab is available for SD-Access fabric. The **Transits and Peers Network** tab contains these **Transit Site Control Plane** KPIs: **BGP Session from Border to Transit Control Plane**, **LISP Session from Border to Transit Site Control Plane**, and **Pub-Sub Session from Border to Transit Site Control Plane**. Check the appropriate KPI check box to display the charts and table with reachability information, such as the destination, IP address, and type.

Mesh Tab
This tab is available for Mesh APs. The **Mesh** tab shows a device's mesh role, mesh profile, downstream MAPs, mesh backhaul channel, hops to RAP, bridge group name, and backhaul interface. It also provides these radio-specific KPIs: **Current Channel**, **Extended Channel(s)**, **Mode**, **RF Profile**, **Band**, **Tx Power**, **Clean Air Status**, **Admin State**, and **Current Channel Width**.

Advanced Analytics Tab

This tab is available for Cisco Catalyst 9800 Series Wireless Controllers and Wireless-enabled Catalyst Switches (eCA).

The **Advanced Analytics** tab displays detailed process-level telemetry KPIs, including:

- Per-Process CPU Utilization (%): Displays the percentage of CPU resources consumed by each process running on the wireless controller over the selected time range. This KPI helps identify processes consuming excessive CPU cycles that may impact device performance and client experience.
- Per Process Memory Utilization (%): Displays the percentage of memory resources consumed by each process running on the wireless controller over the selected time range. This KPI helps identify processes with abnormal memory consumption that could lead to memory exhaustion and device instability.
- Client Delete Count: Displays the number of client deletion events per WNCD process instance over the selected time range. A client deletion occurs when a client session is removed from the controller due to disassociation, deauthentication, session timeout, or administrative action. This KPI helps identify abnormal client churn patterns.
- KPIs: Click the **KPIs** drop-down to view and select from the available Advanced Analytics KPIs. Check the check boxes next to the KPIs you want to display, and click **Apply**. You can select multiple KPIs simultaneously. The available KPIs are: AP Count,Client Count, Client Count Per Band, Client State Stats, Client Association Stats, Client Mobility Stats, Client Roam Stats, Traffic, Traffic Errors, Data Plane – Punt, Data Plane – Software Drops, Data Plane – Hardware Drops, mDNS Stats, AAA Stats – Authentication, AAA Stats – Authorization, AAA Stats – Accounting, AAA Stats – Radius
- Client Count: Displays the total number of wireless clients currently associated with each WNCD process instance on the wireless controller over the selected time range. This KPI provides visibility into client load distribution across wncd processes and helps identify load imbalances.

When you use the time slider to display KPI data for the last 3 hours, 24 hours, or 7 days, note that:

- The 7-day time slider uses a 60-minute window. It reports data based on the start time of that 60-minute window and returns the latest data within that 60-minute interval.
- The 3-hour and 24-hour time sliders use a 10-minute window. They report data based on the start time of that 10-minute window and return the latest data within that 10-minute interval.

Step 16 To compare the health of AP radios across the floor in a building, click the toggle button in the top-right corner to switch between **Detail View** and **Map and Comparison View**.

Map and Comparison View displays a floor map with the AP radios placed on it.

Step 17 From the **View Site** drop-down list, select the floor on which you want to compare the AP radios.

Hover your cursor over the AP icon on the floor map to view the device details of an AP radio, such as **MAC Address**, **Model**, **Mode**, and **Issue Count**.

Step 18 Click **Compare AP Radios** to compare the AP radios on the floor map.

The **Map View** appears by default, showing the last 5 minutes of AP radio data.

Step 19 Click the AP icon on the floor map.

A dialog box appears to select or deselect the radios for comparison.

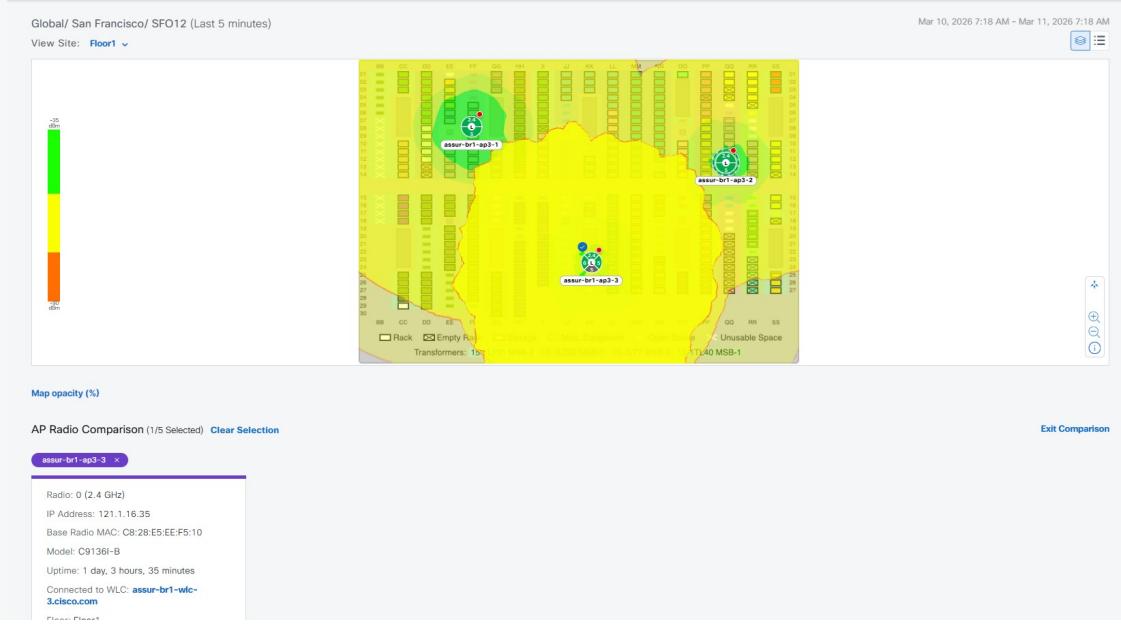
Step 20 Check the check boxes next to the list of radios that you want to compare on a floor.

Note

- By default, Catalyst Center selects the current AP for comparison only if the first radio of the respective AP is in monitor mode.
- **Local**, **Remote**, and **Hybrid** modes are the only AP radio modes enabled for comparison.
- You can select up to five AP radios at a time for comparison.

Step 21 Use **AP Radio Comparison** to view the list of AP radios selected for comparison.

Figure 11: AP Radio Comparison Map View



You can compare **Radio**, **IP Address**, **Model**, **Uptime**, **Connected to WLC**, and **Floor**.

Step 22 Use **Comparative Metrics** to view the comparative metrics for the selected KPIs.

Step 23 From the **Select KPI** drop-down list, select the KPIs for which you want to see the comparative matrices.

You can select from these KPIs:

- Channel Information
- Throughput (Rx Rate)
- Radio Retries
- Interference
- Air Quality
- Management Frames
- Tx Errors
- Tx Power
- Traffic Utilization

- Tx Traffic Utilization
- Throughput (Tx Rate)
- Connected Client Count
- Channel Utilization
- Noise
- Wireless Latency
- Data Frames
- Rx Errors
- Multicast Counter
- Rx Traffic Utilization

Step 24 Click the toggle button to switch between **Map View** and **Table View**.

The **Access Point Radios** table view lists the AP radios.

Step 25 Check the check box next to the AP radios that you want to compare on a floor map.

Step 26 To remove all radios from the comparison in the **AP Radio Comparison** area, click **Clear Selection**.

Step 27 Click **Exit Comparison** to exit.

About Cisco StackWise Virtual and its limitations

Cisco StackWise Virtual is a network system visualization technology that allows two physical switches to operate as a single logical virtual switch using a 40-G or 10-G Ethernet connection.

Supported devices for StackWise Virtual

This table lists the Cisco Catalyst switches that support StackWise Virtual:

Device	Minimum Supported IOS-XE Software Version
Cisco Catalyst 9300 Series Switches	16.11+
Cisco Catalyst 9400 Series Switches	16.11+
Cisco Catalyst 9500 Series Switches	16.11+

StackWise Virtual Limitations

Cisco StackWise Virtual has these known limitations:

- After you have configured Cisco StackWise Virtual, the second switch still appears in the inventory, and stops responding because it does not have its own IP address. As a workaround, do these steps:
  1. Delete both the switches from the inventory. See Delete a network device, on page 62.
  2. Configure StackWise Virtual. (Configure the two switches into one virtual switch.)

3. Discover the devices. See Discover your network using an IP address range or CIDR, on page 24, Discover your network using CDP, on page 21, or Discover your network using LLDP, on page 26.



Note After StackWise Virtual is discovered, one switch plays the active role, while the other a standby role. Both switches in the stack get associated with one primary management IP address.

- After you remove Cisco StackWise Virtual, the two switches are independent. They both have the same IP address and operate in Dual Active Detection (DAD) state. As a workaround, do these steps:

  1. Configure a different IP address on the second switch.
  2. Rediscover the devices. See Discover your network using an IP address range or CIDR, on page 24, Discover your network using CDP, on page 21, or Discover your network using LLDP, on page 26.

About Cisco StackWise and its limitations

The Cisco StackWise technology provides an innovative new method for collectively utilizing the capabilities of a stack of switches. Individual switches intelligently join to create a single switching unit with a 32-Gbps switching backplane. Configuration and routing information is shared by every switch in the stack, creating a single switching unit.

Supported devices for Cisco StackWise

These devices support Cisco StackWise:

- Cisco Catalyst 3650 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 9300 Series Switches

Cisco StackWise limitations

Cisco StackWise has these known limitations:

- Ring status is not displayed in the **Device 360** header.
- Link Speed information is not provided in the. **Detail Information** > **Interfaces** tab.

Configure health score settings for network devices

Use this procedure to configure the health score settings for network devices. You can customize the health score calculation for network devices by changing the KPI thresholds and specifying the KPIs that are included for the calculation. Health score settings is not applicable to third party devices.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health** > **Health Score Settings**.

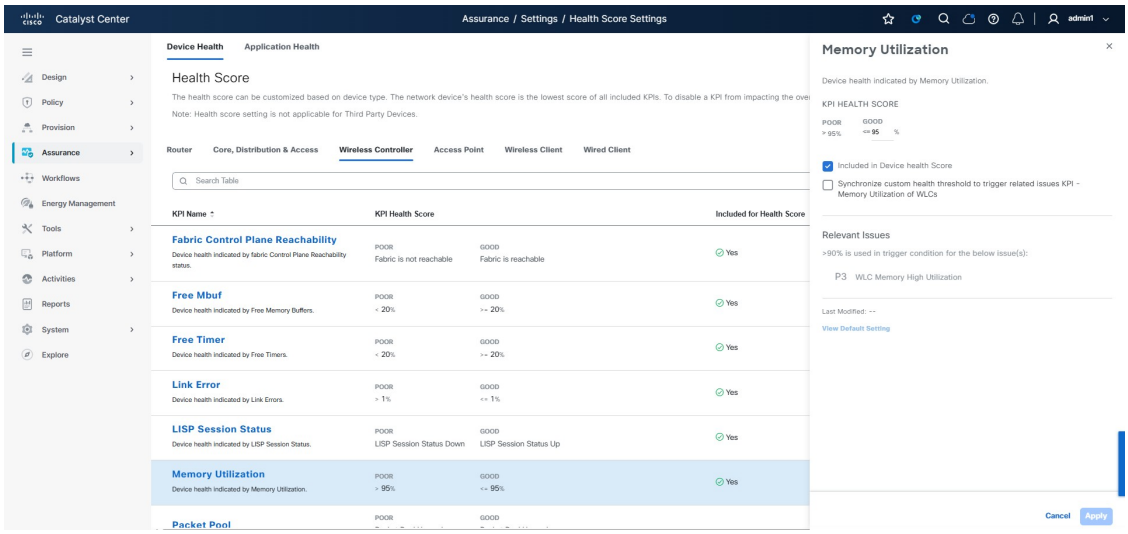
The **Health Score** window appears.

Step 2 Click the **Device Health** category to customize its health score calculation settings.

The screen displays the Key Performance Indicators (KPIs) table that includes KPI Name, KPI Health Score, Included for Health Score, Current Setting, and Last Modified.

Step 3 From the **KPI Name** column, click the KPI name link.

The slide-in pane for the KPI appears.



Step 4 Configure the KPI health score settings:

a) If the KPI threshold is quantitative, you can customize the threshold value for what is considered a good health score.

b) To sync or unsync the common KPI threshold between the health and issues settings, use the Synced toggle button. The sync works vice versa when it is synced from health or issue settings page and it is applicable only for wireless controllers.

c) To remove the KPI from the health score calculation, uncheck the **Included in Device health Score** check box.

Note: The synchronization of the common KPI threshold between the health and issues settings using the Synced toggle button applies only to the Wireless controllers device category.

> **Note**
> A network device's health score is the lowest score from all its included KPI scores.
>
> **Restriction**
> At least one KPI must be included for the health score calculation.
>
> **Attention**
> When viewing the KPI health scores for a network device, excluded KPIs display a `NA` instead of a health score.

d) To restore the default settings, hover your cursor over **View Default Setting** and click **Use Default**.

Step 5 Click **Apply**.

A confirmation dialog box appears.

Enable SNMP Collector metrics for fabric devices

For the health score to populate correctly for fabric devices, you must enable the SNMP Collector metrics.

Procedure

Step 1 From the main menu, choose **System** > **Data Platform**.

Step 2 Click **Collectors**.

A list of collectors appears.

Step 3 Click **COLLECTOR-SNMP**.

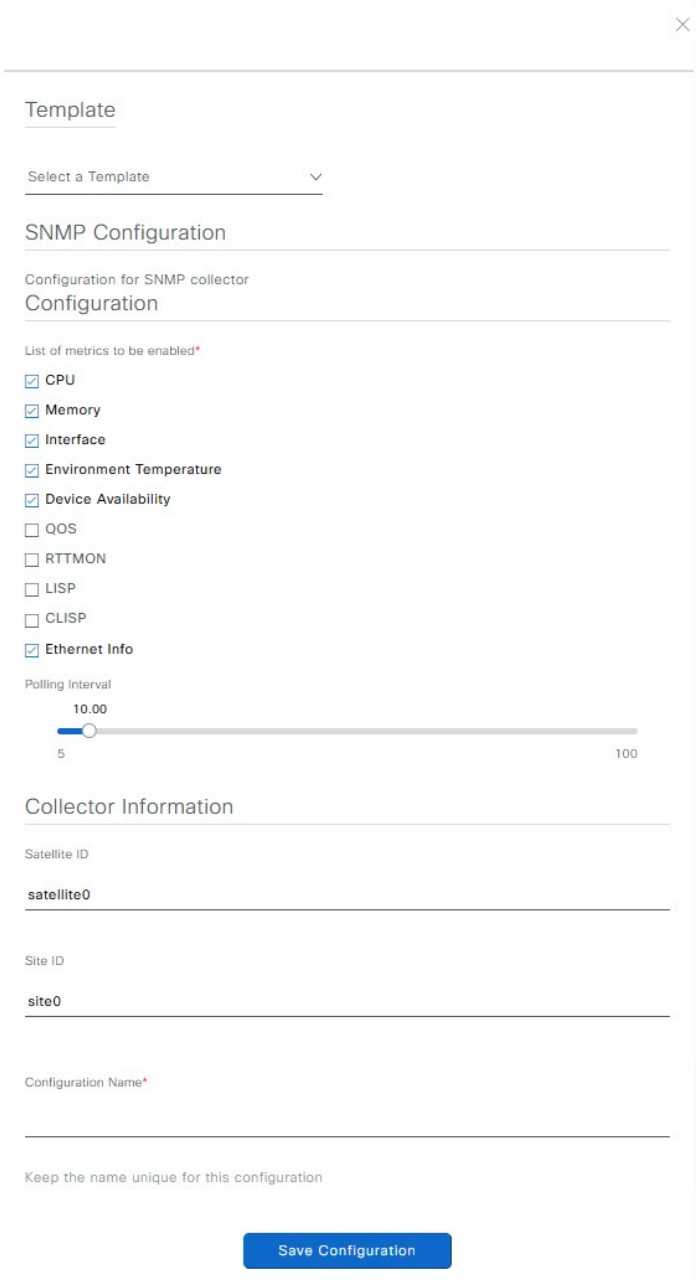
The **COLLECTOR-SNMP** window opens.

Step 4 Click **+ Add**.

The **SNMP Configuration** dialog box opens.

Step 5 Choose a template from **Select a Template** drop-down list.

Figure 12: SNMP Configuration



Step 6 In the **Configuration Name** field, enter a unique name for the SNMP configuration.

Step 7 Click **Save Configuration**.

Understand network health score and KPI metrics

This section provides information about how the network health scores and KPI metrics are computed.

Network Health score

The Network Health score is a percentage of the number of healthy network devices (a health score from 8 to 10) divided by the total number of network devices (excluding devices in maintenance mode). The score is calculated every 5 minutes.

For example:

90% (health score) = 90 (network devices with health score from 8 to 10) ÷ 100 (total number of network devices - devices in maintenance mode)

Device Category Health score

The Device Category Health score (Access, Core, Distribution, Router, Wireless) is the percentage of the number of healthy network devices (a health score from 8 to 10) in a target category, divided by the total number of network devices in that category (excluding devices in maintenance mode). The score is calculated every 5 minutes.

For example:

90% (health score) = 90 (network devices in a target category with health score from 8 to 10) ÷ 100 (network devices in that category - devices in maintenance mode)

Individual Device Health score

The Individual Device Health score is the minimum score of these KPI metric health scores: System Health, Data Plane Connectivity, and Control Plane Connectivity. The KPI metric score is based on the threshold that is defined per KPI.

Device Health Score = MIN (System Health, Data Plane Connectivity, Control Plane Connectivity)

Depending on the type of device, the metrics vary.

System health	
Device type	**Description**
Switch (Access and Distribution)	Includes system-monitoring metrics, such as CPU utilization and memory utilization.
Wireless	Includes these system-monitoring metrics: • For wireless controllers, it includes memory utilization, free timers, and free Mbufs. • For APs, it includes CPU utilization and memory utilization.
Router	Includes system-monitoring metrics, such as CPU utilization and memory utilization.
Fabric	Includes system-monitoring metrics, such as CPU utilization and memory utilization.

Data plane connectivity	
Device type	**Description**
Switch (Access and Distribution)	Includes metrics, such as link errors and link status. For switches, the Inter-device Link Availability metric counts physical stack ports, network device-connected links, and fabric edge-facing port channels.
Wireless	Includes these metrics: • For wireless controllers, it includes metrics like WQE pool, packet pools, and link errors. • For AP, it includes RF metrics like interface, noise, air quality, and radio utilization.
Router	Includes metrics, such as link errors.

Control plane connectivity	
Device type	**Description**
Wireless	Includes these KPIs: • For wireless controllers, it includes connectivity to the Control Plane node servers. • For fabric devices, it includes metrics, such as connectivity to the Control Plane node.

Switch Health score

The Switch Health score is the minimum subscore of these parameters:

Note Devices in maintenance mode are not included in the calculation of a device's health score.

Parameter	Score calculation
CPU Utilization	• If CPU utilization is 95 percent or less, the score is 10. • If CPU utilization is more than 95 percent, the score is 1.
Memory Utilization	• If memory utilization is 95 percent or less, the score is 10. • If memory utilization is more than 95 percent, the score is 1.
Link Errors (Rx and Tx)	Only infrastructure links are considered for link errors. Infrastructure links are topological links connecting Catalyst Center-managed network devices, such as switches, routers, wireless controllers, and APs. If a physical infrastructure interface has errors, the score is 8. If all links are down, the score is 1. Otherwise, the score is 10.

Parameter	Score calculation
Link Discards	Only infrastructure links are considered for link discards. Infrastructure links are topological links connecting Catalyst Center-managed network devices, such as switches, routers, wireless controllers, and APs. If a physical infra link has packet drops (discards), the score is 8. If all links encounter discards, the score is 1. Otherwise, the score is 10.
Link Status	Only infrastructure links are considered for link status UP/DOWN. Infrastructure links are topological links connecting Catalyst Center-managed network devices, such as switches, routers, wireless controllers, and APs. If a physical infrastructure interface is down, the score is 8. If all interfaces are down, the score is 1. Otherwise, the score is 10.
Inter-device Link Availability	The **Inter-device Link Availability** KPI monitors the connectivity status between your network devices • GOOD: This status is triggered when all inter-device links are up . • POOR: This status is triggered when all inter-device links are down.
Reachability to Control Plane Node—Fabric Devices Only (Edge and Border)	• If the Control Plane node is reachable, the score is 10. • If the Control Plane node is unreachable, the score is 1. **Note** • If there is more than one Control Plane node in a fabric network, and all the Control Plane nodes are reachable, the score is 10; otherwise, the score is 1. • In the case of a collocated Edge or Border with Control Plane, Reachability to Control Plane is not considered. • For the health score to populate correctly for fabric devices, enable SNMP Collector metrics. See Enable SNMP Collector metrics for fabric devices, on page 111.

Router Health score

The Router Health score is the minimum subscore of these parameters:

Note Devices in maintenance mode are not included in the calculation of a device's health score.

Parameter	Score calculation
CPU Utilization	• If CPU utilization is 95 percent or less, the score is 10. • If CPU utilization is more than 95 percent, the score is 1.

Parameter	Score calculation
Memory Utilization	• If memory utilization is 95 percent or less, the score is 10. • If memory utilization is more than 95 percent, the score is 1.
WAN Connectivity	• If the WAN connectivity is down, the score is 1. • If the WAN connectivity is up, the score is 10.
Link Errors	Only infrastructure links are considered for link errors. Infrastructure links are topological links connecting Catalyst Center-managed network devices, such as switches, routers, wireless controllers, and APs. If a physical infrastructure interface has errors, the score is 8. If all links are down, the score is 1. Otherwise, the score is 10.
Link Discards	Only infrastructure links are considered for link discards. Infrastructure links are topological links connecting Catalyst Center-managed network devices, such as switches, routers, wireless controllers, and APs. If a physical infra link has packet drops (discards), the score is 8. If all links encounter discards, the score is 1. Otherwise, the score is 10.
Inter-device Link Availability	The **Inter-device Link Availability** KPI monitors the connectivity status between your network devices • GOOD: This status is triggered when all inter-device links are up . • POOR: This status is triggered when all inter-device links are down.
Reachability to Control Plane Node—Fabric Devices Only (Edge and Border)	• If the Control Plane node is reachable, the score is 10. • If the Control Plane node is unreachable, the score is 1. **Note** • If there is more than one Control Plane node in a fabric network, and all the Control Plane nodes are reachable, the score is 10; otherwise, the score is 1. • In the case of a collocated Edge or Border with Control Plane, Reachability to Control Plane is not considered. • For the health score to populate correctly for fabric devices, enable SNMP Collector metrics. See Enable SNMP Collector metrics for fabric devices, on page 111.

AP Health score

The AP Health score is the minimum subscore of these parameters:



Note Devices in maintenance mode are not included in the calculation of a device's health score.

Parameter	Score calculation
CPU Utilization	• If CPU utilization is 90 percent or less, the score is 10. • If CPU utilization is more than 90 percent, the score is 1.
Memory Utilization	• If memory utilization is less than 90 percent, the score is 10. • If available memory is 90 percent or more, the score is 1.
Radio Utilization Score	The score is calculated individually for each radio, and then averaged across all radios to obtain the overall utilization score. • If radio utilization is less than 70 percent, the score is 10. • If radio utilization is 70 percent or more, the score is 1.
Interference Score	The score is calculated individually for each radio, and then averaged across all radios to obtain the overall interference score. For 2.4-GHz radio: • If interference is less than or equal to 50 percent, the score is 10. • If interference is more than 50 percent, the score is 1. For 5-GHz radio or 6-GHz radio: • If interference is less than or equal to 20 percent, the score 10. • If interference is more than 20 percent, the score is 1.
RF Noise Score	The score is calculated individually for each radio, and then the averaged across all radios to obtain the overall noise score. For 2.4-GHz radio: • If RF noise is less than -81 dBm, the score is 10. • If RF noise is -81 dBm or more, the score is 1. For 5-GHz radio or 6-GHz radio: • If RF noise is less than -83 dBm, the score is 10. • If RF noise is -83 dBm or more, the score is 1.

Parameter	Score calculation
Air Quality Score	The score is calculated individually for each radio, and then averaged across all radios to obtain the overall air quality score. For 2.4-GHz radio: • If air quality is 60 percent or more, the score is 10. • If air quality is less than 60 percent, the score is 1. For 5-GHz radio or 6-GHz radio: • If air quality is 75 percent or more, the score is 10. • If air quality is less than 75 percent, the score is 1.
Link Error Score	The score is calculated individually for each Ethernet interface and then averaged across all Ethernet interfaces to obtain the overall link error score. • If link errors are less than 1 percent, the score is 10. • If link errors are 1 percent or more, the score is 1.

Wireless Controller Health score

The Wireless Controller Health score is the minimum subscore of these parameters:

Note Devices in maintenance mode are not included in the calculation of a device's health score.

Parameter	Score calculation
Memory Utilization	• If memory utilization is less than 90 percent, the score is 10. • If the available memory is 90 percent or more, the score is 1.
Free Timer Score	• If the number of free timers is 20 percent or more, the score is 10. • If the number of free timers is 20 percent or less, the score is 1.
Free Memory Buffers (MBufs)	• If the number of free memory buffer is 20 percent or more, the score is 10. • If the number of free memory buffer is less than 20 percent, the score is 1.
Work Queue Element (WQE) Pool Score	• If the wqe pool is greater than wqe pool threshold, the score is 10. • If the wqe pool is at the same level as or lower than the wqe pool threshold, the score is 1.

Parameter	Score calculation
Packet Pools	• If the packet pool is greater than the packet pool threshold, the score is 10. • If the packet pool is at the same level as or lower than the packet pool threshold, the score is 1.
Link Errors	• If link errors are less than 1 percent, the score is 10. • If link errors are 1 percent or more, the score is 1.
Connection to Control Plane Node—Fabric Wireless Controllers Only	• If the Control Plane node is reachable, the score is good. • If the Control Plane node is unreachable, the score is poor. **Note** If there is more than 1 Control Plane node in a fabric network, and all the Control Plane nodes are reachable, the score is 10; otherwise, the score is 1.

Effects of maintenance mode on network health scores and KPI metrics

When a network device (router, switch, wireless controller, or access point) is placed in maintenance mode, its clients are also placed in maintenance mode. For example, when you place a Cisco Wireless Controller in maintenance mode, any APs associated with the wireless controller are also placed in maintenance mode. Catalyst Center treats all devices in maintenance mode the same, regardless of whether a device was placed in maintenance mode as an administrative action or as a result of its association with a device.

Network health scores and KPI metrics do not include devices that are in maintenance mode, as metrics from such devices may be unreliable or unavailable during this period.

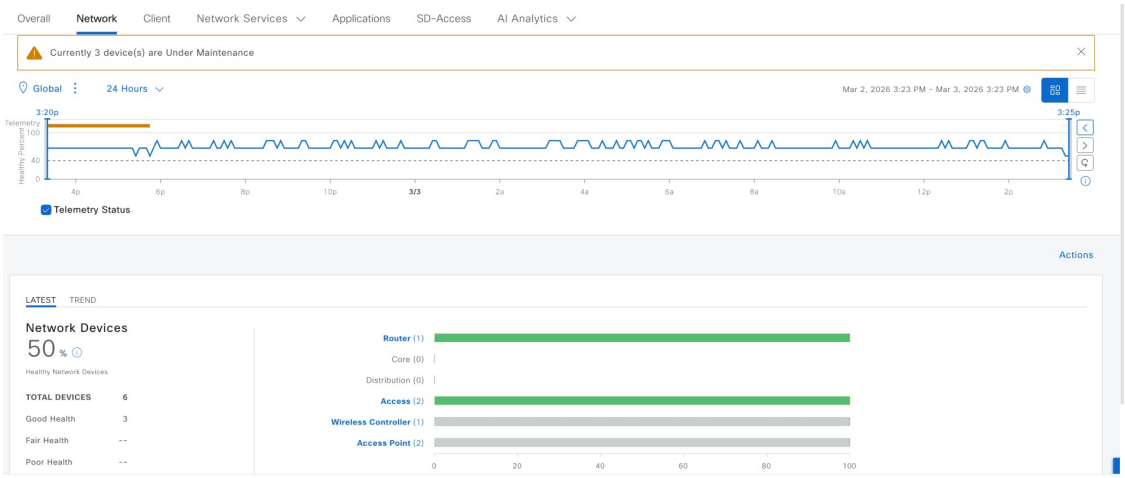
When a device is in maintenance mode, Catalyst Center does not:

- Collect health data
- Gather interface statistics
- Report issues for the device

Health and KPI calculations skip maintenance data. However, reports that show the total number of devices still include those in maintenance mode

When you access network health scores and KPI metrics while a device is in maintenance mode on the **Assurance** > **Health** > **Network** window, Catalyst Center displays a banner indicating that a device is in maintenance mode. In addition, start and end times of the maintenance window are indicated in the device 360 windows and logged as events in the system status log. The dashboards allow you to filter by devices that are in maintenance mode.

Figure 13: Device 360 with maintenance banner



Catalyst Center continues to do these tasks for a device that is in maintenance mode:

- Relevant events are still generated and can be displayed in the event viewer during maintenance mode.
- Maintenance-related operations, such as image upgraded, bulk provisioning, and so on still trigger events.
- The availability report in Assurance is not impacted.
- Topology is not impacted.

Understand RF calculations

Channel utilization, also known as *radio utilization*, is the total channel usage that Catalyst Center detects across Wi-Fi and non-Wi-Fi.

Catalyst Center derives the AP radio interference from this formula:

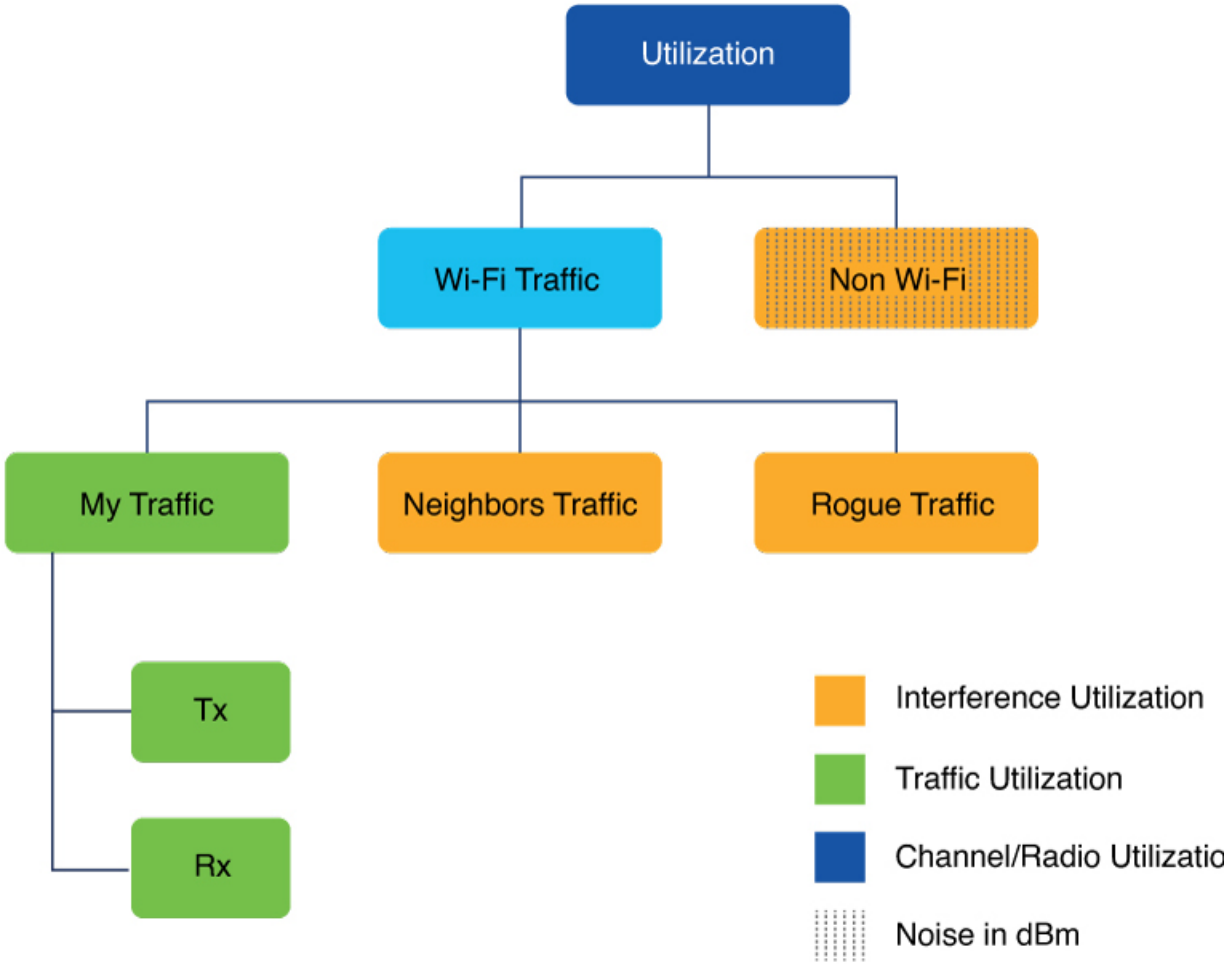
Interference % = Channel Utilization % – Rx Traffic % – Tx Traffic %

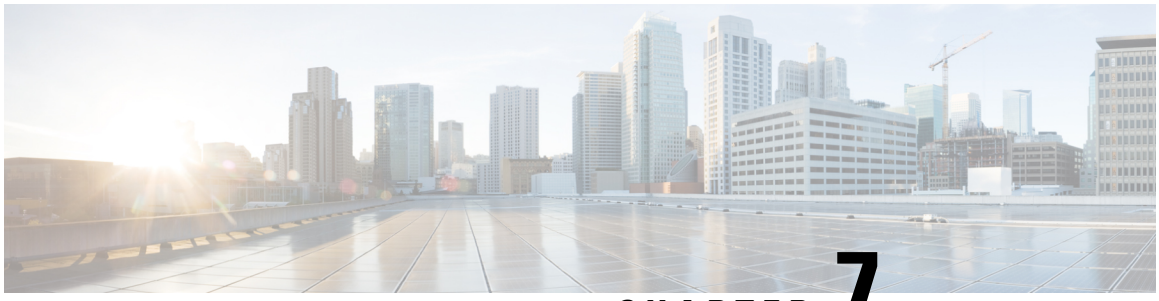
This definition of AP interference includes interference caused by rogue traffic, neighbor traffic, and non-Wi-Fi traffic.

Non-Wi-Fi interference, also known as *noise*, can be measured in % and dBm.

This diagram shows the relationship between the various parameters for the AP radio.

Figure 14: RF parameters in Catalyst Center





CHAPTER 7

Monitor and Troubleshoot Client Health

- Remote LAN support, on page 123
- Workgroup bridge client support, on page 123
- Monitor and troubleshoot the health of all client devices, on page 123
- Monitor and troubleshoot the health of a client device, on page 137
- Client tracking, on page 147
- Configure excluded clients, on page 152
- Understand Client Health score and KPI metrics, on page 153

Remote LAN support

Assurance doesn't support remote LAN (RLAN) or RLAN clients. On the Client 360 window, data might be missing or inaccurate for RLAN clients. On the AP 360 window, for APs with RLAN clients, the RLAN ports don't show RLAN-specific information. It is important to consider that RLAN clients on APs and wireless controllers continue to work normally, but there is no visibility for RLAN clients on Assurance windows. For more information, see "Remote LANs" in the *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*.

Workgroup bridge client support

Assurance doesn't support workgroup bridge (WGB) clients. On the Client 360 window, data might be missing or inaccurate for WGB clients. WGB itself is shown as a wireless client within Assurance and has a Client 360 window. It is important to note that WGB and WGB clients on APs and wireless controllers continue to work normally, but there is no visibility for WGB clients on Assurance windows. For more information, see "Workgroup Bridges" in the *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*.

Monitor and troubleshoot the health of all client devices

A client is an end device (computer, phone, and so on) that is connected to a network device (access point or switch). Catalyst Center supports both wired and wireless clients.

Assurance supports site-based, role-based access control (SRBAC), which limits a user's scope of access to certain network sites. You must ensure you have access to the sites, wired and wireless clients while using

the client health dashboard. For more information on user roles and permissions, see Cisco Catalyst Center Administrator Guide

Use this procedure to get a global view of the health of all wired and wireless clients and to determine if there are potential issues that must be addressed.

Assurance uses machine learning algorithms to extract behavioral patterns in the network and predict trends. These trends are displayed as baselines in the **Client Onboarding Time** and **Client Count Per SSID** dashlets.

Note The client health data might take up to an hour to populate if an HA failover has occurred.

Procedure

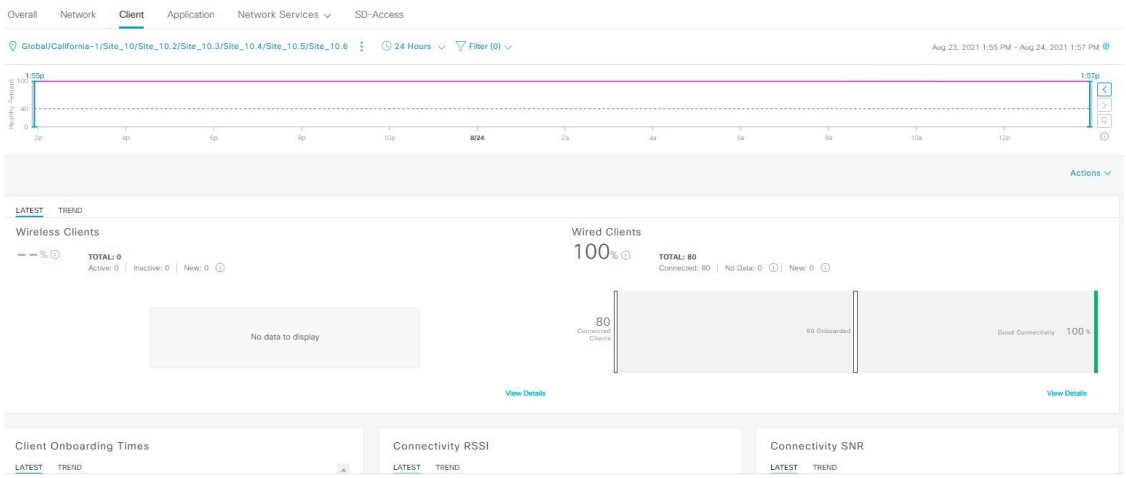
Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Client** tab.

The **Client** health dashboard appears.

Figure 15: Client health dashboard



Step 3 Use the **Client** health dashboard top menu bar for this functionality:

Client health dashboard top menu bar	
Item	**Description**
Global **Location** pane	Click to display these icons: • Click the location option (Global) in the top menu bar to select the site, building, or floor from the Site hierarchy. You cannot select a floor from the network hierarchy. • Click ⋮ next to the location icon and to switch between: • **Site Map**: Provides a geographical view of your network hierarchy. • **Site Table**: Provides a list-based view of all sites, including their health scores and device counts. • Click toggle button to display the sites and buildings from your network in a list format. Click the drop-down list for these options: • **Hierarchical Site View**: Sorts the list at a site level. From the **Go to sites** column, click for a site or building to display data only for that location on the **Network** dashboard. • **Building/Outdoor Area view** : Sorts the list at a building level. From the **Go to sites** column, click for a site or building to display data only for that location on the **Network** dashboard. • Click Export to export the device information to a CSV file. • Click toggle button to display the health of all the network sites on a geographic location-oriented network health map. By default, the network sites are color coded according to the severity of the problem. • Click close icon to hide the map or table view.
24 Hours **Time Range setting**	Click the time range setting (24 Hours) in the top menu bar to specify the time range of data that appears on the dashboard. **a.** From the drop-down menu, select the time range: **3 Hours**, **24 Hours**, or **7 Days**. **b.** Specify the **Start Date** and time, and the **End Date** and time. **c.** Click **Apply**.

Client health dashboard top menu bar	
Item	**Description**
Filter icon	Contains the **SSID** and **Band** options. Select the SSIDs and band frequency from the drop-down list by selecting the check boxes next to them, and then click **Apply**. Depending on your selection, the information in the dashboard is refreshed. **Note** You can select multiple SSIDs. For example, if you select Class 1 and Class 2 SSIDs, the dashboard displays information for the clients that are connected to Class 1 SSID and Class 2 SSID.
Actions drop-down list	Enables you to export the client dashboard to PDF format. Click **Export Dashboard** to view the preview page and click **Save**. Enables you to customize the dashboard display when you select **Edit Dashboards** from the drop-down list. See Change the position of a dashlet, on page 349 and Create a custom dashboard, on page 347.

Step 4 Use the **Timeline Slider** to view the healthy client percentage for a more granular time range.

Hover your cursor within the timeline to view the wireless and wired client health score percentage at a specific time.

You can click and drag the timeline boundary lines to specify the time range. This sets the context for client data that is displayed in the dashboard dashlets.

You can use the arrow buttons on the right of the timeline to view data for up to 30 days.

The dotted horizontal line represents the threshold value for healthy clients, which by default is set to 40%.

To change the threshold value:

a. Hover your cursor over the information ( ) icon.

b. In the tooltip, click the edit ( ) icon.

c. In the **Client Health Threshold** slide-in pane, click and drag the blue line to set the threshold percentage value.

d. Click **Save**.

Note
Changing the custom threshold affects when the Client Summary Health Score is displayed as red. The custom threshold does not change the number of healthy or unhealthy devices.

Step 5 Use the **Client Health Summary** dashlet for this functionality:

Client health summary dashlet	
Item	**Description**
Client Health Summary area	Includes these tabs: • **Latest**: Displayed by default. Includes these options: • **Wireless Clients** and **Wired Clients Health Summary Score**: The Wireless and Wired Client Summary Health score is the percentage of clients that onboarded successfully and have good connectivity. See Client Health score, on page 153. • **Total Devices**: Provides the total number of clients and the count of active, inactive, and new clients. Cisco Catalyst Center defines active, inactive, and new clients based on their activity within a 5-minute health score calculation window, as follows: • **Active**: Clients who have successfully onboarded and are sending sufficient data to meet the data threshold, clients who have successfully onboarded and then disconnected, clients attempting to onboard and fail, and clients attempting to onboard but were excluded. • **Inactive**: Clients who don't send sufficient data to meet the data threshold. After a user-idle timeout period expires, the wireless controller deauthenticates inactive clients. • **New**: Clients who are in the process of onboarding. The health score for these clients is included in the next 5-minute calculation window. • **Charts**: This snapshot-view chart provides the distribution of clients that passed or failed to onboard within the last 5 minutes. Then, from the number of clients that onboarded successfully (passed), the chart provides the percentage of clients that have good or fair connectivity. • **Trend**: Displays a trend chart that shows the health of clients over a time period. For the clients that failed to onboard, the reason for the onboarding failure is provided. Examples include AAA, DHCP, and Other. The color in the charts represents the health of the client devices: ●: Poor client devices. Health score range is 1 to 3. ●: Fair client devices. Health score range is 4 to 7. ●: Good client devices. Health score range is 8 to 10. ●: Inactive client devices. Health score is 0.

Client health summary dashlet	
Item	**Description**

View Details	Click **View Details** to open a slide-in pane with additional details.
	For both wired and wireless clients, you can view the **LATEST** and **TREND** tabs.
	• **LATEST** tab: Displays a bar chart that summarizes the client health by onboarding activity.
	• **TREND** tab: Displays two charts for tracking the client health over time.
	  • Radial bar chart: Displays the distribution of clients that failed to onboard and the reasons for these failures.
	  • Line chart: Displays onboarding failures over time in 5-minute increments.
	Note
	If wired and wireless clients use Cisco ISE for AAA management and authentication fails, you can view the top onboarding AAA and Cisco ISE failure reasons in the **TREND** tab. The AAA failure information is from the wireless controller, and the Cisco ISE information is from Cisco ISE.
	  • For wired clients, click the line chart and then click **Top Authentication Failure Reasons** to view the failure reason details.
	  • For wireless clients, click **AAA** next to the radial bar chart to view the failure reason details.
	In either tab for wireless or wired clients, you can:
	• Click a segment in a chart to view more details more about that segment.
	• Click a data type category displayed below the chart to filter the table data.
	• In the table, use the search bar to search for specific data.
	• In the table, click the device identifier or name to go the relevant **Client 360** or **Device 360** window.

Step 6 Use the KPI dashlets to view specific KPIs and metrics for the clients in your network. These tables describe the KPI dashlets.

Note
The chart data is updated every 5 minutes.

Client onboarding times dashlet	
Item	**Description**
Client Onboarding Times chart	Distribution of all clients' attempts to onboard, in all the sites or a selected site, over time. This dashlet provides the percentage of clients that took less than 10 seconds to successfully onboard. Client onboarding covers Association, Authentication, Addressing, WebAuth, and DNS phases. There are two types of charts: • **Latest**: Displayed by default. This snapshot-view chart provides the distribution of clients that passed or failed to onboard within the last 5 minutes. Then, from the number of clients that onboarded successfully (passed), the chart provides the percentage of clients that have good or fair connectivity. • **Trend**: Contains the **Client Count** and **Baseline** tabs. Click the **Baseline** tab to display the onboarding time baseline chart, which is generated through machine learning. **Note** The **Baseline** tab will be deprecated in the near future. For AI Network Analytics features, you must enable AI Network Analytics. See Configure Cisco AI Network Analytics, on page 77 and Cisco AI Network Analytics Overview, on page 7. **Important** To view the baseline chart, you must select a site and SSID from the **Filter** options. The chart details for the baseline charts are represented by different colors. • **Green band**: Predicted baseline value. • **Solid blue line**: Actual value. For the clients that failed to onboard, the reason for the onboarding failure is provided. Examples include AAA, DHCP, and Other.

Client onboarding times dashlet	
Item	**Description**
View Details	Click **View Details** to open a slide-in pane with additional details: • The left pane contains the **Overall**, **Association**, **Authentication** and **DHCP** tabs. Click the tabs to populate the charts in the right pane. • The right pane contains **Charts** that have these tabs: • **Latest**: Contains the overall average onboarding time. For Authentication and DHCP, the Latest tab contains a drop-down list to filter the data based on the Avg Latency Time, Avg Authentication Time for Authentication, and Avg DHCP Time for DHCP. • **Trend**: Contains the **Baseline** tab, which allows you to view machine learning baseline charts. Depending on the tab you select in the left pane, additional tabs display under **Trend** > **Baseline**. For example, the **Client Count**, **Time Baseline**, or **Failure Baseline** tabs appear for Association, Authentication, or DHCP data. **Note** **Failure Baseline** data is available only for the Global site. **Note** The **Baseline**, **Time Baseline**, and **Failure Baseline** tabs will be deprecated in the near future. For AI Network Analytics features, you must enable AI Network Analytics. See Configure Cisco AI Network Analytics, on page 77 and Cisco AI Network Analytics Overview, on page 7. • Hover and move your cursor over the charts to view synchronized tooltips that display information at a selected point in time. • Click a color segment in the chart to view the options: • Data type categories by client count: **Top Locations**, **Top Access Points**, **Top Host Device Types**, **Top SSIDs**, **Top Bands**, and **Top Host Operating Systems**. • A table with detailed data of the clients in that segment.

Connectivity RSSI dashlet	
Item	**Description**
Connectivity RSSI chart	Received Signal Strength Indication (RSSI) distribution for all clients, in all sites or a selected site. This dashlet provides the percentage of RSSI measurements for all clients whose RSSI measurement is higher than the threshold value of -72 dBm.

Connectivity RSSI dashlet	
Item	**Description**
View Details	Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to view: • Data type categories by client count: **Top Locations**, **Top Access Points**, **Top Host Device Types**, **Top SSIDs**, **Top Bands**, and **Top Host Operating Systems**. • A table with detailed data of the clients in that segment.

Connectivity SNR dashlet	
Item	**Description**
Connectivity SNR chart	Signal-to-Noise ratio (SNR) distribution of all clients, in all sites or a selected site. This dashlet provides the percentage of SNR measurements for all clients whose SNR measurement is higher than the threshold value of 10 dB.
View Details	Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to view: • Data type categories by client count: **Top Locations**, **Top Access Points**, **Top Host Device Types**, **Top SSIDs**, **Top Bands**, and **Top Host Operating Systems**. • A table with detailed data of the clients in that segment.

Client Roaming Times dashlet	
Item	**Description**
Client Roaming Times chart	Distribution of the clients by roaming times and failures. This dashlet provides the percentage of clients with roaming times less than 3000 ms.
View Details	Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to view: • Data type categories by client count: **Top Access Points**, **Top SSIDs**, **Top Host Device Types**, **Top Bands**, **Top Locations**, and **Top Host Operating Systems**. • A table with detailed data of the clients in that segment.

Client Count per SSID dashlet	
Item	**Description**
Client Count per SSID chart	Distribution of the number of clients per SSID, in all sites or a selected site, over time. There are two types of charts: • **Latest**: Displayed by default. This snapshot-view chart provides the distribution of clients per SSID or selected site. • **Trend**: Contains **Client Count** and **Baseline** tabs. Click the **Baseline** tab to display the SSID baseline chart, which is generated through machine learning. **Note** The **Baseline** tab will be deprecated in the near future. For AI Network Analytics features, you must enable AI Network Analytics. See Configure Cisco AI Network Analytics, on page 77 and Cisco AI Network Analytics Overview, on page 7. **Important** To view the SSID machine learning baseline chart, you must select a site and SSID from the **Filter** options. • The chart details for the baseline charts are represented by different colors. • **Green band**: Predicted baseline value. • **Solid blue line**: Actual value.
View Details	Click **View Details** to open a slide-in pane with additional details. Contains two types of charts: • **Latest** • **Trend**: Contains the **Baseline** tab, which allows you to view machine learning baseline charts. **Note** The **Baseline** tab will be deprecated in the near future. For AI Network Analytics features, you must enable AI Network Analytics. See Configure Cisco AI Network Analytics, on page 77 and Cisco AI Network Analytics Overview, on page 7. Hover and move your cursor over the charts to view synchronized tooltips that display information at a selected point in time. Click a color segment in the chart to view this information: • Data type categories by client count: **Top Locations**, **Top Access Points**, **Top Host Device Types**, **Top Bands**, and **Top Host Operating Systems**. • A table with detailed data of the wireless clients in that segment.

Connectivity Physical Link dashlet	
Item	**Description**
Connectivity Physical Link chart	Distribution of wired client device link state—the number of client devices that had their physical links up, down, and had errors.
View Details	Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to view: • Data type categories by client count: **Top Locations**, **Top Switches**, **Top Host Device Types**, and **Top Host Operating Systems**. • A table with detailed data of the clients in that segment.

Client Count per Band dashlet	
Item	**Description**
Client Count per Band chart	Distribution of wireless clients connected to the 2.4-GHz band or 5-GHz band. Hover your cursor over a segment to view the percentage and number of clients connected to a specific band.
View Details	Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to view: • Data type categories by client count: **Top Locations**, **Top Access Points**, **Top Host Device Types**, **Top SSIDs** and **Top Host Operating Systems**. • A table with detailed data of the clients in that segment.

Client Data Rate dashlet	
Item	**Description**
Client Data Rate chart	Distribution of a client's data rates. Use the **Client Protocol** drop-down list to filter clients based on the client protocol they are using. Options are **802.11n/ac/ax** and **802.11a/b/g**.
View Details	Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to view: • Data type categories by client count: **Top Locations**, **Top Access Points**, **Top Host Device Types**, **Top SSIDs**, **Top Bands**, and **Top Host Operating Systems**. • A table with detailed data of the clients in that segment.

Step 7 Use the **Client Devices** dashlet to view detailed information about the clients in your network. This dashlet provides this functionality:

Client Devices dashlet	
Item	**Description**
Type	Filter the table based on client type. Options are **Wired** and **Wireless** clients.
Health	Filter the table based on the client health with these options: • **All** • **Inactive**: Client devices with a health score of 0. • **Poor**: Client devices with a health score range from 1 to 3. • **Fair**: Client devices with a health score range from 4 to 7. • **Good**: Client devices with a health score range from 8 to 10. • **No Data**: Client devices with no data.
Data	Filter the table based on data type with these options: • **Onboarding Time >= 10 s**: Onboarding time is greater than or equal to the 10-second threshold value. • **Association >= 5 s**: Association time is greater than or equal to the 5-second threshold value. • **DHCP >= 5 s**: DHCP time is greater than or equal to the 5-second threshold value. • **Authentication >= 5 s**: Authentication time is greater or equal to 5 seconds. • **RSSI <= -72 dBm**: RSSI is less than or equal to the -72-dBm threshold value. • **SNR <= 9 dB**: SNR is less than or equal to the 9-dB threshold value.

Client Devices dashlet	
Item	**Description**
Client Device table	

Client Devices dashlet	
Item	**Description**
	View detailed client device information in a table format. The client device table displays this information by default: • **Identifier**: Displays the client's user ID, hostname, or MAC address based on availability, in that order. For example, if the user ID is not available, the hostname is displayed. If the user ID and hostname are not available, the MAC address is displayed. The **Identifier** column also has specific icons that allow you to determine if the client device is wired or wireless. For wireless devices, the icon includes a blue dot while the client is connecting and when the client is newly connected. • **MAC Address**: Displays the MAC address, which includes Device MAC and Randomized and Changing MAC Address (RCM). The Private MAC icon appears in front of the RCM. You can filter the table based on the type of MAC address, such as All, Device MAC, and RCM. • **IPv4 Address**: Displays the client's IPv4 address based on availability. **Note** You can display the client's IPv6 address by checking the **IPv6 Address** check box in the menu. • **Device Type**: Displays the device type. • **Health**: Displays the average of the onboarding and connected scores. The Client Health score is calculated every 5 minutes. **Note** A score of -- indicates that the client has recently onboarded (new). New clients are clients that attempted to onboard after the 5-minute health score calculation window started. The health score for these new clients is included in the next 5-minute calculation window. • **Trust Score**: Displays the trust score for the endpoints connected to your network based on the AI Endpoint Analytics trust level. • **Tracked**: Displays client tracking status. • **Last Seen** • **AP Name** (for wireless clients only): Displays the name of the access point. • **Switch** (for wired clients only) • **Port** (for wired clients only) • **Location**: Displays the assigned location of the client. • **Security Group (Tag Value)**: Displays the security group tag value for wired clients only. • **Bridge-Mode Virtual Machine**: Displays bridge mode virtual machine for wireless clients only. • **Average Latency By Access Category**: This includes Avg video, Avg voice, Avg best effort

Client Devices dashlet	
Item	**Description**
	and Avg background latencies. • **Link Speed** (for wired clients only): Indicates the speed capacity of the interface or physical port. If the port has negotiated to a certain speed, the negotiated speed is displayed. **Note** You can display the link speed by checking the **Link Speed** check box in the ⋮ menu.
Tracked Clients	Click **Tracked Clients** to view the slide-in pane that displays a table containing the **MAC Address**, **Last Detected**, **Tracking Duration**, **Description**, and **Randomized MACs**.
Excluded Clients	Click **Excluded Clients** to view the slide-in pane that displays the client exclusion list containing the **Excluded MAC address**, **Excluded Since**, **Impacted Wireless Controllers**, and **Description**. For more information about excluding clients, see Configure excluded clients, on page 152.
View **Client 360** for a client	Display a 360° view of a client by clicking the MAC address or identifier of a client device. **Client 360** provides detailed information for troubleshooting client connectivity issues.
Export	Click **Export** to export the device information to a CSV file.
⚙	Customize the table display: **a.** From the **Table Appearance** tab, set the table density and striping. **b.** From the **Edit Table Columns** tab, select the data you want displayed in the table. **c.** Click **Apply**.

Monitor and troubleshoot the health of a client device

Using the **Client 360** window, a network administrator can easily identify problems that clients experience. The information that is available provides these insights about client issues:

- **What**: Use the **Summary** category to quickly gain insights into what problem a client has experienced, whether it was an onboarding, roaming, or connectivity issue.
- **When**: Use the health timeline slider to identify when a problem occurred. If you know when a problem occurred, you might be able to correlate it with configuration changes.
- **Why**: View the events and KPIs that contributed to a problem.
- **Impact**: Determine whether a problem is isolated to a single user or widespread among many users.

All these features make the IT organization more efficient in operating the network and providing a better experience to their users.

Use this procedure to view details about a specific client device and to determine if there are potential issues that must be addressed. Assurance supports site-based, role-based access control (SRBAC), which limits a user's scope of access to certain client 360. You must ensure you have access to the sites, wired and wireless clients. in the client 360 window. For more information on user roles and permissions, see Cisco Catalyst Center Administrator Guide

Note As a best practice, add both Anchor and Foreign wireless controllers to Catalyst Center for complete visibility of guest anchor or L3 mobility client sessions.

If an HA failover occurs, the client health data might take up to an hour to populate.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Client** tab.

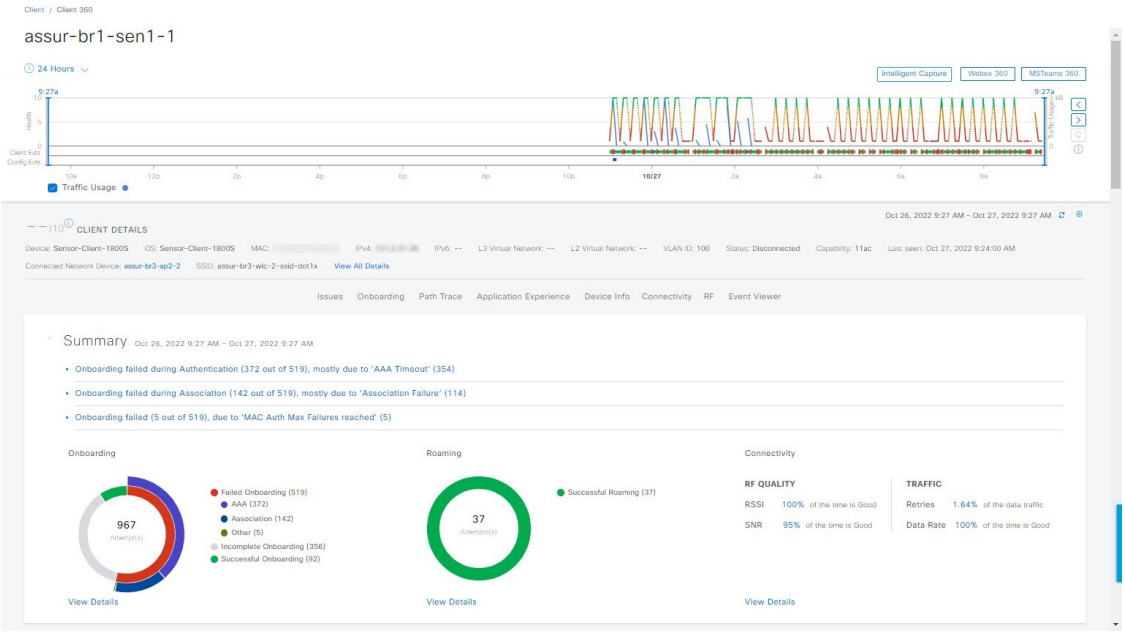
The **Client** health dashboard appears.

Step 3 Do one of these tasks:

- In the **Client Devices** table, click the hyperlinked identifier or the MAC address of the device.
- In the **Search** field, enter one of these elements:
  - User ID (authenticated through Cisco ISE)
  - IP address
  - MAC address

The **Client 360** window displays a 360° view of the client device.

Figure 16: Client 360 window



Step 4 Click the time range setting (24 Hours) in the top menu bar to specify the time range of data that appears on the dashboard.

a) From the drop-down menu, select the time range: **3 Hours**, **24 Hours**, or **7 Days**.

b) Specify the **Start Date** and time, and the **End Date** and time.

c) Click **Apply**.

Step 5 Click **Intelligent Capture** at the top-right corner of the window to view, monitor, and troubleshoot captured onboarding and data packets for a specific client device to determine if there are potential issues that must be addressed. See Run an Onboarding Packet Capture live session for a client device, on page 391.

Note
Intelligent Capture is not supported for all AP models. If **Intelligent Capture** is not displayed, verify that the client is connected to a supported AP model, and that the AP is assigned to a location on the **Network Health** dashboard.

Step 6 Click **MS Teams 360** at the top-right corner above the timeline slider to view and monitor the client MS Teams meetings.

The **Application Experience for MS Teams** slide-in pane is displayed.

To configure a Microsoft Teams integration, see *Configure MS Teams Integration* in the *Cisco Catalyst Center Administrator Guide*.

Use the **Application Experience** slide-in pane for this functionality:

- **Search bar**: You can search for meetings in the table.
- **Time Range filter**: Click the time filter to specify a time range for the data you want to be displayed.
- The Client Meetings table shows the **Meeting Name**, **MS Teams Score**, **Network APM Score**, **Duration**, **Start Time**, **End Time**, **Status**, **Meeting Type**, and **Participants**.

Note

The Network APM score is calculated based on NetFlow data exported from the managed network devices. The data is aggregated every 5 minutes. If the call duration is less than 5 minutes, there might be no matching NetFlow records, so the APM score displays “No data available” for these short-duration calls. For more information regarding APM, see Supported platforms, on page 158.

To select the meeting to view the meeting quality KPI data::

- Click the **Audio Quality** tab to display an **MS Teams Score** and **Network APM Score**. You can see the metrics like **Packet loss**, **Jitter**, and **Media Bitrate** in a graph view.
- Click the **Video Quality** tab to display an **MS Teams Score** and **Network APM Score**. You can see the metrics like **Packet loss**, **Jitter**, and **Media Bitrate** in a graph view.
- Click the **Share Quality** tab to display an **MS Teams Score** and **Network APM Score**. You can see the metrics like **Packet loss**, **Jitter**, and **Media Bitrate** in a graph view.

Step 7 Click **Webex 360** at the top-right corner above the timeline slider to view, monitor the client Webex meetings. The search meeting pop-up window appears.

To configure Webex integration, see *Configure Webex Integration* in the *Cisco Catalyst Center Administrator Guide*.

a) Enter the email associated with the client's Webex meeting.
b) Click **Search Meetings**. The Application Experience for Webex slide-in pane is displayed.
c) Use the Application Experience slide-in pane for this functionality:

- **Search bar**: You can search for meetings in the table displayed.
- **Time Range filter**: Click time filter to specify time range for the data you want to display in the table.
- The Client Meetings table shows the **Meeting Number**, **Meeting Name**, **Application**, **Network Duration**, **Start Time**, **End Time**, and **Status**.

  You can select the meeting to view the meeting quality KPI data displayed below the table as horizontal bars showing Audio quality, Video Quality and Share Quality based on application (data retrieved using Webex API) and network (data retrieved using NetFlow) latencies. You can use the drop-down list to filter the data based on Transmitting and Receiving options to display the application and network latency graphs related metrics such as packet loss, jitter, and so on.

Step 8 Use the timeline slider to view the health and events information about the client device over a period of time.

Use this table for timeline slider functionality.

If you want to...	Then...
View the client telemetry status	**a.** Under the timeline slider, check the **Telemetry Status** check box. The telemetry status line displays in the timeline slider. **b.** Hover your cursor over the timeline slider to view the network device telemetry status, such as Good, Fair, or Poor, in the tool tip. **c.** Under Client Health, click **Telemetry Status** to view a summary of the telemetry status in a slide-in pane.

If you want to...	Then...
View client traffic usage	**a.** Under the timeline slider, check the **Traffic Usage** check box. The traffic usage line displays in the timeline slider. **b.** Hover your cursor over the timeline slider to view the client usage information.
View client health and KPI details	Hover your cursor over the timeline slider to view the client health and KPI details for a 5-minute window. **Note** • Each KPI with a colored circle contributes to the individual client health score. • For the **Data Rate** KPI, the data rate capacity of the interface or physical port is displayed. If the port has negotiated to a certain rate, then that negotiated rate is displayed.
Display a 1-hour time period in timeline	Double-click the timeline. The entire window is refreshed, providing updates for that hour. **Note** To display information for longer than 1 hour, manually move the timeline slider to the desired time range.
View onboarding details	Hover your cursor over the timeline slider to view the client onboarding pass or failure details. • If client onboarding passes, onboarding times, such as association and authentication, are displayed. • If client onboarding fails, the failure type and reason (including the Cisco ISE failure reason if available) are displayed.
View connectivity details	Hover your cursor over the timeline slider to view connectivity details, such as the RSSI and SNR.
View connection details	Hover your cursor over the timeline slider to view connection details, such as the IP address and status.

If you want to...	Then...
View major events details	**a.** Hover your cursor over the timeline slider to view the client's major events. Keep these details in mind. • Event data is displayed as color-coded vertical bars on the graph. Green vertical bars indicate successful events, and red vertical bars indicate events that failed. • Each vertical bar represents 5 minutes of time. Multiple significant events can be generated during each 5-minute window. Hover your cursor over the vertical bar to get more information about the events. **b.** Click **See Full List** to go to the **Event Viewer** dashlet to view all major events for the client.

Step 9 View the individual client health score in the **Client Details** area, below the timeline.

The individual client health score is an aggregate of the client's onboarding status, RSSI, and SNR.

If you search by the user ID, the Individual Client Health score that is displayed is the minimum score of all the monitored client devices associated with that user. For more information, see Individual Client Health score, on page 155.

If you search by MAC address or IP address, the Individual Client Health score is the health score for that client device.

The color of the health score represents its severity. The health is measured on a scale of 1 to 10, with 10 being the best score, and a score of 0 for inactive client devices, where the health data is not applicable:

- : Poor client devices. Health score range is 1 to 3.
- : Fair client devices. Health score range is 4 to 7.
- : Good client devices. Health score range is 8 to 10.
- : Inactive client devices. Health score is 0.

Note
For clients that are disconnected from the network, the score is represented as a - -.

Step 10 Use the **Client Details** area, below the timeline, to view this information:

- For wireless clients, this area provides information about the client device such as its OS version, MAC address includes Device MAC and RCM, IPv4 and IPv6 address, Bridge-Mode Virtual Machine, connected VLAN ID, connection status, Avg Latency, last seen timestamp, connected network device, SSID, and last known location.

  Wi-Fi 7 capable wireless clients and access points connects to any combination of 2.4GHz or 5GHz or 6 GHz bands. MLO (Multiple Link Operational) clients by establishing connections to different bands at the same time results in higher data transfer rate. When wireless client is connected with Wi-Fi 7 capable APs or Zealand APs, Catalyst Center supports four KPIs per link: RSSI, SNR, special stream, and channel. For Wi-Fi 7 capable clients hover over cursor on the timeline to view the connectivity KPIs (Channel, SNR and RSSI) operating in multiple links for a 5-minute window. But the data transfer may happen in single link or multiple links based on the clients.

- For wired clients, this area provides information about the client device such as its MAC address, IPv4 and IPv6 address, Security Group (Tag Value), connected VLAN ID, connection status, last seen timestamp, connected network device, port, and last known location.
- For PoE-capable devices, these elements are also displayed in the client details area: **IEEE Class**, **Negotiated Power Level**, and **PoE Status**.

Step 11 In the **Client Details** area, click **View All Details** to open a slide-in pane with additional details about the client device.

To view client device classification information (such as device type, username, host OS, and hostname), Catalyst Center must be integrated with Cisco ISE, or Cisco AI Endpoint Analytics must be deployed and enabled in Catalyst Center.

Step 12 Use the collapsible categories to view information about issues, onboarding, event viewer, path trace, application experience, and other details:

Summary category
Provides onboarding, roaming, and connectivity information, which includes traffic-retires and data rate, average latency by category (video, voice, best effort, and background) for the selected client in the form of human-readable summaries and graphs for the selected timeframe. Click an issue in the list to display a slide-in window with details about the client's experience at the last location that was visited. The slide-in window displays information based on the client, location, and issue. Depending on the issue, the slide-in pane displays these details: • **Location**: Click the drop-down field and select a building or floor that the client visited in the last 24 hours. Details about the client's experience at that location are displayed. • **Issue radial bar chart**: Summarizes the issue in a graphical chart. • **Top Failure Reasons**: Indicates the number of times that the client encountered the issue. For example, onboarding issues might show the number of DHCP timeouts. **Note** For the onboarding category, you can click **AAA** next to the radial bar chart to view the top AAA or Cisco ISE failure reasons. The AAA failure information is from the wireless controller, and the Cisco ISE failure information is from Cisco ISE. If you click **Top ISE Failure Reasons**, the **Event Viewer** table lists the Cisco ISE authentication event and the corresponding authentication event from the wireless controller so that data can be compared. Note that the number of failure events reported from the wireless controller and Cisco ISE may not match because of the amount of client retries from the wireless controller and the failure report throttling from Cisco ISE. • **Timeline slider**: The timeline slider displays periods of client failures. Click a colored segment in the radial bar chart to filter the timeline slider based on that segment. The line above the bars in the timeline slider indicates when the network experienced the same issue, including other clients at the selected location. APs that the client attempted to connect with are noted. • **Event Viewer**: Click this tab to display information about the failure. • **Impact Analysis**: Click this tab to display the top impacted components, for example, top AP, SSID, band, and so on. Under each component, in parenthesis, is the number of additional clients who were impacted by the component. impact analysis tab • **Correlation**: Click this tab to display timeline charts of KPIs for failures that the client experienced. By default, the top three APs where the client experienced the failure are shown, including the connected wireless controllers and switches. In addition to the default KPIs, you can select more from the KPI drop-down list.

Issues category

Displays any issues that must be addressed. Issues are listed based on the timestamp. The most recent issue is listed first.

Click an issue to open a slide-in pane to view the corresponding details, such as the description of the issue, relevant clients that are experiencing the same type of issue, and suggested actions.

Note
For wireless clients experiencing Cisco ISE authentication failure issues, you can do these tasks:

- View the top Cisco ISE failure reasons for other clients experiencing the same type of issues from the slide-in pane in the **Relevant Clients** tab.
- View the suggested actions to address the failure issues from the slide-in pane in the **Suggested Actions** tab.

From the slide-in pane, you can do these tasks:

- To resolve an issue:
  a. From the drop-down list, select **Resolve**.
  b. To view the list of issues that have been resolved, click **Resolved Issues**.
- To ignore an issue:
  a. From the drop-down list, select **Ignore**.
  b. Set the number of hours to ignore the issue on the slider.
  c. Click **Confirm**.
  d. To view the list of issues that have been ignored, click **Ignored Issues**.

For information about the types of issues, see View and Manage Issues, on page 239.

Onboarding category

Topology of how a client got on the network, including information about these services: AAA and DHCP.

Example of wired client topology: **Client** > **Switch** > **Router**

Example of wireless client topology: **Client** > **SSID** > **Access Point** > **Wireless Controller**

In the topology, you can do these tasks:

- Click a node to display a slide-in window that displays information about the node.
- Hover your cursor over the link ends (dots) to see the status and port details of the link. When a Wi-Fi 7 capable client is connected to multiple bands, the band values (2.4 GHz, 5 GHz and 6 GHz) are displayed on top of the topology link.
- Hover your cursor over a group of devices and click **View Devices List** from the pop-up to view the list of devices and their details.
- In the Search field in the top-right corner of the **Onboarding** area, you can search for a specific device. The specific node is selected, and the corresponding information about the device is displayed.

Event view category
For Wireless Clients: Lists scenarios and the sequence of subevents that led to each scenario. This list allows you to pinpoint during which subevent an issue occurred. When an issue occurs, that event is marked red; otherwise, it's green. The Event Viewer table provides information about the failure, such as the error message, the AP and wireless controller to which the client device is connected, and the timestamp when the event occurred. Click an event to view details about that event in the right pane. **For Wired Clients**: Lists Cisco ISE server events, switch system level syslogs, switch port or interface-specific events, and client-specific events. Successful events are displayed as green; failure events that impact the health score are displayed as red. The Event Viewer table provides information about the failure, such as the type of message, the device information to which the wired client device is connected, and the timestamp when the event occurred. Click an event to view details about that event in the right pane. **Note** To view more details about a Cisco ISE authentication failure event, click the **ISE Authentication** event with a red circle and view the details in the right pane. In the right pane, click **Show ISE Events** to view the Cisco ISE authentication steps completed by the RADIUS server. Each step includes a code number with its corresponding description, which is collected from Cisco ISE.

Path Trace category
Click **Run New Path Trace** to display a network topology between a specified source device and a destination device. The topology includes the path's direction and the devices along the path, including their IP addresses. The display also shows the protocol of the devices along the path (**Switched**, **STP**, **ECMP**, **Routed**, **Trace Route**) or other source type. See Do a path trace, on page 428.

Application Experience category
Applications running on a client device with their qualitative and quantitative metrics. To view the metrics in a chart format, click the radio button next to an application in the table. A slide-in pane opens with the relevant information. See About Application Experience and Application Visibility, on page 157 and View Application Experience of a host, on page 164.

Detail Information category
Click one of these tabs to display the corresponding information: • **Device Info**: Displays basic information about the device. For Samsung devices, this tab displays additional information, such as build number, origin, country code, device type (mobile, tablet, and so on), and host operating system. For Wi-Fi 7 capable clients, the connection information displays channel and band values. For the endpoints connected to your network, this tab displays **Manufacturing** details such as **Hardware Manufacturer**, **Device Type**, **OS**, and **Endpoint Type**. This tab also displays the **Tracked** and **Exclusion** status of the device. If required, click the corresponding hyperlink to update the tracked and exclusion status of the device. For instructions on how to track clients, see Track known clients, on page 148. In the **Exclude clients** slide-in pane, do these steps: **a.** Use the toggle button to configure the exclusion status of the device. **b.** If you enable the toggle button, enter a description in the **Description for Exclusion** field, and check the check box next to the wireless controller for which you want to exclude the device. **c.** Click **Save**. The available security information displayed, such as the authentication type and security policy type, depends on the client connection and if Cisco ISE is integrated with Catalyst Center. Station information, such as the HW model, SW version, AC/DC voltage, is only available for Intel devices. • **RF**: Only available for wireless devices. • **User Defined Network**: Only available for UDN-enabled network devices. This tab displays the registered UDN, connected UDN details, device MAC address, device owner, device name, device type, and current status. • **Connectivity**: Displays the respective KPI charts for Rx/Tx data rate, Tx/Rx packet count, Rx retries connection for radios, DNS request and response count, and Tx drops (% of packet drops). • **PoE**: Only available for PoE-capable clients. • **iOS Analytics**: Only available for Apple devices. • **Intel Connectivity Analytics**: Only available for devices supported by Intel wireless adapters. Displays the roam events, reported errors, temporary disconnection reports, and low RSSI reports reported by the supported client.

Client tracking

Client tracking is an Assurance feature that allows you to

- track and monitor when clients connect to and disconnect from the network,
- track known and new clients, and

- receive notifications for client tracking events.

By proactively monitoring and tracking connectivity for designated critical clients, this feature gives you real-time visibility into their connectivity status. With these capabilities, you can quickly identify and respond to potential disruptions, helping ensure that your most essential devices and users remain connected and operational.

Types of clients

You can track either known clients or new clients.

- Known clients: Clients that have previously connected to the network.
- New clients: Clients that have not previously connected to the network.

Types of tracking notifications

You can configure two types of tracking notifications: connect or disconnect.

- Connect notification: Notify you when the client connects to the network. You can choose to be notified only when the client first connects to the network or every time it connects to the network.
- Disconnect notification: Notify you each time the client disconnects from the network.

Disconnect notification behavior

If you configure disconnect notifications for clients, review this disconnect notification behavior:

- If a client disconnects but reconnects within 5 minutes, no disconnect notification is sent. This approach prevents alerts for brief disruptions that resolve quickly or for normal client roams.
- Disconnect notifications are limited in frequency to prevent spam:
  - For wireless clients: If the client disconnects for the same reason throughout an hour, only one notification is sent. If the disconnect reason changes within the hour, a new notification is sent.
  - For wired clients, a disconnect notification is sent once every hour.

Track known clients

Use this procedure to track and monitor specific known clients, showing when they connect to or disconnect from the network. You can set up tracking notifications so that when a tracked client connects or disconnects, you are notified.

Before you begin

You must meet these requirements:

- Only users with NETWORK-ADMIN-ROLE or SUPER-ADMIN-ROLE permissions can perform this procedure.
- Ensure that the "Tracked Client activity detected on network" event (event ID: NETWORK-CLIENTS-4-370) is enabled, allowing you to receive notifications when clients connect or disconnect. If this event is not enabled, you will not receive notifications for the tracked clients, even if

client tracking is configured. Note that this event was formerly named “Clients detected connecting on network”.

For the steps to create an event notification, see "Create an Event Notification" in the "Build and Deploy Workflows" chapter of the *Cisco Catalyst Center User Guide*.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Client** tab.

Step 3 If you want to track only one client, do these steps:

a) In the **Client Devices** dashlet, click the hyperlinked identifier or the MAC address of the device.
b) On the **Client 360** page, under **Detail Information**, click **No** in the **Tracked** field.
c) In the **Track Client** slide-in pane, click the **Not Tracking** toggle button.
d) Under **Notification Frequency**, check the check boxes to subscribe to the notification types.

- **Connect Notification**: Notify you when the client connects to the network.
- **Disconnect Notification – On every detection**: Notify you each time the client disconnects from the network.

e) If you checked the **Connect Notification** check box, indicate how frequently you want to receive this notification.

- **On First Detection**: Notify you only when the client first connects to the network.
- **On Every Detection**: Notify you every time the client connects to the network.

f) Under **Notification expiration**, indicate when you want these notifications to expire.
g) Click **Save**.

The client is tracked and added to the tracked client list.

Step 4 If you want to track multiple clients, do these steps:

a) In the **Client Devices** dashlet, check the check box next to each client that you want to track.
b) From the **Actions** drop-down list, choose **Track Client**.
c) In the **Track Client** slide-in pane, click the **Not Tracking** toggle button if it's displayed.
d) Under **Notification Frequency**, check the check boxes to subscribe to the notification types.

- **Connect Notification**: Notify you when the client connects to the network.
- **Disconnect Notification – On every detection**: Notify you each time the client disconnects from the network.

e) If you checked the **Connect Notification** check box, indicate how frequently you want to receive this notification.

- **On First Detection**: Notify you only when the client first connects to the network.
- **On Every Detection**: Notify you every time the client connects to the network.

f) Under **Notification expiration**, indicate when you want these notifications to expire.
g) Click **Save**.

The selected clients are tracked and added to the tracked client list.

Track new clients

Use this procedure to track and monitor new clients when they connect to or disconnect from the network. You can set up tracking notifications so that when the new clients connect or disconnect, you are notified.

Before you begin

You must meet these requirements:

- Only users with NETWORK-ADMIN-ROLE or SUPER-ADMIN-ROLE permissions can perform this procedure.
- Ensure that the "Tracked Client activity detected on network" event (event ID: NETWORK-CLIENTS-4-370) is enabled, allowing you to receive notifications when clients connect or disconnect. If this event is not enabled, you will not receive notifications for the tracked clients, even if client tracking is configured. Note that this event was formerly named “Clients detected connecting on network”.

  For the steps to create an event notification, see "Create an Event Notification" in the "Build and Deploy Workflows" chapter of the *Cisco Catalyst Center User Guide*.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**

The **Overall** health dashboard is displayed.

Step 2 Click the **Client** tab.

Step 3 In the **Client Devices** dashlet, click **Tracked Clients**.

The **Tracked Client** slide-in pane opens and lists all currently tracked clients and expired tracked clients by their MAC address.

Step 4 Follow one of these methods to add new clients for tracking.

If you want to...	Then in the Tracked Client slide-in pane...
add clients in bulk,	click **Import Client List (CSV)** and go to Step 5, on page 150.
manually add clients by MAC address,	click **+ Add New** and go to Step 6, on page 151.

Step 5 If you chose to add clients in bulk, do these steps:

a) Click **CSV Sample** to download a sample file.
b) Edit the sample file to include all the required client information.
c) Drag and drop your CSV file into the file upload area.

Alternatively, click **Choose a file**, select your CSV, and click **Upload**.

d) Click **Save**.

The new clients are imported into the system, and they are added to the tracked client list.

Step 6 If you chose to manually add clients, in the **Add New Clients** slide-in pane, do these steps:

a) In the **MAC Address** field, enter the client MAC address.
b) In the **Description for Tracking** field, enter a short description of the client.
c) (Optional) To add more clients, click the plus icon. Then, enter the client MAC address and a description.
d) Under **Notification Frequency**, check the check boxes to subscribe to the notification types.
   - **Connect Notification**: Notify you when the client connects to the network.
   - **Disconnect Notification – On every detection**: Notify you every time the client disconnects from the network.
e) If you checked the **Connect Notification** check box, indicate how frequently you want to receive this notification.
   - **On First Detection**: Notify you only when the client connects to the network.
   - **On Every Detection**: Notify you every time the client connects to the network.
f) Under **Notification expiration**, indicate when you want these notifications to expire.
g) Click **Save**.

The new clients are tracked and added to the tracked client list.

Stop tracking clients

Use this procedure to stop tracking clients and to stop receiving notifications when those clients connect to or disconnect from the network.

You can stop tracking either one client or multiple clients.

Before you begin

Only users with NETWORK-ADMIN-ROLE or SUPER-ADMIN-ROLE permissions can perform this procedure.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**

The **Overall** health dashboard is displayed.

Step 2 Click the **Client** tab.

Step 3 If you want to stop tracking one client, do these steps:

a) In the **Client Devices** dashlet, click the hyperlinked identifier or the MAC address of the device.
b) On the **Client 360** page, under **Detail Information**, click **Yes** in the **Tracked** field.
c) In the **Tracked Client** slide-in pane, click the **Tracking** toggle button. Then click **Save** to disable tracking for this client.

   The selected client is no longer tracked and marked as expired in tracked client list.

Step 4 If you want to stop tracking multiple clients, do these steps:

a) In the **Client Devices** dashlet, click **Tracked Clients**.
b) Check the check boxes for the client devices that you want to stop tracking.
c) From the **Actions** drop-down list, choose **Stop Tracking Client** and then click **Ok**.

The selected clients are no longer tracked and marked as expired in tracked client list.

Configure excluded clients

Use this procedure to configure excluded clients for Cisco Wireless Controllers. Using the **Excluded Clients** option, you can configure these tasks:

- Add clients to the exclusion list.
- Edit the clients in the exclusion list.
- Add the wireless controllers for which you want to exclude clients.
- Delete clients from the exclusion list.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Client** tab.

Step 3 From the **Client Devices** dashlet, click **Excluded Clients**.

Step 4 In the **Excluded Clients** slide-in pane, to add clients to the exclusion list, use one of these methods:

- To select clients from the drop-down list, click **Add** and configure accordingly:
  - **a.** From the **MAC Address** drop-down list, select a MAC address. Alternatively, you can enter a valid MAC address in the search field and click the plus icon to add the MAC address.
  - **b.** In the **Description for Exclusion** field, enter a description.
  - **c.** (Optional) To add another MAC address, click the plus icon.
  - **d.** Click **Next**.
  - **e.** Check the check box next to the wireless controller for which you want to exclude clients.
  - **f.** Click **Save**.
- To import the list of clients in CSV format, click **Import Client List (CSV)** and follow these steps:
  - **a.** Click **CSV Sample** to download the sample CSV file.
  - **b.** Edit the sample CSV file to include the client information.

c. Drag and drop the CSV file into the file upload area. Alternatively, you can click **Choose a file** and navigate to where your CSV file is located, and then click **Upload**.

d. Click **Next**.

e. Check the check box next to the wireless controller for which you want to exclude clients.

f. Click **Save**.

Step 5 To edit the clients in the exclusion list:

a) Check the check box next to the excluded MAC addresses that you want to edit.
b) Hover your cursor over **Actions** and select **Edit**.
c) Edit the description and click **Save**.

Step 6 To add the wireless controllers for which you want to exclude clients:

a) Check the check box next to the excluded MAC addresses for which you want to add wireless controllers.
b) Hover your cursor over **Actions** and select **Add WLC**.
c) Check the check box next to the wireless controller for which you want to exclude clients.
d) Click **Save**.

Step 7 To delete clients from the exclusion list:

a) Check the check box next to the excluded MAC addresses that you want to delete.
b) Hover your cursor over **Actions** and select **Delete**.
c) Click **Yes**.

Understand Client Health score and KPI metrics

This section provides information about how the Client Health scores and KPI metrics are computed.

Client Health score

The Client Health score (Wireless or Wired) is the percentage of the number of healthy client devices (a health score from 8 to 10) in a target category, divided by the total number of client devices in that category. The score is calculated every 5 minutes.

For example: 90% (health score) = 90 (client devices in a target category with health score from 8 to 10) ÷ 100 (total number of client devices in that category)

The Individual Client Health score is the sum of the Client Onboarding score and the Client Connectivity score. The client health score ranges from 1 to 10, with a score of 0 for inactive clients. It is calculated accordingly:

Wired Client: Link to first switch is up, authentication and authorization is successful and IP address is received. KPIs included for health score such as Link Discard, Link Error, and Link Utilization. Client score is 10.

Wireless Client: Client joined the network and has good connection in terms of the RSSI, SNR, Data Rate, and Retires KPIs.

Client Onboarding score

The Client Onboarding score indicates the experience of a client device *while* connecting to the network.

- If a client connects to the network successfully, the score is 4.
- If a client failed to connect to the network, the score is 1.
- If a client is idle, the score is 0.

The Client Onboarding score is calculated accordingly:

Wired Client: Link to the first switch is up, authentication and authorization is successful, and IP address is received.

Wireless Client: Client Onboarding score range is from 1 to 4. When the client connects to the network successfully, the score is 4. If the client failed to connect to the network, the score is 1.

Client Connectivity score

The **Client Connectivity** score indicates the experience of the client device *after* the device is connected to the network. The score is calculated accordingly:

Wired Client: Connectivity score can be 2 or 6. Link errors determine the Connectivity score and the resulting Overall Health score accordingly:

- If a client onboards successfully but has link errors, the Connectivity score is 2 and the Overall Health score is 6.
- If the client onboards successfully and there are no link errors between the client and the first-hop switch, the Connectivity score is 6 and the Overall Health score is 10.

Wireless Client: Connectivity score can be 0, 4, or 10. The RSSI and SNR range determines the Connectivity score and the resulting Overall Health score is calculated as the weighted average of the RSSI-driven Connectivity score and the SNR-driven Connectivity score.

RSSI-driven connectivity score	
Client's RSSI	**RSSI-driven connectivity score**
If RSSI is less than or equal -72 dBm.	The client receives a RSSI-driven connectivity score of 4 and is considered to be in fair health.
If RSSI is greater to -72 dBm.	The client receives a RSSI-driven connectivity score of 10 and is considered to be in good health.

SNR-driven connectivity score	
Client's SNR	**SNR-driven connectivity score**
If SNR is less than or equal to 9.	The client receives a SNR-driven connectivity score of 4 and is considered to be in fair health.
If SNR is greater than 9.	The client receives a SNR-driven connectivity score of 10 and is considered to be in good health.

Retries-driven health score	
Client's Retries	**Retries-driven health score**
If Retries are greater than 50%.	The client is considered to be in poor health.
If Retries are less than or equal to 50%.	The client is considered to be in good health

Wireless Client Health indicated by Data Rate	
Protocol	**Data rate-driven health score**
802.11 a/b/g	The client data rate threshold less than 5 Mbps is considered poor health, while 5 Mbps or higher is considered to be good health.
802.11 n/ac	The client data rate threshold less than 24 Mbps is considered poor health, while 24 Mbps or higher is considered to be good health.
802.11 ax/ax6/be	The client data rate threshold less than 54 Mbps is considered poor health, while 54 Mbps or higher is considered to be good health.

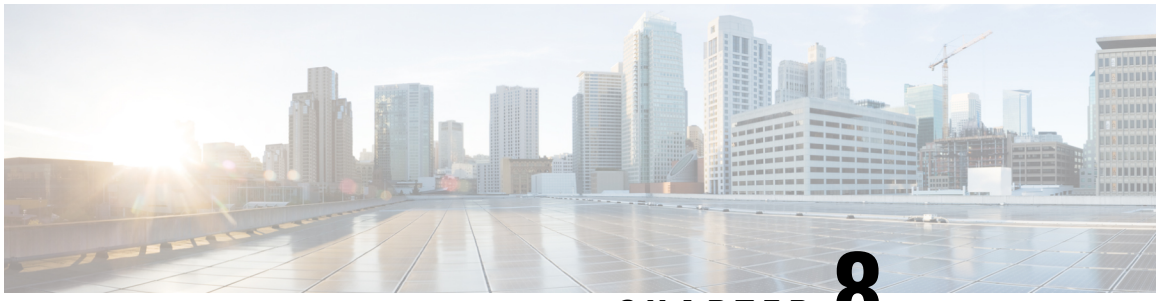
Individual Client Health score

The Individual Client Health score is the sum of the Client Onboarding score and the Client Connectivity score. The Client Health score ranges from 1 to 10, with a score of 0 for inactive clients. It is calculated accordingly:

Wired Client: Link to first switch is up, authentication and authorization is successful, and IP address is received. Client score is 10.

Wireless Client: Client joined the network and has good connection in terms of RSSI and SNR KPIs.

Client's onboarding and connectivity	Resulting Client Health score
If the client failed onboarding.	The client receives a health score of 1 and is considered to be in poor health.
If the client's RSSI and SNR are below threshold.	The client receives a health score of 4 and is considered to be in fair health.
If either the client's RSSI or SNR is below threshold.	The client receives a health score of 7 and is considered to be in fair health.
If the client's RSSI and SNR is above threshold.	The client receives a health score of 10 and is considered to be in good health.



CHAPTER 8

Monitor Application Health

- About Application Experience and Application Visibility, on page 157
- Supported platforms, on page 158
- Criteria for enabling application telemetry on devices, on page 159
- Application health prerequisites, on page 161
- Provision application telemetry settings, on page 163
- View Application Experience of a host, on page 164
- View Application Experience of a network device, on page 165
- Monitor the health of all applications, on page 166
- Monitor the health of an application, on page 178
- Configure health score settings for applications, on page 189
- Understand application health score and KPI metrics, on page 189

About Application Experience and Application Visibility

Assurance processes complex application data and presents the findings in Assurance health dashboards to provide insight into the performance of applications.

You can view the health data from a device perspective (**Device 360** window), from the user perspective (**Client 360** window), or from the application perspective (**Application 360** window).

Depending from where the data is collected, you can see some or all of this information:

- Application name
- Throughput
- DSCP markings
- Performance metrics (Latency, Jitter, and Packet Loss)

Application Name and Throughput are collectively referred to as **Quantitative** metrics. Data for the Quantitative metrics comes from enabling **Application Visibility**.

DSCP Markings and Performance Metrics (Latency, Jitter, and Packet Loss) are collectively referred to as **Qualitative** metrics. Data for the Qualitative metrics comes from enabling **Application Experience**.

Application Visibility

Application Visibility data is collected from switches running IOS-XE, and from wireless controllers running AireOS.

For switches running IOS-XE, Application Visibility data is collected using a predefined NBAR template that is applied bidirectionally (ingress and egress) to the physical layer access switch ports.

For wireless controllers running AireOS, Application Visibility data is collected at the wireless controller, and then streaming telemetry is used to transport this data to Catalyst Center.

For wireless devices, both the management interface and wireless management interface may be present. The interface used for device discovery determines the source interface for Application Visibility and Control (AVC) configuration. If the expectation is to use wireless management interface instead of the network management interface for configuring AVC, the device must be discovered in Catalyst Center using the wireless management interface.

Application Experience

Application Experience data is collected from Cisco IOS-XE router platforms, specifically using the Cisco Performance Monitor (PerfMon) feature and the Cisco Application Response Time (ART) metrics.

Examples of router platforms include ASR 1000, ISR 4000, and CSR 1000v. For device compatibility with Catalyst Center, see the *Cisco Catalyst Center Compatibility Matrix*.

To view the Cisco Performance Monitor feature availability, use the Cisco Feature Navigator tool. Click **Research Features**, and then add **Easy Performance Monitor Phase II** in the filter field.

Optimized Application Performance Monitoring

Optimized Application Performance Monitoring (APM) is a feature on the device that reduces the overhead in collecting NetFlow data. APM is supported on Cisco IOS-XE routers, Cisco 9800 series wireless controllers, and the Catalyst Center Traffic Telemetry Appliance. For minimum software versions, see Supported platforms, on page 158.

Supported platforms

This table lists the supported platforms, type of data collection, and software and license requirements.

Note For device compatibility with Catalyst Center, see the *Cisco Catalyst Center Compatibility Matrix*.

Cisco platform support for Application Experience and Application Visibility in Catalyst Center		
Platform	**Data collection**	**Notes**
Cisco IOS XE Routers	Application Experience data collection.	• Requires an active NBAR2 license. • Cisco IOS XE 16.3 minimum software version. • For Optimized APM: Cisco IOS XE 17.3 minimum software version.

Cisco platform support for Application Experience and Application Visibility in Catalyst Center		
Platform	**Data collection**	**Notes**
Catalyst 9000 Series Switches	Application Visibility data collection for 9200, 9300, 9400.	• Requires an Advantage license. • Cisco IOS XE 16.10.1 minimum software version. • IP routing must be enabled.
Cisco C9350 Series Smart Switches	Application Visibility data collection for 9200, 9300, 9400.	• Requires an Advantage license. • Cisco IOS XE 26.1.1 minimum software version.
Cisco AireOS Wireless Controllers	Application Visibility data collection.	• Requires an Advantage license. • Requires 8.8 MR2 software version 8.8.114.130 or later.
Cisco 9800 Series Wireless Controller	Application Visibility data collection for Flex/Fabric SSIDs. Application Experience data collection for central switching/local SSIDs, and Flex/Fabric SSIDs.	• Application Visibility for Optimized APM: Cisco IOS XE 16.12.1 minimum software version. • Application Experience for local mode: Cisco IOS XE 16.12.1 minimum software version. For flex/fabric mode: Cisco IOS XE 17.10.1 minimum software version.
Catalyst Center Traffic Telemetry Appliance	Application Experience data collection.	• Requires an Advantage license. • For Optimized APM: Cisco IOS XE 17.3 minimum software version.

Criteria for enabling application telemetry on devices

Catalyst Center automatically enables application telemetry on all applicable interfaces or WLANs that are selected based on the new automatic interfaces or WLAN selection algorithm.

Note

- The conventional tagging-based algorithm is supported and has precedence over the newer automatic interfaces or WLAN selection algorithm.
- If you want to switch over from the automatic selection algorithm to the tagging-based algorithm, you must disable telemetry before provisioning the tagged SSIDs to the devices.
- Tagging-based algorithm applies to both greenfield and brownfield deployments.

This table provides the criteria for selecting interfaces and WLANs using both the conventional tagging-based algorithm (with **lan** keyword) and the new automatic selection algorithm for all the supported platforms.

Platform	Conventional tagging-based algorithm	Automatic selection algorithm

Router	• Interface description has the **lan** keyword.[1, 2]
	• Interface has an IP address other than the management IP address.
		• Interface has an IP address other than the management IP address.
		• Interface is not any of these types:
		  • WAN
		  Note An interface is treated as a WAN-facing interface if it has a public IP address, and if there is a route rule with a public IP address that routes through the interface.
		  In this context, a public IP address is not in a private range (for example, not in 192.168.x.x, 172.16.y.y, 10.z.z.z), or is an IP address that is not in the system's IP pools.
		  Route rules can be dynamically learned. In this context, the **show ip route** command does not show a route to a public IP address that goes through this interface.
		  • Loopback.
		  • Management interface: GIGABITETHERNET0, GIGABITETHERNET0/0, MGMT0, FASTETHERNET0, or FASTETHERNET1.

Switch	• Interface description has the **lan** keyword.[1, 2]
	• Switch port is configured as an access port.
	• Switch port is configured with the **switch-mode access** command.
		• Interface is a physical interface.
		• Access port does not have neighbors.
		• Interface is not any of these types:
		  • Management interface: FASTETHERNET0, FASTETHERNET1, GIGABITETHERNET0/0, or MGMT0
		  • LOOPBACK0, Bluetooth, App Gigabit, WPAN, Cellular, or Async
		  • VSL interface.

Platform	Conventional tagging-based algorithm	Automatic selection algorithm
Cisco AireOS Controller	WLAN profile name is tagged with the **lan** keyword.[1, 2]	If the SSIDs are mixed, that is Local mode, Flex mode, and Fabric mode, Wireless Service Assurance (WSA) processing is enabled. If all the SSIDs are in Local mode, NetFlow is enabled.
Cisco Catalyst 9800 Series Wireless Controller with Optimized Application Performance Monitoring (APM) profile and IOS 16.12.1 and later.	WLAN profile name is tagged with the **lan** keyword.[1, 2]	If the SSIDs are mixed—that is, central switching, Flex mode, and Fabric mode—the Cisco Application Visibility and Control (AVC) basic record is configured. If all the SSIDs use central switching, the Optimized APM record is configured. For Cisco Catalyst 9800 Series Wireless Controllers with IOS 17.10 and later, Catalyst Center pushes the APM profile, not the AVC basic profile, for flex and fabric SSIDs.
	Note NetFlow configurations are pushed to the policy profile with the "lan" keyword, not directly to the WLAN profile. In brownfield deployments, the workaround is to create a new policy profile with the "lan" keyword, delete the existing policy profile, and associate the new one with the existing WLAN profile. Renaming the policy profile directly is not supported.	
Catalyst Center Traffic Telemetry Appliance with Optimized APM profile and IOS 17.3 and later.	• Interface description has the **lan** keyword.[1, 2] • Interface is a physical interface.	• Interface is a physical interface. • Interface is not a management interface: GIGABITETHERNET0, GIGABITETHERNET0/0, MGMT0, FASTETHERNET0, and FASTETHERNET1.

[1] The **lan** keyword is case insensitive and can be separated by a space, hyphen, or underscore.
[2] Resynchronize the network device to read the **lan** keyword.

For example, to use the conventional tagging-based algorithm to enable application telemetry:

- the WLAN profile name *test-lan* on this Cisco Catalyst 9800 Series Wireless Controller includes the **lan** keyword

```
WLAN Profile Name               SSID                    VLAN Status
-------------------------------------------------------------------------------
1    test-lan                   test1-ssid              137   UP
```

- the interface description *wired-lan* on this switch includes the **lan** keyword

```
interface GigabitEthernet1/0/1
description wired-lan
```

Application health prerequisites

This topic provides the prerequisites relating to application health for routers, Cisco AireOS Wireless Controllers, and switches.

Application Experience prerequisites on routers

- Requires Cisco IOS XE software with an active NBAR2 license.
- Application flows within the Layer 3 network are not visible.
- Traffic associated with the management interface is not part of Application Experience.
- Ports cannot be enabled for ETA.
- Clocks must be synchronized between Catalyst Center and the device for Assurance to display Application Health data.
- The conventional tagging-based algorithm (with keyword **`lan`**) is supported, but the newer automatic interface or WLAN selection algorithm allows you to enable Application Telemetry on interfaces or WLANs without tagging them with the keyword **`lan`**. For information about the criteria that is used, see Criteria for enabling application telemetry on devices, on page 159.

Application Visibility prerequisites on switches

- Requires Cisco IOS XE software.
- Requires an Advantage license.
- Implemented only on access ports that contain the command **`switchport mode access`**.
- Support for L2 logical interfaces is not available.
- Limited visibility if the switch port is connected to an AP and configured with **`switchport mode access`**.
- Ports cannot be enabled for ETA.
- Only IPv4 flows are monitored.
- These management interfaces cannot be used as a source interface of a NetFlow export:
  - GIGABITETHERNET0/0
  - MGMT0
  - FASTETHERNET0
  - FASTETHERNET1
  - GIGABITETHERNET0
- Clocks must be synchronized between Catalyst Center and the device for Assurance to display Application Health data.
- The conventional tagging-based algorithm (with keyword **`lan`**) is supported, but the newer automatic interface or WLAN selection algorithm allows you to enable Application Telemetry on interfaces or WLANs without tagging them with the keyword **`lan`**. For information about the criteria that is used, see Criteria for enabling application telemetry on devices, on page 159.

Application Visibility prerequisites on AireOS Wireless Controllers

- Requires an Advantage license.

- Supported only on wireless controllers that have AireOS software and not on wireless controllers that have IOS XE software.
- NetFlow must be enabled on the Cisco AireOS Wireless Controllers.
- Clocks must be synchronized between Catalyst Center and the device for Assurance to display Application Health data.
- Flexible NetFlow (FNF) flow monitors are not implemented. Instead, Application Visibility data is collected using streaming telemetry by subscribing to the Client-app-stat-events channel.
- The conventional tagging-based algorithm (with keyword **`lan`**) is supported, but the newer automatic interface or WLAN selection algorithm allows you to enable Application Telemetry on interfaces or WLANs without tagging them with the keyword **`lan`**. For information about the criteria that is used, see Criteria for enabling application telemetry on devices, on page 159.

Application Visibility prerequisites on Cisco 9800 Series Wireless Controller

- Requires IOS XE software for Optimized APM. See Criteria for enabling application telemetry on devices, on page 159.
- Clocks must be synchronized between Catalyst Center and the device for Assurance to display Application Health data.

Application Experience prerequisites on traffic telemetry appliance

- Requires an Advantage license.
- Requires IOS XE software for Optimized APM. See Criteria for enabling application telemetry on devices, on page 159.
- Clocks must be synchronized between Catalyst Center and the device for Assurance to display Application Health data.
- To enable visibility of CAPWAP-encapsulated wireless traffic, manually enter the **ip nbar classification tunneled-traffic CAPWAP** command on the appliance.

Provision application telemetry settings

You can configure NetFlow application telemetry settings on the device.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The Inventory window displays the device information gathered during the discovery process. To view devices available in a particular site, expand the Global site in the left pane and select the site, building, or floor.

Step 2 Select the devices that you want to provision.

Step 3 From the **Actions** drop-down list, select **Telemetry** and do one of these steps:

Note
The **Enable Application Telemetry** and **Disable Application Telemetry** options are enabled only when the device supports application telemetry from Catalyst Center.

a) **Enable Application Telemetry**: To configure NetFlow application telemetry for the selected devices.
b) **Disable Application Telemetry**: To remove the NetFlow application telemetry configuration from the chosen devices.

Step 4 Click **Apply**.

The **Application Telemetry** column shows the telemetry configuration status. If you don't see the **Application Telemetry** column in the default column setting, click the ellipsis icon (⋮) at the right end of the column headings and check the **Application Telemetry** check box.

View Application Experience of a host

Use this procedure to view the qualitative and quantitative metrics of the applications running on a host.

Before you begin

- Make sure that the devices (routers, switches, wireless controllers, and access points) are discovered. See Discover your network using an IP address range or CIDR, on page 24, Discover your network using CDP, on page 21, or Discover your network using LLDP, on page 26.
- Enable and configure Application Telemetry profile on network devices. See Provision application telemetry settings, on page 163.
- See Application health prerequisites, on page 161.

Procedure

Step 1 From the **Client 360** window, expand the **Application Experience** category.

Step 2 From the **Application Experience** category, you can do these steps:

a) View the Application Experience data in table format from a specific business relevance group by clicking its corresponding tab. The tabs are: **Business Relevant**.

Note
The displayed data is based on the time you selected from the drop-down menu in the **Client 360** window. Options are: **3 Hours**, **24 Hours**, and **7 Days**. Default is **24 Hours**.

b) View Application Experience data in the table.

- **Name**: The application name.
- **Health**: The health score is calculated on the basis of a combination of metrics of packet loss, latency, and jitter. You can also include application delay for health score calculation. For more information, see Individual application health score, on page 190.
- **Usage Bytes**: The number of bytes transferred by the client for this application.

- **Average Throughput**: The rate of the application traffic (in Mbps) flowing between the client and the server.
- **DSCP**: The application's current (**Observed**) and default (**Expected**) DSCP value.

  Note
  This metric is not available for Optimized APM.

- **Packet Loss**: The percentage (maximum and average) of packet loss.
- **Network Latency**: The network latency time (maximum and average) in milliseconds.
- **Jitter**: The variance in time delay in milliseconds (maximum and average) between data packets over your network.

c) To view the Application Experience metrics in chart format, click the radio button next to an application. The metrics are: **Throughput**, **Packet Loss**, **Jitter**, **Network Latency**, **Client Network Latency**, **Server Network Latency**, and **Application Server Latency**.

Note
Application Visibility data that is exported by a Cisco Catalyst 9200 switch, Cisco Catalyst 9300 switch, or a Cisco AireOS wireless controller only provides data for Application Name, Usage, and Throughput.

View Application Experience of a network device

Use this procedure to view the qualitative and quantitative metrics of the applications running on a network device.

Before you begin

- Make sure that the devices (routers, switches, wireless controllers, and access points) are discovered. See Discover your network using an IP address range or CIDR, on page 24, Discover your network using CDP, on page 21, or Discover your network using LLDP, on page 26.
- Enable and configure Application Telemetry profile on network devices. See Provision application telemetry settings, on page 163.
- See Application health prerequisites, on page 161.

Procedure

Step 1 From the **Device 360** window, expand the **Application Experience** category.

Step 2 From the **Application Experience** category, you can do these steps:

a) The **Netflow Exporter Summary** displays the number of netflow packet count, data-record count, packet drops, record drops, and total bytes.

b) View the Application Experience data in table format from a specific business relevance group by clicking its corresponding tab: **Business Relevant**, **Business Irrelevant**, or **Default**.

Note

The displayed data is based on the time you selected from the drop-down menu in the **Device 360** window. Options are **3 Hours**, **24 Hours** (the default), and **7 Days**.

c) Filter the Application Experience data for a specific VRF or a specific router interface by using the appropriate filters: **All VRFs** and **All Interfaces**.

Note
The **All VRFs** and **All Interfaces** filters are only available for routers.

d) View Application Experience data in the table:

- **Name**: The application name.
- **Health**: The health score is calculated on the basis of a combination of metrics of packet loss, latency, and jitter. You can also include application delay for health score calculation.

  Note
  The health score is not available for Cisco Catalyst 9000 Series Switches and Cisco AireOS wireless controller. These devices do *not* poll the KPIs that are required to calculate a health score.

- **Usage Bytes**: The number of bytes transferred by the client for this application.
- **Average Throughput**: The rate of the application traffic (in Mbps) flowing between the client and the server.
- **DSCP**: The application's current (**Observed**) and default (**Expected**) DSCP value.

  Note
  This metric is not available for Optimized APM.

- **Packet Loss**: The percentage (maximum and average) of packet loss.
- **Network Latency**: The network latency time (maximum and average) in milliseconds.
- **Jitter**: The variance in time delay in milliseconds (maximum and average) between data packets over your network.

e) To view the Application Experience metrics in chart format, click the radio button next to an application. The metrics are **Throughput**, **Packet Loss**, **Jitter**, **Network Latency**, **Client Network Latency**, **Server Network Latency**, **Application Server Latency**, and **Application Response Time**.

Note
Application Visibility data that is exported by a Cisco Catalyst 9200 switch, Cisco Catalyst 9300 switch, or a Cisco AireOS wireless controller only provides data for Application Name, Usage, and Throughput.

Monitor the health of all applications

Use this procedure to get a global view of applications at a site.

Before you begin

- Make sure that the devices (routers, switches, wireless controllers, and access points) are discovered. See Discover your network using an IP address range or CIDR, on page 24, Discover your network using CDP, on page 21, or Discover your network using LLDP, on page 26.
- Enable and configure the Application Telemetry profile on network devices. See Provision application telemetry settings, on page 163.
- See Application health prerequisites, on page 161.

Procedure

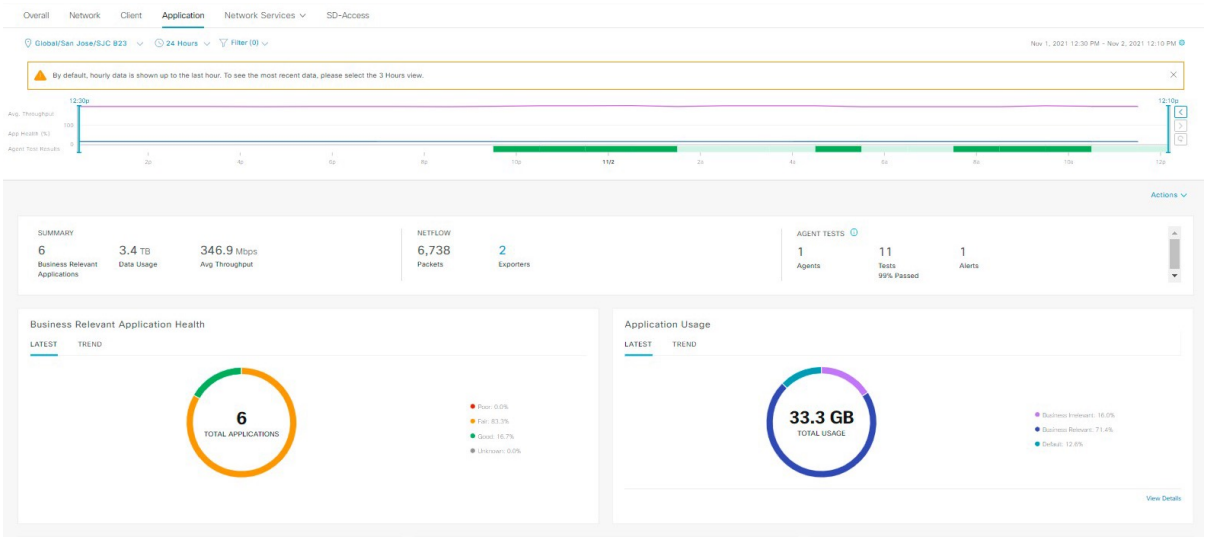
Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Application** tab.

The **Application** health dashboard appears.

Figure 17: Application Health Dashboard



Step 3 Use the **Application** health dashboard top-menu bar for this functionality:

Application Health Dashboard Top-Menu Bar	
Item	**Description**
Global **Location** drop-down list	Click to display the location icon. Click the location icon to display the **Site List View**. To view the application information from a specific site or building, click **Go to Site** in the appropriate row. The information is refreshed in the dashboard based on your selection.

Application Health Dashboard Top-Menu Bar	
Item	**Description**
 **Time Range** setting	Enables you to display data within a specified time range on the dashboard. Do these steps: **a.** From the drop-down menu, select the length of the range: **3 Hours**, **24 Hours**, or **7 Days**. **b.** Specify the **Start Date** and time; and the **End Date** and time. **c.** Click **Apply**.
Filter	Select the SSID from the drop-down list and then click **Apply**. Depending on your selection, the information in the dashboard is refreshed.
Actions drop-down list	Enables you to customize the dashboard display when you select **Edit Dashboards** from the drop-down list. See Change the position of a dashlet, on page 349 and Create a custom dashboard, on page 347.
Application Health Timeline Slider	Enables you to view the healthy business-relevant application percentage, throughput, and agent test result for a more granular time range. Hover your cursor within the timeline to view the health score percentage at a specific time. You can click and drag the timeline boundary lines to specify the time range. This sets the context for application data that is displayed in the dashboard dashlets. You can use the arrow buttons on the right of the timeline to view data for up to 30 days.

Step 4 Use the **Summary** dashlet for this functionality:

Summary Dashlet	
Item	**Description**
Summary	Displays the total number of business-relevant applications, data usage, and average throughput in your overall network, or selected site.

Summary Dashlet	
Item	**Description**
ThousandEyes Tests	Displays the total number of ThousandEyes enterprise agents, tests, and active alerts running on your supported Cisco Catalyst 9300 or 9400 Series switch. These types of ThousandEyes agent tests are supported: • Network agent-to-server test: Collects network data, including jitter, packet loss, and latency. • Web HTTP server test: Collects HTTP server data, including response time. • Network agent-to-agent test: Collects network data, including jitter, packet loss and latency. • Voice RTP test: Collects Mean Opinion Score (MOS), packet loss, latency and Packet Delay Variation (PDV). To configure ThousandEyes Integration, see *Configure ThousandEyes Integration* in the *Cisco Catalyst Center Administrator Guide*.

Step 5 Use the **Application Health** dashlet for this functionality:

Application Health dashlet	
Item	**Description**

Business Relevant Application Health	Contains a health score for business-relevant applications. The health score is the percentage of healthy (good) business-relevant applications in your overall network, or selected site. See Understand application health score and KPI metrics, on page 189.
	Click **LATEST** and **TREND** tabs to view the business relevant application health by their health score.
	These charts appear:
	• Circle chart that shows the count of business-relevant applications categorized by the application's health score. You can click a category to show the list of applications with the lowest health score within the category.
	• Application count distribution trend chart that shows the count of all business-relevant applications over time, which is shown as a stacked area chart based on their health scores.
	• Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can:
	  • Click a specific health category in the chart to filter the application list and it displays the detailed information in the **Application** table
	  • Click a category in the chart to display the applications and its detailed information in the **Application** table.

Application Health dashlet	
Item	**Description**
Application Usage	Click **Latest** to display the total application usage categorized by the application's business-relevance group (Business Relevant, Business Irrelevant, and Default). You can click a category to show the list of the top 10 applications by usage within the category. Click **Trend** to display a stacked area graph showing how bandwidth usage percentages for each category have changed over a 24-hour period. **Note** The application usage is taken from the application's bidirectional traffic. • From the **Trend** tab, click **View Details** to open a slide-in pane that shows All Applications by Application Usage with the latest and trend tabs in the chart. From the slide-in pane, you can: • Click the **All Applications**, **Business Relevant**, **Business Irrelevant**, and **Default** tabs to display a chart with its application usage and the top 10 applications by usage. • Use the **Breakdown by** drop-down list at the top right to filter the chart by **Application Group** or **Traffic Class**. • Click a specific application in the chart to filter the application and its detailed information in the **Application** table, including Name, Health, Business Relevance, Usage, Average Throughput, Packet Loss, Latency, and Jitter.
Top Applications by Throughput	Click **LATEST** and **TREND** tabs to view the top 5 applications by their average throughput values. Each application name is clickable and redirects to the relevant Application 360 page. • Click **View Details** to open a slide-in pane that shows the Top Applications by Throughput chart with the latest and trend tabs. From the slide-in pane, you can: • Click a specific application in the chart to filter the top application by throughput and its detailed information in the application table, including Name, Health, Business Relevance, Usage, Average Throughput, Packet Loss, Latency, and Jitter.
Top Endpoints by Throughput	Click **LATEST** and **TREND** tabs to view the top 5 endpoints by their average throughput values. Each endpoint identifier (IP address) is clickable and redirects to the relevant Client 360 page. • Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can: • Click a specific endpoints/bar in the chart to filter the top endpoints by throughput and its detailed information in the Client Devices table, including Identifier, , IP Address, Device Type, Health, Location, Last Seen, Switch and VLAN ID.

Application Health dashlet	
Item	**Description**
Worst Applications	Click **LATEST** and **TREND** tabs to view the worst 5 application by their health score. Use the drop-down menu to filter the applications by specific performance criteria, such as **Health Score**, **Jitter**, **Packet Loss**, **Client Network Delay**, **Server Network Delay**, or **Application Delay**. Each application name is clickable and redirects to the relevant Application 360 page. • Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can: • Click a specific application in the chart to filter the top endpoints by worst applications and its detailed information in the application table, including Name, Health, Business Relevance, Usage, Average Throughput, Packet Loss, Latency, and Jitter. **View Details**: Click **View Details** to open a slide-in pane with additional details about the worst applications by different health KPIs, such as packet loss and jitter.

Step 6 Use the **Application** dashlet for this functionality:

Application dashlet	
Item	**Description**
Type	Filter the table based on the business-relevance groups. Options are **Business Relevant**, **Business Irrelevant**, **Default**, and **All**.
Health	Filter the table based on the application's health scores. Options are: • **Poor**: Applications with a health score range from 1 to 3. • **Fair**: Applications with a health score range from 4 to 7. • **Good**: Applications with a health score range from 8 to 10. • **All**: All applications. • **Unknown**: Applications are missing qualitative metrics for determining a health score.

Application dashlet	
Item	**Description**
Application table	View detailed application information in a table format. The application table displays this information by default: • **Name**: Displays the application name. The names are based on the standard applications from Cisco Next Generation Network-Based Application Recognition (NBAR). Changing an application's name with the Application Policy package does not show the changed name in Application Experience. There is no integration between the Application Policy package and Application Experience. • If an application is not a standard application from the NBAR, its HTTP hostname or SSL common name is displayed, if available. These applications are assigned to the **Default** business-relevance group. You can click the name to display a 360° view of an application. See Monitor the health of an application, on page 178. • The application table lists new applications: **ms-teams-video**, **ms-teams-app-sharing**, **ms-teams-audio**, **ms-teams-media** and **ms-teams** applications are grouped under **microsoft-teams**, which collects the relevant data. Click **microsoft-teams** to display an MS Teams 360 view of Microsoft Teams applications. See Monitor and troubleshoot the health of a Microsoft Teams application, on page 185. webex-video, webex-audio, and webex-app-sharing are grouped under **webex**, which collects the relevant data. Click **webex** to display a Webex 360 view of Webex applications. See Monitor and troubleshoot health of a Webex application, on page 182. • **Health**: Displays the health score of the application. • **Business Relevance**: Possible values are **All**, **Business Relevant**, **Business Irrelevant**, and **Default**. • **Usage**: The number of bytes transferred for this application. • **Average Throughput**: The rate of application traffic (in Mbps) flowing between the client and server. • **Packet Loss (%)**: The percentage of packet loss. • **Network Latency**: The network latency time, in milliseconds, for Transmission Control Protocol (TCP)-based applications. • **Jitter**: The variance in time delay in milliseconds between data packets over your network. Jitter is for Real-time Transport Protocol (RTP)-based applications.

Application dashlet	
Item	**Description**
	Customize the data that you want displayed in the table: **a.** From the **Table Appearance** tab, set the table density and striping. **b.** From the **Edit Table Columns** tab, check the check boxes for the data you want displayed in the table. **c.** Click **Apply**.
	Click **Export** to export the table data to a CSV file.

Step 7 Use the **ThousandEyes Enterprise Agent Tests** dashlet for this functionality:

ThousandEyes Enterprise Agent Tests	
Item	**Description**
Enterprise Agent Tests table	View detailed **ThousandEyes Enterprise Agent Tests** information in a table format. The agent table displays these details: • **Test Name**: Displays the enterprise agent test name. Click the name to go to the ThousandEyes Agent page. • **Test Type**: Displays the name of the test type. • **Target**: Displays the target server used for the agent test. • **Device Name**: Displays the device name. • **Average Packet Loss (%)**: The average percentage of packet loss during data collection between agents and servers. • **Average Jitter**: The variance in time delay in milliseconds between data packets over your network. Jitter is for RTP-based applications. • **Average Latency**: The network latency time, in milliseconds, for TCP-based applications. • **# of Active Alerts**: Displays the number of active alerts during the agent test. • **# of Alerts**: Displays the total number of alerts during the agent test. • **# of Failed Tests**: Displays the number of failed agent tests. • **MOS**: Displays average and latest of mean opinion score. • **PDV (ms)**: Displays average and latest score of packet delay variation.
Install Agents	Click **Install Agents** to install the ThousandEyes Enterprise Agents. Cisco Catalyst 9000 series switches (such as the Catalyst 9300 and 9400) support running ThousandEyes Enterprise Agents as an application directly on the switch. See Install ThousandEyes Enterprise Agents, on page 174.

ThousandEyes Enterprise Agent Tests	
Item	**Description**
Manage Agents	Click **Manage Agents** to manage all the installed enterprise agents and perform uninstall, upgrade, start, stop, resync, assign Test, or add new test in the manage agents window. You can view global agent stats such as running, stopped, failed, and in progress agents. See Manage enterprise agents and tests, on page 176.
	Customize the data that you want displayed in the table: **a.** From the **Table Appearance** tab, set the table density and striping. **b.** From the **Edit Table Columns** tab, check the check boxes for the data you want displayed in the table. **c.** Click **Apply**.
	Click **Export** to export the table data to a CSV file.

Install ThousandEyes Enterprise Agents

Use this procedure to install the ThousandEyes Enterprise agents onto Catalyst 9300 and 9400 series switches and IE3500 and IE9300 series switches. If you have installed agents previously, you can manage agents and add tests to run on them.

Catalyst Center supports ThousandEyes multivariant app packages across CPU architectures. For ThousandEyes, Catalyst Center can recognize architecture-specific variants of the same app family, such as x86_64 and aarch64. It automatically resolve the right variant per device during install or upgrade and provides variant-aware life cycle operations.

Before you begin

- Ensure that the ThousandEyes agent account is connected to Catalyst Center. For more information, see *Configure ThousandEyes Integration* in the Cisco Catalyst Center Administrator Guide.

Procedure

Step 1 In the **Connect ThousandEyes** window, choose the ThousandEyes Account Group from the **Thousand Eyes Account Group** drop-down list and click **Next**.

Step 2 In the **Select Applications** window, select the application for which you want to install the agents and do enhanced application monitoring from these options:

- Microsoft 365
- Slack
- Webex

- Salesforce
- Zoom
- AWS Console
- Custom Application.

Step 3 In the **Configure Application** window, you can configure the application based on the application you selected.

If you chose	Then
Microsoft 365	Configure these microsoft 365 parameters and tests: • **Subdomain name** - Enter the Microsoft 365 subdomain name. • **Test interval** - Select the test interval from the **Test interval** drop-down list. The test interval values are 1 minute, 2 minutes, 5 minutes, 10 minutes, 15 minutes, 30 minutes, and 1 hour. • To select the tests to be added, check the **Test included** check box. The available tests are **M365 - OneDrive Web**, **M365 - Login Web**, **M365 - App Portal Web**, **M365 - Sharepoint Web**, **M365 - Outlook Web**. You must configure at least one test to run the test on the application.
Slack	Configure these Slack parameters and tests: • **Subdomain name** - Enter the Slack subdomain name. • **Test interval** - Select the test interval from the **Test interval** drop-down list. The test interval values are 1 minute, 2 minutes, 5 minutes, 10 minutes, 15 minutes, 30 minutes, and 1 hour. • To add a test, check the **Test included** check box. The available tests are **Slack - Web**, and **Slack - api.slack.com**. You must configure at least one test to run the test on the application.
Webex	Configure these Webex parameters and tests: • **Webex site ID** - Enter the Webex site ID. • **Test interval** - Select the test interval from the **Test interval** drop-down list. The test interval values are 1 minute, 2 minutes, 5 minutes, 10minutes, 15 minutes, 30 minutes, and 1 hour. • To add a test check the **Test included** check box. The available test is **Webex - Server**. You must configure at least one test to run the test on the application.
Salesforce	Configure these Salesforce parameters and tests: • **Subdomain name** - Enter the salesforce subdomain name. • **Test interval** - Select the test interval from the **Test interval** drop-down list. The test interval values are 1 minute, 2 minutes, 5 minutes, 10 minutes, 15 minutes, 30 minutes, and 1 hour. • To add a test, check the **Test included** check box. The available tests are **Salesforce - Classic**, **Salesforce - Lighting**, **Salesforce - Login**, **Salesforce - Files**, and **Salesforce - Static Assets**. You must configure at least one test to run the test on the application.

If you chose	Then
Zoom	Configure these Zoom parameters and tests: • **Subdomain name** - Enter the Zoom subdomain name. • **Test interval** - Select the test interval from the **Test interval** drop-down list. The test interval values are 1 minute, 2 minutes, 5 minutes, 10 minutes, 15 minutes, 30 minutes, and 1 hour. • To add a test, check the **Test included** check box. The available test is **Zoom - Web** You must configure at least one test to run the test on the application.
AWS Console	Configure these AWS console parameters and tests: • **Template** - Enter the AWS template name. • **Test interval** - Select the test interval from the **Test interval** drop-down list. The test interval values are 1 minute, 2 minutes, 5 minutes, 10 minutes, 15 minutes, 30 minutes, and 1 hour. • To add a test, check the **Test included** check box. The available test is **AWS - Web** You must configure at least one test to run the test on the application.
Custom Application	Configure the custom application parameters and tests: • **Target domain** - Enter the target domain url or IP address. • **Target port** - Enter the target port number. • **Test interval** - Select the test interval from the **Test interval** drop-down list. The test interval values are 1 minute, 2 minutes, 5 minutes, 10 minutes, 15 minutes, 30 minutes, and 1 hour. • **Template name** - Enter the AWS template name. • To add a test, check the **Test included** check box. The available test is **Custom application - Network** You must configure at least one test to run the test on the application. You can create a maximum of 10 custom applications.

Or

(Optional) If you want to skip setting up an application, select **Continue without an application** and click **Next**.

Step 4 In the **Select Locations** window, select the location from the location drop-down list and click **Next.**

Step 5 In the **Select Switches**, select the switch and configure the **switch configuration**, and **proxy settings**.

Step 6 In the **Summary** window, review the application monitoring settings and click **Complete setup**.

What to do next

You can now manage the enterprise agents and tests. See Manage Enterprise Agents and Tests.

Manage enterprise agents and tests

Use this procedure to manage all installed enterprise agents. You can uninstall, upgrade, start, stop, resync, assign test, or add new test on the manage agents page.

Before you begin

Ensure that you have installed ThousandEyes Enterprise agents and tests. To install agents and add tests, see Install ThousandEyes Enterprise Agents, on page 174.

Procedure

Step 1 From the Catalyst Center home page, click the **Assurance** tab, and then choose **Health** > **Applications**.

The **Applications** page appears.

Step 2 From the **ThousandEyes Enterprise Agent Tests** table, click **Manage Agents**. The **ThousandEyes Integration Enterprise Agents** window appears. You can view only the switches and hubs where ThousandEyes is deployed.

The Global agent stats area displays the status of the running, stopped, failed, and in progress agents in the **All Agents** table.

Step 3 Use the **Search Hierarchy** search field or the filter icon to find a site, building, or area to view the agent and test information.

Step 4 Use the **Enterprise Agents** page to view this information:

Enterprise agents	
Item	**Description**
Global agent stats	Displays the number of running, stopped, failed, and in progress agents in the application.

All Agents table	Displays the agent's status, hostname, tests, test type and so on.
	• From the **All Agents** table, check the check box to select the agent name and do these tasks:
	  • Uninstall
	  • Upgrade
	  • Start
	  • Stop
	  • Resync
	  • Assign Test
	  • Add New Test
	• In the **All Agents** table, click on the host name to open a slide-in pane, agents details tab displays the agents data such as resources, network and docker run time options. To download technical supports logs, click **Tech Support Logs**
	• Click **Tests** tab in the slide-in pane to view the test name, test type and interval and target values assigned to the added to the agent. To detach the tests from agent, check the check box near the test name column and click **Detach from this agent**.

Step 5 To upgrade an agent:

a) In the **All Agents** list, select the check box next to the agent(s) you want to upgrade.
b) Click **Upgrade**. The **Agent(s) Upgrade** slide-in pane appears.
c) Configure proxy settings by selecting the proxy type from the **Proxy type** drop down:

- **Direct**: No additional configuration is required.
- **Static**: Enter the **Proxy location** and **Proxy bypass list**, and select the **Proxy Auth type** if required.
- **PAC**: Enter the **PAC File URL** and select the **Proxy Auth type** if required.
- (Optional) To customize Docker runtime options, toggle the **Upgrade with below docker runtime options** switch to the "on" position and enter the required configurations in the **Additional Docker runtime options** field.
- Click **Upgrade** to initiate the process. Monitor the **Status** column to verify that the agent successfully transitions to the updated version.

Monitor the health of an application

Use this procedure to view details about a specific application.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Application** tab.

The **Application** health dashboard appears.

Step 3 In the **Application** table, click the name of an application.

The **Application 360** window appears, which provides a 360° view of the application.

Step 4 Click the time range setting ( ) at the top-left corner to specify the time range for the data that you want displayed on the window:

a) From the drop-down menu, select a time range: **3 hours**, **24 hours**, or **7 days**.
b) Specify the **Start Date** and time; and the **End Date** and time.
c) Click **Apply**.

Step 5 To display application information for a particular location, select the location from the *Location* drop-down list.

Step 6 From the **Filter** drop-down list, select the SSID and click **Apply** to display the information for a particular SSID.

Step 7 Use the application health timeline slider to view the application's health score for a more granular time range and to view the application quality information.

Hover your cursor within the timeline to view this information:

Health Score: The health score at a specific time is displayed. Metrics that are color-code in the Quality area contribute to the health score.

Quality: The Quality information area displays information about latency, jitter, and packet loss. For latency, these aspects of delay between the client and the application appear:

- LAN delay: The delay in milliseconds between the client and router.
- WAN delay: The delay in milliseconds between the router and server.
- Application delay: The delay in milliseconds between the server and the application.

Under Maintenance: When a device is under maintenance mode during the specific time period, the specific device name is displayed below the Under Maintenance banner.

You can click and drag the timeline boundary lines to specify the time range. This sets the context for the application data that is displayed in the Application 360 window.

Step 8 Use the **Application Details** area, below the timeline, to view this information:

Application details	
Item	**Description**
Health Score	The health score of an application is calculated based on the weighted average of the application's qualitative metrics, which include packet loss, network latency, and jitter. **Note** The health score is not available for Cisco Catalyst 9000 Series Switches and Cisco AireOS wireless controller. These devices do *not* poll the KPIs that are required to calculate a health score.
Time and Date range	Displays the time and date range for the data that is displayed in the **Application 360** window.
Business Relevance **Traffic Class** **Category**	Displays the application's Next Generation Network-Based Application Recognition (NBAR) classifying information.
Issues tab	Click to view the list of issues.
Exporters tab	Click to view the list of devices that send NetFlow traffic to Catalyst Center and other details.

Step 9 Click **Issues** to view this information:

Issues
Displays any issues that must be addressed. Issues are listed based on the timestamp. The most recent issue is listed first. Click an issue to open a slide-in pane to view the corresponding details, such as the description of the issue, impact, and suggested actions. From the slide-in pane, you can do these tasks: • To resolve an issue: **a.** From the drop-down list, select **Resolve**. **b.** To view the list of issues that have been resolved, click **Resolved Issues**. • To ignore an issue: **a.** From the drop-down list, select **Ignore**. **b.** Set the number of hours to ignore the issue on the slider. **c.** Click **Confirm**. **d.** To view the list of issues that have been ignored, click **Ignored Issues**. For information about the types of issues, see View and Manage Issues, on page 239.

Step 10 Click **Exporters** to view this information:

Exporters	
Item	**Description**
Device	Displays the list of devices that is sending NetFlow traffic to Catalyst Center such as router, switch, wireless controller, and appliance. **Note** This warning message appears for the device under maintenance mode during specific time range: The exporters with warning icon were in maintenance mode during the selected period of time.
Health Score	The last 5-minute health score. The health score is calculated on the basis of the application's qualitative metrics, which include packet loss, network latency, and jitter. **Note** The health score is not available for Cisco Catalyst 9000 Series Switches and Cisco AireOS wireless controller. These devices do *not* poll the KPIs that are required to calculate a health score.
Traffic Class	Displays the application's NBAR classifying information if available.
Go to Device 360	Click to open the **Device 360** window for a specific device.

Step 11 To view metric charts:

- For routers and appliances, click the exporter row to display charts (below the row) for these metrics: usage, average throughput, packet loss, jitter, and latency.
- For switches and wireless controllers, click the device name to open a slide-in pane to view charts for these metrics: usage and average throughput.

  You can also click **Device 360** in the slide-in pane to open the **Device 360** window for a specific device.

Metric charts	
Charts	**Description**
Usage	The number of bytes transferred by the client for the particular application.
Throughput	The rate of the application traffic (in Mbps) flowing between the client and the server.
Packet Loss	The percentage (maximum and average) of packet loss. **Note** This metric is not available for switches and wireless controllers.
Latency	The network latency time (maximum and average) in milliseconds. These latency charts are available: • Network Latency • Client Network Latency • Server Network Latency • Application Network Latency **Note** This metric is not available for switches and wireless controllers.
Jitter	The variance in time delay in milliseconds (maximum and average) between data packets over your network. **Note** This metric is not available for switches and wireless controllers.
DSCP	• **Observed**: The application's current DSCP value. • **Expected**: The default DSCP value assigned by NBAR. **Note** This metric is not available for Optimized APM.

Step 12 View the list of clients that are accessing the application in the **Application Endpoint** table (displayed after the metric charts).

Click the **Managed Clients** tab, if you want to view only the clients that are managed by Catalyst Center.

Details about each client is provided in the table, such as identifier (user ID, hostname, IP address, or MAC address, whichever is available in that order), client, client health, app health, usage, device type, MAC address, and VLAN ID.

For active clients, you can click the **Identifier** column to open the **Client 360** window.

You can view up to 100 clients in this table. To view additional clients, click **Show More**.

Monitor and troubleshoot health of a Webex application

Use this procedure to view details about a Webex application.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

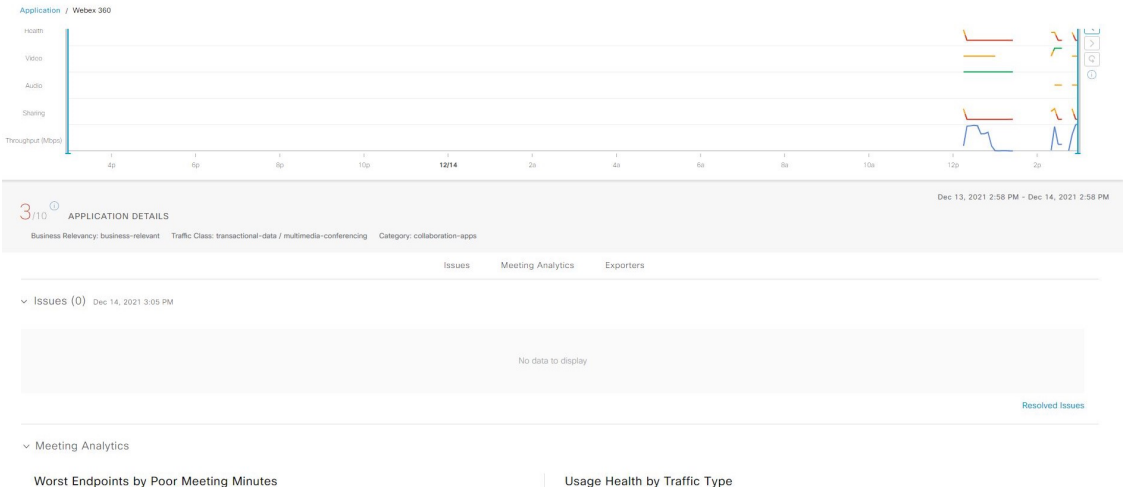
Step 2 Click the **Application** tab.

The **Application** health dashboard appears.

Step 3 In the **Application** table, click the **Webex** application.

The **Webex 360** window appears, which provides a 360° view of the application.

Figure 18: Webex 360 window



Step 4 Use the **Summary dashlet** to view the total number of data usage, average throughput, and active clients in your overall network, or selected site.

Step 5 Click the time range setting ( ) at the top-left corner to specify the time range for the application data that you want displayed on the window:

a) From the drop-down menu, select a time range: **3 hours**, **24 hours**, or **7 days**.

b) Specify the **Start Date** and time; and the **End Date** and time.

c) Click **Apply**.

Step 6 To display application information for a particular location, select the location from the *Location* drop-down list.

Step 7 Use the application health timeline slider to view the application's health score for a more granular time range, sub applications, the network quality and application quality information.

Hover your cursor within the timeline to view the health score at a specific time.

Step 8 Use the **Application Details** area, below the timeline, to view this information:

Application details	
Item	**Description**
Health Score	The health score of an application is calculated based on the weighted average of the application's qualitative metrics, which include packet loss, network latency, and jitter.
Time and Date range	Displays the time and date range for the data that is displayed in the **Webex 360** window.
Business Relevance **Traffic Class** **Category**	Displays the application's Next Generation Network-Based Application Recognition (NBAR) classifying information.
Issues category	Click to view the list of issues.
Meeting Analytics	Click to view the Meeting Analytics data.
Exporters tab	Click to view the list of devices that send NetFlow traffic to Catalyst Center and other details.

Step 9 You can view information about issues from the **Issues** category:

a) Click an issue to open a slide-in pane to view the corresponding details, such as description of the issue, impact, and suggested actions.

b) From the slide-in pane, you can do these tasks:

- To resolve an issue:
  1. From the **Status** drop-down list, select **Resolve**.
  2. Click **Resolved Issues** to view the list of issues that are resolved.
- To ignore an issue:
  1. From the **Status** drop-down list, select **Ignore**.
  2. Set the number of hours to ignore the issue on the slider.
  3. Click **Confirm**.

For information about issues, see View and Manage Issues, on page 239.

Step 10 Use the **Meeting Analytics** dashlets for this functionality:

Worst endpoints by poor meeting minutes
Click **Latest** and **Trend** chart to view the status of worst endpoints by poor meeting minutes. You can filter the data based on **By Percentage** or **By Total Poor Minutes**.

Usage health by traffic type
Click **Latest** to view the chart to view usage health based on the traffic type for Audio, Sharing, and Video. Click **Trend** to view the chart displays usage health based on the traffic type for Audio, Sharing, and Video. You can hover on a color segment in the chart to view the percentage of health.

Step 11 Click **Exporters** to view this information:

Exporters	
Item	**Description**
Device	Displays the list of devices that is sending NetFlow traffic to Catalyst Center such as router, switch, wireless controller, and appliance. **Note** This warning message appears for the device under maintenance mode during specific time range: The exporters with warning icon were in maintenance mode during the selected period of time.
Health Score	The last 5-minute health score. The health score is calculated on the basis of the application's qualitative metrics, which include packet loss, network latency, and jitter. **Note** The health score is not available for Cisco Catalyst 9000 Series Switches and Cisco AireOS wireless controller. These devices do *not* poll the KPIs that are required to calculate a health score.
Traffic Class	Displays the application's NBAR classifying information if available.
Go to Device 360	Click to open the **Device 360** window for a specific device.

Step 12 To view metric charts for audio, video and sharing:

Metric charts	
Charts	**Description**
Usage	The number of bytes transferred by the client for the particular application.
Throughput	The rate of the application traffic (in Mbps) flowing between the client and the server. You can hover your cursor over chart to view the throughput value for audio, video, and sharing.
Packet Loss	The percentage (maximum and average) of packet loss. **Note** This metric is not available for switches and wireless controllers.

Metric charts	
Charts	**Description**
Latency	The network latency time (maximum and average) in milliseconds. These latency charts are available: • Network Latency • Client Network Latency • Server Network Latency • Application Network Latency **Note** This metric is not available for switches and wireless controllers.
Jitter	The variance in time delay in milliseconds (maximum and average) between data packets over your network. **Note** This metric is not available for switches and wireless controllers.

Step 13 View the list of clients that are accessing the application in the **Application Endpoint** table (displayed after the metric charts).

Details about each client is provided in the table, such as identifier (user ID, hostname, IP address, or MAC address, whichever is available in that order), client, client health, app health, usage, device type, MAC address, and VLAN ID.

For active clients, you can click the **Identifier** column to open the **Client 360** window.

You can view up to 100 clients in this table. To view additional clients, click **Show More**.

Monitor and troubleshoot the health of a Microsoft Teams application

Use this procedure to view details about a **Microsoft Teams** application.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard is displayed.

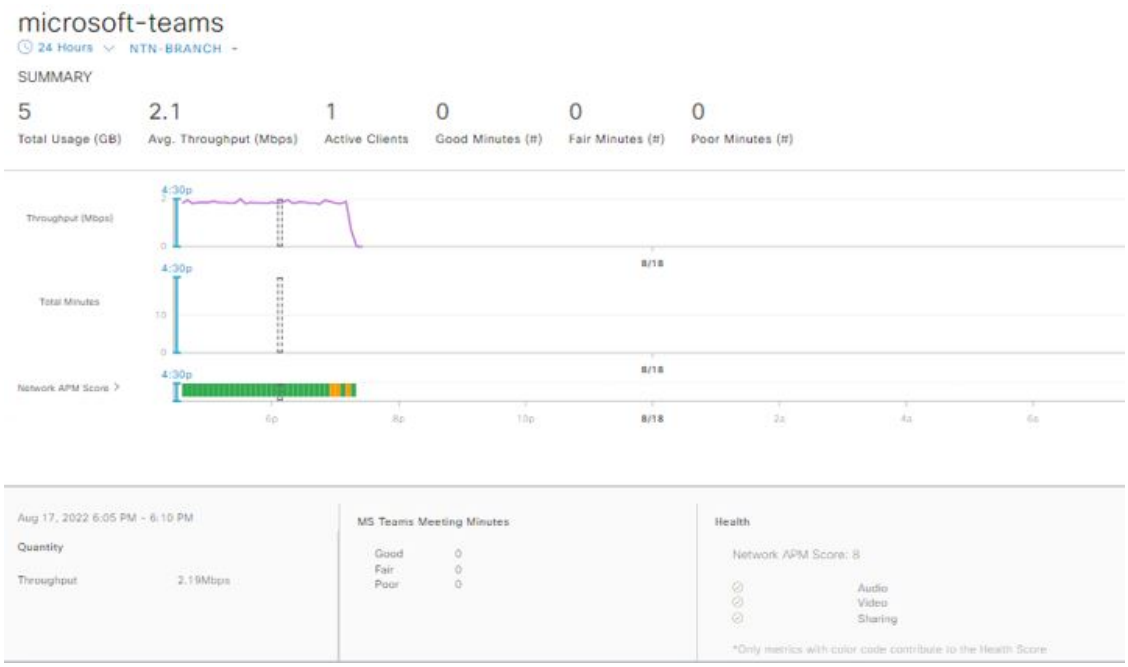
Step 2 Click the **Application** tab.

The **Application** health dashboard appears.

Step 3 In the **Application** table, click a **microsoft-teams** application.

An **MS Teams 360** window appears, which provides a 360° view of an application.

Figure 19: MS Teams 360 window



Step 4 Use the **Summary** dashlet to view the total number of data usage, average throughput, active clients, good minutes, fair minutes, and poor minutes in your overall network or selected site.

Step 5 In the top-left corner, click the time range setting ( ) to specify the time range for the application data that you want to be displayed on the window.

a) From the drop-down menu, select a time range: **3 hours**, **24 hours**, or **7 days**.
b) Specify the **Start Date** and time and the **End Date** and time.
c) Click **Apply**.

Note
By default, selected site and time range in the Application dashboard is displayed in an MS Teams 360.

Step 6 Use the application health timeline slider to view the **Throughput**, **Total Minutes**, and **Network APM Score**.

Hover your cursor in the timeline to view the health score at a specific time.

Note
Network APM score is a health score, which is calculated based on NetFlow exported from the managed network devices. For more information regarding APM, see Supported platforms, on page 158.

Step 7 Use the **Application Details** area, below the timeline, to view this information:

Application details	
Item	**Description**
Time and Date range	Displays the time and date range for the data that is displayed in the **MS Teams 360** window.
Health	Displays the health score of **Audio**, **Video**, and **Sharing**.
Quantity	Displays **Throughput** data.

Application details	
Item	**Description**
MS Teams Meeting Minutes	Displays information about **Good**, **Fair**, and **Poor** minutes.
Business Relevance **Traffic Class** **Category**	Displays the application's next generation Network-Based Application Recognition (NBAR) classifying information.
Issues category	Click to view the list of issues.
Meeting Analytics	Click to view the Meeting Analytics data.
Exporters tab	Click to view the list of devices that send NetFlow traffic to Catalyst Center and other details.

Step 8 You can view information about issues from the **Issues** category:

a) Click an issue to open a slide-in pane to view the corresponding details, such as a description of the issue, impact, and suggested actions.

b) From the slide-in pane, you can do these tasks:

- To resolve an issue:
  - **a.** From the **Status** drop-down list, select **Resolve**.
  - **b.** Click **Resolved Issues** to view the list of issues that are resolved.
- To ignore an issue:
  - **a.** From the **Status** drop-down list, select **Ignore**.
  - **b.** Set the number of hours to ignore the issue on the slider.
  - **c.** Click **Confirm**.

For information about issues, see View and Manage Issues, on page 239.

Step 9 Use the **Meeting Analytics** dashlets for this functionality:

Meeting analytics	
Item	**Description**
Top Access Devices	Click the **Latest** and **Trend** charts to view the status of top access devices by good and poor minutes. You can filter the data based on **By Poor Meeting Minutes**, **By Total Meeting Minutes**, **By Total Usage**, and **By Poor Network APM Score**.
Top Endpoints	Click the **Latest** and **Trend** charts to view the status of top endpoints by good and poor minutes. You can filter the data based on **By Poor Meeting Minutes**, **By Total Meeting Minutes**, **By Total Usage**, and **By Poor Network APM Score**.

Step 10 Click **Exporters** to view this information:

Exporters	
Item	**Description**
Device	Displays the devices that are sending NetFlow traffic to Catalyst Center. **Note** This warning message is displayed for the device under maintenance mode during a specific time range: The exporters with warning icon were in maintenance mode during the selected period of time.
Health Score	The last 5-minute health score. The health score is calculated based on the application's qualitative metrics, which include packet loss, network latency, and jitter. **Note** The health score is not available for Cisco Catalyst 9000 Series Switches and Cisco AireOS wireless controller. These devices do *not* poll the KPIs that are required to calculate a health score.
Traffic Class	Displays the application's NBAR classifying information, if available.

Step 11 To view metric charts for audio, video, and sharing:

Metric charts	
Charts	**Description**
Usage	The number of bytes transferred by the client for the particular application.
Throughput	The rate of the application traffic (in Mbps) flowing between the client and the server. You can hover your cursor over the chart to view the throughput value for audio, video, and sharing.
Packet Loss	The percentage (maximum and average) of packet loss. **Note** This metric is not available for switches and wireless controllers.
Jitter	The variance in time delay in milliseconds (maximum and average) between data packets over your network. **Note** This metric is not available for switches and wireless controllers.

Step 12 View the list of clients that are accessing the application in the **Application Endpoint** table (displayed after the metric charts).

The table shows details about each client, such as identifier (user ID, hostname, IP address, or MAC address), client health, Network APM score, Microsoft Teams Score, usage, device type, MAC address, and VLAN ID.

For active clients, click the **Identifier** column to open the **Client 360** window.

You can view up to 100 clients in this table. To view additional clients, click **Show More**.

Configure health score settings for applications

Use this procedure to configure the health score settings for applications. You can customize the health score calculation for applications by changing the KPI thresholds on a per-traffic class basis and specifying the KPIs that are included for the calculation.

Procedure

Step 1 From the main menu, choose **Assurance** > **Settings** > **Health Score Settings**.

Step 2 Click the **Application Health** tab.

Step 3 Click the tab of the application category to customize its health score calculation settings.

The tab displays the KPIs that affect the health score calculation of the application.

Step 4 From the **KPI Name** column, click the KPI name link.

The slide-in pane for the KPI appears.

Step 5 Configure the KPI health score settings:

a) Customize the KPI threshold value for **Poor**, **Fair**, and **Good** health score.
b) **Weight**: Valid weights are between 1–10. The higher the weight is, the KPI has more impact on the application health.
c) Check **Include for health score** check box if you want this KPI to be included in the health score calculation.
d) Click **Reset to Default** to restore the default KPI settings.

Step 6 Click **Apply**.

Understand application health score and KPI metrics

This section provides information about how the overall and individual application health scores and KPI metrics are computed.

Overall application health score

The application health score is the percentage of the number of healthy business-relevant applications (a health score from 8 to 10), divided by the total number of business relevant applications. The score is calculated over the latest 5-minute interval.

Example: 90% (health score) = 90 (business-relevant applications with a health score from 8 to 10) ÷ 100 (total number of business-relevant applications)

Individual application health score

The individual application health score is calculated based on the weighted average of the application's qualitative metrics, which include packet loss, network latency, and jitter.

The individual application health is measured on a scale of 1 to 10, with 10 being the best score. This formula is used to calculate the individual application health score:

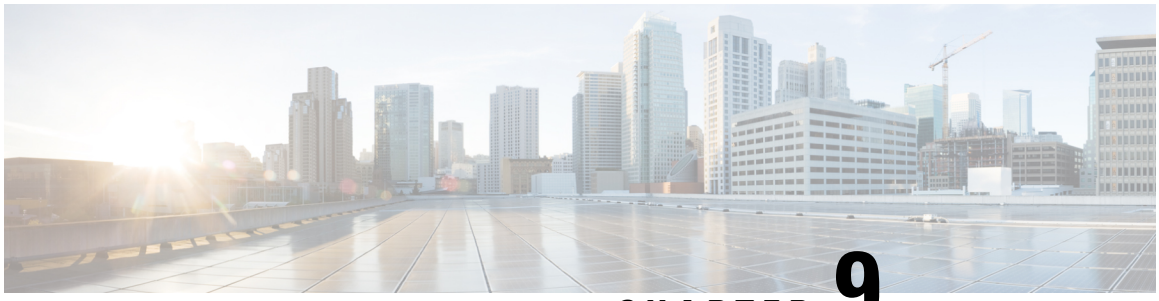
Individual application health score = (Latency_Weight * Latency_VoS_Score + Jitter_Weight * Jitter_VoS_Score + PacketLoss_Weight * PacketLoss_VoS_Score) ÷ (Latency_Weight + Jitter_Weight + PacketLoss_Weight)



Note The health score is not available for Cisco Catalyst 9000 Series Switches and Cisco AireOS Wireless Controller. These devices do *not* poll the KPIs that are required to calculate a health score.

The workflow for calculating the individual application health score includes:

1. Obtain the KPIs: Jitter, Latency, and Packet Loss.
2. Determine the application's Traffic Class based on the DSCP value from the flow record.
3. Convert the KPI numbers into Validation of Service score (VoS score) using the Cisco Validated Design (CVD) thresholds for each Traffic Class and KPI metric.
4. Get the weightage of the KPIs based on the application's Traffic Class and Tolerance level. The weightage is based on RFC4594.
5. Calculate the application health score. This is the weighted average of packet loss, network latency, and jitter.



CHAPTER 9

Monitor Network Services

- Monitor the AAA network service, on page 191
- Monitor the DHCP network service, on page 195
- Monitor the DNS network service, on page 198

Monitor the AAA network service

Use this procedure to view and monitor all AAA server transactions reported by wireless controllers and switches in your network.

Note **AAA Limitations**

- AAA network service supports wireless clients, wired clients, and Local mode.
- AAA network service does not support
  - Cisco AireOS Wireless Controllers,
  - Flex mode or fabric mode

Before you begin

Ensure that you have installed a Cisco Catalyst 9800 Series Wireless Controller with version 17.6.1 or later and deployed it with a local mode AP. Assurance supports site-based, role-based access control (SRBAC), which limits a user's scope of access to certain network sites. You must ensure you have access to the sites and devices, and associated AAA network services. For more information on user roles and permissions, refer to the Cisco Catalyst Center Administrator Guide.

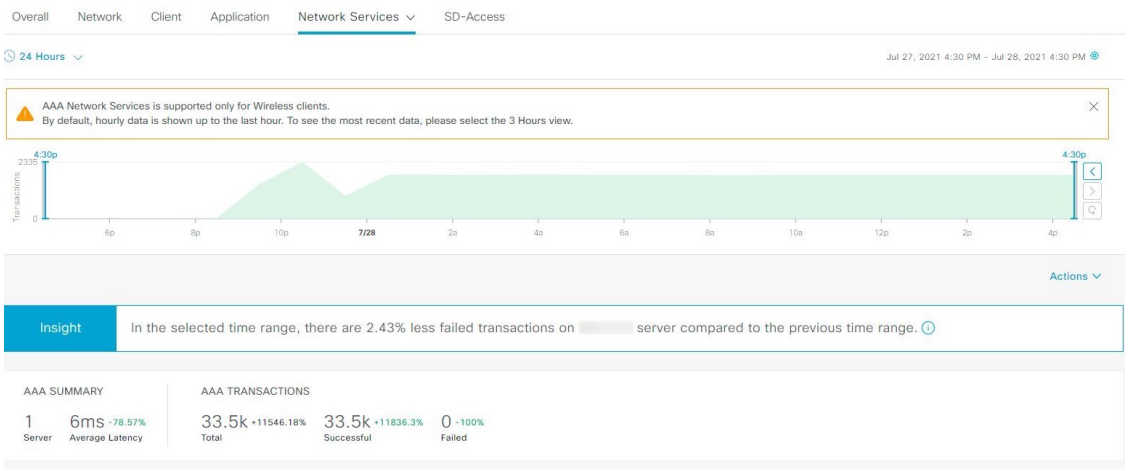
Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.
The **Overall** health dashboard appears.

Step 2 Choose **Network Services** > **AAA**.

The **AAA** dashboard appears.

Figure 20: AAA dashboard



Step 3 Click the time range setting ( ) at the top-left corner to specify the time range of the data that you want displayed:

a) From the drop-down menu, select a time range: **3 hours**, **24 hours**, or **7 days**.

b) Specify the **Start Date** and time and the **End Date** and time.

c) Click **Apply**.

Step 4 Click the autorefresh setting at the top-right corner to enable or disable the **Data Auto Refresh** on the supported Assurance pages in a 5-minute refresh interval.

Step 5 Use the timeline slider to view the information about the total successful and failed transactions of the AAA server over a period of time. The timeline slider has this functionality:

- Hover your cursor over the timeline slider to view the AAA server transactions for a 5-minute window.
- Double-click the timeline to move the timeline slider to a 1-hour time period. The entire window is refreshed, providing updates for that hour.

Step 6 Click the **Actions** drop-down list below the timeline slider for this functionality:

- **Edit Dashboard**: Customize the dashboard display. See Change the position of a dashlet, on page 349 and Create a custom dashboard, on page 347.

Step 7 Use the **Insight** area, below the timeline, to view the percentage of successful AAA server transactions compared with the current and previous time range.

Step 8 Use the AAA summary dashlet to view this information:

AAA summary	
Item	**Description**
AAA Summary	Displays the number of AAA servers and average latency (in ms) of your network.
AAA Transactions	Displays the percentage of total number of AAA transactions, successful transactions, and failed transactions in your network.

Step 9 Use the AAA server dashlets for this functionality:

Top sites by highest latency
The chart displays the top sites with the highest AAA server latency, in milliseconds. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can: • Hover your cursor over a site in the chart to view its location details and the corresponding highest AAA server latency. • Click a site in the chart to view the highest AAA server latencies and the top-affected data associated with these latencies in that site. • Click a data type category displayed as horizontal bars, such as the top AAA servers and sites, to filter the client table.

Top sites by transaction failures
The chart displays the top sites with the highest AAA server transaction failures. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can: • Hover your cursor over a site in the chart to view its location details and the corresponding transaction failure count. • Click a site in the chart to view its server transaction failures and the top-affected data associated with these failures. • Click a data type category displayed as horizontal bars, such as top AAA servers, Cisco ISE failures, or SSIDs, to filter the client table.

AAA server latency
The chart displays the average AAA latency for each AAA server. You can filter the latencies based on **All**, **MAB**, or **EAP**. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can: • Hover your cursor over the chart to view the server IP address and its corresponding average latency. • Click an area of the chart to view AAA server latencies and the top-affected data associated with these latencies. If the chart displays multiple servers, click the server IP address in the legend below to view details for that server. • Click a data type category displayed as horizontal bars, such as the top sites and SSIDs, to filter the client table. **Note** Information shown for the client list is based on the client's most recent activity and transactions.

AAA server transactions
The chart displays the average AAA server transaction status for each AAA server reported by wireless controllers and switches. You can filter the status based on **All**, **Failures**, or **Successes**. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can: • Hover your cursor over the chart to view the server IP address and its corresponding transaction count. • Click an area of the chart to view the AAA server transactions and the top-affected data associated with these transactions. If the chart displays multiple servers, click the server IP address in the legend below the chart to view details for that server. • Click a data type category displayed as horizontal bars, such as the top Cisco ISE failures or sites, to filter the client table.

Step 10 Use the AAA Servers by wireless controller and switches dashlets for this functionality:

AAA server by wireless controller and switches dashlet	
Item	**Description**
AAA Servers By Device table	View the AAA server information in a table format that contains AAA server IP address, device name, device location, device family(switch and wireless controller), transactions, failures, average latency, and so on. Click the AAA server IP address to open a slide-in pane that displays the AAA server average latency and transaction charts. From the slide-in pane, you can: • Hover your cursor over a chart to view more information. • Click an area of the chart to view the server latency and transactions details and the top-affected data associated with these transactions. • Click a data type category displayed as horizontal bars, such as the top Cisco ISE failures or sites, to filter the client table.
Export	Click **Export** to export the device information to a CSV file.
	Customize the data that you want displayed in the table: **a.** From the **Table Appearance** tab, set the table density and striping. **b.** From the **Edit Table Columns** tab, check the check boxes for the data that you want displayed in the table. **c.** Click **Apply**.

Monitor the DHCP network service

Use this procedure to view and monitor all the DHCP server transactions reported by wireless controllers and switches in your network.

Note **DHCP Limitations**

- DHCP network service supports wireless clients, wired clients, and local mode.
- DHCP network service does not support:
  - SD-Access fabric clients
  - AireOS Wireless Controller
  - Flex mode or fabric mode

Before you begin

- Ensure that you have installed a Cisco Catalyst 9800 Series wireless controller with version 17.6.1 or later.
- Ensure that you have installed a Cisco Catalyst 9000 IOS_XE Series Switches with version 26.01.02 or later.
- Assurance supports site-based, role-based access control (SRBAC), which limits a user's scope of access to certain network sites. You must ensure you have access to the sites and devices, and associated DHCP network services. For more information on user roles and permissions, see Cisco Catalyst Center Administrator Guide

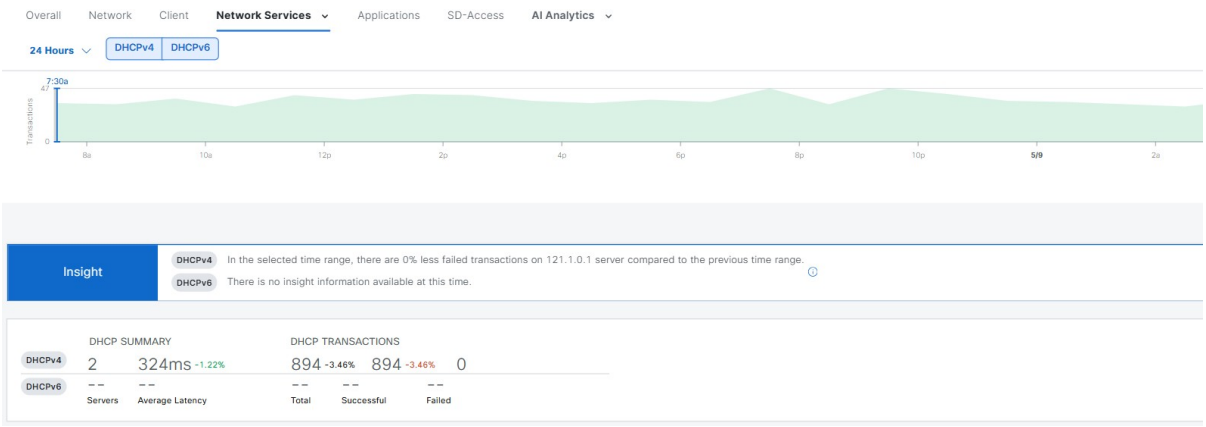
Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.
The **Overall** health dashboard appears.

Step 2 Choose **Network Services** > **DHCP**.

The **DHCP** dashboard appears.

Figure 21: DHCP dashboard



Step 3 Click the time range setting ( ) at the top-left corner to specify the time range of the data that you want displayed in the window:

a) From the drop-down menu, select a time range: **3 hours**, **24 hours**, or **7 days**.

b) Specify the **Start Date** and time and the **End Date** and time.

c) Click **Apply**.

Step 4 Choose the desired **DHCP** protocol (**DHCPv4** and/or **DHCPv6**) to filter the dashboard, which automatically refreshes the **Insight**, **DHCP Summary**, and **DHCP Transactions** sections to display metrics specific to your selection.

Step 5 Click the autorefresh setting at the top-right corner to enable or disable the **Data Auto Refresh** on the supported Assurance pages in a 5-minute refresh interval.

Step 6 Use the timeline slider to view the information about the total successful and failed transactions of the DHCP server over a period of time. The timeline slider has this functionality:

- You can hover your cursor over the timeline slider to view the DHCP server transactions for a 5-minute window.
- When you double-click the timeline, it brings the timeline slider to a 1-hour time period. The entire window is refreshed, providing updates for that hour.

Step 7 Click the **Actions** drop-down list below the timeline slider for this functionality:

- **Edit Dashboard**: Enables you to customize the dashboard display. See Change the position of a dashlet, on page 349 and Create a custom dashboard, on page 347.

Step 8 Use the **Insight** area below the timeline to view the percentage of successful DHCP server transactions compared with the current and previous time range.

Step 9 Use the DHCP summary dashlet to view this information:

DHCP summary	
Item	**Description**
DHCP 4 and DHCP 6 Summary	Displays the count of DHCP servers and average latency (in ms) of your network.
DHCP 4 and DHCP 6 Transactions	Displays the percentage of total number of DHCP transactions, successful transactions, and failed transactions in your network.

Step 10 Use the DHCP server dashlets for this functionality:

Top sites by highest latency
The chart displays the top sites with the highest DHCP server latency, in milliseconds. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can hover on a color segment in the chart to view the site with highest DHCP server latency. You can select the data displayed as horizontal bars to filter the client table based on the top DHCP servers, sites, SSIDs, and APs.

Top sites by transaction failures
The chart displays the top sites with the most DHCP server transaction failures. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can hover on a color segment in the chart or its corresponding legend to view the site with the most DHCP server transaction failures. You can select the data displayed as horizontal bars to filter the client table based on the top DHCP servers, sites, SSIDs, and APs.

DHCP server latency
The chart displays the average DHCP latency for each DHCP server. You can filter the latencies based on **All**, **Discover-offer**, or **Request-Ack**. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can: • Hover your cursor over the chart to view the server IP address and its corresponding average latency. • Click an area of the chart to view DHCP server latencies and the top-affected data associated with these latencies. If the chart displays multiple servers, click the server IP address in the legend below to view details for that server. • Click a data type category displayed as horizontal bars, such as the top sites and SSIDs, to filter the client table.

DHCP server transactions
The chart displays the average DHCP server transactions status for each DHCP server reported by wireless controllers. You can filter the status based on **All**, **Failures**, or **Successes**. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can: • Hover your cursor over the chart to view the server IP address and its corresponding transaction count. • Click an area of the chart to view the DHCP server transactions and the top-affected data associated with these transactions. If the chart displays multiple servers, click the server IP address in the legend below the chart to view details for that server. • Click a data type category displayed as horizontal bars, such as the top sites and SSIDs, to filter the client table.

Step 11 Use the DHCP servers by wireless controller and switches dashlets for this functionality:

DHCP server by wireless controller and switches dashlet	
Item	**Description**
DHCP Server table	View the DHCP server information in a table format that contains DHCP Server IP, Device Name, Device Location, Transactions, Failures, Avg Latency, and so on. Click **DHCP Server IP** to open the slide-in pane that display the Server Avg Latency and Transaction charts. You can select the data displayed as horizontal bars to filter the client table based on the top DHCP servers, sites, SSIDs, APs, and so on.
Export	Click **Export** to export the device information to a CSV file.
	Customize the data that you want displayed in the table: **a.** From the **Table Appearance** tab, set the table density and striping. **b.** From the **Edit Table Columns** tab, check the check boxes for the data you want displayed in the table. **c.** Click **Apply**.

Monitor the DNS network service

Use this procedure to monitor DNS server transactions reported by wireless controllers, switches, and routers in your network.

Note **DNS Limitations**

- DNS network service is only supported for Local mode or Central mode APs. It is not supported for Flex mode APs or APs in fabric mode. DHCP network service supports wireless clients, wired clients, and local mode.
- The UI doesn't display DNS data per client.

Before you begin

- Make sure NetFlow is enabled on the network devices you plan to monitor.
- Enable Application Telemetry on Catalyst Center. For information, see Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry, on page 76.
- Minimum supported versions for DNS telemetry support:
  - Cisco IOS XE Routers - 17.9
  - Traffic Telemetry Appliance - 17.9
  - Cisco Catalyst 9200/9300/9400 Series Switches - 17.9.2

- Cisco Catalyst 9800 Series wireless controller - 17.10.1

Assurance supports site-based, role-based access control (SRBAC), which limits a user's scope of access to certain network sites. You must ensure you have access to the sites and devices, and associated DNS network services. For more information on user roles and permissions, see Cisco Catalyst Center Administrator Guide

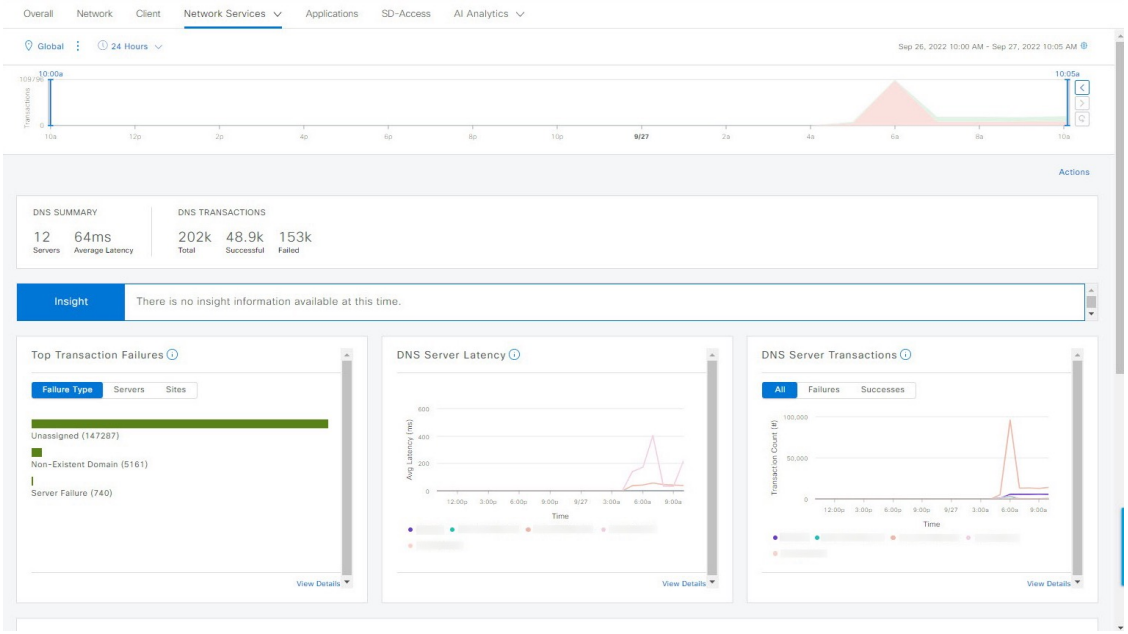
Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.
The **Overall** health dashboard appears.

Step 2 Choose **Network Services** > **DNS**.

The **DNS** dashboard appears.

Figure 22: DNS dashboard



Step 3 Click the time range setting ( ) at the top-left corner to specify the time range of the data that you want displayed in the window:

a) From the drop-down menu, choose a time range: **3 hours**, **24 hours**, or **7 days**.
b) Specify the **Start Date** and time and the **End Date** and time.
c) Click **Apply**.

Step 4 Click the autorefresh setting at the top-right corner to enable or disable the **Data Auto Refresh** on the supported Assurance pages in a 5-minute refresh interval.

Step 5 Use the timeline slider to view the information about the total successful and failed transactions of the DNS server over a period of time. The timeline slider has this functionality:

- You can hover your cursor over the timeline slider to view the DNS server transactions for a 5-minute window.

- When you double-click the timeline, it brings the timeline slider to a 1-hour time period. The entire window is refreshed, providing updates for that hour.

Step 6 To customize the dashboard display, click the **Actions** drop-down list below the timeline slider and choose **Edit Dashboard**. See Change the position of a dashlet, on page 349 and Create a custom dashboard, on page 347.

Step 7 Use the DNS summary dashlet to view this information:

DNS summary	
Item	**Description**
DNS Summary	Displays the count of DNS servers and average latency (in ms) of your network.
DNS Transactions	Displays the percentage of total number of DNS transactions, successful transactions, and failed transactions in your network.

Step 8 Use the **Insight** area to view the percentage of successful DNS server transactions compared with the current and previous time range.

Step 9 Use the DNS server dashlets for this functionality:

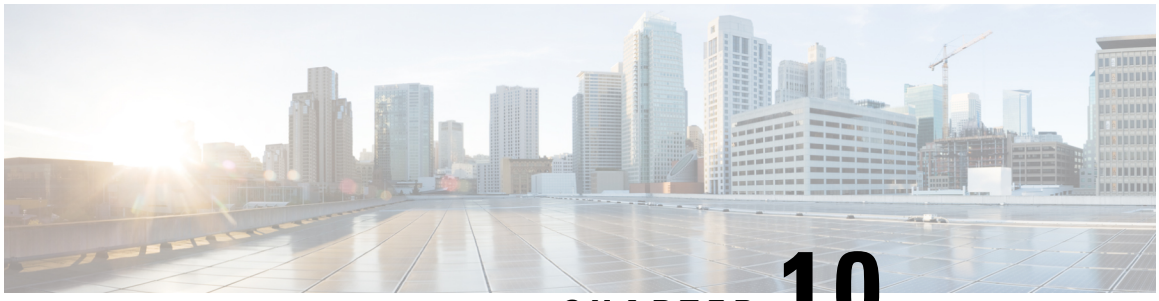
Top transaction failures
The chart displays the top DNS server transaction failure types, servers, and sites. You can hover your cursor on a color segment in the chart to view the number of transaction failures for each element. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click on a color segment in the chart to view more details about the failure.

DNS server latency
The chart displays the average DNS latency for each DNS server. You can hover your cursor over the chart to display the latency (in ms) of each server. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click the timeline to view more details.

DNS server transactions
The chart displays the average DNS server transactions status for each DNS server reported by wireless controllers. You can filter the status based on **All**, **Failures**, or **Successes**. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can display the chart based on the filter selection to view the DNS server transactions. You can select the data displayed as horizontal bars to filter the client table based on the top DNS servers, sites, SSIDs, APs, and so on.

Step 10 Use the **DNS Servers** by Device dashlet for this functionality:

DNS servers by device	
Item	**Description**
DNS Server table	View the DNS server information in a table format that contains the DNS server name, IP address, location, and so on. Click a server name to open the slide-in pane that displays **Device 360** information.
Export	Click **Export** to export the device information to a CSV file.
	Customize the data that you want displayed in the table: **a.** From the **Table Appearance** tab, set the table density and striping. **b.** From the **Edit Table Columns** tab, check the check boxes for the data you want displayed in the table. **c.** Click **Apply**.



CHAPTER 10

Monitor and Troubleshoot SD-Access Health

- SD-Access fabric, on page 203
- Monitor and troubleshoot the health of your SD-Access fabric, on page 209
- Monitor the health of a fabric site, on page 214
- Monitor the health of a transit and peer network, on page 218
- Monitor the health of a virtual network, on page 223

SD-Access fabric

Fabric technology is an integral part of SD-Access. A fabric network is a logical group of devices that is managed as a single entity in one or multiple locations. Having a fabric network in place enables several capabilities, such as the creation of virtual networks and user and device groups, and advanced reporting. Other capabilities include intelligent services for application recognition, traffic analytics, traffic prioritization, and steering for optimum performance and operational effectiveness.

Catalyst Center allows you to add devices to a fabric network. These devices can be configured to act as control plane, border, or edge devices within the fabric network.

Add a fabric site

Before you begin

You can create a fabric site only if IP Device Tracking (IPDT) is already configured for the site. To enable IPDT, go to **Design** > **Network Settings** > **Telemetry** and in the **Wired Endpoint Data Collection** area, click the **Enable Catalyst Center Wired Endpoint Data Collection At This Site** radio button.

Ensure these requirements are met for IPv6 underlay support.

- Supported platforms: Cisco IOS XE 26.1.1 and later, Cisco ISE Release 3.5 Patch 3.
- Supported products: Cisco Catalyst 9000 Series Switches.

  Cisco Catalyst 9200, IE9300, and IE3500 Series Switches are not supported in fabric edge roles but are supported in extended node and policy extended node roles. Cisco Catalyst 9200 Series Switches are supported in supplicant based extended role.

  Cisco Catalyst C9350, C9610, 9550, 9600x, and 9500x Series Switches are not supported for any fabric roles in an IPv6 underlay fabric and for dual stack border role in an IPv4 fabric site.

- A fabric site supports either IPv4 or IPv6 underlay, but not both.
- IPv6 underlay is supported only with LISP Pub/Sub SDA fabric.
- IPv6 overlay multicast is supported in HER/Unicast mode for both IPv4 and IPv6 underlay fabric sites.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of the fabric sites.

The resulting window displays every fabric site that has already been created and its information (such as Health Score, Fabric Zones, Fabric Devices, Fabric Roles, and Connected Transits) in a tabular format.

You can customize the table view to display only selected columns. Use the gear icon at the top right corner of the window to edit the **Table Settings** and **Apply** the changes.

Step 3 Click **Create Fabric Sites**.

Alternatively, instead of the first three steps, click the menu icon and choose **Workflow** > **Create Fabric Sites and Fabric Zones**.

Step 4 In the **Create Fabric Sites** window, click **Let's Do it** to go directly to the workflow.

Step 5 In the **Fabric Site Location** window, select an area, building, or floor to add as a fabric site.

Step 6 In the **Wired Endpoint Data Collection** window, ensure that the **Wired Endpoint Data Collection** check box is checked.

Step 7 Choose the **Underlay IP Addressing** for the fabric.

- For dual stack Catalyst Center deployments, you can choose either **IPv4** or **IPv6**.
- For single stack Catalyst Center deployments, the underlay IP addressing type is chosen by default, either **IPv4** or **IPv6**.

Step 8 In the **Authentication Template** window, do these steps:

a) Select an authentication template for the fabric site:

Template option	Description
Closed Authentication	Any traffic before authentication is dropped, including DHCP, DNS, and ARP.
Open Authentication	A host is allowed network access without having to go through 802.1X authentication.
Low Impact	Security is added by applying an ACL to the switch port, to allow very limited network access before authentication. After a host has been successfully authenticated, additional network access is granted.
None	None.

b) (Optional) If you select **Closed Authentication**, **Open Authentication**, or **Low Impact**, click **Edit** to edit the authentication settings:

Setting	Task
First Authentication Method	Select **802.1x** or **MAC Authentication Bypass (MAB)**.
802.1x Timeout (in seconds)	Use the slider to specify the 802.1x timeout, in seconds.
Wake on LAN	Select **Yes** or **No**.
Number of Hosts	Select **Unlimited** or **Single**.
Voice VLAN	Use this check box to enable or disable the default voice VLAN (VLAN 2046) for the site.
BPDU Guard	Use this check box to enable or disable the Bridge Protocol Data Unit (BPDU) guard on all the **Closed Authentication** ports.
Pre-Authentication Access Control List	You can configure Pre-authentication Access Control List (ACLs) for IPv4 and IPv6. **1.** Enable the toggle button to configure preauthentication control for **Low Impact** authentication. **2.** From the **Implicit Action** drop-down list, choose an implicit action and enter a description for the rule. **3.** To add an access contract, click **Add Contract Action**, choose the rules, and click **Apply Table**.

Step 9 (Optional) In the **Fabric Zones** window, choose one of these options:

Option	Task
To designate fabric zones later	Click **Setup Fabric Zones Later**.
To designate fabric zones and create scoped subnets	Click **Setup Fabric Zones Now** and select a fabric site from the displayed network hierarchy.

Step 10 In the **Summary** window, review the fabric site settings.

You can edit any of the fabric site or zone settings here.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 64.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 64.

Step 12 On the **Tasks** window, monitor the task deployment.

Step 13 It takes a few seconds for the site and zones to be provisioned. Upon successful creation of the site, a Fabric Site Creation Completed message displays.

Next, you are provided with options to either create a new fabric site or view the activities on the **Tasks** window.

Add a device to a fabric

After you have created a fabric site, you can add devices to the fabric site. You can also specify whether the device should act as a control plane node, an edge node, or a border node.

You can add a new device to the fabric site only if IP Device Tracking (IPDT) is configured for the fabric site. To enable IPDT, go to **Design** > **Network Settings** > **Telemetry** and in the **Wired Endpoint Data Collection** area, click the **Enable Catalyst Center Wired Endpoint Data Collection At This Site** radio button.

A device that is assigned the Access role and has been provisioned before enabling IPDT on the site can't be added to the fabric. Reprovision such devices before adding them to the fabric site. Check the Provision workflow to confirm the status of **Deployment of IPDT** on the device.

Note

- It's optional to designate the devices in a fabric site as control plane nodes or border nodes. You might have devices that don't occupy these roles. However, every fabric site must have at least one control plane node device and one border node device. In the current release for wired fabric, you can add up to six control plane nodes for redundancy.
- Currently, the Cisco Wireless Controller communicates only with two control plane nodes.
- You cannot change a device's role after it is added to the fabric. To change the role, remove the device from the fabric and re-add it.

Before you begin

Provision the device if you haven't already provisioned it:

- The **Provision** > **Network Devices** > **Inventory** window displays the discovered devices.
- The topology view shows a device in gray if it has passed the fabric readiness checks and is ready to be provisioned.
- If an error is detected during any of the fabric readiness checks, an error notification is displayed on the topology area. Click **See more details** to check the problem area listed in the resulting window. Correct the problem and click **Re-check** to ensure that the problem is resolved.
- If you update the device configuration as a part of problem resolution, ensure that you resynchronize the device information by doing an **Inventory** > **Resync** for the device.

Note You can continue to provision a device that has failed the fabric readiness checks.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 Select the fabric site to add a device.

The resulting topology view displays all devices in the network that have been inventoried. In the topology view, any device that is added to the fabric is shown in blue.

Step 4 From the **List** view under the **Fabric Infrastructure** tab, click a device. A slide-in pane displays these **Fabric** options:

Option	Description
Edge Node	Toggle the button next to this option to enable the selected device as an edge node.
Border Node	Toggle the button next to this option to enable the selected device as a border node.
Control Plane Node	Toggle the button next to this option to enable the selected device as a control plane node.

To configure a device as a fabric-in-a-box, select the **Control Plane Node**, **Border Node**, and **Edge Node** options.

To configure the device as a control plane and a border node, select both **Control Plane Node** and **Border Node**.

Step 5 (Optional) To enable the wireless capability for the device, under **Capability**, click the **Embedded Wireless LAN Controller** toggle button and do these steps:

Alternatively, if the toggle button is already enabled, you can click **Configure** to configure the wireless settings.

a) If you have not installed the wireless package on the device yet, Catalyst Center displays a warning message indicating that the embedded wireless controller software image is necessary for enabling the capability. In the warning dialog box, click **OK** to install the image manually.

b) Under **Download Image**, click **Choose File** to navigate to a software image stored locally, or **Enter image URL** to specify an HTTP or FTP source from which to import the software image.

c) Click **Import**.

The progress of the image import is displayed. To exit the window, and view the progress of the import and schedule the installation later, click **Close**.

d) After the image import is complete, under **Schedule Image Installation** on **Download Image**, choose one of these options:

- **Now**: Immediately install the image.
- **Later**: Schedule the image installation for a later date or time.

e) In the **Task Name** field, update the task name, if required.

f) If you chose **Later**, do these tasks:

- Under **Start Date/Time**, specify a start date and time for the image installation.
- To use the default site time zone for the image installation, check the **Site Settings** check box. To select a time zone, uncheck the **Site Settings** check box and choose a time zone from the drop-down list.

g) Click **Apply**.

To view the status of image installation, go to the **Activities** > **Tasks** window and open the relevant work item. After the software image is distributed and activated on the switch, you must resynchronize the device using the **Provision** > **Inventory** > **Resync** option.

h) Under **Manage Scope**, assign the managed AP locations for the embedded wireless controller:

- Under the **Primary** tab, check the check box next to the required site name.
- Under the **Secondary** tab, check the check box next to the required site name.

You can select either a parent site or individual sites. If you select a parent site, all the children under the parent site are also selected. You can uncheck the check box to deselect an individual site.

You can also use the **Search Hierarchy** search field or the filter icon to find a site.

i) Click **Next**.

j) Under **Advanced**, configure the required settings.

- To enable the Rolling AP Upgrade feature, check the **Rolling AP Upgrade** check box.

  (Optional) If you check this check box, from the **AP Reboot Percentage** drop-down list, select the percentage of APs that can be rebooted with minimal client disruptions. The default value is 25%.

- To renew the Locally Significant Certificate (LSC) for the associated APs before its expiry, check the **AP LSC Certificate Renewal** check box.

  If you check this check box, complete these configurations:

  - From the **Renewal Profile** drop-down list, select an AP LSC renewal profile.
  - (Optional) If you select an AP LSC renewal profile for staggered renewal, from the **AP Reboot %** drop-down list, select the percentage of APs that can be rebooted with minimal client disruptions. The default value is 25%.

Note
If configured, the same AP reboot percentage value applies to both the Rolling AP Upgrade and staggered AP LSC renewal processes. For example, if you set the AP reboot percentage to 25%, only 25% of APs will reboot at a time during both Rolling AP Upgrade and staggered AP LSC renewal.

k) Click **Next**.

l) Under **Summary**, review the configuration settings.

m) Click **Save**.

If the wireless capability is enabled for a device and there are changes in the wireless network settings, to push the changes to the device, you must click **Configure** and save the configuration.

Step 6 Click **Add** to save the configurations.

Step 7 Click **Deploy** under the **Fabric Infrastructure** tab to configure the device.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 64.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 64.

Note
A device is added to the fabric only if the device runs a software release that is compatible with the Catalyst Center release. For information about fabric device compatibility, see Cisco SD-Access Compatibility Matrix.

For a given fabric role, if the software image on the device isn't compatible with the Catalyst Center release, the device isn't added to the fabric and an error message is displayed.

Step 9 On the **Tasks** window, monitor the task deployment.

What to do next

After a device is added to the fabric, fabric compliance checks are automatically performed to ensure that the device is fabric-compliant. The topology displays a device that has failed the fabric compliance check in blue color with a cross-mark beside it. Click **See more details** on the error notification to identify the problem area and correct it.

Monitor and troubleshoot the health of your SD-Access fabric

Use this procedure to get a global view of your SD-Access fabric and to determine if there are potential issues that must be addressed.

A fabric network is a logical group of devices that is managed as a single entity in one or multiple locations. Catalyst Center allows you to add devices to a fabric network. These devices can be configured to act as control plane, border, or edge devices within the fabric network.

Before you begin

To monitor and troubleshoot fabric sites, you must first configure the fabric site. See Add a fabric site, on page 203 and Add a device to a fabric, on page 206.

Assurance supports site-based, role-based access control (SRBAC), which limits a user's scope of access to certain client 360. The Assurance SD-Access fabric features depends on the user role and site defined in the access group. For more information on user roles and permissions, see *Cisco Catalyst Center Administrator Guide*.

For additional details and to understand multisite fabric sites, see the "Provision Your Network" chapter in the *Cisco Catalyst Center User Guide*.

Note Subtended and extended nodes are not part of fabric health because during fabric provisioning, these nodes are not given a fabric role, such as edge, border, or control plane.

Procedure

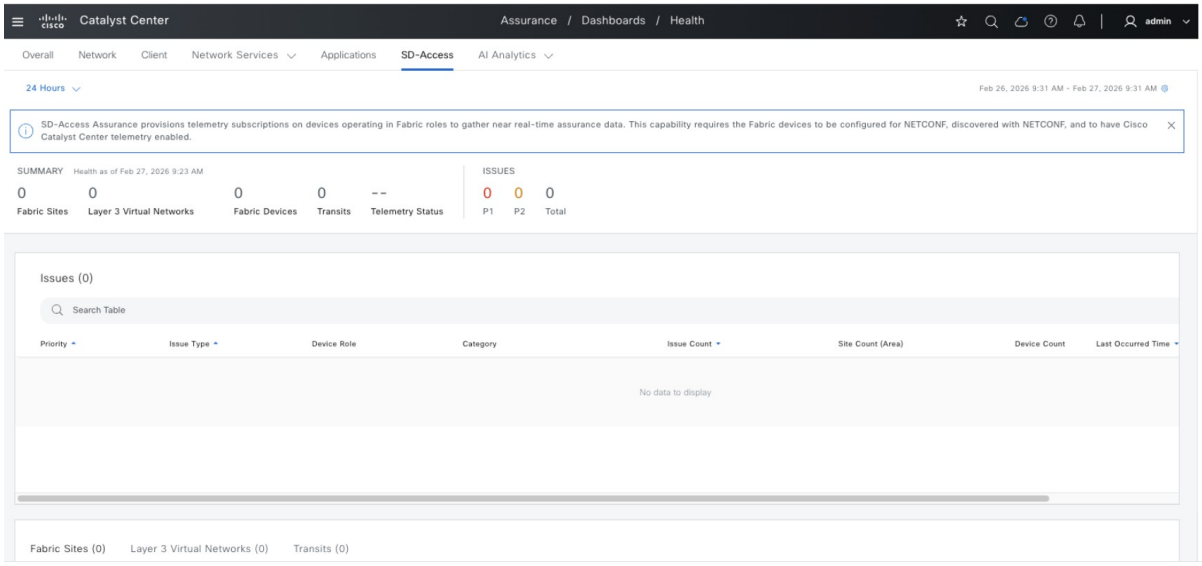
Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **SD-Access** tab.

The **SD-Access** health dashboard appears.

Figure 23: SD-Access Health Dashboard



Step 3 Click the time range setting (24 Hours) in the top-menu bar to specify the time range of data that appears on the dashboard.

a) From the drop-down menu, select the time range: **3 Hours**, **24 Hours**, or **7 Days**.

b) Specify the **Start Date** and time; and the **End Date** and time.

c) Click **Apply**.

Step 4 Use the SD-Access Health Summary dashlet for this functionality:

Item	Description
Summary	• **Fabric Sites**: Number of fabric sites. • **Layer 3 Virtual Networks**: Number of layer 3 virtual networks. • **Fabric Devices**: Number of fabric devices. • **Transits and Peer Networks**: Number of transits and peer networks. • **Telemetry Status**: Displays the telemetry status of the fabric sites.
Issues	• **P1**: Number of priority 1 issues. • **P2**: Number of priority 2 issues. • **Total**: Total number of P1, P2, and P3 issues.

Step 5 Use the SD-Access **Top 10 Issue Types** dashlet for this functionality:

Top 10 Issue Type Dashlet
Displays the top 10 issues, if any, that must be addressed. The issues are color coded and sorted by their preassigned priority level, starting with P1. Click an issue to open a slide-in pane with additional details about the issue type. From the slide-in pane, click an issue instance where, as required, you can do these tasks: • To resolve the issue instance, from the **Status** drop-down list, select **Resolve**. • To ignore the issue instance: **a.** From the **Status** drop-down list, select **Ignore**. **b.** Set the number of hours to ignore the issue on the slider. **c.** Click **Confirm**. Click **View All Open Issues** to open the **Open Issues** window.

Step 6 Use the **Fabric Sites** dashlet to view detailed information about the fabric sites in your network. This dashlet provides the functionality listed in this table:

Fabric Sites Dashlet	
Item	**Description**
Health	Filter the table based on the client health with these options: • **All** • **Poor**: Fabric sites with a health score range from 1 to 3. • **Fair**: Fabric sites with a health score range from 4 to 7. • **Good**: Fabric sites with a health score range from 8 to 10. • **No Data**: Fabric sites with no data.
Fabric Site table	View detailed fabric site information in a table format. The fabric site table displays this information by default: • **Fabric Site**: Name of the fabric site. You can click the name to display a 360° view of a fabric site. See Monitor the health of a fabric site, on page 214. • **# of Fabric Devices**: Number of fabric devices in the fabric site. • **Fabric Site Health**: • **Overall**: Overall health of the fabric site. • **Fabric Site Connectivity**: Health of the connectivity with the fabric site. • **Fabric Control Plane**: Health of the control plane in the fabric site. • **Fabric Infrastructure**: Health of the devices that make up the fabric site.

Fabric Sites Dashlet	
Item	**Description**
Export	Click **Export** to export the table data to a CSV file. **Note** The data from all available columns is included even if the column was not selected for the table. Filters applied to the client table are applied to the exported data.
⚙	Customize the table display: **a.** From the **Table Appearance** tab, set the table density and striping. **b.** From the **Edit Table Columns** tab, select the data you want displayed in the table. **c.** Click **Apply**.

Step 7 Use the **Virtual Networks** dashlet to view detailed information about the virtual networks in your fabric site. This dashlet provides this functionality:

Virtual Networks Dashlet	
Item	**Description**
Health	Filter the table based on the virtual network health with these options: • **All** • **Poor**: Virtual networks with a health score range from 1 to 3. • **Fair**: Virtual networks with a health score range from 4 to 7. • **Good**: Virtual networks with a health score range from 8 to 10. • **No Data**: Virtual networks with no data.

Virtual Networks table	View detailed virtual network information in a table format. The virtual network table displays this information by default:
	• **VN Name**: Name of the virtual network.
	You can click the name to display a 360° view of a virtual network. See Monitor the health of a virtual network, on page 223.
	• **# of Active Sites**: Number of active sites in the virtual network.
	• **# of Clients**: Number of endpoints in the virtual network.
	• **Virtual Network Health**:
	  • **Overall**: Overall health of the virtual network.
	  • **Fabric Control Plane**: Health of the control plane in the virtual network.
	  • **VN Services**: Health of the virtual network services.

Virtual Networks Dashlet	
Item	**Description**
Export	Click **Export** to export the table data to a CSV file. **Note** The data from all available columns is included even if the column was not selected for the table. Filters applied to the client table are applied to the exported data.
	Customize the table display: **a.** From the **Table Appearance** tab, set the table density and striping. **b.** From the **Edit Table Columns** tab, select the data you want displayed in the table. **c.** Click **Apply**.

Step 8 Use the **Transits and Peer Networks** dashlet to view the detailed information about the transits and peer networks in your fabric site. This dashlet provides this functionality:

Item	Description
Health	Filter the table based on the transit and peer network health with these options: • **All** • **Poor**: Transits and peer networks with a health score range from 1 to 3. • **Fair**: Transits and peer networks with a health score range from 4 to 7. • **Good**: Transits and peer networks with a health score range from 8 to 10. • **No Data**: Transits and peer networks with no data.

Transits and Peer Networks table	View detailed transits and peer network information in a table format. The transits and peer network table displays this information by default:
	• **Transit/ Peer Network Name**: Name of the Transit network.
	You can click the name to display a 360° view of a transit network. See Monitor the health of a transit and peer network, on page 218.
	• **Type**: Number of active sites in the transit network.
	• **# of Clients**: Number of endpoints in the transit network.
	• **Associated Fabric Sites**
	• **Transit and Peer Networks Health**:
	  • **Overall**: Overall health of the transit and peer network.
	  • **Transit Control Plane**: Health of the transit control plane.

Item	Description
Export	Click **Export** to export the table data to a CSV file. **Note** The data from all available columns is included even if the column was not selected for the table. Filters applied to the client table are applied to the exported data.
⚙	Customize the table display: **a.** From the **Table Appearance** tab, set the table density and striping. **b.** From the **Edit Table Columns** tab, select the data you want displayed in the table. **c.** Click **Apply**.

Monitor the health of a fabric site

Use this procedure to view details about a specific fabric site.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **SD-Access** tab.

The **SD-Access** health dashboard appears.

Step 3 In the **Fabric Site** table, click the name of a fabric site.

The **Fabric Site** window appears, which provides a 360° view of the fabric site.

Figure 24: Fabric Site 360



Step 4 Click the time range setting (24 Hours) at the top-left corner to specify the time range for the data that you want displayed in the window:

a) From the drop-down list, select a time range: **3 hours 24 hours**, or **7 days**.

b) Specify the **Start Date** and time; and the **End Date** and time.

c) Click **Apply**.

Step 5 Use the health timeline slider to view the health score for a more granular time range and to view quality information.

Hover your cursor within the timeline to view this information:

Check the **Telemetry Status** check box below the timeline to view the horizontal bar in the timeline. Hover your cursor over the horizontal bar to view the Telemetry Status of fabric site such as **Good**, **Fair**, or **Poor**. Click the **Telemetry Status** in the tool tip to open a slide-in pane to view the telemetry status summary of the fabric sites.

Fabric Site Health: Health is the percentage of healthy fabric nodes in this site. Device health of control planes is not included. Fabric Sub Category Health is the minimum of underlying KPI scores.

Note
The KPI is not included for health score.

Fabric Site Connectivity: Lists the KPI subcategories that contribute to the site reachability status, such as control plane reachability, extended node connectivity, and so on.

Fabric Control Plane

Fabric Infrastructure

Click and drag the timeline boundary lines to specify the time range. This boundary sets the context for the fabric site data that is displayed in the **Fabric Site 360** window.

Click the **Latest** and **Trend** tabs to change the scope of data displayed in the category:

- **Latest**: Displays the data from the selected time window in the timeline on the top of the window.
- **Trend**: Displays data from the last 24 hours.

Step 6 Use the **Fabric Site Health** area, below the timeline, to view this information:

Fabric site health	
Item	**Description**
Latest	Displayed by default. Includes two panes. The left pane provides the network health summary score and the total number of devices. The right pane displays charts. • **Health Fabric Nodes**: The percentage of healthy (good) nodes in your selected site. • **Total Devices**: Total number of network devices and the count of devices with Good Health, Fair Health, Poor Health, and No Health Data. • **Charts**: This color-coded, snapshot-view chart shows the fabric site connectivity and infrastructure over the last 5 minutes. Hover your cursor over a color to display the health score and the number of devices that are associated with that color. If the chart shows a low health score (red or orange), the KPIs that contributed to the low health score are provided next to the bar. Examples include Fabric CP reachability, Multicast RP, AAA Server Status, and so on. This KPI monitors the status of each AAA server's Session Manager Daemon (SMD) and Wireless Network Control Daemon (WNCD) instances, which are responsible for Dot1 x and MAB authentication for wired and wireless devices. The iOS instance, responsible for Telnet and SSH authentication, is not monitored. This KPI applies only to Edge and Extended Node roles. Click a hyperlinked fabric category in the charts to open a side pane to view the respective KPI subcategories: • **Fabric Site Connectivity**: Control Plane Reachability, Extended Node Connectivity, BGP Session from Border to Control Plane, and BGP Session from Border to Peer Node for INFRA VN. • **Fabric Control Plane**: LISP Session Status. • **Fabric Infrastructure**: AAA Server Status, Pub-Sub Session Status for INFRA VN, CTS Environment Data Download.
Trend	Click the **Trend** tab to display a trend chart. This color-coded trend chart shows the performance of devices over a time range. Hover your cursor over the chart to display the total number of devices and their health over time. The color in the chart represents the health of the network devices: ●: Poor network devices. Health score range is 1 to 3. ●: Fair network devices. Health score range is 4 to 7. ●: Good network devices. Health score range is 8 to 10. ●: No health data. Health score is 0.

Step 7 Use the **Top 10 Issue Types** area to view this information:

Issues
Displays any issues that must be addressed. Issues are listed based on the timestamp. The most recent issue is listed first. Click an issue to open a slide-in pane to view the corresponding details, such as the description of the issue, impact, and suggested actions. From the slide-in pane, you can do these tasks: • To resolve an issue: **a.** From the drop-down list, select **Resolve**. **b.** To view the list of issues that have been resolved, click **Resolved Issues**. • To ignore an issue: **a.** From the drop-down list, select **Ignore**. **b.** Set the number of hours to ignore the issue on the slider. **c.** Click **Confirm**. **d.** To view the list of issues that have been ignored, click **Ignored Issues**. For information about the types of issues, see View and Manage Issues, on page 239.

Step 8 Use the **Fabric Nodes** dashlet for the functionality listed in this table:

Network Devices dashlet	
Item	**Description**
Type	Filter the table based on the fabric node type with these options: **All**, **Fabric Control Plane**, **Fabric Border**, **Fabric Edge**, **Fabric WLC**, **Fabric AP**, and **Extended Node**.
Fabric Site Health	Filter the table based on the overall health score of the fabric site with these options: • **All** • **Poor**: Devices with a health score range from 1 to 3. • **Fair**: Devices with a health score range from 4 to 7. • **Good**: Devices with a health score range from 8 to 10. • **No Health**: Devices with no health data.

Network Devices dashlet	
Item	**Description**
Fabric Node table	View device information for all the fabric nodes for the selected site in a table format. **Note** The overall health score is the minimum subscore of these KPI metric health scores: fabric site connectivity and fabric infrastructure. The **Name**, **Issue Type Count**, and **Fabric Role** columns display the fabric name, issue count, and fabric role (Edge, Border, Map Server, and so on). Under **Device Fabric Site Health**, in the **Overall** column, hover your cursor over a health score. The overall **Device Fabric Site Health** score is displayed along with the health and percentage value of all the KPI metrics. Hover your cursor over the **Fabric Site Connectivity**, **Fabric Control Plane**, and **Fabric Infrastructure** icons to display the health scores.
Device 360	Display a 360° view of a device by clicking the device name in the **Name** column. **Device 360** provides detailed information for troubleshooting device issues.
Export	Click **Export** to export the device information to a CSV file.
	Customize the data that you want displayed in the table: **a.** Click . A list of options is displayed. **b.** Check the check boxes for the data you want displayed in the table. **c.** Click **Apply**.

Monitor the health of a transit and peer network

Use this procedure to view the details about a specific transit network.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

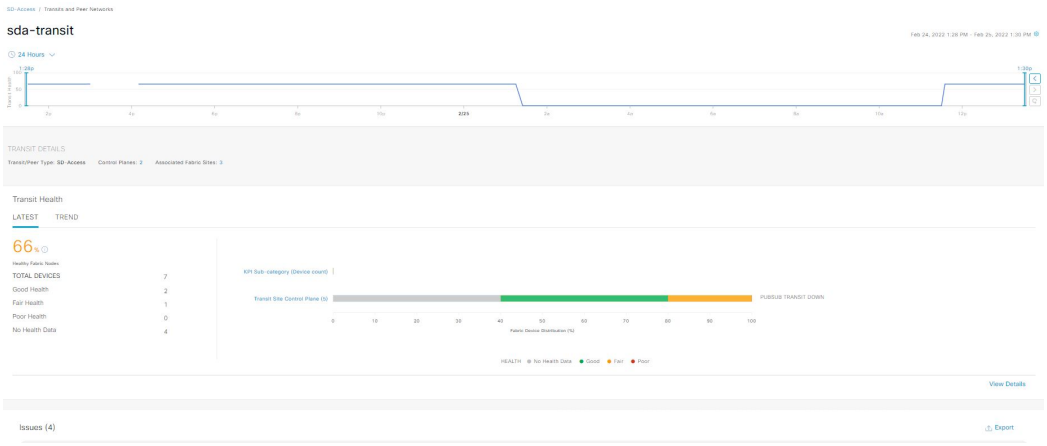
Step 2 On the **Overall** health dashboard, click the **SD-Access** tab.

The **SD-Access** health dashboard appears.

Step 3 In the **Transit and Peer Network** table, click the name of a transit.

The **Transit Site 360** window appears, which provides a 360° view of the fabric site.

Figure 25: Transit 360 window



Step 4 Click the time range setting (24 Hours) at the top-left corner to specify the time range for the data that you want displayed in the window:

a) From the drop-down list, select a time range: **3 hours**, **24 hours**, or **7 days**.

b) Specify the **Start Date** and time; and the **End Date** and time.

c) Click **Apply**.

Step 5 Use the health timeline slider to view the health score for a more granular time range and to view quality information.

Hover your cursor within the timeline to view this information:

Transit Network Health: The health score is the percentage of healthy fabric nodes in this site; it does not include the device health of control planes. The fabric category health is the minimum of underlying KPI scores.

Transit Site Control Plane: Lists the KPI subcategory, such as LISP and PubSub session of the transits. If the Transit health score is low, click **View Device List** to display a list of devices that contribute to the low score and their associated down sessions. Click of the hyperlinked name of the device to display device information.

Check the **Telemetry Status** check box below the timeline to view the horizontal bar in the timeline. To view the telemetry status:

- Hover your cursor over the horizontal bar to view the information such as percentage of Transit Network Health, Telemetry Status such as **Good**, **Fair**, or **Poor**, Transit Site Control Pane and Transit Services in the tool tip.
- Click the **Telemetry Status** in the tool tip to open a slide-in pane to view the telemetry status summary.

To change the scope of the data displayed in the category, click one of these tabs:

- **Latest**: Displays the data from the selected time window in the timeline at the top of the window.
- **Trend**: Displays data from the last 24 hours.

Step 6 Use the **Transit Health** area, below the timeline, to view this information:

Item	Description
LATEST	Displayed by default. Includes two panes. The left pane provides the network health summary score and the total number of devices. The right pane displays charts. • **Health Fabric Nodes**: The percentage of healthy (good) nodes in your selected site. • **Total Devices**: The total number of network devices and the count of devices with Good Health, Fair Health, Poor Health, and No Health Data. • **Charts**: This color-coded snapshot-view chart shows the transit control plane over the last 5 minutes. Hover your cursor over a color to display the health score and the number of devices that are associated with that color. You can also click a hyperlinked **Transit Control Plane** in the charts to open a side pane to view these KPI subcategories in the Transit Control plane: • **BGP Session from Border to Transit Control Plane** • **LISP session from Border to Transit Control Plane** • **PubSub session from Border to Transit Control Plane** You can hover on a color segment in the chart to view the fabric node details in the table format such as name of the fabric node, issue count, fabric role, fabric site and device transit health.
TREND	Click the **TREND** tab to display a trend chart. This color-coded trend chart shows the performance of devices over a time range. Hover your cursor over the chart to display the total number of devices and their health over time. The color in the chart represents the health of the network devices: ●: Poor network devices. The health score range is 1 to 3. ●: Fair network devices. The health score range is 4 to 7. ●: Good network devices. The health score range is 8 to 10. ●: No Health data. The health score is 0.

Step 7 Use the **Top 10 Issue Types** area to view this information:

Issues
Displays any issues that must be addressed. Issues are listed based on the timestamp. The most recent issue is listed first. Click an issue to open a slide-in pane to view the corresponding details, such as the description of the issue, impact, and suggested actions. From the slide-in pane, you can do these tasks: • To resolve an issue: **a.** From the drop-down list, select **Resolve**. **b.** To view the list of issues that have been resolved, click **Resolved Issues**. • To ignore an issue: **a.** From the drop-down list, select **Ignore**. **b.** Set the number of hours to ignore the issue on the slider. **c.** Click **Confirm**. **d.** To view the list of issues that have been ignored, click **Ignored Issues**. For information about the types of issues, see View and Manage Issues, on page 239.

Step 8 Use the **Associated Fabric Sites** dashlet for this functionality:

Item	Description
Health	Filter the table based on the overall health score of the fabric site with these options: • **All** • **Poor**: Devices with a health score range from 1 to 3. • **Fair**: Devices with a health score range from 4 to 7. • **Good**: Devices with a health score range from 8 to 10. • **No Health**: Devices with no health data.
Associated Fabric Sites table	Displays these details in the fabric table: **Fabric Site**, **Health**, number of available **Connected Transit/ Peer Networks**, **Layer 3 Virtual Networks**, and **Fabric Devices**.
Device 360	Display a 360° view of a device by clicking the device name in the **Name** column. The **Device 360** window provides detailed information for troubleshooting device issues.
Export	Click **Export** to export the device information to a CSV file.

Item	Description
	Customize the data that you want displayed in the table: **a.** Click the settings icon (). A list of options is displayed. **b.** In the Table Settings slide-in pane, enable the toggle buttons for the data you want displayed in the table. **c.** Click **Apply**.

Step 9 Use the **Fabric Nodes** dashlet for this functionality:

Item	Description
Type	Filter the table based on the fabric node type with these options: **All**, **Transit Control Plane**, and **Border**.
Transit and Peer Network Health table	Filter the table based on the overall health score of the transit with these options: • **All** • **Poor**: Devices with a health score range from 1 to 3. • **Fair**: Devices with a health score range from 4 to 7. • **Good**: Devices with a health score range from 8 to 10. • **No Health**: Devices with no health data.
Fabric Node table	View device information for all the fabric nodes for the selected transit in a table format. **Note** The overall health score is the minimum subscore of these KPI metric health scores: Transit Site Control Plane. The **Name**, **Issue Type Count**, **Fabric Role**, and **Fabric Site** columns display the fabric name, issue count, fabric role, and fabric site. In the **Overall** column, under **Device Transit Health**, hover your cursor over a health score. The overall **Device Transit Health** score is displayed along with the health and percentage value of all the KPI metrics. Hover your cursor over the **Transit Site Control Plane** icons to display the health scores.
Device 360	Display a 360° view of a device by clicking the device name in the **Name** column. The **Device 360** window provides detailed information for troubleshooting device issues.
	Click **Export** to export the device information to a CSV file.

Item	Description
⚙	Customize the data that you want displayed in the table: **a.** Click the settings icon (⚙). **b.** In the Table Settings slide-in pane, enable the toggle buttons for the data you want displayed in the table. **c.** Click **Apply**.

Monitor the health of a virtual network

Use this procedure to view details about a specific virtual network.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **SD-Access** tab.

The **SD-Access** health dashboard appears.

Step 3 Scroll down and click **Virtual Network**.

Step 4 In the **Virtual Network** table, click the name of a virtual network.

The **Virtual Network 360** window appears, which provides a 360° view of the virtual network.

Figure 26: Virtual Network 360



Step 5 Click the time range setting (24 Hours) at the top-left corner to specify the time range for the data that you want displayed in the window:

a) From the drop-down menu, select a time range: **3 hours**, **24 hours**, or **7 days**.
b) Specify the **Start Date** and time; and the **End Date** and time.
c) Click **Apply**.

Step 6 Use the virtual network health timeline slider to view the virtual network's health score for a more granular time range and to view the virtual network's quality information.

Hover your cursor within the timeline to view this information:

Virtual Network Health: Health score is the percentage of healthy devices in the VN. VN Category Health is the minimum of corresponding subcategory KPI scores. **VN Services** includes **BGP Session from Border to Peer Node**, **Multicast (external RP)**, **Default Route Registration**, and **VN Control Plane**.

If the VN health score is low, click **View Device List** to display a list of devices that contribute to the low score and their associated down sessions. Click the hyperlinked name of the device to display device information.

Check the **Telemetry Status** check box below the timeline to view the horizontal bar in the timeline. To view the telemetry status:

- Hover your cursor over the horizontal bar to view information such as percentage of Virtual Network Health, Telemetry Status such as **Good**, **Fair**, or **Poor**, Fabric Control Pane and VN Services, and VN Exit in the tool tip.
- Click the **Telemetry Status** in the tool tip to open a slide-in pane to view the telemetry status summary of the virtual networks.

Click and drag the timeline boundary lines to specify the time range. This sets the context for the data that is displayed in the 360 window.

Click the **Latest** and **Trend** tabs to change the scope of data displayed in the category:

- Latest: Displays the data from the selected time window in the timeline on the top of the window.
- Trend: Displays data from the last 24 hours.

Step 7 Use the **Virtual Network Health** area, below the timeline, to view this information:

Virtual network health	
Item	**Description**
Latest	Displayed by default. The left pane provides the virtual network health summary score and the total number of devices. The right pane displays charts. • **Healthy Fabric Nodes**: The percentage of healthy (good) nodes in your selected site. • **Total Devices**: Total number of fabric devices and the count of devices with Good Health, Fair Health, Poor Health, and No Health data. • **Charts**: This color-coded, snapshot-view chart shows the KPIs with subcategories such as **VN Control Plane** (Pub-Sub Sessions Status) and **VN Services** (BGP Session from Border to Peer Node, Multicast-external RP, and Default Route Registration). Hover your cursor over a color to display the health score and the number of devices that are associated with that color. If the chart shows a low health score (red or orange), the KPIs that contributed to the low health score are provided next to the bar. Click a hyperlinked category to open a side pane with more details.
Trend	Click the **Trend** tab to display a trend chart. This color-coded trend chart shows the performance of devices over a time range. Hover your cursor over the chart to display the total number of devices and their health over time. The color in the chart represents the health of the network devices: ●: Poor network devices. Health score range is 1 to 3. ●: Fair network devices. Health score range is 4 to 7. ●: Good network devices. Health score range is 8 to 10. ●: No Health data. Health score is 0.

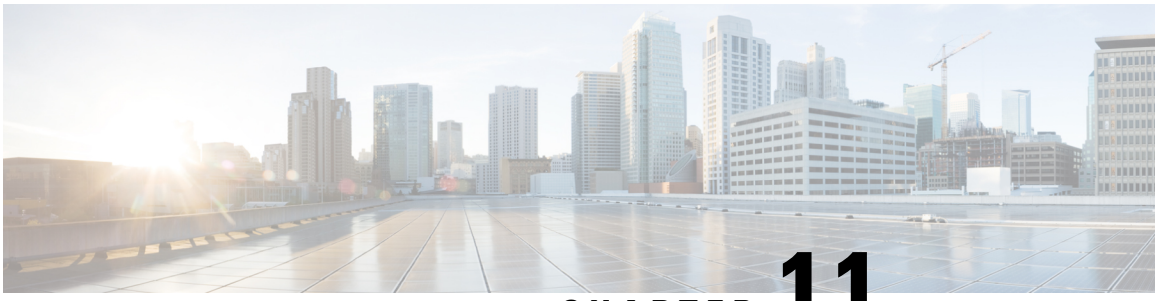
Step 8 Use the **Top 10 Issue Types** area to view this information:

Issues
Displays any issues that must be addressed. Issues are listed based on the timestamp. The most recent issue is listed first. Click an issue to open a slide-in pane to view the corresponding details, such as the description of the issue, impact, and suggested actions. From the slide-in pane, you can do these tasks: • To resolve an issue: **a.** From the drop-down list, select **Resolve**. **b.** To view the list of issues that have been resolved, click **Resolved Issues**. • To ignore an issue: **a.** From the drop-down list, select **Ignore**. **b.** Set the number of hours to ignore the issue on the slider. **c.** Click **Confirm**. **d.** To view the list of issues that have been ignored, click **Ignored Issues**. For information about the types of issues, see View and Manage Issues, on page 239.

Step 9 Use the **Virtual Network Devices** dashlet for this functionality:

Virtual network devices dashlet	
Item	**Description**
Type	Filter the table based on the type.
Virtual Network Health	Filter the table based on the overall health score of the virtual network with these options: • **All** • **Poor**: Devices with a health score range from 1 to 3. • **Fair**: Devices with a health score range from 4 to 7. • **Good**: Devices with a health score range from 8 to 10. • **No Health**: Devices with no health data.
Virtual Network Devices table	View device information for the selected item in a table format. **Note** The overall health score is the minimum subscore of these KPI metric health scores: virtual network connectivity and infrastructure. Hover your cursor over the various health scores and icons to display additional information. \

Virtual network devices dashlet	
Item	**Description**
Device 360	Display a 360° view of a device by clicking the device name in the **Name** column. **Device 360** provides detailed information for troubleshooting device issues.
Export	Click **Export** to export the device information to a CSV file.
	Customize the data that you want displayed in the table: **a.** Click . A list of options appear. **b.** Check the check boxes for the data you want displayed in the table. **c.** Click **Apply**.



CHAPTER 11

Monitor and Troubleshoot Your Network Using Site Analytics

- About Site Analytics, on page 229
- Site Analytics dashboard insights, on page 231
- View Site Analytics, on page 234
- Configure Site Analytics settings, on page 238

About Site Analytics

Site Analytics provides you with visibility for network troubleshooting and allows you to drill down to the most problematic site, building, and floor or AP. You can set thresholds for KPIs and monitor the trend per KPI before the issue occurs.

You can define KPI thresholds that can be used to inform you of network-wide issues. Based on a KPI value, you can determine the site with the worst performance and drill down to the specific building and floor to find the problem. You can analyze issues pertaining to onboarding attempts, onboarding duration, roaming attempts, roaming duration, coverage, and connection speed.

The **Site Analytics** window helps you answer these questions when investigating performance issues:

- **What**: Use the KPIs to find out more about a problem. The KPI cards display the name of the KPI, the success rate of the KPI, and the name and score of the worst performer. If a KPI threshold is being met, the KPI score is shown in black. If the percentage is less than the threshold value, the score is shown in red.

  These categories are available:

  - **Onboarding Attempts**: Measures the percentage of wireless clients that are able to successfully onboard to an AP in the given site. An SLA is met when a wireless client successfully joins the network, and an SLA is a failure when a wireless client doesn't successfully join the network. For example, 100 clients attempt to onboard to the network. 50 clients onboard successfully, and 50 fail to onboard. The **Onboarding Attempts** KPI value is 50%.

  - **Onboarding Duration**: Measures the percentage of successfully onboarded wireless clients that are able to onboard to an AP within the configured threshold time (see Configure Site Analytics settings, on page 238 for configuring thresholds). If a wireless client fails to onboard, it is not counted in the metric. If a wireless client successfully onboards, but takes longer than the configured SLA duration, it is counted as a failure. For example, out of the 50 clients who onboarded successfully,

30 clients took less than 10 seconds, and 20 clients took more than 10 seconds. So, the **Onboarding Duration** KPI value is 60%.

- **Roaming Attempts**: Measures the percentage of wireless clients that are able to successfully roam from one AP to another AP in the given site. An SLA is met when a wireless client successfully roams and joins the network via another AP, and is considered a failure when the wireless client doesn't successfully join the network. For example, 100 clients attempted to roam in a given duration. 50 clients roamed successfully, and 50 failed to roam. The **Roaming Attempts** KPI value is 50%.
- **Roaming Duration**: Measures the percentage of wireless clients that are able to successfully roam from one AP to another AP within the configured threshold time. If a wireless client fails to roam successfully, it is not counted in this metric. If a wireless client successfully roams, but takes longer than the configured threshold for roaming duration, it is counted as a failure. For example, out of the 50 clients who roamed successfully, 30 clients took less than 10 seconds, and 20 clients took more than 10 seconds. The **Roaming Duration** KPI value is 60%.
- **Connection Speed**: Measures the percentage of time that wireless clients have data traffic with over-the-air data rates that are higher than the configured threshold rate. For example, among the data rates sampled by the controller for the 50 successfully onboarded clients, 200 samples were higher than the threshold of 11 Mbps and 50 samples were lower. The **Connection Speed** KPI value is 80%.
- **Coverage**: Measures the percentage of time that wireless clients have data traffic with RSSI values that are higher than the configured threshold value. For example, among the RSSI values of the 50 successfully onboarded clients sampled by the controller, 200 samples were higher than the threshold of -72 dBm and 50 samples were lower. The **Coverage** KPI value is 80%.

- **When**: Click the time-range setting (24 Hours) to specify the time period to use for the KPIs, timeline slider, and heatmap.
- **Where**: Drill down from the site level to the building, floor, and device level.
  - Easily identify poor performing sites and buildings and their corresponding KPI values by their red or green color in the heatmap. Green indicates that the KPI threshold is being met, and red indicates that the KPI is not being met.
  - Drill down to the building level, where you can see several key factors that have contributed to the low KPI score.
  - View access points in a floor heatmap that shows their health status and device details.
  - View a list of access points on a given floor along with each access point's specific KPI score and client count.
  - Click an access point to display its **Device 360** window.

The Site Analytics dashboard is available from the Assurance health dashboard **AI Analytics** menu option.

The **AI Analytics** menu option also provides access to AI Network Analytics tools. For information about these tools, see Observe Network Trends and Gain Insights, on page 353.

Site Analytics dashboard insights

Site Analytics helps you monitor KPIs in your wireless networks. The KPIs are onboarding attempts, onboarding duration, roaming attempts, roaming duration, connection speed, and coverage. You can set performance thresholds for each of these KPIs. Then, you can monitor them on the **Assurance** > **Health** > **Overall** heath dashboard or the **Assurance** > **Health** > **AI Analytics** > **Site Analytics** dashboard.

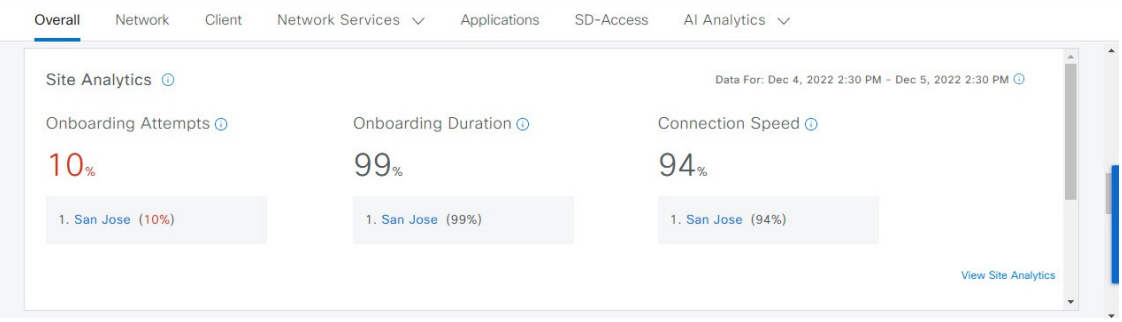
The **Overall** health dashboard has a **Site Analytics** dashlet, which shows the scores of your KPIs. If the performance of any of these KPIs dips below your configured threshold, the sites with the lowest performance are displayed. From the **Site Analytics** dashboard, you can drill down to the floor and device level to pinpoint exactly where the issue is, when it happened, and what the root cause is.

Let's look at this example to determine what the issue is, when it happened, and where.

You set the onboarding attempts KPI to 85%. This KPI means that if at least 85 out of 100 onboarding attempts succeed, the site meets its performance criteria, at least in this KPI category.

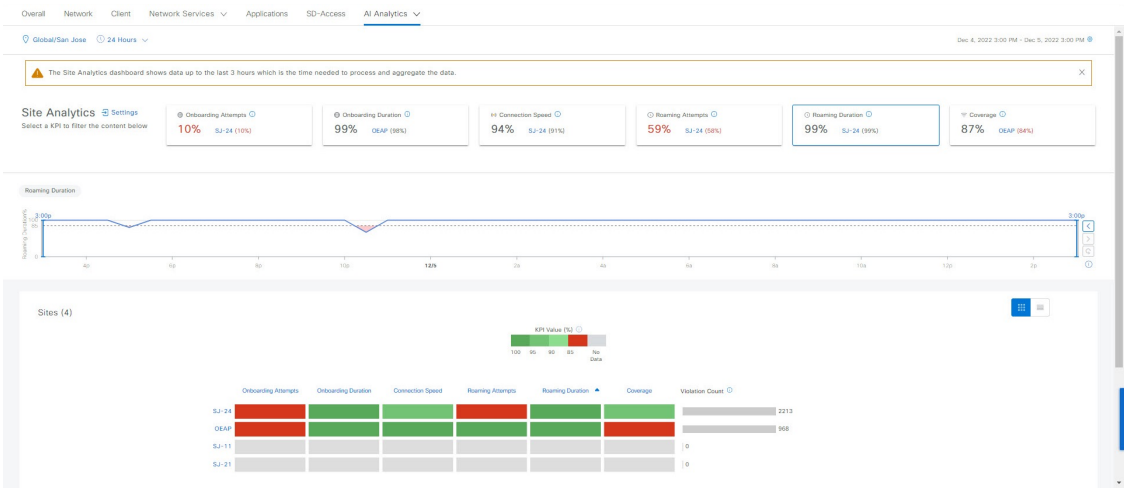
From the **Overall** health dashboard, with the Global drop-down list (Global) set to **Global**, the **Site Analytics** dashlet shows that the San Jose site is the worst performing site with only 10% of the onboarding attempts being successful. This percentage means that 10 out of 100 onboarding attempts were successful. To learn more about how a KPI is calculated, hover your cursor over the **i** icon next to the KPI name.

Figure 27: Overall health dashboard showing site analytics dashlet



To find out where the impact is and what is contributing to the failure, you can click the name of the site, San Jose. The **Site Analytics** dashboard is displayed. Notice that the Global drop-down list (Global) displays **Global/San Jose** as the scope. Analytics for the buildings in the San Jose site are shown, including the worst performing building for each KPI.

Figure 28: Site Analytics for a site showing timeline slider and heatmap graphic

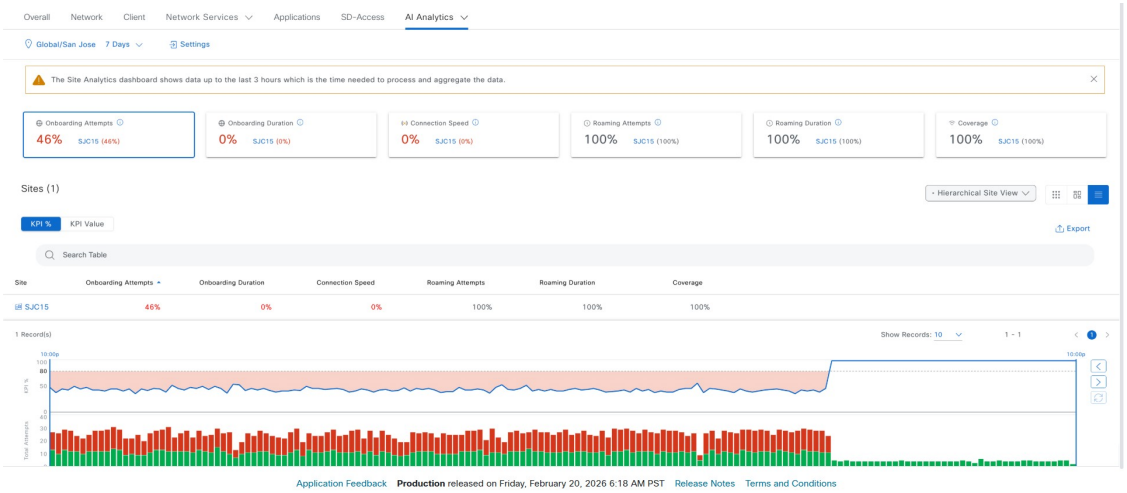


In the timeline slider, the baseline is at 85%, and the trendline shows the percentage of successful onboarding attempts over a 24-hour period (as set in the time-range setting (24 Hours).

So, the San Jose site has an onboarding issue, but where specifically? Below the timeline slider is a heatmap that shows color-coded data. The green bars indicate degrees of success based on the percentage of the KPI value. Darker green signifies a higher percentage of success and lighter green signifies a lower percentage of success. Red bars indicate failed KPIs, and gray bars indicate no data. The **Violation Count** indicates the raw number of KPI failures for a building.

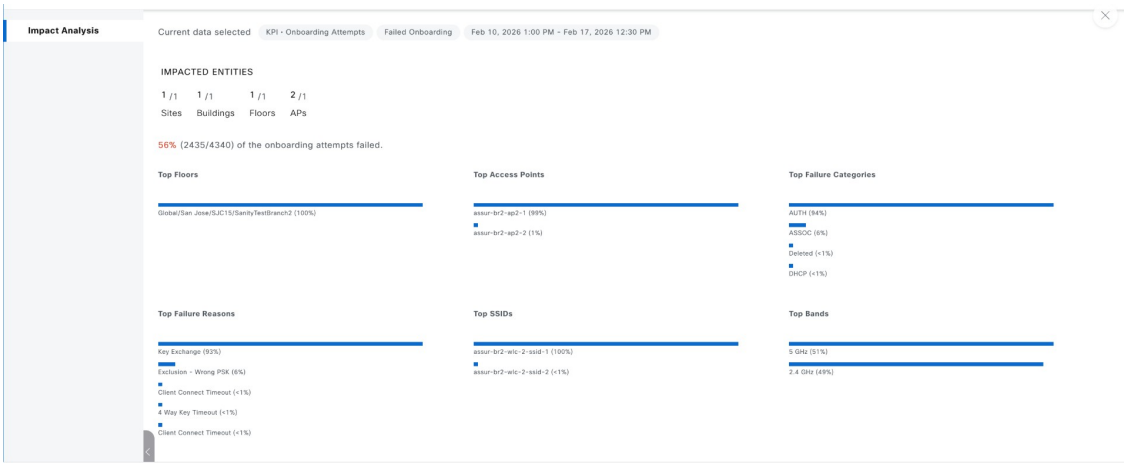
Hover your cursor over the red bars to display information about the site and the particular KPI. Alternatively, click the **List View** toggle button ( ) to display the details for all the buildings and KPIs.

Figure 29: Site Analytics for a site showing timeline slider and heatmap table



According to the data shown, building SJ-24 has the highest onboarding attempts failures. To see the impact analysis, click the name of the building, in this case SJ-24.

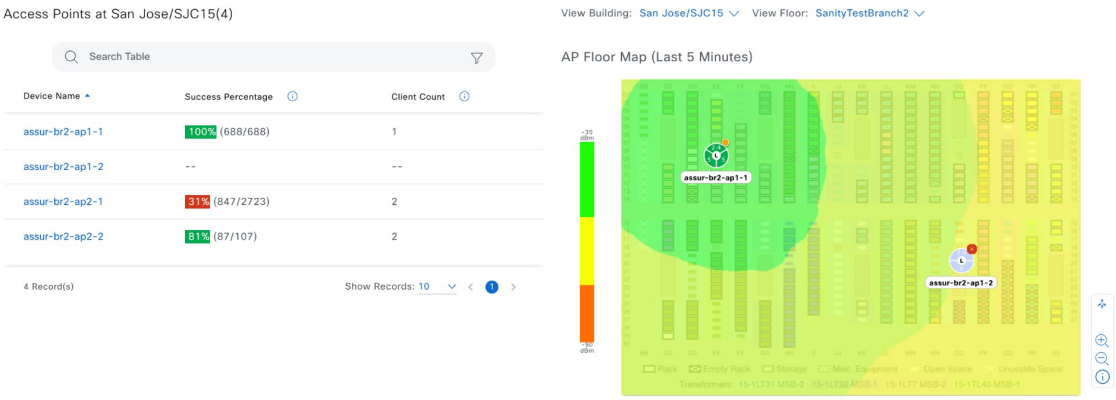
Figure 30: Site Analytics for a building showing the impact analysis



The **Site Analytics** dashboard for the floors is displayed, including the **Impact Analysis** dashlet with various information, such as the top floors, top access points, top failure categories, top failure reasons, and so on.

Scroll down to see the AP floor map.

Figure 31: Site Analytics for a floor showing the Access Points table and floor heatmap



The **View Floor** drop-down list shows the floor that is selected.

The table shows the devices on the selected floor, the percentage of successful onboarding attempts, and the number of clients that were successfully able to onboard.

In the floor heatmap, hover your cursor over an AP to display more information about it. To the right of the heatmap is a toolbar. If you are unfamiliar with the icons on the heatmap, click the **i** icon to display the map legend.

Click a device in the table to display the **Device 360** window for that device. For example, click the SJC24-11A-AP10 device, which has a 45% successful onboarding. The **Device 360** shows very detailed information to help you troubleshoot the issue further. For information, see Monitor and troubleshoot the health of a device, on page 95.

View Site Analytics

Monitor and troubleshoot issues pertaining to onboarding, roaming, connection rates, and wireless coverage for sites, buildings, and floors.

Before you begin

- AI Network Analytics must be enabled for site analytics data to be collected. Click the **Enable AI Network Analytics** link to go directly to the **Cisco AI Analytics** window where you can configure this system setting. For more information, see Configure Cisco AI Network Analytics, on page 77.

  If AI Network Analytics isn't enabled, Assurance displays an example dashlet with sample data.

- Configure site analytic settings. For details, see Configure Site Analytics settings, on page 238.

Procedure

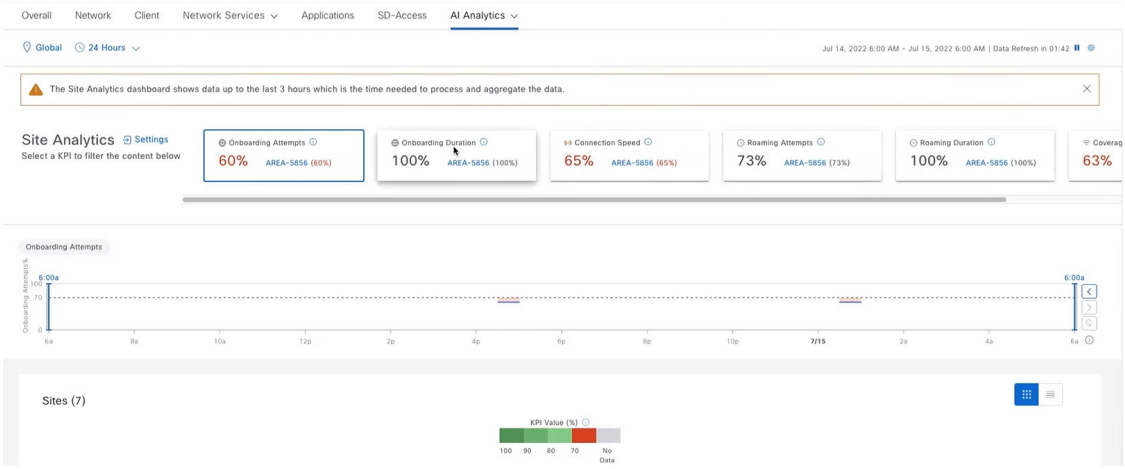
Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Choose **AI Analytics** > **Site Analytics**.

The **Site Analytics** health dashboard appears. The information that is displayed depends on the location chosen in the Global drop-down list (Global). If a Global is selected, all of the sites in the network are shown. If a site is selected, all of the buildings in the site are shown. If a building is selected, all of the floors in the building are shown. For the purposes of explaining Site Analytics in this guide, we begin with the Global location.

Figure 32: Site Analytics health dashboard



Step 3 Use the top menu bar for this functionality:

Item	Description
Global **Location** pane	• Click Global to choose the site, building, or floor from the Site hierarchy.
Time range	Enables you to display data for the last 3 hours, 24 hours, or 7 days.

Step 4 In the **Site Analytics** area (at the Global or site level), do one of these tasks:

- Click a KPI category. The timeline slider is updated to reflect the KPI that you have chosen.

  Each KPI category includes the aggregated KPI value (as a percentage) and the sites or buildings with the lowest performance in each category. These categories are available:

  - **Onboarding Attempts**: Measures the percentage of wireless clients that are able to successfully onboard to an AP in the given site. An SLA is met when a wireless client successfully joins the network, and an SLA is a failure when a wireless client doesn't successfully join the network. For example, 100 clients attempt to onboard to the network. 50 clients onboard successfully, and 50 fail to onboard. The **Onboarding Attempts** KPI value is 50%.
  - **Onboarding Duration**: Measures the percentage of successfully onboarded wireless clients that are able to onboard to an AP within the configured threshold time. If a wireless client fails to onboard, it is not counted in the metric. If a wireless client successfully onboards, but takes longer than the configured SLA duration, it is counted as a failure. For example, out of the 50 clients who onboarded successfully, 30 clients took less than 10 seconds, and 20 clients took more than 10 seconds. So, the **Onboarding Duration** KPI value is 60%.
  - **Roaming Attempts**: Measures the percentage of wireless clients that are able to successfully roam from one AP to another AP in the given site. An SLA is met when a wireless client successfully roams and joins the network via another AP, and is considered a failure when the wireless client doesn't successfully join the network. For example, 100 clients attempted to roam in a given duration. 50 clients roamed successfully, and 50 failed to roam. The **Roaming Attempts** KPI value is 50%.
  - **Roaming Duration**: Measures the percentage of wireless clients that are able to successfully roam from one AP to another AP within the configured threshold time. If a wireless client fails to roam successfully, it is not counted in this metric. If a wireless client successfully roams, but takes longer than the configured threshold for roaming duration, it is counted as a failure. For example, out of the 50 clients who roamed successfully, 30 clients took less than10 seconds, and 20 clients took more than 10 seconds. The **Roaming Duration** KPI value is 60%.
  - **Connection Speed**: Measures the percentage of time that wireless clients have data traffic with over-the-air data rates that are higher than the configured threshold rate. For example, among the data rates sampled by the controller for the 50 successfully onboarded clients, 200 samples were higher than the threshold of 11 Mbps and 50 samples were lower. The **Connection Speed** KPI value is 80%.
  - **Coverage**: Measures the percentage of time that wireless clients have data traffic with RSSI values that are higher than the configured threshold value. For example, among the RSSI values of the 50 successfully onboarded clients sampled by the controller, 200 samples were higher than the threshold of -72 dBm and 50 samples were lower. The **Coverage** KPI value is 80%.

- To display information about a site or building and its performance, click the site or building name in the KPI category.
- To view information about a KPI category in the timeline slider, click the KPI category.

Step 5 Use the timeline slider with the stacked chart, to display information about the selected KPI for the selected time range.

Use the timeline slider to view this information:

- The dotted horizontal line in the timeline and the stacked chart represents the configured threshold value.
- Hover your cursor within the timeline to view the KPI percentage for a specific time range.
- Hover your cursor over the chart to view the KPI information for a specific time range, for example, **Onboarding Attempts** are represented using these color codes:
  - : Total number of good attempts
  - - Total number of poor attempts
  - - % of onboarding attempts
- Click and drag the timeline boundary lines to specify the time range. This sets the context for KPI data that is displayed below the timeline.
- Use the arrow buttons on the right of the timeline to view data for up to 30 days.

Step 6 In the **Site** area, use the heatmap view for this information:

Items	Description
 Heatmap view	Click this toggle button to display the data for the corresponding KPI values in the Heatmap view. Choose the **Hierarchical Site** or **Building** view from the drop-down list to display the corresponding building or site level heatmap data. Heatmap data is color coded. Green bars indicate degrees of success based on the percentage of the KPI value. Red bars indicate failed KPIs, and grey bars indicate no data. **Violation Count** indicates the raw number of KPI failures for a particular site or building. Click the down arrow next to a KPI column to sort the KPI in ascending or descending order. The order is based on the violation count.
Summary dashlet	You can view the number of impacted entities such as sites, buildings, floors, and APs. The color-coded charts show the distributions and insights for the entities based on the KPIs. Click View Details to open a slide-in pane with additional details.

Step 7 In the **Site** area, use the Bubble view for this information:

Items	Description
 Bubble view	Click this toggle button to display the data for the corresponding KPI values in Bubble view. You can choose the Hierarchical Site or Building view from the drop-down list to display the corresponding building-level or site-level heatmap data. Use the **Count** drop-down list to filter the KPI data displayed in the bubble chart based on **AP Count** or **Client Count**. Bubble chart data is color-coded. Green circle indicates degrees of success based on the percentage of the KPI value. Red circle indicates failed KPIs. Grey circle indicates no data. The size of the circle represents the number of clients and APs connected. A small circle has a lower client count and a large circle has a higher client count. Hover your cursor over a bubble chart to display details. In the **Summary** dashlet, you can view the number of impacted entities such as sites, buildings, floors, and APs. The color-coded charts show the distributions and insights for the entities based on the KPIs. Click **View Details** to open a slide-in pane with additional details.

Step 8 In the **Site** area, use the Table view for this information:

Items	Description
 Table view	Click this toggle button to display data about the specific site or building for the KPI categories, in table format. You can choose the **Hierarchical Site** or **Building** view from the drop-down list to display the building-level or site-level data for each KPI. Click **Export** to export the table to a CSV file.
Summary dashlet	You can view the number of impacted entities such as sites, buildings, floors, and APs. The color-coded charts show the distributions and insights for the entities based on the KPIs. Click **View Details** to open a slide-in pane with additional details.

Step 9 Drill down to the building-level view by clicking a building name in either the **Site Analytics** area or in the heatmap.

The building-level view includes these additional areas:

- **Impact Analysis**: The information that is displayed depends on the KPI category that is selected. For example, if the **Onboarding Attempts** category is selected, the information in the **Impact Analysis** area relates to the onboarding attempt failures. The information includes top access points, top failure categories, top SSIDs, top bands, and so on.

- **Access Points** table: For the floor in the **View Floor** drop-down list, the APs, onboarding attempts, and client counts are shown. The client count for each AP is the number of distinct clients that have connected to the network over the selected time range.

  To display the **Device 360** view for a particular device, click the device name.

- **AP Floor Map (Last 5 Minutes)**: For the floor chosen from the **View Floor** drop-down list, the heatmap displays a floor map view, showing the existing APs and their status.

  In the heatmap, hover your cursor over an AP to display more information about it. To the right of the heatmap is a toolbar where you can view the status of the wireless controller and zoom in and out. If you are unfamiliar with the icons on the heatmap, click the **i** icon to view the map's legend.

Configure Site Analytics settings

This procedure shows you how to configure the thresholds for key client performance metrics.

Procedure

Step 1 From the main menu, choose **Assurance** > **Site Analytics Settings**.

The **Site Analytics Settings** window appears.

Step 2 To change the threshold **KPI Value %**, do these steps:

a) Click **Edit**.

b) In the slide-in pane, enter the target percentage for the site performance metrics. This threshold defines a healthy percentage of KPI data points for any site. The target for green (GOOD) is 100% and cannot be changed. The target for red (POOR) must be a number between 0 and 95. These target values affect all the client performance metrics.

Step 3 From the **KPI Name** column, click the KPI name link.

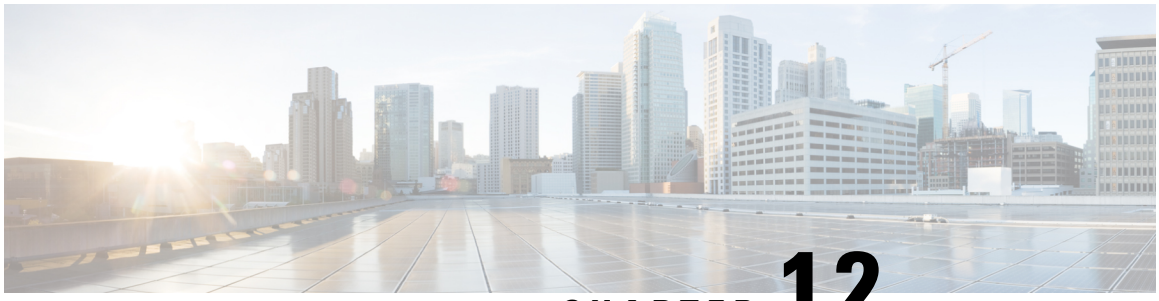
The slide-in pane for the KPI appears.

Step 4 Configure the KPI threshold settings:

- If the KPI threshold is quantitative, you can customize the threshold value for what is considered a good health score.
- To return to the default setting, click **View Default Setting**.

Step 5 Click **Apply**.

A confirmation dialog box appears.



CHAPTER 12

View and Manage Issues

- About issues, on page 239
- About the Machine Reasoning Engine, on page 240
- About the Layer 2 Loop issue involving VLANs, on page 240
- View open issues, on page 241
- Troubleshoot wired client issues using MRE, on page 254
- View resolved issues, on page 257
- View ignored issues, on page 259
- Resolve or ignore issues, on page 261
- No Activity on Radio issue triggers, on page 262
- Automatic issue resolution, on page 263
- Manage global issue settings, on page 266
- Manage user-defined issue settings, on page 267
- Manage Custom Issue Settings, on page 269
- Enable issue notifications, on page 270
- Assurance, Cisco AI Network Analytics, and MRE issues, on page 273

About issues

Assurance provides both system-guided as well as self-guided troubleshooting. For a large number of issues, Assurance provides a system-guided approach. It correlates multiple Key Performance Indicators (KPIs), uses results from tests and sensors to determine the root cause of the problem, and then possible actions to resolve the issues. The focus is on highlighting an issue rather than monitoring data. Quite frequently, Assurance does the work of a Level 3 support engineer.

With Catalyst Center, you can view and troubleshoot AI-driven issues using Cisco AI Network Analytics. Cisco AI Network Analytics leverages a cloud-based learning platform with advanced artificial intelligence (AI) and machine learning (ML) technologies to provide intelligent issue detection and analysis. It detects anomalies to determine their root causes and ease troubleshooting.

Cisco AI Network Analytics can detect these types of cloud-based AI-driven issues:

- **Connection Issues** (Onboarding Issues): Excessive Time, Excessive Failures, Excessive Association Time, Excessive Association Failures, Excessive Authentication Time, Excessive Authentication Failures, Excessive DHCP Time, and Excessive DHCP Failures

- **Application Experience Issues**: Total Radio Throughput, Media Application Throughput, Cloud Application Throughput, Collab Application Throughput, and Social Application Throughput.

Note Unlike standard Assurance issues, AI-generated issues are not displayed instantly in the GUI. AI-generated issues undergo cloud-side batch processing before being polled and ingested by the Catalyst Center appliance. Due to this multi-step process, you should expect a delay of up to 5 hours before AI-generated issues appear in the GUI.

About the Machine Reasoning Engine

The Machine Reasoning Engine (MRE) is a network automation engine that uses artificial intelligence (AI) to automate complex network operation workflows. It encapsulates human knowledge and expertise into a fully automated inference engine to help you perform complex root cause analysis, detect issues and vulnerabilities, and either manually or automatically perform corrective actions. MRE is powered by a cloud-hosted knowledge base, built by Cisco networking experts.

You can use the MRE to troubleshoot wired client, Layer 2 loop, and PoE issues. For the list of issues, see MRE issues, on page 289.

For procedures, see Troubleshoot wired client issues using MRE, on page 254, Issue Instance Details for Layer 2 Loop issue, on page 249, and Issue Instance Details for a PoE issue, on page 251.

About the Layer 2 Loop issue involving VLANs

A Layer 2 Loop issue occurs when a forwarding loop forms in the path of one or more VLANs. In this case, packets are forwarded and multiplied indefinitely along the affected path, until the links and devices reach maximum capacity. A broadcast storm occurs and the entire Layer 2 network shuts down very quickly. The MRE enables you to troubleshoot the Layer 2 Loop issue by:

- Viewing the VLANs and ports that are involved in the probable loop.
- Viewing the devices that are associated with the loop.

Note The scale constraints for the Layer 2 loop include:

- The number of VLANs is 10.
- The number of devices per VLAN is 30.

Important Currently, the MRE does not perform root cause analysis on Layer 2 loops that occur as a result of unmanaged network devices, virtual machines, or other entities that are not part of the topology known to Catalyst Center.

View open issues

Use this procedure to view all open issues, which fall under these categories:

- **Threshold-based issues**: Issues detected by Assurance.
- **AI-Driven Issues**: Issues detected by Cisco AI Network Analytics. These issues are triggered based on deviations from the predicted baseline for your specific network environment.

  If you have installed and configured the Cisco AI Network Analytics application with Catalyst Center, you can view these types of cloud-based, AI-driven issues:

  - **Connection Issues** (Onboarding Issues): Excessive Time, Excessive Failures, Excessive Association Time, Excessive Association Failures, Excessive Authentication Time, Excessive Authentication Failures, Excessive DHCP Time, and Excessive DHCP Failures.



Note For Connection issues to display, make sure that the APs are properly assigned to sites.

  - **Application Experience Issues**: Total Radio Throughput, Media Application Throughput, Cloud Application Throughput, Collab Application Throughput, and Social Application Throughput.



Note For Application Experience issues to display, make sure that Application Visibility and Control (AVC) is enabled on the wireless controllers. The throughput issues rely on the AVC data for baselining and anomaly detection.

- **Layer 2 Loop Issue** and **PoE Issue**: Issues detected by Assurance that you can troubleshoot using the MRE workflow. See About the Machine Reasoning Engine, on page 240.

Before you begin

- To view AI-driven, cloud-based issues that use artificial intelligence (AI) and machine learning (ML) technologies to provide intelligent issue detection and analysis, make sure that you have configured Cisco AI Network Analytics data collection. See Configure Cisco AI Network Analytics, on page 77.
- To view syslog messages, make sure that you have configured syslog. See Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry, on page 76.

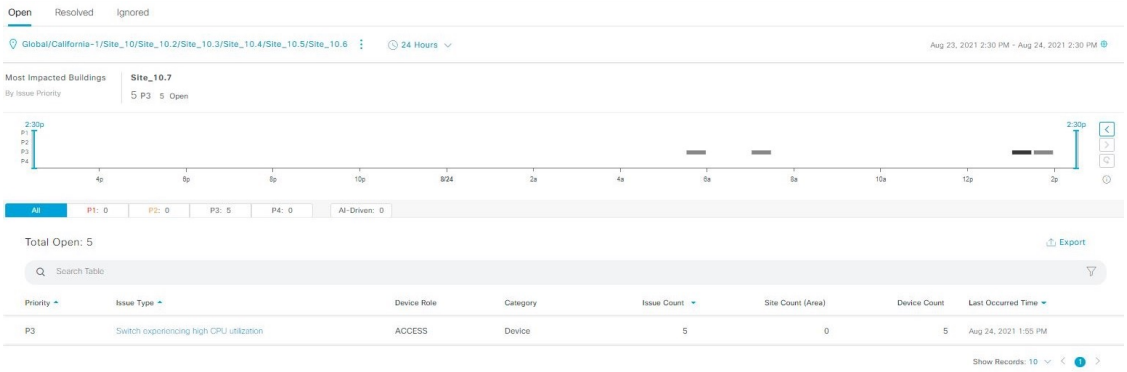
Procedure

Step 1 Do one of these tasks:

- From the Catalyst Center home page, in the **Assurance Summary** > **Critical Issues** area, choose **View Details**.
- From the main menu, choose **Assurance** > **Issues and Events**.

The **Open Issues** dashboard appears with this information:

Figure 33: Open Issues dashboard



Open Issues dashboard	
Item	**Description**
Global	• Click Global in the top menu bar to choose the site, building, or floor from the Site hierarchy. • Click next to the location icon and choose **Site Table** to view the Sites table. • Choose **Hierarchical Site View** or **Building View** from the drop-down list. Based on what you choose, the table is refreshed. • From the **Go to sites** column, click for a site or building to display data only for that location on the **Open Issues** dashboard.
24 Hours **Time Range** setting	Allows you to display information on the window based on the time range you select. The default is **24 Hours**. Do these steps: **a.** From the **24 Hours** drop-down list, choose a time range: **3 hours**, **24 hours**, or **7 days**. **b.** Specify the **Start Date** and time, and the **End Date** and time. **c.** Click **Apply**. This sets the range of the timeline.

Open Issues dashboard	
Item	**Description**
Timeline Slider	Allows you to specify a more granular time range. Click and drag the timeline boundary lines to specify the time range. The colors represent the issue priority: : P1 : P2 : P3 and P4 **Note** The intensity of the color indicates its significance, whether more or fewer issues have occurred for that priority level. For example, a lighter shade of yellow indicates fewer P2 issues (still open) than a deeper shade of yellow.
Most Impacted Locations by Issue Priority	Provides information about the areas that are most impacted based on issue priority. Click the hyperlinked location hierarchy to find the impacted areas, buildings, floors, and outdoor areas where the issue occurred.

Step 2 Click the **All**, **P1**, **P2**, **P3**, **P4**, or **AI-Driven** toggle to display a list of issues in that category in the **Issue Type** table.

The **AI-Driven** toggle only works when a Cloud Agent is active. If the Cloud Agent is not running, the toggle will be disabled.

Issue type table in the Open Issues window	
Item	**Description**
Total Open	Provides the total count of open issues that require action. The **Total Open** value changes depending on the tab you choose. Options are **All** (the default), **P1**, **P2**, **P3**, **P4**, and **AI-Driven**.
Priority	Preassigned priority level of the issue type.
Issue Type	Type of issue. **Note** For AI-driven issues, the AI icon appears in front of the issue type.
Device Role	Role assigned to the device on which the issue was detected. The role is Access, Core, Distribution, Border Router, or Unknown.
Category	Category under which the issue type falls, such as Connectivity, Availability, Onboarding, and Utilization.
Issue Count	Number of times this type of issue occurred.
Site Count (Area)	Number of sites where this type of issue occurred.
Device Count	Number of devices that were impacted by this type of issue.
Last Occurred Time	Most recent date and time this issue occurred.

Step 3 From the **Issue Type** table, click an issue type.

The first slide-in pane, **Issue Instances**, lists all the issues for that issue type with this information:

Issue instances (first slide-in pane)	
Item	**Description**
Open Issues	Number of open issues for that issue type.
Area	Number of buildings and floors that are impacted by the issue.
Device	Number of devices that are impacted by the issue.
Actions drop-down list	Allows you to resolve or ignore a single issue or a bulk of issues at a time. See Resolve or ignore issues, on page 261.
Issue	Description of the issue. If you're an admin user, you can add, edit, and delete notes. Click the Note icon ( ) and then click **Add**. If you're any other type of user, you can only view note information.
Site	Site, building, or floor that was impacted by the issue.
Device	Device that was impacted by the issue. Click the device name to open the **Device 360** window.
Device Type	Type of device that was impacted by the issue.
Issue Count	Number of times this type of issue occurred.
Last Occurred Time	Date and time this issue occurred.
Last Updated Time	Date and time this issue was last updated.
Updated By	Name of the entity who updated this issue.

Step 4 From the **Issue** column in the **Issue Instances** slide-in pane, click an issue.

A second slide-in pane, **Issue Instance Details**, provides specific details about the issue. Depending on the issue, the description and suggested actions are displayed. See these sections for more details about these issues:

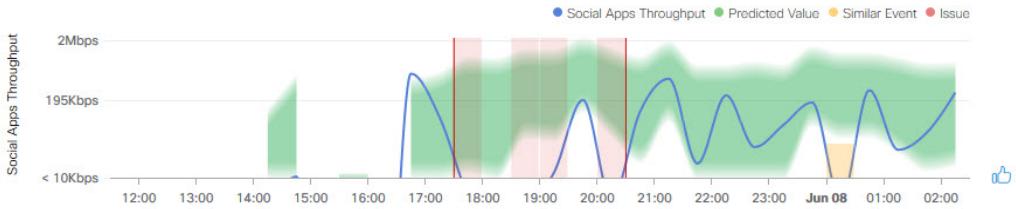
- Issue Instance Details for AI-driven issues, on page 245
- Issue Instance Details for AP-Disconnect Issues, on page 248
- Issue Instance Details for Layer 2 Loop issue, on page 249
- Issue Instance Details for a PoE issue, on page 251

Issue Instance Details for AI-driven issues

Note The **Issue Instance Details** slide-in pane is part of the **Open Issues** workflow. See Step 4 in View open issues, on page 241.

For AI-driven issues, the **Issue Instance Details** (second slide-in pane) provides this information:

Issue Instance Details (second slide-in pane)	
Item	**Description**
Description	Description of the issue.
Status drop-down list	Allows you to change the status of the issue. Do these tasks: • To resolve an issue, from the **Status** drop-down list, select **Resolve**. • To stop an issue from being reported: 1. From the **Status** drop-down list, select **Ignore**. 2. Set the number of hours to ignore the issue on the slider, and then click **Confirm**.
Note icon ( )	If you're an admin user, you can add, edit, and delete notes. Click the Note icon ( ) and then click **Add**. If you're any other type of user, you can only view note information.
Summary area	Brief summary of the issue, which can include information such as the radios that are impacted, the location of the radios, the time and date the issue occurred, and the location of the issue.
Impacted Summary for this Network	Displays information about the location that was impacted and the number of clients that were impacted by the issue.
Feedback icon	Click the icon to provide your comments on whether the information on this page was helpful, and then click **Submit**.

Issue Instance Details (second slide-in pane)	
Item	**Description**
Problem	Provides brief text that describes the problem along with a chart that provides a visual of how the actual KPI value deviated from the predicted normal behavior. By default, the chart is zoomed-in, 6 hours before and 6 hours after the issue, as shown in this figure: ***Figure 34: Problem chart***  The chart details for the AI-driven issues are represented by different colors. • **Green band**: Predicted normal behavior for your network based on machine learning. • **Solid blue line**: Actual KPI value. • **Vertical red line or bars**: Indicates an issue. When the blue line (actual KPI value) falls outside the green band (predicted normal behavior), an issue is raised. • **Vertical yellow bars**: Indicates that a similar event has occurred. Hover and move your cursor over the charts to view synchronized information, such as the KPI value, the predicted lower value, and the predicted upper value at a selected point in time.
Impact	Provides information about the connected clients, APs, devices, and applications that are impacted by the issue. For Excessive Onboarding Time and Failures; and Excessive DHCP, Association, or Authentication Time and Failures, these tabs are provided: **Impacted Clients** and **Top 10 Impacted APs**. For Total Radio Throughput and Applications Throughput (Cloud, Collab, Media, and Social), these tabs are provided: **Impacted Clients**, **Device Breakout**, and **Applications by TX/RX**. Click the tab to update the chart and the table below the chart.

Issue Instance Details (second slide-in pane)	
Item	**Description**
Root Cause Analysis	Provides the issue along with the probable network causes for that issue, displayed in charts, as shown in this figure: ***Figure 35: Root cause analysis charts***  For Excessive Onboarding Time and Failures, these tabs are provided: **Network Causes**, **Failed Distribution**, **Failed Percentage**, and **Failed Count**. For Excessive DHCP, Association, or Authentication Time, these tabs are provided: **Network Causes**, **Top Impacted APs**, and **Top Impacted Times**. For Excessive DHCP, Association, or Authentication Failures, these tabs are provided: **Network Causes**, **Top Impacted APs**, and **Top Impacted Failures**. For Total Radio Throughput and Applications Throughput (Cloud, Collab, Media, and Social), these tabs are provided: **Network Causes**. Click the tab to update the charts below. To view the charts for additional KPIs, click the **KPI** icon, select the KPI, and then click **Apply**.
Suggested Actions	Provides the actions you can take to resolve the issue.

Issue Instance Details for AP-Disconnect Issues

Note The **Issue Instance Details** slide-in pane is part of the **Open Issues** workflow. See Step 4 in View open issues, on page 241.

For AP-Disconnect issues, the **Issue Instance Details** (second slide-in pane) provides this information:

AP-Disconnect Issue Instance Details (second slide-in pane)	
Item	**Description**
Status drop-down list	• To resolve an issue, from the **Status** drop-down list, select **Resolve**. • To stop an issue from being reported: 1. From the **Status** drop-down list, select **Ignore**. 2. Set the number of hours to ignore the issue on the slider, and then click **Confirm**.
Note icon ( )	If you're an admin user, you can add, edit, and delete notes. Click the Note icon ( ) and then click **Add**. If you're any other type of user, you can only view note information.
Insights	Provides a brief summary of the issue, which can include information such as the switch that is impacted, the date and time of the issue, and the location of the switch.
Impact Summary	Displays the counts of impacted sites, clients, and APs.
Problem Details	Provides these details: • Description of the devices involved with the issue, if known. • Related issue, if any, with a link directly to the issue details. • Details about the problem, such as the impacted APs, their location and power information, and the reason for the disconnect. • Physical neighbor topology, which includes the switch and the neighboring devices that are connected to it.
Impact Details	Lists the wireless clients that were connected to the impacted APs and their locations.
Suggested Actions	Provides the actions you can take to resolve the issue.

Issue Instance Details for Layer 2 Loop issue

Note The **Issue Instance Details** slide-in pane is part of the **Open Issues** workflow. See Step 4 in View open issues, on page 241.

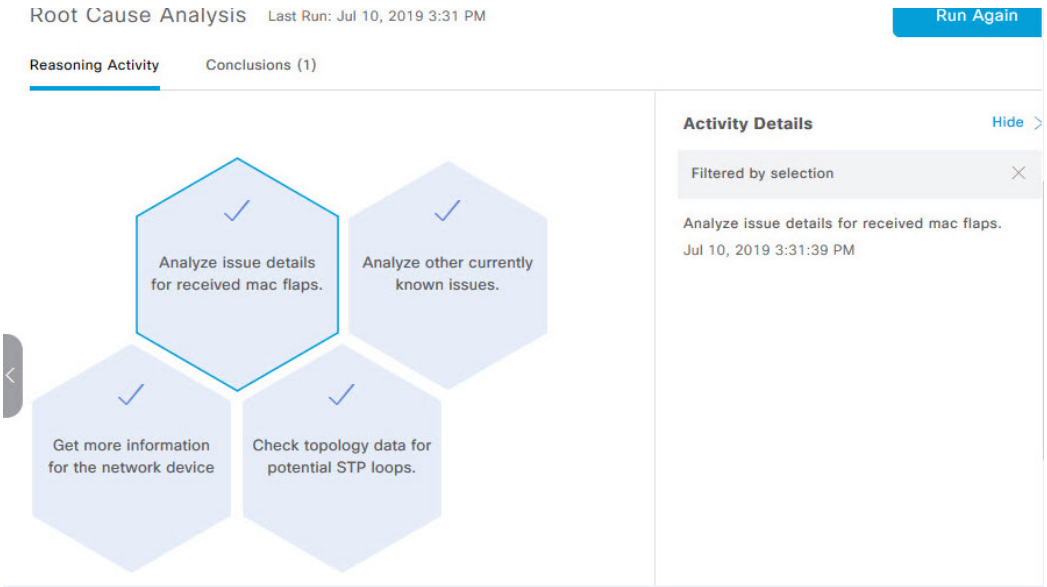
To understand the Layer 2 Loop issue and the Machine Reasoning Engine, see About the Machine Reasoning Engine, on page 240.

Note The scale constraints for the Layer 2 Loop include:

- Number of VLANS is 10.
- Number of devices per VLAN is 30.

For the Layer 2 Loop issue, which supports Machine Reasoning, the **Issue Instance Details** slide-in pane contains this information:

Issue Instance Details (second slide-in pane)	
Item	**Description**
Status drop-down list	Allows you to change the status of the issue. Do these tasks: • To resolve an issue, from the **Status** drop-down list, select **Resolve**. • To stop an issue from being reported: 1. From the **Status** drop-down list, select **Ignore**. 2. Set the number of hours to ignore the issue on the slider, and then click **Confirm**.
Note icon ( )	If you're an admin user, you can add, edit, and delete notes. Click the Note icon ( ) and then click **Add**. If you're any other type of user, you can only view note information.
Summary	Brief summary of the issue, which can include information, such as device, role, time, location. and potential root cause. This also provides the initial assessment, such as the VLANs and ports in the potential loop.
Problem Details	Provides a brief text that describes the problem along with these tasks: • **Relevant Events** drop-down list: Lists the events that occurred during the loop. Click an event to view details in the side pane. • **Potential Loop Details** drop-down list: Provides loop information, such as the device, role, port in the loop, duplex mode, and VLAN that was involved in the loop.

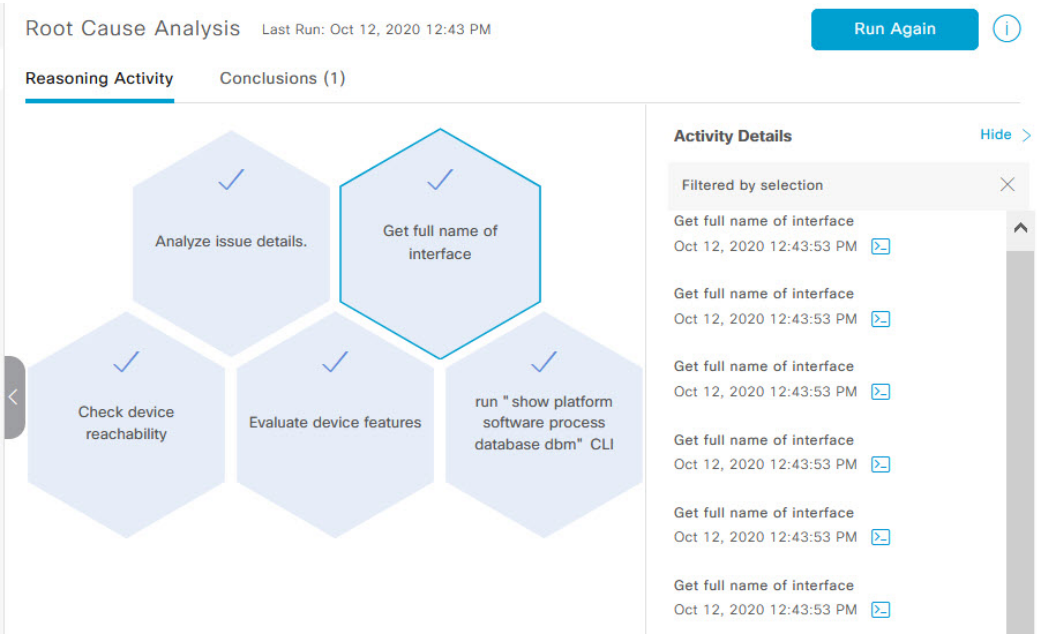
Issue Instance Details (second slide-in pane)	
Item	**Description**
Root Cause Analysis	The Machine Reasoning Engine (MRE) allows you to perform complex root cause analysis and suggests corrective actions. 1. Click **Run Machine Reasoning** to allow the MRE to start troubleshooting. After the troubleshooting is completed, the **Machine Reasoning Completed** pop-up dialog box appears. 2. In the pop-up dialog box, click **View Details**. The **Root Cause Analysis** area appears with the **Conclusions** tab opened by default providing the details of the root cause analysis. 3. From the **Conclusions** area, click **View Relevant Activities** to view activity details. The activity shows commands that were used at each step of the root cause analysis. 4. Click the  icon to provide your feedback, whether the information on this page was helpful or not, and then click **Submit**. 5. Click the **Reasoning Activity** tab to understand how the MRE reached that conclusion. Each reasoning activity is provided in hexagon shaped blocks as shown in this figure. Click each hexagon shaped block to view activity details in the right pane. To cancel the reasoning activity while it is running, click **Stop**. **Note** The check mark indicates that the step is complete. ***Figure 36: Reasoning activity***  6. Click **Run Again** if you want to rerun the MRE.
Topology icon	Click the  icon to view the topology of the network segment in which the loop occurred.

Issue Instance Details for a PoE issue

Note The **Issue Instance Details** slide-in pane is part of the **Open Issues** workflow. See Step 4 in View open issues, on page 241.

For a PoE issue, which supports Machine Reasoning, the Issue Instance Details slide-in pane contains this information:

Issue Instance Details (second slide-in pane)	
Item	**Description**
Status drop-down list	Allows you to change the status of the issue. Do these tasks: • To resolve an issue, from the **Status** drop-down list, select **Resolve**. • To stop an issue from being reported: 1. From the **Status** drop-down list, select **Ignore**. 2. Using the slider, set the number of hours to ignore the issue and click **Confirm**.
Note icon ( )	If you're an admin user, you can add, edit, and delete notes. Click the Note icon ( ) and then click **Add**. If you're any other type of user, you can only view note information.
Summary	Summary of the issue, which can include information, such as device, role, time, location, and potential root cause.
Problem Details	Provides a brief description of the problem along with this information: • **Event Types** tabs: Contains tabs for the types of events that occurred. Click an event tab to view the list of errors for the event type. • **Errors**: Errors that occurred for each event type. The errors are refreshed based on the **Event Types** tab you click. • **Detailed Information** Click an error to view additional information about it.

Issue Instance Details (second slide-in pane)	
Item	**Description**
Root Cause Analysis	The Machine Reasoning Engine (MRE) allows you to do complex root cause analysis and suggests corrective actions. **1.** Click **Run Machine Reasoning** to allow the MRE to start troubleshooting. After the troubleshooting is completed, the **Machine Reasoning Completed** dialog box appears. **2.** In the pop-up dialog box, click **View Details**. The **Root Cause Analysis** area appears with the **Conclusions** tab opened by default providing the details of the root cause analysis. **3.** From the **Conclusions** area, click **View Relevant Activities** to view activity details. The activity shows commands that were used at each step of the root cause analysis. **4.** Click the  icon to provide your feedback, whether the information on this page was helpful or not. **5.** Click the **Reasoning Activity** tab to understand how the MRE reached that conclusion. Each reasoning activity is provided in hexagon shaped blocks as shown in this figure. Click each hexagon shaped block to view **Activity Details** in the right pane. To cancel the reasoning activity while it is running, click **Stop**. **Note** The check mark indicates that the step is complete. ***Figure 37: Reasoning activity***  **6.** Click **Run Again** if you want to rerun the MRE.

Issue Instance Details for Application health degradation issue

A application health degradation issue is a network event indicator that

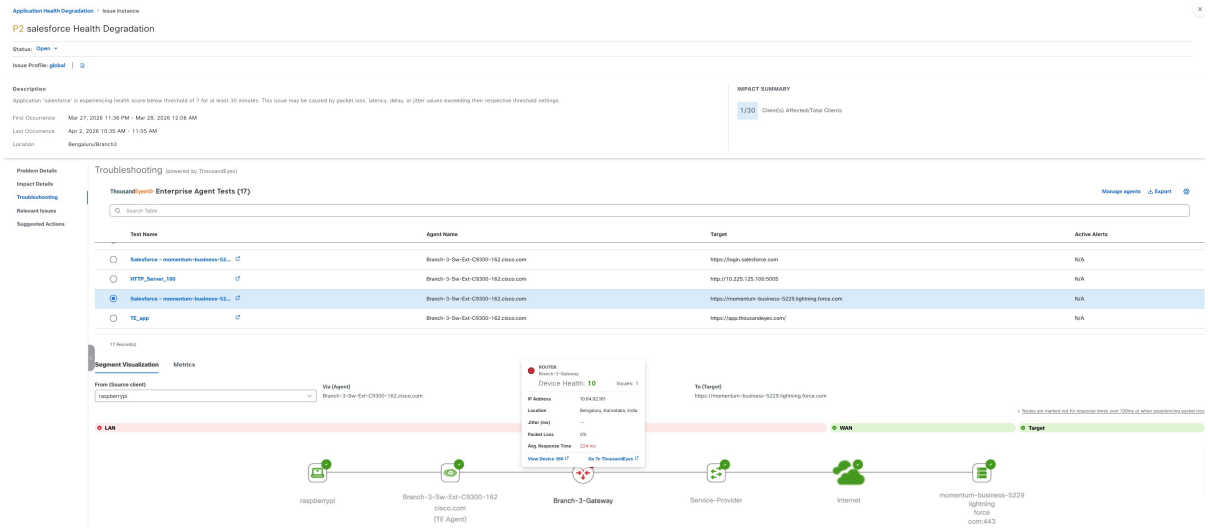
- identifies when an application's health score drops below a configured threshold,
- presents detailed information to help assess client impact and troubleshoot performance causes, and
- integrates data from ThousandEyes to enhance root cause analysis and remediation.

The **Issue Instance Details** slide-in pane is part of the **Open Issues** workflow. See Step 4 in View open issues, on page 241.

For Application Degradation issues, the Issue Instance Details slide-in pane provides this information:

- Status: Displays the current state of the issue.
- Issue Profile: Identifies the configuration profile Global that triggered the issue.
- Description: Summarizes why the issue was raised, including the duration of the degradation and the specific metrics such as packet loss, latency and jitter that exceeded thresholds.
- Occurrences: Shows the First Occurrence and Last Occurrence timestamps.
- Location: Specifies the site or branch where the degradation is occurring.
- Impact Summary: Displays the number of impacted clients relative to the total number of clients using the application at that site.

Figure 38: Issue Instance Details (second slide-in pane)



Issue Instance Details (second slide-in pane)	
Item	**Description**
Status drop-down list	Allows you to change the status of the issue. Do these tasks: • To resolve an issue, from the **Status** drop-down list, select **Resolve**. • To stop an issue from being reported: 1. From the **Status** drop-down list, select **Ignore**. 2. Using the slider, set the number of hours to ignore the issue and click **Confirm**.
Problem Details	View the current application health score and historical performance charts. This tab identifies the specific metrics contributing to the low health score.
Impact Details	Analyze the scope of the issue using bar graphs that display top affected locations, access points (APs), and switches. This tab also provides a list of impacted clients.
Troubleshooting	Use this tab to correlate application health data with ThousandEyes test results: • ThousandEyes Enterprise Agent Tests: View, manage, or export test data associated with the application. • Segment Visualization: Use the hop-by-hop path trace to identify where the issue resides. Nodes with high response times or packet loss are highlighted, allowing you to isolate the problem to the LAN, WAN, or target server.
Suggested Actions	Follow the recommended steps to investigate and resolve the issue.
Relevant Issues	View other active issues within the same location to determine if the application degradation is part of a broader network event.

Troubleshoot wired client issues using MRE

Use this procedure to view wired client issues detected by Assurance and troubleshoot them using the MRE workflow. For a list of wired client issues that support MRE, see MRE issues, on page 289.

Before you begin

Make sure that the MRE knowledge base is updated with the latest knowledge packs. See Update the Machine Reasoning Knowledge Base, on page 80.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Client** tab.

The **Client** health dashboard appears.

Step 3 In the **Wired Clients** summary area, click **View Details** to open a slide-in pane.

Step 4 In the slide-in pane, in the **Wired Clients** chart, click **Authentication** or **DHCP**.

If you click **Authentication**, this information appears below the chart: Top Authentication Failure Reason, Top Location, Top Switch, Top Host Device Type. A table is also displayed, which provides a list of clients that failed authentication.

If you click **DHCP**, this information appears below the chart: Top DHCP Failure Reason, Top Location, Top Switch, Top Host Device Type. A table also appears.

Step 5 Do one of these tasks:

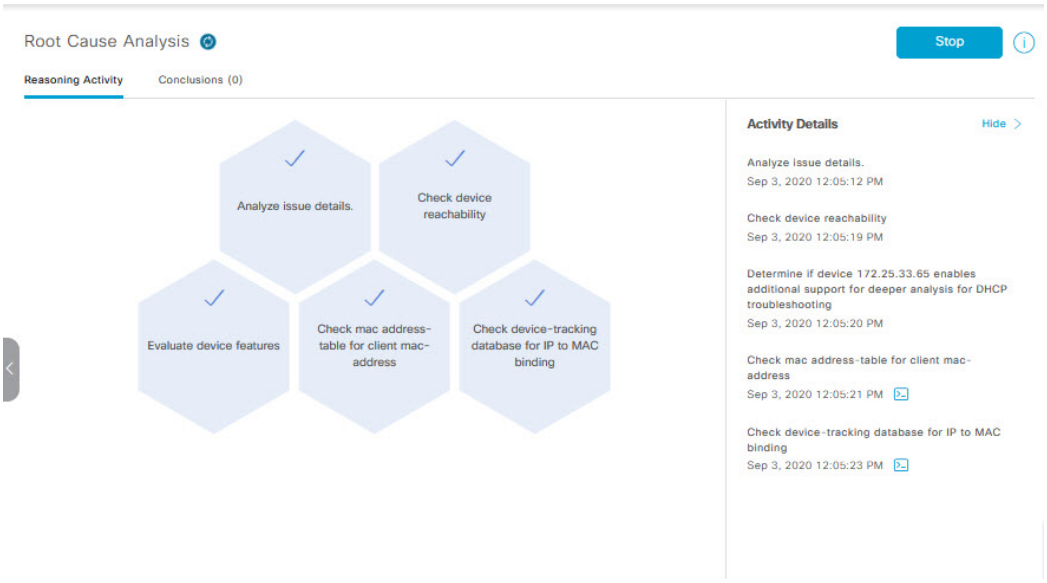
- If you are a user with SUPER-ADMIN-ROLE privileges, enter the client's MAC address in the search tool.
- In the table, from the **Identifier** column, click the hyperlinked identifier.

The **Client 360** window for the client appears.

Step 6 In the **Client 360** window, from the **Issues** dashlet, click an authentication or DHCP issue.

The **Issue Details** window appears with this information:

Issue details	
Item	**Description**
Status drop-down list	Provides the current status of the issue, which you can change. Do these tasks: • To resolve an issue, from the **Status** drop-down list, select **Resolve**. • To stop an issue from being reported: **a.** From the **Status** drop-down list, select **Ignore**. **b.** Set the number of hours to ignore the issue on the slider, and then click **Confirm**.
Note icon ( )	If you're an admin user, you can add, edit, and delete notes. Click the Note icon ( ) and then click **Add**. If you're any other type of user, you can only view note information.
Summary	Brief summary of the issue, which can include information, such as device, role, time, location. and potential root cause.

Issue details	
Item	**Description**
Root Cause Analysis	The Machine Reasoning Engine (MRE) allows you to perform complex root cause analysis and suggests corrective actions. **a.** Click **Run Machine Reasoning** to allow the MRE to start troubleshooting. After the troubleshooting is completed, the **Machine Reasoning Completed** dialog box appears. **b.** In the dialog box, click **View Details**. The **Root Cause Analysis** area appears with the **Conclusions** tab opened by default providing the details of the root cause analysis. **c.** From the **Conclusions** area, click **View Relevant Activities** to view activity details. **d.** Click the icon to provide your feedback, whether the information on this page was helpful or not, and then click **Submit**. **e.** Click the **Reasoning Activity** tab to understand how the MRE reached that conclusion. Each reasoning activity is provided in hexagon shaped blocks, as shown in this figure. Click each hexagon shaped block to view activity details in the right pane. To stop the reasoning activity while it is running, click **Stop**. **Note** The check mark indicates that the step is complete. ***Figure 39: Reasoning activity***  **f.** Click **Run Again** if you want to rerun the MRE.

View resolved issues

Use this procedure to view all resolved issues, which fall under these categories:

- Threshold-based issues: Issues detected by Assurance.
- AI-driven issues: Issues detected by Cisco AI Network Analytics. These issues are triggered based on deviations from the predicted baseline for your specific network environment.

Before you begin

To view AI-driven resolved issues, make sure that you have configured Cisco AI Network Analytics data collection. See Configure Cisco AI Network Analytics, on page 77.

Procedure

Step 1 From the main menu, choose **Assurance** > **Issues and Events**.

The **Open Issues** dashboard appears.

Step 2 From the **Status** drop-down list, select **Resolved**.

The **Resolved Issues** window appears.

Step 3 Use the **Resolved Issues** window to view this information:

Resolved Issues window	
Item	**Description**
Global	• Click Global in the top menu bar to select the site, building, or floor from the Site hierarchy. • Click next to the location icon and select **Site Table** to view the Sites table. • Select **Hierarchical Site View** or **Building View** from the drop-down list. Based on what you select, the table is refreshed. • From the **Go to sites** column, click for a site or building to display data only for that location on the **Resolved Issues** dashboard.

Resolved Issues window	
Item	**Description**
24 Hours drop-down list	Allows you to display information on the window based on the time range you select. The default is **24 Hours**. Do these steps: **a.** From the **24 Hours** drop-down list, select a time range: **3 hours**, **24 hours**, or **7 days**. **b.** Specify the **Start Date** and time and the **End Date** and time. **c.** Click **Apply**. This sets the range of the timeline.
Timeline slider	Allows you to specify a more granular time range. Click and drag the timeline boundary lines to specify the time range.

Step 4 Click the **All**, **P1**, **P2**, **P3**, **P4**, or **AI-Driven** tab to display a list of issues in that category in the **Issue Type** table.

Issue Type Table in the Resolved Issues window	
Item	**Description**
Total Resolved	Provides the total count of resolved issues. The **Total Resolved** value changes depending on the tab you select. Options are **All** (the default), **P1**, **P2**, **P3**, **P4**, and **AI-Driven**.
Priority	Preassigned priority level of the issue type.
Issue Type	Type of issue. **Note** For AI-driven issues, the AI icon appears in front of the issue type.
Device Role	Role assigned to the device on which the issue was detected. Roles are Access, Core, Distribution, Border Router, or Unknown.
Category	Category under which the issue type falls, such as Connectivity, Availability, Onboarding, and Utilization.
Issue Count	Number of times this type of issue occurred.
Site Count (Area)	Number of sites where this type of issue occurred.
Device Count	Number of devices that were impacted by this type of issue.
Last Occurred Time	Most recent date and time this issue occurred.

Step 5 From the **Issue Type** table, click an issue type.

The first slide-in pane, **Issue Instances**, lists all the resolved issues for that issue type and information such as site, device, device type, occurrence, last occurrence timestamp, last updated timestamp, and the name of the entity that updated the issue. If you're an admin user, you can add, edit, and delete notes. Click the Note icon ( ) and then click **Add**. If you're any other type of user, you can only view note information.

If the issue condition no longer exists, the system automatically resolves the issue and displays **System** in the **Updated By** column. See Automatic issue resolution, on page 263.

Step 6 From the **Issue** column in the **Issue Instances** slide-in pane, click an issue.

A second slide-in pane, **Issue Instance Details**, provides details about the issue, the name of the entity that resolved the issue, and the timestamp. Depending on the issue, the description and suggested actions are displayed. If you're an admin user, you can add, edit, and delete notes. Click the Note icon ( ) and then click **Add**. If you're any other type of user, you can only view note information.

View ignored issues

Use this procedure to view all issues that are marked as ignored. Ignored issues fall under these categories:

- Threshold-based issues: Issues detected by Assurance.
- AI-driven Issues: Issues detected by Cisco AI Network Analytics. These issues are triggered based on deviations from the predicted baseline for your specific network environment.

Before you begin

To view the AI-driven ignored issues, make sure that you have configured Cisco AI Network Analytics data collection. See Configure Cisco AI Network Analytics, on page 77.

Procedure

Step 1 From the main menu, choose **Assurance** > **Issues and Events**.

The **Open Issues** dashboard appears.

Step 2 From the **Status** drop-down list, choose **Ignored**.

The **Ignored Issues** window appears.

Step 3 Use the **Ignored Issues** window to view this information:

Ignored Issues window	
Item	**Description**
Global	• Click Global in the top menu bar to select the site, building, or floor from the Site hierarchy. • Click next to the location icon and select **Site Table** to view the Sites table. • Select **Hierarchical Site View** or **Building View** from the drop-down list. Based on what you select, the table is refreshed. • From the **Go to sites** column, click for a site or building to display data only for that location on the **Ignored Issues** dashboard.
24 Hours drop-down list	Allows you to display information on the window based on the time range you select. The default is **24 Hours**. Do these steps: **a.** From the **24 Hours** drop-down list, select a time range: **3 hours**, **24 hours**, or **7 days**. **b.** Specify the **Start Date** and time and the **End Date** and time. **c.** Click **Apply**. This sets the range of the timeline.
Timeline slider	Allows you to specify a more granular time range. Click and drag the timeline boundary lines to specify the time range.

Step 4 Click the **All**, **P1**, **P2**, **P3**, **P4**, or **AI-Driven** tab to display a list of issues in that category in the **Issue Type** table.

Issue Type table in the Ignored Issues window	
Item	**Description**
Total Ignored	Provides the total count of ignored issues. The **Total Ignored** value changes depending on the tab you select. Options are **All** (the default), **P1**, **P2**, **P3**, **P4**, and **AI-Driven**.
Priority	Preassigned priority level of the issue type.
Issue Type	Type of issue. **Note** For AI-driven issues, the AI icon appears in front of the issue type.
Device Role	Role assigned to the device on which the issue was detected. Roles are Access, Core, Distribution, Border Router, or Unknown.
Category	Category under which the issue type falls, such as Connectivity, Availability, Onboarding, and Utilization.

Issue Type table in the Ignored Issues window	
Item	**Description**
Issue Count	Number of times this type of issue occurred.
Site Count (Area)	Number of sites where this type of issue occurred.
Device Count	Number of devices that were impacted by this type of issue.
Last Occurred Time	Most recent date and time this issue occurred.

Step 5 From the **Issue Type** table, click an issue type.

The first slide-in pane, **Issue Instances** lists all the ignored issues for that issue type and information such as site, device, device type, occurrence, and the time stamp of the last occurrence.

Step 6 From the **Issue** column in the **Issue Instances** slide-in pane, click an issue.

A second slide-in pane, **Issue Instance Details**, provides details about the issue. Depending on the issue, the description and suggested actions are displayed. If you're an admin user, you can add, edit, and delete notes. Click the Note icon ( ) and then click **Add**. If you're any other type of user, you can only view note information.

Resolve or ignore issues

Use this procedure to resolve or ignore a bulk of issues or to resolve or ignore a single issue.

Procedure

Step 1 From the main menu, choose **Assurance** > **Issues and Events**.

The **Open Issues** dashboard appears.

Step 2 To resolve or ignore a bulk of issues:

a) From the **Issue Type** table in the **Open Issues** dashboard, click an issue type.

The first slide-in pane, **Issue Instances**, opens, which lists all the open issues for that issue type. This slide-in-pane allows you to resolve or ignore a bulk of issues. If you're an admin user, you can add, edit, and delete notes. Click the Note icon ( ) and then click **Add**. If you're any other type of user, you can only view note information.

b) Do one of these tasks:

- To resolve or ignore specific issues, check the check boxes adjacent to those issues.
- To resolve or ignore all open issues that are displayed in the browser window for an issue type, check the check box adjacent to the **Issue** column. All the issues that are displayed in the browser window are selected.
- If the open issue count is more than 25 (for example, 100), the first 25 issues are displayed in the browser window. To select all the open issues:

1. Check the check box adjacent to the **Issue** column.

   The first 25 issues are selected and the **Select all *number* open issues** tab appears next to the **Actions** drop-down list.

2. Click the **Select all *number* open issues** to select all open issues for that issue type (for example, all 100 issues).

3. (Optional) To view the next 25 issues in the browser window, click **Show More** located on the bottom of the page. The next 25 issues are appended to the browser window increasing the displayed issue count to 50. Click **Show More** to view the next 25 issues on the browser window, and so on.

c) To resolve the issues, from the **Actions** drop-down list, select **Resolve**.

In the Warning dialog box, click **Yes** to continue with the action.

After the issues are resolved, the **View resolved issues** tab is displayed. Click the **View resolved issues** to open the **Resolved Issues** window.

d) To ignore the issues, from the **Actions** drop-down list, select **Ignore**.

Set the number of hours to ignore the issues on the slider, and then click **Confirm**.

After the issues are ignored, the **View ignored issues** tab is displayed. Click the **View ignored issues** tab to open the **Ignored Issues** window.

Note
If you try to resolve or ignore more than 750 issues, a warning message appears letting you know that it might take up to a minute to complete the action.

Step 3 To resolve or ignore a single issue:

a) From the **Issue** column in the **Issue Instances** slide-in pane (first slide-in pane), click an issue.

A second slide-in pane, **Issue Instance Details**, opens, which provides details about the issue. This second slide-in-pane allows you to resolve or ignore the issue that you are viewing. If you're an admin user, you can add, edit, and delete notes. Click the Note icon ( ) and then click **Add**. If you're any other type of user, you can only view note information.

b) To resolve an issue, from the **Status** drop-down list, select **Resolve**.

c) To stop an issue from being reported:

1. From the **Status** drop-down list, select **Ignore**.

2. Set the number of hours to ignore the issue on the slider, and then click **Confirm**.

No Activity on Radio issue triggers

A "No Activity on Radio" issue is triggered when all of these conditions are met for 60 minutes, which is the default trigger time.

Note To change the default trigger time, choose **Assurance** > **Manage** > **Issue Settings**. See Manage global issue settings, on page 266.

- The AP radio operation state is **up**.
- The AP mode is Local or FlexConnect.
- The client count on this radio is equal to 0.
- The RX data or management frame count is *not* increasing.
- The AP radio channel utilization is equal to 0.
- The AP is not an **`isolated`** AP.

Automatic issue resolution

For these issues, if the issue condition no longer exists, the system automatically resolves the issue:

Issue name
Wireless Controller/Switch/Router unreachable.
Switch fan failure.
Switch power failure.
Interface is down.
Stack Member Removal.
Stack Port Link has failed
AP Disconnect from wireless controller.
No activity on radio.

These issues are auto resolved based on time duration since the last occurrence:

Issue name	Time duration to auto resolve
Network Device Interface Connectivity - BGP Flap	24 hours
Interface is Flapping On Network Device	24 hours
Network Device HA Switchover	24 hours
WLC Reboot Unexpectedly	24 hours
AP Reboot Crash	24 hours
Device Reboot	24 hours

Issue name	Time duration to auto resolve
AP Anomaly	24 hours
AP Flap	24 hours
Poor RF (5 GHz) on a floor	24 hours
Radio Poor RF (6 GHz)	24 hours
Poor RF (2.4 GHz) on a floor	24 hours
AP CPU High Utilization	24 hours
AP Memory High Utilization	24 hours
AP License Exhausted on WLC	24 hours
Switch experiencing high memory utilization	24 hours
Device experiencing high memory utilization	24 hours
Switch experiencing high CPU utilization	24 hours
Router experiencing high CPU utilization	24 hours
High input/output utilization on Switch interfaces	24 hours
High input/output error on Switch interfaces	24 hours
High input/output discard on Switch interfaces	24 hours
High input/output discard on Switch WAN interfaces	24 hours
High input/output utilization on Switch WAN interfaces	24 hours
High input/output utilization on Router interfaces	24 hours
High input/output utilization on Router WAN interfaces	24 hours
High input/output discard on Router interfaces	24 hours
High input/output discard on Router WAN interfaces	24 hours
High input/output utilization on Router WAN interfaces	24 hours
Fabric BGP session from Border node to Transit Control Plane node is down	6 hours
Fabric BGP session status is down with Peer Device (per VN)	6 hours
BGP session from Border node to Control Plane node is down	6 hours
Fabric Border node internet is unavailable (per VN)	6 hours
Fabric Border node remote internet is unavailable (per VN)	6 hours

Issue name	Time duration to auto resolve
Fabric AAA Server Status	6 hours
Fabric LISP Session Status to Control Plane node	6 hours
Fabric LISP PubSub session status per VN is down	6 hours
Cisco TrustSec Environment data is not complete on Fabric node	6 hours
Fabric LISP Extranet policy status is down	6 hours
High input/output utilization on Third Party Device interfaces	24 hours
High input/output error on Third Party Device interfaces	24 hours
High input/output discard on Third Party Device interfaces	24 hours
High input/output utilization on Third Party Device WAN interfaces	24 hours
High input/output discard on Third Party Device WAN interfaces	24 hours
TCAM Utilization High Issues	24 hours
Fabric Devices Connectivity - Border Underlay	6 hours
Fabric Devices Connectivity - Border Overlay	6 hours
Fabric Devices Connectivity - Multicast RP	6 hours
Fabric Devices Connectivity - Control Underlay	6 hours
Fabric Devices Connectivity - Control Border Underlay	6 hours
Fabric Devices Connectivity - AAA Server	6 hours
Fabric Devices Connectivity - DHCP Overlay	6 hours
Fabric Devices Connectivity - DHCP Underlay	6 hours
Fabric Devices Connectivity - DNS Overlay	6 hours
Fabric Devices Connectivity - DNS Underlay	6 hours
Fabric WLC to MapServer Connectivity	6 hours
Fabric LISP session status on Control Plane node	6 hours
Fabric LISP PubSub session status is down	6 hours
Fabric Border node internet is unavailable	6 hours
Fabric Border node remote internet is unavailable	6 hours

Issue name	Time duration to auto resolve
Fabric BGP session status is down with Peer Device	6 hours

You can view whether an issue is resolved automatically or manually. In the **Issue Settings** > **Global Profile** window, the **Issue Resolution** column displays either **Auto** for issues that are resolved by the system or **Manual** for issues that you must resolve.

After the issue is resolved, the **Updated By** column in the **Resolved Issues** > **Issue Instance** slide-in pane displays **System**. See View resolved issues, on page 257.

Manage global issue settings

Use this procedure to manage the settings for issues. You can enable or disable specific issues, change the priority, and set thresholds for when an issue is triggered. Additionally, for reachability events, you can configure site-level correlation to group multiple device failures into a single incident, reducing notification noise during site-wide outages.

Assurance supports site-based, role-based access control (SRBAC), which limits a user's scope of access to issues. You must ensure you have access to the sites, devices and their issue settings. For more information on user roles and permissions, see Cisco Catalyst Center Administrator Guide

Procedure

Step 1 From the main menu, choose **Assurance** > **Issue Settings**.

The **Issue Settings** window appears, with the **Global Profile** tab selected.

Step 2 Set the **DEVICE TYPE** and **CATEGORY** filters to view the types of issues in the Issue settings table. The Issue settings table includes Priority, Issue Name, Issue Resolution, Enabled, Global, Current Setting, Last Modified, and Subscription.

Note
For AI-driven issues, the AI icon appears in front of the issue type.

Issue Resolution column displays either Auto for issues that are resolved by the system or Manual for issues that you must resolve.

Step 3 The Issue table Click an issue in the **Issue Name** column to open a slide-in pane with these settings:

Note
For some issues, changes made to the settings are shared across multiple device types. In the slide-in pane, hover your cursor over the information icon ( ) to display the affected device types.

a) To enable or disable if the issue can be triggered, click the **Enabled** toggle.
b) To set the issue priority, click the **Priority** drop-down list and select the priority. The options are:
   - **P1**: A critical issue that needs immediate attention which can result in wider impact on network operations.
   - **P2**: A major issue that can potentially impact multiple devices or clients.
   - **P3**: A minor issue that has a localized or minimal impact.

- **P4**: A warning issue that may not be an immediate problem but addressing it can optimize the network performance.

c) (For certain issues) In the **Trigger Condition** area, you can change the threshold value for when the issue is reported.

Note
For the Unreachable network devices issue:

- Device Threshold: Enter the minimum number of devices that must be unreachable to trigger the site-level issue.
- Site Level: Select the hierarchy level for correlation (Area, Building, or Floor). If the threshold is met at the selected level, a single correlated issue is generated.
- Time Range: This issue uses a fixed 15-minute window to detect multiple failures. This duration is not configurable.
- Detection Logic: Reachability is checked every 1 minute. A device is marked unreachable after three consecutive failed pings.

For "No Activity on Radio" trigger conditions, see No Activity on Radio issue triggers, on page 262.

Examples of a trigger condition:

```
No Activity on Radio(2.4 GHz) >= 60 minutes.
```

```
Memory Utilization of Access Points greater than 90%
```

```
Unreachable network devices at Building level >= 3 devices within 15 minutes.
```

d) (Optional) If there are any changes to the settings, you can hover your cursor over **View Default Settings** to display the default issues. Click **Use Default** to restore all the issue settings to the default values.

e) Click **Apply**.

Step 4 (For certain issues) Click **Manage Subscription** to subscribe to external notifications for supported issues when they are triggered. See Enable issue notifications, on page 270.

Manage user-defined issue settings

Use this procedure to manage user-defined issue settings. You can create user-defined issues, enable or disable specific issues that can be triggered, change the priority for issues, change the threshold for when an issue is triggered, and subscribe to external notifications for issues when they are triggered.

Procedure

Step 1 From the main menu, choose **Assurance** > **Issue Settings**.

The **Issue Settings** window appears, with the **Global Profile** tab selected.

Step 2 Click the **User Defined** tab to view the list of user-defined issues.

Step 3 Click an issue in the **Issue Name** column to open the **Create an Issue** slide-in pane.

Step 4 To configure user-defined issues based on the syslog details, do these steps in the **Create an Issue** slide-in pane:

a) In the **Issue Name** field, enter the issue name.

b) In the **Description** field, enter the description of the issue.

c) In the **Syslog Details**, from the **Severity** drop-down list, select a severity from 0 to 6.

Assurance supports all syslogs that have a severity of 0, 1, 2 (Emergency, Alert, Critical), as well as some syslogs of severity 3, 4, 5, 6 (Error, Warning, Notice, and Info). When you create a user-defined issue, you can see and select the supported syslogs.

d) In the **Facility** field, enter the facility name.

e) In the **Mnemonic** field, enter the mnemonic name and click **Next**.

f) In the **Message Pattern** field, enter the syslog message. You can preview the syslog message below the message pattern.

g) In the **Occurrences** field, enter the value for occurrences.

h) In the **Duration** drop-down list, select the duration of an issue.

i) To enable or disable if the issue can be triggered, click the **Enabled** toggle.

j) To set the issue priority, click the **Priority** drop-down list and select a priority level:

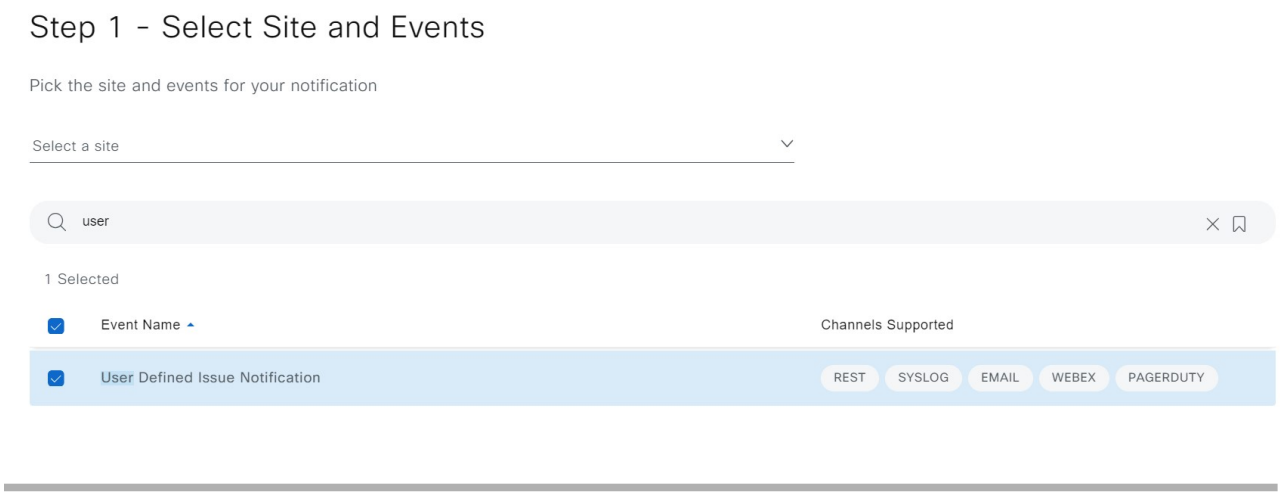
- **P1**: A critical issue that needs immediate attention and can have a wide impact on network operations.
- **P2**: A major issue that can potentially impact multiple devices or clients.
- **P3**: A minor issue that has a localized or minimal impact.
- **P4**: A warning issue that may not be an immediate problem but addressing it can optimize the network performance.

k) To enable or disable the issue notification, click the **Notification** toggle.

l) Click **Save**.

Step 5 Click **Manage Subscription** to subscribe to external notifications for issues when they are triggered. See Enable issue notifications, on page 270. You will create a subscription for the **User Defined Issue Notification** event, shown:

Figure 40: User Defined Issue Notification event



Manage Custom Issue Settings

You can create custom issue settings for a specific site or group of sites. These settings are called network profiles for Assurance and can be managed from both Assurance and Catalyst Center.

By creating a network profile for Assurance, you can control which issue settings are monitored, and you can change the issue priority.

Notes:

- Synchronization to the network device health score is available only for global issue settings, not custom issue settings. For information, see Monitor and troubleshoot the health of a device, on page 95.
- Some global issues are not customizable. These issues are not displayed in the list of custom issues for you to modify.
- To display modified issues at the top of the list, sort by **Last Modified**.
- To delete custom settings, you need to unassign all the sites first.

Procedure

Step 1 From the main menu, choose **Assurance** > **Issue Settings**.

The **Issue Settings** window appears, with the **Global Profile** tab selected.

Step 2 Click the **Custom Profile** tab.

Step 3 Click **+Add a Profile**.

Step 4 In the **Profile Name** field, enter a valid profile name and click **Next**.

Catalyst Center adds the profile and the profile table is displayed with Profile Name, Sites, and Action.

Step 5 To assign the profile to sites, click **Assign Sites** in the **Sites** column name to open a **Add Sites to Profile** slide-in pane. Check the check box next to the sites that you want to associate with this profile and click **Save**.

The **Edit Profile** window appears.

Note
You can select a parent node or the individual sites. If you select a parent node, all the children under the parent node are also selected. You can uncheck the check box to deselect a site.

From the **Action** column, click **Copy** to duplicate the existing profile.

Step 6 Set the **DEVICE TYPE** and **CATEGORY** filters to view the type of issues in the Issue settings table. The Issue settings table includes Priority, Issue Name, Issue Resolution, Enabled, Global, Current Setting, Last Modified, and Subscription.

Note
For AI-driven issues, the AI icon appears in front of the issue type.

Issue Resolution column displays either Auto for issues that are resolved by the system or Manual for issues that you must resolve.

Step 7 Click the **User Defined** tab to view the list of user-defined issues.

Step 8 Click an issue in the **Issue Name** column to open a slide-in pane with the settings.

Note
For some issues, changes made to the settings are shared across multiple device types. In the slide-in pane, Catalyst Center displays a caution that indicates the affected device types.

Step 9 To enable or disable whether Catalyst Center monitors the issue, click the **Enabled** toggle button.

Step 10 To set the issue priority, click the **Priority** drop-down list and select the priority. The options are:

- **P1**: A critical issue that needs immediate attention which can result in wider impact on network operations.
- **P2**: A major issue that can potentially impact multiple devices or clients.
- **P3**: A minor issue that has a localized or minimal impact.
- **P4**: A warning issue that may not be an immediate problem but addressing it can optimize the network performance.

Step 11 (For certain issues) In the **Trigger Condition** area, you can change the threshold value for when the issue is reported.

Note
Site-level correlation for Unreachable network devices can be customized per site profile. For example, you can set a higher device threshold for a large building and a lower threshold for a specific floor.

Examples of a trigger condition:

```
No Activity on Radio(2.4 GHz) >= 60 minutes.
```

```
Memory Utilization of Access Points greater than 90%
```

Step 12 (Optional) If there are any changes to the settings, you can hover your cursor over **View Default Settings** to display the default settings. Click **Use Default** to restore all the issue settings to the default values.

Step 13 Click **Apply**.

Step 14 (For certain issues) Click **Manage Subscription** to subscribe to external notifications for supported issues when they are triggered.

Step 15 Click **Edit** in the issue syslog message to edit a user-defined issue and click **Save**.

Step 16 Click **Done**.

The newly added profile appears on the **Issue Settings** window, in the **Custom Profile** tab.

Enable issue notifications

Use this procedure to receive external notifications for when specific issues are triggered in Assurance. When an issue is triggered and there is a status change, Assurance can generate a REST or email notification.

Procedure

Step 1 From the main menu, choose **Assurance** > **Issue Settings**.

The **Issue Settings** window appears.

Step 2 Click **Manage Subscription**. The **Event Notifications** window appears.
The **Platform** > **Developer Toolkit** > **Event Notifications** window is displayed. Each notification is represented by a tile and contains a link to view notification details.

Step 3 From the **CHANNELS** area in the left pane, click the radio button next to the channels for which you want to view the respective notification tiles.

The supported channels are **REST, PAGERDUTY, SNMP, SYSLOG, WEBEX and EMAIL**. Assurance events do not support SNMP.

Note

- You must create a notification for an event with respective channels and trigger the notification. For more information, see **Create an Event Notification** in the *Cisco Catalyst Center User Guide*.
- One event notification supports more than one channel.
- All user-defined issues map to the **User Defined Issue Notification** event name. So, for user-defined issues, you must subscribe to that notification event.

Step 4 Click a notification tile link for which you want to view the notification details.

The **Notification Details** slide-in pane displays these notification details based on the selected channel:

- **Name**: name of the event.
- **Description**: event description.
- **Sites**
- **Events**
- **REST**: appears only when you want to view REST notification details. The **REST** area shows this information:
  - **URL**: the URL address of the REST API endpoint that event will be sent to.
  - **Method**: either the PUT or POST method.
  - **Trust certificate**: whether a trust certificate is required for REST API endpoint notification.
  - **Headers**: the **Header Name** and **Header Value**.
- **PAGERDUTY**: appears only when you want to view PAGERDUTY notification details. The **PAGERDUTY** area shows this information:
  - PagerDuty Events API URL
  - PagerDuty Integration Key
  - PagerDuty Events API Version
- **SNMP**: appears only when you want to view **SNMP** notification details.
- **SYSLOG**: appears only when you want to view **SYSLOG** notification details.
- **WEBEX**: appears only when you want to view **WEBEX** notification details.
- **EMAIL**: appears only when you want to view **EMAIL** notification details. The **EMAIL** area shows the email recipients **From** and **To** along with email **Subject**.

Step 5 In the **Notification Details** slide-in pane, click the toggle button at the top-right corner to enable or disable the respective notification.

Step 6 To edit a particular notification, click the **Actions** drop-down list and select **Edit**.

Step 7 In the **EDIT NOTIFICATION** window, do this configuration based on the selected channel:

a. In the **Name** field, enter a unique name.

b. In the **Description** field, enter the description of respective event.

c. Expand the **Site and Events** and select a site from the **Select a site** drop-down list.

d. Click the plus icon next to an event, or click **Add All** to add all the events to the respective notification.

e. To remove an event from the notification, click the cross icon next to an event that you want to remove, or click **Remove All** to remove all events from the respective notification.

f. Expand **Configuration** to edit the configuration of the selected notification channel.

To specify details in the **Configuration** area, see **Create an Event Notification** in the *Cisco Catalyst Center User Guide*.

Note
In the **Configuration** area, the fields shown depend on the type of selected notification channel.

Step 8 Click the toggle button at the top-right corner to toggle between the tile view and list view.

Step 9 Click the **Event Catalog** tab to view the list of created events.

Note
You can adjust the events that appear by entering a keyword in the **Search** field.

Step 10 Review the data on an individual event within the table.

This **Event Details** tab data appears:

- **Description**: brief description of the event and how it is triggered.
- **Event ID**: identification number of the event.
- **Version**: version number of the event.
- **Namespace**: namespace of the event.
- **Severity**: 1 through 5.

  Note
  Severity 1 is the most important or critical priority and should be assigned for this type of an event.

- **Domain**: REST API domain to which the event belongs.
- **Subdomain**: subgroup under the REST API domain to which the event belongs.
- **Category**: Error, Warn, Info, Alert, Task Progress, Task Complete.
- **Note**: additional information about the event or to assist in further understanding the event.
- **Event Link**: event broadcast using REST URL.
- **Tags**: tags indicate what Catalyst Center component is affected by the event.

- **Channels**: what channels are supported for the event notifications (REST API, email, webex, and so on).
- **Model Schema**: presents model schema about the event:
  - **Details**: example of model schema detail for the event.
  - **REST Schema**: REST schema format for the event.

Step 11 Click the **Notifications** tab to view the active notification associated to the respective event.

Assurance, Cisco AI Network Analytics, and MRE issues

Router issues

This table lists the router issues detected by Assurance:

Router issues		
Category	**Issue name**	**Summary**
Connectivity	BGP tunnel connectivity	Border Gateway Protocol (BGP) connectivity failure with peer due to wrong autonomous system (AS) number.
Connectivity	Interface connecting network devices is down	An interface connecting to network devices is down. This issue applies to the interfaces that are connected to other devices (interdevice-connected link). This issue does not apply to client-connected interfaces or links.
Connectivity	Layer 2 loop symptoms	Host MAC address flapping seen on network device.
Connectivity	Network device Interface connectivity - BGP Flap	Border Gateway Protocol (BGP) connectivity is flapping with neighbor.
Connectivity	Network Device Interface Connectivity - BGP Down	BGP connectivity is down with neighbor.
Connectivity	Network device interface connectivity - EIGRP adjacency failure	Enhanced Interior Gateway Routing Protocol (EIGRP) adjacency failed with neighbor.
Connectivity	Network device interface connectivity - Interface down	Interface on device is down.
Connectivity	Network device interface connectivity - ISIS adjacency failure	Intermediate System Intermediate System (ISIS) adjacency failed on device.
Connectivity	Network device interface connectivity - OSPF adjacency failure	Open Shortest Path First (OSPF) adjacency failed with neighbor.
Connectivity	WAN Interface Down	A WAN interface is down.

Router issues		
Category	**Issue name**	**Summary**
Connected	Failure to install an access policy for SGT	Failure to install a Security Group Access Control List (SGACL) access policy for a Security Group Tag (SGT).
Connected	High input/output error on router interfaces	A high input or output error is detected on the router interfaces. The threshold values can be customized.
Connected	High input/output discards on router interfaces	A high input or output discard is detected on the router interfaces. The threshold values can be customized.
Connected	High input/output utilization on router interfaces	High input or output utilization is detected on the router interfaces. The threshold values can be customized.
Connected	High input/output discards on router WAN interfaces	A high input or output discard is detected on the router's WAN interface. The threshold values can be customized.
Connected	High input/output utilization on router WAN interfaces	High input/output utilization on WAN interfaces. High input or output utilization is detected on the router's WAN interfaces. The threshold values can be customized.
Connected	SGT access policy download failed on the device	Failed to download the Security Group Access Control List (SGACL) access control entries ACEs for a Security Group Tag (SGT).
Connected	SGT access policy installation failed on the device	Failure to install an access policy for a Security Group Tag (SGT). Policy rule error found in Role Based Access Control List (RBACL).
Connected	Unable to download SGT access policy from the policy server	Failure to download the source list for access policy for Security Group Tag (SGT).
Connected	Uninstall of SGT access policy failed on the device	Failure to uninstall an Security Group Access Control List (SGACL) access policy for Security Group Tag (SGT).
Device	Catalyst Center and network device time has drifted	Excessive time lag between Catalyst Center and device.
Device	Issues based on syslog events - High temperature	Issues created by single occurrence of syslog event related to high temperature.
Device	Router experiencing high CPU utilization	The router is experiencing high CPU utilization. The threshold values can be customized.
Device	Router experiencing high memory utilization	The router is experiencing high memory utilization. The threshold values can be customized.
Availability	Network device HA switchover	The network device went through an High Availability (HA) switchover.
Availability	Router unreachable	The router is unreachable from Catalyst Center through ICMP or SNMP.

Core, distribution, and access issues

This table lists the core, distribution, and access issues detected by Assurance:

Core, distribution, and access issues		
Category	**Issue name**	**Summary**
Connectivity	BGP tunnel connectivity	BGP connectivity failure with peer due to wrong autonomous system (AS) number.
Connectivity	Interface connecting network devices is down	An interface connecting to network devices is down. This issue applies to the interfaces that are connected to other devices (interdevice-connected link). This issue does not apply to client-connected interfaces or links.
Connectivity	Layer 2 loop symptoms	Host MAC address flapping seen on a network device.
Connectivity	Network Device Interface Connectivity- BGP Down	BGP connectivity is down with neighbor.
Connectivity	Network device Interface connectivity - BGP Flap	BGP connectivity is flapping with neighbor.
Connectivity	Network device interface connectivity - EIGRP adjacency failure	EIGRP (Enhanced Interior Gateway Routing Protocol) adjacency failed with neighbor.
Connectivity	Network device interface connectivity - Interface down	Interface on device is down.
Connectivity	Network device interface connectivity - ISIS adjacency failure	Intermediate System Intermediate System (IS-IS) adjacency failed on the device.
Connectivity	Network device interface connectivity - OSPF adjacency failure	Open Shortest Path First (OSPF) adjacency failed with neighbor.
Connectivity	WAN Interface Down	A WAN interface is down.
Connectivity	Dual Active Detection link failed on network device	The Dual Active Detection link has failed on the network device *Switch Name*.
Connectivity	StackWise Virtual link failed on network device	The StackWise Virtual link has failed on the network device *Switch Name*.
Connectivity	StackWise link failed on network device	The StackWise link has failed on the network device *Switch Name*.
Connectivity	Low transmit power on transceiver interface	Transmit power value has fallen below low alarm threshold value on transceiver interface .
Connectivity	High transmit power on transceiver interface	Transmit power value has exceeded high alarm threshold value on transceiver interface .
Connectivity	Low receive power on transceiver interface	Receive power $value$dBm has fallen below low alarm threshold of transceiver interface.

Core, distribution, and access issues		
Category	**Issue name**	**Summary**
Connectivity	High receive power on transceiver interface	Receive power has exceeded high alarm threshold of transceiver interface.
Connectivity	High temperature on transceiver interface	Temperature has exceeded high alarm threshold on transceiver interface.
Connectivity	Low voltage on transceiver interface	Voltage has fallen below low alarm threshold of transceiver interface.
Connectivity	High voltage on transceiver interface	Voltage has exceeded high alarm threshold of transceiver interface.
Connected	Fabric devices connectivity - Border overlay	The fabric edge lost connectivity to the fabric border in the virtual network.
Connected	Fabric devices connectivity - Border underlay	The fabric edge lost connectivity to the fabric border in the physical network.
Connected	Fabric devices connectivity - Control border underlay	The fabric node lost connectivity to the co-located fabric border and control plane in the physical network.
Connected	Fabric devices connectivity - Control underlay	The fabric node lost connectivity to the fabric control plane device in the physical network.
Connected	Fabric devices connectivity - DHCP overlay	The fabric node lost connectivity to the DHCP server in the virtual network.
Connected	Fabric devices connectivity - DHCP underlay	The fabric node lost connectivity to the DHCP server in the physical network.
Connected	Fabric devices connectivity - DNS overlay	The fabric node lost connectivity to the DNS server in the virtual network.
Connected	Fabric devices connectivity - DNS underlay	The fabric node lost connectivity to the DNS server in the physical network.
Connected	Fabric devices connectivity - External URL	The fabric border cannot reach the user-provisioned external URL.
Connected	Fabric devices connectivity - ISE server	The fabric edge lost connectivity to the ISE server in the physical network.
Connected	Fabric WLC to MapServer connectivity	The fabric wireless controller lost connectivity to the fabric control plane node.
Connected	Fabric facing port channel connectivity	The fabric node connecting the port channel is down.
Connected	Fabric AAA Server Status	The AAA server status on the fabric node is down.
Connected	Fabric devices connectivity - Multicast RP	The fabric border node lost connectivity to the multicast rendezvous point (RP).
Connected	BGP session Status to Fabric Control Plane	The BGP session is down on the border with the control plane in the fabric site.

Core, distribution, and access issues		
Category	**Issue name**	**Summary**
Connected	Fabric Control Plane - LISP Session Status	The LISP session to the control plane node is down.
Connected	Fabric Devices Connectivity - Internet Availability	The internet is unavailable because the default route on the control plane node is lost.
Connected	Fabric Extranet policy status	The fabric extranet policy status is down.
Connected	Fabric Control Plane - LISP Pubsub Session Status	The LISP PubSub session to the control plane node is down.
Connected	Fabric devices connectivity - AAA server	The fabric edge node lost connectivity to the AAA server in the physical network.
Connected	Fabric Devices Connectivity - Remote Internet Availability	The remote internet service on the control plane node is lost.
Connected	BGP session Status to Peer Device	The BGP session is down on the border for the IP transit peer in the site.
Connected	BGP session Status to Transit Control Plane	The BGP session is down on the border connected to the SD-Access transit.
Connected	Fabric devices connectivity - Border anchored	The fabric border node lost connectivity to the fabric anchored border node in the physical network.
Connected	Failure to install an access policy for SGT	Failure to install an SGACL access policy for SGT.
Connected	High input/output error on switch interfaces	A high input or output error is detected on the switch interfaces. The threshold values can be customized.
Connected	High input/output discard on switch interfaces	A high input or output discard is detected on the switch interfaces. The threshold values can be customized.
Connected	High input/output utilization on switch interfaces	High input or output utilization is detected on the switch interfaces. The threshold values can be customized.
Connected	SGT access policy download failed on the device	Failed to download SGACL ACEs for SGT.
Connected	SGT access policy installation failed on the device	Failure to install an access policy for SGT. Policy rule error found in RBACL.
Connected	Unable to download SGT access policy from the policy server	Failure to download the source list for access policy for SGT.
Connected	Uninstall of SGT access policy failed on the device	Failure to uninstall an SGACL access policy for SGT.
Device	Device reboot crash	Device has rebooted due to a hardware or software crash.

Core, distribution, and access issues		
Category	**Issue name**	**Summary**
Device	Device time has drifted from Catalyst Center	Excessive time lag between Catalyst Center and the device network.
Device	Interface is flapping on network device	A port interface is flapping on a switch. By default, this issue is triggered when the interface flaps three or more times within a 30-minute period. You can change the default flap trigger.
Device	Issues based on syslog events - High temperature	Issues created by single occurrence of syslog event related to high temperature.
Device	Issues based on syslog events - POE	Issues created by single occurrence of syslog event related to power.
Device	PoE port in error state	PoE port is error disabled as reported by a syslog event.
Device	PoE powered device flagged faulty	PoE-capable device connected to a PoE port has been flagged faulty as reported by a syslog event.
Device	Power denied for PoE powered device	PoE-capable device connected to a PoE port has been power denied as reported by a syslog event.
Device	Stack member removal	Stack member was removed.
Device	Stack member running incompatible image	Stack member is running an incompatible image.
Device	Switch experiencing high CPU utilization	The switch is experiencing high CPU utilization. The threshold values can be customized.
Device	Switch experiencing high memory utilization	The switch is experiencing high memory utilization. The threshold values can be customized.
Device	Switch fan failure	Fan failure on the switch.
Device	Switch power failure	Power supply failure on the switch.
Device	TCAM utilization high issues	Issues for TCAM exhaustion in Layer 2, Layer 3, QoS, and SGACL.
Availability	Network device HA switchover	The network device went through an HA switchover.
Availability	Switch unreachable	The switch is unreachable from Catalyst Center through ICMP or SNMP.
Utilization	Map cache limit reached	Map cache entries have exceeded the limit on the map server.
System	Assurance Telemetry status is poor	The network devices, or wired or wireless clients are impacted due to data loss.

Third-party device issues

This table lists the third-party device issues detected by Assurance:

Third-party device issues		
Category	**Issue name**	**Summary**
Availability	Third Party Device unreachable	The Third-Party device is unreachable from the Catalyst Center via ICMP or SNMP.
Connected	High input/output error on Third-Party Device interfaces	High input or output error is detected on the third-party device interfaces. The threshold values can be customized.
Connected	High input/output discard on Third-Party Device interfaces	A high input or output discard is detected on the third-party device interfaces. The threshold values are customized.
Connected	High input/output utilization on Third-Party Device interfaces	High input or output utilization is detected on the third-party device interfaces. The threshold values can be customized.
Connected	High input/output discards on Third-Party Device WAN interfaces	A high input or output discard is detected on the third-party device WAN interfaces. The threshold values can be customized.
Connected	High input/output utilization on Third-Party Device WAN interfaces	High input or output utilization is detected on the third-party device WAN interfaces. The threshold values can be customized.

Controller issues

This table lists the controller issues detected by Assurance:

Controller issues		
Category	**Issue name**	**Summary**
Connectivity	Interface connecting network devices is down	An interface connecting to network devices is down. This issue applies to the interfaces that are connected to other devices (interdevice-connected link). This issue does not apply to client-connected interfaces or links.
Connected	Fabric WLC to MapServer connectivity	The fabric wireless controller lost connectivity to the fabric control plane node.
Device	Device time has drifted from Catalyst Center	Excessive time lag between Catalyst Center and the network device. This issue is triggered when the time difference between Catalyst Center and the device is longer than 10 minutes.
Availability	Network device HA switchover	The network device went through an HA switchover.
Availability	WLC monitor	The network controller is not receiving data from the wireless controller.
Availability	WLC power supply failure	The power supply failed on this wireless controller.

Controller issues		
Category	**Issue name**	**Summary**
Availability	WLC reboot crash	A wireless controller reboot crash occurred.
Availability	WLC unreachable	The wireless controller is unreachable from Catalyst Center through ICMP or SNMP.
Utilization	AP license exhausted on WLC	The wireless controller currently has no free AP licenses.
Utilization	WLC memory high utilization	The wireless controller is experiencing high memory utilization.

Access point issues

This table lists the access point issues detected by Assurance:

Access point issues		
Category	**Issue name**	**Summary**
Availability	AP coverage hole	The wireless LAN controller detected a coverage hole around the AP.
Availability	AP disconnected from WLC	The AP is disconnected from the wireless LAN controller. The AP's CAPWAP link to the wireless LAN controller is down. This is an issue per AP when the AP is disconnected from the wireless controller. This issue appears in the AP 360 window; it does not appear in the Issues dashboard. You can subscribe to notifications for this issue. We recommend that you subscribe to the **AP(s) disconnected from WLC on Switch** issue, not the **AP disconnected from WLC** issue.
Availability	AP(s) disconnected from WLC on Switch	The AP is disconnected from the wireless LAN controller on the switch. This issue is aggregated on the access switch. Regardless of the number of APs that get disconnected on the switch, only one issue is generated per access switch. For example, if 10 APs get disconnected on two switches, Assurance generates two issues. The issue details show the APs that were disconnected. This issue appears in the Issues dashboard. You can subscribe to notifications for this issue.
Availability	AP flap	The AP has flapped. The AP disconnected from the wireless LAN controller and then connected back to the wireless LAN controller. This issue is triggered when the AP flaps more than two times within a 15-minute period.
Availability	AP reboot crash	AP has rebooted due to a hardware or software crash.
Utilization	AP CPU high utilization	AP is experiencing high CPU utilization.
Utilization	AP memory high utilization	AP is experiencing high memory utilization.

Access point issues		
Category	**Issue name**	**Summary**
Utilization	Radio high utilization (2.4GHz)	2.4-GHz radios on APs are experiencing high utilization.
Utilization	Radio high utilization (5GHz)	5-GHz radios on APs are experiencing high utilization.
Utilization	Radio high utilization (6GHz)	6-GHz radios on APs are experiencing high utilization.
Utilization	No activity on radio (2.4GHz)	No activity on 2.4-GHz radio on AP.
Utilization	No activity on radio (5GHz)	No activity on 5-GHz radio on AP.
Utilization	No activity on radio (6GHz)	No activity on 6-GHz radio on AP.
AP Anomaly	AP anomaly	AP encountered anomaly issue.
Availability	Poor RF (2.4 GHz) on a floor	This issue is triggered when APs have a poor wireless experience. The poor RF issue occurs when at least one AP has interference or noise above the threshold within a 30-minute timeframe.
Availability	Poor RF (5 GHz) on a floor	This issue is triggered when APs have a poor wireless experience. The poor RF issue occurs when at least one AP has interference or noise above the threshold within a 30-minute timeframe.
Availability	Poor RF (6 GHz) on a floor	This issue is triggered when APs have a poor wireless experience. The poor RF issue occurs when at least one AP has interference or noise above the threshold within a 30-minute timeframe.
Availability	Radio Down (2.4GHz)	2.4-GHz radio is down on AP.
Availability	Radio Down (5GHz)	5-GHz radio is down on AP.
Availability	Radio Down (6GHz)	6-GHz radio is down on AP.

Wired client issues

This table lists the wired client issues detected by Assurance:

Wired client issues		
Category	**Issue name**	**Summary**
Onboarding	Client DHCP reachability issue	The client has failed to obtain an IP address from DHCP server.
Onboarding	Wired client authentication failures - Dot1.x failure	The wired client failed authentication due to Dot1.x problems. **Note** This issue is applicable only for single wired clients.

Wired client issues		
Category	**Issue name**	**Summary**
Onboarding	Wired client authentication failures - MAB failure	The wired client failed authentication due to MAC authentication bypass problems. **Note** This issue is applicable only for single wired clients.

Wireless client issues

This table lists the wireless client issues detected by Assurance:



Note These issues are applicable for both single clients and multiple clients.

Wireless client issues		
Category	**Issue name**	**Summary**
Onboarding	802.11r client roaming slowly	While roaming, a wireless client capable of fast roaming is doing full authentication instead of fast authentication.
Onboarding	Client DHCP reachability issue	The client has failed to obtain an IP address from DHCP server.
Onboarding	Wireless client excluded - Client was excluded before roaming	Wireless client excluded - Client was excluded before roaming.
Onboarding	Wireless client failed to connect - Client timeout	Wireless client failed to connect - Failed to authenticate due to client timeout.
Onboarding	Wireless client failed to connect - DHCP timeout	Wireless clients took longer than 10 seconds to connect. The delay was in the IP Learning phase due to DHCP server or client timeout.
Onboarding	Wireless client failed to connect - Incorrect PSK	Multiple wireless clients failed to connect and were excluded by the wireless controller. They were excluded because the client's PSK did not match the configured WLAN PSK.
Onboarding	Wireless client failed to connect - WLC internal error	Wireless client failed to connect - wireless controller internal error.
Onboarding	Wireless client failed to roam - AAA server rejected client	Wireless client failed to roam - AAA server rejected client.
Onboarding	Wireless client failed to roam - AAA server timeout	Wireless client failed to roam - AAA server timeout.
Onboarding	Wireless client failed to roam - Client PMK not found	Wireless client failed to roam - Client PMK not found.

Wireless client issues		
Category	**Issue name**	**Summary**
Onboarding	Wireless client failed to roam - Client timeout	Wireless client failed to roam - Failed to authenticate due to client timeout.
Onboarding	Wireless client failed to roam - Security parameter mismatch	Wireless client failed to roam - Security parameter mismatch.
Onboarding	Wireless client failed to roam - WLC configuration error	Wireless client failed to roam - wireless controller configuration error.
Onboarding	Wireless client failed to roam - WLC internal error	Wireless client failed to roam - wireless controller internal error.
Onboarding	Wireless client failed to roam between APs - External error	Wireless client failed to roam between APs - External error.
Onboarding	Wireless client failed to roam between APs - WLC configuration mismatch	Multiple wireless clients failed to roam between APs due to a wireless LAN controller configuration mismatch.
Onboarding	Wireless clients took a long time to connect - Excessive time due to authentication timeouts	Multiple wireless clients took a long time to connect. The excessive onboarding time was due to authentication timeouts. The clients that run into this problem are grouped by AAA server or wireless controller.
Onboarding	Wireless clients took a long time to connect - Excessive time due to DHCP server failures	Multiple wireless clients took a long time to connect. The excessive onboarding time is due to DHCP server failures. The clients that run into this problem are grouped by the DHCP server or wireless controller.
Onboarding	Wireless clients took a long time to connect - Excessive time due to failed credentials	Multiple wireless clients took a long time to connect. The excessive onboarding time was due to authentication delays caused by failed credentials. The clients that run into this problem are grouped by AAA server or wireless controller.
Onboarding	Wireless clients took a long time to connect - Excessive time due to WLC failures	Multiple wireless clients took a long time to connect. The excessive onboarding time was due to wireless LAN controller failures during authentication. The clients that run into this problem are grouped by wireless controller.
Onboarding	Wireless clients took a long time to connect - Excessive time for authentication due to AAA server or network delays	Multiple wireless clients took a long time to connect. The excessive onboarding time was due to authentication delays. The authentication delays were caused by AAA server or network delays.
Onboarding	Wireless clients excluded - IP theft issue	Multiple wireless clients have been excluded from connecting to the wireless network. IP theft issues were detected on the clients. The clients that run into this problem are grouped by wireless controller.
Onboarding	Wireless clients failed to connect - AAA server rejected clients	Multiple wireless clients failed during authentication with a AAA Server Reject failure reason. The AAA server rejected the client's authentication requests. The clients that run into this problem are grouped by AAA server or wireless controller.

Wireless client issues		
Category	**Issue name**	**Summary**
Onboarding	Wireless clients failed to connect - AAA server timeout	Multiple wireless clients failed during authentication with a AAA Server Timeout failure. This failure occurs when the wireless controller doesn't receive a response from the AAA to the client's authentication messages and times out after retries. The clients that run into this problem are grouped by AAA server or wireless controller.
Onboarding	Wireless clients failed to connect - Client PMK not found	Multiple wireless clients failed to connect due to authentication problems. The client's PMK was not found.
Onboarding	Wireless clients failed to connect - DHCP server timeout	Multiple wireless clients failed to connect. The failure was in the IP Learning phase due to DHCP server timeout. The DHCP server timed out and did not respond to DHCP messages. The clients that run into this problem are grouped by DHCP server or wireless controller.
Onboarding	Wireless clients failed to connect - Failed to authenticate due to client timeouts	Multiple wireless clients failed to connect. They failed to authenticate due to client timeouts. The clients failed to respond in time to authentication messages. The clients that run into this problem are grouped by site or AP group.
Onboarding	Wireless clients failed to connect - Failed to get an IP address due to client timeouts	Multiple wireless clients failed to connect. They failed to get an IP address due to client timeouts. The clients failed to respond in time to DHCP messages. The clients that run into this problem are grouped by site or AP group.
Onboarding	Wireless clients failed to connect - Failed to get an IP address due to DHCP server or client timeouts	Multiple wireless clients failed to connect. They failed to get an IP address due to DHCP server timeouts or client timeouts. Either the DHCP server or the clients failed to respond in time to DHCP messages. The clients that run into this problem are grouped by site or AP group.
Onboarding	Wireless clients failed to connect - Security parameter mismatch	Multiple wireless clients failed to connect due to authentication problems caused by a security parameter mismatch.
Onboarding	Wireless clients failed to connect - WLC configuration error	Multiple wireless clients failed to connect due to authentication problems. There are wireless LAN controller configuration errors. The clients that run into this problem are grouped by wireless controller.
Onboarding	Wireless clients failed to roam - Client exclusion policies on the WLC	Multiple wireless clients failed to roam. Clients were excluded due to client exclusion policies on the wireless LAN controller. The clients that run into this problem are grouped by wireless controller.
Onboarding	Wireless clients failed to roam - Clients were excluded before roaming	Multiple wireless clients failed to roam. The clients were excluded on the wireless LAN controller before roaming. The clients that run into this problem are grouped by wireless controller.
Onboarding	Wireless clients failed to roam - WLC configuration mismatch	Multiple wireless clients failed to roam between APs due to a wireless LAN controller configuration mismatch.

Wireless client issues		
Category	**Issue name**	**Summary**
Onboarding	Wireless clients took a long time to connect - WLC failures	Multiple wireless clients took a long time to connect. The excessive onboarding time was due to wireless LAN controller failures during authentication. The clients that run into this problem are grouped by wireless controller.
Connected	Dual band capable client prefers 2.4 GHz over 5 GHz	Dual-band capable client is consistently connecting to a 2.4-GHz radio, even though a 5-GHz radio that provides a better experience is available.
Connected	Wireless client has poor RF	Wireless client is experience poor RF condition because the client has no better neighboring APs to roam to.
Connected	Wireless client shows sticky behavior	Wireless client is maintaining an association with an AP that has a weaker signal. It should roam to an available AP that has the stronger signal.

Enable AAA Failure Root Cause Analysis issues

Catalyst Center integrates with Cisco ISE syslogs to troubleshoot these issues:

- Wireless clients failed to connect: AAA server rejected clients
- Wireless clients failed to connect: AAA server timeout

The troubleshooting workflow is an MRE workflow that you access from a single client issue in the **Client 360** window, or from wireless client issues in the **Issues** dashboard.

Catalyst Center shows the syslogs generated by Cisco ISE for client authentication failures, enabling you to determine the root cause of the client authentication failure without having to log in to Cisco ISE and search for clients there.

To enable AAA Failure Root Cause Analysis issues in Assurance:

Procedure

Step 1 In Catalyst Center, choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers** and add and configure Cisco ISE to the Catalyst Center cluster. This step adds the Cisco ISE policy service node (PSN) to the syslog allowed list.

Step 2 In Cisco ISE, choose **Administration** > **System** > **Logging** > **Remote Logging Targets** and add Catalyst Center as a syslog destination.

Step 3 In Cisco ISE, choose **Administration** > **System** > **Logging** > **Logging Categories** and add the target that you added in the previous step to these logging categories: **Failed Attempts**, **Authentication Flow Diagnostics**, and **RADIUS Diagnostics**.
Cisco ISE syslogs can now be sent to Catalyst Center. Catalyst Center processes and saves the Cisco ISE syslogs for client onboarding problems.

Application issues

This table lists the application issues detected by Assurance:

Application issues		
Category	**Issue name**	**Summary**
Application	Application experience issues	All issues pertaining to Application Experience.

Sensor issues

This table lists the sensor issues detected by Assurance.

When two or more sensors on the same floor fail a test in a 30-minute period, the sensor can raise an issue based on the failed root cause. These sensor issues are all global issues, meaning that the sensor issue from any floor is escalated and shown in the **Issues** dashboard.

Sensor issues		
Category	**Issue name**	**Summary**
Sensor Test	Sensors - Speed test HTTP error	Multiple sensors are reporting speed test HTTP error while accessing query server.
Sensor Test	Sensors - DHCP failures	Multiple sensors failed to get an IPv4 address.
Sensor Test	Sensors - DNS resolution failed	Multiple sensors failed to resolve domain name with DNS server.
Sensor Test	Sensors - Failed association during onboarding	Multiple sensors failed to associate during onboarding.
Sensor Test	Sensors -Failed authentication during onboarding	Multiple sensors failed to authenticate during onboarding.
Sensor Test	Sensors - FTP test fail	Multiple sensors are reporting unable to connect to FTP server.
Sensor Test	Sensors - FTP transfer fail	Multiple sensors are reporting failed to transfer file with FTP server.
Sensor Test	Sensors - FTP unreachable	Multiple sensors are reporting unreachable FTP server.
Sensor Test	Sensors - IPerf invalid config error	Multiple sensors have failed to conduct the iPerf test due to receiving invalid iPerf configurations.
Sensor Test	Sensors - IPerf server busy	Multiple sensors have failed to conduct the iPerf test due to an iPerf busy error.
Sensor Test	Sensors - IPerf test network error	Multiple sensors have failed to conduct the iPerf test due to an iPerf network error.
Sensor Test	Sensors - IPerf undefined error	Multiple sensors have failed to conduct the iPerf test due to an undefined error.
Sensor Test	Sensors - IPSLA no IP address	Multiple sensors are reporting IPSLA test IP address not received from Catalyst Center.

Sensor issues		
Category	**Issue name**	**Summary**
Sensor Test	Sensors - IPSLA no response	Multiple sensors are reporting IPSLA test - no response from IPSLA responder.
Sensor Test	Sensors - IPSLA socket error	Multiple sensors are reporting IPSLA test socket error.
Sensor Test	Sensors - IPSLA test fail	Multiple sensors are reporting IPSLA test failed.
Sensor Test	Sensors - IPSLA unsupported probe type	Multiple sensors are reporting IPSLA test unsupported probe type.
Sensor Test	Sensors - Mail server test fail	Multiple sensors are reporting failed to connect to mail server.
Sensor Test	Sensors - Mail server unreachable	Multiple sensors are reporting unreachable mail server.
Sensor Test	Sensors - No NDT server	Multiple sensors are reporting speed test NDT server does not exist.
Sensor Test	Sensors - Onboarding failures	Sensors failed to connect to the wireless network.
Sensor Test	Sensors - Outlook server test fail	Multiple sensors are reporting failed to connect to Outlook Web Access.
Sensor Test	Sensors - Outlook server unreachable	Multiple sensors are reporting unreachable Outlook Web Access host.
Sensor Test	Sensors - Query server timeout	Multiple sensors are reporting speed test query server timeout.
Sensor Test	Sensors - RADIUS authentication fail	Multiple sensors are reporting failed to authenticate with RADIUS server.
Sensor Test	Sensors - Speed test fail	Multiple sensors are reporting speed test failed.
Sensor Test	Sensors - Speed test generic error	Multiple sensors are reporting speed test generic failure.
Sensor Test	Sensors - Speed test uplink timeout	Multiple sensors are reporting speed test uplink test timeout.
Sensor Test	Sensors - Speed test URL error	Multiple sensors are reporting speed test URL error while accessing query server.
Sensor Test	Sensors - Unreachable host	Multiple sensors are reporting ping failure to the host. Unreachable host.
Sensor Test	Sensors - Unreachable RADIUS	Multiple sensors are reporting unreachable RADIUS server.
Sensor Test	Sensors - Web authentication fail	Multiple sensors are reporting clients are failing web authentication test.
Sensor Test	Sensors - Web server test failed	Multiple sensors are reporting failed to load page from web server.
Sensor Test	Sensors - Web server unreachable	Multiple sensors are reporting unreachable web server.
Sensor Test	Sensors - Web socket error	Multiple sensors are reporting speed test websocket error during the test.
Sensor Test	Sensors - Speed test uplink proxy error	Multiple sensors are reporting speed test uplink test proxy error.

AI-driven issues

This table lists the AI-driven issues detected by Cisco AI Network Analytics:

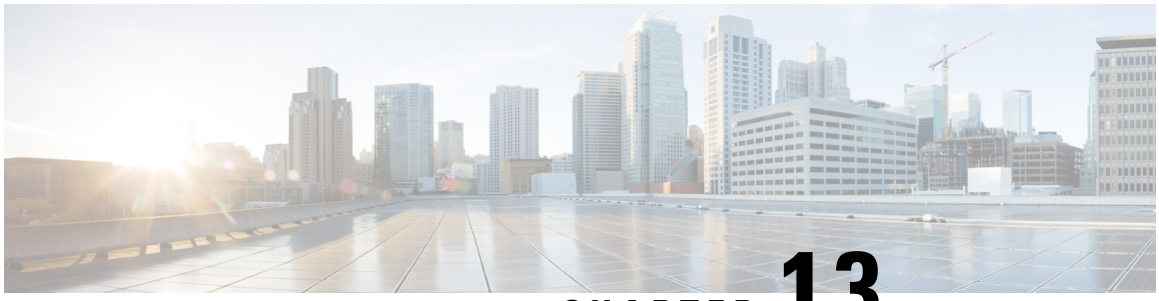
AI-driven issues		
Connection issues		
Onboarding	AI Excessive time to connect - High deviation from baseline	The network is experiencing excessive onboarding time compared to usual. Clients are taking longer than the usual time to connect to *SSID*.
Onboarding	AI Excessive failures to connect - High deviation from baseline	The network is experiencing excessive onboarding failures compared to usual. Clients are taking longer than the usual time to connect to *SSID*.
Onboarding	AI Wireless clients took a long time to connect - Total time above baseline	Wireless clients took longer to connect to *SSID* at *location*.
AAA	AI Excessive time to get Associated - High deviation from baseline	Excessive time to get associated - At least *value*% increase in time on *SSID*.
AAA	AI Excessive failures to Associate - High deviation from baseline	Excessive failures to get associated - At least *value*% increase in failures on *SSID*.
AAA	AI Excessive time to get Authenticated - High deviation from baseline	Excessive time to get authenticated - At least *value*% increase in time on *SSID*.
AAA	AI Excessive failures to get Authenticated - High deviation from baseline	Excessive failures to get authenticated - At least *value*% increase in failures on *SSID*.
DHCP	AI Excessive time to get an IP Address - High deviation from baseline	Excessive time to get an IP address - At least *value*% increase in time from *server_IP*.
DHCP	AI Excessive failures to get an IP address - High deviation from baseline	Excessive failures to get an IP address - At least *value*% increase in failures from *server_IP*.
Network Connectivity issue		
Connectivity	AI Host MAC address flapping seen on network device	Network is experiencing Layer 2 loop symptoms.
Roaming issues		
Onboarding	AI Excessive time to connect - High deviation from baseline	The network is experiencing excessive onboarding time compared to usual.
Onboarding	AI Excessive failures to roam - High deviation from baseline	The network is experiencing excessive roaming time compared to usual.
Application Experience issues		
Throughput	AI Drop in total radio throughput for All Applications	APs in network are experiencing a drop in total radio throughput for all applications. These radios are in the *frequency* band. These radios are located at *location*.

AI-driven issues		
Throughput	AI Drop in radio throughput for Cloud Applications	APs in network are experiencing a drop in Cloud Applications throughput. These radios are in the *frequency* band. These radios are located at *location*.
Throughput	AI Drop in radio throughput for Social Applications	APs in network are experiencing a drop in Social Applications throughput. These radios are in the *frequency* band. These radios are located at *location*.
Throughput	AI Drop in radio throughput for Media Applications	APs in network are experiencing a drop in Media Applications throughput. These radios are in the *frequency* band. These radios are located at *location*.
Throughput	AI Drop in radio throughput for Collab Applications	APs in network are experiencing a drop in Collab Applications throughput. These radios are in the *frequency* band. These radios are located at *location*.

MRE issues

This table lists the issues detected by Assurance that you can troubleshoot using the MRE workflow:

MRE issues		
Category	**Issue name**	**Summary**
Wired client issues		
Onboarding	Client DHCP reachability issue	The client has failed to obtain an IPv4 address from the DHCP server.
Onboarding	Wired client authentication failures - Dot1.x failure	The wired client failed authentication due to Dot1.x problems. **Note** This issue is applicable only for single wired clients.
Onboarding	Wired client authentication failures - MAB failure	The wired client failed authentication due to MAC authentication bypass problems. **Note** This issue is applicable only for single wired clients.
PoE issue		
Device	PoE powered device flagged faulty	Syslog event flagged a PoE-capable device connected to a PoE port as faulty.



CHAPTER 13

View and Manage Events

- Events dashboard overview, on page 291
- View device events, on page 291
- View endpoint events, on page 295
- View event analytics dashboard, on page 299

Events dashboard overview

The **Events** dashboard provides a contextual view of events for devices (routers, switches, wireless controllers, APs, and third party device) and endpoints (wired and wireless). Instead of having to search for events triggered by devices that are connected to other devices involved in an event, Assurance provides these details for you.

By default, the **Events** dashboard displays a timeline chart and a list view.

The timeline chart provides a color representation of the number of events by device type that occurred over a period of time.

The list view displays a table of events. Up to 10,000 events can be displayed, even if more events have been logged. You can export up to 5000 events to a CSV file. If you have more than 5000 events, you cannot export them. A warning message appears in the GUI that states "*Multiple selection for device family filter is not supported for Event counts more than 5000*".

From the list view, you can click an event to view its details, including events triggered by connected devices. You can configure the event time period in 15-minute increments, up to one hour (+/- 15 minutes, +/- 30 minutes, +/- 45 minutes, +/- 1 hour).

When you select more than one event, you can view multiple cards with event details. When you have multiple event cards displayed, you can minimize, maximize, and close cards. For example, to view the connected device events table for an event, maximize the event card. To return to the multiple card view, minimize the card.

View device events

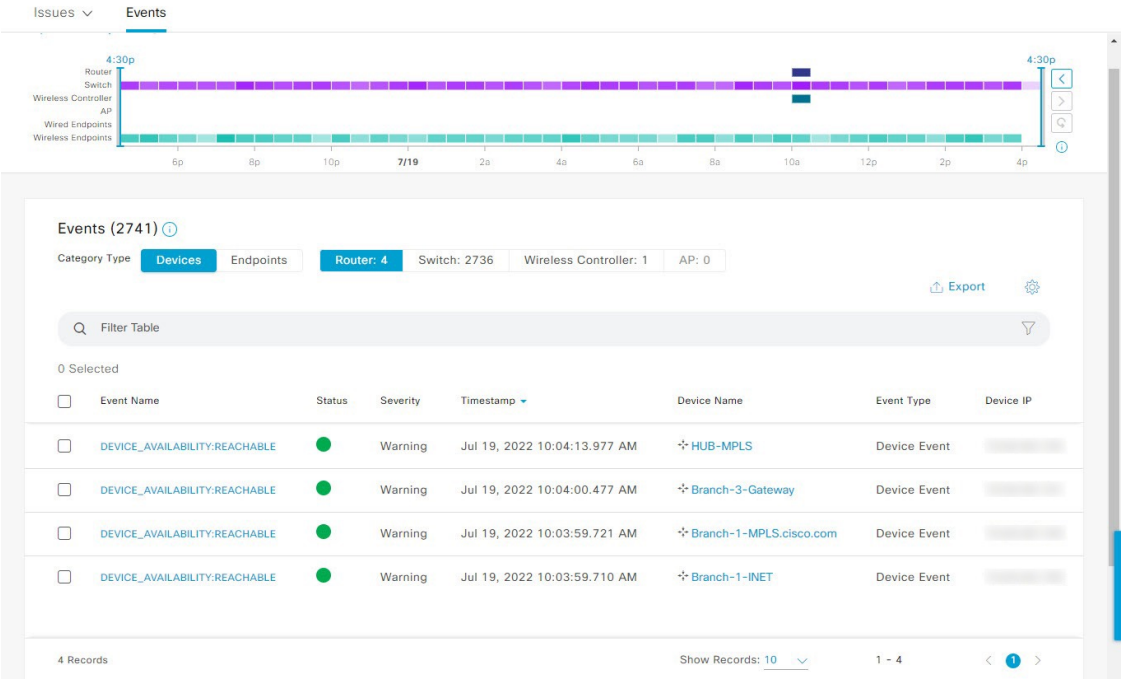
Use this procedure to view events generated by routers, switches, wireless controllers, APs and third party device .

Procedure

Step 1 From the main menu, choose **Assurance** > **Dashboards** > **Issues and Events**.

The **Events** dashboard opens with **Device** selected as the **Category Type** by default.

Figure 41: Device Events dashboard



Device Events dashboard	
Item	**Description**
Global	• Click Global in the top menu bar to select the site, building, or floor from the Site hierarchy. • Click next to the location icon and select **Site Details** to view the event counts for each site. • Select **Hierarchical Site View** or **Building View** from the drop-down list. Based on what you select, the table is refreshed. • From the **Go to sites** column, click for a site or building to display events for only that location.

Device Events dashboard	
Item	**Description**
 **Time Range** setting	Allows you to display information on the window based on the time range you select. The default is **24 Hours**. Do these steps: **a.** From the **24 Hours** drop-down list, select a time range: **3 hours**, **24 hours**, or **7 days**. **b.** If you chose **Presets**, you can select from the **CURRENT** column (Today, Week, or Month) or the **LAST** column (24 hours, 7 days, 14 days, 30 days, or 60 days). **c.** Specify the **Start Date** and time, and the **End Date** and time. **d.** Click **Apply**. This sets the range of the timeline.
Timeline Slider	Allows you to specify a more granular time range. Click and drag the timeline boundary lines to specify the time range. The colors represent the device type: : Router : Switch : Wireless controller : AP : Third Party Device The intensity of the color indicates its significance, whether more or fewer events have occurred for that device. For example, a lighter shade of blue indicates fewer router events than a deeper shade of blue.
Total Events	The total number of events for all device types for a specific time range.

Step 2 Under **Events**, for the **Category Type**, click the **Router**, **Switch**, **Wireless Controller**, **AP**, or **Third Party Device** tab to display a list of events for that device type in the table.

Events table	
Item	**Description**

Filter table option	Use the Filter Table bar at the top to perform search in the table.
	• **Match All**: Displays only the events that meet **every** specified condition.
	• **Match Any**: Displays events that meet at least one of the specified conditions.
	• From the **Column Name** drop-down, select the specific attribute to filter by such as Severity, Timestamp, Device Name, Event Type, or Device IP, .
	• **Operator** defines the logic of the filter.
	  • **Equals**: Exact match
	  • **Not Equals**: Excludes the specified value
	  • **Contains**: Matches any value that includes the specified string.
	• **Value input**: Enter the specific text or ID you are searching for. Fields marked with a red asterisk (*) are mandatory.
	• To add more rows of criteria, click the **(+)** icon located to the right of the filter row. This allows for complex, multi-layered troubleshooting (filtering for a specific *Event Type* on a specific *Switch*).

Event Name	Name of the event. Click the event name to open a slide-in pane with details about the event. **Note** For Syslog events, in the slide-in pane, click on the **Create an Issue** link and click **Confirm** to launch the User Defined Issue page to directly create an issue. Events associated with the Intel devices are labeled with tags.
Status	Status of the device. The color represents the severity of the event. ●: Error. ●: Warning. ●: Info. ●: No data available.
Severity	Severity of the event: Critical and above (Emergency and Alert) and less severe than Critical level (Error, Warning, Notice, and Info).
Timestamp	Date and time when the event occurred.
Device Name	Name of the device that was impacted by the event. Click the device name to open the **Device 360** window.
Event Type	Category of the event: **Syslog**, **Trap**, **Event**, or **AP Event**.

Events table	
Item	**Description**
Device IP	IP address of the device.

Step 3 To view multiple events, check the check box next to each event you want to view and click **Show Selected Events**.

The **Multiple Events** slide-in pane opens with each event displayed in a separate card.

From inside a card, you can do these tasks:

- Minimize, maximize, and close a card.
- Display more details by clicking the down arrow.
- Click hyperlinks to launch the respective device 360 window.

When a card is maximized, any connected device events appear.

Step 4 From the **Multiple Events** slide-in pane, click the list view icon to display a compilation of all the subevents sequentially in a list.

To return to the card view, click the card view icon.

View endpoint events

Use this procedure to view events generated by wired and wireless endpoints.

Procedure

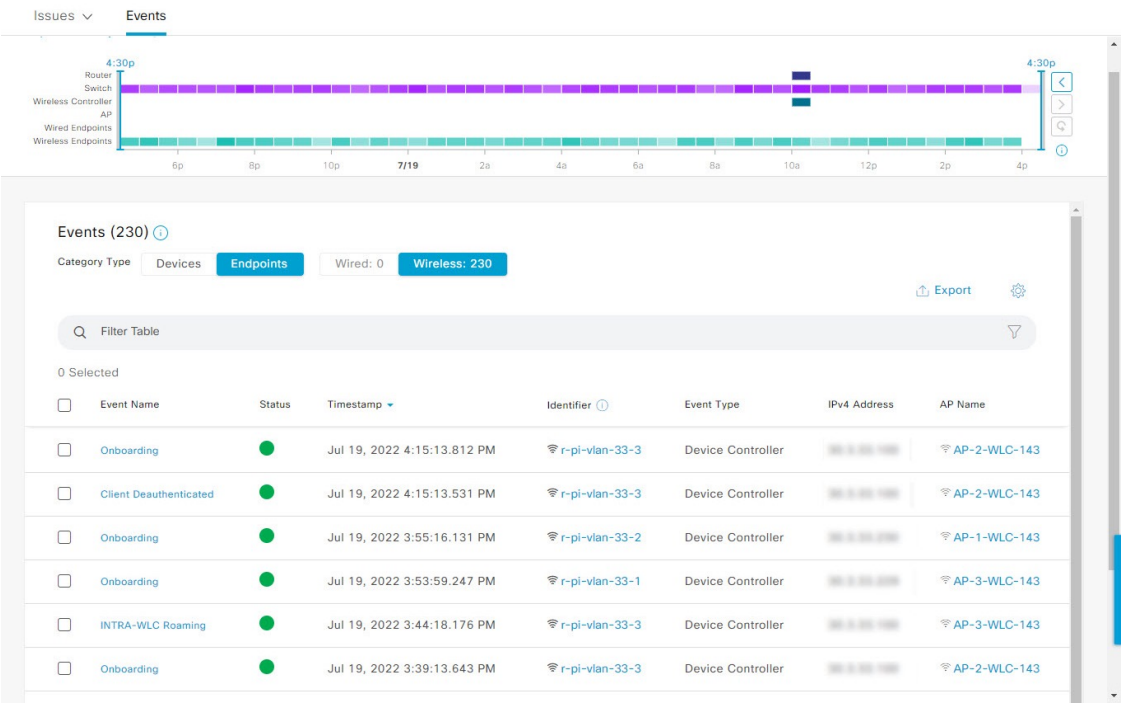
Step 1 From the main menu, choose **Assurance** > **Dashboards** > **Issues and Events**.

Step 2 Click the **Events** tab.

The **Events** dashboard opens.

Step 3 For the **Category Type**, click the **Endpoints** tab.

Figure 42: Endpoint Events dashboard



Device Events dashboard	
Item	**Description**
Global	• Click Global in the top menu bar to select the site, building, or floor from the Site hierarchy. • Click next to the location icon and select **Site Details** to view the event counts for each site. • Select **Hierarchical Site View** or **Building View** from the drop-down list. Based on what you select, the table is refreshed. • From the **Go to sites** column, click for a site or building to display events for only that location.
Time Range setting	Allows you to display information on the window based on the time range you select. The default is **24 Hours**. Do these steps: **a.** From the **24 Hours** drop-down list, select a time range: **3 hours**, **24 hours**, or **7 days**. **b.** Specify the **Start Date** and time, and the **End Date** and time. **c.** Click **Apply**. This sets the range of the timeline.

Device Events dashboard	
Item	**Description**
Timeline Slider	Allows you to specify a more granular time range. Click and drag the timeline boundary lines to specify the time range. The colors represent the endpoint type: : Wired : Wireless The intensity of the color indicates its significance, whether more or fewer events have occurred for that device. For example, a lighter shade of purple indicates fewer endpoint events than a deeper shade of purple.
Total Events	The total number of events for all endpoint types for a specific time range.

Step 4 Click the **Wired** or **Wireless** tab to display a list of events for that endpoint type in the table.

Events table	
Item	**Description**

Filter table option	Use the Filter Table bar at the top to perform search in the table.
	• **Match All**: Displays only the events that meet **every** specified condition.
	• **Match Any**: Displays events that meet at least one of the specified conditions.
	• From the **Column Name** drop-down, select the specific attribute to filter by.
	• **Operator** defines the logic of the filter.
	  • **Equals**: Exact match
	  • **Not Equals**: Excludes the specified value
	  • **Contains**: Matches any value that includes the specified string.
	• **Value input**: Enter the specific text or ID you are searching for. Fields marked with a red asterisk (*) are mandatory.
	• To add more rows of criteria, click the **(+)** icon located to the right of the filter row. This allows for complex, multi-layered troubleshooting (filtering for a specific *Event Type* on a specific *endpoint*).

Event Name	Name of the event. Click the event name to open a slide-in pane with more details.
Status (Wired Endpoints Only)	The color represents the severity of the event. : Error. : Warning. : Info. : No data available.

Events table	
Item	**Description**
Severity (Wired Endpoints Only)	Severity of the event. Severity can be critical and above (Emergency and Alert) and less severe (Error, Warning, Notice, and Info).
Timestamp	Date and time when the event occurred.
Identifier	Identifier of the endpoint. It can be either user ID, hostname, IP Address, or MAC address, depending on the availability in that order. Click the identifier to open a slide-in pane with more details.
Event Type	Category of the event: **Syslog**, **Trap**, **Event**, or **AP Event**.
IPv4 Address	IPv4 address of the device that is connected to the endpoint.
AP Name (Wireless Endpoints Only)	Name of the AP that is connected to the wireless endpoint. Click the AP name to open the AP **Device 360** window.
Switch (Wired Endpoints Only)	Name of the switch that is connected to the wired endpoint. Click the switch name to open the **Device 360** window.
MAC Address	MAC address of the device that is connected to the endpoint.
Port (Wired Endpoints Only)	Switch port that is connected to the wired endpoint.
VLAN ID (Wired Endpoints Only)	VLAN ID of the switch port that is connected to the wired endpoint.
Switch IP Address (Wired Endpoints Only)	IP address of the switch connected to the wired endpoint.
AP MAC (Wireless Endpoints Only)	MAC address of the AP that is connected to the wireless endpoint.
SSID (Wireless Endpoints Only)	SSID that the wireless endpoint is using.
UserID (Wireless Endpoints Only)	User ID of the wireless endpoint.
Wireless Controller Name (Wireless Endpoints Only)	Name of the wireless controller that is connected to the wireless endpoint.
Band (Wireless Endpoints Only)	Radio band that the wireless endpoint is using.
DHCP Server (Wireless Endpoints Only)	DHCP server that the wireless endpoint is using.

Step 5 Click the event name to view more information about that event in a slide-in pane.

The slide-in pane displays basic information (such as the identifier and severity), hyperlinked data, and connected device events details.

Note
If a wireless endpoint uses Cisco ISE for AAA management, Catalyst Center gets Cisco ISE authentication event details from Cisco ISE and displays them in the **ISE Authentication** events. In the event slide-in pane, you can view the Cisco ISE authentication steps completed by the AAA server by clicking **Show ISE Events**.

In the **Connected Device Events** dashlet, you can view a maximum of 10,000 connected device events in the table by clicking **Show Events**. In this dashlet, you can either filter or export the event data.

- From the **+_15 mins** drop-down list in the top-right corner of the dashlet, select a timeframe to view all the events that occurred within that timeframe.
- Click a device tab, such as **Switch** or **AP**, to view the events connected to that device.
- Click **Export** in the top-right corner of the table to export up to 5,000 events from the table as a CSV file.
- Click the gear icon in the top-right corner of the table to customize the table settings.
- Use the table search bar to filter the table for specific data.

Step 6 To view multiple events, check the check box next to each event that you want to view and click **Show Selected Events**.

The **Multiple Events** slide-in pane displays each event in a separate card in the default card view.

In the **Multiple Events** slide-in pane, you can change views using the view switcher ( ).

From inside a card, you can

- Minimize, maximize, and close a card;
- Display more details by clicking the down arrow; and
- Click any hyperlinked data.

When a card is maximized, any connected device events are displayed.

View event analytics dashboard

The **Events Analytics** dashboard provides a visualization of syslog messages and different types of network events to identify trends and correlate events across different data sources.

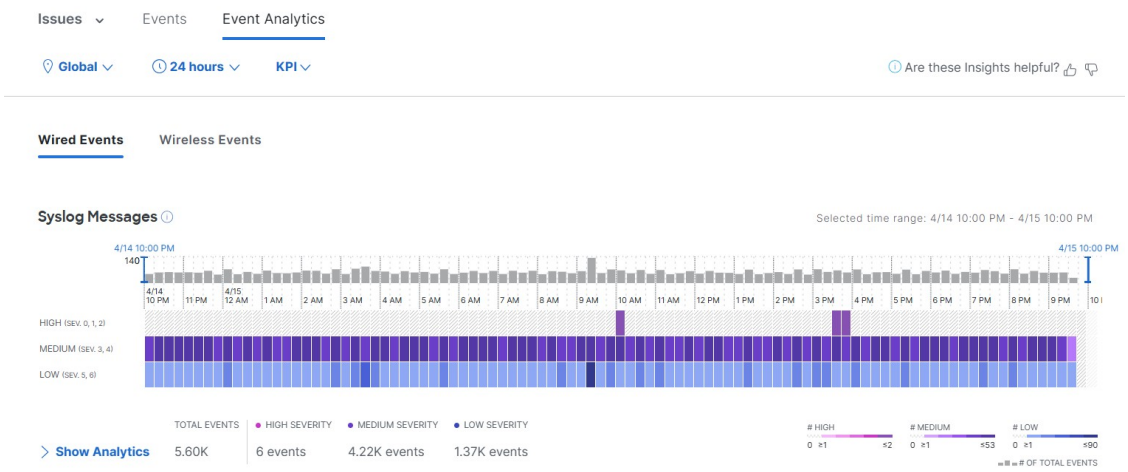
Use this procedure to view analytics and insights represented as heatmaps, which display the count of syslog messages and reachability transitions of wired and wireless network events.

Procedure

Step 1 From the main menu, choose **Assurance** > **Dashboards** > **Issues and Events**.

Step 2 Click the **Event Analytics** tab. The Event Analytics dashboard opens with wired events.

Figure 43: Event Analytics dashboard



Event Analytics Dashboard	
Item	**Description**
Global	Click this icon in the top menu bar to select the site, building, or floor in the site hierarchy from the **Select a location** slide-in pane.
24 Hours **Time Range** setting	Allows you to display information on the window based on the time range you select. The default is **24 Hours**. To set the range of the timeline: **a.** From the **24 Hours** drop-down list, select a time range: **3 hours**, **24 hours**, or **7 days**. **b.** If you chose **Presets**, you can select from the **CURRENT** column (Today, Week, or Month) or the **LAST** column (24 hours, 7 days, 14 days, 30 days, or 60 days). **c.** Specify the **Start Date** and time, and the **End Date** and time. **d.** Click **Apply**.
KPI	Click this drop down to toggle the visibility of specific event categories such as Syslog Messages, Reachability Transitions, Client Onboardings, or Radio Events for Wired or Wireless devices.

Step 3 Click **Wired Events** to view the heatmaps that display the count of syslog messages and reachability transitions from the wired devices. The heatmaps include a breakdown of message severity data with a granularity of 15 minutes for up to a 24-hour time period. At 7 days, the granularity is 4 hours. At 14 and 30 days, the granularity is 12 hours. At 60 days, the granularity is 24 hours.

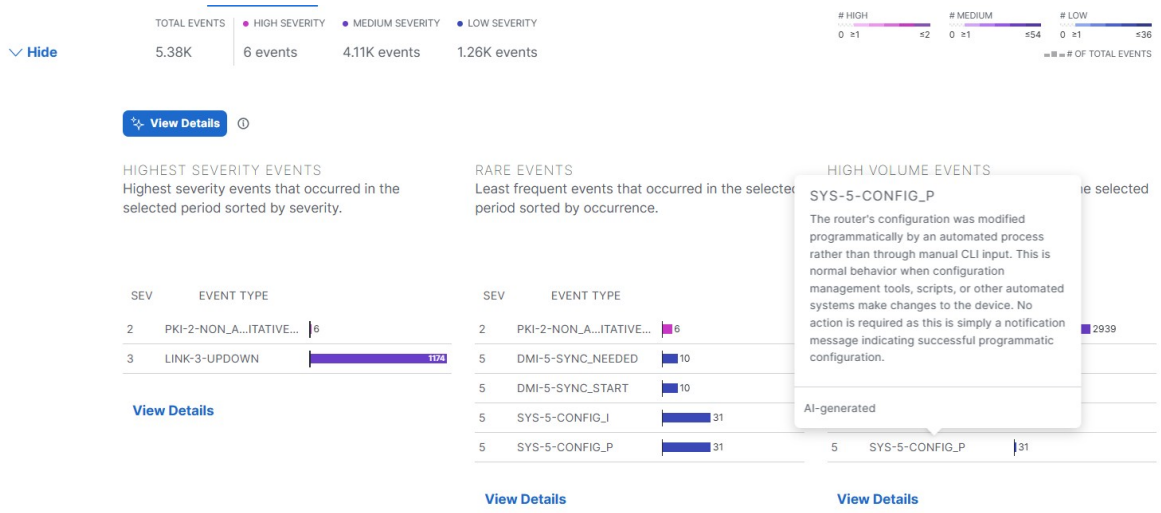
Syslog Messages:

- Use the time slider on the top of the heatmap to set the specific time period in the syslog messages heatmaps. View the total number of events and the count of high, medium, and low message severities.
- To view insights and analytics data syslog messages, click **Show Analytics**. A series of cards with different visualizations displays the counts of syslog messages or devices, with an order that is based on different analytics criteria. Syslog messages support these analytics:
  - Highest severity events: Highest severity events that occurred in the selected period sorted by severity.

- Rare events: Least frequent events that occurred in the selected period sorted by occurrence.
- High volume events: Most frequent events that occurred in the selected period sorted by occurrence.
- Message volume increase: Events with the highest increase in volume within the selected period sorted by variation.
- Message volume decrease: Events with the highest decease in volume within the selected period sorted by variation.
- New events: Events that started occurring at the end of the selected period sorted by occurrence.
- Most active devices: Devices that generated the highest volume of events in the selected period sorted by volume.

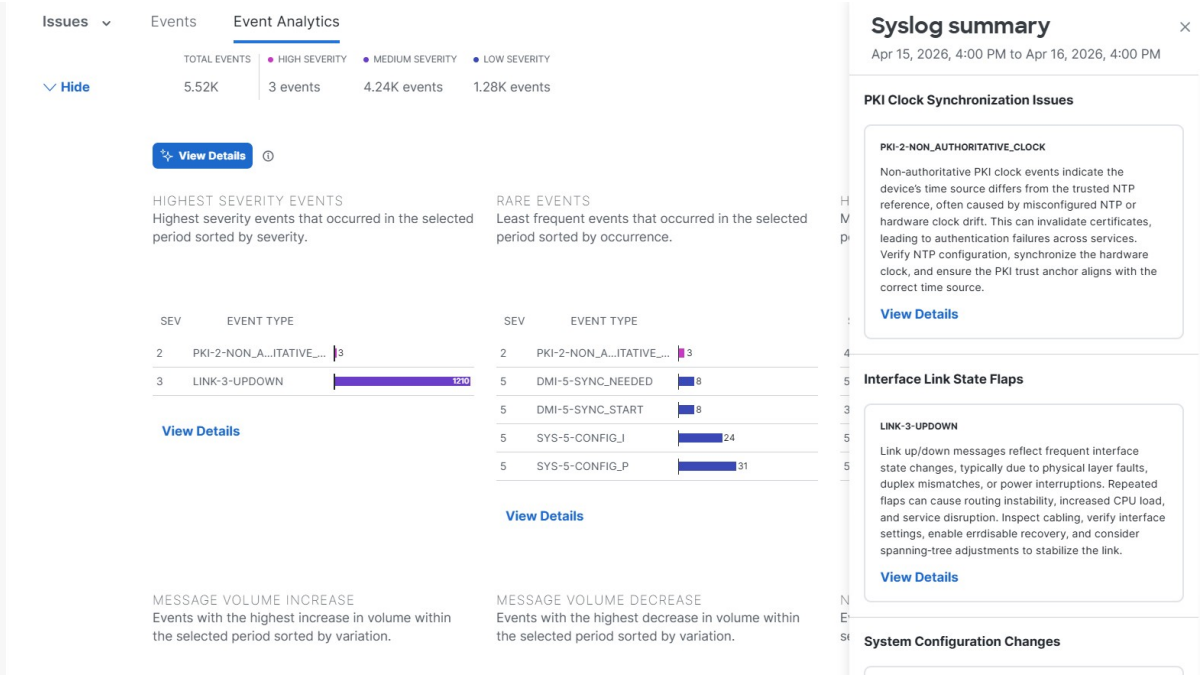
To quickly understand the purpose of a specific syslog, hover your cursor over the mnemonic. A tool tip displays a brief description explaining the event and providing guidance on whether to investigate further or ignore the event.

Figure 44: Analytics for syslog messages



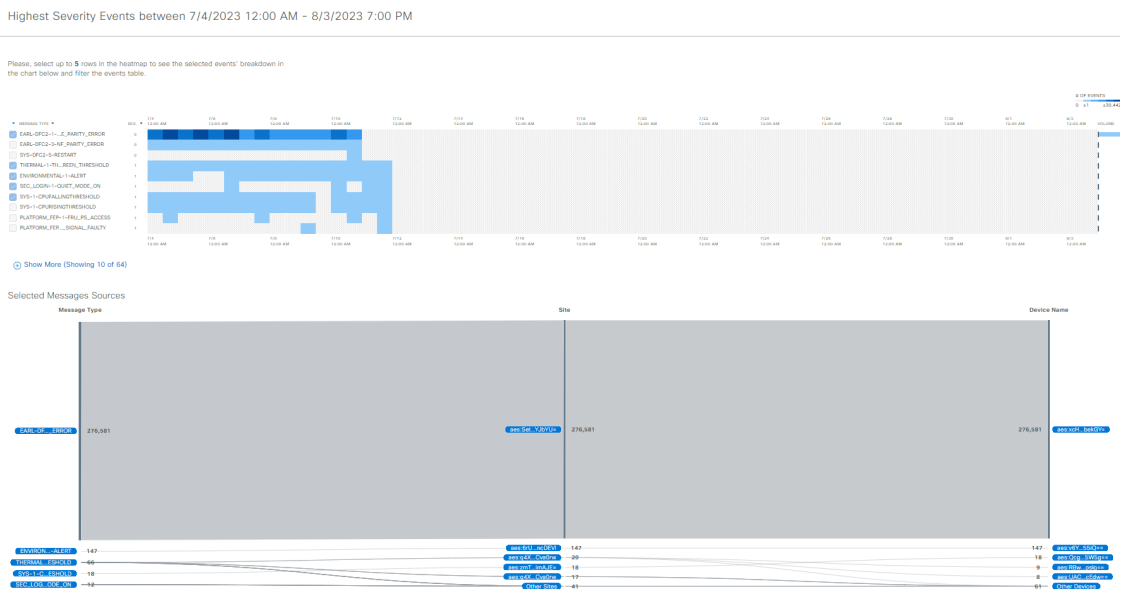
- Click View Details to view an AI syslog summarization and explanation that transforms raw syslog data into actionable insights.

Figure 45: AI syslog summarization and explanation



- Click **View Details** to view the detailed heatmap with a time series of event counts for each event type. You can select up to five syslog message types in the heatmap to filter the Sankey chart to show the distribution of the selected event type and to learn about the specific sites and device-generated events.

Figure 46: Syslog events heatmaps with Sankey chart



- You can select the message type, site, or device in the Sankey chart to filter the events table below the chart. Up to 10,000 events can be displayed in the events table. To create a user-defined issue, click messages in the events table and click **Confirm**.

Reachability Transitions:

- Use the time slider on the top of the heatmap to set the specific time period to view the total number of events, unreachable events, reachable events, and ping-reachable events.
- To view insights and analytics data for each reachability transition (top status transitions, top devices by events) from wired devices in a separate card, click **Show Analytics**.
- Click **View Details** to view the detailed heatmap with a time series of event counts for each event type. You can select up to five events in the heatmap to filter the Sankey chart to show the distribution of the selected event type and to learn about the specific sites and device-generated events.
- Select the from event, to event, site, or device in the Sankey chart to filter the events table to show the reachability transitions for each event. Up to 10,000 events can be displayed in the events table.

Step 4 Click **Wireless Events** to view the heatmaps that display the count of syslog messages and reachability transitions from the wireless devices. The heatmaps include a breakdown of message severity data with a granularity of 15 minutes.

Syslog Messages:

- Use the time slider on the top of the heatmap to set the specific time period in the syslog messages heatmaps. View the total number of events and the count of high, medium, and low message severities.
- To view insights and analytics data for each syslog message displayed in a separate card, click **Show Analytics**. The analytics cards are displayed for the available syslog messages with the severity and event type. Hover your cursor over the mnemonic on the syslog messages to view a tool tip with a brief description of the event.

  Click 

to view an AI syslog summarization and explanation that transforms raw syslog data into actionable insights.
- Click **View Details** to view the detailed heatmap with a time series of event counts for each event type. You can select up to five syslog message types in the heatmap to filter the Sankey chart to show the distribution of the selected event type and to learn about the specific sites and device-generated events.
- Select the message type, site, or device in the Sankey chart to filter the events table to show the syslog messages. Up to 10,000 events can be displayed in the events table.

Reachability Transitions:

- Use the time slider on the top of the heatmap to set the specific time period to view the total number of events, unreachable events, reachable events, and ping-reachable events.
- To view insights and analytics data for each reachability transition (top status transitions, top devices by events) from wireless devices displayed in a separate card, click **Show Analytics**.
- Click **View Details** to view the detailed heatmap with a time series of event counts for each event type. You can select up to five events in the heatmap to filter the Sankey chart to show the distribution of the selected event type and to learn about the specific sites and device-generated events.
- Select the from event, to event, site, or device in the Sankey chart to filter the events table to show the reachability transitions for each event. Up to 10,000 events can be displayed in the events table.

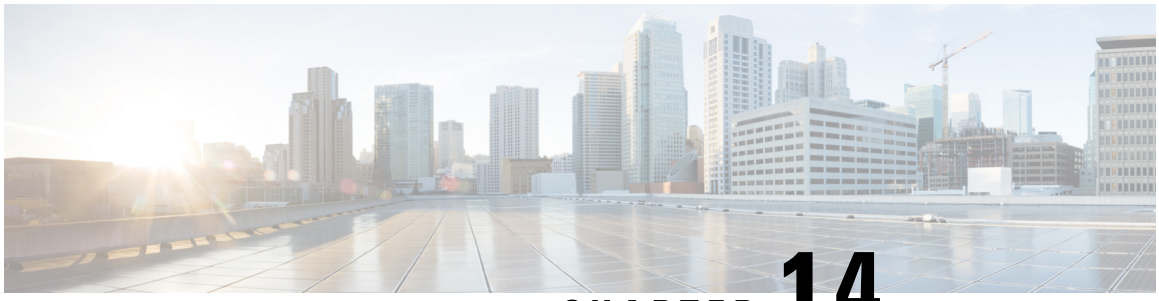
Step 5 In the events table below the Sankey chart, click 

for individual logs to transform raw syslog data into actionable insights. Review the AI-generated response for a detailed analysis, including:

- Summary: The AI generates concise summaries of syslog activity, highlighting the most impactful messages and trends.
- Impact: The potential effect of the event on your network. Assurance continuously gathers syslog messages from network devices. (Syslog data is retained for 3 months.)
- Cause: An analysis of why the event occurred.
- Remediation: Assurance offers suggestions to resolve issues efficiently, supported by Cisco's extensive networking expertise embedded in the OpenAI models.

Note
To disable the AI syslog summarization and tooltip, choose **System** > **Settings** > **External Services** > **Cisco AI Analytics**. Toggle off the **Enable AI Network Analytics** toggle button and click **Update**. Note that in doing so, you're disabling AI analytics collection for your Catalyst Center deployment.

To disable AI insights, choose **System** > **Settings** > **External Services** > **Cisco AI Analytics**. Toggle off the **Enable Non-anonymized Syslog Message Text Export** toggle button and click **Update**.



CHAPTER 14

Manage Sensors and Sensor-Driven Tests

- About sensors and sensor-driven tests, on page 305
- Provision sensors, on page 305
- Monitor and troubleshoot network health with sensors, on page 310
- Manage sensors and backhaul settings, on page 317
- Manage SCEP profiles, on page 321
- Sensor-driven tests, on page 322

About sensors and sensor-driven tests

Sensors use sensor-driven tests to determine the health of wireless networks. A wireless network includes AP radios, WLAN configurations, and wireless network services.

Assurance supports a dedicated sensor, which is dedicated hardware for doing sensor functions.

The dedicated Cisco Aironet 1800s Active Sensor gets bootstrapped using PnP. After this sensor obtains Assurance server-reachability details, it directly communicates with the Assurance server.

Provision sensors

Provision the wireless Cisco Aironet 1800s Active Sensor

Procedure

Step 1 If you are using the Cisco Aironet AP 1800s Sensor without an Ethernet module, you must enable `CiscoProvisioningSSID` on the wireless controller.

Note
For the Cisco Aironet 1800s Active Sensor earlier than Software Release 1.3.1.2, make sure that you do not select the sensor device profile **`CiscoProvisioningSSID`**. Instead, select your own SSID for backhaul purposes. See Manage backhaul settings, on page 319.

For Cisco Wireless Controllers, see Enable Provisioning SSID on the wireless controller, on page 306.

For Cisco Catalyst Wireless Controllers, see Enable Provisioning SSID on the Cisco Catalyst Wireless Controller, on page 307.

Step 2 Create a backhaul configuration for the sensor.

See Manage backhaul settings, on page 319.

Step 3 Provision the Cisco Aironet 1800s Active Sensor.

See Provision an AP or sensor device, on page 308.

Step 4 (Optional) After the sensor device is available in the device inventory, you can select to upgrade the software image. See the "Provision Software Images" topic in the *Cisco Catalyst Center User Guide*.

Enable Provisioning SSID on the wireless controller

Procedure

Step 1 Log in to the Cisco Wireless Controller.

The **Network Summary** page appears.

Step 2 Click the **Advanced** tab.

The **Summary** page appears.

Step 3 In the top menu bar, click the **Management** tab.

Step 4 From the left-navigation pane, choose **Cloud Services** > **Sensor**.

The **Backhaul Configuration** page appears.

Step 5 In the **SSID** field, enter **`TFTP`**.

Step 6 From the **Auth-type** drop-down list, select **Open**.

Step 7 From the **Provisioning** drop-down list, select **Enable**.

Step 8 Make sure that the **DHCP Interface** drop-down list is set to **management**.

Step 9 Click **Apply**.

After provisioning is enabled, a hidden WLAN called `CiscoSensorProvisioning` is created, and the sensor joins using an EAP-TLS client certificate. This enables the sensor to find the Catalyst Center IP address, which is done using DHCP Option 43 or through DNS.

Enable Provisioning SSID on the Cisco Catalyst Wireless Controller

Procedure

Step 1 Log in to the Cisco Catalyst Wireless Controller GUI.

Step 2 From the left-navigation pane, choose **Configuration** > **Cloud Services**.

The **Cloud Services** page appears.

Step 3 In the **Network Assurance** tab, do these steps:

a) From the **Network Assurance Configuration** area, set the **Service Status** toggle to **Enabled**.

b) From the **Provisioning** area, set the **Provisioning** toggle to **Enabled**.

Step 4 (Optional) In the **VLAN Interface** field, enter the name of the VLAN interface.

Step 5 Click **Apply**.

After Provisioning is enabled, a hidden WLAN called **CiscoSensorProvisioning** is created.

This error message appears in the bottom-right corner of the window.

```
Error in Configuring
CLI Line 2 Please associate the wlan and policy profile CiscoSensorProvisioning to the desired AP.
```

Note
This message is not an error. The message provides information about the action that must be done.

Step 6 Verify that the **CiscoSensorProvisioning** policy profile is created.

a) From the left-navigation pane, choose **Configuration** > **Policy**.

The **Policy Profile** page appears.

b) Verify that the **CiscoSensorProvisioning** policy appears under the **Policy Tag Name** column.

Step 7 Associate the WLAN and policy profile **CiscoSensorProvisioning** to the appropriate AP. Do these steps:

a) From the left-navigation pane, choose **Configuration** > **Tags**.

The **Manage Tags** page appears.

b) In the **Policy** tab, click **Add**.

c) In the **Name** field, enter a unique name for the Policy Tag.

d) Click **Add**.

e) From the **WLAN Profile** drop-down list, select **CiscoSensorProvisioning**.

f) From the **Policy Profile** drop-down list, select **CiscoSensorProvisioning**.

g) Click ✓.

h) Click **Save & Apply to Device** to save the Policy Tag.

Note
Changing the Policy Tag on an AP may cause clients associated with the AP to disconnect and reconnect.

Provision an AP or sensor device

Use this procedure to claim an AP or sensor device from the Plug and Play Devices list. Alternatively, you can claim a device from the device **Details** window by clicking **Claim**.

Before you begin

- Ensure that Cisco network devices to be provisioned have a supported software release and are in a factory-default state. If you are using a network device that was previously configured or is in an unknown state, check the device clean-up and reset details in the Network Plug and Play Troubleshooting Guide.
- For APs in intent-based networks, define the site within the network hierarchy. Refer to Network hierarchy, on page 30.
- Define the CLI and SNMP credentials for the devices.

Note You can claim wireless devices using CLI, SNMPv2c, or SNMPv3 credentials. If you use SNMPv2c, provide both Read Only and Read Write credentials.

- For provisioning a sensor device, ensure that the sensor is reachable through the Catalyst Center enterprise IP address (private/enp9s0). A DHCP option 43 string makes the device reachable in unclaimed mode in Catalyst Center; however, to claim the device, it must be reachable from the interface enp9s0 IP address. In the DHCP server, configure the NTP server (DHCP option 42) and the vendor-specific DHCP option 43 with ACSII value "5A1D;B2;K4;I172.16.x.x;J80;", where 172.16.x.x is the virtual IP address of Catalyst Center associated with the enp9s0 interface.

Procedure

Step 1 Navigate to the **Plug and Play** to choose the required devices.

a) From the main menu, choose **Provision** > **Plug and Play**.
b) View the devices in the table.

You can use the search bar to find specific devices.

c) Check the check box next to the devices that you want to claim.
d) From the menu bar above the device table, choose **Actions** > **Claim**.

Step 2 (Optional) In the **Assign Site** window, do these steps:

a) Change the device hostname, if needed.
b) Assign a site by doing any of these tasks:

- To assign a different site to each device, click **Assign**, and from the **Select a Site** drop-down list, select a site.
- To assign the same site as the first device to all other devices, in the **Actions** column, hover your cursor over the ellipsis icon and select **Apply Site to All**.
- To assign a site from any device to some other devices, in the **Actions** column, hover your cursor over the ellipsis icon and select **Assign this Site to Other Devices**, select the devices, and click **Assign**.
- To clear the site assigned to the devices, click **Clear Site**.

If the wireless network profile associated with the assigned site has an onboarding template, Catalyst Center uses this template for PnP onboarding.

Note
In the **System** > **Settings** > **Device Settings** > **PnP AP Location** window:

- If the **Configure AP Location** check box is checked, Configure APs assigns this site as the AP location during PnP onboarding.
- If the **Configure AP Location** check box is unchecked, Catalyst Center does not configure this site as the AP location during PnP onboarding. You can configure the AP location using the **Configure Access Points** workflow.

For more information, refer to "Configure AP location for PnP onboarding" in the *Cisco Catalyst Center Administrator Guide*.

c) Click **Next**.

Step 3 In the **Assign Configuration** window, do these steps:

a) In the **Configuration** column, click **Assign** for the device that you want to configure.

b) If the device configuration doesn't need any changes, click **Cancel** and continue to the next step. Otherwise, change or configure any of these settings:

- **Device Name**: Change the device hostname, if needed.
- **Template**: From this drop-down list, select an onboarding configuration template to apply to the device. If there is only one onboarding configuration template defined for this device type, it is chosen by default.

  Note
  If you have not assigned the device to a site, you must choose a template for the device. The template that you choose must include the CLI commands necessary to configure the global device credentials on the device. Otherwise, the device is added to the inventory in an unmanaged state.

- For an AP, select an AP zone from the **AP Zone** drop-down list. The **RF Profile** is auto-populated, and the SSID count appears based on the selected AP zone. When you select the default AP zone, choose the RF profile.
- For an AP, in the **Radio Frequency Profile** drop-down list, select a radio frequency profile to apply to the device. This may be set if you designated one profile as a default.
- For a sensor, in the **Sensor Settings** drop-down list, select the sensor device profile (backhaul) to apply to the device.

  Note
  For Cisco Aironet 1800s Active Sensor earlier than 1.3.1.2, make sure that you do not select the sensor device profile `CiscoProvisioningSSID`. Instead, select your own SSID for backhaul purposes.

- If you made any changes, click **Save**; otherwise, click **Cancel** to return to the list and configure other devices.

c) From the **Clear Configuration** drop-down list, select any these options:

- **Clear Device Certificates**: Select this option and check the check box next to each of the devices that you want to clear the certificate from, and click **Clear**.
- **Clear Images**: Select this option and check the check box next to each of the devices that you want to clear the image from, and click **Clear**.

- **Clear Templates**: Select this option and check the check box next to each of the devices that you want to clear the template from, and click **Clear**.
- **Clear License Levels**: Select this option and check the check box next to each of the devices that you want to clear the license level from, and click **Clear**.

d) To apply an image or template from one device to other devices, in the **Actions** column, hover your cursor over the ellipsis icon and select **Apply Image to Other Devices** or **Apply Template to Other Devices**.
e) If you selected multiple devices to provision, click **Assign** for the next device in the list and repeat the configuration steps, until you have done this for all devices.
f) After you have configured all the devices, click **Next**.

Step 4 In the **Provision Templates** window, select the template from the **Devices** area, enter your domain name in the **domain** field, and click **Next**.

Note
If device is assigned to a site, click **Next**.

Step 5 In the **Summary** window, view details about the devices and their configuration preview.

Step 6 Check the **Device Configuration** column for each device to verify if the configuration preview succeeded.

If the preview shows an error, you can click the **Actions** link in the error message above the table to verify what actions you need to take. You can click an action to open a new tab with the window where a change is needed. You must resolve any issues before claiming the device, to avoid provisioning errors. You may need to go back to the **Assign Configuration** step and change the configuration, revisit the **Design** area to update network design settings, or resolve any network connectivity issues. After you have resolved the problem, you can go back to this tab, click **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**. Ensure that the wireless controller that is managing a device has been added to the inventory and assigned to the site where the device is assigned.

Step 7 In the **Device Configuration** column, click **Preview Configuration** to review the configuration.

Step 8 Click **Claim**.

Step 9 In the confirmation dialog box, click **Yes** to claim the devices and start the provisioning process.

Note
If there is a conflicting operation for the selected site, to continue with the current configuration, you must either wait for the existing, scheduled, or pending-review operations to complete or discard the operations.

What to do next

If you have configured network settings, provision these settings on the devices. For more information, refer to the "Complete the provisioning process" in the *Cisco Catalyst Center User Guide*.

Monitor and troubleshoot network health with sensors

Monitor and troubleshoot network health with all wireless sensors

Use this procedure to get a global view of the network health from the data received from all wireless sensors.

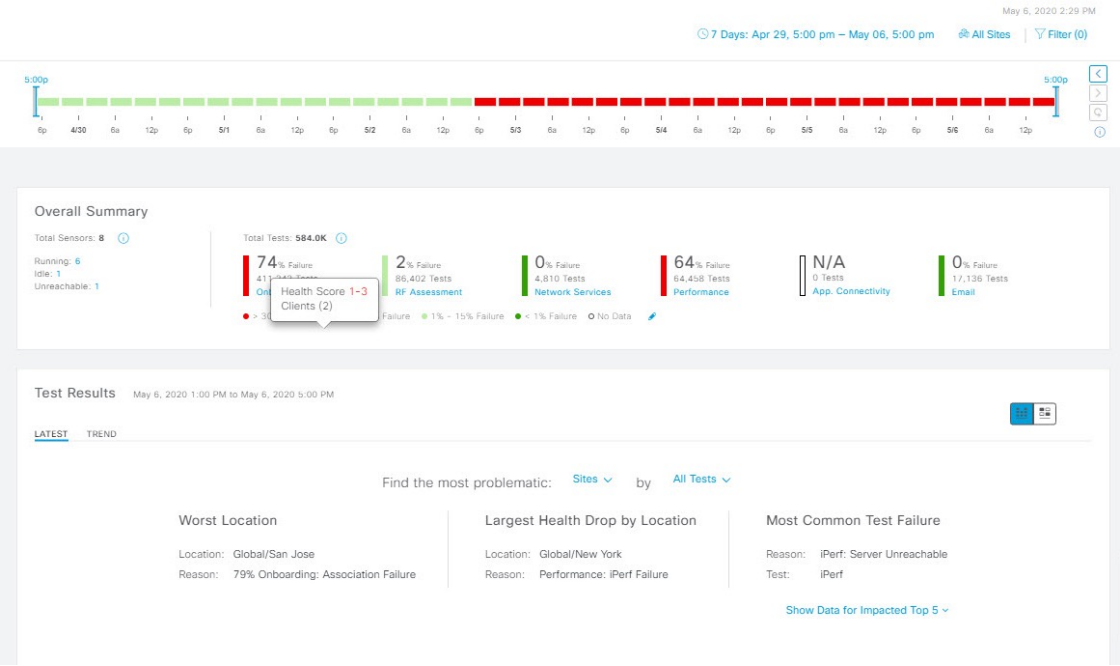
Before you begin

Make sure you have added and scheduled sensor-driven tests. See Create and run sensor-driven tests using templates, on page 322.

Procedure

Step 1 From the main menu, choose **Assurance** > **Dashboards** > **Wireless Sensors**.

Figure 47: Wireless sensors dashboard



Step 2 Use the **Wireless Sensors** dashboard top-menu bar for this functionality:

Timeline area	
Item	**Description**
Time Range setting	Enables you to display data within a specified time range on the dashboard. Do these steps: **a.** From the drop-down menu, select the length of the range: **3 Hours**, **24 Hours**, or **7 Days**. **b.** Specify the **Start Date** and time; and the **End Date** and time. **c.** Click **Apply**.

Timeline area	
Item	**Description**
 **Hierarchy Location** setting	Enables you to select the data displayed on the dashboard from the selected locations in your network. Check the check boxes for the sites, buildings, or floors in your network to display its sensor data on the dashboard. **Note** You can't exclude all locations from displaying data on the dashboard. Unchecking all locations results in data from all locations to be displayed on the dashboard.
Filter icon	Enables you to select the data displayed on the dashboard based on SSIDs and radio frequency bands. To add filters: **a.** Click **Filter**. **b.** From the drop-down menu, click the **SSID** tab and check the check boxes for the desired SSIDs. **c.** From the drop-down menu, click the **Band** tab and select the radio button for **2.4 GHz** or **5 GHz**. **d.** Click **Apply**. To remove all selected filters: **a.** Click the **Filter** icon. **b.** Click **Clear Filters**.

Step 3 Use the **Timeline** to view the percentage of overall test failures for a specific time within a time range.

The time range is determined by what is configured in the setting above the timeline.

The blocks in the timeline represents a specific time window within the time range. The period of time for each block is determined by time range set for the timeline:

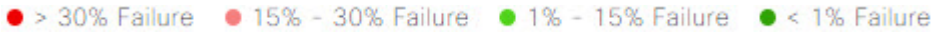
- For a **3 Hours** time range, each block represents 15 minutes.
- For a **24 Hours** time range, each block represents 30 minutes.
- For a **7 Days** time range, each block represents 4 hours.

The blocks are color-coded to indicate the severity of percentage of test failures.

Hover your cursor over a block to view a breakdown of percentage of test result failures for each test category.

Step 4 Use the **Overall Summary** dashlet for this functionality:

Overall summary dashlet	
Item	**Description**
Total Sensors area	Provides an overall view of all the sensors in your network and their status. The status types of the sensor include: • **Idle**: The sensor is onboarded and does not have any scheduled tests. • **Running**: The sensor is onboarded and is included in a test suite or test template. • **Unreachable**: No heartbeat received from the sensor. Click the hyperlinked number next to the status type to open a slide-in pane that displays the sensors with that status. In the slide-in pane, you can click the sensor name under the **Name** column to get a 360° view of that sensor. See Monitor and troubleshoot network health with a wireless sensor, on page 315.
Total Tests	Displays the total number of tests performed by all sensors and a breakdown of the test results based on these test categories: **Onboarding** **RF Assessment** **Network Services** **Performance** **App. Connectivity** **Email** You can click a test category to open a slide-in pane with additional details about its test results. In the slide-in pane, click the test type tabs on the left to populate the slide-in pane with data from the test type. The slide-in pane displays: • A chart that displays the test results, future trends, and list of APs used in the tests. **Note** For the **RF Assessment** test category, the chart displays the KPIs data rate and SNR, instead of test results. • Data type categories: **Top Failure Reasons** (if applicable), **Top APs**, **Top Locations**, **Top Bands**, and **Top SSIDs** (if applicable). • A table with detailed data of the sensors that ran the tests. You can click the data segments from the data type categories to filter the data that appears in the table.

Overall summary dashlet	
Item	**Description**
 **Edit Threshold**	Enables you to customize the thresholds of the color-coded ranges that indicate the severity of percentage of test result failures.  To customize the thresholds: **a.** Click the edit () icon. **b.** In the **Edit Threshold** menu, enter the percentage values in the fields for each color-coded range. **c.** Click **Apply**.

Step 5 Use the **Test Results** dashlet to view the locations in your network with the most sensor test result failures:

Test results dashlet	
Item	**Description**
Latest tab and **Trend** tab	These tabs determine the scope of the data that is displayed in the dashlet: • **Latest**: Displays the data from the selected time window in the timeline on the top of the window. • **Trend**: Displays data from the last 24 hours.
 **Heatmap View** and **Card View** toggle	This toggle button allows you to change the view of the dashlet to the **Heatmap View** and the **Card View**. The **Heatmap View** is displayed by default.

Test results dashlet	
Item	**Description**
Heatmap View	Displays the top 5 rankings of these statistical categories at the top of the dashlet: • **Worst Location, Buildings, Floors,** or **Sensors**: Sites, buildings, floors, or sensors with the highest test result failure percentage. • **Largest Health Drop by Location, Buildings, Floors,** or **Sensors**: Sites, buildings, floors, or sensors with the largest sudden drop. • **Most Common Test Failure**: Test types that had the highest test result failures. Only the top spot for each statistical category is displayed. Click **Show Data for Impact Top 5** to see the complete rankings. Below the rankings is a heatmap representation of the sensor test result failures. In the heatmap, the blocks are color-coded to indicate the severity of percentage of test result failures. • Use the drop-down lists in the **Find the most problematic** area to sort the data that is displayed in the rankings and heatmap. In the first drop-down list you can sort the data by locations or sensors. In the second drop-list you can sort the data by test types. • Use the search field to filter the heatmap for specific locations or sensors. • Hover your cursor over a block to view the exact percentage value for test result failures. • Click a color-coded block to open a slide-in pane with further details about the test results at that intersect.
Card View	Displays the data in a card format for high-level monitoring and comparison. Use the drop-down lists in the **Find the most problematic** area to sort the data.

Monitor and troubleshoot network health with a wireless sensor

Use this procedure to get a 360° view of a specific wireless sensor. You can view a sensor's test results, performance trends, and neighboring APs. You can also view and download a sensor's event logs.

Procedure

Step 1 From the main menu, choose **Assurance** > **Dashboards** > **Wireless Sensors**.

The **Sensor Dashboard** appears.

Step 2 From the **Sensors Dashboard**, do one of these tasks:

- In the **Overall Summary** dashlet, click the hyperlinked number from the **Running**, **Idle**, or **Unreachable** areas.

Then in the **Sensor Status** slide-in pane, click the hyperlinked name of the sensor.

- In the **Overall Summary** dashlet, click a hyperlinked test category.

  In the slide-in pane, click the hyperlinked name of the sensor from the table.

- In the **Test Results** dashlet, click a color-coded box from the heatmap.

  In the slide-in pane, click the hyperlinked name of the sensor from the table.

A 360° view of the sensor appears.

Step 3 Click the **Time Range** setting at the top-right corner to specify the time range of data that is displayed on the window:

a) From the drop-down menu, select a time range: **3 hours**, **24 hours**, or **7 days**.
b) Specify the Start date and time; and the End date and time.
c) Click **Apply**.

Step 4 Use the header above the timeline to view the basic information of the sensor such as the sensor's serial number, current state, uptime, backhaul type, IP address, and so on. You can also view and download the sensor's event logs.

To view and download the event logs:

a) Click **View Logs** at the end of the header.
The **Event Logs** slide-in pane appears which displays the event logs.
b) In the **Event Logs** slide-in pane, click **Request Support Bundle** to generate the support bundle file which contains the event logs.

Attention
It takes about three to five minutes for a support bundle request to be ready for download.

c) Click **Download Support Bundle** to open the download prompt for the support bundle.

Step 5 Use the timeline to view the percentage of overall test failures for a specific time within a specified time range. The timeline has this functionality:

- Set the time range with the **Time Range** setting above the time line.
- View the percentage of overall test failures for a specific time window indicated by the blocks in the timeline. You can hover your cursor over a block to view a breakdown of percentage of test result failures for each test category.

Step 6 Use the collapsible categories to view information about test results, performance trends, and neighboring APs:

Test results category

Displays a heatmap representation of the sensor test result failures for each tested AP. In the heatmap, the blocks are color-coded to indicate the severity of percentage of test result failures.
• Use the **Test Type** drop-down list to sort the data by test type.
• Use the search field to filter the heatmap for specific APs.
• Hover your cursor over a block to view the exact percentage value for test result failures.
• Click the **Latest** and **Trend** tabs to change the scope of data displayed in the category:
  • **Latest**: Displays the data from the selected time window in the timeline on the top of the window.
  • **Trend**: Displays data from the last 24 hours.

Sensor performance trend category
Displays a line graph or chart of the sensor performance data based on test types. For time-based test types, a comparative view is used to display the performance of the current sensor, top performing sensor, and worst performing sensor. • Use the **Test Type** drop-down list to display data for a specific test type. • For time-based test types, click **+ Add Custom Location** to add the sensor performance data for a specific location using the menu. You can select the sensor performance for sites, buildings, or floors.

Neighboring APs category
Displays the sensor's neighboring APs along with its RSSI in a list view and a map view. To filter the APs based on frequency bands, use the radio buttons in the **Band** area. **Note** The sensor scans for neighboring APs every 30 minutes.

Manage sensors and backhaul settings

Manage sensors in your network

Use this procedure to view the onboarded sensors in your network. You can enable SSH, the status LED, and change the name for these sensors.

Before you begin

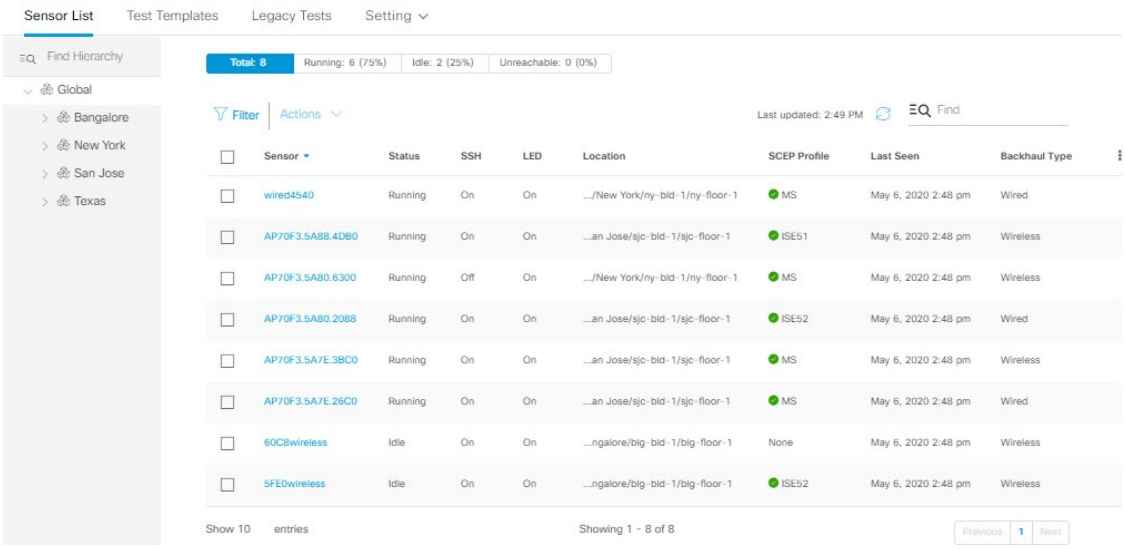
Make sure the sensors are assigned to a site.

Procedure

Step 1 From the main menu, choose **Assurance** > **Settings** > **Sensors**.

The **Sensor List** window appears.

Figure 48: Sensor List window



Step 2 Use the left pane to specify the network hierarchy you want to view.

Step 3 Click the categories above the table to view the sensors that fit their criteria. The categories are:

- **Total**: All the sensors in the selected network hierarchy.
- **Running**: Displays the sensors that are currently running tests.
- **Idle**: Displays the sensors that have no assigned tests.
- **Unreachable**: Displays the sensors that are onboarded but are not responding.

Step 4 You can customize the data that is displayed in the table:

a) Click ⋮.
b) From the menu, check the check boxes of the data you want displayed in the table.
c) Click **Apply**.

Step 5 To configure the SSH settings for a sensor:

a) Check the check box of the sensor.
b) Hover your cursor over the **Actions** drop-down list and select **Edit SSH**.

The **Edit SSH** slide-in pane appears.

c) In the **Edit SSH** slide-in pane, click the **SSH** toggle to enable SSH.
d) In the **Username** and **Password** fields, enter the desired SSH credentials.
e) Click **Save**.

Step 6 To change the status LED of a sensor:

a) Check the check box of the sensor.
b) Hover your cursor over the **Actions** drop-down list and select **Edit LED**.

The **Edit LED** slide-in pane appears.

c) In the **Edit LED** slide-in pane, click the **LED** toggle to enable or disable the status LED.

Step 7 Click **Save**.

Step 8 To change the name of a sensor:

a) Check the check box of the sensor.

b) From the **Actions** drop-down list, select **Edit Sensor Name(s)**.

The **Edit Sensor Name(s)** slide-in pane appears.

c) In the **Edit Sensor Name(s)** slide-in pane, enter the name in the **Name** field.

d) Click **Save**.

Step 9 To enroll the sensors using SCEP profiles:

a) Check the check box of the sensor.

b) From the **Actions** drop-down list, select **Enroll using SCEP**.

The **Enroll using SCEP** slide-in pane appears.

c) Select the SCEP profile from the **Select SCEP Profile** drop-down list.

See Manage SCEP Profiles for more information.

d) Select the **Username** and **Password** and provide the required details. If you select the **Custom** username option, then select **No Password**.

e) Click **Save**.

f) To check status, see the **SCEP Profile** column in the **Sensor List** window. A green check mark (✓) indicates success, and a red **X** icon indicates failure. Hover your cursor over the ✓ or **X** icon to get more information.

Manage backhaul settings

Use this procedure to view, create, and manage backhaul configurations for wireless sensors. A wireless sensor requires a backhaul SSID to communicate with Catalyst Center.

For information about a persistent wireless backhaul connection, see Persistent wireless backhaul connections on sensor devices, on page 321.

Procedure

Step 1 From the main menu, choose **Assurance** > **Settings** > **Sensors**.

The **Sensor List** window appears.

Step 2 Hover your cursor over the **Settings** tab and select **Backhaul Settings**.

Step 3 You can add and manage backhaul SSIDs by doing these steps:

a) Click **+ Add Backhaul**.

The **Create Sensor Backhaul SSID Assignment** window appears with two areas: **Wired Backhaul** and **Wireless Backhaul**.

b) In the **Settings Name** field, enter a name for the backhaul SSID.

c) In the **Wired Backhaul** area, do this configuration:

- **Level of Security**: Displays the encryption and authentication type used by the selected SSID. The available security options are:
  - **802.1x EAP**: Standard used for passing Extensible Authentication Protocol (EAP) over wired LAN.
  - **Open**: No security or authentication is used.
- **EAP Method**: If you select **802.1x EAP**, you must select one of these EAP methods for user authentication from the drop-down list:
  - **EAP-FAST**: Enter the username and password in the fields provided.
  - **PEAP-MSCHAPv2**: Enter the username and password in the fields provided.
  - **EAP-TLS**: Select **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

    If you select **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click **+ Add New Certificate Bundle**, and enter the username and certificate bundle password.
  - **PEAP-TLS**: Select **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

    If you select **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click **+ Add New Certificate Bundle**, and enter the username and certificate bundle password.

d) In the **Wireless Network Name (SSID)** area, select the wireless network (SSID) and do this configuration.

- **Level of Security**: Displays the encryption and authentication type used by the selected SSID. The available security options are:
  - **WPA2 Enterprise**: Provides a higher level of security using Extensible Authentication Protocol (EAP) (802.1x) to authenticate and authorize network users with a remote RADIUS server.
  - **WPA2-Personal**: Provides a good security using a passphrase or a preshared key (PSK). This allows anyone with the passkey to access the wireless network.

    If you select **WPA2 Personal**, enter the passphrase in the **Passphrase** text box.
  - **PSK Format**: The available preshared key formats are:
    - **ASCII**: Supports ASCII PSK passphrase.
    - **HEX**: Supports 64-character HEX key PSK password.
  - **Open**: No security or authentication is used.

e) Click **Save**.

Step 4 You can edit the existing backhaul configurations by doing these steps:

a) Check the check box of the backhaul configuration.
b) Hover your cursor over the **Actions** drop-down list and select **Edit**.

Step 5 You can delete a backhaul configuration by doing these steps:

a) Check the check box of the backhaul configuration.
b) Hover your cursor over the **Actions** drop-down list and select **Delete**.

Persistent wireless backhaul connections on sensor devices

Catalyst Center supports a persistent wireless backhaul connection on sensor devices, which means that the wireless connection is "always on" regardless of wireless testing activities.

- With a dedicated backhaul connection, the wireless sensor uses these two MAC addresses for backhaul and wireless purposes:
  - Base Radio + 0x10 (Backhaul SSID)
  - Base Radio + 0x11 (Test SSID)

  The wired sensor uses the Base Radio + 0x10 (Test SSID) MAC address for testing purposes.
- The sensor uses *dual* concurrent radio operations, one for the backhaul connection and the other for wireless tests.
- Backhaul connection interruptions occur during scanning and switching interfaces to test different bands.
- The frequency of backhaul connection disruptions is dependent on the test configuration.
- The backhaul connection is not persistent if both backhaul and test SSIDs are in one band.

Manage SCEP profiles

Use this procedure to view, create, and manage Simple Certificate Enrollment Protocol (SCEP) profiles, which are used to enroll wireless sensors.

Procedure

Step 1 From the main menu, choose **Assurance** > **Settings** > **Sensors**.

Step 2 Click **Setting** > **SCEP Profiles**.

Step 3 To add and manage an SCEP profile:

a) Click **Add SCEP Profiles**.

The **Create SCEP Profile** window appears.

b) In the **Create SCEP Profile** window, provide these details:

- **SCEP Profile Name**: Enter a name for the SCEP profile.
- **URL Base**: Enter a valid server.

  Note
  For **ISE**, enter this information:

  http://*ISE_IP_or_FQDN_Name***:9090/auth/caservice/pkiclient.exe**

  For **Microsoft CA**, enter this information:

  http://*Microsoft_SCEP_IP_or_FQDN_Name*/**CertSrv/mscep/mscep.dll**

- **Common Name**: Enter a valid name.

- **State**
- **Country Code**
- **Locality**
- **Organization**
- **Organization Unit**
- **Email**
- **Server certificate fingerprint**

c) Click **Save**.

Step 4 To edit an existing SCEP profile:

a) Check the check box next to the SCEP profile.
b) From the **Actions** drop-down list, select **Edit**.

Step 5 To delete a SCEP profile:

a) Check the check box next to the SCEP Profile.
b) From the **Actions** drop-down list, select **Delete**.

Sensor-driven tests

Create and run sensor-driven tests using templates

Use this procedure to create and run sensor-driven tests using templates. The workflow for sensor-driven tests using templates consists of two parts:

1. **Create the test template**: Configure the test configurations such as the SSIDs to test, test types to use, and the AP coverage.
2. **Deploy the test template**: After a test template is created, select the locations for testing and set the test schedule. After a test template is deployed, it is ready to be run.

Using templates is beneficial if you have a use case that requires a sensor-driven test to be run at different locations and with different schedules. With templates, you can create duplicates that can be deployed for each instance of the test location and schedule. This saves you time from having to recreate the same test for each instance.

Before you begin

- If you are using the Cisco Aironet 1800s Active Sensor to run sensor-driven tests, make sure that the sensor is provisioned using PnP, so that it displays under **Inventory**. See Provision the wireless Cisco Aironet 1800s Active Sensor, on page 305.
- If a sensor test template restarts, all sensors on that template begin running their tests at the same time, which causes the result graphs to show a cyclical pattern.

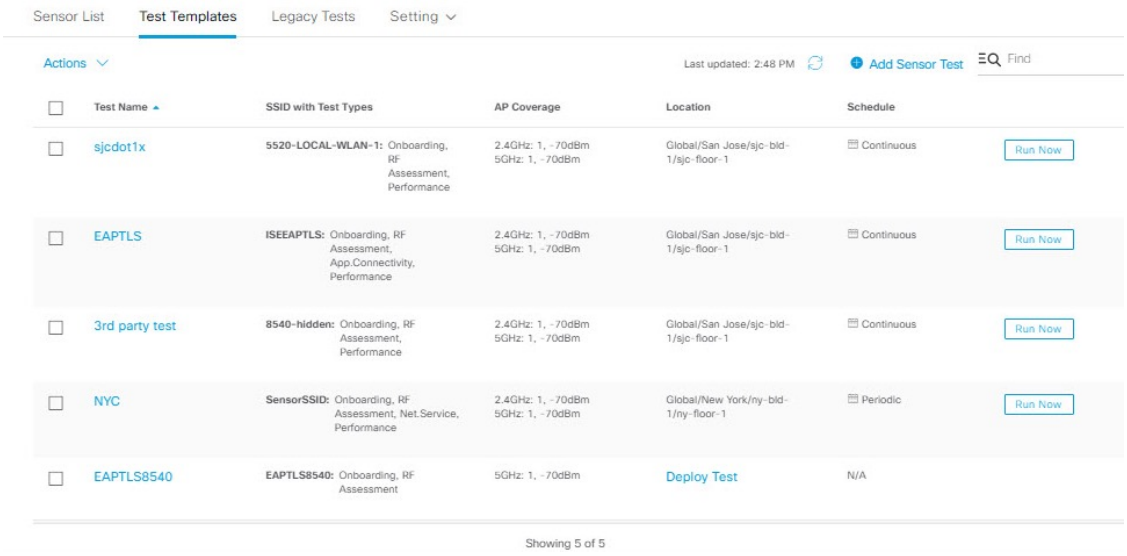
Procedure

Step 1 From the main menu, choose **Assurance** > **Sensors**.

Step 2 Click the **Test Templates** tab.

The **Test Templates** window appears.

Figure 49: Test Templates window



Step 3 Click **+ Add Sensor Test** to create a new sensor test template.
The workflow for creating a sensor test template appears.

Step 4 On the **Set up Sensor Test** window, configure these settings:

- **Test Template Name**: Enter the name for the test.

  Note
  Use only letters, numbers, underscores, hyphens, and periods.

- **SSID Selection**: Check the check boxes for the SSIDs you want to include for the sensor test.

Step 5 On the **Enter SSID Credentials** window, enter the credentials for the selected SSIDs:

- For SSIDs with **Open** security, select these options:
  - **Open**: For SSIDs with WebAuth passthrough, enter the email address.
  - **ISE Guest Portal**: Select the labels for the ISE guest portal.
  - **Clearpass Guest Portal**: Select the labels for the Clearpass guest portal and then click **Apply**.
- For SSIDs with **WPA2 Personal** security, enter the password.
- For SSIDs with **WPA2 Enterprise** security, enter the EAP method, username, and password.

Step 6 To enable proxy settings:

a. Check the **Add Proxy Settings** check box.

b. Configure these proxy settings:

- **Proxy Server**
- **Proxy Port**
- **Proxy UserName**
- **Proxy Password**

Step 7 On the **Define Sensor Test Category Details** window, check the check boxes for the tests that you want to include:

a) For the **Onboarding** test category, the test types are **Association**, **Authentication**, and **DHCP**.

Note
All of these test types are selected by default and cannot be excluded from the test template.

b) For the **RF Assessment** test category, the test types are **Data Rate** and **SNR**.

Note
All of these test types are selected by default and cannot be excluded from the test template.

c) For the **Network Services Tests** test category, select from these test types:

- **DNS**: Resolves the IP address for the domain name.
- **RADIUS**: The sensor acts as a Dot1x supplicant and authenticates through wireless.

d) For the **Performance Tests** test category, select from these test types:

- **Internet (NDT)**: Does a speed test using Network Diagnostic Tool (NDT).

  If you have a Network Diagnostics Test (NDT) server, enter the IP address of the NTD server in the field provided. If the NDT server is reachable through a proxy server, enter the IP address of the proxy server in the field provided.

- **iPerf3**: iPerf3 test is a tool used to measure network performance. This feature allows you to perform a speed test in the network with a certain amount of traffic to determine whether the test is able to pass through the traffic.

  To run the iPerf3 test, check the iPerf3 check box, and then enter the IP address of the iPerf3 server, UDP bandwidth, and port details in the fields provided.

  iPerf3 Limitations

  - You can add up to five iPerf3 servers.
  - You can configure each iPerf3 server to use a maximum of five ports per template. Sensors randomly select the port in which it wants to run the iPerf3 test.
  - Two sensors cannot connect to the same port concurrently on a given iPerf3 server.
  - The “iPerf: Server Busy" error message indicates that there are not enough iPerf3 instances to support the number of the sensors that are running the iPerf3 test.

    To resolve this issue, do one of these tasks:

- Add iPerf3 server instances. To do so, expand the ports that support iPerf3 testing on the existing servers.
- Reduce the number of sensors that are configured to run the iPerf3 test. To do so, create a separate template for iPerf3 testing.

- **IP SLA**: Runs UDP jitter, UDP echo, packet loss, and latency measurements from sensor to APs.

  To run the IPSLA test, select a **Service Level** option for each SSID from the drop-down list. Options are **Platinum** (voice), **Gold** (video), **Silver** (best effort), and **Bronze** (background).

e) For the **Application Tests** test category, select from these test types:

- **Host Reachability**: Tests for reachability using (ICMP) echo request.
- **Web**: Tests for access to the provided URL and verification of the response data.
- **FTP**: Tests for file upload and download operations

  Note
  The maximum file size for the sensor test is 5 MB.

f) For the **Email** test category, select from these test types:

- **POP3**: Post Office Protocol3, connects to POP3 server TCP port (110).
- **IMAP**: Internet Message Access Protocol, connects to IMAP server TCP port (143).
- **Outlook Web Access**: Logs into the Outlook Web Server (OWS) and verifies access.

Step 8 On the **Select AP Coverage** window, do these steps:

a) Check the frequency band check boxes (**2.4GHz** and **5GHz**) that you want to test.
b) From the **Number of Target APs** drop-list for the selected bands, select the number of APs that you want the sensor to test against.

Note
You can select a maximum of five APs.

c) In the **RSSI Range** slider for the selected bands, drag the slider to the desired RSSI threshold.

Step 9 On the **Summary** window, review the template settings.

To reconfigure the settings, click **Edit** in the **SSIDs** and **AP Coverage** dashlets.

Step 10 Click **Create Test** to create the template.
The test template is created and a dialog box appears for confirmation.

Step 11 On the **Done! Sensor Test Created** confirmation window, click **Deploy Test to Locations** to configure the locations and schedule for the test template.

Important
If you return to the **Test Templates** window without deploying the test, click **Deploy Test** from the **Location** column to continue to the next step of deploying the test.

Step 12 On the **Select Location** window, from the left tree hierarchy, check the check boxes of the sites where you want to deploy the test template.

Step 13 On the **Set Schedule** window, select one of the test frequency options:

- **Periodic**: Runs the test at specified intervals. Use the **Interval** drop-down list to select the time between intervals.
- **Scheduled**: Runs the tests on designated days of the weeks for a specified duration:
  a. Click the **S**, **M**, **T**, **W**, **T**, **F**, and **S** buttons to select the days of the week to run the test.
  b. For the selected days, specify the start and end time for the test period from the **From** time pickers.
  c. From the **Select Value** drop-down menu, select the desired test duration for the test period.
  d. To add another test period for the selected day, click **+ Add** to add a new row for configuring the test period.
  e. To remove a test period, click the trash can icon.
- **Continuous**: The test runs indefinitely and repeats after completion.

Step 14 On the **Summary** window, review the deployment details.

To update the details, click **Edit** in the **Location** and **Schedule** dashlets.

Step 15 Click **Deploy Test**.

If you plan to run IP SLA performance tests, the **Warning** dialog box appears. Click **Deploy** to confirm that you want to enable IP SLA on the wireless controllers in the selected sites, so the sensors can run IP SLA tests against the APs.

The test template displays in the **Test Templates** table on the **Test Templates** window.

Step 16 Click the test template's corresponding **Run Now** to run the test.

Manage sensor-driven test templates

Use this procedure to manage sensor-driven test templates. You can duplicate and delete sensor-driven test templates, as well as undeploy running sensor-driven test templates.

Before you begin

Create sensor-driven test templates. See Create and run sensor-driven tests using templates, on page 322.

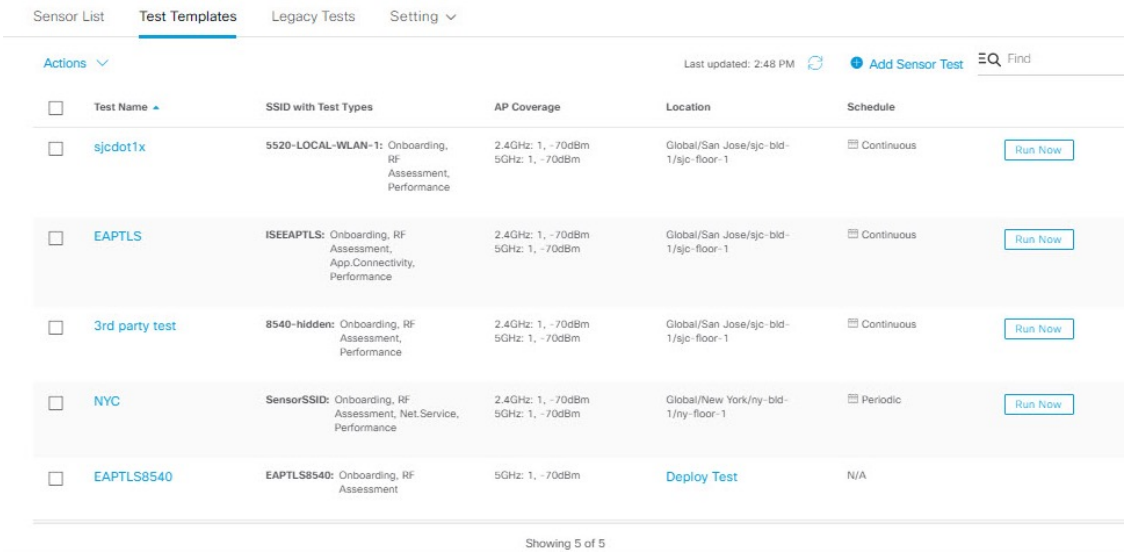
Procedure

Step 1 From the main menu, choose **Assurance** > **Sensors**.

Step 2 Click the **Test Templates** tab.

The **Test Templates** window appears.

Figure 50: Test Templates window



Step 3 To duplicate a test template:

a) Check the check box for the test template that you want to duplicate.
b) From the **Actions** drop-down list, select **Duplicate**.
c) In the **Input the new Test Name** dialog box, enter a name for the duplicate test template.
d) Click **Save**.
The duplicate of the test template displays in the **Test Templates** window. To deploy the test, click the test template's corresponding **Deploy Test** from the **Location** column.

Step 4 To delete a test template:

a) Check the check box for the test template that you want to delete.
b) From the **Actions** drop-down list, select **Delete**.
c) In the **Warning** dialog box, click **Yes**.
The test template is deleted.

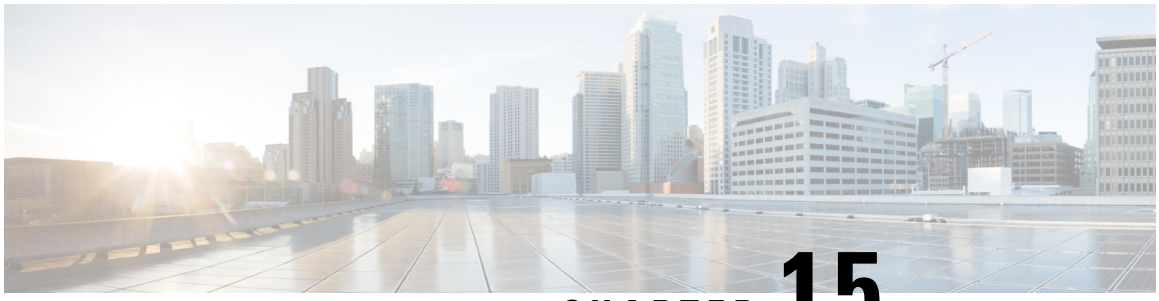
Step 5 To undeploy a test template:

a) Check the check box for the running test template that you want to undeploy.
b) From the **Actions** drop-down list, select **Undeploy**.
c) In the **Warning** dialog box, click **Undeploy**.

Note
If the test template is configured to run IP SLA performance tests, clicking **Undeploy** confirms that you want to disable IP SLA on the wireless controllers in the selected sites, so the sensors don't run IP SLA tests against the APs.

The test template stops running.

Warning
If you undeploy a test template, its location and schedule settings are removed.



CHAPTER 15

Monitor Wi-Fi Readiness

- Wi-Fi Readiness assessments, on page 329
- Assure the Wi-Fi readiness of your network, on page 329

Wi-Fi Readiness assessments

A Wi-Fi Readiness assessment feature determines:

- The percentage of clients that are Wi-Fi 6E, 6 and 7 capable.
- The percentage of AP infrastructure that is Wi-Fi 6E, 6 and 7 ready.
- Based on the preceding information, recommendations are provided about the actions that you can take to experience the full benefits of the Wi-Fi 6E, 6 and 7 network.

To provide these recommendations, Catalyst Center, the assessment:

- Assesses the Wi-Fi capabilities of wireless clients.
- Collects AP inventory to determine which of the APs are managed by Catalyst Center, and then assesses the Wi-Fi capabilities of those APs.
- Determines the types of wireless controllers that are in the network and whether the software that is installed on the wireless controllers is Wi-Fi 6E, 6 and 7 ready.
- Determines the wireless LAN configuration and whether are not Wi-Fi 6E, 6 and 7 features are enabled.

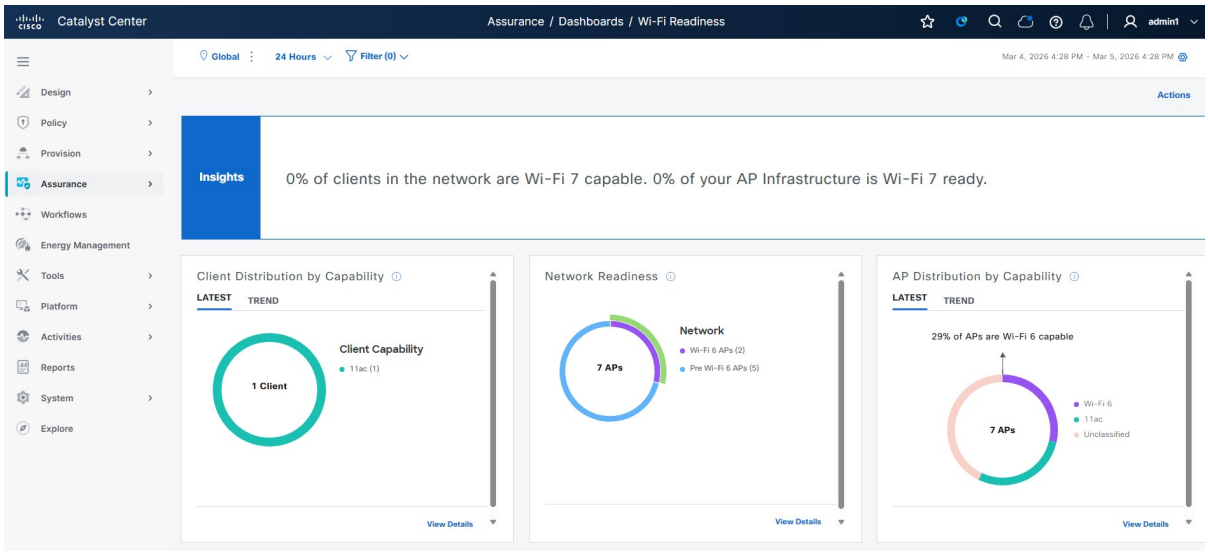
Assure the Wi-Fi readiness of your network

Use this procedure to assure the readiness of your Wi-Fi 7, Wi-Fi 6E, and Wi-Fi 6 network.

Procedure

Step 1 From the main menu, choose **Assurance** > **Wi-Fi Readiness**.

The **Wi-Fi Readiness** dashboard appears.



Step 2 Click the location option (Global) in the top menu bar to select the site, building, or floor from the Site hierarchy.

Step 3 Click ⋮ next to the location icon and to switch between:

- **Site Map**: Provides a geographical view of your network hierarchy.
- **Site Table**: Provides a list-based view of all sites, including their health scores and device counts.

The location pane has this functionality:

Item	Description
toggle button **List View**	Click this toggle button to display the sites and buildings from your network in a table format. Click the drop-down list for these options: • **Hierarchical Site View**: Sorts the list at a site level. From the **Go to sites** column, click for a site or building to display data only for that location on the **Network** dashboard. • **Building/Outdoor Area view** : Sorts the list at a building level. From the **Go to sites** column, click for a site or building to display data only for that location on the **Network** dashboard.
Export	Click **Export** to export the device information to a CSV file.
toggle button **Map View**	Click this toggle button to display the health of all the network sites on a geographic location-oriented network health map. By default, the network sites are color coded according to the severity of the problem.

Item	Description
	Click this close icon to hide the map or table view.
 **Time Range** setting	Enables you to display data within a specified time range on the dashboard. Do these steps: **a.** From the drop-down menu, select the length of the range: **3 Hours**, **24 Hours**, or **7 Days**. **b.** Specify the **Start Date** and time; and the **End Date** and time. **c.** Click **Apply**.
Filter icon	Contains the **SSID** and **Band** options. Select the SSIDs and band frequency from the drop-down list by selecting the check boxes adjacent to them, and then click **Apply**. Depending on your selection, the information in the dashboard is refreshed.
Actions drop-down list	Enables you to export the dashboard to PDF format. Click **Export Dashboard** to view the preview page and click **Save**. Enables you to customize the dashboard display when you select **Edit Dashboards** from the drop-down list. See Change the position of a dashlet, on page 349 and Create a custom dashboard, on page 347.

Step 4 Use the **Insights** area to get an insight about your network. It provides this information:

- The percentage of clients that are Wi-Fi 7, Wi-Fi 6E, and Wi-Fi 6 capable.
- The percentage of AP infrastructure that is Wi-Fi 7, Wi-Fi 6E, and Wi-Fi 6 ready.
- Based on the above information, recommendations on what actions you can take to enjoy the full benefits of the Wi-Fi 7, Wi-Fi 6E, and Wi-Fi 6 network are provided.

Step 5 Use the **Client Distribution By Capability** dashlet to compare the distribution capability of clients between Wi-Fi 7, Wi-Fi 6E, and Wi-Fi 6 and to determine if the Wi-Fi 7, Wi-Fi 6E, and Wi-Fi 6 capable clients joined to the network.

Based on the AP to which the clients are associated, the clients might function at their Wi-Fi 7 capability or at a lesser capability. For example, a Wi-Fi 6 client associated to a 11ac AP will function as an 11ac client.

Client distribution by capability dashlet

You can view all the available wireless capabilities of the clients in the network such as Wi-Fi 7, Wi-Fi 6E, and Wi-Fi 6.

This dashlet includes these tabs:

- **Latest**: Displayed by default.
  - The circle shows the actual wireless capability of the clients joined to the network. The wireless clients are capable of functioning in one of these protocols:
    - **Wi-Fi 7**: 802.11be capable client(s).
    - **Wi-Fi 6E**: 802.11ax 6 GHz capable client(s).
    - **Wi-Fi 6**: 802.11ax capable client(s).
    - **11ac**: 802.11ac Wave1 and Wave2 capable client(s).
    - **11n**: 802.11n capable client(s).
    - **11abg**: 802.11a, b, or g capable client(s).
    - **Unclassified**: The client is listed under **Unclassified** due to these reasons:
      - The capabilities of the client device is not reported due to network delay.
      - The AP or wireless controller to which the client device is connected, does not have the correct software version installed.

  Hover your cursor over a color in the chart to display the number of clients associated with that color.
- **Trend**: Click the **Trend** tab to display a trend chart. This color-coded trend chart shows the number of the clients that are associated to Wi-Fi 7, Wi-Fi 6E, and Wi-Fi 6, or unclassified protocols over a time range.

  Hover your cursor over the chart to display the total number of clients and their protocol for that specific day and time.

Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to refresh the data in the table that is displayed below the chart.

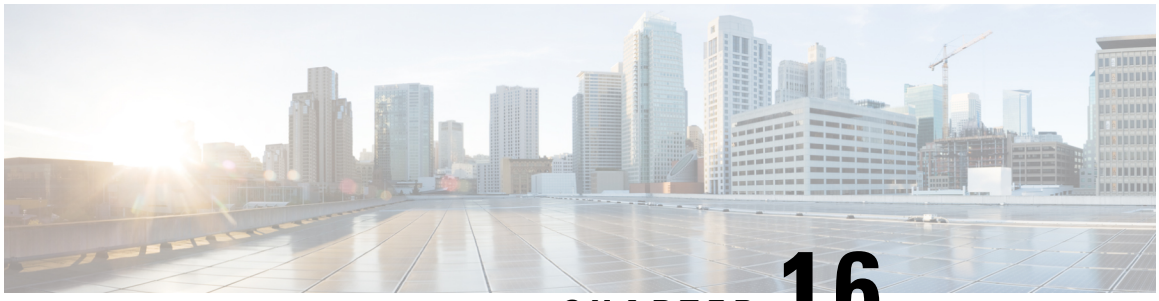
Step 6 Use the **Network Readiness** dashlet to determine how many APs are Wi-Fi 7, Wi-Fi 6E, and Wi-Fi 6 capable and are configured (enabled) to operate.

Network Readiness dashlet
You can view all the available wireless capabilities of the clients associated with the wireless network such as Wi-Fi 7, Wi-Fi 6E, and Wi-Fi 6. • The **outer** segment of the circle shows the number of Wi-Fi 6E APs with the 6-GHz band enabled or Wi-Fi 6 APs with 11ax disabled. **Note** Wi-Fi 6E APs can operate in Wi-Fi 6E mode only if the wireless controllers and APs are running a software version that supports 6 GHz band. • The **inner** circle shows the number of APs that are Wi-Fi 6E, Wi-Fi 6, and non-Wi-Fi 6 (11ac/n/a/b/g) capable. **Note** Wi-Fi 6 APs can operate in Wi-Fi 6 mode under these conditions: • The 11ax configuration on the Wi-Fi 6 APs is enabled. • The wireless controllers and APs are running a software version that supports Wi-Fi 6 (11ax). Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, click a color segment in the chart; **AP** and **WLC** tabs display. Click the **AP** and **WLC** tabs to display Wi-Fi 6 readiness at radio and band levels, respectively.

Step 7 Use the **AP Distribution by Protocol** dashlet to determine the number of APs that have the hardware capability to support the Wi-Fi standards: Wi-Fi 7, Wi-Fi 6E, and Wi-Fi 6

AP distribution by protocol dashlet

This dashlet includes these tabs:
• **Latest**: Displayed by default. It shows the number of APs that support Wi-Fi 7, Wi-Fi 6E, and Wi-Fi 6
  • **Wi-Fi 7**: 802.11be capable client(s).
  • **Wi-Fi 6E**: 802.11ax 6 GHz band capable AP(s).
  • **Wi-Fi 6**: 802.11ax capable AP(s).
  • **11ac**: 802.11ac capable AP(s).
  • **11n**: 802.11n capable AP(s).
  • **11abg**: 802.11a/b/g capable AP(s).
  Hover your cursor over a color in the chart to display the number of APs associated with that color.
• **Trend**: Click the **Trend** tab to display a trend chart. This color-coded trend chart shows the number of the APs that are associated to the different protocols Wi-Fi 7, Wi-Fi 6E, and Wi-Fi 6) over a time range.
  Hover your cursor over the chart to display the total number of APs and their protocol for that specific day and time.
Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to refresh the data in the table that is displayed below the chart.



CHAPTER 16

Monitor Power over Ethernet

- About Power over Ethernet, on page 335
- Setup workflow for PoE telemetry, on page 335
- Configure NETCONF on your devices for PoE telemetry, on page 337
- Update telemetry settings for PoE telemetry, on page 339
- Monitor PoE-capable devices in your network, on page 340

About Power over Ethernet

The Catalyst Center Power over Ethernet (PoE) enables you to monitor the PoE-capable devices in your network. It also monitors the power summary of switches supplying PoE, which provides information such as a switch's power budget, used power, remaining power, and power usage. PoE also lets you view the allocated power and power load of switches.

Setup workflow for PoE telemetry

To enable PoE telemetry and analytics in Assurance, you need to do the required setup tasks. A basic workflow for setup involves these tasks:

1. Configure NETCONF on the network devices used for PoE telemetry.

   For details, see Configure NETCONF on your devices for PoE telemetry, on page 337.

2. Update the telemetry settings in Catalyst Center.

   For details, see Update telemetry settings for PoE telemetry, on page 339.

Setup workflows

The setup workflow for PoE telemetry varies depending on the software version and configuration of Catalyst Center and network devices that support PoE telemetry.

If you are doing a fresh installation of Catalyst Center, refer to this table:

Fresh installation of Catalyst Center	
Network device configuration	**Required setup tasks**
• IOS XE version is 16.12.3s. • NETCONF is disabled.	**1.** Enable NETCONF on the device. **2.** Update the telemetry settings in Catalyst Center.
• IOS XE version is upgraded from 16.12.2 to 16.12.3s with SWIM. • NETCONF is disabled.	**1.** Enable NETCONF on the device. **2.** Update the telemetry settings in Catalyst Center.
• IOS XE version is upgraded from 16.12.2 to 16.12.3s with SWIM. • NETCONF is enabled.	**1.** Update the telemetry settings in Catalyst Center.

If you are upgrading to Catalyst Center from an earlier release, refer to this table:

Upgrade from an earlier release	
Network device configuration	**Required setup tasks**
• IOS XE version is upgraded from 16.12.2 to 16.12.3s with SWIM. • NETCONF disabled.	**1.** Enable NETCONF on the device. **2.** Update the telemetry settings in Catalyst Center.
• IOS XE version is upgraded from 16.12.2 to 16.12.3s with SWIM. • NETCONF is enabled.	**1.** Update the telemetry settings in Catalyst Center.
• IOS XE version is 16.12.3s. • NETCONF is disabled.	**1.** Enable NETCONF on the device. **2.** Update the telemetry settings in Catalyst Center.
• IOS XE version is 16.12.3s. • NETCONF is enabled.	**1.** Update the telemetry settings in Catalyst Center.

If there are changes to the network device that supports PoE telemetry in **Inventory**, refer to this table:

Network device changes in inventory	
Change to network device	**Required setup tasks**
Remove a device from Catalyst Center **Inventory**, and then add it back.	**1.** Enable NETCONF on the device. **2.** Update the telemetry settings in Catalyst Center.
Add a new device to Catalyst Center **Inventory**.	**1.** Enable NETCONF on the device. **2.** Update the telemetry settings in Catalyst Center.

Network device changes in inventory	
Change to network device	**Required setup tasks**
Use a replacement device in Catalyst Center **Inventory**.	**1.** Enable NETCONF on the device. **2.** Update the telemetry settings in Catalyst Center.

Configure NETCONF on your devices for PoE telemetry

Use this procedure to configure NETCONF on your network devices for PoE telemetry. To use PoE telemetry, the supporting network devices must have NETCONF enabled.

Before you begin

Depending on the configuration of your Catalyst Center and network devices, you might not need to do this procedure to set up PoE telemetry. For details, see Setup workflow for PoE telemetry, on page 335.

Procedure

Step 1 Configure the NETCONF port for an existing network device:

a) From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window appears.

b) Check the check box of the network device to be configured to enable NETCONF.

c) From the **Actions** drop-down list, choose **Inventory** > **Edit Device**.

d) From the **Type** drop-down list, choose **Network Device**.

e) Expand the **NETCONF** area.

f) In the **Port** field, enter `830`.

Note
NETCONF provides a mechanism to install, manipulate, and delete configurations of network devices.

g) Click **Update**.

The device's NETCONF port is configured.

Step 2 Create a **Template Editor** project for NETCONF configuration:

a) From the main menu, choose **Tools** > **Template Editor**.

The **Template Editor** window appears.

b) From the left pane, click the icon and choose **Create Project**.

c) In the **Name** field, enter a name for the project.

d) Click **Add**.

The project is added to the left pane of **Template Editor**.

Step 3 Create a template in the project for NETCONF configuration:

a) From the left pane, hover your cursor over the ⚙ icon to the right of the project and choose **Add Template**.
b) In the **Name** field, enter a name for the template.
c) In the **Device Type(s)** field, click **Edit**.
d) Check the check box of **Switches and Hubs** to apply the template to add switches and hubs.

Note
If you want to specify the exact models of the switches, expand **Switches and Hubs** and check the check box of the specific switch model.

e) Click **Back to Add New Template**.
f) Click the **Software Type** drop-down list and choose **IOS-XE**.
g) Click **Add**.

The template is created and appears.

Step 4 Add content in the template:

a) In the template, enter this:

```
netconf-yang
```

b) From the **Actions** drop-down list, select **Save**.

The content is saved to the template.

c) From the **Actions** drop-down list, select **Commit**.
d) In the **Commit Note** text box, enter a note.
e) Click **Commit**.

Step 5 Create a network profile and associate the template:

a) From the main menu, choose **Design** > **Network Profile**.

The **Network Profiles** window appears.

b) Click **+Add Profile** and select **Switching**.
c) In the **Profile Name** field, enter a name for the network profile.
d) Click the **Day-N Templates** tab.
e) Click **+Add**.
f) From the **Device Type** drop-down list, select **Switches and Hubs**.
g) From the **Template** drop-down list, select the template that was created in Step 3.
h) Click **Save**.

The network profile is created and appears in the **Network Profiles** window.

Step 6 Assign the site(s) for the network profile:

a) From the **Sites** column, click **Assign Site**.
b) Check the check box of the site that the network device is assigned to.
c) Click **Save**.

Step 7 Provision the NETCONF configuration to the network device:

a) From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window appears.

b) Check the check box of the network device for PoE telemetry.
c) From the **Actions** drop-down list, choose **Provision** > **Provision Device**.
d) In the **Assign Site** step, click **Next**.
e) In the **Advanced Configuration** step, check the **Provision these templates even if they have been deploy before** check box.
f) Click **Next**.
g) In the **Summary** step, click **Deploy**.
h) Click **Apply**.

Provisioning starts and the NETCONF configuration is pushed to the network device.

Update telemetry settings for PoE telemetry

Use this procedure to update the telemetry settings in Catalyst Center. This is a required step after setting the NETCONF port and pushing the NETCONF configuration to the network devices for PoE telemetry.

Before you begin

Ensure that the network devices being set up for PoE telemetry have an established NETCONF port and the correct NETCONF configuration. For details, see Configure NETCONF on your devices for PoE telemetry, on page 337.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window appears.

Step 2 Check the check boxes of the network devices that have been set up for PoE telemetry.

Step 3 From the **Actions** drop-down list, choose **Telemetry** > **Update Telemetry Settings**.

Step 4 Check the **Force Configuration Push** check box.

Note
This option pushes the configuration changes to the device.

Step 5 Click **Next**.

Step 6 Set the schedule for when the telemetry settings are updated by clicking a radio button:

- **Now**: Select this option to update the telemetry settings immediately.
- **Later**: Select this option to schedule the task for another time. Specific the time and date.

Step 7 Click **Apply**.

Monitor PoE-capable devices in your network

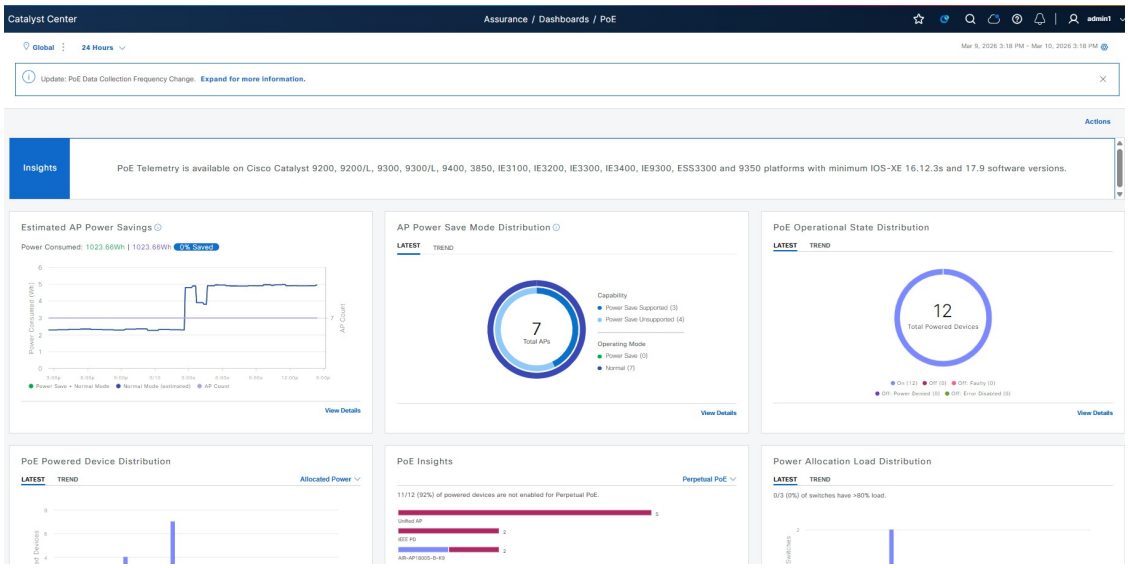
Use this procedure to get a global view of PoE-capable devices in your network.

Procedure

Step 1 From the main menu, choose **Assurance** > **PoE**.

The **PoE** dashboard appears.

Figure 51: PoE dashboard



Step 2 Click the location option (Global) in the top menu bar to select the site, building, or floor from the Site hierarchy.

Step 3 Click next to the location icon and to switch between:

- **Site Map**: Provides a geographical view of your network hierarchy.
- **Site Table**: Provides a list-based view of all sites, including their health scores and device counts.

The location pane has this functionality:

Location option	
Item	**Description**
 toggle button **List View**	Click this toggle button to display the sites and buildings from your network in a list format. Click the drop-down list for these options: • **Hierarchical Site View**: Sorts the list at a site level. From the **Go to sites** column, click  for a site or building to display data only for that location on the **Network** dashboard. • **Building/Outdoor Area view** : Sorts the list at a building level. From the **Go to sites** column, click  for a site or building to display data only for that location on the **Network** dashboard.
	Click **Export** to export the device information to a CSV file.
 toggle button **Map View**	Click this toggle button to display the health of all the network sites on a geographic location-oriented network health map. By default, the network sites are color coded according to the severity of the problem.
	Click this close icon to hide the map or table view.

Step 4 Click the time range setting () in the top menu bar to specify the time range of data that appears on the dashboard.

a) From the drop-down menu, select the time range: **3 Hours**, **24 Hours**, or **7 Days**.
b) Specify the **Start Date** and time, and the **End Date** and time.
c) Click **Apply**.

Step 5 Click the **Actions** drop-down list in the top-menu bar for this functionality:

- **Export Dashboard**: Enables you to export the PoE dashboard to PDF format. Click **Export Dashboard** to view the preview page and click **Save**.
- **Edit Dashboard**: Enables you to customize the dashboard display. See Change the position of a dashlet, on page 349 and Create a custom dashboard, on page 347.

Step 6 Use the PoE dashlets for this functionality:

AP Power Save Mode Distribution

AP Power Save Mode Distribution displays AP power save capability as well as the average number of APs in Power Save vs Normal mode.

The **Latest** tab shows the number of APs that support the Power Save Capability and the Power Save mode versus Normal mode.

The **Trend** tab provides this information:

- If you chose 24 hours in the time range settings, the trend chart provides 10-minute data points for the entire 24-hour range.
- If you chose greater than 24 hours in the time range settings, the trend chart provides 1-hour data points (aggregated from the 10-minute data) for the entire time range.

Note
The data point that is displayed is the start time of the corresponding 10-minute or 1-hour window. For example, all the data that is received between 10:00 to 10:10 is displayed with the time value of 10:00. Similarly, for the hourly window, the data that is received between 10:00 to 11:00 is displayed with a time stamp of 10:00. This data point is available at the end of the corresponding time window.

Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, hover your cursor over the color-coded chart to view the total number of APs distributed in power save capability over Power save mode and Normal mode at a specific time. You can filter the data in the table that is displayed below the chart based on the number of the APs in the top sites and top device types.

AP Power Savings

AP Power Savings mode will either shut down AP's radio or reduce their radio spatial stream to decrease power consumption, and displays overall power consumed and saved during the time range.

- If you chose 24 hours in the time range settings, the trend chart provides 10-minute data points for the entire 24-hour range.
- If you chose greater than 24 hours in the time range settings, the trend chart provides 1-hour data points (aggregated from the 10-minute data) for the entire time range.

Note
The data point displayed is the start time of the corresponding 10-minute or 1-hour window. For example, all the data that is received between 10:00 to 10:10 is displayed with the time value of 10:00. Similarly, for the hourly window, the data that is received between 10:00 to 11:00 is displayed with a time stamp of 10:00. This data point is available at the end of the corresponding time window.

Click **View Details** to open a **AP Power Savings** slide-in pane with additional details. On the slide-in pane, the color-coded chart shows the power consumed by APs over a time range. Hover your cursor over the chart to view the total number of APs, power saved in power save mode, and normal mode over a period of time.

PoE AP power mode distribution
Displays the distribution of fully powered and partially powered APs. The **Latest** tab provides a 10-minute snapshot view. The **Trend** tab provides this information: • If you chose 24 hours in the time range settings, the trend chart provides 10-minute data points for the entire 24-hour range. • If you chose greater than 24 hours in the time range settings, the trend chart provides 1-hour data points (aggregated from the 10-minute data) for the entire time range. **Note** The data point displayed is the start time of the corresponding 10-minute or 1-hour window. For example, all the data that is received between 10:00 to 10:10 is displayed with the time value of 10:00. Similarly, for the hourly window, the data that is received between 10:00 to 11:00 is displayed with a time stamp of 10:00. This data point is available after the end of the corresponding window. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart or its corresponding legend to refresh the data in the table that is displayed below the chart.

PoE operational state distribution
Displays the number of PoE-capable devices in your network. The color-coded chart provides the count of devices based on whether they are being supplied with PoE or not. For devices that are not being supplied with PoE, this is further characterized by the reason why. The **Latest** tab provides a 10-minute snapshot view. The **Trend** tab provides this information: • If you chose 24 hours in the time range settings, the trend chart provides 10-minute data points for the entire 24-hour range. • If you chose greater than 24 hours in the time range settings, the trend chart provides 1-hour data points (aggregated from the 10-minute data) for the entire time range. **Note** The data point displayed is the start time of the corresponding 10-minute or 1-hour window. For example, all the data that is received between 10:00 to 10:10 is displayed with the time value of 10:00. Similarly, for the hourly window, the data that is received between 10:00 to 11:00 is displayed with a time stamp of 10:00. This data point is available after the end of the corresponding window. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart or its corresponding legend to refresh the data in the table that is displayed below the chart.

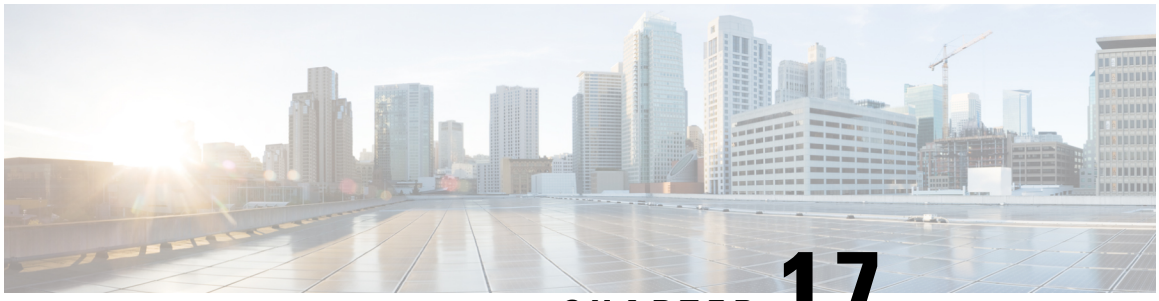
PoE powered device distribution
View the distribution of the devices currently using PoE for a certain criteria. Use the drop-drop list to specify this criteria: • **Allocated Power** • **Powered Device Class** The **Latest** tab provides a 10-minute snapshot view. The **Trend** tab provides this information: • If you chose 24 hours in the time range settings, the trend chart provides 10-minute data points for the entire 24-hour range. • If you chose greater than 24 hours in the time range settings, the trend chart provides 1-hour data points (aggregated from the 10-minute data) for the entire time range. **Note** The data point displayed is the start time of the corresponding 10-minute or 1-hour window. For example, all the data that is received between 10:00 to 10:10 is displayed with the time value of 10:00. Similarly, for the hourly window, the data that is received between 10:00 to 11:00 is displayed with a time stamp of 10:00. This data point is available after the end of the corresponding window. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart or its corresponding legend to refresh the data in the table that is displayed below the chart.

Power allocation load distribution
View the distribution of switches based on its power load for PoE. The **Latest** tab provides a 10-minute snapshot view. The **Trend** tab provides this information: • If you chose 24 hours in the time range settings, the trend chart provides 10-minute data points for the entire 24-hour range. • If you chose greater than 24 hours in the time range settings, the trend chart provides 1-hour data points (aggregated from the 10-minute data) for the entire time range. **Note** The data point displayed is the start time of the corresponding 10-minute or 1-hour window. For example, all the data that is received between 10:00 to 10:10 is displayed with the time value of 10:00. Similarly, for the hourly window, the data that is received between 10:00 to 11:00 is displayed with a time stamp of 10:00. This data point is available after the end of the corresponding window. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart or its corresponding legend to refresh the data in the table that is displayed below the chart.

PoE insights
View the percentage of the devices currently using PoE which are configured to support these PoE technologies or meet IEEE Compliance: • **Perpetual PoE** • **Fast PoE** • **IEEE Compliant** • **UPOE+** Use the drop-down list to select the characteristic. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart or its corresponding legend to refresh the data that is displayed in the table below the chart.

Power usage
View the total power consumption and allocated power by devices currently using PoE. Use the drop-down list to select **Consumption** or **Allocation** view to display the respective data in the Latest and Trend tab. The **Latest** tab provides a 10-minute snapshot view. The pie chart displays the Power Allocation details such as PoE Power Allocation, System Power Allocation, and Available Power, and Power Consumption details such as PoE Power Consumption and System Power Consumption measured in watts. The **Trend** tab provides this information: • If you chose 24 hours in the time range settings, the trend chart provides 10-minute data points for the entire 24-hour range of power usage. • If you chose greater than 24 hours in the time range settings, the trend chart provides 1-hour data points (aggregated from the 10-minute data) for the entire time range. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click on a color segment in the chart or its corresponding legend to view the System Power information (System Power Consumption and System Power Allocation) and PoE Power information (PoE Power Consumption and PoE Power Allocation) of the devices over a time period in the table that is displayed below the chart. You can select the data displayed as horizontal bars to filter the preceding table that is displayed based on the power usage, device role and location.

PoE port availability
View the availability of ports based on their power load for PoE. The **Latest** tab provides a 10-minute snapshot view. The **Trend** tab provides this information: • If you chose 24 hours or less in the time range settings, the trend chart provides 1-hour data points (aggregated from the 10-minute data) for the entire time range. • If you chose 7 days in the time range settings, the trend chart provides 12-hour data points (aggregated from the 1-hour data) for the entire time range. Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a 1-hour data point in the chart to refresh the data in the table that is displayed below the chart.



CHAPTER 17

Manage Dashboards

- About dashboards, on page 347
- Create a custom dashboard, on page 347
- View a dashboard, on page 348
- Edit or delete a dashboard, on page 348
- Duplicate a dashboard, on page 349
- Mark a dashboard as a favorite, on page 349
- Change the position of a dashlet, on page 349
- Configure filter group settings, on page 350

About dashboards

You can create custom dashboards for monitoring your network. Dashboards contain one or more dashlets, which include charts, tables, geographic maps, and other types of information.

Any custom dashboard that you create is visible only to your user account. Other users cannot see your custom dashboards.

Create a custom dashboard

Procedure

Step 1 From the main menu, choose **Assurance** > **Dashboard Library**.
The **Dashboard Library** window appears, listing all the defined dashboards.

Step 2 Click **+ Create a Dashboard**.

Step 3 In the **Create a Dashboard** dialog box, enter a title for the dashboard.

Step 4 Click **Save**.
A blank dashboard appears.

Step 5 You can do these steps in your dashboard:

a) Click **+ Add Dashlet** to add content to the dashboard.

b) Check the check box next to the dashlet that you want to add to your dashboard.

Note
You can search for a dashlet by choosing a category from the drop-down list or by using the search box on the right.

c) Click **Add** to include the dashlet in your dashboard.

Step 6 (Optional) Drag and drop any dashlet to customize its location on your dashboard.

Step 7 You can remove a dashlet from your dashboard by doing these steps:

a) Click the trash can icon located in the top-right corner of the dashlet.

b) In the dialog box, click **Delete**.

Step 8 Click **Save** to save the dashboard.

View a dashboard

Procedure

Step 1 From the main menu, choose **Assurance** > **Dashboard Library**.
The **Dashboard Library** window appears, listing all the defined dashboards. You can use the **Sort By** control to sort dashboards by date or name. You can search for a dashboard by entering its name in the **Find** field.

Note
When you sort the dashboards by **Date Modified**, even if no modifications were made on the dashboards, the dashboards get sorted by the last time the dashboards were open.

Step 2 To see dashboards marked as favorites, click the **Favorite Dashboards** tab.

Step 3 Click the dashboard that you want to view.

Step 4 In the dashboard controls, click **Show** or **Hide** to show or hide the map, if applicable.

Step 5 (Optional) Filter dashboard data by time period, sites, or domains by choosing the appropriate values from the filters.

Edit or delete a dashboard

Procedure

Step 1 From the main menu, choose **Assurance** > **Dashboard Library**.
The **Dashboard Library** window appears, listing all the defined dashboards. You can use the **Sort By** control to sort dashboards by date or name. You can search for a dashboard by entering its name in the **Find** field.

Step 2 Click the dashboard that you want to edit or delete.

Step 3 Do one of these tasks:

- To make changes, select **Edit Dashboard** from the **Actions** menu. You can add or delete dashlets and drag dashlets to different positions in the dashboard. Click **Save** when you are done.

- To delete the dashboard, select **Delete Dashboard** from the **Actions** menu. Click **Delete** in the confirmation dialog.

Duplicate a dashboard

Procedure

Step 1 From the main menu, choose **Assurance** > **Dashboard Library**.
The **Dashboard Library** window appears, listing all the defined dashboards. You can use the **Sort By** control to sort dashboards by date or name. You can search for a dashboard by entering its name in the **Find** field.

Step 2 Click the duplicate icon for a dashboard (next to the star icon).

Step 3 In the **Duplicate Dashboard** dialog box, enter a title for the dashboard copy.

Step 4 Click **Save**.

Step 5 You can change this copied dashboard by adding, deleting, or rearranging dashlets.

Step 6 Click **Save** to save the dashboard.
A confirmation dialog appears.

Step 7 Click **OK**.

Mark a dashboard as a favorite

Procedure

Step 1 From the main menu, choose **Assurance** > **Dashboard Library**.

The **Dashboard Library** window appears, listing all the defined dashboards. You can use the **Sort By** control to sort dashboards by date or name. You can search for a dashboard by entering its name in the **Find** field.

Step 2 Click by the dashlet name to mark it as a favorite.

Note
You can access favorite dashboards by clicking the **Favorite Dashboards** tab.

Change the position of a dashlet

You can change the position of the dashlets in the default Assurance dashboards.

Procedure

Step 1 Do one of these tasks:

- From the main menu, choose **Assurance** > **Health**.

  The **Overall Health** dashboard appears.

- From the main menu, choose **Assurance** > **Health** > **Network Health**.

  The **Network Health** dashboard appears.

- From the main menu, choose **Assurance** > **Health** > **Client Health**.

  The **Client Health** dashboard appears.

- From the main menu, choose **Assurance** > **Health** > **Application Health**.

  The **Application Health** dashboard appears.

Step 2 Click the **Actions** drop-down list and select **Edit Dashboard**.
The dashboard is refreshed and becomes editable.

Step 3 Click the dashlet that you want to move and drag it to a different position in the dashboard.

Step 4 Click **Save**.

Configure filter group settings

Use this procedure to define the scope and configure the specific filters for the Client and Network template dashboards.

Procedure

Step 1 From the main menu, choose **Assurance** > **Filter Group Settings**.

The **Filter Group Settings** window appears.

Step 2 Click **Add New**.

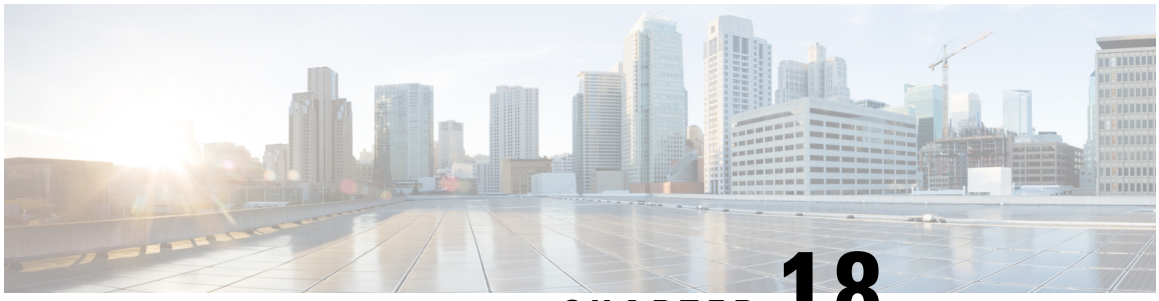
Step 3 In the **Add New** slide-in pane, configure the filter groups settings.

a) In the **Filter Group Name** field, enter the filter group name.
b) From the **Filter Group Type** drop-down list, select the filter group type as **Client** or **Network**.
c) Click **Add a Filter**.
d) From the **Filter** drop-down list, select the filter and corresponding value from the drop-down list next to the filter. Filters listed are based on the selected filter group type.

   Supported filters for Client filter group: Site, Device Type, SSIDs, MAC Address, IP Address, and Host Name.

   Supported filters for Network filter group: Site, Network Device Type, Network OS, Host Name, and IP Address.

e) Click **Confirm**.



CHAPTER 18

Observe Network Trends and Gain Insights

- About network trends and insights, on page 353
- View wireless AP performance advisories, on page 353
- View network trends and obtain insights, on page 357
- Compare APs and switches in network heatmaps, on page 362
- Compare KPI values with peers in your network, on page 366
- Compare buildings, AP model families, and wireless endpoint types, on page 367
- View and monitor network performance using baselines, on page 370
- View the RF network using the AI-enhanced RRM dashboard, on page 373

About network trends and insights

Cisco AI Network Analytics uses machine learning algorithms and AI techniques to provide this information:

- **Trends and Insights**: Determine global patterns (trends) and deviations to provide system-generated insights.
- **AP Performance Advisories**: Detect APs that have a consistently poor client experience, and provide a root cause and suggested actions.
- **Comparative Analytics**, which includes:
  - **AI-Driven AP Comparisons in Network Heatmaps**: Compare all of the APs in your network for a given month in a heatmap to spot trends and gain insights.
  - **AI-Driven Peer Comparisons**: Determine how your network is performing in comparison to your peer networks for a selected Key Performance Indicator (KPI).
  - **AI-Driven Network Comparisons**: View, compare, and identify performance improvement opportunities for objects in your network (buildings, AP model families, wireless endpoints) across selected KPIs.

View wireless AP performance advisories

Cisco AI Network Analytics uses machine learning algorithms to identify wireless APs with a potentially poor client experience. APs are continually analyzed over long periods and those suspected of providing a

suboptimal client experience are grouped by underlying root cause and suggested improvements. Insights are generated, which consist of a set of radio and network features that can be used to diagnose any underlying issue that can be rectified. Insights have these main components:

- Discover underperforming APs via various client experience KPIs.
- Find appropriate features that can discriminate between APs with a poor or good client experience that is both significant and actionable by the customer as a basis of root-cause analysis (RCA).

APs are analyzed on separate frequency bands of 2.4 GHz, 5 GHz and 6GHz. Poor client experience is detected using statistical analysis of different KPIs, such as SNR, RSSI, link speed, packet retries, and packet failures.

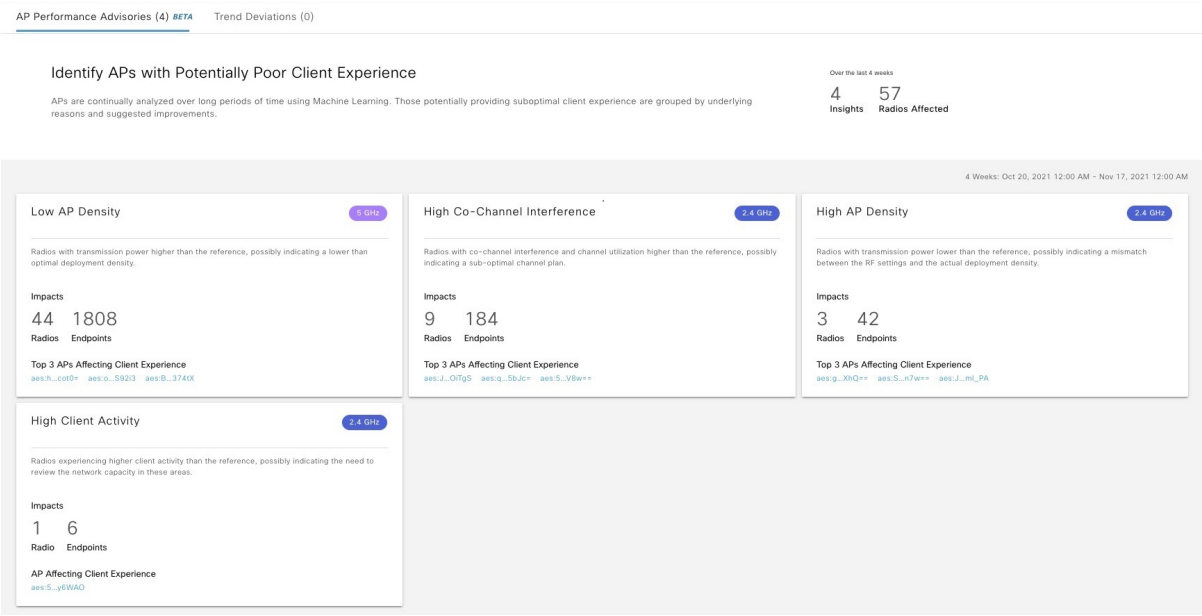
Use this procedure to view AP performance advisories that highlight the most active APs with poor client experience based on analysis of four weeks of data.

Procedure

Step 1 From the main menu, choose **Assurance** > **Trends and Insights** > **AP Performance Advisories**.

Step 2 Click the **AP Performance Advisories** tab, which provides a summary of the number of different types of insights with common root-cause analysis category and affected radios.

Figure 52: AP Performance Advisories



The possible occurrences of insights with common root-cause analysis include:

- External RF load
- External RF load with high client activity
- Frequent channel change
- High RF load

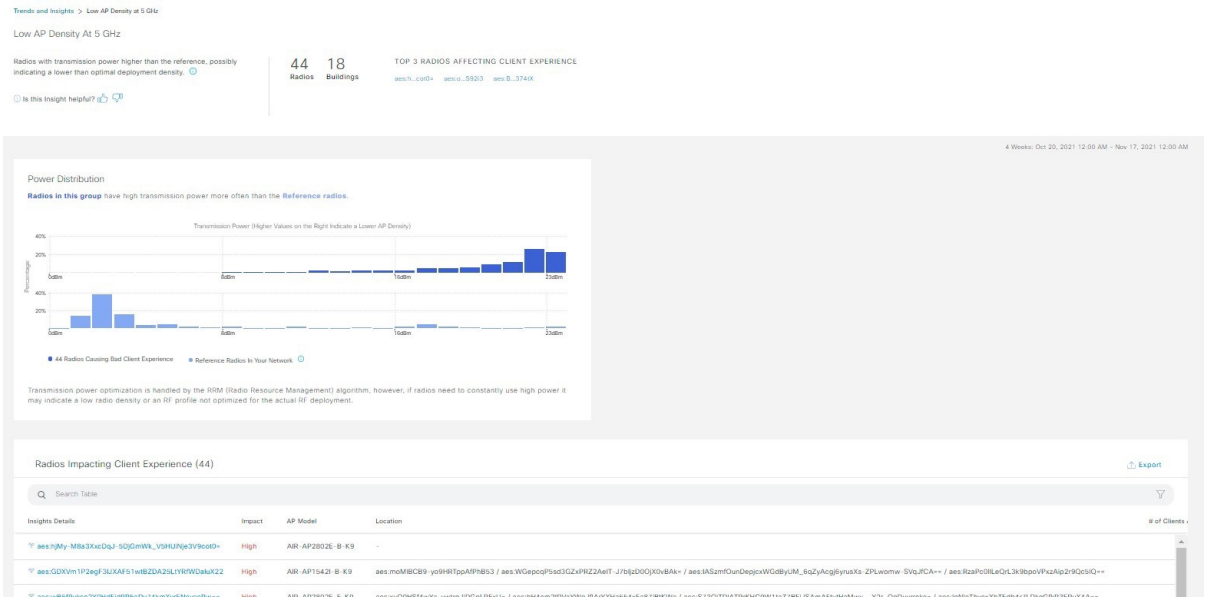
- High channel utilization
- High client activity
- High client load
- High AP deployment density
- Low AP deployment density
- Low AP deployment density and external interference
- Low AP deployment density and high load

Step 3 Use the **AP Performance Advisories** dashboard for this insights summary:

Network overview window	
Item	**Description**
Insights Summary	Displays the name of the insight (Low AP Density, High Client Activity, and so on) and problem definition for a particular frequency band.
Impacts	Displays the number of impacted **Radios** and **Endpoints** for each insight.
Top 3 APs Affecting Client Experience	Displays the top three impacted APs for a particular frequency band. These are hyperlinks to the detailed page, shown in Step 5.

Step 4 Click each insight dashlet for information, where a common root-cause analysis is provided with the suggested actions for all radios in this category.

Figure 53: Insights summary dashboard for impacted radios



Insight dashboard	
Item	**Description**
Summary	Displays the total number of radios analyzed over four weeks, the number of buildings, and the top three impacted APs.
KPI charts	Displays multiple KPI charts depending on the RCA category, which indicates the distribution of the KPI across all the radios. The charts can be used to compare and contrast the performance of radios with this common RCA, against reference radios that have no detected client experience problem.
Radios Impacting Client Experience table	Contains Insights Details, Impact (low, medium, or severe), AP Model, Location, # of Clients Affected, and KPIs Impacting Client Experience.
Export	Click **Export** to export the table data to a CSV file.

Step 5 In the **Radios Impacting Client Experience** table, click the hyperlinked AP to view these detailed insights summary for a specific AP.

Figure 54: Insight summary for AP



Insight dashboard	
Item	**Description**
Top bar	Provides information such as AP model, location, impacted clients, and additional AP details hyperlinked to the Assurance Device window. Also provides suggested actions that are specific to the identified root cause and anomalous KPIs to improve the client experience.

Insight dashboard	
Item	**Description**
Client Experience KPIs	• The histogram shows the distribution of the different KPIs that impact client experience, facilitating a comparison between the individual AP and the reference AP across the customer's network (APs without observed client experience problems). • By default, only KPIs with detected anomalies are shown. You can add more numbers of KPIs that display the distribution of KPIs, including the SNR, RSSI, link speed, packet retries, and packet failures. • You can hover your cursor over the histogram bin value to view additional details of the observed occurrence rate in the selected AP, versus the reference set of APs.
Radio Specific Root-Cause Context	• The histogram shows the distribution of the different root-cause analysis KPIs that impact radios. By default, only KPIs with detected anomalies are shown. • You can add more numbers of KPIs that display the distribution of RCA KPIs, including the SNR, RSSI, link speed, packet retries, and packet failures. • You can hover your cursor over the histogram bin value to view additional details of the observed occurrence rate in the selected radio, versus the reference set of radios.

View network trends and obtain insights

Trends are long-term evolutions of behavior in your network observed over a time period. These trends provide insights about the performance of your network (represented in beeswarm charts). These types of insights are provided:

- **Intra-Site**: Cisco AI Network Analytics looks into a single site or building and highlights the outlier device only within that building. In this case, the entity in the beeswarm chart is a radio and it is represented by a circle.
- **Inter-Site**: Cisco AI Network Analytics looks at the global network and identifies an outlier building with respect to the selected KPI. In this case, the entity in the beeswarm chart is a building and it is represented by a polygon.

Use this procedure to view trends in your network.

Procedure

Step 1 From the main menu, choose **Assurance** > **Trends and Insights** > **Trend Deviations**.

The **Network Insights** window appears with the filters **Capacity** (the default), **Coverage**, and **Throughput**. Click the appropriate filter to refresh the data in the table.

Note

The filters are dynamic. If there are no insights available for a filter, that filter is not displayed.

Insights table	
Item	**Description**
Occurrence	Time duration when this trend was observed, such as May 27 - June 03 2023.
Insight Type	List of **Daily** and **Weekly** insight types.
Insight	List of all the AI-driven insights that were observed during a specific time period.
Category	Category under which the insight was observed. Insight KPIs are grouped under these categories: • **Capacity**: Radio Client Count, Channel Change Count • **Coverage**: Interference, Avg Client SNR, Avg Client RSSI, Traffic, Utilization • **Throughput**: Total Radio Throughput
Frequency band	Band frequency used on the AP on which the insight was observed. Values are **2.4 GHz**, **5 GHz**, **6GHz**, or all the band frequencies.
KPI	KPI for that specific insight.
icon	Allows you to customize the columns that you want displayed in the Insights table. Click the icon, uncheck the check box for the column that you do not want displayed, and then click **Apply**.

Step 2 From the **Insight** column, click an insight to open a slide-in pane with this information:

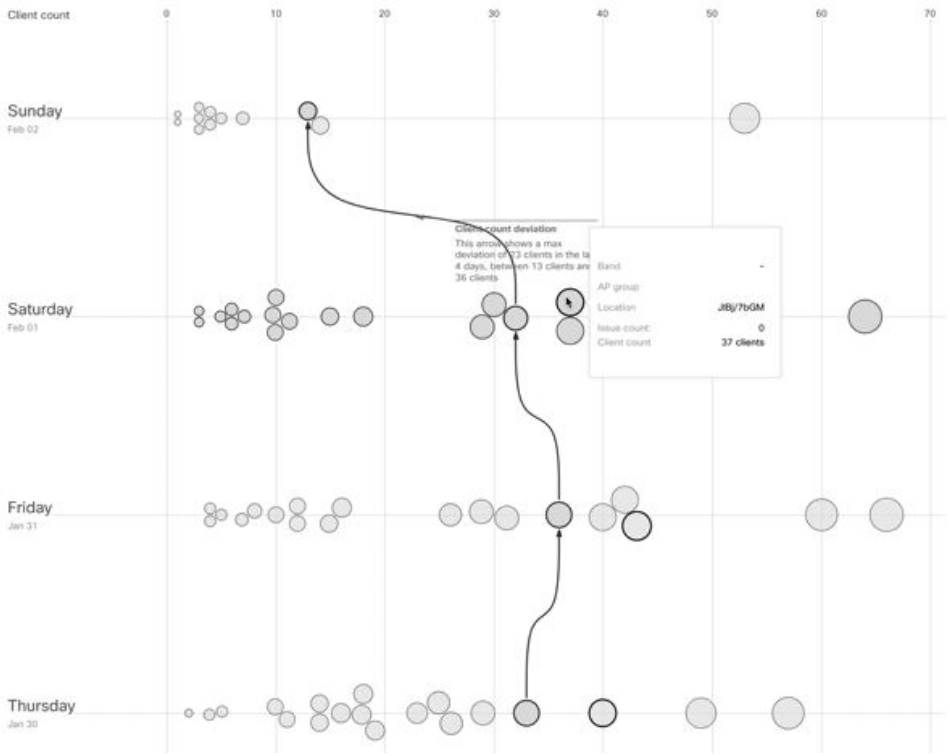
Insight details slide-in pane	
Item	**Description**
Cisco AI	Provides information about how the insights are computed. Click Learn More to get an overview of Artificial Intelligence.
Insight Summary	A brief summary about the trend that is observed in the beeswarm chart. The summary provides information such as the name of the site or AP, client count, radio band frequency, and time period during which the deviation was observed.
Weekly Client Load	Client load per week.

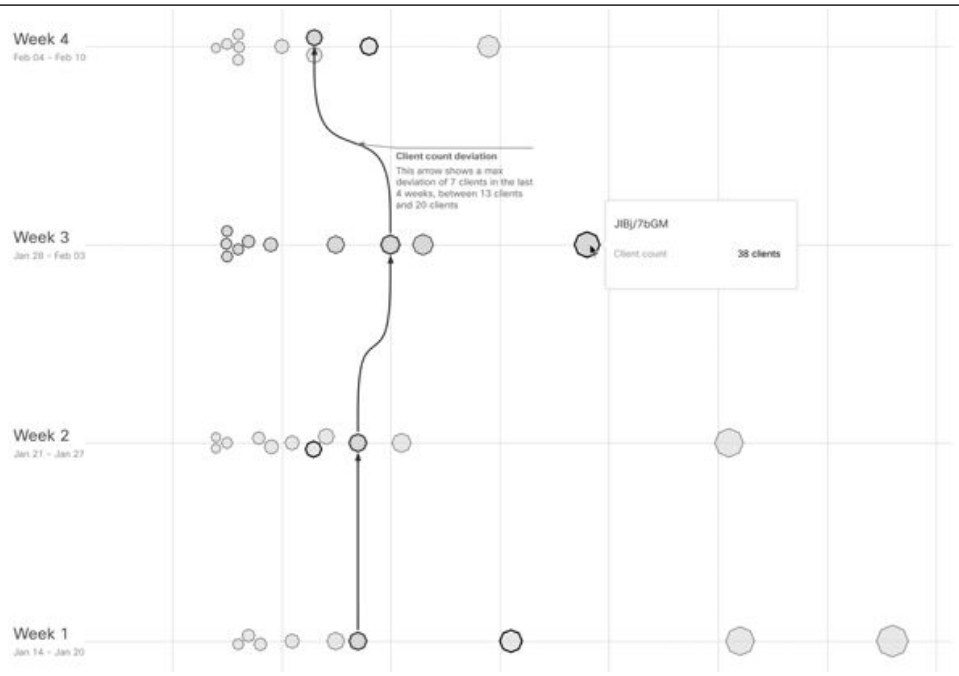
Insight details slide-in pane	
Item	**Description**

Troubleshoot	Provides links that allow you to troubleshoot and fix the trend before it becomes a critical issue:
	• **Network Heatmap** opens the heatmap and provides information about the AP or building that is highlighted in the beeswarm chart. The heatmap that displays is for the specific month in which the trend was observed.
	  • **Intra-Site**: The heatmap launches with the specific AP highlighted and prioritized in the list.
	  • **Inter-Site**: The heatmap launches with the filtered view of the APs in the building (site).
	• ***AP_Name*** opens the **Device 360** page for that AP.

Issue Count	Issue count gradient.

Insight details slide-in pane	
Item	**Description**
Chart	

Insight details slide-in pane	
Item	**Description**
	The beeswarm chart displays the performance of the client devices in your network in a 4-day (daily insights) and week (weekly insights) time interval as shown in this figure. If there is a systematic deviation of network behavior over a time period, that trend appears by arrows in the chart. ***Figure 55: Beeswarm chart*** **Daily Insights**  **Weekly Insights**

Insight details slide-in pane	
Item	**Description**
	 **Note** • Each circle in the beeswarm chart represents this data: • **Intra-Site**: The circle represents a radio. • **Inter-Site**: The polygon represents a building. • The size of the circle represents the number of clients in the AP. A small circle has a lower client count; a large circle has a higher client count.

Step 3 Hover your cursor over a circle in the chart for information, such as the name and MAC address of the AP, the band frequency, the AP group, the location of the AP, issue count, client count, and the KPI value.

Note
For Global sites, when you hover your cursor over a circle in the chart, you see information about the building in which the trend was observed and the client count.

Compare APs and switches in network heatmaps

Use the Network Heatmap to visually compare all of the APs in your network for a given month to spot trends and gain insights. You can decide to compare APs across different KPIs and band frequencies. The insights you gain provide information about the most congested KPIs, the most congested APs, and within those APs, which APs are being used. This information allows you to further drill down to the site or building in which

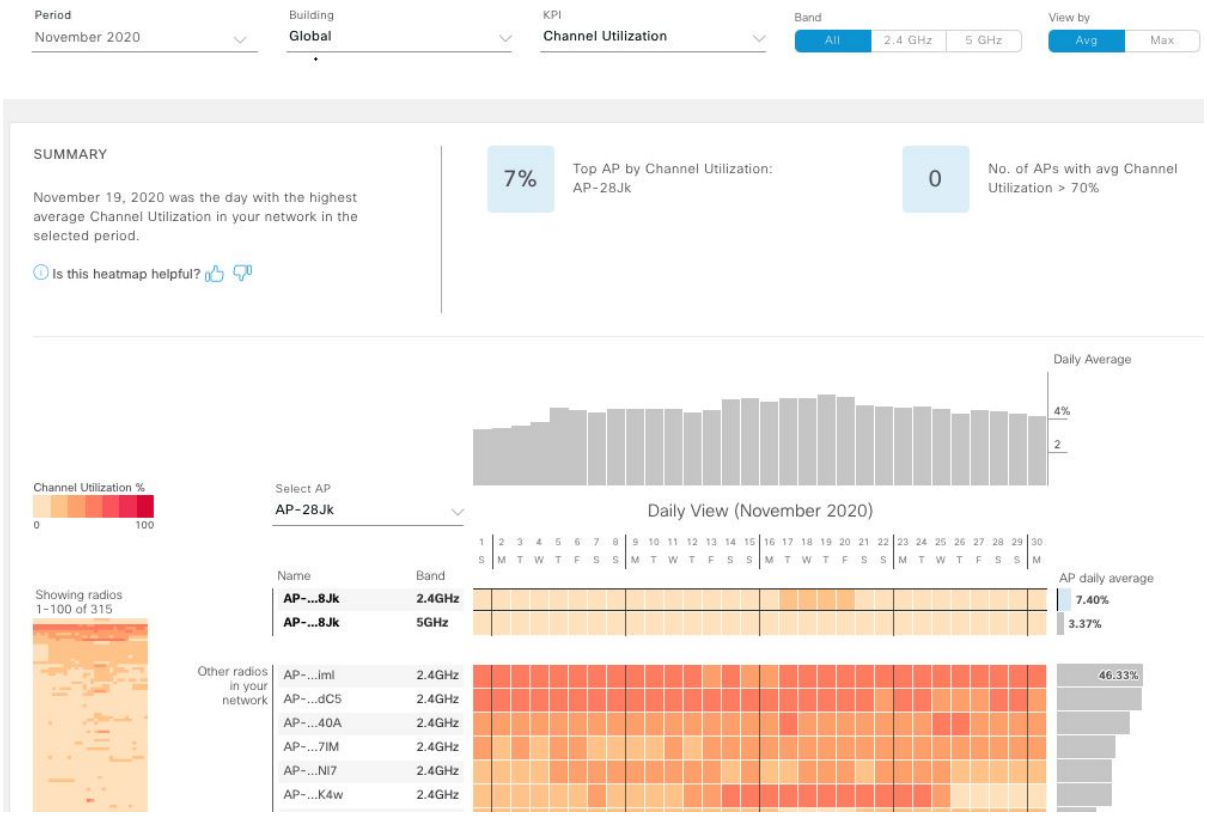
the trend has been observed. After you have pinpointed your AP or a group of APs, you can determine how those APs are behaving historically: per day, per week, and during the entire month.

Procedure

Step 1 From the main menu, choose **Assurance** > **Network Heatmap**.

The **Network Heatmap** window appears with this information:

Figure 56: Network Heatmap window



Network Heatmap window	
Item	**Description**
Show	Display heatmap information based on the device type that you select from the drop-down list. You can select **Access Points** (the default) or **Switches**.
KPI drop-down list	Display information in the heatmap for the KPI that you select from the drop-down list. For Access Points, the default KPI is **Client Count**. For Switches, the default KPI is **Temperature: All Sensors**.

Network Heatmap window	
Item	**Description**
Switch Family drop-down list	Display information in the heatmap based on the switch family that you select from the drop-down list. This drop-down list is displayed only when you select the device type Switches from the **Show** drop-down.
Time Range	Click the **Time Range** drop-down to select **Month** or **Day** and display information in the heatmap for a specific month or a day.
Location	Display information in the heatmap for your entire global network or for a specific site and building that you select from the drop-down list. The default is **Global**.
Band	Display information in the heatmap for the band frequency that you select. Options are **2.4 GHz**, **5 GHz**, and **6 GHz**. By default, all three band frequencies are selected.
View By	View the information in the heatmap based on the option that you select. Based on the KPI that you select, the options displayed in the **View By** list vary. Some KPIs allow you to sort by **Avg**, **Min**, or **Max**, some by **Avg** or **Max**, while other KPIs do not provide any options.
Summary area	Display a summary of the insight gained from the heatmap analysis: • The day of the month that was the busiest. • Number of APs or switches that had no clients per radio. • Number of APs or switches that had more than 50 clients per radio.
Feedback icon	Click the  icon to provide your comments on whether the information on this page was helpful, and then click **Submit**.
KPI gradient	Depending on the KPI you select from the KPI drop-down list, this area provides information about the performance of the KPI in a color gradient. The darker color block indicates a significant KPI score. For example, a lower RSSI score is more significant than a higher RSSI score. A higher client count score is more significant than a lower client count score.
Search AP drop-down list	Search for and select an AP: **a.** Click the **Search AP** drop-down list and enter the AP name in the search filter. The AP that you searched for is highlighted in the drop-down list. **b.** Click the highlighted AP to select it. The individual radios of the AP are displayed separately on the heatmap.

Network Heatmap window	
Item	**Description**
Network Daily Avg, **Min**, or **Max** graph	Depending on the **View By** option you choose, the appropriate graph is displayed. • If you select **Avg**, the graph shows the daily average value and highlights the highest daily average. • If you select **Min** or **Max**, the graph shows minimum or maximum daily value, and highlights accordingly. Hover your cursor over the bar on the graph to view the KPI value for each day.
Showing Radios heatmap	Provides a compressed view of the heatmap. By default, this area displays the heatmap for the first 100 radios. To view the heatmap data for additional radios, scroll down to the bottom of the compressed heatmap, and then select the appropriate option from the drop-down list.
AP Heatmap area	Contains this information: • **Radios in Your Network**: Displays the name of the AP and the band frequency that was used by the client. Click the icon next to the AP to open the **Device 360** window for that AP. Depending on the band frequency you select from the **Band** options, this area lists the APs in the corresponding chosen band. • **AP Heatmap**: Allows you to determine how the APs are behaving historically: per hour, per day, per week, and during the entire month. The intensity of the color in the blocks indicates its significance. The darker color block is more significant than the lighter color block. Each row in the heatmap represents one AP. Hover your cursor over a color block in the **Heatmap** to get information about the AP, such as its name and MAC address, band frequency, location, and daily average KPI score. • **AP Daily Average** or **AP Daily Max**: Depending on what you select in the **Sort By** option, this area displays the average KPI score or the max KPI score for each AP during the month. The AP with the highest score is listed on top. Hover your cursor over the **AP Daily Average** or the **AP Daily Max** area to determine the average or max KPI value for an AP during the month.
Export	Click **Export** to export the heatmap data to a CSV file. APs and filters applied to the heatmaps are applied to the exported data. Export is enabled only on the daily view and not on the hourly view.

Step 2 To view heatmap data for additional radios, scroll down to the bottom of the window and select the appropriate option from the drop-down list.

Compare KPI values with peers in your network

Use this procedure to determine how your network is performing compared to your peer networks for a selected Key Performance Indicator (KPI).

Note Peer networks used for comparison have a similar size.

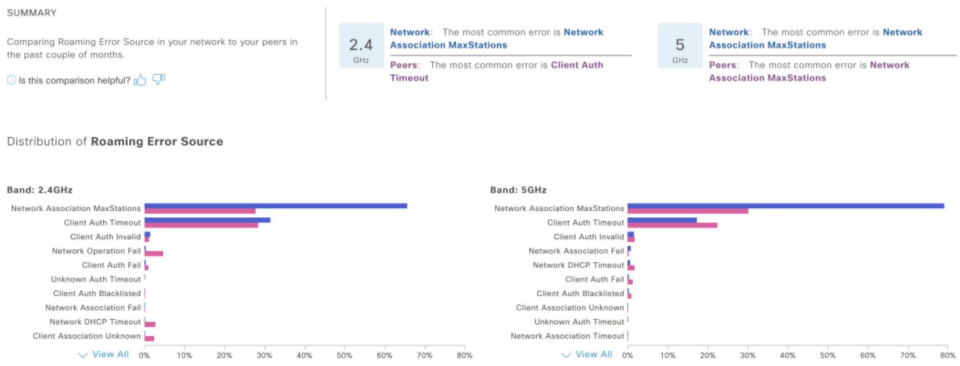
Peer comparisons use data from the most recent three months.

Procedure

Step 1 From the main menu, choose **Assurance** > **Peer Comparison**.

The **Peer Comparison** window appears with this information:

Peer comparison window	
Item	**Description**
KPI drop-down list	Select a KPI from the drop-down list. Options are **Radio Throughput** (the default), **Cloud Apps Throughput**, **Radio Resets**, **Packet Failure Rate**, **Interference**, **Onboarding Error Source**, **Roaming Error Source**, and **RSSI**.
Show	Select the day for which you want to compare the KPI values between your network and your peer networks. The default is **All Days**.
Summary	AI Network Analytics analyzes the bar graphs and provides a brief summary about the findings: • **2.4 GHz**: Summary of the Network and Peer values for the 2.4-GHz band frequency. • **5 GHz**: Summary of the Network and Peer values for the 5-GHz band frequency. • **6 GHz**: Summary of the Network and Peer values for the 6-GHz band frequency.
Highlight Peers toggle button	Allows you to toggle between your network and the peer network graphs.

Peer comparison window	
Item	**Description**
Peer Comparison Bar Graph	By default, highlights the KPI values for your network in the **Band 2.4 GHz** and **Band 5 GHz** graphs, as shown in this figure. To highlight the KPI values for the peer networks, click the **Highlight Peers** button. ***Figure 57: Peer comparison bar graph***  The colors in the graph represent these networks: • **Blue**: Your network. • **Pink**: Peer networks.

Step 2 To display the KPI values for your network and your peer networks for a specific day, select the appropriate day from the **Show** area.

Compare buildings, AP model families, and wireless endpoint types

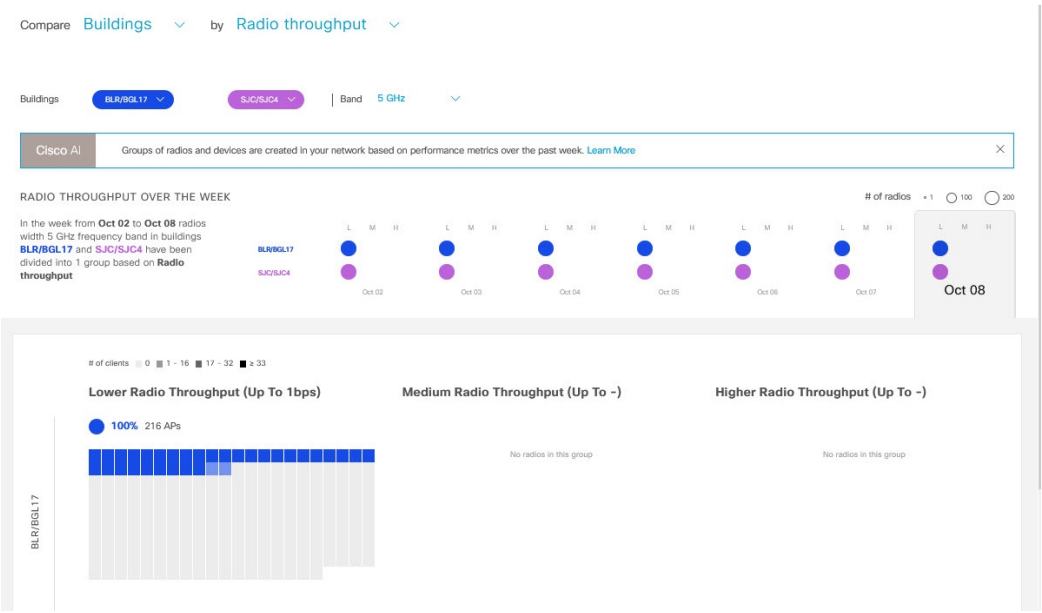
Use this procedure to view, compare, and identify performance improvement opportunities for objects in your network (buildings, AP model families, and wireless endpoints) across selected Key Performance Indicators (KPIs).

Procedure

Step 1 From the main menu, choose **Assurance** > **Network Comparison**.

The **Network Comparison** window appears with this information:

Figure 58: Network Comparison window



Network Comparison window	
Item	**Description**
Compare drop-down list	Select the object in your network that you want to compare. Options include: • **Buildings** (sites) • **AP Model Families** • **Wireless Endpoints** (Android device, Android phone, iOS tablet, iOS phone, Linux workstation, and so on)

Network Comparison window	
Item	**Description**
By KPI drop-down list	Select a KPI that you want to use to compare the objects in your network. For **Buildings**, the options include: • **Radio Throughput** • **Channel Utilization** • **Average Client RSSI** • **Average Client SNR** • **Average Onboarding Time** • **Average Authorization Time** • **Average DHCP Time** • **Cloud Throughput** • **Media Throughput** • **Social Throughput** • **Interference** For **AP Model Families**, the options include: • **Radio Throughput** • **Interference** • **Media Apps Throughput** • **Average Client RSSI** • **Channel Utilization** • **Average Client SNR** • **Cloud Throughput** • **Social Throughput** For **Wireless Endpoints**, the options include: • **Average AAA Time** • **Average Onboarding Time** • **Average DHCP Time**

Network Comparison window	
Item	**Description**
Buildings **AP Model Families** or **Wireless Endpoints** drop-down list	Select the first network object (building, AP model family, or wireless endpoint) for which you want to compare the KPI values. The first network object is represented in blue. Select the second network object whose KPI values you want to compare with the first network object. The second network object is represented in pink/purple.
Band	Select the band frequency. Options are **Band 2.4 GHz** and **Band 5 GHz**.
Summary/Timeline	Displays the average KPI performance for each day of the week, for each network object.
Client Count gradient or **Device Count** gradient	For certain KPIs, such as **Radio Throughput** and **Average Client RSSI**, this area provides the client count per radio for each of the sites. For certain KPIs, such as **Onboarding Time**, this area provides the number of devices for each of the sites. The intensity of the color in the blocks indicates the client count or device count. Darker color blocks represent more clients compared to lighter color blocks.
AP Clusters or **Device Type Clusters**	This area displays two sets of clusters, one for each network object. From this area you can visually compare the performance of the two network objects. It provides this information: • KPI performance, as a percentage. • How the objects in your network are clustered in each site. • Objects in your network that are experiencing low, medium, and high KPI values. For certain KPIs, such as **Onboarding Time** and **Authorization Time**, this area displays information including: • The types of devices that the clients onboarded in each site, such as Windows workstation, OS X workstation, Linux workstation, Android phone, iOS device, and so on. • The number of each device type. • The number of devices that are experiencing slow, medium, and fast KPI time.

Step 2 Hover your cursor over a color block in the cluster to get information about the AP, such as the date, the building in which the AP resides, the model number of the AP, radio protocol, and the radio client count. A darker color block has more clients than a lighter color block.

View and monitor network performance using baselines

Cisco AI Network Analytics uses the most advanced machine learning techniques to define the baseline that is relevant to your specific network and sites. With this information Cisco AI Network Analytics determines what is normal for each network and site at a specific moment, and identify the most important issues.

Use this procedure to explore and monitor the network performance using baselines derived from machine learning algorithms.

Procedure

Step 1 From the main menu, choose **Assurance** > **Baselines**.

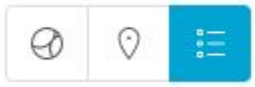
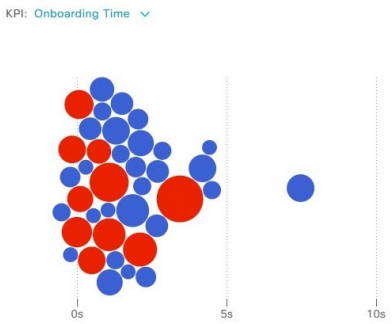
The **Baselines** dashboard appears.

Figure 59: Baselines dashboard



Step 2 Use the **Network Overview** window to view this information:

Network Overview window	
Item	**Description**
Summary	Displays the total number of buildings, buildings impacted by issues, and wireless controllers in your network.
AI Driven Issues	Displays the issues detected by Cisco AI Network Analytics, triggered based on deviations from the predicted baseline for your specific network environment.
Global Location drop-down list	Click the location icon to open the slide-in pane to select a site or building. The information is refreshed in the dashboard based on your selection.
Time Range setting	Enables you to display data within a specified time range on the dashboard. Do these tasks: • From the drop-down menu, select the length of the range: 24 hours, or a custom range. • Specify the start and end dates. • Click **Apply**.

Network Overview window	
Item	**Description**
KPI drop-down list	Select a KPI from the drop-down list. Options include: • **Onboarding Time** (default) • **Onboarding Failures** • **DHCP Time** • **Authentication Time** • **Association Failures**
 Map View	Click this toggle button to display the health of all network sites on a map view oriented by geographic location.
 List View	Click this toggle button to display the sites and buildings from your network in a list format.
 Beeswarm Chart	Click this toggle button to view the beeswarm chart, which provides insights about the performance of the client devices of your network according to the selected KPI.  In this case, the entity in the beeswarm chart is a building and it is represented in circles. Each circle in the beeswarm chart represents information such as: • **Blue**: The circle represents a building. Hover your cursor over a circle in the chart to get information, such as location, KPI, SSID, wireless controllers, and client count. • **Red**: The circle represents a building impacted with issues. Hover your cursor over a circle in the chart to get information, such as location, KPI value, SSID, wireless controllers, client count, and AI-driven issues. • The size of the circle represents the number of clients connected. A small circle has a lower client count and the large circle has a higher client count.

Step 3 From the beeswarm chart, click a circle to display the building view for this information:

Building view
Displays the specific information of a site or building. You can select the KPIs, SSID, and wireless controller from the respective drop down list to view the data. Use the timeline slider to specify a more granular time range by clicking and dragging the timeline boundary lines. Use the color-coded charts below the timeline slider to determine how your network is performing. View issues based on the deviations from the predicted baseline for a selected KPI within the specified time period. Hover and move your cursor over the charts to view synchronized tooltips that display duration, predicted upper, and predicted lower range at a selected point in time. The color codes represent this information: • **Red** represents AI-driven issues • **Blue** represents the average KPI duration • **Green** represents the predicted KPI Click **View Details** to open a slide-in pane with additional details, depending on the KPI you select from the KPI charts. In the slide-in pane, the color-coded charts appear for Average KPI Duration(s) (such as Onboarding Time, DHCP Time, Onboarding Failures, and Authentication Time) and Unique Clients. Sankey charts are displayed to emphasize the major flow between floors and device type (client devices). Below the charts, you can see the AP name, onboardings, failed onboardings, percentage of failed onboardings, client count, and so on. **Note** The client count shown in the table is an average of selected time interval over the individual client count readings observed in the 30-minute window.

View the RF network using the AI-enhanced RRM dashboard

Cisco AI Network Analytics uses machine learning algorithms to define the behavior of a radio frequency (RF) network within a building enabled with enhanced Radio Resource Management (RRM).

Before you begin

- Assurance supports site-based, role-based access control (SRBAC), which limits a user's scope of access to certain network sites. You must ensure you have access to the sites and devices while using AI-Enhanced RRM dashboard. For more information on user roles and permissions, see Cisco Catalyst Center Administrator Guide.
- You must assign a location to an AI RF profile to view the AI-Enhanced RRM dashboard. For more information, see **Assign Location to an Existing AI RF Profile** in the *Cisco Catalyst Center User Guide*.
- You must provision the devices across the AI RF profile assigned locations to access AI-Enhanced RRM insights. For more information, see **Provision Wireless Devices** in the *Cisco Catalyst Center User Guide*.

- Cisco AI-Enhanced RRM is supported only on Cisco Catalyst 9800 Series Wireless Controllers and Cisco IOS XE Release 17.7.1 or later.
- To use the **Run RRM Simulation**, **Insights**, and **Service Bundle** options, you must be a **Super Admin** or **Network Admin**.

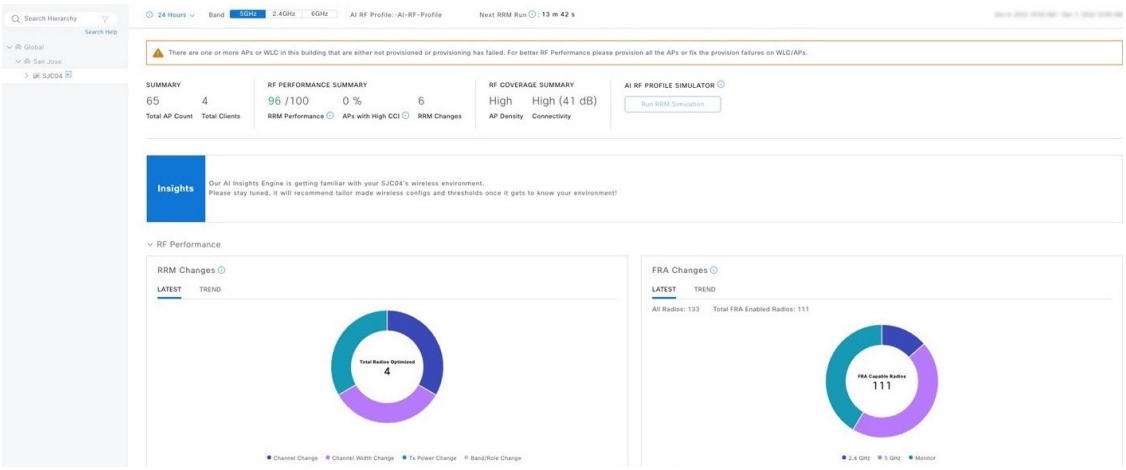
Procedure

Step 1 From the main menu, choose **Assurance** > **AI-Enhanced RRM**.

Step 2 In the left pane, you can either search for a site by entering its name in the **Find Hierarchy** field or expand **Global** to select the sites.

The **AI-Enhanced RRM** dashboard appear.

Figure 60: AI-Enhanced RRM dashboard



Step 3 Use the **AI-Enhanced RRM** dashboard top-menu bar for this functionality:

Item	Description
Time Range	Enables you to display data within a specified time range on the dashboard. The available time ranges are **24 Hours**, **7 Days**, or **14 Days**.
Band	Enables you to toggle between the **2.4GHz**, **5GHz**, and **6GHz** bands to display the data for a particular band.
AI RF Profile	Displays the current AI RF profile assigned to the building.
Next RRM Run	AI-Enhanced RRM computation occurs every 30 minutes. RRM decisions are updated and pushed to the device after the computation.

Step 4 Use the summary dashlet to view this information:

Item	Description
Summary	Displays the total number of AP counts and clients in your network. If there are any APs that don't meet the license requirements, this dashlet displays the  icon with the number of noncompliant APs for the bands that are not operational. You can click the corresponding hyperlink to view the dialog box with the details. In the dialog box, you can click **License Manager** to open the **License Manager** window and enable the required licenses. For more information, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
RF PERFORMANCE SUMMARY	• **RRM Performance**: Shows a composite metric based on several KPIs, such as co-channel interference, noise, SNR, and radio utilization. • **APs with High CCI**: Shows the percentage of APs seeing high co-channel interference. • **RRM Changes**: Shows the total number of RRM channel changes, channel bandwidth changes, and Tx power change events by the time of the day.
RF COVERAGE SUMMARY	• **AP Density**: Shows the density of APs as low, medium, or high in RF coverage. • **Connectivity**: Shows the connectivity of APs in RF coverage.

Step 5 Under **AI RF Profile Simulator**, click **Run RRM Simulation** to simulate RF configurations, visualize the impact, and update or create an RF profile.

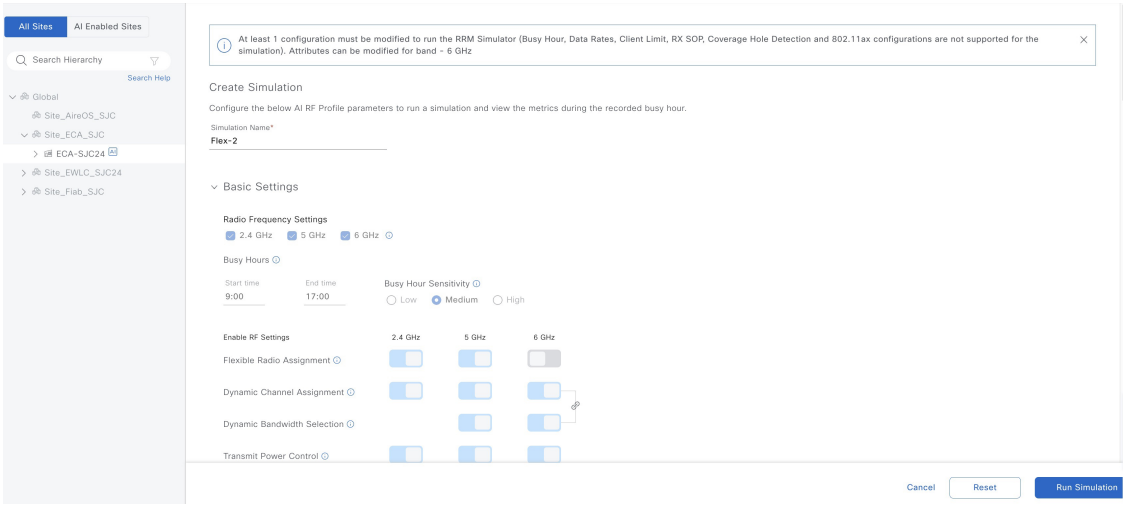
The AI RF Profile Simulator allows you to simulate changes to the current RF profile and visualize the projected outcomes against the AI-Enhanced RRM dashlets.

Note
The RRM simulation runs based on the radio band that you selected on the AI RF profile and cannot be modified in the simulator.

a) In the **Welcome to RRM Simulator** window, click **Create Simulation**.

The current AI RF profile information appears.

Figure 61: Create simulation window



b) You can modify the attributes under the band that is selected for simulation, as needed, to see the metrics.

Note

- For 5 GHz, the attributes such as **Busy Hour**, **Data Rates**, **Client Limit**, **RX SOP**, **Zero Wait DFS**, **Coverage Hole Detection**, and **802.11ax** are not considered for simulation.
- For 2.4 GHz, the attributes such as **Busy Hour**, **Data Rates**, **Client Limit**, **RX SOP**, **Coverage Hole Detection**, **802.11ax** are not considered for simulation.
- For 6 GHz, the attributes such as **Busy Hour**, **Data Rates**, **Client Limit**, **RX SOP**, **Coverage Hole Detection**, **802.11ax**, and **802.11be** are not considered for simulation.

c) Click **Reset** to change the AI RF profile attribute value to the corresponding base AI RF profile value.

d) Click **Run Simulation**.

Note

Ensure that you have modified the AI RF profile attributes before you run the simulation.

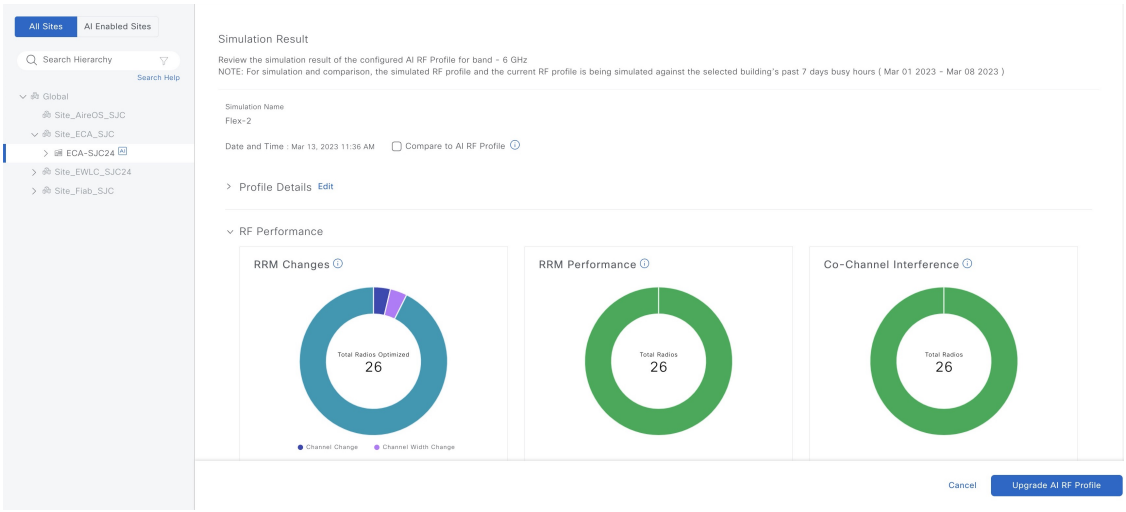
A message stating that the **Simulation in Progress** appears.

e) In the **Simulation Result** window, review the simulation configured on the AI RF profile for the selected band.

- **Simulation Name**
- **Profile Details**
- **RF Performance**
- **RF Coverage**

To edit any AI RF profile attributes, click the **Edit** option in the **Profile Details** area.

Figure 62: Simulation Result window



f) To compare the simulated and currently applied AI RF profile configurations, check the **Compare to AI RF Profile** check box.

g) Click **Upgrade AI RF Profile**.

h) If the AI RF profile is assigned to multiple locations, create and assign a new RF profile with the recommended settings by entering a new profile name and clicking **Save**.

i) In the **Apply RRM Simulation Settings** window, schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 64.

  Note
  After submitting a task for immediate or scheduled deployment, make the necessary edits in the **Upgrading AI RF Profile** dialog box based on the assigned locations of the AI RF profile.

  - If an AI RF profile is assigned to multiple buildings, a new RF profile is created and you can edit the RF profile name and task name.
  - If an AI RF profile is assigned to one building, you can edit the task name but cannot edit the RF profile name.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 64.

Note
Upgrading the AI RF profile causes the AP to momentarily lose association with the wireless controller, which may result in client connectivity disruption.

j) On the **Tasks** window, monitor the task deployment.

Step 6 Use the **Insights** dashlet to review the insights generated by the AI-Enhanced RRM. The insights are configuration recommendations that can be applied to the AI RF profile.

The **Insights** dashlet displays these possible insights:

- Busy Hours
- Channel Width
- Channel List
- Enable FRA
- Preferred Scanning Channel (PSC) Enforcement
- TPC Threshold

Step 7 Click the **Insights** icon to view the Cisco recommended insights.

a) In the **Review Cisco AI Recommendations** window, review and check the check box of the configurations for the AI RF profile from the available recommendations for the selected site.
b) Click **Apply**.
c) If the AI RF profile is assigned to multiple locations, create and assign a new RF profile with the recommended settings by entering a new profile name and clicking **Save**.
d) In the **Apply RRM Recommendations** window, schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 64.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 64.

Note
Upgrading the AI RF profile causes the AP to momentarily lose association with the wireless controller, which may result in client connectivity disruption.

e) On the **Tasks** window, monitor the task deployment.

Step 8 Expand **RF Performance** for this functionality:

Item	Description
RRM Changes dashlet	Includes these tabs: • **LATEST**: Shows the total number of RRM channel changes, channel bandwidth changes, Tx power change, and band or role change events in the last 30 minutes. • **TREND**: Shows the channel changes, channel bandwidth change, Tx power change, and band or role change events for APs and selected time in the time range. **Note** • Band or role change event is not applicable for the **6 GHz** band. • Channel bandwidth change event is not applicable for the **2.4 GHz** band. Click either the color segment in the graph or the **View Details** link to open the **RRM Changes** slide-in pane. **a.** Hover your cursor over the color segment in the graph to view the **Change Category** and **Total Affected APs**. **b.** Click a segment in the graph to view the device data in the **Access Points** table that is displayed below the chart: • Radio • Change Category **c.** Click the radio button next to the AP to view the **Event Reasoning** of change categories managed by RRM. **Note** In the **Access Points** table, hover your cursor over the **i** icon to view more details. **d.** Click **Export** to download the AP table data to your local machine.

Item	Description
FRA Changes dashlet	Displays the number of total radios, Flexible Radio Assignment (FRA)-capable radios, and FRA-enabled radios for these radio modes: • 2.4 GHz • 5 GHz • Monitor **Note** **FRA Changes** dashlet is not shown for the **6 GHz** band as FRA is not applicable for 6 GHz. Includes these tabs: • **LATEST**: Shows the total number of FRA-capable and FRA-enabled radios. Also shows a split of FRA-capable radios between 2.4-GHz, 5-GHz, and monitor radio modes. • **TREND**: Shows the number of FRA-enabled radios for 2.4-GHz, 5-GHz, and monitor radio modes for the selected time in the time range. Click either a color segment in the graph or the **View Details** link to open the **FRA Changes Details** slide-in pane. **a.** Hover your cursor over a color segment in the graph to view the number of FRA-enabled radios for the corresponding radio mode. **b.** Click the color segment in the graph to view the AP device data in the **Radios** table that is displayed below the chart: • AP Name • Slot ID • COF % • Suggested mode • Channel **Note** In the **Radios** table, hover your cursor over the **i** icon to view more details. **c.** Click **Export** to download the data to your local machine.

Item	Description
RRM Performance dashlet	Includes these tabs: • **LATEST**: Shows the total number of APs contributing to **Poor**, **Fair**, and **Good** AP health scores in the last 30 minutes. • **TREND**: Shows the **Poor**, **Fair**, and **Good** RRM health score of APs for the percentage of AP count and selected time in the time range. Click either a color segment in the graph or the **View Details** link to open the **RRM Health** slide-in pane. **a.** Hover your cursor over the color segment in the graph to view the **Fair**, **Poor**, and **Good** RF performance score of the AP and its radio. **b.** Click the color segment in the graph to view this device data in the **Access Points** table that appears below the chart: • AP Name • Slot ID • Neighbor • Interference • Noise • Client **Note** In the **Access Points** table, hover your cursor over the **i** icon to view more details. **c.** Click **Export** to download the AP table data to your local machine.

Item	Description
Co-Channel Interference dashlet	Includes these tabs: • **LATEST**: Shows the total number of APs experiencing **Low**, **Medium**, and **High** co-channel interference in the last 30 minutes. • **TREND**: Shows the percentage of **Low**, **Medium**, and **High** co-channel interference of APs for the percentage of AP count and selected time in the time range. Click either a color segment in the graph or the **View Details** link to open the **Co-Channel Interference** slide-in pane. **a.** Hover your cursor over the color segment in the graph to view the **Low**, **Medium**, and **High** co-channel interference of APs. **b.** Click the color segment in the graph to view this device data in the **Access Points** table that appears below the chart: • AP Name • Slot ID • Channel • Impact Score • CCI (dBm) • Duty Cycle **Note** In the **Access Points** table, hover your cursor over the **i** icon to view more details. **c.** Click **Export** to download the AP table data to your local machine.

Item	Description
Utilization Per Channel dashlet	Displays the utilization chart. For the 6-GHz band, the utilization chart is based on the UNII level that you select in the **View by** drop-down list. The UNII levels are **PSC**, **UNII 5**, **UNII 6 & 7**, and **UNII 8**. The default view is **PSC**. The **LATEST** tab displays the total number of APs experiencing co-channel interference in the last 30 minutes. Hover your cursor over the chart to view these details: • Channel Number • Utilization • Interference • Max Utilization • Min Utilization The **TREND** tab displays the utilization per channel details for the percentage of utilization and selected time in the time range. **Note** The **Select Channel** drop-down list allows you to search a channel by entering its name or select a channel from the list to display the details.
AP and Radar per Channel dashlet	Displays the AP and radar information per channel for the 5-GHz band. The **LATEST** tab displays the AP and radar per channel details in the chart for APs and channels in the last 30 minutes. Hover your cursor over the chart to view these details for the 5-GHz band: • Channel # • No. of Radios • No. of Radar Event per Channel The **Trend** tab displays the number of radios and radar event for the selected channel.
AP per Channel dashlet	Displays the AP information per channel for the 2.4-GHz and 6-GHz bands. The **LATEST** tab displays the channel number and number of radios on that channel. Hover your cursor over the chart to view these details: • Number of channels • Tx/Rx utilization • Interference The **TREND** tab displays the number of radios for the selected channel.

Step 9 Expand **RF Coverage** for this functionality:

Item	Description
AP Spatial Density dashlet	The AP spatial density value represents the number of APs that are the neighbors of a selected AP in your infrastructure at or above -70 dBm. The density of APs affects the optimal effective values of channels, channel width, and Tx power. • **LATEST**: Shows the number of APs that are the neighbors of a selected AP in your infrastructure for the percentage of radio count, AP neighbor density, and percentage of client count in the last 30 minutes. Hover your cursor over the chart to view this information: • AP Neighbor Density • Radio Count • Client Count • **TREND**: Shows the average neighbor density number and radio count for the AP count and selected time in the time range. Average neighbor density ranges are **<5**, **5-10**, **10-15**, **15-20**, **20-25**, and **>=25**. Click either a color segment in the graph or the **View Details** link to open the **AP Spatial Density Details** slide-in pane. **a.** Click a color segment in the graph to view the **Top APs** graph by lower/higher neighbor density and this device data in the **Access Points** table: • AP Name • Slot ID • Neighbor Density Metric • Total Rx Neighbors • Highest on Channel Neighbor RSSI • Total on Channel Neighbors **Note** In the **Access Points** table, hover your cursor over the **i** icon to view more details. **b.** In the **Top APs** area, click the drop-down list to select top APs by lowest neighbor density or highest neighbor density. **c.** Hover your cursor over the **Top APs** chart to view the **Min**, **Max**, and **Latest** APs in the chart for AP and neighbor count. **d.** Click **Export** to download the AP table data to your local machine.

Item	Description
Power Distribution dashlet	

Item	Description

	The power distribution chart helps you visualize the physical Wi-Fi coverage areas in your environment. It also allows you to identify the APs that are operating at maximum and minimum power levels.
	
	You can display the data based on **Power Level** or **Power dBm** that you select in the **Filter** drop-down list.
	
	• **LATEST**: Shows the number of APs that are operating at different power level along with radio count percentage and neighbor count percentage in the last 30 minutes.
	
	• Hover your cursor over the chart to view this information:
	  • Operating Power Level (for the power level view)
	  • Operating Power dBm (for the power dBm view)
	  • Radio Count
	  • Neighbor Count
	
	• **TREND**: Shows the operating power level, radio count, and selected time in the time range.
	
	Hover your cursor over the trend chart to view the radio count percentage operating at different power levels.
	
	The power levels calculations are from **Level 1** (maximum power level) to **Level 8** (minimum power level).
	
	Click either a color segment in the graph or the **View Details** link to open the **Power Distribution Details** slide-in pane.
	
	a. Click a color segment in the graph to view the **Top APs** graph by lower/higher neighbor density and this device data in the **Radios** table:
	  • AP Name
	  • Slot ID
	  • Coverage Hole Count
	  • Tx Power (dBm)
	  • Neighbor Count
	  • Neighbor Density Metric
	  • Delta Average Neighbor Tx power (dB)
	
	For the 6-GHz band, if you filter the data using **Power dBm**, this device data appears in the **Radios** table:
	  • AP Name
	  • Slot ID
	  • Coverage Hole Count

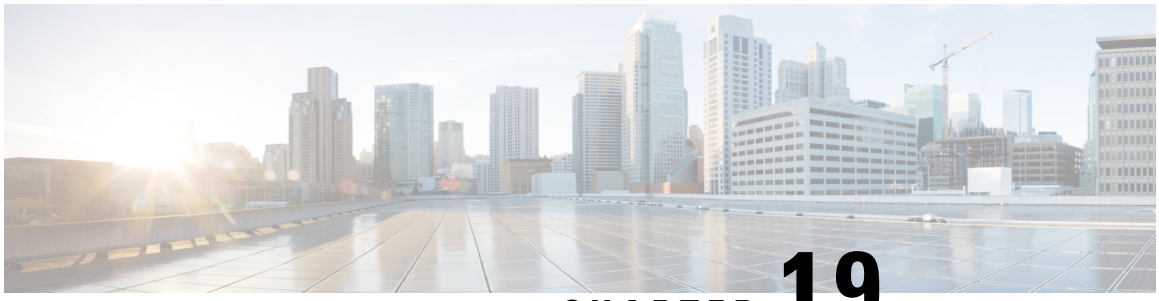
Item	Description
	• Tx Power (dBm) • Neighbor Count • Neighbor Density Metric • Delta Average Neighbor Tx power (dB) • Channel Width (MHz) **Note** In the **Access Points** table, hover your cursor over the **i** icon to view more details. **b.** Click **Export** to download the AP table data to your local machine.

Step 10 Expand **Additional Site Level Information** to download a service bundle.

Step 11 In the **Service Bundle** area, click the **Request a Latest Service Bundle** link to download a service bundle for the last one hour for the selected building.

Step 12 To download service bundle data for any other time period in the past 14 days, in the **SELECT A PERIOD TO DOWNLOAD** area, specify the **Start Date**, **Start Time**, **End Date**, and **End Time**, and then click **Download Service Bundle**.

A service bundle is saved to your local machine that contains configuration parameters and RRM telemetry used for RRM algorithms at the selected time period. This service bundle can be provided to Cisco Technical Assistance Center (TAC) for troubleshooting.



CHAPTER 19

Manage Intelligent Capture

- About Intelligent Capture, on page 389
- Supported devices for Intelligent Capture, on page 389
- Intelligent Capture best practices, on page 390
- How to configure and use Intelligent Capture, on page 390
- Troubleshoot Intelligent Capture, on page 418

About Intelligent Capture

For Catalyst Center, all information about device and client health is typically available from Cisco Wireless Controllers. Intelligent Capture (iCAP) provides support for a direct communication link between Catalyst Center and access points (APs), so each of the APs can communicate with Catalyst Center directly. Using this channel, Catalyst Center can receive packet capture data, AP and client statistics, and spectrum data. With the direct communication link between Catalyst Center and APs, iCAP allows you to access data from APs that is not available from wireless controllers.

To ensure that the iCAP feature functions effectively, APs need to establish a connection to the Catalyst Center. If any firewalls exist between the APs and the Catalyst Center, make sure to open these TCP ports:

- TCP 443: Used by APs to initiate an HTTPS connection to Catalyst Center for iCAP
- TCP 32626: Used to establish a gRPC channel for receiving AP/client statistics and packet capture data related to the Cisco Catalyst Assurance iCAP feature.

Note

- iCAP is only supported for APs in either local or FlexConnect mode.
- iCAP is not supported in SDA deployments.

Supported devices for Intelligent Capture

For more information about the wireless controllers and APs that support Intelligent Capture (iCAP), see Feature Matrix for Cisco Wireless Access Points.

Intelligent Capture best practices

Follow these best practices to ensure Intelligent Capture (iCAP) functions optimally in Catalyst Center:

- After a new wireless controller device is added to Catalyst Center, disable any iCAP global settings, and then re-enable those settings so that they will be configured on the new wireless controller.
- Before deleting a wireless controller device from Catalyst Center, disable all iCAP settings.
- Before upgrading any of managed wireless controllers or reimaging Catalyst Center, disable all iCAP settings, and then re-enable them after completing the upgrade.
- When removing a wireless controller from your inventory, select the **Clean Up Configuration** option. This ensures that all iCAP configurations are removed from the controller and its associated APs. If you encounter an error during this process due to stale data, simply retry the deletion.
- Before retiring an AP or performing an RMA, go to **Assurance > Intelligent Capture Settings > Access Point**. Review the **AP Stats Capture** and **Anomaly Capture** windows. If the capture mode is set to "Specific - select specific APs," ensure that you disable iCAP for the specific AP being removed.
- Before starting an upgrade, check the status of your capture sessions under **Assurance > Intelligent Capture Settings > Wireless Packet Capture** and **OTA Sniffer Capture**. If any sessions (ICAP Full, Onboarding, Spectrum, or OTA) are currently in progress, wait for these sessions to finish before proceeding with the upgrade.

How to configure and use Intelligent Capture

Onboarding Packet Capture for a client device

About Onboarding Packet Capture for a client device

Onboarding Packet Capture sessions capture packets that the client device uses to join a wireless network, such as 802.11 management frames, DHCP, and EAP packets, and collects the client's RF statistics in 5-second samples. The data displays in the **Client 360** > **Intelligent Capture** window. The session can be started immediately or scheduled to run later. The default duration of the session is 30 minutes and can be set up to eight hours. By default, Onboarding Packet Capture is enabled on the last client-connected wireless controller. You can select up to three wireless controllers to cover the client roaming scenario.



Note

- "Client Schedule Capture" is now rebranded as "Onboarding Packet Capture". While streamlining this nomenclature, you may see the former and rebranded names used in different collaterals. However, "Client Schedule Capture" and "Onboarding Packet Capture" refer to the same feature.
- "Live Capture", "Scheduled Capture", and "Onboarding Packet Capture" all refer to the same feature. These names are used interchangeably throughout different collateral.

Onboarding Packet Capture session limitations

Onboarding Packet Capture sessions have these limitations:

- There are a total of 16 time slots allocated for capture sessions (live and scheduled), where each client in a session uses one time slot and each client can be enabled on up to three wireless controllers.

  If these maximum values are exceeded, for example, you try to start a seventeenth live capture session, an error message is displayed. To schedule another capture session when the maximum time-slot limit is met, you can either stop a running capture session or wait for a capture session to complete. Then you can start a new capture session.



Note The 16-time-slot limit is enforced by the wireless controller.

When capture sessions are configured on Catalyst Center, any live or scheduled capture sessions that Catalyst Center is not aware of (such as partial packet capture sessions that were directly configured on the wireless controller) are removed.

- A maximum of 100 packets involved in onboarding events can be captured during the time period surrounding the event.
- There is a 3.5-GB limit on the total size of all scheduled onboarding packet files that reside on Catalyst Center. If the limit is exceeded, packet files are removed, starting with the oldest, until the total size falls below the 3.5-GB limit. Additionally, any onboarding packet files that are more than 14 days old are removed, even if the total size limit has not been reached.

About client statistics

Onboarding Packet Capture sessions are global settings that enable supported APs to collect client statistics over 5-second intervals.

Client statistics are also collected over 30-second intervals when AP Statistics is enabled for the AP to which the client is connected.

When client statistics are collected, they appear in the RF statistic charts in the **Client 360** > **Intelligent Capture** window.

Run an Onboarding Packet Capture live session for a client device

Use this procedure to enable a live capture session for a specific client device and view data packets for the onboarding events and RF statistics.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Client Health** tab.

The **Client Health** window appears.

Step 3 Open the **Client 360** window of a specific client by doing one of these tasks:

- In the **Client Devices** table, click the hyperlinked identifier or the MAC address of the device.
- In the **Search** field, enter one of these elements:
  - User ID (authenticated through Cisco ISE)
  - IP address
  - MAC address

A 360° view of the client device appears.

Step 4 In the **Client 360** window, click **Intelligent Capture**.

The **Intelligent Capture:** *Client Device* window appears with this information:

Attention

If a ⚠ icon with the message **GRPC link is not ready (CONNECTING)** appears next to the client name, see Client or AP unable to send Intelligent Capture data to Catalyst Center, on page 418 for more details.

Figure 63: Intelligent Capture window of a client



Step 5 Use the timeline slider for this functionality:

Timeline slider	
Item	**Description**
1 hour drop-down list	Click the drop-down list and select a duration to set the range of the timeline. Options are **1 hour**, **3 hours**, and **5 hours**. Default is **1 hour**.

Timeline slider	
Item	**Description**
Timeline Slider	The timeline slider determines the time window of all data displayed. A line chart of onboarding events is displayed for the results of a live capture. Green indicates onboarding events and red indicates anomaly events. To adjust the timeline to a different time window, click the < and > buttons to the desired time window. **Note** The timeline can display data from up to two weeks in the past. For more customization of the timeline range, click and drag the boundary lines.

Step 6 To do a live capture session:

a) Click **Start Live Capture** at the top-right corner to start a live capture session.

During a live capture session, data packets for the **Onboarding Events** and **RF Statistics** dashlets are collected.

b) Click **Stop Live Capture** to stop the live capture session.

c) View the running live capture sessions in the **Intelligent Capture Settings** window for clients.

Step 7 Use the **Onboarding Events** dashlet to view events that are associated with establishing a network connection:

Onboarding events dashlet	
Item	**Description**
All and Anomaly PCAP filter	Allows you to filter the onboarding events. Options are: • **All**: Displays all events. This is the default. • Anomaly PCAP: Filters for only anomaly events that have packets. **Note** If the client has issues joining the network, the word "PCAP" is displayed in red beside the specific event. If the client has no issues joining the network, the word "PCAP" is displayed in gray beside the specific event.
Export PCAP	You can download the packets for a range of specified events: **a.** Click **Export PCAP**. **b.** Specify the first and last events that you want to include in the PCAP. **c.** Click **Download PCAP** to start the download. **Note** Since heuristics are used to determine which packets belong to an event, packets from one minute before the first event and one minute after the last event are included in the download. This ensures that all relevant packets are in the downloaded PCAP. Each export is limited to the first 2000 packets, starting from the oldest timestamp.

Onboarding events dashlet	
Item	**Description**
List of Onboarding, Incomplete, and Anomaly Events	View the list onboarding, incomplete, and anomaly events in chronological order. Events are color-coded to indicate these details: : Successful onboarding event. : Incomplete event. : Anomaly event. **Note** An event with the word "PCAP" displayed beside it indicates that data packets for this event have been captured for download or analysis. You can click the parent event group to expand it and view the individual events for that group.
Event Details	You can click an event group or individual event to view these sections with further details: **Client Location**: Displays the map of the client location and the client's movement during the event. **Auto Packet Analyzer**: This section appears if a live capture, scheduled capture, or anomaly capture session has captured packets for the event. The word "PCAP" that displays next to the event indicates that the event has captured packets. The **Auto Packet Analyzer** section displays a graph with this information: • The packets (up to 100) surrounding the event are divided into two groups. Gray sections indicate packets that precede the start of an onboarding session. White sections indicate packets in the onboarding session. Deauthentication packets and unexpected patterns of packets are represented by red triangles. These are potentially significant packets that can degrade the client's onboarding experiences. You can download the packets by clicking **Download Packets** for further analysis. • Packet (from client or from AP) • Onboard packet stage identifier • Interpacket gap (ms) • RSSI (dBm) per packet • Associated AP **RF Statistics**: Displays charts with the RF statistic data for the 10-minute interval surrounding the event. The RF statistic data is composed of RSSI and SNR measurements in decibels, Rx average data rate and Rx last data rate, Tx packets and Rx packets, and Tx packet retry. **Note** If Anomaly Capture is enabled, the packets for anomaly events are captured even if a live or scheduled capture is not running.

Step 8 Use the **Client Location** dashlet to view the a floor map with this information:

- The location of the client and APs on the floor.
- Heatmap with the color intensity representing the strength of the coverage.
- The real-time location of the client on the floor map. If the client moves to another location, its movement is displayed.
- Client trail tracking with color-coded display of connectivity using the RF statistics: RSSI, SNR, data rate, throughput, and packet drop rate.

  The following colors on the map indicates the client's health:

  🟢: Good 🟠: Fair 🔴: Poor
- The tracking of the client for a one-minute intervals surrounding the time of the selected onboarding event.
- The replay, stop and start controls below the map can be used to control the viewing.

Note
The Client Location feature requires that CMX is integrated with Catalyst Center. For details, see the Integrate Cisco CMX for Wireless Maps, on page 431 chapter.

Step 9 Use the **RF Statistics** dashlet to view detailed RF information.

Four charts that display AP client statistics. For more information, see About client statistics, on page 391. The color-coded data contains this information:

- RSSI and SNR measurements in decibels.
- Rx average data rate (from the past 5 seconds) and Rx last data rate.
- Tx packets and Rx packets.
- Tx packet retry.

You can do these tasks in the charts:

- Hover your cursor over the chart to see the statistics for a particular time.
- Click and drag within the chart to zoom in on a time period. To change the view to the default, click the  icon.

Schedule an Onboarding Packet Capture session for a client device

You can schedule an onboarding packet capture session for a client device.

Onboarding Packet Capture sessions collect this data:

- Data packets for onboarding events and **RF Statistics** chart data (5-second samples) display in the **Client 360** > **Intelligent Capture** window. See Run an Onboarding Packet Capture live session for a client device, on page 391.
- Data for the charts and tables display in the **Device 360** > **Intelligent Capture** window. See View RF Statistics of an AP, on page 406 and View spectrum analysis data of an AP, on page 413.

Procedure

Step 1 From the main menu, choose **Assurance** > **Intelligent Capture Settings**.

The **Onboarding Packet Capture** window appears.

Step 2 Click + **Schedule Client Capture**.

Note
If an existing Onboarding Packet Capture task is incomplete, attempting to start a new packet capture session on the same wireless controllers fails because of the conflicting, incomplete task. To start a new task, either wait for the existing task to complete or discard it.

Step 3 In the **Schedule Client Capture** slide-in pane, do these steps:

a. From the **Select client devices** drop-down list, select the client devices.

b. From the **Duration** drop-down list, select the time duration of the Onboarding Packet Capture session.

The default duration is 30 minutes.

c. Check the check boxes next to the wireless controllers on which you want to enable Onboarding Packet Capture.

You can select up to three wireless controllers.

d. Click **Next**.

All Onboarding Packet Capture sessions display on the **Assurance** > **Intelligent Capture Settings** window in the **Onboarding Packet Capture** tab.

Step 4 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 64.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 64.

Step 5 On the **Tasks** window, monitor the task deployment.

Stop in-progress Onboarding Packet Capture sessions on a client device

You can stop an in-progress Onboarding Packet Capture session on a client device.

Procedure

Step 1 From the main menu, choose **Assurance** > **Intelligent Capture Settings**.

The **Onboarding Packet Capture** window appears..

Step 2 Under **In-progress Captures**, check the check boxes next to the wireless controllers that you want to stop running Onboarding Packet Capture sessions on.

Step 3 Click **Stop Capture**.

Full Packet Capture for a client device

About Full Packet Capture for a client device

Full Packet Capture allows you to capture network data and download the data as PCAP files, which can be viewed in Wireshark. For more information, see Run a Full Packet Capture session on a client device, on page 397.

Note "Client Data Packet Capture" is now rebranded as “Full Packet Capture”. While streamlining this nomenclature, you may see the former and rebranded names used in different collateral’s. However, "Client Data Packet Capture" and "Full Packet Capture" refer to the same feature.

For a complete list of supported access points, see Feature Matrix for Cisco Wireless Access Points.

Full Packet Capture Limitations

Full Packet Capture limitations include:

- Only one Full Packet Capture session can run at a time.
- As for all Intelligent Capture features, clocks must be synchronized between Catalyst Center and the Cisco Wireless Controller for Full Packet Capture to work. Ensure that the wireless controller is connected to a Network Time Protocol (NTP) server.
- Each Full Packet Capture session can capture up to 1 GB of rolling data. The 1 GB of data is broken into ten 100-MB files for faster downloads.

Run a Full Packet Capture session on a client device

You can run a Full Packet Capture session on a client device.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Client Health** tab.

The **Client Health** window is displayed.

Step 3 Open the **Client 360** window of a specific client by doing one of these tasks:

- In the **Client Devices** table, click the hyperlinked identifier or the MAC address of the device.

- In the **Search** field, enter one of these elements:
  - User ID (authenticated through Cisco ISE)
  - IP address
  - MAC address

A 360-degree view of the client device appears.

Step 4 In the **Client 360** window, click **Intelligent Capture**.

The **Intelligent Capture:** *Client Device* window appears.

Attention

If a ⚠ icon with the message **GRPC link is not ready (CONNECTING)** appears next to the client name, see Client or AP unable to send Intelligent Capture data to Catalyst Center, on page 418.

Step 5 Use the timeline slider for this functionality:

- **1 hour** drop-down list: Click the drop-down list and select a duration to set the range of the timeline. Options are **1 hour**, **3 hours**, and **5 hours**. The default is **1 hour**.
- **Timeline Slider**: The timeline slider determines the time window of all data displayed. To adjust the timeline to a different time window, click the < and > buttons to the desired time window. For more customization of the timeline range, click and drag the boundary lines.

  Note
  The timeline can display data from up to two weeks in the past.

Step 6 Click **Run Packet Capture**.

The **Run a Data Packet Capture** slide-in pane appears, and the **Onboarding Packet Capture** tab is selected by default.

Step 7 In the **Run a Data Packet Capture** slide-in pane, click the **Full Packet Capture** tab.

Note
If an existing Full Packet Capture task is incomplete, attempting to start a new packet capture session on the same wireless controllers fails because of the conflicting, incomplete task. To start a new task, either wait for the existing task to complete or discard it.

Step 8 From the **Duration** drop-down list, select the time duration of the packet capture.

The default duration is 30 minutes.

Step 9 Check the check boxes next to the wireless controllers that you want to enable Full Packet Capture on.

You can select up to three wireless controllers.

Step 10 Click **Next**.

Note
- All Full Packet Capture sessions are displayed under **Assurance** > **Intelligent Capture Settings** > **Full Packet Capture**.

- When a packet capture session is configured on Catalyst Center, any packet capture session that Catalyst Center is not aware of is removed (such as Full Packet Capture sessions that were directly configured on the wireless controller).

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 64.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 64.

Step 12 On the **Tasks** window, monitor the task deployment.

Note
Based on the duration of the task, Catalyst Center automatically runs enable and disable tasks for the Full Packet Capture session. To view the configuration preview of the enable or disable tasks, go to the **Tasks** window, open the task, and click **View Work Item Details**. If you don't view the configuration preview before the task completes, the option to preview will no longer be available.

Step 13 To download PCAP files from completed Full Packet Capture and OTA Packet Capture sessions, on the **Intelligent Capture:** *Client Device* window, click **Download**.

You can download files containing information on wireless data, which includes 802.11 files for packets moving between the AP and the client.

Note
Data packet captures are divided into separate 100-MB files. There is a 4-GB limit on the total size of all data packet capture files that reside on Catalyst Center. If the limit is exceeded, packet files are removed, starting with the oldest, until the total size falls below the 4-GB limit. Additionally, any data packet capture files that are more than 14 days old are removed, even if the total size limit has not been reached.

View Full Packet Capture history

Use this procedure to view the history of the full packet capture sessions, such as the time the first packet and the last data packet was captured, the total size of the captured data packets, and the type of packet.

Procedure

Step 1 From the main menu, choose **Assurance** > **Intelligent Capture Settings**.

The **Onboarding Packet Capture** window appears.

Step 2 Click the **Full Packet Capture** tab.

The **Full Packet Capture** window appears.

Step 3 Use the **Intelligent Capture Settings - Full Packet Capture** window to view this information:

Option	Description
Identifier	Displays the client's user ID or hostname. Click the user ID or hostname to open the **Intelligent Capture:** *Client Device* window.
MAC Address	Displays the MAC address of the client device.
Wireless Controller	Displays the name of the wireless controller.
First Packet Time	Displays the time the first data packet was captured.
Last Packet Time	Displays the time the last data packet was captured.
Total Size	Displays the total size of the captured data.
Currently Running	Displays whether the data packet capture is currently running.
Type of Packet	Displays the type of packet, for example, **Wired** or **Wireless**.
Duration	Displays the duration of the packet capture.
Last Start Time	Displays the last started time of the packet capture.
Configuration Status	Displays the configuration status of the devices.

OTA Sniffer Capture for a Wi-Fi band and channel

About OTA Sniffer Capture for a Wi-Fi band and channel

Catalyst Center allows you to perform OTA sniffer captures on up to four radios across two access points (APs). If a selected radio does not support the 'radio role sniffer' function, Catalyst Center automatically switches the AP from client-serving mode to dedicated sniffer mode. Otherwise, the 'radio role sniffer' is used to capture packets without interrupting client service.

Note If a static default route to gateway is not available, set a static route to 127.0.0.1

Run an OTA Sniffer Capture session on a Wi-Fi band and channel

You can run an OTA Sniffer Capture session on a Wi-Fi band and channel.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**

The **Overall** health dashboard appears.

Step 2 Click the **Client Health** tab.

The **Client Health** window appears.

Step 3 Open the **Client 360** window of a specific client by doing one of these tasks:

- In the **Client Devices** table, click the hyperlinked identifier or the MAC address of the device.
- In the **Search** field, enter one of these: user ID (authenticated through Cisco ISE), IP address, or MAC address.

Step 4 In the **Client 360** window, click **Intelligent Capture**.

The **Intelligent Capture:** *Client Device* window appears.

Attention

If a ⚠ icon with the message **GRPC link is not ready (CONNECTING)** appears next to the client name, see Client or AP unable to send Intelligent Capture data to Catalyst Center, on page 418.

Step 5 Use the timeline slider for this functionality:

- **1 hour** drop-down list: Click the drop-down list and select a duration to set the range of the timeline. Options are **1 hour** (default), **3 hours**, and **5 hours**.
- **Timeline Slider**: The timeline slider determines the time window of all data displayed. To adjust the timeline to a different time window, click the < and > buttons to the desired time window. For more customization of the timeline range, click and drag the boundary lines.

  Note
  The timeline can display data from up to two weeks in the past.

Step 6 Click **Run Packet Capture**.

The **Client Packet Capture** slide-in pane appears, and the **Onboarding Packet Capture** tab selects by default.

Step 7 In the **Client Packet Capture** slide-in pane, click the **OTA Sniffer** tab.

The floor map view appears by default.

Step 8 Select which APs to run radio or AP sniffing on by doing one the of these tasks:

- On the floor map, click the APs.
- Click the list icon in the view switcher, and then check the check boxes next to the APs.

  Catalyst Center shows only the radios that the OTA Sniffer supports.

Note
The OTA Sniffer captures Wi-Fi packets on a specific AP radio's band and channel. The same AP radio can't be reused for OTA if it was previously used for OTA in the last 15 minutes. To re-enable OTA on the same AP radio, you must wait until the **Device 360** window for that AP radio displays new client-serving data.

Step 9 Click **Next**.

Step 10 Select a band, radio, channel width, and channel from the respective drop-down lists.

Note
For APs that support dual-radios, run the OTA Sniffer data packet capture using either the primary or secondary radio accordingly:

- When dual-radio mode is disabled on the AP, use the primary radio to do the data packet capture.

- When dual-radio mode is enabled on the AP, use the secondary radio to do the data packet capture.

Step 11 Click **Next**.

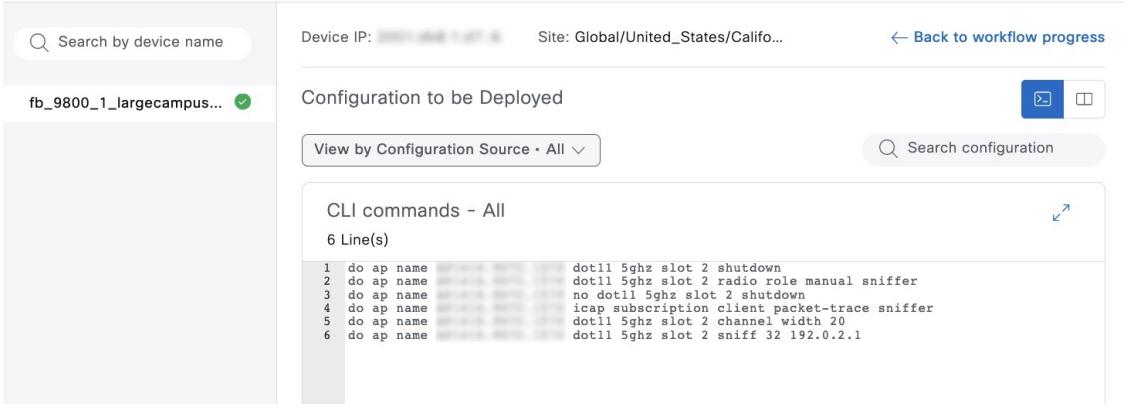
Step 12 If a **Warning** dialog box about changing radio modes and losing client connectivity displays, click **OK** to acknowledge and continue.

Step 13 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 64.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 64.

Note
When reviewing the device configurations under **Configuration to be Deployed** on the **Preview Configuration** window, the configured destination IP address is ignored at the device level. For example, in this figure, you can see the destination IP address is configured as 192.0.2.1. Instead of sending the packet data to the destination IP address, it is sent to Catalyst Center.



Step 14 On the **Tasks** window, monitor the task deployment.

Note

- Because the OTA Sniffer Capture duration is 15 minutes, Catalyst Center automatically runs enable and disable tasks. To view the configuration preview of the enable or disable tasks, go to the **Tasks** window, open the task, and click **View Work Item Details**. If you don't view the configuration preview before the task completes, the option to preview will no longer be available.
- All OTA Sniffer Capture sessions are displayed under **Assurance** > **Intelligent Capture Settings** > **OTA Sniffer**. OTA Sniffer data captures are divided into separate 500-MB files. There is a 15-GB limit on the total size of all OTA Sniffer Capture files that reside on Catalyst Center. If the limit is exceeded, packet files are removed, starting with the oldest, until the total size falls below the 15-GB limit. Additionally, any OTA sniffer capture files that are more than 24 hours old are removed, even if the total size limit has not been reached.

Download PCAP files from a completed OTA Sniffer Capture session

You can download the PCAP files from a completed OTA Sniffer Capture session from one of these windows:

- **Device 360**: When you download the PCAP files from the **Device 360** window, only the data from the completed OTA Sniffer Capture sessions for that specific device are downloaded.
- **Client 360**: When you download the PCAP files from the **Client 360** window, the data from both the completed Full Packet Capture and OTA Sniffer Capture sessions for that specific client are downloaded.
- **Intelligent Capture Settings**: Under the **OTA Sniffer Capture** > **Completed Captures** tabs on the **Intelligent Capture Settings** window, only the data of selected APs from the completed OTA Sniffer Capture sessions are downloaded.

Use this procedure to download the PCAP files from the **Intelligent Capture Settings** window.

Procedure

Step 1 From the main menu, choose **Assurance** > **Intelligent Capture Settings**.

Step 2 On the **Intelligent Capture Settings** window, click the **OTA Sniffer Capture** tab.

On the **OTA Sniffer Capture** window, the **In-progress Captures** tab is selected by default.

Step 3 Click the **Completed Captures** tab.

The **Completed Captures** table lists the completed OTA Sniffer Captures sessions.

Step 4 Under the **Download** column, click the down arrow icon corresponding to the relevant completed capture session to download its PCAP files.

The data packet files contain information on wireless data, which includes 802.11 files for packets moving between the AP and the client.

Note
OTA Sniffer Capture data packet files are divided into separate 500-MB files. There is a 15-GB limit on the total size of all OTA Sniffer Capture files stored on Catalyst Center. If this limit is exceeded, the oldest packet files are removed until the total size falls below the 15-GB threshold. Additionally, any OTA Sniffer Capture files older than 24 hours are automatically deleted, even if the total size limit has not been reached.

AP Statistics Capture for APs and wireless controllers

About AP Statistics Capture for APs and wireless controllers

The Intelligent Capture feature allows you to enable or disable AP Statistics Capture on specific APs and capable wireless controllers. When it's enabled, this data is captured:

- AP radio and WLAN statistics, which appear in the **RF Statistics** tab of the **Device 360** > **Intelligent Capture** window.
- AP Client statistics (30-second samples), which are displayed in the **RF Statistics** area of the **Client 360** > **Intelligent Capture** window for all clients associated with the selected APs.

Enable or disable AP Statistics Capture on a specific AP

You can enable and manage one or more APs to capture AP Statistics data, including AP radio statistics, WLAN statistics, and AP Client statistics. Catalyst Center can support up to 1000 APs for AP Statistics Capture.

Procedure

Step 1 From the main menu, choose **Assurance** > **Intelligent Capture Settings**.

Step 2 On the **Intelligent Capture Settings** window, click the **Access Point** tab.

On the **Access Point** window, the **AP Stats Capture** tab is selected by default.

Step 3 Under **Configure AP Enablement**, click **Specific - select specific APs and enable** and then click **Get Started**.

The left pane displays the left tree hierarchy, and the right pane displays the default view because no floor is selected.

Step 4 In the left pane, expand **Global** and drill down to the site > building > floor.

In the right pane, the **Disabled APs** tab is selected, and a list of disabled APs on the selected floor appears.

Note
If you want to enable or disable AP Statistics Capture on all APs managed by a wireless controller and the **Global - enable or disable capable WLCs** radio button is dimmed, you must first disable this feature on all enabled APs listed under the **Enabled APs** tab.

Step 5 Do one of these tasks:

- To enable AP Statistics Capture on specific APs, continue to Step 6, on page 404.
- To disable AP Statistics Capture on specific APs, click the **Enabled APs** tab and continue to Step 6, on page 404.

Step 6 Check the check boxes next to the APs that you want to enable or disable AP Statistics Capture on.

Step 7 Enable or disable AP Statistics Capture on the selected APs.

- To enable AP Statistics Capture on the selected APs, click **Enable**.
- To disable AP Statistics Capture on the selected APs, click **Disable**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 64.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 64.

Step 9 On the **Tasks** window, monitor the task deployment.

Enable or disable AP Statistics Capture on a wireless controller

You can enable or disable AP Statistics Capture on capable wireless controllers. You can enable up to three wireless controllers. When this feature is enabled, all APs managed by the wireless controller capture AP Statistics data, including AP radio statistics, WLAN statistics, and AP Client statistics.

Catalyst Center can support up to 1000 APs for AP Statistics Capture.

Procedure

Step 1 From the main menu, choose **Assurance** > **Intelligent Capture Settings**.

Step 2 On the **Intelligent Capture Settings** window, click the **Access Point** tab.

On the **Access Point** window, the **AP Stats Capture** tab is selected by default.

Step 3 Under **Configure AP Enablement**, click **Global - enable or disable capable WLCs** and then click **Get Started**.

Step 4 In the **Warning** dialog box, click **Yes** to continue.

Note
If you want to enable or disable AP Statistics Capture on specific APs and the **Specific - select specific APs and enable** radio button is dimmed, you must first disable this feature on all enabled wireless controllers.

The **AP Stats Capture** tab is selected, and the table lists capable wireless controllers. Under the **Configuration Status** column, one of these statuses appears for each wireless controller:

- **Success**: Catalyst Center successfully enabled AP Statistics Capture on the wireless controller.
- **Not Configured**: Catalyst Center has not enabled AP Statistics Capture on the wireless controller.
- **In Progress**: Catalyst Center is enabling AP Statistics Capture on the wireless controller.
- **Failed**: Catalyst Center failed to enabled AP Statistics Capture on the wireless controller because the wireless controller didn't accept the configuration.

  Tip
  If the **Configuration Status** is **Failed**, disable AP Statistics Capture on the wireless controller and then re-enable it on the wireless controller.

- **Unknown**: Catalyst Center enabled AP Statistics Capture on the wireless controller, but Catalyst Center doesn't know the device status.

  Tip
  If the **Configuration Status** is **Unknown**, disable AP Statistics Capture on the wireless controller and then re-enable it on the wireless controller.

Step 5 Check the check boxes next to the wireless controllers that you want to enable or disable AP Statistics Capture on.

Step 6 Enable or disable AP Statistics Capture on all APs managed by wireless controllers.

- To enable AP Statistics Capture on all APs managed by wireless controllers, click **Enable**.
- To disable AP Statistics Capture on all APs managed by wireless controllers, click **Disable**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 64.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 64.

Step 8 On the **Tasks** window, monitor the task deployment.

View incompatible APs for AP Statistics Capture

You can view incompatible APs for AP Statistics Capture only when you choose **Specific - select specific APs and enable** for the type of AP enablement.

Procedure

Step 1 From the main menu, choose **Assurance** > **Intelligent Capture Settings**.

Step 2 On the **Intelligent Capture Settings** window, click the **Access Point** tab.

On the **Access Point** window, the **AP Stats Capture** tab is selected by default.

Step 3 Under **Configure AP Enablement**, click **Specific - select specific APs and enable** and then click **Get Started**.

The left pane displays the left tree hierarchy, and the right pane displays the default view because no floor is selected.

Step 4 In the left pane, expand **Global** and drill down to the site > building > floor.

In the right pane, the **Disabled APs** tab is selected, and a list of disabled APs on the selected floor appears.

Step 5 Click the **Not-Ready APs** tab.

Note
Incompatible APs have these conditions:

- The operation mode is not set to `local` or `FlexConnect`.
- The OS release that is installed on the AP is not compatible. For more information about the wireless controllers and APs that support Intelligent Capture (iCAP), see Feature Matrix for Cisco Wireless Access Points.

View RF Statistics of an AP

You can view RF statistics of a specific AP using this procedure.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Network Health** tab.

The **Network Health** window appears.

Step 3 Do one of these tasks:

- From the **Network Devices** dashlet, click the device name (hyperlinked identifier) for the AP to view the details for the AP.
- In the **Search** field (located at the top-right corner), enter the device name, IP address, or MAC address.

A 360° view of the AP appears.

Step 4 In the **Device 360** window, click **Intelligent Capture** at the top-right corner.

The **Intelligent Capture:** *AP Name* window appears.

Attention

If a ⚠ icon with the message **GRPC link is not ready (CONNECTING)** appears next to the AP name, see Client or AP unable to send Intelligent Capture data to Catalyst Center, on page 418.

Step 5 Click the **RF Statistics** tab to view details about RF statistics.

Note
If **AP Stats Capture** has not been enabled, enable it. See Enable or disable AP Statistics Capture on a specific AP, on page 404 or Enable or disable AP Statistics Capture on a wireless controller, on page 405.

Step 6 Use the timeline to view the RF statistics for a given time and specify the scope of the data:

Timeline slider	
Item	**Description**
1 hour drop-down list	Click the drop-down list and select a duration to set the range of the timeline. Options are **1 hour** (the default), **3 hours**, and **5 hours**.
Timeline Slider	The timeline slider determines the time window of all data displayed. The timeline slider is color-coded to display the health of the AP. You can hover your cursor at a specific time to see details such as the device health score, system resources, and data plane. To adjust the timeline to a different time window, click the < and > buttons to the desired time window. For more customization of the timeline range, click and drag the boundary lines.

Step 7 Use the radio frequency selector under the timeline to filter the data in the dashlets based on the frequency bands.

Click the drop-down list and select **Radio 0 (2.4 GHz or 5 GHz)**, **Radio 1 (5 GHz)**, or **Radio 2 (6 GHz)** (depending on the number of radios supported).

Step 8 Use the dashlets to view the RF statistics details:

Note
You can do these tasks in the charts that appear in the dashlets:

- Hover your cursor over the charts to view details.

- Click and drag within the chart to zoom in on a period. To change the view to the default, click .
- Click the color-coded data types below the chart to disable or enable the data type that appear in the chart.

Dashlets	Description
Clients dashlet	Displays the number of clients using the AP. The data source is from the AP WLAN statistics.
Top Clients with Tx Failed Packets by SSID dashlet	Displays the list of SSIDs in the table. The data source for the table is from the AP WLAN statistics. The data source for the bar chart is from AP client statistics. Select an SSID to see the top clients with transmit failed packets for that SSID.
Channel Utilization dashlet	Displays the channel utilization percentage used by the AP and other wireless and non-wireless devices. The data source for the bar chart is from AP Radio Statistics.
Channel Utilization by this Radio dashlet	Displays the current channel utilization percentage used by the AP and a list of SSIDs, the number of clients connected to it, and the number of packets sent or received over the last 15 minutes for its clients. The data source for the table is from the AP WLAN statistics. The data source for the circle chart is from AP radio statistics.
Frame Count dashlet	Displays the number of management and data frames. The data source is from the AP radio statistics.
Frame Errors dashlet	Displays the number of transmit and receive errors. The data source is from the AP radio statistics.
Tx Power and Noise Floor dashlet	Displays the transmit power and noise floor. The data source is from the AP radio statistics.
Multicast/Broadcast Counter dashlet	Displays the multicast and broadcast counts for each SSID. The data source is from the AP WLAN statistics.

Anomaly Capture for APs and wireless controllers

About Anomaly Capture for APs and wireless controllers

The Intelligent Capture feature allows you to enable or disable Anomaly Capture on a specific AP or wireless controller. When it's enabled, all anomaly onboarding events for all clients that are associated with the selected APs are captured for download or display.

AP Capture limitation

There is a 1.05-GB limit on the total size of all anomaly triggered packet files that reside on Catalyst Center. If the limit is exceeded, packet files are removed, starting with the oldest, until the total size falls below the 1.05-GB limit.

Enable or disable Anomaly Capture on a specific AP

You can enable and manage one or more APs to capture anomaly onboarding events of all clients that are associated with one or more APs. Enabling Anomaly Capture ensures that all anomaly onboarding events for all clients associated with the selected APs are captured for download and display. Disabling Anomaly Capture ensures that all anomaly onboarding events for all clients associated with the selected APs are not captured for download and display.

Procedure

Step 1 From the main menu, choose **Assurance** > **Intelligent Capture Settings**.

Step 2 On the **Intelligent Capture Settings** window, click the **Access Point** tab.

On the **Access Point** window, the **AP Stats Capture** tab is selected by default.

Step 3 Click the **Anomaly Capture** tab.

Step 4 Under **Configure AP Enablement**, click the **Specific - select specific APs and enable** and then click **Get Started**.

The left pane displays the left tree hierarchy, and the right pane displays the default view because no floor is selected.

Note
If you want to enable or disable Anomaly Capture on all APs managed by a wireless controller and the **Global - enable or disable capable WLCs** radio button is dimmed, you must first disable this feature on all enabled APs listed under the **Enabled APs** tab.

Step 5 In the left pane, expand **Global** and drill down to the site > building > floor.

In the right pane, the **Disabled APs** tab is selected, and a list of disabled APs on the selected floor appears.

Note
If a previous attempt to enable the AP failed, an error message appears in the **Config Status** column.

Step 6 Do one of these tasks:

- To enable Anomaly Capture on specific APs, continue to Step 7, on page 409.
- To disable Anomaly Capture on specific APs, click the **Enabled APs** tab and then continue to Step 7, on page 409.

Step 7 Check the check boxes next to the APs that you want to enable or disable Anomaly Capture on.

Step 8 Enable or disable Anomaly Capture on the selected APs.

- To enable Anomaly Capture on the selected APs, click **Enable**.
- To disable Anomaly Capture on the selected APs, click **Disable**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 64.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 64.

Step 10 On the **Tasks** window, monitor the task deployment.

Enable or disable Anomaly Capture on a wireless controller

You can enable or disable Anomaly Capture on capable wireless controllers, and you can enable up to three wireless controllers. Enabling Anomaly Capture ensures that all anomaly events of clients associated with APs managed by the wireless controller are captured for download and display. Disabling Anomaly Capture ensures that all anomaly onboarding events of clients associated with APs managed by the wireless controller are not captured for download and display.

Procedure

Step 1 From the main menu, choose **Assurance** > **Intelligent Capture Settings**.

Step 2 On the **Intelligent Capture Settings** window, click the **Access Point** tab.

On the **Access Point** window, the **AP Stats Capture** tab is selected by default.

Step 3 Click the **Anomaly Capture** tab.

Step 4 Under **Configure AP Enablement**, click **Global - enable or disable capable WLCs** and then click **Get Started**.

Step 5 In the **Warning** dialog box, click **Yes** to continue.

Note
If you want to enable or disable Anomaly Capture on specific APs and the **Specific - select specific APs and enable** radio button is dimmed, you must first disable this feature on all enabled wireless controllers.

The **Anomaly Capture** tab is selected, and the table lists capable wireless controllers. Under the **Configuration Status** column, one of these statuses appears for each wireless controller:

- **Success**: Catalyst Center successfully enabled Anomaly Capture on the wireless controller.
- **Not Configured**: Catalyst Center has not enabled Anomaly Capture on the wireless controller.
- **In Progress**: Catalyst Center is enabling Anomaly Capture on the wireless controller.
- **Failed**: Catalyst Center failed to enabled Anomaly Capture on the wireless controller because the wireless controller didn't accept the configuration.

  Tip
  If the **Configuration Status** is **Failed**, disable Anomaly Capture on the wireless controller and then re-enable it on the wireless controller.

- **Unknown**: Catalyst Center enabled Anomaly Capture on the wireless controller, but Catalyst Center doesn't know the device status.

  Tip
  If the **Configuration Status** is **Unknown**, disable Anomaly Capture on the wireless controller and then re-enable it on the wireless controller.

Step 6 Check the check boxes next to the wireless controllers that you want to enable or disable Anomaly Capture on.

Step 7 Enable or disable Anomaly Capture on all APs managed by the selected wireless controllers.

- To enable Anomaly Capture on all APs managed by the selected wireless controllers, click **Enable**.

  If the **Warning** dialog box (about not being able to make any further changes until the AP enablement is complete) displays, click **Yes** to continue.

- To disable Anomaly Capture on all APs managed by the selected wireless controllers, click **Disable**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 64.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 64.

Step 9 On the **Tasks** window, monitor the task deployment.

View incompatible and supported APs for Anomaly Capture

You can view incompatible and supported APs for Anomaly Capture only when you select **Specific - select specific APs and enable** for the type of AP enablement.

Procedure

Step 1 From the main menu, choose **Assurance** > **Intelligent Capture Settings**.

Step 2 On the **Intelligent Capture Settings** window, click the **Access Point** tab.

On the **Access Point** window, the **AP Stats Capture** tab is selected by default.

Step 3 Click the **Anomaly Capture** tab.

Step 4 Under **Configure AP Enablement**, click the **Specific - select specific APs and enable** and then click **Get Started**.

The left pane displays the left tree hierarchy, and the right pane displays the default view because no floor is selected.

Step 5 In the left pane, expand **Global** and drill down to the site > building > floor.

In the right pane, the **Disabled APs** tab is selected and a list of disabled APs on the selected floor appears

Step 6 To view incompatible APs for Anomaly Capture, click the **Not-Ready APs** tab.

Note
Incompatible APs have these conditions:

- The operation mode is not set to `local` or `FlexConnect`.
- The OS release that is installed on the AP is not compatible. For more information about the wireless controllers and APs that support Intelligent Capture (iCAP), see Feature Matrix for Cisco Wireless Access Points.

Step 7 To display the list of APs that support Intelligent Capture, click the information icon next to the **Not-Ready APs** tab.

Spectrum Analysis for APs

About Cisco AP functionality during spectrum analysis

This FRA radio operates on 2.4 GHz, but can be assigned to operate on 5 GHz. Its mode can be changed to differ from the APs operational mode. When you configure the APs FRA radio to operate in 5 GHz, no client radios can operate in the 2.4-GHz band.

For a complete list of supported access points, see Feature Matrix for Cisco Wireless Access Points.

APs with 2 radio slots	APs with 3 radio slots
Aironet 1560 APs	Catalyst 9120 AP
Catalyst IW6300 Heavy Duty Series APs	Catalyst 9130 APs
Catalyst IW6300 Heavy Duty Series APs	**Note** If data packet capture is running, radio slots 0 and 1 are enabled. If data packet capture is not running, radio slot 2 is enabled. AP spectrum analysis data is not displayed for the 2.4-GHz channel band. Also, if there is no AP radio serving the 2.4-GHz band, the **Radio Mode** and **Channel** fields are empty. This occurs if the FRA radio is set to operate in 5 GHz and packet capture is enabled.

Start a spectrum analysis session on an AP

You can start a spectrum analysis session on a specific AP using this procedure.

Note
- The duration of a spectrum analysis session is 10 minutes.
- The maximum number of concurrent spectrum analysis sessions is 10.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

Step 2 Click the **Network Health** tab.

Step 3 Do one of these tasks:

- From the **Network Devices** dashlet, click the device name (hyperlinked identifier) for the AP to view the details for the AP.
- In the **Search** field (located at the top-right corner), enter the device name, IP address, or MAC address.

A 360° view of the AP appear.

Step 4 In the **Device 360** window, click **Intelligent Capture** at the top-right corner.

The **Intelligent Capture:** *AP Name* window appears.

Attention

If a ⚠ icon with the message **GRPC link is not ready (CONNECTING)** is displayed next to the AP name, see Client or AP unable to send Intelligent Capture data to Catalyst Center, on page 418.

Step 5 Click the **Spectrum Analysis** tab.

Step 6 Click **Start Spectrum Analysis**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 64.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 64.

Step 8 On the **Tasks** window, monitor the task deployment.

Note
Based on the 10-minute spectrum analysis duration, Catalyst Center automatically runs enable and disable tasks for the capture session. To view the configuration preview of the enable and disable tasks, go to the **Tasks** window, open the task, and click **View Work Item Details**. If you don't view the configuration preview before the task completes, the option to preview is no longer available when it completes.

View spectrum analysis data of an AP

You can view the spectrum analysis data of an AP using this procedure.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

Step 2 Click the **Network Health** tab.

Step 3 Do one of these tasks:

- From the **Network Devices** dashlet, click the device name (hyperlinked identifier) for the AP to view the details for the AP.
- In the **Search** field (located at the top-right corner), enter the device name, IP address, or MAC address.

A 360° view of the AP appears.

Step 4 In the **Device 360** window, click **Intelligent Capture** at the top-right corner.

The **Intelligent Capture:** *AP Name* window appears.

Attention

If a ⚠ icon with the message **GRPC link is not ready (CONNECTING)** appears next to the AP name, see Client or AP unable to send Intelligent Capture data to Catalyst Center, on page 418.

Step 5 Click the **Spectrum Analysis** tab.

Step 6 Use the timeline to view the spectrum analysis data for a given time and specify the scope of the data to display:

Timeline slider	
Item	**Description**
1 hour drop-down list	Click the drop-down list and select a duration to set the range of the timeline. Options are **1 hour** (the default), **3 hours**, and **5 hours**.
Timeline Slider	The timeline slider determines the time window of data that is displayed. The timeline slider is color-coded to display the health of the AP. You can hover your cursor at a specific time to see the details, such as the device health score, system resources, and data plane. For spectrum analysis, the time range is set to a 5-minute window. To adjust the timeline to a different time window, click the < and > buttons to the desired time window. **Note** The timeline can display data from up to two weeks in the past. Click and drag the boundary lines to view data for a specific time.

Step 7 Use the radio frequency selector under the timeline to filter the data in the charts based on the frequency bands. Click **2.4 GHz**, **5 GHz**, or **6 GHz**.

Note
If **Radio Mode** and **Channel** (above the **Spectrum Analysis** charts) do not display any data, this indicates that the AP has no radios operating on the selected band. This occurs when an AP has both the client serving radios operating on **5 GHz**, while the radio frequency selector is set to **2.4 GHz**.

For more details, see About Cisco AP functionality during spectrum analysis, on page 412.

Step 8 Use the **Spectrum Analysis** charts for this functionality:

Spectrum analysis charts	
Item	**Description**
Top chart (Persistence)	This chart provides in real time the amplitude (power) and the channel frequency for each heard signal in the RF environment. The X axis represents the amplitude and the Y axis represents the channel frequency. The colors in the chart represent how many signals are heard at the same amplitude and channel frequency within the selected 5-minute time period: • Blue indicates a low number of overlapping signals (or signals heard at the same amplitude and frequency). • Red indicates a high number of overlapping signals. The intensity of the color increases (from blue > green > yellow > orange > red) as more signals are heard. As the lines in the chart overlap and intersect, they change color. The transparency of the colors represents the age of the signal data, with older data being more transparent. To view the RF environment in real time, click **Realtime FFT** (Fast Fourier Transform) to enable it. Enabling Realtime FFT limits the persistence chart to display "one" most recent data stream, rather than a collection of data streams from a 5-minute time period. To zoom in and view data for a specific range of channels, click and drag your mouse to select the range. The chart refreshes and displays data for the specific channels that you selected. To zoom out and view the entire chart, click the magnifying glass on the top-right corner.
Bottom chart (Waterfall)	This chart provides a time-wise interpretation of data. The chart provides the same information as the Persistence chart but in a different format. The X axis shows the time and the Y axis shows the channel frequency. The lines in the chart represent the exact order in which the events have occurred, which can enable you to troubleshoot the root cause if a problem occurs. The colors in the chart represent the amplitude. Blue indicates a low value (-100 dBm) and red indicates a high value (-20 dBm).

Step 9 Use the **Interference and Duty Cycle** chart to view:

- Detected interference and its severity:
  - Interference is plotted as a circle where the radius represents the bandwidth of the interference. The X axis represents the frequency in which the interference was heard on and the Y axis represent the severity.
  - Severity measures the impact of the interference and the range. Range is from 0, which indicates no impact, to 100, which indicates a huge impact.
  - The interference type is determined by its RF signature, which is identified by Cisco CleanAir Technology.
- The duty cycle of each channel.

Packet capture for wired client devices

To help troubleshoot a wired client device's connectivity or traffic issues, you can initiate a packet capture from Assurance to collect packet data from the relevant switch port.

Prerequisites

Before you start a wired packet capture, make sure that:

- The **Automation - Intelligent Capture** package is installed.
- The wired client is connected to a Cisco Catalyst 9200, 9300, 9400, 9500, or 9600 series switch.
- The switch is running Cisco IOS XE 17.9 or later.
- You know which wired client or switch port you want to troubleshoot.
- Another wired packet capture is not currently active on the same device.

Limitations

Keep these limitations in mind when you run a packet capture on a wired client device:

- Only one wired packet capture can be active on a device at a time.
- Capture retention is not based on a fixed time period alone.
- A packet capture of a wired client device is configured to be linear, with a 100 MB buffer. When the buffer is full, the switch stops capturing packets. At this point:
  1. Catalyst Center stops the capture session.
  2. The content of the switch's buffer is sent to Catalyst Center.
  3. Catalyst Center saves the packet capture to a PCAP file and makes it available for download.
- Older capture files may be removed when storage or buffer capacity have been exhausted.

Warning Download packet capture files promptly if you need to keep them. Catalyst Center may remove older files automatically.

Run a packet capture on a wired client device

Complete these steps to run a packet capture on a wired client device that is managed by Catalyst Center.

Only one packet capture can run on a wired device at a time. If a capture is already running, you must stop it before you can start another capture on the same device.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Network** tab.

The **Network** window is displayed.

Step 3 Open the **Device 360** window of a specific device by clicking its hyperlinked identifier in the **Network Devices** table.

A 360-degree view of the device appears.

Step 4 In the **Tools** section, locate the **Intelligent Packet Capture** field and click **Start**.

The **Intelligent Packet Capture** slide-in pane opens.

Step 5 Complete the wizard, noting that values are already set for the **Location** and **Connected Network Device** fields:

a) Choose the port you want to use from the drop-down list.

b) Specify the packet capture's duration (from one to 60 minutes).

c) (Optional) Enter a filter to limit the traffic that is collected.

For more information, see Configure a packet capture filter, on page 417.

d) Click **Next**.

Note
A window opens that links to both a video and documentation that describe the **Visibility and Control of Configurations** feature. Click **Close** to proceed.

e) Choose a deployment option:

- If you choose **Now or Later**, complete the steps described in Deploy your device configurations now or later, on page 64.
- If you choose **Preview and Deploy**, complete the steps described in Preview and deploy your device configurations, on page 64.

After the capture starts, Assurance submits the configuration to the switch and runs the capture in the background.

Configure a packet capture filter

Use a filter to reduce the amount of traffic that Catalyst Center collects during a packet capture of a wired client device and focus on the packets that are relevant to the issue you are troubleshooting. For example, the filter `ipv4 any host 1.1.1.1` captures all packets with destination IP address 1.1.1.1.

Packet capture filters for wired client devices currently support:

- IPv4 traffic
- IPv6 traffic
- Source-based matching
- Destination-based matching
- Protocol-based matching

Filtering capabilities are restricted to inline filters and do not support ACL-based filtering.

Stop a running capture

Complete these steps if you want to stop an active packet capture on a wired client device.

Procedure

Step 1 From the main menu, choose **Assurance** > **Intelligent Capture Settings**.

Step 2 Click **Wired Packet Capture**.

Step 3 Click **Stop** for the packet capture you want to stop.

Download a completed packet capture

Complete these steps to download a specific packet capture for a wired client device.

Procedure

Step 1 From the main menu, choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Network** tab.

The **Network** window is displayed.

Step 3 Open the **Device 360** window for the relevant client device by clicking its hyperlinked identifier in the **Network Devices** table.

A 360-degree view of the device appears.

Step 4 In the **Tools** section, locate the **Intelligent Packet Capture** field and click **Download**.

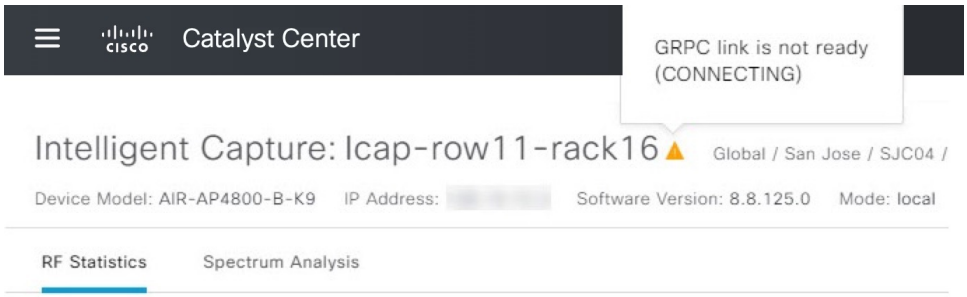
Step 5 Review the list of captures that are available for the switch.

Step 6 Select the capture that you want to download, then click **Download**.

Troubleshoot Intelligent Capture

Client or AP unable to send Intelligent Capture data to Catalyst Center

Problem: Client or access point is unable to send Intelligent Capture data to Catalyst Center. The warning (⚠) icon appears with the message **GRPC link is not ready (CONNECTING)**:



Background: In order for APs to send Intelligent Capture data to Catalyst Center, the Intelligent Capture port number on the Cisco Catalyst 9800 Series Wireless Controller or Cisco Wireless Controller must be set to 32626. Typically, when the Catalyst 9800 Series Wireless Controller or wireless controller is discovered by Catalyst Center, the port number is automatically set to 32626.

However, there are some upgrade paths for Catalyst Center that can cause the port number from being properly set.

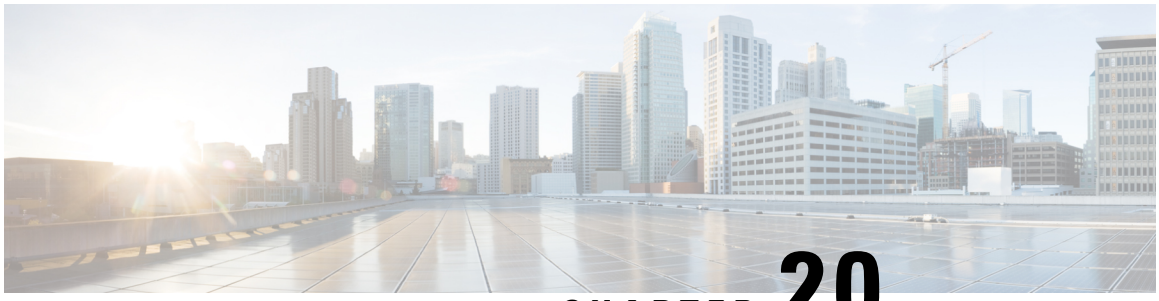
Solution: To resolve this issue:

1. Check that the Catalyst 9800 Series Wireless Controller or wireless controller has the Intelligent Capture server port number is set to 32626.
2. If the port number is not set to 32626, manually set it.

Troubleshoot wired packet capture issues

If you have trouble using the wired packet capture feature:

- Verify that the client device is a supported switch and has a supported Cisco IOS software release.
- Confirm that the wired client is connected to the right device and port.
- Ensure that you selected the correct interface.
- If you are unable to start a new capture for a client device, check whether another wired capture is already active on that device.
- If the capture does not include the expected traffic, review the filter expression and enter a broader filter.
- If a capture is no longer available for download, it may have been removed by buffer rotation.



CHAPTER 20

Manage SSID Monitoring Settings

- About SSID monitoring, on page 421
- Configure SSID monitoring settings, on page 422
- View the provisioning status for SSID monitoring, on page 422

About SSID monitoring

By default, Cisco Catalyst Assurance monitors and collects telemetry data about all SSIDs. However, there might be scenarios where you don't want to monitor all the SSIDs in your network. For example, when providing guest or public Wi-Fi services as in retail, transportation, or hospitality use cases, user counts can be very high. In such scenarios, you might want to turn off monitoring for these SSIDs, while continuing to collect rich data for corporate SSIDs from the same infrastructure.

You can enable or disable SSID monitoring for specific SSIDs without impacting the SSID configuration or wireless connection to these SSIDs. There's no impact on the SSID functionality in APs. Wireless clients continue to connect to these SSIDs and all other SSIDs, as has been configured. Clients on monitored SSIDs continue to have detailed data available on the **Client 360** window.

When an SSID isn't monitored, Cisco Catalyst Assurance doesn't collect its client data. So, detailed data and charts aren't available for these clients on the **Client 360** window. Also, other data such as client health, client-specific issues, and intelligent capture aren't available for these clients. In addition, the dashlets on the **Client Health** window don't include data from clients in unmonitored SSIDs.

Note SSID monitoring is not supported on Cisco AireOS Wireless Controllers. In Cisco AireOS Wireless Controllers, Catalyst Center drops the telemetry data for the SSIDs for which monitoring is disabled.

From the main menu, choose **Assurance** > **SSID Monitoring Settings** to view the **SSID Monitoring** window, from **SSID Monitoring** window, you can do these tasks:

- View SSID monitoring settings.
- Enable or disable SSID monitoring for specific SSIDs. For more information, see Configure SSID monitoring settings, on page 422.
- View and manage the provisioning request for the configured SSID monitoring action. For more information, see View the provisioning status for SSID monitoring, on page 422.

Configure SSID monitoring settings

By default, all SSIDs are monitored. However, you can disable and re-enable monitoring on one or more SSIDs at any time. Use this procedure to update the SSID monitoring settings.

Procedure

Step 1 From the main menu, choose **Assurance** > **SSID Monitoring Settings**.
The **SSID Monitoring** window opens and lists your SSIDs.

Step 2 (Optional) To narrow down your list of SSIDs, click the filter icon ( ) and enter values in any of the active fields (**Network Name (SSID)**, **Monitoring Status**, **Action**, or **Controller Config Status**).

Use the filter to exclude the SSIDs that you don't want to view or that you aren't troubleshooting. For example, you might not want to view the SSIDs that were created for testing, internal IT purposes, or guest SSIDs, such as those in an airport or subway.

Step 3 In the **Action** column, click the corresponding **Disable** or **Enable** option for an SSID.

Step 4 In the slide-in pane, do these steps:

a) Decide whether you want to provision the SSID monitoring changes now, schedule it for later, or create a preview that you can use later to deploy the settings on selected devices.
b) In the **Task Name** field, enter a name for the task.
c) Click **Apply**.

What to do next

To view the status of the scheduled SSID monitoring tasks, in the **SSID Monitoring** window, click **Activity Page**. Alternatively, click the menu icon and choose **Activities** > **Tasks**.

If you chose **Generate Preview**, to view the work item's status, click the menu icon and choose **Activities** > **Tasks**.

View the provisioning status for SSID monitoring

Use this procedure to view the provisioning status for SSID monitoring settings:

Procedure

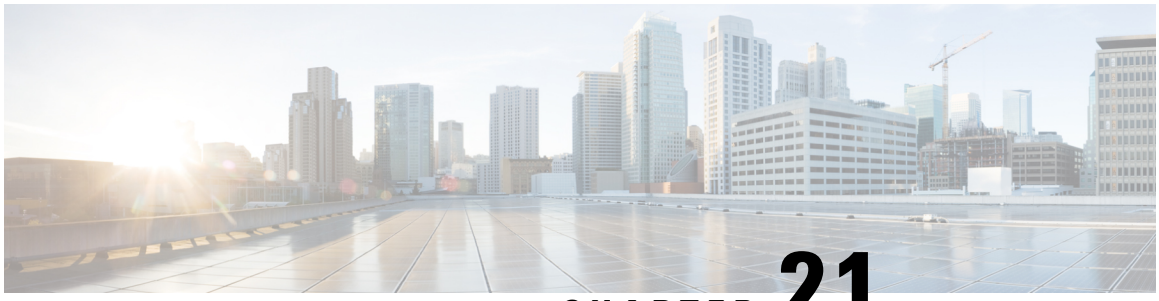
Step 1 From the main menu, choose **Assurance** > **SSID Monitoring Settings**.
The **SSID Monitoring** window opens.

Step 2 Click the required SSID name in the table.
The resulting slide-in pane displays the status of the provisioning request for SSID monitoring of the SSID.

Provisioning status	Description
Configuring	Indicates that the wireless controller is being configured with the SSID monitoring action.
Not Started	Indicates that the wireless controller isn't yet configured with the SSID monitoring action, but that the configuration will start soon.
Pending	Indicates that the SSID monitoring action is queued, and the wireless controller will be configured soon.
Success	Indicates that the wireless controller is provisioned with the SSID monitoring action.
Failed	Indicates that the wireless controller isn't provisioned with the SSID monitoring action.
Not Applicable	Indicates that the wireless controller is running software that doesn't support disabling the telemetry. Catalyst Center drops the telemetry data for the SSID.

What to do next

If the provisioning status for an SSID is **Failed** and you want to try to provision the wireless controller again, click **Retry Failed Configuration**.



CHAPTER 21

Trace the Path of a Device

- About path trace, on page 425
- Path trace limitations, on page 425
- Do a path trace, on page 428

About path trace

You can do a path trace between two nodes in your network—a specified source device and a specified destination device. The two nodes can be a combination of wired or wireless hosts or Layer 3 interfaces or both. In addition, you can specify the protocol that the Catalyst Center controller should use to establish the path trace connection, either TCP or UDP.

When you initiate a path trace, the Catalyst Center controller reviews and collects network topology and routing data from the discovered devices. It then uses this data to calculate a path between the two hosts or Layer 3 interfaces, and displays the path in a path trace topology. The topology includes the path direction and the devices along the path, including their IP addresses. The display also shows the protocol of the devices along the path (**Switched**, **STP**, **ECMP**, **Routed**, **Trace Route**) or other source type.

Path trace limitations

Path trace has these limitations and restrictions.

- Path trace from a third-party device in Catalyst Center is not supported.
- Path trace between a fabric client and a nonfabric client is not supported.
- Path trace between two fabric clients over multi virtual routing and forwarding (VRF) virtual networks (VNs) is not supported.
- Path trace between two fabric clients over multi sites (domains) is not supported.
- Clients connected in the same fabric and same site where either edge switch is not part of the fabric is not supported.
- Path trace from a router's loopback interface is not supported.
- Overlapping IP addresses are not supported with or without fabric.

- For path trace to work on a Locator ID/Separation Protocol (LISP) fabric, make sure that the traffic is running and cache is available on the edge switches.
- Path trace in Cisco Adaptive Security Appliances (ASA) is not supported because Cisco ASA does not support CDP. It is not possible to identify the path through the Cisco ASA appliance.
- Path trace is not supported for the management interface in wireless controllers in untagged mode.
- Path trace for centralized Wireless Mobility Modes Asymmetric Mobility Tunneling is not supported.
- Path trace for Virtual Switching System (VSS), Multi-Link Aggregation Control Protocol (MLACP), or Virtual PortChannel (vPC) is not supported.
- Path trace for Equal-Cost Multi-Path Routing (ECMP) over Switched Virtual Interface (SVI) is not supported.
- Path trace is not supported on devices with NAT or firewall.
- Cisco Performance Routing (PfR) is not supported with DMVPN tunnels.
- Path trace that has VLAN ACLs (VACLs) enabled is not supported.
- For a Non Periodic Refresh (NPR) path scenario, after an upgrade, the controller does not refresh the path. Additionally, statistics collection stops. To continue statistics collection, you must initiate a new path request.
- Path trace from a host in a Hot Standby Router Protocol (HSRP) VLAN to a host in a non-HSRP VLAN that is connected to any of the HSRP routers is not supported.
- Object groups are not supported in an ACL trace.
- Port-channel Port Aggregation Protocol (PAgP) mode is not supported. Only LACP mode is supported.
- Applying a performance monitor configuration using Catalyst Center fails if there is a different performance monitor policy configuration on the interface. Remove the performance monitor configuration on the interface and resubmit the path trace request.
- Path trace for Performance Monitor statistics is not supported for Cisco ASR 1000 Series routers (Cisco IOS XE 16.3.1).
- Path trace for Performance Monitor statistics is not supported for the Cisco Catalyst 3850 Switch (Cisco IOS XE 16.2.x and 16.3.1).
- Path trace for Cisco Mobility Express (ME) wireless controllers is not supported.
- Path trace for wireless clients that use OTT in Cisco SD-Access fabric is not supported.
- Path trace from a Layer 2 switch is not supported.
- Cisco's Industrial Ethernet (IE) Switches are extended nodes as part of the SD-Access solution. Currently, path trace does not recognize extended nodes, so if a topology contains extended nodes, you will get an error message.
- Dual stack that has both IPv4 and IPv6 addresses for devices is not supported. If this occurs, an error message displays stating that the given address is unknown.
- Because Cisco wireless controllers do not send SNMP mobility traps, be aware that:
    - For a path trace request, Catalyst Center does not have the right egress virtual interface highlighted on any foreign wireless controller.

- The path trace request does not highlight any ACLs applied on the foreign wireless controller.

Note The workaround is to wait for the inventory cycle to complete.

- Path trace requires client-connected ports to be configured as Layer 2.
- Path trace does not support stand-by WLCs.
- Path trace does not support VM-based devices such as CSRv or C9800-CL due to interface mapping limitations.
- Path trace does not support Cisco Mobility Express (ME) or Embedded Wireless Controllers (EWC).
- Path trace does not support extended nodes, such as the IE4000 series.
- Path trace does not support using a WLC or AP as a source or destination device.
- Path trace in a wireless LISP fabric displays VXLAN tunnels only between source and destination Edges, not the APs.
- Path trace does not support hosts connected via a trunk port.
- Path trace does not support management interfaces for WLCs in untagged mode.
- Path trace does not support VSS, M-LACP, or vPC configurations.
- Path trace does not support ECMP over SVI.
- Path trace does not support port-channel PAgP mode; only LACP mode is supported.
- Path trace does not support VLAN ACLs (VACLs).
- Path trace for NPR (Non-Periodic Refresh) scenarios does not automatically refresh after a system upgrade; a new path request is required to resume statistics collection.
- Path trace from a host in an HSRP VLAN to a host in a non-HSRP VLAN connected to the same HSRP/VRRP/GLBP router is not supported.
- Path trace fails if a conflicting performance monitor configuration exists on an interface; the configuration must be removed before submitting the request.
- Path trace may return a "Database is temporarily unavailable" error if an underlying traceroute operation times out during a periodic database refresh.
- Path trace does not support L2 handoff.
- Path trace does not support "Fabric to unknown" scenarios.
- Path trace in dual-stack setups may display management IPs that do not represent the actual IP type used in the VXLAN tunnel, which can impact UI rendering.

Do a path trace

The path trace feature works in a similar manner in all the devices. You can do a path trace from the **Client 360** or **Device 360** window.

Before you begin

- Review the path trace known limitations. See Path trace limitations, on page 425.
- Make sure that the devices (routers, switches, wireless controllers, and access points) are discovered. See Discover your network using an IP address range or CIDR, on page 24, Discover your network using CDP, on page 21, or Discover your network using LLDP, on page 26.
- Make sure that CDP is enabled in the devices.

Procedure

Step 1 From the **Client 360** or **Device 360** window, in the **Path Trace** category, click **Run New Path Trace**.
The **Set up Path Trace** slide-in pane appears.

Step 2 Enter the source IP address, interface, and port number; and the destination IP address, interface, and port number.

Field	Action
Source IP field	The IP address in the **Source IP** field is pre-populated; however, you can enter another source IP address by doing one of these tasks: • Enter the source IP address. • Click the **Source IP** drop-down, and then select an IP address from the available options. The drop-down list for source IP addresses is limited to a maximum of 100 entries. • Click the **MAC** drop-down, then select a MAC address from the available options, or enter a new MAC address and click the plus icon to add it.
Interface (optional) field	Select an interface from the drop-down list. **Note** This field appears if the source IP address is a network device.
Port (optional) field	Enter the port number of the host from which you want the trace to start.
Destination field	• Enter the IP address of the host or the Layer 3 forwarding interface at which you want the trace to end. • Click the **Destination** field, and then select an IP address from the available options. The drop-down list for destination IP addresses is limited to a maximum of 100 entries. • Click the **MAC** drop-down, then select a MAC address from the available options, or enter a new MAC address and click the plus icon to add it.

Field	Action
Interface (optional) field	Select the interface from the drop-down list. **Note** This field appears if the IP address you select in the Destination field is a network device.
Port (optional) field	Enter the port number of the host from which you want the trace to end.

Step 3 From the **Options** area do these tasks as appropriate:

Field	Action
Protocol drop-down list	(Optional) Select either **tcp** or **udp**.
Live Traffic	Enable this toggle to **On** to capture the network packets traveling through select devices in real time as a .pcap file. **Max number of packets to capture** drop down list - Select the maximum number packets to be captured. **Note** **Refresh Every 30sec** toggle button gets disabled automatically when you enable **Live Traffic** toggle button and vice versa.
Refresh Every 30sec	(Optional) Set this toggle to **On** to configure the path trace topology to refresh every 30 seconds.
ACL Trace	(Optional) Set this toggle to **On** to display matched ACLs and the ACL result (Permit or Deny) for a specific traffic flow.
Include Stats options	(Optional) To configure the path trace to collect additional statistics, check these check boxes as needed: • **Device**: Collects and displays information, such as the device CPU and memory usage. • **Interface**: Collects and displays information about the device interface. • **QoS**: Collects and displays QoS information, such as collector-voice-egress, collector-broadcast-video-egress, collector-real-time-interactive-egress, and so on.

Step 4 Click **Start**.
The path trace topology appears. The IP addresses, protocol, and the time stamp indicating when the path trace was last updated display above the topology.

Step 5 In the path trace topology, you can do these tasks:

a) Hover your cursor over a device to display this information:

- CPU utilization
- Memory utilization
- Average processing delay of ACLs, tunneling, and queues

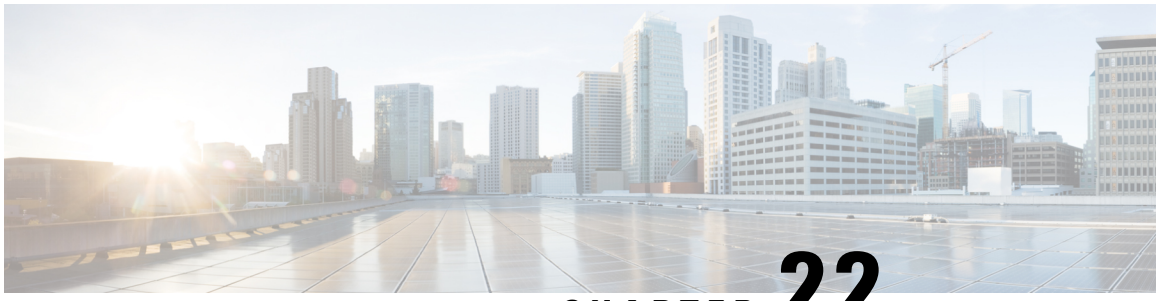
- Packet forward decision, which includes the number of packets forwarded and dropped and the drop reason

If **ACL Trace** is set to **On**, the ACL name and ACL result, such as permit or deny display.

If the 5-tuple values (source IP address and port number, destination IP address and port number, and the protocol in use) are provided, then the ACL trace that appears is 100% accurate. If partial information is provided, the ACL trace that appears is on best effort basis. In such a case, the ACL results might display both Permit and Deny status.

Matched ACLs in a specific traffic flow appear with a colored icon. Green indicates **Permit**. Red indicates **Deny**. For Ingress ACLs, the icon appears on the left side of the device. For Egress ACLs, the icon appears on the right side of the device.

b) Click a device to open a slide-in pane with additional device details.
c) Hover your cursor over a Layer 2 or Layer 3 port channel interface to display information, such as used VLANs and output drops. Click **More Details** to open a slide-in pane with additional information.
d) Hover your cursor over the path to display the protocol of the devices along the path (**Switched**, **STP**, **ECMP**, **Routed**, **Trace Route**) or other source type.



CHAPTER 22

Integrate Cisco CMX for Wireless Maps

- About Cisco Connected Mobile Experiences integration, on page 431
- Add a user for the Cisco CMX API server, on page 431
- Create Cisco CMX settings, on page 432
- Troubleshoot Cisco CMX, on page 434

About Cisco Connected Mobile Experiences integration

Catalyst Center supports the integration of on-premises Cisco Connected Mobile Experiences (CMX) for wireless maps. With the CMX integration, you can get the exact location of your wireless clients, rogue access points, and interferers on the floor map within the Catalyst Center user interface.

Depending on your requirements, you can create CMX settings either at the global level or at the site, building, or floor level. For a small enterprise, you can assign CMX at the global level, which is the parent node. All children inherit their settings from the parent node. For a medium enterprise, you can assign CMX at the building level, and for a large enterprise, you can assign CMX at the floor level.

Note CMX should be anonymized for security purposes.

Add a user for the Cisco CMX API server

Before adding a Cisco CMX instance to Catalyst Center Network Settings, you must add a user for the Cisco CMX API server.

Procedure

Step 1 SSH to Cisco CMX using a cmxadmin account. Enter this command:

```
ssh -l cmxadmin (cmx-ip-address)
```

Step 2 Start the Cisco CMX API server. Enter this command:

```
# cmxos apiserver start
```

Example

```
[root@server]# cmxos apiserver start
Starting CMX API Server...
```

Step 3 Add a user for the Cisco CMX API server. Enter this command:

```
cmxos apiserver user add
```

At the password prompt, use the same password as the Cisco CMX web admin user password.

Example

```
[root@server]# cmxos apiserver user add
Please enter the userid for the CMX API Server: user1
Please enter the password for the CMX API Server: Cisco_CMX_web_admin_password
Please re-enter the password for the CMX API Server: Cisco_CMX_web_admin_password
Restarting CMX API Server...
Stopping CMX API Server...
Starting CMX API Server...
Successfully updated userid/password and restarted the CMX API Server
```

Create Cisco CMX settings

Before you begin

- Ensure that CMX is configured with a valid SSL/TLS certificate. See the CMX 10.5 SSL certificate installation procedure.
- Add a Cisco CMX API user. See Add a user for the Cisco CMX API server, on page 431.

  CMX uses separate API resources for Catalyst Center integration, requiring you to configure two identical user accounts in CMX. You must manually create a CMX API server user that matches your GUI admin user by running the CLI command **cmxos apiserver user add** and following the prompts for username and password. Because CMX enforces a web GUI password rotation policy, you must also update the API server user's password with the same CLI command (**cmxos apiserver user add**) whenever you change the admin GUI password.

  The GUI admin user enables Catalyst Center access to the /v1 API endpoints, while the API Server user provides access to /v3 API endpoints. Both are required for full Catalyst Center integration.

Procedure

Step 1 From the main menu, choose **System** > **Settings**.

Step 2 From the **External Services** section, click **Cisco Spaces/CMX Servers**.

The **Cisco Spaces/CMX Servers** window opens.

Step 3 From the **CMX Servers** table, click **Add**.

Step 4 Complete the fields in the **Add CMX Server** slide-in pane:

- **IP Address**: Enter the valid IP address of the CMX web GUI.
- **Username**: Enter the CMX web GUI admin username.

Note
To assign a CMX server to a site, building, or floor, you must have Write permission on **Network Hierarchy**. For more information, see "Catalyst Center user role permissions" in the *Cisco Catalyst Center Administrator Guide*.

- **Password**: Enter the password credentials.

Note
Ensure CMX is reachable.

Step 5 Click **Add**.

The connection status is shown in these stages:

- **Initiating Connection**: Verifies connectivity to the server.
- **Establishing Trust**: Establishes trust to the CMX server. The CMX server must have a valid SSL/TLS certificate configured to establish trust. If the certificate is not yet stored in Catalyst Center Trusted Certificates, you are prompted to **Accept** the certificate to continue.
- **Connecting CMX Server**: Validates the user credentials provided.

Step 6 To assign a CMX server to a site, building, or a floor, click the menu icon and choose **Design** > **Network Settings**.

Step 7 Click the **Wireless** tab.

Step 8 From the left hierarchy tree, select either **Global** or the required area, building, or floor.

Step 9 Click **Cisco Spaces/CMX Servers**.

Step 10 In the **Cisco Spaces/CMX Servers** section, from the **Location Settings** drop-down list, select the CMX server.

Step 11 Click **Save**.

The **Create CMX Settings** window opens.

After the CMX is added, if you make any changes to the floor on the **Network Hierarchy** page, the changes are synchronized automatically with the CMX.

When the CMX is synced, Catalyst Center starts querying the CMX for the client location and displays the location on the floor map.

Step 12 From the floor map, you can do these tasks:

- View the location of the client, which is shown as a blue dot.
- Hover your cursor over an AP. A dialog box appears with **Info**, **Rx Neighbor**, and **Clients** tabs. Click each tab for more information. Click **Device 360** to open the Device 360 window and view issues. Click an issue to see the location of the issue and the location of the client device.
- Click an AP to open a side bar with details about the AP.
- Do real-time client tracking when Intelligent Capture and CMX are integrated.

Step 13 If the CMX was down when you made changes, you must synchronize manually. To do so, on the **Network Hierarchy** window, hover your cursor over the ellipsis ••• next to the building or floor on which you made the changes in the left hierarchy tree, and then select **Sync: Cisco Spaces/CMX Servers** to push the changes manually.

Step 14 To edit the CMX server details or delete a CMX server:

a) From the main menu, choose **System** > **Settings**.

b) From the **External Services** section, click **Cisco Spaces/CMX Servers**.
c) Select the CMX server that you want to edit, make any changes, and click **Update**.
d) Select the CMX server that you want to delete and click **Delete**.
e) Click **OK** to confirm the deletion.

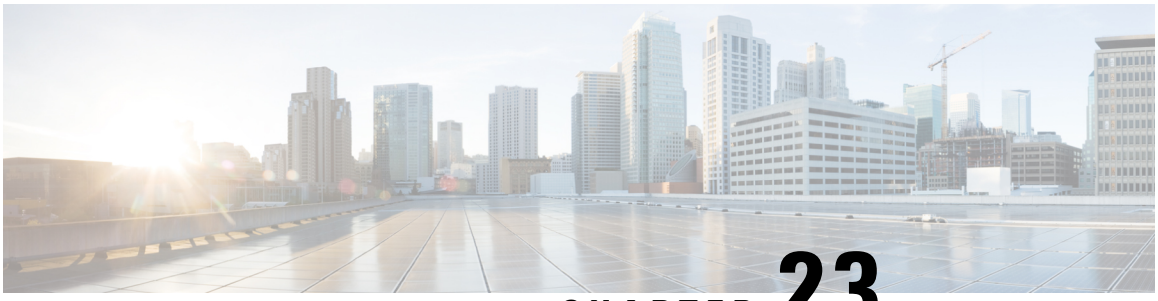
Troubleshoot Cisco CMX

CMX authentication failure

- Check if you are able to log in to the CMX web UI with the credentials that you provided at the time of CMX settings creation on Catalyst Center.
- Check if you are able to log in to the CMX console using SSH.
- Check if you are able to exercise CMX REST APIs using the API documentation link on the CMX UI.

Clients do not appear on the floor map

- Check if the Cisco Wireless Controller on the particular floor is configured with CMX and is active.
- Check if the CMX UI shows clients on the floor map.
- Use the Catalyst Center Maps API to list the clients on the floor: `curl -k -u <user>:<password> -X GET /api/v1/dna-maps-service/domains/<floor group id>/clients?associated=true`



CHAPTER 23

View Assurance Audit Logs

- View audit logs for Assurance, on page 435

View audit logs for Assurance

Audit logs are created to capture critical activities, such as when configuration changes were requested, when the configuration changes were executed, and if errors occurred during the configuration. For Assurance, audit logs are provided when configuration changes are made to Intelligent Capture, issue thresholds, sensors, and AI Network Analytics.

To access the audit logs, choose **Activities** > **Audit Logs**. For a detailed procedure, see the "View Audit Logs" topic in the *Cisco Catalyst Center Administrator Guide*.

For Assurance, this data is captured in the audit logs:

Table 10: Audit logs

Item	Description
Date and Time	Date and time the log was received or executed.
Description	A brief description explaining the audit log.
User	The user that requested or executed the change.

Intelligent Capture audit logs

For Intelligent Capture, audit logs are provided to capture these configuration changes:

- Enable or disable AP Statistics, globally.
- Enable or disable AP Statistics for a set of individual APs.
- Enable or disable Anomaly Capture, globally.
- Enable and disable Anomaly Capture for a set of individual APs.
- Enable or disable Spectrum Analysis.
- Enable or disable Scheduled Capture.
- Enable or disable Live Capture.

- Enable or disable Data Packet Capture.

If any errors occurred during the configuration, that information is also provided in the audit logs.

Issue threshold audit logs

For issue threshold, audit logs are provided to capture these updates:

- Updates on site health.
- Updates on the health score.
- Updates on the issue settings.

Sensor audit logs

For sensors, audit logs are provided to capture these configuration requests:

- Received request to add test suite.
- Received request to update test suite.
- Received request to delete test suite.
- Received request to update tests for certificate bundle.
- Received request to add test status.

AI Analytics audit logs

For AI Analytics, audit logs are provided to capture these AI agent configuration changes:

- Agent onboarded.
- Agent restored.
- Agent reconfigured.