Cisco DNA Assurance User Guide, Release 2.2.2

First Published: 2021-04-23

Last Modified: 2023-07-17

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)

© 2021–2023 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **New and Changed Information** 1

What's New in Cisco DNA Assurance, Release 2.2.2 1

CHAPTER 2 **Cisco DNA Assurance Overview** 5

About Cisco DNA Assurance 5

Assurance Architecture 5

IPv6 Address Support 6

Start with Assurance 7

CHAPTER 3 **Cisco AI Network Analytics Overview** 9

About Cisco AI Network Analytics 9

Cisco AI Network Analytics Benefits 11

Cisco AI Network Analytics Licensing and Deployment 12

Supported Cisco AI Network Analytics Features on the Catalyst 9800 Series Wireless Controller 12

CHAPTER 4 **Set Up Cisco DNA Center to Use Assurance** 13

Limitations and Restrictions 13

Basic Setup Workflow 13

Discover Devices 16

About Discovery 16

Discovery Prerequisites 17

Preferred Management IP Address 17

Discovery Configuration Guidelines and Limitations 18

Discover Your Network Using CDP 18

Discover Your Network Using an IP Address Range 24

Discover Your Network Using LLDP 29

Manage Discovery Jobs 34
Stop and Start a Discovery Job 34
Clone a Discovery Job 34
Delete a Discovery Job 35
View Discovery Job Information 35
Design Network Hierarchy 36
Design a New Network Infrastructure 36
About Network Hierarchy 36
Guidelines for Image Files to Use in Maps 37
Create a Site in a Network Hierarchy 37
Add Buildings 38
Add a Floor to a Building 38
Manage Network Hierarchy 39
Upload an Existing Site Hierarchy 39
Search the Network Hierarchy 40
Edit Sites 41
Delete Sites 41
Edit a Building 41
Delete a Building 41
Edit a Floor 41
Monitor a Floor Map 42
Edit Floor Elements and Overlays 42
Floor View Options 51
Data Filtering 54
Manage Inventory 55
About Inventory 55
Update the Device Polling Interval 55
Display Information About Your Inventory 56
Delete a Network Device 61
Add a Device to a Site 62
About Cisco ISE Configuration for Cisco DNA Center 62
Configure Authentication and Policy Servers 63
Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry 65

Configure Cisco AI Network Analytics Data Collection 66
Disable Cisco AI Network Analytics Data Collection 69
Update the Machine Reasoning Knowledge Base 69
Enable Localization 70
Role-Based Access Control Support for Assurance 71

CHAPTER 5 **Monitor and Troubleshoot Overall Enterprise Health** 73
About Enterprise 73
Monitor and Troubleshoot the Overall Health of Your Enterprise 73

CHAPTER 6 **Monitor and Troubleshoot Network Health** 77
About Network 77
Monitor and Troubleshoot the Health of Your Network 77
Monitor and Troubleshoot the Health of a Device 85
Selected Syslogs Below Error Level for Switches and Routers 94
About Cisco StackWise Virtual and Its Limitations 95
About Cisco StackWise and Its Limitations 96
Configure Health Score Settings for Network Devices 97
Fabric Domains 97
About Fabric Networks 97
Create a Fabric Domain 98
Add a Device to a Fabric 98
Enable SNMP Collector Metrics for Fabric Devices 100
Understand Network Health Score and KPI Metrics 101
Network Health Score 102
Device Category Health Score 102
Individual Device Health Score 102
Switch Health Score 103
Router Health Score 104
AP Health Score 105
Wireless Controller Health Score 106

CHAPTER 7 **Monitor and Troubleshoot Client Health** 109
About Clients 109

Monitor and Troubleshoot the Health of All Client Devices 109
Monitor and Troubleshoot the Health of a Client Device 120
Messages Displayed in the Event Viewer for Wired Clients 125
Understand Client Health Score and KPI Metrics 126
Client Health Score 126
Client Onboarding Score 126
Client Connectivity Score 127
Individual Client Health Score 127

CHAPTER 8 **Monitor Application Health** 129
About Application Experience and Application Visibility 129
Supported Platforms 130
Criteria for Enabling Application Telemetry on Devices 131
Application Health Prerequisites 133
Provision Application Telemetry Settings 135
View Application Experience of a Host 136
View Application Experience of a Network Device 137
Monitor the Health of All Applications 138
Monitor the Health of an Application 143
Configure Health Score Settings for Applications 147
Understand Application Health Score and KPI Metrics 147
Overall Application Health Score 147
Individual Application Health Score 148

CHAPTER 9 **View and Manage Issues** 149
About Issues 149
About Machine Reasoning Engine 150
About Layer 2 Loop Issue 150
View Open Issues 150
Issue Instance Details for AI-Driven Issues 154
Issue Instance Details for Layer 2 Loop and PoE Issues 158
Issue Instance Details for a PoE Issue 160
Troubleshoot Wired Client Issues Using MRE 162
View Resolved Issues 164

View Ignored Issues 166
Resolve or Ignore Issues 167
Radio Outage Issue Triggers 169
Automatic Issue Resolution 169
Manage Issue Settings 170
Enable Issue Notifications 171
Assurance, Cisco AI Network Analytics, and MRE Issues 172
Router Issues 172
Core, Distribution, and Access Issues 173
Controller Issues 176
Access Point Issues 176
Wired Client Issues 177
Wireless Client Issues 178
Application Issues 181
Sensor Issues 181
AI-Driven Issues 183
MRE Issues 184

CHAPTER 10 **Manage Sensors and Sensor-Driven Tests** 187
About Sensors and Sensor-Driven Tests 187
Provision Sensors 187
Provision the Wireless Cisco Aironet 1800s Active Sensor 187
Enable Provisioning SSID on the Wireless Controller 188
Enable Cisco Provisioning SSID on the Cisco Catalyst Wireless Controller 188
Provision a Wireless or Sensor Device 189
Monitor and Troubleshoot Network Health with Sensors 192
Monitor and Troubleshoot Network Health with All Wireless Sensors 192
Monitor and Troubleshoot Network Health with a Wireless Sensor 197
Manage Sensors and Backhaul Settings 199
Manage Sensors in Your Network 199
Manage Backhaul Settings 201
Persistent Wireless Backhaul Connections on Sensor Devices 203
Manage SCEP Profiles 203
Sensor-Driven Tests 204

Create and Run Sensor-Driven Tests Using Templates 204
Manage Sensor-Driven Test Templates 208

CHAPTER 11 **Monitor Wi-Fi 6 Readiness** 211
About Wi-Fi 6 Readiness and Its Benefits 211
Assure the Readiness of Your Wi-Fi 6 Network and Its Benefits 211

CHAPTER 12 **Monitor Power over Ethernet** 219
About PoE 219
Setup Workflow for PoE Telemetry 219
Configure NETCONF on Your Network Devices for PoE Telemetry 221
Update Telemetry Settings for PoE Telemetry 223
Monitor PoE-Capable Devices in Your Network 223

CHAPTER 13 **Monitor the Rogue Management Dashboard** 229
Manage Security Threats on Networks 229

CHAPTER 14 **Manage Dashboards** 231
About Dashboards 231
Create a Custom Dashboard 231
Create a Dashboard from a Template 232
View a Dashboard 233
Edit or Delete a Dashboard 234
Duplicate a Dashboard 234
Mark a Dashboard as a Favorite 234
Change the Position of a Dashlet 235

CHAPTER 15 **Observe Network Trends and Gain Insights** 237
About Network Trends and Insights 237
View Network Trends and Obtain Insights 237
Compare Access Points in Network Heatmaps 241
Compare KPI Values with Peers in Your Network 243
Compare Buildings, AP Model Families, and Wireless Endpoint Types 245

View and Monitor Network Performance Using Baselines 248

CHAPTER 16 **Manage Intelligent Capture** 253

About Intelligent Capture 253

Supported Devices for Intelligent Capture 253

Intelligent Capture Best Practices 255

Live and Scheduled Capture Sessions for a Client Device 255

About Capture Sessions for a Client Device 255

About Client Statistics 256

Enable a Live Capture Session for a Client Device 256

Schedule and Manage Capture Sessions for a Client Device 261

Data Packet Capture for a Client Device 262

About Data Packet Capture for a Client Device 262

About NAM Integration 263

Configure an IP Address on the NAM Data Port 263

Configure the gRPC Collector 264

Run Data Packet Capture for a Client Device 264

View Client Data Packet Capture History 267

Intelligent Capture for Access Points 267

About Intelligent Capture for Access Points 267

Enable and Manage Intelligent Capture for an Access Point 268

View RF Statistics and Manage Spectrum Analysis Data for an Access Point 270

About Cisco AP Functionality During Spectrum Analysis 275

Troubleshoot Intelligent Capture 275

Client or Access Point Unable to Send Intelligent Capture Data to Cisco DNA Center 275

CHAPTER 17 **Trace the Path of a Device** 277

About Path Trace 277

Path Trace Known Limitations 277

Perform a Path Trace 279

CHAPTER 18 **Integrate Cisco CMX for Wireless Maps** 281

About Cisco Connected Mobile Experiences Integration 281

Add a User for the Cisco CMX API Server 281

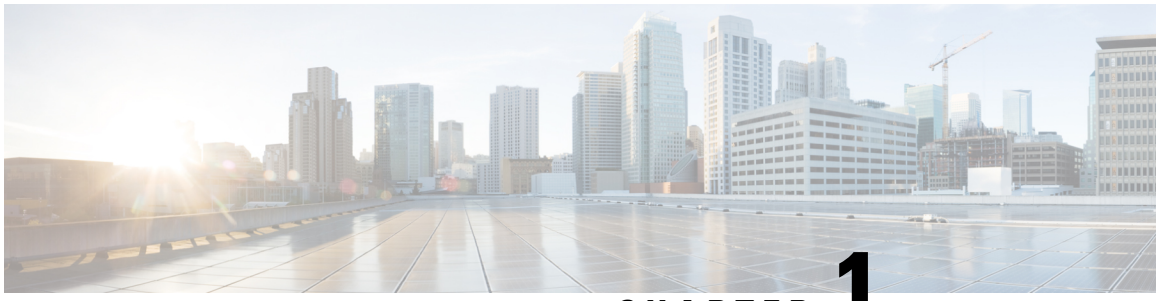
Create Cisco CMX Settings 282
Troubleshoot Cisco CMX 283

CHAPTER 19 **Reports** 285
About Reports 285

CHAPTER 20 **View Assurance Audit Logs** 287
View Audit Logs for Assurance 287

CHAPTER 21 **Troubleshoot Cisco DNA Center Using Data Platform** 289
About Data Platform 289
Troubleshoot Using the Analytics Ops Center 290
View or Update Collector Configuration Information 291
View Data Retention Settings 292
View Pipeline Status 293

CHAPTER 22 **Related Documentation** 295
Related Documentation 295



CHAPTER 1

New and Changed Information

- What's New in Cisco DNA Assurance, Release 2.2.2, on page 1

What's New in Cisco DNA Assurance, Release 2.2.2

The following table summarizes the new and changed features in the *Cisco DNA Assurance User Guide, Release 2.2.2*.

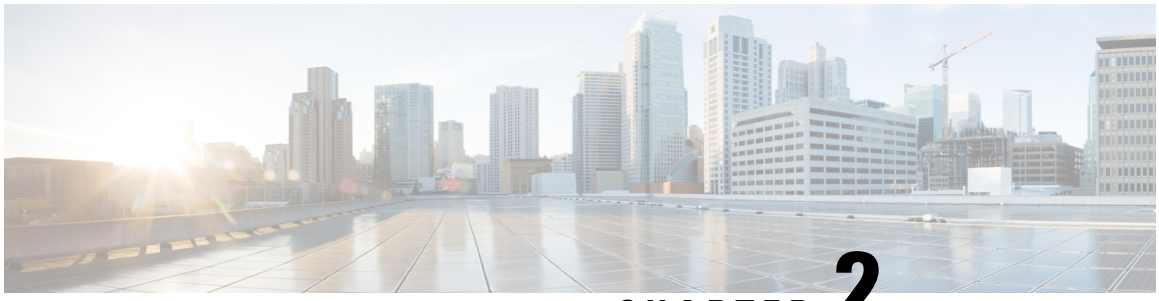
Table 1: New and Changed Features in Cisco DNA Assurance

Feature	Description
Device 360 - Interface Utilization Graph	For interfaces, Tx and Rx Utilization chart values are populated in absolute values (**Percentage** and **Rate**). See Monitor and Troubleshoot the Health of a Device, on page 85.
Network Device Health Summary UI Enhancement - Unmonitored to No Health	The Network Device Health Summary - Total Devices section provides the total number of network devices and the count of Good Health, Fair Health, Poor Health, and No Health data. See Monitor and Troubleshoot the Health of Your Network, on page 77.
Cisco SD-Access: Network Health Dashboard Enhancements	The Network Health Summary dashlet provides new KPIs for fabric domains: • **Fabric CP Reachability** • **External Multicast RP** for Fabric Border • **AAA Server Status** for Fabric Edge and Extended Node In the Network Device dashlet, you can filter the network device table based on the fabric types, including **Extended Node**. See Monitor and Troubleshoot the Health of Your Network, on page 77.

Feature	Description
Cisco SD-Access: Device 360 Enhancements	In the Network Device 360 - Device detail area, below the timeline, you can view additional information about the device such as **Fabric Role**, **Fabric Domain**, and **Fabric Site**. In the Detailed Information area under the Fabric tab, new fabric KPIs are grouped under **Fabric Infrastructure** and **VN Service** included for device health. See Monitor and Troubleshoot the Health of a Device, on page 85.
Cisco SD-Access: Network Topology Enhancements	In the Physical Neighbor Topology for fabric domains, the fabric badge icons identify device fabric groups such as Border, Control Plane, Edge, Extended Node and Wireless. See Monitor and Troubleshoot the Health of a Device, on page 85.
Event Viewer Enhancements	In the Client 360 Dashboard, the Event Viewer detailed information area is enhanced to show: • Associate Start Event: The RSSI and SNR values throughout the session. • Delete Event: Detailed delete reasons for client disconnections.
WAN Link Utilization Dashlet	You can view the status of the WAN link utilization percentage only for the available WAN links in your network. See Monitor and Troubleshoot the Health of Your Network, on page 77.
WAN Link Availability Dashlet	You can view the status of the available WAN links in your network. See Monitor and Troubleshoot the Health of Your Network, on page 77.
Power Stack Visibility	In the Network Device 360 view, you can view the stack power connection details under the PoE tab. See Monitor and Troubleshoot the Health of a Device, on page 85.
Power over Ethernet Dashboard	The PoE dashboard is added to **Assurance > Dashboards > PoE**, which lets you monitor and view the operational state of the PoE-capable devices in your network. The following dashlets are available: PoE Operational State Distribution, PoE Powered Device Distribution, Power Load Distribution, PoE Insights, and PoE Power Usage Dashlet. See Monitor PoE-Capable Devices in Your Network, on page 223.
Sensor Test - Proxy	With this release, proxy support is enabled for Sensor-Driven Tests. You can run the sensor test through proxy settings. See Create and Run Sensor-Driven Tests Using Templates, on page 204.
Application Experience Health Score Calculation Enhancements	You can add the Application Response Time KPI to the Application Experience health score calculation. See View Application Experience of a Network Device, on page 137 and View Application Experience of a Host, on page 136.

Feature	Description
Application Health Score Customization	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. See Configure Health Score Settings for Applications, on page 147.
Monitor Application Health Enhancements	Click the **Managed Clients** tab to view only the clients that are managed by Cisco DNA Center. See Monitor the Health of an Application, on page 143.
View and Manage Issues (Access Point Issues)	A poor RF issue triggers when APs have a poor wireless experience. The poor RF issue instance second slide-in pane supports **Problem Details**, **Impact Details**, **Troubleshooting**, and **Suggested Actions** for poor RF issues. Also, the poor RF issue instance second slide-in pane allows you to compare the health of AP radios across the floor in a building. See Access Point Issues, on page 176.
View and Manage Issues (Wireless Client Issues)	With this release, the Cisco DNA Center machine reasoning engine (MRE) supports root cause analysis (RCA) for AAA server issues. RCA allows you to analyze Cisco ISE syslog messages from various servers to derive the possible root causes that could have triggered the issue. RCA support is extended for the following AAA server issues: • AAA wireless client failed to connect • AAA server timeout • AAA server rejected client See Wireless Client Issues, on page 178.
View and Manage Issues (Radio No Activity Issues)	The radio no activity issue instance identifies and raises an issue for AP radios that fail to serve clients for 60 to 240 minutes. The radio no activity issue instance pane supports **Problem Details**, **Relevant Issue**, and **Suggested Actions**. See Access Point Issues, on page 176.
Monitor and Troubleshoot the Health of a Device	The Device 360 page now supports a **Map and Comparison View** that allows you to compare the last 5 minutes of health of AP radios across the floor in a building. See Monitor and Troubleshoot the Health of a Device, on page 85.
Baselines Dashboard	Cisco AI Network Analytics uses the most advanced machine learning techniques to define the baseline that is relevant to your specific network and sites. See View and Monitor Network Performance Using Baselines, on page 248.
MAC Randomization	With MAC randomization, client devices use unique private MAC Address - RCM Randomized and Changing MAC Address when connecting to the Wi-Fi network. See Monitor and Troubleshoot the Health of All Client Devices, on page 109.

Feature	Description
Deprecated Feature: Sensor-Driven Tests Using the Legacy Method	You can no longer create and run sensor-driven tests using the legacy method. You need to create and run sensor-driven tests using templates. See Create and Run Sensor-Driven Tests Using Templates, on page 204.



CHAPTER 2

Cisco DNA Assurance Overview

- About Cisco DNA Assurance, on page 5
- Assurance Architecture, on page 5
- IPv6 Address Support, on page 6
- Start with Assurance, on page 7

About Cisco DNA Assurance

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

Assurance provides the following 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 performs 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.

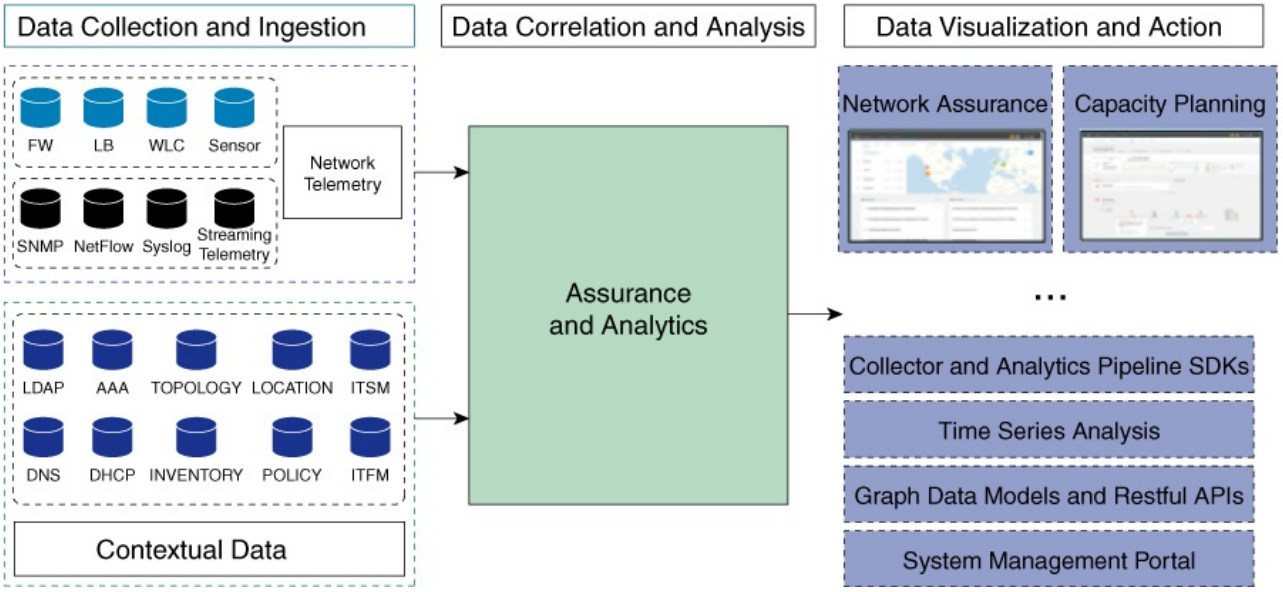
Assurance is a multipurpose, real-time, network data collection and analytics engine that can significantly increase the business potential of network data.

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 Cisco DNA strategy.

The following figure and the information that follows describes the 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, such as Capacity Planning. Assurance is an open system that provides the following:
  - Collector and analytics pipeline SDKs
  - Time-series analysis
  - Graph data models and restful APIs
  - System management portal

IPv6 Address Support

Cisco DNA Center supports IPv6 addresses. A single IPv6 address can be represented in many text formats, but Cisco DNA Center supports the IPv6 address in the canonical format only. The canonical format is also called the normalized compressed format as shown below:

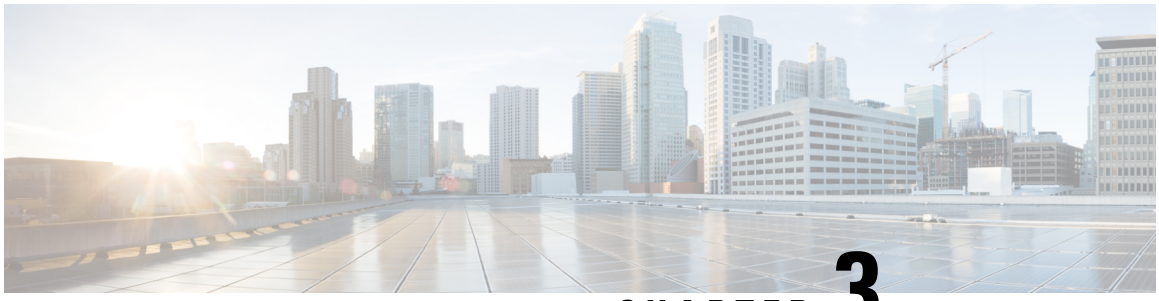
```
2001:db8::1:0:0:1
```

Start with Assurance

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

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

- Existing infrastructure: If you have an existing infrastructure (brownfield 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 13.
- New or nonexisting infrastructure: If you do not have an existing infrastructure and are starting from scratch (greenfield deployment), design a network hierarchy. For information about designing a network hierarchy, see the Cisco DNA Center User Guide.



CHAPTER 3

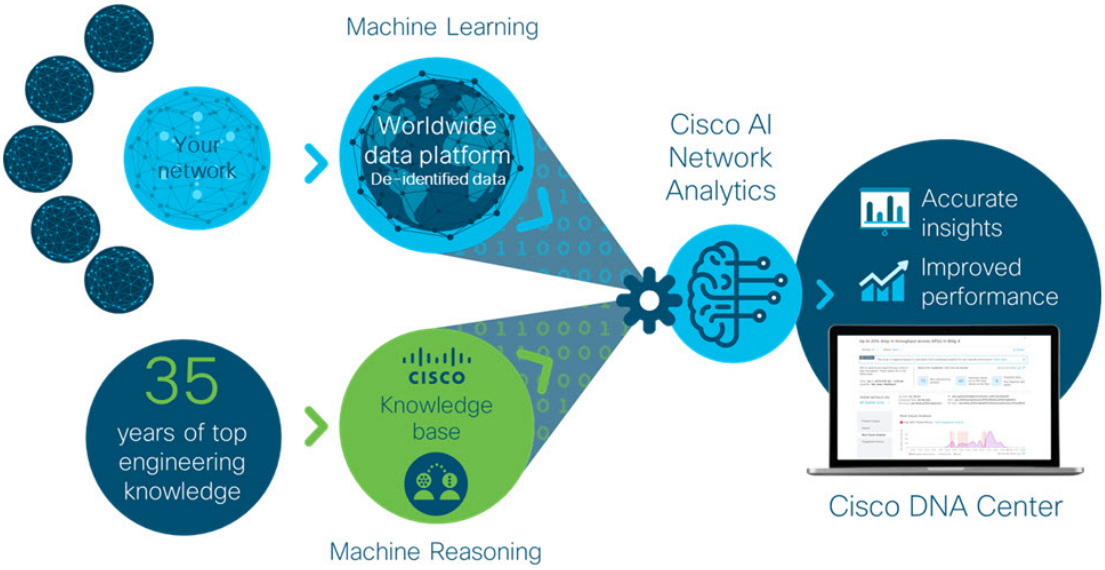
Cisco AI Network Analytics Overview

- About Cisco AI Network Analytics , on page 9
- Cisco AI Network Analytics Benefits, on page 11
- Cisco AI Network Analytics Licensing and Deployment , on page 12
- Supported Cisco AI Network Analytics Features on the Catalyst 9800 Series Wireless Controller, on page 12

About Cisco AI Network Analytics

Cisco AI Network Analytics is an application within Cisco DNA 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. The following figure and the information that follows describes the Cisco AI Network Analytics architecture:

Figure 1: Cisco AI Network Analytics Architecture



Cisco AI Network Analytics consists of the following:

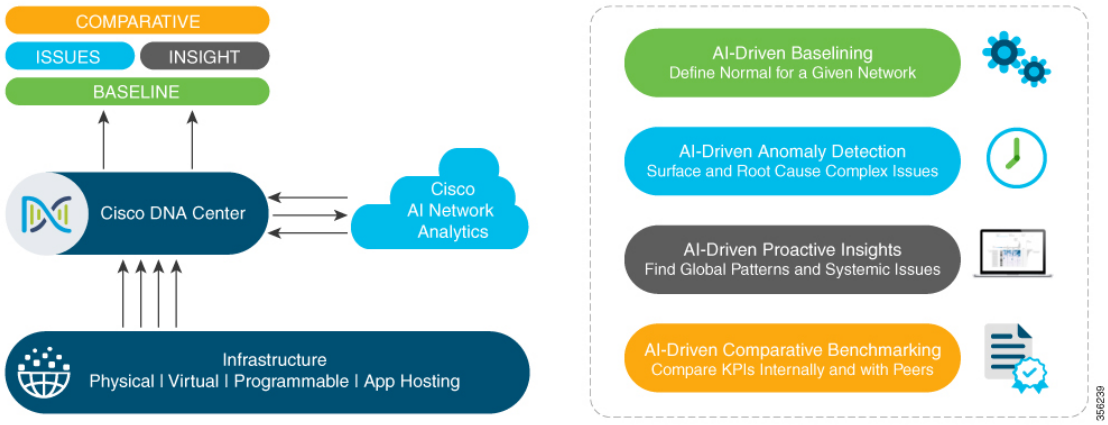
- A worldwide cloud-based data platform where Machine Learning models are built and analyzed for your specific network environment.
- A Machine Reasoning inference engine that automates human expertise and captures the workflows in a knowledge base repository.

Machine Learning

Cisco AI Network Analytics leverages advanced Machine Learning (ML) techniques and an advanced cloud learning platform with de-identifed network event data, to identify critical issues in your network, and provide 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 Cisco DNA Center that is fully integrated with Cisco DNA Assurance.

The following figure and the information that follows describes the Cisco AI Network Analytics features:

Figure 2: Cisco AI Network Analytics Features



Cisco AI Network Analytics provides the following:

- **Cloud-Based Infrastructure**: Network events information is de-identified in Cisco DNA 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 de-identified network event data and brings the issues and overall insights back to Cisco DNA Center.
- **Intelligent Issue Detection and Analysis**, 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 the following 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**, includes:
  - **AI-Driven Proactive Insights**: Determine global patterns (trends) and deviations to provide system-generated insights.
- **Comparative Benchmarking**, 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 Site Comparisons**: Determine how a site (building) is performing compared to another site in your network for a selected KPI.

Machine Reasoning

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.

Cisco AI Network Analytics Benefits

Cisco AI Network Analytics provides the following benefits:

- **More Visibility**: Each network is unique and the network environment is always changing. Cisco AI Network Analytics continuously collects the relevant data from the local networks, correlates the data against the aggregate de-identifed 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 number of 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 the issue. This helps IT detect issues and vulnerabilities, analyze the root causes, and quickly execute corrective actions.

Cisco AI Network Analytics Licensing and Deployment

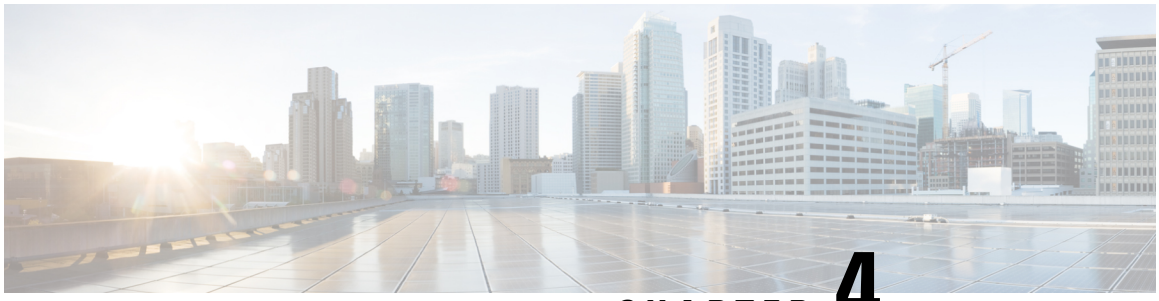
Cisco AI Network Analytics is part of the **Cisco DNA Advantage** software license for Cisco DNA Center. It is provided as an additional component that seamlessly blends in with the Assurance user interface. The solution provides advanced machine learning-generated insights and issues, along with the 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 Cisco DNA 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 Cisco DNA Center global settings. Network event data is de-identified 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 the "Cisco AI Network Analytics Privacy Data Sheet" at https://www.cisco.com/c/en/us/about/trust-center/data-privacy.html.

Supported Cisco AI Network Analytics Features on the Catalyst 9800 Series Wireless Controller

The following table lists the Cisco AI Network Analytics features that are supported on the Catalyst 9800 Series Wireless Controller and the minimum software version.

Cisco DNA Center Release	Supported Features	Minimum Cisco IOS-XE Software Version
2.2.2	• **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** Throughput issues are not supported. • **Trends and Insights**	16.12.1s



CHAPTER 4

Set Up Cisco DNA Center to Use Assurance

Before you begin using the Assurance application, you must configure Assurance. This chapter provides the basic tasks you must do to set up Assurance. Use this chapter in conjunction with the Cisco Digital Network Architecture Center User Guide.

- Limitations and Restrictions, on page 13
- Basic Setup Workflow, on page 13
- Discover Devices, on page 16
- Design Network Hierarchy, on page 36
- Manage Inventory, on page 55
- Add a Device to a Site, on page 62
- About Cisco ISE Configuration for Cisco DNA Center, on page 62
- Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry, on page 65
- Configure Cisco AI Network Analytics Data Collection, on page 66
- Update the Machine Reasoning Knowledge Base, on page 69
- Enable Localization, on page 70
- Role-Based Access Control Support for Assurance , on page 71

Limitations and Restrictions

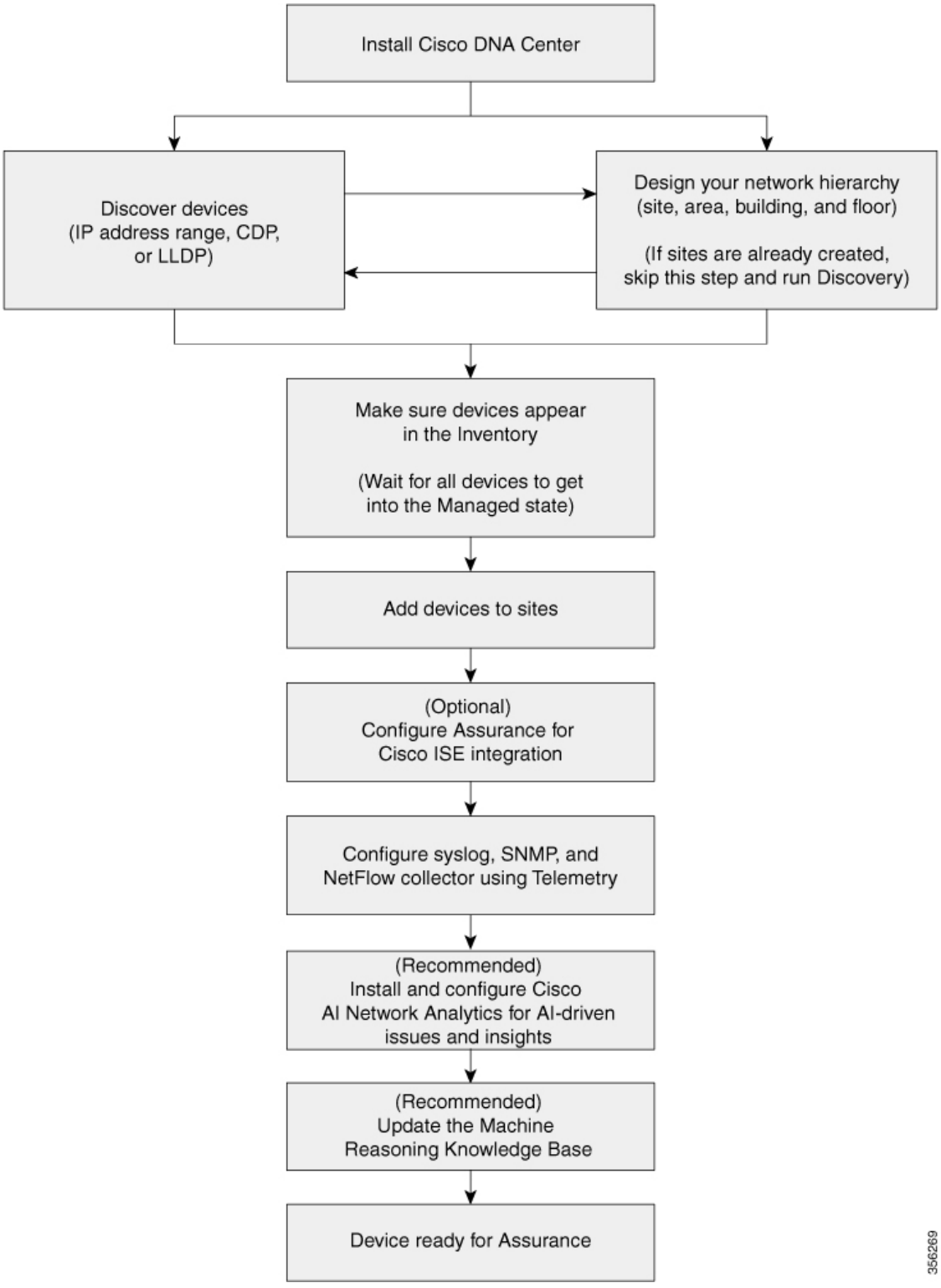
Assurance is not supported over NATed connections to managed devices.

Basic Setup Workflow

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

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

Figure 3: Basic Workflow for Setting Up Cisco DNA Center to Use Assurance



Before you begin

See Limitations and Restrictions, on page 13.

Step 1 Install Cisco DNA Center.

See the Cisco DNA Center Installation Guide.

Step 2 Do the following in any order:

- Discover devices (routers, switches, wireless controllers, and access points).

  See Discover Your Network Using an IP Address Range, on page 24, Discover Your Network Using CDP, on page 18, or Discover Your Network Using LLDP, on page 29.

  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.

- Design your network hierarchy. Configure the location of the device, such as area, site, building, and floor.

  See Create a Site in a Network Hierarchy, on page 37, Add Buildings, on page 38, and Add a Floor to a Building, on page 38.

  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 56.

Note You must wait for all the devices to get into a Managed state.

Step 4 Add devices to sites.

See Add a Device to a Site, on page 62.

Step 5 If you are adding APs, we recommend that you assign and position them on a floor map.

See Add, Position, and Delete APs, on page 43.

Step 6 If your network uses Cisco Identity Services Engine 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 Cisco DNA Center, on page 62.

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 65.

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 Data Collection, on page 66.

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 69.

Step 10 Start using the Assurance application.

Discover Devices

The Discovery feature scans the devices in your network and sends the list of discovered devices to Inventory.

About Discovery

The Discovery feature scans the devices in your network and sends the list of discovered devices to Inventory.

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

There are three ways for you to discover devices:

- Use Cisco Discovery Protocol (CDP) and provide a seed IP address.
- Specify a range of IP addresses. (A maximum range of 4096 devices is supported.)
- Use Link Layer Discovery Protocol (LLDP) and provide a seed IP address.

When configuring the Discovery criteria, remember that there are settings that you can use to help reduce the amount of time it takes to discover your network:

- **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. So, if fewer devices have to be discovered, you can set the level to a lower value.
- **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, or an IP address range, you can specify whether you want Cisco DNA Center to add any of the device's IP addresses or only the device's loopback address.

Note For Cisco SD-Access Fabric and Cisco DNA Assurance, we recommend that you specify the device's loopback address.

Regardless of the method you use, you must be able to reach the device from Cisco DNA Center and configure specific credentials and protocols in Cisco DNA 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 like Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP), the device might be discovered and added to the inventory 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 Cisco DNA Center retrieves for analysis.

Discovery Prerequisites

Before you run Discovery, complete the following minimum prerequisites:

- Understand what devices will be discovered by Cisco DNA Center by viewing the Supported Devices List.
- Understand that the preferred network latency between Cisco DNA Center and devices is 100 ms round-trip time (RTT). (The maximum latency is 200 ms RTT.)
- Ensure at least one SNMP credential is configured on your devices for use by Cisco DNA Center. At a minimum, this can be an SNMPv2C read credential.
- Configure SSH credentials on the devices you want Cisco DNA Center to discover and manage. Cisco DNA Center discovers and adds a device to its inventory if at least one of the following criteria is met:
  - The account that is being used by Cisco DNA 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 18.

Preferred Management IP Address

When Cisco DNA Center discovers a device, it uses one of the device's 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 Cisco DNA Center to use the device's loopback IP address as the preferred management IP address, provided the IP address is reachable from Cisco DNA Center.

When you choose **Use Loopback IP** as the preferred management IP address, Cisco DNA Center determines the preferred management IP address as follows:

- If the device has one loopback interface, Cisco DNA Center uses that loopback interface IP address.
- If the device has multiple loopback interfaces, Cisco DNA Center uses the loopback interface with the highest IP address.
- If there are no loopback interfaces, Cisco DNA Center uses the Ethernet interface with the highest IP address. (Subinterface IP addresses are not considered.)
- If there are no Ethernet interfaces, Cisco DNA 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

The following are the guidelines and limitations for Cisco DNA 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). This is the same CLI username and password that you configure in Cisco DNA Center for the Discovery function. Cisco DNA 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.
- Do not 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 Cisco DNA Center is the same as the TACACS credential defined in the TACACS server.
- 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.

Discover Your Network Using CDP

You can discover devices using Cisco Discovery Protocol (CDP), an IP address range, 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, on page 24 and Discover Your Network Using LLDP, on page 29.

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 17.
- 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.)

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

Step 2 Click **Add Discovery**.
The **New Discovery** window appears.

Step 3 In the **Discovery Name** field, enter a name.

Step 4 Expand the **IP Address/Range** area if it is not already visible, and configure the following fields:

a) For **Discovery Type**, click **CDP**.

b) In the **IP Address** field, enter a seed IP address for Cisco DNA Center to start the Discovery scan.

c) (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 0 to 32.

d) Click +.

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

e) (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.

f) For **Preferred Management IP**, choose one of the following 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, Cisco DNA Center chooses a management IP address using the logic described in Preferred Management IP Address, on page 17.

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 Cisco DNA Center.

Step 5 Expand the **Credentials** area and configure the credentials that you want to use for the Discovery job.

Choose any of the global credentials that have already been created or configure your own Discovery credentials. If you configure your own credentials, you can save them only for the current job by clicking **Save** or you can save them for the current and future jobs by checking the **Save as global settings** check box and then clicking **Save**.

a) Make sure that the global credentials that you want to use are selected. If you do not want to use a credential, deselect it.

b) To add additional credentials, click **Add Credentials**.

c) To configure CLI credentials, configure the following fields:

Table 2: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
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.

Field	Description
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 not displayed in the configuration.

d) Click **SNMP v2c** and configure the following fields:

Table 3: 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 not displayed 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 not displayed in the configuration.

e) (Optional) Click **SNMP v3** and configure the following fields:

Table 4: 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. Choose one of the following modes: • **noAuthNoPriv**: Does not provide authentication or encryption. • **AuthNoPriv**: Provides authentication, but does not provide encryption. • **AuthPriv**: Provides both authentication and encryption.

Field	Description
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: 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 Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as the authentication mode.) Choose one of the following privacy types: • **DES**: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard. • **AES128**: CBC mode AES for encryption. • **None**: No privacy. **Note** DES encryption is being deprecated and will be removed in a future release.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. 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 Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

f) (Optional) Click **SNMP PROPERTIES** and configure the following fields:

Table 5: SNMP Properties

Field	Description
Retries	Number of times Cisco DNA Center tries to communicate with network devices using SNMP.
Timeout	Number of seconds between retries.

g) (Optional) Click **HTTP(S)** and configure the following fields:

Table 6: HTTP(S) 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 from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that 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 from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).

h) (Optional) If you have network devices with NETCONF enabled, click **NETCONF** and enter a port number in the **Port** field.

Note You must enable NETCONF and set the port to 830 to discover Cisco Catalyst 9800 Series Wireless Controller devices. NETCONF provides a mechanism to install, manipulate, and delete configurations of network devices. NETCONF will be disabled if you select Telnet in the **Advanced** area.

Step 6 To configure the protocols to be used to connect with devices, expand the **Advanced** area and do the following tasks:

a) Click the names of the protocols that you want to use. A green check mark indicates that the protocol is selected.

Valid protocols are **SSH** (default) and **Telnet**.

b) Drag and drop the protocols in the order that you want them to be used.

Step 7 Click **Discover** and select whether to run the discovery now or schedule the discovery for a later time.

- To run the discovery now, click the **Now** radio button and click **Start**.
- To schedule the discovery for a later time, click the **Later** radio button, define the date and time, and click **Start**.

Click the notifications icon to view the scheduled discovery tasks. Click **Edit** to edit the discovery task before the discovery starts. Click **Cancel** to cancel the scheduled discovery job before it starts.

The **Discoveries** window displays the results of your scan.

The **Discovery Details** pane shows the status (active or inactive) and the Discovery configuration. The **Discovery Devices** pane displays the host names, IP addresses, and status of the discovered devices.

Discover Your Network Using an IP Address Range

You can discover devices using an IP address range, CDP, or LLDP. This procedure shows you how to discover devices and hosts using an IP address range. For more information about the other Discovery methods, see Discover Your Network Using CDP, on page 18 and Discover Your Network Using LLDP, on page 29.

Before you begin

Your devices must have the required device configurations, as described in Discovery Prerequisites, on page 17.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

Step 2 Click **Add Discovery**.
The **New Discovery** window appears.

Step 3 In the **Discovery Name** field, enter a name.

Step 4 Expand the **IP Address/Ranges** area, if it is not already visible, and configure the following fields:

a) For **Discovery Type**, click **IP Address/Range**.

b) In the **From** and **To** fields, enter the beginning and ending IP addresses (IP address range) for Cisco DNA 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.

c) (Optional) Repeat Step b to enter additional IP address ranges.

d) (Optional) In the **Subnet Filter** field, enter an IP address/range 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 0 to 32.

e) For **Preferred Management IP Address**, choose one of the following 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, Cisco DNA Center chooses a management IP address using the logic described in Preferred Management IP Address, on page 17.

Step 5 Expand the **Credentials** area and configure the credentials that you want to use for the Discovery job.

Choose any of the global credentials that have already been created or configure your own Discovery credentials. If you configure your own credentials, you can save them for only the current job by clicking **Save**, or you can save them for the current and future jobs by checking the **Save as global settings** check box and then clicking **Save**.

a) Make sure that the global credentials that you want to use are selected. If you do not want to use a credential, deselect it.

b) To add additional credentials, click **Add Credentials**.

c) To configure CLI credentials, configure the following fields:

Table 7: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
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 not displayed in the configuration.

d) Click **SNMP v2c** and configure the following fields:

Table 8: 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 not displayed 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 not displayed in the configuration.

e) (Optional) Click **SNMP v3** and configure the following fields:

Table 9: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.

Field	Description
Mode	Security level that an SNMP message requires. Choose one of the following modes: • **noAuthNoPriv**: Does not provide authentication or encryption. • **AuthNoPriv**: Provides authentication, but does not provide encryption. • **AuthPriv**: Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: 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 Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as the authentication mode.) Choose one of the following privacy types: • **DES**: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard. • **AES128**: CBC mode AES for encryption. • **None**: No privacy. **Note** DES encryption is being deprecated and will be removed in a future release.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. 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 Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

f) (Optional) Click **SNMP PROPERTIES** and configure the following fields:

Table 10: SNMP Properties

Field	Description
Retries	Number of times Cisco DNA Center tries to communicate with network devices using SNMP.
Timeout	Number of seconds between retries.

g) (Optional) Click **HTTP(S)** and configure the following fields:

Table 11: HTTP(S) 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 from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that 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 from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).

h) (Optional) If you have network devices with NETCONF enabled, click **NETCONF** and enter a port number in the **Port** field.

Note You must enable NETCONF and set the port to 830 to discover Cisco Catalyst 9800 Series Wireless Controller devices. NETCONF provides a mechanism to install, manipulate, and delete configurations of network devices.

Step 6 (Optional) To configure the protocols that are to be used to connect with devices, expand the **Advanced** area and do the following tasks:

a) Click the protocols that you want to use. A green check mark indicates that the protocol is selected.

Valid protocols are **SSH** (default) and **Telnet**.

b) Drag and drop the protocols in the order that you want them to be used.

Step 7 Click **Discover** and select whether to run the discovery now or schedule the discovery for a later time.

- To run the discovery now, click the **Now** radio button and click **Start**.
- To schedule the discovery for a later time, click the **Later** radio button, define the date and time, and click **Start**.

Click the notifications icon to view the scheduled discovery tasks. Click **Edit** to edit the discovery task before the discovery starts. Click **Cancel** if you want to cancel the scheduled discovery job before it starts.

The **Discoveries** window displays the results of your scan.

The **Discovery Details** pane shows the status (active or inactive) and the Discovery configuration. The **Discovery Devices** pane displays the host names, IP addresses, and status of the discovered devices.

Discover Your Network Using LLDP

You can discover devices using Link Layer Discovery Protocol (LLDP), CDP, or an IP address range. This procedure shows you how to discover devices and hosts using LLDP. For more information about the other discovery methods, see Discover Your Network Using CDP, on page 18 and Discover Your Network Using an IP Address Range, 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 not required to discover hosts; hosts are discovered through the network devices to which they are connected.

Before you begin

- Enable LLDP on your network devices.
- Configure your network devices, as described in Discovery Prerequisites, on page 17.
- 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.)

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

Step 2 Click **Add Discovery**.
The **New Discovery** window appears.

Step 3 In the **Discovery Name** field, enter a name.

Step 4 Expand the **IP Address/Range** area and configure the following fields:

a) For **Discovery Type**, click **LLDP**.

b) In the **IP Address** field, enter a seed IP address for Cisco DNA Center to start the Discovery scan.

c) (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 0 to 32.

d) Click +.

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

e) (Optional) In the **LLDP 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, LLDP level 3 means that LLDP will scan up to three hops from the seed device.

f) For **Preferred Management IP**, choose one of the following options:

- **None**: Allows the device use any of its IP addresses.

- **Use Loopback IP**: Specify the device's loopback interface IP address.

  Note If you choose this option and the device does not have a loopback interface, Cisco DNA Center chooses a management IP address using the logic described in Preferred Management IP Address, on page 17.

  Note To use the loopback interface IP address as the preferred management IP address, make sure that the LLDP neighbor's IP address is reachable from Cisco DNA Center.

Step 5 Expand the **Credentials** area and configure the credentials that you want to use for the Discovery job.

Choose any of the global credentials that have already been created, or configure your own Discovery credentials. If you configure the credentials, you can choose to save them for future jobs by checking the **Save as global settings** check box.

a) Make sure that the global credentials that you want to use are selected. If you do not want to use a credential, deselect it.
b) To add additional credentials, click **Add Credentials**.
c) For CLI credentials, configure the following fields:

Table 12: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
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 not displayed in the configuration.

d) Click **SNMP v2c** and configure the following fields:

Table 13: 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 not displayed 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 not displayed in the configuration.

e) (Optional) Click **SNMP v3** and configure the following fields:

Table 14: 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. Choose one of the following modes: • **noAuthNoPriv**: Does not provide authentication or encryption. • **AuthNoPriv**: Provides authentication, but does not provide encryption. • **AuthPriv**: Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: Authentication based on HMAC-MD5.

Field	Description
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 Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as the authentication mode.) Choose one of the following privacy types: • **DES**: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard. • **AES128**: CBC mode AES for encryption. • **None**: No privacy. **Note** DES encryption is being deprecated and will be removed in a future release.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. 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 Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

f) (Optional) Click **SNMP PROPERTIES** and configure the following fields:

Table 15: SNMP Properties

Field	Description
Retries	Number of times Cisco DNA Center tries to communicate with network devices using SNMP.
Timeout	Number of seconds between retries.

g) (Optional) Click **HTTP(S)** and configure the following fields:

Table 16: HTTP(S) 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 from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).
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 from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).

Step 6 (Optional) To configure the protocols to be used to connect with devices, expand the **Advanced** area and do the following tasks:

a) Click the names of the protocols that you want to use. A green check mark indicates that the protocol is selected. Valid protocols are **SSH** (default) and **Telnet**.
b) Drag and drop the protocols in the order that you want them to be used.

Step 7 Click **Discover** and select whether to run the discovery now or schedule the discovery for a later time.

- To run the discovery now, click the **Now** radio button and click **Start**.
- To schedule the discovery for a later time, click the **Later** radio button, define the date and time, and click **Start**.

Click the notifications icon to view the scheduled discovery tasks. Click **Edit** to edit the discovery task before the discovery starts. Click **Cancel** if you want to cancel the scheduled discovery job before it starts.

The **Discoveries** window displays the results of your scan.

The **Discovery Details** pane shows the status (active or inactive) and the Discovery configuration. The **Discovery Devices** pane displays the host names, IP addresses, and status of the discovered devices.

Manage Discovery Jobs

Stop and Start a Discovery Job

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Discovery**. The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

Step 3 To stop an active Discovery job, perform these steps:

a) From the **Discoveries** pane, select the corresponding job.
b) Click **Stop**.

Step 4 To restart an inactive Discovery job, perform these steps:

a) From the **Discoveries** pane, select the corresponding job.
b) Click **Re-discover** to restart the selected job.

Clone a Discovery Job

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

Before you begin

You should have run at least one Discovery job.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Discovery**. The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

Step 3 From the **Discoveries** pane, select the Discovery job.

Step 4 Click **Copy & Edit**.

Cisco DNA Center creates a copy of the Discovery job, named Copy of *Discovery_Job*.

Step 5 (Optional) Change the name of the Discovery job.

Step 6 Define or update the parameters for the new Discovery job.

Delete a Discovery Job

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

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

Step 3 From the **Discoveries** pane, select the Discovery job that you want to delete.

Step 4 Click **Delete**.

Step 5 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.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

Step 3 From the **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 the following 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 when 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.

Design Network Hierarchy

You can create a network hierarchy that represents your network's geographical locations. Your network hierarchy can contain sites, which contains buildings and areas.

Design a New Network Infrastructure

The **Design** area is where you create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network. Use the **Design** workflow if you do not already have an existing infrastructure. If you have an existing infrastructure, use the **Discovery** feature. For more information, see About Discovery, on page 16.

You can perform these tasks in the **Design** area:

Step 1 Create your network hierarchy.

Step 2 Define global network settings.

Step 3 Define network profiles.

About Network Hierarchy

You can create a network hierarchy that represents your network's geographical locations. Your network hierarchy can contain sites, which in turn contain buildings and areas. You can create site and building IDs to easily identify where to apply design settings or configurations later. By default, there is one site called **Global**.

The network hierarchy has a predetermined hierarchy:

- **Areas** or **Sites** do not have a physical address, such as the United States. You can think of areas as the largest element. Areas can contain buildings and subareas. For example, an area called United States can contain a subarea called California, and the subarea California can contain a subarea called San Jose.
- **Buildings** have a physical address and contain floors and floor plans. When you create a building, you must specify a physical address and latitude and longitude coordinates. Buildings cannot contain areas. By creating buildings, you can apply settings to a specific area.
- **Floors** are within buildings and consist of cubicles, walled offices, wiring closets, and so on. You can add floors only to buildings.

You can change the site hierarchy for non provisioned devices while preserving AP locations on sitemaps.

These are the allowed site hierarchy movements:

- You can move buildings under a new area which is empty without any site hierarchy under it.

- You can move an area under a new area which is empty without any site hierarchy under it.
- You cannot move an existing floor to a different building.

The following is a list of tasks that you can perform:

- Create a new network hierarchy. For more information, see Create a Site in a Network Hierarchy, on page 37.
- Upload an existing network hierarchy from Cisco Prime Infrastructure. For more information, see Upload an Existing Site Hierarchy, on page 39.

Guidelines for Image Files to Use in Maps

- Use a graphical application that can save the map image files to any of these formats: .jpg, .gif, .png, .dxf, and .dwg.
- Ensure that the dimension of an image is larger than the combined dimension of all the buildings and outside areas that you plan to add to the campus map.
- Map image files can be of any size. Cisco DNA Center imports the original image to its database at a full definition, but during display, it automatically resizes them to fit the workspace.
- Obtain the horizontal and vertical dimensions of the site in feet or meters before importing. This helps you to specify these dimensions during map import.

Create a Site in a Network Hierarchy

Cisco DNA 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.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

A world map is displayed in the right pane.

Step 2 In the **Network Hierarchy** window, click **+ Add Site** > **Add Area** or click the gear icon ⚙ next to the parent site in the left pane, and then click **Add Area**.

Step 3 Enter a name for the site in the **Area Name** field.

Step 4 From the **Parent** drop-down list, choose a parent node.

By default, **Global** is the parent node.

Step 5 Click **Add**.

The site is created under the parent node in the left pane.

You can also upload an existing hierarchy. For more information, see Upload an Existing Site Hierarchy, on page 39.

Add Buildings

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

A world map is displayed in the right pane.

Step 2 In the **Network Hierarchy** window, click **+Add Site** > **Add Building**, or click the gear icon ⚙ next to the parent site in the left pane and select **Add Building**.

You can also upload an existing hierarchy.

Step 3 In the **Building Name** field, enter a name for the building.

The building name can contain all special characters except for " & ? ' / < > are allowed.

Step 4 From the **Parent** drop-down list, choose a parent node.

By default, **Global** is the parent node.

Step 5 In the **Address** field, enter an address. If you are connected to the Internet, as you enter the address, the Design Application narrows down the known addresses to the one you enter. The user can move the marker to change the position on the map. When you see that the correct address appears in the window, select it. When you select a known address, the **Longitude** and **Latitude** coordinates fields are automatically populated.

Step 6 Click **Add**.

The building that you created is added under the parent site in the left menu.

Step 7 To add another area or building, in the hierarchy frame, click the gear icon ⚙ next to an existing area or building that you want to be the parent node.

Add a Floor to a Building

After you add a building, create floors and upload a floor map.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 Expand the **Global** site and the previously created area to see all the previously created buildings.

Step 3 Click the gear icon ⚙ next to the building to which you want to add a floor, and then click **Add Floor**.

Step 4 Enter a name for the floor. The floor name contain upto 21 characters. has a 21.

The floor name can contain all special characters except for & > < ? ' / [ ] are not allowed.

The floor name can start with a letter or a hyphen (-) and the string following the first character can include one or more of the following:

- Upper or lower case letters or both
- Numbers
- Underscores (_)
- Hyphens (-)
- Periods (.)

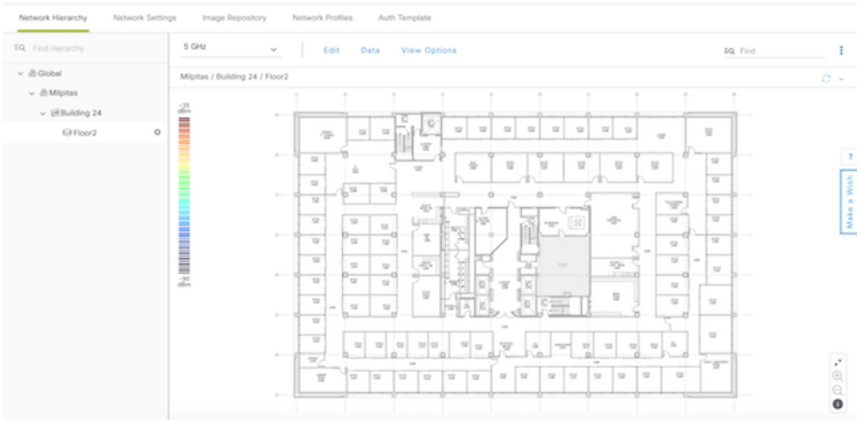
- Spaces ( )

Step 5 Define the type of floor by choosing the Radio Frequency (RF) model from the **Type (RF Model)** drop-down list: **Indoor High Ceiling**, **Outdoor Open Space**, **Drywall Office Only**, and **Cubes And Walled Offices**. This defines if the floor is an open space or a drywall office, and so on. Based on the RF model selected, the wireless signal strength and the distribution of heatmap is calculated.

Step 6 You can drag a floor plan on to the map or upload a file. Cisco DNA Center supports the following file types: .jpg, .gif, .png, .dxf, and .dwg.

After you import a map, make sure that you mark the Overlay Visibility as **On** (**Floor** > **View Option** > **Overlays**). By default, overlays are not displayed after you import a map.

Figure 4: Example of a Floor Plan



Step 7 Click **Add**.

Manage Network Hierarchy

Upload an Existing Site Hierarchy

You can upload a CSV file or a map archive file that contains an existing network hierarchy. For example, you can upload a CSV file with location information that you exported from Cisco Prime Infrastructure. (For information about exporting maps from Cisco Prime Infrastructure, see Export Maps Archive, on page 40.)

Note Before importing a map archive file into Cisco DNA Center, make sure that the devices such as Cisco Wireless Controllers and the associated APs are discovered and listed on the Cisco DNA Center inventory page.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy** and then choose **Import** > **Import Sites**.

A world map is displayed in the right pane.

Step 2 Drag and drop your CSV file, or navigate to where your CSV file is located, then click **Import**.

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

Step 3 To import the Cisco Prime Infrastructure maps tar.gz archive file, choose **Import** > **Map Import**.

Step 4 Drag and drop the map archive file into the boxed area in the **Import Site Hierarchy Archive** dialog box, or click the **click to select** link and browse to the archive file.

Step 5 Click **Save** to upload the file.

The **Import Preview** window appears, which shows the imported file.

Export Maps Archive

You can export maps archive files from Cisco Prime Infrastructure and import them into Cisco DNA Center.

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

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

Step 3 On the **Select Sites** window, configure the following. You can either select map information or calibration information to be included in the maps archive.

- **Map Information**: Click the **On or Off** button to include map information in the archive.
- **Calibration Information**: To export calibration information, click the **On or Off** button. Click the **Calibration Information for selected maps** or the **All Calibration Information** radio button. If you select **Calibration Information for selected maps**, the calibration information for the selected site maps is exported. If you select **All Calibration Information**, the calibration information for the selected map, along with additional calibration information that is available in the system, is also exported.
- In the **Sites** left pane, check one or more check boxes of the site, campus, building floor, or outdoor area that you want to export. Check the **Select All** check box to export all the maps.

Step 4 Click **Generate Map Archive**. A message `Exporting data is in progress` is displayed.
A tar file is created and is saved to your local machine.

Step 5 Click **Done**.

Search the Network Hierarchy

You can search the network hierarchy to quickly find a site, building, or area. This is particularly helpful after you have added many sites, areas, or buildings.

To search the tree hierarchy, in the **Find Hierarchy** search field in the left pane and enter either the partial or full name of the site, building, or floor name that you are searching. The tree hierarchy is filtered based on the text you enter in the search field.

Edit Sites

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, navigate to the corresponding site that you want to edit.

Step 3 Click the gear icon ⚙ next to the site and select **Edit Site**.

Step 4 Make the necessary changes, and click **Update**.

Delete Sites

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, navigate to the site that you want to delete.

Step 3 Click the gear icon ⚙ next to the corresponding site and select **Delete Site**.

Step 4 Confirm the deletion.

Edit a Building

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left tree pane, navigate to the building that you want to edit.

Step 3 Click the gear icon ⚙ next to the building and select **Edit Building**.

Step 4 Make the necessary changes in the **Edit Building** window, and click **Update**.

Delete a Building

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, navigate to the building that you want to delete.

Step 3 Click the gear icon next to the building and select **Delete Building**.

Step 4 Confirm the deletion.

Note Deleting a building deletes all its container maps. APs from the deleted maps are moved to Unassigned state.

Edit a Floor

After you add a floor, you can edit the floor map so that it contains obstacles, areas, and APs on the floor.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 Expand the network hierarchy to find the floor that you want to edit, or enter the floor name in the **Search Hierarchy** text field in the left pane.

Step 3 Make the necessary changes in the **Edit Floor** dialog window, and click **Update**.

Monitor a Floor Map

The floor view navigation pane provides access to multiple map functions like:

- Use the **Find** feature located at the top-right corner of the floor map window to find specific floor elements such as APs, sensors, clients, and so on. The elements that match the search criteria are displayed on the floor map along with a table in the right pane. When you hover your mouse over the table, it points to the search element on the floor map with a connecting line.
- Click the icon at the top-right corner of the floor map window to:
  - Export a floor plan as a PDF.
  - Measure the distance on the floor map.
  - Set the scale to modify the floor dimensions.
- Click the icon at the bottom-right of the floor map window to zoom in on a location. The zooming levels depend upon the resolution of an image. A high-resolution image might provide more zoom levels. Each zoom level comprises of a different style map shown at different scales, each one showing the corresponding details. Some maps are of the same style, but at a smaller or larger scale.
- Click the icon to see a map with fewer details.
- Click the icon to view the map icon legend.

Edit Floor Elements and Overlays

Using the **Edit** option available on the floor area, you can:

- Add, position, and delete the following floor elements:
  - Access Points
  - Sensors
- Add, edit, and delete the following overlay objects:
  - Coverage Areas
  - Obstacles
  - Location Regions
  - Rails
  - Markers
  - GPS Markers

Guidelines for Placing Access Points

Follow these guidelines while placing APs on the floor map:

- Place APs along the periphery of coverage areas to keep devices close to the exterior of rooms and buildings. APs placed in the center of these coverage areas provide good data on devices that would otherwise appear equidistant from all other APs.
- Location accuracy can be improved by increasing overall AP density and moving APs close to the perimeter of the coverage area.
- In long and narrow coverage areas, avoid placing APs in a straight line. Stagger them so that each AP is more likely to provide a unique snapshot of the device location.
- Although the design provides enough AP density for high-bandwidth applications, location suffers because each AP view of a single device is not varied enough. Therefore, location is difficult to determine. Move the APs to the perimeter of the coverage area and stagger them. Each has a greater likelihood of offering a distinctly different view of the device, resulting in higher location accuracy.
- For optimal heatmap visibility on floor maps, configure the AP height to approximately 10 feet (3 meters) or lower.

Add, Position, and Delete APs

Cisco DNA Center computes heatmaps for the entire map that show the relative intensity of the Radio Frequency (RF) signals in the coverage area. The heatmap is only an approximation of the actual RF signal intensity because it does not consider the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions.

Make sure that you have Cisco APs in your inventory. If not, discover APs using the Discovery feature. See About Discovery, on page 16.

Cisco DNA Center supports the following 802.11ax APs:

- Cisco Catalyst 9120 Access Points
- Cisco Catalyst 9117 Access Points
- Cisco Catalyst 9115 Access Points
- Cisco Catalyst 9100 Access Points

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Floor Elements** panel, next to **Access Points**, click **Add**.

Access points that are not assigned to any floors appear in the list.

Step 5 On the **Add APs** window, check the check boxes of the access points to select the APs in bulk, and click **Add Selected**. Alternatively click **Add** next to an access point.

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

Step 6 Close the **Add APs** window after assigning APs to the floor area.

Step 7 Newly added APs appear on the top-right corner of the floor map.

Step 8 In the **Floor Elements** pane, next to Access Points, click **Position** to position the APs correctly on the map.

- To position the APs, click an AP and drag and drop it to the appropriate location on the floor map. Alternatively you can update the x and y coordinates and AP Height in the **Selected AP Details** window. When you drag an access point on the map, its horizontal (x) and vertical (y) position appears in the text field. When selected, the access point details are displayed in the right pane. The **Selected AP Details** window displays the following:
  - **Position by 3 points**: You can draw three points on the floor map and position APs using the points created. To do this:
    a. Click **Position by 3 points**.
    b. To define the points, click anywhere on the floor map to start drawing the first point. Click again to finish drawing a point. A dialog box appears to set the distance to first point. Enter the distance, in meters, and click **Set Distance**.
    c. Define the second and third points similarly, and click **Save**.
  - **Position by 2 Walls**: You can define two walls on the floor map and position APs between the defined walls. This helps you to know the position of APs between the two walls. This helps you to understand the AP position between the walls.
    a. Click **Position by 2 walls**.
    b. To define the first wall, click anywhere on the floor map to start drawing the line. Click again to finish drawing a line. A dialog box appears to set the distance to the first wall. Enter the distance in meters and click **Set Distance**.
    c. Define the second wall similarly and click **Save**.

       The AP is placed automatically as per the defined distance between the walls.
  - **AP Name**: Shows the AP name.
  - **AP Model**: Indicates the AP model for the selected access point.
  - **MAC Address**: Displays the MAC address.
  - **x**: Indicates the horizontal span of the map, in feet.
  - **y**: Indicates the vertical span of the map, in feet.
  - **AP Height**: Indicates the height of the access point.
  - **Protocol**: Protocol for this access point: 802.11a/n/ac, 802.11b/g/n (for Hyper Location APs), or 802.11a/b/g/n.
  - **Antenna**: Antenna type for this access point.

    Note For external APs, you must select an antenna, or the AP will not be present in the map.
  - **Antenna Image**: Shows the AP image.
  - **Antenna Orientation**: Indicates the Azimuth and the Elevation orientations, in degrees.
  - **Azimuth**: This option does not appear for omnidirectional antennas because their pattern is nondirectional in azimuth.

The azimuth is the angle of the antenna measured relative to the x axis. The azimuth range is 0 to 360. In Cisco DNA Center, north is 0 or 360 degrees; east is 90 degrees.

Step 9 After you have completed placing and adjusting access points, click **Save**.

The heatmap is generated based on the new position of the AP.

If a Cisco Connected Mobile Experiences (CMX) is synchronized with Cisco DNA Center, you can view the location of clients on the heatmap. See Create Cisco CMX Settings, on page 282.

Step 10 In the **Floor Elements** panel, next to **Access Points**, click **Delete**.
The **Delete APs** window appears, listing all the assigned and placed access points.

Step 11 Check the check boxes next to the access points that you want to delete, and click **Delete Selected**.

- To delete all the access points, click **Select All** and then **Delete Selected**.
- To delete an access point from the floor, click the **Delete** icon.
- Use **Quick Filter** and search using the AP name, MAC address, model, or controller. The search is case-insensitive. The search result appears in the table. Click the **Delete** icon to delete the APs from the floor area.

Quick View of APs

Hover your cursor over the AP icon on the floor map to view AP details, Rx neighbor information, client information, and Device 360 information.

- Click **Info** to view the following AP details:
  - **Associated**: Indicates whether an AP is associated or not.
  - **Name**: AP name.
  - **MAC Address**: MAC address of the AP.
  - **Model**: AP model number.
  - **Admin/Mode**: Administration status of the AP mode.
  - **Type**: Radio type.
  - **OP/Admin**: Operational status and AP mode.
  - **Channel**: Channel number of the AP.
  - **Antenna**: Antenna name.
  - **Azimuth**: Direction of the antenna.
- Click the **Rx Neighbors** radio button to view the immediate Rx neighbors for the selected AP on the map with a connecting line. The floor map also shows whether the AP is associated or not along with the AP name.
- Click **Device 360** to get a 360° view of a specific network element (router, switch, AP, or Cisco wireless controller). See the *Monitor and Troubleshoot the Health of a Device* topic in the Cisco DNA Assurance User Guide.

Note For Device 360 to open, you must have the Assurance application installed.

Add, Position, and Delete Sensors

Note 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. See the *Provision the Wireless Cisco Aironet 1800s Active Sensor* topic in the Cisco DNA Assurance User Guide.

A *sensor device* is a dedicated AP 1800s sensor. The Cisco Aironet 1800s Active Sensor gets bootstrapped using PnP. After it obtains the Assurance server reachability details, it directly communicates with the Assurance server.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan.

Step 4 In the **Floor Elements** panel, next to **Sensors**, click **Add**.

Step 5 On the **Add Sensors** window, check the check boxes of the sensors that you want to add. Alternatively, click **Add** next to the sensor row to add sensors.

Note You can search for specific sensors using the search option. Use the **Filter** field and search using the name, MAC address, or model of a sensor. The search is case-insensitive. The search results are displayed in the table. Click **Add** to add one or more these sensors to the floor area.

Step 6 Close the **Add Sensors** window after assigning sensors to the floor map.
Newly added sensors appear on the top-right corner of the floor map.

Step 7 To position the sensors correctly, in the **Floor Elements** pane, next to **Sensors**, click **Position** to place them correctly on the map.

Step 8 After you have completed placing and adjusting sensors, click **Save**.

Step 9 To delete a sensor, in the **Floor Elements** pane, next to **Sensors**, click **Delete**.
The **Delete Sensors** window lists all the assigned and placed sensors.

Step 10 Check the check boxes of the sensors that you want to delete, and click **Delete Selected**.

- To delete all the sensors, click **Select All**, and click **Delete Selected**.
- To delete a sensor from the floor, click the **Delete** icon next to that sensor.
- Use **Quick Filter** and search using the name, MAC address, or model. The search is case-insensitive. The search results are displayed in a table. Click the **Delete** icon to delete one or more sensors from the floor area.

Add Coverage Areas

By default, any floor area or outside area defined as part of a building map is considered as a wireless coverage area.

If you have a building that is nonrectangular or you want to mark a nonrectangular area within a floor, you can use the map editor to draw a coverage area or a polygon-shaped area.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **Coverage Areas**, click **Add**.
The **Coverage creation** dialog-box appears.

Step 5 To draw a coverage area, from the **Type** drop-down list, choose **Coverage Area**.

a. Enter the name of the area you are defining, and click **Add Coverage**. The coverage area must be a polygon with at least 3 vertices.

b. Move the drawing tool to the area you want to outline.

c. Click the tool to start and stop a line.

d. After you have outlined the area, double-click the area, which results in the area getting highlighted.

Note The outlined area must be a closed object for it to be highlighted on the map.

Step 6 To draw a polygon-shaped area, from the **Type** drop-down list, choose **Perimeter**.

a. Enter the name of the area you are defining, and click **Ok**.

b. Move the drawing tool to the area you want to outline.

- Click the tool to start and stop a line.
- After you have outlined the area, double-click the area, which results in area getting highlighted on the page.

Step 7 To edit a coverage area, in the **Overlays** panel, next to **Coverage Areas**, click **Edit**.

The available coverage areas are highlighted on the map.

Step 8 Make the changes and click **Save** after the changes.

Step 9 To delete a coverage area, in the **Overlays** panel, next to **Coverage Areas**, click **Delete**.

The available coverage areas are highlighted on the map.

Step 10 Hover your cursor over the coverage area and, click delete.

Step 11 Click **Save** after the deletion.

Create Obstacles

You can create obstacles so that they can be considered while computing Radio Frequency (RF) prediction heatmaps for access points.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **Obstacles**, click **Add**.

Step 5 In the **Obstacle Creation** dialog box, choose an obstacle type from the **Obstacle Type** drop-down list. The type of obstacles that you can create are **Thick Wall**, **Light Wall**, **Heavy Door**, **Light Door**, **Cubicle**, and **Glass**.
The estimated signal loss for the obstacle type you selected is automatically populated. The signal loss is used to calculate RF signal strength near these objects.

Step 6 Click **Add Obstacle**.

Step 7 Move the drawing tool to the area where you want to create an obstacle.

Step 8 Click the drawing tool to start and stop a line.

Step 9 After you have outlined the area, double-click the area to highlight it.

Step 10 In the **Obstacle Creation** window, click **Done**.

Step 11 Click **Save** to save the obstacle on the floor map.

Step 12 To edit an obstacle, in the **Overlays** panel, next to **Obstacles**, click **Edit**.

All the available obstacles are highlighted on the map.

Step 13 Click **Save** after the changes.

Step 14 To delete an obstacle, in the **Overlays** panel, next to **Obstacles**, click **Delete**.

All the available obstacles are highlighted on the map.

Step 15 Hover your cursor over the obstacle and click to delete.

Step 16 Click **Save**.

Location Region Creation

You can create inclusion and exclusion areas to further refine location calculations on a floor. You can define the areas that are included (inclusion areas) in the calculations and those areas that are not included (exclusion areas). For example, you might want to exclude areas such as an atrium or stairwell within a building, but include a work area, such as cubicles, labs, or manufacturing floors.

Guidelines for Placing Inclusion and Exclusion Areas on a Floor Map

- Inclusion and exclusion areas can be any polygon-shaped area and must have at least 3 points.
- You can only define 1 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.
- You can define multiple exclusion regions on a floor area.

Define an Inclusion Region on a Floor

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 In the **Overlays** panel, next to **Location Regions**, click **Add**.

Step 4 In the **Location Region Creation** dialog window, from the **Inclusion Type** drop-down list, choose an option.

Step 5 Click **Add Location Region**.

A drawing icon appears to outline the inclusion area.

Step 6 To begin defining the inclusion area, move the drawing tool to a starting point on the map and click once.

Step 7 Move the cursor along the boundary of the area you want to include and click to end a border line.

Click again to define the next boundary line.

Step 8 Repeat Step 7 until the area is outlined and then double-click the drawing icon.

A solid aqua line defines the inclusion area.

Step 9 Click **Save**.

Define an Exclusion Region on a Floor

To further refine location calculations on a floor, you can define areas that are excluded (exclusion areas) in the calculations. For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion areas are defined within the borders of an inclusion area.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **Location Regions**, click **Add**.

Step 5 In the **Location Region Creation** window, from the **Exclusion Type** drop-down list, choose a value.

Step 6 Click **Location Region**.

A drawing icon appears to outline the exclusion area.

Step 7 To begin defining the exclusion area, move the drawing icon to a starting point on the map and click once.

Step 8 Move the drawing icon along the boundary of the area that you want to exclude.

Click once to start a boundary line, and click again to end the boundary line.

Step 9 Repeat the preceding step until the area is outlined and then double-click the drawing icon. The defined exclusion area is shaded in purple when the area is fully defined.

Step 10 To define more exclusion regions, repeat Step 5 to Step 9.

Step 11 When all the exclusion areas are defined, click **Save**.

Edit Location Regions

Step 1 In the **Overlays** panel, next to **Location Regions**, click **Edit**.
The available location regions are highlighted on the map.

Step 2 Make the necessary changes, and click **Save**.

Delete Location Regions

Step 1 In the **Overlays** panel, next to **Location Regions**, click **Delete**.
The available location regions are highlighted on the map.

Step 2 Hover your cursor over the region that you want to delete, and click **Delete**.

Step 3 Click **Save**.

Create a Rail

You can define a rail line on a floor that represents a conveyor belt. Also, you can define an area around the rail area known as the snap-width to further assist location calculations. This represents the area in which you expect clients to appear. Any client located within the snap-width area is plotted on the rail line (majority) or outside of the snap-width area (minority).

The snap-width area is defined in feet or meters (user-defined) and represents the distance that is monitored on either side (east and west or north and south) of the rail.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **Rails**, click **Add**.

Step 5 Enter a snap-width (feet or meters) for the rail, and click **Add Rail**.

A drawing icon appears.

Step 6 Click the drawing icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.

Step 7 Click the drawing icon twice when the rail line is drawn on the floor map. The rail line appears on the map and is bordered on either side by the defined snap-width region.

Step 8 Click **Save**.

Step 9 In the **Overlays** panel, next to **Rails**, click **Edit**.

The available rails are highlighted on the map.

Step 10 Make changes, and click **Save**.

Step 11 In the **Overlays** panel, next to **Rails**, click **Delete**.

All the available rail lines are highlighted on the map.

Step 12 Hover your cursor over the rail line that you want to delete, and click **Delete**.

Step 13 Click **Save**.

Place Markers

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **Markers**, click **Add**.

A drawing icon appears.

Step 5 Enter the name for the markers, and then click **Add Marker**.

Step 6 Click the drawing icon and place the marker on the map.

Step 7 Click **Save**.

Step 8 In the **Overlays** panel, next to Markers, click **Edit**.

The available markers are highlighted on the map.

Step 9 Make changes, and click **Save**.

Step 10 In the **Overlays** panel, next to **Markers**, click **Delete**.

All the available markers are highlighted on the map.

Step 11 Hover your cursor on the marker that you want to delete, and click delete.

Step 12 Click **Save**.

Floor View Options

Click the **View Options**, which is located above the floor plan in the middle pane. The floor map along with these panels appear in the right pane: **Access Points**, **Sensor**, **Overlay Objects**, **Map Properties**, and **Global Map Properties**.

You can modify the appearance of the floor map by selecting or unselecting various parameters. For example, if you want to view only the access point information on the floor map, check the **Access Point** check box. You can expand each panel to configure various settings available for each floor element.

View Options for Access Points

To view access points on a map, click the **On/Off** button next to **Access Points**. Expand the **Access Points** panel to configure these settings:

- **Display Label**: From the drop-down list, choose a text label that you want to view on the floor map for the AP. The available display labels are:
  - **None**: No labels are displayed for the selected access point.
  - **Name**: AP name.
  - **AP MAC Address**: AP MAC address.
  - **Controller IP**: IP address of Cisco Wireless Controller to which the access point is connected.
  - **Radio MAC Address**: Radio MAC address.
  - **IP Address**

- **Channel**: Cisco Radio channel number or **Unavailable** (if the access point is not connected).
- **Coverage Holes**: Percentage of clients whose signal has become weaker until the client lost its connection. It shows **Unavailable** for access points that are not connected and **MonitorOnly** for access points that are in monitor-only mode.
- **TX Power**: Current Cisco Radio transmit power level (with 1 being high) or **Unavailable** (if the access point is not connected). If you change the radio band, the information on the map changes accordingly.

  The power levels differ depending on the type of access point. The Cisco Aironet 1000 Series Lightweight Access Point accepts a value between **1** and **5**; the Cisco Aironet 1230AG Series Access Point accepts a value between **1** and **7**; and the Cisco Aironet 1240AG Series Access Point and Cisco Aironet 1100 Series Access Point accept a value between **1** and **8**.
- **Channel and Tx Power**: Channel and transmit power level (or **Unavailable** if the access point is not connected).
- **Utilization**: Percentage of bandwidth used by the associated client devices (including receiving, transmitting, and channel utilization). Displays **Unavailable** for disassociated access points and **MonitorOnly** for access points in monitor-only mode.
- **Tx Utilization**: Transmitted (Tx) utilization for the specified interface.
- **Rx Utilization**: Received (Rx) utilization for the specified interface.
- **Ch Utilization**: Channel utilization for the specified access point.
- **Assoc. Clients**: Total number of clients associated.
- **Dual-Band Radios**: Identifies and marks the XOR dual-band radios on the Cisco Aironet 2800 and 3800 Series Access Points.
- **Health Score**: AP health score.
- **Issue Count**
- **Coverage Issues**
- **AP Down Issues**

- **Heatmap Type**: Heatmap is a graphical representation of Radio Frequency (RF) wireless data where the values taken by variable are represented in maps as colors. The current heatmap is computed based on the RSSI prediction model, antenna orientation, and AP transmit power. From the **Heatmap Type** drop-down list, select the heatmap type:
  - **None**
  - **AP RSSI**: Coverage heatmap, which identifies the strength of wireless signal in the specific band.
    - **RSSI Cut off (dBm)**: Drag the slider to set the RSSI cutoff level. The RSSI cutoff ranges from -60 dBm to -90 dBm.
    - **Heatmap Opacity (%)**: Drag the slider between 0 to 100 to set the heatmap opacity.
    - **Heatmap Color Scheme**: The color green indicates good heatmap coverage, and the color red indicates poor heatmap coverage.

- **Client Density**: Density of associated clients.
  - **Map Opacity (%)**: Drag the slider to set the map opacity.
- **IDS**: Heatmap that shows the monitor mode access point coverage provided to the wireless clients on a floor map.
- **Planned Heatmap**: A planned heatmap is a hypothetical heatmap that shows the possible coverage of planned access points on a floor map.
- **Coverage**: Heatmap that excludes monitor-mode access points. (Available only if monitor-mode access points are on the floor plan.)

The AP details are reflected on the map immediately. Hover your cursor over the AP icon on the map to view AP details, RX neighbors details, client details, and switch information.

View Options for Sensors

Click the **Sensors** button to view sensors on the map. Expand the **Sensors** panel to configure these settings:

- **Display Label**: From the drop-down list, choose a text label that you want to view on the floor map for the selected access point. The available display labels are:
  - **None**
  - **Name**: Sensor name.
  - **Sensor MAC Address**: Sensor MAC address.

View Options for Overlay Objects

Expand the **Overlay Objects** panel to configure these settings. Use the **On/Off** buttons to view these overlay objects on the map.

- **Coverage Areas**
- **Location Regions**
- **Obstacles**
- **Rails**
- **Markers**

Configure Map Properties

Expand the **Map Properties** panel to configure:

- **Auto Refresh**—Provides an interval drop-down list to set how often you want to refresh maps data from the database. From the **Auto Refresh** drop-down list, set the time intervals: **None**, **1 min**, **2 mins**, **5 mins**, or **15 mins**.

Configure Global Map Properties

Expand the **Global Map Properties** panel to configure:

- **Unit of Measure**—From the drop-down list, set the dimension measurements for maps to either **Feet** or **Meters**.

Data Filtering

Filter Access Point Data

Click **Access Point** under the **Filters** panel in the right pane.

- Choose the radio type from the drop-down list, located above the floor map in the middle pane: **2.4 GHz**, **5 GHz**, or **2.4 GHz & 5 GHz**.
- Click **+ Add Rule** to add a query:
  - Choose the access point identifier you want to view on the map.
  - Choose the parameter by which you want to filter access points.
  - Enter the specific filter criteria in the text box for the applicable parameters, and click **Go**. The search results appear in a tabular format.
  - Click **Apply Filters to List** to view the filter results on the map. To view a particular access point on the map, check the check box of the access point in the table that is displayed, and click **Show Selected on Maps**.

When you hover your mouse cursor over the search result in the table, the location of the AP is marked by a line on the map.

Filter Sensor Data

Click **Sensor** under the **Filters** panel in the right pane.

- Choose the radio type from the drop-down list, located above the floor map in the middle pane: **2.4 GHz**, **5 GHz**, or **2.4 GHz & 5 GHz**.
- Click **+ Add Rule** to add a query:
  - Choose the sensor identifier you want to view on the map: **Name** and **MAC Address**.
  - Choose the parameter by which you want to filter sensors.
  - Enter the specific filter criteria in the text box for the applicable parameters, and click **Go**. The search results appear in a tabular format.
  - Click **Apply Filters to List** to view the filter results on the map. To view a particular sensor on the map, check the check box of the sensor in the table that is displayed, and click **Show Selected on Maps**.

When you hover your mouse cursor over the search result in the table, the location of the sensor is marked by a line on the map.

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 the following 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 End-point 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 17.

After the initial discovery, Cisco DNA Center maintains the inventory by polling the devices at regular intervals. The default interval is every six hours. However, you can change this interval up to 24 hours, as required for your network environment. For more information, see Update the Device Polling Interval, on page 55. Also, a configuration change in the device triggers an SNMP trap, which in turn triggers device resynchronization. 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.

Update the Device Polling Interval

You can update the polling interval at the global level for all devices by choosing **System** > **Settings** > **Network Resync Interval** or at the device level for a specific device by choosing **Device Inventory**. When you set the polling interval using the **Network Resync Interval**, that value takes precedence over the **Device Inventory** polling interval value.

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.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

Step 2 Select the devices that you want to update.

Step 3 Click **Update Polling Interval**.

Step 4 From the **Update Resync Interval** dialog box, in the **Status** field, click **Enabled** to turn on polling or click **Disabled** to turn off polling.

Step 5 In the **Polling Time** field, enter the time interval (in minutes) between successive polling cycles. Valid values are from 25 to 1440 minutes (24 hours).

Note 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, Cisco DNA Center continues to use the device-specific polling time.

Step 6 Click **Update**.

Display Information About Your Inventory

The **Inventory** table displays information for each discovered device. Click the column header to sort the rows in ascending order. Click the column header again to sort the rows in descending order.

To select which columns to show or hide in the table, click . Note that the column selection does not persist across sessions.

The device selection persists across views. When devices are selected and you choose a different view from the **Focus** drop-down list, the selection persists in the new view.

By default, 25 entries are shown in the **Inventory** table. Click **Show More** to view more entries. You can view up to 200 entries in the **Inventory** table.

The number of entries that are shown in the **Inventory** table persists across views. If there are more than 25 entries in the **Inventory** table and you choose a different view from the **Focus** drop-down list, the same number of entries persists in the new view.

Before you begin

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

In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Provision** > **Inventory**.

The **Inventory** window displays the device information gathered during the discovery process. The following table describes the information that is available.

Table 17: Inventory

Column	Description
Device Name	

Column	Description
	Name of the device. Click the device name to view the following device details: **Details**: Displays details such as device name, reachability status, manageability status, IP address, device model, role, uptime, site, and so on. • **View Assurance 360**: Displays the Assurance 360 window. For 360 to open, you must have installed the Assurance application. • **Interfaces** • **Ethernet Ports** (For all devices): Displays the operational status and administrative status of the Ethernet ports. For Cisco Catalyst 4000 Series, 6000 Series, and 9000 Series Switches and Aggregation Services Routers (ASR) 1000 Series Routers, the ports view displays the details of line cards and supervisor cards if they are available. The line card includes the details of platform, address, serial number, role, and stack member number. The supervisor card includes the details of part number, serial number, switch number, and slot number. The Ports table displays the operational status, admin status, type, MAC address, PoE status, speed, and MTU. The table also displays the ID of the following types of VLANs: • VLAN ID of the manufacturing-supplied default VLAN • VLAN ID of the configured default VLAN • VLAN ID of the configured VLAN For Cisco Catalyst 2000, 3000, and 9000 Series Switches, click either a port in the ports view or click the port name in the Ports table to view the maximum allocated power, allocated power, and power drawn details of the port. • **VLANs** (Only for switches and hubs): The VLAN table displays the operational status, admin status, VLAN type, and IP address. The table also displays the ID of the following types of VLANs: • VLAN ID of the manufacturing-supplied default VLAN • VLAN ID of the configured default VLAN • VLAN ID of the configured VLAN You can click the Search or Filter option to view the details of the desired VLAN. • **Virtual Ports** (Only for wireless devices, controllers, and routers): The ports table displays the operational status, admin status, type, MAC address, PoE status, speed, and MTU. You can click the Search or Filter option to view the details of the desired ports. • **Hardware and Software**: Displays the hardware and software details of the device. • **Configuration**: Displays detailed configuration information, similar to what is

Column	Description
	displayed in the output of the **show running-config** command. This feature is not supported for access points (APs) and wireless controllers. Therefore, configuration data is not returned for these device types. • **Power**: Displays details about the power budgeted for, power consumed by, and power remaining for the device. The Power Supplies table shows the operational status, serial number, and vendor equipment type details. • **Fans**: Displays the operational status, serial number, and vendor equipment type of fans. • **User Defined Fields**: Displays the user-defined fields associated with the device. • **Config Drift**: Displays the configuration changes and allows you to pick any two versions of the same device and compare their running configuration data. **Note** Running configuration data is not supported for devices such as wireless or legacy controllers. • **Wireless Info**: Displays the primary and secondary managed locations. • **Mobility**: Displays the mobility group name, RF group name, virtual IP, and mobility MAC address. **Note** A device name that is displayed in red means that inventory has not polled the device and updated its information for more than 30 minutes.
IP Address	IP address of the device.
Support Type	Shows the device support level as follows: • **Supported**: The device pack is tested for all applications on Cisco DNA Center. You can open a service request if any of the Cisco DNA Center functionalities for these devices do not work. • **Unsupported**: All remaining Cisco and third-party devices that are not tested and certified on Cisco DNA Center. You may try out various functionalities on Cisco DNA Center for these devices, as a best effort. However, we do not expect you to raise a service request or a bug if Cisco DNA Center features do not work as expected. • **Third Party**: Device pack is built by customers or business partners and goes through the certification process. Third party devices will support base automation capabilities such as Discovery, Inventory, Topology, and so on. Cisco TAC provides an initial level of support for these devices. However, if there is a problem with the device pack, you need to contact the business partner.

Column	Description
Reachability	The following is a list of the various statuses: • **Reachable**: The device is reachable by Cisco DNA Center using SNMP, HTTP(S), and NETCONF poll mechanisms. • **Ping Reachable**: The device is reachable by Cisco DNA Center using ICMP polling mechanism and not reachable using SNMP, HTTP(S), and Netconf poll mechanisms. • **Unreachable**: The device is not reachable using SNMP, HTTP(S), Netconf, and ICMP poll mechanisms.
Manageability	Shows the device status as follows: • **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. You can hover the cursor over the error message to view more details about the error and the impacted applications. • **Unmanaged**: Device cannot be reached and no inventory information was collected due to device connectivity issues.
MAC Address	MAC address of the device.
Image Version	Cisco IOS software that is currently running on the device.
Platform	Cisco product part number.
Serial Number	Cisco device serial number.
Uptime	Period of time that the device has been up and running.
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 Cisco DNA 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. Cisco DNA Center does not 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. The following device roles are available: • **Unknown** • **Access** • **Core** • **Distribution** • **Border Router**

Column	Description
Site	The site to which the device is assigned. Click **Assign** if the device is not assigned to any site. Click **Choose a Site**, select a site from the hierarchy, and click **Save**. For more information, see About Network Hierarchy, on page 36.
Last Updated	Most recent date and time that Cisco DNA Center scanned the device and updated the database with new information about the device.
Device Family	Group of related devices, such as routers, switches, hubs, or wireless controllers.
Device Series	Series number of the device; for example, Cisco Catalyst 4500 Series Switches.
Resync Interval	The polling interval for the device. This interval can be set globally in Settings or for a specific device in Inventory. For more information, see Cisco DNA Center Administrator Guide.
Last Sync Status	Status of the last Discovery scan for the device: • **Managed**: Device is in a fully managed state. • **Partial Collection Failure**: Device is in a partial collected state and not all the inventory information has been collected. Hover the cursor over the **Information (i)** icon to display additional information about the failure. • **Unreachable**: Device cannot be reached and no inventory information was collected due to device connectivity issues. This condition occurs when periodic collection takes place. • **Wrong Credentials**: If device credentials are changed after adding the device to the inventory, this condition is noted. • **In Progress**: Inventory collection is occurring.

Delete a Network Device

You can delete devices from the Cisco DNA Center database, as long as they have not already been added to a site.

When you remove a wireless sensor from the inventory, the sensor is reset to the factory defaults so that when it 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.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and 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 you can 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**.

Step 4 In the **Warning** window, check the **Config Clean-Up** check box to remove the network settings and telemetry configuration from the selected device.

Step 5 Confirm the action by clicking **OK**.

Add a Device to a Site

Adding devices to a site configures Cisco DNA Center as the Syslog an SNMP Trap Server, which enables Syslog Level 2 and configure global telemetry settings.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Provision** > **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.

Step 3 From the **Actions** menu, choose **Provision** > **Assign Device to Site**.
The **Assign Device to Site** slide-in pane appears.

Step 4 In the **Assign Device to Site** slide-in pane, click the link next to the icon for the device.
The **Choose a floor** slide-in pane appears.

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

Step 6 Click **Save**.

Step 7 (Optional) If you selected multiple devices to add to the same location, you can check the **Apply to All** check box for the first device to assign its location to the rest of the devices.

Step 8 Click **Assign**.

Step 9 When assigning devices to a site, if Device Controllability is enabled, a workflow is automatically triggered to push the device configuration from the site to the devices.
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.

About Cisco ISE Configuration for Cisco DNA Center

If your network uses Cisco ISE for user authentication, you can configure Cisco DNA 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. The workflow for configuring Cisco ISE is as follows:

1. In the Cisco DNA Center GUI, click the **Menu** icon (≡) and 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

Cisco DNA 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 Cisco DNA Center and Cisco ISE are integrated.
- If you are using another product (not Cisco ISE) to perform AAA functions, make sure to do the following:
  - Register Cisco DNA Center with the AAA server, including defining the shared secret on both the AAA server and Cisco DNA Center.
  - Define an attribute name for Cisco DNA Center on the AAA server.
  - For a Cisco DNA 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:
  1. You deployed Cisco ISE 2.3 or later in your network. If you have a multihost Cisco ISE deployment, integrate with the Cisco ISE admin node.
  2. SSH is enabled on the Cisco ISE node.
  3. The pxGrid service is enabled on the Cisco ISE host with which you plan to integrate Cisco DNA Center, and the ERS service is enabled for read/write operations.

Note Cisco ISE 2.4 and later supports pxGrid 2.0 and pxGrid 1.0. Although pxGrid 2.0 allows up to four pxGrid nodes in the Cisco ISE deployment, Cisco DNA Center does not currently support more than two pxGrid nodes.

  4. The Cisco ISE GUI and Cisco ISE shell username and passwords are the same.
  5. There is no proxy configured between Cisco DNA Center and Cisco ISE. If a proxy server is configured on Cisco ISE, the Cisco DNA Center IP address must bypass that proxy server.
  6. There is no firewall between Cisco DNA Center and Cisco ISE. If there is a firewall, open the communication between Cisco DNA Center and Cisco ISE.
  7. A ping between Cisco DNA Center and Cisco ISE succeeds with both the IP address and hostname.

8. The Cisco ISE admin node certificate contains the Cisco ISE IP address or FQDN in either the certificate subject name or the SAN.
9. If a certificate signed by your internal certificate authority (CA) is used, the certificate includes all IP addresses in the SAN field.
10. The pxGrid approval is set for automatic or manual approval in Cisco ISE to enable the pxGrid connection in Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers**.

Step 2 Click **Add**.

Step 3 Configure the primary AAA server by providing the following information:

- **Server IP Address**: IP address of the AAA server.
- **Shared Secret**: Key for device authentications. The shared secret can contain up to 100 characters.

Step 4 To configure a AAA server (not Cisco ISE), leave the **Cisco ISE Server** toggle to **Off** and proceed to the next step.

To configure a Cisco ISE server, set the **Cisco ISE server** toggle to **On** and enter information in the following fields:

- **Username**: Name that is used to log in to the Cisco ISE CLI.

  Note This user must be a Super Admin.

- **Password**: Password for the Cisco ISE CLI username.
- **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 the following format:

  hostname.domainname.com

  Example: The FQDN for a Cisco ISE server can be ise.cisco.com.

- **SSH Key**:

  The SSH key is a Diffie-Hellman crypto key in base64-encoded format. This key provides security for SSH connections to the Cisco ISE Administration console. You can retrieve the key with the Cisco ISE CLI command **show crypto authorized_keys** and **show crypto host_keys**.

- **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.

Note After the required information is provided, Cisco ISE is integrated with Cisco DNA 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** page and **System 360** page as follows:

Cisco ISE server registration phase:

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

pxGrid subscriptions registration phase:

- **Authentication and Policy Servers** page: "Active"
- **System 360** page: "Primary Available" and "PXGRID Available"

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

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

- **Protocol**: **TACACS** and **RADIUS** (the default). You can select both protocols.

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

- **Authentication Port**: Port used to relay authentication messages to the AAA server. The default is UDP port 1812.
- **Accounting Port**: Port used to relay important events to the AAA server. The information in these events is used for security and billing purposes. The default UDP port is 1813.
- **Port**: Port used by TACAS. Cisco DNA Center supports only port 49 for TACACS; do not change the port number.
- **Retries**: Number of times that Cisco DNA Center attempts to connect with the AAA server before abandoning the attempt to connect. The default number of attempts is 3.
- **Timeout**: Length of time the device waits for the AAA server to respond before abandoning the attempt to connect. The default timeout is 4 seconds.

Step 6 Click **Add**.

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

Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry

With Cisco DNA 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, the syslog server, the NetFlow Collector, or the wired client.

Before you begin

Create a site and assign a device to the site. See Create a Site in a Network Hierarchy, on page 37.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Telemetry**.

Step 2 Expand the **SNMP Traps** area if it is not visible and do one of the following:

a) Check the **Cisco DNA Center as SNMP trap server** check box.

b) 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 Expand the **Syslogs** area if it is not visible and do one of the following:

a) Check the **Use Cisco DNA Center as syslog server** check box.

b) Check the **Add an external syslog server** check box and enter the IP address of the external syslog server.

Step 4 Expand the **NetFlow** area if it is not visible and do one of the following:

a) Check the **Use Cisco DNA Center as NetFlow collector server** check box.

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.

b) Check the **Add an external NetFlow collector server** check box and enter the IP address and port number of the NetFlow Collector server.

The selected server is the destination server for NetFlow export from the network devices. If the NetFlow Collector is not selected, the application telemetry enablement will not work.

Step 5 Expand the **Wired Client Data Collection** area and check the **Monitor wired clients** check box.

This selection turns on IP Device Tracking (IPDT) on the access devices of the site.

By default, IPDT is disabled for the site.

Step 6 Expand the **Wireless Controller, Access Point and Wireless Clients Health** area and check the **Enable Wireless Telemetry** check box.

When selected, you can monitor the health of your network's wireless controller, access points, and wireless clients.

Step 7 Click **Save**.

Configure Cisco AI Network Analytics Data Collection

Use this procedure to enable Cisco AI Network Analytics to export network event data from wireless controllers as well as the site hierarchy to the Cisco DNA Center.

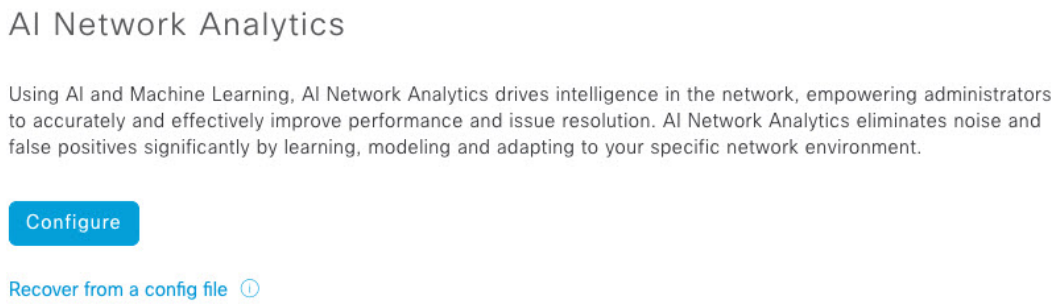
Before you begin

- Make sure that you have the Cisco DNA Advantage software license for Cisco DNA Center. The **AI Network Analytics** application is part of the Cisco DNA Advantage software license.

- Make sure that you have downloaded and installed the **AI Network Analytics** application. See the "Download and Install Packages and Updates" topic in the Cisco Digital Network Architecture Center Administrator Guide.
- Make sure that your network or HTTP proxy is configured to allow outbound HTTPS (TCP 443) access to the following cloud hosts:
  - **api.use1.prd.kairos.ciscolabs.com** (US East Region)
  - **api.euc1.prd.kairos.ciscolabs.com** (EU Central Region)

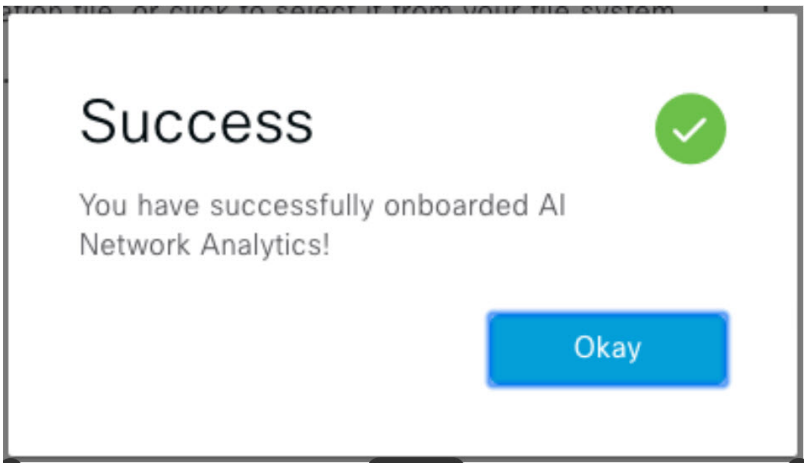
Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Settings**.

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



Step 3 Do one of the following:

- If you have an earlier version of Cisco AI Network Analytics installed in your appliance, do the following:
  a. Click **Recover from a config file**.
     The Restore AI Network Analytics window appears.
  b. Drag-and-drop the configuration files in the area provided or choose 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 appears.



- If this is the first time you are configuring Cisco AI Network Analytics, do the following:

  a. Click **Configure**.

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

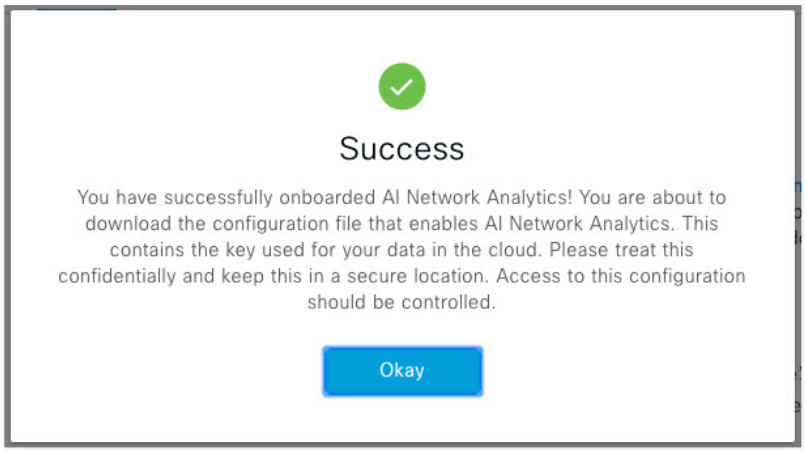
  The system starts testing cloud connectivity as indicated by the **Testing cloud connectivity...** tab. After cloud connectivity testing completes, the **Testing cloud connectivity...** tab changes to **Cloud connection verified**.

  c. Click **Next**.

  The terms and conditions window appears.

  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 appears.



Step 4 In the **Success** dialog box, click **Okay**.
The **AI Network Analytics** window appears, and the **Cloud Connection** area displays ☑.

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

Disable Cisco AI Network Analytics Data Collection

To disable Cisco AI Network Analytics data collection, you must turn off (disable) the connection to the Cisco AI Network Analytics cloud service. This will disable all of the Cisco AI Network Analytics-related features, such as AI-Driven Issues, Network Heatmap, Site Comparison, and Peer Comparison.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Settings**.

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

Step 3 In the **Cloud Connection** area, click the button to off, such that appears.

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 (Optional) 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 Cisco DNA Center to automatically update the Machine Reasoning Knowledge Base on a daily basis, or you can perform a manual update.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Settings**.

Step 2 Scroll down to **External Services** and choose **Machine Reasoning Knowledge Base**.
The **Machine Reasoning Knowledge Base** window shows the following information:

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

When there is a new update to the Machine Reasoning Knowledge Base, the **AVAILABLE UPDATE** area appears 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 Cisco DNA Center on a daily basis.

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 Cisco DNA Center is successfully connected to the Machine Reasoning Engine in the cloud.

Step 4 To manually update the Machine Reasoning Knowledge Base in Cisco DNA Center, do one of the following:

- 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 Cisco DNA Center. Do the following:

  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 Cisco DNA Center.

Enable Localization

You can view the Cisco DNA Center GUI screens in English (the default), Chinese, Japanese, or Korean.

To change the default language, perform the following task:

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

- From Google Chrome, do the following:

  a. Click the icon in the top-right corner, and then choose **Settings**.

  b. Scroll down and click **Advanced**.

  c. From the **Languages** > **Language** drop-down list, choose **Add languages**.

  The **Add languages** pop-up window appears.

  d. Choose **Chinese**, **Japanese**, or **Korean**, and then click **Add**.

- From Mozilla Firefox, do the following:

  a. Click the icon in the top-right corner, and then choose **Options**.

  b. From the **Language and Appearance** > **Language** area, choose **Search for more languages**.

  The **Firefox Language Settings** pop-up window appears.

  c. From the **Select a language to add** drop-down list, choose **Chinese**, **Japanese**, or **Korean**.

  d. Click **Ok**.

Step 2 Log in to Cisco DNA Center.

The GUI screens are shown in the selected language.

Figure 5: Example Localized Login Screen

Role-Based Access Control Support for Assurance

Assurance supports role-based access control (RBAC), which enables a user with SUPER-ADMIN-ROLE privileges to define custom roles that permit or restrict users access to certain Assurance features.

For more information see the "Manage Users" chapter in the *Cisco DNA Center Administrator Guide*.

Use this procedure to define a custom role and then assign a user to that role.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

Step 1 Define a custom role.

a) In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Users and Roles** > **Role Based Access Control**.

b) Click **+ Create New Role**.

The **Create a Role** window appears. After you create the new role, you are asked to assign users to the new role.

c) Click **Let's Do it**.

If you want to skip this screen in the future, check the **Don't show this to me again** check box.

The **Create a New Role** window appears.

d) Enter a name for the role and then click **Next**.
The **Define the Access** window appears with a list of options.

e) Click > next to **Assurance** to expand it.

The following options appear, which allow you to set **Deny**, **Read** (the default), or **Write** permissions for the new role.

- **Monitor and Troubleshooting**: Allows you to monitor your network using the following dashboards: Health, Issues, and Sensors. It also allows you to analyze trends and gain insights, and troubleshoot using the 360° views and issue details.

  If you set the permission level to **Deny**, the user to whom you assign this role cannot view any of the Assurance features.

- **Monitoring Settings**: Allows you to manage data retention and health settings.

  You must have System permissions to manage data retention settings.

- **Troubleshooting Tools**: Allows you to create and schedule sensor tests and manage Intelligent Capture settings.

f) Click **Next**.
The **Summary** window appears.

g) Review the summary. If the information is correct, click **Create Role**. Otherwise, click **Edit** and make the appropriate changes.
The **Done,** ***Role-Name*** window appears.

Step 2 To assign a user to the custom role you just created, click **Add Users**.

The **User Management** > **Internal Users** window appears, which allows you to assign the custom role to an existing user or to a new user.

- To assign the custom role to an existing user, do the following:
  1. In the **Internal Users** window, click the radio button next to the user to whom you want to assign the custom role, and then click **Edit**.

     The **Update Internal User** slide-in pane appears.

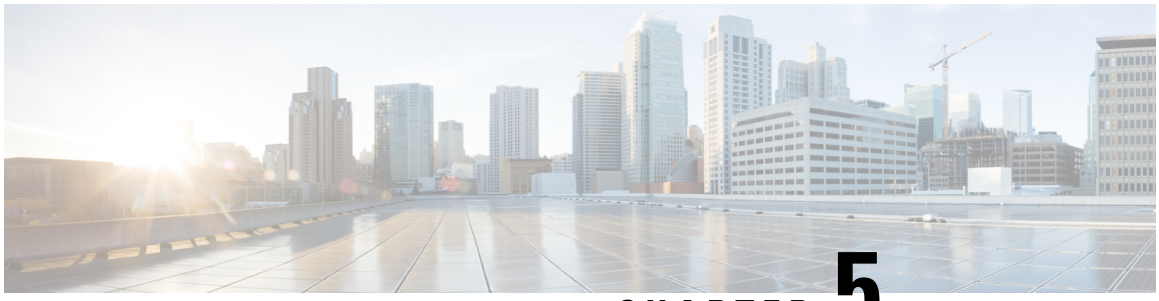
  2. From the **Role List** drop-down list, choose the custom role, and then click **Save**.

- To assign the custom role to a new user, do the following:
  1. Click **+ Add**, located on the top-right corner.

     The **Create Internal User** slide-in pane appears.

  2. Enter the first name, last name, and username in the fields provided.
  3. From the **Role List** drop-down list, choose the custom role to assign to the new user.
  4. Enter the password and then confirm it.
  5. Click **Save**.

Step 3 If you are an existing user who was logged in when the administrator was making changes to your access permissions, you must log out of Cisco DNA Center and then log back in for the new permission settings to take effect.



CHAPTER 5

Monitor and Troubleshoot Overall Enterprise Health

- About Enterprise, on page 73
- Monitor and Troubleshoot the Overall Health of Your Enterprise, on page 73

About Enterprise

You can use Assurance to monitor and troubleshoot the overall health of your enterprise. An 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 are not a 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). Cisco DNA 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.

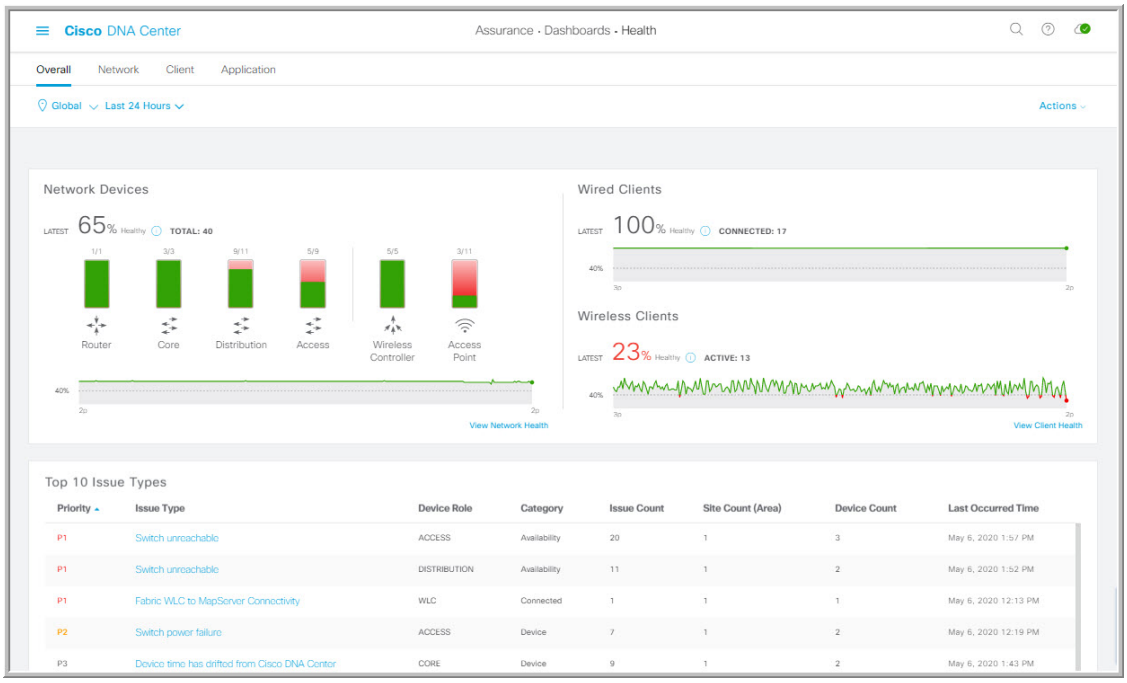
Before you begin

Configure Assurance. See Basic Setup Workflow, on page 13.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Figure 6: Overall Health Dashboard



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

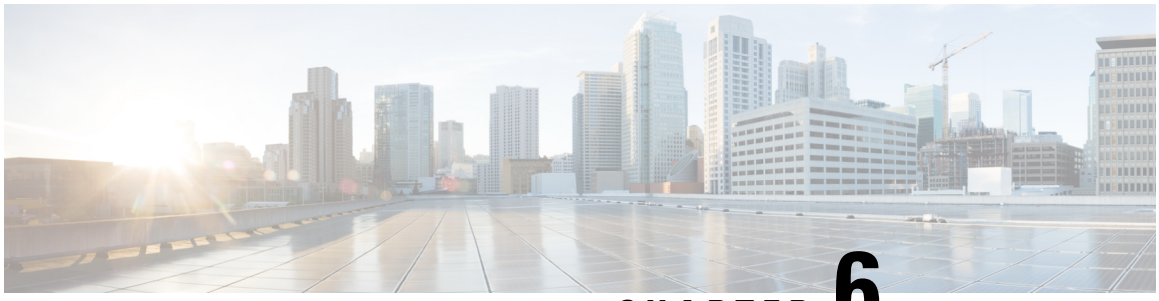
Overall Health Dashboard Top-Menu Bar	
Item	**Description**
Global **Location** pane	Click to display the following icons: • : Click this toggle button and use the drop-down list to select **Hierarchical Site View** or **Building View**. Based on what you choose, the table displays the percentage of 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.
Time range	Enables you to display data for the last 3 hours, 24 hours, or 7 days.
Actions drop-down list	Enables you to customize the dashboard display when you choose **Edit Dashboards** from the drop-down list. See Change the Position of a Dashlet, on page 235 and Create a Custom Dashboard, on page 231.

Step 3 Use the **Overall Health Summary** dashlet for the following 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 102. **Device Category Health Score**: Percentage of healthy (good) network devices for the following device categories: **Router**, **Core**, **Distribution**, **Access**, **Controller** and **Access Point**. **Note** When a **Fabric Domain** is selected, this area provides percentage of healthy network devices for the following 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 77.
Wired Clients and **Wireless Clients**	Provides 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 126. Click **View Client Health** to open the **Client Health** dashboard. See Monitor and Troubleshoot the Health of All Client Devices, on page 109.

Step 4 Use the **Top 10 Issue Type** dashlet for the following 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 the following, as required: • To resolve the issue instance, from the **Status** drop-down list, choose **Resolve**. • To ignore the issue instance: **a.** From the **Status** drop-down list, choose **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 150.



CHAPTER 6

Monitor and Troubleshoot Network Health

- About Network, on page 77
- Monitor and Troubleshoot the Health of Your Network, on page 77
- Monitor and Troubleshoot the Health of a Device, on page 85
- Configure Health Score Settings for Network Devices, on page 97
- Fabric Domains, on page 97
- Enable SNMP Collector Metrics for Fabric Devices, on page 100
- Understand Network Health Score and KPI Metrics, on page 101

About Network

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

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. Note that clients are not a part of the network health score.

Note 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.

Before you begin

Configure Assurance. See Basic Setup Workflow, on page 13.

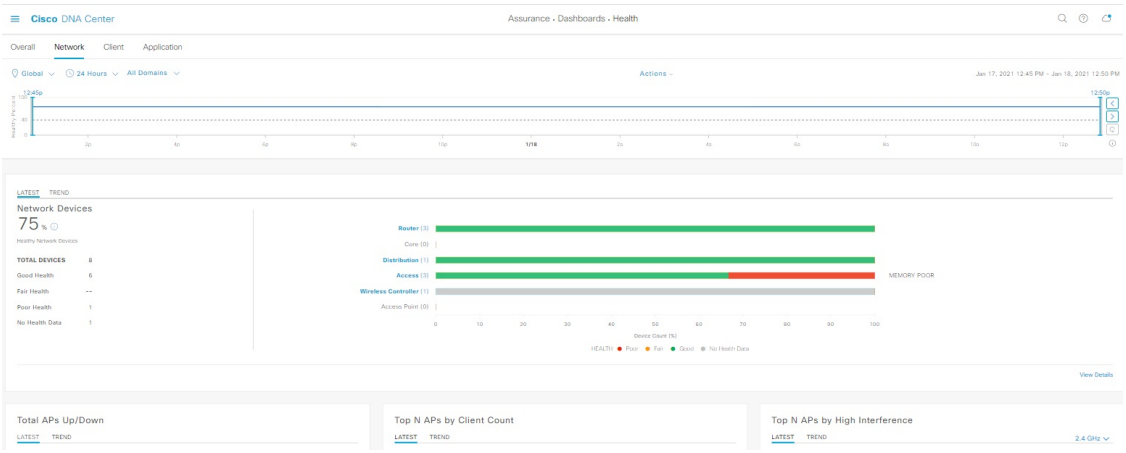
Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Network** tab.

The **Network** health dashboard appears.

Figure 7: Network Health Dashboard



Step 3 Click the location option (Global) in the top-menu bar to display the location pane.

The location pane has the following 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 the following options: • **Hierarchical Site View**: Sorts the list at a site level. From the **Apply to Page Location** column, click **Apply** for a site or building to display data only for that location on to the **Network** dashboard. • **Building View**: Sorts the list at a building level. From the **Apply to Page Location** column, click **Apply** for a building to display data only for that building on to the **Network** dashboard. **Note** For **Fabric Domains**, you must select a site or building from the **All Domains** drop-down list and not from the **Hierarchical Site View** and **Building View** areas.
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 that are represented are color-coded according to the severity of the problem.

Location Option	
Item	**Description**
Topology tool	Click this icon to open the **Topology** tool. The **Topology** window, has the following views: • **Geographical View**: Click this toggle button to display your network in a geographical map. Hover your cursor over a location to view the percentage of healthy devices. • **Topology View**: Click this toggle button to display a topology of how the components in the network are connected. Hover your cursor over a device to display device information, such as device role, IP address, and software version. To obtain a 360° view of the device, click **View Details 360**.

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, choose 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 **All Domains** setting in the top-menu bar for the following options:

- **All Domains**: Displays information for all domains or fabric domain. Default is **All Domains**.
- **Fabric Domains**: To view information about a fabric domain, from the **All Domains** drop-down list, choose the appropriate option. For multisite fabrics, the sites connected to the fabric domain and the transit area are provided in the drop-down list.

  For **Fabric Domains**, you must select a site or building from the **All Domains** drop-down list and not from the **Hierarchical Site View** and **Building View** areas.

  To monitor and troubleshoot fabric domains, you must first configure the fabric domain. See Create a Fabric Domain, on page 98 and Add a Device to a Fabric, on page 98.

  For additional details and to understand multisite fabric domains, see the "Provision Your Network" chapter in the Cisco Digital Network Architecture Center User Guide.

  Note Subtended and Extended nodes are not part of fabric health because during Fabric Provisioning, these nodes were not given a fabric role, such as Edge, Border, or Control Plane.

Step 6 Click the **Actions** drop-down list in the top-menu bar for the following functionality:

- **Edit Dashboard**: Enables you to customize the dashboard display. See Change the Position of a Dashlet, on page 235 and Create a Custom Dashboard, on page 231.

Step 7 Use the **Network Health** timeline for the following functionality:

Enables you to 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**.

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.

Step 8 Use the **Network Devices Health Summary** dashlet for the following functionality:

Network Devices Health Summary Dashlet	
Item	**Description**

Network Devices Health Summary area	Includes two tabs:
	• **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.
	  • **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 102.
	  • **Total Devices**: Provides the total number of network devices and the count of devices which has 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 provided adjacent to the bar. For example, link errors, high CPU, high memory, high noise, low air quality, and so on.
	  For Fabric Domains, the KPIs that contributed to the low health score are provided adjacent to bar. For example, Fabric CP reachability, Multicast RP, AAA Server Status.
	  You can also click a hyperlinked device category (**Access**, **Core**, **Distribution**, **Router**, **Wireless Controller**, and **Access Point**) to open a side pane with additional details.
	  Note For **Fabric Domains**, the color-coded percentage chart shows the performance of the following fabric categories: **Fabric Edge**, **Fabric Border**, **Fabric Control Plane**, **Fabric Wireless**, **Fabric WLC**, **Fabric AP** and **Extended Node**.
	• **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. Health score is 0.

Network Devices Health Summary 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 refresh the data in the table that is displayed below the chart.

Step 9 Use the AP dashlets to view the following information:

Total APs Up/Down Dashlet
Color-coded chart that provides the 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 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 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 choose 2.4 GHz or 5 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 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 the following functionality:

Network Devices Dashlet	
Item	**Description**
Type	Filter the table based on the device type with the following options: **All**, **Access**, **Core**, **Distribution**, **Router**, **WLC**, and **AP**. For SDA Fabric Domain, filter the table based on the fabric type with the following options: **All,** , **Fabric Control Plane**, **Fabric Border**, **Fabric Edge**, **Fabric WLC**, **Fabric AP**, **Extended Node**.
Overall Health	Filter the table based on the overall health score of the device with the following 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 sub-score of the following 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, the following 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 displays the fabric domain name, fabric name and fabric role (Edge, Border, Map Server and so on). The **Reachability** column displays the status of the device (Reachable, Up, Unreachable, Rebooting, and so on).
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.
Export	Click **Export** to export the device information to a CSV file.

Network Devices Dashlet	
Item	**Description**
	Customize the data 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**.

Step 11 Use the Network Devices Reachability dashlet to view the following information:

Network Devices Reachability Dashlet
Color-coded chart shows the information about the devices reachability status of Router, 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 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 the network devices 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 proceeding table based on the reachability status, devices types and location with the following options: All, Access, Core, Distribution, Router and WLC.

Step 12 Use the WAN Link Utilization dashlet to view the following information:

WAN Link Utilization Dashlet
The bar chart shows the status of the WAN link utilization percentage only for the available WAN links. The **Latest** tab provides 10 minutes 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 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 chart to view more detailed data. You can select the data displayed as horizontal bars below the timeline slider to filter the proceeding table based on Top locations, device types and location.

Step 13 Use the WAN Link Availability dashlet to view the following information:

WAN Link Availability Dashlet
Color-coded chart displays the information on the available WAN links in your network. The **Latest** tab provides percentage of WAN links utilized. 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 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 chart to view more detailed data. You can select the data displayed as horizontal bars below the timeline slider to filter the proceeding table based on Top locations (link count), 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.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Network** tab.

The **Network** health dashboard appears.

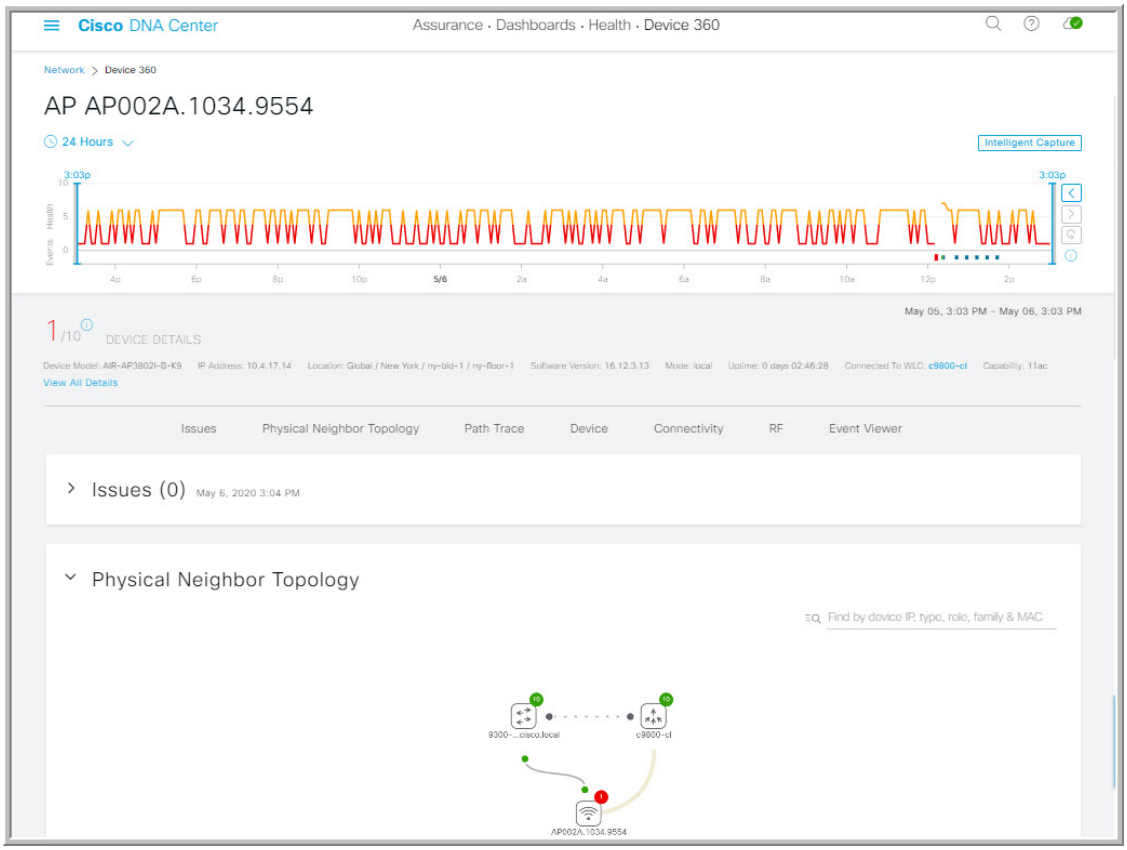
Step 3 Do one of the following:

- In the **Network Devices** dashlet, click a device name in the **Device Name** column.
- In the **Search** field (located at the top-right corner), enter the device name, IP address, or MAC address.

The **Device 360** window appears which displays a 360° view of the network device.

Note The **Map View** appears by default.

Figure 8: Device 360 Window



Step 4 Click the time range setting (24 Hours) at the top-left corner to specify the time range of data that is displayed on 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 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 network device and to determine if there are potential issues that must be addressed. See View RF Statistics and Manage Spectrum Analysis Data for an Access Point, on page 270.

Note Intelligent Capture is not supported for all 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. The timeline slider has the following functionality:

- **Health**: You can hover your cursor over the timeline slider to view the client's 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 brings the timeline slider to a 1-hour time period.

  Note If you want to display information longer than 1 hour, manually move the timeline slider to the desired time range.

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. Note that the timestamp next to each category (**Issues**, **Connectivity**, and so on) is also refreshed.

- **Events**: 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.

Step 7 You can view the device's health score in the **Device Details** area, below the timeline.

The details for the device's health score is as follows:

- **Switch**: The health score for switches is the minimum subscore of the following parameters: memory utilization, CPU utilization, link errors, link discards, uplink availability, and reachability to control plane. In addition, for fabric devices, it includes connectivity to the Control Plane node. For more information, see Switch Health Score, on page 103.

  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 95.

  Cisco StackWise: Uplink availability is based on infrastructure links, and Cisco StackWise links. See About Cisco StackWise and Its Limitations, on page 96.

- **Router**: The health score for routers is the minimum subscore of the following parameters: memory utilization, CPU utilization, link errors, link discards, uplink availability, and reachability to control plane. For more information, see Router Health Score, on page 104.

  Note Uplink availability is based on infrastructure links.

- **AP**: The health score for APs is the minimum subscore of the following parameters: memory utilization, CPU utilization, link errors, radio utilization, interference, noise, and air quality. For more information, see AP Health Score, on page 105.

- **Wireless Controller**: The health score for WLCs is the minimum subscore of the following parameters: memory utilization, free timers, free memory buffers (MBufs), work queue element (WQE) pools, packet pools, link errors. For fabric wireless controllers, it includes connection to the Control Plane node. For more information, see Wireless Controller Health Score, on page 106.

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.

- : 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. 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**, the following elements are displayed in the device details area: **Fabric Role**, **Fabric Domain**, and **Fabric Site.**

For **Cisco StackWise Virtual**, two additional elements are displayed: **Stack Status: StackWise Virtual** and **StackWise Virtual Domain**.

For **Cisco StackWise** an additional element is displayed: **StackWise** along with the number of switches in the stack, for example **StackWise (2)**. A stack can contain a maximum of eight switches.

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.

Step 10 Use the **Issues** category for to view 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 the following:

- To resolve an issue:
  a. From the drop-down list, choose **Resolve**.
  b. Click **Resolved Issues** to view the list of issues that are resolved.
- To ignore an issue:
  a. From the drop-down list, choose **Ignore**.
  b. Set the number of hours to ignore the issue on the slider.
  c. Click **Confirm**.
  d. Click **Ignored Issues** to view the list of 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 the following:

- Click a node to display a slide-in window 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** 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.

  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.

Note For Fabric domain, the fabric groups are displayed with a Fabric Badge icon (<< fabric bage icon to be placed here>>>)

Note 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 View** category to view the audit trail of events for the device:

- **For APs**: Lists scenarios and the sequence of sub-events that led to each scenario. This allows you to pin-point during which sub-event an issue occurred. Radio resource management (RRM) events such as Transmit Power Change, RF Channel Change, Radio Reset, and so on are displayed.

  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.

- **For Switches and Routers**: All syslogs that have a severity of Error and above (Emergency, Alert, and Critical), events for any links that are up or down, and events for devices that are reachable or unreachable are recorded in the Event Viewer. Only a selected list of syslogs that are less severe than Error level (Warning, Notice, and Info) are also displayed. For the list of selected syslog messages that are displayed, see Selected Syslogs Below Error Level for Switches and Routers, on page 94. Click an event to view details about that event in the right pane.

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 Perform a Path Trace, on page 279.

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, in the table. A slide-in pane opens with the relevant information.

See About Application Experience and Application Visibility, on page 129 and View Application Experience of a Host, on page 136.

Note This category is displayed for routers only.

Step 15 Use the **Detail Information** category to view the device's historical KPIs performing over a period of time.

Click the following tabs to view its respective details:

Device Info Tab
Device details, such as CPU, memory, uptime, and so on are displayed. **Note** 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 choose a 3-hour window, 11:00 am – 2:00 pm (in the timeline slider), the downtime is not displayed. This issue occurs because Cisco DNA Center is not able to receive the sys uptime information from the device. To workaround this issue, synchronize the configuration between the device and Cisco DNA Center.

Connectivity Tab

Information about the health of a device's connection with the network is displayed. This tab is available for APs.

- **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 adjacent to the interfaces on the right of the chart. Based on the interfaces you choose, the error percentage for each of the 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 choose a maximum of five interfaces.

- **Ethernet Interface KPI**: Displays the Utilization, Error and Rate shows Tx, Rx, and Total values as applicable.

  Also it summarizes the total and average values for the above KPIs aggregated for a time range selected on the top of AP 360.

- **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 network devices, such as switches, routers, wireless controllers, and APs.

RF Tab

This tab is available for APs and wireless clients.

- The RF tab contains Radio tabs, such as Radio 0, Radio 1, and Radio 2. Click the appropriate Radio tab to display charts for radio channel utilization, interference, noise, air quality, air-time efficiency, wireless latency by client distribution, and so on.

Note **RF Tab Limitation**

When an AP with three radios (for example a Cisco Catalyst 9130 AP) connects to a 17.2+ version of wireless controller, 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 17.1 or older version of wireless controller, the device supports two radios, and two radios (Radio 0 and Radio 1) are displayed under the RF tab.

But if an AP moves from a newer to an older version of wireless controller (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 radio, a DFS tab is displayed that provides information about Dynamic Frequency Selection (DFS) radar events.

Interfaces Tab

Contains the following PORT TYPE tabs: **All**, **Access**, **Auto**, **Routed**, and **Trunk**. Based on the tab you click, the table is refreshed.

Note **Cisco StackWise Virtual**: The **Interfaces** tab contains two additional PORT TYPE tabs: **SVL** and **DAD**.

Cisco StackWise: The **Interfaces** tab contains an additional PORT TYPE tab: **StackWisePort**.

Table with interface information such as the name, description, operational status, link speed, and so on is displayed. The interface table columns are sortable. However, if you try to sort the 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 then that negotiated speed is displayed.

To display the operational status about the interfaces for a particular day and time in a chart format, check the check boxes adjacent to the interfaces. The **Interface Availability**, **Utilization**, **Error**, and **Link Discard** charts are displayed below the table. You can choose a maximum of five interfaces. The first interface in the table is selected by default.

Note 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.

Fabric Tab

This tab is available for fabric domains. Fabric KPIs are grouped under different categories **Fabric Infrastructure** (Control Plane reachability) and **VN Service** (Control Plane, Multicast RP and so on.) charts are displayed. You can filter based on these categories to view the table with reachability information such as the destination, IP address, type is displayed. Check the checkbox adjacent to destination to view the status charts.

Note The uplink status chart shows data only if the Fabric Underlay Automation is used to provision the fabric.

PoE Tab
Displays the device's Power over Ethernet (PoE) telemetry.This tab is available for PoE-capable 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 in the table format which displays 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 supplies power for PoE. The **PoE Interfaces** section lists the PoE-capable devices connected to the switch's interfaces in a table format. At the top of the section is a count of interfaces which are currently off. You can customize the table by doing the following: • Use the **POE CONFIG**, **ADMIN STATUS**, and **POE OPER STATUS (SIGNAL PAIR)** filters above the table to filter the interfaces that are displayed in the table based on the filter's selected value. • Use the search bar to perform searches for specific interfaces, PoE-capable devices, or any other values from the table's columns. • Click ⋮ to open a menu where you can add and remove columns for specific data types.

StackWise Virtual Tab
Table with information about the Cisco StackWise Virtual, such as the serial number, product ID, MAC address, role, state, priority, uptime, and port numbers is displayed. This tab is available for Cisco StackWise Virtual.

StackWise Tab
Table with information about the Cisco StackWise, such as the serial number, product ID, MAC address, role, state, priority, and the neighboring switch number is displayed. This tab is available for Cisco StackWise.

Step 16 To compare the health of access point (AP) radios across the floor in a building click the toggle button in the top-right corner to switch between the **Map 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 Floor** drop-down list in the top-left corner, choose 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 such **MAC Address**, **Model**, **Mode**, and **Issue Count** of an AP radio.

Step 18 Click the **Compare AP Radios** to compare the AP radios on the floor map.

The **Map View** appears by default..

Note The **Map View** displays 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, Cisco DNA 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 5 AP radios at a time for comparison.

Step 21 Use the **AP Radio Comparison** area to view the list of AP radios selected for comparison.

Cisco DNA Center allows you to compare **Radio**, **IP Address**, **Model**, **Uptime**, **Connected to WLC**, and **Floor**.

Step 22 Use the **Comparative Metrics** to view the comparative metrics for the selected key performance indicators (KPIs).

Step 23 From the **Select KPI** drop-down list choose the KPIs for which you want to see the comparative matrices.

Cisco DNA Center allows you to select the following KPIs:

- Channel Information
- Traffic (Rx Rate)
- Connected Client Count
- Radio Retries
- Channel Utilization
- Interference
- Noise
- Air Quality
- Wireless Latency by Client Count
- Management Frames
- Data Frames
- Tx Errors
- Rx Errors
- Tx Power
- Multicast Counter

Step 24 Click the toggle button to switch between the **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 from comparison.

Selected Syslogs Below Error Level for Switches and Routers

The following tables provide the selected list of syslog messages, less than Error level (Warning, Notice, and Info), that are displayed in the **Event Viewer** from the **Device 360** window:

Protocol Events	Layer 2 Events
OSPF-5-ADJCHG	SW_MATM-4-MACFLAP_NOTIF
IFDAMP-5-UPDOWN	MAC_LIMIT-4-PORT_EXCEED
BGP-5-ADJCHANGE	MAC_LIMIT-4-VLAN_EXCEED
DUAL-5-NBRCHANGE	IGMP-6-IGMP_GROUP_LIMIT
BGP-5-ADJCHANGE-bfd	SPANTREE-5-ROOTCHANGE
CLNS-5-ADJCHANGE	UDLD-4-UDLD_PORT_DISABLED
LDP-5-NBRCHG-TDP	PM-4-ERR_DISABLE
LDP-5-NBRCHG-LDP	CDP-4-DUPLEX_MISMATCH
CDP-4-NATIVE_VLAN_MISMATCH	LINK-5-CHANGED
LISP-4-LOCAL_EID_RLOC_INCONSISTENCY	PORT-5-IF_DOWN
LISP-4-LOCAL_EID_NO_ROUTE	PORT-5-IF_UP
LISP-4-CEF_DISABLED	
LISP-4-LOCAL_EID_MAP_REGISTER_FAILURE	
LISP-4-MAP_CACHE_WARNING_THRESHOLD_REACHED	

Hardware Platform Events
SYS-5-CONFIG_I
SYS-5-RELOAD
SYS-5-RESTART
OIR-6-INSCARD
OIR-6-REMCARD
OIR-SP-6-INSCARD
OIR-SP-6-REMCARD
PLATFORM_STACKPOWER-6-CABLE_EVENT
PLATFORM_STACKPOWER-6-LINK_EVENT
PLATFORM_STACKPOWER-4-TOO_MANY_ERRORS
PLATFORM_STACKPOWER-4-VERSION_MISMATCH
PLATFORM_STACKPOWER-4-UNDER_BUDGET
PLATFORM_STACKPOWER-4-INSUFFICIENT_PWR
PLATFORM_STACKPOWER-4-REDUNDANCY_LOSS
ILPOWER-5-POWER_GRANTED
ILPOWER-5-LINKDOWN_DISCONNECT
ILPOWER-5-IEEE_DISCONNECT
ILPOWER-5-INVALID_IEEE_CLASS
ILPOWER-4-LOG_OVERDRAWN
ILPOWER-5-CLR_OVERDRAWN

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

The following 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 the following 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 the following:
  1. Delete both the switches from the inventory. See Delete a Network Device, on page 61.
  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, on page 24, Discover Your Network Using CDP, on page 18, or Discover Your Network Using LLDP, on page 29.

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 the following:
  1. Configure a different IP address on the second switch.
  2. Rediscover the devices. See Discover Your Network Using an IP Address Range, on page 24, Discover Your Network Using CDP, on page 18, or Discover Your Network Using LLDP, on page 29.

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

The following 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 the following 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.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Manage** > **Health Score Settings**.

The **Health Score** window appears.

Step 2 Click the tab of the network device category to customize its health score calculation settings.

The tab displays the KPIs that affect the network device type's health score calculation.

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.

c) To remove the KPI from the health score calculation, uncheck the **Included in Device health Score** check box.

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 is displayed.

Fabric Domains

A fabric is a logical group of devices that is managed as a single entity in one or multiple locations.

About Fabric Networks

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.

Cisco DNA 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.

Create a Fabric Domain

Cisco DNA Center creates a default fabric domain called *Default LAN Fabric*.

Before you begin

Ensure that your network has been designed, the policies have been retrieved from the Cisco Integrated Services Engine (ISE) or created in the Cisco DNA Center, and the devices have been inventoried and added to the sites.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Fabric**.

Step 2 Hover the mouse pointer over **Add Fabric or Transit/Peer Network**.

Step 3 Click **Add Fabric** from the pop-up.

Step 4 Enter a fabric name.

Step 5 Choose one fabric site.

Step 6 Click **Add**.

Add a Device to a Fabric

After you have created a fabric domain, you can add fabric sites, and then add devices to the fabric site. You can also specify whether the devices 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.

A device which is assigned the Access role and has been provisioned before enabling IPDT on the site cannot 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 is optional to designate the devices in a fabric domain as control plane nodes or border nodes. You might have devices that do not occupy these roles. However, every fabric domain 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.

Before you begin

Provision the device if you have not already provisioned it:

1. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.
2. The **Inventory** window displays the discovered devices.
3. The topology view shows a device in gray color if it has passed the fabric readiness checks and is ready to be provisioned.
4. 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.
5. If you update the device configuration as part of problem resolution, ensure that you resynchronize the device information by performing an **Inventory** > **Resync** for the device.

Note You can continue to provision a device that has failed the fabric readiness checks.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Fabric**.
The window displays all the provisioned fabric domains.

Step 2 From the list of fabric domains, choose a fabric.
The resulting screen displays all the sites in that fabric domain.

Step 3 Choose a site.

All devices in the network that have been inventoried are displayed in the topology view. Any device that is added to the fabric is shown in blue.

Step 4 In the List view, click a device. The device details window slides in with the following **Fabric** options:

Option	Description
Edge	Click the toggle button next to this option to enable the selected device as an edge node.
Border	Click the toggle button next to this option to enable the selected device as a border node.
Control Plane	Click the toggle 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**, **Border**, and **Edge** options.

To configure the device as a control plane and a border node, select both **Control Plane** and **Border**.

Step 5 Click **Add**.

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.

Enable SNMP Collector Metrics for Fabric Devices

For the health score to populate correctly for fabric devices, you must enable the SNMP Collector metrics.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Data Platform**.

Step 2 Click **Collectors**.

A list of collectors is displayed.

Step 3 Click **COLLECTOR-SNMP**.

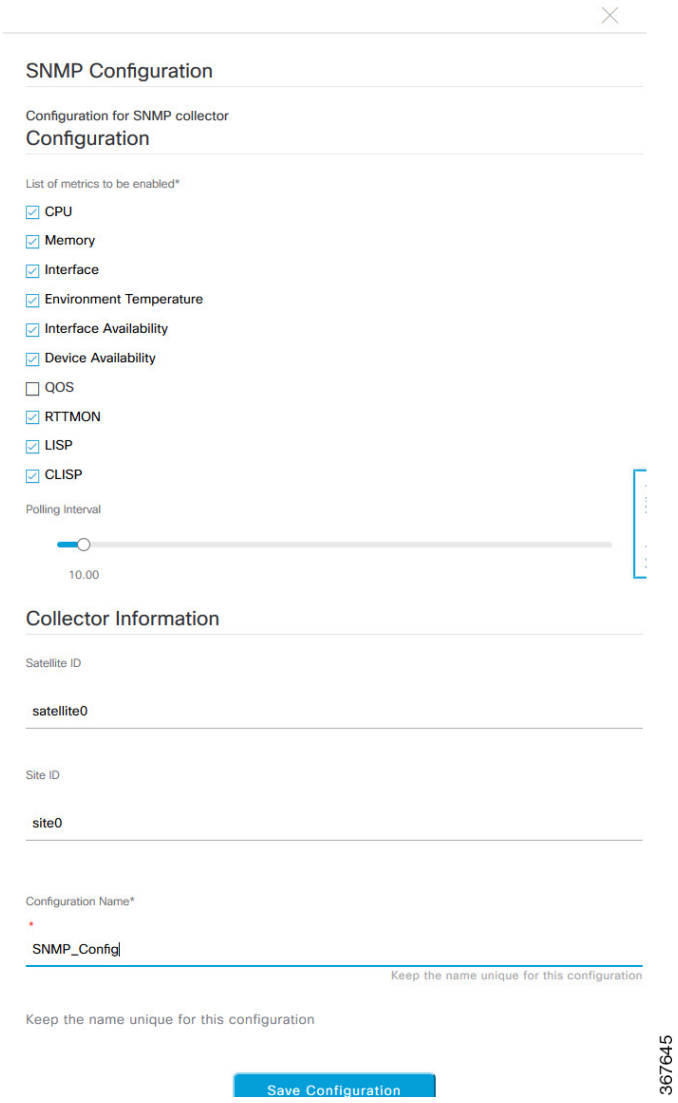
The **COLLECTOR-SNMP** window opens.

Step 4 Click + **Add**.

The **SNMP Configuration** dialog box opens.

Step 5 Check the check boxes adjacent to all the metrics except QOS.

Figure 9: 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. 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)

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. 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)

Individual Device Health Score

The Individual Device Health score is the minimum score of following 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 the following system-monitoring metrics: • For wireless controllers, it includes memory utilization, free timers, and free Mbufs. • For AP, 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.

Data Plane Connectivity	
Device Type	**Description**
Wireless	Includes the following metrics: • For wireless controllers, it includes metrics, such as WQE pool, packet pools, and link errors. • For AP, it includes RF metrics, such as interface, noise, air quality, and radio utilization.
Router	Includes metrics, such as link errors.

Control Plane Connectivity	
Device Type	**Description**
Wireless	Includes the following 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 the following parameters:

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 between 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, it is 1, otherwise it is 10.
Link Discards	Only infrastructure links are considered for link discards. Infrastructure links are topological links between 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, it is 1, otherwise it is 10.

Parameter	Score Calculation
Link Status	Only infrastructure links are considered for link status UP/DOWN. Infrastructure links are topological links between 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, it is 1, otherwise it is 10.
Connection 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 1 Control Plane node in a fabric domain, and all the Control Plane nodes are reachable, the score is 10; otherwise, the score is 1. **Note** For the health score to populate correctly for fabric devices, enable SNMP Collector metrics. See Enable SNMP Collector Metrics for Fabric Devices, on page 100.

Router Health Score

The Router Health score is the minimum subscore of the following parameters:

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.
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 between 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, it is 1, otherwise it is 10.
Link Discards	Only infrastructure links are considered for link discards. Infrastructure links are topological links between 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, it is 1, otherwise it is 10.

AP Health Score

The AP Health score is the minimum subscore of the following parameters:

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 the average radio score is determined. • 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 the average radio score is determined. 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 0. For 5-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 0.
RF Noise Score	The score is calculated individually for each radio, and then the average radio score is determined. For 2.4-GHz radio: • If RF noise is less than -81dBm, the score is 10. • If RF noise is -81dBm or more, the score is 0. For 5-GHz radio: • If RF noise is less than -83dBm, the score is 10. • If RF noise is -83dBm or more, the score is 0.

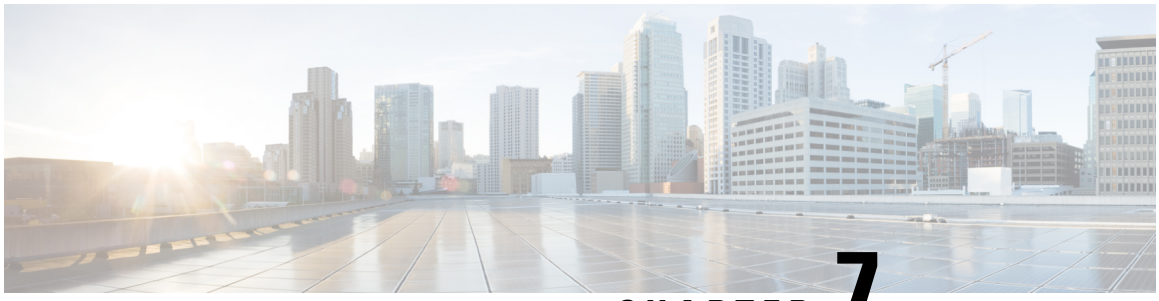
Parameter	Score Calculation
Air Quality Score	The score is calculated individually for each radio, and then the average radio the score is determined. For 2.4-GHz radio: • If air quality is 60 percent or more, the score is 10. • If air quality is less than 60 percent, the score is 0. For 5-GHz radio: • If air quality is 75 percent or more, the score is 10. • If air quality is less than 75 percent, the score is 0.

Wireless Controller Health Score

The Wireless Controller Health score is the minimum subscore of the following parameters:

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.
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.

Parameter	Score Calculation
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 domain, and all the Control Plane nodes are reachable, the score is 10; otherwise, the score is 1.



CHAPTER 7

Monitor and Troubleshoot Client Health

- About Clients, on page 109
- Monitor and Troubleshoot the Health of All Client Devices, on page 109
- Monitor and Troubleshoot the Health of a Client Device, on page 120
- Understand Client Health Score and KPI Metrics, on page 126

About Clients

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

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). Cisco DNA Center supports both wired and wireless clients.

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.

Before you begin

Configure Assurance. See Basic Setup Workflow, on page 13.

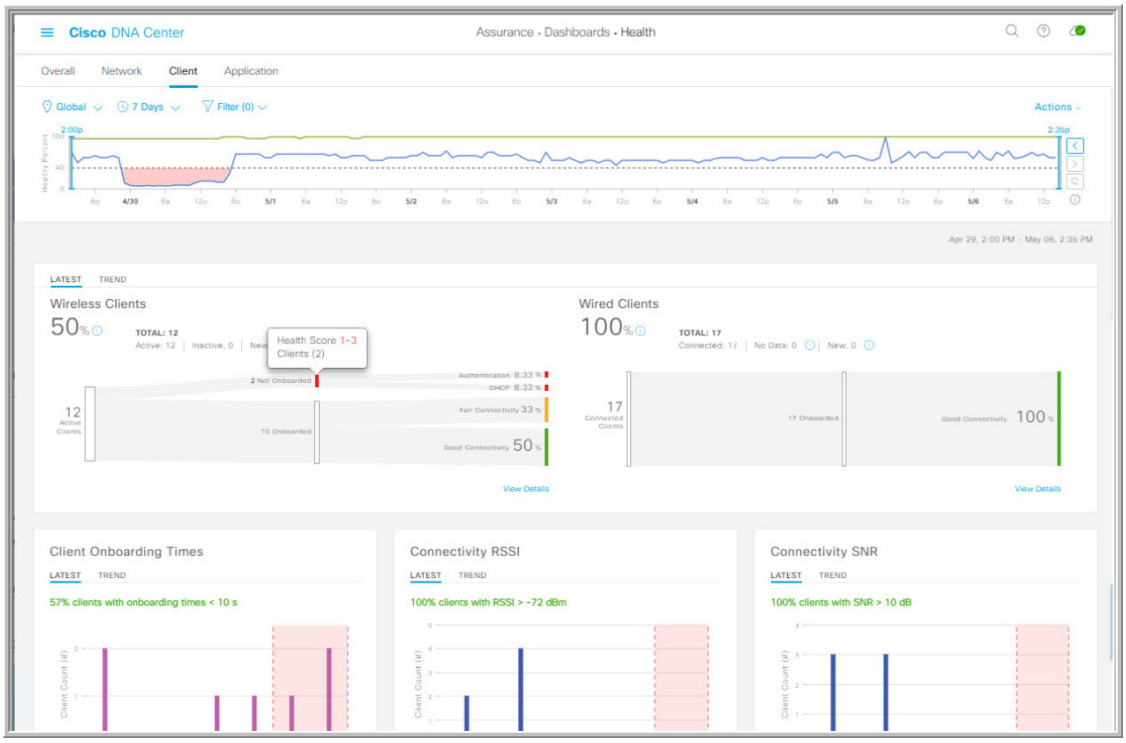
Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Client** tab.

The **Client** health dashboard appears.

Figure 10: Client Health Dashboard



Step 3 Use the **Client** health dashboard top-menu bar for the following functionality:

Client Health Dashboard Top-Menu Bar	
Item	**Description**
Global **Location** pane	Click to display the following icons: • : Click this toggle button and use the drop-down list to view the percentage of healthy clients in a table format for a site or building. Click **Apply** for a location to only display the location's client information in the **Client Health** dashboard. • : Click this toggle button to display the health of all the client sites on a geographic location-oriented client health map. By default, the client 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, with 10 being the best score, and a score of 0 indicating that the client is inactive.
Time Range setting	Enables you to display data within a specified time range on the dashboard. Do the following: **a.** From the drop-down menu, choose 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**.

Client Health Dashboard Top-Menu Bar	
Item	**Description**
Filter icon	Contains the **SSID** and **Band** options. Choose 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. **Note** You can choose multiple SSIDs. For example, if you choose Class 1 and Class 2 SSIDs, the dashboard will display information for the clients that are connected to Class 1 SSID and Class 2 SSID.
Actions drop-down list	Enables you to customize the dashboard display when you choose **Edit Dashboards** from the drop-down list. See Change the Position of a Dashlet, on page 235 and Create a Custom Dashboard, on page 231.

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 the following functionality:

Client Health Summary Dashlet	
Item	**Description**
Client Health Summary area	Includes two tabs: • **Latest**: Displayed by default. Includes the following: • **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 126. • **Total Devices**: Provides the total number of clients and the count of active, inactive, and new clients. Cisco DNA 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. This trend chart shows the health of clients over a time period. For the clients that failed to onboard, the reason for the onboarding failure is provided. For example, AAA, DHCP, Other, and so on. The color in the charts represent 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.
View Details	Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a segment in the chart to view: • Data type categories by client count for that segment. • A table with detailed data of the clients in that segment.

Step 6 Use the KPI dashlets to view specific KPIs and metrics for the clients on your network. The following 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 was 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 Data Collection, on page 66 and Cisco AI Network Analytics Overview, on page 9. **Important** To view the baseline chart, you must choose 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. For example, AAA, DHCP, Other, and so on.

Client Onboarding Times Dashlet	
Item	**Description**

View Details	Click **View Details** to open a slide-in pane with additional details:
	• Left pane contains the **Overall**, **Association**, **Authentication** and **DHCP** tabs. Click the tabs to populate the charts in the right pane.
	• Right pane contains **Charts** that have two tabs:
	  • **Latest**
	  • **Trend**: Contains the **Baseline** tab, which allows you to view machine learning baseline charts.
	  Depending on the tab you choose 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, and 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 Data Collection, on page 66 and Cisco AI Network Analytics Overview, on page 9.
	• 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 following:
	  • 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.
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 was 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 Data Collection, on page 66 and Cisco AI Network Analytics Overview, on page 9. **Important** To view the SSID machine learning baseline chart, you must choose 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 Data Collection, on page 66 and Cisco AI Network Analytics Overview, on page 9. 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 following: • 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. You can hover your cursor over a segment to view the percentage and number of clients connected to the 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 on your network. This dashlet provides the following 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 the following 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 the following options: • **Onboarding Time >= 10 s**: Onboarding time is greater than or equal to the 10-seconds 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	View detailed client device information in a table format. The client device table displays the following 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. • **MAC Address**: Displays the MAC address which includes Device MAC and RCM (Randomized and Changing MAC Address). The Private MAC icon appears in front of the RCM. You can filter the table based on type of MAC Address such as All, Device MAC, 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. • **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. • **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.
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.

Client Devices Dashlet	
Item	**Description**
⋮	Customize the data you want displayed in the table: **a.** Click ⋮ . **b.** Check the check boxes for the data you want displayed in the table. **c.** Click **Apply**.
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.

Monitor and Troubleshoot the Health of a Client Device

Use this procedure to view details about a specific client device and to determine if there are potential issues that must be addressed.

Note The client health data might take up to an hour to populate if an HA failover has occurred.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Client** tab.

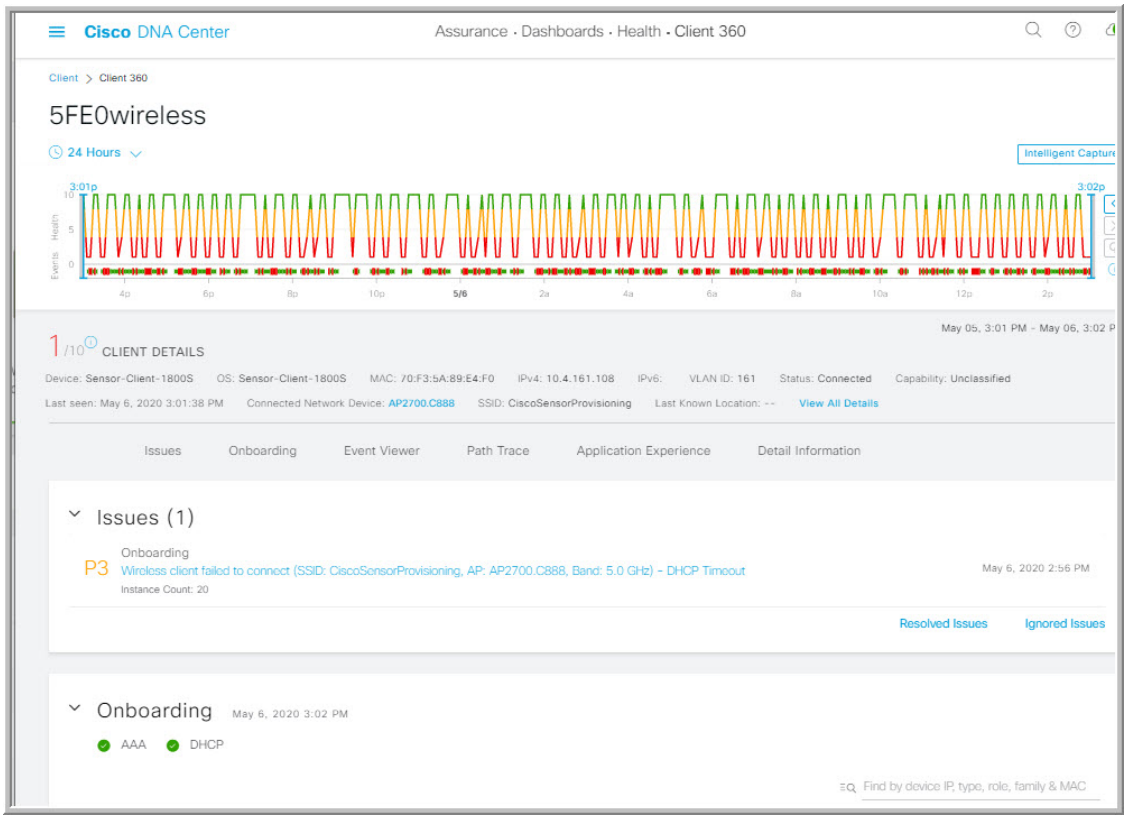
The **Client** health dashboard appears.

Step 3 Do one of the following:

- In the **Client Devices** table, click the hyperlinked Identifier or the MAC address of the device.
- In the **Search** field (located on the top-right corner), enter one of the following: user ID (authenticated through Cisco ISE), IP address, or MAC address.

The **Client 360** window displays a 360° view of the client device.

Figure 11: Client 360 Window



Step 4 Click the time range setting ( ) at the top-left corner to specify the time range of the data that you want displayed on 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 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 Enable a Live Capture Session for a Client Device, on page 256.

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 Use the timeline slider to view the health and events information about the client device over a period of time. The timeline slider has the following functionality:

- **Health**: You can hover your cursor over the timeline slider to view the client's health score and KPIs for a 5-minute window. The KPIs with a colored circle contribute to the individual client health score.

  Note For the **Speed** KPI, the speed capacity of the interface or physical port is displayed. If the port has negotiated to a certain speed then that negotiated speed is displayed.

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. Note that the timestamp next to each category (**Issues**, **Onboarding**, **Event Viewer**, **Connectivity**, and so on) is also refreshed.

Note If you want to display information for longer than 1 hour, manually move the timeline slider to the desired time range.

- **Events**: 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.

Step 7 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 127.

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 8 Use the **Client Details** area, below the timeline, to view the following 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, connected VLAN ID, connection status, last seen timestamp, connected network device, SSID, and last known location.
- For wired clients, this area provides information about the client device such as its MAC address, IPv4 and IPv6 address, connected VLAN ID, connection status, last seen timestamp, connected network device, port, and last known location.

Step 9 Click **View All Details** in the **Client Details** area, to open a slide-in pane with additional details about the client device.

Step 10 Use the collapsible categories to view information about issues, onboarding, event viewer, path trace, application experience, and details:

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, impact, and suggested actions. From the slide-in pane, you can do the following: • To resolve an issue: a. From the drop-down list, choose **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, choose **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 149.

Onboarding Category
Topology of how a client got on the network, including information about the following 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 the following: • 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. • 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 allows you to pinpoint during which subevent an issue occurred. The following scenarios are provided for wireless clients: • **Re-Authentication** • **Broadcast Rekey**: Process of changing the session key—the encryption key of an ongoing communication—to limit the amount of data encrypted with the same key. • **Onboarding** • **DHCP** • **Delete** • **INTRA-Roaming** • **INTER-Roaming** • **ASSOC** • **AUTH** • **EAP** • **DISASSOC** • **DEAUTH** • **11r Failure** • **OKC Failure** • **EAP Failure** When an issue occurs, that event is marked red; otherwise, it is 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 ISE server events, switch system level syslogs, switch port or interface specific events, and client specific events. For the list of messages under each event category, see Messages Displayed in the Event Viewer for Wired Clients, on page 125. 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.

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 Perform a Path Trace, on page 279.

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 129 and View Application Experience of a Host, on page 136.

Detail Information Category
Contains the following tabs: **Device Info**, **RF**, **User Defined Network** (only wireless clients), and **Connectivity**. Click each tab to get the appropriate information. The **User Defined Network** is supported 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. **Note** The **Connectivity** tab displays the new connection KPI named as Retries. The connection retries for radios are displayed in the retries chart. **Note** For Samsung devices, the **Device Info** tab displays additional information, such as build number, origin, country code, device type (mobile, tablet, and so on), and host operating system. **Note** For Apple devices, an **iOS Analytics** tab is provided.

Messages Displayed in the Event Viewer for Wired Clients

The following tables provide the list of messages that are displayed in the **Event Viewer** for wired clients in the **Client 360** window:

ISE Server Event
`Client AUTH FAILURE` `Client AUTH SUCCESS`

Switch System Level Syslogs
`RADIUS-3-ALLDEADSERVER` • `Device UnReachable` • `Device Reachable`

Switch Port or Interface Specific Events
TRAP EVENTS • Link DOWN • Link UP PM-4-ERR_DISABLE ILPOWER-5-POWER_GRANTED ILPOWER-5-IEEE_DISCONNECT ILPOWER-5-INVALID_IEEE_CLASS ILPOWER-4-LOG_OVERDRAWN ILPOWER-3-SHUT_OVERDRAWN

Client Specific Events
DOT1X-5-FAIL MAB-5-FAIL

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 as follows:

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 the RSSI and SNR 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 as follows:

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 as follows:

Wired Client: Connectivity score can be 2 or 6. Link errors determine the Connectivity score and the resulting Overall Health score, as shown below:

- 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.

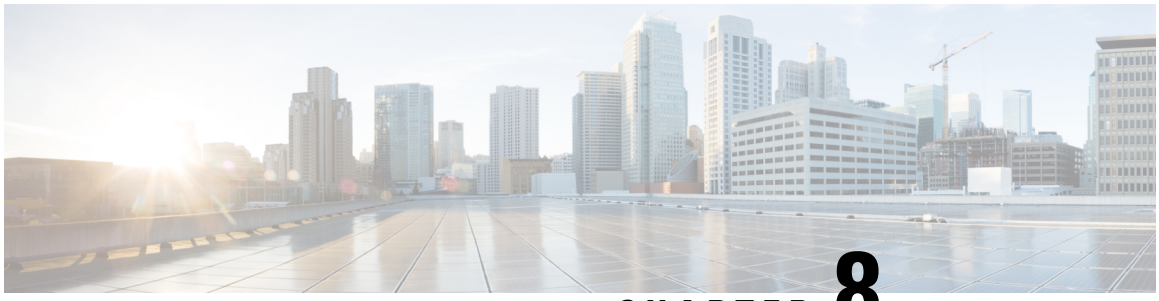
Individual Client Health Score

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 as follows:

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 129
- Supported Platforms, on page 130
- Criteria for Enabling Application Telemetry on Devices, on page 131
- Application Health Prerequisites, on page 133
- Provision Application Telemetry Settings, on page 135
- View Application Experience of a Host, on page 136
- View Application Experience of a Network Device, on page 137
- Monitor the Health of All Applications, on page 138
- Monitor the Health of an Application, on page 143
- Configure Health Score Settings for Applications, on page 147
- Understand Application Health Score and KPI Metrics, on page 147

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 the following:

- 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 Cisco DNA Center.

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 Cisco DNA Center, see Cisco DNA Center Supported Devices.

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 Cisco DNA Traffic Telemetry Appliance. For minimum software versions, see Supported Platforms, on page 130.

Supported Platforms

The following table lists the supported platforms, type of data collection, and software and license requirements.

Note For device compatibility with Cisco DNA Center, see Cisco DNA Center Supported Devices.

Cisco Platform Support for Application Experience and Application Visibility in Cisco DNA Center		
Platform	**Data Collection**	**Notes**
Cisco IOS-XE Routers	Application Experience data collection.	• Requires active NBAR2 license. • IOS XE 16.3 minimum software version. • For Optimized APM—IOS XE 17.3 minimum software version.

Cisco Platform Support for Application Experience and Application Visibility in Cisco DNA Center		
Platform	**Data Collection**	**Notes**
Catalyst 9000 Series Switches	Application Visibility data collection for 9200, 9300, 9400.	• Requires Cisco DNA Advantage license. • IOS XE 16.10.1 minimum software version.
Cisco AireOS Wireless Controllers	Application Visibility data collection.	• Requires Cisco DNA Assurance 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.	• For Optimized APM—IOS XE 16.12.1 minimum software version.
Cisco DNA Traffic Telemetry Appliance	Application Experience data collection.	• Requires Cisco DNA Advantage license. • For Optimized APM—IOS XE 17.3 minimum software version.

Criteria for Enabling Application Telemetry on Devices

Cisco DNA Center automatically enables application telemetry on all applicable interfaces or WLANs that are selected based on the new automatic interfaces or WLAN selection algorithm.

Application telemetry is pushed to WLANs that are provisioned through Cisco DNA Center.

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 automatic selection algorithm to tagging-based algorithm, you must disable telemetry before provisioning the tagged SSIDs to the devices.

The following table provides the criteria for selecting interfaces and WLANs based on 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 is a physical interface.
	• 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 the following:
		  • 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 the following:
		  • 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]	• Not a Guest SSID:
		  • WLAN is not configured as a guest type.
		  • Name of the SSID does not contain the **guest** keyword.
		• SSID is configured in Local mode.

Cisco Catalyst 9800 Series Wireless Controller with Optimized Application Performance Monitoring (APM) profile and IOS release 16.12.1 and later.	• WLAN profile name is tagged with the **lan** keyword.[1, 2]
	• WLAN is configured in Local mode.
		• Not a Guest SSID:
		  • WLAN is not configured as a guest type.
		  • Name of the SSID does not contain the **guest** keyword.
		• If the SSIDs are mixed, that is Local mode, Flex mode, and Fabric mode, the Cisco Application Visibility and Control (AVC) basic record is configured. If all the SSIDs are in Local mode, the Optimized APM record is configured.

	Note If you want to update the telemetry configuration, you must disable telemetry and then enable it after making the configuration changes.	
Cisco DNA Traffic Telemetry Appliance with Optimized APM profile and IOS release 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** interface description.

Application Health Prerequisites

This topic provides the prerequisites relating to application health for routers, 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 Cisco DNA 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 131.

Application Visibility Prerequisites on Switches

- Requires Cisco IOS XE software.
- Requires a Cisco DNA 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.
- Management interface Gig0/0 cannot be used as the source interface of a NetFlow export.
- Clocks must be synchronized between Cisco DNA 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 131.

Application Visibility Prerequisites on AireOS Wireless Controllers

- Requires a Cisco DNA Assurance 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 Cisco DNA 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 SSID is configured in Local mode (not Flex or Fabric).
- 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 131.

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 131.
- Clocks must be synchronized between Cisco DNA Center and the device for Assurance to display Application Health data.

Application Experience Prerequisites on Cisco DNA Traffic Telemetry Appliance

- Requires a Cisco DNA Advantage license.
- Requires IOS XE software for Optimized APM. See Criteria for Enabling Application Telemetry on Devices, on page 131.
- Clocks must be synchronized between Cisco DNA 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 Cisco DNA Traffic Telemetry Appliance.

Provision Application Telemetry Settings

Configure global telemetry settings as described in Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry, on page 65.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Inventory**.

The Inventory page 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 Choose the devices that you want to provision.

Step 3 From the **Actions** drop-down list, choose **Telemetry** and do one of the following:

Note The application telemetry option is enabled only if the device supports application telemetry enablement from Cisco DNA Center.

a) **Enable Application Telemetry**: To configure application telemetry for the selected devices.
b) **Disable Application Telemetry**: To remove the 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 **More** 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, on page 24, Discover Your Network Using CDP, on page 18, or Discover Your Network Using LLDP, on page 29.
- Enable and configure Application Telemetry profile on network devices. See Provision Application Telemetry Settings, on page 135.
- See Application Health Prerequisites, on page 133.

Step 1 From the **Client 360** window, expand the **Application Experience** category.

Step 2 From the **Application Experience** category, you can do the following:

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**, **Business Irrelevant**, or **Default**.

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 148.
- **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, on page 24, Discover Your Network Using CDP, on page 18, or Discover Your Network Using LLDP, on page 29.
- Enable and configure Application Telemetry profile on network devices. See Provision Application Telemetry Settings, on page 135.
- See Application Health Prerequisites, on page 133.

Step 1 From the **Device 360** window, expand the **Application Experience** category.

Step 2 From the **Application Experience** category, you can do the following:

a) 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**.

b) 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.

c) 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.

d) 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, on page 24, Discover Your Network Using CDP, on page 18, or Discover Your Network Using LLDP, on page 29.
- Enable and configure Application Telemetry profile on network devices. See Provision Application Telemetry Settings, on page 135.
- See Application Health Prerequisites, on page 133.

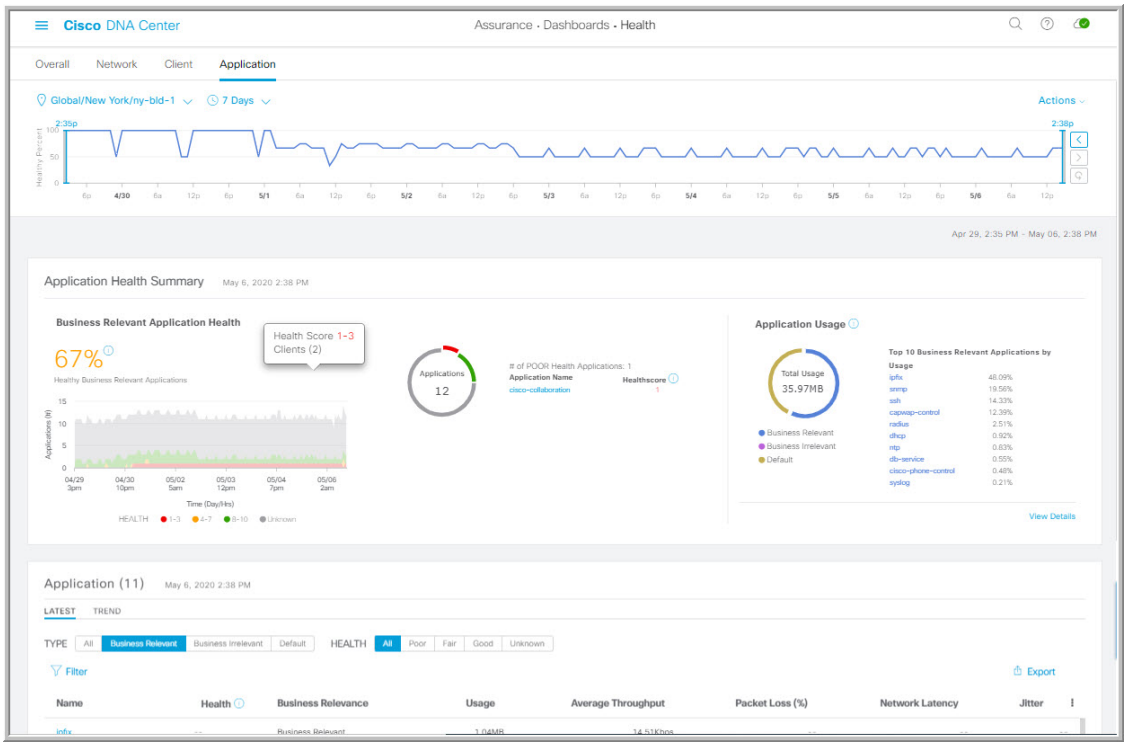
Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Application** tab.

The **Application** health dashboard appears.

Figure 12: Application Health Dashboard



Step 3 Use the **Application** health dashboard top-menu bar for the following 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 **Apply** in the appropriate row. 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 the following: **a.** From the drop-down menu, choose 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**.
Actions drop-down list	Enables you to customize the dashboard display when you choose **Edit Dashboards** from the drop-down list. See Change the Position of a Dashlet, on page 235 and Create a Custom Dashboard, on page 231.

Application Health Dashboard Top-Menu Bar	
Item	**Description**
Application Health Timeline Slider	Enables you to view the healthy business relevant application percentage 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 **Application Health Summary** dashlet for the following functionality:

Application Health Summary 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 147. The following charts are displayed: • 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. • 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 Usage	• Circle chart: Shows the total application usage categorized by the application's business-relevance group. You can click a category to show the list of the top 10 applications by usage within the category.
	Note The application usage is the taken from the application's bidirectional traffic.
	• **View Details**: Click **View Details** to open a slide-in pane with additional details. 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.
	  • Filter the chart by application group or traffic class with the drop-down list at the top right of the slide-in pane.
	  • Click a category in the chart to display the applications and its detailed information in the **Application** table.

Step 5 Use the **Application** dashlet for the following functionality:

Application Dashlet	
Item	**Description**
Type	Filter the table based on the business-relevance groups: Options are **Business Relevant**, **Business Irrelevant**, and **Default**.
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 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 the following 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). **Note** Changing an application's name with the Application Policy package does not show the changed name in Application Experience. Currently there is no integration between the Application Policy package and Application Experience. **Note** If an application is not a standard application from the NBAR, its HTTP host name 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 143. • **Health**: Displays the health score of the application. • **Business Relevance**: Possible values are **Business Relevant**, **Business Irrelevant**, and **Default**. • **Usage Bytes**: 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. For Real-time Transport Protocol (RTP) based applications.
	Customize the data you want displayed in the table: **a.** Click . A list of options appears. **b.** Check the check boxes for the data you want displayed in the table. **c.** Click **Apply**.

Application 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 is not selected for the table. Filters applied to the application table are applied to the exported data.

Monitor the Health of an Application

Use this procedure to view details about a specific application.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and 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, 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 5 To display application information for a particular location, choose the location from the *Location* drop-down list.

Step 6 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 the following 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, the following aspects of delay between the client and the application are displayed:

- 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.

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 7 Use the **Application Details** area, below the timeline, to view the following 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. See step 8.
Exporters tab	Click to view the list of devices that send NetFow traffic to Cisco DNA Center and other details. See step 9.

Step 8 Click **Issues** to view the following 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 the following: • To resolve an issue: **a.** From the drop-down list, choose **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, choose **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 149.

Step 9 Click **Exporters** to view the following information:

Exporters	
Item	**Description**
Device	Displays the list of devices that is sending NetFlow traffic to Cisco DNA Center such as router, switch, wireless controller, and appliance.
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 10 To view metric charts, do the following:

- For routers and appliances, click the exporter row to display charts (below the row) for the following 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 the following 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. The following 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 11 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 Cisco DNA 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**.

Step 12 (Optional) Customize the data you want displayed in the table:

a) Click ⋮.
A list of options appears.
b) Check the check boxes for the data you want displayed in the table.

c) Click **Apply**.

Step 13 (Optional) To export the table data to a CSV file, click **Export**.

Note The data from all available columns is included even if the column is not selected for the table. Filters applied to the application table are applied to the exported data.

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.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Manage** > **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.

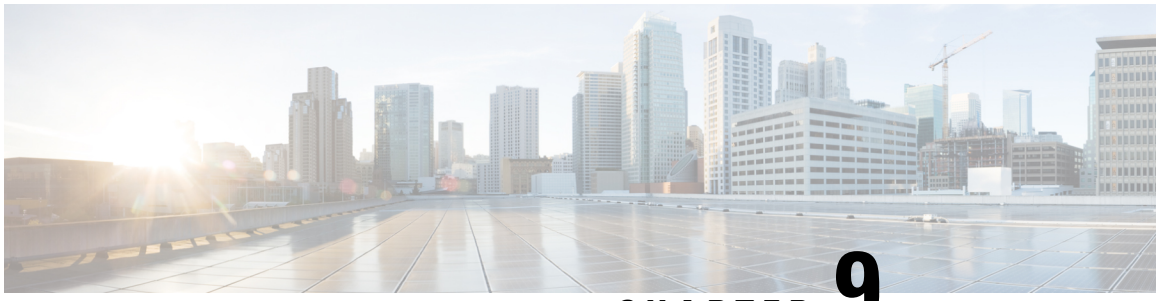
The Individual Application health is measured on a scale of 1 to 10, with 10 being the best score. The following formula is used to calculate the Individual Application Health score:

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 is as follows:

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

View and Manage Issues

- About Issues, on page 149
- About Machine Reasoning Engine, on page 150
- About Layer 2 Loop Issue, on page 150
- View Open Issues, on page 150
- Troubleshoot Wired Client Issues Using MRE , on page 162
- View Resolved Issues, on page 164
- View Ignored Issues, on page 166
- Resolve or Ignore Issues, on page 167
- Radio Outage Issue Triggers, on page 169
- Automatic Issue Resolution, on page 169
- Manage Issue Settings, on page 170
- Enable Issue Notifications, on page 171
- Assurance, Cisco AI Network Analytics, and MRE Issues, on page 172

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, where multiple Key Performance Indicators (KPIs) are correlated, and the results from tests and sensors are used to determine the root cause of the problem, and then possible actions are provided to resolve the problem. The focus is on highlighting an issue rather than monitoring data. Quite frequently, Assurance performs the work of a Level 3 support engineer.

With Cisco DNA 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 the following 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 Currently, Cisco AI Network Analytics use cases are supported only for wireless environments that are running AireOS controllers.

About 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 issues, Layer 2 loop issue, and PoE issue. For the list of issues, see MRE Issues, on page 184.

For procedure, see Troubleshoot Wired Client Issues Using MRE , on page 162, Issue Instance Details for Layer 2 Loop and PoE Issues, on page 158, and Issue Instance Details for a PoE Issue, on page 160.

About Layer 2 Loop Issue

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 allowing you to do the following:

- View the VLANs and ports that are involved in the probable loop.
- View the devices that are associated with the loop.

Note The scale constrains for the Layer 2 Loop are the following:

- Number of VLANS is 10.
- 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 the Cisco DNA Center.

View Open Issues

Use this procedure to view all open issues, which fall under the following 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 Cisco AI Network Analytics application with Cisco DNA Center, you can view the following 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 Machine Reasoning Engine, on page 150.

Before you begin

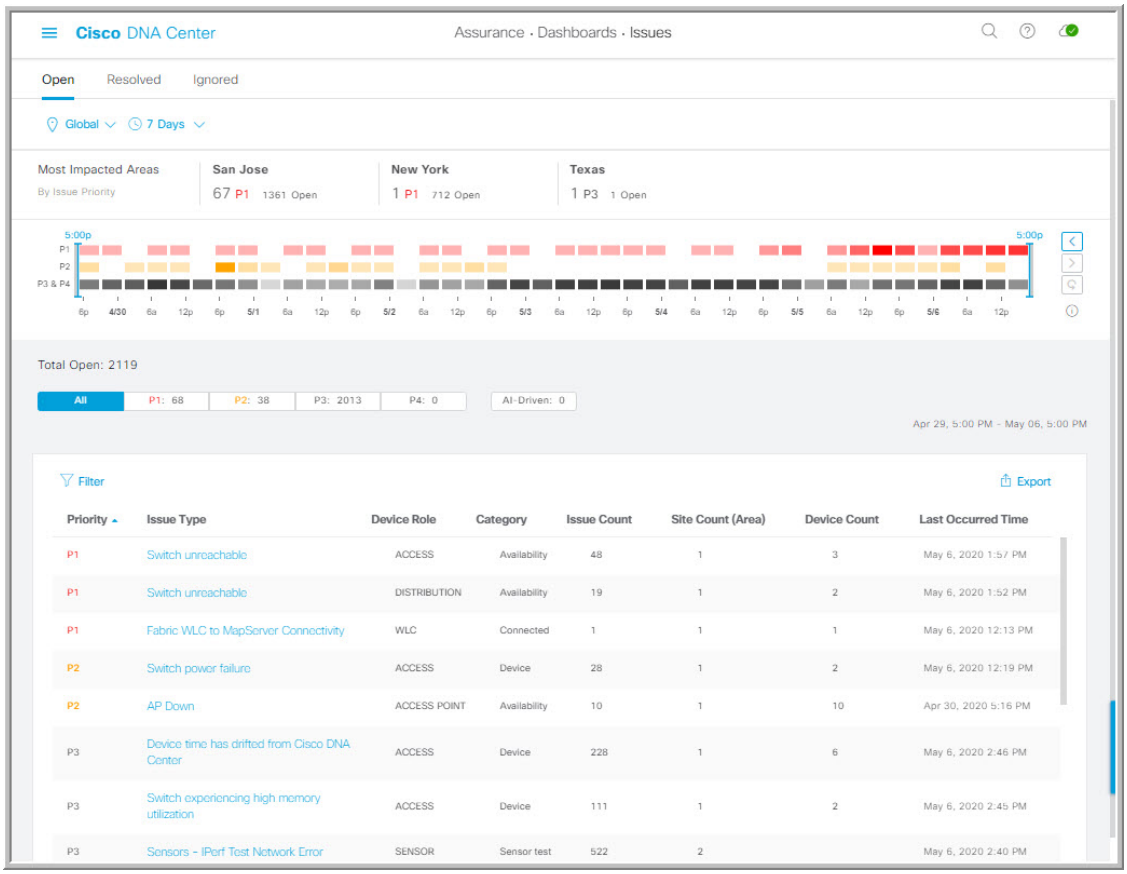
- To view AI-driven cloud-based issues that uses artificial intelligence (AI) and machine learning (ML) technologies to provide intelligent issue detection and analysis, make sure that you have configured Cisco AI Network Analytics data collection. See Configure Cisco AI Network Analytics Data Collection, on page 66.
- 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 65 in Cisco Digital Network Architecture Center User Guide.

Step 1 Do one of the following:

- From the Cisco DNA Center home page, in the **Assurance Summary > Critical Issues** area, choose **View Details**.
- In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Dashboards** > **Issues**.

The **Open Issues** dashboard appears with the following information:

Figure 13: Open Issues Dashboard



Open Issues Dashboard	
Item	**Description**
Global **Location** pane	Allows you to display information on the window based on the location you select. Default is **Global**. To change the location, do the following: **a.** Click **Global**. The Site/Building/Floor table is displayed. **b.** Choose the **Hierarchical Site View** or **Building View** from the drop-down list. Based on what you choose, the table is refreshed. **c.** To view information about a specific site, building, or floor, click **Apply** in the appropriate row; information in the **Open Issues** window is refreshed based on your selection.
Time Range setting	Allows you to display information on the window based on the time range you select. Default is **24 Hours**. Do the following: **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**
Most Impacted Areas	Provides information about the areas that are most impacted based on issue priority. Click the hyper-linked location to drill down to the exact building and floor where the issue has occurred.
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.
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**, **P1**, **P2**, **P3**, **P4**, and **AI-Driven**. Default is **All**.

Step 2 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 Open Issues Window	
Item	**Description**
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. Can be one of the following: Access, Core, Distribution, Border Router, or Unknown.
Category	Category under which the issue type falls. For example, Connectivity, Availability, Onboarding, Utilization, and so on.
Issue Count	Number of times this type of issue has 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**, opens, which lists all the issues for that issue type with the following 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 167.
Issue	Description of the issue.
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**, opens, which provides details about the issue. Depending on the issue, the description and suggested actions are displayed.

Note Some of the suggested actions have a **Run** button adjacent to it. Click **Run** to execute the CLI command on the device.

For AI-driven issues, the **Issue Instance Details** slide-in pane contains AI-driven specific information. See Issue Instance Details for AI-Driven Issues, on page 154.

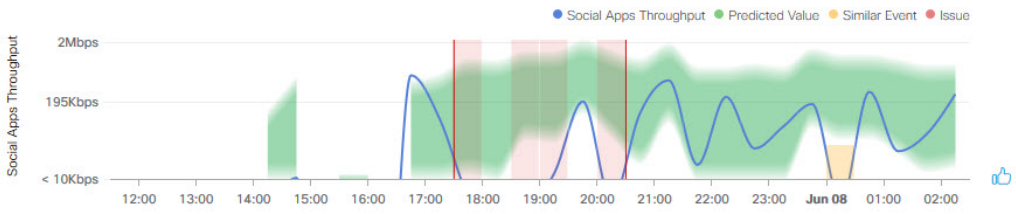
For a Layer 2 loop issue, which support Machine Reasoning, the **Issue Instance Details** slide-in pane contains specific information. See Issue Instance Details for Layer 2 Loop and PoE Issues, on page 158.

For a PoE issue, which support Machine Reasoning, the **Issue Instance Details** slide-in pane contains specific information. See Issue Instance Details for a PoE Issue, on page 160.

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 150.

For AI-driven issues, the **Issue Instance Details** (second slide-in pane) provides the following 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 the following: • To resolve an issue, from the **Status** drop-down list, choose **Resolve**. • To stop an issue from being reported, do the following: 1. From the **Status** drop-down list, choose **Ignore**. 2. Set the number of hours to ignore the issue on the slider, and then click **Confirm**.
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**.
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 the following figure: ***Figure 14: 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.

Issue Instance Details (Second Slide-In Pane)	
Item	**Description**
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, the following tabs are provided: **Impacted Clients** and **Top 10 Impacted APs**. For Total Radio Throughput and Applications Throughput (Cloud, Collab, Media, and Social), the following 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 the following figure: ***Figure 15: Root Cause Analysis Charts*** For Excessive Onboarding Time and Failures, the following tabs are provided: **Network Causes**, **Failed Distribution**, **Failed Percentage**, and **Failed Count**. For Excessive DHCP, Association, or Authentication Time, the following tabs are provided: **Network Causes**, **Top Impacted APs**, and **Top Impacted Times**. For Excessive DHCP, Association, or Authentication Failures, the following tabs are provided: **Network Causes**, **Top Impacted APs**, and **Top Impacted Failures**. For Total Radio Throughput and Applications Throughput (Cloud, Collab, Media, and Social), the following tabs are provided: **Network Causes**. Click the tab to update the charts below. To view the charts for additional KPIs, click the **KPI** icon, choose the KPI, and then click **Apply**.
Suggested Actions	Provides the actions you can take to resolve the issue.

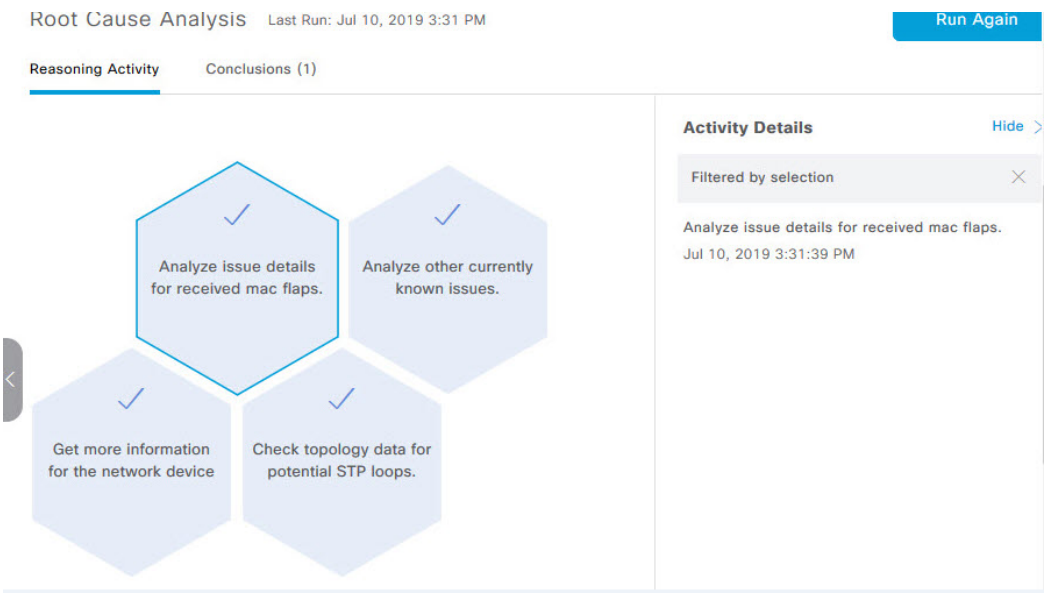
Issue Instance Details for Layer 2 Loop and PoE Issues

Note The **Issue Instance Details** slide-in pane is part of the **Open Issues** workflow. See Step 4 in View Open Issues, on page 150.

To understand the Layer 2 Loop issue and the Machine Reasoning Engine, see About Layer 2 Loop Issue, on page 150.

For Layer 2 Loop issue, which supports Machine Reasoning, the **Issue Instance Details** slide-in pane contains the following information:

Issue Instance Details (Second Slide-In Pane)	
Item	**Description**
Status drop-down list	Allows you to change the status of the issue. Do the following: • To resolve an issue, from the **Status** drop-down list, choose **Resolve**. • To stop an issue from being reported, do the following: 1. From the **Status** drop-down list, choose **Ignore**. 2. Set the number of hours to ignore the issue on the slider, and then click **Confirm**.
Summary	Brief summary of the issue, which can include information, such as device, role, time, location. and potential root cause. For Layer 2 Loop issue, this area provides the initial assessment, such as the VLANs and ports in the potential loop.
Problem Details	**Note** This area is provided for Layer 2 Loop issue. Provides a brief text that describes the problem along with the following: • **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.

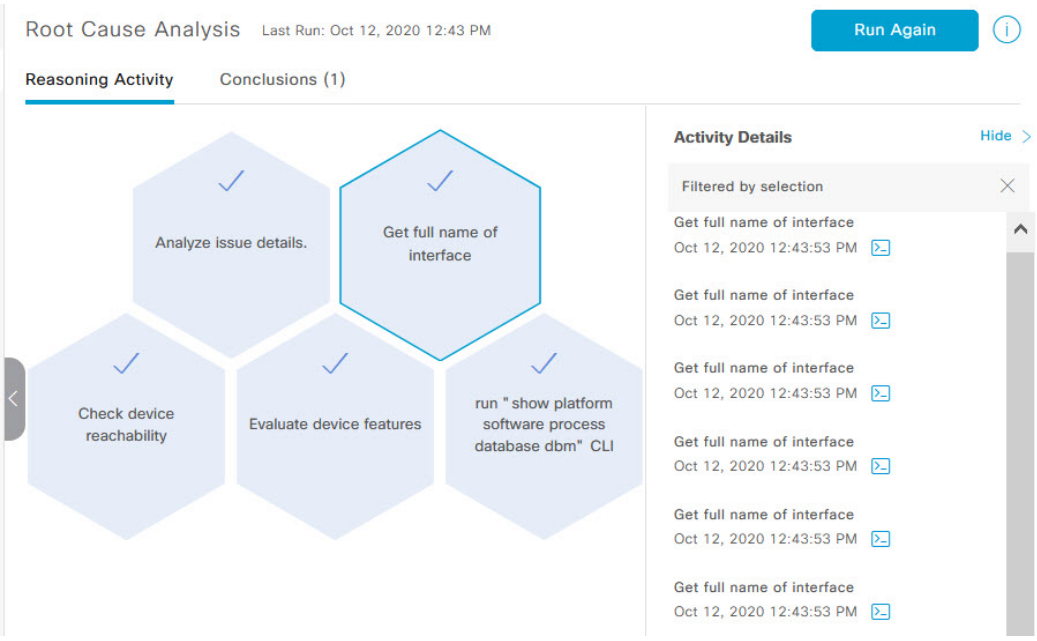
Issue Instance Details (Second Slide-In Pane)	
Item	**Description**
Root Cause Analysis	The Machine Reasoning Engine (MRE) allows you to perform complex root cause analysis and suggests corrective actions. **1.** Click **Run Machine Reasoning** to allow the MRE to start troubleshooting. After the troubleshooting 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. **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 the following 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 16: Reasoning Activity***  **6.** Click **Run Again** if you want to rerun the MRE.
Topology icon	**Note** This icon is provided for Layer 2 Loop issue. 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 150.

For a PoE issue, which supports Machine Reasoning, the Issue Instance Details slide-in pane contains the following information:

Issue Instance Details (Second Slide-In Pane)	
Item	**Description**
Status drop-down list	Allows you to change the status of the issue. Do the following: • To resolve an issue, from the **Status** drop-down list, choose **Resolve**. • To stop an issue from being reported, do the following: 1. From the **Status** drop-down list, choose **Ignore**. 2. Using the slider, set the number of hours to ignore the issue and click **Confirm**.
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 the following: • **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 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** 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 the following 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 17: Reasoning Activity***  **6.** Click **Run Again** if you want to rerun the MRE.

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 184.

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 69.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and 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** as appropriate.

If you click **Authentication**, the following information is displayed 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**, the following information is displayed below the chart: Top DHCP Failure Reason, Top Location, Top Switch, Top Host Device Type. A table is also displayed.

Step 5 Do one of the following:

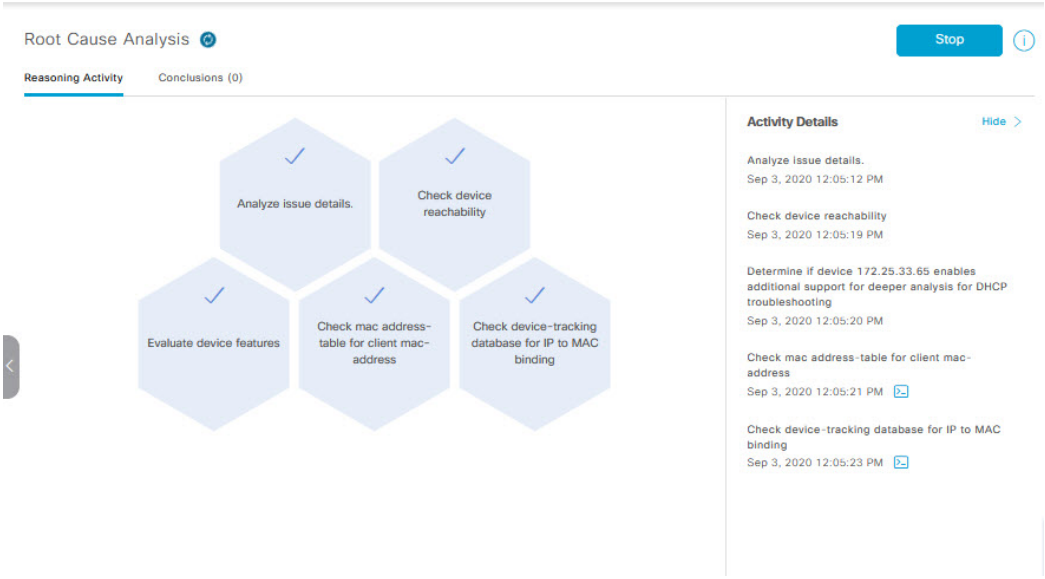
- If you are a user with SUPER-ADMIN-ROLE privileges, enter the client's MAC address in the search tool.
- In the table, from the **Identifier** column, click the hyperlinked identifier.

The **Client 360** window for the client is displayed.

Step 6 In the **Client 360** window, from the **Issues** dashlet, click an authentication or DHCP issue.

The **Issue Details** window is displayed with the following information:

Issue Details	
Item	**Description**
Status drop-down list	Provides the current status of the issue, which you can change. Do the following: • To resolve an issue, from the **Status** drop-down list, choose **Resolve**. • To stop an issue from being reported, do the following: **a.** From the **Status** drop-down list, choose **Ignore**. **b.** Set the number of hours to ignore the issue on the slider, and then click **Confirm**.
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 the following 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 18: 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 the following 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 Data Collection, on page 66.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Dashboards** > **Issues**.

The **Open Issues** dashboard appears.

Step 2 Click the **Resolved** tab.

The **Resolved Issues** window appears.

Step 3 Use the **Resolved Issues** window to view the following information:

Resolved Issues Window	
Item	**Description**
Global	Allows you to display information on the window based on the location you select. Default is **Global**. To change the location, do the following: **a.** Click **Global**. The Site/Building/Floor table is displayed. **b.** Choose the **Hierarchical Site View** or **Building View** from the drop-down list. Based on what you choose, the table is refreshed. **c.** To view information about a specific site, building, or floor, click **Apply** in the appropriate row; information in the **Open Issues** window is refreshed based on your selection.
24 Hours drop-down list	Allows you to display information on the window based on the time range you select. Default is **24 Hours**. Do the following: **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.
Timeline slider	Allows you to specify a more granular time range. Click and drag the timeline boundary lines to specify the time range.

Resolved Issues Window	
Item	**Description**
Total Resolved	Provides the total count of resolved issues. The **Total Resolved** value changes depending on the tab you choose. Options are **All**, **P1**, **P2**, **P3**, **P4**, and **AI-Driven**. Default is **All**.

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**
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. Can be one of the following: Access, Core, Distribution, Border Router, or Unknown.
Category	Category under which the issue type falls. For example, Connectivity, Availability, Onboarding, Utilization, and so on.
Issue Count	Number of times this type of issue has 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**, opens, which 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 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 169.

Step 6 From the **Issue** column in the **Issue Instances** slide-in pane, click an issue.

A second slide-in pane, **Issue Instance Details**, opens, which 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.

View Ignored Issues

Use this procedure to view all issues that are marked as ignored. The list of ignored issues that appear fall under the following two 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 Data Collection, on page 66.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Dashboards** > **Issues**.

The **Open Issues** dashboard appears.

Step 2 Click the **Ignored** tab.

The **Ignored Issues** window appears.

Step 3 Use the **Ignored Issues** window to view the following information:

Ignored Issues Window	
Item	**Description**
Global	Allows you to display information on the window based on the location you select. Default is **Global**. To change the location, do the following: **a.** Click **Global**. The Site/Building/Floor table is displayed. **b.** Choose the **Hierarchical Site View** or **Building View** from the drop-down list. Based on what you choose, the table is refreshed. **c.** To view information about a specific site, building, or floor, click **Apply** in the appropriate row; information in the **Ignored Issues** window is refreshed based on your selection.
24 Hours drop-down list	Allows you to display information on the window based on the time range you select. Default is **24 Hours**. Do the following: **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.
Timeline slider	Allows you to specify a more granular time range. Click and drag the timeline boundary lines to specify the time range.

Ignored Issues Window	
Item	**Description**
Total Ignored	Provides the total count of ignored issues. The **Total Ignored** value changes depending on the tab you choose. Options are **All**, **P1**, **P2**, **P3**, **P4**, and **AI-Driven**. Default is **All**.

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**
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. Can be one of the following: Access, Core, Distribution, Border Router, or Unknown.
Category	Category under which the issue type falls. For example, Connectivity, Availability, Onboarding, Utilization, and so on.
Issue Count	Number of times this type of issue has 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** opens, which 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**, opens, which provides details about the issue. Depending on the issue, the description along with suggested actions are displayed.

Resolve or Ignore Issues

Use this procedure to resolve or ignore a bulk of issues or to resolve or ignore a single issue.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Dashboards** > **Issues**.

The **Open Issues** dashboard appears.

Step 2 To resolve or ignore a bulk of issues, do the following:

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.

b) Do one of the following:

- 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, do the following:

  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, choose **Resolve**.

A Warning dialog box appears. Click **Yes** in the Warning dialog box to proceed 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, choose **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, do the following:

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.

b) To resolve an issue, from the **Status** drop-down list, choose **Resolve**.

c) To stop an issue from being reported, do the following:

1. From the **Status** drop-down list, choose **Ignore**.

2. Set the number of hours to ignore the issue on the slider, and then click **Confirm**.

Radio Outage Issue Triggers

A radio outage issue is triggered when all of the following conditions are met for 60 minutes, which is the default trigger time:

Note To change the default trigger time, go to **Assurance > Manage > Issue Settings**. See Manage Issue Settings, on page 170.

- The AP radio operation state is "up".
- The AP mode is Local or Flex-Connect.
- 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 the following types of issues, if the issue condition no longer exists, the system automatically resolves the issue:

- Interface is down.
- Wireless Controller/Switch/Router unreachable.
- AP Disconnect from WLC.
- No activity on radio.

Note The system automatically resolves this issue when one of the following conditions no longer exist:

- 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.

After the issue is resolved, the **Updated By** column in the **Resolved Issues** > **Issue Instance** slide-in pane, displays **System**. See **Step 3** in View Resolved Issues, on page 164.

Manage Issue Settings

Use this procedure to manage the settings for issues. You can 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.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Manage** > **Issue Settings**.

The **Issue Settings** window appears.

Step 2 Set the **DEVICE TYPE** and **CATEGORY** filters to view the type of issues you want to configure.

To view the AI-driven issues, click the **AI-Driven** tab in the **CATEGORY** filter.

Step 3 Click an issue in the **Issue Name** column to open an 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, 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 radio outage trigger conditions, see Radio Outage Issue Triggers, on page 169.

Examples of a trigger condition:

```
No Activity on Radio(2.4 GHz) >= 60 minutes.
```

```
Memory Utilization of Access Points greater than 90%
```

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 Click **Manage Subscription** to subscribe to external notifications for supported issues when they are triggered. See Enable Issue Notifications, on page 171.

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 status change, Assurance can generate a REST or email notification.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Manage** > **Issue Settings**.

The **Issue Settings** window appears.

Step 2 Click **Manage Subscriptions**.

The **Events** window appears.

Step 3 Check the check boxes of the events that you want to subscribe to.

Note The **Event** name in Cisco DNA Center platform is the same as the **Issue Name** in Assurance.

Step 4 Click **Subscribe**.
The **Subscribe** dialog box appears.

Step 5 In the **Subscribe** dialog box, enter the details for the subscription:

a) Enter a name for the subscription in the **Name** field.

b) Click the **Subscription Type** drop-down list to select the notification type. You can receive REST or email notifications:

Notification Type	Details
REST	Receive a REST notification when the issue/event is triggered. Configure the following settings: • Select the option **Select an existing endpoint** or **Create a new endpoint** to specify the endpoint and configure the subsequent fields for the endpoint. • **Trust Certificate** • **HTTP Method**: Options are **POST** or **PUT**. • **Headers**: Enter the header details in the **Header Key** and **Header Value** fields.
EMAIL	Receive an email notification when an issue/event is triggered. **Important** To receive email notifications, make sure you have the email server configured in the ⚙ > **System Settings** > **Email configuration** window.

c) Click **Subscribe**.

A subscription for the issue/event is created. A notification is sent when the issue/event is triggered and there is a status change.

What to do next

You can view and manage existing event subscriptions in Cisco DNA Center platform. For details, see "*Working with Events*" in the *Cisco DNA Center Platform User Guide*.

Assurance, Cisco AI Network Analytics, and MRE Issues

Router Issues

The following 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	Interface connecting network devices is down.
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 - 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	Interface connecting WAN network is down.
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	High input/output error on interfaces.
Connected	High input/output discards on router interfaces	High input/output discards on interfaces.
Connected	High input/output utilization on router interfaces	High input/output utilization on interfaces.
Connected	High input/output discards on router WAN interfaces	High input/output discard on WAN interfaces.
Connected	High input/output utilization on router WAN interfaces	High input/output utilization on WAN interfaces.

Router Issues		
Category	**Issue Name**	**Summary**
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	DNA Center and network device time has drifted	Excessive time lag between Cisco DNA 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	Device experiencing high CPU utilization.
Device	Router experiencing high memory utilization	Device experiencing high memory utilization
Availability	Network device HA switchover	The network device went through an High Availability (HA) switchover.
Availability	Router unreachable	Network device is unreachable from controller.

Core, Distribution, and Access Issues

The following 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	Interface connecting network devices is down.
Connectivity	Layer 2 loop symptoms	Host MAC address flapping seen on a network device.
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.

Core, Distribution, and Access Issues		
Category	**Issue Name**	**Summary**
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	Interface connecting the WAN network 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*.
Connected	Fabric devices connectivity - Border overlay	Fabric edge lost connectivity to the fabric border in the virtual network.
Connected	Fabric devices connectivity - Border underlay	Fabric edge lost connectivity to the fabric border in the physical network.
Connected	Fabric devices connectivity - Control border underlay	Fabric node lost connectivity to the co-located fabric border and control plane in the physical network.
Connected	Fabric devices connectivity - Control underlay	Fabric node lost connectivity to the fabric control plane device in the physical network.
Connected	Fabric devices connectivity - DHCP overlay	Fabric node lost connectivity to the DHCP server in the virtual network.
Connected	Fabric devices connectivity - DHCP underlay	Fabric node lost connectivity to the DHCP server in the physical network.
Connected	Fabric devices connectivity - DNS overlay	Fabric node lost connectivity to the DNS server in the virtual network.
Connected	Fabric devices connectivity - DNS underlay	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	Fabric edge lost connectivity to the ISE server in the physical network.

Core, Distribution, and Access Issues		
Category	**Issue Name**	**Summary**
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	High input/output error on switch interfaces.
Connected	High input/output discards on switch interfaces	High input/output discards on switch interfaces.
Connected	High input/output utilization on switch interfaces	High input/output utilization on interfaces.
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.
Device	Device time has drifted from Cisco DNA Center	Excessive time lag between Cisco DNA Center and the device.
Device	Interface is flapping on network device	A port interface is flapping on a switch.
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	Device is experiencing high CPU utilization.

Core, Distribution, and Access Issues		
Category	**Issue Name**	**Summary**
Device	Switch experiencing high memory utilization	Device is experiencing high memory utilization.
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	Device is unreachable.
Utilization	Map cache limit reached	Map cache entries have exceeded the limit on the map server.

Controller Issues

The following table lists the controller issues detected by Assurance:

Controller Issues		
Category	**Issue Name**	**Summary**
Connectivity	Interface connecting network devices is down	Interface connecting network devices is down.
Connected	Fabric WLC to MapServer connectivity	Fabric WLC lost connectivity to the fabric control plane node.
Device	Device time has drifted from Cisco DNA Center	Excessive time lag between Cisco DNA Center and the device.
Availability	Network device HA switchover	The network device went through an HA switchover.
Availability	WLC monitor	Network controller is not receiving data from WLC.
Availability	WLC power supply failure	Power supply has failed on this WLC.
Availability	WLC reboot crash	WLC reboot crash.
Availability	WLC unreachable	Device is unreachable.
Utilization	AP license exhausted on WLC	WLC currently has no free AP licenses.
Utilization	WLC memory high utilization	WLC is experiencing high memory utilization.

Access Point Issues

The following table lists the access point issues detected by Assurance:

Access Point Issues		
Category	**Issue Name**	**Summary**
Availability	AP coverage hole	AP has a coverage hole.
Availability	AP Disconnect from Cisco WLC	AP is disconnected.
Availability	AP flap	AP has flapped. This issue is triggered when AP flaps more than two time within a 15-minute time 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.
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	No activity on radio (2.4GHz)	No activity on 2.4-GHz radio *x* on AP.
Utilization	No activity on radio (5GHz)	No activity on 5-GHz radio *x* on AP.
AP Anomaly	AP anomaly	AP encountered anomaly issue.
Availability	Poor RF (2.4 GHz) on a floor	This issue triggered when APs have poor wireless experience. The poor radio frequency (RF) issue includes the following: • Single issue triggers when either interference or noise is above the threshold for a specific AP band within a 30-minute timeframe. • Global issue triggers when at least one AP have either interference or noise above the threshold within a 30-minute timeframe.
Availability	Poor RF (5 GHz) on a floor	This issue triggered when APs have poor wireless experience. The poor RF issue includes the following: • Single issue triggers when either interference or noise is above the threshold for a specific AP band within a 30-minute timeframe. • Global issue triggers when at least one AP have either interference or noise above the threshold within a 30-minute timeframe.

Wired Client Issues

The following 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.

Wired Client Issues		
Category	**Issue Name**	**Summary**
Onboarding	Wired client authentication failures - Dot1.x failure	Wired client authentication failed. User device authentication with Dot1.x failure. **Note** This issue is applicable only for single wired clients.
Onboarding	Wired client authentication failures - MAB failure	Wired client authentication failed. User device authentication failed with MAC authentication bypass issues. **Note** This issue is applicable only for single wired clients.

Wireless Client Issues

The following 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 excluded - IP theft issue	Wireless client excluded - IP theft issue.
Onboarding	Wireless client failed to connect - AAA server rejected client	Wireless client failed to connect - AAA server rejected client.
Onboarding	Wireless client failed to connect - AAA server timeout	Wireless client failed to connect - AAA server timeout.
Onboarding	Wireless client failed to connect - Client PMK not found	Wireless client failed to connect - Client PMK not found.
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 server timeout	Wireless client failed to connect - DHCP server timeout.
Onboarding	Wireless client failed to connect - DHCP timeout	Wireless client failed to connect - DHCP timeout.

Wireless Client Issues		
Category	**Issue Name**	**Summary**
Onboarding	Wireless client failed to connect - Failed to get an IP address due to client timeout	Wireless client failed to connect - Failed to get an IP address due to client timeout.
Onboarding	Wireless client failed to connect - Incorrect PSK	Wireless client failed to connect and was excluded - The client's PSK did not match the configured WLAN PSK.
Onboarding	Wireless client failed to connect - Security parameter mismatch	Wireless client failed to connect - Security parameter mismatch.
Onboarding	Wireless client failed to connect - WLC configuration error	Wireless client failed to connect - WLC configuration error.
Onboarding	Wireless client failed to connect - WLC internal error	Wireless client failed to connect - WLC 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.
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 - WLC configuration error.
Onboarding	Wireless client failed to roam - WLC internal error	Wireless client failed to roam - WLC 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	Wireless client failed to roam between APs - WLC configuration mismatch.
Onboarding	Wireless client took a long time to connect - Excessive time due to authentication timeouts	Wireless client took a long time to connect - Excessive time due to authentication timeouts.
Onboarding	Wireless client took a long time to connect - Excessive time due to DHCP server failures	Wireless client took a long time to connect - Excessive time due to DHCP server failures.

Wireless Client Issues		
Category	**Issue Name**	**Summary**
Onboarding	Wireless client took a long time to connect - Excessive time due to failed credentials	Wireless client took a long time to connect - Excessive time due to failed credentials.
Onboarding	Wireless client took a long time to connect - Excessive time due to WLC failures	Wireless client took a long time to connect - Excessive time due to WLC failures.
Onboarding	Wireless client took a long time to connect - Excessive time for authentication due to AAA server or network delays	Wireless client took a long time to connect - Excessive time for authentication due to AAA server or network delays.
Onboarding	Wireless clients excluded - IP theft issue	Wireless clients excluded - IP theft issue.
Onboarding	Wireless clients failed to connect - AAA server rejected clients	Wireless clients failed to connect - AAA server rejected clients.
Onboarding	Wireless clients failed to connect - AAA server timeout	Wireless clients failed to connect - AAA server timeout.
Onboarding	Wireless clients failed to connect - Client PMK not found	Wireless clients failed to connect - Client PMK not found.
Onboarding	Wireless Clients failed to connect - DHCP server timeout	Wireless Clients failed to connect - DHCP server timeout.
Onboarding	Wireless clients failed to connect - Failed to authenticate due to client timeouts	Wireless clients failed to connect - Failed to authenticate due to client timeouts.
Onboarding	Wireless clients failed to connect - Failed to get an IP address due to client timeouts	Wireless clients failed to connect - Failed to get an IP address due to client timeouts.
Onboarding	Wireless clients failed to connect - Failed to get an IP address due to DHCP server or client timeouts	Wireless clients failed to connect - Failed to get an IP address due to DHCP server or client timeouts.
Onboarding	Wireless clients failed to connect - Incorrect PSK	Wireless clients failed to connect and were excluded - The clients' PSK did not match the configured WLAN PSK.
Onboarding	Wireless clients failed to connect - Security parameter mismatch	Wireless clients failed to connect - Security parameter mismatch during authentication.
Onboarding	Wireless clients failed to connect - WLC configuration error	Wireless clients failed to connect - WLC configuration error.
Onboarding	Wireless clients failed to roam - Client exclusion policies on the WLC	Wireless clients failed to roam - Clients were excluded due to client exclusion policies on the WLC.

Wireless Client Issues		
Category	**Issue Name**	**Summary**
Onboarding	Wireless clients failed to roam - Clients were excluded before roaming	Wireless clients failed to roam - Clients were excluded before roaming.
Onboarding	Wireless clients failed to roam - WLC configuration mismatch	Wireless clients failed to roam between APs - WLC configuration mismatch.
Onboarding	Wireless clients took a long time to connect - Excessive time due to DHCP server failures	Wireless clients took a long time to connect - Excessive time due to DHCP server failures.
Onboarding	Wireless clients took a long time to connect - Failed credentials	Wireless clients took a long time to connect - Excessive time due to failed credentials.
Onboarding	Wireless clients took a long time to connect - WLC failures	Wireless clients took a long time to connect - Excessive time due to WLC failures.
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.

Application Issues

The following 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

The following 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 Issues		
Category	**Issue Name**	**Summary**
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 Cisco DNA Center.
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 Issues		
Category	**Issue Name**	**Summary**
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

The following table lists the AI-Driven issues detected by Cisco AI Network Analytics:

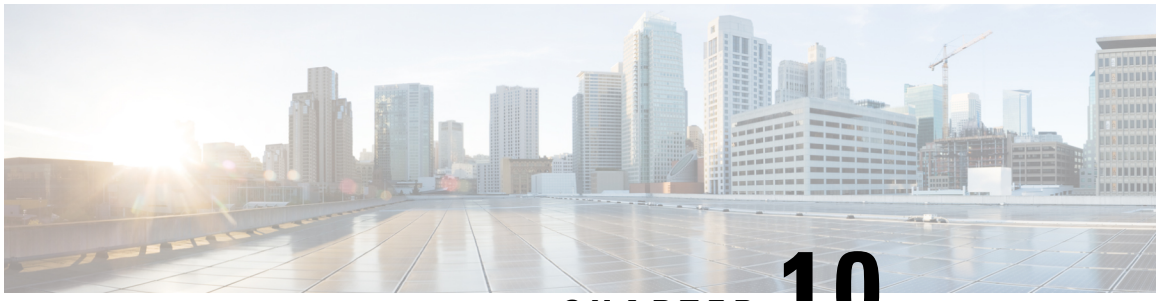
AI-Driven Issues		
Category	**Issue Name**	**Summary**
Connection Issues		
Onboarding	AI Excessive time to connect - High deviation from baseline	The network is experiencing excessive onboarding time compared to usual. Clients are taking longer than the usual time to connect to *SSID*.
Onboarding	AI Excessive failures to connect - High deviation from baseline	The network is experiencing excessive onboarding time 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*.

AI-Driven Issues		
Category	**Issue Name**	**Summary**
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.
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*.
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

The following 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	Wired client authentication failed. User device authentication with Dot1.x failure. **Note** This issue is applicable only for single wired clients.
Onboarding	Wired client authentication failures - MAB failure	Wired client authentication failed. User device authentication failed with MAC authentication bypass issues. **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 10

Manage Sensors and Sensor-Driven Tests

- About Sensors and Sensor-Driven Tests, on page 187
- Provision Sensors, on page 187
- Monitor and Troubleshoot Network Health with Sensors, on page 192
- Manage Sensors and Backhaul Settings, on page 199
- Manage SCEP Profiles, on page 203
- Sensor-Driven Tests, on page 204

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 performing 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

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 choose the sensor device profile **`CiscoProvisioningSSID`**. Instead, choose your own SSID for backhaul purposes. See Manage Backhaul Settings, on page 201.

For Cisco Wireless Controllers, see Enable Provisioning SSID on the Wireless Controller, on page 188.

For Cisco Catalyst Wireless Controllers, see Enable Cisco Provisioning SSID on the Cisco Catalyst Wireless Controller, on page 188.

Step 2 Create a backhaul configuration for the sensor.

See Manage Backhaul Settings, on page 201.

Step 3 Provision the Cisco Aironet 1800s Active Sensor.

See Provision a Wireless or Sensor Device, on page 189.

Step 4 (Optional) After the sensor device is available in the device inventory, you can choose to upgrade the software image. See the "Provision Software Images" topic in the Cisco DNA Center User Guide.

Enable Provisioning SSID on the Wireless Controller

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, choose **Open**.

Step 7 From the **Provisioning** drop-down list, choose **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 Cisco DNA Center IP address, which is done using DHCP Option 43 or through DNS.

Enable Cisco Provisioning SSID on the Cisco Catalyst Wireless Controller

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 the following:

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.

The following 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 performed.

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 the following:

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, choose **CiscoSensorProvisioning**.

f) From the **Policy Profile** drop-down list, choose **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 a Wireless or Sensor Device

Claiming a wireless device provisions it by assigning a configuration to the device and adding it to the inventory. If you claim a device that has not yet booted for the first time, you are planning the device so that it is automatically provisioned when it boots up.

Note When Device Controllability is enabled for a device (it is enabled by default), additional configurations are pushed to the device when it is added to the inventory or assigned to a site. For more information, see the Device Controllability section in the *Cisco DNA Center Administrator Guide*.

This procedure explains how to claim a 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, see the device clean-up and reset details in the Network Plug and Play Troubleshooting Guide for Cisco Digital Network Architecture Center.

- Define the site within the network hierarchy. See About Network Hierarchy, on page 36.
- Define the CLI and SNMP credentials for the devices.
- Optionally, ensure that the software images for any Cisco Catalyst 9800-CL devices to be provisioned are uploaded and marked as golden in the Image Repository, if you want to deploy images.

Note The image deployment process used by Plug and Play during Day-0 provisioning is not the same as that used when updating a device image later. During Plug and Play provisioning, there are no device prechecks, auto flash cleanup, or post-checks done, as it is expected that devices are in the factory default state.

- For provisioning a sensor device, ensure that the sensor is reachable through the Cisco DNA Center enterprise IP address (private/enp9s0). A DHCP option 43 string makes the device reachable in unclaimed mode in Cisco DNA 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 Cisco DNA Center associated with the enp9s0 interface.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Plug and Play**.

Step 2 View the devices in the table.

You can use the **Filter** or **Find** option to find specific devices.

Step 3 Check the check box next to one or more wireless devices that you want to claim.

Step 4 Choose **Actions** > **Claim** in the menu bar above the device table.

The **Claim Devices** window opens, showing the first step, **Assign Site**. If, instead, you see a window that shows mandatory tasks such as defining a site and defining device credentials, you must click on **Add Site** to define a site, and **Add device credentials** to define device credentials. These are prerequisites for the claim process and, once these tasks are completed, you can return to claiming a device by clicking **Refresh** in this window.

Step 5 (Optional) Change the device name, if needed, in the first column.

Step 6 (Optional) Change the device type, if needed, in the second column. You can choose AP (Access Point) or ME (Mobility Express), depending on which mode the device is using.

Choosing the wrong mode causes an error provisioning the device. This item does not appear for wireless LAN controller or sensor devices.

Step 7 From the **Select a Site** drop-down list, choose a site and floor to assign to each device. Access point devices must be assigned to a floor with a wireless controller.

To apply the same site as the first device to all other devices, click the **Apply Site to All** check box. To assign the site from any device to some other devices, click **Assign this Site to Other Devices**, choose the devices, and click **Assign**. Wireless devices can be assigned only to floors within a building, not to the building itself.

Step 8 Click **Next**.
The **Assign Configuration** window appears.

Step 9 (Optional) You can change which columns are displayed in the table by clicking the 3 dots at the right end of the table headings and choosing the desired columns. Click **Apply** to save the changes.

Step 10 In the **Configuration** column, click on **Assign** for the device that you want to configure and follow these steps:

a) View the device configuration summary and click **Cancel** if no changes are needed.

b) (Optional) In the **Device Name** field, change the device name, if needed.

c) For an access point device, in the **Radio Frequency Profile** drop-down list, choose a radio frequency profile to apply to the device. This may be set if you designated one profile as a default.

d) For a wireless LAN controller, enter values in the following fields: **Wireless management IP**, **Subnet mask**, **Gateway**, **IP interface name**, and optionally, **VLAN ID**.

e) For a Mobility Express device, enter values in the following fields: **Wireless management IP**, **Subnet mask**, and **Gateway**.

f) For a wireless sensor device, in the **Sensor Settings** drop-down list, choose the sensor device profile (backhaul) to apply to the device.

Note For Cisco Aironet 1800s Active Sensor, older than Software Release 1.3.1.2, make sure that you do not choose the sensor device profile `CiscoProvisioningSSID`. Instead, choose your own SSID for Backhaul purposes.

g) If you made any changes, click **Save**, otherwise, click **Cancel** to return to the list and configure other devices.

h) You can apply a configuration that you assigned to one device to other devices of the same type by clicking **Apply … to Other Devices** in the **Actions** column.

Step 11 If any devices are a Cisco Catalyst 9800-CL Wireless Controller, click **Assign** next to **Image** in the **Configuration** column and follow these steps:

a) (Optional) In the **Image** drop-down list, choose a golden software image to apply to the device. If there is only one golden image for this device type in the image repository, it is chosen by default.

b) Click **Save**.

Step 12 If you selected multiple devices to provision, click **Assign** for the next device in the list and repeat the configuration, until you have done this for all devices.

Step 13 Click **Next**.
The **Summary** window appears, where you can view details about the devices and configuration.

Step 14 Check the **Day-0 Config** column for each device to see if the configuration preview was successful.

If the preview shows an error, you can click on the **Actions** link in the error message above the table to see what actions you need to take. You can click on 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. Once you have resolved the problem, you can go back to this tab and click the radio button **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**. Ensure that the wireless LAN controller that is managing a device has been added to the inventory and assigned to the site where the wireless device is assigned.

Step 15 Click **Claim**.
A confirmation dialog box is displayed.

Step 16 Click **Yes** to claim the devices and start the provisioning process.

What to do next

To complete the provisioning process, after the device is added to the inventory, go to the **Inventory** tab, select the device and click **Actions > Provision > Provision Device**. Proceed through all the steps and click **Deploy** in the **Summary** step. In the **Summary**, you can see the remaining network settings that will be pushed to the device. This process is required if you intend to push the network settings that you may have configured in the **Design** area. During Plug and Play provisioning, only the device credentials and the Onboarding Configuration are pushed to the device; no other network settings are pushed until provisioning is completed from **Inventory**. Additionally, the device is added to ISE by Cisco DNA Center as a AAA client for RADIUS and TACACS, if these are configured.

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.

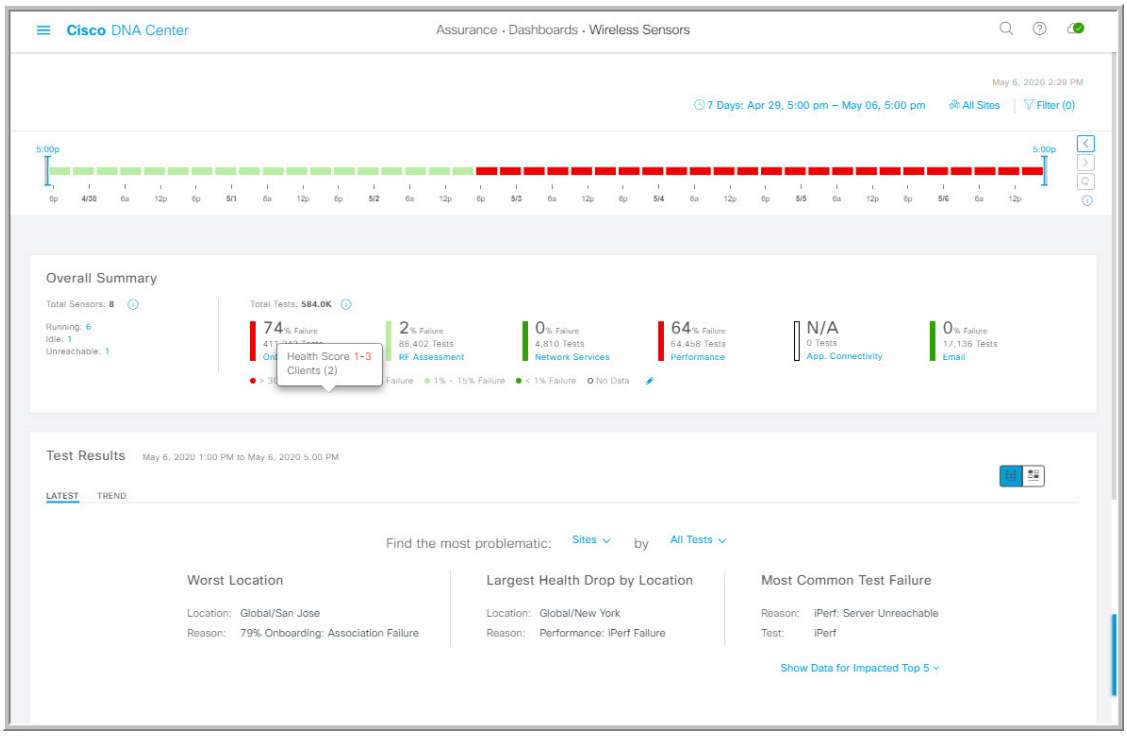
Before you begin

Make sure you have added and scheduled sensor-driven tests. See Create and Run Sensor-Driven Tests Using Templates, on page 204.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Dashboards** > **Wireless Sensors**.

The **Wireless Sensors** dashboard appears.

Figure 19: Wireless Sensors Dashboard



Step 2 Use the **Wireless Sensors** dashboard top-menu bar for the following functionality:

Timeline Area	
Item	**Description**
Time Range setting	Enables you to display data within a specified time range on the dashboard. Do the following: **a.** From the drop-down menu, choose 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**.
Hierarchy Location setting	Enables you to choose 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 cannot exclude all locations from displaying data on the dashboard. Unchecking all locations results in data from all locations to be displayed on the dashboard.

Timeline Area	
Item	**Description**
Filter icon	Enables you to choose 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 the following functionality:

Overall Summary Dashlet	
Item	**Description**
Total Sensors area	Provides an overall view of all the sensors in your network and their status. The following are the status types of the sensor: • **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 197.
Total Tests	Displays the total number of tests performed by all sensors and a breakdown of the test results based on the following 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 the following: • 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. ● > 30% Failure ● 15% - 30% Failure ● 1% - 15% Failure ● < 1% Failure 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 the following 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.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Dashboards** > **Wireless Sensors**.

The **Sensor Dashboard** appears.

Step 2 From the **Sensors Dashboard**, do one of the following:

- 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, 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 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 the following 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, enable the status LED, and change the name for these sensors.

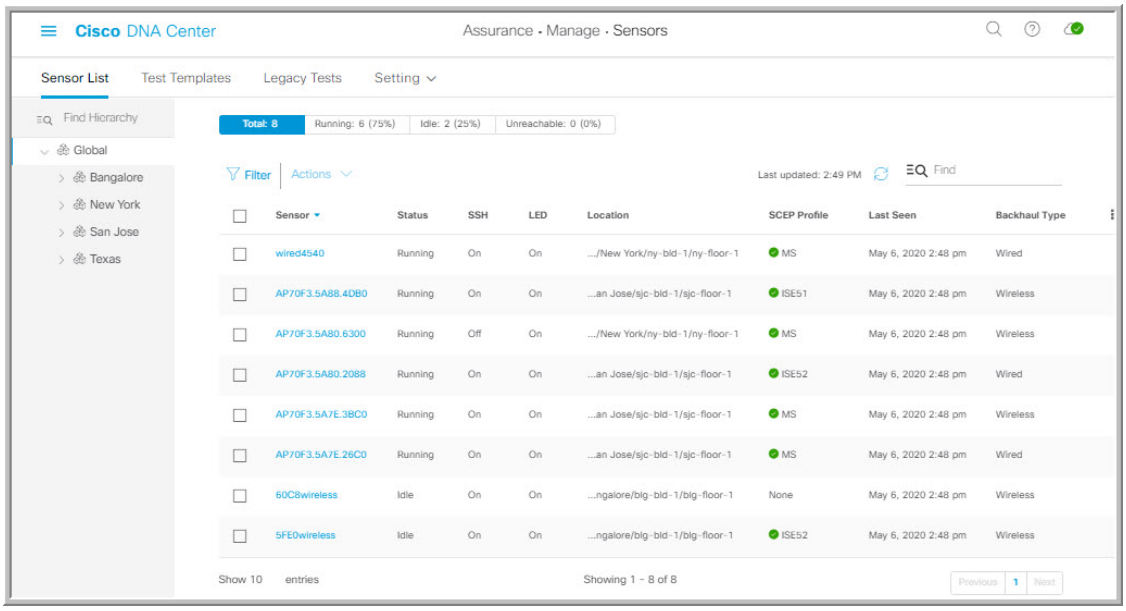
Before you begin

Make sure the sensors are assigned to a site.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Manage** > **Sensors**.

The **Sensor List** window appears.

Figure 20: 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 its 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 to Cisco DNA Center.

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, do the following:

a) Check the check box of the sensor.
b) Hover your cursor over the **Actions** drop-down list and choose **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, do the following:

a) Check the check box of the sensor.
b) Hover your cursor over the **Actions** drop-down list and choose **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, do the following:

a) Check the check box of the sensor.

b) From the **Actions** drop-down list, choose **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, do the following:

a) Check the check box of the sensor.

b) From the **Actions** drop-down list, choose **Enroll using SCEP**.

The **Enroll using SCEP** slide-in pane appears.

c) Choose 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 choose 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 Cisco DNA Center.

For information about a persistent wireless backhaul connection, see Persistent Wireless Backhaul Connections on Sensor Devices, on page 203.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Manage** > **Sensors**.

The **Sensor List** window appears.

Step 2 Click on **Settings** > **Backhaul Settings** tab.

The **Backhaul Settings** window appears.

Step 3 You can add and manage backhaul SSIDs by doing the following:

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, configure the following:

- **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 choose **802.1x EAP**, you must choose one of the following EAP methods for user authentication from the drop-down list:
  - **EAP-FAST**: Enter the user name and password in the fields provided.
  - **PEAP-MSCHAPv2**: Enter the user name and password in the fields provided.
  - **EAP-TLS**: Choose **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

    If you choose **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click **+ Add New Certificate Bundle**, and enter the user name and certificate bundle password.
  - **PEAP-TLS**: Choose **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

    If you choose **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click **+ Add New Certificate Bundle**, and enter the user name and certificate bundle password.

d) In the **Wireless Network Name (SSID)** area, select the wireless network (SSID) and configure the following.

- **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 pre-shared 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 pre-shared 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 the following:

a) Check the check box of the backhaul configuration.
b) Hover your cursor over the **Actions** drop-down list and choose **Edit**.

Step 5 You can delete a backhaul configuration by doing the following:

a) Check the check box of the backhaul configuration.
b) Hover your cursor over the **Actions** drop-down list and choose **Delete**.

Persistent Wireless Backhaul Connections on Sensor Devices

Cisco DNA 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 the following 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.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Manage** > **Sensors**.

Step 2 Click **Setting** > **SCEP Profiles**.

Step 3 To add and manage a SCEP Profile, do the following:

a) Click **Add SCEP Profiles**.

The **Create SCEP Profile** window appears.

b) In the **Create SCEP Profile** window, provide the following details:

- **SCEP Profile Name**: Enter a name for the SCEP profile.
- **URL Base**: Enter a valid server.

  Note For **ISE**, enter the following:

  http://*ISE_IP_or_FQDN_Name***:9090/auth/caservice/pkiclient.exe**

  For **Microsoft CA**, enter the following:

  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, do the following:

a) Check the check box next to the SCEP Profile.
b) From the **Actions** drop-down list, choose **Edit**.

Step 5 To delete a SCEP Profile, do the following:

a) Check the check box next to the SCEP Profile.
b) From the **Actions** drop-down list, choose **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

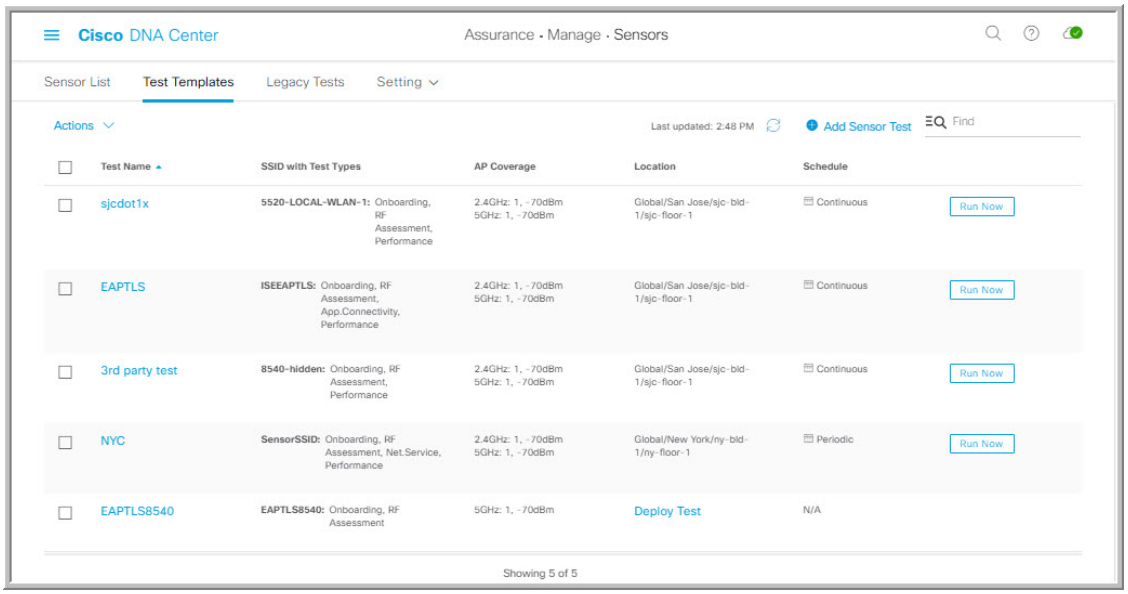
- If you are using the Cisco Aironet 1800s Active Sensor to run sensor-driven tests, make sure that the sensor is provisioned using PnP, so that it displays under **Inventory**. See Provision the Wireless Cisco Aironet 1800s Active Sensor, on page 187.
- Note that if a sensor test template restarts, all sensors on that template begin running their tests at the same time, which causes the result graphs to show a cyclical pattern.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Manage** > **Sensors**.

Step 2 Click the **Test Templates** tab.

The **Test Templates** window appears.

Figure 21: Test Templates Window



Step 3 To create a new sensor test template, click **+ Add Sensor Test**.
The wizard for creating a sensor test template appears.

Step 4 For the **Set up Sensor Test** step, configure the following 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 Click **Next**.

Step 6 For the **Enter SSID Credentials** step, enter the credentials for the selected SSIDs:

- For SSIDs with **Open** security, select the following:
  - **Open**: For SSIDs with WebAuth passthrough, enter the email address.
  - **ISE Guest Portal**: Choose the labels for the ISE guest portal.
  - **Clearpass Guest Portal**: Choose 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 7 Check the **Add Proxy Settings** check box, to enable proxy settings.

Step 8 Configure the following proxy settings:

- **Proxy Server**

- **Proxy Port**
- **Proxy UserName**
- **Proxy Password**

Step 9 Click **Next**.

Step 10 For the **Define Sensor Test Category Details** step, check the check boxes for the test types 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 the following test types:

- **DNS**: Resolves 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 the following test types:

- **Internet (NDT)**: Performs 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 the following:

    - 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, choose 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 the following 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 the following 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 11 Click **Next**.

Step 12 For the **Select AP Coverage** step, do the following:

a) Select the frequency bands to test with the **2.4GHz** and **5GHz** check boxes.

b) In the **Number of Target APs** drop-list for the selected bands, choose the number of APs you want the sensor to test against.

Note You can choose a maximum of five APs.

c) In the **RSSI Range** slider for the selected bands, drag the slider to the desired RSSI.

Step 13 Click **Next**.

Step 14 For the **Summary** step, review the template settings.

Click **Edit** for the **SSIDs** or **AP Coverage** steps to reconfigure its settings.

Step 15 Click **Create Test** to create the template.
The test template is created and a dialog box appears for confirmation.

Step 16 For 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 17 For the **Select Location** step, use the hierarchy menu on the left to check the check boxes for the sites, buildings, or locations that you want to deploy the test template.

Step 18 Click **Next**.

Step 19 For the **Set Schedule** step, select from one of the options for the test frequency:

- **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 selected days, specify the start and end time for the test period from the **From** time pickers.

c. In 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 20 Click **Next**.

Step 21 For the **Summary** step, review the deployment details.

Click **Edit** for the **Location** or **Schedule** steps to reconfigure its settings.

Step 22 Click **Deploy Test**.
The test template appears in the **Test Template** window.

Step 23 Click **Run Now** for the test template 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

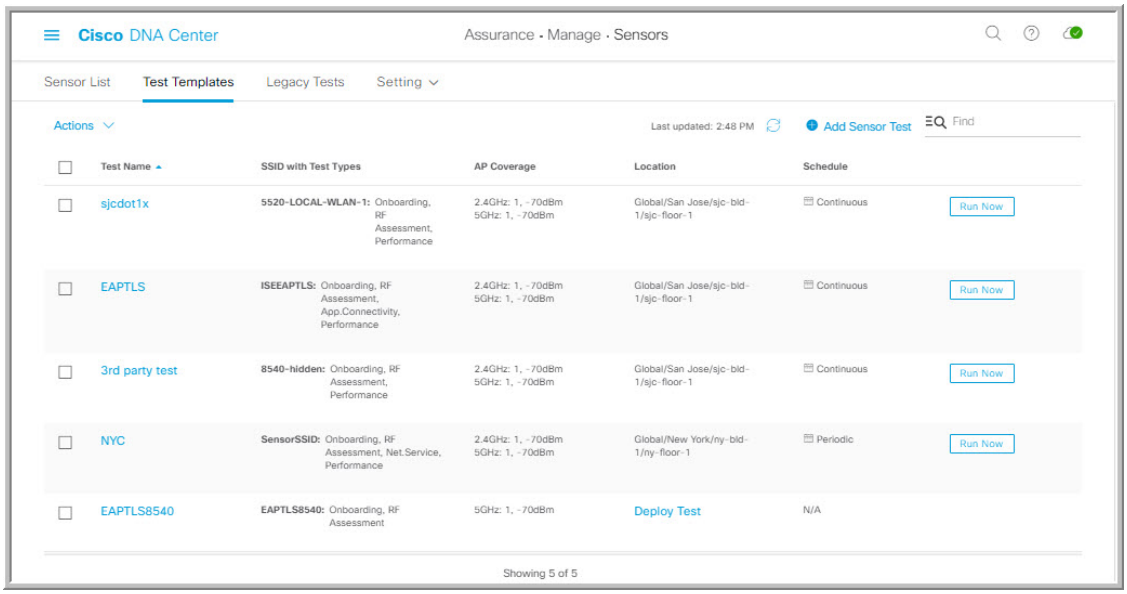
Create sensor-driven test templates. See Create and Run Sensor-Driven Tests Using Templates, on page 204.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Manage** > **Sensors**.

Step 2 Click the **Test Templates** tab.

The **Test Templates** window appears.

Figure 22: Test Templates Window



Step 3 To duplicate a test template, do the following:

a) Check the check box for the test template you want to duplicate.
b) Choose **Actions** > **Duplicate**.
c) In the **Input the new Test Name** dialog box, enter the name for the duplicate of test template.
d) Click **Save**.
The duplicate of the test template appears in the **Test Templates** window. To deploy the test, click **Deploy Test** from the **Location** step.

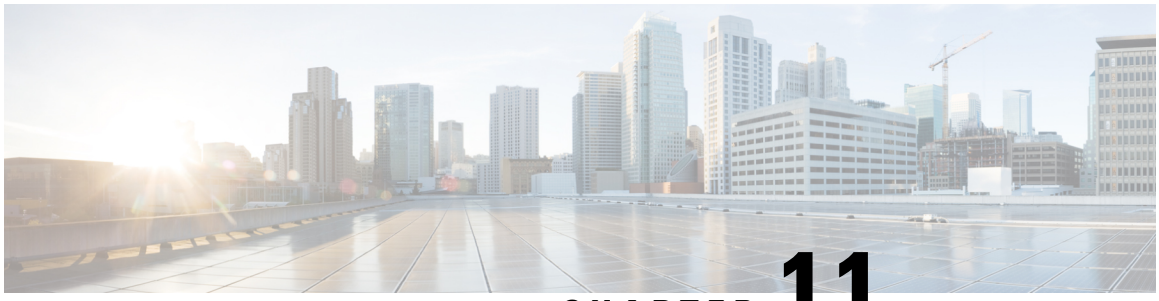
Step 4 To delete a test template, do the following:

a) Check the check box for the test template you want to duplicate.
b) Choose **Actions** > **Delete**.
c) In the **Warning** dialog box, click **Yes**.
The test template is deleted.

Step 5 To undeploy a test template, do the following:

a) Check the check box for the running test template you want to undeploy.
b) Choose **Actions** > **Undeploy**.
c) In the **Warning** dialog box, click **Yes**.
The test template stops running.

Warning If you undeploy a test template, its location and schedule settings are removed.



CHAPTER 11

Monitor Wi-Fi 6 Readiness

- About Wi-Fi 6 Readiness and Its Benefits, on page 211
- Assure the Readiness of Your Wi-Fi 6 Network and Its Benefits, on page 211

About Wi-Fi 6 Readiness and Its Benefits

The Wi-Fi 6 Readiness feature allows you to determine the following:

- The percentage of clients that are Wi-Fi 6 capable.
- The percentage of AP infrastructure that is Wi-Fi 6 ready.
- Based on the above information, recommendations are provided about the actions that you can take to experience the full benefits of the Wi-Fi 6 network.

To provide these recommendations, Cisco DNA Center does the following:

- Assesses the Wi-Fi capabilities of wireless clients.
- Collects AP inventory to determine which of the APs are managed by Cisco DNA 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 6 ready.
- Determines the wireless LAN configuration and whether are not Wi-Fi 6 features are enabled.

Assure the Readiness of Your Wi-Fi 6 Network and Its Benefits

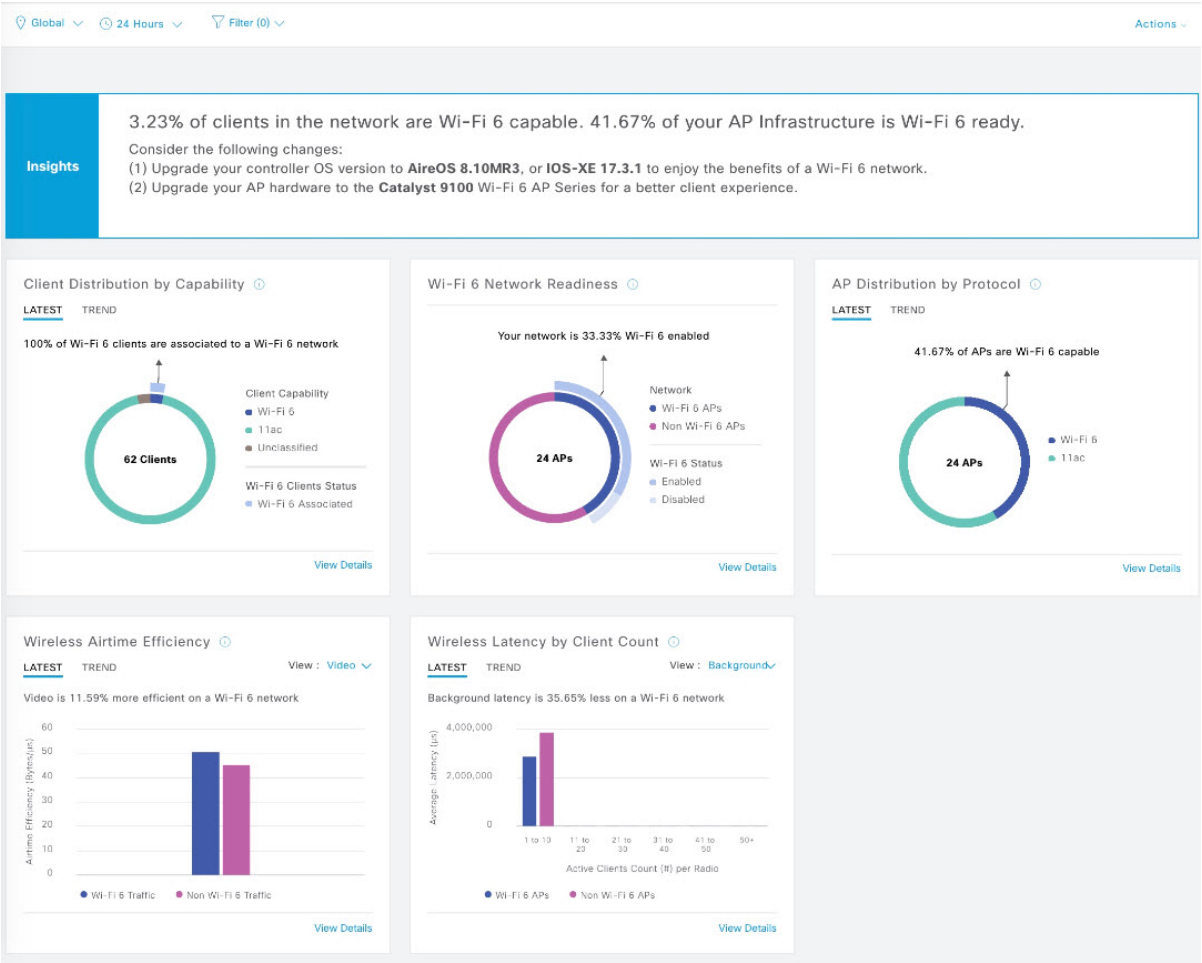
Use this procedure to assure the readiness of your Wi-Fi 6 network and its benefits.

Before you begin

Configure Assurance. See Basic Setup Workflow, on page 13.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Wi-Fi 6**.

The **Wi-Fi 6** dashboard appears.



Step 2 Use the top-menu bar for the following functionality:

Item	Description
Global **Location** pane	Click to display the following icons: • : Click this toggle button to display the **Hierarchical Site View** table. It provides the percentage of wireless clients and wireless network devices in a site. To view information for a particular building, choose **Building View** from the drop-down list. • : 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 that are represented are color coded according to the severity of the problem.
Time Range setting	Enables you to display data within a specified time range on the dashboard. Do the following: **a.** From the drop-down menu, choose 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**.

Item	Description
Filter icon	Contains the **SSID** and **Band** options. Choose 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 customize the dashboard display when you choose **Edit Dashboards** from the drop-down list. See Change the Position of a Dashlet, on page 235 and Create a Custom Dashboard, on page 231.

Step 3 Use the **Insights** area to get an insight about your network. It provides the following information:

- The percentage of clients that are Wi-Fi6 capable.
- The percentage of AP infrastructure that is Wi-Fi6 ready.
- Based on the above information, recommendations on what actions you can take to enjoy the full benefits of the Wi-Fi 6 network are provided.

Step 4 Use the **Client Distribution By Capability** dashlet to determine the protocol capabilities of clients and to determine if the Wi-Fi 6 capable clients joined the Wi-Fi 6 network.

Based on the AP to which the clients are associated, the clients might function at their Wi-Fi 6 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

This dashlet shows all the clients that are associated to the wireless network. It includes two tabs:

- **Latest**: Displayed by default.

  The **outer** segment of the circle shows the number of Wi-Fi 6 capable clients that joined (are associated with) the Wi-Fi 6 network.

  The **inner** circle shows the protocol capabilities of the different clients in the network. The wireless clients are capable of functioning in one of the following protocols:

  - **Wi-Fi 6**: 802.11ax capable clients.
  - **11ac**: 802.11ac Wave1 and Wave2 capable clients.
  - **11n**: 802.11n capable clients.
  - **11abg**: 802.11a, b, or g capable clients.
  - **Unclassified**: The client is listed under **Unclassified** due to the following 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 6 or non-Wi-Fi 6 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 5 Use the **Wi-Fi 6 Network Readiness** dashlet to determine how many APs are Wi-Fi 6 capable and are configured (enabled) to operate in Wi-Fi 6 mode.

Wi-Fi 6 Network Readiness Dashlet

This dashlet provides two levels of details about the APs in the network:

- The **outer** segment of the circle shows the number of Wi-Fi 6 APs that have Wi-Fi 6 (11ax) enabled and the number of Wi-Fi 6 APs that have Wi-Fi 6 disabled.

  Note Even if only one of the radios in an AP has Wi-Fi 6 enabled, then that AP is displayed as operating in Wi-Fi 6 mode.

- The **inner** circle shows the number of APs that are Wi-Fi 6 (11ax) APs and the number of APs that are non-Wi-Fi 6 (11ac,11n, and 11abg) APs.

  Note Wi-Fi6 APs can operate in Wi-Fi 6 mode under the following conditions:

  - The 11ax configuration on the Wi-Fi6 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, the **AP** and **WLC** tabs display. Click the **AP** and **WLC** tabs to display Wi-Fi 6 readiness at radio and band levels respectively.

Step 6 Use the **AP Distribution by Protocol** dashlet to determine the number of APs that have the hardware capability to support the wireless protocols: 802.11ax,11ac, n, or legacy.

AP Distribution by Protocol Dashlet

This dashlet includes two tabs:

- **Latest**: Displayed by default. It shows the number of APs that support Wi-Fi 6 (11ax) protocol and the number of APs that support non-Wi-Fi 6 (11ac, n, or legacy) protocols:
  - **Wi-Fi 6**: 802.11ax capable APs.
  - **11ac**: 802.11ac capable APs.
  - **11n**: 802.11n capable APs.
  - **11abg**: 802.11a, b, or g capable APs.

  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 6 or non-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.

Step 7 Use the **Wireless Airtime Efficiency** dashlet to compare the Average Airtime Efficiency between Wi-Fi 6 traffic and non-Wi-Fi 6 traffic for each of the access categories (voice, video, best effort, and background).

Wireless Airtime Efficiency Dashlet

You can view the wireless airtime efficiency for the following access categories: **Voice**, **Video**, **Best Effort**, **Background**, and **All**. Default is **Voice**.

This dashlet includes two tabs:

- **Latest**: Displayed by default. The bar graph allows you to compare the average airtime efficiency (in units of Bytes per mill-seconds) between Wi-Fi 6 traffic and non-Wi-Fi 6 traffic for the chosen access category.

  The spectrum is efficiently used if the APs radios can send more traffic (successful Bytes transmitted to the client) in less airtime (microseconds) than other networks under similar RF conditions. An efficient network might allow more video or voice calls.

  Traffic is classified as the following:

  - Wi-Fi 6 traffic is the traffic sent from Wi-Fi 6 APs to clients that are associated as Wi-Fi 6.
  - Non-Wi-Fi 6 Traffic is the aggregate of the following:
    - Wi-Fi 6 APs to non-Wi-Fi 6 capable clients.
    - Non-Wi-Fi 6 APs to non-Wi-Fi 6 capable clients.
    - Non-Wi-Fi 6 APs to Wi-Fi 6 capable clients.

  Note A Wi-Fi 6 capable client operates in non-Wi-Fi 6 mode when it connects to a non-Wi-Fi 6 AP.

- **Trend**: Click the **Trend** tab to display a trend chart. This color-coded trend chart shows the number of clients that are associated to the different wireless network modes (Wi-Fi 6 or non-Wi-Fi 6) 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 8 Use the **Wireless Latency by Client Count** dashlet to compare the Average Wireless Latency between Wi-Fi 6 traffic and non-Wi-Fi 6 traffic for each of the access categories (voice, video, best effort, and background).

Typically, AP radios with a higher client count have more latency compared to radios with a lower client count under similar RF conditions.

Wireless Latency by Client Count Dashlet

You can view the wireless latency for the following traffic: **Voice**, **Video**, **Best Effort**, and **Background**. Default is **Voice**.

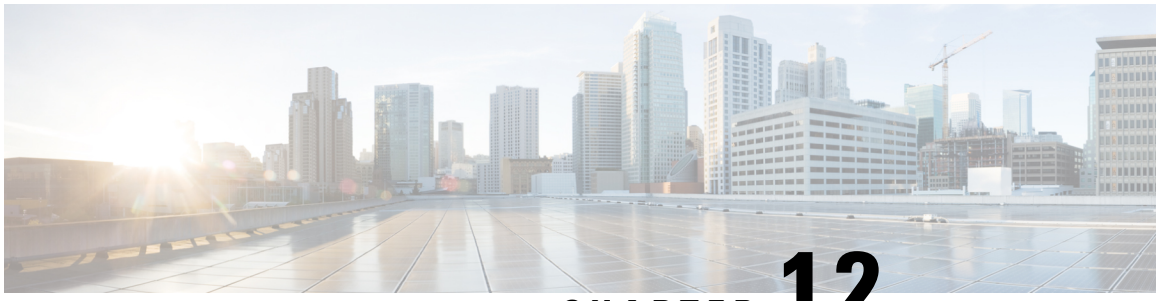
This dashlet includes two tabs:

- **Latest**: Displayed by default. It provides the Average Wireless Latency comparison between the Wi-Fi 6 and non-Wi-Fi 6 AP radios serving similar number of "active" clients. Wireless latency is measured by the time (microseconds) it takes for a packet to be successfully transmitted from an AP to the client.

  Note Active clients include those clients that are associated with the Wi-Fi 6 AP and are actively sending traffic of a given access category.

- **Trend**: Click the **Trend** tab to display a trend chart. The trend chart displays the average wireless latency across all access categories.

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 12

Monitor Power over Ethernet

- About PoE, on page 219
- Setup Workflow for PoE Telemetry, on page 219
- Configure NETCONF on Your Network Devices for PoE Telemetry, on page 221
- Update Telemetry Settings for PoE Telemetry, on page 223
- Monitor PoE-Capable Devices in Your Network, on page 223

About PoE

The Cisco DNA 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 and allows viewing the allocated power and power load of switches.

Setup Workflow for PoE Telemetry

To enable PoE telemetry and analytics in Assurance, you need to perform the required setup tasks. A basic workflow for setup involves the following tasks:

1. Configure NETCONF on the network devices used for PoE telemetry.

   For details, see Configure NETCONF on Your Network Devices for PoE Telemetry, on page 221.

2. Update the telemetry settings in Cisco DNA Center.

   For details, see Update Telemetry Settings for PoE Telemetry, on page 223.

Setup Workflows

The setup workflow for PoE telemetry varies depending on the software version and configuration of Cisco DNA Center and network devices that support PoE telemetry.

If you are doing a fresh installation of Cisco DNA Center, refer to the following table:

Fresh Installation of Cisco DNA 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 Cisco DNA 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 Cisco DNA 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 Cisco DNA Center.

If you are upgrading to Cisco DNA Center from an earlier release, refer to the following 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 Cisco DNA 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 Cisco DNA Center.
• IOS XE version is 16.12.3s. • NETCONF is disabled.	1. Enable NETCONF on the device. 2. Update the telemetry settings in Cisco DNA Center.
• IOS XE version is 16.12.3s. • NETCONF is enabled.	1. Update the telemetry settings in Cisco DNA Center.

If there are changes to the network device that supports PoE telemetry in **Inventory**, refer to the following table:

Network Device Changes in Inventory	
Change to Network Device	**Required Setup Tasks**
Remove a device from Cisco DNA Center **Inventory**, and then add it back.	1. Enable NETCONF on the device. 2. Update the telemetry settings in Cisco DNA Center.

Network Device Changes in Inventory	
Change to Network Device	**Required Setup Tasks**
Add a new device to Cisco DNA Center **Inventory**.	**1.** Enable NETCONF on the device. **2.** Update the telemetry settings in Cisco DNA Center.
Use a replacement device in Cisco DNA Center **Inventory**.	**1.** Enable NETCONF on the device. **2.** Update the telemetry settings in Cisco DNA Center.

Configure NETCONF on Your Network 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 Cisco DNA 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 219.

Step 1 Configure the NETCONF port for an existing network device:

a) In the Cisco DNA Center GUI, click the **Menu** icon (☰) and 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) Click the **Menu** icon (☰) and 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 the following:

```
netconf-yang
```

b) From the **Actions** drop-down list, choose **Save**.

The content is saved to the template.

c) From the **Actions** drop-down list, choose **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) Click the **Menu** icon (☰) and choose **Design** > **Network Profile**.

The **Network Profiles** window appears.

b) Click **+Add Profile** and choose **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, choose **Switches and Hubs**.
g) From the **Template** drop-down list, choose 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) Click the **Menu** icon (☰) and 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 Cisco DNA 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 has an established NETCONF port and the proper NETCONF configuration. For details, see Configure NETCONF on Your Network Devices for PoE Telemetry, on page 221.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and 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**: Choose this option to update the telemetry settings immediately.
- **Later**: Choose this option to schedule the task to update the telemetry settings for another time. Specific the time and date.

Step 7 Click **Apply**.

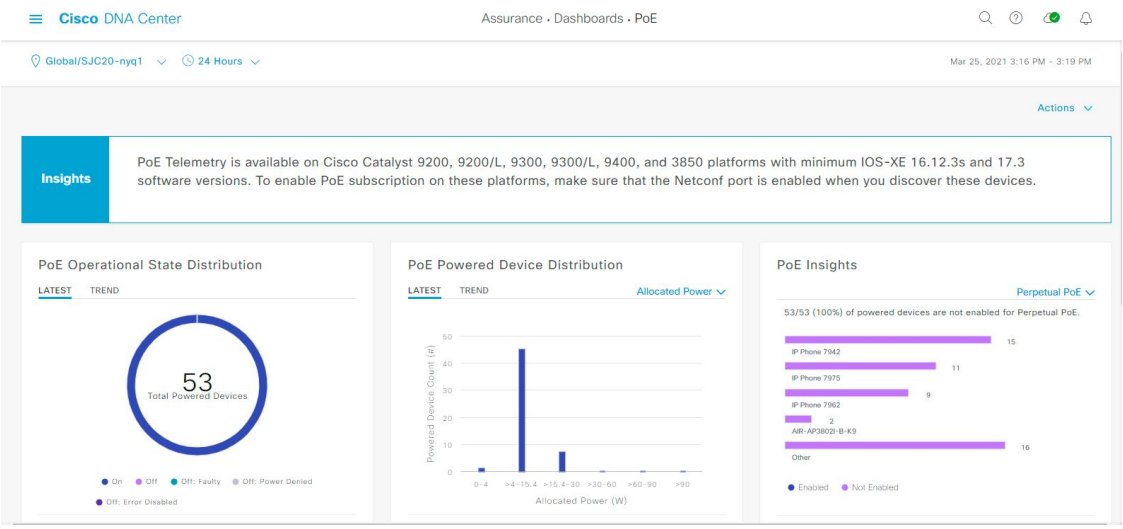
Monitor PoE-Capable Devices in Your Network

Use this procedure to get a global view of PoE-capable devices in your network.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Assurance** > **PoE**

The **PoE** dashboard appears.

Figure 23: PoE Dashboard



Step 2 Click the location option (Global) in the top-menu bar to display the location pane.

The location pane has the following 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 the following options: • **Hierarchical Site View**: Sorts the list at a site level. From the **Apply to Page Location** column, click **Apply** for a site or building to display data only for that location on to the **Network** dashboard. • **Building View**: Sorts the list at a building level. From the **Apply to Page Location** column, click **Apply** for a building to display data only for that building on to the **Network** dashboard.
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 that are represented are color-coded according to the severity of the problem.

Location Option	
Item	**Description**
Topology tool	Click this icon to open the **Topology** tool. The **Topology** window, has the following views: • **Geographical View**: Click this toggle button to display your network in a geographical map. Hover your cursor over a location to view the percentage of healthy devices. • **Topology View**: Click this toggle button to display a topology of how the components in the network are connected. Hover your cursor over a device to display device information, such as device role, IP address, and software version. To obtain a 360° view of the device, click **View Details 360**.

Step 3 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, choose 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 Click the **Actions** drop-down list in the top-menu bar for the following functionality:

- **Edit Dashboard**: Enables you to customize the dashboard display. See Change the Position of a Dashlet, on page 235 and Create a Custom Dashboard, on page 231.

Step 5 Use the PoE dashlets for the following functionality:

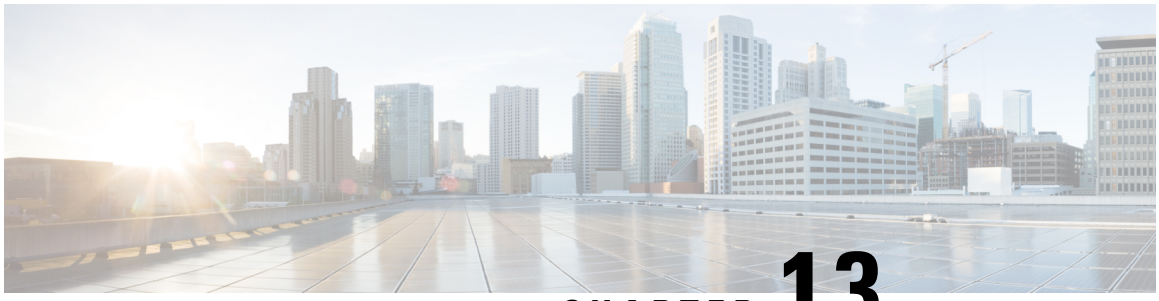
PoE Operation State Distribution Dashlet
Displays the number of PoE-capable devices in your network. The color-coded chart provides the count of devices based on whether they are being supplied with PoE or not. For devices that are not being supplied with PoE, this is further characterized by the reason why. The **Latest** tab provides a 10-minute snapshot view. The **Trend** tab provides the following: • 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 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 to refresh the data in the table that is displayed below the chart.

PoE Powered Device Distribution Dashlet
View the distribution of the devices currently using PoE for a certain criteria. Use the drop-drop list to specify the following criteria: • **Allocated Power** • **Powered Device Class** The **Latest** tab provides a 10-minute snapshot view. The **Trend** tab provides the following: • 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 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 to refresh the data in the table that is displayed below the chart.

Power Load Distribution Dashlet
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 the following: • 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 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 to refresh the data in the table that is displayed below the chart.

PoE Insights Dashlet
View the percentage of the devices currently using PoE which are configured to support the following PoE technologies or meet IEEE Compliance: • **Perpetual PoE** • **Fast PoE** • **IEEE Compliant** • **UPOE+** Use the drop-down list to choose 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 to refresh the data that is displayed in the table below the chart.

PoE Power Usage Dashlet
View the total power usage of devices currently using PoE. The **Latest** tab provides the 10 minutes snapshot view. The pie-chart displays the Consumed Power and Remaining Power of total power usage measured in Watt. The **Trend** tab provides the following: • 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 to view the power usage status of the devices over a time period. You can select the data displayed as horizontal bars to filter the proceeding table based on the power usage, device role and location.



CHAPTER 13

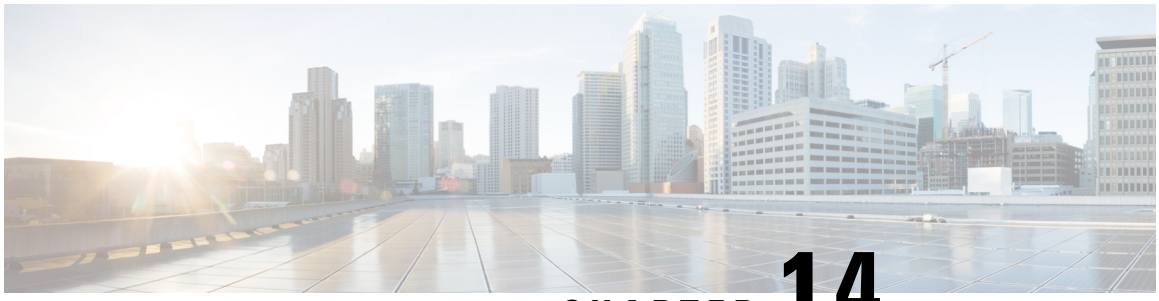
Monitor the Rogue Management Dashboard

• Manage Security Threats on Networks, on page 229

Manage Security Threats on Networks

With the Cisco DNA Center Rogue Management application, you can monitor the threats on your network from unauthorized access points. You can quickly identify the highest priority threats and monitor those threats from the Assurance dashboard.

For details about the Cisco DNA Center Rogue Management application, see the Cisco DNA Center Rogue Management Application Quick Start Guide.



CHAPTER 14

Manage Dashboards

- About Dashboards, on page 231
- Create a Custom Dashboard, on page 231
- Create a Dashboard from a Template, on page 232
- View a Dashboard, on page 233
- Edit or Delete a Dashboard, on page 234
- Duplicate a Dashboard, on page 234
- Mark a Dashboard as a Favorite, on page 234
- Change the Position of a Dashlet, on page 235

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

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and 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 the following 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 the following:

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.

Create a Dashboard from a Template

Creating a dashboard from a template allows you to use a scope to filter the dashboard data. A scope filters devices by location, device type, and other options.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Dashboard Library**.
The **Dashboard Library** window appears, listing all defined dashboards and the templates (at the bottom).

Step 2 In the **Templates** area, click a dashboard template.

Step 3 In the **Create a Dashboard** dialog box, enter a title for the dashboard.

Step 4 Click **Save**.

Step 5 If you want to use an existing scope, select an existing scope and click **Select Scope**.

Skip to Step Step 15 if you selected an existing scope, or continue with the next step if you want to create a new scope.

Step 6 To create a new scope, click **Create New Scope**.
The first step, **Create New Scope**, is displayed.

Step 7 Enter a scope name and click **Next**. If you enter a space in the scope name, the space is converted to an underscore.
The second step, **Select Location(s)**, is displayed.

Step 8 Choose one or more locations to include in the scope by checking or unchecking the check boxes next to them.

Note You can use the search field to filter locations.

Step 9 Click **Next**.
The third step, **Select Filters**, is displayed.

Step 10 If you are using the **Client Health** template, you can use the following filters:

- **Client Type**: Choose wired or wireless to include these types of devices in the scope by checking or unchecking the boxes next to them.
- **SSIDs**: Choose SSIDs to include in the scope by checking or unchecking the boxes next to them. Type in the search field to filter SSIDs. This filter applies only to wireless devices.
- **Host Name**: Enter the hostnames to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.
- **Device Type**: Enter the device OS types (for example, IOS or Android) to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.
- **MAC Address**: Enter the MAC addresses to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.
- **IP Address**: Enter the IP addresses to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.

Step 11 If you are using the **Network Health** template, you can use the following filters:

- **Network Device Type**: Choose one or more device types to include in the scope by checking or unchecking the check boxes next to them. Type in the search field to filter devices.
- **Network OS**: Choose network OS versions to include in the scope by checking or unchecking the check boxes next to them. Type in the search field to filter versions.
- **IP Address**: Enter the IP addresses to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.
- **Host Name**: Enter the hostnames to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.

Step 12 Click **Next**.
The fourth step, **Preview**, is displayed.

Step 13 Click the **Dynamic list** toggle to enable or disable a dynamic list of clients that is updated based on the selected filters.

Step 14 Click **Save** to save the scope.
A confirmation dialog is displayed.

Step 15 (Optional) Drag and drop any dashlet to customize its location on your dashboard.

Step 16 You can remove a dashlet from your dashboard from doing the following:

a) Click the trash can icon located in the top-right corner of the dashlet.
b) In the dialog box, click **Delete**.

Step 17 Click **Save** to save your dashboard.

Note If this is a new scope, it can take up to 15 minutes to display data in the dashboard.

View a Dashboard

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and 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

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and 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 the following:

- To make changes, choose **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, choose **Delete Dashboard** from the **Actions** menu. Click **Delete** in the confirmation dialog.

Duplicate a Dashboard

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and 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 is displayed.

Step 7 Click **OK**.

Mark a Dashboard as a Favorite

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and 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.

Step 1 Do one of the following:

- In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Health**.

  The **Overall Health** dashboard appears.

- In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Health** > **Network Health** tab.

  The **Network Health** dashboard appears.

- In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Health** > **Client Health** tab.

  The **Client Health** dashboard appears.

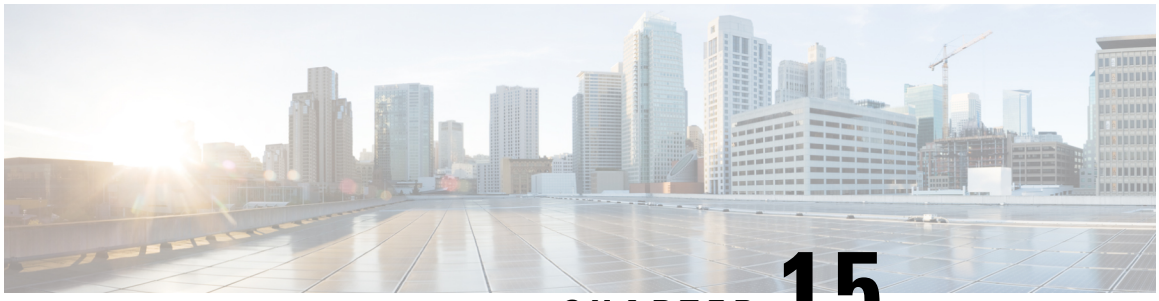
- In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Health** > **Application Health** tab.

  The **Application Health** dashboard appears.

Step 2 Click the **Actions** drop-down list (located at the top-right corner) and choose **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**.



CHAPTER 15

Observe Network Trends and Gain Insights

- About Network Trends and Insights , on page 237
- View Network Trends and Obtain Insights, on page 237
- Compare Access Points in Network Heatmaps, on page 241
- Compare KPI Values with Peers in Your Network, on page 243
- Compare Buildings, AP Model Families, and Wireless Endpoint Types, on page 245
- View and Monitor Network Performance Using Baselines, on page 248

About Network Trends and Insights

Cisco AI Network Analytics uses machine learning algorithms and AI techniques to provide the following:

- **Trends and Insights**: Determine global patterns (trends) and deviations to provide system-generated insights.
- **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 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). The following 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.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Network Insights**.

The **Network Insights** window appears with filters: **Capacity**, **Coverage**, and **Throughput**. Click the appropriate filter to refresh the data in the table. The Capacity filter is selected by default.

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 2019.
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 the following 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 that was used on the AP on which the insight was observed. Values are **2.4 GHz**, **5 GHz**, or both band frequencies.
KPI	Key Performance Indicator (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**.

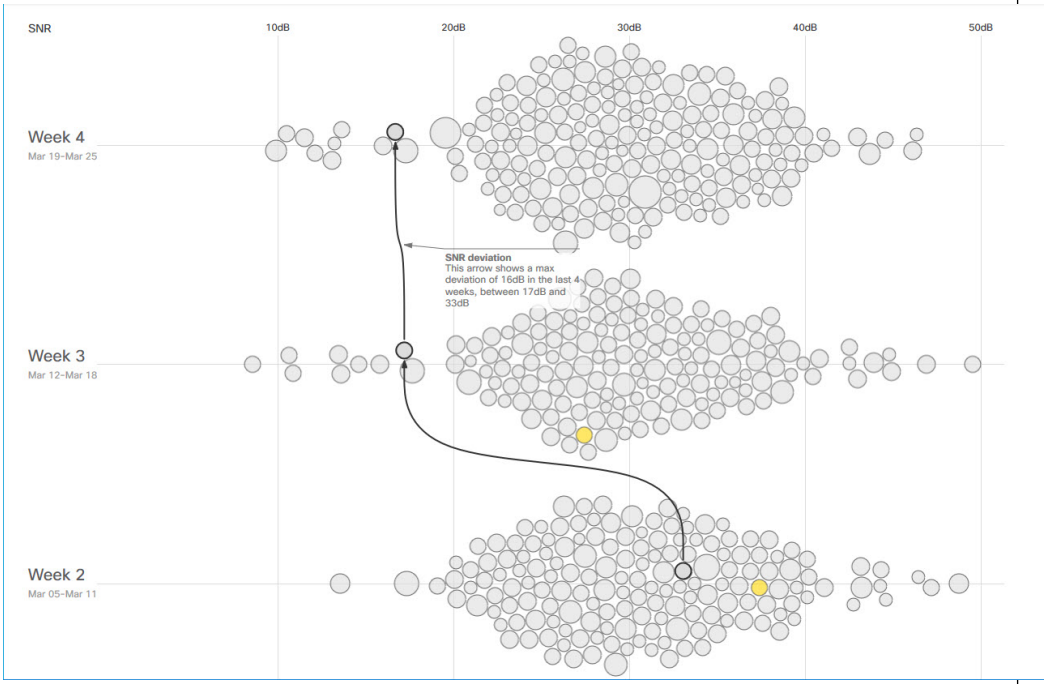
Step 2 From the **Insight** column, click an insight to open a slide-in pane, which provides the following information:

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 Intelligent.
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	The beeswarm chart displays the performance of the client devices in your network in a 4-week time period as shown in the following figure. The bottom of the chart represents week 1; the top of the chart represents week 4. If there is a systematic deviation of network behavior over a time period, that trend is displayed by arrows in the chart. ***Figure 24: Beeswarm Chart***  **Note** • Each circle in the beeswarm chart represents the following: • **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.

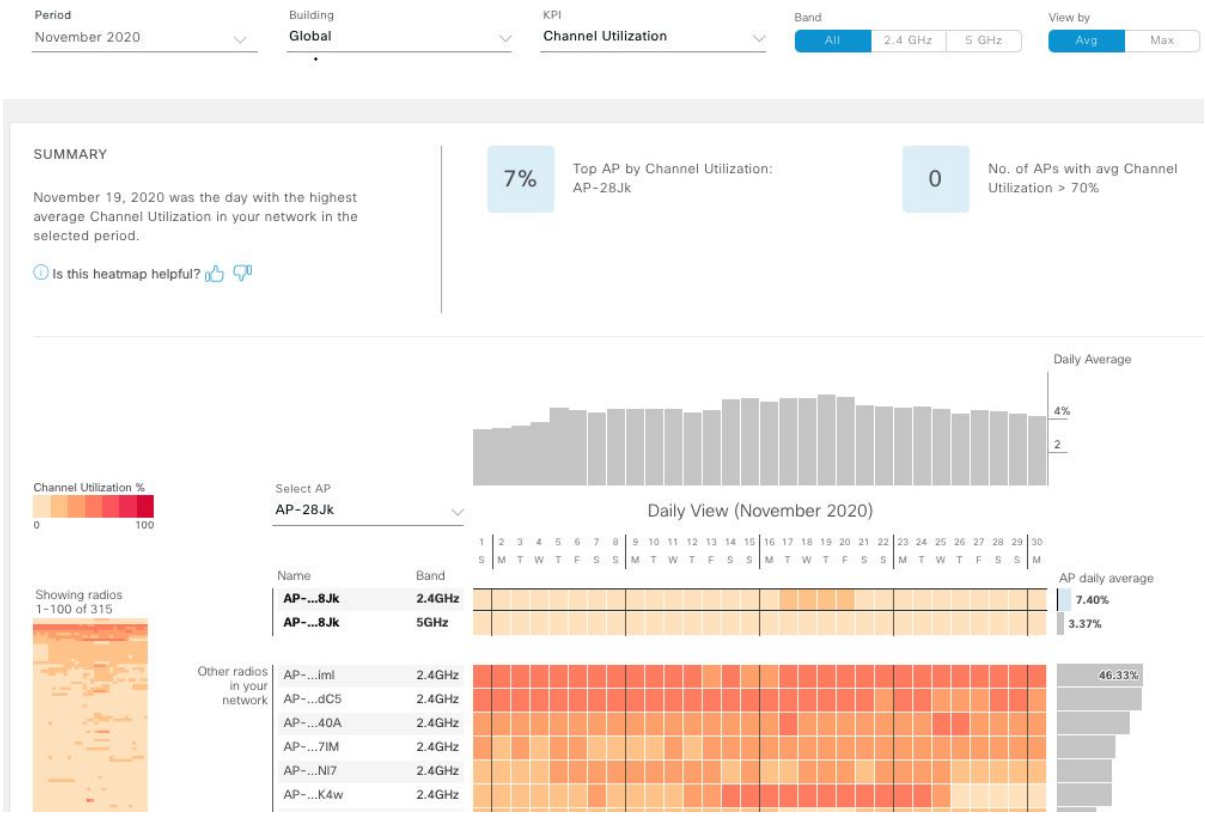
Compare Access Points in Network Heatmaps

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 choose 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.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Network Heatmap**.

The **Network Heatmap** window appears with the following information:

Figure 25: Network Heatmap Window



Network Heatmap Window	
Item	**Description**
Period	Displays information in the heatmap for the month you choose from the drop-down list.
Building	Displays information in the heatmap for your entire global network or for a specific site and building that you choose from the drop-down list. Default is **Global**.

Network Heatmap Window	
Item	**Description**
KPI drop-down list	Displays information in the heatmap for the KPI you choose from the drop-down list. Default is **Client Count**.
Band	Displays information in the heatmap for the band frequency you choose. Options are: **All**, **2.4 GHz**, and **5 GHz**. Default is **All**.
View By	Allows you to view the information in the heatmap based on the option you choose. Based on the KPI you choose, 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	Displays a summary of the insight gained from the heatmap analysis. Provides the following type of information: • The day of the month that was the busiest. • Number of APs that had no clients per radio. • Number of APs 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 choose 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	Allows you to search for and select an AP. Do the following: **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 Daily Avg, **Min**, or **Max** graph	Depending on the **View By** option you chose, the appropriate graph is displayed • If you chose **Avg**, the graph shows the daily average value and highlights the highest daily average. • If you chose **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.

Network Heatmap Window	
Item	**Description**
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 choose the appropriate option from the drop-down list.
AP Heatmap area	Contains the following: • **Radios in Your Network**: Displays the name of the AP and the band frequency that was used by the client. Click on the icon next to the AP to open the **Device 360** page for that AP. Depending on the band frequency you choose 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 choose 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.

Step 2 To view the heatmap data for additional radios, scroll down to the bottom of the window and choose the appropriate option from the drop-down list.

Compare KPI Values with Peers in Your Network

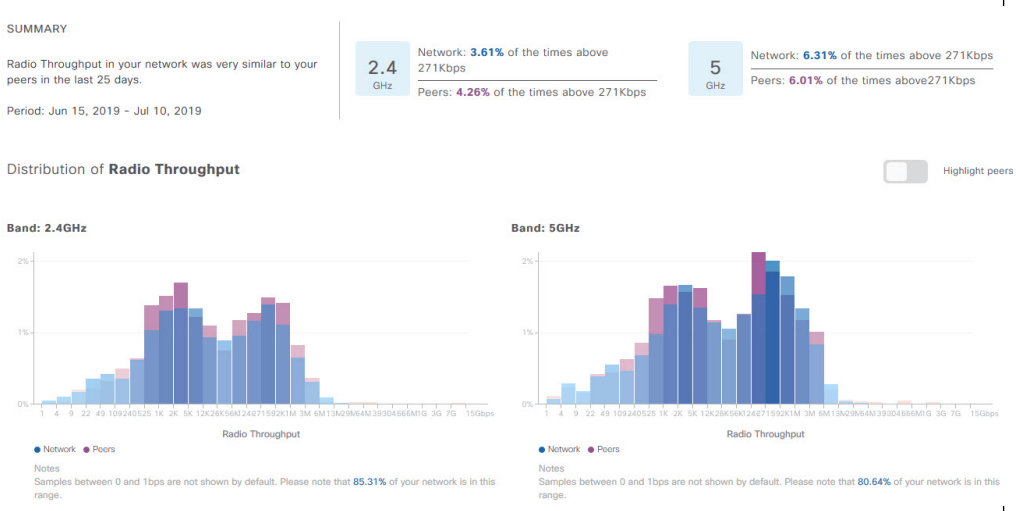
Use this procedure to determine how your network is performing compared to your peer networks for a selected Key Performance Indicators (KPI).

Note The peer networks that are used for comparison are of similar network size.

For computations, peer comparison uses a couple of months data from the date of onboarding.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Peer Comparison**.

The **Peer Comparison** window appears with the following information:

Peer Comparison Window	
Item	**Description**
KPI drop-down list	Choose a KPI from the drop-down list. Options are: **Radio Throughput**, **Cloud Apps Throughput**, **Radio Resets**, **Packet Failure Rate**, **Interference**, and **RSSI**. Default is **Radio Throughput**.
Show	Choose the day for which you want to compare the KPI values between your network and your peer networks. Default is **All**.
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.
Highlight Peers toggle button	Allows you to toggle between your network and the peer network graphs.
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 the following figure. To highlight the KPI values for the peer networks, click the **Highlight Peers** button. ***Figure 26: Peer Comparison Bar Graph***  The colors in the graph represent the following: • **Blue**: Your network. • **Pink**: Peer networks.

Step 2 To display the KPI values for your network and your peer networks for a specific day, choose the appropriate day from the **Show** area.

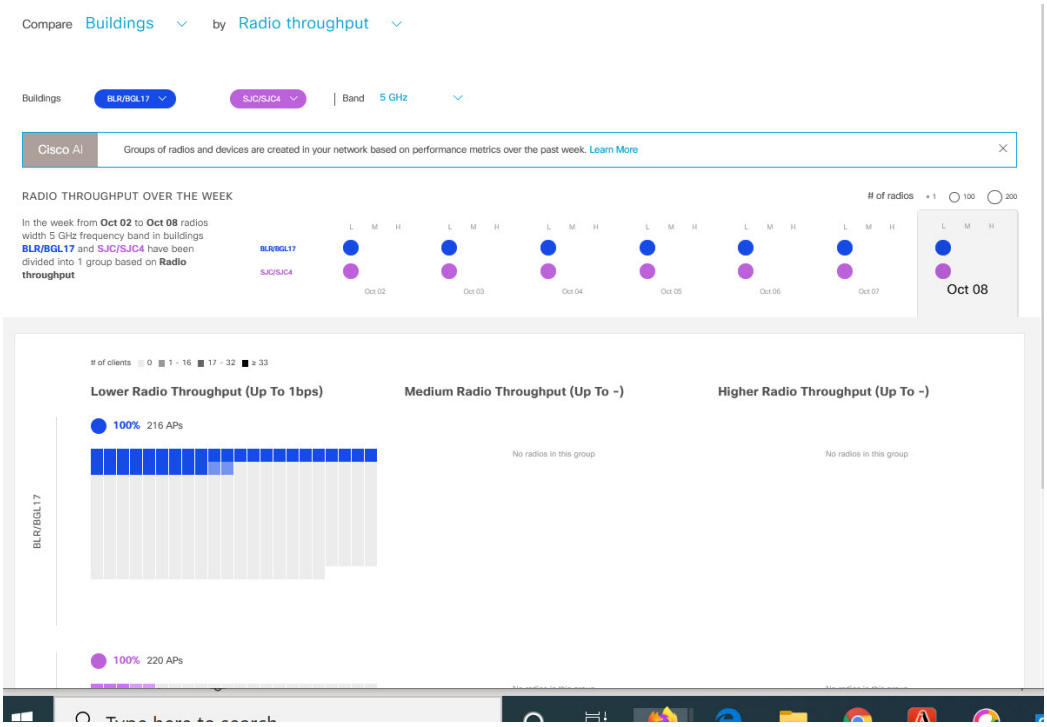
Compare Buildings, AP Model Families, and Wireless Endpoint Types

Use this procedure to view, compare, and identify performance improvement opportunities for objects in your network (buildings, AP model families, wireless endpoints) across selected Key Performance Indicators (KPIs).

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Network Object Comparison**.

The **Network Object Comparison** window appears with the following information:

Figure 27: Network Object Comparison Window



Network Object Comparison Window	
Item	**Description**
Compare drop-down list	Choose the object in your network that you want to compare. Options are: **Buildings** (sites), **AP Model Families**, or **Wireless Endpoints** (Android device, Android phone, IOS tablet, IOS phone, Linux workstation, and so on).

Network Object Comparison Window	
Item	**Description**
By KPI drop-down list	Choose a KPI that you want to use to compare the objects in your network. For **Buildings**, the options are: • **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 are: • **Radio Throughput** • **Interference** • **Media Apps Throughput** • **Average Client RSSI** • **Channel Utilization** • **Average Client SNR** • **Cloud Throughput** • **Social Throughput** For **Wireless Endpoints**, the options are: • **Average AAA Time** • **Average Onboarding Time** • **Average DHCP Time**

Network Object Comparison Window	
Item	**Description**
Buildings **AP Model Families** or **Wireless Endpoints** drop-down list	Choose 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 color. Choose 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 color.
Band	Choose 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. The darker color block has more clients or devices than the lighter color block.
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 the following 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 the following: • The types of devices that the client's onboarded in each site. For example, 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

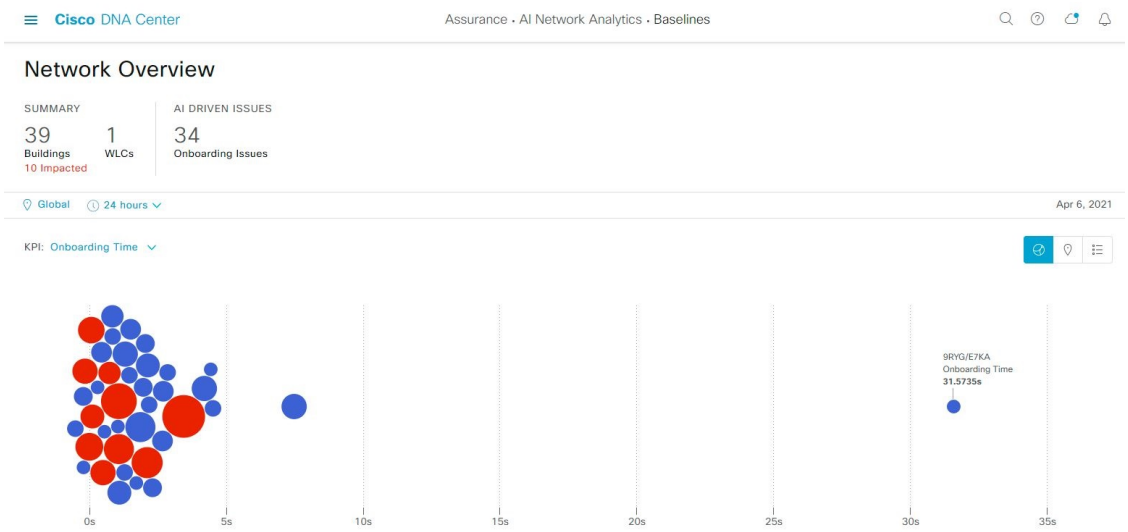
Cisco AI Network Analytics uses the most advanced machine learning techniques to define the baseline that is relevant to your specific network and sites. With this information Cisco AI Network Analytics is able to define what is normal for each network and site at a specific moment, and identify the most important issues.

Use this procedure to explore and monitor the network performance using machine learning algorithm derived baselines.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Baselines**

The **Baselines** dashboard appears.

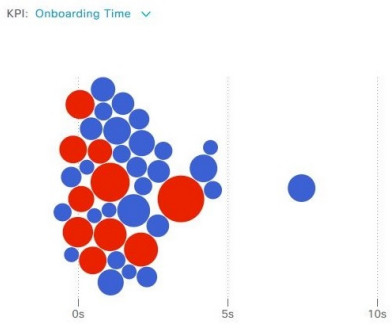
Figure 28: Baselines Dashboard



Step 2 Use the Network Overview window to view the following information:

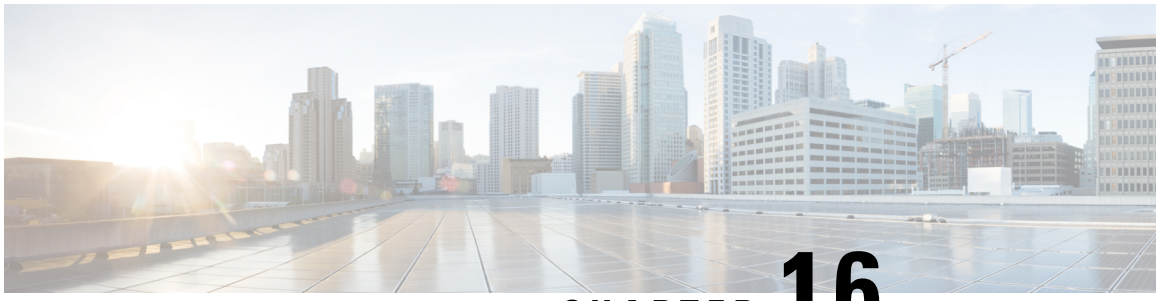
Network Overview Window	
Item	**Description**
Summary	Displays the total number of buildings, buildings impacted with issues and WLCs in your network.
AI Driven Issues	Displays the issues detected by Cisco AI Network Analytics, triggered based on deviations from the predicted baseline for your specific network environment.
Global Location drop-down lsit	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.

Network Overview Window	
Item	**Description**
Time Range setting	Enables you to display data within a specified time range on the dashboard. Do the following: • From the drop-down menu, choose the length of the range: 24 Hours, or the custom range • Specify the Start Date and the End Date. • Click Apply
KPI drop-down list	Choose a KPI from the drop-down list. Options are: **Onboarding Time**, **Onboarding Failures**, **DHCP Time**, **Authentication Time**, and **Association Failures**. Default is **Onboarding Time.**
Map View	Click this toggle button to display the health of all the network sites on a geographic location-oriented map view of your network.
List View	Click this toggle button to display the sites and buildings from your network in a list format.

Network Overview Window	
Item	**Description**
Beeswarm Chart	Click this toggle button to view the beeswarm chart which provides the insights about the performance of the client devices of your network with respect to the selected KPI.  In this case, the entity in the beeswarm chart is a building and it is represented in a circles. Each circle in the Beeswarm chart represents the following: • Blue color: The circle represents a building. Hover your cursor over a circle in the chart to get information, such as location, KPI, SSID, WLCs and client count. • Red color: 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, WLCs, 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 on cirlce to display the building view for the following information:

Building View
Displays the specific information of a site or building. You can select the KPIs, SSID and WLC from the respective drop down list to view the data. Use the timeline slider to specify a more granular time range. You can click and drag the timeline boundary lines to specify the time range. The color coded charts are displayed below the timeline slider, to determine how your network is performing, issues triggered based on the deviations from the predicted baseline for a selected Key Performance Indicator (KPI) within the specified time period. Hover and move your cursor over the charts to view synchronized tooltips that displays duration, predicted upper and predicted lower range at a selected point in time. The color codes represents the following: • Red color represents the AI driven issues • Blue color represents the average KPI duration • Green color represents the predicted KPI Click **View Details** to open a slide-in pane with additional details, depending on the KPI you choose from the KPI charts. In the slide-in pane, the color coded charts are displayed for Average KPI Duration(s) (for example 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, data is displayed in the table contains 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 chosen time interval over the individual client count readings observed in the 30 minute window.



CHAPTER 16

Manage Intelligent Capture

- About Intelligent Capture, on page 253
- Supported Devices for Intelligent Capture, on page 253
- Intelligent Capture Best Practices, on page 255
- Live and Scheduled Capture Sessions for a Client Device, on page 255
- Data Packet Capture for a Client Device, on page 262
- Intelligent Capture for Access Points, on page 267
- Troubleshoot Intelligent Capture, on page 275

About Intelligent Capture

For Cisco DNA Center, all information about device and client health is typically available from Cisco wireless controllers. Intelligent Capture provides support for a direct communication link between Cisco DNA Center and access points (APs), so each of the APs can communicate with Cisco DNA Center directly. Using this channel, Cisco DNA Center can receive packet capture data, AP and client statistics, and spectrum data. With the direct communication link between Cisco DNA Center and APs, Intelligent Capture allows you to access data from APs that is not available from wireless controllers.

Note Intelligent Capture is only supported for APs in either local or FlexConnect mode.

Supported Devices for Intelligent Capture

The following table lists the Cisco Wireless Controllers that support Intelligent Capture:

Supported Cisco Wireless Controllers	
Device	**Minimum Supported Software Version**
Cisco 3504 Wireless Controller	AireOS 8.8.125.0
Cisco 5520 Wireless Controller	AireOS 8.8.125.0
Cisco 8540 Wireless Controller	AireOS 8.8.125.0

The following table lists the Cisco Catalyst Wireless Controllers that support Intelligent Capture:

Supported Cisco Catalyst Wireless Controllers	
Device	**Minimum Supported Software Version**
Cisco Catalyst 9800 Series Wireless Controllers	IOS-XE Gibraltar 16.12.1.s

The following table lists the Cisco APs that support Intelligent Capture:

Supported Cisco APs		
Device	**Minimum Supported AireOS Software Version**	**Minimum Supported IOS-XE Software Version**
Aironet 1540 APs[3]	8.10.105.0	16.12.1.s
Aironet 1560 APs	8.10.105.0	16.12.1s
Aironet 1815 APs[1]	8.10.105.0	16.12.1s
Aironet 1830 APs[1]	8.10.105.0	16.12.1s
Aironet 1840 APs[1]	8.10.105.0	16.12.1s
Aironet 1850 APs[1]	8.10.105.0	16.12.1s
Aironet 2800 Series AP	8.8.125.0 or 8.10	16.12.1s
Aironet 3800 Series APs	8.8.125.0 or 8.10	16.12.1s
Aironet 4800 Series APs[4]	8.8.125.0 or 8.10	16.12.1s
Catalyst 9105 AP[1]	8.10 MR3	17.3.1
Catalyst 9115 AP[1]	8.10.105.0	16.12.1s
Catalyst 9120 AP	8.10.105.0 8.10.112.0 (for Spectrum Analysis)	16.12.1s 17.2.1 (for Spectrum Analysis)
Catalyst 9130 AP[2]	8.10 MR3	17.3.1
Catalyst IW6300 Heavy Duty Series APs	8.10.105.0	17.1.1s
Catalyst ESW6300 Embedded Services APs	8.10.105.0	17.1.1s

[3] Spectrum Analysis is *not supported* on the following APs: Aironet 1540 AP, Aironet 1800 Series APs, Catalyst 9105 AP, and Catalyst 9115 AP.

[4] Data Packet Capture is only supported on Aironet 4800 APs and Catalyst 9130 AP.

Intelligent Capture Best Practices

The following are best practices to ensure Intelligent Capture functions optimally in Cisco DNA Center:

- After a new wireless controller device is added to Cisco DNA Center, disable any Intelligent Capture 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 Cisco DNA Center, disable all Intelligent Capture settings.
- Before upgrading any of managed wireless controllers or reimaging Cisco DNA Center, disable all Intelligent Capture settings, and then re-enable them after completing the upgrade.

Live and Scheduled Capture Sessions for a Client Device

About Capture Sessions for a Client Device

You can run the following types of capture sessions for a client device:

- **Live Capture Sessions**: Live capture sessions can be started immediately and can run for up to three hours for that specific client. See Enable a Live Capture Session for a Client Device, on page 256.
- **Scheduled Capture Sessions**: Scheduled capture sessions are scheduled for a future time and can run for up to eight hours. See Schedule and Manage Capture Sessions for a Client Device, on page 261.

Note Because scheduled capture and live capture sessions collect the same data, a scheduled capture session that is currently running is equivalent to a live capture session.

Live and scheduled capture sessions allow you to collect data for onboarding events (2-second intervals) and RF statistics charts (5-second samples). This data is displayed in the **Client 360** > **Intelligent Capture** window.

Client Capture Session Limitations

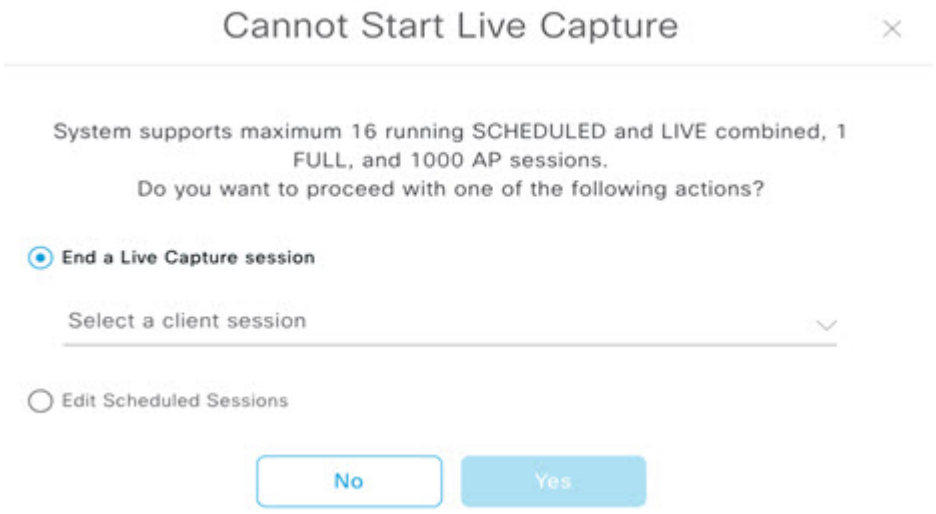
Client capture sessions have the following limitations:

- 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.

  The maximum number of live capture sessions is 16, so if 16 live capture sessions are running at the same time, no slots are available for scheduled capture sessions.

  The maximum number of concurrent scheduled capture sessions is 12, which always leaves four (16 minus 12) available slots for live capture sessions.

  If these maximum values are exceeded, for example, you try to start a seventeenth live capture session, the following error message is displayed. Click **Yes** in the error message dialog box, and then select a capture session for which you want to end the live capture.



Note The 16-time-slot limit is enforced by the wireless controller.

When capture sessions are configured on Cisco DNA Center, any live or scheduled capture sessions that Cisco DNA 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 Cisco DNA 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.

About Client Statistics

Live and scheduled 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 stats are enabled for the AP to which the client is connected.

When client statistics are collected, they are displayed on the four RF statistic charts on the **Client 360** > **Intelligent Capture** window.

Enable a Live Capture 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.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and 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 the following:

- In the **Client Devices** table, click the hyperlinked Identifier or the MAC address of the device.
- In the **Search** field (located on the top-right corner), enter one of the following: user ID (authenticated through Cisco ISE), IP address, or 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 the following information:

Attention If a ⚠ icon with the message **GRPC link is not ready (CONNECTING)** appears next to the client name, see Client or Access Point Unable to Send Intelligent Capture Data to Cisco DNA Center, on page 275 for more details.

Figure 29: Intelligent Capture Window of a Client

Step 5 Use the timeline slider for the following 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	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 perform a live capture session, do the following:

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 Capturing** to stop the live capture session.

Note Live capture sessions run for three hours. After three hours, a dialog box for extending the session appears.

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: Filter for only anomaly events. **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.

Onboarding Events Dashlet	
Item	**Description**
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 will be 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.
List of Onboarding, Incomplete, and Anomaly Events	View the list onboarding, incomplete, and anomaly events in chronological order. Events are color-coded to indicate the following: : Successful onboarding event. : Incomplete event. : Anomaly event. **Note** Events with a icon 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.

Onboarding Events Dashlet	
Item	**Description**
Event Details	You can click an event group or individual event to view the following 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 icon that appears next to the event indicates that the event has captured packets. The **Auto Packet Analyzer** section displays a graph with the following 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. De-authentication 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 the following information:

- The location of the client and APs on the floor.
- Heat map 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, throughtput, and packet drop rate.

  The color on the map indicates the client's health:

: Good : Fair : Poor

- The tracking of the client for a one-minute interval surrounding the time of a selected onboarding event.
- The replay and stop or start controls below the map can be used to control the viewing.

Note The Client Location feature requires that CMX is integrated with Cisco DNA Center. For details, see the Integrate Cisco CMX for Wireless Maps, on page 281 chapter.

Step 9 Use the **RF Statistics** dashlet to view detailed RF information.

There are four charts that displays the AP client statistics for the client. See About Client Statistics, on page 256. The color-coded data contains the following 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 the following 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 period. To change the view to the default, click the icon.

Step 10 To run a Data Packet Capture for a client device, see Run Data Packet Capture for a Client Device, on page 264.

Schedule and Manage Capture Sessions for a Client Device

Use this procedure to schedule a capture session and to stop, edit, or delete a scheduled capture session.

Client capture sessions collect the following data:

- Data packets for onboarding events and **RF Statistics** chart data (5 second samples) displayed in the **Client 360** > **Intelligent Capture** window. See Enable a Live Capture Session for a Client Device, on page 256.
- Data for the charts and tables displayed in the **Device 360** > **Intelligent Capture** window. See View RF Statistics and Manage Spectrum Analysis Data for an Access Point, on page 270.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Assurance** > **Intelligent Capture Settings**.

The **Client Schedule Capture** window appears.

Step 2 To schedule a client capture session, click **+ Schedule Client Capture**.

In the **Schedule Client Capture** slide-in pane, do the following:

a) In the **Start Time** area, specify when you want the capture session to start. Options are **Run Now** and **Run Later**.
b) Click the **Duration** drop-down list to specify the duration.

c) Click the **Select Client Devices** drop-down list and enter a search string that returns matches for the categories: client user ID, host name, or MAC address.

Note Search returns a maximum of 10 matches for each category, so refine your search string if you do not find your entry.

Note For more details about capture sessions, see About Capture Sessions for a Client Device, on page 255.

d) Click **Save**.

Step 3 To stop a running capture session, do the following:

a) Click the **In-progress Captures** tab.
b) Select a client from the table.
c) Click **Stop Capture**.

Step 4 To edit a capture session that has been scheduled for a future time, do the following:

a) Click the **Scheduled Captures** tab.
b) Select a client from the table.
c) Click **Edit Schedule**.

Step 5 To delete a completed capture session, do the following:

a) Click the **Completed Captures** tab.
b) Select a client from the table.
c) Click **Delete Schedule**.

Data Packet Capture for a Client Device

About Data Packet Capture for a Client Device

Data Packet Capture allows you to capture network data into PCAP files, which can be downloaded and viewed in Wireshark. In addition, if you choose to integrate with the Network Analysis Module (NAM), you can capture the following information for a client device: accessed applications and ports, QoS data, packet loss, wireless delay, and jitter. For information about NAM integration, see About NAM Integration, on page 263.

To run Data Packet Capture, see Run Data Packet Capture for a Client Device, on page 264.

Data Packet Capture Limitations

Data Packet Capture has the following limitations:

- Data Packet Capture is only supported on Cisco Aironet 4800 APs and Cisco Catalyst 9130 APs. If Data Packet Capture is enabled and the client roams to an AP that does not support it, packet capture stops until the client reconnects to an AP that supports packet capture.
- Only one Data Packet Capture session can run at a time.

- As for all Intelligent Capture features, clocks must be synchronized between Cisco DNA Center and the Cisco Wireless Controller for Data Packet Capture to work. Ensure that the wireless controller is connected to a Network Time Protocol (NTP) server.
- Each Data 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.

About NAM Integration

If you have a Network Analysis Module (NAM) or vNAM server running software version 6.4(2) or later, you can integrate your NAM server with Cisco DNA Center. For information about installation and configuration, see the *Cisco Prime Virtual Network Analysis Module (vNAM) Installation and Configuration Guide*.

With NAM integration and Full Packet Capture enabled for a client, data is provided to the **Wireless Packet Application Analysis** charts in the **Client 360** > **Intelligent Capture** window. The table and charts provide information on the applications used by the client, their QoS settings, packet loss, wireless delay, and jitter.

To integrate your NAM server with Cisco DNA Center, do the following:

1. Configure an IP address on the NAM data port.
2. Configure the gRPC collector.

Note NAM integration is not supported on Cisco DNA Center clusters that use IPv6 addresses.

Configure an IP Address on the NAM Data Port

Use this procedure to configure a valid IP address on the data port of the NAM or vNAM. This is required to integrate with NAM.

Note The data port is meant for receiving packets only; it does not respond to requests. Consequently, pinging the data port will time out even if you have the IP address configured correctly. Make sure that the IP address is valid and reachable from Cisco DNA Center.

Step 1 Log in to the CLI of the NAM server.

Step 2 Enter the command **show data-port ip-addresses**.
The command displays the port number and IP address:

```
Device# show data-port ip-addresses
Port number: 1
IPv4 address: 172.20.125.125
```

Step 3 If nothing is displayed for the **show data-port ip-addresses** command, enter the command **data-port 1 ip-address** *ip-address* to assign an IP address to port 1.

Step 4 Run the **show data-port ip-addresses** command again to verify that data-port 1 has been assigned an IP address.

Step 5 Record the IP address of data-port 1 or one of the other displayed ports.

Step 6 Verify that **cdb-export** is enabled in Cisco DNA Center. To do this, enter the command **show cdb-export all**. If nothing is displayed, enter the command **cdb-export collector 1 ip-address** *IP-address-of-Cisco-DNA-Center*.

Step 7 Make sure that data packets from Cisco DNA Center are processed by entering the command **autocreate-data-source erspan**.

Step 8 Make sure that the time on the NAM or vNAM server and Cisco DNA Center is synchronized. You can synchronize the time from the NAM user interface by choosing **Administration** > **System** > **System Time**.

Configure the gRPC Collector

Use this procedure to configure a gRPC collector for NAM integration. gRPC is an open source high performance RPC (Remote Procedure Call) framework.

Before you begin

Configure an IP address on the NAM data port. See Configure an IP Address on the NAM Data Port, on page 263.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Data Platform**.

The **Data Platform** window appears.

Step 2 Click the **Collectors** tab.

The **Collectors** window appears.

Step 3 Click **GRPC-COLLECTOR**.

The **GRPC-COLLECTOR** window appears.

Step 4 Click **+ Add**.

The **gRPC Collector Configuration** window appears.

Step 5 Add only one **GRPC-COLLECTOR** configuration. Do the following:

a) In the **ConfigData** area, check the **Agent Export** check box to export the network packet data to NAM.
b) In the **Agent IP Address** field, enter the IP address of the data port recorded (refer to Step 5, on page 263 from Configure an IP Address on the NAM Data Port, on page 263).
c) In the **Configuration Name** field, enter a unique name for the GRPC collector configuration.
d) Click **Save Configuration**.

Run Data Packet Capture for a Client Device

Use this procedure to run a Data Packet Capture for a client device.

Before you begin

To retrieve information about accessed applications and ports, QoS data, packet loss, wireless delay, and jitter, you must enable NAM integration. For details, see About NAM Integration, on page 263.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and 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 the following:

- In the **Client Devices** table, click the hyperlinked Identifier or the MAC address of the device.
- In the **Search** field (located on the top-right corner), enter one of the following: user ID (authenticated through Cisco ISE), IP address, or 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 the following information:

Attention If a ⚠ icon with the message **GRPC link is not ready (CONNECTING)** appears next to the client name, see Client or Access Point Unable to Send Intelligent Capture Data to Cisco DNA Center, on page 275.

Figure 30: Intelligent Capture Window of a Client

Step 5 Use the timeline slider for the following 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. 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 run a Data Packet Capture, use the **Data Packet Capture Area** (located on the top-right corner) for the following functionality:

Data Packet Capture Area	
Item	**Description**
Run Data Packet Capture button	Use this button to start a Data Packet Capture for the client. Data Packet Capture files are used for troubleshooting and the **Wireless Packet Application Analysis** dashlet. If Data Packet Capture is currently running for the client, click **Data Packet Capturing Stop** to stop it. **Note** Only one Data Packet Capture can run at a time. If you click **Run Data Packet Capture** while Data Packet Capture is running, a dialog box appears with the option to either end the current capture or start a new capture. When a Data Packet Capture session is configured on Cisco DNA Center, any Data Packet Capture sessions that Cisco DNA Center is not aware of are removed (such as full packet capture sessions that were directly configured on the wireless controller). **Note** As for all Intelligent Capture features, time zones must be synchronized between Cisco DNA Center and the Cisco Wireless Controller for Data Packet Capture to work. Ensure that the wireless controller is connected to a Network Time Protocol (NTP) server. **Note** New sets of PCAP files are started each time a new capture session is started.
Download button	After full packet PCAP files have been captured from a session, click this button to download PCAP files. Click the icon in the **Download** column to download the data packet files. You can download files for either: • Wireless data: 802.11 files for packets between the AP and the client. • Wired data: Ethernet files for packets between the AP and the switch or wireless controller. **Note** A Data Packet Capture file has a limit of 100 MB. The total of all Data Packet Capture files cannot exceed 3.5 GB. **Note** Only PCAP files from the past seven days can be downloaded.

Step 7 Use the **Wireless Packet Application Analysis** dashlet to view details about the data packet capture.

When a data packet capture is running, this dashlet displays details about the analyzed packets, such as the accessed applications and ports, QoS data, packet loss, wireless delay, and jitter.

Note To view data in this dashlet, you must set up the integration for NAM. See About NAM Integration, on page 263.

View Client Data Packet Capture History

Use this procedure to view the history of the client data 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.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Intelligent Capture Settings**.

The **Client Schedule Capture** window appears.

Step 2 Click the **Client Data Packet Capture** tab.

The **Client Data Packet Control** window appears.

Step 3 Use the **Intelligent Capture Settings - Client Data Packet Capture** window to view the following 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.
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**.

Intelligent Capture for Access Points

About Intelligent Capture for Access Points

The AP Intelligent Capture feature allows you to enable one or more APs to capture the following data:

- **AP Stats Capture**, which includes:

- AP radio and WLAN statistics that are displayed in the **RF Statistics** tab of the **Device 360** > **Intelligent Capture** window.
- AP Client statistics (30-second samples) that are displayed in the **RF Statistics** area of the **Client 360** > **Intelligent Capture** window for all clients associated with the selected APs.

- **Anomaly Capture** for anomaly onboarding events for all clients that are associated with one or more selected APs. Enabling Anomaly Capture ensures that all anomaly onboarding events (global or for all clients associated with the selected APs) are captured for download and display.

AP Capture Limitation

There is a 1.05-GB limit on the total size of all anomaly triggered packet files that reside on Cisco DNA Center. If the limit is exceeded, then packet files are removed, starting with the oldest, until the total size falls below the 1.05-GB limit.

Enable and Manage Intelligent Capture for an Access Point

Use this procedure to enable one or more access points (APs) to capture the following data:

- **AP Statistics**: Includes AP radio statistics, WLAN statistics, and AP Client statistics.
- **Anomaly Capture**: For anomaly onboarding events of all clients that are associated with one or more selected APs. Enabling Anomaly Capture ensures that all anomaly onboarding events (global or for all clients associated with the selected APs) are captured for download and display.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Intelligent Capture Settings**.

The **Client Schedule Capture** window appears.

Step 2 Click the **Access Point** tab.

The **Access Point** window appears.

Step 3 To enable or disable AP Stats Capture, do one of the following:

- If there are no enabled APs, the **Configure AP Enablement** area is displayed. Choose either the **Specific** or **Global** option, and then click **Get Started**.
- If there is least one AP is enabled, the **AP Stats Capture** window appears. From the **AP Stats Capture** window, choose one of the following options:

Option	Description
None - disable all APs	The **None - disable all APs** appears when at least one AP is enabled. Allows you to disable AP Stats Capture on all of the APs in which it is currently enabled.

Option	Description
Specific - select specific APs and enable	Allows you to enable AP Stats Capture for selected APs. Do the following: **a.** Click the **Specific - select specific APs and enable** radio button. **b.** In the left pane, expand **Global**, and drill down to the site > building > floor. The right pane displays the list of APs on that floor and contains three tabs: **Enabled APs**, **Disabled APs**, and **Not-Ready APs**. **c.** To enable AP Stats Capture for selected APs, do the following: • Click the **Disabled APs** tab. A list of APs that have AP Stats Capture currently disabled, is displayed. • Check the check boxes adjacent to the APs for which you want to enable AP Stats Capture, and then click **Enable**. **d.** To view incompatible APs, click the **Not-Ready APs** tab. **Note** Incompatible APs have the following conditions: • The operation mode is not set to `local` or `FlexConnect`. • The OS release that is installed on the AP is not compatible. The OS release must be MR1 or later.
Global - enable all capable APs	Allows you to enable the AP Stats Capture for all capable APs.

Step 4 To enable or disable Anomaly Capture, click the **Anomaly Capture** tab, and then do one of the following:

- If no APs are enabled, the **Configure AP Enablement** area displays, choose one of the following options, and then click **Get Started**.
- If at least one AP is enabled, the **Anomaly Capture** window appears. From the **Anomaly Capture** window, choose one of the following options:

Option	Description
None - disable all APs	The **None - disable all APs** appears when at least one AP is enabled. Allows you to disable Anomaly Capture on all of the APs in which it is currently enabled.

Option	Description
Specific - select specific APs and enable or disable	Allows you to enable or disable Anomaly Capture for selected APs. Do the following: **a.** Click the **Specific - select specific APs and enable or disable** radio button. **b.** In the left pane, expand **Global**, and drill down to the site > building > floor. The right pane displays the list of APs on that floor and contains three tabs: **Enabled APs**, **Disabled APs**, and **Not-Ready APs**. **c.** To enable Anomaly Capture for selected APs, do the following: • Click the **Disabled APs** tab. A list of APs that have Anomaly Capture currently disabled, is displayed. **Note** If a previous attempt to enable the AP failed, an error message is displayed in the **Config Status** column. • Check the check boxes adjacent to the APs for which you want to enable Anomaly Capture, and then click **Enable**. **d.** To disable Anomaly Capture for selected APs, do the following: • Click the **Enabled APs** tab. A list of APs that have Anomaly Capture currently enabled, is displayed. • Check the check boxes adjacent to the APs for which you want to disable Anomaly Capture, and then click **Disable**. **e.** To view incompatible APs, click the **Not-Ready APs** tab. **Note** Incompatible APs have the following conditions: • The operation mode is not set to `local` or `FlexConnect`. • The OS release that is installed on the AP is not compatible. The OS release must be MR1 or later. **f.** To display the list of APs that support Intelligent Capture, click the information (I) icon next to the **Not-Ready APs** tab.
Global - enable all capable APs	Allows you to enable the Anomaly Capture for all capable APs.

View RF Statistics and Manage Spectrum Analysis Data for an Access Point

Use this procedure to view RF statistics and start and manage Spectrum Analysis data for a specific access point.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and 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 the following:

- 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 Access Point Unable to Send Intelligent Capture Data to Cisco DNA Center, on page 275 for more details.

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 and Manage Intelligent Capture for an Access Point, on page 268.

Step 6 In the **RF Statistics** tab you can do the following:

a) 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**, **3 hours**, and **5 hours**. Default is **1 hour**.
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.

b) Use the radio frequency selector under the timeline to filter the data that appears in the dashlets based on the frequency bands. Click the drop-down list and select **Radio 0 (2.4 GHz or 5 GHz)** or **Radio 1 (5 GHz)**.

Note If APs have three radios, the drop-down list provides the following options: **Radio 0 (2.4 GHz)**, **Radio 1 (5 GHz)**, or **Radio 2 (5 GHz)**.

c) Use the dashlets to view the RF statistics details:

Note You can do the following in the charts that are displayed 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 is displayed 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.

Step 7 Click the **Spectrum Analysis** tab.

Step 8 Click **Start Spectrum Analysis** to start a spectrum analysis session.

Note
- The spectrum analysis duration is 10 minutes.
- The maximum number of concurrent spectrum analysis sessions is 20.

Step 9 In the **Spectrum Analysis** tab you can do the following:

a) 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**, **3 hours**, and **5 hours**. Default is **1 hour**.
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.

b) Use the radio frequency selector under the timeline to filter the data that appears in the charts based on the frequency bands. Click the drop-down list and select **Radio 0 (2.4 GHz)** or **Radio 1 (5 GHz)**.

Note If APs have three radios, the drop-down list provides the following options: **Radio 0 (2.4 GHz)**, **Radio 1 (5 GHz)**, or **Radio 2 (5 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 275.

c) Use the **Spectrum Analysis** charts for the following 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).

d) Use the **Interference and Duty Cycle** chart to view the following:

- 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.

About Cisco AP Functionality During Spectrum Analysis

The Cisco Aironet 2800 Series, 3800 Series, and 4800 Series Access Points (APs) have dual band radios with flexible radio assignment (FRA) in slot 0. 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 AP's operational mode. When you configure the AP's FRA radio to operate in 5 GHz, no client radios can operate in 2.4 GHz band.

Note Spectrum Analysis is *not supported* on the Aironet 1540 AP, Aironet 1800 Series APs, and Catalyst 9115 AP.

Note Verify that the APs have the correct software version installed. See the **Supported Cisco APs** table in the Supported Devices for Intelligent Capture, on page 253 topic.

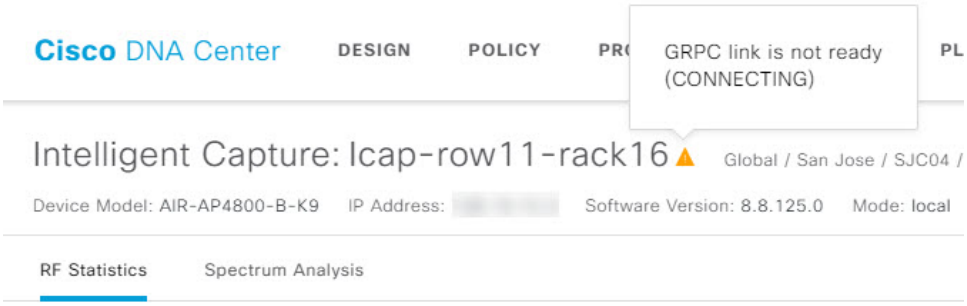
Radio slot assignments for spectrum analysis are as follows:

Device Model	Spectrum Analysis Radio Slot Assignment
Aironet 2800 Series APs Aironet 3800 Series APs Aironet 1560 APs Catalyst IW6300 Heavy Duty Series APs Catalyst IW6300 Heavy Duty Series APs	Radio slots 0 and 1 are enabled.
Aironet 4800 Series APs Catalyst 9120 AP Catalyst 9130 APs	These APs have three radio slots. 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. **Note** 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.

Troubleshoot Intelligent Capture

Client or Access Point Unable to Send Intelligent Capture Data to Cisco DNA Center

Problem: Client or access point is unable to send Intelligent Capture data to Cisco DNA Center. The warning (⚠) icon appears with the message **GRPC link is not ready (CONNECTING)**:

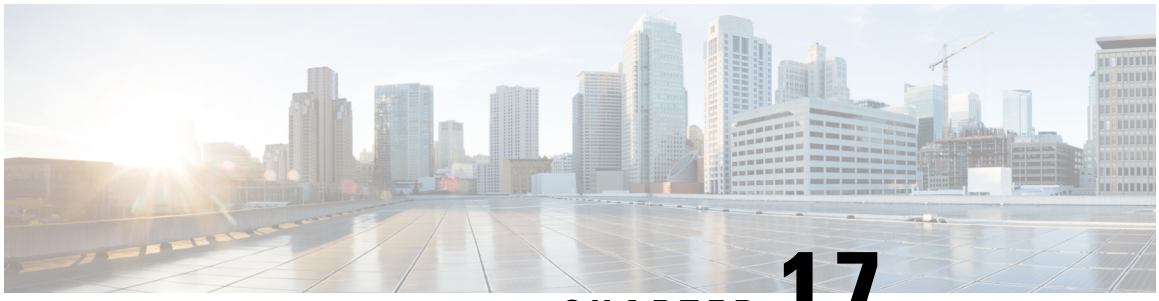


Background: In order for APs to send Intelligent Capture data to Cisco DNA Center, the Intelligent Capture port number on the eWLC or WLC must be set to 32626. Typically, when the eWLC or WLC is discovered by Cisco DNA Center, the port number is automatically set to 32626.

However, there are some upgrade paths for Cisco DNA Center that can cause the port number from being properly set.

Solution: To resolve this issue, do the following:

1. Check that the eWLC or WLC has the Intelligent Capture server port number is set to 32626.
2. If the port number is not set to 32626, manually set it.



CHAPTER 17

Trace the Path of a Device

- About Path Trace, on page 277
- Path Trace Known Limitations, on page 277
- Perform a Path Trace, on page 279

About Path Trace

You can perform 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 Cisco DNA Center controller should use to establish the path trace connection, either TCP or UDP.

When you initiate a path trace, the Cisco DNA 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 Known Limitations

Path trace has the following limitations and restrictions.

- 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 Cisco DNA 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, note the following:
    - For a path trace request, Cisco DNA 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.

Perform a Path Trace

The path trace feature works in a similar manner in all the devices. You can perform a path trace from the **Client 360** or **Device 360** window.

Before you begin

- Review the path trace known limitations. See Path Trace Known Limitations, on page 277.
- Make sure that the devices (routers, switches, wireless controllers, and access points) are discovered. See Discover Your Network Using an IP Address Range, on page 24, Discover Your Network Using CDP, on page 18, or Discover Your Network Using LLDP, on page 29.
- Make sure that CDP is enabled in the devices.

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 field	The IP address in the **Source** field is prepopulated; however, you can enter another source IP address by doing the following: • Enter the source IP address. • Click the **Source** field, and then choose an IP address from the available options.
Interface (optional) field	Choose an interface from the drop-down list. **Note** This field is displayed 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	Do one of the following: • 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 choose an IP address from the available options.
Interface (optional) field	Choose the interface from the drop-down list. **Note** This field is displayed if the IP address you choose in the Destination field is a network device.

Field	Action
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 the following as appropriate:

Field	Action
Protocol drop-down list	(Optional) Choose either **tcp** or **udp**.
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 the following 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 the following:

a) Hover your cursor over a device to display CPU and memory utilization.

If **ACL Trace** is set to **On**, the ACL name and ACL result, such as permit or deny display.

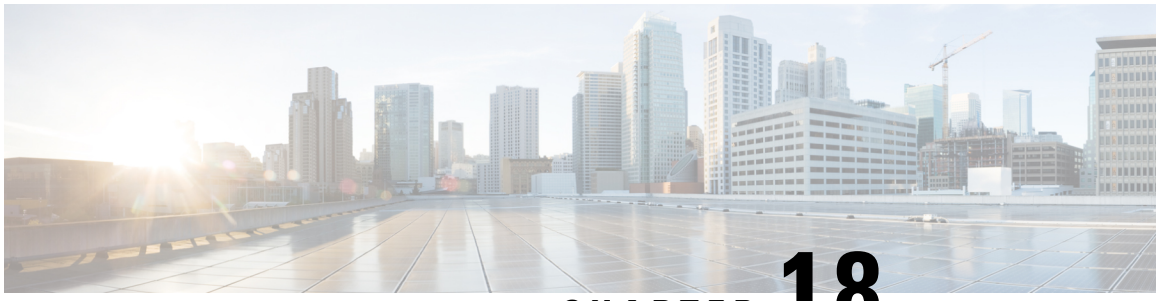
If the following 5-tuple values (source IP address and port number, destination IP address and port number, and the protocol in use) are provided, then the ACL trace that is displayed in 100% accurate. If partial information is provided, the ACL trace that is displayed is on best effort basis. In such a case, the ACL results might display both Permit and Deny.

Matched ACLs in a specific traffic flow are displayed with a colored icon. Green indicates **Permit**. Red indicates **Deny**. For Ingress ACLs, the icon appears on the left side of the device. For Engress 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 18

Integrate Cisco CMX for Wireless Maps

- About Cisco Connected Mobile Experiences Integration, on page 281
- Add a User for the Cisco CMX API Server, on page 281
- Create Cisco CMX Settings, on page 282
- Troubleshoot Cisco CMX, on page 283

About Cisco Connected Mobile Experiences Integration

Cisco DNA Center supports the integration of on-premises 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 Cisco DNA 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 Cisco DNA Center Network Settings, you must add a user for the Cisco CMX API server.

Step 1 SSH to Cisco CMX using a cmxadmin account. Enter the following command:

```
ssh -l cmxadmin (cmx-ip-address)
```

Step 2 Start the Cisco CMX API server. Enter the following command:

```
# cmxos apiserver start
```

Example

The following example shows how to start the Cisco CMX API server:

```
[root@server]# cmxos apiserver start
Starting CMX API Server...
```

Step 3 Add a user for the Cisco CMX API server. Enter the following command:

```
cmxos apiserver user add
```

At the password prompt, use the same password as the Cisco CMX web admin user password.

Example

```
The following example shows how to add a user for the Cisco CMX API server:
[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: password
Please re-enter the password for the CMX API Server: password
Restarting CMX API Server...
Stopping CMX API Server...
Starting CMX API Server...
Successfully updated userid/password and restarted the CMX API Server
```

What to do next

Create Cisco CMX settings in Cisco DNA Center. See Create Cisco CMX Settings, on page 282.

Create Cisco CMX Settings

Before you begin

Add a Cisco CMX API user. See Add a User for the Cisco CMX API Server, on page 281.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Settings** > **External Services** > **CMX Servers**.

The **CMX Servers** window appears.

Step 2 Click **Add**.

The **Add CMX Server** window appears.

Step 3 In the **IP Address** field, enter the valid IP address of the CMX web GUI.

Step 4 In the **User Name** and **Password** fields, enter the CMX web GUI username and password credentials.

Step 5 In the **SSH User Name** and **SSH Password** fields, enter the CMX admin username and password credentials.

Note Make sure that CMX is reachable.

Step 6 Click **Add**.

The CMX server is added successfully.

Step 7 To assign a CMX server to a site, building, or a floor, click the **Menu** icon and choose **Design** > **Network Settings** > **Wireless**.

Step 8 In the left tree view menu, select either Global or the area, building, or floor that you are interested in.

Step 9 Under **CMX Servers**, from the **CMX Servers** drop-down list, select the CMX server.

Step 10 Click **Save**.

The **Create CMX Settings** page appears.

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, Cisco DNA Center starts querying the CMX for the client location and displays the location on the floor map.

From the floor map, you can do the following:

- View the location of the client, which is shown as a blue dot.
- Hover your cursor over an AP. A dialog box is displayed 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.
- Perform real-time client tracking when Intelligent Capture and CMX are integrated.

Step 11 If the CMX was down when you made changes, you must synchronize manually. To do so, on the **Network Hierarchy** page, click the gear icon next to the building or floor on which you made the changes in the left tree pane, and then choose **Sync with CMX** to push the changes manually.

Step 12 To edit the CMX server details or delete a CMX server, do the following:

a) In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Settings** > **External Services** > **CMX Servers**.
b) Select the CMX server that you want to edit, make any changes, and click **Update**.
c) Select the CMX server that you want to delete and click **Delete**.
d) Click **OK** to confirm the deletion.

Troubleshoot Cisco CMX

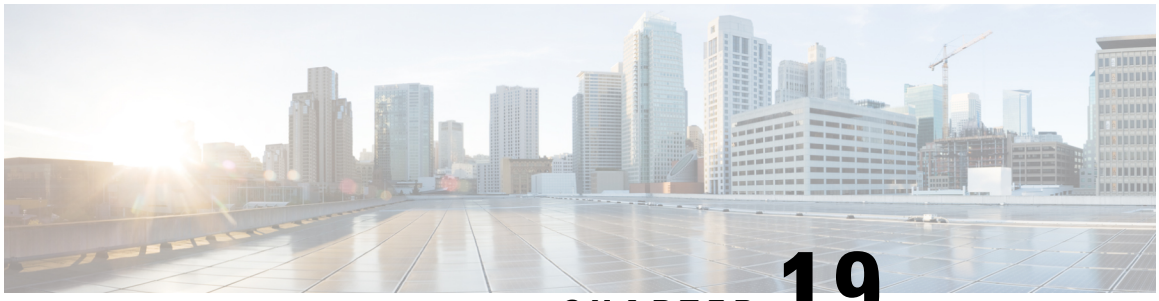
CMX Authentication Failure

- 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 Cisco DNA 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 Cisco DNA 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 19

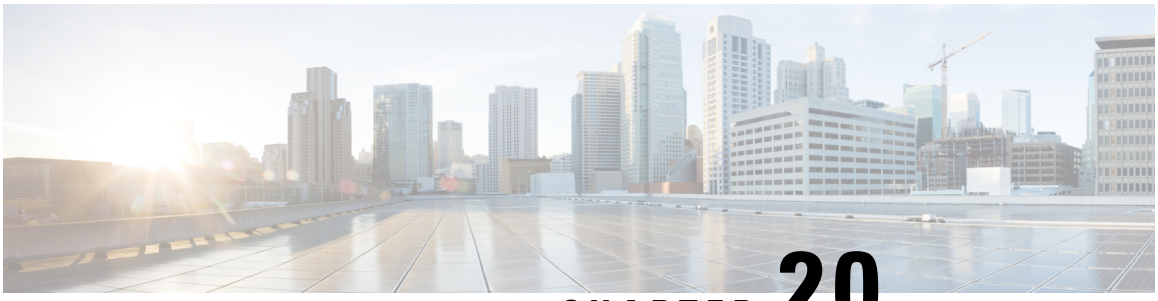
Reports

- About Reports, on page 285

About Reports

You can utilize data from the Reports feature to derive insights into your network and its operation. By reporting this data in several formats and providing flexible scheduling and configuration options, both data and reports are easily customized to meet your operational needs.

For details about the Cisco DNA Center Reports, see the Cisco DNA Center Platform User Guide.



CHAPTER 20

View Assurance Audit Logs

- View Audit Logs for Assurance, on page 287

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 there were errors that 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 using the Cisco DNA Center GUI, click the Menu icon (☰) and choose **Activity** > **Audit Logs**. For detailed procedure, see the "View Audit Logs" topic in the *Cisco DNA Center Administrator Guide*.

For Assurance, the following data is captured in the audit logs:

Table 18: 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 the following 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.

In addition, if there are 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 the following updates:

- Updates on site health.
- Updates on the health score.
- Updates on the issue settings.

Sensor Audit Logs

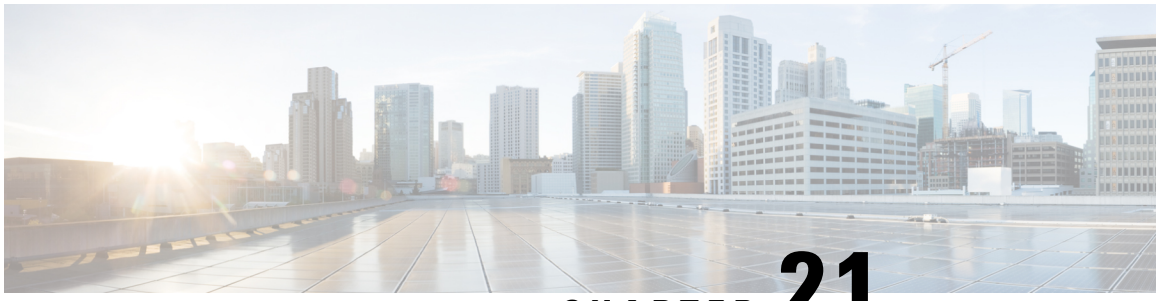
For sensors, audit logs are provided to capture the following configuration requests:

- 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 the following AI agent configuration changes:

- Agent onboarded.
- Agent restored.
- Agent reconfigured.



CHAPTER 21

Troubleshoot Cisco DNA Center Using Data Platform

- About Data Platform, on page 289
- Troubleshoot Using the Analytics Ops Center, on page 290
- View or Update Collector Configuration Information, on page 291
- View Data Retention Settings, on page 292
- View Pipeline Status, on page 293

About Data Platform

Data Platform provides tools that can help you monitor and troubleshoot Cisco DNA Center applications. **Data Platform** displays synthesized data from various inputs to help you identify patterns, trends, and problem areas in your network. For example, if something goes wrong in your network, you can quickly get answers to questions such as whether a pipeline is in an error state and what is the real-time traffic flow in a particular area. The main areas of Data Platform are:

- **Analytics Ops Center**: Provides a graphical representation of how data is streamed through collectors and pipelines and provides Grafana dashboards, which can help you identify patterns, trends, and problem areas in your network. See Troubleshoot Using the Analytics Ops Center, on page 290.
- **Collectors**: Collects a variety of network telemetry and contextual data in real time. As data is ingested, Cisco DNA Center correlates and analysis the data. You can view the status of collectors and quickly identify any problem areas. See View or Update Collector Configuration Information, on page 291.
- **Store Settings**: Allows you to specify how long data is stored for an application. See View Data Retention Settings, on page 292.
- **Pipelines**: Allows Cisco DNA Center applications to process streaming data. A data pipeline encapsulates an entire series of computations that accepts input data from external sources, transforms that data to provide useful intelligence, and produces output data. You can view the status of pipelines and quickly identify any problem areas. See View Pipeline Status, on page 293.

Troubleshoot Using the Analytics Ops Center

The Analytics Ops Center provides a graphical representation of how data is streamed through collectors and pipelines, and provides Grafana dashboards, which can help you identify patterns, trends, and problem areas in your network, such as:

- Missing data in Assurance.
- An inaccurate health score.
- Devices that appear as monitored under Inventory but unmonitored under Assurance.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Data Platform**.

Step 2 Click **Analytics Ops Center**.
A list of applications is displayed.

Step 3 Click the application name for which you want to view metrics; for example, **Assurance**.

A graphical representation of all existing collectors and pipelines in the application appears. CPU or throughput values corresponding to each pipeline are also provided.

The current health status of each component is indicated by its color:

- Red: error
- Yellow: warning
- Gray: normal operation

Step 4 To view historical data of pipelines, click **Timeline & Events**.

A timeline bar providing data for the time interval appears. You can also:

- Move the timeline slider to view data for a specific time.
- Hover your cursor over an event in the timeline bar to display additional details or a group of events that occurred at the same time.
- Click an event to display the Analytics Ops Center visualization at that particular time.

Step 5 To view additional details to help you troubleshoot an issue and determine the cause of an error or warning, click a collector name.

A slide-in pane appears with the following tabs:

- **Metrics**: Provides a selection of available metrics gathered during the last 30 minutes. It displays summary information indicating the component status, start and stop time, and error exceptions. You can also choose a different time interval.
- **Grafana**: Displays a dashboard associated with the respective component for deeper debugging.

Step 6 To view whether data is flowing through a specific pipeline, click a pipeline stream.

A slide-in pane appears with graphs. The graphs display whether the application is receiving data from the underlying pipelines. The graph information is based on the time interval you select from the drop-down list in the slide-in pane. Options are **Last 30 Min**, **Last Hour**, **Last 2 Hours**, and **Last 6 Hours**. The default is **Last 30 Min**.

Step 7 If a pipeline is not flowing at normal levels, hover your cursor over the stream to display the lag metrics.

Step 8 To view detailed information for a specific pipeline, click a pipeline name.

The appropriate *Pipeline* page displays with the following tabs:

Note Make sure to click the **Exceptions** tab to determine if any exceptions occurred in the pipeline. Under normal working conditions, this tab displays **null**.

- **Metrics**: Displays metrics, updated every 30 minutes in a graph.
- **Summary**: Displays summary information such as stats, run-time, and manifest.
- **Exceptions**: Displays any exceptions that occurred on the pipeline.
- **Stages**: Displays the pipeline stages.

Step 9 To change the metrics displayed on the Analytics Ops Center page, click **Key Metrics**, select up to two metrics, and then click **Apply**.

By default, Cisco DNA Center displays CPU and Throughput metrics.

Step 10 To view metrics for a particular flow, do the following:

a) Click **View Flow Details**.
b) Select three connected components (collector, pipeline, and store) by clicking the tilde (~) on the component's top-left corner.
c) Click **View Flow**.
Cisco DNA Center displays the metrics associated with that specific flow.

View or Update Collector Configuration Information

Collectors collect a variety of network telemetry and contextual data in real time. As data is ingested, Cisco DNA Center correlates and analyzes the data. You can view the status of collectors and quickly identify any problem areas.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Data Platform**.

Step 2 Click **Collectors**. The colored dot next to each collector indicates its overall status.

Step 3 To view additional details, click a collector name.

The appropriate *Collector* page appears. By default, Cisco DNA Center displays the **Configurations** tab which displays the list of current configurations.

Step 4 To view, update, or delete a configuration, click a specific configuration name.

Step 5 To add a new configuration, click **+ Add** in the **Configurations** tab.

A slide-in pane appears.

Step 6 In the slide-in pane, enter the required information for the configuration.

Step 7 (Optional) You can anonymize its data for some collectors such as **WIRELESSCOLLECTOR**, by checking the **Anonymize** check box.

Note When you check the **Anonymize** check box, the host name and user ID in the **Client Health** window is scrambled with one-way hash that cannot be decrypted.

Important If you want to anonymize your data, make sure that you check the **Anonymize** check box before you discover devices with the **Discovery** tool. If you anonymize the data after you discovered devices, the new data coming into the system is anonymized but the existing data will not be anonymized.

Step 8 Click **Save Configuration**.

Step 9 To view configured instances, click the **Instances** tab.

Step 10 To view summary information and metrics, choose an instance from the list.

Step 11 (Optional) If Cisco DNA Center integrates with Cisco Connected Mobile Experience (CMX), you have the option of anonymizing data on the CMX side. Do the following:

a) Using an SSH client, log in to Cisco CMX as the cmxadmin CLI user.

b) Change to the root user.

c) Go to `/opt/cmx/etc/node.conf` and under `[location]`, add **`user_options`**. For example:

```
[location]
…
user_options=-Dhideusername=true
```

d) On the Cisco CMX CLI, enter the following commands:

```
cmxctl agent restart
cmxctl location restart
```

View Data Retention Settings

You can view how long data is stored for an application.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Data Platform**.

Step 2 Click **Store Settings**.

Step 3 To view a list of historical purge jobs that have completed, click **Data Purge Schedule**.

The **HISTORY** table lists the name of the purge job, the result, time, and other data. You can sort, filter, and export data in the table.

Step 4 To view the current data retention and purge settings, click **Data Retention & Purge Configuration**. The following is displayed:

- **Document Store**: Settings for all time-based data, such as the maximum size and the low and high watermark threshold.

- **Metric Graph Store**: Settings for all time-based graphical data, such as the maximum size and the low and high watermark threshold.

View Pipeline Status

Data pipelines allow Cisco DNA Center applications to process streaming data. A data pipeline encapsulates an entire series of computations that accepts input data from external sources, transforms that data to provide useful intelligence, and produces output data. You can view the status of pipelines and quickly identify any problem areas.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Data Platform**.

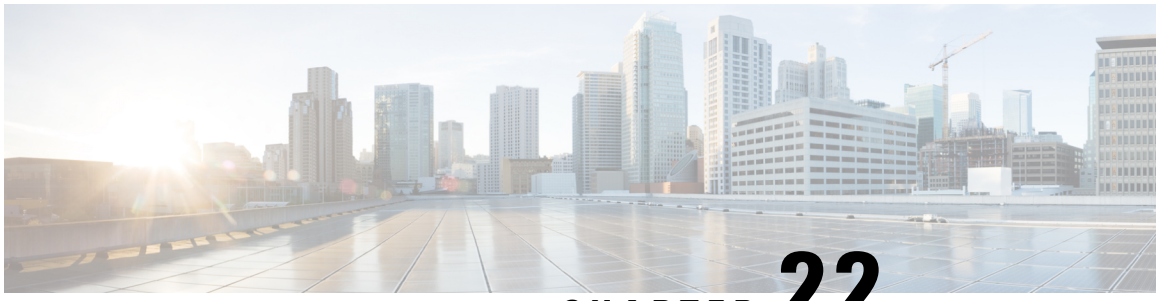
Step 2 Click **Pipelines**.

Step 3 To view whether the application is receiving data from the underlying pipelines, click a pipeline name.

The appropriate *Pipeline* page displays with the following tabs:

Note Make sure to click the **Exceptions** tab to determine if any exceptions have occurred in the pipeline. Under normal working conditions, this tab displays **null**.

- **Metrics**: Displays metrics, updated every 30 minutes in a graph.
- **Summary**: Displays summary information such as stats, run-time, and manifest.
- **Exceptions**: Displays any exceptions that have occurred on the pipeline.
- **Stages**: Displays the pipeline stages.



CHAPTER 22

Related Documentation

- Related Documentation, on page 295

Related Documentation

We recommend that you read the following documents relating to Cisco DNA Center.

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

For This Type of Information...	See This Document...
Release information, including new features, limitations, and open and resolved bugs.	Cisco DNA Center Release Notes
Installation and configuration of Cisco DNA Center, including postinstallation tasks.	Cisco DNA Center Installation Guide
Upgrade information for your current release of Cisco DNA Center.	Cisco DNA Center Upgrade Guide
Use of the Cisco DNA Center GUI and its applications.	Cisco DNA Center User Guide
Configuration of user accounts, security certificates, authentication and password policies, and backup and restore.	Cisco DNA Center Administrator Guide
Security features, hardening, and best practices to ensure a secure deployment.	Cisco DNA Center Security Best Practices Guide
Supported devices, such as routers, switches, wireless access points, and software releases.	Supported Devices
Hardware and software support for Cisco SD-Access.	Cisco SD-Access Hardware and Software Compatibility Matrix

For This Type of Information...	See This Document...
Use of the Cisco DNA Assurance GUI.	Cisco DNA Assurance User Guide
Use of the Cisco DNA Center platform GUI and its applications.	Cisco DNA Center Platform User Guide
Cisco DNA Center platform release information, including new features, deployment, and bugs.	Cisco DNA Center Platform Release Notes
Use of the Cisco Wide Area Bonjour Application GUI.	Cisco Wide Area Bonjour Application User Guide
Use of the Stealthwatch Security Analytics Service on Cisco DNA Center.	Cisco Stealthwatch Analytics Service User Guide
Use of Rogue Management functionality as a dashboard within Cisco DNA Assurance in the Cisco DNA Center GUI.	Cisco DNA Center Rogue Management Application Quick Start Guide