## CONTENTS

### CHAPTER 1
**New and Changed Information**  
What's New in Cisco DNA Assurance, Release 1.3.1.0 1

### CHAPTER 2
**Cisco DNA Assurance Overview** 5  
About Cisco DNA Assurance 5  
Assurance Architecture 5  
Log In 6  
Log In for the First Time as a Network Administrator 7  
Default Home Page 8  
Start with Assurance 12

### CHAPTER 3
**Cisco AI Network Analytics Overview** 13  
About Cisco AI Network Analytics 13  
Cisco AI Network Analytics Benefits 15  
Cisco AI Network Analytics Licensing and Deployment 16

### CHAPTER 4
**Set Up Cisco DNA Center to Use Assurance** 17  
Basic Setup Workflow 17  
Discover Devices 20  
About Discovery 20  
Discovery Prerequisites 21  
Preferred Management IP Address 21  
Discovery Configuration Guidelines and Limitations 22  
Discover Your Network Using CDP 22  
Discover Your Network Using an IP Address Range 27  
Discover Your Network Using LLDP 31
Contents

Manage Discovery Jobs 36
  Stop and Start a Discovery Job 36
  Clone a Discovery Job 37
  Delete a Discovery Job 37
  View Discovery Job Information 37
Design Network Hierarchy 38
  Design a New Network Infrastructure 38
  About Network Hierarchy 38
Guidelines for Image Files to Use in Maps 39
Create a Site in a Network Hierarchy 39
  Add Buildings 40
  Add a Floor to a Building 40
Add, Position, and Delete APs 41
Manage Network Hierarchy 43
  Upload an Existing Site Hierarchy 43
  Search the Network Hierarchy 44
Edit Sites 44
  Delete Sites 45
  Edit a Building 45
  Delete Buildings 45
  Edit a Floor 45
  Monitor a Floor Map 46
  Edit Floor Elements and Overlays 46
  Floor View Options 55
  Data Filtering 57
Manage Inventory 58
  About Inventory 58
  Update Device Resync Interval 59
  Display Information About Your Inventory 59
Add a Device to a Site 62
About Cisco ISE Configuration for Cisco DNA Center 63
  Configure Cisco DNA Center for Cisco ISE Integration 63
  Configure Authentication and Policy Servers 64
  Configure Syslog, SNMP Traps, and Netflow Collector Servers Using Telemetry 67
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Monitor and Troubleshoot Overall Enterprise Health</td>
<td>81</td>
</tr>
<tr>
<td></td>
<td>About Enterprise</td>
<td>81</td>
</tr>
<tr>
<td></td>
<td>Monitor and Troubleshoot the Overall Health of Your Enterprise</td>
<td>81</td>
</tr>
<tr>
<td>6</td>
<td>Monitor and Troubleshoot Network Health</td>
<td>85</td>
</tr>
<tr>
<td></td>
<td>About Network</td>
<td>85</td>
</tr>
<tr>
<td></td>
<td>Monitor and Troubleshoot the Health of Your Network</td>
<td>85</td>
</tr>
<tr>
<td></td>
<td>Monitor and Troubleshoot the Health of a Device</td>
<td>90</td>
</tr>
<tr>
<td></td>
<td>Selected Syslogs Below Error Level</td>
<td>96</td>
</tr>
<tr>
<td></td>
<td>Fabric Domains</td>
<td>97</td>
</tr>
<tr>
<td></td>
<td>Fabric Overview</td>
<td>97</td>
</tr>
<tr>
<td></td>
<td>Create a Fabric Domain</td>
<td>98</td>
</tr>
<tr>
<td></td>
<td>Add a Device to a Fabric</td>
<td>98</td>
</tr>
<tr>
<td></td>
<td>Enable SNMP Collector Metrics for Fabric Devices</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Understand Network Health Score and KPI Metrics</td>
<td>101</td>
</tr>
<tr>
<td></td>
<td>Network Health Score</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>Device Category Health Score</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>Individual Device Health Score</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>Switch Health Score</td>
<td>103</td>
</tr>
<tr>
<td></td>
<td>Router Health Score</td>
<td>104</td>
</tr>
<tr>
<td></td>
<td>AP Health Score</td>
<td>104</td>
</tr>
<tr>
<td></td>
<td>Wireless Controller Health Score</td>
<td>105</td>
</tr>
<tr>
<td>7</td>
<td>Monitor and Troubleshoot Client Health</td>
<td>107</td>
</tr>
<tr>
<td></td>
<td>About Clients</td>
<td>107</td>
</tr>
<tr>
<td></td>
<td>Monitor and Troubleshoot the Health of All Client Devices</td>
<td>107</td>
</tr>
<tr>
<td></td>
<td>Monitor and Troubleshoot the Health of a Client Device</td>
<td>117</td>
</tr>
<tr>
<td></td>
<td>Understand Client Health Score and KPI Metrics</td>
<td>121</td>
</tr>
<tr>
<td></td>
<td>Client Health Score</td>
<td>122</td>
</tr>
<tr>
<td></td>
<td>Client Onboarding Score</td>
<td>122</td>
</tr>
</tbody>
</table>
Contents

Client Connectivity Score 122
Individual Client Health Score 123

CHAPTER 8
Trace the Path of a Device 125
About Path Trace 125
Path Trace Known Limitations 125
Perform a Path Trace 127

CHAPTER 9
Monitor Application Health 129
About Cisco Application Experience 129
Enable Application Visibility 129
Configure Telemetry 130
About Telemetry 130
Apply a Telemetry Profile to the Devices 130
View Application Experience of a Host 131
View Application Experience of a Network Device 132
Monitor the Health of All Applications 133
Monitor the Health of an Application 137
Understand Application Health Score and KPI Metrics 139
Overall Application Health Score 140
Individual Application Health Score 140

CHAPTER 10
Manage Sensors and Sensor-Driven Tests 141
About Sensors and Sensor-Driven Tests 141
View and Manage Sensors in Your Network 142
Manage Backhaul Settings 143
View Sensor-Driven Tests 144
Add a Sensor-Driven Test 146
Monitor and Troubleshoot the Health of Wireless Sensors 150
Provision the Wireless Cisco Aironet 1800s Active Sensor 154
Enable Provisioning SSID on the Wireless Controller 155
Enable Cisco Provisioning SSID on the Cisco Catalyst Wireless Controller 155
Provision a Wireless or Sensor Device 156
Error Messages for Sensor-Driven Test Failures 159
### CHAPTER 11

**Integrate Cisco CMX for Wireless Maps** 171
- About Cisco Connected Mobile Experiences Integration 171
- Add a User for the Cisco CMX API Server 171
- Create Cisco CMX Settings 172
- Troubleshoot Cisco CMX 173

### CHAPTER 12

**Manage Intelligent Capture** 175
- About Intelligent Capture 175
- Supported Devices for Intelligent Capture 175
- Intelligent Capture Best Practices 176
- Manage Intelligent Capture Settings for a Client 177
- About Capture Sessions 178
- Manage Intelligent Capture Settings for an Access Point 178
- Monitor Intelligent Capture Details for a Client 180
- About NAM Integration 184
  - Configure an IP Address on the NAM Data Port 185
  - Configure the gRPC Collector 186
- Monitor Intelligent Capture Details for an AP 186
- About Cisco Aironet AP Functionality During Spectrum Analysis 190
- Troubleshoot Intelligent Capture Issues 191

### CHAPTER 13

**Manage Dashboards** 193
- About Dashboards 193
- Create a Custom Dashboard 193
- Create a Dashboard From a Template 195
- View a Dashboard 196
- Edit or Delete a Dashboard 196
- Duplicate a Dashboard 197
- Mark a Dashboard as a Favorite 197
- Change the Position of a Dashlet 197

### CHAPTER 14

**View and Manage Issues** 199
- About Issues 199
New and Changed Information

- What's New in Cisco DNA Assurance, Release 1.3.1.0, on page 1

What's New in Cisco DNA Assurance, Release 1.3.1.0

The following table summarizes the new and changed features in the *Cisco DNA Assurance User Guide, Release 1.3.1.0*.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco AI Network Analytics</td>
<td>Cisco DNA Center, Release 1.3.1.0 introduces 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. See Cisco AI Network Analytics Overview, on page 13.</td>
</tr>
<tr>
<td>Trends and Insights</td>
<td>Cisco AI Network Analytics allows you to determine global patterns (trends) and deviations in your network and provides system-generated insights. See View Network Trends and Obtain Insights, on page 229.</td>
</tr>
<tr>
<td>Comparative Analytics</td>
<td>With Cisco AI Network Analytics you can compare a site with another site, compare KPI values with peers in your network, and compare the APs in network heatmaps to spot trends and gain insights. See Compare a Site with Another Site in Your Network, on page 235, Compare KPI Values with Peers in Your Network, on page 234, Compare Access Points in Network Heatmaps, on page 232.</td>
</tr>
</tbody>
</table>
### What’s New in Cisco DNA Assurance, Release 1.3.1.0

#### Feature

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Issue enhancements | A new updated and more intuitive **Open Issues** dashboard enables you to easily understand the status of the network. This new dashboard allows you to understand the most impacted sites, the recent trends, and quickly access the AI-driven issues when the Cisco AI Network Analytics application is enabled.  

The issue windows are enhanced and simplified:  

- The **Global Issues** and **All Issues** windows are replaced by **Open Issues**, **Resolved Issues**, and **Ignored Issues**.  


- The AI-driven issue category is added to the **Issue Settings** window.  

  See AI-Driven Issues, on page 226.  

- Machine Reasoning is supported for the Layer 2 Loop issue.  

  See Issue Instance Details for Layer 2 Loop Issue, on page 207.  

- You can configure Cisco DNA Center to send a REST or email notification when supported issues are triggered.  

  See Enable Issue Notifications, on page 213. |
| Data rate KPI for wireless clients | Added a data rate KPI for wireless clients.  

The following GUI enhancements were made for this feature:  

- Enhanced the **Client Health** dashboard by adding the **Client Data Rate** dashlet, which displays the distribution of data rates for wireless clients.  

- Enhanced the **Client 360** window:  

  - Added details about data rate and client protocol under the timeline pane.  

  - Added the **Data Rate** chart to the **Detail Information** category under the **Connectivity** tab. |
| Application Experience support for more network devices | You can view the quantitative metrics of the applications running on the following network devices:  

- Cisco Catalyst 9000 Series Switches  

- Cisco AireOS WLCs |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Sensor enhancements                               | • Added a new GUI window **Assurance > Manage > Sensors > Sensor List.** Use this window to view the onboarded sensors in your network. You can enable SSH, enable the status LED, and change the name for these sensors. See **View and Manage Sensors in Your Network, on page 142**  
• Added a new GUI window **Assurance > Manage > Sensors > Backhaul Settings.** Use this window to view, create, and manage backhaul configurations for sensors. See **Manage Backhaul Settings, on page 143**  
• You can select target APs to test against when creating sensor-driven tests.                                                                 |
| Intelligent Capture support for more network devices | Intelligent Capture support is now available for the following access point models:  
• Cisco Aironet 1815 Series APs  
• Cisco Aironet 1830 Series APs  
• Cisco Aironet 1840 Series APs  
• Cisco Aironet 1850 Series APs  
• Cisco Aironet 1540 Series APs  
• Cisco Aironet 1560 Series APs  
• Cisco Catalyst 9115 APs  
• Cisco Catalyst 9120 APs  
See **Supported Devices for Intelligent Capture, on page 175.** |
Cisco DNA Assurance Overview

- About Cisco DNA Assurance, on page 5
- Assurance Architecture, on page 5
- Log In, on page 6
- Log In for the First Time as a Network Administrator, on page 7
- Default Home Page, on page 8
- Start with Assurance, on page 12

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

Access Cisco DNA Center by entering its network IP address in your browser. For compatible browsers, see the Cisco DNA Center Release Notes. This IP address connects to the external network and is configured during the Cisco DNA Center installation. For more information about installing and configuring Cisco DNA Center, see the Cisco Digital Network Architecture Center Installation Guide.
You should continuously use Cisco DNA Center to remain logged in. If you are inactive for too long, Cisco DNA Center logs you out of your session automatically.

---

**Step 1**
Enter an address in your web browser's address bar in the following format. Here, server-ip is the IP address (or the hostname) of the server on which you have installed Cisco DNA Center:

https://server-ip

Example: https://192.0.2.1

Depending on your network configuration, you might have to update your browser to trust the Cisco DNA Center server security certificate. Doing so will help ensure the security of the connection between your client and Cisco DNA Center.

**Step 2**
Enter the Cisco DNA Center username and password assigned to you by the system administrator. Cisco DNA Center displays its home page.

If your user ID has the NETWORK-ADMIN-ROLE and no other user with the same role has logged in before, you will see a first-time setup wizard instead of the home page. For details, see Log In for the First Time as a Network Administrator, on page 7.

**Step 3**
To log out, click the Gear icon (⚙️) at the top-right corner and click Sign Out.

---

**Log In for the First Time as a Network Administrator**

If your user ID has the NETWORK-ADMIN-ROLE assigned, and no other user with the same role has logged in before, you will be redirected to the Get Started wizard.

The wizard is a quick way to get immediate value from Cisco DNA Center. It consists of a few screens that collect information needed to discover and monitor the condition of your network devices, and then help you visualize your network's overall health using the Cisco DNA Center home page dashboard.

You can perform all of the same tasks the wizard does using other Cisco DNA Center features. Using the wizard does not prevent you from using those features. You can choose to skip the wizard entirely at any point and it will not be shown again for you. However, Cisco DNA Center will continue to display the wizard at login to any user with the same role until one such user completes the wizard steps. After that, Cisco DNA Center never displays the wizard again.

If you skipped the Get Started wizard, you can always revisit it from the Get Started link at the top right of the home page.

**Before you begin**

You need to have the following information to complete the wizard:

- The IP addresses of your SYSLOG and SNMP servers
- The IP address and port of your Netflow server
- For discovery: The IP address to start from (if choosing CDP discovery) or the starting and ending IP addresses (if choosing Range discovery)
- Optional: Your preferred management IP address
- Device CLI credentials, including the Enable password
• SNMP v2c credentials, including the read community string

Step 1
If you have not already done so, log in to Cisco DNA Center normally, as explained in Log In, on page 6. You will be redirected to Get Started wizard if this is your first time login.

Step 2
Click Get Started in the Getting Started wizard to continue device discovery or Exit to return to the Home page.

Step 3
Enter the network properties for device discovery and click Save & Next. Click Back to return to the previous screen.

Step 4
Specify the Discovery Type, Starting IP Address, and CLI Credentials. By default Device Controllability is enabled. You can click Disable to disable device controllability.

Step 5
When you are finished, click Begin Discovery. Cisco DNA Center displays the home page, which slowly fills with network health information as discovery completes.

Default Home Page

After you log in, Cisco DNA Center displays its home page. The home page has the following main areas: Assurance Summary, Network Snapshot, Network Configuration, and Tools.

The Assurance Summary area includes:

• Health: Provides the health score of your overall enterprise, which includes: Network Devices, Wired Clients, and Wireless Clients. Clicking View Details takes you to the Overall Health window.

• Critical Issues: Provides the count of P1 and P2 issues. Clicking View Details takes you to the Open Issues window.
  • P1: Critical issues that need immediate attention which can result in wider impact on network operations.
  • P2: Major issues that can potentially impact multiple devices or clients.

• Trends and Insights: Provides insights about the performance of your network. Clicking View Details takes you to the Network Insights window.

The Network Snapshot area includes:

• Sites: Provides the number of sites discovered on your network along with the number of DNS and NTP servers. Clicking Add Sites takes you to the Add Site window.

• Network Devices: Provides the number of network devices discovered on your network along with the number of unclaimed, unprovisioned, and unreachable devices. Clicking Find New Devices takes you to the New Discovery window.

• Application Policies: Provides the number of application policies discovered on your network along with the number of successful and errored deployments. Clicking Add New Policy takes you to the Application Policies window.
• **Network Profiles**: Provides the number of profiles discovered on your network. Clicking **Manage Profiles** takes you to the **Network Profiles** window.

• **Images**: Provides the number of images discovered on your network along with the number of untagged and unverified images. Clicking **Import Images/SMUs** takes you to the **Image Repository** window.

• **Licensed Devices**: Provides the number of devices that have a Cisco DNA Center license along with the number of switches, routers, and access points. Clicking **Manage Licenses** takes you to the **License Management** window.

The **Network Configuration** area includes:

• **Design**: 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.

• **Policy**: Create policies that reflect your organization's business intent for a particular aspect of the network, such as network access. Cisco DNA Center takes the information collected in a policy and translates it into network-specific and device-specific configurations required by the different types, makes, models, operating systems, roles, and resource constraints of your network devices.

• **Provision**: Prepare and configure devices, including adding devices to sites, assigning devices to the inventory, deploying the required settings and policies, creating fabric domains, and adding devices to the fabric.

• **Assurance**: Provide proactive and predictive actionable insights about the performance and health of the network infrastructure, applications, and end-user clients.

• **Platform**: Allows you to programmatically access your network through Intent APIs, integrate with your preferred IT systems to create end-to-end solutions, and add support for multivendor devices.

**Tools**: Use the **Tools** area to configure and manage your network.
Figure 1: Cisco DNA Center Home Page

![Cisco DNA Center Home Page](image)

**Getting Started**

When you log in to Cisco DNA Center for the first time as a Network Administrator or System Administrator, or when there are no devices in the system, you see the following dashlet. Click **Get Started** and complete the getting started workflow to discover new devices in your network.

In a few simple steps, discover your devices to begin your Cisco DNA Center journey!

[Get Started]

When you log in to Cisco DNA Center for the first time as an Observer, you see the following message:

Ask your Network Administrator to add Network Devices to gather Assurance data.

**Day 0 Home Page**

If you skipped getting started, or when there are no devices in the system, you see the following home page.
When discovery is in progress, you see a progress message with a link to the **Discovery** window.

When there are devices in the system, you see a network snapshot of discovered devices.

Click the icons at the top-right corner of the home page to perform important common tasks:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Cloud Icon" /></td>
<td><strong>Software Updates:</strong> See a list of available software updates. Click the <strong>Go to Software Updates</strong> link to view system and application updates.</td>
</tr>
<tr>
<td><img src="image" alt="Search Icon" /></td>
<td><strong>Search:</strong> Search for devices, users, hosts, and other items, anywhere they are stored in the Cisco DNA Center database.</td>
</tr>
<tr>
<td><img src="image" alt="Tools Icon" /></td>
<td><strong>Tools:</strong> Access the available tools.</td>
</tr>
<tr>
<td><img src="image" alt="Setting Icon" /></td>
<td><strong>Settings:</strong> Configure system settings, view audit logs, see the logged in username, and log out.</td>
</tr>
<tr>
<td>Icon</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>![DescriptionIcon]</td>
<td>Help:</td>
</tr>
</tbody>
</table>
| ![DescriptionIcon] |  • About: Display the current Cisco DNA Center software version. Click **Release Notes** to launch the release notes in a separate browser tab. Click **Packages** to view the system and application package versions. Click **Serial number** to view the serial number of the Cisco DNA Center appliance.  
  • API Reference: Open the Cisco DNA Center platform API documentation in Cisco DevNet.  
  • Developer Resources: Open Cisco DevNet, where you can access developer tools.  
  • Help: Launch context-sensitive online help in a separate browser tab.  
  • Contact Support: Open a support case with the Cisco Technical Assistance Center (TAC).  
  • Make a Wish: Submit your comments and suggestions to the Cisco DNA Center product team. |
| ![DescriptionIcon] | Notifications: See recently scheduled tasks and other notifications.  
  Note: The notification icon may show a color badge next to it. The badge indicates a change in tasks or notifications. A blue badge indicates new notifications, new tasks, or successful tasks. A red badge indicates failed tasks. |

If you are new to Cisco DNA Center, see Start with Assurance, on page 12 for tips and suggestions on how to begin.

**Note**

By default, the login name you provided is displayed in the Welcome text. To change the name, click the name link; for example, **admin**. You are taken to **Users > User Management**, where you can edit the display name.

## 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 17.

- **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 Digital Network Architecture Center User Guide.
### 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 2: 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-identified 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.

Cisco DNA Center, Release 1.3.0 introduced limited on-appliance Cisco AI Network Analytics capabilities for excessive onboarding time.

Cisco DNA Center, Release 1.3.1.0 provides the complete set of feature-rich Cisco AI Network Analytics capabilities.

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

*Figure 3: 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:


- **Application Experience Issues**: Total Radio Throughput, Media Application Throughput, Cloud 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-identified data set, and then leverages sophisticated machine learning models to create baselines that are relevant to specific networks and sites. These baselines learn and adapt as the network environments change and as the 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](https://www.cisco.com/c/en/us/about/trust-center/data-privacy.html).
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.

• Basic Setup Workflow, on page 17
• Discover Devices, on page 20
• Design Network Hierarchy, on page 38
• Manage Inventory, on page 58
• Add a Device to a Site, on page 62
• About Cisco ISE Configuration for Cisco DNA Center, on page 63
• Configure Syslog, SNMP Traps, and Netflow Collector Servers Using Telemetry, on page 67
• Configure Cisco AI Network Analytics Data Collection, on page 74
• Update the Machine Reasoning Knowledge Base, on page 77

Basic Setup Workflow

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

Note

Assurance is not supported over NATed connections to managed devices.

See the following illustration and the procedure that follows to understand the basic workflow.
Figure 4: Basic Workflow for Setting Up Cisco DNA Center to Use Assurance

1. Install Cisco DNA Center
2. Discover devices (IP address range, CDP, or LLDP)
3. Design your network hierarchy (site, area, building, and floor)
   (If sites are already created, skip this step and run Discovery)
4. Make sure devices appear in the Inventory
   (Wait for all devices to get into the Managed state)
5. Add devices to sites
6. (Optional) Configure Assurance for Cisco ISE integration
7. Configure syslog, SNMP, and NetFlow collector using Telemetry
8. (Recommended) Install and configure Cisco AI Network Analytics for AI-driven issues and insights
9. (Recommended) Update the Machine Reasoning Knowledge Base
10. Device ready for Assurance
**Step 1**

Install Cisco DNA Center.

See the Cisco Digital Network Architecture 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 27, Discover Your Network Using CDP, on page 22, or Discover Your Network Using LLDP, on page 31.

  **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 39, Add Buildings, on page 40, and Add a Floor to a Building, on page 40.

  **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 59.

**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 41.

**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 Configure Cisco DNA Center for Cisco ISE Integration, on page 63.

**Step 7**

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

See Configure Syslog, SNMP Traps, and Netflow Collector Servers Using Telemetry, on page 67

**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 74.

**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 77.

**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 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.

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. (The maximum latency is 200 ms.)

- 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 two criteria are 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 22.

- Configure anonymization. Anonymization scrambles the hostname and userid fields. For more information, see View or Update Collector Configuration Information, on page 249.

Important If you anonymize the data after you have run Discovery, the new data coming into the system will get anonymized but the existing data will not get anonymized.

Preferred Management IP Address

When Cisco DNA Center discovers a device, it logs one of the device's IP addresses as the preferred management IP address for the device. The IP address can be that of a built-in management interface of the device, or another physical interface, or a logical interface like Loopback0. You can configure Cisco DNA Center to log the device's loopback IP address as the preferred management IP address, provided the IP address is reachable from Cisco DNA Center.

If you choose to use a device's loopback IP address 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 27 and Discover Your Network Using LLDP, on page 31.

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 that they are connected to.

Before you begin

- Enable CDP on your network devices.

- Configure your network devices, as described in Discovery Prerequisites, on page 21.

- 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
From the Cisco DNA Center home page, click Discovery.

Step 2
In the Discovery Name field, enter a name.

Step 3
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 21.

  **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 4**  
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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or phrase that describes the CLI credentials.</td>
</tr>
<tr>
<td>Username</td>
<td>Name that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td>Password</td>
<td>Password that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td></td>
<td>For security reasons, enter the password again as confirmation.</td>
</tr>
<tr>
<td>Note</td>
<td>Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>
d) Click SNMP v2c and configure the following fields:

**Table 3: SNMPv2c Credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Password</td>
<td>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, enter the enable password again.</td>
</tr>
<tr>
<td></td>
<td>Note: Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>

- **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 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv3 settings that you are adding.</td>
</tr>
<tr>
<td>Username</td>
<td>Name associated with the SNMPv3 settings.</td>
</tr>
<tr>
<td>Mode</td>
<td>Security level that an SNMP message requires. Choose one of the following modes:</td>
</tr>
<tr>
<td></td>
<td>• <strong>noAuthNoPriv</strong>: Does not provide authentication or encryption.</td>
</tr>
<tr>
<td></td>
<td>• <strong>AuthNoPriv</strong>: Provides authentication, but does not provide encryption.</td>
</tr>
<tr>
<td></td>
<td>• <strong>AuthPriv</strong>: Provides both authentication and encryption.</td>
</tr>
</tbody>
</table>
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 8 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.

**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 8 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Retries</strong></td>
<td>Number of times Cisco DNA Center tries to communicate with network devices using SNMP.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>Number of seconds between retries.</td>
</tr>
</tbody>
</table>
g) (Optional) Click HTTP(S) and configure the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Specifies the kind of HTTPS credentials you are configuring. Valid types are Read or Write.</td>
</tr>
<tr>
<td>Read</td>
<td>You can configure up to 5 HTTPS read credentials:</td>
</tr>
<tr>
<td></td>
<td>• Name/Description: Name or description of the HTTPS credentials that you are adding.</td>
</tr>
<tr>
<td></td>
<td>• Username: Name used to authenticate the HTTPS connection.</td>
</tr>
<tr>
<td></td>
<td>• Password: Password used to authenticate the HTTPS connection.</td>
</tr>
<tr>
<td></td>
<td>• Port: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).</td>
</tr>
<tr>
<td>Note</td>
<td>The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain &lt; &gt; @ ’ : ; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
<tr>
<td>Write</td>
<td>You can configure up to 5 HTTPS write credentials:</td>
</tr>
<tr>
<td></td>
<td>• Name/Description: Name or description of the HTTPS credentials that you are adding.</td>
</tr>
<tr>
<td></td>
<td>• Username: Name used to authenticate the HTTPS connection.</td>
</tr>
<tr>
<td></td>
<td>• Password: Password used to authenticate the HTTPS connection.</td>
</tr>
<tr>
<td></td>
<td>• Port: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).</td>
</tr>
<tr>
<td>Note</td>
<td>The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain &lt; &gt; @ ’ : ; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>

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 5 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 6 Click Discover and select whether to run the discovery now or schedule the discovery for a later time.
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 22 and Discover Your Network Using LLDP, on page 31.

Before you begin
Your devices must have the required device configurations, as described in Discovery Prerequisites, on page 21.

Step 1
From the Cisco DNA Center home page, click Discovery.

Step 2
In the Discovery Name field, enter a name.

Step 3
Expand the IPAddress/Ranges area, if it is not already visible, and configure the following fields:

a) For Discovery Type, click 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 Start.

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) 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 21.

Step 4
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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or phrase that describes the CLI credentials.</td>
</tr>
<tr>
<td>Username</td>
<td>Name that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td>Password</td>
<td>Password that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td></td>
<td>For security reasons, enter the password again as confirmation.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Password used to move to a higher privilege level in the CLI.</td>
</tr>
<tr>
<td></td>
<td>For security reasons, enter the enable password again.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>

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

**Table 8: SNMPv2c Credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>• <strong>Name/Description</strong>—Name or description of the SNMPv2c settings that you are adding.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Read Community</strong>—Read-only community string password used only to view SNMP information on the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
<tr>
<td>Write</td>
<td>• <strong>Name/Description</strong>—Name or description of the SNMPv2c settings that you are adding.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Write Community</strong>—Write community string used to make changes to the SNMP information on the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>

e) (Optional) Click **SNMP v3** and configure the following fields:
### Table 9: SNMPv3 Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv3 settings that you are adding.</td>
</tr>
<tr>
<td>Username</td>
<td>Name associated with the SNMPv3 settings.</td>
</tr>
<tr>
<td>Mode</td>
<td>Security level that an SNMP message requires. Choose one of the following modes:</td>
</tr>
<tr>
<td></td>
<td>• noAuthNoPriv: Does not provide authentication or encryption.</td>
</tr>
<tr>
<td></td>
<td>• AuthNoPriv: Provides authentication, but does not provide encryption.</td>
</tr>
<tr>
<td></td>
<td>• AuthPriv: Provides both authentication and encryption.</td>
</tr>
<tr>
<td>Auth Type</td>
<td>Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Choose one of the following authentication types:</td>
</tr>
<tr>
<td></td>
<td>• SHA: Authentication based on HMAC-SHA.</td>
</tr>
<tr>
<td></td>
<td>• MD5: Authentication based on HMAC-MD5.</td>
</tr>
<tr>
<td>Auth Password</td>
<td>SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 characters in length.</td>
</tr>
<tr>
<td>Note</td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
<tr>
<td>Privacy Type</td>
<td>Privacy type. (Enabled if you select AuthPriv as the authentication mode.) Choose one of the following privacy types:</td>
</tr>
<tr>
<td></td>
<td>• DES: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard.</td>
</tr>
<tr>
<td></td>
<td>• AES128: CBC mode AES for encryption.</td>
</tr>
<tr>
<td></td>
<td>• None: No privacy.</td>
</tr>
</tbody>
</table>
Discover Your Network Using an IP Address Range

Set Up Cisco DNA Center to Use Assurance

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Password</td>
<td>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 8 characters long.</td>
</tr>
</tbody>
</table>
| **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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retries</td>
<td>Number of times Cisco DNA Center tries to communicate with network devices using SNMP.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Number of seconds between retries.</td>
</tr>
</tbody>
</table>

Note

`Read` Cisco DNA Assurance User Guide, Release 1.3.1.0

30

Discover Your Network Using an IP Address Range

Set Up Cisco DNA Center to Use Assurance

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Specifies the kind of HTTPS credentials you are configuring. Valid types are <strong>Read</strong> or <strong>Write</strong>.</td>
</tr>
<tr>
<td>Read</td>
<td>You can configure up to 5 HTTPS read credentials:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name/Description</strong>: Name or description of the HTTPS credentials that you are adding.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Username</strong>: Name used to authenticate the HTTPS connection.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Password</strong>: Password used to authenticate the HTTPS connection.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Port</strong>: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain <code>&lt; &gt; @ </code> ' : ; !` or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>
You can configure up to 5 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.
- **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 at least one lower case, one upper case, one digit, and a special character and must not contain < > @ ' , : ; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

**Note**

Step 5

(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 6

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 22 and **Discover Your Network Using an IP Address Range**, on page 27.
• 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 that they are connected to.

### Before you begin

• Enable LLDP on your network devices.

• Configure your network devices, as described in Discovery Prerequisites, on page 21.

• 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**  
From the Cisco DNA Center home page, click **Discovery**.

**Step 2**  
In the **Discovery Name** field, enter a name.

**Step 3**  
Expand the **IPAddress/Range** area if it is not already visible, 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 21.

**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 4**  
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*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or phrase that describes the CLI credentials.</td>
</tr>
<tr>
<td>Username</td>
<td>Name that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td>Password</td>
<td>Password that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td></td>
<td>For security reasons, enter the password again as confirmation.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it.</td>
</tr>
<tr>
<td></td>
<td>For security reasons, enter the enable password again.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>

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

*Table 13: SNMPv2c Credentials*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td><strong>Name/Description</strong>—Name or description of the SNMPv2c settings that you are adding.</td>
</tr>
<tr>
<td></td>
<td><strong>Read Community</strong>—Read-only community string password used only to view SNMP information on the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
<tr>
<td>Write</td>
<td><strong>Name/Description</strong>—Name or description of the SNMPv2c settings that you are adding.</td>
</tr>
<tr>
<td></td>
<td><strong>Write Community</strong>—Write community string used to make changes to the SNMP information on the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>

e) (Optional) Click **SNMP v3** and configure the following fields:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv3 settings that you are adding.</td>
</tr>
<tr>
<td>Username</td>
<td>Name associated with the SNMPv3 settings.</td>
</tr>
<tr>
<td>Mode</td>
<td>Security level that an SNMP message requires. Choose one of the following modes:</td>
</tr>
<tr>
<td></td>
<td>• noAuthNoPriv: Does not provide authentication or encryption.</td>
</tr>
<tr>
<td></td>
<td>• AuthNoPriv: Provides authentication, but does not provide encryption.</td>
</tr>
<tr>
<td></td>
<td>• AuthPriv: Provides both authentication and encryption.</td>
</tr>
<tr>
<td>Auth Type</td>
<td>Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Choose one of the following authentication types:</td>
</tr>
<tr>
<td></td>
<td>• SHA: Authentication based on HMAC-SHA.</td>
</tr>
<tr>
<td></td>
<td>• MD5: Authentication based on HMAC-MD5.</td>
</tr>
<tr>
<td>Auth Password</td>
<td>SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 characters in length.</td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
<tr>
<td>Privacy Type</td>
<td>Privacy type. (Enabled if you select AuthPriv as the authentication mode.) Choose one of the following privacy types:</td>
</tr>
<tr>
<td></td>
<td>• DES: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard.</td>
</tr>
<tr>
<td></td>
<td>• AES128: CBC mode AES for encryption.</td>
</tr>
<tr>
<td></td>
<td>• None: No privacy.</td>
</tr>
</tbody>
</table>
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 8 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Password</td>
<td>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 8 characters long.</td>
</tr>
</tbody>
</table>

**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.


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

**Table 16: HTTP(S) Credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Specifies the kind of HTTPS credentials you are configuring. Valid types are <strong>Read</strong> or <strong>Write</strong>.</td>
</tr>
</tbody>
</table>

**Read**
- You can configure up to 5 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.
  - **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

**Note**
- The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain < > @ , ; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.
Set Up Cisco DNA Center to Use Assurance

Manage Discovery Jobs

Step 5 (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 6 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 From the Cisco DNA Center home page, click Discovery.

Step 2 To stop an active Discovery job, perform these steps:

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

Step 3 To restart an inactive Discovery job, perform these steps:

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

---

**Clone a Discovery Job**

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

**Before you begin**

You should have run at least one Discovery job.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>From the Cisco DNA Center home page, click <strong>Discovery</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>From the <strong>Discoveries</strong> pane, select the Discovery job.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click <strong>Clone &amp; Edit</strong>. Cisco DNA Center creates a copy of the Discovery job, named Copy of <strong>Discovery_Job</strong>.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Change the name of the Discovery job.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Define or update the parameters for the new Discovery job.</td>
</tr>
</tbody>
</table>

**Delete a Discovery Job**

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

**Before you begin**

You should have run at least one Discovery job.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>From the Cisco DNA Center home page, click <strong>Discovery</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>From the <strong>Discoveries</strong> pane, select the Discovery job that you want to delete.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click <strong>Delete</strong>.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Click <strong>OK</strong> to confirm.</td>
</tr>
</tbody>
</table>

**View Discovery Job Information**

You can view information about a Discovery job, such as the settings and credentials that were used. You can also 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>From the Cisco DNA Center home page, click <strong>Discovery</strong>.</td>
</tr>
</tbody>
</table>
**Design Network Hierarchy**

You can create a network hierarchy that represents your network's geographical locations. Your network hierarchy can contain sites, which contain 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 20.

You can perform these tasks in the Design area:

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create your network hierarchy.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Define global network settings.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Define network profiles.</td>
</tr>
</tbody>
</table>

**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.

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 39.
- Upload an existing network hierarchy from Cisco Prime Infrastructure. For more information, see Upload an Existing Site Hierarchy, on page 43.

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 application 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 From the Cisco DNA Center home page, choose Design > Network Hierarchy. A world map is displayed.

Step 2 On the Network Hierarchy window, click + Add Site, or click the gear icon next to the parent site in the left pane, and then select the appropriate option.

Step 3 You can also upload an existing hierarchy. For more information, see Upload an Existing Site Hierarchy, on page 43.

Step 4 Enter a name for the site, and select 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 menu.

---

**Add Buildings**

**Step 1**
From the Cisco DNA Center home page, choose **Design > Network Hierarchy**.

A world map is displayed.

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

**Step 3**
You can also upload an existing hierarchy. See **Upload an Existing Site Hierarchy, on page 43**.

**Step 4**
Enter a name for the building.

**Step 5**
In the **Address** text 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. 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**
From the Cisco DNA Center home page, 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 has a 21-character limit. The floor name must 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 5: Example of a Floor Plan](Image)

**Step 7** Click **Add**.

---

**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 20**.

Cisco DNA Center supports the following 802.11ax APs:

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

---

**Step 1** From the Cisco DNA Center home page, 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 APs in bulk, and click **Add Selected**. Alternatively click **Add** adjacent 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 3 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 2 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.
For external APs, you must select an antenna, otherwise, 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.

### Step 9

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

Heatmap is generated based on the new position of the AP.

If a Cisco Connected Mobile Experiences (CMX) is synchronized with Cisco DNA Center, then you can view the location of clients on the heatmap. See Create Cisco CMX Settings, on page 172.

### Step 10

In the **Floor Elements** panel, next to **Access Points**, click **Delete**.
The **Delete APs** window appears which lists all the assigned and places access points, appears.

### 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 click **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.

---

### 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 more information, see Export Maps Archive, on page 44 on how to export maps from Cisco Prime Infrastructure.

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

### Step 1

From the Cisco DNA Center home page, choose **Design > Network Hierarchy**, and then click **Import > Import Sites**.

### Step 2

Drag and drop your CSV file, or navigate to where your CSV file is located, then click **Import** to import the Cisco Prime Infrastructure Groups CSV file.

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, click **Import > Map Import**.
**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**
From the Cisco DNA Center home page, 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.
## Delete Sites

**Step 1** From the Cisco DNA Center home page, 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** 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 Buildings

**Step 1** From the Cisco DNA Center home page, 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** From the Cisco DNA Center home page, 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

Guidelines for Placing Access Points

Follow these guidelines while placing APs on the floor map:
• Place access points along the periphery of coverage areas to keep devices close to the exterior of rooms and buildings. Access points 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. Hence, 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.

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 20.

Cisco DNA Center supports the following 802.11ax APs:

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

Step 1
From the Cisco DNA Center home page, 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 APs in bulk, and click Add Selected.
Alternatively click Add adjacent 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 3 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 2 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, otherwise, 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.

**Step 9** After you have completed placing and adjusting access points, click **Save**. Heatmap is generated based on the new position of the AP.
If a Cisco Connected Mobile Experiences (CMX) is synchronized with Cisco DNA Center, then you can view the location of clients on the heatmap. See Create Cisco CMX Settings, on page 172.

**Step 10**

In the **Floor Elements** panel, next to **Access Points**, click **Delete**.
The **Delete APs** window appears which lists all the assigned and places access points, appears.

**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 click **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 AP 1800S 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 AP 1800S sensor gets bootstrapped using PnP. After it obtains the Assurance server reachability details, it directly communicates with the Assurance server.

Step 1: From the Cisco DNA Center home page, 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 these 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: From the Cisco DNA Center home page, 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 to 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  From the Cisco DNA Center home page, 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, which results in the area getting highlighted.
**Step 10**  Click Done in the Obstacle Creation window that appears.
**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**  From the Cisco DNA Center home page, 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.
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 From the Cisco DNA Center home page, 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.
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 3 Click Save.

Step 1 From the Cisco DNA Center home page, 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 then 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 to delete.
Step 13 Click Save.

Place Markers

Step 1 From the Cisco DNA Center home page, 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 to 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**

Click the On/Off button next to Access Points to view access points on the map. 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 1000 series APs accept a value between 1 and 5, the 1230 access points accept a value between 1 and 7, and the 1240 and 1100 series access points 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, or Coverage.
  - None
  - Coverage—If you have monitor mode access points on the floor plan, you can select coverage heatmap. A coverage heatmap excludes monitor mode access points.

- **Heatmap Opacity (%)**—Drag the slider between 0 to 100 to set the heatmap opacity.
- **RSSI Cut off (dBm)**—Drag the slider to set the RSSI cutoff level. The RSSI cutoff ranges from -60 dBm to -90 dBm.
- **Map Opacity (%)**—Drag the slider to set the map opacity.

The AP details are reflected on the map immediately. Hover your cursor over the AP icon on the map to view AP details and RX neighbor 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 Maps 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 21.

After the initial discovery, Cisco DNA Center maintains the inventory by polling the devices at regular intervals. The default interval is every 6 hours. However, you can change this interval upto 24 hours, as required for your network environment. For more information, see Update Device Resync Interval, on page
59. 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 a day are displayed. This prevents stale device data, if any, from being displayed. On an average, polling 500 devices takes approximately 20 minutes.

**Update Device Resync Interval**

From the **Inventory** window, you can configure device resynchronization in the following ways:

- You can enable and configure a custom resynchronization interval for a specific device.
- You can enable the preconfigured global resynchronization interval that is set for all the devices. (This setting is configured in the **Settings > System Settings > Settings > Network Resync Interval** window.
- You can disable resynchronization.

**Before you begin**

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

**Step 1**

From the Cisco DNA Center home page, click **Provision**.

The Inventory page displays the device information gathered during the Discovery process.

**Step 2**

Select the devices that you want to update.

**Step 3**

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

The **Edit Device** dialog box is displayed.

**Step 4**

In **Resync Interval** tab, click the radio button that corresponds to the type of resynchronization option you want to configure for the device. Valid choices are **Custom**, **Global**, and **Disable**.

**Step 5**

If you chose **Custom**, in the **Resync Interval (in Mins)** field, enter the time interval (in minutes) between successive polling cycles. Valid values are from 25 to 1440 minutes (24 hours).

**Step 6**

Click **Update**.

**Display Information About Your Inventory**

The **Inventory** table displays information for each discovered device. All of the columns, except the **Config** column, support sorting. Click the column header to sort the rows in ascending order. Click the column header again to sort the rows in descending order.

**Before you begin**

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

From the Cisco DNA Center home page, click **Provision**.

The **Inventory** window displays the device information gathered during the discovery process. The following table describes the information that is available.
Table 17: Inventory

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Name</strong></td>
<td>Name of the device. Click the name to display a dialog box with the following information:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Details</strong>: Displays details such as device name, device type, IP address, serial number, software image, and so on.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Configuration</strong>: Displays detailed configuration information similar to what is displayed in the output of the <code>show running-config</code> command.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: This feature is not supported for access points (APs) and wireless controllers. Therefore, configuration data is not returned for these device types.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Interface</strong>: Displays <strong>Interface Name</strong>, <strong>MAC Address</strong>, and <strong>Status</strong> of the interfaces on the device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Stack</strong>: Displays MAC address, role, state, and priority.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Run Commands</strong>: Opens Command Runner to execute CLI commands on the device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>View 360</strong>: Displays 360 window. For 360 to open, you must have installed the Assurance application.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: 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.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>IP address of the device</td>
</tr>
<tr>
<td><strong>Support Type</strong></td>
<td>Shows the device support level as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Supported</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unsupported</strong>: All remaining Cisco and third party devices which are not tested and certified on Cisco DNA Center. You may try out various functionalities on Cisco DNA Center for these devices as 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Third Party</strong>: Device pack is built by customers/business partners and has gone through the certification process. Third party devices will support base automation capabilities such as Discovery, Inventory, Topology, and so on. Cisco TAC will provide an initial level of support for these devices. However, if there is a problem with the device pack, you must reach out to the business partner for a fix.</td>
</tr>
</tbody>
</table>
The following is a list of the various statuses:

- **Connecting**: Cisco DNA Center is connecting to the device.
- **Reachable**: Cisco DNA Center has connected to the device and is able to execute Cisco commands using the CLI.
  
  **Note** A failure indicates that Cisco DNA Center is connected to the device, but is unable to execute Cisco commands using the CLI. This status usually indicates that the device is not a Cisco device.

- **Authentication Failed**: Cisco DNA Center has connected to the device, but is unable to determine what type of device it is.
- **Unreachable**: Cisco DNA Center is unable to connect to the device.
  
  **Note** Sometimes a device is unreachable because the Discovery job does not have its credentials or the Discovery job has the wrong credentials. If you suspect this might be the case, run a new Discovery job and make sure to specify the device's correct credentials.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reachability</td>
<td>The following is a list of the various statuses:</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address of the device</td>
</tr>
<tr>
<td>Image Version</td>
<td>Cisco IOS software that is currently running on the device</td>
</tr>
<tr>
<td>Platform</td>
<td>Cisco product part number</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Cisco device serial number</td>
</tr>
<tr>
<td>Uptime</td>
<td>Period of time that the device has been up and running</td>
</tr>
<tr>
<td>Device Role</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>If required, you can use the drop-down list in this column to change the assigned device role. The following device roles are available:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Unknown</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Access</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Core</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Distribution</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Border Router</strong></td>
</tr>
</tbody>
</table>
### Add a Device to a Site

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

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td>The site to which the device is assigned. Click <strong>Assign</strong> if the device is not assigned to any site. Click <strong>Choose a Site</strong>, select a site from the hierarchy, and then click <strong>Save</strong>. For more information, see About Network Hierarchy, on page 38.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>Most recent date and time that Cisco DNA Center scanned the device and updated the database with new information about the device.</td>
</tr>
<tr>
<td>Device Family</td>
<td>Group of related devices, such as routers, switches, hubs, or wireless controllers</td>
</tr>
<tr>
<td>Device Series</td>
<td>Series number of the device; for example, Cisco Catalyst 4500 Series Switches</td>
</tr>
<tr>
<td>Resync Interval</td>
<td>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 Digital Network Architecture Center Administrator Guide.</td>
</tr>
<tr>
<td>Last Sync Status</td>
<td>Status of the last Discovery scan for the device:&lt;br&gt;&lt;ul&gt;&lt;li&gt;<strong>Managed</strong>: Device is in a fully managed state.&lt;/li&gt;&lt;li&gt;<strong>Partial Collection Failure</strong>: Device is in a partial collected state and not all the inventory information has been collected. Move the cursor over the Information (i) icon to display additional information about the failure.&lt;/li&gt;&lt;li&gt;<strong>Unreachable</strong>: Device cannot be reached and no inventory information was collected due to device connectivity issues. This condition occurs when periodic collection takes place.&lt;/li&gt;&lt;li&gt;<strong>Wrong Credentials</strong>: If device credentials are changed after adding the device to the inventory, this condition is noted.&lt;/li&gt;&lt;li&gt;<strong>In Progress</strong>: Inventory collection is occurring.&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
</tbody>
</table>

---

**Add a Device to a Site**

1. **Step 1**  From the Cisco DNA Center home page, click **Provision**. The **Inventory** window displays the device information gathered during the **Discovery** process.
2. **Step 2**  Check the check box for the devices that you want to assign to a site.
3. **Step 3**  From the **Actions** menu, choose **Provision > Assign Device to Site**. The **Assign Device to Site** slide-in pane appears.
4. **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.
5. **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**.

---

### 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.

Beginning with Cisco DNA Center Release 1.3, Cisco ISE configuration is centralized within NCP (Network Control Platform). This enables you to configure Cisco ISE at one GUI location. The workflow for configuring Cisco ISE is as follows:

1. Enter the Cisco ISE configuration details in NCP (**System Settings > Settings > Authentication and Policy Servers**).
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 Cisco DNA Center for Cisco ISE Integration

Use this procedure to configure Cisco DNA Center for Cisco ISE integration.

**Before you begin**

- Enable Cisco ISE pxGrid services.
- Make sure the CLI and UI user accounts for Cisco ISE have the same username and password.
- Make sure the Cisco DNA Center version is 1.3 or later.

**Note**

Cisco DNA Center uses Cisco ISE Internal certificate authority (CA)-signed certificates for integration with Assurance. To use a CA-signed certificate:

- The Cisco DNA Center pxGrid client certificate must have “client authentication” in its extended key usage (EKTU) extension.
- Cisco ISE must be the issuer of the certificate in the truststore.jks file.
Configure Authentication and Policy Servers

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, as described in the Cisco Digital Network Architecture Center Installation Guide.

- 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.

---

Step 1
From the Cisco DNA Center home page, choose 🌐 > System Settings > Data Platform > Collectors. The Collectors window appears.

Step 2
Click COLLECTOR-ISE. The COLLECTOR-ISE window appears.

Note: The COLLECTOR-ISE window is read-only mode.

Step 3
In the Current Configurations tab, click Click to configure. The Authentication and Policy Servers window appears.

Step 4
To configure a Cisco ISE server, see Configure Authentication and Policy Servers, on page 64.

Attention: If a configuration exists for the ISE collector, but Cisco ISE is not successfully configured in the Authentication and Policy Servers window, a banner appears. The banner prompts the Cisco DNA Center administrator to add Cisco ISE configuration in the Authentication and Policy Servers window.

Step 5
(Optional) To anonymize (scramble) personal identifiable data, such as user ID and device host name, do the following:

a) Click the 🌐 icon, and then choose System Settings > Settings.

b) Click Anonymize Data. The Anonymize Data window appears.

c) Click Enable Anonymization.

Note: Once you enable anonymization, you can only search for the device using non-anonymized information such as the MAC address, IP address, etc.

- If anonymization was enabled in Cisco DNA Center Release 1.2.10 and earlier, the setting is kept when upgrading to Cisco DNA Center Release 1.3.

Caution: Make sure that you enable Anonymization before you run Discovery. If you anonymize the data after you run Discovery, the new data coming into the system will get anonymized but the existing data will not be anonymized.
• 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 version 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.
  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 third-party certificate 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**  
From the Cisco DNA Center home page, choose 🌐 > System Settings > Settings > 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 be up to 128 characters in length.

**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:

- **Cisco ISE**: Setting that indicates whether the server is a Cisco ISE server. Click the Cisco ISE toggle to enable Cisco ISE.
- **Username**: Name that is used to log into 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.
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.

- **Subscriber Name**: Unique text string that identifies a pxGrid client registering for Cisco ISE pxGrid services; for example, acme. The subscriber name is used during Cisco DNA Center-to-Cisco ISE integration.

- **SSH Key**: Diffie-Hellman-Group14-SHA1 SSH key used to connect and authenticate with Cisco ISE.

- **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 few 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 ISE server is "FAILED" due to password change, click Retry, and update the password to re-sync the ISE connectivity.

**Step 5**

Click View Advanced Settings and configure the settings:

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

  **Attention**: If you do not choose TACAS for Cisco ISE servers, it will not be available for configuring Cisco ISE nodes.

- **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. The default port is 49.

- **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.
Set Up Cisco DNA Center to Use Assurance

Configure Syslog, SNMP Traps, and Netflow Collector Servers Using Telemetry

- **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 Step 2 through Step 6.

---

**Configure Syslog, SNMP Traps, and Netflow Collector Servers Using Telemetry**

**Step 1**
- Create a site and assign a device to the site.
  
  See [Create a Site in a Network Hierarchy](#), on page 39.

**Step 2**
- Configure the IP address for the Syslog, SNMP, and Netflow Collector servers. Do the following:
  a) From the Cisco DNA Center home page, choose **Design > Network Settings > Network**.
  b) In the **SYSLOG Server** field, enter the IP address of a Syslog server.
     
     **Note**
     Make sure the **Cisco DNA Center as syslog server** check box is checked. This is required for Assurance. This option enables Assurance to use Syslog events to trigger certain issues and to display Syslog events in the **Device 360** window.
  c) In the **SNMP Server** field, enter the IP address of an SNMP server.
     
     **Note**
     Make sure the **Cisco DNA Center as snmp server** check box is checked. This is required for Assurance.
  d) In the **Time Zone** drop-down list, choose a time zone for the selected site based on the geographical location of the site.
     
     **Note**
     By default, server time is used in the time zone settings. The timezone is used while scheduling updates to devices or to schedule provisioning.
  e) In the **Message of the day** (MOTD) field, enter a message, which is displayed as an MOTD banner when you log on to a device.
     
     **Note**
     Custom MOTD messages can be up to 40 lines. Each line must be 80 characters or less; alphanumeric characters, uppercase or lowercase characters, and special characters other than # are allowed. Check the check box below the MOTD field if you do not want to override the existing MOTD message on the device.

**Step 3**
- Add the device to a site so that the configuration is pushed from Cisco DNA Center to the devices.
  
  See [Add a Device to a Site](#), on page 62.

**Step 4**
- Apply the Telemetry Quotient (TQ) profile on the device to the right logging level. Do the following:
  a) Choose **Design > Network Settings > Network**, and click **Network Telemetry**.
  b) Click the **Site View** tab.
     A list of devices are displayed.
  c) Check the check box adjacent to the router.
d) From the Actions drop-down list, choose the logging level:

- **Maximal Visibility**: This enables Syslog Level 6 (informational).
- **Optimal Visibility**: This enables Syslog Level 6 and Network on routers.
- **Disable Telemetry**

**Step 5** *(Optional)* To add a NetFlow Collector Server, choose **Design > Network Settings > Network**, and click **Add Servers**. The **Add Servers** window displays.

a) Check the check box for **NetFlow Collector**. The NetFlow Collector Server is added to the **Network** window.

b) In the **NetFlowCollectorServer** area, enter the IP address and port number of the NetFlow Collector Server.

c) Click **Save**.

**Example of Switch Syslog, SNMP Traps, and Netflow Collector and Other Configurations**

```plaintext
exampleofswitchsyslog,snmptraps,netflowcollectorandotherconfigurations

crypto pki trustpoint DNAC-CA
enrollment mode ra
usage ssl-client
revocation-check crl none
!
crypto pki certificate chain DNAC-CA
certificate ca 00156FDDCC160F24A
308202F7 308201DF A0030201 02020900 9156FDDC C160F24A 300D0609 2A864886F7000101 0B050030 1231030 0E060355 0403C0C7 68756265 2D636130 1E170D313B03530 33030335 3923235A 170D3231 30313237 30303539 32335A30 1231030 0E040C07 68756265 2D636130 82012230 0D0609A 864886F7 0D010101 0500036A 010F0030 82010A02 82010100 D4771B0 47DF36C5 26AF54CB 32D606B0 CB96C023 8CD6FDDD 5262A340 715F506D AEF2BF13 37D9BA1C C79577A9 1800424F 5FEE5C9C 5694BE62 A53FEF15 8AC8A186 161A8D88 D44F2F66 BD9D3142 743020BA 31DF43A5 E465E50B EEEC59BF 68280E1A 80622500 9D031B15 9FD45E18 121C2726 69B7D768 8EDAC319 7CDBF68C 137A567E 8EE7D5C5 71B34592 CAD1AB0 590DC57A 8A17276E 104C0850 180F1D0C 28649C5B 73485C9F 0453E248 36937F5E 486191C3 65667BC9 9339B6E6 C0674594 9194EF4E CB48455F 1ACCEB5F 82010A012 548136C5 53015248 0F8D8EA5 3F4281BB 79A31B3A 2276AFAF 20D91016 94CC3939 BF2F9CA4 3D345E2F 80DDC0EA3 45DF5FEB 670C9F6B 02030100 0A350300 4E301D06 03551D0E 04160414 6352B371 86225207 1A79B16E D2645368 929A96C0 301F0603 551D2304 18301680 14362528 71862250 271A79B1 6ED26453 68929A96 C0300C06 03551D03 04053003 01FF3000 D06092A 864886F7 0D01010B 05000382 01010094 5751DB9B 6C460EB0 892A2CE2 450AA9F5 5C7D41AA 87CD02C5 47E78771 C3FEDCA2 76444620 90CAB980 BE0A2C0D 2A2D13523 01956BBE 91FE9EAC 123A6A7F C61277D5 74556B38 4BBD6691 785E87CD 581A95F0 8206101D 54AE51D0 0207F32 041A51E F49A157F 028152C7 E8A53C3C 1282BB0B 0DCCE370 1FF48867 5A88E1A2 9E8E106A 87F43E69 37234547 F00E1773 733CAFP6 058E7A00 158F6501 E1845537 17E3F2BE BCC520D0 C54E960C B18A30F1 AC4DA1E2 809DFB0 23B28E318 18C95393 C31A3FC8 45D8C79D 01A90F87 C9262FDB DDF25B8D 867E0B64 1426B072 3F31BAD8 14F4C4AC5 FC039912 E2881ACF 5F2EC94C D08B220B 3AF84E3F 32C501F3 5E71A656 BEABE3 quit
interface GigabitEthernet1/0/2
ip device tracking maximum 10
!
interface GigabitEthernet1/0/3
ip device tracking maximum 10
!
flow exporter 10.4.48.218
destination 10.4.48.218
!
smtp-server community cisco RO
```

Cisco DNA Assurance User Guide, Release 1.3.1.0

Configure Syslog, SNMP Traps, and Netflow Collector Servers Using Telemetry

Set Up Cisco DNA Center to Use Assurance
snmp-server community cisco123 RW
!
logging host 7.7.7.7
!
snmp-server community cisco1 RO
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps transceiver all
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps rf
snmp-server enable traps memory
snmp-server enable traps wireless bsnMobileStation bsnAccessPoint bsnRogue bsn80211Security bsnAutoRF

bsnGeneral SI mobility mfp RRM AP rogue client
snmp-server enable traps cpu threshold
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps flash insertion removal
snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet police
snmp-server enable traps energywise
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlancedelete
snmp-server enable traps license
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps stackwise
snmp-server enable traps port-security
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps trustsec-sxp conn-srcaddr-err msg-parse-err conn-config-err binding-err
conn-up conn-down binding-expn-fail oper-nodelid-change binding-conflict
snmp-server enable traps trustsec-server radius-server provision-secret
snmp-server enable traps trustsec authz-file-error cache-file-error keystore-file-error
keystore-sync-fail random-number-fail src-entropy-fail
snmp-server enable traps trustsec-interface unauthorized sap-fail authc-fail supplicant-fail authz-fail
snmp-server enable traps trustsec-policy peer-policy-updated authz-sqacl-fail
snmp-server enable traps bgp cbgp2
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change inconsistency
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps event-manager
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps isis
snmp-server enable traps local-auth
snmp-server enable traps msdp
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps vstack
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps syslog
snmp-server enable traps ipsla
snmp-server enable traps ike policy add
snmp-server enable traps ike policy delete
snmp-server enable traps ike tunnel start
snmp-server enable traps ike tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server host 8.8.8.8 public
!
ip http client source-interface GigabitEthernet1/0/1
!
ip ssh source-interface GigabitEthernet1/0/1

Example of Router Syslog, SNMP Traps, and Netflow Collector and Other Configurations

crypto pki trustpoint DNA-CA
  enrollment mode ra
  enrollment terminal
  usage msl-client
  revocation-check crl none
!
crypto pki certificate-chain DNA-CA
  certificate ca 0097DBDF3AEB517E
    308202F7 308201DF A0030201 02020900 D97DBDFA E3EB517E 300D0609 2A864886
    F7000101 08B00300 12311030 0B060355 04030C07 6B756265 2D636130 1B170D31
    3B303531 35303531 31313375A 170D3231 03023030 30353131 31375A30 12311030
    0B060355 04030C07 6B756265 2D636130 82012230 0D06092A 86486867 0D010101
    05000392 010F0030 82010A02 82010A02 0A6A31FC 5423822C CD1E016B A05117BC
    1E0808F5 7B082E41 7F125122 A049FB68 00E65F21 C5E14B5 D5EF89FC
    B87BECB3 9F749B19 46E65924 0B1780F2 4B31CDA3 1E0EED5D FFF4D29F FE935413
    DADD2DB4 9778ACD8 4AF1C1A8 9024F8E4 11ED9E29 979DB4C9 851C3737 98AE61B0
    3B54D6B F4417F8B 8E09658E 523636C 47052F02 E2E234A6 564D7104 4F09D989

C1B5B3B CDED2108 DA04C6B0 7E9A8E5 E03F6913 575C1567 97ECC40A AA53E91A
    7E4B2419 D90E41D 4B40F561 F766A4E2 B76B2482 E95AB7BA 0F6A42C 1E0F048B

97358BED 9A9B8C4F C127D3E8 FA1841F9 41B45392 4E546AEE 396D1D25 4B2DD897

6D5CD7AF 6E342548 2CF1BA48 DAA51C21 20301001 0A350300 48301D06 03551D0E

04160414 A811B663 0573E872 B4913BEF 69A82405 9A922D15 301F0603 551D2304

18301680 1A4811BE 6305373E 7284913B EF698A24 059A2D2F 55506300 5551D18

04053003 0101FF30 0D06092A 864886F7 0D01001B 05000382 01010078 67E62393

B47E8086 575E8F58 18F86578 1373E05E FB381F07 0F306852 A3FD0F2C 2CE40F7F 8251F171 1B82E671 0BA0DC05 4E94D4A8 D13BC4FC 1482B0A1 6ECD607F

EB03C9B9 A6BB9C3 64918957 DD4E0E5 60FDEF22 E468997B 77B9B18 4CC43B34

1A21C571 804AEC36 B6C14C6F 786D1C33 E655B518 E4310B6 33535E73 511189CF

CF472C43 D840ADB3 73BB94E E6434F74 D20DE99 DDE96858 B25C9C7 08C9F030

AE7A68C6 9B9C351C 97FDEDF0 76528507 60E13693 583BAC0B 7AFB3D84 8EF24861

FAC586B8 0F2B4D79 3E61B380 3B3A9BB2 AD85666B 16683040 A515C5D 826E2C0B

A0EDEEE91 12F2420B 86C9FC28 3A12B3EE 7E6DBA7B 58C8355C D94B29
quit
!
flow exporter 10.4.4.218
destination 10.4.4.218
!
smtp-server community cisco RO
snmp-server community cisco123 RW
!
logging host 7.7.7.7
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps pf
snmp-server enable traps flowmon
snmp-server enable traps ds1
snmp-server enable traps entity-perf throughput-notif
snmp-server enable traps ds3
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps casa
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps license
snmp-server enable traps smart-license
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change inconsistency
snmp-server enable traps memory bufferpeak
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dsp card-status
snmp-server enable traps dsp oper-state
snmp-server enable traps dsp video-usage
snmp-server enable traps dsp video-out-of-resource
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps event-manager
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ip local pool
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps atm subif
snmp-server enable traps pki
snmp-server enable traps ethernet evc status create delete
snmp-server enable traps ether-oam
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps entity-state
snmp-server enable traps entity-qfp mem-res-thresh throughput-notif
snmp-server enable traps adsline
snmp-server enable traps vds12line
snmp-server enable traps flash insertion removal lowspace
snmp-server enable traps srp
snmp-server enable traps entity-diag boot-up-fail hm-test-recover hm-thresh-reached scheduled-test-fail
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps cnpd
snmp-server enable traps bfd
snmp-server enable traps otb
snmp-server enable traps ipsla
snmp-server enable traps sonet
snmp-server enable traps dlsw
snmp-server enable traps resource-policy
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps c3g
snmp-server enable traps LTE
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlancedelete
snmp-server enable traps firewall serverstatus
snmp-server enable traps trustsec-sxp conn-srcaddr-err msg-parse-err conn-config-err binding-err
conn-up conn-down binding-expn-fail oper-nodeid-change binding-conflict
snmp-server enable traps lisp
snmp-server enable traps aaa_server
snmp-server enable traps dhcp
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps pw vc
snmp-server enable traps mpls rfc ldp
snmp-server enable traps mpls ldp
snmp-server enable traps mpls rfc traffic-eng
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls fast-reroute protected
snmp-server enable traps rs
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps mvpn
snmp-server enable traps pimstdmib neighbor-loss invalid-register invalid-join-prune rp-mapping-change

interface-election
snmp-server enable traps isis
snmp-server enable traps bgp cbgp2
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps nhrp nhb
snmp-server enable traps nhrp nhc
snmp-server enable traps nhrp nhp
snmp-server enable traps nhrp quota-exceeded
snmp-server enable traps ike policy add
snmp-server enable traps ike policy delete
snmp-server enable traps ike tunnel start
snmp-server enable traps ike tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps gdoi gm-start-registration
snmp-server enable traps gdoi gm-registration-complete
snmp-server enable traps gdoi gm-re-register
snmp-server enable traps gdoi gm-rekey-rcvd
snmp-server enable traps gdoi gm-rekey-fail
snmp-server enable traps gdoi ks-rekey-pushed
snmp-server enable traps gdoi gm-incomplete-cfg
snmp-server enable traps gdoi ks-no-rsa-keys
snmp-server enable traps gdoi ks-new-registration
snmp-server enable traps gdoi ks-reg-complete
snmp-server enable traps gdoi ks-role-change
snmp-server enable traps gdoi ks-gm-deleted
snmp-server enable traps gdoi ks-peer-reachable
snmp-server enable traps gdoi ks-peer-unreachable
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps alarms informational
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps rf
snmp-server enable traps transceiver all
snmp-server enable traps mpls vpn
snmp-server enable traps mpls rfvpn
snmp-server enable traps vmf mib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server host 8.8.8.8 public

ip http client source-interface GigabitEthernet0/0/1
ip ssh source-interface GigabitEthernet0/0/1

Example of Cisco Wireless Controller Syslog, SNMP Traps, and Netflow Collector and Other Configurations

config snmp community create cisco
config snmp community create cisco123
config snmp community mode enable cisco
config snmp community ipaddr 0.0.0.0 0.0.0.0 cisco
config snmp community mode enable cisco123
config snmp community accessmode rw cisco123
config snmp community ipaddr 0.0.0.0 0.0.0.0 cisco123

config network assurance server idtoken 1 6b5af7c9808a0b1b7824fc9a801b5478de751722396b0fe0b221b3be71f3a94ef2fe0716 16 8866db59c40e1f1f2fffc14097897ed62000000
config network assurance server url https://10.4.48.132
config network assurance on-change enable

config flow create exporter 10.4.48.218 10.4.48.218 port 6007
config logging level critical
config logging syslog level 2
config logging syslog facility syslog
config logging syslog host 7.7.7.7
config snmp trapreceiver create 8.8.8.8 8.8.8.8
config snmp trapreceiver ipsec profile none 8.8.8.8
config snmp trapreceiver mode enable 8.8.8.8

config trapflags client enhanced-802.11-deauthenticate enable
config trapflags client enhanced-802.11-associate enable
config trapflags client max-warning-threshold enable
config trapflags client 802.11-authfail disable
config trapflags client 802.11-associate disable
config trapflags client 802.11-disassociate disable
config trapflags client authentication disable
config trapflags client webauthuserlogout enable
config trapflags client 802.11-deauthenticate disable
config trapflags client neighborclientsignal disable
config trapflags client webauthuserlogin enable
config trapflags client 802.11-assocfail disable
config trapflags client excluded enable
config trapflags client enhanced-802.11-sts enable
config trapflags client enhanced-authentication enable
config trapflags client nac-alert enable
config trapflags client enhanced-802.11-disassociate-stats disable
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
From the Cisco DNA Center home page, choose 🕊 > System Settings > Settings > AI Network Analytics. The AI Network Analytics window appears.
Figure 6: AI Network Analytics Window

AI Network Analytics

Using AI and Machine Learning, Cisco AI Network Analytics drives intelligence in the network, empowering administrators to accurately and effectively improve performance and issue resolution. Cisco AI Network Analytics eliminates noise and false positives significantly by learning, modeling and adapting to your specific network environment.

Cloud Connection Test

Your network/HTTP proxy must be configured to allow HTTPS (TCP 443) access to the following host(s):

api.eu1.prd.kairos.ciscolabs.com CLOUD CONNECTION TEST PASSED

Secure Data Storage

Where should we securely store your data?

Europe (Germany) ▼

Restore Configuration

In case of an earlier installation on your appliance, and provided that none of the above values have changed since Karios was initially set up, we strongly recommend the upload of the previously saved configuration.

Drop your configuration file, or click to select it from your file system.

I agree that AI Network Analytics is governed by the Cisco Universal Cloud Agreement and that I have read and acknowledge the Cisco Privacy Statement. Note: If you do not have the authority to bind your company and its affiliates, or if you do not agree with the terms of the Universal Cloud Agreement, do not check this box.

Accept Cisco Universal Cloud Agreement

---

Step 2

In the Secure Data Storage area, choose the location where you would like to securely store your data. Options are: Europe (Germany) or US East (North Virginia).

Step 3

If you have an earlier version of Cisco AI Network Analytics installed in your appliance, drag-and-drop the configuration files in the Restore Configuration area or choose the files from your file system.

If none of the values have changed since the initial Cisco AI Network Analytics setup, we strongly recommend that you upload the previously saved configuration files.

Step 4

Click the Accept Cisco Universal Cloud Agreement check box to agree with the terms and conditions.

Step 5

Click Configure. The following occurs:

a. The Configure button changes to Configuring Data Collection....

b. After the configuration completes, the Registration Successful dialog box appears as shown in the following figure:
In the **Registration Successful** dialog box, click **Okay** to download the configuration and anonymization key.

After the download completes, the **AI Network Analytics** window appears, and the **Data Collection** area displays **Status: Enabled** with a ✔ mark.

---

**Related Topics**
- **Disable Cisco AI Network Analytics Data Collection**, on page 76

---

**Disable Cisco AI Network Analytics Data Collection**

To disable the 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.

---

1. From the Cisco DNA Center home page, choose 🌐 > **System Settings** > **Settings** > **AI Network Analytics**. The **AI Network Analytics** window appears.

2. From the **Data Collection** area, click the button to off, such that the status changes to **Disabled** and an X mark appears.
AI Network Analytics

Using AI and Machine Learning Cisco AI Network Analytics drives intelligence in the network, empowering administrators to accurately and effectively improve performance and issue resolution. Cisco AI Network Analytics eliminates noise and false positives significantly by learning, modeling and adapting to your specific network environment.

Cloud Connection Test

Your network/HTTP proxy must be configured to allow HTTPS (TCP 443) access to the following host(s):

api.eu1.prd.kairos.ciscolabs.com  CLOUD CONNECTION TEST PASSED

Data Collection

Data is being sent to region Europe (Germany).

Status: Disabled

Toggle to disable sending data to the cloud

⚠️ To delete all your data from the Cisco AI Network Analytics Cloud, please open a TAC case

Update

Anonymization

Download the configuration and anonymization key for archival.

**Step 3**

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

**Step 4**

(Optional) If you have misplaced your previous configuration and anonymization key, click **Download the configuration and anonymization key** from the **Anonymization** area.

**Step 5**

Click **Update**.

---

**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 basically 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**

From the Cisco DNA Center home page, click the gear icon and choose **System Settings > Settings > Machine Reasoning**.

The **Machine Reasoning** window appears.

*Figure 9: Machine Reasoning Window*

**Step 2**

(Recommended) To automatically update the Machine Reasoning Knowledge Base in the Cisco DNA Center, enable **Auto Update** by clicking it such that you see a ✔ mark.

The frequency, date, and time of the next update is displayed in the **Frequency** and **Next Attempt** areas.

*Note* You can perform an auto update only if Cisco DNA Center is successfully connected to the Machine Reasoning Engine in the cloud, as shown below:

![Successfully Connected.]

**Step 3**

To perform manual updates, do *one* of the following:

- Download the Machine Reasoning Knowledge Base to your local machine, and then import it to Cisco DNA Center.

  Do the following:

  a. Click the hyper-linked **here** text, as shown below.

    Dynamic updates to the Machine Reasoning knowledge base can immediately apply new Cisco expertise to identify security issues and improve automated analysis. 
    Click **here** to download the latest available knowledge base.

    The **Opening mre_workflow_signed.tar.gz** dialog box appears.

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

  c. To import the downloaded Machine Reasoning Knowledge Base from your local machine to Cisco DNA Center, click **Import from local**.
• To directly import the latest Machine Reasoning Knowledge Base from Cisco Systems into Cisco DNA Center, click **Import Latest from Cisco**. The **Success** pop-up box appears on the bottom-right corner with the status of the update.
Update the Machine Reasoning Knowledge Base
CHAPTER 5

Monitor and Troubleshoot Overall Enterprise Health

- About Enterprise, on page 81
- Monitor and Troubleshoot the Overall Health of Your Enterprise, on page 81

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 17.

Step 1

From the Cisco DNA Center home page, click the Assurance tab.

The Overall Health dashboard appears.
Step 2
Use the Overall Health menu bar for the following functionality:

<table>
<thead>
<tr>
<th>Overall Health Menu Bar</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
</tr>
<tr>
<td>Last 24 hours drop-down list</td>
</tr>
<tr>
<td>Actions</td>
</tr>
</tbody>
</table>

Step 3
Use the location pane for the following functionality:

<table>
<thead>
<tr>
<th>Location Pane</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
</tr>
<tr>
<td>❌ Show</td>
</tr>
</tbody>
</table>
### Location Pane

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Click this icon 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.</td>
</tr>
<tr>
<td><img src="image" alt="Network Health Map" /></td>
<td><strong>Network Health Map</strong>: Click this icon 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.</td>
</tr>
</tbody>
</table>

#### Step 4

Use the **Overall Health Summary** dashlet for the following functionality:

<table>
<thead>
<tr>
<th>Overall Health Summary Dashlet</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Network Devices</strong></td>
<td><strong>Network Score</strong>: Percentage of healthy (good) devices (routers, switches, wireless controllers, and access points) in your overall enterprise. See Network Health Score, on page 102. <strong>Device Category Health Score</strong>: Percentage of healthy (good) network devices for the following device categories: <strong>Router</strong>, <strong>Core</strong>, <strong>Distribution</strong>, <strong>Access</strong>, <strong>Controller</strong> and <strong>Access Point</strong>. <strong>Note</strong>: When a Fabric Domain is selected, this area provides percentage of healthy network devices for the following categories: <strong>Fabric Edge</strong>, <strong>Fabric Border</strong>, and <strong>Fabric Control Plane</strong>. Click View Network Health to open the Network Health dashboard. See Monitor and Troubleshoot the Health of Your Network, on page 85.</td>
</tr>
<tr>
<td></td>
<td><strong>Wired Clients</strong> and <strong>Wireless Clients</strong></td>
<td>Provides score distribution between wired and wireless clients. The <strong>Wired Client</strong> score or the <strong>Wireless Client</strong> score is the percentage of healthy (good) wired or wireless client devices in your overall enterprise. See Client Health Score, on page 122. Click View Client Health to open the Client Health dashboard. See Monitor and Troubleshoot the Health of All Client Devices, on page 107.</td>
</tr>
</tbody>
</table>

#### Step 5

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 200**.
Monitor and Troubleshoot Network Health

- About Network, on page 85
- Monitor and Troubleshoot the Health of Your Network, on page 85
- Monitor and Troubleshoot the Health of a Device, on page 90
- 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.

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 17.

Step 1
From the Cisco DNA Center home page, click the Assurance tab. The Overall Health dashboard appears.

Step 2
Choose Dashboards > Health > Network Health. The Network Health dashboard appears:
Step 3  
Use the **Network Health** timeline for the following functionality:

<table>
<thead>
<tr>
<th><strong>Network Health Timeline</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>24 Hours</strong> drop-down menu</td>
<td>Enables you to display information on the dashboard within a selected time range. Do the following:</td>
</tr>
<tr>
<td></td>
<td>a. From the <strong>24 Hours</strong> drop-down list, choose the length of the range: <strong>3 Hours</strong>, <strong>24 Hours</strong>, or <strong>7 Days</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. Specify the <strong>Start Date</strong> and time; and the <strong>End Date</strong> and time.</td>
</tr>
<tr>
<td></td>
<td>c. Click <strong>Apply</strong>.</td>
</tr>
<tr>
<td></td>
<td>This sets the range of the timeline.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **All Domains** | **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. |
| **Actions ** | 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 197 and Create a Custom Dashboard, on page 193. |
| **Timeline slider with healthy network device percentage** | 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.  
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](image.png) icon.  
**b.** In the tooltip, click the ![Edit](image.png) 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 4** Use the location pane for the following functionality:
### Location Pane

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show</td>
<td>Allows you to hide or display the location pane. By default the location pane is hidden.</td>
</tr>
<tr>
<td>Hide</td>
<td></td>
</tr>
</tbody>
</table>

**Hierarchical Site View and Building View**: Click this icon and use the drop-down list to view the percentage of healthy network devices in a table format for a site or building. Click **Apply** for a location to only display the location's client information in the **Network Health** 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.

**Network Topology**: Click this icon to display a topology view 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**.

**Network Health Map**: Click this icon 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.

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.

### Step 5

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

### Network Devices Health Summary Dashlet

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Devices Health Summary charts</td>
<td>There are two types of charts:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Latest</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Trend</strong>: Displays a trend chart. This trend chart shows the health of clients over a time period.</td>
</tr>
<tr>
<td></td>
<td>For the clients that failed to onboard, the breakdown of the reason for the onboarding failure is provided. For example, AAA, DHCP, Other, and so on.</td>
</tr>
<tr>
<td></td>
<td>The colors in the charts represent the health of the client devices.</td>
</tr>
<tr>
<td></td>
<td>• Red: Poor client devices. Health score range is 1 to 3.</td>
</tr>
<tr>
<td></td>
<td>• Orange: Fair client devices. Health score range is 4 to 7.</td>
</tr>
<tr>
<td></td>
<td>• Green: Good client devices. Health score range is 8 to 10.</td>
</tr>
<tr>
<td></td>
<td>• Gray: Inactive client devices. Health score is 0.</td>
</tr>
<tr>
<td>Network Health Summary Score</td>
<td>The Network Health Summary score is the percentage of healthy (good) devices in your overall network or selected site. See <strong>Network Health Score</strong>, on page 102.</td>
</tr>
</tbody>
</table>
Step 6

Use the **Top APs Up/Down**, **Top N APs by Client Count**, and **Top N APs with High Interference** 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.

There is a 15-minute snapshot view and a 24-hour trend view.

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.

There is a 15-minute snapshot view and a 24-hour trend view.

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 with High Interference Dashlet

Information about the APs that have high interference. You can choose 2.4 GHz or 5 GHz.

There is a 15-minute snapshot view and a 24-hour trend view.

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 **Network Devices** dashlet for the following functionality:

### Network Devices Dashlet

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEVICE</td>
<td>Filter the table with the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Monitored</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Unmonitored</strong>: Unmonitored devices are devices for which Assurance did not receive any telemetry data during the specified time range. Unmonitored devices are included in the Network Health Score computation. They are used as part of the total number of devices against which the health device percentage is calculated.</td>
</tr>
<tr>
<td>TYPE</td>
<td>Filter the table based on the device type with the following options: <strong>All</strong>, <strong>Access</strong>, <strong>Core</strong>, <strong>Distribution</strong>, <strong>Router</strong>, <strong>WLC</strong>, and <strong>AP</strong>.</td>
</tr>
</tbody>
</table>
Network Devices Dashlet

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVERALL HEALTH</td>
<td>Filter the table based on the overall health score of the device with the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>All</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Poor</strong>: Devices with a health score range from 1 to 3.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Fair</strong>: Devices with a health score range from 4 to 7.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Good</strong>: Devices with a health score range from 8 to 10.</td>
</tr>
</tbody>
</table>

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 Control Plane (reachability).

The Reachability column displays the status of the device (Reachable, Up, Unreachable, Rebooting, and so on).

View **Device 360** for a device

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.

Customize the data you want displayed in the table:

a. Click ![icon]

   A list of options is displayed.

b. Check the check boxes for the data you want displayed in the table.

c. Click **Apply**.

---

**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
From the Cisco DNA Center home page, click the Assurance tab. The Overall Health dashboard appears.

Step 2

Step 3
Do one of the following:

- In the Network Devices dashlet, click a device name in the Device 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.

Figure 12: Device 360 Window

Step 4
Click the 24 Hours drop-down menu to specify the time range of data you want displayed on the window:

a) From the 24 Hours 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. This sets the range of the timeline slider.

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 Monitor Intelligent Capture Details for an AP, on page 186.

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
You can view the device's health score which is displayed to the left of the device name.
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, 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** Uplink availability is based on infrastructure links.

- **Router**: The health score for routers 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 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 104.

- **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 105.

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 7** Use the **Device 360** header, which appears above 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.

**Step 8** Click **View Details** at the top-right corner to open a slide-in pane that displays additional attributes of a device, such as general information, network information, and rack location.

**Step 9** 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 10**

Use the collapsible categories to view information about issues, physical neighbor topology, path trace, application experience, and details:

<table>
<thead>
<tr>
<th>Issues Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays any issues that must be addressed. Issues are listed based on the timestamp. The most recent issue is listed first.</td>
</tr>
</tbody>
</table>

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 **Status** 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 **Status** 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.

For information about the types of issues, see View and Manage Issues, on page 199.

<table>
<thead>
<tr>
<th>Physical Neighbor Topology Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays a topology view of a specific device and shows how that device is connected to neighboring devices. You can do the following:</td>
</tr>
</tbody>
</table>

- 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.
### Event Viewer Category

- **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 second column provides additional information about the issue, such as the reason code. The third column provides the time stamp when the event occurred.

- **For switches and routers**: All syslogs that have severity of Error and above (Emergency, Alert, and Critical), events for any links that are up/down, and device reachability or non-reachability events are recorded in the event viewer. Only a selected list of syslogs less severe than Error level (Warning, Notice, and Info) are also displayed. For the list of selected syslog messages, see [Selected Syslogs Below Error Level, on page 96](#).

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 127](#).

### Application Experience Category

Applications running on a router 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 Cisco Application Experience, on page 129](#) and [View Application Experience of a Host, on page 131](#).

**Note** This category is displayed for routers only.
Detail Information Category

Depending on the type of device, historical KPIs performing over a period of time are displayed in appropriate charts under the following tabs:

• **DeviceInfo** tab: Device details, such as CPU, memory, uptime, and so on are displayed.

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

The following are the available charts:

• **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.

  **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: Radio channel width, utilization, interference, noise, air quality, and so on are displayed. This tab is available for APs and wireless clients.

• **Interfaces** tab: Table with interface information such as the name, description, operational status, link speed, and so on are displayed. The interface table columns are sortable.

  **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**, and **Error** charts are displayed below the table. You can choose a maximum of five interfaces. The first interface in the table is selected by default.

• **Fabric** tab: Fabric KPIs, such as reachability and uplink status charts are displayed. This tab is available for fabric domains only.

  **Note** The uplink status chart shows data only if the Fabric Underlay Automation is used to provision the fabric.
Selected Syslogs Below Error Level

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

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

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

Fabric Overview

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

The 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.

### Hardware Platform Events

<table>
<thead>
<tr>
<th>Event Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS-5-CONFIG_I</td>
<td>Configured with new configuration file</td>
</tr>
<tr>
<td>SYS-5-RELOAD</td>
<td>Reboot of the system</td>
</tr>
<tr>
<td>SYS-5-RESTART</td>
<td>System restart</td>
</tr>
<tr>
<td>OIR-6-INSCARD</td>
<td>Inservice card insertion</td>
</tr>
<tr>
<td>OIR-6-REMCARD</td>
<td>Removal of card</td>
</tr>
<tr>
<td>OIR-SP-6-INSCARD</td>
<td>Inservice port card insertion</td>
</tr>
<tr>
<td>OIR-SP-6-REMCARD</td>
<td>Removal of port card</td>
</tr>
<tr>
<td>PLATFORM_STACKPOWER-6-CABLE_EVENT</td>
<td>Cable event on the stackpower-6 module</td>
</tr>
<tr>
<td>PLATFORM_STACKPOWER-6-LINK_EVENT</td>
<td>Link event on the stackpower-6 module</td>
</tr>
<tr>
<td>PLATFORM_STACKPOWER-4-TOO_MANY_ERRORS</td>
<td>Too many errors on the stackpower-4 module</td>
</tr>
<tr>
<td>PLATFORM_STACKPOWER-4-VERSION_MISMATCH</td>
<td>Version mismatch on the stackpower-4 module</td>
</tr>
<tr>
<td>PLATFORM_STACKPOWER-4-UNDER_BUDGET</td>
<td>Under budget on the stackpower-4 module</td>
</tr>
<tr>
<td>PLATFORM_STACKPOWER-4-INSUFFICIENT_PWR</td>
<td>Insufficient power on the stackpower-4 module</td>
</tr>
<tr>
<td>PLATFORM_STACKPOWER-4-REDUNDANCY_LOSS</td>
<td>Redundancy loss on the stackpower-4 module</td>
</tr>
<tr>
<td>ILPOWER-5-POWER_GRANTED</td>
<td>Power granted to the system</td>
</tr>
<tr>
<td>ILPOWER-5-LINKDOWN_DISCONNECT</td>
<td>Link down disconnect</td>
</tr>
<tr>
<td>ILPOWER-5-IEEE_DISCONNECT</td>
<td>IEEE disconnect</td>
</tr>
<tr>
<td>ILPOWER-5-INVALID_IEEE_CLASS</td>
<td>Invalid IEEE class</td>
</tr>
<tr>
<td>ILPOWER-4-LOG_OVERDRAWN</td>
<td>Log overdrawn</td>
</tr>
<tr>
<td>ILPOWER-5-CLR_OVERDRAWN</td>
<td>Clear overdrawn</td>
</tr>
</tbody>
</table>
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.

Create a Fabric Domain

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the Cisco DNA Center home page, click <strong>Provision</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Click the <strong>Fabric</strong> tab.</td>
</tr>
<tr>
<td>3</td>
<td>Click the <strong>Add Fabric Domain or Transit</strong> tab.</td>
</tr>
<tr>
<td>4</td>
<td>Choose <strong>Add Fabric</strong> from the pop-up.</td>
</tr>
<tr>
<td>5</td>
<td>Enter a fabric name.</td>
</tr>
<tr>
<td>6</td>
<td>Choose one fabric site.</td>
</tr>
<tr>
<td>7</td>
<td>Click <strong>Add</strong>.</td>
</tr>
</tbody>
</table>

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.

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 play 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.

Note

Currently, Cisco Wireless Controller communicates only with two control plane nodes.

Before you begin

Provision the device. To provision a device, click the **Provision** tab and choose **Devices**. The topology displays a device in gray color if it has passed the fabric readiness checks and is ready to be provisioned.

If an error is detected during any of the fabric readiness checks, an error notification is displayed on the topology area. Click **See more details** to check the problem area listed in the resulting window. Correct the problem and click **Re-check** to ensure that the problem is resolved. If you update the device configuration as part of problem resolution, ensure that you resynchronize the device information by performing an **Inventory > Resync** for the device.
You can continue to provision a device that has failed the fabric readiness checks.

---

**Step 1**
From the Cisco DNA Center home page, 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. In the topology view, any device that is added to the fabric is shown in blue.

**Step 4**
Click a device; the device details window slides in with the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge Node</td>
<td>Click the toggle button next to this option to enable the selected device as an edge node.</td>
</tr>
<tr>
<td>Border Node</td>
<td>Click the toggle button next to this option to enable the selected device as a border node. For more information, see the <em>Add Device as a Border Node</em> section.</td>
</tr>
<tr>
<td>Control Plane</td>
<td>Click the toggle button next to this option to enable the selected device as a control plane node.</td>
</tr>
</tbody>
</table>
| Guest Border / Control Plane | Allows the following options:  
  • Control Plane: Check this check box if you want the device to act as a control plane.  
  • Border: Check this check box if you want the device to act as a border node.  
  • Select One Guest Virtual Network: All guest virtual networks created are listed. Check the check box of the guest virtual network and click **Enable**.  
  > **Note** Ensure that you have created a guest virtual network in the Policy application. |
| Rendezvous Point        | Click this toggle button to configure Rendezvous Point on device. For more information, see the *Add a Device as a Rendezvous Point* section. |

To configure a device as a fabric-in-a-box, select the **Control Plane**, **Border Node** and **Edge Node** options.
To configure the device as a control plane and a border node, select both **Control Plane** and **Border Node**.

**Step 5**
Click **Save**.

---

**What to do next**

Once 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**
From the Cisco DNA Center home page, click the gear icon 🛠, and then choose **System Settings > 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.
**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.

\[
\text{Device Health Score} = \text{MIN} (\text{System Health}, \text{Data Plane Connectivity}, \text{Control Plane Connectivity})
\]

Depending on the type of device, the metrics vary.

<table>
<thead>
<tr>
<th>System Health</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Type</strong></td>
</tr>
<tr>
<td>Switch (Access and Distribution)</td>
</tr>
</tbody>
</table>
| 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. |

<table>
<thead>
<tr>
<th>Data Plane Connectivity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Type</strong></td>
</tr>
<tr>
<td>Switch (Access and Distribution)</td>
</tr>
</tbody>
</table>
### Data Plane Connectivity

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Score Calculation</th>
<th>Details</th>
</tr>
</thead>
</table>
| **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, else 10. |
| **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, else 10. |
Router Health Score

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Score Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection to Control Plane Node—Fabric Devices Only (Edge and Border)</strong></td>
<td>- If the Control Plane node is reachable, the score is 10.</td>
</tr>
<tr>
<td></td>
<td>- If the Control Plane node is unreachable, the score is 1.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

AP Health Score

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Score Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU Utilization</strong></td>
<td>- If CPU utilization is 95 percent or less, the score is 10.</td>
</tr>
<tr>
<td></td>
<td>- If CPU utilization is more than 95 percent, the score is 1.</td>
</tr>
<tr>
<td><strong>Memory Utilization</strong></td>
<td>- If memory utilization is 95 percent or less, the score is 10.</td>
</tr>
<tr>
<td></td>
<td>- If memory utilization is more than 95 percent, the score is 1.</td>
</tr>
<tr>
<td><strong>WAN Connectivity</strong></td>
<td>- If the WAN connectivity is down, the score is 1.</td>
</tr>
<tr>
<td></td>
<td>- If the WAN connectivity is up, the score is 10.</td>
</tr>
<tr>
<td><strong>Link Errors</strong></td>
<td>Only infrastructure links are considered for link errors. Infrastructure links are topological links between network devices, such as switches, routers, wireless controllers, and APs.</td>
</tr>
<tr>
<td></td>
<td>If a physical infrastructure interface has errors, the score is 8, if all links are down, it is 1, else 10.</td>
</tr>
</tbody>
</table>
### Wireless Controller Health Score

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Score Calculation</th>
</tr>
</thead>
</table>
| **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 0. |
| **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. |
| **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. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Score Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Utilization</td>
<td>• If memory utilization is less than 90 percent, the score is 10.</td>
</tr>
<tr>
<td></td>
<td>• If the available memory is 90 percent or more, the score is 1.</td>
</tr>
<tr>
<td>Free Timer Score</td>
<td>• If the number of free timers is 20 percent or more, the score is 10.</td>
</tr>
<tr>
<td></td>
<td>• If the number of free timers is 20 percent or less, the score is 1.</td>
</tr>
<tr>
<td>Free Memory Buffers (MBufs)</td>
<td>• If the number of free memory buffer is 20 percent or more, the score is 10.</td>
</tr>
<tr>
<td></td>
<td>• If the number of free memory buffer is less than 20 percent, the score is 1.</td>
</tr>
<tr>
<td>Work Queue Element (WQE) Pool Score</td>
<td>• If the wqe pool is greater than wqe pool threshold, the score is 10.</td>
</tr>
<tr>
<td></td>
<td>• If the wqe pool is at the same level as or lower than the wqe pool threshold, the score is 1.</td>
</tr>
<tr>
<td>Packet Pools</td>
<td>• If the packet pool is greater than the packet pool threshold, the score is 10.</td>
</tr>
<tr>
<td></td>
<td>• If the packet pool is at the same level as or lower than the packet pool threshold, the score is 1.</td>
</tr>
<tr>
<td>Link Errors</td>
<td>• If link errors are less than 1 percent, the score is 10.</td>
</tr>
<tr>
<td></td>
<td>• If link errors are 1 percent or more, the score is 1.</td>
</tr>
<tr>
<td>Connection to Control Plane Node—Fabric Wireless Controllers Only</td>
<td>• If the Control Plane node is reachable, the score is good.</td>
</tr>
<tr>
<td></td>
<td>• If the Control Plane node is unreachable, the score is poor.</td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
</tr>
</tbody>
</table>
CHAPTER 7

Monitor and Troubleshoot Client Health

• About Clients, on page 107
• Monitor and Troubleshoot the Health of All Client Devices, on page 107
• Monitor and Troubleshoot the Health of a Client Device, on page 117
• Understand Client Health Score and KPI Metrics, on page 121

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

Use this procedure to get a global view of the health of all the wired and wireless client devices 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.

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.

Before you begin

Configure Assurance. See Basic Setup Workflow, on page 17.

Step 1

From the Cisco DNA Center home page, click the Assurance tab.
The Overall Health dashboard appears.

Step 2

Choose Dashboards > Health > Client Health.
The Client Health dashboard appears.
### Step 3

Use the **Client Health** timeline for the following functionality:

<table>
<thead>
<tr>
<th><strong>Client Health Timeline</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| **24 Hours** drop-down menu | Enables you to display information on the dashboard within a selected time range. Do the following:  
  a. From the **24 Hours** 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**.  
  This sets the range of the timeline. |
| **Filter**                | 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**               | 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 197 and **Create a Custom Dashboard**, on page 193. |
### Client Health Timeline

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Timeline Slider with Healthy Client Percentage | Enables you 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. 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 icon.  
   b. In the tooltip, click the 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 4  Use the location pane for the following functionality:

**Location Pane**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☰ Show</td>
<td>Allows you to hide or display the location pane. By default the location pane is hidden.</td>
</tr>
<tr>
<td>☰ Hide</td>
<td></td>
</tr>
</tbody>
</table>

**Hierarchical Site View and Building View**: Click this icon 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.

**Network Health Map**: Click this icon 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.

### Step 5  Use the **Client Health Summary** dashlet for the following functionality:
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**: Displays a trend chart. This trend chart shows the health of clients over a time period.

For the clients that failed to onboard, the breakdown of the reason for the onboarding failure is provided. For example, AAA, DHCP, Other, and so on.

The colors 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.

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 122.

**TOTAL**: Count of Active, Inactive, and New client devices.

**Note** New clients are clients that attempted to onboard after the 5-minute health score calculation window started. The health score for these clients will be included in the next 5-minute calculation window.

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Client Onboarding Times chart | Distribution of all the client's 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.  
    **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 breakdown of the reason for the onboarding failure is provided. For example, AAA, DHCP, Other, and so on. |

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, AAA, and DHCP data.  
      **Note** Failure Baseline data is available only for the Global Site.  
- 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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connectivity RSSI chart</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connectivity SNR chart</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Roaming Times chart</strong></td>
<td>Distribution of the clients by roaming times and failures. This dashlet provides the percentage of clients with roaming times less than 3000 ms.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.  
  **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.  
• Hover and move your cursor over the charts to view synchronized tooltips that display information at a selected point in time.  
  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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity Physical Link chart</td>
<td>Distribution of wired client device link state—the number of client devices that had their physical links up, down, and had errors.</td>
</tr>
</tbody>
</table>

| 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. |
Monitor and Troubleshoot Client Health

Client Count per Band Dashlet

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Count per Band chart</td>
<td>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 specific band.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Data Rate chart</td>
<td>Distribution of the client's data rates. Use the Client Protocol drop-down list to filter for clients based on what client protocol they are using. Options are 802.11n/ac/ax and 802.11a/b/g.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TYPE</td>
<td>Filter the table based on client type: Options are Wired and Wireless clients.</td>
</tr>
<tr>
<td>HEALTH</td>
<td>Filter the table based on the client health with the following options:</td>
</tr>
<tr>
<td></td>
<td>• All</td>
</tr>
<tr>
<td></td>
<td>• Inactive: Client devices with a health score of 0.</td>
</tr>
<tr>
<td></td>
<td>• Poor: Client devices with a health score range from 1 to 3.</td>
</tr>
<tr>
<td></td>
<td>• Fair: Client devices with a health score range from 4 to 7.</td>
</tr>
<tr>
<td></td>
<td>• Good: Client devices with a health score range from 8 to 10.</td>
</tr>
<tr>
<td></td>
<td>• No Data: Client devices with no data.</td>
</tr>
</tbody>
</table>
## Client Devices Dashlet

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATA</td>
<td>Filter the table based on data type with the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Onboarding Time &gt;= 10 s:</strong> Onboarding time is greater than or equal to the 10-seconds threshold value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Association &gt;= 5 s:</strong> Association time is greater than or equal to the 5-seconds threshold value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCP &gt;= 5 s:</strong> DHCP time is greater than or equal to the 5-seconds threshold value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Authentication &gt;= 5 s:</strong> Authentication time is greater or equal to 5-seconds.</td>
</tr>
<tr>
<td></td>
<td>• <strong>RSSI &lt;= -72 dBm:</strong> RSSI is less than or equal to the -72 dBm threshold value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SNR &lt;= 9 dB:</strong> SNR is less than or equal to the 9 dB threshold value.</td>
</tr>
</tbody>
</table>
### Client Devices Dashlet

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Device</strong></td>
<td>View detailed client device information in a table format. The client device table displays the following information by default:</td>
</tr>
<tr>
<td><strong>table</strong></td>
<td>• <strong>Identifier</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>The Identifier column also has specific icons that allow you to determine if the client device is wired or wireless.</td>
</tr>
<tr>
<td><strong>IPv4 Address</strong></td>
<td>Displays the client's IPv4 address based on availability.</td>
</tr>
<tr>
<td><strong>Device Type</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Health</strong></td>
<td>This score is the average of the onboarding and connected scores. The Client Health score is calculated every 5 minutes.</td>
</tr>
<tr>
<td><strong>Last Seen</strong></td>
<td>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 will be included in the next 5-minute calculation window.</td>
</tr>
<tr>
<td><strong>AP Name</strong></td>
<td>(for wireless clients only): This is the name of the access point.</td>
</tr>
<tr>
<td><strong>Switch</strong></td>
<td>(for wired clients only)</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>(for wired clients only)</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Displays the assigned location of the client.</td>
</tr>
<tr>
<td><strong>Link Speed</strong></td>
<td>(for wired clients only): Indicates the speed capacity of the interface or physical port. If the port has negotiated to a certain speed then that negotiated speed is displayed.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You can display the link speed by checking the <strong>Link Speed</strong> check box in the menu.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| ☰ Customizable Data | 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. |
| Export | 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.

**Step 1**  
From the Cisco DNA Center home page, click the **Assurance** tab.  
The **Overall Health** dashboard appears.

**Step 2**  
Choose **Dashboards > Health > Client Health**.  
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 appears which displays a 360° view of the client device.
Monitor and Troubleshoot Client Health

Step 4
Click the 24 Hours drop-down menu to specify the time range of data you want displayed on the window:

a) From the 24 Hours 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**.

This sets the range of the timeline slider.

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 Monitor Intelligent Capture Details for a Client, on page 180.

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
You can view the individual client health score which is displayed to the left of the client name.

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 123.

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 7 Use the Client 360 header, which appears above the timeline, to view the most current information about the device:

- For wireless clients, this area provides information about the client device such as its OS version, MAC address, IPv4 and IPv6 address, 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, VLAN ID, connection status, last seen timestamp, connected network device, port, and last known location.

Step 8 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 9 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 **Status** 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 **Status** 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.

For information about the types of issues, see View and Manage Issues, on page 199.

---

**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

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:

- 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

When an issue occurs, that event is marked red; otherwise, it is green. The second column provides additional information about the failure, such as the error message, and the AP and wireless controller to which the client device is connected. The third column provides the time stamp 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 127.

Application Experience Category

Applications running on a client device with their qualitative and quantitative metrics.

To view the metrics in a chart format, select the radio button next to an application in the table. A slide-in pane opens with the relevant information.

See About Cisco Application Experience, on page 129 and View Application Experience of a Host, on page 131.

Detail Information Category

Contains the following tabs: Device Info, RF (only wireless clients), and Connectivity. Click each tab to get the appropriate information.

Note For Apple devices, an iOS Analytics tab is provided.

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 is unable to connect to the network, 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 0 to 4. When the client connects to the network successfully, the score is 4. If the client is unable to connect to the network, the score is 0.

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

<table>
<thead>
<tr>
<th>Client's RSSI</th>
<th>RSSI-Driven Connectivity Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>If RSSI is less than or equal -72 dBm.</td>
<td>The client receives a RSSI-driven connectivity score of 4 and is considered to be in fair health.</td>
</tr>
<tr>
<td>If RSSI is greater to -72 dBm.</td>
<td>The client receives a RSSI-driven connectivity score of 10 and is considered to be in good health.</td>
</tr>
</tbody>
</table>

SNR-Driven Connectivity Score

<table>
<thead>
<tr>
<th>Client's SNR</th>
<th>SNR-Driven Connectivity Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>If SNR is less than or equal to 9.</td>
<td>The client receives a SNR-driven connectivity score of 4 and is considered to be in fair health.</td>
</tr>
<tr>
<td>If SNR is greater than 9.</td>
<td>The client receives a SNR-driven connectivity score of 10 and is considered to be in good health.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Client's Onboarding and Connectivity</th>
<th>Resulting Client Health Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the client failed onboarding.</td>
<td>The client receives a health score of 1 and is considered to be in poor health.</td>
</tr>
<tr>
<td>If the client's RSSI and SNR are below threshold.</td>
<td>The client receives a health score of 4 and is considered to be in fair health.</td>
</tr>
<tr>
<td>If either the client's RSSI or SNR is below threshold.</td>
<td>The client receives a health score of 7 and is considered to be in fair health.</td>
</tr>
<tr>
<td>If the client's RSSI and SNR is above threshold.</td>
<td>The client receives a health score of 10 and is considered to be in good health.</td>
</tr>
</tbody>
</table>
Individual Client Health Score
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 non-fabric 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 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. This is 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 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 IPv6 addresses is not supported.

Path trace for Cisco Mobility Express (ME) wireless controllers is not supported.

Path trace for wireless clients that use OTT in SDA Fabric 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.

Because Cisco wireless controllers do not send SNMP mobility traps, note the following:

- For a path trace request, Cisco DNA Center will 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.
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 125.

• 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 27, Discover Your Network Using CDP, on page 22, or Discover Your Network Using LLDP, on page 31.

• 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 Setup 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source field</td>
<td>The IP address in the Source field is prepopulated; however, you can enter another source IP address by doing the following:</td>
</tr>
<tr>
<td></td>
<td>• Enter the source IP address.</td>
</tr>
<tr>
<td></td>
<td>• Click the Source field, and then choose an IP address from the available options.</td>
</tr>
<tr>
<td>Interface (optional) field</td>
<td>Choose an interface from the drop-down list.</td>
</tr>
<tr>
<td>Note</td>
<td>This field is displayed if the source IP address is a network device.</td>
</tr>
<tr>
<td>Port (optional) field</td>
<td>Enter the port number of the host from which you want the trace to start.</td>
</tr>
<tr>
<td>Destination field</td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Enter the IP address of the host or the Layer 3 forwarding interface at which you want the trace to end.</td>
</tr>
<tr>
<td></td>
<td>• Click the Destination field, and then choose an IP address from the available options.</td>
</tr>
<tr>
<td>Interface (optional) field</td>
<td>Choose the interface from the drop-down list.</td>
</tr>
<tr>
<td>Note</td>
<td>This field is displayed if the IP address you choose in the Destination field is a network device.</td>
</tr>
</tbody>
</table>
**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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protocol</strong> drop-down list</td>
<td>(Optional) Choose either <strong>tcp</strong> or <strong>udp</strong>.</td>
</tr>
<tr>
<td><strong>Refresh Every 30sec</strong></td>
<td>(Optional) Set this toggle to <strong>On</strong> to configure the path trace topology to refresh every 30 seconds.</td>
</tr>
<tr>
<td><strong>ACL Trace</strong></td>
<td>(Optional) Set this toggle to <strong>On</strong> to display matched ACLs and the ACL result (Permit or Deny) for a specific traffic flow.</td>
</tr>
<tr>
<td><strong>Include Stats</strong> options</td>
<td>(Optional) To configure the path trace to collect additional statistics, check the following check boxes as needed:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Device</strong>: Collects and displays information, such as the device CPU and memory usage.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Interface</strong>: Collects and displays information about the device interface.</td>
</tr>
<tr>
<td></td>
<td>• <strong>QoS</strong>: Collects and displays QoS information, such as collector-voice-egress, collector-broadcast-video-egress, collector-real-time-interactive-egress, and so on.</td>
</tr>
</tbody>
</table>

**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 Egress ACLs, the icon appears on the right side of the device.

b) Click a device to open a slide-in pane with additional device details.  
c) Hover your cursor over a Layer 2 or Layer 3 port channel interface to display information, such as used VLANs and output drops. Click **More Details** to open a slide-in pane with additional information.  
d) Hover your cursor over the path to display the protocol of the devices along the path (**Switched, STP, ECMP, Routed, Trace Route**) or other source type.
Monitor Application Health

- About Cisco Application Experience, on page 129
- Enable Application Visibility, on page 129
- Configure Telemetry, on page 130
- View Application Experience of a Host, on page 131
- View Application Experience of a Network Device, on page 132
- Monitor the Health of All Applications, on page 133
- Monitor the Health of an Application, on page 137
- Understand Application Health Score and KPI Metrics, on page 139

About Cisco Application Experience

Cisco Application Experience (AX) allows you to monitor the health of an application. Application health is measured using a score value, which is calculated based on the application's qualitative metrics—packet loss, network latency, and jitter.

AX is based on the Application Visibility records exported by routers, switches, and WLCs. Only application performance profiles that include application client-server stats, application response time and media type monitors are supported.

Based on the relevancy of an application, it is classified as Business Relevant, Business Irrelevant, or Default. This classification is done based on the NBAR standard. See "Business-Relevance Groups" in the Cisco Digital Network Architecture Center User Guide.

To view AX, you must enable Application Visibility on the Cisco network device. See Enable Application Visibility, on page 129.

Note

Cisco DNA Center supports configuring Application Visibility on routers, switches, and WLCs. You can view this identification in the Cisco DNA Center Inventory window under Device Role.

Enable Application Visibility

To view the applications running on a network device with their qualitative and quantitative metrics, you must enable Application Visibility on the device. Do the following:
1. Add a description on device interface(s) containing the keyword _lan_. This can be either configured on the device interface manually or by using the **Template Editor** tool in Cisco DNA Center.

2. Resynchronize the network device to read this interface description. The **Network Telemetry** tool looks for interfaces with _lan_ in the description and applies the Application Visibility configuration to only those interfaces.

3. Configure an IP address on the interface. This interface must not be used for management purposes.

4. Apply the **Maximal Visibility** profile to network devices. See **Apply a Telemetry Profile to the Devices**, on page 130.

---

**Note**

Application Visibility is applied only to interfaces that have the description _lan_, have an IP address, and are non-management interfaces.

---

Application visibility is supported on the following network devices:

- Routers with the minimum software version of Cisco IOS XE Denali Release 16.3.1
- Cisco Catalyst 9K Switches with the minimum software version of Cisco IOS XE Everest 16.6.1
- Cisco AireOS WLCs with the minimum software version of AireOS 8.8.120.0

---

**Important**

AireOS 8.9.x does not support application visibility.

---

**Note**

For Cisco AireOS WLCs, its SSID profile name should have keyword _lan_ to enable Application Visibility.

---

**Configure Telemetry**

**About Telemetry**

The Telemetry tool allows you to configure and apply profiles on devices for monitoring and assessing their health.

**Apply a Telemetry Profile to the Devices**

You can apply telemetry assessment profiles to your network devices using the Telemetry tool.

**Before you begin**

Perform the following preliminary tasks:

- Discover the devices in your network using Cisco DNA Center.
• Review and configure the available telemetry profiles using the Telemetry Profile View options and fields.

Step 1  From the Cisco DNA Center home page, click Network Telemetry in Tools.
The Telemetry window appears.

Step 2  Click the Site View tab.

Step 3  Review the Site View table in this tab.
The following information is displayed:
  • Device Name: Name of the device.
  • Address: IP address of the device.
  • Type: Type of device.
  • Family: Device category; for example, switch, router, access point.
  • Version: Software version currently running on the device.
  • Profile: Applied telemetry profile on the device.
  • Details: Telemetry assessment of the device.

Step 4  Check the check box next to the Device Name of a device to add a telemetry profile to that device.

Step 5  Click the Actions button and select a telemetry profile from the drop-down list.
To view Application Experience, you must select the Maximal Visibility profile for the device.

Step 6  From the Show drop-down menu, select the telemetry profile you just applied.
The device should appear in the filtered list, along with any other devices that have also been configured with the same telemetry profile.

What to do next
Cisco DNA Center uses the telemetry profiles configured in this procedure to determine what data types to capture. These data types are then used in monitoring the health of the network devices.
Access Cisco DNA Assurance and review both Assurance Health and Assurance Issues to check the health of your network devices.

View Application Experience of a Host
Use this procedure to view the qualitative and quantitative metrics of the applications running on a host.
View Application Experience of 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 27, Discover Your Network Using CDP, on page 22, or Discover Your Network Using LLDP, on page 31.
- Enable Application Visibility on the network device. See Enable Application Visibility, on page 129.

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 and latency.
   - **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.
   - **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 Experience data exported by a Cisco Catalyst 9K switch or Cisco AireOS WLC only provides data for the 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. Application Experience is supported on routers, Cisco Catalyst 9K Switches, and Cisco AireOS WLCs.
Monitor Application Health

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 27, Discover Your Network Using CDP, on page 22, or Discover Your Network Using LLDP, on page 31.

• Enable Application Visibility on the network device. See Enable Application Visibility, on page 129.

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. 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 Device 360 window. Options are: 3 Hours, 24 Hours, and 7 Days. Default is 24 Hours.

b) Filter the Application Experience data for a specific VRF or a specific router interface by using the appropriate filters. The filters are 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 and latency.

• 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.

• 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, and Application Server Latency.

Note Application Experience data exported by a Cisco Catalyst 9K switch or Cisco AireOS WLC only provides data for the 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 27, Discover Your Network Using CDP, on page 22, or Discover Your Network Using LLDP, on page 31.
- Enable Application Visibility collection on the device. See Enable Application Visibility, on page 129.

**Step 1**

From the Cisco DNA Center home page, click the **Assurance** tab.

The **Overall Health** dashboard appears.

**Step 2**

Choose **Dashboards > Health > Application Health**.

The **Application Health** dashboard appears.

**Step 3**

Use **Application Health Timeline** for the following functionality:

<table>
<thead>
<tr>
<th>Application Health Timeline</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| 24 Hours drop-down menu | Enables you to display application information on the dashboard within a selected time range. Do the following:  
  a. From the 24 Hours: drop-down list, 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**.  
  This sets the range of the timeline. |
| Actions | 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 197 and Create a Custom Dashboard, on page 193. |
| 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. |

**Step 4**

Use the location pane for the following functionality:

<table>
<thead>
<tr>
<th>Location Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>✗ Show</td>
<td>Allows you to hide or display the location pane. By default the location pane is hidden.</td>
</tr>
<tr>
<td>Location Pane</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td></td>
</tr>
<tr>
<td><strong>Item</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td></td>
<td>Click this icon to display the <strong>Site List View</strong>. To view the application information from a specific site or building, click <strong>Apply</strong> in the appropriate row. The information is refreshed in the dashboard based on your selection.</td>
</tr>
</tbody>
</table>

**Step 5**

Use the **Application Health Summary** dashlet for the following functionality:

<table>
<thead>
<tr>
<th>Application Health Summary Dashlet</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
</tr>
<tr>
<td><strong>Business Relevant Application Health</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Application Usage</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Step 6**

Use the **Application** dashlet for the following functionality:
**Application Dashlet**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TYPE</strong></td>
<td>Filter the table based on the business-relevance groups: Options are <strong>Business Relevant</strong>, <strong>Business Irrelevant</strong>, and <strong>Default</strong>.</td>
</tr>
</tbody>
</table>
| **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 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 137.

- **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.
Monitor Application Health

### Application Dashlet

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Customize](image) | Customize the data you want displayed in the table:  
   a. Click ![Customize](image).  
      A list of options appears.  
   b. Check the check boxes for the data you want displayed in the table.  
   c. Click Apply. |
| ![Export](image) | 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**  
From the Cisco DNA Center home page, click the Assurance tab.  
The Overall Health dashboard appears.

**Step 2**  
Choose Dashboards > Health > Application Health.  
The Application Health window 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**  
For the health timeline, you can do the following:

<table>
<thead>
<tr>
<th>Application 360 Health Timeline</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![24 Hours](image) drop-down menu | Enables you to display application information on the dashboard within a selected time range. Do the following:  
   a. From the 24 Hours: drop-down list, 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:  
      This sets the range of the timeline. |
### Application 360 Health Timeline

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Location</strong> filter</td>
<td>Displays the application information for the location you choose from the drop-down list.</td>
</tr>
<tr>
<td><strong>Business Relevance</strong> field</td>
<td>Displays the application's Next Generation Network-Based Application Recognition (NBAR) classifying information.</td>
</tr>
<tr>
<td><strong>Traffic Class</strong> field</td>
<td></td>
</tr>
<tr>
<td><strong>Category</strong> field</td>
<td></td>
</tr>
<tr>
<td><strong>Application Health Timeline</strong> Slider</td>
<td>Enables you to view the application's health score for a more granular time range. Hover your cursor within the timeline to view the health score 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 window.</td>
</tr>
</tbody>
</table>

### Step 5

You can view information about issues from the **Issues** category:

a) Click an issue to open a slide-in pane to view the corresponding details, such as description of the issue, impact, and suggested actions.

b) From the slide-in pane, you can do the following:

   • To resolve an issue:
     a. From the **Status** 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 **Status** drop-down list, choose **Ignore**.
     b. Set the number of hours to ignore the issue on the slider.
     c. Click **Confirm**.

For information about issues, see [View and Manage Issues, on page 199](#).

### Step 6

You can view Application Experience data from the **Application Experience** category:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source Location</strong></td>
<td>The client site that's accessing the particular application.</td>
</tr>
<tr>
<td></td>
<td>Click the radio button for a network device to open a slide-in pane with additional details. From the slide-in pane you can:</td>
</tr>
<tr>
<td></td>
<td>• View charts for each metric: Throughput, packet loss, jitter, network latency, client network latency, server network latency, and application network latency.</td>
</tr>
<tr>
<td></td>
<td>• View the clients that are accessing the application. Details about each of the client is shown such as the client health score, MAC address, IP address, and usage.</td>
</tr>
</tbody>
</table>
## 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.

<table>
<thead>
<tr>
<th>Application Experience Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Column</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| Health                          | The health score is calculated on the basis of a combination of metrics of packet loss and latency.  
**Note** This metric is not available for Cisco Catalyst 9K Switches and Cisco AireOS WLCs. |
| Usage                           | The number of bytes transferred by the client for the particular application. |
| DSCP                            |  
• **Observed**: The application's current DSCP value.  
• **Expected**: The default DSCP value assigned by NBAR. |
| Packet Loss (%)                 | The percentage (maximum and average) of packet loss.  
**Note** This metric is not available for Cisco Catalyst 9K Switches and Cisco AireOS WLCs. |
| Network Latency                 | The network latency time (maximum and average) in milliseconds.  
**Note** This metric is not available for Cisco Catalyst 9K Switches and Cisco AireOS WLCs. |
| Jitter                          | The variance in time delay in milliseconds (maximum and average) between data packets over your network.  
**Note** This metric is not available for Cisco Catalyst 9K Switches and Cisco AireOS WLCs. |

### Step 7
(Optional) Customize the data you want displayed in the table:

a) Click ![Options](image).  
A list of options appears.
b) Check the check boxes for the data you want displayed in the table.
c) Click **Apply**.

### Step 8
(Optional) Export the table data to a CSV file by clicking ![Export](image).

**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.
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)

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 10

Manage Sensors and Sensor-Driven Tests

- About Sensors and Sensor-Driven Tests, on page 141
- View and Manage Sensors in Your Network, on page 142
- Manage Backhaul Settings, on page 143
- View Sensor-Driven Tests, on page 144
- Add a Sensor-Driven Test, on page 146
- Monitor and Troubleshoot the Health of Wireless Sensors, on page 150
- Provision the Wireless Cisco Aironet 1800s Active Sensor, on page 154
- Enable Provisioning SSID on the Wireless Controller, on page 155
- Enable Cisco Provisioning SSID on the Cisco Catalyst Wireless Controller, on page 155
- Provision a Wireless or Sensor Device, on page 156
- Error Messages for Sensor-Driven Test Failures, on page 159

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.

Supported Sensor and Cisco Wireless Controller Software Releases

The sensor functionality requires the following minimum software versions of Cisco Wireless Controllers and Cisco Aironet 1800s Active Sensor images:

<table>
<thead>
<tr>
<th>Supported Sensor and Wireless Controllers</th>
<th>Minimum Software Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Wireless Controller (35xx, 55xx, 85xx)</td>
<td>Software Release 8.5.115.0</td>
</tr>
</tbody>
</table>
### Supported Sensor and Wireless Controllers

<table>
<thead>
<tr>
<th>Supported Sensor and Wireless Controllers</th>
<th>Minimum Software Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Aironet 1800s Active Sensor</td>
<td>Software Release 8.7.258.0</td>
</tr>
</tbody>
</table>

For the following 1.2.10 features, the minimum software is Software Release 8.8.260.x and later:

- Active RF scanning
- Test result error messages
- Hidden SSID support
- Scheduling onboarding only test

**Note**  You can upgrade the Cisco Aironet 1800s Active Sensor with the SWIM App.

### View and 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**  From the Cisco DNA Center home page, click the Assurance tab.

The Overall Health dashboard appears.

**Step 2**  Choose Manage > Sensors > Sensor List.

The Sensor List window appears which displays the onboarded sensors in your network.

**Step 3**  Use the left pane to specify the network hierarchy you want to view.

**Step 4**  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 5**  You can customize the data that is 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 6**  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 7** 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 8** Click Save.

**Step 9** To change the name 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 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.

---

**Manage Backhaul Settings**

Use this procedure to view, create, and manage backhaul configurations for sensors. A sensor requires a backhaul SSID to communicate with Cisco DNA Center.

**Step 1** From the Cisco DNA Center home page, click the Assurance tab. The Overall Health dashboard appears.

**Step 2** Choose Manage > Sensors > Backhaul Settings. 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.
b) In the Create Sensor Backhaul SSID Assignment window, configure the following settings:
   - **Settings Name**: Enter a name for the backhaul SSID.
   - **Wireless Network Name (SSID)**: Select the wireless network (SSID) to use for this backhaul SSID.
   - **Level of Security**: Displays the encryption and authentication type used by the selected SSID. The available security options are:
**Security Option** | **Description**  
--- | ---  
WPA2 Enterprise | Uses Extensible Authentication Protocol (EAP) security for user authentication. Select the EAP method from the drop-down list. If you select EAP-TLS, a certificate and its password is required. You can upload a certificate by clicking the Certificate drop-down menu and then clicking ![Add New Certificate Bundle](image).  
WPA2 Personal | Uses a WP2A encrypted pre-shared key (PSK) for user authentication. Enter the desired PSK in the Password field.  
Open | No security or authentication is used.  

c) Click Save.

**Step 4** You can edit 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 chose Delete.

---

**View Sensor-Driven Tests**

Use this procedure to view all the sensor-driven tests that are configured in Cisco DNA Center and the test results.

**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 154.

**Step 1** From the Cisco DNA Center home page, click the Assurance tab. The Overall Health dashboard appears.

**Step 2** Choose Manage > Sensors > Test Suites. The Test Suites window appears.
The existing sensor-driven tests and its details are displayed in a table format.

**Step 3** Use the **Test Results** column to see information about sensor-driven test results. You can do the following:

a) From the **Last 24 hours** column, view the colorized representation of the test results from the last 24 hours. The colors indicate the following:

<table>
<thead>
<tr>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢</td>
<td>The test passed.</td>
</tr>
<tr>
<td>⚫</td>
<td>The test failed.</td>
</tr>
<tr>
<td>⚪</td>
<td>The test succeeded though the completion time was above the threshold.</td>
</tr>
<tr>
<td>⬤</td>
<td>The test information is not available.</td>
</tr>
</tbody>
</table>

The thresholds for test times are as follows:

<table>
<thead>
<tr>
<th>Test Type</th>
<th>Threshold Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Onboarding</td>
<td>10 sec</td>
</tr>
<tr>
<td>IP addressing</td>
<td>5 sec</td>
</tr>
<tr>
<td>For all other test types</td>
<td>2 sec</td>
</tr>
</tbody>
</table>

b) From the **Last 24 hours** column, you can hover your cursor over the bars to view the number of test results that failed, were slow, or passed within a test interval time frame.

c) From the **Details** column, you can click **Latest** to open a slide-in pane to view sensor details and its test results.
Step 4  To edit or delete a sensor-driven test, hover your cursor over ✔️ from the Actions column. A menu displays with options to edit or delete the test.

Add a Sensor-Driven Test

Use the Add Test wizard to add and schedule a new sensor-driven test, select the tests to run, and then select APs to run as sensors. After you select an AP to run as a sensor, that sensor acts as a client and tests the health of the wireless clients, such as AP radios, WLAN configurations, and network services.

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 154.

Step 1  From the Cisco DNA Center home page, click the Assurance tab. The Overall Health dashboard appears.

Step 2  Choose Manage > Sensors > Test Suites. The Test Suites window appears.

Step 3  To add a new sensor, click ➕ Add Test at the top-right corner. The Add Test window appears.

Figure 17: Add Test Window
For the **Schedule Tests** step, configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Name field</td>
<td>Enter the name for the test suite. Note: Use only letters, numbers, underscores, hyphens, and periods.</td>
</tr>
<tr>
<td>Location drop-down list</td>
<td>Do the following:</td>
</tr>
<tr>
<td></td>
<td>a. Choose the sensor location from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>b. Check the check boxes of the radios from the SSID you want to add to the test.</td>
</tr>
<tr>
<td></td>
<td>c. If applicable, configure the <strong>Credentials</strong> settings:</td>
</tr>
<tr>
<td></td>
<td><strong>Applicable for WebAuth Enabled SSIDs</strong></td>
</tr>
<tr>
<td></td>
<td>For Layer 3 security, if WebAuth is enabled on the SSID, provide the following:</td>
</tr>
<tr>
<td></td>
<td>• For WebAuth with user authentication, provide the necessary credentials.</td>
</tr>
<tr>
<td></td>
<td>• For WebAuth with Passthrough, you can choose to provide an email address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>• Only <strong>Internal Authentication</strong> is supported for sensor testing.</td>
</tr>
<tr>
<td></td>
<td>• WebAuth is supported on Cisco Wireless Controllers and Cisco Aironet 1800s Active Sensors with Software Release 8.7.</td>
</tr>
<tr>
<td></td>
<td><strong>Applicable for WPA2 Enterprise Enabled SSIDs</strong></td>
</tr>
<tr>
<td></td>
<td>The supported methods are <strong>EAP-FAST</strong>, <strong>PEAP-MSCHAPv2</strong>, and <strong>EAP-TLS</strong>.</td>
</tr>
<tr>
<td></td>
<td>If you select EAP-TLS, a certificate and its password is required. You can upload a certificate by clicking the <strong>Certificate</strong> drop-down menu and then clicking <strong>Add New Certificate Bundle</strong>.</td>
</tr>
<tr>
<td>Interval drop-down menu</td>
<td>Specify the schedule for the sensor test. Options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Daily</strong>: The sensor test occurs on an ongoing recurring interval. The default interval is every hour.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Once</strong>: The sensor test occurs one time at a specified date and time.</td>
</tr>
</tbody>
</table>

**Step 5**  
Click **Next** to continue to the **Select Tests** step.

**Step 6**  
For the **Select Tests** step, configure the following settings:

a)  
Check the check boxes for the **Network Tests** that you want to run, and then enter the required information for those tests:
### Networking Tests

<table>
<thead>
<tr>
<th>Test Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Onboarding Tests</strong></td>
<td>Performs a client onboarding test that typically involves association, AAA, and DHCP.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>• This option is selected by default and cannot be unselected.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Onboarding Tests</strong> is supported on Cisco Aironet 1800s Active Sensors with Software Release 8.8.260.0 and later.</td>
</tr>
<tr>
<td><strong>DNS Tests</strong></td>
<td>Resolves IP address for the domain name.</td>
</tr>
<tr>
<td><strong>Host Reachability Tests</strong></td>
<td>Verifies reachability using the Internet Control Message Protocol (ICMP) echo request.</td>
</tr>
<tr>
<td><strong>RADIUS Tests</strong></td>
<td>The sensor acts as a Dot1x supplicant and authenticates through wireless. Dot1x supplicant supports protocols such as Protected Extensible Authentication Protocol (PEAP) with Password Authentication Protocol (PAP) or the Microsoft version of the Challenge-Handshake Authentication Protocol (MS-CHAP).</td>
</tr>
</tbody>
</table>

b) Check the check boxes for the **Performance Tests** that you want to run, and then enter the required information for those tests:

### Performance Tests

<table>
<thead>
<tr>
<th>Test Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Speed Test</strong></td>
<td>If you have an 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.</td>
</tr>
</tbody>
</table>
| **IPSLA Test** | 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). |

**Note** Speed Test and IPSLA Test are supported on Cisco Wireless Controllers and Cisco Aironet 1800s Active Sensors with Software Release 8.8 and later.

c) Check the check boxes for the **Application Tests** that you want to run, and then enter the required information for those tests:
## Email Tests

<table>
<thead>
<tr>
<th>Test Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Tests</td>
<td>Includes the following:</td>
</tr>
<tr>
<td></td>
<td>• POP3: Post Office Protocol3, connects to POP3 server TCP port (110).</td>
</tr>
<tr>
<td></td>
<td>• IMAP: Internet Message Access Protocol, connects to IMAP server TCP port</td>
</tr>
<tr>
<td></td>
<td>(143).</td>
</tr>
<tr>
<td></td>
<td>• Outlook Web Server: Logs into the Outlook Web Server (OWS) and verifies</td>
</tr>
<tr>
<td></td>
<td>access.</td>
</tr>
<tr>
<td>Web Tests</td>
<td>Tests for access to the provided URL and verification of the response data.</td>
</tr>
<tr>
<td>File Transfer Tests</td>
<td>Tests for file upload and download operations.</td>
</tr>
</tbody>
</table>

**Note** The maximum file size for the sensor test is 5MB.

### Step 7
Click [Next] to continue to the **Select Sensors** step.

### Step 8
For the **Select Tests** step, configure the following settings:

- To set the RSSI threshold value for all APs, do the following:
  a. Click **Thresholds** and drag the **RSSI Threshold** slider to the desired value.
  b. From the **Number of Target APs** drop-down list, choose the number of APs you want the sensor to test against.
  c. Click **Apply**.

- To select specific APs to test, do the following:
  a. Check the check boxes of the sensors you want to use for the test.
  b. Click \(\triangleleft\) in the **Target AP #** column to view the all sensor neighboring APs.
  c. Check the check boxes of the desired APs to test in the **Target AP** column.

  **Note**
  - The maximum number of APs you can select is 5.
  - The sensor's neighboring APs are updated every 30 mins.

### Step 9
Click [Next] to create the sensor test.
The new test is added and appears on the **Test Suites** window.
Monitor and Troubleshoot the Health of Wireless Sensors

Use this procedure to get a global view of the health of wireless sensors and to determine if there are potential issues that must be addressed.

Before you begin
Make sure you have added and scheduled sensor-driven tests. See Add a Sensor-Driven Test, on page 146.

---

Step 1  
From the Cisco DNA Center home page, click the Assurance tab. The Overall Health dashboard appears.

Step 2  

*Figure 18: Wireless Sensor Dashboard*

Step 3  
Use the Sensor Timeline Slider for the following functionality:
### Sensors Timeline Slider

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>24 Hours</strong> drop-down menu</td>
<td>Enables you to display information on the dashboard within a selected time range. Do the following:</td>
</tr>
<tr>
<td></td>
<td>a. From the <strong>24 Hours</strong> drop-down menu, choose the length of the range: <strong>3 Hours</strong>, <strong>24 Hours</strong>, or <strong>7 Days</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. Specify the <strong>Start Date</strong> and time; and the <strong>End Date</strong> and time.</td>
</tr>
<tr>
<td></td>
<td>c. Click <strong>Apply</strong>.</td>
</tr>
<tr>
<td></td>
<td>This sets the range of the timeline.</td>
</tr>
<tr>
<td>All SSIDs</td>
<td>Displays information for the SSID you choose from the drop-down list. Default is <strong>All SSIDs</strong>.</td>
</tr>
<tr>
<td>All Bands</td>
<td>Display information for the band frequency you choose from the drop-down list. Options are: <strong>2.4 GHz</strong>, <strong>5 GHz</strong>, or <strong>All Bands</strong>.</td>
</tr>
<tr>
<td>Actions</td>
<td>Enables you to customize the dashboard display when you choose <strong>Edit Dashboards</strong> from the drop-down list. See Change the Position of a Dashlet, on page 197 and Create a Custom Dashboard, on page 193.</td>
</tr>
<tr>
<td>Timeline slider</td>
<td>Allows you to specify a more granular time range of the data to be displayed on the dashboard.</td>
</tr>
<tr>
<td></td>
<td>Move the timeline slider bars to the desired time range.</td>
</tr>
</tbody>
</table>

### Location Pane

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show</td>
<td>Allows you to hide or display the location pane. By default the location pane is hidden.</td>
</tr>
<tr>
<td>Hide</td>
<td></td>
</tr>
<tr>
<td>Hierarchical Site View or Building View drop-down list</td>
<td>Choose the Hierarchical Site View or Building View from the drop-down list. Based on what you choose, the table provides the relevant information. To view information about a specific site, building, or floor, click <strong>Apply</strong> in the appropriate row.</td>
</tr>
</tbody>
</table>

### Test Summary Dashlet

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOTAL</td>
<td>Provides a percentage breakdown of all the sensor-driven test results that were a success, slow, or a failure.</td>
</tr>
</tbody>
</table>
### Test Summary Dashlet

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 5 Test Types by Failure chart</td>
<td>Chart that provides the top 5 test types that failed.</td>
</tr>
<tr>
<td></td>
<td>Hover your cursor over a segment to display the percentage of failure and number of tests that failed for that test type.</td>
</tr>
</tbody>
</table>

### Top Locations by Failure Count Dashlet

Lists the top sites where the sensor-driven tests failed, and provides the number of tests that failed per site.

### Top APs by Failure Count Dashlet

Lists the top APs by failure count, and provides the number of failures per AP.

### Step 6

Use the **Test Results** dashlet for the following functionality:

### Test Results Dashlet

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Results table</td>
<td>Lists all the sensor-driven tests configured for the site. It provides information, such as the test name, location, SSIDs, types of tests that were run, and the test results.</td>
</tr>
</tbody>
</table>

**Note**

In the **Test Results** chart, the colors indicate the following:

- ◆: The test passed.
- ●: The test failed.
- ○: The test passed though the test completion time was above the threshold.
- ✗: Test information is not available.

The test results are presented in time intervals (represented by a bar with colored segments). Hover your cursor over a time interval for the aggregate result of the tests that were run within a 30-minute time frame, as shown in the following example:

January 29, 2019 12:25 am - January 29, 2019 12:55 am
IPSLA Failed

**Test Results details**

You can click on a **Test Results** time interval to open a slide-in pane with additional details for a 30-minute time frame. From the slide-in pane, you can:

- Click a test result bar in the graph to view details for each test result instance in the table below.
- Click a test result failure (red bar) in the graph to display the error message below the graph. The error message provides details on the reason for failure.

For the complete list of possible error messages, see Error Messages for Sensor-Driven Test Failures, on page 159.

- Click to select the data types you want displayed in the table.
- Click Export to export the table data to a CSV file.
Step 7  Use the **Onboarding Tests**, **Network Tests**, and **Application Tests** dashlets to view the following information:

<table>
<thead>
<tr>
<th>Onboarding Tests Dashlet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the fastest, slowest, and average test result times for onboarding test types. You can hover your cursor over the graph to get the test result times for a specific time. The area shaded red indicates test result times above the threshold. Use the filter at the top right of the dashlet to view the data for specific onboarding test types. Options are <strong>Onboarding</strong> and <strong>DHCP</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Tests Dashlet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the fastest, slowest, and average test result times for network test types. You can hover your cursor over the graph to get the test result times for a specific time. The area shaded red indicates test result times above the threshold. Use the filter at the top right of the dashlet to view the data for specific network test types. Options are <strong>DNS</strong>, <strong>Host Reachability</strong>, and <strong>RADIUS</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application Tests Dashlet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the fastest, slowest, and average test result times for application test types. You can hover your cursor over the graph to get the test result times for a specific time. The area shaded red indicates test result times above the threshold. Use the filter at the top right of the dashlet to view the data for specific application test types. Options are <strong>Web</strong>, <strong>Email</strong>, <strong>FTP</strong>, and <strong>Outlook</strong>.</td>
</tr>
</tbody>
</table>

Step 8  Use the **Performance Tests** dashlet to view the test result details for the Speed test and IPSLA test. Use the filter at the top right of the dashlet to specify between Speed test and IPSLA test.

Step 9  Use the **Sensor Devices** dashlet for following functionality:

<table>
<thead>
<tr>
<th>Sensors Devices Dashlet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>Status</td>
</tr>
<tr>
<td>Filter</td>
</tr>
</tbody>
</table>
Sensors Devices Dashlet

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sensor Devices table</strong></td>
<td>View detailed information of the sensor devices in a table format. The sensor devices tables lists the following information:</td>
</tr>
<tr>
<td></td>
<td>• Name: Displays the name of the sensor device.</td>
</tr>
<tr>
<td></td>
<td>The icons by the sensor name indicates the sensor's reachability:</td>
</tr>
<tr>
<td></td>
<td>• [●]: Sensor is reachable.</td>
</tr>
<tr>
<td></td>
<td>• [●]: Sensor is unreachable.</td>
</tr>
<tr>
<td></td>
<td>• Type: The sensor type.</td>
</tr>
<tr>
<td></td>
<td>• Device Model</td>
</tr>
<tr>
<td></td>
<td>• Total Tests</td>
</tr>
<tr>
<td></td>
<td>• Failed Count: Number of failed tests.</td>
</tr>
<tr>
<td></td>
<td>• Tested AP: Number of APs tested.</td>
</tr>
<tr>
<td></td>
<td>• Location: Displays the assigned location of the sensor device.</td>
</tr>
<tr>
<td></td>
<td>• Last Seen: Displays the timestamp of the last heartbeat.</td>
</tr>
</tbody>
</table>

Export

Export the table data to a CSV file.

---

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.

For Cisco Wireless Controllers, see Enable Provisioning SSID on the Wireless Controller, on page 155.

For Cisco Catalyst Wireless Controllers, see Enable Cisco Provisioning SSID on the Cisco Catalyst Wireless Controller, on page 155.

**Step 2** Create a backhaul configuration for the sensor.

See Manage Backhaul Settings, on page 143.

**Step 3** Provision the Cisco Aironet 1800s Active Sensor.

See Provision a Wireless or Sensor Device, on page 156.

**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 Digital Network Architecture 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 Webui.
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.
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**.

gh) 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 device provisions it by assigning a network profile 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.

When a device is claimed, some system configuration CLI commands from Cisco DNA Center are pushed to the device first, before the Onboarding Configuration (Day-0) template that you have defined. If your Onboarding Configuration template has any of the same CLI commands, these will override the system configuration, since they are applied last. The CLI commands pushed by the system include the following:

- Device credentials (CLI and SNMP)
- Enable SSH v2 and SCP server
- Disable HTTP and HTTPS servers
When Device Controllability is enabled for a device (it is enabled by default), the following configurations are added when the device is added into inventory:

- SNMP, NETCONF, and Cisco TrustSec (CTS) credentials
- IPDT enablement
- Controller certificates
- SNMP trap server definitions
- Syslog server definitions
- Netflow collector definitions
- Wireless network assurance

This procedure explains how to claim a device from the main Plug and Play tab. 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 38.
- Define the CLI and SNMP credentials for the devices.
- 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 ASCII 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
From the Cisco DNA Center home page, choose Provision > Devices > 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, Site Assignment.

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 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 **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**

Click on the name of 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 **RF Profile** drop-down list, choose an RF profile to apply to the device. This may be set if you designated one profile as a default.

d) For a Mobility Express device, enter values in the following fields: **Management IP**, **Subnet Mask**, and **Gateway**.

e) For a wireless sensor device, in the **Sensor Settings** drop-down list, choose the sensor device profile to apply to the device.

f) If you made any changes, click **Save**, otherwise, click **Cancel** to return to the list and configure other devices.

g) 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 you selected multiple devices to provision, click the next device in the list and repeat the configuration, until you have done this for all devices.

**Step 12**

Click **Next**.

The **Summary** window appears, where you can view details about the devices and configuration.

**Step 13**

Check the **Day-0 Config Preview Status** column for each device to see if the configuration preview was successful.

If the preview shows an error, you should resolve any issues before claiming the device, to avoid provisioning errors. You may need to go back to the **Configuration** step and change the configuration, revisit the **Design** area to update network design settings, or resolve any network connectivity issues. 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 14**

Click **Claim**.

A confirmation dialog box is displayed.

**Step 15**

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.
Error Messages for Sensor-Driven Test Failures

When a sensor-driven test fails, an error message is provided with details on why the test failed. Error messages for sensor-driven test failures can be viewed in the Test Results dashlet. See Monitor and Troubleshoot the Health of Wireless Sensors, on page 150.

The following table lists the error messages for onboarding test failures:

<table>
<thead>
<tr>
<th>Onboarding Test Errors</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assoc. Failed</td>
<td>Sensor Wireless Connection failed due to unspecified reason</td>
</tr>
<tr>
<td>.11z Failed</td>
<td>Tunneled direct link setup (TDLS) wakeup schedule rejected but alternative schedule provided</td>
</tr>
<tr>
<td>.11z Failed</td>
<td>Tunneled direct link setup (TDLS) wakeup schedule rejected</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Sensor failed to associated to AP because security is disabled</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Sensor failed to associated to AP because of unacceptable lifetime</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Sensor failed to associated to AP because sensor and AP are not in same basic service set (BSS).</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Sensor failed to associated to AP because sensor cannot support all requested capabilities in capability information field</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Sensor failed to re-associated to AP because reassociation denied due to inability to confirm that association exists.</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Sensor failed to associated to AP because association request denied due to reason outside scope of the wireless standard</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Sensor failed to associated to AP because responding station doesn't support specified authentication algorithm</td>
</tr>
<tr>
<td>Auth. Failed</td>
<td>Received authentication frame with authentication transaction sequence number out of expected sequence</td>
</tr>
<tr>
<td>Auth. Failed</td>
<td>Authentication rejected because of challenge failure</td>
</tr>
<tr>
<td>Auth. Failed</td>
<td>Authentication rejected due to timeout waiting for next frame in sequence</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Association denied because AP unable to handle additional associated stations</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Association denied due to requesting station not supporting all data rates in the BSSBasicRateSet parameter, where BSS refers to basic service set</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Association denied due to requesting station not supporting short preamble option</td>
</tr>
<tr>
<td>Onboarding Test Errors</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Error Message - Short Version</strong></td>
<td><strong>Error Message - Long Version</strong></td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Association denied due to requesting station not supporting packet binary convolutional code (PBCC) modulation option</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Association denied due to requesting station not supporting channel agility option</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Association request rejected because spectrum management capability required</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Association request rejected because of unacceptable information in the power capability element</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Association request rejected because of unacceptable information in the supported channels element</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Association denied due to requesting station not supporting short slot time option</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Association denied due to requesting station not supporting direct sequence spread spectrum orthogonal frequency division multiplexing (DSSS-OFDM) option</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Association denied because requesting station doesn't support high throughput (HT) features</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Sensor failed to associated to AP because Pairwise master key (PMK-R0) Key Holder (R0KH) is unreachable</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Association denied because requesting station doesn't support phased coexistence operation (PCO) transition time required by the AP</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Association request rejected temporarily</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>Robust management frame policy violation</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Sensor failed to associated to AP due to Quality of service (QoS)-related failure</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Sensor failed to associated to AP due to association Request decline</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Association request is not successful as one or more parameters have invalid values</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Associated failed due to Invalid information element (doesn't follow 802.11 standard)</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>Associated failed due to invalid group cipher</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>Associated failed due to invalid pairwise cipher</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>Associated failed due to invalid authentication and key management protocol (AKMP)</td>
</tr>
<tr>
<td>Error Message - Short Version</td>
<td>Error Message - Long Version</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>Associated failed due to unsupported robust security network element (RSNE) information element version</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>Associated failed due to invalid RSNE information element capabilities</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>Associated failed due to cipher suite rejected because of security policy</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Associated failed because TS is not created</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Associated failed because direct link is not allowed in the BSS by policy</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Associated failed because Destination station is not present within this BSS</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Associated failed because destination station is not a QoS station</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Association denied because ListenInterval is too large</td>
</tr>
<tr>
<td>Roaming Failure</td>
<td>Fast Roaming failed due to invalid fast transition (FT) action frame count</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>Fast Roaming failed due to invalid pairwise master key identifier (PMKID)</td>
</tr>
<tr>
<td>Roaming Failure</td>
<td>Fast Roaming failed due to invalid mobility domain element (MDE)</td>
</tr>
<tr>
<td>Roaming Failure</td>
<td>Fast Roaming failed due to invalid fast transition element (FTE)</td>
</tr>
<tr>
<td>.11u Failed</td>
<td>HotSpot 2.0 network discovery failed because AP does not support Generic advertisement service (GAS) advertisement protocol</td>
</tr>
<tr>
<td>.11u Failed</td>
<td>HotSpot 2.0 network discovery failed because no outstanding GAS request</td>
</tr>
<tr>
<td>.11u Failed</td>
<td>HotSpot 2.0 network discovery failed because GAS response not received from advertisement server (e.g. WLC)</td>
</tr>
<tr>
<td>.11u Failed</td>
<td>HotSpot 2.0 network discovery failed because GAS response couldn't return in time</td>
</tr>
<tr>
<td>.11u Failed</td>
<td>HotSpot 2.0 network discovery failed because GAS response larger than query response length limit</td>
</tr>
<tr>
<td>.11u Failed</td>
<td>HotSpot 2.0 network discovery request refused because home network doesn't support request</td>
</tr>
<tr>
<td>.11u Failed</td>
<td>HotSpot 2.0 network discovery failed because advertisement server in network not currently reachable</td>
</tr>
<tr>
<td>.11u Failed</td>
<td>HotSpot 2.0 network discovery failed because request refused due to permissions received via SSPN interface</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>Association request refused because AP doesn't support unauthenticated access</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>Association failed due to invalid contents of RSN Element</td>
</tr>
</tbody>
</table>
## Error Messages for Sensor-Driven Test Failures

### Onboarding Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth. Failed</td>
<td>Authentication rejected because anti-clogging token is required</td>
</tr>
<tr>
<td>Auth. Failed</td>
<td>Authentication rejected because the offered finite cyclic group not supported</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Association failed due to transmission failure</td>
</tr>
<tr>
<td>.11u Failed</td>
<td>HotSpot 2.0 network discovery failed because GAS query response timeout</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Association denied because Sensor does not support VHT rate</td>
</tr>
<tr>
<td>Deauthenticated</td>
<td>Sensor deauthenticated due to unspecified reason</td>
</tr>
<tr>
<td>Deauthenticated</td>
<td>Sensor deauthenticated because previous authentication is no longer valid</td>
</tr>
<tr>
<td>Deauthenticated</td>
<td>Deauthenticated because Sensor is leaving</td>
</tr>
<tr>
<td>Disassociated</td>
<td>Disassociated due to inactivity</td>
</tr>
<tr>
<td>Disassociated</td>
<td>Disassociated because access point (AP) unable to handle all currently associated stations</td>
</tr>
<tr>
<td>Deauthenticated</td>
<td>Sensor receives deauth packet because Sensor kept Class2 frame while deauthenticated</td>
</tr>
<tr>
<td>Deauthenticated</td>
<td>Sensor receives deauth packet because Sensor kept send data frame while disassociated</td>
</tr>
<tr>
<td>Disassociated</td>
<td>Disassociated because Sensor is leaving (or has left) AP</td>
</tr>
<tr>
<td>Disassociated</td>
<td>Sensor requesting association or re-association while Sensor is not authenticated by AP</td>
</tr>
<tr>
<td>Disassociated</td>
<td>Sensor is disassociated due to unacceptable information in the power capability element</td>
</tr>
<tr>
<td>Disassociated</td>
<td>Sensor is disassociated due to unacceptable information in the supported channels element</td>
</tr>
<tr>
<td>Disassociated</td>
<td>Sensor is disassociated due to Invalid information (Doesn't follow 802.11 standard)</td>
</tr>
<tr>
<td>Disassociated</td>
<td>Sensor is disassociated due to Message integrity code (MIC) failure</td>
</tr>
<tr>
<td>Key Exchange Failed</td>
<td>Sensor failed to associated due to 4-way handshake timeout</td>
</tr>
<tr>
<td>GTK Failed</td>
<td>Sensor failed to renew broadcast key</td>
</tr>
<tr>
<td>IE Failure</td>
<td>Information element in 4-way handshake different from association request, reassociation request, probe response, or beacon frame</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>Sensor failed to associated due to invalid group cipher</td>
</tr>
<tr>
<td>Error Message - Short Version</td>
<td>Error Message - Long Version</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>Sensor failed to associated due to invalid pairwise cipher</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>Sensor failed to associated due to invalid authentication and key management protocol (AKMP)</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>Sensor failed to associated due to unsupported robust security network (RSN) information element version</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>Sensor failed to associated due to invalid RSN information element capabilities</td>
</tr>
<tr>
<td>Auth. Failed</td>
<td>Sensor failed 802.1x authentication</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>Sensor failed to associated due to Cipher suite rejected because of security policy</td>
</tr>
<tr>
<td>.11z Failure</td>
<td>TDLS direct-link teardown due to TDLS peer STA unreachable via the TDLS direct link</td>
</tr>
<tr>
<td>.11z Failure</td>
<td>TDLS direct-link teardown for unspecified reason</td>
</tr>
<tr>
<td>Disassociated</td>
<td>Sensor disassociated because excessive number of frames need to be acknowledged</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>WPA2-PSK failed due to unspecified reason</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>WPA2-PSK failed due to WPA2 PSK key error</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>WPA2-PSK failed due to first handshake failure on EAP Key 4-way handshake</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>WPA2-PSK failed due to second handshake failure on EAP Key 4-way handshake</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>WPA2-PSK failed due to group key error</td>
</tr>
<tr>
<td>Security Mismatch</td>
<td>WPA2-PSK failed due to master key error</td>
</tr>
<tr>
<td>MSCHAPv2 Failure</td>
<td>MS-CHAPv2 failed due to restricted logon hours</td>
</tr>
<tr>
<td>MSCHAPv2 Failure</td>
<td>MS-CHAPv2 failed because account is disabled</td>
</tr>
<tr>
<td>MSCHAPv2 Failure</td>
<td>MS-CHAPv2 failed due to password expiration,</td>
</tr>
<tr>
<td>MSCHAPv2 Failure</td>
<td>MS-CHAPv2 failed because userID has no dial in permission,</td>
</tr>
<tr>
<td>MSCHAPv2 Failure</td>
<td>MS-CHAPv2 failed due to authentication failure</td>
</tr>
<tr>
<td>MSCHAPv2 Failure</td>
<td>MS-CHAPv2 failed because password is changing</td>
</tr>
<tr>
<td>Cert. Error</td>
<td>EAP-TLS failed because TLS certificate verification failed</td>
</tr>
</tbody>
</table>
## Onboarding Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cert. Error</td>
<td>EAP-TLS failed because TLS certificate is untrusted</td>
</tr>
<tr>
<td>Cert. Error</td>
<td>EAP-TLS failed because TLS certificate is revoked</td>
</tr>
<tr>
<td>Cert. Error</td>
<td>EAP-TLS failed because TLS certificate is invalid</td>
</tr>
<tr>
<td>Cert. Error</td>
<td>EAP-TLS failed because TLS certificate is expired</td>
</tr>
<tr>
<td>Cert. Error</td>
<td>EAP-TLS failed because TLS subject did not match</td>
</tr>
<tr>
<td>Cert. Error</td>
<td>EAP-TLS failed because TLS alt subject did not match</td>
</tr>
<tr>
<td>Cert. Error</td>
<td>EAP-TLS failed because TLS certificate rejected</td>
</tr>
<tr>
<td>Cert. Error</td>
<td>EAP-TLS failed because TLS rejected server certificate on probe-only run</td>
</tr>
<tr>
<td>Cert. Error</td>
<td>EAP-TLS failed because TLS domain suffix did not match</td>
</tr>
<tr>
<td>Cert. Error</td>
<td>EAP-TLS failed because TLS no local certificate is found</td>
</tr>
<tr>
<td>EAP Error</td>
<td>802.1x/EAP authentication failed because username is not found</td>
</tr>
<tr>
<td>EAP Error</td>
<td>802.1x/EAP authentication failed because entered password incorrect</td>
</tr>
<tr>
<td>EAP Error</td>
<td>802.1x/EAP authentication failed because EAP method is not allowed</td>
</tr>
<tr>
<td>EAP Error</td>
<td>802.1x/EAP authentication failed because EAP method is not found</td>
</tr>
<tr>
<td>Internal Error</td>
<td>Internal error(1800), Sensor gets the null SSID</td>
</tr>
<tr>
<td>Internal Error</td>
<td>Internal error(1801), Sensor is stuck in channel scanning state</td>
</tr>
<tr>
<td>No AP Discovered</td>
<td>Sensor failed to find AP with target SSID</td>
</tr>
<tr>
<td>Assoc. Failed</td>
<td>Sensor failed to discover target SSID hence Sensor couldn't make association request</td>
</tr>
<tr>
<td>DHCP Failed</td>
<td>Sensor failed to get wireless IP address because DHCP Discover was not sent</td>
</tr>
<tr>
<td>Auth. Failed</td>
<td>Sensor failed to authenticate because requested Auth method is not available</td>
</tr>
<tr>
<td>DHCP Failed</td>
<td>Sensor failed to get wireless IP address because DHCP OFFER was not received</td>
</tr>
<tr>
<td>DHCP Failed</td>
<td>Sensor failed to get wireless IP address because DHCP REQUEST was not sent</td>
</tr>
<tr>
<td>DHCP Failed</td>
<td>Sensor failed to get wireless IP address because DHCP ACK was not received</td>
</tr>
</tbody>
</table>
### Onboarding Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Failed</td>
<td>Sensor received DHCP ACK but connection timed out</td>
</tr>
</tbody>
</table>

The following table lists the error messages for web authentication test failures:

### Web Authentication Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid Config</td>
<td>WebAuth failed because invalid WLC configuration</td>
</tr>
<tr>
<td>Invalid Security Type</td>
<td>WebAuth failed because invalid WLC security type</td>
</tr>
<tr>
<td>Invalid IP</td>
<td>WebAuth failed because Sensor IP was invalid</td>
</tr>
<tr>
<td>Invalid Username</td>
<td>WebAuth failed because wrong Username entered from Sensor-driven test creation step</td>
</tr>
<tr>
<td>Invalid Password</td>
<td>WebAuth failed because wrong Password entered from Sensor-driven test creation step</td>
</tr>
<tr>
<td>Access IP route add fail</td>
<td>WebAuth failed because sensor fails to reach guest portal</td>
</tr>
<tr>
<td>Access URL Error</td>
<td>WebAuth failed because sensor got HTTP Error from guest portal page</td>
</tr>
<tr>
<td>Access URL Error</td>
<td>WebAuth failed because sensor got URL Error during guest portal page</td>
</tr>
<tr>
<td>Access URL Error</td>
<td>WebAuth failed because sensor got Socket Error from guest portal page</td>
</tr>
<tr>
<td>Access URL Error</td>
<td>WebAuth failed because sensor got exception error while it decode URL</td>
</tr>
<tr>
<td>Access URL contents invalid</td>
<td>WebAuth failed because guest portal includes unsupported content format</td>
</tr>
<tr>
<td>Access URL login URL missing</td>
<td>WebAuth failed because guest portal does not have login page</td>
</tr>
<tr>
<td>Access URL Login URL invalid</td>
<td>WebAuth failed because guest portal page has unsupported page contents</td>
</tr>
<tr>
<td>Access URL Virtual IP missing</td>
<td>WebAuth failed because guest portal page is missing WLC Virtual IP Address</td>
</tr>
<tr>
<td>Access URL Virtual IP Invalid</td>
<td>WebAuth failed because guest portal page has invalid WLC Virtual IP Address</td>
</tr>
<tr>
<td>Virtual IP route add fail</td>
<td>WebAuth failed because sensor failed to route traffic to WLC Virtual IP</td>
</tr>
<tr>
<td>Login URL Error</td>
<td>WebAuth failed because sensor received HTTP Error from login page</td>
</tr>
<tr>
<td>Login URL Error</td>
<td>WebAuth failed because sensor received error from login page</td>
</tr>
<tr>
<td>Login URL Error</td>
<td>WebAuth failed because sensor got socket error from login page</td>
</tr>
</tbody>
</table>
### Web Authentication Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login URL Error</td>
<td>WebAuth failed because sensor got exception error while it process login page</td>
</tr>
<tr>
<td>Login URL contents invalid</td>
<td>WebAuth failed because login page includes unsupported content format</td>
</tr>
<tr>
<td>Login Failure</td>
<td>WebAuth failed due to login failure</td>
</tr>
<tr>
<td>Login Status Unknown</td>
<td>WebAuth failed because login status was not able to identify</td>
</tr>
<tr>
<td>Logout URL Error</td>
<td>WebAuth failed because sensor received HTTP Error from logout page</td>
</tr>
<tr>
<td>Logout URL Error</td>
<td>WebAuth failed because sensor received URL Error from logout page</td>
</tr>
<tr>
<td>Logout URL Error</td>
<td>WebAuth failed because sensor received Socket Error from logout page</td>
</tr>
<tr>
<td>Logout URL Error</td>
<td>WebAuth failed because sensor got exception error while it decode logout URL</td>
</tr>
<tr>
<td>Logout URL contents invalid</td>
<td>WebAuth failed because WebPortal logout page included invalid contents</td>
</tr>
<tr>
<td>Logout Failure</td>
<td>WebAuth failed due to logout failure</td>
</tr>
<tr>
<td>Logout Status Unknown</td>
<td>WebAuth failed because logout status was not able to identify</td>
</tr>
<tr>
<td>Software Exception</td>
<td>WebAuth failed due to exception error from sensor software</td>
</tr>
<tr>
<td>Unknown Error</td>
<td>WebAuth failed due to unidentified reason</td>
</tr>
</tbody>
</table>

The following table lists the error messages for file transfer test failures:

### File Transfer Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not reachable</td>
<td>Sensor failed to ping FTP server</td>
</tr>
<tr>
<td>No response</td>
<td>Sensor failed to establish connection with FTP server</td>
</tr>
<tr>
<td>File missing</td>
<td>FTP test failed because sensors cannot find designated upload file</td>
</tr>
<tr>
<td>File missing</td>
<td>FTP test failed because sensor cannot find designated download file</td>
</tr>
<tr>
<td>File Access Failed</td>
<td>Sensors cannot access designated upload file</td>
</tr>
<tr>
<td>File Access Failed</td>
<td>Sensors cannot access designated download file</td>
</tr>
<tr>
<td>File too large</td>
<td>Sensor test failed because reported file size is too large(&gt;5MB)</td>
</tr>
<tr>
<td>Transfer type mismatch</td>
<td>FTP test failed and reported Invalid transfer type error</td>
</tr>
<tr>
<td>Server Error</td>
<td>FTP test failed and reported unexpected reply error</td>
</tr>
<tr>
<td>Server Error</td>
<td>FTP test failed and server reported temporary error</td>
</tr>
</tbody>
</table>
### File Transfer Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Error</td>
<td>FTP test failed and server reported permanent error</td>
</tr>
<tr>
<td>Server Error</td>
<td>FTP test failed due to protocol error</td>
</tr>
<tr>
<td>Server Error</td>
<td>FTP test failed and sensor reported generic error</td>
</tr>
<tr>
<td>File too large</td>
<td>FTP test failed because too large download file size.(&gt;5MB)</td>
</tr>
<tr>
<td>No response</td>
<td>FTP test failed due to connection failure</td>
</tr>
<tr>
<td>No response</td>
<td>FTP test failed with invalid protocol error</td>
</tr>
<tr>
<td>Server Error</td>
<td>FTP test failed with exception error</td>
</tr>
<tr>
<td>Server Error</td>
<td>FTP test failed with Server Timeout error</td>
</tr>
</tbody>
</table>

The following is the error message displayed for SSH test failures:

### SSH Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH Failure</td>
<td>Sensor failed to complete SSH test</td>
</tr>
</tbody>
</table>

The following table lists the error messages for DNS test failures:

### DNS Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empty Name field</td>
<td>Sensor reported Domain name field is either empty or blank</td>
</tr>
<tr>
<td>No DNS response</td>
<td>Sensors reported Socket Error and Cannot resolve Domain</td>
</tr>
</tbody>
</table>

The following table lists the error messages for mail server test failures:

### Mail Server Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsupported Protocol</td>
<td>Unsupported Protocol returned from Mail server</td>
</tr>
<tr>
<td>Server Unreachable</td>
<td>Mail Server is not reachable by Ping. Check if Mail server block ICMP</td>
</tr>
<tr>
<td>No Response</td>
<td>Failed to connect Mail server and received no response</td>
</tr>
<tr>
<td>Exception Error</td>
<td>Sensor Mail Server Test encountered software error during run.</td>
</tr>
</tbody>
</table>

The following is the error message displayed for ping test failures:

### Ping Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping Failure</td>
<td>Sensor failed to run Ping test</td>
</tr>
</tbody>
</table>
### Ping Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid Address</td>
<td>Ping test failed due to Invalid Address configured</td>
</tr>
<tr>
<td>Address Unreachable</td>
<td>Ping test failed because of timeout connecting to Address</td>
</tr>
<tr>
<td>Exception Error</td>
<td>Ping test encountered exception error</td>
</tr>
</tbody>
</table>

The following tables lists the error messages for web server test failures:

### Web Server Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid URL</td>
<td>Sensor Web Server test failed with Invalid URL error</td>
</tr>
<tr>
<td>URL is not accessible</td>
<td>Sensor Web Server test failed access URL</td>
</tr>
<tr>
<td>Exception Error</td>
<td>Sensor Web Server test encountered software error during run.</td>
</tr>
<tr>
<td>DNS Resolve Fail</td>
<td>Sensor Web Server test failed due to fail to resolve DNS name in URL</td>
</tr>
</tbody>
</table>

The following table lists the error messages for Outlook server test failures:

### Outlook Server Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid Username</td>
<td>Outlook Web Access failed due to Invalid Username</td>
</tr>
<tr>
<td>Invalid Password</td>
<td>Outlook Web Access failed due to Invalid Password</td>
</tr>
<tr>
<td>Invalid URL</td>
<td>Outlook Web Access failed due to Invalid URL</td>
</tr>
<tr>
<td>DNS Resolve Fail</td>
<td>Outlook Web Access failed due to fail to resolve provided DNS name</td>
</tr>
<tr>
<td>Server Unreachable</td>
<td>Outlook Web Access failed due to Ping failure</td>
</tr>
<tr>
<td>Connection Fail</td>
<td>Outlook Web Access failed due to server connection failure</td>
</tr>
<tr>
<td>Login Fail</td>
<td>Outlook Web Access failed to login</td>
</tr>
<tr>
<td>Exception</td>
<td>Outlook Web Access Test encountered software error</td>
</tr>
</tbody>
</table>

The following tables lists the error messages for internet speed test failures:

### Internet Speed Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server unreachable</td>
<td>Speed test Server is unreachable</td>
</tr>
<tr>
<td>Server discovery failed</td>
<td>Sensors received http error on speed test server discovery</td>
</tr>
<tr>
<td>Server discovery failed</td>
<td>Sensor reported URL error Please verify that the URL on the Speed test server is accessible.</td>
</tr>
</tbody>
</table>
### Internet Speed Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server timeout</td>
<td>Sensor reported time out for NDT query server</td>
</tr>
<tr>
<td>Server discovery failed</td>
<td>Sensors reported unavailability of Speed Test server.</td>
</tr>
<tr>
<td>Server connection failed</td>
<td>Sensors reported WebSocket error between Speed test server and sensor</td>
</tr>
<tr>
<td>Uplink test timeout</td>
<td>Sensors failed to run uplink test due to server timeout</td>
</tr>
<tr>
<td>Uplink proxy error</td>
<td>Sensor reported uplink proxy error</td>
</tr>
</tbody>
</table>

The following table lists the error messages for IPSLA test failures:

### IPSLA Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsupported probe type</td>
<td>IP SLA test failed due to unsupported probe type used</td>
</tr>
<tr>
<td>Invalid Probe count</td>
<td>Sensors reported probe count error</td>
</tr>
<tr>
<td>IP SLA connection failure</td>
<td>Sensor failed to connect to IP SLA responder</td>
</tr>
<tr>
<td>No response from DNAC</td>
<td>Internal Error, Sensor does not receive response from DNA Center upon IP SLA test</td>
</tr>
<tr>
<td>Failed to get responder IP</td>
<td>Sensors failed to get IP SLA responder IP</td>
</tr>
<tr>
<td>No response from responder</td>
<td>Sensors reported no response from responder AP</td>
</tr>
<tr>
<td>Error response(400/500) from DNAC</td>
<td>Error Response code (400/500) received from DNAC</td>
</tr>
</tbody>
</table>

The following table lists the error messages for RADIUS test failures:

### RADIUS Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid Server</td>
<td>RADIUS test failed due to Invalid Server configured</td>
</tr>
<tr>
<td>Protocol Mismatch</td>
<td>RADIUS test failed because server does not response on CHAP or PAP</td>
</tr>
<tr>
<td>Invalid Port</td>
<td>RADIUS test failed due to port number mismatch between sensor test and RADIUS server</td>
</tr>
<tr>
<td>Invalid UserName</td>
<td>RADIUS test failed due to Username mismatch</td>
</tr>
<tr>
<td>Invalid Password</td>
<td>RADIUS test failed due to password mismatch</td>
</tr>
<tr>
<td>Invalid Shared Secret</td>
<td>RADIUS test failed due to shared secret mismatch</td>
</tr>
<tr>
<td>Server Unreachable</td>
<td>RADIUS Server is not reachable via Ping</td>
</tr>
<tr>
<td>RADIUS Unreachable</td>
<td>RADIUS Server is unreachable</td>
</tr>
</tbody>
</table>
## RADIUS Test Errors

<table>
<thead>
<tr>
<th>Error Message - Short Version</th>
<th>Error Message - Long Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Timeout</td>
<td>RADIUS Server failed to connect</td>
</tr>
<tr>
<td>RADIUS Denied</td>
<td>RADIUS Server access denied</td>
</tr>
<tr>
<td>Exception Error</td>
<td>RADIUS Server test encountered exception error</td>
</tr>
</tbody>
</table>
Integrate Cisco CMX for Wireless Maps

- About Cisco Connected Mobile Experiences Integration, on page 171
- Add a User for the Cisco CMX API Server, on page 171
- Create Cisco CMX Settings, on page 172
- Troubleshoot Cisco CMX, on page 173

About Cisco Connected Mobile Experiences Integration

Cisco DNA Center supports the integration of on-premise Connected Mobile Experiences (CMX) for wireless maps. With the CMX integration, you can get the exact location of your clients 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 small 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:
Create Cisco CMX Settings

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 172.

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 171.

Step 1
To add a CMX server to the Cisco DNA Center, from the Cisco DNA Center home page, click the gear icon (⚙), and then choose System Settings > Settings > 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, follow these steps.

Step 8
Choose Design > Network Settings > Wireless.

Step 9
In the left tree view menu, select either Global or the area, building, or floor that you are interested in.
Step 10 Under **CMX Servers**, from the **CMX Servers** drop-down list, select the CMX server.

Step 11 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 12 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 13 To edit the CMX server details, from the Cisco DNA Center click the gear icon (⚙️), and then choose **System Settings > CMX Servers**.

Step 14 Select the CMX server that you want to edit, and make any changes, and click **Update**.

Step 15

Step 16 To delete a CMX server, from the Cisco DNA Center click the gear icon (⚙️), and then choose **System Settings > CMX Servers**.

Step 17 Select the CMX server that you want to delete, and click **Delete**.

Step 18 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:

```bash
curl -k -u <user>:<password> -X GET /api/v1/dna-maps-service/domains/<floor_group_id>/clients?associated=true
```
CHAPTER 12

Manage Intelligent Capture

- About Intelligent Capture, on page 175
- Supported Devices for Intelligent Capture, on page 175
- Intelligent Capture Best Practices, on page 176
- Manage Intelligent Capture Settings for a Client, on page 177
- About Capture Sessions, on page 178
- Manage Intelligent Capture Settings for an Access Point, on page 178
- Monitor Intelligent Capture Details for a Client, on page 180
- About NAM Integration, on page 184
- Monitor Intelligent Capture Details for an AP, on page 186
- About Cisco Aironet AP Functionality During Spectrum Analysis, on page 190
- Troubleshoot Intelligent Capture Issues, on page 191

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, the Cisco DNA Center can receive packet capture data, AP and client statistics, and spectrum data. With the direct communication link between the Cisco DNA Center and APs, Intelligent Capture allows you access to data from APs that is not available from the wireless controllers.

Supported Devices for Intelligent Capture

The following table lists the Cisco Wireless Controllers that support Intelligent Capture:

<table>
<thead>
<tr>
<th>Supported Cisco Wireless Controllers</th>
<th>Minimum Supported Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 3504 Wireless Controller</td>
<td>AireOS 8.8</td>
</tr>
<tr>
<td>Cisco 5520 Wireless Controller</td>
<td>AireOS 8.8</td>
</tr>
<tr>
<td>Cisco 8540 Wireless Controller</td>
<td>AireOS 8.8</td>
</tr>
</tbody>
</table>
The following table lists the Cisco Catalyst Wireless Controllers that support Intelligent Capture:

<table>
<thead>
<tr>
<th>Supported Cisco Catalyst Wireless Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device</strong></td>
</tr>
<tr>
<td>Cisco Catalyst 9800 Series Wireless Controllers</td>
</tr>
</tbody>
</table>

The following table lists the Cisco APs that support Intelligent Capture:

<table>
<thead>
<tr>
<th>Supported Cisco APs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device</strong></td>
</tr>
<tr>
<td>Aironet 4800 AP</td>
</tr>
<tr>
<td>Aironet 2800 Series APs</td>
</tr>
<tr>
<td>Aironet 3800 Series APs</td>
</tr>
<tr>
<td>Aironet 1815 Series APs</td>
</tr>
<tr>
<td>Aironet 1830 Series APs</td>
</tr>
<tr>
<td>Aironet 1840 Series APs</td>
</tr>
<tr>
<td>Aironet 1850 Series APs</td>
</tr>
<tr>
<td>Aironet 1540 Series APs</td>
</tr>
<tr>
<td>Aironet 1560 Series APs</td>
</tr>
<tr>
<td>Catalyst 9115 AP</td>
</tr>
<tr>
<td>Catalyst 9120 AP</td>
</tr>
</tbody>
</table>

**Note**
- Full Packet Capture is only supported on Aironet 4800 APs.
- Spectrum Analysis is only supported on the Aironet 4800 APs, Aironet 2800 Series APs, Aironet 3800 APs, and Aironet 1560 Series APs.

**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 any wireless controller device from Cisco DNA Center, disable all Intelligent Capture settings for the APs managed by that wireless controller.
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.

Manage Intelligent Capture Settings for a Client

Use this procedure to view, edit, delete, or stop a live or scheduled client 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 Monitor Intelligent Capture Details for a Client, on page 180.

- Data for the charts and tables displayed in the **Device 360 > Intelligent Capture** window. See Monitor Intelligent Capture Details for an AP, on page 186.

**Step 1**
From the Cisco DNA Center home page, click the **Assurance** tab.
The **Overall Health** dashboard appears.

**Step 2**
Choose **Manage > Intelligent Capture Settings > Client**.
The **Intelligent Capture Settings** window appears.

**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 or delete 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** or **Delete 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**.

**Step 6**
To schedule a client capture session, click **Schedule Client Capture**.
The **Schedule Client Capture** slide-in pane appears.

**Step 7**
In the **Schedule Client Capture** slide-in pane, configure the following settings:

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, and 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.
About Capture Sessions

There are 16 time slots allocated for capture sessions (live and scheduled) where each client in a session uses one time slot. Live capture sessions run for three hours for a specific client. Scheduled capture sessions can run for up to eight hours.

A scheduled capture session can have a maximum of 12 clients. But since there are only 16 time slots, the actual maximum value will be less if there are more than four live capture sessions running. Only one time slot is used per client, so the same client in a concurrent live and scheduled capture session can use only one slot.

Manage Intelligent Capture Settings for an Access Point

Use this procedure to select one or more APs to collect the following data:

- AP radio and WLAN statistics which are displayed in the RF Statistics tab of the Device 360 > Intelligent Capture window. See Monitor Intelligent Capture Details for a Client, on page 180.
- AP Client statistics (30-second samples) which are displayed in the RF Statistics area of the Client 360 > Intelligent Capture window for all clients associated with the selected APs.
- Anomaly Capture for onboarding events for all clients 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. See Monitor Intelligent Capture Details for a Client, on page 180.

Step 1
From the Cisco DNA Center home page, click the Assurance tab. The Overall Health dashboard appears.

Step 2
Choose Manage > Intelligent Capture Settings > Access Point. The Intelligent Capture Settings window appears where you can enable or disable AP statistics capture and anomaly capture.

Step 3
Click the AP Stats Capture tab and select one of the following options:

Note
With the AP Stats Capture tab, you can configure AP radio, WLAN, and AP client statistics.
### Manage Intelligent Capture Settings for an Access Point

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Specific APs - select APs to enable** | Enables the AP statistics for selected APs. You can do the following:   
  a. In the left pane, select a floor to display the APs that belong to that floor.  
  b. Click the **Enabled APs** tab to view and disable the APs that are currently enabled.  
  c. Click the **Disabled APs** tab to view and enable the APs that are currently disabled.  
    **Note** If a previous attempt to enable the AP failed, an error message is displayed in the **Config Status** column.  
  d. Click the **Not-Ready APs** tab to view incompatible access points.  
    **Note** Incompatible APs have the following conditions:  
    • The operation mode is not set to local or FlexConnect.  
    • The OS version is not software release MR1 or later. |
| **Globally - all capable APs** | Globally enables anomaly capture for all APs.                                                                                               |

#### Step 4

Click the **Anomaly Capture** tab and select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Specific APs - select APs to enable** | Enables the Anomaly Capture for selected APs. You can do the following:   
  a. In the left pane, select a floor to display the APs that belong to that floor.  
  b. Click the **Enabled APs** tab to view and disable the APs that are currently enabled.  
  c. Click the **Disabled APs** tab to view and enable the APs that are currently disabled.  
    **Note** If a previous attempt to enable the AP failed, an error message is displayed in the **Config Status** column.  
  d. Click the **Not-Ready APs** tab to view incompatible access points.  
    **Note** Incompatible access points have the following conditions:  
    • The operation mode is not set to local or FlexConnect.  
    • The OS version is not software release MR1 or later. |
| **Globally - all capable APs** | Globally enables anomaly capture for all APs.                                                                                               |
Monitor Intelligent Capture Details for a Client

Use this procedure to view, monitor, and troubleshoot captured onboarding and data packets for a specific client device.

Step 1
From the Cisco DNA Center home page, click the Assurance tab. The Overall Health dashboard appears.

Step 2
Choose Dashboards > Health > Client Health. The Client Health dashboard 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 window for the client device 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 Troubleshoot Intelligent Capture Issues, on page 191 for more details.

Figure 19: Intelligent Capture Window of a Client
Step 5  
Use the **Data Packet Capture Area** for the following functionality:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| ☀ Run Data Packet Capture | Use this button to start a Full Packet Capture for the client. Full Packet Capture files are used for troubleshooting and the **Wireless Packet Application Analysis** dashlet.  
**Note**  
Full Packet Capture is supported only on Cisco Aironet 4800 APs. If Full Packet Capture is enabled and the client roams to an AP that is not a Cisco Aironet 4800 AP, then packet capture stops until the client reconnects to a Cisco Aironet 4800 AP.  
If Full Packet Capture is currently running for the client, click ☀ Data Packet Capturing ▶ Stop to stop it.  
**Note**  
Only one Full Packet Capture can run at a time. If you click ☀ Run Data Packet Capture while Full Packet Capture is running, a dialog box appears with the option to either end the current capture or start a new capture.  
**Note**  
As for all Intelligent Capture features, time zones must be synchronized between Cisco DNA Center and the Cisco Wireless Controller for Full Packet Capture to work. Ensure that the wireless controller is connected to a Network Time Protocol (NTP) server.  
**Note**  
New sets of PCAP files are started each time a new capture session is started. |

| Download                  | 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 Full Packet Capture file has a limit of 100 MB. The total of all Full Packet Capture files cannot exceed 3.5 GB.  
**Note**  
Only PCAP files from the past seven days can be downloaded. |

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 timeline slider for the following functionality:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 hour drop-down list</td>
<td>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.</td>
</tr>
<tr>
<td>Timeline Slider</td>
<td>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 or scheduled capture. Green indicates onboarding events and red indicates anomaly events. To adjust the timeline to a different time window, click the &lt; and &gt; 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.</td>
</tr>
</tbody>
</table>

**Step 8**

Use the **Onboarding Events** dashlet for the following functionality:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All and Anomaly PCAP filter</td>
<td>Allows you to filter the onboarding events. Options are:</td>
</tr>
<tr>
<td></td>
<td>• All: Displays all events. This is the default.</td>
</tr>
<tr>
<td></td>
<td>• Anomaly PCAP: Filter for only anomaly events.</td>
</tr>
<tr>
<td>Export PCAP</td>
<td>You can download the packets for a range of specified events:</td>
</tr>
<tr>
<td></td>
<td>a. Click Export PCAP.</td>
</tr>
<tr>
<td></td>
<td>b. Specify the first and last events that you want to include in the PCAP.</td>
</tr>
<tr>
<td></td>
<td>c. Click Download PCAP to start the download.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>List of Onboarding, Incomplete, and Anomaly Events</td>
<td>View the list onboarding, incomplete, and anomaly events in chronological order. Events are color-coded to indicate the following:</td>
</tr>
<tr>
<td></td>
<td>- Green: Successful onboarding event.</td>
</tr>
<tr>
<td></td>
<td>- Blue: Incomplete event.</td>
</tr>
<tr>
<td></td>
<td>- Red: Anomaly event.</td>
</tr>
<tr>
<td>Note</td>
<td>Events with a 📂 icon indicates that data packets for this event have been captured for download or analysis.</td>
</tr>
<tr>
<td></td>
<td>You can click &gt; to the left of a group to expand it and view the individual events for that group.</td>
</tr>
<tr>
<td>Event Details</td>
<td>You can click an event group or individual event to view the following sections with further details:</td>
</tr>
<tr>
<td></td>
<td><strong>Client Location</strong>: Displays the map of the client location and the client's movement during the event.</td>
</tr>
<tr>
<td></td>
<td><strong>Auto Packet Analyzer</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Auto Packet Analyzer</strong> section displays a graph with the following information:</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>You can download the packets by clicking ➔ Download Packets.</td>
</tr>
<tr>
<td></td>
<td>- The packet source (client or AP).</td>
</tr>
<tr>
<td></td>
<td>- The onboard packet stage identifier.</td>
</tr>
<tr>
<td></td>
<td>- RSSI (dBm) per packet.</td>
</tr>
<tr>
<td></td>
<td>- Interpacket gap (ms).</td>
</tr>
<tr>
<td></td>
<td>- The associated AP.</td>
</tr>
<tr>
<td><strong>RF Statistics</strong>:</td>
<td>Displays charts with the RF statistic data for the 10 minute interval surrounding the event.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Note</td>
<td>If <strong>Anomaly Capture</strong> is enabled, the packets for anomaly events are captured even if a live or scheduled capture is not running.</td>
</tr>
</tbody>
</table>
Step 9  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, throughput, 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.

Step 10  Use the **RF Statistics** dashlet to view detailed RF information.

There are four charts that displays the AP client statistics for the client. 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 11  Use the **Wireless Packet Application Analysis** dashlet to view details about data packet captures.

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 Network Analysis Module (NAM). See About NAM Integration, on page 184.

---

**About NAM Integration**

If you have a NAM (Network Analysis Module) 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.

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 (Network Analysis Module).

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 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 n the NAM or vNAM server and Cisco DNA Center is synchronized. You can synchronize the time from the NAM user interface: Administration > System > System Time.

What to do next
Configure the gRPC collector. See Configure the gRPC Collector, on page 186.
**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 185.

---

**Step 1**
From the Cisco DNA Center home page, choose 🌐 > System Settings > Data Platform > Collectors.
The Collectors window appears.

**Step 2**
Click GRPC-COLLECTOR.
The GRPC-COLLECTOR window appears.

**Step 3**
Click ☐ Add.
The gRPC Collector Configuration window appears.

**Step 4**
Add only one GRPC-COLLECTOR configuration. Do the following:

a) In the ConfigData area, check the AgentExport check box to export the network packet data to NAM.

b) In the AgentIPAddress field, enter the IP address of the data port recorded (refer to Step 5, on page 185 from Configure an IP Address on the NAM Data Port, on page 185).

c) In the ConfigurationName field, enter a unique name for the GRPC collector configuration.

d) Click Save Configuration.

---

**Monitor Intelligent Capture Details for an AP**

Use this procedure to view and monitor captured onboarding and data packets for a specific AP device.

---

**Step 1**
From the Cisco DNA Center home page, click the Assurance tab.
The Overall Health dashboard appears.

**Step 2**
Choose Health > Network.
The Network Health dashboard 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 to open the Intelligent Capture window for that specific device.

**Attention**
If a ⚠ icon with the message GRPC link is not ready (CONNECTING) appears next to the AP name, see Troubleshoot Intelligent Capture Issues, on page 191 for more details.
Step 5 Click the **RF Statistics** tab to view details about RF statistics.

**Note** If AP statistics has not been enabled from the **AP Intelligent Capture** window (see Manage Intelligent Capture Settings for an Access Point, on page 178), click **Enable RF Statistics** in the top-right to enable RF statistics for this AP.

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:

<table>
<thead>
<tr>
<th>Timeline Slider</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>1 hour</strong> drop-down list</td>
<td>Click the drop-down list and select a duration to set the range of the timeline. Options are <strong>1 hour</strong>, <strong>3 hours</strong>, and <strong>5 hours</strong>. Default is <strong>1 hour</strong>.</td>
</tr>
</tbody>
</table>

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 **Radio 1 (5 GHz)**.

c) Use the dashlets to view the RF statistics details. The dashlets provide the following information:

<table>
<thead>
<tr>
<th>Clients Dashlet</th>
<th>Displays the number of clients using the AP. The data source is from the AP WLAN statistics. You can do the following in the chart:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>• Hover your cursor over the chart to view the number of clients using the AP for a particular time.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>• Click and drag within the chart to zoom in on a period. To change the view to the default, click ☐.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>• Click the color-coded data types below the chart to disable or enable the data type that is displayed in the chart.</strong></td>
<td></td>
</tr>
</tbody>
</table>

| 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. You can do the following:

- Hover your cursor over the chart to view the number of clients for each category for a particular time.
- 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.

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. You can do the following:

- Hover your cursor over the chart to view the number of frames for a particular time.
- 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.

Frame Errors Dashlet
Displays the number of transmit and receive errors. The data source is from the AP radio statistics. You can do the following:

- Hover your cursor over the chart to view the number of frame errors for a particular time.
- 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.

Tx Power and Noise Floor Dashlet
Displays the transmit power and noise floor. The data source is from the AP radio statistics. You can do the following:

- Hover your cursor over the chart to view the transmit power and noise floor for a particular time.
- 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.
Multicast/Broadcast Counter Dashlet
Displays the multicast and broadcast counts for each SSID. The data source is from the AP WLAN statistics. You can do the following:

- Hover your cursor over the chart to view the multicast and broadcast counts for a particular time.
- 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.

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:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 hour drop-down list</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 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 Aironet AP Functionality During Spectrum Analysis, on page 190.

c) Use the Spectrum Analysis charts for the following functionality:
Spectrum Analysis Charts

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top chart (Persistence)</td>
<td>This chart plots the amplitude or power at each channel for each heard signal in the RF environment over a 5-minute interval. Color represents how many signals are heard at the same amplitude and channel. Blue indicates low signal and red indicates high signal. The opacity represents the age of the signal data within the 5-minute interval, with older data being more transparent.</td>
</tr>
<tr>
<td>Bottom chart (Waterfall)</td>
<td>This chart plots heard signals over a 5-minute interval for each channel. The color represents the amplitude. Blue indicates a low value (-100 dBm) and red indicates a high value (-20 dBm).</td>
</tr>
</tbody>
</table>

**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 Aironet 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.

Radio slot assignments for spectrum analysis are as follows:

<table>
<thead>
<tr>
<th>Device Model</th>
<th>Spectrum Analysis Radio Slot Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aironet 2800 Series APs</td>
<td>Radio slots 0 and 1 are enabled.</td>
</tr>
<tr>
<td>Aironet 3800 Series APs</td>
<td></td>
</tr>
</tbody>
</table>
### Manage Intelligent Capture

#### Troubleshoot Intelligent Capture Issues

Use this topic to troubleshoot issues you may encounter when using Intelligent Capture.

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

**Issue:** For the client or access point, the ▲ 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 this port number.

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.

---

<table>
<thead>
<tr>
<th>Device Model</th>
<th>Spectrum Analysis Radio Slot Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aironet 4800 Series APs</td>
<td>If data packet capture is running, radio slots 0 and 1 are enabled.</td>
</tr>
<tr>
<td></td>
<td>If data packet capture is not running, radio slot 2 is enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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 <strong>Radio Mode</strong> and <strong>Channel</strong> fields are empty. This occurs if the FRA radio is set to operate in 5 GHz and packet capture is enabled.</td>
</tr>
</tbody>
</table>
Troubleshoot Intelligent Capture Issues
CHAPTER 13

Manage Dashboards

- About Dashboards, on page 193
- Create a Custom Dashboard, on page 193
- Create a Dashboard From a Template, on page 195
- View a Dashboard, on page 196
- Edit or Delete a Dashboard, on page 196
- Duplicate a Dashboard, on page 197
- Mark a Dashboard as a Favorite, on page 197
- Change the Position of a Dashlet, on page 197

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.

Create a Custom Dashboard

Step 1

From the Cisco DNA Center home page, choose Assurance > Dashboards > Dashboard Library. The Dashboard Library window appears, listing all the defined dashboards.
Create a Custom Dashboard

Figure 20: Dashboard Library Window

Step 2  Click located in the top-right corner.

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 this dashboard.
b)  Check the check box next to the dashlet you want to add to your dashboard.

   Note  You can search for a dashlet by choosing a category from the drop-down list or using the search box at the right.

c)  Click Add to include the dashlet to 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 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 8  Click Save to save the dashboard.
A confirmation dialog is displayed.
Create a Dashboard From a Template

Creating a dashboard from a template allows you to use scope to filter the dashboard data. Scope filters devices by location, device type, and other options.

**Step 1**
From the Cisco DNA Center home page, choose Assurance > Dashboards > 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.
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.
- **HostName**: Enter the host names 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.
- **IPAddress**: 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.
- **IPAddress**: 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 host names 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.
A confirmation dialog is displayed.

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 From the Cisco DNA Center home page, choose Assurance > Dashboards > 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 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 From the Cisco DNA Center home page, choose Assurance > Dashboards > 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** From the Cisco DNA Center home page, choose **Assurance > Dashboards > 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 on 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** From the Cisco DNA Center home page, choose **Assurance > Dashboards > 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:

- From the Cisco DNA Center home page, choose **Assurance > Dashboards > Health > Overall Health**.

  The **Overall Health** dashboard appears.
• From the Cisco DNA Center home page, choose **Assurance > Dashboards > Health > Network Health.**
  The **Network Health** dashboard appears.

• From the Cisco DNA Center home page, choose **Assurance > Dashboards > Health > Client Health.**
  The **Client Health** dashboard appears.

• From the Cisco DNA Center home page, choose **Assurance > Dashboards > Health > Application Health.**
  The **Application Health** dashboard appears.

**Step 2**  Click **Actions** (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.**
View and Manage Issues

- About Issues, on page 199
- About Machine Reasoning Engine and the Layer 2 Loop Issue, on page 200
- View Open Issues, on page 200
- View Resolved Issues, on page 209
- View Ignored Issues, on page 210
- Manage Issue Settings, on page 212
- Enable Issue Notifications, on page 213
- Assurance and Cisco AI Network Analytics Issues, on page 214

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, Release 1.3.1.0, 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:


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

Note

Cisco DNA Center, Release 1.3.0 introduced limited on-appliance Cisco AI Network Analytics capabilities for excessive onboarding time. So even if you have not installed the Cisco AI Network Analytics application with the Cisco DNA Center, Release 1.3.1.0, you can still view some of the AI-driven on-prem issues that are available since Cisco DNA Center, Release 1.3.0.
About Machine Reasoning Engine and the Layer 2 Loop Issue

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.

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.

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. The list of open issues that appear 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, Release 1.3.1.0, you can view the following types of cloud-based AI-driven issues:


  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, and Social Application Throughput.
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.

**Note**
Cisco DNA Center, Release 1.3.0 introduced limited on-appliance Cisco AI Network Analytics capabilities for excessive onboarding time. So even if you have *not installed* the Cisco AI Network Analytics application with the Cisco DNA Center, Release 1.3.1.0, you can still view some of the AI-driven on-prem issues that are available since Cisco DNA Center, Release 1.3.0.


**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 74.
- To view syslog messages, make sure that you have configured Optimal Visibility or Maximal Visibility telemetry profile on the device. See the "Configure a Telemetry Profile" topic in the 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.
- From the Cisco DNA Center home page, choose **Assurance** > **Dashboards** > **Issues** > **Open**.

The Open Issues window appears with the following information:
### Open Issues Window

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global</strong></td>
<td>Allows you to display information on the window based on the location you select. Default is Global. To change the location, do the following:</td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Global</strong>. The Site/Building/Floor table is displayed.</td>
</tr>
<tr>
<td></td>
<td>b. Choose the <strong>Hierarchical Site View</strong> or <strong>Building View</strong> from the drop-down list. Based on what you choose, the table is refreshed.</td>
</tr>
<tr>
<td></td>
<td>c. To view information about a specific site, building, or floor, click <strong>Apply</strong> in the appropriate row; information in the <strong>Open Issues</strong> window is refreshed based on your selection.</td>
</tr>
<tr>
<td><strong>24 Hours</strong> drop-down list</td>
<td>Allows you to display information on the window based on the time range you select. Default is 24 Hours. Do the following:</td>
</tr>
<tr>
<td></td>
<td>a. From the 24 Hours drop-down list, choose a time range: 3 hours, 24 hours, or 7 days.</td>
</tr>
<tr>
<td></td>
<td>b. Specify the <strong>Start Date</strong> and time; and the <strong>End Date</strong> and time.</td>
</tr>
<tr>
<td></td>
<td>c. Click <strong>Apply</strong>. This sets the range of the timeline.</td>
</tr>
<tr>
<td><strong>Most Impacted Areas</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
Open Issues Window

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeline Slider</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td><em>P1</em></td>
</tr>
<tr>
<td></td>
<td><em>P2</em></td>
</tr>
<tr>
<td></td>
<td><em>P3 and P4</em></td>
</tr>
<tr>
<td>Note</td>
<td>The intensity of the color indicates its significance, whether more or less issues have occurred for that priority level. For example, a lighter shade of yellow indicates less P2 issues (still open) than a deeper shade of yellow.</td>
</tr>
<tr>
<td>Total Open</td>
<td>Provides the total count of open issues that require action. The <strong>Total Open</strong> value changes depending on the tab you choose. Options are <strong>All</strong>, <strong>P1</strong>, <strong>P2</strong>, <strong>P3</strong>, <strong>P4</strong>, and <strong>AI-Driven</strong>. Default is <strong>All</strong>.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Preassigned priority level of the issue type.</td>
</tr>
<tr>
<td>Issue Type</td>
<td>Type of issue. For AI-driven issues, the icon appears in front of the issue type.</td>
</tr>
<tr>
<td>Device Role</td>
<td>Role assigned to the device on which the issue was detected. Can be one of the following: Access, Core, Distribution, Border Router, or Unknown.</td>
</tr>
<tr>
<td>Category</td>
<td>Category under which the issue type falls. For example, Connectivity, Availability, Onboarding, Utilization, and so on.</td>
</tr>
<tr>
<td>Issue Count</td>
<td>Number of times this type of issue has occurred.</td>
</tr>
<tr>
<td>Site Count (Area)</td>
<td>Number of sites where this type of issue occurred.</td>
</tr>
<tr>
<td>Device Count</td>
<td>Number of devices that were impacted by this type of issue.</td>
</tr>
<tr>
<td>Last Occurred Time</td>
<td>Most recent date and time this issue occurred.</td>
</tr>
</tbody>
</table>

**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)**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Issues</td>
<td>Number of open issues for that issue type.</td>
</tr>
<tr>
<td>Area</td>
<td>Number of buildings and floors that are impacted by the issue.</td>
</tr>
<tr>
<td>Device</td>
<td>Number of devices that are impacted by the issue.</td>
</tr>
<tr>
<td>Issue</td>
<td>Description of the issue.</td>
</tr>
<tr>
<td>Site</td>
<td>Site, building, or floor that was impacted by the issue.</td>
</tr>
<tr>
<td>Device</td>
<td>Device that was impacted by the issue.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Type of device that was impacted by the issue.</td>
</tr>
<tr>
<td>Issue Count</td>
<td>Number of times this type of issue occurred.</td>
</tr>
<tr>
<td>Last Occurred Time</td>
<td>Date and time this issue occurred.</td>
</tr>
</tbody>
</table>

**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 along with 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 204.

For Layer 2 Loop issue, which supports Machine Reasoning, the **Issue Instance Details** slide-in pane contains specific information. See **Issue Instance Details for Layer 2 Loop Issue**, on page 207.

---

**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 200.

For AI-Driven issues, the **Issue Instance Details** (second slide-in pane) provides the following information:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Description of the issue.</td>
</tr>
</tbody>
</table>
## Issue Instance Details (Second Slide-In Pane)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong> drop-down list</td>
<td>Allows you to change the status of the issue. Do the following:</td>
</tr>
<tr>
<td>• To resolve an issue, from the <strong>Status</strong> drop-down list, choose <strong>Resolve</strong>.</td>
<td></td>
</tr>
<tr>
<td>• To stop an issue from being reported, do the following:</td>
<td></td>
</tr>
<tr>
<td>1. From the <strong>Status</strong> drop-down list, choose <strong>Ignore</strong>.</td>
<td></td>
</tr>
<tr>
<td>2. Set the number of hours to ignore the issue on the slider, and then click <strong>Confirm</strong>.</td>
<td></td>
</tr>
<tr>
<td><strong>Summary area</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Impacted Summary for this Network</strong></td>
<td>Displays information about the location that was impacted and the number of clients that were impacted by the issue.</td>
</tr>
<tr>
<td><strong>Feedback icon</strong></td>
<td>Click the icon to provide your comments, whether the information on this page was helpful or not, and then click <strong>Submit</strong>.</td>
</tr>
<tr>
<td><strong>Problem</strong></td>
<td>Provides a brief text that describes the problem along with a chart that provides a visual of how the actual KPI value has deviated from the predicted normal behavior.</td>
</tr>
<tr>
<td></td>
<td>By default, the chart is zoomed-in, 6-hours before and 6-hours after the issue, as shown in the following figure:</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Figure 22: Problem Chart" /></td>
</tr>
<tr>
<td></td>
<td>The chart details for the AI-Driven issues are represented by different colors.</td>
</tr>
<tr>
<td>• <strong>Green band</strong>: Predicted normal behavior for your network based on machine learning.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Solid blue line</strong>: Actual KPI value.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Vertical red line or bars</strong>: Indicates an issue. When the blue line (actual KPI value) falls outside the green band (predicted normal behavior), an issue is raised.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Vertical yellow bars</strong>: Indicates that a similar event has occurred.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
### Issue Instance Details (Second Slide-In Pane)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</td>
<td>Provides information about the connected clients, APs, devices, and applications that are impacted by the issue. Contains tabs such as <strong>Connected Clients</strong>, <strong>Impacted APs</strong>, <strong>Device Breakout</strong>, <strong>Applications by TX/RX</strong>. Click the tab to update the chart and the table below the chart.</td>
</tr>
</tbody>
</table>
| 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 23: Root Cause Analysis Charts*

Contains tabs such as **Network Causes**, **Failed Distribution**, **Failed Percentage**, **Failed Count**. 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 Issue

The Issue Instance Details slide-in pane is part of the Open Issues workflow. See Step 4 in View Open Issues, on page 200.

To understand the Layer 2 Loop issue and the Machine Reasoning Engine, see About Machine Reasoning Engine and the Layer 2 Loop Issue, on page 200.

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

- Number of VLANS is 10.
- Number of devices per VLAN is 30.

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status drop-down list</td>
<td>Allows you to change the status of the issue. Do the following:</td>
</tr>
<tr>
<td></td>
<td>* To resolve an issue, from the Status drop-down list, choose Resolve.</td>
</tr>
<tr>
<td></td>
<td>* To stop an issue from being reported, do the following:</td>
</tr>
<tr>
<td></td>
<td>1. From the Status drop-down list, choose Ignore.</td>
</tr>
<tr>
<td></td>
<td>2. Set the number of hours to ignore the issue on the slider, and then click Confirm.</td>
</tr>
<tr>
<td>Summary</td>
<td>Brief summary of the issue, which can include information, such as device, role, time, location, and potential root cause. This also provides the initial assessment, such as the VLANs and ports in the potential loop.</td>
</tr>
<tr>
<td>Problem Details</td>
<td>Provides a brief text that describes the problem along with the following:</td>
</tr>
<tr>
<td></td>
<td>* Relevant Events drop-down list: Lists the events that occurred during the loop. Click an event to view details in the side pane.</td>
</tr>
<tr>
<td></td>
<td>* 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.</td>
</tr>
</tbody>
</table>
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 **thumbs up** icon to provide your feedback, whether the information on this page was helpful or not, and then click **Submit**.

5. Click the **Reasoning Activity** tab to understand how the MRE reached that conclusion. Each reasoning activity is provided in hexagon shaped blocks as shown in the following figure. Click each hexagon shaped block to view activity details in the right pane.

   To abort the reasoning activity while it is running, click **Stop**.

   **Note** The check mark indicates that the step is complete.

   ![Figure 24: Reasoning Activity](image)

6. Click **Run Again** if you want to rerun the MRE.

**Topology** icon

Click the **topology** icon to view the topology of the network segment in which the loop occurred.
View Resolved Issues

Use this procedure to view all resolved issues. The list of resolved 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 resolved issues, make sure that you have configured Cisco AI Network Analytics data collection. See Configure Cisco AI Network Analytics Data Collection, on page 74.

Step 1

From the Cisco DNA Center home page, choose Assurance > Dashboards > Issues > Resolved.

The Resolved Issues window appears with the following information:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>Allows you to display information on the window based on the location you select. Default is Global. To change the location, do the following:</td>
</tr>
<tr>
<td></td>
<td>a. Click Global. The Site/Building/Floor table is displayed.</td>
</tr>
<tr>
<td></td>
<td>b. Choose the Hierarchical Site View or Building View from the drop-down list. Based on what you choose, the table is refreshed.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>24 Hours drop-down list</td>
<td>Allows you to display information on the window based on the time range you select. Default is 24 Hours. Do the following:</td>
</tr>
<tr>
<td></td>
<td>a. From the 24 Hours drop-down list, choose a time range: 3 hours, 24 hours, or 7 days.</td>
</tr>
<tr>
<td></td>
<td>b. Specify the Start Date and time; and the End Date and time.</td>
</tr>
<tr>
<td></td>
<td>c. Click Apply.</td>
</tr>
<tr>
<td></td>
<td>This sets the range of the timeline.</td>
</tr>
<tr>
<td>Timeline slider</td>
<td>Allows you to specify a more granular time range. Click and drag the timeline boundary lines to specify the time range.</td>
</tr>
<tr>
<td>Total Resolved</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 Resolved Issues Window

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Preassigned priority level of the issue type.</td>
</tr>
<tr>
<td><strong>Issue Type</strong></td>
<td>Type of issue.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>For AI-driven issues, the 🤖 icon appears in front of the issue type.</td>
</tr>
<tr>
<td>Device Role</td>
<td>Role assigned to the device on which the issue was detected. Can be one of the following: Access, Core, Distribution, Border Router, or Unknown.</td>
</tr>
<tr>
<td>Category</td>
<td>Category under which the issue type falls. For example, Connectivity, Availability, Onboarding, Utilization, and so on.</td>
</tr>
<tr>
<td>Issue Count</td>
<td>Number of times this type of issue has occurred.</td>
</tr>
<tr>
<td>Site Count (Area)</td>
<td>Number of sites where this type of issue occurred.</td>
</tr>
<tr>
<td>Device Count</td>
<td>Number of devices that were impacted by this type of issue.</td>
</tr>
<tr>
<td>Last Occurred Time</td>
<td>Most recent date and time this issue occurred.</td>
</tr>
</tbody>
</table>

#### Step 3
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, and the time stamp of the last occurrence.

#### 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 along with suggested actions that might have been taken to resolve the issue 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 74**.

#### Step 1
From the Cisco DNA Center home page, choose **Assurance > Dashboards > Issues > Ignored**.
The **Ignored Issues** window appears with the following information:

<table>
<thead>
<tr>
<th><strong>Ignored Issues Window</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| 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 **EndDate** 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. |
| 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 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.

<table>
<thead>
<tr>
<th><strong>Issue Type Table in the Ignored Issues Window</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Priority</td>
<td>Preassigned priority level of the issue type.</td>
</tr>
</tbody>
</table>
| Issue Type                                    | Type of issue.  
  **Note** For AI-driven issues, the square 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. |
### Issue Type Table in the Ignored Issues Window

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Count</td>
<td>Number of devices that were impacted by this type of issue.</td>
</tr>
<tr>
<td>Last Occurred Time</td>
<td>Most recent date and time this issue occurred.</td>
</tr>
</tbody>
</table>

#### Step 3
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 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 along with suggested actions are displayed.

---

## 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
From the Cisco DNA Center home page, click the **Assurance** tab.

The **Overall Health** dashboard appears.

#### Step 2
Choose **Manage > Issue Settings**.

The **Issue Settings** window appears.

#### Step 3
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 4
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 ![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 only some issues) In the **Trigger Condition** area, you can change the threshold value for when the issue is reported.

Example of a trigger condition:

<table>
<thead>
<tr>
<th>Memory Utilization of Access Points greater than 90%</th>
</tr>
</thead>
</table>

**Note** For issues with multiple trigger conditions, the issue is reported when at least one of the trigger conditions is met.

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 5** Click **Manage Subscription** to subscribe to external notifications for supported issues when they are triggered. See Enable Issue Notifications, on page 213.

---

## 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** From the Cisco DNA Center home page, click the **Assurance** tab.

The **Overall Health** dashboard appears.

**Step 2** Choose **Manage > Issue Settings**.

The **Issue Settings** window appears.

**Step 3** Click **Manage Subscriptions**.

The **Events** window appears.

**Step 4** 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 5** Click **Subscribe**.

The **Subscribe** dialog box appears.

**Step 6** 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, Release 1.3.1.0*.

### Assurance and Cisco Al Network Analytics Issues

#### Router Issues

The following table lists the router issues detected by Assurance:

<table>
<thead>
<tr>
<th>Router Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category</strong></td>
</tr>
<tr>
<td>Connectivity</td>
</tr>
<tr>
<td>Connectivity</td>
</tr>
<tr>
<td>Connectivity</td>
</tr>
<tr>
<td>Connectivity</td>
</tr>
</tbody>
</table>
## Router Issues

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue Name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity</td>
<td>Network device interface connectivity - Interface down</td>
<td>Interface on device is down.</td>
</tr>
<tr>
<td>Connectivity</td>
<td>Network device interface connectivity - OSPF adjacency failure</td>
<td>OSPF (Open Shortest Path First) adjacency failed with neighbor.</td>
</tr>
<tr>
<td>Connected</td>
<td>Failure to install an access policy for SGT</td>
<td>Failure to install an SGACL access policy for SGT.</td>
</tr>
<tr>
<td>Connected</td>
<td>High input/output error on router interfaces</td>
<td>High input/output error on interfaces.</td>
</tr>
<tr>
<td>Connected</td>
<td>High input/output utilization on router interfaces</td>
<td>High input/output utilization on interfaces.</td>
</tr>
<tr>
<td>Connected</td>
<td>SGT access policy download failed on the device</td>
<td>Failed to download SGACL ACEs for SGT.</td>
</tr>
<tr>
<td>Connected</td>
<td>SGT access policy installation failed on the device</td>
<td>Failure to install an access policy for SGT. Policy rule error found in RBACL.</td>
</tr>
<tr>
<td>Connected</td>
<td>Unable to download SGT access policy from the policy server</td>
<td>Failure to download the source list for access policy for SGT.</td>
</tr>
<tr>
<td>Connected</td>
<td>Uninstall of SGT access policy failed on the device</td>
<td>Failure to uninstall an SGACL access policy for SGT.</td>
</tr>
<tr>
<td>Device</td>
<td>DNA Center and network device time has drifted</td>
<td>Excessive time lag between Cisco DNA Center and device.</td>
</tr>
<tr>
<td>Device</td>
<td>Issues based on syslog events - High temperature</td>
<td>Issues created by single occurrence of syslog event related to high temperature.</td>
</tr>
<tr>
<td>Device</td>
<td>Router experiencing high CPU utilization</td>
<td>Device experiencing high CPU utilization.</td>
</tr>
<tr>
<td>Device</td>
<td>Router experiencing high memory utilization</td>
<td>Device experiencing high memory utilization.</td>
</tr>
<tr>
<td>Availability</td>
<td>Network device HA switchover</td>
<td>The network device went through an HA switchover.</td>
</tr>
<tr>
<td>Availability</td>
<td>Router unreachable</td>
<td>Network device is unreachable from controller.</td>
</tr>
</tbody>
</table>
## Core, Distribution, and Access Issues

The following table lists the core, distribution, and access issues detected by Assurance:

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue Name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity</td>
<td>BGP tunnel connectivity</td>
<td>BGP connectivity failure with peer due to wrong AS (autonomous system) number.</td>
</tr>
<tr>
<td>Connectivity</td>
<td>Interface connecting network devices is down</td>
<td>Interface connecting network devices is down.</td>
</tr>
<tr>
<td>Connectivity</td>
<td>Layer 2 loop symptoms</td>
<td>Host MAC address flapping seen on network device.</td>
</tr>
<tr>
<td>Connectivity</td>
<td>Network device Interface connectivity - BGP Flap</td>
<td>BGP connectivity is flapping with neighbor.</td>
</tr>
<tr>
<td>Connectivity</td>
<td>Network device interface connectivity - Interface down</td>
<td>Interface on device is down.</td>
</tr>
<tr>
<td>Connectivity</td>
<td>Network device interface connectivity - OSPF adjacency failure</td>
<td>OSPF (Open Shortest Path First) adjacency failed with neighbor.</td>
</tr>
<tr>
<td>Connected</td>
<td>Fabric devices connectivity - Border overlay</td>
<td>Fabric edge lost connectivity to the fabric border in the virtual network.</td>
</tr>
<tr>
<td>Connected</td>
<td>Fabric devices connectivity - Border underlay</td>
<td>Fabric edge lost connectivity to the fabric border in the physical network.</td>
</tr>
<tr>
<td>Connected</td>
<td>Fabric devices connectivity - Control border underlay</td>
<td>Fabric node lost connectivity to the co-located fabric border and control plane in the physical network.</td>
</tr>
<tr>
<td>Connected</td>
<td>Fabric devices connectivity - Control underlay</td>
<td>Fabric node lost connectivity to the fabric control plane device in the physical network.</td>
</tr>
<tr>
<td>Connected</td>
<td>Fabric devices connectivity - DHCP overlay</td>
<td>Fabric node lost connectivity to the DHCP server in the virtual network.</td>
</tr>
<tr>
<td>Connected</td>
<td>Fabric devices connectivity - DHCP underlay</td>
<td>Fabric node lost connectivity to the DHCP server in the physical network.</td>
</tr>
<tr>
<td>Connected</td>
<td>Fabric devices connectivity - DNS overlay</td>
<td>Fabric node lost connectivity to the DNS server in the virtual network.</td>
</tr>
<tr>
<td>Connected</td>
<td>Fabric devices connectivity - DNS underlay</td>
<td>Fabric node lost connectivity to the DNS server in the physical network.</td>
</tr>
</tbody>
</table>
## Core, Distribution, and Access Issues

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue Name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>Fabric devices connectivity - External URL</td>
<td>The fabric border cannot reach the user-provisioned external URL.</td>
</tr>
<tr>
<td>Connected</td>
<td>Fabric devices connectivity - ISE server</td>
<td>Fabric edge lost connectivity to the ISE server in the physical network.</td>
</tr>
<tr>
<td>Connected</td>
<td>Failure to install an access policy for SGT</td>
<td>Failure to install an SGACL access policy for SGT.</td>
</tr>
<tr>
<td>Connected</td>
<td>High input/output error on switch interfaces</td>
<td>High input/output error on switch interfaces.</td>
</tr>
<tr>
<td>Connected</td>
<td>High input/output utilization on switch interfaces</td>
<td>High input/output utilization on interfaces.</td>
</tr>
<tr>
<td>Connected</td>
<td>SGTL access policy download failed on the device</td>
<td>Failed to download SGACL ACEs for SGT.</td>
</tr>
<tr>
<td>Connected</td>
<td>SGTL access policy installation failed on the device</td>
<td>Failure to install an access policy for SGT. Policy rule error found in RBACL.</td>
</tr>
<tr>
<td>Connected</td>
<td>Unable to download SGTL access policy from the policy server</td>
<td>Failure to download the source list for access policy for SGT.</td>
</tr>
<tr>
<td>Connected</td>
<td>Uninstall of SGTL access policy failed on the device</td>
<td>Failure to uninstall an SGACL access policy for SGT.</td>
</tr>
<tr>
<td>Device</td>
<td>Device reboot crash</td>
<td>Device has rebooted due to a hardware or software crash.</td>
</tr>
<tr>
<td>Device</td>
<td>Device time has drifted from DNAC</td>
<td>Excessive time lag between Cisco DNA Center and device.</td>
</tr>
<tr>
<td>Device</td>
<td>Interface is flapping on network device</td>
<td>A port interface is flapping on a switch.</td>
</tr>
<tr>
<td>Device</td>
<td>Issues based on syslog events - High temperature</td>
<td>Issues created by single occurrence of syslog event related to high temperature.</td>
</tr>
<tr>
<td>Device</td>
<td>Issues based on syslog events - POE</td>
<td>Issues created by single occurrence of syslog event related to power.</td>
</tr>
<tr>
<td>Device</td>
<td>Stack member removal</td>
<td>Stack member was removed.</td>
</tr>
<tr>
<td>Device</td>
<td>Stack member running incompatible image</td>
<td>Stack member is running an incompatible image.</td>
</tr>
<tr>
<td>Device</td>
<td>Switch experiencing high CPU utilization</td>
<td>Device experiencing high CPU utilization.</td>
</tr>
<tr>
<td>Device</td>
<td>Switch experiencing high memory utilization</td>
<td>Device experiencing high memory utilization.</td>
</tr>
<tr>
<td>Device</td>
<td>Switch fan failure</td>
<td>Fan failure on switch.</td>
</tr>
<tr>
<td>Device</td>
<td>Switch power failure</td>
<td>Power supply failure on switch.</td>
</tr>
</tbody>
</table>
Core, Distribution, and Access Issues

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue Name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>TCAM utilization high issues</td>
<td>Issues for TCAM exhaustion in layer 2, layer 3, QoS, and SGACL.</td>
</tr>
<tr>
<td>Availability</td>
<td>Network device HA switchover</td>
<td>The network device went through an HA switchover.</td>
</tr>
<tr>
<td>Availability</td>
<td>Switch unreachable</td>
<td>Device is unreachable.</td>
</tr>
<tr>
<td>Utilization</td>
<td>Map cache limit reached</td>
<td>Map cache entries have exceeded limit on map server.</td>
</tr>
</tbody>
</table>

Controller Issues

The following table lists the controller issues detected by Assurance:

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue Name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity</td>
<td>Interface connecting network devices is down</td>
<td>Interface connecting network devices is down.</td>
</tr>
<tr>
<td>Connected</td>
<td>Fabric WLC to MapServer connectivity</td>
<td>Fabric WLC lost connectivity to the fabric control plane node.</td>
</tr>
<tr>
<td>Device</td>
<td>Device time has drifted from DNAC</td>
<td>Excessive time lag between Cisco DNA Center and device.</td>
</tr>
<tr>
<td>Availability</td>
<td>Network device HA switchover</td>
<td>The network device went through an HA switchover.</td>
</tr>
<tr>
<td>Availability</td>
<td>WLC monitor</td>
<td>Network controller is not receiving data from WLC.</td>
</tr>
<tr>
<td>Availability</td>
<td>WLC power supply failure</td>
<td>Power supply has failed on this WLC.</td>
</tr>
<tr>
<td>Availability</td>
<td>WLC reboot crash</td>
<td>WLC reboot crash.</td>
</tr>
<tr>
<td>Availability</td>
<td>WLC unreachable</td>
<td>Device is unreachable.</td>
</tr>
<tr>
<td>Utilization</td>
<td>AP license exhausted on WLC</td>
<td>WLC currently has no free AP licenses.</td>
</tr>
<tr>
<td>Utilization</td>
<td>WLC memory high utilization</td>
<td>WLC is experiencing high memory utilization.</td>
</tr>
</tbody>
</table>

Access Point Issues

The following table lists the access point issues detected by Assurance:

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue Name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>AP coverage hole</td>
<td>AP has a coverage hole.</td>
</tr>
<tr>
<td>Availability</td>
<td>AP down</td>
<td>AP went down.</td>
</tr>
</tbody>
</table>
### Access Point Issues

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue Name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>AP flap</td>
<td>AP has flapped.</td>
</tr>
<tr>
<td>Availability</td>
<td>AP reboot crash</td>
<td>AP has rebooted due to a hardware or software crash.</td>
</tr>
<tr>
<td>Utilization</td>
<td>AP CPU high utilization</td>
<td>AP is experiencing high CPU utilization.</td>
</tr>
<tr>
<td>Utilization</td>
<td>AP memory high utilization</td>
<td>AP is experiencing high memory utilization.</td>
</tr>
<tr>
<td>Utilization</td>
<td>Radio high utilization (2.4GHz)</td>
<td>2.4 GHz radio on AP(s) are experiencing high utilization.</td>
</tr>
<tr>
<td>Utilization</td>
<td>Radio high utilization (5GHz)</td>
<td>5 GHz radio on AP(s) are experiencing high utilization.</td>
</tr>
<tr>
<td>AP Anomaly</td>
<td>AP anomaly</td>
<td>AP encountered anomaly issue.</td>
</tr>
</tbody>
</table>

### Wired Client Issues

The following table lists the wired client issues detected by Assurance:

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue Name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Onboarding</td>
<td>Client DHCP reachability issue</td>
<td>The client has failed to obtain an IPv4 address from DHCP server.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Client DNS reachability issue</td>
<td>The client failed to obtain a response from the DNS server.</td>
</tr>
</tbody>
</table>
| 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 clients. |
**Note** This issue is applicable only for single clients. |

### Wireless Client Issues

The following table lists the wireless client issues detected by Assurance:

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue Name</th>
<th>Summary</th>
</tr>
</thead>
</table>

**Note** These issues are applicable for both single clients and multiple clients.
## Wireless Client Issues

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue Name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Onboarding</td>
<td>802.11r client roaming slowly</td>
<td>While roaming, a wireless client capable of fast roaming is doing full authentication instead of fast authentication.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Client DHCP reachability issue</td>
<td>The client has failed to obtain an IPv4 address from DHCP server.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Client DNS reachability issue</td>
<td>The client failed to obtain a response from the DNS server.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client excluded - Client was excluded before roaming</td>
<td>Wireless client excluded - Client was excluded before roaming.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client failed to connect - AAA server timeout</td>
<td>Wireless client failed to connect - AAA server timeout.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client failed to connect - Client PMK not found</td>
<td>Wireless client failed to connect - Client PMK not found.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client failed to connect - Client timeout</td>
<td>Wireless client failed to connect - Failed to authenticate due to client timeout.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client failed to connect - DHCP server timeout</td>
<td>Wireless client failed to connect - DHCP server timeout.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client failed to connect - DHCP timeout</td>
<td>Wireless client failed to connect - DHCP timeout.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client failed to connect - Failed to get an IP address due to client timeout</td>
<td>Wireless client failed to connect - Failed to get an IP address due to client timeout.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client failed to connect - Incorrect PSK</td>
<td>Wireless client failed to connect and was excluded - The client's PSK did not match the configured WLAN PSK.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client failed to connect - WLC configuration error</td>
<td>Wireless client failed to connect - WLC configuration error.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client failed to connect - WLC internal error</td>
<td>Wireless client failed to connect - WLC internal error.</td>
</tr>
</tbody>
</table>
## Wireless Client Issues

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue Name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Onboarding</td>
<td>Wireless client failed to roam - Client PMK not found</td>
<td>Wireless client failed to roam - Client PMK not found.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client failed to roam - Client timeout</td>
<td>Wireless client failed to roam - Failed to authenticate due to client timeout.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client failed to roam - WLC configuration error</td>
<td>Wireless client failed to roam - WLC configuration error.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client failed to roam - WLC internal error</td>
<td>Wireless client failed to roam - WLC internal error.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client failed to roam between APs - External error</td>
<td>Wireless client failed to roam between APs - External error.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client failed to roam between APs - WLC configuration mismatch</td>
<td>Wireless client failed to roam between APs - WLC configuration mismatch.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client took a long time to connect - Excessive time due to authentication timeouts</td>
<td>Wireless client took a long time to connect - Excessive time due to authentication timeouts.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client took a long time to connect - Excessive time due to DHCP server failures</td>
<td>Wireless client took a long time to connect - Excessive time due to DHCP server failures.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client took a long time to connect - Excessive time due to failed credentials</td>
<td>Wireless client took a long time to connect - Excessive time due to failed credentials.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client took a long time to connect - Excessive time due to WLC failures</td>
<td>Wireless client took a long time to connect - Excessive time due to WLC failures.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless client took a long time to connect - Excessive time for authentication due to AAA server or network delays</td>
<td>Wireless client took a long time to connect - Excessive time for authentication due to AAA server or network delays.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless clients failed to connect - AAA server rejected clients</td>
<td>Wireless clients failed to connect - AAA server rejected clients.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless clients failed to connect - AAA server timeout</td>
<td>Wireless clients failed to connect - AAA server timeout.</td>
</tr>
<tr>
<td>Category</td>
<td>Issue Name</td>
<td>Summary</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless clients failed to connect - Client PMK not found</td>
<td>Wireless clients failed to connect - Client PMK not found.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless Clients failed to connect - DHCP server timeout</td>
<td>Wireless Clients failed to connect - DHCP server timeout.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless clients failed to connect - Failed to authenticate due to client timeouts</td>
<td>Wireless clients failed to connect - Failed to authenticate due to client timeouts.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless clients failed to connect - Failed to get an IP address due to client timeouts</td>
<td>Wireless clients failed to connect - Failed to get an IP address due to client timeouts.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless clients failed to connect - DHCP server or client timeouts</td>
<td>Wireless clients failed to connect - Failed to get an IP address due to DHCP server or client timeouts.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless clients failed to connect - Incorrect PSK</td>
<td>Wireless clients failed to connect and were excluded - The clients' PSK did not match the configured WLAN PSK.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless clients failed to connect - WLC configuration error</td>
<td>Wireless clients failed to connect - WLC configuration error.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless clients failed to roam - Client exclusion policies on the WLC</td>
<td>Wireless clients failed to roam - Clients were excluded due to client exclusion policies on the WLC.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless clients failed to roam - Clients were excluded before roaming</td>
<td>Wireless clients failed to roam - Clients were excluded before roaming.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless clients failed to roam - APs - WLC configuration mismatch</td>
<td>Wireless clients failed to roam between APs - WLC configuration mismatch.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless clients took a long time to connect - Excessive time due to DHCP server failures</td>
<td>Wireless clients took a long time to connect - Excessive time due to DHCP server failures.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless clients took a long time to connect - Failed credentials</td>
<td>Wireless clients took a long time to connect - Excessive time due to failed credentials.</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Wireless clients took a long time to connect - WLC failures</td>
<td>Wireless clients took a long time to connect - Excessive time due to WLC failures.</td>
</tr>
<tr>
<td>Connected</td>
<td>Dual band capable client prefers 2.4 GHz over 5 GHz</td>
<td>Dual band capable client is consistently connecting to 2.4 GHz radio even though 5 GHz radio, providing a better experience, is available.</td>
</tr>
<tr>
<td>Connected</td>
<td>Wireless client has poor RF</td>
<td>Wireless client is experience poor RF condition because the client has no better neighboring APs to roam to.</td>
</tr>
</tbody>
</table>
### Wireless Client Issues

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue Name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>Wireless client shows sticky behavior</td>
<td>Wireless client is maintaining an association with an AP which has a weaker signal. It should roam to available AP that has the stronger signal.</td>
</tr>
</tbody>
</table>

### Application Issues

The following table lists the application issues detected by Assurance:

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue Name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Application experience issues</td>
<td>All issues pertaining to Application Experience.</td>
</tr>
</tbody>
</table>

### Sensor Issues

The following table lists the sensor issues detected by Assurance:

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue Name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor Test</td>
<td>Sensor - Slow authentication during onboarding</td>
<td>Slow onboarding of sensors due to delays in the 802.1x authentication phase.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - RADIUS reachability slow</td>
<td>Multiple sensors are reporting slow ping response from RADIUS server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Speed test HTTP error</td>
<td>Multiple sensors are reporting speed test HTTP error while accessing query server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Default gateway failed</td>
<td>Multiple sensors are reporting no response from local gateway.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - DHCP failures</td>
<td>Multiple sensors failed to get an IPv4 address.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - DNS resolution failed</td>
<td>Multiple sensors failed to resolve domain name with DNS Server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - DNS server reachability failed</td>
<td>Multiple sensors reporting unreachable DNS server. Pings are failing.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - DNS server slow response</td>
<td>Multiple sensors are getting slow response from DNS Server host via ping.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Failed Association during Onboarding</td>
<td>Multiple sensors failed to associate during onboarding.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - First hop slow response</td>
<td>Multiple sensors are reporting slow ping responses from the local gateway.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - FTP reachability slow</td>
<td>Multiple sensors are reporting slow response from FTP server host.</td>
</tr>
</tbody>
</table>
## Sensor Issues

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue Name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor Test</td>
<td>Sensors - FTP test fail</td>
<td>Multiple sensors are reporting unable to connect to FTP server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - FTP transfer fail</td>
<td>Multiple sensors are reporting failed to transfer file with FTP server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - FTP transfer slow</td>
<td>Multiple sensors are reporting slow ftp transfer time with FTP server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - FTP unreachable</td>
<td>Multiple sensors are reporting unreachable FTP server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - IPSLA no IP address</td>
<td>Multiple sensors are reporting IPSLA test IP address not received from DNAC.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - IPSLA no response</td>
<td>Multiple sensors are reporting IPSLA test - no response from IPSLA responder.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - IPSLA socket error</td>
<td>Multiple sensors are reporting IPSLA test socket error.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - IPSLA test fail</td>
<td>Multiple sensors are reporting IPSLA test failed.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - IPSLA unsupported probe type</td>
<td>Multiple sensors are reporting IPSLA test unsupported probe type.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Mail server reachability slow</td>
<td>Multiple sensors are reporting slow ping response from mail server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Mail server response slow</td>
<td>Multiple sensors are reporting slow connection time to mail server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Mail server test fail</td>
<td>Multiple sensors are reporting failed to connect to mail server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Mail server unreachable</td>
<td>Multiple sensors are reporting unreachable mail server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - No NDT server</td>
<td>Multiple sensors are reporting speed test NDT server does not exist.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Onboarding failures</td>
<td>Sensors failed to connect to the wireless network.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Outlook server first hop slow</td>
<td>Multiple sensors are reporting slow response from Outlook Web Access first hop gateway.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Outlook server response slow</td>
<td>Multiple sensors are reporting slow mail connection time to Outlook Web Access.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Outlook server slow</td>
<td>Multiple sensors are reporting slow ping response from Outlook Web Access host.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Outlook server test fail</td>
<td>Multiple sensors are reporting failed to connect to Outlook Web Access.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Outlook server unreachable</td>
<td>Multiple sensors are reporting unreachable Outlook Web Access host.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Query server timeout</td>
<td>Multiple sensors are reporting speed test query server timeout.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - RADIUS authentication fail</td>
<td>Multiple sensors are reporting failed to authenticate with RADIUS server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - RADIUS authentication slow</td>
<td>Multiple sensors are reporting slow authentication time from RADIUS server.</td>
</tr>
</tbody>
</table>
## Sensor Issues

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue Name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor Test</td>
<td>Sensors - Slow association during onboarding</td>
<td>Slow onboarding of sensors due to delays in the association phase.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Slow DNS name resolution</td>
<td>Multiple sensors are getting slow name resolution from DNS server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Slow IPv4 addressing during onboarding</td>
<td>Multiple sensors are slow to get an IPv4 address.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Slow response from host</td>
<td>Multiple sensors are reporting slow ping response from host.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Speed test fail</td>
<td>Multiple sensors are reporting speed test failed.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Speed test generic error</td>
<td>Multiple sensors are reporting speed test generic failure.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Speed test uplink timeout</td>
<td>Multiple sensors are reporting speed test uplink test timeout.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Speed test URL error</td>
<td>Multiple sensors are reporting speed test URL error while accessing query server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Unreachable host</td>
<td>Multiple sensors are reporting ping failure to the host. Unreachable host.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Unreachable RADIUS</td>
<td>Multiple sensors are reporting unreachable RADIUS server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Web authentication config fail</td>
<td>Multiple sensors are reporting invalid web authentication configuration.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Web authentication fail</td>
<td>Multiple sensors are reporting clients are failing web authentication test.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Web authentication HTTP fail</td>
<td>Multiple sensors are reporting HTTP error for web authentication.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Web authentication slow</td>
<td>Multiple sensors are reporting slow web authentication.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Web server first hop slow</td>
<td>Multiple sensors are reporting slow response from web server first hop gateway.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Web server reachability slow</td>
<td>Multiple sensors are reporting slow ping response from web server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Web server response slow</td>
<td>Multiple sensors are reporting slow web response time from web server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Web server test failed</td>
<td>Multiple sensors are reporting failed to load page from web server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Web server unreachable</td>
<td>Multiple sensors are reporting unreachable web server.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Web socket error</td>
<td>Multiple sensors are reporting speed test websocket error during the test.</td>
</tr>
<tr>
<td>Sensor Test</td>
<td>Sensors - Speed test uplink proxy error</td>
<td>Multiple sensors are reporting speed test uplink test proxy error.</td>
</tr>
</tbody>
</table>
Al-Driven Issues

The following table lists the Al-Driven issues detected by Cisco AI Network Analytics:

<table>
<thead>
<tr>
<th>Al-Driven Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category</strong></td>
</tr>
<tr>
<td><strong>Connection Issues</strong></td>
</tr>
<tr>
<td>Onboarding</td>
</tr>
<tr>
<td>Onboarding</td>
</tr>
<tr>
<td>Onboarding</td>
</tr>
<tr>
<td>AAA</td>
</tr>
<tr>
<td>AAA</td>
</tr>
<tr>
<td>AAA</td>
</tr>
<tr>
<td>AAA</td>
</tr>
<tr>
<td>DHCP</td>
</tr>
<tr>
<td>DHCP</td>
</tr>
<tr>
<td><strong>Network Connectivity Issue</strong></td>
</tr>
<tr>
<td>Connectivity</td>
</tr>
<tr>
<td><strong>Application Experience Issues</strong></td>
</tr>
<tr>
<td>Throughput</td>
</tr>
<tr>
<td>Throughput</td>
</tr>
<tr>
<td>Category</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>Throughput</td>
</tr>
<tr>
<td>Throughput</td>
</tr>
</tbody>
</table>
Observe Network Trends and Gain Insights

• About Network Trends and Insights, on page 229
• View Network Trends and Obtain Insights, on page 229
• Compare Access Points in Network Heatmaps, on page 232
• Compare KPI Values with Peers in Your Network, on page 234
• Compare a Site with Another Site in Your Network, on page 235

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 Site Comparisons**: Determine how a site (building) is performing compared to another site in your network for a selected KPI.

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**

Do one of the following:

- From the Cisco DNA Center home page, in the Assurance Summary > Trends and Insights area, choose **View Details**.
- From the Cisco DNA Center home page, choose Assurance > Trends and Insights > Network Insights.

The Network Insights window appears with three tabs: **Capacity**, **Coverage**, and **Throughput**. The Capacity tab is selected by default with the following information:

<table>
<thead>
<tr>
<th>Insights Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Occurrence</strong></td>
<td>Time duration when this trend was observed. For example, May 27 - June-03-2019.</td>
</tr>
<tr>
<td><strong>Insight</strong></td>
<td>List of all the AI-Driven insights that were observed during a specific time period.</td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td>Category under which the insight was observed. Can be one of the following: <strong>Capacity</strong>, <strong>Coverage</strong>, and <strong>Throughput</strong>.</td>
</tr>
<tr>
<td><strong>Frequency band</strong></td>
<td>Band frequency that was used on the AP on which the insight was observed. Can be <strong>2.4 GHz</strong>, <strong>5 GHz</strong>, or both band frequencies.</td>
</tr>
<tr>
<td><strong>KPI</strong></td>
<td>Key Performance Indicator (KPI) for that specific insight.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Allows you to customize the columns that you want displayed in the Insights table. Click the <img src="image" alt="icon" /> icon, uncheck the check box for the column that you do not want displayed, and then click <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>

**Step 2**

From the **Insight** column, click an insight to open a slide-in pane, which provides the following information:

<table>
<thead>
<tr>
<th>Insight Details Slide-In Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco AI</strong></td>
<td>Provides information about how the insights are computed.</td>
</tr>
<tr>
<td><strong>Insight Summary</strong></td>
<td>A brief summary about the trend that is observed in the Beeswarm chart below. The summary provides information such as the name of the Site or AP, client count, the radio band frequency, and the time period during which the deviation was observed.</td>
</tr>
<tr>
<td><strong>Weekly Client Load</strong></td>
<td>Client load per week.</td>
</tr>
<tr>
<td><strong>Troubleshoot</strong></td>
<td>Links to the Network Heatmap and the AP 360 page, which allow you to troubleshoot and fix the trend before it becomes a critical issue.</td>
</tr>
<tr>
<td><strong>Issue Count</strong></td>
<td>Issue count gradient.</td>
</tr>
</tbody>
</table>
### Insight Details Slide-In Pane

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chart</td>
<td>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 and 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.</td>
</tr>
</tbody>
</table>

#### Figure 25: Beeswarm Chart

- 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 and the large circle has a higher client count.

### Step 3

Hover your cursor over a circle in the chart to get 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 will see information, such as the building in which the trend was observed and the client count.
Compare Access Points in Network Heatmaps

Use this procedure to visually compare all of the APs in your network for a given month in a heatmap 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**
From the Cisco DNA Center home page, choose **Assurance > Trends and Insights**.

**Step 2**
From the **Trends and Insights** drop-down list, choose **Network Heatmap**.

The **Network Heatmap** window appears with the following information:

*Figure 26: Network Heatmap Window*
## Network Heatmap Window

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Period</td>
<td>Displays the month for which the heatmap is displayed.</td>
</tr>
<tr>
<td>KPI drop-down list</td>
<td>Displays information in the heatmap for the KPI you choose from the drop-down list. Default is Client Count.</td>
</tr>
<tr>
<td>Band</td>
<td>Displays information in the heatmap for the band frequency you choose. Options are: All, 2.4 GHz, and 5 GHz. Default is All.</td>
</tr>
</tbody>
</table>
| 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. |
| KPI gradient                | Depending on the KPI you choose from the KPI drop-down list, this area provides information about the performance of that 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. |
| Network Daily Max graph     | Provides a graph that shows you the network daily average percentage for all APs on a specific day. The AP that has the highest daily average score (busiest day) is highlighted. |
| 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: Depending on the band frequency you choose from the Band options, this area lists the band frequency that was used by the clients.  
  • AP Heatmap: Allows you to determine how the APs are behaving historically: 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.  
  • AP Daily Average: Average KPI score for that AP. |

### Step 3
Hover your cursor over the bar on the Network Daily Max graph to view the KPI value for each day.

### Step 4
Hover your cursor over a color block in the Heatmap to get information, such as the name and MAC address of the AP, the band frequency, the AP group, the location of the AP, and the daily average KPI score.

### Step 5
Hover your cursor over the AP Daily Average area to determine the average KPI value for an AP during the time period.

### Step 6
To view the heatmap data for additional radios, scroll down to the bottom of the window, and then 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 in comparison to your peer networks for a selected Key Performance Indicators (KPI).

**Step 1**  
From the Cisco DNA Center home page, choose **Assurance > Trends and Insights**.

**Step 2**  
From the **Trends and Insights** drop-down list, choose **Peer Comparison**.

The **Peer Comparison** window appears with the following information:

<table>
<thead>
<tr>
<th><strong>Peer Comparison Window</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
</tr>
<tr>
<td>KPI drop-down list</td>
</tr>
<tr>
<td>Show</td>
</tr>
</tbody>
</table>
| Summary                   | AI Network Analytics analyzes the bar graphs and provides a brief summary about the findings. Provides the following information:  
|                           | • **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           | Allows you to toggle between your network and the peer network graphs. |
Compare a Site with Another Site in Your Network

Use this procedure to determine how a site (building) is performing compared to another site in your network for a selected Key Performance Indicator (KPI). The KPIs with which you can compare the performance of the two sites are: Radio Throughput, Client RSSI, and Average Onboarding Time. This procedure allows you to determine the number of APs in a site that are seeing good, ok, or bad performance.

**Step 1**
From the Cisco DNA Center home page, choose **Assurance > Trends and Insights**.

**Step 2**
From the **Trends and Insights** drop-down list, choose **Site Comparison**.

The **Site Comparison** window appears with the following information:
Figure 28: Site Comparison Window

<table>
<thead>
<tr>
<th>Client RSSI</th>
<th>Frequency band</th>
<th>Building 1</th>
<th>Building 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2.4 GHz, 5 GHz</td>
<td>BLD-9DXQ</td>
<td>BLD-6zOo</td>
</tr>
</tbody>
</table>

**SUMMARY**

In the week between Aug 06, 2019 and Aug 12, 2019, radios within the 2.4 GHz frequency band in buildings BLD-9DXQ and BLD-6zOo have been divided into three groups based on Client RSSI.

- **48.5% of radios** in BLD-9DXQ were in the lower Client RSSI group.
- **63.5% of radios** in BLD-6zOo were in the medium Client RSSI group.

**Client RSSI groups over the past week in BLD-9DXQ and BLD-6zOo**

- **Lower Client RSSI**
- **Medium Client RSSI**
- **Higher Client RSSI**

**BLD-9DXQ**

- Client count:
  - Up to ~15

**BLD-6zOo**

- Client count:
  - Up to ~5

**Groups of radios and devices are created in your network based on performance metrics over the past week. Learn More.**

BLD-9DXQ has a larger proportion of radios (14 of 16) in this group than BLD-50X2 (20 of 26).

BLD-6zOo has a larger proportion of radios (9 of 20) in this group than BLD-6zOo (2 of 16).
## Site Comparison Window

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clustering KPI</strong> drop-down list</td>
<td>Choose a KPI from the drop-down list. Options are: Radio Throughput, Client RSSI, and Average Onboarding Time. Default is Radio Throughput.</td>
</tr>
<tr>
<td><strong>Frequency Band</strong></td>
<td>Allows you to choose the band frequency. Options are: Band 2.4 GHz and Band 5 GHz.</td>
</tr>
<tr>
<td><strong>Building 1</strong> drop-down list</td>
<td>Choose the first site for which you want to compare the KPI values.</td>
</tr>
<tr>
<td><strong>Building 2</strong> drop-down list</td>
<td>Choose the second site with which you want to compare the KPI values of the first site.</td>
</tr>
<tr>
<td><strong>Timeline</strong></td>
<td>Displays the performance of the AP clusters for each day of the week.</td>
</tr>
<tr>
<td><strong>Client Count or Device Count</strong></td>
<td>For the Radio Throughput and Client RSSI KPIs, this area provides the client count per radio for each of the sites.</td>
</tr>
<tr>
<td></td>
<td>For the Average Onboarding Time KPI, this area provides the number of devices for each of the sites.</td>
</tr>
</tbody>
</table>
| **AP Clusters or Device Type Clusters** | • For the Radio Throughput and Client RSSI KPIs, this area displays two sets of AP clusters, one for each site. From this area you can visually compare the performance of the two sites. It provides the following information:  
  • How the APs are clustered in each site.  
  • The number of APs that are seeing low, medium, and high KPI values.  
  • The KPI performance in percentage (provided above the AP clusters).  
  • For the Average Onboarding Time KPI, 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. |  

---

**Step 3**

For the Radio Throughput and Client RSSI KPIs, hover your cursor on an AP in the AP clusters area to view the AP name and the client count for that AP.
Compare a Site with Another Site in Your Network
CHAPTER 16

Schedule Reports

Use Cisco DNA Center platform to sample and schedule reports. For details, see the Cisco DNA Center Platform User Guide.

• Working with Data and Reports, on page 239
• Sample and Schedule Reports, on page 240
• Review My Downloads, on page 243

Working with Data and Reports

You can utilize data from the Data and Reports feature in the Cisco DNA Center platform 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 also easily customized to meet your operational needs.

Figure 29: Cisco DNA Center Platform Data and Reports Window

The Data and Reports feature supports the following use cases:

• Capacity planning: Understanding how devices within your network are being utilized.
Sample and Schedule Reports

Perform this procedure to configure specialized data reports about your network. You can configure data reports using the Data and Reports window in the Cisco DNA Center GUI.

Before you begin

- Run a successful Discovery job in Cisco DNA Center to configure and schedule reports about device and network data. You can check whether a Discovery job is successful in Device Inventory. From the Home page, choose Provision > Device Inventory > Inventory to view discovery results.

Step 1

From the Cisco DNA Center Home page perform one of the following tasks:

- At the top of the page, choose the Platform tab > Developer Toolkit > Data and Reports.
• Under the **Platform** header (*Network Configuration* field), click **Schedule and Download Data and Reports**.

• At the bottom of the page, under **Tools**, click **Data and Reports**.

The **Catalog** view is the default window for **Data and Reports** and should appear. If it does not appear, click **Catalog** underneath the **Data and Reports** header.

**Step 2**

Review the **Catalog** window.

The **Catalog** window displays supported reporting categories called **catalogs items**. Each catalog item is represented by a tile and contain links to both a sample report and to configure (schedule) a report.

**Step 3**

Determine which catalog item you wish to create a report about in the **Catalog** window.

**Step 4**

In the catalog item tile, click **Sample** to view a sample report.

A **Preview** window appears for the sample report. Use the side bar in the window to scroll down and review the entire sample report. The following data is presented:

• Applied filters (data filters that were used to build the report).

• Graphical representation of the data (including line, bar, and pie graphs).

• Tables that assist you in analyzing the data.

**Note**

You can use the sample report in the **Preview** window to plan how you want your report to look.

**Step 5**

Click **X** to close the preview.

**Step 6**

In the catalog item tile, click **Schedule** to configure parameters to build a report.

The **Schedule** window opens where you can apply filters for data for your reports, as well as set up schedules for the actual report generation.

**Step 7**

In the **Schedule** window, configure the parameters to build your report.

The **Schedule** window is divided into the following fields:

• **Format**: Accept the default report name or create a new one, choose the data type (if there is more than one option for data type), and choose the file type (if there is more than one option for file type).

• **Filters**: Choose the filters for your the data in your report.

• **Schedule**: Choose the date and time for the report generation.

• **Send to**: Enter an email address to send an email with a link for downloading the report.

**Step 8**

In the **Report Name** field, accept the default report name or enter a new one.

**Step 9**

In the **Type** field, click a data type.

For SWIM and Inventory reports, there will not be a data type choice. **All Data** is the default. For Client reports, you can select one of the following:

• **Client Summary**

• **Top N Summary**

• **Client Detail**
Step 10  In the **File Type** field, choose a file type for the complete report.

Depending upon the report that you are creating, the following **File Type** options may be available:

- PDF
- CSV
- Tableau Data Extract
- JSON

For the CSV, JSON, and Tableau Data Extract file types, a **Fields** option will display that permits you to select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Step 11  (Optional) Choose the attribute (fields) for the report.

**Note** For SWIM data and reports, you can select specific fields for both the CSV and Tableau Data Extract file types. For Client data and reports, you can select **Client Detail** and then select specific fields for the CSV, Tableau Data Extract, and JSON file types. For Inventory data and reports, you can select specific fields for both the CSV and Tableau Data Extract file types.

Step 12  If required, choose the **Data Filters** for your report.

The **Data Filters** vary depending upon the type of report you are configuring.

Step 13  In the **Schedule** field, configure a schedule for the report.

The following **Schedule** options are available:

- Schedule Now
- Schedule for Later
- Reoccurring Schedule

Step 14  Enter an email address in the **Send to** field to send out email notifications for the report.

Cisco DNA Center will send out the following email notifications for the report:

- Report is in the queue waiting to be processed.
- Report processing is in progress.
- Report has successfully been compiled and is completed.

The email notification of a successfully compiled report will have a link back to itself and the **My Downloads** page under **Data and Reports**. You can view and download the report from this link and location.

**Note** You must have the appropriate Cisco DNA Center user permissions to view and download the report from the email.

Step 15  Click the **Schedule** button.

The **My Downloads** window opens with instance details of the report that was scheduled.
What to do next

Proceed to review your report instance in My Downloads window.

---

Note

You can download, review, edit, duplicate, or delete the report in the My Downloads window.

---

Review My Downloads

Perform this procedure to download, review, edit, duplicate, or delete a previously generated report.

Before you begin

- Run a successful Discovery job in Cisco DNA Center to configure and schedule reports about device and network data. You can check whether a Discovery job is successful in Device Inventory. From the Home page, click Provision > Device Inventory > Inventory to view discovery results.
- Create a report using the Schedule functionality in the Catalog.

Figure 31: My Reports Tab Window

Step 1

From the Cisco DNA Center home page perform one of the following tasks:

- At the top of the page, choose the Platform tab > Developer Toolkit > Data and Reports.
- Under the Platform header (Network Configuration field), click Schedule and Download Data and Reports.
- At the bottom of the page, under Tools, click Data and Reports.
The Catalog view is the default window for Data and Reports and should appear. If it does not appear, click Catalog underneath the Data and Reports header.

**Step 2**
Click the My Downloads tab.

The following information is displayed:

- **Name**: Name of the report.
  
  If you did not give the report a name, then a default name is given to the report that contains the report type with the date and time of the report.

- **Report Type**: Type of report based upon the catalog options (Client, SWIM, Inventory).

- **File Type**: File format type, for example a PDF or CSV file format.

- **Schedule**: Description of the schedule that generated the report.

- **Last Execution Status**: Displays report execution status and details. The following report execution status types may be displayed:
  
  - **Not Initiated**: Report scheduled but not yet started.
  - **In Queue**: Report scheduled and in the processing queue to be executed.
  - **In Progress**: Report currently being executed.
  - **Completed**: Report execution completed. Clicking on the icon (downward pointing arrow) next to Completed downloads the last generated report.
  - **Expired**: Report expired and no longer available in Cisco DNA Center.
  - **Error**: Report execution failed.

- **Reports**: Number of reports up to a total of 7.
  
  Hover (mouse) over the displayed report number and View Report List appears. Click View Report List to display a reports dialog box. The reports dialog box lists all of the report executions, their status (Not Initiated, In Queue, In Progress, Completed, Expired, and Error) and a Download button to download a copy. Clicking Error displays any errors and warnings for the report execution.

**Important**
Cisco DNA Center platform retains a total of 7 reports. Specifically, Cisco DNA Center platform retains the last 7 reports executed, as well as the last 7 reports executed over the last 7 days (week). For example, if you run 8 reports in a single day, Cisco DNA Center platform will only retain the last 7 reports. If you schedule 1 report for each day, then Cisco DNA Center platform will only keep the most recent 7 reports over the last 7 days (week). You can also export the reports in their various formats from the Cisco DNA Center platform and archive them to a safe location.

- **Actions**: List of tasks you can perform with the reports.

  You can adjust the downloads that are displayed in the GUI by clicking the Filter icon and using the filter, or entering a keyword in the Find field.

**Step 3**
Click Actions to perform one or more of the following tasks:

- **View Config**: Opens a window where the configured parameters for the report are displayed (including the schedule). You can review the configured report parameters in this window. You cannot make any changes to the report.
configuration in this window. This is a read-only view. If you need to edit the configuration, then click Actions > Edit. You can both view and edit a report configuration by clicking Edit.

- **Edit**: Opens a window where configured parameters for the report are displayed (including the schedule). You can review the parameters and also edit them in this window. Click Update Schedule after making any edits to the report.

**Important** Once you edit and update the report configuration, any future report executions will reflect this new configuration. This is important if reports are being generated on a reoccurring schedule. Additionally, if you edit and update a report configuration, all the previous reports in Cisco DNA Center platform will be deleted. The GUI will display a warning about the deletion when clicking the Update Schedule button in the window. You do not have to make any edits in the configuration to click the Update Schedule button and delete all previous reports.

- **Duplicate**: Opens the Schedule window where you can either view or configure the parameters for the report. Click Schedule to generate the report again.

  **Note** If you want to create a new report based upon an existing report and its configuration, then use the Duplicate option and make changes to the configuration. This will permit you to create a new report similar to the existing one, while retaining the existing report and its configuration. If you want to discard the existing report and completely replace it with a new report, then use the Edit option as described above.

- **Run Now**: Starts the process to execute the report. A success message appears after a successful report execution.

  **Note** If you try to execute a report and there are 7 previous reports, then the GUI displays a warning that only the last 7 reports are saved. You use the Run Now option when you need to generate a report outside of an existing schedule for the reports.

- **Delete**: Deletes the report. You are prompted to confirm this action before the report is deleted.
CHAPTER 17

Troubleshoot Cisco DNA Center Using Data Platform

- About Data Platform, on page 247
- Troubleshoot Using the Analytics Ops Center, on page 248
- View or Update Collector Configuration Information, on page 249
- View Data Retention Settings, on page 250
- View Pipeline Status, on page 251

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 248.

- **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 249.

- **Store Settings**: Allows you to specify how long data is stored for an application. See View Data Retention Settings, on page 250.

- **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 251.
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**
From the Cisco DNA Center home page, click the gear icon ⚙ and choose **System Settings > 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**  
From the Cisco DNA Center home page, click the gear icon 🛠 and choose System Settings > 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.
For COLLECTOR-ISE configuration, see Configure Cisco DNA Center for Cisco ISE Integration, on page 63.

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:

```
[lifecycle]
...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
From the Cisco DNA Center home page, click the gear icon and choose System Settings > 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**
From the Cisco DNA Center home page, click the gear icon and choose **System Settings > 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.
View Pipeline Status
Related Documentation

We recommend that you read the following documents relating to Cisco DNA Center:

<table>
<thead>
<tr>
<th>For This Type of Information...</th>
<th>See This Document...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release information, including new features, system requirements, and open and resolved bugs.</td>
<td>Cisco DNA Center Release Notes</td>
</tr>
<tr>
<td>Installation and configuration of Cisco DNA Center, including postinstallation tasks.</td>
<td>Cisco DNA Center Installation Guide</td>
</tr>
<tr>
<td>Upgrade information for your current release of Cisco DNA Center.</td>
<td>Cisco DNA Center Upgrade Guide</td>
</tr>
<tr>
<td>Use of the Cisco DNA Center GUI and its applications.</td>
<td>Cisco DNA Center User Guide</td>
</tr>
<tr>
<td>Configuration of user accounts, security certificates, authentication and password policies, backup and restore, and global discovery settings.</td>
<td>Cisco DNA Center Administrator Guide</td>
</tr>
<tr>
<td>Supported devices, such as routers, switches, wireless access points, and software releases.</td>
<td>Supported Devices</td>
</tr>
<tr>
<td>Hardware and software support for Cisco SD-Access.</td>
<td>Cisco SD-Access Hardware and Software Compatibility Matrix</td>
</tr>
<tr>
<td>Use of the Cisco DNA Assurance GUI.</td>
<td>Cisco DNA Assurance User Guide</td>
</tr>
<tr>
<td>Licenses and notices for open source software used in Cisco DNA Assurance.</td>
<td>Open Source Used in Cisco DNA Assurance</td>
</tr>
<tr>
<td>Use of the Cisco DNA Center platform GUI and its applications.</td>
<td>Cisco DNA Center Platform User Guide</td>
</tr>
<tr>
<td>Cisco DNA Center platform release information, including new features, deployment, and open bugs.</td>
<td>Cisco DNA Center Platform Release Notes</td>
</tr>
<tr>
<td>For This Type of Information...</td>
<td>See This Document...</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Licenses and notices for open source software used in Cisco DNA Center platform.</td>
<td>Open Source Used in Cisco DNA Center Platform</td>
</tr>
<tr>
<td>Key features and scale numbers.</td>
<td>Cisco DNA Center Data Sheet</td>
</tr>
<tr>
<td>Use of the Cisco Wide Area Bonjour Application GUI.</td>
<td>Cisco Wide Area Bonjour Application User Guide</td>
</tr>
<tr>
<td>Use of the Stealthwatch Security Analytics Service on Cisco DNA Center.</td>
<td>Cisco Stealthwatch Analytics Service User Guide</td>
</tr>
</tbody>
</table>